

Integreren en probleemoplossing met SecureX met web security applicatie (WSA)

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Vereiste URL's per regio voor SecureX](#)

[Bereid uw WSA voor op SSE-registratie](#)

[Uw apparaat in SecureX integreren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Registratie van apparaat bij CLI valideren](#)

[Video](#)

Inleiding

Dit document beschrijft de stappen die vereist zijn om de integratie van SecureX met Web Security Appliance (WSA) te integreren, te controleren en problemen op te lossen

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Web security applicatie (WSA)
- Optioneel virtualisatie van afbeeldingen

Gebruikte componenten

- Web security applicatie (WSA)
- Security Services Exchange (SE)
- SecureX-portal

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

Vereiste URL's per regio voor SecureX

Bevestig dat het WSA-apparaat bereikbaar is aan de URL's in poort 443:

Amerikaanse regio

- api-sse.cisco.com

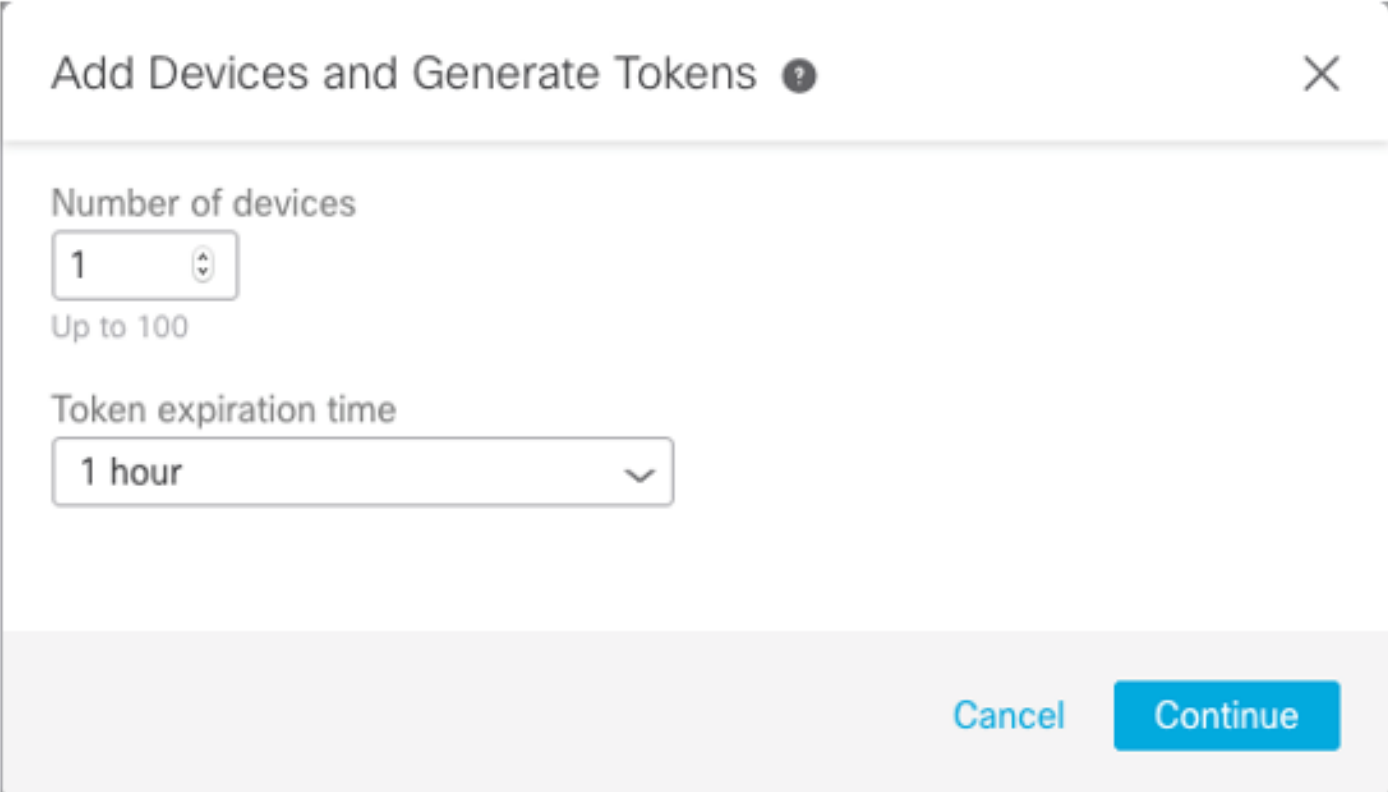
EU-regio

- api.eu.sse.itd.cisco.com

Opmerking: Als u toegang hebt tot SecureX met een URL voor Zuidoost-Azië, Japan en China (<https://visibility.apjc.amp.cisco.com/>), wordt de integratie met het apparaat momenteel niet ondersteund.

