Risoluzione dei problemi relativi ai metodi di di disinstallazione di Secure Endpoint Connector

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Metodi di disinstallazione
Disinstalla manualmente
Disinstallare Connector dalla console di Secure Endpoint.
Disinstalla connettore tramite API
Disinstallare il connettore utilizzando le opzioni della riga di comando
Informazioni correlate

Introduzione

In questo documento viene descritto il processo di disinstallazione di un connettore Cisco Secure Endpoint (CSE) installato nei dispositivi Windows con metodi diversi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Secure Endpoint Connector
- Secure Endpoint Console
- API Secure Endpoint

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Secure Endpoint console versione v5.4.2024042415
- Connettore Windows Secure Endpoint versione v8.2.3.3019
- API Secure Endpoint v3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La procedura descritta in questo documento è utile nelle situazioni in cui si desidera disinstallare il connettore Secure Endpoint.

La disinstallazione del connettore è un'opzione per sbarazzarsi del tutto del connettore, per nuove installazioni o semplicemente non avere più il connettore su un dispositivo Windows.

Metodi di disinstallazione

Per disinstallare il connettore Secure Endpoint su un computer Windows, seguire il metodo più adatto alle proprie esigenze.

Disinstalla manualmente

Per disinstallare un connettore localmente.

Passaggio 1. Nel dispositivo, selezionare Programmi > Cisco > AMP > x (dove x è la versione del connettore CSE).

Passaggio 2. Individuare il file uninstall.exe. Come mostrato nell'immagine.

С

□ > 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	
🖻 libssi-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	
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	
stc.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	

Passaggio 3. Eseguire il file e seguire la procedura guidata fino a visualizzare la schermata Disinstallazione completata. Come mostrato nell'immagine.

Cisco Secure Endpoint Uninstall		_		×
Uninstallation Complete				
Uninstallation Complete				
Uninstall was completed successfully.				
Cisco Secure Endpoint has completed				
Show details				
Silow details				
				. 1
	< Back	Close	Can	cel

Passaggio 4. Al termine del processo di disinstallazione, verrà visualizzata la seguente finestra di dialogo con la richiesta "Si intende installare di nuovo Cisco Secure Endpoint?". Come mostrato nell'immagine.

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



Nota: se si seleziona No nella finestra di dialogo di disinstallazione, sarà necessario riavviare completamente il dispositivo per eliminare completamente tutte le cartelle CSE rimanenti.

Disinstallare Connector dalla console di Secure Endpoint.

Se è necessario eseguire la disinstallazione in remoto dalla console, utilizzare il pulsante Uninstall connector.

Passaggio 1. Nella console passare a Gestione > Computer.

Passaggio 2. Individuare il computer che si desidera disinstallare e fare clic su per visualizzare i dettagli.

Passaggio 3. Fare clic sul pulsante Uninstall Connector (Disinstalla connettore). Come mostrato nell'immagine.

🖩 🔻 🛱 Default-Wintt in group Uninstall test 🍅				
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	a book and the	
Connector GUID		Last Seen		
Processor ID	Reserver.	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	
Ditat Khveton In progress 4 Events 1 ^o Device Trajectory 10 Day 🛃 View Changes				
(0, San.) (0 Degree.) 🔿 Move to Broup. (5 Universit Convects) (2 Degree.)				

Passaggio 4. Quando viene richiesto di confermare l'azione, fare clic su Uninstall. Come mostrato nell'immagine.

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

Passaggio 5. Verrà visualizzato un messaggio di conferma nella parte superiore della console di Secure Endpoint. Come mostrato nell'immagine.

🕽 1 conne	ector is	s scheduled to	o be uninst	alled				×
 							-	

La registrazione del connettore nella console scompare immediatamente. Dopo aver esaminato le informazioni localmente, il connettore passerà momentaneamente a un criterio di disinstallazione e pochi minuti dopo verrà completamente rimosso dal dispositivo. Come mostrato nell'immagine.

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



Nota: tenere presente che il periodo di tempo utilizzato dal connettore per eseguire questa operazione può variare a seconda dell'ambiente.



