Progress®
Kemp® LoadMaster®

Deployment Guide MS Exchange 2013

Generated on: 12 January 2026

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 5

Prerequisites 6

Chapter 2: Exchange 2013 Overview 7

Understanding Server Load Balancing 8

Optimizing the LoadMaster for Exchange 2013 8

SSL Acceleration (SSL Offloading) 9

Idle Connection Timeout. 10

Drop Connections on Real Server Failure 10

Drop at Drain Time End 10

Port Configuration. 11

Connection Scaling. 11

Header Rewriting 11

Enable Subnet Originating Requests Globally 11

100-Continue Handling 12

Additional L7 Header. 12

Chapter 3: Virtual Service Templates 14

Chapter 4: Configuring Virtual Services for Exchange 2013 15

HTTPS Offloaded or Reencrypted without ESP 16

Add SSL/TLS Certificate. 16

Add the Real Servers 17

HTTPS Offloaded Virtual Service or Reencrypted with ESP Virtual Service. 18

Add SSL/TLS Certificate. 19

Add the Real Servers 20
Configure ESP 20
IMAP or IMAPS Virtual Service 22
IMAPS Offloaded or IMAP with STARTTLS Virtual Service 22
POP or POPS Virtual Service 23
POPS Offloaded or POP with STARTTLS Virtual Service 24
SMTP or SMTPS Virtual Service 25
SMTPS Offloaded or SMTP with STARTTLS Virtual Service 25
SMTP with ESP Virtual Service 26

Chapter 5: Exchange 2013 Virtual Service Recommended Settings (Optional) 28
Exchange 2013 HTTP Virtual Service Recommended Settings (Optional) 28
Exchange 2013 IMAP Virtual Service Recommended Settings (Optional) 41
Exchange 2013 POP Virtual Service Recommended Settings (Optional) 46
Exchange 2013 SMTP Virtual Service Recommended Settings (Optional) 51

Chapter 6: References 58

1

Introduction

The LoadMaster combines versatility with ease-of-use to speed deployment of the complete portfolio of advanced messaging applications and protocols used by Microsoft Exchange 2013 (Exchange 2013), including Outlook on the Web, MAPI/HTTP, Outlook Anywhere (OA), Exchange ActiveSync (EAS), Simple Mail Transfer Protocol (SMTP), Post Office Protocol version 3 (POP3), Internet Message Access Protocol version 4 (IMAP4) and Office Online Server (OOS). With built-in SSL acceleration and/or overlay, the LoadMaster offloads a key source of CPU drain to improve the capacity of the Exchange 2013 infrastructure. Layer 7 health checking at the LoadMaster ensures that if one of the client access components becomes inaccessible, the load balancer will take that component offline for that server, while automatically re-routing and reconnecting users to other functioning servers.

The entire LoadMaster product family, including the Virtual LoadMaster (VLM) supports Exchange 2013, and includes a comprehensive first year warranty and technical support agreement.

About This Manual

This manual addresses how to deploy and configure a LoadMaster appliance with Exchange 2013 using Progress Kemp application templates.

Kemp's 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.

Contents

- Prerequisites

Prerequisites

It is assumed that the reader is a network administrator or familiar with networking and general computer terminology. It is further assumed that the Exchange 2013 environment is set up and the LoadMaster is installed.

The LoadMaster documentation is available here: LoadMaster documentation page.

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)

2

Exchange 2013 Overview

Microsoft Exchange Server is a mail server, calendaring software, and contact manager. It runs on Windows Server and is part of the Microsoft Servers line of products. The improvements made in Exchange 2013 have made it easier to load balance Exchange-related traffic.

Exchange 2013 includes the following solutions for switchover and failover redundancy:

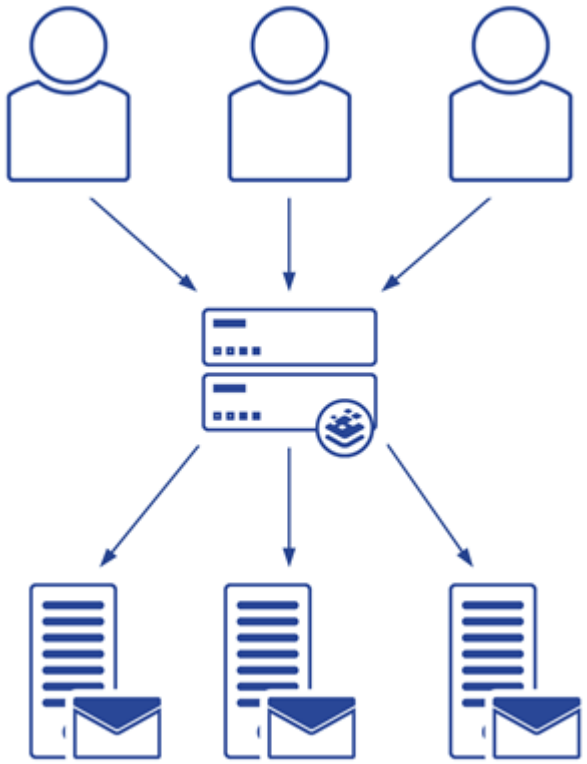
- **High availability:** Exchange 2013 uses Database Availability Groups (DAGs) to keep multiple copies of your mailboxes on different servers synchronized. That way, if a mailbox database fails on one server, users can connect to a synchronized copy of the database on another server.
- **Site resilience:** You can deploy two active directory sites in separate geographic 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:** During an online mailbox move, email accounts are still accessible. Users are only locked out for a brief period at the end of the process when the final synchronization occurs. Online mailbox moves can be performed 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 are 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.

Contents

- Understanding Server Load Balancing
- Optimizing the LoadMaster for Exchange 2013
- Enable Subnet Originating Requests Globally

- 100-Continue Handling
- Additional L7 Header

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 server failures within an exchange organization. In addition, server load balancing ensures that the load on the CAS and transport services are optimally distributed.

As OWA is rendered on the same server that is hosting the user's mailbox database; if a client hits a different CAS, there is no performance degradation because the session rendering for that user is already up and running.

Forms-based authentication is improved. The authentication cookie is provided to the user after logon and it is encrypted using the CAS's SSL certificate. This allows a logged in user to resume their session on a different CAS without having to re-authenticate (if servers share the same SSL certificate).

Optimizing the LoadMaster for Exchange 2013

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 2013 server load balancing requirements.

Contents

- SSL Acceleration (SSL Offloading)
- 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 SSL reencryption. Review the SSL Accelerated Services Feature Description for further details on configuring an SSL reencryption deployment.

With SSL reencryption, 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 2013 configuration instructions indicate that you would first need to export an appropriately signed certificate from Exchange 2013 so that you may import it into the LoadMaster.

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. To make optimal use of your LoadMaster, you should not set these timeout values too low because 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 is found on the **System Configuration > Miscellaneous > L7 Configuration** screen in the WUI.

When this option is enabled, LoadMaster severs all existing connections to a disabled server after the **L7 Connection Drain Time** is reached. Clients are then forced to re-establish a connection to one of the remaining Real Servers. You can configure the **L7 Connection Drain Time** by going to the following screen in the WUI: **System Configuration Miscellaneous Options > L7 Configuration**.

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 https://docs.microsoft.com/en-us/exchange/network-ports-for-clients-and-mail-flow-in-exchange-2013-exchange-2013-help.

Connection Scaling

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

Note: This is only possible with unencrypted or SSL-offloaded traffic.

Enable Subnet Originating Requests Globally

It is best practice to enable the **Subnet Originating Requests** option globally.

In a one-armed setup (where the Virtual Service and Real Servers are on the same network/subnet) **Subnet Originating Requests** is usually not needed. However, enabling **Subnet Originating Requests** should not affect the routing in a one-armed setup.

In a two-armed setup where the Virtual Service is on network/subnet A, for example, and the Real Servers are on network B, **Subnet Originating Requests** should be enabled on LoadMasters with firmware version 7.1-16 and above.



When **Subnet Originating Requests** is enabled, the Real Server sees traffic originating from 10.20.20.21 (LoadMaster eth1 address) and responds correctly in most scenarios.

With **Subnet Originating Requests** disabled, the Real Server sees traffic originating from 10.0.0.15 (LoadMaster Virtual Service address on **eth0**) and responds to **eth0** which could cause asymmetric routing.

When **Subnet Originating Requests** is enabled globally, it is automatically enabled on all Virtual Services. If the **Subnet Originating Requests** option is disabled globally, you can choose whether to enable **Subnet Originating Requests** on a per-Virtual Service basis.

To enable **Subnet Originating Requests** globally, follow the steps below:

1. In the main menu of the LoadMaster User Interface (UI), go to **System Configuration > Miscellaneous Options > Network Options**.
2. Select the **Subnet Originating Requests** check box.

100-Continue Handling

To avoid issues with Exchange Web Services, especially in hybrid configuration, configure 100-continue handling to comply with RFC-7231 instead of the standard setting of RFC-2616.

To resolve this issue, apply the following setting on the LoadMaster.

100-Continue handling = RFC-7231 Complaint

To select **RFC-7231 Compliant** globally, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to **System Configuration > Miscellaneous Options > L7 Configuration**.



2. Select **RFC-7231 Complaint** under **100-Continue Handling**.

Additional L7 Header

When using the built-in Mail client on Mac, you may experience connectivity issues. This happens due to how Mail client on Mac handles Persistent-Auth headers from Exchange server. This behavior is not present on Outlook for Mac clients or any Windows Office clients.

To resolve this issue, apply the following settings on the LoadMaster.

Additional L7 Header = None

To select **None** for **Additional L7 Header** globally, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to **System Configuration > Miscellaneous Options > L7 Configuration**.



2. Select **None** under **Additional L7 Header**.

3

Virtual Service Templates

Progress Kemp have developed templates containing our recommended settings for Exchange 2013. 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**.

