



# Integración Cisco Cloud SEG con Office 365

## Comunidad de Cisco

Fernando Ramos - Technical Consulting Engineer

Jesús Sánchez - Technical Consulting Engineer

José Luis Dávila - Technical Consulting Engineer

Jueves 21 de marzo de 2024



# Conecte, Interactúe, ¡Colabore!

## Soluciones

Ayuda a otros usuarios a encontrar las respuestas correctas en el motor de búsqueda de la comunidad indicando que la duda fue resuelta al activar la opción “Aceptar como solución” u otórgales un voto de utilidad.

Aceptar como solución

## Votos de utilidad

¡Resalta el esfuerzo de otros miembros!

Los votos útiles motivan a otros miembros que colaboran en la comunidad, a seguir ayudándonos a contestar las preguntas abiertas, y ofreciéndoles la oportunidad de ganar premios. ¡Reconoce su esfuerzo!

👍 0 Útil

# Premios Spotlight Awards

¡Destaca por tu esfuerzo y compromiso para mejorar la comunidad y ayudar a otros miembros!

Los Premios Spotlight se otorgan trimestralmente para reconocer a los miembros más destacados.

Conoce a los ganadores de [Agosto-Octubre 2024](#)

¡Ahora también puedes nominar a un candidato! [Haga clic aquí](#)



# Nuestros expertos

## Fernando Ramos



### Team Captain Content Security

Se unió a Cisco en 2018 y desde entonces ha sido parte del equipo de Content Security. A lo largo de su carrera, se ha desempeñado en diferentes roles dentro del equipo de Content Security, y se ha especializado en temas de seguridad de correo electrónico.

Actualmente, Fernando es Capitán del equipo de Content Security en México.

Descarga la presentación <https://bit.ly/CL3doc-mar24>

# Nuestros expertos

## Jesús Sánchez Méndez



Technical Consulting Engineer

Es Consultor de Seguridad con más de 10 años de trayectoria en el área de TI, destacándose por su enfoque en mejorar la satisfacción del cliente y promover mejoras operativas en seguridad.

Ha liderado la implementación de soluciones de seguridad en diversos proyectos de TI para el Gobierno Federal y la iniciativa privada, aunado al dominio que posee de estándares de seguridad como el ISO 27001.

Actualmente, se desempeña como el experto en el servicio de cifrado de correo electrónico en Cisco.

Descarga la presentación <https://bit.ly/CL3doc-mar24>

# Nuestros expertos

## José Luis Dávila Becerril



### Escalation Engineer Content Security

Se unió a Cisco en 2019, como Technical Consulting Engineer en el equipo de Email Security, ayudando a clientes de Cisco alrededor del mundo.

Actualmente, se desempeña como Escalation Engineer para el equipo de Content Security, soportando múltiples tecnologías como Email Security, Web Security y Cisco Defense Orchestrator.

Descarga la presentación <https://bit.ly/CL3doc-mar24>

slido

Join at  
**slido.com**  
**#2154 787**

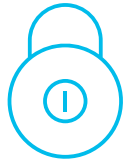
 Passcode: **bwke24**



# Agenda



1. Planteamiento de problema
2. Configuración de correo electrónico de entrada
3. Configuración de correo electrónico de salida
4. Configuración de DNS
5. Probar correo entrada y salida
6. Revisión de logs y troubleshooting básico





Join at  
**slido.com**  
**#2154 787**

🔍 Passcode:  
**bwke24**

**¿Qué protocolos son necesarios para que se pueda entregar un correo electrónico?**

a) SMTP y DNS

0%

b) SMTP y TLS

0%

c) TCP y DNS

0%



# Planteamiento de problema

- Introducción
- Planteamiento de problema**
- Configuración de correo electrónico de entrada
- Configuración de correo electrónico de salida
- Configuración de DNS
- Probar correo entrada y salida
- Revisión de logs y troubleshooting básico



*La presente integración tiene como finalidad atender la necesidad de implementar una solución integral y flexible que garantice la seguridad, la continuidad y la eficiencia en la comunicación empresarial, adaptándose a las necesidades cambiantes del entorno empresarial.*

# Cisco Cloud Security Email Gateway



# Cisco Cloud Security Email Gateway

Los prerequisites son:

- Tener permisos de administrador en todos los entornos (0365 / SEG / DNS)
- Acceso CLI en entorno SEG (Secure Email Gateway) preferentemente
- Contar con el correo de bienvenida por parte de Cisco (ya que se proporciona información técnica y de acceso a su servicio)



# Your Cisco Cloud Email Security (CES) service is ready!

Organization Name: ██████████

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.████████.iphmx.com
- mx2.████████.iphmx.com

## Your Cisco CES portals:

### Email Security

https://dh████████-esa1.iphmx.com

### Security Management

https://dh████████-sma1.iphmx.com

### End User Quarantine

https://dh████████-euq1.iphmx.com

## Please sign in the portals with this user ID:

Username: ██████████

Password: ██████████

**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:

████████.140.105

████████.150.143

████████.143.186

████████.32.98

### Security Management:

████████.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████████.iphmx.com

## Include CES host and IP address in your SPF record:

v=spf1 exists:%{j}.spf.hc████████.iphmx.com ~all



Your Cisco Secure Email Cloud Gateway is using the port(s) 3268 or 389 for LDAP communication. By default, there is no security provision for these ports, making you vulnerable to man-in-the-middle attacks.

Cisco will be closing and blocking these ports (3268 and 389) as of 2023-07-25 (July 25th, 2023), so you must work to ensure that Secure LDAP (LDAPS) is configured within your LDAP environment and that you modify the LDAP configuration on your Secure Email Cloud Gateway to instead use port 3269 (for AD) or 636 (for OpenLDAP). If these ports are not changed by July 25th, 2023, then there may be an impact on your email flow and additional settings and services.

Here is a resource that you can use as a guide for performing this change: <https://docs.ces.cisco.com/docs/non-secure-ldap>

NOTE: This session will expire if left idle for 30 minutes. Any uncommitted configuration changes will be lost. Commit the configuration changes as soon as they are made.

### **Warning!**

You are currently using a demonstration certificate(Cisco ESA Certificate) which is not secure and is not recommended for general use. Create or import a certificate using the certconfig > CERTIFICATE option.

The features/services that are currently using the demonstration certificate are:

```
listener 'OutgoingMail'
```

```
(Machine esa1.hc5588-66.iphmx.com) (SERVICE)>
```

# Configuración de correo electrónico de entrada

- Introducción
- Planteamiento de problema
- Configuración de correo electrónico de entrada**
- Configuración de correo electrónico de salida
- Configuración de DNS
- Probar correo entrada y salida
- Revisión de logs y troubleshooting básico

# Pasos a realizar en Microsoft Office 365

1. Crear Regla
2. Crear Conector






Microsoft

Pick

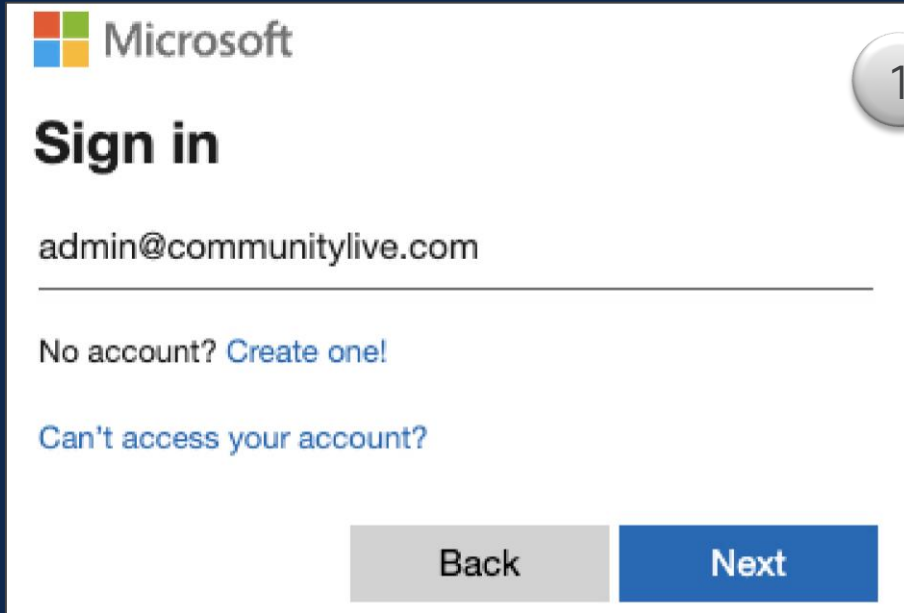
⌵

⋮

+



# Microsoft Office 365



Microsoft

## Sign in

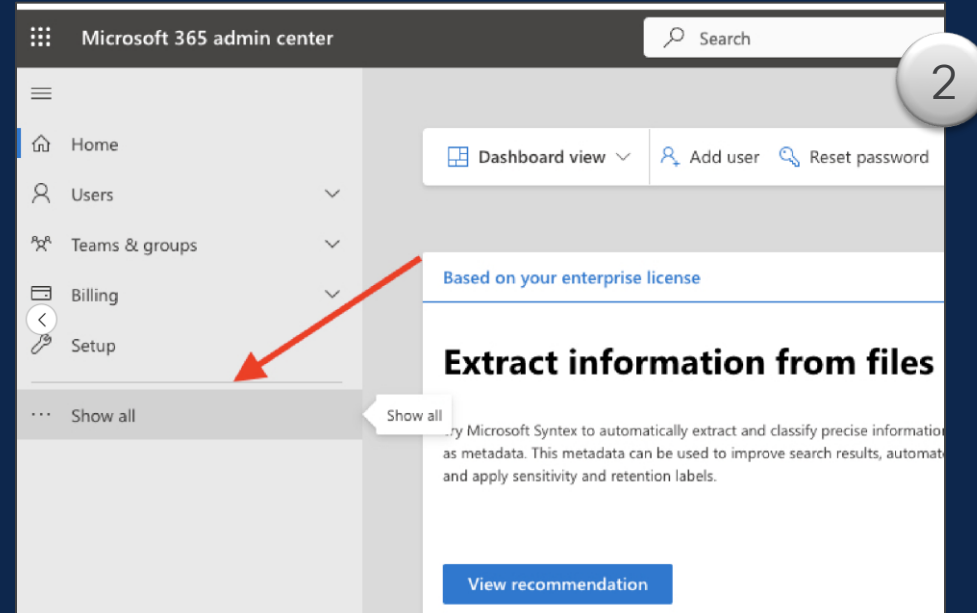
admin@communitylive.com

No account? [Create one!](#)

[Can't access your account?](#)

[Back](#) [Next](#)

1



Microsoft 365 admin center

Search

Dashboard view Add user Reset password

Home Users Teams & groups Billing Setup Show all

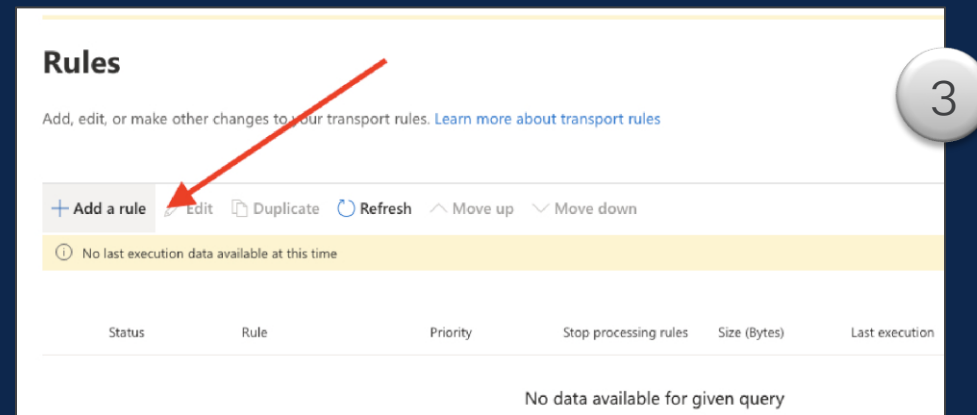
Based on your enterprise license

### Extract information from files

Use Microsoft Syntex to automatically extract and classify precise information from files as metadata. This metadata can be used to improve search results, automate workflows, and apply sensitivity and retention labels.

