Cisco Threat Response(CTR)とESAの統合

内容

概要

このドキュメントでは、Cisco Threat Response(CTR)をEメールセキュリティアプライアンス(ESA)と統合するプロセスと、CTR調査を実行するためにこれを検証する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Threat Response
- E メール セキュリティ アプライアンス

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
- ソフトウェアバージョン13.0.0-392上のESA C100V

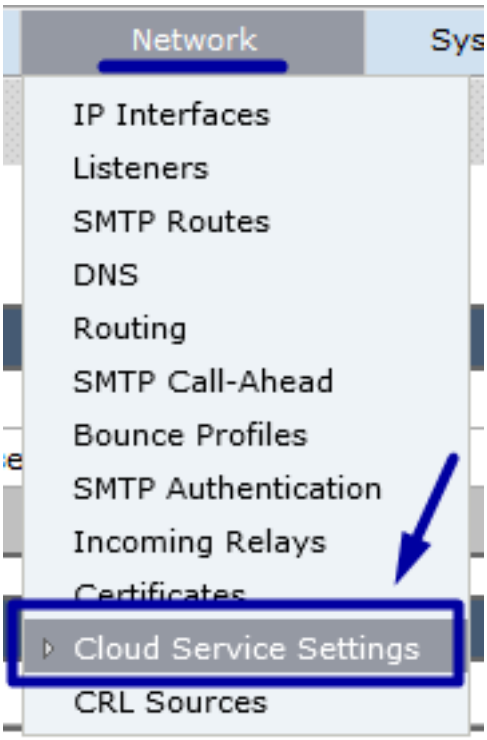
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

統合CTRとESAを設定するには、Eメールセキュリティ仮想アプライアンス(ESA)にログインし、次の手順に従います。

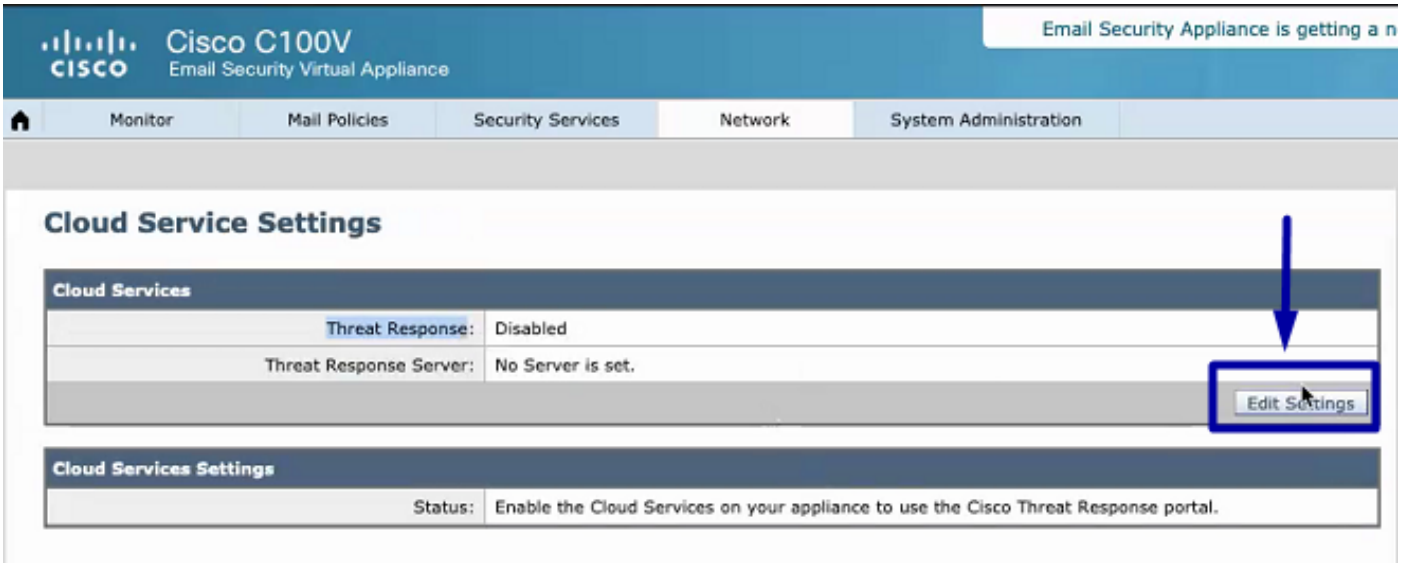
ステップ 1： [Network] > [Cloud Service Settings]に移動します

ESAで、コンテキストメニュー[Network] > [Cloud Service Settings]に移動し、図に示すように現在の[Threat Response Status (Disabled / Enabled)]を表示します。



