Configurare un'ora personalizzata per i download TETRA

Sommario

Introduzione

Questo documento descrive come configurare gli endpoint locali per scaricare gli aggiornamenti TETRA in qualsiasi momento per soddisfare i requisiti di utilizzo della larghezza di banda.

Premesse

TETRA è il motore offline per Secure Endpoint che utilizza firme antivirus per fornire protezione agli endpoint. TETRA riceve aggiornamenti quotidiani del suo database delle firme per stare al passo con tutte le nuove minacce in natura. Poiché questi aggiornamenti possono utilizzare una notevole larghezza di banda in ambienti di grandi dimensioni, ogni endpoint casualizza il tempo di download entro l'intervallo di aggiornamento che, per impostazione predefinita, è impostato su 1 ora. Anche se sono disponibili diversi intervalli di aggiornamento da scegliere per il criterio TETRA, non è possibile scegliere un'ora specifica per avviare questo processo di download. Questo documento fornisce una soluzione per forzare TETRA ad aggiornare le sue firme AV con i processi di pianificazione di Windows.

Prerequisiti

Requisiti

Conoscenze base della configurazione dei criteri per gli endpoint sicuri e dei processi di pianificazione di Windows.

Componenti usati

- Console Secure Endpoint Cloud
- Secure Endpoint connector per Windows 8.1.3
- Windows 10 Enterprise

