思科威脅響應(CTR)和ESA整合

目錄

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

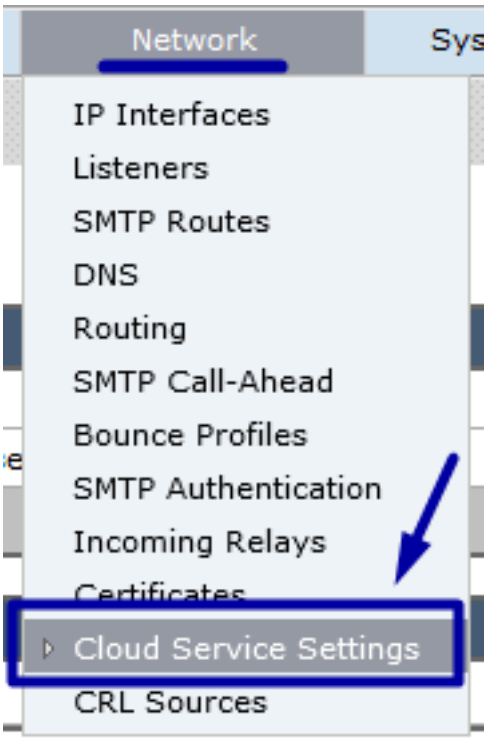
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

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：

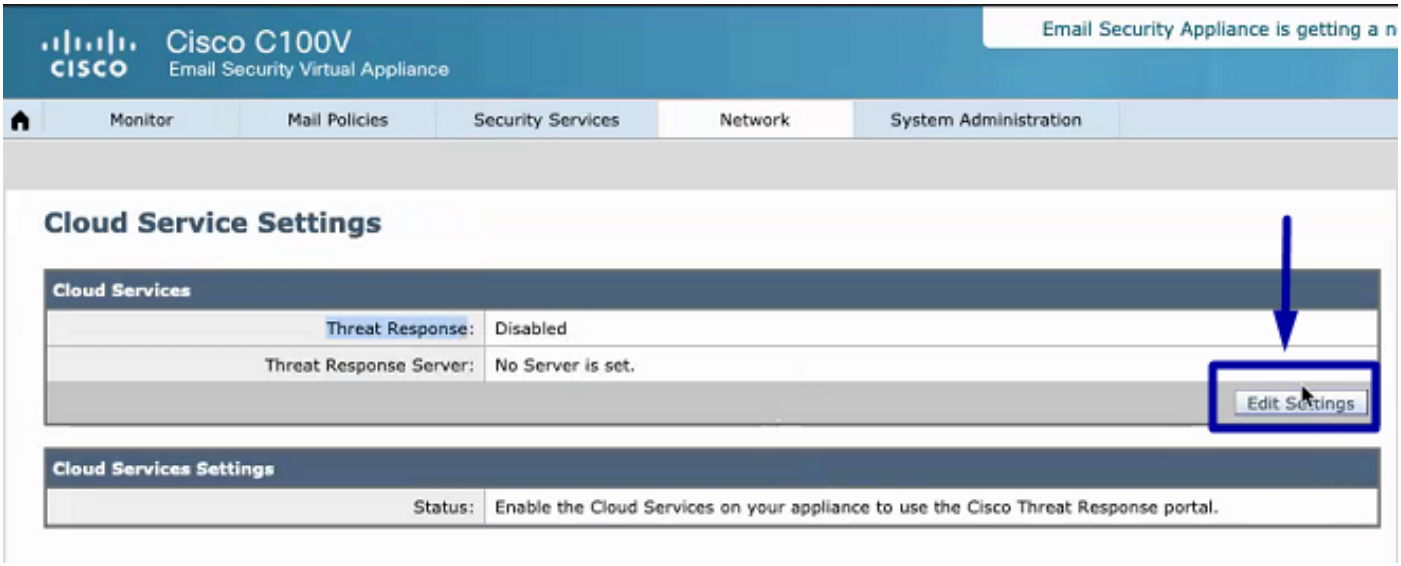
步驟1. 導航到Network > Cloud Service Settings

