

# Configuración de Microsoft 365 con correo electrónico seguro

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configuración de Microsoft 365 con correo electrónico seguro](#)

[Configurar el correo electrónico entrante en Microsoft 365 desde Cisco Secure Email](#)

[Omitir regla de filtrado de correo no deseado](#)

[Conector de recepción](#)

[Configurar el correo desde Cisco Secure Email a Microsoft 365](#)

[Controles de destino](#)

[Tabla de acceso de destinatarios](#)

[Rutas SMTP](#)

[Configuración de DNS \(registro MX\)](#)

[Probar correo electrónico entrante](#)

[Configurar el correo electrónico saliente desde Microsoft 365 a Cisco Secure Email](#)

[Configure RELAYLIST en Cisco Secure Email Gateway](#)

[Activar TLS](#)

[Configurar el correo de Microsoft 365 a CES](#)

[Crear una regla de flujo de correo](#)

[Probar correo electrónico saliente](#)

[Información Relacionada](#)

[Documentación de Cisco Secure Email Gateway](#)

[Documentación de Secure Email Cloud Gateway](#)

[Documentación de Cisco Secure Email and Web Manager](#)

[Documentación de productos de Cisco Secure](#)

---

## Introducción

Este documento describe los pasos de configuración para integrar Microsoft 365 con Cisco Secure Email para la entrega de correo electrónico entrante y saliente.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Secure Email Gateway o Cloud Gateway
- Acceso mediante la interfaz de línea de comandos (CLI) al entorno de Cisco Secure Email Cloud Gateway:  
[Cisco Secure Email Cloud Gateway > Acceso con interfaz de línea de comandos \(CLI\)](#)
- Microsoft 365
- Protocolo Simple Mail Transfer (SMTP)
- Servidor de nombres de dominio o sistema de nombres de dominio (DNS)

## Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

Este documento se puede utilizar para gateways in situ o para gateways de la nube de Cisco.

Si es administrador de Cisco Secure Email, su carta de bienvenida incluye las direcciones IP de su gateway de la nube y otra información pertinente. Además de la carta que ve aquí, se le envía un correo electrónico cifrado que le proporciona detalles adicionales sobre el número de Cloud Gateway (también conocido como ESA) y Cloud Email and Web Manager (también conocido como SMA) aprovisionados para su asignación. Si no ha recibido o no tiene una copia de la carta, póngase en contacto [ces-activations@cisco.com](mailto:ces-activations@cisco.com) con su información de contacto y nombre de dominio en el servicio.

# Your Cisco Cloud Email Security (CES) service is ready!

Organization Name: ██████████

Start Date: 2022-09-09 05:09:04 America/Los\_Angeles

Below you will find information about your login credentials and other important information regarding your CES. Please retain this email for future reference

## MX Records for inbound email from Internet

- mx1.████████.iphmx.com
- mx2.████████.iphmx.com

## Your Cisco CES portals:

### **Email Security**

<https://dh████████-esa1.iphmx.com>

### **Security Management**

<https://dh████████-sma1.iphmx.com>

### **End User Quarantine**

<https://dh████████-euq1.iphmx.com>

## Please sign in the portals with this user ID:

**Username:** ██████████

**Password:** ██████████

**Note:** We recommend changing your password after the initial login.

## Hostname and IP addresses to be whitelisted(for Microsoft/Office365 and G-Suite users):

### **Email Security:**

████████.140.105

████████.150.143

████████.143.186

████████.32.98

### **Security Management:**

████████.157.91

If you are using a Cloud service such as Office365, G-Suite, etc., you should direct your outbound emails to the address below to have them scanned by Cisco Cloud Email Security:

## Host and IP address used for outbound relay from Office365 and G-Suite:

ob1.hc████████.iphmx.com

## Include CES host and IP address in your SPF record:

v=spf1 exists:%{i}.spf.hc████████.iphmx.com ~all

Cada cliente tiene direcciones IP dedicadas. Puede utilizar las direcciones IP o los nombres de host asignados en la configuración de Microsoft 365.



**Nota:** se recomienda encarecidamente realizar la prueba antes de la transición al correo de producción planificada, ya que las configuraciones tardan en replicarse en la consola de Microsoft 365 Exchange. Como mínimo, espere una hora para que todos los cambios surtan efecto.



