セキュアエンドポイントコネクタのアンインス トール方法のトラブルシューティング

| 内容 |
|--|
| <u>はじめに</u> |
| 前提条件 |
| <u>要件</u> |
| <u>使用するコンポーネント</u> |
| <u>背景説明</u> |
| <u>アンインストール方法</u> |
| <u>手動アンインストール</u> |
| <u>セキュアエンドポイントコンソールからコネクタをアンインストールします。</u> |
| <u>APIを使用したコネクタのアンインストール</u> |
| <u>コマンドラインスイッチを使用したコネクタのアンインストール</u> |
| 関連情報 |

はじめに

このドキュメントでは、さまざまな方法でWindowsデバイスにインストールされたCisco Secure Endpoint(CSE)コネクタをアンインストールするプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- セキュアエンドポイントコネクタ
- セキュアなエンドポイントコンソール
- ・ セキュアエンドポイントAPI

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ・ セキュアエンドポイントコンソールバージョンv5.4.2024042415
- ・ セキュアエンドポイントWindowsコネクタバージョンv8.2.3.30119
- ・ セキュアエンドポイントAPI v3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

このドキュメントで説明する手順は、セキュアエンドポイントコネクタをアンインストールする 場合に役立ちます。

コネクタのアンインストールは、コネクタを完全に取り除くためのオプションです。新規インス トールの場合、または単にWindowsデバイスにコネクタを持っていない場合に使用します。

アンインストール方法

WindowsコンピュータでSecure Endpoint Connectorをアンインストールする場合は、ニーズに適した方法に従ってください。

手動アンインストール

コネクタをローカルでアンインストールします。

ステップ1:デバイスで、Program Files > Cisco > AMP > x (xはCSEコネクタのバージョン)に 移動します。

ステップ2: uninstall.exeファイルを探します。図に示すように。

С

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

| 0 6 6 6 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 |
| 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 |
| 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 |

ステップ 3:ファイルを実行し、ウィザードに従って[Uninstallation Complete] (アンインストー ルの完了)画面を表示します。 図に示すように。

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

ステップ 4:アンインストール処理が完了すると、「Do you plan on installing Cisco Secure Endpoint again?」というダイアログボックスが表示されます。図に示すように。

| Cisco Secure Endpoint Uninstall | | × |
|--|---|-----------------------|
| Do you plan on installing Cisco Secure will delete all local data generated by C history and quarantine files. | Endpoint again? Clicki lisco Secure Endpoint i | ing 'No' including |
| | Yes | No |



注:アンインストールダイアログボックスでNoを選択した場合、CSEの残りのフォルダ を完全に削除するには、デバイスを完全に再起動する必要があります。

セキュアエンドポイントコンソールからコネクタをアンインストールします。

コンソールからリモートでアンインストールする必要がある場合は、コネクタのアンインストー ルボタンを使用してアンインストールできます。

ステップ1:コンソールで、Management > Computersの順に移動します。

ステップ2:アンインストールするコンピュータを探し、クリックして詳細を表示します。

ステップ3: Uninstall Connectorボタンをクリックします。 図に示すように。

| 🗑 🔻 🗊 Default-Wint I in group Uninstall test (# | | | | |
|---|---|---------------------------|--------------------------|--|
| Hostname | Default-Win11 | Group de | Uninstall test | |
| Operating System | ¥ 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 territoria a | |
| Connector GUID | And a set of the particular | Last Seen | | |
| Processor ID | Handmann I. | 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 | |
| Orbital Activation in progress | | | | |
| Q. Sain | | | | |

ステップ4:操作の確認を求められたら、Uninstallをクリックします。 図に示すように。

| Uninstall Connector | × |
|---|-----|
| EXAMPLE : Default-Win11 in group Uninstall test will be uninstalled from the endpoint and remo from the computer management page. | wed |
| A This cannot be undone. | |
| | |
| Cancel Uninst | all |

ステップ 5 : セキュアエンドポイントコンソールの上部に確認メッセージが表示されます。 図に 示すように。

| 1 connector is scheduled to be uninstalled | × |
|--|-------------|
| コンソールでのコネクタの登録は即座に消えます。情報をローカルで確認すると、コネー 時的にアンインストールポリシーに移行し、数分後にデバイスから完全に削除されます。 | フタは一 図に示 |