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。



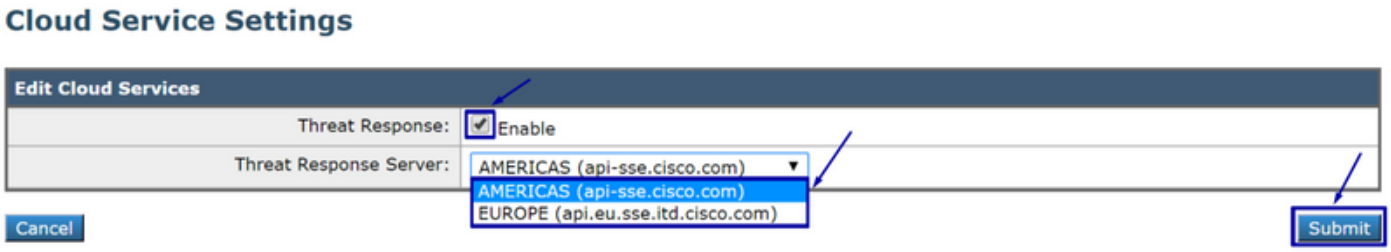
步驟2.點選Edit Settings

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：

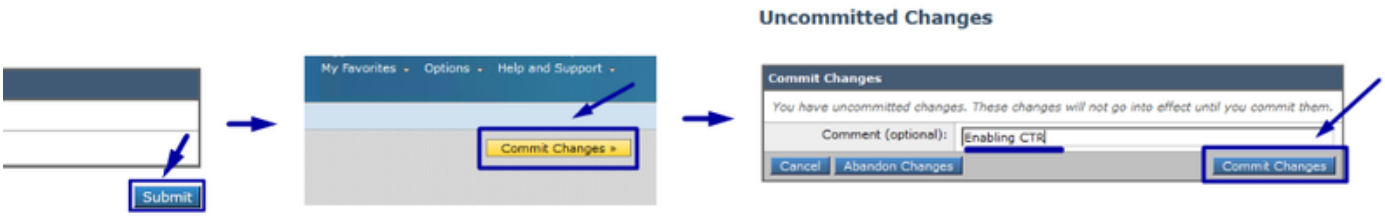


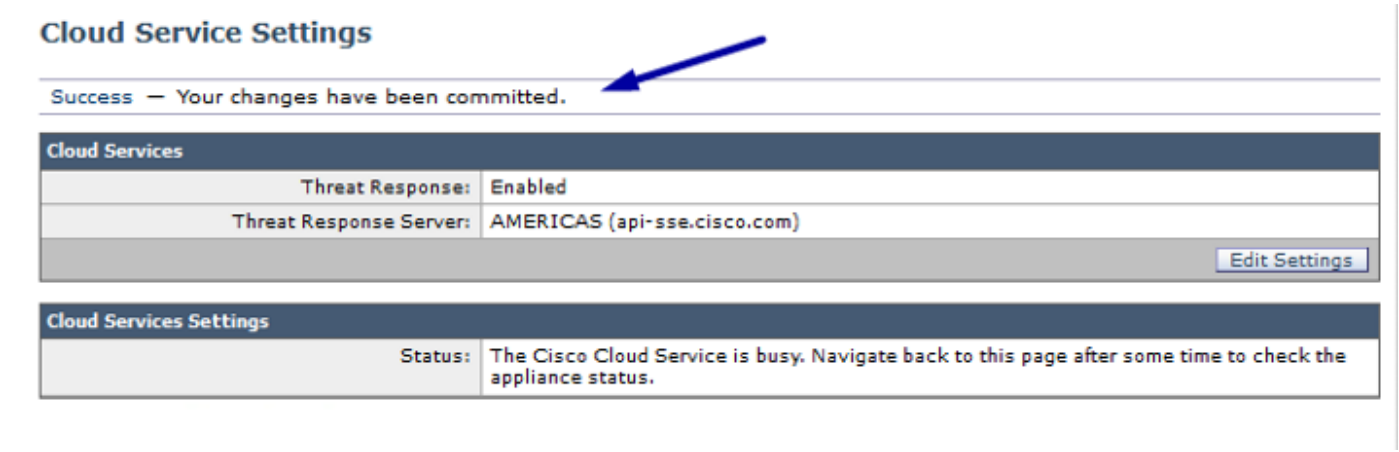
附註：威脅響應伺服器URL的預設選擇為AMERICAS(api-sse.cisco.com)。對於EUROPE企業，請按一下下拉選單並選擇EUROPE(api.eu.sse.itd.cisco.com)

