

# Konfigurieren von Microsoft 365 mit sicherer E-Mail

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren von Microsoft 365 mit sicherer E-Mail](#)

[Konfigurieren von eingehenden E-Mails in Microsoft 365 über Cisco Secure Email](#)

[Umgehen der Spam-Filterregel](#)

[Empfangs-Connector](#)

[Konfigurieren von E-Mails aus Cisco Secure Email für Microsoft 365](#)

[Zielsteuerelemente](#)

[Recipient Access Table](#)

[SMTP-Routen](#)

[DNS-Konfiguration \(MX-Eintrag\)](#)

[Eingehende E-Mails testen](#)

[Konfigurieren von ausgehenden E-Mails aus Microsoft 365 für Cisco Secure Email](#)

[Konfigurieren von RELAYLIST auf Cisco Secure Email Gateway](#)

[Aktivieren von TLS](#)

[Konfigurieren von E-Mails von Microsoft 365 nach CES](#)

[Erstellen einer Mailflow-Regel](#)

[Ausgehende E-Mails testen](#)

[Zugehörige Informationen](#)

[Cisco Secure Email Gateway-Dokumentation](#)

[Secure Email Cloud Gateway - Dokumentation](#)

[Cisco Secure Email und Web Manager-Dokumentation](#)

[Cisco Secure-Produktdokumentation](#)

---

## Einleitung

In diesem Dokument werden die Konfigurationsschritte zur Integration von Microsoft 365 in Cisco Secure Email für die ein- und ausgehende E-Mail-Zustellung beschrieben.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Email Gateway oder Cloud Gateway
- Zugriff über eine Kommandozeile auf Ihre Cisco Secure Email Cloud Gateway-Umgebung: [Cisco Secure Email Cloud Gateway > Zugriff über Kommandozeile \(CLI\)](#)
- Microsoft 365
- Simple Mail Transfer Protocol (SMTP)
- Domain Name Server oder Domain Name System (DNS)

## Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrundinformationen

Dieses Dokument kann für lokale Gateways oder Cisco Cloud Gateways verwendet werden.

Wenn Sie Cisco Secure Email-Administrator sind, enthält Ihr Begrüßungsschreiben Ihre Cloud Gateway-IP-Adressen und andere relevante Informationen. Zusätzlich zu dem hier angezeigten Brief erhalten Sie eine verschlüsselte E-Mail, die Ihnen zusätzliche Informationen zur Anzahl der für Ihre Zuweisung bereitgestellten Cloud Gateways (auch bekannt als ESA) und Cloud E-Mail- und Web-Manager (auch bekannt als SMA) liefert. Wenn Sie den Brief noch nicht erhalten haben oder keine Kopie davon haben, wenden Sie sich mit Ihren Kontaktinformationen und Ihrem Domain-Namen unter Service an [ces-activations@cisco.com](mailto:ces-activations@cisco.com).



Jeder Client verfügt über dedizierte IPs. Sie können die zugewiesenen IP-Adressen oder Hostnamen aus der Microsoft 365-Konfiguration verwenden.

---



**Hinweis:** Es wird dringend empfohlen, vor einer geplanten Umstellung der E-Mail-Produktion zu testen, da die Replikation von Konfigurationen in der Microsoft 365 Exchange-Konsole Zeit in Anspruch nimmt. Warten Sie mindestens eine Stunde, bis alle Änderungen wirksam werden.

---



**Hinweis:** Die IP-Adressen in der Screenshot-Erfassung stehen im Verhältnis zur Anzahl der Cloud Gateways, die für Ihre Zuweisung bereitgestellt werden. Dies xxx.yy.140.105 ist beispielsweise die IP-Adresse der Schnittstelle Data 1 für Gateway 1 und xxx.yy.150.1143 die IP-Adresse der Schnittstelle Data 1 für Gateway 2. Die IP-Adresse der Data 2-Schnittstelle für Gateway 1 lautet xxx.yy.143.186 und die IP-Adresse der Data 2-Schnittstelle für Gateway 2 xxx.yy.32.98. Wenn Ihr Begrüßungsschreiben keine Informationen zu Data 2 (ausgehende Schnittstellen-IPs) enthält, wenden Sie sich an Cisco TAC, um die Data 2-Schnittstelle zu Ihrer Zuweisung hinzuzufügen.

