SecureX with Orbital高級搜尋整合指南

目錄

簡介

Cisco SecureXCisco Orbital Advanced Search

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

必要條件

需求

- AMP
-
- SecureX
-

採用元件

- AMP5.4.20200804
- AMP
- 1.7
- SecureX1.54
- SecureX
- Microsoft Edge84.0.522.52

背景資訊

Orbital是面向終端的思科AMP的高級功能，旨在簡化安全調查和威脅搜尋。它在您的每個AMP終端上提供強大的Osquery技術的實施。Orbital允許您建立自定義查詢，以便在整個網路中查詢感興趣的資訊，但它也隨附了超過一百個預裝查詢，允許您對任何或所有端點快速運行複雜查詢。

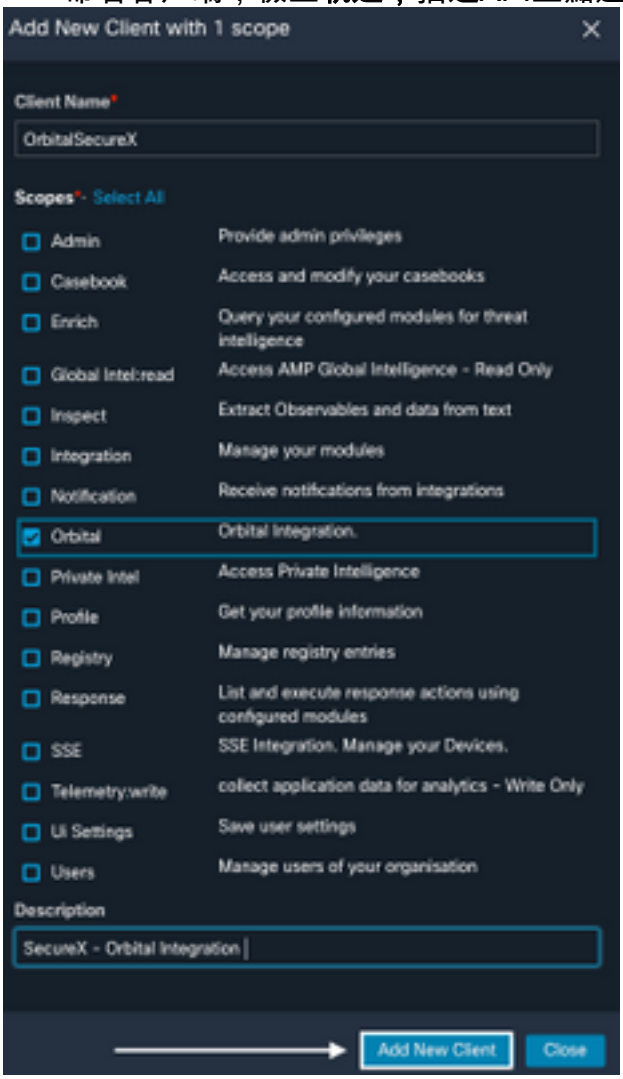
Orbital模組有4個磁貼，您可以將其新增到SecureX儀表板。

- **組織查詢和結果統計**：描述組織查詢和結果的一組度量
- **使用者目錄統計**：描述此使用者最常用目錄查詢的一組度量
- **組織目錄統計**：描述此組織最常用的目錄查詢的一組度量
- **使用者查詢和結果統計**：描述使用者查詢和結果的一組度量

