Fehlerbehebung bei Deinstallationsmethoden von Secure Endpoint Connector

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Deinstallationsmethoden
Manuelle Deinstallation
Deinstallieren Sie Connector von der Konsole für sichere Endgeräte.
Connector mithilfe von APIs deinstallieren
Deinstallieren Sie Connector mithilfe von Befehlszeilenschaltern.
Zugehörige Informationen

Einleitung

In diesem Dokument wird das Deinstallieren eines Cisco Secure Endpoint (CSE)-Connectors beschrieben, der auf Windows-Geräten mit verschiedenen Methoden installiert ist.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sicherer Endgeräteanschluss
- Konsole für sichere Endgeräte
- APIs für sichere Endgeräte

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Version 5.4.2024042415 der Secure Endpoint-Konsole
- Secure Endpoint Windows Connector Version v8.2.3.30119
- API für sichere Endgeräte v3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Das in diesem Dokument beschriebene Verfahren ist in Situationen hilfreich, in denen Sie den Secure Endpoint Connector deinstallieren möchten.

Die Deinstallation des Connectors ist eine Option, um den Connector ganz loszuwerden, entweder für Neuinstallationen oder einfach nicht mehr mit dem Connector auf einem Windows-Gerät.

Deinstallationsmethoden

Wenn Sie den Secure Endpoint Connector auf einem Windows-Computer deinstallieren möchten, folgen Sie der für Ihre Anforderungen am besten geeigneten Methode.

Manuelle Deinstallation

Um einen Steckverbinder lokal zu deinstallieren.

Schritt 1: Navigieren Sie im Gerät zu Programme > Cisco > AMP > x (wobei x die Version des CSE-Connectors ist).

Schritt 2: Suchen Sie die Datei uninstall.exe. Wie im Bild gezeigt.

C

□ > This PC > Windows (C:) > Program Files > Cisco > AMP > 8.2.3.30119 >

	🕽 Sort ~ 🔳 View ~			
Name	Date modified	Туре	Size	
🛐 hs.dll	2/20/2024 2:54 PM	Application exten	3,837 KB	
ipsupporttool.exe	2/20/2024 2:54 PM	Application	693 KB	
libcrypto-1_1-x64.dll	2/20/2024 2:54 PM	Application exten	3,357 KB	
🛐 libssl-1_1-x64.dll	2/20/2024 2:54 PM	Application exten	678 KB	
🖻 mfc140u.dll	2/20/2024 2:54 PM	Application exten	5,527 KB	
🕤 msvcp140.dll	2/20/2024 2:54 PM	Application exten	567 KB	
🖻 msvcp140_1.dll	2/20/2024 2:54 PM	Application exten	35 KB	
🖻 msvcp140_2.dll	2/20/2024 2:54 PM	Application exten	193 KB	
S pthreadVC2.dll	2/20/2024 2:54 PM	Application exten	115 KB	
SecureClientUI.msi	2/20/2024 2:53 PM	Windows Installer	4,836 KB	
SecurityProductInformation.ini	2/20/2024 2:54 PM	Configuration sett	1 KB	
🕦 sfc.exe	2/20/2024 2:54 PM	Application	9,297 KB	
sfc.exe.log	4/27/2024 2:28 PM	Text Document	5,533 KB	
sfc.exe_1.log	4/24/2024 3:05 PM	Text Document	51,200 KB	
sfc.exe_2.log	4/21/2024 11:50 PM	Text Document	51,200 KB	
sfc.exe_3.log	4/17/2024 6:12 PM	Text Document	51,200 KB	
sfc.exe_4.log	4/6/2024 8:28 PM	Text Document	51,200 KB	
sfc.exe_5.log	3/26/2024 1:20 PM	Text Document	51,200 KB	
sfc.exe_6.log	3/7/2024 11:03 AM	Text Document	51,200 KB	
spd.dat	2/20/2024 2:54 PM	DAT File	9 KB	
🖻 ucrtbase.dll	2/20/2024 2:54 PM	Application exten	1,098 KB	
🕦 uninstall.exe	2/20/2024 2:54 PM	Application	34,624 KB	N.
updater.exe	2/20/2024 2:54 PM	Application	1,708 KB	
🗟 vcruntime140.dll	2/20/2024 2:54 PM	Application exten	107 KB	
vcruntime140_1.dll	2/20/2024 2:54 PM	Application exten	49 KB	
windows.phsd	2/20/2024 2:55 PM	PHSD File	8,161 KB	
🔹 zlib.dll	2/20/2024 2:54 PM	Application exten	98 KB	

Schritt 3: Führen Sie die Datei aus, und folgen Sie dem Assistenten, bis der Bildschirm Deinstallation abgeschlossen angezeigt wird. Wie im Bild gezeigt.

