Dépannage des méthodes de désinstallation du connecteur Secure Endpoint

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Méthodes de désinstallation
Désinstaller manuellement
Désinstallez le connecteur de la console Secure Endpoint.
Désinstaller le connecteur à l'aide des API
Désinstaller le connecteur avec les commutateurs de ligne de commande
Informations connexes

Introduction

Ce document décrit le processus de désinstallation d'un connecteur Cisco Secure Endpoint (CSE) installé sur des périphériques Windows avec différentes méthodes.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connecteur de terminal sécurisé
- Console Secure Endpoint
- API Secure Endpoint

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Console Secure Endpoint version 5.4.2024042415
- Connecteur Windows Secure Endpoint version 8.2.3.30119
- API Secure Endpoint v3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau

est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La procédure décrite dans ce document est utile dans les situations où vous cherchez à désinstaller le connecteur Secure Endpoint.

La désinstallation du connecteur est une option permettant de se débarrasser complètement du connecteur, que ce soit pour de nouvelles installations ou simplement ne plus avoir le connecteur sur un périphérique Windows.

Méthodes de désinstallation

Une fois que vous souhaitez désinstaller le connecteur Secure Endpoint sur un ordinateur Windows, suivez la méthode la mieux adaptée à vos besoins.

Désinstaller manuellement

Afin de désinstaller un connecteur localement.

Étape 1. Dans le périphérique, accédez à Program Files > Cisco > AMP > x (où x est la version du connecteur CSE).

Étape 2. Recherchez le fichier uninstall.exe. Comme l'illustre l'image.

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	
🕤 lībssl-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	
s 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	
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	
S vcruntime140.dll	2/20/2024 2:54 PM	Application exten	107 KB	
s 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	

Étape 3. Exécutez le fichier et suivez les instructions de l'assistant jusqu'à ce que l'écran Désinstallation terminée apparaisse. Comme l'illustre l'image.

S Cisco Secure Endpoint Uninstall —		×
Uninstallation Complete		
Uninstallation Complete		
Uninstall was completed successfully.		
Cisco Secure Endpoint has completed		
Chaux datata		
Show details		
	-	,
< Back Close	Car	icel

Étape 4. Une fois le processus de désinstallation terminé, la boîte de dialogue suivante s'affiche : "Prévoyez-vous de réinstaller Cisco Secure Endpoint ?". Comme l'illustre l'image.

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	



Remarque : si vous sélectionnez Non dans la boîte de dialogue de désinstallation, un redémarrage complet du périphérique sera nécessaire pour se débarrasser complètement des dossiers restants du CSE.

Désinstallez le connecteur de la console Secure Endpoint.

Si vous devez désinstaller à distance à partir de la console, vous pouvez le faire à l'aide du bouton Désinstaller le connecteur.

Étape 1. Dans la console, accédez à Gestion > Ordinateurs.

Étape 2. Localisez l'ordinateur que vous souhaitez désinstaller et cliquez sur pour afficher les détails.

Étape 3. Cliquez sur le bouton Désinstaller le connecteur. Comme l'illustre l'image.

🖩 🔻 🖽 Default-Winth in group Universitiest			
Hostname	Defaut-Wn11	Group de	Uninstall test
Operating System	T Windows 11, SP 0.0 (Build 22000.2538)	Policy Ó	uninstall test
Connector Version	T 8.2.3.30119 + Show download URL	Internal IP	
Install Date		External IP	N POPULATION CONTRACTOR OF
Connector GUID		Last Seen	
Processor ID	Reserver.	Definition Version	TETRA 64 bit (None)
Definitions Last Updated	None	Update Server	tetra-defs.amp.clsco.com
Cisco Secure Client ID	N/A	Cisco Security Risk Score	Pending
Othat Activation in progress 4 Exerts. 1 ^o Device Trajectory 10 Day and 10 Wew Changes			
R, Stark 🗘 Dagoose. 🖉 Move to Droup. 🗳 Usingtati Connector 📦 Dentes			

Étape 4. Cliquez sur Désinstaller lorsque vous êtes invité à confirmer l'action. Comme l'illustre l'image.