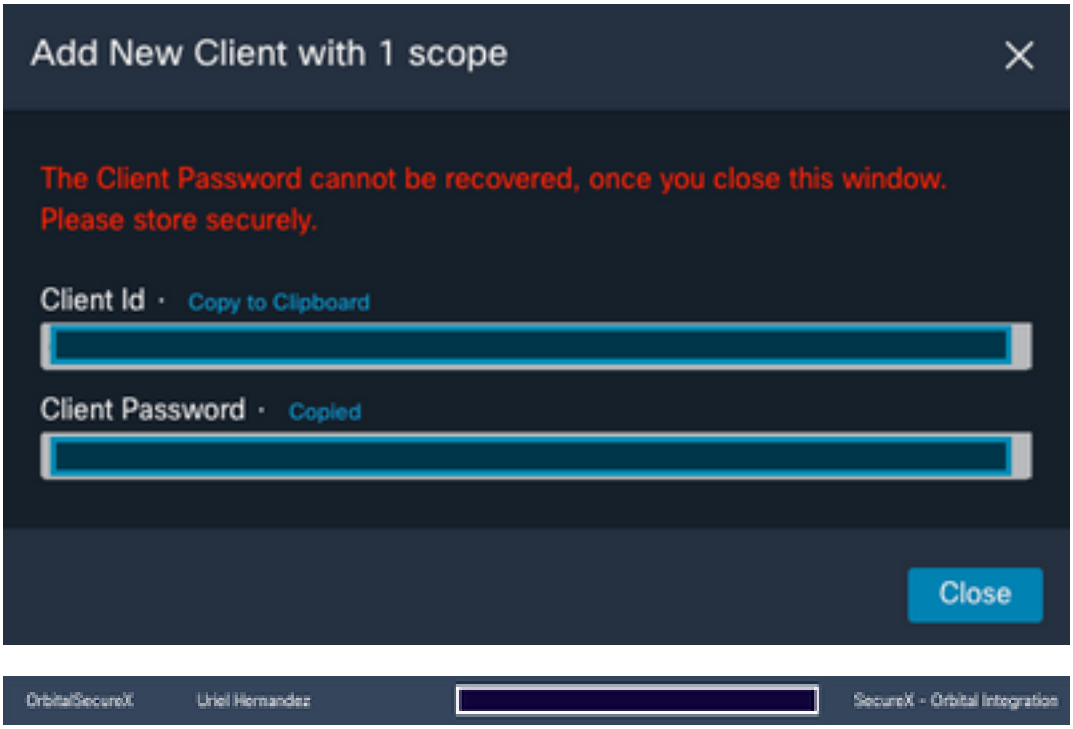
設定

在SecureX控制檯中生成API憑據

- 登入到SecureX
- 導覽至**Integrations > Settings > API Clients**
- 按一下**Generate API Client**
- 命名客戶端，檢查**軌道，**描述API並點選**新增新客戶端**



- 生成API憑據



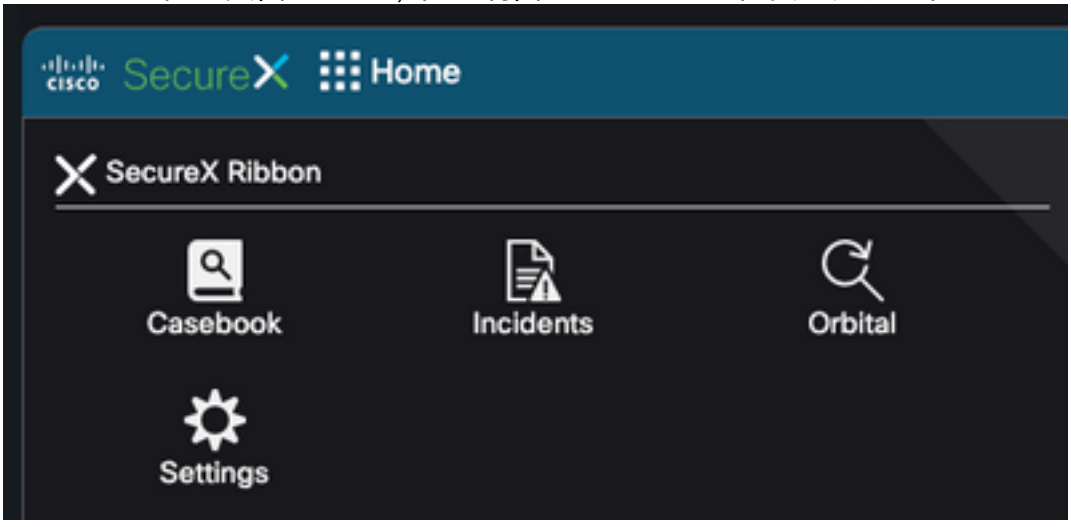
附註：此資訊僅在此視窗中可用，請將憑據儲存在備份檔案中。

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 Ribbon中以應用程式（應用）和工具的形式出現，SecureX Ribbon可以在軌道控制檯中啟用。

