

Erzwingen Sie die Aktualisierung der TETRA-Definitionen manuell - Cisco Secure Endpoints

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument beschreibt das Verfahren, um die neuen TETRA-Definitionen in Cisco Secure Endpoints (AMP) manuell zu erzwingen.

Verfasst von Jesus Javier Martinez und Uriel Torres und herausgegeben von Yeraldin Sanchez, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Windows-Betriebssystem
- AMP für Endgeräte

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Secure Endpoint (AMP) für Windows.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Umgebung erstellt:

- Windows 10-Gerät
- AMP Connector 7.0.5 Version

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Informationen hierzu finden Sie im Benutzerhandbuch. Tetra ist eine vollständige Antivirus-Lösung für Cisco Secure Endpoint Solution. Sie sollte zusammen mit Cisco Secure Endpoint verwendet werden, um den bestmöglichen Schutz zu gewährleisten. Wenn ein Drittanbieter-AV installiert ist, sollten wir den anderen A/V entfernen, um die ordnungsgemäße Installation und den ordnungsgemäßen Betrieb von TETRA sicherzustellen. TETRA kann beim Herunterladen der Definitionen auch beträchtliche Bandbreite beanspruchen.

Vorsicht: Tetra muss vor einer großen Bereitstellung in einer Testumgebung angewendet werden.

Da die AMP-Version 6.3.1 bei Aktivierung der TETRA-Engine und der Aktualisierung der Definitionen deaktiviert werden muss, muss Windows Defender deaktiviert werden. Daher wird Cisco Secure Endpoint als aktiver Antivirus- und Bedrohungsschutz-Anbieter festgelegt.

Die Definitionen werden automatisch heruntergeladen, Sie können jedoch eine manuelle Aktualisierung der TETRA-Definitionen erzwingen.

Fehlerbehebung

Hinweis: Auf Cisco Secure Endpoint Version 7.2.7 und höher können Sie den Connector zwingen, die Aktualisierungen mithilfe des Arguments '-forceupdate' abzurufen.

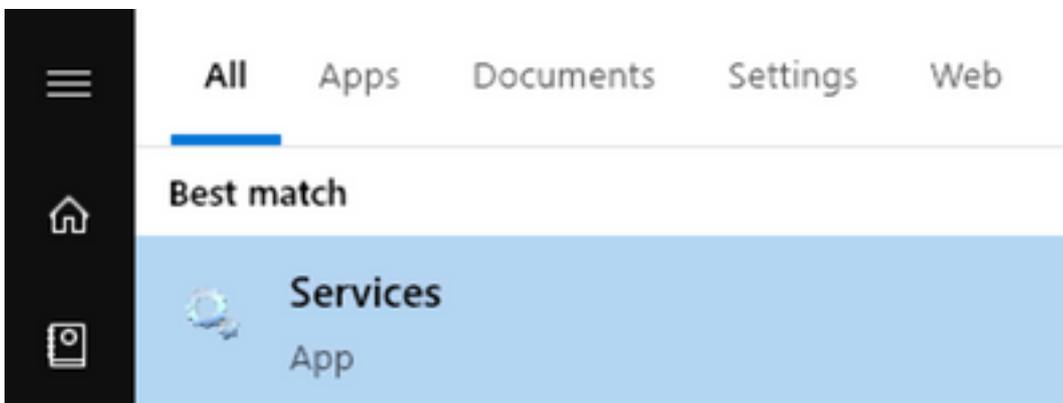
```
C:\Program Files\Cisco\AMP\7.2.7\sfc.exe -forceupdate
```

Um Definitionsaktualisierungen unter Version 7.2.7 zu erzwingen, können Sie diesem Handbuch folgen.

