

パスワードを忘れた場合にAMPコネクタをアンインストールする手順

内容

[概要](#)

[コネクタが接続されています](#)

[コネクタが切断されました](#)

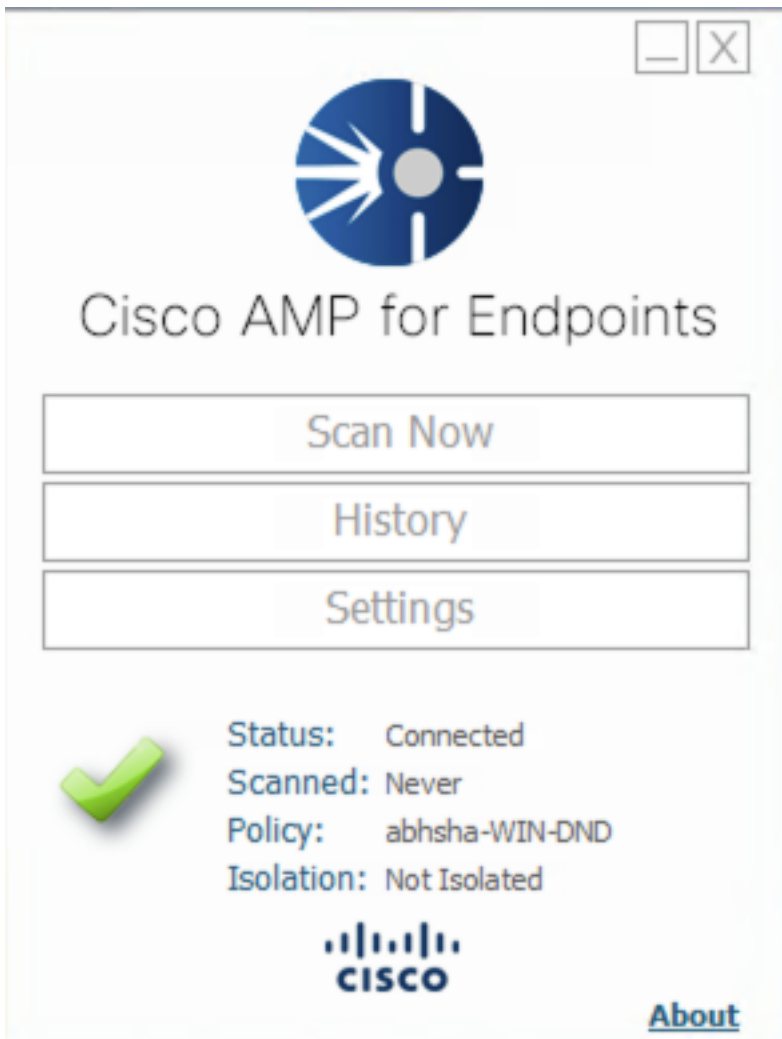
概要

このドキュメントでは、パスワードの入力が必要なコネクタ保護機能によってアンインストールがブロックされ、パスワードを忘れた場合にCisco Advanced Malware Protection(AMP)コネクタをアンインストールする手順について説明します。このケースには2つのシナリオがあり、コネクタがAMPクラウドに「Connected」と表示されるかどうかによって異なります。Connector ProtectionはWindows OSでのみ使用可能な機能であるため、Windows OSにのみ適用されます。

