Cisco Secure Endpoint Connector for Mac Diagnostic Data Collection

内容

概要

このドキュメントでは、Cisco Secure Endpoint Macコネクタで使用可能なサポートツールアプリケーションを介して診断ファイルを生成するために使用されるプロセスと、パフォーマンスの問題のトラブルシューティング方法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Macコネクタ
- MacOS

使用するコンポーネント

このドキュメントの情報は、Secure Endpoint Macコネクタに基づくものです。

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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

Secure Endpoint Macコネクタには、Support Toolと呼ばれるアプリケーションがパッケージされています。このアプリケーションは、Macにインストールされているコネクタに関する診断情報を生成するために使用されます。診断データには、Mac に関する次のような情報が含まれます。

- リソース使用率（ディスク、CPU、メモリ）
- コネクタ固有のログ
- コネクタ設定情報

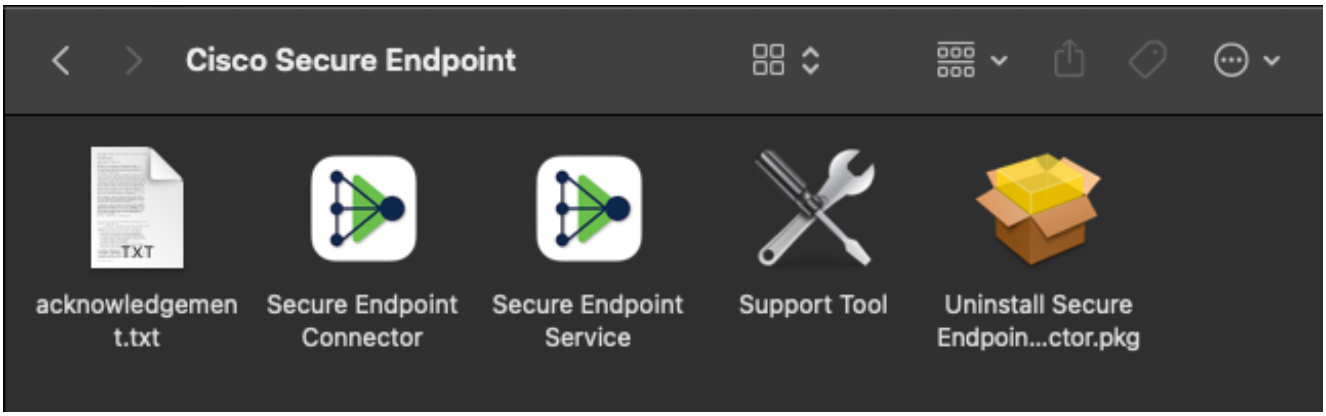
サポート ツールを使用した診断ファイルの生成

このセクションでは、診断ファイルを生成するために GUI または CLI からサポート ツール アプリケーションを起動する方法について説明します。

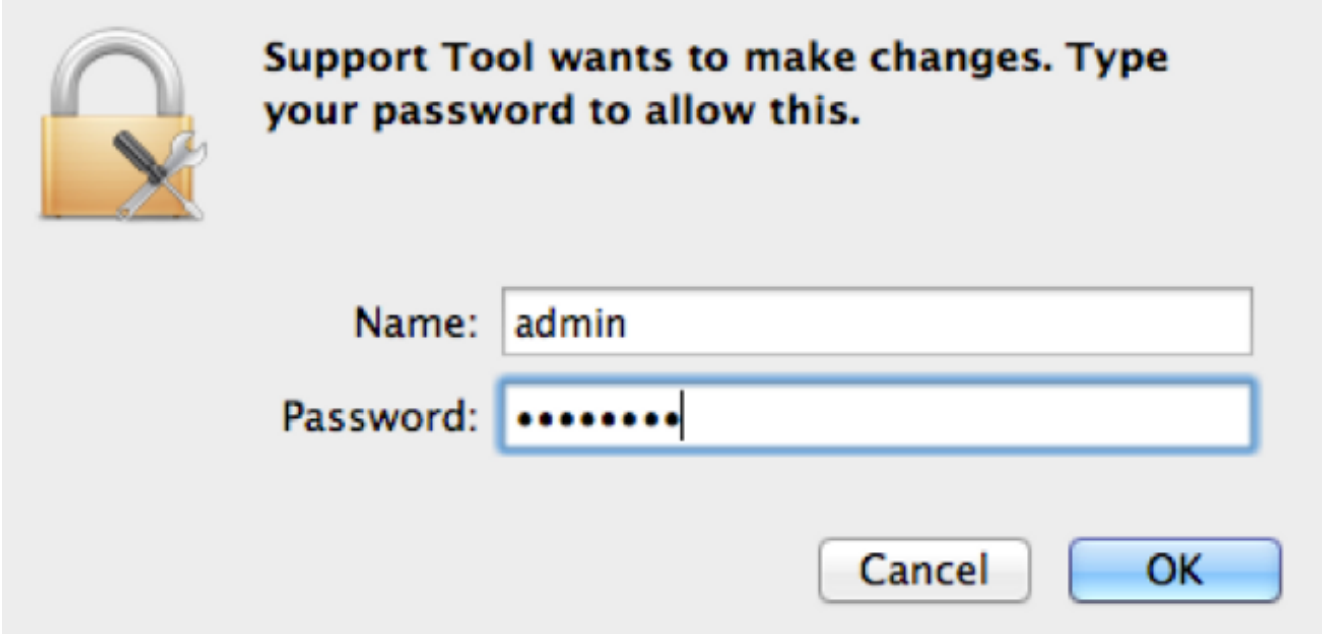
macOS Finderを使用したサポートツールの起動

macOS Finderを使用してセキュアエンドポイントMacコネクタサポートツールを起動するには、次の手順を実行します。

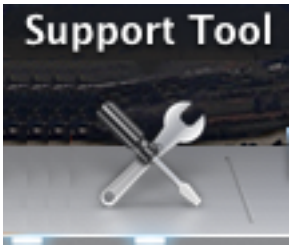
1. アプリケーションフォルダ内のCisco Secure Endpointディレクトリに移動し、サポートツールランチャを見つけます。



