How to Remediate Emails from CTR

Contents

Introduction

This document describes how to remediate emails from Cisco Threat Response (CTR).

Background Information

CTR investigation has been updated to support OnDemand Mail Remediation. Admin can search specific emails from O365 and OnPrem Exchange user mailboxes and remediate them through an Email Security Appliance (ESA) or Security Management Appliance (SMA).

Components Used

The information in this document is based on these software and hardware versions:

- CTR Account
- Cisco Security Services Exchange
- ESA AsycnOs 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. If your network is live, ensure that you understand the potential impact of any command.

> **Note**: Search and Mail Remediation is supported in O365, Exchange 2016 & 2019 Hybrid Deployments, and On-Prem 2013 Exchange Deployments only.

Configure

1. Configure Account Settings in the ESA
2. Configure Chained Profile and Map the Domain(s) to the Account Profile
3. Integrate CTR with either ESA or SMA

Verification

You can investigate the observables in the CTR Portal and select the message for remediation using the below steps:

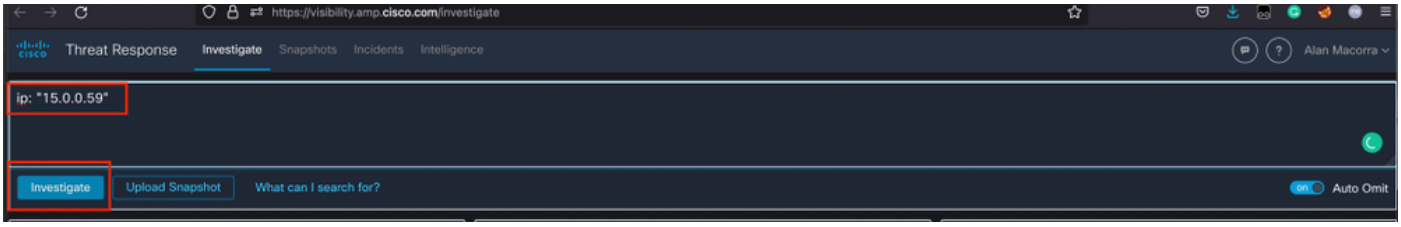
Step 1. Access the CTR Portal based on the access to available servers and investigate

