

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

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[アンインストール方法](#)

[手動アンインストール](#)

[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。](#)

[APIを使用したコネクタのアンインストール](#)

[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](#)

[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

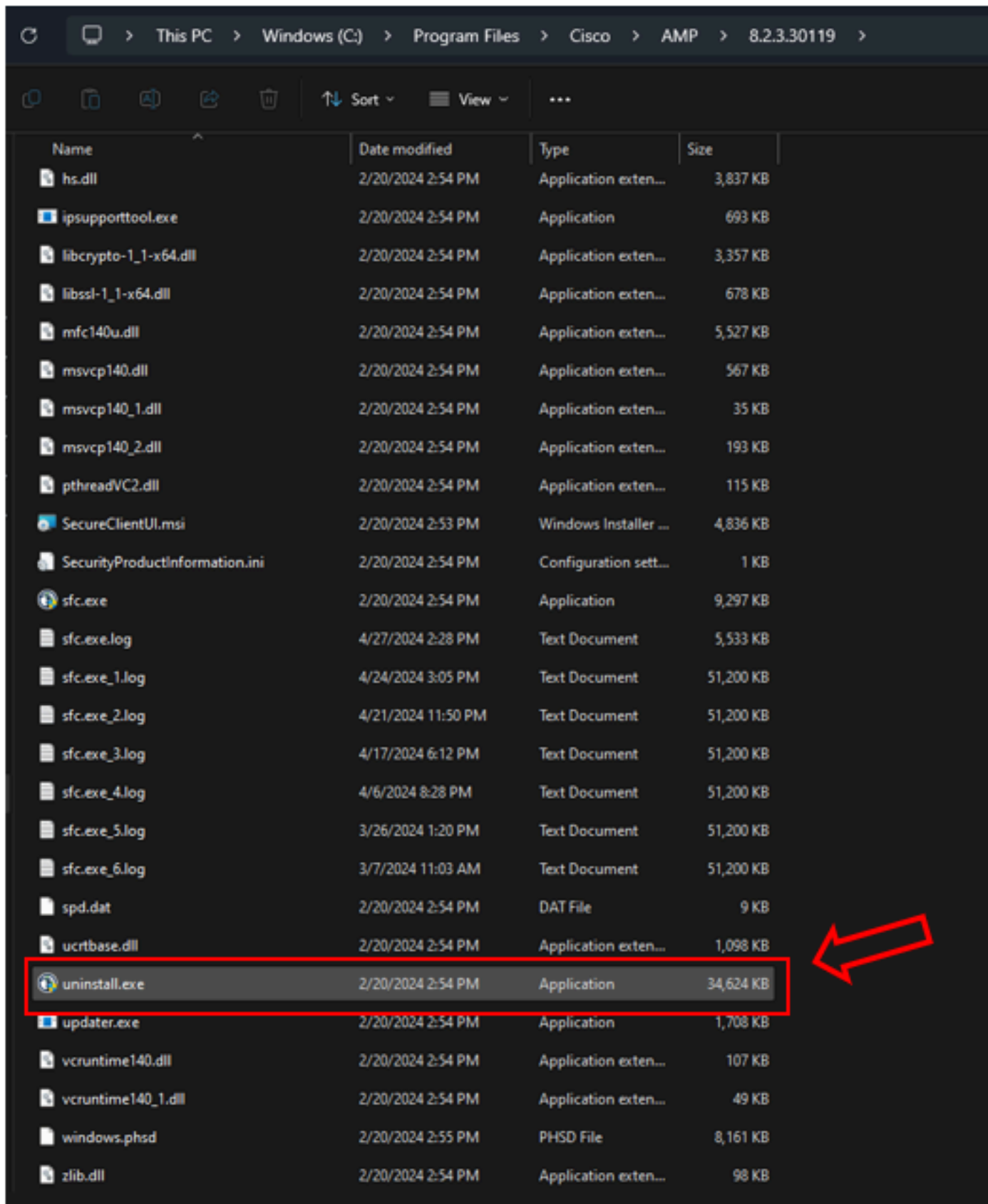
WindowsコンピュータでSecure Endpoint Connectorをアンインストールする場合は、ニーズに適した方法に従ってください。

