Mac の診断データ収集用の FireAMP コネクタ

目次

概要

このドキュメントでは、Cisco FireAMP Connector for Macintosh（Mac）マシン上で使用可能なサポート ツール アプリケーションにより診断ファイルを生成するために使用するプロセス、およびパフォーマンス上の問題をトラブルシューティングする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推奨されます。

- Cisco FireAMP Connector for Mac
- Mac OSX

使用するコンポーネント

この文書に記載する情報は、Cisco FireAMP Connector for Mac に基づきます。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

Cisco FireAMP Connector for Mac は、 *サポート ツール*と呼ばれるアプリケーションをインストールします。これは、Mac にインストールされた FireAMP Connector の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)
- FireAMP 特定のログ
- FireAMP 設定情報

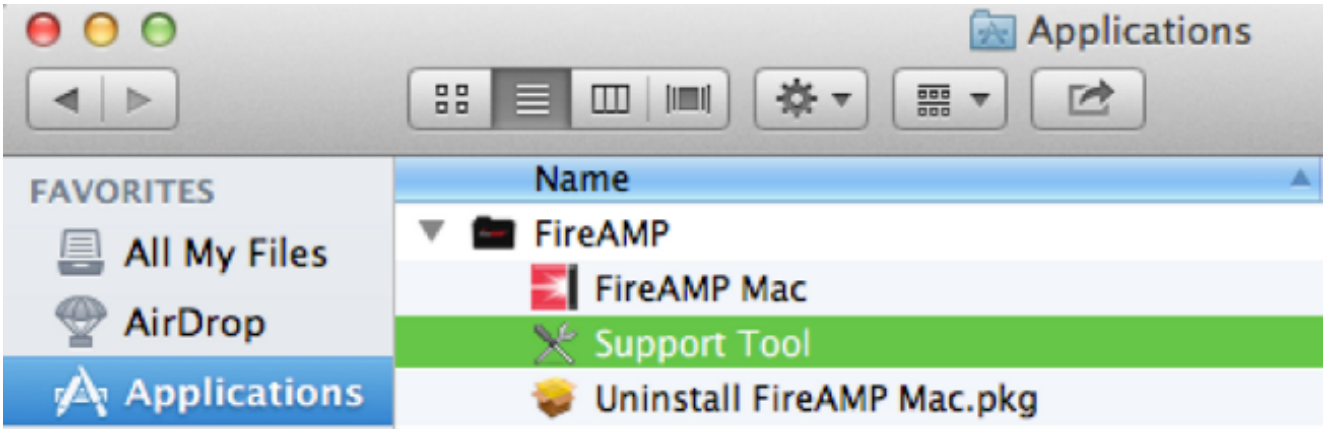
サポート ツールを使用した診断ファイルの生成

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。

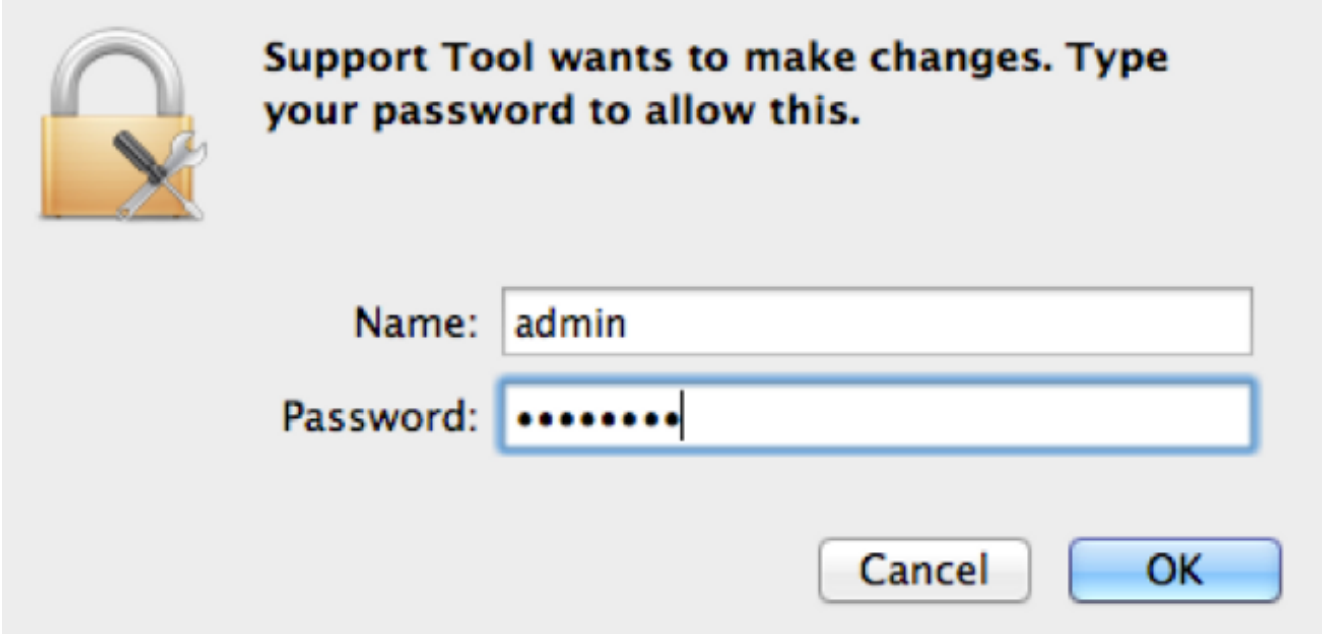
GUI からのサポート ツールの起動

GUI から FireAMP Connector for Mac サポート ツールを起動するには、次の手順を実行してください。

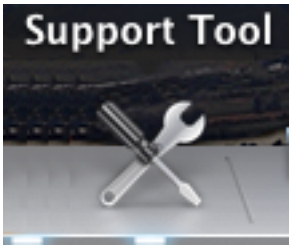
1. [Applications] フォルダ内の [FireAMP] ディレクトリに移動し、サポート ツール ランチャを見つけます。



