

Cisco Secure Endpoint : コマンドラインスイッチの説明

内容

[はじめに](#)

[背景説明](#)

[Cisco Secureエンドポイントコマンドラインスイッチ](#)

[セキュアなエンドポイントインストーラスイッチ](#)

[amp_installer.exe](#)

[セキュアエンドポイントサポート診断ツールスイッチ](#)

[ipsupporttool.exe \(登録ユーザ専用\)](#)

[セキュアエンドポイントUIスイッチ](#)

[iptraytool.exe](#)

[セキュアエンドポイントSFCスイッチ](#)

[sfc.exe \(ダウンロード\)](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco Secure Endpointで使用できるコマンドライン(CLI)スイッチについて説明します。

背景説明

Cisco Secure Endpointには、コマンドラインスイッチを使用してエンドポイントでローカルに実行できる、カスタマイズ可能な機能やアクションが多数含まれています。このドキュメントでは、それらの例を示します。

Cisco Secureエンドポイントコマンドラインスイッチ

セキュアなエンドポイントインストーラスイッチ

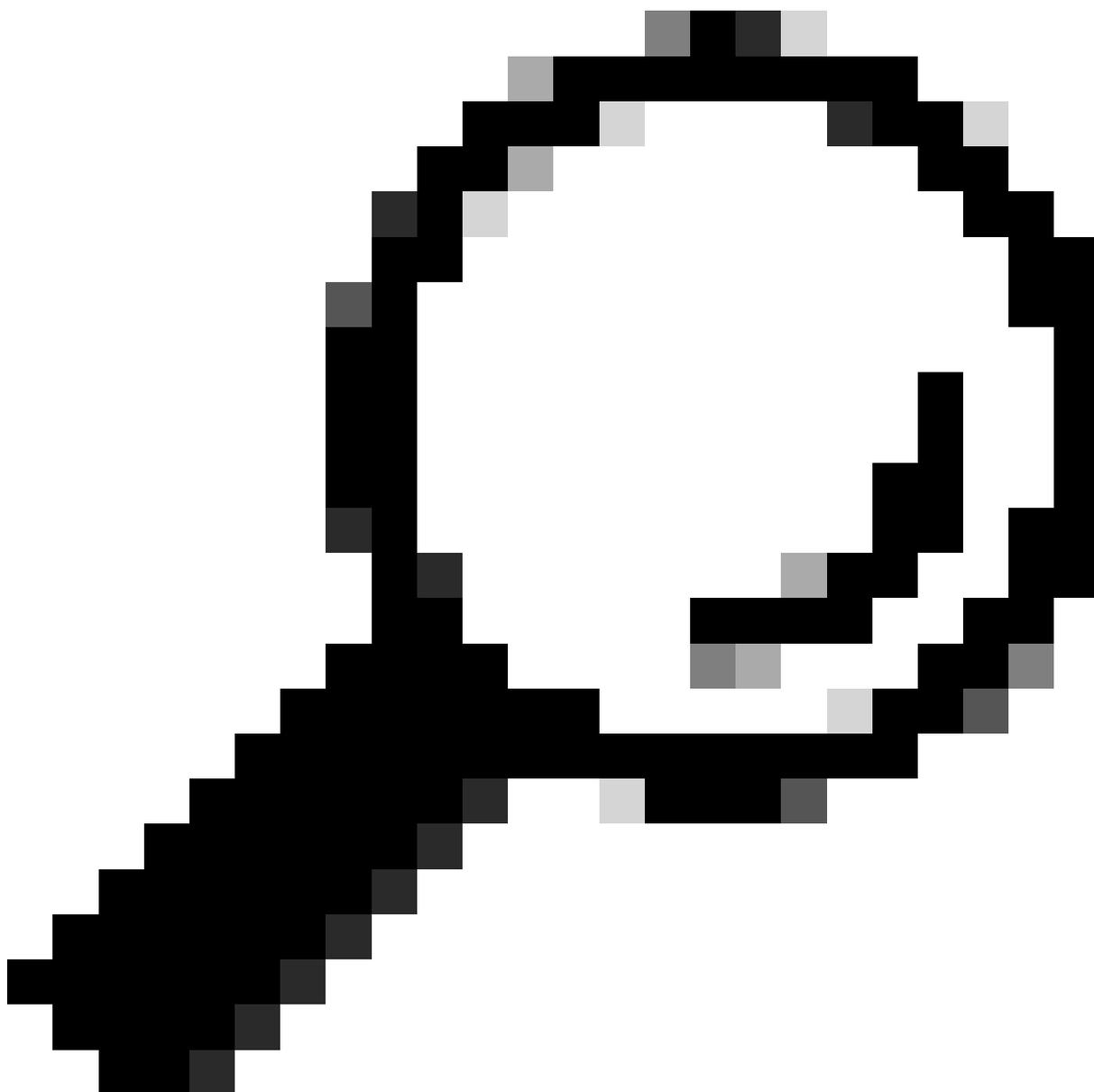
amp_installer.exe

1. Windowsでコマンドプロンプトを開きます。
2. コマンドプロンプトで、インストーラが置かれているフォルダに移動します (次の例では Downloads フォルダを使用) 。

```
cd C:\Users\sysadmin\Downloads
```

- 提供された使用可能なスイッチを実行します。
amp_protect.exe <switch>

 注：コマンドを実行しても出力は返されません。



ヒント：複数のスイッチを同時に使用できます。

コマンドライン	コマンドの説	特記事項
---------	--------	------

スイッチ	明	
/S	インストーラをサイレントモードに切り替える場合に使用します。	
