

# E-mails van CTR verhelpen

## Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Gebruikte componenten](#)

[Configureren](#)

[Verificatie](#)

[Stap 1. Toegang tot het CTR-portal op basis van de toegang tot beschikbare servers en onderzoek](#)

[Stap 2. Onderzoek de geleverde berichten die kwaadaardig of bedreigend lijken te zijn door gebruik te maken van de ondersteunde wachtwoorden. De waarnemingen kunnen aan de hand van de volgende criteria worden bezocht, zoals in de afbeelding wordt getoond:](#)

[2.1 Onderstaand een voorbeeld van een onderzoek en onderzoek in het kader van het OT, zoals blijkt uit de beelden:](#)

[2.2 Dit krijgt u in uw inbox voordat het bericht wordt hersteld, zoals in de afbeelding wordt getoond:](#)

[2.3 Selecteer in het menu-opties een van de ondersteunde bewerkingsacties zoals in de afbeelding:](#)

[2.4 In dit voorbeeld wordt "Vooruit openen" geselecteerd en verschijnt een Success pop-up-venster in de rechterbenedenhoek, zoals in de afbeelding:](#)

[2.5 In het ESA, kunt u de volgende logbestanden zien onder "mail logs" die laten zien dat het "CTR"-herstel start, de geselecteerde actie en de definitieve status.](#)

[2.6 Het bericht "\[Bericht geremedieerd\]" wordt in het bericht voorgedrukt, zoals in de afbeelding weergegeven:](#)

[2.7 Het e-mailadres dat u typt bij het configureren van de ESA/SMA-module, is het e-mailadres dat u ontvangt wanneer u de optie "Voorwaarts" of "Voorwaarts/Verwijderen" selecteert, zoals in de afbeelding wordt weergegeven:](#)

[2.8 Ten slotte, als je kijkt naar de informatie-tracking details van de nieuwe interface van de ESA/SMA, dan zie je dezelfde logbestanden die zijn verkregen in "mail logs" en "Laatste Staat" als "Geremedieerd", zoals in de afbeelding getoond wordt:](#)

## Inleiding

Dit document beschrijft hoe u e-mails van Cisco Threat Response (CTR) kunt verbeteren.

## Achtergrondinformatie

Het CTR-onderzoek is bijgewerkt om de correctie van OnDemand Mail te ondersteunen. Admin kan specifieke e-mails van O365 en OnPrem Exchange-gebruikersmailboxes doorzoeken en deze herstellen door een e-mail security applicatie (ESA) of security Management-applicatie (SMA).

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CTR-account
- Cisco Security Services exchange
- ESR AS 14.0.1-033

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

**Opmerking:** Zoeken en mailverbetering wordt alleen ondersteund in O365, Exchange 2016 & 2019 Hybrid-implementaties en On-Prem 2013 Exchange implementaties.

## Configureren

1. [Accountinstellingen instellen in de ESA](#)
2. [Geketend profiel configureren en de domein\(en\) in kaart brengen naar het accountprofiel](#)
3. [Integreren met CTR of ESA of SMA](#)

## Verificatie

U kunt de observeermiddelen in het CTR-portal onderzoeken en het bericht voor herstel selecteren in de volgende stappen:

