FORTRA

Configuring Clearswift Secure Email Gateway to work with Microsoft Office 365

(v3.5, November 2024)

Copyright Terms and Conditions

202411040419

Contents

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.

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.

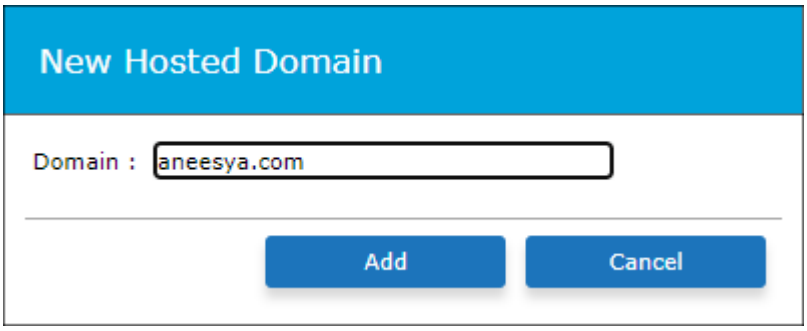
Configure the SEG to Scan Inbound Email Before Routing to Office 365

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

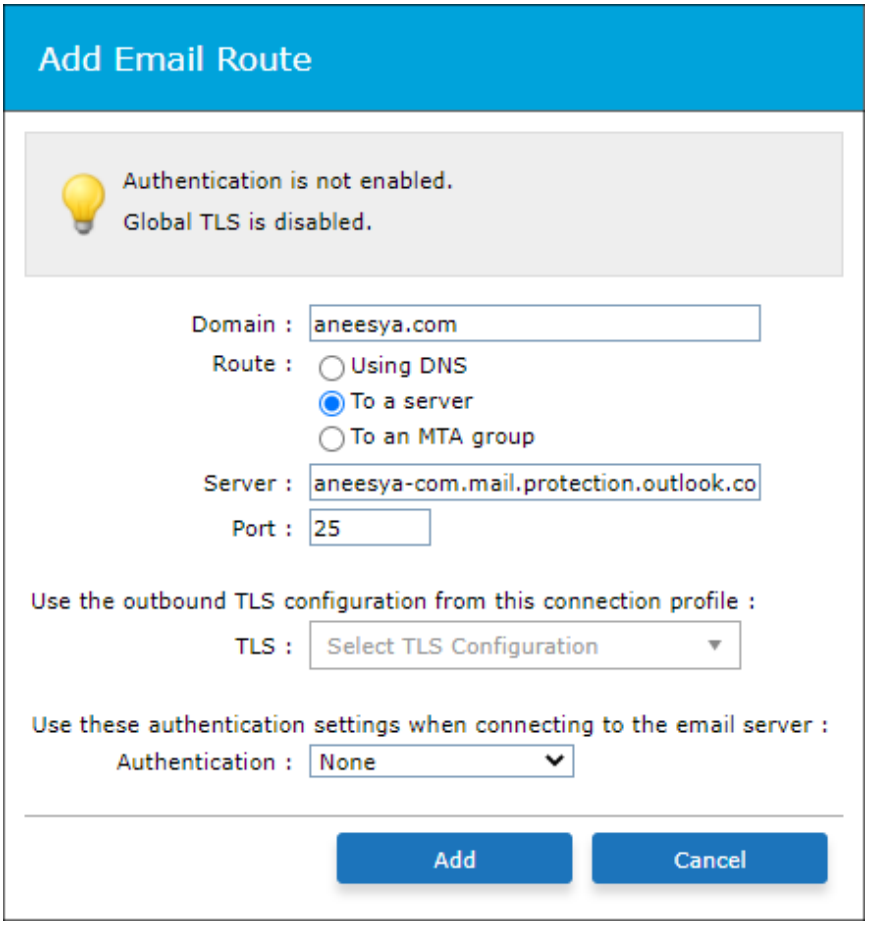
The SEG(s) will then process emails according to policy and valid messages will be routed to your organization's Office 365 deployment.

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**.

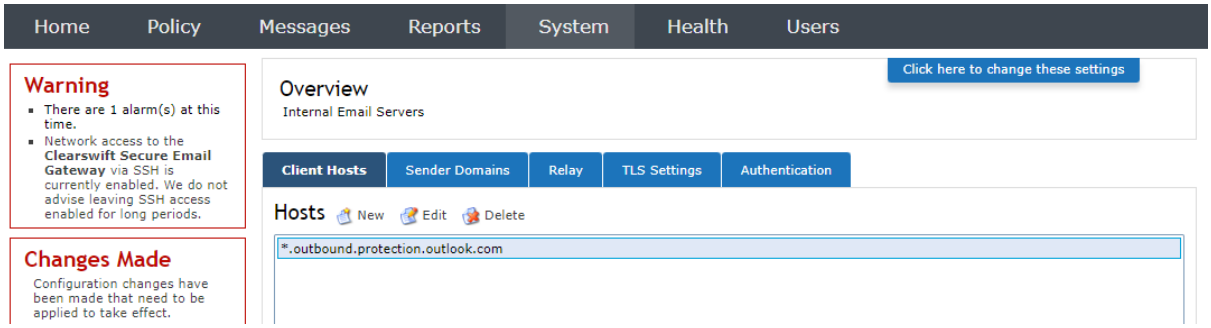

Add Email Route
Authentication is not enabled.
Global TLS is disabled.
Domain :
aneesya.com
Route :
Using DNS
To a server
To an MTA group
Server :
aneesya-com.mail.protection.outlook.co
Port :
25
Use the outbound TLS configuration from this connection profile :
TLS :
Select TLS Configuration
Use these authentication settings when connecting to the email server :
Authentication :
None
Add
Cancel

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**.

