

Verfahren zur Deinstallation des AMP Connectors bei vergessenem Kennwort

Inhalt

[Einführung](#)

[Anschluss ist verbunden](#)

[Verbindung getrennt](#)

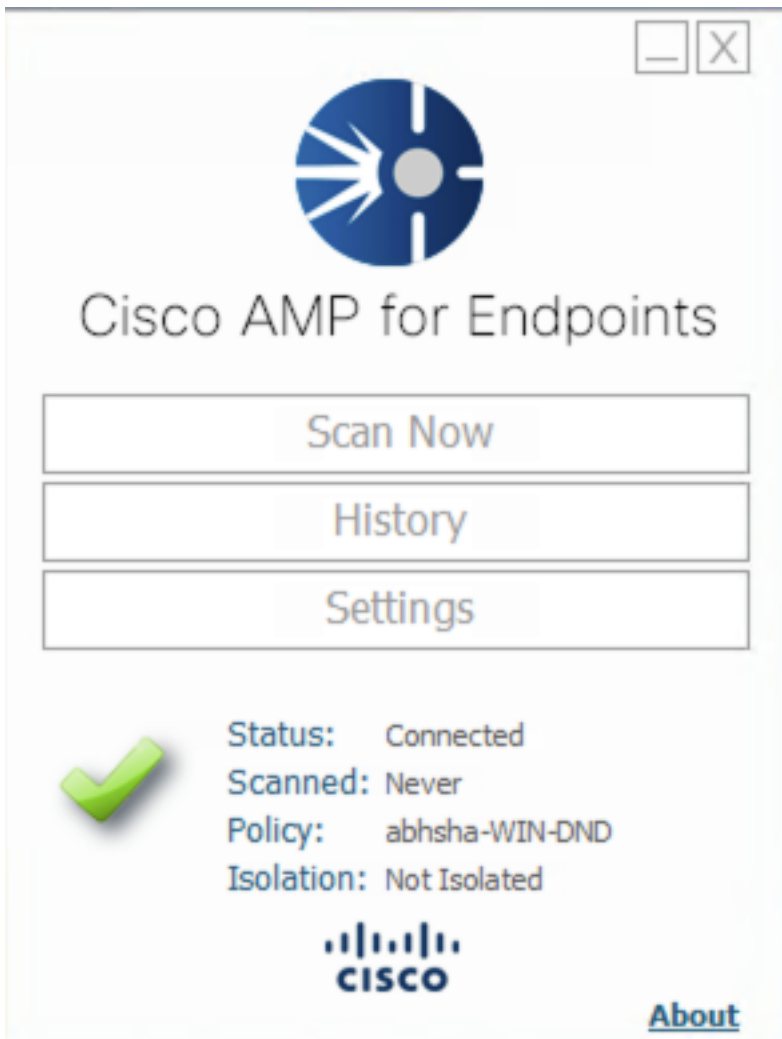
Einführung

In diesem Dokument wird das Verfahren zur Deinstallation des Cisco Advanced Malware Protection (AMP)-Connectors beschrieben, falls die Deinstallation durch die Anschlussschutzfunktion blockiert wird, für die ein Kennwort eingegeben werden muss und dieses Kennwort vergessen wird. In diesem Fall gibt es zwei Szenarien, die davon abhängen, ob der Connector "Connected" (Verbunden) zur AMP-Cloud anzeigt. Sie gilt nur für das Windows-Betriebssystem, da der Connector-Schutz eine Funktion ist, die nur unter Windows verfügbar ist.

Anschluss ist verbunden

Schritt 1: Klicken Sie auf das Taskleistensymbol, und öffnen Sie den Cisco AMP für Endpoints-Connector.

