



# Exchange 2010 Deployment Guide

Revised December 2010

**Worldwide 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

Copyright © 2000 - 2010 KEMP Technologies, Inc. All rights reserved.

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 and Exchange 2010 Client Access Server are registered trademarks of Microsoft Corporation. All other trademarks and registered trademarks are the property of their respective owners.

# Table of Contents

About KEMP Technologies .....	4
Load Balancing Microsoft Exchange Server 2010 .....	4
About This Manual .....	5
Prerequisites .....	5
Exchange 2010 Overview .....	6
Understanding Server Load Balancing .....	6
Advantages to using a KEMP LoadMaster .....	8
Optimizing the KEMP LoadMaster for Exchange 2010 .....	9
SSL Acceleration (SSL Offloading).....	9
L7 Transparency.....	10
Compression .....	11
Caching .....	11
Persistence.....	11
Idle Connection Timeout.....	11
Port.....	12
Connection Scaling.....	12
Header Rewriting.....	12
Load Balancing Client Access Server Services .....	13
Configuring KEMP LoadMaster with a Consolidated Virtual Service for HTTPS- based Exchange 2010 Clients and Services.....	14
Configuring a Virtual Service for HTTPS-based services (with SSL Offload) .....	15
Configuring KEMP LoadMaster for Outlook MAPI .....	18
Configuring KEMP LoadMaster with unique Virtual Services .....	20
Exchange ActiveSync (EAS) .....	27
Outlook Anywhere (OA) .....	30
Exchange Web Services (EWS).....	33
Autodiscover Service (AS) .....	35
Internet Message Access Protocol (IMAP4) .....	39
Post Office Protocol (POP3).....	42
Edge Transport Servers .....	45
Configuring KEMP LoadMaster for SMTP .....	45
Appendix.....	48
Connection Scaling For Large Scale Deployments.....	48
Logging X-Forwarded-For .....	49
Configuration Table .....	50
Acronyms .....	51

## About KEMP Technologies

Since 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 Exchange Server 2010

The big changes Microsoft has made to its core server architecture in Exchange 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 Exchange 2010 strategy to emphasize scale-out, rather than scale-up, making the right load balancing solution more critical than ever. Now that Exchange 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.

KEMP LoadMaster 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), Exchange 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 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 (631) 345-5292.

## About This Manual

This manual addresses how to deploy and configure a LoadMaster appliance with Microsoft Exchange 2010. Specifically, configuration information applies to Outlook Web App (OWA), Exchange Control Panel (ECP), Exchange ActiveSync (EAS), Outlook Anywhere (OA), Internet Message Access Protocol (IMAP), Post Office Protocol (POP), RPC Client Access (RPC CA), Exchange Address Book service (EAB), AutoDiscover (AS), Offline Address Book (OAB), Exchange 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 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. Documentation is available at <http://www.kemptechnologies.com/documentation>.

At a minimum, you should have:

- Installed your Microsoft Exchange Servers, Active Directories and followed other Microsoft requirements.
- Installed LoadMaster on the same network as the Exchange 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>).

## Exchange 2010 Overview

Microsoft Exchange Server 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 Exchange 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 Exchange 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.

