Microsoft 365でのセキュリティで保護された電子メールの設定

内容

はじめに

このドキュメントでは、受信および送信の電子メール配信用にMicrosoft 365をCisco Secure Email(SEE)に統合するための設定手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Email Gateway または Cloud Gateway
- Cisco Secure Email Cloud Gateway環境へのコマンドラインインターフェイス(CLI)アクセス：
  Cisco Secure Email Cloud Gateway >コマンドラインインターフェイス(CLI)アクセス
- Microsoft 365
- Simple Mail Transfer Protocol（SMTP）
- ドメインネームサーバ(DNS)またはドメインネームシステム(DNS)

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントは、オンプレミスゲートウェイまたはCisco Cloud Gatewayのいずれかに使用できます。

Cisco Secure Email管理者のウェルカムレターには、クラウドゲートウェイのIPアドレスとその他の関連情報が記載されます。ここに表示されている文字に加えて、暗号化された電子メールが送信されます。この電子メールには、割り当てに対してプロビジョニングされたクラウドゲートウェイ（ESAとも呼ばれる）およびクラウド電子メールおよびWebマネージャ（SMAとも呼ばれる）の数の詳細が記載されます。手紙を受け取っていない場合、または手紙のコピーを持っていない場合は、サービス中の連絡先とドメイン名を連絡してください ces-activations@cisco.com。

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

各クライアントには専用のIPがあります。割り当てられた IP またはホスト名を Microsoft 365 の設定で使用できます。

注:Microsoft 365 Exchangeコンソールで設定を複製するには時間がかかるため、実稼働メールのカットオーバーを計画する前にテストすることを強く推奨します。少なくとも、すべての変更が有効になるまで1時間かかります。

注：画面キャプチャのIPアドレスは、割り当てにプロビジョニングされたクラウドゲートウェイの数に比例します。たとえば、xxx.yy.140.105 はゲートウェイ1のデータ1インターフェイスIPアドレスで、 xxx.yy.150.1143 はゲートウェイ2のデータ1インターフェイスIPアドレスです。ゲートウェイ1のデータ2インターフェイスのIPアドレスはxxx.yy.143.186 で、ゲートウェイ2のデータ2インターフェイスのIPアドレスは xxx.yy.32.98です。データ2（発信インターフェイスIP）の情報が案内状に含まれていない場合は、Cisco TACに連絡して、データ2インターフェイスを割り当てに追加してください。

Microsoft 365でのセキュリティで保護された電子メールの設定

Cisco Secure Email から Microsoft 365 に着信する電子メールの設定

スパムフィルタリングルールのバイパス

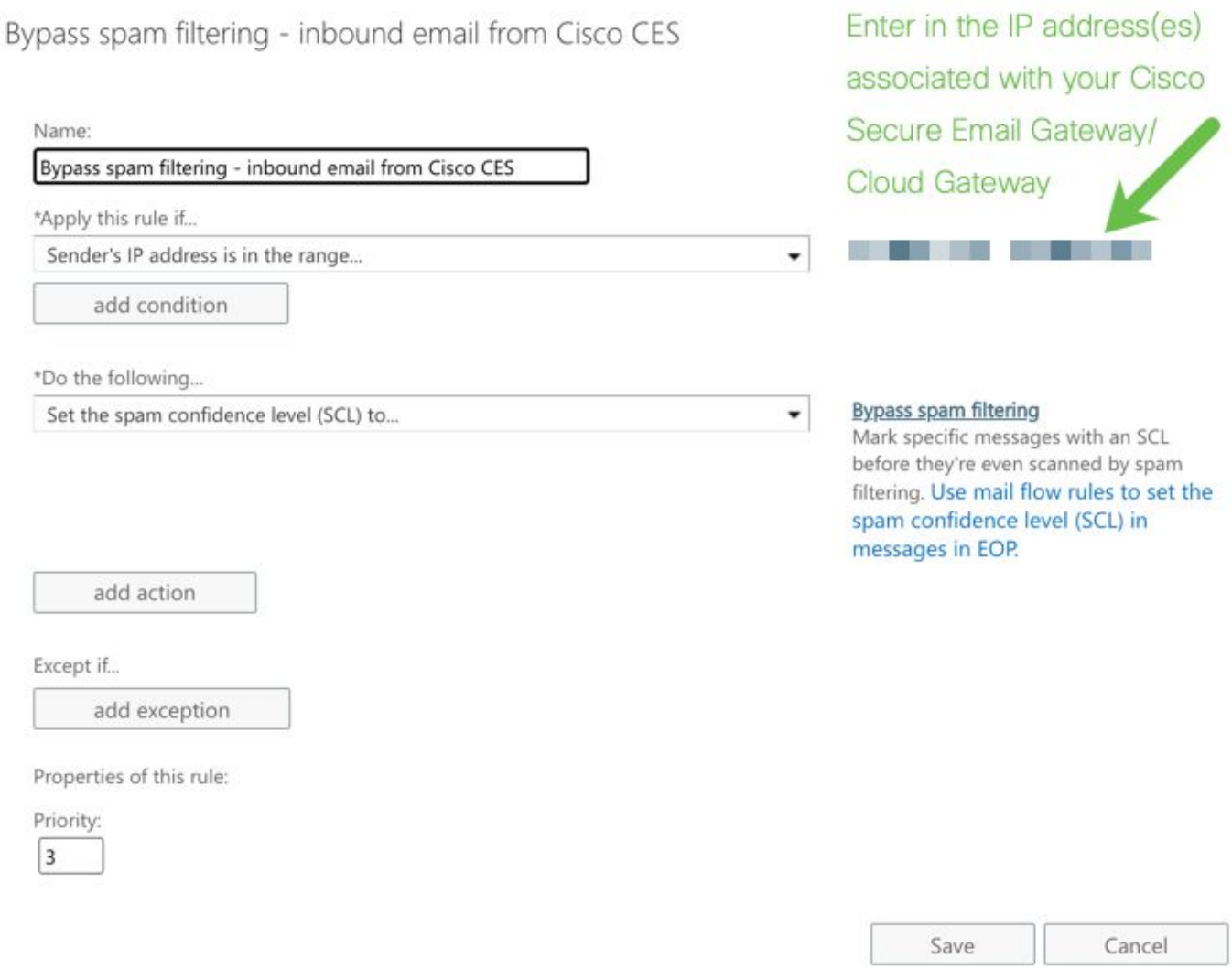
- Microsoft 365 Admin Center(https://portal.microsoft.com)にログインします。
- 左側のメニューで、 **Admin Centers**.
- クリック **Exchange**.
- 左側のメニューから、 **Mail flow** > **Rules**.
- をクリック **[+]** して、新しいルールを作成します。
- ドロップダウンリストか**Bypass spam filtering...** ら選択します。
- 新しいルールの名前を入力してください： **Bypass spam filtering - inbound email from Cisco CES**.
- [*このルールを適用する条件…]で、 **The sender - IP address is in any of these ranges or exactly matches**.

