

忘记密码时卸载AMP连接器的步骤

目录

[简介](#)

[连接器已连接](#)

[连接器已断开](#)

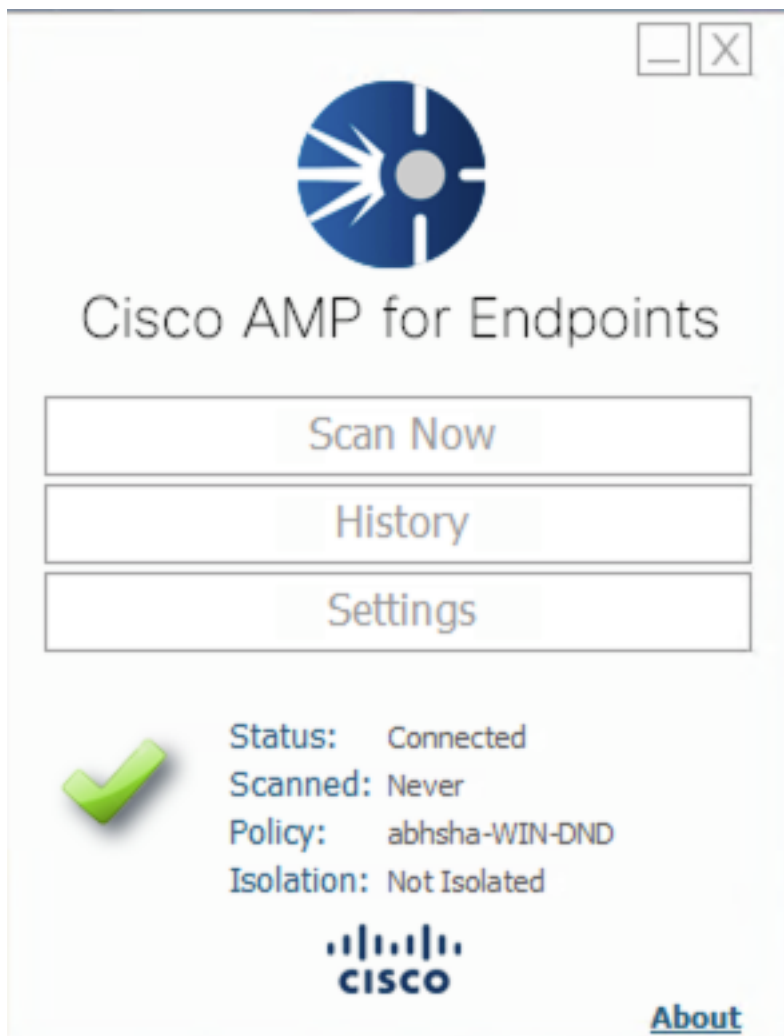
简介

本文档介绍卸载思科高级恶意软件防护(AMP)连接器的过程，以防因连接器保护功能而阻止卸载，而该功能要求提供密码，并且忘记了该密码。本例中有2种场景，具体取决于连接器是否显示“已连接”到AMP云。它仅适用于Windows操作系统，因为连接器保护是仅在Windows操作系统上可用的功能。

连接器已连接

步骤1. 点击托盘图标并打开面向终端的思科AMP连接器。

步骤2. 确保连接器显示为已连接。



步骤3.注意策略已分配给该连接器。

步骤4.导航至面向终端的AMP控制台并搜索之前记录的策略。

步骤5.展开策略，然后点击Duplicate，如图所示。

The screenshot shows the configuration page for a policy named 'abhsha-WIN-DND'. The interface is divided into several sections: 'Modes and Engines', 'Exclusions', 'Proxy', and 'Groups'. The 'Exclusions' section lists 'AbhishekSha-TEST' and 'Microsoft Windows Default'. The 'Proxy' section is 'Not Configured'. The 'Groups' section lists 'abhsha-DND'. Below these sections is the 'Outbreak Control' section, which includes 'Custom Detections - Simple', 'Custom Detections - Advanced', 'Application Control', and 'Network'. At the bottom of the page, there are several buttons: 'View Changes', 'Download XML', 'Duplicate' (highlighted with a red circle), 'Edit', and 'Delete'. The 'Duplicate' button is a blue button with a copy icon.

步骤6.新策略，称为“.....的副本”的双曲余切值。单击Edit以编辑此策略，如图所示。

The screenshot shows the configuration page for a policy named 'Copy of abhsha-WIN-DND'. The interface is divided into several sections: 'Modes and Engines', 'Exclusions', 'Proxy', and 'Groups'. The 'Exclusions' section lists 'AbhishekSha-TEST' and 'Microsoft Windows Default'. The 'Proxy' section is 'Not Configured'. The 'Groups' section is 'Not Configured'. Below these sections is the 'Outbreak Control' section, which includes 'Custom Detections - Simple', 'Custom Detections - Advanced', 'Application Control', and 'Network'. At the bottom of the page, there are several buttons: 'View Changes', 'Download XML', 'Duplicate', 'Edit' (highlighted with a red circle), and 'Delete'. The 'Edit' button is a blue button with a pencil icon.

