Forcer manuellement la mise à jour des définitions TETRA - Cisco Secure Endpoints

Contenu

Introduction

Ce document décrit la procédure à suivre pour forcer manuellement les nouvelles définitions TETRA dans Cisco Secure Endpoints (AMP).

Avec la collaboration de Jesus Javier Martinez et Uriel Torres et sous la direction de Yeraldin Sanchez, ingénieurs du TAC de Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Windows OS
- AMP pour les points terminaux

Components Used

Les informations de ce document sont basées sur Cisco Secure Endpoint(AMP) pour Windows.

Les informations de ce document ont été créées à partir des périphériques d'un environnement spécifique :

- Périphérique Windows 10
- Connecteur AMP version 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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Reportez-vous au Guide de l'utilisateur, Tetra est une solution antivirus complète pour la solution Cisco Secure Endpoint. Il doit être utilisé avec Cisco Secure Endpoint pour obtenir la meilleure protection possible. Si nous avons un AV 3^{tiers} installé, nous devrions retirer l'autre A/V pour assurer l'installation et le fonctionnement appropriés de TETRA. TETRA peut également consommer une bande passante importante lorsque les définitions sont téléchargées.

> **Attention** : Le tétra doit être exercé dans un environnement d'essai avant un déploiement important.

Depuis AMP version 6.3.1 lorsque le moteur TETRA est activé et que ses définitions sont à jour, Windows Defender doit être désactivé. Par conséquent, Cisco Secure Endpoint est désigné comme fournisseur actif de protection contre les virus et les menaces.

Les définitions sont téléchargées automatiquement, mais vous pouvez forcer manuellement la mise à jour des définitions TETRA.

Dépannage

Note: Sur Cisco Secure Endpoint version 7.2.7 et ultérieure, vous pouvez forcer le connecteur à récupérer les mises à jour à l'aide de l'argument '-forceupdate'

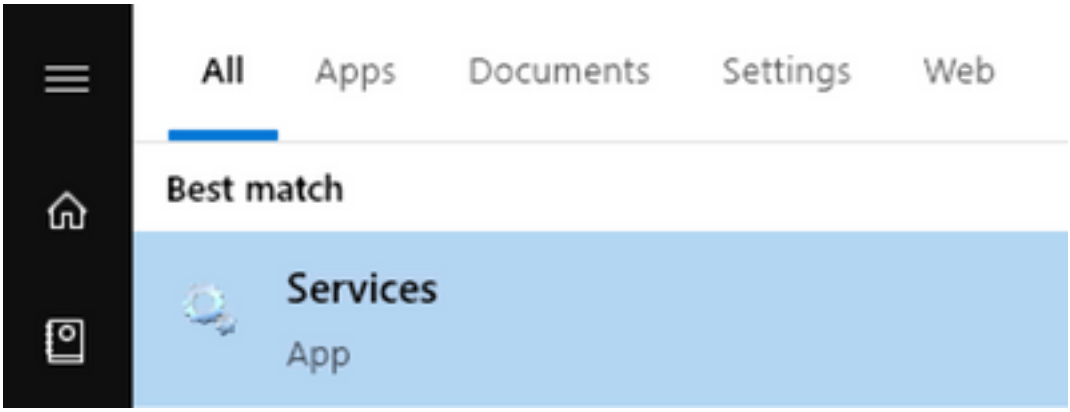
```
C:\Program Files\Cisco\AMP\7.2.7\sfc.exe -forceupdate
```

Afin de forcer les mises à jour de définition sous la version 7.2.7, vous pouvez suivre ce guide.

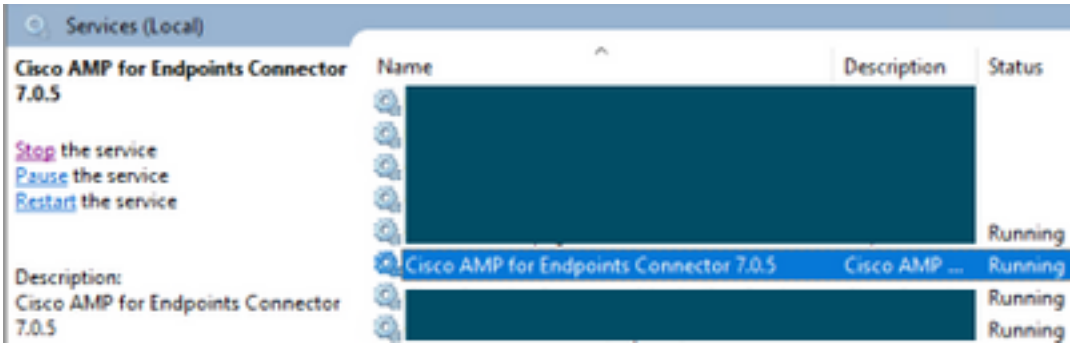
Étape 1. Arrêtez le service AMP.

