

配置與SecureX的SMA整合

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[SMA整合](#)

[SMA Web](#)

[SMA電子郵件](#)

[驗證](#)

[疑難排解](#)

[SecureX SMA磁貼/SecureX威脅響應SMA模組顯示錯誤「SMA模組上存在意外錯誤」](#)

[影片](#)

[相關資訊](#)

簡介

本文檔介紹了內容安全管理裝置(SMA)與SecureX整合的配置、驗證和故障排除過程。

必要條件

需求

思科建議您瞭解以下主題：

- 安全管理裝置(SMA)
- 電子郵件安全裝置(ESA)
- 網路安全裝置(WSA)
- 思科威脅回應(CTR)
- SecureX控制面板

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行AsyncOS 13.6.2的SMA (用於SMA — 電子郵件模組)
- 運行AsyncOS 12.5的SMA (用於SMA - Web模組)

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

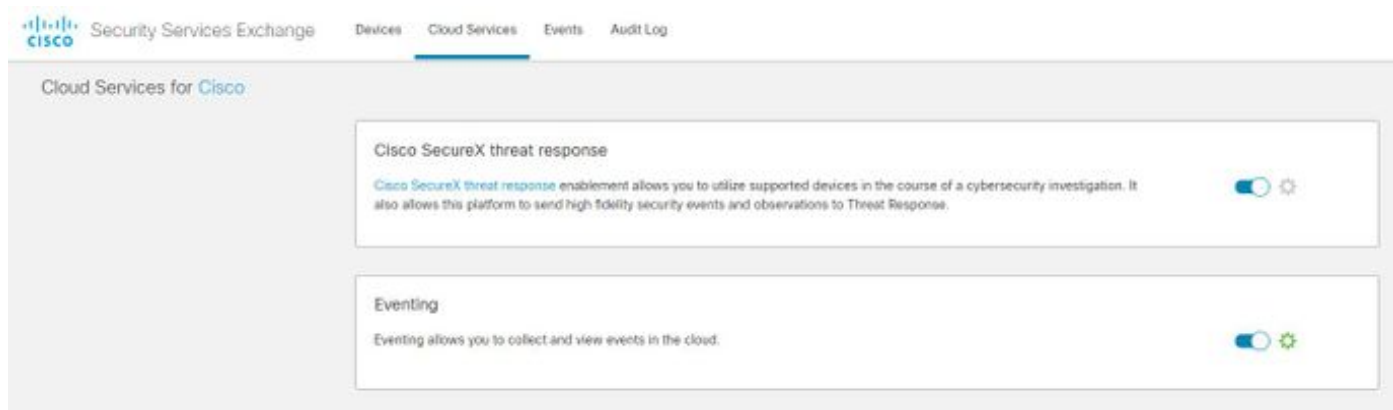
設定

SMA整合

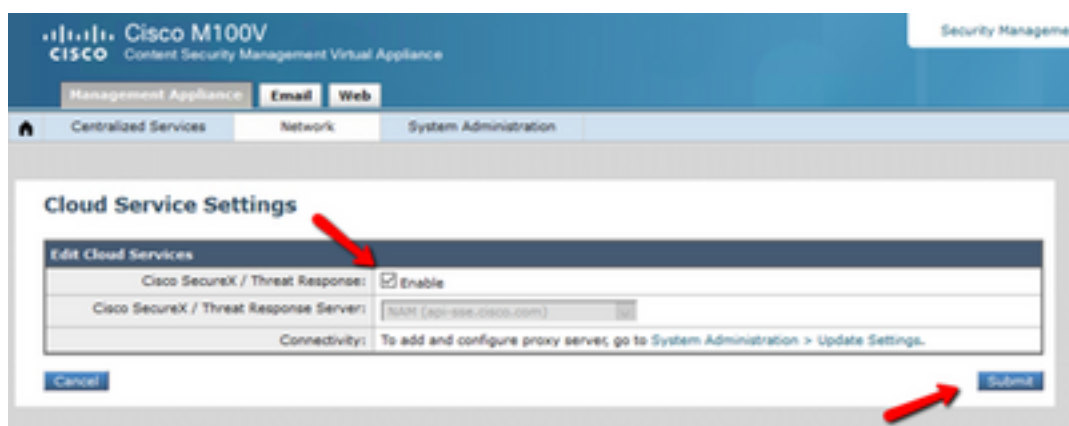
步驟1.在SMA中，導航到**網路>雲服務設定>編輯設定**，啟用整合，並確認SMA已準備好接受註冊令牌。

