TETRAダウンロードのカスタム時間の設定

内容

概要

このドキュメントでは、帯域幅の使用に関する要件を満たすために、必要な時間にTETRAアップデートをダウンロードするようにローカルエンドポイントを設定する方法について説明します。

背景説明

TETRAはSecure Endpoint用のオフラインエンジンで、アンチウイルスシグニチャを使用してエンドポイントを保護します。TETRAは、世界中のすべての新しい脅威に対応するために、シグニチャデータベースの更新を毎日受け取っています。これらのアップデートは大規模な環境で大量の帯域幅を使用する可能性があるため、各エンドポイントはデフォルトで1時間に設定されているアップデート間隔内でダウンロードの時間をランダム化します。 TETRAポリシーで選択可能な更新間隔は異なりますが、このダウンロードプロセスをトリガーする特定の時間を選択することはできません。このドキュメントでは、TETRAにWindows ScheduleジョブでAVシグニチャを更新するように強制する回避策について説明します。

前提条件

要件

セキュアエンドポイントポリシーの設定およびWindowsスケジュールジョブに関する基本的な知識。

使用するコンポーネント

- セキュアエンドポイントクラウドコンソール
- Secure Endpoint Connector for Windows 8.1.3
- Windows 10 Enterprise

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく

ださい。

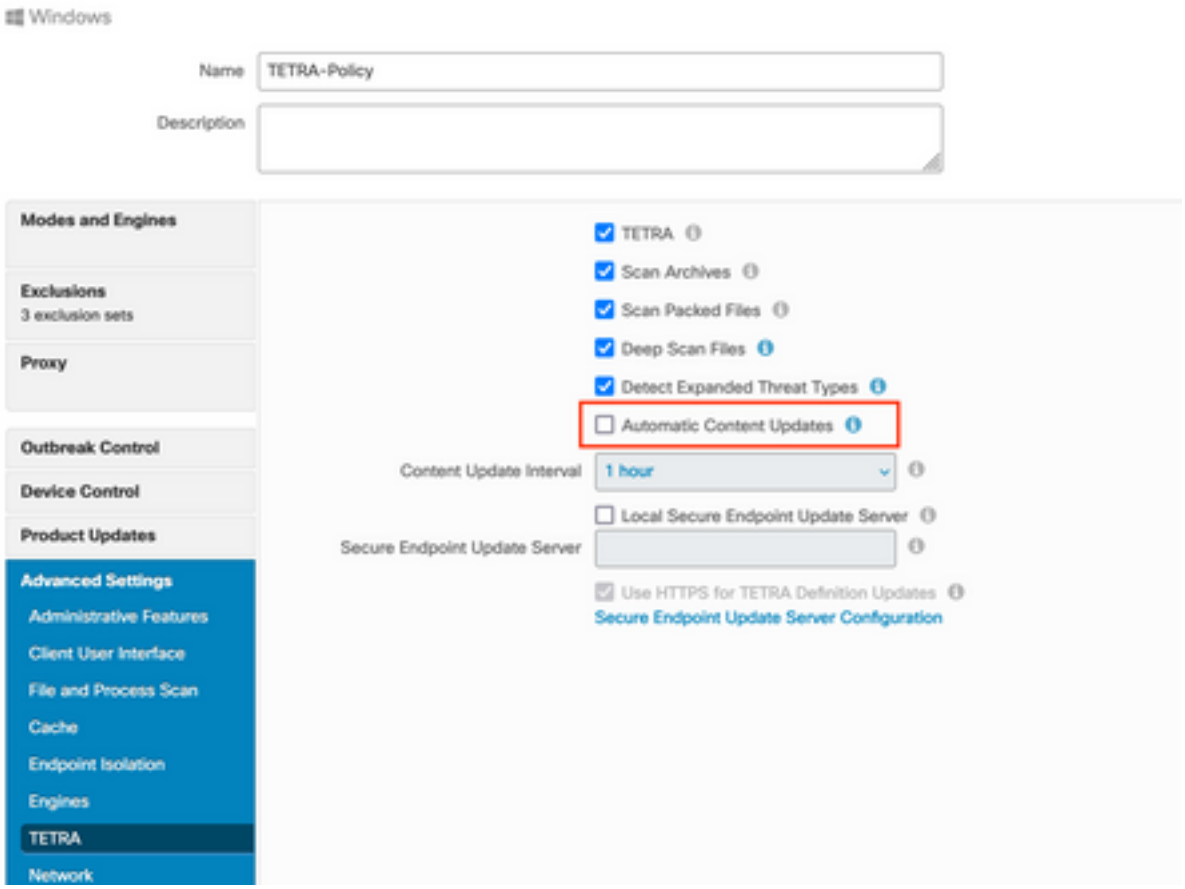
設定

> **警告**:「背景説明」セクションで説明したように、TETRAアップデートは大量の帯域幅を消費する可能性があります。デフォルトでは、Secure Endpointはこの影響を減らし、デフォルトで1時間に設定されている更新間隔内でTETRA更新をランダム化しようとします。特に大規模な環境では、すべてのコネクタに対して定義を同時に更新するように強制することは推奨されません。このプロセスは、アップデートの時間を制御することが重要な特殊な状況でのみ使用する必要があります。それ以外の場合は、自動更新が推奨されます。

カスタムTETRAダウンロード時間用に設定するセキュアエンドポイントポリシーを選択します。

> **注**：この設定はポリシーベースで行われ、このポリシー内のすべてのエンドポイントが影響を受けることに注意してください。そのため、カスタムTETRAアップデート用に制御するすべてのデバイスを同じセキュアエンドポイントポリシーに配置することをお勧めします。

Secure Endpoint Management Consoleにログインし、[Management] > [Policies] に移動して、使用するポリシーを選択し、[edit] をクリックします。ポリシー設定ページが表示されたら、[TETRA] セクションに移動します。このセクションで、[Automatic Content Updates] チェックボックスをオフにし、ポリシーを**保存**します。これは、すべてSecure Endpoint Cloudコンソールの設定に関連しています。

