Konfigurieren einer benutzerdefinierten Uhrzeit für TETRA-Downloads

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie lokale Endgeräte so konfiguriert werden, dass sie zu einem beliebigen Zeitpunkt TETRA-Updates herunterladen können, um die Bandbreitennutzungsanforderungen zu erfüllen.

Hintergrundinformationen

TETRA ist die Offline-Engine für Secure Endpoint, die Antivirus-Signaturen verwendet, um die Endpunkte zu schützen. TETRA erhält tägliche Updates zu seiner Signaturdatenbank, um mit allen neuen Bedrohungen in freier Wildbahn Schritt zu halten. Diese Updates können in großen Umgebungen eine erhebliche Bandbreite beanspruchen. Daher wird für jeden Endpunkt die Zeit für den Download innerhalb des Aktualisierungsintervalls zufällig festgelegt, das standardmäßig auf 1 Stunde festgelegt ist. Obwohl verschiedene Aktualisierungsintervalle für die TETRA-Richtlinie zur Auswahl stehen, ist es nicht möglich, eine bestimmte Zeit für die Auslösung dieses Downloadprozesses auszuwählen. Dieses Dokument bietet eine Problemumgehung, um TETRA zu zwingen, seine AV-Signaturen mit Windows Schedule-Jobs zu aktualisieren.

Voraussetzungen

Anforderungen

Grundlegendes Wissen über die Konfiguration von Richtlinien für sichere Endgeräte und über Windows-Zeitplanaufträge.

