配置與SecureX的SMA整合

目錄

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。

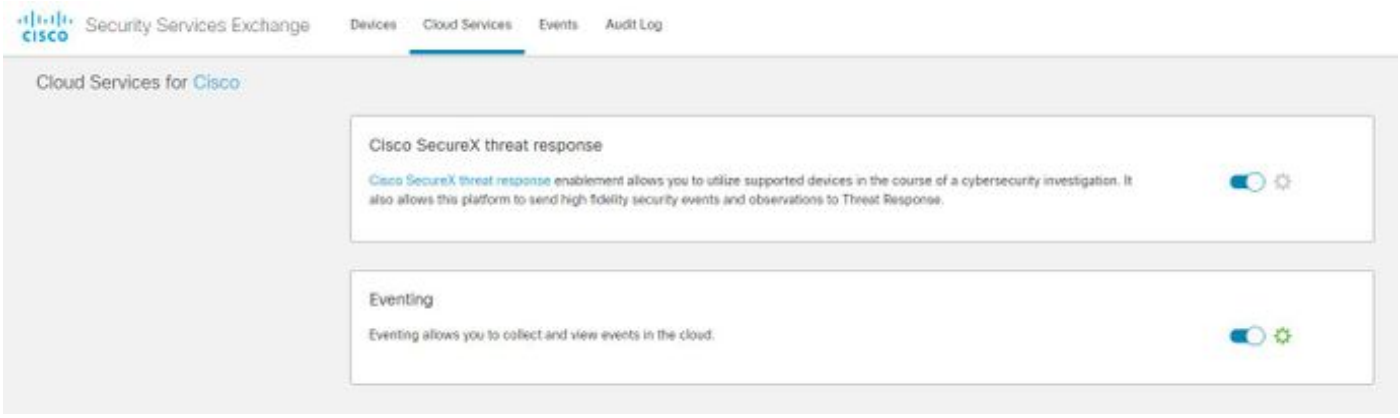
設定

SMA整合

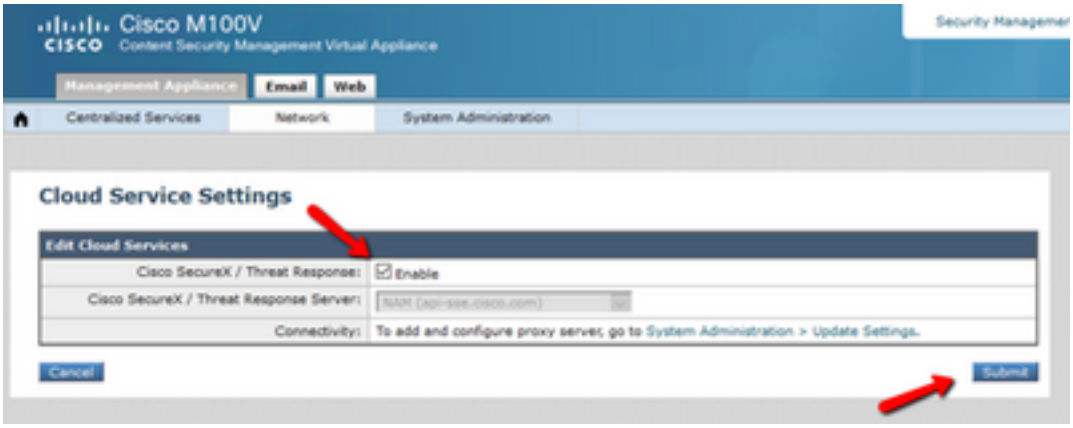
步驟1.在SMA中，導航到**網路>雲服務設定>編輯設定**，啟用整合，並確認SMA已準備好接受註冊令牌。

