

WSA met CTR integreren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Registreer de applicatie](#)

[Verifiëren](#)

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

Choose 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

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

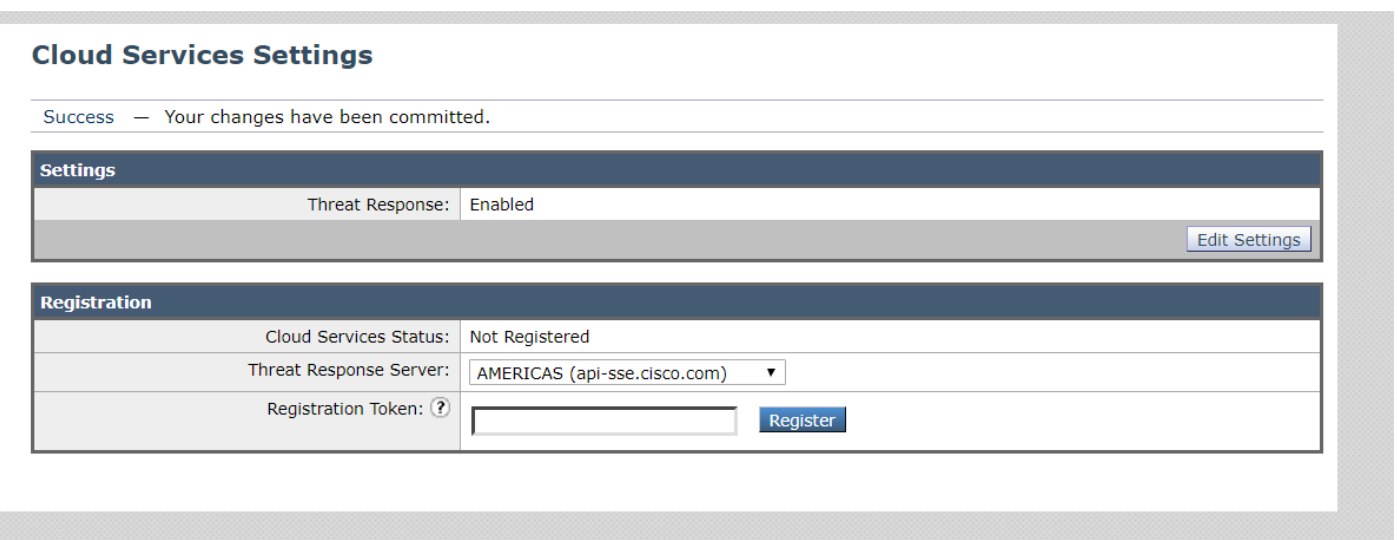
Choose the operation you want to perform:
COUNTERS - Limit counters recorded by the reporting system.
WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries.
AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
WEBEVENTBUCKETING - Enable or Disable web transaction 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.

Cloud Services Settings



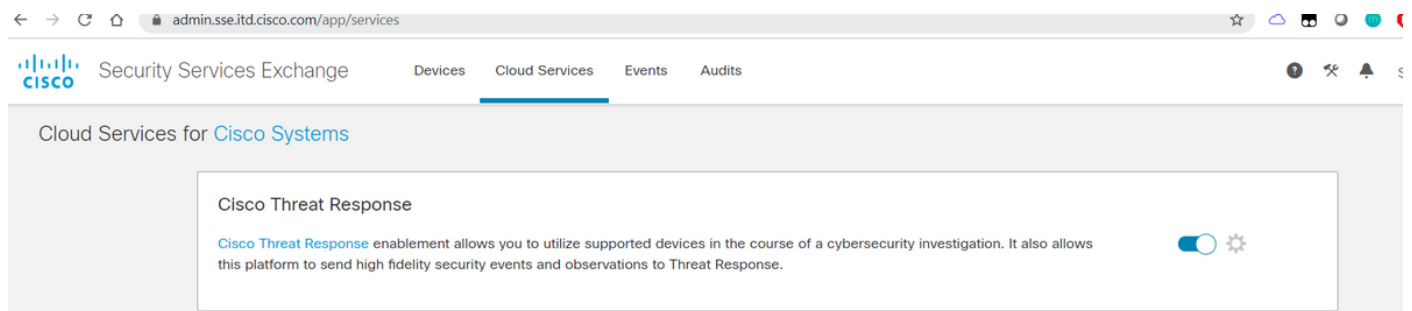
Kies de cloud op uw locatie, zoals in de afbeelding wordt weergegeven.



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:

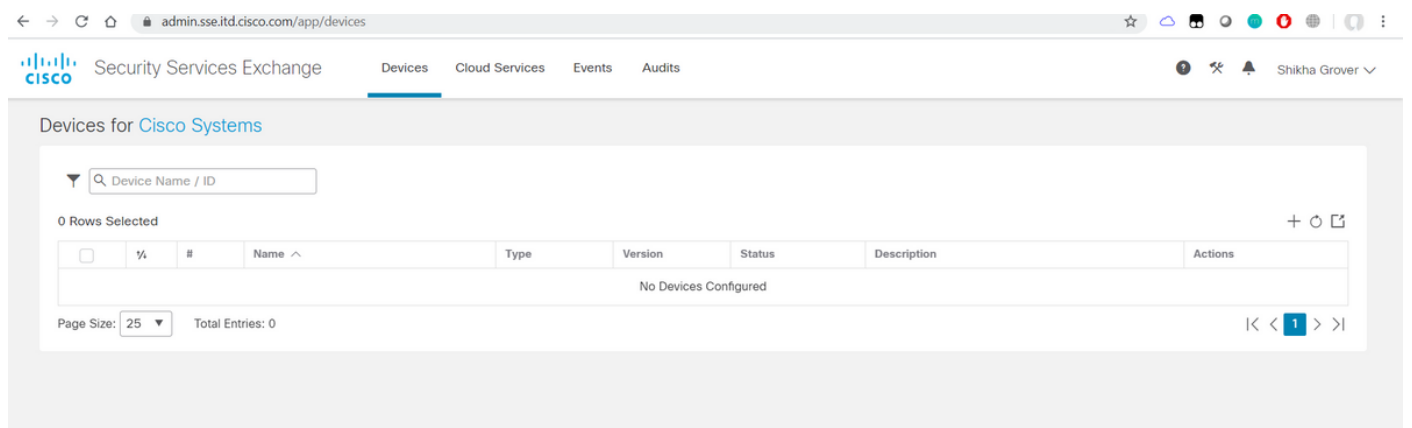
- api.eu.sse.itd.cisco.com (Europa)
- api-se.cisco.com (Amerika)

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.



Add Devices and Generate Tokens ✕

Number of devices

Up to 100

Token expiration time

[Cancel](#) [Continue](#)

Add Devices and Generate Tokens ✕

The following tokens have been generated and will be valid for 1 hour(s):

Tokens	
ef1324a199c106371542ee4d2d1bf1e7	

[Close](#) [Copy to Clipboard](#) [Save To File](#)

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

Cloud Services Settings

Success — Your changes have been committed.

Settings	
Threat Response:	Enabled Edit Settings

Registration	
Cloud Services Status:	Not Registered
Threat Response Server:	AMERICAS (api-sse.cisco.com) ▼
Registration Token: ?	<input style="width: 150px;" type="text" value="ef1324a199c106371542ee4d2d"/> Register

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.

Cloud Services Settings

Success — Your appliance is successfully registered with the Cisco Threat Response portal.

Settings

Threat Response: Enabled

Edit Settings

Registration

Cloud Services Status: Registered

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

Deregister Appliance: [Deregister](#)

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

admin.sse.itd.cisco.com/app/devices

Security Services Exchange

Devices Cloud Services Events Audits

Shikha Grover

Devices for Cisco Systems

Device Name / ID

0 Rows Selected

	%	#	Name ^	Type	Version	Status	Description	Actions
<input type="checkbox"/>	>	1	WSA-12-0-1-173.COM	WSA	12.0.1-173	Registered	S300V	/ 🗑️ 🔍

Page Size: 25 Total Entries: 1

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

visibility.amp.cisco.com/settings/devices

Threat Response Investigate Snapshots Incidents **Total** Intelligence Modules

Shikha Grover

Settings > Devices

Devices

Manage Devices Reload Devices

Name	Type	Version	Description	ID	IP Address
WSA-12-0-1-173.COM	WSA	12.0.1-173	S300V	3af01d56-a93e-4edc-926e-de1a4588409d	10.150.215.123

25 per page 1-1 of 1

Previous Next

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



Settings
Your Account
Devices
API Clients
▼ Modules
 Available Modules
Users

Add New Web Security Appliance Module

Module Name*

Registered Device*

Request Timeframe (days)

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:

Threat Response Investigate Snapshots Incidents **Beta** Intelligence Modules

New Investigation Assign to Incident Snapshots ... Automatic Layout

1 Target 1 Observable 0 Indicators 0 Domains 0 File Hashes 0 IP Addresses 1 URL 2 Modules

Investigation 1 of 1 enrichments complete

url: http://amazon.com/

Investigate Clear Reset What can I search for?

Relations Graph Showing 3 nodes

Clean URL http://amazon.com/

Hosted By URL http://amazon.com/ Connected To Target endpoint IP: 10.10.51.99 USER: 10.10.51.99

Sightings Timeline

My Environment Global 1 Sighting in My Environment First: Aug 28, 2019 Last: Aug 28, 2019

Observables

http://amazon.com/ Clean URL

My Environment Global 1 Sighting in My Environment First: Aug 28, 2019 Last: Aug 28, 2019

Judgement (1) Verdict (1) Sighting (1)

Module	Observed	Description	Confidence	Severity	Details	Resolution	Sensor
Web Security Appliance	4 hours ago	Transaction processed by Web Proxy Services	High	Low	Allowed	network proxy	

Threat Response Investigate Snapshots Incidents **Beta** Intelligence Modules

New Investigation Assign to Incident Snapshots ... Automatic Layout

0 Targets 1 Observable 0 Indicators 1 Domain 0 File Hashes 0 IP Addresses 0 URLs 1 Module

Investigation 1 of 1 enrichments complete with 5 Alerts

www.cisco.com

Investigate Clear Reset What can I search for?

Relations Graph Showing 1 node Expand

Domain www.cisco.com

Sightings Timeline

My Environment Global 0 Sightings in My Environment

Observables

www.cisco.com Domain

My Environment Global 0 Sightings in My Environment

Judgements (1) Verdicts (1)

Module	Observable	Disposition	Reason
Talos Intelligence	DOMAIN: www.cisco.com	Unknown	Neutral Talos Intelligence reputation s

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.