Integration von Cisco Threat Response (CTR) und ESA

Inhalt

Einführung

In diesem Dokument wird der Prozess zur Integration von Cisco Threat Response (CTR) mit E-Mail Security Appliance (ESA) beschrieben. Außerdem wird erläutert, wie Sie dies überprüfen können, um CTR-Untersuchungen durchzuführen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Reaktion auf Bedrohungen von Cisco
- E-Mail Security Appliance

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- CTR-Konto
- Cisco Security Services Exchange
- ESA C100V auf Softwareversion 13.0.0-392

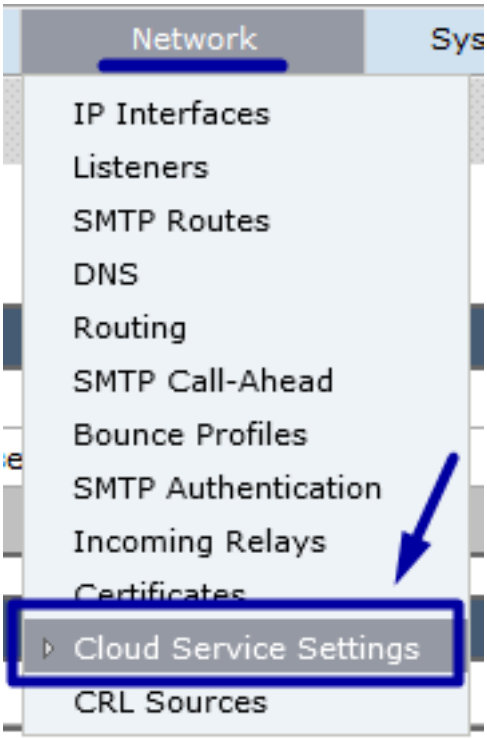
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Um die Integration CTR und ESA zu konfigurieren, melden Sie sich bei Ihrer E-Mail Security Virtual Appliance an und befolgen Sie die folgenden Schritte:

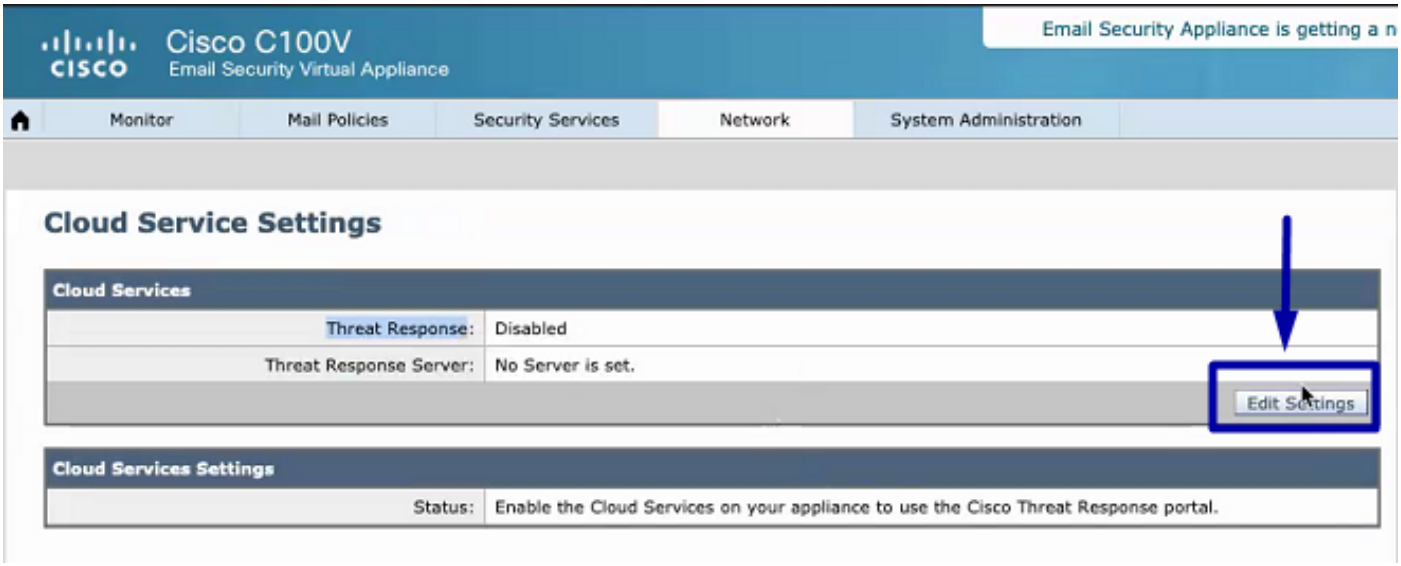
Schritt 1: Navigieren Sie zu Netzwerk > Cloud Service Settings.

Navigieren Sie in der ESA zum Kontextmenü Netzwerk > Cloud Service Settings, um den aktuellen Bedrohungsreaktionsstatus (Deaktiviert/Aktiviert) anzuzeigen, wie im Bild gezeigt.



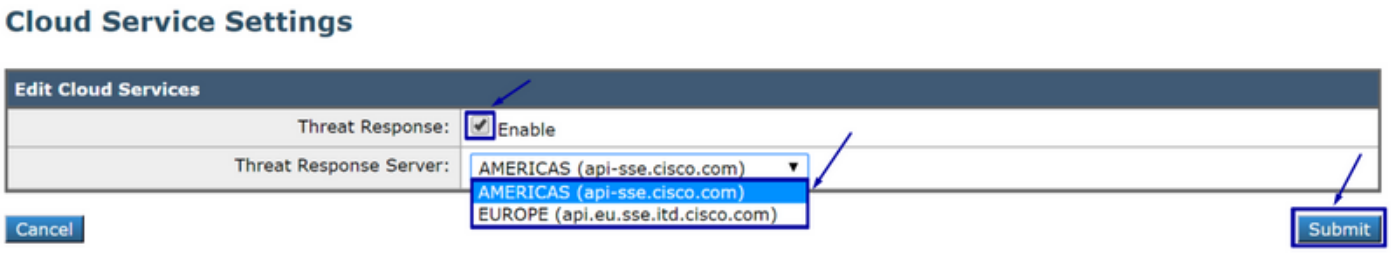
Schritt 2: Klicken Sie auf Einstellungen bearbeiten.

