Configurazione di Microsoft 365 con Secure Email

Sommario

Introduzione

In questo documento viene descritta la configurazione necessaria per integrare Microsoft 365 con Cisco Secure Email per il recapito dei messaggi e-mail in entrata e in uscita.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Email Gateway o Cloud Gateway
- Accesso CLI (Command Line Interface) all'ambiente Cisco Secure Email Cloud Gateway: Cisco Secure Email Cloud Gateway > Accesso all'interfaccia della riga di comando (CLI)
- Microsoft 365
- Protocollo SMTP (Simple Mail Transfer Protocol)
- DNS (Domain Name Server)

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questo documento può essere usato sia per i gateway locali che per i Cisco Cloud Gateway.

Se si è un amministratore di Cisco Secure Email, la lettera di benvenuto include gli indirizzi IP del gateway cloud e altre informazioni pertinenti. Oltre alla lettera che vedi qui, ti viene inviata un'e-mail crittografata che ti fornisce ulteriori dettagli sul numero di Cloud Gateway (anche noto come ESA) e Cloud Email e Web Manager (anche noto come SMA) forniti per la tua allocazione. Se non è stata ricevuta o non si dispone di una copia della lettera, contattare ces-activations@cisco.com specificando le informazioni di contatto e il nome di dominio.

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

Ogni client dispone di IP dedicati. È possibile usare gli indirizzi IP o i nomi host assegnati nella configurazione di Microsoft 365.

Nota: si consiglia di eseguire il test prima di qualsiasi interruzione pianificata della posta di produzione, in quanto le configurazioni richiedono tempo per la replica nella console Microsoft 365 Exchange. Consentire almeno un'ora per rendere effettive tutte le modifiche.

Nota: gli indirizzi IP nell'acquisizione schermo sono proporzionali al numero di gateway cloud forniti per l'allocazione. Ad esempio, xxx.yy.140.105 è l'indirizzo IP dell'interfaccia Data 1 per il Gateway 1 ed xxx.yy.150.1143 è l'indirizzo IP dell'interfaccia Data 1 per il Gateway 2. L'indirizzo IP dell'interfaccia dati 2 per il gateway 1 è xxx.yy.143.186 e l'indirizzo IP dell'interfaccia dati 2 per il gateway 2 è xxx.yy.32.98. Se la lettera di benvenuto non include informazioni per Data 2 (Outgoing interface IPs), contattare Cisco TAC per richiedere l'aggiunta dell'interfaccia Data 2 all'allocazione.

Configurazione di Microsoft 365 con Secure Email

Configurazione delle e-mail in arrivo in Microsoft 365 da Cisco Secure Email

Regola Ignora il filtro posta indesiderata

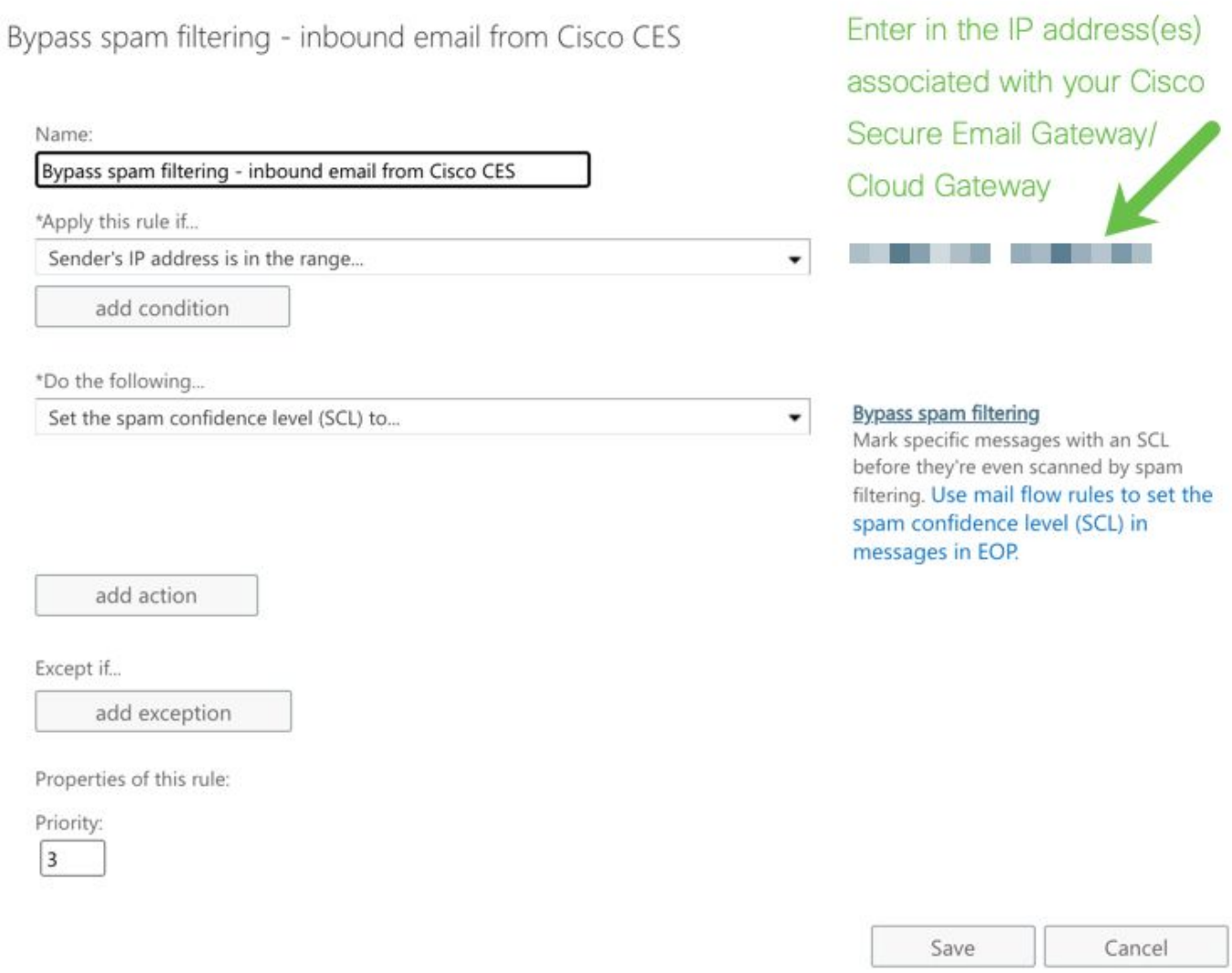
- Accedere a Microsoft 365 Admin Center (https://portal.microsoft.com).
- Nel menu a sinistra, espandere **Admin Centers**.
- Fare clic su **Exchange**.
- Dal menu a sinistra, passare a **Mail flow > Rules**.
- Fare clic **[+]** per creare una nuova regola.
- Selezionare **Bypass spam filtering...** una voce dall'elenco a discesa.
- Immettere un nome per la nuova regola: **Bypass spam filtering - inbound email from Cisco CES**.
- Per *Applicare questa regola se..., scegliere **The sender - IP address is in any of these ranges or exactly matches**.

1. Per visualizzare la schermata di popup specifica intervalli di indirizzi IP, aggiungere gli indirizzi IP forniti nella lettera di benvenuto di Cisco Secure Email.
2. Fare clic su **OK**.