---

Konfigurieren von Microsoft 365 mit sicherer E-Mail

Konfigurieren von eingehenden E-Mails in Microsoft 365 über Cisco Secure Email

### Umgehen der Spam-Filterregel

- Melden Sie sich beim Microsoft 365 Admin Center an (<https://portal.microsoft.com>).
  - Erweitern Sie im Menü auf der linken Seite **Admin Centers**.
  - Klicken Sie auf **Exchange**.
  - Navigieren Sie im Menü links zu **Mail flow > Rules**.
  - Klicken Sie auf, [+] um eine neue Regel zu erstellen.
  - Wählen Sie **Bypass spam filtering...** eine Option aus der Dropdown-Liste aus.
  - Geben Sie einen Namen für die neue Regel ein: **Bypass spam filtering - inbound email from Cisco CES**.
  - Wählen Sie für \*Diese Regel anwenden, wenn... **The sender - IP address is in any of these ranges or exactly matches**.
1. Fügen Sie in dem Popup-Fenster zur Angabe des IP-Adressbereichs die IP-Adressen hinzu, die in Ihrem Cisco Secure Email-Begrüßungsschreiben angegeben sind.
  2. Klicken Sie auf **OK**.

- Für \*Do the following... wurde die neue Regel vorausgewählt: **Set the spam confidence level (SCL) to... - Bypass spam filtering**.
- Klicken Sie auf **Save**.

Ein Beispiel für das Aussehen einer Regel:

### Bypass spam filtering - inbound email from Cisco CES

Name:

\*Apply this rule if...

\*Do the following...

Except if...

Properties of this rule:  
 Priority:

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



**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.

### Empfangs-Connector

- Verbleiben Sie im Exchange-Verwaltungszentrum.
- Navigieren Sie im Menü links zu **Mail flow > Connectors**.
- Klicken Sie auf, [+] um einen neuen Steckverbinder zu erstellen.
- Wählen Sie im Popup-Fenster "Mail-Fluss auswählen" Folgendes aus:

1. Von: Partner organization

- Zu: **Office365**
  
- Klicken Sie auf **Next**.
- Geben Sie einen Namen für den neuen Connector ein: **Inbound from Cisco CES**.
- Geben Sie bei Bedarf eine Beschreibung ein.
- Klicken Sie auf **Next**.
- Klicken Sie auf **Use the sender's IP address**.
- Klicken Sie auf **Next**.
- Klicken Sie auf, [+] und geben Sie die IP-Adressen ein, die in Ihrem Begrüßungsschreiben für Cisco Secure Email angegeben sind.
- Klicken Sie auf **Next**.
- Auswählen **Reject email messages if they aren't sent over Transport Layer Security (TLS)**.
- Klicken Sie auf **Next**.
- Klicken Sie auf **Save**.

Ein Beispiel, wie Ihre Steckverbinderkonfiguration aussieht:

# 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: 

[Edit sent email identity](#)

## Security restrictions

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

[Edit restrictions](#)

Konfigurieren von E-Mails aus Cisco Secure Email für Microsoft 365

## Zielsteuerelemente

Setze eine Selbstdrosselung in eine Zustellungsdomäne in den Zielsteuerelementen ein. Natürlich können Sie die Drosselung später entfernen, aber dies sind neue IPs zu Microsoft 365, und Sie wollen keine Drosselung durch Microsoft aufgrund seiner unbekanntes Reputation.

- Melden Sie sich bei Ihrem Gateway an.
- Navigieren Sie zu **Mail Policies > Destination Controls**.
- Klicken Sie auf **Add Destination**.

