

思科威脅響應(CTR)和ESA整合

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[步驟1. 導航到Network > Cloud Service Settings](#)

[步驟2. 點選Edit Settings](#)

[步驟3. 選中Enable和Threat Response Server覆取方塊](#)

[步驟4. 提交和提交更改](#)

[步驟5. 登入到CTR門戶並生成ESA中請求的註冊令牌](#)

[步驟6. 在ESA中貼上註冊令牌 \(從CTR門戶生成 \)](#)

[步驟7. 驗證您的ESA裝置是否在SSE門戶中](#)

[步驟8. 導航到CTR門戶並新增新的ESA模組](#)

[驗證](#)

[疑難排解](#)

[CTR門戶中未顯示ESA裝置](#)

[CTR調查未顯示來自ESA的資料](#)

[ESA沒有請求註冊令牌](#)

[註冊失敗，因為令牌無效或已過期](#)

[相關資訊](#)

簡介

本檔案介紹將思科威脅回應(CTR)與電子郵件安全裝置(ESA)整合的流程，以及如何驗證該流程以便執行某些CTR調查。

必要條件

需求

思科建議您瞭解以下主題：

- 思科威脅回應
- 電子郵件安全裝置

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- CTR帳戶

- 思科安全服務交換
- 軟體版本13.0.0-392上的ESA C100V

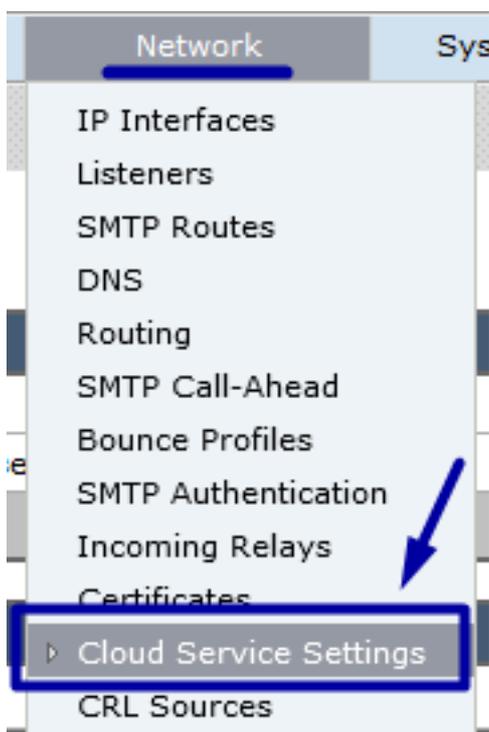
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

要配置整合CTR和ESA，請登入您的郵件安全虛擬裝置並執行以下快速步驟：

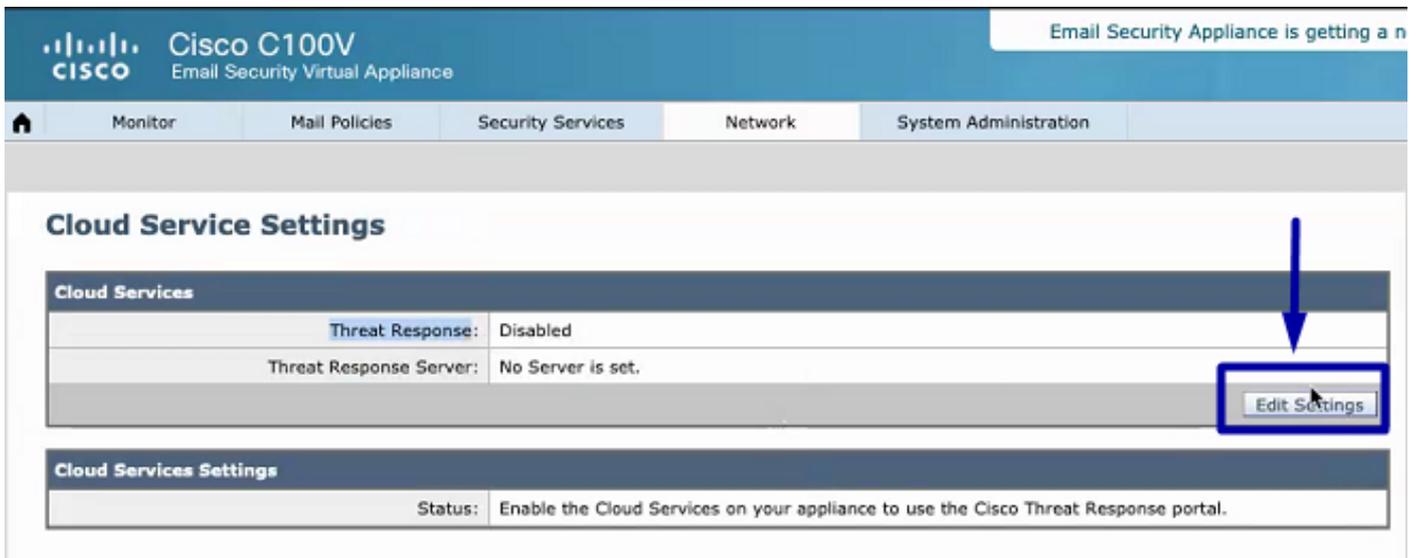
步驟1. 導航到Network > Cloud Service Settings