1. [IPアドレス範囲の指定]ポップアップで、Cisco Secure Emailのウェルカムレターに記載されているIPアドレスを追加します。
2. クリック **OK**.

- 「*次の操作を行う…」では、新しいルールが事前に選択されています。 **Set the spam confidence level (SCL) to... - Bypass spam filtering**.

- クリック **Save**.

ルールの例を次に示します。



受信コネクタ

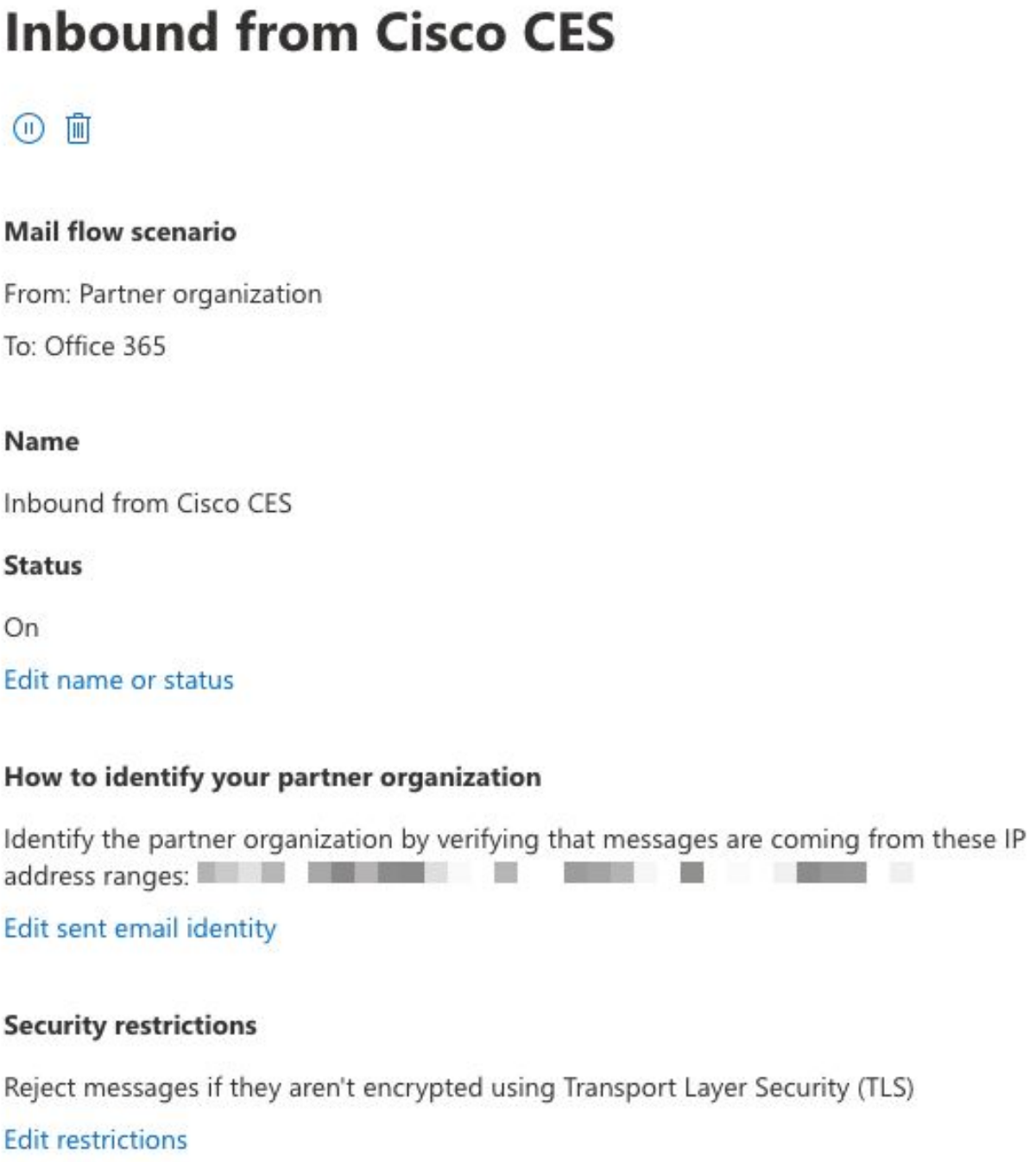
- Exchange管理センターに残ります。
- 左側のメニューから、 **Mail flow** > **Connectors**.
- をクリック **[+]** して、新しいコネクタを作成します。
- Select your mail flow scenarioポップアップウィンドウで、次の項目を選択します。

1. From: Partner organization

    - これを、次のように変更します。 **Office365**

- クリック **Next**.
- 新しいコネクタの名前を入力してください： **Inbound from Cisco CES**.
- 必要に応じて説明を入力します。
- クリック **Next**.
- クリック **Use the sender's IP address**.
- クリック **Next**.
- Cisco Secure Emailのウェルカムレターに記載されているIPアドレスをクリックし **[+]** て入力します。
- クリック **Next**.
- 選択 **Reject email messages if they aren't sent over Transport Layer Security (TLS)**.
- クリック **Next**.
- クリック **Save**.

コネクタ設定の例を次に示します。



Cisco Secure Email から Microsoft 365 への電子メールの設定

送信先コントロール

宛先制御で配信ドメインにセルフスロットルを適用します。当然、スロットルは後で削除できますが、これらはMicrosoft 365への新しいIPであり、レピュテーションが不明であるためMicrosoftによるスロットリングは必要ありません。

- ゲートウェイにログインします。
- 移動先 **Mail Policies** > **Destination Controls**.
- クリック **Add Destination**.

- 利用:

1. 宛先：ドメイン名を入力します。

2. [同時接続数（Concurrent Connections）]： **10**

   - [接続あたりの最大メッセージ数（Maximum Messages Per Connection）]： **20**
   - [TLS のサポート（TLS Support）]： **Preferred**

- クリック **Submit**.
- ユーザインターフェイス(UI)の右上にある**Commit Changes** をクリックして、設定の変更を保存します。

宛先制御テーブルの例を次に示します。

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.

