Progress®
Kemp® LoadMaster®

Deployment Guide MS Exchange 2019

Generated on: 21 April 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

About This Manual 5

Prerequisites 6

Chapter 2: Exchange 2019 Overview 7

Understanding Server Load Balancing 8

Enable Subnet Originating Requests Globally 8

100-Continue Handling 9

Additional L7 Header 10

Chapter 3: Virtual Service Templates 11

Chapter 4: Configuring Virtual Services for Exchange 2019 13

HTTPS Offloaded Virtual Service or Reencrypted without ESP Virtual Service 14

Add SSL/TLS Certificate 14

HTTPS Offloaded and Reencrypted with ESP 16

Add SSL/TLS Certificate 17

Configure ESP 19

HTTPS Pass-through Virtual Service 20

IMAP and IMAPS Virtual Service 20

IMAPS Offloaded and IMAP with STARTTLS Virtual Service 21

POP and POPS Virtual Service 22

POPS Offloaded and POP with STARTTLS Virtual Service 22

SMTP and SMTPS Virtual Service 23

SMTPS Offloaded and SMTP with STARTTLS Virtual Service 24

SMTP with ESP Virtual Service 25
Office Online Server Virtual Service 26
WAF Virtual Services 27
Exchange 2019 HTTPS Offload with WAF 28
Exchange 2019 HTTPS Offload with ESP and WAF 30
Exchange 2019 HTTPS re-encrypted with WAF 33
Exchange 2019 HTTPS re-encrypted with ESP and WAF 35

Chapter 5: Exchange 2019 Virtual Service Recommended Settings (Optional) 39
Exchange 2019 HTTP Virtual Service Recommended Settings (Optional) 40
Exchange 2019 HTTPS Pass-through Virtual Service Recommended Settings (Optional) 64
Exchange 2019 IMAP Virtual Service Recommended Settings (Optional) 66
Exchange 2019 POP Virtual Service Recommended Settings (Optional) 71
Exchange 2019 SMTP Virtual Service Recommended Settings (Optional) 76
Exchange 2019 Office Online Server Virtual Service Recommended Settings (Optional) 82
Exchange 2019 WAF Recommended Settings (Optional) 84
Exchange 2019 HTTPS Offload with WAF Recommended Settings (Optional) 84
Exchange 2019 HTTPS Offload with ESP and WAF Recommended Settings (Optional) . . . 97
Exchange 2019 HTTPS re-encrypted with WAF Recommended Settings (Optional) 115
Exchange 2019 HTTPS re-encrypted with ESP and WAF Recommended Settings (Optional) 128
Content Rules 145

Chapter 6: References 151

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 2019 (Exchange 2019), 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 2019 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 2019, and includes a comprehensive first year warranty and technical support agreement.

Contents

- About This Manual
- Prerequisites

About This Manual

This manual addresses how to deploy and configure a LoadMaster appliance with Exchange 2019 using Progress Kemp application templates.

Progress 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.

Prerequisites

This guide assumes the reader is a network administrator or familiar with networking and general computer terminology. It is further assumed that the Exchange 2019 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 2019 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 2019 have made it easier to load balance Exchange-related traffic.

Exchange 2019 includes the following solutions for switchover and failover redundancy:

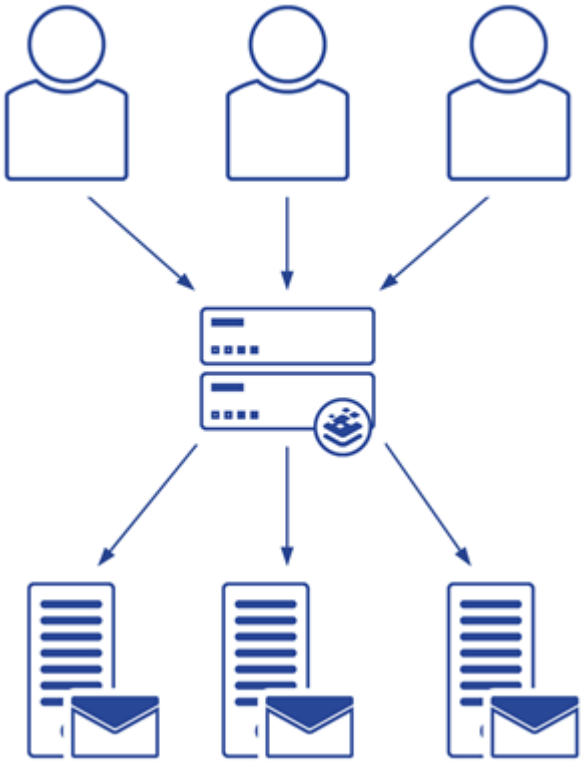
- **High availability:** Exchange 2019 uses Database Availability Groups (DAGs) to keep multiple copies of your mailboxes on different servers synchronized. That way, if a mailbox database fails on one server, users can connect to a synchronized copy of the database on another server.
- **Site resilience:** 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 of time 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
- 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).

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

1. 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 the Mail client on Mac handles Persistent-Auth headers from the 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 2019. 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 steps for setting up Virtual Services using Progress Kemp Application Templates. The Exchange 2019 templates currently available are grouped in three downloadable files as follows:

- **Exchange2019Core**
  - 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 2019.
- **Exchange2019ESP**
  - 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.
- **Exchange2019Additional**
  - This set contains templates for IMAP, POP, and SMTP services, including variants for STARTTLS and SSL secured services.
- **Exchange2019WAF**

- This set contains templates for SSL offloaded HTTPS, SSL offloaded HTTPS with ESP enabled, and HTTPS re-encryption (both with and without ESP enabled) - all with WAF enabled.
- These services are only required if you want to use WAF functionality.

Note: The maximum number of WAF-enabled Virtual Services (or SubVSs) is the total (unused or available) RAM (in MB)/512 MB. For example: 8 GB/512 MB = 16 WAF-enabled Virtual Services. When the maximum is reached, no additional Virtual Services can be enabled with WAF.

Note: For further details on WAF, refer to the WAF Feature Description.

- WAF is only available with Enterprise Plus subscriptions.

4

Configuring Virtual Services for Exchange 2019

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 2019 Virtual Service Recommended API Settings (Optional) section 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 Virtual Service or Reencrypted without ESP Virtual Service
- HTTPS Offloaded and Reencrypted with ESP
- HTTPS Pass-through Virtual Service
- IMAP and IMAPS Virtual Service
- IMAPS Offloaded and IMAP with STARTTLS Virtual Service
- POP and POPS Virtual Service
- POPS Offloaded and POP with STARTTLS Virtual Service
- SMTP and SMTPS Virtual Service

- SMTPS Offloaded and SMTP with STARTTLS Virtual Service
- SMTP with ESP Virtual Service
- Office Online Server Virtual Service
- WAF Virtual Services

HTTPS Offloaded Virtual Service or Reencrypted without ESP Virtual Service

The steps are the same when using Exchange HTTPS Offload and Exchange HTTPS Reencrypted with ESP application templates. To add the Virtual Services for Exchange HTTPS Offload 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 2019 HTTPS Offloaded** or the **Exchange 2019 HTTPS ReEncrypted** template from the **Use Template** drop-down list depending on your preference.

5. Click **Add This Virtual Service**.

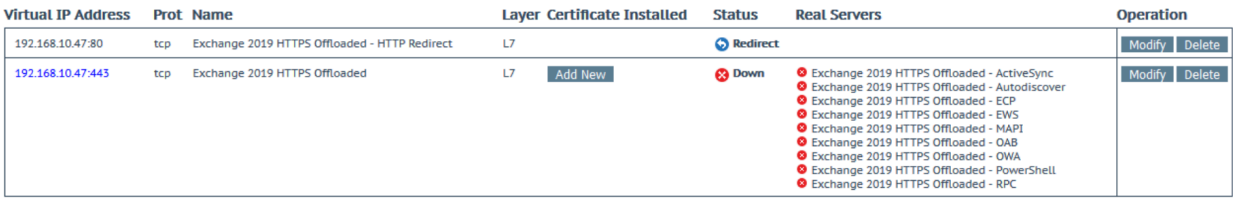
Contents

- Add SSL/TLS Certificate

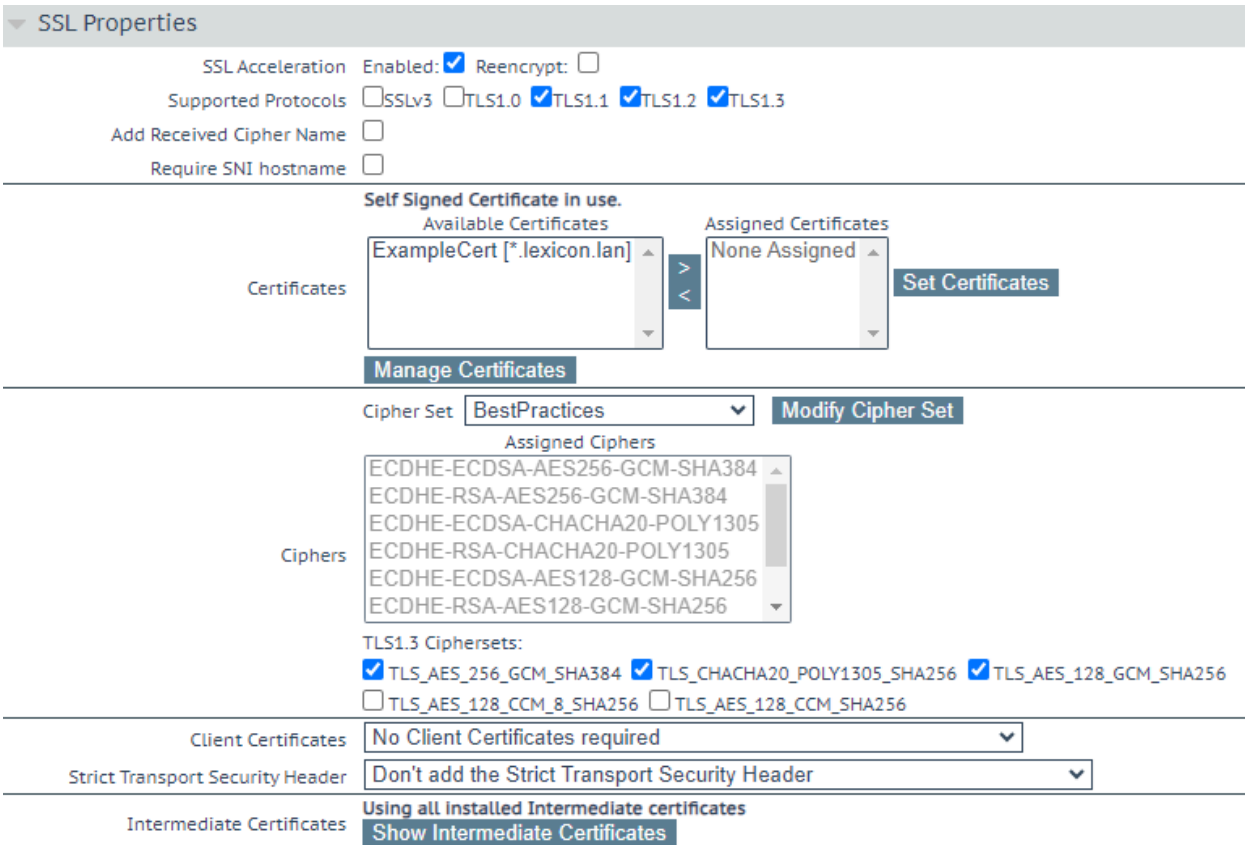
Add SSL/TLS Certificate

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 2019 HTTPS Offloaded** Virtual Service on port 443 (or **Exchange 2019 HTTPS Reencrypted** if that was selected during the creation)
3. Expand **SSL Properties (Acceleration Enabled)**.

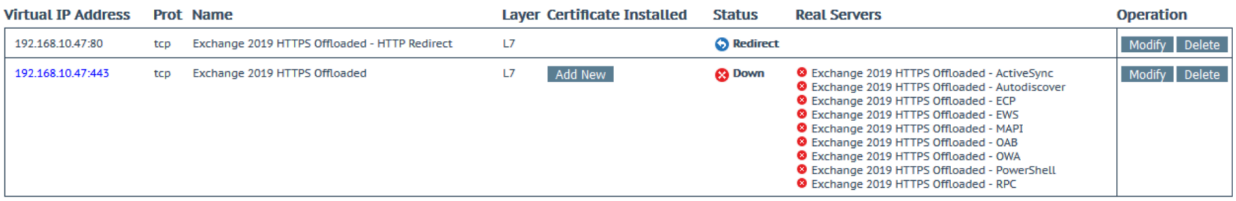


4. Select the certificate to use in the **Available Certificates** and click the “arrow” > to move it to **Assigned Certificates**.
5. Click **Set Certificate**.

Note: The **Reencrypt** check box is selected when using the **Exchange 2019 HTTPS Reencrypted with ESP** template.