[View recommendation](#)

2



## Rules

Add, edit, or make other changes to your transport rules. [Learn more about transport rules](#)

+ Add a rule Edit Duplicate Refresh Move up Move down

No last execution data available at this time

Status	Rule	Priority	Stop processing rules	Size (Bytes)	Last execution
--------	------	----------	-----------------------	--------------	----------------

No data available for given query

3

# Microsoft Office 365 – Regla

**Rules**

Add, edit, or make other changes to your transport rules. [Learn more about transport rules](#)

+ Add a rule Edit Duplicate Refresh Move up Move down

- Create a new rule
- Apply Office 365 Message Encryption and rights protection to messages
- Apply custom branding to OME messages
- Apply disclaimers
- Filter messages by size
- Modify messages
- Restrict managers and their direct reports
- Restrict messages by sender or recipient
- Send messages to a moderator
- Send messages and save a copy for review

**New transport rule**

● Set rule conditions  
○ Set rule settings  
○ Review and finish

## Set rule conditions

Name and set conditions **Add action** transport rule

Name \*  
Bypass Spam Filtering

Apply this rule if \*  
The sender IP address is in any of these ranges ...  
Sender's IP address is in the range [Enter words](#)

Do the following \*  
Select one Select one

Except if  
Select one Select one

**specify IP address ranges**

Enter an IPv4 or IPv6 address, or range **Add**

Edit Delete **1 item**

- ✓ 2 1

# Microsoft Office 365 – Regla

The image displays three sequential screenshots of the Microsoft Office 365 transport rule configuration interface, numbered 1, 2, and 3.

**Screenshot 1: Set rule conditions**  
This screen shows the initial configuration step. The left sidebar lists the steps: "Set rule conditions" (selected), "Set rule settings", and "Review and finish". The main content area is titled "Set rule conditions" and includes a progress indicator. The "Name" field is set to "Bypass Spam Filtering". Under "Apply this rule if", the condition is "The sender" with the sub-condition "IP address is in any of these ranges ...". The specific range is "Sender's IP address is in the range: '216.71.150.41'". Under "Do the following", the action is "Modify the message properties" with the sub-action "set the spam confidence level (SCL)". The specific setting is "Set the spam confidence level (SCL) to '-1'". The "Except if" section is currently empty.

**Screenshot 2: Set settings for your transport rule**  
This screen shows the "Set settings for your transport rule" step. The left sidebar shows "Set rule conditions" as completed and "Set rule settings" as the current step. The "Rule mode" is set to "Enforce". The "Severity" is "Not specified". There are options to "Activate this rule on" (3/13/2024 at 2:30 PM) and "Deactivate this rule on" (3/13/2024 at 2:30 PM). There are also checkboxes for "Stop processing more rules" and "Defer the message if rule processing doesn't complete". The "Match sender address in message" is set to "Header". A "Comments" text area is present. A "Next" button is visible at the bottom right.

**Screenshot 3: New transport rule**  
This screen shows the "New transport rule" step. The left sidebar shows all three steps as completed. A green banner at the top indicates "Transport rule created successfully". A "Done" button is visible at the bottom right.


Microsoft

Pick

⌵

⋮

+



# Microsoft Office 365 – Connector

Home

Recipients

Mailboxes

Groups

Resources

Contacts

Mail flow

Message trace

Rules

Remote domains

Accepted domains

Connectors

Alerts

Alert policies

Home > Connectors

## Connectors

Connectors help control the flow of email messages to and from your Office 365 organization. We recommend that you [check to see if you should create a connector](#), since most organizations don't use them.

[+ Add a connector](#) [Refresh](#)

Status	Name	From
--------	------	------

### Add a connector

**New connector**

- Name
- Authenticating sent email
- Security restrictions
- Review connector

## New connector

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.

**Connection from**

Office 365

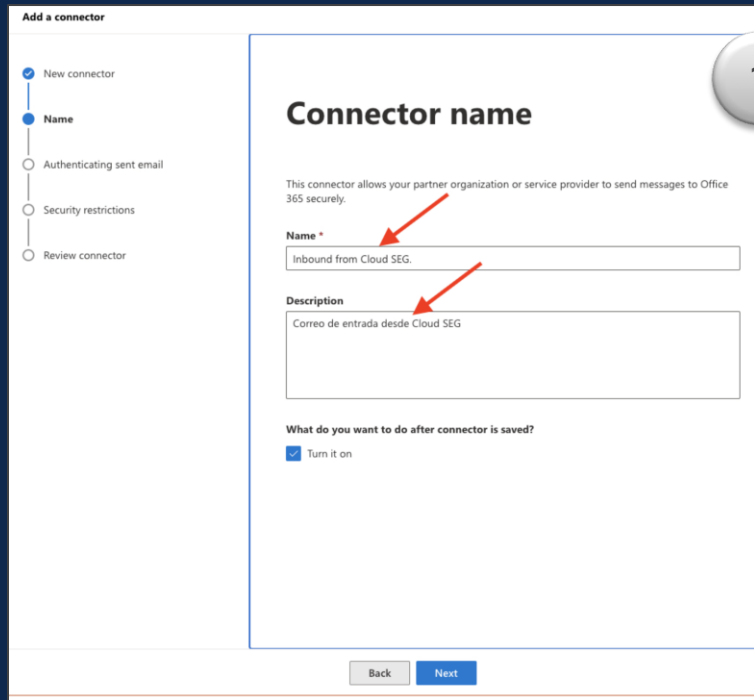
Your organization's email server

Partner organization

**Connection to**

Office 365

# Microsoft Office 365 – Connector



**Add a connector**

- New connector
- Name**
- Authenticating sent email
- Security restrictions
- Review connector

## Connector name

This connector allows your partner organization or service provider to send messages to Office 365 securely.

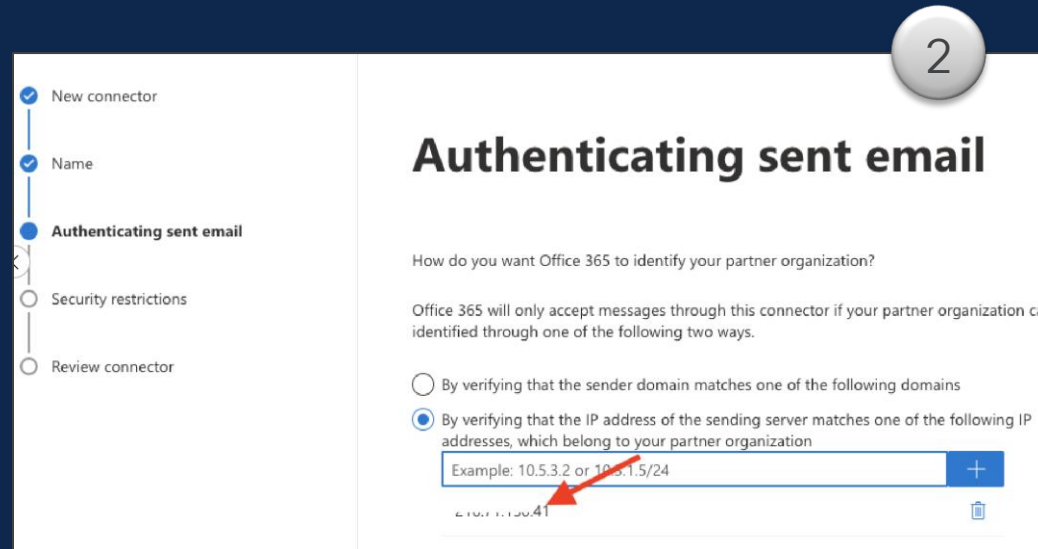
**Name \***  
Inbound from Cloud SEG.

**Description**  
Correo de entrada desde Cloud SEG

What do you want to do after connector is saved?  
 Turn it on

Back Next

1



**Add a connector**

- New connector
- Name
- Authenticating sent email**
- Security restrictions
- Review connector

## Authenticating sent email

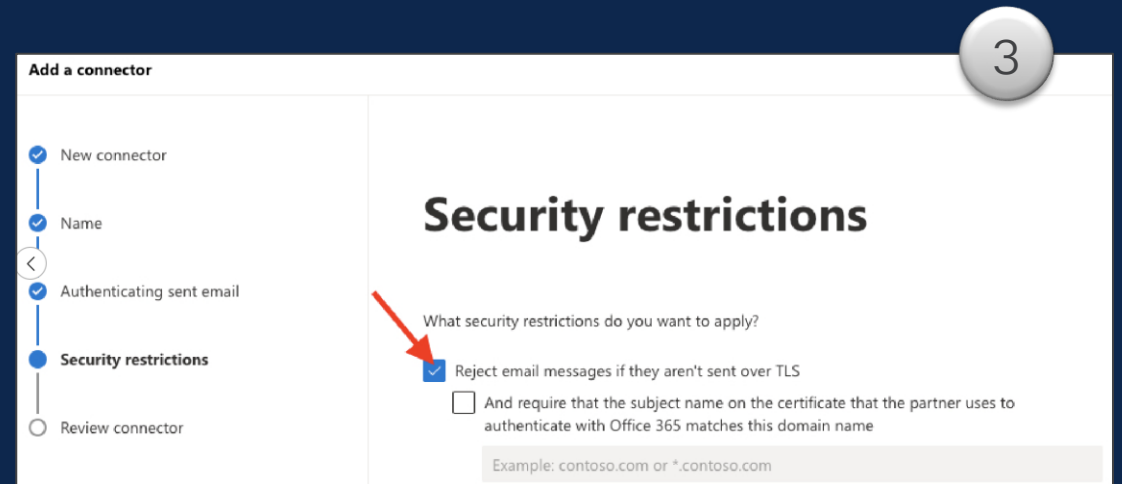
How do you want Office 365 to identify your partner organization?

Office 365 will only accept messages through this connector if your partner organization can be identified through one of the following two ways.

- By verifying that the sender domain matches one of the following domains
- By verifying that the IP address of the sending server matches one of the following IP addresses, which belong to your partner organization

Example: 10.5.3.2 or 10.5.1.5/24

2



**Add a connector**

- New connector
- Name
- Authenticating sent email
- Security restrictions**
- Review connector

## Security restrictions

What security restrictions do you want to apply?