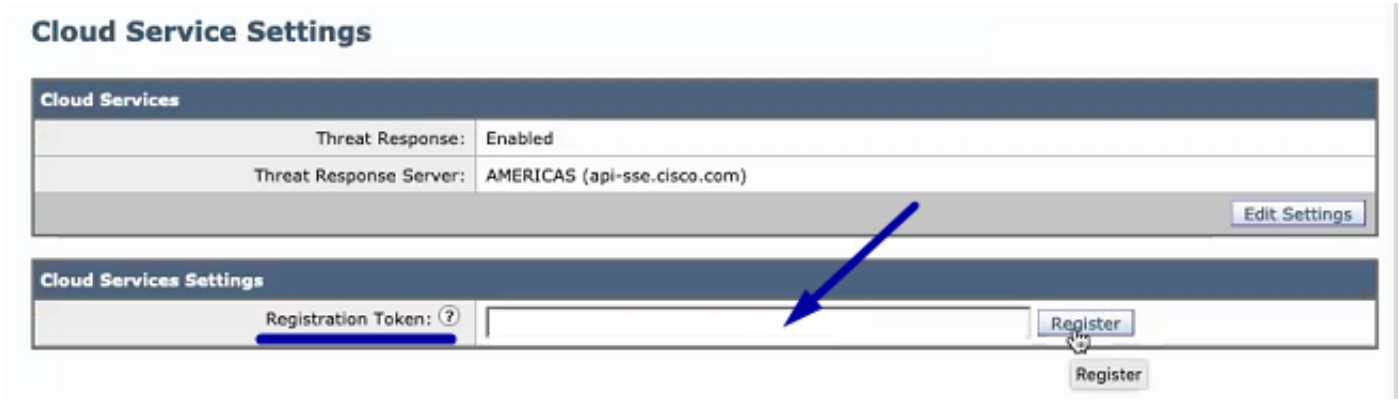
步驟4.提交和提交更改

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。

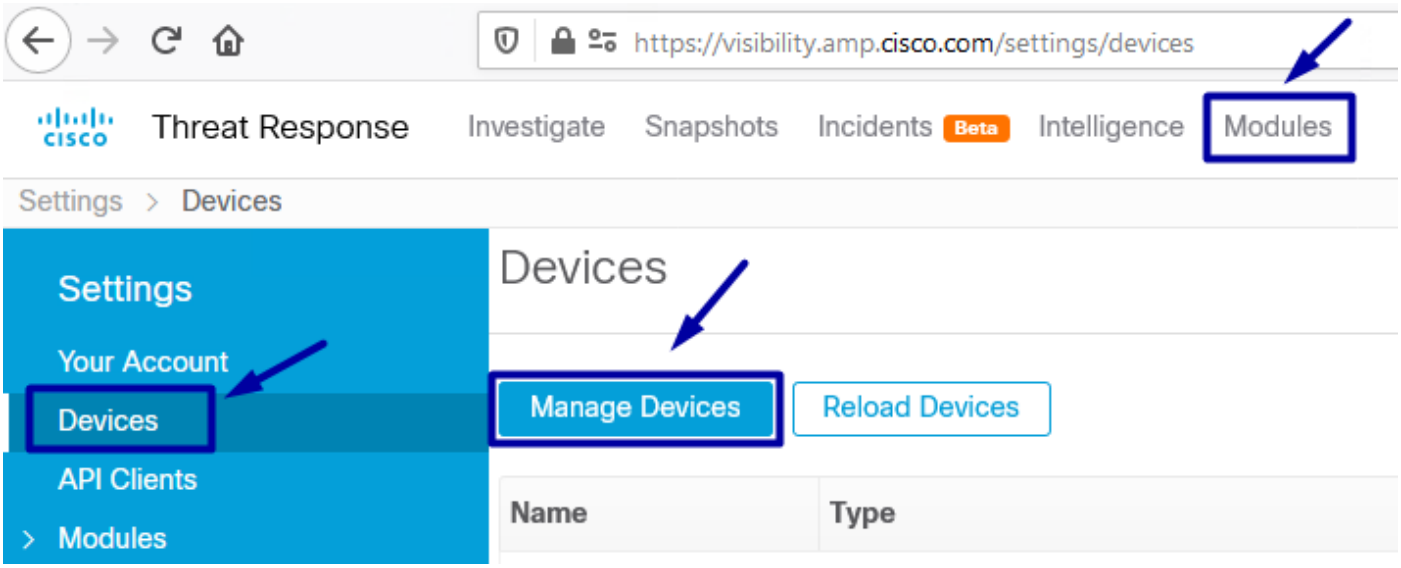




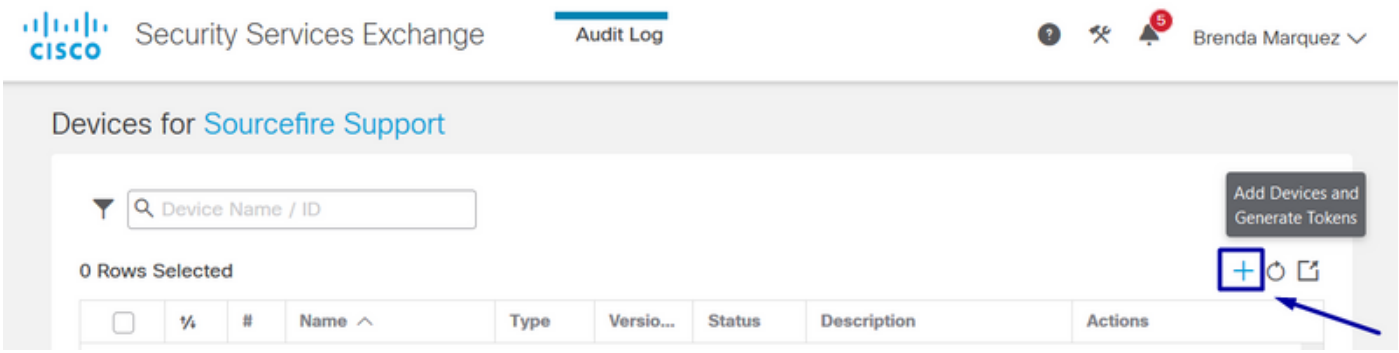


步驟5.登入到CTR門戶並生成ESA中請求的註冊令牌

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

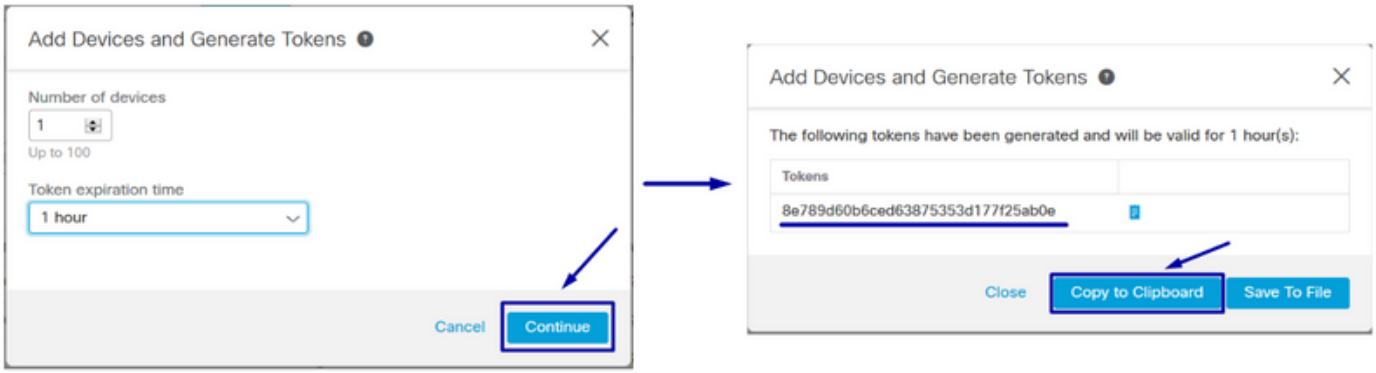