步驟2.點選Settings圖示（齒輪），然後點選**Devices > Manage Devices**，以轉至Security Services Exchange(SSE)。

確保在**雲服務**下啟用所有選項。



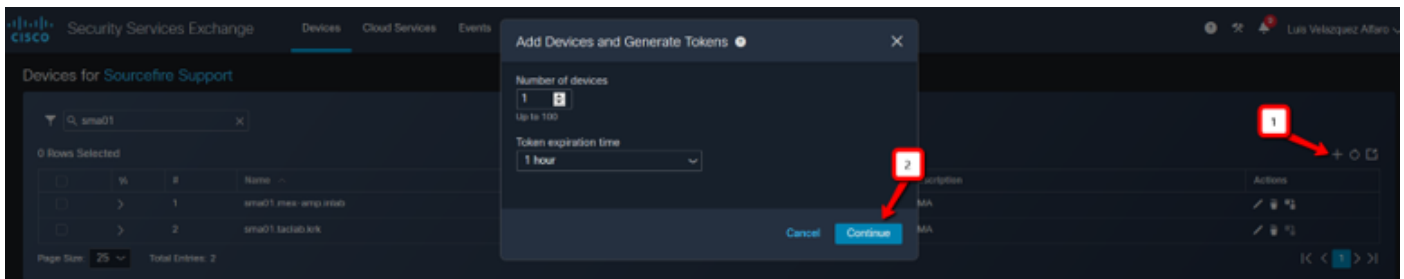
步驟3.在Cloud Services頁籤上啟用思科威脅響應整合，然後點選Devices頁籤並點選+圖示新增新裝置（需要SMA Admin帳戶）。



步驟4.從SecureX例項登入到SSE門戶。

步驟5.從Secure X門戶導航到**Integrations > Devices > Manage devices**

步驟6.在SSE門戶上建立新的令牌並指定令牌過期時間（預設值為1小時），然後按一下**Continue**。



步驟7.複製生成的令牌並確認已建立裝置。

步驟8.導航到您的SMA (網路>雲服務設定) 以插入令牌，然後按一下註冊。

Cloud Service Settings

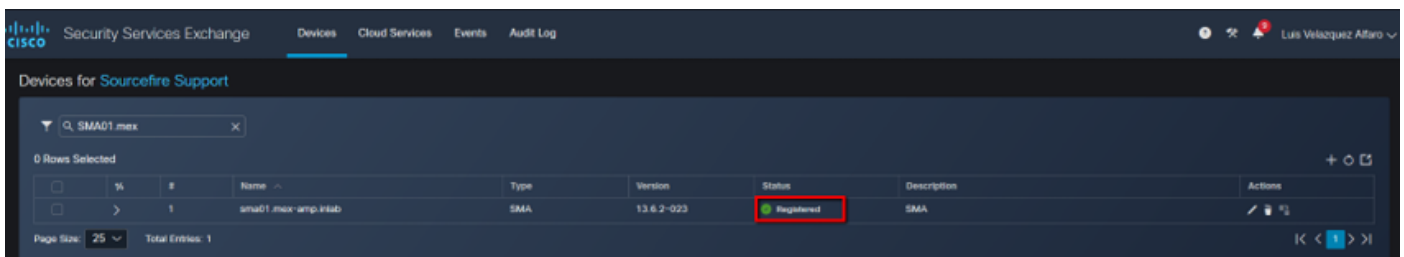
Cloud Services	
Cisco SecureX / Threat Response:	Enabled
Cisco SecureX / Threat Response Server:	NAM (api-sse.cisco.com)
Connectivity:	Proxy Not In Use

