Integración Cisco Cloud SEG con Office 365

Comunidad de Cisco

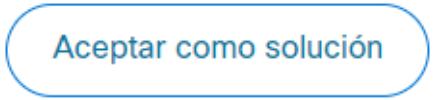
Fernando Ramos – Technical Consulting Engineer
Jesús Sánchez – Technical Consulting Engineer
José Luis Dávila – Technical Consulting Engineer

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.



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!

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

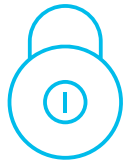
Join at

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

Active poll

0

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

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 prerrequisitos 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)

TAC Tip

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

Organization Name: [redacted]
Start Date: 2022-09-09 05:09:04 America/Los_Angeles

Below you will find information about your login credentials and other important information regar ding your CES. Please retain this email for future reference

MX Records for inbound email from Internet

- mx1.[redacted].iphmx.com
- mx2.[redacted].iphmx.com

Your Cisco CES portals:

Email Security
https://dh[redacted]-esa1.iphmx.com
Security Management
https://dh[redacted]-sma1.iphmx.com
End User Quarantine
https://dh[redacted]-euq1.iphmx.com

Please sign in the portals with this user ID:

Username: [redacted]
Password: [redacted]
Note: We recommend changing your password after the initial login.

Hostname and IP addresses to be whitelisted(for Microsoft/Office365 and G-Suite u sers):

Email Security:
[redacted].140.105
[redacted].150.143
[redacted].143.186
[redacted].32.98
Security Management:
[redacted].157.91

If you are using a Cloud service such as Office365, G-Suite, etc., you should direct your o utbound emails to the address below to have them scanned by Cisco Cloud Email Securit y:

Host and IP address used for outbound relay from Office365 and G-Suite:
ob1.hc[redacted].iphmx.com

Include CES host and IP address in your SPF record:

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

TAC Tip

```
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

Pasos a realizar en Microsoft Office 365

1. Crear Regla
2. Crear Conector

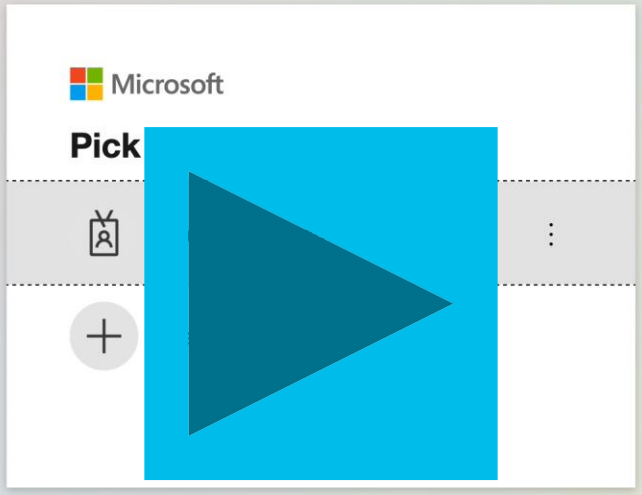
Firefox File Edit View History Bookmarks Tools Window Help

Wed 20 Mar 7:55 a.m.

Sign in to your account

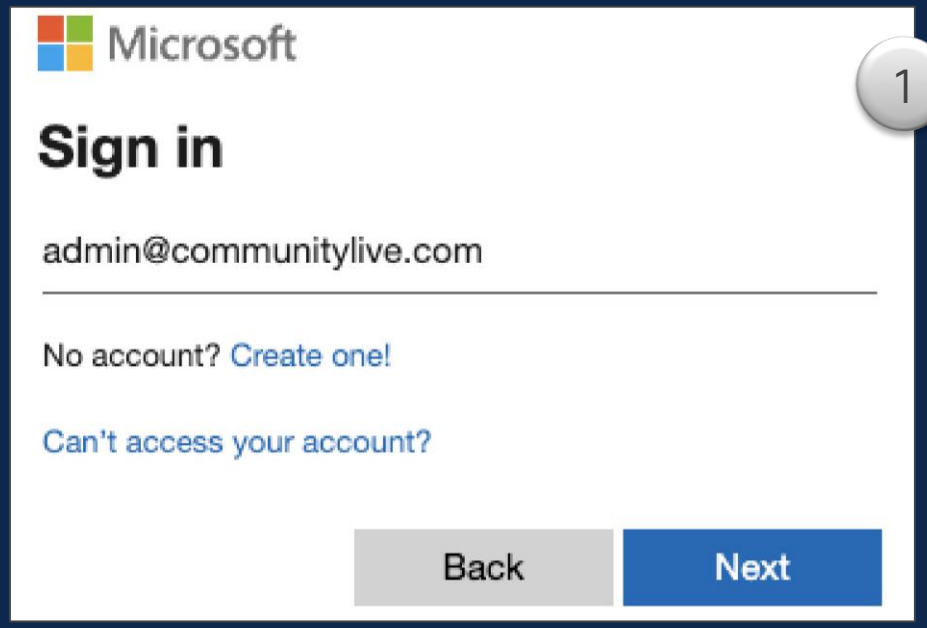
https://login.microsoftonline.com/common/oauth2/authorize?client_id=497effe9-df71-4043-a8bb-14cf78c4b63b&response_ 110%

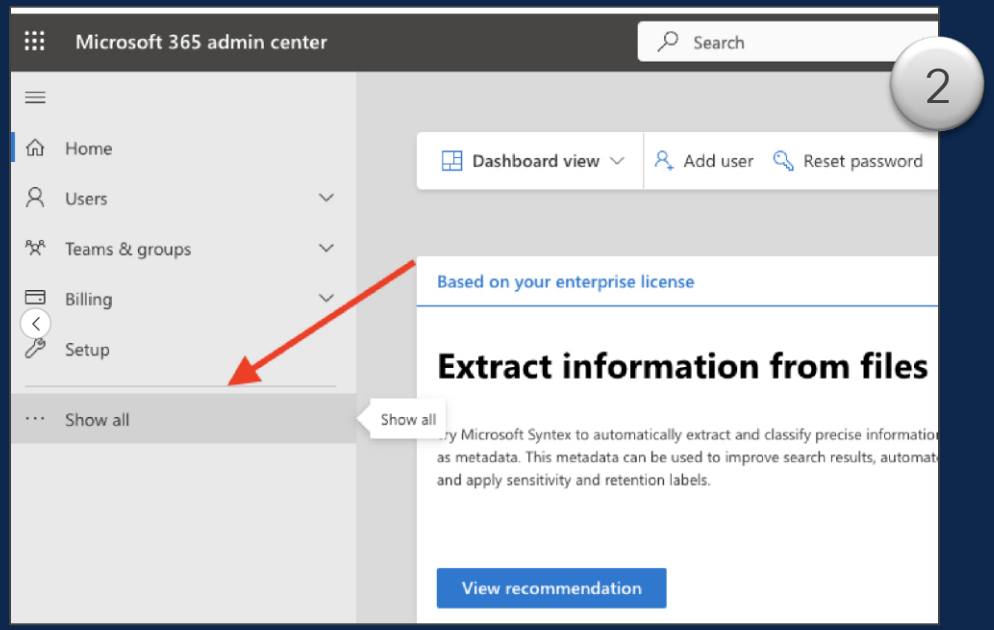
Employee Connecti... Help Zone eStore SAML SSO External ... Thank you for using... ATLAS - Login USA Cloud Email Securit... AGARI: Login CES-LAB trading Global Bootcamp(s) Other Bookmarks

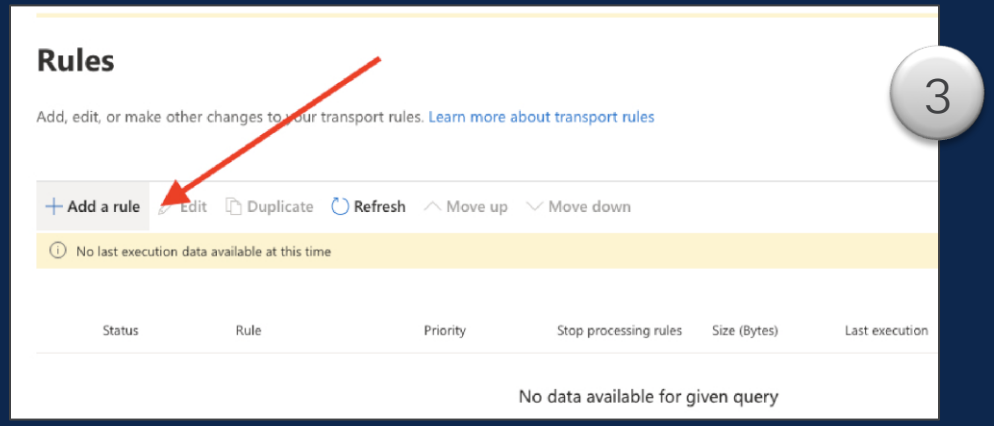


Terms of use Privacy & cookies ...

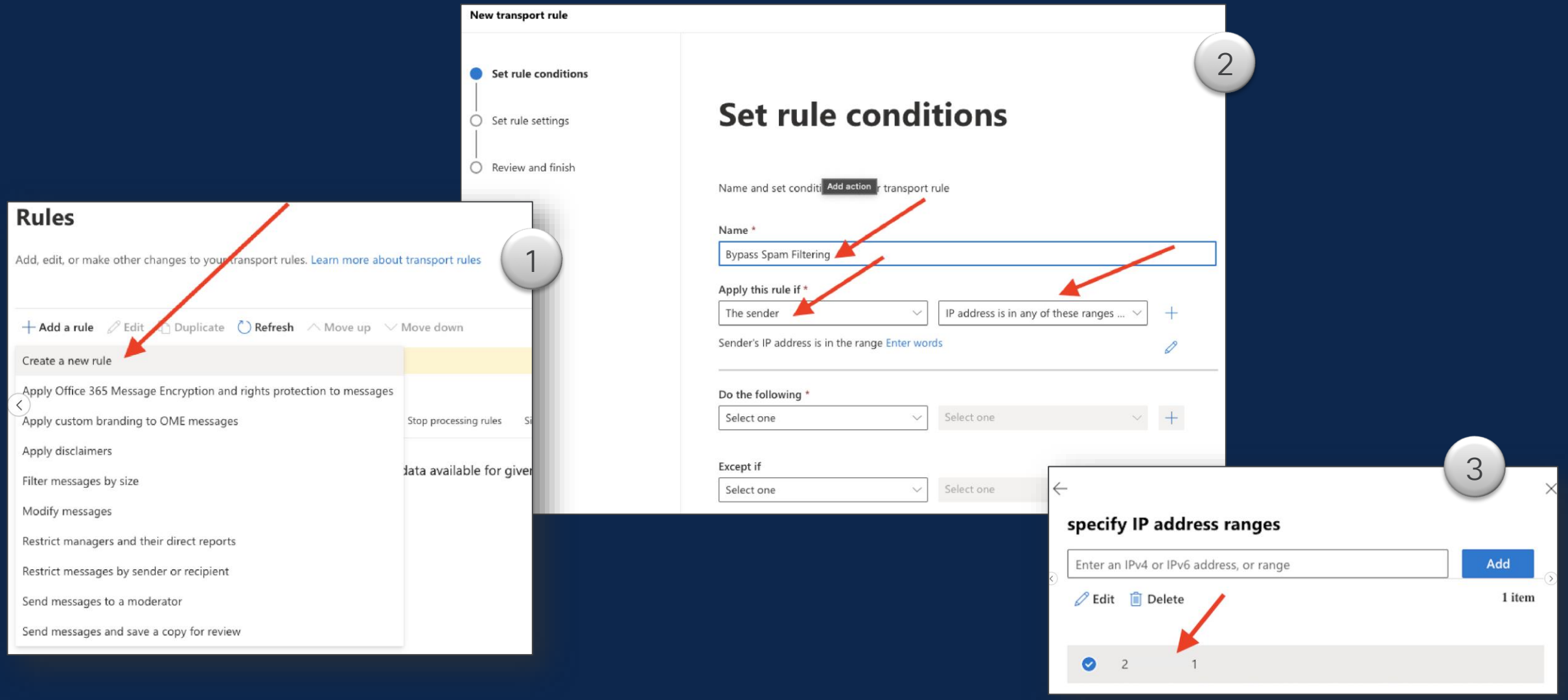
Microsoft Office 365



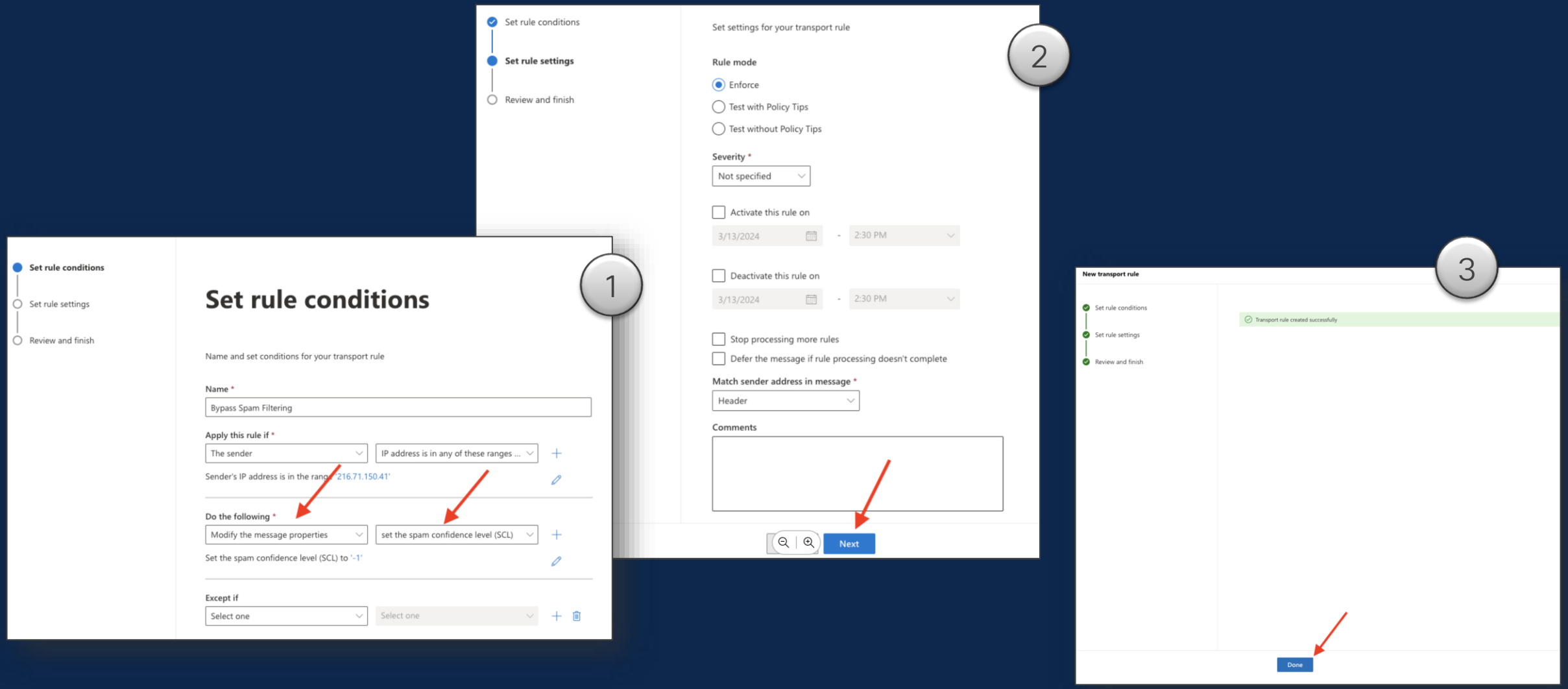




Microsoft Office 365 – Regla



Microsoft Office 365 – Regla



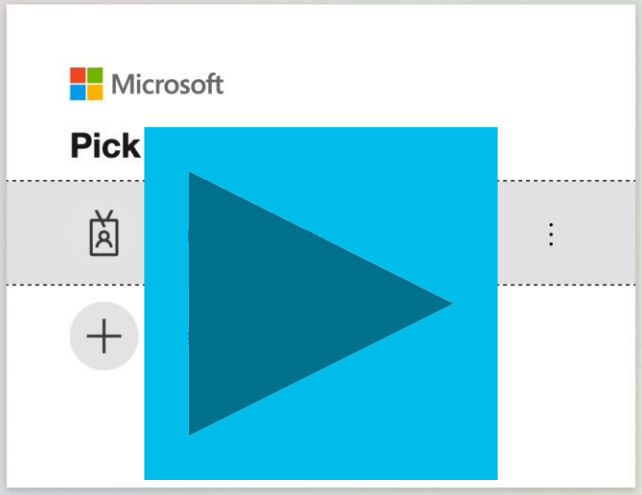
Firefox File Edit View History Bookmarks Tools Window Help

Wed 20 Mar 8:20 a.m.

Sign in to your account

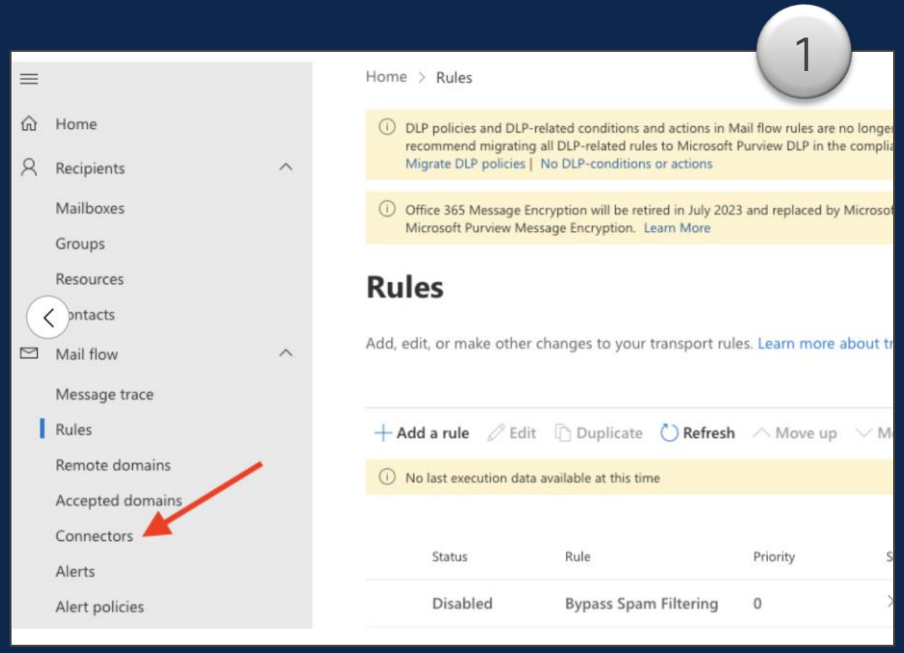
https://login.microsoftonline.com/common/oauth2/authorize?client_id=497effe9-df71-4043-a8bb-14cf78c4b63b&response_ 110%

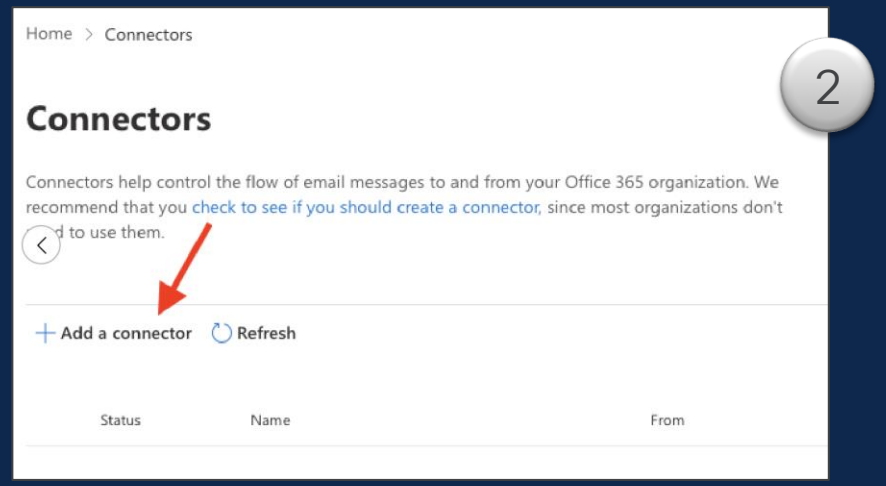
Employee Connecti... Help Zone eStore SAML SSO External ... Thank you for using... ATLAS - Login USA Cloud Email Securit... AGARI: Login CES-LAB trading Global Bootcamp(s) Other Bookmarks

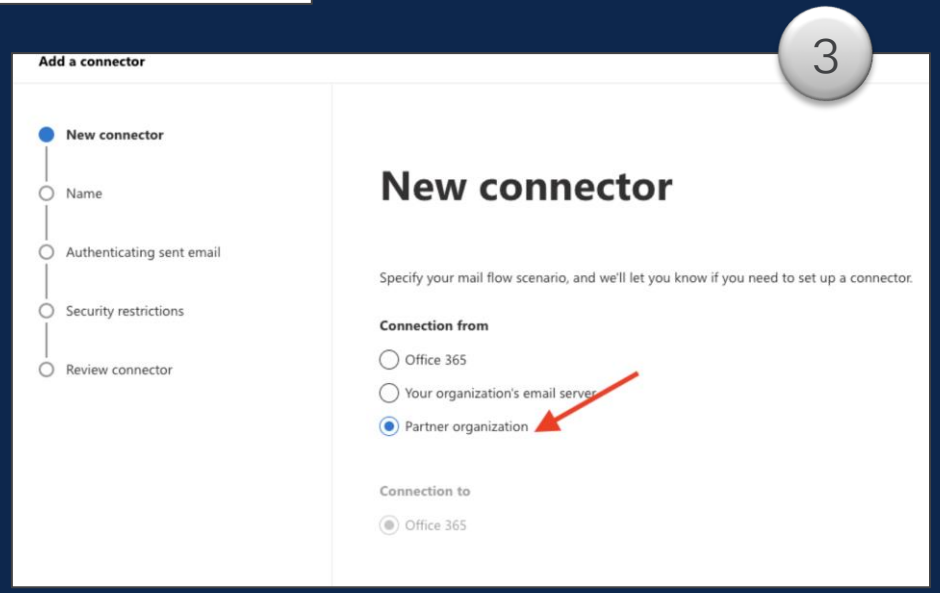


Terms of use Privacy & cookies ...

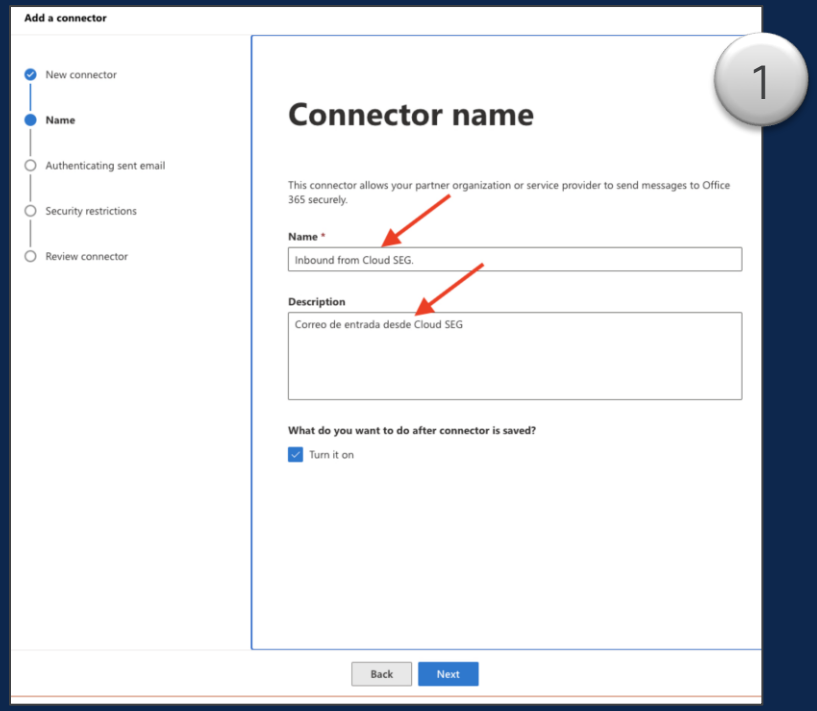
Microsoft Office 365 – Connector

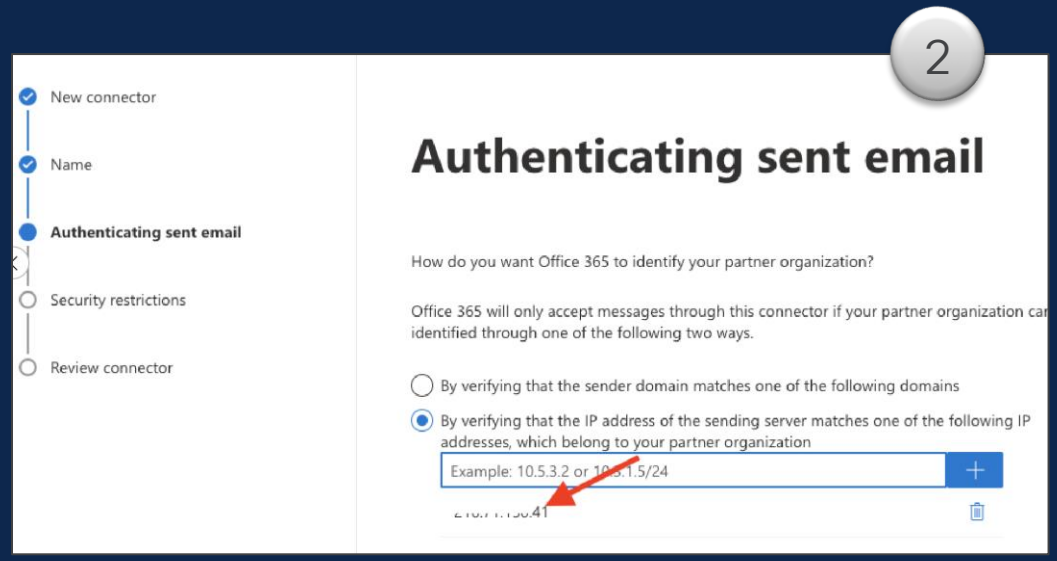


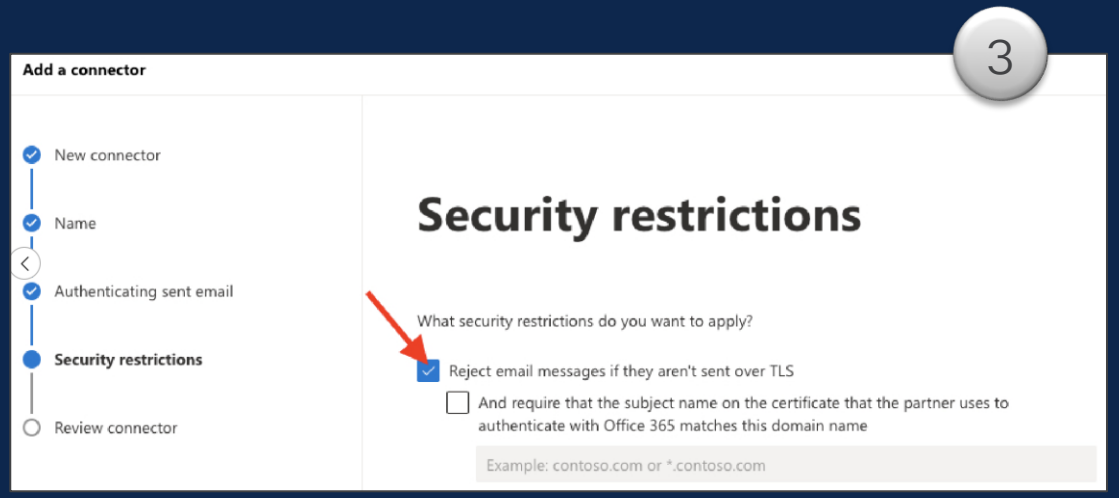




Microsoft Office 365 – Connector

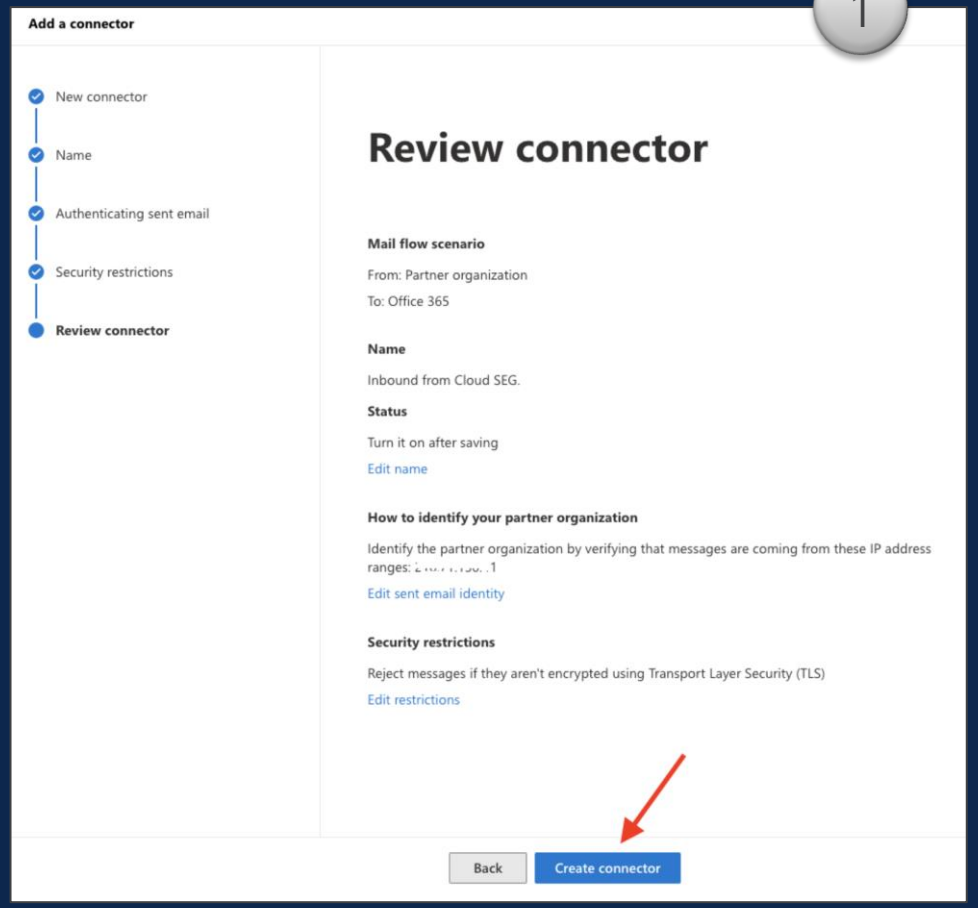




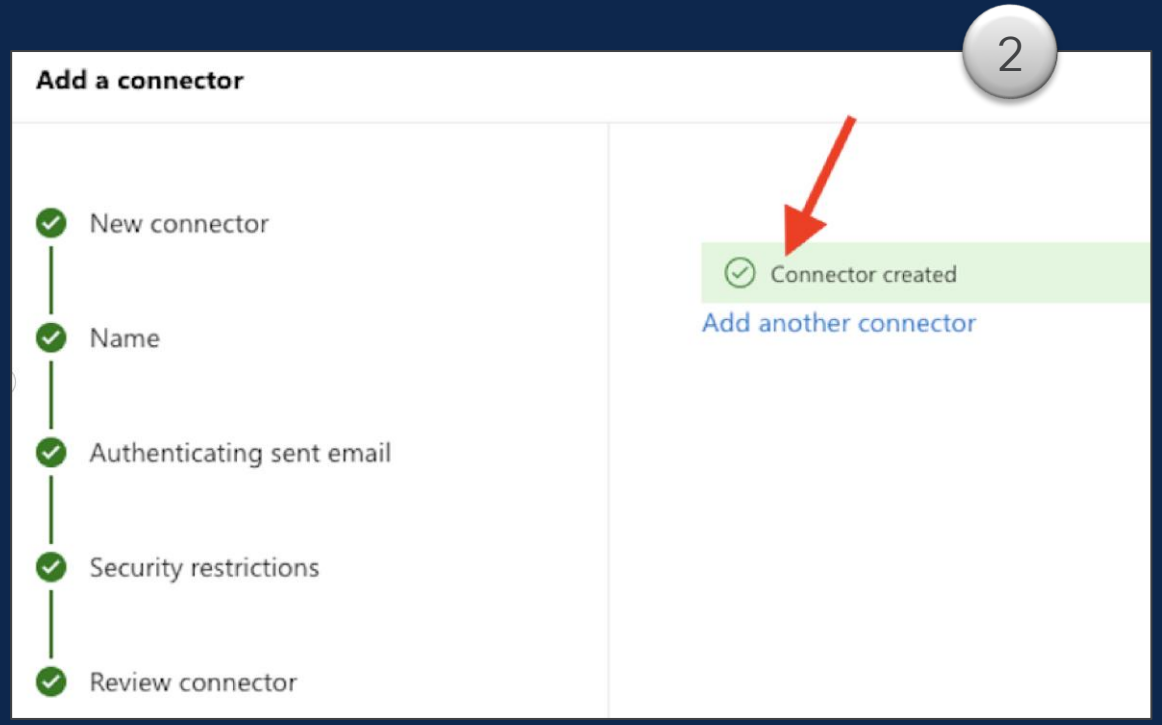


Microsoft Office 365 – Connector

1



2



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

Firefox File Edit View History Bookmarks Tools Window Help — Wed 20 Mar 8:38 a.m.

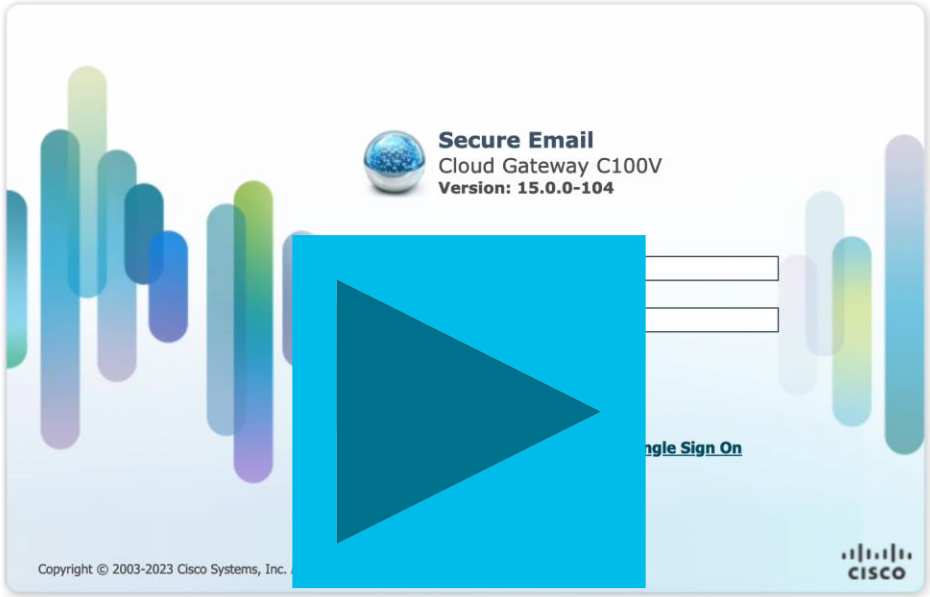
Exchange admin center | Cisco Cloud Gateway C100V (d

https://dh5560-esa1.iphmx.com/login — 110%

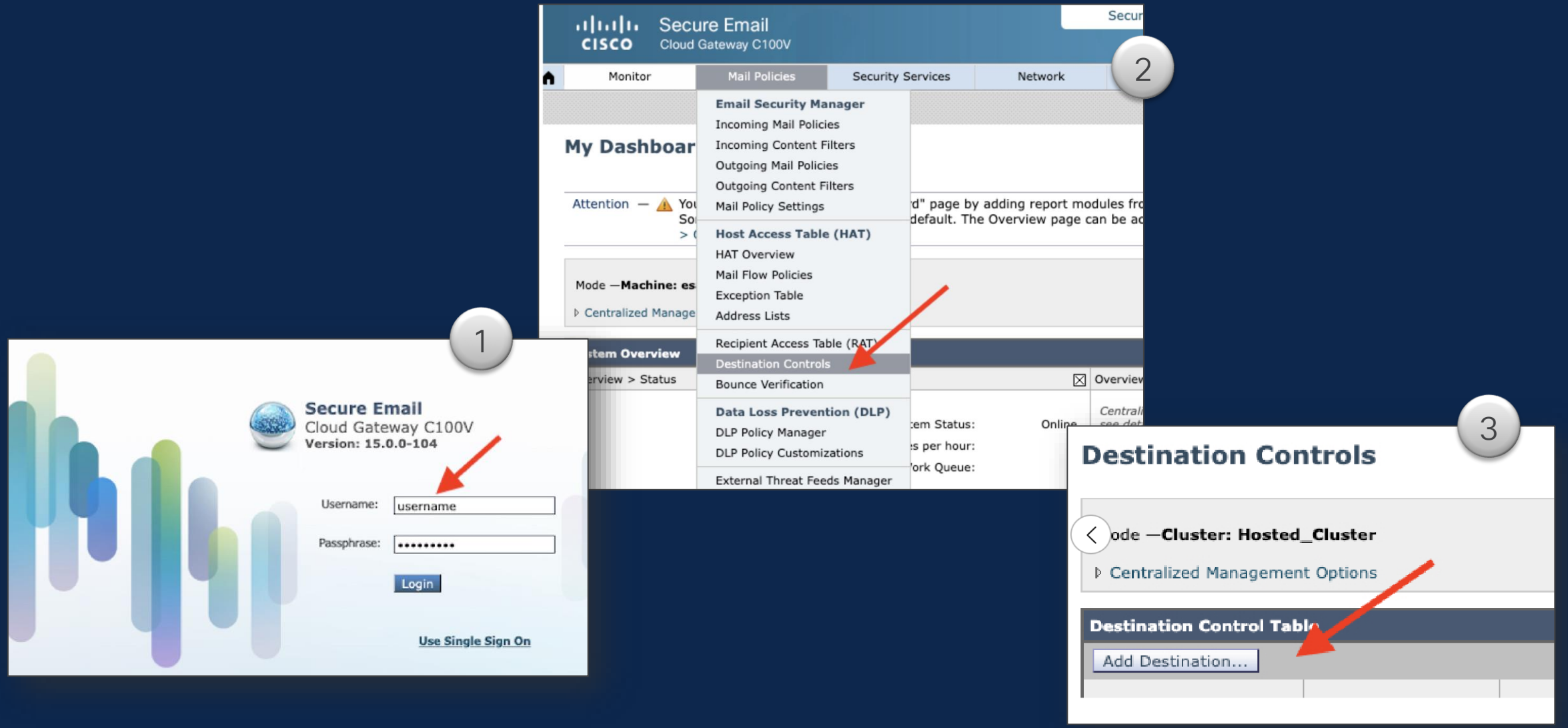