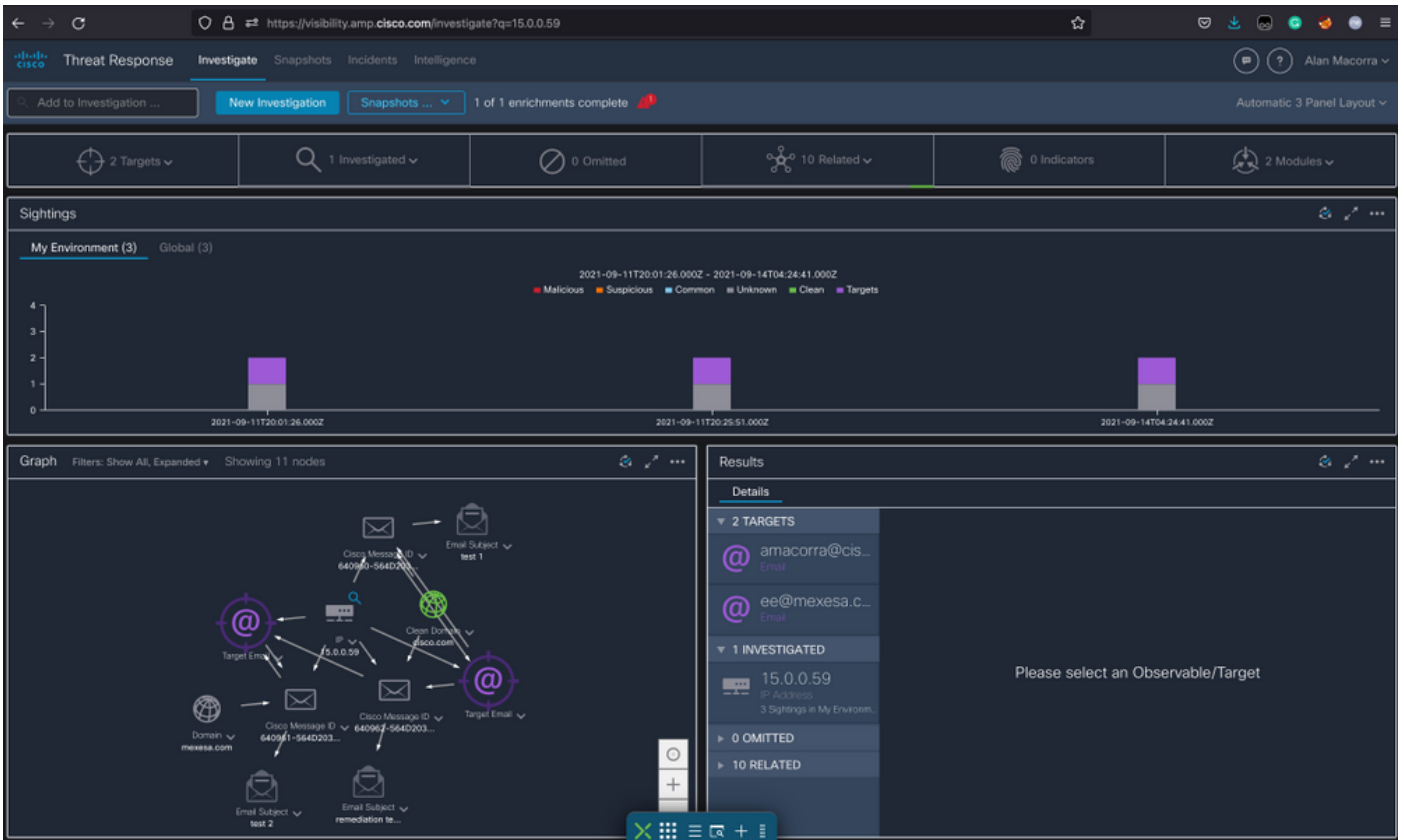
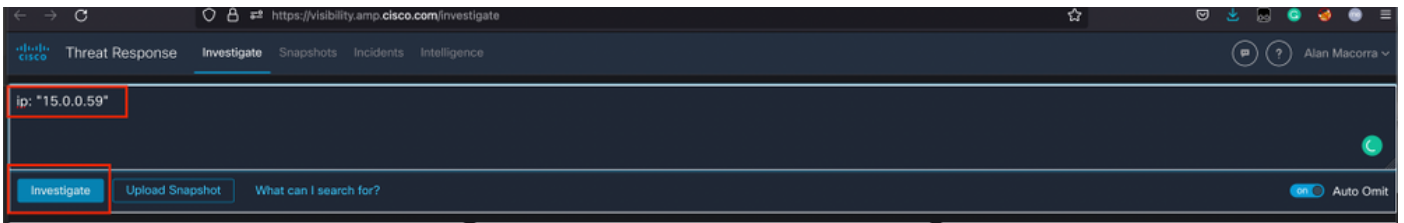
### Stap 1. Toegang tot het CTR-portal op basis van de toegang tot beschikbare servers en onderzoek

