Configure Microsoft 365 with Secure Email

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure Microsoft 365 with Secure Email

- Configure Incoming Email in Microsoft 365 from Cisco Secure Email
  - Bypass Spam Filtering Rule
  - Receiving Connector
- Configure Mail from Cisco Secure Email to Microsoft 365
  - Destination Controls
  - Recipient Access Table
  - SMTP Routes
  - DNS (MX Record) Configuration
  - Test Inbound Email
- Configure Outgoing Email from Microsoft 365 to Cisco Secure Email
  - Configure RELAYLIST on the Cisco Secure Email Gateway
  - Enable TLS
  - Configure Mail from Microsoft 365 to CES
  - Create a Mail Flow Rule
  - Prevent Open Relay
  - Option 1: Prevent Open Relay via GUI
  - Option 2: Prevent Open Relay via CLI
  - Test Outbound Email

Related Information

- Cisco Secure Email Gateway Documentation
- Secure Email Cloud Gateway Documentation
- Cisco Secure Email and Web Manager Documentation
- Cisco Secure Product Documentation

Introduction

This document describes the configuration steps to integrate Microsoft 365 with Cisco Secure Email for inbound and outbound email delivery.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Email Gateway or Cloud Gateway
- Command Line Interface (CLI) access to your Cisco Secure Email Cloud Gateway environment: Cisco Secure Email Cloud Gateway > Command Line Interface (CLI) Access
- Microsoft 365
- Simple Mail Transfer Protocol (SMTP)
- Domain Name Server or Domain Name System (DNS)

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document can be used for either on-premises Gateways or Cisco Cloud Gateways.

If you are a Cisco Secure Email administrator, your welcome letter includes your Cloud Gateway IP addresses and other pertinent information. In addition to the letter you see here, an encrypted email is sent to you that provides you with additional details on the number of Cloud Gateway (also known as ESA) and Cloud Email and Web Manager (also known as SMA) provisioned for your allocation. If you have not received or do not have a copy of the letter, contact ces-activations@cisco.com with your contact information and domain name under service.

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

Each client has dedicated IPs. You can use the assigned IPs or hostnames in the Microsoft 365 configuration.

Note: It is highly recommended that you test before any planned production mail cutover because configurations take time to replicate in the Microsoft 365 Exchange console. At a minimum, allow one hour for all changes to take effect.

Note: The IP addresses in the screen capture are proportional to the number of Cloud Gateways provisioned to your allocation. For example, xxx.yy.140.105 is the Data 1 interface IP address for Gateway 1, and xxx.yy.150.143 is the Data 1 interface IP address for Gateway 2. Data 2 interface IP address for Gateway 1 is xxx.yy.143.186, and Data 2 interface IP address for Gateway 2 is xxx.yy.32.98. If your welcome letter does not include information for Data 2 (outgoing interface IPs), contact Cisco TAC to obtain the Data 2 interface added to your allocation.

Configure Microsoft 365 with Secure Email

Configure Incoming Email in Microsoft 365 from Cisco Secure Email

Bypass Spam Filtering Rule

1. Log in to the Microsoft Exchange Admin Center
2. From the left-hand menu, navigate to **Mail flow** > **Rules**.
3. Click on **Add a rule** to create a new rule.
4. Enter a name for your new rule: **Bypass spam filtering - inbound email from Cisco CES**.
5. For *Apply this rule if..., choose **The sender - IP address is in any of these ranges or exactly matches**.
    1. For the specify IP address ranges pop-up, add the IP addresses provided in your Cisco Secure Email welcome letter.
    2. Click **OK**.
6. For *Do the following..., select **Modify the message properties** and choose **set the spam confidence level (SCL)**using **Bypass spam filtering**.
7. Click **Next**.
8. Select **Enforce** and click on Next.
9. And Finish.

An example of how your rule looks:

Bypass spam filtering - inbound email from Cisco CES

Edit rule conditions Edit rule settings

Status: Disabled

Enable or disable rule

Disabled

Rule settings

Rule name
Bypass spam filtering - inbound email from Cisco CES

Severity
Not specified

Senders address
Matching Header

For rule processing errors
Ignore

Mode
Enforce

Set date range
Specific date range is not set

Priority
2

Rule description

Apply this rule if

sender ip addresses belong to one of these ranges: '1[redacted] or '1[redacted]' or '1[redacted]'

Do the following

Set the spam confidence level (SCL) to '-1'

