為TETRA下載配置自定義時間

目錄

簡介

本文檔介紹如何配置本地終端以在任何所需時間下載TETRA更新，以滿足頻寬使用要求。

背景資訊

TETRA是安全終端的離線引擎，它使用防病毒簽名為終端提供保護。TETRA每天都會收到對其特徵資料庫的更新，以便及時應對各種新的威脅。這些更新在大型環境中可能會使用大量頻寬，因此，每個端點都會在預設設定為1小時的更新間隔內隨機選擇下載時間。 即使在TETRA策略上可以選擇不同的更新間隔，也不能選擇特定時間觸發此下載過程。本文檔提供解決方法，以強制TETRA使用Windows計畫作業更新其AV簽名。

必要條件

需求

安全終端策略配置和Windows計畫作業的基本知識。

採用元件

- 安全終端雲端主控台
- 適用於Windows 8.1.3的安全終端聯結器
- Windows 10企業版

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

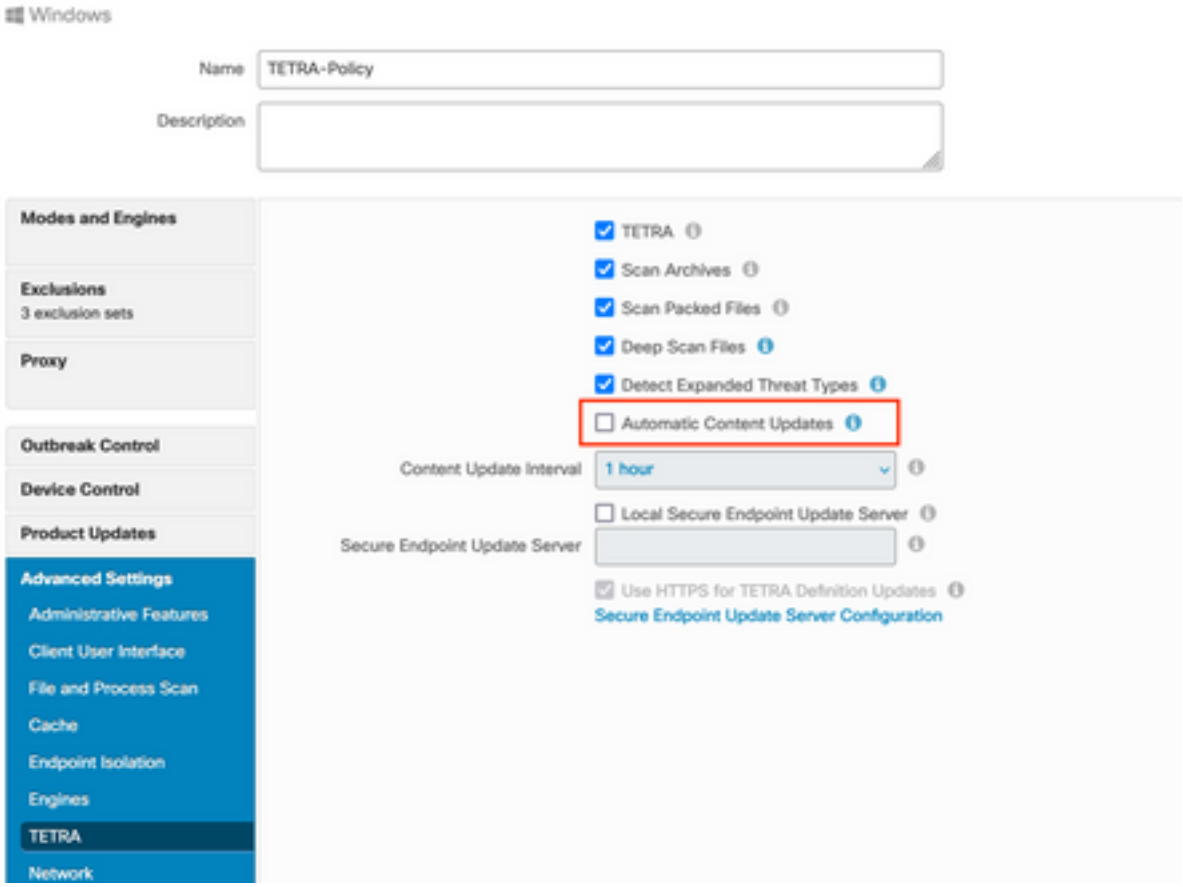
> **警告**：如背景部分所述，TETRA更新可能會佔用大量頻寬。預設情況下，安全端點會嘗試減少此影響，並在預設情況下設定為1小時的更新間隔內隨機化TETRA更新。建議不要強制所有

