# Solucionar problemas dos métodos de desinstalação do conector de endpoint seguro

## Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
<u>Métodos de Desinstalação</u>
Desinstalar manualmente
Desinstale o Connector do console do Ponto de Extremidade Seguro.
Desinstalar o Conector Usando APIs
Desinstalar o Conector Usando Comutadores de Linha de Comando
Informações Relacionadas

## Introdução

Este documento descreve o processo para desinstalar um conector Cisco Secure Endpoint (CSE) instalado em dispositivos Windows com métodos diferentes.

## Pré-requisitos

#### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conector de endpoint seguro
- Console de endpoint seguro
- APIs de endpoint seguras

#### **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software e hardware:

- Console Secure Endpoint versão v5.4.2024042415
- Conector Secure Endpoint Windows versão v8.2.3.30119
- API v3 de endpoint seguro

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

## Informações de Apoio

O procedimento descrito neste documento é útil em situações em que você está procurando desinstalar o conector de Ponto de Extremidade Seguro.

Desinstalar o conector é uma opção para se livrar do conector completamente, seja para novas instalações ou simplesmente não ter mais o conector em um dispositivo Windows.

## Métodos de Desinstalação

Quando quiser desinstalar o conector de Ponto de Extremidade Seguro em um computador Windows, siga o método que melhor atenda às suas necessidades.

#### Desinstalar manualmente

Para desinstalar um conector localmente.

Etapa 1. No dispositivo, navegue até Program Files > Cisco > AMP > x (onde x é a versão do conector CSE).

Etapa 2. Localize o arquivo uninstall.exe. Conforme mostrado na imagem.

_		

□ > 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	
🛐 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	
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	1
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	

Etapa 3. Execute o arquivo e siga o assistente até obter a tela Desinstalação concluída. Conforme mostrado na imagem.

Sisco Secure Endpoint Uninstall		_		×
Uninstallation Complete				
Uninstall was completed successfully.				
Cisco Secure Endpoint has completed				
Show details				
	< Back	Close	Cani	:el

Etapa 4. Após concluir o processo de desinstalação, você verá a seguinte caixa de diálogo perguntando "Você planeja instalar o Cisco Secure Endpoint novamente?". Conforme mostrado na imagem.

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? Click Cisco Secure Endpoint	ing 'No' including
	Yes	No



Observação: caso você selecione Não na caixa de diálogo de desinstalação, será necessária uma reinicialização completa do dispositivo para se livrar completamente de qualquer pasta restante do CSE.

Desinstale o Connector do console do Ponto de Extremidade Seguro.

Se precisar desinstalar remotamente do console, você pode fazer isso usando o botão Desinstalar conector.

Etapa 1. No console, navegue até Gerenciamento > Computadores.

Etapa 2. Localize o computador que deseja desinstalar e clique em para exibir os detalhes.

Etapa 3. Clique no botão Uninstall Connector. Conforme mostrado na imagem.

🖩 🔻 🖽 Default-Winth in group Uninetial test 📁					
Hostname	Default-Win11	Group de	Uninstall test		
Operating System	¥ 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			
Connector GUID	And a set of the particular	Last Seen			
Processor ID	Reserved.	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		
- Othial Activation in progress e Events 12 Device Trajectory 10 Diagna Conference Confe					
R, Scars. 🕅 Diagnose. 🖉 Universitad Connector 🖬 Dealer.					

Etapa 4. Clique em Desinstalar quando for solicitado que você confirme a ação. Conforme mostrado na imagem.

Uninstall Connector	$\times$
<b>Default-Win11</b> in group <b>Uninstall test</b> will be uninstalled from the endpoint and re from the computer management page.	emoved
This cannot be undone.	
Cancel	install

Etapa 5. Você receberá uma mensagem de confirmação na parte superior do console do Secure Endpoint. Conforme mostrado na imagem.

1 connector is scheduled to be uninstalled	×
O registro do conector no console desaparecerá instantaneamente. Após a revisão local das	

O registro do conector no console desaparecera instantaneamente. Apos a revisao local das informações, o conector moverá momentaneamente para uma política de desinstalação e, alguns minutos depois, será completamente removido do dispositivo. Conforme mostrado na imagem.

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



Observação: lembre-se de que o período de tempo que o conector usa para executar essa tarefa pode variar dependendo do seu ambiente.



Cuidado: verifique se o dispositivo que recebe a desinstalação permanece conectado durante todo o processo.



Observação: esta função só pode ser executada individualmente, ou seja, não permite desinstalação em massa ou desinstalação de um grupo de dispositivos. Para obter mais detalhes sobre o recurso, consulte o Guia do usuário na seção Desinstalação remota do <u>Guia do usuário do ponto de extremidade seguro</u>.

#### Desinstalar o Conector Usando APIs

Caso você não tenha desinstalado o conector por meio do console do Secure Endpoint, uma opção viável é usar APIs.

A API do Secure Endpoint requer acesso por meio de uma conta autenticada e autorizada. Somente contas autorizadas podem enviar solicitações para operações de API. Todas as operações devem se comunicar através de uma conexão HTTPS segura.



Observação: para obter mais informações sobre a Autenticação de Ponto de Extremidade Seguro para API, consulte o seguinte artigo: <u>Autenticação de API de Ponto de</u> <u>Extremidade Seguro.</u>

Etapa 1. Integre o Secure Endpoint com o SecureX. Conforme mostrado na imagem.



Etapa 2. Registre o cliente da API SecureX. Conforme mostrado na imagem.

Client Name*	
Remote Uninstall Te	st
Client Preset	
	× `
API Clients OA	uth Code Clients
Scopes*	Select Non
Search	(
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
	Add New Client Close

Etapa 3. Armazenar credenciais com segurança. Conforme mostrado na imagem.