- Per *Fare quanto segue..., la nuova regola è stata preselezionata: **Set the spam confidence level (SCL) to... - Bypass spam filtering**.

- Fare clic su **Save**.

Esempio di regola:



Connettore di ricezione

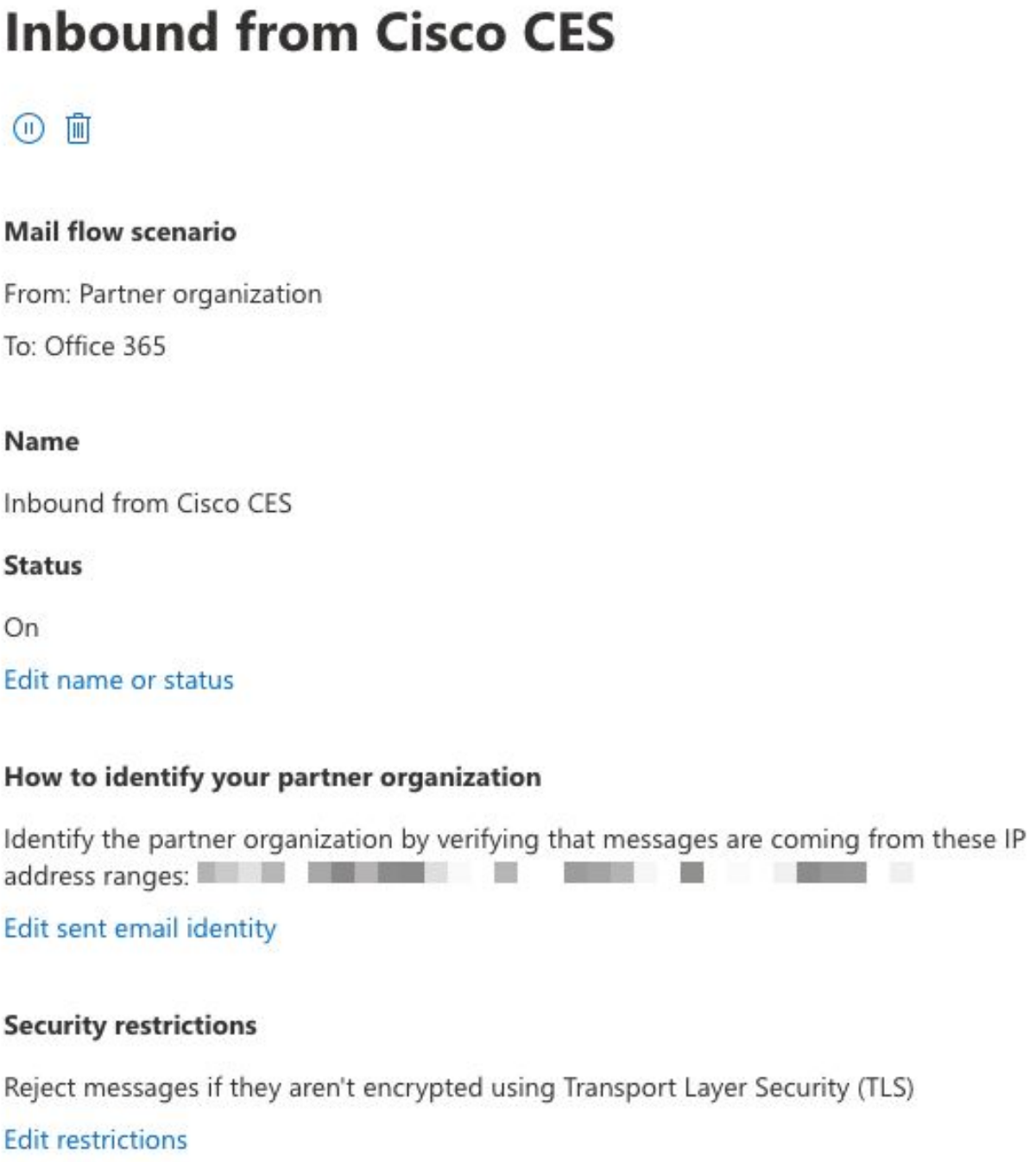
- Rimanere nell'interfaccia di amministrazione di Exchange.
- Dal menu a sinistra, passare a **Mail flow > Connectors**.
- Fare clic **[+]** per creare un nuovo connettore.
- Nella finestra popup Selezionare lo scenario del flusso di posta, scegliere:

1. Da: Partner organization

    - A: **Office365**

- Fare clic su **Next**.
- Immettere un nome per il nuovo connettore: **Inbound from Cisco CES**.
- Se desiderato, immettere una descrizione.
- Fare clic su **Next**.
- Fare clic su **Use the sender's IP address**.
- Fare clic su **Next**.
- Fare clic **[+]** e immettere gli indirizzi IP indicati nella lettera di benvenuto di Cisco Secure Email.
- Fare clic su **Next**.
- Scegli **Reject email messages if they aren't sent over Transport Layer Security (TLS)**.
- Fare clic su **Next**.
- Fare clic su **Save**.

Di seguito è riportato un esempio della configurazione del connettore:



Configurazione delle e-mail inviate da Cisco Secure Email a Microsoft 365

Controlli di destinazione

Imporre un'autoaccelerazione a un dominio di recapito nei controlli di destinazione. Naturalmente, è possibile rimuovere la limitazione in seguito, ma si tratta di nuovi IP per Microsoft 365 e non si desidera alcuna limitazione da parte di Microsoft a causa della sua reputazione sconosciuta.

- Accedere al gateway.
- Passa a **Mail Policies > Destination Controls**.
- Fare clic su **Add Destination**.

- Utilizzo:

1. Destinazione: immettere il nome di dominio

2. Connessioni simultanee: **10**

   - Numero di messaggi massimo per connessione: **20**
   - Supporto TLS: **Preferred**

- Fare clic su **Submit**.

- Fare clic su **Commit Changes** nell'angolo superiore destro dell'interfaccia utente per salvare le modifiche apportate alla configurazione.

Esempio di tabella di controllo di destinazione:

Destination Control Table — Items per page: 20

Add Destination... | Import Table

Domain	IP Address Preference	Destination Limits	TLS Support	DANE Support ^	Bounce Verification *	Bounce Profile	All Delete
your_domain_here.com	Default	10 concurrent connections, 20 messages per connection, Default recipient limit	Preferred	Default	Default	Default	☐
Default	IPv6 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	None	None	Off	Default	

Export Table | Delete

** 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.

Tabella di accesso destinatari

Impostare quindi la tabella di accesso destinatari, o RAT (Recipient Access Table), per accettare l'e-mail nei tuoi domini:

- Passa a **Mail Policies > Recipient Access Table (RAT)**.

Nota: assicurarsi che il listener sia per il listener in arrivo, IncomingMail o MailFlow, in base al nome effettivo del listener per il flusso di posta principale.

