將WSA與CTR整合

目錄

簡介

本檔案介紹將網路安全裝置(WSA)與思科威脅回應(CTR)入口網站整合的步驟。

作者：Shikha Grover，編輯者：Yeraldin Sanchez，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- WSA訪問
- CTR門戶訪問
- 思科資安帳戶

採用元件

本文中的資訊係根據以下軟體和硬體版本：

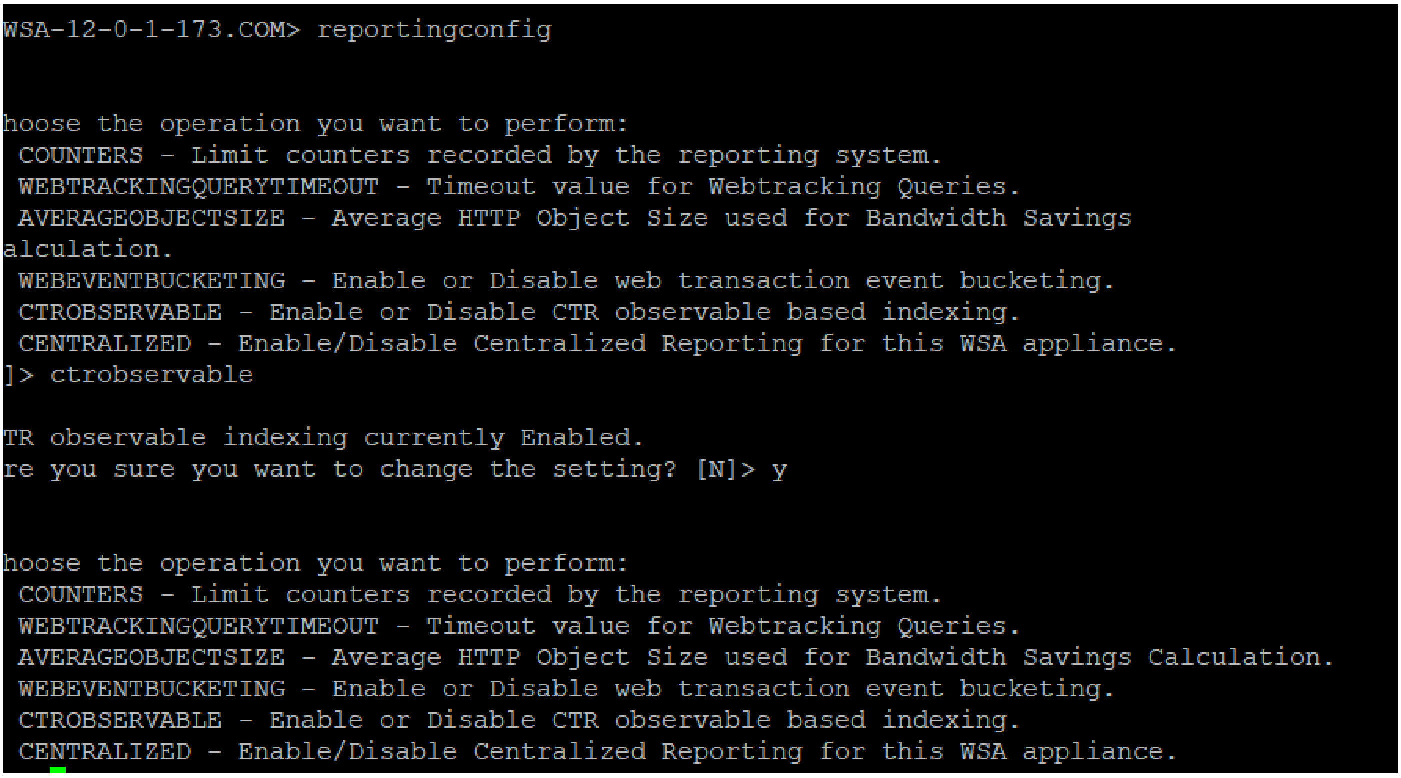
- 非同步作業系統版本12.x或更高版本

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

> **注意**：如果您使用亞太地區的亞太、日本和中國的URL(https://visibility.apjc.amp.cisco.com/)訪問CTR，則當前不支援與您的裝置整合。

步驟1.在CLI中REPORTINGCONFIG下啟用**CTROBSERVABLE，然後提交更改，如下圖所示。**



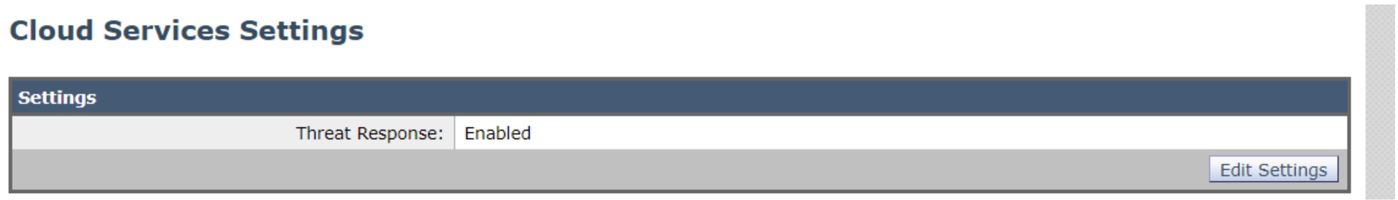
```
WSA-12-0-1-173.COM> reportingconfig


hoose 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


hoose 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.
```