This guide outlines the step for setting up Virtual Services using Progress Kemp Application Templates.

The Exchange 2013 templates currently available are grouped in three downloadable files as follows:

- **Exchange2013Core** This file contains templates for non-SSL offloaded HTTPS, SSL offloaded HTTPS, and SMTP Virtual Services.This is the primary set of services required to balance Exchange 2013.
- **Exchange2013ESP** This set contains individual templates for a HTTPS service with SSL offloading and an SMTP service, both with ESP enabled. These services are only necessary if you want to use ESP functionality.
- **Exchange2013Additional** This set contains templates for IMAP, POP, and SMTP services, including variants for STARTTLS and SSL secured services.

4

Configuring Virtual Services for Exchange 2013

Follow the instructions below to set up an Exchange Virtual Services using application templates.

To configure the Virtual Services using the Application Programming Interface (API), refer to the RESTful API documentation.

The Exchange 2013 Virtual Service Recommended API Settings (Optional) outlines the recommended settings and values. You can use the API parameters and values when using the LoadMaster API and automation tools.

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.

Contents

- HTTPS Offloaded or Reencrypted without ESP
- HTTPS Offloaded Virtual Service or Reencrypted with ESP Virtual Service
- IMAP or IMAPS Virtual Service
- IMAPS Offloaded or IMAP with STARTTLS Virtual Service
- POP or POPS Virtual Service
- POPS Offloaded or POP with STARTTLS Virtual Service
- SMTP or SMTPS Virtual Service

- SMTPS Offloaded or SMTP with STARTTLS Virtual Service
- SMTP with ESP Virtual Service

HTTPS Offloaded or Reencrypted without ESP

The steps are the same when using Exchange HTTPS Offloaded and Exchange HTTPS Reencrypted application templates. To add the Virtual Services for Exchange HTTPS Offloaded or Exchange HTTPS Reencrypted, using the template, follow the steps below:

1. Click **Virtual Services**.
2. Click **Add New**.
3. Enter a **Virtual Address**.
4. Select the **Exchange 2013 HTTPS Offloaded** or the **Exchange 2013 HTTPS ReEncrypted** template from the **Use Template** drop-down list depending on your preference.
5. Click **Add This Virtual Service**.

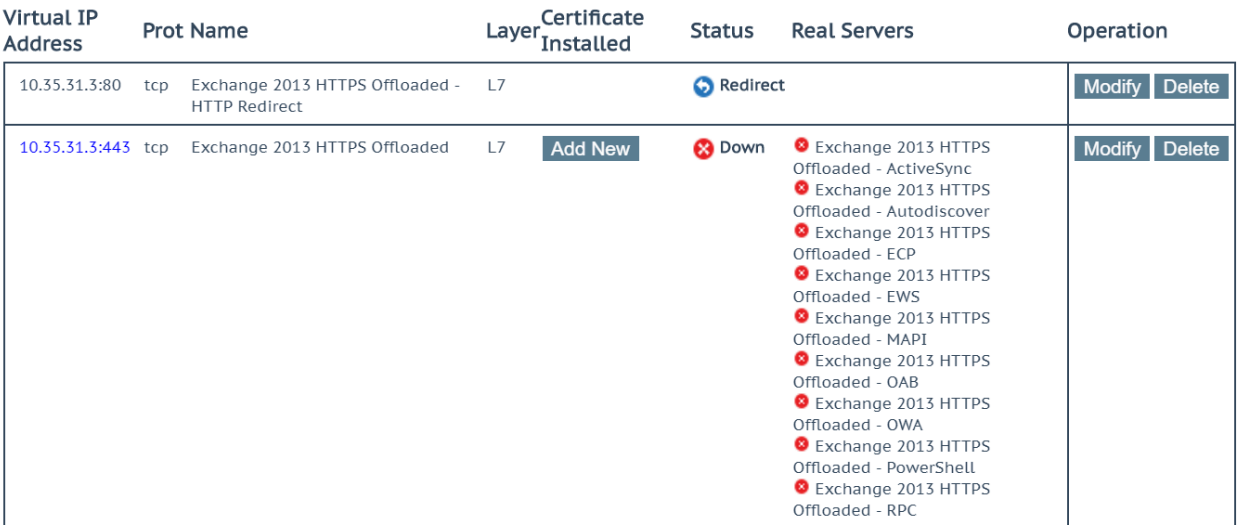
Contents

- Add SSL/TLS Certificate
- Add the Real Servers

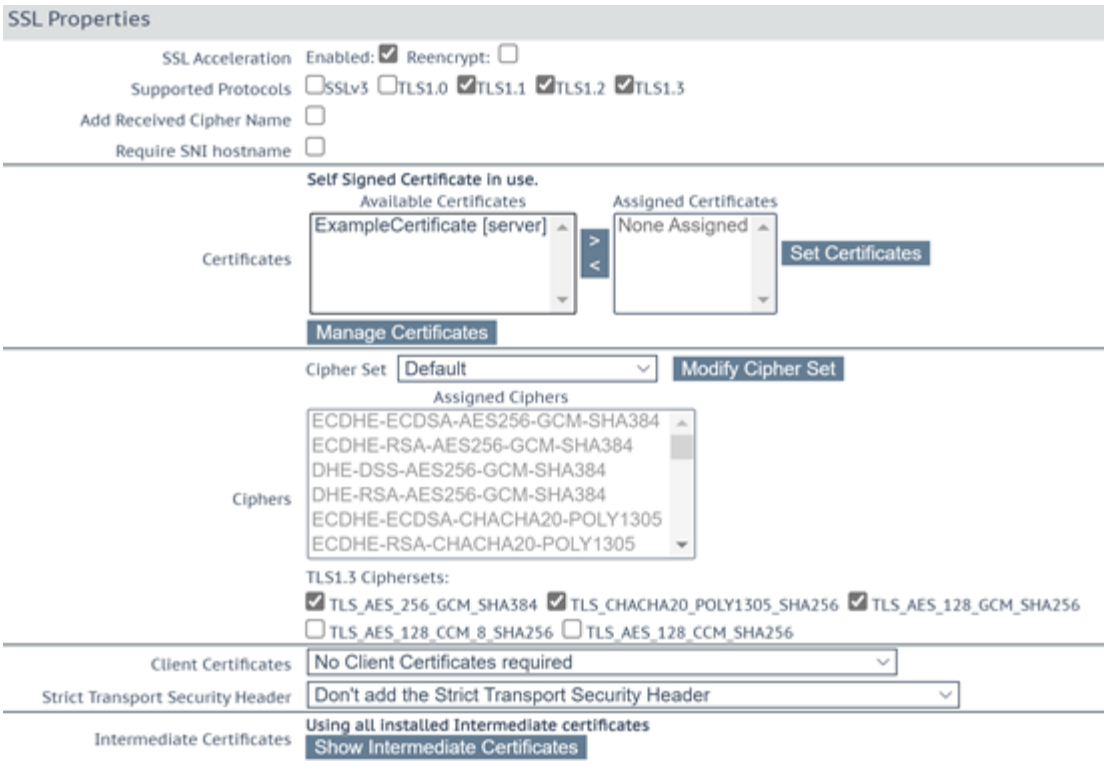
Add SSL/TLS Certificate

This guide assumes an SSL/TLS certificate is imported into the LoadMaster. For more information and steps for SSL/TLS configuration, refer to the SSL Accelerated Services Feature Description.

1. Click **View/Modify Services** in the left-hand navigation.



2. Click **Modify** for the **Exchange 2013 HTTPS Offloaded** Virtual Service on port 443 (or **Exchange 2013 HTTPS Reencrypted** if that was selected during the creation)
3. Expand **SSL Properties (Acceleration Enabled)**.

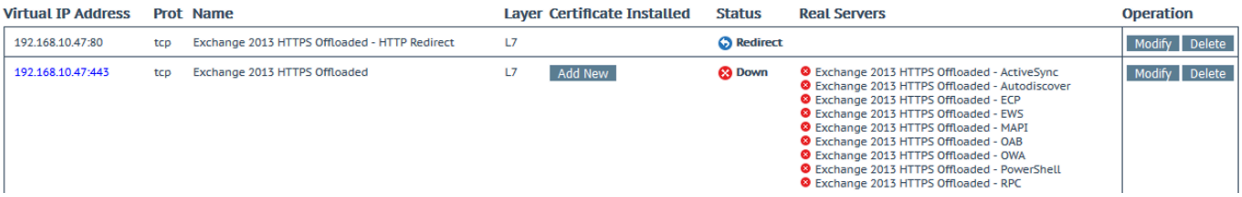


4. Select the certificate to use in the **Available Certificates** and click the “arrow” > to move it to **Assigned Certificates**.
5. Click **Set Certificate**.

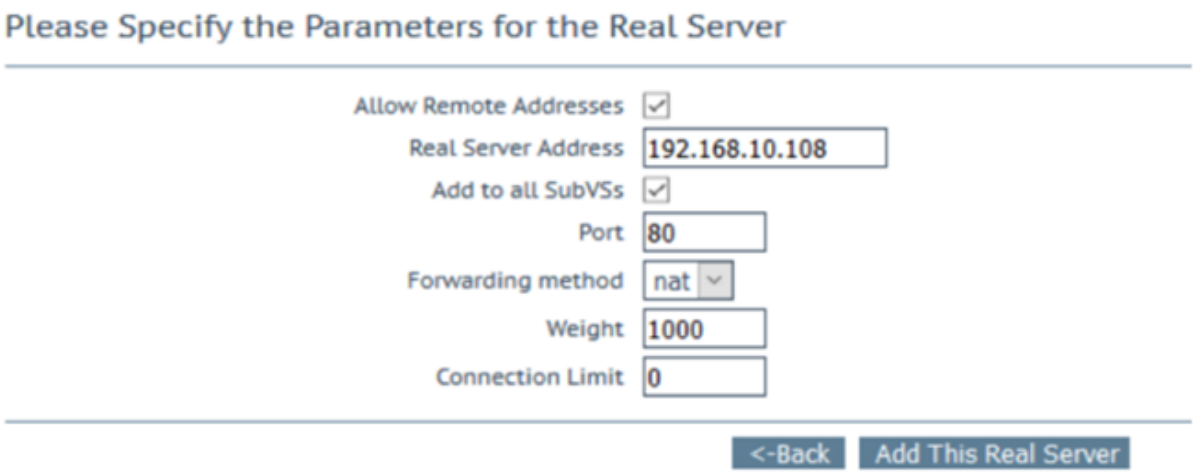
Note: The **Reencrypt** check box is selected when using the Exchange 2013 HTTPS Reencrypted template.