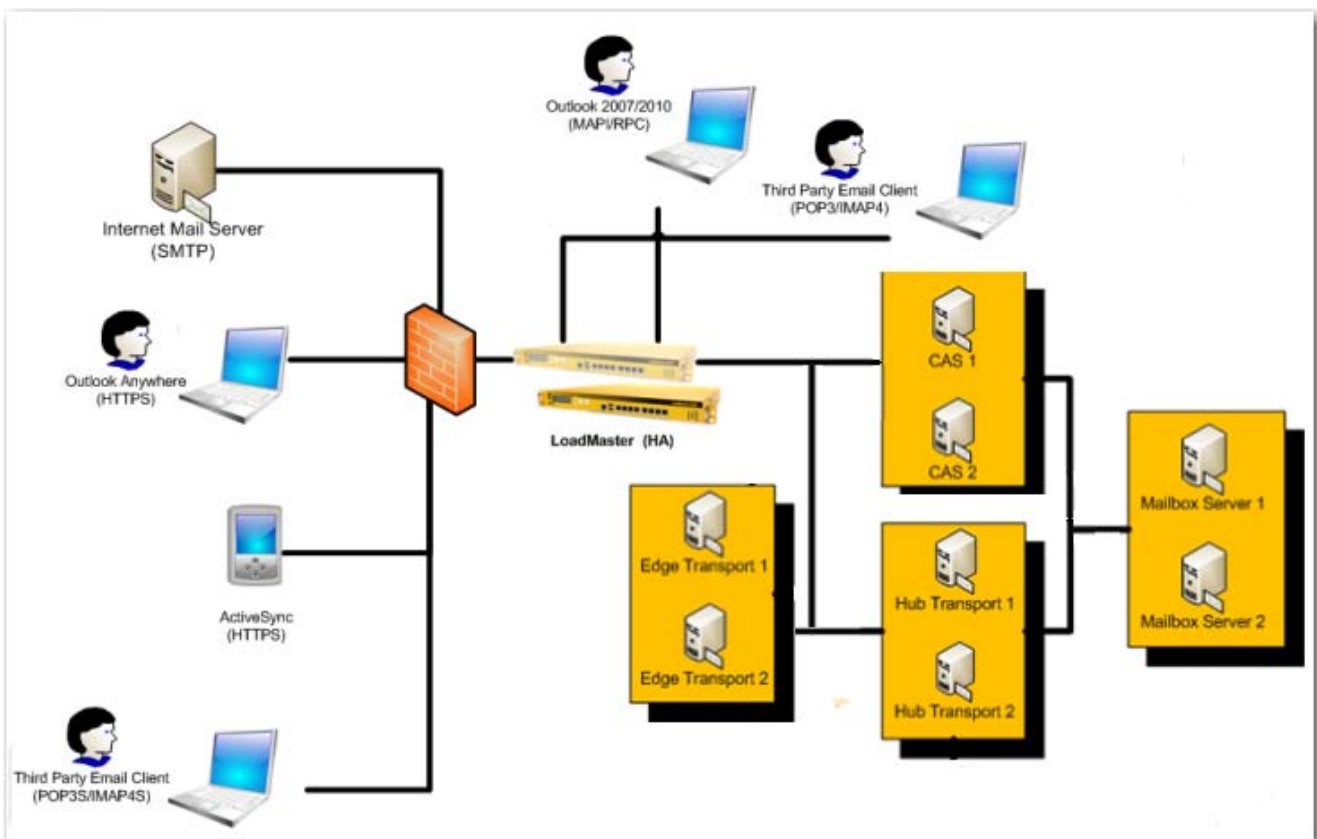
Server load balancing reduces the impact of a single Client Access Server failure within one of your Active Directory sites and ensures that the load on your Exchange Servers is evenly distributed. Architectural changes with respect to earlier versions of Exchange make server load balancing even more 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 Exchange. 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 Exchange or service pack versions of Exchange within the same array.

Several changes in Exchange 2010 make server load balancing important for your organization. The Exchange 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 Exchange, 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

KEMP LoadMasters offer 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), Exchange 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 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. For example, the KEMP LoadMaster has options to prefer one or more CAS servers over other via features such as weighted round robin, least connection and so on.

## Optimizing the KEMP LoadMaster for 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 cookie-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 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. Cookie 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 cookie 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

Enabling this option makes the Virtual Service transparent (non-NAT'd). However, if the client resides on the same subnet as the Virtual IP and Real Servers the Virtual Services will automatically NAT the source IP (enable non-transparency).

