

# Cisco Threat Response (CTR) en ESA-integratie

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Stap 1. Navigeren in naar Network > Cloud Service-instellingen](#)

[Stap 2. Klik op Instellingen bewerken](#)

[Stap 3. Selecteer het selectieteken Inschakelen en de Threat Response Server](#)

[Stap 4. Breng wijzigingen aan en verbind deze](#)

[Stap 5. Meld u aan bij het CTR-portaal en genereert u het in het ESR-systeem gevraagde registratietoken](#)

[Stap 6. Plakt het registratietoken \(gegenereerd vanuit het CTR-portaal\) in het ESA](#)

[Stap 7. Controleer dat uw ESA-apparaat in het SSE-portaal staat](#)

[Stap 8. Navigeer naar het CTR-portaal en voeg een nieuwe ESA-module toe](#)

[Verifiëren](#)

[Problemen oplossen](#)

[ESA-voorziening is niet aangegeven in het CTR-portaal](#)

[Het CTR-onderzoek toont geen gegevens van de ESA](#)

[ESA vraagt niet om het Registratiepunt](#)

[Registratie mislukt vanwege een ongeldig of verlopen token](#)

[Gerelateerde informatie](#)

## 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

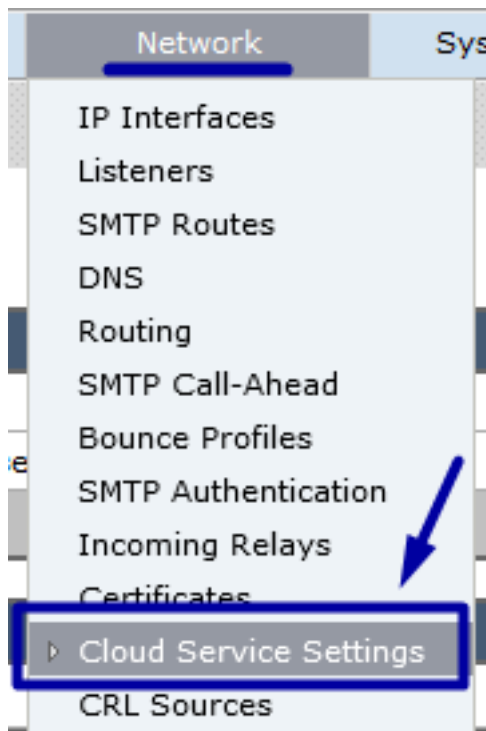
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht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

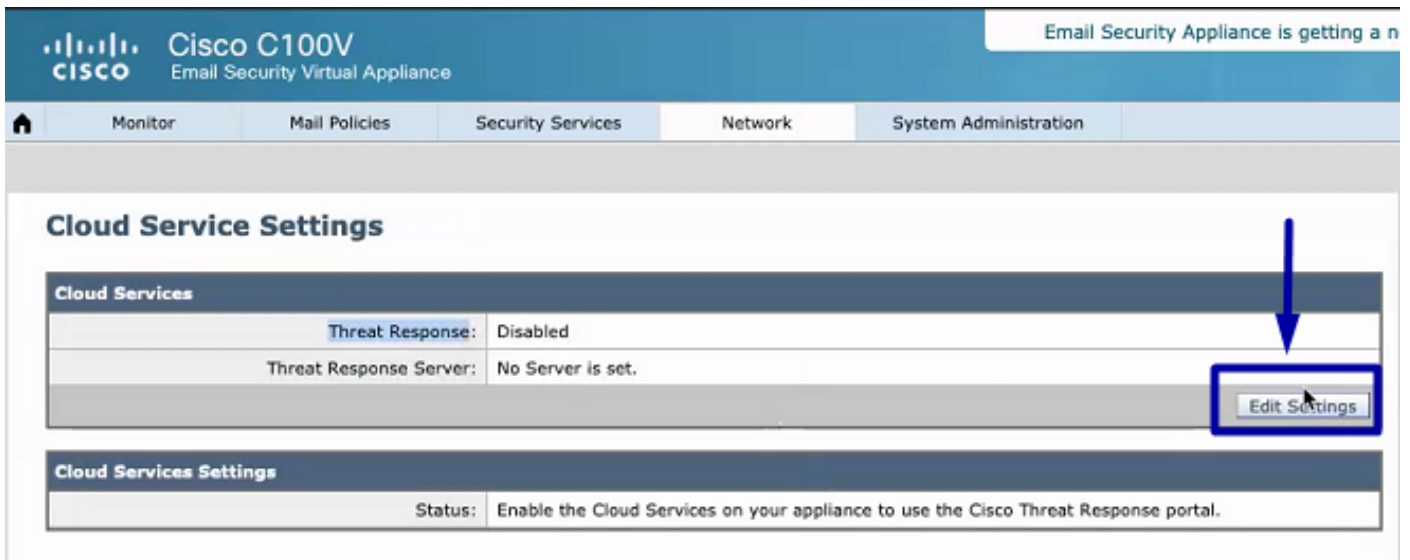
### Stap 1. Navigeren in naar Network > Cloud Service-instellingen