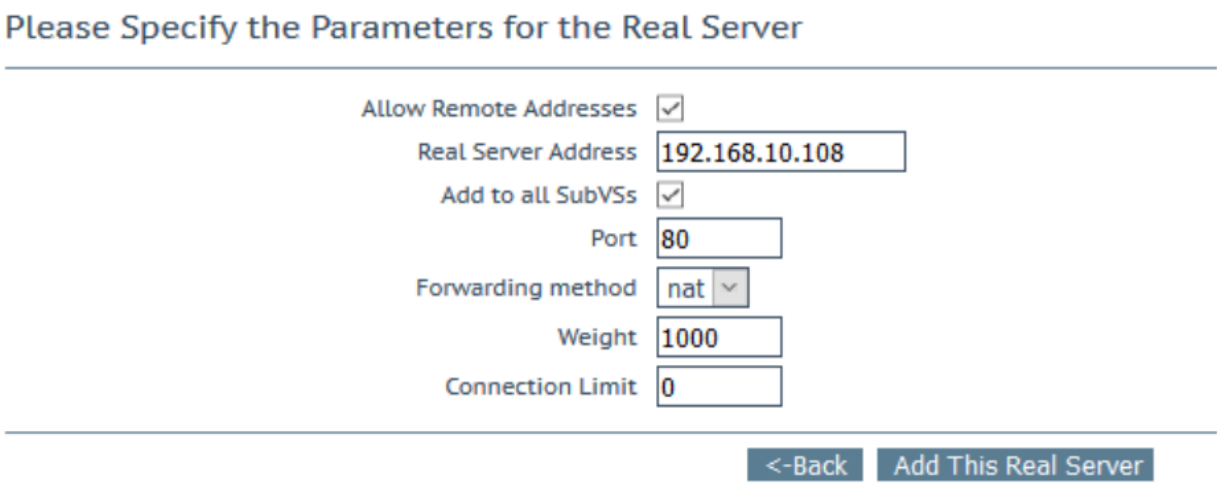
Add the Real Servers

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



2. Click **Modify** for the **Exchange 2019 HTTPS Offloaded** Virtual Service on port 443 (or the **Exchange 2019 HTTPS Reencrypted** if that was selected during the creation).
3. Expand the **SubVSs** section.
4. Click **Modify** for **Exchange 2019 HTTPS Offloaded - ActiveSync** (or the **Exchange 2019 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 and Reencrypted with ESP

The steps are the same when using Exchange HTTPS Offload and Exchange HTTPS Reencrypted with ESP application template. To add the Virtual Services for Exchange HTTPS Offload 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 2019 HTTPS Offloaded with ESP** or the **Exchange 2019 HTTPS ReEncrypted with ESP** template from the **Use Template** drop-down list depending on your preference.
5. Click **Add This Virtual Service**.

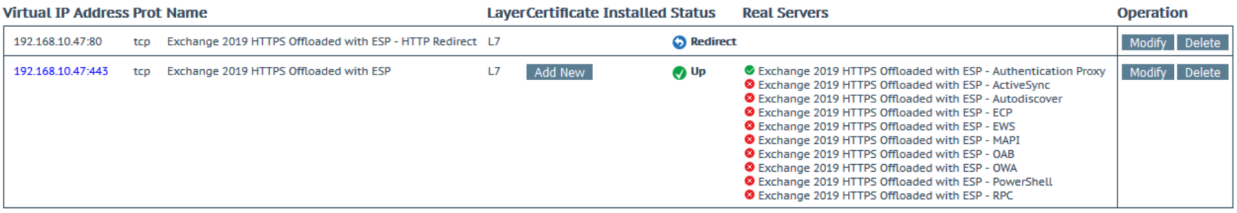
Contents

- Add SSL/TLS Certificate
- Configure ESP

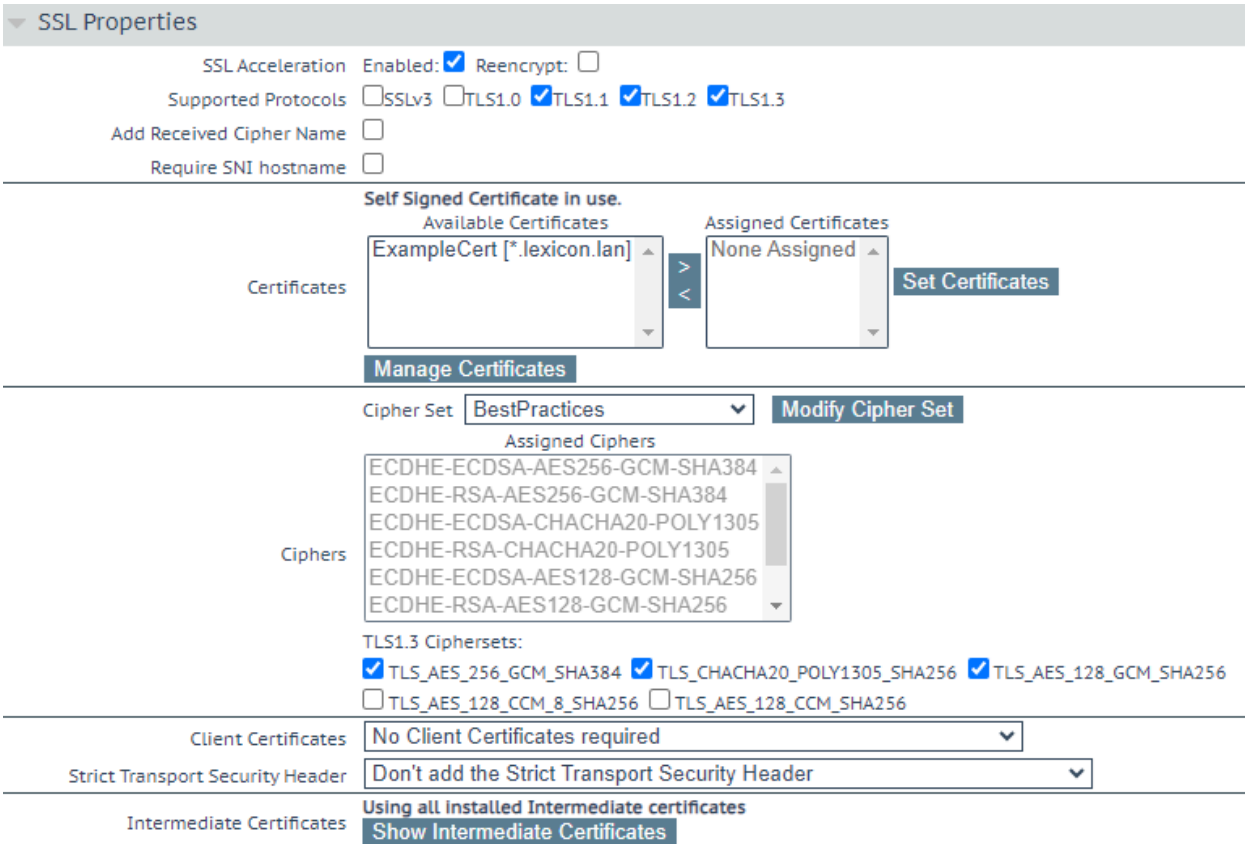
Add SSL/TLS Certificate

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



2. Click **Modify** for the **Exchange 2019 HTTPS Offloaded with ESP** Virtual Service on port 443 (or **Exchange 2019 HTTPS Reencrypted with ESP** if that was selected during the creation)
3. Expand **SSL Properties (Acceleration Enabled)**.

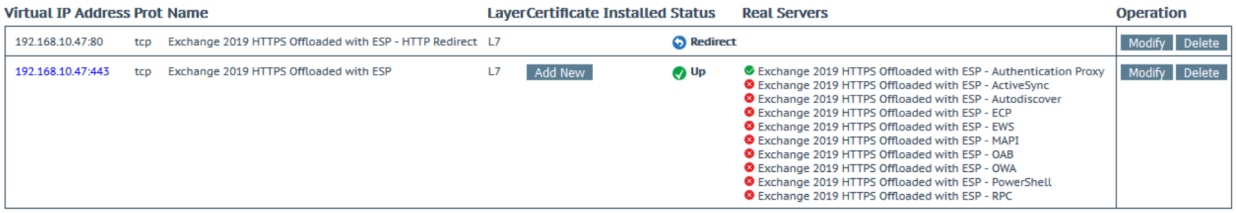


4. Select the certificate to use in the **Available Certificates** and click the “arrow” > to move it to **Assigned Certificates**.
5. Click **Set Certificate**.

Note: The **Reencrypt** check box is selected when using the **Exchange 2019 HTTPS Reencrypted with ESP** template.

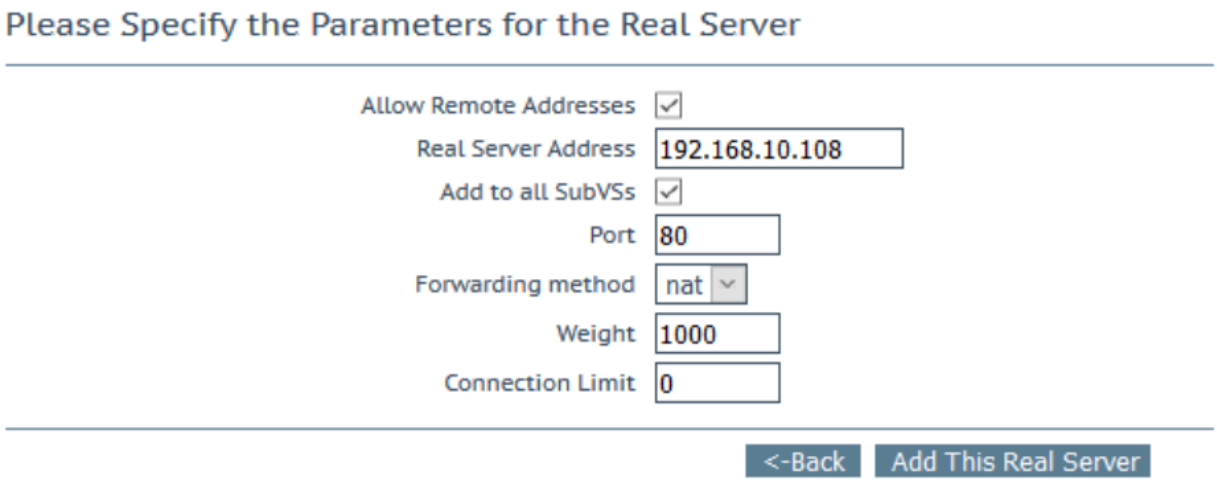
Add the Real Servers

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



2. Click **Modify** for the **Exchange 2019 HTTPS Offloaded with ESP** Virtual Service on port 443 (or the **Exchange 2019 HTTPS Reencrypted with ESP** if that was selected during the creation).
3. Expand the **SubVSs** section.
4. Click **Modify** for **Exchange 2019 HTTPS Offloaded with ESP - Authentication Proxy** (or the **Exchange 2019 HTTPS Reencrypted with ESP - Authentication Proxy** if that was selected during the creation).
5. Expand the **Real Servers** section.
6. Click **Add New**.

Note: In the ESP-enabled Virtual Services, there should be no Real Servers in the Authentication Proxy SubVS, unless you are using Kerberos server-side authentication. For further details on Kerberos Constrained Delegation (KCD), refer to the Kerberos Constrained Delegation Feature Description.



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.

Note: Ensure to delete the Real Server from the Authentication Proxy SubVS if you are not using Kerberos server-side authentication.

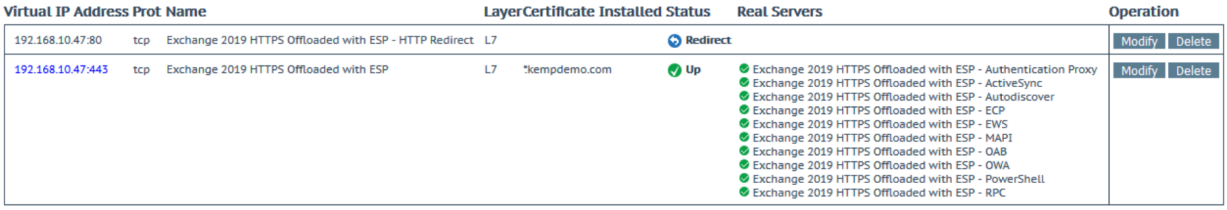
---

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 2019 HTTPS Offloaded with ESP** Virtual Service on port 443 (or the **Exchange 2019 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
API	n/a	n/a	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**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.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**.

HTTPS Pass-through Virtual Service

To add the Virtual Services for Exchange HTTPS Pass-through using the template, follow the steps below:

1. Click **Virtual Services**.
2. Click **Add New**.
3. Enter a **Virtual Address**.
4. Select the **Exchange 2019 HTTPS pass-through** 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 the **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.