Die Funktion "Threat Response" in der ESA ist bisher deaktiviert. Klicken Sie zum Aktivieren der Funktion auf "Edit Settings" (Einstellungen bearbeiten), wie im Bild gezeigt:



Schritt 3: Aktivieren Sie das Kontrollkästchen Enable (Aktivieren) und Threat Response Server.

Aktivieren Sie das Kontrollkästchen Enable (Aktivieren), und wählen Sie dann den Threat Response Server aus. Weitere Informationen finden Sie in der Abbildung unten:

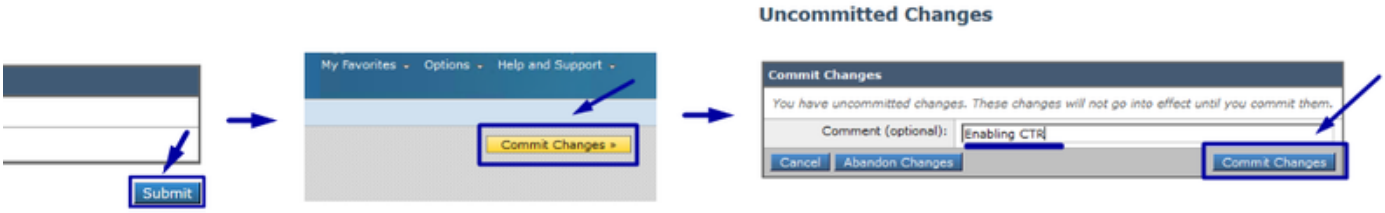


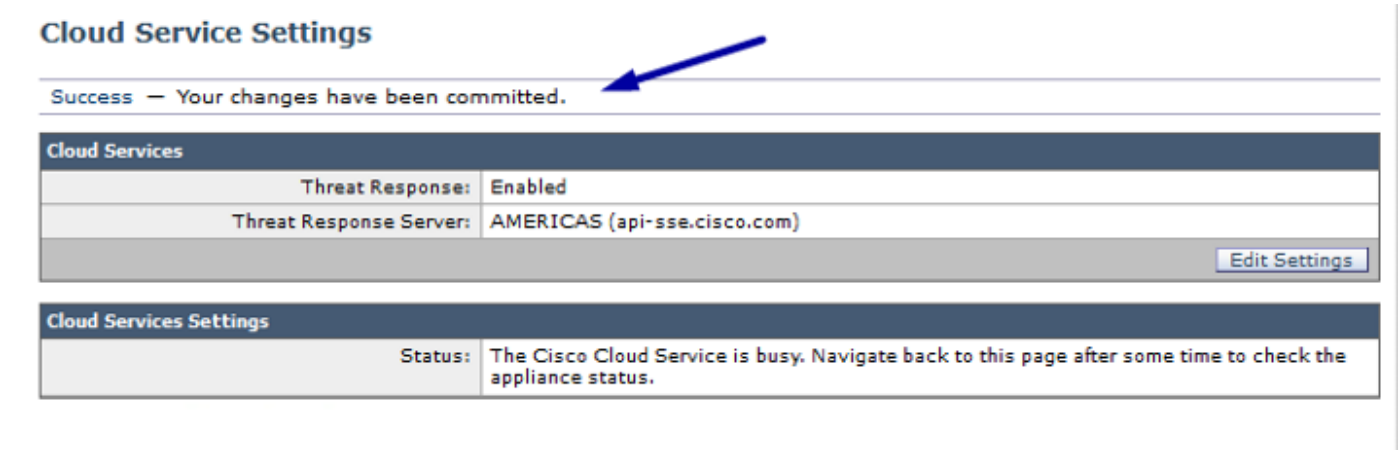
Hinweis: Die Standardauswahl für die URL des Threat Response-Servers lautet AMERICAS (api-sse.cisco.com). Klicken Sie für EUROPE-Unternehmen auf das Dropdown-Menü, und wählen Sie EUROPE (api.eu.sse.itd.cisco.com).

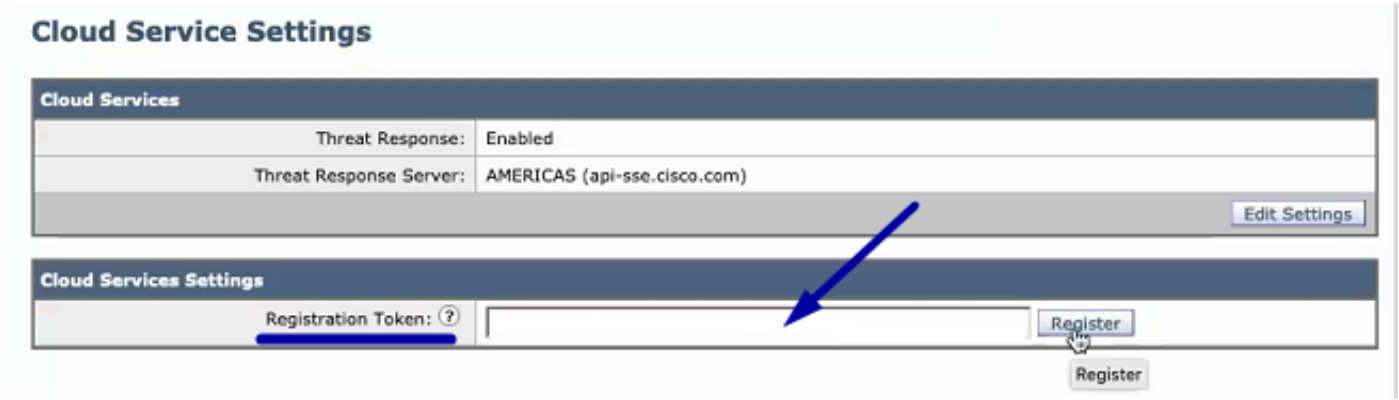
Schritt 4: Änderungen senden und bestätigen

Die Änderungen müssen eingesendet und bestätigt werden, um sie zu speichern und anzuwenden. Wenn nun die ESA-Schnittstelle aktualisiert wird, wird ein Registrierungstoken angefordert, um die Integration zu registrieren, wie in der Abbildung unten gezeigt.

