Cisco Threat Response (CTR) en ESA-integratie

Inhoud

Inleiding

Dit document beschrijft het proces om Cisco Threat Response (CTR) te integreren met e-mail security applicatie (ESA) en hoe u dit kunt controleren om een aantal CTR-onderzoeken te kunnen uitvoeren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Threat-respons
- E-mail security applicatie

Gebruikte componenten

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

- CTR-account
- Cisco Security Services exchange
- ESR C100V op softwareversie 13.0.0-392

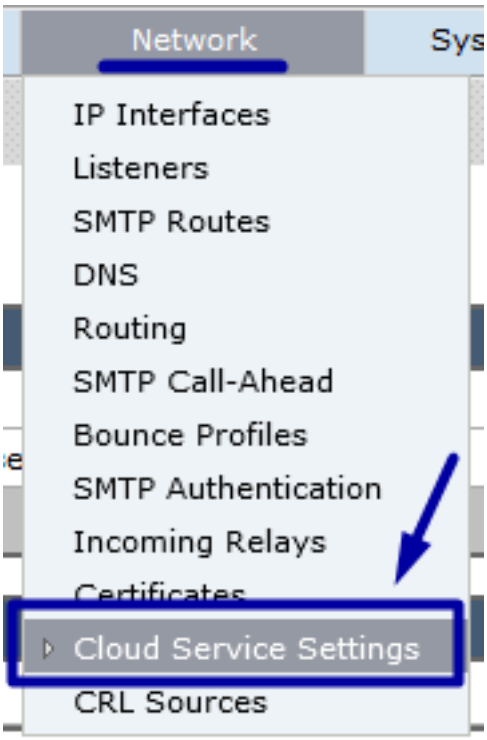
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht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

Configureren

Om de Integration CTR en ESA te configureren logt u in bij uw e-mail security virtuele applicatie en volgt u deze snelle stappen:

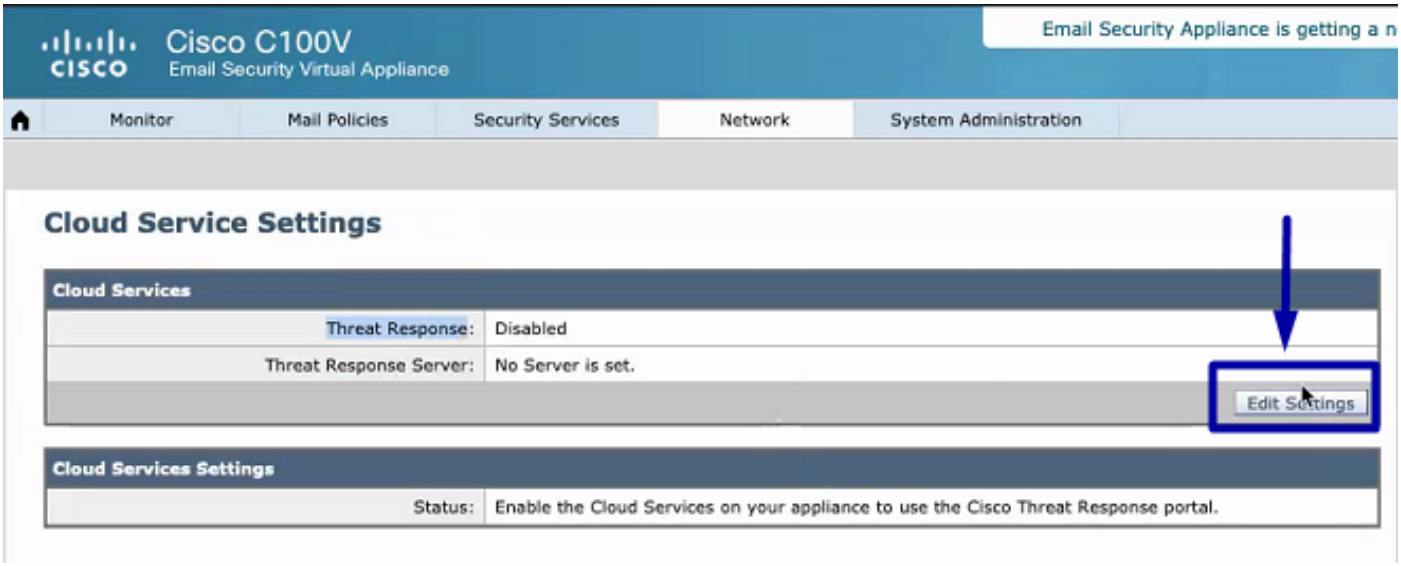
Stap 1. Navigeren in naar Network > Cloud Service-instellingen

Druk eenmaal in het ESA op het contextmenu Network > Cloud Service Settings om de huidige status van de Threat Response (uitgeschakeld/ingeschakeld) te zien zoals in de afbeelding.



Stap 2. Klik op Instellingen bewerken

Tot nu is de optie Threat Response in het ESA uitgeschakeld. Om deze functie in te schakelen, klikt u op Bewerken Instellingen zoals in de afbeelding:



Stap 3. Selecteer het selectieteken Inschakelen en de Threat Response Server

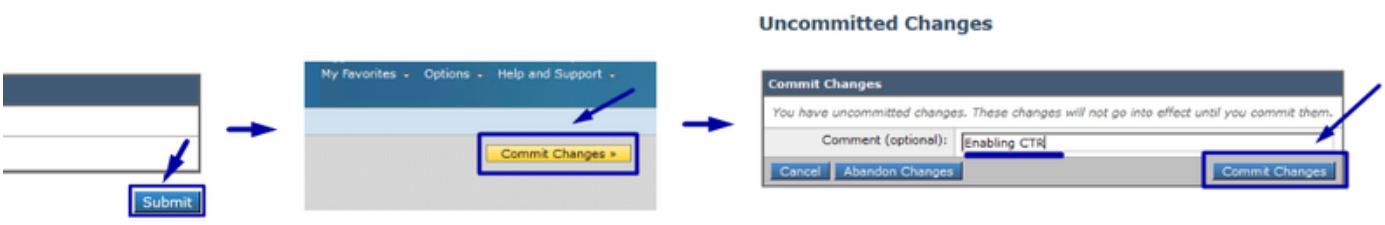
Selecteer het aanvinkvakje Enable, kies vervolgens de Threat Response Server. Zie het onderstaande beeld:

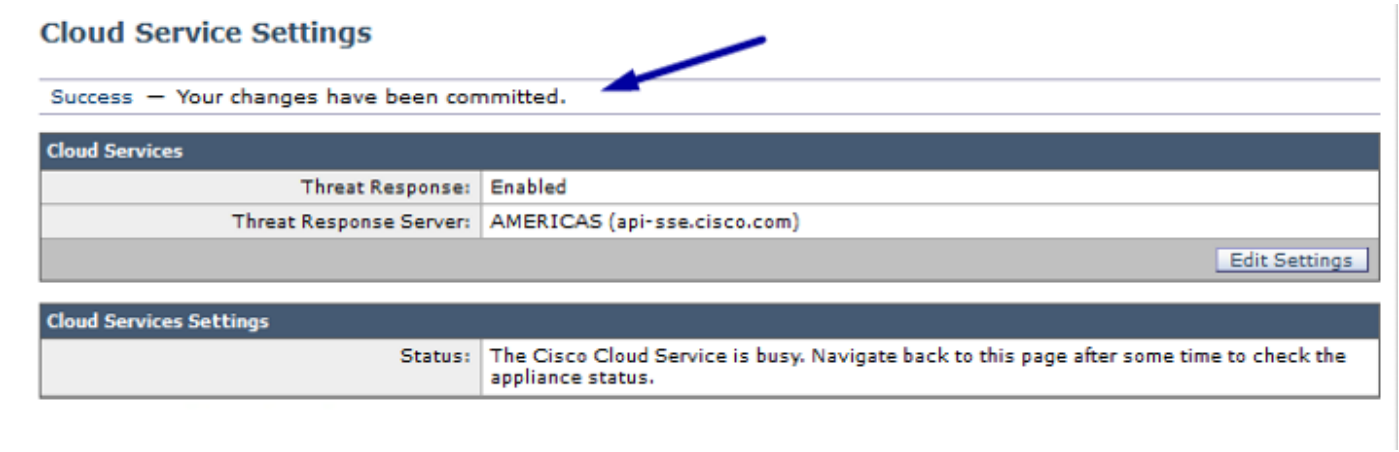
> Opmerking: De standaardselectie voor de URL van de Threat Response Server is AMERICAS (api-sse.cisco.com). Voor bedrijven in EUROPA klikt u op het vervolgkeuzemenu en kiest u EUROPA (api.eu.sse.itd.cisco.com)

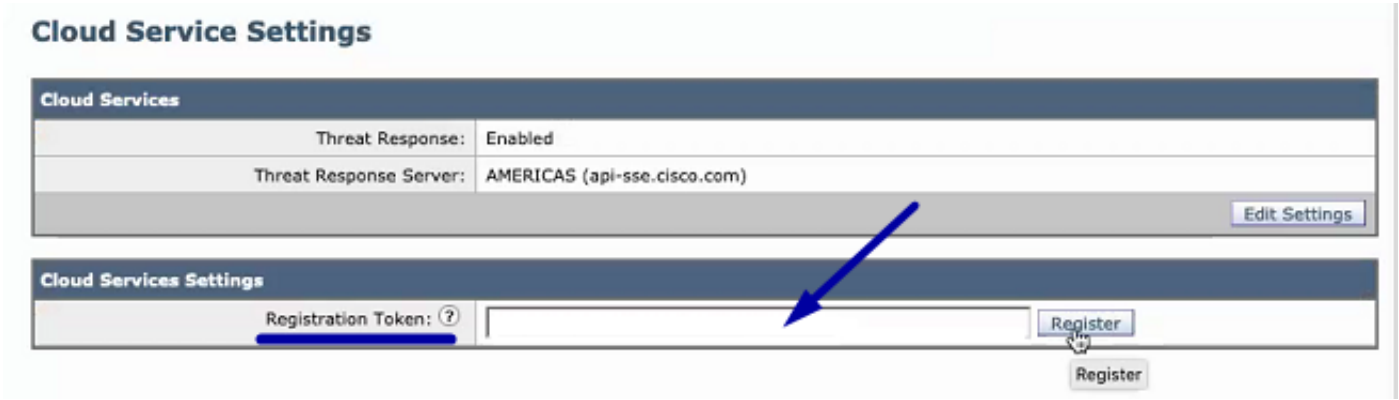
Stap 4. Breng wijzigingen aan en verbind deze

De wijzigingen moeten worden ingediend en vastgelegd, zodat deze kunnen worden opgeslagen en toegepast. Wanneer de ESA-interface is ververst, wordt om een Registratieteken verzocht om de integratie te registreren, zoals in de afbeelding hieronder wordt weergegeven.

> Opmerking: U kunt een Success bericht zien: Uw wijzigingen zijn geëngageerd.