Bereid uw WSA voor op SSE-registratie

1.- Ga op het SSE Portal naar Apparaten en klik vervolgens op het pictogram (+) **Add Devices and Generate Tokens**, zoals in de afbeelding:



Add Devices and Generate Tokens ?

Number of devices

1

Up to 100


Token expiration time

1 hour

Cancel Continue

2. - Klik op doorgaan en het token voor het WSA wordt gegenereerd, zoals in de afbeelding.

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

Tokens	
[REDACTED]7120c58e1b4	

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

3.- **CTROBSERVABLE** inschakelen in de WSA-opdrachtregel-interface (CLI), onder **REPORTINGCONFIG** kunt u de optie selecteren om **CTROBSERVABLE** in te schakelen, zoals in de afbeelding wordt getoond:

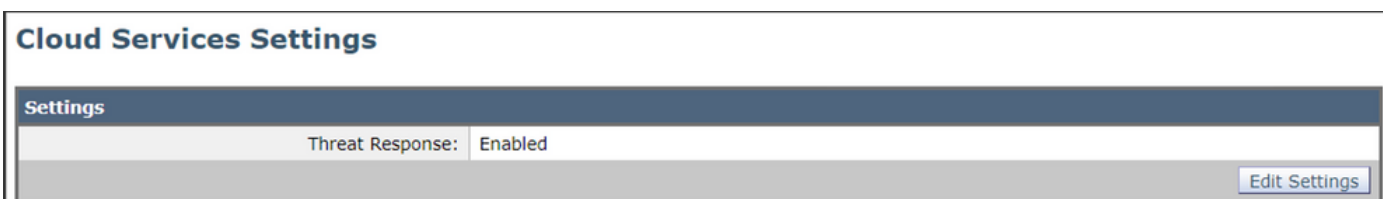
```
WSA-[REDACTED].COM> reportingconfig

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.
re 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.
```

4. - Schakel het wolvenportaal Security Service Exchange (SSE) in, navigeer naar **Network > Cloud Services-instellingen > Instellingen bewerken**, klik op **Enable** en **Submit**, zoals in het beeld wordt getoond:



5.- Selecteer de cloud waarop u wilt aansluiten:

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 type="text"/> Register

6.- Voer het token in dat u op SEE hebt gegenereerd (controleer of u het token hebt gebruikt voor de verlooptijd):

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 type="text"/> Register

7.- Zodra het token is geregistreerd, ziet u een bericht dat aangeeft dat het apparaat met succes is geregistreerd

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

8.- Daarna ziet u het apparaat dat op het SSE-portaal is geregistreerd:

Security Services Exchange Devices Cloud Services Events Audit Log Daniel Benitez

Devices for Sourcefire Support

WSA

0 Rows Selected

	W	#	Name	Type	Version	Status	Description	Actions
<input type="checkbox"/>	>	1	ift-wsa.mohsoni.lab	WSA	12.5.0-569	Registered	S300V	
<input type="checkbox"/>	∨	2	wsa02.mex-amp.lab	WSA	12.0.1-268	Registered	S100V	

ID: 3631b56-e9e5-4dba-888a-640868b6ae54 IP Address: 10.10.10.19 Connector Version:

Created: 2020-05-28 04:55:38 UTC

Uw apparaat in SecureX integreren

Stap 1. Om de WSA met SecureX te integreren, navigeer dan naar **Integraties**>**Nieuwe module toevoegen** en selecteer **Web security applicatie**, selecteer vervolgens uw apparaat, stel de **Time-out** bij **aanvraag** en klik op **Opslaan**, zoals in de afbeelding.