2. サポート ツール ランチャをダブルクリックすると、管理者のクレデンシャルを入力するように求められます。

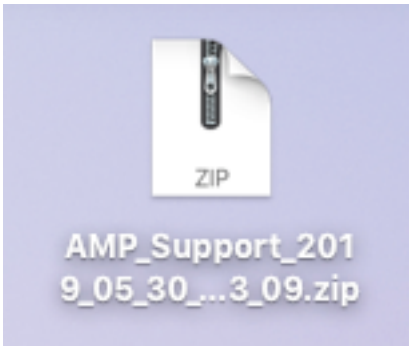


3. クレデンシャルを入力すると、ドックにサポート ツール アイコンが表示されます。

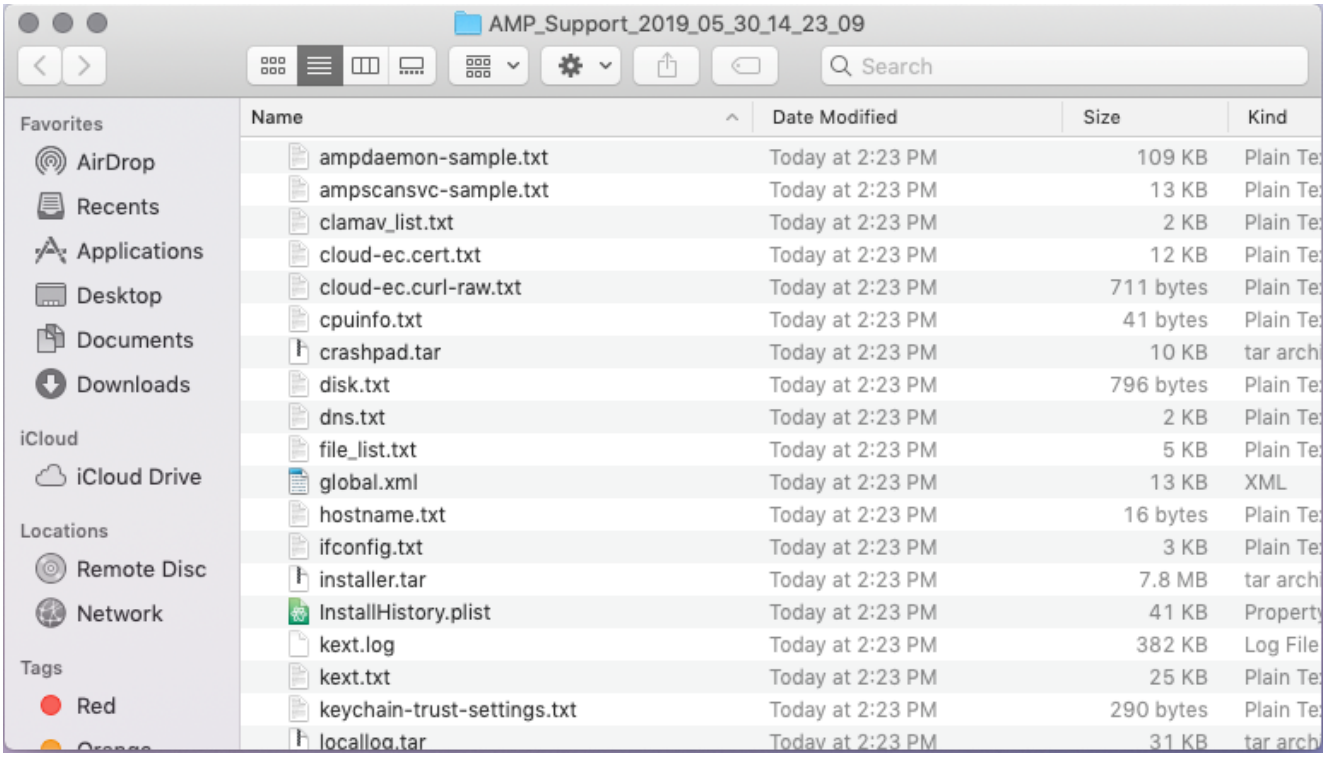


注：サポート ツール アプリケーションがバックグラウンドで実行され、完了するまでしばらく時間がかかります (約 20 ~ 30 分) 。

4. サポート ツール アプリケーションが完了すると、ファイルが生成され、デスクトップに配置されます。



次に、非圧縮出力の例を示します。



5. データを分析するために、シスコ テクニカル サポート チームにこのファイルを提供します。

macOS端末を使用したサポートツールの起動

サポート ツール ランチャは次のディレクトリ内にあります。

```
/Library/Application Support/Cisco/AMP for Endpoints Connector/