手動アンインストール

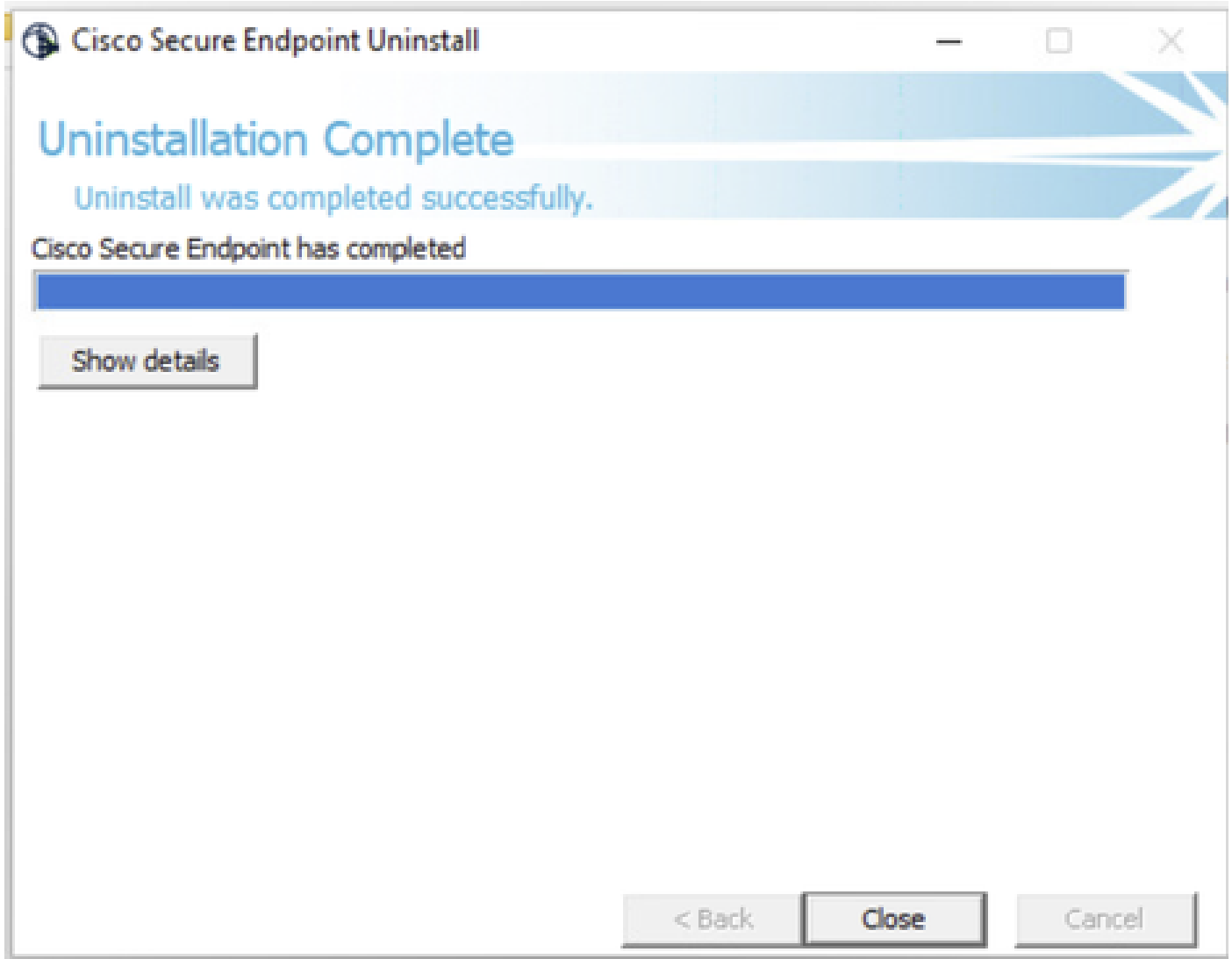
コネクタをローカルでアンインストールします。

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。

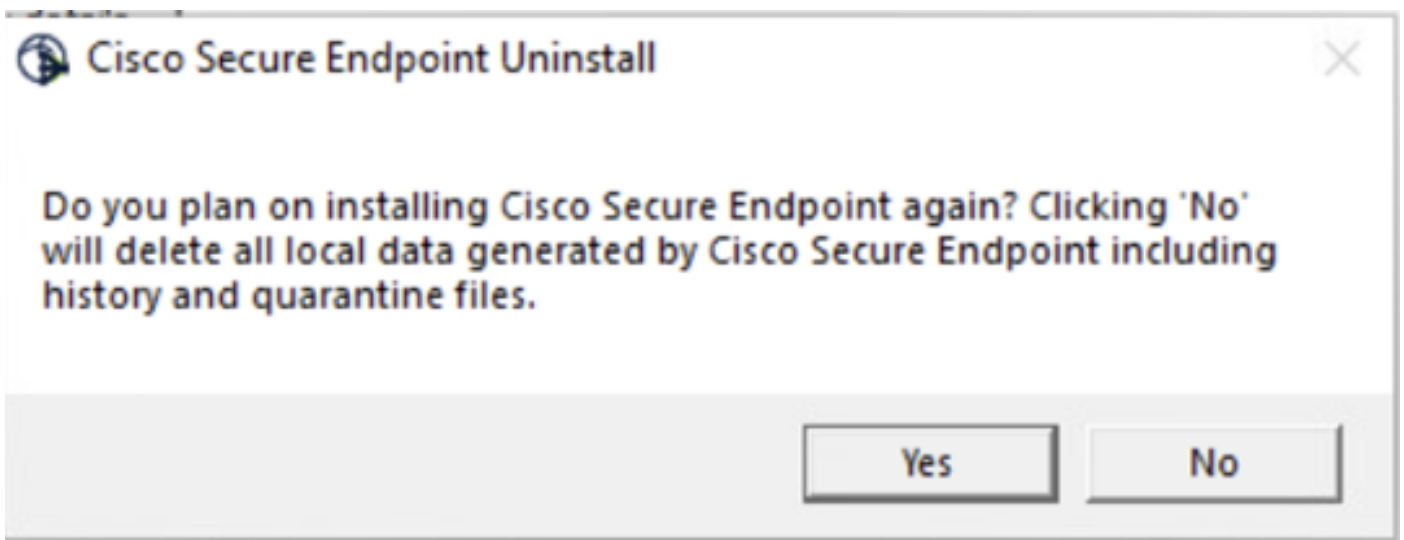
ステップ 2 : uninstall.exeファイルを探します。図に示すように。



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。



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。





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。

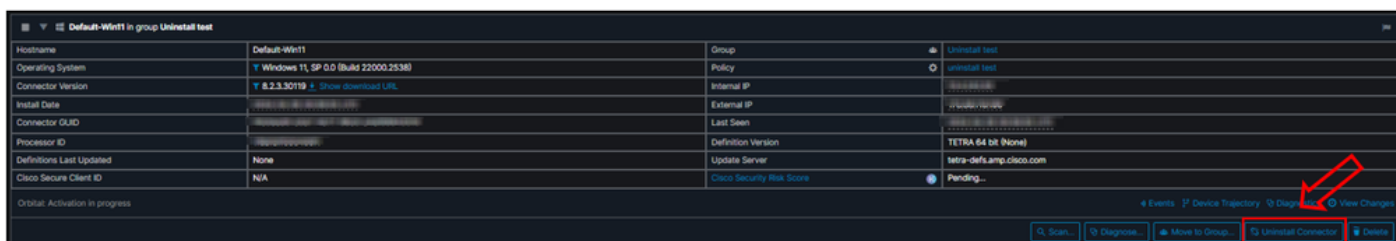
セキュアエンドポイントコンソールからコネクタをアンインストールします。

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。

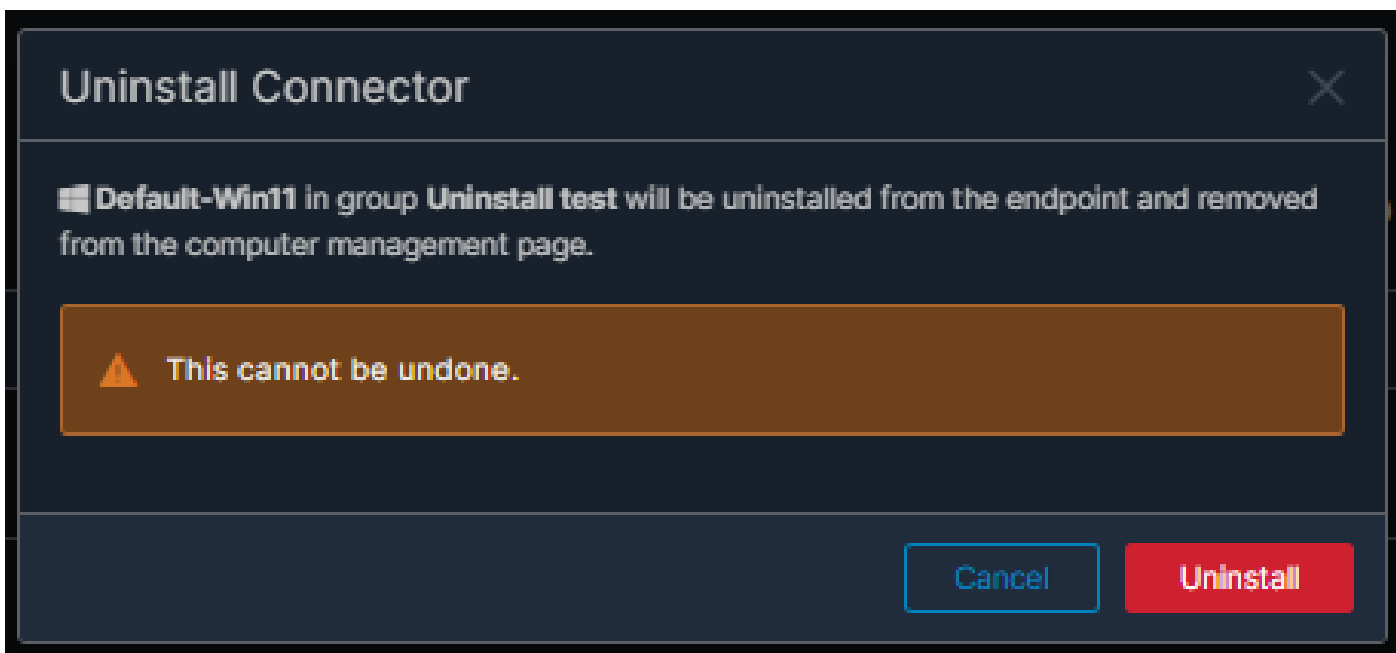
ステップ 1：コンソールで、Management > Computersの順に移動します。

