

# Remediación de correos electrónicos de CTR

## Contenido

[Introducción](#)

[Antecedentes](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificación](#)

[Paso 1. Acceda al portal CTR en función del acceso a los servidores disponibles e investigue](#)

[Paso 2. Investigue los mensajes entregados que parecen ser maliciosos o una amenaza utilizando los observables admitidos. Se puede buscar en los objetos observables según los siguientes criterios, como se muestra en la imagen:](#)

[2.1 Ejemplo de una investigación e investigación de IP a continuación, como se muestra en las imágenes:](#)

[2.2 Esto es lo que obtiene en la bandeja de entrada antes de que se solucione el mensaje, como se muestra en la imagen:](#)

[2.3 Al hacer clic en "ID de mensaje de Cisco", seleccione entre las opciones de menú cualquiera de las acciones remediadas admitidas, como se muestra en la imagen:](#)

[2.4 En este ejemplo, se selecciona "Iniciar reenvío" y aparece una ventana emergente de éxito en la esquina inferior derecha, como se muestra en la imagen:](#)

[2.5 En el ESA, puede ver los siguientes registros en "mail logs" que muestran que se inicia la remediación "CTR", la acción seleccionada y el estado final.](#)

[2.6 La instrucción "\[Message Remediated\]" aparece precedida en el asunto del mensaje, como se muestra en la imagen:](#)

[2.7 La dirección de correo electrónico que escriba al configurar el módulo ESA/SMA es la que recibe los correos electrónicos corregidos al seleccionar la opción "Reenviar" o "Reenviar/Eliminar", como se muestra en la imagen:](#)

[2.8 Por último, si observa los detalles del seguimiento de mensajes de la nueva interfaz de ESA/SMA, puede ver los mismos registros obtenidos en los "mail logs" y el "Last State" como "Remediated", como se muestra en la imagen:](#)

## Introducción

Este documento describe cómo solucionar los correos electrónicos de Cisco Threat Response (CTR).

## Antecedentes

La investigación de CTR se ha actualizado para admitir OnDemand Mail Remediation. Los administradores pueden buscar correos específicos de los buzones de correo de usuario de O365 y OnPrem Exchange y remediarlos mediante un dispositivo de seguridad de correo electrónico (ESA) o un dispositivo de administración de seguridad (SMA).

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cuenta CTR
- Intercambio de servicios de seguridad de Cisco
- ESA AsyncOs 14.0.1-033

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

**Nota:** La búsqueda y la remediación de correo se admiten únicamente en implementaciones híbridas de O365, Exchange 2016 y 2019 y en implementaciones de Exchange in situ 2013.

## Configurar

1. [Configuración de la Configuración de la Cuenta en el ESA](#)
2. [Configure el perfil en cadena y asigne los dominios al perfil de cuenta](#)
3. [Integración de CTR con ESA o SMA](#)

## Verificación

Puede investigar los elementos observables en el portal CTR y seleccionar el mensaje para la remediación mediante los pasos siguientes:

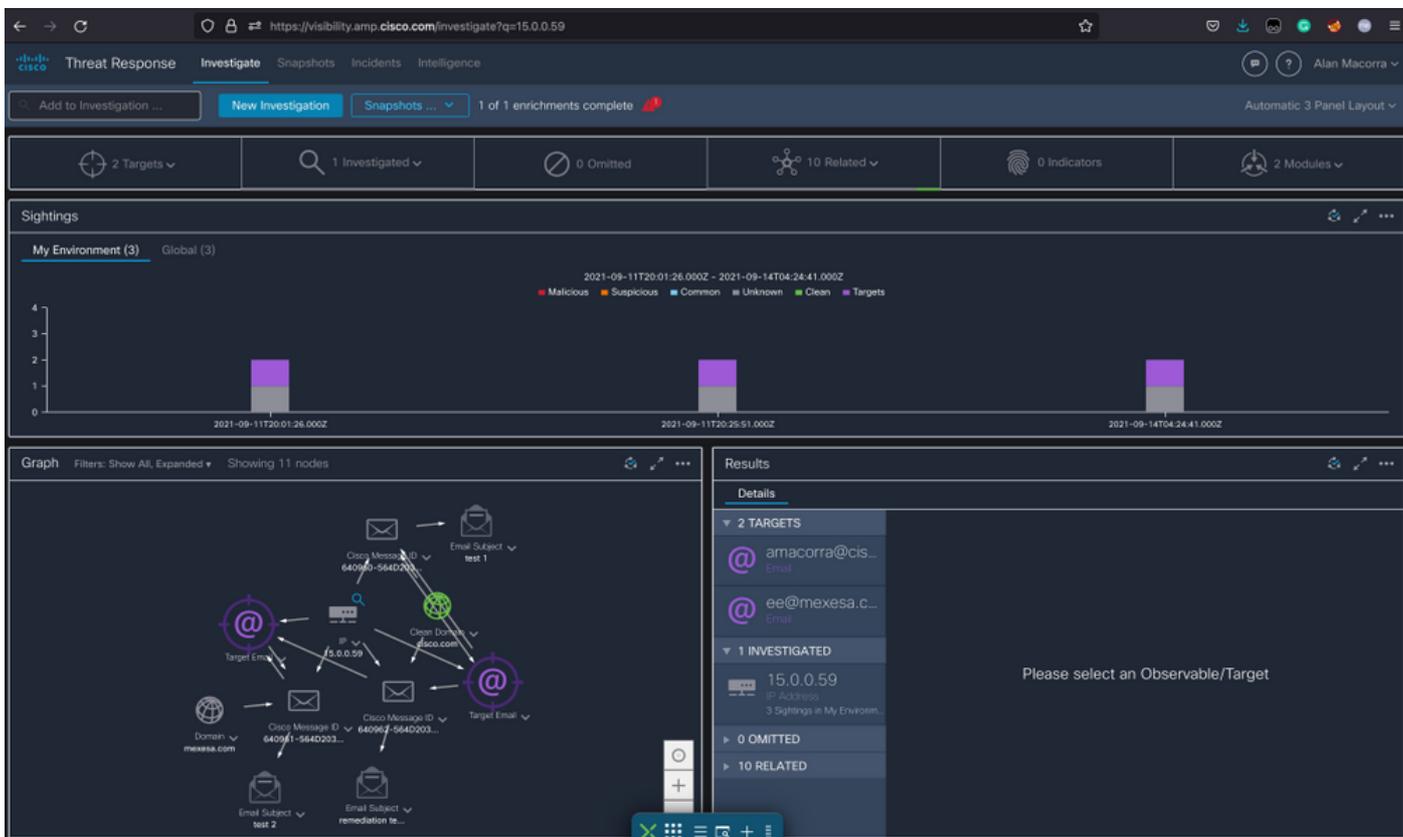
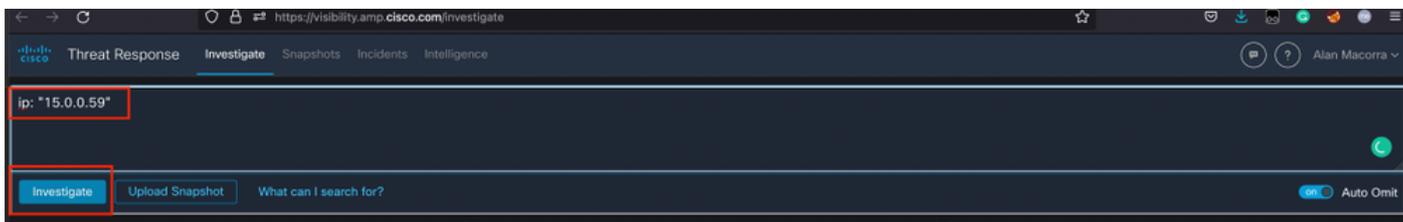
### Paso 1. Acceda al portal CTR en función del acceso a los servidores disponibles e investigue

- EE. UU. <https://visibility.amp.cisco.com/investigate>
- APJC <https://visibility.apjc.amp.cisco.com/investigate>
- UE <https://visibility.eu.amp.cisco.com/investigate>