- Reject email messages if they aren't sent over TLS
- And require that the subject name on the certificate that the partner uses to authenticate with Office 365 matches this domain name

Example: contoso.com or \*.contoso.com

3

# Microsoft Office 365 – Connector

1

**Add a connector**

- ✓ New connector
- ✓ Name
- ✓ Authenticating sent email
- ✓ Security restrictions
- Review connector

## Review connector

**Mail flow scenario**  
From: Partner organization  
To: Office 365

**Name**  
Inbound from Cloud SEG.

**Status**  
Turn it on after saving  
[Edit name](#)

**How to identify your partner organization**  
Identify the partner organization by verifying that messages are coming from these IP address ranges: 200.1.1.1  
[Edit sent email identity](#)

**Security restrictions**  
Reject messages if they aren't encrypted using Transport Layer Security (TLS)  
[Edit restrictions](#)

[Back](#) [Create connector](#)

2

**Add a connector**

- ✓ New connector
- ✓ Name
- ✓ Authenticating sent email
- ✓ Security restrictions
- ✓ Review connector

✓ Connector created  
[Add another connector](#)





# Pasos que realizar en Cisco Cloud Security Email Gateway

1. Crear *Destination Control*
2. Crear registro en *Recipient Access Table (RAT)*
3. Creación de ruta SMTP



Success — You have been logged out.

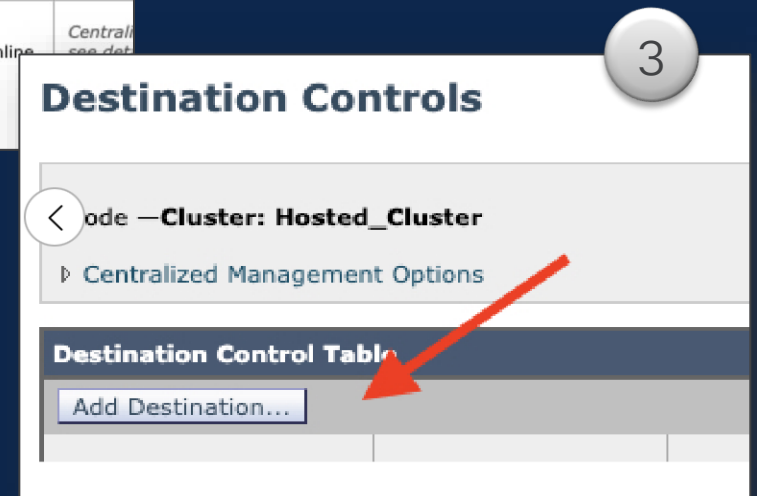
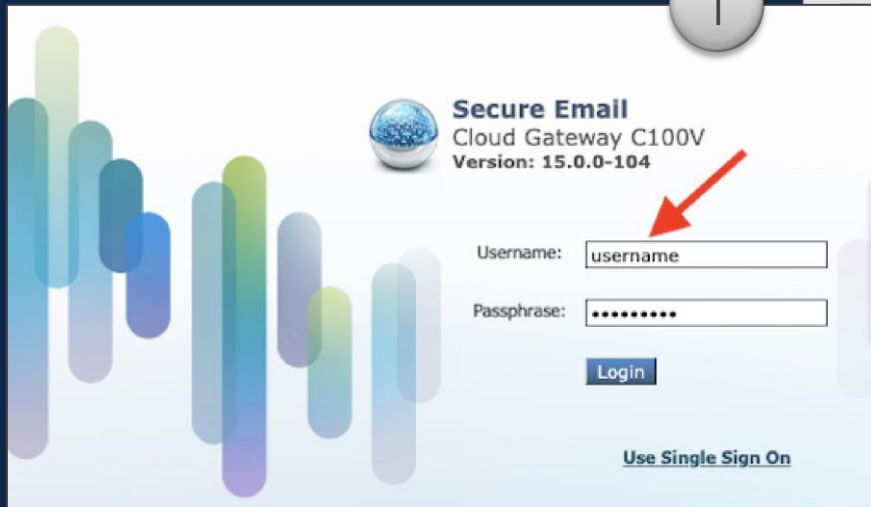
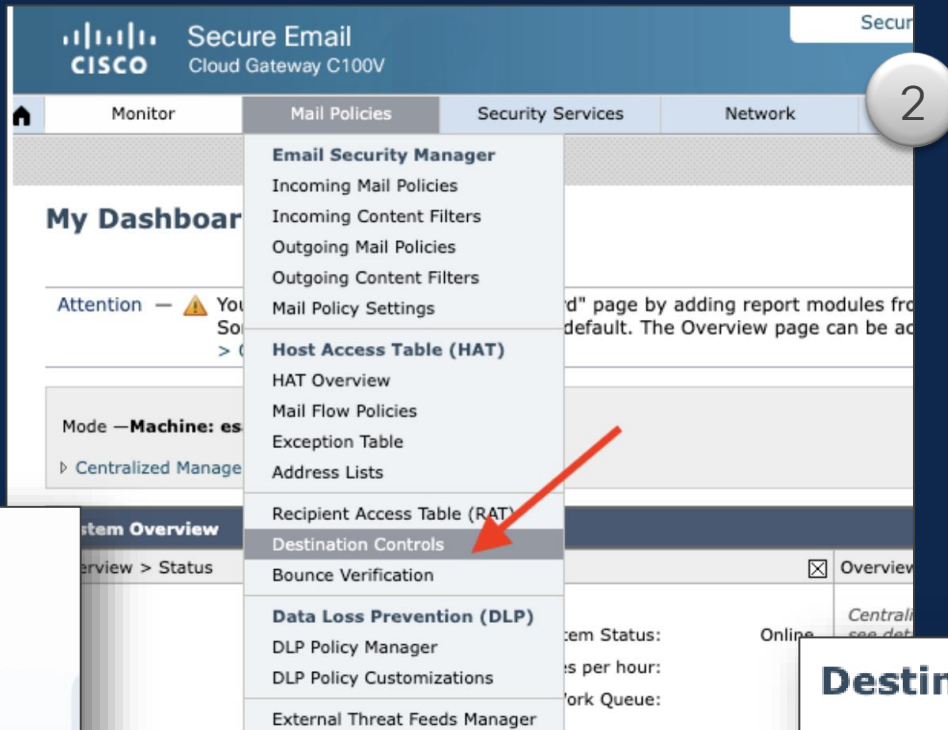
Secure Email  
Cloud Gateway C100V  
Version: 15.0.0-104

Single Sign On

Copyright © 2003-2023 Cisco Systems, Inc. CISCO

The splash screen features a large blue play button icon in the center. The background is light blue with vertical bars of various colors (teal, green, purple) on the left and right sides. The Cisco logo is in the bottom right corner.

# Cisco Cloud Security Email Gateway Destination Control



# Cisco Cloud Security Email Gateway Destination Control

**Add Destination Controls**

Mode — Cluster: **Hosted\_Cluster** Change Mode...

Centralized Management Options

**Destination Controls**

Destination:

IP Address Preference:

Limits:

Concurrent Connections:  Use Default (500)  Maximum of  (between 1 and 1,000)

Maximum Messages Per Connection:  Use Default (50)  Maximum of  (between 1 and 1,000)

Recipients:  Use Default (No Limit)  Maximum of  per  minutes  
Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60

Apply limits: Per Secure Email hostname:  System Wide  Each Virtual Gateway  
(recommended if Virtual Gateways are in use)

TLS Support:

Certificate:

DANE Support:

Bounce Verification: Perform address tagging:  Default (No)  No  Yes  
Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.

Bounce Profile:

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

Cancel Submit

tacmexesa.com	Default	10 concurrent connections, 20 messages per connection, Default recipient limit	Default	Default	Default	Default	Default
---------------	---------	--	---------	---------	---------	---------	---------



# Cisco Cloud Security Email Gateway Destination Control



- Si no se especifica un destination control , se utiliza el predeterminado

**Destination Controls**

Mode —Cluster: **Hosted\_Cluster** Change Mode...

Centralized Management Options

**Destination Control Table** Items per page 20

[Add Destination...](#) Import Table

Domain ▲	IP Address Preference	Destination Limits	TLS Support	Certificate	DANE Support ^	Bounce Verification *	Bounce Profile	All <input type="checkbox"/> Delete
diegogo.net	Default	10 concurrent connections, 20 messages per connection, Default recipient limit	Default	Default	Default	Default	Default	<input type="checkbox"/>
gmail.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Preferred	Default	Opportunistic	Default	Default	<input type="checkbox"/>
hotmail.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	Default	<input type="checkbox"/>
lall.com.mx	Default	10 concurrent connections, 20 messages per connection, Default recipient limit	Default	Default	Default	Default	Default	<input type="checkbox"/>
mexesa.com	Default	2 concurrent connections, 2 messages per connection, Default recipient limit	Default	Default	Default	Default	Default	<input type="checkbox"/>
tacmexesa.com	Default	10 concurrent connections, 20 messages per connection, Default recipient limit	Default	Default	Default	Default	Default	<input type="checkbox"/>
texashealthpartners.com	Default	Default connection limit, 50 messages per connection, Default recipient limit	Preferred	Default	None	Default	Default	<input type="checkbox"/>
yahoo.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	Default	<input type="checkbox"/>
Default	IPv4 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	Preferred	ciscoss1_signed_cert	None	Off	Default	<input type="checkbox"/>

[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.



No Changes Pending

# My Dashboard

Printable PDF

Attention — You can customize this "My Dashboard" page by adding report modules from different reports. Some modules are added for you by default. The Overview page can be accessed from Monitor > Overview.

Mode —Machine: esa1.hc5588-66.iphmx.com

Change Mode...

Centralized Management Options

## System Overview

Overview > Status	Overview > Quarantines - Top 3 by Disk Usage (Policy and Virus)	Overview > Threat Level
<p>System Status: Online</p> <p>Incoming Messages per hour: 0</p> <p>Messages in Work Queue: 0</p>	<p>Centralized Services are enabled (For Policy, Virus and Outbreak Quarantines). Please see details at SMA 68.232.130.237.</p>	<p>Centralized Services are enabled (For Policy, Virus and Outbreak Quarantines). Please see details at SMA 68.232.130.237.</p>
System Status Details	Local Quarantines	Outbreak Details

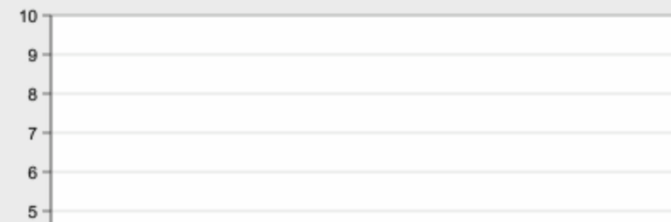
General No modules currently selected for this section.

