WSA met CTR integreren

Inhoud

Inleiding

Dit document beschrijft de stappen om Web Security Appliance (WSA) te integreren met Cisco Threat Response (CTR) portal.

Bijgedragen door Shikha Grover en bewerkt door Yeraldin Sanchez Cisco TAC-engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- WSA-toegang
- Toegang tot CTR-portal
- Cisco-beveiligingsaccount

Gebruikte componenten

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

- Async Operating System versie 12.x of hoger

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

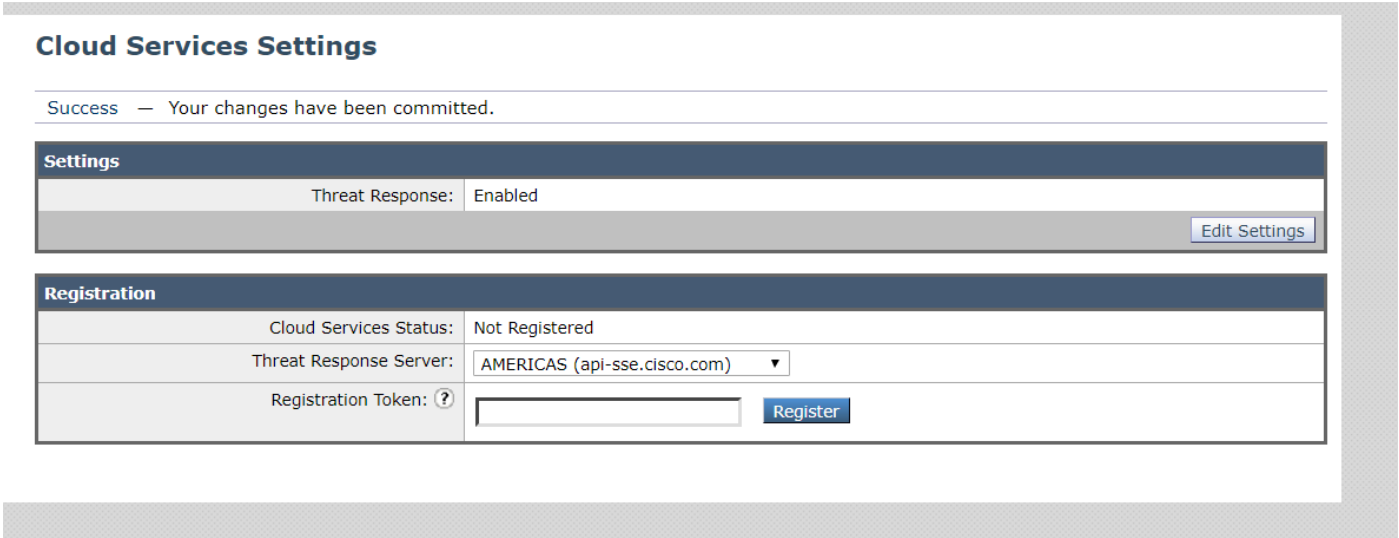
> **Voorzichtig:** Als u toegang hebt tot CTR met een regionale Zuidoost-Azië, Japan en China URL (https://visibility.apjc.amp.cisco.com/), wordt de integratie met uw apparaat momenteel niet ondersteund.

Stap 1. Schakel **CTROBSERVABLE in** onder CONFIG RAPPORTEREN in de CLI en sluit de wijzigingen aan, zoals in de afbeelding.

```
WSA-12-0-1-173.COM> reportingconfig


hoose the operation you want to perform:
 COUNTERS - Limit counters recorded by the reporting system.
 WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
 AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings
alculation.
 WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
 CTROBSERVABLE - Enable or Disable CTR observable based indexing.
 CENTRALIZED - Enable/Disable Centralized Reporting for this WSA appliance.
]> ctrobservable

TR observable indexing currently Enabled.
re you sure you want to change the setting? [N]> y


hoose the operation you want to perform:
 COUNTERS - Limit counters recorded by the reporting system.
 WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
 AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
 WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
 CTROBSERVABLE - Enable or Disable CTR observable based indexing.
 CENTRALIZED - Enable/Disable Centralized Reporting for this WSA appliance.
```

Stap 2. Configureer het cloudportal voor Security Service Exchange (SSE), navigeer naar **Network >Cloud Services-instellingen > Instellingen bewerken**, klik op **Enable** en **Submit**, zoals in de afbeelding.

