

# Integrate and Troubleshoot SecureX with Web Security Appliance (WSA)

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Configure](#)

[Required URLs per Region for SecureX](#)

[Prepare your WSA for SSE registration](#)

[Integrate your device to SecureX](#)

### [Verify](#)

### [Troubleshoot](#)

[Validate device enrollment from CLI](#)

### [Video](#)

---

## Introduction

This document describes the steps required to integrate, verify, and troubleshoot the integration of SecureX with Web Security Appliance (WSA)

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Web Security Appliance (WSA)
- Optional Virtualization of images

### Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Configure

### Required URLs per Region for SecureX

Validate the WSA appliance has reachability to the URLs on port 443:


US Region

- api-sse.cisco.com

EU Region

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

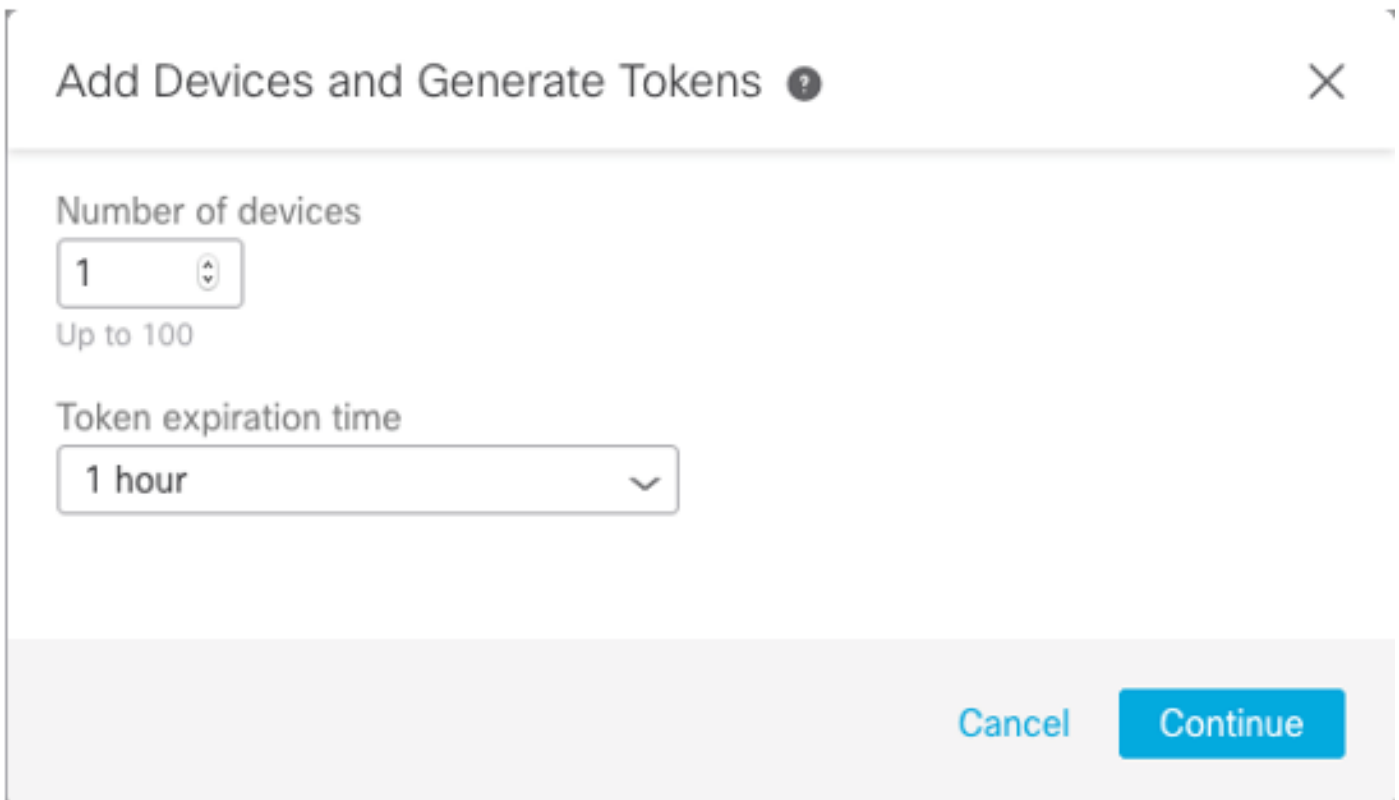
---

 **Note:** If access to SecureX with an Asia Pacific, Japan, and China URL (<https://visibility.apjc.amp.cisco.com/>), the integration with the appliance is not currently supported.

