

將SecureX與網路安全裝置(WSA)整合並進行故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[SecureX的每個區域所需的URL](#)

[為SSE註冊準備WSA](#)

[將裝置整合到SecureX](#)

[驗證](#)

[疑難排解](#)

[從CLI驗證裝置註冊](#)

[影片](#)

簡介

本文檔介紹將SecureX與網路安全裝置(WSA)整合進行整合、驗證和故障排除所需的步驟

必要條件

需求

思科建議您瞭解以下主題：

- 網路安全裝置(WSA)
- 映像的可選虛擬化

採用元件

- 網路安全裝置(WSA)
- 安全服務交換(SSE)
- SecureX門戶

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

SecureX的每個區域所需的URL

驗證WSA裝置是否可訪問埠443上的URL:

美國地區

- api-sse.cisco.com

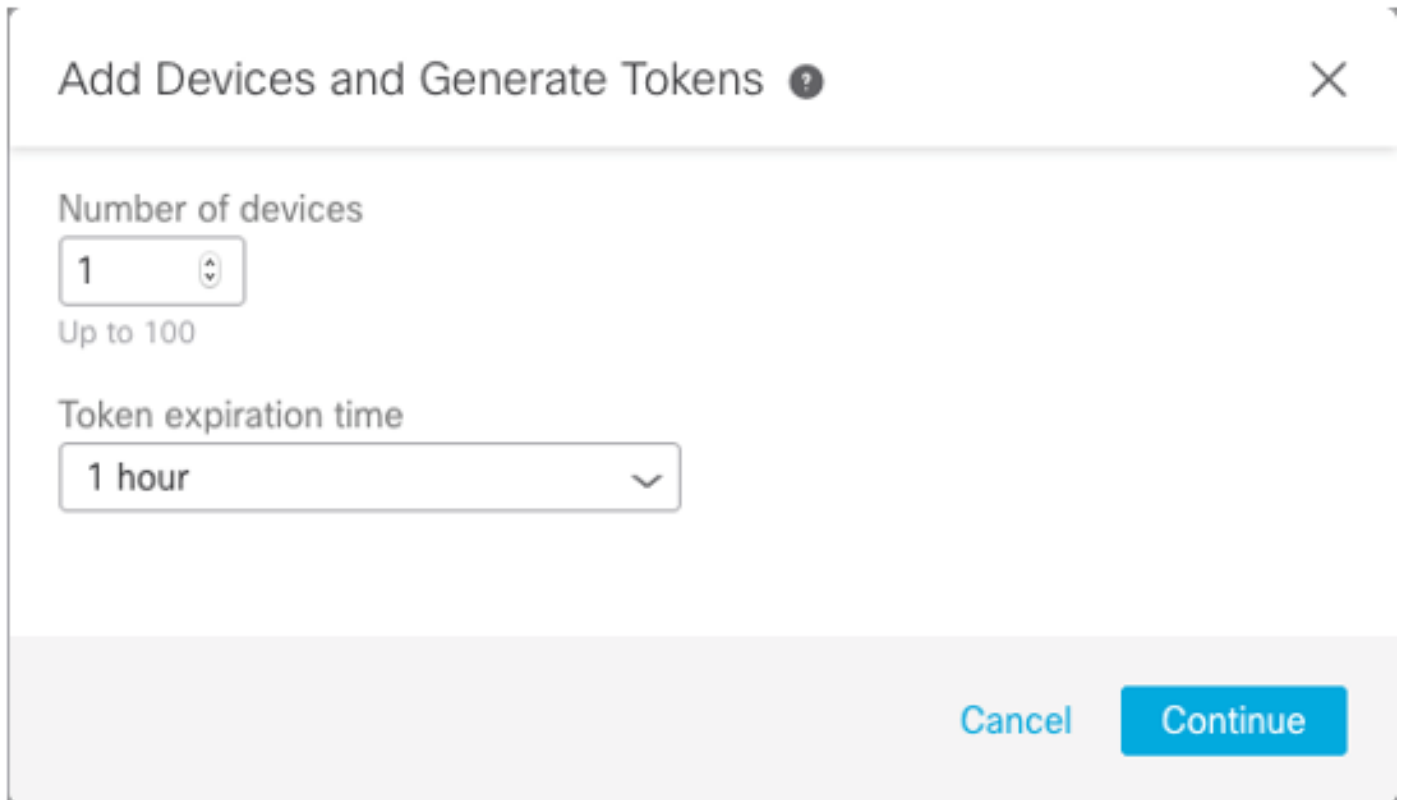
歐盟地區

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

附註：如果使用亞太地區、日本和中國URL(<https://visibility.apjc.amp.cisco.com/>)訪問SecureX，則當前不支援與裝置的整合。

為SSE註冊準備WSA

1. — 在SSE門戶上，導航至Devices，然後點選(+)Add Devices and Generate Token圖示，如下圖所示：



Add Devices and Generate Tokens ?