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。



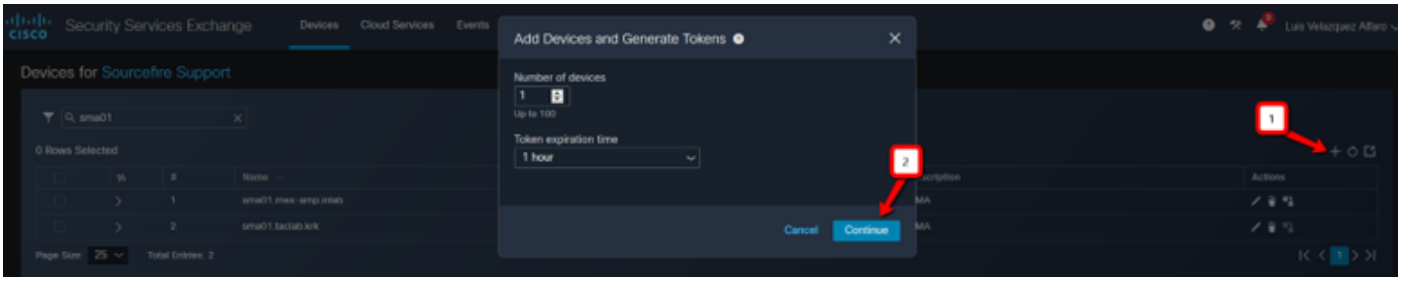
步驟3.在Cloud Services頁籤上啟用思科威脅響應整合，然後點選Devices頁籤並點選+圖示新增新裝置（需要SMA Admin帳戶）。



步驟4.從SecureX例項登入到SSE門戶。

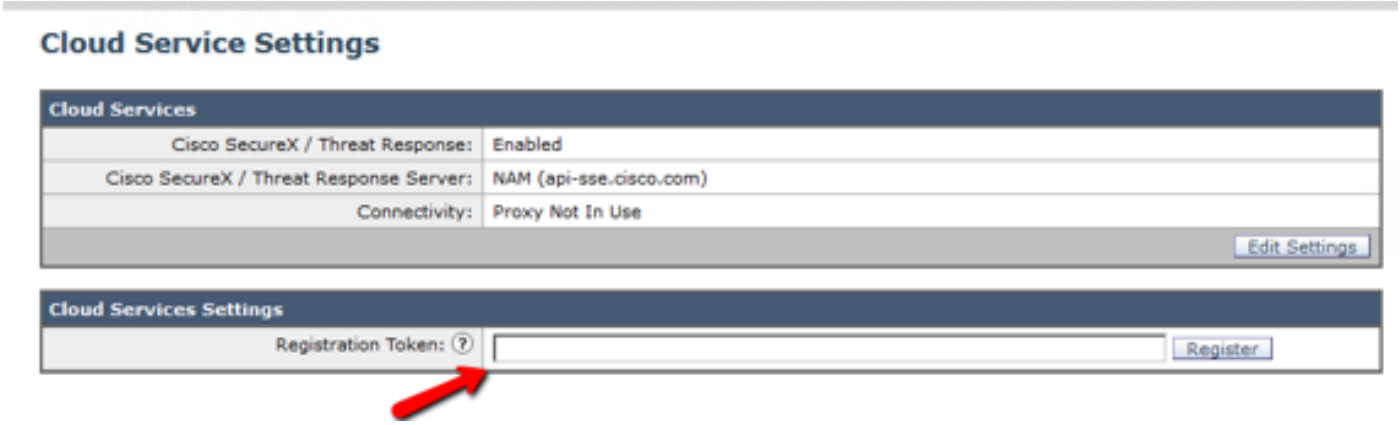
步驟5.從Secure X門戶導航到**Integrations > Devices > Manage devices**