Employee Connecti... | Help Zone | eStore | SAML SSO External ... | Thank you for using... | ATLAS - Login USA | Cloud Email Securit... | AGARI: Login | CES-LAB | trading | Global Bootcamp(s) | Other Bookmarks

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

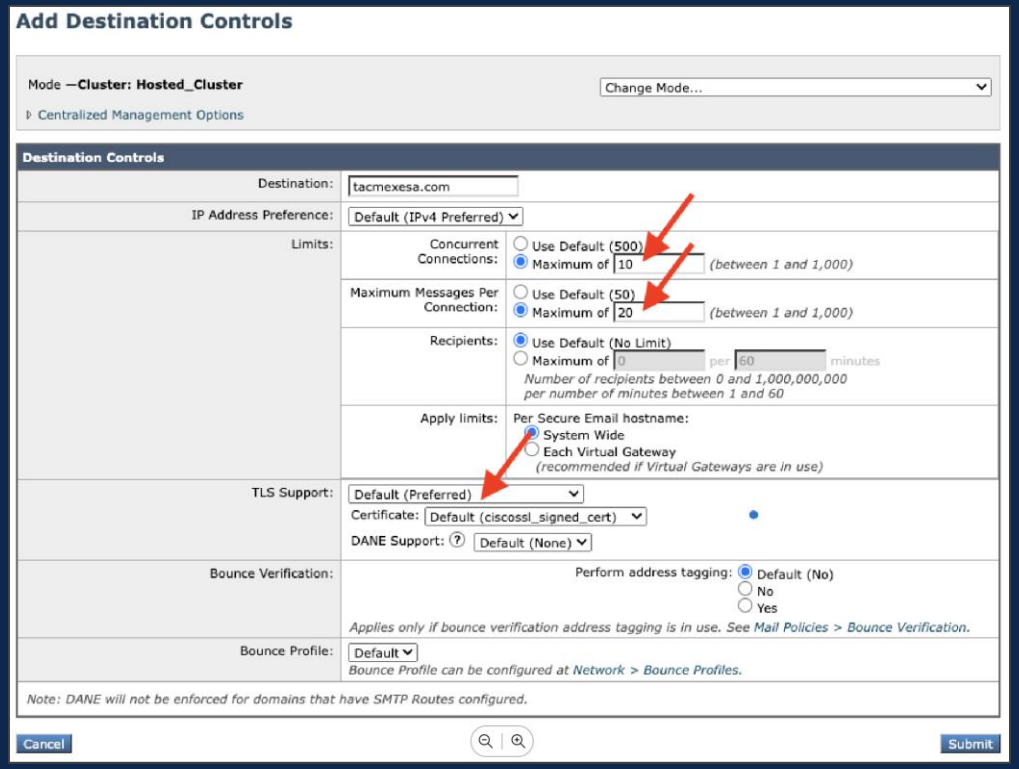
Success — You have been logged out.



Cisco Cloud Security Email Gateway Destination Control



Cisco Cloud Security Email Gateway Destination Control

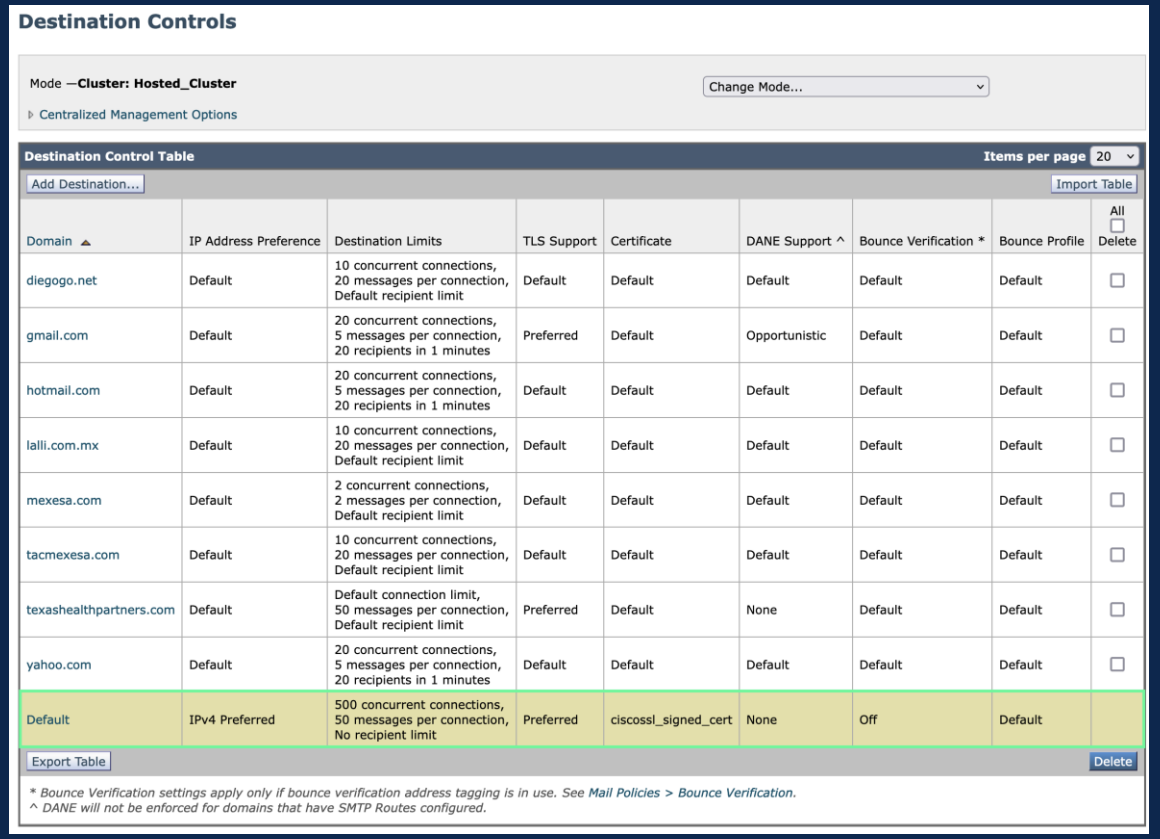


tacmexesa.com	Default	10 concurrent connections, 20 messages per connection, Default recipient limit	Default	Default	Default	Default	Default

Cisco Cloud Security Email Gateway Destination Control

TAC Tip

- 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 Delete
diegogo.net	Default	10 concurrent connections, 20 messages per connection, Default recipient limit	Default	Default	Default	Default	Default	
gmail.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Preferred	Default	Opportunistic	Default	Default	
hotmail.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	Default	
lalli.com.mx	Default	10 concurrent connections, 20 messages per connection, Default recipient limit	Default	Default	Default	Default	Default	
mexesa.com	Default	2 concurrent connections, 2 messages per connection, Default recipient limit	Default	Default	Default	Default	Default	
tacmexesa.com	Default	10 concurrent connections, 20 messages per connection, Default recipient limit	Default	Default	Default	Default	Default	
texashealthpartners.com	Default	Default connection limit, 50 messages per connection, Default recipient limit	Preferred	Default	None	Default	Default	
yahoo.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	Default	
Default	IPv4 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	Preferred	ciscossl_signed_cert	None	Off	Default	

Export Table Delete

** Bounce Verification settings apply only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.*
^ DANE will not be enforced for domains that have SMTP Routes configured.

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

System Status:	Online
Incoming Messages per hour:	0
Messages in Work Queue:	0

System Status Details

Overview > Quarantines - Top 3 by Disk Usage (Policy and Virus)

Centralized Services a... ...reak Quarantines). Please see details at S...

Local Quarantines

Overview > Threat Level

