排除Secure Endpoint Connector解除安裝方法故障

目錄
<u>必要條件</u>
<u>需求</u>
採用元件
<u>背景資訊</u>
<u>解除安裝方法</u>
<u>手動解除安裝</u>
從Secure Endpoint控制檯解除安裝聯結器。
使用API解除安裝聯結器
<u>使用命令列開關解除安裝聯結器</u>
相關資訊

簡介

本文檔介紹使用不同方法解除安裝安裝在Windows裝置上的Cisco Secure Endpoint (CSE)聯結器的 過程。

必要條件

需求

思科建議您瞭解以下主題:

- 安全端點聯結器
- 安全終端控制檯
- 安全終端API

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 安全終端控制檯5.4.2024042415版
- 安全終端Windows聯結器8.2.3.30119版
- 安全終端API v3

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

本文檔中介紹的過程在您希望解除安裝安全終端聯結器時非常有用。

解除安裝聯結器是徹底清除聯結器的選項,無論是對於全新安裝,還是只是在Windows裝置上不再 安裝聯結器。

解除安裝方法

當您要在Windows電腦上解除安裝安全終結點聯結器後,請遵循更適合您需求的方法。

手動解除安裝

在本機解除安裝聯結器。

步驟 1.在裝置中,導航到Program Files > Cisco > AMP > x(其中x是CSE聯結器的版本)。

步驟 2.找到uninstall.exe檔案。如圖所示。

C

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

0 6 @ @ 1	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	
nsvcp140_2.dll	2/20/2024 2:54 PM	Application exten	193 KB	
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	X
updater.exe	2/20/2024 2:54 PM	Application	1,708 KB	
S 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	

步驟 3.執行檔案並遵循精靈,直到取得[解除安裝完成]畫面。 如圖所示。

Cisco Secure Endpoint Uninstall		_		×
Uninstallation Complete				
Uninstall was completed successfully				1
Cisco Secure Endpoint has completed				
Show details				
	< Back	Close	Cano	:el

步驟 4.完成解除安裝過程後,您將看到以下對話方塊,詢問「Do you plan on installing Cisco Secure Endpoint again?」。如圖所示。

S Cisco Secure Endpoint Uninstall	×
Do you plan on installing Cisco Secure Endpoint again? Clicking 'No' will delete all local data generated by Cisco Secure Endpoint including history and quarantine files.	
Yes No	



註:如果在uninstall對話方塊中選擇No,則需要完全重新啟動裝置以完全清除所有剩餘的 CSE資料夾。

從Secure Endpoint控制檯解除安裝聯結器。

如果需要從控制檯遠端解除安裝,可以使用Uninstall connector 按鈕執行此操作。

步驟 1.在控制檯中, 導航到管理>電腦。

步驟 2.找到要解除安裝的電腦,然後按一下以顯示詳細資訊。

步驟 3.按一下Uninstall Connector 按鈕。 如圖所示。

🔳 🔻 🖽 Default-Winth in group Uninetial test 📨				
Hostname	Default-Win11	Group da	Uninstall test	
Operating System	T Windows 11, SP 0.0 (Build 22000.2538)	Policy C	uninstall test	
Connector Version	T 8.2.3.30119 ± Show download URL	Internal IP		
Install Date		External IP		
Connector GUID	And a set of the particular	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	
Othat Activation in progress 6 Events 19 Device Trajectory 10 Diagna 20 View Charges				
Q. Scan Do Diagnose 🖨 Move to Group				

步驟 4.當系統要求您確認操作時,按一下Uninstall。 如圖所示。

Uninstall Connector	×
EXAMPLE : Default-Win11 in group Uninstall test will be uninstalled from the endpoint and remain from the computer management page.	wed
A This cannot be undone.	
Cancel Unins	tall

步驟 5.您將在Secure Endpoint控制檯頂部收到確認消息。 如圖所示。

1 connector is scheduled to be uninstalled	×

控制檯中的聯結器註冊將立即消失。在本地檢視資訊時,聯結器將立即轉到解除安裝策略,幾分鐘 後,聯結器將完全從裝置中移除。如圖所示。

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



附註:請記住,聯結器用來執行此作業的時間可能會因您的環境而異。



注意:請確保接收解除安裝的裝置在整個過程中保持連線狀態。



注意:此函式只能單獨執行,即不允許成批解除安裝或解除安裝一組裝置。有關該功能的 詳細資訊,請參閱<u>安全終端使用手冊</u>的「遠端解除安裝」部分中的「使用手冊」。

使用API解除安裝聯結器

如果無法通過Secure Endpoint控制檯解除安裝聯結器,一個可行的選項是使用API。

安全終端API要求透過經過身份驗證和授權的帳戶進行訪問。只有授權帳戶才能向API操作提交請求 。所有操作必須透過安全的HTTPS連線進行通訊。



注意:有關API的安全端點身份驗證的詳細資訊,請參閱以下文章:<u>安全端點API身份驗證</u> <u>。</u>

步驟 1.將安全終端與SecureX整合。 如圖所示。



步驟 2.註冊SecureX API客戶端。 如圖所示。

Client Name*	
Remote Uninstall Te	st
Client Preset	
	× ~
API Clients OA	uth 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 unin	stall using API
	Add New Client Close