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。



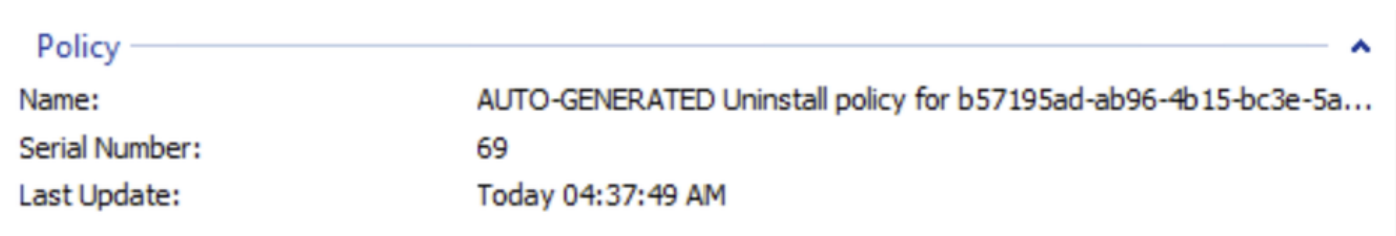
ステップ 4：操作の確認を求められたら、Uninstall をクリックします。図に示すように。

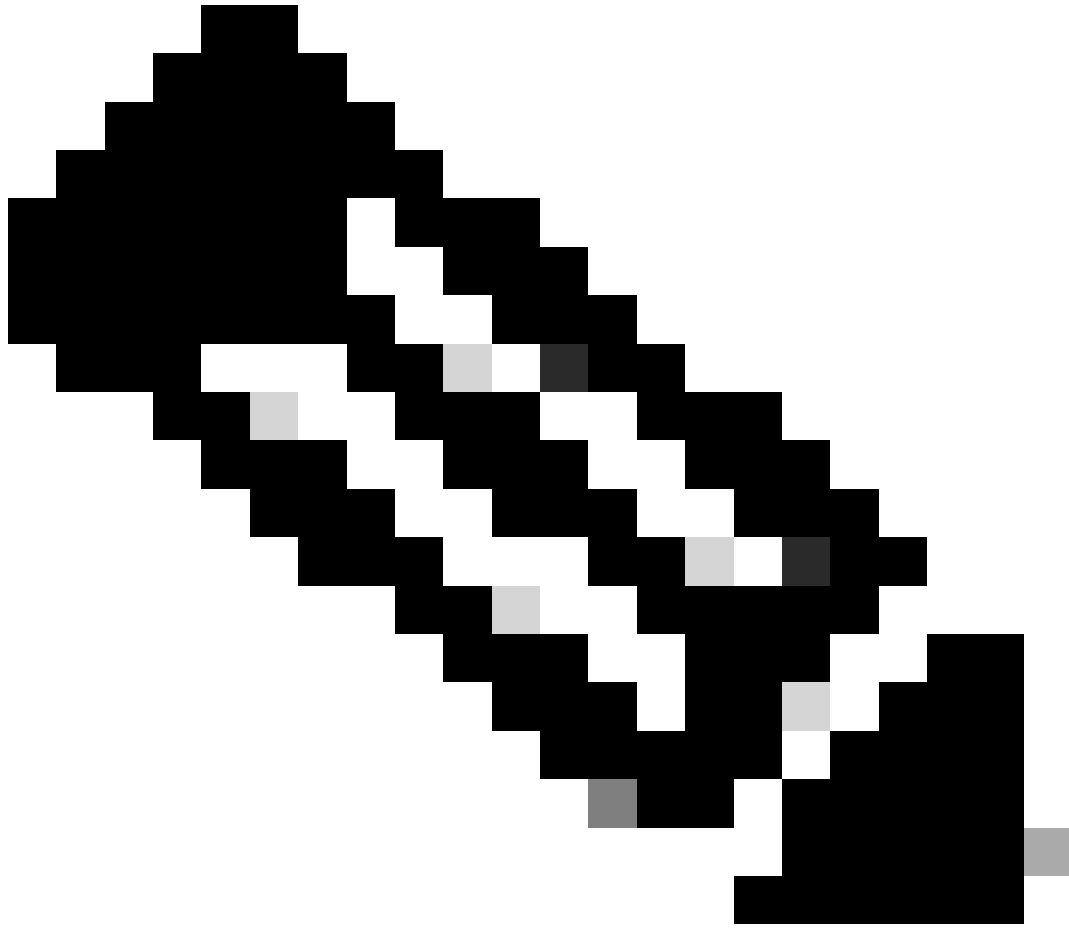


ステップ 5：セキュアエンドポイントコンソールの上部に確認メッセージが表示されます。図に示すように。

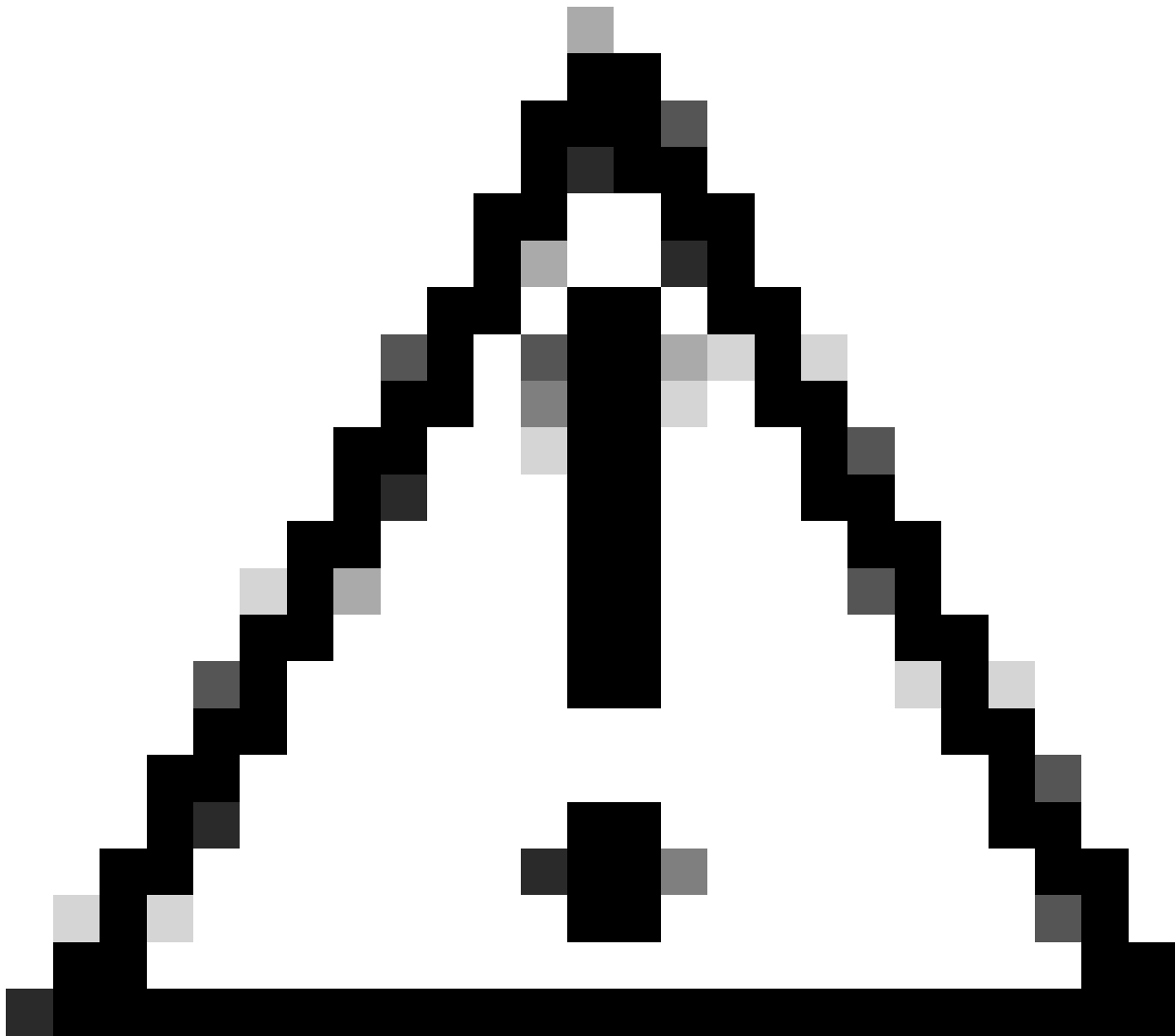


コンソールでのコネクタの登録は即座に消えます。情報をローカルで確認すると、コネクタは一時的にアンインストールポリシーに移行し、数分後にデバイスから完全に削除されます。図に示すように。

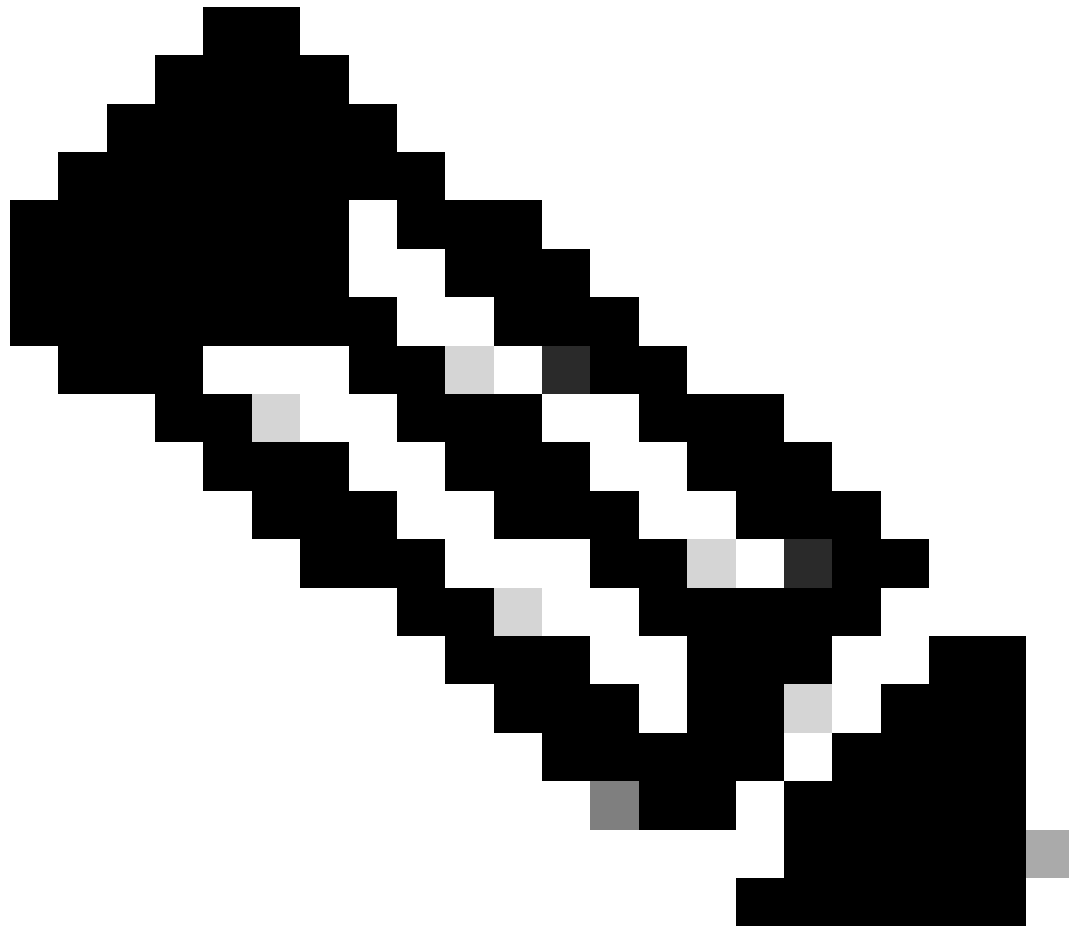




注：コネクタがこのタスクを実行するために使用する期間は、環境によって異なる可能性があることに注意してください。



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「[セキュアエンドポイントユーザガイド](#)」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、「[Secure Endpoint APIの認証](#)」を参照してください。