Add the Real Servers

1. Click **View/Modify Services** in the left-hand navigation.



2. Click **Modify** for the **Exchange 2013 HTTPS Offloaded** Virtual Service on port 443 (or the **Exchange 2013 HTTPS Reencrypted** if that was selected during the creation).
3. Expand the **SubVSs** section.
4. Click **Modify** for **Exchange 2013 HTTPS Offloaded – ActiveSync** (or the **Exchange 2013 HTTPS Reencrypted – ActiveSync** if that was selected during the creation).
5. Expand the **Real Servers** section.
6. Click **Add New**.



7. For the **Real Server Address**, enter the IP Address for one of the Exchange Servers.
8. Select the **Add to all SubVSs** check box.
9. Click **Add This Real Server**.
10. Add additional Real Servers using the **Add to all SubVSs** check box.

Note: The **Authentication Proxy** SubVS should not have a Real Server unless Kerberos Constrained Delegation (KCD) is in use.

HTTPS Offloaded Virtual Service or Reencrypted with ESP Virtual Service

The steps are the same when using Exchange HTTPS Offloaded and Exchange HTTPS Reencrypted with ESP application template. To add the Virtual Services for Exchange HTTPS Offloaded or Exchange HTTPS Reencrypted with ESP using the template, follow the steps below:

1. Click **Virtual Services**.
2. Click **Add New**.
3. Enter a **Virtual Address**.
4. Select the **Exchange 2013 HTTPS Offloaded with ESP** or the **Exchange 2013 HTTPS ReEncrypted with ESP** template from the **Use Template** drop-down list depending on your preference.
5. Click **Add This Virtual Service**.

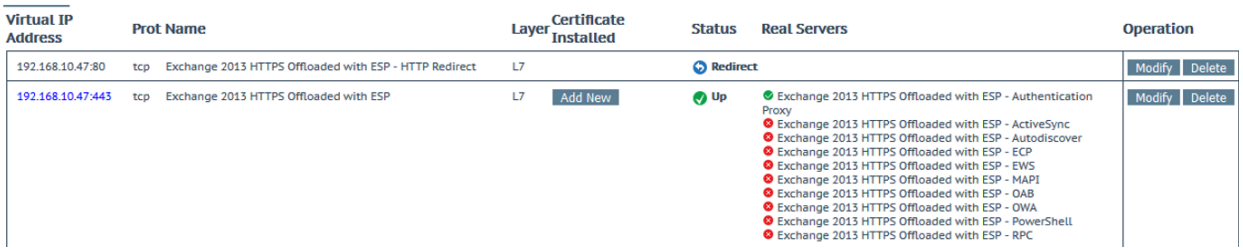
Contents

- Add SSL/TLS Certificate
- Add the Real Servers
- Configure ESP

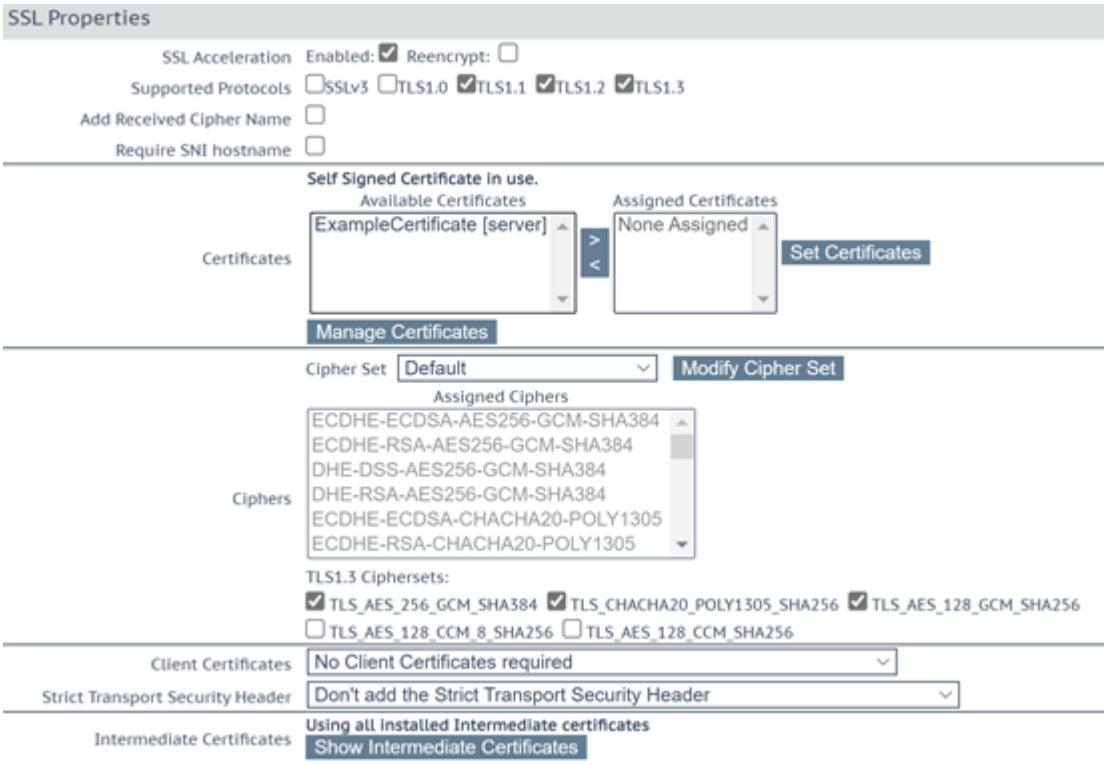
Add SSL/TLS Certificate

This guide assumes an SSL/TLS certificate is imported into the LoadMaster. For more information and steps for SSL/TLS configuration, refer to the SSL Accelerated Services Feature Description.

1. Click **View/Modify Services** in the left-hand navigation.



2. Click **Modify** for the **Exchange 2013 HTTPS Offloaded with ESP** Virtual Service on port 443 (or **Exchange 2013 HTTPS Reencrypted with ESP** if that was selected during the creation)
3. Expand **SSL Properties (Acceleration Enabled)**.

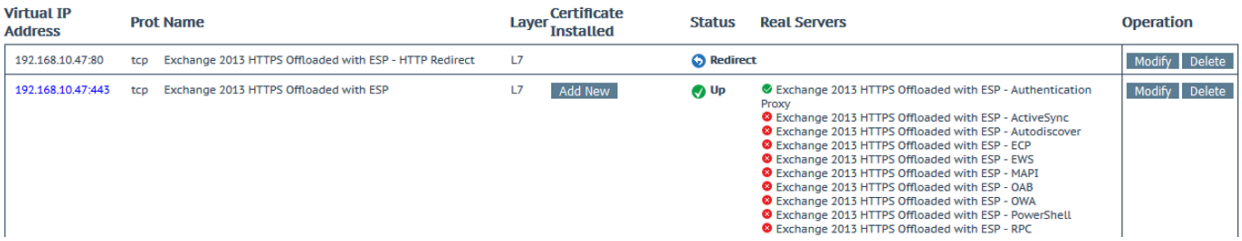


4. Select the certificate to use in the **Available Certificates** and click the “arrow” > to move it to **Assigned Certificates**.
5. Click **Set Certificate**.

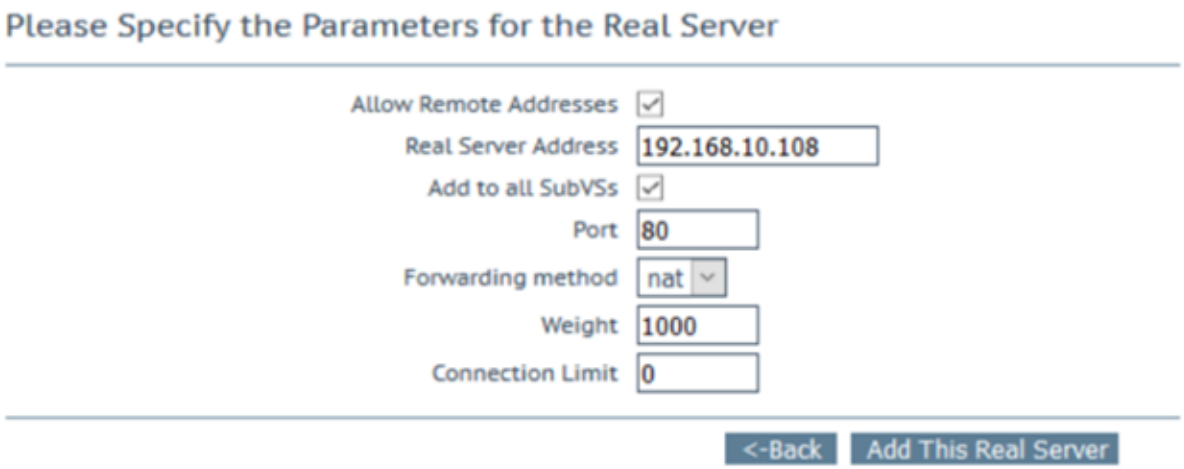
Note: The **Reencrypt** check box is selected when using the **Exchange 2013 HTTPS Reencrypted with ESP** template.