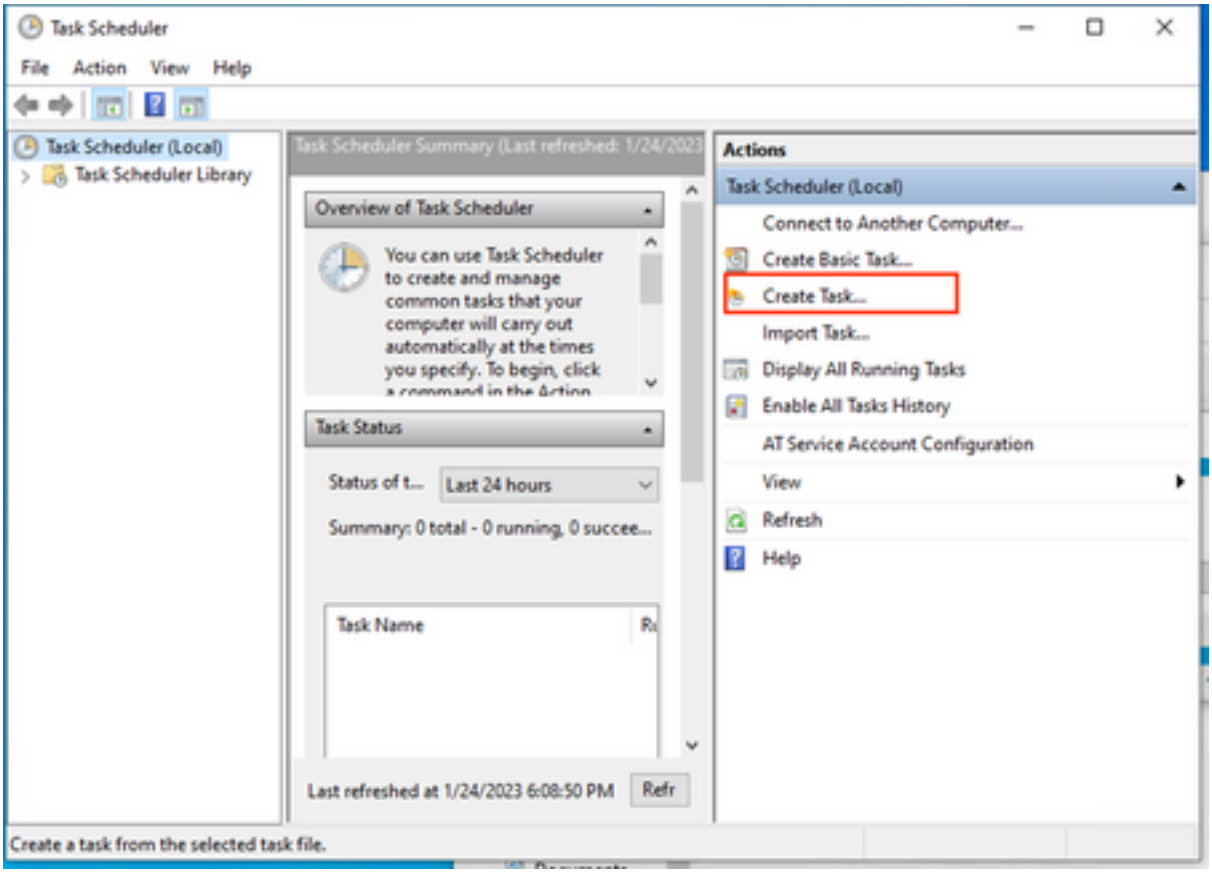


次の設定では、Windowsデバイスにアクセスし、新しいメモ帳ファイルを開いて次の行を追加します。