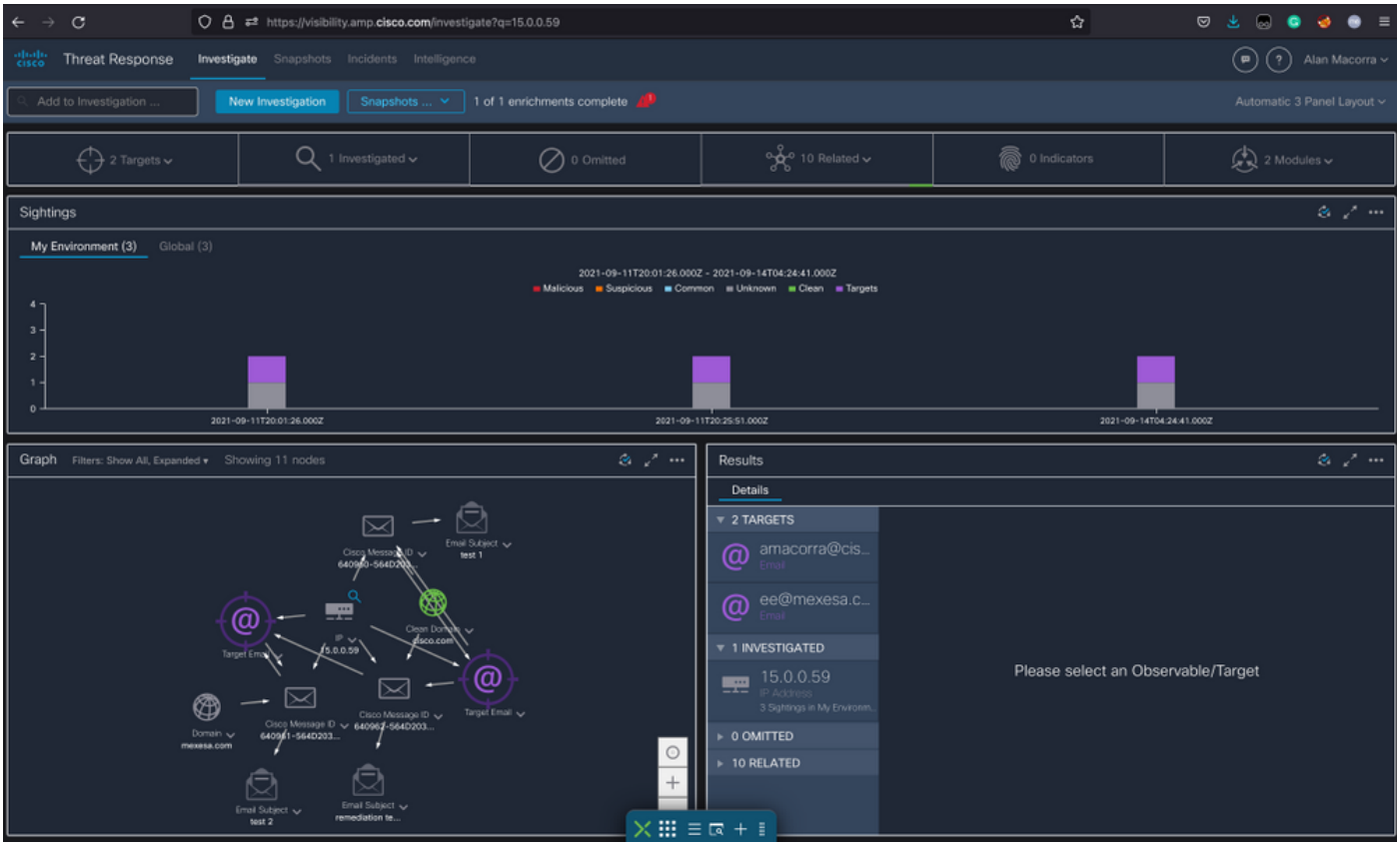
- US https://visibility.amp.cisco.com/investigate
- APJC https://visibility.apjc.amp.cisco.com/investigate
- EU https://visibility.eu.amp.cisco.com/investigate

Step 2. Investigate the delivered messages that seem to be malicious or a threat by using the supported observables. Observables can be searched by the following criteria, as shown in the image:

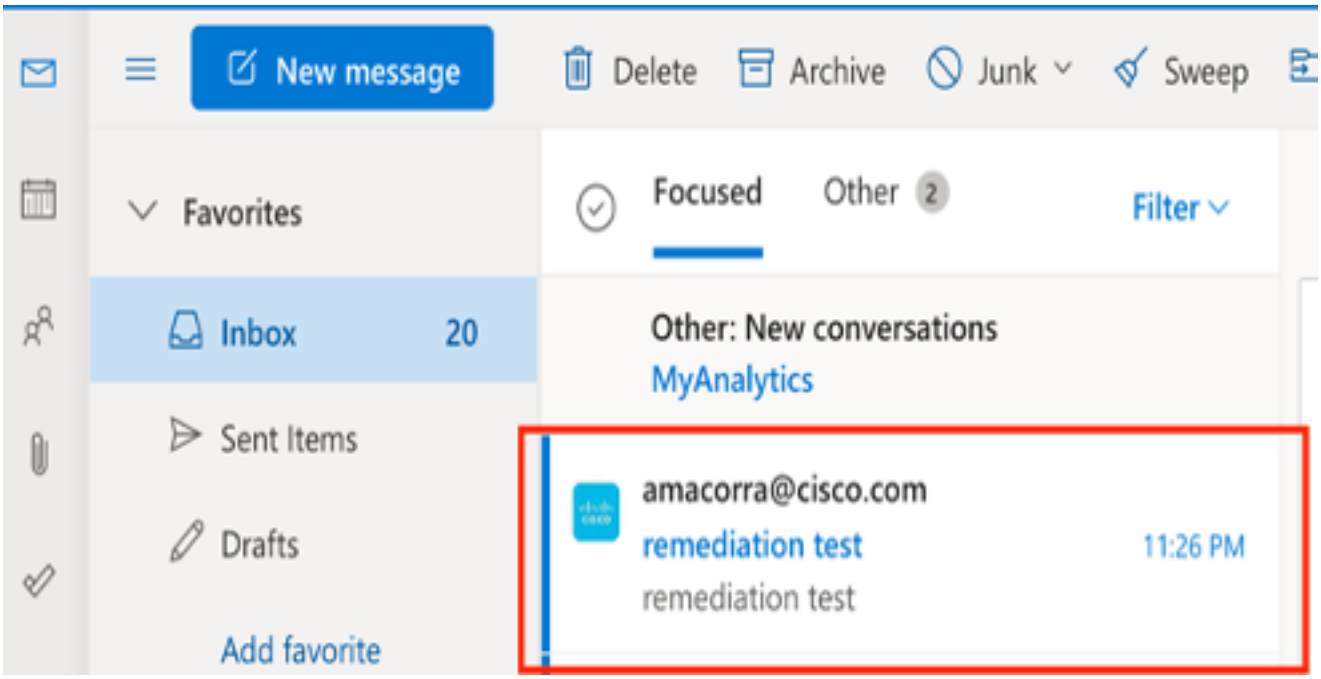
IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file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