IMAP and IMAPS Virtual Service

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

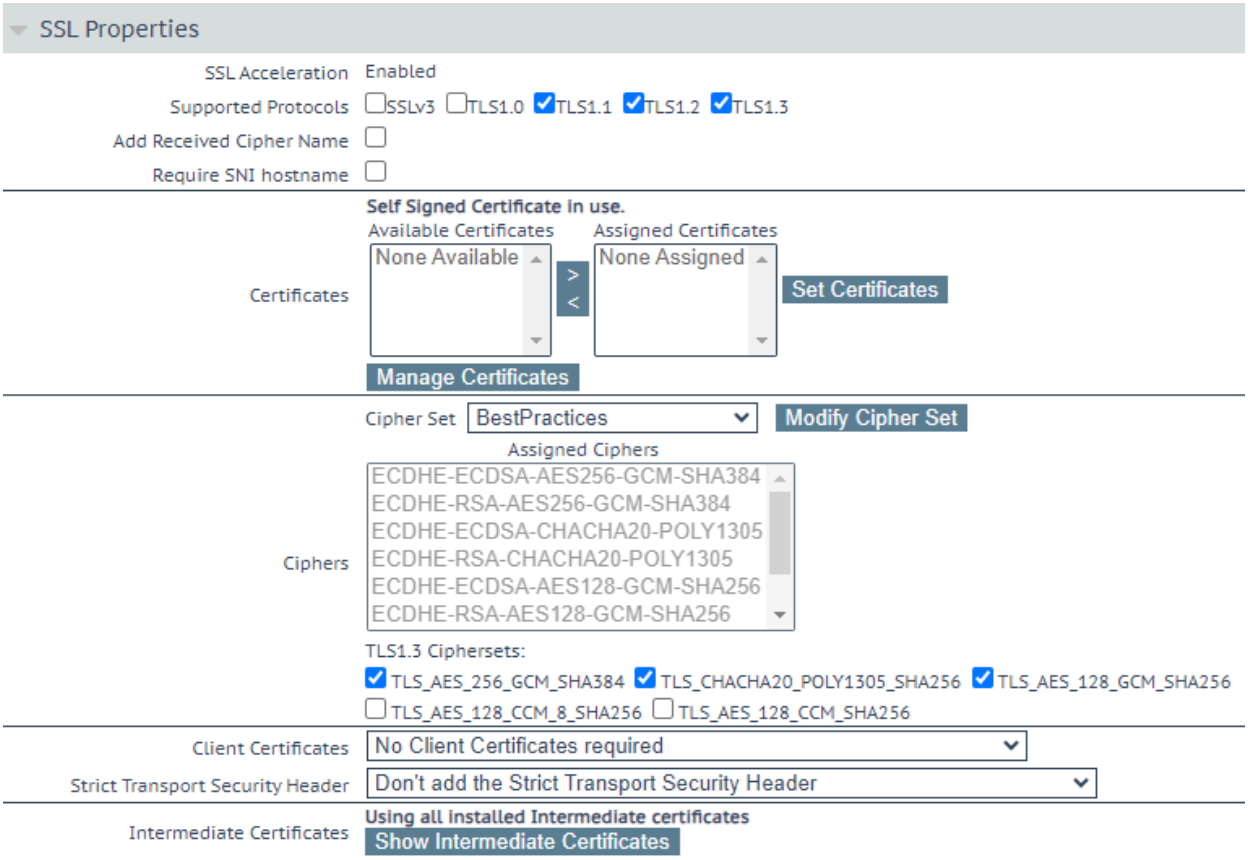
1. Click **Virtual Services**.
2. Click **Add New**.
3. Enter a **Virtual Address**.
4. Select the **Exchange 2019 IMAP** or the **Exchange 2019 IMAPS** template from the **Use Template** drop-down list depending on your preference.
5. Click **Add This Virtual Service**.
6. Expand the **Real Servers** 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 and 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 2019 IMAP** or the **Exchange 2019 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)**.

Note: SSL acceleration only does offloading (and not re-encrypting) for this Virtual Service.



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 and 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:

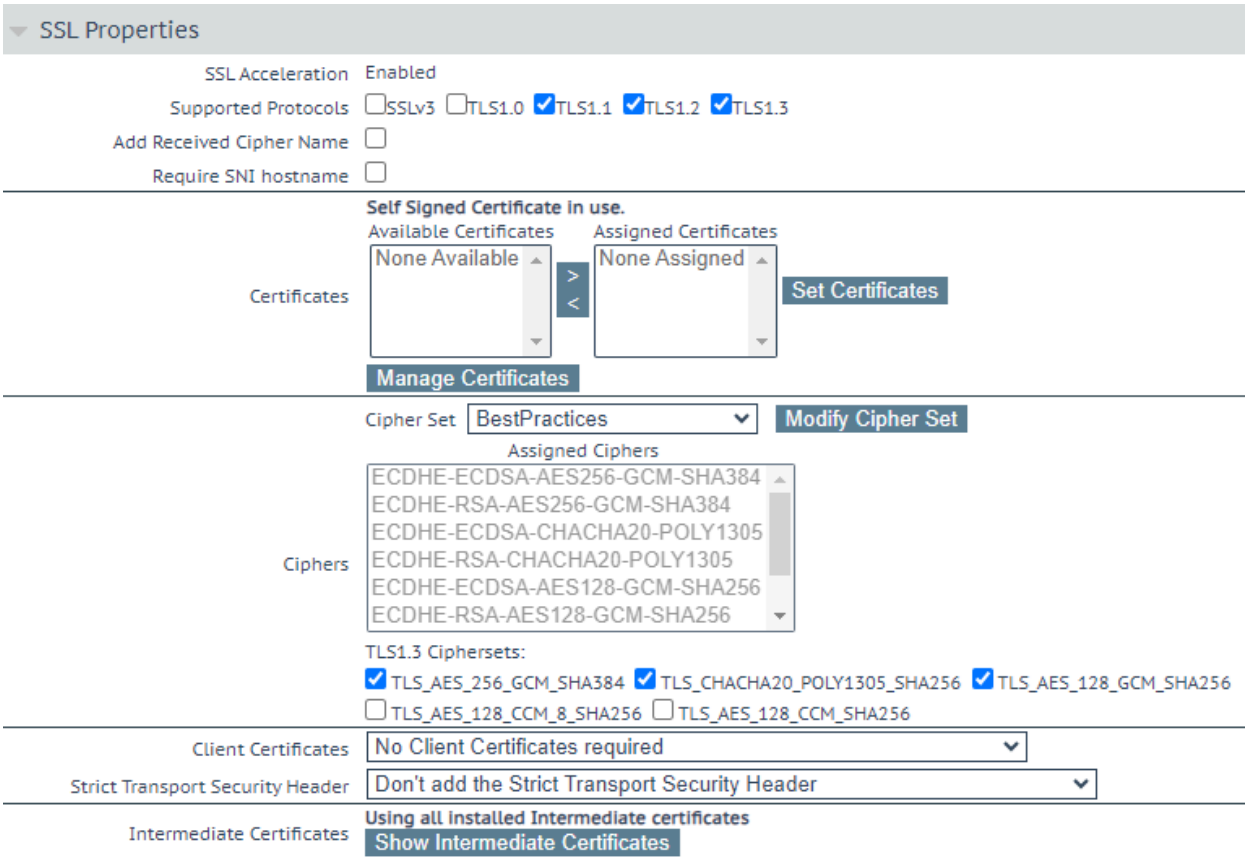
1. Click **Virtual Services**.
2. Click **Add New**.
3. Enter a **Virtual Address**.
4. Select the **Exchange 2019 POP** or the **Exchange 2019 POPS** template from the **Use Template** drop-down list depending on your preference.
5. Click **Add This Virtual Service**.
6. Expand the **Real Servers** section.
7. Click **Add New**.
8. For the **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 and 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 2019 IMAP** or the **Exchange 2019 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)**.

    Note: SSL acceleration only does offloading (and not re-encrypting) for this Virtual Service.



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 the **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 and 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 2019 SMTP** or the **Exchange 2019 SMTPS** template from the **Use Template** drop-down list depending on your preference.

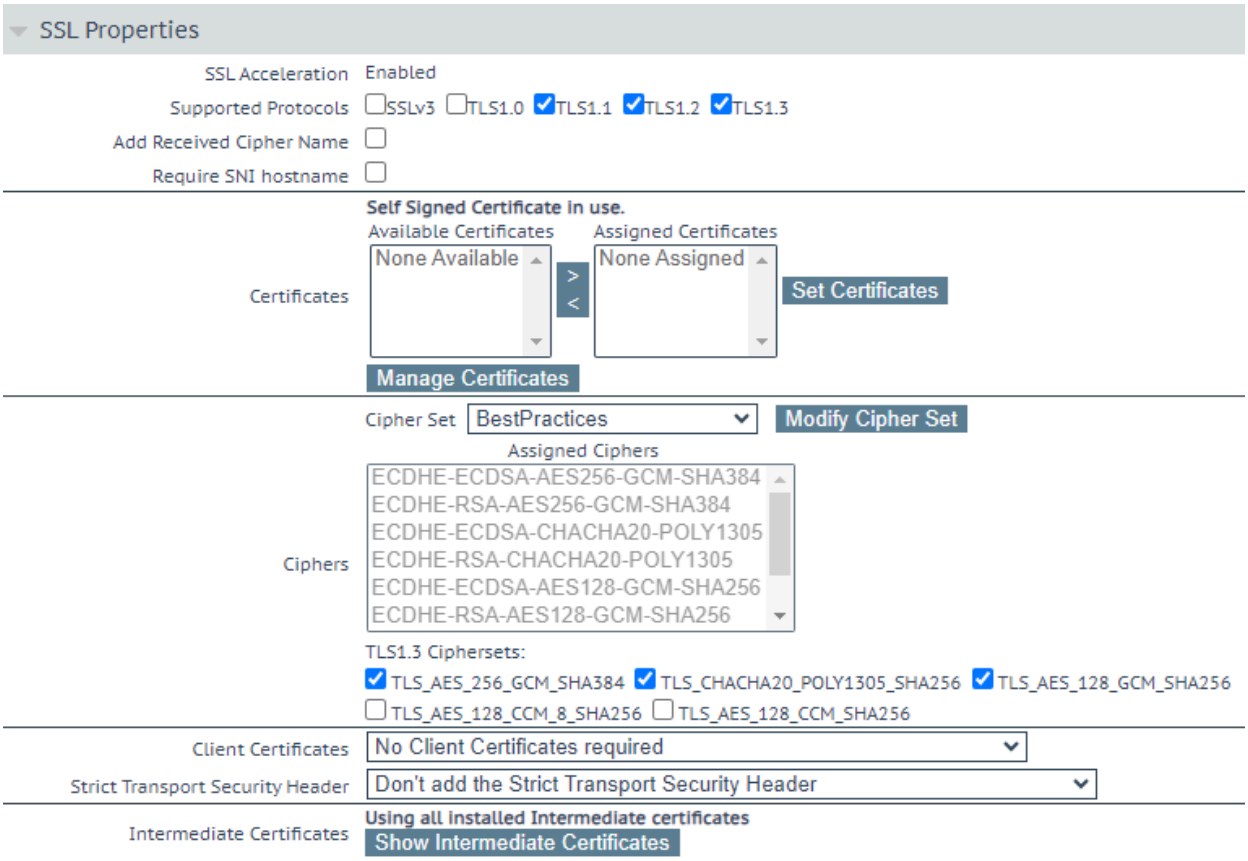
5. Click **Add This Virtual Service**.
6. Expand the **Real Servers** section.
7. Click **Add New**.
8. For the **Real Server Address**, enter the IP Address for one of the Exchange Servers.
9. Click **Add this Real Server**.
10. Add any additional Real Servers as required.

SMTPS Offloaded and 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 2019 SMTP** or the **Exchange 2019 SMTPS** template from the **Use Template** drop-down list depending on your preference.
4. Click **Add This Virtual Service**.
5. Expand **SSL Properties (Acceleration Enabled)**.

Note: SSL acceleration only does offloading (and not re-encrypting) for this Virtual Service.



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 the **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 2019 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 2019 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**.

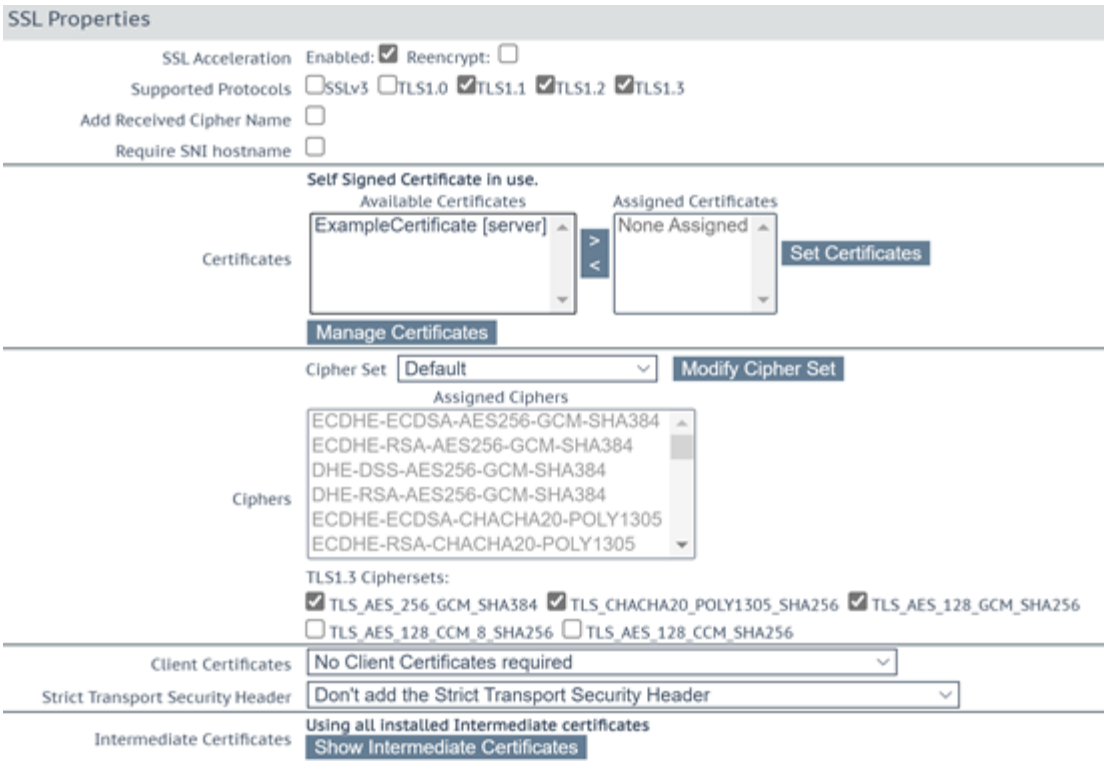
Note: If this text box is empty, no domains are allowed and all mail is stopped.

7. Expand the **Real Servers** section.
8. Click **Add New**.
9. For the 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.