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

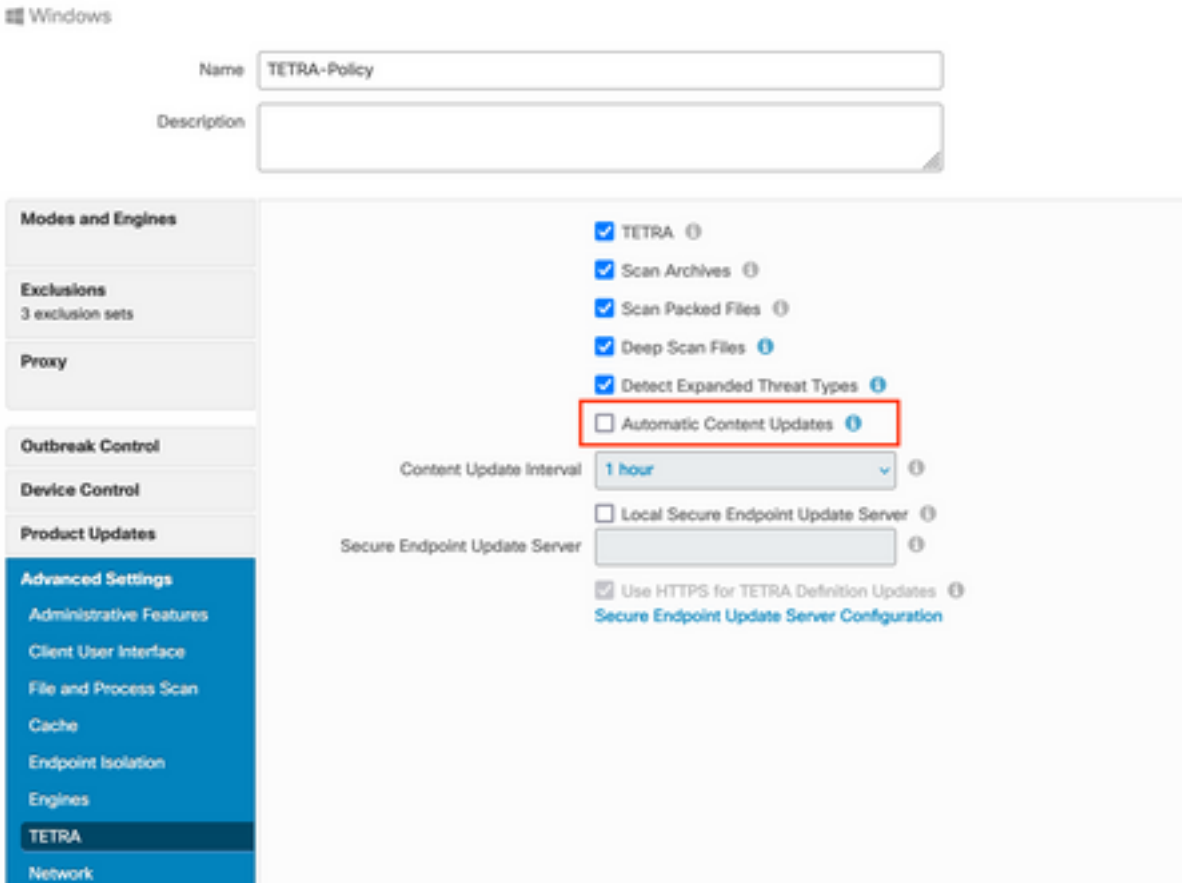
Configurazione

> **Avviso**: come descritto nella sezione in background, gli aggiornamenti TETRA possono utilizzare una notevole larghezza di banda. Per impostazione predefinita, Secure Endpoint tenta di ridurre questo impatto e di casualizzare gli aggiornamenti TETRA all'interno dell'intervallo di aggiornamento che è impostato su 1 ora per impostazione predefinita. Non è consigliabile forzare tutti i connettori ad aggiornare contemporaneamente le definizioni, soprattutto in ambienti di grandi dimensioni. Questo processo deve essere utilizzato solo in situazioni particolari in cui è fondamentale controllare l'ora dell'aggiornamento. In qualsiasi altro scenario, è preferibile eseguire aggiornamenti automatici.

Scegliere un criterio Endpoint sicuro da configurare per il tempo di download TETRA personalizzato.

> **Nota**: questa configurazione viene eseguita in base a un criterio e ha effetto su tutti gli endpoint del criterio. Pertanto, si consiglia di includere tutti i dispositivi che si desidera controllare per gli aggiornamenti TETRA personalizzati nello stesso criterio dell'endpoint sicuro.

Accedere a Secure Endpoint Management Console e selezionare **Gestione > Criteri**, quindi cercare il criterio scelto e fare clic su **Modifica**. Una volta visualizzata la pagina di configurazione dei criteri, passare alla **sezione TETRA**. In questa sezione deselezionare la casella di controllo **Aggiornamenti automatici contenuto** e **salvare** il criterio. Tutto ciò è correlato alla configurazione nella console di Secure Endpoint Cloud.