2.- Manage Devices（管理裝置）連結將您重定向至Security Services Exchange(SSE)，在此連結後，按一下Add Devices（新增裝置）和Generate Token（生成令牌）圖示，如下圖所示。



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。

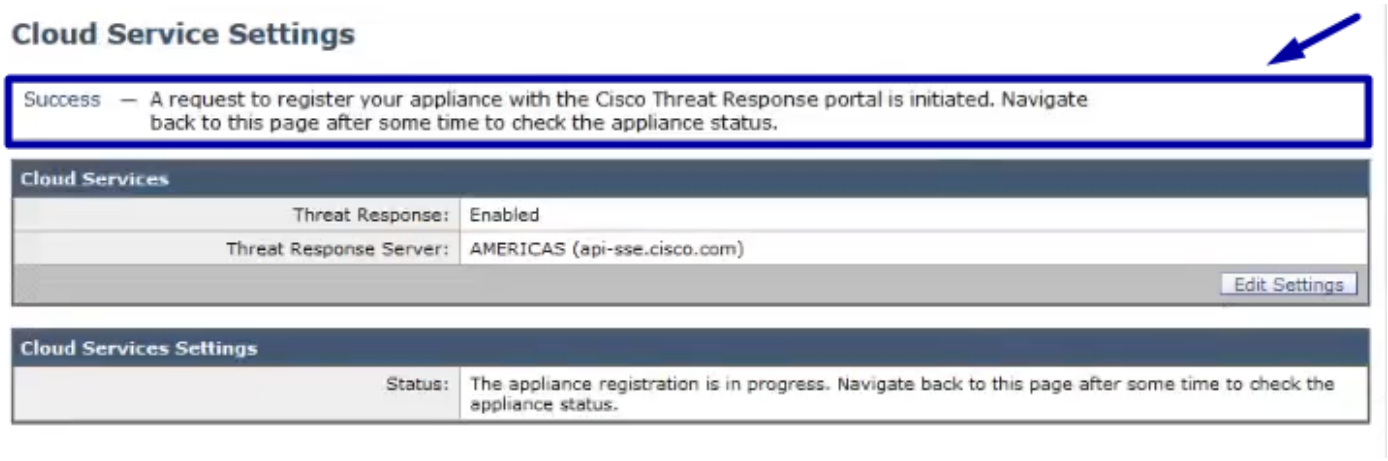
提示：您可以選擇要新增的裝置數量（從1到100），還可以選擇令牌過期時間（1小時、2小時、4小時、6小時、8小時、12小時、01天、02天、03天、04天和05天）。



步驟6.在ESA中貼上註冊令牌（從CTR門戶生成）

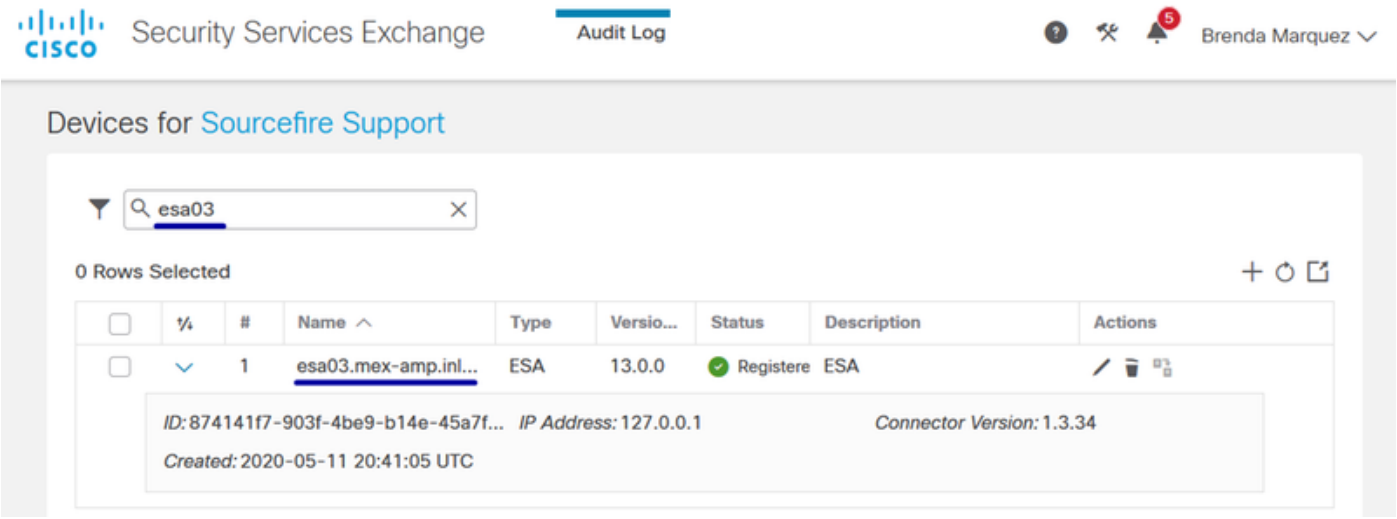
生成註冊令牌後，將其貼上到ESA的Cloud Services Settings部分，如下圖所示。

