Force Manually the TETRA Definitions Update - Cisco Secure Endpoints

Contents

Introduction

This document describes the procedure to force manually the new TETRA definitions in Cisco Secure Endpoints(AMP).

Contributed by Jesus Javier Martinez and Uriel Torres and Edited by Yeraldin Sanchez, Cisco TAC Engineers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Windows OS
- AMP for endpoints

Components Used

The information in this document is based on Cisco Secure Endpoint(AMP) for Windows.

The information in this document was created from the devices in a specific environment:

- Windows 10 device
- AMP connector 7.0.5 version

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Refer to the User Guide, Tetra is a full antivirus solution for Cisco Secure Endpoint Solution. It should be used with Cisco Secure Endpoint to get the best protection. If we have a 3rd party AV installed, we should remove the other A/V to ensure proper installation and operation of TETRA. TETRA can also consume significant bandwidth when the definitions are downloaded.

> **Caution**: Tetra must be exercised in a test environment before a large deployment.

Since AMP version 6.3.1 when the TETRA engine is enabled and its definitions are up to date, Windows Defender needs to be disabled, therefore Cisco Secure Endpoint is designated as the active Antivirus and Threat Protection provider.

The definitions are downloaded automatically, however, you can force manually TETRA definitions update.

Troubleshoot

Note: On Cisco Secure Endpoint version 7.2.7 and above, you can force the connector to fetch the updates using the argument '-forceupdate'

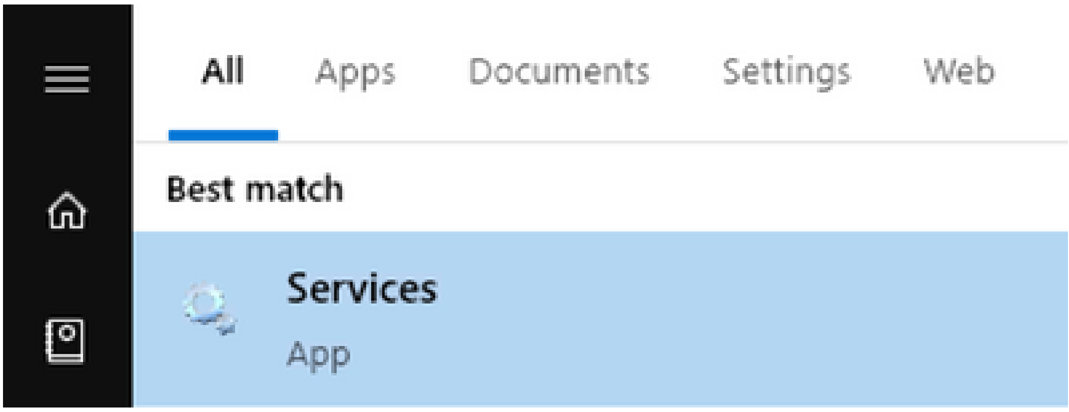
```
C:\Program Files\Cisco\AMP\7.2.7\sfc.exe -forceupdate
```

In order to force the definition updates below version 7.2.7, you can follow this guide.

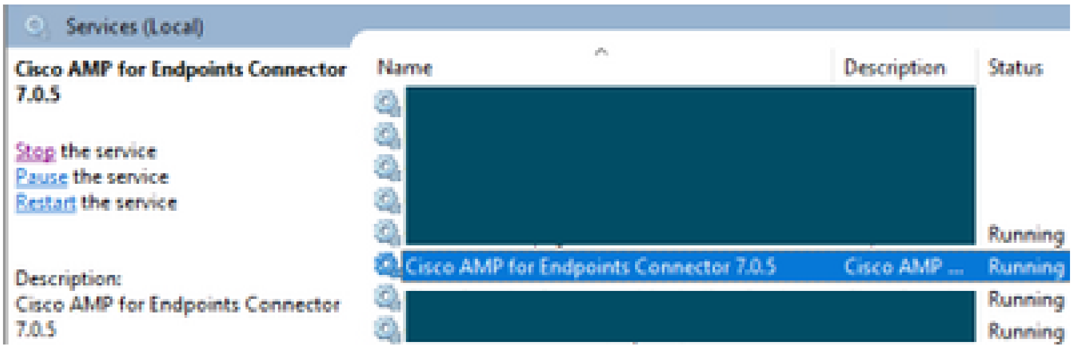
Step 1. Stop the AMP service.

