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 Cisco Secure Email Gateway
  - Enable TLS
  - Configure Mail from Microsoft 365 to CES
  - Create a Mail Flow Rule
  - 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

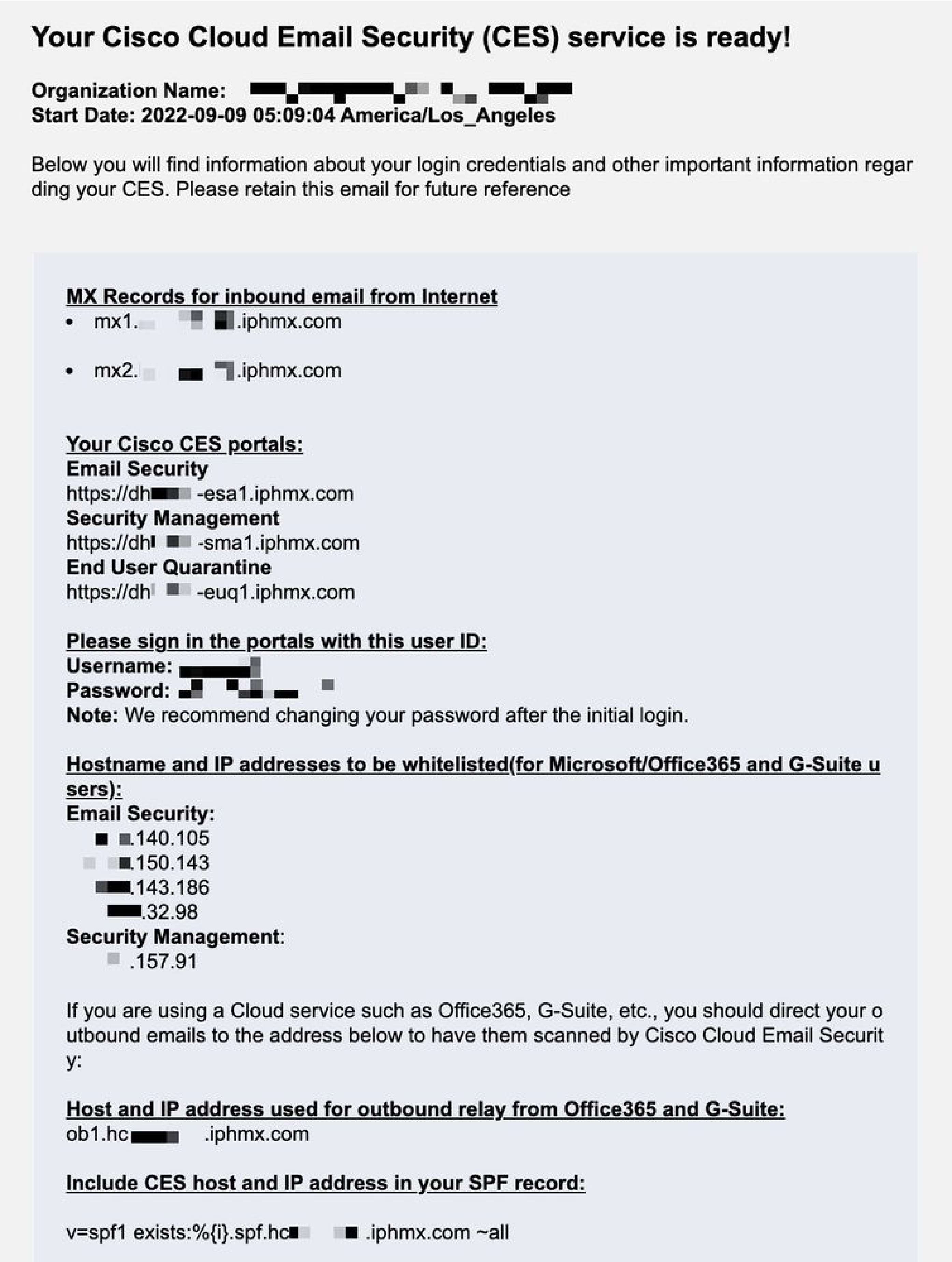
This document is not restricted to specific software and hardware versions.

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 regarding 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 users):
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 outbound emails to the address below to have them scanned by Cisco Cloud Email Security:

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.150.1143` 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 get the Data 2 interface added to your allocation.

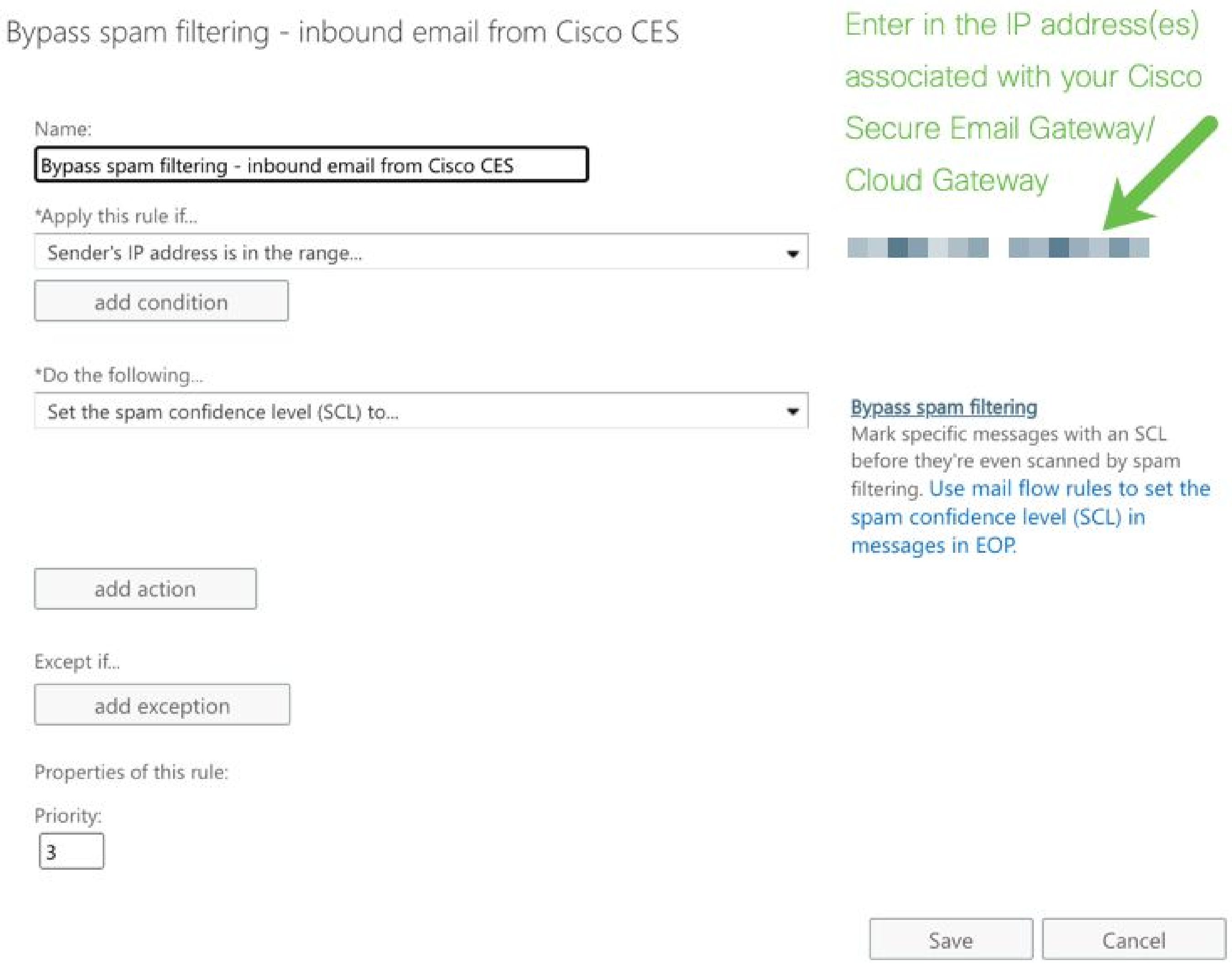
Configure Microsoft 365 with Secure Email

