

Forzar manualmente la actualización de las definiciones de TETRA - Terminales seguros de Cisco

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe el procedimiento para forzar manualmente las nuevas definiciones de TETRA en Cisco Secure Endpoints(AMP).

Colaborado por Jesús Javier Martínez y Uriel Torres y editado por Yeraldin Sanchez, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- SO Windows
- AMP para terminales

Componentes Utilizados

La información de este documento se basa en Cisco Secure Endpoint (AMP) para Windows.

La información de este documento se creó a partir de los dispositivos en un entorno específico:

- dispositivo Windows 10
- Conector AMP versión 7.0.5

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Refiérase a la guía del usuario, Tetra es una solución antivirus completa para Cisco Secure Endpoint Solution. Se debe utilizar con Cisco Secure Endpoint para obtener la mejor protección. Si tenemos un AV de ^{terceros} instalado, deberíamos retirar el otro A/V para garantizar la instalación y el funcionamiento adecuados de TETRA. TETRA también puede consumir un ancho de banda significativo cuando se descargan las definiciones.

Precaución: Tetra debe ejercerse en un entorno de prueba antes de una implementación de gran tamaño.

Puesto que AMP versión 6.3.1 cuando el motor TETRA está habilitado y sus definiciones están actualizadas, Windows Defender debe estar inhabilitado, por lo tanto, Cisco Secure Endpoint se designa como el proveedor activo de Antivirus y Threat Protection.

Las definiciones se descargan automáticamente, sin embargo, puede forzar la actualización manual de las definiciones de TETRA.

Troubleshoot

Nota: En Cisco Secure Endpoint versión 7.2.7 y superiores, puede forzar al conector a buscar las actualizaciones usando el argumento '-force update'

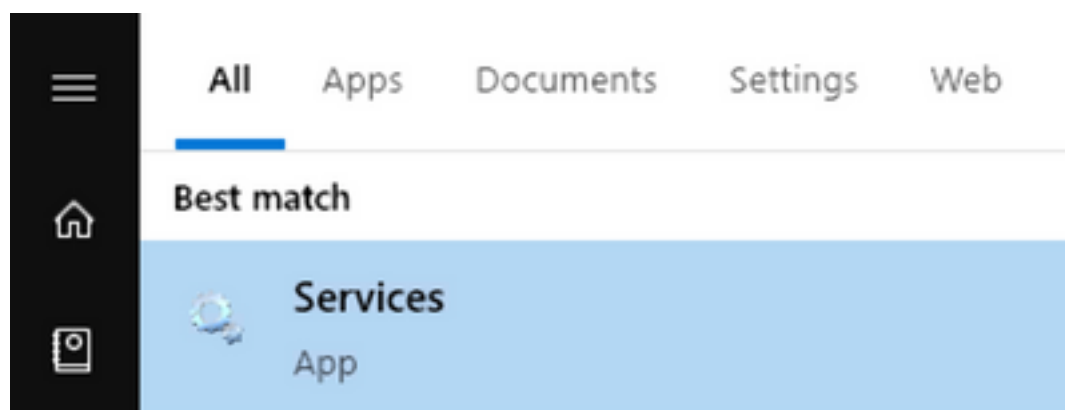
```
C:\Program Files\Cisco\AMP\7.2.7\sfc.exe -forceupdate
```

Para forzar las actualizaciones de definición a continuación de la versión 7.2.7, puede seguir esta guía.

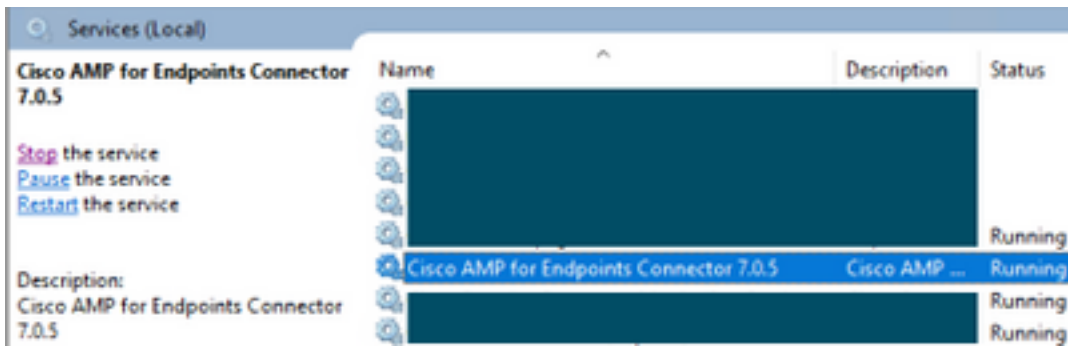
Paso 1. Detenga el servicio AMP.