步驟 3.安全地儲存憑據。 如圖所示。

Add New Client with 25 scopes	×
The Client Password cannot be recovered, once you close this window. Please store securely.	
Client Id · Copy to Clipboard client-	
Client Password · Copied	
Clo	se

步驟 4.使用您選擇的任何指令碼檔案程式運行examples.sh(從examples.sh檢索)。

步驟 5.執行檔案並輸入您的認證。如圖所示。



步驟 6. 捲動至找到「存取權杖」。複製此值,以便稍後使用API進行身份驗證。如圖所示。





附註:為建立本檔案,我們使用git.bash。思科不支援此工具,如果有任何疑問或相關問題 ,建議聯絡此工具的支援人員。

步驟 7. 一旦獲得身份驗證令牌, 您就可以使用允許使用API的工具。



附註:為建立本檔案,我們使用Postman。思科不支援此工具,如果有任何疑問或相關問題 ,建議聯絡此工具的支援人員。

步驟 8. 根據API參考語法(<u>請求聯結器解除安裝</u>)。使用要解除安裝之裝置的GUID提出聯結器解除安 裝要求。



注意:您可以使用下列兩種簡單方法取得聯結器GUID:

- 在安全終端門戶上,導航到管理>電腦>導航到所需電腦>顯示詳細資訊>獲取GUID。
- 打開工作列圖示>導航到「統計資訊」頁籤>獲取GUID。

步驟 9.選擇Bearer Token作為身份驗證方法,並輸入先前在第6步獲得的訪問令牌。如圖所示。

tttps://api.amp.cisco.com/v3/organiza	tions	mputers/ 💭 Save 🦄	0 🗉
PUT V https://api.amp.cisco.co	m/v3/organizations.	computers/	Send 🗠
Params Authorization • Headers (9)	Body Pre-request Script Tests	Settings	Cookies
Type Bearer Tok_ ~	(i) Heads up! These parameters hold environment, we recommend using	d sensitive data. To keep this data secure while working in a collabora g variables. Learn more about <u>variables</u> .	stive 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 🖾 Sa	ive as example
Pretty Raw Preview Visualize	Text 👻 🛱		6 Q

步驟 10.填寫API呼叫的必填欄位,然後按一下Send按鈕。等待「204:無內容」響應。如圖所示。

https://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 v	Heads up! These parameter environment, we recommend.	eters hold sensitive data. To keep this data secure while wo rend using variables. Learn more about <u>variables</u> .	rking 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 S	ize: 512 B 🖾 Save as example 🚥
Pretty Raw Preview Visualize	Text 🗸 📅		6 Q

控制檯中的聯結器註冊將立即消失。在本地檢視資訊時,聯結器將立即轉到解除安裝策略,幾分鐘 後,聯結器將完全從裝置中移除。如圖所示。

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



附註:請記住,聯結器用來執行此作業的時間可能會因您的環境而異。



注意:請確保接收解除安裝的裝置在整個過程中保持連線狀態。

如果上述所有例項(解除安裝方法)都已用完,並且您仍然未能成功解除安裝所需的聯結器,則可 以選擇以下方法中列出的最後選用選項。

使用命令列開關解除安裝聯結器

安裝程式具有內建命令列開關,該命令列開關允許您在終端中執行許多操作(如以下文章中所述):<u>安全終端的命令列開關</u>。

要解除安裝帶有命令列開關的CSE聯結器,請使用以下說明。

步驟 1.以管理許可權開啟命令提示字元。

步驟 2.導航到安裝軟體套件所在的位置。如圖所示。

C:\Users\Mex-Amp>cd Downloads

步驟 3.鍵入軟體套件名稱,後跟要執行的命令列開關。 如圖所示。

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

步驟 4. 請遵循精靈的指示操作,直到出現「解除安裝完成」畫面。 如圖所示。

S Cisco Secure Endpoint Uninstall		-		×
University Review Convertees				
Uninstallation Complete				
Uninstall was completed successfully.				
Cisco Secure Endpoint has completed				
Show details				
An over the second				
	< Back	Close	Car	locel



注意:解除安裝的開關必須針對安裝套件執行,而非uninstall.exe

要對聯結器執行靜默和完全解除安裝,交換機為:

FireAMPSetup.exe /R /S /remove 1



注意:也可以透過刪除/S開關在非靜默模式下執行這些操作。

要對具有口令保護的聯結器執行完整解除安裝,交換機需執行以下操作:

FireAMPSetup.exe /uninstallpassword [Connector Protection Password]

作為最後的方法,在需要解除安裝聯結器的裝置上執行解除安裝程式將會解決需求。

步驟 1.以管理許可權開啟命令提示字元。

步驟 2.導航到Secure Endpoint聯結器所在的位置。 其中x是CSE聯結器的版本。如圖所示。

C:\Program Files\Cisco\AMP\x>

C:\Program Files\Cisco\AMP>cd 8.2.3.30119

步驟 3.使用下列引數執行檔案。如圖所示。

uninstall.exe/full 1

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

步驟 4. 請遵循精靈的指示操作, 直到出現「解除安裝完成」畫面。如圖所示。

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



注意:如果AMP路徑不存在,您必須不指明路徑而運行命令,只需使用指示的引數運行命 令即可。



注意:如有必要,可以運行另一個聯結器的uninstaller.exe,以解除安裝所需的聯結器。

相關資訊

- 安全終端使用手冊
- <u>技術支援與文件 Cisco Systems</u>
- <u>安全終端API v3</u>

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。