Hinweis: Sie sehen eine Erfolgsmeldung: Ihre Änderungen wurden übernommen.

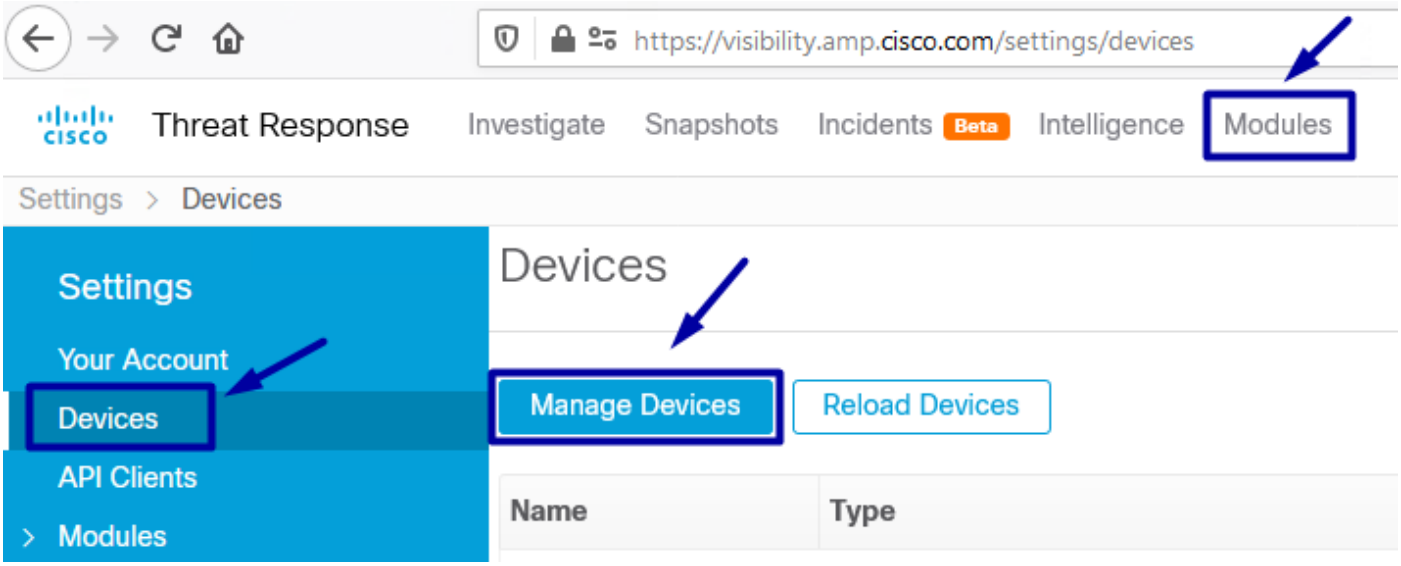




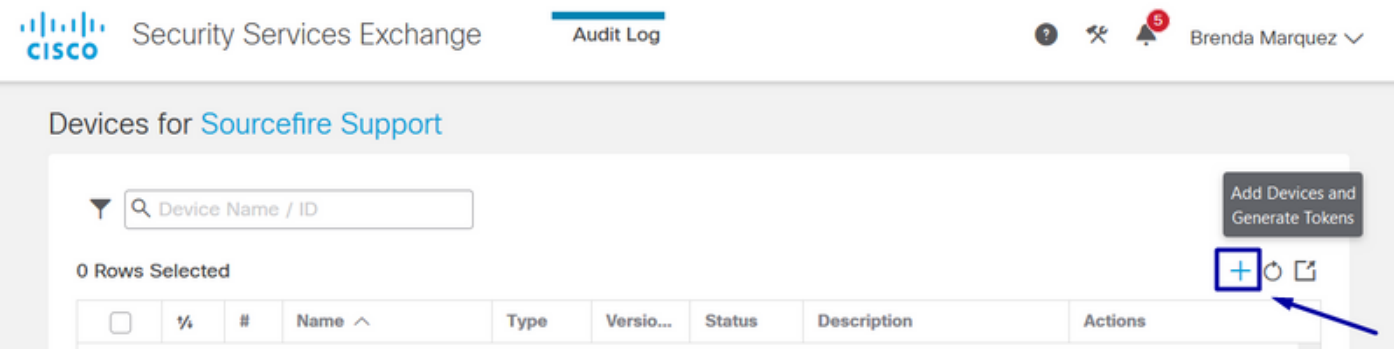


Schritt 5: Melden Sie sich beim CTR-Portal an, und generieren Sie das in der ESA angeforderte Registrierungs-Token.

1.- Navigieren Sie im CTR-Portal zu Modules > Devices > Manage Devices (Module > Geräte > Geräte verwalten), sehen Sie das nächste Bild.

