

Configuring the Clearswift Secure Email Gateway to Work with Microsoft Office 365

Version 3.3

April 2022

Copyright Terms and Conditions

Copyright Help/Systems LLC and its group of companies.

The content in this document is protected by the Copyright Laws of the United States of America and other countries worldwide. The unauthorized use and/or duplication of this material without express and written permission from HelpSystems is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to HelpSystems with appropriate and specific direction to the original content. HelpSystems and its trademarks are properties of the HelpSystems group of companies. All other marks are property of their respective owners.

Contents

Introduction	4
Configure the SEG to Scan Inbound Email Before Routing to Office 365.....	5
Configure the SEG to Scan Outbound Email from Office 365.....	7
Configure the SEG to Detect Spam in an Office 365 Environment	10
Configure an Office 365 Connector to Route Outgoing Email to the SEG	11
Configure an Office 365 Rule to Route Outgoing Email to the SEG.....	15
Configure the SEG to Prevent Relaying Spoofed Email from Office 365	17
Configure Office 365 Connector to Accept Incoming Email from the SEG	19
Configure the SEG for a hybrid environment.....	23
Configure the SEG to Only Send and Receive Messages from Valid Email Addresses in your Domain	24
Configure the SEG to Scan Internal Office 365 Email.....	25
Configure Office 365 to Route Internal Email via the SEG.....	27
Configure the SEG to Detect Malicious URLs in an Office 365 Environment	29
Further Information.....	31

Introduction

This document explains how to integrate the Clearswift Secure Email Gateway (SEG) with Microsoft Office 365 to provide enhanced Adaptive Data Loss Prevention (A-DLP) defenses and complement the Office 365 hygiene components.

There are numerous Office 365 packages suited to different customer requirements. This document is based on the Office 365 Enterprise E3 package which is Microsoft's target platform for mid and larger sized enterprises.

This document assumes that you are familiar with how to configure the SEG. If you would like more information on basic configuration of the SEG, please refer to the online help.

You will need to ensure that any SPF, DKIM, DMARC, etc. records that you have published by your DNS provider will need to be updated to include details of your SEG(s). If your domain is managed by Microsoft, you may need to contact Microsoft directly to get your DNS records updated.

It is recommended that you install a valid TLS certificate on your SEG, as this will allow you to configure a TLS connection between your Office 365 instance and SEG, where you can validate the TLS certificate used by the SEG. You can learn more about configuring TLS on the SEG in this [document](#).

The process for configuring the Clearswift SEG to work properly with Microsoft Office 365 can be broken down into several steps:

- Add *.outbound.protection.outlook.com to Internal Email Servers
- Enable global spam settings
- For each hosted domain, where the SEG will be receiving outbound messages from O365,
 - Configure O365 to add the access token
 - Wait for any messages already in the queue to go through
 - Configure the access token for that domain in the SEG

Failure to perform these steps may leave you with a Gateway that permits other O365 tenants to use your Gateway for routing and also means that inbound mail from other O365 tenants are not checked for spam.

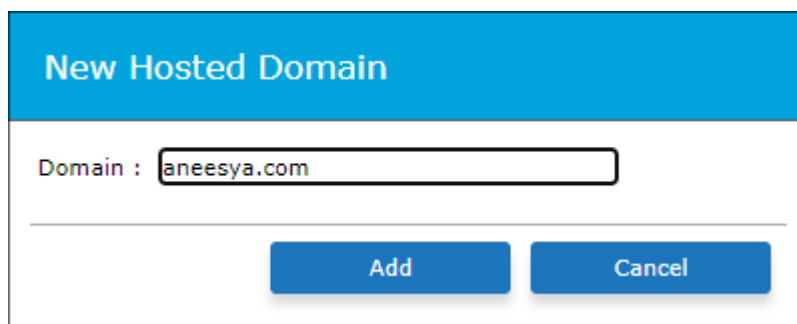
Configure the SEG to Scan Inbound Email Before Routing to Office 365

In this scenario your organization should ensure that your DNS MX records are directed to your SEG server(s).

The SEG(s) will then process emails according to policy and valid messages will be routed to your organization's Office 365 deployment.


To configure the SEG to accept messages for your organization's domain and route traffic to your Office 365 instance:

1. In the Clearswift Secure Email Gateway user interface, click on the **System > SMTP Settings > Mail Domains and Routing**.
2. In the **Hosted Domains** tab, click on **New**.
3. In the **New Hosted Domain** dialog, enter your organization's email domain (e.g. aneesya.com) into the **Domain** field and click on **Add**.



4. In the **Email Routing** tab, click on **New**.
5. In the **Add Email Route** dialog:
 - a. Enter your organization's email domain (e.g. aneesya.com) into the **Domain** field.
 - b. Select the **To a server** radio button.
 - c. Enter the Host Name for your organization's Office 365 deployment (this can be obtained from your Office 365 portal, under Domains and the Domain Settings for the relevant domain, e.g. aneesya-com.mail.protection.outlook.com) in the **Server** field.
 - d. The value in the **Port** field should be 25.
 - e. Ensure that the **TLS** drop down is set to none (you can enable mandatory TLS later if you wish, please refer to the Help documentation).
 - i. It is recommended that you enable opportunistic TLS under **System > Encryption > TLS Configuration** as a minimum when communicating between Office 365 and your SEG(s).
 - f. Ensure that the **Authentication** drop down is set to **None**.
 - g. Click on **Add**.

Add Email Route

 Authentication is not enabled.
Global TLS is disabled.

Domain :

Route : Using DNS
 To a server
 To an MTA group

Server :

Port :

Use the outbound TLS configuration from this connection profile :

TLS :

Use these authentication settings when connecting to the email server :

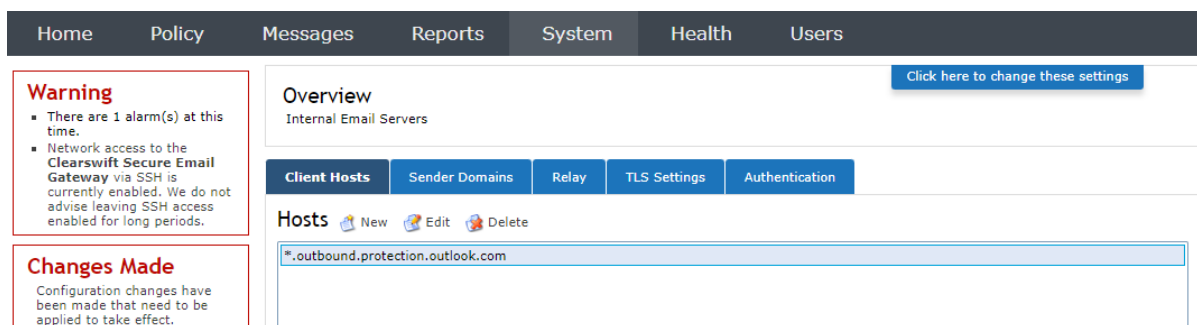
Authentication :

Configure the SEG to Scan Outbound Email from Office 365

You now need to configure your SEG to allow Office 365 to send messages through your SEG. You can do this by adding *.outbound.protection.outlook.com as a Client Host under your Internal Email Servers Connection. This then treats any servers that have hostnames ending with outbound.protection.outlook.com as an internal email server. This is necessary, because your emails originating from Office 365 can be sent from any one of thousands of mail servers.