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。



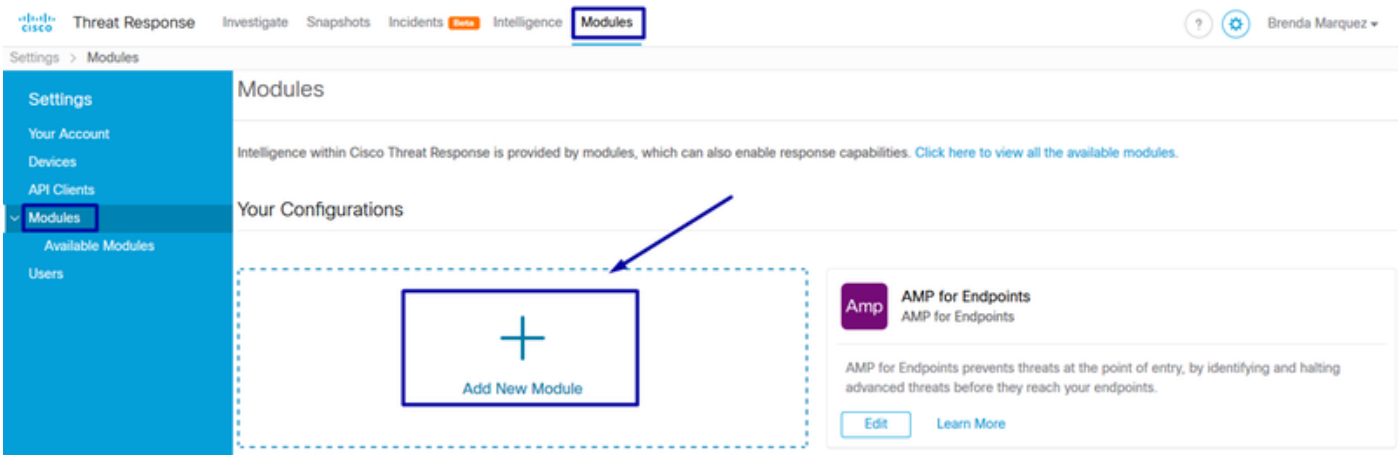
步驟7.驗證您的ESA裝置是否在SSE門戶中

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。