Number of devices

1

Up to 100

Token expiration time

1 hour


Cancel Continue

2. — 按一下「繼續」，生成WSA令牌，如下圖所示。

Add Devices and Generate Tokens ?



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. — 在WSA命令列介面(CLI)中啟用CTROBSERVABLE，在REPORTINGCONFIG下，可以找到啟用CTROBSERVABLE的選項，如下圖所示：

```
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

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. — 啟用安全服務交換(SSE)雲門戶，導航到網路>雲服務設定>編輯設定，按一下啟用和提交，如下圖所示：

Cloud Services Settings

Settings	
Threat Response:	Enabled

[Edit Settings](#)

5. — 選擇要連線的雲：

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. — 輸入在SEE上生成的令牌 (確保在到期時間之前使用令牌) :

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. — 註冊令牌後，您會看到一條消息，指示裝置已成功註冊

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. — 之後，您會看到在SSE門戶上註冊的裝置：

Security Services Exchange Devices Cloud Services Events Audit Log Daniel Benitez

Devices for Sourcefire Support

WSA

0 Rows Selected

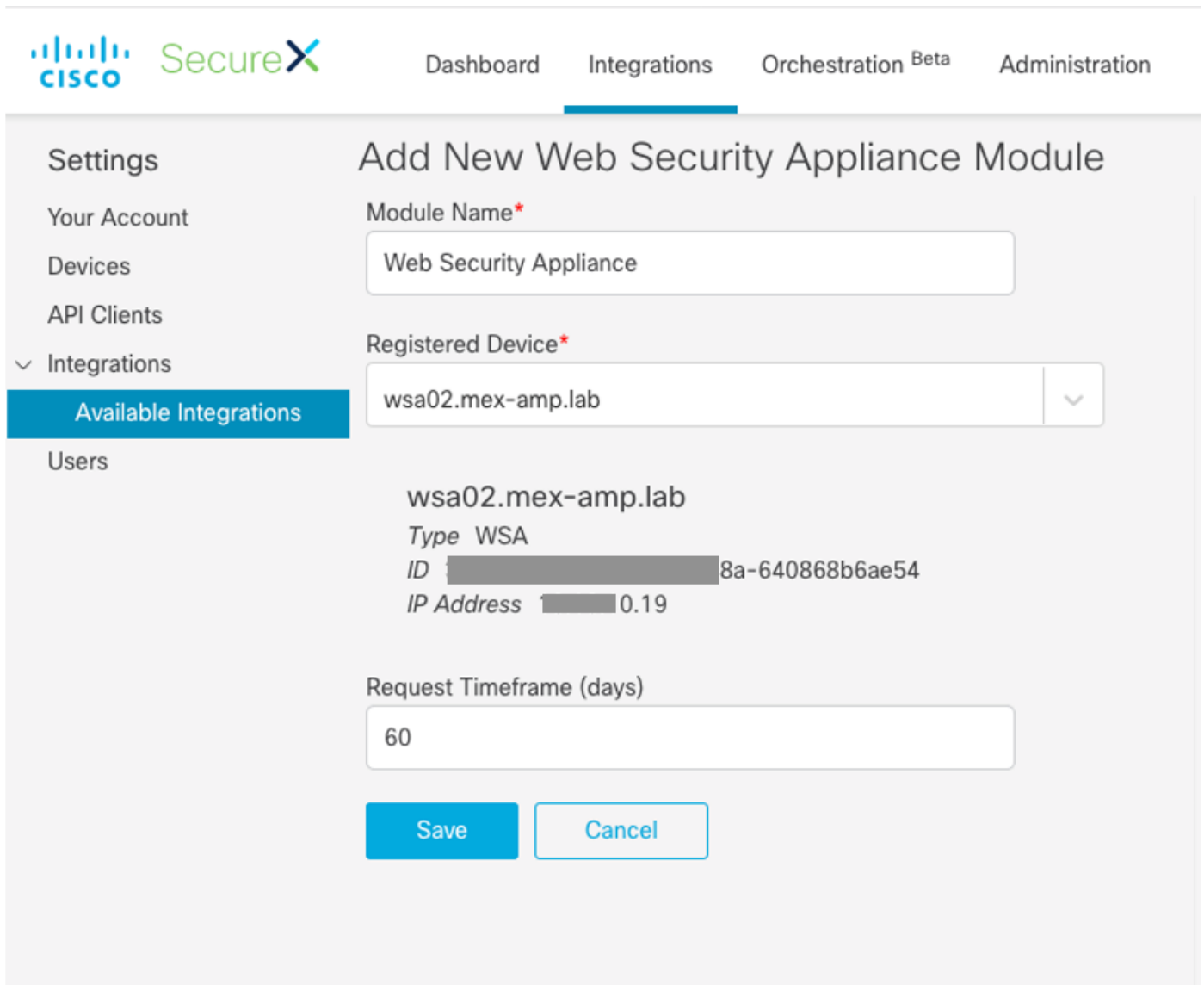