To do this:

1. In the Clearswift Secure Email Gateway user interface, click on the **System > SMTP Settings > Connections**.
2. Select the **Internal Email Servers** entry and then click on **Edit**.
3. In the **Client Hosts** tab, click on **New**.
4. In the **New Client Host** dialog:
 - a. Enter the following in the **Host** field: *.outbound.protection.outlook.com
 - b. Click on **Add**.



The screenshot shows the Clearswift Secure Email Gateway user interface. The top navigation bar includes Home, Policy, Messages, Reports, System, Health, and Users. The main content area is titled "Overview" and "Internal Email Servers". There is a "Warning" box on the left stating "There are 1 alarm(s) at this time." and "Network access to the Clearswift Secure Email Gateway via SSH is currently enabled. We do not advise leaving SSH access enabled for long periods." Below the warning is a "Changes Made" box stating "Configuration changes have been made that need to be applied to take effect." The main content area has a "Client Hosts" tab selected, with sub-tabs for "Sender Domains", "Relay", "TLS Settings", and "Authentication". The "Hosts" section shows a list of hosts with a "New" button and "Edit" and "Delete" icons. The host list contains one entry: "*.outbound.protection.outlook.com". A button "Click here to change these settings" is located in the top right corner of the main content area.

It is recommended that you configure mandatory TLS between the SEG and Office 365.

To do this:

1. In the Clearswift Secure Email Gateway user interface, click on the **System > SMTP Settings > Connections**.
2. Select the **Internal Email Servers** entry and then click on **Edit**.
3. Click on the **TLS Settings** tab.

4. Configure the **Outbound (When Acting as a Client)** section as follows:
 - a. Select the **Use Mandatory TLS for this connection profile** check box.
 - b. Select the **Use global settings (TLS 1.2)** check box.
 - c. Select the **Use global settings (Medium)** check box.
 - d. Ensure the **No validation** radio button is selected.
 - e. Click on **Save**.

Outbound (When Acting as a Client)

Use Mandatory TLS for this connection profile

Supported protocols
TLS versions in use for communication:

Use global settings (TLS 1.2)

1.0 - (Not recommended).

1.1 - (Recommended only if 1.2 connections are not possible).

1.2 - (Recommended).

Minimum cipher strength
TLS communication will use at least the following cipher strength :

Use global settings (Medium)

High

Medium

Any

Server certificate validation

No validation

Validate the receiving server certificate SAN/CN

Validation requires SAN/CN to match:

5. Configure the **Inbound (When Acting as a Server)** section as follows:
 - a. Select the **Require valid client certificate** check box.
 - b. Click on **Save**.

Inbound (When Acting as a Server)

Use Mandatory TLS for this connection profile

Encryption strength
Encryption should meet or exceed : bits

Client certificate validation

Require valid client certificate:

(Leave blank to indicate the hostname of the client)


CN of the certificate must match the following field :

CN of the certificate issuer must match the following field :

6. Click on the **System > SMTP Settings > Mail Domains and Routing**.
7. Click on the **Email Routing** tab.
8. Use the check box to select the entry for your organization's email domain that you created earlier and then click on **Edit**.

9. In the **Edit Email Route** dialog:
 - a. Use the TLS drop down to select: **Internal Email Servers**
 - b. Click on **Update**.

Edit Email Route

 Authentication is not enabled.
Using mandatory TLS from selected connection profile.

Domain :

Route : Using DNS
 To a server
 To an MTA group

Server :

Port :

Use the outbound TLS configuration from this connection profile :

TLS :

Use these authentication settings when connecting to the email server :

Authentication :

Please note that for security reasons, Office 365 certificates do change from time to time, so you should consult Microsoft documentation to obtain the current certificate details:
<https://docs.microsoft.com/en-us/office365/securitycompliance/exchange-online-uses-tls-to-secure-email-connections>

Configure the SEG to Detect Spam in an Office 365 Environment

If using SEG's Office 365 integration you should only enable DMARC, DKIM, Junk Mail and Spoof detection. The other spam detection techniques must not be enabled.

Spam Policy [Click here to change these settings](#)

Every external gateway that connects to your **Email Gateway** will be given a reputation rating by TRUSTmanager that is covered by the four bandings below. You now have the opportunity to configure the behavior based on this reputation rating.

TRUSTmanager Reputation Rating

Good	Neutral	Suspicious	Bad
Green	Yellow	Orange	Purple

If Reputation Good Disabled [G N S B] | **If Reputation Bad** Disabled [G N S B] | **Real-time IP Blocklist** Disabled [G N S B]

Spoof Detection Hold in area [G N S B] | **Validate Sender Domain** Disabled [G N S B] | **BATV Address Validation** Disabled [G N S B]

DMARC Reject Reject [G N S B] | **DMARC Quarantine** Hold in area [G N S B] | **SPF Hard Fail** Disabled [G N S B]

SPF Soft Fail Disabled [G N S B] | **DKIM Hard Fail** Hold in area [G N S B] | **DKIM Soft Fail** Disabled [G N S B]

Greylisting Disabled [G N S B] | **Confirmed Junk Email** Hold in area [G N S B] | **Suspected Junk Email** Hold in area [G N S B]

For more information on configuring Spam detection, please see the Online Help.