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 selectietekentje Inschakelen en de Threat Response Server

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

#### Cloud Service Settings

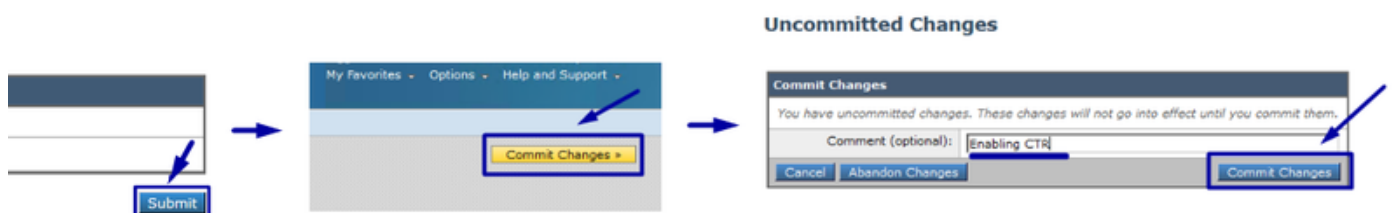


Opmerking: De standaardselectie voor de URL van de Threat Response Server is AMERICAS (api-sse.cisco.com). Voor bedrijven in EUROPA klikt u op het vervolgkeuzemenu en kiest u EUROPA (api.eu.sse.itd.cisco.com)

### 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 ververs, 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.



## Cloud Service Settings

Success — Your changes have been committed.

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
<a href="#">Edit Settings</a>	

Cloud Services Settings	
Status:	The Cisco Cloud Service is busy. Navigate back to this page after some time to check the appliance status.

## Cloud Service Settings

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
<a href="#">Edit Settings</a>	

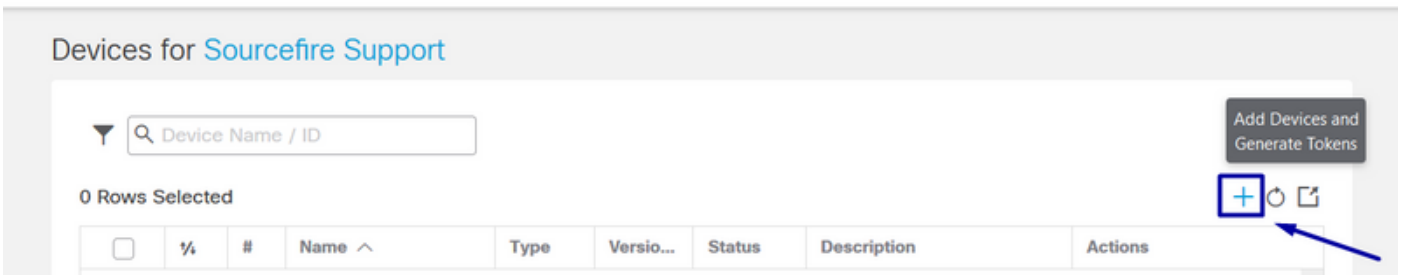
Cloud Services Settings	
Registration Token: ?	<input type="text"/>
<a href="#">Register</a>	

## 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.

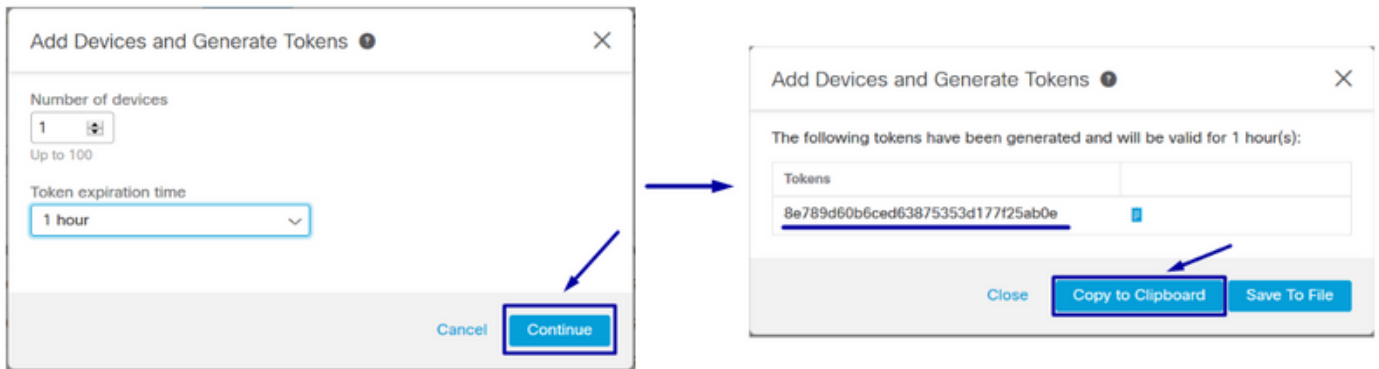
The screenshot shows a web browser at the URL <https://visibility.amp.cisco.com/settings/devices>. The navigation menu includes Threat Response, Investigate, Snapshots, Incidents (Beta), Intelligence, and Modules. The 'Modules' menu item is highlighted with a blue box and an arrow. Below the navigation, the breadcrumb 'Settings > Devices' is shown. The 'Devices' page header is also highlighted with a blue box and an arrow. In the left sidebar, 'Your Account' is highlighted with a blue box and an arrow, and 'Devices' is highlighted with a blue box and an arrow. In the main content area, the 'Manage Devices' button is highlighted with a blue box and an arrow. Below the buttons, a table with columns 'Name' and 'Type' is visible.

