

CTRからの電子メールの修復方法

内容

[概要](#)

[背景説明](#)

[使用するコンポーネント](#)

[設定](#)

[確認](#)

[ステップ1：使用可能なサーバへのアクセスに基づいてCTRポータルにアクセスし、](#)

[ステップ2：サポートされている回答を使用して、悪意のあるメッセージや脅威と思われるメッセージを調査します。回答は、図に示すように、次の基準で検索できます。](#)

[2.1次の図に示すように、IP調査と調査の例を示します。](#)

[2.2次の図に示すように、メッセージが修復される前に受信トレイに表示されるものは次のとおりです。](#)

[2.3 \[Cisco Message ID \(シスコメッセージID \) \]をクリックし、次の図に示すように、サポートされている修復アクションのいずれかをメニューオプションから選択します。](#)

[2.4この例では、「Initiate Forward」が選択され、図に示すように、右下隅にSuccessポップアップウィンドウが表示されます。](#)

[2.5 ESAでは、「mail logs」の下に、「CTR」修復が開始したこと、選択されたアクション、および最終ステータスを示す次のログが表示されます。](#)

[2.6図に示すように、メッセージの件名の前に「\[Message Remediated\]」という文が表示されます。](#)

[2.7 ESA/SMAモジュールを設定するときに入力する電子メールアドレスは、「転送」または「転送/削除」オプションを選択したときに修復された電子メールを受信する電子メールアドレスです \(図を参照 \) 。](#)

[2.8最後に、ESA/SMAの新しいインターフェイスのメッセージトラッキングの詳細を見ると、図に示すように、「mail logs」と「Last State」で取得したものと同一ログが「Remediated」として表示されます。](#)

概要

このドキュメントでは、Cisco Threat Response(CTR)から電子メールを修復する方法について説明します。

背景説明

CTR調査は、オンデマンドメール修復をサポートするように更新されています。管理者は、O365およびOnPrem Exchangeのユーザメールボックスから特定の電子メールを検索し、Eメールセキュリティアプライアンス(ESA)またはセキュリティ管理アプライアンス(SMA)を介してそれらを修復できます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CTRアカウント
- Cisco Security Services Exchange
- ESA AsyncOs 14.0.1-033

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

注：検索とメールの修復は、O365、Exchange 2016および2019ハイブリッド展開、およびオンプレミスの2013 Exchange展開でのみサポートされます。

設定

1. [ESAでのアカウント設定](#)
2. [チェーンプロファイルの設定とドメインのアカウントプロファイルへのマッピング](#)
3. [CTRをESAまたはSMAと統合](#)