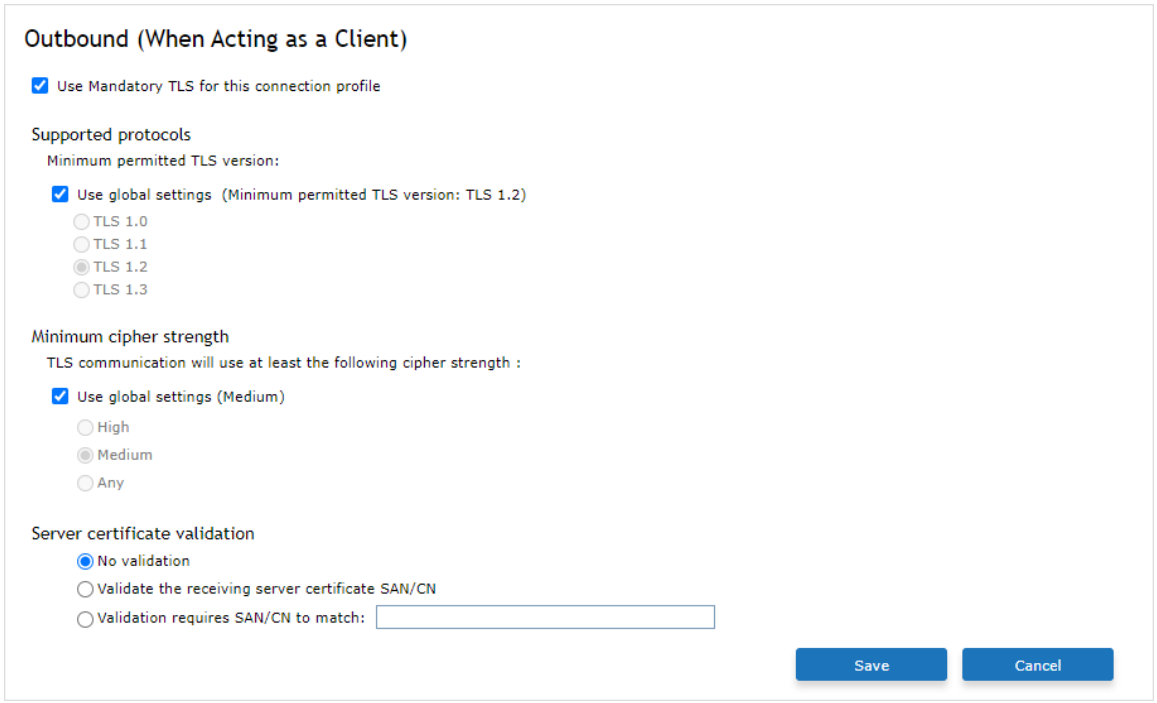


It is recommended that you configure mandatory TLS between the SEG and

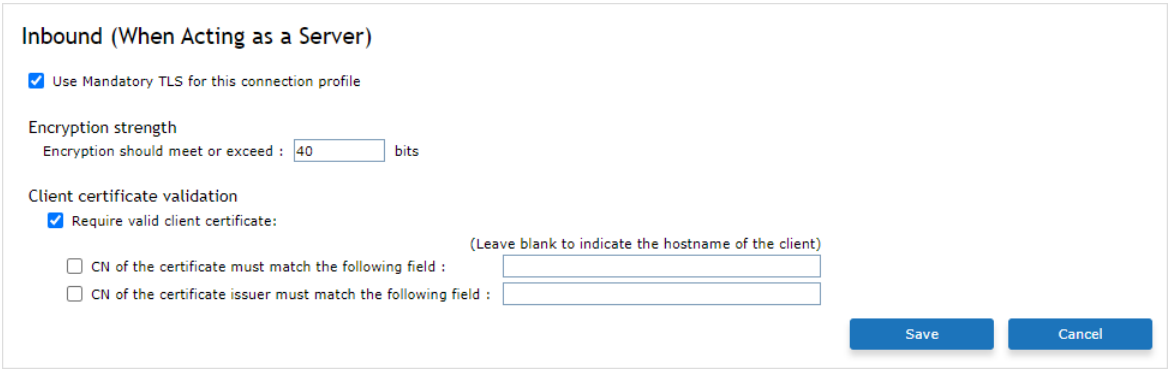
Office 365. To do this:

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.

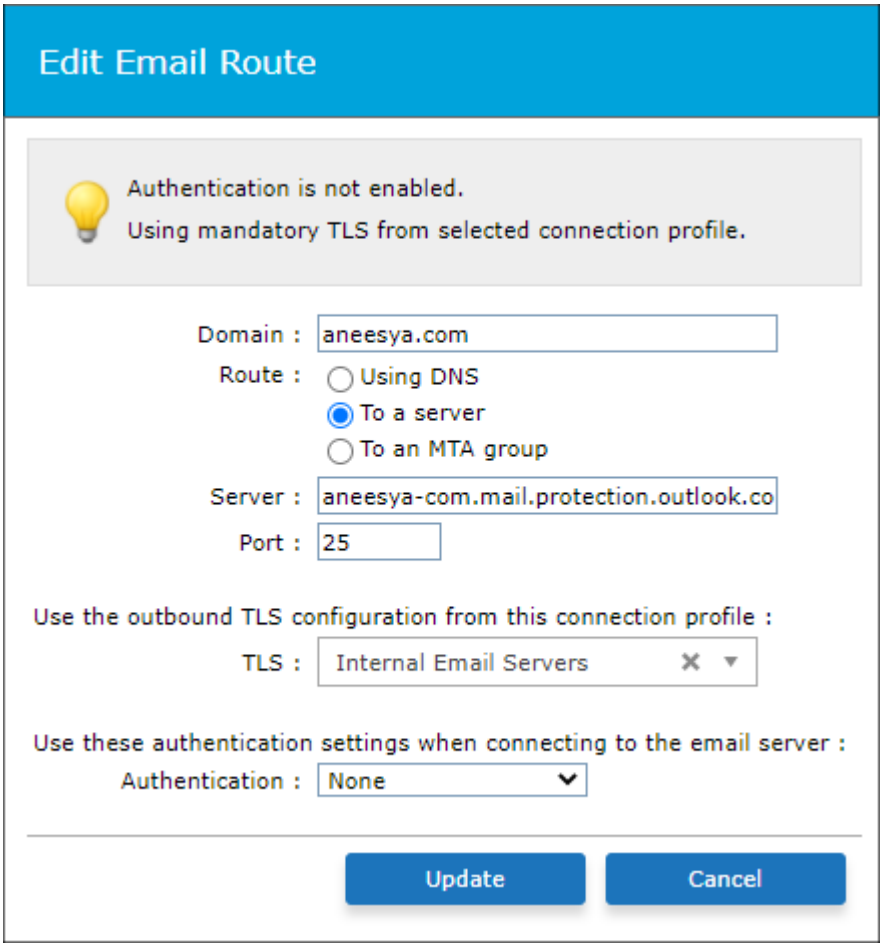
4. Configure the **Outbound (When Acting as a Client)** section as follows:
    a. Select the **Use Mandatory TLS for this connection profile** check box.
    b. Select the **Use global settings (Minimum permitted TLS version: TLS 1.2)** check box.
    c. Select the **Use global settings (Medium)** check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



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**.



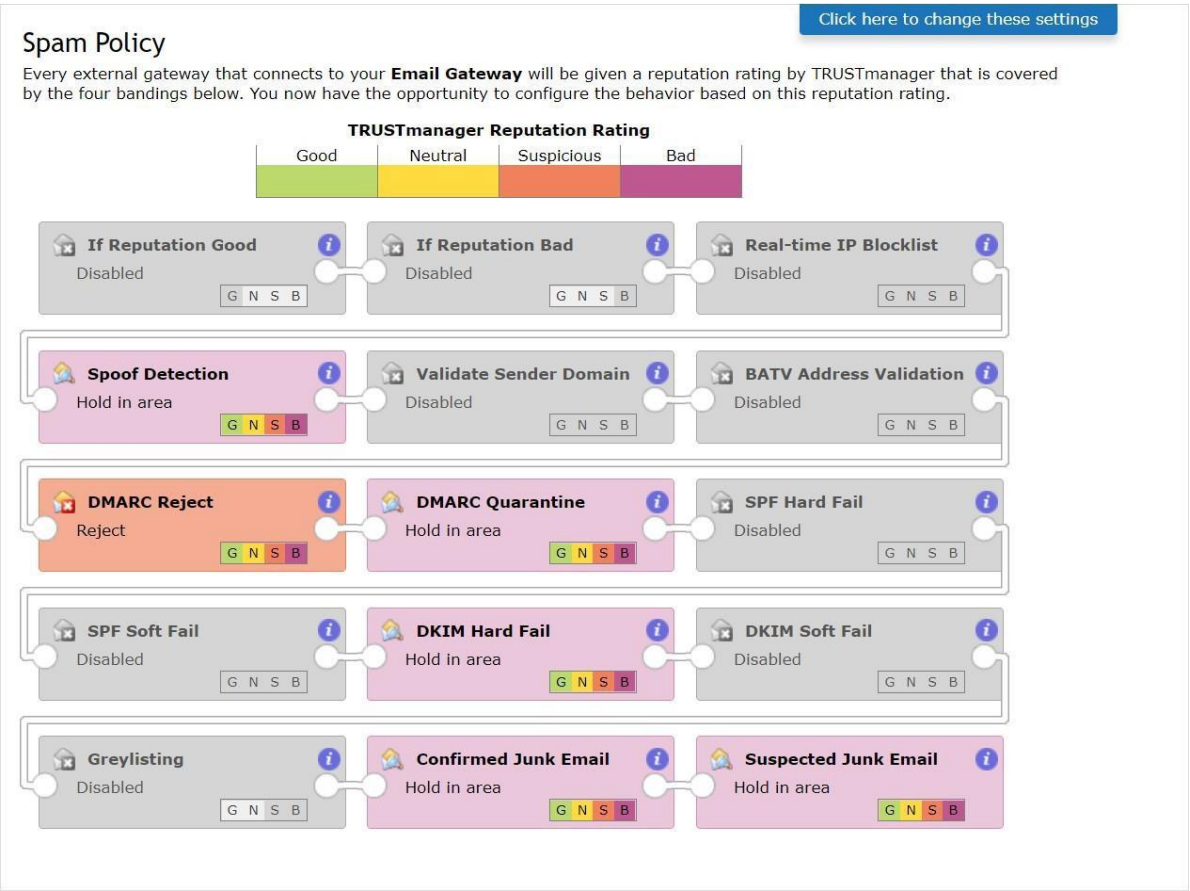
6. Click on the **System** > **SMTP Settings** > **Mail Domains and Routing**.
7. Click on the **Email Routing** tab.
8. Use the check box to select the entry for your organization's email domain that you created earlier and then click on **Edit**.
9. In the **Edit Email Route** dialog:
    a. Use the TLS drop down to select: **Internal Email Servers**
    b. Click on **Update**.