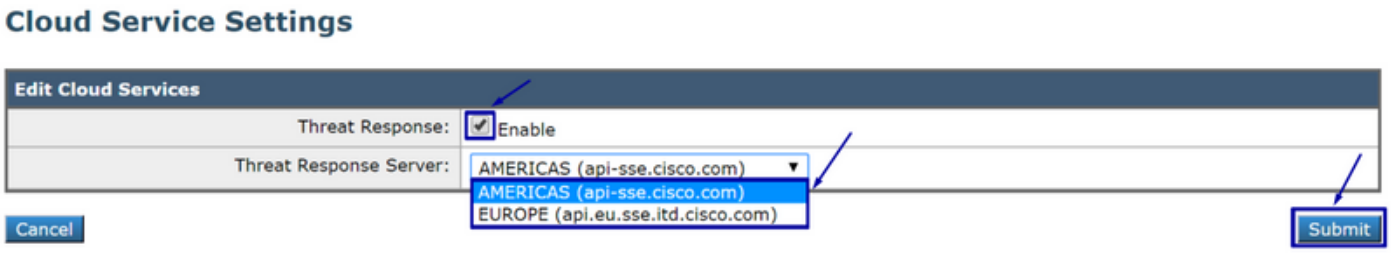
ステップ2:[Edit Settings]をクリックします

ESAの脅威応答機能が無効になるまで、この機能を有効にするには、図に示すように[Edit Settings]をクリックします。



ステップ3:[Enable]チェックボックスと[Threat Response Server]チェックボックスをオンにします

[Enable]チェックボックスをオンにしてから、[Threat Response Server]を選択します。次の図を参照してください。

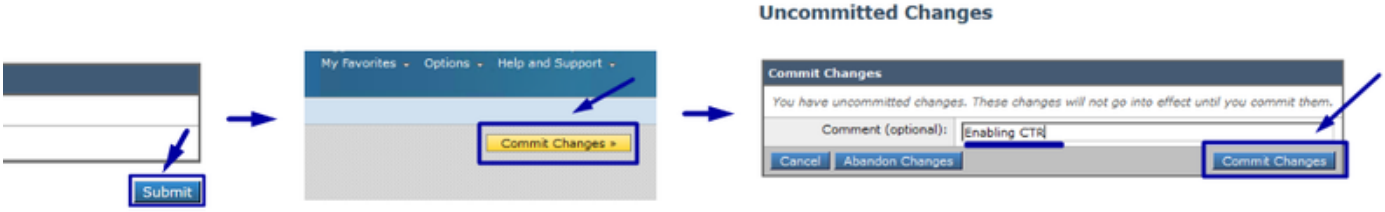


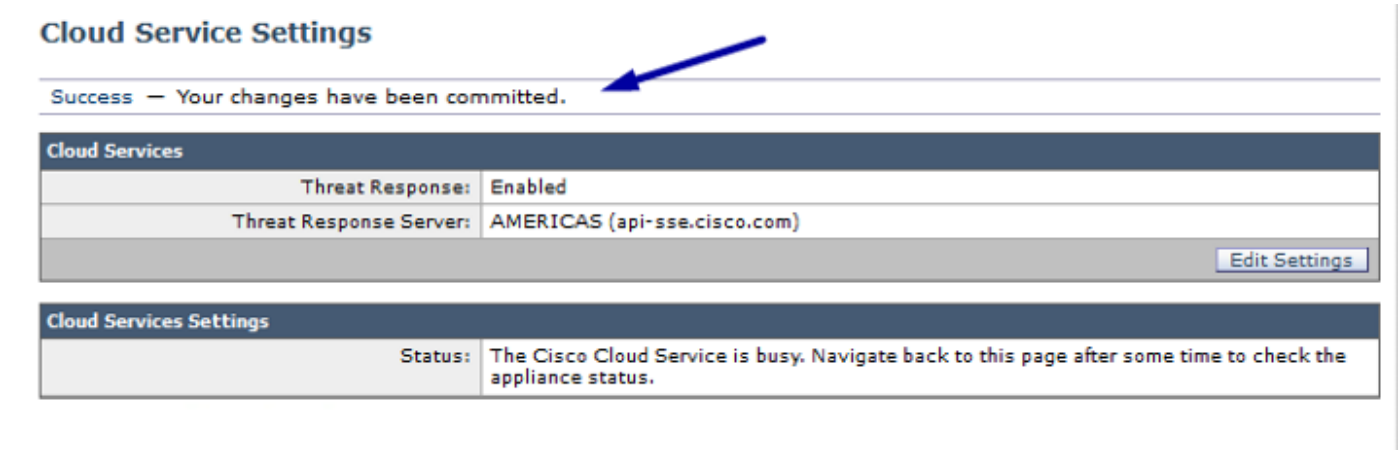
注：Threat Response Server(THREAT)URLのデフォルト選択はAMERICAS(api-sse.cisco.com)です。ヨーロッパの企業では、ドロップダウンメニューをクリックして[EUROPE(api.eu.sse.itd.cisco.com)]を選択します

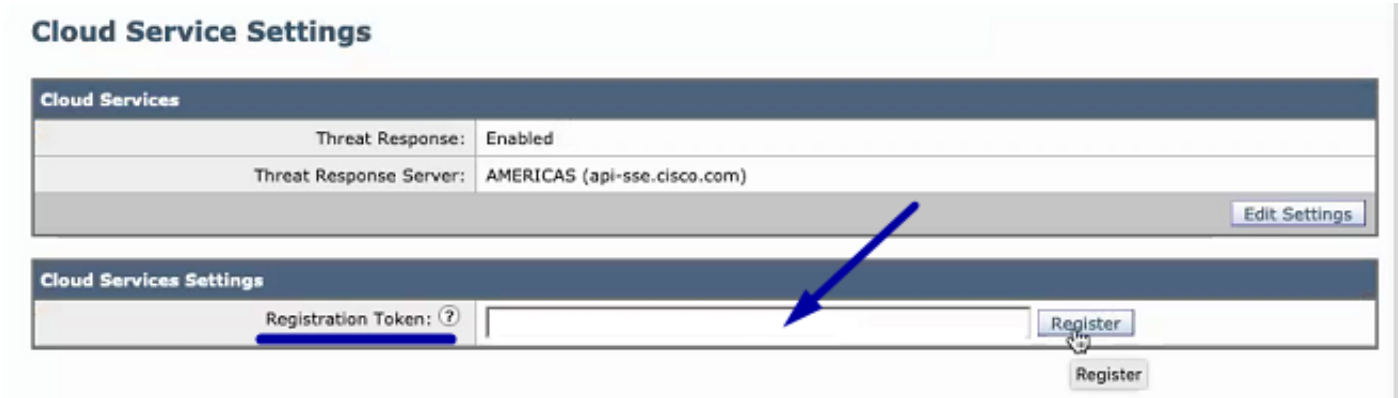
ステップ4：変更を送信して確定する

変更を保存して適用するには、変更を送信して確定する必要があります。次の図に示すように、ESAインターフェイスが更新されると、統合を登録するために登録トークンが要求されます。