受信者アクセステーブル

次に、使用しているドメインへのメールを受け入れるように受信者アクセステーブル（RAT）を設定します。

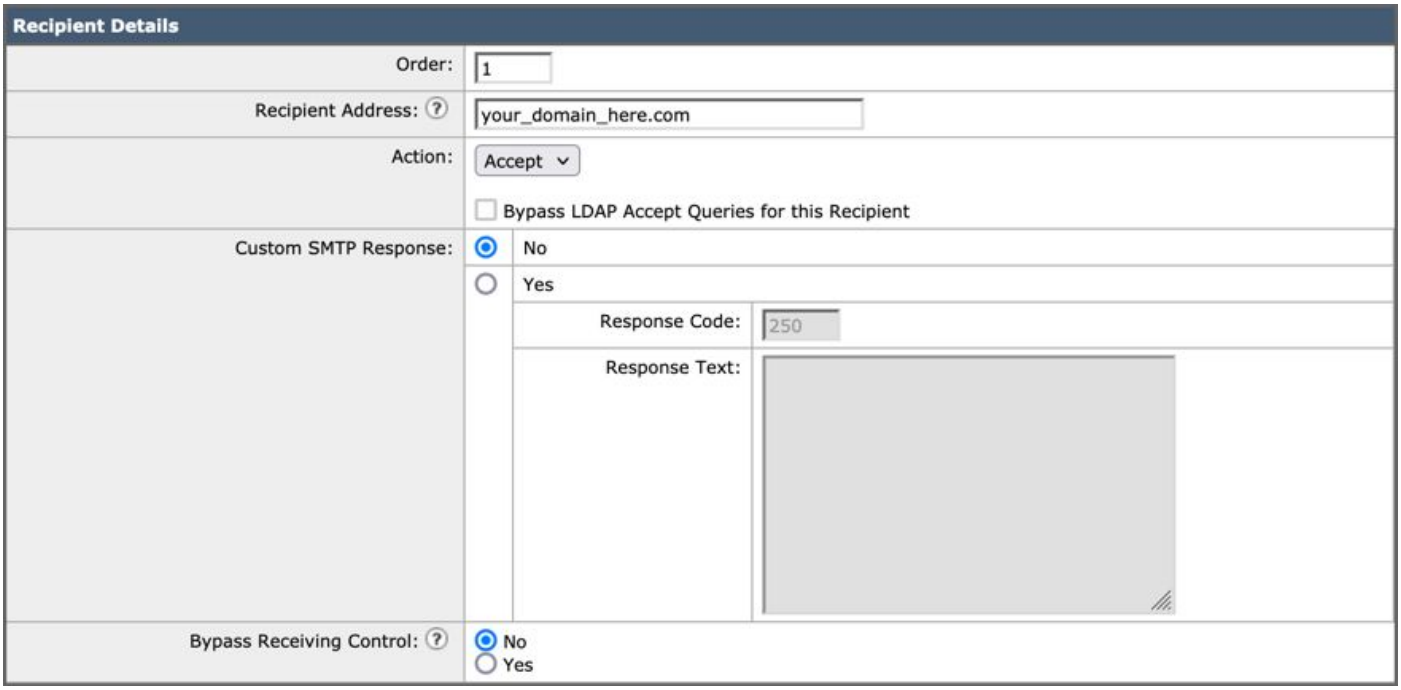
- 移動先 **Mail Policies** > **Recipient Access Table (RAT)**.

> **注**：プライマリメールフローのリスナーの実際の名前に基づいて、リスナーが着信リスナー、着信メール、またはメールフロー用であることを確認します。

- クリック **Add Recipient**.
- Recipient Addressフィールドにドメインを追加します。
- のデフォルトアクションを選択します。 **Accept**.

- クリック **Submit**.
- UI**Commit Changes** の右上にあるをクリックして、設定の変更を保存します。

RATエントリの例を次に示します。

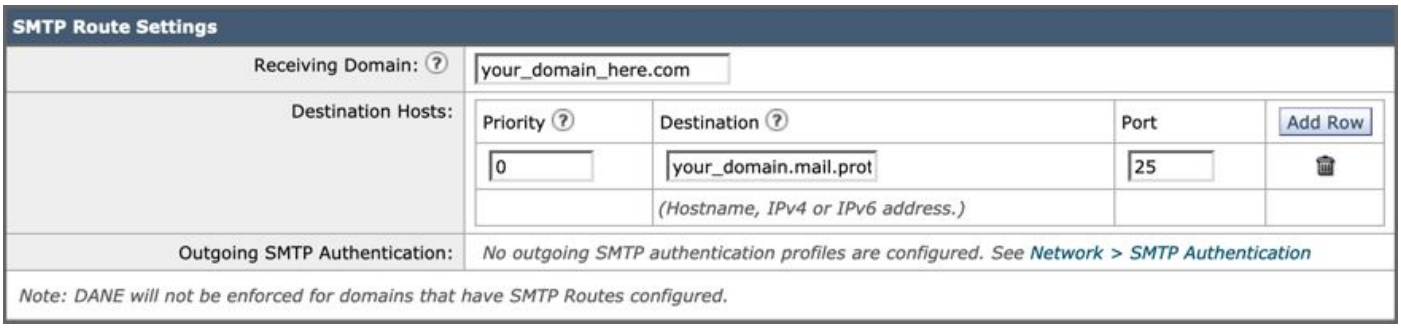


SMTP ルート

Cisco Secure EmailからMicrosoft 365ドメインにメールを配信するためのSMTPルートを設定します。

- 移動先 **Network** > **SMTP Routes**.
- クリック **Add Route...**
- 受信ドメイン：ドメイン名を入力します。
- 宛先ホスト：元のMicrosoft 365 MXレコードを追加します。
- クリック **Submit**.
- UI**Commit Changes** の右上にあるをクリックして、設定の変更を保存します。

