Een aangepaste tijd voor TETRA-downloads configureren

Inhoud

Inleiding

Dit document beschrijft hoe u lokale endpoints kunt configureren om op elk gewenst moment TETRA-updates te downloaden om aan de vereisten van bandbreedtegebruik te voldoen.

Achtergrondinformatie

TETRA is de offline engine voor Secure Endpoint die antivirushandtekeningen gebruikt om de endpoints te beschermen. TETRA ontvangt dagelijks updates van zijn handtekeningendatabase om op de hoogte te blijven van alle nieuwe bedreigingen in het wild. Deze updates kunnen aanzienlijke bandbreedte op grote omgevingen gebruiken, waardoor elk eindpunt de tijd voor de download willekeurig verdeelt binnen het updateinterval dat standaard is ingesteld op 1 uur. Hoewel er verschillende update-intervallen beschikbaar zijn om te kiezen voor het TETRA-beleid, is het niet mogelijk om een specifieke tijd te kiezen om dit downloadproces te activeren. Dit document biedt een tijdelijke oplossing om TETRA te dwingen zijn AV-handtekeningen bij te werken met Windows Schema-taken.

Voorwaarden

Vereisten

Basiskennis van Secure Endpoint beleidsconfiguratie en Windows Schedule-taken.

Gebruikte componenten

- Secure Endpoint-cloudconsole
- Secure Endpoint-connector voor Windows 8.1.3
- Windows 10 Enterprise-software