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.

### Cloud Service Settings



## Cloud Service Settings

Success — A request to register your appliance with the Cisco Threat Response portal is initiated. Navigate back to this page after some time to check the appliance status.

### Cloud Services

Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)

[Edit Settings](#)

### Cloud Services Settings

Status:	The appliance registration is in progress. Navigate back to this page after some time to check the appliance status.
---------	--

## 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.

Security Services Exchange Audit Log Brenda Marquez

### Devices for Sourcefire Support

Search:

0 Rows Selected

	%	#	Name ^	Type	Versio...	Status	Description	Actions
<input type="checkbox"/>	▼	1	esa03.mex-amp.inl...	ESA	13.0.0	Registere	ESA	

ID: 874141f7-903f-4be9-b14e-45a7f... IP Address: 127.0.0.1 Connector Version: 1.3.34  
Created: 2020-05-11 20:41:05 UTC

## 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.

Threat Response Investigate Snapshots Incidents Intelligence **Modules** Brenda Marquez

Settings > Modules

### Modules

Intelligence within Cisco Threat Response is provided by modules, which can also enable response capabilities. [Click here to view all the available modules.](#)

#### Your Configurations

[Add New Module](#)

**Amp** AMP for Endpoints  
AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach your endpoints.  
[Edit](#) [Learn More](#)

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

Settings

Your Account

Devices

API Clients

Modules

Available Modules

Users

## Available Modules

Select a module you would like to add, or [click here to learn more](#) about modules configuration.

**Amp** AMP for Endpoints

AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach your endpoints.

[Add New Module](#) [Learn More](#) · [Free Trial](#)

**Esa** Email Security Appliance

The Cisco Email Security Appliance (ESA) provides advanced threat protection capabilities to detect, block, and remediate threats faster, prevent data loss, and secu...

[Add New Module](#) [Learn More](#)

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.

Threat Response Investigate Snapshots Incidents Beta Intelligence Modules Brenda Marquez

Settings > Modules > Available Modules > Email Security Appliance > Add New Module

### Add New Email Security Appliance Module

Module Name\*

Registered Device\*

esa03.mex-amp.inlab  
Type ESA  
ID 874141f7-903f-4be9-b14e-45a7f34a2032  
IP Address 127.0.0.1

Request Timeframe (days)

[Save](#) [Cancel](#)

#### Quick Start [Help](#)

When configuring Email Security Appliance (ESA) integration, you must first enable the integration in ESA. You then enable Threat Response in Security Services Exchange, add the device and register it. After this is completed, you add the ESA module.

**Prerequisite:** ESA running minimum AsyncOS 13.0.0-314 (LD) release.

**Note:** Customers with multiple ESAs reporting to an SMA can use the SMA Module configuration for Email Security. Customers that do not have an SMA, can use the ESA Module for integration.

- In ESA, navigate to **Networks > Cloud Service Settings > Edit Settings**, enable integration and confirm that the ESA is ready to accept a registration token.
- Click the **Settings** icon (gear) and then click **Devices > Manage Devices** to be taken to Security Services Exchange.
- Enable **Cisco Threat Response** integration on the **Cloud Services** tab, and then click the **Devices** tab and click the + icon to add a new device.
- Specify the token expiration time (the default is 1 hour), and click **Continue**.
- Copy the generated token and confirm the device has been created.
- Navigate to your ESA (**Network > Cloud Service Settings**) to insert the token, and then click **Register**. Confirm successful registration by reviewing the status in Security Services Exchange and confirm the ESA is displayed on the **Devices** page.
- Complete the **Add New Email Security Appliance Module** form:
  - Module Name** - Leave the default name or enter a name that is meaningful to you.
  - Registered Device** - From the drop-down list, choose the device you registered in Security Services Exchange.
  - Request Timeframe (days)** - Enter the timeframe (in days) for querying the API endpoint (default is 30 days).
- Click **Save** to complete the ESA module configuration.

