為Microsoft 365配置安全電子郵件

目錄

簡介

本文檔介紹將Microsoft 365與思科安全郵件整合以進行入站和出站郵件傳送的配置步驟。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Secure Email Gateway 或 Cloud Gateway
- 對思科安全郵件雲網關環境的命令列介面(CLI)訪問：
  Cisco Secure Email Cloud Gateway > Command Line Interface (CLI)訪問

- Microsoft 365
- 簡易郵件傳輸通訊協定(SMTP)
- 網域名稱伺服器或網域名稱系統(DNS)

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文檔可用於本地網關或思科雲網關。

如果您是思科安全郵件管理員，歡迎信中將包含您的雲網關IP地址和其他相關資訊。除了您在此處看到的信以外，還會向您傳送一封加密電子郵件，提供有關為分配調配的雲網關（也稱為ESA）以及雲郵件和網路管理器（也稱為SMA）數量的更多詳細資訊。如果您尚未收到或沒有收到該信件的副本，請聯絡ces-activations@cisco.com，並提供您的聯絡資訊和服務項下的域名。

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

每個客戶端都有專用IP。您可以在 Microsoft 365 組態中使用指派的 IP 或主機名稱。

注意：強烈建議您在計畫的生產郵件轉換之前進行測試，因為在Microsoft 365 Exchange控制檯中複製配置需要時間。至少要等待一小時，所有變更才會生效。

注意：螢幕截圖中的IP地址與分配給您的分配的雲網關數量成比例。例如，xxx.yy.140.105 是網關1的資料1介面IP地址，xxx.yy.150.1143 是網關2的資料1介面IP地址。網關1的資料2介面IP地址為xxx.yy.143.186 ，網關2的資料2介面IP地址為xxx.yy.32.98。如果您的歡迎信不包含資料2（傳出介面IP）的資訊，請聯絡思科TAC，獲取增加到分配中的資料2介面。

為Microsoft 365配置安全電子郵件

設定從 Cisco Secure Email 傳入 Microsoft 365 的內送電子郵件

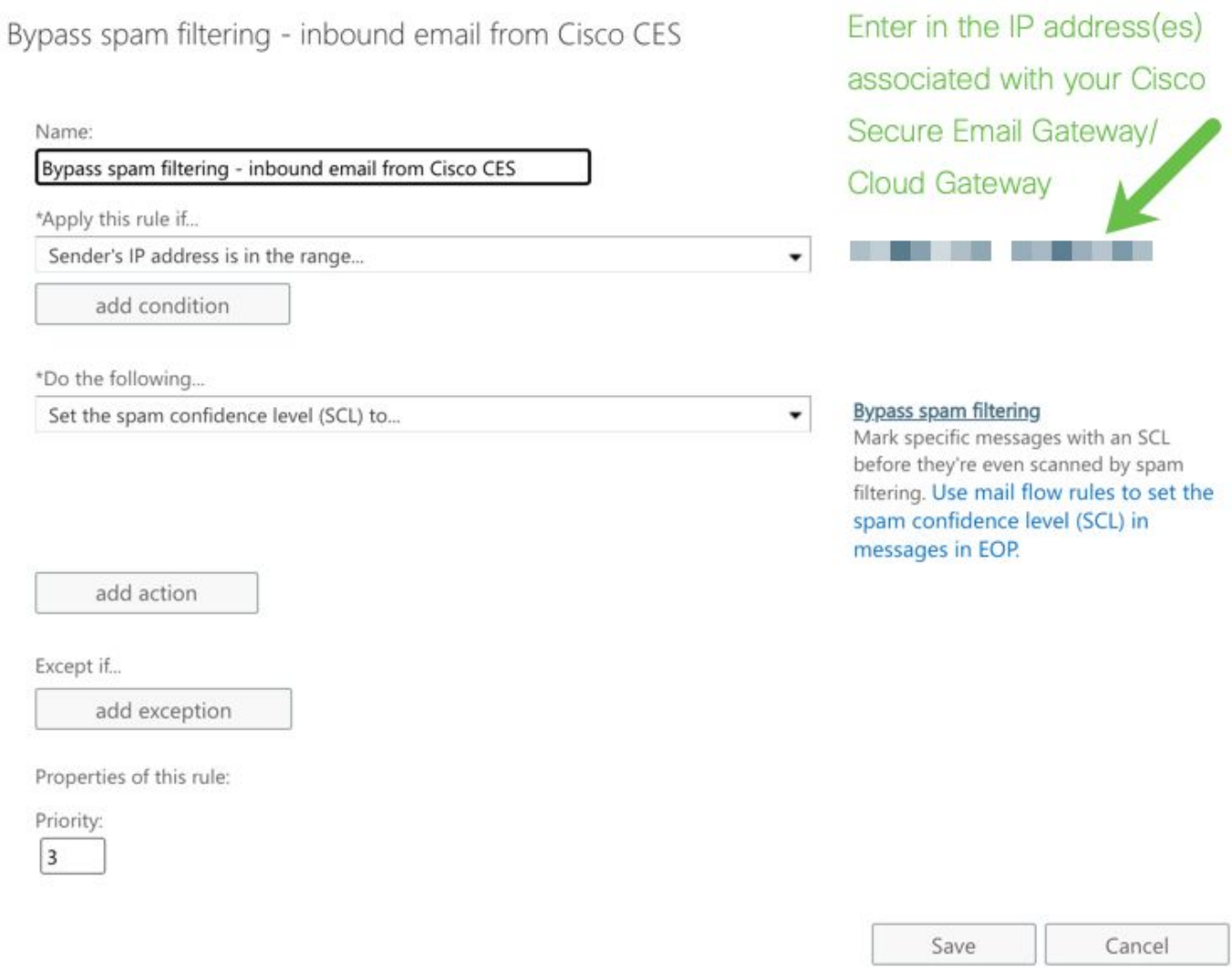
略過垃圾郵件篩選規則

- 登入到Microsoft 365管理中心(https://portal.microsoft.com)。
- 在左邊的功能表中，展開 **Admin Centers**.
- 按一下 **Exchange**.
- 從左側功能表瀏覽至 **Mail flow** > **Rules**.
- 點選 **[+]** 以建立新規則。
- 從下拉選單中選擇**Bypass spam filtering...** 。
- 輸入新規則的名稱： **Bypass spam filtering - inbound email from Cisco CES**.
- 對於*Apply this rule if...，選擇 **The sender - IP address is in any of these ranges or exactly matches**.

  1. 對於「指定IP地址範圍」彈出窗口，請增加Cisco Secure Email歡迎信中提供的IP地址。
  2. 按一下 **OK**.

- 對於*Do the following...，已預先選取新規則： **Set the spam confidence level (SCL) to... - Bypass spam filtering**.
- 按一下 **Save**.