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**。

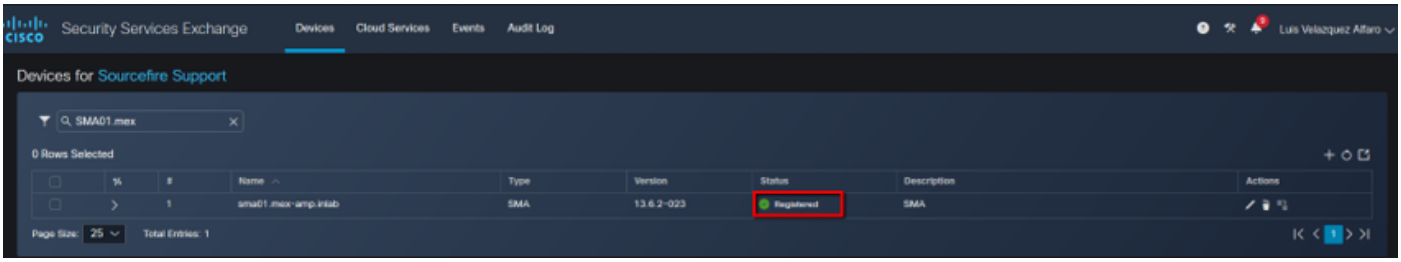


步驟7.複製生成的令牌並確認已建立裝置。

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。



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：

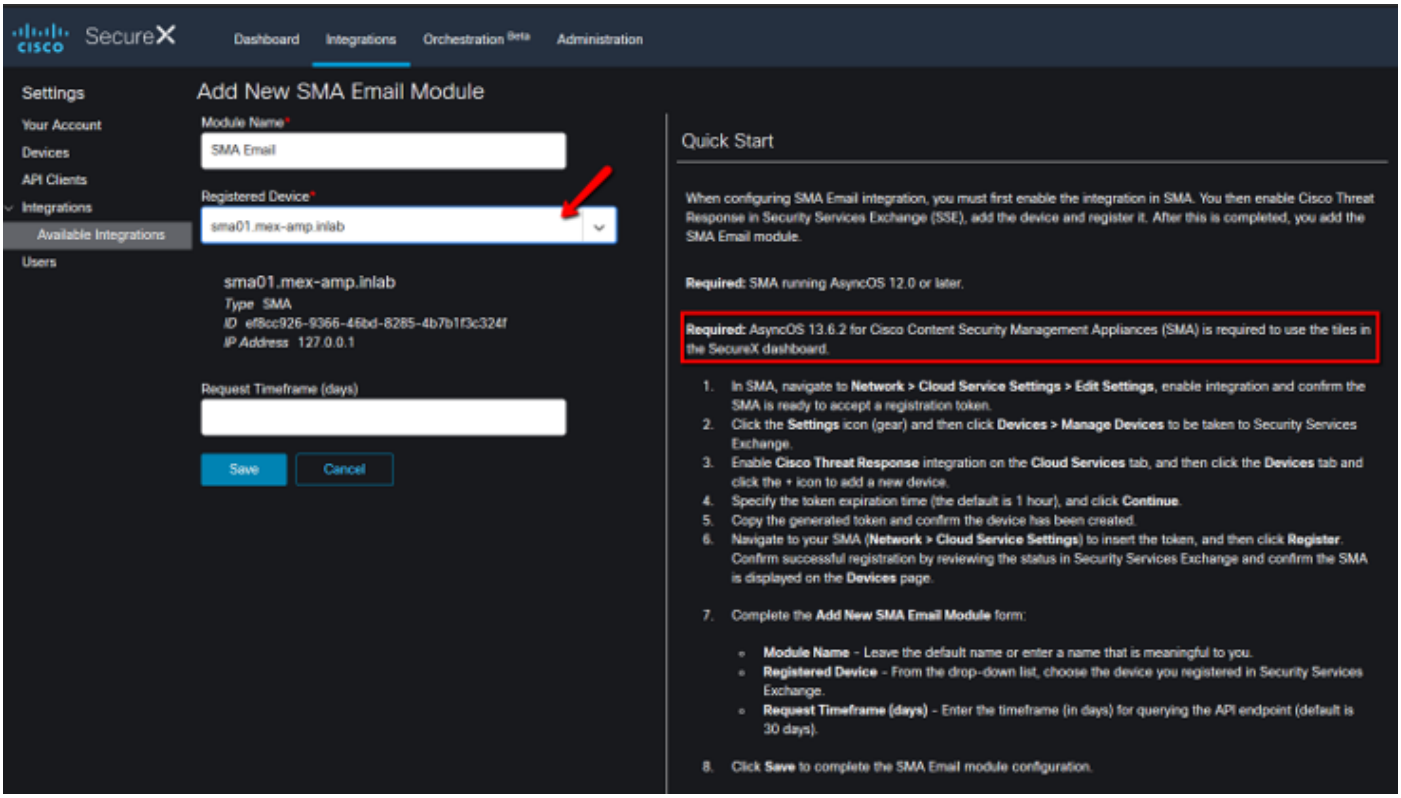
- 模組名稱 — 保留預設名稱或輸入對您有意義的名稱。
- Registered Device — 從下拉選單中，選擇您在Security Services Exchange中註冊的裝置。
- 請求時間範圍（天） — 輸入API終結點查詢的時間範圍（以天為單位）（預設值為30天）。