/temppath	インストールファイルを抽出して実行するカスタムの一時的な場所を指定するために使用します。	/temppath C:\
/desktopicon 0	デスクトップアイコンが作成されないように指定する場合に使用します。	これはデフォルト設定であり、指定する必要はありません。
/desktopicon 1	デスクトップアイコンが作成されるように指定する場合に使用します。	
/startmenu 0	[Start] メニューのショートカットは作成されません。	
/startmenu 1	[Start] メニューのショートカットが作成されます。	これはデフォルト設定であり、指定する必要はありません。
/contextmenu 0	右クリック コ	

	<p>ンテキスト メニューの [Scan Now] が無効になります。</p>	
/contextmenu 1	<p>右クリック コンテキスト メニューの [Scan Now] が有効になります。</p>	<p>これはデフォルト設定であり、指定する必要はありません。</p>
/remove 0	<p>コネクタをアンインストールし、後で再インストールできるようにファイルを残します。</p>	<p>UUIDを持つXMLファイルはそのまま残り、コネクタを再インストールするときに既存のコンピュータオブジェクトを再利用できます。ログ・ファイルも同様に保存されます。コネクタ保護パスワードが使用中の場合は、/uninstallpasswordフラグを使用して指定する必要があります。</p>
/remove 1	<p>コネクタをアンインストールし、関連付けられたすべてのファイルを削除します。</p>	<p>コネクタ保護パスワードが使用中の場合は、/uninstallpasswordフラグを使用して指定する必要があります。</p>
/uninstallpassword	<p>/removeフラグを使用する場合のアンインストールパスワードを指定します。コネクタ保護機能を有効にする場合は、指定する必要があります</p>	<p>フラグの後にアンインストールパスワードを指定します。</p>
/skipdfc 1	<p>DFC ドライバのインストー</p>	<p>このフラグを使用してインストールされたコネクタは、ネットワークエンジンが無効になっているポリシーを持つグルー</p>