Configure Incoming Email in Microsoft 365 from Cisco Secure Email

Bypass Spam Filtering Rule

1. Log in to the Microsoft 365 Admin Center (https://portal.microsoft.com).
2. In the left-hand menu, expand **Admin Centers**.
3. Click **Exchange**.
4. From the left-hand menu, navigate to **Mail flow** > **Rules**.
5. Click **[+]** to create a new rule.
6. Choose **Bypass spam filtering...** from the drop-down list.
7. Enter a name for your new rule: **Bypass spam filtering - inbound email from Cisco CES**.
8. 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**.
9. For *Do the following..., the new rule has been pre-selected: **Set the spam confidence level (SCL) to... - Bypass spam filtering**.
10. Click **Save**.

An example of how your rule looks:



Bypass spam filtering - inbound email from Cisco CES

Name: Bypass spam filtering - inbound email from Cisco CES

*Apply this rule if... Sender's IP address is in the range...

*Do the following... Set the spam confidence level (SCL) to...

Properties of this rule:

Priority: 3

Enter in the IP address(es) associated with your Cisco Secure Email Gateway/ Cloud Gateway

[redacted] [redacted]

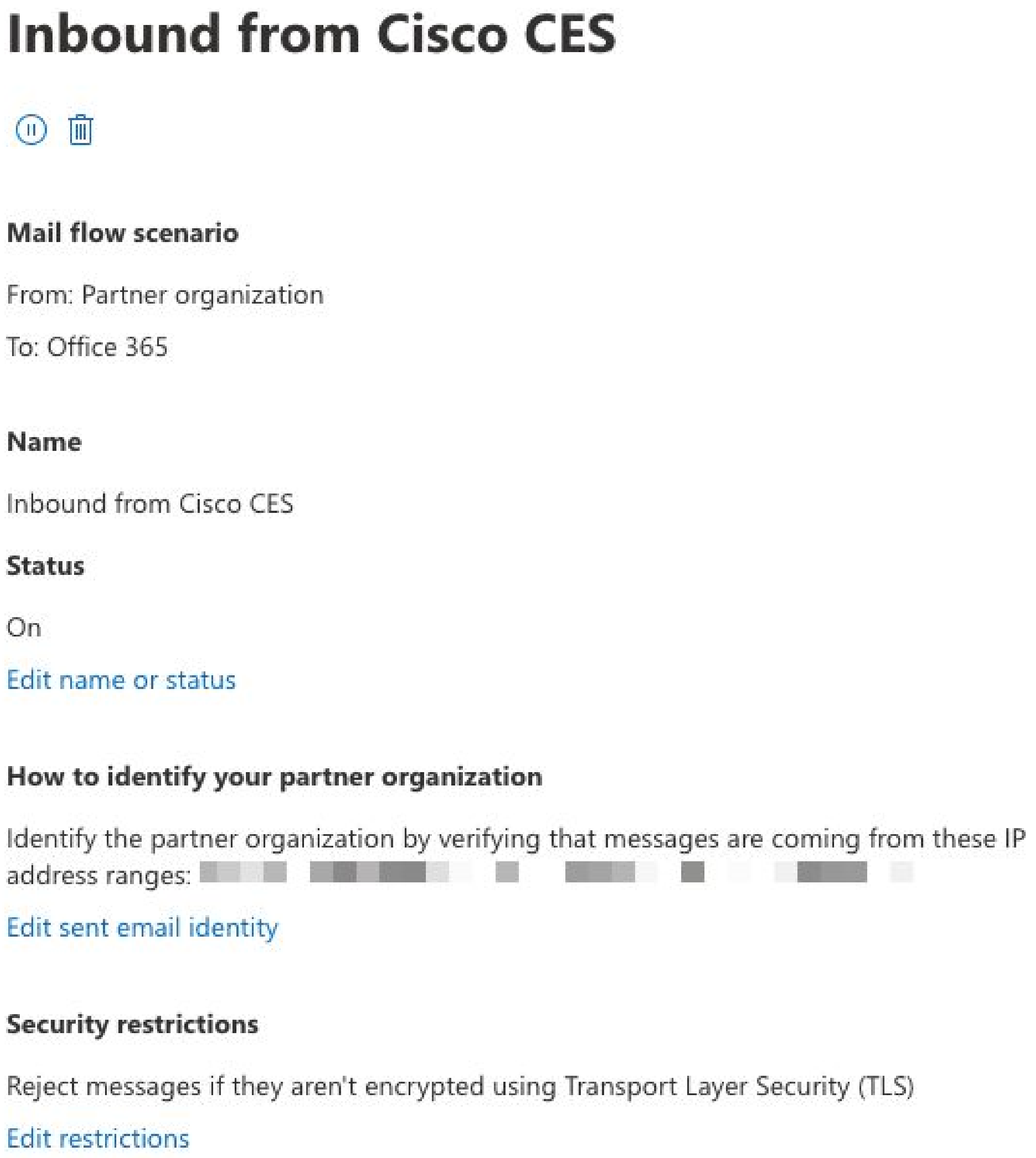
Bypass spam filtering

Mark specific messages with an SCL before they're even scanned by spam filtering. Use mail flow rules to set the spam confidence level (SCL) in messages in EOP.

Receiving Connector

1. Remain in the Exchange Admin Center.
2. From the left-hand menu, navigate to **Mail flow** > **Connectors**.
3. Click **[+]** 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, if you wish.
8. Click **Next**.
9. Click **Use the sender's IP address**.
10. Click **Next**.
11. Click **[+]** and enter the IP addresses that are indicated in your Cisco Secure Email welcome letter.
12. Click **Next**.
13. Choose **Reject email messages if they aren't sent over Transport Layer Security (TLS)**.
14. Click **Next**.
15. Click **Save**.

An example of how your connector configuration looks:



Inbound from Cisco CES

Mail flow scenario

From: Partner organization

To: Office 365

Name

Inbound from Cisco CES

Status

On

Edit name or status

How to identify your partner organization

Identify the partner organization by verifying that messages are coming from these IP address ranges: [redacted]

Edit sent email identity

Security restrictions

Reject messages if they aren't encrypted using Transport Layer Security (TLS)

