Progress®
Kemp® LoadMaster®

Deployment Guide MS Exchange 2010

Generated on: 16 September 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 6

Load Balancing Microsoft Exchange Server 2010 6

About This Manual 7

Prerequisites 7

Chapter 2: Exchange 2010 Overview 8

Understanding Server Load Balancing 9

Optimizing the LoadMaster for Exchange 2010 10

SSL Acceleration (SSL Offloading) 10

Persistence 11

Idle Connection Timeout 11

Drop Connections on Real Server Failure 12

Drop at Drain Time End 12

Port Configuration 12

Connection Scaling 12

Header Rewriting 13

Preconfigured Virtual Services 13

RPC Client Access Service 13

Hub-Edge-SMTP 13

Enforce Secure Access 14

All HTTPS Services 14

Chapter 3: Virtual Service Templates 15

Chapter 4: Load Balancing CAS Services 17

Configuring LoadMaster with a Consolidated Virtual Service for HTTPS-based Exchange 2010 Clients and Services 19

Configuring a Virtual Service for HTTPS-based services (with SSL Offload and without ESP) 19

Configuring a Virtual Service for HTTPS-based services (with SSL Offload and with ESP) 22

Create the Content Rules 22

Configure the Virtual Service 24

Configuring a Virtual Service for HTTPS-based Services (without SSL Offload) 30

Configuring the HTTP Redirect Virtual Service 31

Configuring the LoadMaster for Outlook MAPI 32

Creating the Virtual Service for the RPC CA (MAPI) & Address Book Service 32

Configuring the LoadMaster with Unique Virtual Services 34

Outlook Web App (OWA) 34

Control Panel (ECP) 38

ActiveSync (EAS) 41

Outlook Anywhere (OA) 44

Web Services (EWS) 48

Autodiscover Service (AS) 51

Internet Message Access Protocol (IMAP4) 55

Post Office Protocol (POP3) 59

Simple Mail Transfer Protocol (SMTP) 64

Importing and Assigning an SSL Certificate 71

Chapter 5: Exchange 2010 Site Resiliency and Progress Kemp GEO LoadMaster 73

Exchange 2010 Data Center Failover 73

Chapter 6: Appendix A: Connection Scaling For Large Scale Deployments 76

Chapter 7: Appendix B: Persistence Methods Supported by Each CAS Service 78

Chapter 8: Appendix C: Configuration Table 80

Chapter 9: Glossary 85

Chapter 10: References 88

1

Introduction

Since the year 2000, and with thousands of customers world-wide, Progress 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. Progress Kemp's LoadMaster family of purpose-built hardware and Virtual Load Masters (VLMs) offer advanced Layer 4 and Layer 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.

Related Links

- Load Balancing Microsoft Exchange Server 2010
- About This Manual
- Prerequisites

Load Balancing Microsoft Exchange Server 2010

The 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), ActiveSync (EAS), Simple Mail Transfer Protocol (SMTP), Post Office Protocol version 3 (POP3), Internet Message Access Protocol version 4 (IMAP4) and Remote Procedure Call (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 (CASs). Layer 7 health checking at the LoadMaster ensures that if one of the servers and/or workloads become inaccessible, the load balancer will take that server offline, while automatically re-routing and reconnecting users to other functioning servers.

The entire LoadMaster product family, including the Virtual LoadMaster (VLM) supports Microsoft 2010.

About This Manual

This manual addresses how to deploy and configure a LoadMaster appliance with Microsoft Exchange 2010.

The 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 and at the same time you need to access a website then you should do so in a new and different browser session (that is, 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 the Exchange 2010 environment has been set up and the LoadMaster has been installed.

LoadMaster documentation is available at https://docs.progress.com.

At a minimum, you should have:

- Installed the Microsoft Servers, Active Directories and followed other Microsoft requirements
- Installed the LoadMaster on the same network as the servers.
- Established access to the LoadMaster Web User Interface (WUI)
- Created a Client Access array using the “New-ClientAccessArray” cmdlet (see steps at http://technet.microsoft.com/en-us/library/ee332317.aspx).

We recommend changing the default gateway on the Real Servers to point to the LoadMaster. This allows accurate server-side access logging of client IP addressing. We recommend performing this change during a maintenance window to avoid disruption of customer traffic.

2

Exchange 2010 Overview

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

High availability and site resilience: You have the option of deploying two Active Directory (AD) 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 are 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 did not complete.

Related Links

- Understanding Server Load Balancing
- Optimizing the LoadMaster for Exchange 2010
- Preconfigured Virtual Services

Understanding Server Load Balancing

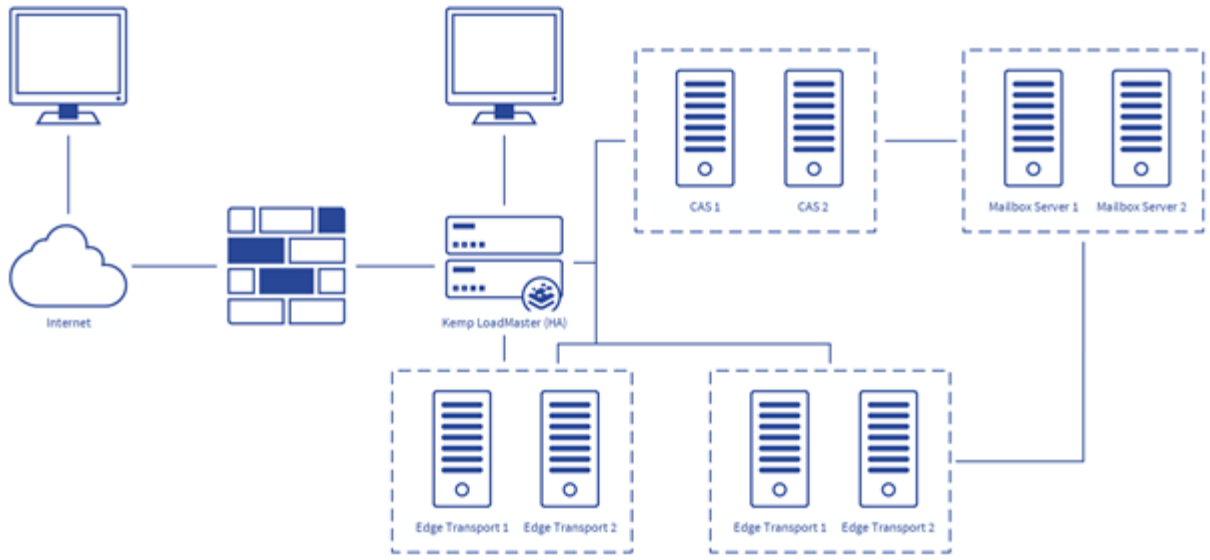
Server load balancing is a way to manage which servers receive traffic. Server load balancing provides failover redundancy to ensure users continue to receive service in case of failure. It also enables your deployment to handle more traffic than one server can process while offering a single host name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

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

Server load balancing reduces the impact of a single CAS 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 Exchange make server load balancing even more important than in the past. A load-balanced array of CASs is recommended for each Active Directory site and for each version of Exchange. It is not possible to share one load-balanced array of CASs for multiple Active Directory sites or to mix different versions of or service pack versions of within the same array.

Several aspects of Exchange 2010 make server load balancing important. The RPC CAS on the CAS 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 CAS 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 CAS role, both external and internal Outlook connections must be load-balanced across the array of CASs in a deployment to achieve fault tolerance and optimal performance.

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



When a 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 is sent to an Exchange 2010 CAS server in the CAS array using any available 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 LoadMaster for Exchange 2010

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

Related Links

- SSL Acceleration (SSL Offloading)
- Persistence
- Idle Connection Timeout
- Drop Connections on Real Server Failure
- Drop at Drain Time End
- Port Configuration
- Connection Scaling
- Header Rewriting

SSL Acceleration (SSL Offloading)

The 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 Transactions Per Second (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.

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).

Using cookies with Outlook 2003 on Windows XP is not supported by Microsoft. The client does not know how to handle this extra information and will close down the connection. Outlook 2007 is able to work but Progress Kemp recommends using **Source IP Address** persistence. Only clients running Windows 7 and above, running Outlook 2010 or newer can use cookies without problems. Cookies may work with Outlook 2003 and 2007 on Windows 7 but it is not supported by Microsoft. If having difficulty, the best option for these clients is to use **Source IP Address** persistence. Another recommendation is to turn off additional headers as these can also cause problems.

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 can be adjusted per service type by modifying the **Idle Connection Timeout** field in the **Standard Options** section of the Virtual Service modify screen.

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

Note: Setting the **Idle Connection Timeout** to **0** ensures that the default L7 connection timeout is used. You can modify the default **Connection Timeout** value by going to **System Configuration > Miscellaneous Options > Network Options**.

Drop Connections on Real Server Failure

By default existing connections are not closed if a Real Server fails. This can lead to issues with Outlook clients if an Exchange CAS server fails. A solution to this is to enable the **Drop Connections on RS Failure** option which can be found on the **System Configuration > Miscellaneous > L7 Configuration** screen in the WUI.

When this option is enabled, LoadMaster tracks all the incoming connections and which Real Servers they are connected to. When a Real Server fails, all connections to the Real Server are immediately dropped, forcing the connections to reconnect to a different Real Server.

Enabling this option has the added benefit of allowing relatively higher Idle Connection Timeout values to be set as the danger of the client retaining a connection to a failed server is removed.

Drop at Drain Time End

By default existing connections are not closed when a real server is disabled. This can lead to issues with Outlook clients if an Exchange CAS server is administratively disabled. A solution to this is to enable the **Drop at Drain Time End** option which can be found on the **System Configuration > Miscellaneous > L7 Configuration** screen in the WUI.

When this option is enabled, LoadMaster will sever all existing connections to a disabled server after the L7 Connection Drain Time is reached. Clients will then be forced to re-establish a connection to one of the remaining Real Servers.

For further details on the **Drop at Drain Time End** and **L7 Connection Drain Time** fields, refer to the L7 Configuration section of the WUI Configuration Guide.

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 Request For Comment (RFC). However, your 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 Appendix A: Connection Scaling For Large Scale Deployments.

Header Rewriting

Your 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. For more information, refer to the **Content Rules, Feature Description** on the Documentation Page.

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.

Note: The LoadMaster Exchange is a deprecated product and is no longer available for purchase.

The four preconfigured services are described in the sections below.

Related Links

- RPC Client Access Service
- Hub-Edge-SMTP
- Enforce Secure Access
- All HTTPS Services

RPC Client Access Service

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

The change in Exchange 2010 to move all processing to the CAS was implemented to provide all data access through a single, common path of the CAS. 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 a perimeter network. Designed to minimize the attack surface, the Edge Transport server handles all Internet-facing mail flow, which provides Simple Mail Transfer Protocol (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 are 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, the 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 all services are provided using a single FQDN, a simple single SSL certificate can be installed to provide security for all connections. Alternatively, these services can be provided on distinct FQDNs by installing a Unified Communications Certificate (UCC) (multi-named) certificate and setting DNS resolution for all FQDNs to the same virtual IP address.

Note: These Virtual Services are treated as any other Virtual Service and may be modified or deleted, as required.

Note: The LoadMaster Exchange is a deprecated product and is no longer available for purchase.

3

Virtual Service Templates

Progress Kemp have developed templates containing our recommended settings for Exchange 2010. These templates can be installed on the LoadMaster and can be used when creating each of the Virtual Services. Using a template automatically populates the settings in the Virtual Services. This is quicker and easier than manually configuring each Virtual Service. If needed, you can make changes to any of the Virtual Service settings after using the templates.

Download released templates from the following page: LoadMaster Templates.

For more information and steps on how to import and use templates, refer to the Virtual Services and Templates, Feature Description.

For steps on how to manually add and configure the Virtual Services, refer to the sections below.

The Exchange 2010 templates currently available are grouped in three downloadable files as follows:

Core Services

This set contains templates for MAPI/RPC, SMTP and both SSL offloaded and SSL pass-through HTTP/HTTPS services.

This is the primary set of services needed to balance Exchange 2010.

Extended Services

This set contains individual templates for both SSL offloaded and SSL pass-through versions of services for OWA, EAS, OA, ECP, EWS, and AS.

These services are only necessary if you want to break out each service type into its own Virtual Service.

Additional Services

This set contains templates for IMAP, POP and SMTP services, including variants for STARTTLS and SSL secured services.

Note: If you create another Virtual Service using the same template, ensure to change the **Service Name** to a unique name.

When using SNMP monitoring of ESP-enabled Virtual Services that were created using a template, ensure to monitor each SubVS directly rather than relying on the master service. This is because the Authentication Proxy sub-service will always be marked as up and, as a consequence, so will the master service.

4

Load Balancing CAS Services

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

Each service handled by the 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 Exchange, a specific version of Internet Explorer was required 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 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 a mailbox from a web browser. It replaces the old OWA options page included with the previous version of Exchange Server.

Outlook Anywhere: Outlook Anywhere (OA), 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 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 CASs 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 only public folders are used for distributing the Offline Address Book (OAB).

ActiveSync: Exchange ActiveSync (EAS) is enabled by default when you install the CAS 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 are working offline.

Note: When using the Web Application Firewall (WAF) in a Microsoft Exchange environment, ensure to enable WAF at the SubVS level to avoid issues with ActiveSync because standard WAF is unable to interpret the protocols used by ActiveSync.

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 Exchange Web Services (EWS) is enabled by default when you install the CAS role. EWS is a web services Application Programming Interface (API) that can be used by 3rd party applications to access mailbox data. It is also used by various Microsoft applications and devices for integration with Exchange.

Autodiscover Service: The Autodiscover Service (AS) is enabled by default when you install the CAS 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. AS cannot be used with earlier versions of Outlook, including Outlook 2003.

RPC Client Access Service: The RPC Client Access (RPC CA) service is enabled by default when the Exchange 2010 Client Access Server role is installed. The RPC CA service handles the Outlook MAPI connections. The change in Exchange 2010 to move all processing to the CAS was implemented to provide all data access through a single, common path of the CAS. 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 CAS, in Exchange 2010, directory access is also handled by the CAS.

Address Book Service: The Exchange Address Book (EAB) service is enabled by default when you install the Exchange 2010 CAS 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 CAS 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 does not 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 CAS role. IMAP offers offline and online access, but like POP3, IMAP4 does not offer advanced collaboration features such as calendaring, contacts, and tasks.

Related Links

- Configuring LoadMaster with a Consolidated Virtual Service for HTTPS-based Exchange 2010 Clients and Services
- Configuring a Virtual Service for HTTPS-based services (with SSL Offload and without ESP)
- Configuring a Virtual Service for HTTPS-based services (with SSL Offload and with ESP)

- Configuring a Virtual Service for HTTPS-based Services (without SSL Offload)
- Configuring the LoadMaster for Outlook MAPI
- Configuring the LoadMaster with Unique Virtual Services

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

For most configurations, Progress 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 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 do not use port 443 like the above-mentioned client access methods and services.

In the configuration services below, refer to the Web User Interface (WUI), Configuration Guide for detailed descriptions of each of the WUI fields.

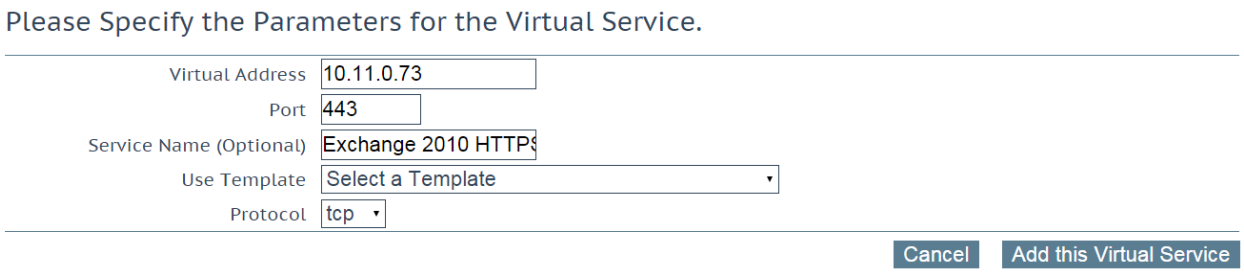
Configuring a Virtual Service for HTTPS-based services (with SSL Offload and without ESP)

Configuring a Virtual Service for HTTPS-based services (with SSL Offload and without ESP)

When you choose to offload SSL, you should follow the recommendations set by Microsoft. Progress Kemp understands these recommendations to be:

- Enable SSL Offloading for Exchange (as per instructions): http://social.technet.microsoft.com/wiki/contents/articles/1267.how-to-configure-ssl-offloading-in-exchange-2010-en-us.aspx
- Disable “Require SSL” on IIS: http://technet.microsoft.com/en-us/library/cc732341(WS.10).aspx.

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter a valid **Virtual Address**.
4. Enter **443** as the **Port**.
5. Enter a recognizable **Service Name**, for example Exchange 2010 HTTPS Offloaded.
6. Select **tcp** as the **Protocol**.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

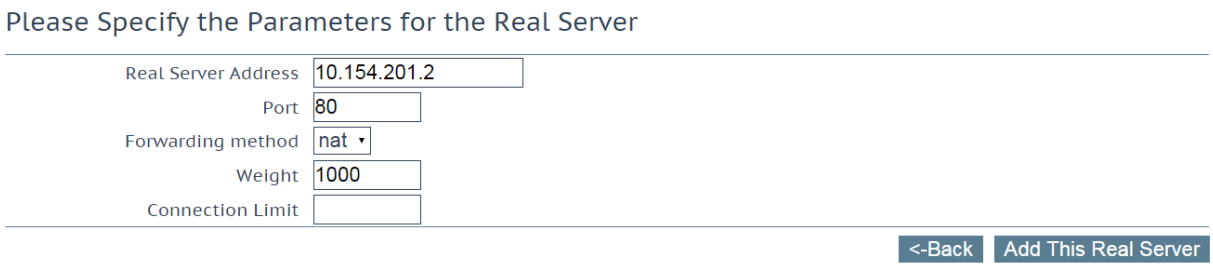
7. Click **Add this Virtual Service**.
8. Configure the settings as shown in the following table:

* By default, a self-signed certificate is used. Click **OK** when a message displays indicating that there is no SSL certificate currently available for your Virtual Service and that a temporary one is used until a valid certificate is installed. **Optional:** You can 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 to export the certificate and private key as a Personal Information File (PFX). An SSL certificate can also be obtained 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 the LoadMaster. **Optional:** You can import the appropriate PFX certificate and key file into the LoadMaster. For instructions on how to do this, refer to the Importing and Assigning an SSL Certificate section.

Section	Option	Value	Comment
SSL Properties	SSL Acceleration	Enabled*	
Standard Options	Transparency	Disabled	
	Persistence Mode	Super HTTP	
	Persistence Timeout	1 Hour	
	Scheduling Method	round robin	
	Idle Connection Timeout	900	Click **Set Idle Timeout**.
Advanced Properties	Add Header to Request	FRONT-END-HTTP:ON	Click **Set Header**.
	Redirect URL	https://%h%s	Click **Add HTTP Redirector**. This creates a redirect Virtual Service on port 80 with the same IP

Section	Option	Value	Comment
			address.
Real Servers	Real Server Check Method	HTTP Protocol	
	Checked Port	80	Click **Set Check Port**.
	URL		A URL must be entered and set in the **URL** text box. The URL varies depending on the service to be checked. Review the Configuration Table in Appendix C: Configuration Table. As an example, if you were configuring Outlook Web App (OWA), the URL would be **/owa**.