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

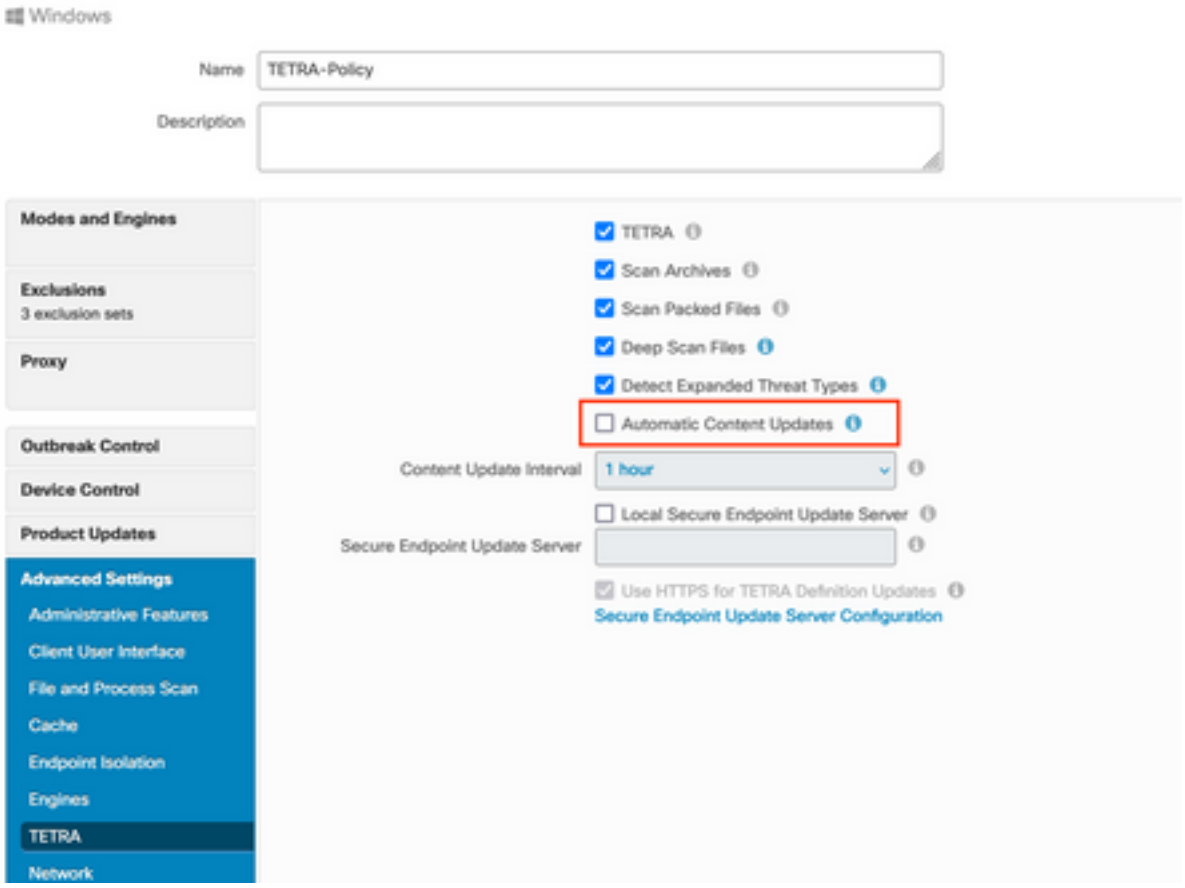
Configureren

> **Waarschuwing**: zoals beschreven in het achtergrondgedeelte, kunnen TETRA-updates aanzienlijke bandbreedte verbruiken. Standaard probeert Secure Endpoint deze impact te verminderen en de TETRA-updates willekeurig te verdelen binnen het updateinterval dat standaard op 1 uur is ingesteld. Het is niet aan te raden om alle connectors te dwingen om de definities tegelijkertijd bij te werken, met name in grote omgevingen. Dit proces mag alleen worden gebruikt in bijzondere situaties waarin het van cruciaal belang is het tijdstip van de bijwerking te beheersen. In alle andere gevallen is een automatische update de voorkeur.

Kies een Secure Endpoint beleid om te configureren voor aangepaste TETRA downloadtijd.

> **Opmerking**: houd er rekening mee dat deze configuratie op beleidsbasis wordt uitgevoerd en dat alle eindpunten in dit beleid worden beïnvloed. Daarom is het aan te raden om alle apparaten die u wilt besturen voor aangepaste TETRA-updates op hetzelfde Secure Endpoint beleid te zetten.

Log in op uw Secure Endpoint Management console en navigeer naar **Management > Beleid**, en zoek vervolgens naar het beleid dat u wilt gebruiken, klik op **bewerken**. Zodra u op de pagina van de beleidsconfiguratie bent, navigeer aan de **Sectie** van **TETRA**. Schakel onder deze sectie het aanvinkvakje **Automatische updates van inhoud uit** en **sla** het beleid op. Dit heeft alles te maken met de configuratie op de Secure Endpoint Cloud-console.