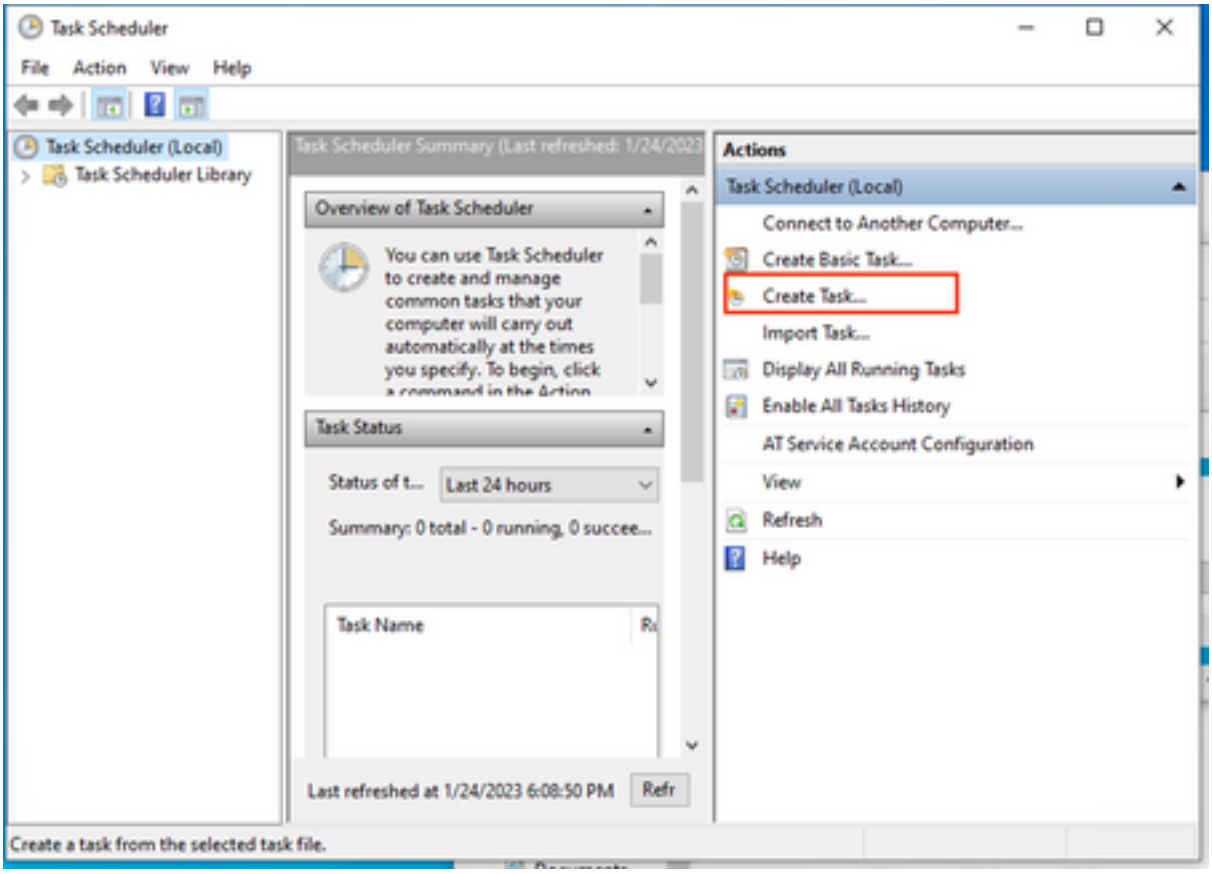


Per la configurazione successiva, accedere al dispositivo Windows e aprire un nuovo file del Blocco note per aggiungere le righe seguenti:

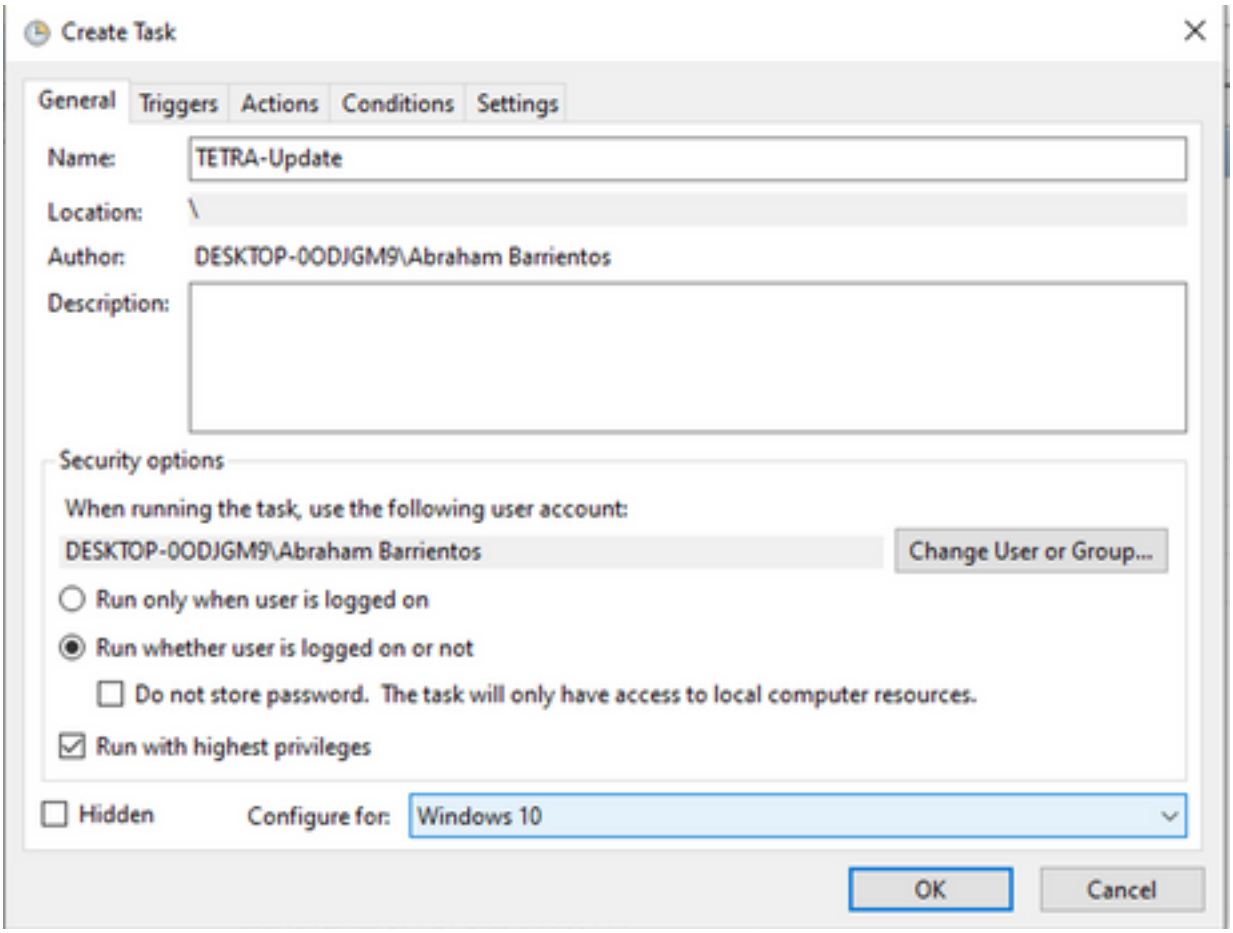
```
cd C:\Program Files\Cisco\AMP\8.1.3.21242
sfc.exe -forceupdate
```

Si noti che è necessario utilizzare la versione dell'endpoint protetto (8.1.3.21242v per questo esempio) che corrisponde alla versione attualmente installata sull'endpoint. Se non si è certi della versione, è possibile fare clic sull'icona a forma di ingranaggio dell'interfaccia utente di **Secure Endpoint** e quindi sulla **scheda Statistiche** per controllare la versione corrente. Dopo aver aggiunto queste righe al blocco note, fare clic su **File**, quindi su **Salva con nome.** Quindi fare clic su **Salva come tipo** e selezionare **Tutti i file**. Digitare infine il nome del file e salvarlo con l'estensione BAT. Se si desidera salvare il file nella cartella C:\, è necessario eseguire il Blocco note con privilegi di amministratore. Come nota rapida è possibile eseguire il file BAT per forzare l'aggiornamento TETRA per come test.

