手动强制更新TETRA定义 — 思科安全终端

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用目信息</u> <u>故障排除</u> 相关信息

简介

本文档介绍在思科安全终端(AMP)中手动强制新TETRA定义的过程。

作者: Jesus Javier Martinez和Uriel Torres,编辑者: Cisco TAC工程师Yeraldin Sanchez。

先决条件

要求

Cisco 建议您了解以下主题:

- Windows操作系统
- 面向终端的 AMP

使用的组件

本文档中的信息基于适用于Windows的思科安全终端。

本文档中的信息是从特定环境中的设备创建的:

- Windows 10设备
- AMP连接器7.0.5版

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

请参阅《用户指南》,Tetra是适用于思科安全终端解决方案的完整防病毒解决方案。它应与思科安 全终端一起使用,以获得最佳保护。如果我们安装了第^{三方}AV,我们应移除其他A/V,以确保 TETRA的正确安装和运行。下载定义时,TETRA也会消耗大量带宽。 警告:在大规模部署之前,必须在测试环境中执行Tetra。

由于AMP版本6.3.1启用TETRA引擎且其定义为最新,因此需要禁用Windows Defender,因此 Cisco安全终端被指定为活动的防病毒和威胁保护提供商。

定义会自动下载,但是,您可以强制手动更新TETRA定义。

故障排除

注意:在思科安全终端版本7.2.7及更高版本上,您可以强制连接器使用参数" — forceupdate"获取 更新

C:\Program Files\Cisco\AMP\7.2.7\sfc.exe -forceupdate 为了强制在7.2.7版以下更新定义,您可以按照本指南操作。

步骤1.停止AMP服务。

• 如果您没有密码保护

步骤1.1.打**开Services.msc**,如图所示。



步骤1.2.导航至Services > Cisco AMP for Endpoints Connector 7.0.5,如图所示。



步骤1.3.停止AMP服务,如图所示。

Service Control

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

Cisco AMP for Endpoints Connector 7.0.5

Close	

• 如果您有密码保护

步骤1.4.打开AMP用户界面并选择设置(如图所示)。



步骤1.5.导航至适**用于终端的思**科AMP设置,如图所示。

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

步骤1.6.输入密码,然后单击"停**止服务**",如图所示。

General Settings	T		
Scan Settings	T		
Notification Settings	T		
Proxy Settings	T		
Cisco AMP Connector Setting	5 🔺		
Service Status:	Stopped		
To start the service please	use the Windows Service	vice Control Mana	ager
Debug Logging Status:	Stopped		
Enable Debug Logging			

步骤₂.导航至AMP文件夹,通常位于C:\Program Files\Cisco\AMP,如图所示。

步骤2.1.删除C:\Program Files\Cisco\AMP\tetra\Plugins\文件夹内的所有内容,如图所示

File Home	gins Share	View			
← → × ↑	> This	PC > Local Disk (C:) > Program Files	> Cisco > AMP > tetra >	Plugins	
+ Ould access		Name	Date modified	Туре	Size
Parking Decker	A CONCERCIENT	7zip.xmd	11/8/2019 1:02 PM	XMD File	41 KB
Desktop	Desktop x*	File Access Denied	-	• ×	6 K.B
Downloads				17 KB	
Documents	. *	You'll need to provide administrat		6 KB	
Fictures	*	7zip.xmd		48 KB	
AMP	*	Type: XMD File	13 KB		
h Music	*	Date modified: 11/8/	2 K8		
Videos			1 KB		
	Do this for all current items				
 OneDrive 		Continue Skin Cancel			652 KB
_	_	Contract	sup 6	in the	12.405.KR

步骤2.2.删除C:\Program Files\Cisco\AMP\update\Plugins\ 文件夹内的所有内容,如图所示。



步骤3.启动面向终端的思科AMP Endpoints Connector 7.0.5服务,如图所示。



步骤₄.打开AMP用户界面,如图所示。

步骤4.1.单击"设置",如图所示。





Cisco AMP for Endpoints

Scan Now

History

Settings



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

cisco

步骤4.2.选择"同**步策略**",如图所示。



步骤₅.当pólicy同步时,将下载Tetra定义。

注意:下载定义后,AMP连接器即为默认AV,如图所示。

♡ 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

即使TETRA定义自动下载,也可以手动强制更新定义。这取决于您的要求。

相关信息

• AMP4E - TETRA定义更新视频

• <u>技术支持和文档 - Cisco Systems</u>