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。

SecureX

SecureX integration: Enabled

Disable

Name: Auto-created for Cisco - MSSP - Monsanc

GUID: 3186786e-ad75-4192-9a7d-7974075808dc3

Enable incident promotion

Yes

No

Minimum severity for incident promotion ?

Low



Low, medium, high, and critical incidents will be promoted to SecureX.

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。

Integration Modules Orchestration Insights Administration

Client Name*
Remote Uninstall Test

Client Preset
[] X v

API Clients OAuth Code Clients

Scopes* [Select None](#)

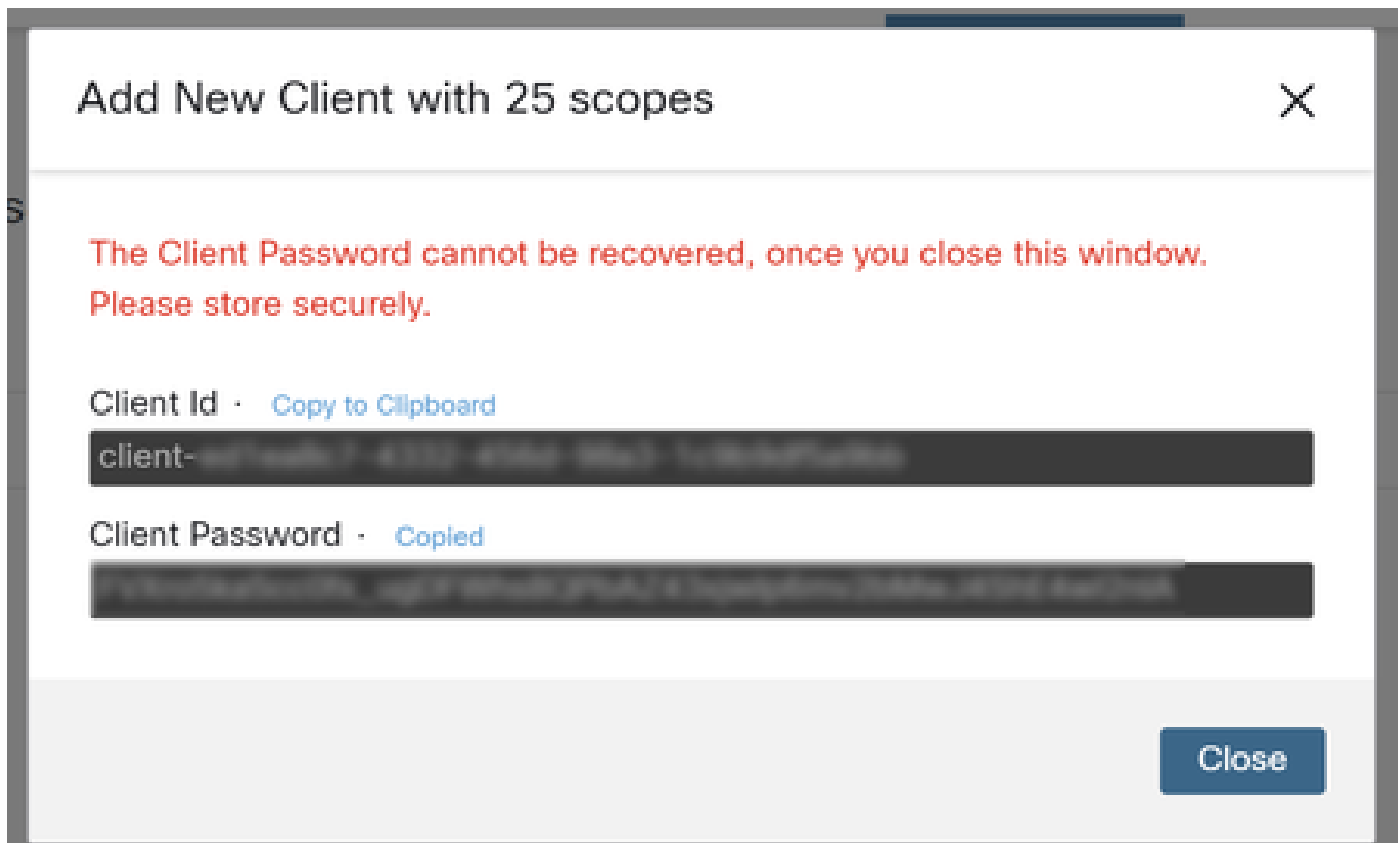
Search []

