# 手動によるTETRA定義の更新の強制: Cisco Secure Endpoints

### 内容

<u>概要</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>トラブルシュート</u>
関連情報

### 概要

このドキュメントでは、Cisco Secure Endpoints(AMP)で新しいTETRA定義を手動で強制する手順について説明します。

著者: Cisco TACエンジニア、Yeraldin Sanchez、Javier MartinezおよびUriel Torres

### 前提条件

#### 要件

次の項目に関する知識があることが推奨されます。

- Windows OS
- AMP for Endpoints

#### 使用するコンポーネント

このドキュメントの情報は、Cisco Secure Endpoint(AMP)for Windowsに基づいています。

このドキュメントの情報は、特定の環境にあるデバイスから作成されたものです。

• Windows 10デバイス

• AMPコネクタ7.0.5バージョン

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

### 背景説明

『User Guide, Tetra is a full antivirus solution for Cisco Secure Endpoint Solution』を参照してく ださい。最高の保護を得るには、Cisco Secure Endpointとともに使用する必要があります。3つ の<sup>サードパーティ</sup>AVがインストールされている場合は、TETRAの適切なインストールと動作を保証 するために、他のA/Vを削除する必要があります。TETRAは、定義のダウンロード時にも大きな 帯域幅を消費する可能性があります。

注意:テトラは、大規模な導入の前にテスト環境で実行する必要があります。

TETRAエンジンが有効で、その定義が最新の場合AMPバージョン6.3.1を使用するため、 Windows Defenderを無効にする必要があります。したがって、Cisco Secure Endpointは、アク ティブなウイルス対策および脅威保護プロバイダーとして指定されます。

定義は自動的にダウンロードされますが、手動でTETRA定義を更新することもできます。

### トラブルシュート

注:Cisco Secure Endpointバージョン7.2.7以降では、引数'-forceupdate'を使用してコネクタに強 制的にアップデートをフェッチさせることができます

C:\Program Files\Cisco\AMP\7.2.7\sfc.exe -forceupdate バージョン7.2.7以降の定義を強制的に更新するには、このガイドに従ってください。

ステップ1:AMPサービスを停止します。

•パスワード保護がない場合

ステップ1.1:図に示すようにServices.mscを開きます。

≡	All	Apps	Documents	Settings	Web
ሴ	Best m	atch			
0	Ċ,	Services App			

ステップ1.2:図に示すように、[Services] > [Cisco AMP for Endpoints Connector 7.0.5]に移動します。

Services (Local)			
Cisco AMP for Endpoints Connector 7.0.5	Name ^	Description	Status
Stop the service Pause the service Restart the service	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		
Description	Cisco AMP for Endpoints Connector 7.0.5	Cisco AMP	Running
Cisco AMP for Endpoints Connector 7.0.5	4 4		Running Running

ステップ1.3:図に示すように、AMPサービスを停止します。

Service Control	×
Windows is attempting to stop the following service on Local Computer Cisco AMP for Endpoints Connector 7.0.5	
Close	

• パスワード保護がある場合

ステップ1.4:AMPユーザインターフェイスを開き、図に示すように[Settings]を選択します。





# Cisco AMP for Endpoints

Scan Now History

Settings



Status: Connected Scanned: 12/5/2019 10:37:08 AM Policy: Windows10 Isolation: Not Isolated

cisco

ステップ1.5:図に示すように、[Cisco AMP for Endpoints Settings]に移動します。

General Settings	•
Scan Settings	
Notification Settings	•
Proxy Settings	•
Cisco AMP Connector Settings	•
Service Status:	Started
Password:	
Stop Service	
Debug Logging Status:	Stopped

ステップ1.6:パスワードを入力し、図に示すように[Stop Service]をクリックします。

General Settings		
Scan Settings	•	
Notification Settings	•	
Proxy Settings	•	
Cisco AMP Connector Sett	ings 🔺	
Service Status:	Stopped	
To start the service plea	se use the Windows Service	Control Manager
Debug Logging Status:	Stopped	
Enable Debug Logging		

<sub>ステップ2 : 図</sub>に示すように、AMPフォルダに移動します。通常は**C:\Program Files\Cisco\AMP**にあり ます。

ステップ2.1:図に示すように、C:\Program Files\Cisco\AMP\tetra\Plugins\フォルダ内のすべての コ**ンテンツ**を削除します

File Home	Share	View			
← → × ↑ 📙	> This	PC > Local Disk (C:) > Program Files	> Cisco > AMP > tetra >	Plugins	
A Chick scores		Name	Date modified	Туре	Size
P QUICK access		7zip.xmd	11/8/2019 1:02 PM	XMD File	41 KB
Desktop	1	File Access Denied	-	0 X	6 K8
Downloads	~				17 K3
Documents	1	You'll need to provide administrat	or permission to delete this file		6 K3
Fictures	1	7zip.xmd			48 KS
AMP	*	Type: XMD File			13 KB
h Music	1	Date modified: 11/8/2019 1:02 PM			2 KS
Videos					1 KI
in the contract of the contrac		Do this for all current items			10 KB
<ul> <li>OneDrive</li> </ul>		Continue	Stin	ancel	652 KB
		Concinde	sop C		12.405 KR

ステップ2.2:図に示すように、C:\Program Files\Cisco\AMP\update\Plugins\ フォルダ内のすべてのコンテンツを削除します。

📑   🕑 📙 🖬   Plu	gins				
File Home	Share	View			
← → * ↑ 📕	> This	PC > Local Disk (C:) > Program Files	> Cisco > AMP > update	e > Plugins	
1 A idaama		Name	Date modified	Туре	Size
P Quick access		7zip.xmd	11/8/2019 1:02 PM	XMD File	41 KB
Desktop	1	File Access Denied	-	• ×	6 KB
Downloads	~		17 KB		
Documents	Documents 🖈 You'll need to provide administrator permission to delete this file				6 KB
Pictures	*	arjamd		48 KB	
AMP	*	Type: XMD File Size: 9.70 KB		13 KB	
Music	1	Date modified: 10/14/	2 KB		
Videos				1 KB	
		Do this for all current items			10 KB
<ul> <li>OneDrive</li> </ul>		Continue	Skip	ancel	652 KB
		Comme			13,455,60

ステップ3:図に示すようにCisco AMP for Endpoints Connector 7.0.5サービスを開始します。



# Cisco AMP for Endpoints Connector 7.0.5

# Start the service

Description: Cisco AMP for Endpoints Connector 7.0.5

ステップ4:図に示すように、AMPユーザインターフェイスを開きます。

ステップ4.1:図に示すように、[Settings]をクリックします。





# Cisco AMP for Endpoints

Scan Now

History

Settings



Status: Connected Scanned: 12/5/2019 10:37:08 AM Policy: Windows10 Isolation: Not Isolated

cisco

ステップ4.2:図に示すように[Sync Policy]を選択します。



ステップ5:ポリシーが同期されると、Tetra定義がダウンロードされます。

**注**:定義がダウンロードされると、図に示すように、AMPコネクタがデフォルトのAVになります。

# ♡ 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

TETRA定義が自動的にダウンロードされても、手動で定義の更新を強制できます。要件によって 異なります。

### 関連情報

<u>AMP4E - TETRA定義更新ビデオ</u>
テクニカル サポートとドキュメント – Cisco Systems