

# 配置TETRA下载的定义时间

## 目录

[简介](#)

[背景信息](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

## 简介

本文档介绍如何配置本地终端以在任何所需时间下载TETRA更新，以满足带宽使用要求。

## 背景信息

TETRA是安全终端的脱机引擎，它使用防病毒签名为终端提供保护。TETRA每天都会收到其签名数据库的更新，以便及时应对各种新的威胁。这些更新可以在大型环境中使用大量带宽，因此，每个终端在默认设置为1小时的更新间隔内随机化下载时间。即使在TETRA策略上有不同的更新间隔可供选择，也不能选择特定的时间触发此下载过程。本文档提供了强制TETRA使用Windows计划作业更新其AV签名的解决方法。

## 先决条件

### 要求

安全终端策略配置和Windows计划作业的基本知识。

### 使用的组件

- 安全终端云控制台
- 适用于Windows 8.1.3的安全终端连接器
- Windows 10企业版

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 配置

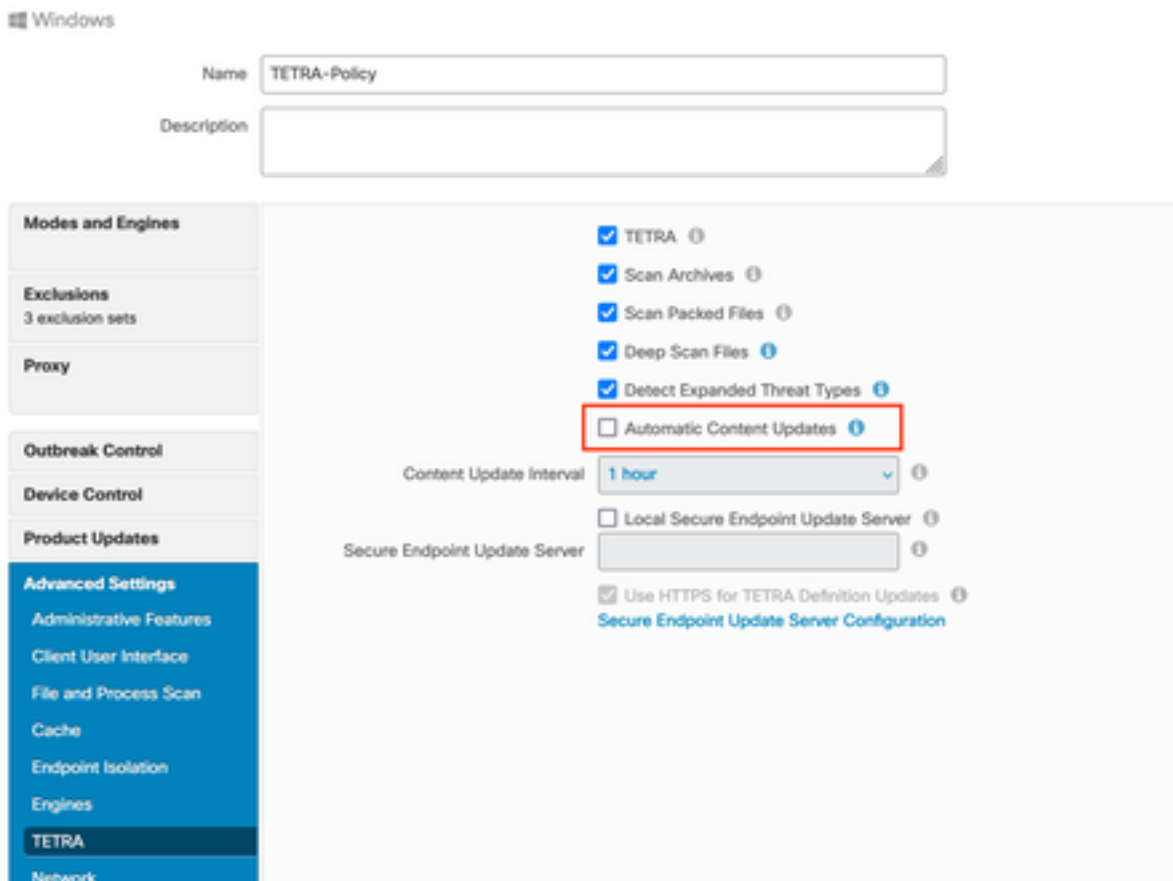
**警告：**如背景部分所述，TETRA更新可能会消耗大量带宽。默认情况下，安全终端会尝试降低此影响，并在默认情况下设置为1小时的更新间隔内随机化TETRA更新。建议不要强制所有