Verwendete Komponenten

- Secure Endpoint Cloud-Konsole
- Secure Endpoint Connector für Windows 8.1.3

- Windows 10 Enterprise

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

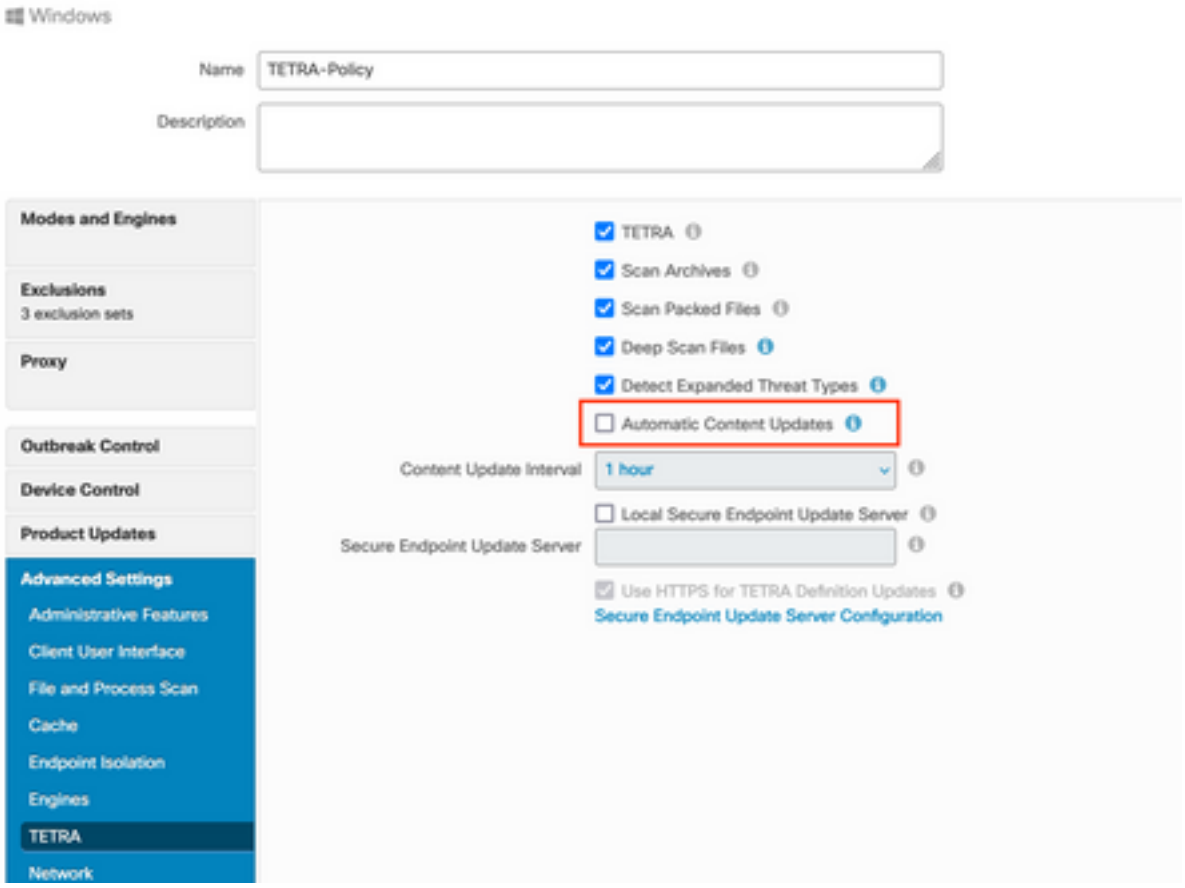
Konfigurieren

> **Warnung**: Wie im Hintergrundabschnitt beschrieben, können TETRA-Updates erhebliche Bandbreite beanspruchen. Standardmäßig versucht Secure Endpoint, diese Auswirkungen zu reduzieren und die TETRA-Updates innerhalb des Aktualisierungsintervalls, das standardmäßig auf 1 Stunde festgelegt ist, nach dem Zufallsprinzip zu aktualisieren. Es wird nicht empfohlen, alle Steckverbinder zu zwingen, die Definitionen gleichzeitig zu aktualisieren, insbesondere in großen Umgebungen. Dieser Prozess darf nur in besonderen Situationen verwendet werden, in denen es wichtig ist, den Zeitpunkt der Aktualisierung zu steuern. Bei allen anderen Szenarien sind automatische Updates vorzuziehen.

Wählen Sie eine Richtlinie für sichere Endgeräte aus, die für die benutzerdefinierte TETRA-Downloadzeit konfiguriert werden soll.

> **Hinweis**: Beachten Sie, dass diese Konfiguration auf einer Richtlinienbasis erfolgt und alle Endpunkte in dieser Richtlinie betroffen sind. Es wird daher empfohlen, alle Geräte, die Sie für benutzerdefinierte TETRA-Updates steuern möchten, in derselben Richtlinie für sichere Endgeräte zu speichern.

Melden Sie sich bei der Konsole für die sichere Endpunktverwaltung an, navigieren Sie zu **Verwaltung > Richtlinien**, suchen Sie nach der Richtlinie, die Sie verwenden möchten, und klicken Sie auf **Bearbeiten**. Sobald Sie sich auf der Seite für die Richtlinienkonfiguration befinden, navigieren Sie zum **TETRA-Abschnitt**. Deaktivieren Sie in diesem Abschnitt das Kontrollkästchen **Automatische Inhaltsaktualisierung**, und **speichern Sie** die Richtlinie. Das alles bezieht sich auf die Konfiguration in der Secure Endpoint Cloud-Konsole.