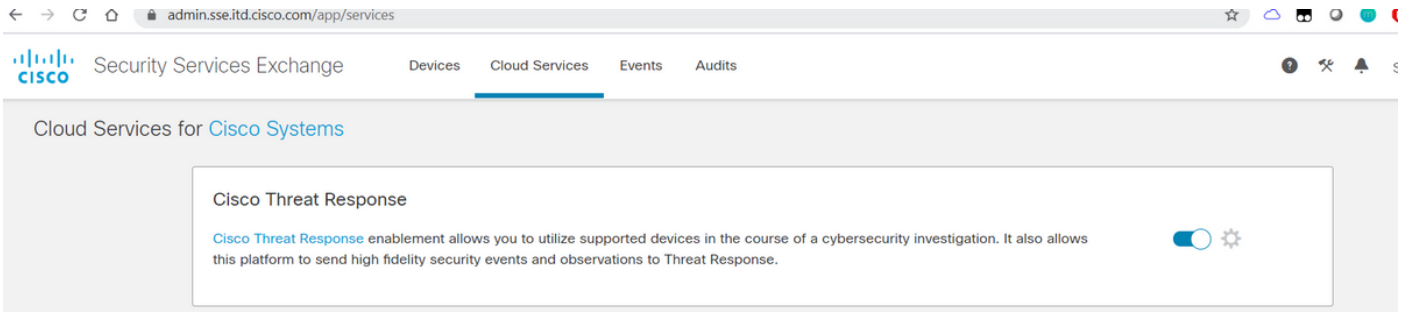
Kies de cloud op uw locatie, zoals in de afbeelding wordt weergegeven.



Stap 3. Als u geen Cisco Security-account hebt, kunt u een gebruikersaccount maken in het Cisco Threat Response-portaal met admin-toegangsrechten.

Als u een nieuwe gebruikersaccount wilt maken, navigeer dan naar de inlogpagina van het Cisco Threat Response-portaal.

Stap 4. Schakel Cisco Threat Response in onder Cloud Services op het SSE-portal, zoals in de afbeelding.



Stap 5. Zorg ervoor dat WSA bereikbaarheid heeft op poort 443 naar het SSE-portaal:

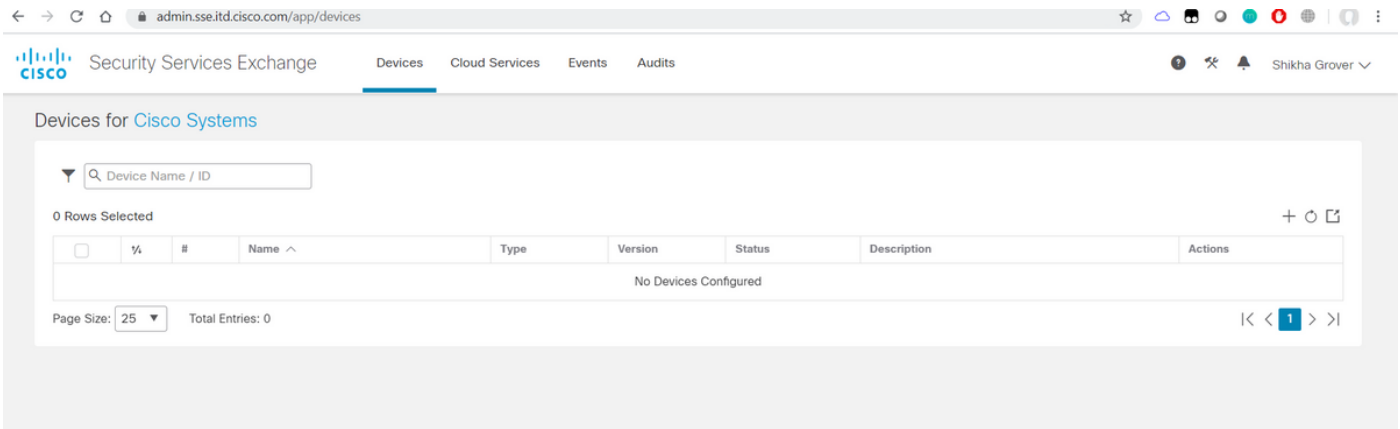
- api.eu.sse.itd.cisco.com (Europa)
- api-se.cisco.com (Amerika)

