Configuración de una hora personalizada para las descargas TETRA

Contenido

Introducción

Este documento describe cómo configurar los terminales locales para descargar las actualizaciones de TETRA en cualquier momento deseado para cumplir con los requisitos de uso de ancho de banda.

Antecedentes

TETRA es el motor fuera de línea para Secure Endpoint que utiliza firmas antivirus para proporcionar protección a los terminales. TETRA recibe actualizaciones diarias a su base de datos de firmas para mantenerse al día con todas las nuevas amenazas en el mundo. Estas actualizaciones pueden utilizar un ancho de banda significativo en entornos grandes, por lo tanto, cada terminal aleatoriza el tiempo para la descarga dentro del intervalo de actualización que, de forma predeterminada, está configurado en 1 hora. Aunque hay diferentes intervalos de actualización disponibles para elegir en la política de TETRA, no es posible elegir un momento específico para activar este proceso de descarga. Este documento proporciona una solución alternativa para forzar a TETRA a actualizar sus firmas AV con trabajos de Programación de Windows.

Prerequisites

Requirements

Conocimientos básicos sobre la configuración de directivas de terminales seguros y los trabajos de programación de Windows.

Componentes Utilizados

- Consola de nube de terminal seguro
- Conector de terminal seguro para Windows 8.1.3

