Configuración de Microsoft 365 con correo electrónico seguro

Contenido

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 con su información de contacto y nombre de dominio en el servicio.

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

Organization Name: [redacted]
Start Date: 2022-09-09 05:09:04 America/Los_Angeles

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

MX Records for inbound email from Internet

- mx1.[redacted].iphmx.com
- mx2.[redacted].iphmx.com

Your Cisco CES portals:

Email Security
https://dh[redacted]-esa1.iphmx.com
Security Management
https://dh[redacted]-sma1.iphmx.com
End User Quarantine
https://dh[redacted]-euq1.iphmx.com

Please sign in the portals with this user ID:

Username: [redacted]
Password: [redacted]
Note: We recommend changing your password after the initial login.

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

Email Security:
[redacted].140.105
[redacted].150.143
[redacted].143.186
[redacted].32.98
Security Management:
[redacted].157.91

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

Host and IP address used for outbound relay from Office365 and G-Suite:
ob1.hc[redacted].iphmx.com

Include CES host and IP address in your SPF record:

v=spf1 exists:%{i}.spf.hc[redacted].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

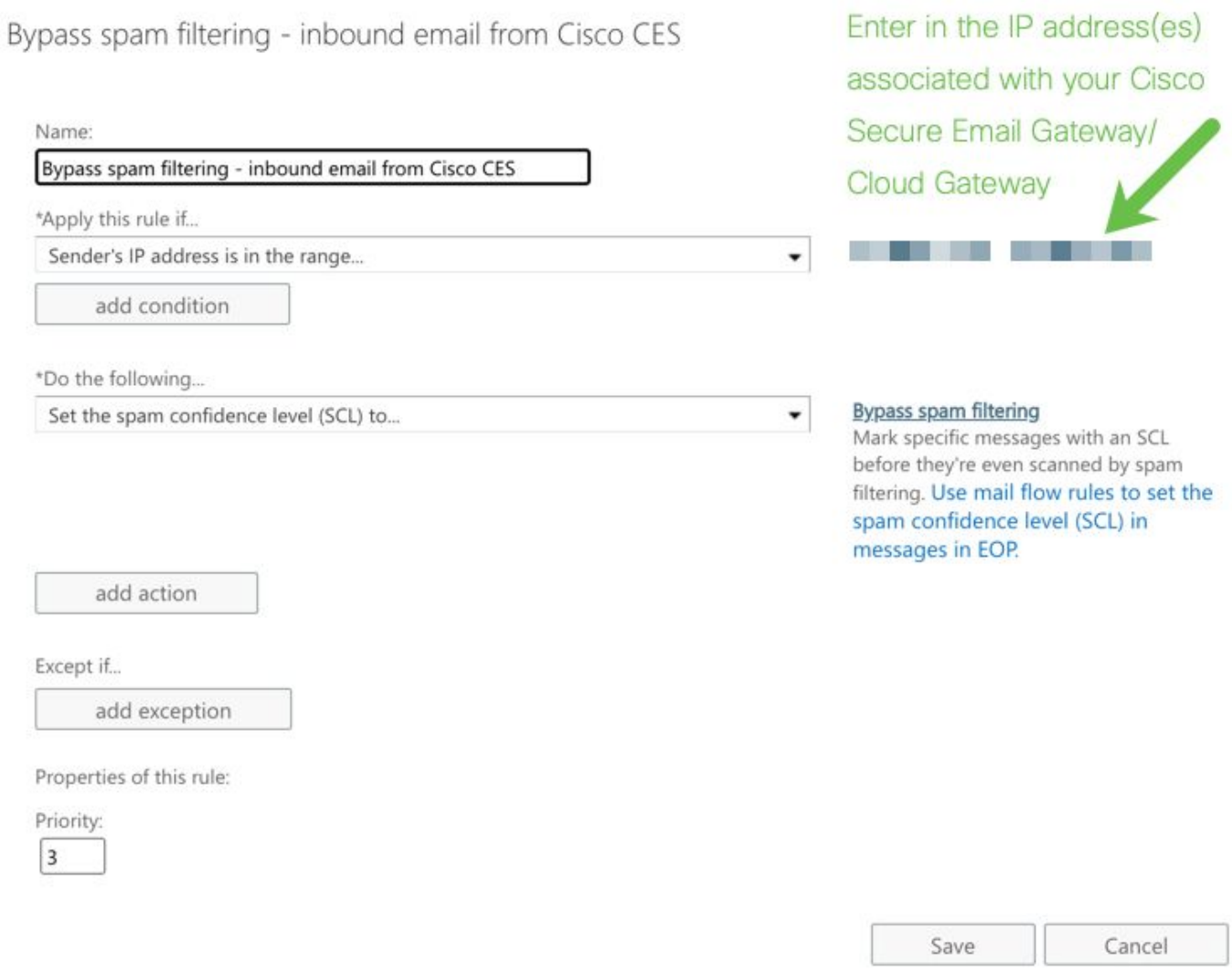
- Inicie sesión en el Centro de administración de Microsoft 365 (https://portal.microsoft.com).
- En el menú de la izquierda, expanda **Admin Centers**.
- Haga clic en **Exchange**.
- En el menú de la izquierda, vaya a **Mail flow > Rules**.
- Haga clic **[+]** para crear una nueva regla.
- Elija **Bypass 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:



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.