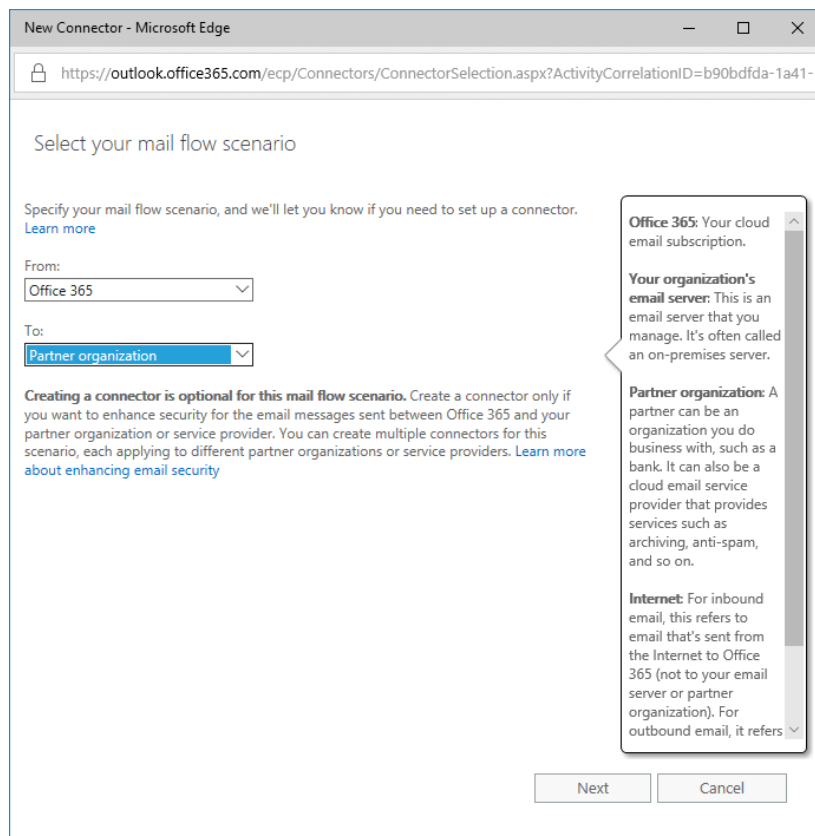
Note: It is important to enable Spoof detection to allow detection of rogue O365 tenants trying to send mail through your SEG and pretending to be your organization.

Configure an Office 365 Connector to Route Outgoing Email to the SEG

The next step is to reconfigure your organization's Office 365 portal to redirect all outbound email to the SEG server(s). You should begin by creating a new connector to route emails from your Office 365 deployment to the SEG server(s).

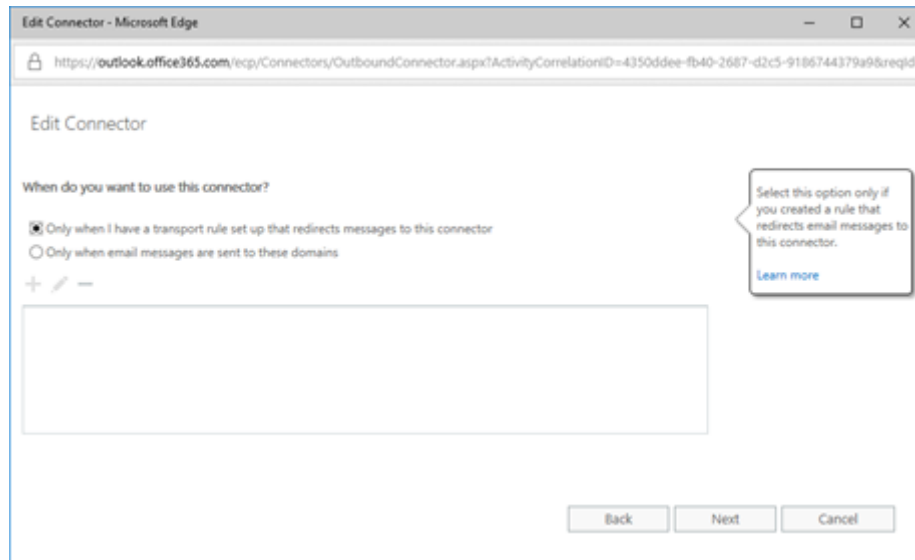
To do this:

1. In your organization's Office 365 instance, click on **Admin centers, Exchange**.
2. Click on **mail flow**.
3. Click on **connectors**.
4. In the connectors section, click on **+**.
5. In the Select your mail flow scenario dialog:
 - a. Use the From drop down to select **Office 365**.
 - b. Use the To drop down to select **Partner organization**.
 - c. Click on **Next**.

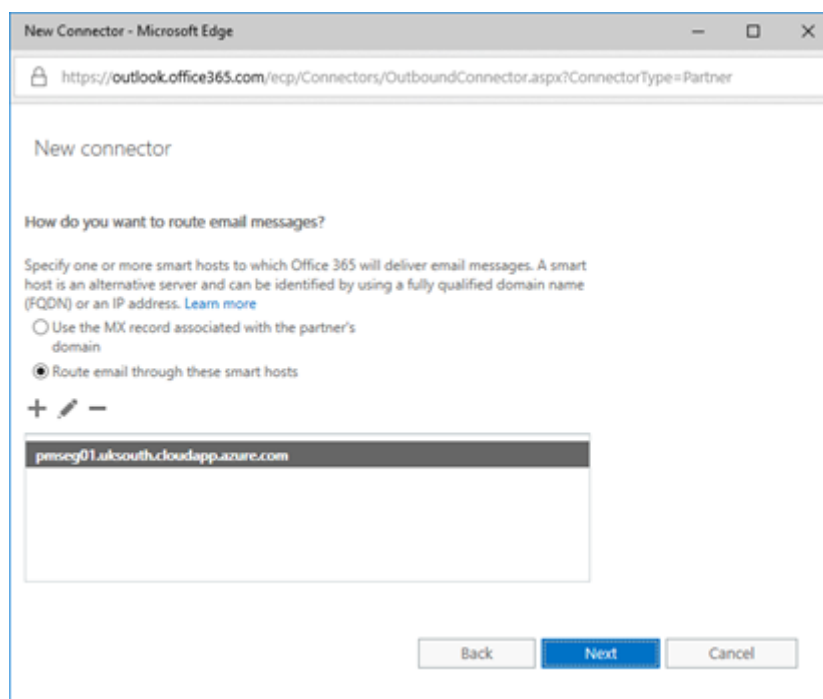


6. In the New connector dialog:
 - a. Enter a name for the connector.
 - b. Enter a description.
 - c. Ensure that the **Turn it on** check box is selected.
 - d. Click on **Next**.

7. In the When do you want to use this connector? dialog:
 - a. Select the **Only when I have a transport rule set up that redirects messages to this connector** radio button.
 - b. Click on **Next**.



8. In the How do you want to route email messages? dialog:
 - a. Select the **Route email through these smart hosts** radio button.
 - b. Select **+**.
 - c. In the add smart host dialog, enter the IP address/hostname of the SEG and then click on **Save**.
 - d. Repeat for any additional SEGs.
 - e. Click on **Next**.



9. In the How should Office 365 connect to your partner organization's email server? dialog:
 - a. Specify if a mandatory TLS connection should be used and the appropriate settings (it is recommended to at least use the default settings and you should consider validating against the certificate used by the SEG).
 - b. Click on **Next**.

New Connector - Microsoft Edge

https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=Partner

New connector

How should Office 365 connect to your partner organization's email server?