Add the Real Servers

1. Click **View/Modify Services** in the left-hand navigation.



2. Click **Modify** for the **Exchange 2013 HTTPS Offloaded with ESP** Virtual Service on port 443 (or the **Exchange 2013 HTTPS Reencrypted with ESP** if that was selected during the creation).
3. Expand the **SubVSs** section.
4. Click **Modify** for **Exchange 2013 HTTPS Offloaded with ESP – Authentication Proxy** (or the **Exchange 2013 HTTPS Reencrypted with ESP – Authentication ctiveSync** if that was selected during the creation).
5. Expand the **Real Servers** section.
6. Click **Add New**.

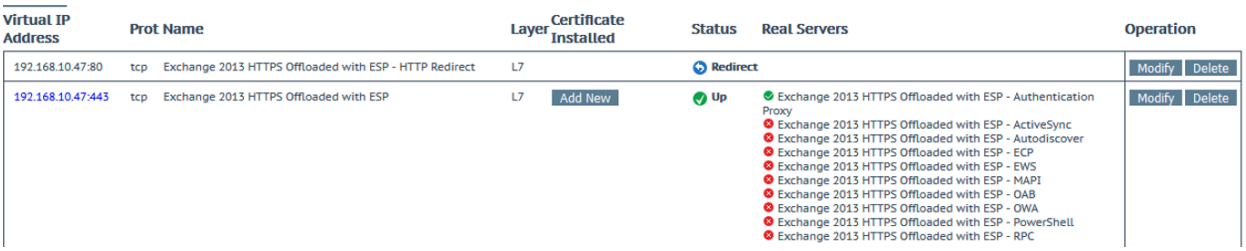


7. For the **Real Server Address**, enter the IP Address for one of the Exchange Servers.
8. Select the **Add to all SubVSs** check box.
9. Click **Add This Real Server**.
10. Add additional Real Servers using the **Add to all SubVSs** check box.

Configure ESP

This guide assumes an SSO Domain is configured on the LoadMaster. For more information and steps for setting up an SSO Domain, refer to the Edge Security Pack (ESP) Feature Description.

1. Click **View/Modify Services** in the left-hand navigation.



2. Click **Modify** for the **Exchange 2013 HTTPS Offloaded with ESP** Virtual Service on port 443 (or the **Exchange 2013 HTTPS Reencrypted with ESP** if that was selected during the creation).
3. Expand the **SubVSs** section.
4. For each SubVS the following fields must be configured. Click the **set** button next to each field entered.

SubVS Name	Pre-Authorization Excluded Directories	Allowed Virtual Hosts	Logoff String	User Password Form
Authentication Proxy	n/a	Required	n/a	n/a
ActiveSync	n/a	Required	n/a	n/a
Autodiscover	n/a	Required	n/a	n/a
ECP	n/a	Required	n/a	n/a
EWS	n/a	Required	n/a	n/a
MAPI	n/a	Required	n/a	n/a
OAB	n/a	Required	n/a	n/a
OWA	/owa/<guid@smtpdomain>*[1]	Required	/owa/logoff.owa	https://<Exchange URL> /owa/auth/expiredpassword.aspx?url=/owa/auth.owa
PowerShell	n/a	Required	n/a	n/a
RPC	n/a	Required	n/a	n/a

Note: [1]GUID is unique to each Exchange deployment. To find the correct GUID, run the following command on the Exchange Server: **Get-Mailbox -Arbitration | where {$_.PersistedCapabilities -like "OrganizationCapabilityClientExtensions"} | fl exchangeGUID, primarysmtpaddress**

Note: The **Logoff String** must be set to **/owa/logoff.owa** in the OWA SubVS. In a customized environment, if the OWA logoff string has been changed, the modified logoff string must be entered in the **Logoff String** text box.

Note: The SSO Greeting Message field accepts HTML code, so the users can insert their own image if desired. The grave accent character (` ) is not supported. If this character is entered in the SSO Greeting Message, the character will not display in the output, for example, **a`b`c** becomes **abc**.

IMAP or IMAPS Virtual Service

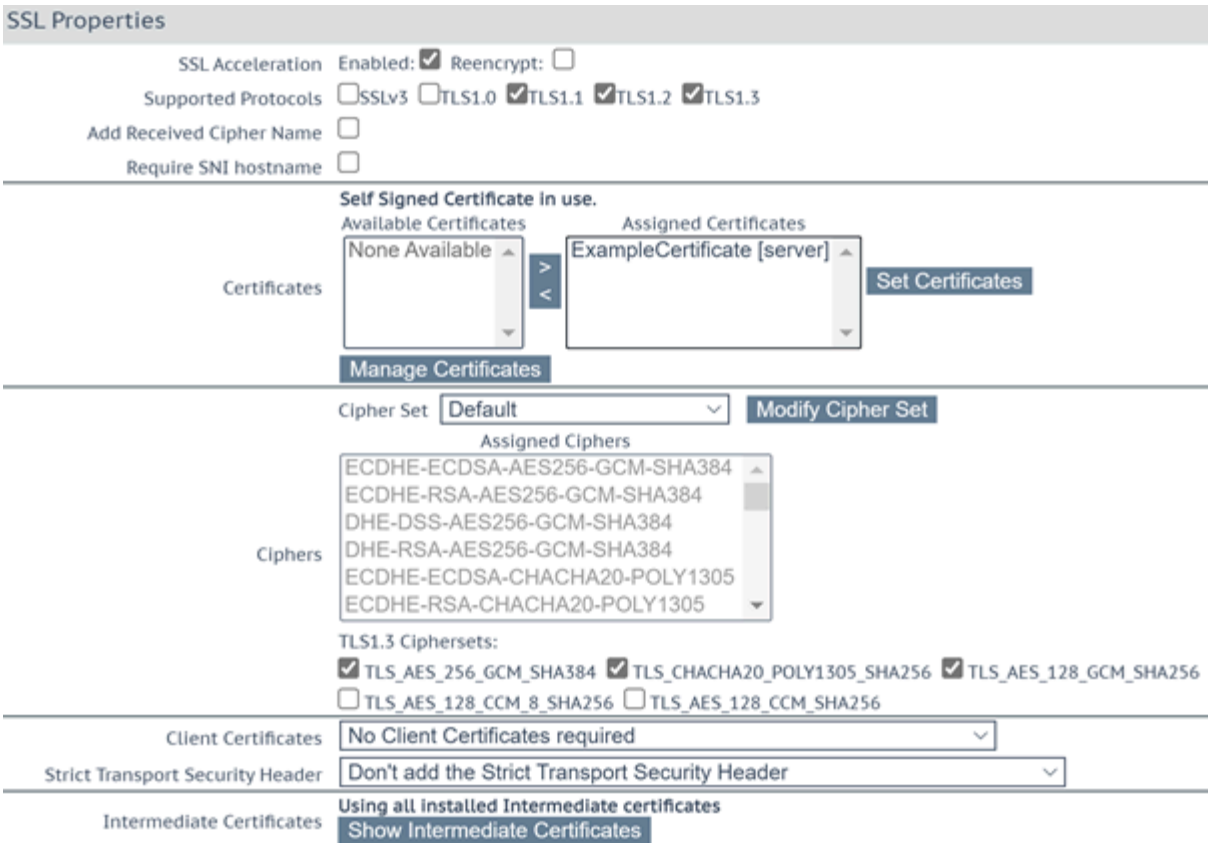
The steps are the same when using Exchange IMAP and Exchange IMAPS application templates. When using IMAPS, this is a TLS pass through Virtual Service because using reencryption is not supported. To add the Virtual Services for Exchange IMAP and Exchange IMAPS using the template, follow the steps below:

1. Click **Virtual Services**.
2. Click **Add New**.
3. Enter a **Virtual Address**.
4. Select the **Exchange 2013 IMAP** or the **Exchange 2013 IMAPS** template from the **Use Template** drop-down list depending on your preference.
5. Click **Add This Virtual Service**.
6. Expand the **Real Servers** section.
7. Click **Add New**.
8. For **Real Server Address**, enter the **IP Address** for one of the Exchange Servers.
9. Click **Add this Real Server**.
10. Add any additional Real Servers as required.

IMAPS Offloaded or IMAP with STARTTLS Virtual Service

The steps are the same when using Exchange IMAPS Offloaded and Exchange IMAP with STARTTLS application templates. To add the Virtual Services for Exchange IMAPS Offloaded and Exchange IMAP with STARTTLS using the template, follow the steps below:

1. Click **Virtual Services**.
2. Click **Add New**.
3. Enter a **Virtual Address**.
4. Select the **Exchange 2013 IMAP Offloaded** or the **Exchange 2013 IMAPS** template from the **Use Template** drop-down list depending on your preference.
5. Click **Add This Virtual Service**.
6. Expand **SSL Properties (Acceleration Enabled)**.



7. Select the certificate to use in the **Available Certificates** and click the “arrow” > to move it to **Assigned Certificates**.
8. Click **Set Certificate**.
9. Expand the **Real Servers** section.
10. Click **Add New**.
11. For **Real Server Address**, enter the IP Address for one of the Exchange Servers.

    Note: Ensure port 143 is entered in the **Port** field.