9. Click the **Add New...** button.



10. Enter the CAS address in the **Real Server Address** text box.
11. Ensure the **Port** is set to 80.
12. Click **Add This Real Server**.
13. Click **OK** in response to the confirmation that the Real Server was added.

To view, modify or delete any Virtual Services that have been added, select the **Virtual Services** > **View/ Modify Services** option in the main menu of the LoadMaster WUI.

The settings in the HTTP redirect Virtual Service need to be configured. To do this, follow the steps in the Configuring the HTTP Redirect Virtual Service section.

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

Refer to the sections below for instructions on how to configure a Virtual Service for HTTPS-based services (with SSL Offload and ESP).

Related Links

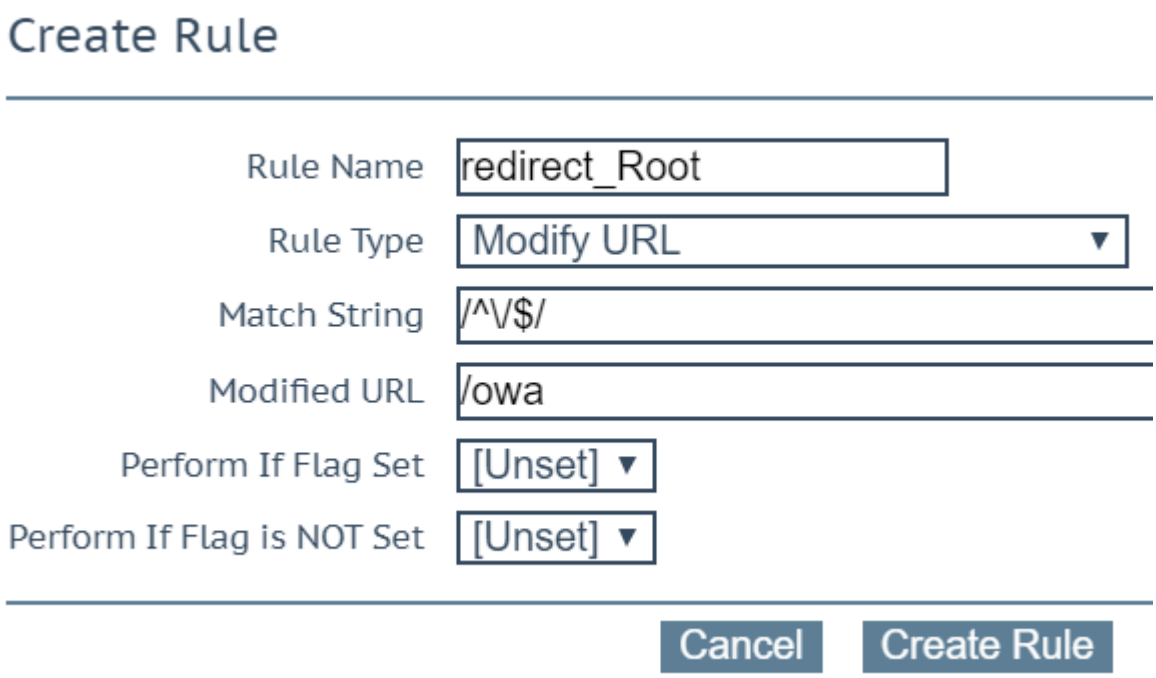
- Create the Content Rules
- Configure the Virtual Service

Create the Content Rules

Content Rules need to be created for the Virtual Service to function correctly.

To create the Modify URL rule for **owa** please complete the following steps:

1. Select the **Rules & Checking > Content Rules** menu option.
2. Click the **Create New** button.

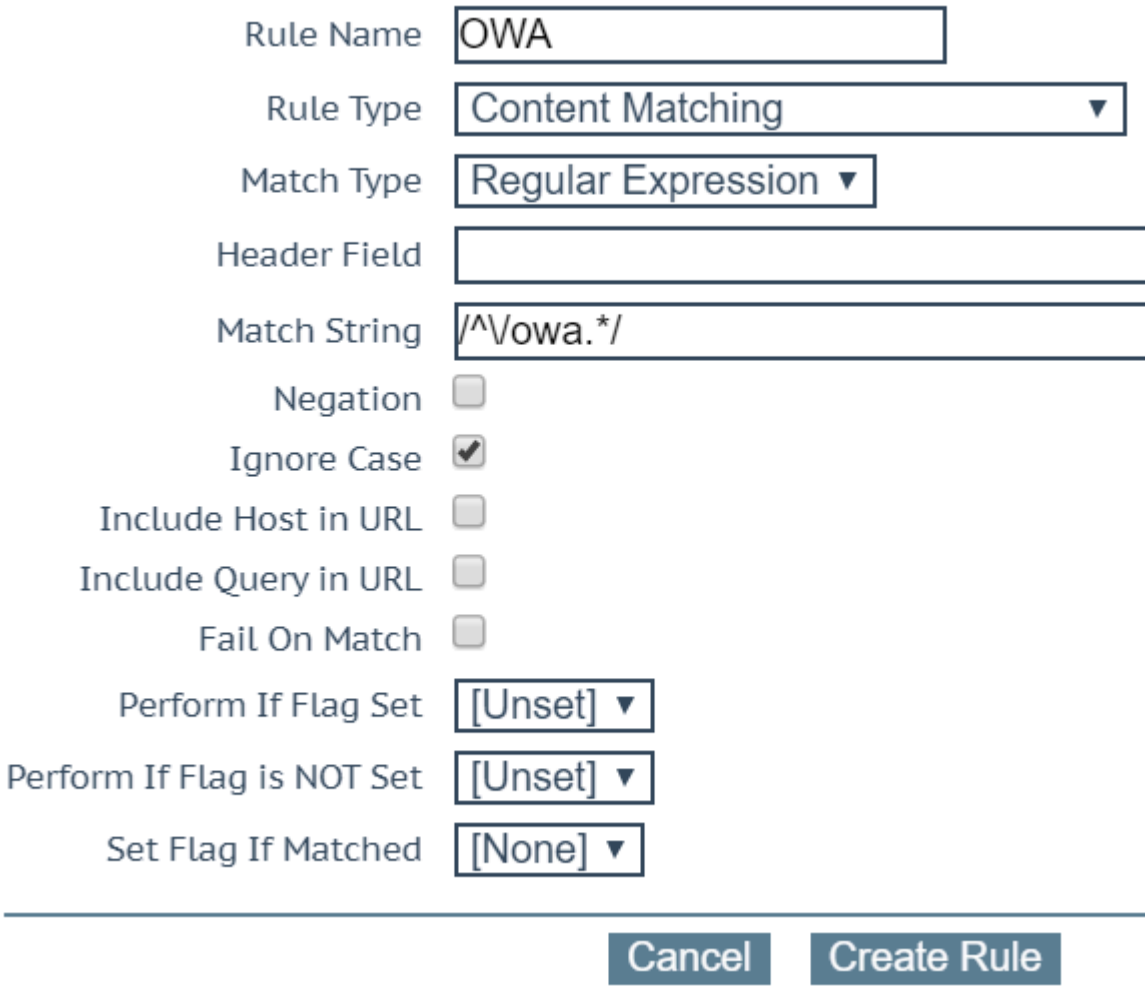


3. Enter a relevant name, for example **Redirect_Root** in the **Rule Name** field.
4. Select the **Modify URL** option in the **Rule Type** drop-down.
5. Enter **/^\/$/** in the **Match String** field.
6. Enter **/owa** in the **Modified URL** field.

7. Click the **Create Rule** button.
8. To create a Content Matching rule for **owa** please complete the following steps:
9. Select the **Rules & Checking > Content Rules** menu option.



10. Click the **Create New** button.
11. Enter a relevant name, for example **OWA** in the **Rule Name** field.



12. Select the **Content Matching** option is selected in the **Rule Type** drop-down list.
13. Ensure the **Regular Expression** option is selected in the **Match Type** drop-down list.
14. Enter /^\/owa.*/ in the **Match String** field.
15. Select the **Ignore Case** checkbox.
16. Click the **Create Rule** button.

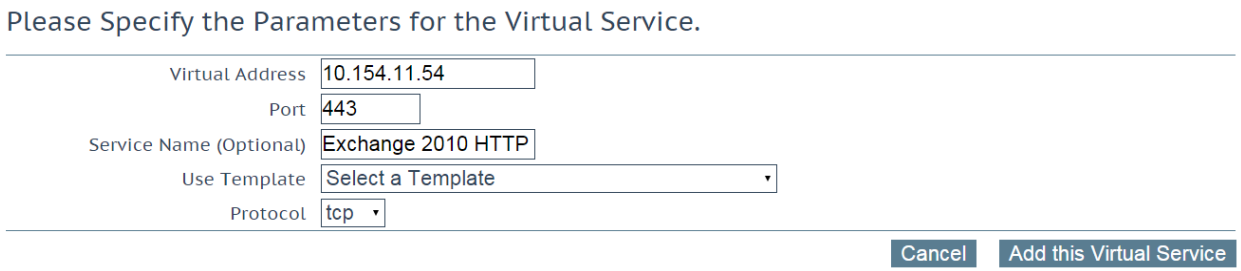
Create additional Content Matching rules following steps 1 to 8 above but using the values as described in the table below.

Rule Name	Match String	Ignore Case
ActiveSync	/^\/microsoft-server-activesync.*/	yes
Autodiscover	/^\/autodiscover.*/	yes
ECP	/^\/ecp.*/	yes
EWS	/^\/ews.*/	yes
OAB	/^\/oab.*/	yes
PowerShell	/^\/powershell.*/	yes
RPC	/^\/rpc.*/	yes
Root	/^\/$/	No
Authentication Proxy	/^\/lm_auth_proxy.*$/	Yes

Configure the Virtual Service

To configure a Virtual Service for HTTPS-based services, with SSL offloading and ESP enabled, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services > Add New**.

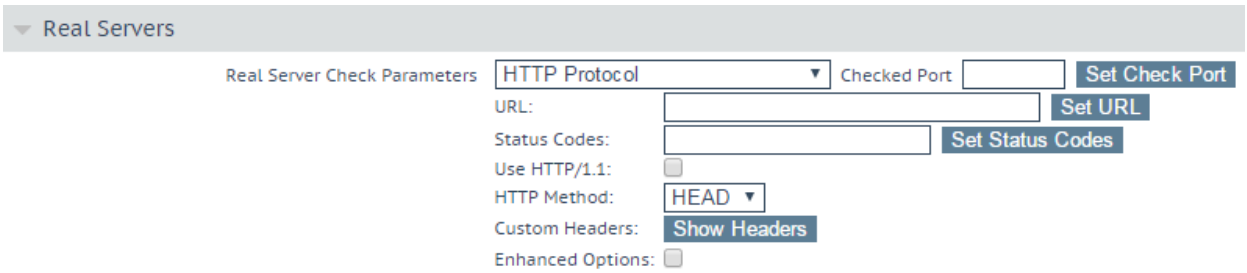


2. Enter a valid **Virtual Address**.
3. Enter **443** as the **Port**.
4. Enter a recognizable **Service Name**.
5. Click **Add this Virtual Service**.
6. Configure the settings as shown in the following table:

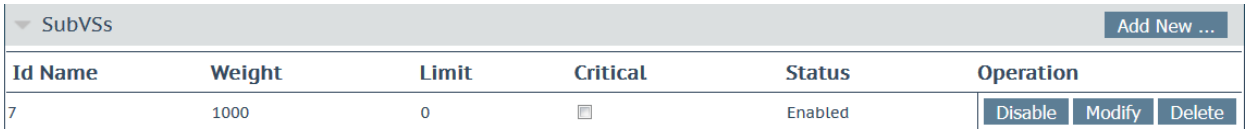
   * By default, a self-signed certificate is used. Click **OK** when a message displays indicating that there is no SSL certificate currently available for your Virtual Service and that a temporary one is used until a valid certificate is installed. **Optional:** You can export the appropriate certificate and key from Exchange 2010 using the Microsoft export information found at http://technet.microsoft.com/en-us/library/bb310778.aspx. Ensure to export the certificate and private key as a Personal Information File (PFX). An SSL certificate can also be obtained 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 the LoadMaster. **Optional:** You can import the appropriate PFX certificate and key file into the LoadMaster. For instructions on how to do this, refer to the Importing and Assigning an SSL Certificate section.

Section	Option	Value	Comment
SSL Properties	SSL Acceleration	Enabled*	Click **OK**.
Standard Options	Transparency	Disabled	
	Idle Connection Timeout	900	Click **Set Idle Timeout**.
Advanced Properties	Click **Show Header Rules**.	Select the **Modify URL** rule.	Click **Add**. Then, click **Back**.
	Add Header to Request	FRONT-END-HTTP:ON	Click **Set Header**.
	Redirect URL	https://%h%s	Click **Add HTTP Redirector**. This creates a redirect Virtual Service on port 80 with the same IP address.

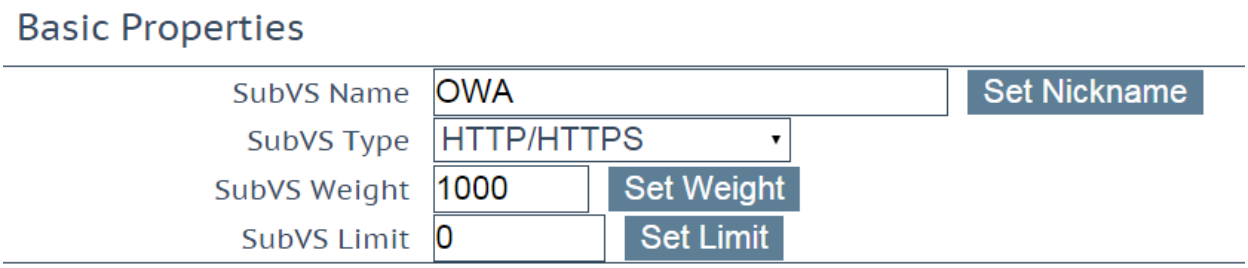
7. Now the SubVSs need to be added. Expand the **Real Servers** section.



8. Click **Add SubVS**.
9. Click **OK**.



10. To configure the SubVS, click **Modify**.



11. Configure the settings as shown in the following table:

* There are several characters that are not supported. These are the grave accent character (` ) and the single quotes (’). If a grave accent character is used in the **SSO Greeting Message**, the character does not display in the output. For example, a`b`c becomes abc. If a single quote is used, users will not be able to log in.

Section	Option	Value	Comment
Basic Properties	SubVS Name		Enter a recognizable name, for example **OWA**, and click **Set Nickname**.
Standard Options	Transparency	Disabled	
	Persistence Mode	Super HTTP	
	Persistence Timeout	1 Hour	
ESP Options	Enable ESP	Enabled	
	Client Authentication	Form Based	

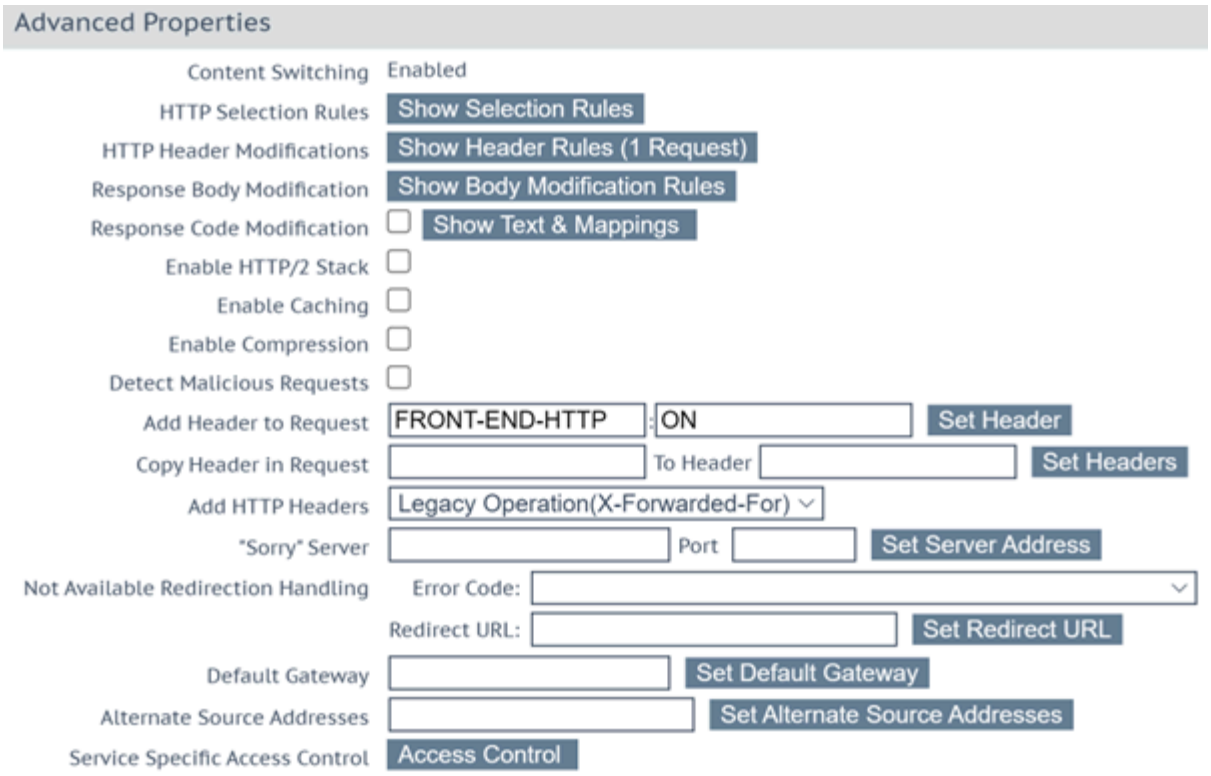
Section	Option	Value	Comment
	Mode		
	SSO Domain		Select the relevant domain.
	Allowed Virtual Hosts		Enter any required **Allowed Virtual Hosts** and click **Set Allowed Virtual Hosts**.
	Allowed Virtual Directories	/owa*	Click **Set Allowed Directories**.
	Server Authentication Mode	Basic Authentication	
	SSO Image Set	Exchange	
	SSO Greeting Message	Please enter your Exchange credentials.	Click **Set SSO Greeting Message**.*
Real Servers	Checked Port	443	Click **Set Check Port**.
	URL	/owa	Click **Set URL**.
	Use HTTP/1.1	Enabled	
	HTTP Method	GET	

12. Now, add the remaining required SubVSs. The specific settings for the additional SubVSs, which differ from the above steps, are in the table below.

SubVS Name	Allowed Virtual Directories		Client Auth. mode	Server Auth. mode	SSO Image Set	SSO Greeting Message	Health Check URL
Autodiscover	/autodiscover*		None	None	n/a		/autodiscover
ECP	/ecp*		Form Based	Basic Auth.	Exchange	Please enter your Exchange credentials.	/ecp

SubVS Name	Allowed Virtual Directories		Client Auth. mode	Server Auth. mode	SSO Image Set	SSO Greeting Message	Health Check URL
EWS	/ews*		None	None	n/a		/ews
ActiveSync	/microsoft-server-activesync*		Basic Auth.	Basic Auth.	n/a		/microsoft-server-activesync
OAB	/oab*		None	None	n/a		/oab
Powershell	/powershell*		None	None	n/a		/powershell
RPC	/rpc*		None	None	n/a		/rpc
Authentication Proxy	/*		Form Based	Basic Auth.	Exchange	Please enter your Exchange credentials.	