注：成功メッセージが表示されます。変更がコミットされました。

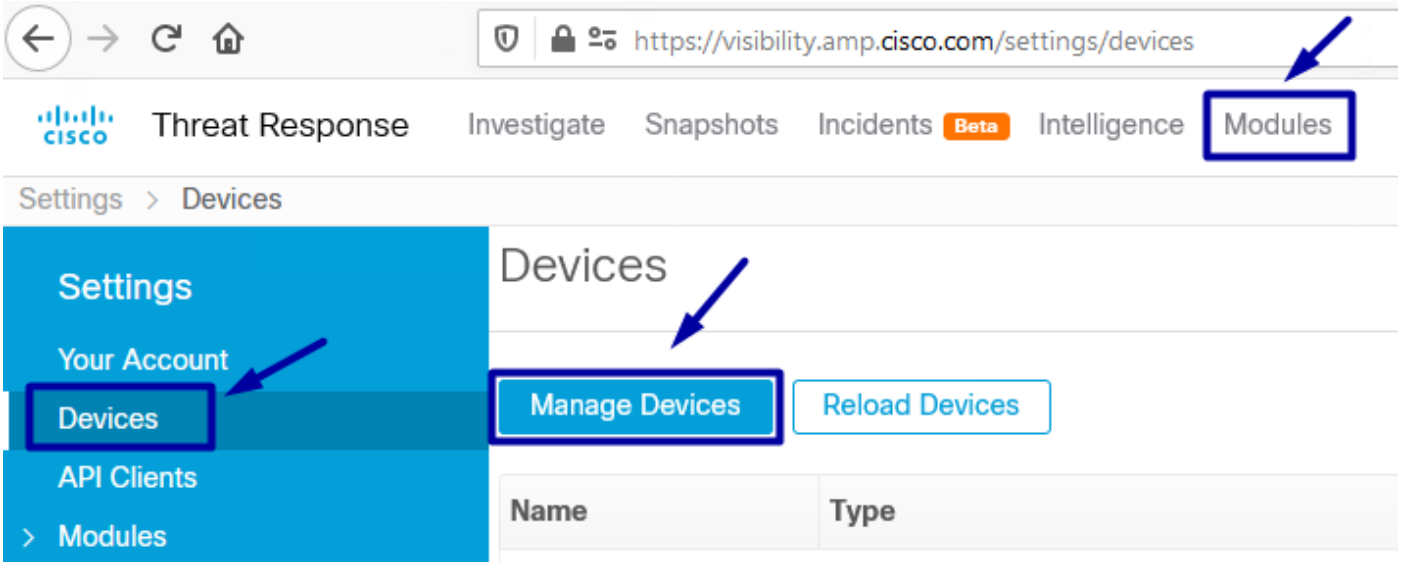




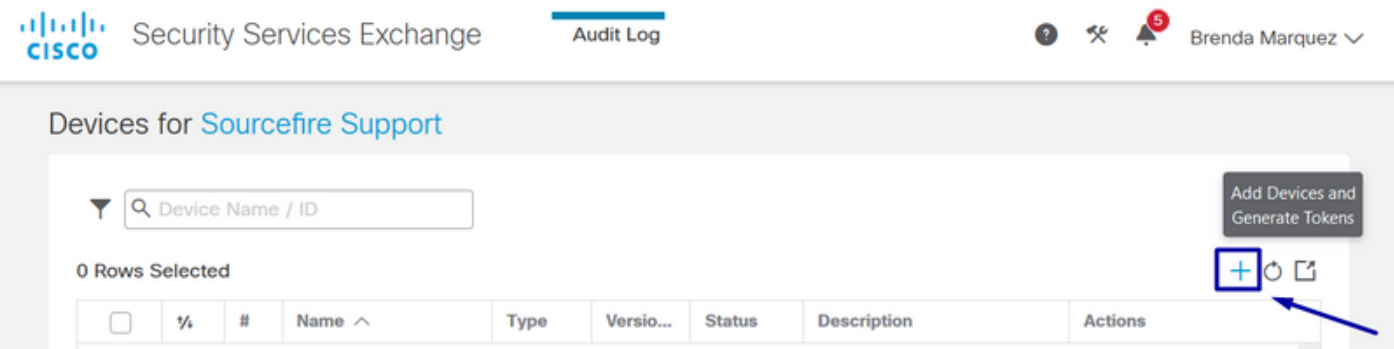


ステップ5:CTRポータルにログインし、ESAで要求される登録トークンを生成します

1.- CTRポータルで、[Modules（モジュール）] > [Devices（デバイス）] > [Manage Devices（デバイスの管理）]に移動し、次の図を参照してください。