12. Click **Add this Real Server**.
13. Add any additional Real Servers as required.

POP or POPS Virtual Service

The steps are the same when using Exchange POP and Exchange POPS application templates. To add the Virtual Services for Exchange POP and Exchange POPS using the template, follow the steps below:

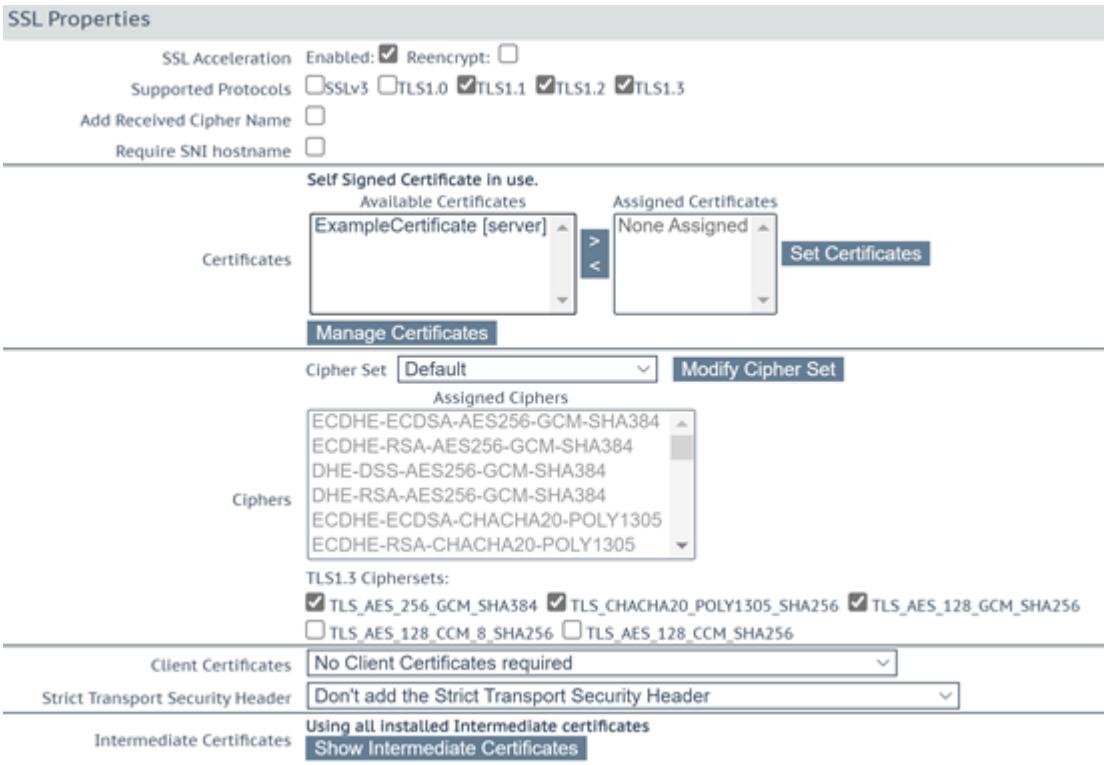
1. Click **Virtual Services**.
2. Click **Add New**.
3. Enter a **Virtual Address**.
4. Select the **Exchange 2013 POP** or the **Exchange 2013 POPS** template from the **Use Template** drop-down list depending on your preference.

5. Click **Add This Virtual Service**.
6. Expand the **Real Servers** section.
7. Click **Add New**.
8. For **Real Server Address**, enter the IP Address for one of the Exchange Servers.
9. Click **Add this Real Server**.
10. Add any additional Real Servers as required.

POPS Offloaded or POP with STARTTLS Virtual Service

The steps are the same when using Exchange IMAPS Offloaded and Exchange IMAP with STARTTLS application templates. To add the Virtual Services for Exchange IMAPS Offloaded and Exchange IMAP with STARTTLS using the template, follow the steps below:

1. Click **Virtual Services**.
2. Click **Add New**.
3. Enter a **Virtual Address**.
4. Select the **Exchange 2013 POPS Offloaded** or the **Exchange 2013 POP with StartTLS** template from the **Use Template** drop-down list depending on your preference.
5. Click **Add This Virtual Service**.
6. Expand **SSL Properties (Acceleration Enabled)**.



7. Select the certificate to use in the **Available Certificates** and click the “arrow” > to move it to **Assigned**

Certificates.

8. Click **Set Certificate**.
9. Expand the **Real Servers** section.
10. Click **Add New**.
11. For **Real Server Address**, enter the IP Address for one of the Exchange Servers.

    Note: Ensure port 110 is entered in the **Port** Field.

12. Click **Add this Real Server**.
13. Add any additional Real Servers as required.

SMTP or SMTPS Virtual Service

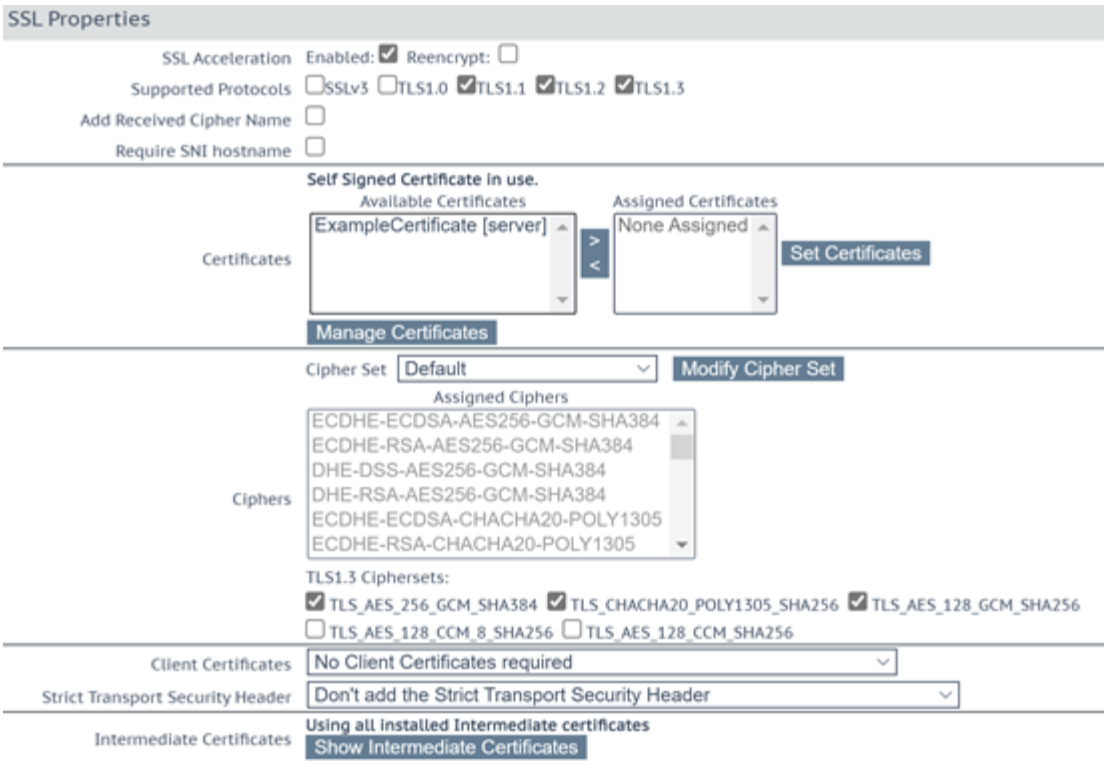
The steps are the same when using Exchange SMTP and Exchange SMTPS application templates. To add the Virtual Services for Exchange SMTP and Exchange SMTPS using the template, follow the steps below:

1. Click **Virtual Services**.
2. Click **Add New**.
3. Enter a **Virtual Address**.
4. Select the **Exchange 2013 SMTP** or the **Exchange 2013 SMTPS** template from the **Use Template** drop-down list depending on your preference.
5. Click **Add This Virtual Service**.
6. Expand the **Real Servers** section.
7. Click **Add New**.
8. For **Real Server Address**, enter the IP Address for one of the Exchange Servers.
9. Click **Add this Real Server**.
10. Add any additional Real Servers as required.

SMTPS Offloaded or SMTP with STARTTLS Virtual Service

The steps are the same when using Exchange SMTPS Offloaded and Exchange SMTP with STARTTLS application templates. To add the Virtual Services for Exchange SMTPS Offloaded and Exchange SMTP with STARTTLS using the template, follow the steps below:

1. Click the **Add New** button.
2. Enter a **Virtual Address**.
3. Select the **Exchange 2013 SMTP Offloaded** or the **Exchange 2013 SMTPwith STARTTLS** template from the **Use Template** drop-down list depending on your preference.
4. Click **Add This Virtual Service**.
5. Expand **SSL Properties (Acceleration Enabled)**.



6. Select the certificate to use in the **Available Certificates** and click the “arrow” > to move it to **Assigned Certificates**.
7. Click **Set Certificate**.
8. Expand the **Real Servers** section.
9. Click **Add New**.
10. For **Real Server Address**, enter the IP Address for one of the Exchange Servers.

Note: Ensure port 25 is entered in the **Port** Field.

11. Click **Add this Real Server**.
12. Add any additional Real Servers as required.

Note: SMTPS can be configured as offloaded as outlined above but cannot be set to Reencrypt.

SMTP with ESP Virtual Service

To add the Virtual Services for Exchange 2013 SMTP with ESP using the template, follow the steps below:

1. Click the **Add New** button.
2. Enter a **Virtual Address**.
3. Select the **Exchange 2013 SMTP with ESP** template from the **Use Template** drop-down list depending on your preference.
4. Click **Add This Virtual Service**.
5. Expand **ESP Options**.



6. Enter the Permitted SMTP Domain for the Organization and click **Set Permitted Domains**.
7. Expand the **Real Servers** section.
8. Click **Add New**.
9. For **Real Server Address**, enter the IP Address for one of the Office Online Servers.
10. Click **Add this Real Server**.
11. Add any additional Real Servers as necessary.

5

Exchange 2013 Virtual Service Recommended Settings (Optional)

These tables outline the recommended settings using the Progress Kemp application template. You can use these settings with scripts and automation tools.