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）。



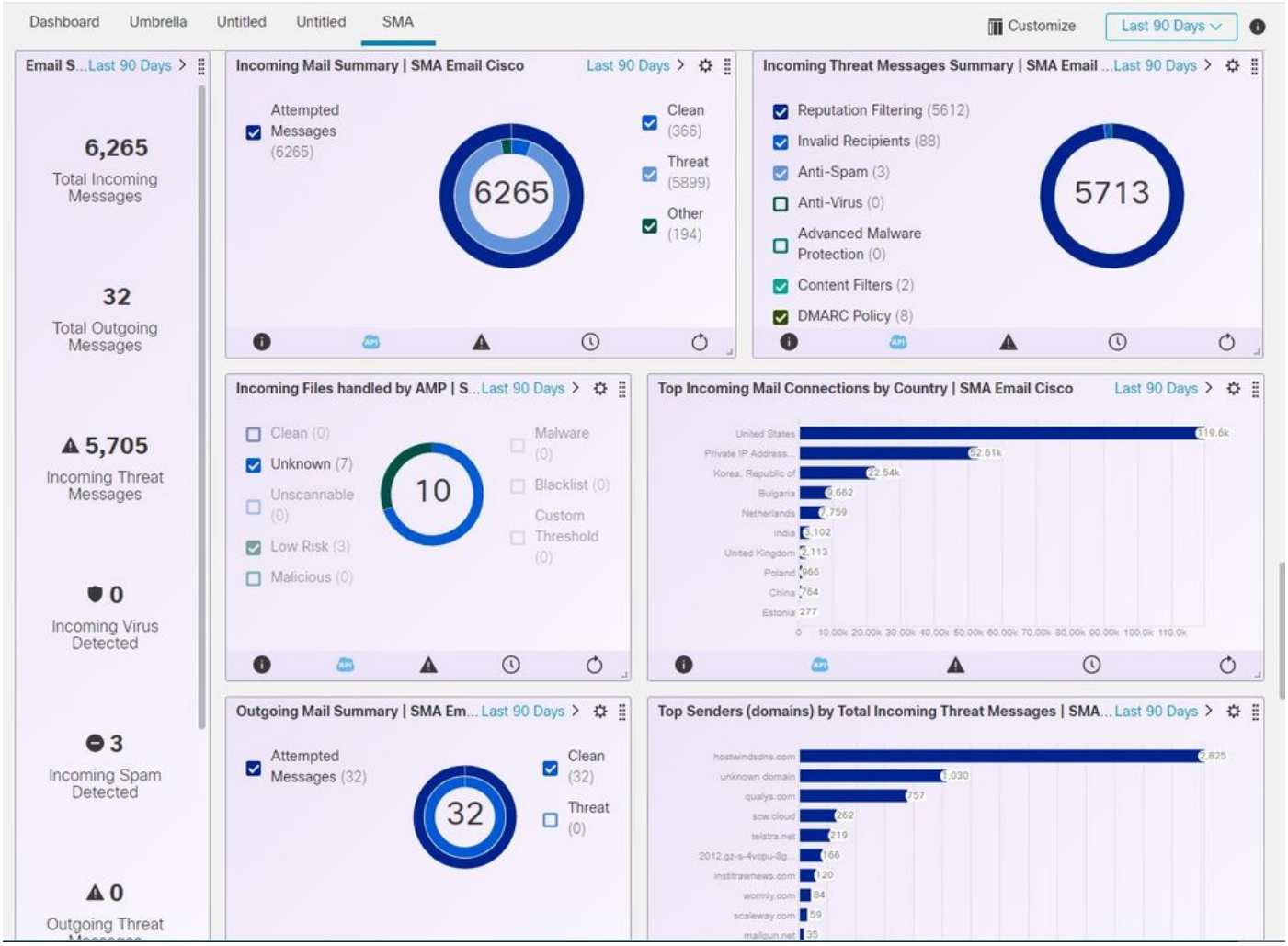
如果SMA裝置名稱不在下拉選單中，請在下拉欄位中鍵入該名稱進行搜尋。