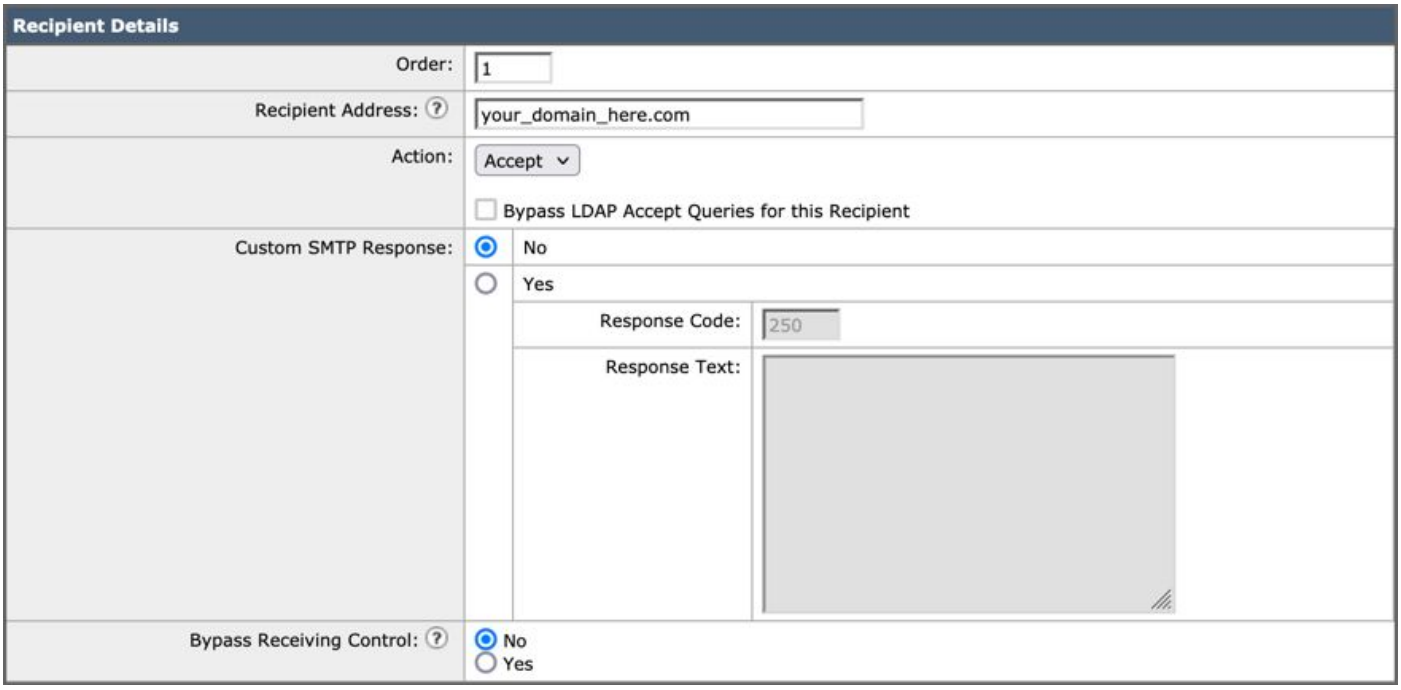
- Fare clic su **Add Recipient**.

- Aggiungere i domini nel campo Indirizzo destinatario.

- Scegliere l'azione predefinita di **Accept**.

- Fare clic su **Submit**.
- Fare clic su **Commit Changes** nell'angolo superiore destro dell'interfaccia utente per salvare le modifiche alla configurazione.

Ecco un esempio di come appare la voce RAT:

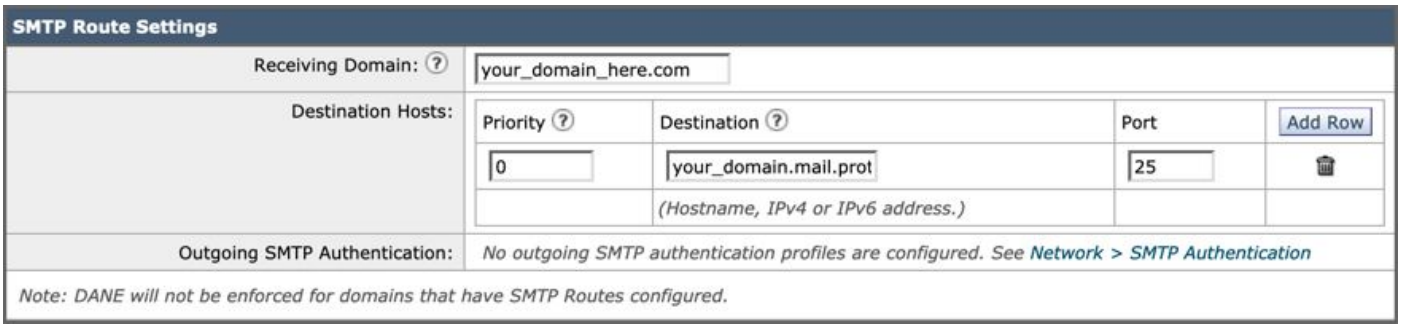


Route SMTP

Impostare il percorso SMTP per il recapito della posta da Cisco Secure Email al dominio Microsoft 365:

- Passa a **Network > SMTP Routes**.
- Fare clic su **Add Route...**
- Dominio di ricezione: immettere il nome di dominio.
- Host di destinazione: aggiungere il record Microsoft 365 MX originale.
- Fare clic su **Submit**.
- Fare clic su **Commit Changes** nell'angolo superiore destro dell'interfaccia utente per salvare le modifiche alla configurazione.

Di seguito è riportato un esempio di impostazioni di route SMTP:



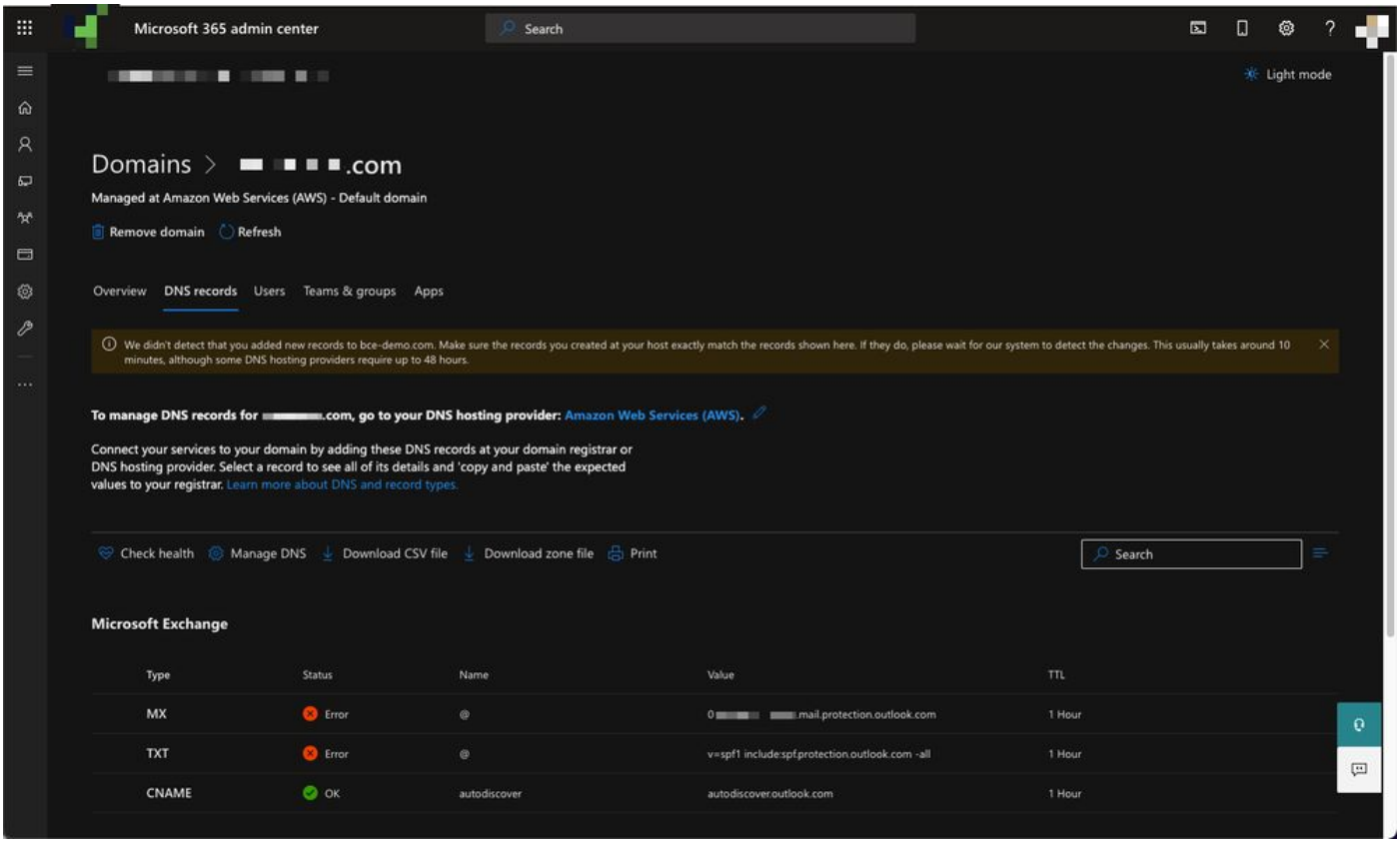
Configurazione DNS (record MX)

È ora possibile tagliare il dominio tramite una modifica del record di Mail Exchange (MX). Rivolgersi all'amministratore DNS per risolvere i record MX negli indirizzi IP dell'istanza di Cisco Secure Email Cloud, come indicato nella lettera di benvenuto di Cisco Secure Email.

Verificare la modifica apportata al record MX anche dalla console Microsoft 365:

- Accedere alla console di amministrazione di Microsoft 365 (https://admin.microsoft.com).
- Passa a **Home > Settings > Domains**.
- Scegliere il nome di dominio predefinito.
- Fare clic su Check Health.

Questo fornisce i record MX correnti di come Microsoft 365 cerca i record DNS e MX associati al tuo dominio:



Nota: in questo esempio, il DNS è ospitato e gestito da Amazon Web Services (AWS). In qualità di amministratore, è probabile che venga visualizzato un avviso se il DNS è ospitato in un punto qualsiasi al di fuori dell'account Microsoft 365. È possibile ignorare avvisi quali: "Non è stato rilevato che hai aggiunto nuovi record a your_domain_here.com. Verifica che i documenti che hai creato sull'host corrispondano a quelli mostrati qui..." Le istruzioni dettagliate reimpostano i record MX su quello che era stato inizialmente configurato per il reindirizzamento all'account Microsoft 365. In questo modo Cisco Secure Email Gateway viene rimosso dal flusso del traffico in entrata.

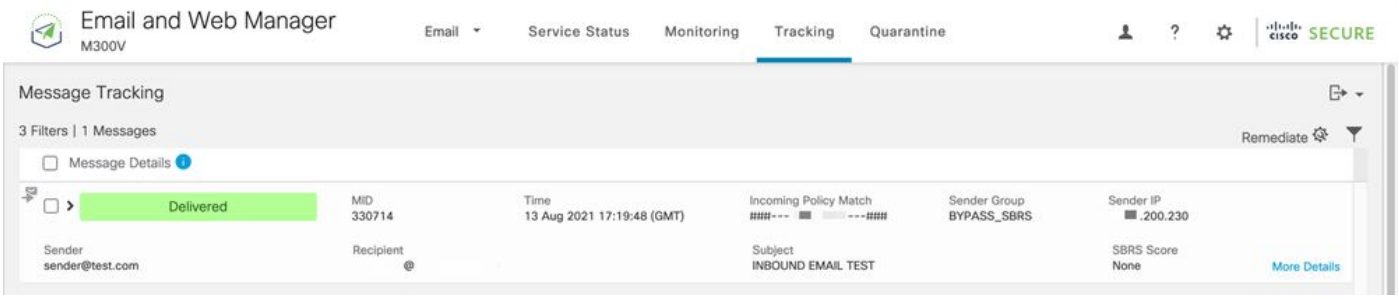
Test posta in arrivo

Prova la posta in arrivo sul tuo indirizzo e-mail Microsoft 365. Quindi, verificare che arrivi nella Posta in arrivo di Microsoft 365.

Convalidare i log di posta in Verifica messaggi su Cisco Secure Email e Web Manager (noto anche come SMA) forniti con l'istanza.

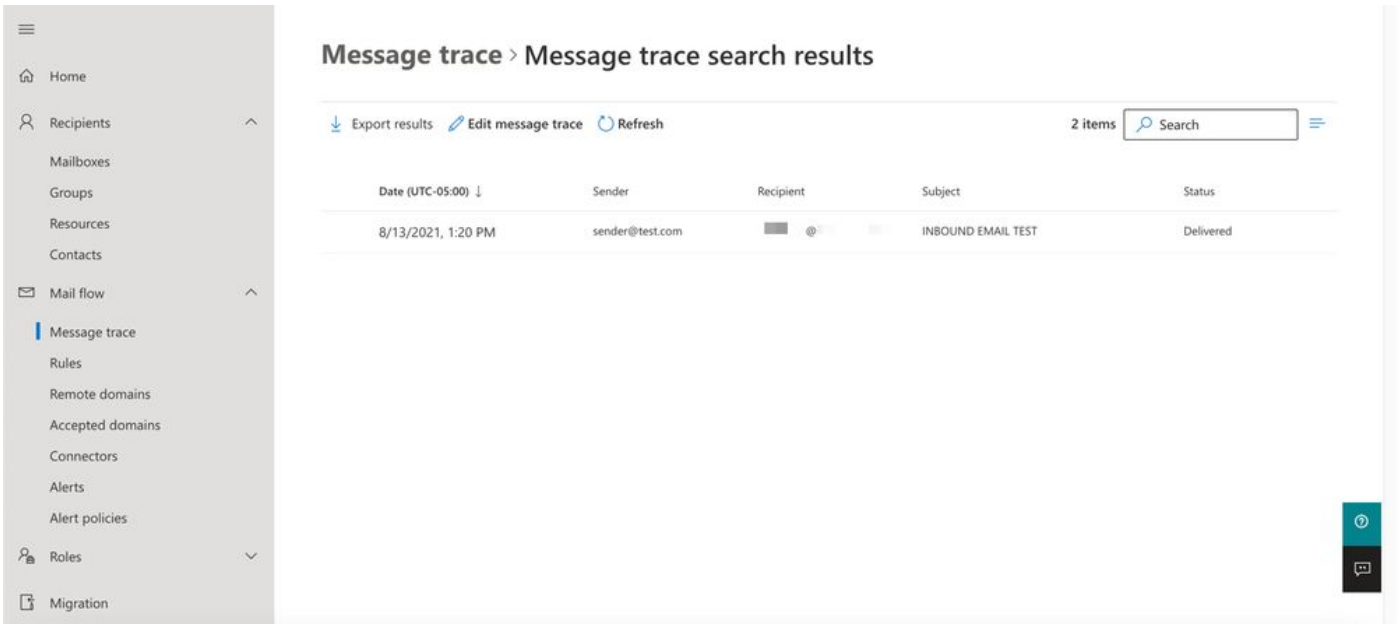
Per visualizzare i log di posta su SMA:

- Accedere all'SMA (https://sma.iphmx.com/ng-login).
- Fare clic su **Tracking**.
- Immettere i criteri di ricerca necessari e fare clic su **Search**; e si prevede di visualizzare tali risultati:



Per visualizzare i log di posta in Microsoft 365:

- Accedere a Microsoft 365 Admin Center (https://admin.microsoft.com).
- Espansione **Admin Centers**.
- Fare clic su **Exchange**.
- Passa a **Mail flow > Message trace**.
- In Microsoft sono disponibili i criteri predefiniti per la ricerca. Ad esempio, scegliere **Messages received by my primary domain in the last day** di avviare la query di ricerca.
- Immettere i criteri di ricerca necessari per i destinatari e fare clic su **Search** e prevedere risultati simili a:



Configurazione delle e-mail in uscita da Microsoft 365 a Cisco Secure Email

Configurazione di RELAYLIST su Cisco Secure Email Gateway

Fare riferimento alla lettera di benvenuto di Cisco Secure Email. Inoltre, viene specificata un'interfaccia secondaria per i messaggi in uscita tramite il gateway.

- Accedere al gateway.
- Passa a **Mail Policies > HAT Overview**.

Nota: assicurarsi che il listener sia per il listener in uscita, OutgoingMail o MailFlow-Ext, in base al nome effettivo del listener per il flusso di posta esterno/in uscita.

- Fare clic su **Add Sender Group...**
- Configurare il gruppo di mittenti come:

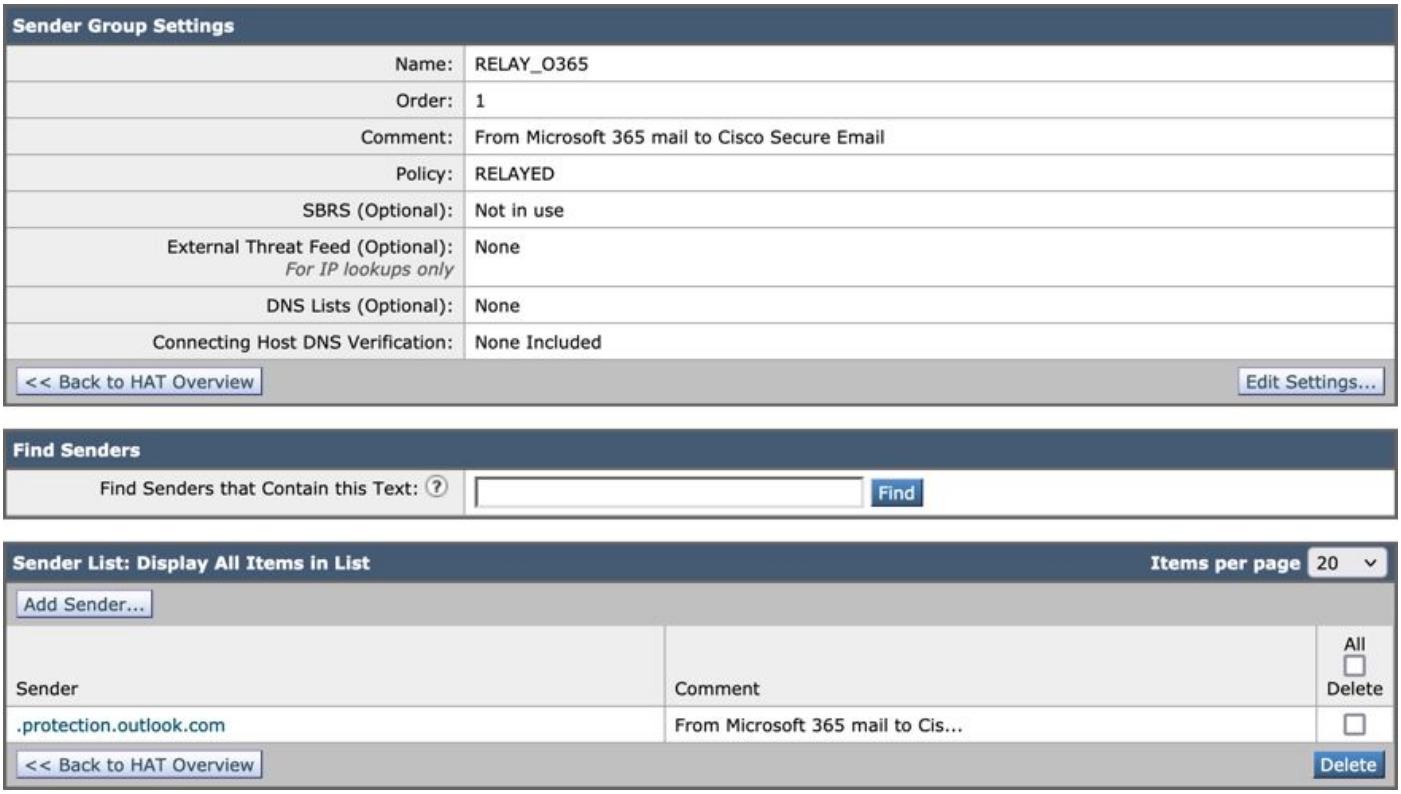
1. Nome: RELAY_O365
2. Commento: <<immettere un commento se si desidera inviare una nota al gruppo di mittenti>>
3. Criterio: INOLTRATO
4. Fare clic su **Submit and Add Senders**.

- Mittente: **.protection.outlook.com**

Nota: il **file.** (punto) all'inizio del nome di dominio del mittente è obbligatorio.

- Fare clic su **Submit**.
- Fare clic su **Commit Changes** nell'angolo superiore destro dell'interfaccia utente per salvare le modifiche alla configurazione.

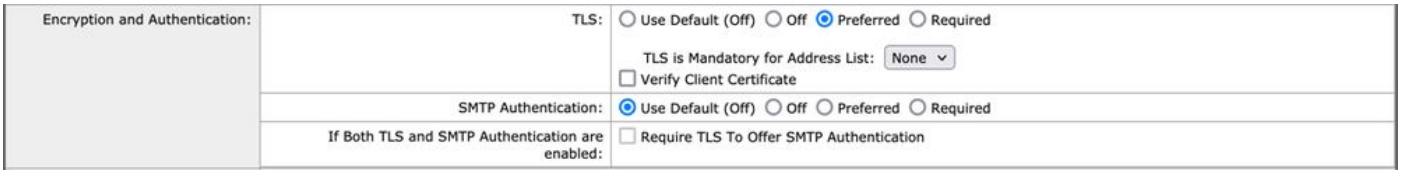
Di seguito è riportato un esempio di impostazioni del gruppo di mittenti:



Abilitazione TLS

- Fare clic su **<<Back to HAT Overview**.
- Fare clic sulla Policy di flusso con nome: **RELAYED**.
- Scorrere verso il basso e cercare nella **Security Features** sezione **Encryption and Authentication**.
- Per TLS, selezionare: **Preferred**.
- Fare clic su **Submit**.
- Fare clic su **Commit Changes** nell'angolo superiore destro dell'interfaccia utente per salvare le modifiche alla configurazione.