<input checked="" type="checkbox"/>	Admin	Provide admin privileges
<input checked="" type="checkbox"/>	AO	Manage and execute Automation workflows and related objects
<input checked="" type="checkbox"/>	Asset	Access and modify your assets
<input checked="" type="checkbox"/>	Casebook	Access and modify your casebooks
<input checked="" type="checkbox"/>	...	Query your configured modules for threat

Description
Test for remote uninstall 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。



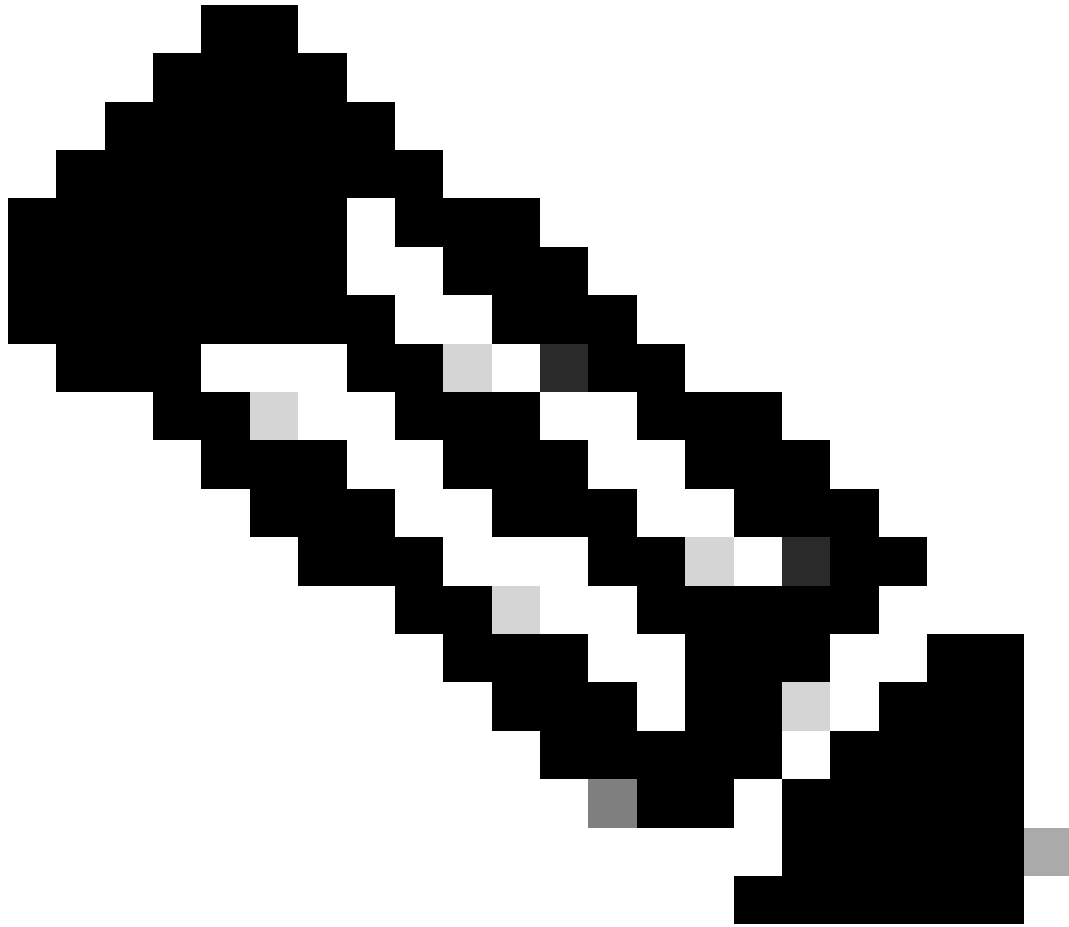
ステップ 4 : 任意のスクリプトファイルプログラムを使用して、ファイルに examples.sh(examples.shから取得)を実行します。

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。

```
Mex-Amp@Default-Win11 MINGW64 ~/Documents
$ bash uninstall.bash
client_id:
client_secret:
```

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。

```
{
  "access_token": "
}
```



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。

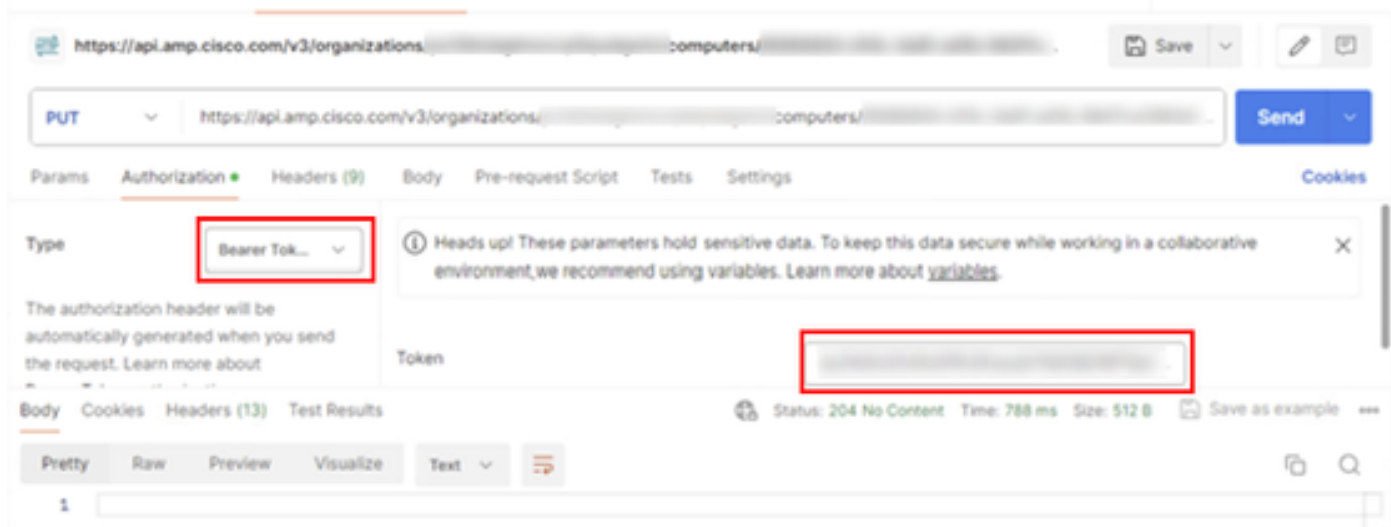
ステップ 8：API参照構文に基づく([コネクタのアンインストールの要求](#))。アンインストールするデバイスのGUIDを使用して、コネクタのアンインストール要求を行います。