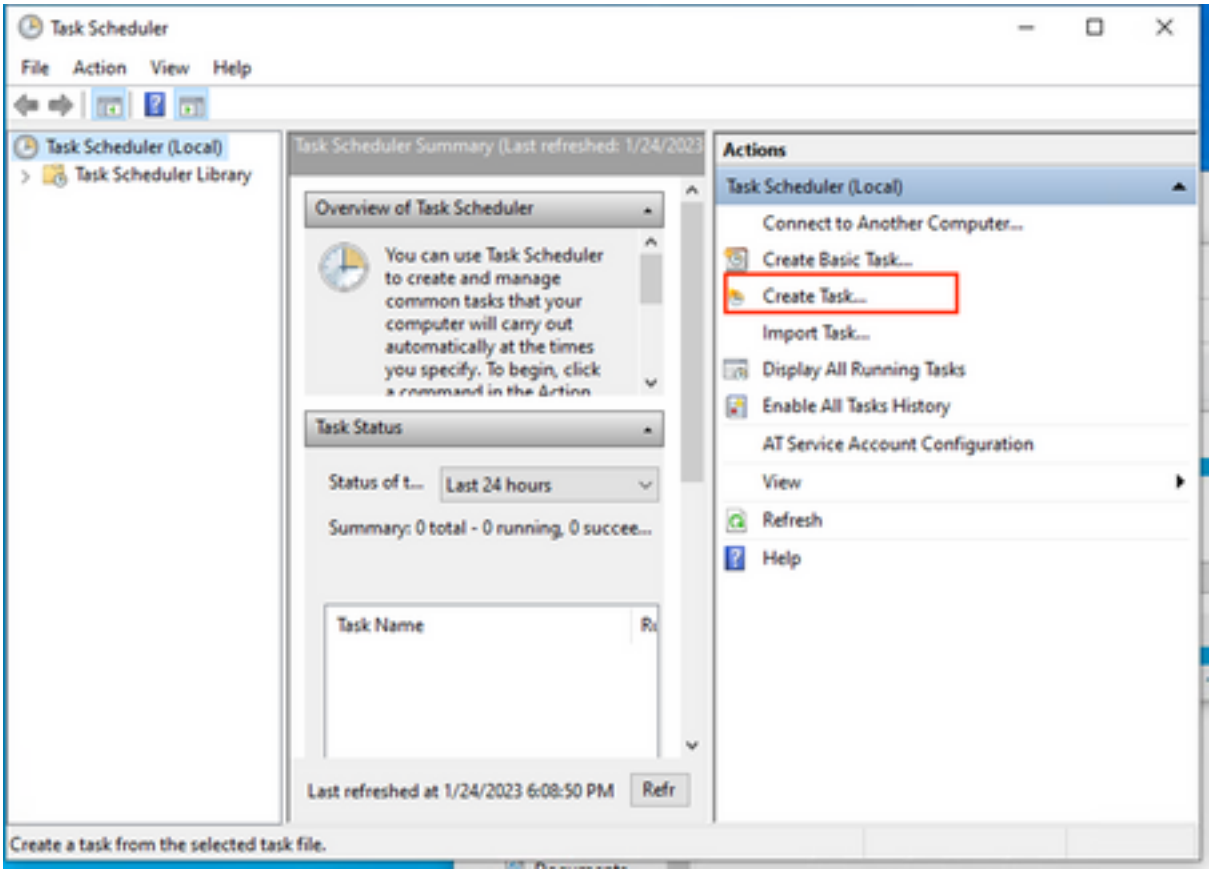


Ga voor het volgende configuratiestuk naar uw Windows-apparaat en open een nieuw Notepad-bestand om deze lijnen toe te voegen:

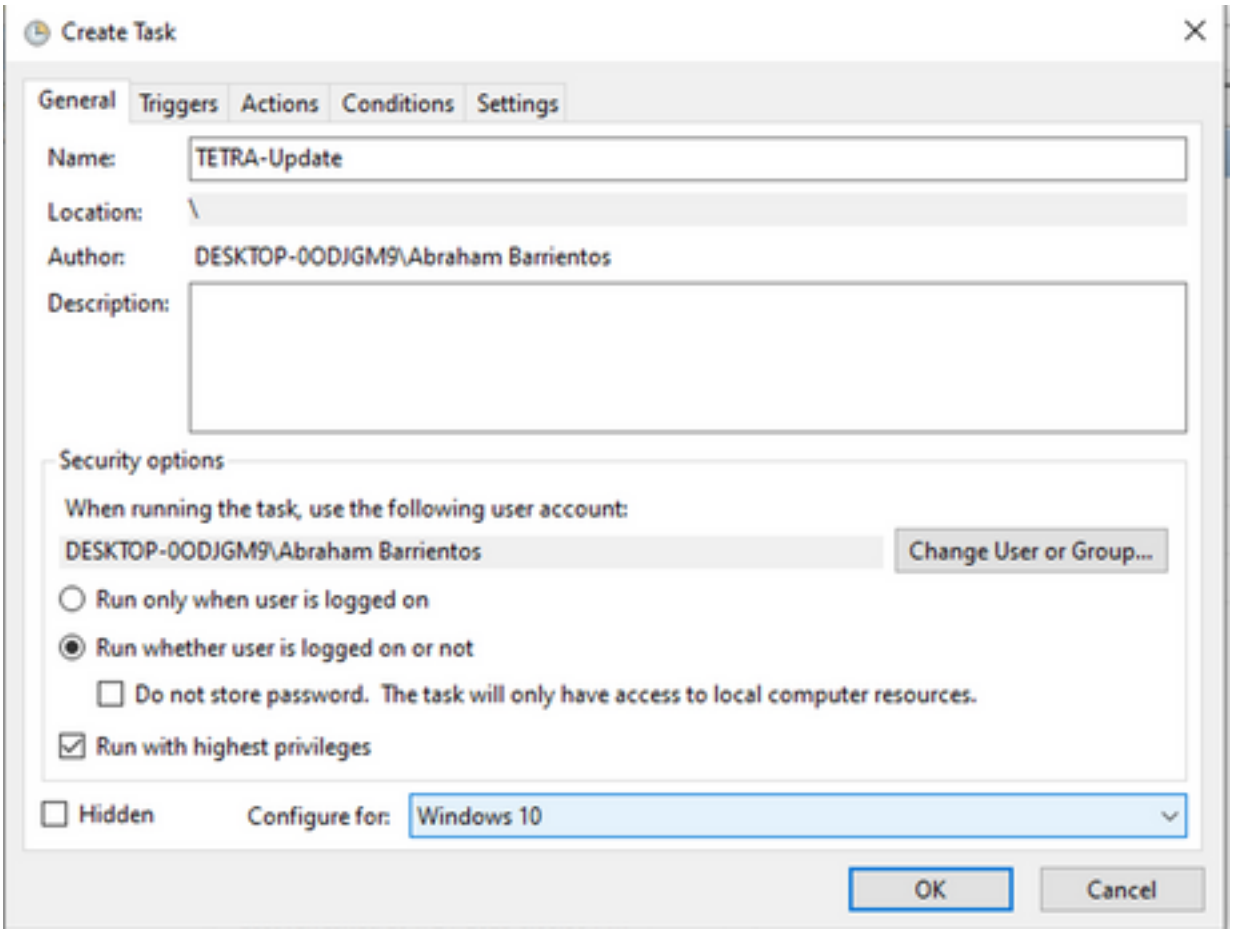
```
cd C:\Program Files\Cisco\AMP\8.1.3.21242
sfc.exe -forceupdate
```

Let op: u moet de Secure Endpoint versie (8.1.3.21242v) gebruiken die overeenkomt met de huidige geïnstalleerde versie op het endpoint. Als u niet zeker bent van de versie, kunt u op het pictogram **Secure Endpoint** gebruikersinterface tandwiel en vervolgens op het **tabblad Statistieken** klikken om de huidige versie te controleren. Nadat u deze regels aan de blocnote hebt toegevoegd, klikt u op **Bestand** en vervolgens op **Opslaan als.** Klik vervolgens op **Opslaan als type** en selecteer **Alle bestanden**. Typ tot slot de naam van het bestand en sla het op als de extensie .BAT. Als u het bestand wilt opslaan onder C:\ map, moet u blocnote met Admin rechten uitvoeren. Als zijaantekening kunt u het BAT-bestand uitvoeren om de TETRA-update als test af te dwingen.