CISCO SecureX Dashboard Integrations Orchestration ^{Beta} Administration

Settings
Your Account
Devices
API Clients
∨ Integrations
Available Integrations
Users

Add New Web Security Appliance Module

Module Name*
Web Security Appliance

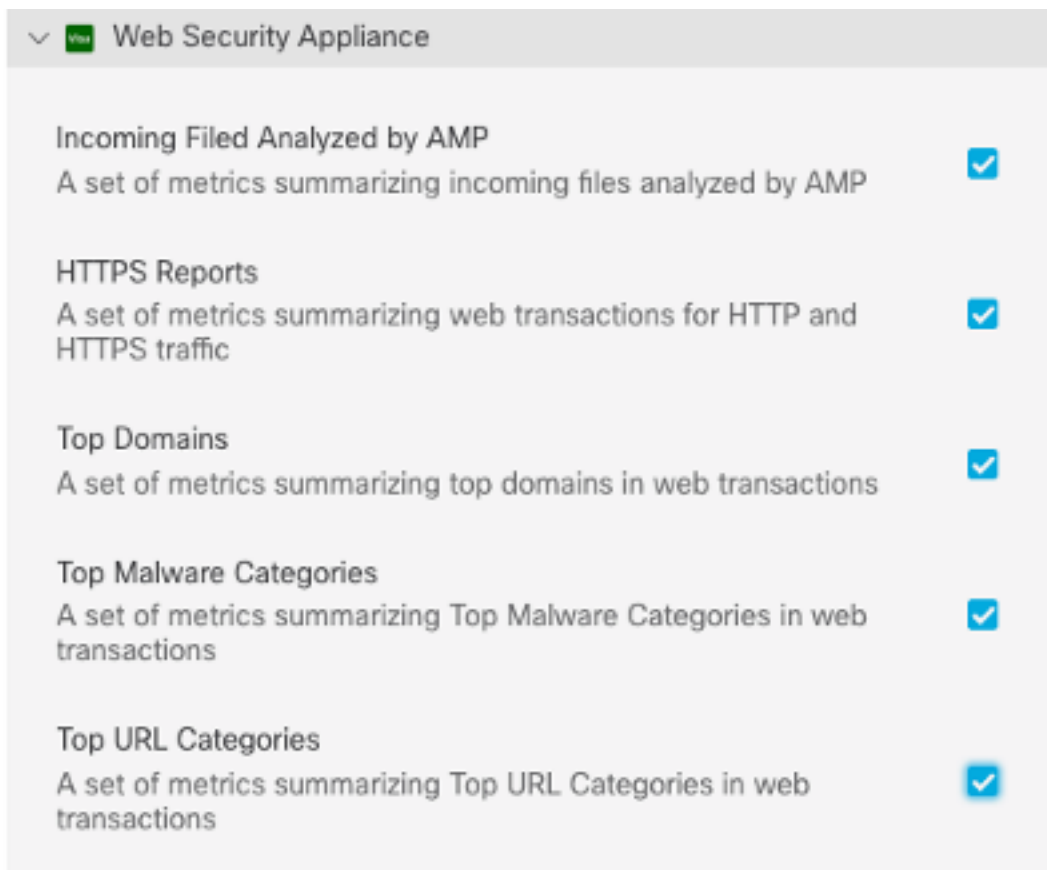
Registered Device*
wsa02.mex-amp.lab

wsa02.mex-amp.lab
Type WSA
ID ██████████8a-640868b6ae54
IP Address ████████0.19

Request Timeframe (days)
60

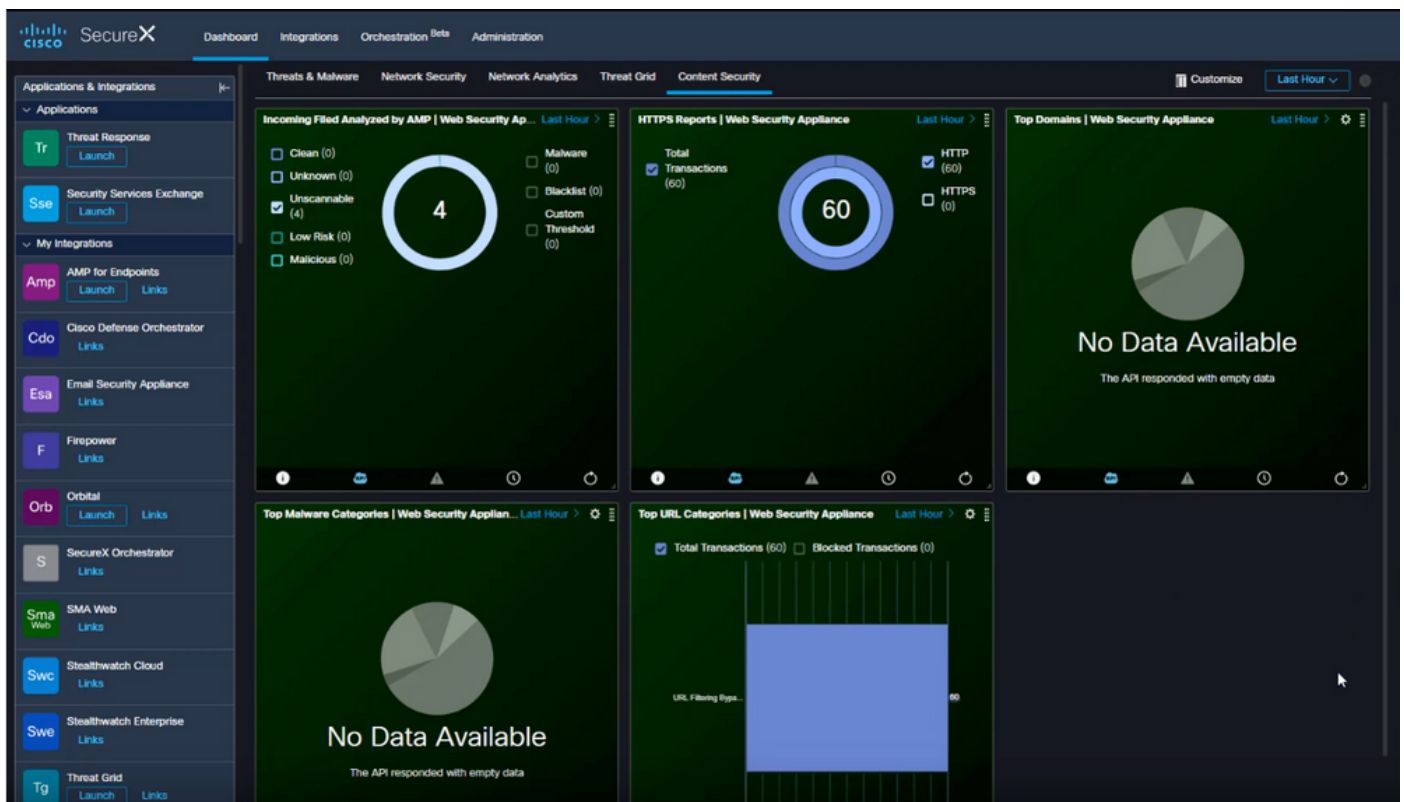
Save Cancel

Stap 2. Klik op het pictogram **+ New Dashboard** om uw Dashboard te maken en selecteer een naam en een berg die u voor het Dashboard wilt gebruiken.



Verifiëren

Nadat u de integratie hebt uitgevoerd kunt u de informatie over het Dashboard-formulier SSE zien ingevuld, kunt u op een van de gedetecteerde bedreigingen klikken en wordt het SSE-portal gestart met het filter voor Event Type op het portal.



Problemen oplossen

Registratie van apparaat bij CLI valideren

Stap 1. Start de opdracht Krullen op de achterkant om de verbindingstatus te controleren. Kijk naar het statusveld onder exchange van de krullenuitvoer samen met velden als FQDN (volledig gekwalificeerde domeinnaam), inschrijving. Het geregistreerde apparaat is in de ingeschreven staat:

```