- Si no dispone de protección mediante contraseña

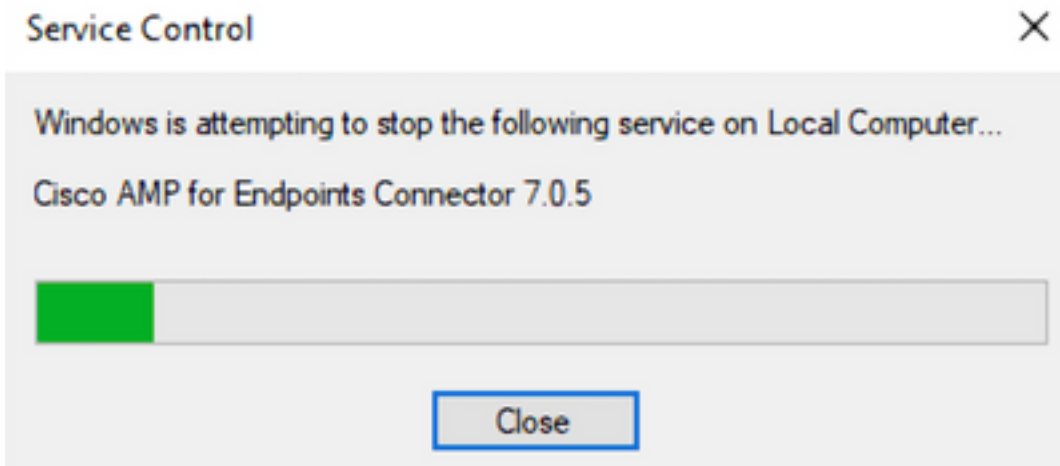
Paso 1.1. Abra **Services.msc**, como se muestra en la imagen.



Paso 1.2. Vaya a **Services > Cisco AMP para terminales Connector 7.0.5** como se muestra en la imagen.