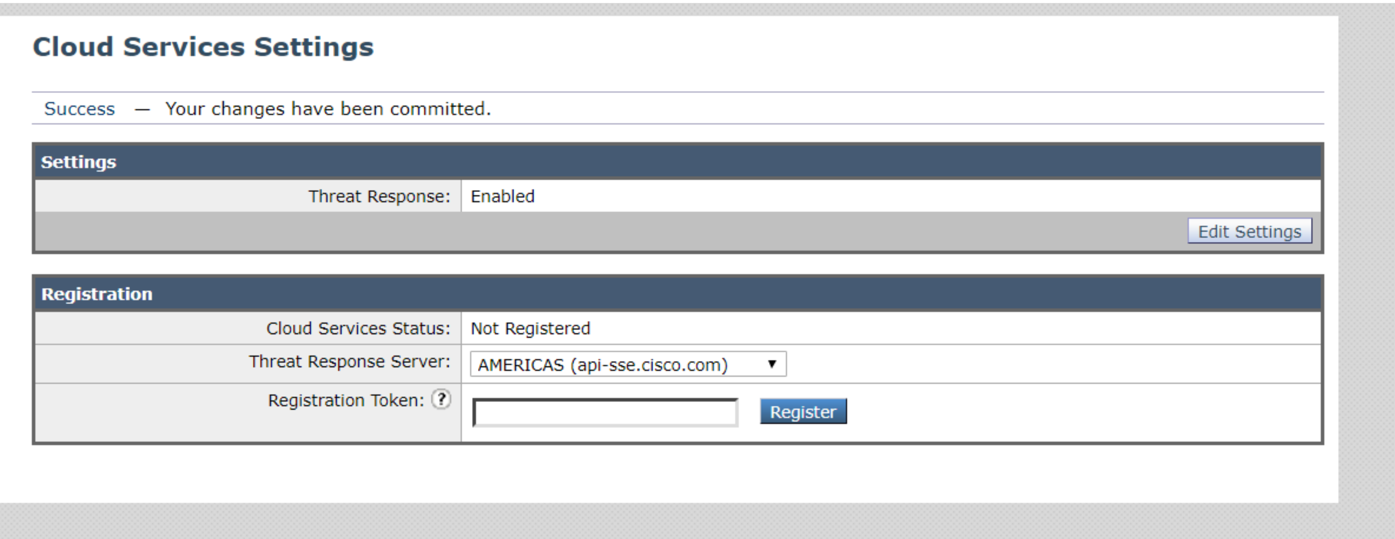
步驟2.設定安全服務交換(SSE)雲端入口網站，導覽至**Network >Cloud Services Settings > Edit settings**，按一下**Enable和Submit**，如下圖所示。



Cloud Services Settings

Settings	
Threat Response:	Enabled

根據您的位置選擇雲，如下圖所示。



Cloud Services Settings

Success — Your changes have been committed.

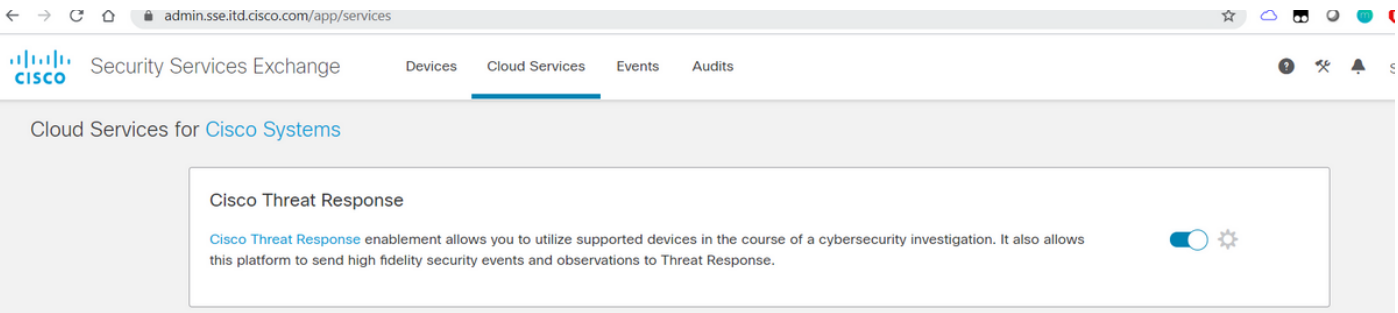
Settings	
Threat Response:	Enabled

Registration	
Cloud Services Status:	Not Registered
Threat Response Server:	AMERICAS (api-sse.cisco.com) ▼
Registration Token: ?	