Edit restrictions

Configure Mail from Cisco Secure Email to Microsoft 365

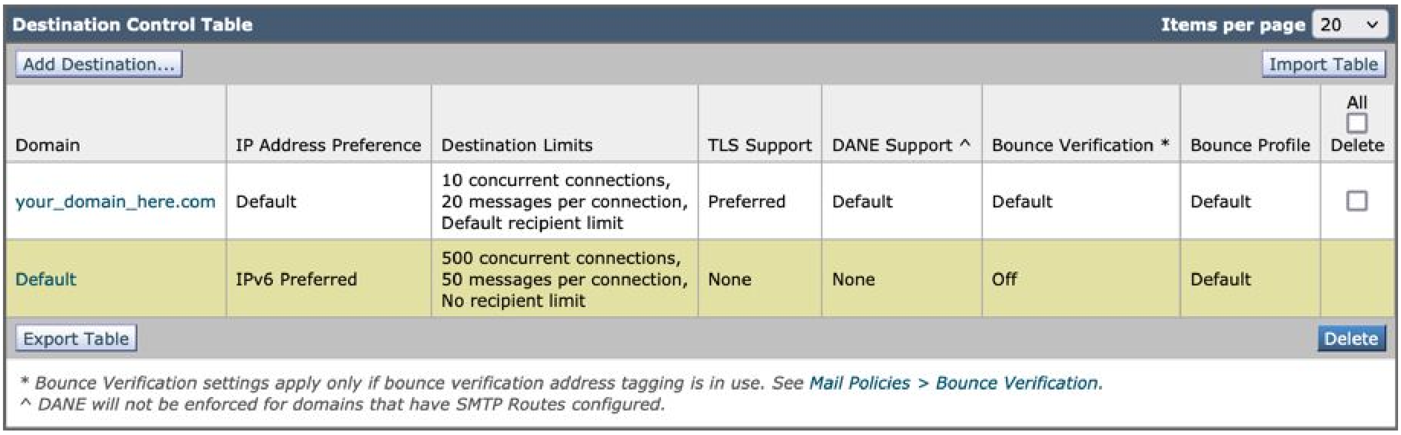
Destination Controls

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

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	

** 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

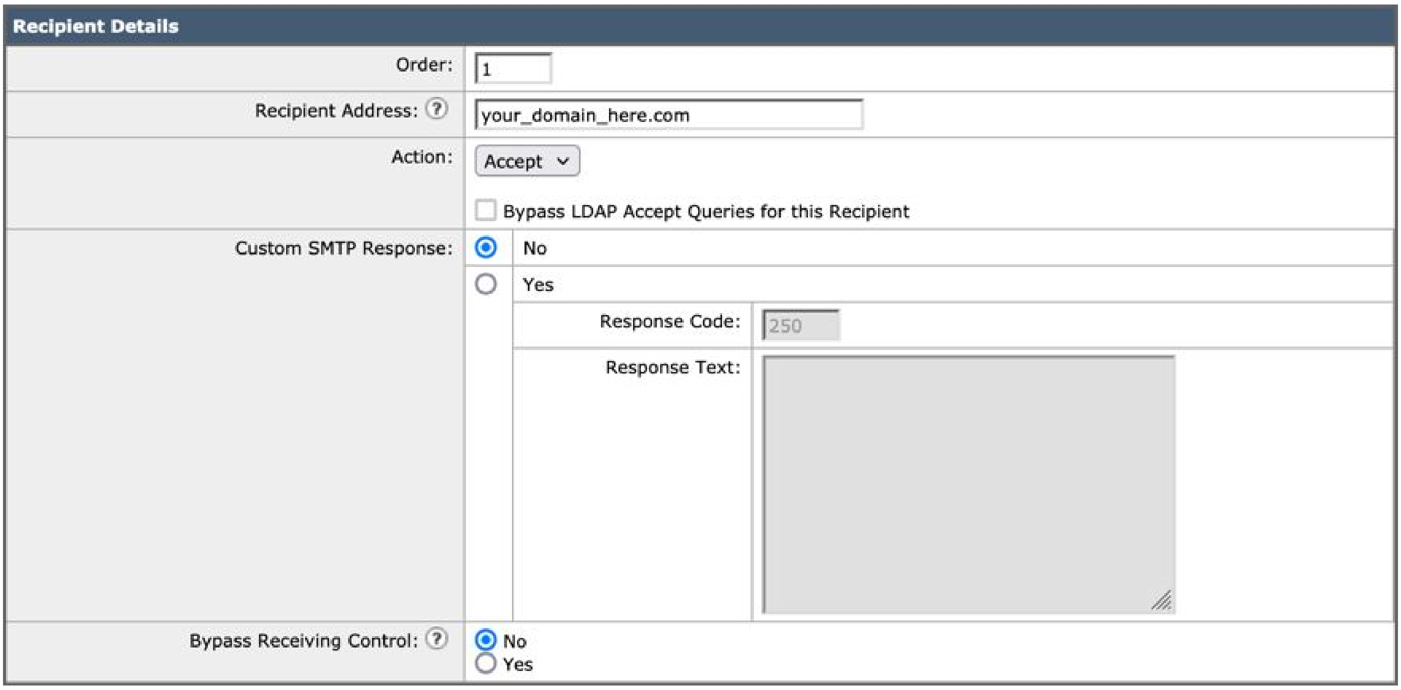
Next, set the Recipient Access Table (RAT) to accept mail for your domains:

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.

2. Click **Add Recipient**.
3. Add your domains in the Recipient Address field.
4. Choose the default action of **Accept**.
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 RAT entry looks:



Recipient Details

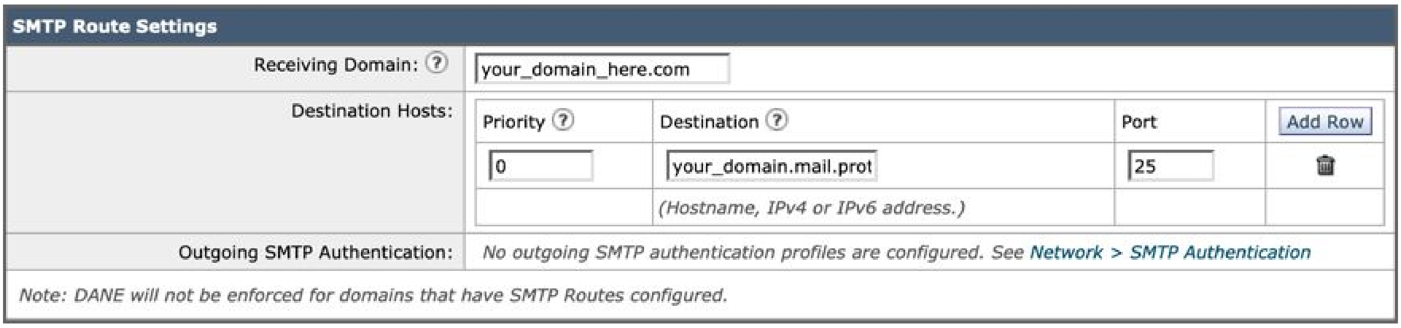
Order:	1
Recipient Address: ?	your_domain_here.com
Action:	Accept □ Bypass LDAP Accept Queries for this Recipient
Custom SMTP Response:	● No ○ Yes Response Code: 250 Response Text:
Bypass Receiving Control: ?	● No ○ Yes

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:



SMTP Route Settings

Receiving Domain: ?	your_domain_here.com
Destination Hosts:	Priority ? 0 / Destination ? your_domain.mail.prot / Port 25 (Hostname, IPv4 or IPv6 address.)
Outgoing SMTP Authentication:	*No outgoing SMTP authentication profiles are configured. See Network > SMTP Authentication*

Note: DANE will not be enforced for domains that have SMTP Routes configured.