- Si vous n'avez pas de protection par mot de passe

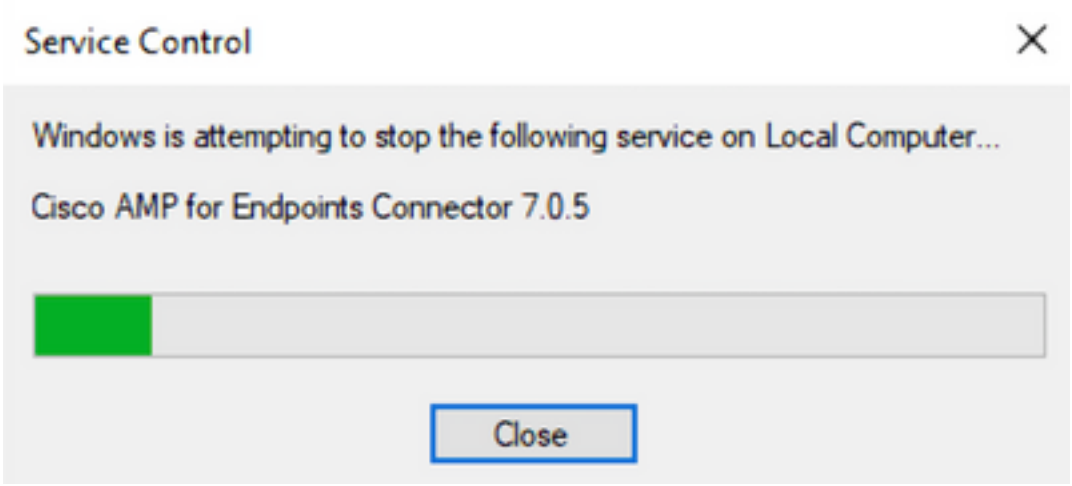
Étape 1.1. Ouvrez **Services.msc,** comme indiqué dans l'image.



Étape 1.2. Accédez à **Services > Cisco AMP for Endpoints Connector 7.0.5** comme illustré dans l'image.