连接器同时更新定义，特别是在大型环境中。此过程仅适用于控制更新时间至关重要的特殊情况。在任何其他情况下，最好是自动更新。

选择要为自定义TETRA下载时间配置的安全终端策略。

**注意：**请注意，此配置是根据策略完成的，此策略中的所有终端都会受到影响。因此，建议将所有要控制自定义TETRA更新的设备放在同一安全终端策略上。

登录到安全终端管理控制台并导航到**Management > Policies**，然后搜索您选择要使用的策略，然后单击**edit**。进入策略配置页面后，导航至**TETRA**部分。在此部分下，取消选中**Automatic Content Updates**复选框并**保存**该策略。这与安全终端云控制台上的配置相关。

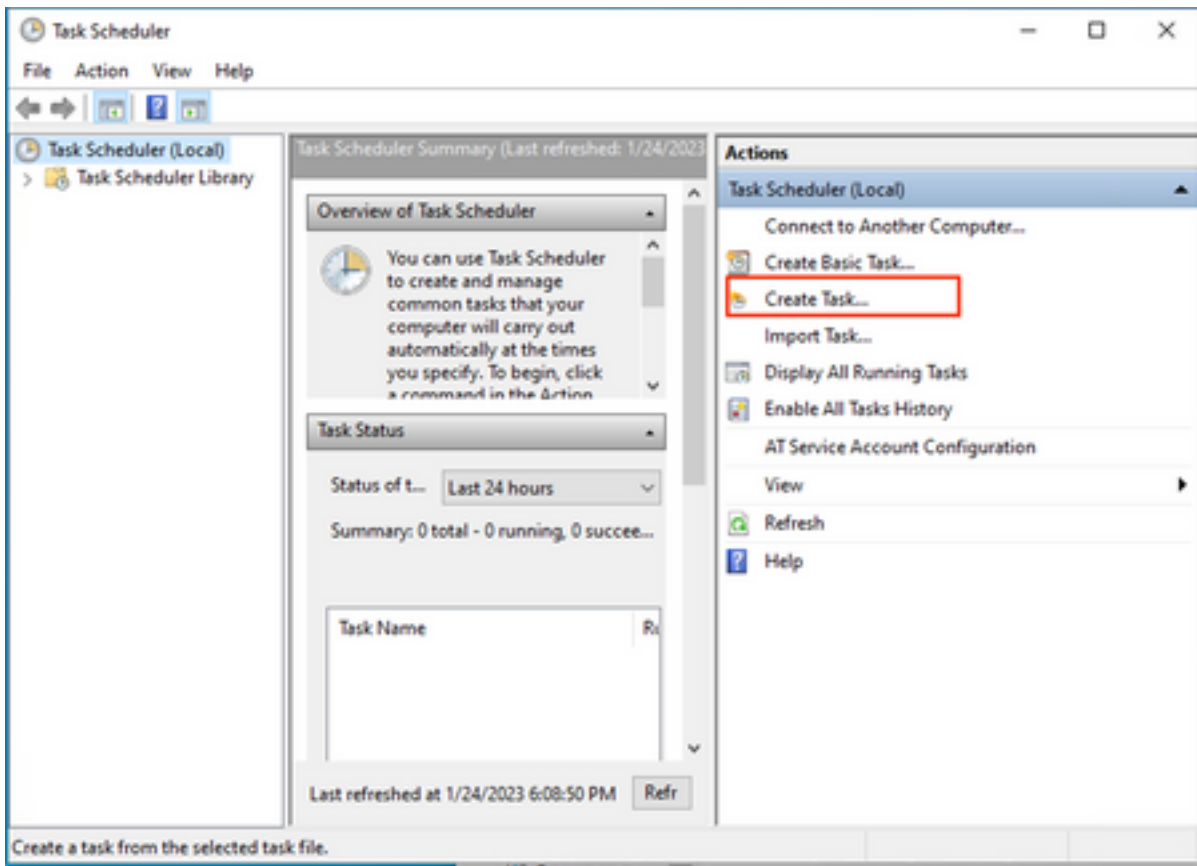


对于下一个配置片段，请访问您的Windows设备并打开一个新的记事本文件以添加以下行：

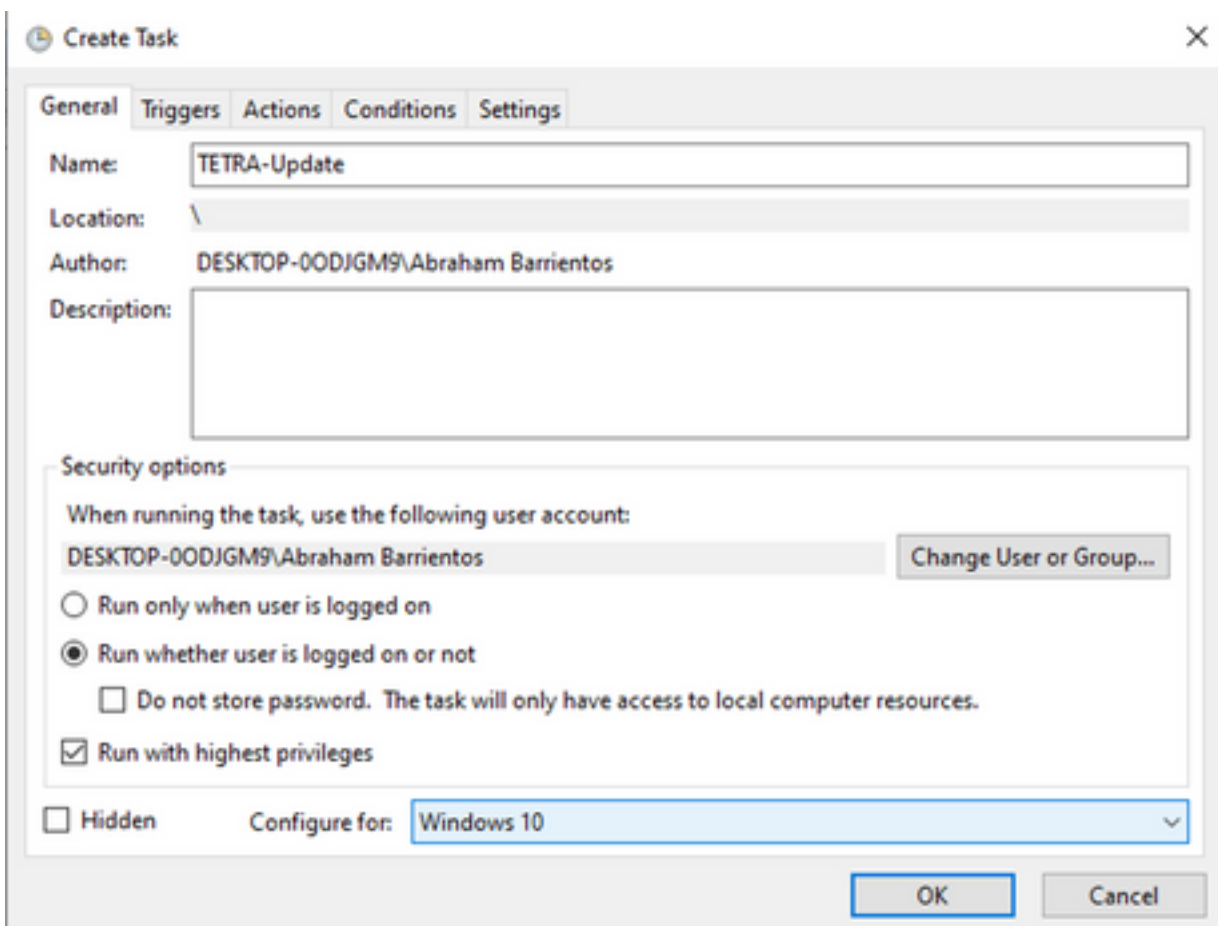
```
cd C:\Program Files\Cisco\AMP\8.1.3.21242
sfc.exe -forceupdate
```