- Windows 10 Enterprise

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

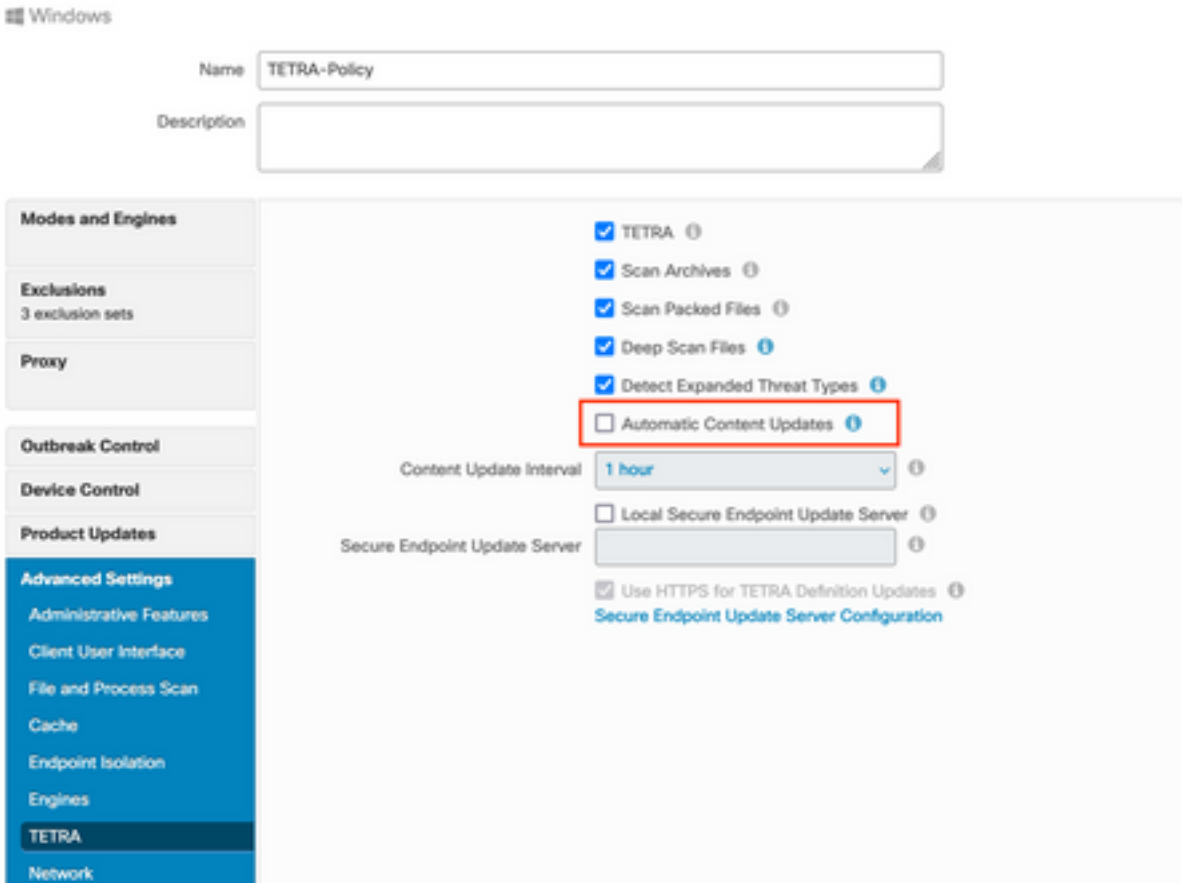
Configurar

> **Advertencia**: Como se describe en la sección de fondo, las actualizaciones de TETRA pueden consumir un ancho de banda significativo. De forma predeterminada, Secure Endpoint intenta reducir este impacto y randomizar las actualizaciones de TETRA dentro del intervalo de actualización que está configurado en 1 hora de forma predeterminada. No se recomienda obligar a todos los conectores a actualizar las definiciones al mismo tiempo, especialmente en entornos grandes. Este proceso solo se debe utilizar en situaciones especiales en las que es fundamental controlar la hora de la actualización. En cualquier otro caso, es preferible realizar actualizaciones automáticas.

Elija una política de terminal seguro para configurar para el tiempo de descarga de TETRA personalizado.

> **Nota**: Tenga en cuenta que esta configuración se realiza según una política y que todos los terminales de esta política se ven afectados. Por lo tanto, se recomienda colocar todos los dispositivos que desee controlar para las actualizaciones TETRA personalizadas en la misma política de terminal seguro.

Inicie sesión en Secure Endpoint Management Console y navegue hasta **Administración > Políticas**, busque la política que ha elegido utilizar y haga clic en **editar**. Una vez que esté en la página de configuración de políticas, navegue hasta la **sección TETRA**. En esta sección, desmarque la casilla de verificación **Actualizaciones automáticas de contenido** y **guarde** la política. Todo esto está relacionado con la configuración de la consola de Secure Endpoint Cloud.