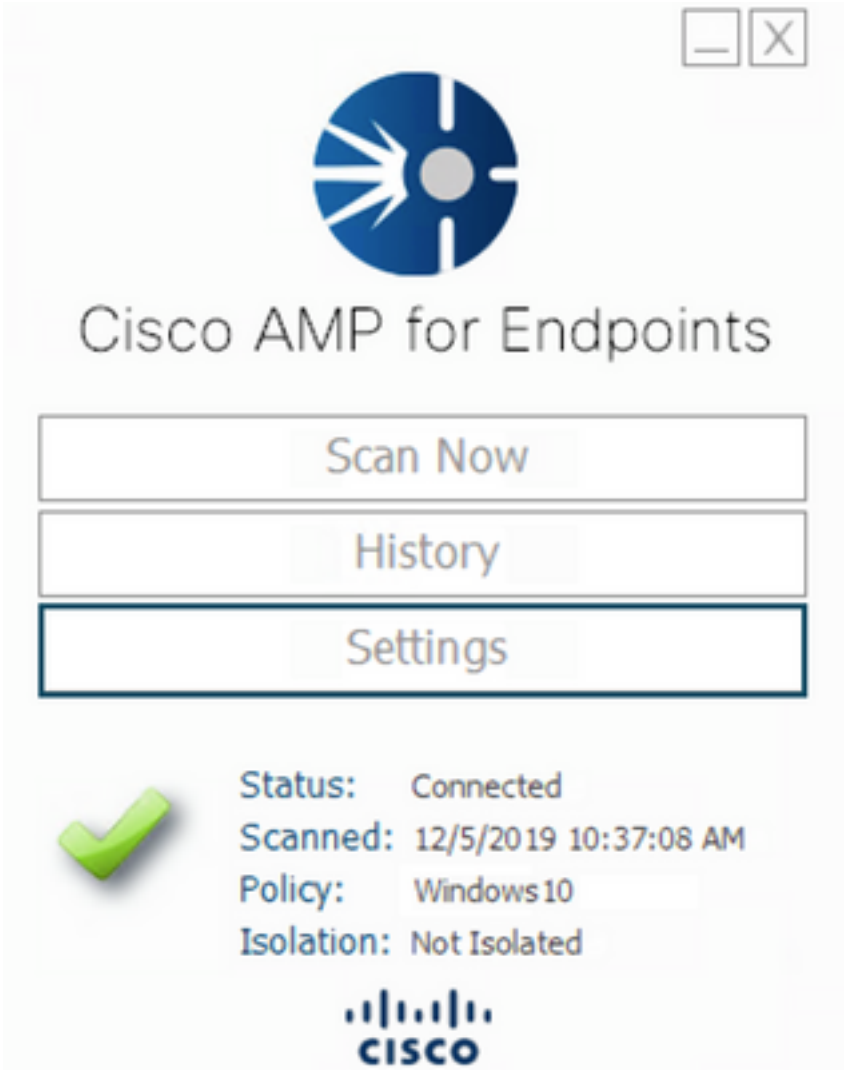


Étape 1.3. Arrêtez le service AMP comme indiqué dans l'image.



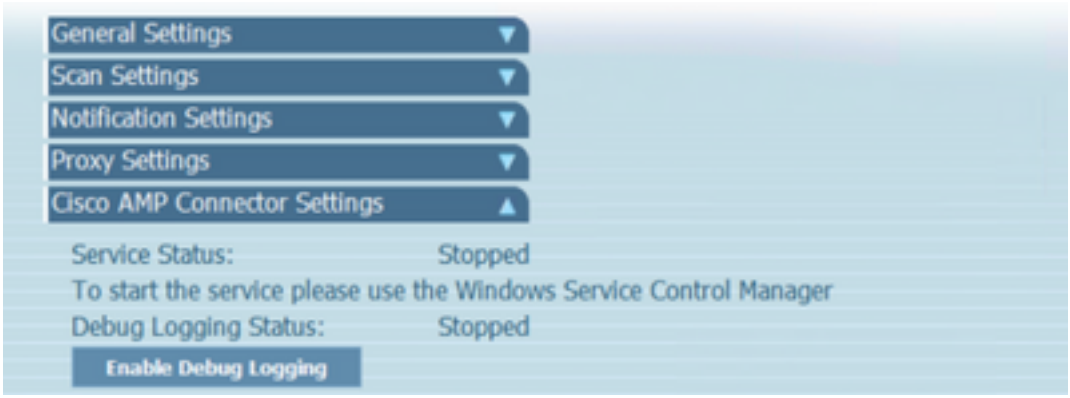
- Si vous disposez d'une protection par mot de passe

Étape 1.4. Ouvrez l'interface utilisateur AMP et sélectionnez **Paramètres** comme indiqué dans l'image.



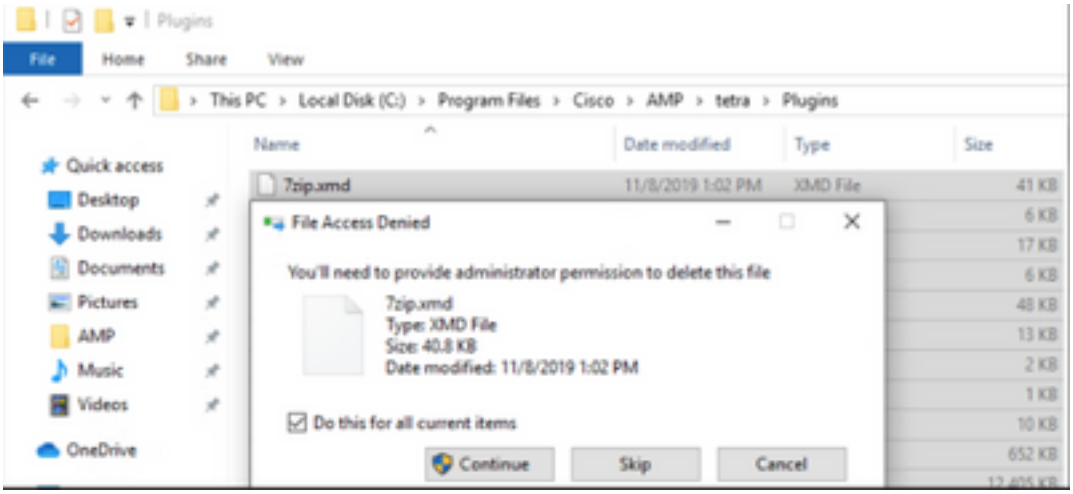
Étape 1.5. Accédez à **Cisco AMP for Endpoints Settings** comme indiqué dans l'image.