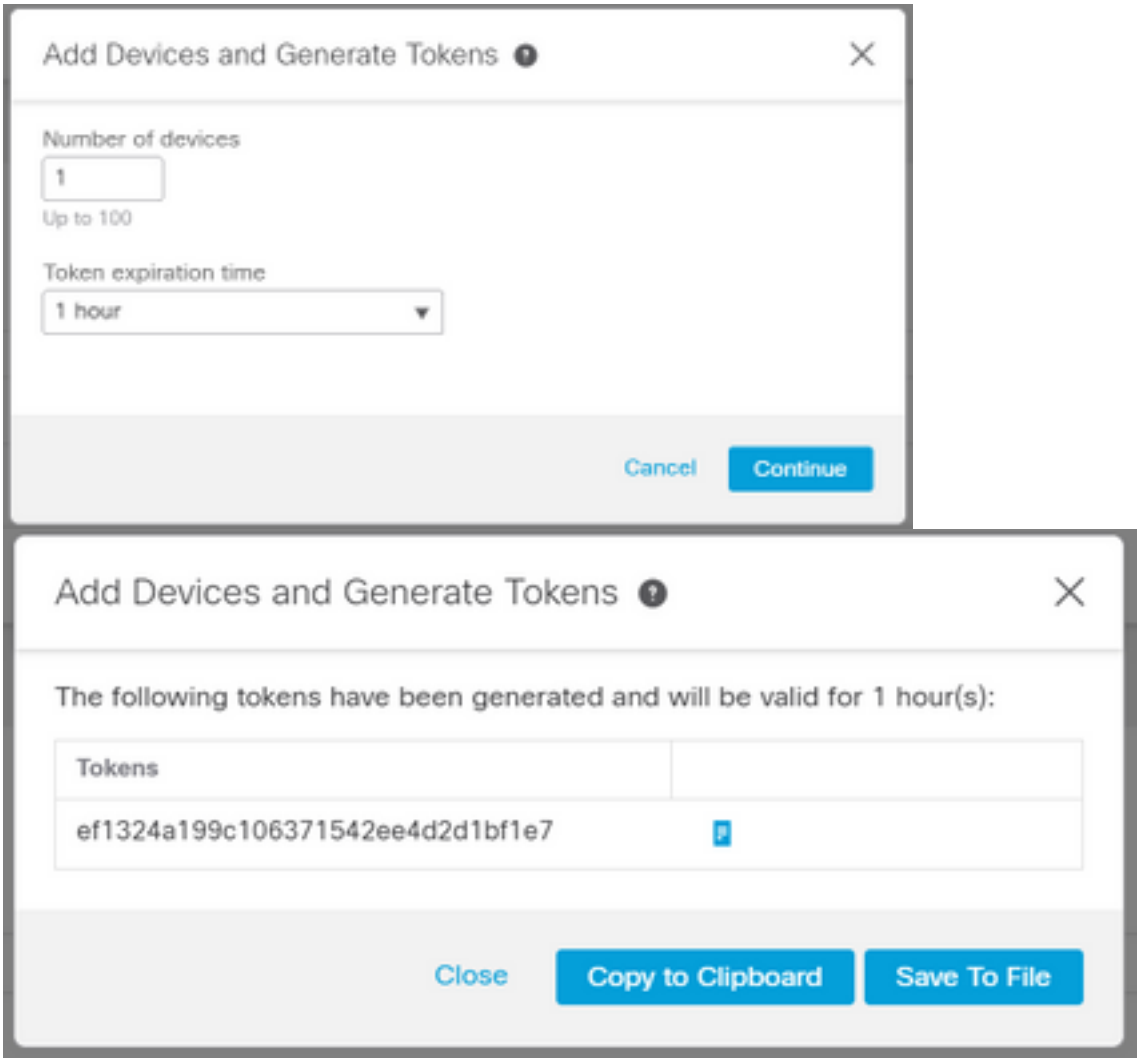
Registreer de applicatie

Stap 1. Verkrijg een registratiepunt van de Security Services Exchange (SSE)-portal om uw apparaat te registreren met de Security Services Exchange-portal.