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.



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

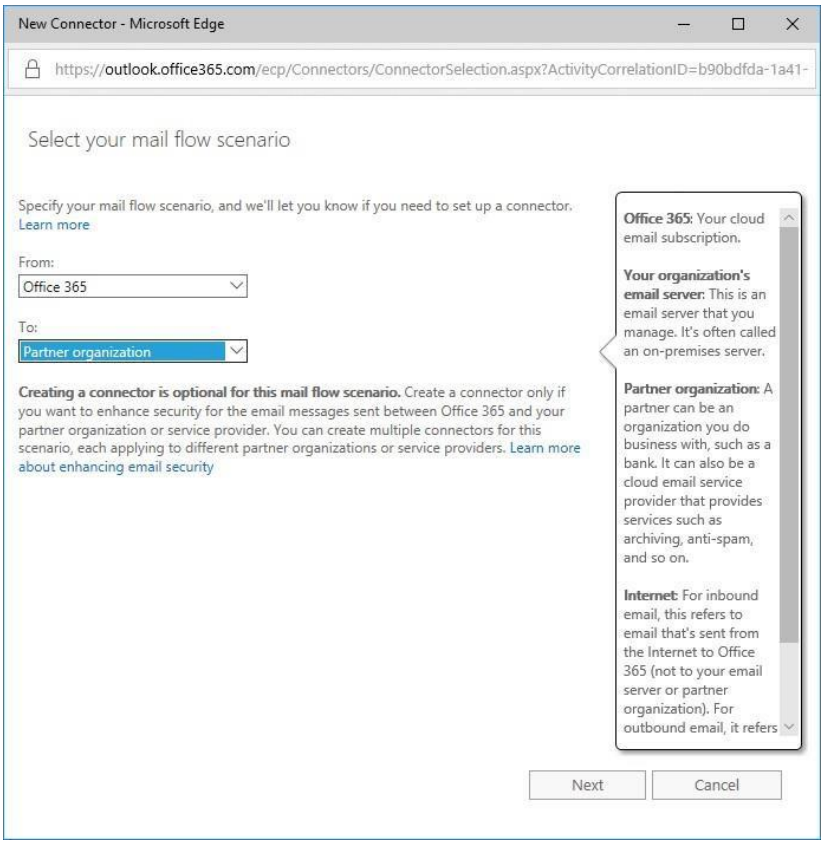
Note: It is important to enable Spoof detection to allow detection of rogue O365 tenants trying to send mail through your SEG and pretending to be your organization.

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).

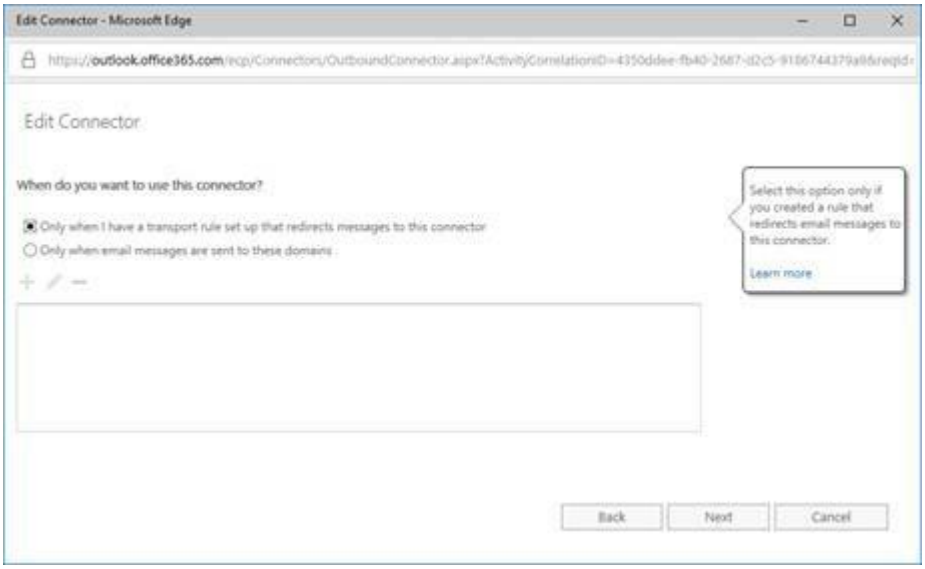
To do this:

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**.

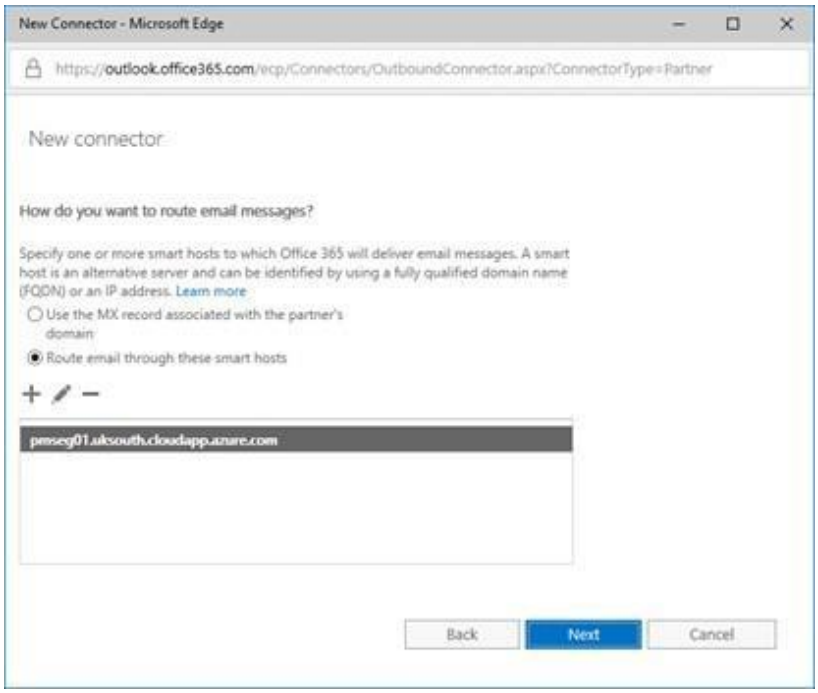


6. In the New connector dialog:
    a. Enter a name for the connector.
    b. Enter a description.
    c. Ensure that the **Turn it on** check box is selected.
    d. Click on **Next**.