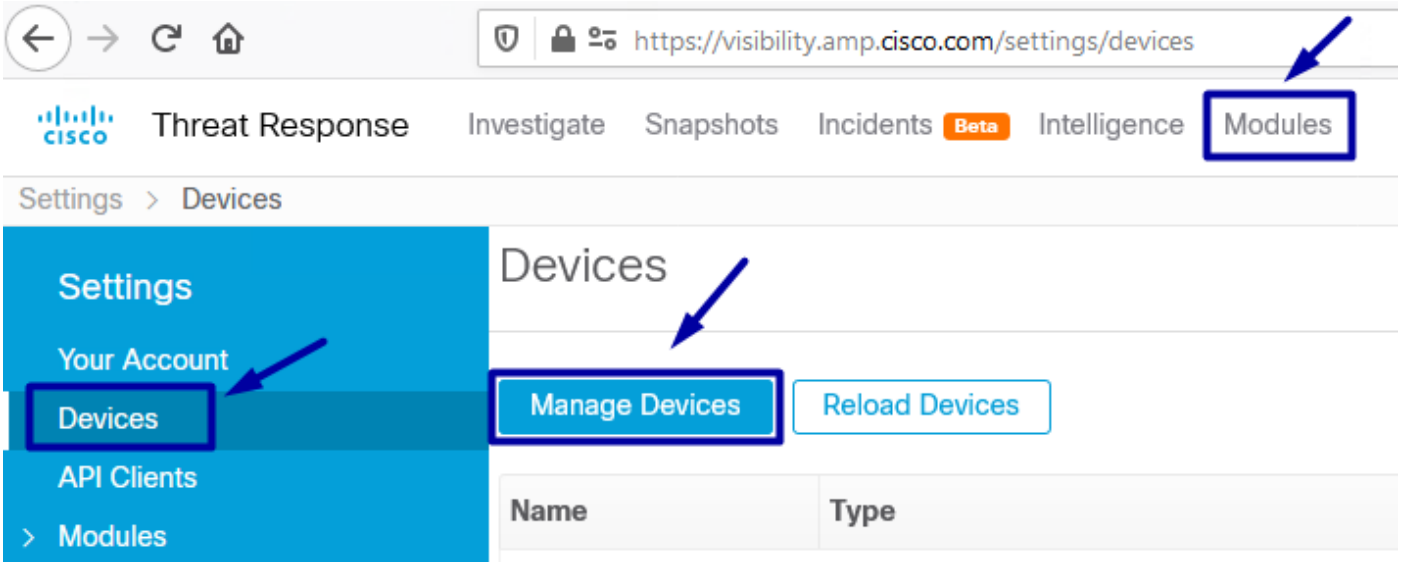




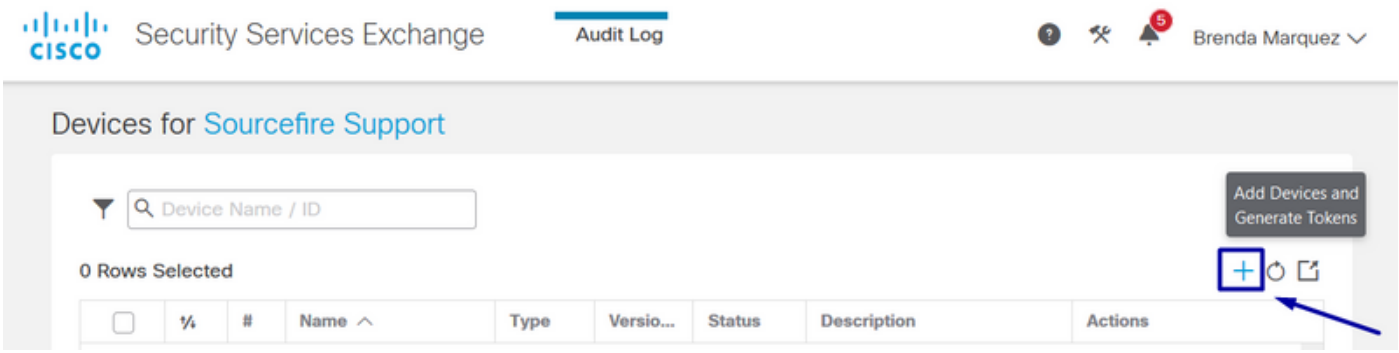


Stap 5. Meld u aan bij het CTR-portaal en genereert u het in het ESR-systeem gevraagde registratietoken

1. - Eerst in het CTR-portal, navigeer naar modules > Apparaten > Apparaten beheren, raadpleeg de volgende afbeelding.

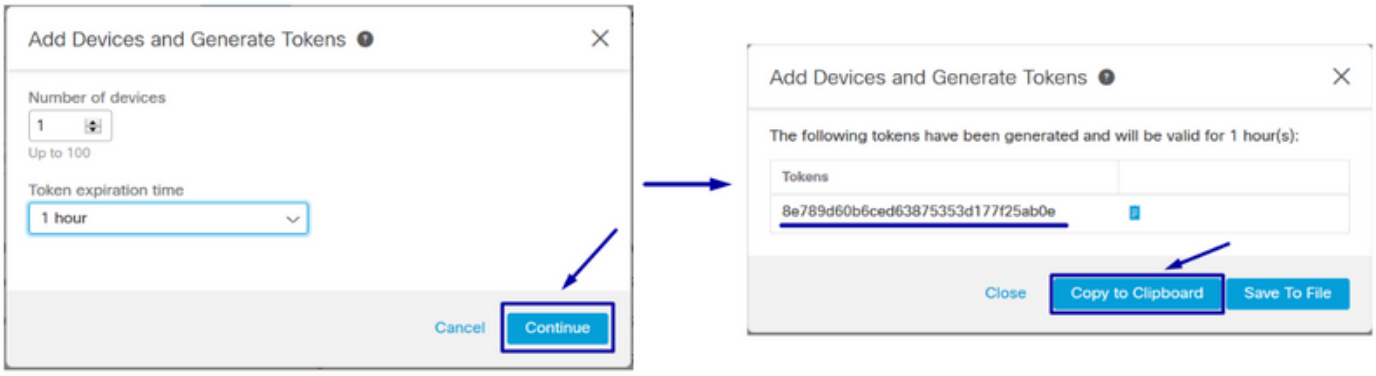


2.- De verbinding van Managed Devices richt u op de Uitwisseling van de Beveiliging (SSE), zodra daar, klik op het pictogram Add Devices en Generate Tokens zoals in de afbeelding.