- If you don't have password protection

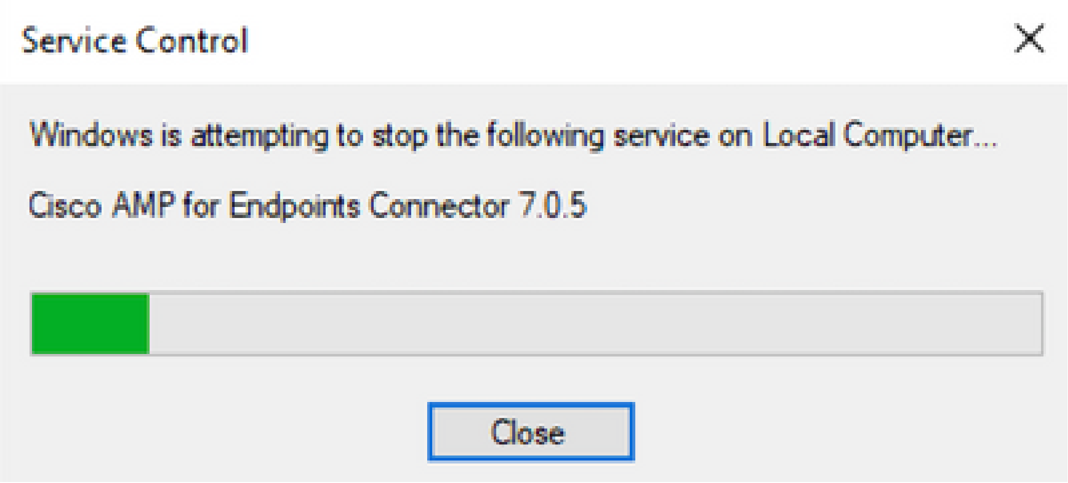
Step 1.1. Open **Services.msc,** as shown in the image.



Step 1.2. Navigate to **Services > Cisco AMP for Endpoints Connector 7.0.5** as shown in the image.



Step 1.3. Stop the AMP Service as shown in the image.