[Edit Settings](#)

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

[Register](#)

要確認成功註冊，請檢視Security Services Exchange中的狀態，並確認SMA顯示在「裝置」頁面上。



SMA Web

步驟1.填寫新增新SMA Web模組表格：

- 模組名稱 — 保留預設名稱或輸入對您有意義的名稱。
- Registered Device — 從下拉選單中，選擇您在Security Services Exchange中註冊的裝置。
- 請求時間範圍 (天) — 輸入API終結點查詢的時間範圍 (以天為單位) (預設值為30天)。

步驟2.按一下儲存完成SMA Web模組配置。

SMA電子郵件

步驟1.填寫新增新SMA電子郵件模組表格。

- 模組名稱 — 保留預設名稱或輸入對您有意義的名稱。
- Registered Device — 從下拉選單中，選擇您在Security Services Exchange中註冊的裝置。
- 請求時間範圍 (天) — 輸入API終結點查詢的時間範圍 (以天為單位) (預設值為30天)。

Settings

Your Account

Devices

API Clients

Integrations

Available Integrations

Users

Add New SMA Email Module

Module Name*
SMA Email

Registered Device*
sma01.mex-amp.inlab

sma01.mex-amp.inlab
Type SMA
ID e88cc926-9366-46bd-8285-4b7b1f3c324f
IP Address 127.0.0.1

Request Timeframe (days)
[Input Field]

Save Cancel

Quick Start

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

Required: SMA running AsyncOS 12.0 or later.

Required: AsyncOS 13.6.2 for Cisco Content Security Management Appliances (SMA) is required to use the tiles in the SecureX dashboard.

1. In SMA, navigate to **Network > Cloud Service Settings > Edit Settings**, enable integration and confirm the SMA is ready to accept a registration token.
2. Click the **Settings** icon (gear) and then click **Devices > Manage Devices** to be taken to Security Services Exchange.
3. 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.
4. Specify the token expiration time (the default is 1 hour), and click **Continue**.
5. Copy the generated token and confirm the device has been created.
6. Navigate to your SMA (**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 SMA is displayed on the **Devices** page.
7. Complete the **Add New SMA Email 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).
8. Click **Save** to complete the SMA Email module configuration.

