# Configure uma hora personalizada para downloads de TETRA

## Contents



## Introduction

Este documento descreve como configurar endpoints locais para baixar atualizações TETRA a qualquer momento desejado para atender aos requisitos com uso de largura de banda.

## Informações de Apoio

O TETRA é o mecanismo off-line do Secure Endpoint que usa assinaturas de antivírus para fornecer proteção aos endpoints. A TETRA recebe atualizações diárias na sua base de dados de assinaturas para acompanhar todas as novas ameaças em estado selvagem. Essas atualizações podem usar largura de banda significativa em ambientes grandes, portanto, cada endpoint torna aleatório o tempo de download dentro do intervalo de atualização que, por padrão, é definido como 1 hora.  Mesmo que diferentes intervalos de atualização estejam disponíveis para escolher na política TETRA, não é possível escolher um horário específico para acionar esse processo de download. Este documento fornece uma solução alternativa para forçar a TETRA a atualizar suas assinaturas AV com trabalhos do Agendamento do Windows.

## Prerequisites

### Requirements

Conhecimento Básico da configuração de política de Ponto de Extremidade Seguro e dos trabalhos do Agendamento do Windows.

### Componentes Utilizados

- Console de nuvem de endpoint seguro
- Conector de ponto de extremidade seguro para Windows 8.1.3
- Windows 10 Enterprise