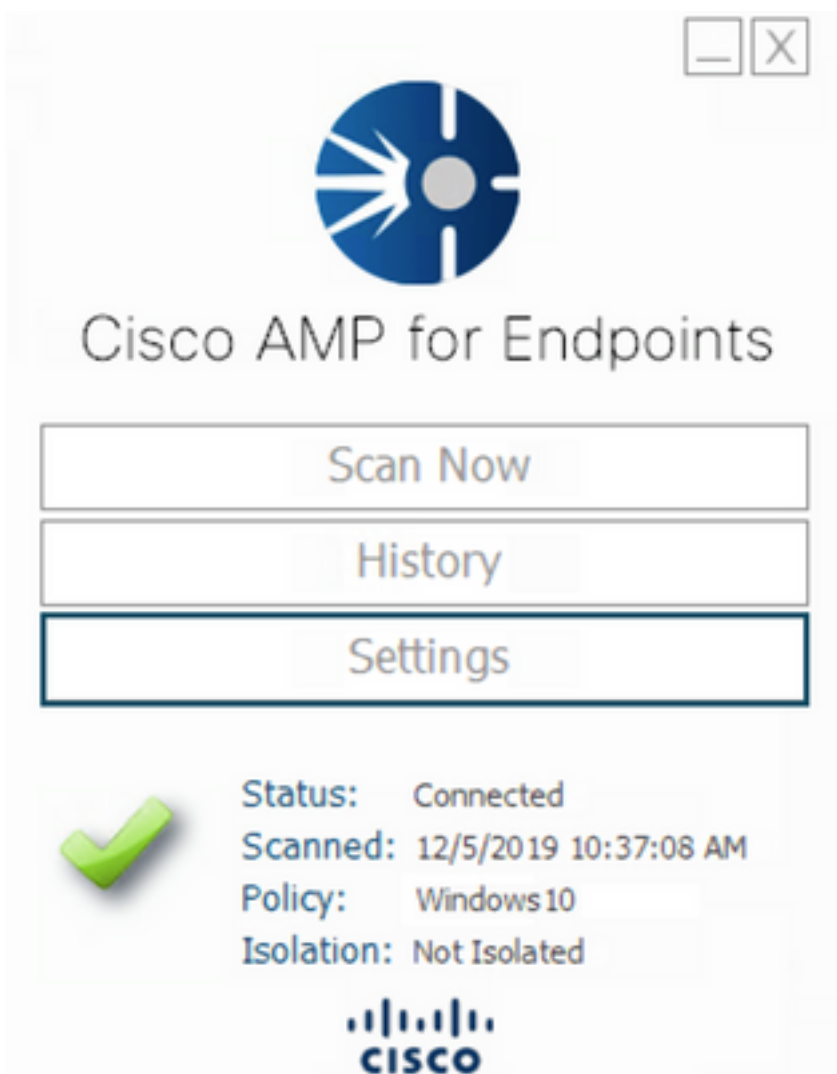


Paso 1.3. Detenga el servicio AMP como se muestra en la imagen.

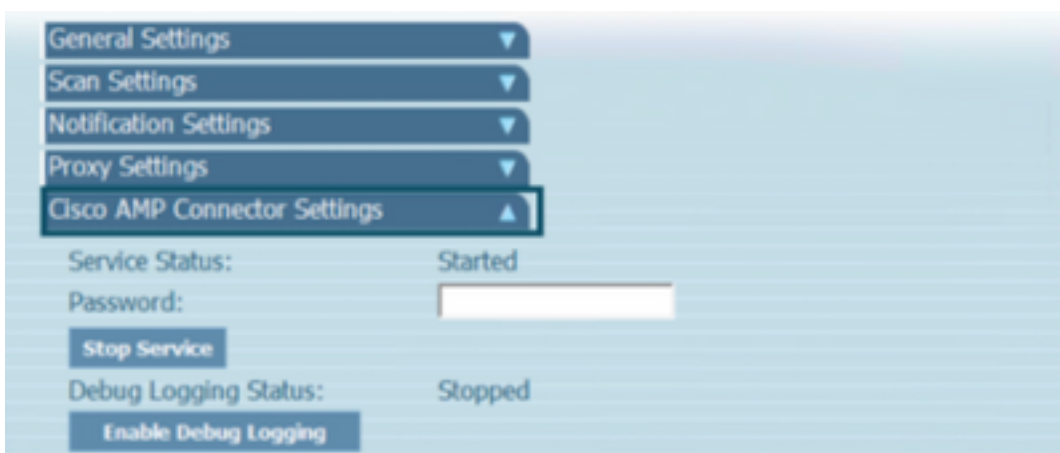


- Si dispone de protección mediante contraseña

Paso 1.4. Abra la interfaz de usuario de AMP y seleccione **Configuración** como se muestra en la imagen.



Paso 1.5. Vaya a **Configuración de AMP de Cisco para terminales** como se muestra en la imagen.