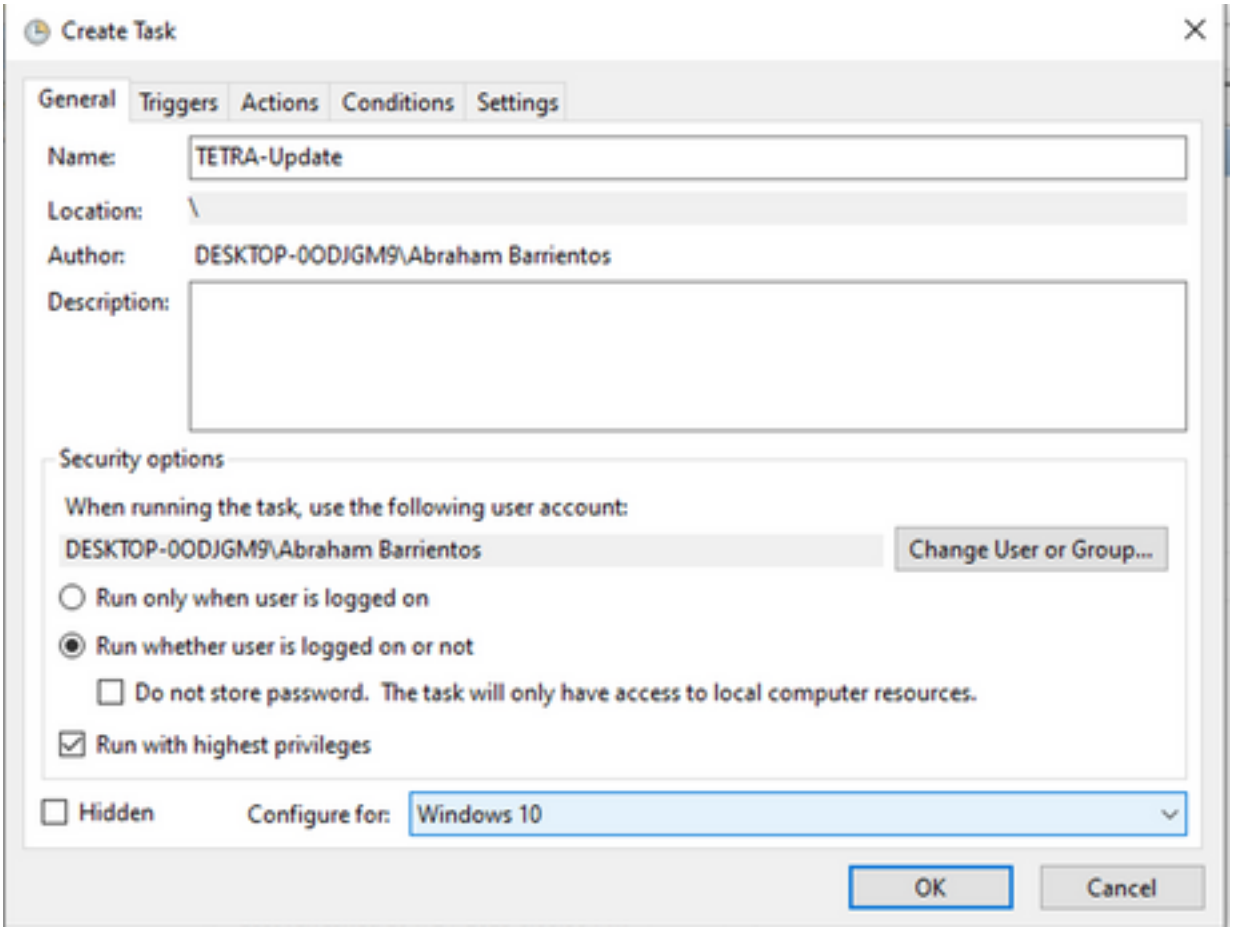
```
cd C:\Program Files\Cisco\AMP\8.1.3.21242
sfc.exe -forceupdate
```