```

サポートツールアプリケーションを起動するには、次のコマンドを入力します。

> **注**：このコマンドはルートとして実行する必要があるため、ルートに切り替えるか、コマンドの前に **sudo** と入力します。

```
root@mac# cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector root@mac#
./SupportTool
```

> **注：このコマンドの実行は長時間かかります。これが完了すると、診断ファイルが生成され、デスクトップに配置されます。**

トラブルシューティング

このセクションでは、パフォーマンスの問題をトラブルシューティングするために、セキュアエンドポイントMacコネクタでデバッグモードを有効または無効にする方法について説明します。

デバッグ モードの有効化

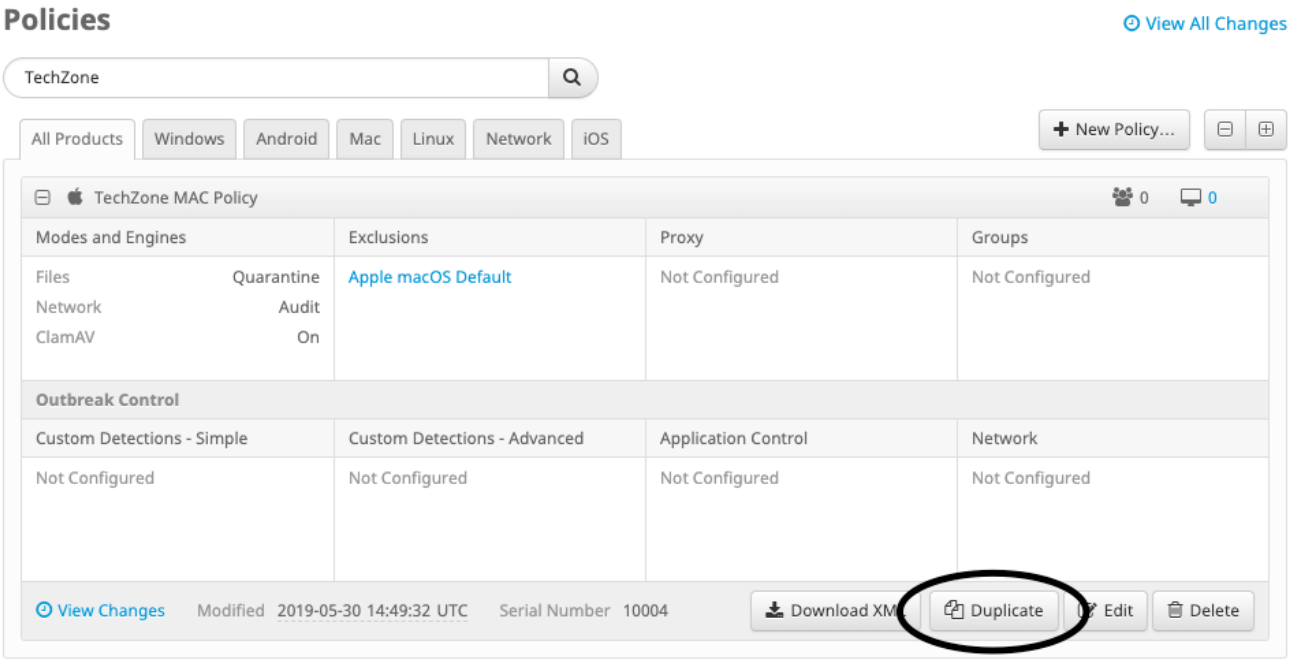
> **警告**：デバッグモードは、Ciscoテクニカルサポートのエンジニアがこのデータを要求した