请注意，您需要使用与终端上当前安装的版本匹配的安全终端版本(本示例为8.1.3.21242v)。如果不确定版本，可以单击**Secure Endpoint**用户界面齿轮图标，然后单击**Statics**选项卡以检查当前版本。将这些行添加到记事本后，单击**File**，然后单击**Save As**。然后单击**Save as a Type**并选择**All files**。最后，键入文件的名称，并将其另存为.BAT扩展名。如果要将文件保存在C:\文件夹下，您需要使用管理员权限执行记事本。作为附带说明，您可以执行BAT文件以强制TETRA更新作为测试。

在Windows计算机上打开“计划任务打开任务计划程序”，然后单击位于右列的“创建任务”按钮。



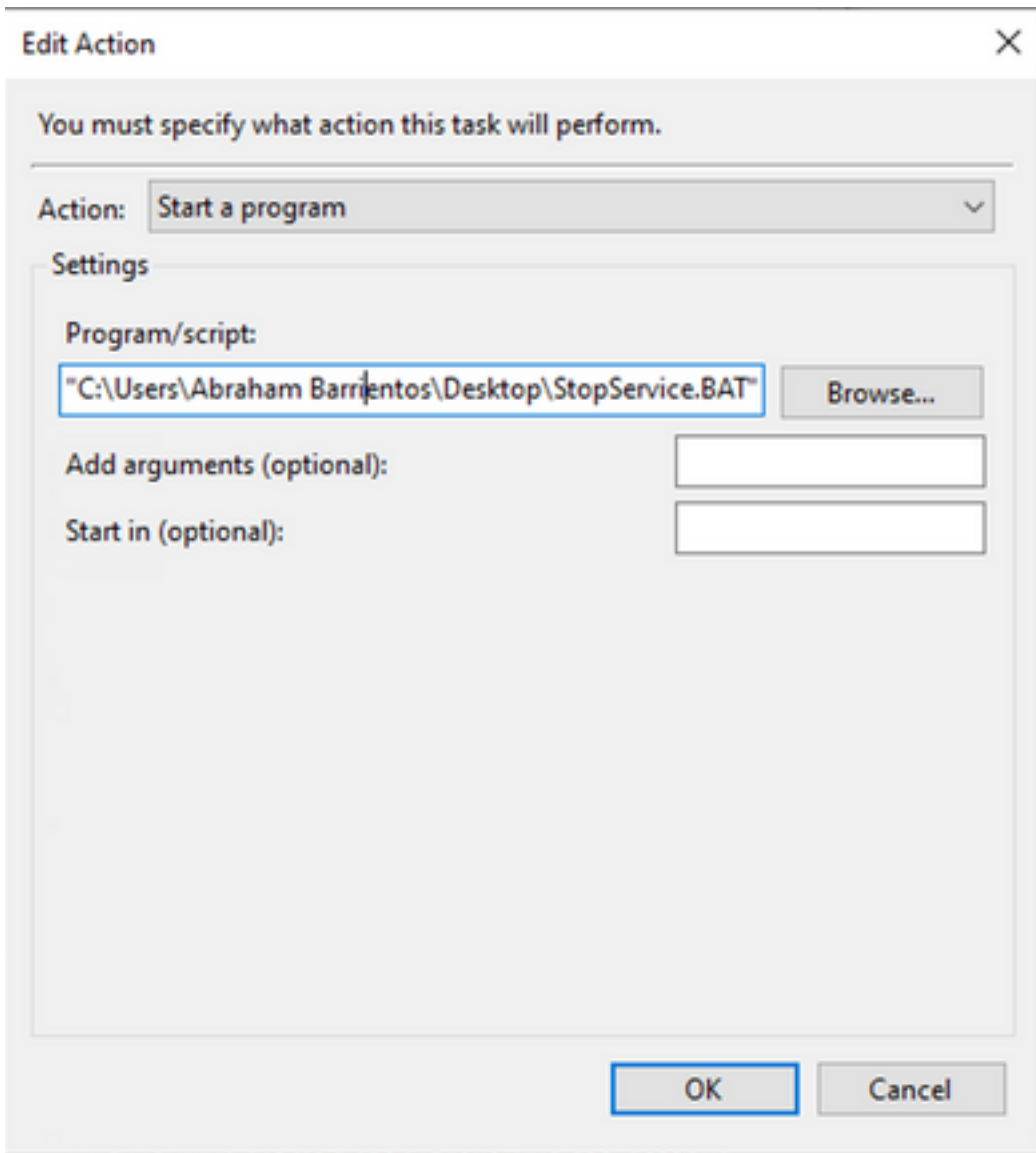
在General Tab下，键入此任务的名称，然后选择Run whenever user is logged or not logged。选中Run with the highest privileges复选框。在configure for选项下，选择应用的操作系统。在本演示中，使用了Windows 10。