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

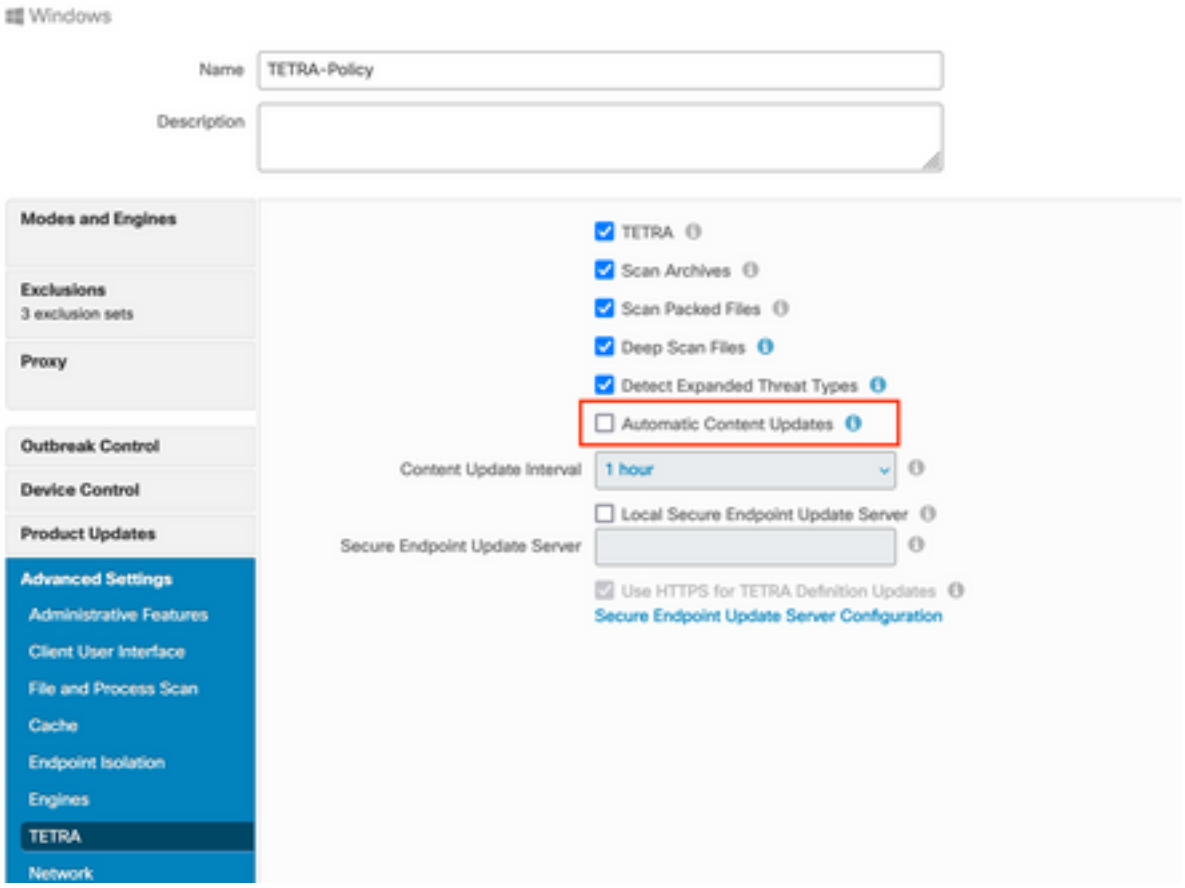
# Configurar

> **Aviso**: conforme descrito na seção de background, as atualizações TETRA podem consumir uma largura de banda significativa. Por padrão, o Secure Endpoint tenta reduzir esse impacto e tornar aleatórias as atualizações TETRA dentro do intervalo de atualização, que é definido como 1 hora por padrão. Não é recomendável forçar todos os conectores a atualizar as definições ao mesmo tempo, especialmente em ambientes grandes. Esse processo deve ser usado somente em situações especiais em que seja crítico controlar o tempo da atualização. Em qualquer outro cenário de caso, as atualizações automáticas são preferíveis.

Escolha uma política de Ponto de Extremidade Seguro para configurar o tempo de download TETRA personalizado.

> **Observação**: lembre-se de que essa configuração é feita com base em políticas e todos os endpoints nessa política são afetados. Portanto, é recomendável colocar todos os dispositivos que você deseja controlar para atualizações TETRA personalizadas na mesma política de endpoint seguro.

Efetue login no Console do Secure Endpoint Management e navegue para **Gerenciamento** > **Políticas**, depois procure a política que você escolheu usar, clique em **editar**. Quando estiver na página de configuração de política, navegue até a **Seção TETRA**. Nesta seção, desmarque a caixa de seleção **Atualizações automáticas de conteúdo** e **salve** a diretiva. Tudo isso está relacionado à configuração no console Secure Endpoint Cloud.