Centralized Services are enabled (For Policy, Virus and Outbreak Quarantines). Please see details at SMA 68.232.130.237.

Outbreak Details

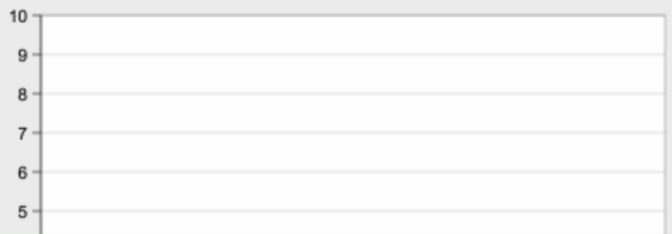
General No modules currently selected for this section.

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

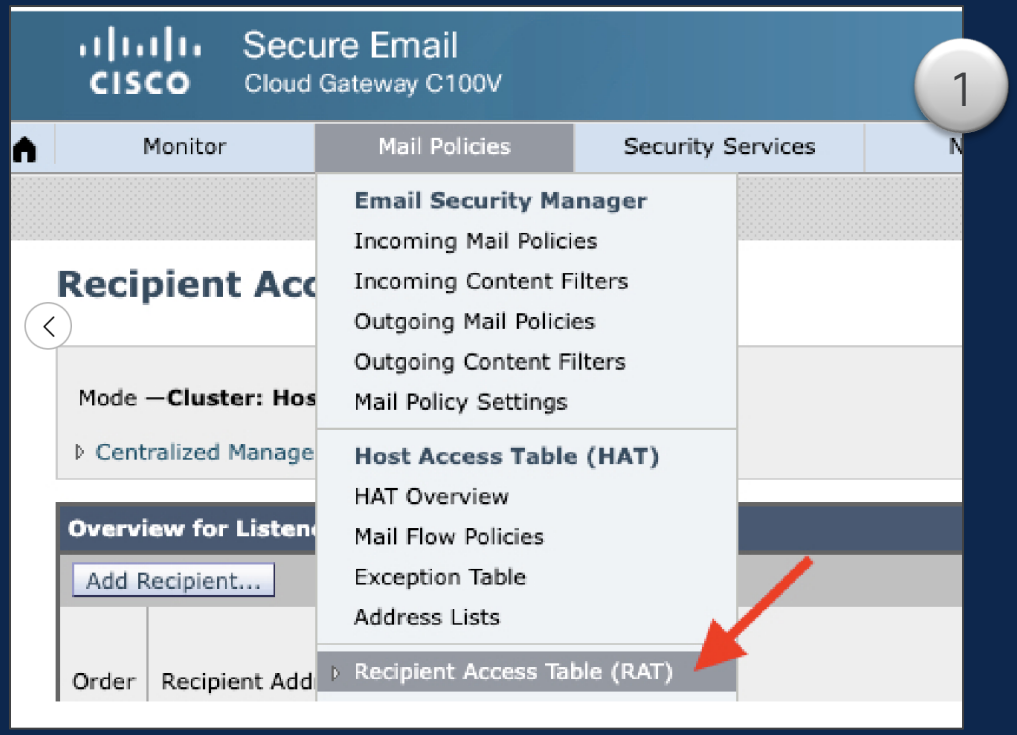


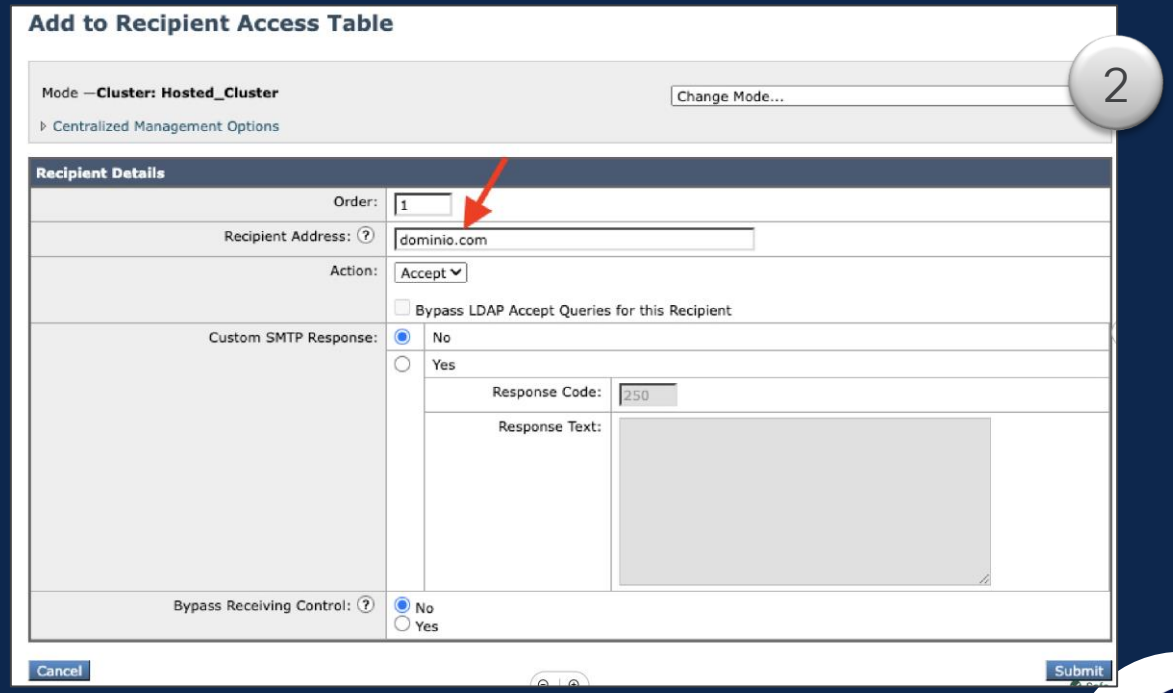
Overview > Incoming Mail Summary

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-Tos

Cisco Cloud Security Email Gateway Recipient Access Table (RAT)





Cisco Cloud Security Email Gateway Recipient Address Table (RAT)

TAC Tip

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

Firefox File Edit View History Bookmarks Tools Window Help — Wed 20 Mar 8:50 a.m.

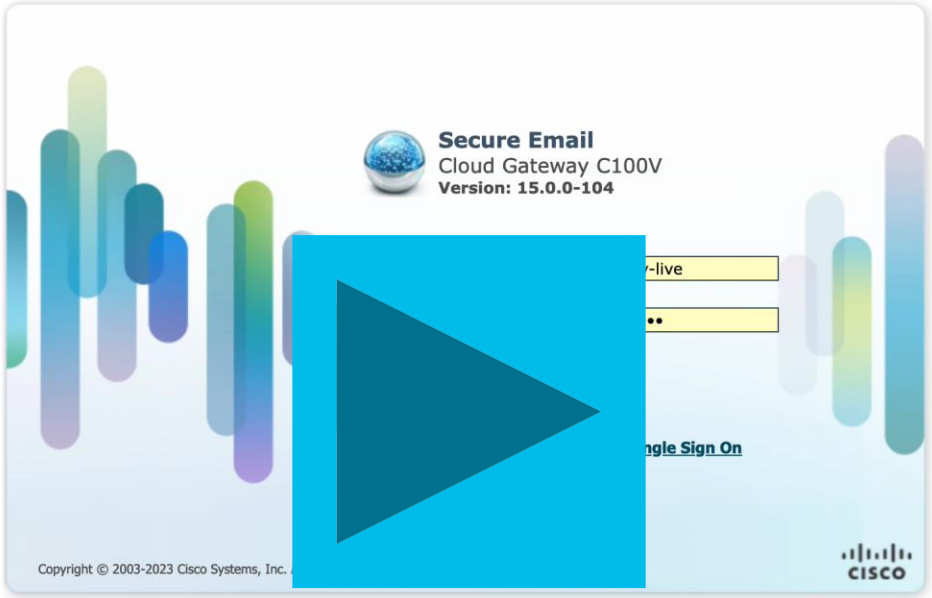
Exchange admin center | Cisco Cloud Gateway C100V (d

https://dh5560-esa1.iphmx.com/login — 110%

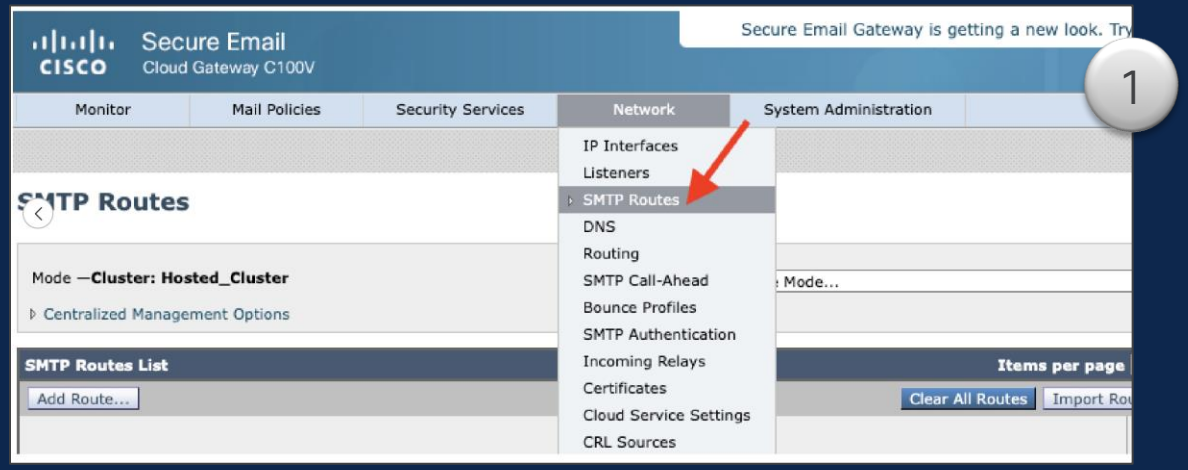
Employee Connecti... | Help Zone | eStore | SAML SSO External ... | Thank you for using... | ATLAS - Login USA | Cloud Email Securit... | AGARI: Login | CES-LAB | trading | Global Bootcamp(s) | Other Bookmarks

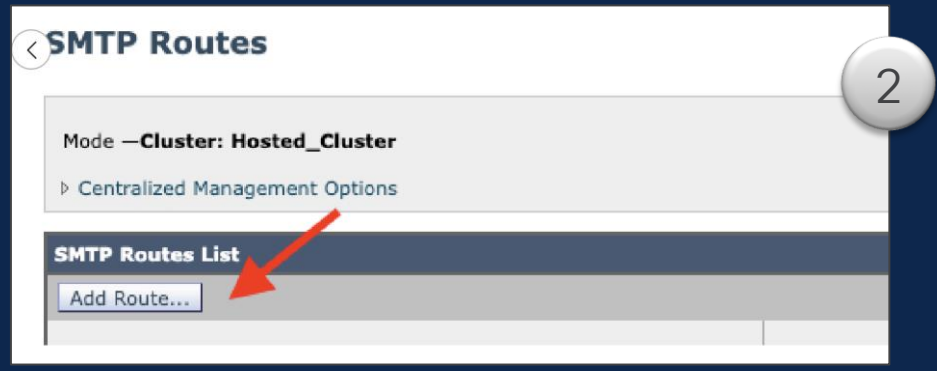
Login Host: **esa1.hc5588-66.iphmx.com**
Help and Support

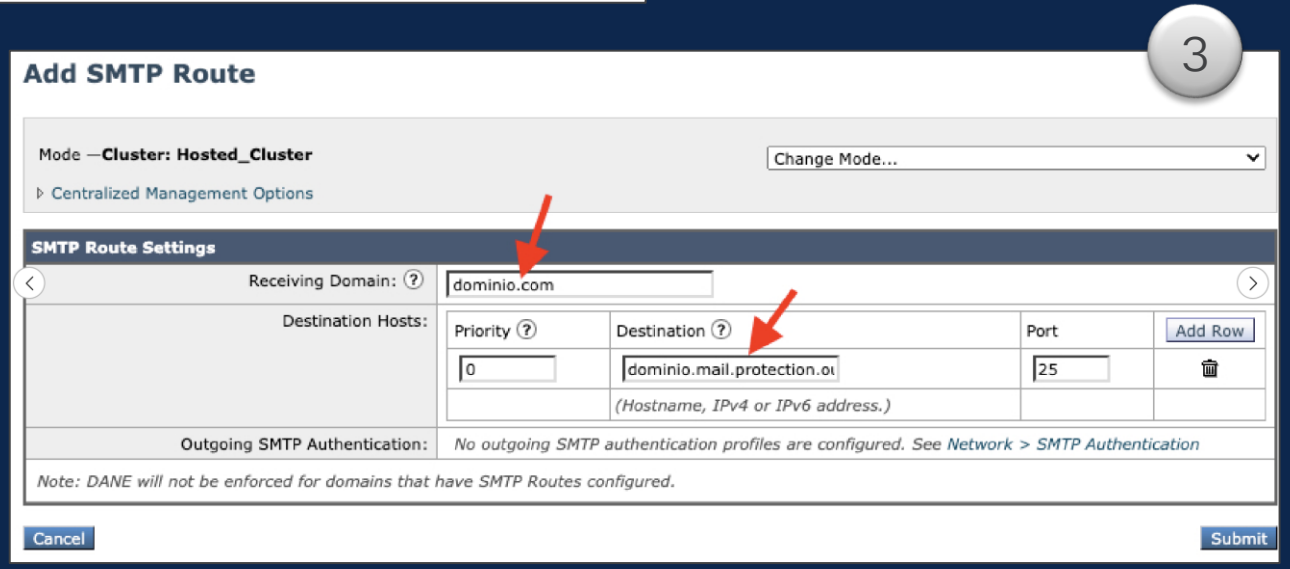
Success — You have been logged out.



Cisco Cloud Security Email Gateway SMTP Routes







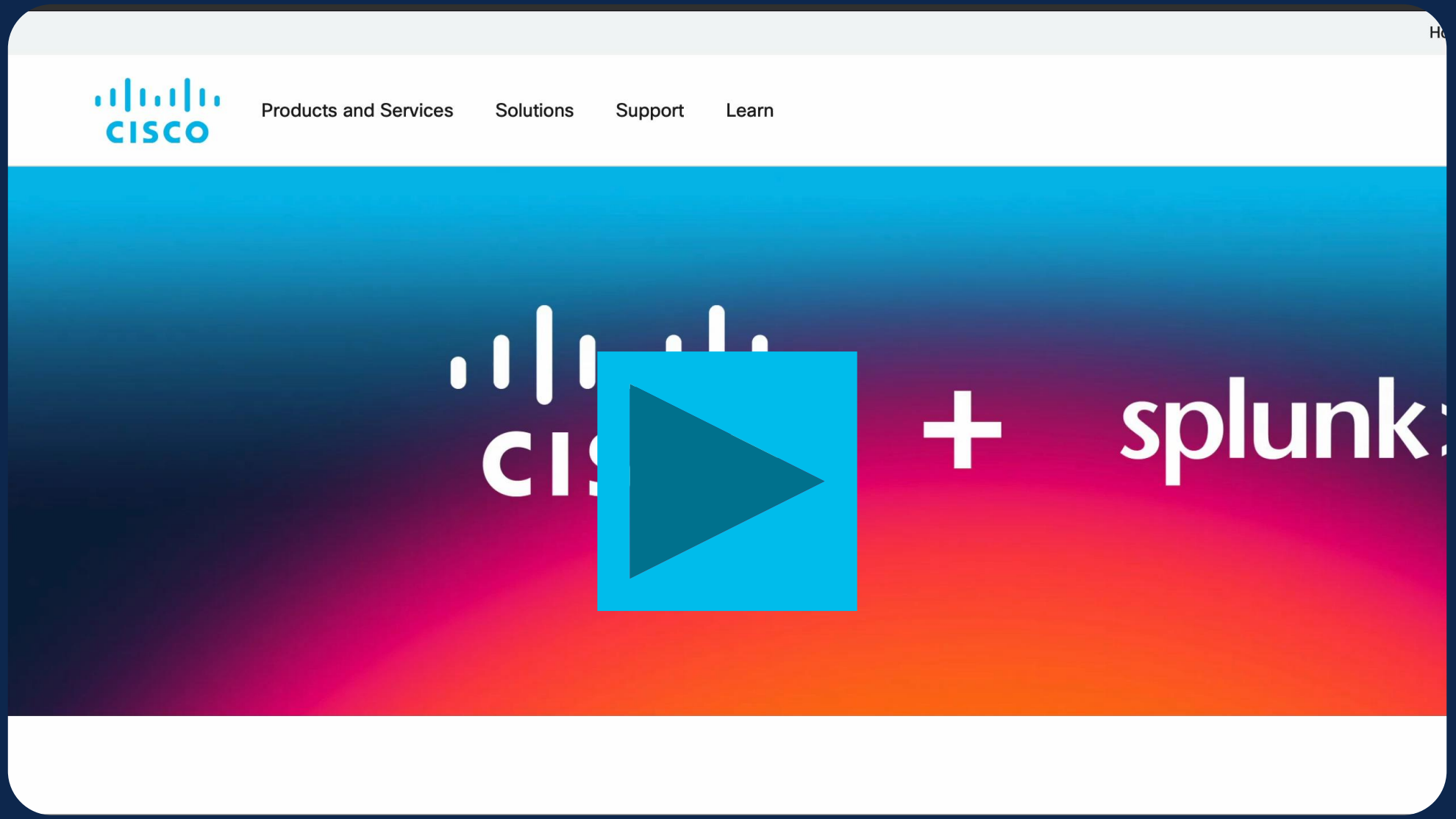
Recomendaciones

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 dia 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)

Cisco Cloud Security Email Gateway

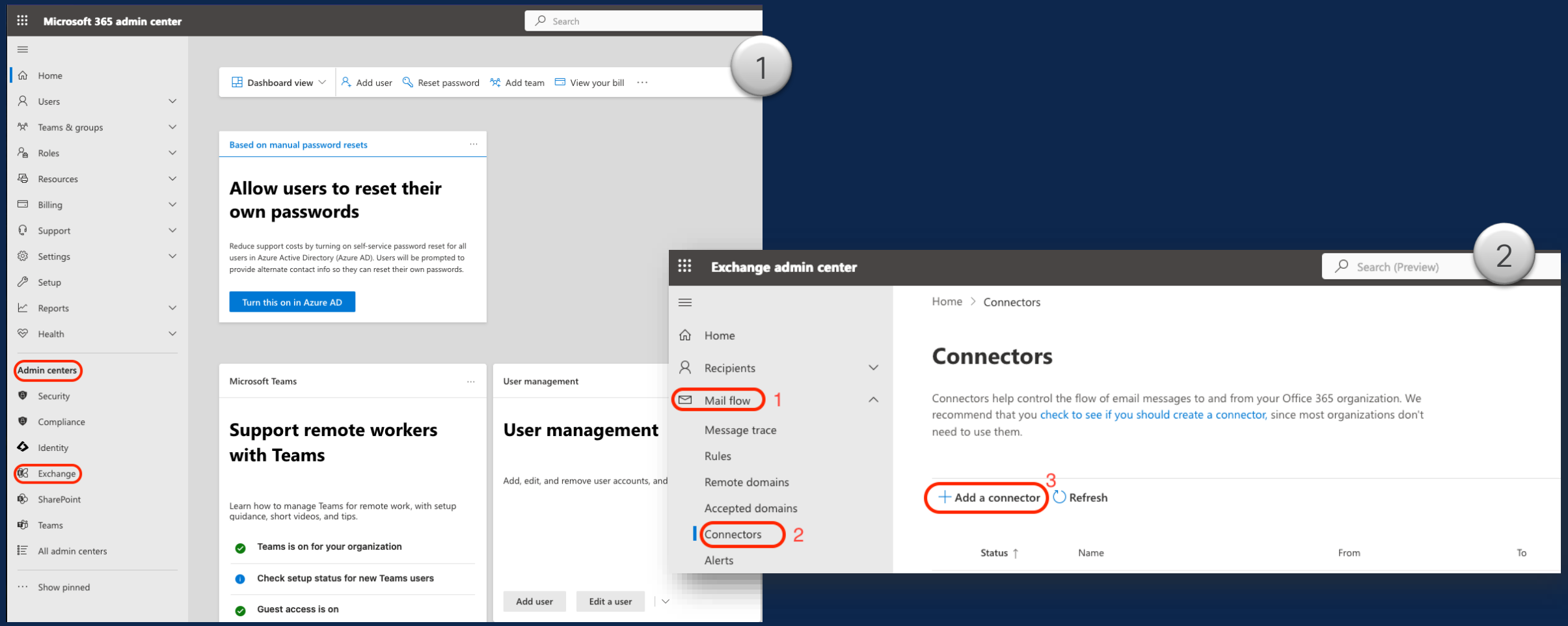


Recomendaciones

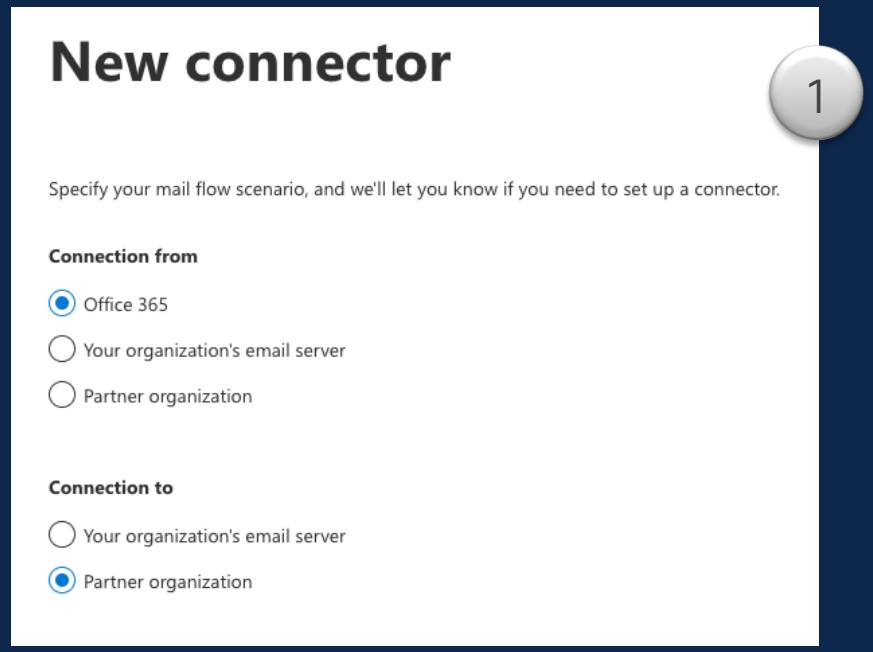
TAC Tip

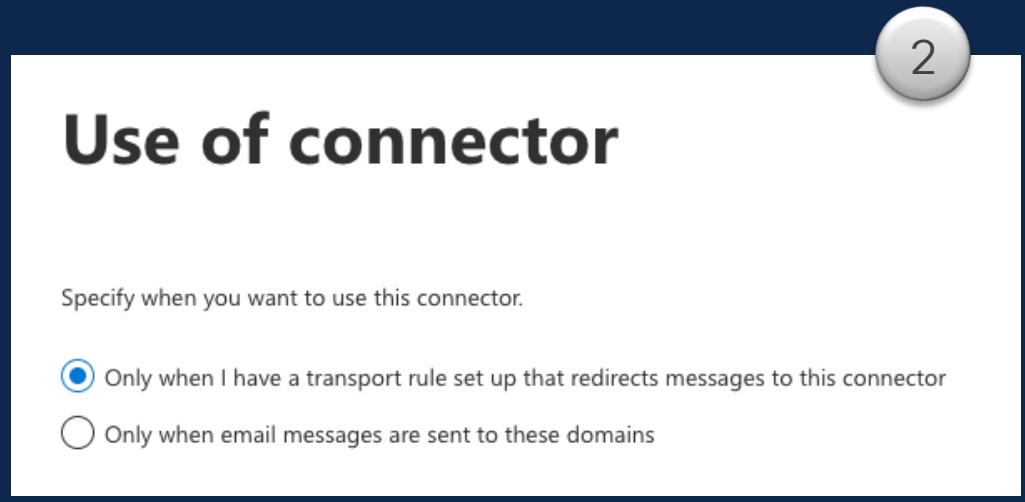
1. **Sender Group:** Asegurarse de utilizar/configurar el Listener correcto.
2. **Sender Group:** Utilizar nombre significativo.
3. **Hostname SG**: Usar el wildcard .protection.outlook.com

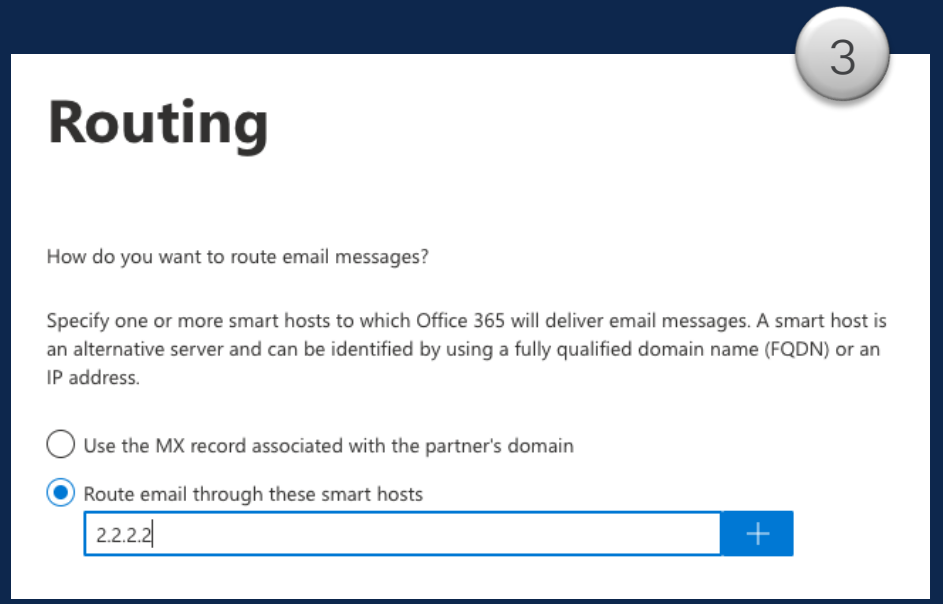
Microsoft Office 365



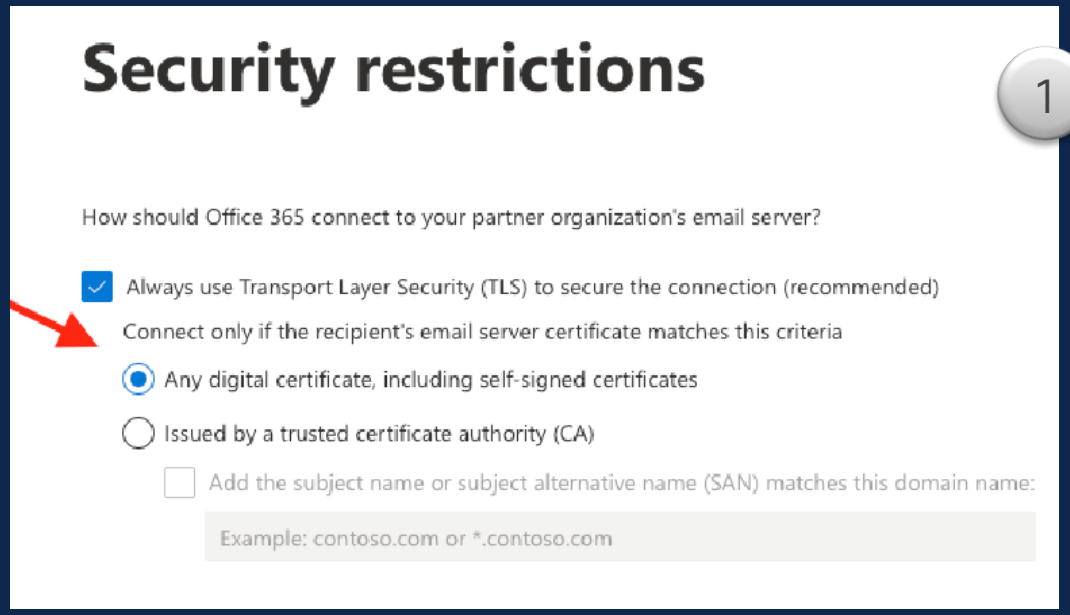
Microsoft Office 365

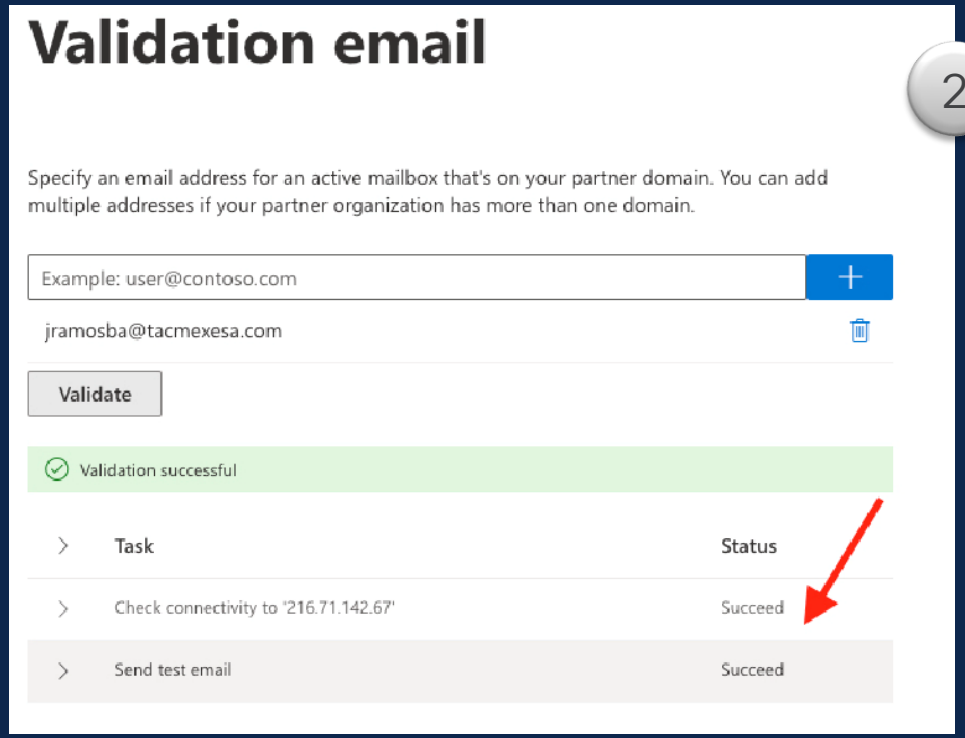






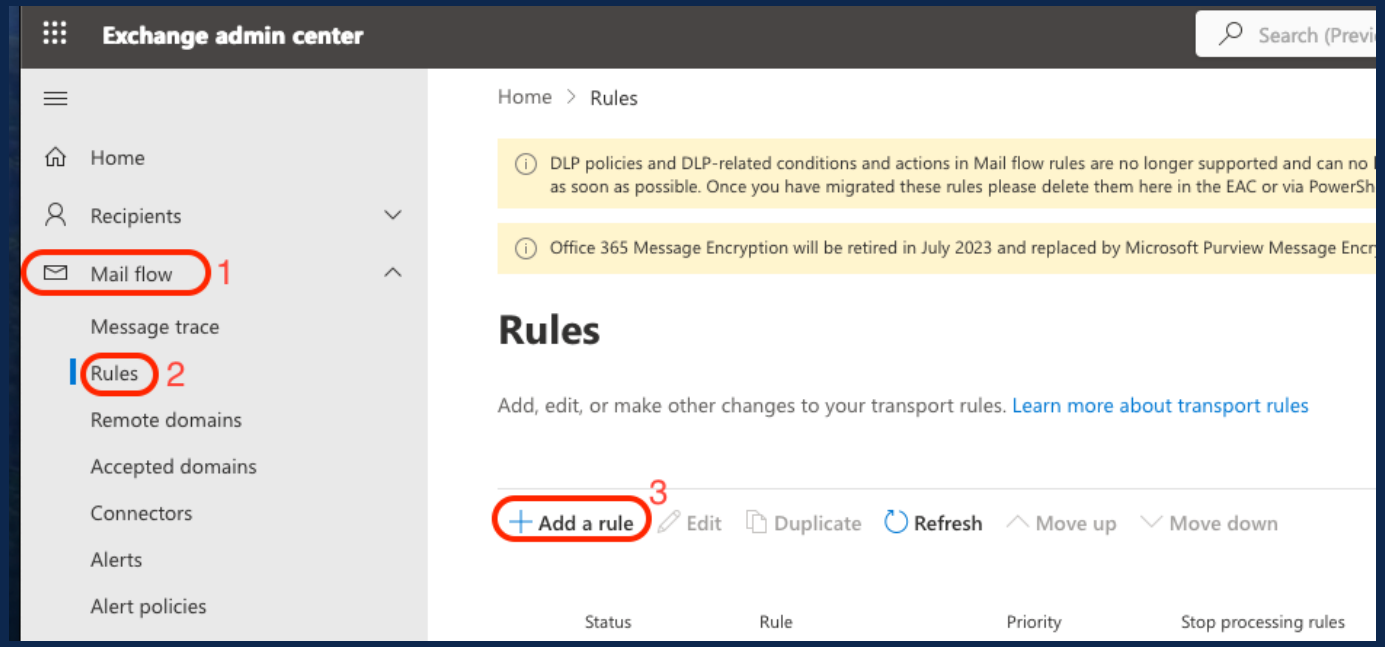
Microsoft Office 365





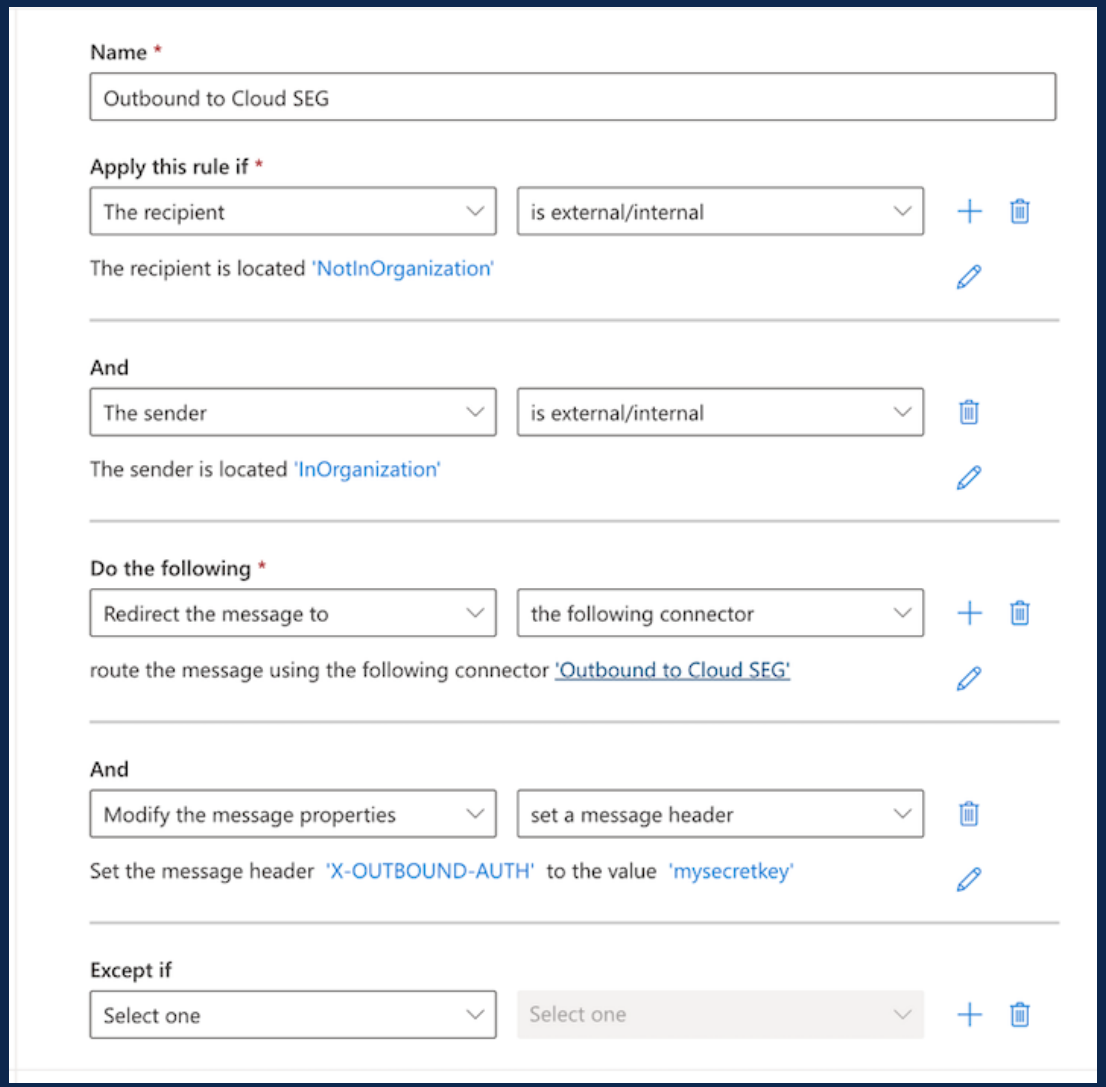
Microsoft Office 365

Crear una regla de Flujo de correo



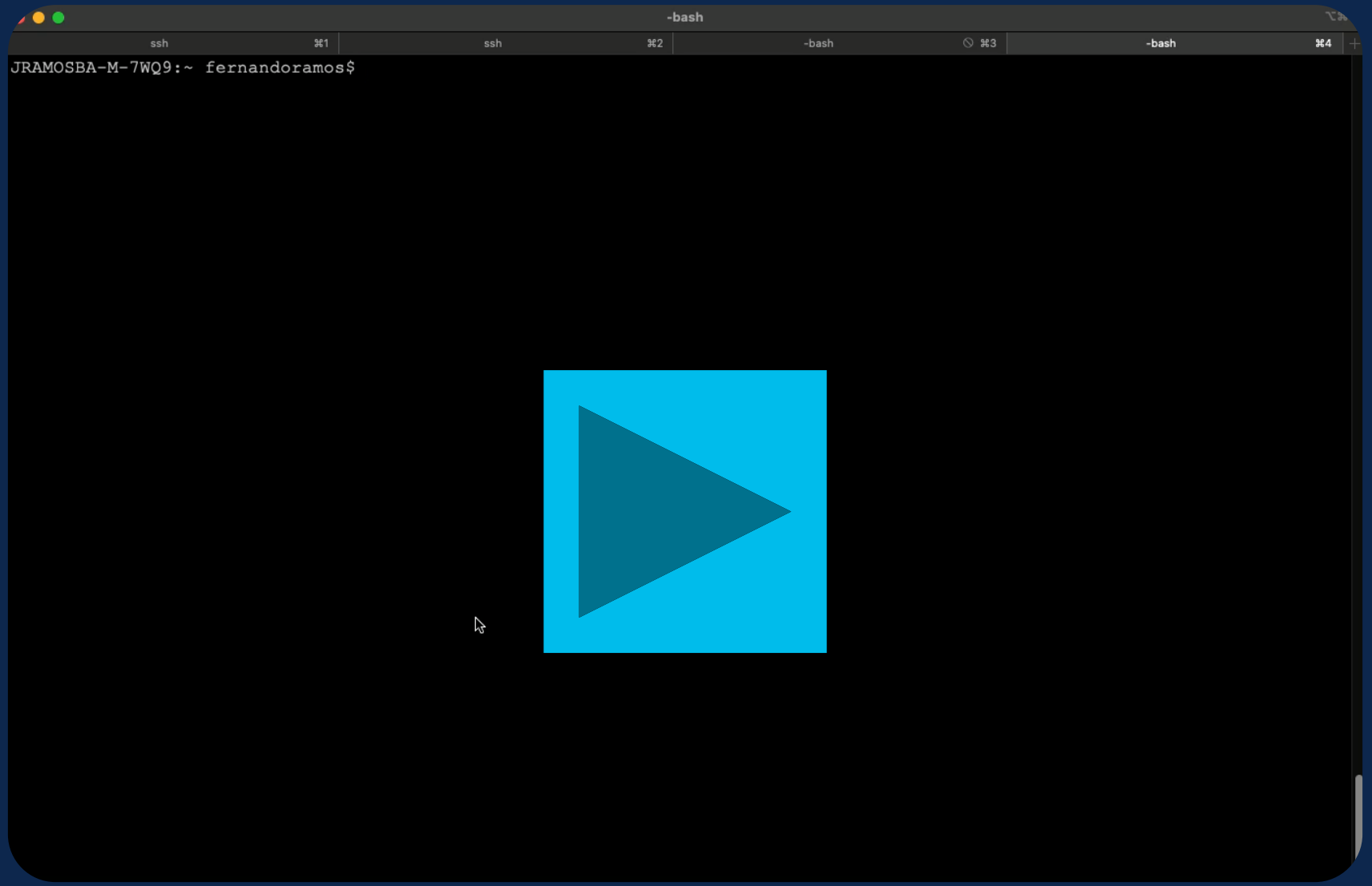