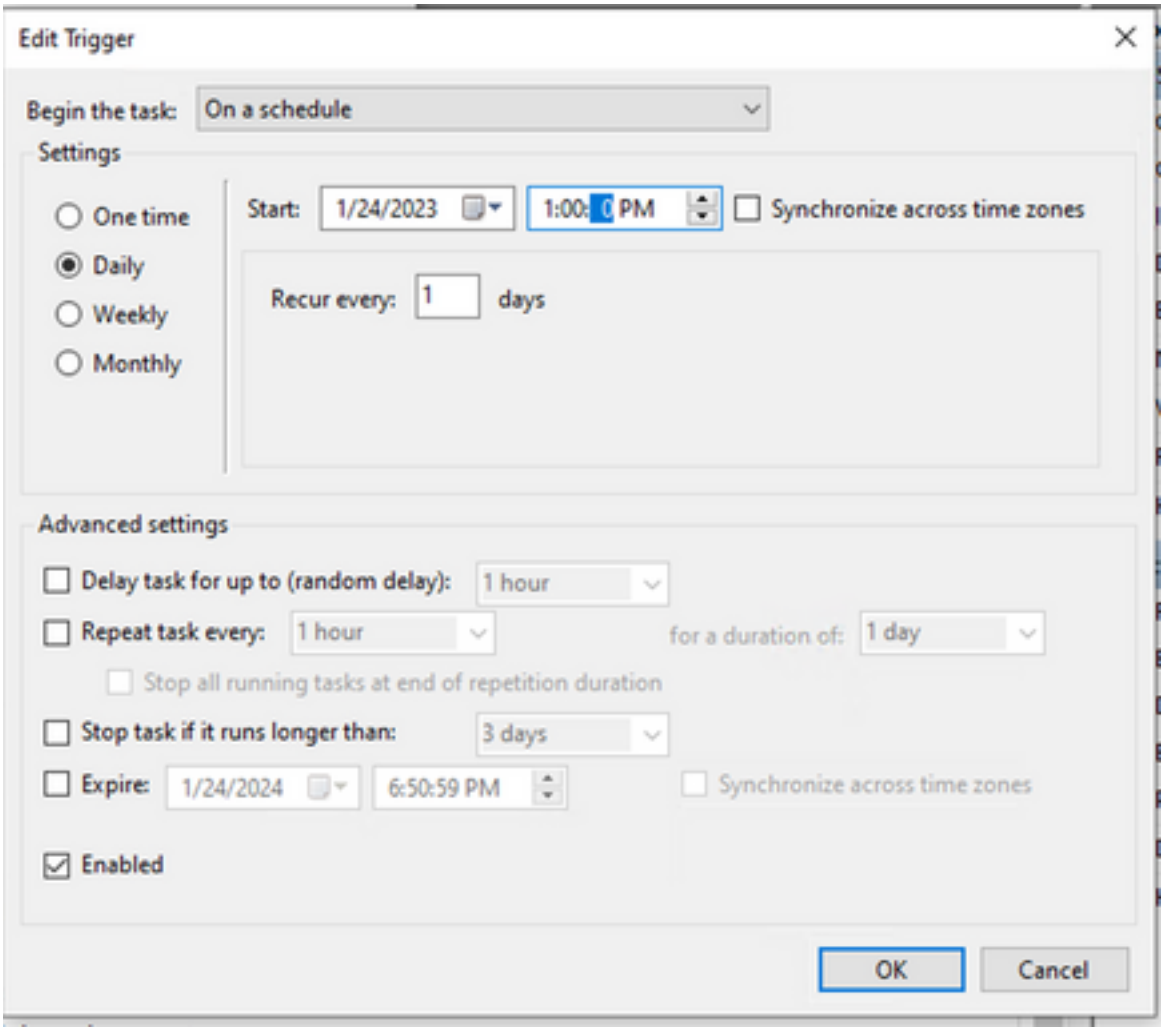
Open de Scheduler voor taken openen op uw Windows-computer en klik op **Een taak maken** aan de rechterkolom.