步驟2.按一下**Save**完成SMA電子郵件模組配置

驗證

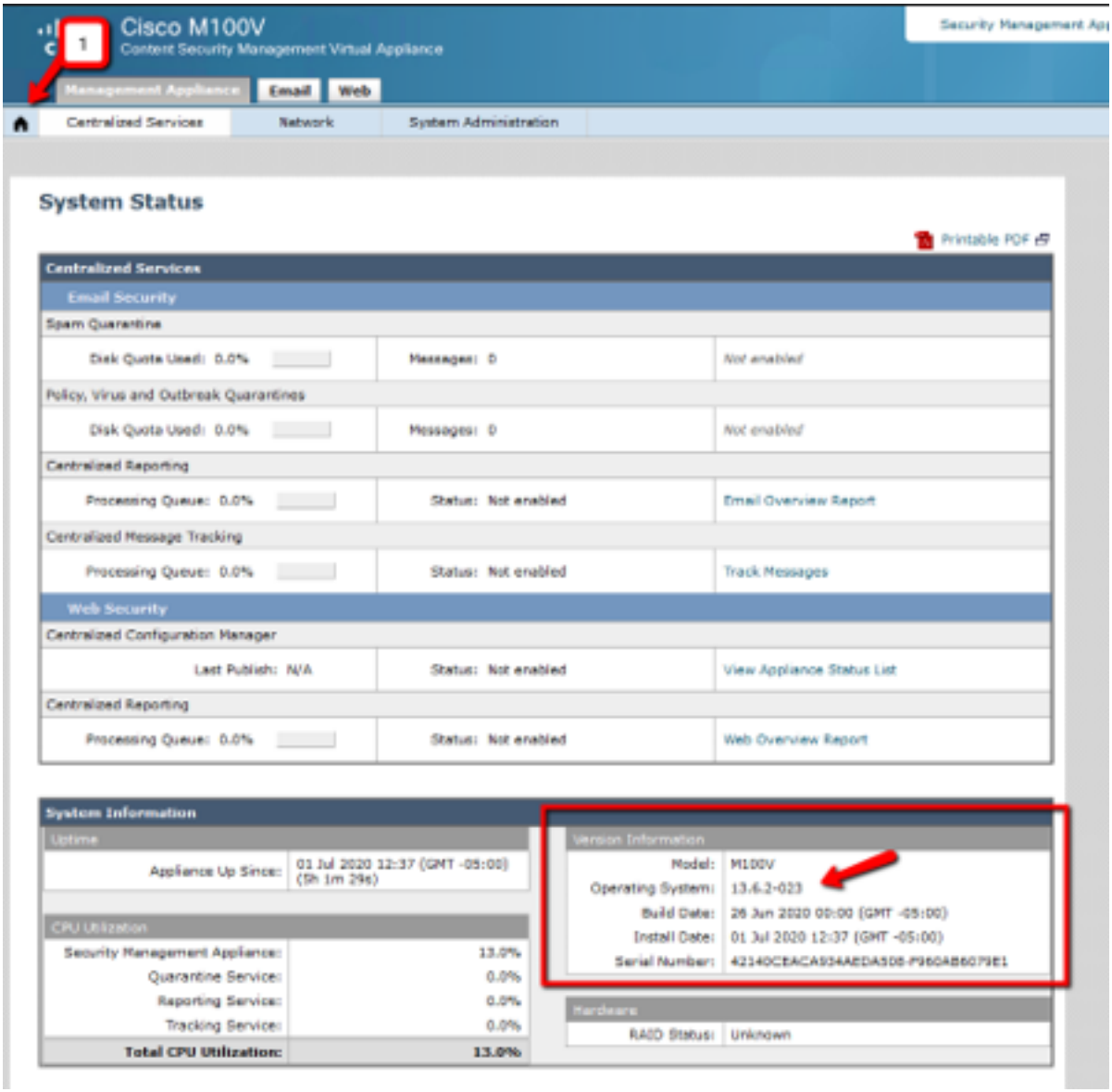
步驟1.新增新的儀表板並新增磁貼，以檢視您對SMA模組感興趣的資訊