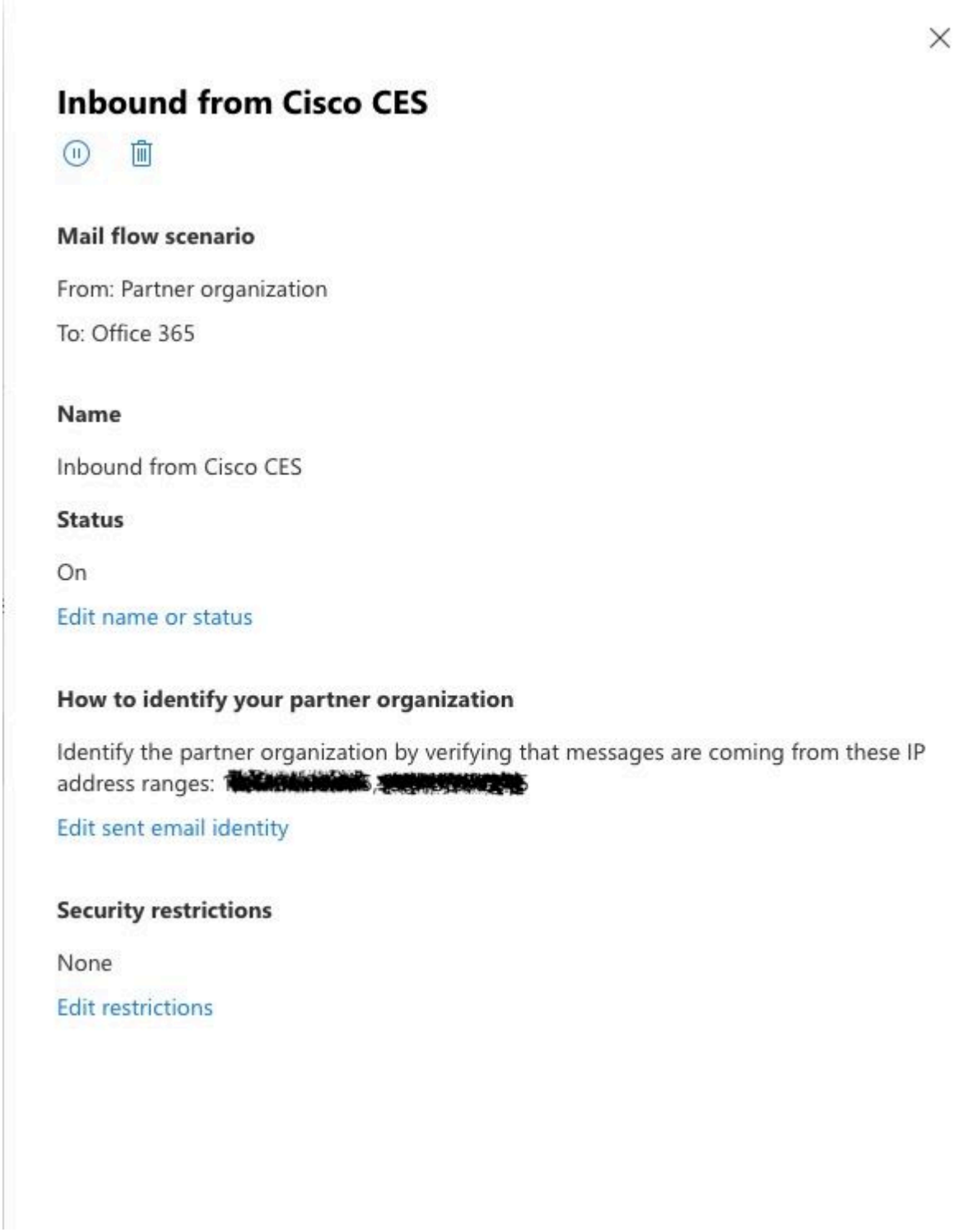
Rule comments

Bypass Rule

Receiving Connector

1. Remain in the Exchange Admin Center.
2. From the left-hand menu, navigate to **Mail flow** > **Connectors**.
3. Click **[+ Add a connector]** to create a new connector.
4. In the Select your mail flow scenario pop-up window, choose:
    1. From: Partner organization
    2. To: **Office365**
5. Click **Next**.
6. Enter a name for your new connector: **Inbound from Cisco CES**.
7. Enter a description, (optional).
8. Click **Next**.
9. Select **By verifying that the IP address of the sending...**
10. Click **[+]** and add the IP addresses provided in the welcome letter and used in the Bypass Spam filtering rule.
11. Click **Next**.
12. Choose **Reject email messages if they aren't sent over Transport Layer Security (TLS)**.
13. Click **Next**.
14. Click **Save**.

An example of how your connector configuration looks:



Connector inbound

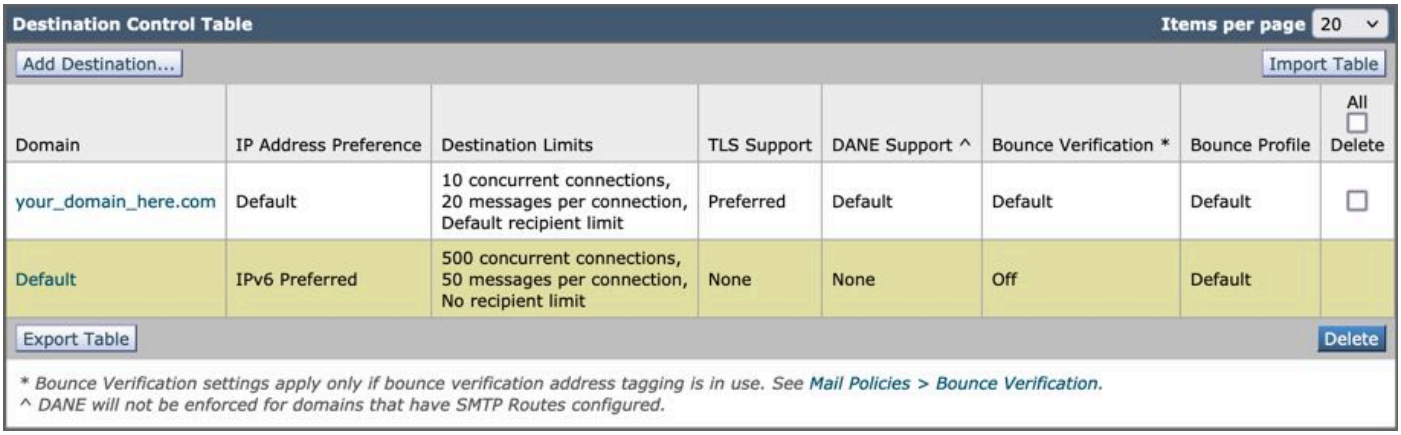
Configure Mail from Cisco Secure Email to Microsoft 365

Destination Controls

Impose a self-throttle to a delivery domain in your Destination Controls. Of course, you can remove the throttle later, but these are new IPs to Microsoft 365, and you do not want any throttling by Microsoft due to its unknown reputation.

1. Log in to your Gateway.
2. Navigate to **Mail Policies** > **Destination Controls**.
3. Click **Add Destination**.
4. Use:
    1. Destination: enter your **domain name**
    2. Concurrent Connections: **10**
    3. Maximum Messages Per Connection: **20**
    4. TLS Support: **Preferred**
5. Click **Submit**.
6. Click **Commit Changes** in the upper right-hand of the User Interface (UI) to save your configuration changes.

An example of how your Destination Control Table looks:



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.

Recipient Access Table

Next, set the Recipient Access Table (RAT) to accept mail for your domains:

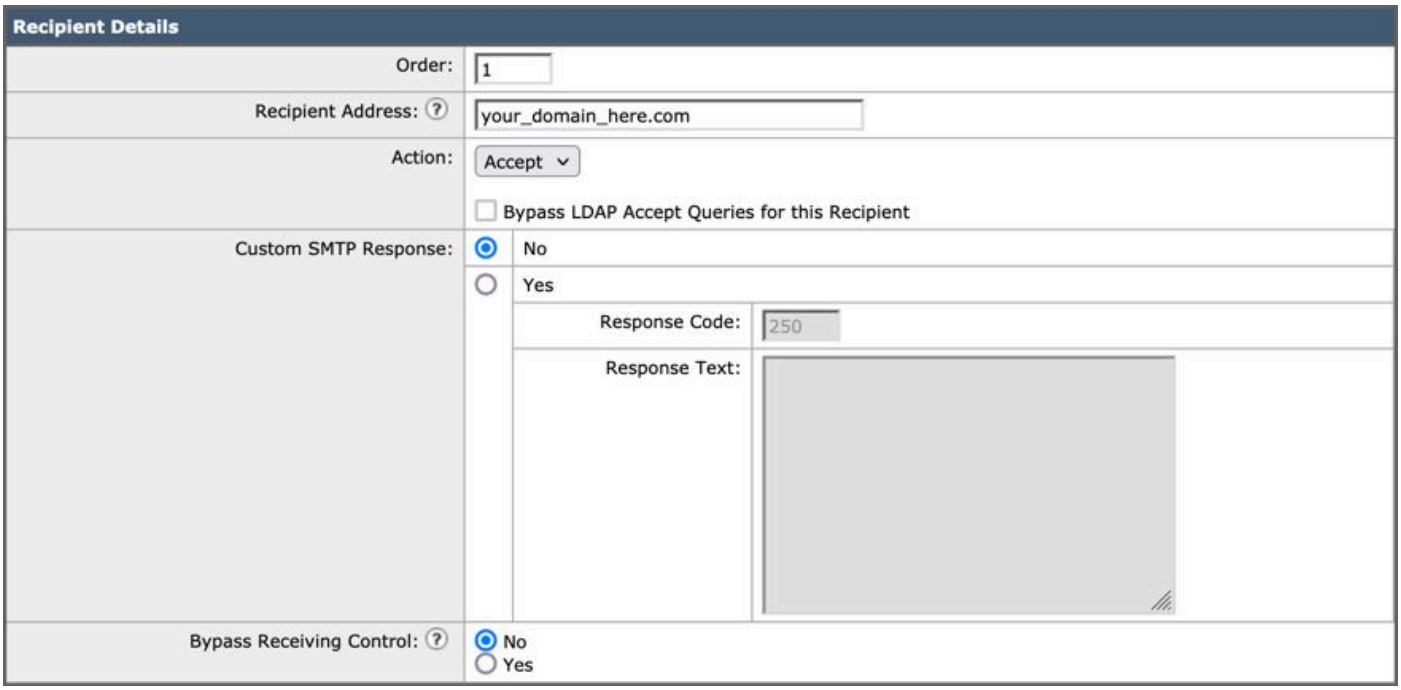
1. Navigate to **Mail Policies** > **Recipient Access Table (RAT)**.

Note: Make sure the Listener is for Incoming Listener, IncomingMail, or MailFlow, based on the actual name of your Listener for your primary mail flow.

---

1. Click **Add Recipient**.
2. Add your domain(s) in the Recipient Address field.
3. Choose the default action of **Accept**.
4. Click **Submit**.
5. Click **Commit Changes** in the upper right-hand of the UI to save your configuration changes.