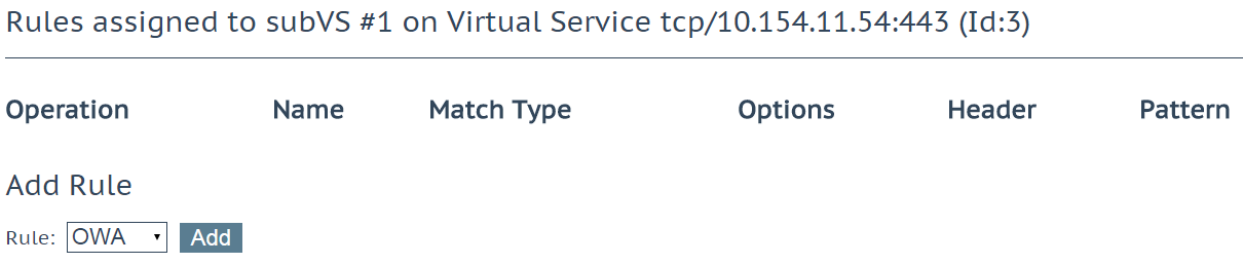
13. When all the SubVSs have been added, go to the parent Virtual Service modify screen and expand the **Advanced Properties** section.



14. Click **Enable** to enable **Content Switching**.
15. Now, the content rules need to be assigned to each of the SubVSs. To do this, expand the **SubVSs** section.



16. Click **None**.



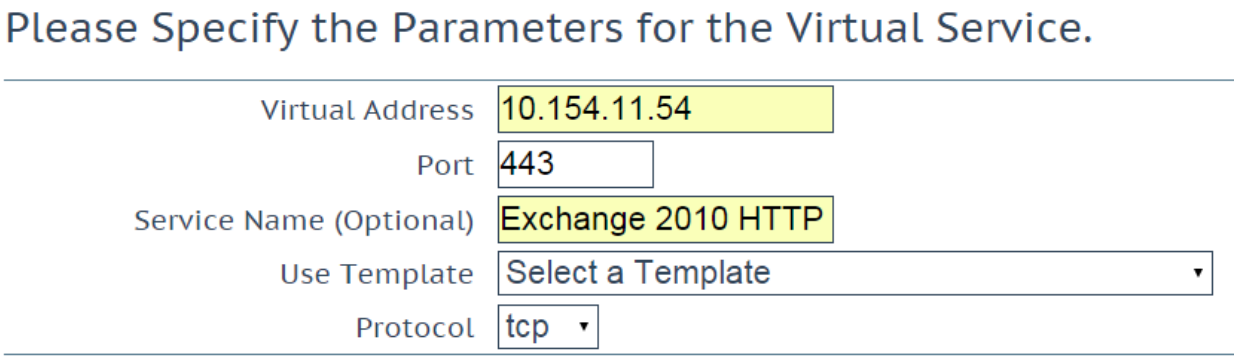
17. Select the relevant rule for the SubVS selected and click **Add**.
18. Repeat the previous two steps to add rules to each of the SubVSs.

Note: In addition to the OWA rule, the **root** rule should also be assigned to the OWA SubVS.

Configuring a Virtual Service for HTTPS-based Services (without SSL Offload)

To configure a Virtual Service for HTTPS-based services, without SSL offload, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter a valid **Virtual Address**.
4. Enter **443** as the **Port**.

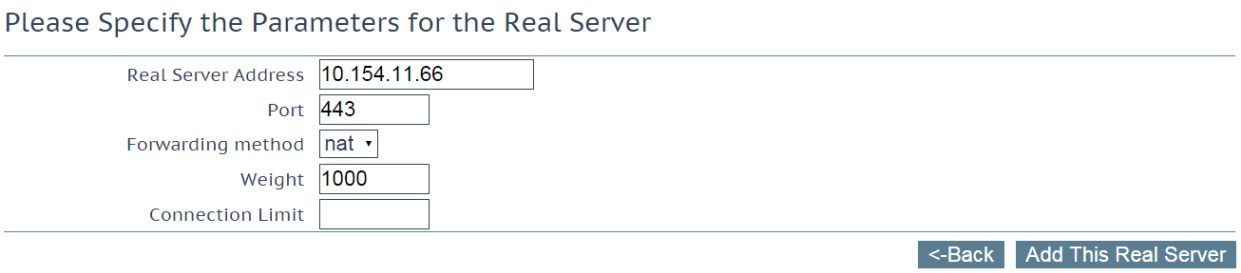
Note: Select **tcp** as the **Protocol**. The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

5. Click **Add this Virtual Service**.
6. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Persistence Mode	Source IP Address	
	Persistence Timeout	1 Hour	
	Scheduling Method	round robin	
	Idle Connection Timeout	900	Click **Set Idle Timeout**.
Advanced Properties	Redirection URL	https://%h%s	Click **Add HTTP Redirector**. This creates a redirect Virtual Service on port 80 with the same IP

Section	Option	Value	Comment
			address.
Real Servers	Real Server Check Method	HTTPS Protocol	
	Checked Port	443	Click **Set Check Port**.
	URL	/owa	Click **Set URL**.

7. Click the **Add New…** button.



8. Enter the **Real Server Address**.
9. Enter **443** as the **Port**.
10. Click **Add This Real Server**.
11. Click **OK** in response to the confirmation that the Real Server was added.

To view, modify, or delete any Virtual Services or Real Servers that have been added, click **View/Modify Services**.

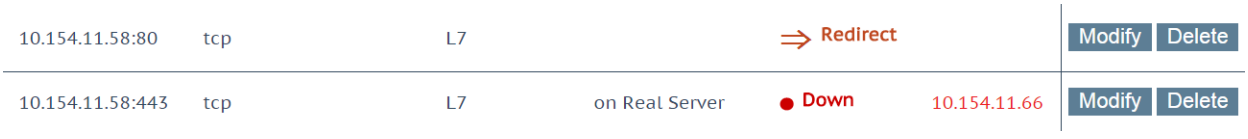
Related Links

- Configuring the HTTP Redirect Virtual Service

Configuring the HTTP Redirect Virtual Service

The HTTP redirect Virtual Service needs to be configured. Follow the steps below to do this:

1. In the main menu, go to **Virtual Services > View/Modify Virtual Services**.



2. Click the **Modify** button on the **Redirect** Virtual Service.
3. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Basic Properties	Service Name		Enter a recognizable name, such as **Exchange 2010 HTTPS - HTTP Redirect**.
Standard Options	Persistence Mode	None	
Real Servers	Real Server Check Method	None	

Configuring the LoadMaster for Outlook MAPI

In Exchange 2010, MAPI traffic to the user's mailbox goes to the endpoint configured in the database. By default, it is set to the FQDN of the Exchange server. If the database is created after creating the Client Access Array, the new database automatically uses the CAS Array FQDN and will go to the load balancer if DNS is configured correctly.

Public folder traffic is also MAPI but it does not use the CAS Array FQDN and this behaviour cannot be changed. This traffic will always bypass the load balancer in Exchange 2010.

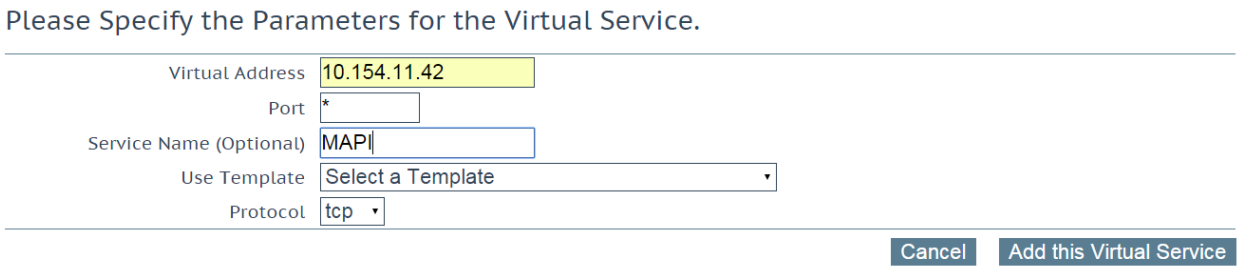
Related Links

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

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

Follow the steps below to create the Virtual Service for Outlook MAPI connectivity:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter a valid **Virtual Address**.
4. Enter ***** (asterisk) as the **Port**.

Note: 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. You can enter a specific port number for each Virtual Service.

Note: Do not change the wildcard service to Layer 4 as doing so will cause inoperability.

5. Select **tcp** as the **Protocol**.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

6. Click **Add this Virtual Service**.
7. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Persistence Mode	Source IP Address	
	Persistence Timeout	1 Hour	
	Scheduling Method	round robin	
	Idle Connection Timeout	86400	Click **Set Idle Timeout**. This provides an idle timeout of 24 hours and prevents Outlook Users having to re-authenticate during the working day.
Real Servers	Real Server Check Method	TCP Connection Only	
	Checked Port	135	Click **Set Check Port**.

8. Click the **Add New…** button.
9. Enter the **Real Server Address**.
10. Click **Add This Real Server**.
11. Click **OK** in response to the confirmation that the Real Server was added.

To view, modify, or delete any Virtual Services or Real Servers that have been added, select **Virtual Services** > **View/Modify Services** in the main menu of the LoadMaster WUI.

Configuring the 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.

Note: When using a unique Virtual Service for each CAS service, the same FQDN and port cannot be shared 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.

The following sections contain steps necessary for creating a Virtual Service for each of the available CASs in Exchange 2010.

Related Links

- Outlook Web App (OWA)
- Control Panel (ECP)
- ActiveSync (EAS)
- Outlook Anywhere (OA)
- Web Services (EWS)
- Autodiscover Service (AS)
- Internet Message Access Protocol (IMAP4)
- Post Office Protocol (POP3)
- Simple Mail Transfer Protocol (SMTP)
- Importing and Assigning an SSL Certificate

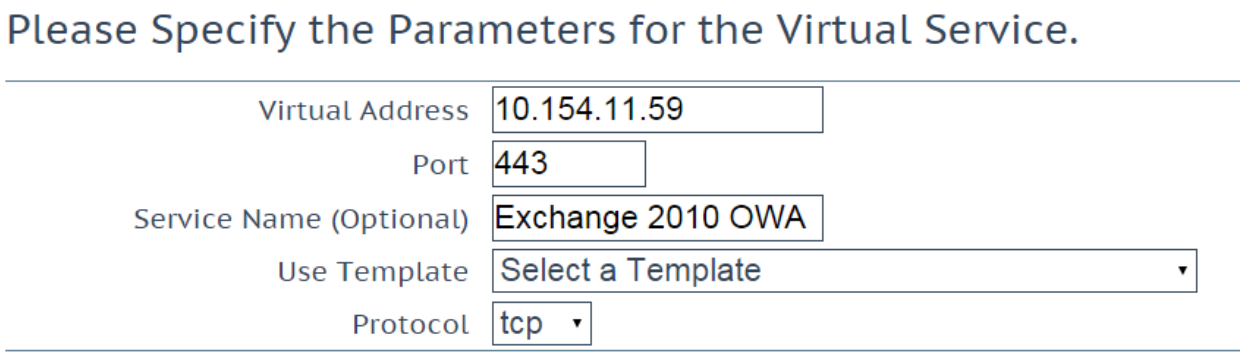
Outlook Web App (OWA)

Configuring a Virtual Service for OWA (with SSL Offload)

When offloading SSL for OWA, you should follow the recommendations set by Microsoft. Progress Kemp understands these recommendations to be:

- Enable SSL Offloading (as per instructions): http://technet.microsoft.com/en-us/library/bb885060(EXCHG.80).aspx
- Disable “Require SSL” on IIS:http://technet.microsoft.com/en-us/library/cc732341(WS.10).aspx.

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter a valid **Virtual Address**.
4. Enter **443** as the **Port**.
5. Enter a recognisable **Service Name**, for example **Exchange 2010 OWA**.
6. Select **tcp** as the Protocol.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

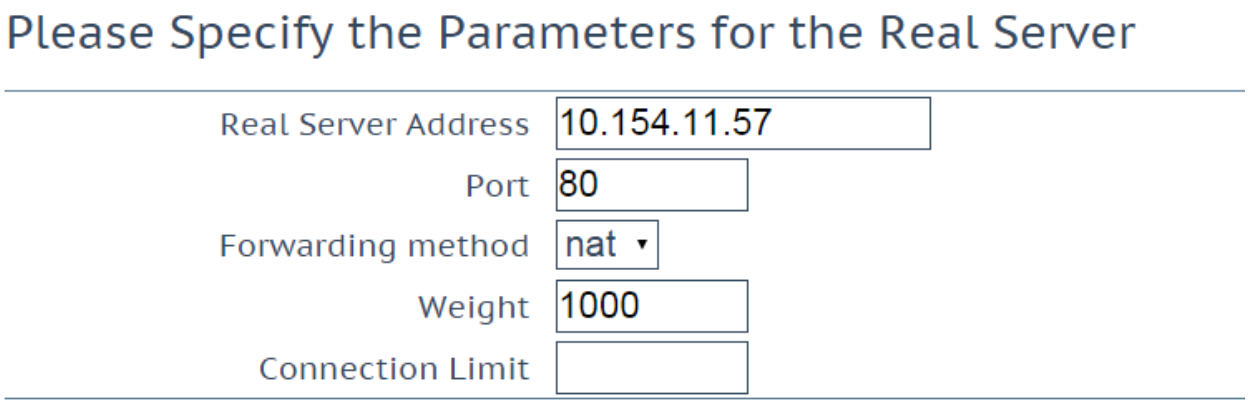
7. Click **Add this Virtual Service**.
8. Configure the settings as shown in the following table:

* By default, a self-signed certificate is used. Click **OK** when a message displays indicating that there is no SSL certificate currently available for your Virtual Service. **Optional:** You can 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 to export the certificate and private key as a Personal Information File (PFX). An SSL certificate can be obtained 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 the LoadMaster. **Optional:** You can import the appropriate PFX certificate and key file into the LoadMaster. For instructions on how to do this, refer to the Importing and Assigning an SSL Certificate section.

Section	Option	Value	Comment
SSL Properties	SSL Acceleration	Enabled*	
Standard Options	Transparency	Disabled	
	Persistence Mode	Super HTTP	
	Persistence Timeout	1 Hour	
	Idle Connection Timeout	900	Click **Set Idle Timeout**.
Advanced Properties	Add Header to Request	FRONT-END-HTTP:ON	Click **Add Header**.
	Redirection URL	https://%h%s	Click **Add HTTP Redirector**. This creates a

Section	Option	Value	Comment
			redirect Virtual Service on port 80 with the same IP address.
Real Servers	Real Server Check Method	HTTP Protocol	
	Checked Port	80	Click **Set Check Port**.
	URL	/owa	Click **Set URL**.

9. Click the **Add New...** button.



10. Enter the **Real Server Address**.
11. Enter **80** as the **Port**.
12. Click **Add This Real Server**.
13. Click **OK** in response to the confirmation that the Real Server was added.

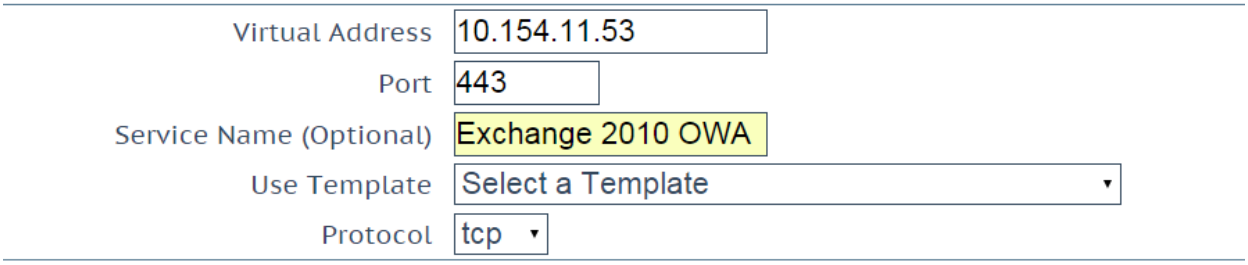
To view, modify, or delete any Real Servers that have been added, select the **Virtual Services** > **View/ Modify Services** option in the main menu of the LoadMaster WUI.

The HTTP redirect Virtual Service needs to be configured. Refer to the Creating the Virtual Service for the RPC CA (MAPI) & Address Book Service **section** for instructions on how to do this.

Configuring a Virtual Service for OWA (without SSL Offload)

To configure a Virtual Service for OWA, without SSL offload, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter a valid **Virtual Address**.
4. Enter **443** as the **Port**.
5. Select **tcp** as the Protocol.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

6. Click **Add this Virtual Service**.
7. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Persistence Mode	Source IP Address	
	Persistence Timeout	1 Hour	
	Scheduling Method	round robin	
	Idle Connection Timeout	900	Click **Set Idle Timeout.**
Advanced Properties	Redirection URL	https://%h%s	Click **Add HTTP Redirector**. This creates a redirect Virtual Service on port 80 with the same IP address.
Real Servers	Real Server Check Method	HTTPS Protocol	
	Checked Port	443	Click **Set Check Port**.
	URL	/owa	Click **Set URL**.

8. Click the **Add New…** button.
9. Enter the **Real Server Address**.
10. Enter **443** as the **Port**.
11. Click **Add This Real Server**.

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

To view, modify, or delete any Virtual Services or Real Servers that have been added, select the **Virtual Services** > **View/Modify Services** menu option.

The HTTP redirect Virtual Service needs to be configured. Refer to the Creating the Virtual Service for the RPC CA (MAPI) & Address Book Service **section** for instructions on how to do this.

Control Panel (ECP)

Refer to the following sections for details on how to configure a Virtual Service for ECP with and without SSL offloading.

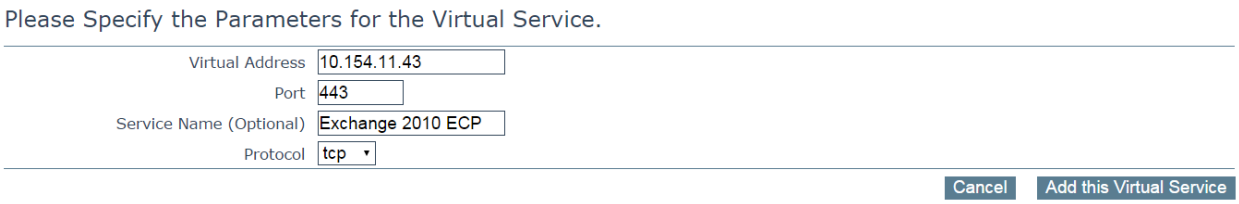
Related Links

- Configuring a Virtual Service for ECP (with SSL Offload)
- Configuring a Virtual Service for ECP (without SSL Offload)

Configuring a Virtual Service for ECP (with SSL Offload)

When you choose to offload SSL for ECP, please follow the recommendations set by Microsoft. Progress Kemp understands these recommendations to be; disable “Require SSL” on IIS: http://technet.microsoft.com/en-us/library/cc732341(WS.10).aspx.