Étape 1.6. Entrez le mot de passe et cliquez sur **Arrêter le service** comme indiqué dans l'image.

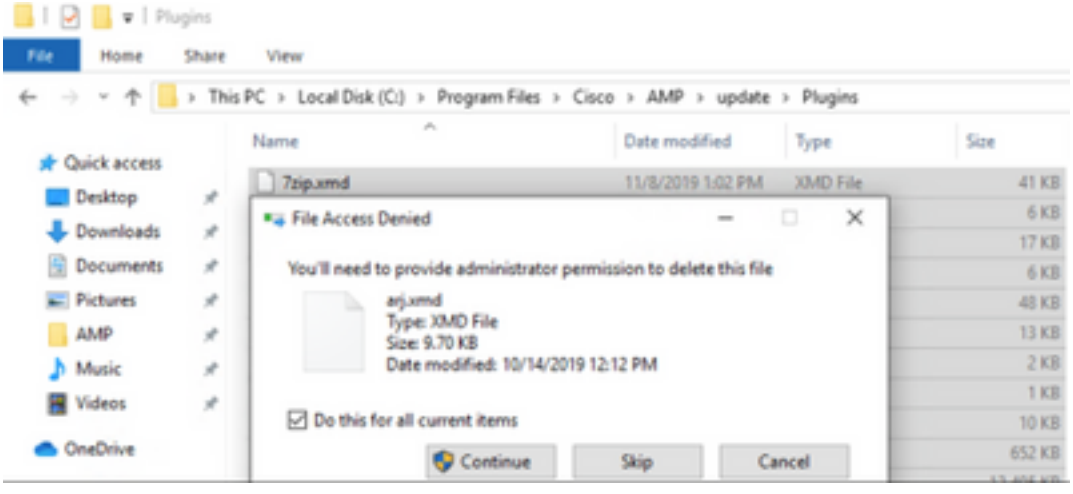


Étape 2. Accédez au dossier AMP, généralement situé dans **C:\Program Files\Cisco\AMP** comme indiqué dans l'image.

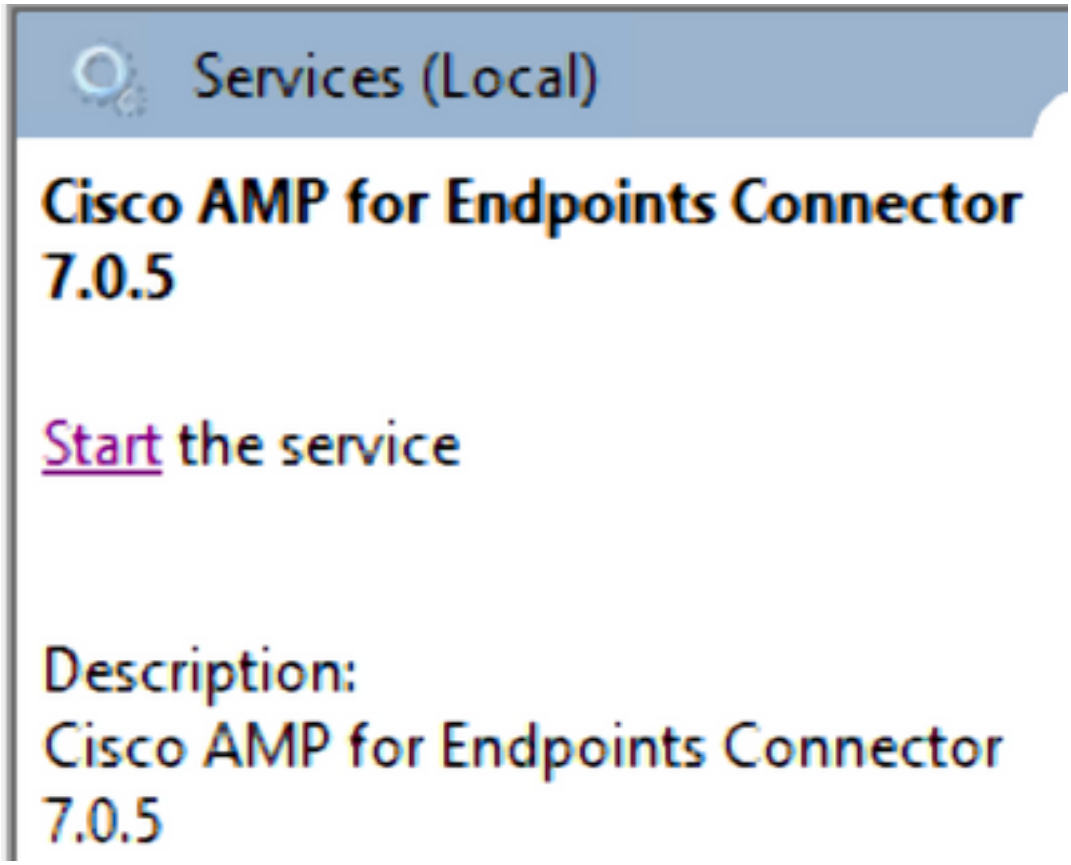
Étape 2.1. Supprimer tout le contenu du dossier **C:\Program Files\Cisco\AMP\tetra\Plugins**, comme illustré dans l'image



