面向終端的具有高級惡意軟體防護(AMP)的SecureX整合指南

目錄

簡介

Cisco SecureX(AMP)

作者：Yeraldin Sanchez和Uriel Torres，編輯者：Jorge Navarrete，思科TAC工程師。

必要條件

需求

-
- SecureX
-

採用元件

- AMP5.4.20200804
- AMP
- SecureX1.54
- SecureX
- Microsoft Edge84.0.522.52

背景資訊

面向終端的思科高級惡意軟體防護(AMP)是終端安全平台的核心部分，部署為可支援Windows、MacOS、Linux、Android和iOS裝置的檢測和/或響應功能的預防和調查工具，面向終端的AMP模組提供5個磁貼。

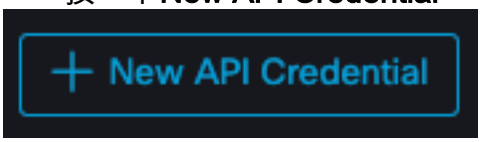
- **AMP檢測到的威脅**：總結由AMP檢測到的危害的一組指標
- **AMP電腦摘要：一組總結AMP電腦狀態的度量**
- **AMP摘要：彙總了AMP檢測和響應的一組指標**
- **AMP隔離區：按時間彙總AMP隔離區的一組指標**
- **AMP檢測到的MITER ATT&CK策略：一組彙總了AMP檢測到的MITER ATT&CK策略的度量**