Time Range: Day

19 Mar 2024 01:00 to 20 Mar 2024 01:54 (GMT -06:00)

Data in time range:99.93 % complete

## Overview > Incoming Mail Graph



## Overview > Incoming Mail Summary

Message Category	%	Messages
Stopped by IP Reputation Filtering	66.7%	10
Stopped by Domain Reputation Filtering	0.0%	0
Stopped as Invalid Recipients	0.0%	0
Spam Detected	0.0%	0

How-To's

# Cisco Cloud Security Email Gateway Recipient Access Table (RAT)

**Secure Email**  
Cloud Gateway C100V

Monitor | Mail Policies | Security Services

**Recipient Access Table (RAT)**

- Email Security Manager
  - Incoming Mail Policies
  - Incoming Content Filters
  - Outgoing Mail Policies
  - Outgoing Content Filters
  - Mail Policy Settings
- Host Access Table (HAT)**
  - HAT Overview
  - Mail Flow Policies
  - Exception Table
  - Address Lists
  - Recipient Access Table (RAT)**

Mode — Cluster: Hosted\_Cluster

Centralized Management Options

Overview for Listening

Add Recipient...

Order | Recipient Address

**Add to Recipient Access Table**

Mode — Cluster: Hosted\_Cluster Change Mode...

Centralized Management Options

**Recipient Details**

Order:

Recipient Address:

Action:

Bypass LDAP Accept Queries for this Recipient

Custom SMTP Response:  No  Yes

Response Code:

Response Text:

Bypass Receiving Control:  No  Yes

Cancel Submit



# Cisco Cloud Security Email Gateway Recipient Address Table (RAT)

TAC Tip



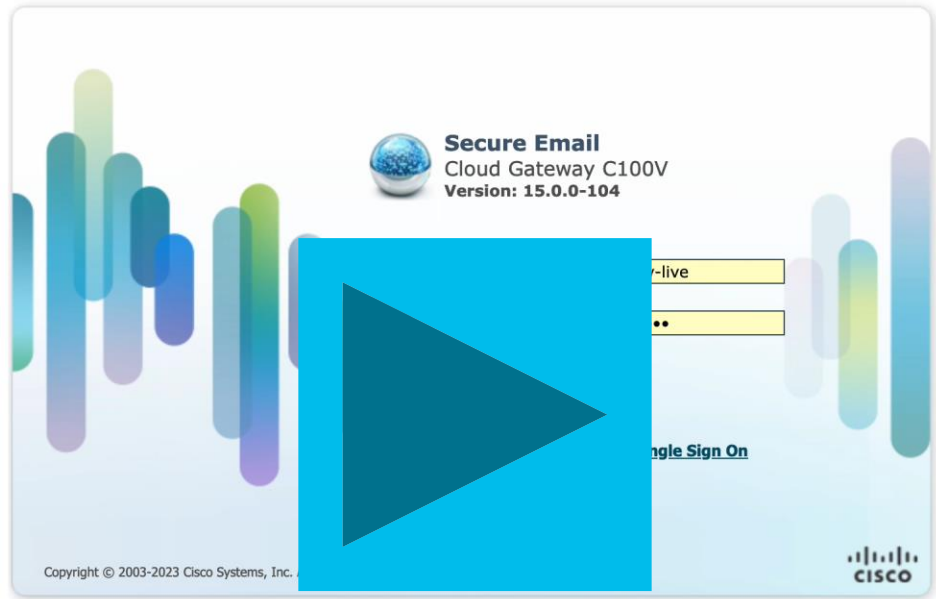
- Si no está en la Recipient Address Table, no te abre la puerta.





Login Host: **esa1.hc5588-66.iphmx.com**  
Help and Support

Success — You have been logged out.



# Cisco Cloud Security Email Gateway SMTP Routes

Secure Email Gateway is getting a new look. Try

Secure Email  
Cloud Gateway C100V

Monitor Mail Policies Security Services **Network** System Administration

IP Interfaces  
Listeners  
**SMTP Routes**  
DNS  
Routing  
SMTP Call-Ahead  
Bounce Profiles  
SMTP Authentication  
Incoming Relays  
Certificates  
Cloud Service Settings  
CRL Sources

SMTP Routes

Mode —Cluster: Hosted\_Cluster

Centralized Management Options

SMTP Routes List

Add Route...

Items per page

Clear All Routes Import Routes

SMTP Routes

Mode —Cluster: Hosted\_Cluster

Centralized Management Options

SMTP Routes List

Add Route...

Add SMTP Route

Mode —Cluster: Hosted\_Cluster

Change Mode...

Centralized Management Options

SMTP Route Settings

Receiving Domain: ? dominio.com

Destination Hosts:

Priority ?	Destination ?	Port	
0	dominio.mail.protection.oi	25	Add Row
	(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.

Cancel Submit



# Recomendaciones

TAC Tip

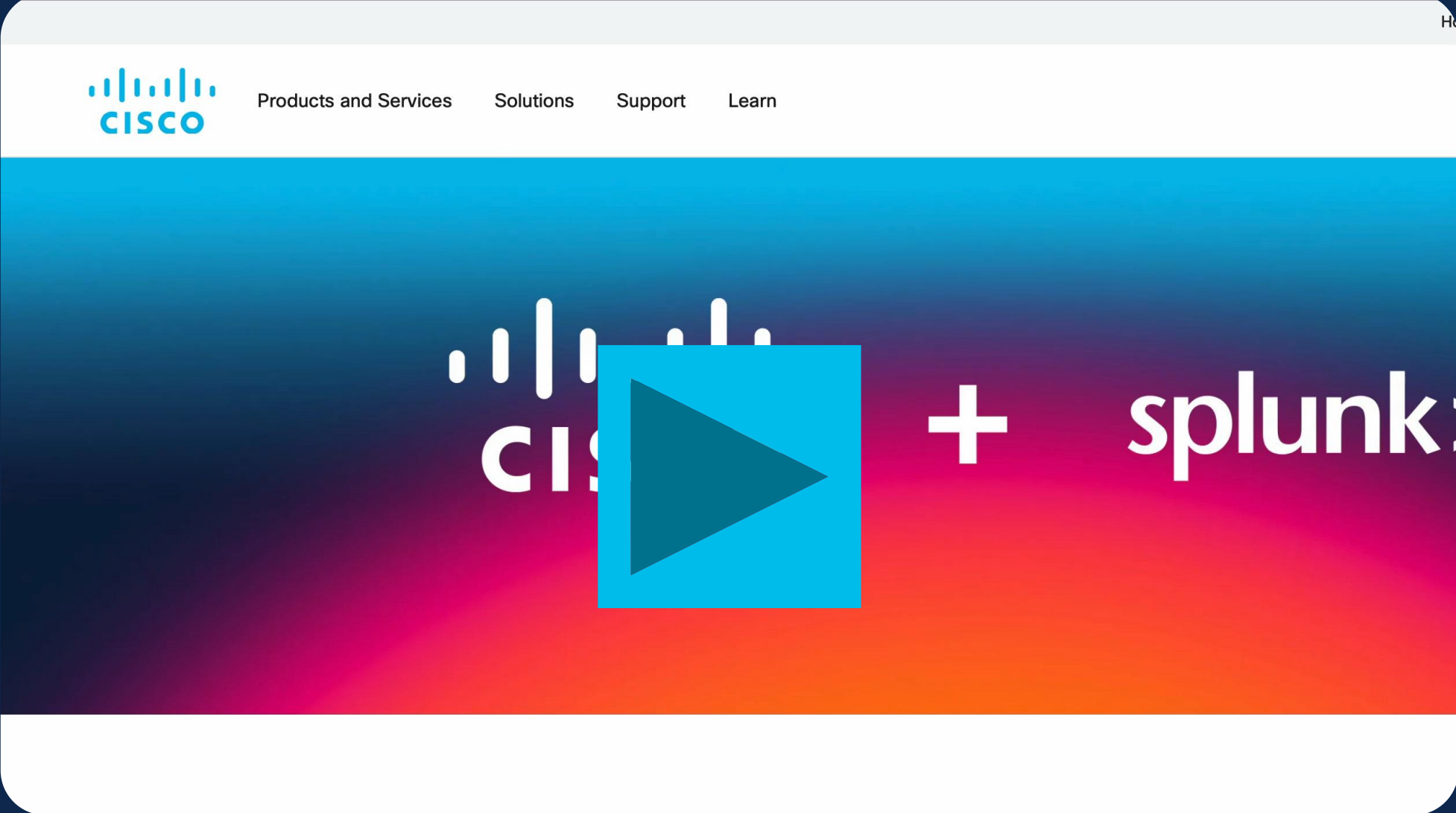


- Welcome Letter siempre a la mano durante la integración (Confidencial)
- Contar con los permisos apropiados en todas las plataformas (SEG / O365 / DNS)
- Recuerda los registros MX
- El servicio de TLS hoy en día se considera por defecto
- Recuerda que en los destination Control se puede ajustar tráfico de correo
- Si no está en la Recipient Address Table, no te abre la puerta
- 2 X 3 (2 en O365 y 3 en Security Email Gateway)

# Configuración para correo saliente (Relay)

- Introducción
- Planteamiento de problema
- Configuración de correo electrónico de entrada
- Configuración de correo electrónico de salida**
- Configuración de DNS
- Probar correo entrada y salida
- Revisión de logs y troubleshooting básico

# Cisco Cloud Security Email Gateway



# Recomendaciones

TAC Tip



1. **Sender Group:** Asegurarse de utilizar/configurar el Listener correcto.
2. **Sender Group:** Utilizar nombre significativo.
3. **Hostname SG:** Usar el wildcard `.protection.outlook.com`

# Microsoft Office 365

Microsoft 365 admin center

Search

Dashboard view Add user Reset password Add team View your bill

Based on manual password resets

### Allow users to reset their own passwords

Reduce support costs by turning on self-service password reset for all users in Azure Active Directory (Azure AD). Users will be prompted to provide alternate contact info so they can reset their own passwords.

Turn this on in Azure AD

Microsoft Teams

### Support remote workers with Teams

Learn how to manage Teams for remote work, with setup guidance, short videos, and tips.

- Teams is on for your organization
- Check setup status for new Teams users
- Guest access is on

User management

### User management

Add, edit, and remove user accounts, and

Add user Edit a user

1

Exchange admin center

Search (Preview)

Home > Connectors

## Connectors

Connectors help control the flow of email messages to and from your Office 365 organization. We recommend that you [check to see if you should create a connector](#), since most organizations don't need to use them.

+ Add a connector Refresh

Status ↑	Name	From	To
----------	------	------	----

Mail flow 1

Connectors 2

3

# Microsoft Office 365

## New connector

1

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.

### Connection from

- Office 365
- Your organization's email server
- Partner organization

### Connection to

- Your organization's email server
- Partner organization

## Use of connector

2

Specify when you want to use this connector.

- Only when I have a transport rule set up that redirects messages to this connector
- Only when email messages are sent to these domains

## Routing

3

How do you want to route email messages?

Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address.

- Use the MX record associated with the partner's domain
- Route email through these smart hosts

2.2.2.2





# Microsoft Office 365

## Security restrictions

1

How should Office 365 connect to your partner organization's email server?

- Always use Transport Layer Security (TLS) to secure the connection (recommended)  
Connect only if the recipient's email server certificate matches this criteria
- Any digital certificate, including self-signed certificates
- Issued by a trusted certificate authority (CA)
  - Add the subject name or subject alternative name (SAN) matches this domain name:  
Example: contoso.com or \*.contoso.com

## Validation email

2

Specify an email address for an active mailbox that's on your partner domain. You can add multiple addresses if your partner organization has more than one domain.