3.- Klik op Doorgaan om Token te genereren zodra Token gegenereerd is, klikt u op in Kopie naar klembord, zoals in de afbeelding.

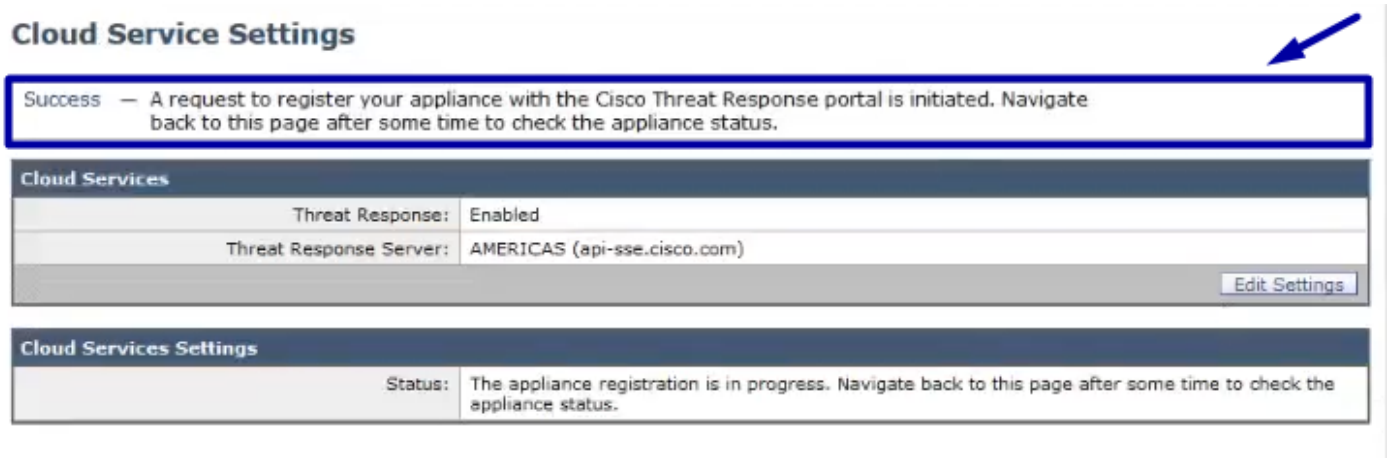
> **Tip**: U kunt het aantal toe te voegen apparaten selecteren (van 1 en tot 100) en ook de Token verlooptijd selecteren (1 uur, 2 uur, 4 uur, 6 uur, 8 uur, 12 uur, 12 dagen, 20 dagen, 30 dagen, 40 dagen en 5 dagen).



Stap 6. Plakt het registratietoken (gegenereerd vanuit het CTR-portaal) in het ESA

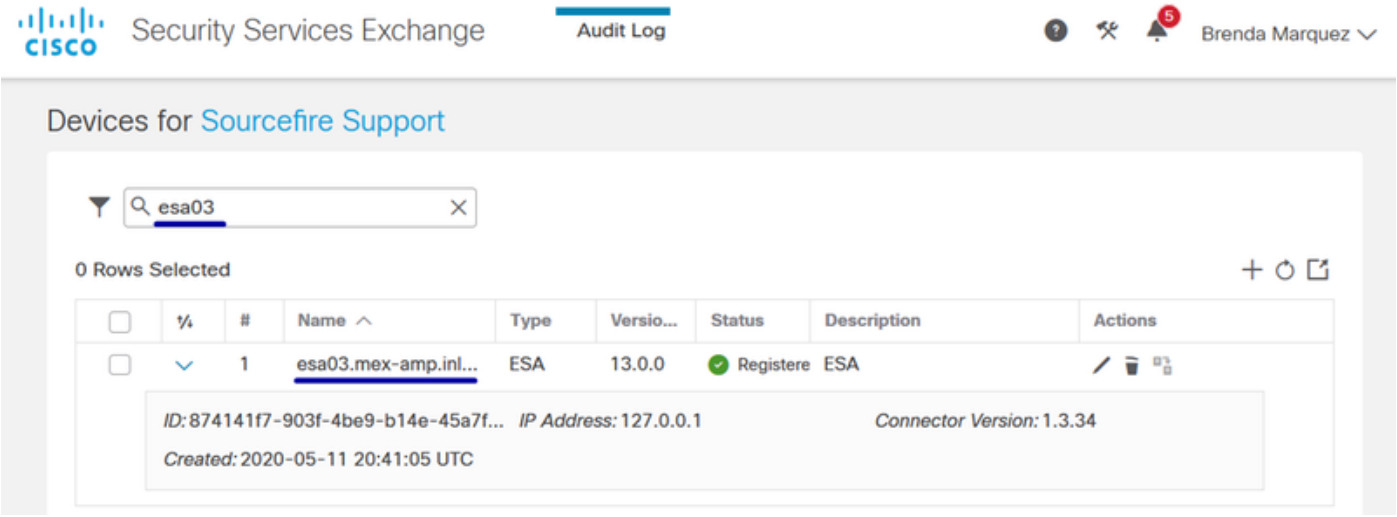
Nadat het Registratieteken is gegenereerd, plakt u het in het gedeelte Cloud Services-instellingen in het ESR, zoals de afbeelding hieronder.

> Opmerking: U kunt een Success bericht zien: Een verzoek om uw apparaat te registreren met het Cisco Threat Response-portaal wordt gestart. Navigeer na enige tijd naar deze pagina om de status van het apparaat te controleren.