規則外觀範例：



接收連接器

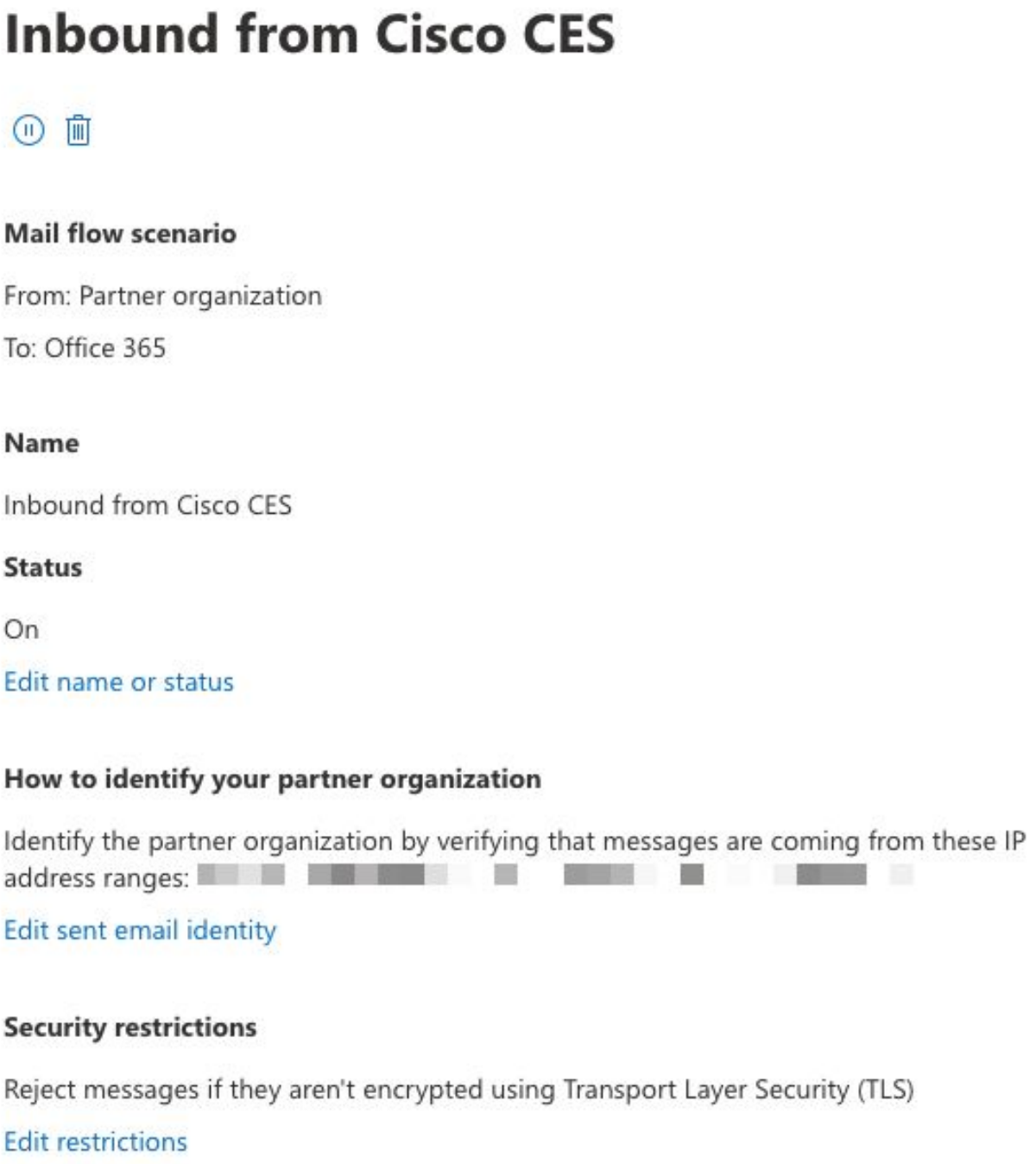
- 留在 Exchange 系統管理中心中.
- 從左側功能表瀏覽至 **Mail flow > Connectors**.
- 按一 **[+]** 下以建立新的聯結器。
- 在「選擇郵件流方案」彈出窗口中，選擇：

1. 寄件者： Partner organization
    - 收件者： **Office365**

- 按一下 **Next**.

- 輸入新聯結器的名稱： **Inbound from Cisco CES**.
- 如有需要，請輸入說明。
- 按一下 **Next**.
- 按一下 **Use the sender's IP address**.
- 按一下 **Next**.
- 點選 **[+]** 並輸入您的Cisco Secure Email歡迎信中所示的IP地址。
- 按一下 **Next**.
- 選擇 **Reject email messages if they aren't sent over Transport Layer Security (TLS)**.
- 按一下 **Next**.
- 按一下 **Save**.

聯結器組態的外觀範例：



設定從 Cisco Secure Email 傳至 Microsoft 365 的郵件

目的地控制

對目標控制中的傳遞域實施自動限制。當然，您可以稍後刪除限制，但這些是Microsoft 365的新IP，並且由於未知的聲譽，您不希望Microsoft進行任何限制。

- 登入您的閘道。
- 導覽至 **Mail Policies > Destination Controls**.
- 按一下 **Add Destination**.

- 使用:

1. 目的地：輸入您的網域名稱

2. 同時連線數： **10**

   - 每次連線郵件數上限： **20**
   - TLS 支援： **Preferred**

- 按一下 **Submit**.
- 按一下使用者介面(UI)右上角的**Commit Changes** 以儲存配置更改。

「目標控制表」的示例如下：

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.

收件者存取表

接著，設定網域的收件人存取表 (RAT) 以接受郵件：

- **導覽至 Mail Policies > Recipient Access Table (RAT)**.