	%	#	Name ^	Type	Version	Status	Description	Actions
<input type="checkbox"/>	>	1	lft-wsa.mohsoni.lab	WSA	12.5.0-569	Registered	S300V	/ 🗑️ 📄
<input type="checkbox"/>	∨	2	wsa02.mex-amp.lab	WSA	12.0.1-268	Registered	S100V	/ 🗑️ 📄

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

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

將裝置整合到SecureX

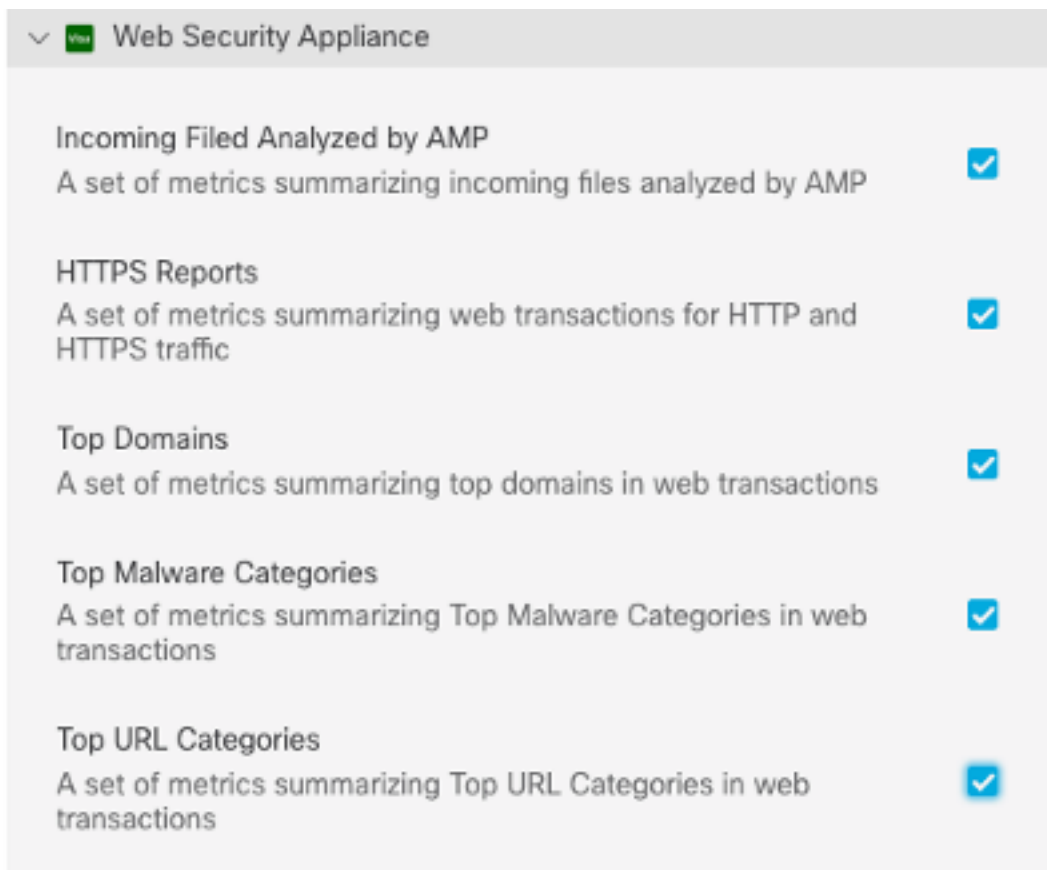
步驟1。若要將WSA與SecureX整合，請導覽至Integrations>Add New module，然後選擇Web Security Appliance，然後選擇您的裝置，設定Request Timeframe，然後按一下Save，如下圖所示。



The screenshot shows the Cisco SecureX interface for adding a new Web Security Appliance (WSA) module. The page title is "Add New Web Security Appliance Module". On the left, there is a navigation menu with "Integrations" expanded and "Available Integrations" selected. The main content area contains the following fields and information:

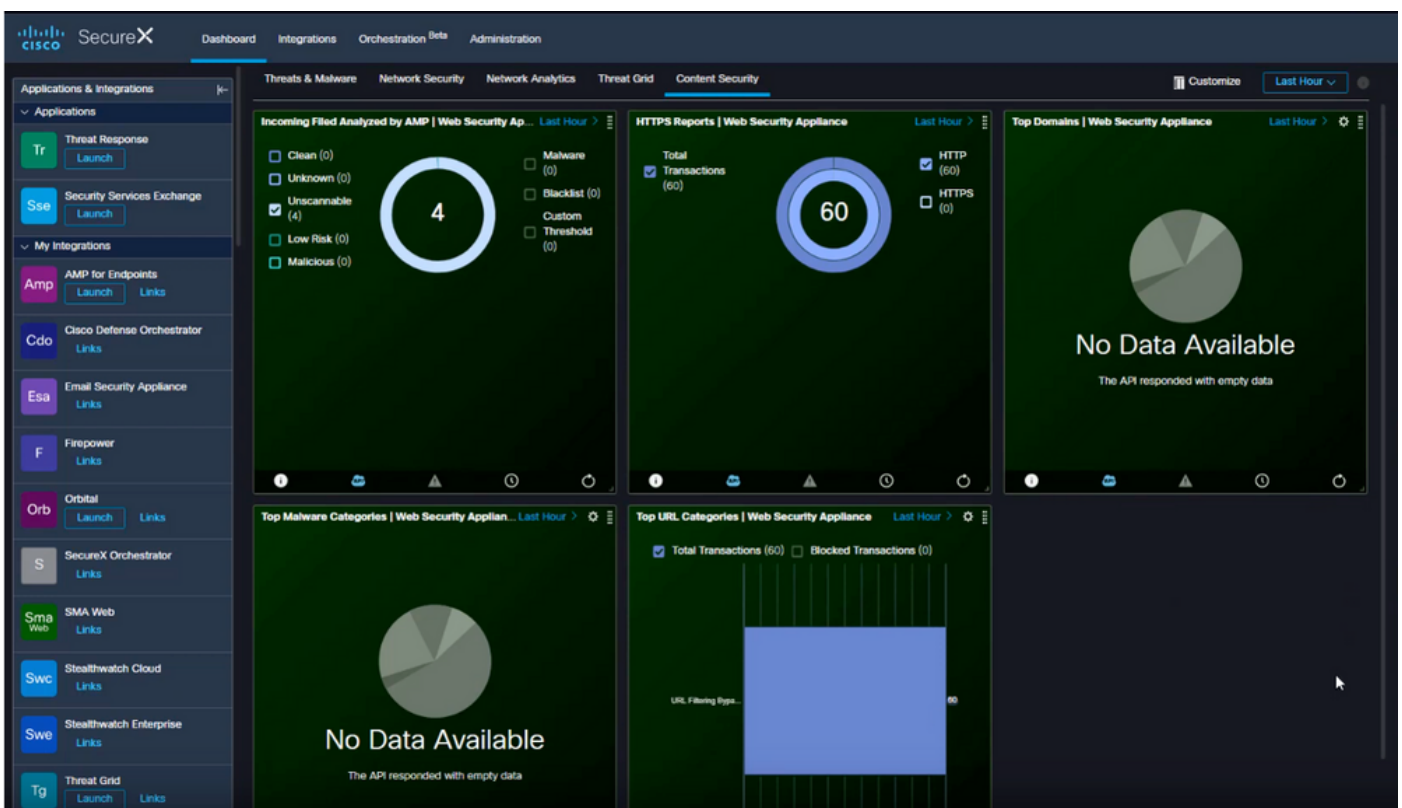
- Module Name***: A text input field containing "Web Security Appliance".