1. Para **Aplicar esta regla si...** *The sender is located...*
2. Para la ventana emergente, seleccionar la ubicación del remitente como: *Inside the organization*

Microsoft Office 365



Message Filter

TAC Tip



Recomendaciones

TAC Tip

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

Active poll

0

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)

DNS

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

Organization Name: [redacted]
Start Date: 2022-09-09 05:09:04 America/Los_Angeles

Below you will find information about your login credentials and other important information regar ding your CES. Please retain this email for future reference

MX Records for inbound email from Internet
- mx1.[redacted].iphmx.com
- mx2.[redacted].iphmx.com

Your Cisco CES portals:
Email Security
https://dh[redacted]-esa1.iphmx.com
Security Management
https://dh[redacted]-sma1.iphmx.com
End User Quarantine
https://dh[redacted]-euq1.iphmx.com

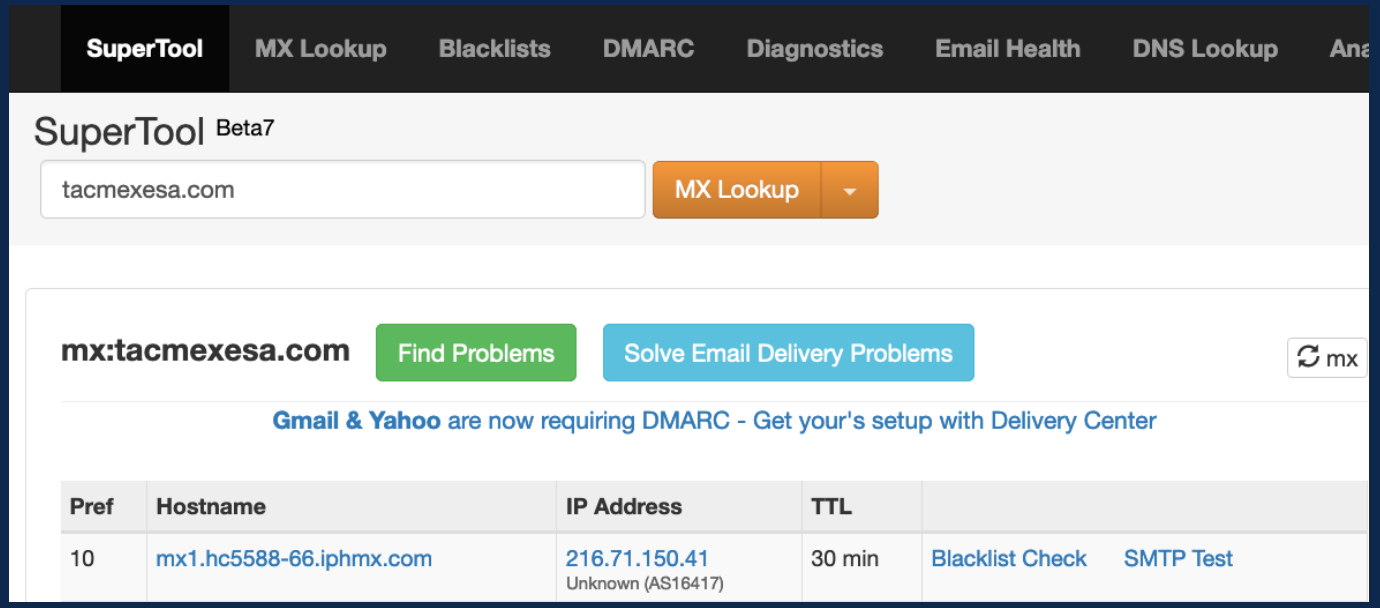
If you are using a Cloud service such as Office365, G-Suite, etc., you should direct your o utbound emails to the address below to have them scanned by Cisco Cloud Email Securit y:

Host and IP address used for outbound relay from Office365 and G-Suite:
ob1.hc[redacted].iphmx.com

Include CES host and IP address in your SPF record:

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

DNS



Active poll

0

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

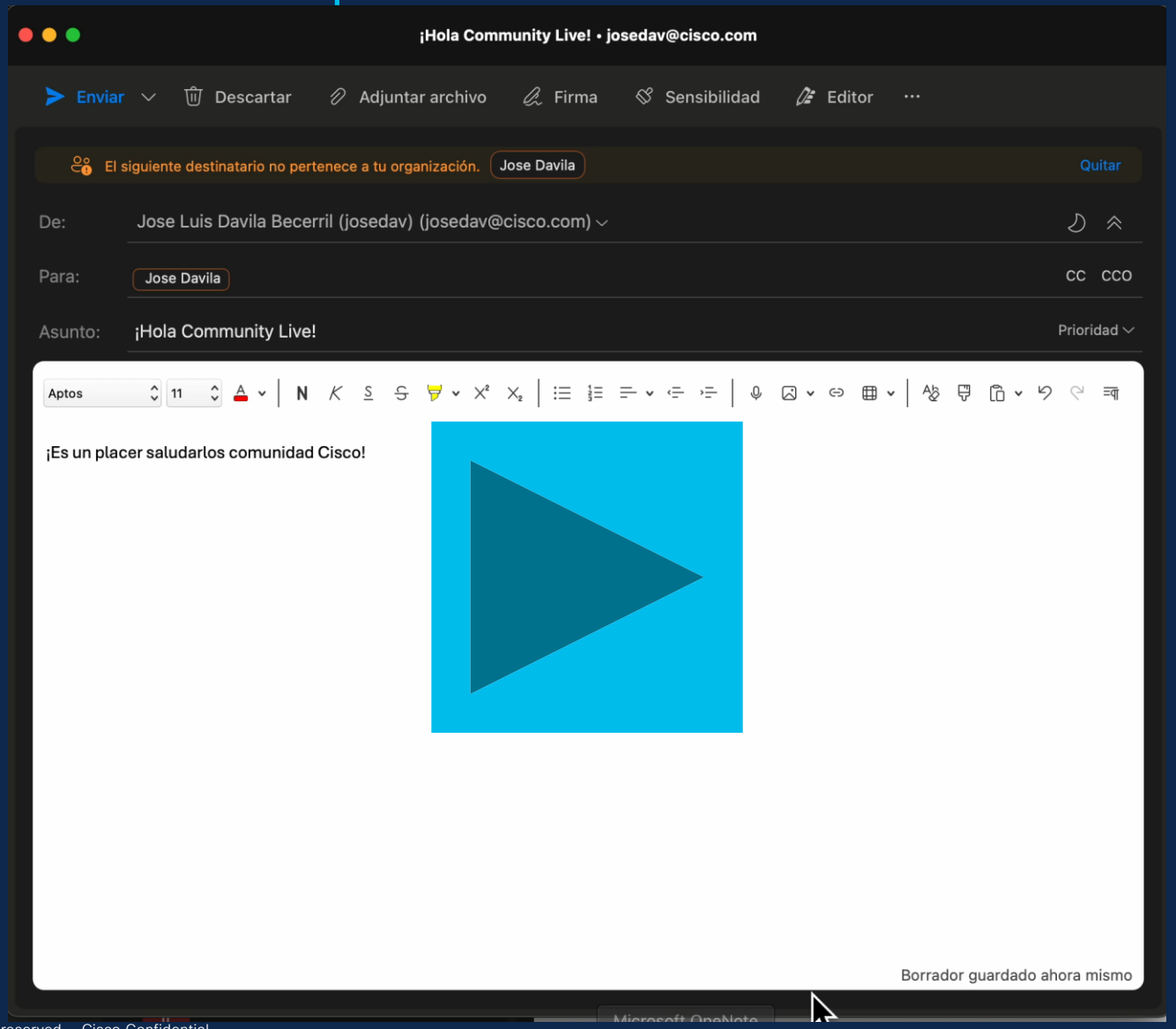
0%

c) Ob1

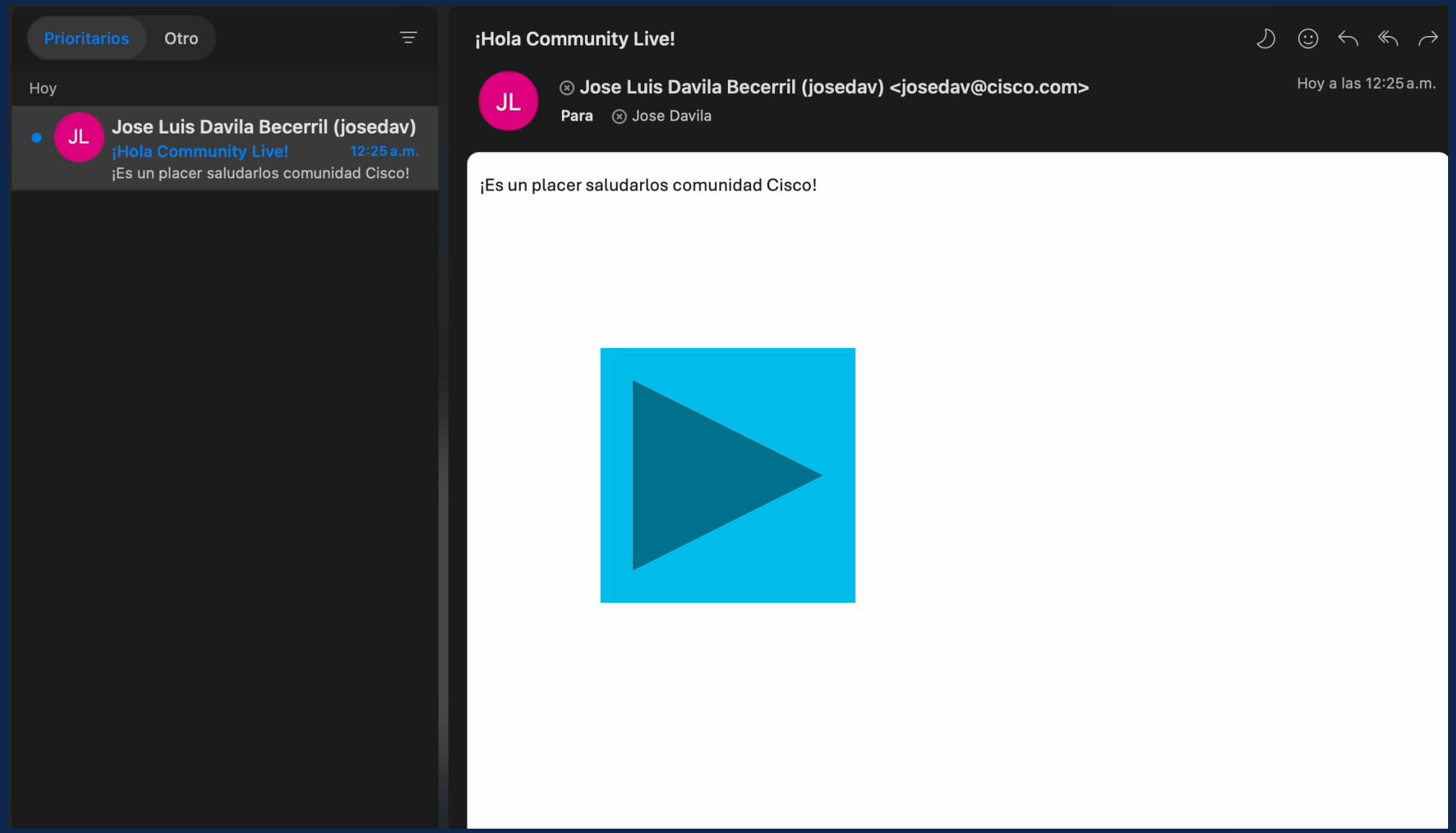
0%

Probar correo entrada y salida

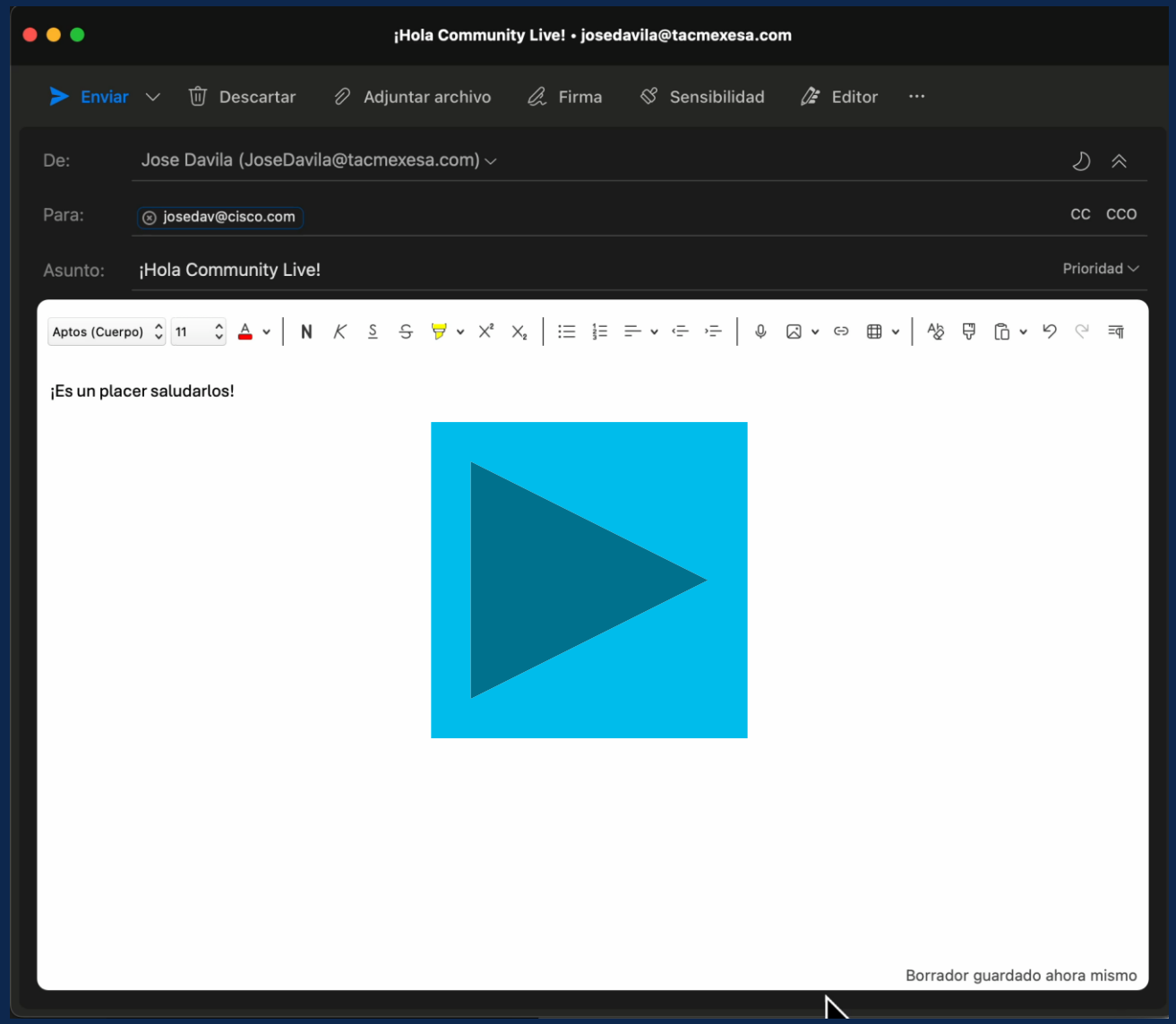
Correo de entrada: probando



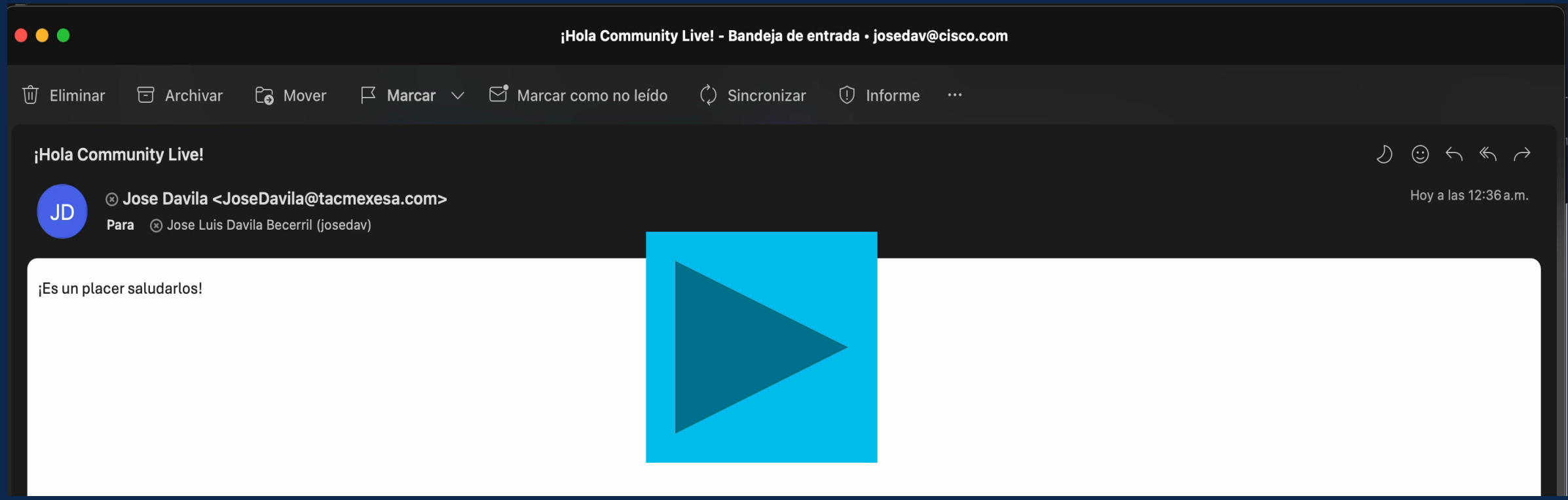
Correo de entrada: recibido



Correo de salida: probando



Correo de salida: Enviado



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?

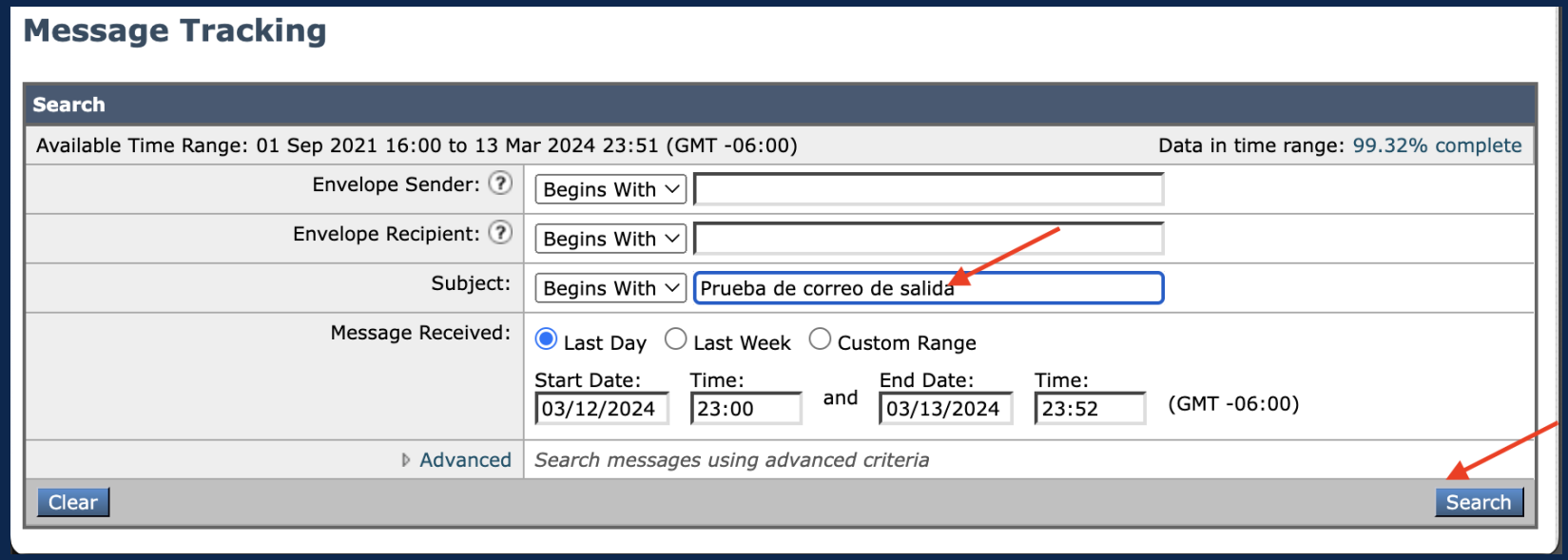
Identificador de conexión

- 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



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 respons

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 SM

Displaying 1 — 2 of 2 items.

1

2

Message Details

Envelope and Header Summary	
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
Sending Host Summary	
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
```