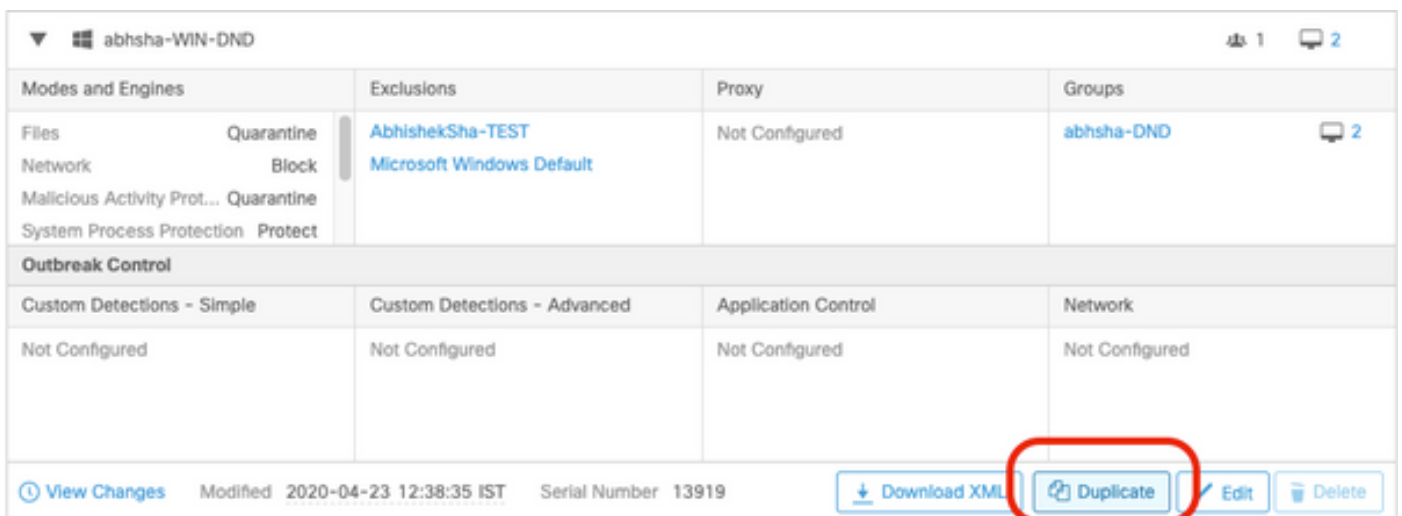
Schritt 2: Stellen Sie sicher, dass der Connector als verbunden angezeigt wird.



Schritt 3: Beachten Sie, dass die Richtlinie diesem Anschluss zugewiesen wurde.

Schritt 4: Navigieren Sie zu Ihrer AMP für Endgeräte-Konsole, und suchen Sie nach der zuvor erwähnten Richtlinie.

Schritt 5: Erweitern Sie die Richtlinie, und klicken Sie auf **Duplizieren** wie im Bild gezeigt.



Schritt 6: Eine neue Richtlinie mit dem Namen "Kopie von.." wird erstellt. Klicken Sie auf **Bearbeiten**, um diese Richtlinie wie im Bild gezeigt zu bearbeiten.

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](#)

Schritt 7: Navigieren Sie auf der Seite **Richtlinie bearbeiten** zu **Erweiterte Einstellungen > Verwaltungsfunktionen**.

Schritt 8: Ersetzen Sie im Feld **Connector Password Protection (Connector-Kennwortschutz)** das Kennwort durch ein neues Kennwort, das wie im Bild gezeigt aufgerufen werden kann.

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: i
- Connector Log Level: i
- Tray Log Level: i
- Enable Connector Protection i
- Connector Protection Password: i
- Automated Crash Dump Uploads i
- Command Line Capture i
- Command Line Logging i

Schritt 9: Klicken Sie auf die Schaltfläche **Speichern**, um diese Richtlinie zu speichern.

Schritt 10: Navigieren Sie zu **Verwaltung > Gruppen**, und erstellen Sie eine neue Gruppe.

Groups [View All Changes](#)

Schritt 11: Geben Sie einen Gruppennamen ein, und wählen Sie die **Windows-Richtlinie** als zuvor bearbeitete Richtlinie aus. Klicken Sie auf die Schaltfläche **Speichern**, wie im Bild gezeigt.

< 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)"/>

Schritt 12: Navigieren Sie zu **Verwaltung > Computer**, und suchen Sie nach dem Computer, auf dem Sie versuchen, den AMP-Anschluss zu deinstallieren.

Schritt 13: Erweitern Sie den Computer, und klicken Sie auf **Zu Gruppe verschieben**. Wählen Sie im angezeigten Dialogfeld die zuvor erstellte Gruppe aus.

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](#)

Schritt 14: Warten Sie, bis die Richtlinie auf dem Endpunkt aktualisiert wird. Dieser Vorgang dauert in der Regel zwischen 30 und 1 Stunde und hängt vom konfigurierten Intervall ab.