Example: user@contoso.com



jramosba@tacmexesa.com



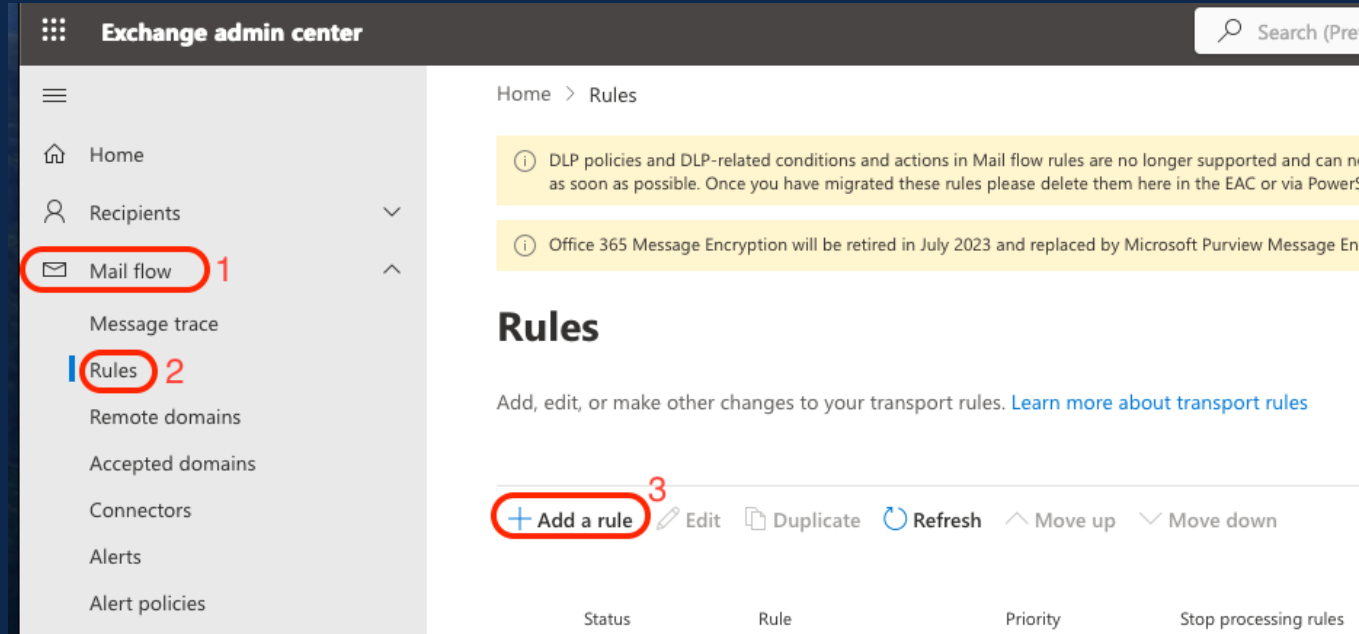
Validate

✓ Validation successful

> Task	Status
> Check connectivity to '216.71.142.67'	Succeed
> Send test email	Succeed

# Microsoft Office 365

## Crear una regla de Flujo de correo



1. Para Aplicar esta regla si... *The sender is located...*
2. Para la ventana emergente, seleccionar la ubicación del remitente como: *Inside the organization*

# Microsoft Office 365

**Name \***

Outbound to Cloud SEG

**Apply this rule if \***

The recipient is external/internal

The recipient is located 'NotInOrganization'

**And**

The sender is external/internal

The sender is located 'InOrganization'

**Do the following \***

Redirect the message to the following connector

route the message using the following connector 'Outbound to Cloud SEG'

**And**

Modify the message properties set a message header

Set the message header 'X-OUTBOUND-AUTH' to the value 'mysecretkey'

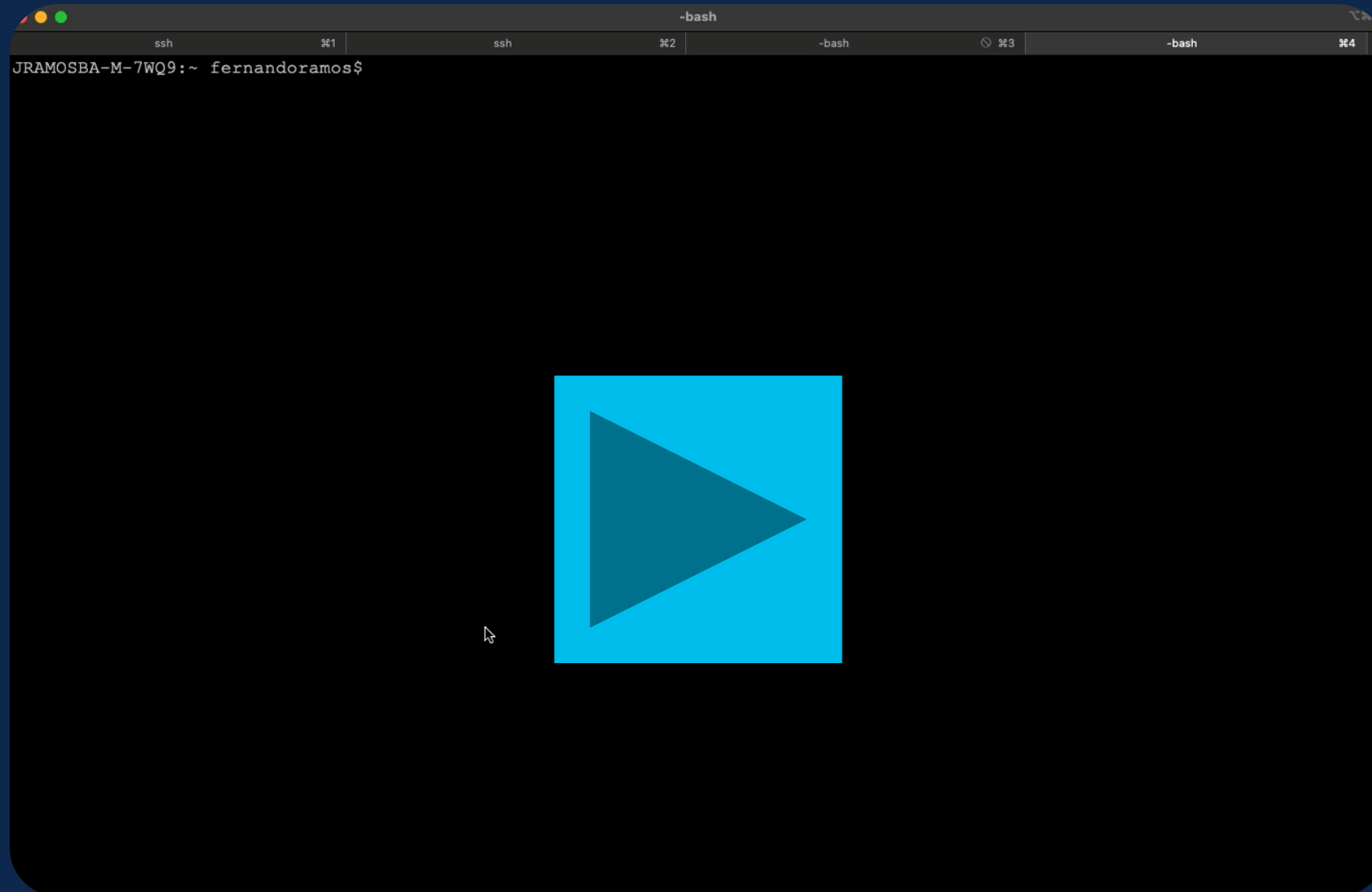
**Except if**

Select one



# Message Filter

TAC Tip



# Recomendaciones

TAC Tip



1. **Conector de O365:** Tener la Welcome Letter
2. **Message Filter:** Acceso al CLI de nuestro Cloud Secure Email Gateway.
3. **Message Filter:** Evitar relay de algún otro Tenant



Join at  
**slido.com**  
**#2154 787**

🔍 Passcode:  
**bwke24**

**¿Qué registro DNS debe de modificarse para redirigir el servicio de correo electrónico?**

a) A record  
 0%

b) TXT record  
 0%

c) MX Record  
 0%

# Configuración de DNS (Records MX)

- Introducción
- Planteamiento de problema
- Configuración de correo electrónico de entrada
- Configuración de correo electrónico de salida
- **Configuración de DNS**
- Probar correo entrada y salida
- Revisión de logs y troubleshooting básico

# DNS

## Your Cisco Cloud Email Security (CES) service is ready!

Organization Name: ██████████  
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. ██████.iphmx.com
- mx2. ██████.iphmx.com

### Your Cisco CES portals:

#### Email Security

https://dh█████-esa1.iphmx.com

#### Security Management

https://dh█████-sma1.iphmx.com

#### End User Quarantine

https://dh█████-euq1.iphmx.com

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█████.iphmx.com

### Include CES host and IP address in your SPF record:

v=spf1 exists:%{i}.spf.hc█████.iphmx.com ~all



# DNS

SuperTool Beta7

tacmexesa.com MX Lookup

**mx:tacmexesa.com** Find Problems Solve Email Delivery Problems mx

[Gmail & Yahoo are now requiring DMARC - Get your's setup with Delivery Center](#)

Pref	Hostname	IP Address	TTL	
10	mx1.hc5588-66.ipmx.com	216.71.150.41 Unknown (AS16417)	30 min	<a href="#">Blacklist Check</a> <a href="#">SMTP Test</a>



Join at  
**slido.com**  
**#2154 787**

🔍 Passcode:  
**bwke24**

**¿Cuál es el nombre de la interfaz que debemos configurar para entrega de nuestro dominio al exterior en el Cloud SEG?**

a) Data1  
 0%

b) Management  
 0%

c) Ob1  
 0%

# Probar correo entrada y salida

- Introducción
- Planteamiento de problema
- Configuración de correo electrónico de entrada
- Configuración de correo electrónico de salida
- Configuración de DNS
- Probar correo entrada y salida**
- Revisión de logs y troubleshooting básico

# Correo de entrada: probando



¡Hola Community Live! • josedav@cisco.com

Enviar Descartar Adjuntar archivo Firma Sensibilidad Editor

El siguiente destinatario no pertenece a tu organización. Jose Davila Quitar


De: Jose Luis Davila Becerril (josedav) (josedav@cisco.com)

Para: Jose Davila CC CCO

Asunto: ¡Hola Community Live! Prioridad

Aptos 11

¡Es un placer saludarlos comunidad Cisco!



Borrador guardado ahora mismo



# Correo de entrada: recibido

Prioritarios Otro

Hoy


**JL** Jose Luis Davila Becerril (josedav)  
¡Hola Community Live! 12:25 a.m.  
¡Es un placer saludarlos comunidad Cisco!

¡Hola Community Live!

Jose Luis Davila Becerril (josedav) <josedav@cisco.com>  
Para Jose Davila

Hoy a las 12:25 a.m.

¡Es un placer saludarlos comunidad Cisco!