Esempio di configurazione dei criteri di flusso della posta:



Configurazione dell'e-mail da Microsoft 365 a CES

- Accedere a Microsoft 365 Admin Center (https://admin.microsoft.com).
- Espansione **Admin Centers**.
- Fare clic su **Exchange**.
- Passa a **Mail flow > Connectors**.
- Fare clic su[+] per creare un nuovo connettore.
- Nella finestra popup Selezionare lo scenario del flusso di posta, scegliere:

1. Da: Office365
    - A:Partner organization

- Fare clic su **Next**.
- Immettere un nome per il nuovo connettore: **Outbound to Cisco CES**.
- Se desiderato, immettere una descrizione.
- Fare clic su **Next**.
- Per Quando si desidera utilizzare questo connettore:

1. Scegli: **Only when I have a transport rule set up that redirects messages to this connector**.
    - Fare clic su **Next**.

- Fare clic su **Route email through these smart hosts**.

- Fare clic su **[+]** e immettere gli indirizzi IP in uscita o i nomi host forniti nella lettera di benvenuto del CES.
- Fare clic su **Save**.
- Fare clic su **Next**.
- Per stabilire la connessione di Office 365 al server di posta elettronica dell'organizzazione partner,

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

    - SceglieteAny digital certificate, including self-signed certificates.
    - Fare clic su **Next**.

- Viene visualizzata la schermata di conferma.
- Fare clic su **Next**.
- Utilizzare **[+]** per immettere un indirizzo e-mail valido e fare clic su **OK**.
- Fare clic su **Validate** e consentire l'esecuzione della convalida.
- Al termine, fare clic su **Close**.
- Fare clic su Save.

Di seguito è riportato un esempio dell'aspetto del connettore in uscita:

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

Regola Crea un flusso di posta

1. Per il popup di selezione della località del mittente, scegliere: **Inside the organization**.

    - Fare clic su **OK**.

- Fare clic su **More options...**
- Fare clic su **add condition** Pulsante e inserire una seconda condizione:

    1. Scegli **The recipient...**

        - Scegli: **Is external/internal**.
        - Per il popup di selezione della località del mittente, scegliere: **Outside the organization** .
        - Fare clic su **OK**.

- Per *Fare quanto segue..., scegliere: **Redirect the message to...**

    1. Selezionare: **il seguente connettore**.
    2. E selezionare il connettore **Outbound to Cisco CES**.
    3. Fare clic su **OK**.

- Tornare a "*Fare quanto segue..." e inserire una seconda azione:

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

        - Scegli: **set the message header**
        - Impostare l'intestazione del messaggio su: **X-OUTBOUND-AUTH**.
        - Fare clic su **OK**.
        - Impostare il valore: **mysecretkey**.

- Fare clic su **OK**.

- Fare clic su **Save**.

Nota: per impedire la ricezione di messaggi non autorizzati da parte di Microsoft, è possibile contrassegnare un'intestazione x segreta quando i messaggi lasciano il dominio Microsoft 365. Tale intestazione viene valutata e rimossa prima del recapito a Internet.

Esempio di configurazione del routing di Microsoft 365:

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

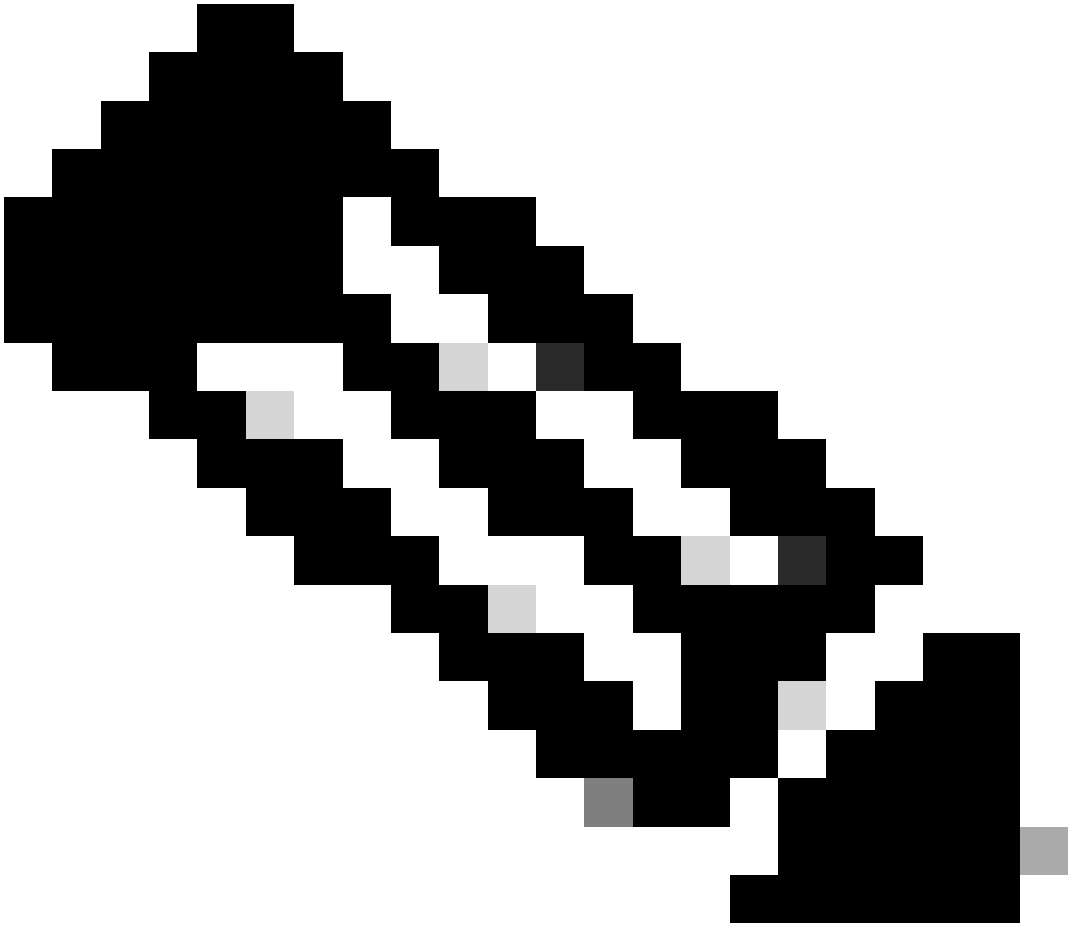
PCI

Comments:

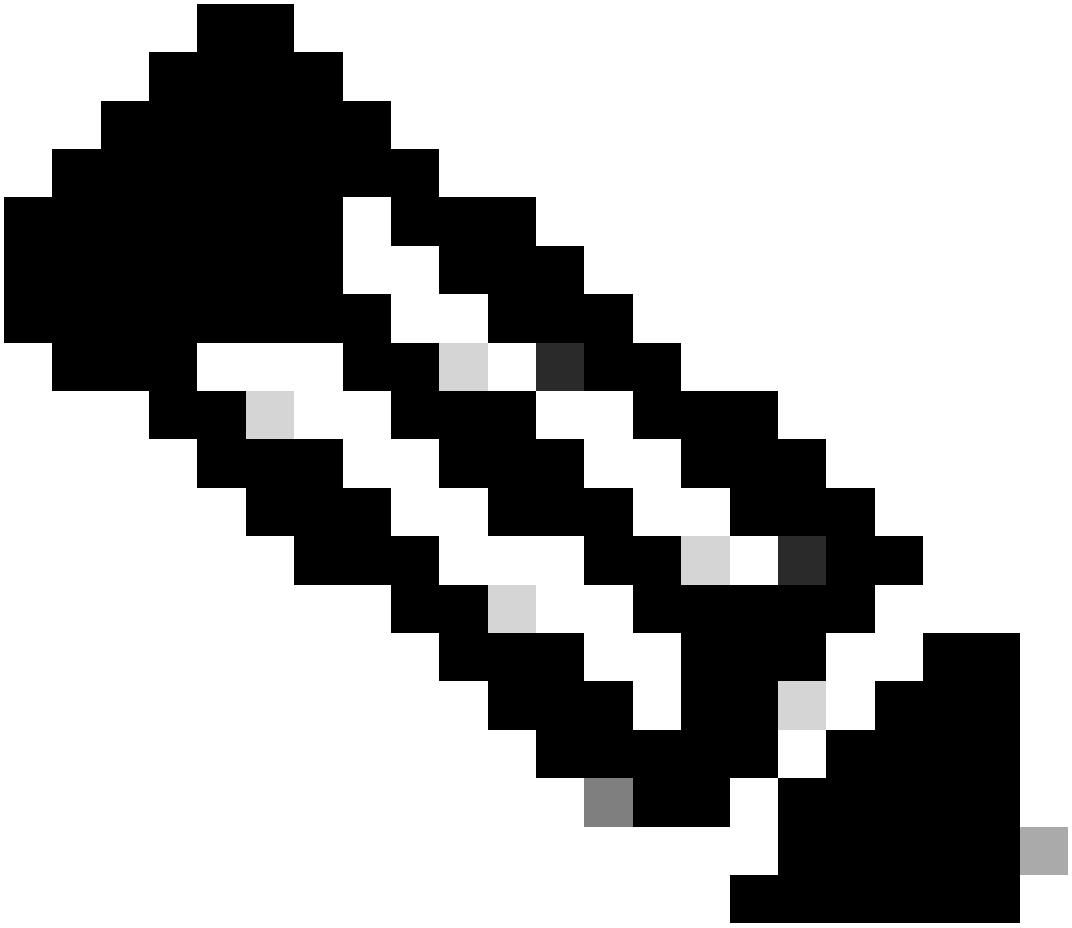
ℹ Rights Management Services (RMS) is a premium feature that requires an Enterprise Client Access License (CAL) or a RMS Online license for each user mailbox. Learn more

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

- Premere Ritorno una volta per creare una nuova riga vuota.
- Immettere **[.]** nella nuova riga per terminare il nuovo filtro messaggi.
- Fare clic **return** una volta per uscire dal menu Filtri.
- Eseguire il **Commit** comando per salvare le modifiche alla configurazione.



Nota: evitare caratteri speciali per la chiave segreta. ^ e $ mostrati nel filtro messaggi sono caratteri regex e vengono utilizzati come indicato nell'esempio.



Nota: rivedere il nome della configurazione di RELAYLIST. Può essere configurato con un nome alternativo oppure è possibile avere un nome specifico basato sul criterio di inoltro o sul provider di posta.

Test posta elettronica in uscita

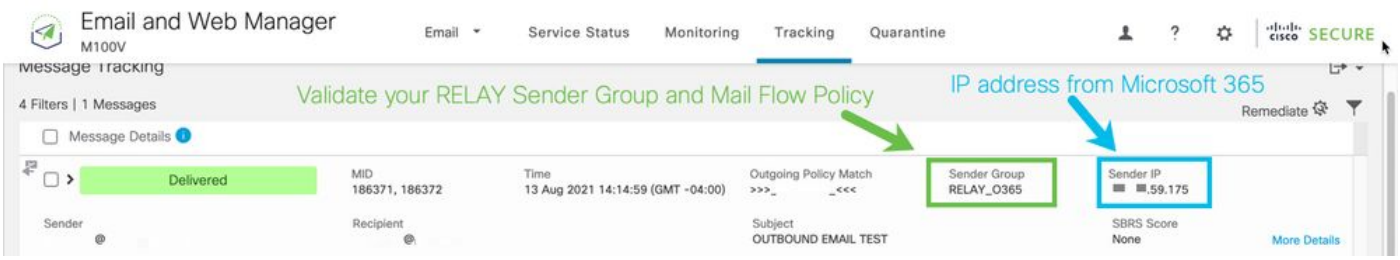
Verifica la posta in uscita dal tuo indirizzo di posta elettronica Microsoft 365 a un destinatario del dominio esterno. È possibile rivedere il Message Tracking da Cisco Secure Email e Web Manager per verificare che sia instradato correttamente in uscita.

Nota: rivedere la configurazione TLS (**Amministrazione sistema > Configurazione SSL**) sul gateway e le cifrature utilizzate per