Office Online Server Virtual Service

To add the Virtual Services for Office Online Server using the template, follow the steps below:

1. Click the **Add New** button.
2. Enter a **Virtual Address**.
3. Select the **Exchange 2019 Office Online Server** template from the **Use Template** drop-down list depending on your preference.
4. Click **Add This Virtual Servic**e.
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 the **Real Server Address**, enter the IP Address for one of the Office Online Servers.
11. Click **Add this Real Server**.
12. Add any additional Real Servers as required.

WAF Virtual Services

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

To fully configure WAF (including false positive tuning), we recommend engaging with our Professional Services team. For further details, refer to the following links:

- WAF False Positive Analysis (FPA) Service
- WAF Rule Writing Service

For further information on WAF in general, refer to the WAF Feature Description.

Contents

- Exchange 2019 HTTPS Offload with WAF

- Exchange 2019 HTTPS Offload with ESP and WAF
- Exchange 2019 HTTPS re-encrypted with WAF
- Exchange 2019 HTTPS re-encrypted with ESP and WAF

Exchange 2019 HTTPS Offload with WAF

Follow the instructions below to set up the parent **Exchange 2019 HTTPS Offload with WAF** Virtual Service:

1. Click **Virtual Services**.
2. Click **Add New**.
3. Enter a **Virtual Address**.
4. Select the **Exchange 2019 HTTPS Offload with WAF** template from the **Use Template** drop-down list.
5. Click **Add this Virtual Service**.

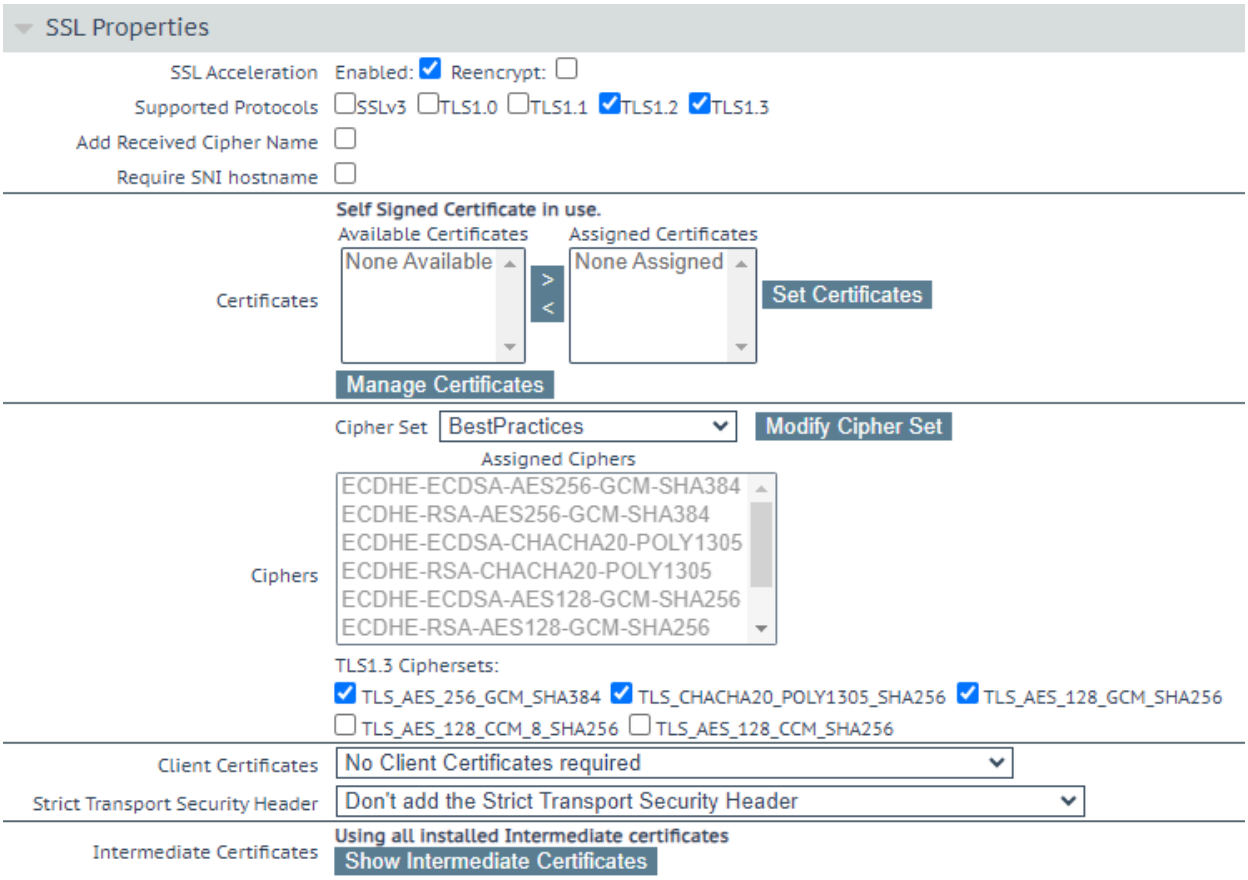
Contents

- Add SSL/TLS Certificate

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** (under **Virtual Services**) in the left-hand navigation.
2. Click **Modify** for the **Exchange 2019 HTTPS Offload with WAF** Virtual Service on port 443 (or **Exchange 2019 HTTPS Reencrypted with WAF** if that was selected during creation).
3. Expand **SSL Properties (Acceleration Enabled)**.

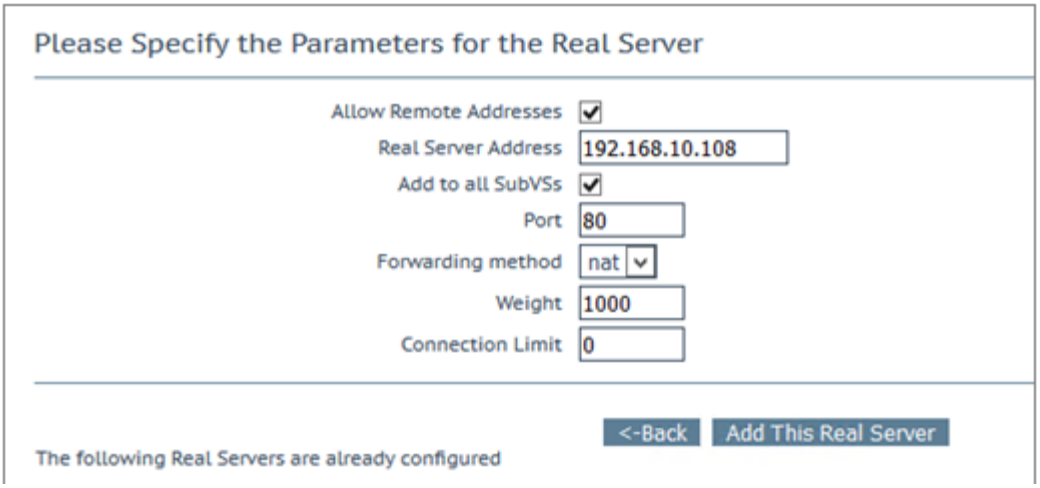


4. Select the certificate to use in the **Available Certificates** and click the “arrow” (>) to move it to **Assigned Certificates**.
5. Click **Set Certificates**.

Note: The **Reencrypt** check box is selected when using the **Exchange 2019 HTTPS Reencrypted with WAF** template.

Add the Real Servers

1. Click **View/Modify Services** in the left-hand navigation.
2. Click **Modify** for the **Exchange 2019 HTTPS Offload with WAF** Virtual Service on port 443 (or the **Exchange 2019 HTTPS Reencrypted with WAF** if that was selected during the creation).
3. Expand the **SubVSs** section.
4. Click **Modify** for **Exchange 2019 HTTPS Offload with ESP - ActiveSync** (or **Exchange 2019 HTTPS Reencrypted with ESP - ActiveSync** if the reencrypted template 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 of 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.

Exchange 2019 HTTPS Offload with ESP and WAF

Follow the instructions below to set up the parent **Exchange 2019 HTTPS Offloaded with ESP and WAF** Virtual Service:

1. Click **Virtual Services**.
2. Click **Add New**.
3. Enter a **Virtual Address**.
4. Select the **Exchange 2019 HTTPS Offload with ESP and WAF** template from the **Use Template** drop-down list.
5. Click **Add this Virtual Service**.

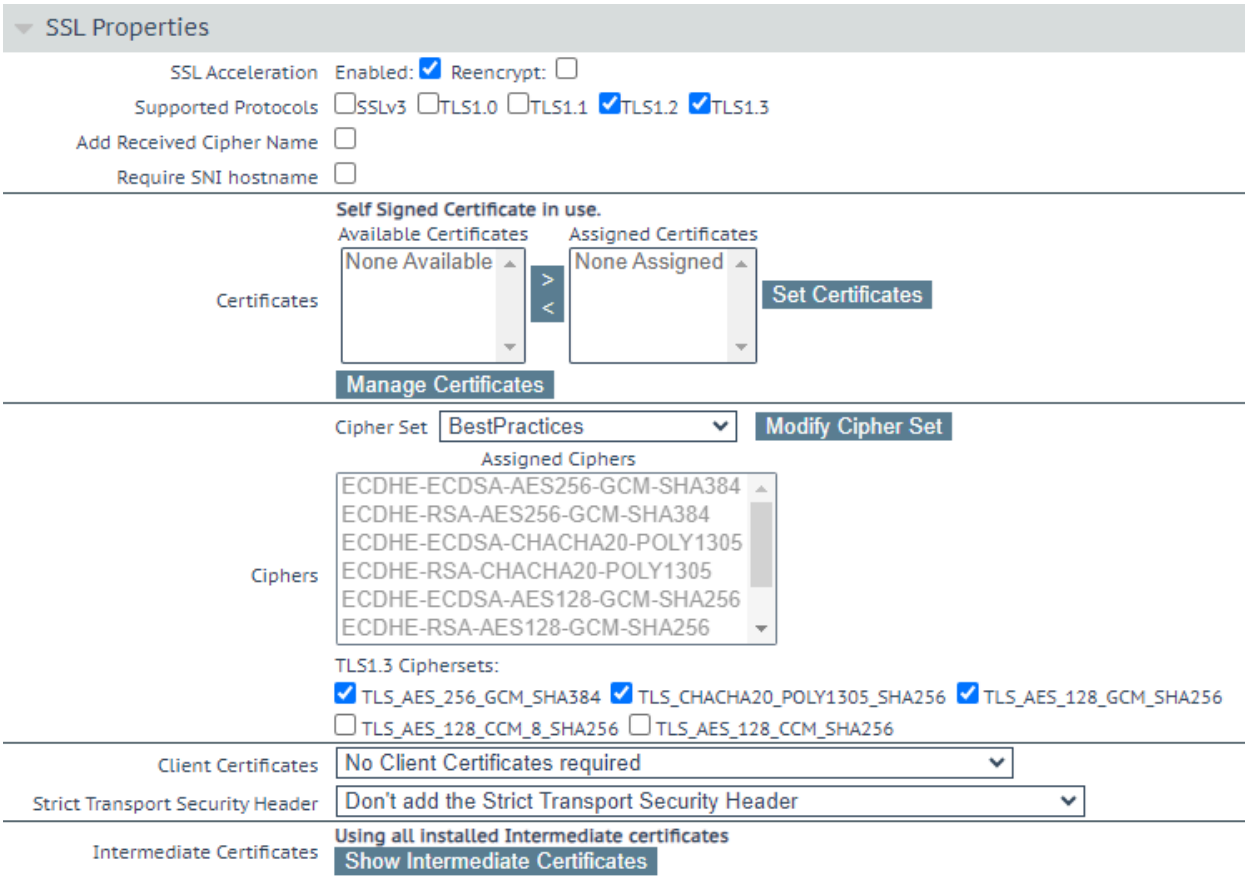
Contents

- Add SSL/TLS Certificate
- 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, reference the SSL Accelerated Services Feature Description.

1. Click **View/Modify Services** (under **Virtual Services**) in the left-hand navigation.
2. Click **Modify** for the **Exchange 2019 HTTPS Offload with ESP and WAF** Virtual Service on port 443 (or **Exchange 2019 HTTPS Reencrypted with ESP and WAF** if that was selected during the creation)
3. Expand **SSL Properties (Acceleration Enabled)**.



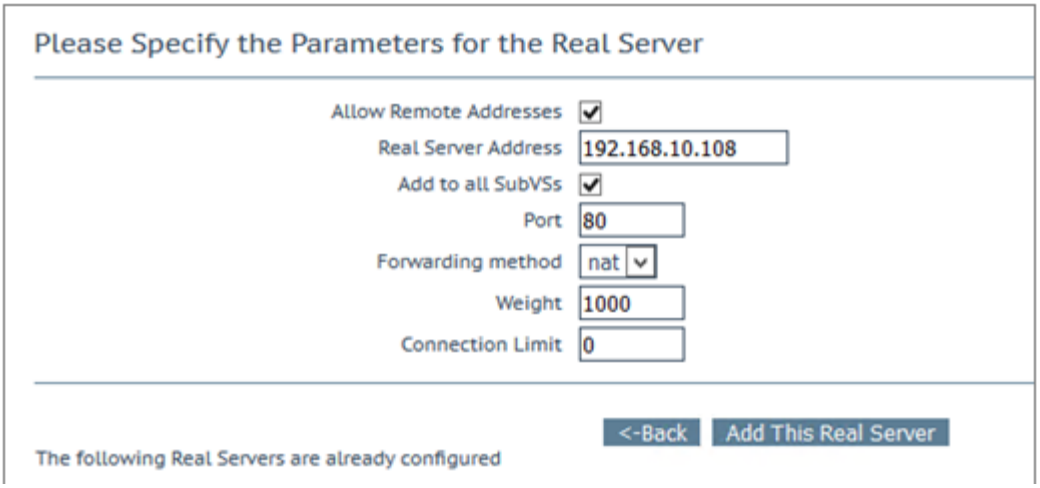
4. Select the certificate to use in the **Available Certificates** and click the “arrow” > to move it to **Assigned Certificates**.
5. Click **Set Certificate**.

