Methoden voor verwijdering van Secure Endpoint Connector

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Achtergrondinformatie
Methoden voor verwijderen
Handmatig verwijderen
Verwijder Connector van Secure Endpoint console.
Connector verwijderen met API's
Connector verwijderen met Switches voor opdrachtregel
Gerelateerde informatie

Inleiding

Dit document beschrijft het proces om een Cisco Secure Endpoint (CSE)-connector te verwijderen die op Windows-apparaten met verschillende methoden is geïnstalleerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Secure Endpoint-connector
- Secure Endpoint-console
- Secure Endpoint API's

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Secure Endpoint console versie v5.4.2024042415
- Secure Endpoint Windows-connector versie v8.2.3.30119
- Secure Endpoint API v3

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De procedure die in dit document wordt beschreven, is handig in situaties waarin u de Secure Endpoint-connector wilt verwijderen.

Het verwijderen van de connector is een optie om van de connector af te komen, hetzij voor verse installaties of gewoon niet meer de connector op een Windows-apparaat.

Methoden voor verwijderen

Zodra u de Secure Endpoint-connector op een Windows-computer wilt verwijderen, volgt u de methode die beter op uw behoeften aansluit.

Handmatig verwijderen

Zo verwijdert u lokaal een -aansluiting.

Stap 1. Ga in het apparaat naar Program Files > Cisco > AMP > x (waarbij x de versie van de CSE-connector is).

Stap 2. Zoek het bestand uninstall.exe. Zoals in de afbeelding.

С

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

0 6 0 0 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	
🖻 msvcp140_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	
stc.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	
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	

Stap 3. Voer het bestand uit en volg de wizard totdat u het scherm Installatie voltooid hebt ontvangen. Zoals in de afbeelding.

S Cisco Secure Endpoint Uninstall		_		×
Uningtallation Complete				
Uninstallation Complete				-
Uninstall was completed successfully.				
Cisco Secure Endpoint has completed				
Show details				
	Real I	dees	C	
<	. Back	uose	Cance	1

Stap 4. Na het verwijderen van de installatie, krijgt u het volgende dialoogvenster met de vraag "Bent u van plan Cisco Secure Endpoint opnieuw te installeren?". Zoals in de afbeelding.

Cisco Secure Endpoint Uninstall	×
Do you plan on installing Cisco Secure Endpoint again? Clickin will delete all local data generated by Cisco Secure Endpoint in history and quarantine files.	ig 'No' icluding
Yes	No



Opmerking: als u Nee selecteert in het dialoogvenster verwijderen, moet het apparaat volledig opnieuw worden opgestart om alle resterende mappen van CSE volledig te verwijderen.

Verwijder Connector van Secure Endpoint console.

Als u op afstand van de console moet verwijderen, kunt u dit doen met behulp van de Uninstall connector knop.

Stap 1. Navigeer in de console naar Management > Computers.

Stap 2. Zoek de computer die u wilt verwijderen en klik om de details weer te geven.

Stap 3. Klik op de knop Uninstall Connector. Zoals in de afbeelding.

🔳 🔻 🌐 Default-Wintt in group Uninetal text					
Hostname	Defaut-Wn11	Group 🌰	Uninstall test		
Operating System	T 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			
Connector GUID		Last Seen			
Processor ID	Tempineers .	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 4 Exerts: 1 ^o Device Trajectory 10 Day Long View Orlanger.					
P. Scan. D Diagnose. D Diagnos					

Stap 4. Klik op Verwijderen als u gevraagd wordt de actie te bevestigen. Zoals in de afbeelding.

Uninstall Connector	×
EXAMPLE 1 In group Uninstall test will be uninstalled from the endpoint and rem from the computer management page.	oved
This cannot be undone.	
Cancel	tall

Stap 5. U ontvangt een bevestigingsbericht bovenaan de Secure Endpoint console. Zoals in de afbeelding.

1 connector is scheduled to	be uninstalled	×
De connector registratie bekeken, gaat de conne wordt hij volledig van he	in de console zal onmiddellijk verdwijnen. Nadat de informatie loka ector tijdelijk over op een verwijderingsbeleid en een paar minuten la et apparaat verwijderd. Zoals in de afbeelding.	al is ater
Policy Name:	AUTO-GENERATED Uninstall policy for b57195ad-ab96-4b15-bc3e	-5a

69

Today 04:37:49 AM

Serial Number:

Last Update:

. _ .