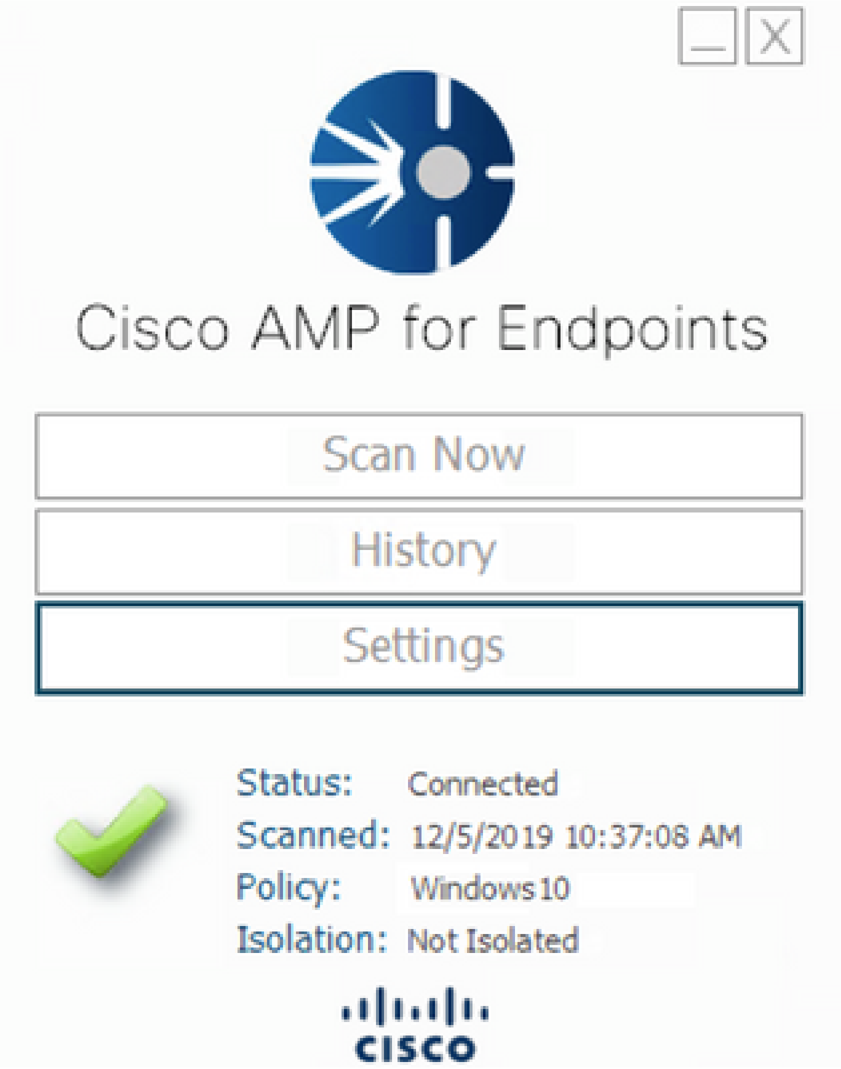
Service Control

Windows is attempting to stop the following service on Local Computer...

Cisco AMP for Endpoints Connector 7.0.5

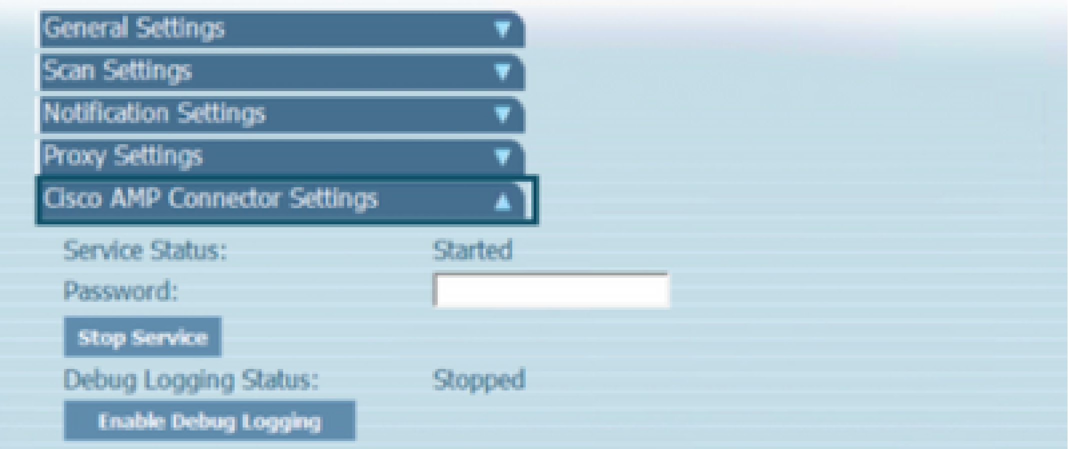
- If you have password protection

  Step 1.4. Open the AMP User Interface and select **Settings** as shown in the image.



Status: Connected
Scanned: 12/5/2019 10:37:08 AM
Policy: Windows 10
Isolation: Not Isolated

Step 1.5. Navigate to **Cisco AMP for Endpoints Settings** as shown in the image.