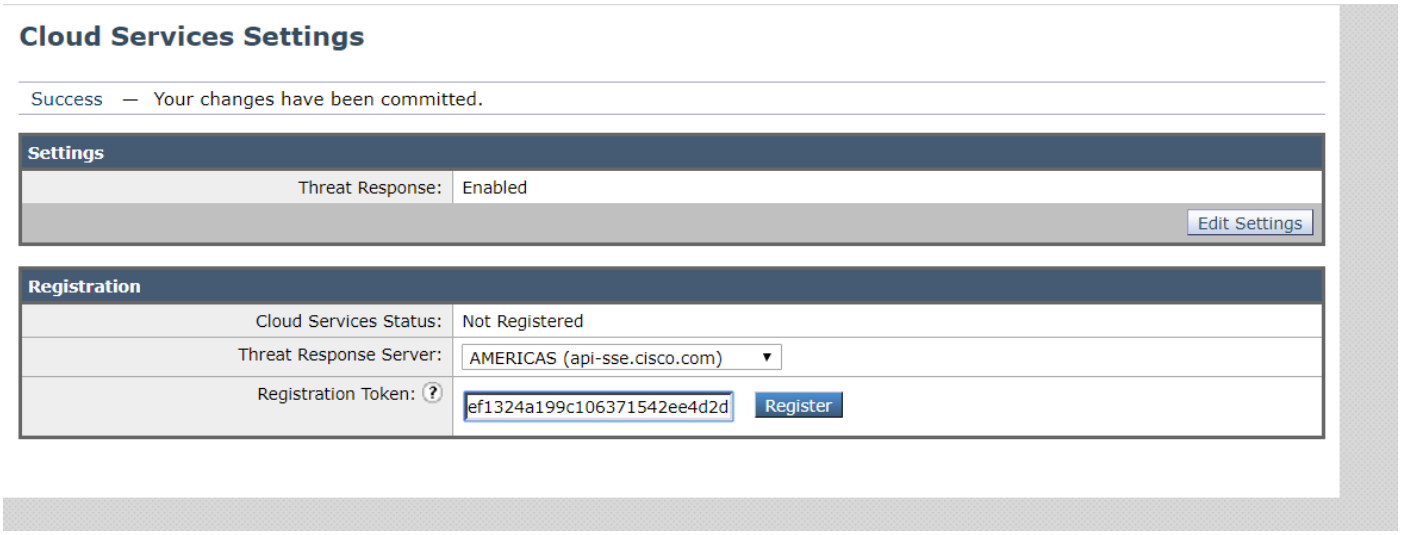
SSE portal link is https://admin.sse.itd.cisco.com/app/devices.

> Opmerking: Gebruik CTR-accountreferenties om in te loggen op SSE-portal.