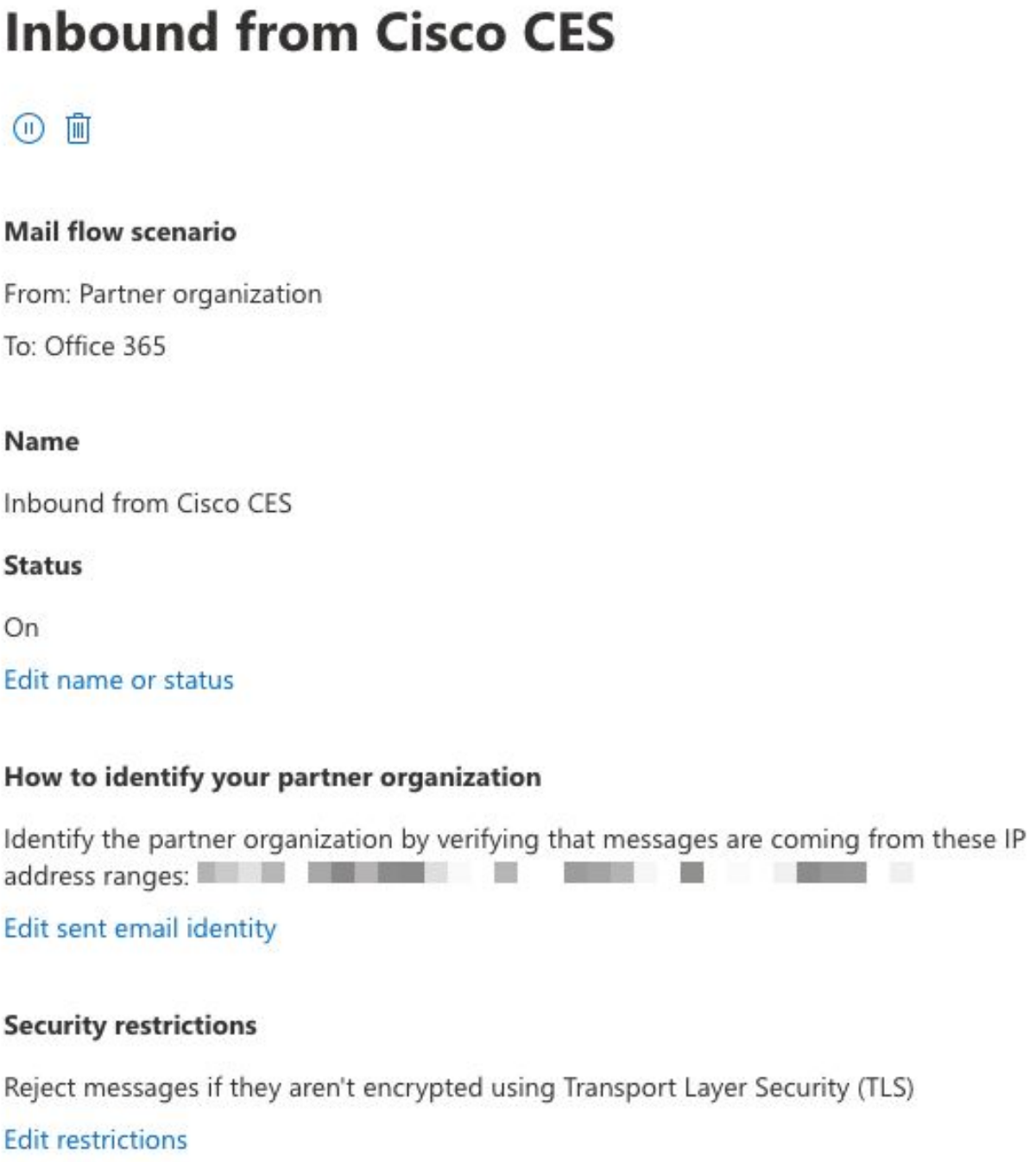
- En la ventana emergente Seleccione su escenario de flujo de correo, elija:

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:



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:

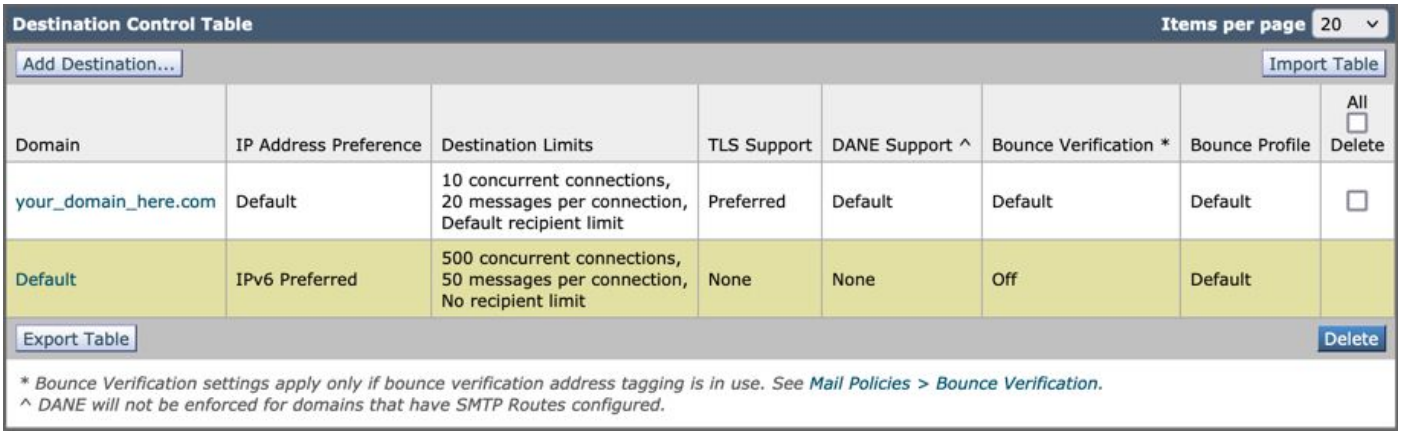


Tabla de acceso de destinatarios

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)**.