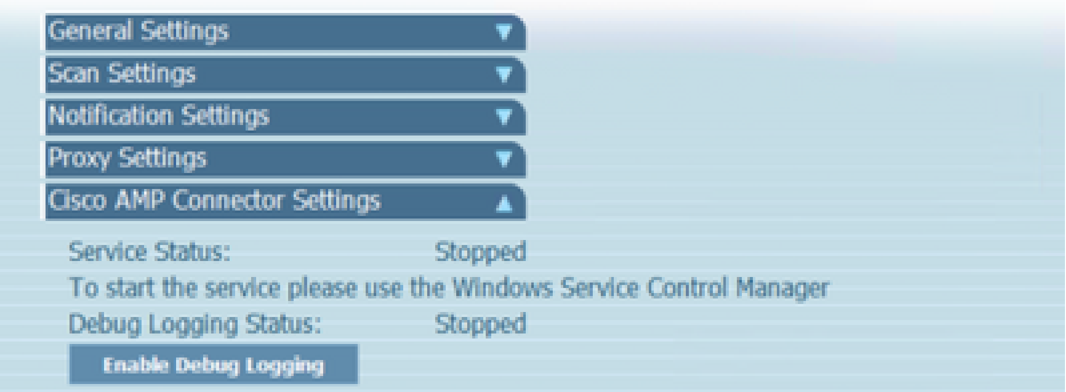


Service Status: Started

Password:

Debug Logging Status: Stopped

Step 1.6. Enter the password and click on **Stop Service** as shown in the image.



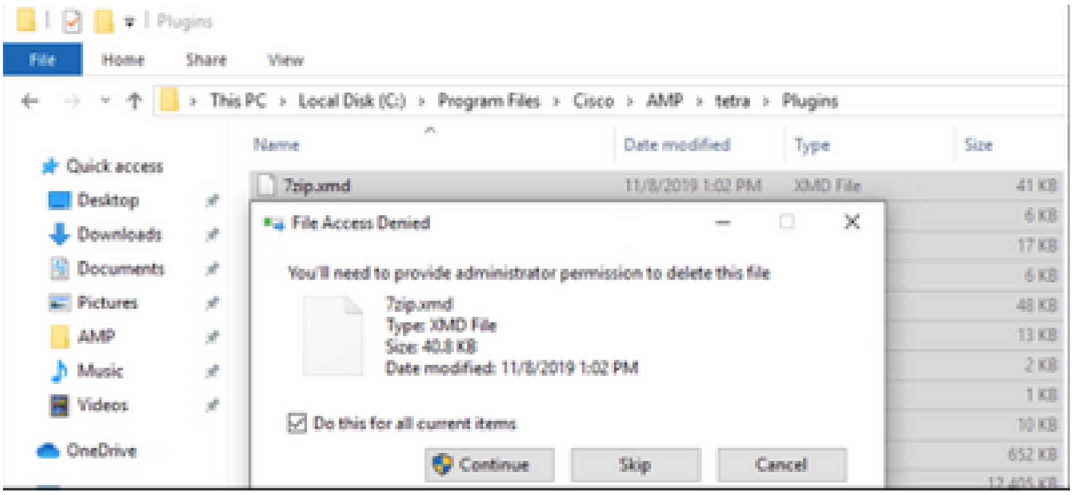
Service Status: Stopped

To start the service please use the Windows Service Control Manager

Debug Logging Status: Stopped

Step 2. Navigate to the AMP folder, generally located in **C:\Program Files\Cisco\AMP** as shown in the image.

Step 2.1. Delete all the content inside **C:\Program Files\Cisco\AMP\tetra\Plugins\** folder, as shown in the image



Name	Date modified	Type	Size
7zip.xmd	11/8/2019 1:02 PM	XMD File	41 KB
			6 KB
			17 KB
			6 KB
			48 KB
			13 KB
			2 KB
			1 KB
			10 KB
			652 KB
			12,405 KB