Attenzione: assicurarsi che il dispositivo che riceve la disinstallazione rimanga collegato durante l'intero processo.



Nota: questa funzione può essere eseguita solo singolarmente, ovvero non consente la disinstallazione di massa o la disinstallazione di un gruppo di dispositivi. Per ulteriori informazioni su questa funzione, consultare il Manuale dell'utente nella sezione relativa alla disinstallazione remota del <u>Manuale dell'utente di Secure Endpoint</u>.

Disinstalla connettore tramite API

Se non è stato possibile disinstallare il connettore tramite la console Secure Endpoint, è possibile utilizzare le API.

L'API Secure Endpoint richiede accesso tramite un account autenticato e autorizzato. Solo gli account autorizzati possono inviare richieste alle operazioni API. Tutte le operazioni devono comunicare tramite una connessione HTTPS protetta.



Nota: per ulteriori informazioni su Secure Endpoint Authentication for API, fare riferimento all'articolo seguente: <u>Secure Endpoint API Authentication</u>.

Passaggio 1. Integrazione di Secure Endpoint con SecureX. Come mostrato nell'immagine.



Passaggio 2. Registra client API SecureX. Come mostrato nell'immagine.

Remote Uninstall Te	st
Client Preset	
	×
API Clients OA	uth Code Clients
Scopes*	Select Non
Search	C
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 unir	stall using API

Passaggio 3. Archiviare le credenziali in modo sicuro. Come mostrato nell'immagine.



Passaggio 4. Eseguire example.sh (recuperato da <u>example.sh</u>) sul file utilizzando un qualsiasi programma di file script scelto.

Passaggio 5. Eseguire il file e immettere le credenziali. Come mostrato nell'immagine.



Passaggio 6. Scorrere fino a trovare "token di accesso". Copiare questo valore per eseguire l'autenticazione in un secondo momento utilizzando le API. Come mostrato nell'immagine.





Nota: per la creazione di questo documento abbiamo utilizzato git.bash. Questo strumento non è supportato da Cisco, per qualsiasi dubbio o domanda ad esso correlata, si consiglia di contattare il supporto di questo strumento.

Passaggio 7. Una volta ottenuto il token di autenticazione, è possibile utilizzare uno strumento che consente l'utilizzo delle API.



Nota: per la creazione di questo documento abbiamo fatto uso di Postman. Questo strumento non è supportato da Cisco, per qualsiasi dubbio o domanda ad esso correlata, si consiglia di contattare il supporto di questo strumento.

Passaggio 8. In base alla sintassi di riferimento dell'API (<u>richiesta di disinstallazione del</u> <u>connettore</u>). Eseguire la richiesta di disinstallazione del connettore utilizzando il GUID della periferica da disinstallare.



Nota: è possibile ottenere il GUID del connettore nei due modi seguenti:

- Sul portale Secure Endpoint passare a Gestione > Computer > Passare al computer desiderato > Visualizzare i dettagli > Ottieni GUID.
- Aprire Icona barra delle applicazioni > Passare alla scheda Statistiche > Ottieni GUID.

Passaggio 9. Selezionare Bearer Token come metodo di autenticazione e immettere il token di accesso ottenuto in precedenza al passo 6. Come mostrato nell'immagine.

https://api.amp.cisco.com/v3/organiza	tions comp	suters/ . 🖾 Save	~ 0 2
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_ ~	Heads up! These parameters hold s environment, we recommend using	ensitive data. To keep this data secure while working in a collabo variables. Learn more about <u>variables</u> .	prative 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 8 🗋	Save as example +++
Pretty Raw Preview Visualize	Text 🗸 📅		ΓQ

Passaggio 10. Compilare i campi obbligatori della chiamata API e fare clic sul pulsante Send. Attendere la risposta 204: nessun contenuto. Come mostrato nell'immagine.

https://api.amp.cisco.com/v3/organization/v	tions	computers/ . 🖾 Save 🗸	1 🗉
PUT v https://api.amp.cisco.co	m/v:lorganizations/	Computers/	end ~
Params Authorization Headers (9)	Body Pre-request Script	Tests Settings	Cookies
Type Bearer Tok v	Heads upl These paramet environment, we recomme	ters hold sensitive data. To keep this data secure while working in a collaborative end using variables. Learn more about <u>variables</u> .	×
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 8 🔛 Save as	example ++
Pretty Raw Preview Visualize	Text 🗸 📅		6 Q

La registrazione del connettore nella console scompare immediatamente. Dopo aver esaminato le informazioni localmente, il connettore passerà momentaneamente a un criterio di disinstallazione e pochi minuti dopo verrà completamente rimosso dal dispositivo. Come mostrato nell'immagine.