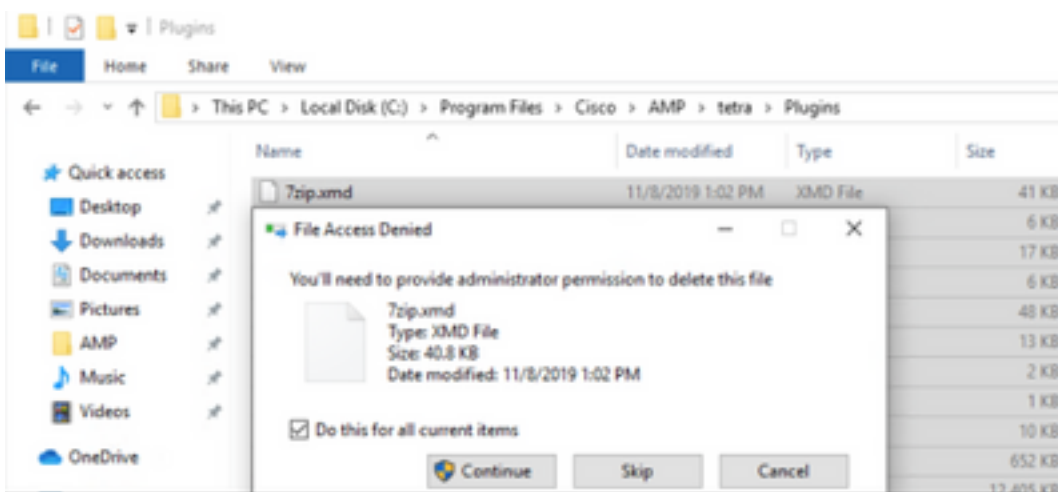


Paso 1.6. Ingrese la contraseña y haga clic en **Detener servicio** como se muestra en la imagen.

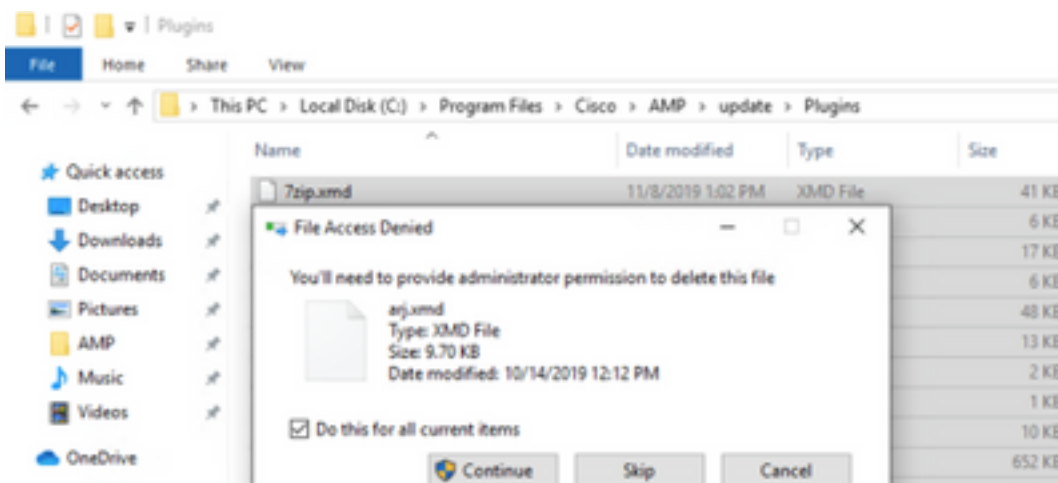


Paso 2. Navegue hasta la carpeta AMP, que generalmente se encuentra en **C:\Program Files\Cisco\AMP** como se muestra en la imagen.

Paso 2.1. Elimine todo el contenido de la carpeta **C:\Program Files\Cisco\AMP\tetra\Plugins**, como se muestra en la imagen



Paso 2.2. Elimine todo el contenido de la carpeta **C:\Program Files\Cisco\AMP\update\Plugins**, como se muestra en la imagen.



Paso 3. Inicie el servicio **Cisco AMP para terminales Connector 7.0.5**, como se muestra en la imagen.



Services (Local)