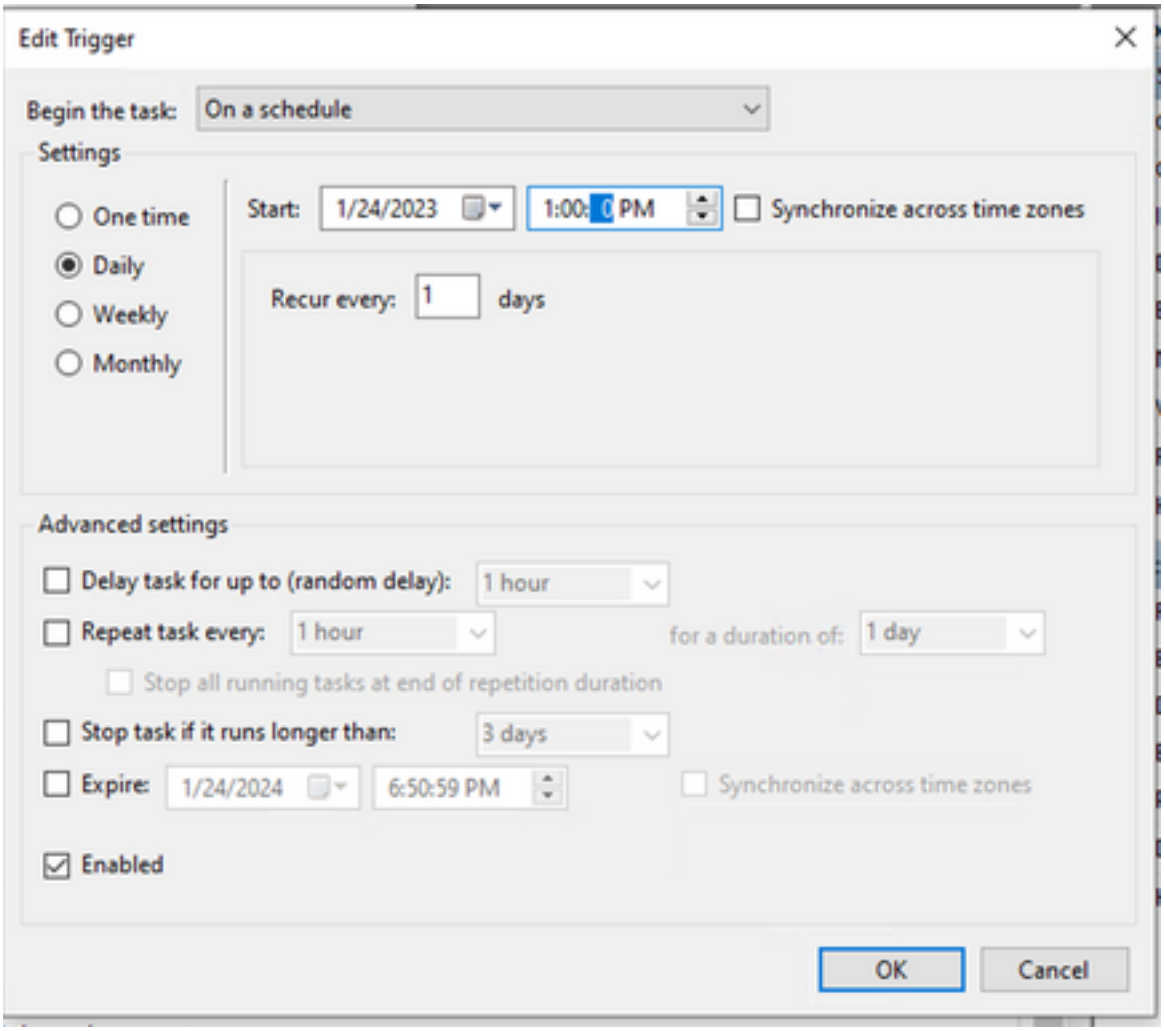
Aprire l'Utilità di pianificazione Aprire l'Utilità di pianificazione sul computer Windows e fare clic su **Crea un** pulsante **Attività** nella colonna destra.