聯結器同時更新定義，特別是在大型環境中。只有在控制更新時間非常關鍵的特殊情況下，才能使用此過程。在任何其它情況下，最好是自動更新。

選擇要為自定義TETRA下載時間配置的安全終端策略。

注意：請注意，此配置是在策略基礎上完成的，此策略中的所有終端都會受到影響。因此，建議您將要控制的用於自定義TETRA更新的所有裝置放在同一個安全終結點策略上。

登入到安全端點管理控制檯並導航到**管理 > 策略**，然後搜尋已選擇使用的策略，然後按一下**編輯**。進入策略配置頁面後，導航到**TETRA Section**。在此部分下，取消選中**Automatic Content Updates**覈取方塊並**儲存**該策略。這與安全終結點雲控制檯上的配置相關。

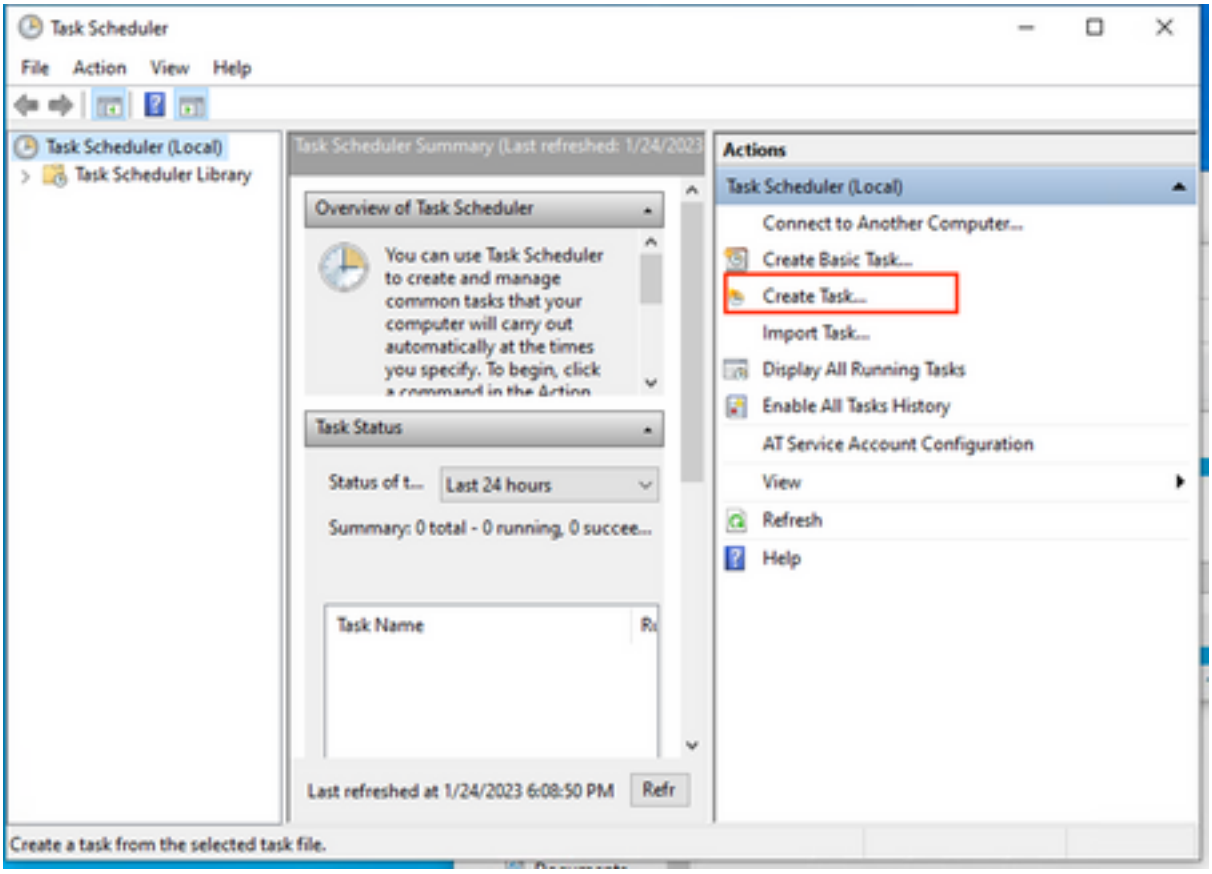


在下一個配置條目中，訪問您的Windows裝置並開啟一個新的記事本檔案以新增以下行：

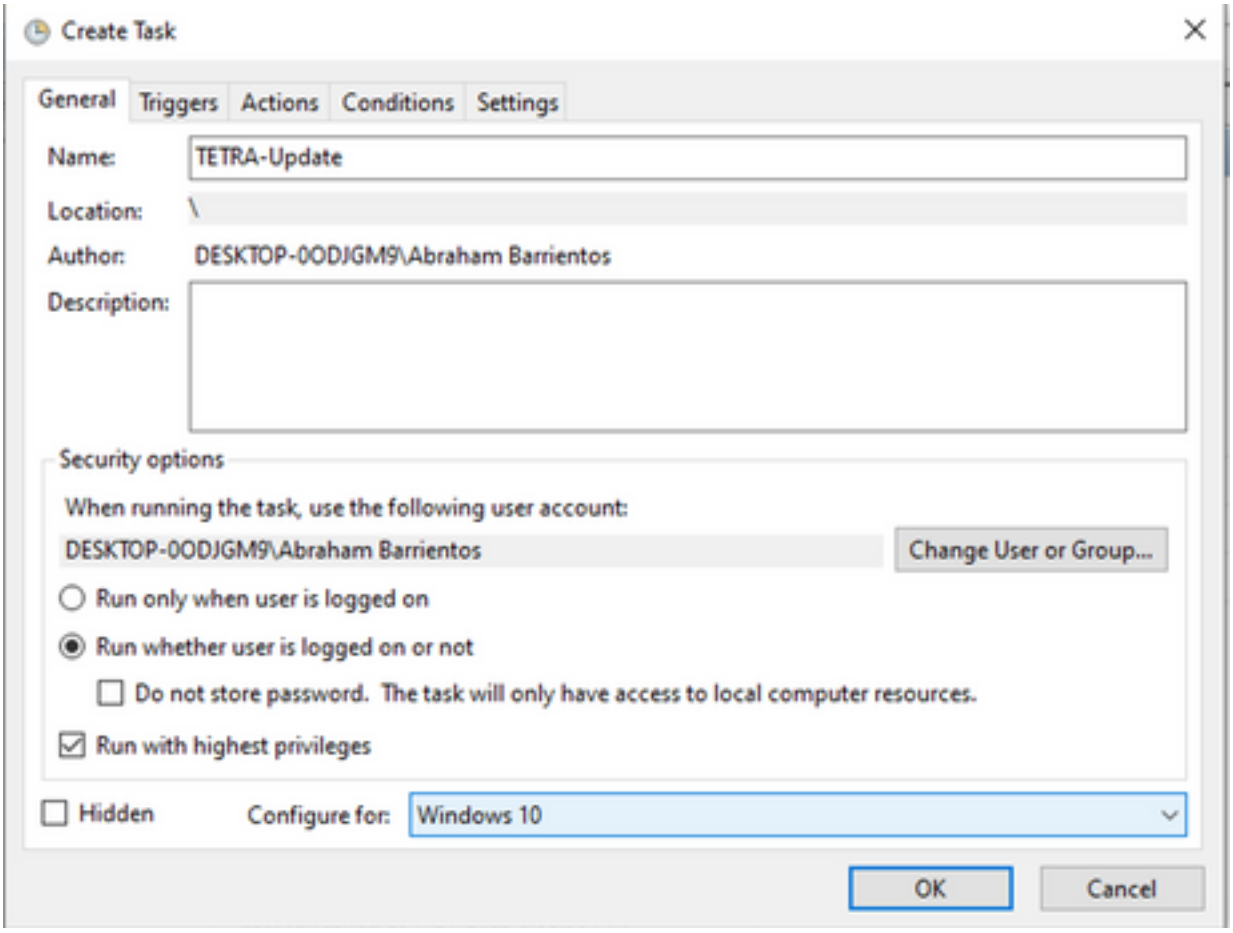
```
cd C:\Program Files\Cisco\AMP\8.1.3.21242
sfc.exe -forceupdate
```