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.

**Cisco C100V**  
Email Security Virtual Appliance

Monitor | Mail Policies | Security Services | Network | System Administration

### Message Tracking

**Search**

Available Time Range: 14 May 2020 12:44 to 14 May 2020 13:41 (GMT +00:00) Data in time range: 100.0% complete

Envelope Sender: ? Begins With [ ]

Envelope Recipient: ? Begins With [ ]

Subject: Begins With test test

Message Received:  Last Day  Last Week  Custom Range

Start Date: 05/13/2020 Time: 13:00 and End Date: 05/14/2020 Time: 13:42 (GMT +00:00)

Advanced Search messages using advanced criteria

Clear Search

Generated: 14 May 2020 13:42 (GMT +00:00) Export All... | Export...

### Results

Items per page 20

Displaying 1 — 1 of 1 items.

1	14 May 2020 13:23:57 (GMT +00:00)	MID: 8	Show Details
---	-----------------------------------	--------	--------------

SENDER: mgmt01@cisco.com  
RECIPIENT: testingBren@cisco.com  
SUBJECT: test test  
LAST STATE: Message 8 to testingBren@cisco.com received remote SMTP response 'ok: Me:

Displaying 1 — 1 of 1 items.

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



The screenshot shows the Cisco Threat Response Investigate interface. At the top, there are navigation tabs: Threat Response, Investigate, Snapshots, Incidents, Intelligence, and Modules. The user is logged in as Brenda Marquez. The interface displays search filters for 1 Target, 1 Observable, 0 Indicators, 0 Domains, 0 File Hashes, 0 IP Addresses, 0 URLs, and 1 Module. The search query is `email_subject:'test test'`. The Relations Graph shows a central 'Email Subject test test' node connected to 'Target Email', 'Email Subject test test', 'Cisco Message ID 8', and 'Email Address mgmt01@cisco.c...'. The Sighting table shows one sighting from the 'esa03' module (Email Security Appliance) observed 9 hours ago, with a description of an incoming message and a confidence of High and severity of Low.

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

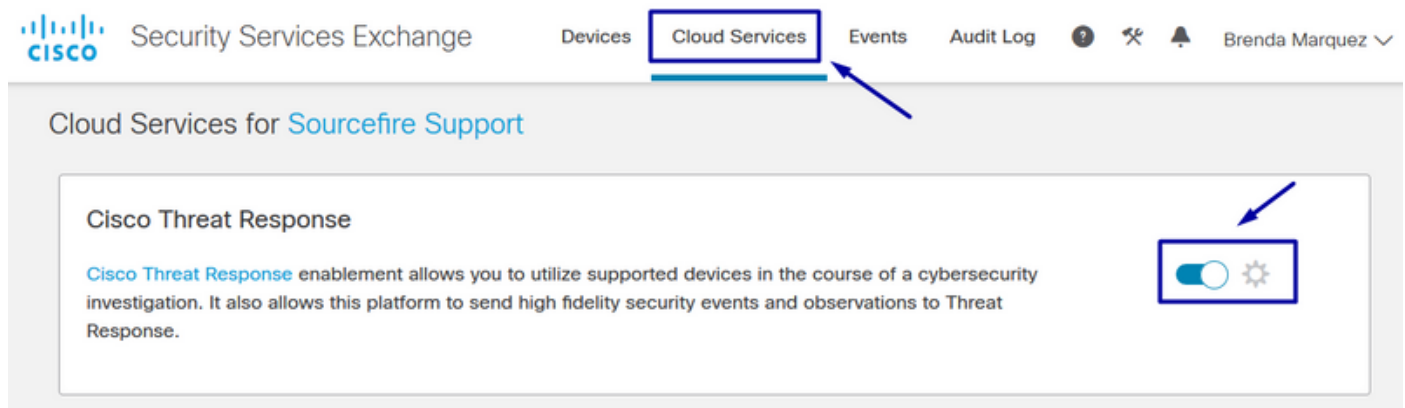
IP address	<code>ip:"4.2.2.2"</code>	Email subject	<code>email_subject:"Invoice Due"</code>
Domain	<code>domain:"cisco.com"</code>	Cisco Message ID (MID)	<code>cisco_mid:"12345"</code>
Sender email address	<code>email:"noreply@cisco.com"</code>	SHA256 filehash	<code>sha256:"sha256filehash"</code>
Email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

## 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](#)