

Integration und Fehlerbehebung von SecureX mit der Web Security Appliance (WSA)

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Erforderliche URLs pro Region für SecureX](#)

[Vorbereitung der WSA auf die SSE-Registrierung](#)

[Integrieren Sie Ihr Gerät in SecureX](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Validieren der Geräteregistrierung über die CLI](#)

[Video](#)

Einführung

Dieses Dokument beschreibt die erforderlichen Schritte zur Integration, Verifizierung und Fehlerbehebung von SecureX in die Web Security Appliance (WSA).

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Web Security Appliance (WSA)
- Optionale Virtualisierung von Bildern

Verwendete Komponenten

- Web Security Appliance (WSA)
- Security Services Exchange (SSE)
- SecureX-Portal

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Erforderliche URLs pro Region für SecureX

Überprüfen Sie, ob die WSA-Appliance über die Erreichbarkeit der URLs auf Port 443 verfügt:

Region USA

- api-sse.cisco.com

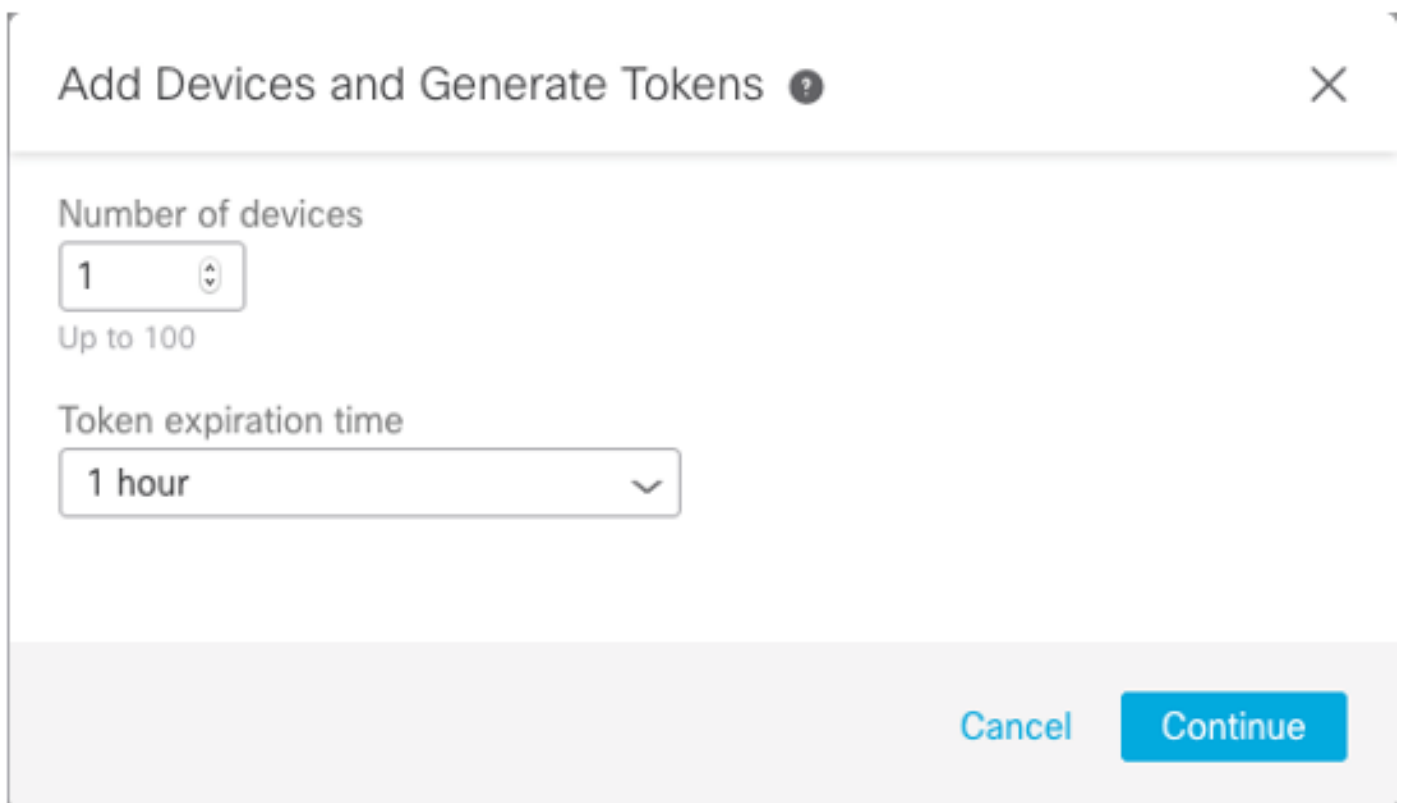
Region EU

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

Hinweis: Beim Zugriff auf SecureX mit einer URL für den Asien-Pazifik-Raum, Japan und China (<https://visibility.apjc.amp.cisco.com/>) wird die Integration mit der Appliance derzeit nicht unterstützt.

Vorbereitung der WSA auf die SSE-Registrierung

1.- Navigieren Sie im SSE-Portal zu "Geräte", und klicken Sie dann auf das Symbol **Add Devices** (Geräte hinzufügen) und **Generate Tokens** (Token generieren), wie im Bild gezeigt:



Add Devices and Generate Tokens ?

Number of devices

1

Up to 100

Token expiration time

1 hour



Cancel Continue

2.- Klicken Sie auf "Weiter", und das Token für die WSA wird generiert, wie im Bild gezeigt.

Add Devices and Generate Tokens ?



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


Tokens	
 7120c58e1b4	

Close

Copy to Clipboard

Save To File

3.- Aktivieren Sie **CTROBSERVABLE** in der WSA-Befehlszeilenschnittstelle (CLI). Unter **REPORTINGCONFIG** finden Sie die Option zum Aktivieren von **CTROBSERVABLE**, wie im Bild gezeigt:

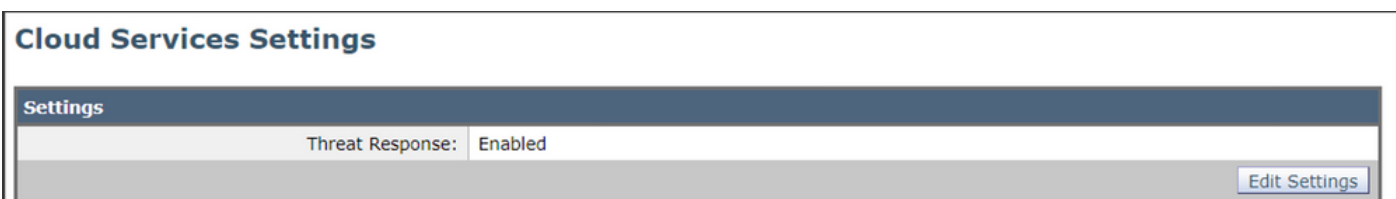
```
WSA-.COM> reportingconfig

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.
]> ctobservable

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.- Aktivieren Sie das Cloud-Portal von Security Service Exchange (SSE), navigieren Sie zu **Netzwerk > Cloud Services Settings > Edit settings**, klicken Sie auf **Aktivieren** und **Senden**, wie im Bild gezeigt:



5.- Wählen Sie die Cloud aus, mit der Sie eine Verbindung herstellen möchten:

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: ?

[Register](#)

6.- Geben Sie den bei SEE generierten Token ein (stellen Sie sicher, dass Sie das Token vor Ablauf der Gültigkeit verwenden):

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: ?

[Register](#)

7.- Sobald das Token registriert ist, wird eine Meldung angezeigt, die anzeigt, dass das Gerät erfolgreich registriert wurde.

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.- Danach wird das Gerät im SSE-Portal registriert:

Security Services Exchange Devices Cloud Services Events Audit Log Daniel Benitez

Devices for Sourcefire Support

WSA

0 Rows Selected

<input type="checkbox"/>	%	#	Name ^	Type	Version	Status	Description	Actions