To avoid IP routing problems, simply disable L7 Transparency. Keep in mind though; as a result your Real Servers will only "see" the LoadMaster as the source of all traffic. If that is not an option for you, enable L7 transparency and ensure the following:

- a) The Real Server settings must ensure that all client requests are routed through the LoadMaster. Typically, this is achieved by making the LoadMaster the Real Server's default gateway.
- b) Clients must not be in the same IP subnet with the Real Servers.

**Note:** Virtual Services operating on L4 always act transparently.

## Compression

The LoadMaster data compression feature reduces the amount of data to be transferred for HTTP objects by utilizing gzip compression available in all modern web browsers. Leveraging Lempel-Ziv (LZ) compression and HTTP/1.1 GNU zip (gzip) content encoding reduces bandwidth utilization for high compression files such as text files (HTML, CSS, and JavaScript). Data compression allows LoadMaster to compress the application payload per request, reducing network bandwidth consumption without degrading content quality and response time resulting in an improvement for the end-users' overall experience. Data compression is supported on all files. Compression ratios vary by file type.

The compression feature should be deployed simultaneously with the caching feature to reduce the real-time inline compression requirements. Using only compression can potentially bottleneck Virtual Service throughput depending on hardware platform.

## Caching

The LoadMaster advanced caching engine saves valuable Real Server processing power and bandwidth, which can be dedicated to performing critical core business application logic. Significant server performance gains can be achieved when implementing caching. Chatty protocols such as HTTP require frequent creating and closing of connections for fetching of static resources, creating unnecessary resource utilization on Real Server(s) and the network. By enabling LoadMaster caching you can re-purpose connection related resources for more relevant business logic. By deploying LoadMaster caching your organization can reduce web traffic to Real Server(s) saving on bandwidth in-front of your Real Server(s).

## 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 Exchange 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 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 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. If you wish to use URL rewriting, you may wish to execute the Header Rewriting procedure located in the Appendix of this manual.

## Load Balancing Client Access Server Services

In this section provides step by step instructions on how you configure the KEMP LoadMaster to load balance the different services on the Exchange 2010 Client Access server role. But first each service handled by the Client Access server role is listed with a brief description:

- **Outlook Web App** Outlook Web App (OWA) is enabled by default when you install the Client Access server role. OWA lets you access your Exchange mailbox from a Web browser. In previous versions of Exchange, 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.
- **Exchange Control Panel** The Exchange 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 Exchange mailbox from a Web browser. It replaces the old OWA options page included with previous version of Exchange 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 Exchange 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 Exchange 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 Exchange 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.
- **Exchange ActiveSync** Exchange 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 Exchange 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 Exchange. 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. Exchange 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).

- **Exchange Web Services** The Exchange 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 Exchange.
- **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.
- **Exchange Address Book Service** The Exchange 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), Exchange Control Panel (ECP), Outlook Anywhere (OA), Offline Address Book (OAB), Exchange ActiveSync (EAS), Exchange Web Services (EWS) and the Autodiscover service.

Using a single virtual service keeps the load balancer configuration simple and let you have a single fully qualified domain name (FQDN) and associated SSL certificate for all Exchange 2010 client access methods and services.

### Note

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 Exchange (as per Exchange 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\(W.S.10\).aspx](http://technet.microsoft.com/en-us/library/cc732341(W.S.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

Cancel Add this Virtual Service

3. Enter the **Virtual Address** using the format **###.###.###.###**.
4. Enter 443 as the **Port**.
5. Select **tcp** as the **Protocol**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, "Exchange 2010 HTTPS". Click **Set Nickname**.

8. 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.
9. 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 Exchange 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.
10. 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.
11. For **Rewrite Rules**, use the drop down list and select **HTTPS**.
12. 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**.
13. For **Persistence Options**, select **Super HTTP** as the **Mode**. Use the **Timeout** drop down list to select **1 Hours**.
14. For **Real Server Check Parameters** select **HTTP Protocol**. Input **"/rpc/rpcproxy.dll"** in the **URL:** edit window and click **Set URL**.
15. Select **round robin** as the **Scheduling Method**.
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**.