Cisco Secure Endpoint Uninstall		_		X
Uninstallation Complete				
Uninstallation Complete				-
Uninstall was completed successfully.				
Cisco Secure Endpoint has completed				
Show details				
	< Back	Close	Can	cel

Schritt 4: Nach Abschluss der Deinstallation wird das folgende Dialogfeld mit der Frage angezeigt: "Planen Sie eine erneute Installation von Cisco Secure Endpoint?" Wie im Bild gezeigt.

Cisco Secure Endpoint Uninstall		×
Do you plan on installing Cisco Secure will delete all local data generated by history and quarantine files.	e Endpoint again? Clicki Cisco Secure Endpoint i	ng 'No' ncluding
	Yes	No



Hinweis: Falls Sie im Deinstallationsdialogfeld Nein auswählen, ist ein vollständiger Neustart des Geräts erforderlich, um alle verbleibenden CSE-Ordner zu entfernen.

Deinstallieren Sie Connector von der Konsole für sichere Endgeräte.

Wenn Sie eine Ferninstallation von der Konsole aus durchführen müssen, können Sie dies über die Schaltfläche Connector deinstallieren tun.

Schritt 1: Navigieren Sie in der Konsole zu Verwaltung > Computer.

Schritt 2: Suchen Sie den Computer, den Sie deinstallieren möchten, und klicken Sie auf, um Details anzuzeigen.

Schritt 3: Klicken Sie auf die Schaltfläche Connector deinstallieren. Wie im Bild gezeigt.

圏 🔻 🤹 Default-Wint1 in group Universitä Kest					
Hostname	Default-Win11	Group 🌰	Uninstall test		
Operating System	Y Windows 11, SP 0.0 (Build 22000.2538)	Policy O	uninstall test		
Connector Version	T 8.2.3.30119 ± Show download URL	Internal IP			
Install Date		External IP	at boost of the sec		
Connector GUID	And a set an	Last Seen			
Processor ID	Handmann I.	Definition Version	TETRA 64 bit (None)		
Definitions Last Updated	None	Update Server	tetra-defs.amp.cisco.com		
Cisco Secure Client ID	N/A	Cisco Security Risk Score	Pending		
Othial Activation in progress					
Q. Sam. D Diagnose de More la Group					

Schritt 4: Klicken Sie auf Deinstallieren, wenn Sie aufgefordert werden, die Aktion zu bestätigen. Wie im Bild gezeigt.

Uninstall Connector	\times
E Default-Win11 in group Uninstall test will be uninstalled from the endpoint and remo from the computer management page.	wed
A This cannot be undone.	
Cancel	tall

Schritt 5: Sie erhalten eine Bestätigungsmeldung oben auf der Konsole für sichere Endgeräte. Wie im Bild gezeigt.

1 connector is scheduled to be uninstalled	×
Die Connector-Registrierung in der Konsole wird sofort gelöscht. Nach der lokalen Überprüfung	g
der Informationen wechselt der Connector vorübergehend zu einer Deinstallationsrichtlinie, un	d
einige Minuten später wird er vollständig vom Gerät entfernt. Wie im Bild gezeigt.	





Hinweis: Beachten Sie, dass der Zeitraum, den der Connector für diese Aufgabe benötigt, je nach Umgebung variieren kann.



Vorsicht: Stellen Sie sicher, dass das Gerät, das die Deinstallation empfängt, während des gesamten Vorgangs verbunden bleibt.



Hinweis: Diese Funktion kann nur einzeln ausgeführt werden, d.h. sie erlaubt keine Massendeinstallation oder -deinstallation einer Gerätegruppe. Weitere Informationen zu dieser Funktion finden Sie im Benutzerhandbuch im Abschnitt Remote Uninstall (Remote-Deinstallation) unter <u>Secure Endpoint User Guide (Sicheres Endgerät -</u> <u>Benutzerhandbuch)</u>.

Connector mithilfe von APIs deinstallieren

Falls Sie den Connector nicht über die Secure Endpoint-Konsole deinstallieren konnten, können Sie auch APIs verwenden.

Die Secure Endpoint API erfordert den Zugriff über ein authentifiziertes und autorisiertes Konto. Nur autorisierte Konten können Anfragen an API-Vorgänge senden. Alle Vorgänge müssen über eine sichere HTTPS-Verbindung kommunizieren.



Hinweis: Weitere Informationen zur Secure Endpoint Authentication für API finden Sie im folgenden Artikel: <u>Secure Endpoint API Authentication.</u>

Schritt 1: Integration von Secure Endpoint in SecureX Wie im Bild gezeigt.