Étape 2.2. Supprimez tout le contenu du dossier **C:\Program Files\Cisco\AMP\update\Plugins** , comme indiqué dans l'image.

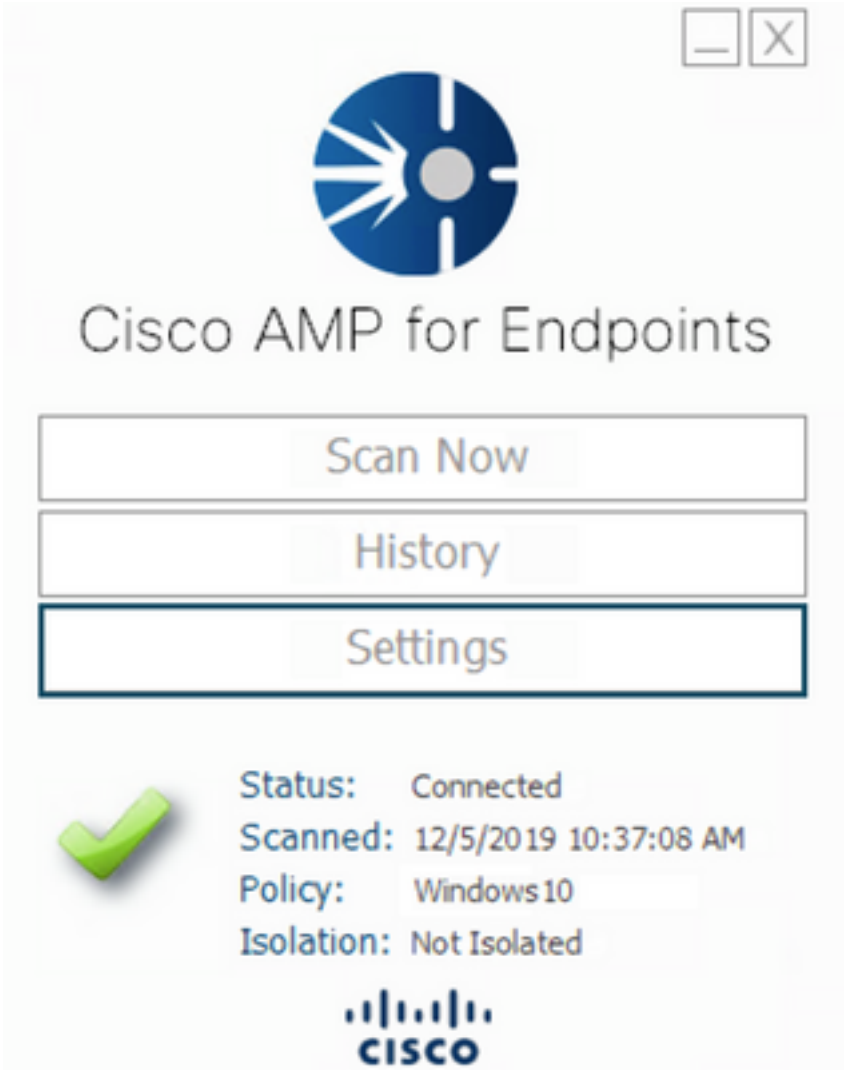


Étape 3. Démarrez le service **Cisco AMP for Endpoints Connector 7.0.5**, comme illustré dans l'image.