DNS (MX Record) Configuration

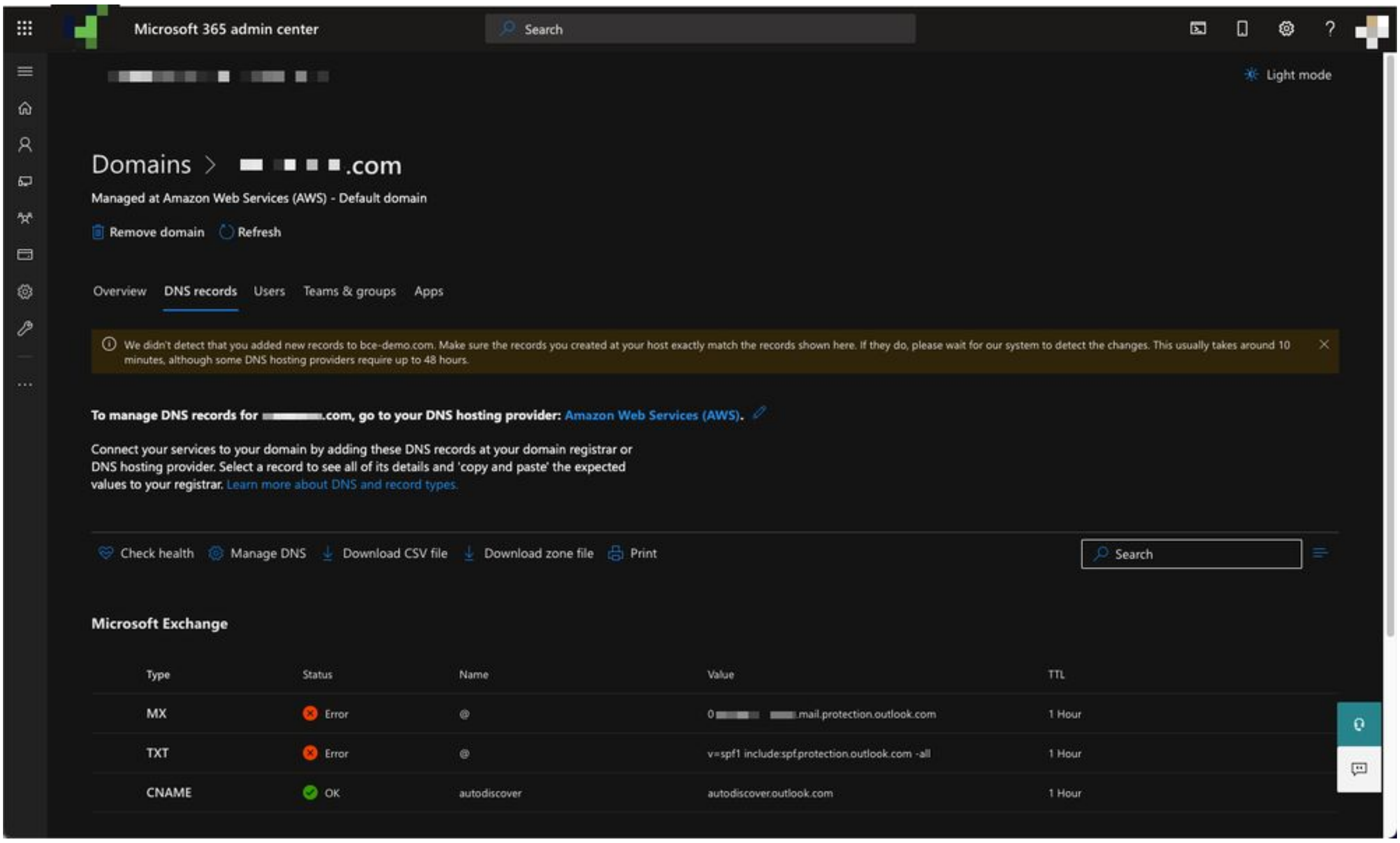
You are ready to cut over the domain through a Mail Exchange (MX) record change. Work with your DNS administrator to resolve your MX records to the IP addresses for your Cisco Secure Email Cloud instance, as provided in your Cisco Secure Email welcome letter.

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

1. Log in to the Microsoft 365 Admin console (https://admin.microsoft.com).

2. Navigate to **Home** > **Settings** > **Domains**.
3. Choose your default domain name.
4. ClickCheck Health.

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



Domains > [redacted].com

Managed at Amazon Web Services (AWS) - Default domain

We didn't detect that you added new records to bce-demo.com. Make sure the records you created at your host exactly match the records shown here. If they do, please wait for our system to detect the changes. This usually takes around 10 minutes, although some DNS hosting providers require up to 48 hours.

To manage DNS records for [redacted].com, go to your DNS hosting provider: Amazon Web Services (AWS).

Connect your services to your domain by adding these DNS records at your domain registrar or DNS hosting provider. Select a record to see all of its details and 'copy and paste' the expected values to your registrar. Learn more about DNS and record types.

Microsoft Exchange

Type	Status	Name	Value	TTL
MX	Error	@	0 [redacted] [redacted].mail.protection.outlook.com	1 Hour
TXT	Error	@	v=spf1 include:spf.protection.outlook.com -all	1 Hour
CNAME	OK	autodiscover	autodiscover.outlook.com	1 Hour

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.

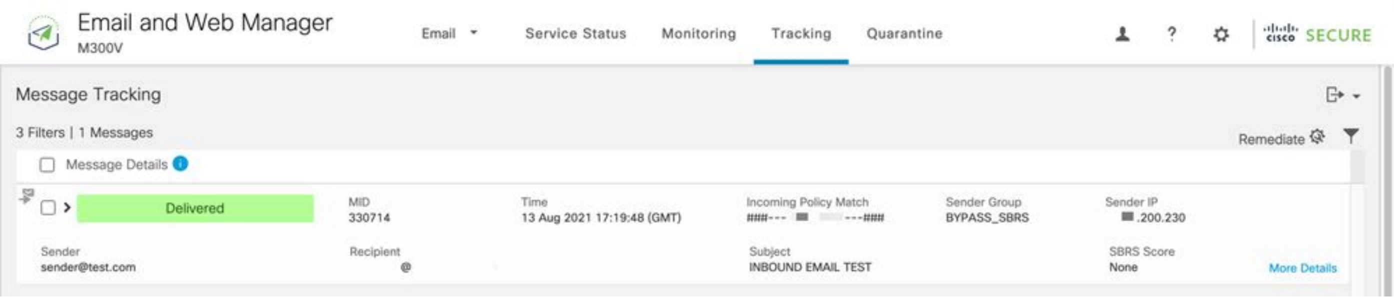
Test Inbound Email

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 (https://sma.iphmx.com/ng-login).
2. Click **Tracking**.
3. Enter the needed search criteria and click **Search**; and expect to see such results:



3 Filters | 1 Messages

Delivered

MID 330714

Time 13 Aug 2021 17:19:48 (GMT)

Incoming Policy Match ###--- [redacted] ---###

Sender Group BYPASS_SBRS

Sender IP [redacted].200.230

Sender sender@test.com

Recipient [redacted]@[redacted]