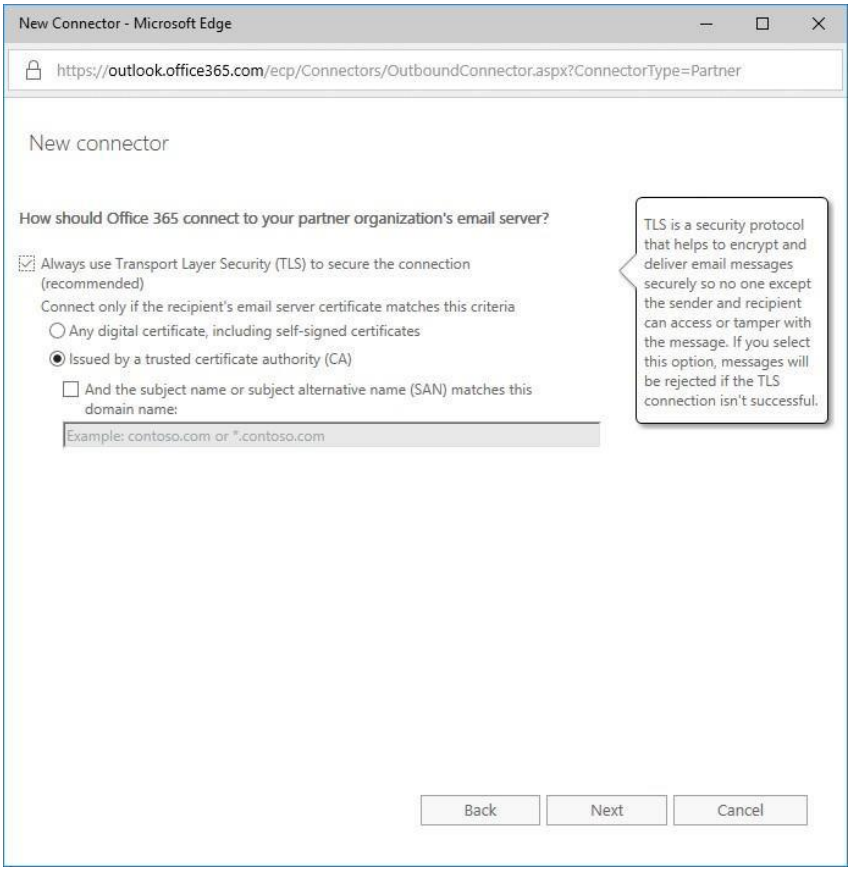
7. In the When do you want to use this connector? dialog:
    a. Select the **Only when I have a transport rule set up that redirects messages to this connector** radio button.
    b. Click on **Next**.



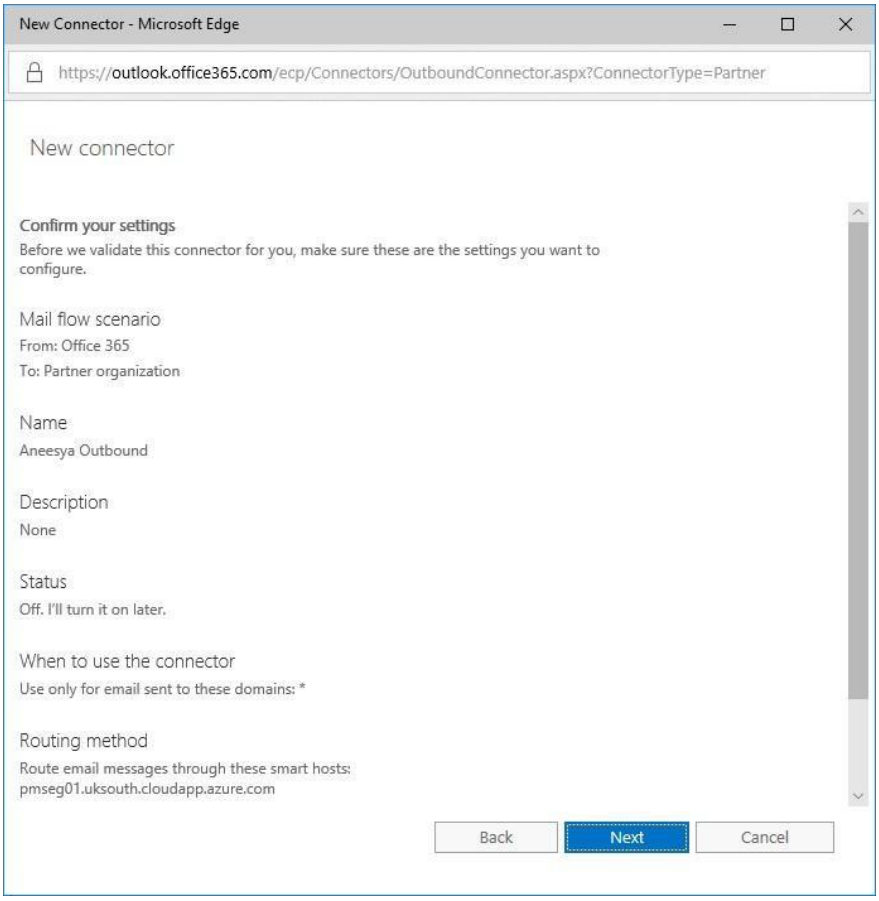
8. In the How do you want to route email messages? dialog:
    a. Select the **Route email through these smart hosts** radio button.
    b. Select **+**.
    c. In the add smart host dialog, enter the IP address/hostname of the SEG and then click on **Save**.
    d. Repeat for any additional SEGs.
 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



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**.

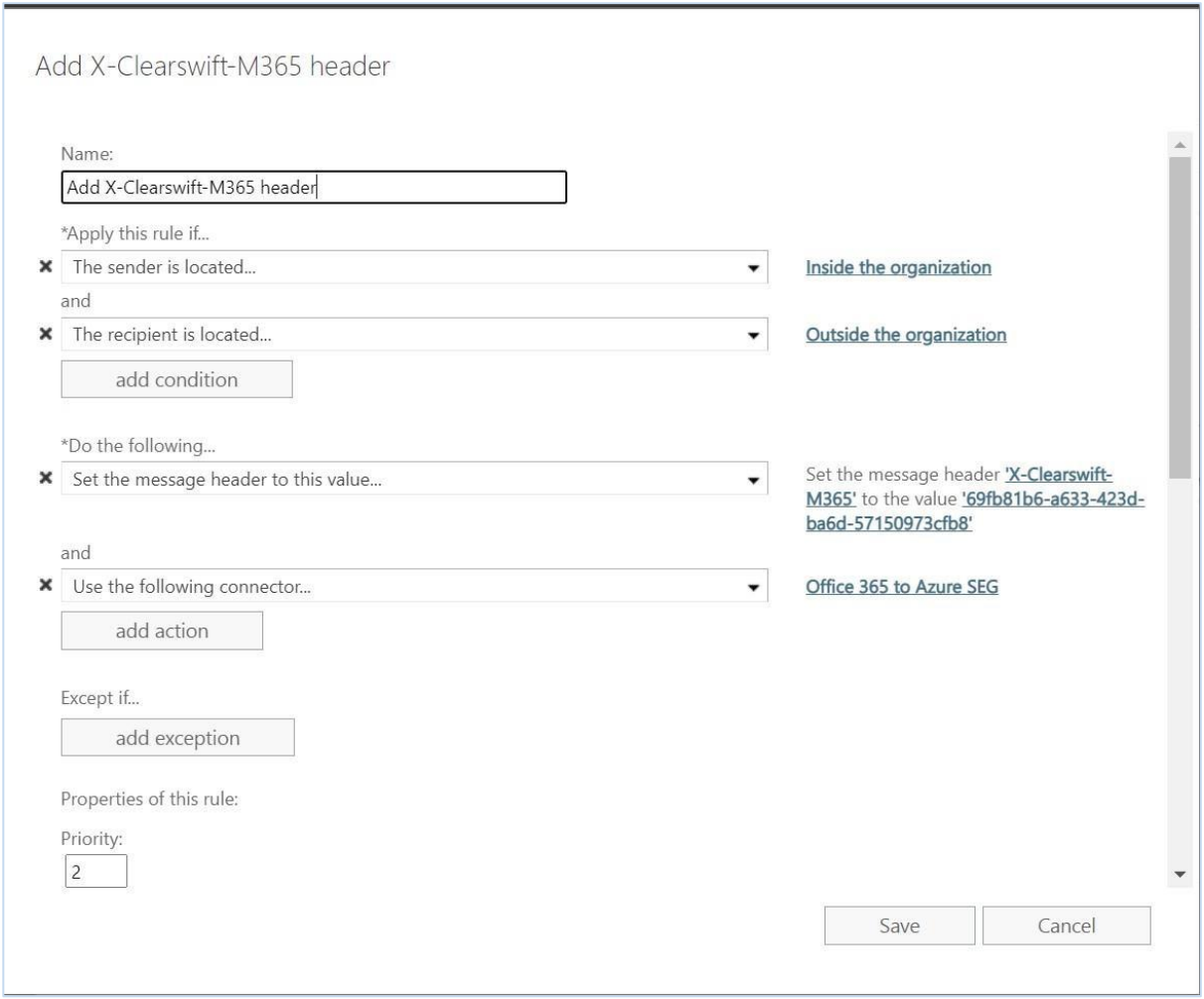
You now have a connector configured to route messages from Office 365 via the Secure Email Gateway.