SMTPルート設定の例を次に示します。



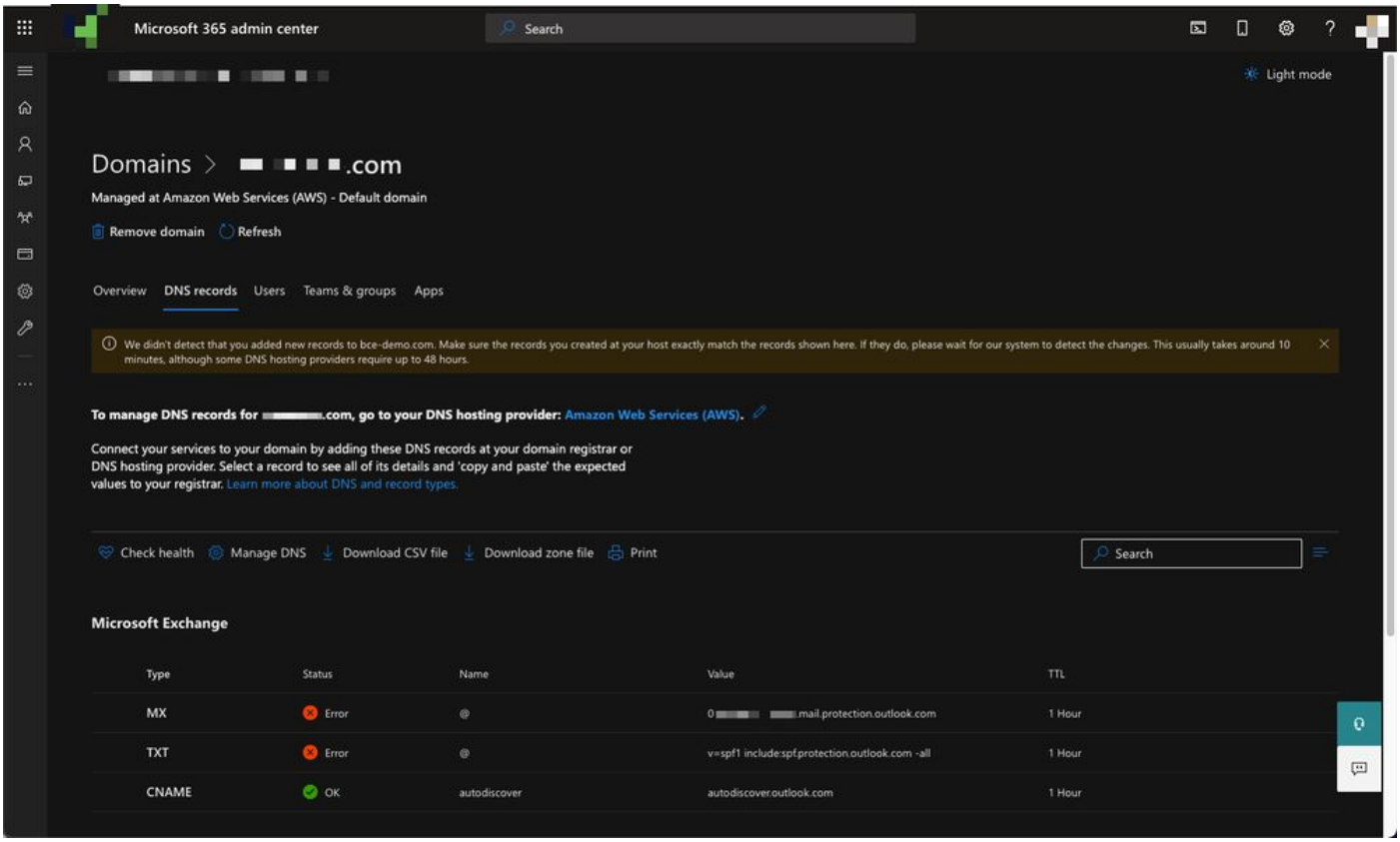
DNS（MX レコード）設定

メール交換(MX)レコードの変更によってドメインをカットオーバーする準備が整いました。DNS管理者と協力して、MXレコードをCisco Secure Email CloudインスタンスのIPアドレスに解決します（Cisco Secure Emailの案内状に記載されています）。

Microsoft 365コンソールからMXレコードへの変更も確認します。

- Microsoft 365管理コンソール(https://admin.microsoft.com)にログインします。
- 移動先 **Home** > **Settings** > **Domains**.
- デフォルトのドメイン名を選択します。
- クリックCheck Health.

これにより、ドメインに関連付けられているDNSレコードとMXレコードがMicrosoft 365でどのように検索されるかについての現在のMXレコードが提供されます。



注：この例では、DNSはアマゾンウェブサービス(AWS)によってホストおよび管理されています。管理者として、DNSがMicrosoft 365アカウント以外の場所でホストされている場合は、警告が表示されます。「your_domain_here.comに新しいレコードが追加されたことを検出できませんでした。ホストで作成したレコードが、ここに表示されているレコードと一致していることを確認してください...」 手順に従って操作すると、MXレコードが、Microsoft 365アカウントにリダイレクトするように最初に設定した値にリセットされます。これにより、Cisco Secure Email Gatewayが着信トラフィックフローから削除されます。

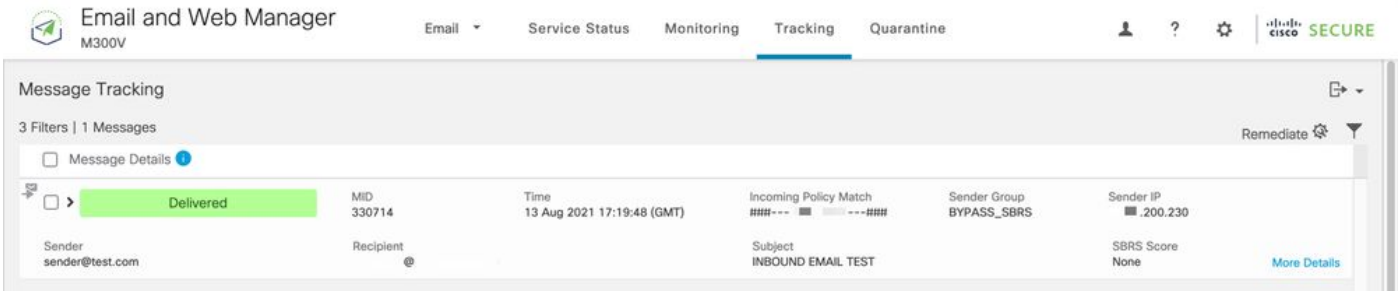
受信電子メールのテスト

Microsoft 365の電子メールアドレスへの着信メールをテストします。次に、Microsoft 365の電子メールの受信トレイに着信したことを確認します。

インスタンスに付属しているCisco Secure Email and Web Manager（SMAとも呼ばれる）のメッセージトラッキングでメールログを検証します。

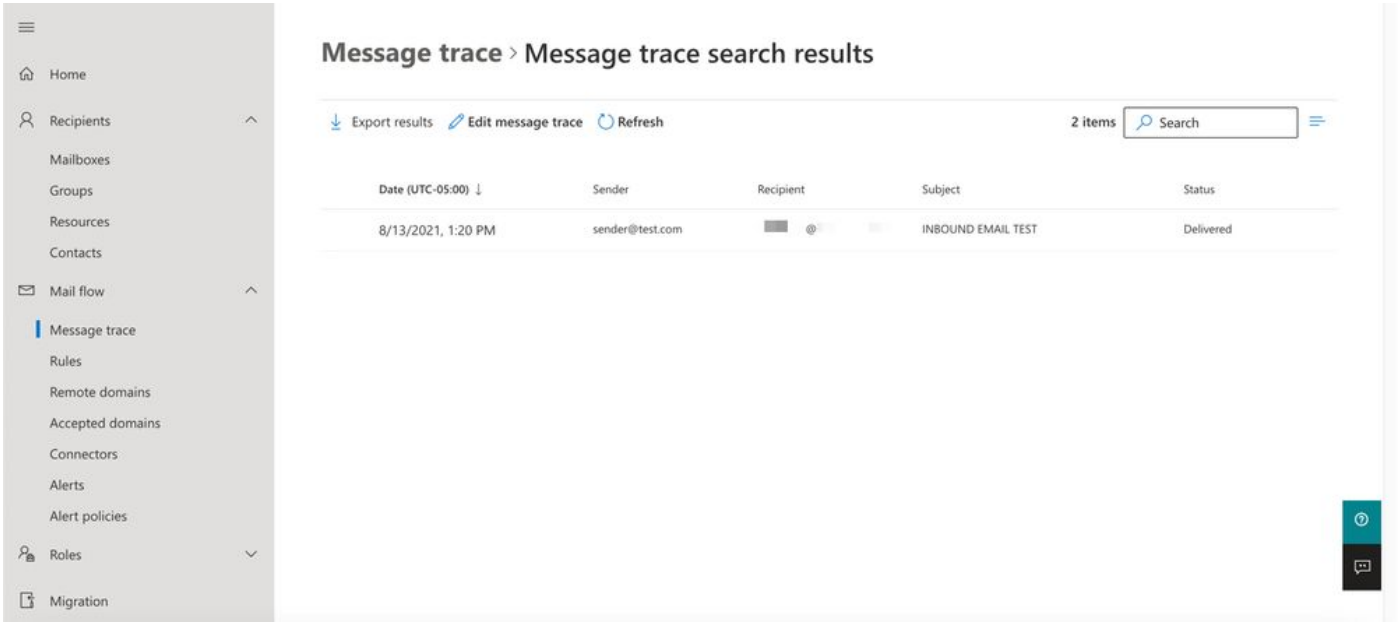
SMA でメールログを確認するには、次の手順に従います。

- SMA(https://sma.iphmx.com/ng-login)にログインします。
- クリック **Tracking**.
- 必要な検索条件を入力して、 **Search**をクリックします。これにより、次のような結果が表示されます。