步驟3.如果您沒有思科安全帳戶，則可以在思科威脅響應門戶中建立具有管理員訪問許可權的使用者帳戶。

若要建立新的使用者帳戶，請導航到思科威脅響應門戶登錄頁面。

步驟4.在SSE門戶的雲服務下啟用思科威脅響應，如下圖所示。


admin.sse.itd.cisco.com/app/services
Security Services Exchange
Devices
Cloud Services
Events
Audits

Cloud Services for Cisco Systems

Cisco Threat Response

Cisco Threat Response enablement allows you to utilize supported devices in the course of a cybersecurity investigation. It also allows this platform to send high fidelity security events and observations to Threat Response.

步驟5. 確保WSA在埠443上可訪問SSE門戶：

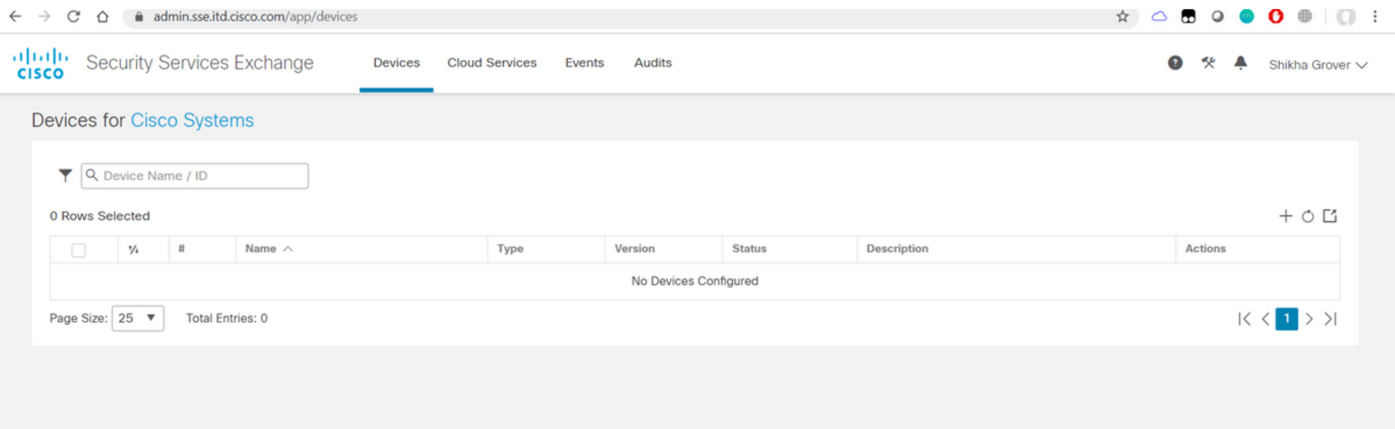
- api.eu.sse.itd.cisco.com(歐洲)
- api-sse.cisco.com（美洲）

註冊裝置

步驟1.從安全服務交換(SSE)門戶獲取註冊令牌，以向安全服務交換門戶註冊裝置。

SSE門戶連結為https://admin.sse.itd.cisco.com/app/devices。

> **附註**：使用CTR帳戶憑證登入到SSE門戶。


admin.sse.itd.cisco.com/app/devices
Security Services Exchange
Devices
Cloud Services
Events
Audits
Shikha Grover