設定

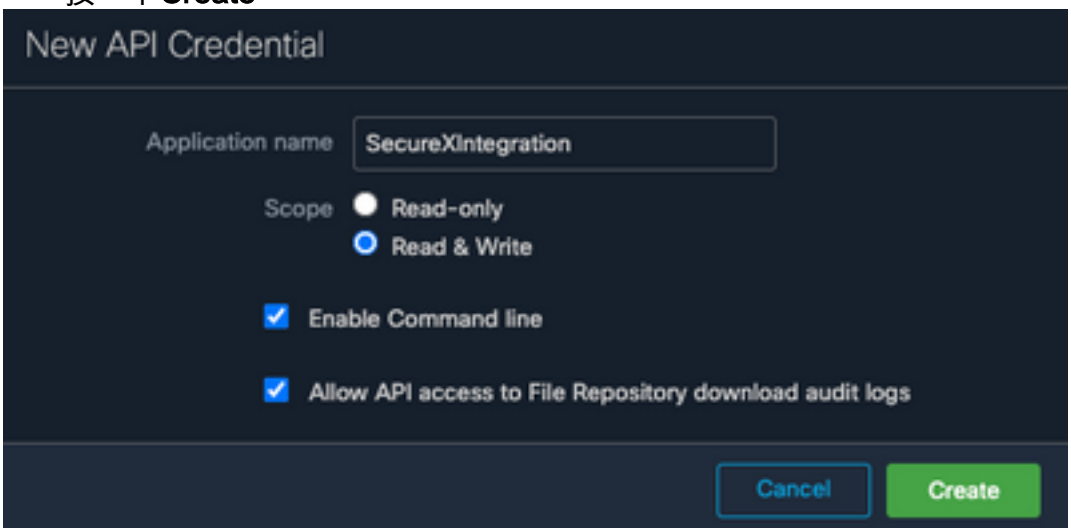
在AMP控制檯中生成API憑據

在AMP控制檯中，建立新的API憑證。

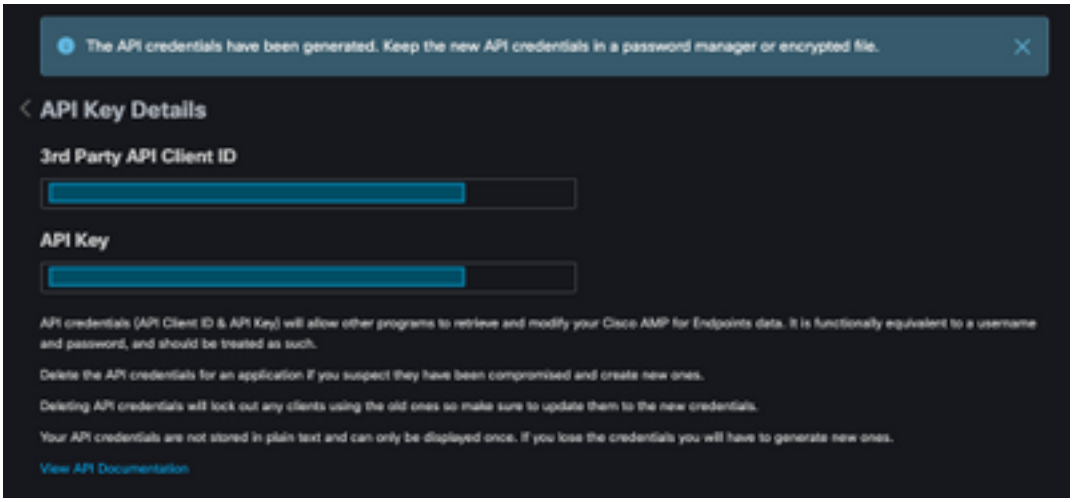
- 以管理員許可權登入到AMP控制檯
- 在AMP控制檯上，導航到**Accounts > API Credentials**
- 按一下**New API Credential**



- 為應用程式命名
- 選擇**讀寫**
- 選中**Enable Command Line** 和**Allow API access to File Repository download audit logs**
- 按一下**Create**