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter a valid **Virtual Address**.
4. Enter **443** as the **Port**.
5. Enter a recognisable **Service Name**, for example **Exchange 2010 ECP**.
6. Select **tcp** as the Protocol.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

7. Click **Add this Virtual Service**.
8. Configure the settings as shown in the following table:

Optional: Import the appropriate PFX certificate and key file into the LoadMaster. For instructions on how to do this, refer to the Importing and Assigning an SSL Certificate section.

Optional: You can 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 to export the certificate and private key as a Personal Information File (PFX). An SSL certificate can also be

obtained 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 the LoadMaster.

* By default, a self-signed certificate is used. Click **OK** when a message displays indicating that there is no SSL certificate currently available.

Section	Option	Value	Comment
SSL Properties	SSL Acceleration	Enabled*	
Standard Options	Transparency	Disabled	
	Persistence Mode	Super HTTP	
	Persistence Timeout	1 Hour	
	Idle Connection Timeout	900	Click **Set Idle Timeout**.
Advanced Properties	Add Header to Request	FRONT-END-HTTP:ON	Click **Set Header**.
	Redirection URL	https://%h%s	Click **Add HTTP Redirector**. This creates a redirect Virtual Service on port 80 with the same IP address.
Real Servers	Real Server Check Method	HTTP Protocol	
	Checked Port	80	Click **Set Check Port**.
	URL	/ecp	Click **Set URL**.

9. Click the **Add New…** button.
10. Enter the **Real Server Address**.
11. Enter **80** as the **Port**.
12. Click **Add This Real Server**.
13. Click **OK** in response to the confirmation that the Real Server was added.

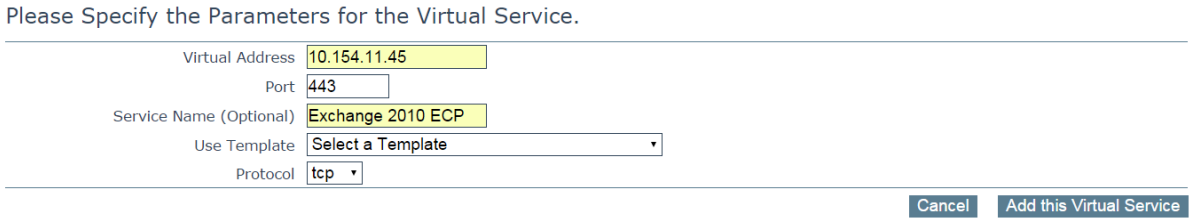
To view, modify, or delete any Virtual Services or Real Servers, select **Virtual Services** > **View/Modify Services** in the main menu of the LoadMaster WUI.

The HTTP redirect Virtual Service needs to be configured. Refer to the Creating the Virtual Service for the RPC CA (MAPI) & Address Book Service section for instructions on how to do this.

Configuring a Virtual Service for ECP (without SSL Offload)

To configure a Virtual Service for ECP, without SSL offload, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual** Services.
2. Select **Add New**.



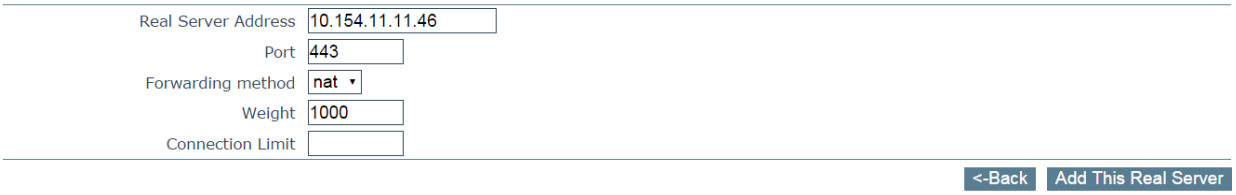
3. Enter a valid **Virtual Address**.
4. Enter **443** as the **Port**.
5. Select **tcp** as the **Protocol**.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

6. Click **Add this Virtual Service**.
7. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Persistence Mode	Source IP Address	
	Persistence Timeout	1 Hour	
	Scheduling Method	round robin	
Real Servers	Real Server Check Method	HTTPS Protocol	
	Checked Port	443	Click **Set Check Port**.
	URL	/ecp	Click **Set URL**.

8. Click the **Add New…** button.



9. Enter the **Real Server Address**.

10. Enter **443** as the **Port**.
11. Click **Add This Real Server**.
12. Click **OK** in response to the confirmation that the Real Server was added.

To view, modify, or delete any Virtual Services or Real Servers, select **Virtual Services** > **View/Modify Services** in the main menu of the LoadMaster WUI.

The HTTP redirect Virtual Service needs to be configured. Refer to the Creating the Virtual Service for the RPC CA (MAPI) & Address Book Service section for instructions on how to do this.

ActiveSync (EAS)

To configure a Virtual Service for EAS with or without SSL offload, refer to the below sub-sections.

Related Links

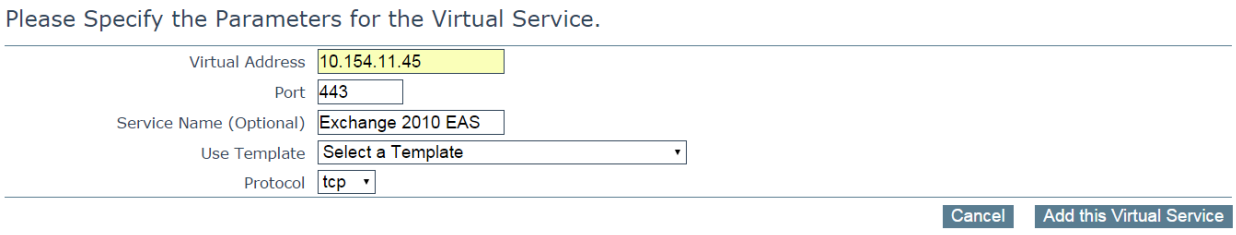
- Configuring a Virtual Service for EAS (with SSL Offload)
- Configuring a Virtual Service for EAS (without SSL Offload)

Configuring a Virtual Service for EAS (with SSL Offload)

When offloading SSL for EAS, follow the recommendations set by Microsoft. Progress Kemp 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.

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. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter a valid **Virtual Address**.
4. Enter **443** as the **Port**.
5. Enter a recognisable **Service Name**, for example **Exchange 2010 EAS**.
6. Select **tcp** as the **Protocol**.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

7. Click **Add this Virtual Service**.
8. Configure the settings as shown in the following table:

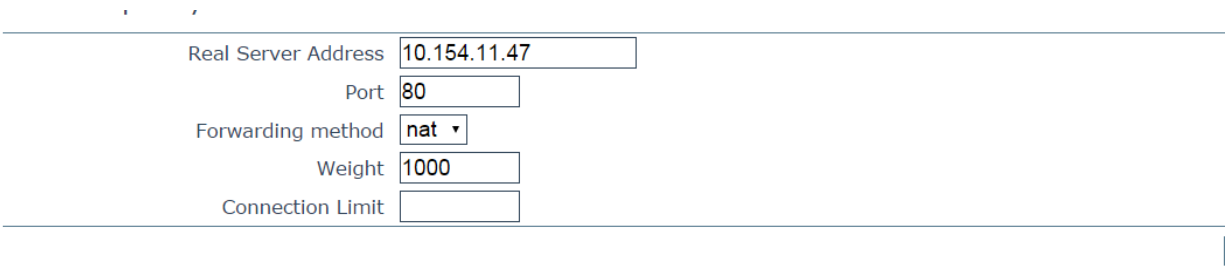
Optional: Import the appropriate PFX certificate and key file into the LoadMaster. For instructions on how to do this, refer to the Importing and Assigning an SSL Certificate section.

Optional: You can 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 to export the certificate and private key as a Personal Information File (PFX). You can also obtain an SSL certificate 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.

* By default, a self-signed certificate is used. Click **OK** when a message displays indicating that there is no SSL certificate currently available.

Section	Option	Value	Comment
SSL Properties	SSL Acceleration	Enabled*	
Standard Options	Transparency	Disabled	
	Persistence Mode	Super HTTP	
	Persistence Timeout	1 Hour	
	Idle Connection Timeout	900	Click **Set Idle Timeout**.
Real Servers	Checked Port	80	Click **Set Check Port**.
	URL	/Microsoft-server-activesync	Click **Set URL**.

9. Click the **Add New…** button.



10. Enter the **Real Server Address**.
11. Enter **80** as the **Port**.
12. Click **Add This Real Server**.
13. Click **OK** in response to the confirmation that the Real Server was added.

To view, modify, or delete any Virtual Services or Real Servers, select the **Virtual Services** > **View/Modify Services** option in the main menu of the LoadMaster WUI.

The HTTP redirect Virtual Service needs to be configured. Refer to the Creating the Virtual Service for the RPC CA (MAPI) & Address Book Service section for instructions on how to do this.

Configuring a Virtual Service for EAS (without SSL Offload)

To configure a Virtual Service for EAS, without SSL offload, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



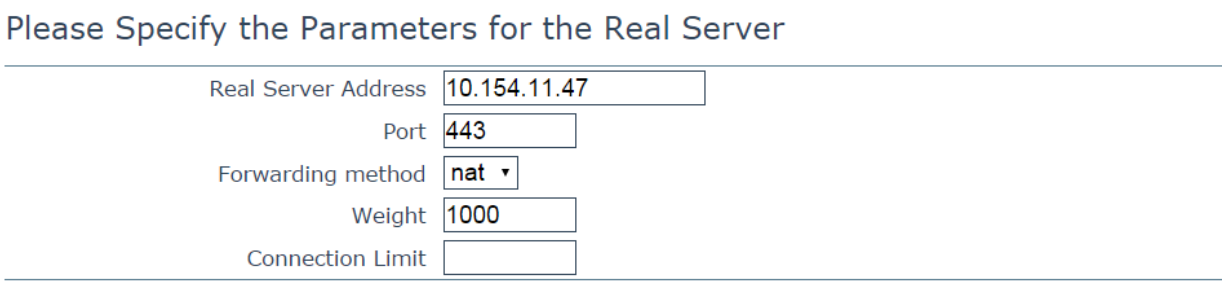
3. Enter a valid **Virtual Address**.
4. Enter **443** as the **Port**.
5. Select **tcp** as the **Protocol**.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

6. Click **Add this Virtual Service**.
7. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Persistence Mode	Source IP Address	
	Persistence Timeout	1 Hour	
	Scheduling Method	round robin	
	Idle Connection Timeout	900	Click **Set Idle Timeout**.
Real Servers	Real Server Check Method	HTTPS Protocol	
	Checked Port	443	Click **Set Check Port**.
	URL	/Microsoft-Server-ActiveSync	Click **Set URL**.

8. Click the **Add New...** button.



9. Enter the **Real Server Address**.
10. Enter **443** as the **Port**.
11. Click **Add This Real Server**.
12. Click **OK** in response to the confirmation that the Real Server was added.
13. To view, modify, or delete any Virtual Services or Real Servers that have been added, select the **Virtual Services** > **View/Modify Services** option in the main menu of the LoadMaster WUI.

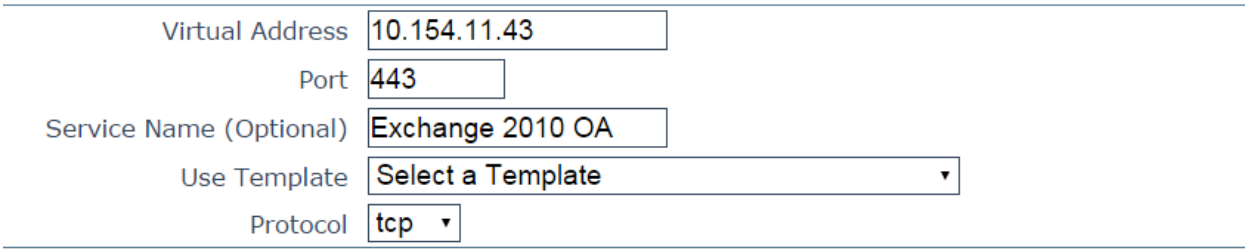
The HTTP redirect Virtual Service needs to be configured. Refer to the Creating the Virtual Service for the RPC CA (MAPI) & Address Book Service section for instructions on how to do this.

Outlook Anywhere (OA)

Configuring a Virtual Service for OA (with SSL Offload)

When SSL offloading OA, you should follow the recommendations set by Microsoft. Progress Kemp understands the recommendations to be; configuring SSL Offloading for OW per: http://technet.microsoft.com/en-us/library/aa998346.aspx.

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter a valid **Virtual Address**.
4. Enter **443** as the **Port**.
5. Enter a recognisable **Service Name**, for example **Exchange 2010 OA**.
6. Select **tcp** as the **Protocol**.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

7. Click **Add this Virtual Service**.

8. Configure the settings as shown in the following table:

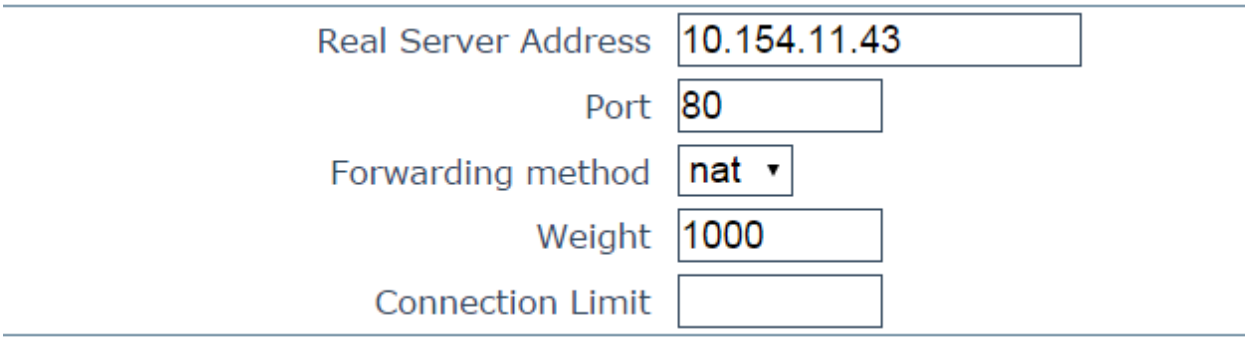
   Optional: Import the appropriate PFX certificate and key file into the LoadMaster. For instructions on how to do this, refer to the Importing and Assigning an SSL Certificate section.

   Optional: You can 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 to export the certificate and private key as a Personal Information File (PFX). You can also obtain an SSL certificate 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.

   * By default, a self-signed certificate is used. Click **OK** when a message displays indicating that there is no SSL certificate currently available.

Section	Option	Value	Comment
SSL Properties	SSL Acceleration	Enabled*	
Standard Options	Transparency	Disabled	
	Persistence Mode	Super HTTP	
	Persistence Timeout	1 Hour	
	Idle Connection Timeout	900	Click **Set Idle Timeout**.
Advanced Properties	Add Header to Request	FRONT-END-HTTP:ON	Click **Set Header**.
	Redirection URL	https://%h%s	Click **Add HTTP Redirector**. This creates a redirect Virtual Service on port 80 with the same IP address.
Real Servers	Real Server Check Method	HTTP Protocol	
	Checked Port	80	Click **Set Check Port**.
	URL	/rpc/rpcproxy.dll	Click **Set URL**.

9. Click the **Add New…** button.



10. Enter the **Real Server Address**.
11. Enter **80** as the **Port**.
12. Click **Add This Real Server**.
13. Click **OK** in response to the confirmation that the Real Server was added.

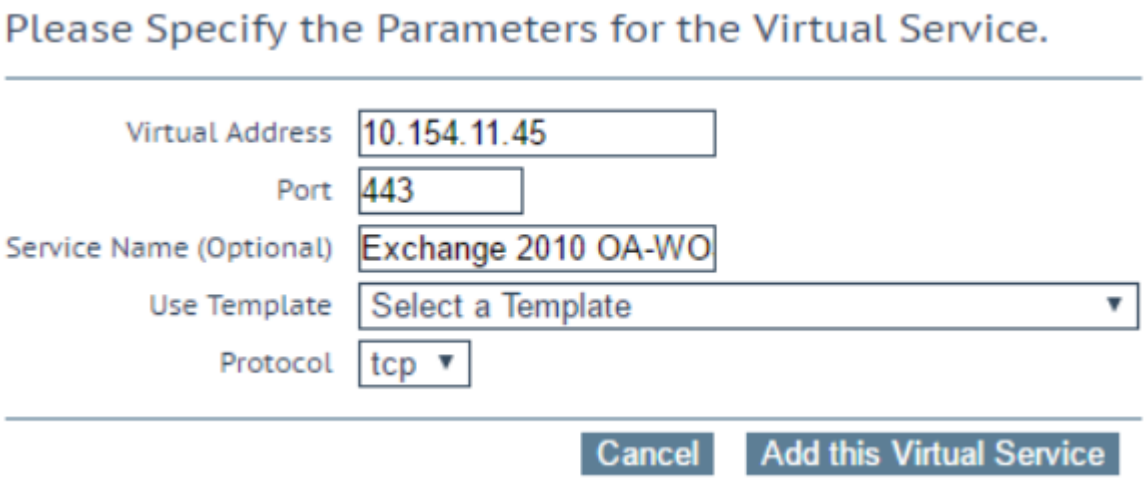
To view, modify, or delete any Virtual Services or Real Servers that have been added, select the **Virtual Services** > **View/Modify Services** option in the main menu of the LoadMaster WUI.

The HTTP redirect Virtual Service needs to be configured. Refer to the Creating the Virtual Service for the RPC CA (MAPI) & Address Book Service section for instructions on how to do this.

Configuring a Virtual Service for OA (without SSL Offload)

To configure a Virtual Service for OA, without SSL offload, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter a valid **Virtual Address**.
4. Enter **443** as the **Port**.

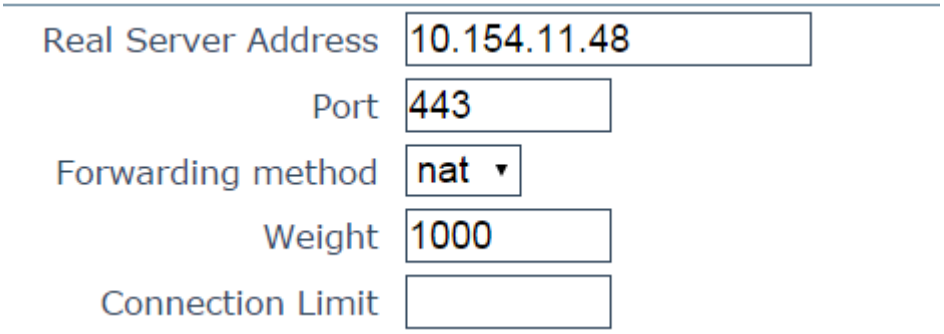
5. Enter a recognizable **Service Name**, for example **Exchange 2010 OA-WOSSL**.
6. Select **tcp** as the **Protocol**.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

7. Click **Add this Virtual Service**.
8. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Persistence Mode	Source IP Address	
	Persistence Timeout	1 Hour	
	Scheduling Method	round robin	
	Idle Connection Timeout	900	Click **Set Idle Timeout**.
Real Servers	Real Server Check Method	HTTPS Protocol	
	Checked Port	443	Click **Set Check Port**.
	URL	/rpc/rpcproxy.dll	Click **Set URL**.