# Correo de salida: probando



¡Hola Community Live! - josedavila@tacmexesa.com

Enviar Descartar Adjuntar archivo Firma Sensibilidad Editor

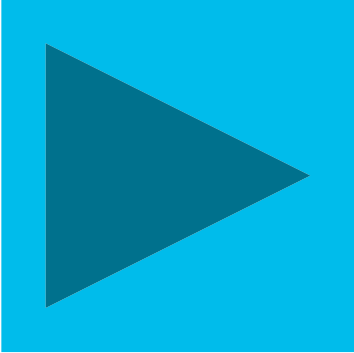
De: Jose Davila (JoseDavila@tacmexesa.com)

Para: josedav@cisco.com

Asunto: ¡Hola Community Live!

Aptos (Cuerpo) 11

¡Es un placer saludarlos!



Borrador guardado ahora mismo

# Correo de salida: Enviado



¡Hola Community Live! - Bandeja de entrada - josedav@cisco.com

Eliminar Archivar Mover Marcar Marcar como no leído Sincronizar Informe

¡Hola Community Live!

JD Jose Davila <JoseDavila@tacmexesa.com> Para Jose Luis Davila Becerril (josedav)

Hoy a las 12:36 a.m.

¡Es un placer saludarlos!

# Revisión de logs y troubleshooting básico

- Introducción
- Planteamiento de problema
- Configuración de correo electrónico de entrada
- Configuración de correo electrónico de salida
- Configuración de DNS
- Probar correo entrada y salida
- Revisión de logs y troubleshooting básico**



# ¿Cómo podemos encontrar eventos de un mensaje?

## Message tracking:

- Obtiene un reporte gráfico sobre el mensaje procesado. Puede consultarse de manera centralizada o local.
- Podemos buscar un mensaje por: fecha, hora, remitente, etcétera, y exportarlos.
- Es la primera opción para confirmar si un mensaje fue procesado por un SEG.

## Logs

- Obtiene detalles específicos sobre el mensaje procesado. Se mantienen por SEG.
- Se encuentran en formato texto y pueden ser buscados con identificadores clave.
- Es la opción que permite un análisis más profundo sobre cómo un mensaje fue procesado.

# ¿Cómo identificar a un mensaje dentro del SEG?

## Identificador de conexión

- Para cada conexión entrante, tendremos un **ICID**
- Para cada conexión saliente, tendremos un **DCID**
- Permiten obtener información de qué sucedió con una conexión, si fue exitosa o fallida.

## Identificador de Mensaje

- Para cada mensaje, tendremos un **MID**
- Permite conocer como fue procesado detalladamente un mensaje en los motores del SEG

# Rastreando un mensaje en Message Tracking

**Message Tracking**

**Search**

Available Time Range: 01 Sep 2021 16:00 to 13 Mar 2024 23:51 (GMT -06:00) Data in time range: 99.32% complete

Envelope Sender: ?	Begins With ▾	<input type="text"/>				
Envelope Recipient: ?	Begins With ▾	<input type="text"/>				
Subject:	Begins With ▾	<input type="text" value="Prueba de correo de salida"/>				
Message Received:	<input checked="" type="radio"/> Last Day <input type="radio"/> Last Week <input type="radio"/> Custom Range					
	Start Date:	Time:	and	End Date:	Time:	(GMT -06:00)
	<input type="text" value="03/12/2024"/>	<input type="text" value="23:00"/>		<input type="text" value="03/13/2024"/>	<input type="text" value="23:52"/>	
<a href="#">Advanced</a>		Search messages using advanced criteria				

# Rastreando un mensaje en Message Tracking

Results				Items per page 20
Displaying 1 — 2 of 2 items.				
1	13 Mar 2024 23:15:20 (GMT -06:00)	MID: 4977607	HOST: esa1.hc5588-66.iphmx.com (216.71.150.41)	Show Details
SENDER: JoseDavila@tacmexesa.com				
RECIPIENT: joseluisdavila90@gmail.com				
SUBJECT: Prueba de correo de salida				
LAST STATE: Message 4977607 to joseluisdavila90@gmail.com received remote SMTP response				
2	13 Mar 2024 23:13:18 (GMT -06:00)	MID: 4977605	HOST: esa1.hc5588-66.iphmx.com (216.71.150.41)	Show Details
SENDER: JoseDavila@tacmexesa.com				
RECIPIENT: josedav@cisco.com				
SUBJECT: Prueba de Correo de Salida				
LAST STATE: Message 4977606 to JoseDavila@tacmexesa.com received remote SMTP response				
Displaying 1 — 2 of 2 items.				

Message Details	
<b>Envelope and Header Summary</b>	
Received Time:	13 Mar 2024 23:15:20 (GMT -06:00)
MID:	4977607
Message Size:	9.54 (KB)
Subject:	Prueba de correo de salida
Envelope Sender:	JoseDavila@tacmexesa.com
Envelope Recipients:	joseluisdavila90@gmail.com
Message ID Header:	<SJ2P222MB0880833B235FB95CD9CD17BEC0292@SJ2P222MB0880.NAMP222.PROD.OUTLOOK.COM>
Cisco IronPort Host:	esa1.hc5588-66.iphmx.com (216.71.150.41)
SMTP Auth User ID:	N/A
Attachments:	N/A
<b>Sending Host Summary</b>	
Reverse DNS Hostname:	mail-dm6nam11lp2169.outbound.protection.outlook.com (verified)
IP Address:	104.47.57.169
SBRS Score:	not enabled

# Rastreando conexiones en los logs del SEG

```
(Machine esa1.hc123.cisco.com) (SERVICE)> grep "ICID 2183260" mail_logs
```

```
Thu Mar 14 00:08:45 2024 Info: New SMTP ICID 2183260 interface Data 1  
(216.71.150.41) address 68.232.145.94 reverse dns host esa2.hc5588-  
66.iphmx.com verified yes
```

```
Thu Mar 14 00:08:45 2024 Info: ICID 2183260 ACCEPT SG UNKNOWNLIST match  
68.232.145.94 SBRS None country United States
```

```
Thu Mar 14 00:08:46 2024 Info: ICID 2183260 TLS success protocol TLSv1.2  
cipher ECDHE-RSA-AES256-GCM-SHA384
```

```
Thu Mar 14 00:08:46 2024 Info: Start MID 4977611 ICID 2183260
```

```
Thu Mar 14 00:08:46 2024 Info: MID 4977611 ICID 2183260 From:  
<josedav@cisco.com>
```

```
Thu Mar 14 00:08:46 2024 Info: MID 4977611 ICID 2183260 RID 0 To:  
<josedavila@tacmexesa.com>
```

```
Thu Mar 14 00:08:51 2024 Info: ICID 2183260 close
```

# Rastreando conexiones en los logs del SEG

```
(Machine esa1.hc123.cisco.com) (SERVICE)> grep "DCID 17422384" mail_logs
```

```
Thu Mar 14 00:08:47 2024 Info: New SMTP DCID 17422384 interface  
216.71.150.41 address 52.101.10.8 port 25
```

```
Thu Mar 14 00:08:47 2024 Info: DCID 17422384 TLS success protocol TLSv1.2  
cipher ECDHE-RSA-AES256-GCM-SHA384
```

```
Thu Mar 14 00:08:49 2024 Info: Delivery start DCID 17422384 MID 4977611 to  
RID [0]
```

```
Thu Mar 14 00:08:51 2024 Info: Message done DCID 17422384 MID 4977611 to  
RID [0] [('from', '"Jose Luis Davila Becerril (josedav)"  
<josedav@cisco.com>'), ('to', '"josedavila@tacmexesa.com"  
<josedavila@tacmexesa.com>')]
```

```
Thu Mar 14 00:08:56 2024 Info: DCID 17422384 close
```

# Rastreando un mensaje en los logs del SEG

```
(Machine esa1.hc123.cisco.com) (SERVICE)> grep "MID 4977612" mail_logs
```

```
Thu Mar 14 00:08:46 2024 Info: Start MID 4977612 ICID 2183260
```

```
Thu Mar 14 00:08:46 2024 Info: MID 4977612 ICID 2183260 From:  
<josedav@cisco.com>
```

```
Thu Mar 14 00:08:46 2024 Info: MID 4977612 SDR: Domains for which SDR is  
requested: reverse DNS host: esa2.hc5588-66.iphmx.com, helo: esa2.hc5588-  
66.iphmx.com, env-from: cisco.com, header-from: Not Present, reply-to: Not  
Present
```

```
Thu Mar 14 00:08:46 2024 Info: MID 4977612 SDR: Consolidated Sender Threat  
Level: Favorable, Threat Category: N/A, Suspected Domain(s) : N/A (other  
reasons for verdict). Sender Maturity: 30 days (or greater) for domain:  
esa2.hc5588-66.iphmx.com
```

```
...
```

```
Thu Mar 14 00:08:49 2024 Info: Message finished MID 4977612 done
```

# Recomendaciones



- Obtén el reporte de *message tracking* para el mensaje que deseas buscar.

Printable (PDF)

Message Details	
<b>Envelope and Header Summary</b>	
Received Time:	18 Mar 2024 21:03:12 (GMT -06:00)
MID:	12463383
Message Size:	13.18 (KB)
Subject:	Hola Community Live 18 de marzo!
Envelope Sender:	josedav@cisco.com
Envelope Recipients:	josedavila@tacmexesa.com
Message ID Header:	<BYAPR11MB29673F8153D559CAB3FE398FA02C2@BYAPR11MB2967.namprd11.prod.outlook.com>
Cisco IronPort Host:	esa2.hc5588-66.iphmx.com (68.232.145.94)
SMTP Auth User ID:	N/A
Attachments:	N/A
<b>Sending Host Summary</b>	
Reverse DNS Hostname:	alln-iport-2.cisco.com (verified)
IP Address:	173.37.142.89
SBRs Score:	3.5
<b>Processing Details</b>	
	MAIL POLICY "tacmexesa" MATCHED THESE RECIPIENTS: josedavila@tacmexesa.com
18 Mar 2024 21:03:12 (GMT -06:00)	Incoming connection (ICID 2677386) has sender_group: UNKNOWNLIST, sender_ip: 173.37.142.89 and sbrs: 3.5
18 Mar 2024 21:03:12 (GMT -06:00)	Protocol SMTP interface Data 1 (IP 68.232.145.94) on incoming connection (ICID 2677386) from sender IP 173.37.142.89. Reverse DNS host alln-iport-2.cisco.com verified yes.
18 Mar 2024 21:03:12 (GMT -06:00)	(ICID 2677386) ACCEPT sender group UNKNOWNLIST match 173.37.142.0/24 SBRs 3.5 sender IP 173.37.142.89 country United States
18 Mar 2024 21:03:12 (GMT -06:00)	Incoming connection (ICID 2677386) successfully accepted TLS protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384.
18 Mar 2024 21:03:12 (GMT -06:00)	Message 12463383 Sender Domain: cisco.com
18 Mar 2024 21:03:12 (GMT -06:00)	Start message 12463383 on incoming connection (ICID 2677386).
18 Mar 2024 21:03:12 (GMT -06:00)	Message 12463383 enqueued on incoming connection (ICID 2677386) from josedav@cisco.com.
18 Mar 2024 21:03:12 (GMT -06:00)	Message 12463383 direction: incoming
18 Mar 2024 21:03:12 (GMT -06:00)	Message 12463383 Domains for which SDR is requested: reverse DNS host: alln-iport-2.cisco.com, helo: alln-iport-2.cisco.com, env-from: cisco.com, header from: Not Present, reply to: Not Present



# Recomendaciones



- Siempre conserva una suscripción de log local.