- Nutzung:

1. Ziel: Geben Sie Ihren Domännennamen ein.

2. Concurrent Connections (Gleichzeitige Verbindungen): **10**

- Maximum Messages Per Connection (Maximale Anzahl an Nachrichten pro Verbindung): **20**
- TLS Support (TLS-Unterstützung): **Preferred**

- Klicken Sie auf **Submit**.
- Klicken Sie rechts oben **Commit Changes** in der Benutzeroberfläche auf, um die Konfigurationsänderungen zu speichern.

Ein Beispiel für das Aussehen der Zielsteuerelemententabelle:

Destination Control Table							Items per page 20
Domain	IP Address Preference	Destination Limits	TLS Support	DANE Support ^	Bounce Verification *	Bounce Profile	All <input type="checkbox"/> Delete
<a href="#">your_domain_here.com</a>	Default	10 concurrent connections, 20 messages per connection, Default recipient limit	Preferred	Default	Default	Default	<input type="checkbox"/>
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

Legen Sie als Nächstes die Recipient Access Table (RAT) fest, um E-Mails für Ihre Domänen zu akzeptieren:

- Navigieren Sie zu **Mail Policies > Recipient Access Table (RAT)**.



**Hinweis:** Stellen Sie sicher, dass der Listener für den eingehenden Listener, die eingehende Mail oder den MailFlow verwendet wird, basierend auf dem tatsächlichen Namen des Listeners für den primären E-Mail-Fluss.

- Klicken Sie auf **Add Recipient**.
- Fügen Sie Ihre Domänen im Feld Empfängeradresse hinzu.
- Wählen Sie die Standardaktion **Accept**.



- Klicken Sie auf **Submit**.
- Klicken Sie rechts oben **Commit Changes** in der Benutzeroberfläche auf, um Ihre Konfigurationsänderungen zu speichern.

Ein Beispiel für den RAT-Eintrag:

Recipient Details				
Order:	<input type="text" value="1"/>			
Recipient Address: <span>?</span>	<input type="text" value="your_domain_here.com"/>			
Action:	<input type="button" value="Accept"/> <input type="checkbox"/> Bypass LDAP Accept Queries for this Recipient			
Custom SMTP Response:	<input checked="" type="radio"/> No			
	<input type="radio"/> Yes			
	<table border="1"> <tr> <td>Response Code:</td> <td><input type="text" value="250"/></td> </tr> <tr> <td>Response Text:</td> <td><div style="background-color: #cccccc; height: 100px;"></div></td> </tr> </table>	Response Code:	<input type="text" value="250"/>	Response Text:
Response Code:	<input type="text" value="250"/>			
Response Text:	<div style="background-color: #cccccc; height: 100px;"></div>			
Bypass Receiving Control: <span>?</span>	<input checked="" type="radio"/> No <input type="radio"/> Yes			

## SMTP-Routen

Legen Sie die SMTP-Route für die Zustellung von E-Mails von Cisco Secure Email an Ihre Microsoft 365-Domäne fest:

- Navigieren Sie zu **Network > SMTP Routes**.
- Klicken Sie auf **Add Route...**
- Domäne: Geben Sie Ihren Domänennamen ein.
- Ziel-Hosts: fügen Sie Ihre ursprüngliche Microsoft 365 MX-Datensatz.
- Klicken Sie auf **Submit**.
- Klicken Sie rechts oben **Commit Changes** in der Benutzeroberfläche auf, um Ihre Konfigurationsänderungen zu speichern.

Ein Beispiel für die SMTP-Routeneinstellungen:

SMTP Route Settings			
Receiving Domain: ?	<input type="text" value="your_domain_here.com"/>		
Destination Hosts:	Priority ?	Destination ?	Port
	<input type="text" value="0"/>	<input type="text" value="your_domain.mail.prot"/> <small>(Hostname, IPv4 or IPv6 address.)</small>	<input type="text" value="25"/>
			<input type="button" value="Add Row"/>
Outgoing SMTP Authentication:	No outgoing SMTP authentication profiles are configured. See <a href="#">Network &gt; SMTP Authentication</a>		
<i>Note: DANE will not be enforced for domains that have SMTP Routes configured.</i>			

### DNS-Konfiguration (MX-Eintrag)

Sie sind bereit, die Domäne durch eine Änderung der Mail Exchange (MX)-Datensätze zu entfernen. Lösen Sie Ihre MX-Datensätze zusammen mit Ihrem DNS-Administrator unter den IP-Adressen Ihrer Cisco Secure Email Cloud-Instanz auf, wie in Ihrem Begrüßungsschreiben zu Cisco Secure Email angegeben.