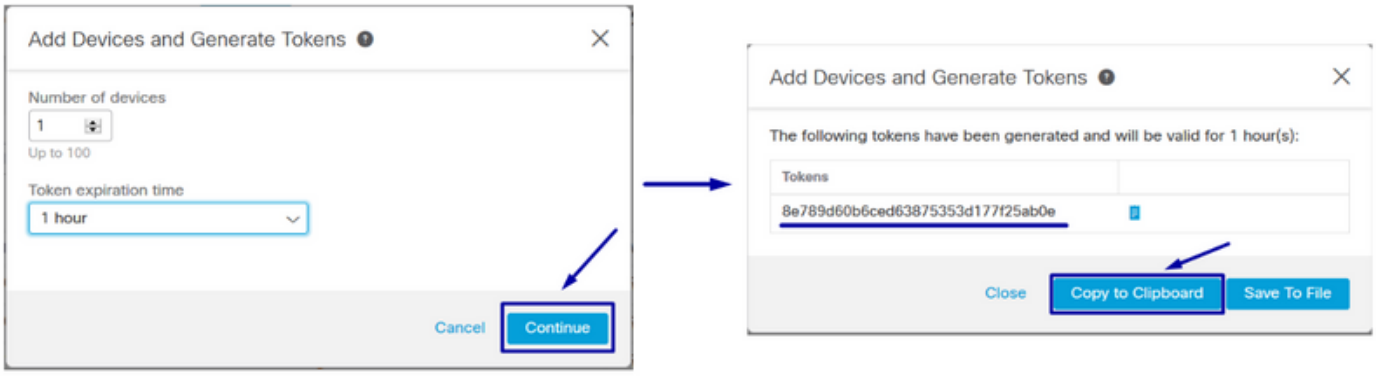


2.- Der Link "Geräte verwalten" leitet Sie zur Security Services Exchange (SSE) um. Wenn Sie dort sind, klicken Sie auf das Symbol "Geräte hinzufügen" und "Token generieren", wie im Bild gezeigt.



3.- Klicken Sie auf Weiter, um das Token zu generieren. Wenn das Token generiert wurde, klicken Sie auf Kopieren in die Zwischenablage, wie im Bild gezeigt.

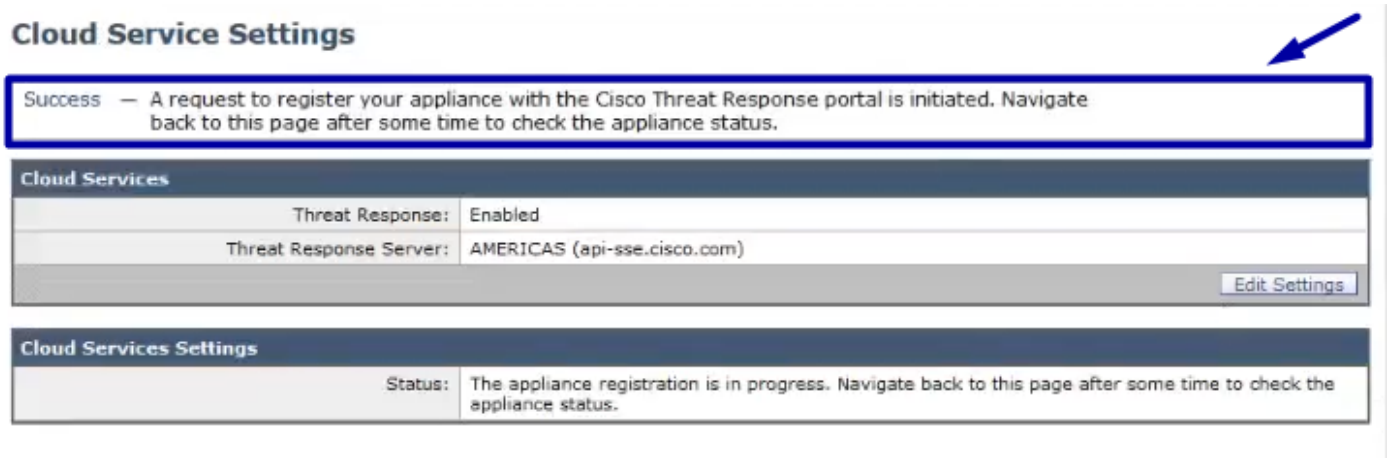
> **Tipp**: Sie können die Anzahl der hinzuzufügenden Geräte auswählen (von 1 bis zu 100) und außerdem die Ablaufzeit für Token auswählen (1 Stunde, 2 Stunden, 4 Stunden, 6 Stunden, 8 Stunden, 12 Stunden, 01 Tage, 02 Tage, 03 Tage, 04 Tage und 05 Tage).



Schritt 6: Fügen Sie das Registrierungstoken (vom CTR-Portal generiert) in die ESA ein.

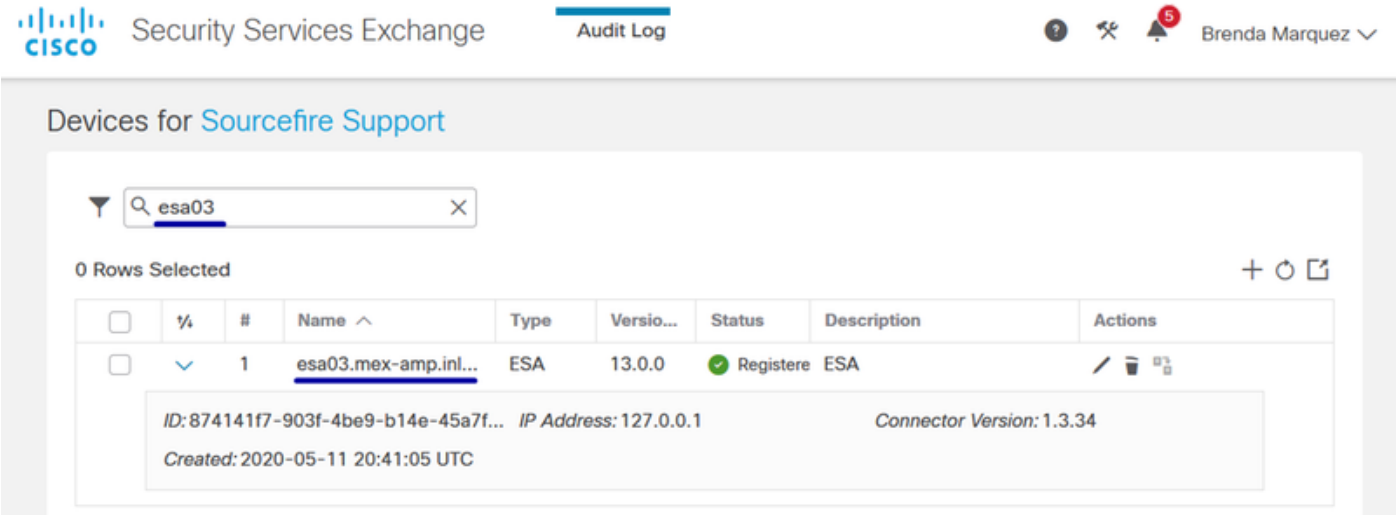
Nachdem das Registrierungstoken generiert wurde, fügen Sie es wie unten abgebildet im Abschnitt "Cloud Services Settings" der ESA ein.