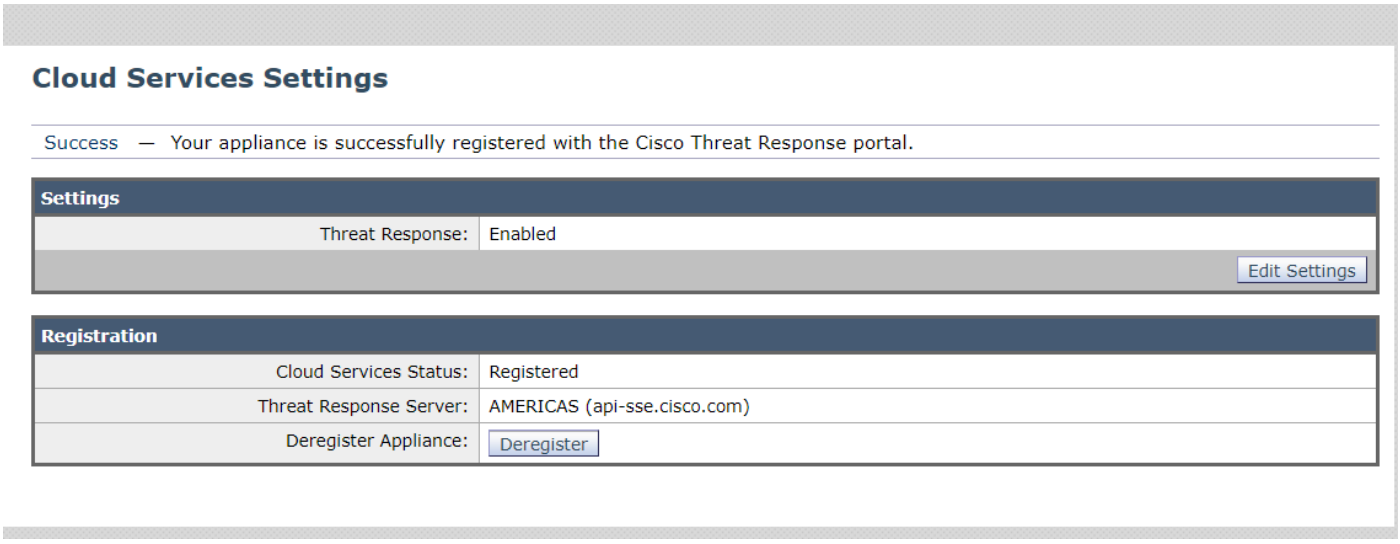


Stap 2. Voer het registratieteken in dat van het Exchange-portaal voor beveiligingsservices in WSA is verkregen en klik op **Registreer** zoals in de afbeelding.

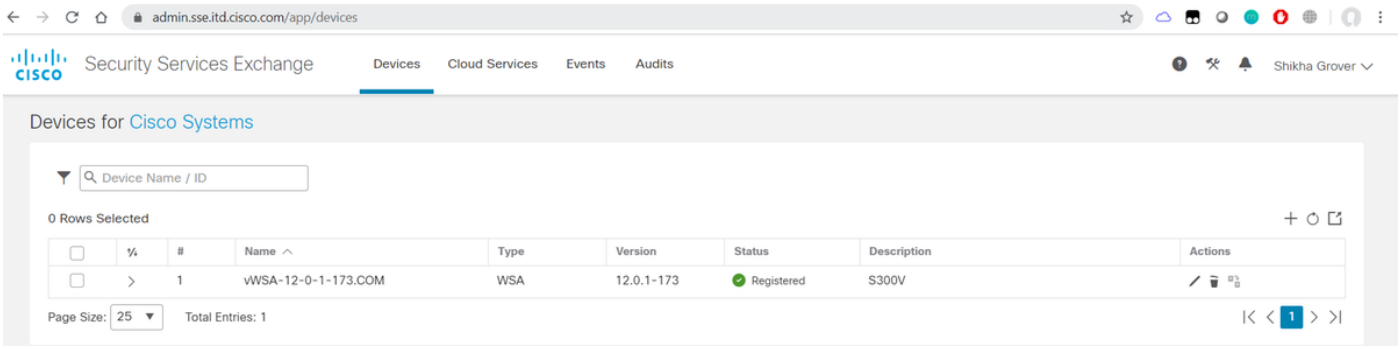


Stap 3. Na een paar seconden ziet u dat de registratie succesvol is.

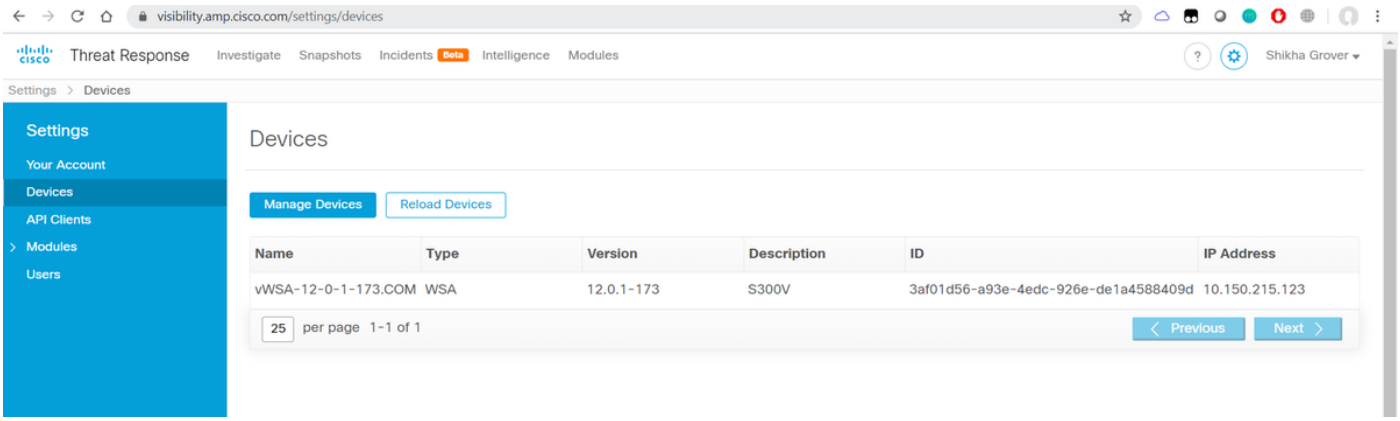
Voorzichtig: Zorg ervoor dat het gegenereerde token gebruikt wordt voordat het verlopen is.