Microsoft 365 でメールログを確認するには、次の手順に従います。

- Microsoft 365 Admin Center(https://admin.microsoft.com)にログインします。
- 拡張 **Admin Centers**.
- クリック **Exchange**.
- 移動先 **Mail flow** > **Message trace**.
- Microsoftでは、デフォルトの検索条件を提供しています。たとえば、
Messages received by my primary domain in the last dayを選択して検索クエリを開始します。
- 受信者に必要な検索条件を入力し、をクリック **Search** すると、次のような結果が表示されます。



Microsoft 365 から Cisco Secure Email に送信される電子メールの設定

Cisco Secure Email Gateway での RELAYLIST の設定

Cisco Secure Emailの案内状を参照してください。さらに、ゲートウェイ経由の発信メッセージ用にセカンダリインターフェイスが指定されています。

- ゲートウェイにログインします。
- 移動先 **Mail Policies** > **HAT Overview**.

> **注**：外部/発信メールフローのリスナーの実際の名前に基づいて、リスナーが発信リスナー、発信メール、またはメールフロー拡張用であることを確認します。

- クリック **Add Sender Group...**
- 送信者グループを次のように設定します。

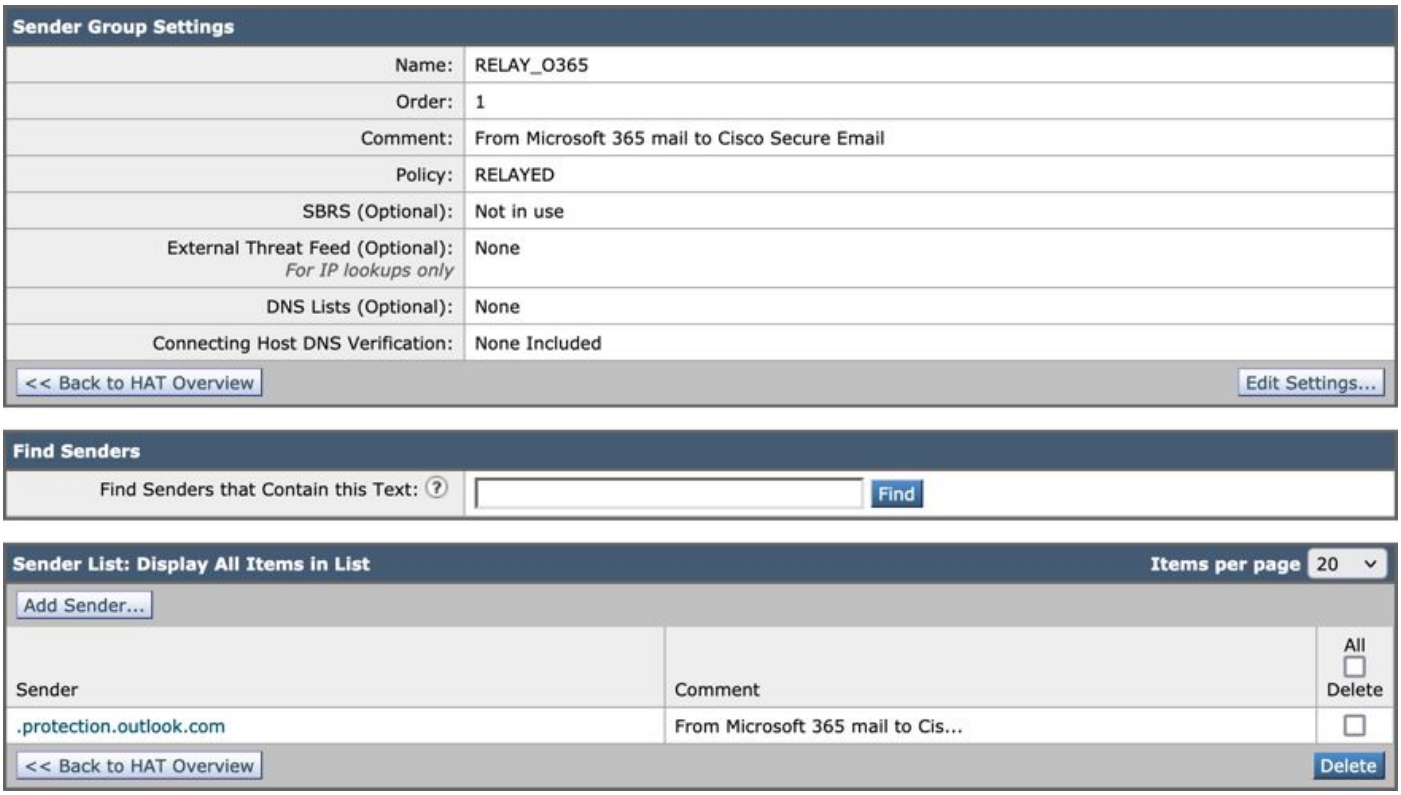
1. 名前： RELAY_O365
2. コメント： **<<送信者グループに通知する場合はコメントを入力>>**
3. ポリシー：リレー
4. クリック **Submit and Add Senders**.

- 送信者: **.protection.outlook.com**

> **注:**.送信者のドメイン名の先頭には（ドット）が必要です。

- クリック **Submit**.
- UI**Commit Changes** の右上にあるをクリックして、設定の変更を保存します。

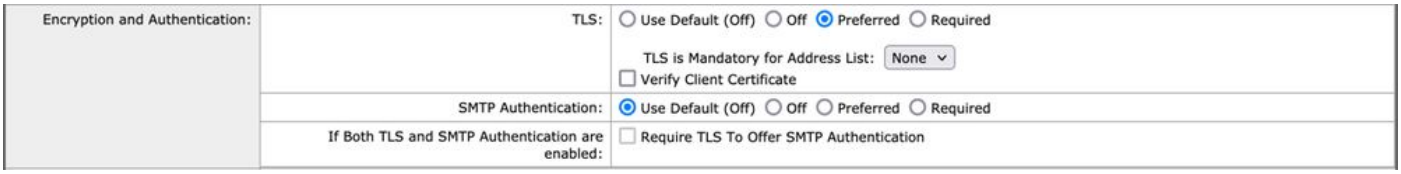
送信者グループの設定の例を次に示します。



TLSの有効化

- クリック <<**Back to HAT Overview**.
- 次の名前のメールフローポリシーをクリックします： **RELAYED**.
- 下にスクロールして、 **Security Features** のセクションで **Encryption and Authentication**.
- TLS の場合は、次を選択します： **Preferred**.
- クリック **Submit**.
- UI**Commit Changes** の右上にあるをクリックして、設定の変更を保存します。

メールフローポリシー設定の例を次に示します。



Microsoft 365 から CES へのメールの設定

- Microsoft 365 Admin Center(https://admin.microsoft.com)にログインします。

- 拡張 **Admin Centers**.