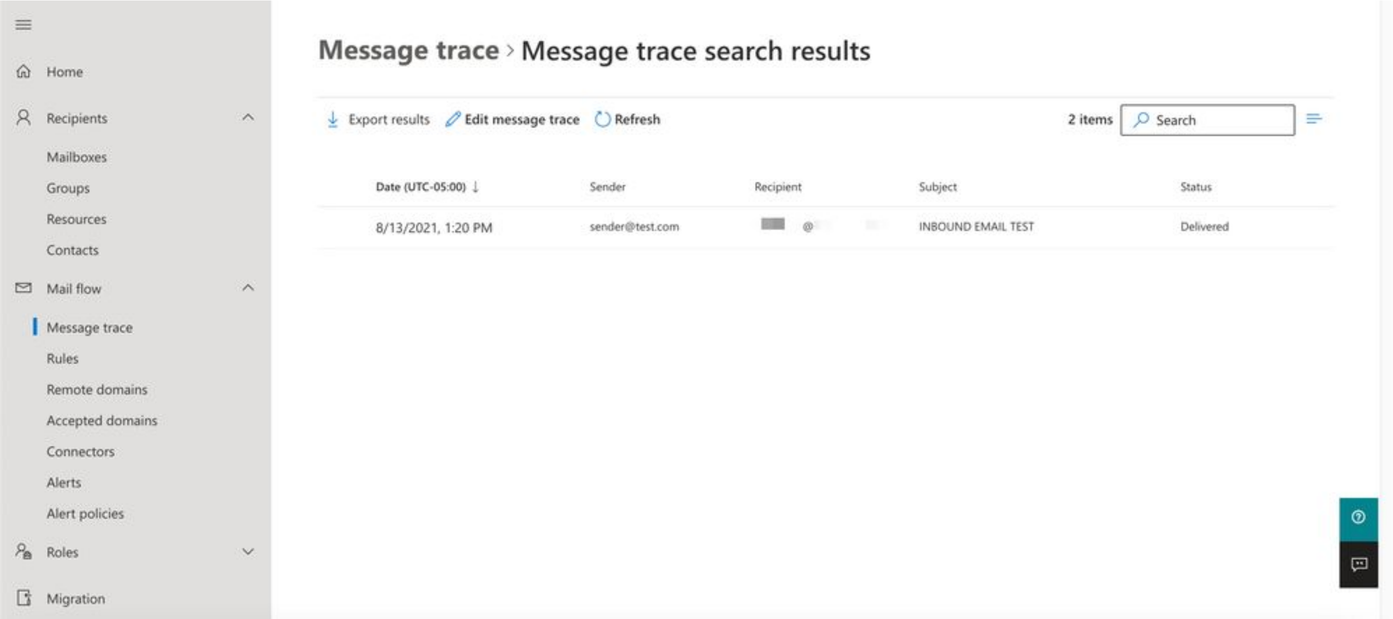
Subject INBOUND EMAIL TEST

SBRS Score None

More Details

To see mail logs in Microsoft 365:

1. Log in to the Microsoft 365 Admin Center (https://admin.microsoft.com).
2. Expand **Admin Centers**.
3. Click **Exchange**.
4. Navigate to **Mail flow** > **Message trace**.
5. 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.
6. Enter the needed search criteria for recipients and click **Search** and expect to see results similar to:



Message trace > Message trace search results

2 items

Date (UTC-05:00) ↓	Sender	Recipient	Subject	Status
8/13/2021, 1:20 PM	sender@test.com	[redacted] @[redacted]	INBOUND EMAIL TEST	Delivered

Configure Outgoing Email from Microsoft 365 to Cisco Secure Email

Configure RELAYLIST on 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 for Outgoing Listener, OutgoingMail, or MailFlow-Ext, based on the actual name of your Listener for your external/outbound mail flow.

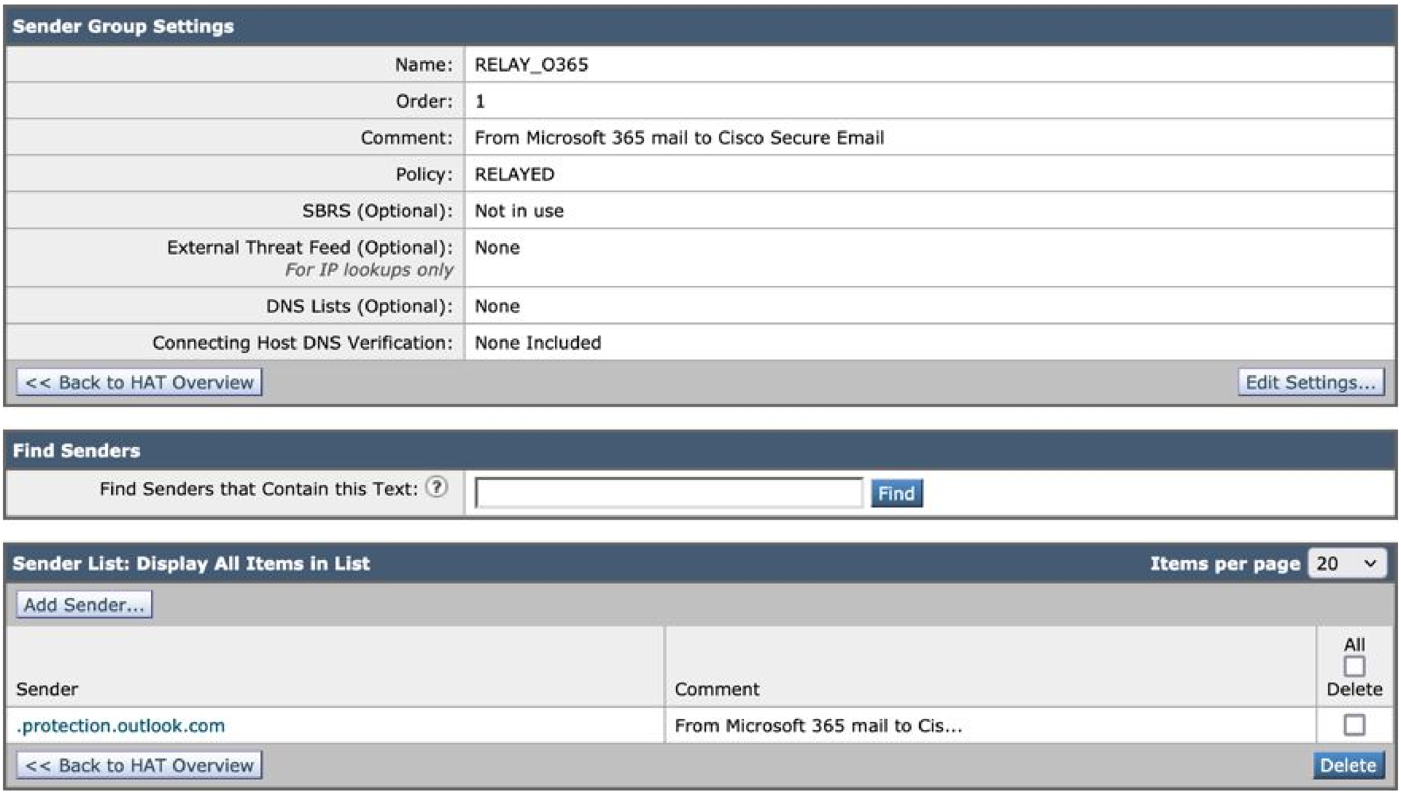
3. Click **Add Sender Group...**
4. Configure the Sender Group as:

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:



Sender Group Settings

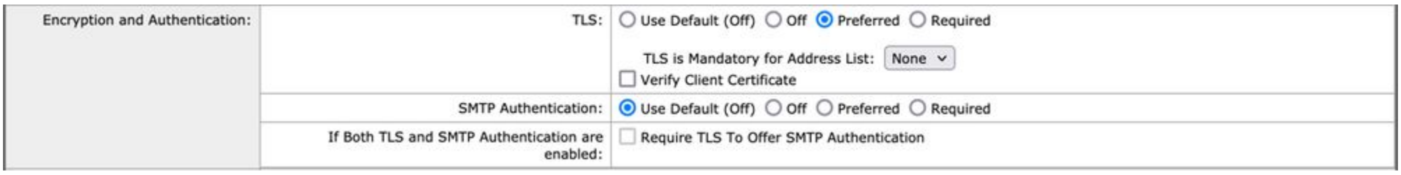
Name:	RELAY_O365
Order:	1
Comment:	From Microsoft 365 mail to Cisco Secure Email
Policy:	RELAYED
SBRS (Optional):	Not in use
External Threat Feed (Optional): *For IP lookups only*	None
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

Sender	Comment	All □ Delete
.protection.outlook.com	From Microsoft 365 mail to Cis...	□

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:



Encryption and Authentication:

TLS: ○ Use Default (Off) ○ Off ● Preferred ○ Required

TLS is Mandatory for Address List: None

□ Verify Client Certificate

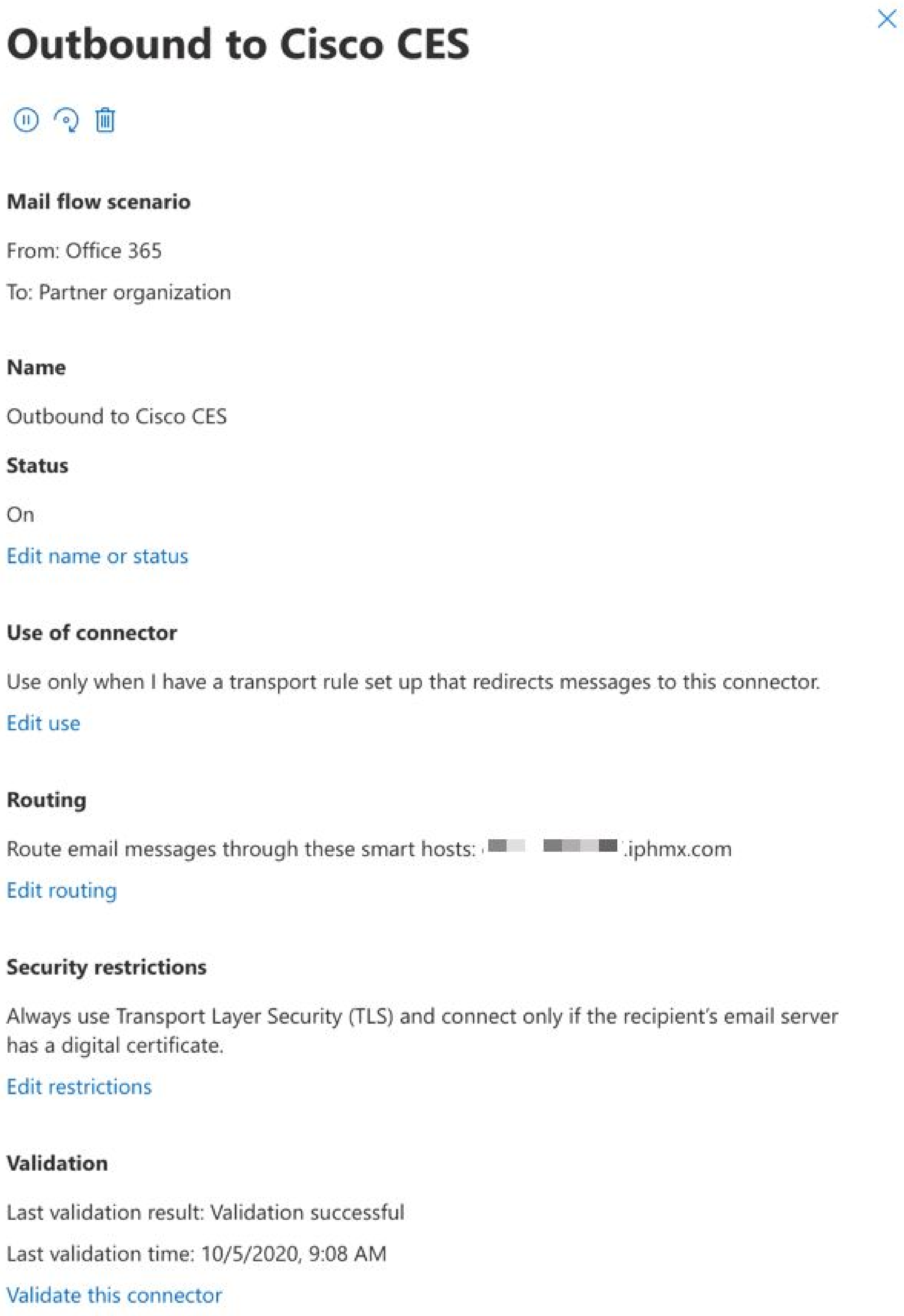
SMTP Authentication: ● Use Default (Off) ○ Off ○ Preferred ○ Required

If Both TLS and SMTP Authentication are enabled: □ Require TLS To Offer SMTP Authentication

Configure Mail from Microsoft 365 to CES

1. Log in to the Microsoft 365 Admin Center (https://admin.microsoft.com).
2. Expand **Admin Centers**.
3. Click **Exchange**.
4. Navigate to **Mail flow** > **Connectors**.
5. Click [+] to create a new connector.
6. In the Select your mail flow scenario pop-up window, choose:
    1. From: Office365
    2. To:Partner organization
7. Click **Next**.
8. Enter a name for your new connector: **Outbound to Cisco CES**.
9. Enter a description, if you wish.
10. Click **Next**.
11. 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**.
12. Click **Route email through these smart hosts**.
13. Click **[+]** and enter the outbound IP addresses or hostnames provided in your CES welcome letter.
14. Click **Save**.
15. Click **Next**.
16. For How should 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**.
17. You are presented with the confirmation screen.
18. Click **Next**.
19. Use **[+]** to enter a valid email address and click **OK**.
20. Click **Validate** and allow the validation to run.
21. Once complete, click **Close**.
22. ClickSave.

An example of how your Outbound Connector looks:



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

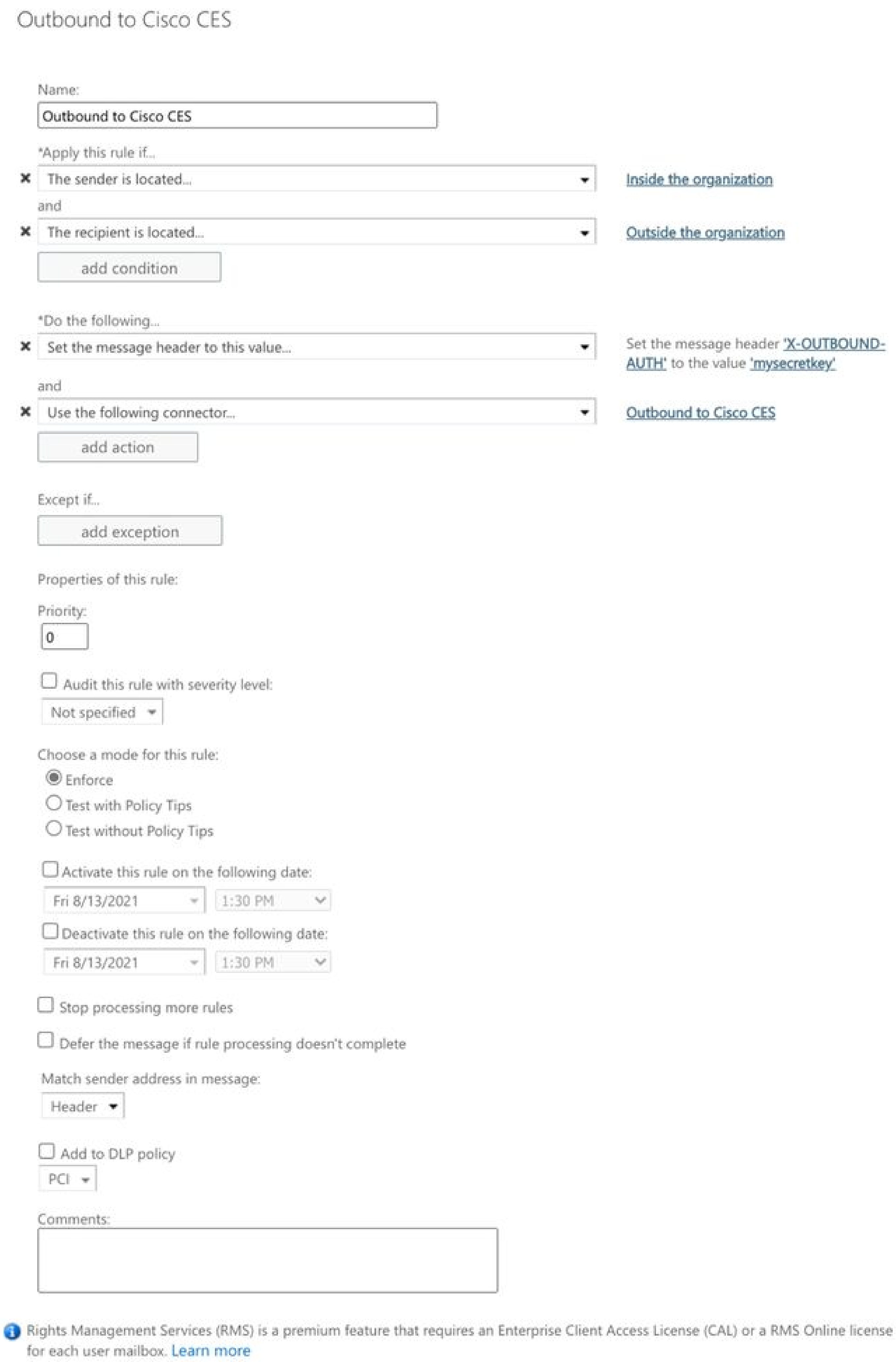
Last validation time: 10/5/2020, 9:08 AM