場合にのみ有効にしてください。デバッグ モードを長時間にわたって有効にしておくと、ディスク スペースがすぐに占有され、ファイル サイズの超過が原因で Connector Log データと Tray Log データをサポート診断ファイルに収集できなくなる可能性があります。

デバッグモードは、セキュアエンドポイントコネクタのパフォーマンスの問題をトラブルシューティングする場合に便利です。デバッグモードを有効にして診断データを収集するには、次の手順を実行します。

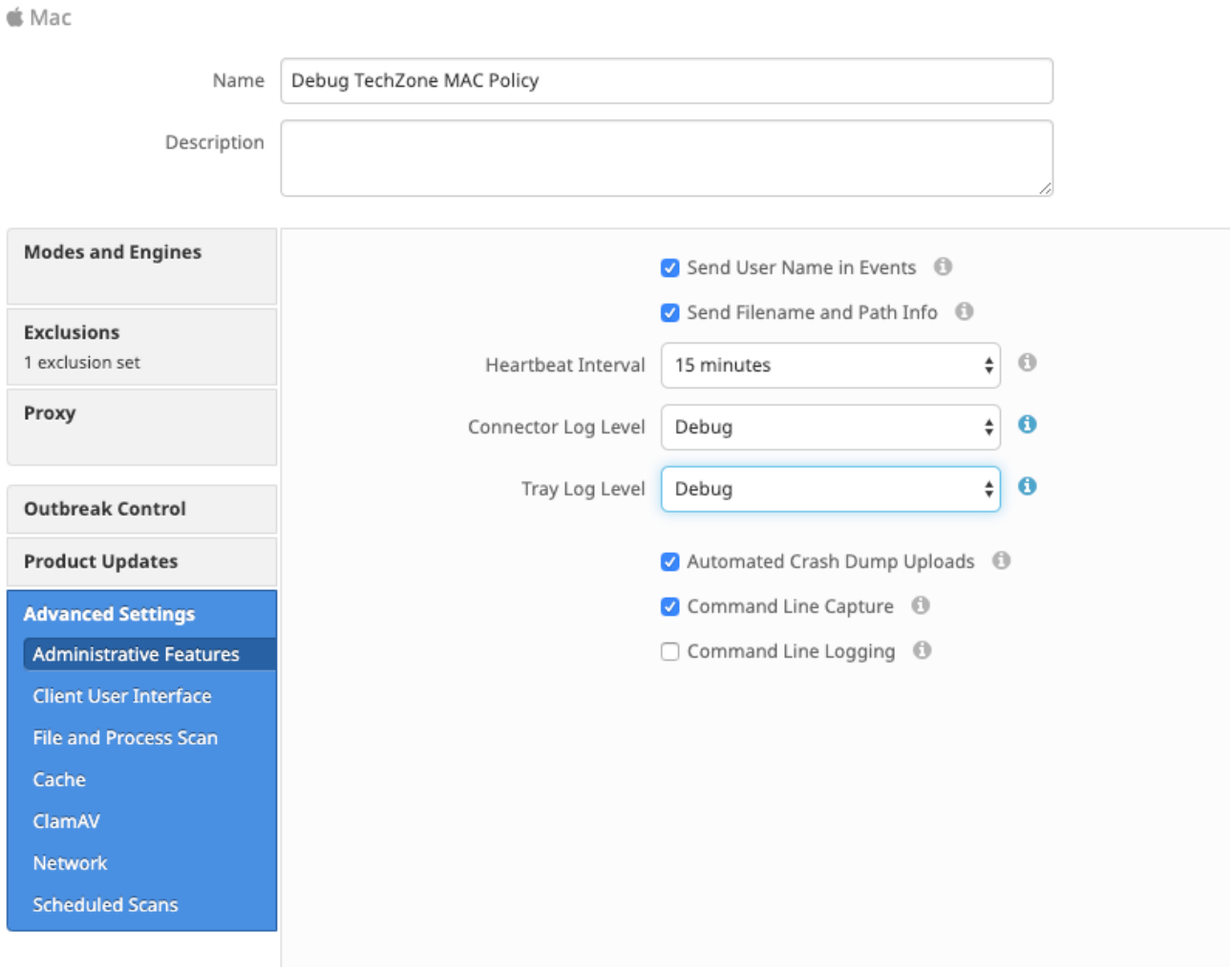
1. セキュアエンドポイントコンソールにログインします。
2. [Management] > [Policies] に移動します。