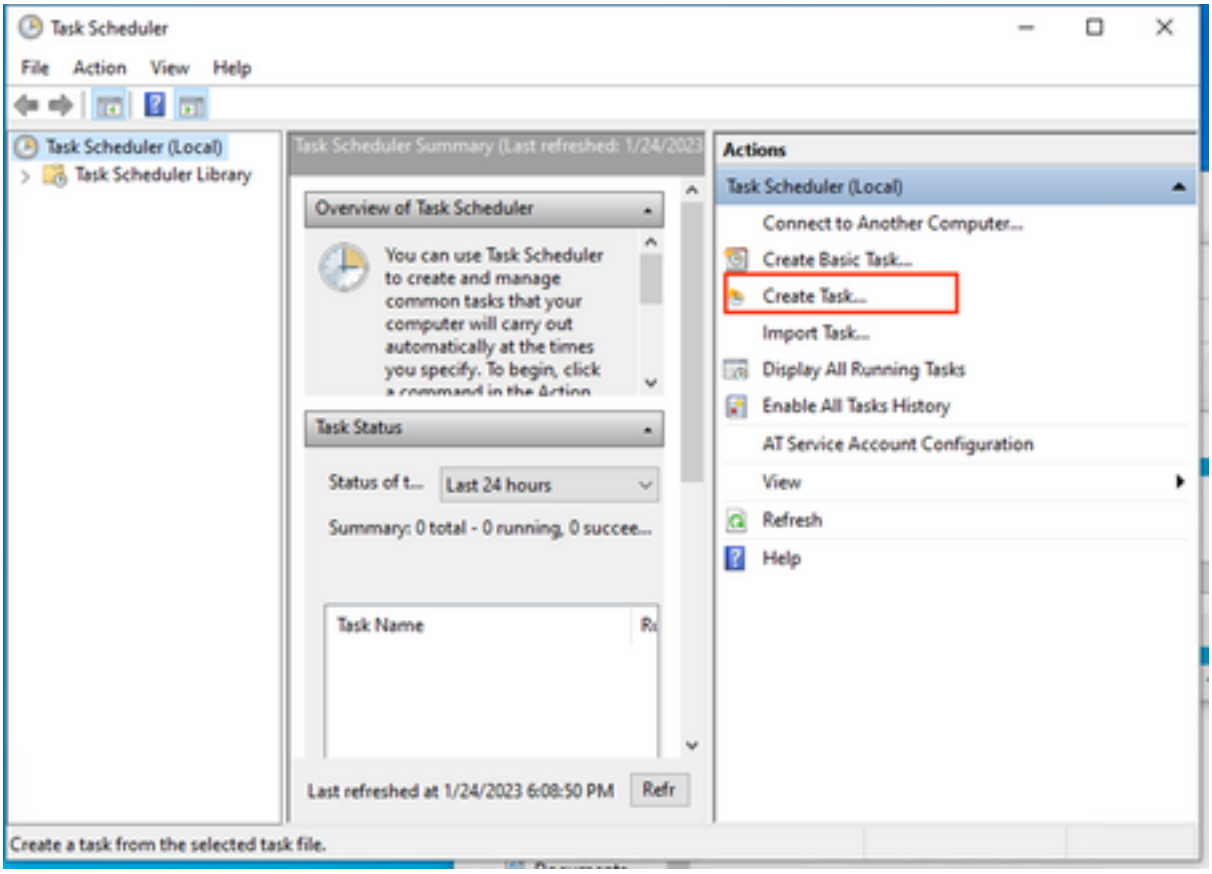


Para la siguiente configuración, acceda al dispositivo Windows y abra un nuevo archivo de Bloc de notas para agregar estas líneas:

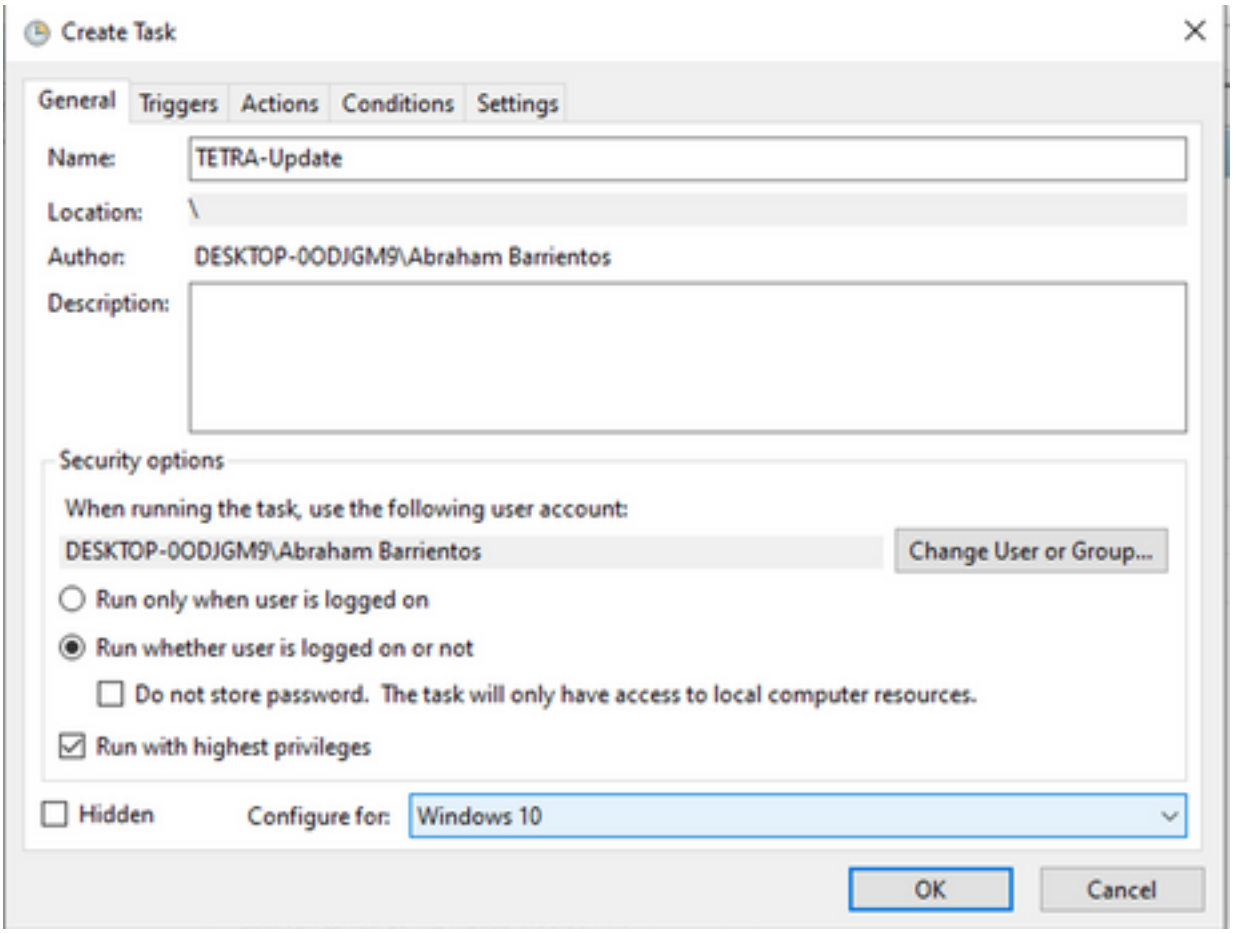
```
cd C:\Program Files\Cisco\AMP\8.1.3.21242
sfc.exe -forceupdate
```

Tenga en cuenta que debe utilizar la versión de Secure Endpoint (8.1.3.21242v para este ejemplo) que coincida con la versión instalada actual en el terminal. Si no está seguro de la versión, puede hacer clic en el icono de engranaje de la interfaz de usuario de **Secure Endpoint** y, a continuación, en la **ficha estática** para comprobar la versión actual. Una vez agregadas estas líneas al bloc de notas, haga clic en **Archivo** y, a continuación, en **Guardar como. A continuación, haga clic en Guardar como tipo** y seleccione **Todos los archivos**. Por último, escriba el nombre del archivo y guárdelo como extensión .BAT. Si desea guardar el archivo en la carpeta C:\, debe ejecutar el bloc de notas con privilegios de administrador. Como nota al margen, puede ejecutar el archivo BAT para forzar la actualización de TETRA como prueba.