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

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

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 HTTPS-based services (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**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, "OA-EAS-EWS-WOSSL". Click **Set Nickname**.
8. Select the **Force L7** check box.
9. Deselect the **L7 Transparency** check box.
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 **255.255.255.255**.
11. For **Real Server Check Parameters** select **HTTPS Protocol**.
12. Select **round robin** as the **Scheduling Method**.
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**.

## 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 MAPI Endpoint Mapper (TCP/135)

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 135 as the **Port**.
5. Select **tcp** as the **Protocol**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, "MAPI-Endpoint". Click **Set Nickname**.
8. Select the **Force L7** check box.
9. Deselect the **L7 Transparency** check box.
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 **255.255.255.255**.
11. For **Real Server Check Parameters** select **TCP Connection Only**.
12. Select **least connection** as the **Scheduling Method**.
13. Enter 3600 as the **Idle Connection Timeout** and click **Set Idle Timeout**.
14. Add Real Servers. Click **Add New...**

15. For each CAS, input its IP address as the **Real Server Address** on **Port 135**. Click **Add This Real Server**.
16. Click **OK** in response to the confirmation that the Real Server was added.

### **Creating the Virtual Service for the RPC CA & 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.*
4. Select **tcp** as the **Protocol**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
5. Click **Add this Virtual Service**.
6. Enter a **Service Nickname**. This is for display purposes only. For example, "MAPI". Click **Set Nickname**.
7. Select the **Force L7** checkbox.
8. Deselect the **L7 Transparency** check box.
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. For **Real Server Check Parameters** select **TCP Connection Only**.
11. Select **least connection** as the **Scheduling Method**.
12. Enter 3600 as the **Idle Connection Timeout** and click **Set Idle Timeout**.
13. Add Real Servers. Click **Add New...**
14. Enter the same (step 15) **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 Exchange (as per Exchange 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**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, "Exchange 2010 OWA". Click **Set Nickname**.
8. 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.
9. 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 Exchange 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.
10. 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.

11. 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**.
12. For **Persistence Options**, select **Active Cookie** as the **Mode**. Use the **Timeout** drop down list to select **15 Minutes**. You may safely leave **Cookie Name** blank.
13. For **Real Server Check Parameters** select **HTTP Protocol**. Input **"/owa"** in the **URL:** edit window and click **Set URL**.
14. Select **round robin** as the **Scheduling Method**.
15. Input 900 as the **Idle Connection Timeout** and click **Set Idle Timeout**.
16. Select the **Enable Caching** check box. Using the **Maximum Cache usage** drop down list, select **90%**.
17. Select the **Enable Compression** check box.
18. Select the **Detect Malicious Requests** check box.
19. 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.*
20. For **Not Available Redirection Handling**, input **"https://%h%s"** in the **Redirect URL:** edit window. Click **Set Redirect URL**.
21. Add Real Servers. Click **Add New...**
22. 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	<input type="text" value="80"/>
Forwarding method	<input type="text" value="nat"/>
Weight	<input type="text" value="1000"/>

23. Click **OK** in response to the confirmation that the Real Server was added.

24. 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)