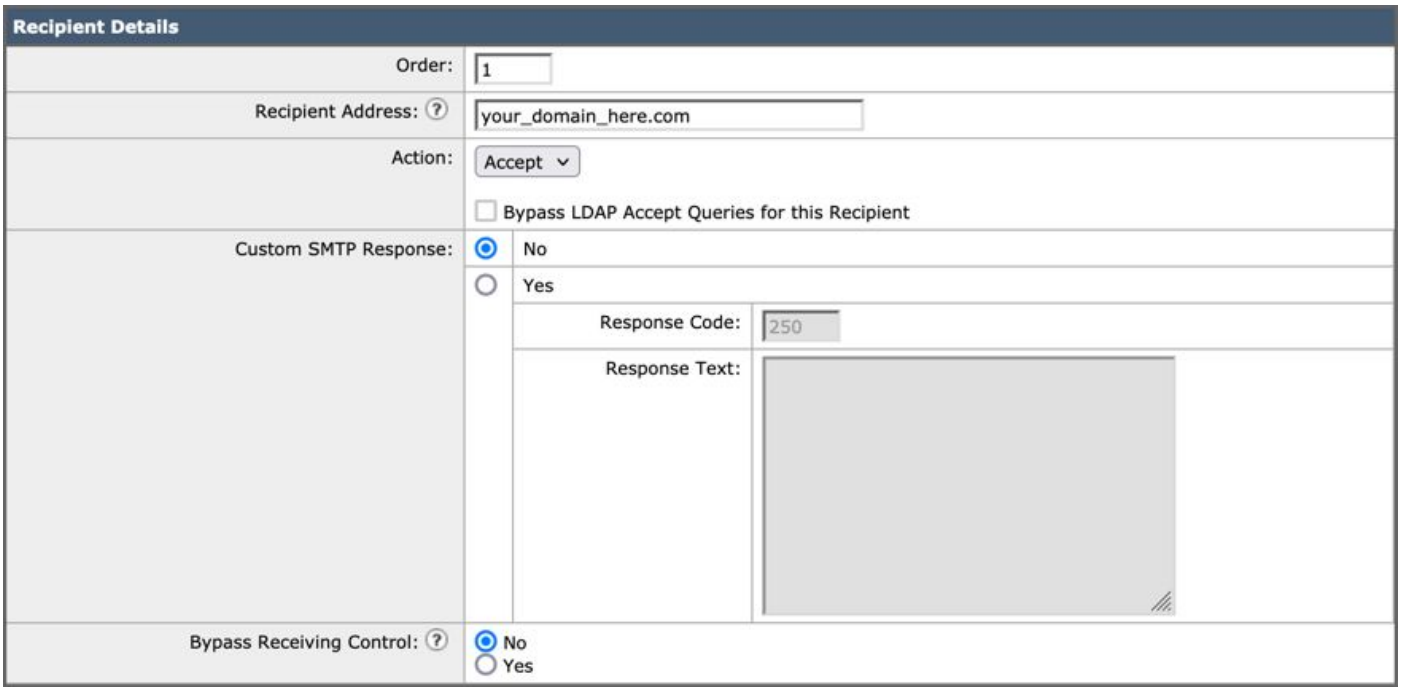
Nota: Asegúrese de que Listener es para Receptor Entrante, Correo Entrante o MailFlow, basándose en el nombre real de Listener para el flujo de correo principal.

- 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:



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...**

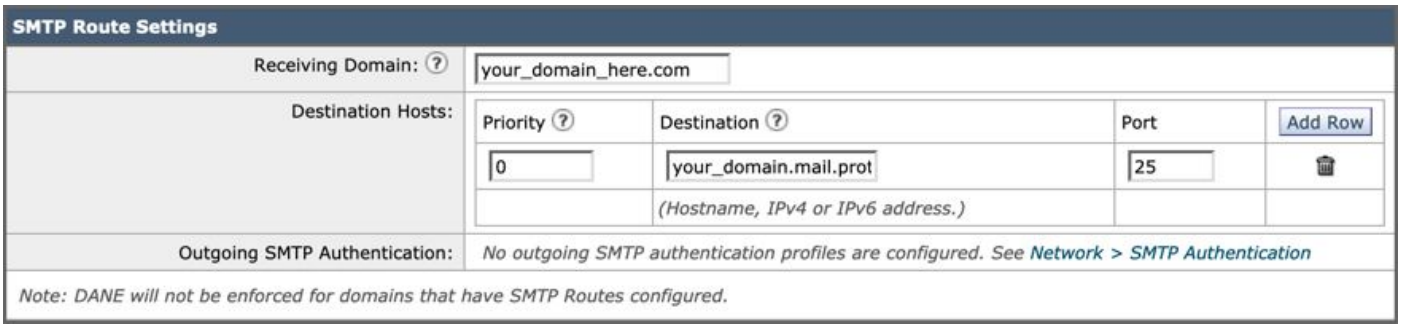
- Dominio de recepción: introduzca el nombre de dominio.

- 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:



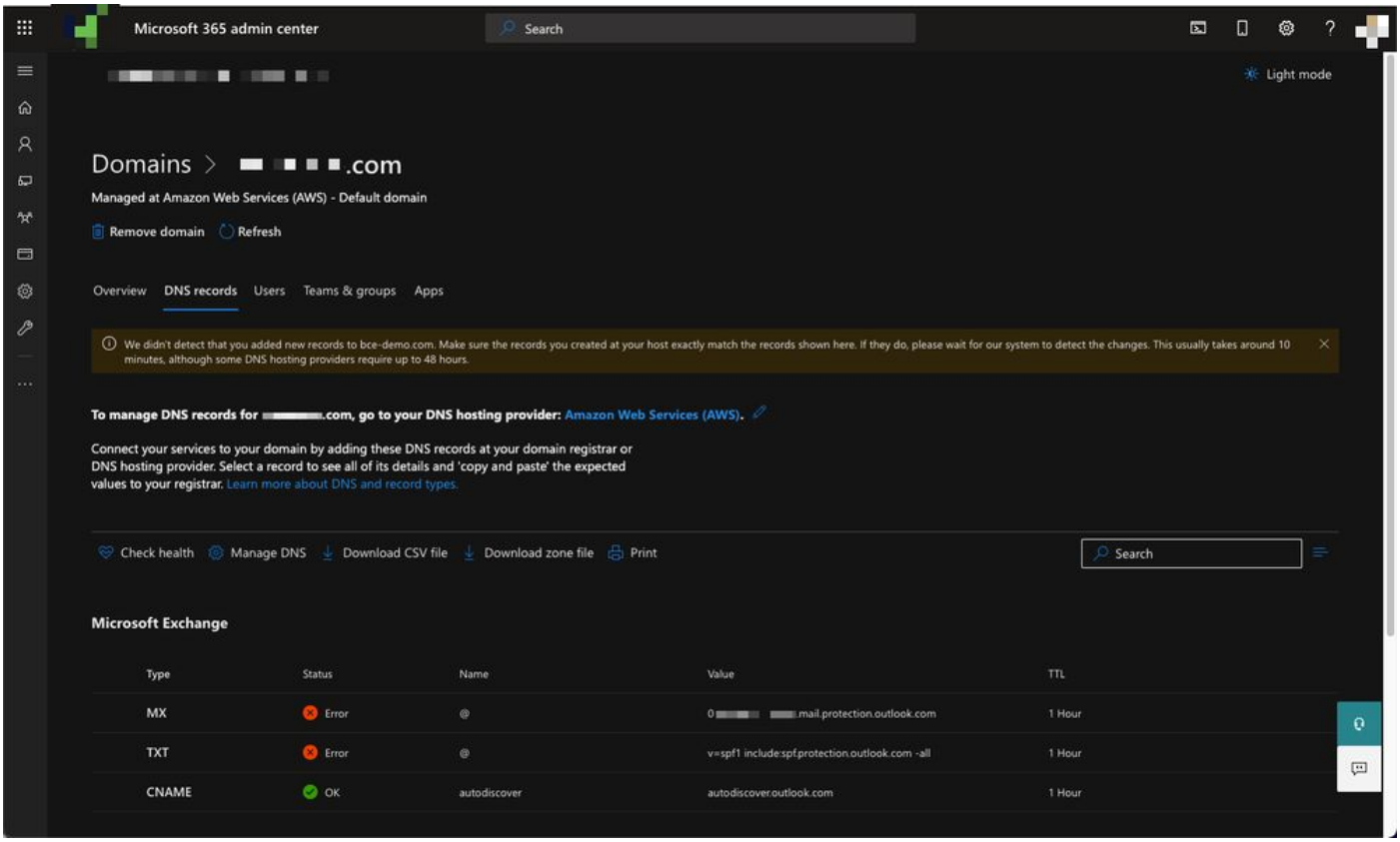
Configuración de DNS (registro MX)

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 enCheck Health.

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



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.

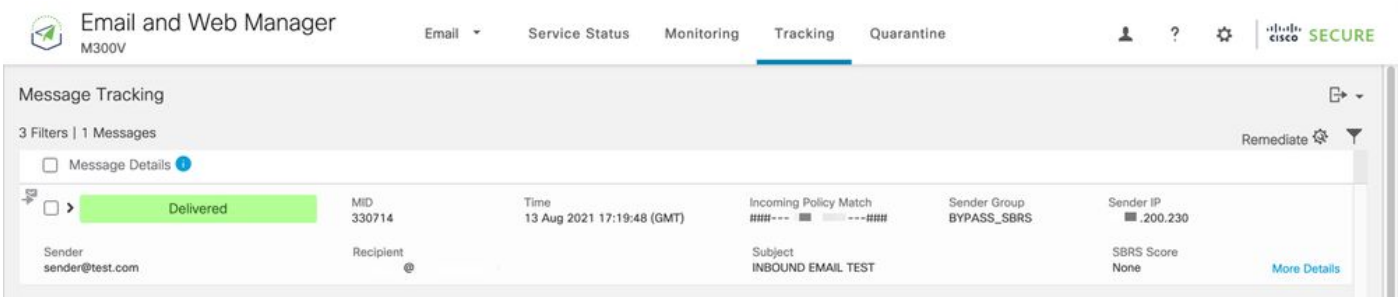
Probar correo electrónico entrante

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.