- Registered Device***: A dropdown menu showing "wsa02.mex-amp.lab".
- Device Details**:
 - wsa02.mex-amp.lab
 - Type: WSA
 - ID: [Redacted] 8a-640868b6ae54
 - IP Address: [Redacted] 0.19
- Request Timeframe (days)**: A text input field containing "60".
- At the bottom, there are two buttons: "Save" (highlighted in blue) and "Cancel".

步驟2.要建立儀表板，請按一下+ New Dashboard圖示，選擇要用於儀表板的名稱和磁貼。



驗證

執行整合後，您可以看到從SSE填充的儀表板資訊，可以按一下任何檢測到的威脅，然後使用事件型別過濾器啟動SSE門戶。



疑難排解

從CLI驗證裝置註冊

步驟1.在後端運行curl命令檢查連線狀態。從curl輸出中查詢exchange下的狀態欄位以及FQDN(完全限定域名)和註冊等欄位。註冊的裝置處於註冊狀態：

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

步驟2.在此輸出中，您還可以檢查聯結器所執行的查詢：

```
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"
```

步驟3.您還可以檢查從聯結器到SSE的檢測訊號（預設情況下為5分鐘）：

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

步驟4.為了檢查WSA上的聯結器日誌，您需要導航到：

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

可以在sse_connector_log.current中找到的資訊

- 與上交所的註冊交易
- 富集查詢的日誌
- SSE門戶註銷日誌

影片

您可以在此影片中找到本文檔中包含的資訊