您可以看到裝置資訊反映在本節中。



步驟2.驗證SMA版本

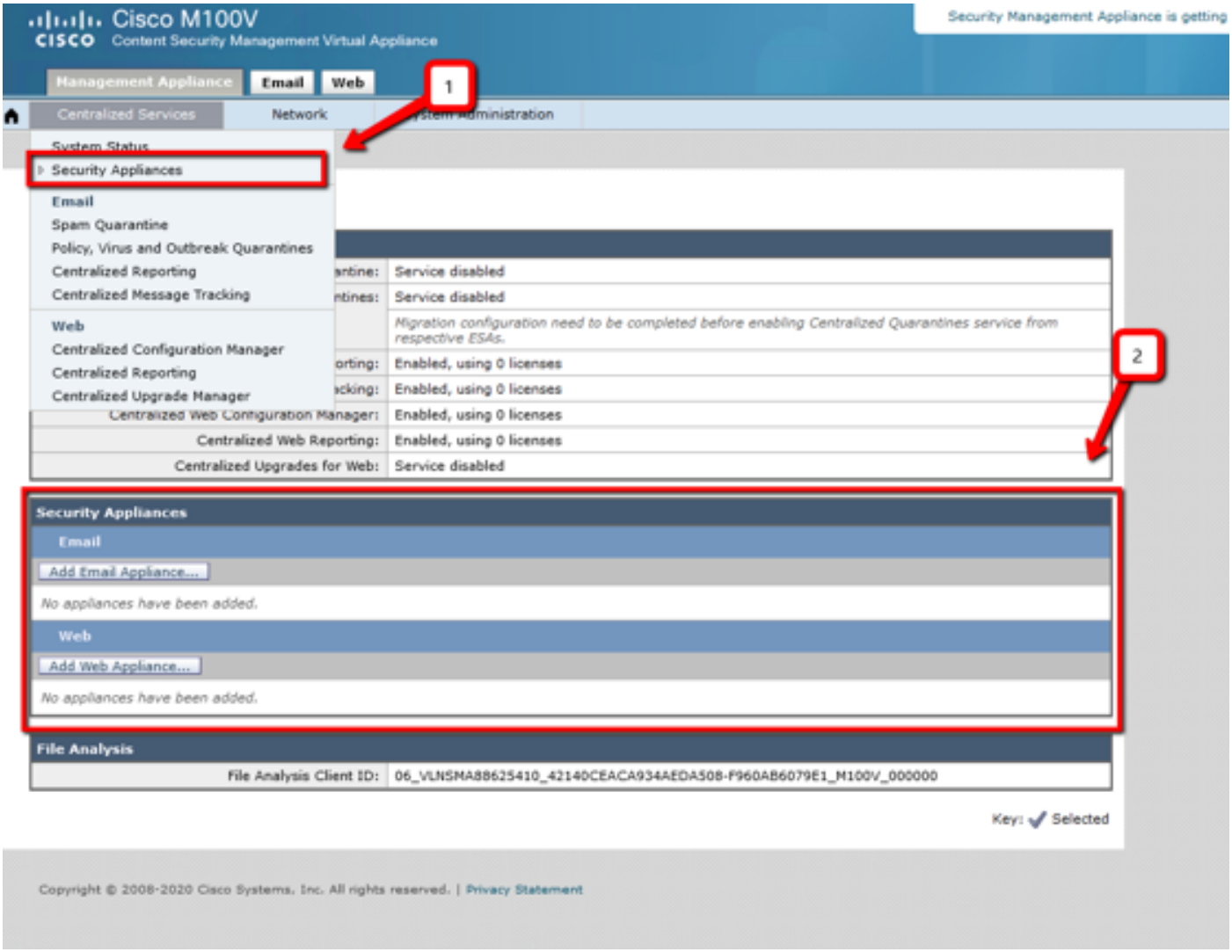
在SMA上，導航到**Home > Version Information**。