Always use Transport Layer Security (TLS) to secure the connection (recommended)

Connect only if the recipient's email server certificate matches this criteria

Any digital certificate, including self-signed certificates

Issued by a trusted certificate authority (CA)

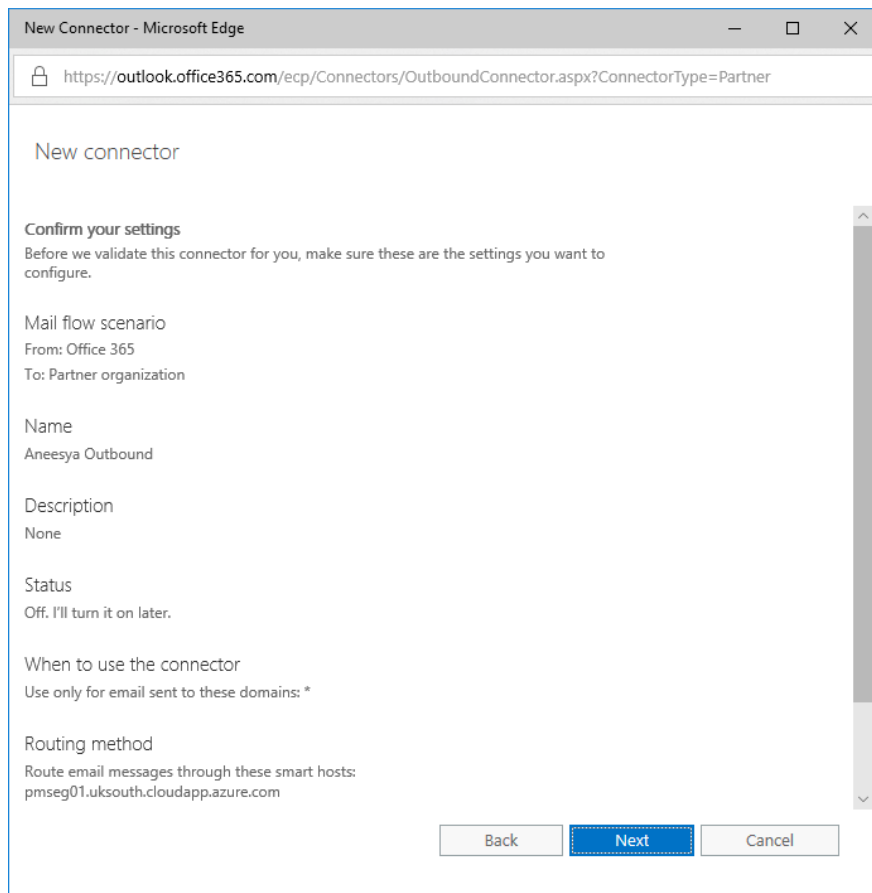
And the subject name or subject alternative name (SAN) matches this domain name:

Example: contoso.com or *.contoso.com

TLS is a security protocol that helps to encrypt and deliver email messages securely so no one except the sender and recipient can access or tamper with the message. If you select this option, messages will be rejected if the TLS connection isn't successful.

Back Next Cancel

10. In the Confirm your settings dialog, click on **Next**.



11. In the Validate this connector dialog, enter one or more email addresses to send the validation message to and then click on **Validate**.

12. Click on **Close**.

13. Click on **Save**.

You now have a connector configured to route messages from Office 365 via the Secure Email Gateway.

Configure an Office 365 Rule to Route Outgoing Email to the SEG

The next step is to configure your organization's Office 365 portal to route emails to the SEG server(s) for scanning via the new connector.

To do this:

1. In your organization's Office 365 instance, click on **Admin centers, Exchange**.
2. Click on **mail flow**.
3. Click on **rules**.
4. In the rules section, click on **+, Create a new rule...**
5. In the new rule dialog:
 - a. Enter a name for the rule.
 - b. Click on **More options...**
 - c. Use the Apply this rule if... drop down to select **The sender..., is external/internal**.
 - d. In the select sender location dialog:
 - i. Use the drop down to select **Inside the organization**.
 - ii. Click on **OK**.
 - e. Click on **add condition**.
 - f. Use the Apply this rule if...and drop down to select **The recipient..., is external/internal**.
 - g. In the select recipient location dialog:
 - i. Use the drop down to select **Outside the organization**.
 - ii. Click on **OK**.
 - h. Use the Do the following... drop down to select **Modify the message properties..., set a message header**.
 - i. Click on the Set the message header ***Enter text...** link.
 - j. In the message header dialog:
 - i. Enter **X-Clearswift-M365** as the name for the message header.
 - ii. Click on **OK**.
 - k. Click on the to the value ***Enter text...** link.
 - l. In the header value dialog:
 - i. Enter the Access Token for the message header. This can be any alphanumeric string but for security we recommend using a GUID either generated online or via PowerShell. It is also possible to use the Gateway UI to create it. See [Error! Not a valid bookmark self-reference..](#)
 - ii. Click on **OK**.
 - m. Click on **add action**.
 - n. Use the Do the following...and drop down to select **Redirect the message to..., the following connector**.
 - o. In the select connector dialog:
 - i. Use the Connector drop down to select the outbound Office 365 to partner organization connector that you created earlier (e.g. **Office 365 to Azure SEG**).
 - ii. Click on **OK**.
 - p. Click on **Save**.

Add X-Clearswift-M365 header

Name:

*Apply this rule if...

The sender is located... [Inside the organization](#)

and

The recipient is located... [Outside the organization](#)

*Do the following...

Set the message header to this value... Set the message header '[X-Clearswift-M365](#)' to the value '[69fb81b6-a633-423d-ba6d-57150973cfb8](#)'

and

Use the following connector... [Office 365 to Azure SEG](#)

Except if...

Properties of this rule:

Priority:

Configure the SEG to Prevent Relaying Spoofed Email from Office 365

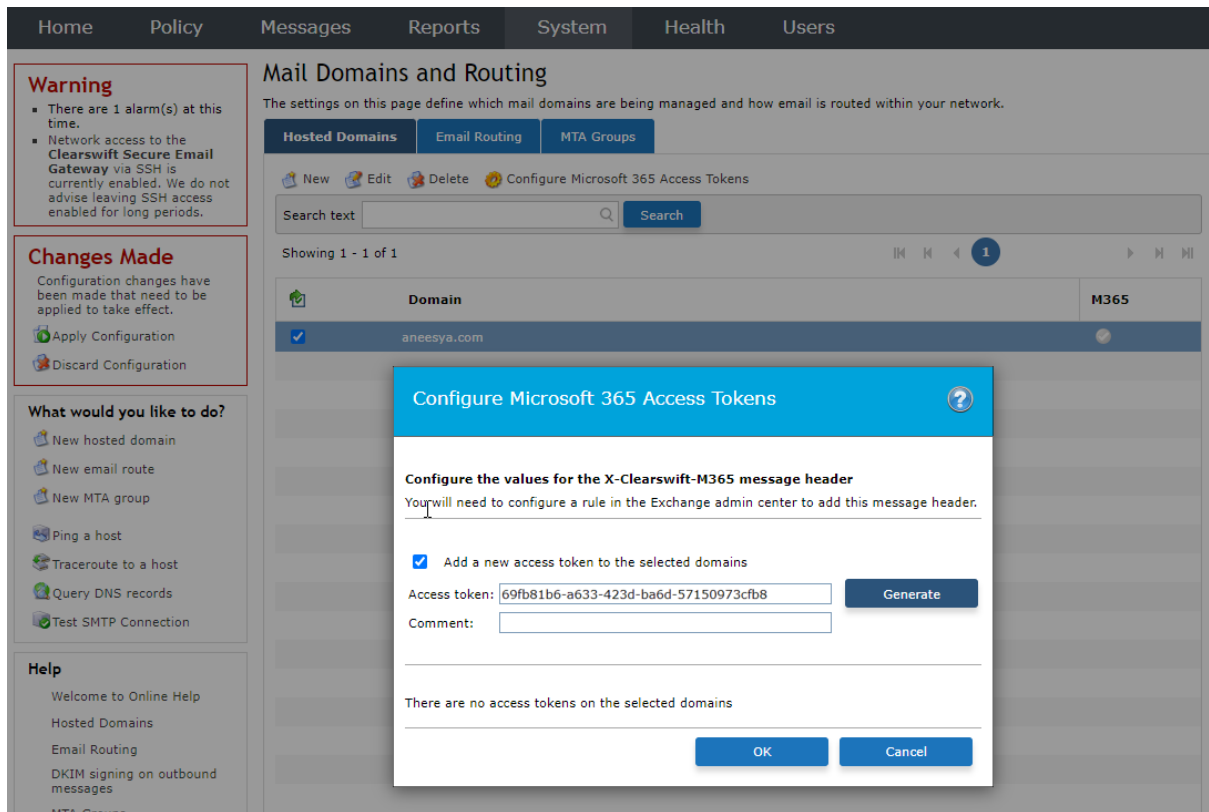
To further limit the ability of third parties to use Office 365 accounts to relay spoofed messages through your SEG it is recommended that you configure Office 365 to add an X-Header to all of the emails that originate from **each of** your domains. You can then configure your SEG to only deliver messages that originate from your email domains and contain the appropriate X-Header value. This will help to address any attempts by third parties to use their own Office 365 account to spoof messages so that they appear to originate from one of your email domains.

The "[Configure an Office 365 Rule to Route Outgoing Email to the SEG](#)" section of this guide will take you through the steps to configure Office 365 to add an X-Header containing a specific value to any emails originating from one of your domains. Please note that you should not apply this policy change to your SEG(s) until you have completed the steps in the "[Configure an Office 365 Rule to Route Outgoing Email to the SEG](#)" section.

In this step, you will configure the SEG to scan for that X-Header and the correct value.

To do this:

1. In the Clearswift Secure Email Gateway user interface, click on the **System > Mail Domains and Routing**.
2. Select your own domains.
3. Click on **Configure Microsoft 365 Access Tokens**.
4. In the **Configure Microsoft 365 Access Tokens** dialog, select the **Add a new access token to the selected domains** check box.
5. In the **Access token** field, you can enter the string used in l.i
6. In the **Comment** field, you can enter an optional description.
7. Click on **OK**.



Note:

The X-header is stripped after processing to ensure that the details of the access token is not exposed externally

It is possible to define multiple Access Tokens per domain.

It is also necessary that the Global Spoof Detection option is enabled in the Spam Policy to hold/reject attempts to send through your Gateway using your domain name.

Configure Office 365 Connector to Accept Incoming Email from the SEG

The next step is to reconfigure your organization's Office 365 portal to accept inbound email from the SEG server(s). This is strictly only necessary if you wish to enforce TLS on this connection.

To do this:

1. In your organization's Office 365 instance, click on **Admin centers, Exchange**.
2. Click on **mail flow**.
3. Click on **connectors**.
4. In the connectors section, click on **+**.
5. In the Select your mail flow scenario dialog:
 - a. Use the From drop down to select **Partner organization**.
 - b. Use the To drop down to select **Office 365**.
 - c. Click on **Next**.

New Connector - Microsoft Edge

https://outlook.office365.com/ecp/Connectors/ConnectorSelection.aspx?ActivityCorrelationID=3e1a59b6-af6c-9

Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.
[Learn more](#)

From:
Partner organization

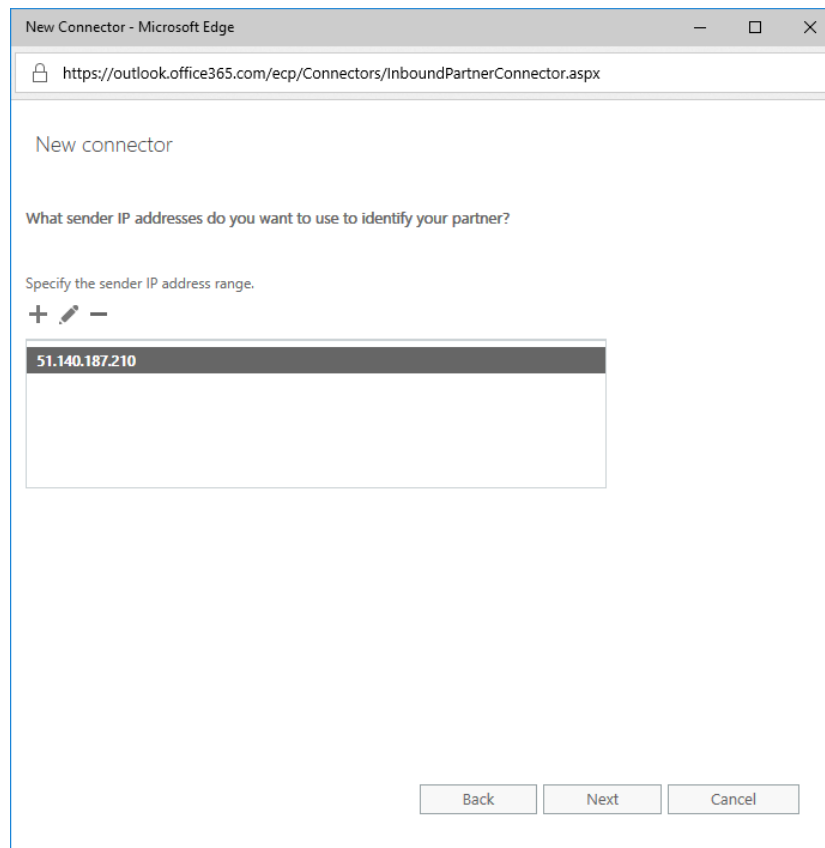
To:
Office 365

Creating a connector is optional for this mail flow scenario. Create a connector only if you want to enhance security for the email messages sent between your partner organization or service provider and Office 365. You can create multiple connectors for this scenario, each applying to different partner organizations or service providers. [Learn more about enhancing email security](#)