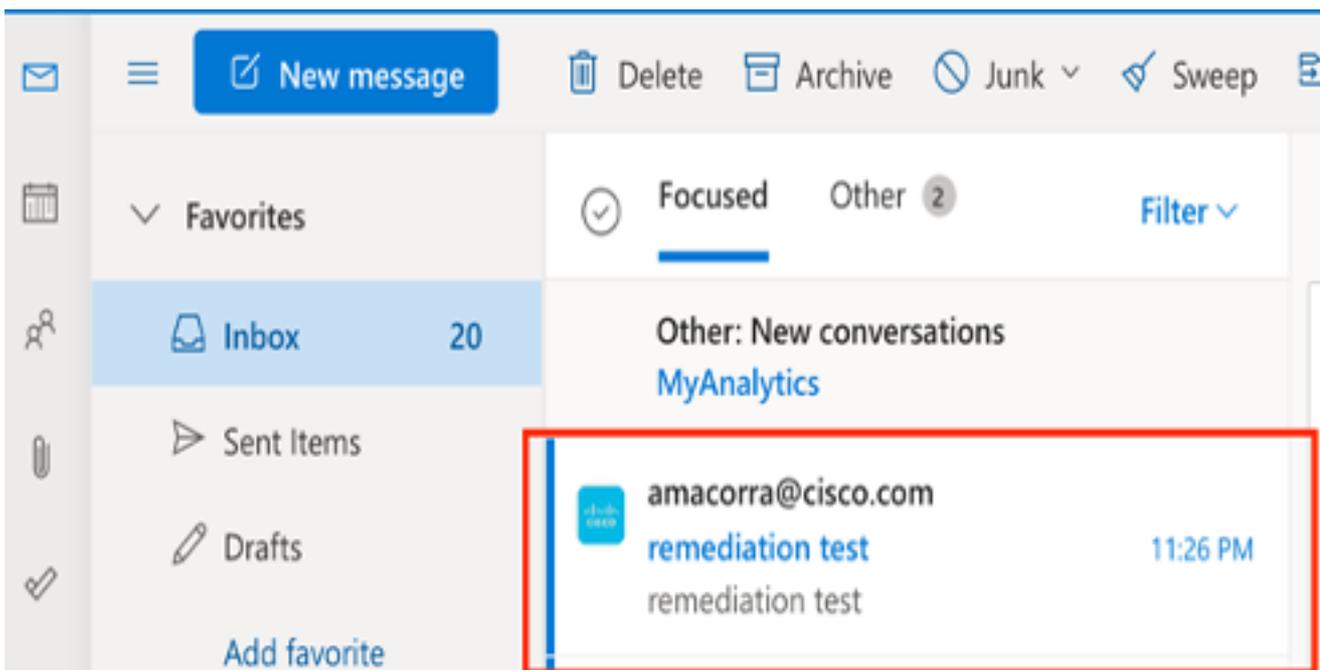
**Paso 2. Investigue los mensajes entregados que parecen ser maliciosos o una amenaza utilizando los observables admitidos. Se puede buscar en los objetos observables según los siguientes criterios, como se muestra en la imagen:**

IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file name	file_name:"invoice.pdf"

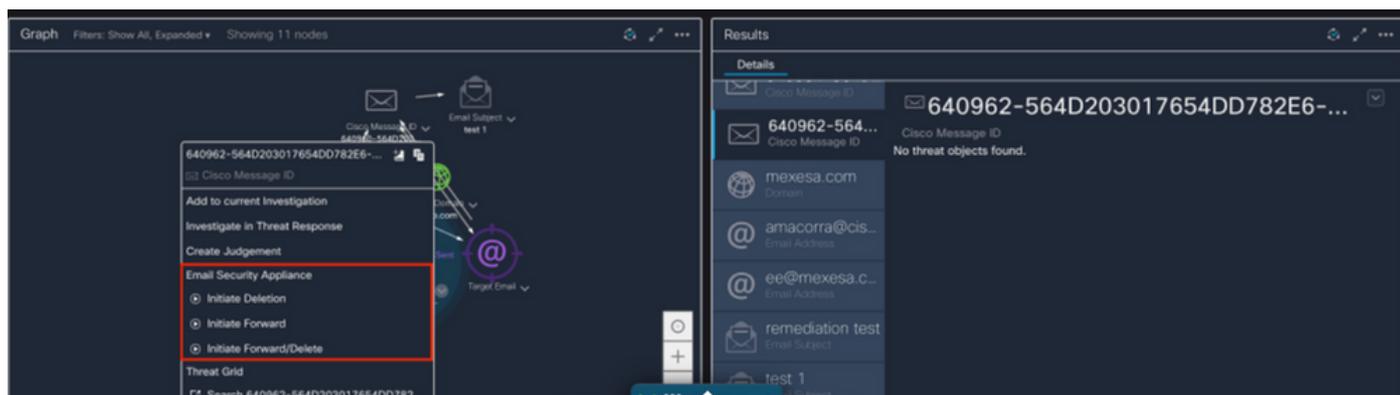
**2.1 Ejemplo de una investigación e investigación de IP a continuación, como se muestra en las imágenes:**