確認

CTRポータルで回答を調査し、次の手順を使用して修復のメッセージを選択できます。

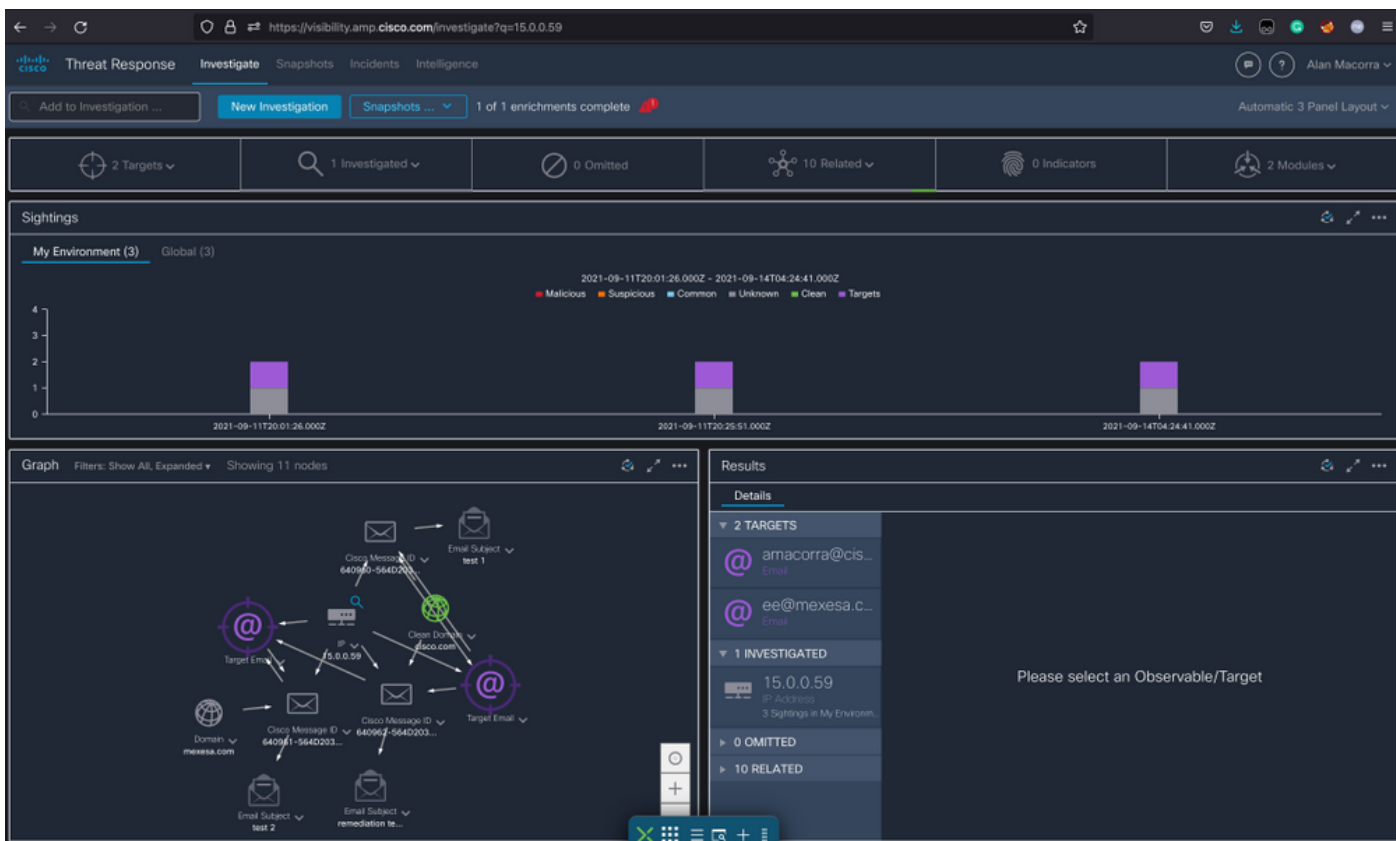
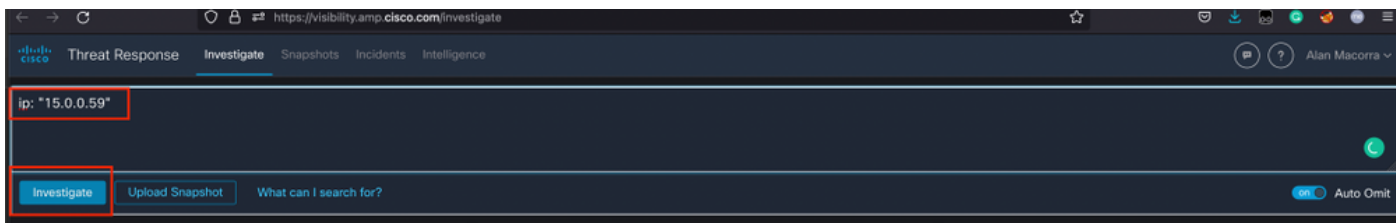
ステップ1：使用可能なサーバへのアクセスに基づいてCTRポータルにアクセスし、