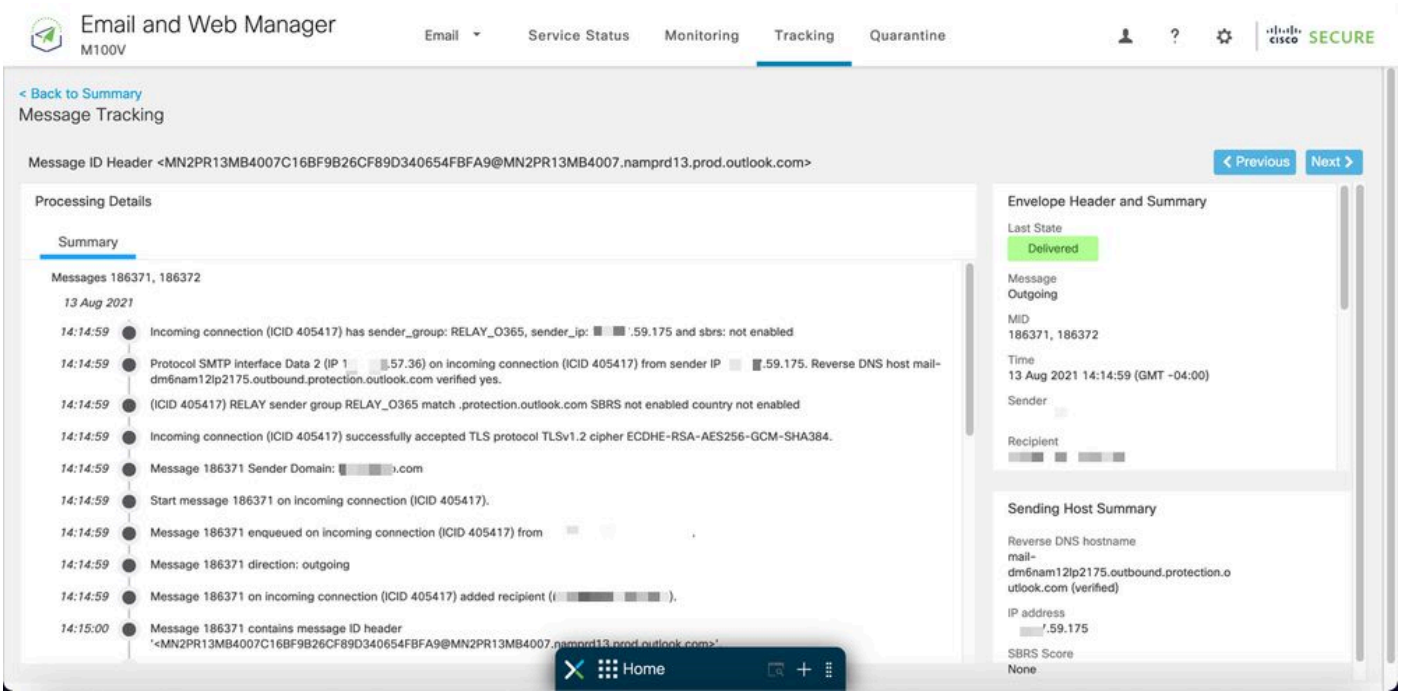
SMTP in uscita. Cisco Best Practices consiglia:

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

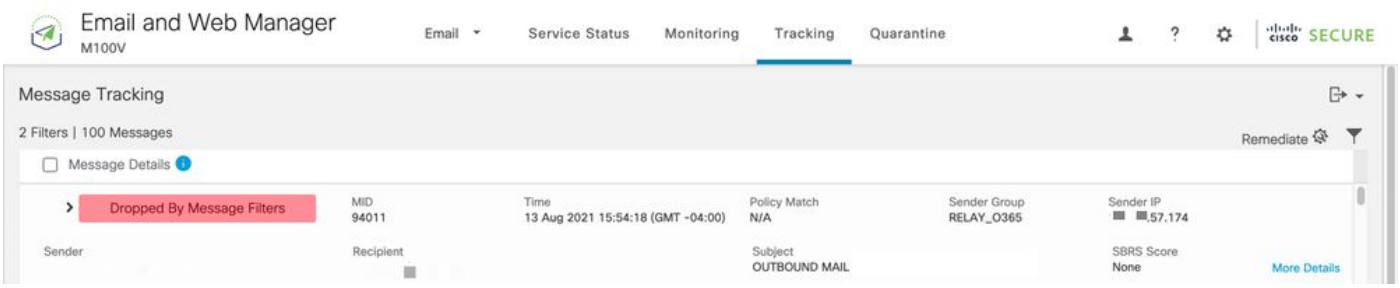
Un esempio di monitoraggio con consegna riuscita:

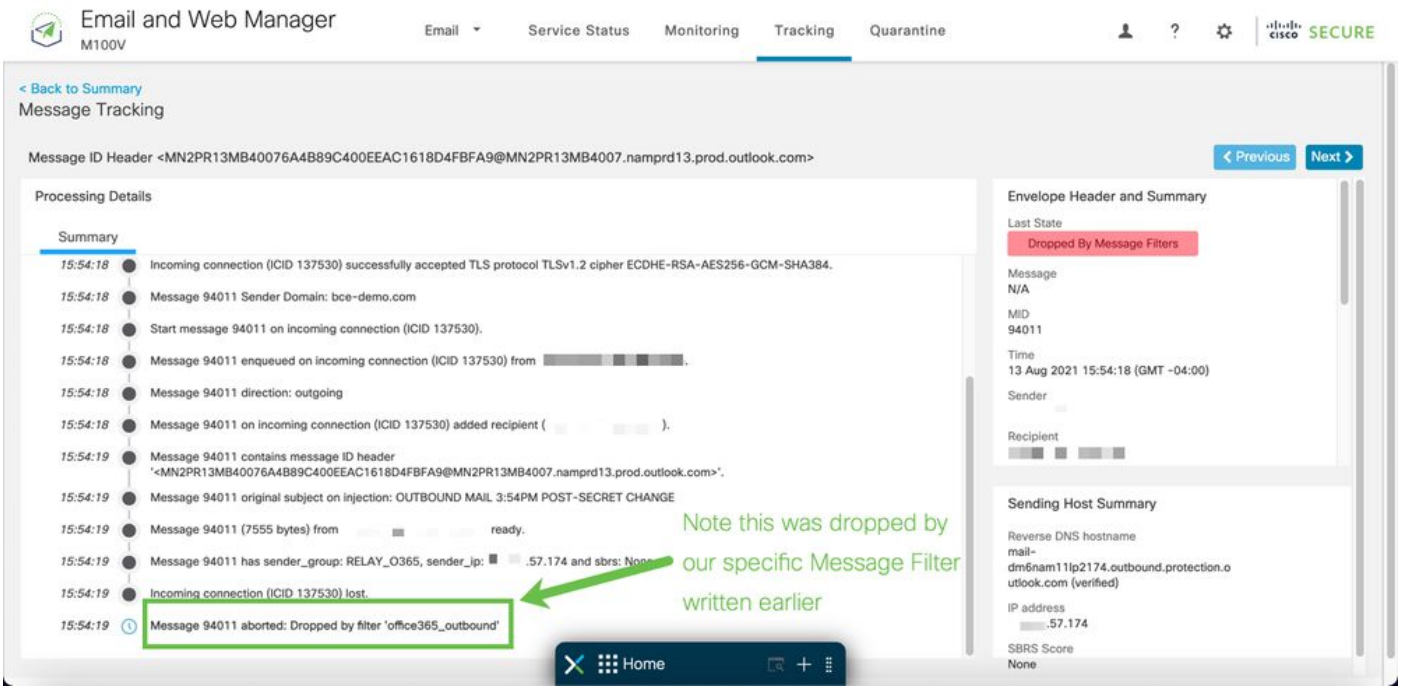


Fare clic **More Details** per visualizzare i dettagli completi del messaggio:



Un esempio di monitoraggio dello stato dei messaggi con x-header non corrispondente:





Informazioni correlate

Documentazione di Cisco Secure Email Gateway

- Note sulla release
- Guida dell'utente
- Guida di riferimento CLI
- Guide alla programmazione API per Cisco Secure Email Gateway
- Open Source utilizzato in Cisco Secure Email Gateway
- Guida all'installazione di Cisco Content Security Virtual Appliance (include vESA)

Documentazione su Secure Email Cloud Gateway

- Note sulla release
- Guida dell'utente

Documentazione di Cisco Secure Email e Web Manager

- Note sulla versione e matrice di compatibilità

    - Guida dell'utente
- Guide alla programmazione API per Cisco Secure Email e Web Manager
- Guida all'installazione di Cisco Content Security Virtual Appliance (include vSMA)

Documentazione del prodotto Cisco Secure

- Architettura di denominazione del portafoglio Cisco Secure

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).