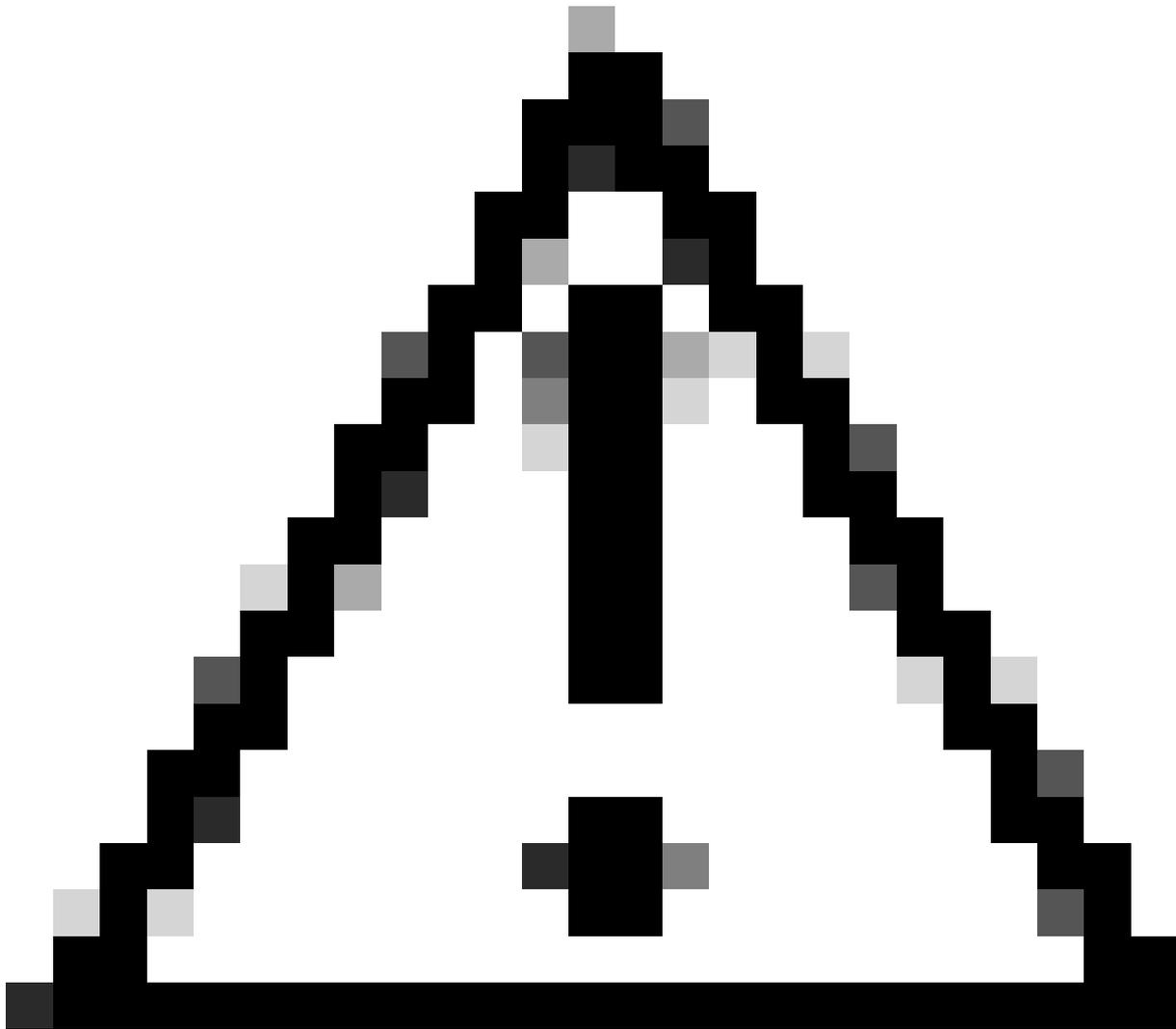
	ルをスキップします。	プに属している必要があります。
/skiptetra 1	TETRA ドライバのインストールをスキップします。	このフラグを使用してインストールされたコネクタは、Tetraフラグがオフになっているポリシーを持つグループに属している必要があります。
/D=[PATH]	インストールを実行するディレクトリを指定するために使用します。例：/D=C:\	<p>これは、最後のパラメータとして指定する必要があります。</p> <p>/D= コマンドラインスイッチのデフォルトのインストールディレクトリはオペレーティングシステムによって異なります。次に、Service Pack 3 搭載した Microsoft Windows XP のデフォルトのインストールディレクトリを示します。</p> <p>x86 プラットフォームの場合：</p> <p>C:\Program Files (x86)\Cisco\AMP</p> <p>x64 プラットフォームの場合：</p> <p>C:\Program Files\Cisco\AMP</p>
/goldenimage 1	ゴールデンイメージ用にコネクタをインストールします。	<p>このフラグは、仮想環境でゴールデンイメージを準備するのに役立つように設計されています。このフラグを使用すると、ゴールデンイメージの作成中にコネクタが開始および登録されなくなります。詳細については、以下を参照してください。</p> <p>セキュアエンドポイントでゴールデンイメージを準備する方法</p> <p>https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214462-how-to-prepare-a-golden-image-with-amp-f.html</p>
/skiposcheck 1	インストール中にOSチェックをスキップします。	このフラグは、互換性のないオペレーティングシステムにセキュアエンドポイントをインストールするために使用できません。

セキュアエンドポイントサポート 診断ツールスイッチ

ipsupporttool.exe (登録ユーザ専用)