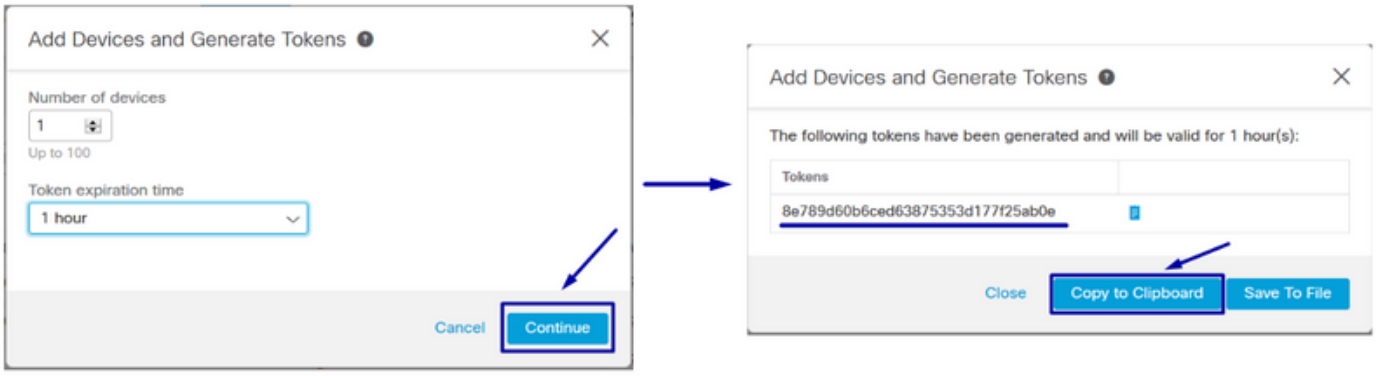


2.- [デバイスの管理(Manage Devices)]リンクをクリックすると、セキュリティサービス交換(SSE)にリダイレクトされます。次の図に示すように、[デバイスの追加(Add Devices)]アイコンと[トークンの生成(Generate Tokens)]アイコンをクリックします。



3.- [Continue]をクリックしてトークンを生成し、トークンが生成されたら、図に示すように[Copy to Clipboard]をクリックします。

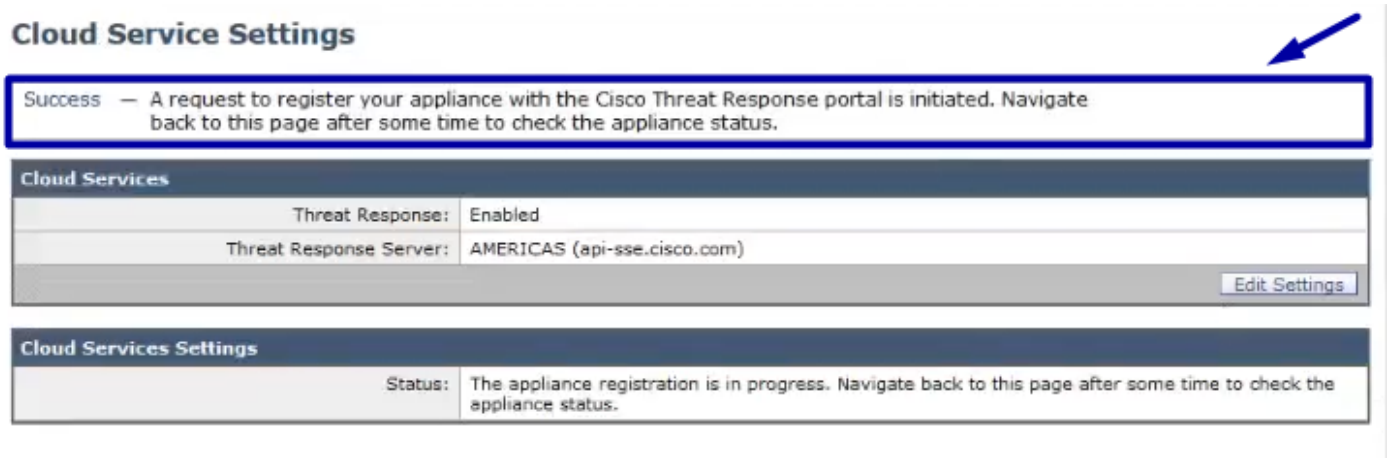
> **ヒント**：追加するデバイスの数(1 ~ 100)を選択し、トークンの有効期限（1時間、2時間、4時間、6時間、8時間、12時間、01日、02日、03日、04日、および05日）も選択できます。



ステップ6：登録トークン（CTRポータルから生成）をESAに貼り付けます

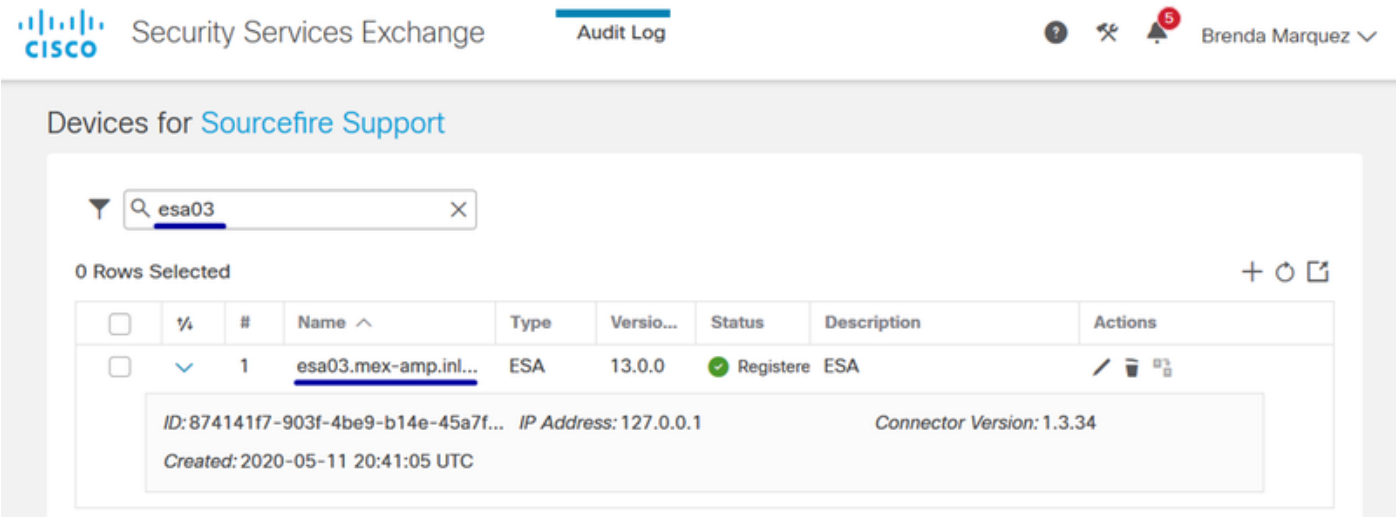
Registration Tokenが生成されたら、次の図のように、ESAの[Cloud Services Settings]セクションに貼り付けます。