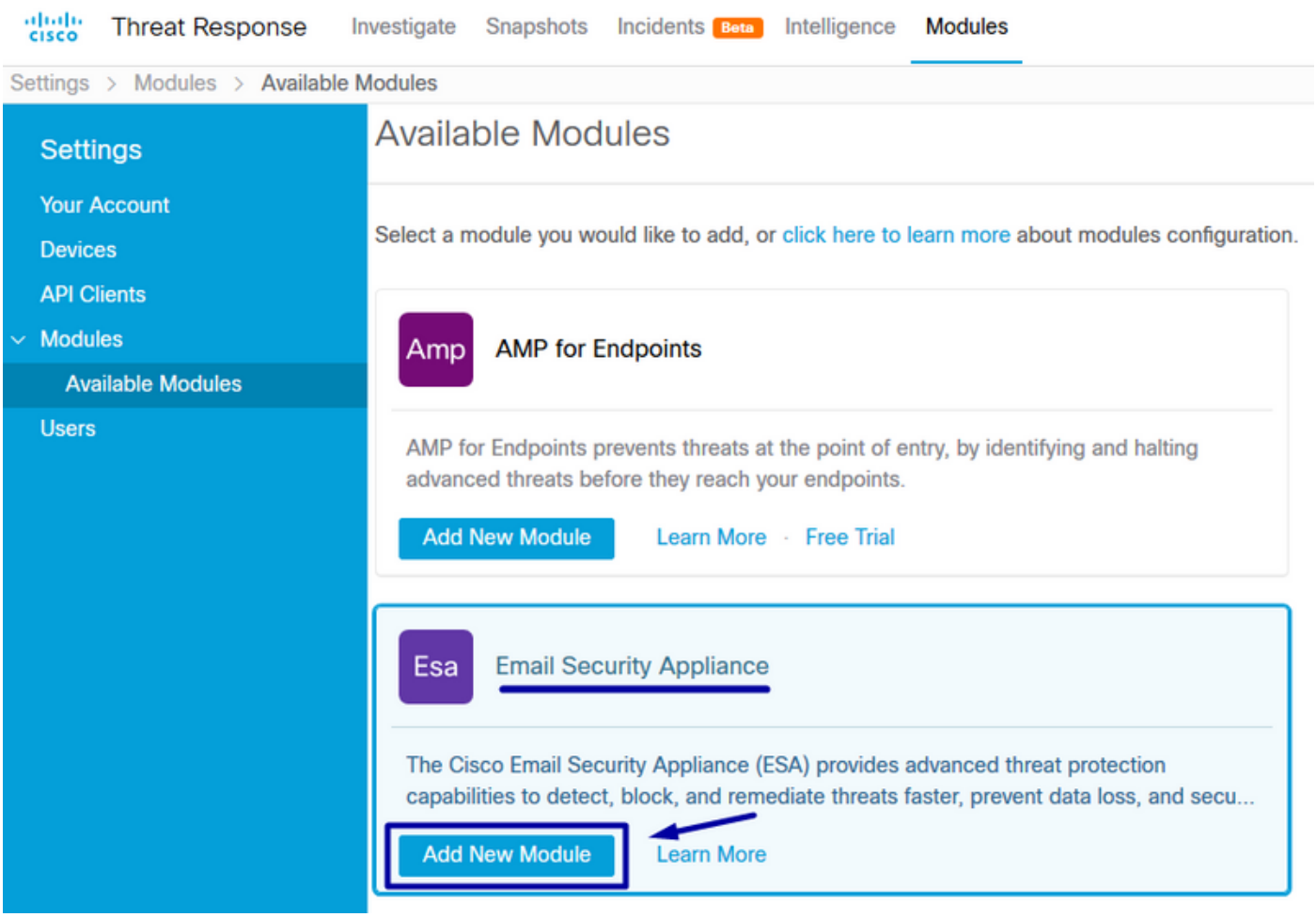


步驟8.導航到CTR門戶並新增新的ESA模組

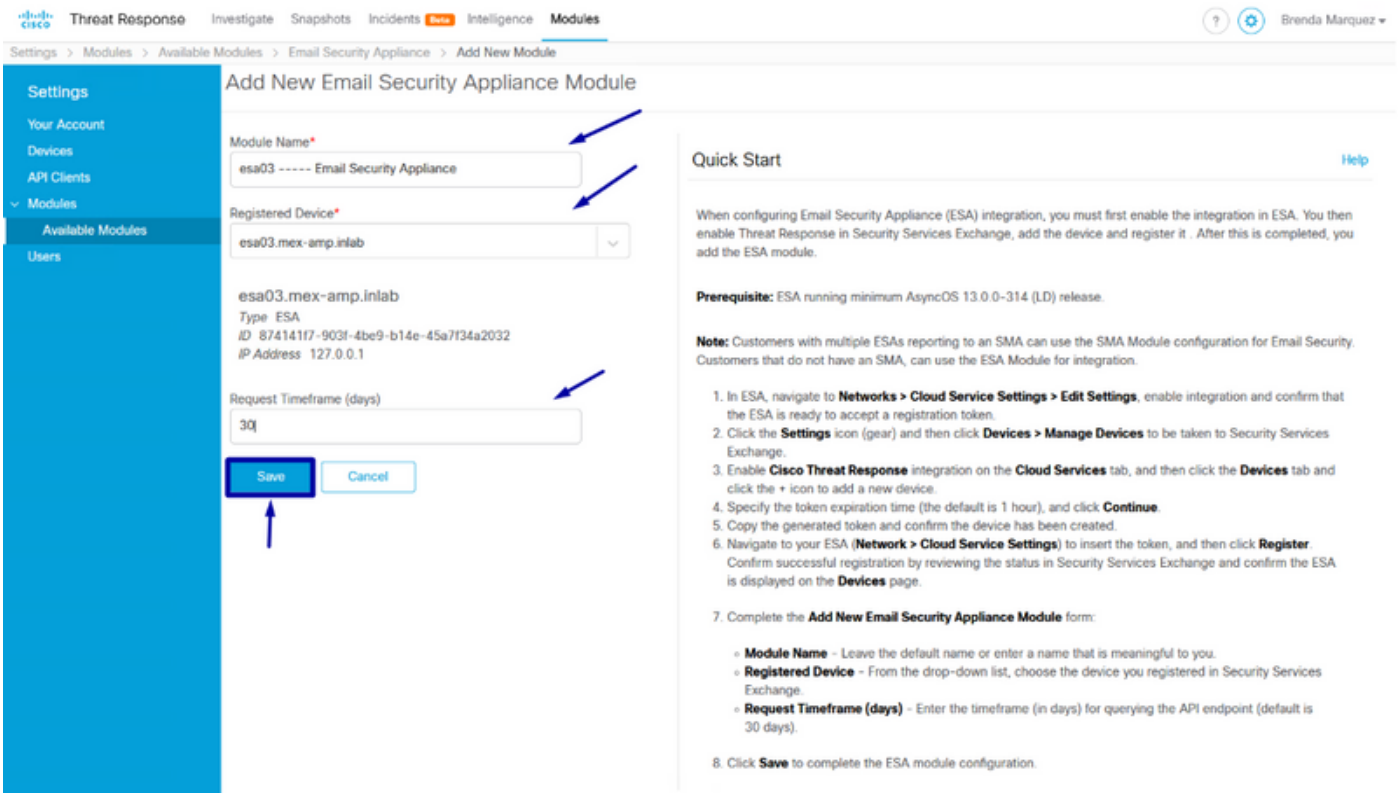
1. — 進入CTR門戶後，請導航至Modules > Add New Module，如下圖所示。