コネクタが接続されています

ステップ1：トレイアイコンをクリックし、Cisco AMP for Endpoints Connectorを開きます。

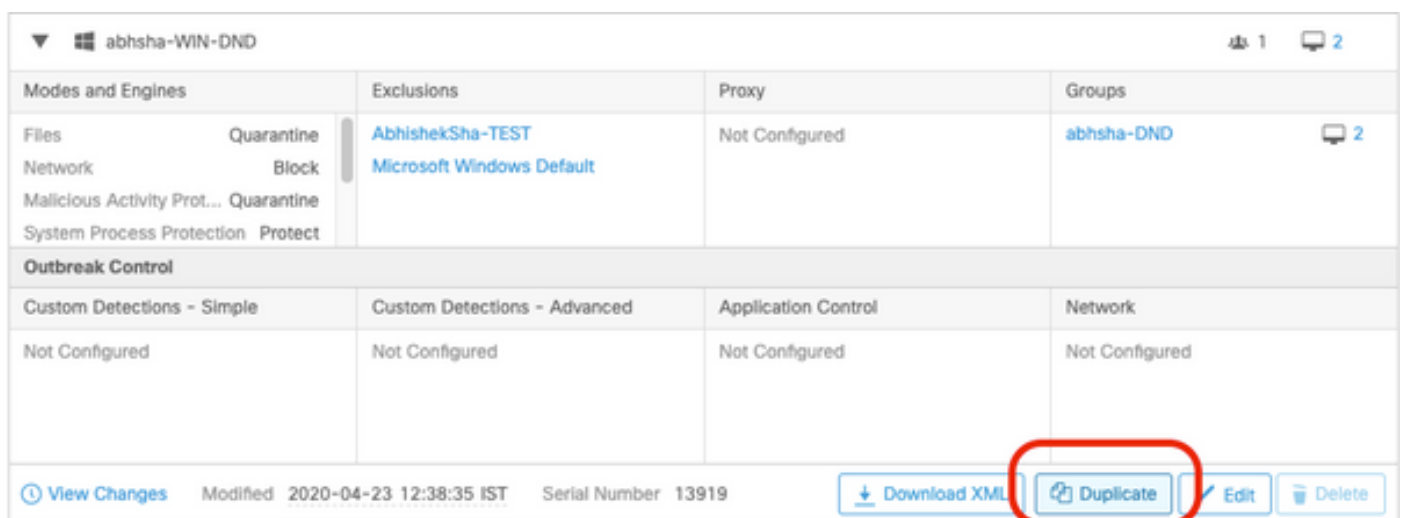
ステップ2：コネクタが接続済みと表示されていることを確認します。



ステップ3 : ポリシーがそのコネクタに割り当てられていることに注意してください。

ステップ4:AMP for Endpointsコンソールに移動し、前にメモしたポリシーを検索します。

ステップ5 : ポリシーを展開し、図に示すように[Duplicate]をクリックします。



ステップ6:「コピー」という新しいポリシー will be created.図に示すように、このポリシーを編集するには、[Edit]をクリックします。

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](#)

ステップ7:[Edit Policy]ページで、[Advanced Settings] > [Administrative Features]に移動します。

ステップ8:[Connector Password Protection]フィールドで、パスワードを、図に示すように呼び出し可能な新しいパスワードに置き換えます。

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 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: i
- Automated Crash Dump Uploads i
- Command Line Capture i
- Command Line Logging i

ステップ9:[Save]ボタンをクリックし、このポリシーを保存します。

ステップ10:[管理(Management)] > [グループ(Groups)]に移動し、新しいグループを作成します。

Groups [View All Changes](#)

ステップ11: グループ名を入力し、以前に編集したポリシーとしてWindowsポリシーを選択します。図に示すように[保存]ボタンをクリックします。

< 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)"/>

ステップ12:[Management] > [Computers]に移動し、AMPコネクタをアンインストールしようとするコンピュータを検索します。

ステップ13: コンピュータを展開し、[グループに移動]をクリックします。表示されるダイアログボックスで、以前に作成したグループを選択します。

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](#)