> **注**：成功メッセージが表示されます。Cisco Threat Responseポータルへのアプライアンスの登録要求が開始されます。しばらくしてこのページに戻り、アプライアンスのステータスを確認します。



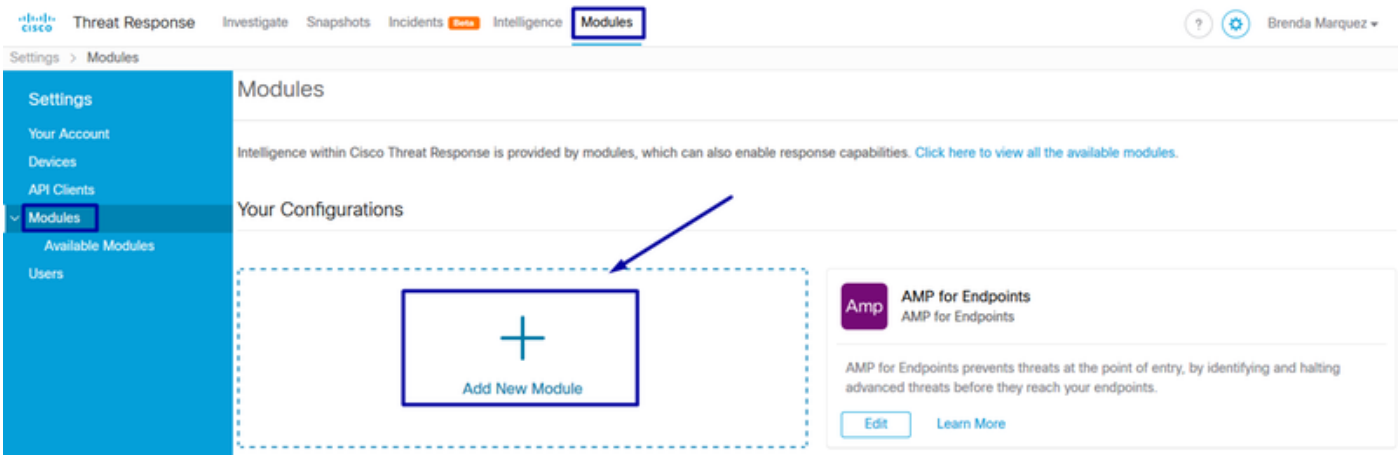
ステップ7:ESAデバイスがSSEポータルにあることを確認します

SSEポータル([CTR] > [Modules] > [Devices] > [Manage Devices])に移動し、[Search]タブでESAデバイスを確認します（図を参照）。