請注意，您需要使用與終端上當前已安裝版本匹配的安全終端版本(本例中為8.1.3.21242v)。如果不確定版本，可以按一下**Secure Endpoint**使用者介面裝置圖示，然後按一下**Statics**頁籤檢查當前版本。將這些行新增到記事本後，按一下**File**，然後按一下**Save As。然後按一下Save as a Type**，然後選擇**All files**。最後，鍵入檔案的名稱並將其另存為.BAT副檔名。如果要將檔案儲存在C:\資料夾下，則需要使用管理員許可權執行記事本。作為附帶說明，您可以執行BAT檔案以強制TETRA更新作為測試。

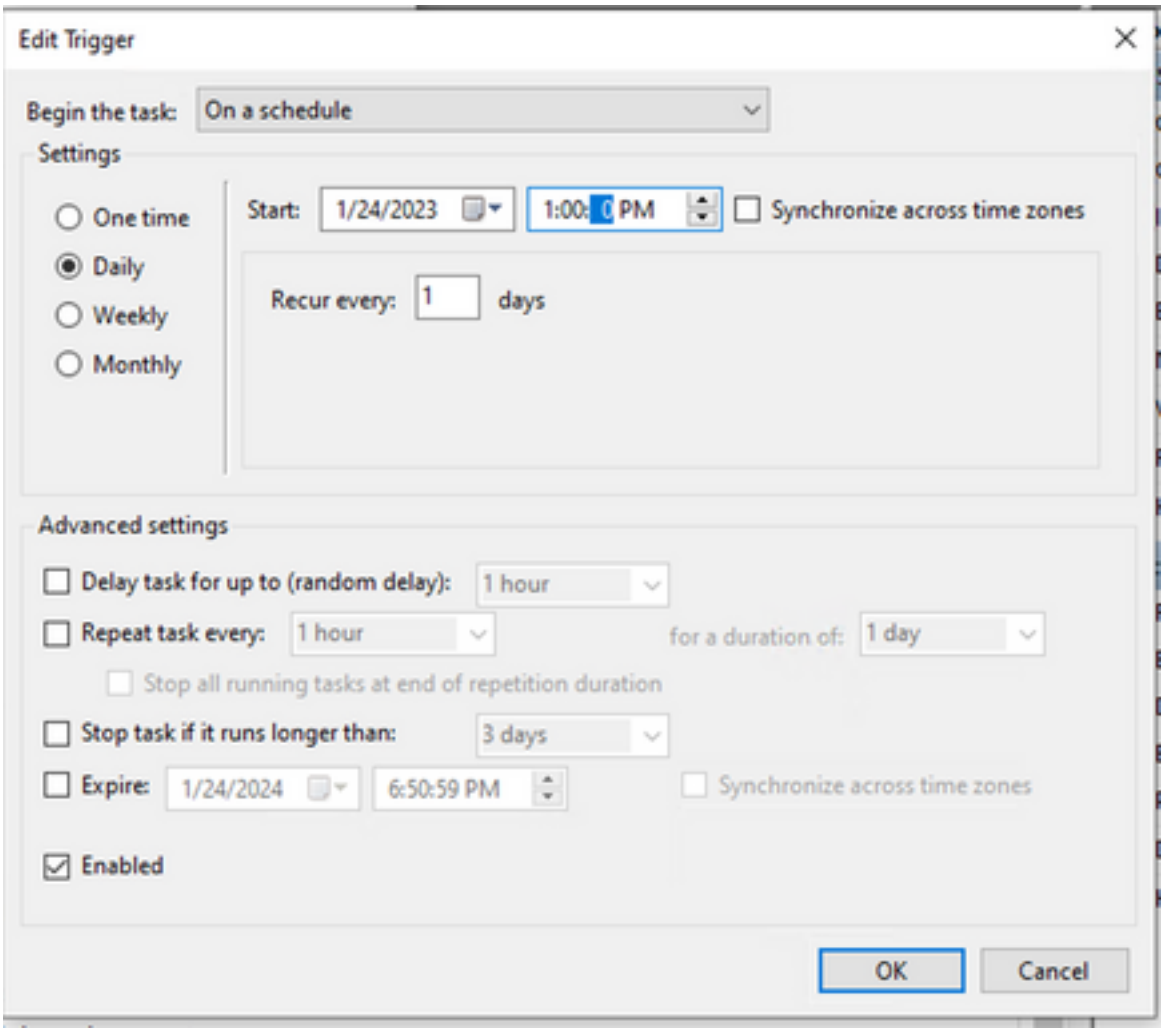
在Windows電腦上開啟Schedule Task Open Task Scheduler（計畫任務開啟任務計畫程式），然後按一下**Create a Task**（建立任務）按鈕（位於右列）。