Contents

- Exchange 2013 HTTP Virtual Service Recommended Settings (Optional)
- Exchange 2013 IMAP Virtual Service Recommended Settings (Optional)
- Exchange 2013 POP Virtual Service Recommended Settings (Optional)
- Exchange 2013 SMTP Virtual Service Recommended Settings (Optional)

Exchange 2013 HTTP Virtual Service Recommended Settings (Optional)

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
HTTP Redirect				
port	80	Port	80	All
prot	tcp	Protocol	tcp	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
nickname	Exchange%20Redirect	Service Name (Optional)	Exchange Redirect	All
ForceL7	1	Force L4	Disabled	All
Errorcode	302	Error Code	302 Found	All
ErrorUrl	https:%5C%2F%5C%2F%25h%25s	Redirection URL	https:\/\/%h%s	All
CheckType	none	Real Server Check Method	None	
Content Rules				
Authentication Proxy				
name	Authentication_Proxy	Rule Name	Authentication_Proxy	ESP Enabled
matchtype	Regex	Match Type	Regular Expression	ESP Enabled
pattern	%2F%5E%5C%2Flm_auth_proxy%2A%24%2F	Match String	/^\/lm_auth_proxy*$/	ESP Enabled
Nocase	1	Ignore Case	Enabled	ESP Enabled
ActiveSync				
Name	ActiveSync	Rule Name	ActiveSync	All
matchtype	Regex	Match Type	Regular Expression	All
pattern	%2F%5E%5C%2Fmicrosoft-server-activesync.%2A%2F	Match String	/^\/microsoft-server-activesync.*/	All
Nocase	1	Ignore Case	Enabled	All
Autodiscover				
name	Autodiscover	Rule Name	Autodiscover	All
matchtype	Regex	Match Type	Regular Expression	All
pattern	%2F%5E%5C%2Fautodiscover.%2A%2F	Match String	/^\/autodiscover.*/	All
Nocase	1	Ignore Case	Enabled	All
ECP				
name	ECP	Rule Name	ECP	All
matchtype	Regex	Match Type	Regular Expression	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Pattern	%2F%5E%5C%2Fecp.%2A%2F	Match String	/^\/ecp.*/	All
Nocase	1	Ignore Case	Enabled	All
EWS				
name	EWS	Rule Name	EWS	All
matchtype	Regex	Match Type	Regular Expression	All
Pattern	%2F%5E%5C%2Fews.%2A%2F	Match String	/^\/ews.*/	All
Nocase	1	Ignore Case	Enabled	All
MAPI				
name	MAPI	Rule Name	MAPI	All
matchtype	Regex	Match Type	Regular Expression	All
Pattern	%2F%5E%5C%2Fmapi.%2A%2F	Match String	/^\/mapi.*/	All
Nocase	1	Ignore Case	Enabled	All
OAB				
name	OAB	Rule Name	OAB	All
matchtype	Regex	Match Type	Regular Expression	All
Pattern	%2F%5E%5C%2Foab.%2A%2F	Match String	/^\/oab.*/	All
Nocase	1	Ignore Case	Enabled	All
OWA				
name	OWA	Rule Name	OWA	All
matchtype	Regex	Match Type	Regular Expression	All
Patterns	%2F%5E%5C%2Fowa.%2A%2F	Match String	/^\/owa.*/	All
Nocase	1	Ignore Case	Enabled	All
PowerShell				
name	powershell	Rule Name	powershell	All
matchtype	Regex	Match Type	Regular Expression	All
Pattern	%2F%5E%5C%2Fpo	Match String	/^\/powershell.*/	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
	wershell.%2A%2F			
Nocase	1	Ignore Case	Enabled	All
RPC				
name	RPC	Rule Name	RPC	All
matchtype	Regex	Match Type	Regular Expression	All
Pattern	%2F%5E%5C%2Frpc.%2A%2F	Match String	/^\/rpc.*/	All
Nocase	1	Ignore Case	Enabled	All
Main Virtual Service				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
VStype	http	Service Type	HTTP-HTTP/ 2-HTTPS	All
nickname	Exchange%20HTTPS%20 Offloaded	Service Name (Optional)	Exchange HTTPS Offloaded	Create Unique Name
ForceL7	1	Force L4	Disabled	All
Transparent	0	Transparency	Disabled	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
SSLAcceleration	1	SSL Acceleration	Enabled	All
SSLReencrypt	0 or 1	Reencrypt	Disabled or Enabled	0 for Offload 1 for Reencrypt
TLSType	1	Supported Protocols	TLS1.0, TLS1.1, TLS1.2, and TLS1.3 (Enabled)	All
CipherSet	BestPractices	Cipher Set	BestPractices	All
Tls13CipherSet	TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_128_GCM_SHA256, TLS_AES_128_CCM_8_SHA256, TLS_AES_128_CCM_SHA256	TLS1.3 Ciphersets	TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_128_GCM_SHA256, TLS_AES_128_CCM_8_SHA256, and TLS_AES_128_CCM_SHA256	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Persist	None	Persistence Options	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	1800	Idle Connection Timeout	1800	All
Sub Virtual Service				
Authentication Proxy				
port	443	Port	443	ESP Enabled
prot	tcp	Protocol	tcp	ESP Enabled
Nickname	Authentication%20Proxy	Service Name (Optional)	Authentication Proxy	ESP Enabled
Errorcode	503	Error Code	503 Service Unavailable	ESP Enabled
ErrorUrl	Endpoint%20not%20available	Redirection URL	Endpoint not available	ESP Enabled
CheckType	None	Real Server Check Method	None	ESP Enabled
EspEnabled	1	Enable ESP	Enabled	ESP Enabled
ESPLogs	7	ESP Logging	User Access, Security, and Connection (Enabled)	ESP Enabled
InputAuthMode	2	Client Authentication Mode	Form Based	ESP Enabled
OutputAuthMode	2	Server Authentication Mode	Form Based	ESP Enabled
AllowedHosts	Mail.example.com%20autodiscover.example.com	Allowed Virtual Hosts	Mail.example.com autodiscover.example.com	ESP Enabled
AllowedDirectories	%2F%2A	Allowed Virtual Directories	/*	ESP Enabled
SingleSignOnMessage	Please%20enter%20your%20Exchange%20credentials	SSO Greeting Message	Please enter your Exchange credentials	ESP Enabled
ActiveSync				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Nickname	ActiveSync	Service Name (Optional)	ActiveSync	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	None	Persistence Options	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	1800	Idle Connection Timeout	1800	All
CheckPort	443	Checked Port	443	All
CheckType	https	Real Server Check Method	HTTPS Protocol	All
CheckUrl	%2Fmicrosoft-server-activesync%2Fhealthcheck.htm	URL	/microsoft-server-activesync/healthcheck.htm	All
CheckUse1.1	0	Use HTTP/1.1	Disabled	All
CheckUseGet	1	HTTP Method	GET	All
EspEnabled	1	Enable ESP	Enabled	ESP Enabled
ESPLogs	7	ESP Logging	User Access, Security, and Connection (Enabled)	ESP Enabled
InputAuthMode	1	Client Authentication Mode	Basic Authentication	ESP Enabled
OutputAuthMode	1	Server Authentication Mode	Basic Authentication	ESP Enabled
AllowedHosts	Mail.example.com%20autodiscover.example.com	Allowed Virtual Hosts	Mail.example.com autodiscover.example.com	ESP Enabled
AllowedDirectories	%2Fmicrosoft-server-activesync%2A	Allowed Virtual Directories	/microsoft-server-activesync*	ESP Enabled
Autodiscover				
Port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	Autodiscover	Service Name (Optional)	Autodiscover	All
SubnetOriginating	1	Subnet Originating	Enabled	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
		Requests		
Persist	None	Persistence Options	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	1800	Idle Connection Timeout	1800	All
CheckPort	443	Checked Port	443	All
CheckType	https	Real Server Check Method	HTTPS Protocol	All
CheckUrl	%2Fautodiscover%2Fhealthcheck.htm	URL	/autodiscover/healthcheck.htm	All
CheckUse1.1	0	Use HTTP/1.1	Disabled	All
CheckUseGet	1	HTTP Method	GET	All
EspEnabled	1	Enable ESP	Enabled	ESP Enabled
ESPLogs	7	ESP Logging	User Access, Security, and Connection (Enabled)	ESP Enabled
InputAuthMode	0	Client Authentication Mode	Delegate to Server	ESP Enabled
OutputAuthMode	0	Server Authentication Mode	None	ESP Enabled
AllowedHosts	Mail.example.com%20autodiscover.example.com	Allowed Virtual Hosts	Mail.example.com autodiscover.example.com	ESP Enabled
AllowedDirectories	%2Fautodiscover%2A	Allowed Virtual Directories	/autodiscover*	ESP Enabled
ECP				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	ECP	Service Name (Optional)	ECP	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	None	Persistence Options	None	All
Schedule	lc	Scheduling Method	least connection	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Idletime	1800	Idle Connection Timeout	1800	All
CheckPort	443	Checked Port	443	All
CheckType	https	Real Server Check Method	HTTPS Protocol	All
CheckUrl	%2Fecp%2Fhealthcheck.htm	URL	/ecp/healthcheck.htm	All
CheckUse1.1	0	Use HTTP/1.1	Disabled	All
CheckUseGet	1	HTTP Method	GET	All
EspEnabled	1	Enable ESP	Enabled	ESP Enabled
ESPLogs	7	ESP Logging	User Access, Security, and Connection (Enabled)	ESP Enabled
InputAuthMode	2	Client Authentication Mode	Form Based	ESP Enabled
OutputAuthMode	2	Server Authentication Mode	Form Based	ESP Enabled
AllowedHosts	Mail.example.com%20autodiscover.example.com	Allowed Virtual Hosts	Mail.example.com autodiscover.example.com	ESP Enabled
AllowedDirectories	%2Fecp%2A	Allowed Virtual Directories	/ecp*	ESP Enabled
SingleSignOnMessage	Please%20enter%20your%20Exchange%20credentials	SSO Greeting Message	Please enter your Exchange credentials	ESP Enabled
EWS				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	EWS	Service Name (Optional)	EWS	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	None	Persistence Options	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	1800	Idle Connection	1800	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
		Timeout		
CheckPort	443	Checked Port	443	All
CheckType	https	Real Server Check Method	HTTPS Protocol	All
CheckUrl	%2Fews%2Fhealthcheck.htm	URL	/ews/healthcheck.htm	All
CheckUse1.1	0	Use HTTP/1.1	Disabled	All
CheckUseGet	1	HTTP Method	GET	All
EspEnabled	1	Enable ESP	Enabled	ESP Enabled
ESPLogs	7	ESP Logging	User Access, Security, and Connection (Enabled)	ESP Enabled
InputAuthMode	0	Client Authentication Mode	Delegate to Server	ESP Enabled
OutputAuthMode	0	Server Authentication Mode	None	ESP Enabled
AllowedHosts	Mail.example.com%20autodiscover.example.com	Allowed Virtual Hosts	Mail.example.com autodiscover.example.com	ESP Enabled
AllowedDirectories	%2Fews%2A	Allowed Virtual Directories	/ews*	ESP Enabled
MAPI				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	MAPI	Service Name (Optional)	MAPI	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	None	Persistence Options	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	1800	Idle Connection Timeout	1800	All
CheckPort	443	Checked Port	443	All
CheckType	https	Real Server Check	HTTPS Protocol	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
		Method		
CheckUrl	%2Fmapi%2Fhealthcheck.htm	URL	/mapi/healthcheck.htm	All
CheckUse1.1	0	Use HTTP/1.1	Disabled	All
CheckUseGet	1	HTTP Method	GET	All
EspEnabled	1	Enable ESP	Enabled	ESP Enabled
ESPLogs	7	ESP Logging	User Access, Security, and Connection (Enabled)	ESP Enabled
InputAuthMode	0	Client Authentication Mode	Delegate to Server	ESP Enabled
OutputAuthMode	0	Server Authentication Mode	None	ESP Enabled
AllowedHosts	Mail.example.com%20autodiscover.example.com	Allowed Virtual Hosts	Mail.example.com autodiscover.example.com	ESP Enabled
AllowedDirectories	%2Fmapi%2A	Allowed Virtual Directories	/mapi*	ESP Enabled
OAB				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	OAB	Service Name (Optional)	OAB	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	None	Persistence Options	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	1800	Idle Connection Timeout	1800	All
CheckPort	443	Checked Port	443	All
CheckType	https	Real Server Check Method	HTTPS Protocol	All
CheckUrl	%2Foab%2Fhealthcheck.htm	URL	/oab/healthcheck.htm	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
CheckUse1.1	0	Use HTTP/1.1	Disabled	All
CheckUseGet	1	HTTP Method	GET	All
EspEnabled	1	Enable ESP	Enabled	ESP Enabled
ESPLogs	7	ESP Logging	User Access, Security, and Connection (Enabled)	ESP Enabled
InputAuthMode	0	Client Authentication Mode	Delegate to Server	ESP Enabled
OutputAuthMode	0	Server Authentication Mode	None	ESP Enabled
AllowedHosts	Mail.example.com%20autodiscover.example.com	Allowed Virtual Hosts	Mail.example.com autodiscover.example.com	ESP Enabled
AllowedDirectories	%2Foab%2A	Allowed Virtual Directories	/oab*	ESP Enabled
OWA				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	OWA	Service Name (Optional)	OWA	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	None	Persistence Options	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	1800	Idle Connection Timeout	1800	All
CheckPort	443	Checked Port	443	All
CheckType	https	Real Server Check Method	HTTPS Protocol	All
CheckUrl	%2Fowa%2Fhealthcheck.htm	URL	/owa/healthcheck.htm	All
CheckUse1.1	0	Use HTTP/1.1	Disabled	All
CheckUseGet	1	HTTP Method	GET	All
EspEnabled	1	Enable ESP	Enabled	ESP Enabled