エンドポイントに現在インストールされているバージョンと一致するセキュアエンドポイントのバージョン(この例では8.1.3.21242v)を使用する必要があることに注意してください。バージョンが不明な場合は、**Secure Endpoint**のユーザインターフェイス(UI)の歯車アイコンをクリックし、次に**Statics Tab**をクリックして現在のバージョンを確認できます。これらの行をメモ帳に追加したら、[File] をクリックし、[Save As] をクリックします。**次に、[Save as a Type]** をクリックし、[All files] を選択します。最後に、ファイルの名前を入力し、.BAT拡張子として保存します。C:\フォルダにファイルを保存する場合は、管理者権限でメモ帳を実行する必要があります。サイドノートとして、BATファイルを実行して、テストとしてTETRAの更新を強制することができます。

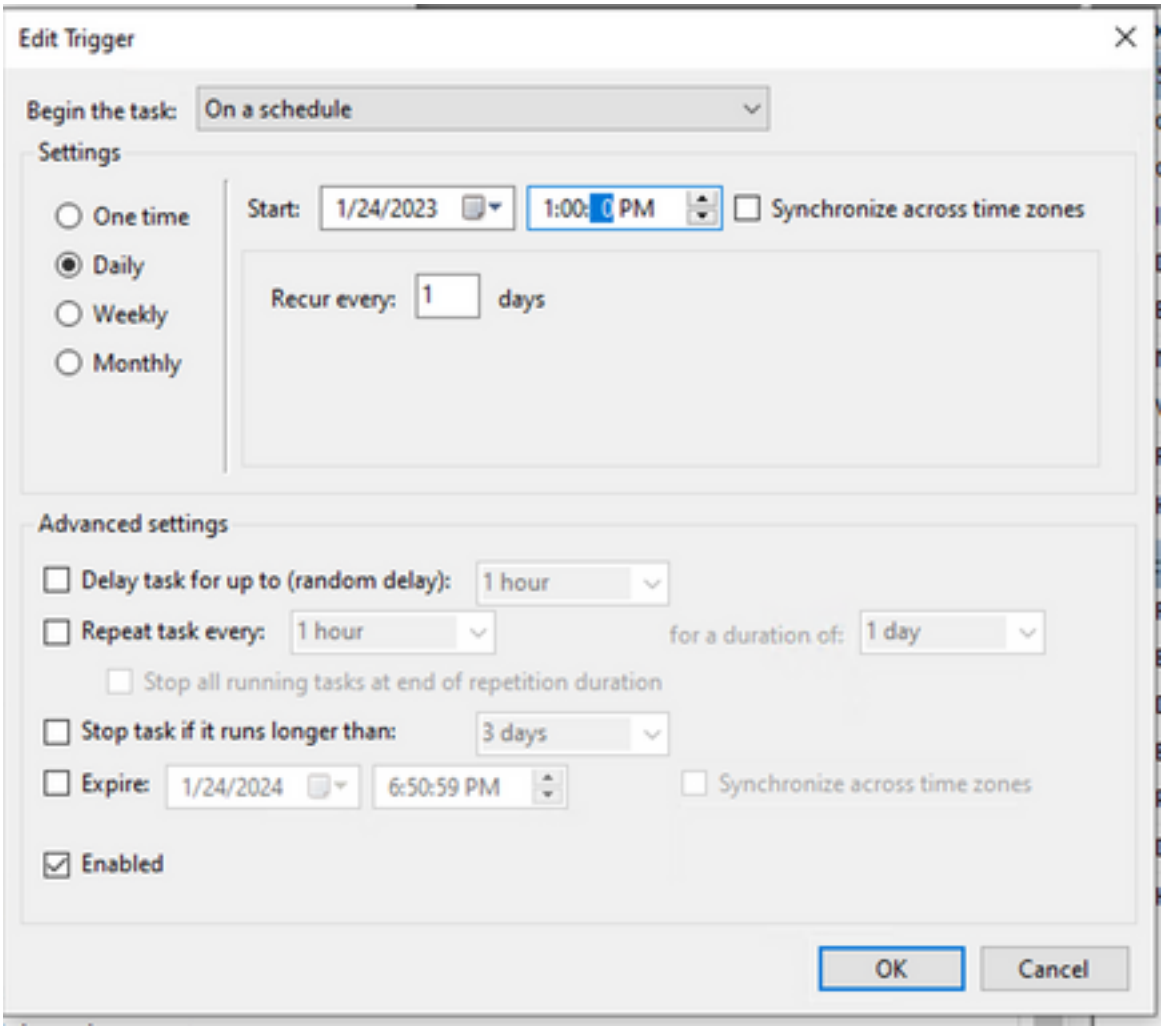
WindowsマシンでSchedule Task Open Task Schedulerを開き、右側の列にある**Create a Task**ボタンをクリックします。