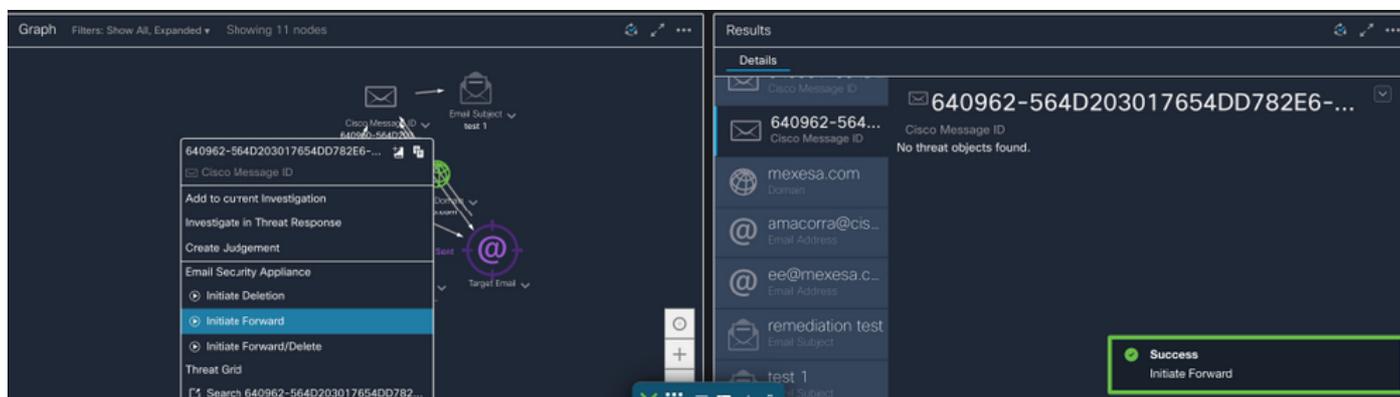
2.2 Esto es lo que obtiene en la bandeja de entrada antes de que se solucione el mensaje, como se muestra en la imagen:



2.3 Al hacer clic en "ID de mensaje de Cisco", seleccione entre las opciones de menú cualquiera de las acciones remediadas admitidas, como se muestra en la imagen:



2.4 En este ejemplo, se selecciona "Iniciar reenvío" y aparece una ventana emergente de éxito en la esquina inferior derecha, como se muestra en la imagen:

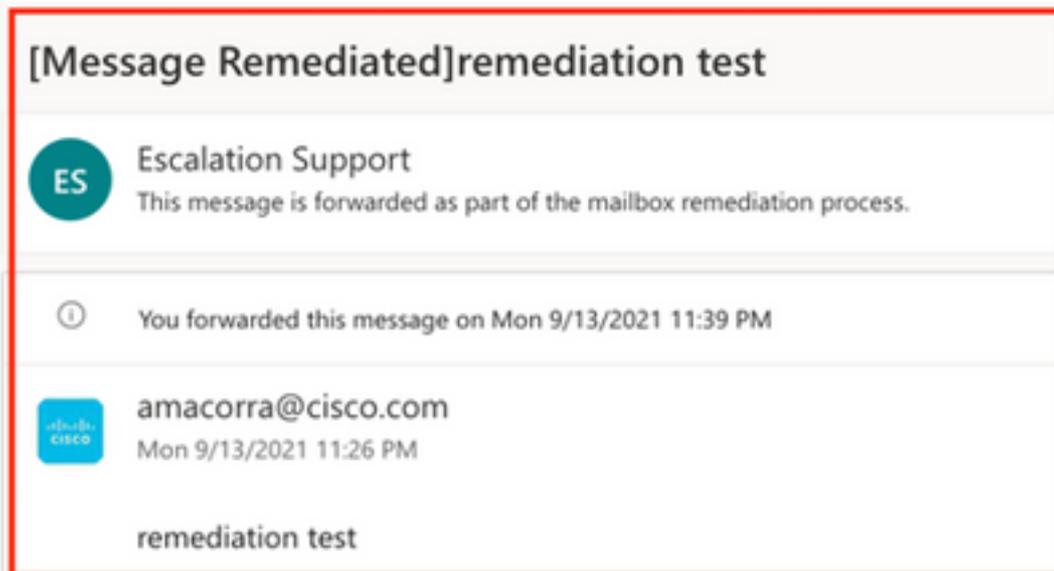


2.5 En el ESA, puede ver los siguientes registros en "mail\_logs" que muestran que se inicia la remediación "CTR", la acción seleccionada y el estado final.

```
Mon Sep 13 23:38:03 2021 Info: Message 640962 was initiated for 'Forward' remedial action by 'admin' from source 'CTR' in batch '2b46dcac-9b3d-404c-9327-f114fd5d89c7'.
```

```
Mon Sep 13 23:38:06 2021 Info: Message 640962 was processed with 'Forward' remedial action for recipient 'ee@mexesa.com' in batch '2b46dcac-9b3d-404c-9327-f114fd5d89c7'. Remediation status: Remediated.
```