- 登入到Orbital Console
- 論軌道控制檯
- 導覽至**<Yout User> > Settings**
- 啟用SecureX功能區

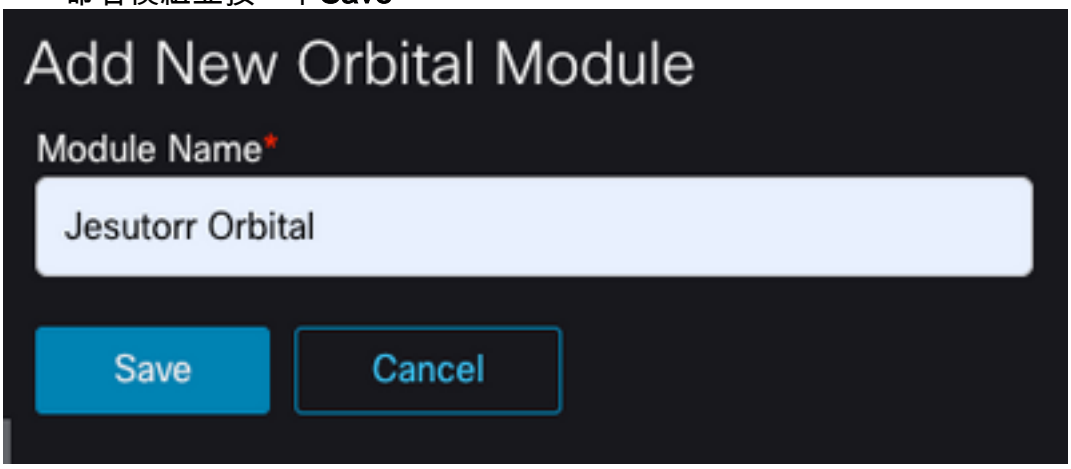
- 功能區位於頁面的下部，在控制面板和環境中其他安全產品之間移動時仍繼續存在



在SecureX中整合軌道模組

Orbital可以豐富威脅響應關係圖中的資訊，如果您進入Orbital查詢並收集有關主機、IP、IP4、IP6、MAC和作業系統等的其他情報。Orbital應用程式在SecureX功能區上可用，允許您運行即時查詢。您還可以在右窗格中檢視度量和最近的查詢。