> **Hinweis**: Sie sehen eine Erfolgsmeldung: Es wird eine Anfrage zur Registrierung Ihrer Appliance beim Cisco Threat Response-Portal gestellt. Navigieren Sie nach einiger Zeit wieder zu dieser Seite, um den Status der Appliance zu überprüfen.



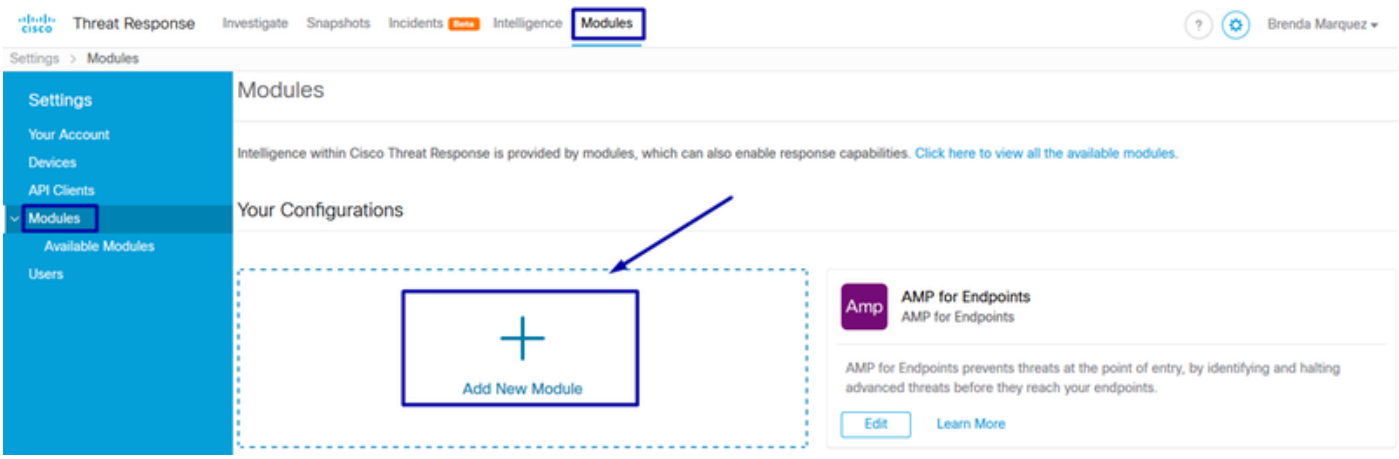
Schritt 7: Überprüfen Sie, ob sich Ihr ESA-Gerät im SSE-Portal befindet.

Sie können zum SSE-Portal (CTR > Module > Devices > Manage Devices) navigieren und auf der Registerkarte Search (Suchen) Ihr ESA-Gerät anzeigen, wie im Bild gezeigt.



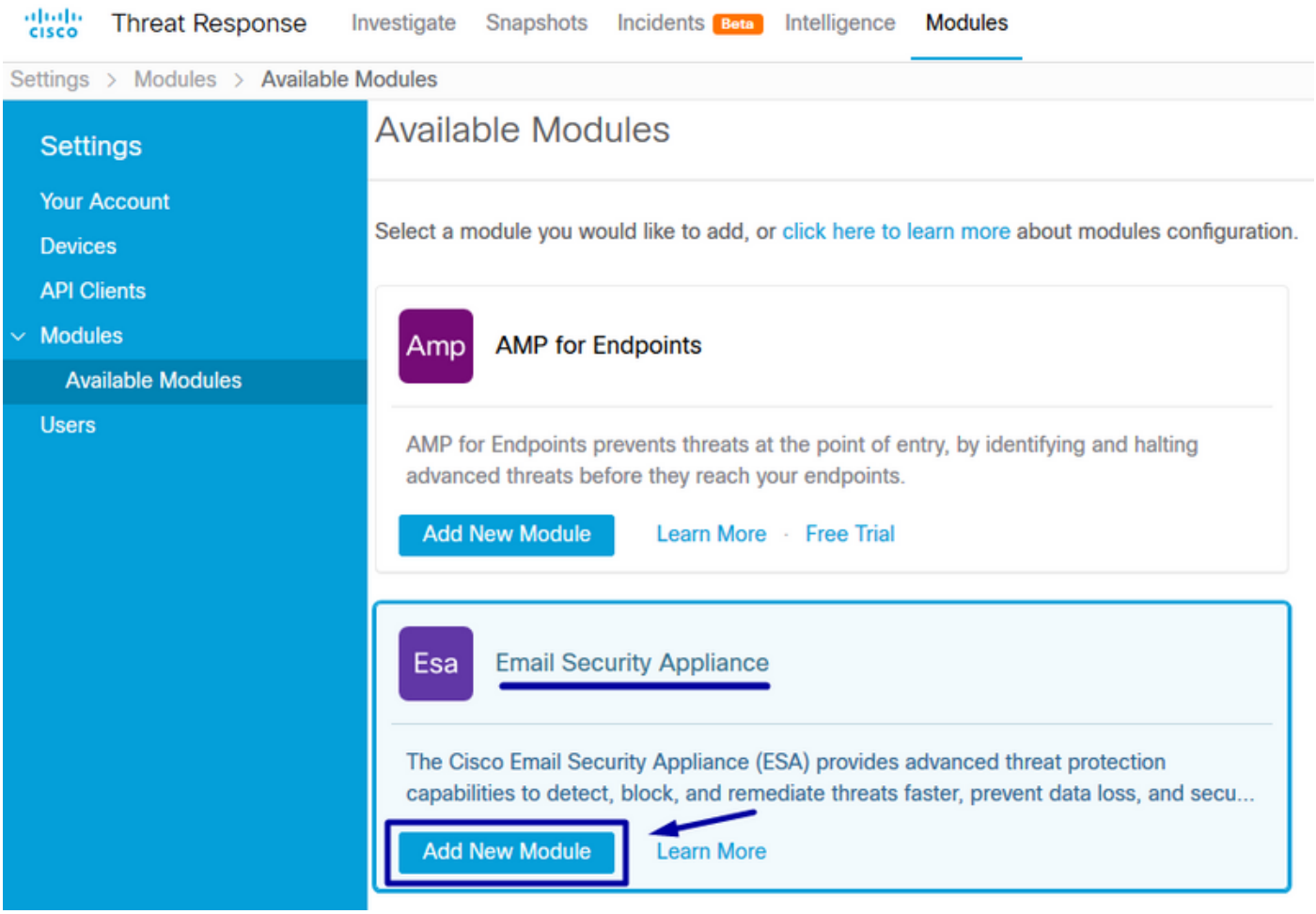
Schritt 8: Navigieren Sie zum CTR-Portal, und fügen Sie ein neues ESA-Modul hinzu.