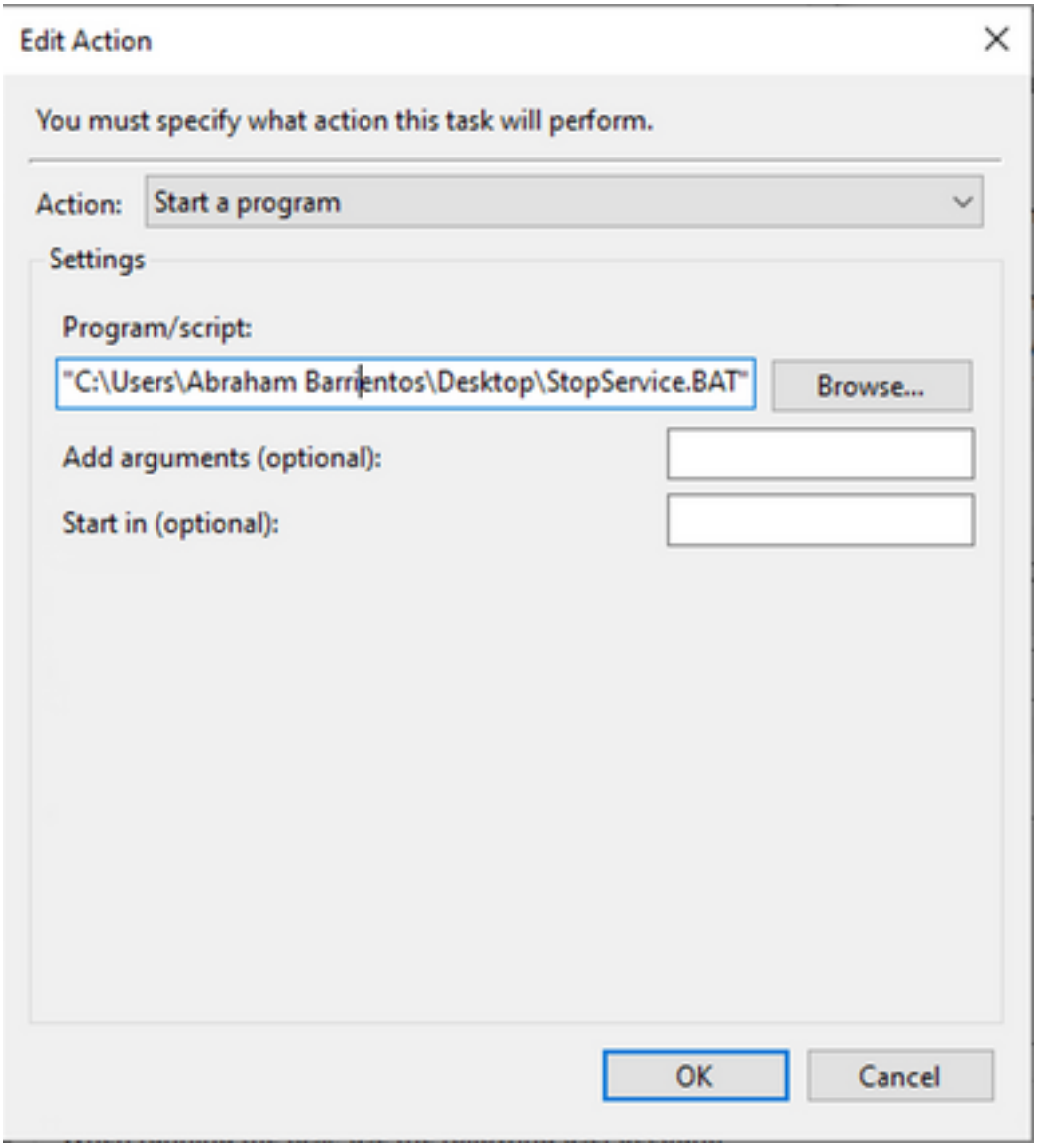
在**General**頁籤下，鍵入此任務的名稱，然後選擇**Run whenever user is logged or not logged**。選中**Run with the highest privelages**覈取方塊。在**configure for**選項下，選擇應用的作業系統。本演示使用Windows 10。