Validate this connector

Create a Mail Flow Rule

✎ : 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:

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();
}
}
```

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 use 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.

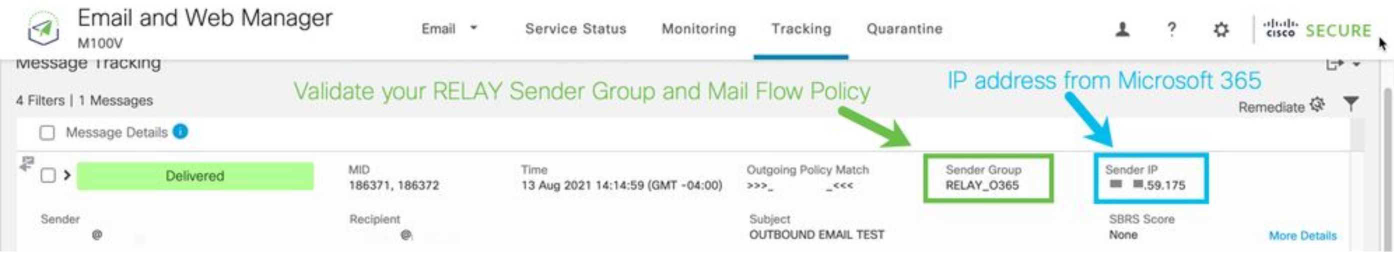
Test Outbound Email

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:



Message Tracking

4 Filters | 1 Messages

Validate your RELAY Sender Group and Mail Flow Policy

IP address from Microsoft 365

□ Message Details

□ > Delivered

MID
186371, 186372

Time
13 Aug 2021 14:14:59 (GMT -04:00)

Outgoing Policy Match
>>>_ _<<<

Sender Group
RELAY_O365

Sender IP
[redacted].59.175

Sender
[redacted]@[redacted]

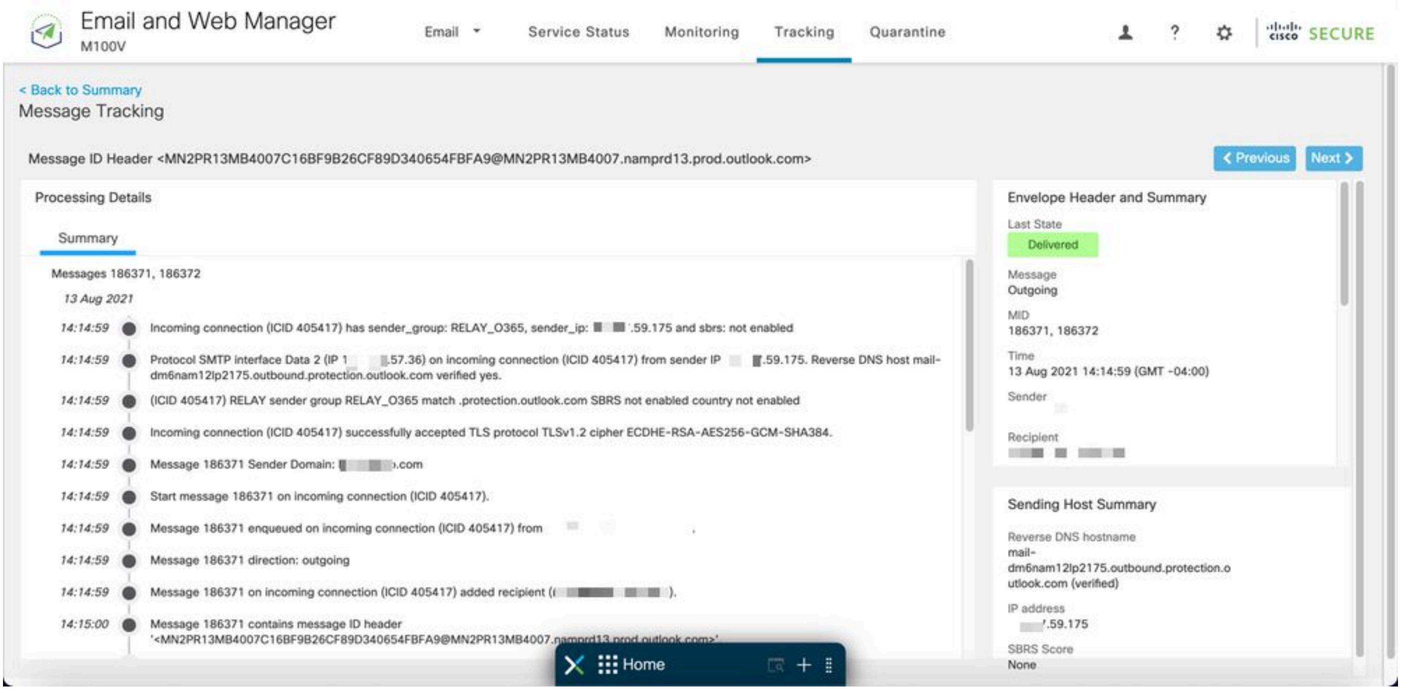
Recipient
[redacted]@[redacted]

Subject
OUTBOUND EMAIL TEST

SBRS Score
None

More Details

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



< Back to Summary

Message Tracking

Message ID Header <MN2PR13MB4007C16BF9B26CF89D340654FBFA9@MN2PR13MB4007.namprd13.prod.outlook.com>

Processing Details

Summary