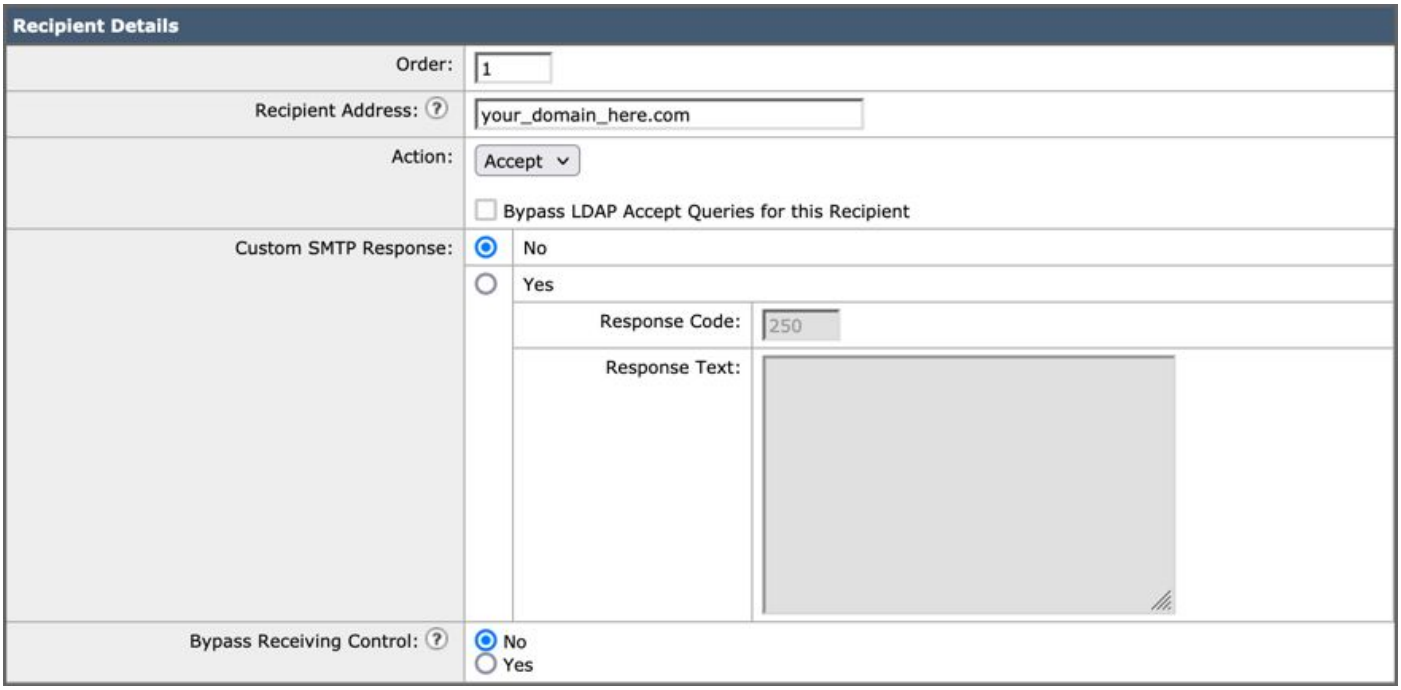
注意：根據主要郵件流程監聽器的實際名稱，確定監聽器適用於傳入監聽器、傳入郵件或郵件流。

- 按一下 **Add Recipient**.
- 在「收件人地址」欄位中新增網域.
- 選擇預設操作 **Accept**.

- 按一下 **Submit**.

- 點選UI右上角的**Commit Changes** 以儲存您的配置更改。

RAT條目顯示內容的示例：



SMTP 路由

設定SMTP路由以將郵件從Cisco Secure Email傳送到您的Microsoft 365域：

- 導覽至 **Network > SMTP Routes**.

- 按一下 **Add Route...**

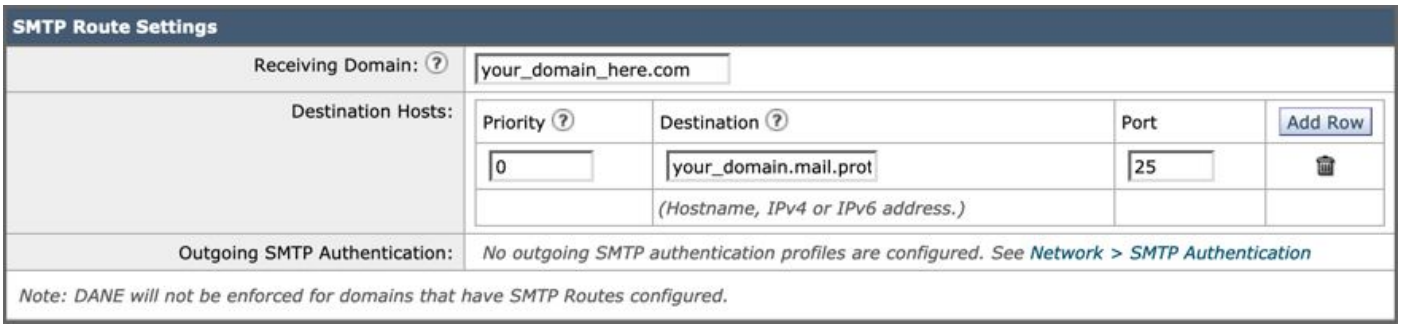
- 接收域：輸入您的域名。

- 目標主機：增加原始Microsoft 365 MX記錄。

- 按一下 **Submit**.