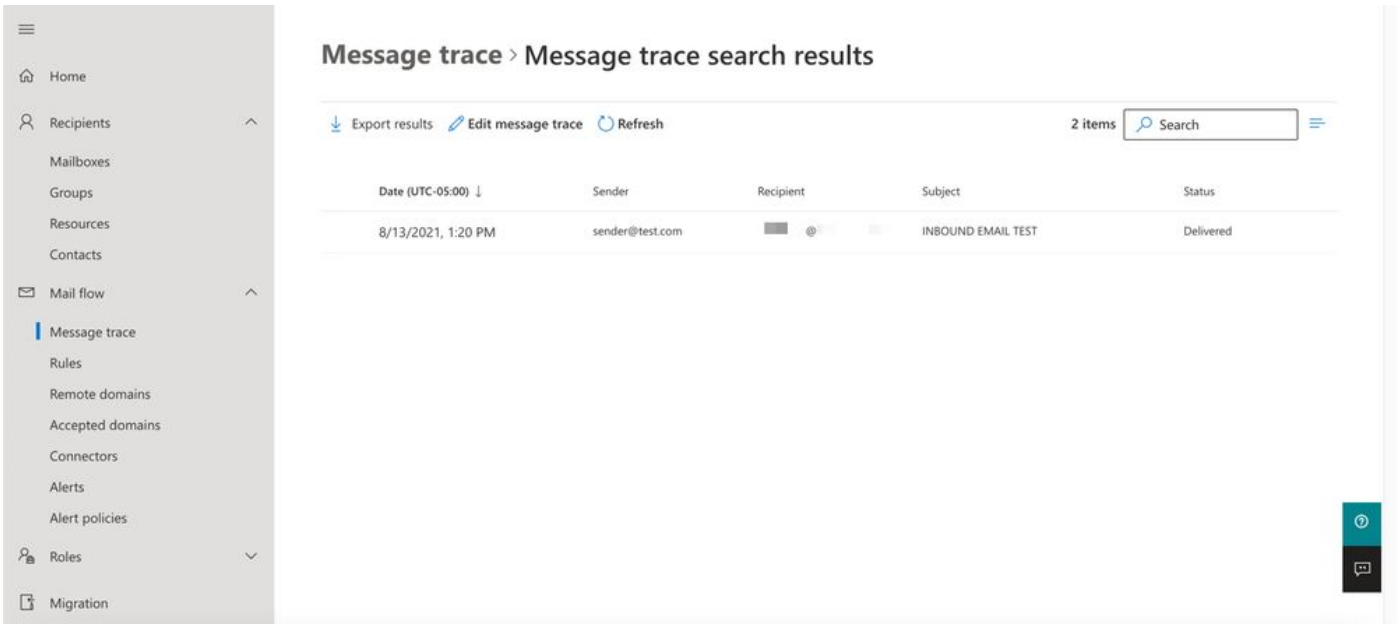
Para ver los registros de correo en su SMA:

- 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:



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** 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:



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:

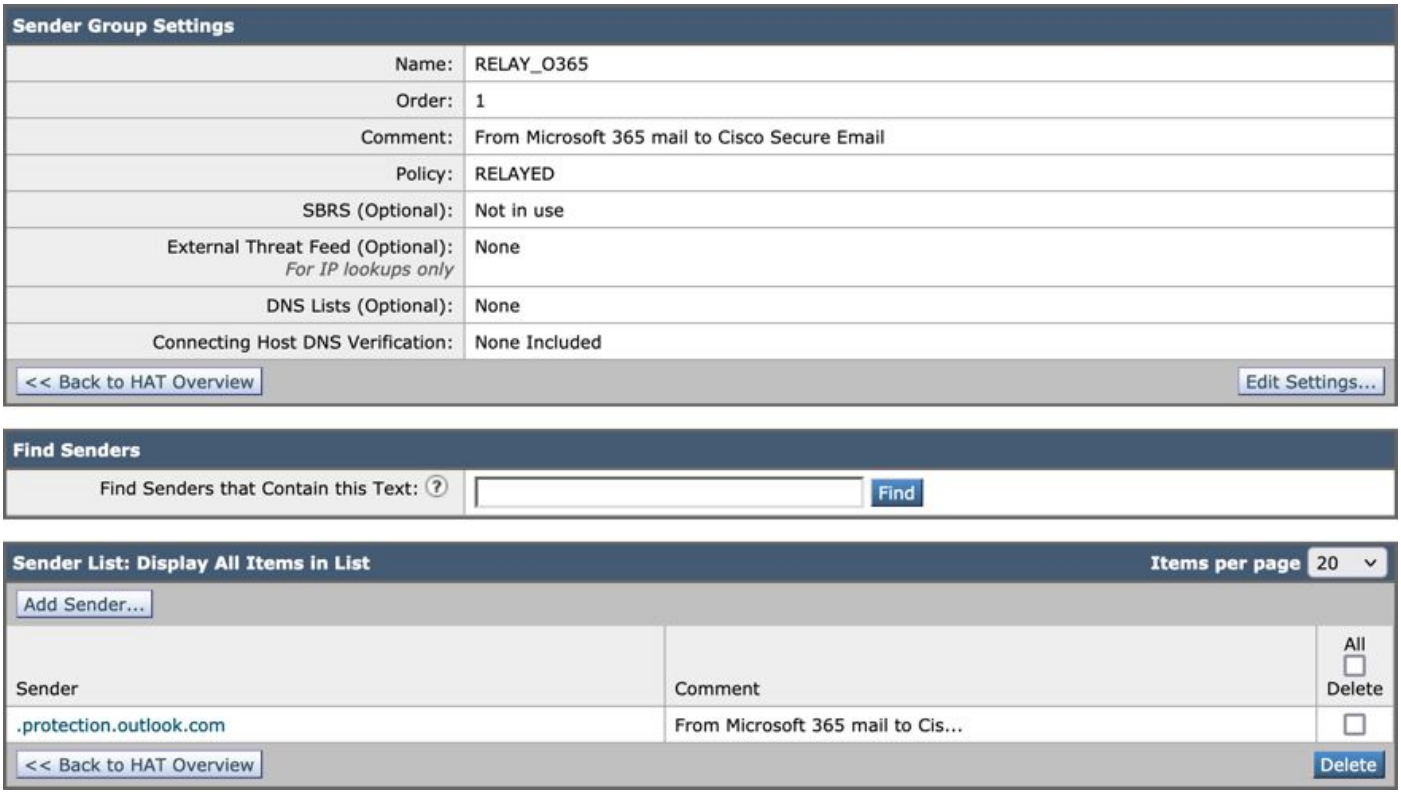
1. Nombre: RELAY_O365
2. Comentario: <<enter a comment if you wish to notate your sender group>>
3. Política: RETRANSMITIDA
4. Haga clic en **Submit and Add Senders**.

- 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.