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 "Configure the SEG to Prevent Relaying Spoofed Email from Office 365".
        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:
Add X-Clearswift-M365 header
*Apply this rule if...
The sender is located...
Inside the organization
and
The recipient is located...
Outside the organization
add condition
*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
add action
Except if...
add exception
Properties of this rule:
Priority:
2
Save
Cancel

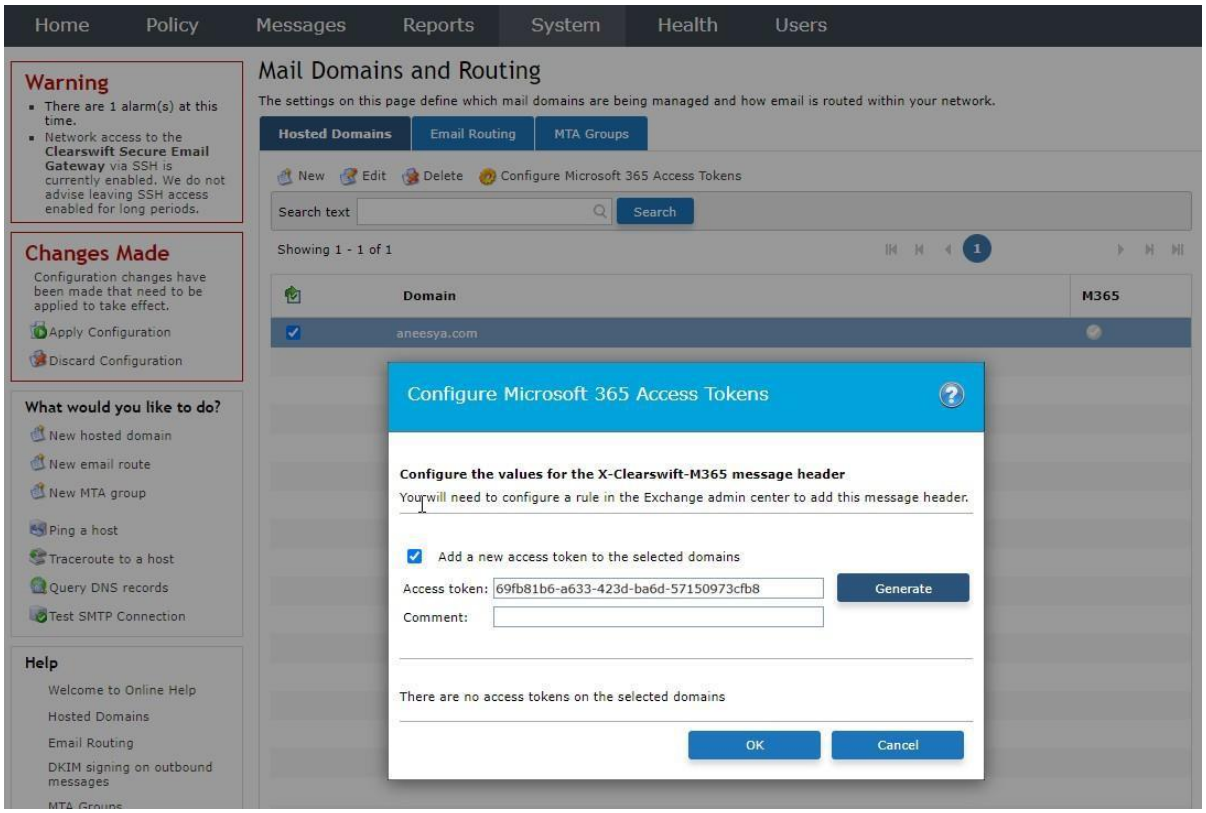
Configure the SEG to Prevent Relaying Spoofed Email from Office 365

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.

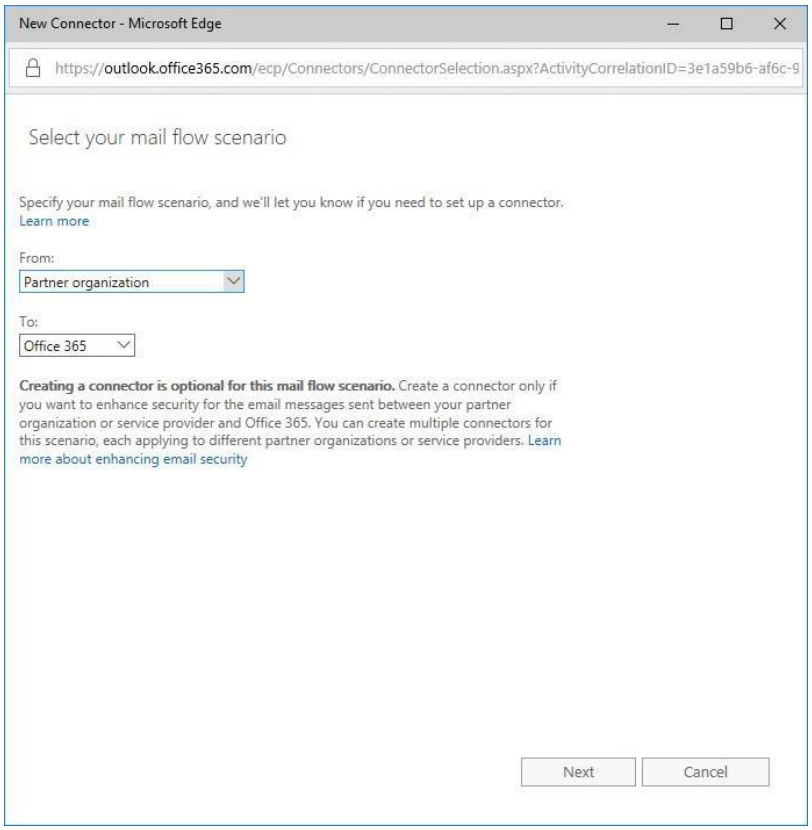
It is also necessary that the Global Spoof Detection option is enabled in the Spam Policy to hold/reject attempts to send through your Gateway using your domain name.

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.

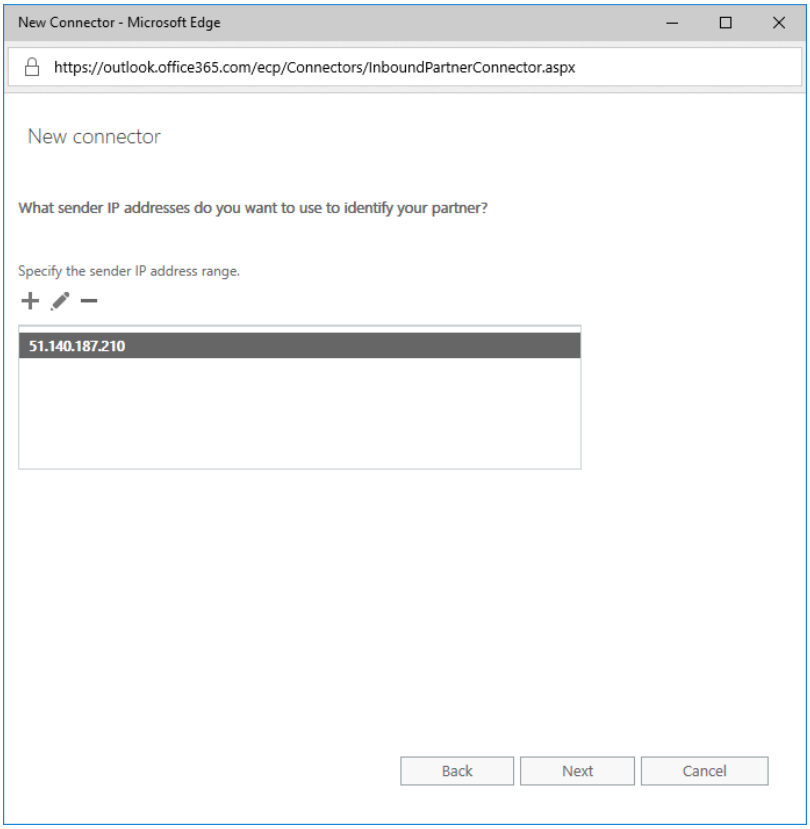
To do this:

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**.