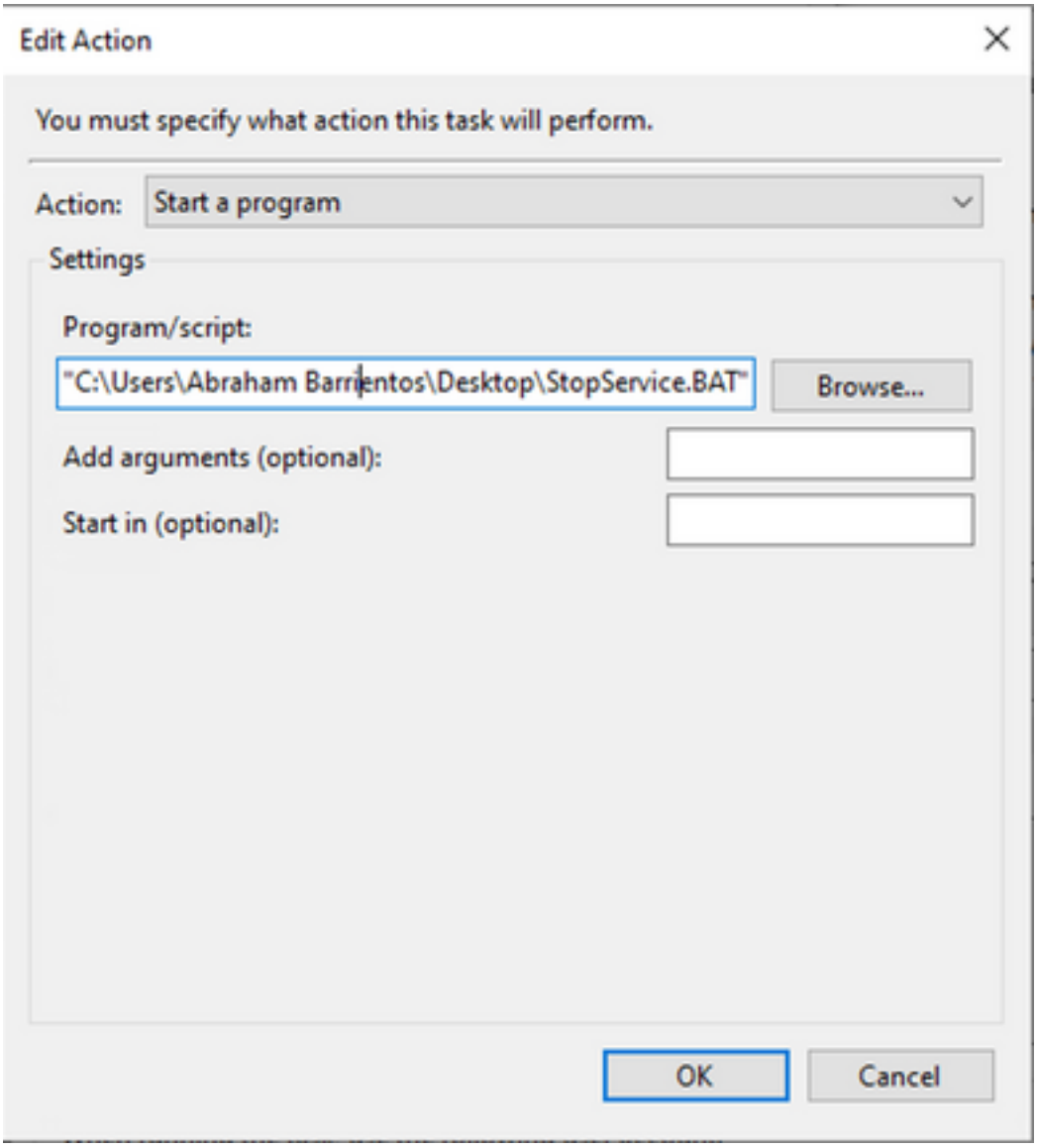
In **Scheda Generale**, digitare il nome dell'attività e selezionare **Esegui ogni volta che l'utente viene registrato o meno**. Selezionare **la** casella di controllo **Esegui con i privilegi più elevati**. In **Configura per**, scegliere il sistema operativo applicabile. Per questa dimostrazione è stato utilizzato Windows 10.