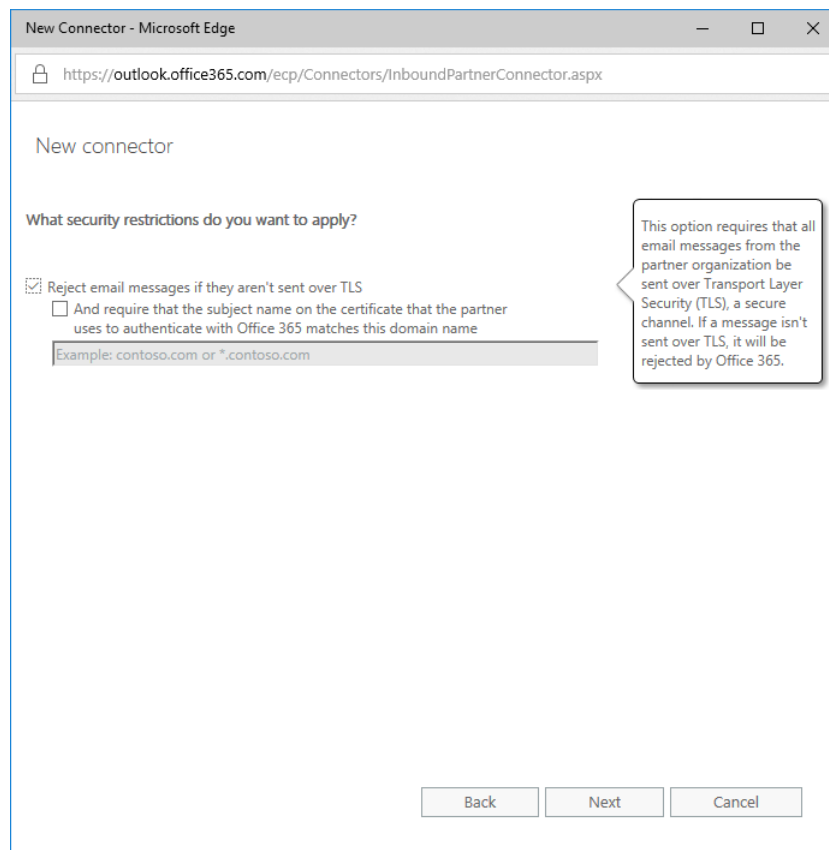
Next Cancel

6. In the New connector dialog:
 - a. Enter a name for the connector.
 - b. Enter a description.
 - c. Ensure that the **Turn it on** check box is selected.
 - d. Click on **Next**.

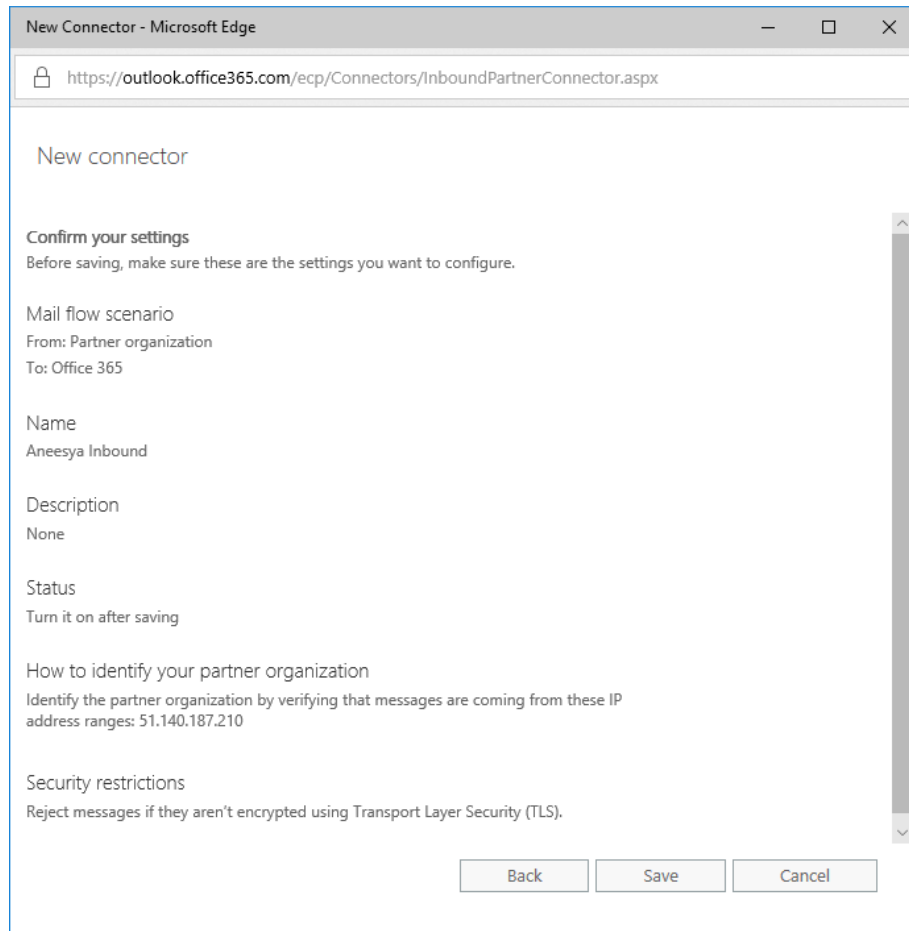
7. In the How do you want to identify the partner organization? dialog:
 - a. Select the **Use the sender's IP address** radio button.
 - b. Click on **Next**.
8. In the What sender IP addresses do you want to use to identify your partner? dialog:
 - a. Select **+**.
 - b. In the add ip address dialog, enter the IP address of the SEG and then click on **OK**.
 - c. Repeat for any additional SEGs.
 - d. Click on **Next**.



9. In the What security restrictions do you want to apply? dialog:
 - a. Specify if a mandatory TLS connection should be used and the appropriate settings (it is recommended to at least use the default settings and you should consider validating against the certificate used by the SEG).
 - b. Click on **Next**.



10. In the Confirm your settings dialog, click on **Next**.



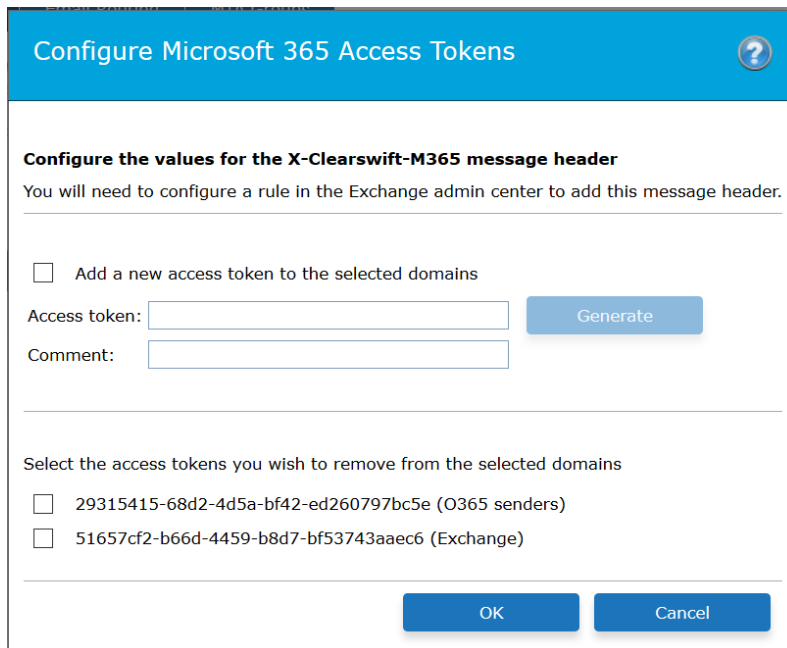
You should now be able to receive messages securely in Office 365 via the Secure Email Gateway.