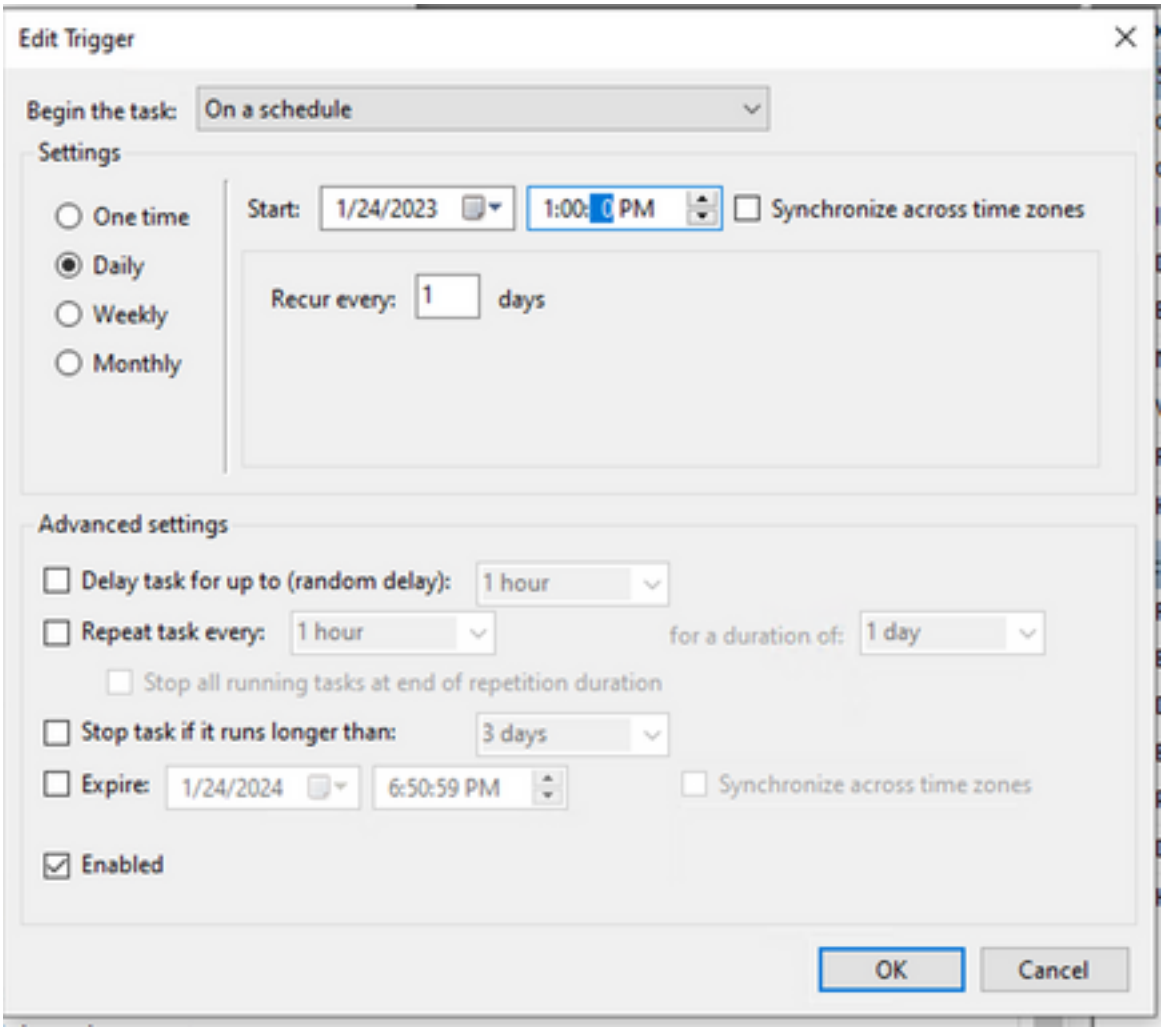
Abra Planificar tarea Abrir Programador de tareas en su equipo de Windows y haga clic en el botón **Crear una tarea** situado en la columna derecha.