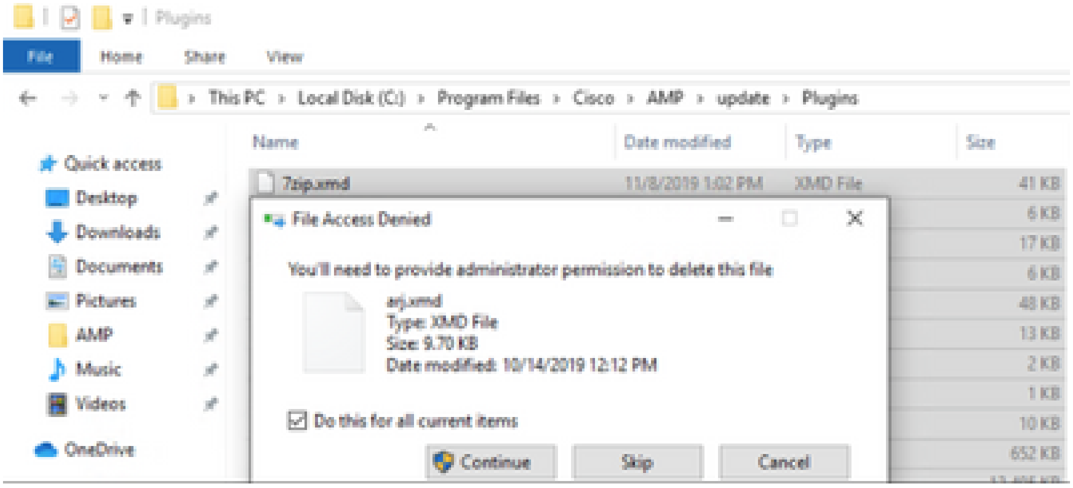
File Access Denied

You'll need to provide administrator permission to delete this file

7zip.xmd
Type: XMD File
Size: 40.8 KB
Date modified: 11/8/2019 1:02 PM

☑ Do this for all current items

Step 2.2. Delete all the content inside **C:\Program Files\Cisco\AMP\update\Plugins\** folder, as shown in the image.



File Access Denied

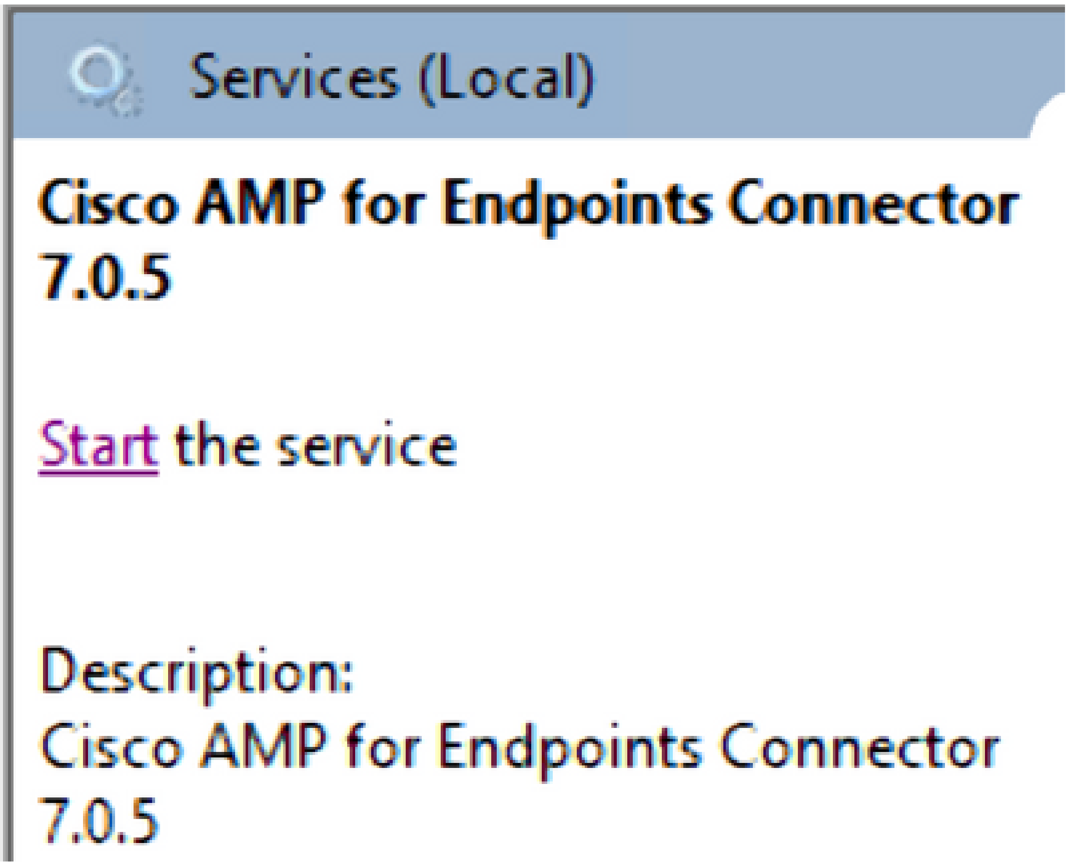
You'll need to provide administrator permission to delete this file

arj.xmd
Type: XMD File
Size: 9.70 KB
Date modified: 10/14/2019 12:12 PM

☑ Do this for all current items

Continue Skip Cancel

Step 3. Start the **Cisco AMP for Endpoints Connector 7.0.5** service, as shown in the image.