_



Opmerking: houd er rekening mee dat de periode die de connector gebruikt om deze taak uit te voeren, kan variëren afhankelijk van uw omgeving.



Waarschuwing: zorg ervoor dat het apparaat dat de verwijdering ontvangt, tijdens het proces verbonden blijft.



Opmerking: deze functie kan alleen afzonderlijk worden uitgevoerd, d.w.z. het is niet toegestaan om een groep apparaten massaal te verwijderen of te verwijderen. Raadpleeg voor meer informatie over deze functie de Gebruikershandleiding in de sectie <u>Secure</u> <u>Endpoint User Guide (Beveiligde eindpuntgebruikershandleiding)</u> van de <u>afstandsbediening</u>.

Connector verwijderen met API's

Als u er niet in bent geslaagd om de connector via de Secure Endpoint console te verwijderen, is het een haalbare optie om API's te gebruiken.

De Secure Endpoint API vereist toegang via een geverifieerde en geautoriseerde account. Alleen erkende accounts kunnen verzoeken indienen bij API-bewerkingen. Alle bewerkingen moeten communiceren via een beveiligde HTTPS-verbinding.



Opmerking: voor meer informatie over Secure Endpoint Verification voor API, raadpleegt u het volgende artikel: <u>Secure Endpoint API Verification.</u>

Stap 1. Integreer beveiligde endpoints met SecureX. Zoals in de afbeelding.



Stap 2. SecureX API-client registreren. Zoals in de afbeelding.

Clier	nt Name*	
Rer	note Uninstall 1	lest .
Clier	nt Preset	
		× ×
AF	PI Clients O	Auth Code Clients
Sco	pes*	Select None
Sea	arch	Q
~	Admin	Provide admin privileges
✓	AO	Manage and execute Automation workflows and related objects
\checkmark	Asset	Access and modify your assets
✓	Casebook	Access and modify your casebooks
_		Query your configured modules for threat
Desc	cription	
Tes	t for remote un	install using API
		Add New Client Close





Stap 4. Voer voorbeelden.sh (opgehaald uit <u>voorbeelden.sh</u>) het bestand uit met behulp van een script-bestandsprogramma van uw keuze.

Stap 5. Start het bestand en voer uw referenties in. Zoals in de afbeelding.



Stap 6. Scroll tot u "access token" vindt. Kopieer deze waarde om later te verifiëren in het gebruik van API's. Zoals in de afbeelding.





Opmerking: Voor het maken van dit document hebben we gebruik gemaakt van git.bash. Deze tool wordt niet ondersteund door Cisco, enige twijfel of vraag die hiermee verband houdt, wordt aanbevolen contact op te nemen met de ondersteuning van deze tool.

Stap 7. Zodra het verificatietoken is verkregen, kunt u een tool gebruiken waarmee API's kunnen worden gebruikt.



Opmerking: Voor de creatie van dit document hebben we gebruik gemaakt van Postman. Deze tool wordt niet ondersteund door Cisco, enige twijfel of vraag die hiermee verband houdt, wordt aanbevolen contact op te nemen met de ondersteuning van deze tool.

Stap 8. Gebaseerd op de API-referentiesyntaxis (verzoek om verwijdering van de connector). Maak de connector deïnstallatieaanvraag met behulp van de GUID van het te verwijderen apparaat.



Opmerking: u kunt de connector GUID op de volgende twee eenvoudige manieren verkrijgen:

- Op het Secure Endpoint portal navigeer je naar Management > Computers > Navigeer naar de gewenste computer > Geef de details weer > Get GUID.
- Open het pictogram van het Dienblad > Navigeer aan het tabblad Statistieken > Get GUID.

Stap 9. Selecteer Token aan toonder als verificatiemethode en voer het toegangstoken in dat eerder is verkregen in stap 6. Zoals in de afbeelding.

ttps://api.amp.cisco.com/v3/organiza	tions	computers/	🛱 Save 🗸 🖉 🗉
PUT V https://api.amp.cisco.co	m/v3/organizations.	computers/	. Send v
Params Authorization • Headers (9)	Body Pre-request Script Te	sts Settings	Cookies
Type Bearer Tok_ ~	(i) Heads up! These parameters h environment, we recommend up	old sensitive data. To keep this data secure while work sing variables. Learn more about <u>variables</u> .	ing 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	1: 512 8 🖾 Save as example 🚥
Pretty Raw Preview Visualize	Text 🗸 📅		60

Stap 10. Vul de vereiste velden van de API-aanroep in en klik op Verzend knop. Wacht op 2004: Geen contentrespons. Zoals in de afbeelding.