Nella scheda **Trigger** fare clic su **Nuovo trigger.** Nella pagina Configurazione nuovo trigger è possibile personalizzare il momento in cui si desidera che TETRA aggiorni le proprie firme. Per questo esempio, è stata utilizzata una pianificazione giornaliera eseguita alle 13 ora locale del computer. L'opzione Data inizio definisce quando l'attività diventa attiva. Al termine, fare clic su **OK.**



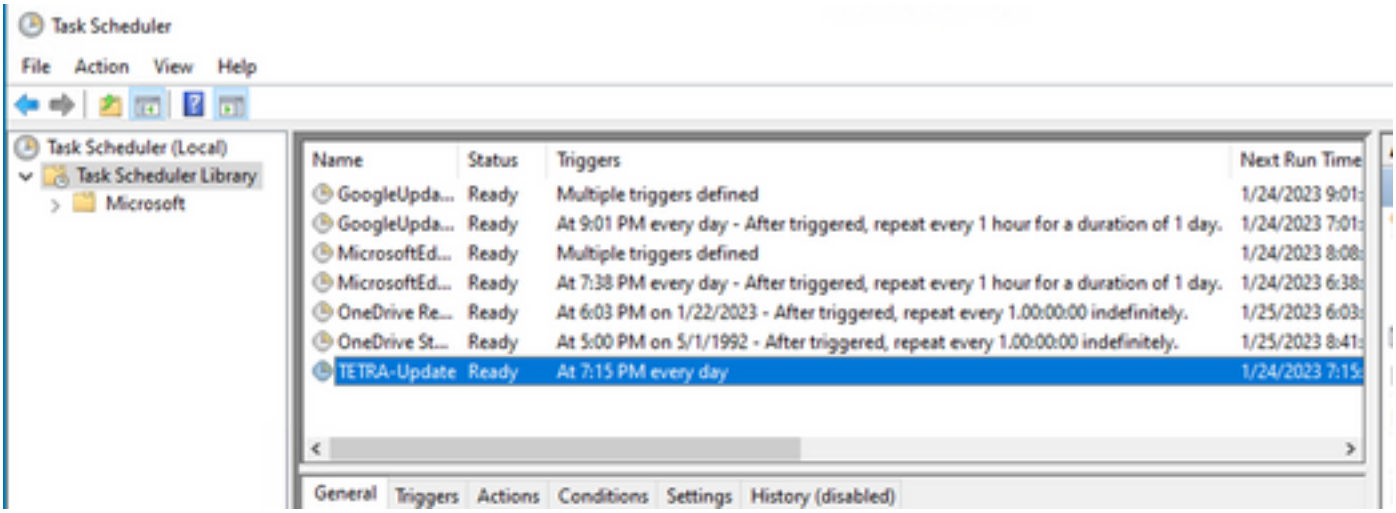
Nella scheda **Azioni** fare clic su **Nuova azione**. Nella scheda **Nuova azione** scegliere **Avvia un programma** per l'impostazione **Azione**. In Programmi/Impostazioni fare clic su **Sfoglia,** quindi cercare e selezionare lo script BAT. Fare clic su **OK** per creare l'azione. Lasciare le altre impostazioni predefinite e fare clic su **OK** per creare l'operazione.