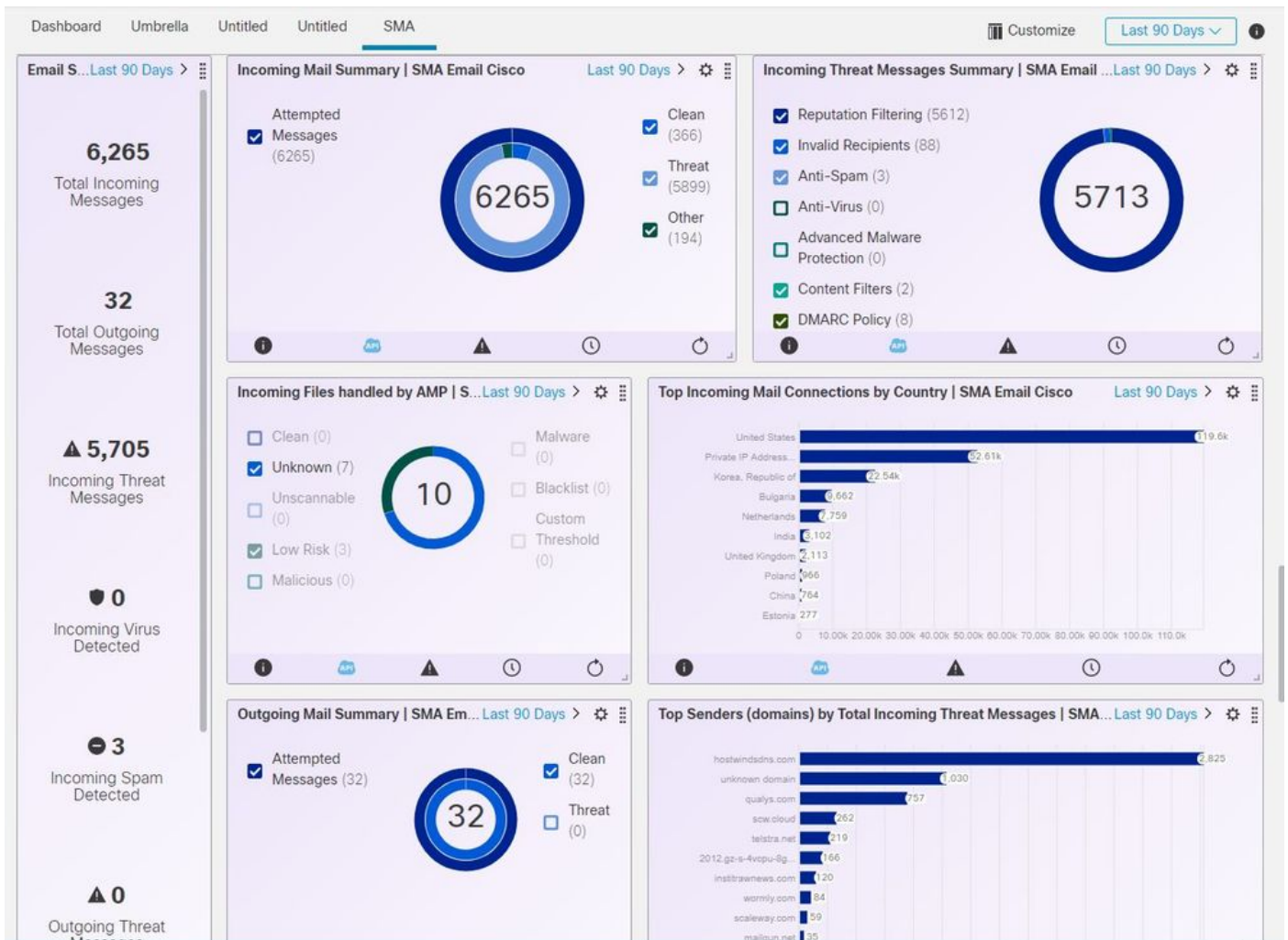
如果SMA裝置名稱不在下拉選單中，請在下拉欄位中鍵入該名稱進行搜尋。

步驟2.按一下**Save**完成SMA電子郵件模組配置

驗證

步驟1.新增新的儀表板並新增磁貼，以檢視您對SMA模組感興趣的資訊

您可以看到裝置資訊反映在本節中。



步驟2. 驗證SMA版本

在SMA上，導航到Home > Version Information。

Cisco M100V
Content Security Management Virtual Appliance

Management Appliance | Email | Web

Centralized Services | Network | System Administration

System Status

Printable PDF

Centralized Services

Email Security

Spam Quarantine	Disk Quota Used: 0.0%	Messages: 0	Not enabled
Policy, Virus and Outbreak Quarantines	Disk Quota Used: 0.0%	Messages: 0	Not enabled
Centralized Reporting	Processing Queue: 0.0%	Status: Not enabled	Email Overview Report
Centralized Message Tracking	Processing Queue: 0.0%	Status: Not enabled	Track Messages

Web Security

Centralized Configuration Manager	Last Publish: N/A	Status: Not enabled	View Appliance Status List
Centralized Reporting	Processing Queue: 0.0%	Status: Not enabled	Web Overview Report

System Information

Uptime	Appliance Up Since: 01 Jul 2020 12:37 (GMT -05:00) (5h 1m 29s)
CPU Utilization	Security Management Appliance: 13.0%
	Quarantine Service: 0.0%
	Reporting Service: 0.0%
	Tracking Service: 0.0%
Total CPU Utilization:	13.0%