進入ESA後，導航到上下文選單Network > Cloud Service Settings，以檢視當前威脅響應狀態（禁用/啟用），如下圖所示。



步驟2. 點選Edit Settings

ESA中的「Threat Response」（威脅響應）功能已禁用，要啟用該功能，請按一下「Edit Settings」（編輯設定），如下圖所示：



步驟3.選中Enable和Threat Response Server覈取方塊

選中Enable覈取方塊，然後選擇Threat Response Server，請參閱以下影象：

Cloud Service Settings

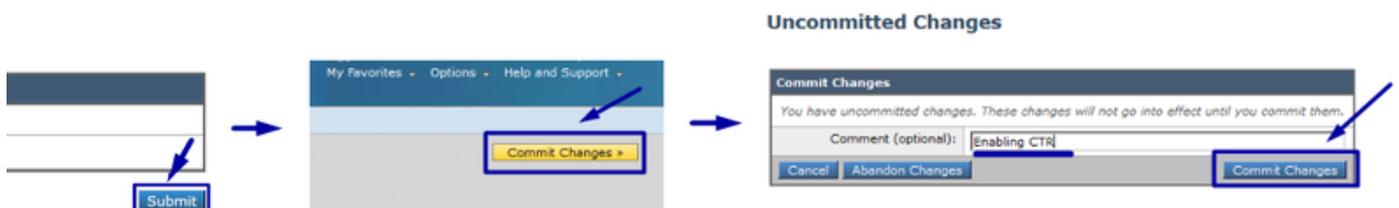


附註：威脅響應伺服器URL的預設選擇為AMERICAS(api-sse.cisco.com)。對於EUROPE企業，請按一下下拉選單並選擇EUROPE(api.eu.sse.itd.cisco.com)

步驟4.提交和提交更改

提交和提交更改是儲存和應用更改所必需的。現在，如果ESA介面刷新，則請求註冊令牌以註冊整合，如下圖所示。

附註：您可以看到一條成功消息：您的更改已提交。



Cloud Service Settings

Success — Your changes have been committed.

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
Edit Settings	

Cloud Services Settings	
Status:	The Cisco Cloud Service is busy. Navigate back to this page after some time to check the appliance status.

Cloud Service Settings

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
Edit Settings	

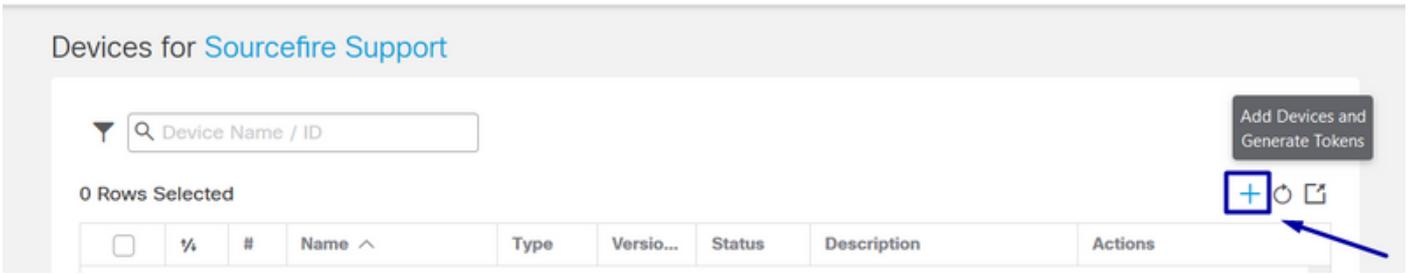
Cloud Services Settings	
Registration Token: ?	<input type="text"/>
Register	