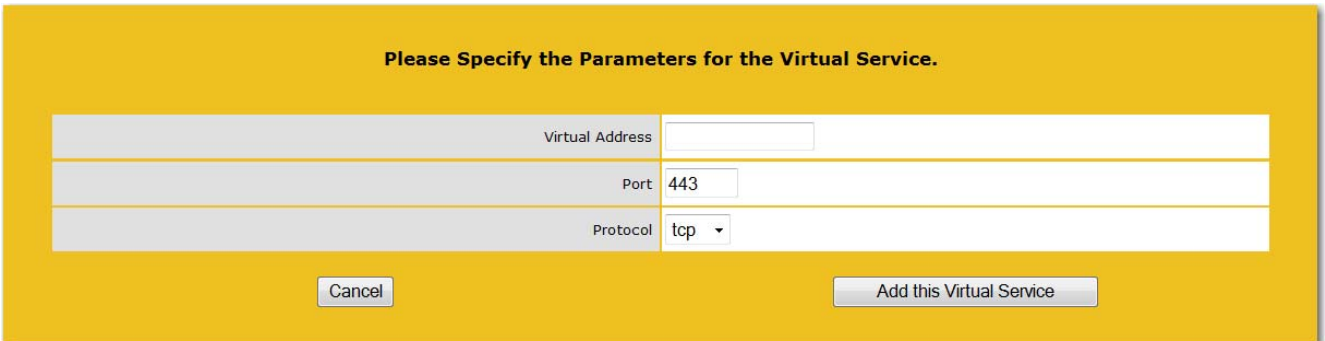
1. Connect and log in to your LoadMaster.
2. Create a virtual service. Click **Virtual Services** and then click **Add New**.
3. Enter the **Virtual Address** using the format *###.###.###.###*.
4. Enter 443 as the **Port**.
5. Select **tcp** as the **Protocol**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, "Exchange 2010 OWA WOSSL". Click **Set Nickname**.
8. Select the **Force L7** check box.
9. Deselect the **L7 Transparency** check box.
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 **255.255.255.255**.
11. For **Real Server Check Parameters** select **HTTPS Protocol**.
12. Select **round robin** as the **Scheduling Method**.
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**.

### **Exchange 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**.



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**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, “Exchange 2010 ECP”. Click **Set Nickname**.
8. 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.
9. 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 Exchange 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.

10. 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.
11. 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**.
12. For **Persistence Options**, select **Active Cookie** as the **Mode**. Use the **Timeout** drop down list to select **15 Minutes**. You may safely leave **Cookie Name** blank.
13. For **Real Server Check Parameters** select **HTTP Protocol**. Input **"/ecp"** in the **URL:** edit window and click **Set URL**.
14. Select **round robin** as the **Scheduling Method**.
15. Input 900 as the **Idle Connection Timeout** and click **Set Idle Timeout**.
16. Select the **Enable Caching** check box. Using the **Maximum Cache usage** drop down list, select **90%**.
17. Select the **Enable Compression** check box.
18. Select the **Detect Malicious Requests** check box.
19. 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.*
20. For **Not Available Redirection Handling**, input **"https://%h%s"** in the **Redirect URL:** edit window. Click **Set Redirect URL**.
21. Add Real Servers. Click **Add New...**
22. 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	<input type="text" value="80"/>
Forwarding method	<input type="text" value="nat"/>
Weight	<input type="text" value="1000"/>

23. Click **OK** in response to the confirmation that the Real Server was added.
24. 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**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, "Exchange 2010 ECP WOSSL". Click **Set Nickname**.
8. Select the **Force L7** check box.
9. Deselect the **L7 Transparency** check box.
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 **255.255.255.255**.
11. For **Real Server Check Parameters** select **HTTPS Protocol**.
12. Select **round robin** as the **Scheduling Method**.
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**.

## Exchange ActiveSync (EAS)

### Configuring a Virtual Service for EAS (without 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-ActiveSyncVirtualDirectory cmdlet (<http://technet.microsoft.com/en-us/library/aa998363.aspx>).

#### Note

SSL offloading for Exchange 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**.

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**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, “Exchange 2010 EAS”. Click **Set Nickname**.
8. 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.

9. 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 Exchange 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.
10. 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.
11. For **Rewrite Rules**, use the drop down list and select **HTTPS**.
12. 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**.
13. For **Persistence Options**, select **Super HTTP** as the **Mode**. Use the **Timeout** drop down list to select **1 Hours**.
14. For **Real Server Check Parameters** select **HTTP Protocol**. Input **"/iisstart.html"** in the **URL:** edit window and click **Set URL**.
15. Select **round robin** as the **Scheduling Method**.
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**.