Version Information

Model:	M100V
Operating System:	13.6.2-023
Build Date:	26 Jun 2020 00:00 (GMT -05:00)
Install Date:	01 Jul 2020 12:37 (GMT -05:00)
Serial Number:	42140CBACAS34A2DASDB-F960AB6079E1

Hardware

RAID Status:	Unknown
--------------	---------

如果整合後SecureX上沒有可用的資料。您可以執行後續步驟。

步驟1. 驗證ESA/WSA裝置向SMA報告

在SMA上，導航到**Centralized Services > Security Appliances**，並驗證ESA/WSA裝置是否顯示在**Security Appliances**下。

Cisco M100V
Content Security Management Virtual Appliance

Management Appliance | Email | Web

Centralized Services | Network | System Administration

System Status

Security Appliances

Email

- Spam Quarantine: Service disabled
- Policy, Virus and Outbreak Quarantines: Service disabled
- Centralized Reporting: Enabled, using 0 licenses
- Centralized Message Tracking: Enabled, using 0 licenses

Web

- Centralized Configuration Manager: Enabled, using 0 licenses
- Centralized Reporting: Enabled, using 0 licenses
- Centralized Upgrade Manager: Enabled, using 0 licenses
- Centralized Web Configuration Manager: Enabled, using 0 licenses
- Centralized Web Reporting: Enabled, using 0 licenses
- Centralized Upgrades for Web: Service disabled

Security Appliances

Email

[Add Email Appliance...](#)

No appliances have been added.

Web

[Add Web Appliance...](#)

No appliances have been added.

File Analysis

File Analysis Client ID: 06_VLNSMA88625410_42140CEACA934AEDA508-F960AB6079E1_M100V_000000

Key: Selected

Copyright © 2008-2020 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

步驟2. 驗證是否已在 **Centralized Services > Security Appliances** 下許可並啟用了 SMA 許可證，以進行集中電子郵件跟蹤。

Cisco M100V Content Security Management Virtual Appliance

Security Management Appliance is getting...

Management Appliance | Email | Web

Centralized Services | Network | System Administration

Security Appliances

Centralized Service Status	
Spam Quarantine:	Service disabled
Policy, Virus and Outbreak Quarantines:	Service disabled
	Migration configuration need to be completed before enabling Centralized Quarantines service from respective ESAs.
Centralized Email Reporting:	Enabled, using 0 licenses
Centralized Email Message Tracking:	Enabled, using 0 licenses
Centralized Web Configuration Manager:	Enabled, using 0 licenses
Centralized Web Reporting:	Enabled, using 0 licenses
Centralized Upgrades for Web:	Service disabled

Security Appliances

Email

[Add Email Appliance...](#)

No appliances have been added.

Web

[Add Web Appliance...](#)

No appliances have been added.

File Analysis	
File Analysis Client ID:	06_VUNSMAB8625410_42140CEACA934AEDA508-F960AB6079E1_M100V_000000