Services (Local)

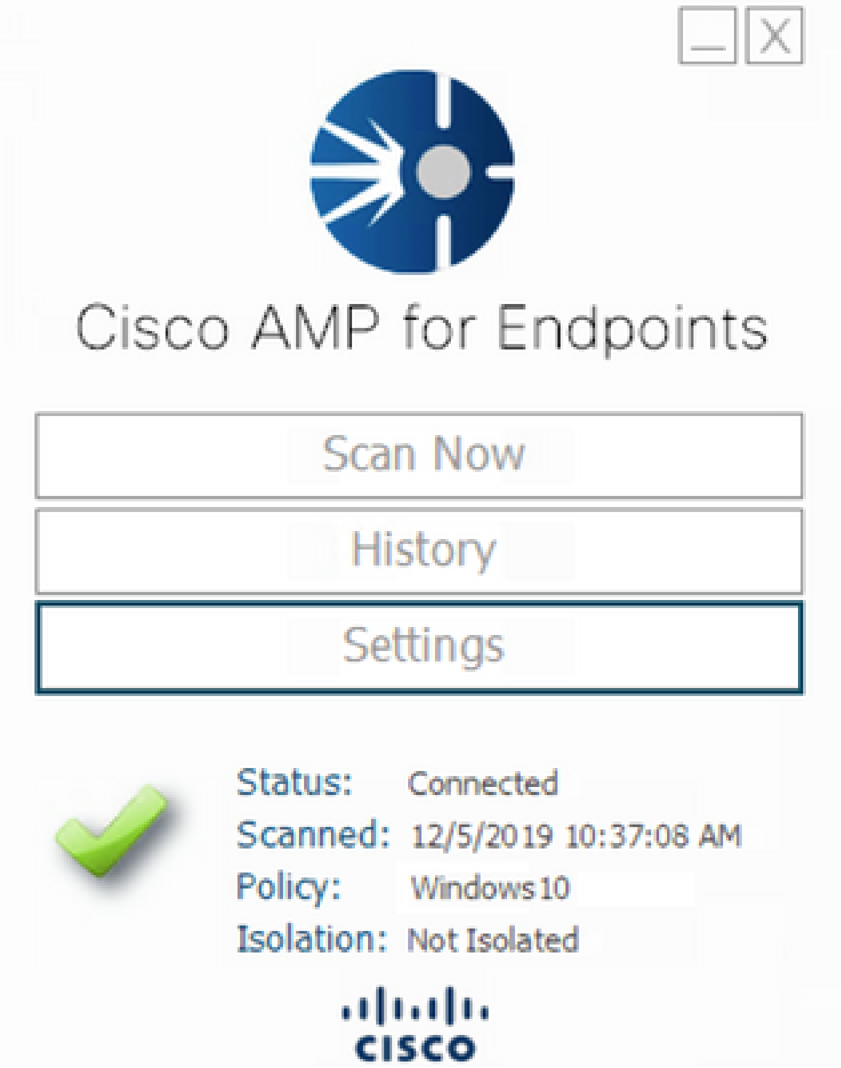
Cisco AMP for Endpoints Connector 7.0.5

Start the service

Description:
Cisco AMP for Endpoints Connector 7.0.5

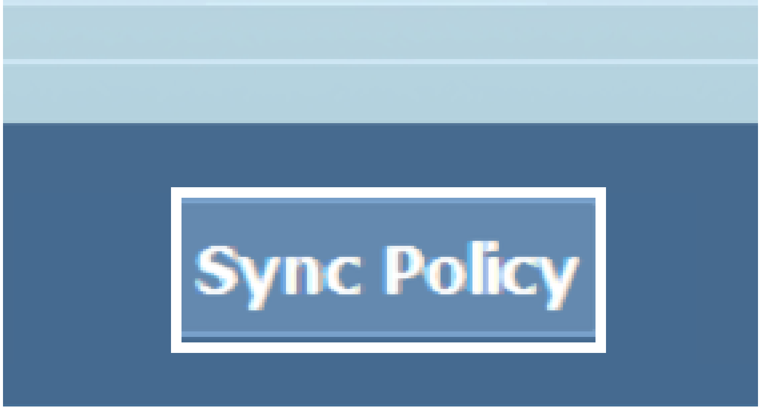
Step 4. Open the AMP User Interface, as shown in the image.