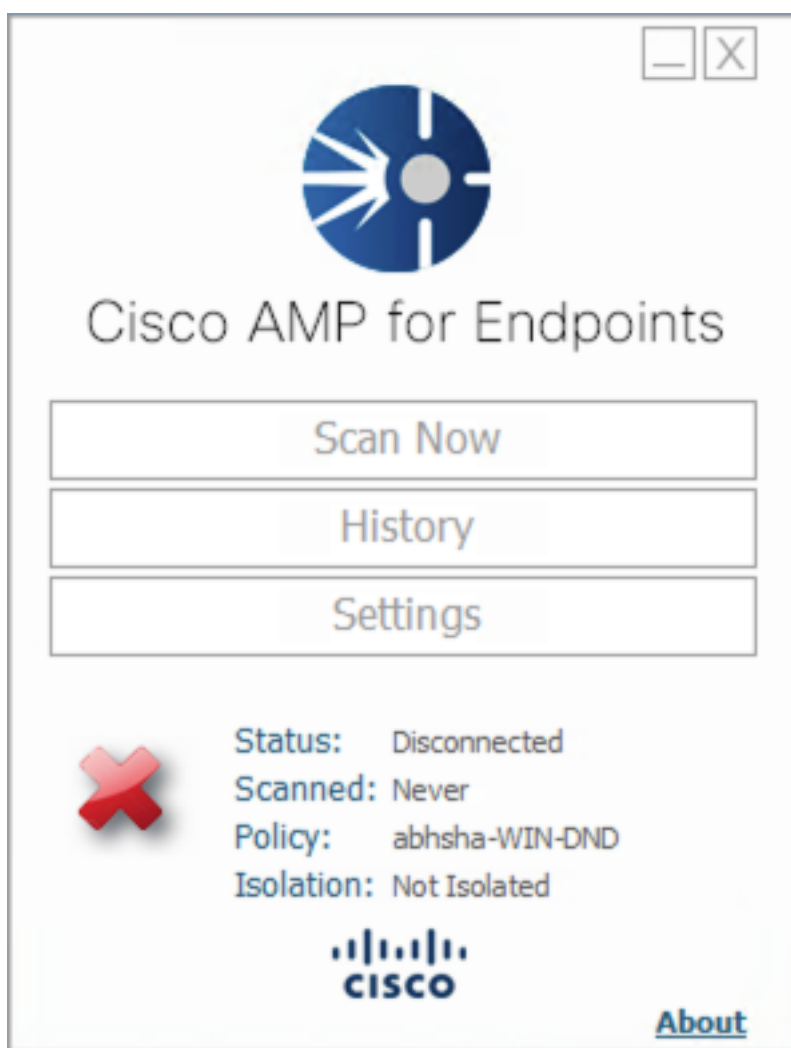
Schritt 15: Nachdem die Richtlinie auf dem Endgerät aktualisiert wurde, können Sie den Connector mithilfe des neu konfigurierten Kennworts deinstallieren.

Verbindung getrennt

Wenn der Connector von der AMP-Cloud getrennt wird, ist es wichtig, den Computer im abgesicherten Modus starten zu können.

Schritt 1: Klicken Sie auf das Taskleistensymbol, und öffnen Sie den Cisco AMP für Endpoints-Connector.

Schritt 2: Stellen Sie sicher, dass der Anschluss als getrennt angezeigt wird.



Schritt 3: Beachten Sie die Richtlinie, die diesem Anschluss zugewiesen wurde.

Schritt 4: Navigieren Sie zu Ihrer AMP für Endgeräte-Konsole, und suchen Sie nach der zuvor erwähnten Richtlinie.

Schritt 5: Erweitern Sie die Richtlinie, und klicken Sie auf **Duplizieren** wie im Bild gezeigt.

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](#)

Schritt 6: Eine neue Richtlinie mit dem Namen "Kopie von.." wird erstellt. Klicken Sie auf **Bearbeiten**, um diese Richtlinie zu bearbeiten.

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](#)

Schritt 7: Navigieren Sie auf der Seite Richtlinie bearbeiten zu **Erweiterte Einstellungen > Verwaltungsfunktionen**.

Schritt 8: Ersetzen Sie im Feld **Connector Password Protection (Connector-Kennwortschutz)** das Kennwort durch ein neues Kennwort, das Sie zurückrufen können.

Schritt 9: Klicken Sie auf die Schaltfläche **Speichern**, um diese Richtlinie zu speichern.

Schritt 10: Navigieren Sie zu **Management > Policies (Verwaltung > Richtlinien)**, und suchen Sie nach der Richtlinie, die neu dupliziert wurde.

Schritt 11: Erweitern Sie die Richtlinie, und klicken Sie auf **XML herunterladen**. Eine Datei mit dem Namen **policy.xml** wird auf Ihrem Computer gespeichert.