- 生成API憑據

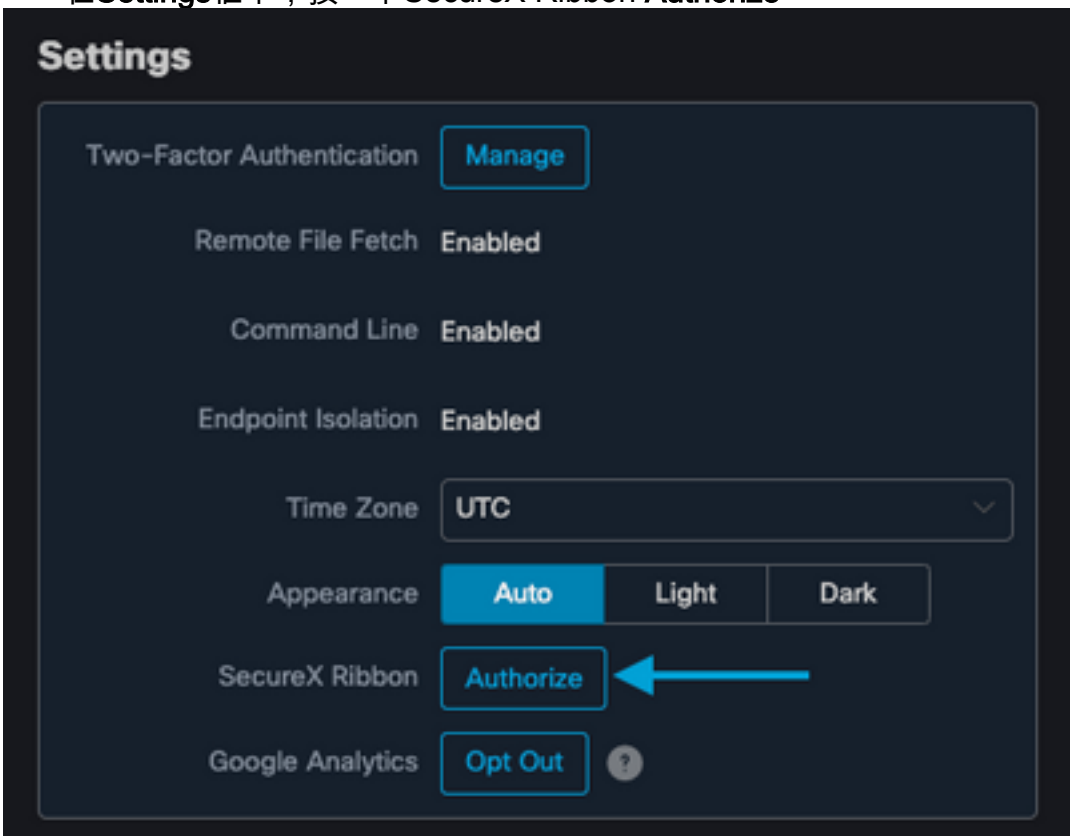


附註：此資訊僅在此視窗中可用，請將憑據儲存在備份檔案中。

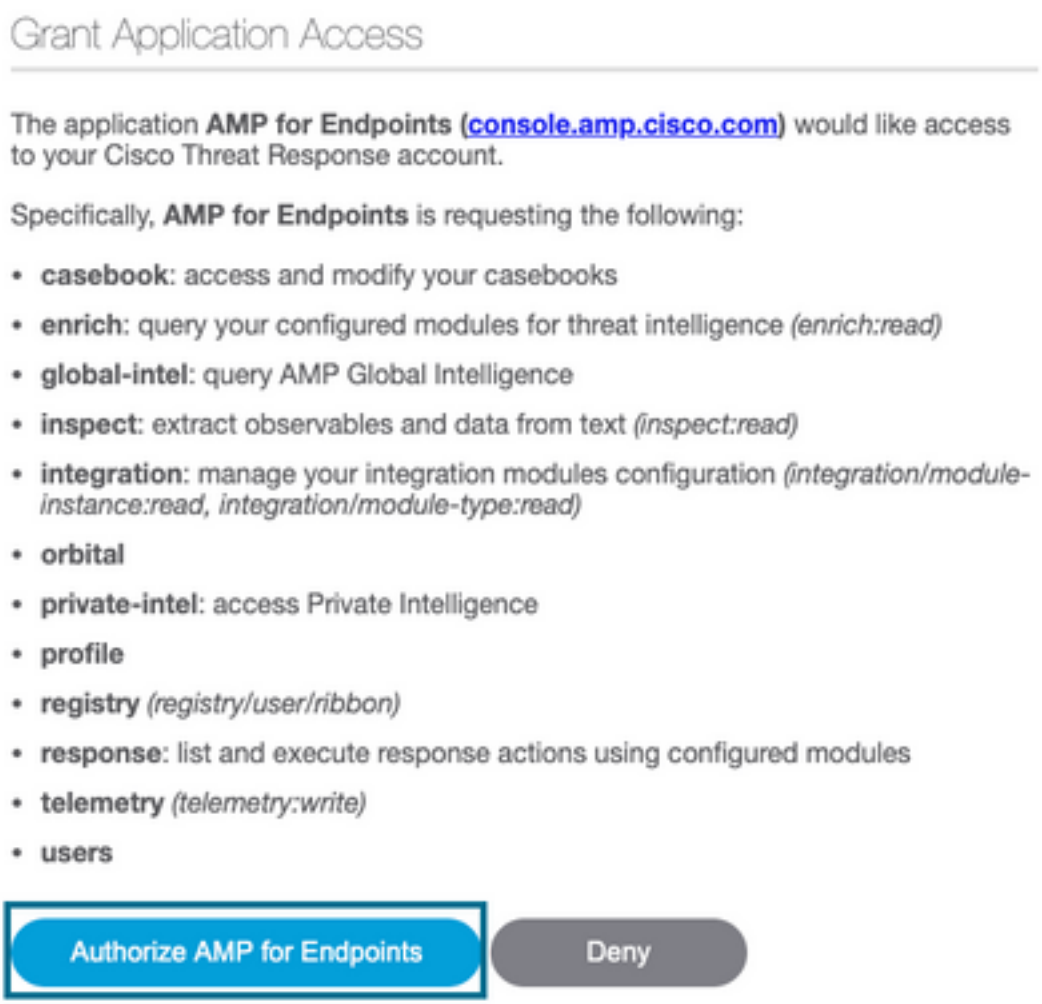
在AMP控制檯中啟用SecureX功能區

SecureX既是集中式控制檯，也是一套分散式功能，可統一可視性、實現自動化、加快事件響應工作流程以及改進威脅搜尋。這些分散式功能在SecureX功能區中以應用程式（應用）和工具的形式顯示，SecureX功能區可以在AMP控制檯中啟用。