9. Click the **Add New…** button.



10. Enter the **Real Server Address**.
11. Enter **443** as the **Port**.
12. Click **Add This Real Server**.
13. Click **OK** in response to the confirmation that the Real Server was added.

To view, modify, or delete any Virtual Services or Real Servers that have been added, select the **Virtual Services** > **View/Modify Services** option in the LoadMaster WUI.

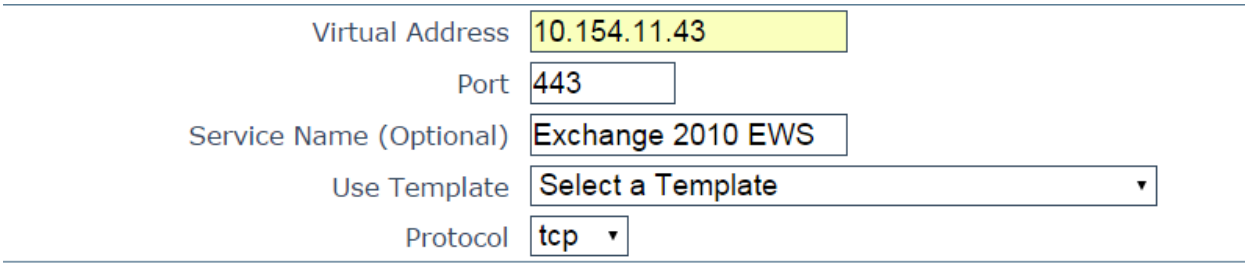
The HTTP redirect Virtual Service needs to be configured. Refer to the Creating the Virtual Service for the RPC CA (MAPI) & Address Book Service section for instructions on how to do this.

Web Services (EWS)

Configuring a Virtual Service for EWS (with SSL Offload)

When offloading SSL for EWS, follow the recommendations set by Microsoft. Progress Kemp understands the recommendations to be; Enable or Disable SSL on the EWS Virtual Directory: http://technet.microsoft.com/en-us/library/ee633481.aspx.

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter a valid **Virtual Address**.
4. Enter **443** as the **Port**.
5. Enter a recognizable **Service Name**, for example **Exchange 2010 EWS**.
6. Select **tcp** as the **Protocol**.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

7. Click **Add this Virtual Service**.
8. Configure the settings as shown in the following table:

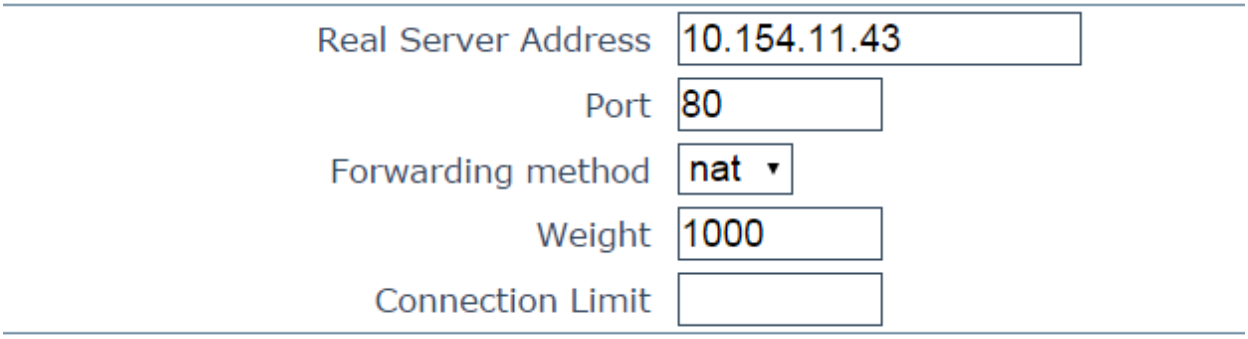
Optional: Import the appropriate PFX certificate and key file into the LoadMaster. For instructions on how to do this, refer to the Importing and Assigning an SSL Certificate section.

Optional: You can 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 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.

* By default, a self-signed certificate is used. Click **OK** when a message displays indicating that there is no SSL certificate currently available.

Section	Option	Value	Comment
SSL Properties	SSL Acceleration	Enabled*	
Standard Options	Transparency	Disabled	
	Persistence Mode	Super HTTP	
	Persistence Timeout	1 Hour	
	Scheduling Method	round robin	
	Idle Connection Timeout	900	Click **Set Idle Timeout**.
Advanced Properties	Add Header to Request	FRONT-END-HTTP:ON	Click **Set Header**.
	Redirection URL	https://%h%s	Click **Add HTTP Redirector**. This creates a redirect Virtual Service on port 80 with the same IP address.
Real Servers	Real Server Check Method	HTTP Protocol	
	URL	/ews/exchange.asmx	Click **Set URL**.
	Click **Show Headers**.	FRONT-END-HTTP:ON	Click **Set Header**. Header injection is a legacy option and is not required as per Microsoft.

9. Click the **Add New…** button.



10. Enter the **Real Server Address**.
11. Enter **80** as the **Port**.
12. Click **Add This Real Server**.
13. Click **OK** in response to the confirmation that the Real Server was added.

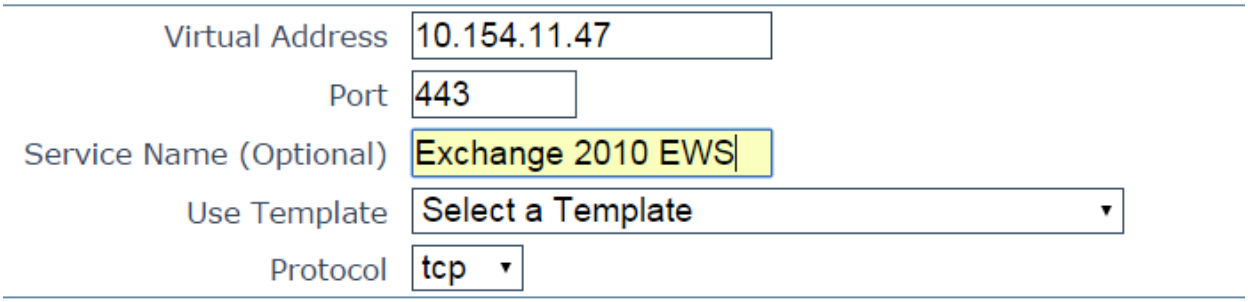
To view, modify, or delete any Virtual Services or Real Servers, select **Virtual Services** > **View/Modify Services** from the main menu of the LoadMaster WUI.

The HTTP redirect Virtual Service needs to be configured. Refer to the Creating the Virtual Service for the RPC CA (MAPI) & Address Book Service section for instructions on how to do this.

Configuring a Virtual Service for EWS (without SSL Offload)

To configure a Virtual Service for EWS, without SSL offload, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter a valid **Virtual Address**.
4. Enter **443** as the **Port**.
5. Enter a recognizable **Service Name**, for example **Exchange 2010 EWS HTTPS**.
6. Select **tcp** as the **Protocol**.

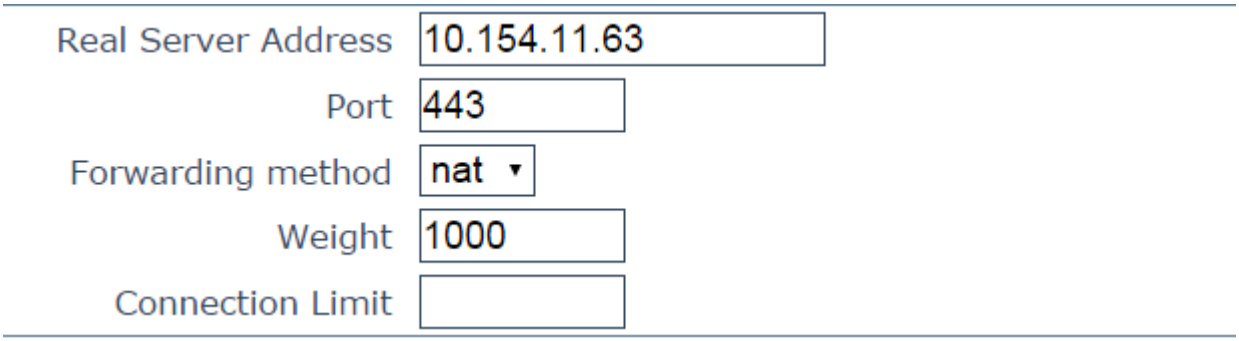
Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

7. Click **Add this Virtual Service**.
8. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Persistence Mode	Source IP Address	
	Persistence Timeout	1 Hour	
	Scheduling Method	round robin	
	Idle Connection Timeout	900	Click **Set Idle Timeout**.

Section	Option	Value	Comment
Advanced Properties	Redirection URL	https://%h%s	Click **Add HTTP Redirector**. This creates a redirect Virtual Service on port 80 with the same IP address.
Real Servers	Real Server Check Method	HTTPS Protocol	
	Checked Port	443	Click **Set Check Port**.
	URL	/ews/exchange.asmx	Click **Set URL**.

9. Click the **Add New...** button.



10. Enter the **Real Server Address**.
11. Enter **443** as the **Port**.
12. Click **Add This Real Server**.
13. Click **OK** in response to the confirmation that the Real Server was added.

To view, modify, or delete any Virtual Services or Real Servers, select the **Virtual Services** > **View/Modify Services** option in the main menu of the LoadMaster WUI.

The HTTP redirect Virtual Service needs to be configured. Refer to the Creating the Virtual Service for the RPC CA (MAPI) & Address Book Service section for instructions on how to do this.

Autodiscover Service (AS)

To configure a Virtual Service for AS with or without SSL offload, refer to the below sub-sections.

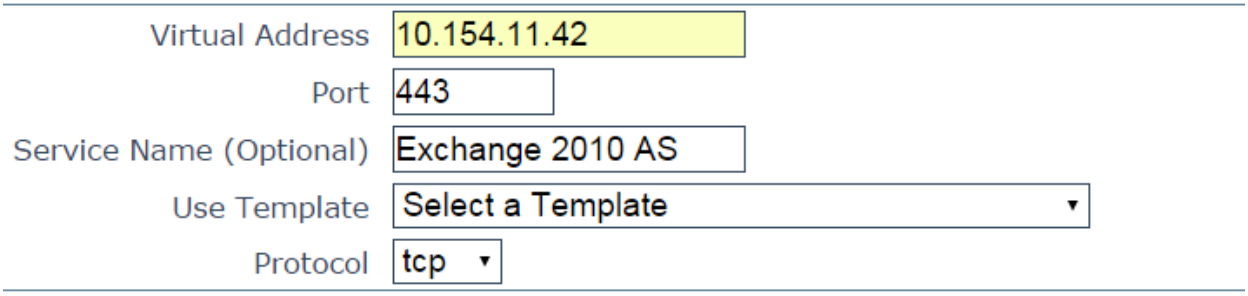
Related Links

- Configuring a Virtual Service for AS (with SSL Offload)
- Configuring a Virtual Service for AS (without SSL Offload)

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. Progress Kemp understands the recommendations to be; Enable or Disable SSL on the AS Virtual Directory (http://technet.microsoft.com/en-us/library/ee633481.aspx).

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter a valid **Virtual Address**.
4. Enter **443** as the **Port**.
5. Enter a recognizable **Service Name**, for example **Exchange 2010 AS**.
6. Select **tcp** as the **Protocol**.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

7. Click **Add this Virtual Service**.
8. Configure the settings as shown in the following table:

Optional: Import the appropriate PFX certificate and key file into the LoadMaster. For instructions on how to do this, refer to the Importing and Assigning an SSL Certificate section.

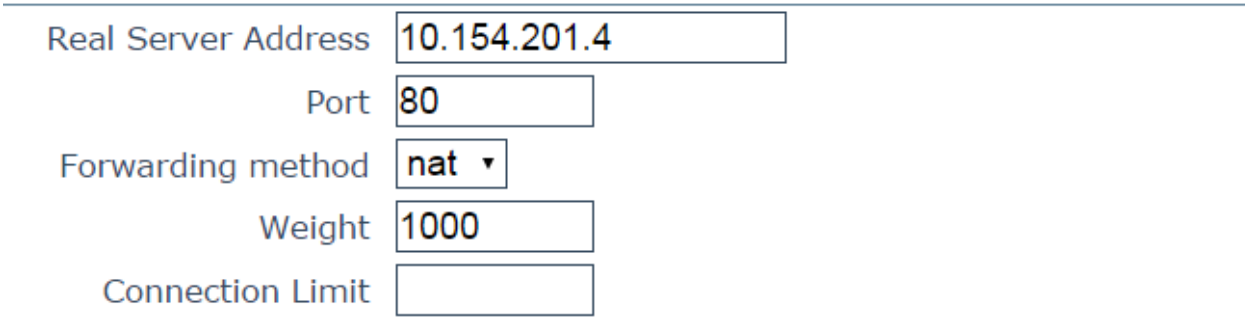
Optional: If you have not already done so, export the appropriate certificate and key from Exchange 2010 using the Microsoft export information found at http://technet.microsoft.com/en-us/library/bb310778.aspx. Ensure to export the certificate and private key as a Personal Information File (PFX). An SSL certificate can be obtained 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.

* By default, a self-signed certificate is used. Click **OK** when a message displays indicating that there is no SSL certificate currently available.

Section	Option	Value	Comment
SSL Properties	SSL Acceleration	Enabled*	Click **OK**.
Real Servers	Checked Port	80	Click **Set Check Port**.

Section	Option	Value	Comment
	URL	/autodiscover/ autodiscover.xml	Click **Set URL**.

9. Click the **Add New…** button.



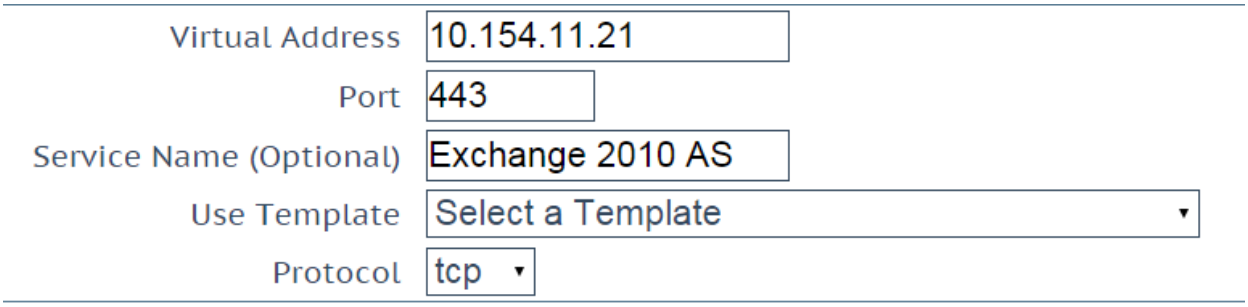
10. Enter the **Real Server Address**.
11. Enter **80** as the **Port**.
12. Click **Add This Real Server**.
13. Click **OK** in response to the confirmation that the Real Server was added.

To view, modify, or delete any Virtual Services or Real Servers, click **Virtual Services** > **View/Modify Services** in the LoadMaster main menu.

Configuring a Virtual Service for AS (without SSL Offload)

To configure a Virtual Service for AS, without SSL offload, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



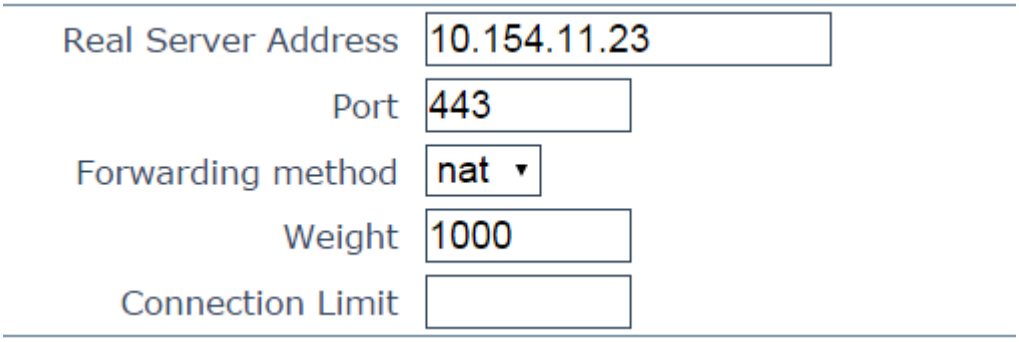
3. Enter a valid **Virtual Address**.
4. Enter **443** as the **Port**.
5. Enter a recognizable **Service Name**, for example **Exchange 2010 AS**.
6. Select **tcp** as the **Protocol**.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

7. Click **Add this Virtual Service**.
8. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Idle Connection Timeout	900	Click **Set Idle Timeout**.
Advanced Properties	Redirection URL	https://%h%s	Click **Add HTTP Redirector**. This creates a redirect Virtual Service on port 80 with the same IP address.
Real Servers	Checked Port	443	Click **Set Check Port**.
	URL	/autodiscover/ autodiscover.xml	Click **Set URL**.

9. Click the **Add New…** button.



10. Enter the **Real Server Address**.
11. Enter **443** as the **Port**.
12. Click **Add This Real Server**.
13. Click **OK** in response to the confirmation that the Real Server was added.

To view, modify, or delete any Virtual Services or Real Servers that have been added, select **Virtual Services** > **View/Modify Services** from the main menu of the LoadMaster WUI.

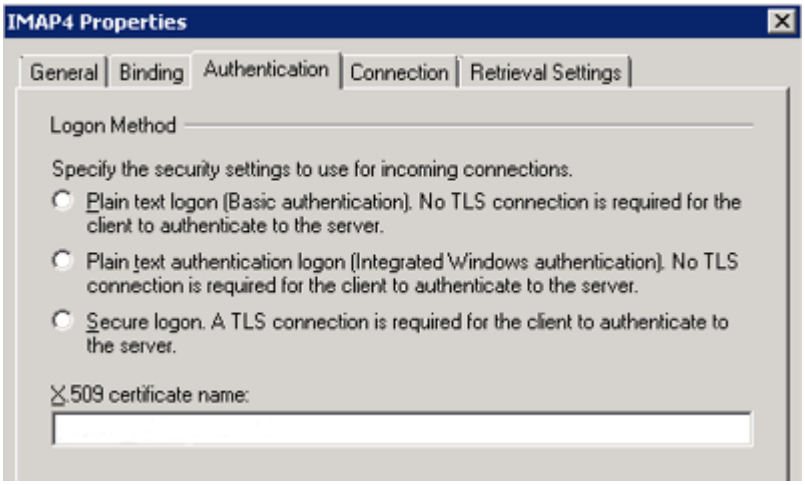
The HTTP redirect Virtual Service needs to be configured. Refer to the Creating the Virtual Service for the RPC CA (MAPI) & Address Book Service section for instructions on how to do this.