/usr/local/bin/curl -XGET -v http://localhost:8823/v1/contexts/default
"exchange": [
  {
    "type": "registration",
    "status": "Enrolled",
    "name": "",
    "description": "Device has been enrolled."
  }
]
```

Stap 2. Vanuit deze uitvoer kunt u ook de vragen vanuit de connector controleren:

```
type": "administration",
  "statistics": {
    "transactionsProcessed": 20,
    "failedTransactions": 0,
    "lastFailedTransaction": "0001-01-01T00:00:00Z",
    "requestFetchFailures": 0,
    "responseUploadFailures": 0,
    "commandsProcessed": 20,
    "commandsFailed": 0,
    "lastFailedCommand": "0001-01-01T00:00:00Z"
  }
}
```

Stap 3. U kunt ook de hartslagen controleren die van de connector naar SSE zijn gemaakt (standaard 5 minuten):

```
refresh": {
  "registration": {
    "timestamp": "2010-06-29T03:51:45Z",
    "timeTaken": 1.387869786,
    "successCount": 6,
    "failureCount": 0
  }
}
```

Stap 4. Om de connector op WSA te kunnen controleren, moet u navigeren naar:

```
/data/pub/sse_connectord_logs/sse_connectord_log.current
```

De informatie die te vinden is in **sse_connectord_log.huidige**

- Registratietransactie met SSE
- Logs van een Verrijkingdienst
- Logs voor deregulering met het SSE Portal

Video

U vindt de informatie in dit document in deze video