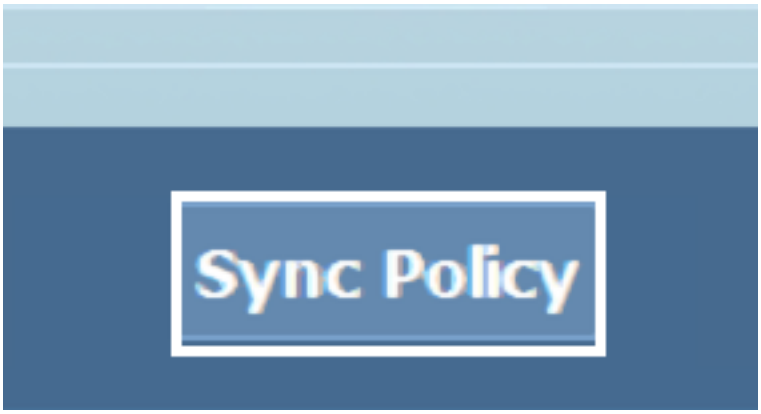


Étape 4. Ouvrez l'interface utilisateur AMP, comme illustré dans l'image.

Étape 4.1. Cliquez sur **Paramètres** comme indiqué dans l'image.

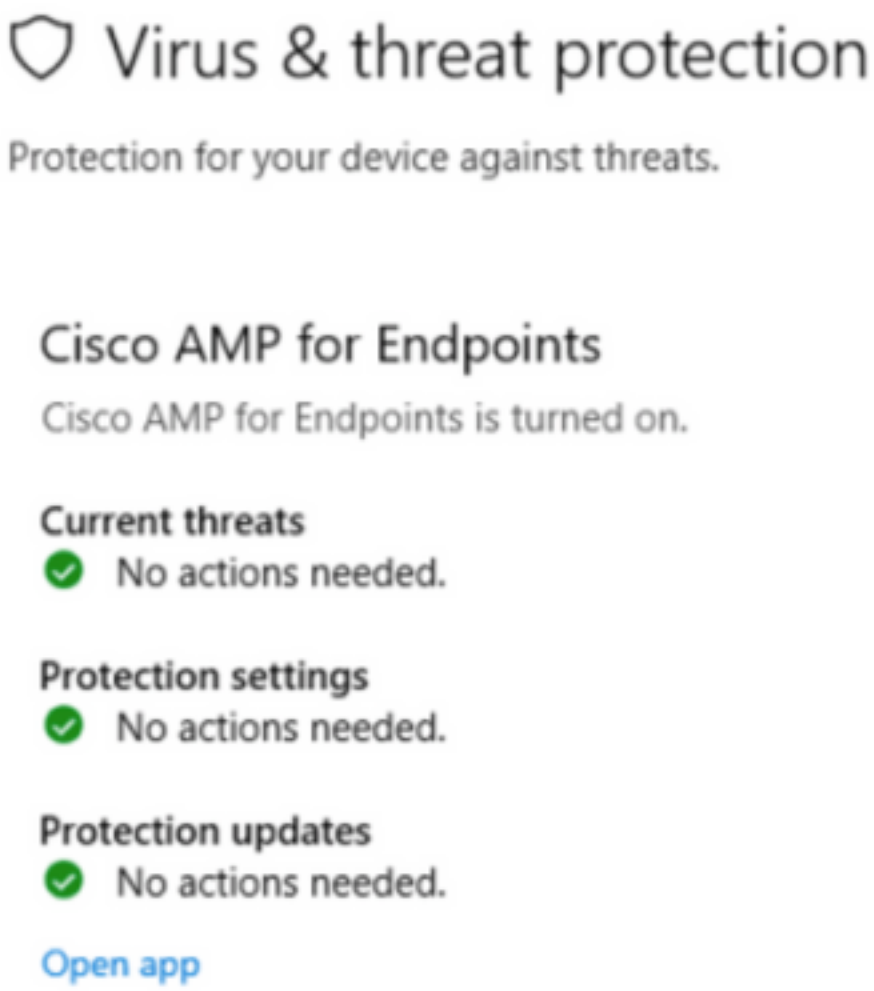


Étape 4.2. Sélectionnez **Stratégie de synchronisation** comme indiqué dans l'image.



Étape 5. Lorsque la politique est synchronisée, les définitions Tetra sont téléchargées.

> **Note**: Une fois les définitions téléchargées, le connecteur AMP est l'AV par défaut, comme l'illustre l'image.



Même si les définitions TETRA sont téléchargées automatiquement, vous pouvez forcer manuellement une mise à jour des définitions. Cela dépend de vos besoins.

Informations connexes

- AMP4E - Vidéo de mise à jour des définitions TETRA
- Support et documentation techniques - Cisco Systems