---

## Prepare your WSA for SSE registration

1.- On the SSE Portal, navigate to Devices and then click on the (+) **Add Devices and Generate Tokens** icon, as shown in the image:



Add Devices and Generate Tokens ? X

Number of devices

1

Up to 100

Token expiration time

1 hour

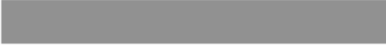

Cancel Continue

2.- Click continue and the token for the WSA is generated, as shown in the image.

## 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.- Enable **CTROBSERVABLE** in the WSA command-line interface (CLI), under **REPORTINGCONFIG** you can find the option to enable **CTROBSERVABLE**, as shown in the image:

```
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.
]> ctrobservable

TR 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.- Enable the Security Service Exchange (SSE) cloud portal, Navigate to **Network > Cloud Services Settings > Edit settings**, click **Enable** and **Submit**, as shown in the image:

### Cloud Services Settings

Settings	
Threat Response:	Enabled

[Edit Settings](#)

5.- Select the cloud you want to connect to:

## 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.- Enter the token you generated on SEE (ensure you use the token before the expiration time):

## 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.- Once the token is registered, you see a message that indicates the device is successfully registered

## 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.- After this, you see the device registered on SSE portal:

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	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: 363f1b56-e9e5-4dba-888a-640868b6ae54    IP Address: 10.10.10.19    Connector Version:

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

## Integrate your device to SecureX

Step 1. To integrate the WSA with SecureX, navigate to **Integrations>Add New module** and select **Web Security Appliance**, then select your device, set up the **Request Timeframe**, and click **Save**, as shown in the image.

CISCO SecureX    Dashboard    Integrations    Orchestration <sup>Beta</sup>    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

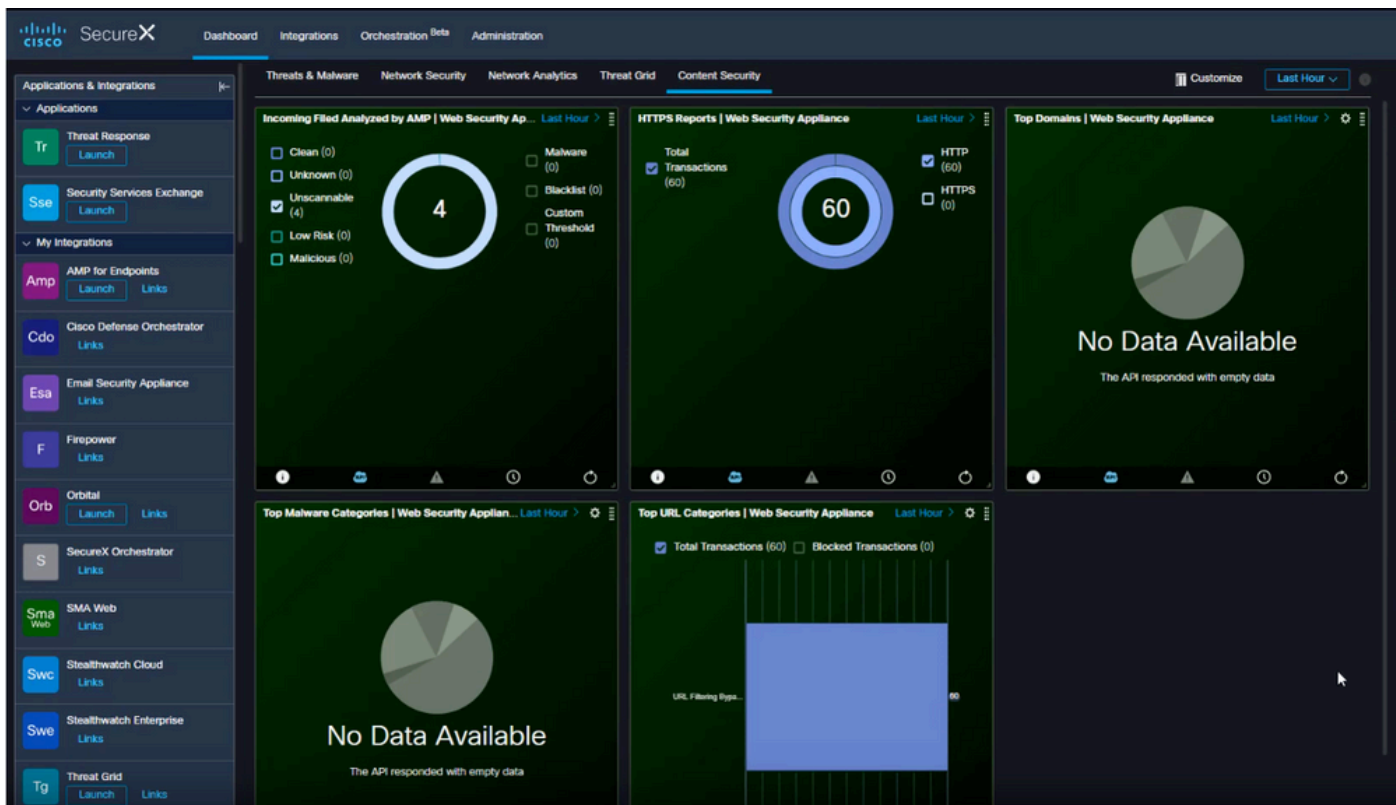
Save    Cancel