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。

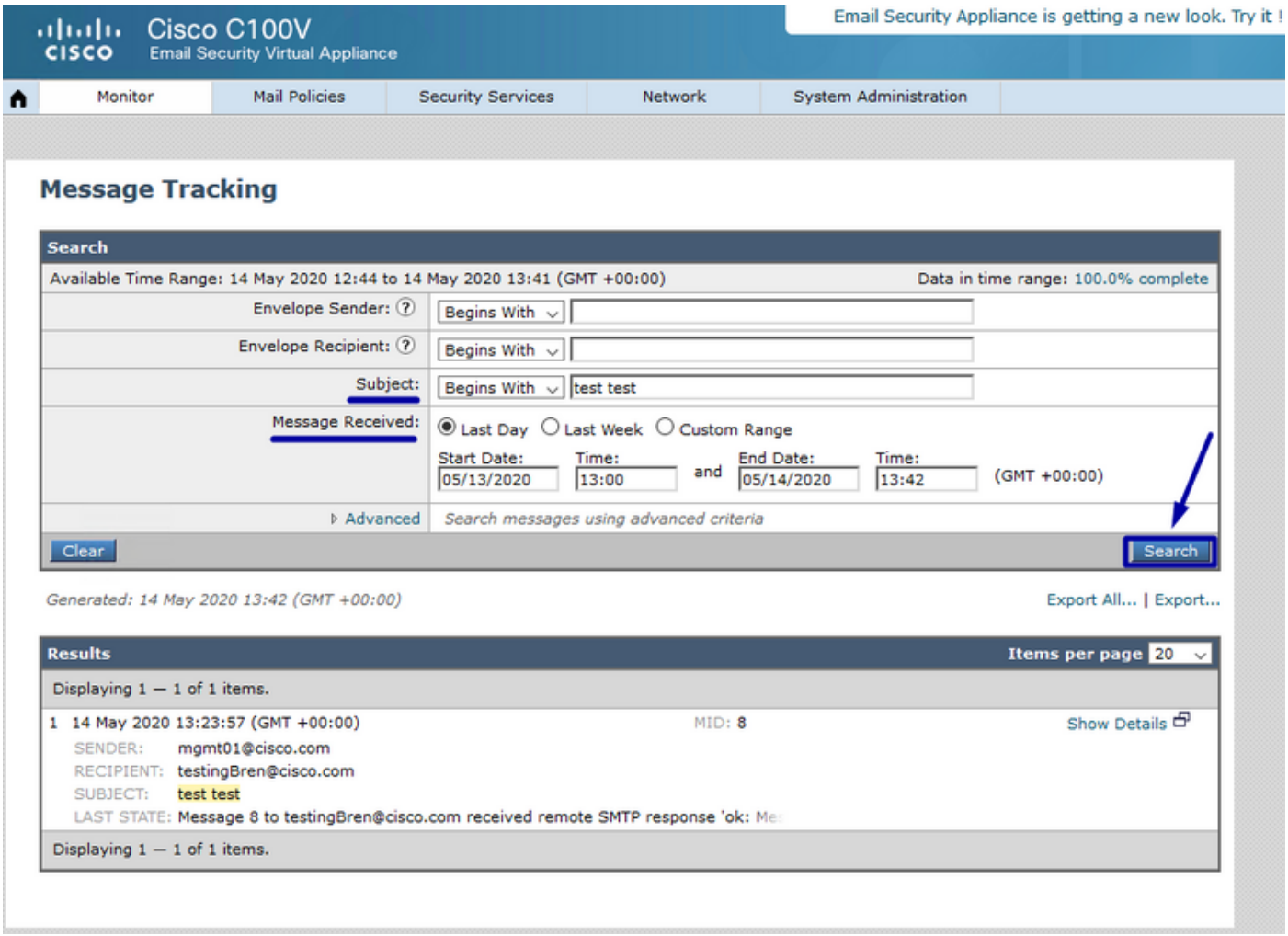


3. — 輸入欄位：模組名稱、已註冊裝置（選擇以前註冊的裝置）、請求時間範圍（天）和儲存，如下圖所示。

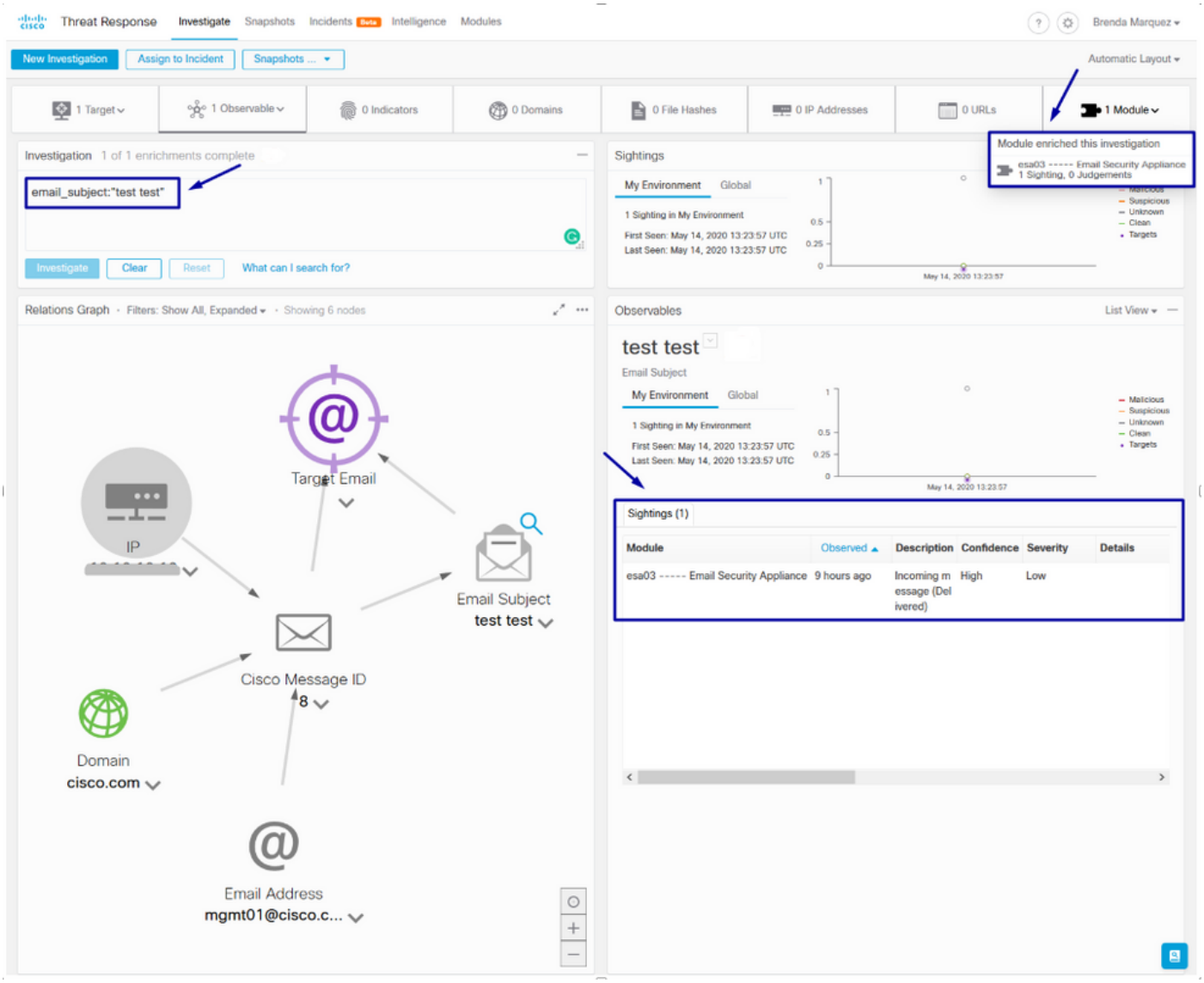


驗證

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。