Überprüfen Sie auch die Änderung des MX-Datensatzes von der Microsoft 365-Konsole aus:

- Melden Sie sich bei der Microsoft 365-Administratorkonsole an (<https://admin.microsoft.com>).
- Navigieren Sie zu **Home > Settings > Domains**.
- Wählen Sie Ihren Standard-Domänennamen aus.
- Klicken Sie auf Check Health.

Hier finden Sie die aktuellen MX-Datensätze, die zeigen, wie Microsoft 365 Ihre DNS- und MX-Datensätze sucht, die mit Ihrer Domäne verknüpft sind:

Microsoft 365 admin center

Search

Light mode

Domains > [redacted].com

Managed at Amazon Web Services (AWS) - Default domain

Remove domain Refresh

Overview DNS records Users Teams & groups Apps

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.](#)

Check health Manage DNS Download CSV file Download zone file Print

Search

Microsoft Exchange

Type	Status	Name	Value	TTL
MX	Error	@	0 [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

**Hinweis:** In diesem Beispiel wird der DNS von Amazon Web Services (AWS) gehostet und verwaltet. Als Administrator sollten Sie eine Warnung erwarten, wenn Ihr DNS außerhalb des Microsoft 365-Kontos gehostet wird. Sie können Warnungen ignorieren wie: "Wir haben nicht erkannt, dass Sie neue Datensätze zu your\_domain\_here.com hinzugefügt haben. Vergewissern Sie sich, dass die von Ihnen auf Ihrem Host erstellten Datensätze mit den hier gezeigten übereinstimmen..." Durch die schrittweisen Anweisungen werden die MX-Datensätze auf den ursprünglichen Wert zurückgesetzt, der für die Umleitung an Ihr Microsoft 365-Konto konfiguriert war. Das Cisco Secure Email Gateway wird aus dem eingehenden Datenverkehrsfluss entfernt.

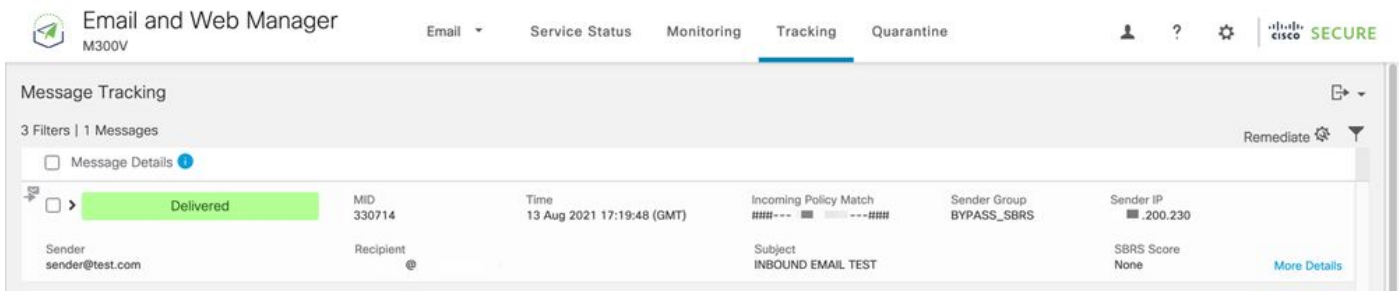
## Eingehende E-Mails testen

Testen Sie eingehende E-Mails an Ihre Microsoft 365-E-Mail-Adresse. Überprüfen Sie dann, ob es in Ihrem Microsoft 365 E-Mail-Posteingang ankommt.