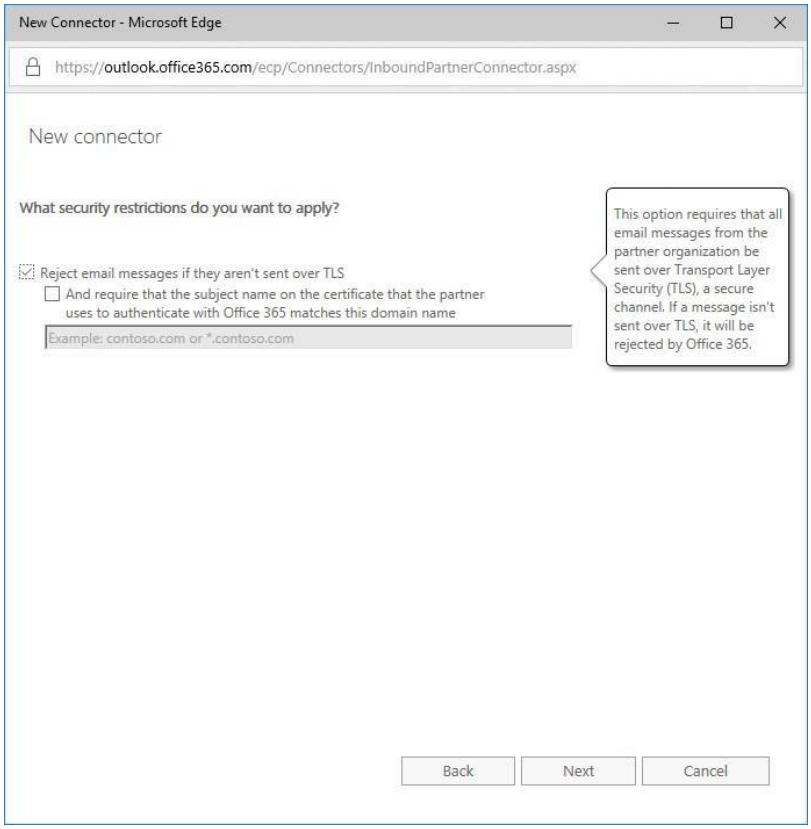


6. In the New connector dialog:
    a. Enter a name for the connector.
    b. Enter a description.
    c. Ensure that the **Turn it on** check box is selected.
    d. Click on **Next**.

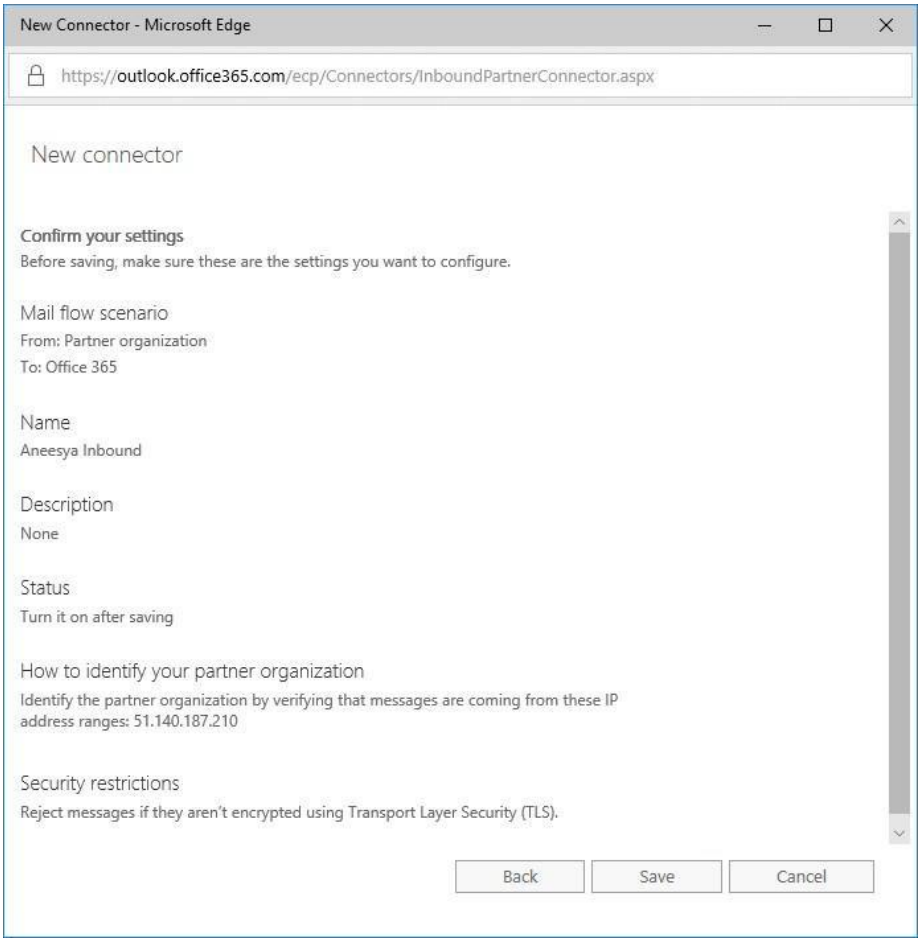
7. In the How do you want to identify the partner organization? dialog:
    a. Select the **Use the sender's IP address** radio button.
    b. Click on **Next**.
8. In the What sender IP addresses do you want to use to identify your partner? dialog:
    a. Select **+**.
    b. In the add ip address dialog, 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**.



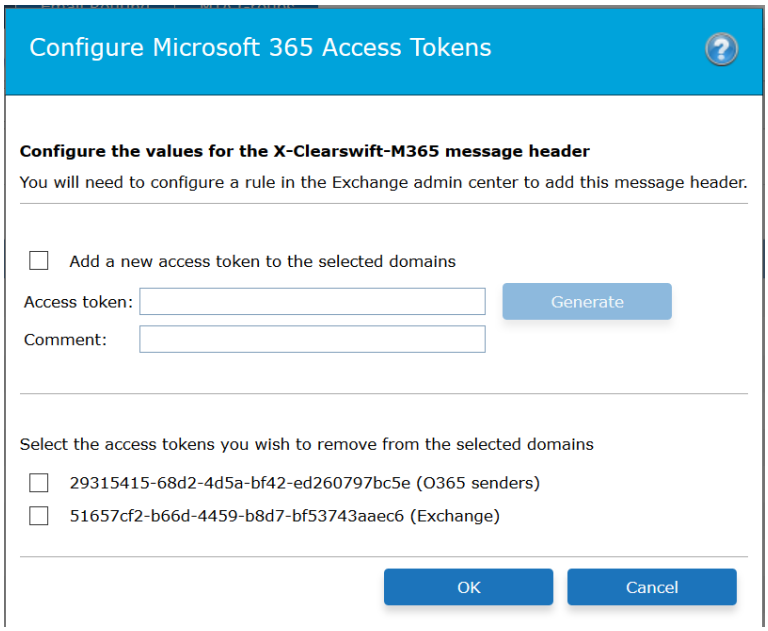
You should now be able to receive messages securely in Office 365 via the Secure Email Gateway.

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 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.