Note: The **Reencrypt** check box is selected when using the **Exchange 2019 HTTPS Reencrypted with ESP and WAF** template.

Add the Real Servers

1. Click **View/Modify Services** in the left-hand navigation.
2. Click **Modify** for the **Exchange 2019 HTTPS Offloade with ESP and WAF** Virtual Service on port 443 (or the **Exchange 2019 HTTPS Reencrypted with ESP and WAF** if that was selected during the creation).
3. Expand the **SubVSs** section.
4. Click **Modify** for **Exchange 2019 HTTPS Offload with ESP and WAF - Authentication Proxy** (or the **Exchange 2019 HTTPS Reencrypted with ESP and WAF - Authentication Proxy** if that template was selected during creation).
5. Expand the **Real Servers** section.
6. Click **Add New**.

Note: In the ESP-enabled Virtual Services, there should be no Real Servers in the Authentication Proxy SubVS, unless you are using Kerberos server-side authentication. For further details on Kerberos Constrained Delegation (KCD), refer to the Kerberos Constrained Delegation Feature Description.



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.

   Note: Ensure to delete the Real Server from the Authentication Proxy SubVS if you are not using Kerberos server-side authentication.

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** (under **Virtual Services**) in the left-hand navigation.
2. Click **Modify** for the **Exchange 2019 HTTPS Offload with ESP and WAF** Virtual Service on port 443 (or the **Exchange 2019 HTTPS Reencrypted with ESP and WAF** if that was selected during 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	Logoff String	User Password Form
Authentication Proxy	/api /autodiscover/ autodiscover.svc /autodiscover/ autodiscover.json /autodiscover/ autodiscover.svc/wssecurity /ews/exchange.asmx/ wssecurity /ews/ exchange.asmx /ews/ mrsproxy.svc	n/a	n/a
ActiveSync	n/a	n/a	n/a

SubVS Name	Pre-Authorization Excluded Directories	Logoff String	User Password Form
API	n/a	n/a	n/a
Autodiscover	n/a	n/a	n/a
ECP	n/a	n/a	n/a
EWS	n/a	n/a	n/a
MAPI	n/a	n/a	n/a
OAB	n/a	n/a	n/a
OWA	/owa/<guid@smtpdomain>*[1]	/owa/logoff.owa	
PowerShell	n/a	n/a	n/a
RPC	n/a	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**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.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**.

Exchange 2019 HTTPS re-encrypted with WAF

Follow the instructions below to set up the parent **Exchange 2019 HTTPS re-encrypted with WAF** Virtual Service:

1. Click **Virtual Services**.
2. Click **Add New**.
3. Enter a **Virtual Address**.
4. Select the **Exchange 2019 HTTPS re-encrypted with WAF** template from the **Use Template** drop-down list.
5. Click **Add this Virtual Service**.

Contents

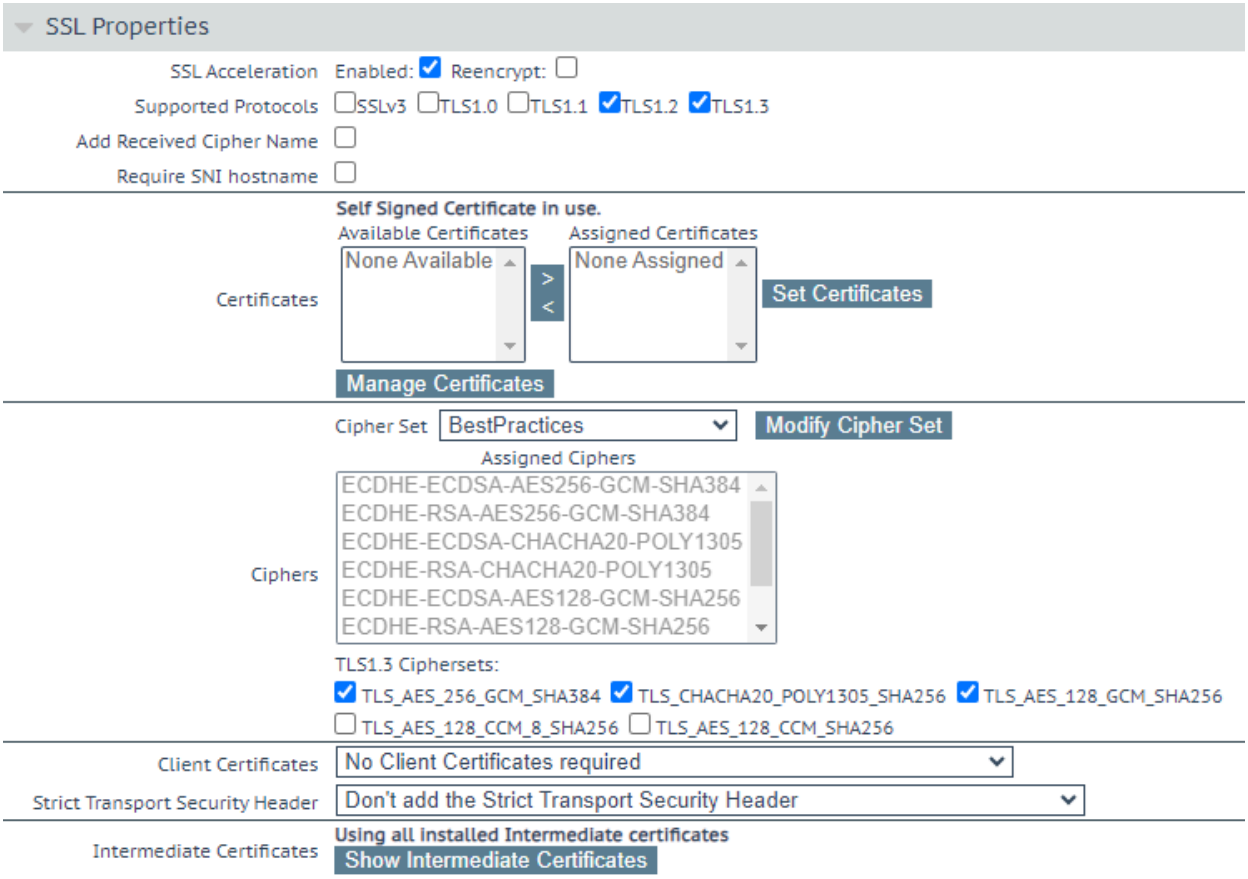
- Add SSL/TLS Certificate

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** (under **Virtual Services**) in the left-hand navigation.
2. Click **Modify** for the **Exchange 2019 HTTPS Offload with WAF** Virtual Service on port 443 (or **Exchange 2019 HTTPS Reencrypted with WAF** if that was selected during creation).
3. Expand **SSL Properties (Acceleration Enabled)**.



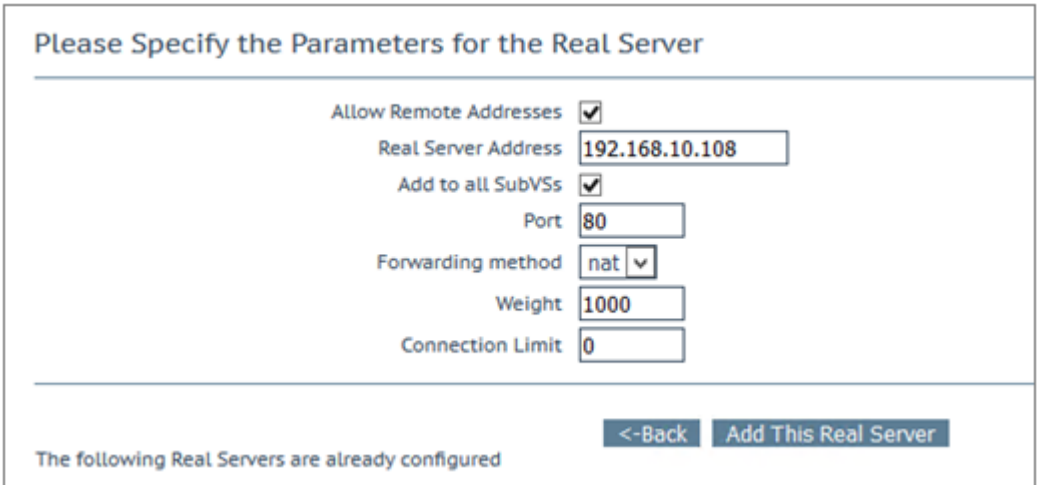
4. Select the certificate to use in the **Available Certificates** and click the “arrow” (>) to move it to **Assigned Certificates**.
5. Click **Set Certificates**.

Note: The **Reencrypt** check box is selected when using the **Exchange 2019 HTTPS Reencrypted with WAF** template.

Add the Real Servers

1. Click **View/Modify Services** in the left-hand navigation.
2. Click **Modify** for the **Exchange 2019 HTTPS Offload with WAF** Virtual Service on port 443 (or the **Exchange 2019 HTTPS Reencrypted with WAF** if that was selected during the creation).
3. Expand the **SubVSs** section.
4. Click **Modify** for **Exchange 2019 HTTPS Offload with ESP - ActiveSync** (or **Exchange 2019 HTTPS Reencrypted with ESP - ActiveSync** if the reencrypted template 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 of 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.

Exchange 2019 HTTPS re-encrypted with ESP and WAF

Follow the instructions below to set up the parent **Exchange 2019 HTTPS re-encrypted with ESP and WAF** Virtual Service:

1. Click **Virtual Services**.
2. Click **Add New**.
3. Enter a **Virtual Address**.
4. Select the **Exchange 2019 HTTPS re-encrypted with ESP and WAF** template from the **Use Template** drop-down list.
5. Click **Add this Virtual Service**.

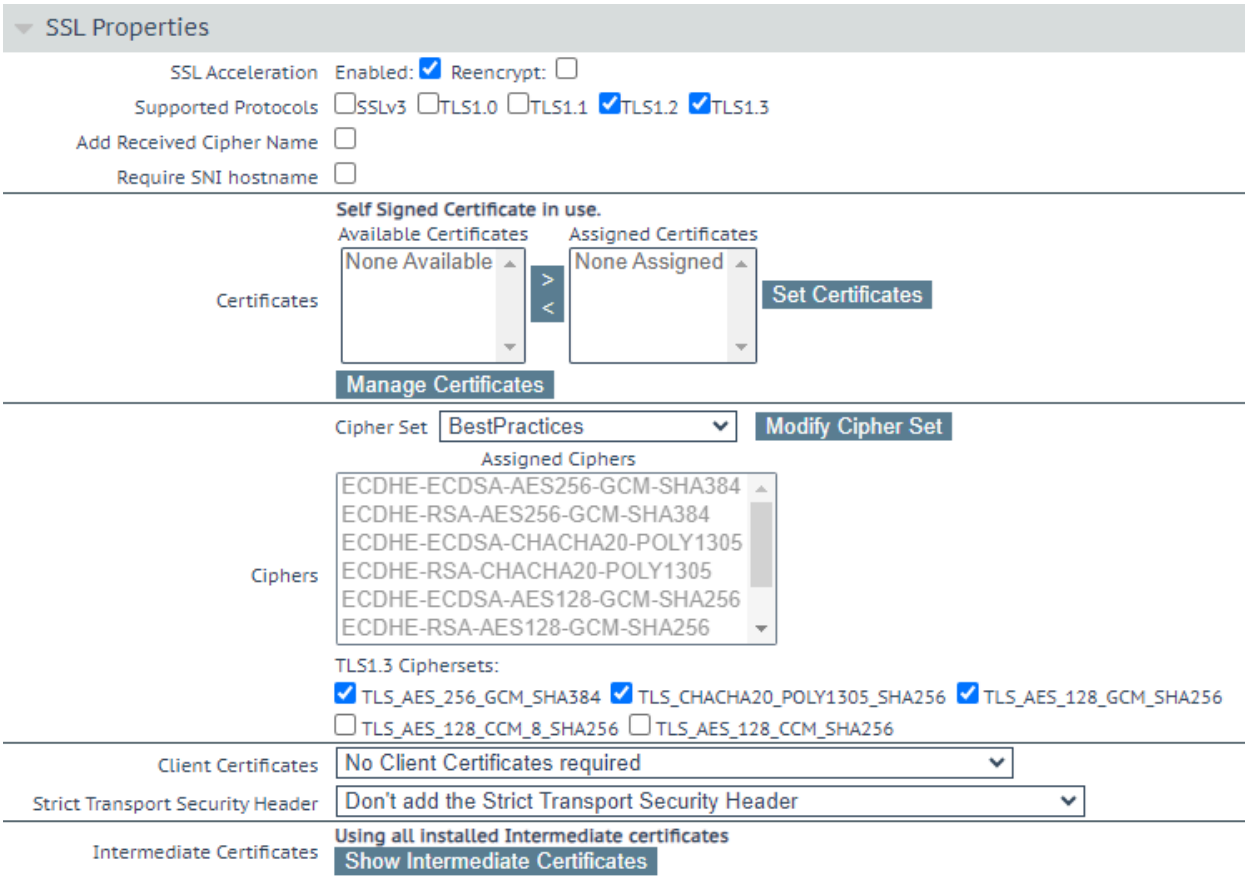
Contents

- Add SSL/TLS Certificate
- 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, reference the SSL Accelerated Services Feature Description.