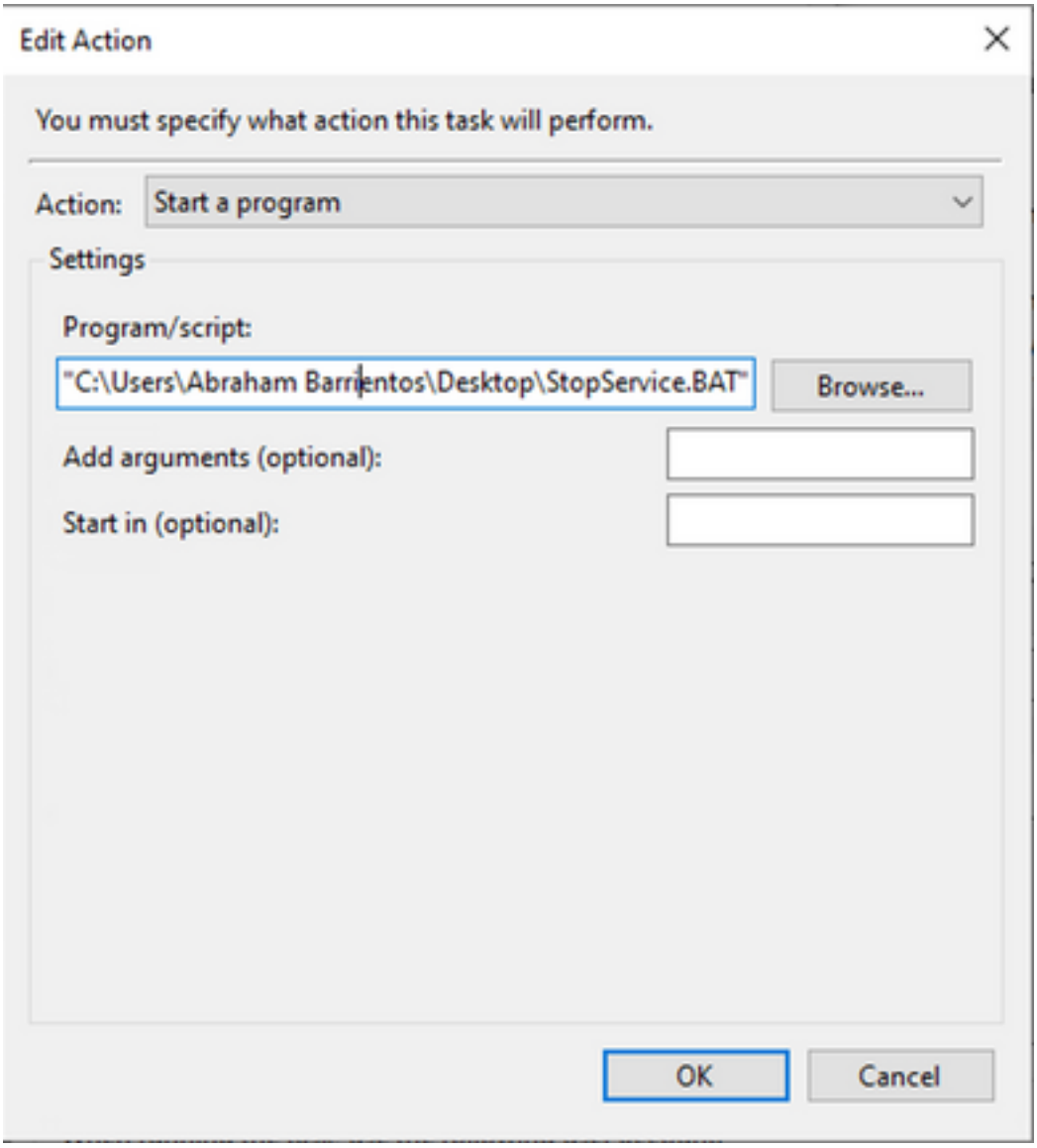
En la **ficha General**, escriba el nombre de esta tarea y seleccione **Ejecutar siempre que se registre o no el usuario**. Marque **la** casilla de verificación **Ejecutar con los mayores privilegios**. En la opción **Configure for**, elija el sistema operativo que corresponda. Para esta demostración, se utilizó Windows 10.