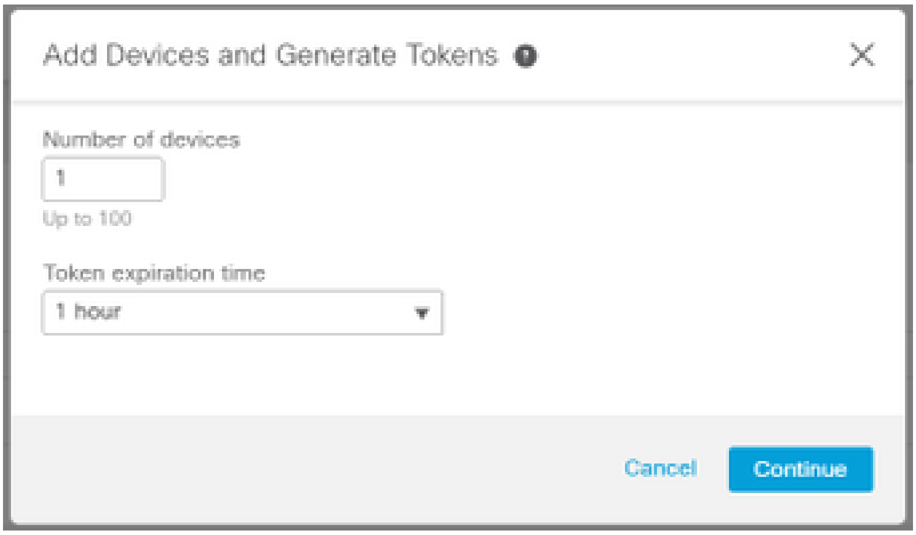
Devices for Cisco Systems

Device Name / ID

0 Rows Selected

□	⁰⁄₀	#	Name	Type	Version	Status	Description	Actions
					No Devices Configured			

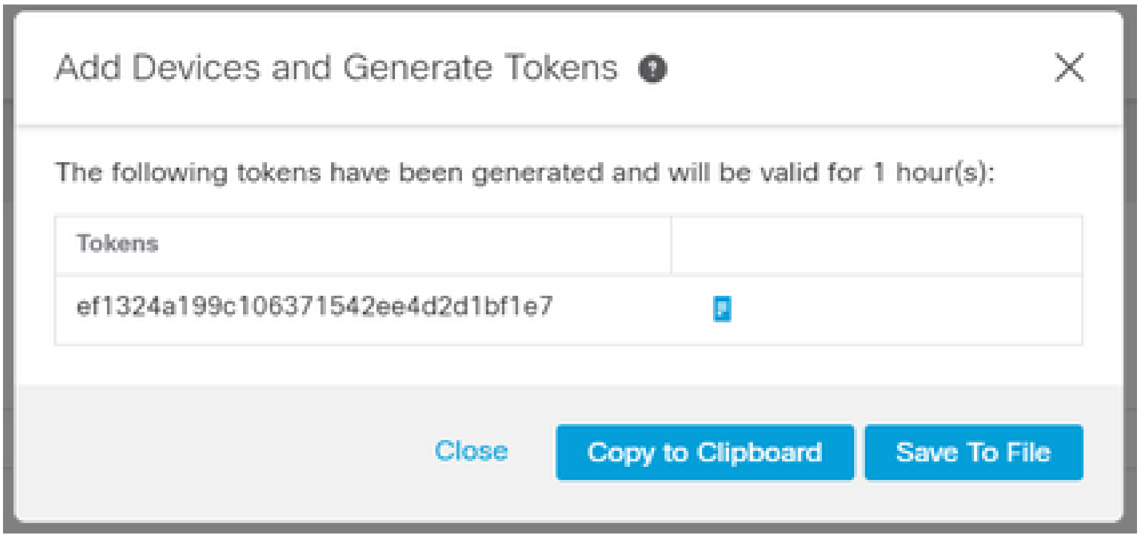
Page Size: 25 Total Entries: 0


Add Devices and Generate Tokens

Number of devices: 1

Up to 100

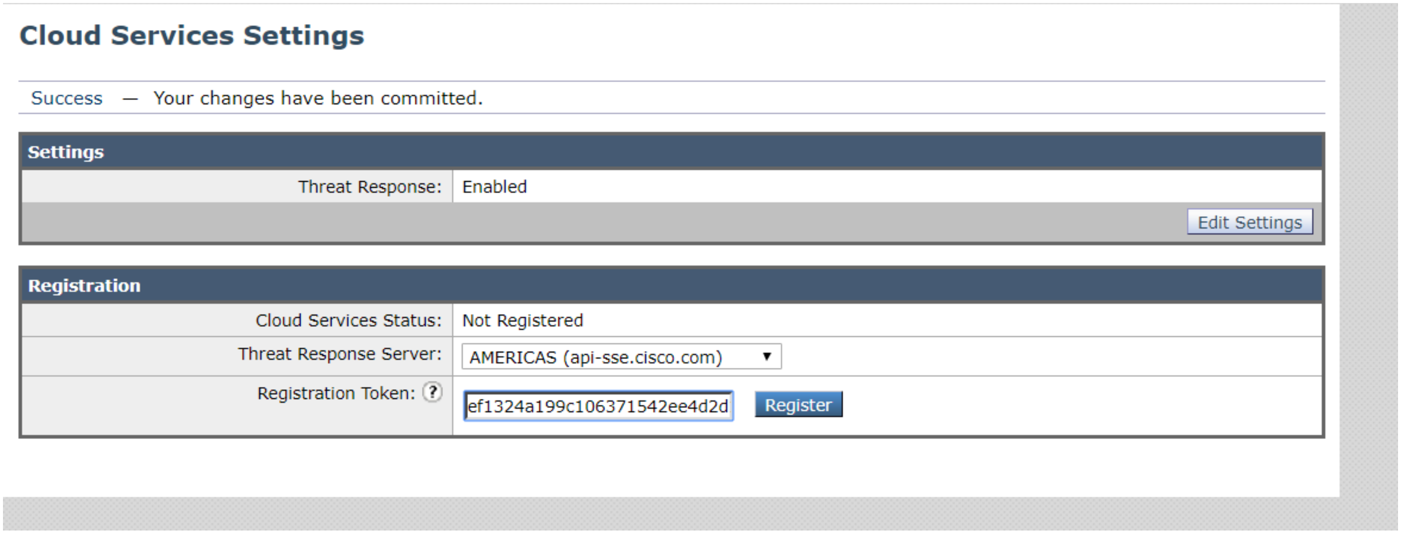
Token expiration time: 1 hour



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

Tokens	
ef1324a199c106371542ee4d2d1bf1e7	

步驟2.在WSA中輸入從Security Services Exchange門戶獲取的註冊令牌，然後點選**Register，如下圖所示。**



Cloud Services Settings