Validieren Sie die E-Mail-Protokolle in der Nachrichtenverfolgung auf Ihrem Cisco Secure Email und Web Manager (auch SMA genannt), der mit Ihrer Instanz bereitgestellt wird.

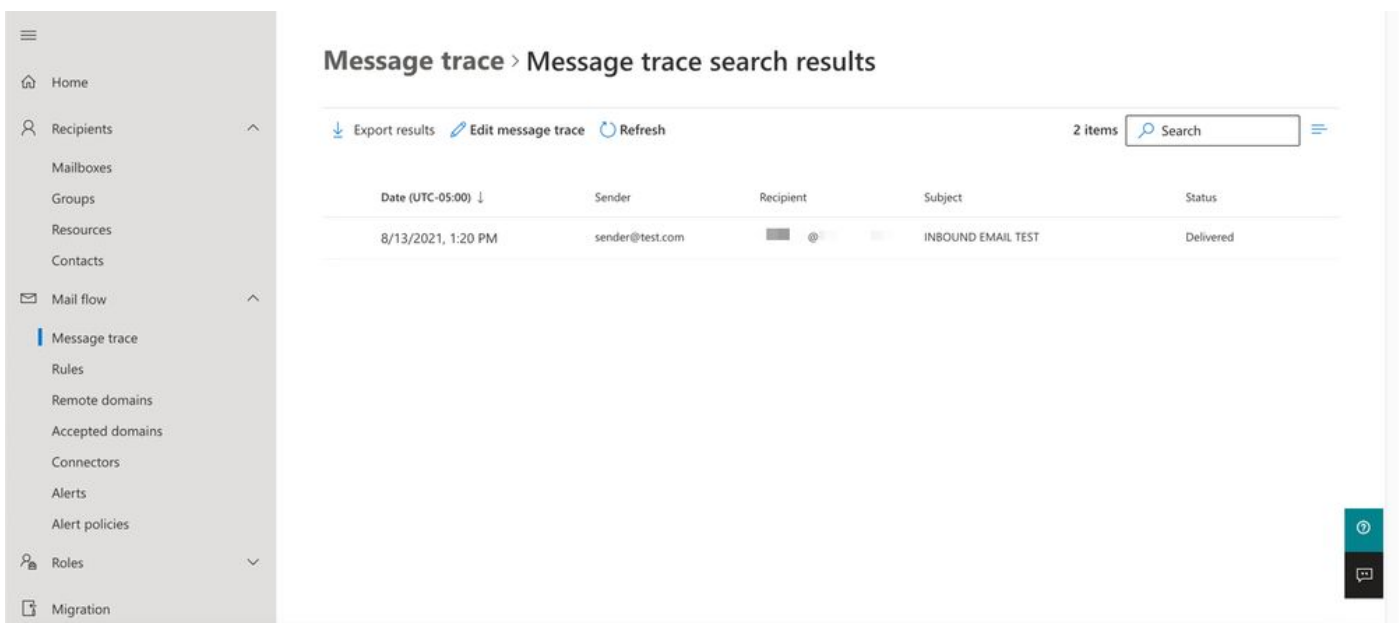
So zeigen Sie E-Mail-Protokolle Ihres SMA an:

- Melden Sie sich bei Ihrer SMA an (<https://sma.iphmx.com/ng-login>).
- Klicken Sie auf **Tracking**.
- Geben Sie die erforderlichen Suchkriterien ein, und klicken Sie auf **Search**, um die gewünschten Ergebnisse anzuzeigen.



