## **Troubleshoot Secure Endpoint Connector Uninstall Methods**

## Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Uninstall Methods
Manually Uninstall
Uninstall Connector from Secure Endpoint console.
Uninstall Connector Using APIs
Uninstall Connector Using Command Line Switches
Related Information

## Introduction

This document describes the process to uninstall a Cisco Secure Endpoint (CSE) connector installed on Windows devices with different methods.

## Prerequisites

#### Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Endpoint Connector
- Secure Endpoint Console
- Secure Endpoint APIs

#### **Components Used**

The information in this document is based on these software and hardware versions:

- Secure Endpoint console version v5.4.2024042415
- Secure Endpoint Windows connector version v8.2.3.30119
- Secure Endpoint API 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. If your network is live, ensure that you understand the potential impact of any command.

## **Background Information**

The procedure described in this document is helpful in situations where you are looking to uninstall the Secure Endpoint connector.

Uninstalling the connector is an option to get rid of the connector altogether, either for fresh installations or simply not having the connector on a Windows device anymore.

## **Uninstall Methods**

Once you want to uninstall the Secure Endpoint connector on a Windows computer, follow the mehtod that better suits your needs.

#### **Manually Uninstall**

In order to uninstall a connector locally.

Step 1. In the device, navigate to **Program Files** > **Cisco** > **AMP** > **x** (Where x is the version of the CSE connector).

Step 2. Locate the **uninstall.exe** file. As shown in the image.

-		
· ·		

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	
s 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	
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	4
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	

Step 3. Execute the file and follow the wizard until getting the Uninstallation Complete screen. As shown in the image.

Cisco Secure Endpoint Uninstall	-	×
Uningtallation Complete		
Uninstallation Complete		
Uninstall was completed successfully.		
Cisco Secure Endpoint has completed		
Show details		
Silow details		
	_	
< Back Close	Ca	ncel

Step 4. After finishing the uninstallation process, you will get the following dialog box asking **"Do you plan on installing Cisco Secure Endpoint again?"**. As shown in the image.

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	ing 'No' including
	Yes	No



**Note**: In case you select **No** on the uninstall dialog box, a full reboot of the device will be required to get completely rid of any CSE remaining folders.

#### Uninstall Connector from Secure Endpoint console.

If you need to uninstall remotely from the console, you can do it using the Uninstall connector button.

Step 1. In the console, navigate to **Management > Computers**.

Step 2. Locate the computer you want to uninstall and click to display details.

Step 3. Click on Uninstall Connector button. As shown in the image.

🗮 🔻 🛱 Default-Wint1 in group Uninstall test			н. Н		
Hostname	Default-Win11	Oroup 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	a burne data and		
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		
Orbitat: Activation in progress			4 Events 2 Device Trajectory (3 Diagnatics (3 View Changes		
			역, Scan [영 Diagnose] 🐟 Move to Group [양 Uninstall Connector 📦 Delete		

Step 4. Click **Uninstall** when you are asked to connfirm the action. As shown in the image.

Uninstall Connector	×
<b>E Default-Win11</b> in group <b>Uninstall test</b> will be uninstalled from the endpoint and remo from the computer management page.	wed
A This cannot be undone.	
Cancel	all

Step 5. You will receive a confirmation message at the top of Secure Endpoint console. As shown in the image.

i 1 con	nector is	s sched	duled 1	to be	uninstal	led									×

The connector registration in the console will disappear instantly. Upon reviewing the information locally, the connector will momentarily move to an uninstall policy and a few minutes later, it will be completely removed from the device. As shown in the image.

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



**Note**: Keep on mind that the period of time that the connector uses to perform this to perform this task may vary depending on your environment.



Caution: Ensure that the device receiving the uninstall remains connected throughout the process.



**Note**: This function can only be executed individually, i.e. it does not allow mass uninstallation or uninstallation of a group of devices. For more details on the feature, please refer to the User Guide in the Remote Uninstall section <u>Secure Endpoint User Guide</u>.

#### **Uninstall Connector Using APIs**

In case you have failed to uninstall the connector via the Secure Endpoint console, a viable option is to use APIs.

The Secure Endpoint API requires access via an authenticated and authorized account. Only authorized accounts are able to submit requests to API operations. All operations must communicate over a secure HTTPS connection.



**Note**: For further information regarding Secure Endpoint Authentication for API, refer to the following article: <u>Secure Endpoint API Authentication</u>.

Step 1. Integrate Secure Endpoint with SecureX. As shown in the image.



Step 2. Register SecureX API client. As shown in the image.

Client Name*	
Remote Uninstall T	est
Client Preset	
	× ~
API Clients O/	Auth Code Clients
Scopes*	Select None
Search	Q
Admin	Provide admin privileges
VA 🔽	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 uni	nstall using API
	Add New Client Close

Step 3. Securely store credentials. As shown in the image.