Key: Selected

Copyright © 2008-2020 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

提示：如果您在執行調查或向SecureX新增磁貼時收到超時錯誤，可能是由於您的裝置傳送的資訊量過大。嘗試降低模組配置中的「請求時間(天)」設定。

SMA SSH控制檯上使用的命令

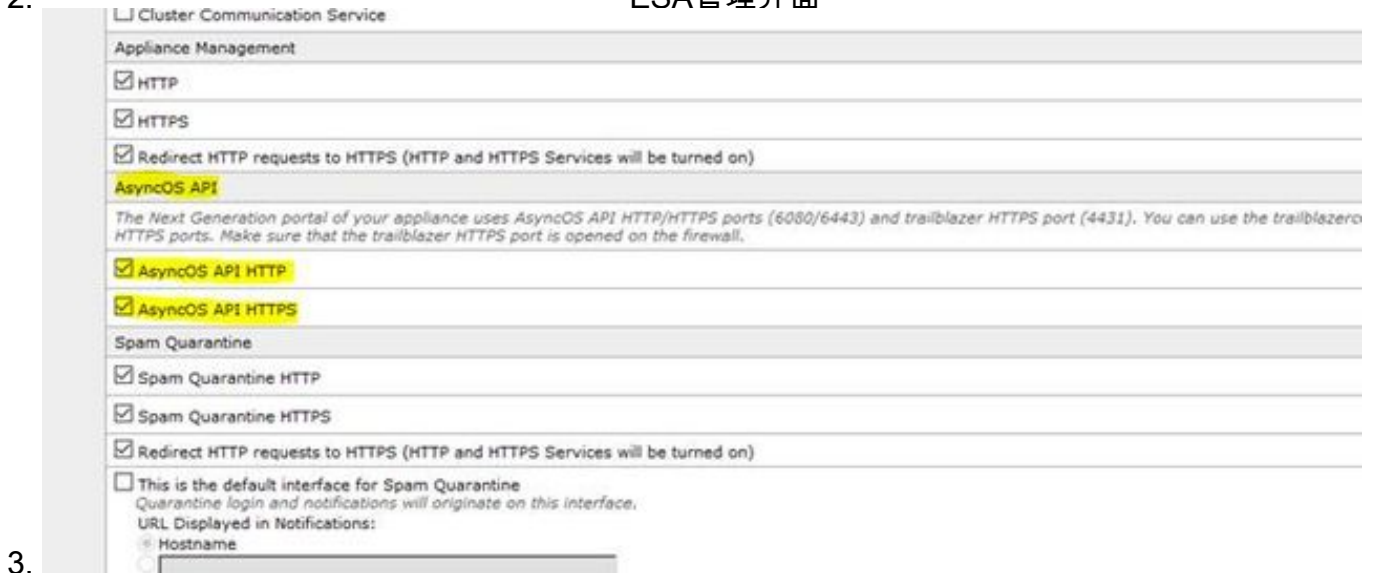
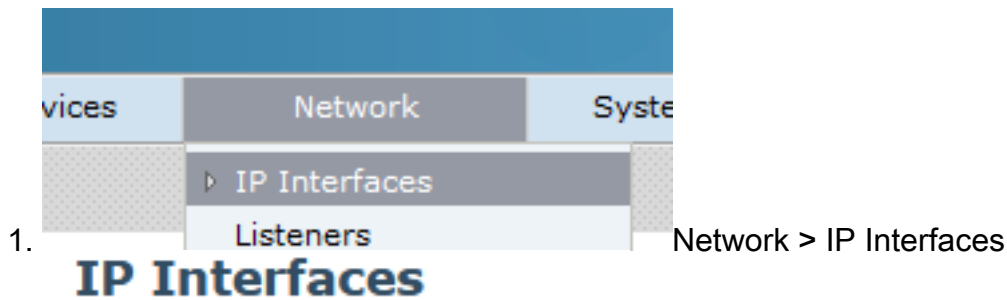
- 要驗證SMA的實際版本和許可證，可以使用以下命令 >Showlicense>版本
- 包含註冊事件的整合日誌 >cat ctr_logs/ctr_logs.current
- SSE門戶連通性測試 >telnet api-sse.cisco.com 443

SecureX SMA磁貼/SecureX威脅響應SMA模組顯示錯誤「SMA模組上存在意外錯誤」

SMA要求通過管理介面啟用AsyncOS API HTTP和HTTPS配置才能與SecureX/CTR門戶通訊。

對於內部SMA，從SMA門戶GUI配置此設定，請轉至**Network > IP Interfaces > Management**

interface > AsyncOS API並啟用HTTP和HTTPS。



非同步API > HTTP和HTTPS

對於CES (基於雲的SMA) ，此配置需要由SMA TAC工程師從後端完成，它將要求訪問受影響的CES的支援隧道。

影片

相關資訊

- 您可以在此處找到有關如何配置產品整合的[影片](#)。
- 如果您的裝置不由SMA管理，則可以單獨為[ESA](#)或[WSA](#)新增模組。
- [技術支援與文件 - Cisco Systems](#)