- Windowsでコマンドプロンプトを開きます。
- コマンドプロンプトでフォルダに移動します。デフォルトパス : `C:\Program Files\Cisco\AMP\X.X.X\`。X.X.Xはバージョン番号を示します。
`cd C:\Program Files\Cisco\AMP\8.2.1.21612\`
- 提供された使用可能なスイッチを実行します。
`ipsupporttool.exe <switch>`

 注 : スイッチを実行しても、出力は返されません。



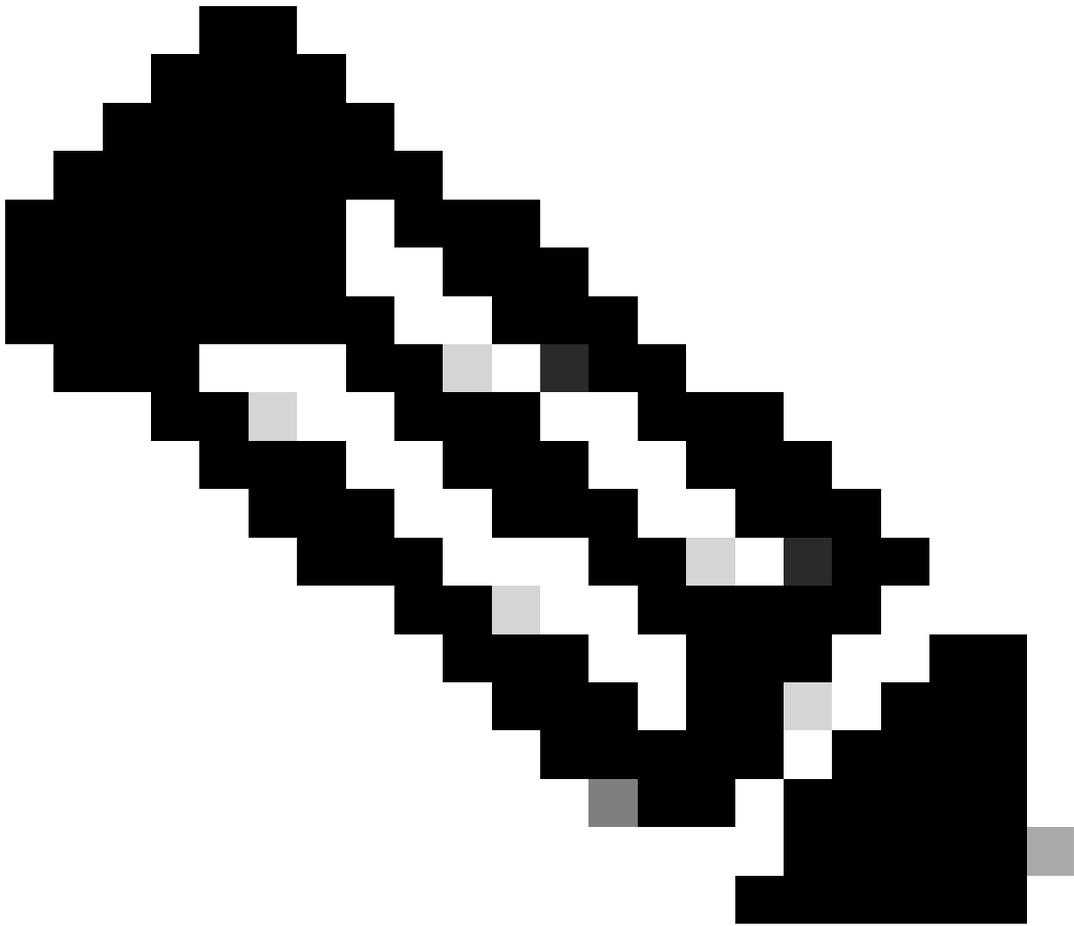
注意：フォルダ選択を参照するスイッチには、そのフォルダがすでに存在している必要があります。

コマンドラインスイッチ	コマンドの説明	特記事項
-o <パス>	サポートツールの出力フォルダを指定します。	このオプションが指定されていない場合は、デフォルトでデスクトップが使用されます。
-d <install_path>	Windowsサポートツールがファイルを取得できるフォルダを指定します。	指定しない場合は、既定でSecure Endpointの既定のインストールディレクトリが使用されます。