- 點選UI右上角的**Commit Changes** 以儲存您的配置更改。

SMTP路由設定顯示內容的示例：



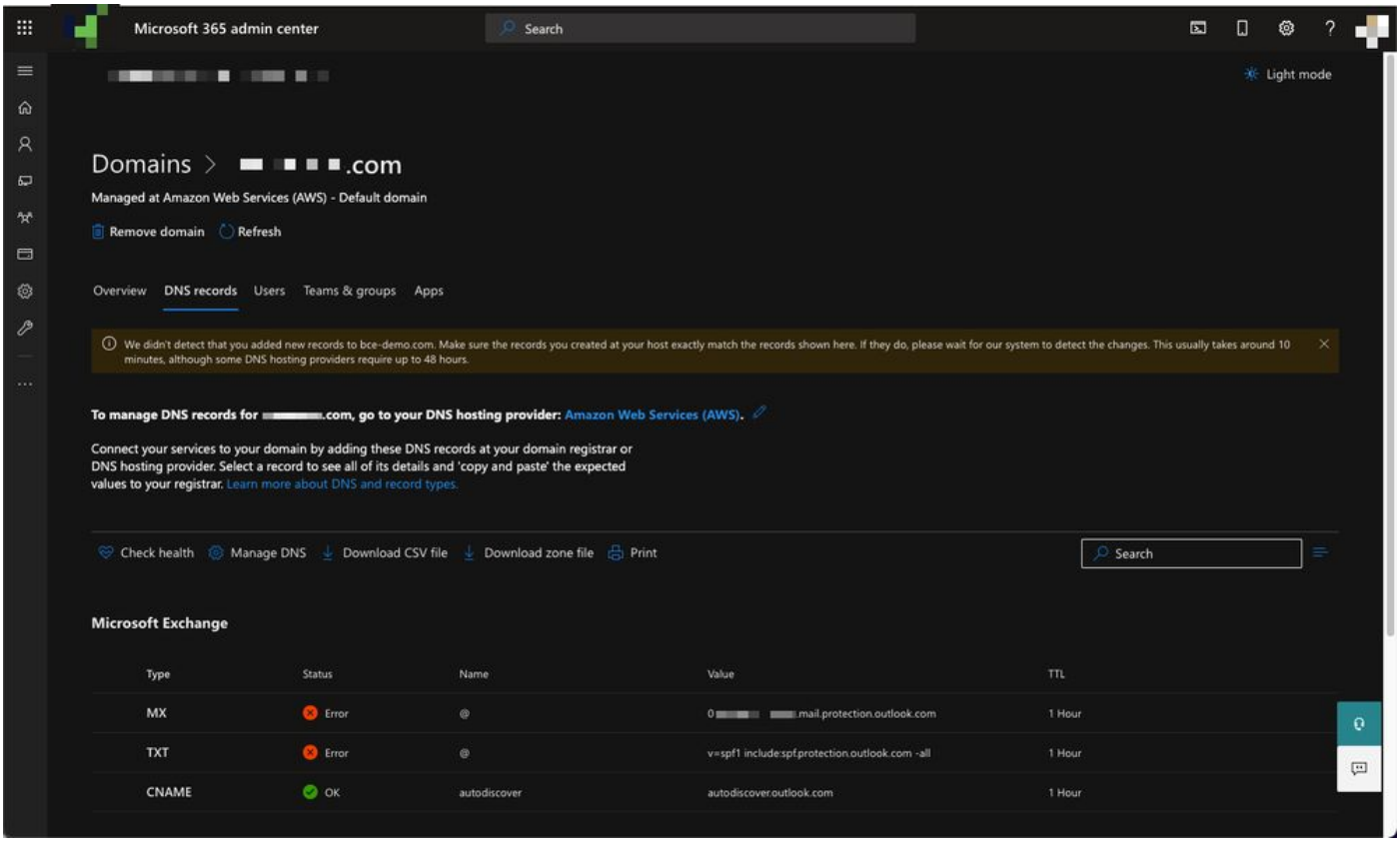
DNS（MX 記錄）組態

您已經準備好透過郵件交換(MX)記錄更改來切換域。按照思科安全電子郵件歡迎信中的說明，與您的DNS管理員合作，將MX記錄解析為思科安全電子郵件雲例項的IP地址。

從Microsoft 365控制檯驗證對MX記錄的更改：

- 登入到Microsoft 365管理控制檯(https://admin.microsoft.com)。
- 導覽至 **Home > Settings > Domains**.
- 選擇您的預設網域名稱。
- 按一下Check Health.

這提供了Microsoft 365如何查詢與您的域相關聯的DNS和MX記錄的當前MX記錄：



注意：在本示例中，DNS由Amazon Web Services (AWS)託管和管理。作為管理員，如果您的DNS託管在Microsoft 365帳戶以外的任何位置，將會看到警告。您可以忽略如下警告：「我們沒有檢測到您向your_domain_here.com增加新記錄。確保您在主機建立的記錄與此處顯示的記錄匹配...」 分步說明將MX記錄重置為最初配置為重定向到您的Microsoft 365帳戶的記錄。這將從傳入流量中刪除思科安全郵件網關。

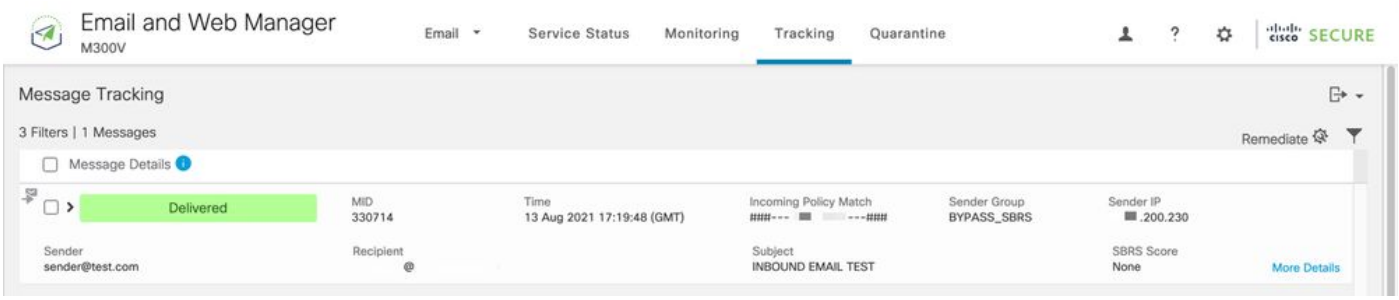
測試入站電子郵件

測試傳入您的Microsoft 365電子郵件地址的入站郵件。然後，請檢查它是否到達您的Microsoft 365電子郵件收件箱。

驗證例項隨附的Cisco Secure Email and Web Manager （ 也稱為SMA ）上郵件跟蹤中的郵件日誌。

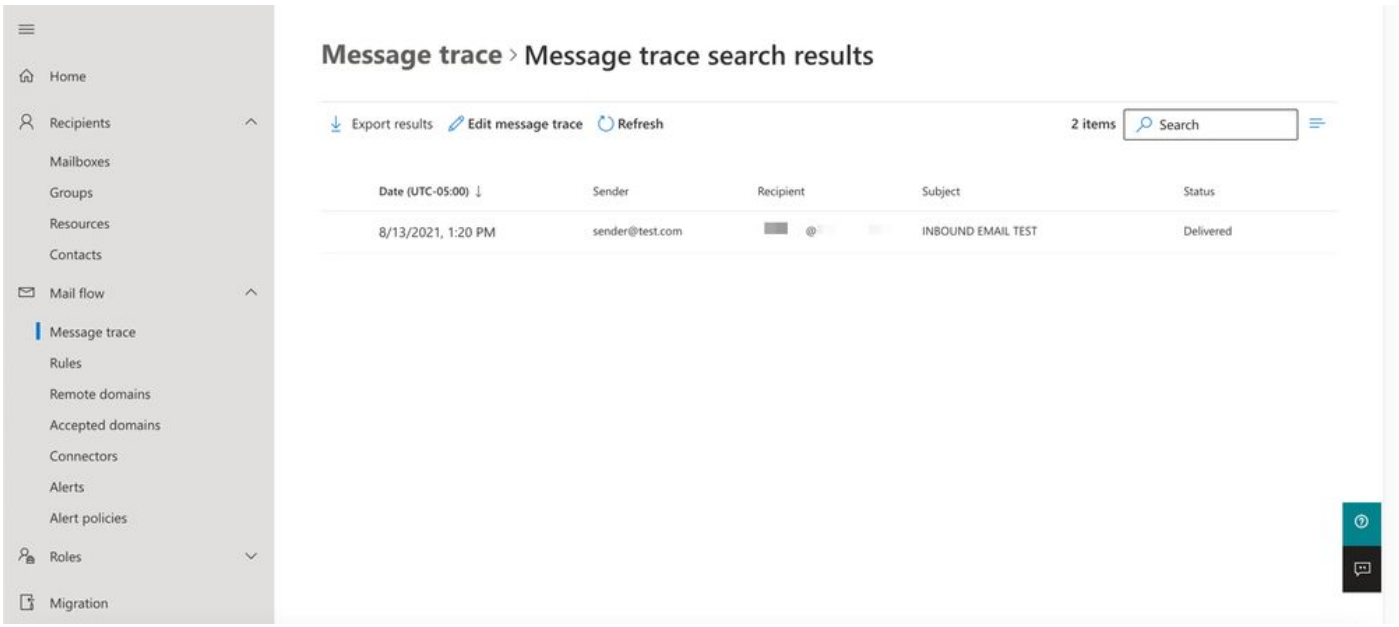
在 SMA 上查看郵件記錄：

- 登入您的SMA(https://sma.iphmx.com/ng-login)。
- 按一下 **Tracking**.
- 輸入所需的搜尋標準並按一下 **Search**；然後希望看到以下結果：