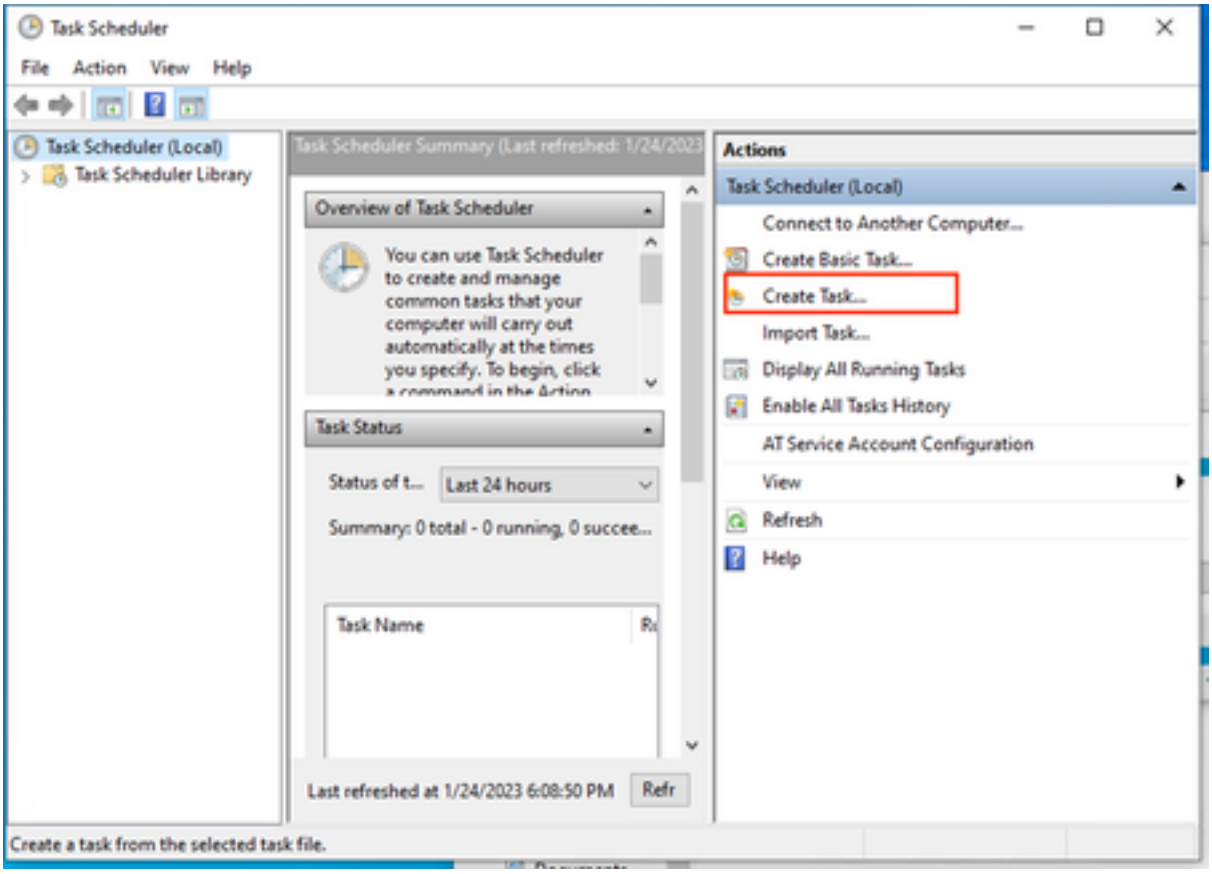


Öffnen Sie für die nächste Konfiguration Ihr Windows-Gerät, und fügen Sie folgende Zeilen in eine neue Editor-Datei ein:

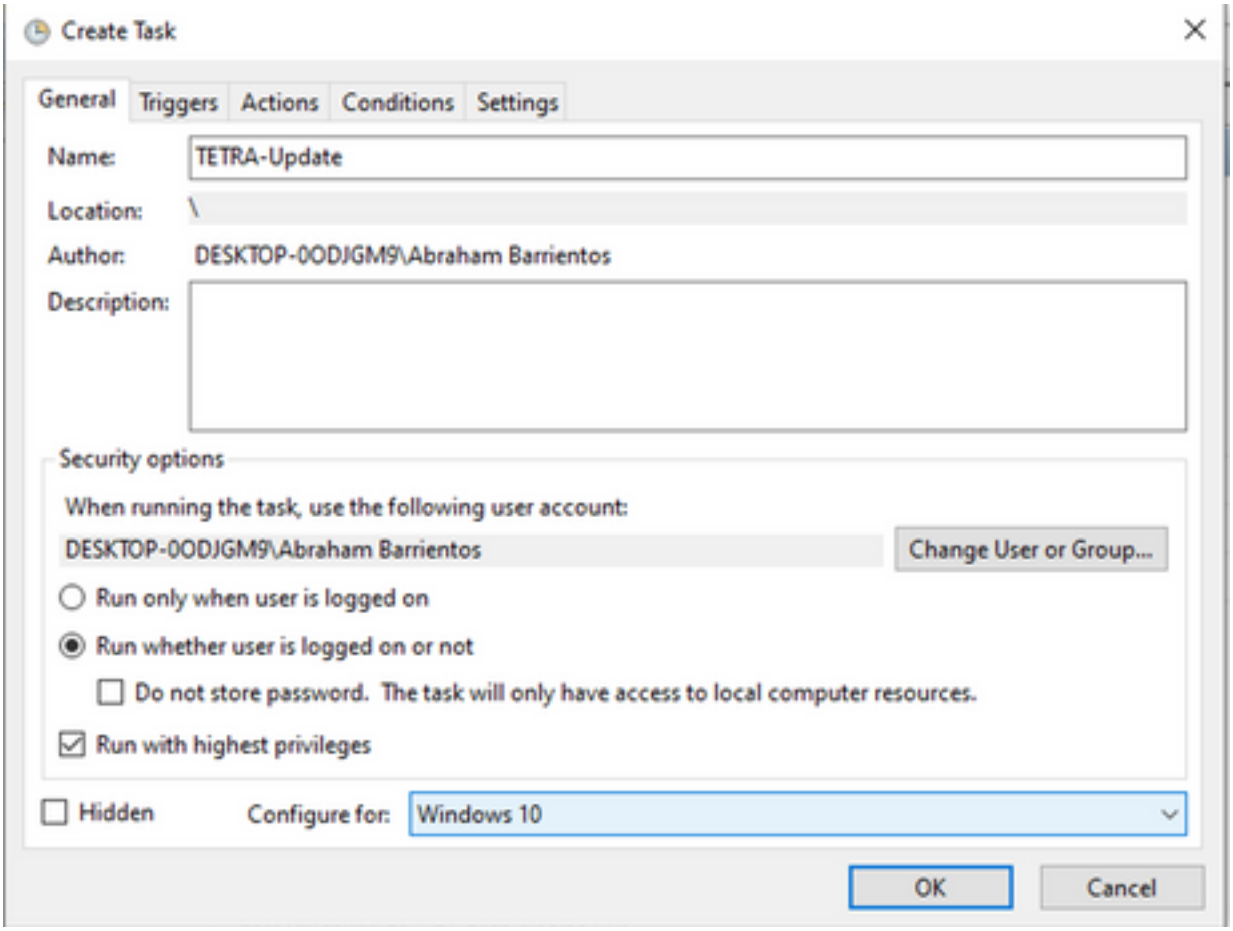
```
cd C:\Program Files\Cisco\AMP\8.1.3.21242
sfc.exe -forceupdate
```

Beachten Sie, dass Sie die Secure Endpoint-Version (in diesem Beispiel 8.1.3.21242v) verwenden müssen, die mit der aktuell auf dem Endpunkt installierten Version übereinstimmt. Wenn Sie sich nicht sicher sind, welche Version verwendet wird, können Sie auf das Zahnradsymbol **Secure Endpoint** User Interface und dann auf die **Registerkarte Static (Statistiken)** klicken, um die aktuelle Version zu überprüfen. Wenn Sie diese Zeilen dem Notizblock hinzugefügt haben, klicken Sie auf **Datei** und dann auf **Speichern unter.** Klicken Sie dann auf **Als Typ speichern** und wählen Sie **Alle Dateien**. Geben Sie abschließend den Namen der Datei ein, und speichern Sie sie als BAT-Erweiterung. Wenn Sie die Datei im Ordner C:\ speichern möchten, müssen Sie Notepad mit Administratorrechten ausführen. Als Nebenbemerkung können Sie die BAT-Datei ausführen, um das TETRA-Update für als Test zu erzwingen.