Configure the SEG for a hybrid environment

If you have a hybrid environment where email can be sent out via O365 or Exchange using the same email domain you should use add the **X-Clearswift-M365** token across each channel.

For separation you can define multiple tokens for each domain you host, and the SEG can be configured for each

For example:



Configure Microsoft 365 Access Tokens 

Configure the values for the X-Clearswift-M365 message header
You will need to configure a rule in the Exchange admin center to add this message header.

Add a new access token to the selected domains

Access token:

Comment:

Select the access tokens you wish to remove from the selected domains

29315415-68d2-4d5a-bf42-ed260797bc5e (O365 senders)

51657cf2-b66d-4459-b8d7-bf53743aaec6 (Exchange)

Configure the SEG to Only Send and Receive Messages from Valid Email Addresses in your Domain

To limit the ability of third parties to use Office 365 accounts to relay spoofed messages through your SEG it is recommended that you replace the standard My Company address list on the SEG with one that contains only valid email addresses within your organization.

To do this:

1. In the Clearswift Secure Email Gateway user interface, click on the **Policy > Policy References > Email Addresses**.
2. Create a My Company (Valid Addresses) address list by performing one of the following:
 - a. Edit the My Company address list to contain all of your organization's valid email addresses and remove any wildcarded entries (e.g. *@aneesya.com).
 - b. Create a new **LDAP Synchronized Address List** that will query your directory server for all of the valid email addresses in your organization.
3. Click on the **Policy > Mail Policy Routes**.
4. Replace all instances of the My Company address list with the newly created My Company (Valid Addresses) list.

Warning

- There are 1 alarm(s) at this time.
- Network access to the Clearswift Secure Email Gateway via SSH is currently enabled. We do not advise leaving SSH access enabled for long periods.

Changes Made

Configuration changes have been made that need to be applied to take effect.

[Apply Configuration](#)

[Discard Configuration](#)

Manage Policy Routes

Using this page you should create the routes that describe the ways users within your organization communicate. For each route you will need to supply a default action and order the content rules that should be performed.

[New](#) [Identify](#) Show Route Selectors Show rules

3 Routes defined (applied in the order shown)

	Action	From	To	Rules
1. <input type="checkbox"/>	Deliver the message	My Company (Valid Addresses) Empty Senders	Anyone	18
2. <input type="checkbox"/>	Deliver the message	Anyone	My Company (Valid Addresses)	21
3. <input type="checkbox"/>	Drop the message	For all email that does not match another route		

You have now limited the ability of third parties to relay emails through your SEG(s) from inside Office 365.

Configure the SEG to Scan Internal Office 365 Email

It is possible to route your internal Office 365 emails via the SEG in order to enforce an internal email security and A-DLP policy.

If you wish to do this, the first step is to configure your SEG to allow Office 365 to send internal emails through your SEG. You will need to create an internal My Company (Valid Addresses) to My Company (Valid Addresses) policy route.

To do this:

1. In the Clearswift Secure Email Gateway user interface, click on the **Policy > Manage Policy Definition > Mail Policy Routes**.
2. Click on **New**.
3. In the **For Mail Sent** section, click on **New**.
4. In the **Add Route Selector** dialog:
 - a. In the **From** section, select the **My Company (Valid Addresses)** check box.
 - b. In the **To** section, select the **My Company (Valid Addresses)** check box.
 - c. Click on **Add**.

Add Route Selector

From :

To :

Anyone

Address Lists

Blocklisted Senders

Employee Monitoring

Empty Senders

HR

Inform Senders

My Company (Valid Addresses)

Valid Recipients

Anyone

Address Lists

Blocklisted Senders

Employee Monitoring

HR

Inform Senders

My Company (Valid Addresses)

Valid Recipients

5. Ensure that the **By Default Perform This Disposal Action** section is set to: **Deliver the message**

By Default Perform This Disposal Action

Deliver the message

[Click here to change these settings](#)

6. Click on the **Policy > Manage Policy Definition > Mail Policy Routes**.
7. Select the **My Company (Valid Addresses)** to **My Company (Valid Addresses)** policy route and move it to the top of the policy route table.

Home
Policy
Messages
Reports
System
Health
Users

Warning

- There are 1 alarm(s) at this time.
- Network access to the Clearswift Secure Email Gateway via SSH is currently enabled. We do not advise leaving SSH access enabled for long periods.

Changes Made

Configuration changes have been made that need to be applied to take effect.

Apply Configuration

Discard Configuration

What would you like to do?

New policy route

Manage Policy Routes

Using this page you should create the routes that describe the ways users within your organization communicate. For each route you will need to supply a default action and order the content rules that should be performed.

New
 Identify

 Show Route Selectors
 Show rules

4 Routes defined (applied in the order shown)

		Action	From	To	Rules
1.	<input type="checkbox"/>	Deliver the message	My Company (Valid Addresses)	My Company (Valid Addresses)	18
2.	<input type="checkbox"/>	Deliver the message	My Company (Valid Addresses) Empty Senders	Anyone	18
3.	<input type="checkbox"/>	Deliver the message	Anyone	My Company (Valid Addresses)	21
4.	<input type="checkbox"/>	Drop the message	For all email that does not match another route		