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

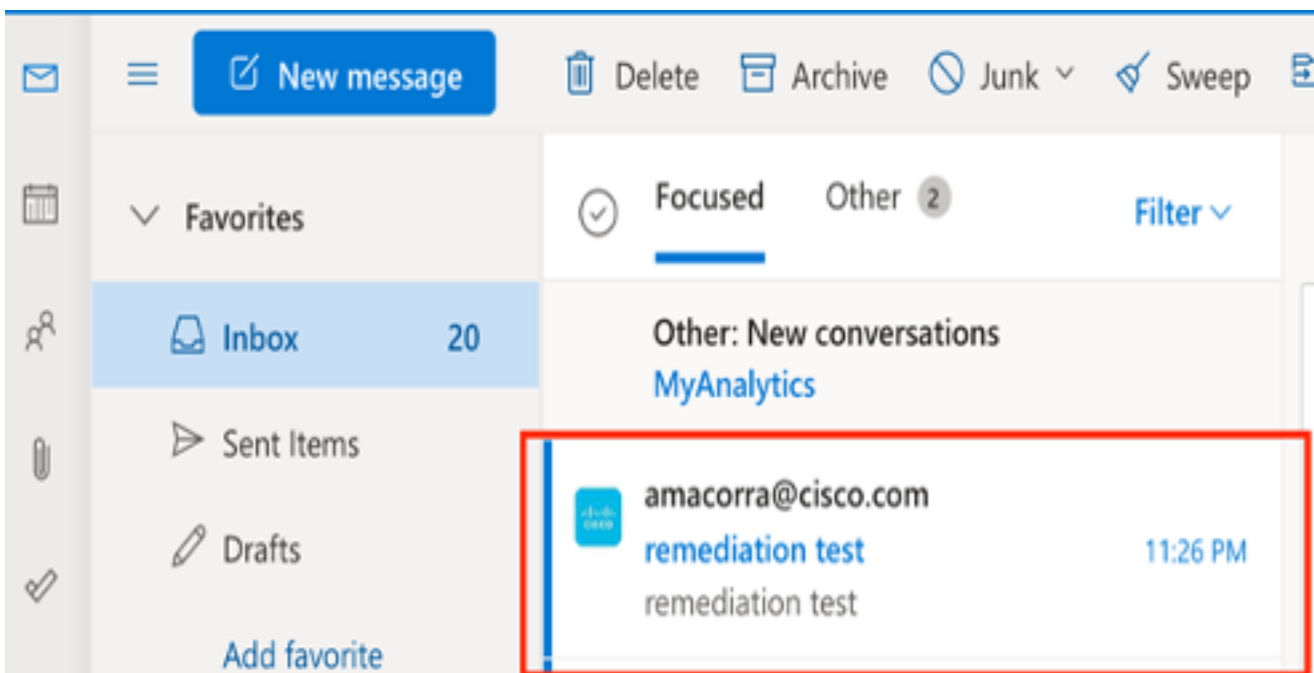
ステップ2：サポートされている回答を使用して、悪意のあるメッセージや脅威と思われるメッセージを調査します。回答は、図に示すように、次の基準で検索できます。

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"