Internet Message Access Protocol (IMAP4)

Configuring a Virtual Service for IMAPS (with SSL Offload)

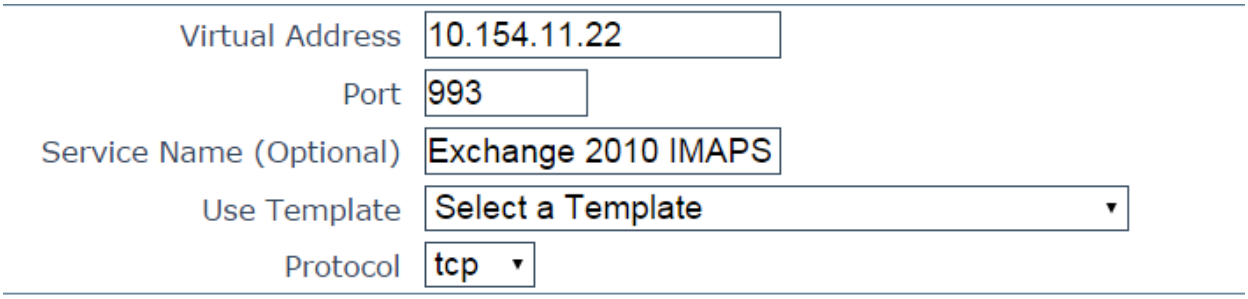
In general, SSL offload for IMAP represents a trade-off. When servers are running near capacity, offloading SSL can allow you to accommodate additional traffic with a given set of servers, at a cost of some diminished security checks. When you choose to SSL offload you should follow the recommendations set by Microsoft. Progress Kemp understands the recommendations to be; Disabling Secure Login Authentication using instructions found at http://technet.microsoft.com/en-us/library/bb691401.aspx.

- When using the IMAP or POP3 service, TLS must be turned off on the Exchange server. If TLS is on, the server will attempt to force TLS and this may break the connection.



When configuring the **IMAP4 Properties**, ensure to select one of the first 2 options because TLS should not be enabled.

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter a valid **Virtual Address**.
4. Enter **993** as the **Port**.
5. Enter a recognizable **Service Name**, for example **Exchange 2010 IMAPS Offloaded**.
6. Select **tcp** as the **Protocol**.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

7. Click **Add this Virtual Service**.
8. Configure the settings as shown in the following table:

   Optional: Import the appropriate PFX certificate and key file into the LoadMaster. For instructions on how to do this, refer to the Importing and Assigning an SSL Certificate section.

   Optional: 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 to export the certificate and private key as a Personal Information File (PFX). An SSL certificate can be obtained 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 the LoadMaster.

   * By default, a self-signed certificate is used. Click **OK** when a message displays indicating that there is no SSL certificate currently available.

Section	Option	Value	Comment
SSL Properties	SSL Acceleration	Enabled*	
Standard Options	Transparency	Disabled	
	Server Initiating Protocols	IMAP4	
	Idle Connection Timeout	3600	Click **Set Idle Timeout**.
Real Servers	Real Server Check Method	Mailbox (IMAP) Protocol	
	Checked Port	143	Click **Set Check Port**.

9. Click the **Add New…** button.
10. Enter the **Real Server Address**.
11. Enter **143** as the **Port**.
12. Click **Add This Real Server**.
13. Click **OK** in response to the confirmation that the Real Server was added.

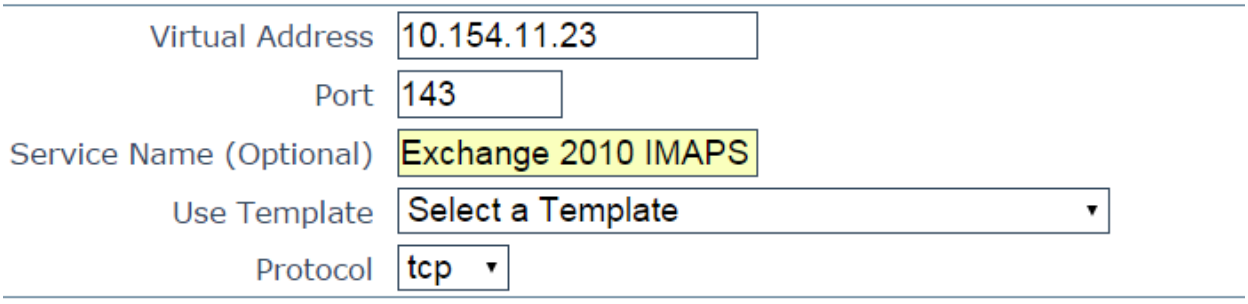
To view, modify, or delete any Virtual Services or Real Servers that have been added, select **Virtual Services** and **View/Modify Services** in the main menu of the LoadMaster WUI.

Configuring a Virtual Service for IMAP (without SSL Offload)

To configure a Virtual Service for IMAP, without SSL offload, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.

2. Select **Add New**.



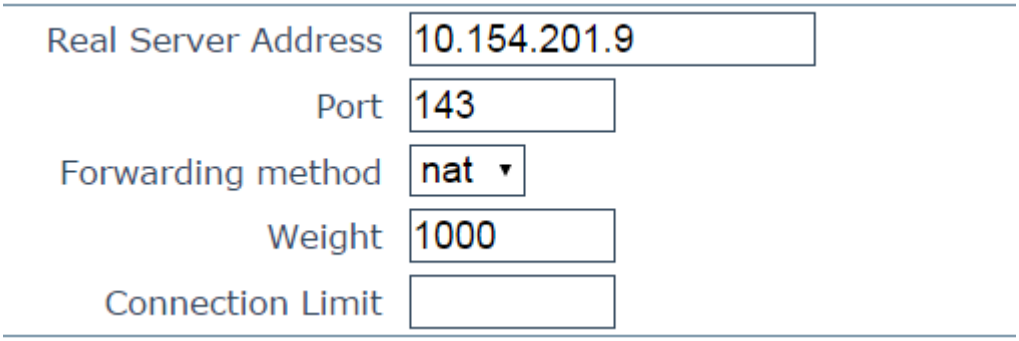
3. Enter a valid **Virtual Address**.
4. Enter **143** as the **Port**.
5. Enter a valid **Service Name**, for example **Exchange 2010 IMAP**.
6. Select **tcp** as the **Protocol**.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

7. Click **Add this Virtual Service**.
8. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Idle Connection Timeout	3600	Click **Set Idle Timeout**.
Real Servers	Real Server Check Method	Mailbox (IMAP) Protocol	
	Checked Port	143	Click **Set Check Port**.

9. Click the **Add New…** button.



10. Enter the **Real Server Address**.

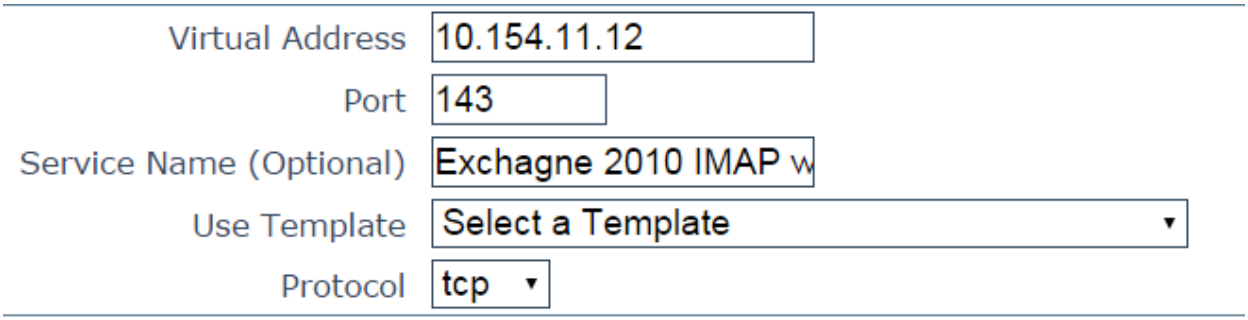
11. Enter **143** as the **Port**.
12. Click **Add This Real Server**.
13. Click **OK** in response to the confirmation that the Real Server was added.

To view, modify, or delete any Virtual Services or Real Servers that have been added, select the **Virtual Services** > **View/Modify Services** option from the main menu of the LoadMaster WUI.

Configuring a Virtual Service for IMAP (without SSL Offload and with STARTTLS)

To configure a Virtual Service for IMAP (without SSL offload and with STARTTLS), follow the steps below in the LoadMaster WUI:

1. In the main menu, select **Virtual Services > Add New**.



2. Enter a valid IP address in the **Virtual Address** text box.
3. Enter **143** as the **Port**.
4. Enter a recognizable **Service Name**, for example **Exchange 2010 IMAP with STARTTLS**.
5. Click **Add this Virtual Service**.
6. Configure the settings as shown in the following table:

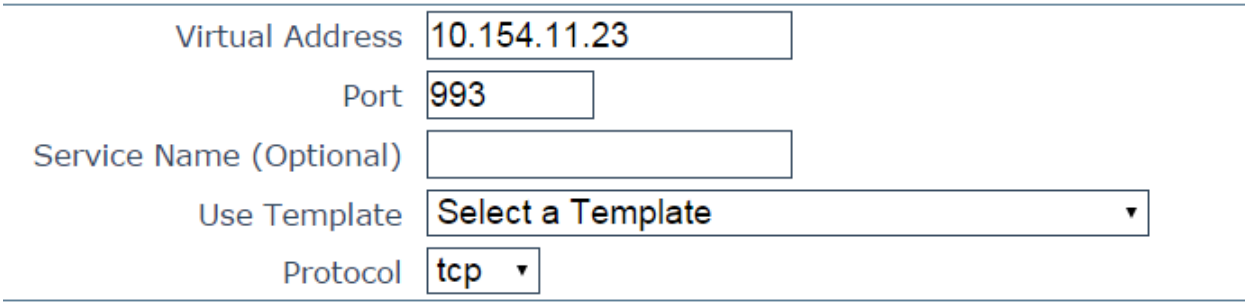
Section	Option	Value	Comment
Basic Properties	Service Type	STARTTLS protocols	
Standard Options	Transparency	Disabled	
	Idle Connection Timeout	3600	Click **Set Idle Timeout**.
Real Servers	Checked Port	143	Click **Set Check Port**.

7. Add any Real Servers as needed.

Configuring a Virtual Service for IMAPS

To configure a Virtual Service for IMAPS, follow the steps below.

1. In the main menu, select **Virtual Services > Add New**.



2. Enter a valid **Virtual Address**.
3. Enter **993** as the **Port**.
4. Enter a recognizable **Service Name**, for example **Exchange 2010 IMAPS**.
5. Click **Add this Virtual Service**.
6. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Standard Options	Transparency	Disabled	
	Server Initiating Protocols	IMAP4	
	Idle Connection Timeout	3600	Click **Set Idle Timeout**.
Real Servers	Checked Port	993	Click **Set Check Port**.

7. Add any Real Servers as needed.

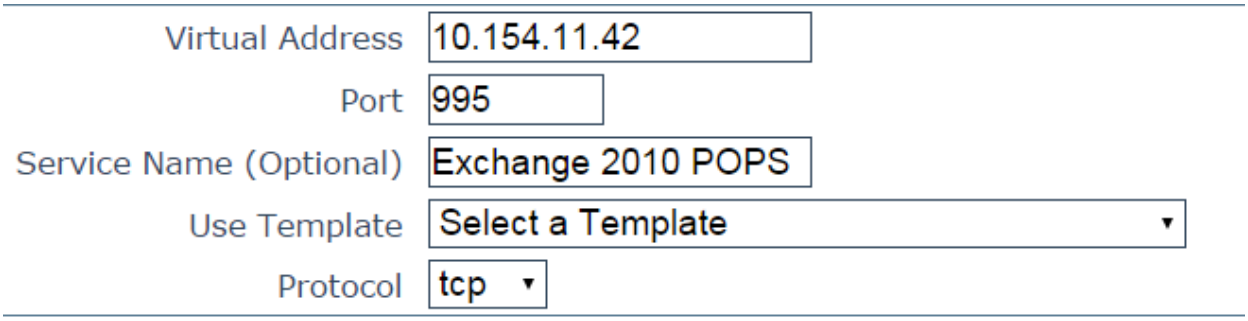
Post Office Protocol (POP3)

Configuring a Virtual Service for POP3 (with SSL Offload)

In general, SSL offloading for POP3 represents a trade-off. When servers are running at 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 using SSL offload with POP3, follow the recommendations set by Microsoft. Progress Kemp understands the recommendations to be; Disable Secure Login as the Authentication method by following the instructions at: http://technet.microsoft.com/en-us/library/

bb676455.aspx.

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter a valid **Virtual Address**.
4. Enter **995** as the **Port**.
5. Enter a recognizable **Service Name**, for example **Exchange 2010 POPS Offloaded**.
6. Select **tcp** as the **Protocol**.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

7. Click **Add this Virtual Service**.
8. Configure the settings as shown in the following table:

Optional: Import the appropriate PFX certificate and key file into the LoadMaster. For instructions on how to do this, refer to the Importing and Assigning an SSL Certificate section.

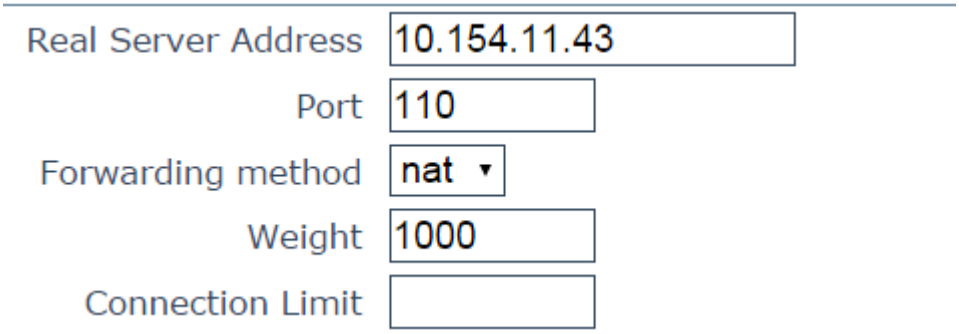
Optional: You can export the appropriate certificate and key from Exchange 2010 using the Microsoft export information found at http://technet.microsoft.com/en-us/library/bb310778.aspx. Ensure to export the certificate and private key as a Personal Information File (PFX). An SSL certificate can be obtained 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 the LoadMaster.

* By default, a self-signed certificate is used. Click **OK** when a message displays indicating that there is no SSL certificate currently available.

Section	Option	Value	Comment
SSL Properties	SSL Acceleration	Enabled*	
Standard Options	Transparency	Disabled	
	Server Initiating Protocols	POP3	
	Idle Connection Timeout	3600	Click **Set Idle Timeout**.

Section	Option	Value	Comment
Real Servers	Real Server Check Method	Mailbox (POP3) Protocol	
	Checked Port	110	Click **Set Check Port**.

9. Click the **Add New…** button.



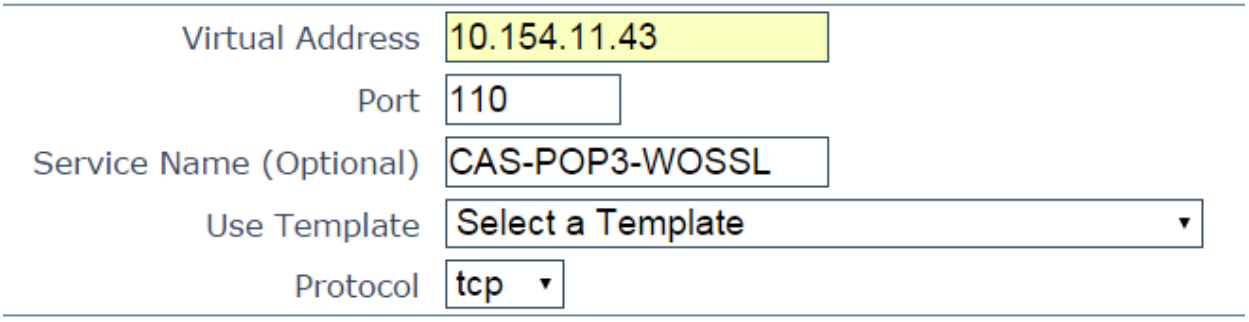
10. Enter the **Real Server Address**.
11. Click **Add This Real Server**.
12. Click **OK** in response to the confirmation that the Real Server was added.

To view, modify, or delete any Virtual Services or Real Servers that have been added, select the **Virtual Services** > **View/Modify Services** option from the main menu of the LoadMaster WUI.

Configuring a Virtual Service for POP (without SSL Offload)

To configure a Virtual Service for POP3, without SSL offload, follow the steps bellow:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter the **Virtual Address**.
4. Enter **110** as the **Port**.

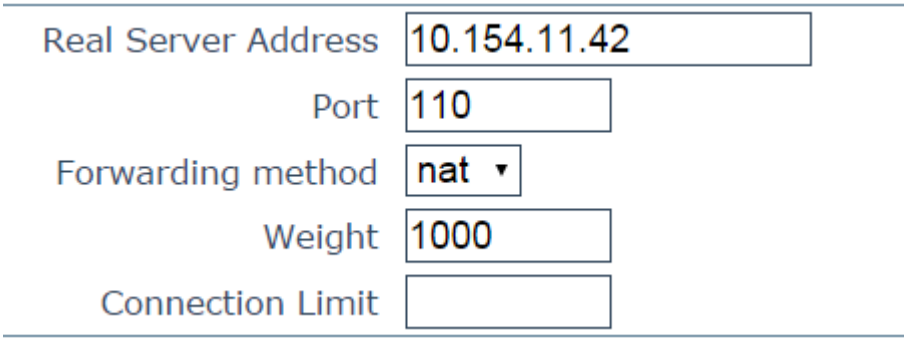
5. Enter a recognizable **Service Name**, for example **CAS-POP3-WOSSL**.
6. Select **tcp** as the **Protocol**.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

7. Click **Add this Virtual Service**.
8. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Idle Connection Timeout	3600	Click **Set Idle Timeout**.
Real Servers	Checked Port	110	Click **Set Check Port**.

9. Click the **Add New…** button.



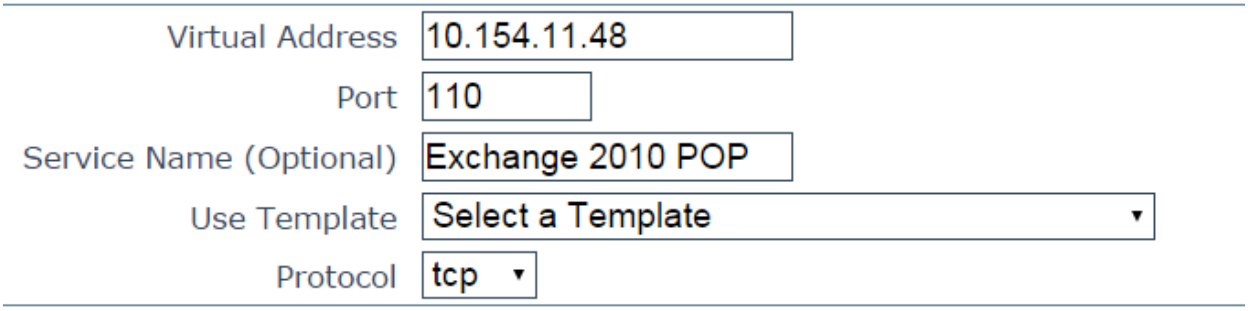
10. Enter the **Real Server Address**.
11. Enter **110** as the **Port**.
12. Click **Add This Real Server**.
13. Click **OK** in response to the confirmation that the Real Server was added.