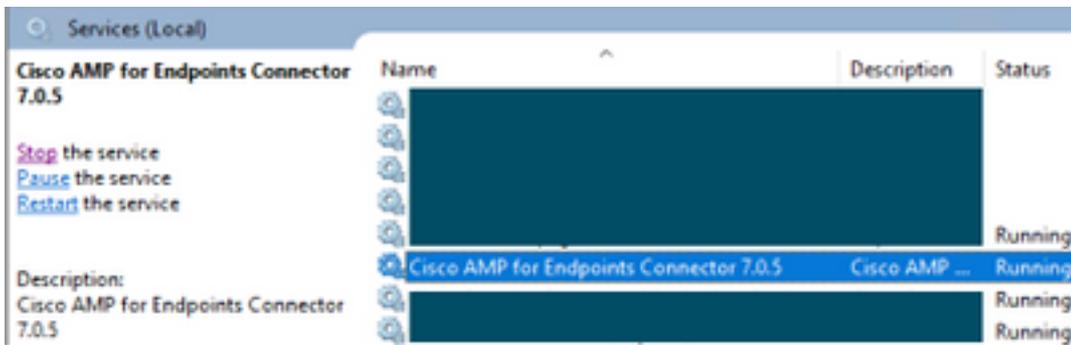
Schritt 1: Beenden Sie den AMP-Dienst.

- Wenn Sie keinen Kennwortschutz haben

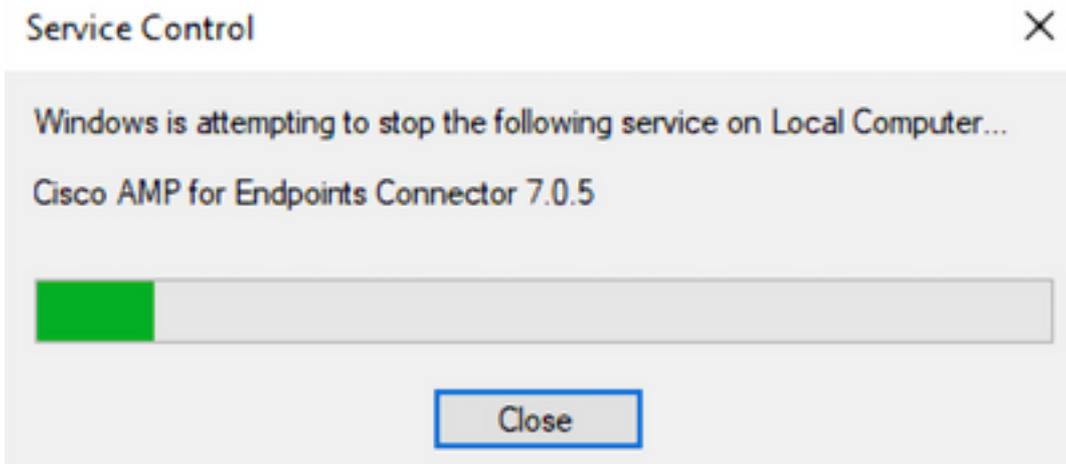
Schritt 1.1: Öffnen Sie **Services.msc**, wie im Bild gezeigt.



Schritt 1.2: Navigieren Sie zu **Services > Cisco AMP für Endpoints Connector 7.0.5** wie im Bild gezeigt.