步驟5.登入到CTR門戶並生成ESA中請求的註冊令牌

1. — 進入CTR門戶後，導航至Modules > Devices > Manage Devices，請參見下一個映像。

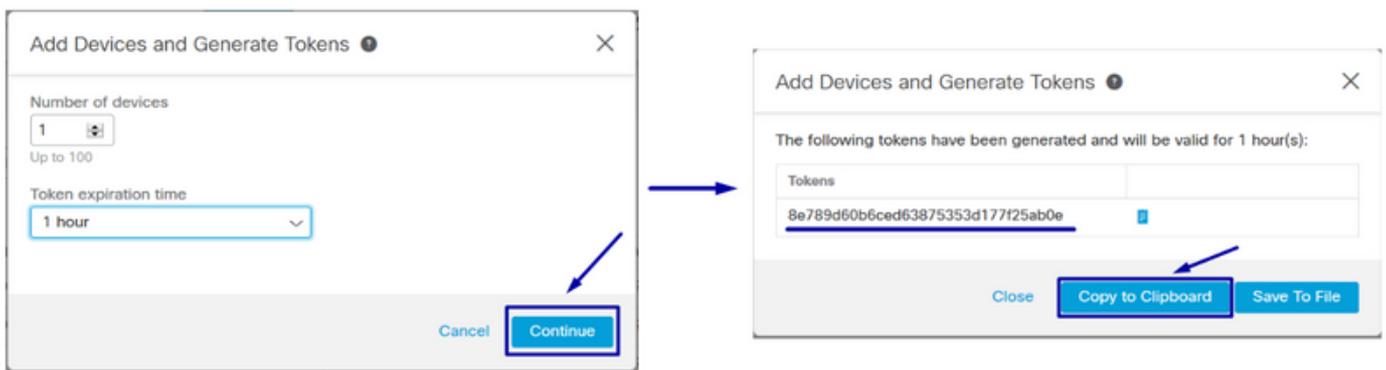
The screenshot shows the Cisco Threat Response web interface. The browser address bar displays <https://visibility.amp.cisco.com/settings/devices>. The navigation menu includes Threat Response, Investigate, Snapshots, Incidents (Beta), Intelligence, and Modules. The 'Modules' link is highlighted with a blue box and an arrow. Below the navigation menu, the breadcrumb 'Settings > Devices' is shown. The 'Devices' section is active, displaying a 'Manage Devices' button (highlighted with a blue box and arrow) and a 'Reload Devices' button. A sidebar on the left contains a 'Settings' menu with 'Your Account', 'Devices' (highlighted with a blue box and arrow), 'API Clients', and '> Modules'.

2.- Manage Devices (管理裝置) 連結將您重定向至Security Services Exchange(SSE)，在此連結後，按一下Add Devices (新增裝置) 和Generate Token (生成令牌) 圖示，如下圖所示。



3. — 按一下「繼續」以生成令牌，生成令牌後，按一下「複製到剪貼簿」，如下圖所示。

提示：您可以選擇要新增的裝置數量（從1到100），還可以選擇令牌過期時間（1小時、2小時、4小時、6小時、8小時、12小時、01天、02天、03天、04天和05天）。



步驟6.在ESA中貼上註冊令牌（從CTR門戶生成）

生成註冊令牌後，將其貼上到ESA的Cloud Services Settings部分，如下圖所示。

附註：您可以看到一條成功消息：向思科威脅響應門戶註冊裝置的請求已啟動。一段時間後導航回此頁面以檢查裝置狀態。

Cloud Service Settings



Cloud Service Settings

Success — A request to register your appliance with the Cisco Threat Response portal is initiated. Navigate back to this page after some time to check the appliance status.

Cloud Services

Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)

[Edit Settings](#)

Cloud Services Settings

Status:	The appliance registration is in progress. Navigate back to this page after some time to check the appliance status.
---------	--

步驟7. 驗證您的ESA裝置是否在SSE門戶中

您可以導覽至SSE入口網站(CTR > Modules > Devices > Manage Devices)，然後在Search頁籤中檢視ESA裝置，如下圖所示。

Security Services Exchange Audit Log Brenda Marquez

Devices for Sourcefire Support

Search:

0 Rows Selected

	%	#	Name ^	Type	Versio...	Status	Description	Actions
<input type="checkbox"/>	▼	1	esa03.mex-amp.inl...	ESA	13.0.0	Registered	ESA	/ 🗑️ 🔍

ID: 874141f7-903f-4be9-b14e-45a7f... IP Address: 127.0.0.1 Connector Version: 1.3.34
Created: 2020-05-11 20:41:05 UTC

步驟8. 導航到CTR門戶並新增新的ESA模組

1. — 進入CTR門戶後，請導航至Modules > Add New Module，如下圖所示。

Threat Response Investigate Snapshots Incidents Intelligence **Modules** Brenda Marquez

Modules

Intelligence within Cisco Threat Response is provided by modules, which can also enable response capabilities. [Click here to view all the available modules.](#)

Your Configurations

[+](#)
Add New Module

Amp AMP for Endpoints
AMP for Endpoints

AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach your endpoints.

