FORTRA

Configuring Clearswift Secure Email Gateway to work with Microsoft Office 365 (v3.3, April 2022)

Copyright Terms and Conditions

Copyright © Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.

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 Fortra is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to Fortra with appropriate and specific direction to the original content.

202305250958

Contents

Copyright Terms and Conditions2
Contents
Introduction
Configure the SEG to Scan Inbound Email Before Routing to Office 365
Configure the SEG to Scan Outbound Email from Office 3657
Configure the SEG to Detect Spam in an Office 365 Environment
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
Configure the SEG to Only Send and Receive Messages from Valid Email Addresses in your Domain
Configure the SEG to Scan Internal Office 365 Email 25
Configure Office 365 to Route Internal Email via the SEG
Configure the SEG to Detect Malicious URLs in an Office 365 Environment
Further Information

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 <u>document</u>.

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**.

New Hosted Do	omain	
Domain : aneesya.com	n	
	Add	Cancel

- 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).
 - 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**.

Home	Policy	Messages	Reports	System	Health	Users	
Warning There are 1 time.	alarm(s) at this	Overview Internal Email S	ervers				Click here to change these settings
Clearswift	Secure Email a SSH is abled. We do not	Client Hosts	Sender Domains	Relay	TLS Settings	Authentication	
advise leavin enabled for	ng SSH access long periods.	Hosts 👌 New	🧭 Edit 🛛 🎯 Delete	•			
Changes I	Made	*.outbound.prot	ection.outlook.com				
Configuration been made th applied to tak	changes have at need to be e effect.						

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

Office 365. To do this:

- 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:	
	Save Cancel

- 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 : 40 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 :		
	Save	Cancel

- 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 : 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 : Internal Email Servers X v
Use these authentication settings when connecting to the email server : Authentication : None 🗸
Update Cancel

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).

- 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**.

New Connector - Microsoft Edge	1770)
https://outlook.office365.com/ecp/Connectors/ConnectorSelection.aspx?ActivityConnectorSelectio	CorrelationID=	b90bdfda-	1a4
Select your mail flow scenario			
Specify your mail flow scenario, and we'll let you know if you need to set up a connector. team more Trom: Office 365 Partner organization 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 Office 365 and your partner organization or service provider. You can create multiple connectors for this scenario, each applying to different partner organizations or service providers. Learn more about enhancing email security	Office 365: email subsc Your organ email serve email serve email serve email serve an on-pren Partner org partner org partner can organizatio business wi bank. It can cloud email provider th services suc archiving, a and so on. Internet Fo email, this r email that's the Internet 365 (not to server or pp organizatio outbound e	Your cloud ription. ization s en This is an r that you s often callel isses server, yanization: A be an n you do th, such as a also be a l service at provides th as nti-spam, or inbound efers to sent from to Office your email artner your email	d l

- 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.

		-		×
A https://outlook.office365.com/ecp/Cor	nnectors/OutboundConnector.aspx?Con	nectorType=Partne	e .	
New connector				
How do you want to route email messages?	(
Specify one or more smart hosts to which Office nost is an alternative server and can be identifie FQDN) or an IP address. Learn more	e 365 will deliver email messages. A smart ed by using a fully qualified domain name			
O Use the MX record associated with the part domain	ther's			
Route email through these smart hosts				
+/-				
pmseg01.uksouth.cloudapp.anare.com				
pmseg01.uksouth.cloudapp.azure.com				
pmseg01aksouth.cloudapp.anare.com				
pmseg01.uksouth.cloudapp.azure.com				
pmseg01.uksouth.cloudapp.azure.com				

- 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**.

▲ 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: Issample: contoso.com or *.contoso.com Back Next	New Connector - Microsoft Edge	126		Х
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 connection isn't successful. Example: contoso.com or *.contoso.com Back Next	https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?Connector	torType=Partnei	t)	
How should Office 365 connect to your partner organization's email server? Mayas 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 Image: Security of the subject name or subject alternative name (SAN) matches this domain name: Example: contoso.com or *.contoso.com Example: contoso.com or *.contoso.com	New connector			
 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 	How should Office 365 connect to your partner organization's email server?	TLS is a securit	y protoco	
Any digital certificate, including self-signed certificates Image: State of the subject name or subject alternative name (SAN) matches this domain name: Example: contoso.com or *.contoso.com	Always use Transport Layer Security (TLS) to secure the connection (recommended) Connect only if the recipient's email server certificate matches this criteria	that helps to e deliver email n securely so no the sender and can access or t	ncrypt an nessages one exce I recipien amper wi	pt t ith
And the subject name or subject alternative name (SAN) matches this domain name: Example: contoso.com or *.contoso.com Back Next Cancel	Any digital certificate, including self-signed certificates Issued by a trusted certificate authority (CA)	the message. I	f you sele	ct
Example: contoso.com or *.contoso.com Back Next Cancel	And the subject name or subject alternative name (SAN) matches this domain name:	be rejected if t connection isn	he TLS 't success	sful.
Back Next Cancel				
	Back Next	Cai	ncel	