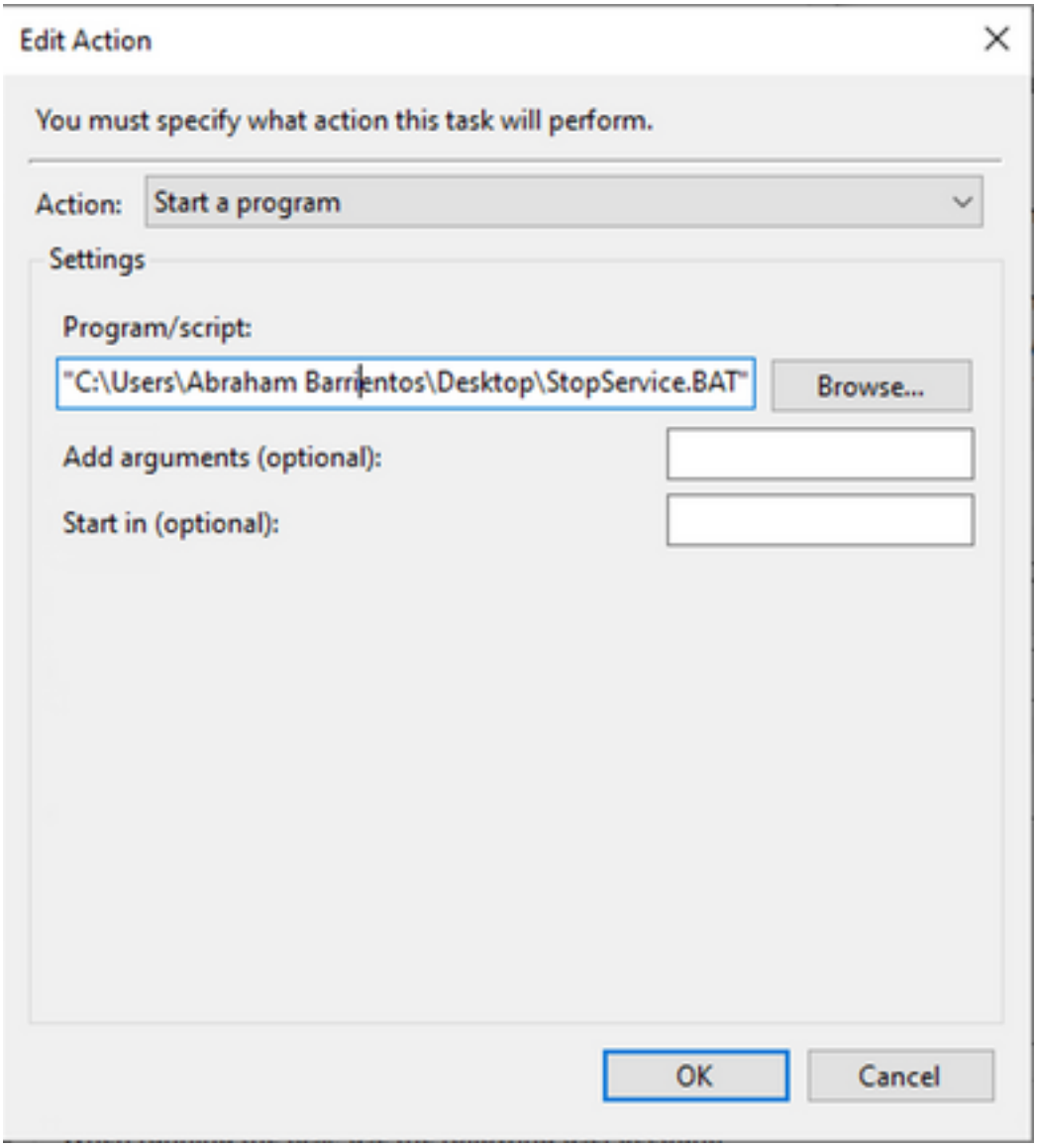
Typ onder het **tabblad Algemeen** de naam voor deze taak en selecteer **Uitvoeren wanneer een gebruiker is aangemeld of niet**. Controleer **Uitvoeren met het** aanvinkvakje **Higherst privelages**. Kies onder **configureren voor** optie het besturingssysteem dat van toepassing is. Voor deze demonstratie werd Windows 10 gebruikt.