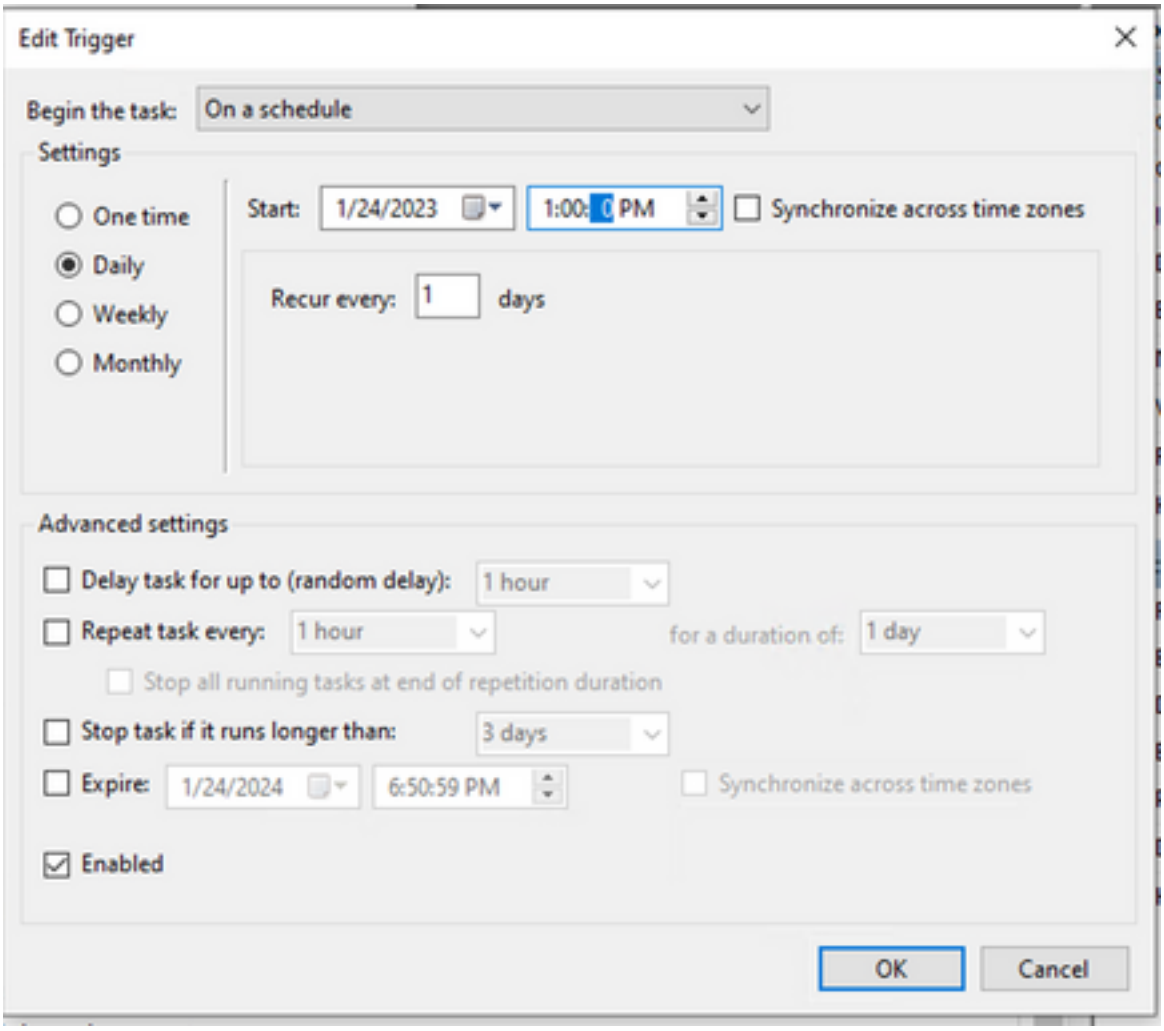
Öffnen Sie die Aufgabenplanung ansetzen Öffnen der Aufgabenplanung auf Ihrem Windows-Computer, und klicken Sie in der rechten Spalte auf **die** Schaltfläche **Aufgabe erstellen**.