- クリック **Exchange**.

- 移動先 **Mail flow** > **Connectors**.

[+]

- をクリックして、新しいコネクタを作成します。

- Select your mail flow scenarioポップアップウィンドウで、次の項目を選択します。

1. From: Office365

    - これを、次のように変更します。Partner organization

- クリック **Next**.

- 新しいコネクタの名前を入力してください： **Outbound to Cisco CES**.

- 必要に応じて説明を入力します。

- クリック **Next**.

- [このコネクタを使用するタイミング]:

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

    - クリック **Next**.

- クリック **Route email through these smart hosts**.

[+]

- をクリックし、CESウェルカムレターに記載されている発信IPアドレスまたはホスト名を入力します。

- クリック **Save**.

- クリック **Next**.

- Office 365をパートナー組織の電子メールサーバーに接続する方法

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

- 選択.Any digital certificate, including self-signed certificates

- クリック **Next**.

- 確認画面が表示されます。

- クリック **Next**.

[+]

- を使用して有効な電子メールアドレスを入力し、 **OK**.

- をクリック **Validate** し、検証の実行を許可します。

- 完了したら、 **Close**.

- クリックSave.

送信コネクタの外観の例：

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

メールフロールールの作成

1. [送信者の場所の選択]ポップアップで、次のいずれかを選択します。 **Inside the organization**.

    - クリック **OK**.

- クリック **More options...**
- ボタ **add condition** ンをクリックし、2番目の条件を挿入します。

    1. 選択 **The recipient...**

        - 選択: **Is external/internal**.
        - [送信者の場所の選択]ポップアップで、次のいずれかを選択します。 **Outside the organization** .
        - クリック **OK**.

- [*次の操作を行う…]で、次のいずれかを選択します。 **Redirect the message to...**

    1. 選択：**次のコネクタを選択します。**
    2. **Outbound to Cisco CES**コネクタを選択します。
    3. [OK] をクリックします。

- 「*次の操作…」に戻り、2番目のアクションを挿入します。

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

        - 選択: **set the message header**
        - 次のメッセージヘッダーを設定します： **X-OUTBOUND-AUTH**.
        - クリック **OK**.
        - 次の値を設定します： **mysecretkey**.

- クリック **OK**.

- クリック **Save**.

注: Microsoftからの不正なメッセージを防ぐために、メッセージがMicrosoft 365ドメインから発信される際にシークレットヘッダーxがスタンプされます。このヘッダーは、インターネットに配信される前に評価され、削除されます。

Microsoft 365ルーティング設定の例を次に示します。

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:

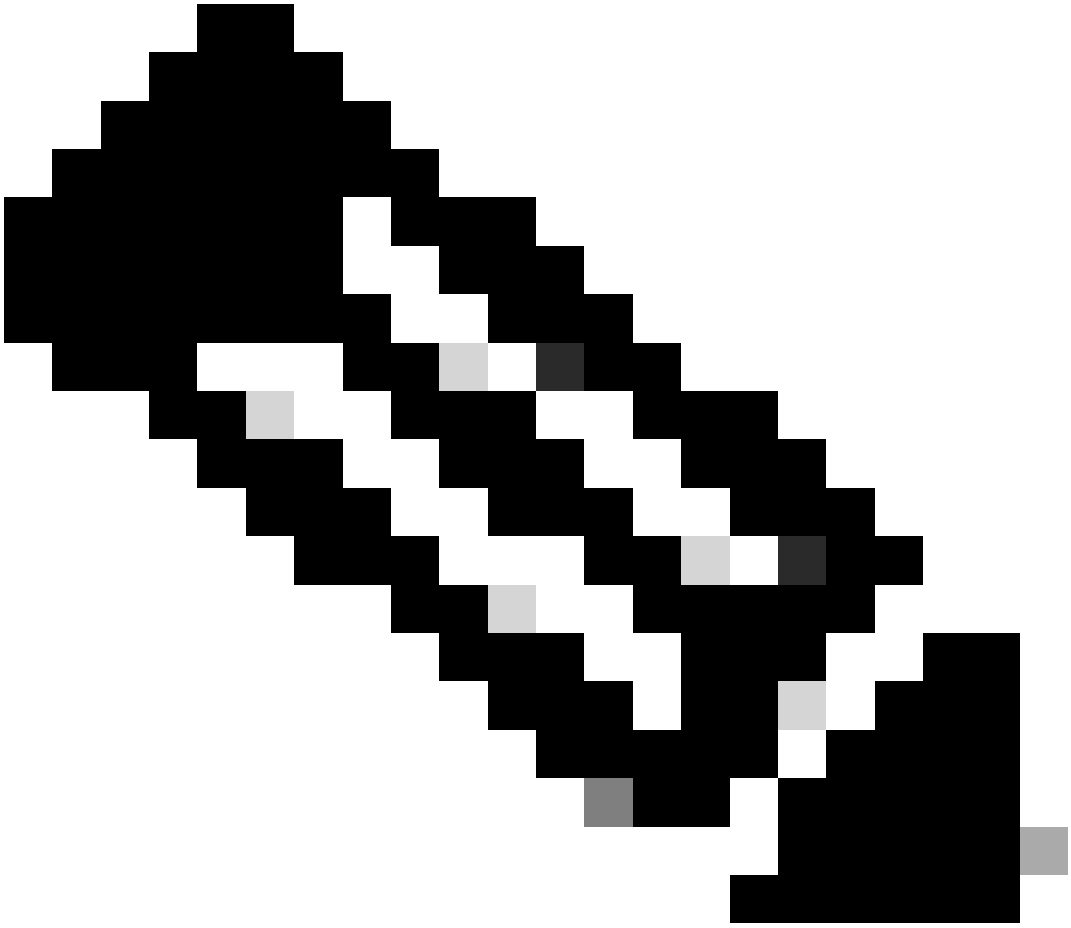
ℹ Rights Management Services (RMS) is a premium feature that requires an Enterprise Client Access License (CAL) or a RMS Online license for each user mailbox. Learn more