若要在 Microsoft 365 中查看郵件記錄：

- 登入到Microsoft 365管理中心(https://admin.microsoft.com)。
- 拓展 **Admin Centers**.
- 按一下 **Exchange**.
- 導覽至 **Mail flow** > **Message trace**.
- Microsoft提供了用於搜尋的預設條件。例如，選擇 **Messages received by my primary domain in the last day**以開始您的搜尋查詢。
- 輸入所需的收件人搜尋條件，然後點選 **Search** 並期望看到類似以下內容的結果：



設定從 Microsoft 365 傳至 Cisco Secure Email 的外寄電子郵件

在 Cisco Secure Email Gateway 上設定 RELAYLIST

請參閱您的Cisco Secure Email歡迎信。此外，透過網關為出站消息指定輔助介面。

- 登入您的閘道。
- 導覽至 **Mail Policies > HAT Overview**.

> **注意**：根據外部/外寄郵件流程監聽器的實際名稱，確定監聽器是外寄監聽器、外寄郵件或外寄郵件流程監聽器。

- 按一下 **Add Sender Group...**
- 將寄件者群組設為：

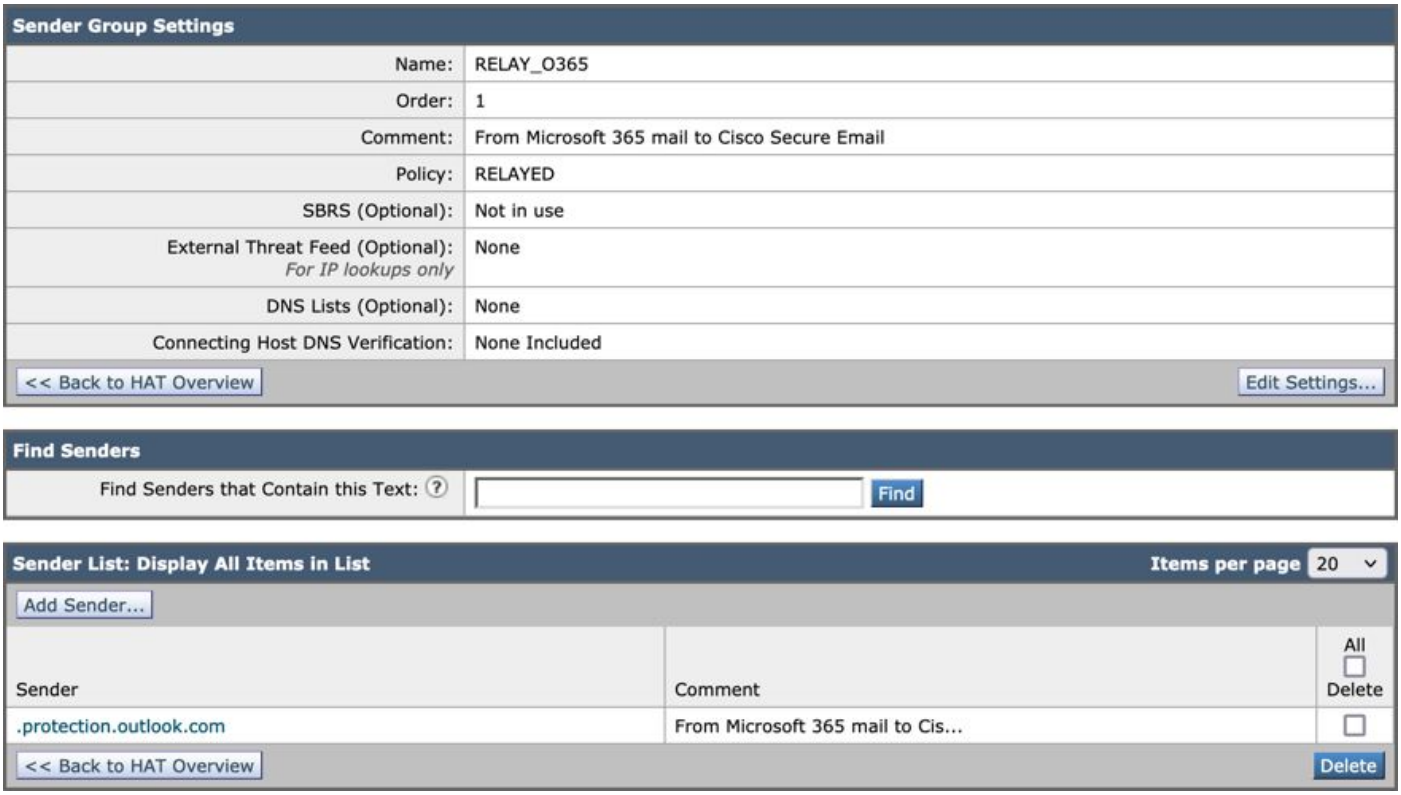
1. 名稱：RELAY_O365
2. 備註： **<<如果您要通知寄件者群組，請輸入備註>>**
3. 策略：已中繼
4. 按一下 **Submit and Add Senders**.

    - 寄件者： **.protection.outlook.com**

附註：。網域名稱開頭的「.」（點）為必要項目.