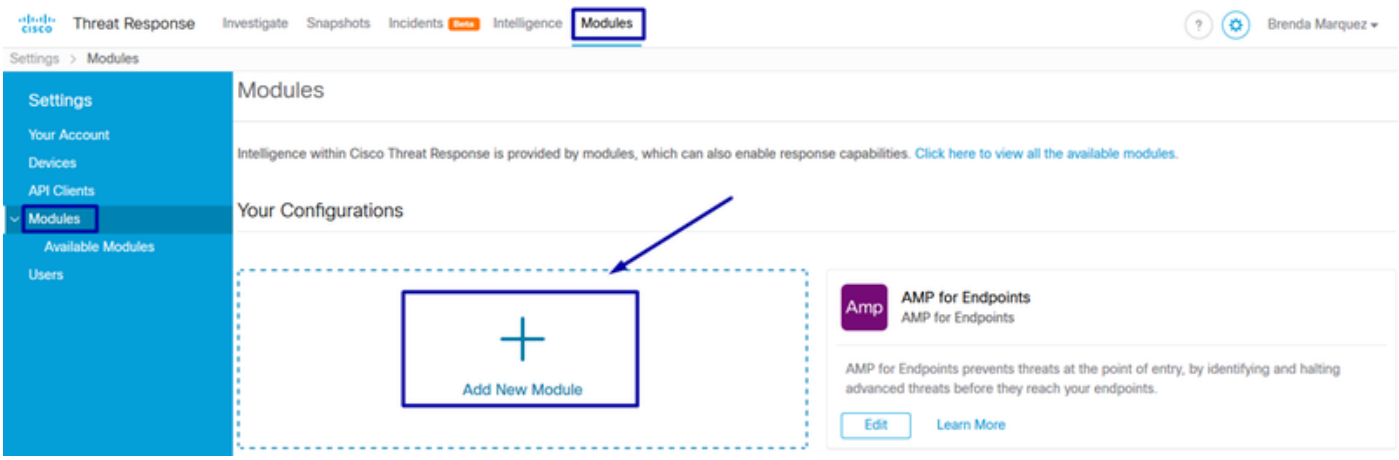
Stap 7. Controleer dat uw ESA-apparaat in het SSE-portaal staat

U kunt navigeren naar het SSE-portaal (CTR > Modules > Apparaten > Apparaten beheren) en in het tabblad Zoeken naar uw ESA-apparaat, zoals in de afbeelding weergegeven.