So zeigen Sie E-Mail-Protokolle in Microsoft 365 an:

- Melden Sie sich beim Microsoft 365 Admin Center an (<https://admin.microsoft.com>).
- Erweitern **Admin Centers**.
- Klicken Sie auf **Exchange**.
- Navigieren Sie zu **Mail flow > Message trace**.
- Microsoft stellt Standardkriterien für die Suche bereit. Wählen Sie beispielsweise aus **Messages received by my primary domain in the last day**, um Ihre Suchanfrage zu starten.
- Geben Sie die erforderlichen Suchkriterien für Empfänger ein, klicken Sie auf **Search** und erwarten Sie Ergebnisse wie:



Konfigurieren von ausgehenden E-Mails aus Microsoft 365 für Cisco Secure Email

### Konfigurieren von RELAYLIST auf Cisco Secure Email Gateway

Weitere Informationen erhalten Sie in Ihrem Begrüßungsschreiben zu Cisco Secure Email. Darüber hinaus wird eine sekundäre Schnittstelle für ausgehende Nachrichten über Ihr Gateway angegeben.

- Melden Sie sich bei Ihrem Gateway an.
- Navigieren Sie zu **Mail Policies > HAT Overview**.



**Hinweis:** Stellen Sie sicher, dass der Listener für den ausgehenden Listener, für ausgehendeMail oder für MailFlow-Ext vorhanden ist, basierend auf dem tatsächlichen Namen des Listeners für den externen/ausgehenden E-Mail-Fluss.

---

- Klicken Sie auf **Add Sender Group...**
- Konfigurieren Sie die Absendergruppe als:

1. Name: RELAY\_O365

2. Comment (Kommentar): <<enter a comment if you wish to notate your sender group>>

3. Richtlinie: RELAYED

4. Klicken Sie auf **Submit and Add Senders**.

- Absender: **.protection.outlook.com**



**Hinweis:** Die . (Punkt) am Anfang des Absender-Domännennamens erforderlich.

---

- Klicken Sie auf **Submit**.
- Klicken Sie rechts oben **Commit Changes** in der Benutzeroberfläche auf, um Ihre Konfigurationsänderungen zu speichern.

Ein Beispiel für das Aussehen Ihrer Absendergruppeneinstellungen:

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): <i>For IP lookups only</i>	None
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included
<a href="#">&lt;&lt; Back to HAT Overview</a> <span style="float: right;"><a href="#">Edit Settings...</a></span>	

Find Senders	
Find Senders that Contain this Text: ?	<input type="text"/> <input type="button" value="Find"/>

Sender List: Display All Items in List		Items per page 20
<a href="#">Add Sender...</a>		
Sender	Comment	All <input type="checkbox"/> Delete
<a href="#">.protection.outlook.com</a>	From Microsoft 365 mail to Cis...	<input type="checkbox"/>
<a href="#">&lt;&lt; Back to HAT Overview</a>		<input type="button" value="Delete"/>

## Aktivieren von TLS

- Klicken Sie auf **<<Back to HAT Overview**.
- Klicken Sie auf folgende Mailflow-Richtlinie: **RELAYED**.
- Blättern Sie nach unten, und suchen Sie im **Security Features** Abschnitt nach **Encryption and Authentication**.
- Wählen Sie für TLS Folgendes aus: **Preferred**.
- Klicken Sie auf **Submit**.
- Klicken Sie rechts oben **Commit Changes** in der Benutzeroberfläche auf, um Ihre Konfigurationsänderungen zu speichern.

Ein Beispiel für die Konfiguration der Mail Flow Policy:

Encryption and Authentication:	TLS:	<input type="radio"/> Use Default (Off) <input type="radio"/> Off <input checked="" type="radio"/> Preferred <input type="radio"/> Required
		TLS is Mandatory for Address List: <input type="text" value="None"/>
		<input type="checkbox"/> Verify Client Certificate
	SMTP Authentication:	<input checked="" type="radio"/> Use Default (Off) <input type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required
	If Both TLS and SMTP Authentication are enabled:	<input type="checkbox"/> Require TLS To Offer SMTP Authentication

## Konfigurieren von E-Mails von Microsoft 365 nach CES

- Melden Sie sich beim Microsoft 365 Admin Center an (<https://admin.microsoft.com>).
- Erweitern **Admin Centers**.