An example of how your RAT entry looks:

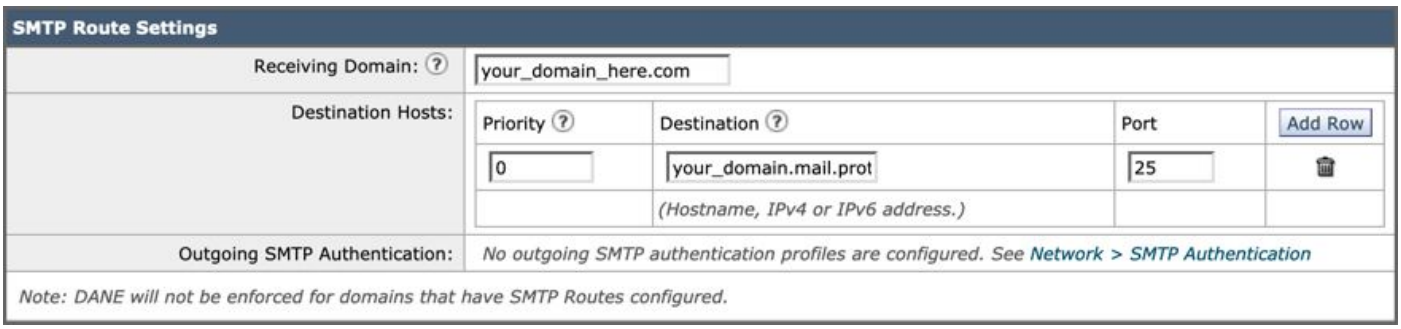


SMTP Routes

Set the SMTP route to deliver mail from Cisco Secure Email to your Microsoft 365 domain:

1. Navigate to **Network** > **SMTP Routes**.
2. Click **Add Route...**
3. Receiving Domain: enter your **domain name**.
4. Destination Hosts: add your **original Microsoft 365 MX record**.
5. Click **Submit**.
6. Click **Commit Changes** in the upper right-hand of the UI to save your configuration changes.

An example of how your SMTP Route Settings looks:



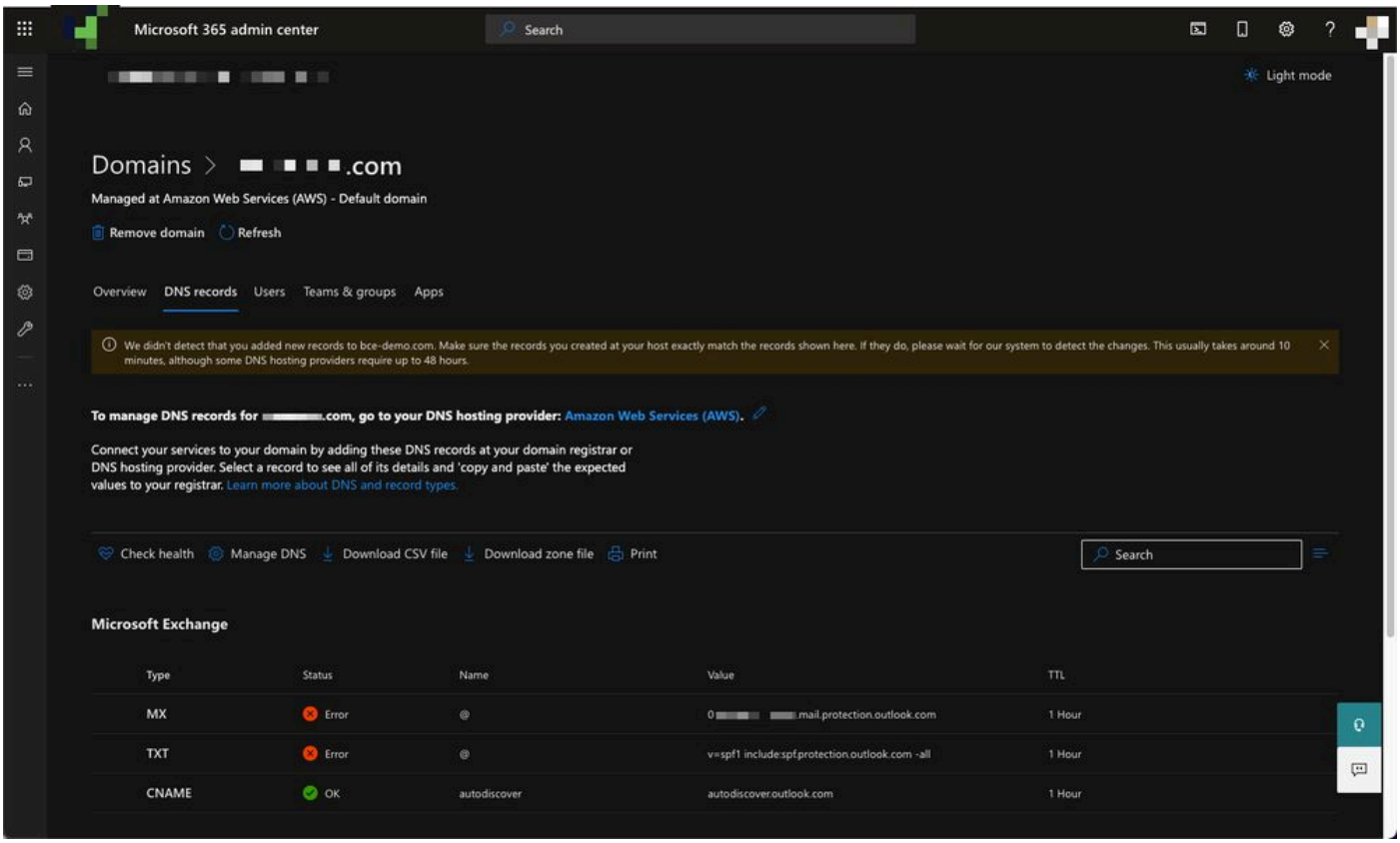
DNS (MX Record) Configuration

You are ready to cut over the domain through a Mail Exchange (MX) record change. Work with your DNS administrator to resolve your MX records to the IP addresses for your Cisco Secure Email Cloud instance, as provided in your Cisco Secure Email welcome letter.

Verify the change to the MX record from your Microsoft 365 console as well:

1. Log in to the Microsoft Office 365 Admin Console.
2. Navigate to **Home** > **Settings** > **Domains**.
3. Choose your **default domain name**.
4. Click**Check Health**.

This provides the current MX Records of how Microsoft 365 looks up your DNS and MX records associated with your domain:



Note: In this example, the DNS is hosted and managed by Amazon Web Services (AWS). As an administrator, expect to see a warning if your DNS is hosted anywhere outside of the Microsoft 365 account. You can ignore warnings like: "We didn't detect that you added new records to your_domain_here.com. Make sure the records you created at your host match those shown here..." The step-by-step instructions reset the MX records to what was initially configured to redirect to your Microsoft 365 account. This removes the Cisco Secure Email Gateway from the incoming traffic flow.

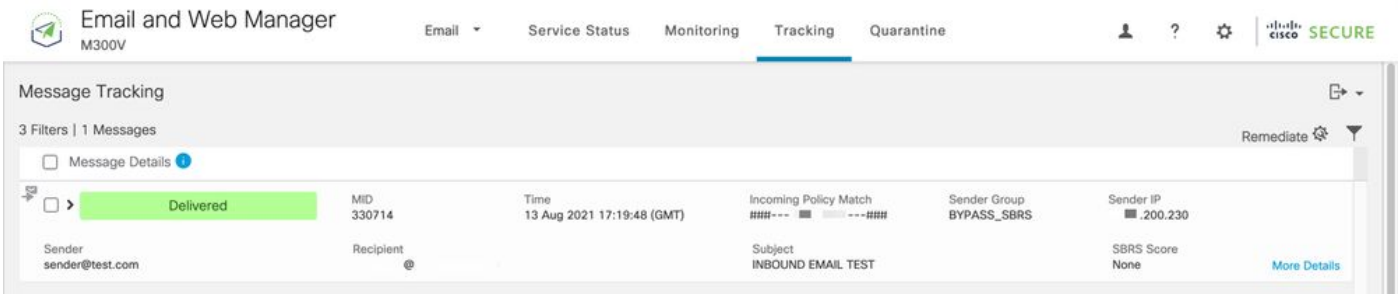
Test Inbound Email

Test inbound mail to your Microsoft 365 email address. Then, check to see that it arrives in your Microsoft 365 email inbox.