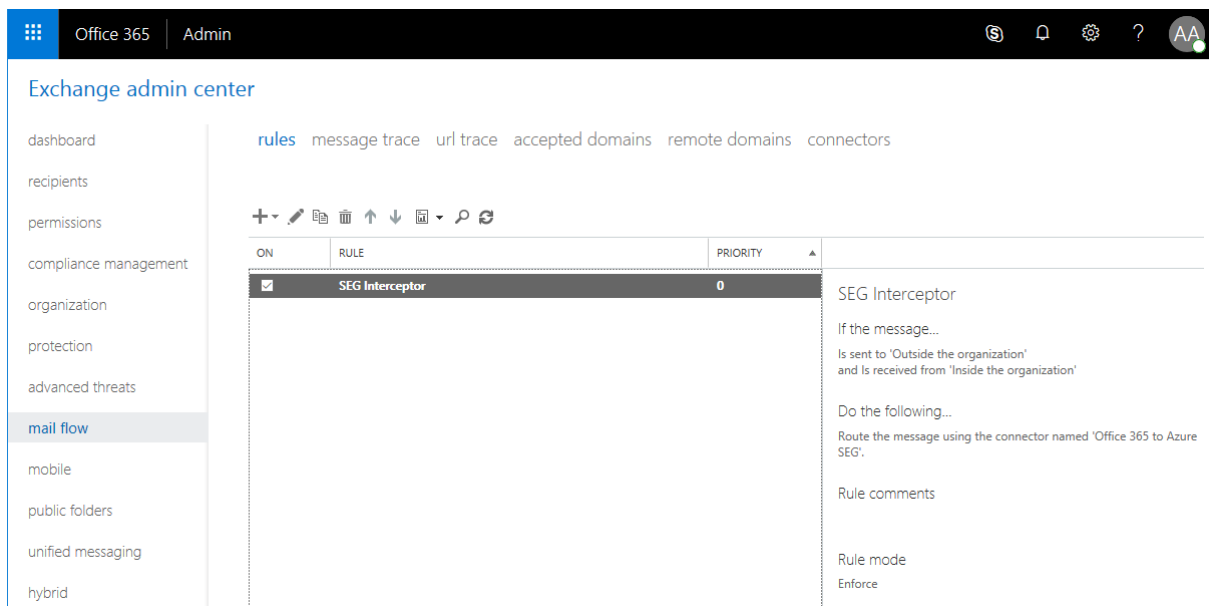
You have now configured your SEG to scan internal Office 365 emails in order to enforce a security and A-DLP policy on them. You can create a more granular policy for incoming, outgoing and internal emails by creating additional policy routes as required.

Configure Office 365 to Route Internal Email via the SEG

The next step is to reconfigure your organization's Office 365 portal to route internal emails to the SEG server(s) for scanning.

To do this:

1. In your organization's Office 365 instance, click on **Admin centers, Exchange**.
2. Click on **mail flow**.
3. Click on **rules**.
4. Select the outbound Office 365 rule that you created earlier (e.g. **SEG Interceptor**) and then click on the **Edit** button (the pencil icon).



5. In the Rule dialog:
 - a. Use **x** to delete the **The recipient is located...Outside the organization** condition.
 - b. Click on **Save**.

The screenshot shows the 'SEG Interceptor' rule configuration dialog. The 'Name' field is 'SEG Interceptor'. Under '*Apply this rule if...', the condition is 'The sender is located...' with a dropdown arrow pointing to 'Inside the organization'. There is an 'add condition' button below. Under '*Do the following...', there are two actions: 1) 'Set the message header to this value...' with a dropdown arrow pointing to 'Set the message header 'X-Clearswift-M365' to the value '69fb81b6-a633-423d-ba6d-57150973cfb8''; 2) 'Use the following connector...' with a dropdown arrow pointing to 'Office 365 to Azure SEG'. There is an 'add action' button below. There is an 'Except if...' section with an 'add exception' button. Under 'Properties of this rule:', the 'Priority' is '0' and the 'Audit this rule with severity level:' checkbox is checked. 'Save' and 'Cancel' buttons are at the bottom right.

You have now configured Office 365 to route internal emails via the SEG in order to enforce an internal email security and A-DLP policy. If you wish to exempt certain internal emails from being routed via the SEG, then you can use the add exception button in the rule that you just amended to exempt the appropriate emails from the rule.

Configure the SEG to Detect Malicious URLs in an Office 365 Environment

As well as detecting Malware and Spam, the SEG can also be configured to detect and block messages that contain malicious URLs.

To do this:

1. In the Clearswift Secure Email Gateway user interface, click on the **Policy > Manage Policy Definition > Mail Policy Routes**.
2. Select route 2, which should be Anyone to My Company.
3. Click on **Edit** which will open the **Modify Policy Route** page.
4. In the **Unless One of These Content Rules Triggers** panel, click on **New**.
5. In the **Add a Content Rule** dialog, click on **Create New** and select **Sanitize Message** and then select **Close**.
6. This will have created a **Sanitize Message** content rule at the bottom of the list of rules.
7. Select this new rule and press **Edit**.
8. In the **What To Look For** panel, click on **Click here to change these settings**.
9. In the **URLs and Hyperlinks**:
 - a. Select **Message subjects**.
 - b. Select **Message bodies**.
 - c. Select **Only the URLs defined in the selected lists**.
 - d. Select both Sophos and MailShell URL list.
 - e. Click **Save**.
10. In the **What To Do** panel, click on **Click here to change these settings**.
11. In the **Disposal Action**, change the **Perform no action** to **Hold in Virus area** and click **Save**.

Overview
Click here to change these settings

Sanitize Message

What To Look For?

In order for this content rule to trigger the test conditions detailed on this panel must be met by the message being processed. If the conditions are met, then the collection of actions described within the **'What to do?'** panel will be carried out.

Which Message Types

Select the message type(s) you wish to apply this content rule to:

All messages

Selected messages

- Virus Outbreak
- Confirmed Phishing
- Suspected Phishing
- Confirmed Spam
- Suspected Spam
- Newsletter

Mode

Select the content rule mode:

Detect only

Detect and sanitize

HTML and RTF Email Bodies

Convert message to plain text

Detect or remove possible threats in email bodies:

- Embedded content (e.g. images, other data)
- Active content (e.g. scripts)
- Links to resources (e.g. links to images, stylesheets)

URLs and Hyperlinks

Detect or sanitize URLs and hyperlinks in:

- Message subjects
- Message bodies

Detect or sanitize the following:

All URLs and hyperlinks

Re-write URLs using the format:

Only the URLs defined in the selected lists:

- Mailshell Real-time Malicious URL List
- Sophos Real-time Malicious URL List

12. Once again, from the **Policy > Manage Policy Definition > Mail Policy Routes**, select the route and click **Edit** to display the **Modify Policy Route** page.

13. In the **Modify Policy Route** page, select the **Sanitize Message** content rule (currently at the bottom of the list) and click the up arrow until the rule is at position 2 in the list.

Further Information

This document explained how to integrate the Clearswift Secure Email Gateway (SEG) with Microsoft Office 365 in order to provide enhanced Adaptive Data Loss Prevention defenses and complement the Office 365 hygiene components.

If you require further assistance, you can refer to the:

- Online Help:
Available through the Clearswift Secure Email Gateway user interface as well as the [HelpSystems Community Portal](#)
- Clearswift Support Portal and Solutions:
<https://www.clearswift.com/support/portals>
- Clearswift Professional Services team:
<https://www.clearswift.com/training-and-support/professional-services>
- Scheduled classroom and webinar training courses:
<https://www.clearswift.com/training-and-support/training-courses>