Klik onder **het** tabblad **Triggers** op **Nieuwe trigger.** Op de pagina Nieuwe trigger configuratie kunt u de tijd aanpassen wanneer u wilt dat TETRA haar handtekeningen bijwerkt. Bij dit voorbeeld werd een dagelijks schema gebruikt dat om 13.00 uur lokale machinetijd liep. De optie Begindatum definieert wanneer deze taak actief wordt. Klik op **OK** als u klaar bent met de planningsinstellingen**.**



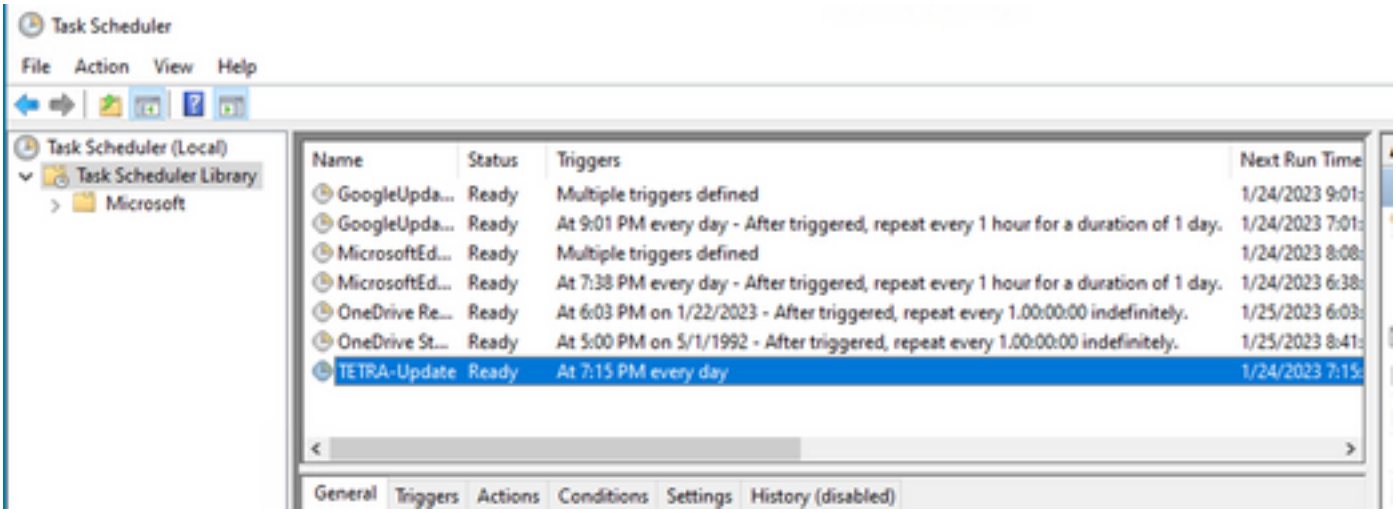
Klik op het tabblad **Acties** op **Nieuwe actie**. Kies op het tabblad **Nieuwe actie een programma** voor de instelling **Actie starten**. Klik onder Programma/instellingen op **Bladeren,** en zoek vervolgens naar het BAT-script. Klik op **OK** om de actie te maken. Laat de rest van de instellingen standaard en klik op **OK** om de taak te maken.