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

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

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**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, "Exchange 2010 EAS-WOSSL". Click **Set Nickname**.
8. Select the **Force L7** check box.
9. Deselect the **L7 Transparency** check box.
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 **255.255.255.255**.
11. For **Real Server Check Parameters** select **HTTPS Protocol**.
12. Select **round robin** as the **Scheduling Method**.
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**.

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**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, "Exchange 2010 OA". Click **Set Nickname**.
8. 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.
9. 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 Exchange 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.

10. 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.
11. For **Rewrite Rules**, use the drop down list and select **HTTPS**.
12. 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**.
13. For **Persistence Options**, select **Super HTTP** as the **Mode**. Use the **Timeout** drop down list to select **1 Hours**.
14. For **Real Server Check Parameters** select **HTTP Protocol**. Input “/rpc/rpcproxy.dll” in the **URL:** edit window and click **Set URL**.
15. Select **round robin** as the **Scheduling Method**.
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**.

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

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

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)

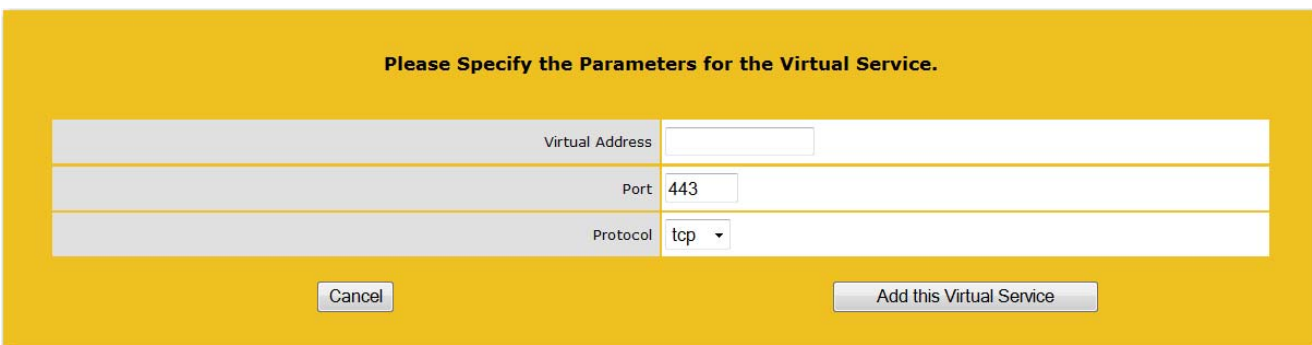
1. Connect and log in to your LoadMaster.
2. Create a virtual service. Click **Virtual Services** and then click **Add New**.
3. Enter the **Virtual Address** using the format *###.###.###.###*.
4. Enter 443 as the **Port**.
5. Select **tcp** as the **Protocol**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, "Exchange 2010 OA-WOSSL". Click **Set Nickname**.
8. Select the **Force L7** check box.
9. Deselect the **L7 Transparency** check box.
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 **255.255.255.255**.
11. For **Real Server Check Parameters** select **HTTPS Protocol**.
12. Select **round robin** as the **Scheduling Method**.
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**.

## Exchange 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**.



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**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, "Exchange 2010 EWS". Click **Set Nickname**.
8. 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.
9. 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 Exchange 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.

10. 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.
11. For **Rewrite Rules**, use the drop down list and select **HTTPS**.
12. 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**.
13. For **Persistence Options**, select **Super HTTP** as the **Mode**. Use the **Timeout** drop down list to select **1 Hours**.
14. For **Real Server Check Parameters** select **HTTP Protocol**. Input “/iisstart.html” in the **URL:** edit window and click **Set URL**.
15. Select **round robin** as the **Scheduling Method**.
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**.

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

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

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**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, "Exchange 2010 EWS-WOSSL". Click **Set Nickname**.
8. Select the **Force L7** check box.
9. Deselect the **L7 Transparency** check box.
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 **255.255.255.255**.
11. For **Real Server Check Parameters** select **HTTPS Protocol**.
12. Select **round robin** as the **Scheduling Method**.
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**.