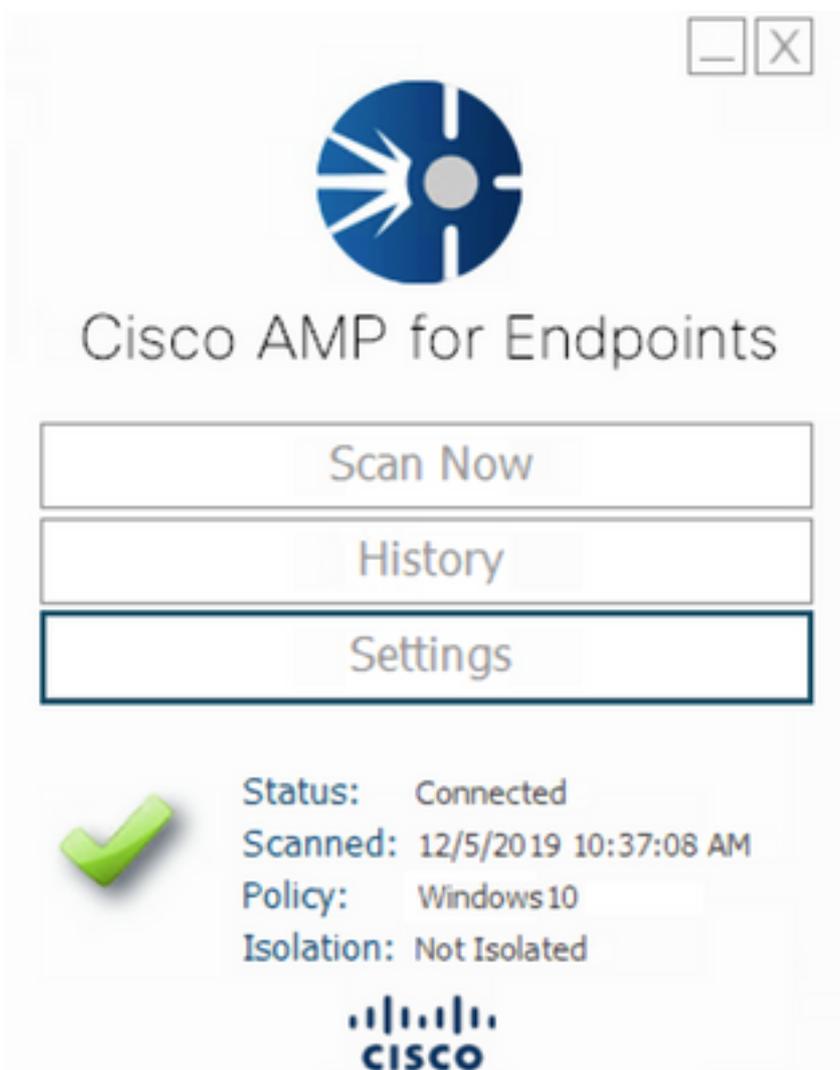


Schritt 1.3: Beenden Sie den AMP-Dienst, wie im Bild gezeigt.

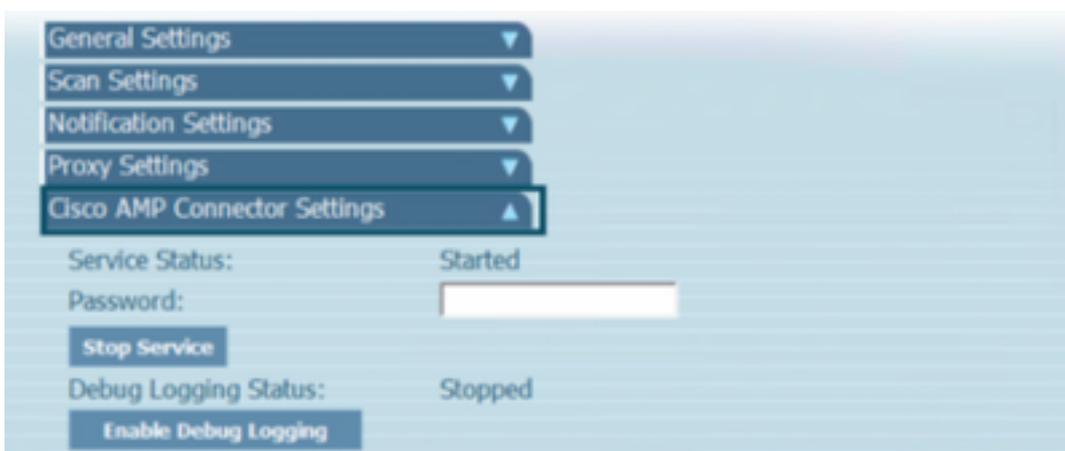


- Wenn Sie über Kennwortschutz verfügen

Schritt 1.4: Öffnen Sie die AMP-Benutzeroberfläche, und wählen Sie **Einstellungen** aus, wie im Bild gezeigt.



Schritt 1.5: Navigieren Sie zu **Cisco AMP für Endgeräte-Einstellungen** wie im Bild gezeigt.