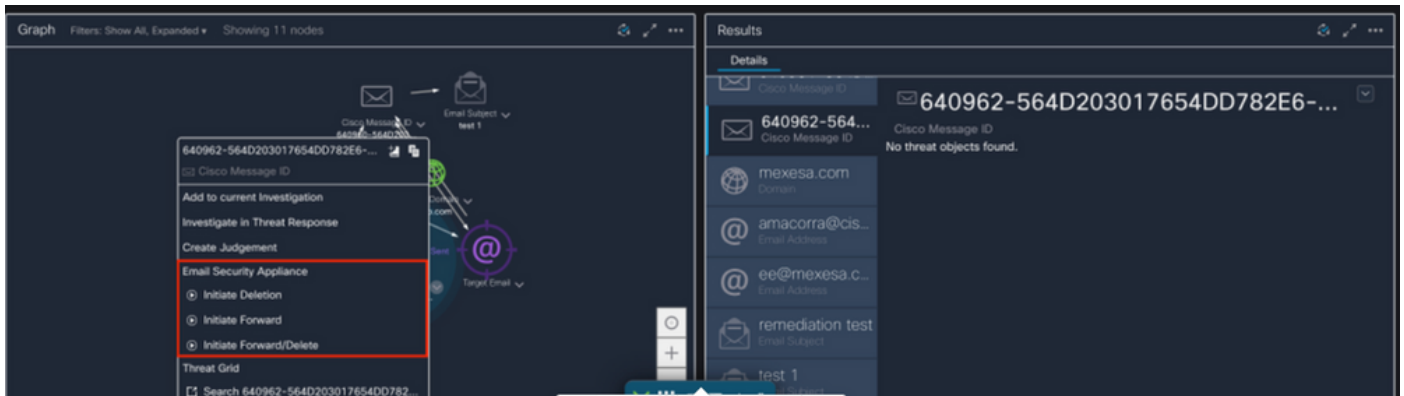
2.1次の図に示すように、IP調査と調査の例を示します。



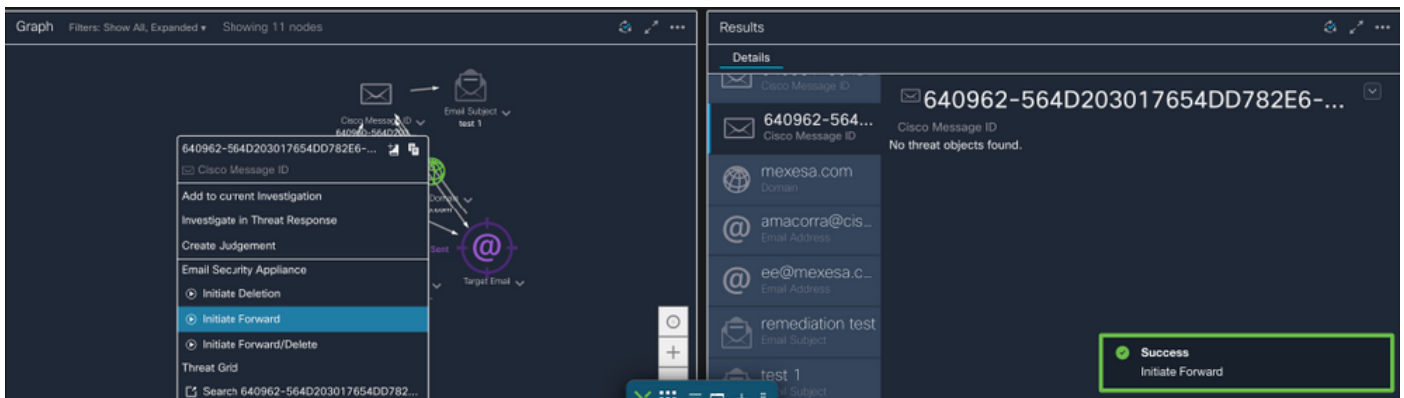
2.2次の図に示すように、メッセージが修復される前に受信トレイに表示されるものは次のとおりです。



2.3 [Cisco Message ID (シスコメッセージID)]をクリックし、次の図に示すように、サポートされている修復アクションのいずれかをメニューオプションから選択します。



2.4この例では、「Initiate Forward」が選択され、図に示すように、右下隅にSuccessポップアップウィンドウが表示されます。

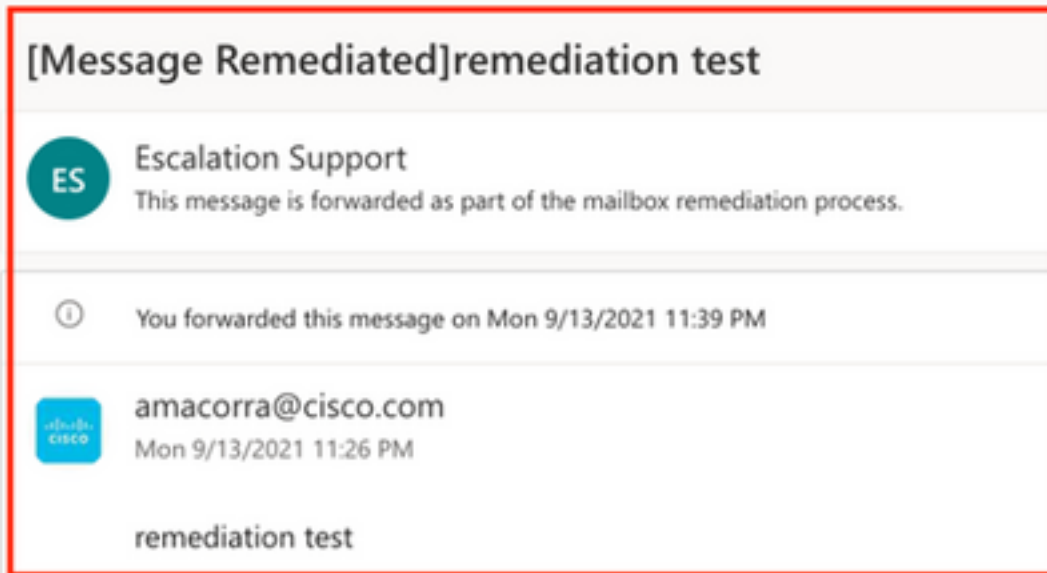


2.5 ESAでは、「mail_logs」の下に、「CTR」修復が開始したこと、選択されたアクション、および最終ステータスを示す次のログが表示されます。

```
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図に示すように、メッセージの件名の前に「[Message Remediated]」という文が表示されます。



2.7 ESA/SMAモジュールを設定するときに入力する電子メールアドレスは、「転送」または「転送/削除」オプションを選択したときに修復された電子メールを受信する電子メールアドレスです (図を参照)。



2.8最後に、ESA/SMAの新しいインターフェイスのメッセージトラッキングの詳細を見ると、図に示すように、「mail_logs」と「Last State」で取得したものと同一ログが「Remediated」として表示されます。

Message Tracking

Message ID Header <18fb395jhu2@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 '<18fb395jhu2@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 <18fb395jhu2@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

注：ESA/SMAで検索と修復の機能を設定すると、CTRとESA/SMAから同じメッセージを修復できます。これにより、統合モジュールで設定した電子メールアドレスとは異なる電子メールアドレスに同じメッセージを転送できます。