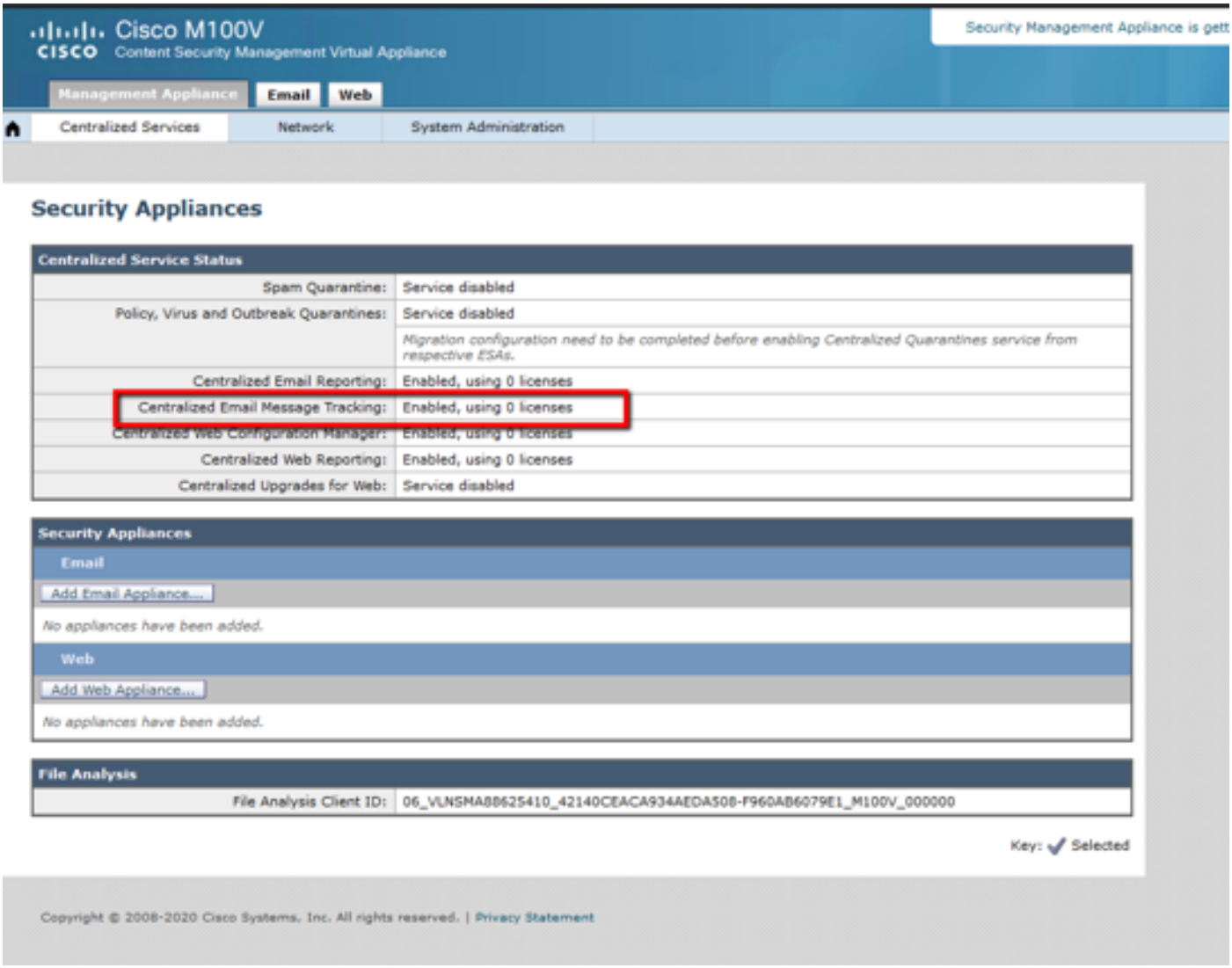
如果整合後SecureX上沒有可用的資料。您可以執行後續步驟。

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。



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。



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

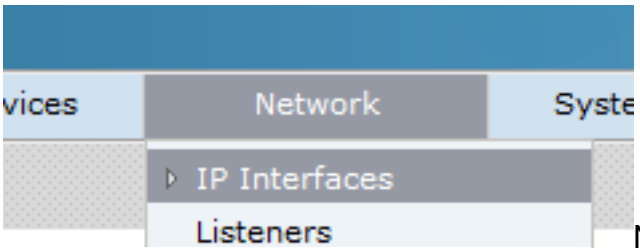
- 要驗證SMA的實際版本和許可證，可以使用以下命令 >Showlicense>版本
- 包含註冊事件的整合日誌 >cat ctr_logs/ctr_logs.current