- Klicken Sie auf **Exchange**.
- Navigieren Sie zu **Mail flow > Connectors**.
- Klicken Sie [+] hier, um einen neuen Steckverbinder zu erstellen.
- Wählen Sie im Popup-Fenster "Mail-Fluss auswählen" Folgendes aus:

1. Von: Office365

- Zu: Partner organization

- Klicken Sie auf **Next**.
- Geben Sie einen Namen für den neuen Connector ein: **Outbound to Cisco CES**.
- Geben Sie bei Bedarf eine Beschreibung ein.
- Klicken Sie auf **Next**.
- Für Wann möchten Sie diesen Connector verwenden?:

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

- Klicken Sie auf **Next**.

- Klicken Sie auf **Route email through these smart hosts**.
- Klicken Sie auf, [+] und geben Sie die ausgehenden IP-Adressen oder Hostnamen ein, die in Ihrem CES-Begrüßungsschreiben angegeben sind.
- Klicken Sie auf **Save**.
- Klicken Sie auf **Next**.
- Wie sollte Office 365 mit dem E-Mail-Server Ihrer Partnerorganisation verbunden werden?

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

- Wählen Any digital certificate, including self-signed certificates Sie.

- Klicken Sie auf **Next**.
  
- Der Bestätigungsbildschirm wird angezeigt.
  
- Klicken Sie auf **Next**.
  
- Geben Sie [+] eine gültige E-Mail-Adresse ein, und klicken Sie auf **OK**.
  
- Klicken Sie auf, **Validate** und lassen Sie die Validierung laufen.
  
- Klicken Sie abschließend auf **Close**.
  
- Klicken Sie auf Save.

Ein Beispiel für den Outbound Connector:



# 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:   .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. Wählen Sie im Popup-Fenster "Absenderstandort auswählen" Folgendes aus: **Inside the organization**.

- Klicken Sie auf **OK**.
  
- Klicken Sie auf **More options...**
  
- Klicken Sie auf die **add condition** Schaltfläche, und fügen Sie eine zweite Bedingung ein:

1. Auswählen **The recipient...**

- Auswahl: **Is external/internal**.
  
- Wählen Sie im Popup-Fenster "Absenderstandort auswählen" Folgendes aus: **Outside the organization** .
  
- Klicken Sie auf **OK**.
  
  
- Wählen Sie für \* Folgendes aus: **Redirect the message to...**

1. Wählen Sie **den folgenden Steckverbinder aus**.

2. Wählen Sie den **ausgehenden Anruf für den Cisco CES-Anschluss** aus.

3. Klicken Sie auf **OK**.

- Kehren Sie zu "\*Do the following..." zurück, und fügen Sie eine zweite Aktion ein:


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

- Auswahl: **set the message header**
  
- Legen Sie folgenden Nachrichten-Header fest: **X-OUTBOUND-AUTH**.
  
- Klicken Sie auf **OK**.
  
- Legen Sie den Wert fest: **mysecretkey**.

- Klicken Sie auf **OK**.

- Klicken Sie auf **Save**.

---

 **Hinweis:** Um nicht autorisierte Nachrichten von Microsoft zu verhindern, kann ein geheimer x-Header gestempelt werden, wenn Nachrichten Ihre Microsoft 365-Domäne verlassen. Dieser Header wird ausgewertet und vor der Zustellung an das Internet entfernt.

---

Ein Beispiel für die Microsoft 365 Routing-Konfiguration:

## 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:

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

- Klicken Sie auf Return (Rücklauf), um eine neue, leere Zeile zu erstellen.
- Geben Sie [,] in der neuen Zeile ein, um den neuen Nachrichtenfilter zu beenden.
- Klicken Sie **return** einmal, um das Menü Filters (Filter) zu verlassen.
- Führen Sie den **Commit** Befehl aus, um die Änderungen an der Konfiguration zu speichern.



**Hinweis:** Vermeiden Sie Sonderzeichen für den geheimen Schlüssel. Die im Nachrichtenfilter gezeigten Zeichen ^ und \$ sind reguläre Zeichen und werden wie im Beispiel angegeben verwendet.