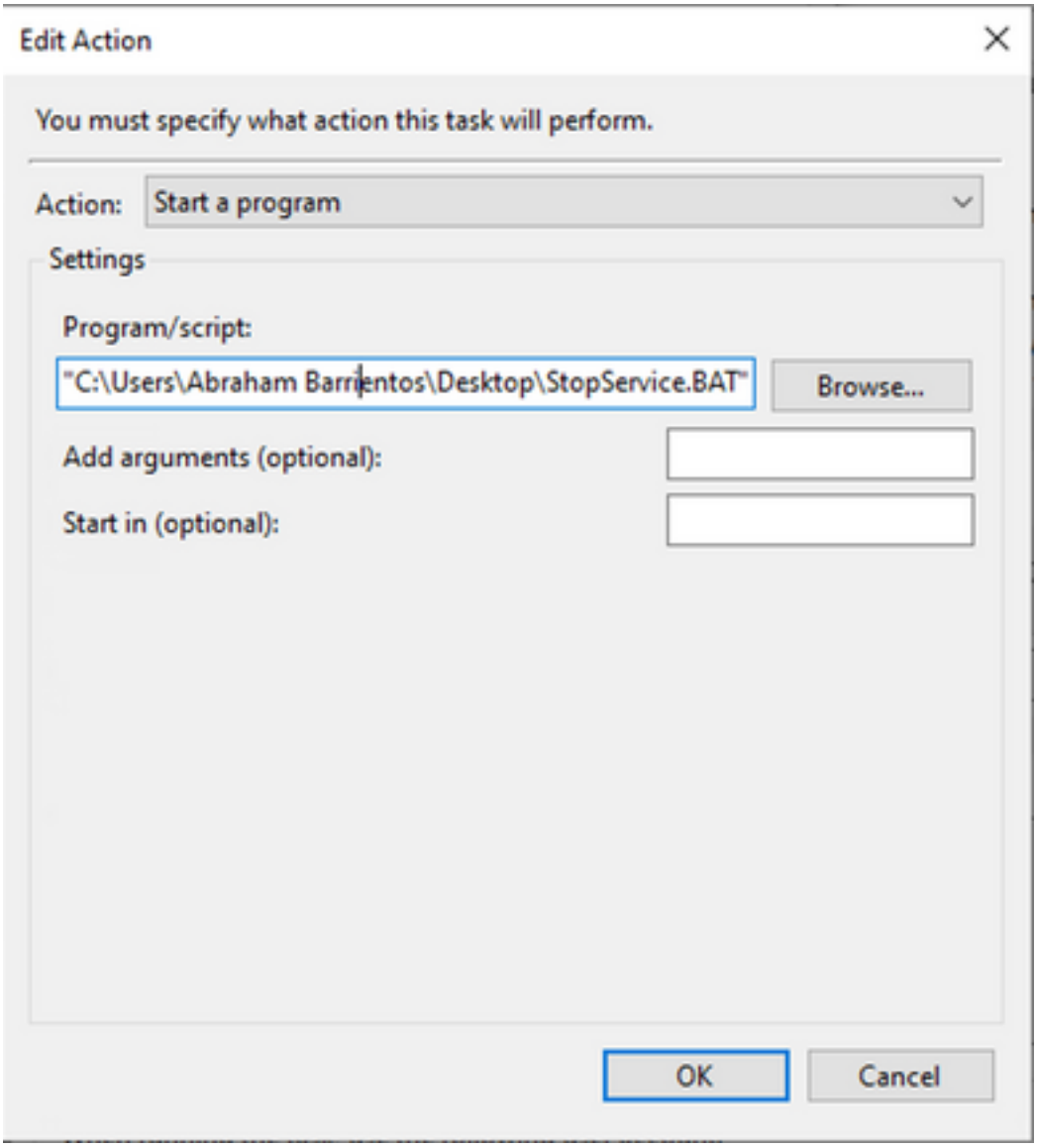
[General] タブで、このタスクの名前を入力し、[Run anytime user is logged or not] を選択します。[Run with the highest privelages] チェックボックスをオンにします。**configure for**オプションで、適用するOSを選択します。このデモンストレーションでは、Windows 10を使用しました。