**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**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, "Exchange 2010 AS". Click **Set Nickname**.
8. 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.
9. 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 Exchange 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.
10. 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.
11. For **Rewrite Rules**, use the drop down list and select **HTTPS**.

12. 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**.
13. For **Persistence Options**, select **Super HTTP** as the **Mode**. Use the **Timeout** drop down list to select **1 Hours**.
14. For **Real Server Check Parameters** select **HTTP Protocol**. Input “/iisstart.html” in the **URL:** edit window and click **Set URL**.
15. Select **round robin** as the **Scheduling Method**.
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**.

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

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

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**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, "Exchange 2010 AS". Click **Set Nickname**.
8. Select the **Force L7** check box.
9. Deselect the **L7 Transparency** check box.
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 **255.255.255.255**.
11. For **Real Server Check Parameters** select **HTTPS Protocol**.
12. Select **round robin** as the **Scheduling Method**.
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>.

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**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, "CAS-IMAP4-Secure". Click **Set Nickname**.
8. 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.
9. 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 Exchange 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.
10. 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.
11. 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**.

12. For **Persistence Options**, select **None**.
13. For **Real Server Check Parameters** select **Mailbox (IMAP) Protocol**.
14. Select **least connection** as the **Scheduling Method**.
15. Enter 3600 as the **Idle Connection Timeout** and click **Set Idle Timeout**.
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**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, "CAS-IMAP4-WOSSL". Click **Set Nickname**.
8. Select the **Force L7** check box.
9. Deselect the **L7 Transparency** check box.
10. For **Persistence Options**, select **None**.
11. For **Real Server Check Parameters** select **Mailbox (IMAP) Protocol**.
12. Select **least connection** as the **Scheduling Method**.
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**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, "CAS-POP3-Secure". Click **Set Nickname**.
8. 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.
9. 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 Exchange 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.
10. 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.

11. 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**.
12. For **Persistence Options**, select **None**.
13. For **Real Server Check Parameters** select **Mailbox (POP3) Protocol**.
14. Select **least connection** as the **Scheduling Method**.
15. Input 3600 as the **Idle Connection Timeout** and click **Set Idle Timeout**.
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**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Input a **Service Nickname**. This is for display purposes only. For example, "CAS-POP3-WOSSL". Click **Set Nickname**.
8. Select the **Force L7** check box.
9. Deselect the **L7 Transparency** check box.
10. For **Persistence Options**, select **None**.
11. For **Real Server Check Parameters** select **Mailbox (POP3) Protocol**.

12. Select **least connection** as the **Scheduling Method**.
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**.

## Edge Transport Servers

### Configuring KEMP LoadMaster for SMTP

In Microsoft Exchange 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 Exchange 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 Exchange 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 Exchange 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**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Input a **Service Nickname**. This is for display purposes only. For example, "Hub-Edge-Secure". Click **Set Nickname**.
8. Select the **Force L7** check box.
9. Use the **Server Initiating Protocols** drop down list and select **SMTP**.
10. 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.
11. 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 Exchange 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.
12. 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.
13. 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**.
14. For **Persistence Options**, select **None**.
15. For **Real Server Check Parameters** select **Mail (SMTP) Protocol**.
16. Select **least connection** as the **Scheduling Method**.
17. Input 120 as the **Idle Connection Timeout** and click **Set Idle Timeout**.
18. Add Real Servers. Click **Add New...**
19. For each Hub Transport Server, input its IP as the **Real Server Address** on **Port 25**. 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 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**. *Note that the combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Enter a **Service Nickname**. This is for display purposes only. For example, "Hub-Edge-WOSSL". Click **Set Nickname**.
8. Select the **Force L7** check box.
9. Use the **Server Initiating Protocols** drop down list and select **SMTP**.
10. For **Persistence Options**, select **None**.
11. For **Real Server Check Parameters** select **Mail (SMTP) Protocol**.
12. Select **least connection** as the **Scheduling Method**.
13. Enter 120 as the **Idle Connection Timeout** and click **Set Idle Timeout**.
14. Add Real Servers. Click **Add New...**
15. For each Hub Transport Server, input its IP as the **Real Server Address** on **Port 25**. 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**.