ステップ14：エンドポイントでポリシーが更新されるまで待ちます。通常は30分から1時間かかり、設定された間隔によって異なります。

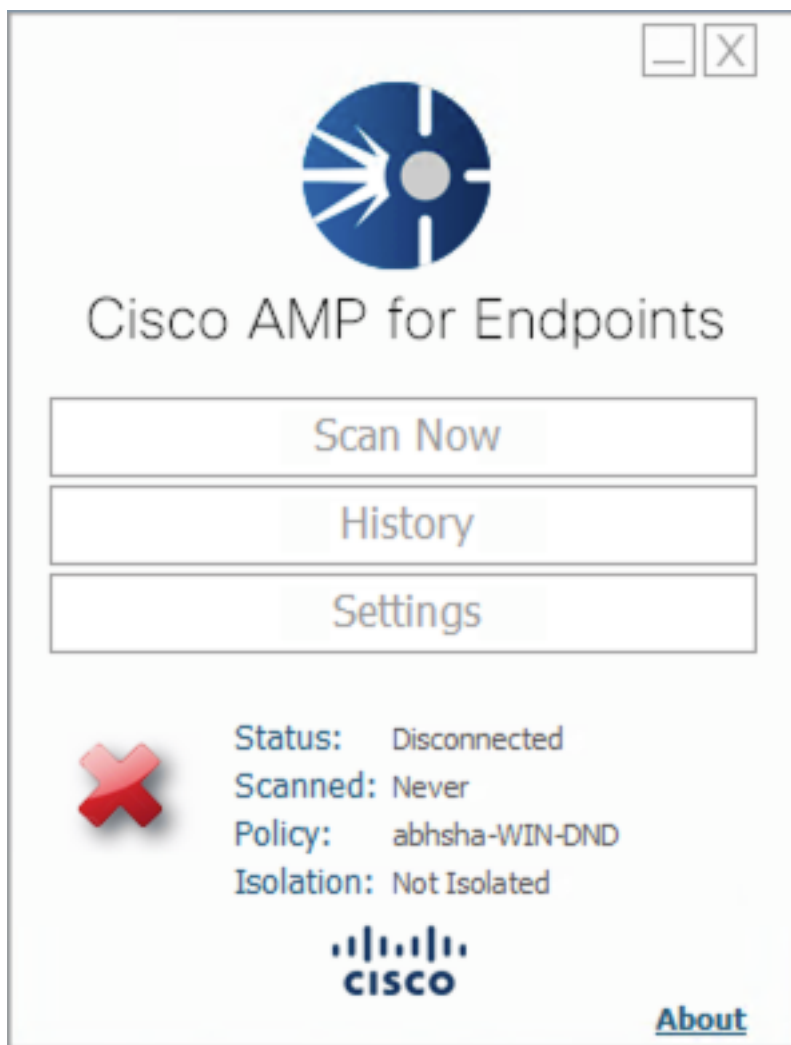
ステップ15：エンドポイントでポリシーが更新されると、新しく設定したパスワードを使用してコネクタをアンインストールできるようになります。

コネクタが切断されました

コネクタがAMPクラウドから切断されている場合は、コンピュータをセーフモードで起動できることが重要です。

ステップ1：トレイアイコンをクリックし、Cisco AMP for Endpoints Connectorを開きます。

ステップ2：コネクタが接続解除と表示されていることを確認します。



ステップ3：そのコネクタに割り当てられているポリシーをメモします。

ステップ4:AMP for Endpointsコンソールに移動し、前にメモしたポリシーを検索します。

ステップ5：ポリシーを展開し、図に示すように[Duplicate]をクリックします。

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	AbhishekSha-TEST	Not Configured	abhsha-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](#)

ステップ6: 「コピー」という新しいポリシー will be created.[Edit]をクリックし、このポリシーを編集します。

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](#)

ステップ7:[Edit Policy]ページで、[Advanced Settings] > [Administrative Features]に移動します。

ステップ8:[Connector Password Protection]フィールドで、パスワードをリコール可能な新しいパスワードに置き換えます。

Modes and Engines	<input checked="" type="checkbox"/> Send User Name in Events ⓘ
Exclusions 2 exclusion sets	<input checked="" type="checkbox"/> Send Filename and Path Info ⓘ
Proxy	Heartbeat Interval: 15 minutes ⓘ
Outbreak Control	Connector Log Level: Debug ⓘ
Product Updates	Tray Log Level: Default ⓘ
Advanced Settings	<input checked="" type="checkbox"/> Enable Connector Protection ⓘ
Administrative Features	Connector Protection Password:
Client User Interface	<input checked="" type="checkbox"/> Automated Crash Dump Uploads ⓘ
File and Process Scan	<input checked="" type="checkbox"/> Command Line Capture ⓘ
Cache	<input type="checkbox"/> Command Line Logging ⓘ
Endpoint Isolation	