1.- Navigieren Sie im CTR-Portal zu Module > Add New Module (Neues Modul hinzufügen), wie im Bild gezeigt.

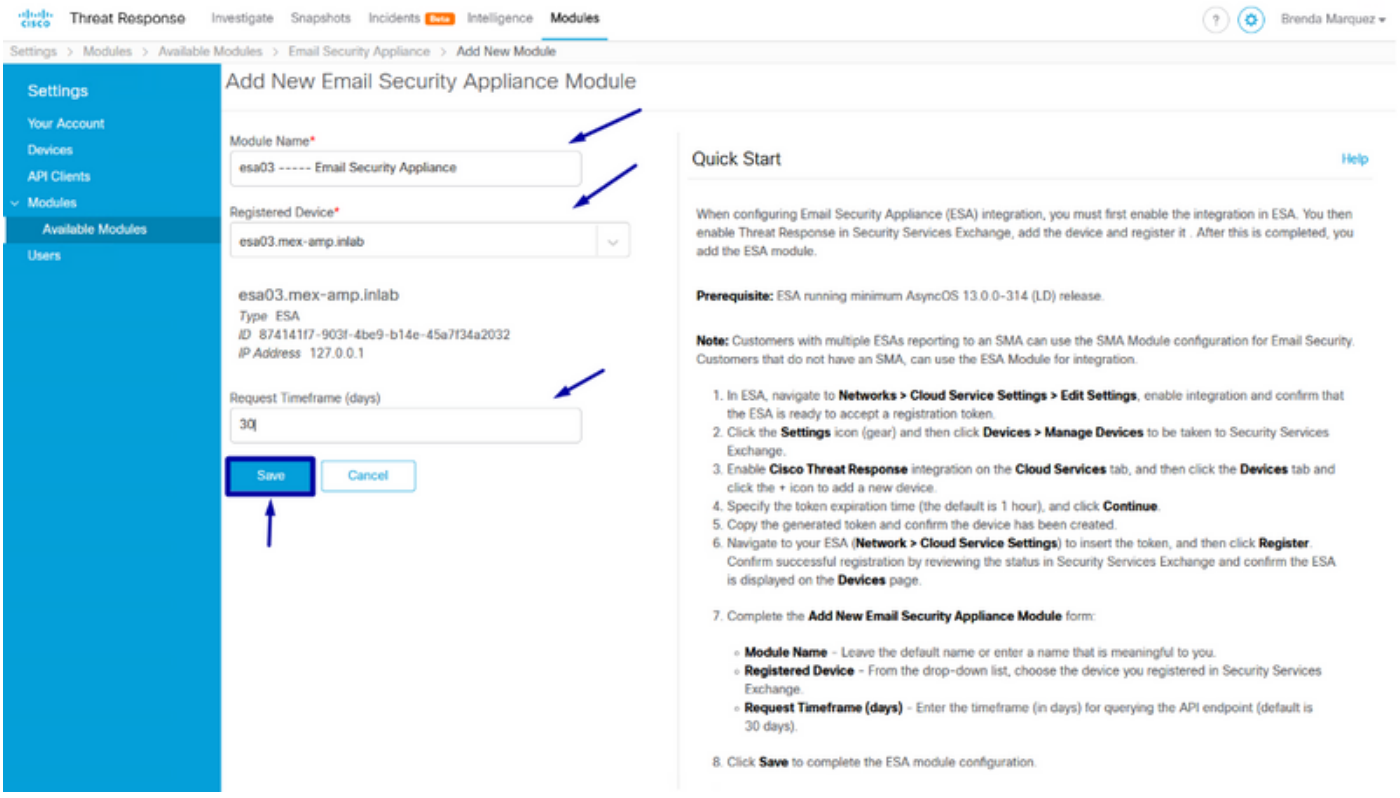


2.- Wählen Sie den Modultyp aus. In diesem Fall ist das Modul ein E-Mail-Security-Appliance-

Modul wie unten abgebildet.