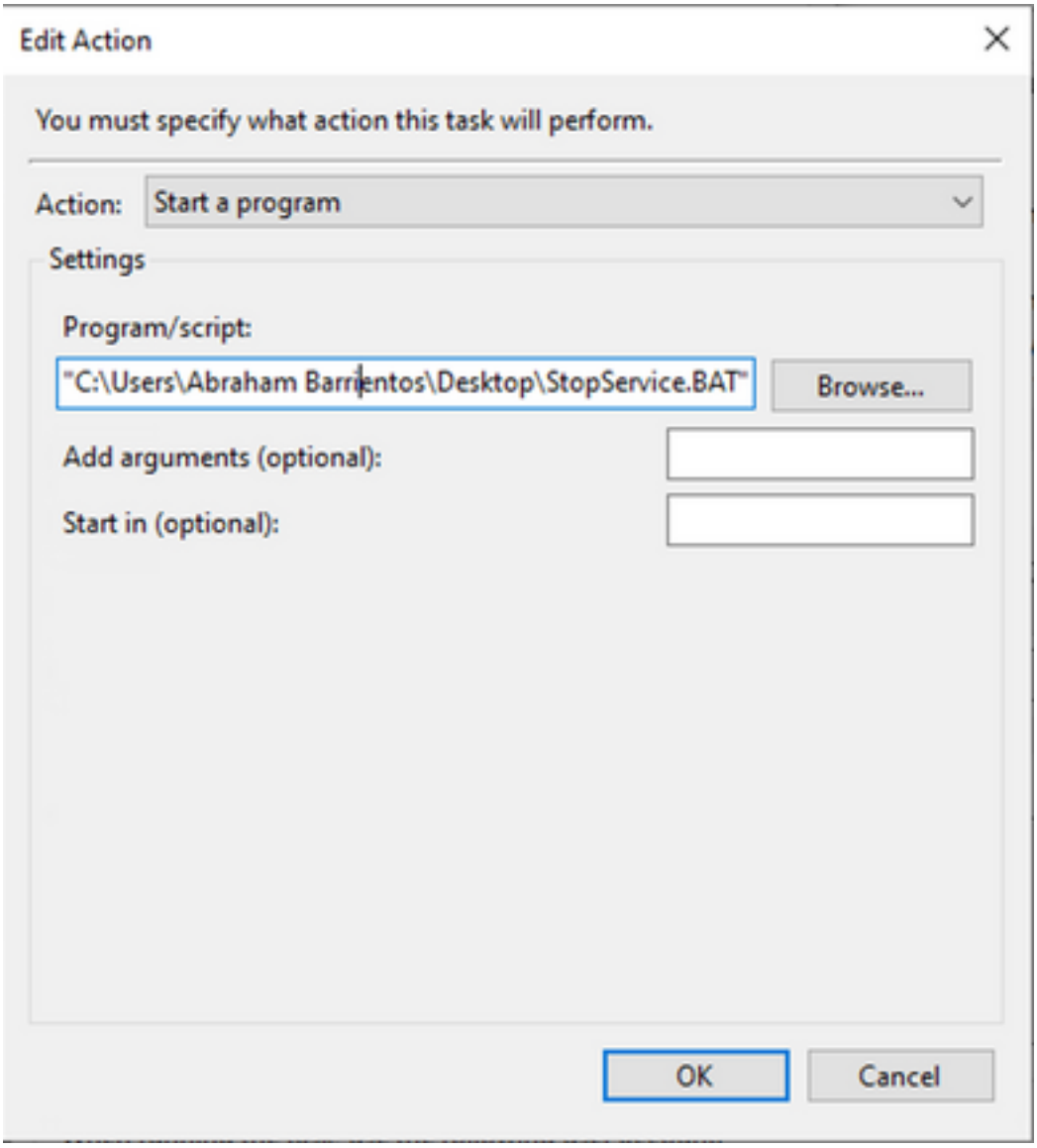
Geben Sie auf der **Registerkarte Allgemein** den Namen für diesen Task ein, und wählen Sie **Immer ausführen, wenn der Benutzer angemeldet ist oder nicht**. Aktivieren Sie **das** Kontrollkästchen **Mit den höchsten Berechtigungen ausführen**. Wählen Sie unter **configure for** option (Option **konfigurieren für**) das entsprechende Betriebssystem aus. Für diese Demonstration wurde Windows 10 verwendet.