Validate the mail logs in Message Tracking on your Cisco Secure Email and Web Manager (also known as SMA) provided with your instance.

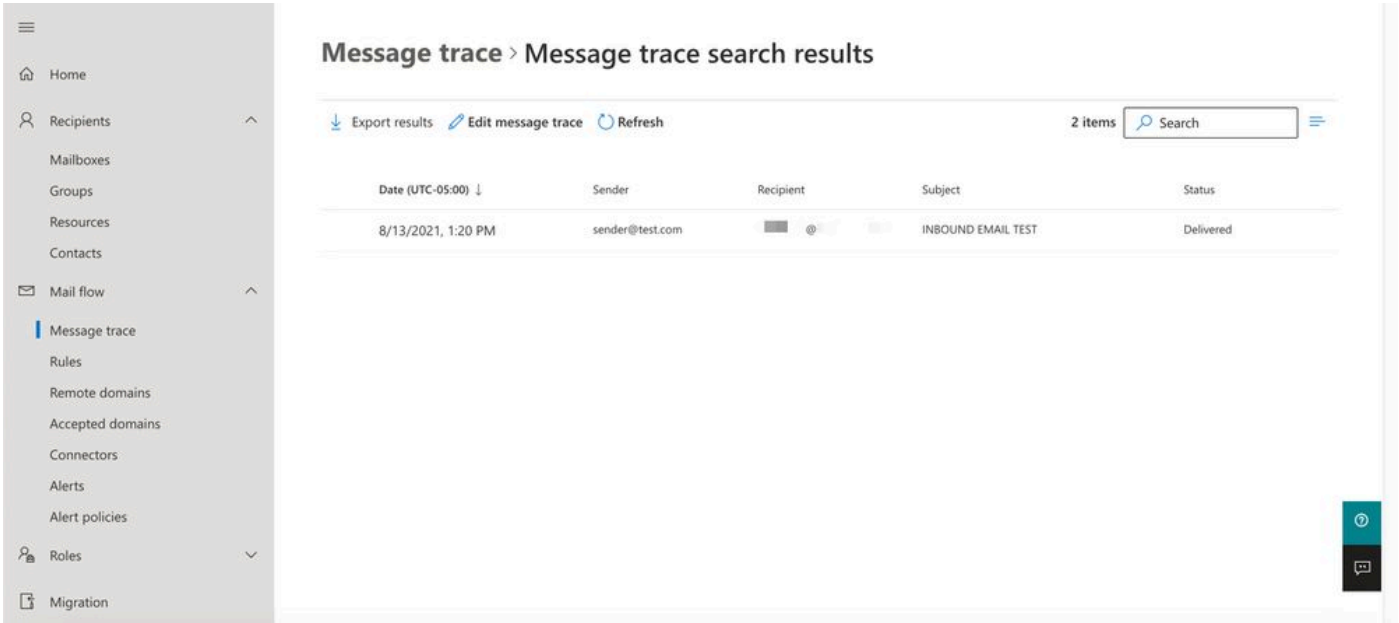
To see mail logs on your SMA:

1. Log in to your SMA.
2. Click **Tracking**.
3. Enter the needed search criteria and click **Search**;and expect to see these results:



To see mail logs in Microsoft 365:

1. Log in to the Microsoft Exchange Admin Center.
2. Navigate to **Mail flow** > **Message Trace**.
3. Microsoft provides default criteria to search with. For example, choose **Messages received by my primary domain in the last day** to start your search query.
4. Enter the needed search criteria for recipients and click **Search** and expect to see results similar to:



Configure Outgoing Email from Microsoft 365 to Cisco Secure Email

Configure RELAYLIST on the Cisco Secure Email Gateway

Refer to your Cisco Secure Email welcome letter. In addition, a secondary interface is specified for outbound messages via your Gateway.

1. Log in to your Gateway.
2. Navigate to **Mail Policies** > **HAT Overview**.

Note: Make sure the Listener is set to Outgoing Listener, OutgoingMail, or MailFlow-Ext, based on the actual name of your Listener for your external/outbound mail flow.

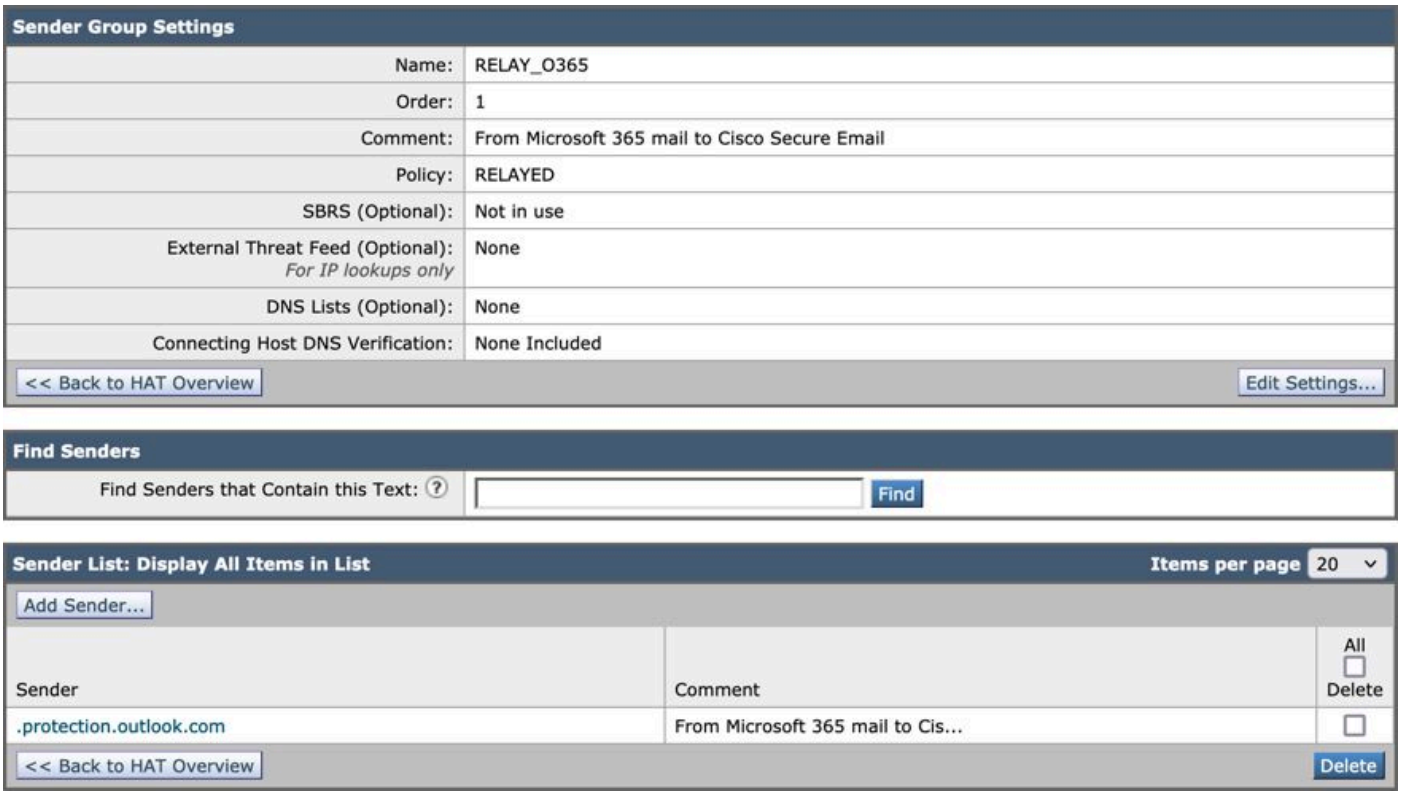
---

3. Click **Add Sender Group...**
4. Configure the Sender Group as:
    1. Name: **RELAY_O365**
    2. Comment: <<enter a comment if you wish to notate your sender group>>
    3. Policy: **RELAYED**
    4. Click **Submit and Add Senders**.
    5. Sender: **.protection.outlook.com**.