2.1 An example of an IP investigation and Investigation below, as shown in the images:

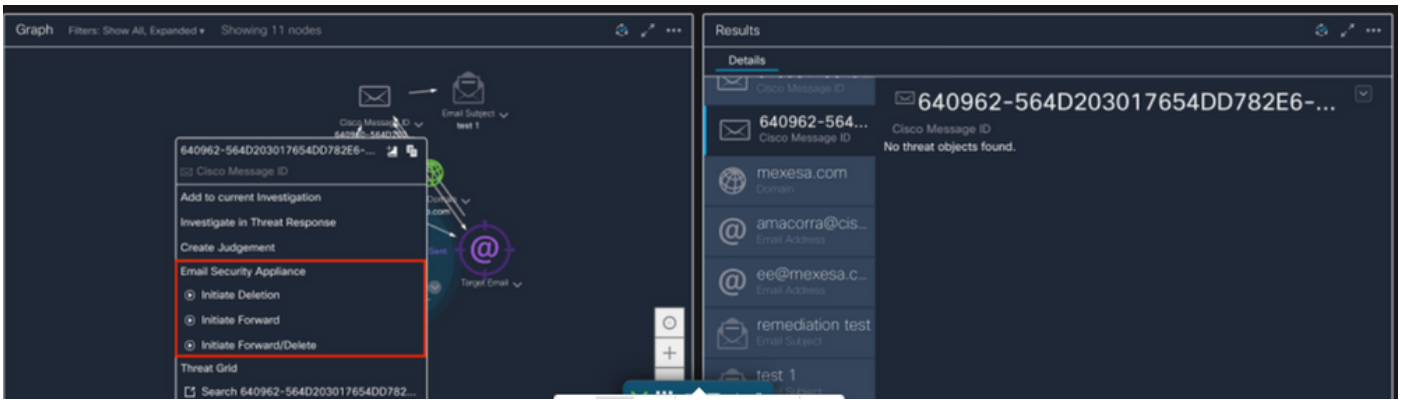




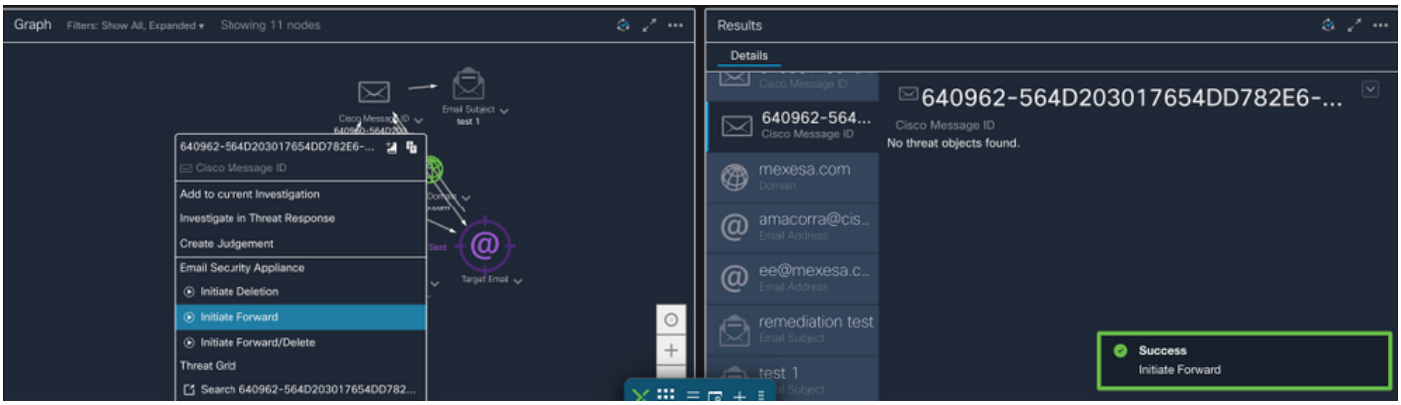
2.2 Here is what you get in your inbox before the message gets remediated, as shown in the image:



2.3 On clicking "Cisco Message ID", select from menu options any of the supported Remediated Actions, as shown in the image:



2.4 In this example, "Initiate Forward" is selected and a Success popup window appears in the lower right corner, as shown in the image:

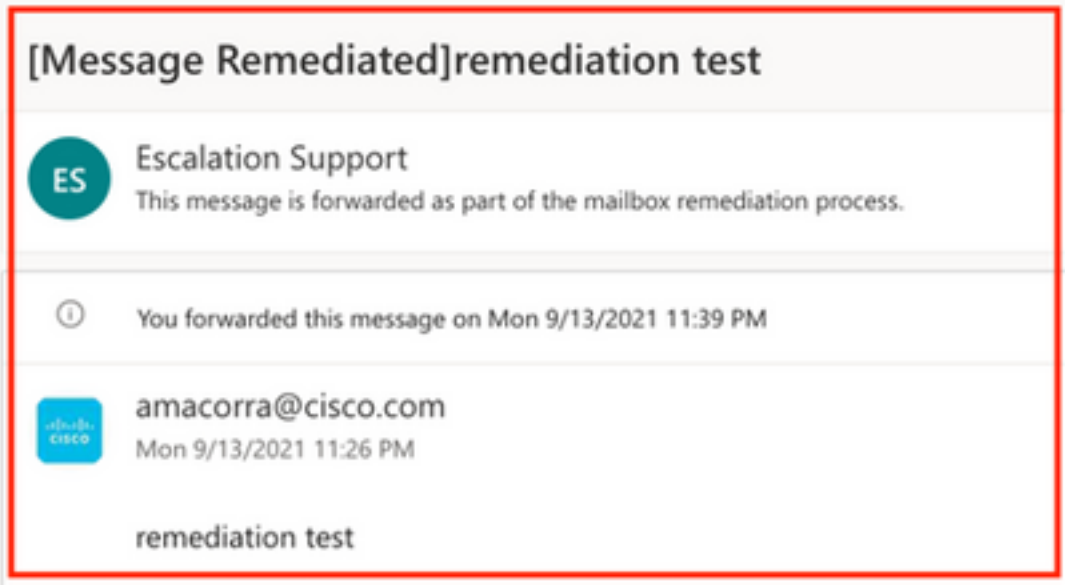


2.5 In the ESA, you can see the following logs under "mail_logs" that show that the "CTR" remediation initiates, the action selected, and the final status.