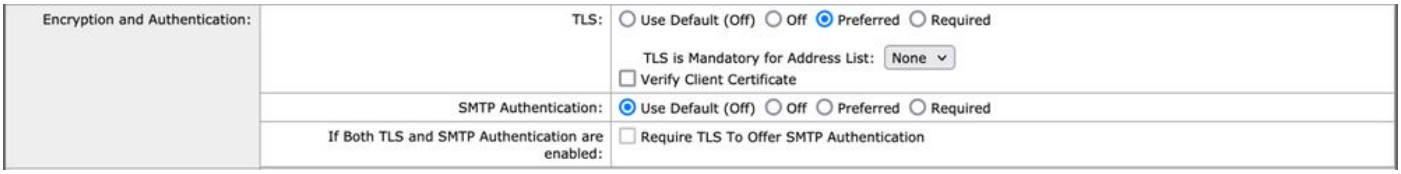
Un ejemplo de cómo se ve su configuración de Grupo de Remitentes:



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:



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: [redacted].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

Crear una regla de flujo de correo

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

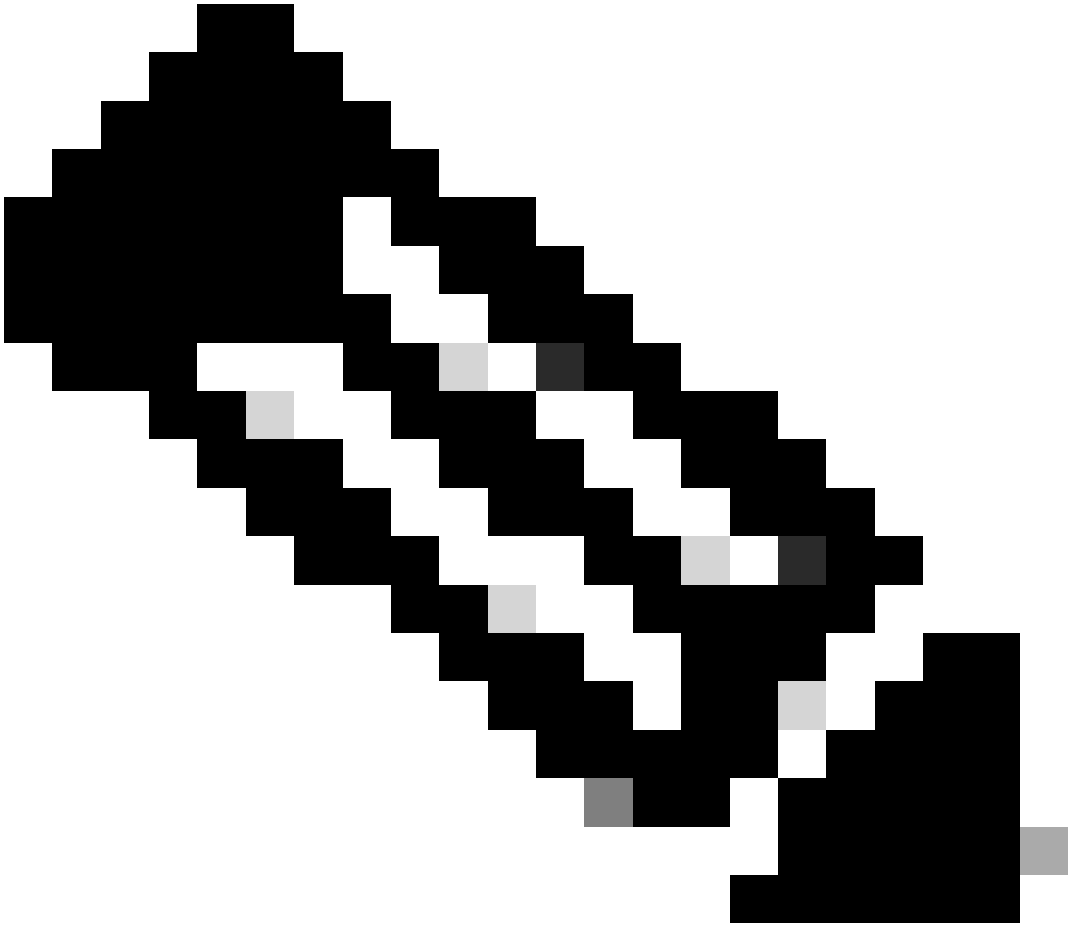
PCI

Comments:

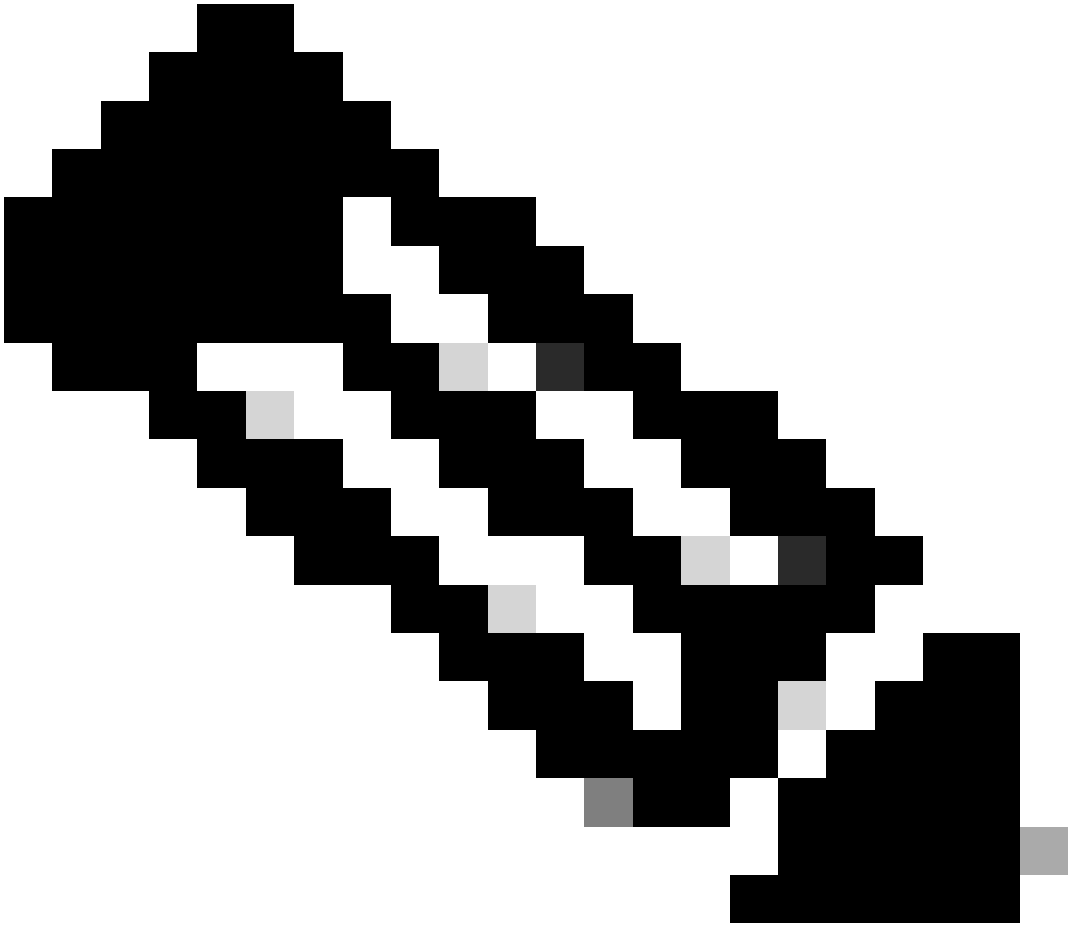
ℹ Rights Management Services (RMS) is a premium feature that requires an Enterprise Client Access License (CAL) or a RMS Online license for each user mailbox. Learn more

```
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

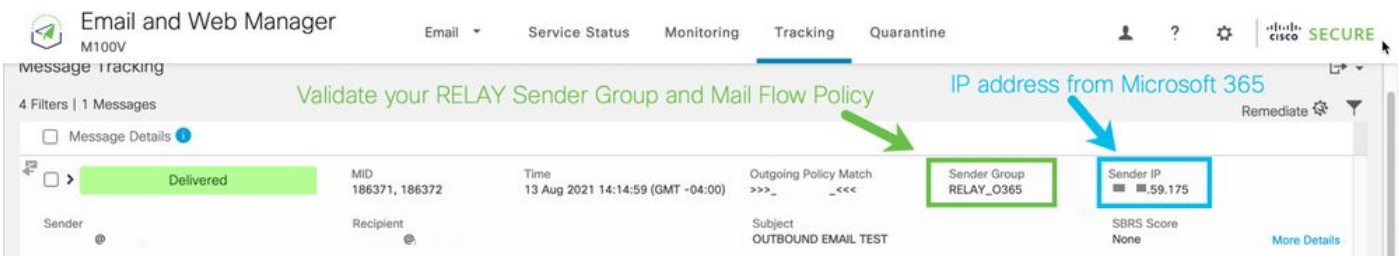
Pruebe el correo saliente de su dirección de correo electrónico de Microsoft 365 a un destinatario de dominio externo. Puede revisar el rastreo de mensajes desde Cisco Secure Email and Web Manager para asegurarse de que se enruta correctamente hacia el exterior.