在「**Triggers**」頁籤下，按一下**New Trigger**。 在「新建觸發器配置」頁上，可以自定義希望TETRA更新其簽名的時間。在本例中，使用了本地電腦時間下午1點運行的每日計畫。開始日期選項定義此任務何時啟用。完成計畫設定後，按一下**ok**。



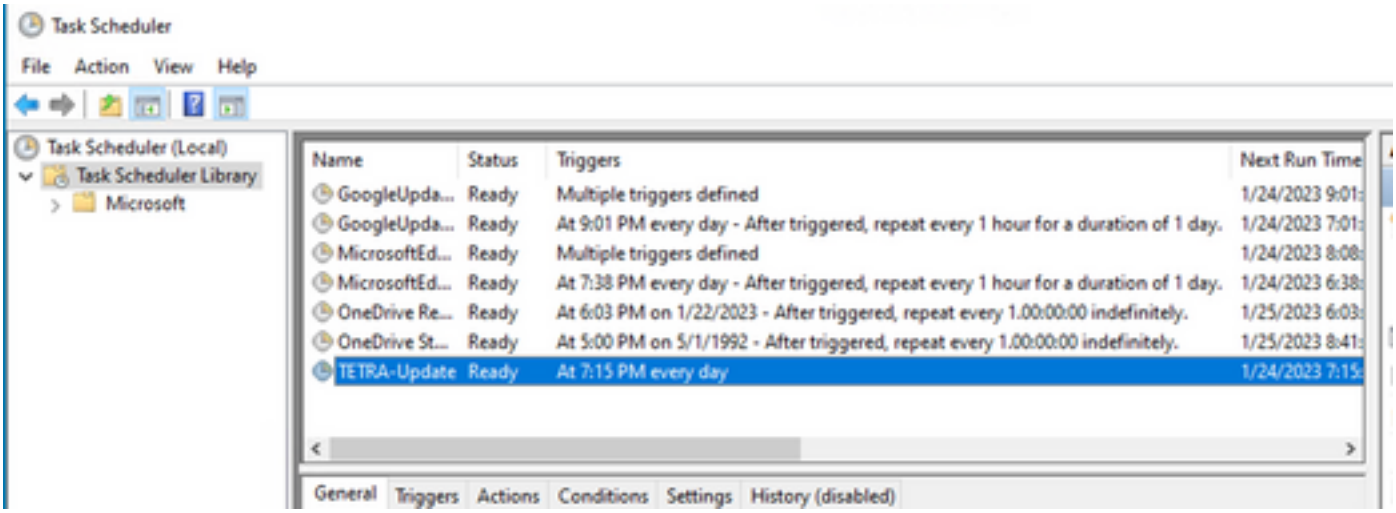
在「**Actions**」頁籤上，按一下**New Action**。在「**New Action**」頁籤上，為「**Action**」設定選擇「**Start a program**」。在Program/Settings下，按一下**Browse**，然後選擇BAT指令碼。按一下**Ok**以建立操作。將其餘設定保留為預設值，然後按一下**Ok**以建立Task。