- VS <https://visibility.amp.cisco.com/investigate>
- APJC <https://visibility.apjc.amp.cisco.com/investigate>
- EU <https://visibility.eu.amp.cisco.com/investigate>

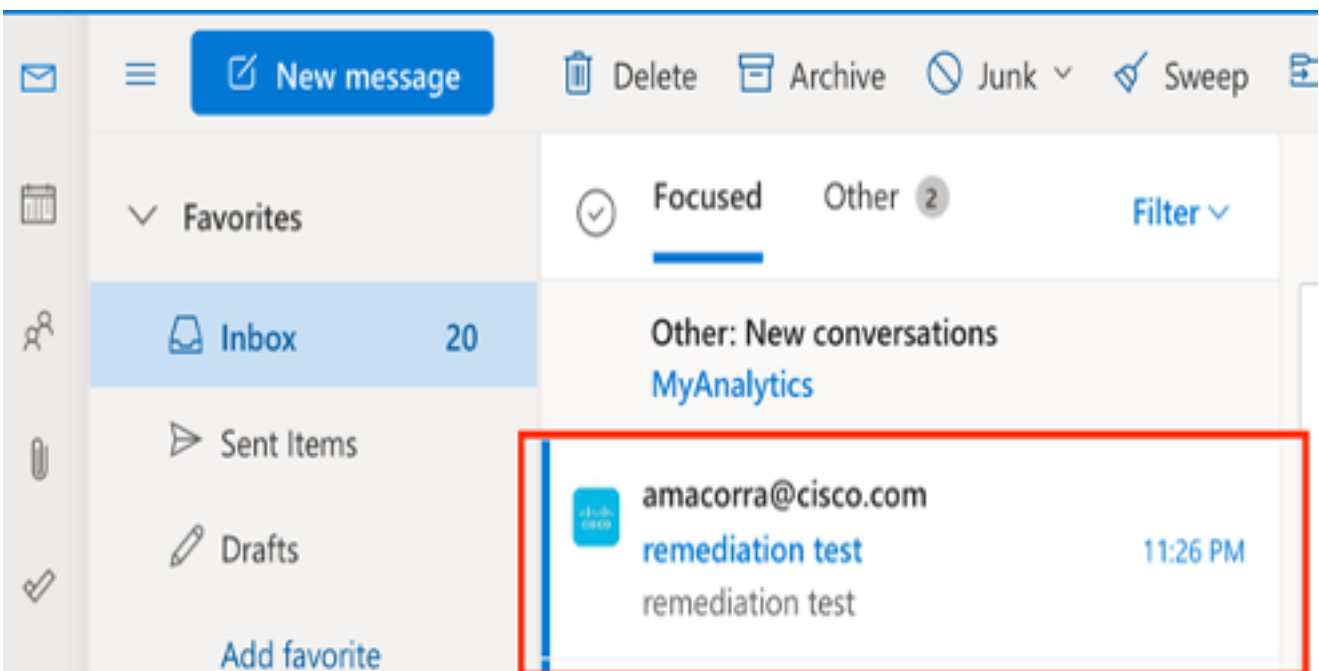
Stap 2. Onderzoek de geleverde berichten die kwaadaardig of bedreigend lijken te zijn door gebruik te maken van de ondersteunde wachtwoorden. De waarnemingen kunnen aan de hand van de volgende criteria worden bezocht, zoals in de afbeelding wordt getoond:

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"