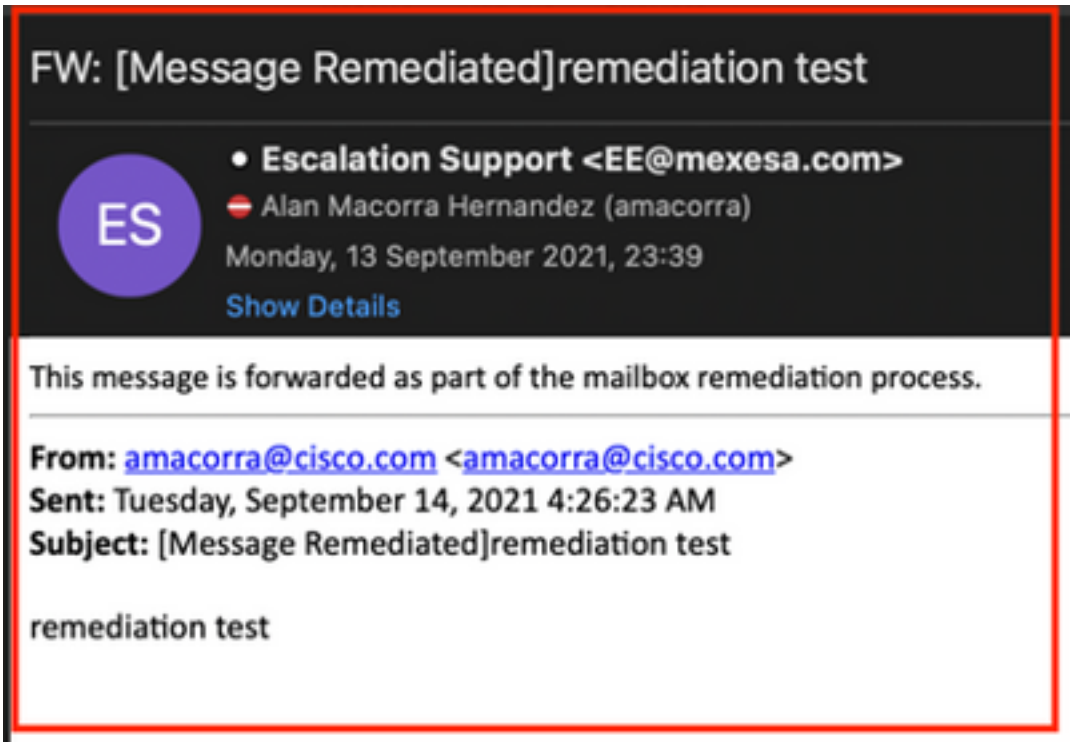
```
Mon Sep 13 23:38:03 2021 Info: Message 640962 was initiated for 'Forward' remedial action by
'admin' from source 'CTR' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89c7'.

Mon Sep 13 23:38:06 2021 Info: Message 640962 was processed with 'Forward' remedial action for
recipient 'ee@mexesa.com' in batch '2b46dcaf-9b3d-404c-9327-f114fd5d89c7'. Remediation status:
Remediated.
```