[Edit](#) [Learn More](#)

2. — 選擇模組型別，在這種情況下，該模組是郵件安全裝置模組，如下圖所示。

Settings

Your Account

Devices

API Clients

Modules

Available Modules

Users

Available Modules

Select a module you would like to add, or [click here to learn more](#) about modules configuration.

Amp AMP for Endpoints

AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach your endpoints.

[Add New Module](#) [Learn More](#) · [Free Trial](#)

Esa Email Security Appliance

The Cisco Email Security Appliance (ESA) provides advanced threat protection capabilities to detect, block, and remediate threats faster, prevent data loss, and secu...

[Add New Module](#) [Learn More](#)

3. 輸入欄位：模組名稱、已註冊裝置（選擇以前註冊的裝置）、請求時間範圍（天）和儲存，如下圖所示。

Settings > Modules > Available Modules > Email Security Appliance > Add New Module

Add New Email Security Appliance Module

Module Name*

Registered Device*

esa03.mex-amp.inlab
Type ESA
ID 874141f7-903f-4be9-b14e-45a7f34a2032
IP Address 127.0.0.1

Request Timeframe (days)

[Save](#) [Cancel](#)

Quick Start [Help](#)

When configuring Email Security Appliance (ESA) integration, you must first enable the integration in ESA. You then enable Threat Response in Security Services Exchange, add the device and register it. After this is completed, you add the ESA module.

Prerequisite: ESA running minimum AsyncOS 13.0 0-314 (LD) release.

Note: Customers with multiple ESAs reporting to an SMA can use the SMA Module configuration for Email Security. Customers that do not have an SMA, can use the ESA Module for integration.

- In ESA, navigate to **Networks > Cloud Service Settings > Edit Settings**, enable integration and confirm that the ESA is ready to accept a registration token.
- Click the **Settings** icon (gear) and then click **Devices > Manage Devices** to be taken to Security Services Exchange.
- Enable **Cisco Threat Response** integration on the **Cloud Services** tab, and then click the **Devices** tab and click the + icon to add a new device.
- Specify the token expiration time (the default is 1 hour), and click **Continue**.
- Copy the generated token and confirm the device has been created.
- Navigate to your ESA (**Network > Cloud Service Settings**) to insert the token, and then click **Register**. Confirm successful registration by reviewing the status in Security Services Exchange and confirm the ESA is displayed on the **Devices** page.
- Complete the **Add New Email Security Appliance Module** form:
 - Module Name** - Leave the default name or enter a name that is meaningful to you.
 - Registered Device** - From the drop-down list, choose the device you registered in Security Services Exchange.
 - Request Timeframe (days)** - Enter the timeframe (in days) for querying the API endpoint (default is 30 days).
- Click **Save** to complete the ESA module configuration.

驗證

為了驗證CTR和ESA整合，您可以傳送測試電子郵件（也可以從ESA中檢視），導航到Monitor > Message Tracking，然後查詢測試電子郵件。在本例中，我按郵件主題過濾為下圖。

Cisco C100V
Email Security Virtual Appliance

Monitor | Mail Policies | Security Services | Network | System Administration

Message Tracking

Search

Available Time Range: 14 May 2020 12:44 to 14 May 2020 13:41 (GMT +00:00) Data in time range: 100.0% complete

Envelope Sender: ? Begins With []

Envelope Recipient: ? Begins With []

Subject: Begins With test test

Message Received: Last Day Last Week Custom Range

Start Date: 05/13/2020 Time: 13:00 and End Date: 05/14/2020 Time: 13:42 (GMT +00:00)

Advanced Search messages using advanced criteria

Clear Search

Generated: 14 May 2020 13:42 (GMT +00:00) Export All... | Export...

Results

Items per page 20

Displaying 1 — 1 of 1 items.

1	14 May 2020 13:23:57 (GMT +00:00)	MID: 8	Show Details
---	-----------------------------------	--------	--------------

SENDER: mgmt01@cisco.com
RECIPIENT: testingBren@cisco.com
SUBJECT: test test
LAST STATE: Message 8 to testingBren@cisco.com received remote SMTP response 'ok: Me:

Displaying 1 — 1 of 1 items.