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

Étape 5. Vous recevrez un message de confirmation en haut de la console Secure Endpoint. Comme l'illustre l'image.

l'image.

1 connector is scheduled to be uninstalled	×
L'enregistrement du connecteur dans la console disparaît instantanément. Lors de la vérification	on
locale des informations, le connecteur passe momentanément à une stratégie de désinstallation et quelques minutes plus tard, il est complètement retiré du périphérique. Comme l'illustre	'n

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



Remarque : gardez à l'esprit que la période que le connecteur utilise pour effectuer cette tâche peut varier en fonction de votre environnement.



Attention : assurez-vous que le périphérique recevant la désinstallation reste connecté tout au long du processus.



Remarque : cette fonction ne peut être exécutée qu'individuellement, c'est-à-dire qu'elle ne permet pas la désinstallation en masse ou la désinstallation d'un groupe de périphériques. Pour plus de détails sur la fonctionnalité, veuillez vous reporter au Guide de l'utilisateur dans la section Désinstallation à distance <u>Guide de l'utilisateur de Secure Endpoint</u>.

Désinstaller le connecteur à l'aide des API

Si vous ne parvenez pas à désinstaller le connecteur via la console Secure Endpoint, vous pouvez utiliser des API.

L'API Secure Endpoint nécessite un accès via un compte authentifié et autorisé. Seuls les comptes autorisés peuvent soumettre des demandes aux opérations de l'API. Toutes les opérations doivent communiquer via une connexion HTTPS sécurisée.



Remarque : pour plus d'informations sur l'authentification Secure Endpoint pour l'API, reportez-vous à l'article suivant : <u>Authentification Secure Endpoint API.</u>

Étape 1. Intégrez Secure Endpoint à SecureX. Comme l'illustre l'image.



Étape 2. Enregistrez le client SecureX API. Comme l'illustre l'image.

Client Name*	
Remote Uninstall Te	st
Client Preset	
	× ×
API Clients OA	uth Code Clients
Scopes*	Select None
Search	Q
Admin	Provide admin privileges
VAO	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	nstall using API
·	
	Add New Client Close

Étape 3. Stockez les informations d'identification en toute sécurité. Comme l'illustre l'image.



Étape 4. Exécutez exemples.sh (récupéré à partir d'<u>exemples.sh</u>) le fichier en utilisant n'importe quel programme de fichier de script de votre choix.

Étape 5. Exécutez le fichier et saisissez vos informations d'identification. Comme l'illustre l'image.



Étape 6. Faites défiler jusqu'à ce que vous trouviez « jeton d'accès ». Copiez cette valeur pour l'authentifier ultérieurement lors de l'utilisation des API. Comme l'illustre l'image.





Note : Pour la création de ce document, nous avons utilisé git.bash. Cet outil n'est pas pris en charge par Cisco, tout doute ou question s'y rapportant, il est recommandé de contacter le support de cet outil.

Étape 7. Une fois le jeton d'authentification obtenu, vous pouvez utiliser un outil qui permet l'utilisation d'API.



Note : Pour la création de ce document, nous avons utilisé Postman. Cet outil n'est pas pris en charge par Cisco, tout doute ou question s'y rapportant, il est recommandé de contacter le support de cet outil.

Étape 8. Basé sur la syntaxe de référence API (<u>Demander la désinstallation d'un connecteur</u>). Effectuez la demande de désinstallation du connecteur en utilisant le GUID du périphérique à désinstaller.



Remarque : vous pouvez obtenir le GUID du connecteur de deux manières simples :

- Sur le portail Secure Endpoint, accédez à Gestion > Ordinateurs > Accédez à l'ordinateur souhaité > Affichez les détails > Obtenir le GUID.
- Ouvrez l'icône de la barre d'état > Accédez à l'onglet Statistiques > Obtenir le GUID.