1. Click **View/Modify Services** (under **Virtual Services**) in the left-hand navigation.
2. Click **Modify** for the **Exchange 2019 HTTPS Offload with ESP and WAF** Virtual Service on port 443 (or **Exchange 2019 HTTPS Reencrypted with ESP and WAF** if that was selected during the creation)
3. Expand **SSL Properties (Acceleration Enabled)**.



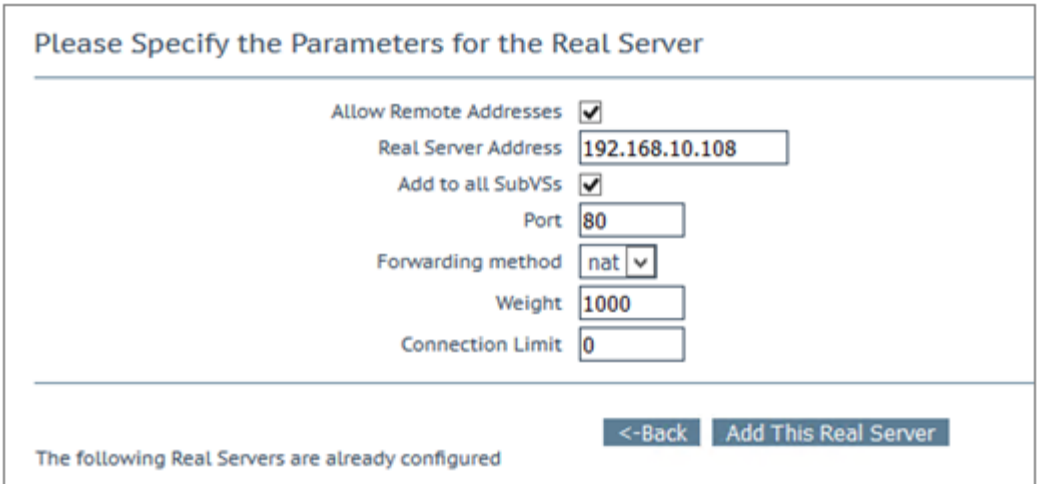
4. Select the certificate to use in the **Available Certificates** and click the “arrow” > to move it to **Assigned Certificates**.
5. Click **Set Certificate**.

Note: The **Reencrypt** check box is selected when using the **Exchange 2019 HTTPS Reencrypted with ESP and WAF** template.

Add the Real Servers

1. Click **View/Modify Services** in the left-hand navigation.
2. Click **Modify** for the **Exchange 2019 HTTPS Offloade with ESP and WAF** Virtual Service on port 443 (or the **Exchange 2019 HTTPS Reencrypted with ESP and WAF** if that was selected during the creation).
3. Expand the **SubVSs** section.
4. Click **Modify** for **Exchange 2019 HTTPS Offload with ESP and WAF - Authentication Proxy** (or the **Exchange 2019 HTTPS Reencrypted with ESP and WAF - Authentication Proxy** if that template was selected during creation).
5. Expand the **Real Servers** section.
6. Click **Add New**.

Note: In the ESP-enabled Virtual Services, there should be no Real Servers in the Authentication Proxy SubVS, unless you are using Kerberos server-side authentication. For further details on Kerberos Constrained Delegation (KCD), refer to the Kerberos Constrained Delegation Feature Description.



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.

   Note: Ensure to delete the Real Server from the Authentication Proxy SubVS if you are not using Kerberos server-side authentication.

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** (under **Virtual Services**) in the left-hand navigation.
2. Click **Modify** for the **Exchange 2019 HTTPS Offload with ESP and WAF** Virtual Service on port 443 (or the **Exchange 2019 HTTPS Reencrypted with ESP and WAF** if that was selected during 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	Logoff String	User Password Form
Authentication Proxy	/api /autodiscover/ autodiscover.svc /autodiscover/ autodiscover.json /autodiscover/ autodiscover.svc/wssecurity /ews/exchange.asmx/ wssecurity /ews/ exchange.asmx /ews/ mrsproxy.svc	n/a	n/a
ActiveSync	n/a	n/a	n/a

SubVS Name	Pre-Authorization Excluded Directories	Logoff String	User Password Form
API	n/a	n/a	n/a
Autodiscover	n/a	n/a	n/a
ECP	n/a	n/a	n/a
EWS	n/a	n/a	n/a
MAPI	n/a	n/a	n/a
OAB	n/a	n/a	n/a
OWA	/owa/<guid@smtpdomain>*[1]	/owa/logoff.owa	
PowerShell	n/a	n/a	n/a
RPC	n/a	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**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.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**.

5

Exchange 2019 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 2019 HTTP Virtual Service Recommended Settings (Optional)
- Exchange 2019 HTTPS Pass-through Virtual Service Recommended Settings (Optional)
- Exchange 2019 IMAP Virtual Service Recommended Settings (Optional)
- Exchange 2019 POP Virtual Service Recommended Settings (Optional)
- Exchange 2019 SMTP Virtual Service Recommended Settings (Optional)
- Exchange 2019 Office Online Server Virtual Service Recommended Settings (Optional)
- Exchange 2019 WAF Recommended Settings (Optional)

Exchange 2019 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
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	Redirect 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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
API				
name	api	Rule Name	api	All
matchtype	Regex	Match Type	Regular Expression	All
Pattern	%2F%5E%5C%2Fapi.%2A%2F	Match String	/^\/api.*/	All
Nocase	1	Ignore Case	Enabled	All
ECP				
name	ECP	Rule Name	ECP	All
matchtype	Regex	Match Type	Regular Expression	All
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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
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				

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
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%2Fpowershell.%2A%2F	Match String	/^\/powershell.*/	All
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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Nocase	1	Ignore Case	Enabled	All
Main Virtual Service				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
VStype	http	Service Type	http	All
nickname	Exchange%20HTTPS%20 Offloaded	Service Name (Optional)	HTTP-HTTP/ 2-HTTPS	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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
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	1	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
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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
prot	tcp	Protocol	tcp	All
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

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	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
API				
Port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	API	Service Name (Optional)	API	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	%2Fapi%2Fhealthcheck.htm	URL	/api/healthcheck.htm	All
CheckUse1.1	0	Use HTTP/1.1	Disabled	All
CheckUseGet	1	HTTP Method	GET	All
EspEnabled	0	Enable ESP	Enabled	All
Autodiscover				
Port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	Autodiscover	Service Name (Optional)	Autodiscover	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	None	Persistence Options	None	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
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.exampl	Allowed Virtual Hosts	Mail.example.com autodiscover.example	ESP Enabled

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
	e.com		.com	
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
Idletime	1800	Idle Connection Timeout	1800	All
CheckPort	443	Checked Port	443	All
CheckType	https	Real Server Check Method	HTTPS Protocol	All
CheckUrl	%2Fecp%2Fhealthch	URL	/ecp/healthcheck.htm	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
	eck.htm			
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				

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
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 Timeout	1800	All
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

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	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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
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	%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.exampl	Allowed Virtual Hosts	Mail.example.com autodiscover.example	ESP Enabled

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
	e.com		.com	
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%2Fhealthch	URL	/oab/healthcheck.htm	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
	eck.htm			
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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Nickname	OWA	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
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
ESPLogs	7	ESP Logging	User Access, Security and Connection (Enabled)	ESP Enabled

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
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	Logoff String	/owa/logoff.owa	ESP Enabled
PowerShell				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	PowerShell	Service Name (Optional)	PowerShell	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
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
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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
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)	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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
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, 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	%2Frpc%2A	Allowed Virtual Directories	/rpc*	ESP Enabled

Exchange 2019 HTTPS Pass-through Virtual Service Recommended Settings (Optional)

API Parameter	API Value	WUI Field Name	WUI Field Value
HTTPS Pass-through			
port	443	Port	443
prot	tcp	Protocol	tcp
VStype	http	Service Type	HTTP-HTTP/2-HTTPS
nickname	Exchange%202019%20HTTPS%20pass-through	Service Name (Optional)	Exchange 2019 HTTPS pass-through
ForceL7	1	Force L4	Disabled
Transparent	0	Transparency	Disabled
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	none	Persistence Options	None
Schedule	lc	Scheduling Method	least connection
Idletime	1800	Idle Connection Timeout	1800
CheckType	https	Real Server Check Method	HTTPS Protocol

API Parameter	API Value	WUI Field Name	WUI Field Value
CheckPort	443	Checked Port	443
CheckUrl	%2Fowa%2Fhealthcheck.htm	URL	/owa/healthcheck.htm
CheckUse1.1	0	Use HTTP/1.1	Disabled
CheckUseGet	1	HTTP Method	GET
HTTPS Pass-through Redirect			
port	80	Port	80
prot	tcp	Protocol	tcp
VStype	http	Service Type	HTTP-HTTP/2-HTTPS
nickname	Exchange%202019%20HTTPS%20pass-through%20-%20HTTP%20Redirect	Service Name (Optional)	Exchange 2019 HTTPS pass-through - HTTP Redirect
ForceL7	1	Force L4	Disabled
Errorcode	301	Error Code	301 Moved Permanently
ErrorUrl	https:%2F%2F%25h%25s	Redirect URL	https://%h%s
CheckType	none	Real Server Check Method	None

Exchange 2019 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
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

API Parameter	API Value	WUI Field Name	WUI Field Value
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
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

API Parameter	API Value	WUI Field Name	WUI Field Value
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
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

API Parameter	API Value	WUI Field Name	WUI Field Value
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			
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

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

Exchange 2019 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
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	None	Persistence Options	None
Schedule	rr	Scheduling Method	round robin
Idletime	3600	Idle Connection Timeout	3600

API Parameter	API Value	WUI Field Name	WUI Field Value
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
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	None	Persistence Options	None
Schedule	rr	Scheduling Method	round robin
Idletime	3600	Idle Connection Timeout	3600

API Parameter	API Value	WUI Field Name	WUI Field Value
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
ServerInit	Pop3	Server Initiating Protocols	POP3
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	None	Persistence Options	None
Schedule	rr	Scheduling Method	round robin

API Parameter	API Value	WUI Field Name	WUI Field Value
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	BestPractice	CipherSet	BestPractices
CheckType	Pop3	Real Server Check Method	Mailbox (POP3) Protocol
CheckPort	110	Checked Port	110
POP with STARTTLS			
port	110	Port	110
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

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

Exchange 2019 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
Persist	src	Persistence Options	Source IP Address
PersistTimeout	3600	Timeout	1 Hour
Schedule	rr	Scheduling Method	round robin

API Parameter	API Value	WUI Field Name	WUI Field Value
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
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	src	Persistence Options	Source IP Address
PersistTimeout	3600	Timeout	1 Hour

API Parameter	API Value	WUI Field Name	WUI Field Value
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
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	1 Hour
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
SMTP with STARTTLS			
port	25	Port	25
prot	tcp	Protocol	tcp
VStype	StartTLS	Service Type	STARTTLS protocols

API Parameter	API Value	WUI Field Name	WUI Field Value
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	1 Hour
Schedule	rr	Scheduling Method	round robin
Idletime	120	Idle Connection Timeout	120
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

API Parameter	API Value	WUI Field Name	WUI Field Value
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
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	src	Persistence Options	Source IP Address
PersistTimeout	3600	Timeout	1 Hour
Schedule	rr	Scheduling Method	round robin

API Parameter	API Value	WUI Field Name	WUI Field Value
IdleTime	120	Idle Connection Timeout	120
EnableESP	1	Enable ESP	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

Exchange 2019 Office Online Server Virtual Service Recommended Settings (Optional)

API Parameter	API Value	WUI Field Name	WUI Field Value
Office Online Server			
port	443	Port	443
prot	tcp	Protocol	tcp
VStype	http	Service Type	HTTP-HTTP/2-HTTPS
nickname	Exchange%20Office%20Online	Service Name (Optional)	Exchange Office Online

API Parameter	API Value	WUI Field Name	WUI Field Value
ForceL7	1	Force L4	Disabled
Transparent	0	Transparency	Disabled
SubnetOriginating	1	Subnet Originating Requests	Enabled
Persist	Super-src	Persistence Options	Super HTTP and Source IP
PersistTimeout	1800	Timeout	30 Minutes
Schedule	lc	Scheduling Method	least connection
Idletime	1800	Idle Connection Timeout	1800
SSLAcceleration	1	SSL Acceleration	Enabled
SSLReencrypt	1	Reencrypt	Enabled
TLSType	1	Supported Protocols	TLS1.0, TLS1.1, TLS1.2, and TLS1.3 (Enabled)
CipherSet	BestPractices	CipherSet	BestPractices
CheckType	https	Real Server Check Method	HTTPS Protocol
CheckPort	443	Checked Port	443

API Parameter	API Value	WUI Field Name	WUI Field Value
CheckUrl	/hosting/discovery	URL	/hosting/discovery
CheckUse1.1	1	Use HTTP/1.1	Enabled
CheckUseGet	1	HTTP Method	GET

Exchange 2019 WAF Recommended Settings (Optional)

These tables in the following sections outline the recommended settings using the WAF application templates. You can use these settings with scripts and automation tools.