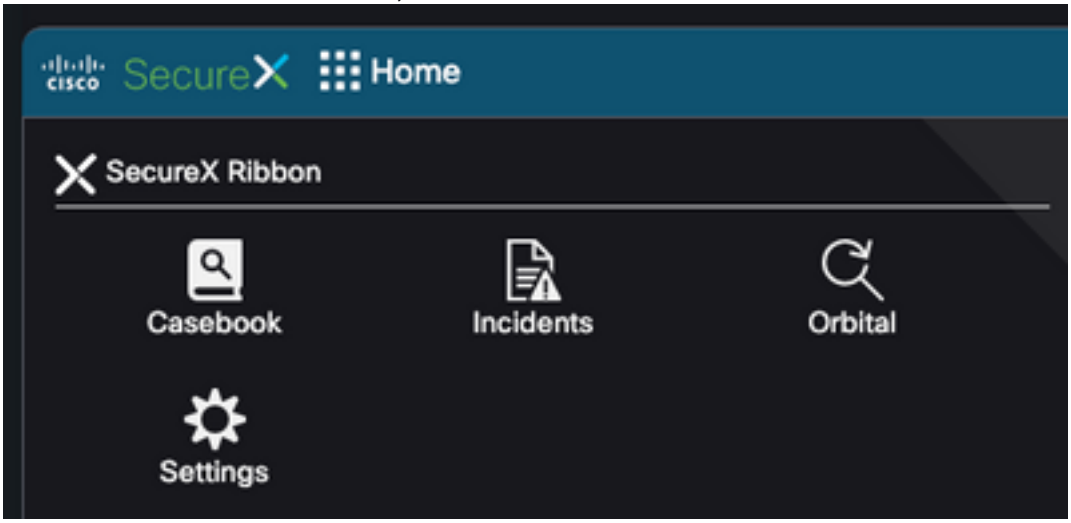
- 登入到SecureX
- 在AMP控制檯上
- 導航到**Accounts > Users >** Click on your **User**
- 在**Settings**框中，按一下SecureX Ribbon **Authorize**