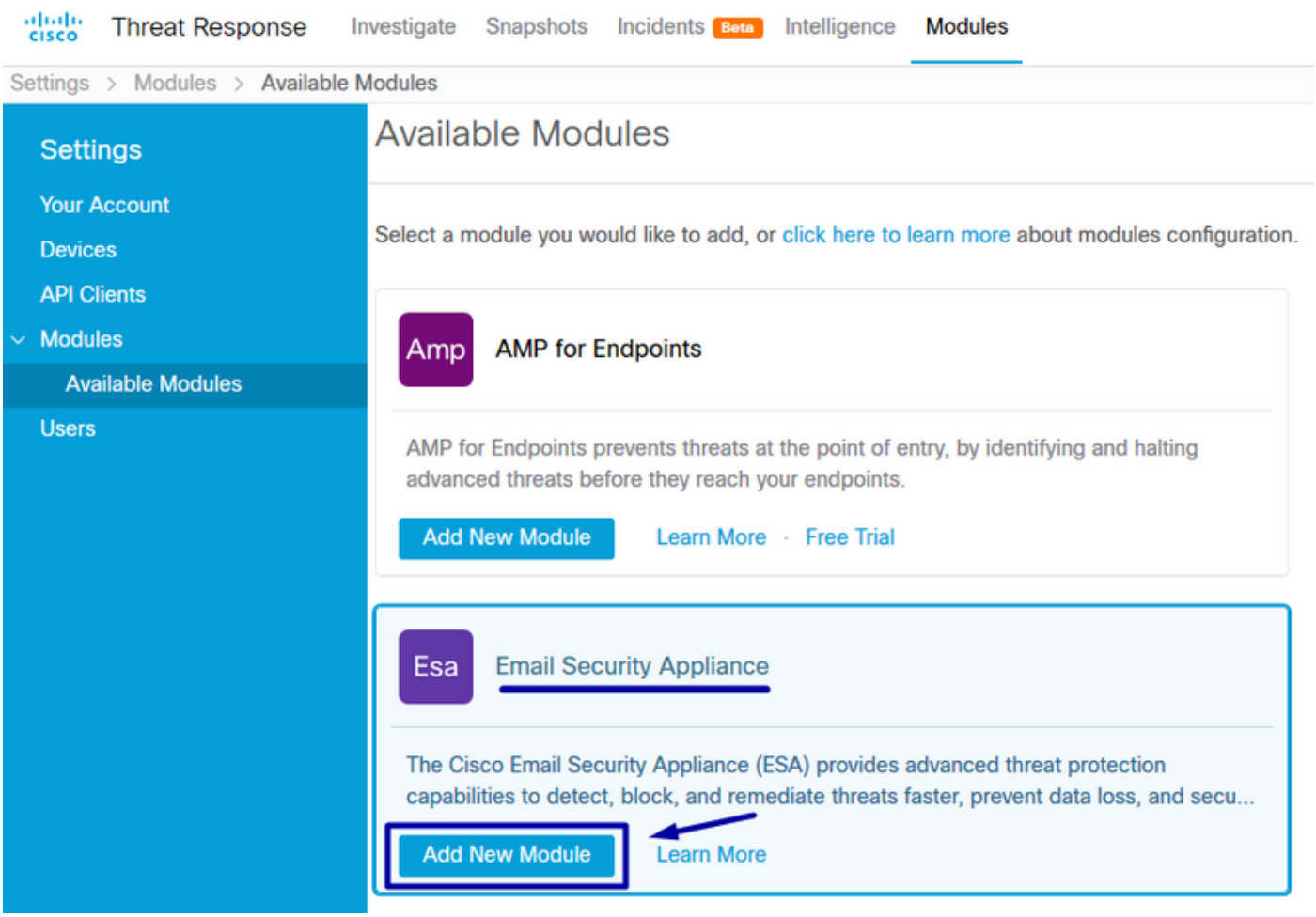


Stap 8. Navigeer naar het CTR-portaal en voeg een nieuwe ESA-module toe

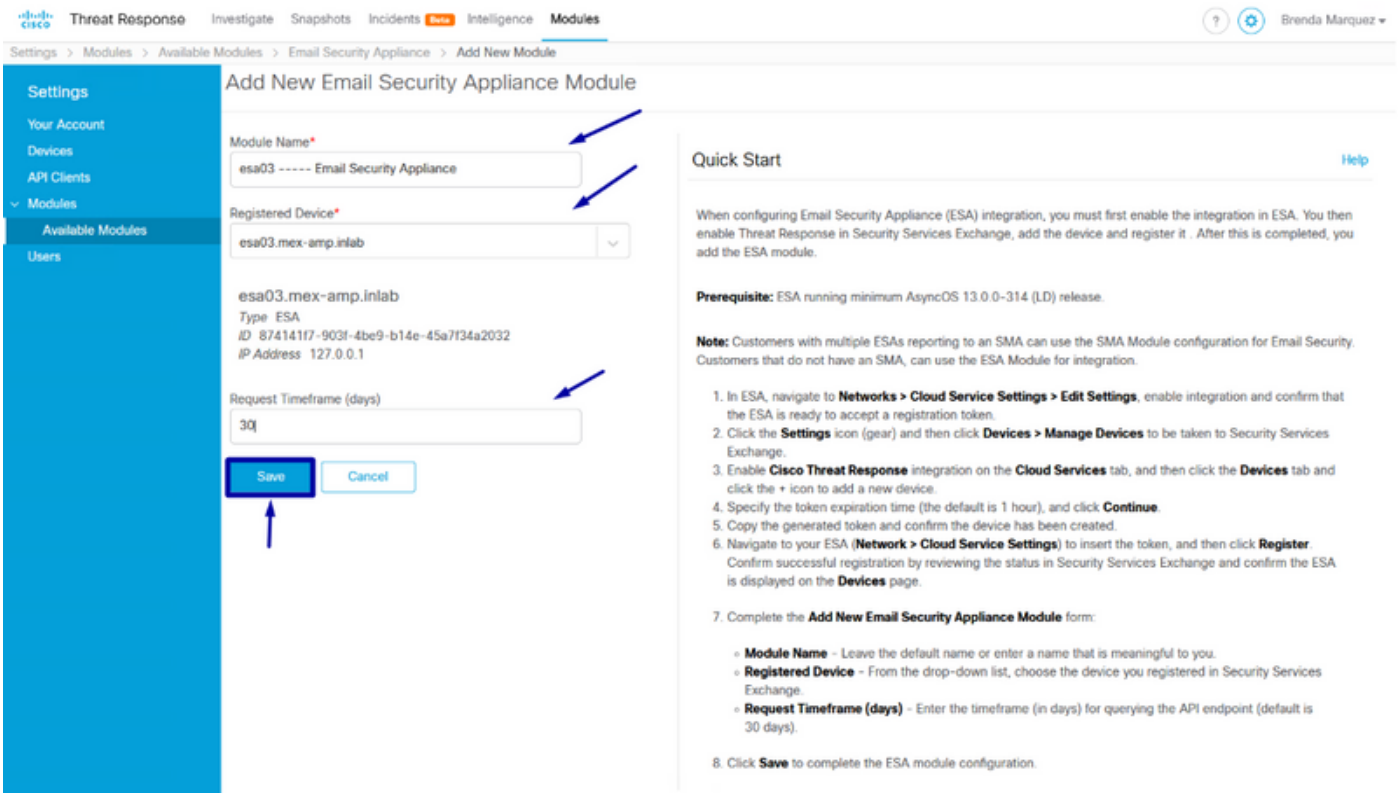
1.- Zodra u in het CTR-portal bent, navigeer dan naar modules > Nieuwe module toevoegen, zoals in de afbeelding.



2.- Kies het moduletype, in dit geval is de module een e-mail security applicatiemodule zoals in de onderstaande afbeelding.