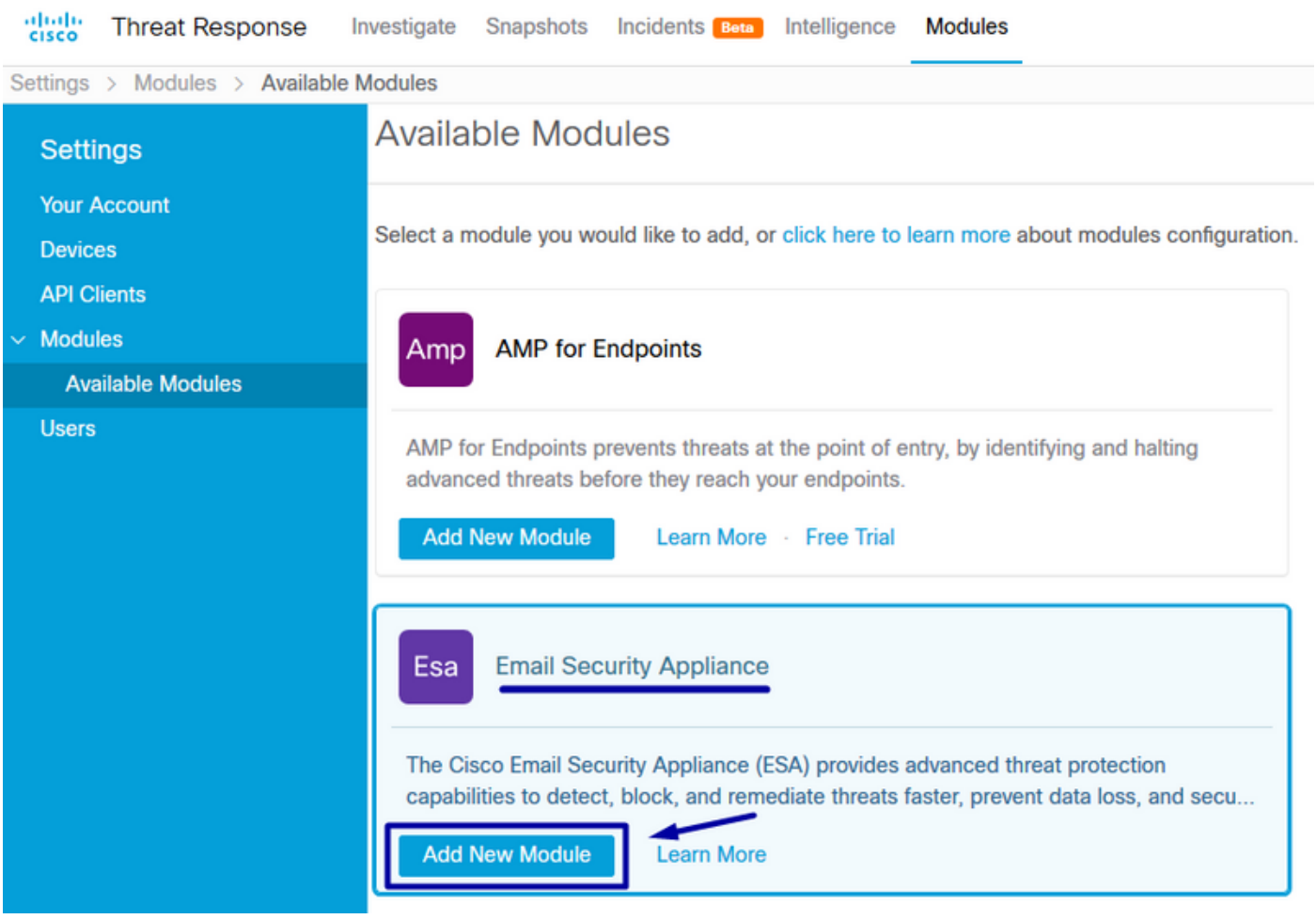


ステップ8:CTRポータルに移動し、新しいESAモジュールを追加します

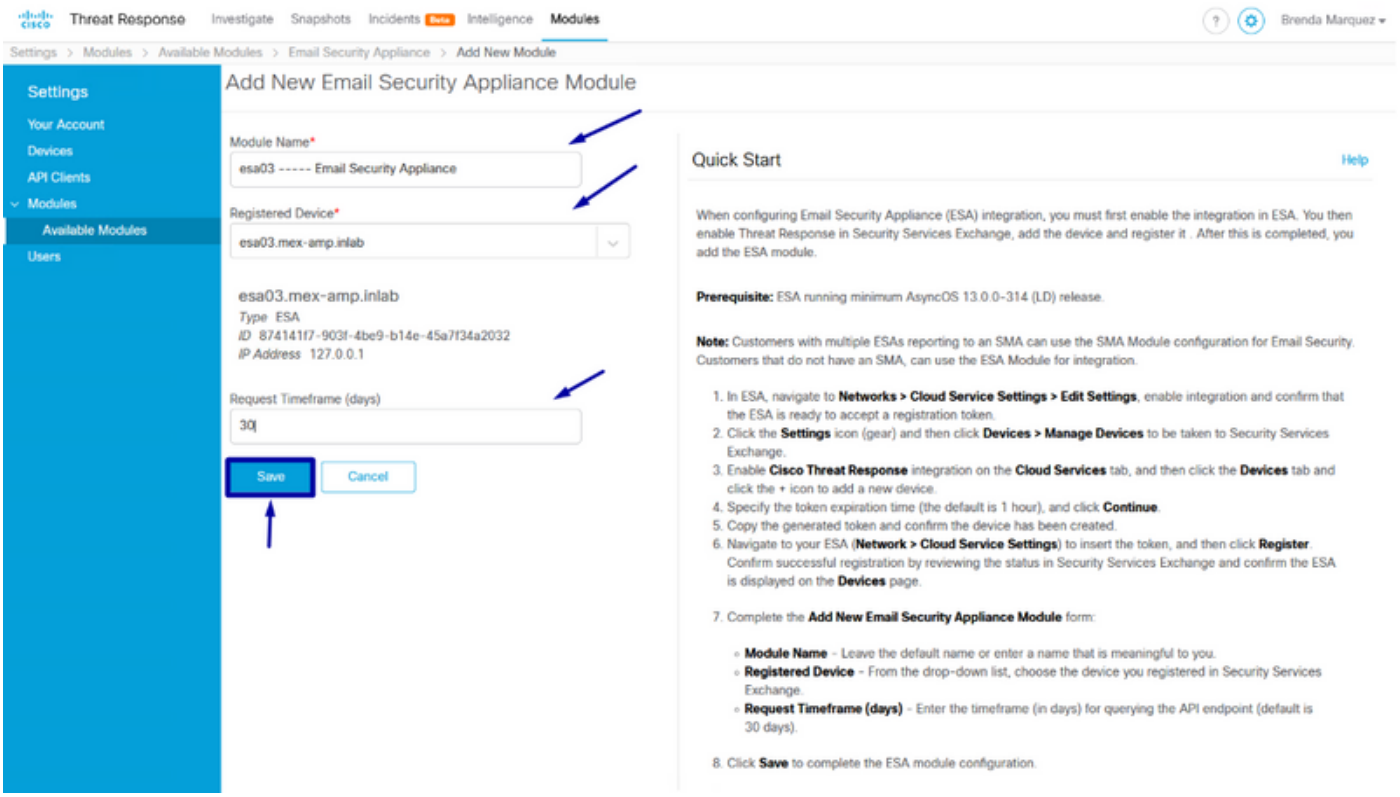
1.- CTRポータルで、図に示すように、[Modules] > [Add New Module]に移動します。