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
ESPLogs	7	ESP Logging	User Access, Security, and Connection (Enabled)	ESP Enabled
InputAuthMode	2	Client Authentication Mode	Form Based	ESP Enabled
OutputAuthMode	2	Server Authentication Mode	Form Based	ESP Enabled
AllowedHosts	Mail.example.com%20autodiscover.example.com	Allowed Virtual Hosts	Mail.example.com autodiscover.example.com	ESP Enabled
AllowedDirectories	%2Fowa%2A	Allowed Virtual Directories	/owa*	ESP Enabled
ExcludedDirectories	%2Fowa%2Fguid%40smtpdomain%2A	Pre-Authorization Excluded Directories	/owa/guid@smtpdomain*	ESP Enabled
SingleSignOnMessage	Please%20enter%20your%20Exchange%20credentials	SSO Greeting Message	Please enter your Exchange credentials	ESP Enabled
Logoff	%2Fowa%2Flogoff.owa		/owa/logoff.owa	ESP Enabled
PowerShell				
port	443	port	443	All
prot	tcp	Protocol	tcp	All
Nickname	PowerShell	Service Name (Optional)	PowerShell	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	None	Persistence Options	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	1800	Idle Connection Timeout	1800	All
CheckPort	443	Checked Port	443	All
CheckType	https	Real Server Check Method	HTTPS Protocol	All
CheckUrl	%2Fpowershell%2Fhealthcheck.htm	URL	/powershell/healthcheck.htm	All
CheckUse1.1	0	Use HTTP/1.1	Disabled	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
CheckUseGet	1	HTTP Method	GET	All
EspEnabled	1	Enable ESP	Enabled	ESP Enabled
ESPLogs	7	ESP Logging	User Access, Security, and Connection (Enabled)	ESP Enabled
InputAuthMode	0	Client Authentication Mode	Delegate to Server	ESP Enabled
OutputAuthMode	0	Server Authentication Mode	None	ESP Enabled
AllowedHosts	Mail.example.com%20autodiscover.example.com	Allowed Virtual Hosts	Mail.example.com autodiscover.example.com	ESP Enabled
AllowedDirectories	%2Fpowershell%2A	Allowed Virtual Directories	/powershell*	ESP Enabled
RPC				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	RPC	Service Name (Optional)	RPC	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	None	Persistence Options	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	1800	Idle Connection Timeout	1800	All
CheckPort	443	Checked Port	443	All
CheckType	https	Real Server Check Method	HTTPS Protocol	All
CheckUrl	%2Frpc%2Fhealthcheck.htm	URL	/rpc/healthcheck.htm	All
CheckUse1.1	0	Use HTTP/1.1	Disabled	All
CheckUseGet	1	HTTP Method	GET	All
EspEnabled	1	Enable ESP	Enabled	ESP Enabled
ESPLogs	7	ESP Logging	User Access,	ESP Enabled

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
			Security, and Connection (Enabled)	
InputAuthMode	0	Client Authentication Mode	Delegate to Server	ESP Enabled
OutputAuthMode	0	Server Authentication Mode	None	ESP Enabled
AllowedHosts	Mail.example.com%20autodiscover.example.com	Allowed Virtual Hosts	Mail.example.com autodiscover.example.com	ESP Enabled
AllowedDirectories	%2Frpc%2A	Allowed Virtual Directories	/rpc*	ESP Enabled

Exchange 2013 IMAP Virtual Service Recommended Settings (Optional)

API Parameter	API Value	WUI Field Name	WUI Field Value
IMAP			
port	143	Port	143
prot	tcp	Protocol	tcp
VStype	gen	Service Type	Generic
nickname	Exchange%20IMAP	Service Name (Optional)	Exchange IMAP
ForceL7	1	Force L4	Disabled
Transparent	0	Transparency	Disabled

API Parameter	API Value	WUI Field Name	WUI Field Value
ServerInit	Imap4	Server Initiating Protocols	IMAP4
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	None	Persistence Options	None
Schedule	rr	Scheduling Method	round robin
Idletime	3600	Idle Connection Timeout	3600
CheckType	Imap4	Real Server Check Method	Mailbox (IMAP) Protocol
CheckPort	110	Checked Port	110
IMAPS			
port	993	Port	993
prot	tcp	Protocol	tcp
VStype	gen	Service Type	Generic
nickname	Exchange%20IMAPS	Service Name (Optional)	Exchange IMAPS
forceL7	1	Force L4	Disabled
Transparent	0	Transparency	Disabled

API Parameter	API Value	WUI Field Name	WUI Field Value
ServerInit	Imap4	Server Initiating Protocols	IMAP4
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	None	Persistence Options	None
Schedule	rr	Scheduling Method	round robin
Idletime	3600	Idle Connection Timeout	3600
CheckType	tcp	Real Server Check Method	TCP Connection Only
CheckPort	993	Checked Port	993
IMAPS Offloaded			
port	993	Port	993
prot	tcp	Protocol	tcp
VStype	gen	Service Type	Generic
nickname	Exchange%20IMAPS%20Offload	Service Name (Optional)	Exchange IMAPS Offload
ForceL7	1	Force L4	Disabled

API Parameter	API Value	WUI Field Name	WUI Field Value
Transparent	0	Transparency	Disabled
ServerInit	Imap4	Server Initiating Protocols	IMAP4
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	None	Persistence Options	None
Schedule	rr	Scheduling Method	round robin
Idletime	3600	Idle Connection Timeout	3600
SSLAcceleration	1	SSL Acceleration	Enabled
SSLReencrypt	0	Reencrypt	Disabled
TLSType	1	Supported Protocols	TLS1.0, TLS1.1, TLS1.2, and TLS1.3 (Enabled)
CipherSet	BestPractices	CipherSet	BestPractices
CheckType	Imap4	Real Server Check Method	Mailbox (IMAP) Protocol
CheckPort	143	Checked Port	143
IMAP with STARTTLS			