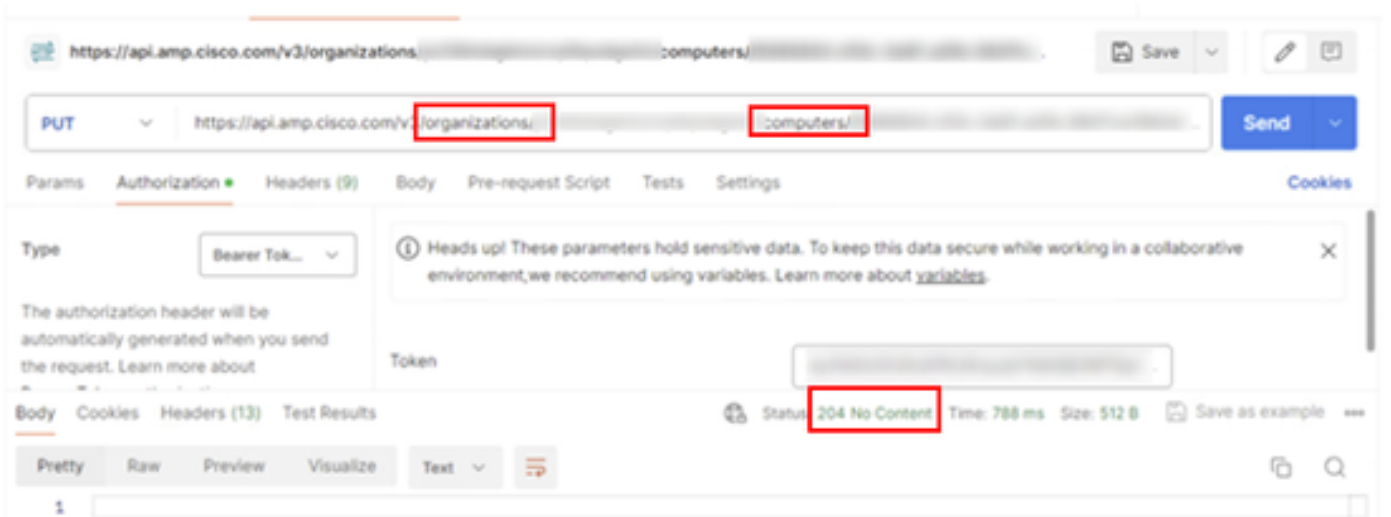
注：コネクタGUIDは、次の2つの簡単な方法で取得できます。

- 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。



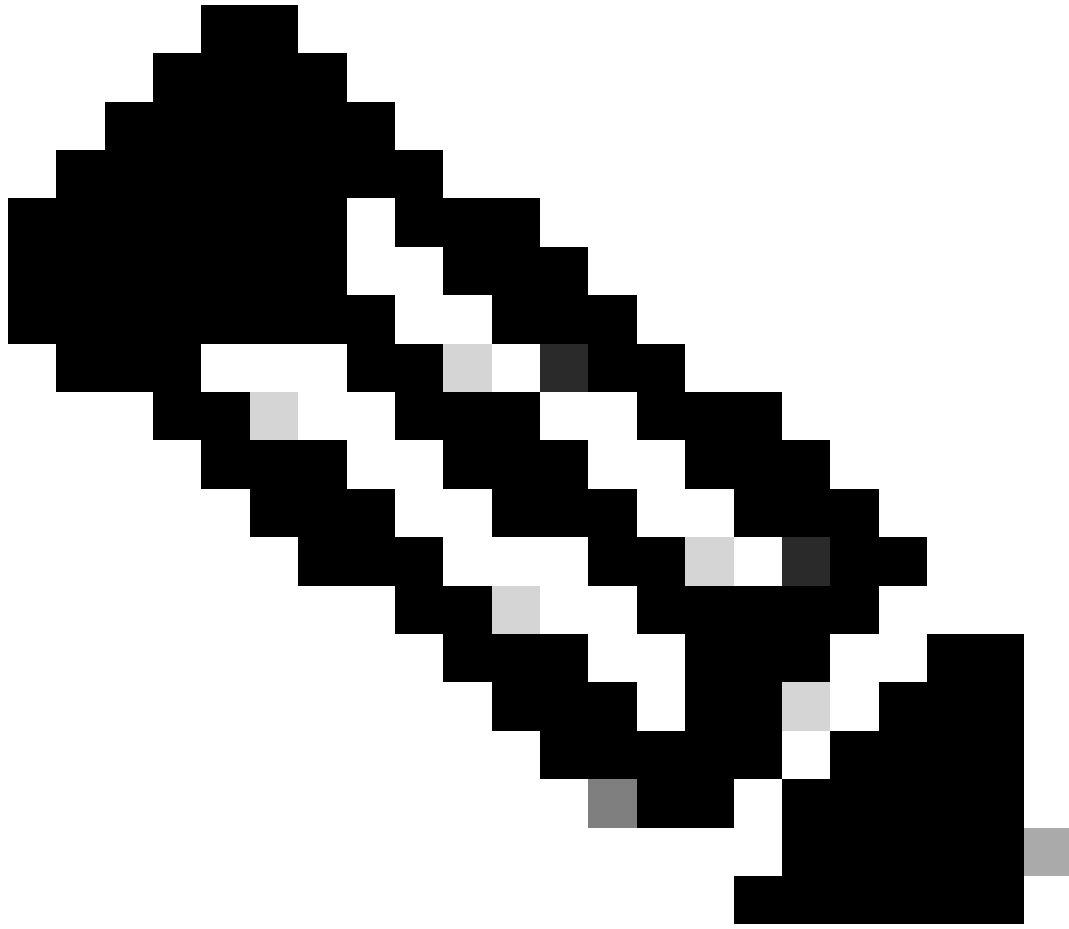
ステップ 10 : APIコールの必須フィールドに入力し、Sendボタンをクリックします。「204: No Content response」が表示されるまで待ちます。図に示すように。