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

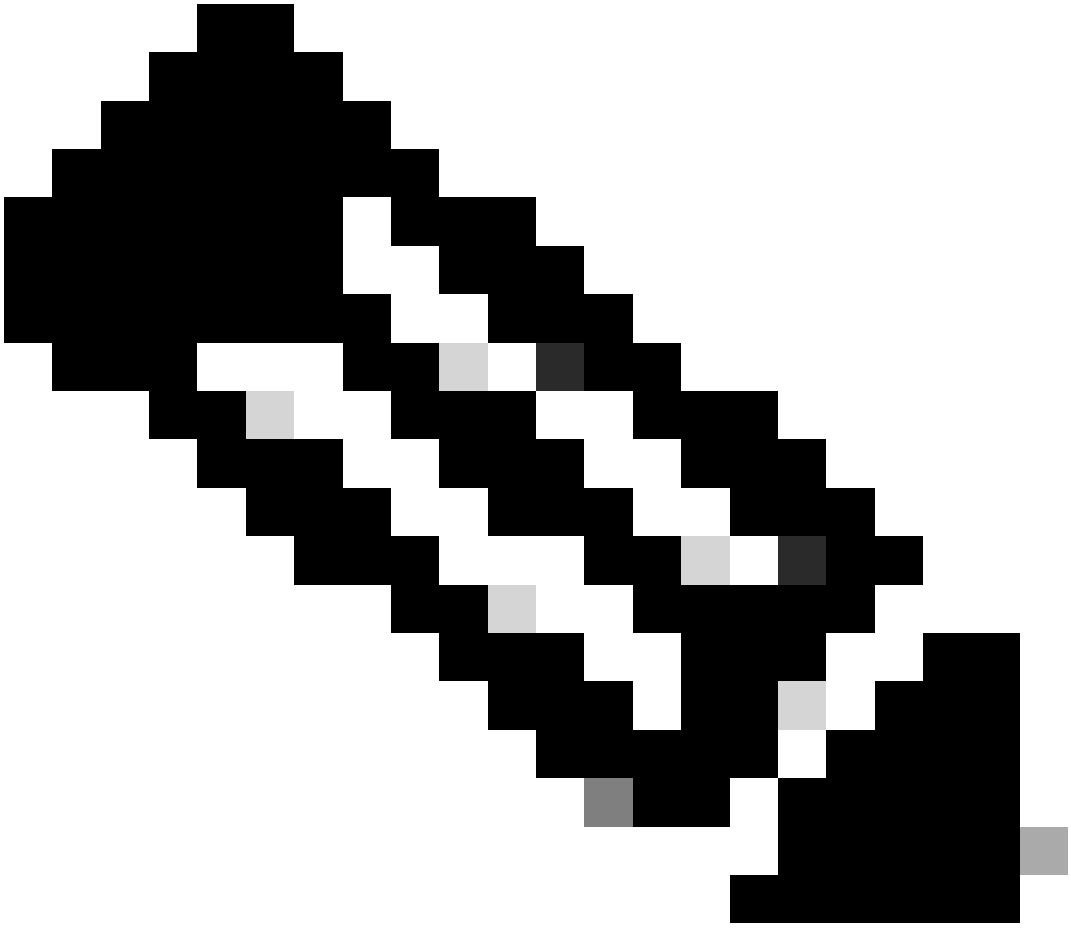
- Returnキーを1回押すと、新しい空白行が作成されます。
- 新しい行に **[.]** と入力し、新しいメッセージフィルタを終了します。
- 1回 **return** クリックすると、[フィルタ]メニューが終了します。

Commit

- コマンドを実行して、設定の変更を保存します。



注：秘密キーには特殊文字を使用しないでください。メッセージフィルタに表示される^および$は正規表現文字であり、例に示すように使用されます。



注:RELAYLISTの設定方法の名前を確認してください。この名前は、代替名を使用して設定することも、リレーポリシーまたはメールプロバイダーに基づいて特定の名前を使用することもできます。

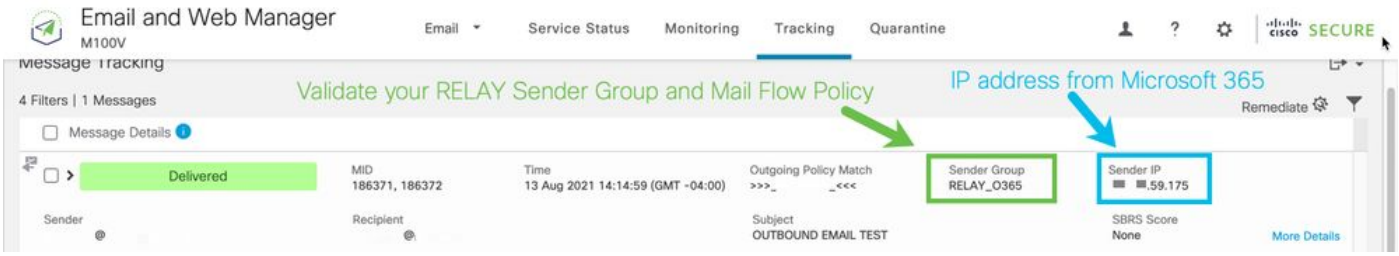
送信電子メールのテスト

Microsoft 365の電子メールアドレスから外部ドメインの受信者への送信メールをテストします。Cisco Secure Email and Web Managerからメッセージトラッキングを確認して、メッセージが適切にアウトバウンドにルーティングされていることを確認できます。

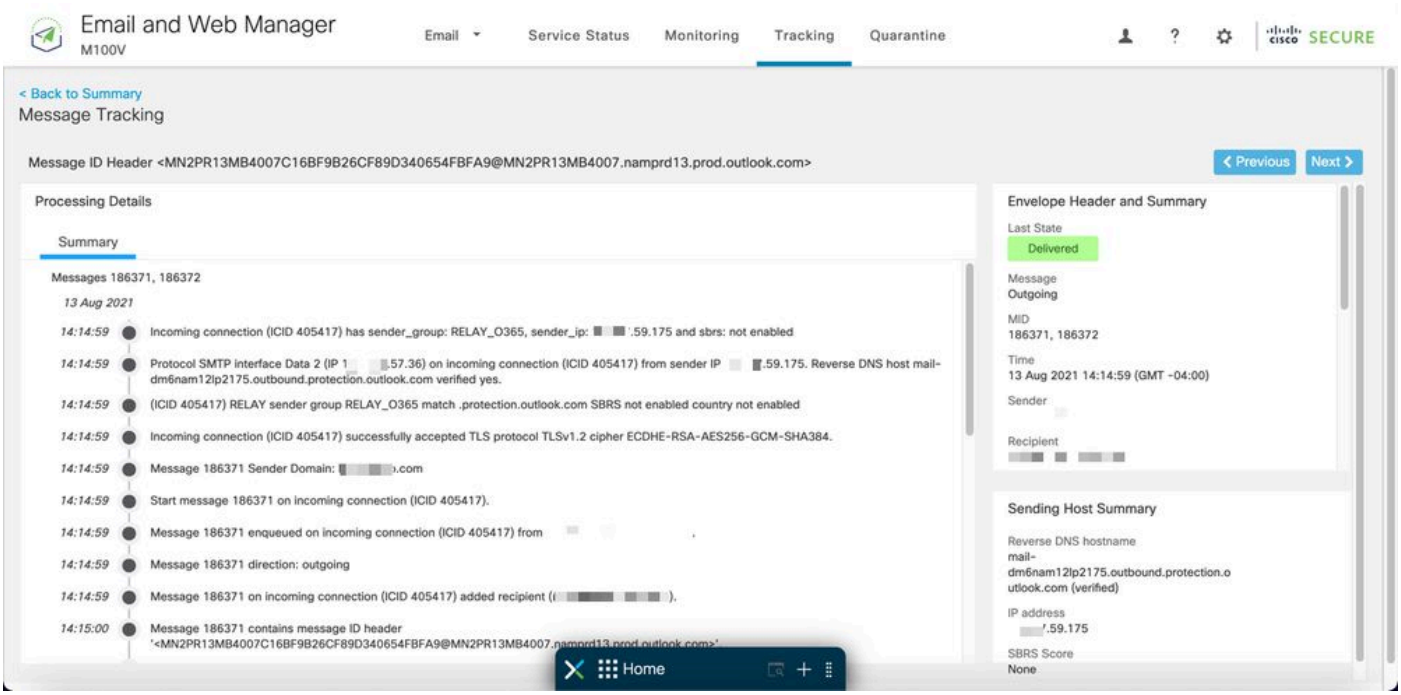
注：ゲートウェイ上のTLS設定(**System Administration** > **SSL設定**)と、発信SMTPに使用される暗号を確認してください。シスコのベストプラクティスでは次のことを推奨しています。