ステップ9:[Save]ボタンをクリックし、このポリシーを保存します。

ステップ10:[Management] > [Policies]に移動し、新しく複製されたポリシーを検索します。

ステップ11：ポリシーを展開し、[XMLのダウンロード]をクリックします。policy.xmlという名前のファイルがマシンに保存されます。

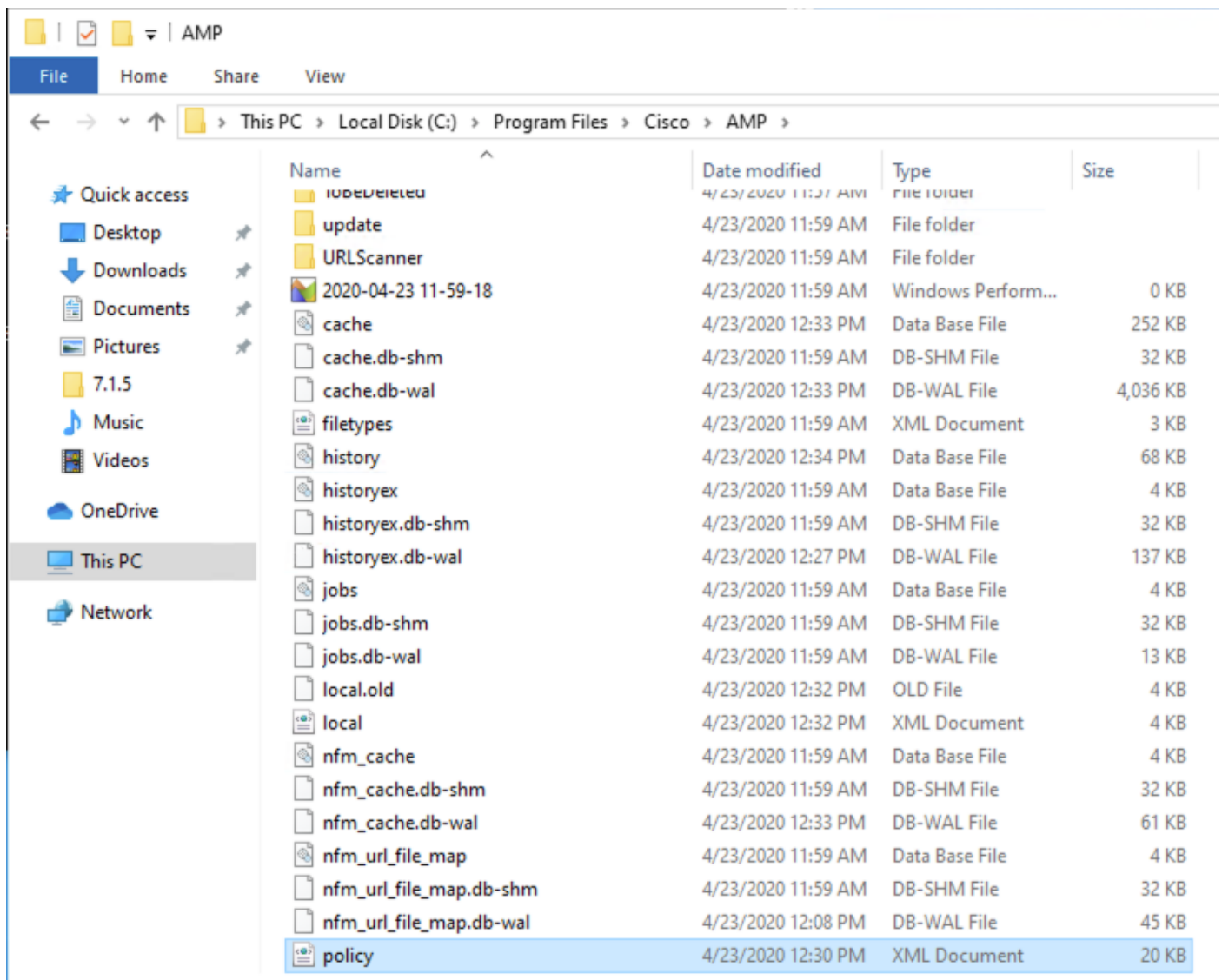
absha-WIN-DND				1	2
Modes and Engines	Exclusions	Proxy	Groups		
Files Network Malicious Activity Prot... System Process Protection	Quarantine Block Quarantine Protect	Not Configured	absha-DND ⓘ 2		
Outbreak Control					
Custom Detections - Simple	Custom Detections - Advanced	Application Control	Network		
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		

ステップ12：このpolicy.xmlを該当するエンドポイントにコピーします。

ステップ13：影響を受けるエンドポイントをセーフモードでリブートします。

ステップ14：影響を受けるエンドポイントがセーフモードできたら、C:\Program Files\Cisco\AMPに移動します。

ステップ15：このフォルダで、policy.xmlという名前のファイルを検索し、その名前をpolicy_old.xmlに変更します。



ステップ16：前にコピーしたpolicy.xmlをこのフォルダに貼り付けます。

ステップ17：ファイルがコピーされた後、アンインストールは正常に実行できます。パスワードプロンプトで、新しく設定したパスワードを入力する必要があります。

ステップ18：これはオプションのステップです。コンピュータの切断時にコネクタがアンインストールされたため、コンピュータのエントリはコンソールに残ります。したがって、[Management] > [Computers]に移動し、影響を受けるエンドポイントを展開できます。[Delete]をクリックして、エンドポイントを削除します。