Klicken Sie auf der Registerkarte **Trigger** auf **Neuer Trigger.** Auf der Seite Neue Trigger-Konfiguration können Sie die Zeit anpassen, zu der TETRA seine Signaturen aktualisieren soll. Für dieses Beispiel wurde ein Tageszeitplan verwendet, der um 13 Uhr (Ortszeit des Computers) ausgeführt wird. Die Option Startdatum definiert, wann diese Aufgabe aktiv wird. Wenn Sie mit den Zeitplaneinstellungen fertig sind, klicken Sie auf **OK.**



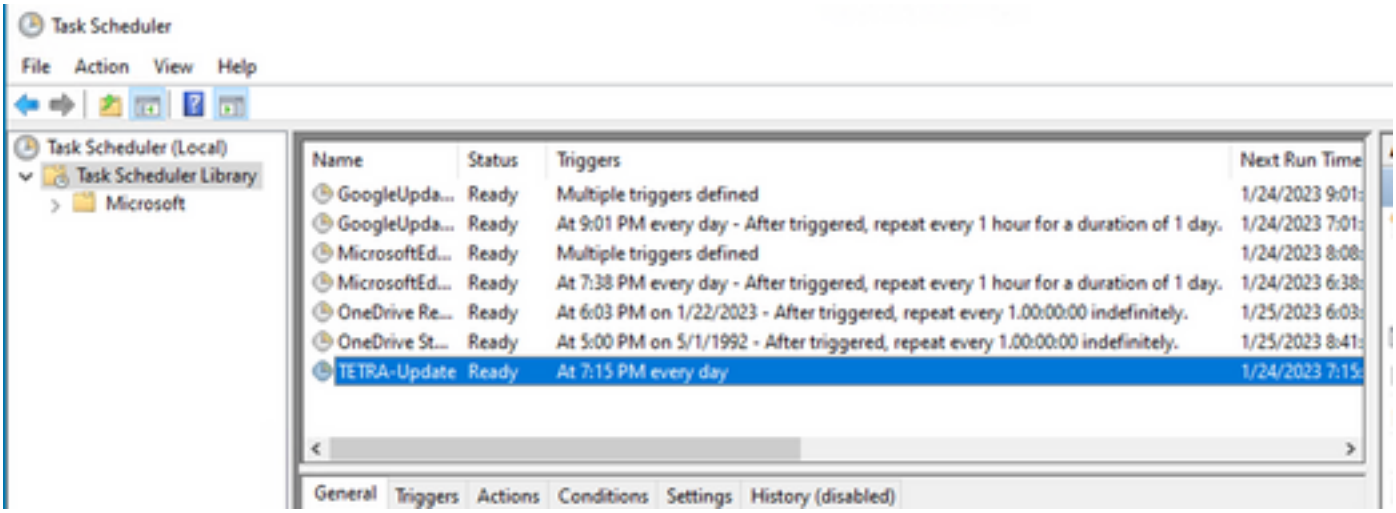
Klicken Sie auf der Registerkarte **Aktionen** auf **Neue Aktion**. Wählen Sie auf der Registerkarte **Neue Aktion** die Option **Programm starten** für die Einstellung **Aktion**. Klicken Sie unter Programm/Einstellungen auf **Durchsuchen**, und wählen Sie das BAT-Skript aus. Klicken Sie auf **OK**, um die Aktion zu erstellen. Belassen Sie die restlichen Standardeinstellungen unverändert, und klicken Sie auf **OK**, um die Aufgabe zu erstellen.



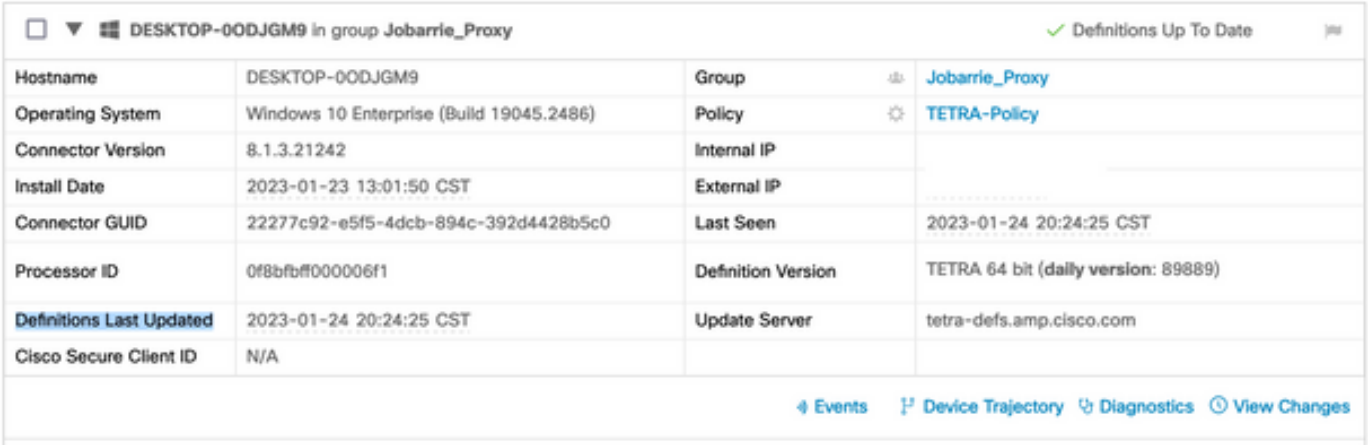
Schließlich benötigt diese Aufgabenplanung Administratorberechtigungen, um die Aufgabe zu erstellen, da "Mit höchsten Berechtigungen ausführen" ausgewählt wurde. Nach der Authentifizierung mit Admin-Anmeldedaten kann die Aufgabe ausgeführt werden, um dem Secure Endpoint-Dienst mitzuteilen, wann TETRA entsprechend dem konfigurierten Zeitplan aktualisiert werden muss.