**Nota:** las direcciones IP de la captura de pantalla son proporcionales al número de gateways de nube proporcionados a su asignación. Por ejemplo, xxx.yy.140.105 es la dirección IP de la interfaz de datos 1 para la puerta de enlace 1 y xxx.yy.150.1143 es la dirección IP de la interfaz de datos 1 para la puerta de enlace 2. La dirección IP de la interfaz de datos 2 para la puerta de enlace 1 es xxx.yy.143.186 y la dirección IP de la interfaz de datos 2 para la puerta de enlace 2 es xxx.yy.32.98. Si su carta de bienvenida no incluye información para Data 2 (IP de interfaz saliente), póngase en contacto con el TAC de Cisco para que se agregue la interfaz de Data 2 a su asignación.

---

Configuración de Microsoft 365 con correo electrónico seguro

Configurar el correo electrónico entrante en Microsoft 365 desde Cisco Secure Email

#### Omitir regla de filtrado de correo no deseado

- Inicie sesión en el Centro de administración de Microsoft 365 (<https://portal.microsoft.com>).
- En el menú de la izquierda, expanda **Admin Centers**.
- Haga clic en **Exchange**.
- En el menú de la izquierda, vaya a **Mail flow > Rules**.
- Haga clic [+] para crear una nueva regla.
- Elija **Bypass spam filtering...** de la lista desplegable.
- Introduzca un nombre para la nueva regla: **Bypass spam filtering - inbound email from Cisco CES**.
- Para \*Aplicar esta regla si..., elija **The sender - IP address is in any of these ranges or exactly matches**.
  1. Para la ventana emergente especificar intervalos de direcciones IP, agregue las direcciones IP proporcionadas en la carta de bienvenida de Cisco Secure Email.
  2. Haga clic en **OK**.

- Para \*Realice lo siguiente..., se ha preseleccionado la nueva regla: **Set the spam confidence level (SCL) to... - Bypass spam filtering**.
- Haga clic en **Save**.

Un ejemplo de cómo se ve la regla:

### Bypass spam filtering - inbound email from Cisco CES

Name:

\*Apply this rule if...

\*Do the following...

Except if...

Properties of this rule:  
 Priority:

Enter in the IP address(es) associated with your Cisco Secure Email Gateway/ Cloud Gateway



**Bypass spam filtering**  
 Mark specific messages with an SCL before they're even scanned by spam filtering. Use mail flow rules to set the spam confidence level (SCL) in messages in EOP.

### Conector de recepción

- Permanecer en el Centro de administración de Exchange.
- En el menú de la izquierda, vaya a **Mail flow > Connectors**.
- Haga clic [+] para crear un nuevo conector.
- En la ventana emergente Seleccione su escenario de flujo de correo, elija:

1. Desde: Partner organization

- A: **Office365**
  
- Haga clic en **Next**.
- Introduzca un nombre para el nuevo conector: **Inbound from Cisco CES**.
- Si lo desea, ingrese una descripción.
- Haga clic en **Next**.
- Haga clic en **Use the sender's IP address**.
- Haga clic en **Next**.
- Haga clic [+] e introduzca las direcciones IP que se indican en la carta de bienvenida de Cisco Secure Email.
- Haga clic en **Next**.
- Elegir **Reject email messages if they aren't sent over Transport Layer Security (TLS)**.
- Haga clic en **Next**.
- Haga clic en **Save**.

Un ejemplo de cómo se ve la configuración del conector:

# Inbound from Cisco CES



## Mail flow scenario

From: Partner organization

To: Office 365

## Name


Inbound from Cisco CES

## Status

On

[Edit name or status](#)

## How to identify your partner organization

Identify the partner organization by verifying that messages are coming from these IP address ranges: 

[Edit sent email identity](#)

## Security restrictions

Reject messages if they aren't encrypted using Transport Layer Security (TLS)

[Edit restrictions](#)

Configurar el correo desde Cisco Secure Email a Microsoft 365

## Controles de destino

Imponga un autoacelerador a un dominio de entrega en los controles de destino. Por supuesto, puede eliminar el acelerador más adelante, pero estas son nuevas IP para Microsoft 365, y no desea ninguna limitación por parte de Microsoft debido a su reputación desconocida.

- Inicie sesión en el gateway.
- Desplácese hasta **Mail Policies > Destination Controls**.
- Haga clic en **Add Destination**.

- Uso:

1. Destino: introduzca su nombre de dominio

2. Conexiones simultáneas: **10**

- Cantidad máxima de mensajes por conexión: **20**
- Compatibilidad con TLS: **Preferred**

- Haga clic en **Submit**.
- Haga clic **Commit Changes** en la parte superior derecha de la interfaz de usuario (IU) para guardar los cambios de configuración.