在**触发器**选项卡下，单击**新建触发器**。在“新建触发器配置”(New trigger configuration)页面上，您可以自定义希望TETRA更新其签名的时间。在本例中，使用了本地机器时间下午1点运行的每日计划。开始日期选项定义此任务何时激活。完成计划设置后，单击**确定**。

The image shows the "Edit Trigger" dialog box in Windows Task Scheduler. The "Begin the task" dropdown is set to "On a schedule". Under the "Settings" section, the "Daily" radio button is selected. The "Start" date is set to "1/24/2023" and the time is "1:00:00 PM". The "Recur every" is set to "1 days". The "Advanced settings" section includes options for "Delay task for up to (random delay)", "Repeat task every", "Stop all running tasks at end of repetition duration", "Stop task if it runs longer than", and "Expire". The "Repeat task every" is set to "1 hour" and "for a duration of" is set to "1 day". The "Expire" date is "1/24/2024" and time is "6:50:59 PM". The "Enabled" checkbox is checked. The "OK" and "Cancel" buttons are at the bottom right.

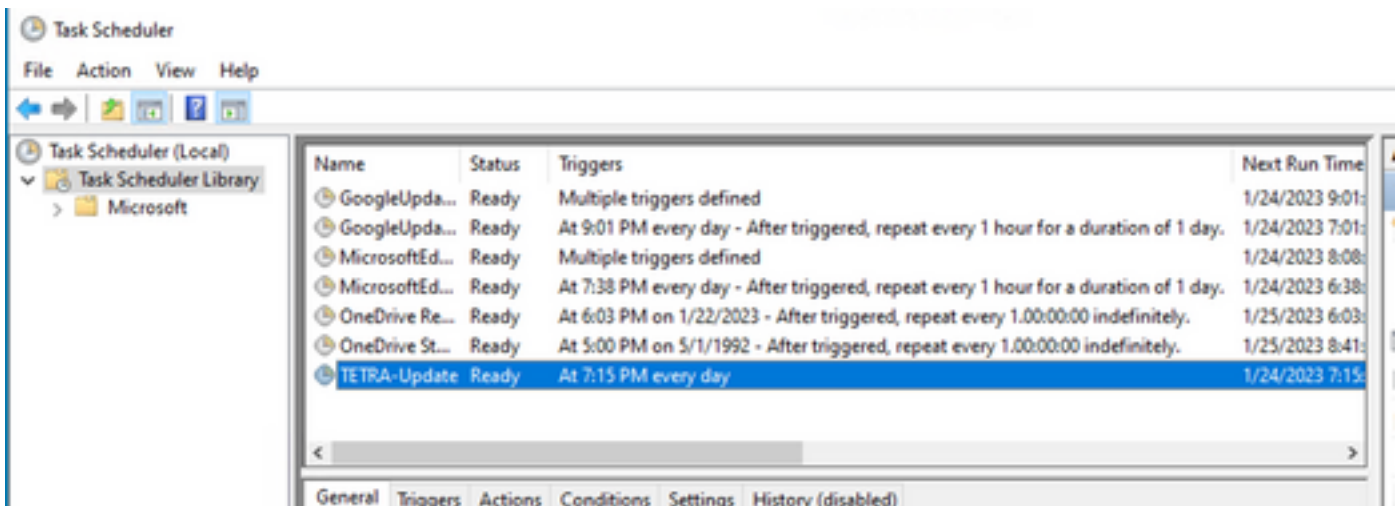
在**Actions(操作)**选项卡上，单击**New Action(新建操作)**。在**New Action**选项卡上，为**Action**设置选择**Start a program**。在**Program/Settings**下，单击**Browse**，然后选择BAT脚本。单击**Ok**以创建操作。保留其余设置默认值，然后单击**Ok**创建任务。