Contents

- Exchange 2019 HTTPS Offload with WAF Recommended Settings (Optional)
- Exchange 2019 HTTPS Offload with ESP and WAF Recommended Settings (Optional)
- Exchange 2019 HTTPS re-encrypted with WAF Recommended Settings (Optional)
- Exchange 2019 HTTPS re-encrypted with ESP and WAF Recommended Settings (Optional)
- Content Rules

Exchange 2019 HTTPS Offload with WAF 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%202019%20HTTPS%20Offloaded%20with%20WAF%20HTTP%20Redirect	Service Name	Exchange 2019 HTTPS Offloaded with WAF - HTTP Redirect	All
Errorcode	302	Error Code	302 Found	All
ErrorUrl	https:%2F%2F%25h%25s	Redirect URL	https://%h%s	All
CheckType	http	Real Server Check Method	HTTP Protocol	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%202019%20HTTPS%20Offload%20with%20WAF	Service Name	Exchange 2019 HTTPS Offload with WAF	Create Unique Name
SSLAcceleration	1	SSL Acceleration	Enabled	All
SSLReencrypt	0	Reencrypt	Disabled	0 for Offload 1 for Reencrypt

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
TLSType	7	Supported Protocols	TLS1.2 and TLS1.3 (Enabled)	All
CipherSet	BestPractices	Cipher Set	BestPractices	All
Tls13CipherSet	TLS_AES_256_GCM_SHA384%20TLS_CHACHA20_POLY1305_SHA256%20TLS_AES_128_GCM_SHA256	TLS1.3 Ciphersets	TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, and TLS_AES_128_GCM_SHA256 enabled	All
Persist	none	Persistence Options	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	1800	Idle Connection Timeout	1800	All
SubVSs				
ActiveSync				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	ActiveSync	SubVS Name	ActiveSync	All
SubnetOriginating	1	Subnet Originating	Enabled	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
		Requests		
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
CheckPort	80	Checked Port	80	All
CheckType	http	Real Server Check Method	HTTP 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	0	Enable ESP	Disabled	All
API				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Nickname	API	SubVS Name	API	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
CheckPort	80	Checked Port	80	All
CheckType	http	Real Server Check Method	HTTP Protocol	All
CheckUrl	%2Fapi%2Fhealthcheck.htm	URL	/api/healthcheck.htm	All
CheckUse1.1	0	Use HTTP/1.1	Disabled	All
CheckUseGet	1	HTTP Method	GET	All
EspEnabled	0	Enable ESP	Disabled	All
Autodiscover				
port	443	Port	443	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
prot	tcp	Protocol	tcp	All
Nickname	Autodiscover	SubVS Name	Autodiscover	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
CheckPort	80	Checked Port	80	All
CheckType	http	Real Server Check Method	HTTP 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	0	Enable ESP	Disabled	All
ECP				

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	ECP	SubVS Name	ECP	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
Interceptmode	2	OWAP Core Rule Set WAF	Enabled	WAF Enabled
CheckPort	80	Checked Port	80	All
CheckType	http	Real Server Check Method	HTTP 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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
EspEnabled	0	Enable ESP	Disabled	All
EWS				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	EWS	SubVS Name	EWS	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
CheckPort	80	Checked Port	80	All
CheckType	http	Real Server Check Method	HTTP Protocol	All
CheckUrl	%2Fews%2Fhealthcheck.htm	URL	/ews/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	0	Enable ESP	Disabled	All
MAPI				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	MAPI	SubVS Name	MAPI	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
CheckPort	80	Checked Port	80	All
CheckType	http	Real Server Check Method	HTTP Protocol	All
CheckUrl	%2Fmapi%2Fhealthcheck.htm	URL	/mapi/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	0	Enable ESP	Disabled	All
OAB				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	OAB	SubVS Name	OAB	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
CheckPort	80	Checked Port	80	All
CheckType	http	Real Server Check Method	HTTP Protocol	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
CheckUrl	%2Foab%2Fhealthcheck.htm	URL	/oab/healthcheck.htm	All
CheckUse1.1	0	Use HTTP/1.1	Disabled	All
CheckUseGet	1	HTTP Method	GET	All
EspEnabled	0	Enable ESP	Disabled	All
OWA				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	OWA	SubVS Name	OWA	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
Interceptmode	2	OWASP Core Rule Set WAF	Enabled	WAF enabled

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
CheckPort	80	Checked Port	80	All
CheckType	http	Real Server Check Method	HTTP 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	0	Enable ESP	Disabled	All
PowerShell				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	PowerShell	SubVS Name	PowerShell	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Idletime	0	Idle Connection Timeout	Empty	All
CheckPort	80	Checked Port	80	All
CheckType	http	Real Server Check Method	HTTP Protocol	All
CheckUrl	%2Fpowershell%2Fhealthcheck.htm	URL	/powershell/healthcheck.htm	All
CheckUse1.1	0	Use HTTP/1.1	Disabled	All
CheckUseGet	1	HTTP Method	GET	All
EspEnabled	0	Enable ESP	Disabled	All
RPC				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	RPC	SubVS Name	RPC	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
CheckPort	80	Checked Port	80	All
CheckType	http	Real Server Check Method	HTTP 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	0	Enable ESP	Disabled	All

Exchange 2019 HTTPS Offload with ESP and WAF Recommended Settings (Optional)

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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
prot	tcp	Protocol	tcp	All
nickname	Exchange%202019%20HTTPS%20Offloaded%20with%20ESP%20and%20WAF%20HTTP%20Redirect	Service Name	Exchange 2019 HTTPS Offloaded with ESP and WAF - HTTP Redirect	All
Errorcode	302	Error Code	302 Found	All
ErrorUrl	https:%2F%2F%25h%25s	Redirect URL	https://%h%s	All
CheckType	http	Real Server Check Method	HTTP Protocol	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%202019%20HTTPS%20Offload%20with%20ESP%20and%20WAF	Service Name	Exchange 2019 HTTPS Offload with ESP and WAF	Create Unique Name
Transparent	1	Transparency	Enabled	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
SSLAcceleration	1	SSL Acceleration	Enabled	All
SSLReencrypt	0	Reencrypt	Disabled	0 for Offload 1 for Reencrypt
TLSType	7	Supported Protocols	TLS1.2 and TLS1.3 (Enabled)	All
CipherSet	BestPractices	Cipher Set	BestPractices	All
Tls13CipherSet	TLS_AES_256_GCM_SHA384%20TLS_CHACHA20_POLY1305_SHA256%20TLS_AES_128_GCM_SHA256	TLS1.3 Ciphersets	TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, and TLS_AES_128_GCM_SHA256 enabled	All
Persist	none	Persistence Options	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	1800	Idle Connection Timeout	1800	All
SubVSs				
Authentication Proxy				
port	443	Port	443	ESP Enabled

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
prot	tcp	Protocol	tcp	ESP Enabled
Nickname	Authentication%20Proxy	SubVS Name	Authentication Proxy	ESP Enabled
Errorcode	503	Error Code	503 Service Unavailable	ESP Enabled
ErrorUrl	Endpoint%20not%20available	Error Message	Endpoint not available	ESP Enabled
CheckType	http	Real Server Check Method	HTTP Protocol	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
AllowedDirectories	%2F%2A	Allowed Virtual Directories	/*	ESP Enabled
SingleSignOnMessage	Please%20enter%20your%20Exchange%20credentials	SSO Greeting Message	Please enter your Exchange credentials	ESP Enabled

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
ActiveSync				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	ActiveSync	SubVS Name	ActiveSync	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
CheckPort	80	Checked Port	80	All
CheckType	http	Real Server Check Method	HTTP 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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
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
AllowedDirectories	%2Fmicrosoft-server-activesync%2A	Allowed Virtual Directories	/microsoft-server-activesync*	ESP Enabled
API				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	API	SubVS Name	API	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
CheckPort	80	Checked Port	80	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
CheckType	http	Real Server Check Method	HTTP Protocol	All
CheckUrl	%2Fapi%2Fhealthcheck.htm	URL	/api/healthcheck.htm	All
CheckUse1.1	0	Use HTTP/1.1	Disabled	All
CheckUseGet	1	HTTP Method	GET	All
EspEnabled	0	Enable ESP	Disabled	All
Autodiscover				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	Autodiscover	SubVS Name	Autodiscover	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
CheckPort	80	Checked Port	80	All
CheckType	http	Real Server Check Method	HTTP 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
AllowedDirectories	%2Fautodiscover%2A	Allowed Virtual Directories	/autodiscover*	ESP Enabled
ECP				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Nickname	ECP	SubVS Name	ECP	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
Interceptmode	2	OWASP Core Rule Set WAF	Enabled	WAF enabled
CheckPort	80	Checked Port	80	All
CheckType	http	Real Server Check Method	HTTP 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,	ESP Enabled

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
			Security and Connection (Enabled)	
InputAuthMode	2	Client Authentication Mode	Form Based	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	SubVS Name	EWS	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
CheckPort	80	Checked Port	80	All
CheckType	http	Real Server Check Method	HTTP 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
AllowedDirectories	%2Fews%2A	Allowed Virtual Directories	/ews*	ESP Enabled
MAPI				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Nickname	MAPI	SubVS Name	MAPI	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
CheckPort	80	Checked Port	80	All
CheckType	http	Real Server Check Method	HTTP Protocol	All
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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
InputAuthMode	0	Client Authentication Mode	Delegate to Server	ESP Enabled
AllowedDirectories	%2Fmapi%2A	Allowed Virtual Directories	/mapi*	ESP Enabled
OAB				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	OAB	SubVS Name	OAB	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
CheckPort	80	Checked Port	80	All
CheckType	http	Real Server Check Method	HTTP Protocol	All
CheckUrl	%2Foab%2Fhealthch	URL	/oab/healthcheck.htm	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
	eck.htm			
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
AllowedDirectories	%2Foab%2A	Allowed Virtual Directories	/oab*	ESP Enabled
OWA				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	OWA	SubVS Name	OWA	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
Interceptmode	2	OWASP Core Rule Set WAF	Enabled	WAF enabled
CheckPort	80	Checked Port	80	All
CheckType	http	Real Server Check Method	HTTP 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
ESPLogs	7	ESP Logging	User Access, Security and Connection (Enabled)	ESP Enabled
InputAuthMode	2	Client Authentication Mode	Form Based	ESP Enabled
AllowedDirectories	%2Fowa%2A	Allowed Virtual Directories	/owa*	ESP Enabled

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
ExcludedDirectories	%2Fowa%2Fguid%40smtpdomain%2AExchange%20credentials	Pre-Authorization Excluded Directories	/owa/guid@smtpdomain*	ESP Enabled
SingleSignOnMessage	Please%20enter%20your%20	SSO Greeting Message	Please enter your Exchange credentials	ESP Enabled
Logoff	%2Fowa%2Flogoff.owa	Logoff String	/owa/logoff.owa	ESP Enabled
PowerShell				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	PowerShell	SubVS Name	PowerShell	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
CheckPort	80	Checked Port	80	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
CheckType	http	Real Server Check Method	HTTP Protocol	All
CheckUrl	%2Fpowershell%2Fhealthcheck.htm	URL	/powershell/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
AllowedDirectories	%2Fpowershell%2A	Allowed Virtual Directories	/powershell*	ESP Enabled
RPC				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	RPC	SubVS Name	RPC	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
CheckPort	80	Checked Port	80	All
CheckType	http	Real Server Check Method	HTTP 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, Security and Connection (Enabled)	ESP Enabled
InputAuthMode	0	Client Authentication Mode	Delegate to Server	ESP Enabled

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
AllowedDirectories	%2Frpc%2A	Allowed Virtual Directories	/rpc*	ESP Enabled

Exchange 2019 HTTPS re-encrypted with WAF 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
nickname	Exchange%202019%20HTTPS%20re-encrypted%20with%20WAF%20HTTP%20Redirect	Service Name	Exchange 2019 HTTPS re-encrypted with WAF - HTTP Redirect	All
Errorcode	302	Error Code	302 Found	All
ErrorUrl	https:%2F%2F%25h%25s	Redirect URL	https://%h%s	All
CheckType	http	Real Server Check Method	HTTP Protocol	All
Main Virtual Service				

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
VStype	http	Service Type	HTTP-HTTP/ 2-HTTPS	All
nickname	Exchange%202016% 20HTTPS%20re- encrypted%20with%2 0WAF	Service Name	Exchange 2016 HTTPS re-encrypted with WAF	Create Unique Name
Transparent	0	Transparency	Disabled	All
SSLAcceleration	1	SSL Acceleration	Enabled	All
SSLReencrypt	1	Reencrypt	Enabled	0 for Offload 1 for Reencrypt
TLSType	7	Supported Protocols	TLS1.2 and TLS1.3 (Enabled)	All
CipherSet	BestPractices	Cipher Set	BestPractices	All
Tls13CipherSet	TLS_AES_256_GCM _SHA384%20TLS_C HACHA20_POLY130 5_SHA256%20TLS_ AES_128_GCM_SH A256	TLS1.3 Ciphersets	TLS_AES_256_GCM _SHA384, TLS_CHACHA20_P OLY1305_SHA256, and TLS_AES_128_GCM _SHA256 enabled	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	1800	Idle Connection Timeout	1800	All
SubVSs				
ActiveSync				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	ActiveSync	SubVS Name	ActiveSync	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
CheckPort	443	Checked Port	443	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
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	0	Enable ESP	Disabled	All
API				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	API	SubVS Name	API	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
CheckPort	443	Checked Port	443	All
CheckType	https	Real Server Check Method	HTTPS Protocol	All
CheckUrl	%2Fapi%2Fhealthcheck.htm	URL	/api/healthcheck.htm	All
CheckUse1.1	0	Use HTTP/1.1	Disabled	All
CheckUseGet	1	HTTP Method	GET	All
EspEnabled	0	Enable ESP	Disabled	All
Autodiscover				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	Autodiscover	SubVS Name	Autodiscover	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Idletime	0	Idle Connection Timeout	Empty	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	0	Enable ESP	Disabled	All
ECP				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	ECP	SubVS Name	ECP	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
Interceptmode	2	OWASP Core Rule Set WAF	Enabled	WAF enabled
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	0	Enable ESP	Disabled	All
EWS				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	EWS	SubVS Name	EWS	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
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	0	Enable ESP	Disabled	All
MAPI				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Nickname	MAPI	SubVS Name	MAPI	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
CheckPort	443	Checked Port	443	All
CheckType	https	Real Server Check Method	HTTPS Protocol	All
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	0	Enable ESP	Disabled	All
OAB				
port	443	Port	443	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
prot	tcp	Protocol	tcp	All
Nickname	OAB	SubVS Name	OAB	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	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
CheckUse1.1	0	Use HTTP/1.1	Disabled	All
CheckUseGet	1	HTTP Method	GET	All
EspEnabled	0	Enable ESP	Disabled	All
OWA				