-t <分>	Windowsサポートツールから指定された時間、時間制限デバッグレベル診断を実行します。期間は分単位で指定します。	
--------	---	--

セキュアエンドポイントUIスイッチ

iptraytool.exe



注：iptraytool.exeファイルは、Secure Endpointのレガシーバージョンでのみ使用できます。

- Windowsでコマンドプロンプトを開きます。
- コマンドプロンプトでフォルダに移動します。デフォルトパス：C:\Program Files\Cisco\AMP\X.X.X\。X.X.Xはバージョン番号を表します。
cd C:\Program Files\Cisco\AMP\7.5.3.20938\
- 提供された使用可能なスイッチを実行します。
iptray.exe <switch>

コマンドラインスイッチ	コマンドの説明	特記事項
-f	クライアント・ユーザー・インタフェースをコマンド・ラインからアクティブにできます。	これは、エンドポイントでStart Client User Interfaceがオフの状態、ポリシーを介してGUIがオフになっている場合にのみ必要です。

セキュアエンドポイントSFCスイッチ

sfc.exe (ダウンロード)

- Windowsでコマンドプロンプトを開きます。
- コマンドプロンプトでフォルダに移動します。デフォルトパス：C:\Program Files\Cisco\AMP\X.X.X\。X.X.Xはバージョン番号を表します。
cd C:\Program Files\Cisco\AMP\8.2.1.21612\
- 提供された利用可能なスイッチを実行します。
sfc.exe <switch>

コマンドラインスイッチ	コマンドの説明	特記事項
-s	Immunet Protect (Windows Connector)サービスを開始します。サービスを開始するには、SCMにサービスがすでに登録されている必要があります。	

	す。	
-k	Immunet Protect (Windows Connector)サービスを停止します。	Connector Protectionが有効になっている場合は、サービスを正常に停止するために、-kの後にパスワードを入力します。
-u	Immunet Protect (Windows Connector)サービスをアンインストールします。Windows Service Control Manager(SCM)でサービスの登録を解除します。このオプションは、Windowsコネクタサービスをアンインストールするためにデインストーラによって使用されます。	
-r	Immunet Protect (Windows Connector)サービスをリセットします。これは-iオプションに非常によく似ていますが、サービスをインストールしません。これは、local.xmlの破損を修正するのに役立ちます。	
-l開始	デバッグとカーネルのロギングを動的に切り替えます(トリガーは小文字のLです)。	この状態は、オフに切り替えられるか、サービスが再起動されるか、ログレベルを変更するために新しいポリシーが設定されるまで続きます。
-l停止	デバッグとカーネルのロギングを動的にオフにします(トリガーは小文字のLです)。	
-SHA_of_fileのブロックを解除	このオプションは、プロセスの実行のブロックを解除します。このコマンドスイッチの実行後、アプリケーションはアプリケーションブロッキングリストのローカルカーネルキャッシュから削除されます。	このコマンドは、誤検出または誤りによってアプリケーションがブロックされた場合に、30分待ったりマシンを再起動したりすることなく、アプリケーションのブロックを迅速に解除したい場合に使用できます。
-再登録	このオプションを使用すると、サービスの実行中にlocal.xmlとレジストリからuuidと証明書をクリアし、再登録をトリガーできます。Local.xmlとレジストリが新しい値で更	コネクタ保護が有効になっている場合は、次のコマンドを入力する必要があります。 sfc.exe -reregister _password_

	<p>新されます。ただし、ID同期が有効になっていて、コネクタが既存のUUIDを再度取得する場合、これはブロックされます。これにより、初期インストールに使用されるインストールパッケージが変更された場合、再登録後にコネクタをデフォルトのグループ/ポリシーに配置できません。</p>	
-forceupdate	<p>このオプションは、コネクタにTETRA定義を強制的に更新させます。</p>	
-forceapdeupdate	<p>このオプションを選択すると、コネクタは動作保護定義を更新します。</p>	<p>セキュアエンドポイントダッシュボードのデバイスラジェクトリーで、エンドポイントにインストールされている現在の動作保護定義を確認できます。</p>

関連情報

- [テクニカル サポートとドキュメント - Cisco Systems](#)
- [Cisco Secure Endpoint – テクニカルノート](#)
- [Cisco Secure Endpoint – ユーザガイド](#)
- [セキュアエンドポイントMac/Linux CLIの使用](#)

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。