- 按一下 **Submit**.
- 點選UI右上角的**Commit Changes** 以儲存您的配置更改。

發件人組設定的外觀示例：



啟用 TLS

- 按一下 **<<Back to HAT Overview**.
- 按一下「郵件流程原則」名稱： **RELAYED**.
- 向下滾動並檢視 **Security Features** 部分，瞭解 **Encryption and Authentication**.
- 若為 TLS，請選擇： **Preferred**.
- 按一下 **Submit**.
- 點選UI右上角的**Commit Changes** 以儲存您的配置更改。

郵件流策略配置的示例如下：

設定從 Microsoft 365 傳至 CES 的郵件

- 登入到Microsoft 365管理中心(https://admin.microsoft.com)。
- 拓展 **Admin Centers**.
- 按一下 **Exchange**.
- 導覽至 **Mail flow** > **Connectors**.
- 按一下[+]可建立新聯結器。
- 在「選擇郵件流方案」彈出窗口中，選擇：

1. 寄件者： Office365
    - 收件者：Partner organization

- 按一下 **Next**.
- 輸入新聯結器的名稱： **Outbound to Cisco CES**.
- 如有需要，請輸入說明。
- 按一下 **Next**.
- 對於何時要使用此聯結器？：

1. 選擇: **Only when I have a transport rule set up that redirects messages to this connector**.
    - 按一下 **Next**.

- 按一下 **Route email through these smart hosts**.

- 按一下 **[+]** 並輸入CES歡迎信中提供的出站IP地址或主機名。
- 按一下 **Save**.
- 按一下 **Next**.
- Office 365應如何連線至您合作夥伴組織的電子郵件伺服器？

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

        - 選擇.Any digital certificate, including self-signed certificates
        - 按一下 **Next**.

- 此時將顯示確認螢幕。
- 按一下 **Next**.
- 使用 **[+]** 輸入有效的電子郵件地址，然後按一下 **OK**.
- 點選 **Validate** 並允許運行驗證。
- 完成後，按一下 **Close**.
- 按一下Save.

輸出聯結器外觀範例：

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

1. 對於「選擇發件人位置」彈出窗口，選擇： **Inside the organization**.

    - 按一下 **OK**.

- 按一下 **More options...**
- 按一下 **add condition** 按鈕並插入第二個條件：

    1. 選擇 **The recipient...**

        - 選擇: **Is external/internal**.
        - 對於「選擇發件人位置」彈出窗口，選擇： **Outside the organization** .
        - 按一下 **OK**.

- 對於*執行以下操作……，選擇： **Redirect the message to...**

    1. 選取：**下列聯結器。**
    2. 並選擇您的**Outbound to Cisco CES**聯結器。
    3. 按一下「**OK**」（確定）。

- 返回「*執行以下操作……」並插入第二個操作：

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

        - 選擇: **set the message header**
        - 設定郵件標頭： **X-OUTBOUND-AUTH**.
        - 按一下 **OK**.
        - 設定值： **mysecretkey**.

- 按一下 **OK**.

- 按一下 **Save**.

注意：為防止來自Microsoft的未授權郵件，可以在郵件離開您的Microsoft 365域時對x信頭進行簽名；在郵件送達網際網路之前，將評估和刪除此信頭。

Microsoft 365路由配置的示例如下：

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

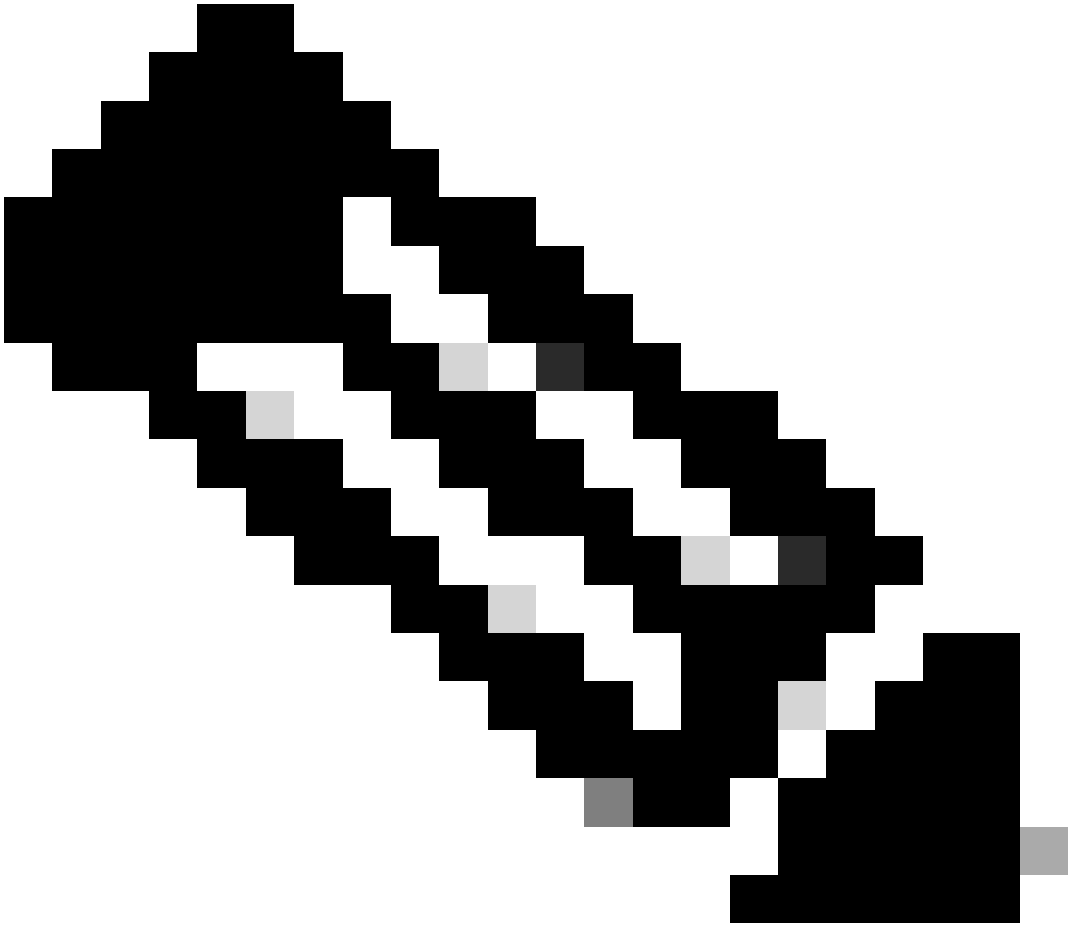
PCI

Comments:

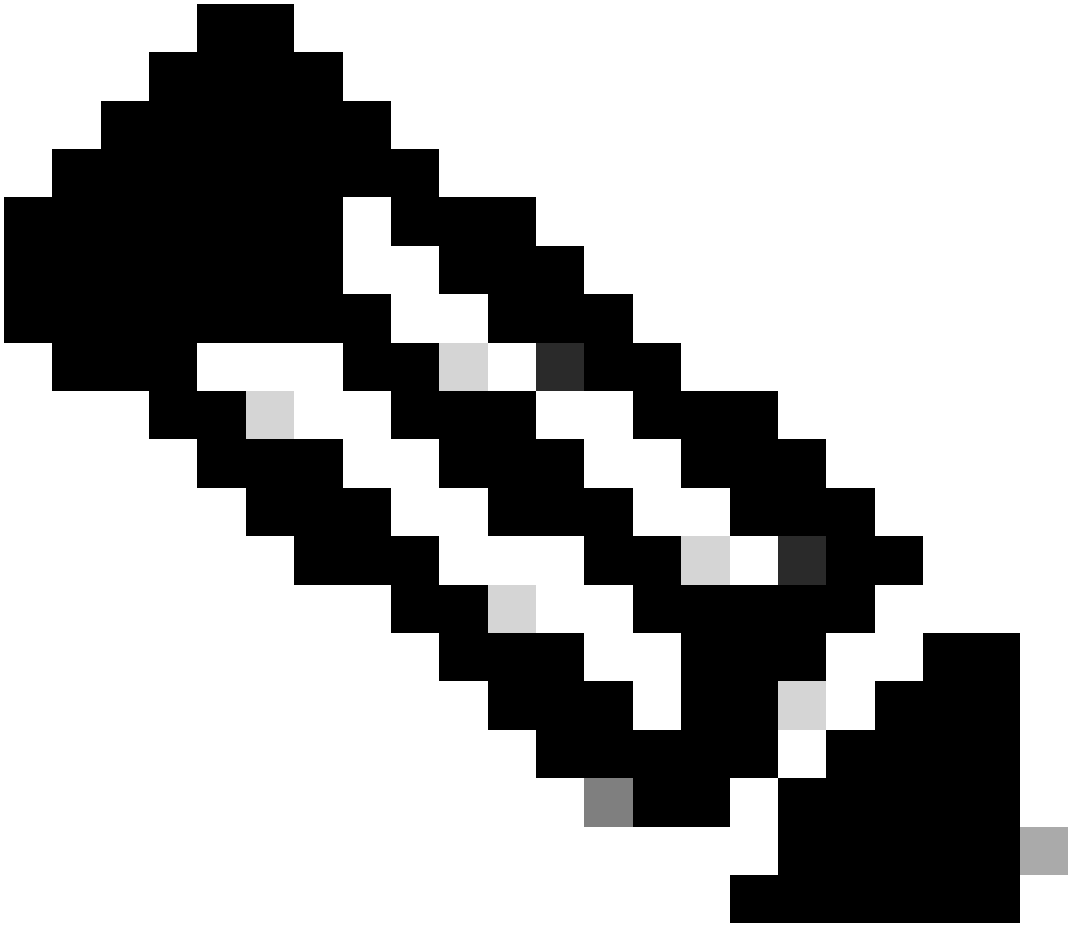
ℹ Rights Management Services (RMS) is a premium feature that requires an Enterprise Client Access License (CAL) or a RMS Online license for each user mailbox. Learn more

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

- 點擊返回一次，以建立新的空白行.
- 在新行中輸入 **[.]** 以結束新的郵件過濾器。
- 按一 **return** 下以退出「濾鏡」選單。
- 運行**Commit** 命令以儲存對配置所做的更改。



注意：避免使用金鑰的特殊字元。消息過濾器中顯示的^和$是正規表示式字元，如示例中所示。



注意：請複習如何配置RELAYLIST的名稱。可以使用備用名稱進行配置，也可以使用基於中繼策略或郵件提供商的特定名稱。

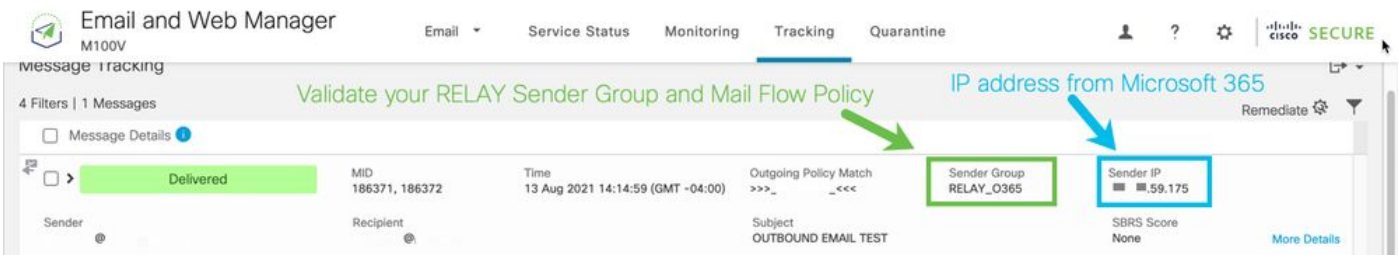
測試出站電子郵件

測試從您的Microsoft 365電子郵件地址寄出郵件給外部網域收件者。您可以從思科安全電郵和Web管理器檢視郵件跟蹤，以確保其被適在地路由到出站。

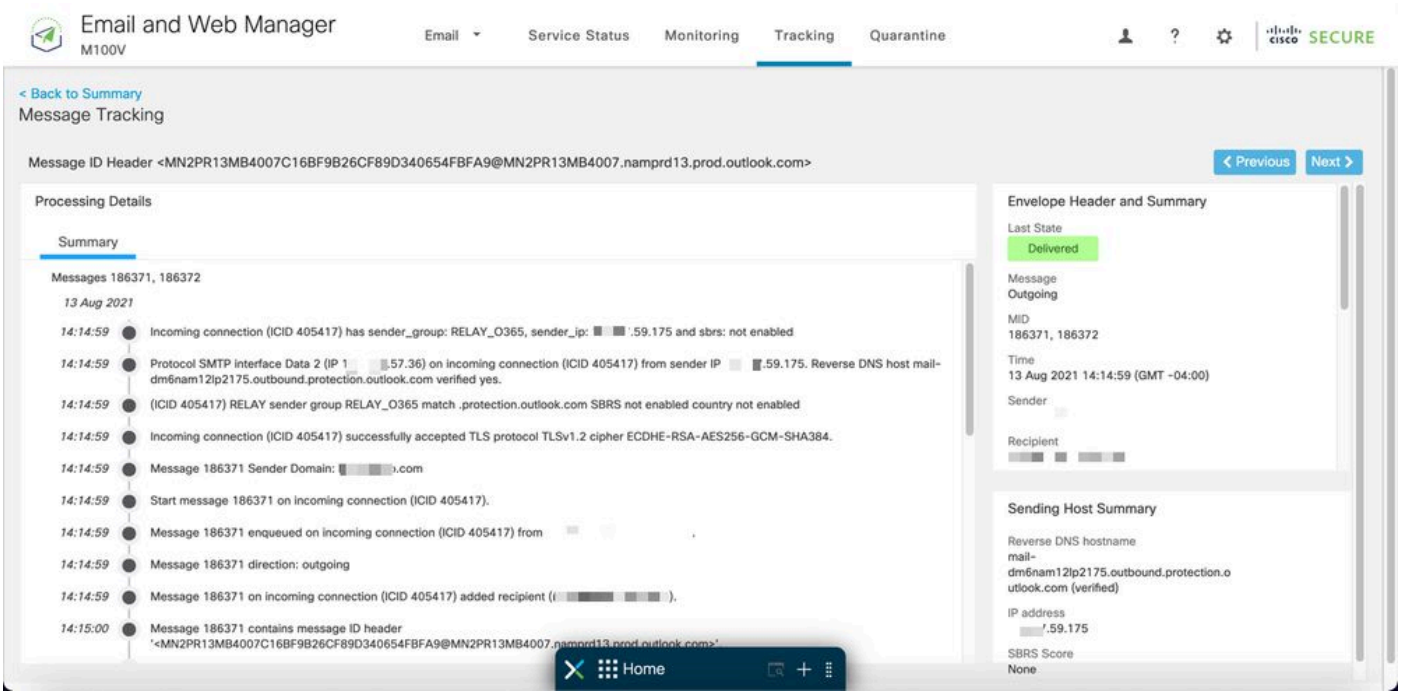
注意：檢查網關上的TLS配置(**系統管理> SSL配置**)以及用於出站SMTP的密碼。思科最佳實踐建議：