---



**Hinweis:** Überprüfen Sie den Namen der RELAYLIST-Konfiguration. Es kann mit einem alternativen Namen konfiguriert werden, oder Sie können einen bestimmten Namen haben, der auf Ihrer Relay-Richtlinie oder Ihrem Mail-Provider basiert.

---

### **Ausgehende E-Mails testen**

Testen Sie ausgehende E-Mails von Ihrer Microsoft 365-E-Mail-Adresse an einen externen Domänenempfänger. Sie können die Nachrichtenverfolgung über Ihren Cisco Secure Email und Web Manager überprüfen, um sicherzustellen, dass der ausgehende Datenverkehr ordnungsgemäß weitergeleitet wird.



**Hinweis:** Überprüfen Sie Ihre TLS-Konfiguration (**Systemverwaltung > SSL-Konfiguration**) für das Gateway und die für ausgehenden SMTP verwendeten Chiffren. Cisco Best Practices empfiehlt Folgendes:

HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3DES:!SSLv2:!SSLv3

Beispiel für die Nachverfolgung bei erfolgreicher Zustellung:

The screenshot shows the 'Tracking' tab in the Email and Web Manager. A message with MID 186371, 186372 is shown as 'Delivered'. The outgoing policy match is '>>>\_<<<<'. The sender group is 'RELAY\_O365' and the sender IP is '59.175'. A green arrow points to the 'Sender Group' field with the text 'Validate your RELAY Sender Group and Mail Flow Policy'. A blue arrow points to the 'Sender IP' field with the text 'IP address from Microsoft 365'. A 'More Details' link is visible at the bottom right.

Klicken Sie hier, **More Details** um die vollständigen Nachrichtendetails anzuzeigen:

The screenshot shows the 'More Details' view for the message. The 'Processing Details' section includes a 'Summary' of the message flow: incoming connection, SMTP interface data, RELAY sender group match, TLS protocol acceptance, message enqueue, and outgoing direction. The 'Envelope Header and Summary' section shows the last state as 'Delivered', message ID, time, sender, and recipient. The 'Sending Host Summary' section shows the reverse DNS hostname, IP address, and SBRS score.

Beispiel für die Nachrichtenverfolgung, bei dem der x-Header nicht übereinstimmt:

The screenshot shows the 'Tracking' tab in the Email and Web Manager. A message with MID 94011 is shown as 'Dropped By Message Filters'. The outgoing policy match is 'N/A'. The sender group is 'RELAY\_O365' and the sender IP is '59.174'. A 'More Details' link is visible at the bottom right.



[Email and Web Manager](#) M100V
 
[Email](#)
[Service Status](#)
[Monitoring](#)
[Tracking](#)
[Quarantine](#)

[?](#)
[cisco](#) **SECURE**

[< Back to Summary](#)  
**Message Tracking**

[< Previous](#)
[Next >](#)

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 queued 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'**

**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

Note this was dropped by our specific Message Filter written earlier

Zugehörige Informationen

Cisco Secure Email Gateway-Dokumentation

- [Versionshinweise](#)
- [Benutzerhandbuch](#)
- [CLI-Referenzhandbuch](#)
- [API-Programmierhandbücher für Cisco Secure Email Gateway](#)
- [Open Source für Cisco Secure Email Gateway](#)
- [Installationsanleitung für die Cisco Content Security Virtual Appliance](#) (einschließlich vESA)

Secure Email Cloud Gateway - Dokumentation

- [Versionshinweise](#)
- [Benutzerhandbuch](#)

Cisco Secure Email und Web Manager-Dokumentation

- [Versionshinweise und Kompatibilitätstmatrix](#)

- [Benutzerhandbuch](#)
- [API-Programmierhandbücher für Cisco Secure Email und Web Manager](#)
- [Installationsanleitung für die Cisco Content Security Virtual Appliance](#) (einschließlich vSMA)

Cisco Secure-Produktdokumentation

- [Cisco Secure Portfolio Naming Architecture](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.