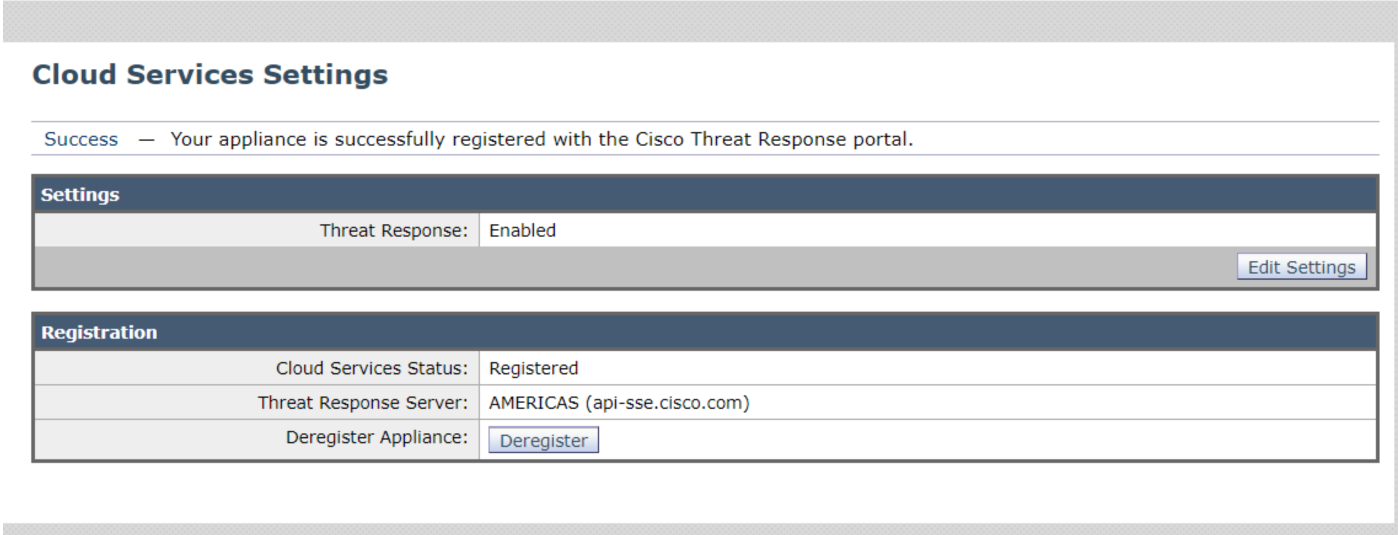
Success — Your changes have been committed.

Settings	
Threat Response:	Enabled

Registration	
Cloud Services Status:	Not Registered
Threat Response Server:	AMERICAS (api-sse.cisco.com)
Registration Token: ?	ef1324a199c106371542ee4d2d

步驟3.幾秒鐘後，您會看到註冊成功。

注意：確保在生成的令牌過期之前已使用該令牌。



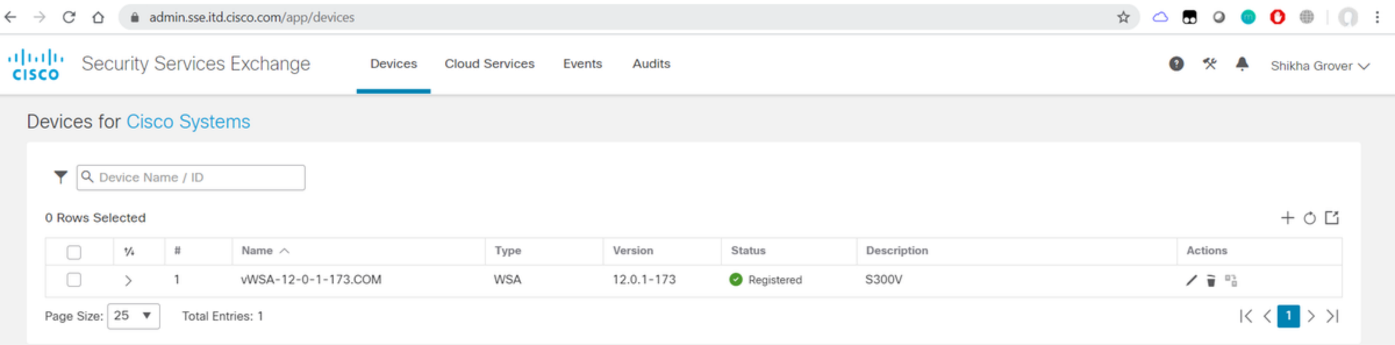
Cloud Services Settings

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

Settings	
Threat Response:	Enabled

Registration	
Cloud Services Status:	Registered
Threat Response Server:	AMERICAS (api-sse.cisco.com)
Deregister Appliance:	Deregister