2. – モジュールタイプを選択します。この場合、モジュールは次の図のようにEメールセキュリティアプライアンスモジュールです。

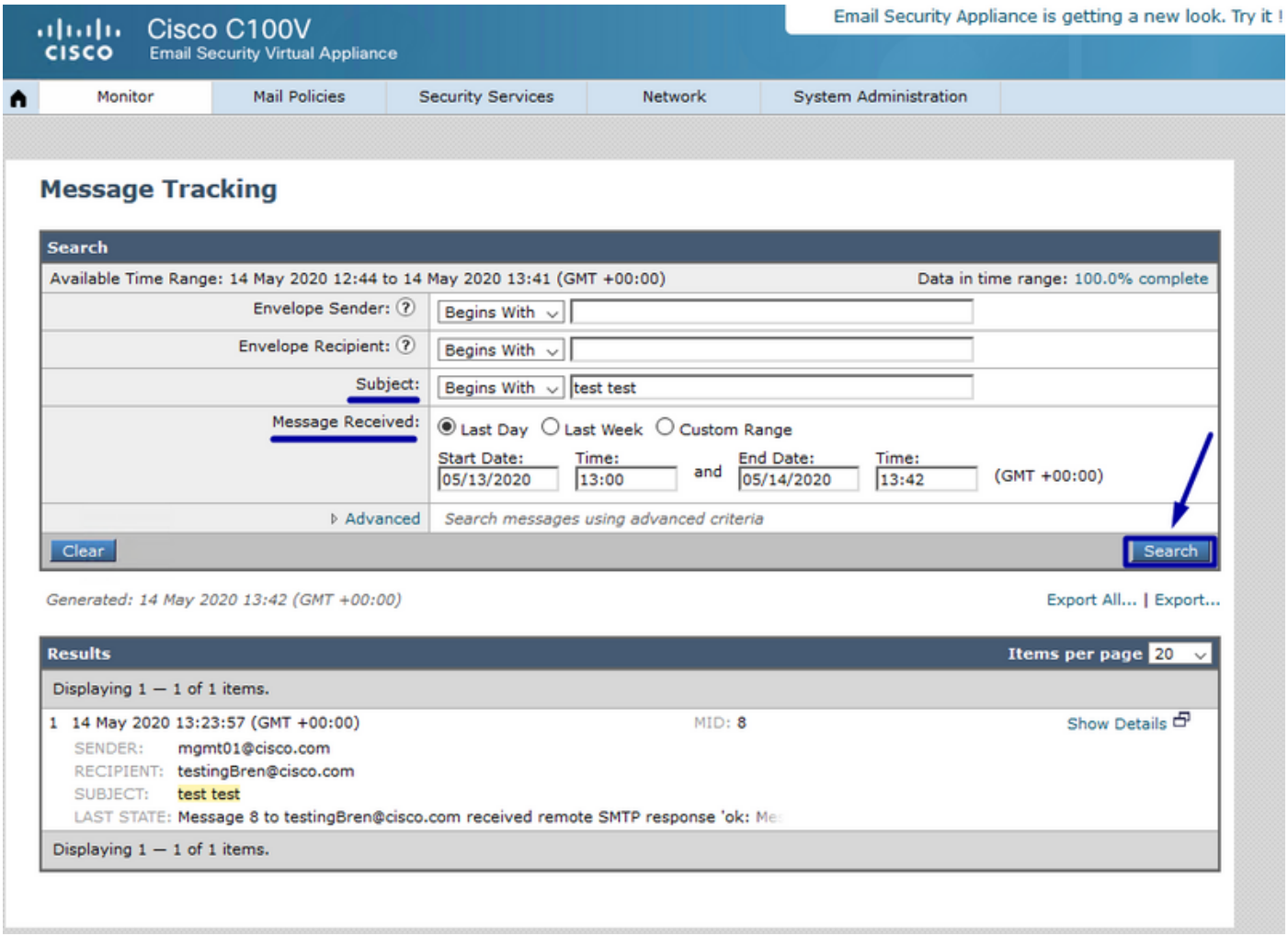


3. – フィールドを入力します。図に示すように、[Module Name]、[Registered Device]（以前に登録したデバイスを選択）、[Request Timeframe (days)]、および[Save]をクリックします。