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

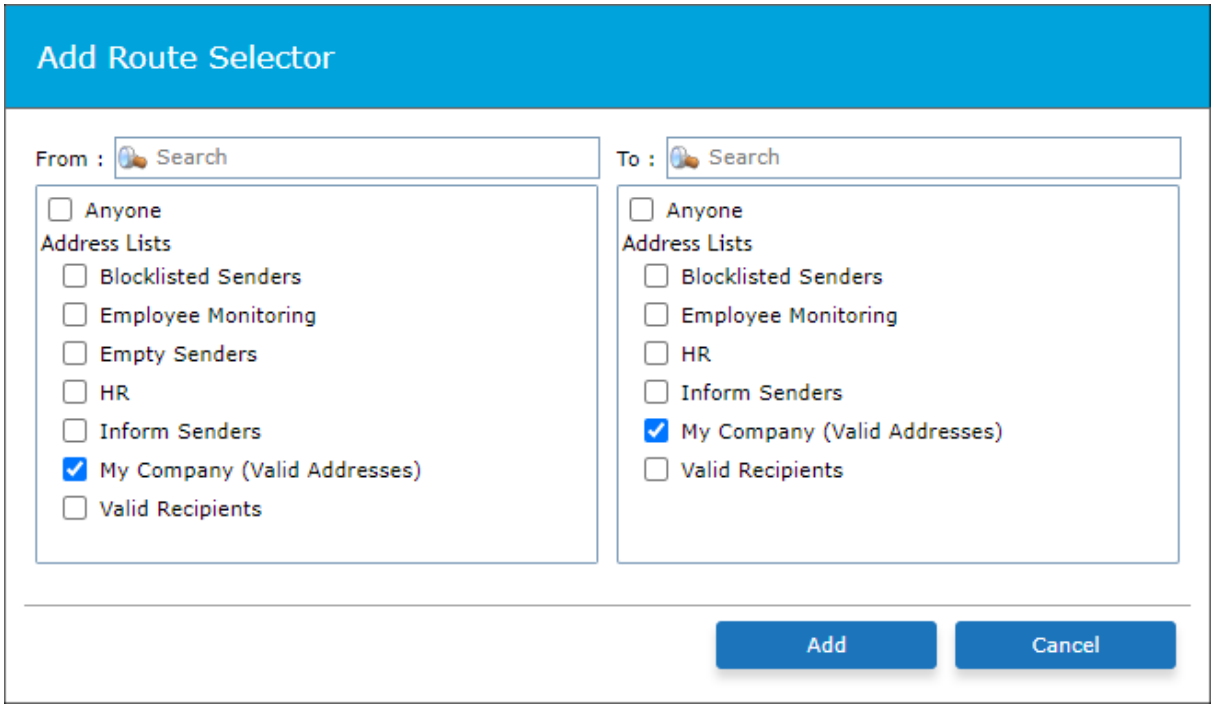
Configure the SEG to Scan Internal Office 365 Email

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.

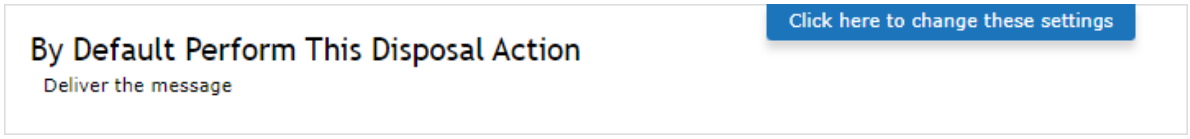
If you wish to do this, the first step is to configure your SEG to allow Office 365 to send internal emails through your SEG. You will need to create an internal My Company (Valid Addresses) to My Company (Valid Addresses) policy route.

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**.

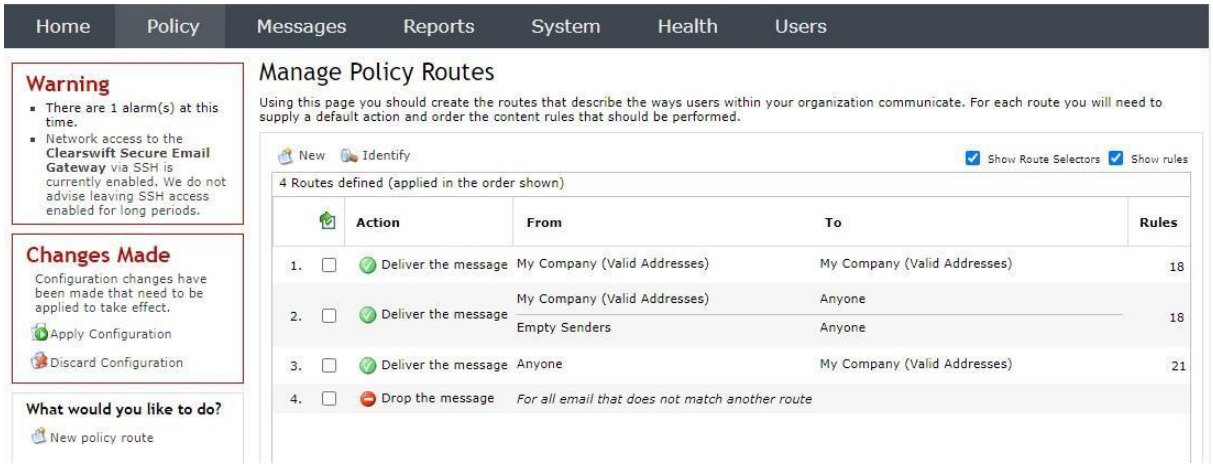


5. Ensure that the **By Default Perform This Disposal Action** section is set to: **Deliver the message**



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.



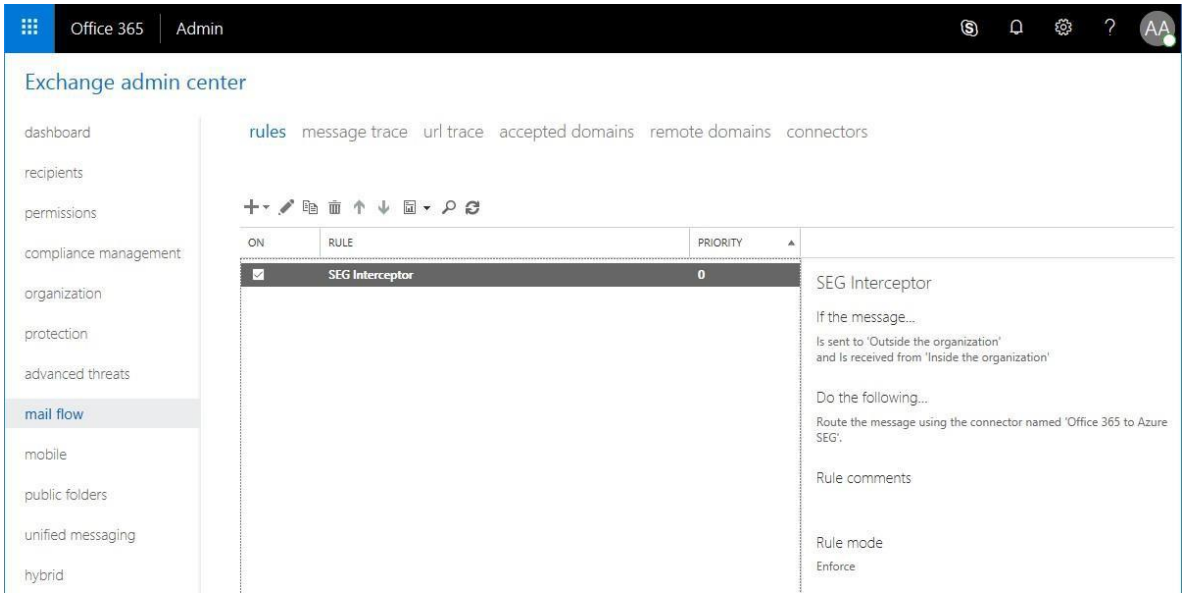
You have now configured your SEG to scan internal Office 365 emails in order to enforce a security and A-DLP policy on them. You can create a more granular policy for incoming, outgoing and internal emails by creating additional policy routes as required.