步驟4.在SSE門戶上，您可以檢視裝置狀態。



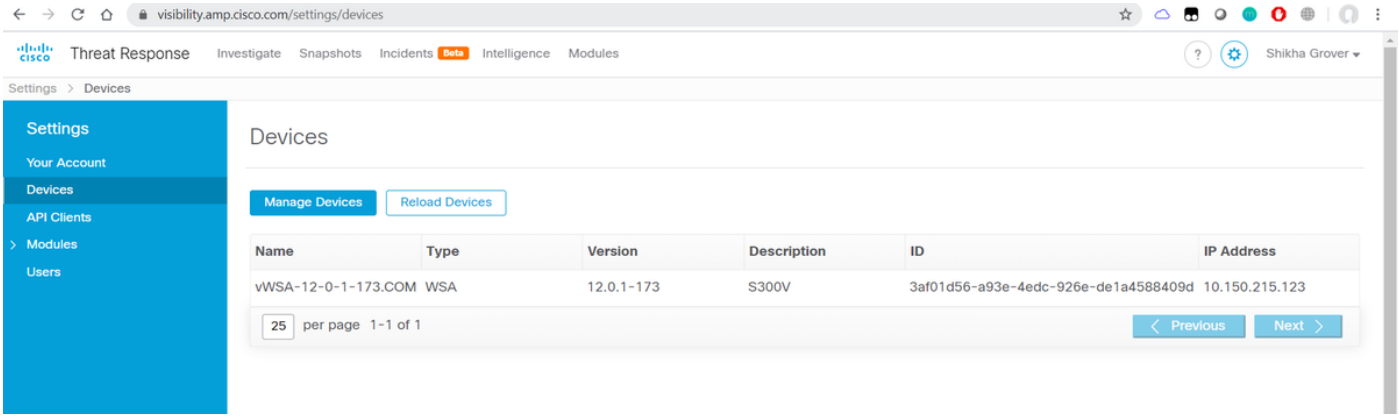
Devices for Cisco Systems

0 Rows Selected

	⅟ₓ	#	Name	Type	Version	Status	Description	Actions
□	>	1	vWSA-12-0-1-173.COM	WSA	12.0.1-173	● Registered	S300V	