Un ejemplo de cómo se ve la tabla de control de destino:

Destination Control Table							Items per page 20
Domain	IP Address Preference	Destination Limits	TLS Support	DANE Support ^	Bounce Verification *	Bounce Profile	All <input type="checkbox"/> Delete
<a href="#">your_domain_here.com</a>	Default	10 concurrent connections, 20 messages per connection, Default recipient limit	Preferred	Default	Default	Default	<input type="checkbox"/>
Default	IPv6 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	None	None	Off	Default	

\* Bounce Verification settings apply only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.  
 ^ DANE will not be enforced for domains that have SMTP Routes configured.

### Tabla de acceso de destinatarios

A continuación, defina la tabla de acceso de destinatarios (RAT) para que acepte el correo de sus dominios:

- Desplácese hasta **Mail Policies > Recipient Access Table (RAT)**.



**Nota:** Asegúrese de que Listener es para Receptor Entrante, Correo Entrante o MailFlow, basándose en el nombre real de Listener para el flujo de correo principal.

- Haga clic en **Add Recipient**.
- Agregue sus dominios en el campo Dirección del destinatario.
- Elija la acción predeterminada de **Accept**.



- Haga clic en **Submit**.
- Haga clic **Commit Changes** en la parte superior derecha de la interfaz de usuario para guardar los cambios de configuración.

Un ejemplo de cómo se ve tu entrada RAT:

Recipient Details				
Order:	<input type="text" value="1"/>			
Recipient Address: ?	<input type="text" value="your_domain_here.com"/>			
Action:	<input type="button" value="Accept"/> <input type="checkbox"/> Bypass LDAP Accept Queries for this Recipient			
Custom SMTP Response:	<input checked="" type="radio"/> No			
	<input type="radio"/> Yes			
	<table border="1"> <tr> <td>Response Code:</td> <td><input type="text" value="250"/></td> </tr> <tr> <td>Response Text:</td> <td><div style="background-color: #cccccc; height: 100px;"></div></td> </tr> </table>	Response Code:	<input type="text" value="250"/>	Response Text:
Response Code:	<input type="text" value="250"/>			
Response Text:	<div style="background-color: #cccccc; height: 100px;"></div>			
Bypass Receiving Control: ?	<input checked="" type="radio"/> No <input type="radio"/> Yes			

## Rutas SMTP

Establezca la ruta SMTP para enviar correo de Cisco Secure Email a su dominio de Microsoft 365:

- Desplácese hasta **Network > SMTP Routes**.
- Haga clic en **Add Route...**
- Dominio de recepción: introduzca el nombre de dominio.
- Hosts de destino: agregue su registro MX de Microsoft 365 original.
- Haga clic en **Submit**.
- Haga clic **Commit Changes** en la parte superior derecha de la interfaz de usuario para guardar los cambios de configuración.

Un ejemplo de cómo se ve la configuración de la ruta SMTP:

**SMTP Route Settings**

Receiving Domain:

Destination Hosts:	Priority <sup>?</sup>	Destination <sup>?</sup>	Port	Add Row
	<input type="text" value="0"/>	<input type="text" value="your_domain.mail.prot"/> <small>(Hostname, IPv4 or IPv6 address.)</small>	<input type="text" value="25"/>	

Outgoing SMTP Authentication: *No outgoing SMTP authentication profiles are configured. See Network > SMTP Authentication*

*Note: DANE will not be enforced for domains that have SMTP Routes configured.*

### Configuración de DNS (registro MX)

Ya puede cortar el dominio mediante un cambio de registro de intercambio de correo (MX). Póngase en contacto con el administrador de DNS para resolver los registros MX en las direcciones IP de la instancia de Cisco Secure Email Cloud, tal y como se proporciona en la carta de bienvenida de Cisco Secure Email.


Compruebe también el cambio en el registro MX de la consola de Microsoft 365:

- Inicie sesión en la consola de administración de Microsoft 365 (<https://admin.microsoft.com>).
- Desplácese hasta **Home > Settings > Domains**.
- Elija el nombre de dominio predeterminado.
- Haga clic en **Check Health**.

Esto proporciona los registros MX actuales de cómo Microsoft 365 busca sus registros DNS y MX asociados con su dominio:

The screenshot shows the Microsoft 365 admin center interface. The main content area displays the 'Domains' section for a specific domain. It indicates that the domain is managed at Amazon Web Services (AWS). There are options to 'Remove domain' and 'Refresh'. Below this, there are tabs for 'Overview', 'DNS records', 'Users', 'Teams & groups', and 'Apps'. A notification banner states: 'We didn't detect that you added new records to bce-demo.com. Make sure the records you created at your host exactly match the records shown here. If they do, please wait for our system to detect the changes. This usually takes around 10 minutes, although some DNS hosting providers require up to 48 hours.' Below the notification, there is a link to 'Amazon Web Services (AWS)'. A section titled 'Microsoft Exchange' contains a table of DNS records:

Type	Status	Name	Value	TTL
MX	Error	@	0 mail.protection.outlook.com	1 Hour
TXT	Error	@	v=spf1 include:spf.protection.outlook.com -all	1 Hour
CNAME	OK	autodiscover	autodiscover.outlook.com	1 Hour

 **Nota:** en este ejemplo, el DNS está alojado y administrado por Amazon Web Services (AWS). Como administrador, debe ver una advertencia si su DNS está alojado en cualquier lugar fuera de la cuenta de Microsoft 365. Puede ignorar advertencias como: "No detectamos que agregó nuevos registros a your\_domain\_here.com. Asegúrese de que los registros que ha creado en su host coinciden con los que se muestran aquí..." Las instrucciones paso a paso restablecen los registros MX a lo que se configuró inicialmente para redirigir a su cuenta Microsoft 365. Esto elimina Cisco Secure Email Gateway del flujo de tráfico entrante.

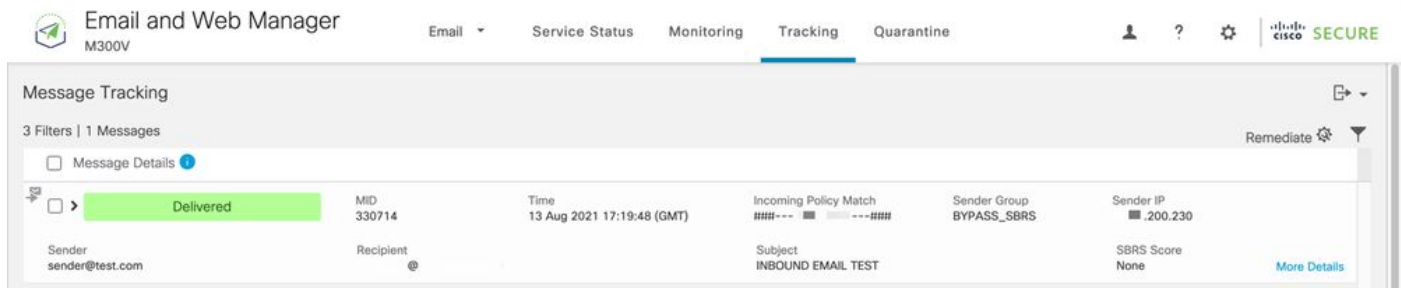
## Probar correo electrónico entrante

Pruebe el correo entrante en su dirección de correo electrónico de Microsoft 365. A continuación, compruebe que aparece en la bandeja de entrada de correo electrónico de Microsoft 365.

Valide los registros de correo en Rastreo de mensajes de su Cisco Secure Email and Web Manager (también conocido como SMA) proporcionado con su instancia.

Para ver los registros de correo en su SMA:

- Inicie sesión en el SMA (<https://sma.iphmx.com/ng-login>).
- Haga clic en **Tracking**.
- Introduzca los criterios de búsqueda necesarios y haga clic en **Search**; y espere ver estos resultados:



The screenshot shows the Cisco Email and Web Manager (SMA) interface. The top navigation bar includes "Email", "Service Status", "Monitoring", "Tracking" (highlighted), and "Quarantine". The main content area is titled "Message Tracking" and shows a table of message details. The table has columns for "Message Details", "MID", "Time", "Incoming Policy Match", "Sender Group", "Sender IP", "Sender", "Recipient", "Subject", and "SBR Score". A single message is listed with a status of "Delivered".

Message Details	MID	Time	Incoming Policy Match	Sender Group	Sender IP	Sender	Recipient	Subject	SBR Score
Delivered	330714	13 Aug 2021 17:19:48 (GMT)	###- - - - -###	BYPASS_SBRS	.200.230	sender@test.com	@	INBOUND EMAIL TEST	None

Para ver los registros de correo en Microsoft 365:

- Inicie sesión en el Centro de administración de Microsoft 365 (<https://admin.microsoft.com>).
- Expandir **Admin Centers**.
- Haga clic en **Exchange**.
- Desplácese hasta **Mail flow > Message trace**.
- Microsoft proporciona los criterios predeterminados con los que buscar. Por ejemplo, elija **Messages received by my primary domain in the last day** para iniciar la consulta de búsqueda.
- Introduzca los criterios de búsqueda necesarios para los destinatarios y haga clic en **Search** y espere ver resultados similares a los siguientes:

**Message trace > Message trace search results**

Export results Edit message trace Refresh 2 items Search

Date (UTC-05:00) ↓	Sender	Recipient	Subject	Status
8/13/2021, 1:20 PM	sender@test.com	[redacted]	INBOUND EMAIL TEST	Delivered

Configurar el correo electrónico saliente desde Microsoft 365 a Cisco Secure Email

### Configure RELAYLIST en Cisco Secure Email Gateway

Consulte la carta de bienvenida de Cisco Secure Email. Además, se especifica una interfaz secundaria para los mensajes salientes a través de la puerta de enlace.