步骤7.在“编辑策略”页面，导航至“高级设置”>“管理功能”。

步骤8.在Connector Password Protection字段中，用新密码替换该密码，如图所示，可以重新调用该密码。

Modes and Engines

Exclusions
2 exclusion sets

Proxy

Outbreak Control

Product Updates

Advanced Settings

- Administrative Features
- Client User Interface
- File and Process Scan
- Cache
- Endpoint Isolation

Send User Name in Events ⓘ

Send Filename and Path Info ⓘ

Heartbeat Interval: 15 minutes ⓘ

Connector Log Level: Debug ⓘ

Tray Log Level: Default ⓘ

Enable Connector Protection ⓘ

Connector Protection Password:

Automated Crash Dump Uploads ⓘ

Command Line Capture ⓘ

Command Line Logging ⓘ

步骤9.单击“保存”按钮以保存此策略。

步骤10.导航到**Management > Groups**并创建新组。

Groups [View All Changes](#)

Search

步骤11.输入组名，并选择Windows策略作为之前编辑的策略。单击“保存”按钮，如图所示。

< New Group

Name	<input type="text" value="TZ-TEST-GROUP"/>
Description	<input type="text"/>
Parent Group	<input type="text"/>
Windows Policy	<input type="text" value="Copy of abhsha-WIN-DND - #1"/>
Android Policy	<input type="text" value="Default Policy (Vanilla Android)"/>
Mac Policy	<input type="text" value="Default Policy (Vanilla OSX)"/>
Linux Policy	<input type="text" value="Default Policy (Vanilla Linux)"/>
Network Policy	<input type="text" value="Default Policy (network_policy)"/>
iOS Policy	<input type="text" value="Default Policy (Audit)"/>

步骤12. 导航至 **Management > Computers**，并搜索尝试卸载AMP连接器的计算机。

步骤13. 展开计算机，然后单击“移动到组”。从显示的对话框中，选择之前创建的组。

DESKTOP-RESMRDG in group abhsha-DND		Definitions Outdated	
Hostname	DESKTOP-RESMRDG	Group	abhsha-DND
Operating System	Windows 10 Pro	Policy	abhsha-WIN-DND
Connector Version	7.2.7.11687	Internal IP	10.197.225.213
Install Date	2020-04-23 12:35:56 IST	External IP	72.163.220.18
Connector GUID	48838c52-f04f-454a-8c3a-5e55f7366775	Last Seen	2020-04-23 12:49:01 IST
Definition Version	TETRA 64 bit (None)	Definitions Last Updated	None
Update Server	tetra-defs.amp.cisco.com		
Processor ID	0fabfbff000006f2		

[Events](#) [Device Trajectory](#) [Diagnostics](#) [View Changes](#)