    Note: The . (dot) at the beginning of the sender domain name is required.

    6. Click **Submit**.
    7. Click **Commit Changes** in the upper right-hand of the UI to save your configuration changes.

An example of how your Sender Group Settings looks:



Enable TLS

1. Click <<**Back to HAT Overview**.
2. Click the Mail Flow Policy named: **RELAYED**.
3. Scroll down and look in the **Security Features** section for **Encryption and Authentication**.
4. For TLS, choose: **Preferred**.
5. Click **Submit**.
6. Click **Commit Changes** in the upper right-hand of the UI to save your configuration changes.

An example of how your Mail Flow Policy configuration looks:

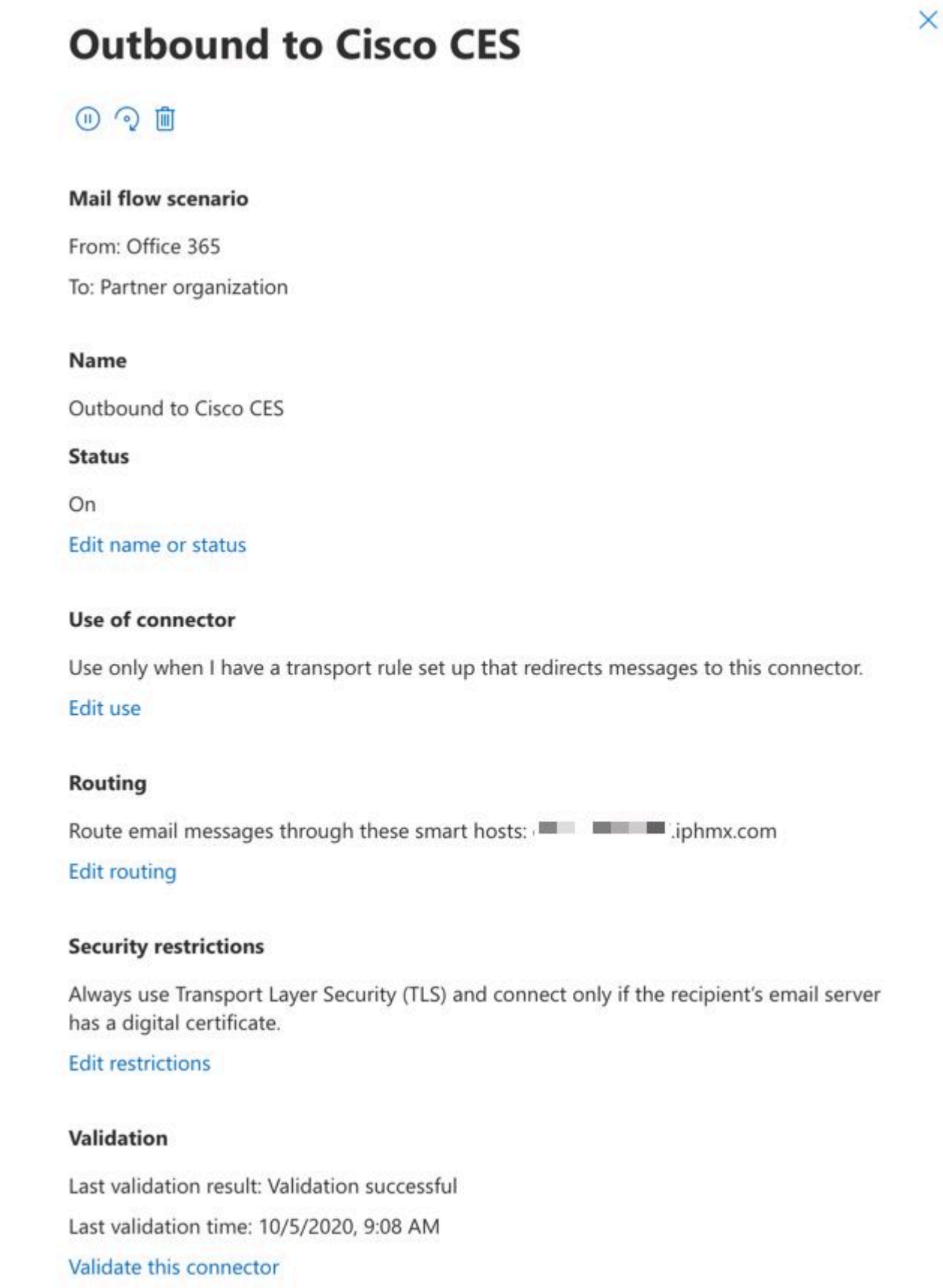


Configure Mail from Microsoft 365 to CES

1. Log in to the Microsoft Exchange Admin Center.
2. Navigate to **Mail flow** > **Connectors.**
3. Click [+ Add a connetor] to create a new connector.
4. In the Select your mail flow scenario pop-up window, choose:
    1. From: Office365
    2. To:Partner organization
5. Click **Next**.

6. Enter a name for your new connector: **Outbound to Cisco CES**.
7. Enter a description (optional).
8. Click **Next**.
9. For "When do you want to use this connector?":
    1. Choose: **Only when I have a transport rule set up that redirects messages to this connector**.
    2. Click **Next**.
10. Click **Route email through these smart hosts**.
11. Click **[+]** and enter the outbound IP addresses or hostnames provided in your CES welcome letter.
12. Click **Save**.
13. Click **Next**.
14. For "How Office 365 connect to your partner organization's email server?":
    1. Choose: **Always use TLS to secure the connection (recommended)**.
    2. ChooseAny digital certificate, including self-signed certificates.
    3. Click **Next**.
15. You are presented with the confirmation screen.
16. Click **Next**.
17. Use **[+]** to enter a valid email address and click **OK**.
18. Click **Validate** and allow the validation to run.
19. Once complete, click **Close**.
20. ClickSave.

An example of how your Outbound Connector looks:



Create a Mail Flow Rule

1. Log in to your Exchange Admin Center.
2. Click **Mail Flow**;and be sure you're on the rules tab.
3. Click **[+]** to add a new rule.
4. Choose **Create a new rule**.
5. Enter a name for your new rule: **Outbound to Cisco CES**.
6. For *Apply this rule if..., choose: **The sender is located...**
    1. For the select sender location pop-up, choose: **Inside the organization**.
    2. Click **OK**.
7. Click **More options...**
8. Click the **add condition** button and insert a second condition:
    1. Choose **The recipient...**
    2. Choose: **Is external/internal**.
    3. For the select sender location pop-up, choose: **Outside the organization**.
    4. Click **OK**.
9. For *Do the following..., choose: **Redirect the message to...**
    1. Select: **the following connector**.
    2. And select your **Outbound to Cisco CES** connector.
    3. Click **OK**.
10. Return to "*Do the following..." and insert a second action:
    1. Choose: **Modify the message properties...**
    2. Choose: **set the message header**.
    3. Set the message header: **X-OUTBOUND-AUTH**.
    4. Click **OK**.
    5. Set the value: **mysecretkey**.
        1. **mysecretkey** is simply a placeholder. Please customize this so it is specific to your environment.
    6. Click **OK**.
11. Click **Save**.