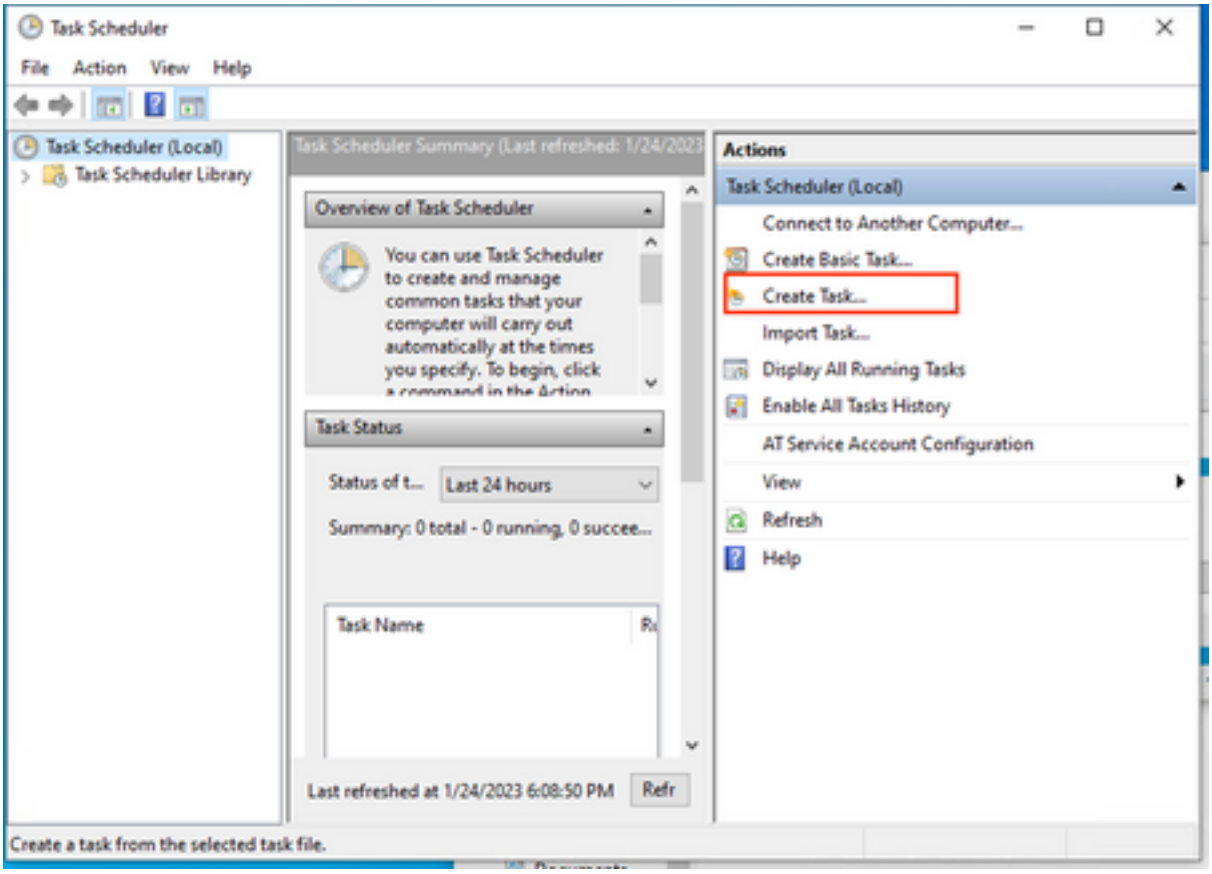



Para a próxima configuração, acesse seu dispositivo Windows e abra um novo arquivo do Bloco de Notas