To view, modify, or delete any Virtual Services or Real Servers, select **Virtual Services** > **View/Modify Services** from the main menu of the LoadMaster WUI.

Configuring a Virtual Service for POP with STARTTLS

To configure a Virtual Service for POP with STARTTLS, follow the steps below:

1. Select **Virtual Services > Add New**.



2. Enter a valid **Virtual Address**.
3. Enter **110** as the **Port**.
4. Enter a recognizable **Service Name**, for example **Exchange 2010 POP with STARTTLS**.
5. Click **Add this Virtual Service**.
6. Configure the settings as shown in the following table:

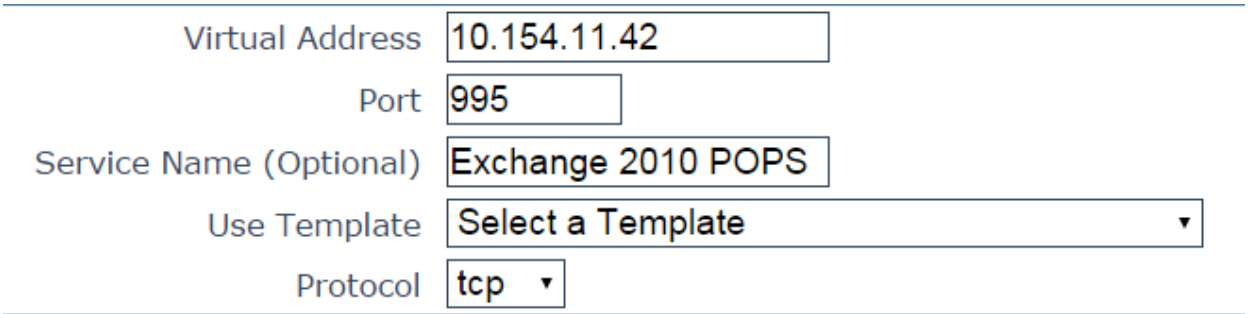
Section	Option	Value	Comment
Basic Properties	Service Type	STARTTLS protocols	
Standard Options	Transparency	Disabled	
	Idle Connection Timeout	3600	Click **Set Idle Timeout**.
Real Servers	Checked Port	110	Click **Set Check Port**.

7. Add any Real Servers as needed.

Configuring a Virtual Service for POPS

To configure a Virtual Service for POPS, follow the steps below:

1. In the main menu, select **Virtual Services > Add New**.



2. Enter a valid **Virtual Address**.
3. Enter **995** as the **Port**.

4. Enter a recognizable **Service Name**, for example **Exchange 2010 POPS**.
5. Click **Add this Virtual Service**.
6. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Standard Options	Transparency	Disabled	
	Server Initiating Protocols	POP3	
	Idle Connection Timeout	3600	Click **Set Idle Timeout**.
Real Servers	Checked Port	995	Click **Set Check Port**.

7. Add any Real Servers as needed.

Simple Mail Transfer Protocol (SMTP)

Edge Transport Servers - Configuring LoadMaster for SMTP

In Microsoft Server 2010, the Edge Transport server role is deployed in an 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 are 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 does not 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.

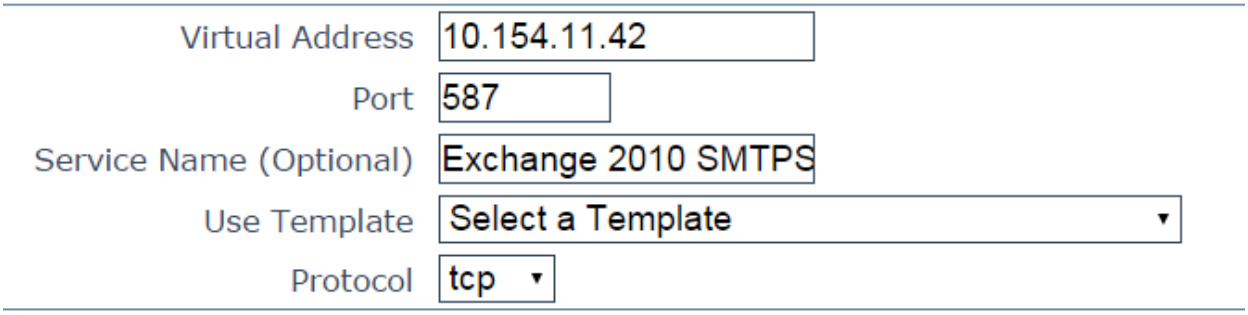
You can install more than one Edge Transport server in the perimeter network. Deploying more than one Edge Transport server provides redundancy and failover capabilities for your inbound message flow. You can load-balance SMTP traffic to your organization between Edge Transport servers by defining more 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 Progress Kemp sales team at http://www.kemptechnologies.com.

Configuring a Virtual Service for SMTPS (with SSL Offload but without ESP)

To configure a Virtual Service for SMTP, with SSL offload, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



3. Enter a valid **Virtual Address**.
4. Enter **587** as the **Port**.
5. Enter a recognizable **Service Name**, for example **Exchange 2010 SMTPS Offloaded**.
6. Select **tcp** as the **Protocol**.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

7. Click **Add this Virtual Service**.
8. Configure the settings as shown in the following table:

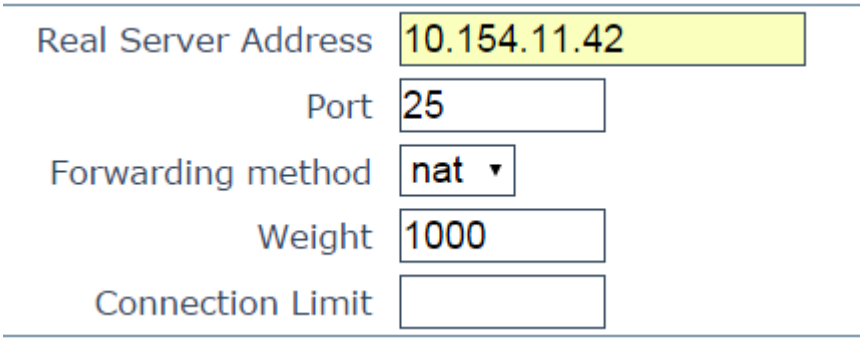
Optional: Import the appropriate PFX certificate and key file into the LoadMaster. For instructions on how to do this, refer to the Importing and Assigning an SSL Certificate section.

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). An SSL certificate can be obtained 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 the LoadMaster.

* By default, a self-signed certificate is used. Click **OK** when a message displays indicating that there is no SSL certificate currently available.

Section	Option	Value	Comment
Standard Options	SSL Acceleration	Enabled*	
	Transparency	Disabled	
	Server Initiating Protocols	SMTP	
	Persistence Mode	Source IP Address	
	Persistence Timeout	1 Hour	
	Idle Connection Timeout	120	Click **Set Idle Timeout**.
Real Servers	Real Server Check Method	Mail (SMTP) Protocol	
	Checked Port	25	Click **Set Check Port**.

9. Click the **Add New…** button.



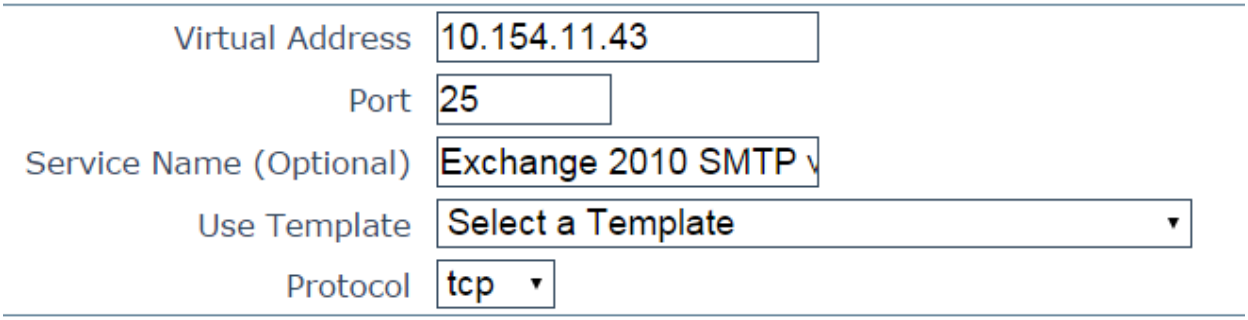
10. Enter the **Real Server Address**.
11. Enter **25** as the **Port**.
12. Click **Add This Real Server**.
13. Click **OK** in response to the confirmation that the Real Server was added.

To view, modify, or delete any Virtual Services or Real Servers that have been added, select **Virtual Services** > **View/Modify Services** in the main menu of the LoadMaster WUI.

Configuring a Virtual Service for SMTP (with ESP)

To configure a Virtual Service for SMTP, with ESP enabled, follow the steps below in the LoadMaster WUI:

1. In the main menu, select **Virtual Services > Add New**.



2. Enter a valid IP address in the **Virtual Address** text box.
3. Enter **25** as the **Port**.
4. Enter a recognizable **Service Name**, for example **Exchange 2010 SMTP with ESP**.
5. Click **Add this Virtual Service**.
6. Configure the settings as shown in the following table:

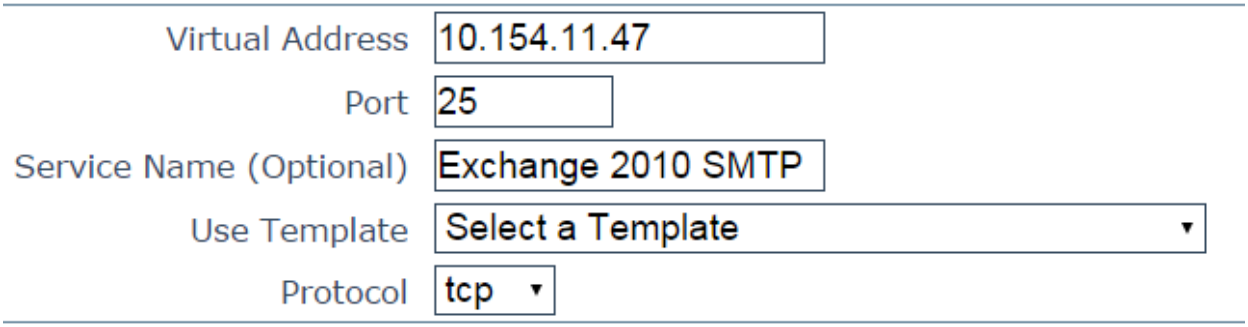
Section	Option	Value	Comment
Standard Options	Transparency	Disabled	
	Persistence Mode	Source IP Address	
	Persistence Timeout	1 Hour	
	Idle Connection Timeout	120	Click **Set Idle Timeout**.
ESP Options	Enable ESP	Enabled	
	Permitted Domains		Enter any **Permitted Domains** and click **Set Permitted Domains**.
Real Servers	Checked Port	25	Click **Set Check Port**.

7. Add any Real Servers as needed.

Configuring a Virtual Service for SMTP (without SSL Offload)

To configure a Virtual Service for SMTP, without SSL offload, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services**.
2. Select **Add New**.



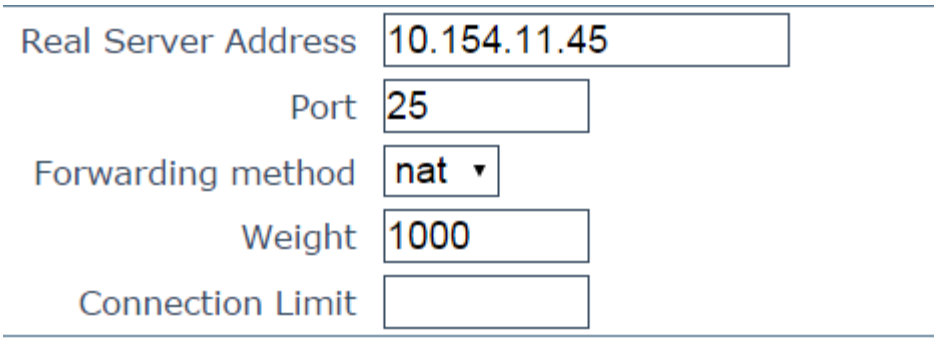
3. Enter a valid **Virtual Address**.
4. Enter **25** as the **Port**.
5. Enter a recognizable **Service Name**, for example **Exchange 2010 SMTP**.
6. Select **tcp** as the **Protocol**.

Note: The combination of **Virtual Address**, **Port** and **Protocol** must be unique within the LoadMaster.

7. Click **Add this Virtual Service**.
8. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Standard Options	Force L4	Disabled	
	Transparency	Disabled	
	Server Initiating Protocols	SMTP	
	Persistence Mode	Source IP Address	
	Persistence Timeout	1 Hour	
	Idle Connection Timeout	120	Click **Set Idle Timeout**.
Real Servers	Real Server Check Method	Mail (SMTP) Protocol	
	Checked Port	25	Click **Set Check Port**.

9. Click the **Add New…** button.



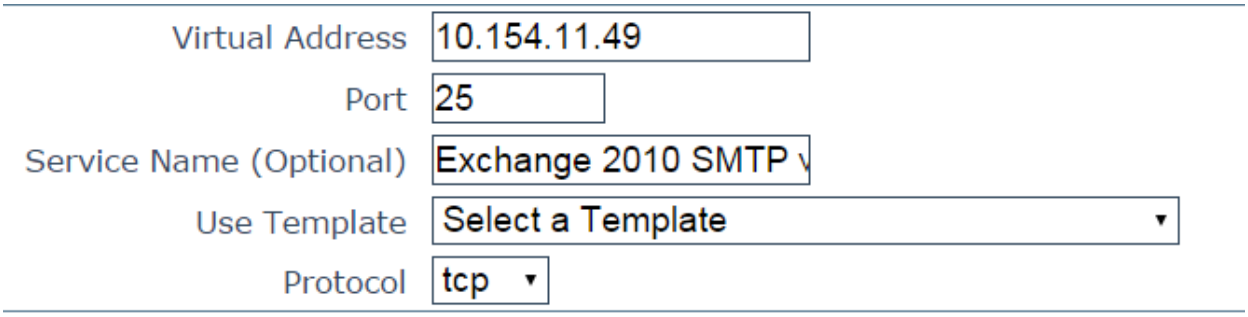
10. Enter the **Real Server Address**.
11. Enter **25** as the **Port**.
12. Click **Add This Real Server**.
13. Click **OK** in response to the confirmation that the Real Server was added.

To view, modify, or delete any Virtual Services or Real Servers that have been added, select **Virtual Services** > **View/Modify Services** in the LoadMaster WUI.

Configuring a Virtual Service for SMTP (with STARTTLS)

To configure a Virtual Service for SMTP with STARTTLS, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services > Add New**.



2. Enter a valid **Virtual Address**.
3. Enter **25** as the **Port**.
4. Enter a recognizable name in the **Service Name** text box, for example **Exchange 2010 SMTP with STARTTLS**.
5. Click **Add this Virtual Service**.
6. Configure the settings as shown in the following table:

Section	Option	Value	Comment
Basic Properties	Service Type	STARTTLS protocols	
Standard Options	Transparency	Disabled	

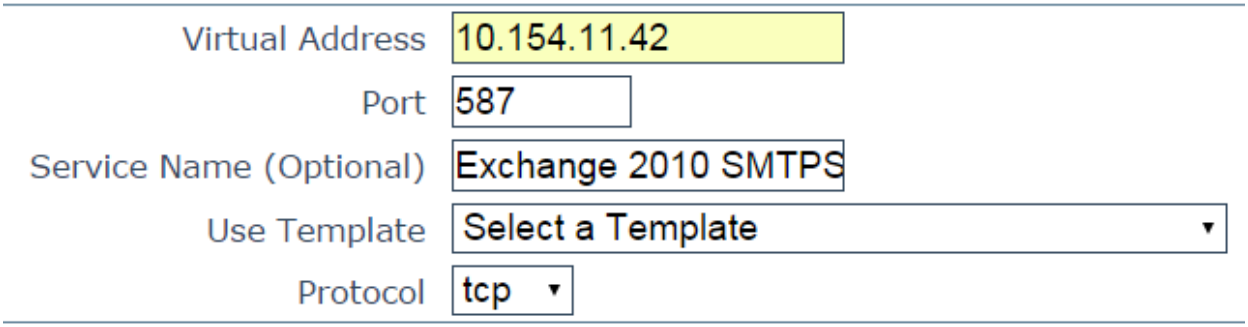
Section	Option	Value	Comment
	Persistence Mode	Source IP Address	
	Persistence Timeout	1 Hour	
	Idle Connection Timeout	120	Click **Set Idle Timeout**.
Real Servers	Checked Port	25	Click **Set Check Port**.

7. Add any Real Servers as needed.

Configuring a Virtual Service for SMTPS

To configure a Virtual Service for SMTPS, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **Virtual Services > Add New**.



2. Enter a valid **Virtual Address**.
3. Enter **587** as the **Port**.
4. Enter a recognizable **Service Name**, for example **Exchange 2010 SMTPS**.
5. Click **Add this Virtual Service**.
6. Configure the settings as shown in the following table:

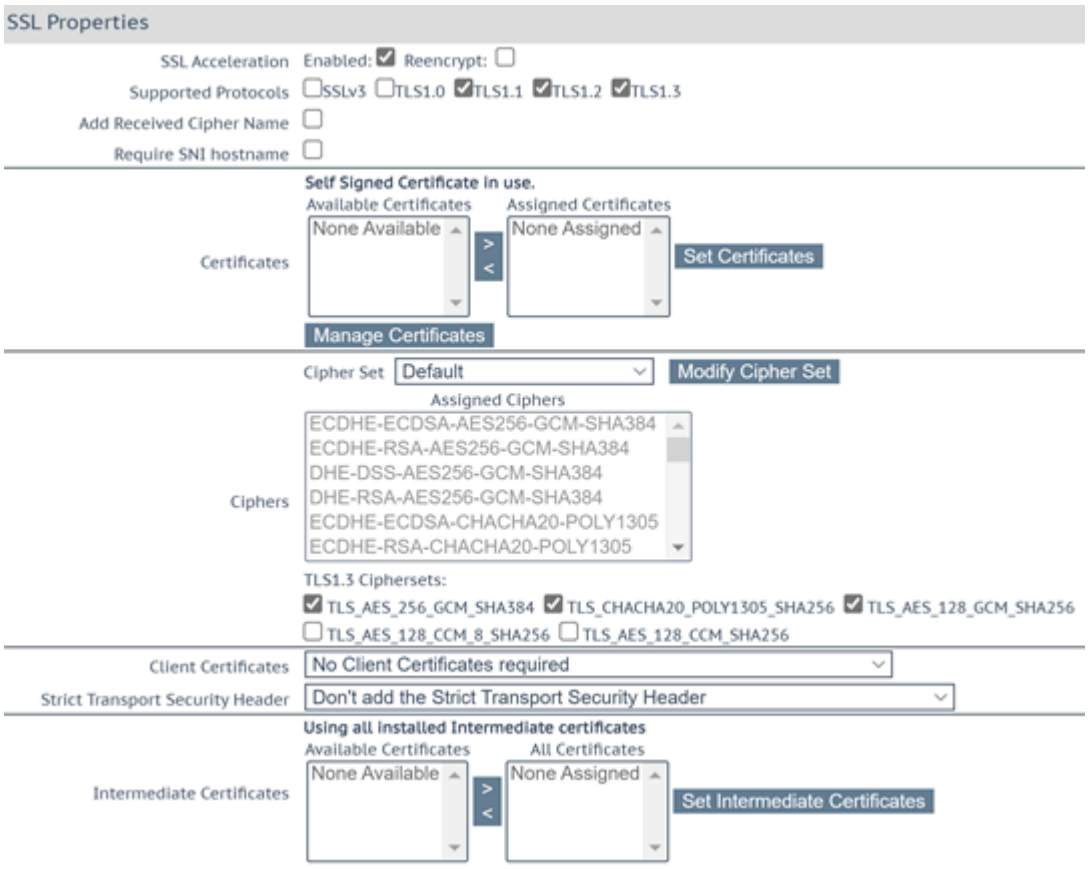
Section	Option	Value	Comment
Standard Options	Transparency	Disabled	
	Server Initiating Protocols	SMTP	
	Persistence Mode	Source IP Address	
	Persistence Timeout	1 Hour	
	Idle Connection Timeout	120	Click **Set Idle Timeout**.