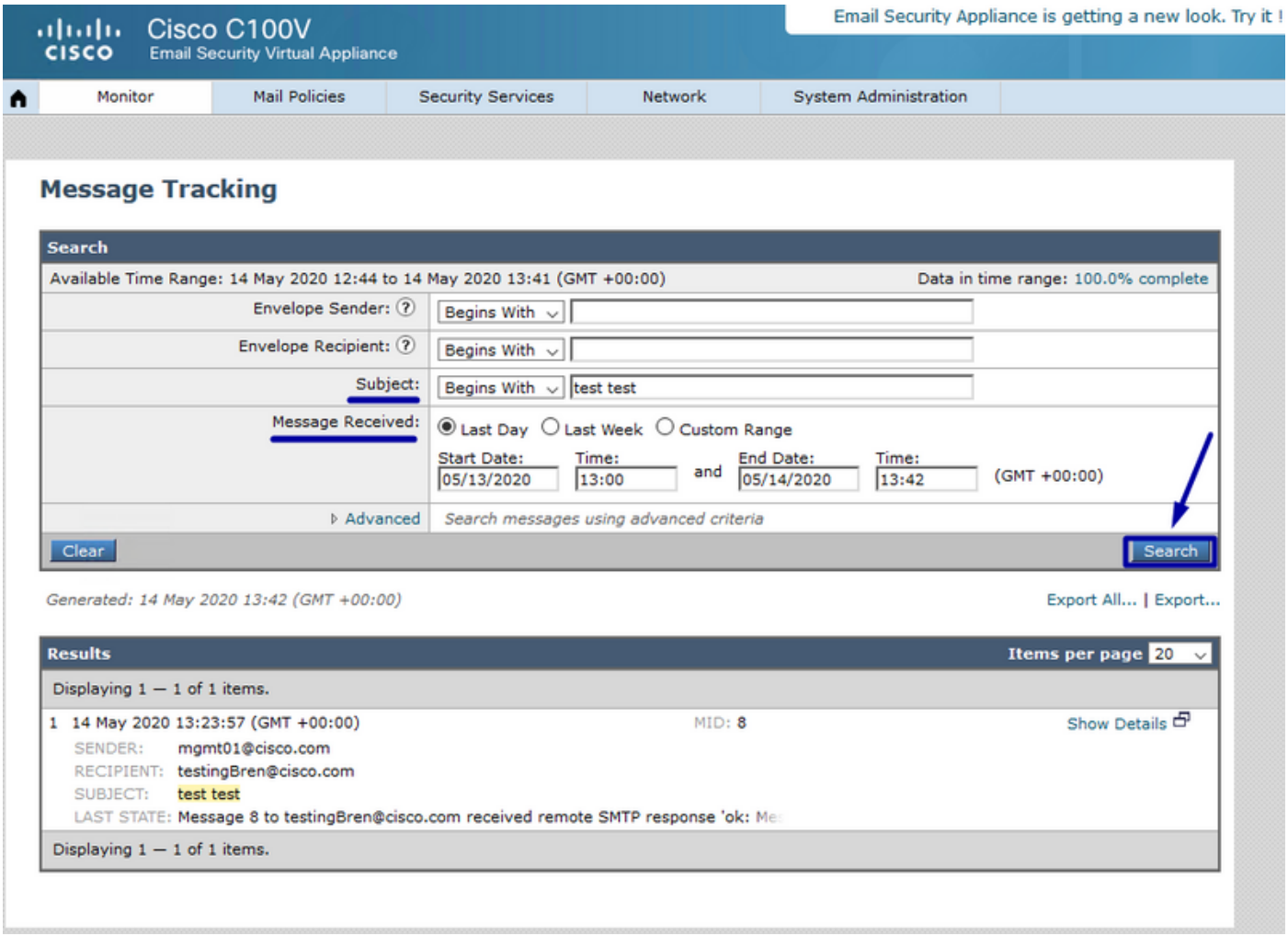


3.- Geben Sie die Felder ein: Modulname, registriertes Gerät (wählen Sie das zuvor registrierte aus) und Anforderungszeitrahmen (Tage) sowie Speichern, wie im Bild gezeigt.