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

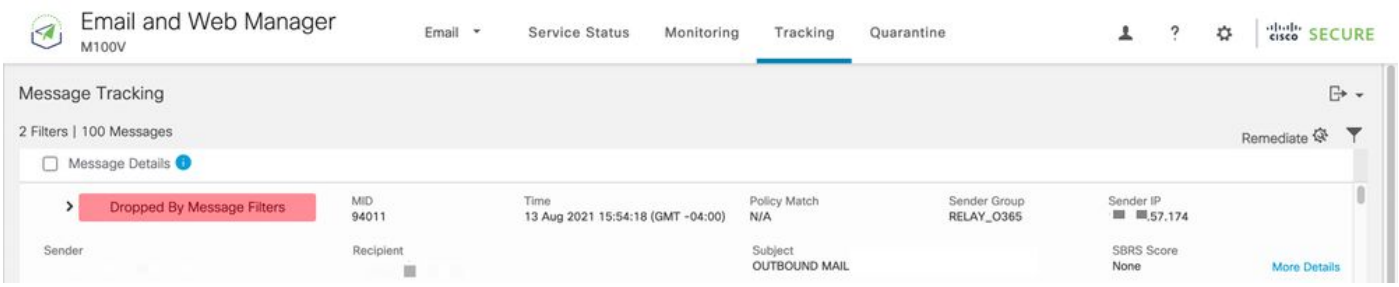
配信が成功した場合のトラッキングの例：

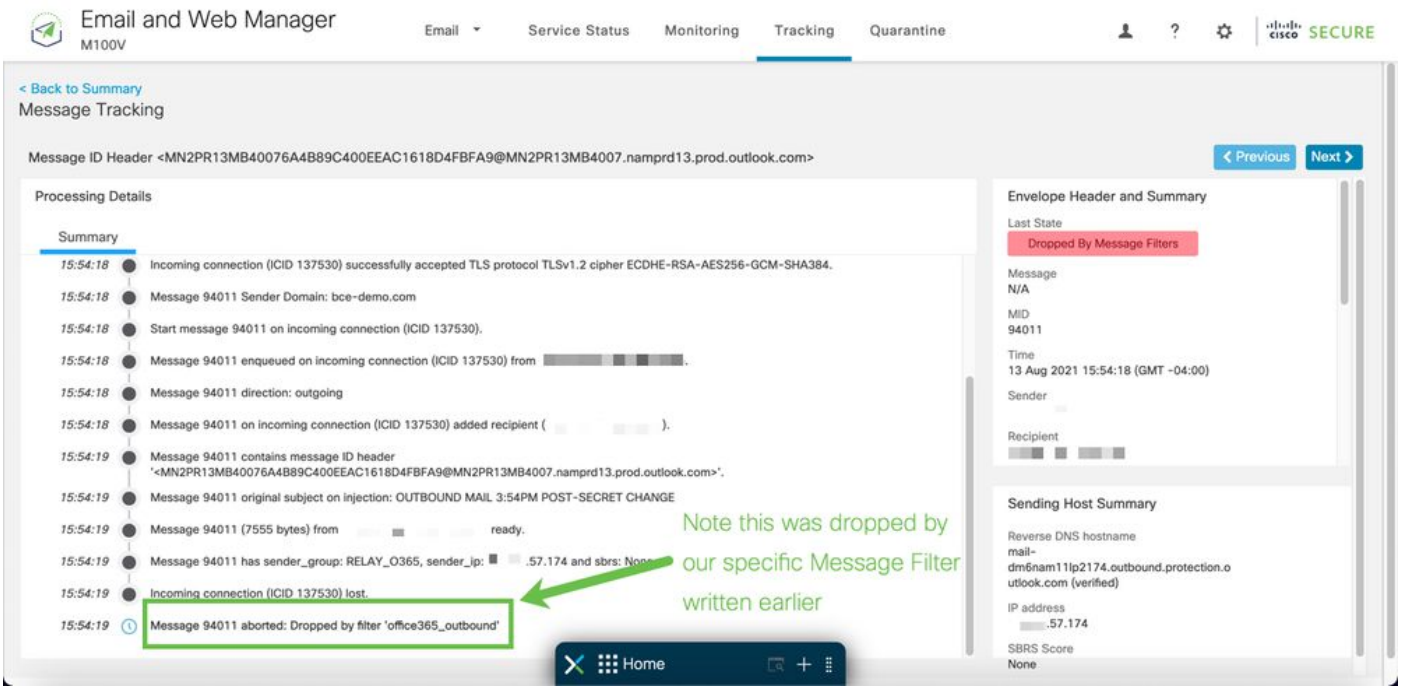


メッセージの詳細を確認するには、**More Details** をクリックしてください：



x ヘッダーが一致しないメッセージトラッキングの例：





関連情報

Cisco Secure Email Gatewayに関するドキュメント

- リリース ノート
- ユーザガイド
- CLIリファレンスガイド
- Cisco Secure Email GatewayのAPIプログラミングガイド
- Cisco Secure Email Gatewayで使用されるオープンソース
- シスココンテンツセキュリティ仮想アプライアンスインストールガイド（vESAを含む）

セキュアなEメールクラウドゲートウェイに関する文書

- リリース ノート
- ユーザガイド

Cisco Secure Email and Web Managerに関するドキュメント

- リリースノートと互換性マトリクス

- ユーザガイド
- Cisco Secure Email and Web ManagerのAPIプログラミングガイド
- シスココンテンツセキュリティ仮想アプライアンスインストールガイド（vSMAを含む）

Cisco Secure製品ドキュメント

- Cisco Secureポートフォリオの命名アーキテクチャ

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。