Step 4. Run examples.sh (retrieved from examples.sh) the file using any script file program of your choice.

Step 5. Run the file and enter your credentials. As shown in the image.



Step 6. Scroll until you find "access token". Copy this value to later authenticate in the use of APIs. As shown in the image.





**Note:** For the creation of this document we made use of **git.bash**. This tool is not supported by Cisco, any doubt or question related to it, it is recommended to contact the support of this tool.

Step 7. Once the authentication token is obtained, you can use a tool that allows the use of APIs.



**Note**: For the creation of this document we made use of **Postman**. This tool is not supported by Cisco, any doubt or question related to it, it is recommended to contact the support of this tool.

Step 8. Based on the API reference syntax (<u>Request a connector uninstallation</u>). Make the connector uninstallation request using the GUID of the device to be uninstalled.



Note: You can get the connector GUID in the following two simple ways:

- On the Secure Endpoint portal navigate to Management > Computers > Navigate to the desired computer > Display the details > Get GUID.
- Open Tray Icon > Navigate to Statistics tab > Get GUID.

Step 9. Select **Bearer Token** as authentication method and enter the access token previously obtained on Step 6. As shown in the image.

ttps://api.amp.cisco.com/v3/organiza	tions	computers/	🛱 Save 🗸 🖉
PUT V https://api.amp.cisco.co	m/v3/organizations.	computers/	Send 🗸
Params Authorization • Headers (9)	Body Pre-request Script Te	its Settings	Cookies
Type Bearer Tok_ ~	(1) 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. Siz	e: 512 8 💮 Save as example 🚥
Pretty Raw Preview Visualize	Text 🗸 📅		ri Q
1			

Step 10. Fill in the required fields of the API call and click on **Send** button. Wait for the *204: No Content response*. As shown in the image.

nttps://api.amp.cisco.com/v3/organiza	tions	computers/ . 🖺 Sav	re ~ 🖉 🖾
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	(1) Heads up! These parameter environment, we recommend.	eters hold sensitive data. To keep this data secure while working in a col rend using variables. Learn more about <u>variables</u> .	laborative 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 🗸 📅		6 Q
1			

The connector registration in the console will disappear instantly. Upon reviewing the information locally, the connector will momentarily move to an uninstall policy and a few minutes later, it will be completely removed from the device. As shown in the image.

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



**Note**: Keep on mind that the period of time that the connector uses to perform this to perform this task may vary depending on your environment.



Caution: Ensure that the device receiving the uninstall remains connected throughout the process.

If all the above instances (uninstalling methods) have been exhausted and you still have not succeeded in uninstalling the desired connector, you can opt for the last resort option listed in the following method.

#### **Uninstall Connector Using Command Line Switches**

The Installer has built-in command line switches that allows you to perform numerous actions in the endpoint as mentioned in the following article: <u>Command Line Switches for Secure Endpoint</u>.

In order to uninstall the CSE connector with command-line switches use the following instructions.

Step 1. Open Command Prompt with administrative privileges.

Step 2. Navigate to the location where the installation package is located. As the example shown in the image.

# C:\Users\Mex-Amp>cd Downloads

Step 3. Type the package name followed by the command line switches to be executed. As shown in the image.

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

Step 4. Follow the wizard until getting the Uninstallation Complete screen. As shown in the image.

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



**Note**: The switch for uninstallation must be run against the installation package and not uninstall.exe

To perform a silent and **complete** uninstallation of the connector, the switch is:

FireAMPSetup.exe /R /S /remove 1



Note: You can also perform these in non-silent modes by removing the /S switch.

To perform a **complete** uninstallation of a connector that has password protection, the switch is:

FireAMPSetup.exe /uninstallpassword [Connector Protection Password]

As a last resort, running the uninstaller on the device on which the connector needs to be uninstalled will solve the need.

Step 1. Open Command Prompt with administrative privileges.

Step 2. Navigate to the location where the Secure Endpoint connector is located. Where x is the version of the CSE connector. As shown in the image.

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

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

Step 3. Execute the file using the following arguments. As shown in the image.

uninstall.exe/full 1

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

Step 4. Follow the wizard until getting the Uninstallation Complete screen. As shown in the image.

Cisco Secure Endpoint Uninstall		-		$\times$
Uninstallation Complete				
Uninstallation Complete				-
Cisco Secure Endpoint has completed				
Show details				
	< Back	Close	Can	cel



**Note**: In case the AMP path does not exist, you have to run the command without indicate the path, just run the command with the indicated arguments.



**Note**: If necessary, it is possible to run the uninstaller.exe of another connector in order to uninstall the desired connector.

## **Related Information**

- Secure Endpoint User Guide
- <u>Technical Support & Documentation Cisco Systems</u>
- Secure Endpoint API v3