3. コンピュータに適用されているポリシーを見つけて、ポリシーウィンドウを展開するポリシーをクリックし、 **重複**.セキュアエンドポイントコンソールが複製されたポリシーで更新されます。

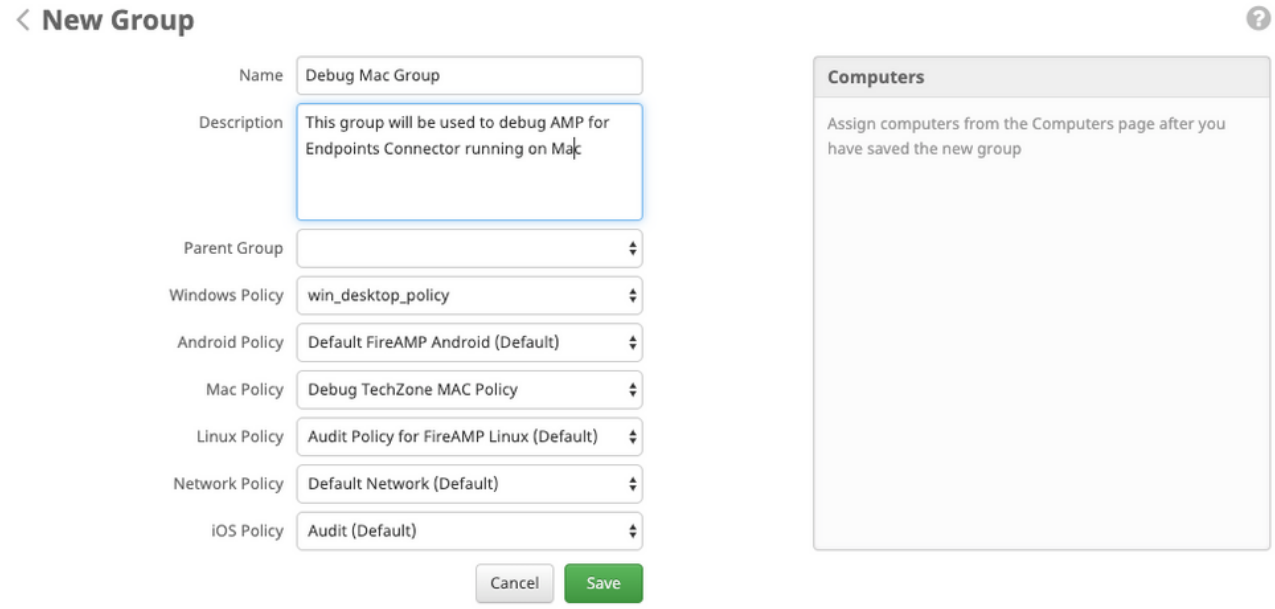


4. [duplicate policy]ウィンドウを選択して展開し、 **編集** ポリシーの名前を変更します。たとえば、 *TechZone MACポリシーのデバッグ*.