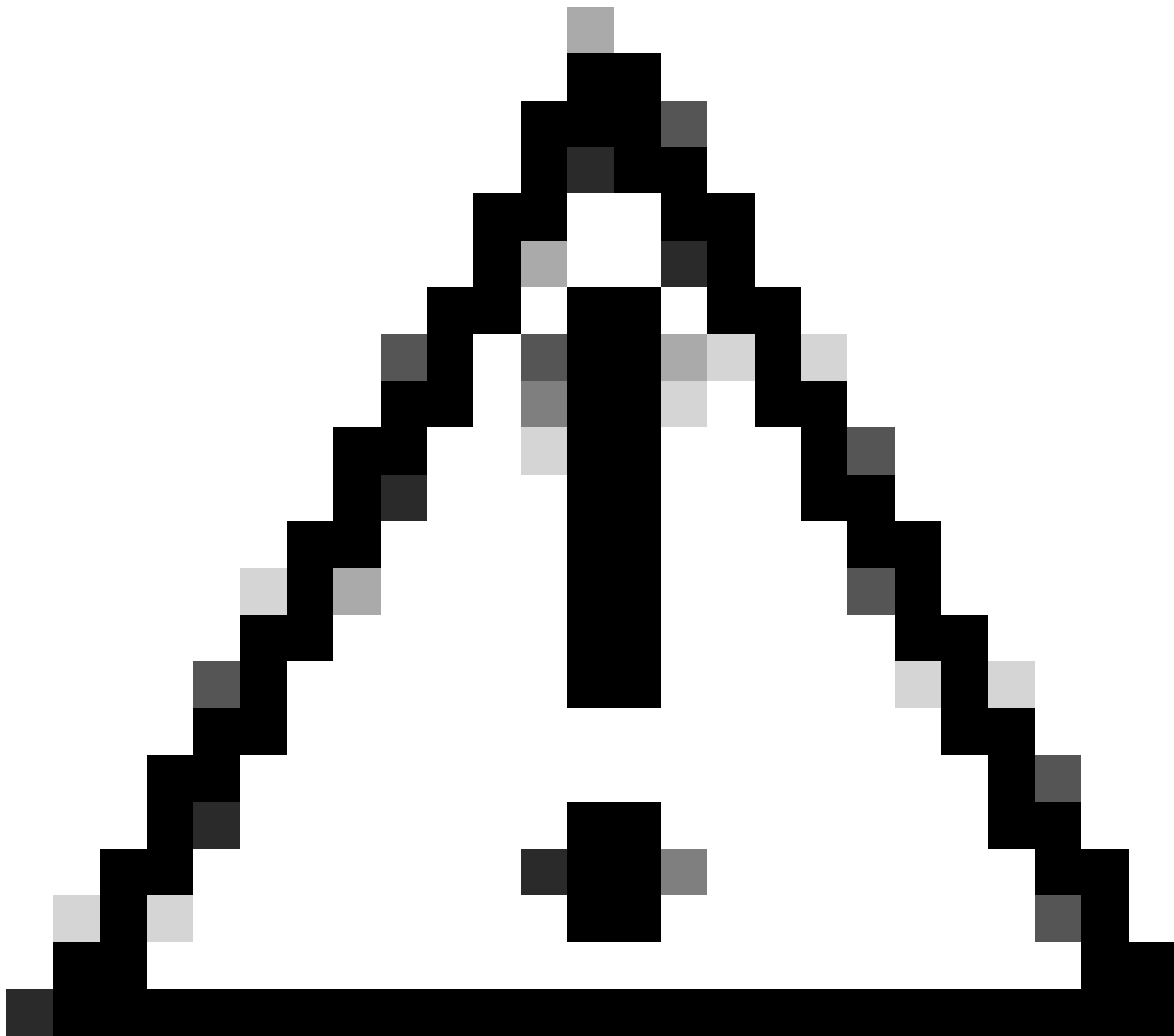
コンソールでのコネクタの登録は即座に消えます。情報をローカルで確認すると、コネクタは一時的にアンインストールポリシーに移行し、数分後にデバイスから完全に削除されます。図に示すように。

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([セキュアエンドポイント用のコマンドラインスイッチ](#)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。