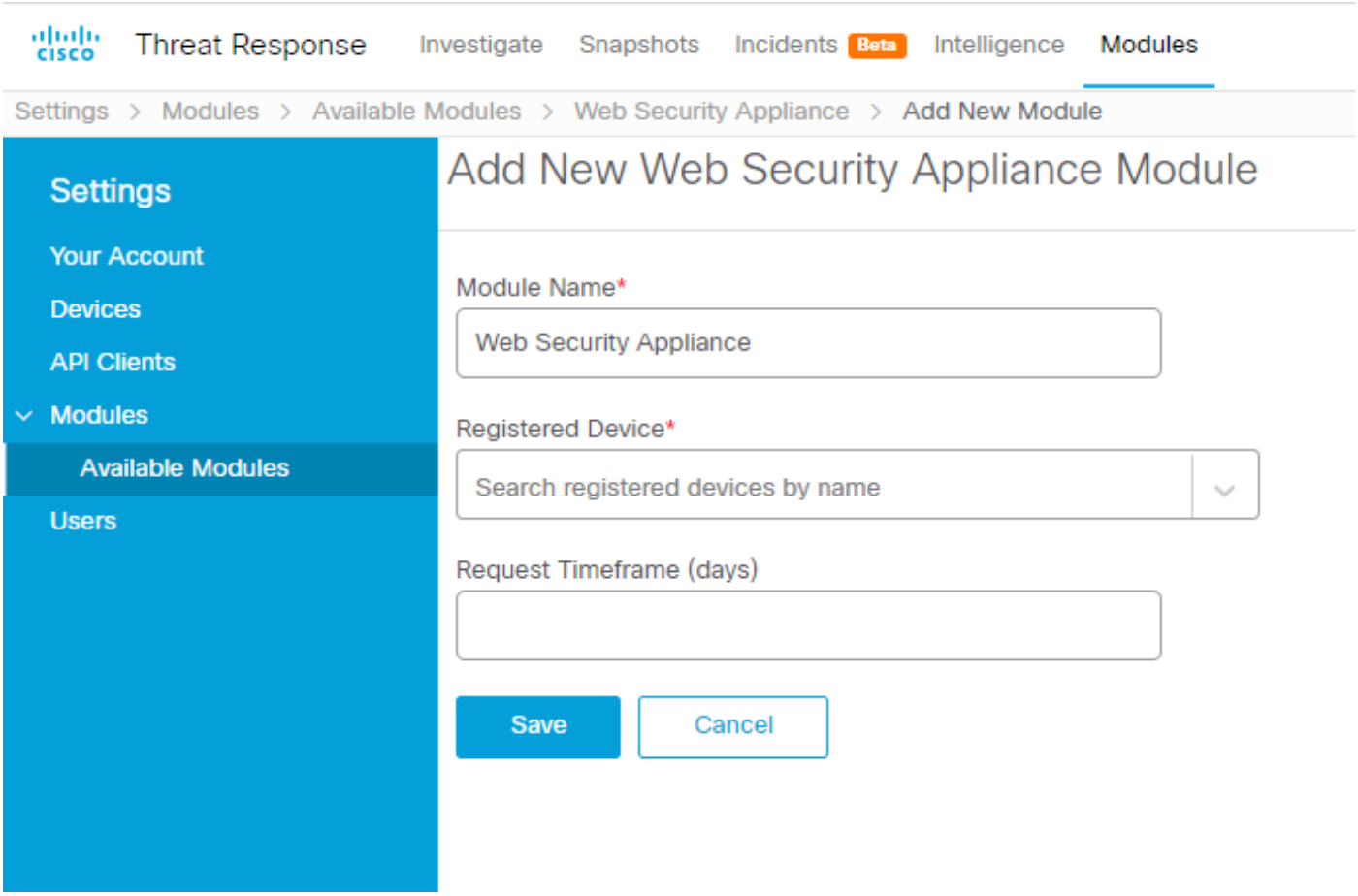
Stap 4.U kunt de status van het apparaat in het SSE-portaal zien.