para adicionar estas linhas:

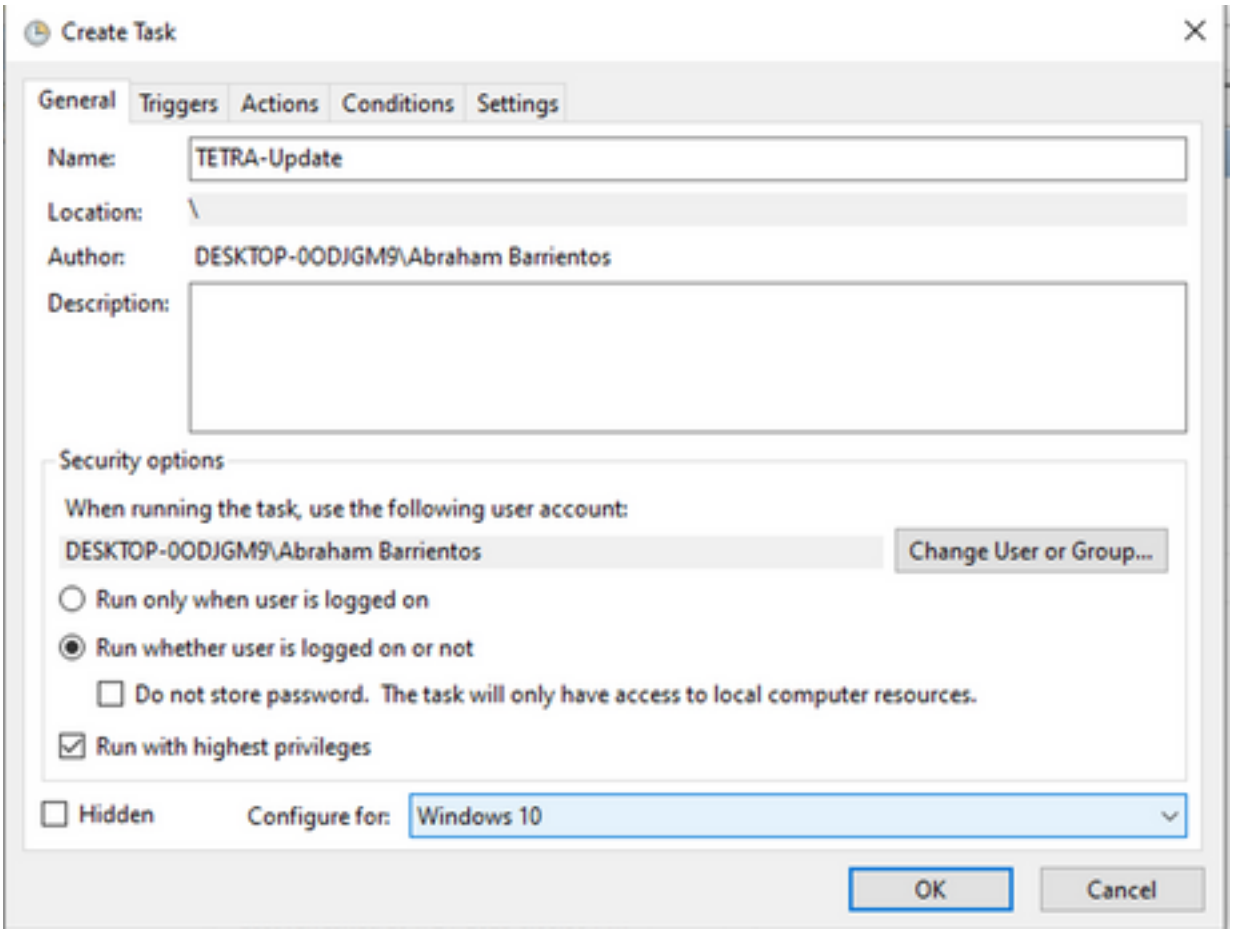
```
cd C:\Program Files\Cisco\AMP\8.1.3.21242
sfc.exe -forceupdate
```