Modes and Engines	Exclusions	Proxy	Groups
Files Quarantine Network Block Malicious Activity Prot... Quarantine System Process Protection Protect	AbhishekSha-TEST Microsoft Windows Default	Not Configured	abhsa-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

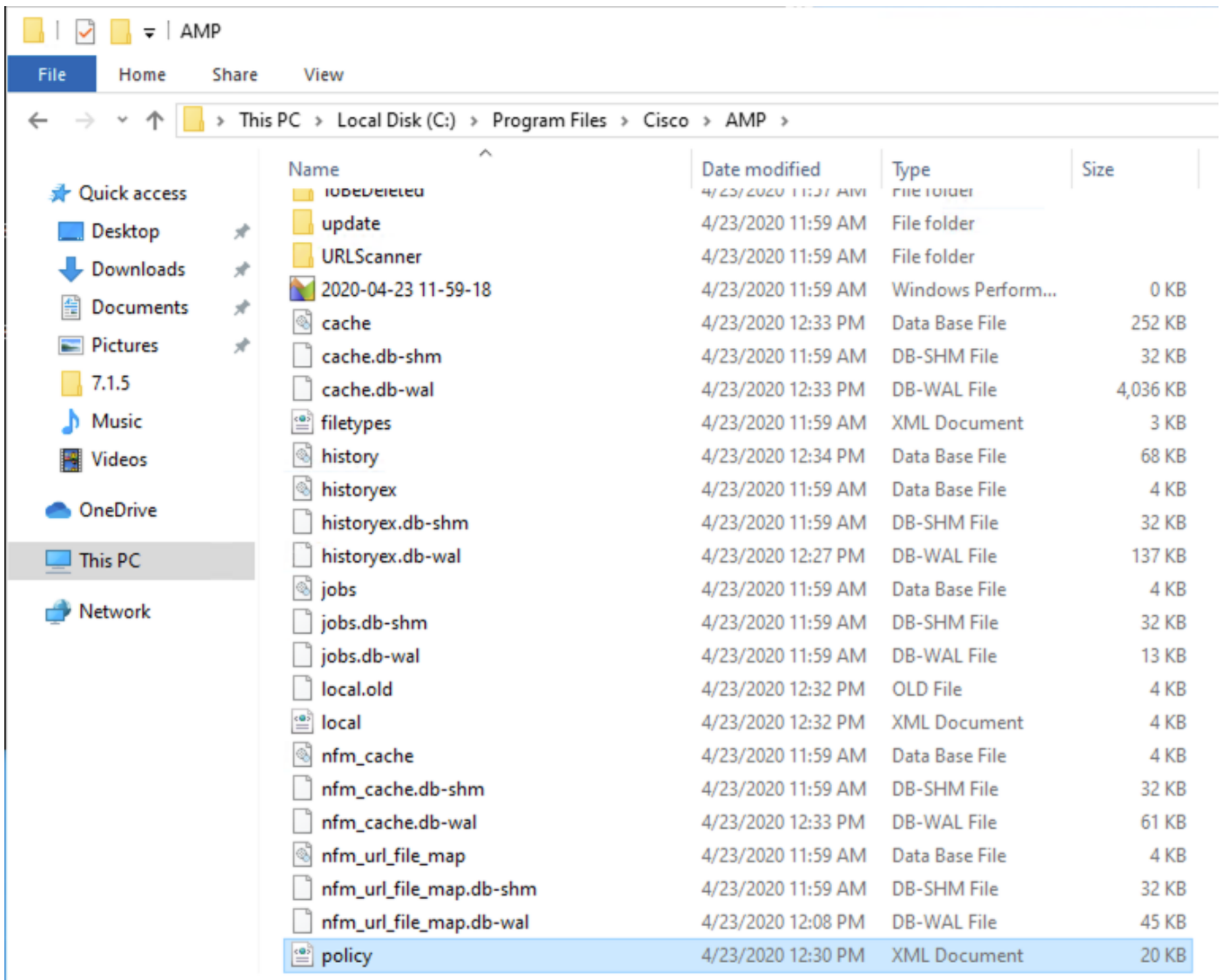
Download XML Duplicate Edit Delete

Schritt 12: Kopieren Sie diese **policy.xml** auf den betroffenen Endpunkt.

Schritt 13: Starten Sie den betroffenen Endpunkt im **abgesicherten Modus neu**.

Schritt 14: Sobald sich der betroffene Endpunkt im **abgesicherten Modus** befindet, navigieren Sie zu **C:\Program Files\Cisco\AMP**.

Schritt 15: Suchen Sie in diesem Ordner nach einer Datei mit dem Namen **policy.xml**, und benennen Sie diese in **policy_old.xml** um.



Schritt 16: Fügen Sie nun die zuvor kopierte **policy.xml** in diesen Ordner ein.

Schritt 17: Nachdem die Datei kopiert wurde, kann die Deinstallation normal ausgeführt werden. Bei der Kennworteingabeaufforderung muss das neu konfigurierte Kennwort eingegeben werden.

Schritt 18: Dies ist ein optionaler Schritt. Da der Anschluss beim Trennen der Verbindung deinstalliert wurde, bleibt der Computereintrag auf der Konsole. Daher können Sie zu **Management > Computers** navigieren und den betroffenen Endpunkt erweitern. Klicken Sie auf **Löschen**, um den Endpunkt zu löschen.