- Inicie sesión en el gateway.
- Desplácese hasta **Mail Policies > HAT Overview**.



**Nota:** Asegúrese de que Listener es para Receptor saliente, Correo saliente o MailFlow-Ext, basándose en el nombre real de Listener para el flujo de correo externo/saliente.

- Haga clic en **Add Sender Group...**
- Configure el grupo emisor como:


1. Nombre: RELAY\_O365

2. Comentario: <<enter a comment if you wish to notate your sender group>>

3. Política: RETRANSMITIDA

4. Haga clic en **Submit and Add Senders**.

- Remitente: **.protection.outlook.com**

 **Nota:** El . (punto) al comienzo del nombre de dominio del remitente es obligatorio.

- Haga clic en **Submit**.
- Haga clic **Commit Changes** en la parte superior derecha de la interfaz de usuario para guardar los cambios de configuración.

Un ejemplo de cómo se ve su configuración de Grupo de Remitentes:

Sender Group Settings	
Name:	RELAY_O365
Order:	1
Comment:	From Microsoft 365 mail to Cisco Secure Email
Policy:	RELAYED
SBRS (Optional):	Not in use
External Threat Feed (Optional): <i>For IP lookups only</i>	None
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included
<a href="#">&lt;&lt; Back to HAT Overview</a> <span style="float: right;"><a href="#">Edit Settings...</a></span>	

Find Senders	
Find Senders that Contain this Text: 	<input type="text"/> <span style="float: right;"><a href="#">Find</a></span>

Sender List: Display All Items in List		Items per page 20 
<a href="#">Add Sender...</a>		
Sender	Comment	All <input type="checkbox"/> Delete
.protection.outlook.com	From Microsoft 365 mail to Cis...	<input type="checkbox"/>
<a href="#">&lt;&lt; Back to HAT Overview</a>		<a href="#">Delete</a>

## Activar TLS

- Haga clic en **<<Back to HAT Overview**.
- Haga clic en la política de flujo de correo denominada: **RELAYED**.
- Desplácese hacia abajo y busque en la **Security Features** sección **Encryption and Authentication**.
- Para TLS, elija: **Preferred**.
- Haga clic en **Submit**.
- Haga clic **Commit Changes** en la parte superior derecha de la interfaz de usuario para guardar los cambios de configuración.

Un ejemplo de cómo se ve la configuración de la política de flujo de correo:

Encryption and Authentication:	TLS:	<input type="radio"/> Use Default (Off) <input type="radio"/> Off <input checked="" type="radio"/> Preferred <input type="radio"/> Required
		TLS is Mandatory for Address List: <input type="text" value="None"/>
		<input type="checkbox"/> Verify Client Certificate
	SMTP Authentication:	<input checked="" type="radio"/> Use Default (Off) <input type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required
	If Both TLS and SMTP Authentication are enabled:	<input type="checkbox"/> Require TLS To Offer SMTP Authentication

## Configurar el correo de Microsoft 365 a CES

- Inicie sesión en el Centro de administración de Microsoft 365 (<https://admin.microsoft.com>).
- Expandir **Admin Centers**.
- Haga clic en **Exchange**.
- Desplácese hasta **Mail flow > Connectors**.
- Haga clic [+] para crear un nuevo conector.
- En la ventana emergente Seleccione su escenario de flujo de correo, elija:

1. Desde: Office365

- A:Partner organization
- Haga clic en **Next**.
- Introduzca un nombre para el nuevo conector: **Outbound to Cisco CES**.
- Si lo desea, ingrese una descripción.
- Haga clic en **Next**.
- Para ¿Cuándo desea utilizar este conector?:

1. Elija: **Only when I have a transport rule set up that redirects messages to this connector**.

- Haga clic en **Next**.

- Haga clic en **Route email through these smart hosts**.
- Haga clic [+] e introduzca las direcciones IP o los nombres de host salientes proporcionados en la carta de bienvenida de CES.
- Haga clic en **Save**.
- Haga clic en **Next**.
- Para ¿Cómo debe conectarse Office 365 al servidor de correo electrónico de su organización partner?