Stap 5. Op het CTR-portaal verschijnt het geregistreerde apparaat.



U kunt dit apparaat koppelen aan een module, navigeer naar **modules > Nieuwe module toevoegen > Web security applicatie**, zoals in de afbeelding getoond.



Het apparaat is nu geïntegreerd. U kunt door het verkeer van de WSA gaan en bedreigingen op het CTR portaal onderzoeken.

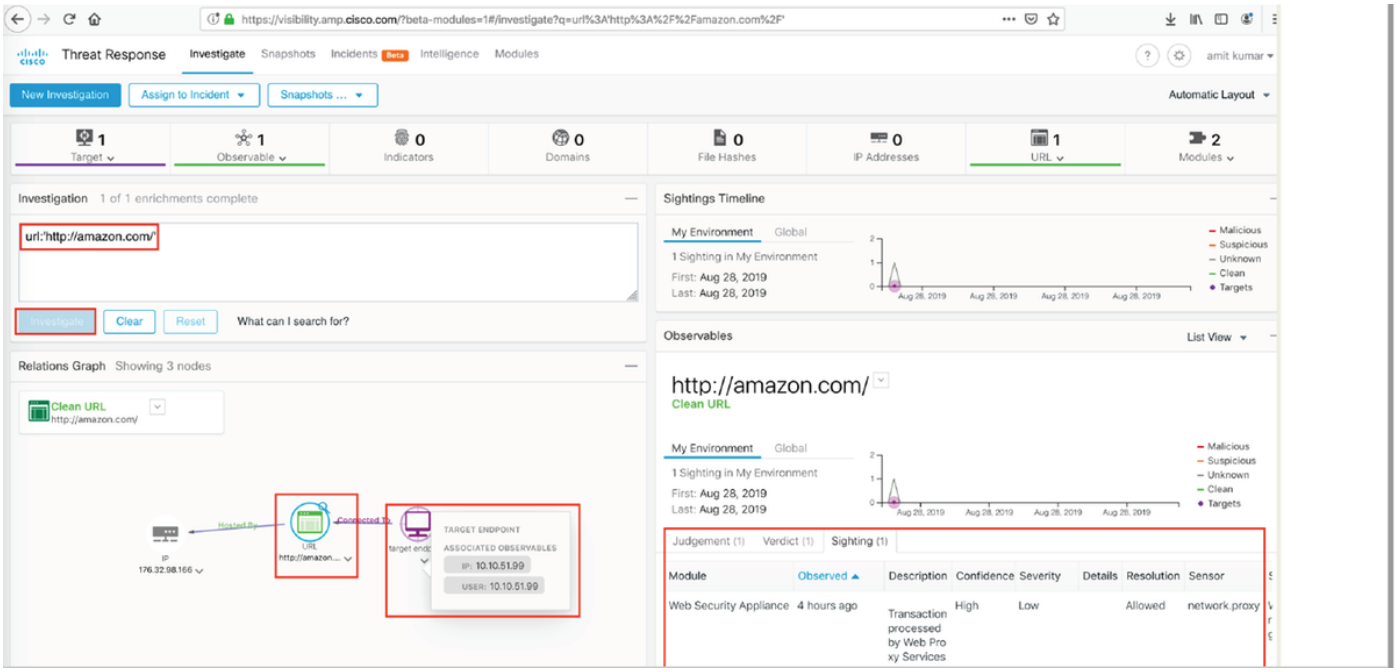
Verifiëren

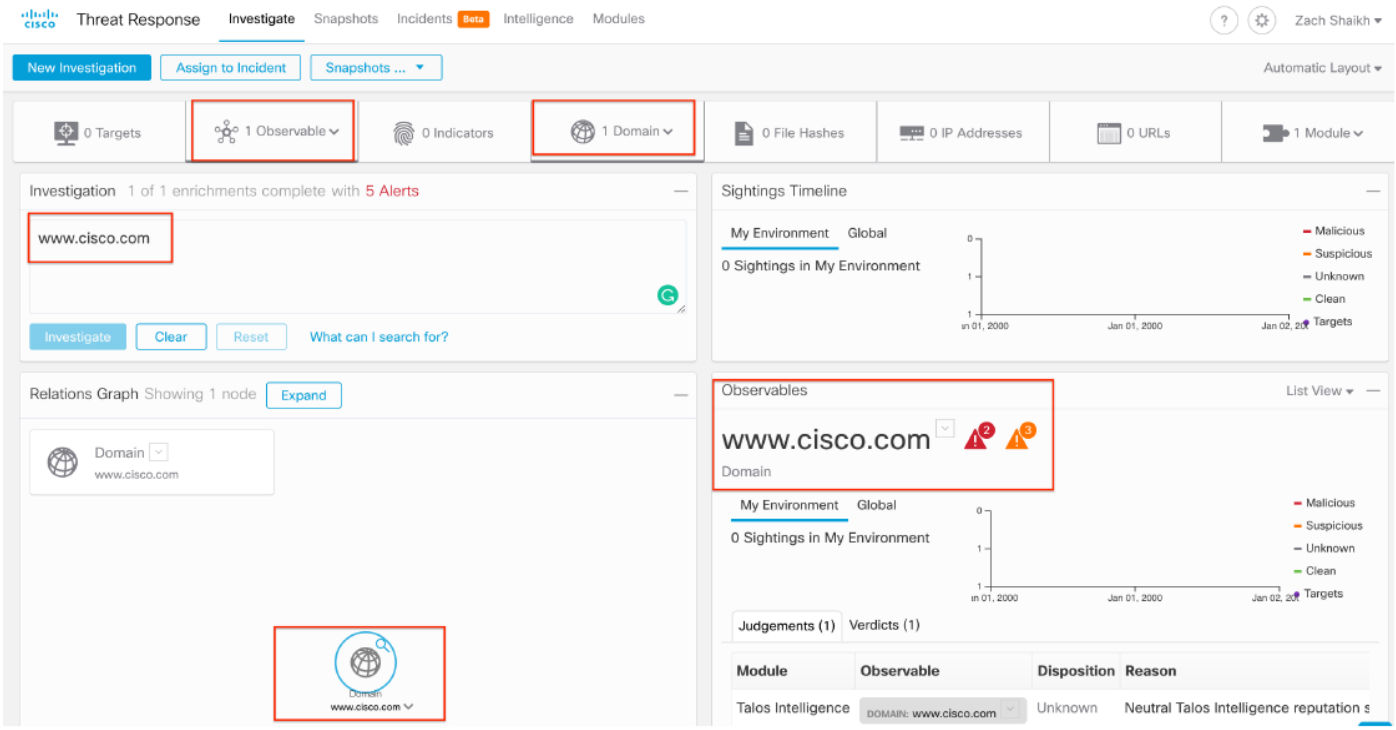
Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Vervangingen ("Querying the WSA logs") beschikbaar voor de WSA-module en hun ondersteunde indeling voor het uitvoeren van de query vanuit het CTR-portaal:

- Domain - domain:"com"
- URL - url:"http://www.neverssl.com"
- SHA256 - sha256:"8d3aa8badf6e5a38e1b6d59a254969b1e0274f8fa120254ba1f7e02991872379"
- IP - ip:"172.217.26.164"
- Bestandsnaam - file_name:"test.txt"

Aanpassingen in gebruik als voorbeeld:





Laat me weten of ik iets heb gemist dat moet worden toegevoegd. Laat me weten of ik iets heb gemist dat moet worden toegevoegd. Laat me weten of ik iets heb gemist dat moet worden toegevoegd. Laat me weten of ik iets heb gemist dat moet worden toegevoegd.