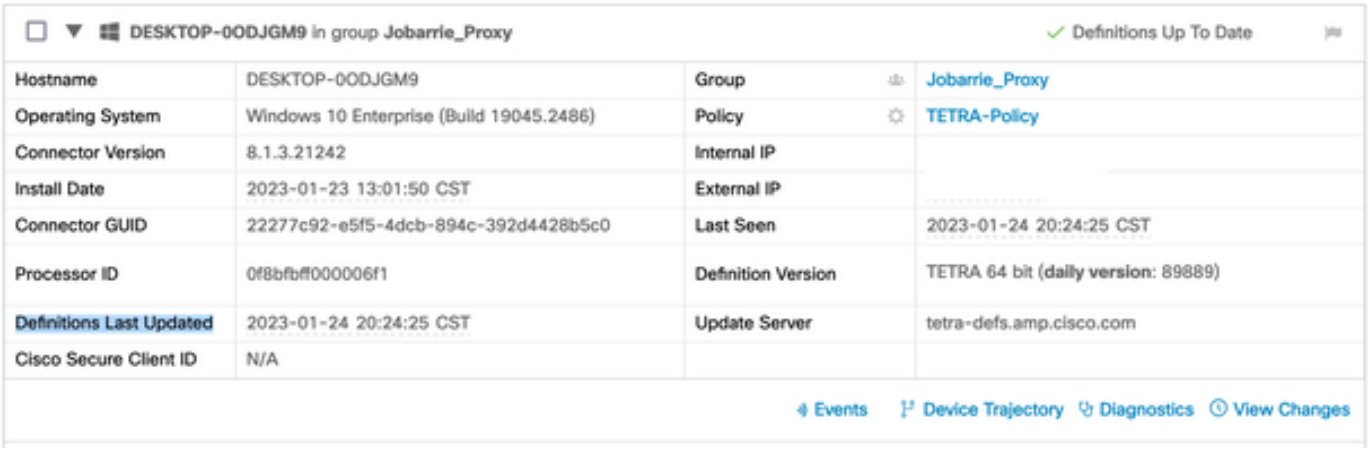
L'Utilità di pianificazione richiede infine credenziali amministrative per la creazione dell'attività, poiché è stata selezionata l'opzione "Esegui con i privilegi più elevati". Dopo l'autenticazione con le credenziali di amministratore, l'attività è pronta per essere eseguita per indicare al servizio Endpoint protetto quando aggiornare TETRA in base alla pianificazione configurata.

Verifica

Fare clic sulla cartella **Libreria Utilità di pianificazione** nella colonna sinistra. Verificare che la pianificazione sia stata creata ed elencata come previsto.



Èpossibile controllare l'ultimo numero di definizione TETRA scaricato dal connettore in **Interfaccia utente endpoint sicuro >** scheda **Statistiche**. È possibile utilizzare questo numero per confrontare le definizioni più recenti disponibili sulla console in **Gestione > Riepilogo definizioni Av** per scoprire se il dispositivo è aggiornato con le definizioni più recenti. In alternativa è possibile monitorare il valore "Ultimo aggiornamento definizioni" per l'endpoint specifico nella console dell'endpoint sicuro.



Risoluzione dei problemi

Quando le definizioni non vengono aggiornate come previsto, è possibile esaminare i log per cercare un errore di aggiornamento TETRA. A tale scopo, abilitare la modalità di debug nell'interfaccia utente dell'endpoint sicuro nella scheda Avanzate prima dell'ora di attivazione dell'attività Pianificazione. Lasciare che il connettore venga eseguito in questa modalità per almeno 20 minuti dopo l'attivazione dell'attività di pianificazione e quindi esaminare il file **sfcx.exe.log** più recente disponibile in **C:\Program Files\Cisco\AMP\X.X.X** (dove X.X.X è la versione corrente di Secure Endpoint nel sistema).

ForceWakeUpdateThreadAbout indica che TETRA è attivato dal processo di pianificazione per l'aggiornamento previsto. Se il registro non viene visualizzato, è possibile che si tratti di un problema relativo alla configurazione dell'attività di pianificazione di 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
```

Nel caso in cui il processo di pianificazione attivi correttamente TETRA per aggiornare le definizioni, è necessario cercare eventuali errori TETRA correlati nei log. Questo è un esempio di un codice di errore TETRA 2200 che indica che il servizio è stato interrotto durante il processo di aggiornamento. La risoluzione dei problemi relativi agli errori TETRA generali esula tuttavia dalle finalità del presente documento. I collegamenti alla fine di questo documento sono utili articoli di Cisco sulla risoluzione dei problemi relativi ai codici di errore TETRA.

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

Informazioni correlate

- Risoluzione dei problemi relativi agli errori di aggiornamento delle definizioni TETRA
- Cisco Secure Endpoint - Errore di aggiornamento delle definizioni Tetra con errore 3000
- Codici di errore TETRA - Windows

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).