Schritt 2: Registrieren Sie den SecureX API-Client. Wie im Bild gezeigt.

Client Name*	
Remote Uninstall Te	est
Client Preset	
	× ~
API Clients OA	auth Code Clients
Scopes*	Select None
Search	Q
Admin	Provide admin privileges
AO	Manage and execute Automation workflows and related objects
Asset	Access and modify your assets
Casebook	Access and modify your casebooks
	Query your configured modules for threat
Description	
Test for remote unit	nstall using API
	Add New Olient

Schritt 3: Sichere Speicherung von Anmeldedaten Wie im Bild gezeigt.



Schritt 4: Führen Sie example.sh (abgerufen von <u>example.sh</u>) in der Datei mit einem beliebigen Skriptdateiprogramm Ihrer Wahl aus.

Schritt 5: Führen Sie die Datei aus, und geben Sie Ihre Anmeldeinformationen ein. Wie im Bild gezeigt.



Schritt 6: Navigieren Sie, bis Sie "Zugriffstoken" gefunden haben. Kopieren Sie diesen Wert, um ihn später mithilfe von APIs zu authentifizieren. Wie im Bild gezeigt.





Hinweis: Für die Erstellung dieses Dokuments haben wir git.bash verwendet. Dieses Tool wird nicht von Cisco unterstützt. Bei Zweifeln oder Fragen bezüglich dieses Tools wird empfohlen, den Support für dieses Tool zu kontaktieren.

Schritt 7. Sobald das Authentifizierungstoken abgerufen wurde, können Sie ein Tool verwenden, das die Verwendung von APIs ermöglicht.



Hinweis: Für die Erstellung dieses Dokuments haben wir Postman verwendet. Dieses Tool wird nicht von Cisco unterstützt. Bei Zweifeln oder Fragen bezüglich dieses Tools wird empfohlen, den Support für dieses Tool zu kontaktieren.

Schritt 8: Basierend auf der API-Referenzsyntax (<u>Request a connector uninstallation</u>). Führen Sie die Deinstallationsanforderung für den Connector unter Verwendung der GUID des zu deinstallierenden Geräts aus.



Hinweis: Sie können die Connector-GUID auf zwei einfache Arten erhalten:

- Navigieren Sie im Secure Endpoint-Portal zu Verwaltung > Computer > Navigieren Sie zum gewünschten Computer > Anzeigen der Details > GUID abrufen.
- Öffnen Sie das Taskleistensymbol > Navigieren Sie zur Registerkarte Statistik > GUID abrufen.

Schritt 9. Wählen Sie als Authentifizierungsmethode Träger-Token aus, und geben Sie das zuvor in Schritt 6 erhaltene Zugriffstoken ein. Wie im Bild gezeigt.

2 https://api.amp.cisco.com/v3/organiza	ations	nputers)	Save 🗸 🖉 🕑
PUT v https://api.amp.cisco.co	om/v3/organizations	computers/	Send 🗠
Params Authorization • Headers (9)	Body Pre-request Script Tests	Settings	Cookies
Type Bearer Tok_ ~	(1) Heads up! These parameters hold environment, we recommend using	sensitive data. To keep this data secure while working in a gvariables. Learn more about <u>variables</u> .	a collaborative X
The authorization header will be automatically generated when you send the request. Learn more about	Token		
Body Cookies Headers (13) Test Results		Status: 204 No Content. Time: 788 ms. Size: 512 (B 🔂 Save as example 🚥
Pretty Raw Preview Visualize	Text -> 📅		60

Schritt 10. Füllen Sie die erforderlichen Felder des API-Aufrufs aus und klicken Sie auf die Schaltfläche Senden. Warten Sie auf die Antwort 204: No Content. Wie im Bild gezeigt.

nttps://api.amp.cisco.com/v3/organiza	tions	computers/	🖺 Save 🗸 🖉 🖾
PUT v https://api.amp.cisco.co	m/v: lorganizations.	Computers/	Send ~
Params Authorization • Headers (9)	Body Pre-request Script	Tests Settings	Cookies
Type Bearer Tok	Heads up! These parame environment, we recommend the second se	ters hold sensitive data. To keep this data secure while working end using variables. Learn more about <u>variables</u> .) in a collaborative X
The authorization header will be automatically generated when you send the request. Learn more about	Token		
Body Cookies Headers (13) Test Results		Status 204 No Content Time: 788 ms Size: 5	J12 8 🖾 Save as example 🚥
Pretty Raw Preview Visualize	Text 🗸 🛱		60

Die Connector-Registrierung in der Konsole wird sofort gelöscht. Nach der lokalen Überprüfung der Informationen wechselt der Connector vorübergehend zu einer Deinstallationsrichtlinie, und einige Minuten später wird er vollständig vom Gerät entfernt. Wie im Bild gezeigt.