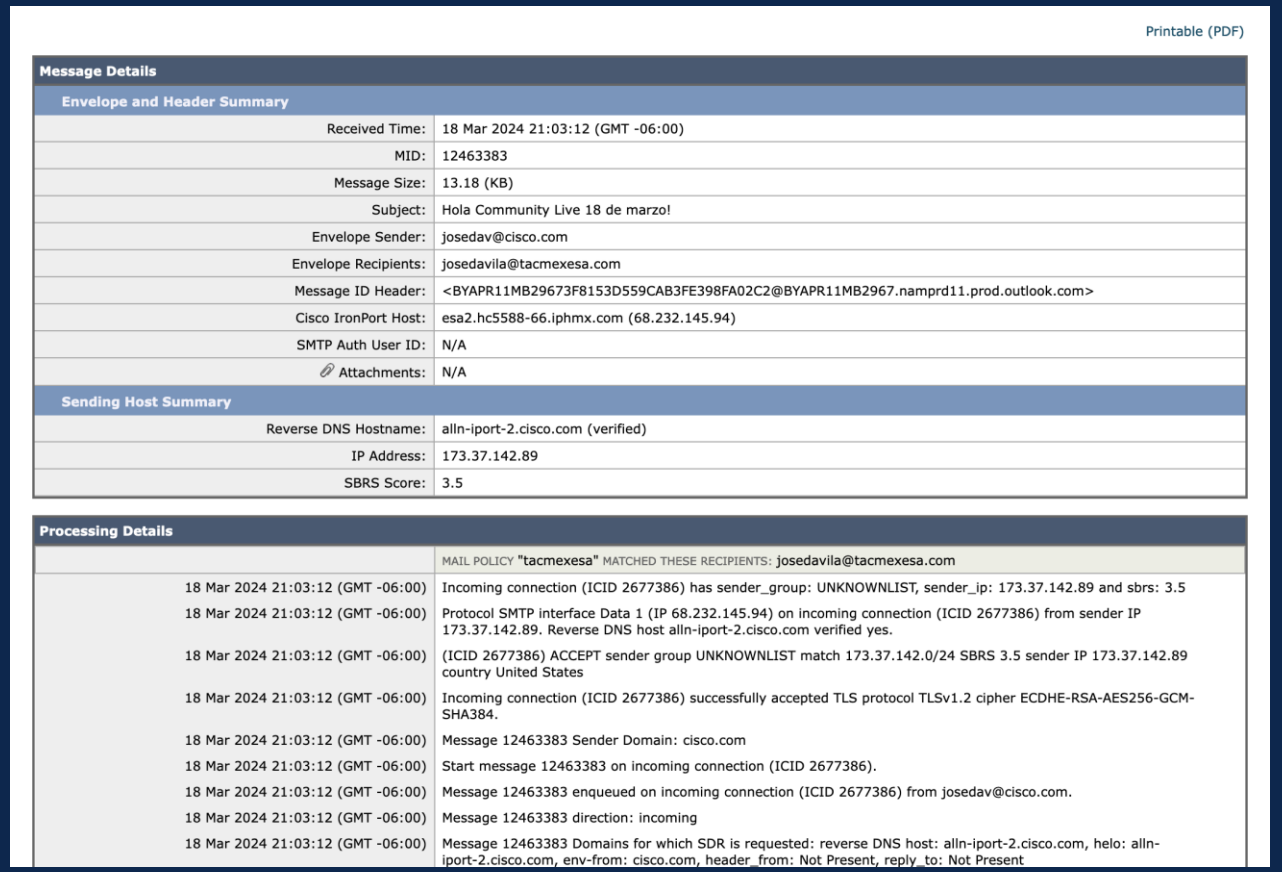
Rastreando un mensaje en los logs del SEG

```
(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

TAC Tip

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



Printable (PDF)

Message Details

Envelope and Header Summary	
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
Sending Host Summary	
Reverse DNS Hostname:	alln-iport-2.cisco.com (verified)
IP Address:	173.37.142.89
SBRS Score:	3.5

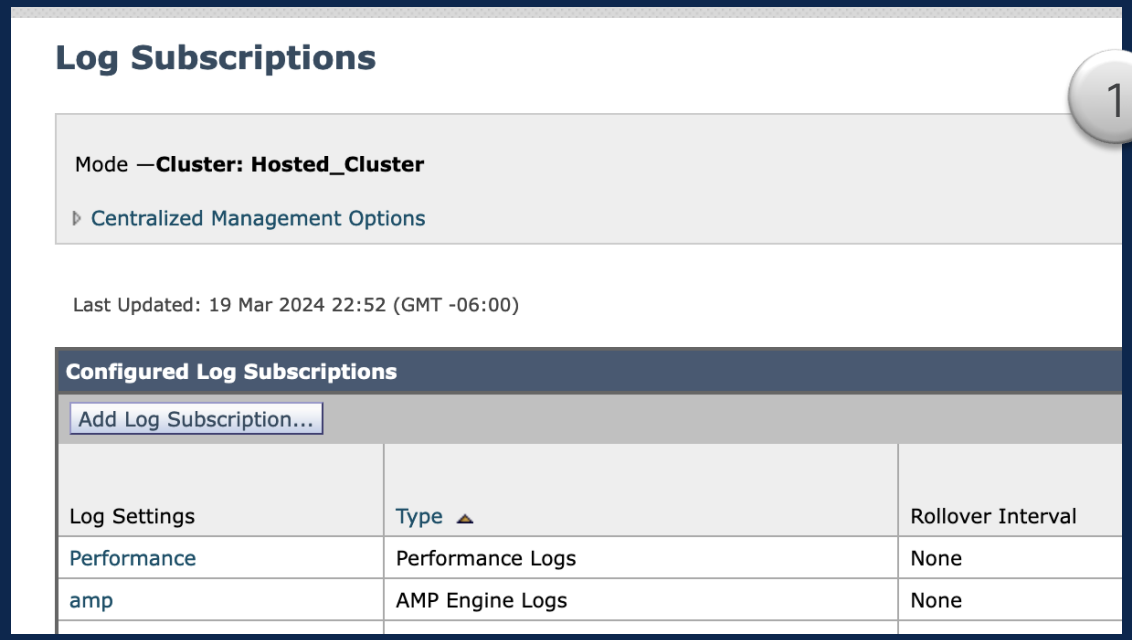
Processing Details

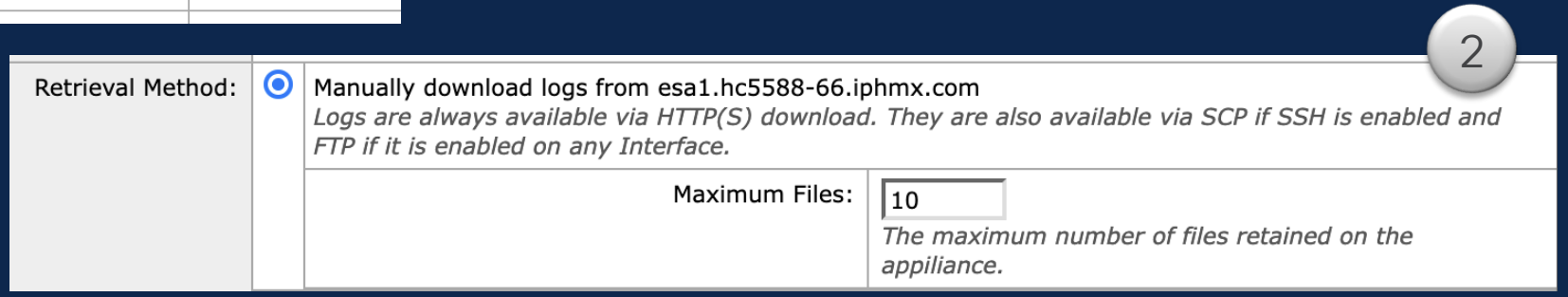
	MAIL POLICY "tacmexesa" MATCHED THESE RECIPIENTS: josedavila@tacmexesa.com
18 Mar 2024 21:03:12 (GMT -06:00)	Incoming connection (ICID 2677386) has sender_group: UNKNOWNLIST, sender_ip: 173.37.142.89 and sbrs: 3.5
18 Mar 2024 21:03:12 (GMT -06:00)	Protocol SMTP interface Data 1 (IP 68.232.145.94) on 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

TAC Tip

- Siempre conserva una suscripción de log local.





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

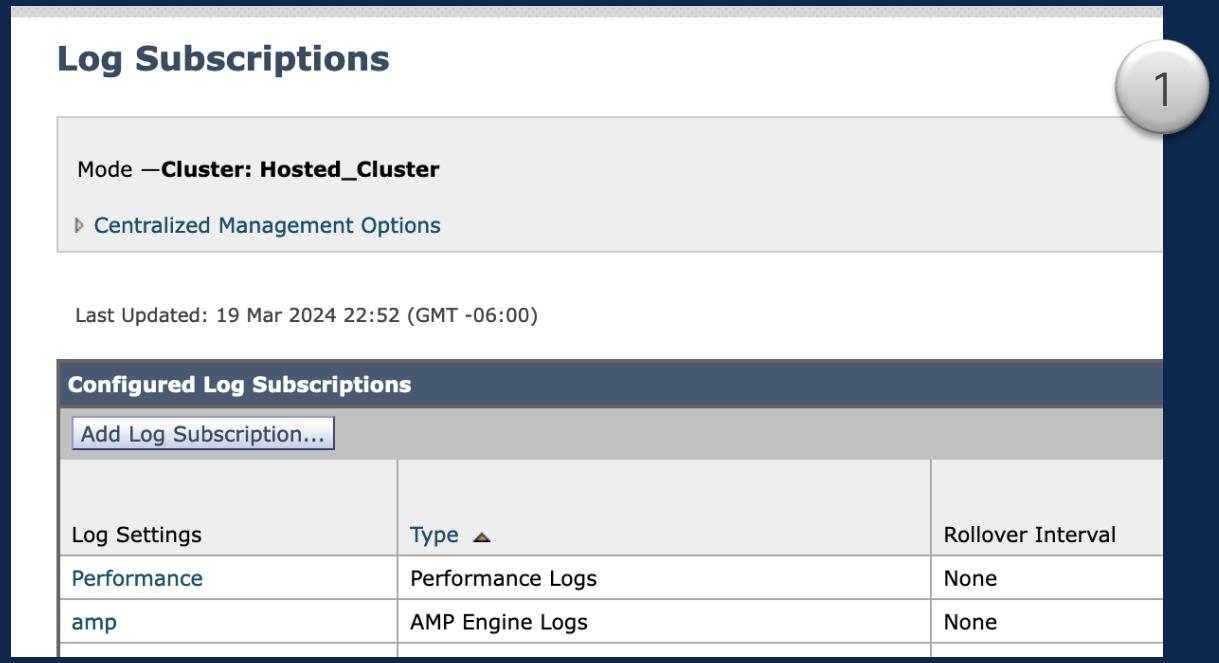
- Observa el código resultante de la entrega del correo electrónico de salida.

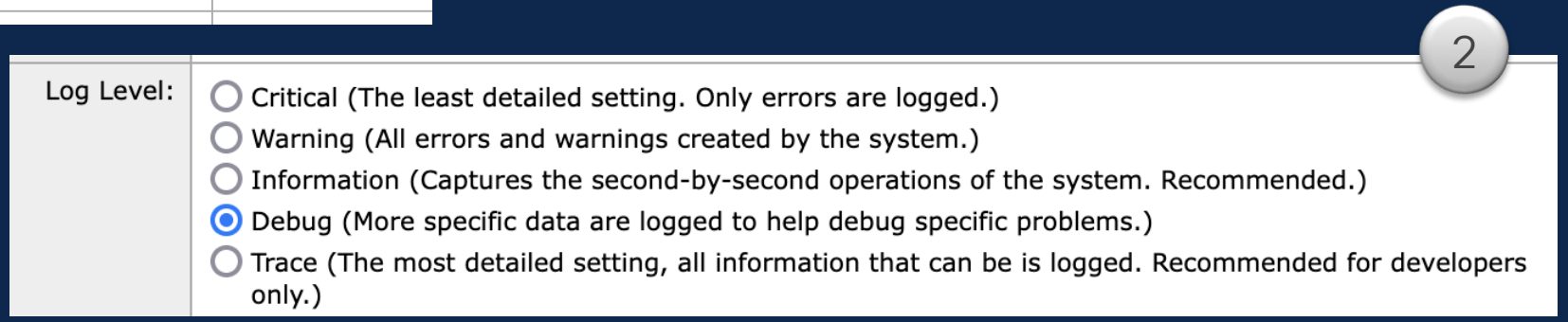
```
Mon Mar 18 20:56:47 2024 Info: Bounced: DCID 8330333 MID 12463381 to RID 0 -
Bounced by destination server with response: 5.3.0 - Other mail system
problem ('554', ['Too many hops']) [('from', '"Jose Luis Davila Becerril
(josedav)" <josedav@cisco.com>'), ('to', 'Jose Davila
<josedavila@tacmexesa.com>')]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