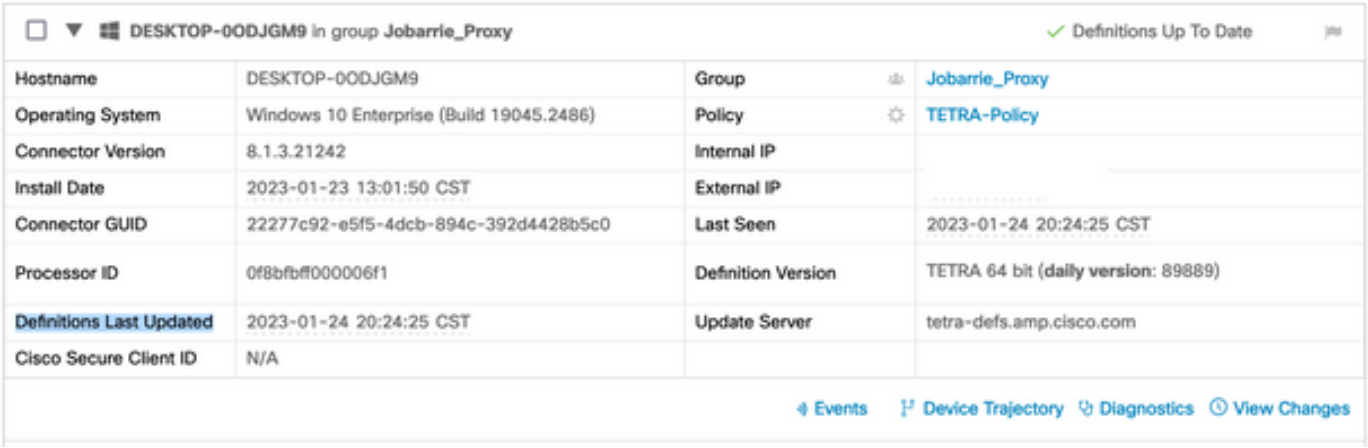
最後，此任務計畫程式需要管理憑據才能建立任務，因為選擇了「使用最高許可權運行」。使用管理員憑據進行身份驗證後，任務即可運行並執行以通知Secure Endpoint Service何時根據配置的計畫相應地更新TETRA。

驗證

按一下左列中的**Task Scheduler Library**資料夾。驗證是否已按預期建立並列出計畫。



您可以檢查聯結器在**安全端點使用者介面 > 靜態**頁籤下下載的最新TETRA定義編號。您可以使用此數字在**Management > Av Definitions summary**下比較控制檯中可用的最新定義，以查詢裝置是否最新和最新定義。另一種替代方法是在安全端點控制檯中監視特定端點的「定義上次更新」值。



疑難排解

當定義沒有按預期更新時，您可以檢視日誌，以搜尋TETRA更新錯誤。為此，請在Schedule任務觸發時間之前，在Advanced頁籤下的Secure Endpoint使用者介面上啟用調試模式。在「計畫任務觸發器」之後，讓聯結器在此模式下運行至少20分鐘，然後檢視位於**C:\Program Files\Cisco\AMP\X.X.X**（其中X.X.X是系統上的安全端點的當前版本）下的最新**sfcx.exe.log**檔案。

ForceWakeUpdateThreadAbout向我們顯示，TETRA由計畫作業觸發，以便按預期進行更新。如果您沒有看到此日誌，則可能是與Windows計畫任務配置相關的問題。

```
(99070187, +0 ms) Jan 24 20:30:01 [3544]: ForceWakeUpdateThreadAbout to force update thread
awake. Forcing tetra def update.
(99070187, +0 ms) Jan 24 20:30:01 [1936]: UpdateThread: Tetra ver string retrieved from config:
(99070781, +0 ms) Jan 24 20:30:02 [1936]: UpdateTetra entered...
(99070781, +0 ms) Jan 24 20:30:02 [1936]: UpdateTetra: elapsed: cur: 1674621002, last: 0,
interval:180
```

如果計畫作業成功觸發TETRA更新定義，則需要在日誌中搜尋任何相關的TETRA錯誤。這是TETRA錯誤代碼2200，它表示服務在更新過程中被中斷。如何對一般TETRA錯誤進行故障排除不在本檔案的範圍之內，但是，本文檔末尾的連結是關於對TETRA錯誤代碼進行故障排除的思科文章。

```
ERROR: TetraUpdateInterface::update Update failed with error -2200
```

相關資訊

- TETRA
- — Tetra3000
- TETRA — Windows

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）。