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

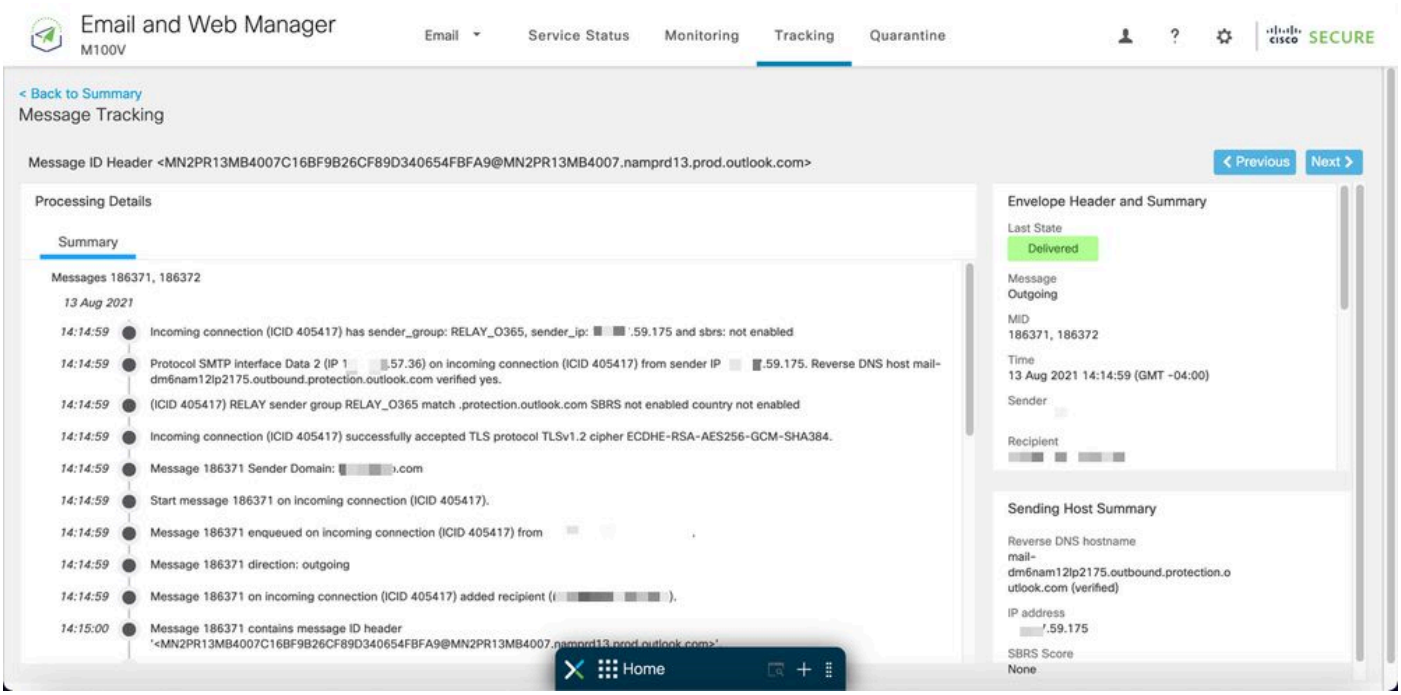
utilizados para SMTP saliente. Las prácticas recomendadas de Cisco recomiendan:

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

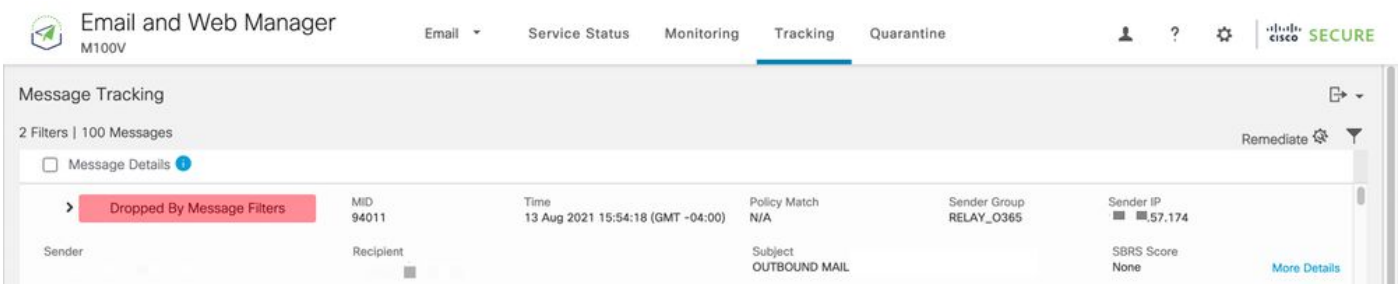
Un ejemplo de seguimiento con entrega exitosa:

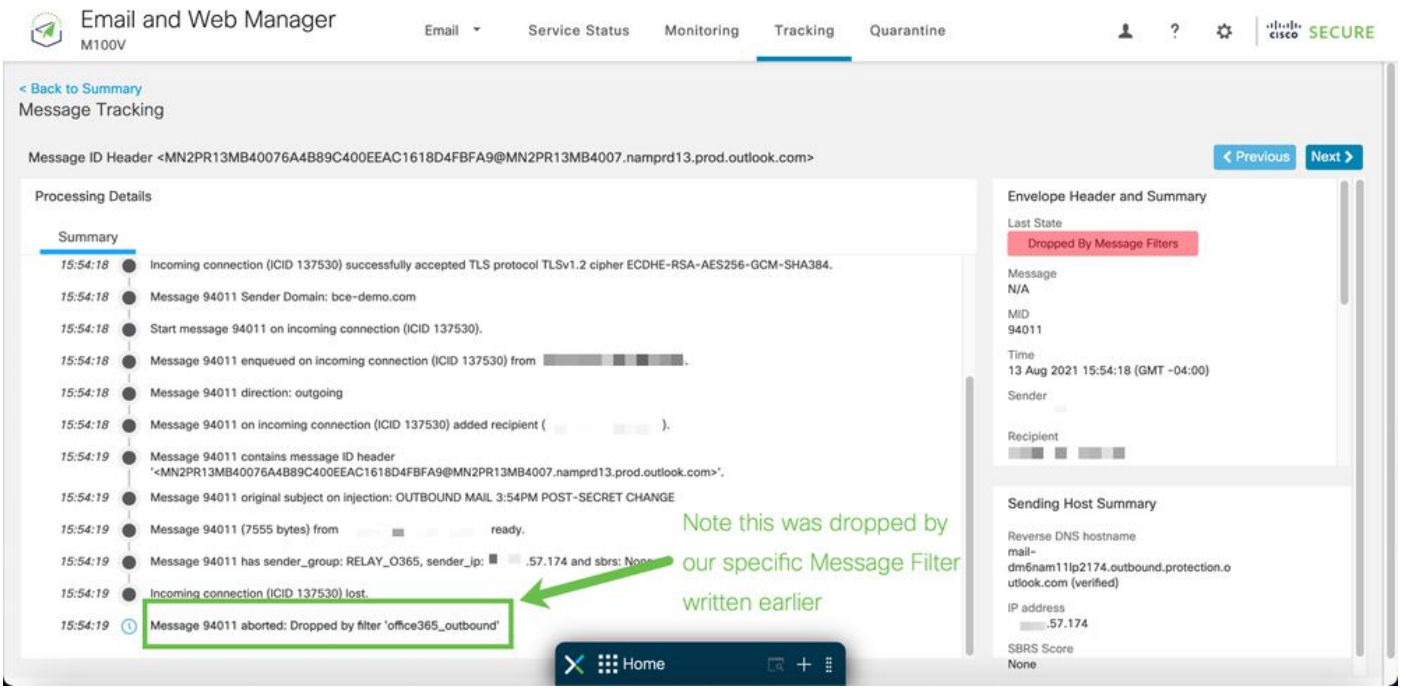


Haga clic **More Details** para ver los detalles completos del mensaje:



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





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).