Recomendaciones

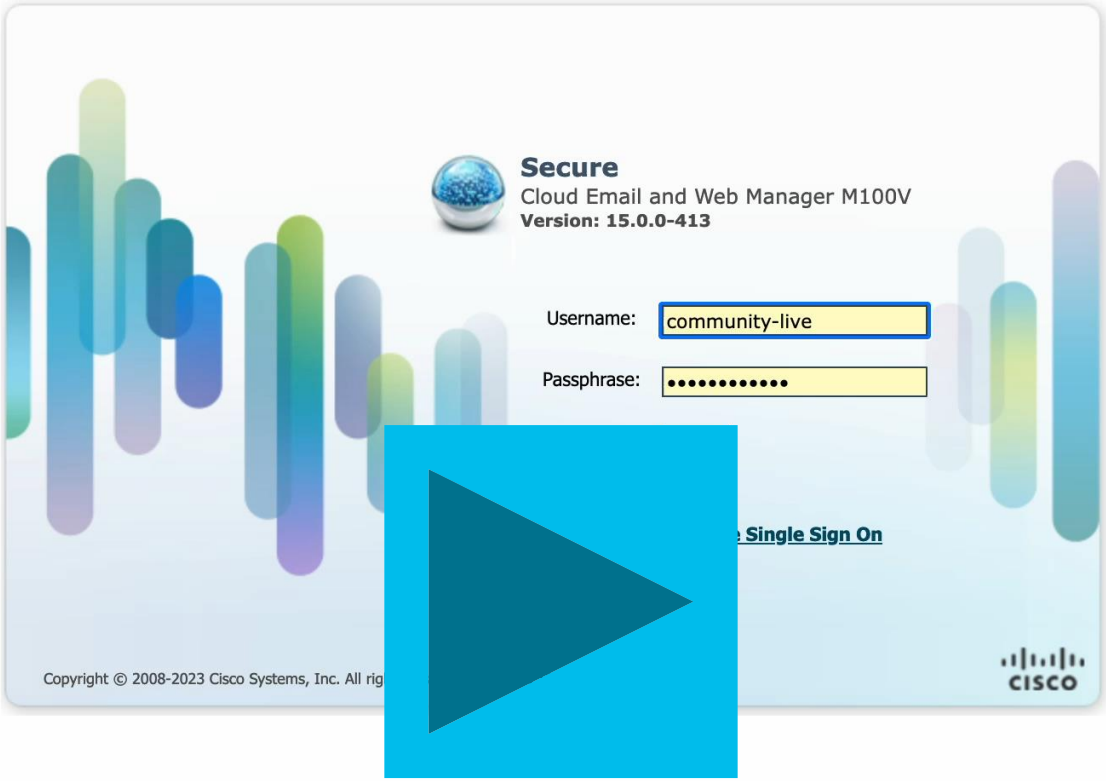
TAC Tip

- Cambia los logs a modo debug.