Cisco AMP for Endpoints Connector 7.0.5

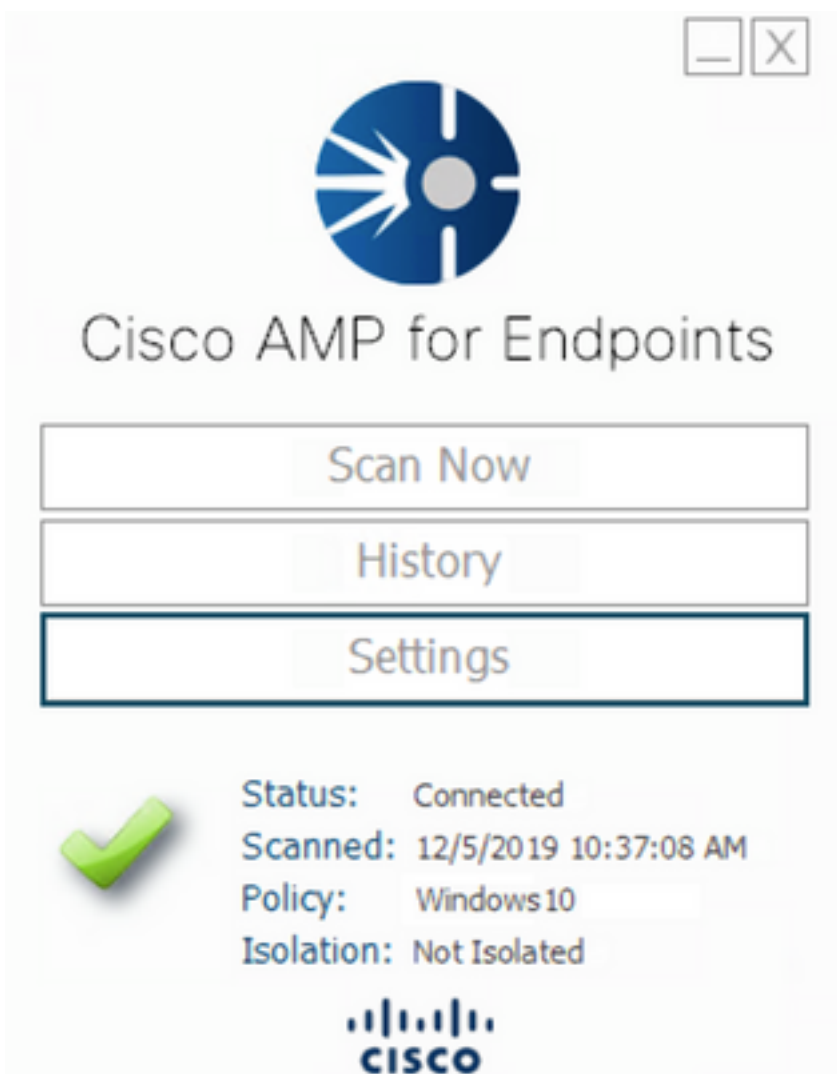
[Start](#) the service

Description:

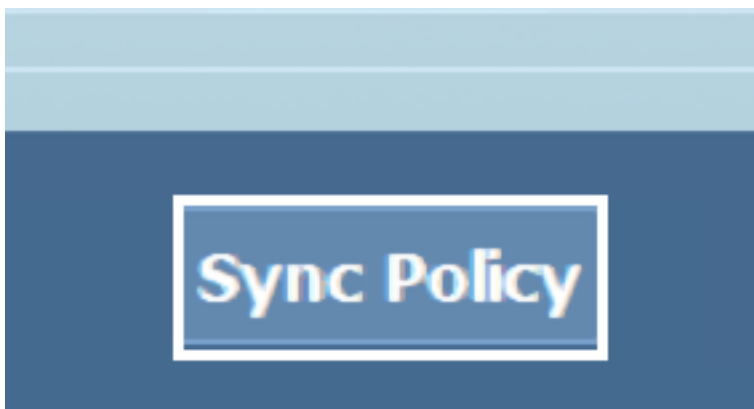
Cisco AMP for Endpoints Connector
7.0.5

Paso 4. Abra la interfaz de usuario de AMP, como se muestra en la imagen.

Paso 4.1. Haga clic en **Settings** como se muestra en la imagen.



Paso 4.2. Seleccione **Sync Policy** como se muestra en la imagen.



Paso 5. Cuando se sincroniza el pólícy se descargan las definiciones de Tetra.

Nota: Una vez descargadas las definiciones, el conector de AMP es el AV predeterminado, como se muestra en la imagen.

Virus & threat protection

Protection for your device against threats.

Cisco AMP for Endpoints

Cisco AMP for Endpoints is turned on.

Current threats

 No actions needed.

Protection settings

 No actions needed.

Protection updates

 No actions needed.

[Open app](#)

Incluso si las definiciones de TETRA se descargan automáticamente, puede forzar manualmente una actualización de definición. Depende de sus requisitos.

Información Relacionada

- [AMP4E - Vídeo de actualización de definiciones de TETRA](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)