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	(i) Heads up! These parame environment, we recommend the second secon	rters hold sensitive data. To keep this data secure while work end using variables. Learn more about <u>variables</u> .	ing in a collaborative X
The authorization header will be automatically generated when you send the request. Learn more about	Token		
Body Cookles Headers (13) Test Results		Status 204 No Content, Time: 788 ms Siz	e: 512 B 🖾 Save as example 🚥
Pretty Raw Preview Visualize	Text 🗸 🚍		6 Q

De connector registratie in de console zal onmiddellijk verdwijnen. Nadat de informatie lokaal is bekeken, gaat de connector tijdelijk over op een verwijderingsbeleid en een paar minuten later wordt hij volledig van het apparaat verwijderd. Zoals in de afbeelding.

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



Opmerking: houd er rekening mee dat de periode die de connector gebruikt om deze taak uit te voeren, kan variëren afhankelijk van uw omgeving.



Waarschuwing: zorg ervoor dat het apparaat dat de verwijdering ontvangt, tijdens het proces verbonden blijft.

Als alle bovenstaande gevallen (verwijderingsmethoden) zijn uitgeput en u er nog steeds niet in bent geslaagd de gewenste connector te verwijderen, kunt u kiezen voor de laatste resortoptie die in de volgende methode wordt vermeld.

Connector verwijderen met Switches voor opdrachtregel

De installateur heeft ingebouwde switches in de opdrachtregel waarmee u talrijke acties in het eindpunt kunt uitvoeren zoals vermeld in het volgende artikel: <u>Command Line Switches voor</u> <u>Secure Endpoint</u>.

Gebruik de volgende switches om de CSE-connector met opdrachtregel te verwijderen.

Stap 1. Opdrachtprompt met beheerdersrechten openen.

Stap 2. Navigeer naar de locatie waar het installatiepakket zich bevindt. Zoals het voorbeeld in de afbeelding.



Stap 3. Typ de pakketnaam gevolgd door de switches van de opdrachtregel die uitgevoerd moeten worden. Zoals in de afbeelding.

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

Stap 4. Volg de wizard totdat u het scherm Ongedaan maken hebt ontvangen. Zoals in de afbeelding.

S Cisco Secure Endpoint Uninstall		-		×
Uninstallation Complete				
Uninstallation Complete				
Uninstall was completed successfully.				_
Cisco Secure Endpoint has completed				
				í –
Chaus datale				
Show details				
	< Back	Close	Can	cel



Opmerking: de switch voor het verwijderen moet worden uitgevoerd tegen het installatiepakket en niet uninstall.exe

De switch is om het stille en volledige verwijderen van de -aansluiting uit te voeren:

FireAMPSetup.exe /R /S /remove 1



Opmerking: u kunt deze ook uitvoeren in niet-stille modi door de /S switch te verwijderen.

De switch is om een volledige installatie van een connector met wachtwoordbeveiliging uit te voeren:

FireAMPSetup.exe /uninstallpassword [Connector Protection Password]

Als laatste redmiddel, zal het uitvoeren van de uninstaller op het apparaat waarop de connector moet worden verwijderd de noodzaak oplossen.

Stap 1. Opdrachtprompt met beheerdersrechten openen.

Stap 2. Navigeer naar de locatie waar de Secure Endpoint-connector zich bevindt. Waarbij x de versie van de CSE-connector is. Zoals in de afbeelding.



Stap 3. Voer het bestand uit met de volgende argumenten. Zoals in de afbeelding.

uninstall.exe/full 1

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

Stap 4. Volg de wizard totdat u het scherm Ongedaan maken hebt ontvangen. Zoals in de afbeelding.

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



Opmerking: als het AMP-pad niet bestaat, moet u de opdracht uitvoeren zonder het pad aan te geven, maar moet u de opdracht uitvoeren met de aangegeven argumenten.



Opmerking: indien nodig is het mogelijk om het uninstaller.exe van een andere connector uit te voeren om de gewenste connector te verwijderen.

Gerelateerde informatie

- Gebruikershandleiding Secure Endpoint
- <u>Technische ondersteuning en documentatie Cisco Systems</u>
- <u>Secure Endpoint API v3</u>

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.