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。



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"

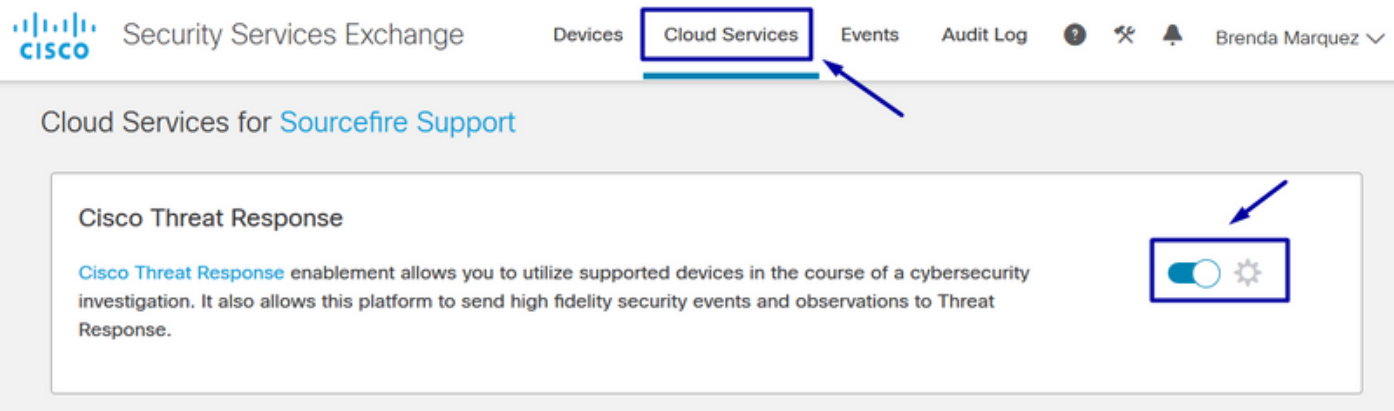
疑難排解

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**