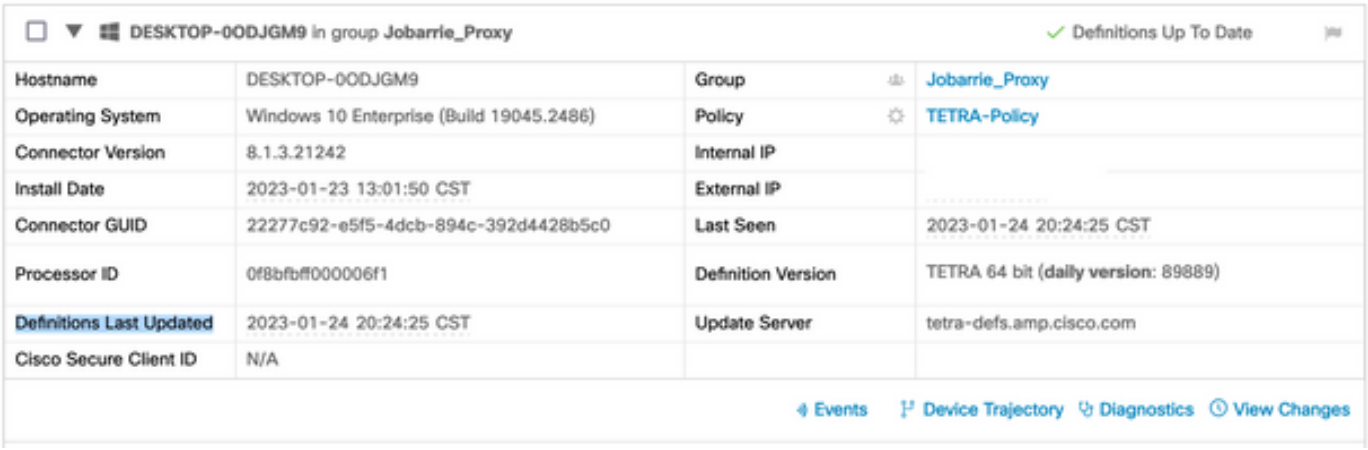
Tot slot vereist deze taakplanner administratieve referenties om de taak te maken omdat "Uitvoeren met hoogste rechten" is geselecteerd. Na verificatie met beheerdersreferenties is de taak klaar om te starten en uit te voeren om de Secure Endpoint-service te vertellen wanneer TETRA moet worden bijgewerkt volgens het ingestelde schema.

Verifiëren

Klik in de linkerkolom op de map **Taakplannerbibliotheek**. Controleer of het schema is gemaakt en weergegeven zoals verwacht.



U kunt het laatste TETRA-definitienummer controleren dat door de connector is gedownload onder **Secure Endpoint User interface > statics** tab. U kunt dit nummer gebruiken om de nieuwste definities die beschikbaar zijn op de console onder **Management > Av Definitions samenvatting** te vergelijken om erachter te komen of apparaat up-to-date is met de nieuwste definities. Een ander alternatief is om de waarde "Definitions Last Update" te monitoren voor het specifieke eindpunt in de Secure Endpoint Console.



Problemen oplossen

Wanneer definities niet worden bijgewerkt zoals verwacht, kunt u een kijkje nemen in de logbestanden om te zoeken naar een TETRA update fout. Om dit te doen, schakel de debug-modus in op de Secure Endpoint-gebruikersinterface onder het tabblad Advanced voordat de tijd voor het starten van de taak Schedule is verstreken. Laat de connector ten minste 20 minuten na de Schedule Task Trigger op deze modus draaien en kijk vervolgens naar het laatste bestand **sfcx.exe.log** onder **C:\Program Files\Cisco\AMP\X.X.X** (waar X.X.X de huidige versie van Secure Endpoint op het systeem is).

De ForceWakeUpdateThreadAbout laat zien dat TETRA wordt geactiveerd door onze Schedule Job om te updaten zoals verwacht. Als u dit logbestand niet ziet, kan er een probleem zijn met betrekking tot de taakconfiguratie voor Windows.

```
(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
```

In het geval dat Schedule Job met succes TETRA activeert om definities bij te werken, moet u zoeken naar een gerelateerde TETRA-fout in de logboeken. Dit is een voorbeeld van een TETRA-foutcode 2200, wat betekent dat de service tijdens het updateproces werd onderbroken. Hoe u algemene TETRA-fouten kunt oplossen valt buiten het bereik van dit document. De links aan het eind van dit document zijn echter nuttige Cisco-artikelen over probleemoplossing TETRA-foutcodes.

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

Gerelateerde informatie

- Problemen oplossen met TETRA-definities en update fouten
- Cisco Secure Endpoint - fout in Tetra Definitions Update met 3000-fout
- TETRA foutcodes - Windows

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.