# Secure Endpoint for Windowsデバイスのデバッ グログファイルの収集

# 内容

概要 <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>背景説明</u> <u>Cisco Secure Endpoint for Windowsのデバッグログファイルの収集</u> <u>バージョン7.5.5以前</u> <u>バージョン8.0.1以降(Cisco Secure Client)</u>

### 概要

このドキュメントでは、Cisco Secure Endpoint Connectorからデバッグバンドルファイルを生成 する手順について説明します。

著者: Cisco TACエンジニア、Javi Martinez

# 前提条件

#### 要件

Cisco Secure Endpoint Connectorに関する知識があることが推奨されます。

#### 使用するコンポーネント

このドキュメントで使用する情報は、次のソフトウェアバージョンに基づいています。

- Microsoft Windowsオペレーションシステム
- Cisco Secure Endpoint Connector 6.3.7以降

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、初期(デフォルト)設定の状態から起動しています 。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

Microsoft Windows Operative SystemのCisco Secure Endpoint Connectorでパフォーマンスの問題が発生した場合は、Cisco Technical Assistance Center(TAC)に連絡してください。 Ciscoテク ニカルサポートエンジニアは、デバッグバンドルファイルで利用可能なログを分析して、根本的 な問題を見つけます。

**注**: デバイスをリブートした場合、IPトレイインターフェイスからデバッグモードを有効 にしても、リブート後は有効になりません。リブートの場合は、セキュアエンドポイントコ ンソールのポリシー設定からデバッグモードを有効にできます。

# Cisco Secure Endpoint for Windowsのデバッグログファイルの収 集

バージョン7.5.5以前

ステップ1:タスクバーの**トレイアイコン**を使用して、図に示すように[Open Cisco Secure Endpoint] を選択します。

	Open Cisco Secure Endpoint				
	Presentation Mode Start FlashScan				
	Hide Tray Icon				
→ 48°F Clear へ 空 <sup>(1)</sup> LAA	へ 聖 (小)) ENG 2:16 PM し LAA 4/21/2020 い				

ステップ2:図に示すように、セキュアエンドポイントコネクタで[Settings] オプションを選択します。

Secure Endpoir Scanning	nt
History	
Settings	
Status: Connected Scanned: Never Policy: Isolation: Not Isolated	About

ステップ3:[Settings] に移動し、図に示すように[Cisco Secure Endpoint Connector Settings] メニ ューを選択します。

Wildcard Exclusions: C:\\WINDOWS\\Security\\databa C:\\WINDOWS\\Security\\databa C:\\WINDOWS\\Security\\databa C:\\WINDOWS\\Security\\databa C:\\WINDOWS\\Security\\databa C:\\WINDOWS\\Security\\databa	ise\\.*\.chk ise\\.*\.edb ise\\.*\.jrs ise\\.*\.log ise\\.*\.sdb tion\\Datastore	e\\Logs\\.*\.log		
Scan Settings	T			
Notification Settings	•			
Proxy Settings				
Cisco Secure Endpoint Settings				
	Up	date TETRA S	Sync Policy	Close

ステップ4:図に示すように、[Enable Debug Logging] ボタンを選択します。



ステップ4.1:ボタン名が[Disable Debug Logging] に変更されます。これで、図に示すように、 **デバッグモード**になります。



ステップ5:問題を再作成し、デバイスで少なくとも30分間実行します。

ステップ6:30分後にWindowsの検索を開き、**サポート診断ツール**を記述すると、診断ツールが表示されます。次の図に示すように、**管理者**権限でツールを実行します。



**注**: Secure Endpoint Connector v7.5.5からは、デバッグログを収集するためにサポート診 断ツールを開く際に、管理者権限を持つWindowsアカウントは必要ありません。<u>リリース</u> ノート:「サポート診断ツールを更新し、管理者特権を必要としないようにします。」

ステップ7:図に示すように、一時的なWindowsの黒い画面が表示されます。 (数秒待つと、Windowsの黒い画面が自動的に閉じられます)。



ステップ8:図に示すように、数分後に**デバッグバンドル**ファイルがデスクトップに表示されます



0

ステップ9:**Debug Bundle**ファイルを生成したら、**デバッグモード**を無効にできます。図に示すように、[Disable Debug Logging] ボタンを選択します。



ステップ9.1:図に示すように、ボタン名が[Enable Debug Logging] に変更されます。



**注:デバッグ**モードは、デバッグバンドルファイルを収集するためだけに有効にする必要が あります。デバッグモードを長時間有効にすると、ディスク領域がいっぱいになる可能性が あります。

ステップ10:デバッグバンドルファイルを収集したら、<u>https://cway.cisco.com/csc/</u>にアップロー ドします。

**注:サー**ビス要求番号を参照してください。

#### バージョン8.0.1以降(Cisco Secure Client)

ステップ1:図に示すように、タスクバーのトレイアイコンを起動します。



ステップ2:図に示すように、セキュアエンドポイントコネクタで[Advance Window] オプション を選択します。

- [	🕲 Cisco Secu	ire Client	<del></del>		×
		Secure Endpoint: Connected. Flash Scan	~	Start	
⇒[	<b>‡</b> (1)				altath cisco
	Advanced	Window			

ステップ3:[Advanced] タブに移動し、図に示すように[Enable Debug Logging] ボタンを選択します。

Sisco Secure Client		00-00	×
cisco Se	cure Client		()
Secure Endpoint			
Statistics Update Advanced			
Debug Logging:	Stopped		
	Enable Debug Logging		
200			100

ステップ4:デバッグログボタンの名前が「Started」に変わります。 次の図に示すように、デバッグモードになります。

S Cisco Secure Client	-	<del>2</del> 8	×
Secure Client			0
Secure Endpoint Statistics Update Advanced			
Debug Logging: Started			

ステップ5:問題を再作成し、デバイスで少なくとも30分間実行します。

ステップ6:30分後に、WindowsのSearch and write Support Diagnostic Toolを開きます。

•診断ツールが表示されます。Administrator権限でツールを実行します。

(一時的なWindowsの黒い画面が表示され、数秒待つと、Windowsの黒い画面が自動的に閉じら れます)。

•数分後、次の図に示すように、デバッグバンドルファイルがデスクトップに表示されます。



ステップ7:デバッグバンドルファイルを生成した後、デバッグモードを無効にできます。 [Disable Debug Logging] ボタンを選択します。図に示すように、デバッグログボタンの名前が「 **Stopped**」に変わります。

Sisco Secure Client			×
cisco	Secure Client		1
Secure Endpoint Statistics Update Ad	Ivanced		
Debug Logging:	Stopped		
	Enable Debug Logging		

**注:デバッグ**モードは、デバッグバンドルファイルを収集するためだけに有効にする必要が あります。デバッグモードを長時間有効にすると、ディスク領域がいっぱいになる可能性が あります。

ステップ8:デバッグバンドルファイルを収集したら、<u>https://cway.cisco.com/csc/</u>にアップロー ドします。

**注:サー**ビス要求番号を参照してください。

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。