En la ficha **Desencadenadores**, haga clic en **Nuevo desencadenador.** En la página Nueva configuración del disparador, puede personalizar el momento en que desea que TETRA actualice sus firmas. Para este ejemplo, se utilizó una programación diaria que se ejecuta a las 13:00, hora local del equipo. La opción Fecha de inicio define cuándo se activa esta tarea. Cuando haya terminado con la configuración de la programación, haga clic en **aceptar.**



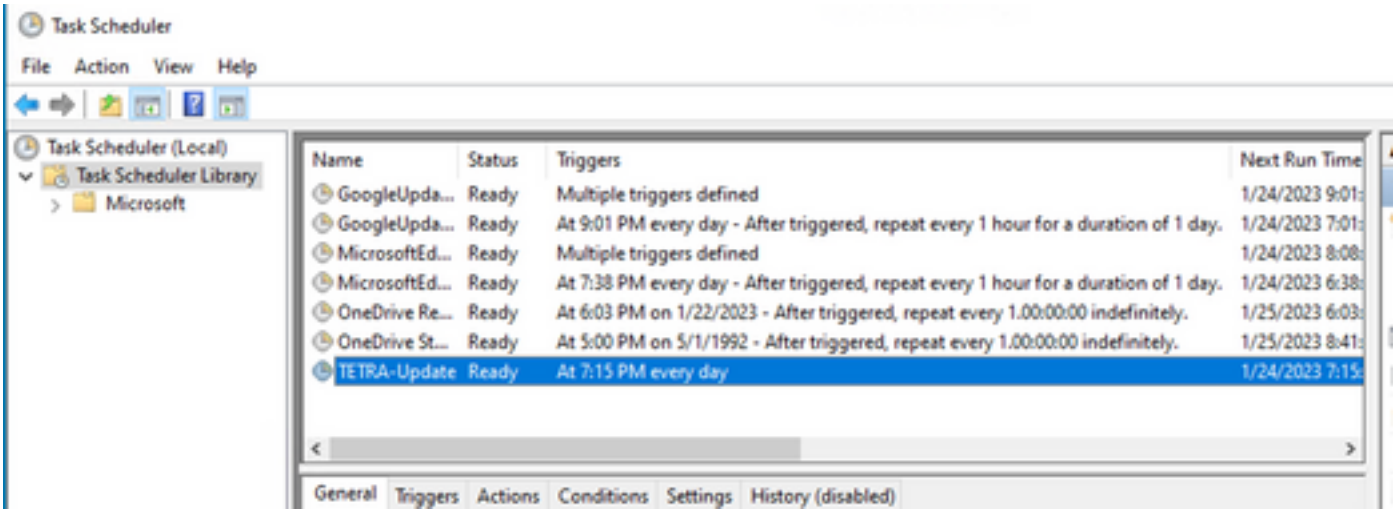
En la ficha **Acciones**, haga clic en **Nueva acción**. En la ficha **Nueva acción**, elija **Iniciar un programa** para la configuración **Acción**. En Program/Settings (Programa/Configuración), haga clic en **Browse** y busque y, a continuación, seleccione el script BAT. Haga clic en **Aceptar** para crear la acción. Deje el resto de la configuración predeterminada y haga clic en **Aceptar** para crear la tarea.