1. Elija: **Always use TLS to secure the connection (recommended)**.

- ElijaAny digital certificate, including self-signed certificates.
- Haga clic en **Next**.
- Aparecerá la pantalla de confirmación.
- Haga clic en **Next**.
- Utilícelo [+] para introducir una dirección de correo electrónico válida y hacer clic en **OK**.
- Haga clic en **Validate** y deje que se ejecute la validación.
- Una vez completada, haga clic en **Close**.
- Haga clic enSave.

Un ejemplo de cómo se ve el conector de salida:



# Outbound to Cisco CES



## Mail flow scenario

From: Office 365

To: Partner organization

## Name

Outbound to Cisco CES

## Status

On



[Edit name or status](#)

## Use of connector

Use only when I have a transport rule set up that redirects messages to this connector.

[Edit use](#)

## Routing

Route email messages through these smart hosts:   .iphmx.com

[Edit routing](#)

## Security restrictions

Always use Transport Layer Security (TLS) and connect only if the recipient's email server has a digital certificate.

[Edit restrictions](#)

## Validation

Last validation result: Validation successful

Last validation time: 10/5/2020, 9:08 AM

[Validate this connector](#)



1. Para la ventana emergente de selección de ubicación del remitente, seleccione: **Inside the organization**.

- Haga clic en **OK**.
- Haga clic en **More options...**
- Haga clic en el **add condition** botón e inserte una segunda condición:

1. Elegir **The recipient...**

- Elija: **Is external/internal**.
- Para la ventana emergente de selección de ubicación del remitente, seleccione: **Outside the organization** .
- Haga clic en **OK**.
- Para *\*Haga lo siguiente...*, elija: **Redirect the message to...**

1. Seleccione: **el siguiente conector**.

2. Y seleccione el conector **Outbound to Cisco CES**.

3. Click OK.

- Vuelva a *"\*Haga lo siguiente..."* e inserte una segunda acción:


1. Elija: **Modify the message properties...**

- Elija: **set the message header**
- Defina el encabezado del mensaje: **X-OUTBOUND-AUTH**.
- Haga clic en **OK**.
- Defina el valor: **mysecretkey**.

- Haga clic en **OK**.

- Haga clic en **Save**.

---

 **Nota:** para evitar mensajes no autorizados de Microsoft, se puede estampar un x-encabezado secreto cuando los mensajes salen de su dominio de Microsoft 365; este encabezado se evalúa y se quita antes de enviarlo a Internet.

---

Un ejemplo de cómo se ve su configuración de Microsoft 365 Routing:

## Outbound to Cisco CES

Name:

Outbound to Cisco CES

\*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-OUTBOUND-AUTH](#)' to the value '[mysecretkey](#)'.

and

Use the following connector... ▼

[Outbound to Cisco CES](#)

add action

Except if...

add exception

Properties of this rule:

Priority:

0

Audit this rule with severity level:

Not specified ▼

Choose a mode for this rule:

Enforce

Test with Policy Tips

Test without Policy Tips

Activate this rule on the following date:

Fri 8/13/2021 ▼

1:30 PM ▼

Deactivate this rule on the following date:

Fri 8/13/2021 ▼

1:30 PM ▼

Stop processing more rules

Defer the message if rule processing doesn't complete

Match sender address in message:

Header ▼

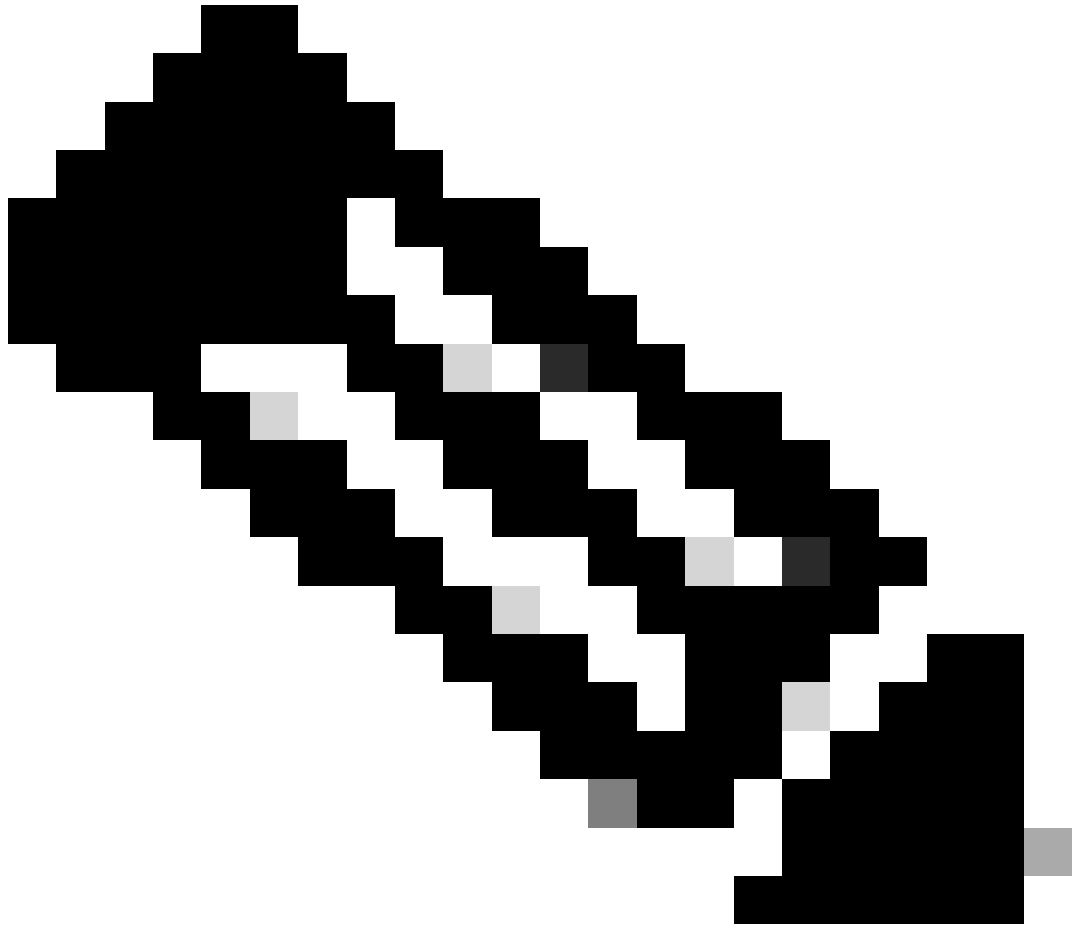
Add to DLP policy

PCI ▼

Comments:

```
office365_outbound: if sendergroup == "RELAYLIST" {  
  if header("X-OUTBOUND-AUTH") == "^mysecretkey$" {  
    strip-header("X-OUTBOUND-AUTH");  
  } else {  
    drop();  
  }  
}
```

- Presione Volver una vez para crear una nueva línea en blanco.
- Introduzca [.] en la nueva línea para finalizar el nuevo filtro de mensajes.
- Haga clic **return** una vez para salir del menú Filtros.
- Ejecute el **Commit** comando para guardar los cambios en la configuración.



**Nota:** evite los caracteres especiales de la clave secreta. Los caracteres ^ y \$ que se muestran en el filtro de mensajes son caracteres regex y se utilizan como se indica en el ejemplo.

---



**Nota:** Revise el nombre de la configuración de RELAYLIST. Se puede configurar con un nombre alternativo o puede tener un nombre específico basado en su política de retransmisión o proveedor de correo.

---

### Probar correo electrónico saliente

Pruebe el correo saliente de su dirección de correo electrónico de Microsoft 365 a un destinatario de dominio externo. Puede revisar el rastreo de mensajes desde Cisco Secure Email and Web Manager para asegurarse de que se enruta correctamente hacia el exterior.

---

 **Nota:** Revise la configuración de TLS (**Administración del sistema > Configuración SSL**) en la puerta de enlace y los cifrados

---



utilizados para SMTP saliente. Las prácticas recomendadas de Cisco recomiendan:

HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3DES:!SSLv2:!SSLv3

Un ejemplo de seguimiento con entrega exitosa:

Message Tracking

4 Filters | 1 Messages

Validate your RELAY Sender Group and Mail Flow Policy

IP address from Microsoft 365

Message Details	MID	Time	Outgoing Policy Match	Sender Group	Sender IP
Delivered	186371, 186372	13 Aug 2021 14:14:59 (GMT -04:00)	>>>_<<<<	RELAY_O365	59.175

Sender: @ Recipient: Subject: OUTBOUND EMAIL TEST SBRS Score: None

Haga clic **More Details** para ver los detalles completos del mensaje:

Message Tracking

Message ID Header <MN2PR13MB4007C16BF9B26CF89D340654FBFA9@MN2PR13MB4007.namprd13.prod.outlook.com>