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	OWA	SubVS Name	OWA	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
Interceptmode	2	OWASP Core Rule Set WAF	Enabled	WAF enabled
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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
EspEnabled	0	Enable ESP	Disabled	All
PowerShell				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	PowerShell	SubVS Name	PowerShell	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	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	0	Enable ESP	Disabled	All
RPC				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	RPC	SubVS Name	RPC	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	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

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	0	Enable ESP	Disabled	All

Exchange 2019 HTTPS re-encrypted with ESP and WAF 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
nickname	Exchange%202019%20HTTPS%20re-encrpted%20with%20ESP%20and%20WAF%20HTTP%20Redirect	Service Name	Exchange 2019 HTTPS re-encrypted with ESP and WAF - HTTP Redirect	All
Errorcode	302	Error Code	302 Found	All
ErrorUrl	https:%2F%2F%25h%25s	Redirect URL	https://%h%s	All
CheckType	http	Real Server Check	HTTP Protocol	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
		Method		
Main Virtual Service				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
VStype	http	Service Type	HTTP-HTTP/ 2-HTTPS	All
nickname	Exchange%202016%20HTTPS%20re-encrypted%20with%20ESP%20and%20WAF	Service Name	Exchange 2016 HTTPS re-encrypted with ESP and WAF	Create Unique Name
Transparent	0	Transparency	Disabled	All
SSLAcceleration	1	SSL Acceleration	Enabled	All
SSLReencrypt	1	Reencrypt	Enabled	0 for Offload 1 for Reencrypt
TLSType	7	Supported Protocols	TLS1.2 and TLS1.3 (Enabled)	All
CipherSet	BestPractices	Cipher Set	BestPractices	All
Tls13CipherSet	TLS_AES_256_GCM	TLS1.3 Ciphersets	TLS_AES_256_GCM	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
	_SHA384%20TLS_CHACHA20_POLY1305_SHA256%20TLS_AES_128_GCM_SHA256		_SHA384, TLS_CHACHA20_POLY1305_SHA256, and TLS_AES_128_GCM_SHA256 enabled	
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	1800	Idle Connection Timeout	1800	All
SubVSs				
Authentication Proxy				
port	443	Port	443	ESP Enabled
prot	tcp	Protocol	tcp	ESP Enabled
Nickname	Authentication%20Proxy	SubVS Name	Authentication Proxy	ESP Enabled
Errorcode	503	Error Code	503 Service Unavailable	ESP Enabled
ErrorUrl	Endpoint%20not%20available	Error Message	Endpoint not available	ESP Enabled

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
CheckType	https	Real Server Check Method	HTTPS Protocol	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
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
Nickname	ActiveSync	SubVS Name	ActiveSync	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	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
AllowedDirectories	%2Fmicrosoft-server-activesync%2A	Allowed Virtual Directories	/microsoft-server-activesync*	ESP Enabled
API				

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	API	SubVS Name	API	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
CheckPort	443	Checked Port	443	All
CheckType	https	Real Server Check Method	HTTPS Protocol	All
CheckUrl	%2Fapi%2Fhealthcheck.htm	URL	/api/healthcheck.htm	All
CheckUse1.1	0	Use HTTP/1.1	Disabled	All
CheckUseGet	1	HTTP Method	GET	All
EspEnabled	0	Enable ESP	Disabled	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Autodiscover				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	Autodiscover	SubVS Name	Autodiscover	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
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
AllowedDirectories	%2Fautodiscover%2A	Allowed Virtual Directories	/autodiscover*	ESP Enabled
ECP				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	ECP	SubVS Name	ECP	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Interceptmode	2	OWASP Core Rule Set WAF	Enabled	WAF Enabled
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
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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
EWS				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	EWS	SubVS Name	EWS	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
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
AllowedDirectories	%2Fews%2A	Allowed Virtual Directories	/ews*	ESP Enabled
MAPI				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	MAPI	SubVS Name	MAPI	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
CheckPort	443	Checked Port	443	All
CheckType	https	Real Server Check Method	HTTPS Protocol	All
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
AllowedDirectories	%2Fmapi%2A	Allowed Virtual Directories	/mapi*	ESP Enabled
OAB				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Nickname	OAB	SubVS Name	OAB	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	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
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

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
InputAuthMode	0	Client Authentication Mode	Delegate to Server	ESP Enabled
AllowedDirectories	%2Foab%2A	Allowed Virtual Directories	/oab*	ESP Enabled
OWA				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	OWA	SubVS Name	OWA	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
Interceptmode	2	OWASP Core Rule Set WAF	Enabled	WAF Enabled
CheckPort	443	Checked Port	443	All
CheckType	https	Real Server Check Method	HTTPS Protocol	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
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
ESPLogs	7	ESP Logging	User Access, Security and Connection (Enabled)	ESP Enabled
InputAuthMode	2	Client Authentication Mode	Form Based	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	Logoff String	/owa/logoff.owa	ESP Enabled
PowerShell				

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	PowerShell	SubVS Name	PowerShell	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	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
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	0	Client Authentication Mode	Delegate to Server	ESP Enabled
AllowedDirectories	%2Fpowershell%2A	Allowed Virtual Directories	/powershell*	ESP Enabled
RPC				
port	443	Port	443	All
prot	tcp	Protocol	tcp	All
Nickname	RPC	SubVS Name	RPC	All
SubnetOriginating	1	Subnet Originating Requests	Enabled	All
Persist	none	Persistence Mode	None	All
Schedule	lc	Scheduling Method	least connection	All
Idletime	0	Idle Connection Timeout	Empty	All
CheckPort	443	Checked Port	443	All

API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
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, Security and Connection (Enabled)	ESP Enabled
InputAuthMode	0	Client Authentication Mode	Delegate to Server	ESP Enabled
AllowedDirectories	%2Frpc%2A	Allowed Virtual Directories	/rpc*	ESP Enabled

Content Rules

SubVSs	API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Authentication Proxy					
	name	Authentication_Proxy	Rule Name	Authentication Proxy	ESP Enabled
	matchtype	Regex	Match Type	RegEx	ESP Enabled

SubVSs	API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
	pattern	%2F%5E%5C%2Flm_auth_proxy%2A%24%2F	Match String	/^\/lm_auth_proxy*$/	ESP Enabled
	Nocase	1	Ignore Case	Enabled	ESP Enabled
ActiveSync					
	name	ActiveSync	Rule Name	ActiveSync	ESP Enabled
	matchtype	Regex	Match Type	RegEx	ESP Enabled
	pattern	%2F%5E%5C%2Fmicrosoft-server-activesync.%2A%2F	Match String	/^\/microsoft-server-activesync.*/	ESP Enabled
	Nocase	1	Ignore Case	Enabled	ESP Enabled
API					
API (Content rule)					
	name	API	Rule Name	API	All
	matchtype	Regex	Match Type	RegEx	All
	pattern	%2F%5E%5C%2Fapi.%2A%2F	Match String	/^\/api.*/	All
	Nocase	1	Ignore Case	Enabled	All
Autodiscover wssecurity (Content rule)					
	name	Autodiscover_wssecurity	Rule Name	Autodiscoverwssecurity	All
	matchtype	Regex	Match Type	RegEx	All
	pattern	%2F%5E%5C%2Fautodiscover%5C%2Fautodiscover%5C.svc%2Fwssecurity%24%2F	Match String	/^\/autodiscover\/autodiscover\.svc/wssecurity$/	All
	Nocase	1	Ignore Case	Enabled	All

SubVSs	API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
Autodiscover svc (Content rule)					
	name	Autodiscover_svc	Rule Name	Autodiscover svc	All
	matchtype	Regex	Match Type	RegEx	All
	pattern	%2F%5E%5C%2Fautodiscover%5C%2Fautodiscover%5C.svc%24%2F	Match String	^\/autodiscover\/autodiscover\.svc$/	All
	Nocase	1	Ignore Case	Enabled	All
Autodiscover json (Content rule)					
	name	Autodiscover_json	Rule Name	Autodiscover json	All
	matchtype	Regex	Match Type	RegEx	All
	pattern	%2F%5E%5C%2Fautodiscover%5C%2Fautodiscover%5C.json%24%2F	Match String	^\/autodiscover\/autodiscover\.json$/	All
	Nocase	1	Ignore Case	Enabled	All
EWS wssecurity (Content rule)					
	name	EWS_wssecurity	Rule Name	EWS wssecurity	All
	matchtype	Regex	Match Type	RegEx	All
	pattern	%2F%5E%5C%2Fews%5C%2Fexchnage%5Casmx%5C%2Fwssecurity%24%2F	Match String	/^\/ews\/exchange\.asmx\/wssecurity$/	All
	Nocase	1	Ignore Case	Enabled	All
EWS exchange (Content rule)					
	name	EWS_exchange	Rule Name	EWS exchange	All
	matchtype	Regex	Match Type	RegEx	All

SubVSs	API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
	pattern	%2F%5E%5C%2Fews%5C%2Fexchnage%5C.asmx%24%2F	Match String	/^\/ews\/exchange\.asmx$/	All
	Nocase	1	Ignore Case	Enabled	All
EWS mrsproxy svc (Content rule)					
	name	EWS_mrsproxy_svc	Rule Name	EWS mrsproxy svc	All
	matchtype	Regex	Match Type	RegEx	All
	pattern	%2F%5E%5C%2Fews%5C%2Fexchnage%5C.svc%24%2F	Match String	/^\/ews\/mrsproxy\.svc$/	All
	Nocase	1	Ignore Case	Enabled	All
Autodiscover					
	name	Autodiscover	Rule Name	Autodiscover	ESP Enabled
	matchtype	Regex	Match Type	RegEx	ESP Enabled
	pattern	%2F%5E%5C%2Fautodiscover.%2A%2F	Match String	/^\/autodiscover.*/	ESP Enabled
	Nocase	1	Ignore Case	Enabled	ESP Enabled
ECP					
	name	ECP	Rule Name	ECP	ESP Enabled
	matchtype	Regex	Match Type	RegEx	ESP Enabled
	pattern	%2F%5E%5C%2Fecp.%2A%2F	Match String	/^\/ecp.*/	ESP Enabled
	Nocase	1	Ignore Case	Enabled	ESP Enabled
EWS					
	name	EWS	Rule Name	EWS	ESP Enabled
	matchtype	Regex	Match Type	RegEx	ESP Enabled
	pattern	%2F%5E%5C%2Fews.%2A%2F	Match String	/^\/ews.*/	ESP Enabled

SubVSs	API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
	Nocase	1	Ignore Case	Enabled	ESP Enabled
MAPI					
	name	MAPI	Rule Name	MAPI	ESP Enabled
	matchtype	Regex	Match Type	RegEx	ESP Enabled
	pattern	%2F%5E%5C%2Fmapi.%2A%2F	Match String	/^\/mapi.*/	ESP Enabled
	Nocase	1	Ignore Case	Enabled	ESP Enabled
OAB					
	name	OAB	Rule Name	OAB	ESP Enabled
	matchtype	Regex	Match Type	RegEx	ESP Enabled
	pattern	%2F%5E%5C%2Foab.%2A%2F	Match String	/^\/oab.*/	ESP Enabled
	Nocase	1	Ignore Case	Enabled	ESP Enabled
OWA					
OWA (Content Rule)					
	name	OWA	Rule Name	OWA	ESP Enabled
	matchtype	Regex	Match Type	RegEx	ESP Enabled
	pattern	%2F%5E%5C%2Fowa.%2A%2F	Match String	/^\/owa.*/	ESP Enabled
	Nocase	1	Ignore Case	Enabled	ESP Enabled
Root (Content Rule)					
	name	Root	Rule Name	Root	ESP Enabled
	matchtype	Regex	Match Type	RegEx	ESP Enabled
	pattern	%2F%5E%5C%2F%24%2F	Match String	/^\/$/	ESP Enabled
	Nocase	1	Ignore Case	Enabled	ESP Enabled
PowerShell					
	name	PowerShell	Rule Name	PowerShell	ESP Enabled
	matchtype	Regex	Match Type	RegEx	ESP Enabled

SubVSs	API Parameter	API Value	WUI Field Name	WUI Field Value	Use with Template
	pattern	%2F%5E%5C%2Fpowershell.%2A%2F	Match String	/^\/powershell.*/	ESP Enabled
	Nocase	1	Ignore Case	Enabled	ESP Enabled
RPC					
	name	RPC	Rule Name	RPC	ESP Enabled
	matchtype	Regex	Match Type	RegEx	ESP Enabled
	pattern	%2F%5E%5C%2Frpc.%2A%2F	Match String	/^\/rpc.*/	ESP Enabled
	Nocase	1	Ignore Case	Enabled	ESP Enabled

Note: The **Authentication Proxy** SubVS is only applicable for the **Exchange HTTPS Offload with ESP and WAF** and **Exchange HTTPS re-encrypted with ESP and WAF** Virtual Services.

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 2013 Deployment Guide

Exchange Team Blog post on Load Balancing in Exchange 2016