Überprüfung

Klicken Sie in der linken Spalte auf den Ordner **Aufgabenplanungsbibliothek**. Überprüfen Sie, ob der Zeitplan erstellt und wie erwartet aufgeführt wurde.



Sie können die neueste TETRA-Definitionsnummer, die vom Connector heruntergeladen wurde, unter **Secure Endpoint User interface > Static** (**Sichere Endgeräte-Benutzeroberfläche >** Registerkarte **"Statistiken"** überprüfen. Mit dieser Nummer können Sie die neuesten Definitionen vergleichen, die in der Konsole unter **Verwaltung > Übersicht über Av-Definitionen** verfügbar sind, um herauszufinden, ob das Gerät mit den neuesten Definitionen auf dem neuesten Stand ist. Eine weitere Alternative besteht darin, den Wert "Definitions Last Updated" (Zuletzt aktualisierte Definitionen) für den jeweiligen Endpunkt in der Konsole für sichere Endpunkte zu überwachen.



Fehlerbehebung

Wenn Definitionen nicht wie erwartet aktualisiert werden, können Sie in den Protokollen nach einem TETRA-Aktualisierungsfehler suchen. Aktivieren Sie dazu den Debugmodus auf der Benutzeroberfläche von Secure Endpoint auf der Registerkarte Advanced (Erweitert) vor dem Trigger-Zeitpunkt für die Aufgabe Schedule (Zeitplan). Lassen Sie den Connector in diesem Modus nach dem Auslöser für Aufgabe planen mindestens 20 Minuten laufen, und sehen Sie sich dann die neueste Datei **sfcx.exe.log** unter **C:\Program Files\Cisco\AMP\X.X.X an (**wobei X.X.X die aktuelle Version von Secure Endpoint auf dem System ist).

The ForceWakeUpdateThreadAbout zeigt uns, dass TETRA durch unseren Zeitplanauftrag ausgelöst wird, um wie erwartet aktualisiert zu werden. Wenn dieses Protokoll nicht angezeigt wird, kann es sich um ein Problem im Zusammenhang mit der Konfiguration der Windows-Zeitplanaufgabe handeln.

```
(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
```

Falls Schedule Job erfolgreich TETRA auslöst, um Definitionen zu aktualisieren, müssen Sie nach verwandten TETRA-Fehlern in den Protokollen suchen. Dies ist ein Beispiel für einen TETRA-Fehlercode 2200, was bedeutet, dass der Dienst während des Aktualisierungsvorgangs unterbrochen wurde. Die Vorgehensweise zur Behebung allgemeiner TETRA-Fehler wird in diesem Dokument nicht behandelt. Die Links am Ende dieses Dokuments stellen jedoch nützliche Cisco Artikel zur Behebung von TETRA-Fehlercodes dar.

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

Zugehörige Informationen

- Fehlerbehebung bei Aktualisierungsfehlern von TETRA-Definitionen
- Cisco Secure Endpoint - Fehler beim Update der Tetradefinitionen mit Fehler 3000
- TETRA-Fehlercodes - Windows

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.