步骤14. 等待策略在终端上更新。通常需要30分钟到1小时，具体取决于配置的间隔。

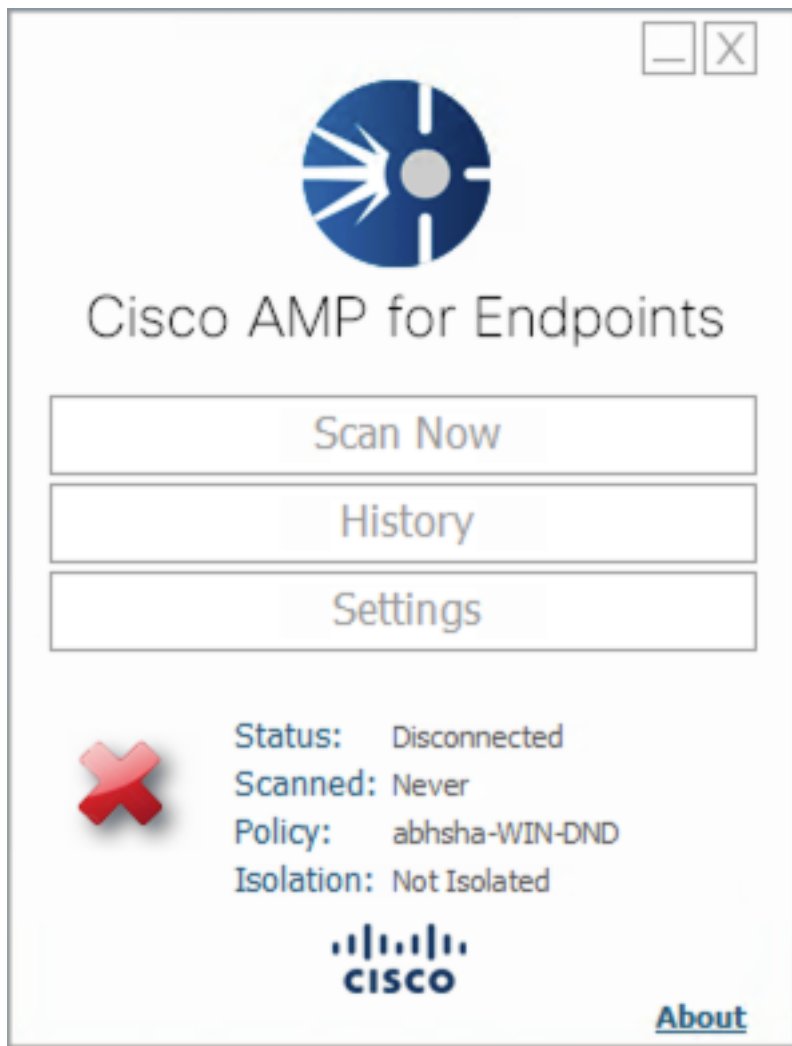
步骤15.策略在终端上更新后，您将能够使用新配置和密码卸载连接器。

连接器已断开

如果连接器与AMP云断开连接，则必须能够在安全模式下启动计算机。

步骤1.点击托盘图标并打开面向终端的思科AMP连接器。

步骤2.确保连接器显示为已断开。



步骤3.记录已分配给该连接器的策略。

步骤4.导航至面向终端的AMP控制台并搜索之前记录的策略。

步骤5.展开策略，然后点击Duplicate，如图所示。

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	AbhishekSha-TEST	Not Configured	abhsa-DND 2
Network	Block	Microsoft Windows Default		
Malicious Activity Prot...	Quarantine			
System Process Protection	Protect			
Outbreak Control				
Custom Detections - Simple		Custom Detections - Advanced	Application Control	Network
Not Configured		Not Configured	Not Configured	Not Configured

[View Changes](#) Modified 2020-04-23 12:38:35 IST Serial Number 13919
 [Download XML](#)

[Duplicate](#)
[Edit](#)
[Delete](#)

步骤6.新策略，称为“.....的副本”的双曲余切值。单击“编辑”以编辑此策略。

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	AbhishekSha-TEST	Not Configured	Not Configured
Network	Block	Microsoft Windows Default		
Malicious Activity Prot...	Quarantine			
System Process Protection	Protect			
Outbreak Control				
Custom Detections - Simple		Custom Detections - Advanced	Application Control	Network
Not Configured		Not Configured	Not Configured	Not Configured

[View Changes](#) Modified 2019-05-21 12:12:01 IST Serial Number 12267
 [Download XML](#)
[Duplicate](#)
[Edit](#)
[Delete](#)

步骤7.在Edit Policy (编辑策略) 页面，导航至Advanced Settings (高级设置) > **Administrative Features (管理功能)**。

步骤8.在Connector Password Protection **字段**中，将口令替换为可以撤回的新口令。

The screenshot shows the configuration interface for 'Advanced Settings' in the Cisco AMP console. The left sidebar contains a navigation menu with the following items: Modes and Engines, Exclusions (2 exclusion sets), Proxy, Outbreak Control, Product Updates, and Advanced Settings. Under 'Advanced Settings', the sub-menu 'Administrative Features' is selected, with other options including Client User Interface, File and Process Scan, Cache, and Endpoint Isolation.

The main configuration area includes the following settings:

- Send User Name in Events *i*
- Send Filename and Path Info *i*
- Heartbeat Interval: 15 minutes *i*
- Connector Log Level: Debug *i*
- Tray Log Level: Default *i*
- Enable Connector Protection *i*
- Connector Protection Password:
- Automated Crash Dump Uploads *i*
- Command Line Capture *i*
- Command Line Logging *i*

步骤9.单击“保存”按钮以保存此策略。

步骤10.导航至Management > Policies并搜索新复制的策略。

步骤11.展开策略，然后单击“下载XML”。将名为policy.xml的文件保存到计算机。

The screenshot shows the configuration page for a policy named 'abhsa-WIN-DND'. The page is divided into several sections:

- Modes and Engines:** Files (Quarantine), Network (Block), Malicious Activity Prot... (Quarantine), System Process Protection (Protect).
- Exclusions:** AbhishekSha-TEST, Microsoft Windows Default.
- Proxy:** Not Configured.
- Groups:** abhsa-DND (2 notifications).
- Outbreak Control:** Custom Detections - Simple (Not Configured), Custom Detections - Advanced (Not Configured), Application Control (Not Configured), Network (Not Configured).