# Appendix

## Persistence Methods Supported by each Exchange 2010 CAS Service

	Workload	Preferred Session Persistence Method
HTTP-Based Workloads	Outlook Web App (OWA)	1. Client IP 2. Cookie
	Exchange Control Panel (ECP)	1. Client IP 2. Cookie
	Exchange ActiveSync (EAS)	1. Client IP 2. Authorization header
	Exchange Web Services (EWS)	1. Cookie 2. SSL ID
	Outlook Anywhere (OA)	1. Client IP 2. No affinity/persistence
	Offline Address Book (OAB)	1. Client IP 2. SSL ID
	Autodiscover Service (AS)	No affinity/persistence
TCP Socket Oriented Workloads	RPC Client Access Service (RPC CA)	1. Client IP
	Exchange Address Book (EAB)	1. Client IP
	RPC Endpoint Mapper	1. Client 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.

1. You must disable L7 Transparency in order to use connection scaling.
2. To use connection scaling, click **System Configuration**.

3. Click **Miscellaneous Options**.
4. Click **L7 Configuration**.
5. Use the **Allow connection scaling over 64K Connections** drop down list and select **Yes**.

Allow connection scaling over 64K Connections Yes ▾

6. Click **Virtual Services**.
7. Click **View/Modify Services**.
8. Click the **Modify** button of the appropriate (presumably just created) Virtual IP Address.
9. 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.
10. Click the **Set Alternate Addresses** button.
11. Return to the next step of the configuration procedure you were following prior to executing this procedure.

## Logging X-Forwarded-For

If your HTTP/HTTPS Virtual Service is Non-Transparent you can still obtain source IP information on the Real Servers. LoadMaster will inject an HTTP Header with the client IP, which can be logged on your Web Server. To enable header injection and logging:

1. To enable source IP injection via X-Forwarded-For, click **System Configuration**.
2. Click **Miscellaneous Options**.
3. Click **L7 Configuration**.
4. Use the Additional L7 Header drop down list to select **X-Forwarded-For**.

Additional L7 Header X-Forwarded-For ▾

5. Follow the instructions at the following URL:  
<http://blogs.msdn.com/b/david.wang/archive/2005/09/28/howto-isapi-filter-which-logs-original-client-ip-for-load-balanced-iis-servers.aspx>. The instructions at the aforementioned URL are carried out on you Real Server and not the LoadMaster.

## Configuration Table

The following 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: "/owa"	80/TCP, 443/TCP (SSL)	round robin	Enabled
IMAP4	Mailbox (IMAP) Protocol	143/TCP (TLS), 993/TCP (SSL)	least connection	Disabled Enabled
MAPI (RPC)	TCP Connection Only	135/TCP, TCP 1024-65535	least connection	Disabled
OA	HTTP Protocol URL: "/owa"	80/TCP, 443/TCP (SSL)	round robin	Enabled
OWA	HTTP Protocol URL: "/owa"	80/TCP, 443/TCP (SSL)	round robin	Enabled
POP3	Mailbox (POP3) Protocol	110/TCP (TLS), 995/TCP (SSL)	least connection	Disabled Enabled
SMTP	Mail (SMTP) Protocol	25/TCP 587/TCP (SSL)	least connection	Disabled Enabled

## Acronyms

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	Exchange ActiveSync
ECP	Exchange Control Panel
EWS	Exchange Web Services
FQDN	Fully Qualified Domain Name
IMAP4	Internet Message Access Protocol
MAPI	Messaging Application Program Interface
MX	Mail Exchange
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 Exchange 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
UDP	User Datagram Protocol
VIP	Virtual IP
WNLB	Windows Network Server load balancing