最后，由于选择了“使用最高权限运行”，此任务计划程序需要管理凭据才能创建任务。使用管理员凭据进行身份验证后，任务已准备就绪，可以运行和执行以通知Secure Endpoint service何时根据配置的计划相应地更新TETRA。

## 验证

单击左列中的**任务计划程序库**文件夹。验证是否已按预期创建并列出计划。



您可以在**Secure Endpoint User interface > static**选项卡下检查连接器下载的最新TETRA定义编号。您可以使用此数字比较控制台上**Management > Av Definitions summary**下的最新定义，了解设备是否最新且最新定义。另一种替代方法是在安全终端控制台中监控特定终端的“上次更新定义”值。

DESKTOP-00DJGM9 in group Jobarrie_Proxy		Definitions Up To Date	
Hostname	DESKTOP-00DJGM9	Group	Jobarrie_Proxy
Operating System	Windows 10 Enterprise (Build 19045.2486)	Policy	TETRA-Policy
Connector Version	8.1.3.21242	Internal IP	
Install Date	2023-01-23 13:01:50 CST	External IP	
Connector GUID	22277c92-e5f5-4dcb-894c-392d4428b5c0	Last Seen	2023-01-24 20:24:25 CST
Processor ID	0f8bfbff000006f1	Definition Version	TETRA 64 bit (daily version: 89889)
Definitions Last Updated	2023-01-24 20:24:25 CST	Update Server	tetra-defs.amp.cisco.com
Cisco Secure Client ID	N/A		

[Events](#) [Device Trajectory](#) [Diagnostics](#) [View Changes](#)

## 故障排除

当定义未按预期更新时，您可以查看日志以搜索TETRA更新错误。为此，请在Schedule任务触发时间之前，在Advanced选项卡下的Secure Endpoint用户界面上启用调试模式。在Schedule Task Trigger之后，让连接器在此模式下运行至少20分钟，然后查看位于**C:\Program Files\Cisco\AMP\X.X.X**（其中X.X.X是系统上的安全终端的当前版本）下的最新**sfcx.exe.log**文件。

ForceWakeUpdateThreadAbout向我们显示，TETRA由我们的计划作业触发，以按预期更新。如果未看到此日志，则可能是与Windows计划任务配置相关的问题。

```
(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
```

如果计划作业成功触发TETRA更新定义，则需要在日志中搜索任何相关的TETRA错误。这是TETRA错误代码2200的示例，它表示服务在更新过程中被中断。如何排除一般TETRA错误不在本文档的讨论范围之内，但是，本文档末尾的链接是有关TETRA错误代码故障排除的思科文章。

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

## 相关信息

- [TETRA](#)
- [— Tetra3000](#)
- [TETRA — Windows](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。