- SSE門戶連通性測試 >telnet api-sse.cisco.com 443

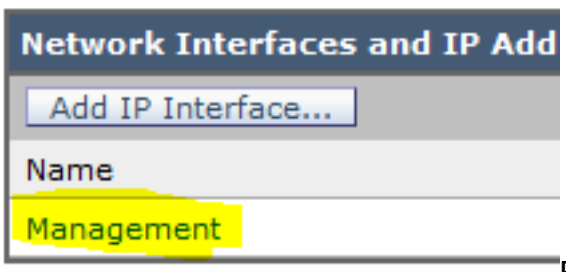
SecureX SMA磁貼/SecureX威脅響應SMA模組顯示錯誤「SMA模組上存在意外錯誤」

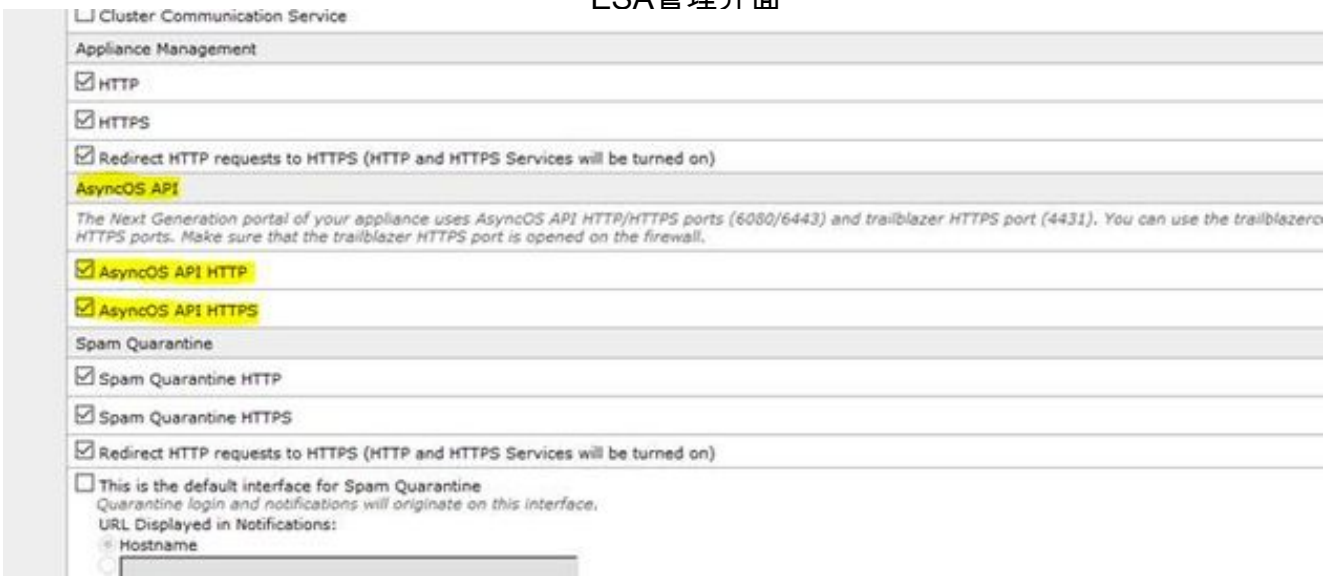
SMA要求通過管理介面啟用AsyncOS API HTTP和HTTPS配置才能與SecureX/CTR門戶通訊。

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。

1. 

Network > IP Interfaces


2. ESA管理介面


3. 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