Page Size: 25 Total Entries: 1

步驟5.在CTR入口上顯示裝置已註冊。

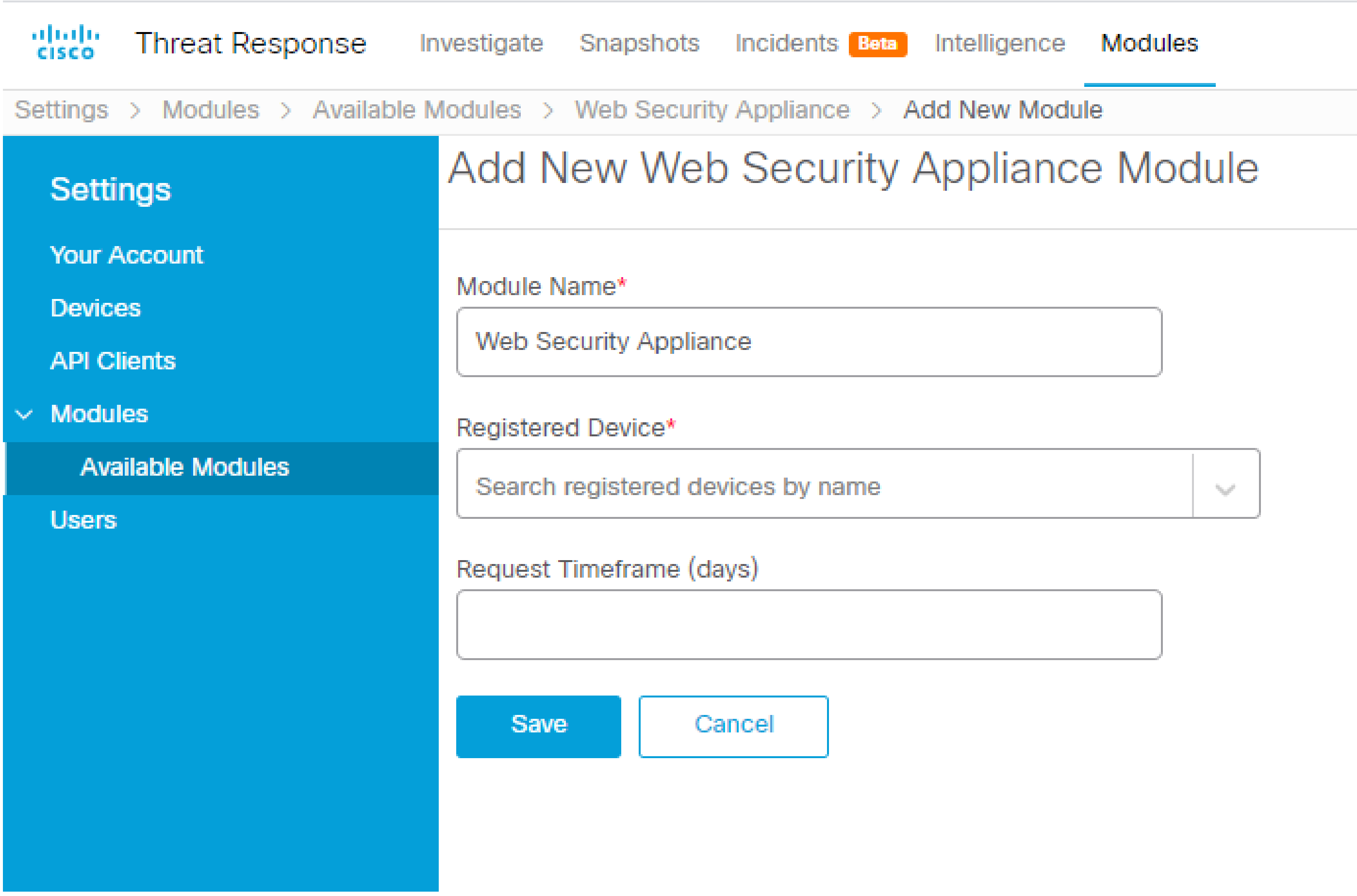


Devices

Name	Type	Version	Description	ID	IP Address
vWSA-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

您可以將此裝置關聯到模組，導航到**模組>新增新模組>網路安全裝置**，如下圖所示。



Add New Web Security Appliance Module

Module Name*: Web Security Appliance

Registered Device*: Search registered devices by name

Request Timeframe (days):