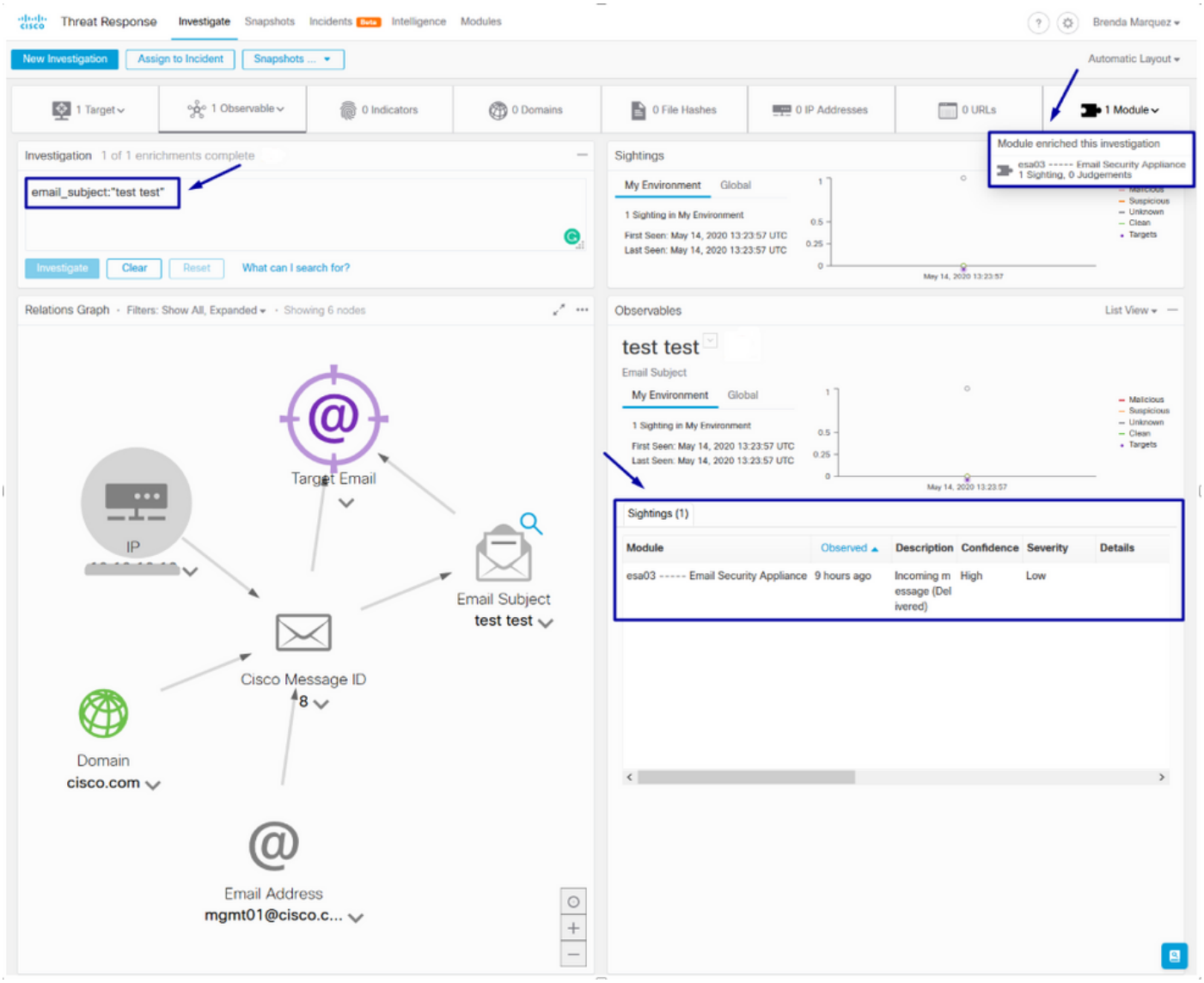


確認

CTRとESAの統合を確認するには、テスト電子メールを送信します。この電子メールは、ESAからも確認できます。[Monitor] > [Message Tracking]に移動し、テスト電子メールを検索します。この場合、Eメールの件名を下の画像としてフィルタリングしました。



これで、CTRポータルから調査を実行し、[Investigate]に移動して、図に示すように電子メールの回答を使用できます。



ヒント：他の電子メールの回答に対して、次の図と同じ構文を使用できます。

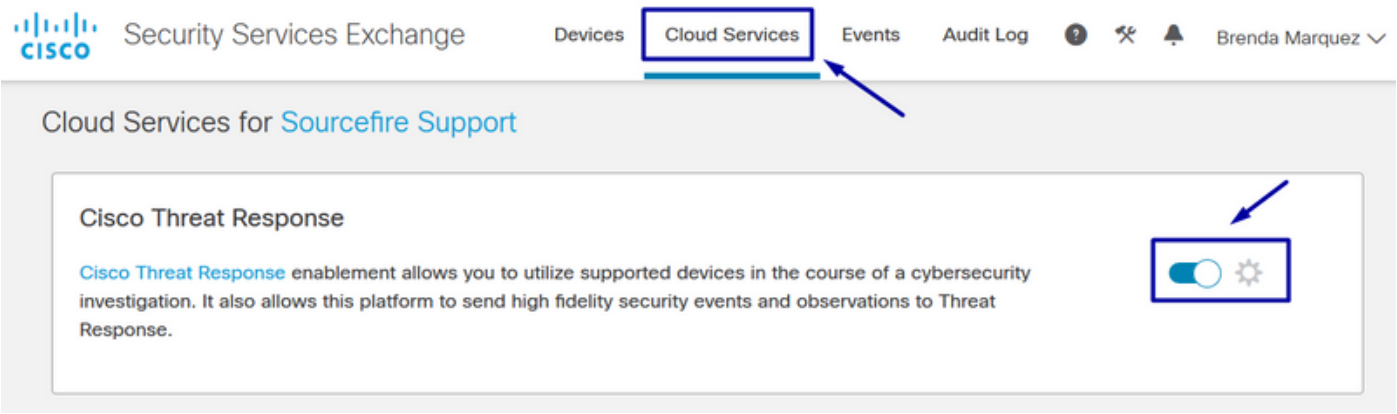
IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file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

トラブルシュート

CESのお客様、またはSMAを介してESAデバイスを管理する場合は、SMAを介してのみThreat Responseに接続できます。SMAがAsyncOS 12.5以降を実行していることを確認してください。SMAでESAを管理せず、ESAを直接統合する場合は、AsyncOSバージョン13.0以降であることを確認します。

ESAデバイスがCTRポータルに表示されない

ESAモジュールがCTRポータルに追加されている間にESAデバイスが[Registered Device]ドロップダウンに表示されない場合は、CTRがSSEで有効になっていることを確認し、CTRで[Modules] > [Devices] > [Manage Devices]に移動してCTRをを有効します。



CTR調査でESAからのデータが表示されない

次のことを確認してください。

- 調査の構文が正しく、上記の「Verify」セクションにEメールの回答が示されています。
- 適切なThreat Response Server(THREAT)またはクラウド（南・北・中央アメリカ/ヨーロッパ）を選択しました。

ESAが登録トークンを要求していない

Threat Responseが有効になっている場合は、変更を確定してください。有効になっていない場合は、変更はESAの[Threat Response]セクションに適用されません。

無効または期限切れのトークンが原因で登録に失敗しました

トークンが正しいクラウドから生成されていることを確認してください。

ESAにヨーロッパ(EU)クラウドを使用する場合は、次の方法でトークンを生成します。
https://admin.eu.sse.itd.cisco.com/

ESAにアメリカ(NAM)クラウドを使用する場合は、次の方法でトークンを生成します。
https://admin.sse.itd.cisco.com/

また、登録トークンには有効期限があります（統合を完了するのに最も便利な時間を選択してください）。

関連情報

- **この記事の情報は、『Cisco Threat Response and ESA Integration(Cisco Threat Response and ESA Integration)』ビデオで確認できます。**
- テクニカル サポートとドキュメント – Cisco Systems