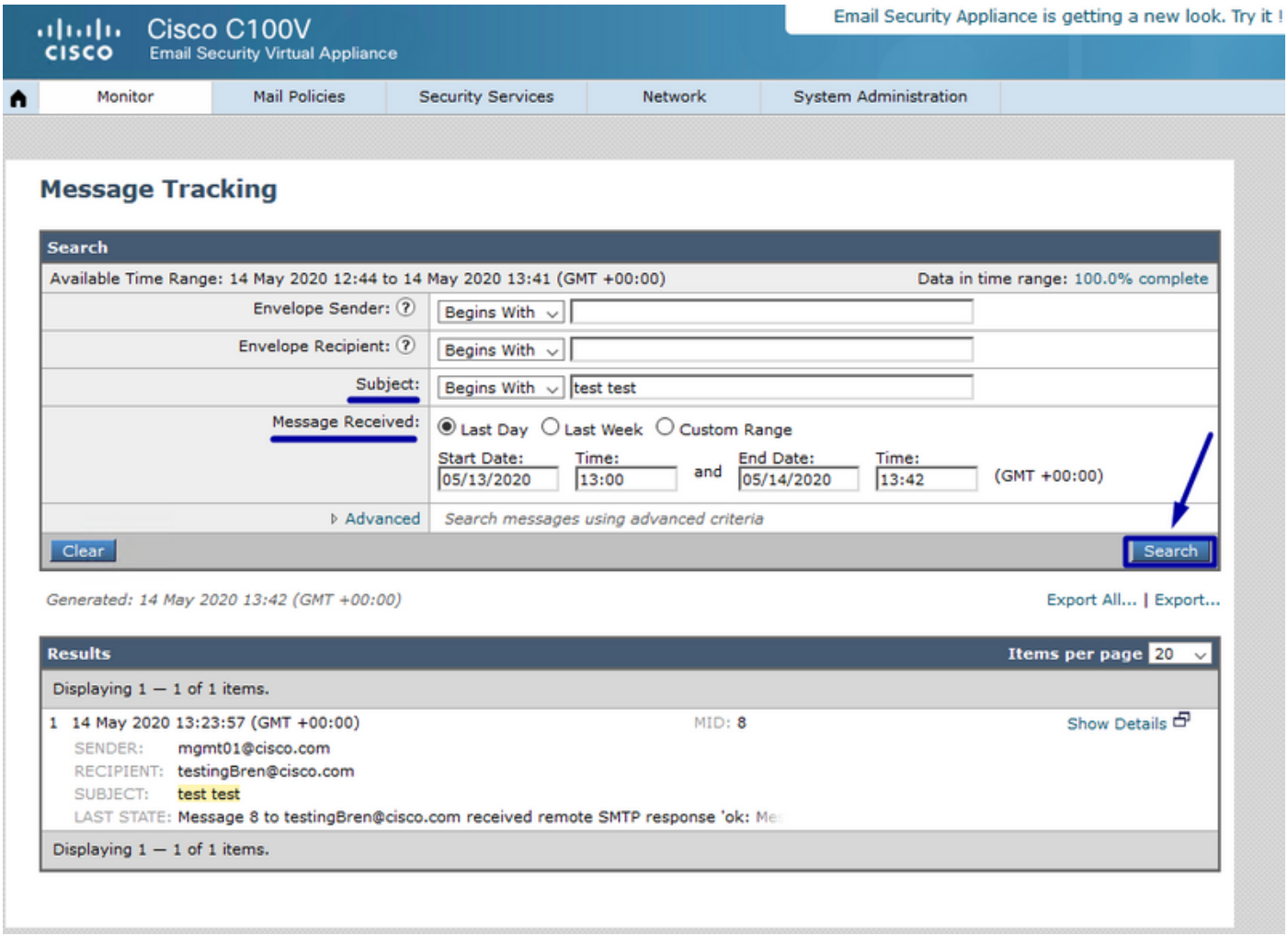


3.- Voer de velden in: Module naam, geregistreerd apparaat (selecteer het apparaat dat eerder geregistreerd is) en Time-frame (dagen) aanvragen en opslaan, zoals in de afbeelding.