```
Messages 186371, 186372
  13 Aug 2021
14:14:59  Incoming connection (ICID 405417) has sender_group: RELAY_O365, sender_ip: [redacted].59.175 and sbrs: not enabled
14:14:59  Protocol SMTP interface Data 2 (IP 1[redacted].57.36) on incoming connection (ICID 405417) from sender IP [redacted].59.175. Reverse DNS host mail-
          dm6nam12lp2175.outbound.protection.outlook.com verified yes.
14:14:59  (ICID 405417) RELAY sender group RELAY_O365 match .protection.outlook.com SBRS not enabled country not enabled
14:14:59  Incoming connection (ICID 405417) successfully accepted TLS protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384.
14:14:59  Message 186371 Sender Domain: [redacted].com
14:14:59  Start message 186371 on incoming connection (ICID 405417).
14:14:59  Message 186371 enqueued on incoming connection (ICID 405417) from [redacted].
14:14:59  Message 186371 direction: outgoing
14:14:59  Message 186371 on incoming connection (ICID 405417) added recipient ([redacted]).
14:15:00  Message 186371 contains message ID header
          '<MN2PR13MB4007C16BF9B26CF89D340654FBFA9@MN2PR13MB4007.namprd13.prod.outlook.com>'
```

Envelope Header and Summary

Last State
Delivered

Message
Outgoing

MID
186371, 186372

Time
13 Aug 2021 14:14:59 (GMT -04:00)

Sender
[redacted]

Recipient
[redacted]

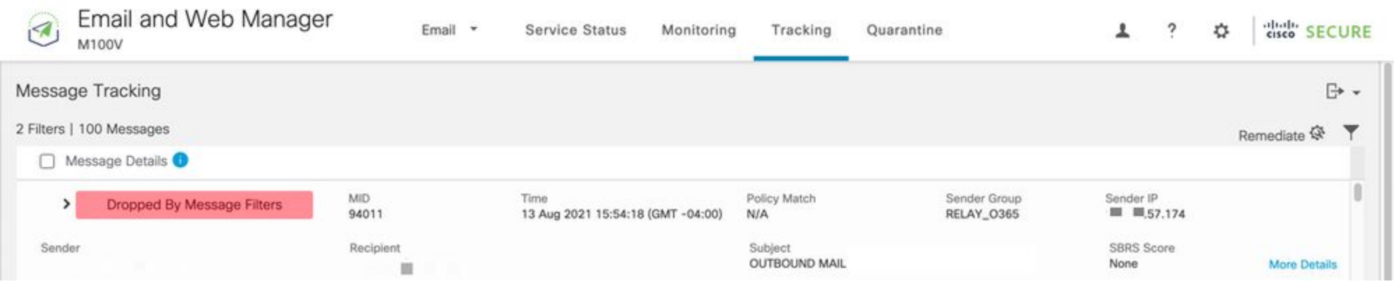
Sending Host Summary

Reverse DNS hostname
mail-dm6nam12lp2175.outbound.protection.outlook.com (verified)

IP address
[redacted].59.175

SBRS Score
None

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



Message Tracking

2 Filters | 100 Messages

□ Message Details

> Dropped By Message Filters

MID
94011

Time
13 Aug 2021 15:54:18 (GMT -04:00)

Policy Match
N/A

Sender Group
RELAY_O365

Sender IP
[redacted].57.174

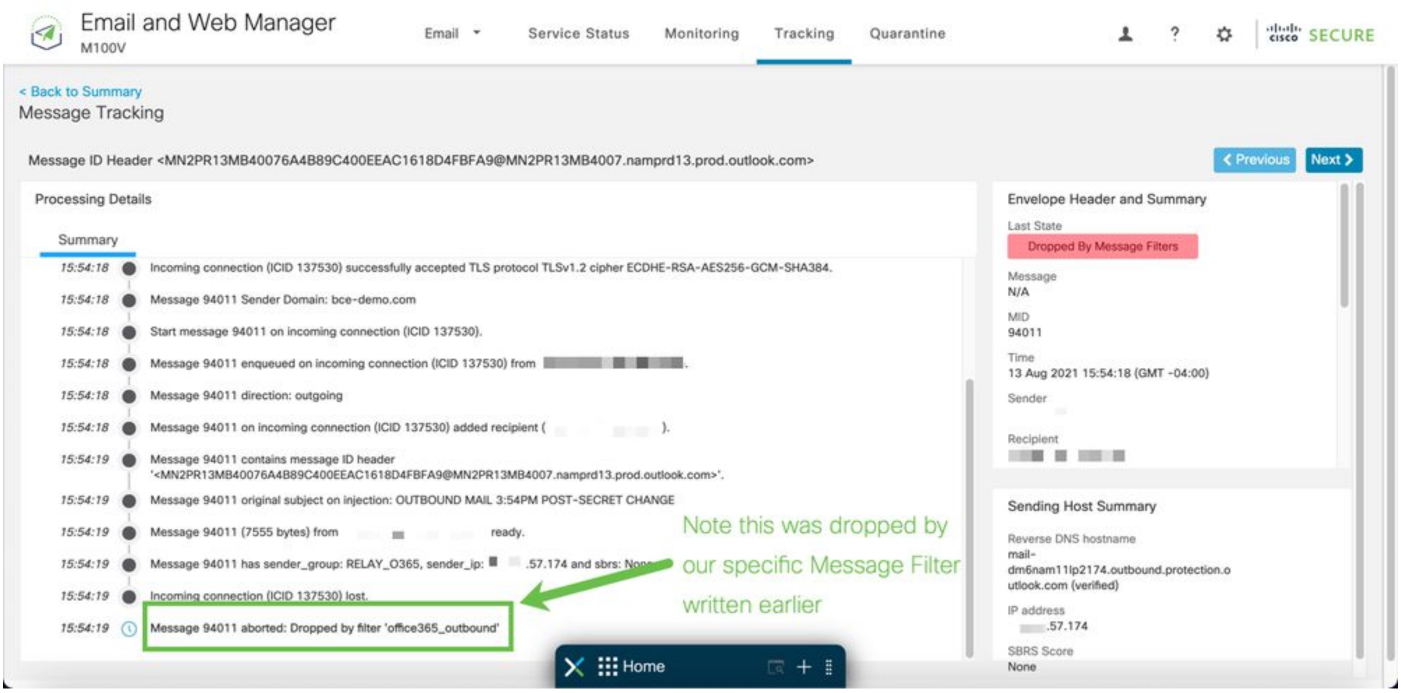
Sender
[redacted]

Recipient
[redacted]

Subject
OUTBOUND MAIL

SBRS Score
None

More Details



Message Tracking

Message ID Header <MN2PR13MB40076A4B89C400EEAC1618D4FBFA9@MN2PR13MB4007.namprd13.prod.outlook.com>

Processing Details

Summary

```
15:54:18  Incoming connection (ICID 137530) successfully accepted TLS protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384.
15:54:18  Message 94011 Sender Domain: bce-demo.com
15:54:18  Start message 94011 on incoming connection (ICID 137530).
15:54:18  Message 94011 enqueued on incoming connection (ICID 137530) from [redacted].
15:54:18  Message 94011 direction: outgoing
15:54:18  Message 94011 on incoming connection (ICID 137530) added recipient ([redacted]).
15:54:19  Message 94011 contains message ID header
          '<MN2PR13MB40076A4B89C400EEAC1618D4FBFA9@MN2PR13MB4007.namprd13.prod.outlook.com>'.
15:54:19  Message 94011 original subject on injection: OUTBOUND MAIL 3:54PM POST-SECRET CHANGE
15:54:19  Message 94011 (7555 bytes) from [redacted] ready.
15:54:19  Message 94011 has sender_group: RELAY_O365, sender_ip: [redacted].57.174 and sbrs: None
15:54:19  Incoming connection (ICID 137530) lost.
15:54:19  Message 94011 aborted: Dropped by filter 'office365_outbound'
```

Note this was dropped by our specific Message Filter written earlier

Envelope Header and Summary

Last State
Dropped By Message Filters

Message
N/A

MID
94011

Time
13 Aug 2021 15:54:18 (GMT -04:00)

Sender
[redacted]

Recipient
[redacted]

Sending Host Summary

Reverse DNS hostname
mail-dm6nam11lp2174.outbound.protection.outlook.com (verified)

IP address
[redacted].57.174

SBRS Score
None

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