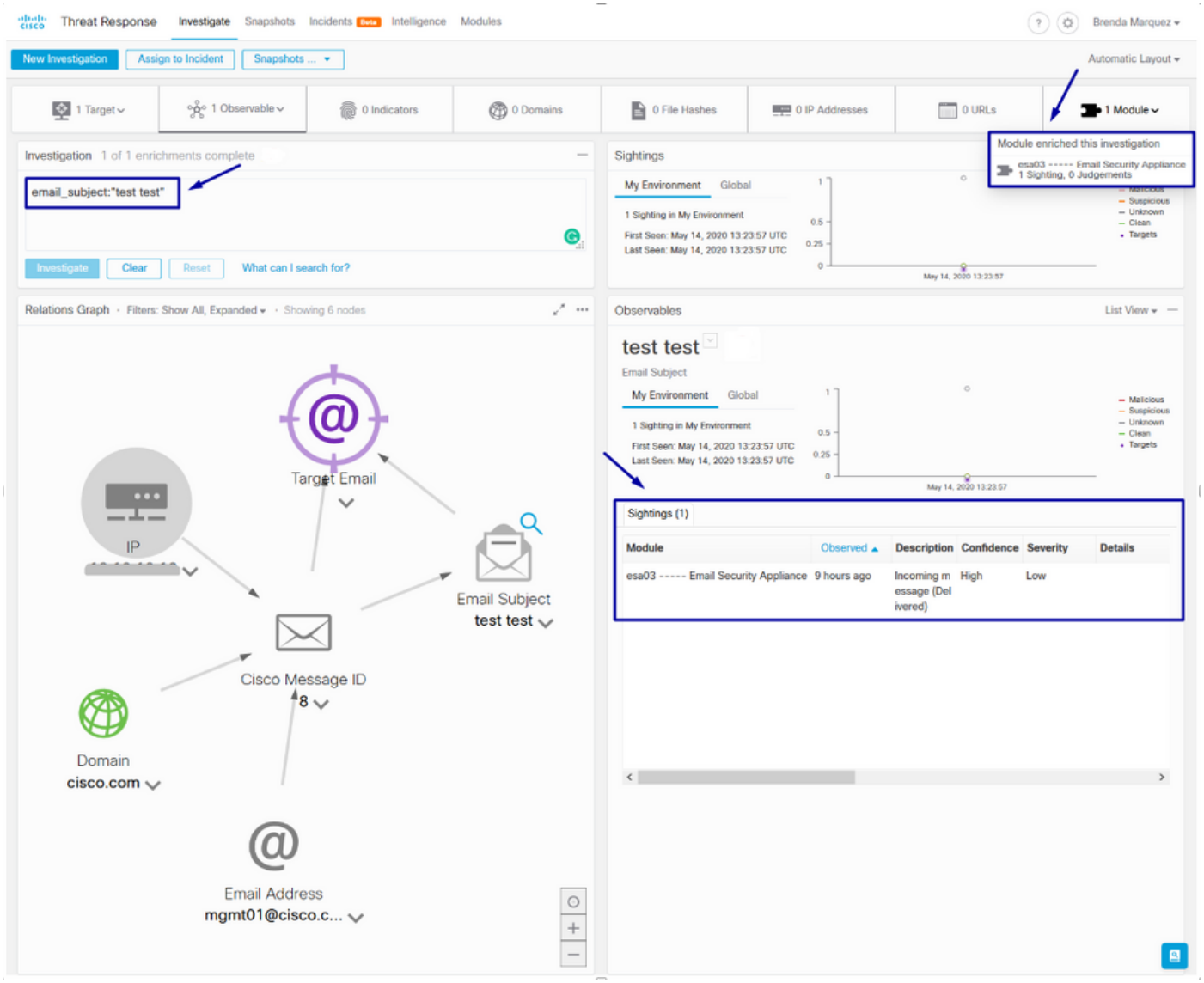


Überprüfen

Um die CTR- und ESA-Integration zu überprüfen, können Sie eine Test-E-Mail senden, die Sie auch von der ESA aus sehen können. Navigieren Sie zu Monitor > Message Tracking (Überwachung > Nachrichtenverfolgung), und suchen Sie die Test-E-Mail. In diesem Fall habe ich nach E-Mail Betreff wie das Bild unten gefiltert.



Im CTR-Portal können Sie jetzt eine Untersuchung durchführen, zu Investigate navigieren und einige E-Mail-Beobachtungsmaterialien verwenden, wie im Bild gezeigt.



Tipp: Sie können die gleiche Syntax für andere E-Mail-Observables wie im Bild verwenden.

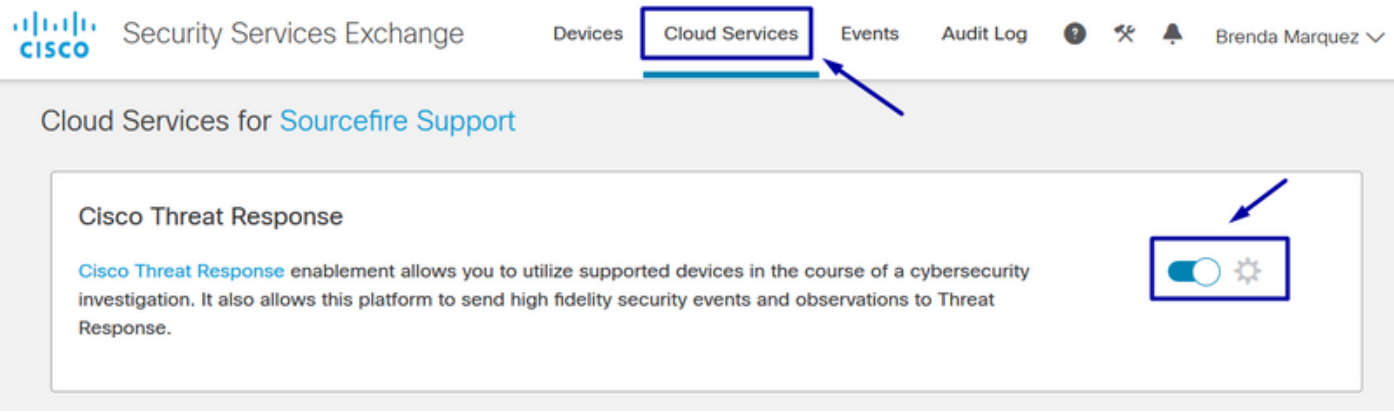
IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file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

Fehlerbehebung

Wenn Sie ein CES-Kunde sind oder Ihre ESA-Geräte über eine SMA verwalten, können Sie nur über Ihre SMA eine Verbindung mit Threat Response herstellen. Stellen Sie sicher, dass Ihre SMA AsyncOS 12.5 oder höher ausführt. Wenn Sie Ihre ESA nicht mit einer SMA verwalten und die ESA direkt integrieren, stellen Sie sicher, dass die ESA ab AsyncOS Version 13.0 verfügbar ist.

ESA-Gerät wird nicht im CTR-Portal angezeigt.

Wenn Ihr ESA-Gerät nicht im Dropdown-Menü für registrierte Geräte angezeigt wird, während das ESA-Modul im CTR-Portal hinzugefügt wird, stellen Sie sicher, dass CTR in SSE aktiviert ist. Navigieren Sie im CTR zu Module > Devices > Manage Devices (Geräte > Geräte verwalten), und navigieren Sie im SSE-Portal zu Cloud Services, und aktivieren Sie CTR (siehe unten):



CTR-Untersuchungen zeigen keine Daten von der ESA.

Stellen Sie sicher, dass

- Die Syntax der Untersuchung ist korrekt. Die E-Mail-Beobachtungen sind oben im Abschnitt Überprüfen aufgeführt.
- Sie haben den richtigen Threat Response Server oder die richtige Cloud (Nord- und Südamerika/Europa) ausgewählt.

Die ESA fordert das Registrierungstoken nicht an.

Stellen Sie sicher, dass Sie die Änderungen bestätigen, wenn die Bedrohungsantwort aktiviert wurde. Andernfalls werden die Änderungen nicht auf den Abschnitt "Bedrohungsantwort" der ESA angewendet.

Die Registrierung ist aufgrund eines ungültigen oder abgelaufenen Tokens fehlgeschlagen.

Stellen Sie sicher, dass der Token aus der richtigen Cloud generiert wird:

Wenn Sie Europa (EU) Cloud für ESA verwenden, erstellen Sie das Token aus: https://admin.eu.sse.itd.cisco.com/

Wenn Sie Americas (NAM) Cloud für ESA verwenden, generieren Sie das Token aus: https://admin.sse.itd.cisco.com/

Denken Sie auch daran, dass das Registrierungstoken eine Ablaufzeit hat (wählen Sie den für den rechtzeitigen Abschluss der Integration günstigsten Zeitpunkt aus).

Zugehörige Informationen

- Die Informationen in diesem Artikel finden Sie im Video zur Cisco Threat Response- und ESA-Integration.

- Technischer Support und Dokumentation - Cisco Systems