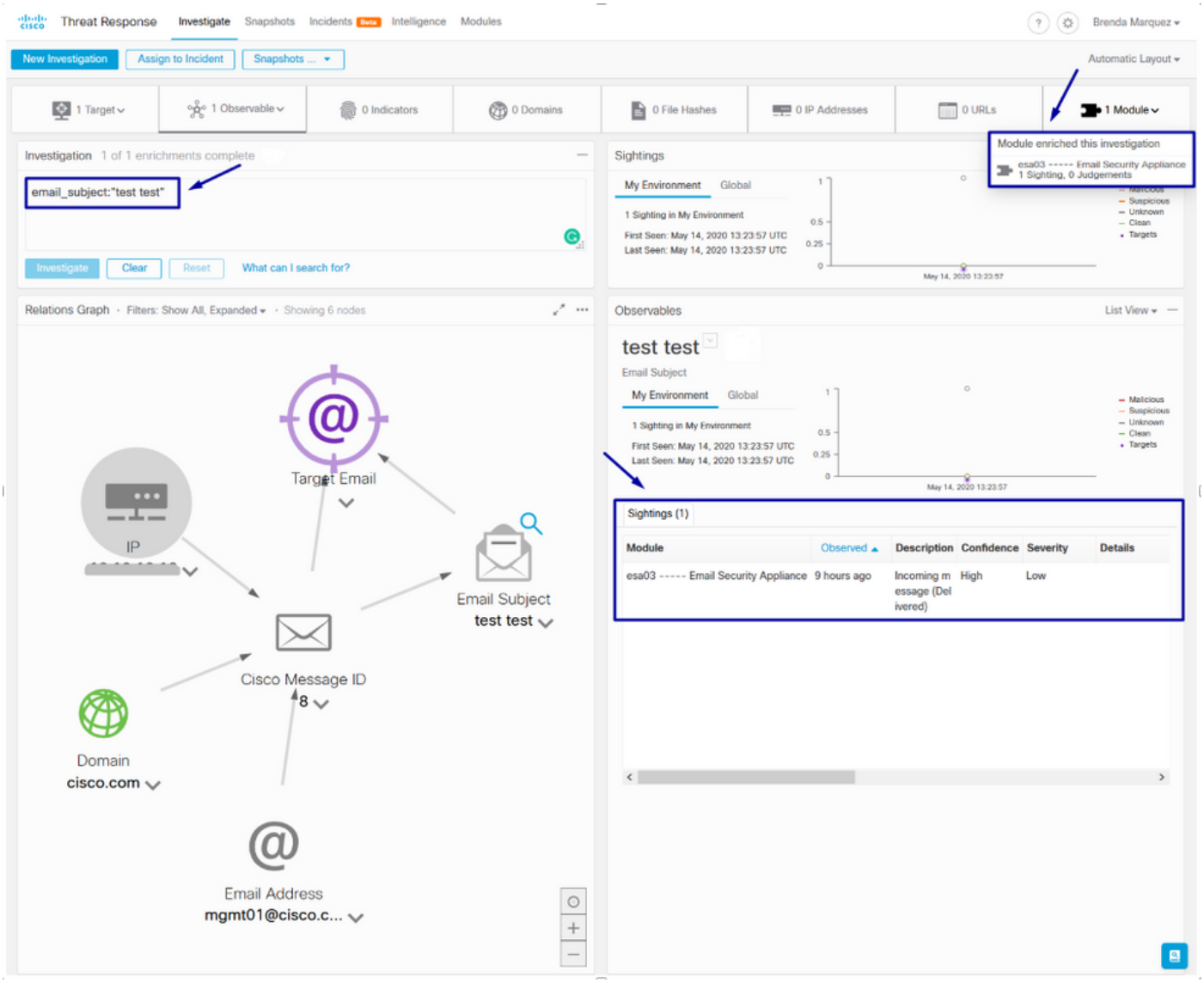


Verifiëren

Om de CTR en ESA Integratie te verifiëren kunt u een test e-mail verzenden, die u ook van uw ESA kunt zien, navigeren om > Message Tracking te controleren en de test e-mail te vinden. In dit geval heb ik per e-mail onderwerpt als de afbeelding hieronder.



Vanaf het CTR-portaal kun je een onderzoek uitvoeren, navigeren om te onderzoeken, en sommige e-mailobserveermiddelen gebruiken, zoals in de afbeelding.



Tip: U kunt de syntaxis van hetzelfde bestand gebruiken voor andere e-mailwaarnemingen als volgt in de afbeelding.

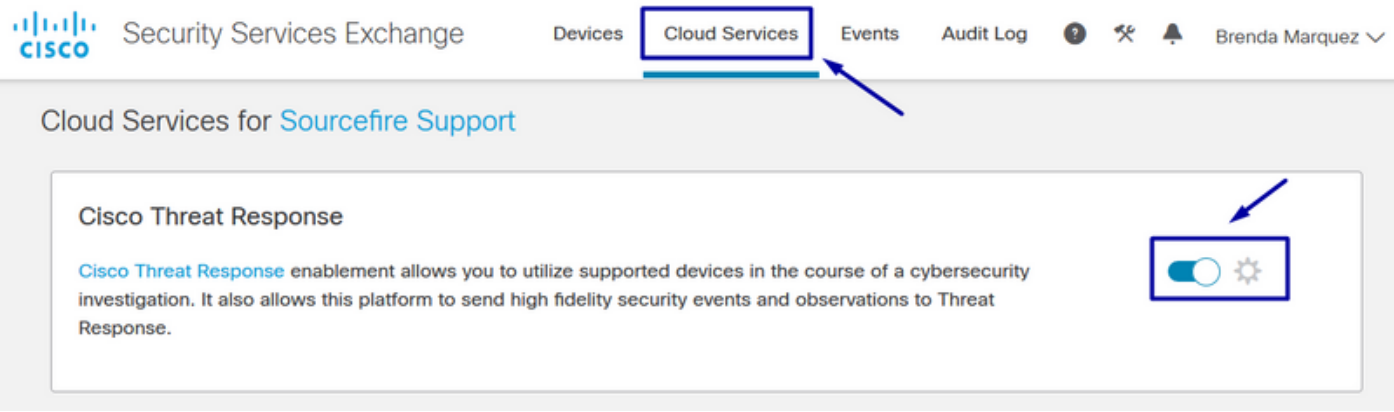
IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file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

Problemen oplossen

Als u een CES-klant bent of als u uw ESA-apparaten beheert via een SMA, kunt u alleen verbinding maken met Threat Response via uw SMA. Zorg ervoor dat uw SMA AsyncOS 12.5 of hoger draait. Als u de ESA niet bestuurt met een SMA en u de ESA niet direct integreert, zorg er dan voor dat deze bij AsyncOS versie 13.0 of hoger is.

ESA-voorziening is niet aangegeven in het CTR-portaal

Als uw ESA apparaat niet wordt getoond in het vervolgkeuzemodules Geregistreerd Apparaat terwijl de ESA module wordt toegevoegd in het CTR portal, zorg er dan voor dat CTR in SSE is ingeschakeld, in CTR navigeer naar modules > Apparaten > Apparaten beheren, dan in SSE portal navigeren naar Cloud Services en CTR inschakelen, zoals de afbeelding hieronder:



Het CTR-onderzoek toont geen gegevens van de ESA

Zorg ervoor dat:

- De syntaxis van het onderzoek is juist, de e-mailwachtrijen worden hierboven weergegeven in de sectie Verifiëren.
- U hebt de juiste dreigingsserver of de juiste cloud geselecteerd (Amerika/Europa).

ESA vraagt niet om het Registratiepunt

Zorg ervoor dat de wijzigingen worden vastgelegd, als Threat Response is ingeschakeld, anders worden de wijzigingen niet toegepast op de Threat Response sectie in de ESA.

Registratie mislukt vanwege een ongeldig of verlopen token

Zorg ervoor dat het token gegenereerd is vanuit de juiste cloud:

Als u Europa (EU) Cloud for ESA gebruikt, leid het token op: https://admin.eu.sse.itd.cisco.com/

Als u de America's (NAM) Cloud for ESA gebruikt, genereert u het token op: https://admin.sse.itd.cisco.com/

Bedenk ook dat het Registratieteken een verlooptijd heeft (selecteer de meest geschikte tijd om de Integratie op tijd te voltooien).

Gerelateerde informatie

- **U kunt de informatie in dit artikel vinden in de Cisco Threat Response en ESA Integration video.**
- Technische ondersteuning en documentatie – Cisco Systems