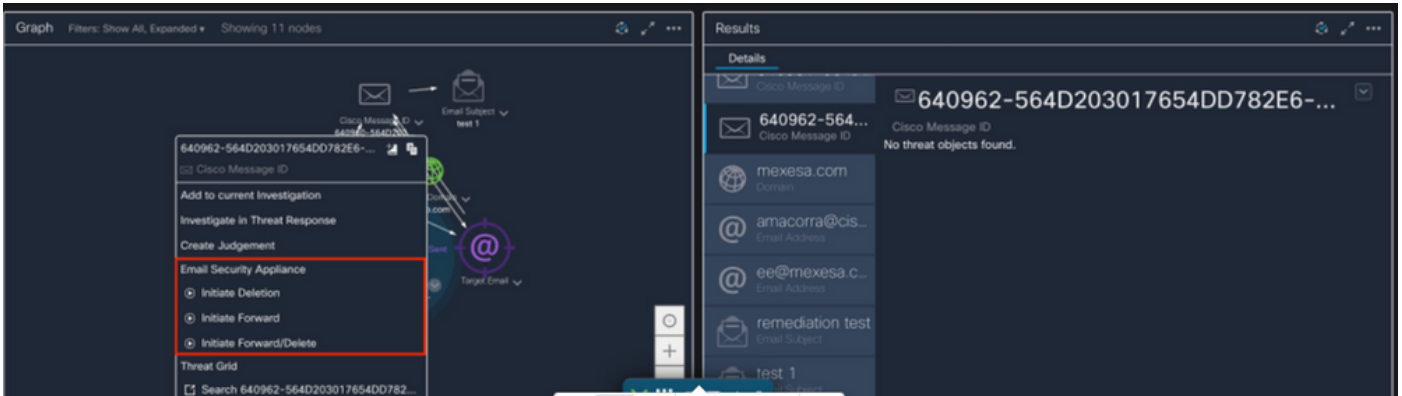
2.1 Onderstaand een voorbeeld van een onderzoek en onderzoek in het kader van het OT, zoals blijkt uit de beelden:



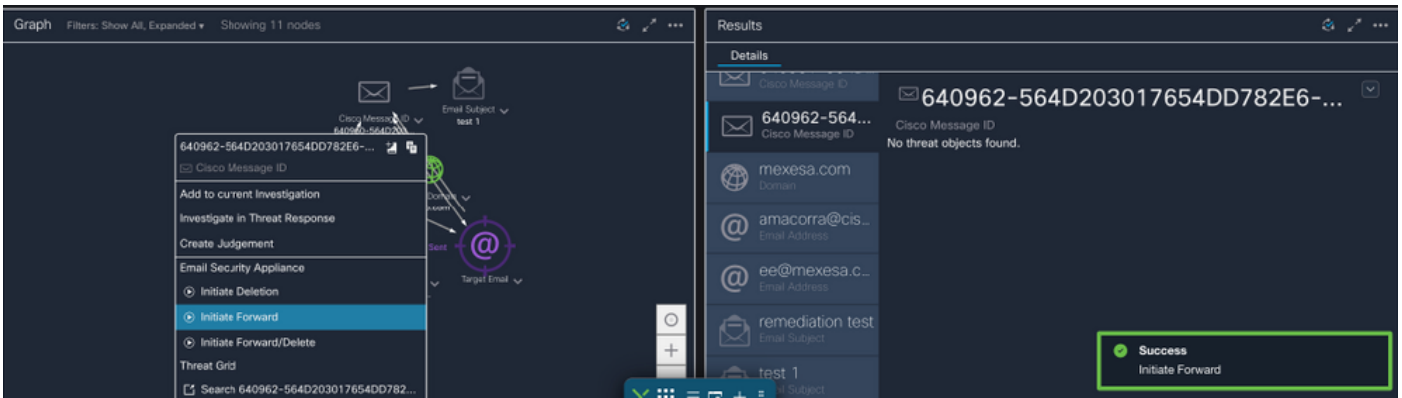
2.2 Dit krijgt u in uw inbox voordat het bericht wordt hersteld, zoals in de afbeelding wordt getoond:



2.3 Selecteer in het menu-opties een van de ondersteunde bewerkingsacties zoals in de afbeelding:



2.4 In dit voorbeeld wordt "Vooruit openen" geselecteerd en verschijnt een Success pop-up venster in de rechterbenedenhoek, zoals in de afbeelding:

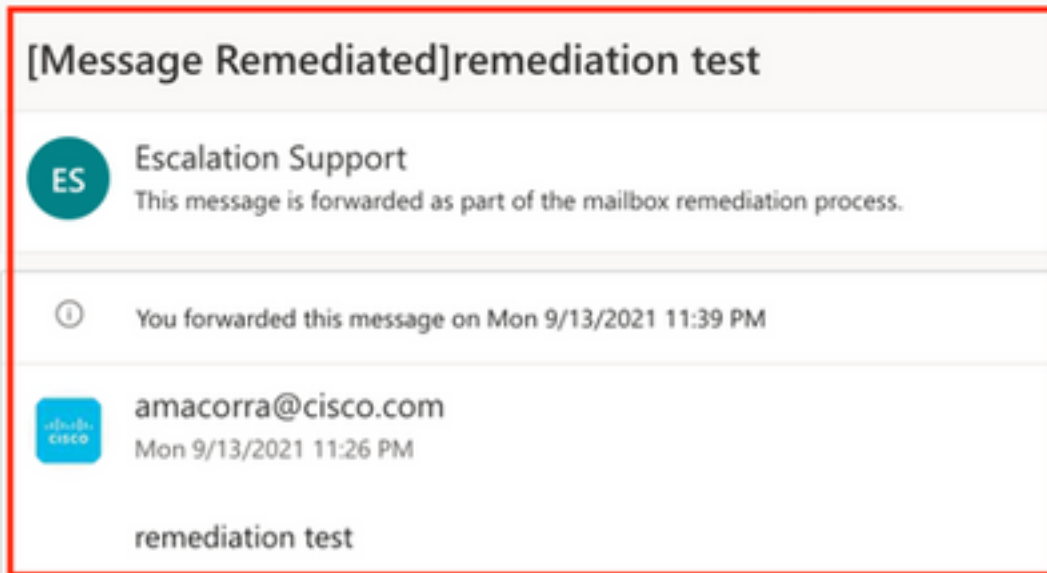


2.5 In het ESA, kunt u de volgende logbestanden zien onder "mail\_logs" die laten zien dat het "CTR"-herstel start, de geselecteerde actie en de definitieve status.

```
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 Het bericht "[Bericht geremedieerd]" wordt in het bericht voorgedrukt, zoals in de afbeelding weergegeven:



2.7 Het e-mailadres dat u typt bij het configureren van de ESA/SMA-module, is het e-mailadres dat u ontvangt wanneer u de optie "Voorwaarts" of "Voorwaarts/Verwijderen" selecteert, zoals in de afbeelding wordt weergegeven:



2.8 Ten slotte, als je kijkt naar de informatie-tracking details van de nieuwe interface van de ESA/SMA, dan zie je dezelfde logbestanden die zijn verkregen in "mail\_logs" en "Laatste Staat" als "Geremedieerd", zoals in de afbeelding getoond wordt:

Message Tracking

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

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

Copyright X Home + Privacy Statement

**Opmerking:** Er kunnen verschillende corrigerende maatregelen worden genomen. Als u de functie in uw ESA/SMA instelt om te zoeken en te verbeteren, dan kunt u hetzelfde bericht corrigeren vanaf CTR en ook via ESA/SMA. Hierdoor kunt u hetzelfde bericht doorsturen naar een ander e-mailadres dan het bericht dat in de [integratiemodule](#) is ingesteld.