Note: To prevent unauthorized messages from Microsoft, a secret x-header can be stamped when messages leave your Microsoft 365 domain; this header is evaluated and removed before delivery to the Internet.

An example of how your Microsoft 365 Routing configuration looks:

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

Prevent Open Relay



Warning: This is a crucial step. Securing the Outgoing Listener is essential to prevent unauthorized users from relaying email through the device.

There are two options listed below. It is recommended to use the Message Filter (CLI) or the Content Filter (GUI) for those less familiar with CLI (Command Line Interface).

Option 1: Prevent Open Relay via GUI

Create two Content Filters in the GUI:

- The first filter takes action on any emails that either do not have the X-OUTBOUND-AUTH header or do not contain the value previously configured in Microsoft Office 365.
- The second filter applies to legitimate emails sent from the Microsoft Office 365 tenant. This filter removes the X-OUTBOUND-AUTH header so it cannot be misused in the future.

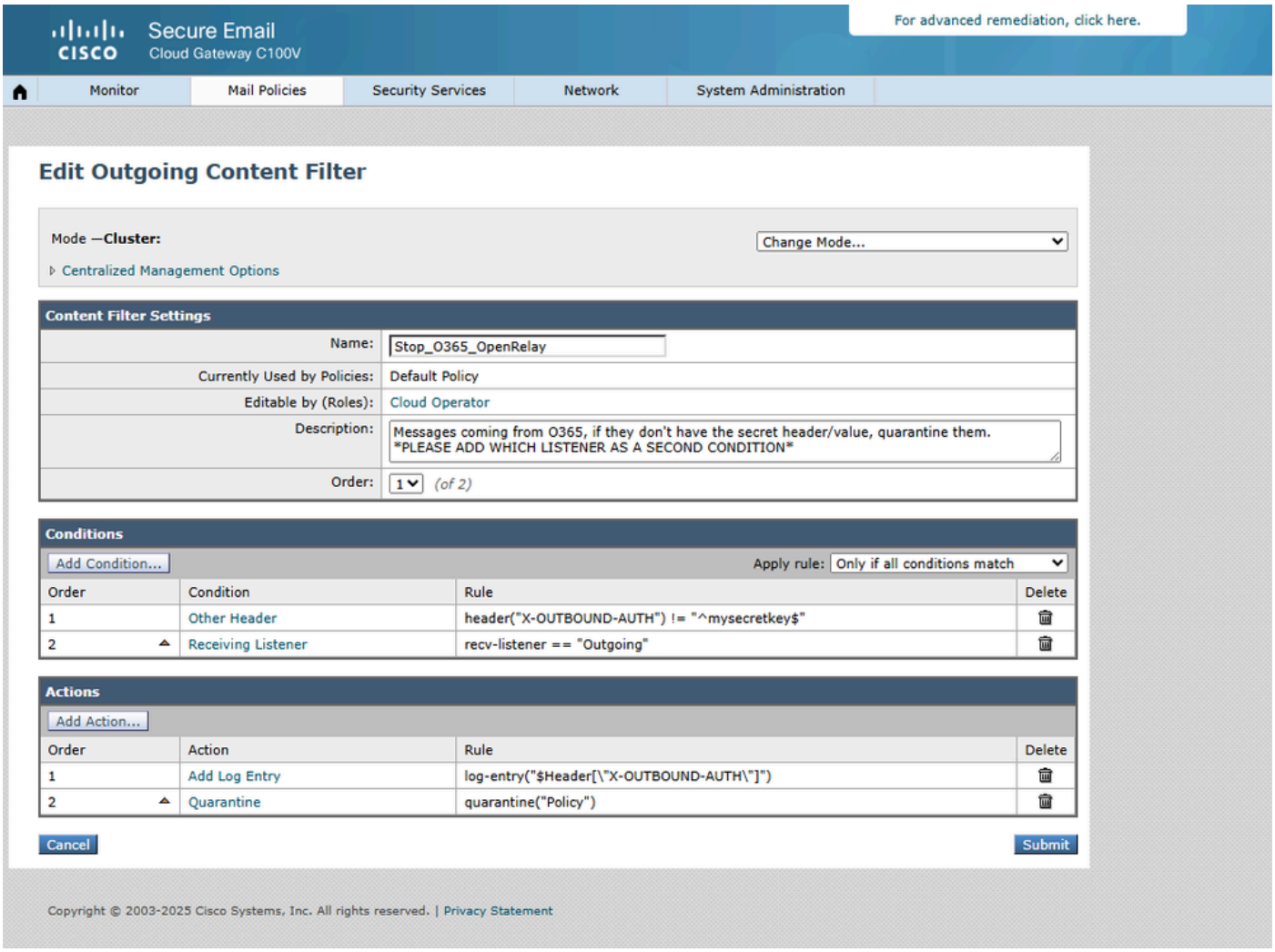
1. From the GUI, navigate to **Mail Policies** >> **Outgoing Content Filters** >> select **Stop_O365_OpenRelay** (select **Add Filter...** if this is not available).
2. Make sure the *first* Content Filter is configured:
    - Name: **<this can be anything>**
    - Description: **<this can be anything>**
    - Apply rule: **Only if all conditions match**
    - **Conditions**
        - Other Header:
            - **Header Name:** <Enter header name previously listed during creation of Mail Flow Rule on Microsoft Office 365) (for example, **X-OUTBOUND-AUTH)**.
                - Some customers may have this configuration predefined using a header value of **X-IronPort-Tenant**. While this can also be used, the crucial part is simply to make sure the header value entered in the Content Filter condition matches the header value that was configured in the **Mail Flow Rule** on Microsoft Office 365.
            - **Header value (Does Not Equal):** <Enter the value of the header previously listed during the creation of the Mail Flow Rule on Microsoft Office 365 (such as, **mysecretkey**).
        - Receiving Listener (Is): **Outgoing**
    - **Actions**
        - Add Log Entry: **$Header["X-OUTBOUND-AUTH"]**
            - Some customers may have this configuration predefined using a header value of **X-IronPort-Tenant**. While this can also be used, the crucial part is to ensure the header value entered in the Content Filter condition matches the header value that was configured in the **Mail Flow Rule** on Microsoft Office 365.
        - Quarantine: <select respective quarantine>
    - Please avoid using any special characters other than those previously listed (such as *, (, |, etc.), as they may cause false positive matches and could result in legitimate emails being quarantined.

- Click **Submit**.