2.6 La instrucción "[Message Remediated]" aparece precedida en el asunto del mensaje, como se muestra en la imagen:



2.7 La dirección de correo electrónico que escriba al configurar el módulo ESA/SMA es la que recibe los correos electrónicos corregidos al seleccionar la opción "Reenviar" o "Reenviar/Eliminar", como se muestra en la imagen:



2.8 Por último, si observa los detalles del seguimiento de mensajes de la nueva interfaz de ESA/SMA, puede ver los mismos registros obtenidos en los "mail\_logs" y el "Last State" como "Remediated", como se muestra en la imagen:

Message Tracking

Message ID Header <18fb395\$ju2@mail.sergio.com>

< Previous Next >

Processing Details

Summary

- 23:24:47 ● Start message 640962 on incoming connection (ICID 31).
- 23:24:47 ● Message 640962 enqueued on incoming connection (ICID 31) from amacorra@cisco.com.
- 23:24:47 ● Message 640962 direction: incoming
- 23:24:48 ● Message 640962 on incoming connection (ICID 31) added recipient (ee@mexesa.com).
- 23:25:07 ● Message 640962 original subject on injection: remediation test
- 23:25:07 ● Message 640962 not evaluated for Sender Domain Reputation. Reason: Disabled at Mail Flow Policy
- 23:25:07 ● Message 640962 (145 bytes) from amacorra@cisco.com ready.
- 23:25:07 ● Message 640962 has sender\_group: whitelist, sender\_ip: 15.0.0.59 and sbrs: None
- 23:25:07 ● Message 640962 matched per-recipient policy ee for inbound mail policies.
- 23:25:07 ● Message 640962 scanned by Advanced Malware Protection engine. Final verdict: SKIPPED(no attachment in message)
- 23:25:07 ● Message 640962 scanned by Outbreak Filters. Verdict: Negative
- 23:25:07 ● Message 640962 contains message ID header '<18fb395\$ju2@mail.sergio.com>'.
- 23:25:07 ● Message 640962 queued for delivery.
- 23:25:08 ● (DCID 6) Delivery started for message 640962 to ee@mexesa.com.
- 23:25:10 ● (DCID 6) Delivery details: Message 640962 sent to ee@mexesa.com
- 23:29:10 ● Message 640962 to ee@mexesa.com received remote SMTP response '2.6.0 <18fb395\$ju2@mail.sergio.com> [InternalId:27221502727676, Hostname=BY3PR19MBS169.namprd19.prod.outlook.com] 8351 bytes in 0.165, 49.369 KB/sec Queued mail for delivery'.
- 23:29:50 ● Incoming connection (ICID 31) lost.
- 23:38:03 ● Message 640962 was initiated for 'Forward' remedial action by 'admin' from source 'CTR' in batch '2b46dcdf-9b3d-404c-9327-f114fd5d89c7'.
- 23:38:06 ● Message 640962 was processed with 'Forward' remedial action for recipient 'ee@mexesa.com' in batch '2b46dcdf-9b3d-404c-9327-f114fd5d89c7'. Remediation status: Remediated.

Envelope Header and Summary

Last State  
**Remediated**

Message  
 Incoming

MID  
 640962

Time  
 13 Sep 2021 23:24:41 (GMT -05:00)

Sender  
 amacorra@cisco.com

Recipient  
 ee@mexesa.com

Subject  
 remediation test

Sender Group  
 whitelist

Cisco Hostname  
 (Name unresolved, SN:564D203017654DD782E6-AD81CB8ECD45)

Incoming Policy Match  
 ee

Message Size  
 145 (Bytes)

Attachments  
 N/A

Sending Host Summary

Reverse DNS hostname  
 (unverified)

IP address  
 15.0.0.59

SIBRS Score  
 None

**Nota:** Pueden ocurrir varias soluciones, si configura en su ESA/SMA la función para buscar y remediar, puede remediar el mismo mensaje de CTR y también de ESA/SMA. Esto puede permitirle reenviar el mismo mensaje a una dirección de correo electrónico diferente a la configurada en el [módulo de integración](#).