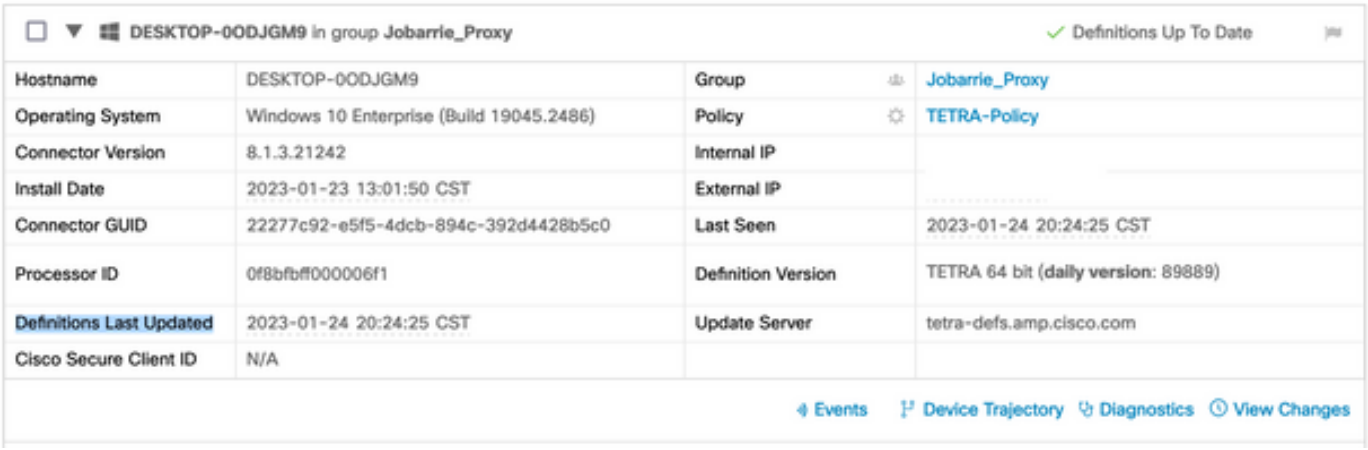
Por último, el Programador de tareas requiere credenciales administrativas para crear la tarea, ya que se ha seleccionado "Ejecutar con privilegios más altos". Después de la autenticación con credenciales de administrador, la tarea está lista para ejecutarse y ejecutarse para indicar al servicio Secure Endpoint cuándo actualizar TETRA según la programación configurada.

Verificación

Haga clic en la carpeta **Biblioteca del Programador de tareas** en la columna de la izquierda. Compruebe que la programación se ha creado y aparece como se esperaba.



Puede verificar el último número de definición de TETRA descargado por el conector en la pestaña **Interfaz de usuario de terminal seguro > estática**. Puede utilizar este número para comparar las definiciones más recientes disponibles en la consola bajo **Administración > Resumen de definiciones de Av** para averiguar si el dispositivo está actualizado con las definiciones más recientes. Otra alternativa es supervisar el valor "Definiciones actualizadas por última vez" para el terminal concreto en Secure Endpoint Console.



Troubleshoot

Cuando las definiciones no se actualizan como se esperaba, puede echar un vistazo a los registros para buscar un error de actualización de TETRA. Para ello, habilite el modo de depuración en la interfaz de usuario de Secure Endpoint en la ficha Opciones avanzadas antes de la hora de activación de la tarea Programar. Deje que el conector se ejecute en este modo durante al menos 20 minutos después del Desencadenador de tareas de programación y luego eche un vistazo al último archivo **sfcx.exe.log** ubicado en **C:\Program Files\Cisco\AMP\X.X.X** (donde X.X.X es la versión actual de Secure Endpoint en el sistema).

ForceWakeUpdateThreadAbout nos muestra que TETRA es activado por nuestro trabajo de programación para actualizarse según lo esperado. Si no ve este registro, puede ser un problema relacionado con la configuración de tareas de programación de 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
```

En caso de que Planificar Trabajo active con éxito TETRA para actualizar las definiciones, debe buscar cualquier error TETRA relacionado en los registros. Este es un ejemplo de un código de error TETRA 2200 que significa que el servicio se interrumpió durante el proceso de actualización. La forma de resolver los errores generales de TETRA está fuera del alcance de este documento, sin embargo, los links al final de este documento son artículos útiles de Cisco sobre cómo resolver los códigos de error de TETRA.

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

Información Relacionada

- Troubleshooting de fallas de actualización de definiciones TETRA
- Cisco Secure Endpoint - Error de actualización de definiciones de Tetra con error 3000
- Códigos de error de TETRA - Windows

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).