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

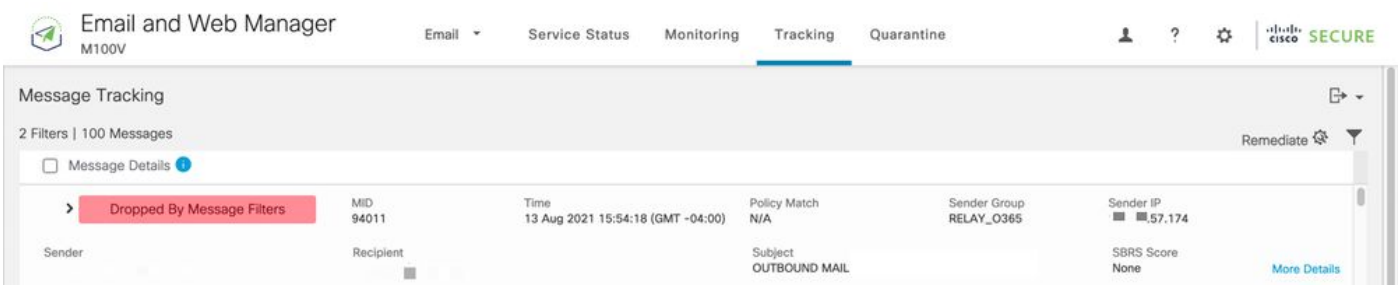
藉由成功遞進行追蹤的送範例：

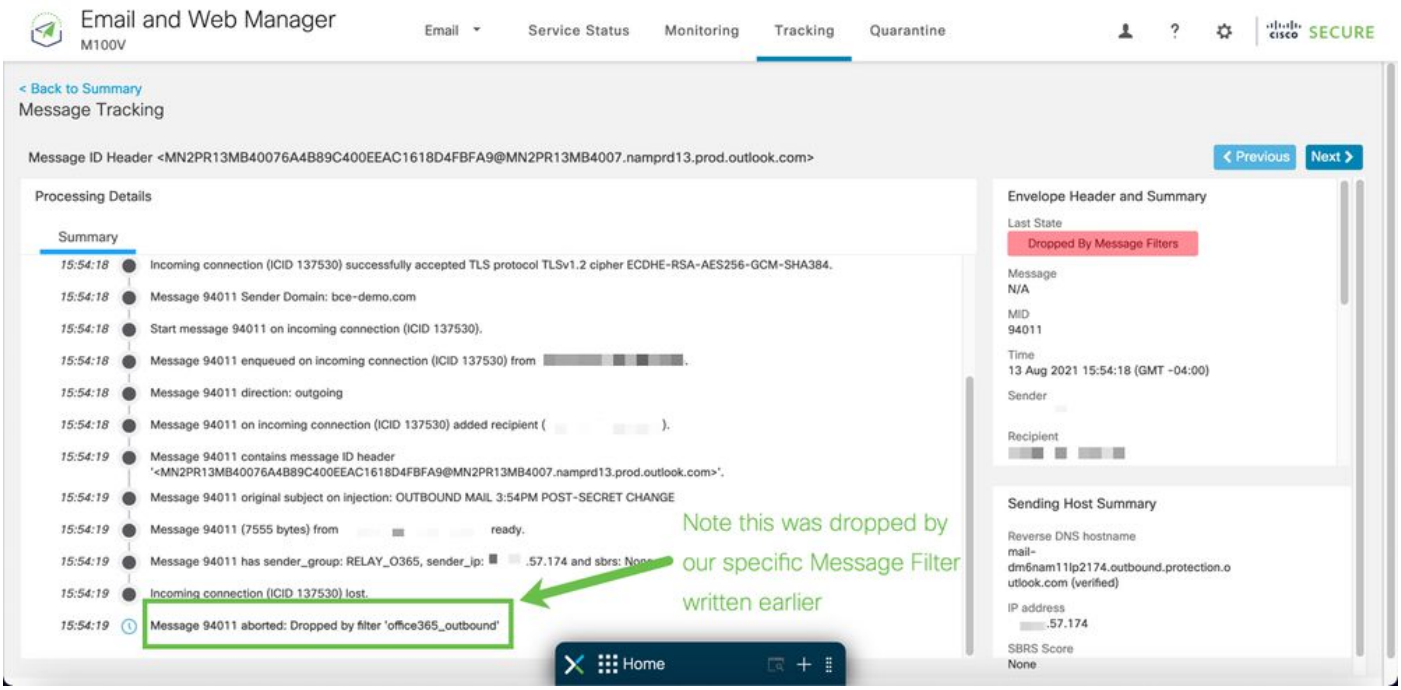


點選**More Details** 可檢視完整的消息詳細資訊：



X 標頭不相符的郵件追蹤範例：





相關資訊

Cisco Secure Email Gateway文檔

- 版本資訊
- 使用手冊
- CLI參考指南
- 思科安全郵件網關API程式設計指南
- 思科安全郵件網關中使用的開源
- 思科內容安全虛擬裝置安裝指南（包括vESA）

安全電郵雲網關文檔

- 版本資訊
- 使用手冊

Cisco Secure Email and Web Manager文檔

- 版本說明和相容性矩陣

- 使用手冊
- Cisco Secure Email and Web Manager的API程式設計指南
- 思科內容安全虛擬裝置安裝指南（包括vSMA）

Cisco Secure產品文檔

- 思科安全產品組合命名架構

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。