5. クリック **高度な設定**、選択 **管理機能** をクリックし、 **デバッグ** [コネクタのログレベル(Connector Log Level)]と[トレイログレベル(Tray Log Level)]の両方のドロップダウンメニューについて、次の手順を実行します。



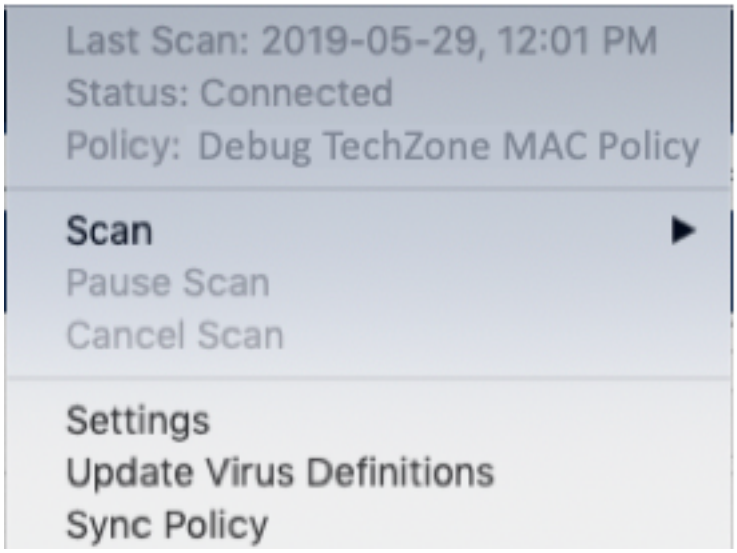
6. ポリシーの横の [レポート（Report）] **保存します。** ボタンをクリックします。
7. 移動先 **Management > Groups** をクリックし、 **グループの作成** 画面の右上付近に表示されます。
8. グループの名前を入力します。たとえば、*Debug TechZone Mac Group*を使用できます。



9. Macポリシーの変更元 *デフォルトMacポリシー* 作成したばかりの複製された新しいポリシーに対して、 **Debug TechZone Mac Policy** この例の場合は.クリック **保存します。**.
10. 移動先 **Management > Computers** リストでコンピュータを特定します。これを選択し、

グループに移動...

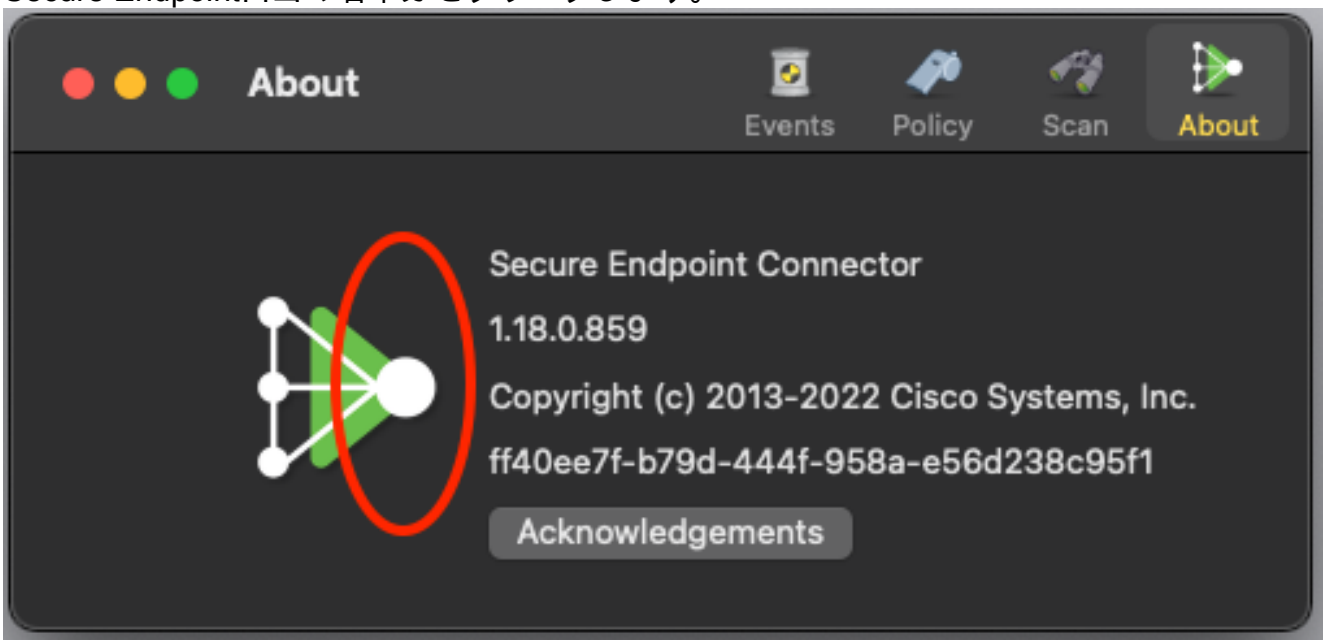
11. 新しく作成したグループを **グループの選択** ドロップダウンメニュークリック **移動** 選択したコンピュータを新しいグループに移動します。これで Mac に機能デバッグ ポリシーが設定されました。メニューバーに表示される[Secure Endpoint]アイコンを選択して、新しいポリシーが適用されていることを確認できます。