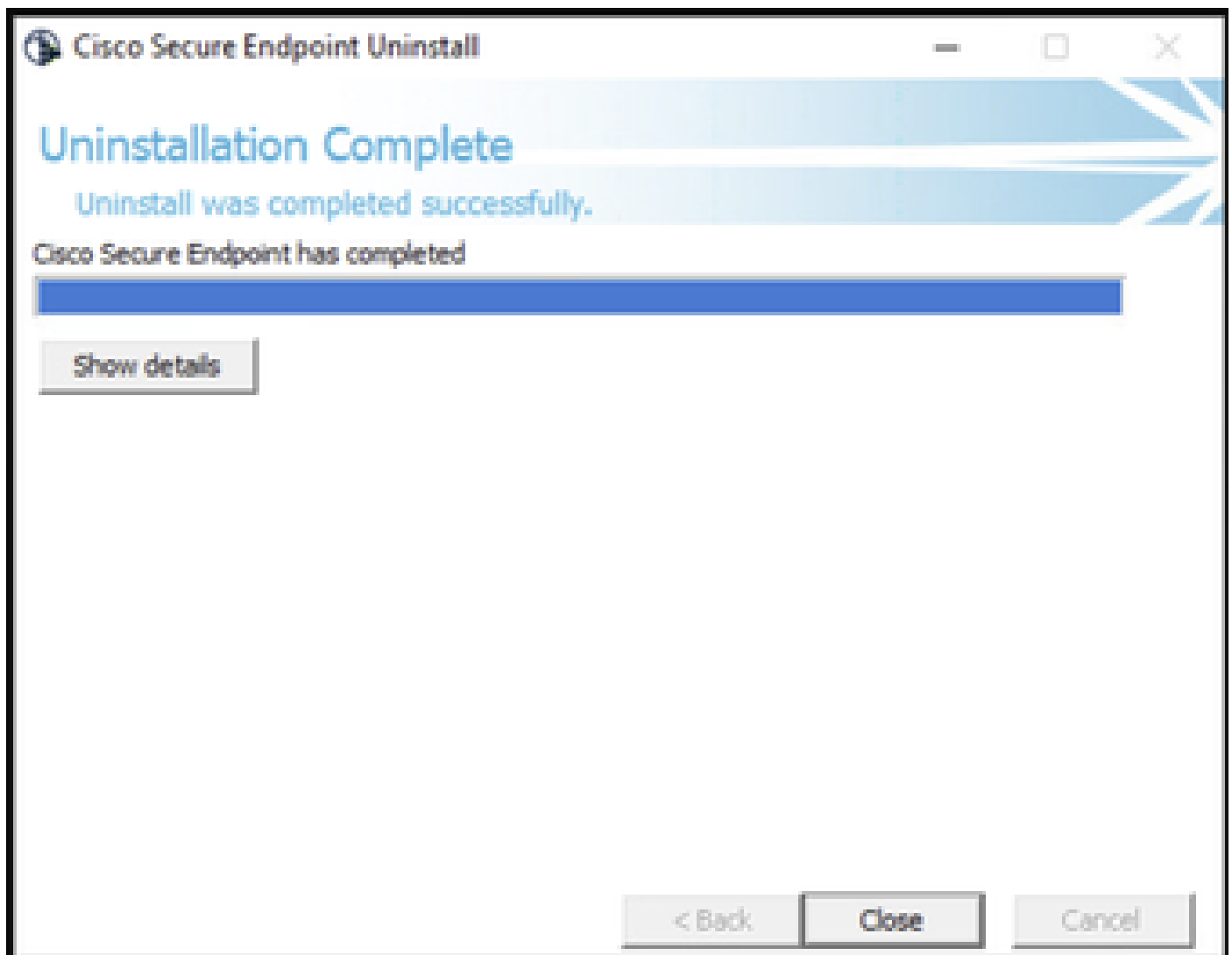
ステップ 2：インストールパッケージがある場所に移動します。図に示す例と同様です。

```
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。





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へ移動します。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\>

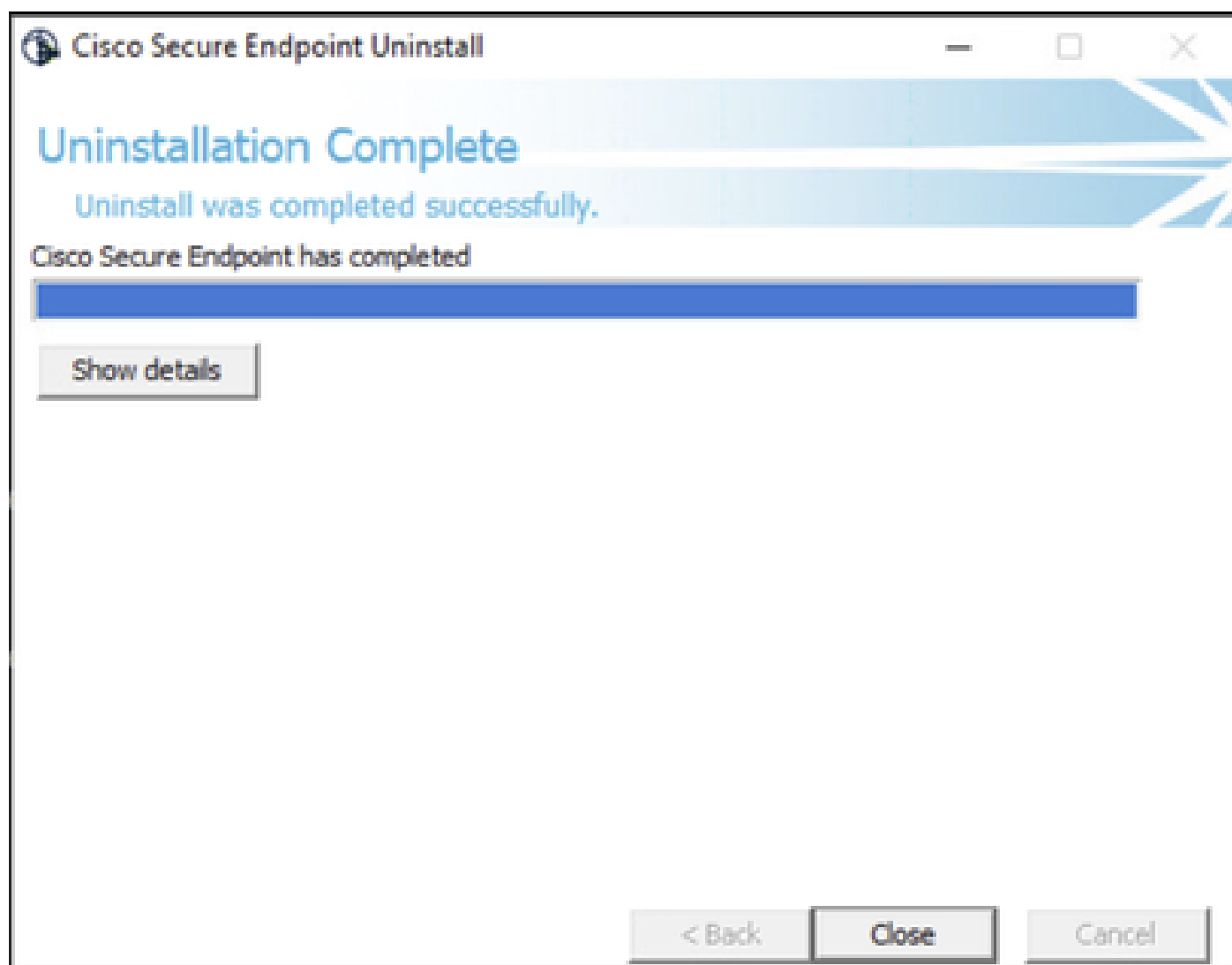
```
C:\Program Files\Cisco\AMP>cd 8.2.3.30119
```

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
```

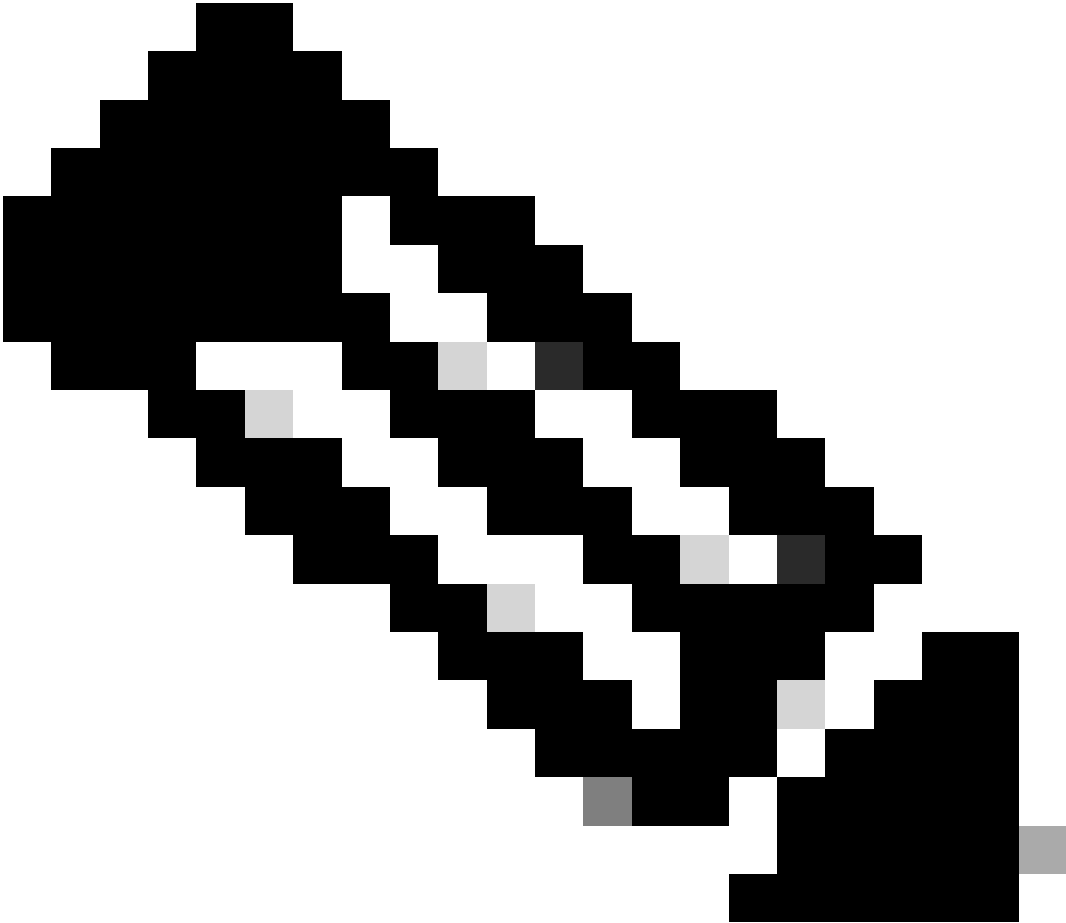
```
C:\Program Files\Cisco\AMP\8.2.3.30119>uninstall.exe/full 1
```

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。





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](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)
- [セキュアエンドポイントAPI v3](#)

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。