すように。

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



注:コネクタがこのタスクを実行するために使用する期間は、環境によって異なる可能 性があることに注意してください。



注意:アンインストールを受信するデバイスが、プロセス全体を通じて接続されたまま であることを確認してください。



注:この機能は個別にのみ実行できます。つまり、デバイスグループの一括アンインス トールまたは一括アンインストールは許可されません。機能の詳細については、「リモ ートアンインストール」セクション「<u>セキュアエンドポイントユーザガイド</u>」のユーザ ガイドを参照してください。

APIを使用したコネクタのアンインストール

セキュアエンドポイントコンソールを使用してコネクタのアンインストールに失敗した場合は、 APIを使用する方法が実行可能です。

Secure Endpoint APIには、認証および承認されたアカウントを介したアクセスが必要です。承認 されたアカウントのみがAPI操作に要求を送信できます。すべての操作は、セキュアなHTTPS接 続を介して通信する必要があります。



注:APIのSecure Endpoint Authenticationの詳細については、「<u>Secure Endpoint APIの認</u> 証」を参照してください<u>。</u>

ステップ1:セキュアエンドポイントをSecureXと統合します。図に示すように。



ステップ2: SecureX APIクライアントを登録します。 図に示すように。

| Client Name* | | |
|----------------------|--|---|
| Remote Uninstall Te | st | |
| | | |
| Client Preset | | _ |
| | × × | 1 |
| API Clients OA | uth Code Clients | |
| Scopes* | Select None | е |
| Search | 0 | 2 |
| 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 | |
| | | |

ステップ 3:クレデンシャルを安全に保存します。 図に示すように。



ステップ4:任意のスクリプトファイルプログラムを使用して、ファイルに examples.sh(<u>examples.sh</u>から取得)を実行します。

ステップ5:ファイルを実行し、資格情報を入力します。図に示すように。



手順 6:「access token」が見つかるまでスクロールします。この値をコピーして、後でAPIを使用して認証します。図に示すように。





注:このドキュメントの作成にはgit.bashを使用しました。このツールはシスコのサポート対象外です。関連する疑問点やご質問がある場合は、このツールのサポート担当者にお問い合わせください。

手順7:認証トークンを取得したら、APIを使用できるツールを使用できます。



注:このドキュメントの作成には、Postmanを使用しました。このツールはシスコのサポート対象外です。関連する疑問点やご質問がある場合は、このツールのサポート担当者にお問い合わせください。

ステップ 8: API参照構文に基づく(<u>コネクタのアンインストールの要求</u>)。アンインストールする デバイスのGUIDを使用して、コネクタのアンインストール要求を行います。



注:コネクタGUIDは、次の2つの簡単な方法で取得できます。

- セキュアエンドポイントポータルで、Management > Computers > Navigate to the desired computer > Display the details > Get GUIDの順に移動します。
- ・トレイアイコンを開き、[統計]タブに移動> [GUIDの取得]を選択します。

ステップ9:認証方式としてBearer Tokenを選択し、ステップ6で取得したアクセストークンを入力します。図に示すように。

| ttps://api.amp.cisco.com/v3/organiza | tions | computers) | we ~ 🖉 🗉 |
|--|---|--|-----------------|
| PUT v https://api.amp.cisco.co | m/v3/organizations/ | computers/ | Send 🕑 |
| Params Authorization • Headers (9) | Body Pre-request Script | Tests Settings | Cookies |
| Type Bearer Tok_ ~ | (1) Heads up! These paramete environment, we recomment | rs hold sensitive data. To keep this data secure while working in a co d using variables. Learn more about <u>variables</u> . | llaborative 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 🗸 🚍 | | 5 Q |

ステップ 10 : APIコールの必須フィールドに入力し、Sendボタンをクリックします。「204: No Content response」が表示されるまで待ちます。図に示すように。

| PUT v https://api.amp.cisco.c | om/v: /organizations/ | computers/ Se | nd ~ |
|---|--|---|--------|
| Params Authorization Headers (9) | Body Pre-request Script | Tests Settings | Cookie |
| Bearer Tok | Heads up! These parameter environment, we recomment | ars hold sensitive data. To keep this data secure while working in a collaborative nd using variables. Learn more about <u>variables</u> . | × |
| The authorization header will be sutomatically generated when you send he request. Learn more about | Token | | |
| | | Ch. Statut 204 No Content Time 788 ms. Size: 512 B (2) Save as r | xample |
| ody Cookies Headers (13) Test Result | - | 40 min to hit being the first of the | |