現在，您可以從CTR門戶執行調查、導航到Investigate並使用某些電子郵件可觀察量，如圖所示。

The screenshot shows the Cisco Threat Response Investigate interface. At the top, there are navigation tabs: Threat Response, Investigate, Snapshots, Incidents, Intelligence, and Modules. Below the navigation, there are filters for 1 Target, 1 Observable, 0 Indicators, 0 Domains, 0 File Hashes, 0 IP Addresses, 0 URLs, and 1 Module. The search bar contains the query 'email_subject:"test test"'. Below the search bar, there are buttons for 'Investigate', 'Clear', and 'Reset'. The main area is divided into three panels: 'Relations Graph' showing a network of nodes (IP, Target Email, Email Subject, Cisco Message ID, Domain, Email Address), 'Sightings' showing a graph of sightings over time, and 'Observables' showing a list of sightings. A blue box highlights the search query, and another blue box highlights the resulting sighting in the table.

Module	Observed	Description	Confidence	Severity	Details
esa03	9 hours ago	Incoming message (Delivered)	High	Low	

提示：您可以對其它電子郵件觀察量使用相同的語法，如下圖所示。

IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file name	file_name:"invoice.pdf"

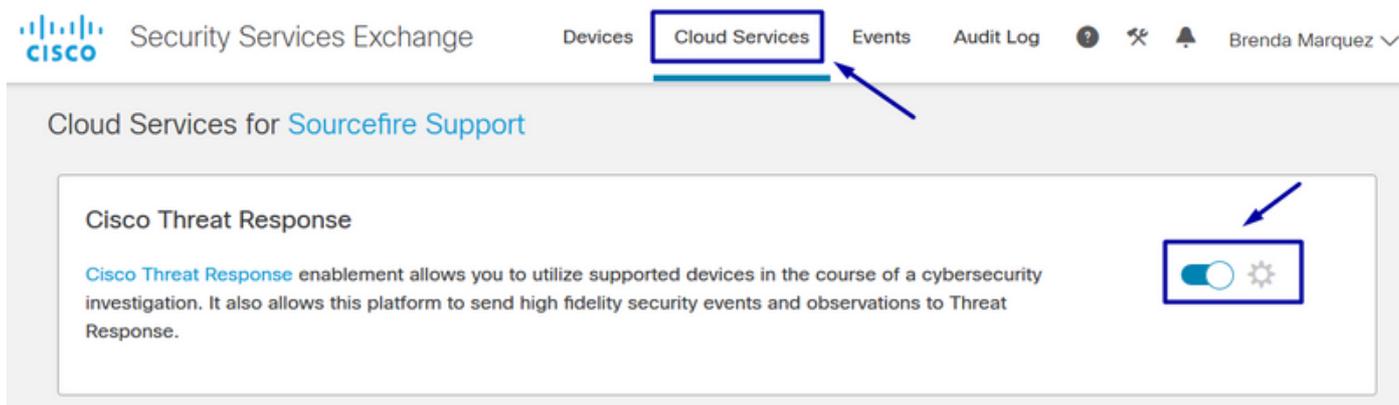
疑難排解

如果您是CES客戶，或者通過SMA管理ESA裝置，則只能通過SMA連線到Threat Response。請確保您的SMA運行AsyncOS 12.5或更高版本。如果您沒有使用SMA管理ESA，並且直接整合ESA，請確保它是AsyncOS 13.0版或更高版本。

CTR門戶中未顯示ESA裝置

如果在CTR門戶中新增ESA模組時，您的ESA裝置未顯示在下拉註冊裝置中，請確保在SSE中啟用

了CTR，在CTR中導航到Modules > Devices > Manage Devices，然後在SSE門戶中導航到Cloud Services並啟用CTR，如下圖所示：



CTR調查未顯示來自ESA的資料

請確保：

- 調查的語法是正確的，郵件可觀察量顯示在上面的驗證部分中。
- 您已選擇正確的威脅響應伺服器或雲（美洲/歐洲）。

ESA沒有請求註冊令牌

請確保在啟用威脅響應後提交更改，否則這些更改將不會應用於ESA中的威脅響應部分。

註冊失敗，因為令牌無效或已過期

請確保從正確的雲生成令牌：

如果將Europe(EU)Cloud for ESA，請從以下位置生成令牌：<https://admin.eu.sse.itd.cisco.com/>

如果將Americas(NAM)Cloud for ESA，請從以下位置生成令牌：<https://admin.sse.itd.cisco.com/>

此外，請記住，註冊令牌有到期時間（選擇最方便的時間及時完成整合）。

相關資訊

- 可以在[思科威脅響應和ESA整合影片](#)中找到本文包含的資訊。
- [技術支援與文件 - Cisco Systems](#)