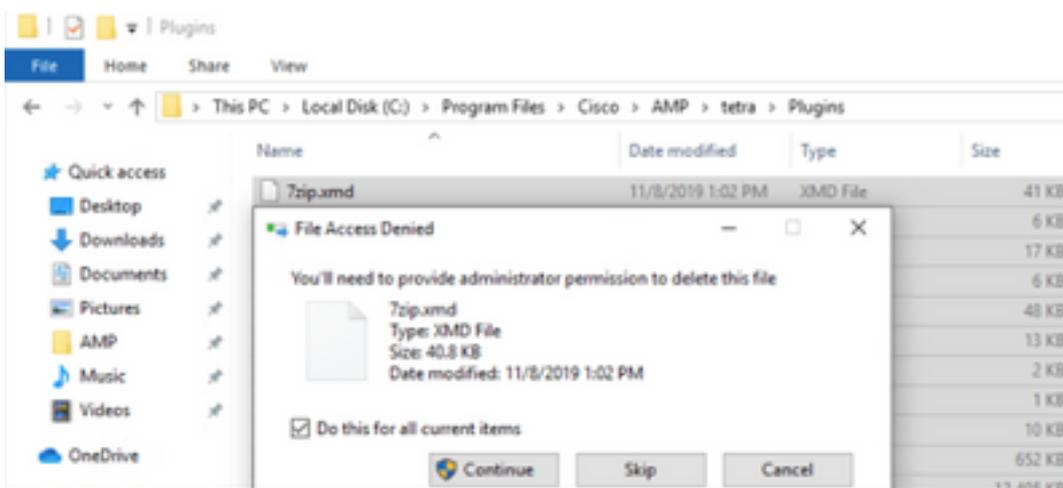


Schritt 1.6: Geben Sie das Kennwort ein, und klicken Sie auf **Service beenden**, wie im Bild gezeigt.

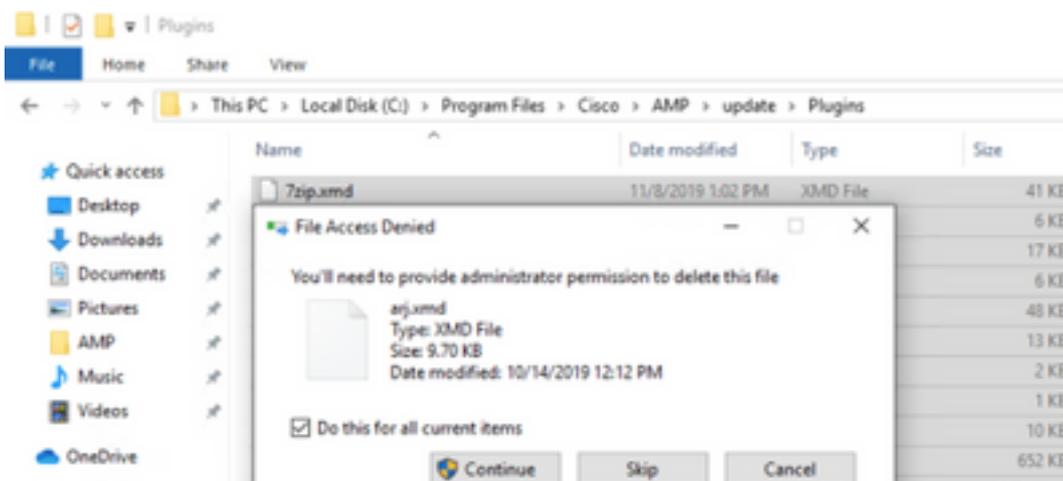


Schritt 2: Navigieren Sie zum AMP-Ordner, der sich normalerweise in **C:\Program Files\Cisco\AMP** befindet, wie im Bild gezeigt.

Schritt 2.1: Löschen Sie alle Inhalte im Ordner **C:\Program Files\Cisco\AMP\tetra\Plugins**, wie im Bild gezeigt



Schritt 2.2: Löschen Sie alle Inhalte im **C:\Program Files\Cisco\AMP\update\Plugins** -Ordner, wie im Bild gezeigt.



Schritt 3: Starten Sie den Dienst **Cisco AMP für Endgeräte Connector 7.0.5**, wie im Bild gezeigt.



Services (Local)