Étape 9. Sélectionnez Bearer Token comme méthode d'authentification et entrez le jeton d'accès précédemment obtenu à l'étape 6. Comme l'illustre l'image.

mttps://api.amp.cisco.com/v3/organiz	ations. con	sputers/	🖺 Save 🗸 🖉
PUT v https://apl.amp.cisco.c	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 workin g variables. Learn more about <u>variables</u> .	g 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 Result		Status: 204 No Content Time: 788 ms Size:	512 B 🖾 Save as example 🚥
Pretty Raw Preview Visualize	Text V 📅		6 Q

Étape 10. Remplissez les champs obligatoires de l'appel API et cliquez sur le bouton Send. Attendez la réponse 204 : Pas de contenu. Comme l'illustre l'image.

https://api.amp.cisco.com/v3/organiza	tions	computers/ . 🖾 Save 🗸 🖉
PUT v https://api.amp.cisco.co	m/v:lorganizations.	Send 🗸
Params Authorization • Headers (9)	Body Pre-request Script	Tests Settings Cookies
Type Bearer Tok v	 Heads up! These parameter environment, we recommend 	ters hold sensitive data. To keep this data secure while working in a collaborative X 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

L'enregistrement du connecteur dans la console disparaît instantanément. Lors de la vérification locale des informations, le connecteur passe momentanément à une stratégie de désinstallation et, quelques minutes plus tard, il est complètement retiré du périphérique. Comme l'illustre l'image.

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



Remarque : gardez à l'esprit que la période que le connecteur utilise pour effectuer cette tâche peut varier en fonction de votre environnement.



Attention : assurez-vous que le périphérique recevant la désinstallation reste connecté tout au long du processus.

Si toutes les instances ci-dessus (méthodes de désinstallation) ont été épuisées et que vous n'avez toujours pas réussi à désinstaller le connecteur souhaité, vous pouvez opter pour l'option de dernier recours répertoriée dans la méthode suivante.

Désinstaller le connecteur avec les commutateurs de ligne de commande

Le programme d'installation dispose de commutateurs de ligne de commande intégrés qui vous permettent d'effectuer de nombreuses actions sur le point d'extrémité, comme indiqué dans l'article suivant : <u>Commutateurs de ligne de commande pour point d'extrémité sécurisé</u>.

Pour désinstaller le connecteur CSE avec des commutateurs de ligne de commande, procédez comme suit.

Étape 1. Ouvrez Command Prompt avec des privilèges d'administration.

Étape 2. Accédez à l'emplacement du package d'installation. Comme l'exemple illustré dans l'image.



Étape 3. Tapez le nom du package suivi des commutateurs de ligne de commande à exécuter. Comme l'illustre l'image.

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

Étape 4. Suivez les instructions de l'assistant jusqu'à l'écran Désinstallation terminée. Comme l'illustre l'image.

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



Remarque : le commutateur de désinstallation doit être exécuté sur le package d'installation et non sur uninstall.exe

Pour effectuer une désinstallation silencieuse et complète du connecteur, le commutateur est :

FireAMPSetup.exe /R /S /remove 1



Remarque : vous pouvez également effectuer ces opérations en mode non silencieux en supprimant le commutateur /S.

Pour effectuer la désinstallation complète d'un connecteur protégé par mot de passe, le commutateur est :

FireAMPSetup.exe /uninstallpassword [Connector Protection Password]

En dernier recours, l'exécution du programme de désinstallation sur le périphérique sur lequel le connecteur doit être désinstallé permettra de résoudre le problème.

Étape 1. Ouvrez Command Prompt avec des privilèges d'administration.

Étape 2. Naviguez jusqu'à l'emplacement du connecteur Secure Endpoint. x étant la version du connecteur CSE. Comme l'illustre l'image.



Étape 3. Exécutez le fichier à l'aide des arguments suivants. Comme l'illustre l'image.

uninstall.exe/full 1

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

Étape 4. Suivez les instructions de l'assistant jusqu'à l'écran Désinstallation terminée. Comme l'illustre l'image.

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



Remarque : si le chemin AMP n'existe pas, vous devez exécuter la commande sans indiquer le chemin. Exécutez simplement la commande avec les arguments indiqués.



Remarque : si nécessaire, il est possible d'exécuter le fichier uninstaller.exe d'un autre connecteur afin de désinstaller le connecteur souhaité.

Informations connexes

- Guide de l'utilisateur Secure Endpoint
- <u>Assistance et documentation techniques Cisco Systems</u>
- <u>API Secure Endpoint v3</u>

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.