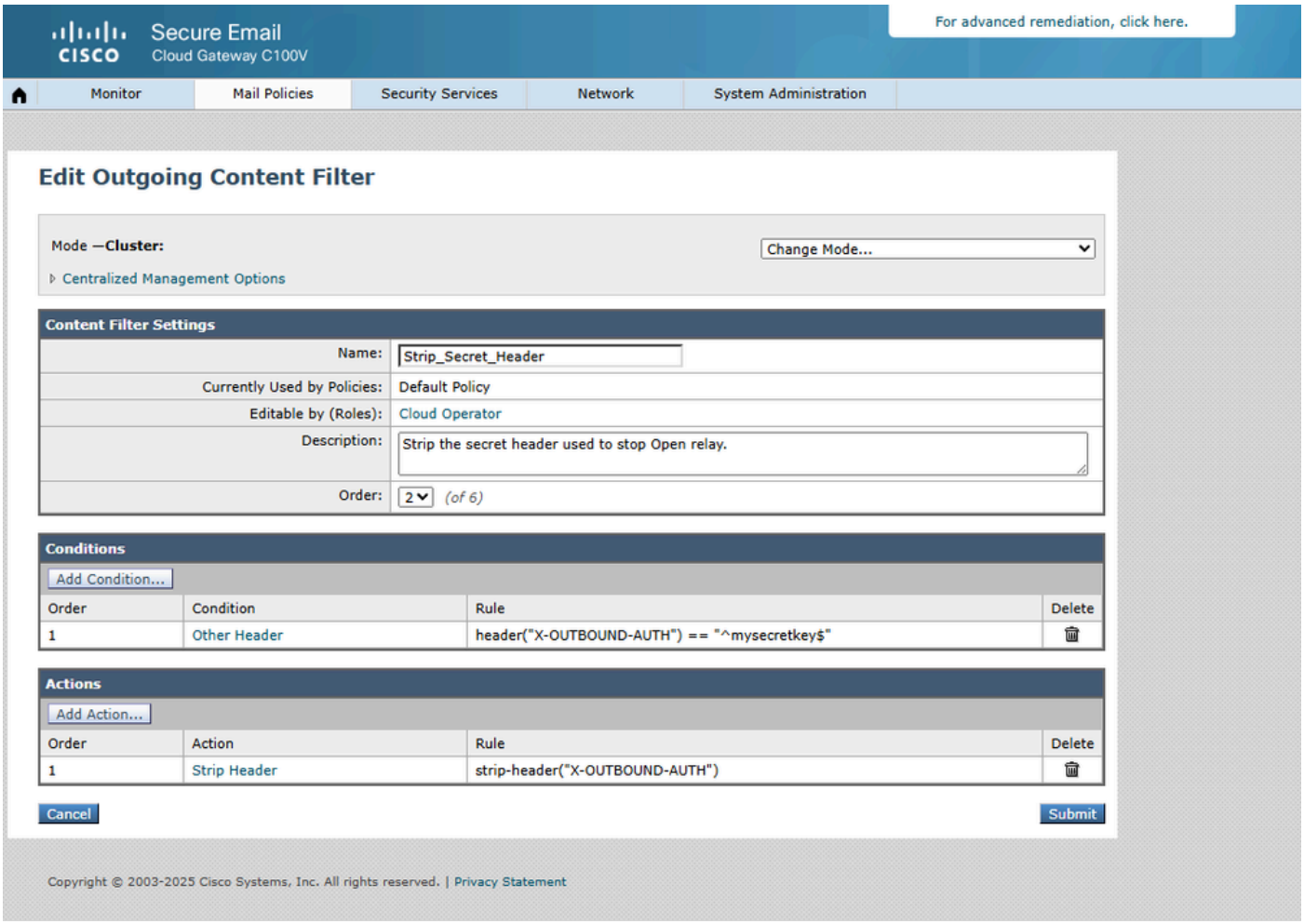
3. Next, select the **Strip_Secret_Header** Content Filter and configure: (select **Add Filter...** if not available):
    - Name: **<this can be anything>**
    - Description: **<this can be anything>**
    - **Conditions**
        - Other Header:
            - **Header Name:** <Enter the header name previously listed during the creation of Mail Flow Rule on Microsoft Office 365) (for example, **X-OUTBOUND-AUTH)**.
                - Some customers may have this configuration predefined using a header value of **X-IronPort-Tenant**. While this can also be used, the crucial part is to ensure the header value entered in the Content Filter condition matches the header value that was configured in the **Mail Flow Rule** on Microsoft Office 365.
            - **Header value (Equals):** <Enter the value of the header previously listed during the creation of the Mail Flow Rule on Microsoft Office 365 (such as, **mysecretkey**).
    - **Actions**
        - Strip Header
            - **Header Name:** <Enter header name previously listed during creation of Mail Flow Rule on Microsoft Office 365) (such as, **X-OUTBOUND-AUTH**).
                - Some customers may have this configuration predefined using a header value of **X-IronPort-Tenant**. While this can also be used, the crucial part is simply to make sure that the header value entered in the Content Filter condition, matches the header value that was configured in the **Mail Flow Rule** on Microsoft Office 365.
                - Click **Submit**, then navigate to **Mail Policies** >> **Outgoing Mail Policies**.
4. Ensure that the newly created Content Filters are now enabled under the **Default Policy**, and any other required policies.
    - Make sure that the **Strip_Secret_Header** Content Filter is in the proper order on the Mail Policy(s). It must be placed *after* the **Stop_O365_OpenRelay** Content Filter, or you may impact the mail flow and/or the Content Filters may not work as intended.
5. **Submit** >> **Commit** your changes.
6. Proceed with testing your Outgoing email traffic.



Tip: After your tests have completed successfully and mail delivery is working as expected, it is recommended to change the action in the Content Filter from "quarantine" to "drop."



Stop_O365_OpenRelay Content Filter



Strip_Secret_Header Content Filter

Option 2: Prevent Open Relay via CLI

Access the CLI for your Cisco Secure Email Gateway.

Note: Cisco Secure Email Cloud Gateway > Command Line Interface (CLI) Access.

Create a message filter to inspect the presence and value of the x-header and remove the header if it exists. If no header exists, drop the message.

1. Log in to your Gateway via the CLI.
2. Run the **filters** command.
3. If your Gateway is clustered, hit **return** to edit the filters in Cluster mode.
4. Use the **New** command to create a Message Filter, copy, and paste:

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

```
drop();
}
}
```

5. Hit **return** one time to create a new, blank line.
6. Enter **[.]** on the new line to end your new message filter.
7. Click **return** one time to exit the Filters menu.
8. Run the **commit** command to save the changes to your configuration.

Note: Avoid special characters for the secret key. The ^ and $ shown in the message filter are regex characters and are used as provided in the example.

Note: Please review the name of how your RELAYLIST is configured. It can be configured with an alternative name, or you can have a specific name based on your relay policy or mail provider.

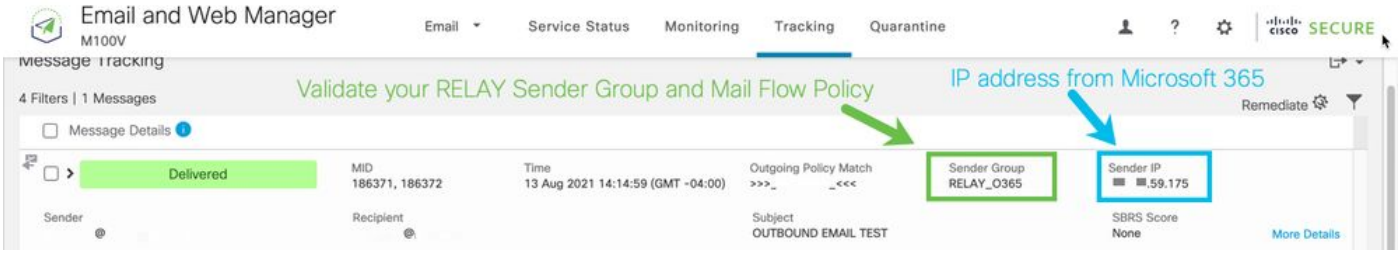
Test Outbound Email

Test outbound mail from your Microsoft 365 email address to an external domain recipient. You can review Message Tracking from your Cisco Secure Email and Web Manager to ensure it is appropriately routed outbound.