Observe que você precisa usar a versão do Secure Endpoint ( 8.1.3.21242v para este exemplo ) que corresponda à versão instalada no momento no endpoint. Se não tiver certeza da versão, você pode clicar no ícone do equipamento da interface do usuário do **Secure Endpoint** e, em seguida, na **guia Statics** para verificar a versão atual. Depois de adicionar essas linhas ao bloco de notas, clique em **Arquivo** e em **Salvar como. Em seguida, clique em Salvar como um tipo** e selecione **Todos os arquivos**. Por fim, digite o nome do arquivo e salve-o como extensão .BAT. Se quiser salvar o arquivo na pasta C:\, você precisará executar o notepad com privilégios de Administrador. Como nota lateral, você pode executar o arquivo BAT para forçar a atualização TETRA para como um teste.

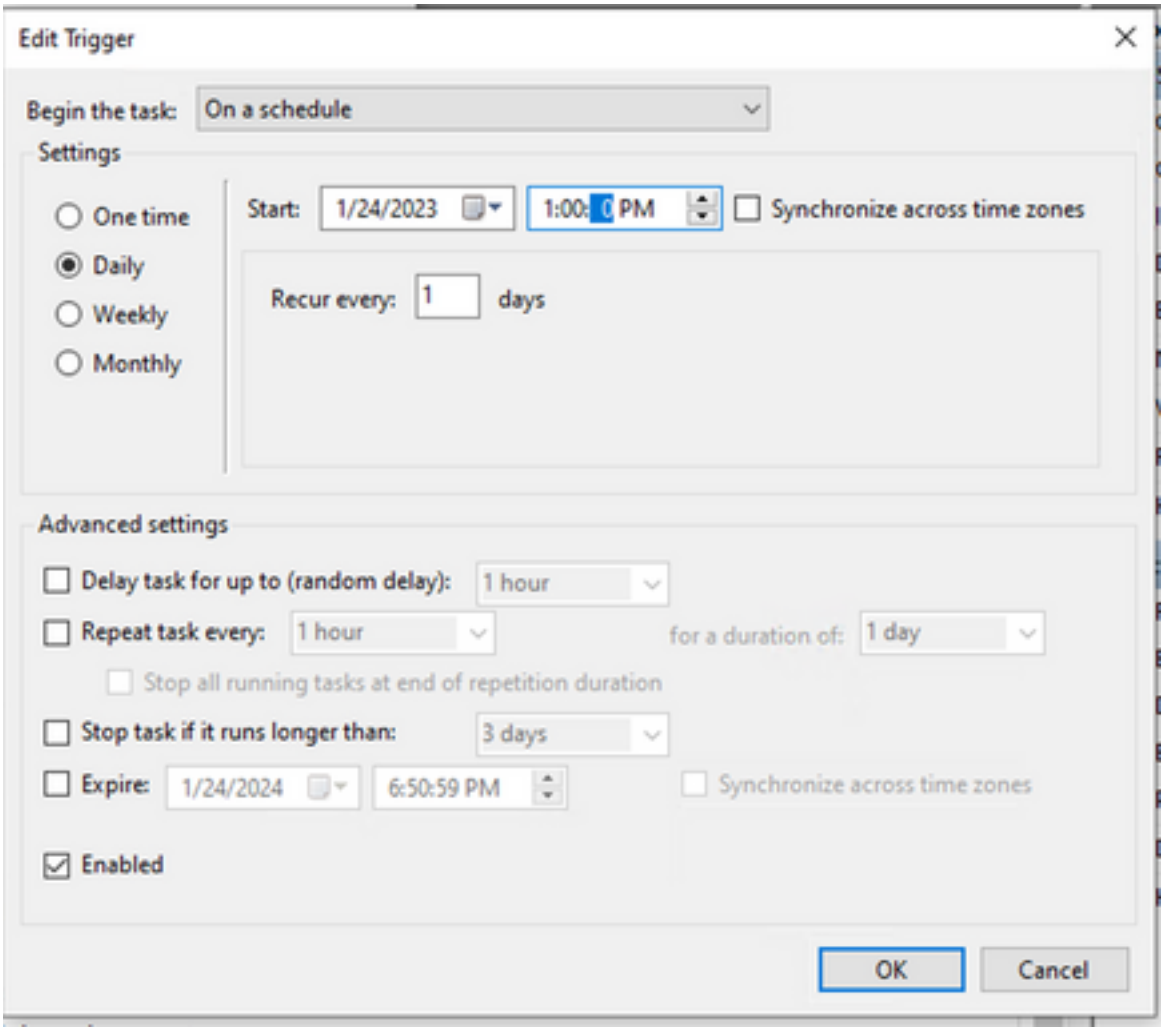
Abra o Agendamento de Tarefas Abrir Agendador de Tarefas na máquina com o Windows e clique no botão **Criar uma Tarefa** localizado na coluna direita.