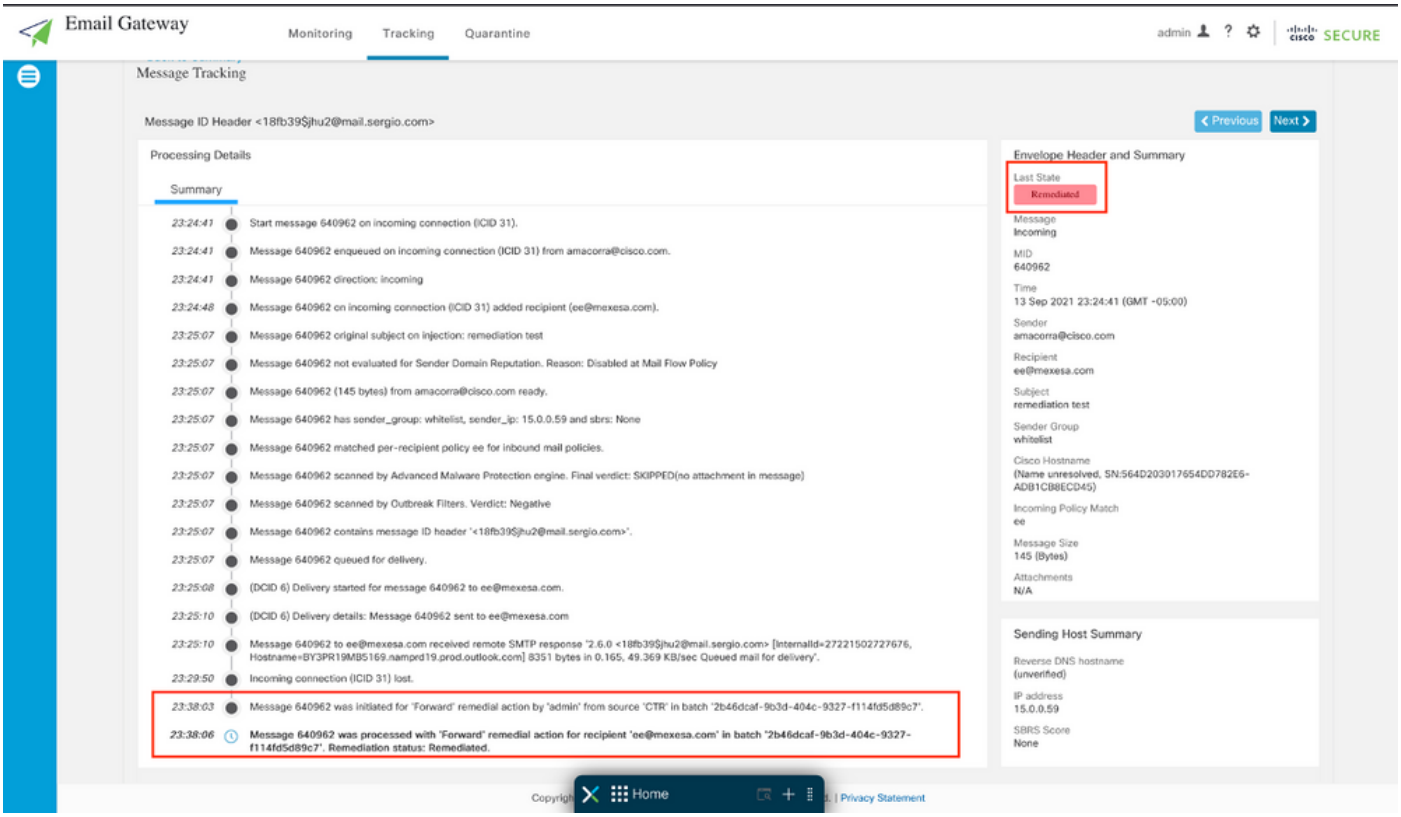
2.6 The statement "[Message Remediated]" appears prepended in the subject of the message, as shown in the image:



2.7 The email address you type in when configuring the ESA/SMA module is the one that receives the remediated emails when selecting the "Forward" or "Forward/Delete" option, as shown in the image:



2.8 Finally, if you look at the message tracking details of the new interface of the ESA/SMA, you can see the same logs obtained in the "mail_logs" and the "Last State" as "Remediated", as shown in the image:



Note: Several remediations can happen, if you configure in your ESA/SMA the feature to search and remediate, you can remediate the same message from CTR and also from ESA/SMA. This can allow you to forward the same message to a different email address than the one configured in the integration module.