Step 2. To create your Dashboard, click the + **New Dashboard** icon, select a name and Tile that you want to use for the Dashboard.

Web Security Appliance	
<b>Incoming Files Analyzed by AMP</b> A set of metrics summarizing incoming files analyzed by AMP	<input checked="" type="checkbox"/>
<b>HTTPS Reports</b> A set of metrics summarizing web transactions for HTTP and HTTPS traffic	<input checked="" type="checkbox"/>
<b>Top Domains</b> A set of metrics summarizing top domains in web transactions	<input checked="" type="checkbox"/>
<b>Top Malware Categories</b> A set of metrics summarizing Top Malware Categories in web transactions	<input checked="" type="checkbox"/>
<b>Top URL Categories</b> A set of metrics summarizing Top URL Categories in web transactions	<input checked="" type="checkbox"/>

## Verify

After you perform the integration you can see the Dashboard information populated from SSE, you can click on any of the Threats detected and the SSE portal is launched with the Event Type filter on it.



## Troubleshoot

### Validate device enrollment from CLI

Step 1. Run the curl command in the backend to check the connection status. Look for the status field under exchange from the curl output along with fields like FQDN(Fully qualified domain name), enrolment. The registered device is in the enrolled state:

```
<#root>
```

```
/usr/local/bin/curl -XGET -v
```

```
http://localhost:8823/v1/contexts/default
```

```
"exchange": [
  {
    "type": "registration",
    "status": "Enrolled"
  },
  {
    "name": "",
    "description": "Device has been enrolled."
  }
]
```

Step 2. From this output you can also check the queries made from the connector:

```
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"
```

Step 3. You can also check the heartbeats made from the connector to SSE (5 minutes by default):

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

Step 4. In order to check the Connector logs on WSA, you need to navigate to:

<#root>

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

The information that can be found in the **sse\_connectord\_log.current**

- Registration transaction with SSE
- Logs fro an Enrichment Query
- Logs for deregistration with the SSE Portal

## Video

You can find the information contained in this document in this video