Login Host: **sma1.hc5588-66.iphmx.com**
Help and Support



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

The following message to <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

Final-Recipient: rfc822;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 s rejected.' (delivery attempts: 0)

De: "Jose Luis Davila Becerril (josedav)" <josedav@
Asunto: **Hola Community Live !**
Fecha: 18 de marzo de 2024, 5:46:29 p.m. GMT-6
Para: Jose Davila <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: Consolida                    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 497767                    d by sender
Mon Mar 18 02:02:06 2024 Info: Message finished MID 49776
(Machine esa1.hc5588-66.iphmx.com) (SERVICE)>
```

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

System Status:	Online
Incoming Messages per hour:	0
Messages in Work Queue:	0

System Status Details

Overview > Quarantines - Top 3 by Disk Usage (Policy and Virus)

Centralized Services a... ...reak Quarantines). Please see details at S...

Local Quarantines

Overview > Threat Level

Centralized Services are enabled (For Policy, Virus and Outbreak Quarantines). Please see details at SMA 68.232.130.237.

Outbreak Details

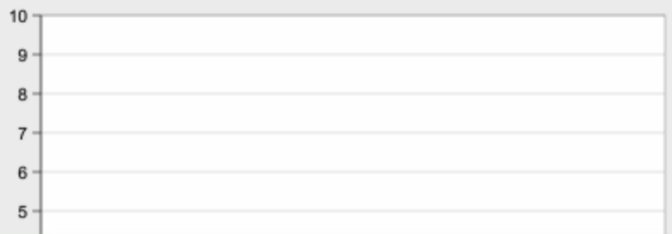
General No modules currently selected for this section.

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-Tos

The following message to <josedavila@tacmexesa.com> was undeliverable.
The reason for the problem:
5.3.0 - Other mail system problem 554-'Too many hops'

The IP address of the MTA to which the message could not be sent:
216.71.150.41

---------- A copy of the message begins below this line ----------
X-CSE-ConnectionGUID: RjsFOORQR7KOwzln4Fhs8g==
X-CSE-MsgGUID: iAYp7cjORcyJzO4W6v3LTA==
Received-SPF: SoftFail (esa1.hc5588-66.iphmx.com: domain of
joseluisdavila90@gmail.com is inclined to not designate
216.71.150.41 as permitted sender) identity=mailfrom;
client-ip=216.71.150.41; receiver=esa1.hc5588-66.iphmx.com;
envelope-from="joseluisdavila90@gmail.com";
x-sender="joseluisdavila90@gmail.com";
x-conformance=spf_only; x-record-type="v=spf1";
x-record-text="v=spf1 include:_netblocks.google.com
include:_netblocks2.google.com include:_netblocks3.google.com
~all"
Authentication-Results: esa1.hc5588-66.iphmx.com; spf=SoftFail smtp.mailfrom=joseluisdavila90@gmail.com; dkim=hardfail (body hash did not verify [final]) header.i=@gmail.com; dkim=hardfail (body hash did not verify [final]) header.i=@gmail.com; dmarc=fail (p=none dis=none) d=gmail.com
IronPort-SDR: 65f8dabe_unPUn1Pa3W0QgZ/ZRNyXL+r/JZp9jKiaCR67EUR5l9FJnnZ
iutL1hrp/h2MaLkk7167foXkCwSvTDEXsoj2w9A==
X-ThreatScanner-Verdict: Negative
X-IPAS-Result: =?us-ascii?q?A0GlFjMhmSBl/ymWR9haHgEBCxIMgVuCGIIBBoFMLQlOh?=
=?us-ascii?q?h6NcYZhhwMwAn0ZHoYTA4EmA4pYKxMPAQEBAQEBAQEBCAFCAgQBAQMEhVEJh?=
=?us-ascii?q?jYCL0IBAgECAQEBAQEDAgMBAQEBAQEBAgEBAQQBAQECAQECBAIBAQEBAoEGE?=
=?us-ascii?q?4VoDYI3DgwDA4EpWwIFAzkBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBA?=
=?us-ascii?q?QEBAQEBAQEFAix1BycBGx4DEhABXREBBQFJDoJcgioBAzEDAaRSgSgBdzQ/A?=
=?us-ascii?q?hAYASkXAQyBC4shBQIWgQGCCgYFAgEDghStNgoZKA1tPYEfAgcJAQoVhW4jg?=
=?us-ascii?q?xgBhDSDLIEsgSGCKIE8HIg2g0eCLwSDfpZBAQcHGQ0SAwMLAgIBAQIDAgIBA?=
=?us-ascii?q?gEGAQoJBgIFAQ0CAQEBAgQCAwYCAgEFAwUCAg0DAQEHBgIEBAUCAwQCAgICB?=
=?us-ascii?q?AIRBAMBAwIDAwMEAQMJBAICAwIBAQIBAwIBAwMCBQQDAwMCBQIFAQIBBAEDA?=
=?us-ascii?q?wIDAgMDAwQBAgIBCwkDAwICAgQCAgMDAwMBDQMBAwECAgMCAQMRBAQBAgECA?=
=?us-ascii?q?QQBAwMDAhACAwMDAQQBAgMCAgICBQUFCwQCAQMDAgQCAgICAgIGBgkCAgEBA?=
=?us-ascii?q?QECAQEBAQECBwMCAQECAgMHBgIJAgIBAQMCAQIBBwgBBAICAgICAwIDAgICA?=
=?us-ascii?q?QIMCAIBBgEEAxQBAhMBAQYFAwYHAgUBAwUBAgICAwUEAQQDAwIFAgIDAgICA?=
=?us-ascii?q?xQEAQMLAwMBAQIBBAMDAgIDAgQBAhAFAwMTDQEFAgICAhYCBgUIAwcEBAMGF?=
=?us-ascii?q?QwCCAECAQECAgILAQIEAQICAgICAgICAgECBgMGAwIFAgIDAwICAgMCBAIJA?=
=?us-ascii?q?gICBAIBBQICAwIFAgQGAQICAgMDAwMDAgcIBQMDAQcCBAgDAgUDBQEHBwIEA?=
=?us-ascii?q?gIBAgsDAQYDAwIDAwcFCQQJBwICAgICCgMHAwIsAwEGCAEEAQkBAgIFAwICA?=
=?us-ascii?q?wIFCAcBAwICAgsBEQICGwUCAgMCBAIDAQIBCRIDAgQFAhwEAgMDAgMDAwMDA?=
=?us-ascii?q?wMDAQYCAwMCAwMDAxsCAwMCAwMDAwICBQUJBQICAgIFBAYIAgIUAgEBBwIEA?=
=?us-ascii?q?gICBQEZBgMLAwUBAgQCBAIGBAMDBQQCAgYFAQEBAQIEAgIKAwMCAgMCAwMBB?=
=?us-ascii?q?=us-ascii?q?QUBAwEDAQICAQQDBAIMBSURAgMLDQUWAgMCAgMDBAkCAgQCAgIPDR0PEAUDA?=
=?us-ascii?q?=us-ascii?q?gkCBQYFBQICBAIBAwUBAgQBAgsMBAsBAwYFAgIBAgYKAQgNBQcCAwICBQMDA?=
=?us-ascii?q?=us-ascii?q?QEFAgMDAwUBAgMDAgMDAgIIAwMCBAECAgIDBAICAgIHBAIQAREIAwMBBAUCA?=
=?us-ascii?q?=us-ascii?q?gUKGAQBAwIDAwMDAgEDAwMBDAgDBAIKAQIFAwICBRMCAgQQBgIBARUBGgELB?=
=?us-ascii?q?=us-ascii?q?AMJAgcBAhUDAQEBCAEDBA4BAgMFAQEBAQUCAQEBAgYCBQICAQQIBAQBDAMDA?=
=?us-ascii?q?=us-ascii?q?gkBBAEDBAELAgEDBAICAgIBAgIDAgIGAgMCBAEDAwMCAwECAQMCAgwDAwIIA?=
=?us-ascii?q?=us-ascii?q?wMFAQIDAgICBAICAgICAwQBBAQFAgECAwIGBgMEAwIFAgMFAQEEAggGAQMCA?=
=?us-ascii?q?=us-ascii?q?wIHCwIBBgICAQQBAQIUAQQBAQIDBQICBgMDAwIDAgIIBQgDAgEBAgEEAwECA?=
=?us-ascii?q?=us-ascii?q?QEZAgIMBwMBBQICAQUDBwEEAQEBAwcBAwMCAg4CAgoFBQIGAgQCHAICAhABA?=
=?us-ascii?q?=us-ascii?q?gECAQMLAwcCAgECEAICAQIKBwIDAgUFAQUBBAIBAgYBCAICEgUGCAIBAQQCC?=
=?us-ascii?q?=us-ascii?q?wMCAQECAgIGBwIFBQMDBAIPBwUCAQIGAgEBAxAIBwECDgYCAwQCAgUCAQIDA?=

```
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-                                    eply-to: Not Present
Mon Mar 18 18:22:22 2024 Info: MID 4977776 SDR: Consolida                                    Level: Favorable, Threat Category: N/A, Suspected Domain
(s) : N/A (other reasons for verdict). Sender Maturity: 3                                    ) for domain: esa1.hc5588-66.iphmx.com
Mon Mar 18 18:22:22 2024 Info: MID 4977776 SDR: Tracker H                                    nPUn1Pa3W0QgZ/ZRNyXL+r/JZp9jKiaCR67EUR5l9FJnnZiutL1hrp/h
2MaLkk7167foXkCwSvTDEXsoj2w9A==
Mon Mar 18 18:22:22 2024 Info: MID 4977776 ready 391664 b                                    sdavila90@gmail.com>
Mon Mar 18 18:22:22 2024 Info: MID 4977776 matched all re                                    ecipient policy tacmexesa in the inbound table
Mon Mar 18 18:22:22 2024 Info: MID 4977776 interim graym                                     (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
```

Add SMTP Route

Mode —**Group: F4_Group**

Change Mode...

Centralized Management Options

SMTP Route Settings

Receiving Domain:				
Destination Hosts:	Priority	Destination	Port	Add Row
	0		25	
		(Hostname, IPv4 or IPv6 address.)		
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

How-Tos

“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.

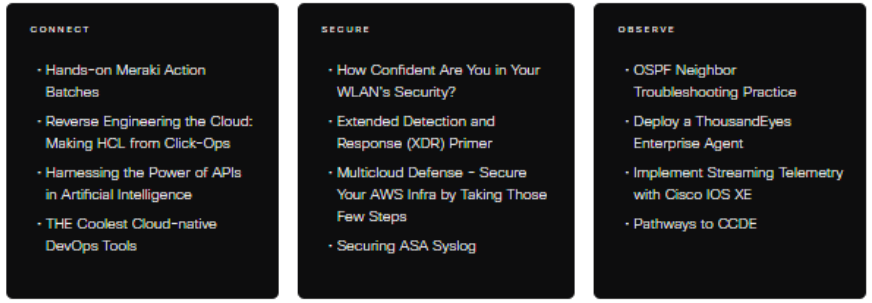
Miércoles 24 de abril 2024 (*sesiones en inglés)

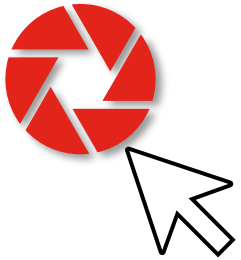
Estamos trayendo la luz sobre los temas y las tecnologías más importantes -desde los fundamentos y las mejores prácticas, hasta las habilidades especializadas- mismas que generan las principales tendencias e innovaciones actuales. Entérese de las más recientes estrategias y tecnologías para conectar,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





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.

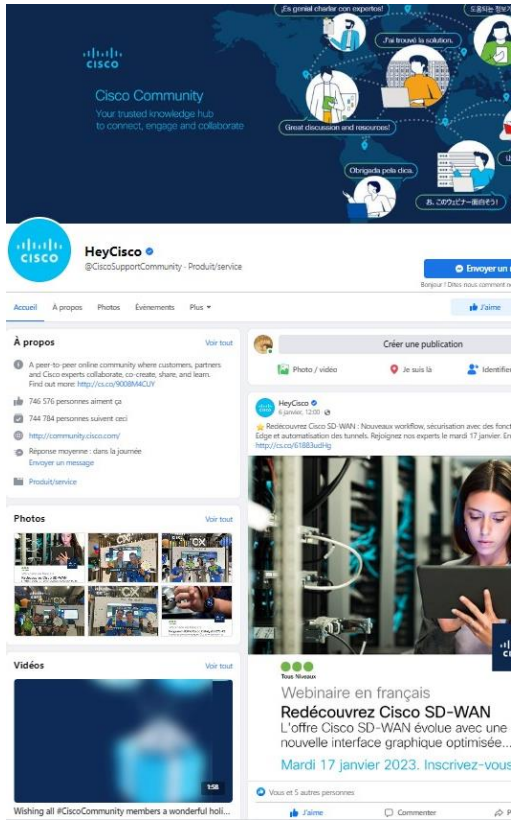
Nuestras Redes Sociales

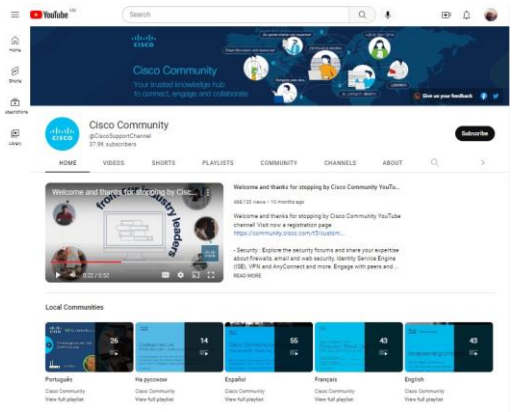
LinkedIn
[Cisco Community]

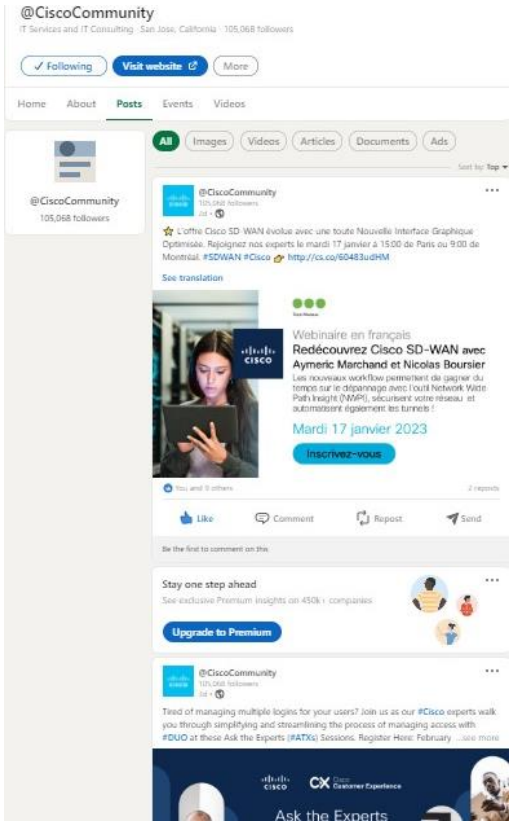
Twitter
[@CiscoCommunity]

YouTube
[CiscoCommunity]

Facebook
[CiscoCommunity]







The bridge to possible