<input type="checkbox"/>	>	1	lft-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: 363f1b56-e9e5-4dba-888a-640868b6ae54 IP Address: 10.10.10.19 Connector Version:

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

Integrieren Sie Ihr Gerät in SecureX

Schritt 1: Um die WSA mit SecureX zu integrieren, navigieren Sie zu **Integrations>Add New module** und wählen Sie **Web Security Appliance** aus, wählen Sie dann Ihr Gerät aus, richten Sie den **Zeitraumen für Anfragen ein** und klicken Sie auf **Save** (Speichern), wie im Bild gezeigt.

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

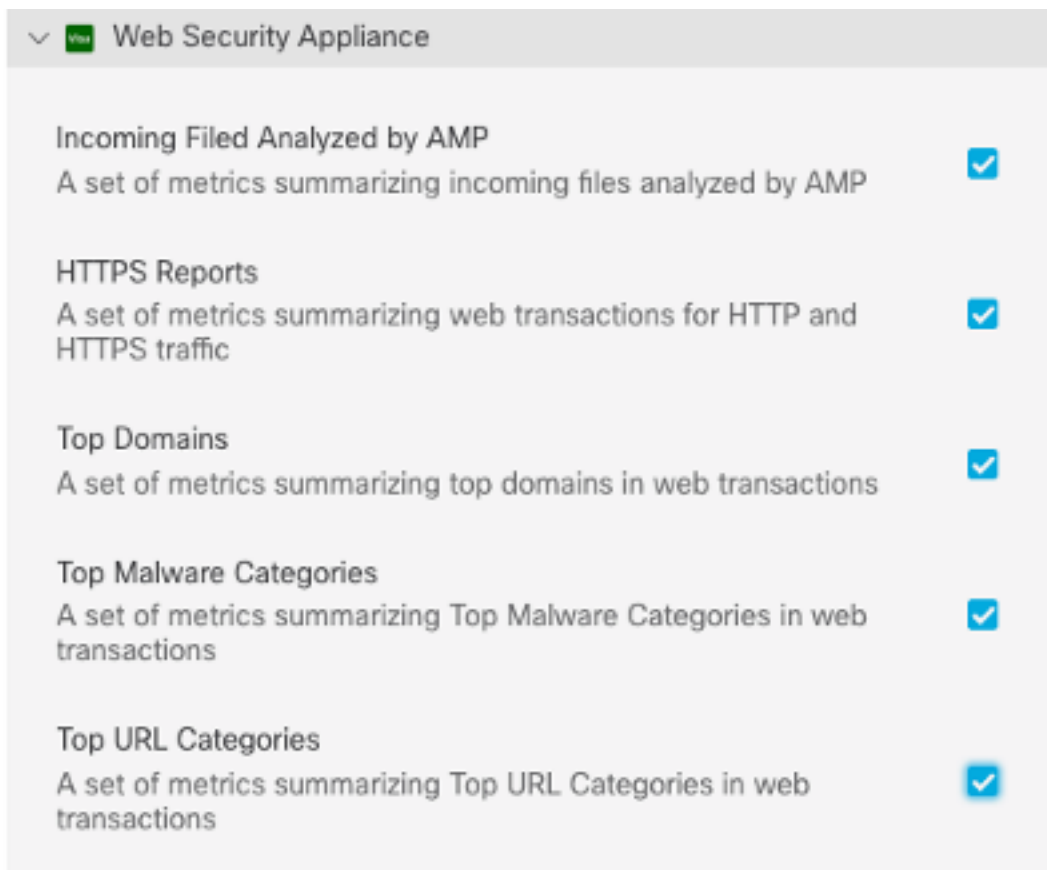
Registered Device*
wsa02.mex-amp.lab

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

Request Timeframe (days)
60

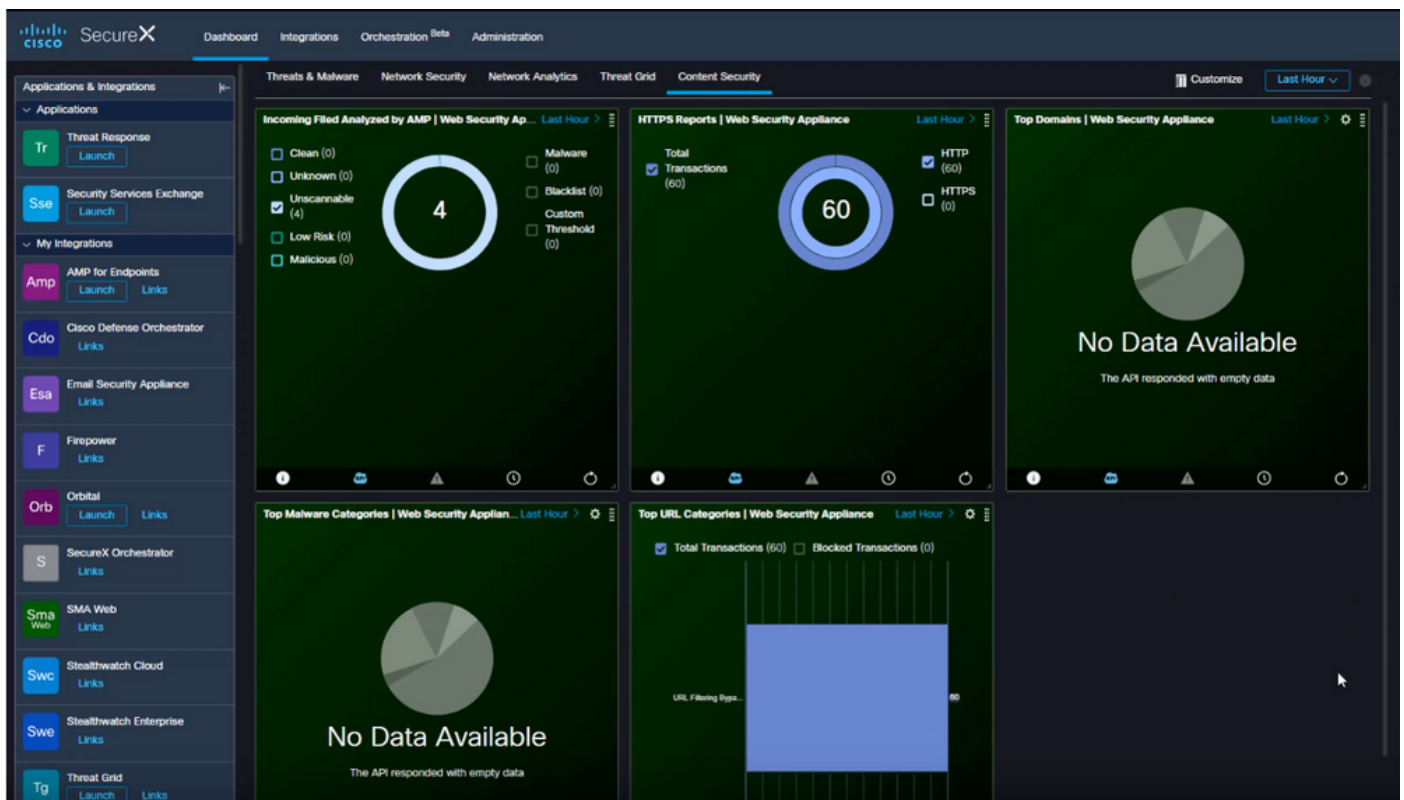
Save Cancel

Schritt 2: Klicken Sie zum Erstellen des Dashboards auf das Symbol **+ New Dashboard**, und wählen Sie einen Namen und eine Kachel aus, die Sie für das Dashboard verwenden möchten.



Überprüfen

Nachdem Sie die Integration durchgeführt haben, sehen Sie die von SSE ausgefüllten Dashboard-Informationen. Sie können auf eine der erkannten Bedrohungen klicken und das SSE-Portal wird mit dem Ereignistypfilter gestartet.



Fehlerbehebung

Validieren der Geräteregistrierung über die CLI

Schritt 1: Führen Sie den Befehl curl im Backend aus, um den Verbindungsstatus zu überprüfen. Suchen Sie neben Feldern wie FQDN (Vollqualifizierter Domänenname) und der Registrierung das Statusfeld, das an der Curl-Ausgabe ausgetauscht wird. Das registrierte Gerät ist eingeschrieben:

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

Schritt 2: In dieser Ausgabe können Sie auch die Abfragen aus dem Anschluss überprüfen:

```
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"
  }
}
```

Schritt 3: Sie können auch die Heartbeats vom Anschluss an SSE überprüfen (standardmäßig 5 Minuten):

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

Schritt 4: Um die Connector-Protokolle bei der WSA zu überprüfen, müssen Sie zu Folgendes navigieren:

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

Die Informationen, die in der Datei `sse_connected_log.current` zu finden sind

- Registrierungstransaktion mit SSE
- Protokolle für eine Bereichsabfrage
- Protokolle für die Deregistrierung beim SSE-Portal

Video

Die Informationen in diesem Dokument finden Sie in diesem Video