Section	Option	Value	Comment
Real Servers	Checked Port	587	Click **Set Check Port**.

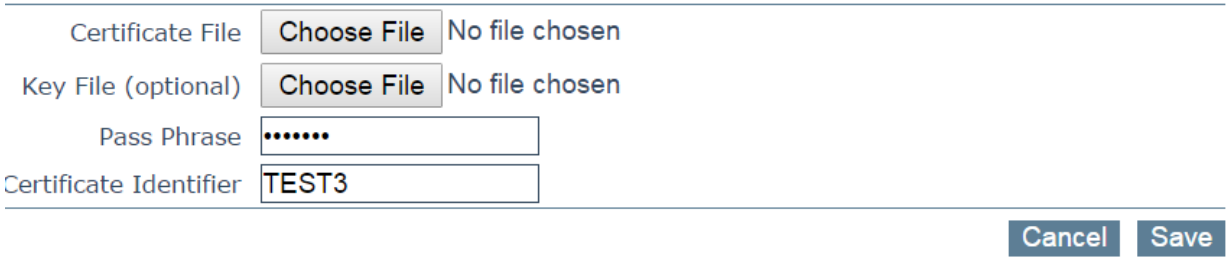
7. Add any Real Servers as needed.

Importing and Assigning an SSL Certificate

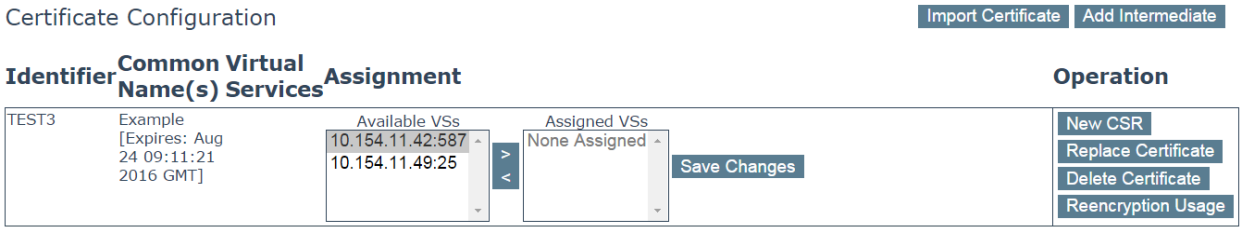
To import an SSL certificate from within the Virtual Services modify screen, in the **SSL Properties** section:



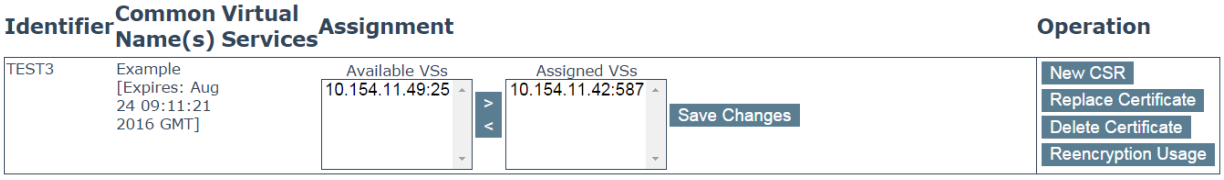
1. Click the **Manage Certificates** button.
2. Click the **Import Certificate** button.



3. Click the **Choose File** button next to **Certificate File**.
4. Locate and open the PFX file.
5. Import a **Key File** if needed.
6. Enter the **Pass Phrase**.
7. Enter a name in the **Certificate Identifier** text box.
8. Click the **Save** button.



9. Select the relevant **Virtual Service**(s) on the left.



10. Click the right arrow to assign the certificate to the Virtual Service.
11. Click **Save Changes**.

You are brought back to the Virtual Service modify screen.

For more information about certificates, refer to the SSL Accelerated Services, Feature Description.

5

Exchange 2010 Site Resiliency and Progress Kemp GEO LoadMaster

The term “site resiliency” refers to the recovery process used to activate an alternate or standby datacenter when the primary datacenter is no longer able to provide a sufficient level of service to meet the needs of the organization.

The term includes the process of re-activating a primary datacenter that has been recovered, restored or recreated. You can configure your messaging solution to enable site resilience using the GEO LoadMaster in conjunction with the built-in features and functionality in Exchange 2010.

Related Links

- Exchange 2010 Data Center Failover

Exchange 2010 Data Center Failover

To better understand the concept of site resiliency, it's helpful to understand the basic operation of an Exchange 2010 data center failover.

1. Typically a site-resilient deployment will contain a stretched Database Availability Group (DAG), that is, a DAG that has members in both data centers. Within a stretched DAG, the majority of the DAG members should be located in the primary data center or, when each data center has the same number of members, the primary data center hosts the witness server. This design guarantees that service will provided in the primary data center, as it will have ‘quorum’, even if network connectivity between the two data centers fails.

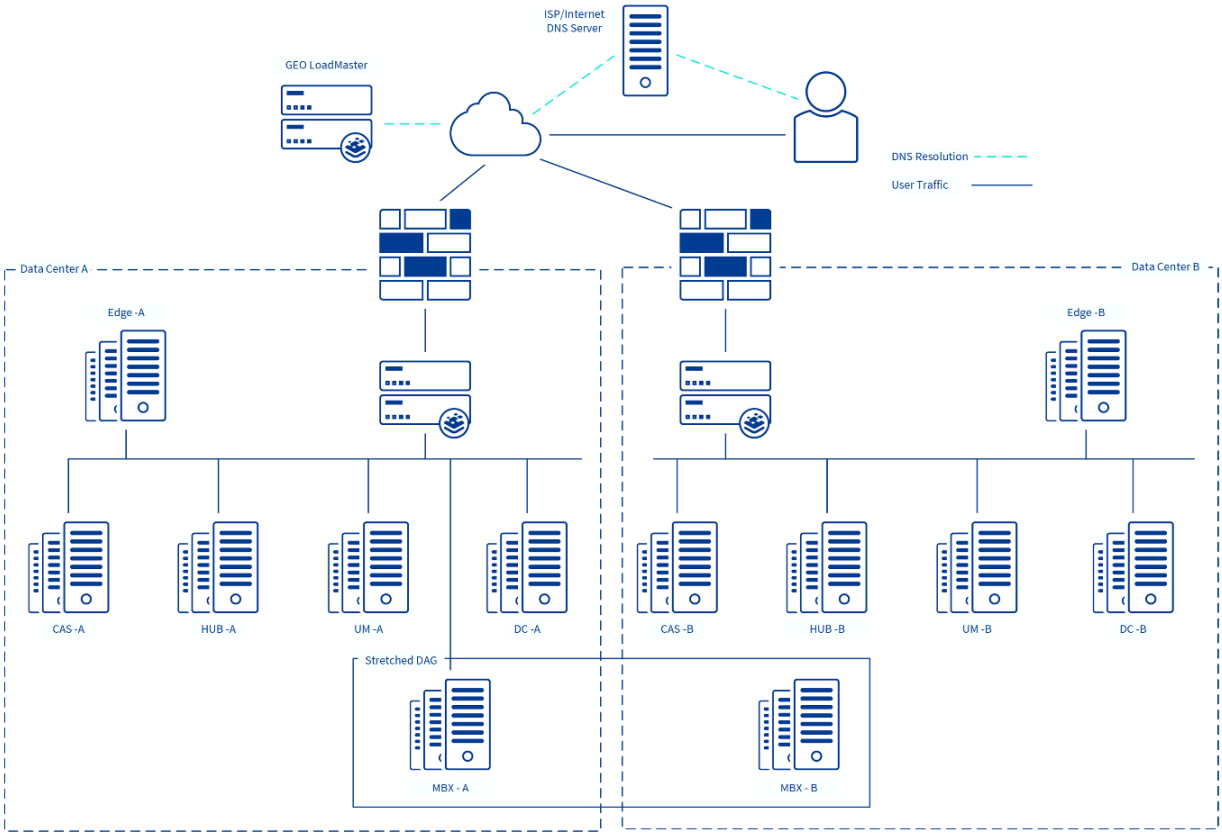
However, it also means that when the primary data center fails the quorum is lost for the members in the second data center.

2. From the point-of-view of site resiliency, the GEO LoadMaster provides automatic site failover options for disaster recovery.

   The GEO LoadMaster also offers DNS load balancing for all active data centers. The GEO LoadMaster can be deployed in a distributed (Active/Active) high availability configuration, with both GEO LoadMaster appliances securely synchronizing information.

   Introducing GEO LoadMaster in your existing Authoritative Domain Name Services (DNS) requires minimal integration work and risk, allowing you to fully leverage your existing DNS investment.

3. The LoadMaster server load balancers located within the datacenter provide highly-available, high-performance load balancing functionality within the individual datacenters. They can also provide a single point for consolidated health checking and provide the GEO LoadMaster with real-time health check information for the datacenter.



With the configuration as described in the above image, when a data center fails, a second data center can be rapidly activated to serve the failed data center's clients. However, a data center or site failure is managed differently from the types of failures that can cause a server or database failover. In a high availability configuration, automatic recovery is initiated by the system, and the failure typically leaves the messaging system in a fully functional state. By contrast, a data center failure is considered to be a disaster recovery event. For recovery to occur, a combination of automatic and manual steps must be performed and completed for the client service to be restored, and for the outage to end. The process followed is referred to as a data center failover.

When a data center or site failure occurs, a number of automatic and manual steps occur. The GEO LoadMaster detects the site failure and automatically switches all traffic from the servers in the failed data center, with the exception of the Mailbox servers, to the servers in the second data center.

Because implementing a data center failover is not a trivial event, it can be useful to avoid such a failover for only transient failures of the primary data center. Upon detection of a site failure, the GEO LoadMaster can be configured to delay initiating the site failover for an administratively-specified period of time. If after the delay the site has recovered, the failover is not initiated. If the site has not recovered, the failover is initiated as per normal. This option ensures that site failovers do not occur because of temporary issues within a site.

The Exchange deployment administrators must now perform a number of steps to complete the data center failover:

1. **Terminate services within the failed data center**. All Mailbox and Unified Messaging services still running within the failed data center must be terminated.
2. **Validate the health of the second data center**. The health of the second data center must be determined to ensure that it is capable of providing adequate service.
3. **Activate the Mailbox servers**. This involves a process of marking the failed servers from the primary data center as unavailable followed by activation of the servers in the secondary data center.

Note: How Step 3 is managed depends on whether the DAG is in Database Activation Coordination (DAC) mode or not. If it is, activating the Mailbox servers can be completed using Exchange site resilience cmdlets. If not, the Windows Failover Cluster tools must be used.

The Failure Delay option can also be useful to ensure that the Exchange deployment administrators have sufficient time to perform the required manual steps as described below. This enables the mailboxes to be correctly configured before the clients begin to attempt access to the secondary data center.

As can be seen from the previous description, a data center failover is not a fully automated process and may take some time to complete. If the failed data center recovers then issues may arise if an attempt to restore services to the recovered data center is initiated (a failback) before the initial failover process is complete and/or until the recovered data center is deemed to be healthy and the mailbox databases are ready for use. It's important that a failback not be performed until the infrastructure dependencies for Exchange have been reactivated, are functioning and stable, and have been validated. If these dependencies are not available or healthy, it's likely that the failback process will cause a longer than necessary outage, and it is possible the process could fail altogether.

To ensure that this cannot occur, the GEO LoadMaster can be configured to administratively disable the failed data center upon the initiation of a failover. This ensures that, even if the failed **data center recovers, administrator intervention is required before the data center is available** for a failback to occur.

For further information on how to configure the GEO LoadMaster to provide Exchange 2010 site resiliency, please refer to the GEO LoadMaster documentation.

6

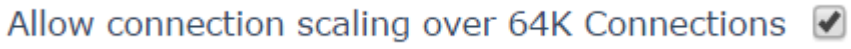
Appendix A: Connection Scaling For Large Scale Deployments

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

You must disable L7 Transparency to use connection scaling.

To use connection scaling, follow the steps below:

1. In the main menu of the LoadMaster WUI, select **System Configuration**.
2. Select **Miscellaneous Options**.
3. Select **L7 Configuration**.



4. Select the **Allow connection scaling over 64K Connections** check box.
5. In the main menu of the LoadMaster WUI, select **Virtual Services**.
6. Select **View/Modify Services**.
7. Click the **Modify** button of the appropriate Virtual Service.
8. Expand the **Advanced Properties** section.
9. Enter a list of **Alternate Source Addresses**.

Note: Multiple IPv4 addresses must be separated with a space, each must be unallocated and allow 64K connections.

10. Click the **Set Alternate Source Addresses** button.

7

Appendix B: Persistence Methods Supported by Each CAS Service

	Workload	Preferred Persistence Method
HTTP-Based Workloads	Outlook Web App (OWA)	1. Super HTTP 2. Source IP
	Exchange Control Panel (ECP)	1. Super HTTP 2. Source IP
	Exchange ActiveSync (EAS)	1. Super HTTP 2. Source IP
	Exchange Web Services (EWS)	1. Super HTTP 2. Source IP

	Workload	Preferred Persistence Method
	Outlook Anywhere (OA)	1. Super HTTP 2. Source IP
	Autodiscover Service (AS)	No affinity/persistence
TCP Socket Oriented Workloads	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)	Source IP

8

Appendix C: Configuration Table

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

Service	Port	Protocol	Server Init	Persist Mode	Persist Timeout	Scheduler	Idle	SSL	Rewrite	Checker	Checker port/ URL
HTTPS offloaded	443	TCP	None	Super	1 Hour	Round Robin	900	Y	None	HTTP	80 /owa
HTTPS	443	TCP	None	Source	1 Hour	Round Robin	900	N		HTTPS	443 /owa
SMTP	25	TCP	SMTP	Source	1 Hour	Round Robin	120	N		SMTP	25
MAPI	*	TCP	Other	Source	1 Hour	Round	86400	N		TCP	135

Service	Port	Protocol	Server Init	Persist Mode	Persist Timeout	Scheduler	Idle	SSL	Rewrite	Checker	Checker port/ URL
						Robin					
HTTPS AS offloaded	443	TCP	None	None		Round Robin	900	Y	None	HTTP	80 /autodiscover/autodiscover.xml
HTTPS AS	443	TCP	None	None		Round Robin	900	N		HTTPS	443 /autodiscover/autodiscover.xml
HTTPS EAS offloaded	443	TCP	None	Super or Source	1 Hour	Round Robin	900	Y	None	HTTP	80 /Microsoft-Server-Activesync
HTTPS EAS	443	TCP	None	Source	1 Hour	Round Robin	900	N		HTTPS	443 /Microsoft-Server-Activesync
HTTPS ECP offloaded	443	TCP	None	Super or Source	1 Hour	Round Robin	900	Y	None	HTTP	80 /ecp

Service	Port	Protocol	Server Init	Persist Mode	Persist Timeout	Scheduler	Idle	SSL	Rewrite	Checker	Checker port/ URL
HTTPS ECP	443	TCP	None	Source	1 Hour	Round Robin	900	N		HTTPS	443 /ecp
HTTPS EWS offloaded	443	TCP	None	Super	1 Hour	Round Robin	900	Y	None	HTTP	80 /ews/exchange.asmx
HTTPS EWS	443	TCP	None	Source	1 Hour	Round Robin	900	N		HTTPS	443 /ews/exchange.asmx
HTTPS OA offloaded	443	TCP	None	Super or Source	1 Hour	Round Robin	900	Y	None	HTTP	80 /rpc/rpcproxy.dll
HTTPS OA	443	TCP	None	Source	1 Hour	Round Robin	900	N		HTTPS	443 /rpc/rpcproxy.dll
HTTPS OWA offloaded	443	TCP	None	Super or Source	1 Hour	Round Robin	900	Y	None	HTTP	80 /owa
HTTPS OWA	443	TCP	None	Source	1 Hour	Round Robin	900	N		HTTPS	443 /owa

Service	Port	Protocol	Server Init	Persist Mode	Persist Timeout	Scheduler	Idle	SSL	Rewrite	Checker	Checker port/ URL
IMAP	143	TCP	IMAP4	None		Round Robin	3600	N		IMAP	143
IMAP with START TLS	143	START TLS		None		Round Robin	3600	Y		IMAP	143
IMAPS	993	TCP	IMAP4	None		Round Robin	3600	N		TCP	993
IMAPS Offloaded	993	TCP	IMAP4	None		Round Robin	3600	Y		IMAP	143
POP	110	TCP	POP3	None		Round Robin	3600	N		POP3	110
POP with START TLS	110	START TLS	POP3	None		Round Robin	3600	Y		POP3	110
POPS	995	TCP	POP3	None		Round Robin	3600	N		TCP	995
POPS Offloaded	995	TCP	POP3	None		Round Robin	3600	Y		POP3	110
SMTP	25	TCP	SMTP	Source IP	1 Hour	Round Robin	120	N		SMTP	25

Service	Port	Protocol	Server Init	Persist Mode	Persist Timeout	Scheduler	Idle	SSL	Rewrite	Checker	Checker port/ URL
SMTP with STARTTLS	25	STARTTLS		Source IP	1 Hour	Round Robin	120	Y		SMTP	25
SMTPS	587	TCP	SMTP	Source IP	1 Hour	Round Robin	120	N		TCP	587
SMTP Offloaded	587	TCP	SMTP	Source IP	1 Hour	Round Robin	120	Y		SMTP	587

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

9

Glossary

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

Acronym	Meaning
AD LDS	Active Directory Lightweight Directory Services
AutoD	AutoDiscover
CAS	Client Access Server
DNS	Domain Name System
EAS	ActiveSync
ECP	Exchange Control Panel

Acronym	Meaning
EWS	Exchange 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

Acronym	Meaning
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
VIP	Virtual IP
VS	Virtual Service
WNLB	Windows Network Server Load Balancing

10

References

Unless otherwise specified, the below documents can be found at:

https://docs.progress.com

SSL Accelerated Services, Feature Description

Web User Interface (WUI), Configuration Guide

Content Rules, Feature Description

Virtual Services and Templates, Feature Description