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

New Connector - Microsoft Edge			1777		>
https://outlook.office365.com/ecp/Connectors/Out	boundConnector.asp	x?ConnectorType=	Partner		
New connector					
Confirm your settings					
Before we validate this connector for you, make sure these ar configure.	e the settings you wan	t to			
Mail flow scenario					
From: Office 365					
To: Partner organization					
Name					
Aneesya Outbound					
Description					
None					
Status					
Off. I'll turn it on later.					
When to use the connector					
Use only for email sent to these domains: *					
Routing method					
Route email messages through these smart hosts: pmseg01.uksouth.cloudapp.azure.com					
	Back	Next	Cano	el	

- 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.

- 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.
 - I. 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 selfreference..
 - 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.

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	
and	ba6d-57150973cfb8'
and	
Use the following connector	✓ Office 365 to Azure SEG
add action	
Event if	
add avcention	
add exception	
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 "<u>Configure an Office 365 Rule to Route Outgoing Email to the SEG</u>" 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 "<u>Configure an Office 365 Rule to Route Outgoing Email to the SEG</u>" 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.**

Home	Policy	Messages	Reports	System	Health	Users	
Warning • There are 1	alarm(s) at this	Mail Domai	ns and Rout	ing mail domains are be	ing managed and	how email is routed within your network	L.
time. Network ac	cess to the	Hosted Domai	ns Email Routin	ng MTA Groups			
Gateway v currently er	Secure Email ita SSH is nabled. We do not	👌 New 🕑 Ed	it 🎯 Delete 👩 🤅	Configure Microsoft	365 Access Tokens	5	
advise leav enabled for	ing SSH access long periods.	Search text		Q	Search		
Changes	Made	Showing 1 - 1 o	f 1			IR R 4 1	> ⊨ H
Configuration been made th applied to tal	changes have hat need to be ke effect.	1	Domain				M365
Apply Conf	iguration		aneesya.com				0
Discard Co	nfiguration		-				
			Configure	Microsoft 365	Access Toke	ens 🕐	
What would	you like to do?						
Mew hoste	d domain						
New email	route		Configure the v	alues for the X-C	earswift-M365 n	nessage header	
🖑 New MTA ç	Iroup		Yourwill need to	configure a rule in t	he Exchange admir	n center to add this message header.	
Ping a host							
Traceroute	to a host		🗹 🛛 Add a new	access token to the	selected domains		
Query DNS	records		Access token: 6	9fb81b6-a633-423d	l-ba6d-57150973c	fb8 Generate	
Test SMTP	Connection		Comment:				
Help							
Welcome to	o Online Help		There are no acc	ess tokens on the s	elected domains		
Hosted Dor	mains						
Email Rout	ing					OK Cancel	
DKIM signi messages	ng on outbound						

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.

- 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**.

		0.00		×
A https://outlook.office365.com/ecp/Connectors/ConnectorSelection.	aspx?ActivityCorrelati	onID=3e	1a59b6-	af6c-
Select your mail flow scenario				
Specify your mail flow scenario, and we'll let you know if you need to set up a c Learn more	onnector,			
From:				
Partner organization V				
To:				
Office 365 V				
rins scenario, each appying to unretent partner organizations of service provide more about enhancing email security	ers, Learn			

- 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**.

New Connector - Microsoft Edge	-		×
A https://outlook.office365.com/ecp/Connectors/InboundPartnerConnector.aspx			
New connector			
What sender IP addresses do you want to use to identify your partner?			
Specify the sender IP address range.			
51.140.187.210			
Back Next	Car	ncel	

- 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**.

