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.

Cisco AMP for Endpoints
Scan Now
History
Settings
Status: Connected Scanned: Never Policy: abhsha-WIN-DND Isolation: Not Isolated
About

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.

▼ 👹 abhsha-WIN-DND			ab.1 🖵 2
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	abhsha-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			

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.

▼ III Copy of abhsha-WIN-DND 本 0 □ 0				
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	Not Configured	
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		Send User Name in Events 💿	
Exclusions		Send Filename and Path Info ①	
2 exclusion sets	Heartbeat Interval	15 minutes 🗘 🕄	
Proxy	Connector Log Level	Debug 💠 🕄	
	Tray Log Level	Default 😫 🕄	
Outbreak Control			
Product Updates		Enable Connector Protection (1)	
Advanced Settings	Connector Protection Password		
Administrative Features			
Client User Interface		Automated Crash Dump Uploads 10	
File and Process Scan		Command Line Capture ①	
Cache		Command Line Logging (1)	
Endpoint Isolation			

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
Search	Q	Create Group

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	TZ-TEST-GROUP	
Description		
Parent Group		\$
Windows Policy	Copy of abhsha-WIN-DND - #1	\$
Android Policy	Default Policy (Vanilla Android)	\$
Mac Policy	Default Policy (Vanilla OSX)	\$
Linux Policy	Default Policy (Vanilla Linux)	\$
Network Policy	Default Policy (network_policy)	\$
iOS Policy	Default Policy (Audit)	\$
	Cancel	Save

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-RE	SMRDG 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				
Q Scan 😲 Diagnose 🕼 Move to Group 🗑 Delete					

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.

▼ ■ abhsha-WIN-DND				
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	abhsha-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				

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

Copy of abhsha-WIN-DND				
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	Not Configured	
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.

Modes and Engines		Send User Name in Events I
Exclusions		Send Filename and Path Info ①
2 exclusion sets	Heartbeat Interval	15 minutes 😫 🕄
Proxy	Connector Log Level	Debug 🗘 1
	Tray Log Level	Default 💠 🕄
Outbreak Control		
Product Updates		Enable Connector Protection (1)
Advanced Settings	Connector Protection Password	
Administrative Features		
Client User Interface		Automated Crash Dump Uploads
File and Process Scan		Command Line Capture ①
Cache		Command Line Logging
Endpoint Isolation		

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.

V 🖬 abhsha-WIN-DND			盘1 🖵 2	
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	abhsha-DND 📮 2	
Outbreak Control				
Custom Detections - Simple	Custom Detections - Advanced	Application Control	Network	
Not Configured	Not Configured	Not Configured	Not Configured	
③ View Changes Modified 2020-04-23 12:38:35 IST Serial Number 13919				

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**.

- 🔄 🔄 ╤ AMP					
File Home Share View					
← → * ↑	> This	s PC → Local Disk (C:) → Program	Files > Cisco > AMP >		
📌 Quick access			Date modified 4/25/2020 11:57 AIVI	Туре	Size
Desktop	*	update	4/23/2020 11:59 AM	File folder	
Downloads	*	URLScanner	4/23/2020 11:59 AM	File folder	
		2020-04-23 11-59-18	4/23/2020 11:59 AM	Windows Perform	0 KB
Dicture Dicture	Ĩ.	🚳 cache	4/23/2020 12:33 PM	Data Base File	252 KB
Pictures	Я	cache.db-shm	4/23/2020 11:59 AM	DB-SHM File	32 KB
7.1.5		cache.db-wal	4/23/2020 12:33 PM	DB-WAL File	4,036 KB
🁌 Music		📄 filetypes	4/23/2020 11:59 AM	XML Document	3 KB
📑 Videos		🚳 history	4/23/2020 12:34 PM	Data Base File	68 KB
		🗟 historyex	4/23/2020 11:59 AM	Data Base File	4 KB
OneDrive		historyex.db-shm	4/23/2020 11:59 AM	DB-SHM File	32 KB
This PC		historyex.db-wal	4/23/2020 12:27 PM	DB-WAL File	137 KB
A 1 1 1		🚳 jobs	4/23/2020 11:59 AM	Data Base File	4 KB
Network		📄 jobs.db-shm	4/23/2020 11:59 AM	DB-SHM File	32 KB
		📄 jobs.db-wal	4/23/2020 11:59 AM	DB-WAL File	13 KB
		local.old	4/23/2020 12:32 PM	OLD File	4 KB
		🔮 local	4/23/2020 12:32 PM	XML Document	4 KB
		Infm_cache	4/23/2020 11:59 AM	Data Base File	4 KB
		nfm_cache.db-shm	4/23/2020 11:59 AM	DB-SHM File	32 KB
		nfm_cache.db-wal	4/23/2020 12:33 PM	DB-WAL File	61 KB
		🚳 nfm_url_file_map	4/23/2020 11:59 AM	Data Base File	4 KB
		nfm_url_file_map.db-shm	4/23/2020 11:59 AM	DB-SHM File	32 KB
		nfm_url_file_map.db-wal	4/23/2020 12:08 PM	DB-WAL File	45 KB
		🔮 policy	4/23/2020 12:30 PM	XML Document	20 KB

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.