シングルハートビートデバッグモードの有効化

この手順は、1.0.4コネクタ以上でのみ使用できます。これにより、次のハートビートまで1つのコネクタをデバッグモードにすることができます。状況に応じて、これは開発者に十分な情報を提供しますが、ハートビートの長さに応じて、完全な診断分析を行うために必要なすべてのプロセスを捕捉しないリスクがあります。単一のハートビートに対してデバッグを有効にする手順は、次のとおりです。

1. コネクタのメニューバーにアクセスし、 **設定.**
2. クリック **バージョン情報**
3. Secure Endpointロゴの右半分をクリックします。



4. 正しく行われた場合、次の通知が画面の右側にポップアップ表示されます。

デバッグは、次のハートビート後に自動的に無効になります。

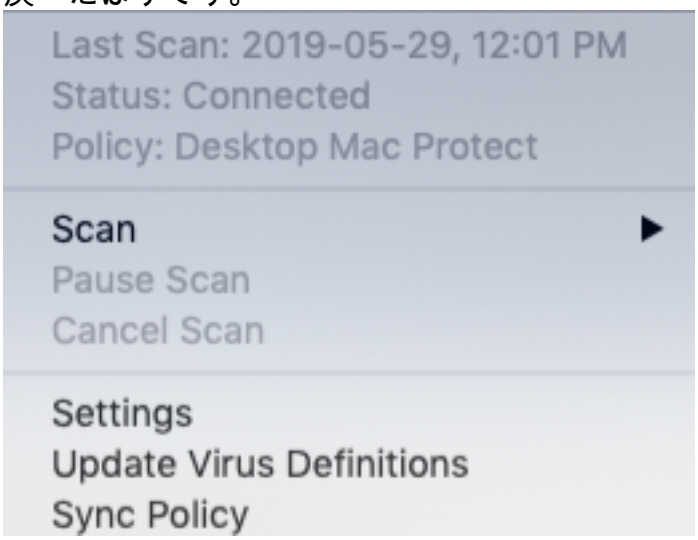
デバッグ モードの無効化

デバッグモードの診断データを取得したら、セキュアエンドポイントコネクタを通常モードに戻す必要があります。デバッグ モードを無効にするには、次の手順を実行してください。

1. Secure Endpointコンソールにログインします。
2. [Management] > [Groups] に移動します。

3. デバッグモードで作成した新しいグループ*Debug TechZone Mac Group*を見つけます。
4. [Edit] をクリックします。

5. 画面の右上にある[Computers]ウィンドウで、リストからコンピュータを探します。これを選択すると、Computerspageに移動します。もう一度、リストからコンピュータを選択し、**[Move to Group...]をクリックします。**.
6. [グループの選択(Select Groupgroup)]ドロップダ**ウンメニュー**から前のグループを選択します。[移動]をクリックして、選択したコンピュータを前のグループに移動します。
7. メニューバーの[Secure Endpoint] アイコンをクリックします。メニューから[Sync Policies]を選択します。
8. ポリシーが前のデフォルト値に戻ったことを検証します。これをメニュー バーで確認します。ポリシーは、*Debug TechZone Mac Group*に変更する前に使用していた元のポリシーに戻ったはずです。



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。