New Connector - Microsoft Edge		1		×
https://outlook.office365.com/ecp/Connectors/InboundPartnerConnector.aspx				
New connector				
What security restrictions do you want to apply?	This o email	ption re message	quires the	at all ne
☑ Reject email messages if they aren't sent over TLS ☐ And require that the subject name on the certificate that the partner uses to authenticate with Office 365 matches this domain name	sent c Securi chann	er organi iver Tran ity (TLS), iel. If a m	sport Lay a secure lessage is	er in't
Example: contoso.com or *.contoso.com	reject	ed by Of	fice 365.	
Back Next		Ca	ncel	

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	e Microsoft 365 Access Tokens	?
Configure the You will need to	e values for the X-Clearswift-M365 message header to configure a rule in the Exchange admin center to add this message h	neader.
Add a ne Access token: Comment:	ew access token to the selected domains Generate Generate	
Select the acce 2931541 51657cf2	ess tokens you wish to remove from the selected domains 15-68d2-4d5a-bf42-ed260797bc5e (O365 senders) f2-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.

Home	Policy	Messages	Reports	System	Health	Users	
Warning There are 1 time. Network ac	alarm(s) at this cess to the	Manage Using this pag supply a defau	Policy Routes you should create the rould action and order the cou	outes that describe the v ntent rules that should l	vays users witl be performed.	hin your organization communicate. For each route y	ou will need to
Clearswift Gateway v	Secure Email ia SSH is	👌 New 🤅	🍋 Identify			🗹 Show Route Sele	ectors 🗹 Show rules
currently er advise leav	nabled. We do not no SSH access	3 Routes d	efined (applied in the orde	r shown)			
enabled for	long periods.	1	Action	From		То	Rules
Changes	Made			My Company (Valid Ad	dresses)	Anyone	
Configuration been made th applied to tak	changes have nat need to be ce effect.	1. 🗌	⊘ Deliver the message	Empty Senders		Anyone	18
Apply Conf	iguration	2.	⊘ Deliver the message	Anyone		My Company (Valid Addresses)	21
🎲 Discard Co	nfiguration	3. 🗆	Drop the message	For all email that does	not match and	other 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**.

 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**



- 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	Messa	iges	Reports	System	Health U	sers	
Warning There are 1 time.	alarm(s) at this	Mana Using th supply a	is pag defai	Policy Routes be you should create the ro ult action and order the cor	utes that describe the ntent rules that should	ways users within you be performed.	r organization communicate. For each route you will r	eed to
 Network ac Clearswift 	Secure Email	👌 Ne	ew (b Identify			Show Route Selectors 🗸	Show rules
currently enabled. We do not		4 Rou	ites d	efined (applied in the orde	r shown)			
enabled for	long periods.		1	Action	From		То	Rules
Changes Configuration	Made	1,		Oeliver the message	My Company (Valid A	ddresses)	My Company (Valid Addresses)	18
been made th applied to tal	been made that need to be applied to take effect		-	A 5 1	My Company (Valid A	ddresses)	Anyone	
Apply Conf	iguration	2.	U	Upeliver the message	Empty Senders		Anyone	18
🎲 Discard Co	nfiguration	3.		⊘ Deliver the message	Anyone		My Company (Valid Addresses)	21
What would	you like to do?	4.		ᅌ Drop the message	For all email that doe	s not match another ro	oute	
C New policy	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.

- 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).

III Office 365 Admin					S D & ? AA
Exchange admin cent	ter				
dashboard	rules	message trace url trace acce	pted domains remot	te domains	connectors
recipients					
permissions	+- 🖉	≞ m ↑ ↓ ⊡ · ዖ♂			
compliance management	ON	RULE		PRIORITY	*
organization		SEG Interceptor		0	SEG Interceptor
protection					If the message
protection					Is sent to 'Outside the organization' and Is received from 'Inside the organization'
advanced threats					Do the following
mail flow					Route the message using the connector named 'Office 365 to Azure SEG'.
mobile					2.4
public folders					Rule comments
unified messaging					Rule mode
hybrid					Enforce

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

Name:		
SEG Interceptor		
*Apply this rule if		
The sender is located	✓ Inside the organization	
add condition		
*Do the following		
Set the message header to this value	 Set the message header 'X-Clearswit M365' to the value '60th 81b6 a623 	<u>ft-</u>
	ba6d-57150973cfb8'	4230
and		
Use the following connector	Office 365 to Azure SEG	
add action		
Except if		
add exception		
Properties of this rule:		
Priority:		
0		
Audit this rule with severity level:		

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.

- 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**.

Click here to change these settings

Overview 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

O 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 Fortra Community Portal
- Support for Fortra's Clearswift and Professional Services: <u>https://www.clearswift.com/support/portals</u>