Policy	· · · · · · · · · · · · · · · · · · ·
Name:	AUTO-GENERATED Uninstall policy for b57195ad-ab96-4b15-bc3e-5a
Serial Number:	69
Last Update:	Today 04:37:49 AM



Hinweis: Beachten Sie, dass der Zeitraum, den der Connector für diese Aufgabe benötigt, je nach Umgebung variieren kann.



Vorsicht: Stellen Sie sicher, dass das Gerät, das die Deinstallation empfängt, während des gesamten Vorgangs verbunden bleibt.

Wenn alle oben genannten Instanzen (Deinstallationsmethoden) erschöpft sind und Sie den gewünschten Connector immer noch nicht deinstallieren konnten, können Sie die letzte Resort-Option wählen, die in der folgenden Methode aufgeführt ist.

Deinstallieren Sie Connector mithilfe von Befehlszeilenschaltern.

Das Installationsprogramm verfügt über integrierte Befehlszeilenschalter, mit denen Sie zahlreiche Aktionen auf dem Endpunkt ausführen können, wie im folgenden Artikel beschrieben: Befehlszeilenschalter für sichere Endpunkte.

Um den CSE-Connector mit Befehlszeilenschaltern zu deinstallieren, befolgen Sie die folgenden Anweisungen.

Schritt 1: Öffnen Sie Eingabeaufforderung mit Administratorberechtigungen.

Schritt 2: Navigieren Sie zum Speicherort des Installationspakets. Wie im Bild gezeigt.



Schritt 3: Geben Sie den Paketnamen gefolgt von den auszuführenden Befehlszeilenschaltern ein. Wie im Bild gezeigt.

C:\Users\Mex-Amp\Downloads>FireAMPSetup.exe /R /remove 1

Schritt 4: Folgen Sie dem Assistenten, bis der Bildschirm Deinstallation abgeschlossen angezeigt wird. Wie im Bild gezeigt.

S Cisco Secure Endpoint Uninstall		-		×
Uninstallation Complete				
Uninstall was completed successfully.				
Cisco Secure Endpoint has completed				
Show details				
	< Back	Close	Cano	el



Hinweis: Der Switch für die Deinstallation muss für das Installationspaket ausgeführt werden und darf nicht uninstall.exe sein.

Um eine automatische und vollständige Deinstallation des Steckverbinders durchzuführen, ist der Switch wie folgt:

FireAMPSetup.exe /R /S /remove 1



Hinweis: Sie können diese auch im nicht automatischen Modus ausführen, indem Sie den Schalter /S entfernen.

Um eine vollständige Deinstallation eines Steckverbinders mit Kennwortschutz durchzuführen, muss der Switch wie folgt vorgehen:

FireAMPSetup.exe /uninstallpassword [Connector Protection Password]

Als letztes Mittel kann das Deinstallationsprogramm auf dem Gerät ausgeführt werden, auf dem der Anschluss deinstalliert werden muss.

Schritt 1: Öffnen Sie Eingabeaufforderung mit Administratorberechtigungen.

Schritt 2: Navigieren Sie zu dem Ort, an dem sich der Secure Endpoint Connector befindet. wobei x die Version des CSE-Connectors ist. Wie im Bild gezeigt.



Schritt 3: Führen Sie die Datei mit den folgenden Argumenten aus. Wie im Bild gezeigt.

uninstall.exe/full 1

C:\Program Files\Cisco\AMP\8.2.3.30119>uninstall.exe/full 1

Schritt 4: Folgen Sie dem Assistenten, bis der Bildschirm Deinstallation abgeschlossen angezeigt wird. Wie im Bild gezeigt.

GCisco Secure Endpoint Uninstall		-		×
Uninstallation Complete				
Uninstall was completed successfully				-
Cisco Secure Endpoint has completed				~ /
Show details				
	< Back	Close	Can	cel



Hinweis: Falls der AMP-Pfad nicht existiert, müssen Sie den Befehl ohne Angabe des Pfads ausführen. Führen Sie einfach den Befehl mit den angegebenen Argumenten aus.



Hinweis: Falls erforderlich, ist es möglich, die Datei uninstaller.exe eines anderen Connectors auszuführen, um den gewünschten Connector zu deinstallieren.

Zugehörige Informationen

- Secure Endpoint Benutzerhandbuch
- Technischer Support und Dokumentation für Cisco Systeme
- API für sichere Endgeräte v3

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.