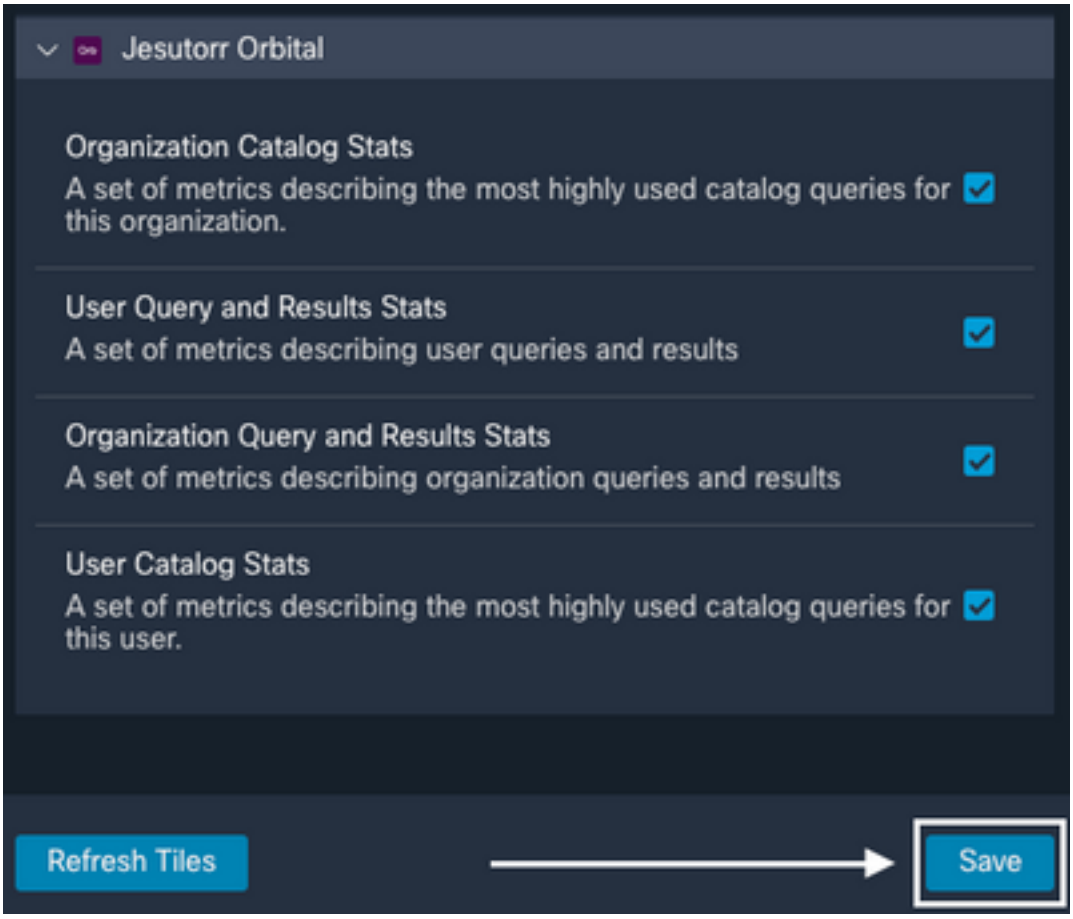
- 在SecureX上
- 導覽至**Integrations > Add New Module**
- 選擇Orbital並按一下**Add New Module**
- 命名模組並按一下**Save**