Step 4.1. Click on **Settings** as shown in the image.



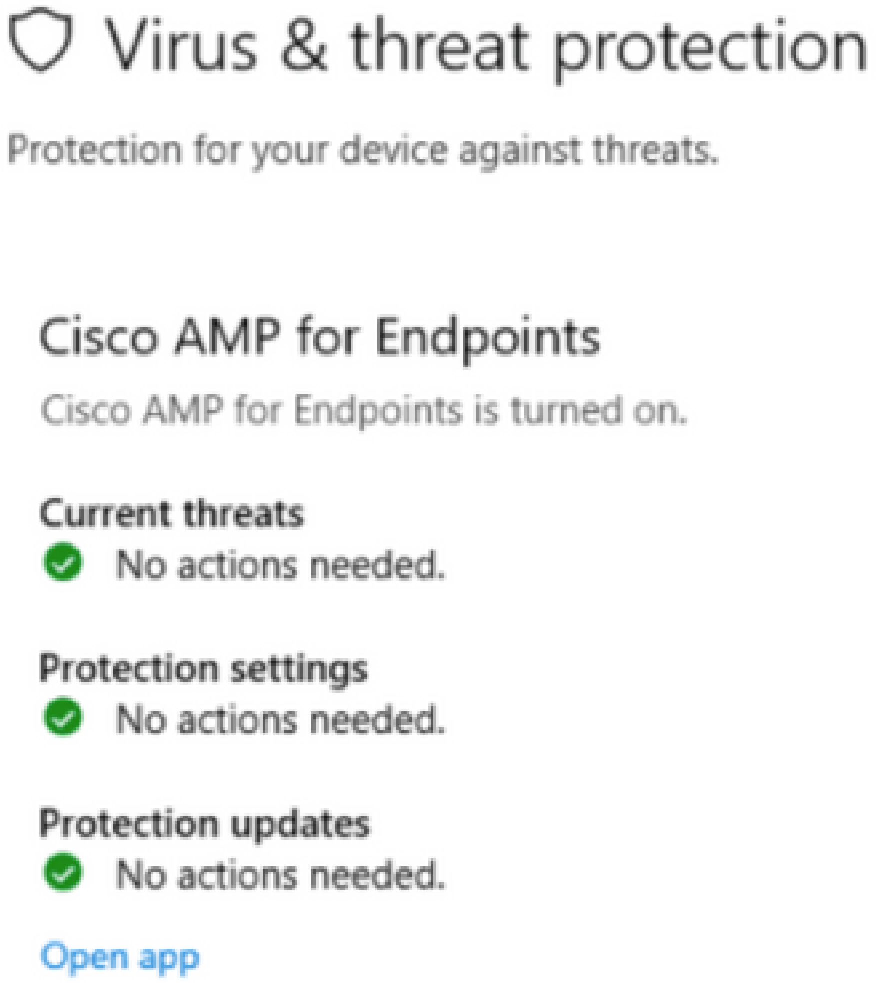
Status: Connected
Scanned: 12/5/2019 10:37:08 AM
Policy: Windows 10
Isolation: Not Isolated

Step 4.2. Select **Sync Policy** as shown in the image.



Step 5. When the pólicy is synced the Tetra definitions are downloaded.

Note: Once the definitions are downloaded the AMP connector is the default AV, as shown in the image.



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.

Even if the TETRA definitions are downloaded automatically, you can manually force a definition update. It depends on your requirements.

Related Information

- **AMP4E - TETRA Definitions Update Video**
- **Technical Support & Documentation - Cisco Systems**