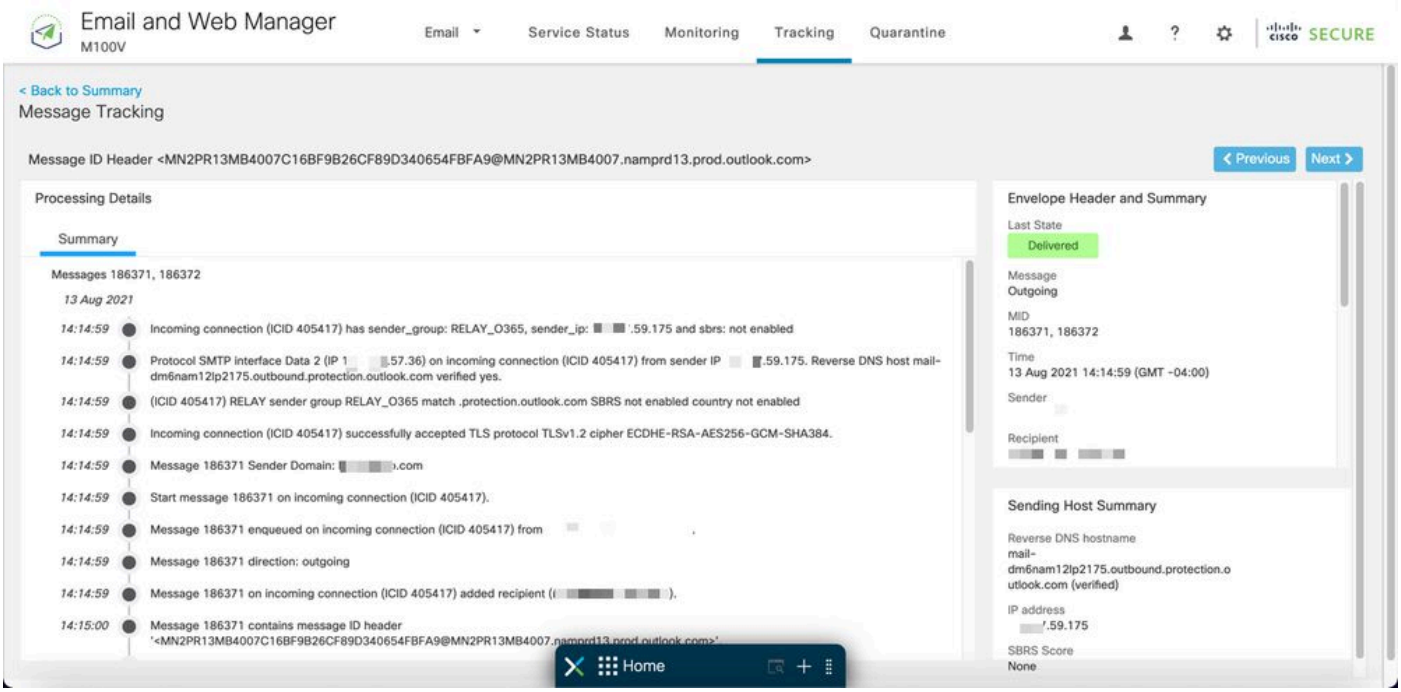
Note: Review your TLS configuration (**System Administration** > **SSL Configuration**) on the Gateway and the ciphers used for Outbound SMTP. Cisco Best Practices recommends:

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

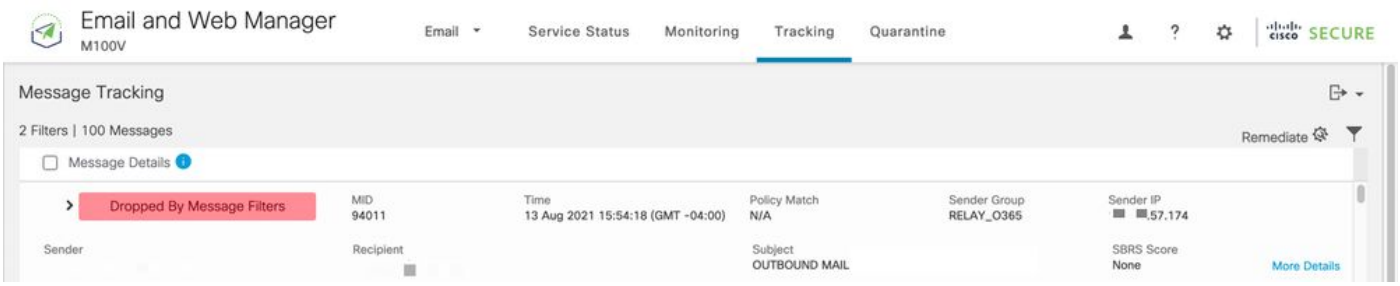
An example of Tracking with successful delivery:

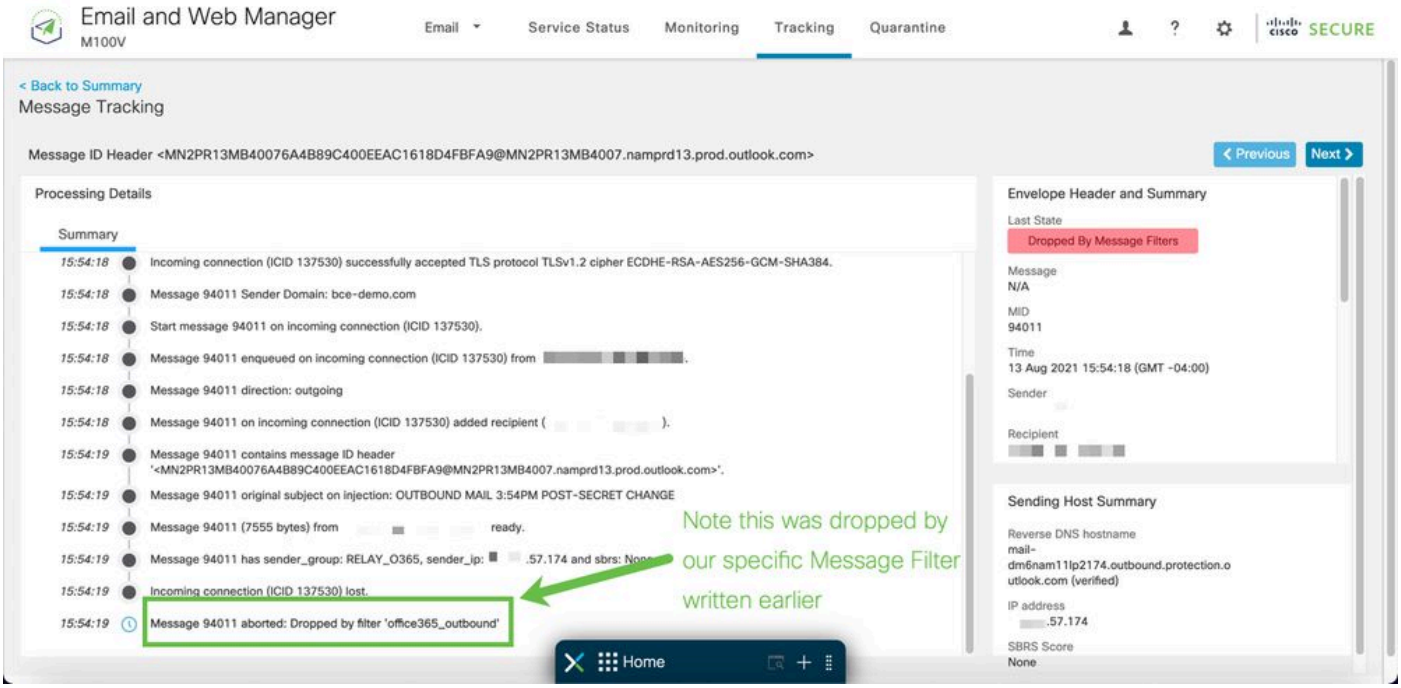


Click**More Details**to see the complete message details:



An example of Message Tracking where the x-header do not match:





Related Information

Cisco Secure Email Gateway Documentation

- Release Notes
- User Guide
- CLI Reference Guide
- API Programming Guides for Cisco Secure Email Gateway
- Open Source Used in Cisco Secure Email Gateway
- Cisco Content Security Virtual Appliance Installation Guide (includes vESA)

Secure Email Cloud Gateway Documentation

- Release Notes
- User Guide

Cisco Secure Email and Web Manager Documentation

- Release Notes and Compatibility Matrix
- User Guide
- API Programming Guides for Cisco Secure Email and Web Manager
- Cisco Content Security Virtual Appliance Installation Guide (includes vSMA)

Cisco Secure Product Documentation

- Cisco Secure Portfolio Naming Architecture