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



Nota: tenere presente che il periodo di tempo utilizzato dal connettore per eseguire questa operazione può variare a seconda dell'ambiente.



Attenzione: assicurarsi che il dispositivo che riceve la disinstallazione rimanga collegato durante l'intero processo.

Se tutte le istanze precedenti (metodi di disinstallazione) sono esaurite e non è stato ancora possibile disinstallare il connettore desiderato, è possibile scegliere l'opzione di ultima istanza elencata nel metodo seguente.

Disinstallare il connettore utilizzando le opzioni della riga di comando

L'Installer dispone di opzioni della riga di comando incorporate che consentono di eseguire numerose azioni nell'endpoint, come indicato nell'articolo seguente: <u>Switch della riga di comando</u> <u>per endpoint sicuri</u>.

Per disinstallare il connettore CSE con switch della riga di comando, attenersi alle seguenti istruzioni.

Passaggio 1. Aprire il prompt dei comandi con privilegi amministrativi.

Passaggio 2. Passare alla posizione in cui si trova il pacchetto di installazione. Come mostrato nell'immagine.



Passaggio 3. Digitare il nome del pacchetto seguito dalle opzioni della riga di comando da eseguire. Come mostrato nell'immagine.

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

Passaggio 4. Seguire la procedura guidata fino a visualizzare la schermata Disinstallazione completata. Come mostrato nell'immagine.

S Cisco Secure Endpoint Uninstall			-		×
Uninstallation Consults					
Uninstallation Complete					_
Uninstall was completed successfully.					_
Cisco Secure Endpoint has completed					
Show details					
	< Back	Clos	e	Can	cel



Nota: l'opzione per la disinstallazione deve essere eseguita sul pacchetto di installazione e non su uninstall.exe

Per eseguire una disinstallazione invisibile all'utente e completa del connettore, lo switch è:

FireAMPSetup.exe /R /S /remove 1



Nota: è possibile eseguire queste operazioni anche in modalità non silenziosa rimuovendo l'opzione /S.

Per eseguire una disinstallazione completa di un connettore protetto da password, lo switch è:

FireAMPSetup.exe /uninstallpassword [Connector Protection Password]

Come ultima risorsa, l'esecuzione del programma di disinstallazione sul dispositivo su cui deve essere disinstallato il connettore risolverà la necessità.

Passaggio 1. Aprire il prompt dei comandi con privilegi amministrativi.

Passaggio 2. Passare alla posizione in cui si trova il connettore dell'endpoint protetto. Dove x è la versione del connettore CSE. Come mostrato nell'immagine.



Passaggio 3. Eseguire il file utilizzando gli argomenti seguenti. Come mostrato nell'immagine.

uninstall.exe/full 1

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

Passaggio 4. Seguire la procedura guidata fino a visualizzare la schermata Disinstallazione completata. Come mostrato nell'immagine.

Cisco Secure Endpoint Uninstall		_		\times
Uninstallation Complete				_
Uninstall was completed successfully.				_
Cisco Secure Endpoint has completed				
Show details				
	< Back	Close	Car	icel



Nota: se il percorso AMP non esiste, è necessario eseguire il comando senza indicare il percorso. Eseguire il comando con gli argomenti indicati.



Nota: se necessario, è possibile eseguire uninstaller.exe di un altro connettore per disinstallare il connettore desiderato.

Informazioni correlate

- Guida per l'utente di Secure Endpoint
- Documentazione e supporto tecnico Cisco Systems
- <u>API Secure Endpoint v3</u>

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).