Processing Details

Summary

Messages 186371, 186372

13 Aug 2021

- 14:14:59 Incoming connection (ICID 405417) has sender\_group: RELAY\_O365, sender\_ip: 59.175 and sbrs: not enabled
- 14:14:59 Protocol SMTP interface Data 2 (IP 57.36) on incoming connection (ICID 405417) from sender IP 59.175. Reverse DNS host mail-dm6nam12lp2175.outbound.protection.outlook.com verified yes.
- 14:14:59 (ICID 405417) RELAY sender group RELAY\_O365 match .protection.outlook.com SBRS not enabled country not enabled
- 14:14:59 Incoming connection (ICID 405417) successfully accepted TLS protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384.
- 14:14:59 Message 186371 Sender Domain: .com
- 14:14:59 Start message 186371 on incoming connection (ICID 405417).
- 14:14:59 Message 186371 enqueued on incoming connection (ICID 405417) from
- 14:14:59 Message 186371 direction: outgoing
- 14:14:59 Message 186371 on incoming connection (ICID 405417) added recipient ( ).
- 14:15:00 Message 186371 contains message ID header <MN2PR13MB4007C16BF9B26CF89D340654FBFA9@MN2PR13MB4007.namprd13.prod.outlook.com>

Envelope Header and Summary

Last State: Delivered

Message Outgoing

MID: 186371, 186372

Time: 13 Aug 2021 14:14:59 (GMT -04:00)

Sender: Recipient:

Sending Host Summary

Reverse DNS hostname: mail-dm6nam12lp2175.outbound.protection.outlook.com (verified)

IP address: 59.175

SBRS Score: None

Un ejemplo de seguimiento de mensajes donde el encabezado x no coincide:

Message Tracking

2 Filters | 100 Messages

Dropped By Message Filters

Message Details	MID	Time	Policy Match	Sender Group	Sender IP
Dropped By Message Filters	94011	13 Aug 2021 15:54:18 (GMT -04:00)	N/A	RELAY_O365	59.174

Sender: Recipient: Subject: OUTBOUND MAIL SBRS Score: None

Message ID Header <MN2PR13MB40076A4B89C400EEAC1618D4FBFA9@MN2PR13MB4007.namprd13.prod.outlook.com>

Processing Details

Summary

- 15:54:18 Incoming connection (ICID 137530) successfully accepted TLS protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384.
- 15:54:18 Message 94011 Sender Domain: bce-demo.com
- 15:54:18 Start message 94011 on incoming connection (ICID 137530).
- 15:54:18 Message 94011 enqueued on incoming connection (ICID 137530) from [redacted].
- 15:54:18 Message 94011 direction: outgoing
- 15:54:18 Message 94011 on incoming connection (ICID 137530) added recipient ([redacted]).
- 15:54:19 Message 94011 contains message ID header '<MN2PR13MB40076A4B89C400EEAC1618D4FBFA9@MN2PR13MB4007.namprd13.prod.outlook.com>'.  
Message 94011 original subject on injection: OUTBOUND MAIL 3:54PM POST-SECRET CHANGE
- 15:54:19 Message 94011 (7555 bytes) from [redacted] ready.
- 15:54:19 Message 94011 has sender\_group: RELAY\_O365, sender\_ip: [redacted].57.174 and sbrs: None
- 15:54:19 Incoming connection (ICID 137530) lost.
- 15:54:19 Message 94011 aborted: Dropped by filter 'office365\_outbound'

Note this was dropped by our specific Message Filter written earlier

Envelope Header and Summary

Last State  
Dropped By Message Filters

Message  
N/A

MID  
94011

Time  
13 Aug 2021 15:54:18 (GMT -04:00)

Sender  
[redacted]

Recipient  
[redacted]

Sending Host Summary

Reverse DNS hostname  
mail-dm6nam11lp2174.outbound.protection.outlook.com (verified)

IP address  
[redacted].57.174

SBRS Score  
None

## Información Relacionada

### Documentación de Cisco Secure Email Gateway

- [Release Notes](#)
- [Guía del usuario](#)
- [Guía de referencia de CLI](#)
- [Guías de programación de API para Cisco Secure Email Gateway](#)
- [Código abierto utilizado en Cisco Secure Email Gateway](#)
- [Guía de instalación del appliance virtual de seguridad de contenido de Cisco \(incluye vESA\)](#)

### Documentación de Secure Email Cloud Gateway

- [Release Notes](#)
- [Guía del usuario](#)

### Documentación de Cisco Secure Email and Web Manager

- [Notas de la versión y matriz de compatibilidad](#)



- [Guía del usuario](#)
- [Guías de programación de API para Cisco Secure Email y Web Manager](#)
- [Guía de instalación del appliance virtual de seguridad de contenido de Cisco](#) (incluye vSMA)

#### Documentación de productos de Cisco Secure

- [Arquitectura de nomenclatura de la cartera Cisco Secure](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).