[Triggers] タブで、[New Trigger] をクリックします。 [New trigger configuration]ページでは、TETRAがシグニチャを更新する時刻をカスタマイズできます。この例では、ローカルマシン時刻の午後1時に実行される日次スケジュールが使用されました。[開始日]オプションでは、このタスクがアクティブになる時期を定義します。スケジュールの設定が完了したら、[ok]をクリックします。



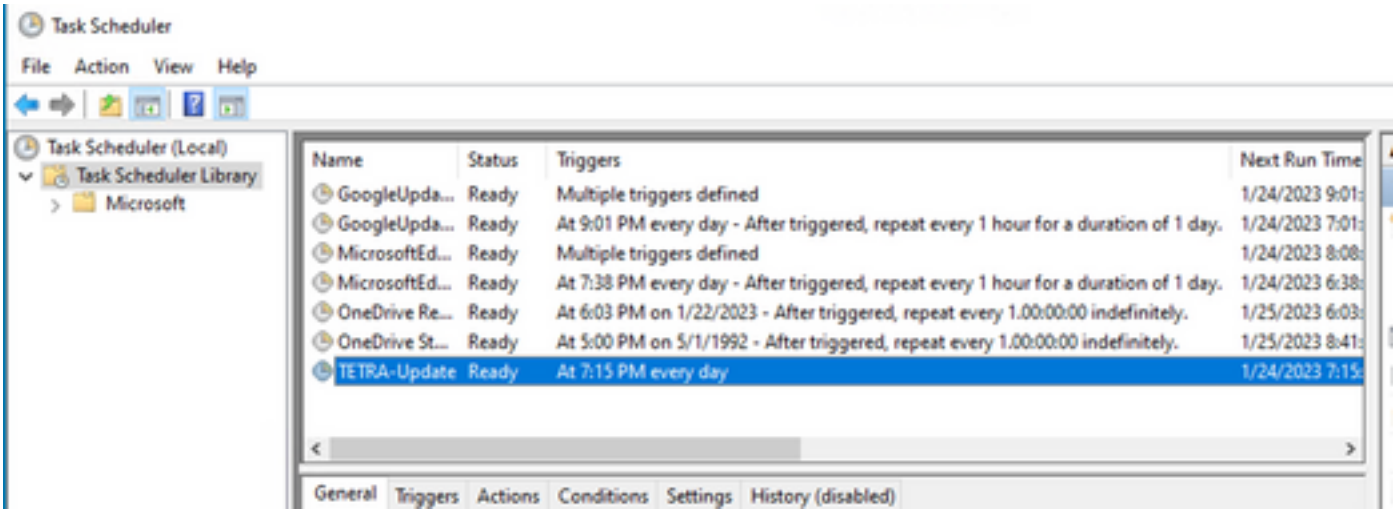
[Actions] タブで、[New Action] をクリックします。[New Action] タブで、[Action] 設定の[Start a program] を選択します。[Program/Settings]で[Browse] をクリックし、BATスクリプトを検索して選択します。**Ok**をクリックしてアクションを作成します。残りの設定はデフォルトのままにし、[OK] をクリックしてタスクを作成します。