コンソールでのコネクタの登録は即座に消えます。情報をローカルで確認すると、コネクタは一 時的にアンインストールポリシーに移行し、数分後にデバイスから完全に削除されます。図に示 すように。

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



注:コネクタがこのタスクを実行するために使用する期間は、環境によって異なる可能 性があることに注意してください。



注意:アンインストールを受信するデバイスが、プロセス全体を通じて接続されたまま であることを確認してください。

上記のすべてのインスタンス(アンインストール方法)を使い果たしても目的のコネクタをアン インストールできない場合は、次の方法でリストされている最後のリゾートオプションを選択で きます。

コマンドラインスイッチを使用したコネクタのアンインストール

インストーラには、エンドポイントで多数のアクションを実行できるコマンドラインスイッチが 組み込まれています(<u>セキュアエンドポイント用のコマンドラインスイッチ</u>を参照)。

コマンドラインスイッチでCSEコネクタをアンインストールするには、次の手順を実行します。

ステップ1:管理者権限でコマンドプロンプトを開きます。

ステップ2:インストールパッケージがある場所に移動します。図に示す例と同様です。

C:\Users\Mex-Amp>cd Downloads

ステップ 3:パッケージ名を入力し、続けて実行するコマンドラインスイッチを入力します。 図 に示すように。

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

ステップ 4: ウィザードの指示に従って、 [Uninstallation Complete] (アンインストールの完了)画面を表示します。 図に示すように。

| S Cisco Secure Endpoint Uninstall | | - | | × |
|---------------------------------------|--------|-------|------|-----|
| University Consults | | | | |
| Uninstallation Complete | | | | _ |
| Uninstall was completed successfully. | | | | |
| Cisco Secure Endpoint has completed | | | | |
| | | | | í |
| Show details | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | < Back | Close | Cano | sel |



注:アンインストール用のスイッチは、uninstall.exeではなく、インストールパッケージ に対して実行する必要があります

コネクタのサイレントアンインストールと完全なアンインストールを実行するスイッチは次のと おりです。

FireAMPSetup.exe /R /S /remove 1



注:/Sスイッチを取り外して、non-silentモードで実行することもできます。

パスワードで保護されたコネクタの完全なアンインストールを実行するには、スイッチが次の状 態になります。

FireAMPSetup.exe /uninstallpassword [Connector Protection Password]

最後の手段として、コネクタをアンインストールする必要があるデバイスでアンインストーラを 実行すると、この問題が解決します。

ステップ1:管理者権限でコマンドプロンプトを開きます。

ステップ2:セキュアエンドポイントコネクタが配置されている場所に移動します。 xはCSEコ ネクタのバージョンです。図に示すように。

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

ステップ3:次の引数を使用してファイルを実行します。図に示すように。

uninstall.exe/full 1

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

ステップ 4: ウィザードの指示に従って、 [Uninstallation Complete] (アンインストールの完了)画面を表示します。図に示すように。

| Cisco Secure Endpoint Uninstall | | - | - | | × |
|---------------------------------------|--------|-------|---|-------|---|
| Uninstallation Complete | | | | | |
| Uninstallation Complete | | | | | |
| Uninstall was completed successfully. | | | | | _ |
| Cisco Secure Endpoint has completed | | | | | |
| | | | | | |
| Show details | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | < Back | Close | | Cance | 1 |



注:AMPパスが存在しない場合は、パスを指定せずにコマンドを実行する必要があります。 指定した引数でコマンドを実行してください。



注:必要に応じて、別のコネクタのuninstaller.exeを実行して目的のコネクタをアンイン ストールすることもできます。

関連情報

- セキュアエンドポイントユーザガイド
- ・ <u>テクニカル サポートとドキュメント Cisco Systems</u>
- ・ <u>セキュアエンドポイントAPI v3</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。