API Parameter	API Value	WUI Field Name	WUI Field Value
port	143	Port	143
prot	tcp	Protocol	tcp
VStype	StartTLS	Service Type	STARTTLS protocols
nickname	Exchange%20IMAP%20STARTTLS	Service Name (Optional)	Exchange IMAP STARTTLS
ForceL7	1	Force L4	Disabled
Transparent	0	Transparency	Disabled
StartTLSMode	Imap	Server Initiating Protocols	IMAP4
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	None	Persistence Options	None
Schedule	rr	Scheduling Method	round robin
Idletime	3600	Idle Connection Timeout	3600
SSLAcceleration	1	SSL Acceleration	Enabled
TLSType	1	Supported Protocols	TLS1.0, TLS1.1, TLS1.2, and TLS1.3 (Enabled)

API Parameter	API Value	WUI Field Name	WUI Field Value
CipherSet	BestPractices	CipherSet	BestPractices
CheckType	Imap	Real Server Check Method	Mailbox (IMAP) Protocol
CheckPort	143	Checked Port	143

Exchange 2013 POP Virtual Service Recommended Settings (Optional)

API Parameter	API Value	WUI Field Name	WUI Field Value
POP			
port	110	Port	110
prot	tcp	Protocol	tcp
VStype	gen	Service Type	Generic
nickname	Exchange%20POP	Service Name (Optional)	Exchange POP
ForceL7	1	Force L4	Disabled
Transparent	0	Transparency	Disabled
ServerInit	Pop3	Server Initiating Protocols	POP3

API Parameter	API Value	WUI Field Name	WUI Field Value
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	None	Persistence Options	None
Schedule	rr	Scheduling Method	round robin
Idletime	3600	Idle Connection Timeout	3600
CheckType	Pop3	Real Server Check Method	Mailbox (POP3) Protocol
CheckPort	110	Checked Port	110
POPS			
port	995	Port	995
prot	tcp	Protocol	tcp
VStype	gen	Service Type	Generic
nickname	Exchange%20POPS	Service Name (Optional)	Exchange POPS
ForceL7	1	Force L4	Disabled
Transparent	0	Transparency	Disabled
ServerInit	Pop3	Server Initiating Protocols	POP3

API Parameter	API Value	WUI Field Name	WUI Field Value
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	None	Persistence Options	None
Schedule	rr	Scheduling Method	round robin
Idletime	3600	Idle Connection Timeout	3600
CheckType	tcp	Real Server Check Method	TCP Connection Only
CheckPort	993	Checked Port	993
POPS Offloaded			
port	995	Port	995
prot	tcp	Protocol	tcp
VStype	gen	Service Type	Generic
nickname	Exchange%20POPS%20Offload	Service Name (Optional)	Exchange POPS Offload
ForceL7	1	Force L4	Disabled
Transparent	0	Transparency	Disabled

API Parameter	API Value	WUI Field Name	WUI Field Value
ServerInit	Pop3	Server Initiating Protocols	POP3
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	None	Persistence Options	None
Schedule	rr	Scheduling Method	round robin
Idletime	3600	Idle Connection Timeout	3600
SSLAcceleration	1	SSL Acceleration	Enabled
SSLReencrypt	0	Reencrypt	Disabled
TLSType	1	Supported Protocols	TLS1.0, TLS1.1, TLS1.2, and TLS1.3 (Enabled)
CipherSet	BestPractices	CipherSet	BestPractices
CheckType	Pop3	Real Server Check Method	Mailbox (POP3) Protocol
CheckPort	110	Checked Port	110
POP with STARTTLS			
port	110	Port	110

API Parameter	API Value	WUI Field Name	WUI Field Value
prot	tcp	Protocol	tcp
VStype	StartTLS	Service Type	STARTTLS protocols
nickname	Exchange%20IMAP%20STARTTLS	Service Name (Optional)	Exchange IMAP STARTTLS
ForceL7	1	Force L4	Disabled
Transparent	0	Transparency	Disabled
StartTLSMode	Pop3	Server Initiating Protocols	POP3
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	None	Persistence Options	None
Schedule	rr	Scheduling Method	round robin
Idletime	3600	Idle Connection Timeout	3600
SSLAcceleration	1	SSL Acceleration	Enabled
TLSType	1	Supported Protocols	TLS1.0, TLS1.1, TLS1.2, and TLS1.3 (Enabled)
CipherSet	BestPractices	CipherSet	BestPractices

API Parameter	API Value	WUI Field Name	WUI Field Value
CheckType	pop	Real Server Check Method	Mailbox (POP3) Protocol
CheckPort	110	Checked Port	110

Exchange 2013 SMTP Virtual Service Recommended Settings (Optional)

API Parameter	API Value	WUI Field Name	WUI Field Value
SMTP			
port	25	Port	25
prot	tcp	Protocol	tcp
VStype	gen	Service Type	Generic
nickname	Exchange%20STMP	Service Name (Optional)	Exchange STMP
ForceL7	1	Force L4	Disabled
Transparent	0	Transparency	Disabled
ServerInit	smtp	Server Initiating Protocols	SMTP
SubnetOriginating	1	Subnet Originating Requests	Enabled

API Parameter	API Value	WUI Field Name	WUI Field Value
Persist	src	Persistence Options	Source IP Address
PersistTimeout	3600	Timeout	3600
Schedule	rr	Scheduling Method	round robin
Idletime	120	Idle Connection Timeout	120
CheckType	smtp	Real Server Check Method	Mailbox (SMTP) Protocol
CheckPort	25	Checked Port	25
SMTPS			
port	587	Port	587
prot	tcp	Protocol	tcp
VStype	gen	Service Type	Generic
nickname	Exchange%20SMTPS	Service Name (Optional)	Exchange STMPS
ForceL7	1	Force L4	Disabled
Transparent	0	Transparency	Disabled
ServerInit	smtp	Server Initiating Protocols	SMTP

API Parameter	API Value	WUI Field Name	WUI Field Value
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	src	Persistence Options	Source IP Address
PersistTimeout	3600	Timeout	3600
Schedule	rr	Scheduling Method	round robin
Idletime	120	Idle Connection Timeout	120
CheckType	tcp	Real Server Check Method	tcp
CheckPort	587	Checked Port	587
SMTPS Offloaded			
port	587	Port	587
prot	tcp	Protocol	tcp
VStype	gen	Service Type	Generic
nickname	Exchange%20SMTPS%20Offload	Service Name (Optional)	Exchange STMPS Offload
ForceL7	1	Force L4	Disabled

API Parameter	API Value	WUI Field Name	WUI Field Value
Transparent	0	Transparency	Disabled
ServerInit	smtp	Server Initiating Protocols	SMTP
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	src	Persistence Options	Source IP Address
PersistTimeout	3600	Timeout	3600
Schedule	rr	Scheduling Method	round robin
Idletime	120	Idle Connection Timeout	120
SSLAcceleration	1	SSL Acceleration	Enabled
SSLReencrypt	0	Reencrypt	Disabled
TLSType	1	Supported Protocols	TLS1.0, TLS1.1, TLS1.2, and TLS1.3 (Enabled)
CipherSet	BestPractices	CipherSet	BestPractices
CheckType	smtp	Real Server Check Method	Mail (SMTP) Protocol
CheckPort	25	Checked Port	25

API Parameter	API Value	WUI Field Name	WUI Field Value
SMTP with STARTTLS			
port	25	Port	25
prot	tcp	Protocol	tcp
VStype	StartTLS	Service Type	STARTTLS protocols
nickname	Exchange%20SMTP%20STARTTLS	Service Name (Optional)	Exchange STMP STARTTLS
ForceL7	1	Force L4	Disabled
Transparent	0	Transparency	Disabled
StartTLSMode	smtp	Server Initiating Protocols	SMTP
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	src	Persistence Options	Source IP Address
PersistTimeout	3600	Timeout	3600
Schedule	rr	Scheduling Method	round robin
Idletime	120	Idle Connection Timeout	120

API Parameter	API Value	WUI Field Name	WUI Field Value
SSLAcceleration	1	SSL Acceleration	Enabled
TLSType	1	Supported Protocols	TLS1.0, TLS1.1, TLS1.2, and TLS1.3 (Enabled)
CipherSet	BestPractices	CipherSet	BestPractices
CheckType	smtp	Real Server Check Method	Mail (SMTP) Protocol
CheckPort	25	Checked Port	25
SMTP with ESP			
port	25	Port	25
prot	tcp	Protocol	tcp
VStype	gen	Service Type	Generic
nickname	Exchange%20STMP%20ESP	Service Name (Optional)	Exchange STMP ESP
ForceL7	1	Force L4	Disabled
Transparent	0	Transparency	Disabled
ServerInit	smtp	Server Initiating Protocols	SMTP

API Parameter	API Value	WUI Field Name	WUI Field Value
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	src	Persistence Options	Source IP Address
PersistTimeout	3600	Timeout	3600
Schedule	rr	Scheduling Method	round robin
IdleTime	120	Idle Connection Timeout	120
EnableESP	1	ESP Enable	Enabled
ESPLog	4	ESP Logging	Connection (Enabled)
Smtpallow	“Example.com”	SMTP Allowed Domains	Example.com
CheckType	smtp	Real Server Check Method	Mail (SMTP) Protocol
CheckPort	25	Checked Port	25

6

References

Other useful documents are as follows:

Web User Interface (WUI) Configuration Guide

Virtual Services and Templates Feature Description

Edge Security Pack (ESP) Feature Description

Microsoft Exchange 2010 Deployment Guide

Microsoft Exchange 2016 Deployment Guide

Exchange Team Blog post on Load Balancing in Exchange 2013

KCD Feature Description

View or configure Outlook Web App virtual directories