Etapa 4. Execute examples.sh (recuperado de <u>examples.sh</u>) o arquivo usando qualquer programa de arquivo de script de sua escolha.

Etapa 5. Execute o arquivo e insira suas credenciais. Conforme mostrado na imagem.



Etapa 6. Role até encontrar "access token". Copie esse valor para autenticar posteriormente no uso de APIs. Conforme mostrado na imagem.





Observação: para a criação deste documento, usamos git.bash. Esta ferramenta não é suportada pela Cisco, qualquer dúvida ou pergunta relacionada a ela, é recomendável entrar em contato com o suporte desta ferramenta.

Passo 7. Depois que o token de autenticação for obtido, você poderá usar uma ferramenta que permita o uso de APIs.



Nota: Para a criação deste documento, utilizamos o Postman. Esta ferramenta não é suportada pela Cisco, qualquer dúvida ou pergunta relacionada a ela, é recomendável entrar em contato com o suporte desta ferramenta.

Etapa 8. Baseado na sintaxe de referência da API (<u>Solicitar desinstalação do conector</u>). Faça a solicitação de desinstalação do conector usando o GUID do dispositivo a ser desinstalado.



Observação: você pode obter o GUID do conector das duas seguintes maneiras simples:

- No portal Secure Endpoint, navegue até Management > Computers > Navigate to the desirable computer > Display the details > Get GUID.
- Abra o ícone da bandeja > Navegue até a guia Estatísticas > Obter GUID.

Etapa 9. Selecione Bearer Token como método de autenticação e insira o token de acesso obtido anteriormente na Etapa 6. Conforme mostrado na imagem.

ttps://api.amp.cisco.com/v3/organiza	tions. com	puters/	Save 🗸 🖉 🖾
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 environment, we recommend using	sensitive data. To keep this data secure while working in a variables. Learn more about <u>variables</u> .	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: 512 8	Save as example •••
Pretty Raw Preview Visualize	Text 🗸 📅		ତ ହ

Etapa 10. Preencha os campos obrigatórios da chamada à API e clique no botão Send. Aguarde a resposta 204: Sem conteúdo. Conforme mostrado na imagem.

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 v	Heads up! These paramet environment, we recommend the second s	ters hold sensitive data. To keep this data secure while work and using variables. Learn more about <u>variables</u> .	king 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		C Status 204 No Content Time: 788 ms Siz	ie: 512 8 🖾 Save as example 🔹
Pretty Raw Preview Visualize	Text 🗸 📅		6 Q

O registro do conector no console desaparecerá instantaneamente. Após a revisão local das informações, o conector moverá momentaneamente para uma política de desinstalação e, alguns minutos depois, será completamente removido do dispositivo. Conforme mostrado na imagem.

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



Observação: lembre-se de que o período de tempo que o conector usa para executar essa tarefa pode variar dependendo do seu ambiente.



Cuidado: verifique se o dispositivo que recebe a desinstalação permanece conectado durante todo o processo.

Se todas as instâncias acima (métodos de desinstalação) tiverem sido esgotadas e você ainda não tiver conseguido desinstalar o conector desejado, você poderá optar pela opção de último recurso listada no método a seguir.

#### Desinstalar o Conector Usando Comutadores de Linha de Comando

O instalador tem switches de linha de comando incorporados que permitem executar várias ações no endpoint, conforme mencionado no seguinte artigo: <u>Switches de linha de comando para</u> <u>endpoint seguro</u>.

Para desinstalar o conector CSE com switches de linha de comando, use as instruções a seguir.

Etapa 1. Abra o Command Prompt com privilégios administrativos.

Etapa 2. Navegue até o local onde o pacote de instalação está localizado. Como o exemplo mostrado na imagem.



Etapa 3. Digite o nome do pacote seguido pelas opções de linha de comando a serem executadas. Conforme mostrado na imagem.

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

Etapa 4. Siga o assistente até obter a tela Desinstalação concluída. Conforme mostrado na imagem.

S Cisco Secure Endpoint Uninstall			-		×
Uninstallation Complete					
Uninstall was completed successfully.					
Cisco Secure Endpoint has completed					
Show details					
	1000				
	< Back	Close	!	Can	cel



Observação: a opção de desinstalação deve ser executada no pacote de instalação e não no uninstall.exe

Para executar uma desinstalação silenciosa e completa do conector, o switch é:

FireAMPSetup.exe /R /S /remove 1



Observação: você também pode executá-los em modos não silenciosos removendo a opção /S.

Para executar uma desinstalação completa de um conector que tenha proteção por senha, o switch é:

FireAMPSetup.exe /uninstallpassword [Connector Protection Password]

Como último recurso, executar o desinstalador no dispositivo no qual o conector precisa ser desinstalado resolverá a necessidade.

Etapa 1. Abra o Command Prompt com privilégios administrativos.

Etapa 2. Navegue até o local onde o conector de Ponto de Extremidade Seguro está localizado. Onde x é a versão do conector CSE. Conforme mostrado na imagem.



Etapa 3. Execute o arquivo usando os seguintes argumentos. Conforme mostrado na imagem.

uninstall.exe/full 1

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

Etapa 4. Siga o assistente até obter a tela Desinstalação concluída. Conforme mostrado na imagem.

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



Observação: caso o caminho do AMP não exista, você terá que executar o comando sem indicar o caminho, basta executar o comando com os argumentos indicados.



Observação: se necessário, é possível executar o uninstaller.exe de outro conector para desinstalar o conector desejado.

## Informações Relacionadas

- Guia do usuário do Secure Endpoint
- Suporte Técnico e Documentação Cisco Systems
- <u>API v3 de endpoint seguro</u>

#### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.