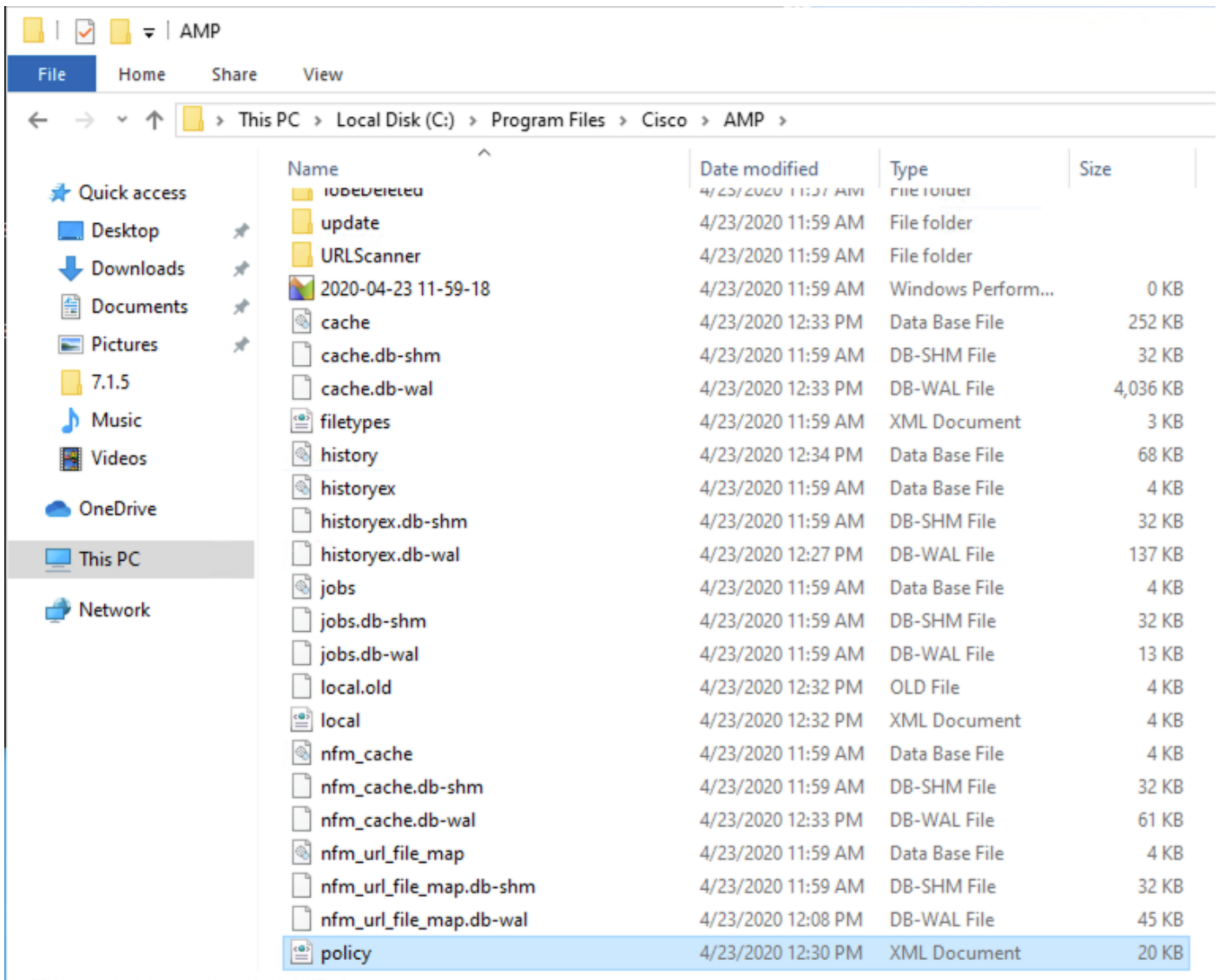
At the bottom of the page, there is a metadata bar showing 'View Changes', 'Modified 2020-04-23 12:38:35 IST', and 'Serial Number 13919'. Below this are four action buttons: 'Download XML', 'Duplicate', 'Edit', and 'Delete'.

步骤12.将此策略.xml复制到受影响的终端。

步骤13.在安全模式下重新启动受影响的终端。

步骤14.一旦受影响的终端处于安全模式，请导航至C:\Program Files\Cisco\AMP。

步骤15.在此文件夹中，搜索名为policy.xml的文件，并将其重命名为policy_old.xml。



步骤16.现在，将之前复制的policy.xml粘贴到此文件夹。

步骤17.复制文件后，可以正常执行卸载，并且必须在密码提示符下输入新配置的密码。

步骤18.这是可选步骤。由于连接器在计算机断开连接时被卸载，计算机条目将保留在控制台上。因此，您可以导航至Management > Computers并展开受影响的终端。单击Delete以删除终端。