Cisco AMP for Endpoints Connector 7.0.5

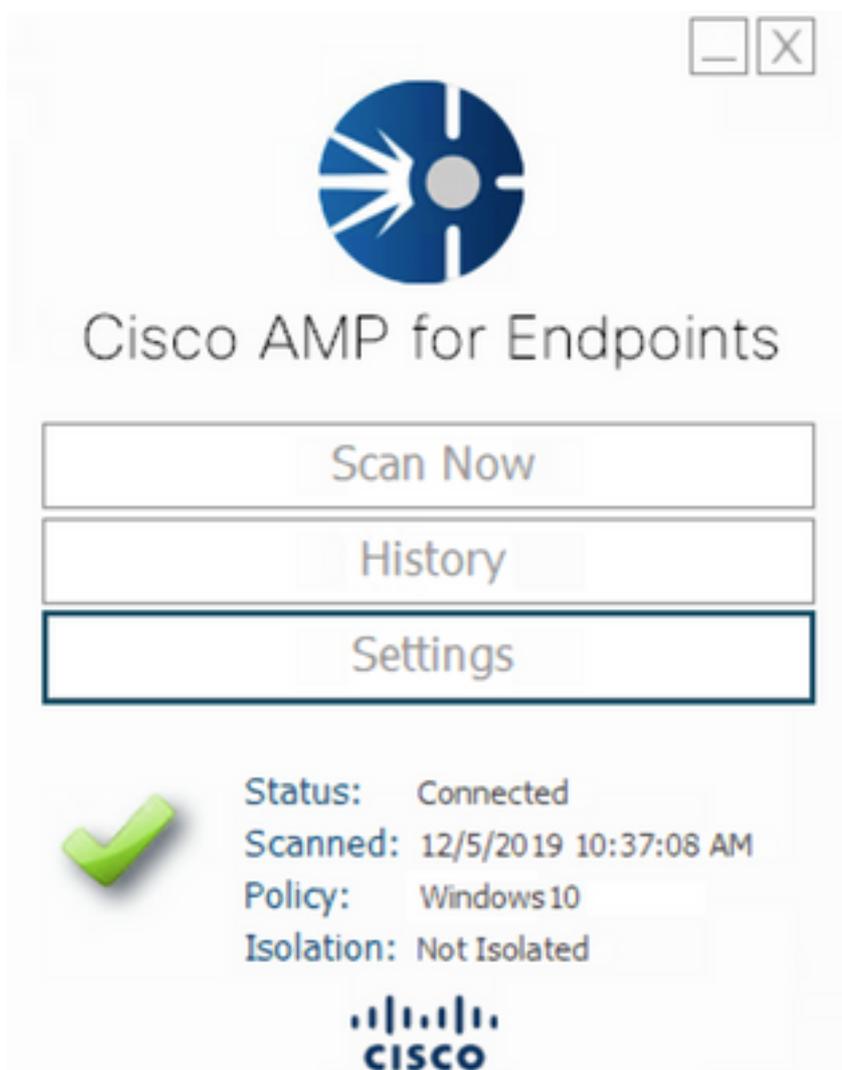
[Start](#) the service

Description:

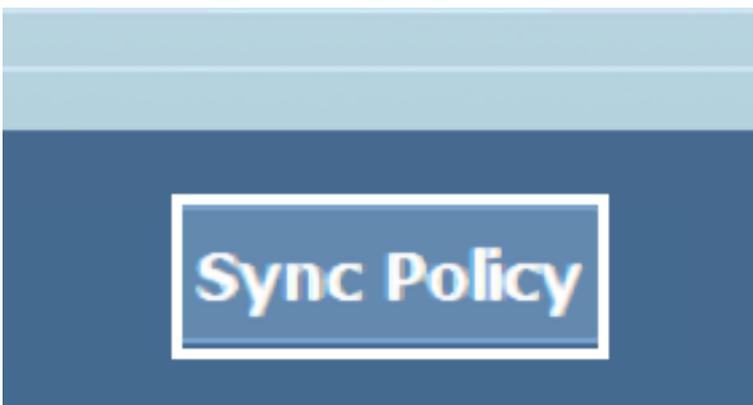
Cisco AMP for Endpoints Connector
7.0.5

Schritt 4: Öffnen Sie die AMP-Benutzeroberfläche, wie im Bild gezeigt.

Schritt 4.1: Klicken Sie auf **Einstellungen** wie im Bild gezeigt.



Schritt 4.2: Wählen Sie **Synchronisierungsrichtlinie** wie im Bild gezeigt aus.



Schritt 5: Wenn die Policy synchronisiert wird, werden die Tetra-Definitionen heruntergeladen.

Hinweis: Sobald die Definitionen heruntergeladen wurden, ist der AMP-Anschluss der Standard-AV, wie im Bild gezeigt.

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](#)

Auch wenn die TETRA-Definitionen automatisch heruntergeladen werden, können Sie manuell eine Definitions-Aktualisierung erzwingen. Das hängt von Ihren Anforderungen ab.

Zugehörige Informationen

- [AMP4E - Video zu TETRA-Definitionen](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)