### Log Subscriptions

Mode —Cluster: Hosted\_Cluster

▸ Centralized Management Options

Last Updated: 19 Mar 2024 22:52 (GMT -06:00)

#### Configured Log Subscriptions

Add Log Subscription...

Log Settings	Type ▲	Rollover Interval
Performance	Performance Logs	None
amp	AMP Engine Logs	None

1

Retrieval Method:	<input checked="" type="radio"/> Manually download logs from esa1.hc5588-66.iphmx.com <i>Logs are always available via HTTP(S) download. They are also available via SCP if SSH is enabled and FTP if it is enabled on any Interface.</i>
	Maximum Files: <input type="text" value="10"/> <i>The maximum number of files retained on the appliance.</i>

2

# Recomendaciones

TAC Tip



- Consulta los logs tan pronto como sea posible.

```
esa2.hc123.iphmx.com (SERVICE)> grep "Mar 19 11:11" mail_logs
```

```
Tue Mar 19 11:11:32 2024 Info: New SMTP DCID 8331163 interface 68.232.145.94  
address 68.232.130.237 port 7025
```

```
Tue Mar 19 11:11:32 2024 Info: DCID 8331163 TLS success protocol TLSv1.2  
cipher ECDHE-RSA-AES256-GCM-SHA384 the.cpq.host
```

```
Tue Mar 19 11:11:34 2024 Info: New SMTP ICID 2678183 interface Data 1  
(68.232.145.94) address 136.143.176.50 reverse dns host unknown verified no
```

```
Tue Mar 19 11:11:34 2024 Info: ICID 2678183 ACCEPT SG None match ALL SBRS 2.5  
country United States
```

```
Tue Mar 19 11:11:34 2024 Info: ICID 2678183 lost
```

```
Tue Mar 19 11:11:34 2024 Info: ICID 2678183 close
```

# Recomendaciones

TAC Tip



- Observa el código resultante de la entrega del correo electrónico de salida.

```
Mon Mar 18 20:56:47 2024 Info: Bounced: DCID 8330333 MID 12463381 to RID 0 -  
Bounced by destination server with response: 5.3.0 - Other mail system  
problem ('554', ['Too many hops']) [('from', '"Jose Luis Davila Becerril  
(josedav)" <josedav@cisco.com>'), ('to', 'Jose Davila  
<josedavila@tacmexesa.com>')]
```

# Recomendaciones

TAC Tip



- Cambia los logs a modo debug.

**Log Subscriptions** 1

Mode —Cluster: Hosted\_Cluster

▸ Centralized Management Options

Last Updated: 19 Mar 2024 22:52 (GMT -06:00)

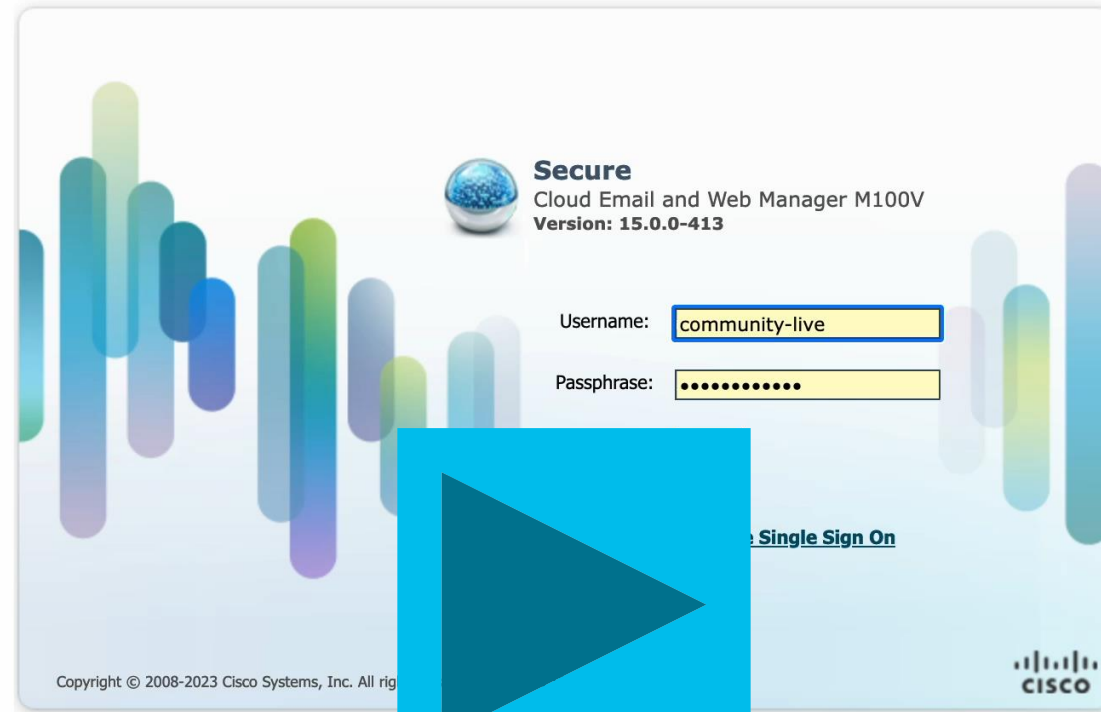
**Configured Log Subscriptions**

Add Log Subscription...

Log Settings	Type ▲	Rollover Interval
Performance	Performance Logs	None
amp	AMP Engine Logs	None

**Log Level:** 2

- Critical (The least detailed setting. Only errors are logged.)
- Warning (All errors and warnings created by the system.)
- Information (Captures the second-by-second operations of the system. Recommended.)
- Debug (More specific data are logged to help debug specific problems.)
- Trace (The most detailed setting, all information that can be is logged. Recommended for developers only.)



**Secure**  
Cloud Email and Web Manager M100V  
Version: 15.0.0-413

Username:

Passphrase:

[Single Sign On](#)

Copyright © 2008-2023 Cisco Systems, Inc. All rights reserved. CISCO

The login page features a decorative background of vertical bars in various shades of blue and green. A large blue play button icon is overlaid on the bottom center of the page. The Cisco logo is located in the bottom right corner of the login area.



Your Cisco Secure Email Cloud Gateway is using the port(s) 3268 or 389 for LDAP communication. By default, there is no security provision for these ports, making you vulnerable to man-in-the-middle attacks.

Cisco will be closing and blocking these ports (3268 and 389) as of 2023-07-25 (July 25th, 2023), so you must work to ensure that Secure LDAP (LDAPS) is configured within your LDAP environment and that you modify the LDAP configuration on your Secure Email Cloud Gateway to instead use port 3269 (for AD) or 636 (for OpenLDAP). If these ports are not changed by July 25th, 2023, then there may be an impact on your email flow and additional settings and services.

Here is a resource that you can use as a guide for performing this change: <https://docs.ces.cisco.com/docs/non-secure-ldap>

NOTE: This session will expire if left idle for 30 minutes. Any uncommitted configuration changes will be lost. Commit the configuration changes as soon as they are made.

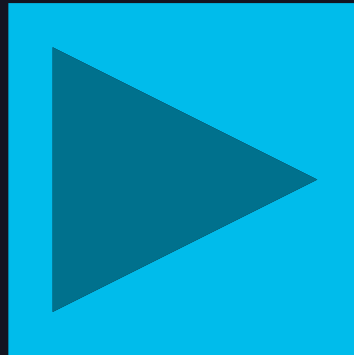
### Warning!

You are currently using a demonstration certificate(Cisco ESA Certificate) which is not secure and is not recommended for general use. Create or import a certificate using the `certconfig > CERTIFICATE` option.

The features/services that are currently using the demonstration certificate are:

listener 'OutgoingMail'

(Machine esa1.hc5588-66.iphmx.com) (SERVICE)> █



MS

## Mail Delivery System

Delivery Status Notification (Failure)

Para: [josedav@cisco.com](mailto:josedav@cisco.com)



The following message to [<josedavila@tacmexesa.com>](mailto:josedavila@tacmexesa.com) was undeliverable.

The reason for the problem:

5.1.0 - Unknown address error 550-'#5.1.0 Address rejected.'

Reporting-MTA: dns; [alln-iport-2.cisco.com](mailto:alln-iport-2.cisco.com)

Final-Recipient: rfc822;[josedavila@tacmexesa.com](mailto:josedavila@tacmexesa.com)

Action: failed

Status: 5.0.0 (permanent failure)

Remote-MTA: dns; [68.232.145.94]

Diagnostic-Code: smtp; 5.1.0 - Unknown address error 550-'#5.1.0 Address rejected.' (delivery attempts: 0)

De: "Jose Luis Davila Becerril (josedav)" [<josedav@cisco.com>](mailto:josedav@cisco.com)

Asunto: **Hola Community Live !**

Fecha: 18 de marzo de 2024, 5:46:29 p.m. GMT-6

Para: Jose Davila [<josedavila@tacmexesa.com>](mailto:josedavila@tacmexesa.com)



```
(Machine esa1.hc5588-66.iphmx.com) (SERVICE)> grep "MID 4977676" mail_logs
```

```
Mon Mar 18 02:02:06 2024 Info: Start MID 4977676 ICID 2190106
```

```
Mon Mar 18 02:02:06 2024 Info: MID 4977676 ICID 2190106 From: <josedav@cisco.com>
```

```
Mon Mar 18 02:02:06 2024 Info: MID 4977676 SDR: Domains for which SDR is requested: reverse DNS host: alln-iport-5.cisco.com, helo: alln-iport-5.cisco.com, env-from: cisco.com, header-from: Not Present, reply-to: Not Present
```

```
Mon Mar 18 02:02:06 2024 Info: MID 4977676 SDR: Consolidated SDR Level: Favorable, Threat Category: N/A, Suspected Domain (s) : N/A (other reasons for verdict). Sender Maturity: 3 ( ) for domain: alln-iport-5.cisco.com
```

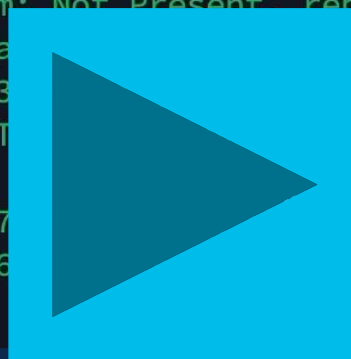
```
Mon Mar 18 02:02:06 2024 Info: MID 4977676 ICID 2190106 T (esa.com) Rejected by RAT
```

```
Mon Mar 18 02:02:06 2024 Info: MID 4977676 Subject ""
```

```
Mon Mar 18 02:02:06 2024 Info: Message aborted MID 4977676 d by sender
```

```
Mon Mar 18 02:02:06 2024 Info: Message finished MID 4977676
```

```
(Machine esa1.hc5588-66.iphmx.com) (SERVICE)> █
```





No Changes Pending

### My Dashboard

Printable PDF

Attention — ⚠ You can customize this "My Dashboard" page by adding report modules from different reports. Some modules are added for you by default. The Overview page can be accessed from Monitor > Overview.