裝置現在已整合。您可以通過WSA的流量並調查CTR門戶上的威脅。

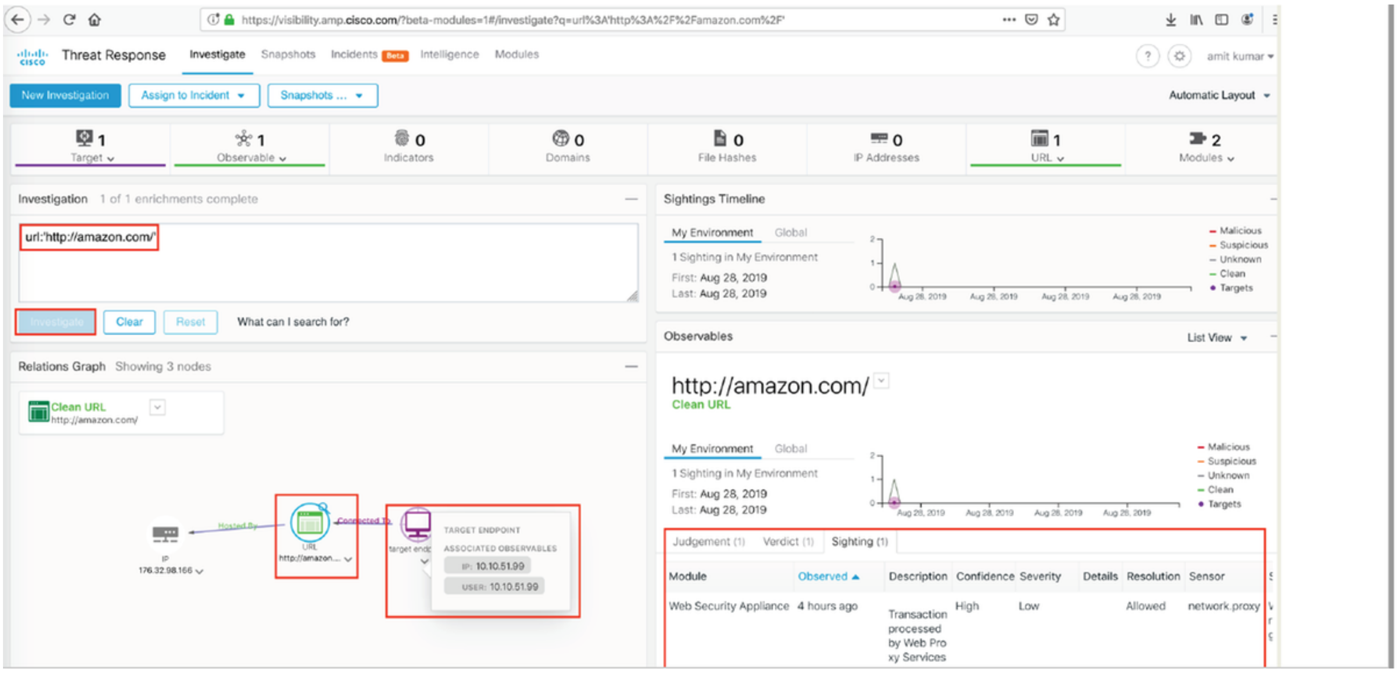
驗證

使用本節內容，確認您的組態是否正常運作。

可用於從CTR門戶運行查詢的WSA模組及其支援的格式的豐富內容（查詢WSA日誌）：

- 域-域："com"
- URL - url:"http://www.neverssl.com"
- SHA256 - sha256:"8d3a8badf6e5a38e1b6d59a254969b1e0274f8fa120254ba1f7e02991872379"
- IP - ip:"172.217.26.164"
- Filename - file_name:"test.txt"

使用中的豐富示例：



https://visibility.amp.cisco.com/?beta-modules=1#/investigate?q=url%3A'http%3A%2F%2Famazon.com%2F'

Investigation 1 of 1 enrichments complete

url:'http://amazon.com/'

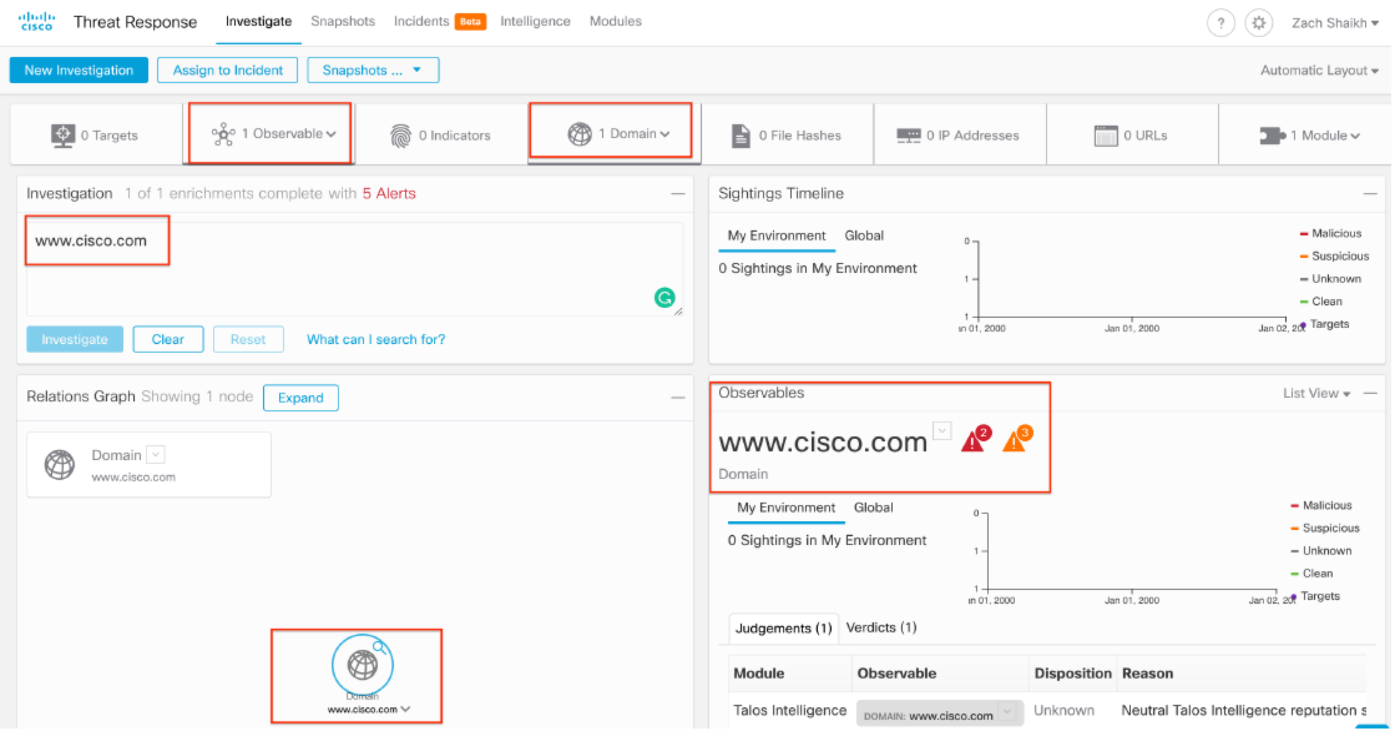
1 Sighting in My Environment
First: Aug 28, 2019
Last: Aug 28, 2019

http://amazon.com/
Clean URL

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



Investigation 1 of 1 enrichments complete with 5 Alerts

www.cisco.com

0 Sightings in My Environment

www.cisco.com
Domain

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

如果漏掉了一些應該包括的內容，請隨時通知我。 如果漏掉了一些應該包括的內容，請隨時通知我。 如果漏掉了一些應該包括的內容，請隨時通知我。 如果漏掉了一些應該包括的內容，請隨時通知我。