- 系統會將您重定向至SecureX威脅響應
- 按一下「**Authorize AMP for Endpoints**」



- 功能區位於頁面的下部，在控制面板和環境中其他安全產品之間移動時仍繼續存在

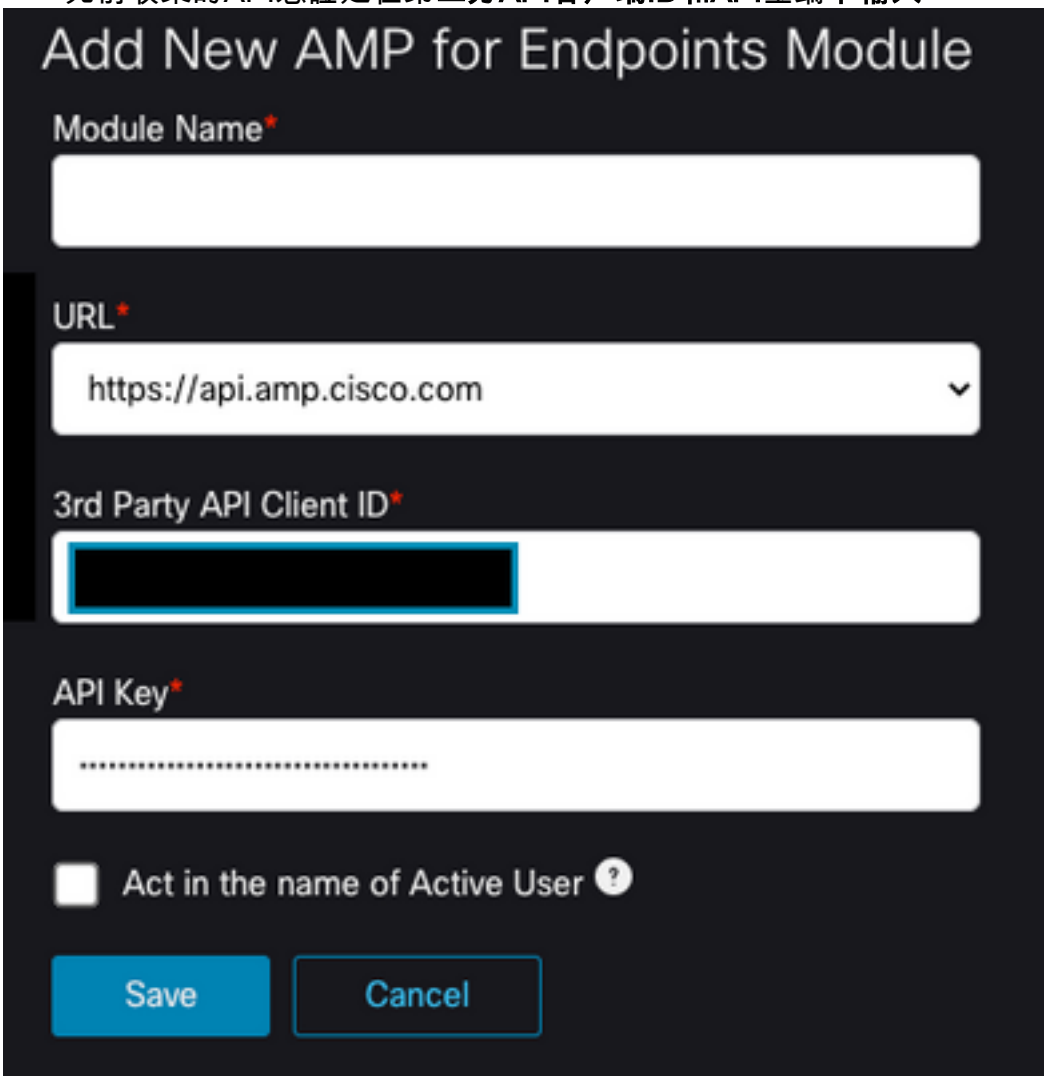


在SecureX中整合面向終端的AMP模組

面向終端的AMP模組允許您從跨安全產品的整合中調查和識別多個具有上下文資訊的檔案。它提供了有關受影響的終端和裝置的詳細資訊，包括IP地址、作業系統和AMP GUID。

- 在SecureX控制檯上，導航到**Integrations > Click Add New Module**
- 選擇**AMP for Endpoints**模組，然後按一下**Add New Module**
- 為模組命名
- 選擇AMP雲