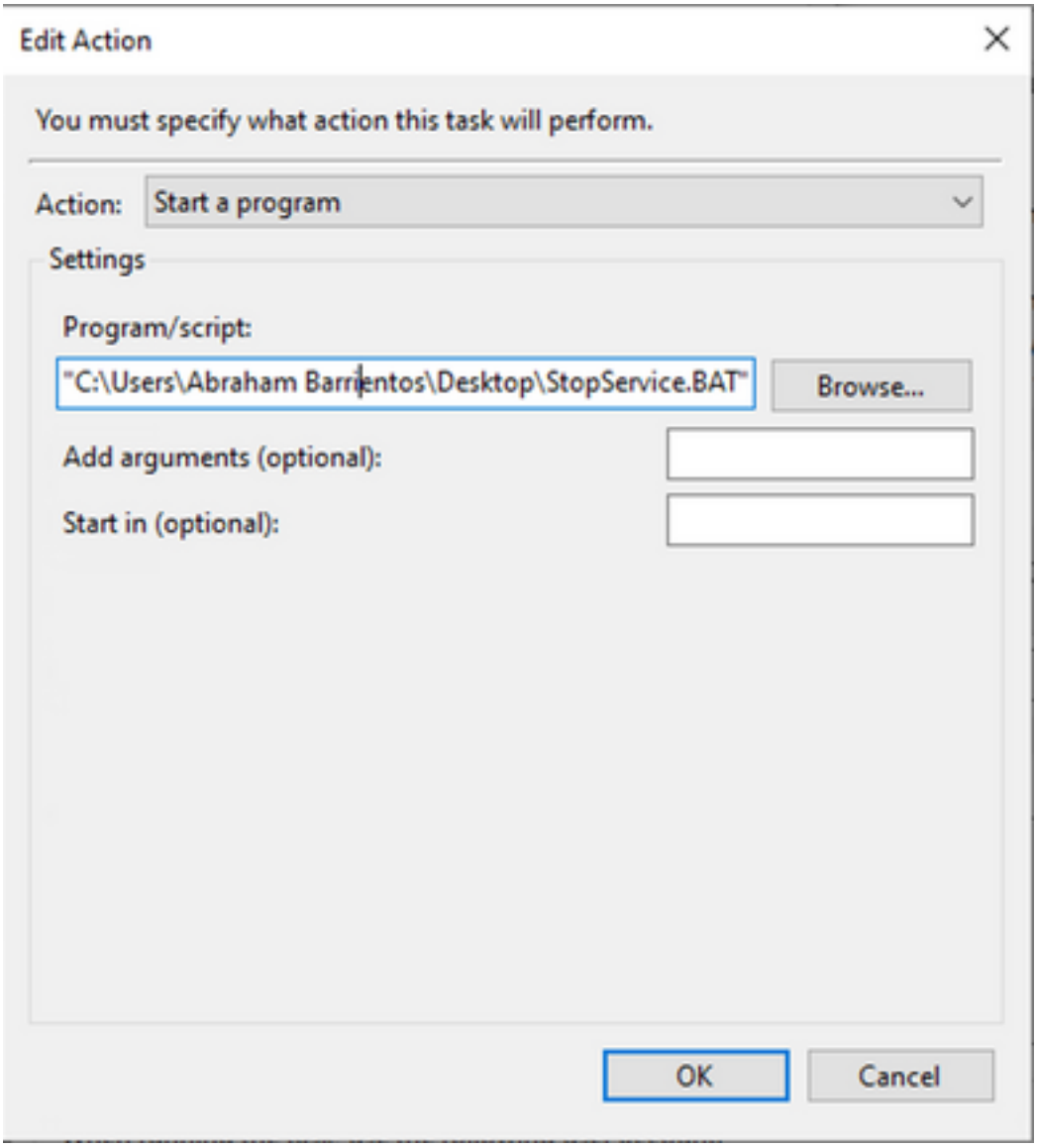

Em **Guia Geral**, digite o nome desta Tarefa e selecione **Executar sempre que o usuário estiver conectado ou não**. Marque a caixa de seleção **Run with the higherst privelages**. Na opção **configure for**, escolha o sistema operacional aplicável. Para esta demonstração, foi usado o Windows 10.



Na guia **Triggers**, clique em **New Trigger.** Na página Nova configuração de gatilho, você pode personalizar o horário em que deseja que o TETRA atualize suas assinaturas. Para este exemplo, foi usada uma programação diária executada às 13:00 hora da máquina local. A opção Data de início define quando esta tarefa se torna ativa. Quando terminar de usar as configurações de agendamento, clique em **ok.**



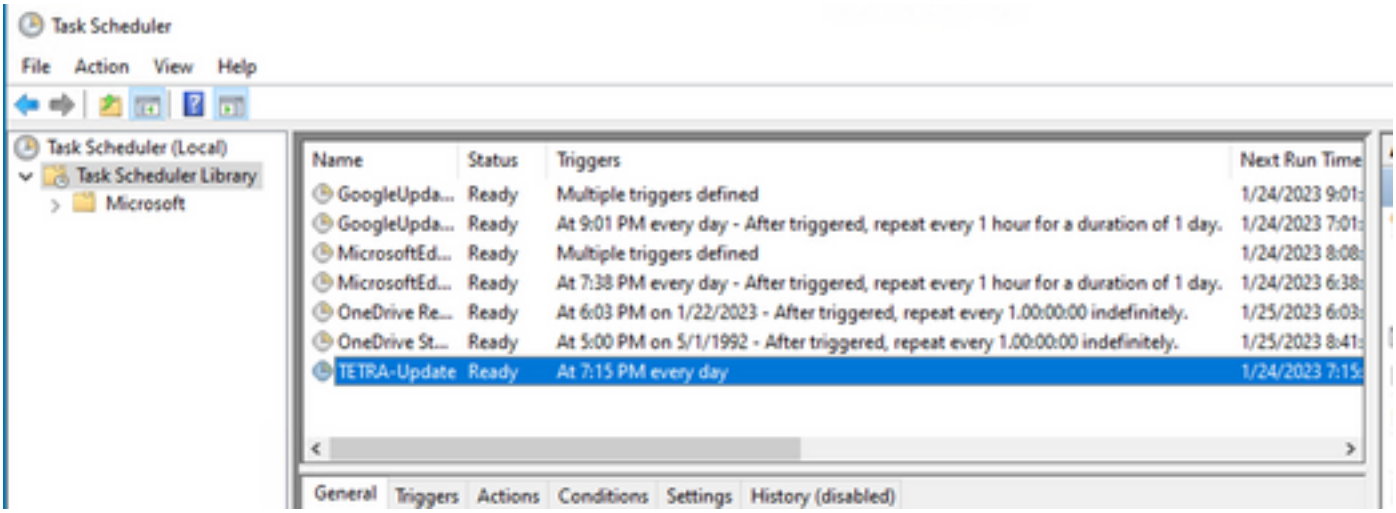

Na guia **Actions**, clique em **New Action**. Na guia **Nova ação**, escolha **Iniciar um programa** para a configuração **Ação**. Em Program/Settings (Programas/Configurações), clique em **Browse (Procurar)** e pesquise e selecione o script BAT. Clique em **Ok** para criar a ação. Deixe o restante das configurações padrão e clique em **Ok** para criar a Tarefa.