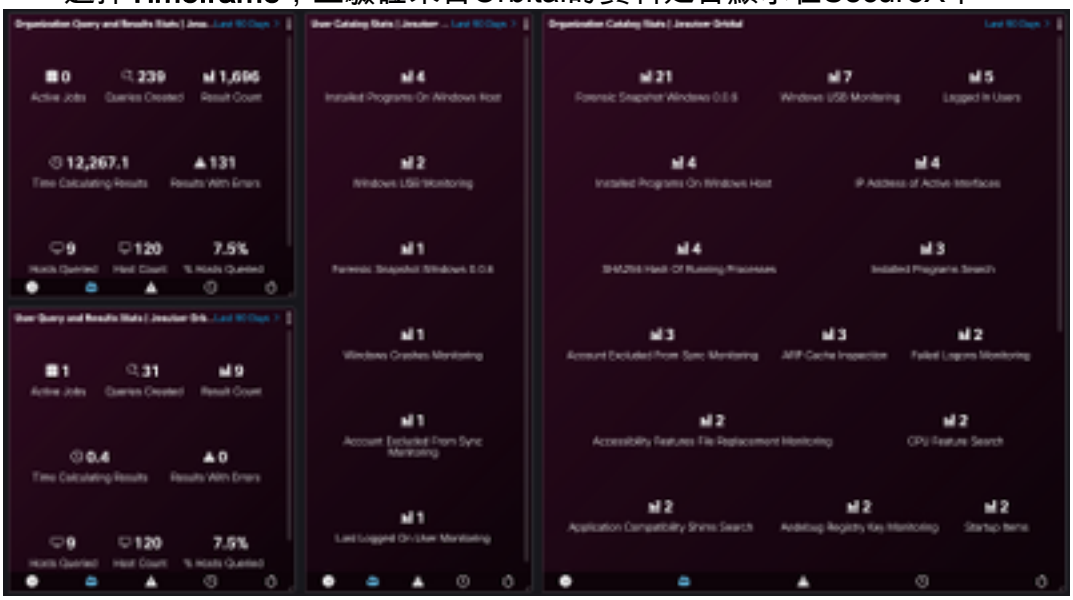
驗證

驗證Orbital Advanced Se控制檯中的資訊是否顯示在SecureX控制面板中。

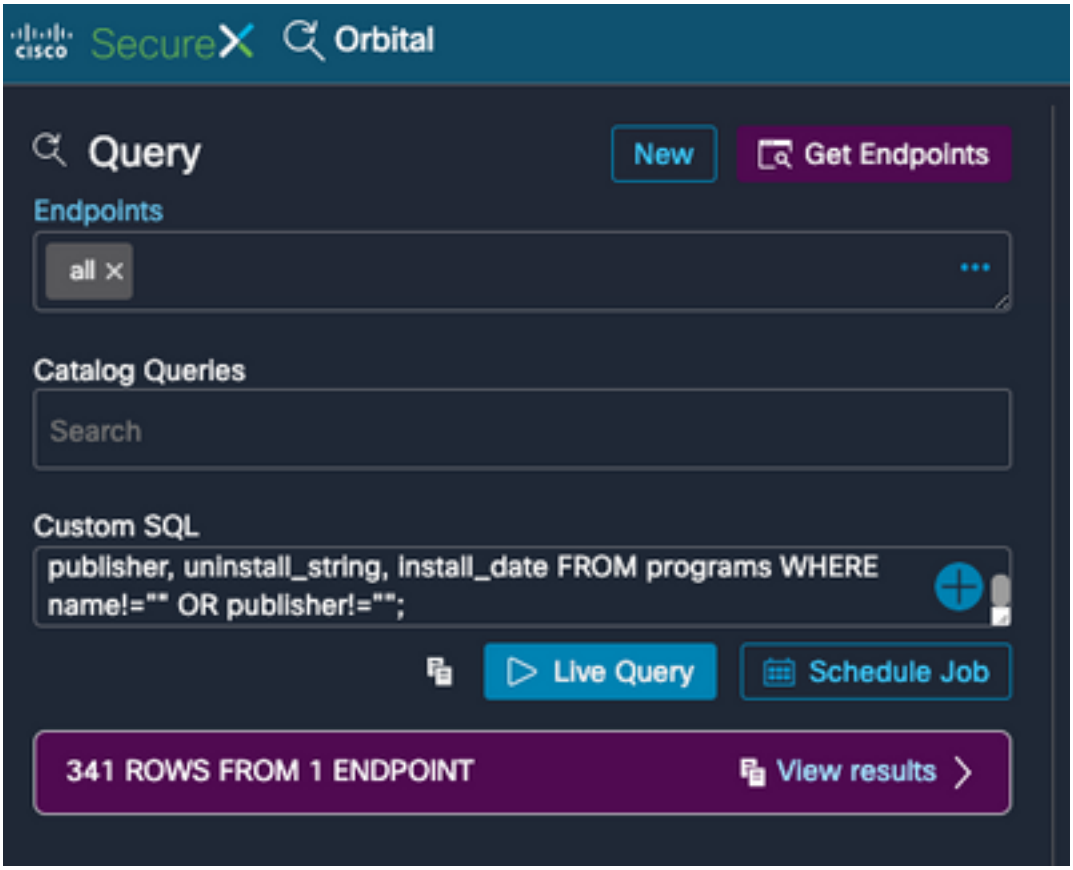
- 在SecureX上導航到控制**面板**
- 按一下**New Dashboard**並將其命名
- 選擇以前生成的軌道模組
- 選擇磁貼，對於本指南，所有磁貼均已新增
- 按一下**「Save」**



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



- 可以從SecureX功能區啟動調查
- 導覽至**SecureXRibbon > Orbital >** 執行軌道查詢



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。
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。