Configure Office 365 to Route Internal Email via the SEG

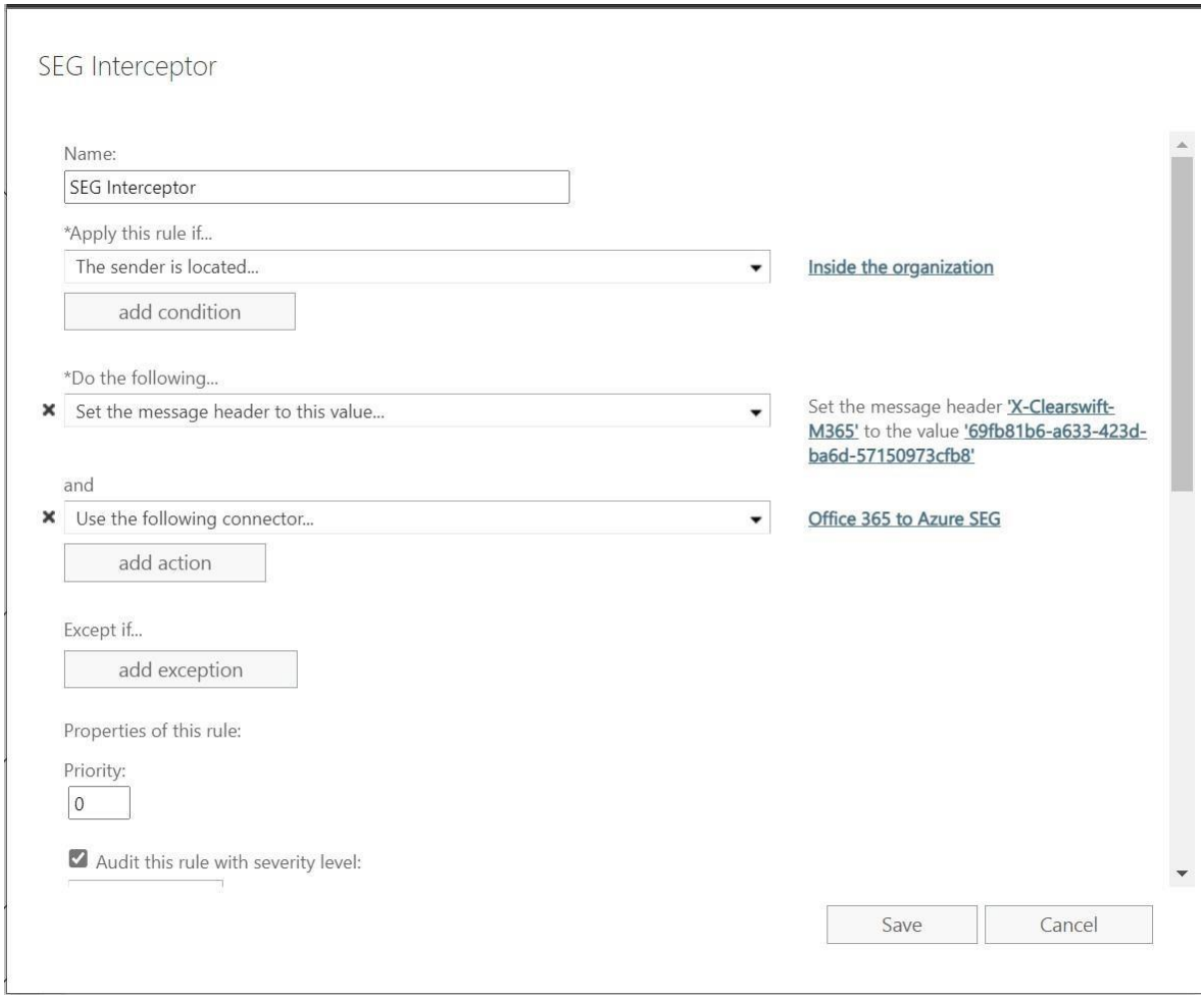
The next step is to reconfigure your organization's Office 365 portal to route internal emails to the SEG server(s) for scanning.

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**.



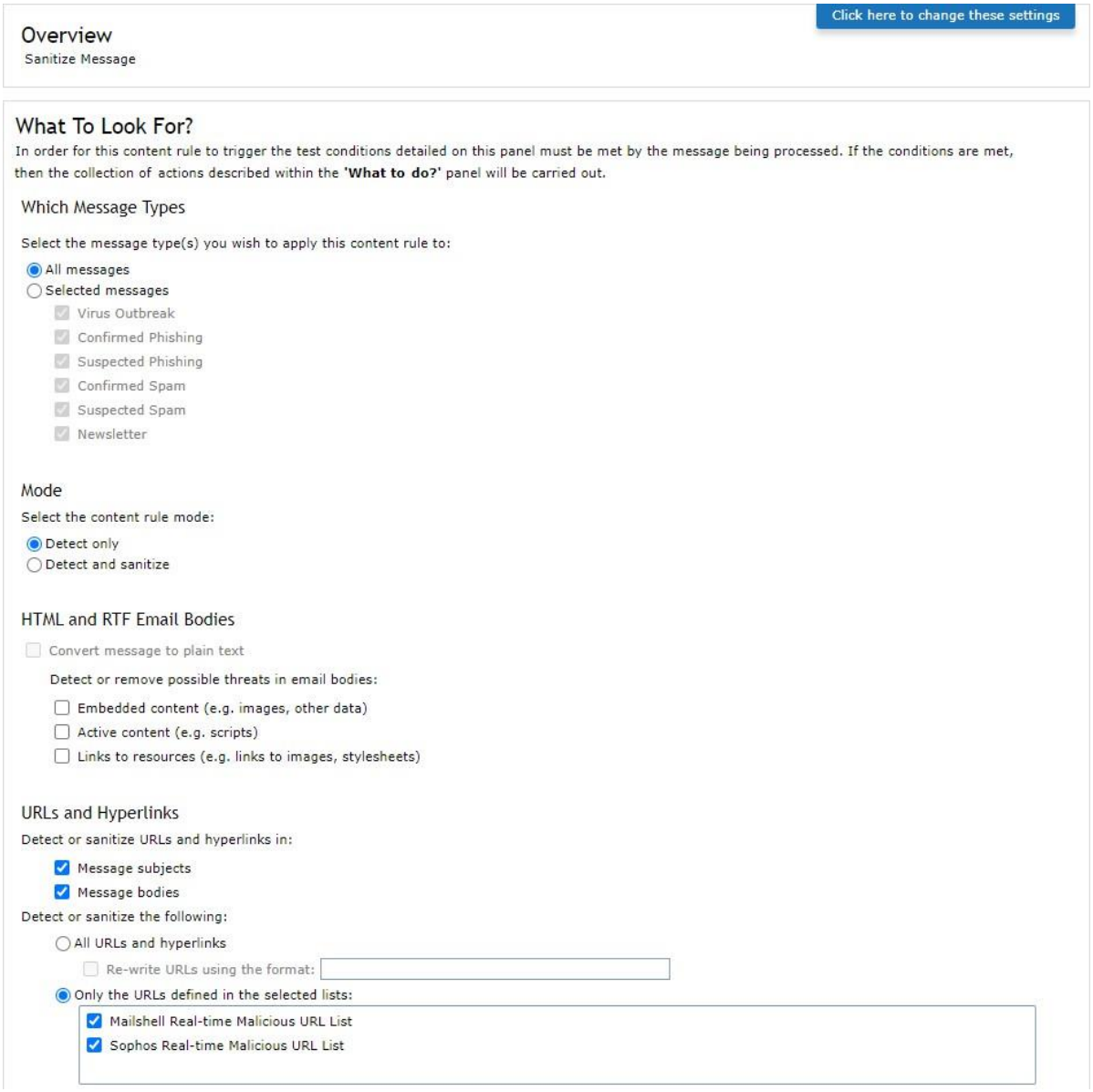
You have now configured Office 365 to route internal emails via the SEG in order to enforce an internal email security and A-DLP policy. If you wish to exempt certain internal emails from being routed via the SEG, then you can use the add exception button in the rule that you just amended to exempt the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



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.

Contact Fortra

For more information about the Fortra's Clearswift products and cybersecurity solutions, please visit our website.

You can contact us for questions, and to receive technical bulletins, updates, program fixes and other information on your product via email or Internet.

Fortra Support Portal

Fortra Support Portal offers various helpful resources, such as product documentation and knowledge articles. You can also contact our Technical Support, using the Fortra Support Portal.

For support issues, please:

- Check this guide's table of contents and topics for information that addresses your concern.
- Check the Knowledge Base in the Fortra Support Portal for information that addresses your concern.
- Gather and organize as much information as possible about the problem, including job/error logs, screenshots or anything else to document the issue.