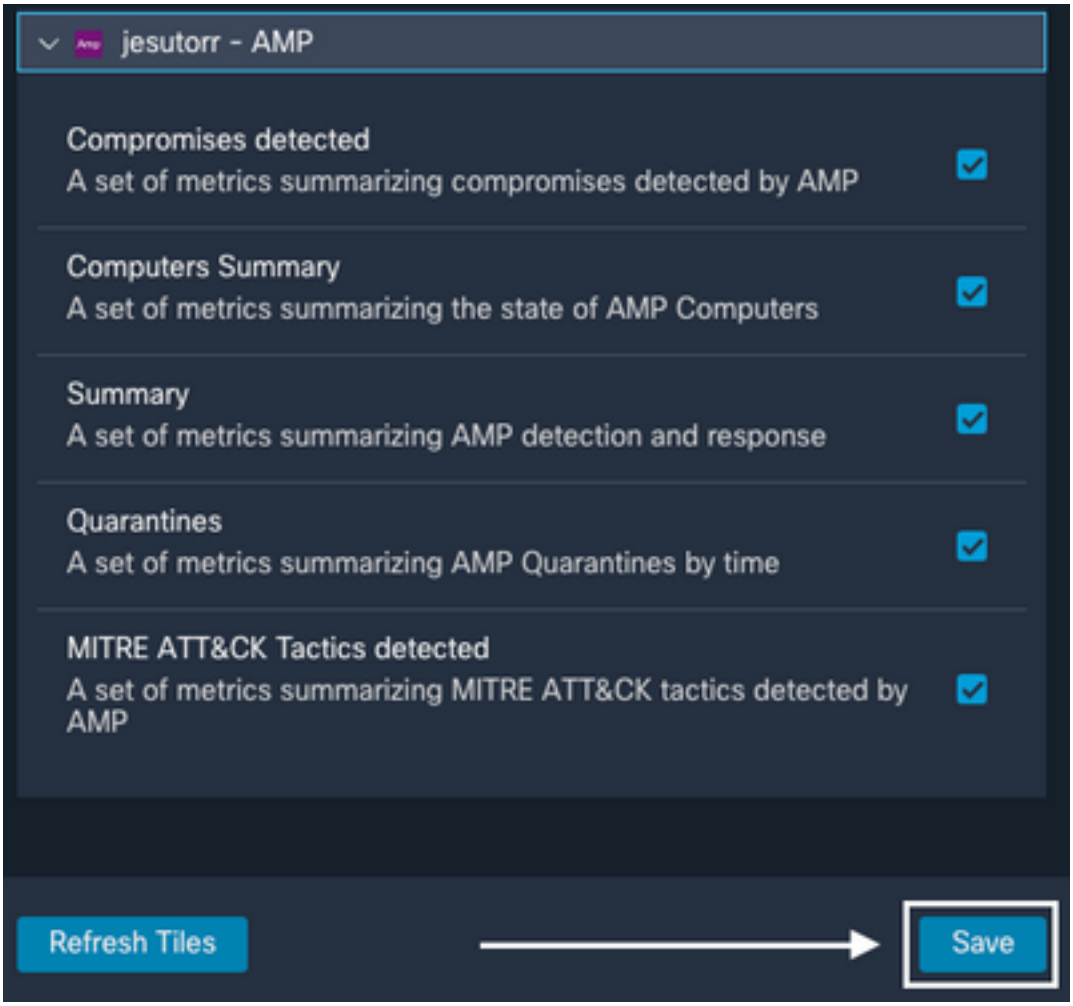
- 先前收集的API憑證是在第**三方API客戶端ID和API金鑰下輸入**



驗證

驗證AMP控制檯中的資訊是否顯示在SecureX控制面板中。

- 在SecureX上導航到控制**面板**
- 按一下**New Dashboard**並為其命名
- 選擇以前生成的AMP模組
- 選擇磁貼，對於本指南，所有磁貼均已新增
- 按一下**「Save」**



- 選擇**Timeframe**，並驗證來自AMP的資料是否顯示在SecureX中

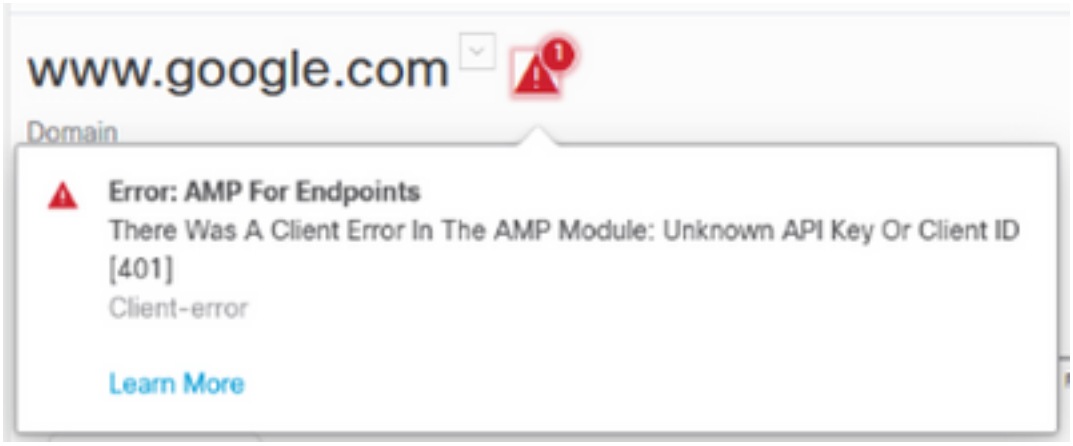
疑難排解

API客戶端沒有寫訪問許可權[403]

SecureX — 面向終端的AMP整合需要面向終端的**讀寫**AMP API，如果不需要，則會顯示錯誤消息，如下圖所示。

錯誤：未知API金鑰或客戶端ID [401]

如果在SecureX威脅響應中執行調查（如圖所示），則API無效。



驗證API憑證是否有效或者是否存在AMP控制檯中，如果不存在，請嘗試使用新憑證。

如果您檢視上述資訊後仍有問題，請聯絡支援人員。

影片指南