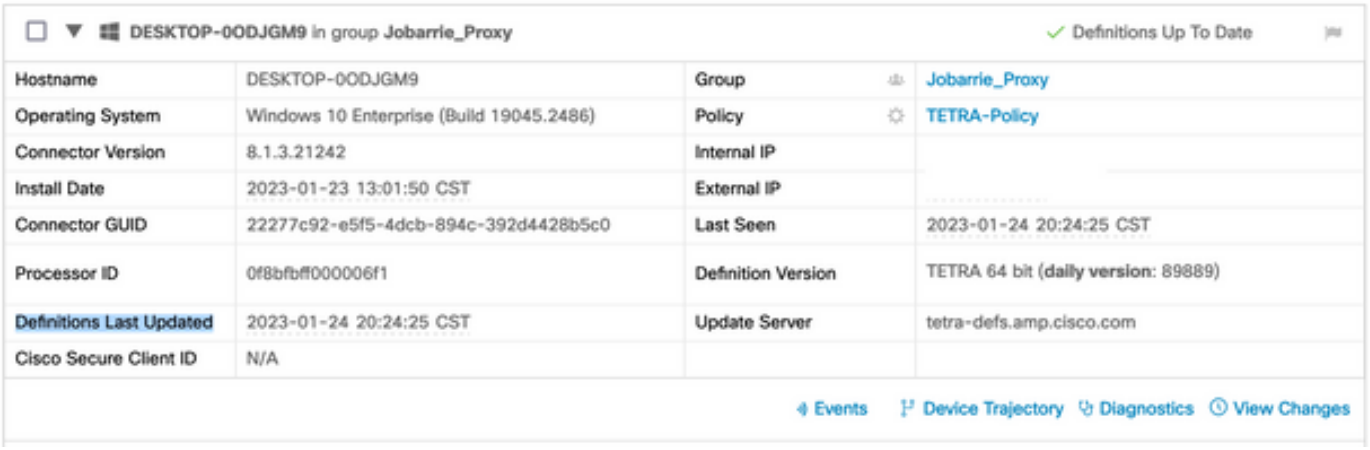
最後に、このタスクスケジューラでは、[最高の特権で実行]が選択されているため、タスクを作成するために管理者の資格情報が必要です。管理者クレデンシャルによる認証後、タスクを実行して実行し、設定されたスケジュールに従ってTETRAを更新するタイミングをセキュアエンドポイントサービスに通知する準備が整います。

確認

左側の列で[Task Scheduler Library] フォルダをクリックします。スケジュールが作成され、期待どおりにリストされていることを確認します。



コネクタによってダウンロードされた最新のTETRA定義番号は、[Secure Endpoint User interface] > [static] タブで確認できます。この番号を使用して、コンソールの[Management] > [Av Definitions summary] で使用できる最新の定義を比較し、デバイスが最新の定義を使用しているかどうかを確認できます。別の方法として、セキュアエンドポイントコンソールで特定のエンドポイントの[Definitions Last Updated]値を監視する方法もあります。



トラブルシュート

定義が期待どおりに更新されない場合は、ログを参照してTETRA更新エラーを検索できます。これを行うには、[Schedule task trigger time]の前に、[Advanced]タブの[Secure Endpoint]ユーザインターフェイスでデバッグモードを有効にします。[Schedule Task Trigger]の後、少なくとも20分間このモードでコネクタを実行し、次に**C:\Program Files\Cisco\AMP\X.X.X**の下にある最新の**sfcx.exe.log**ファイル（X.X.Xはシステム上のセキュアエンドポイントの現在のバージョン）を調べます。

ForceWakeUpdateThreadAboutは、TETRAがスケジュールジョブによってトリガーされ、期待どおりに更新されることを示します。このログが表示されない場合は、windowsスケジュールタスクの構成に関連する問題である可能性があります。

```
(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
```

スケジュールジョブが正常にTETRAをトリガーして定義を更新する場合は、ログで関連するTETRAエラーを検索する必要があります。これは、TETRAエラーコード2200の例です。これは、更新プロセス中にサービスが中断されたことを意味します。一般的なTETRAエラーのトラブルシューティング方法は、このドキュメントの範囲外ですが、このドキュメントの最後にあるリンクは、「TETRAエラーコードのトラブルシューティング」に関するシスコの有用な記事です。

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

関連情報

- TETRA
- Cisco Secure Endpoint - Tetra Definitions3000
- TETRA – Windows

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。