Mode —Machine: esa1.hc5588-66.ipmx.com

Change Mode...

Centralized Management Options

#### System Overview

Overview > Status <input checked="" type="checkbox"/>	Overview > Quarantines - Top 3 by Disk Usage (Policy and Virus) <input checked="" type="checkbox"/>	Overview > Threat Level <input checked="" type="checkbox"/>
<p>System Status: Online</p> <p>Incoming Messages per hour: 0</p> <p>Messages in Work Queue: 0</p>	<p>Centralized Services are enabled (For Policy, Virus and Outbreak Quarantines). Please see details at SMA 68.232.130.237.</p>	<p>Centralized Services are enabled (For Policy, Virus and Outbreak Quarantines). Please see details at SMA 68.232.130.237.</p>
System Status Details	Local Quarantines	Outbreak Details

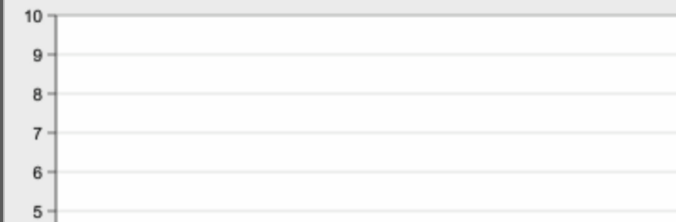
General No modules currently selected for this section.

Time Range: Day

19 Mar 2024 01:00 to 20 Mar 2024 01:54 (GMT -06:00)

Data in time range: 99.93 % complete

#### Overview > Incoming Mail Graph



#### Overview > Incoming Mail Summary

Message Category	%	Messages
Stopped by IP Reputation Filtering	66.7%	10
Stopped by Domain Reputation Filtering	0.0%	0
Stopped as Invalid Recipients	0.0%	0
Spam Detected	0.0%	0

How-To's



Mon Mar 18 18:22:22 2024 Info: MID 4977776 ICID 2191303 From: <joseluisdavila90@gmail.com>  
Mon Mar 18 18:22:22 2024 Info: MID 4977776 SDR: Domains for which SDR is requested: reverse DNS host: esa1.hc5588-66.iphmx.com, hel  
o: esa1.hc5588-66.iphmx.com, env-from: gmail.com, header-from: Not Present, reply-to: Not Present  
Mon Mar 18 18:22:22 2024 Info: MID 4977776 SDR: Consolidated Sender Threat Level: Favorable, Threat Category: N/A, Suspected Domain  
(s) : N/A (other reasons for verdict). Sender Maturity: 30 days (or greater) for domain: esa1.hc5588-66.iphmx.com  
Mon Mar 18 18:22:22 2024 Info: MID 4977776 ICID 2191303 RID 0 To: <josedavila@tacmexesa.com>  
Mon Mar 18 18:22:22 2024 Info: MID 4977776 using engine: SPF Verdict Cache using cached verdict  
Mon Mar 18 18:22:22 2024 Info: MID 4977776 SPF: mailfrom identity joseluisdavila90@gmail.com SoftFail (v=spf1)  
Mon Mar 18 18:22:22 2024 Info: MID 4977776 DKIM: permfail body hash did not verify [final] (d=gmail.com s=20230601 i=@gmail.com)  
Mon Mar 18 18:22:22 2024 Info: MID 4977776 DMARC: Message from domain gmail.com, DMARC fail, (SPF aligned False, DKIM aligned False  
) DMARC policy is none, applied policy is none  
Mon Mar 18 18:22:22 2024 Info: MID 4977776 DMARC: Verification failed.  
Mon Mar 18 18:22:22 2024 Info: MID 4977776 DMARC: No action taken by DMARC policy.  
Mon Mar 18 18:22:22 2024 Info: MID 4977776 Message-ID '<1C5DCFDf-E14F-4B2E-9BD5-F0B79BF46031@gmail.com>'  
Mon Mar 18 18:22:22 2024 Info: MID 4977776 Subject "Hola Community Live! "  
Mon Mar 18 18:22:22 2024 Info: MID 4977776 SDR: Domains for which SDR is requested: reverse DNS host: esa1.hc5588-66.iphmx.com, hel  
o: esa1.hc5588-66.iphmx.com, env-from: gmail.com, header- [REDACTED] reply-to: Not Present  
Mon Mar 18 18:22:22 2024 Info: MID 4977776 SDR: Consolidated Sender Threat Level: Favorable, Threat Category: N/A, Suspected Domain  
(s) : N/A (other reasons for verdict). Sender Maturity: 30 days (or greater) for domain: esa1.hc5588-66.iphmx.com  
Mon Mar 18 18:22:22 2024 Info: MID 4977776 SDR: Tracker Hash: nPUn1Pa3W0QgZ/ZRNyXL+r/JZp9jKiaCR67EUR5l9FJnnZiutL1hrp/h  
2MaLkk7167foXkCwSvTDEXsoj2w9A==  
Mon Mar 18 18:22:22 2024 Info: MID 4977776 ready 391664 b [REDACTED] sdavila90@gmail.com>  
Mon Mar 18 18:22:22 2024 Info: MID 4977776 matched all re [REDACTED] ecipient policy tacmexesa in the inbound table  
Mon Mar 18 18:22:22 2024 Info: MID 4977776 interim graymail (0) <Clean message>  
Mon Mar 18 18:22:23 2024 Info: MID 4977776 interim verdict using engine: CASE negative  
Mon Mar 18 18:22:23 2024 Info: MID 4977776 using engine: CASE spam negative  
Mon Mar 18 18:22:23 2024 Info: MID 4977776 interim AV verdict using McAfee CLEAN  
Mon Mar 18 18:22:23 2024 Info: MID 4977776 interim AV verdict using Sophos CLEAN  
Mon Mar 18 18:22:23 2024 Info: MID 4977776 antivirus negative  
Mon Mar 18 18:22:23 2024 Info: MID 4977776 AMP file reputation verdict : SKIPPED (no attachment in message)  
Mon Mar 18 18:22:23 2024 Info: MID 4977776 using engine: GRAYMAIL negative  
Mon Mar 18 18:22:23 2024 Info: MID 4977776 Outbreak Filters: verdict positive  
Mon Mar 18 18:22:23 2024 Info: MID 4977776 Threat Level=1 Category=Phish Type=Phish  
Mon Mar 18 18:22:23 2024 Info: MID 4977776 queued for delivery

No Changes Pending

## Add SMTP Route

Mode —Group: F4\_Group Change Mode...

Centralized Management Options

### SMTP Route Settings

Receiving Domain: ?	<input type="text"/>		
Destination Hosts:	Priority ?	Destination ?	Port
	<input type="text" value="0"/>	<input type="text"/>	<input type="text" value="25"/>
		<small>(Hostname, IPv4 or IPv6 address.)</small>	
Outgoing SMTP Authentication:	No outgoing SMTP authentication profiles are configured.		

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

Cancel

Submit





*“El éxito es la suma de pequeños esfuerzos repetidos día tras día”*

---

Robert Collier

Autor estadounidense

# Q&A

# Es el evento virtual definitivo para estudiantes de tecnología de todo el mundo. ¡Y es gratis!

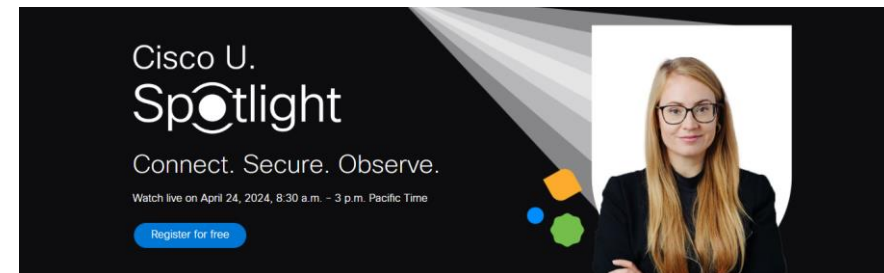
Únase a nosotros para nuestra primera transmisión en vivo de Cisco U.

Miércoles 24 de abril 2024 (\*sesiones en inglés)

Estamos trayendo la luz sobre los temas y las tecnologías más importantes -desde los fundamentos y las mejores prácticas, hasta las habilidades especializadas- mismas que generan las principales tendencias e innovaciones actuales. Entérese de las más recientes estrategias y tecnologías para conectar, proteger y observar los entornos de red más complejos hoy en día.

Explore más de 25 sesiones dirigidas por técnicos, líderes de la industria y expertos de Cisco o tecnologías adyacentes, y sumérjase en conferencias, talleres prácticos, presentaciones a nivel experto ¡o las tres cosas!

Aprenda hoy, lidere mañana. Desarrolle las habilidades para avanzar, destacarse y generar la próxima innovación para su organización.



Take a sneak peek at our lineup

**CONNECT**

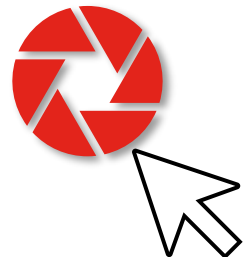
- Hands-on Meraki Action Batches
- Reverse Engineering the Cloud: Making HCL from Click-Ops
- Harnessing the Power of APIs in Artificial Intelligence
- THE Coolest Cloud-native DevOps Tools

**SECURE**

- How Confident Are You in Your WLAN's Security?
- Extended Detection and Response (XDR) Primer
- Multicloud Defense - Secure Your AWS Infra by Taking Those Few Steps
- Securing ASA Syslog

**OBSERVE**

- OSPF Neighbor Troubleshooting Practice
- Deploy a ThousandEyes Enterprise Agent
- Implement Streaming Telemetry with Cisco IOS XE
- Pathways to CCDE



Why attend

The more you learn, the more you and your organization can do. Amp up your tech knowledge and unlock the transformative power of disruptive technologies. We'll light the way and show you and your IT team what's possible when you can connect, secure, and observe the network.

Who should attend

Cisco U. Spotlight offers something for everyone. Whether you're an individual or team lead, these sessions can help you or your team thrive in current roles, increase scalability, and innovate faster. From our targeted classroom sessions focused on helping you understand the current landscape of technology and tools, to our hands-on sessions delivering practical experience, this event will be a game changer for





## ¿Aún tiene dudas?

Si hizo una pregunta en el panel de preguntas y respuestas o regresa a la comunidad en los días posteriores a nuestro webinar ¡Nuestros expertos aún pueden ayudarlo!

Participe en el foro Ask Me Anything (AMA) antes del viernes 5 de abril de 2024

<https://bit.ly/CL3ama-mar24>



## Haga valer su opinión

Responda a nuestra encuesta para...

- Sugerir nuevos temas
- Calificar a nuestros expertos y el contenido
- Enviar sus comentarios o sugerencias

**¡Ayúdenos respondiendo a 5 preguntas de opción múltiple!**

Al término de esta sesión, se abrirá una encuesta en su navegador.





# Nuestras Redes Sociales

LinkedIn  
[Cisco Community](#)

Twitter  
[@CiscoCommunity](#)

YouTube  
[CiscoCommunity](#)

Facebook  
[CiscoCommunity](#)





The bridge to possible