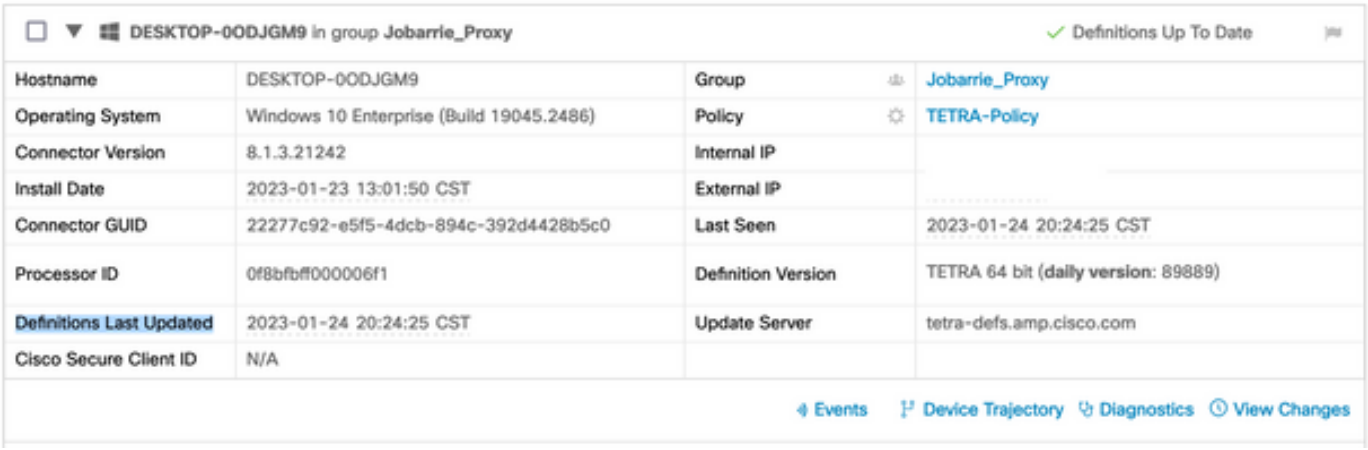

Finalmente, este Agendador de Tarefas requer credenciais administrativas para criar a tarefa, pois "Executar com privilégios mais altos" foi selecionado. Após a autenticação com credenciais de administrador, a tarefa está pronta para ser executada e executada para informar ao serviço de Ponto de Extremidade Seguro quando atualizar o TETRA de acordo com o agendamento configurado.

## Verificar

Clique na pasta **Biblioteca do Agendador de Tarefas** na coluna esquerda. Verifique se o agendamento foi criado e listado como esperado.




Você pode verificar o número de definição TETRA mais recente baixado pelo conector na guia **Secure Endpoint User interface > statics**. Você pode usar esse número para comparar as definições mais recentes disponíveis no console em **Management > Av Definitions summary** para descobrir se o dispositivo está atualizado com as definições mais recentes. Outra alternativa é monitorar o valor de "Definições Atualizadas pela Última Vez" para o endpoint específico no Console de Endpoint Seguro.




# Troubleshoot

Quando as definições não são atualizadas como esperado, você pode dar uma olhada nos logs para procurar um erro de atualização de TETRA. Para fazer isso, habilite o modo de depuração na interface de usuário do Secure Endpoint na guia Avançado antes da hora de disparo da tarefa Agendar. Deixe o conector executar nesse modo por pelo menos 20 minutos após o disparador de tarefa de agendamento e examine o arquivo **sfcx.exe.log** mais recente localizado em **C:\Program Files\Cisco\AMP\X.X.X** (onde X.X.X é a versão atual do Secure Endpoint no sistema).

O ForceWakeUpdateThreadAbout nos mostra que o TETRA é acionado pelo nosso Trabalho de Agendamento para atualização conforme esperado. Se esse log não for exibido, pode ser um problema relacionado à configuração da tarefa de agendamento do 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
```

No caso em que a tarefa de agendamento aciona com sucesso o TETRA para atualizar definições, você precisa procurar qualquer erro TETRA relacionado nos logs. Este é um exemplo de um código de erro TETRA 2200, que significa que o serviço foi interrompido durante o processo de atualização. Como solucionar erros gerais de TETRA está fora do escopo deste documento, no entanto, os links no final deste documento são artigos úteis da Cisco sobre solucionar problemas de códigos de erro de TETRA.

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

# Informações Relacionadas

- Troubleshooting de falhas de atualização de definições TETRA
- Cisco Secure Endpoint - Falha de Atualização de Definições Tetra com Erro 3000
- Códigos de erro TETRA - Windows

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.