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。



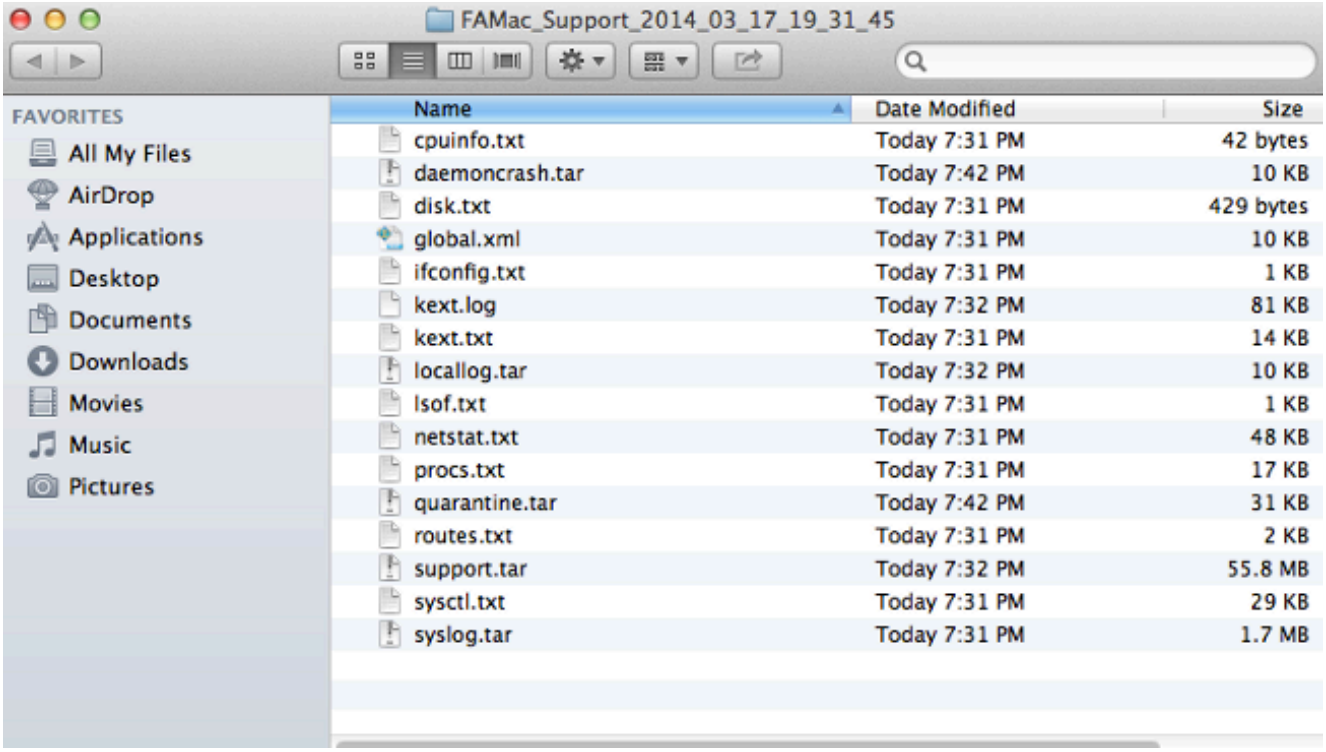
3. クレデンシャルを入力すると、ドックにサポート ツール アイコンが表示されます。



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。

CLI からのサポート 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/Sourcefire/FireAMP Mac/
```

サポート ツール アプリケーションを起動するために、CLI で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/Sourcefire/FireAMP\ Mac
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

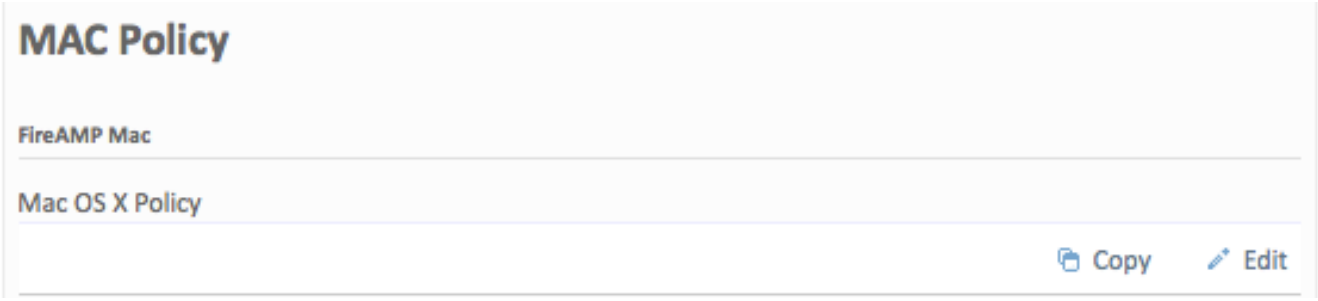
この項では、パフォーマンス上の問題をトラブルシューティングするために FireAMP Connector のデバッグ モードを有効または無効にする方法について説明します。

デバッグ モードの有効化

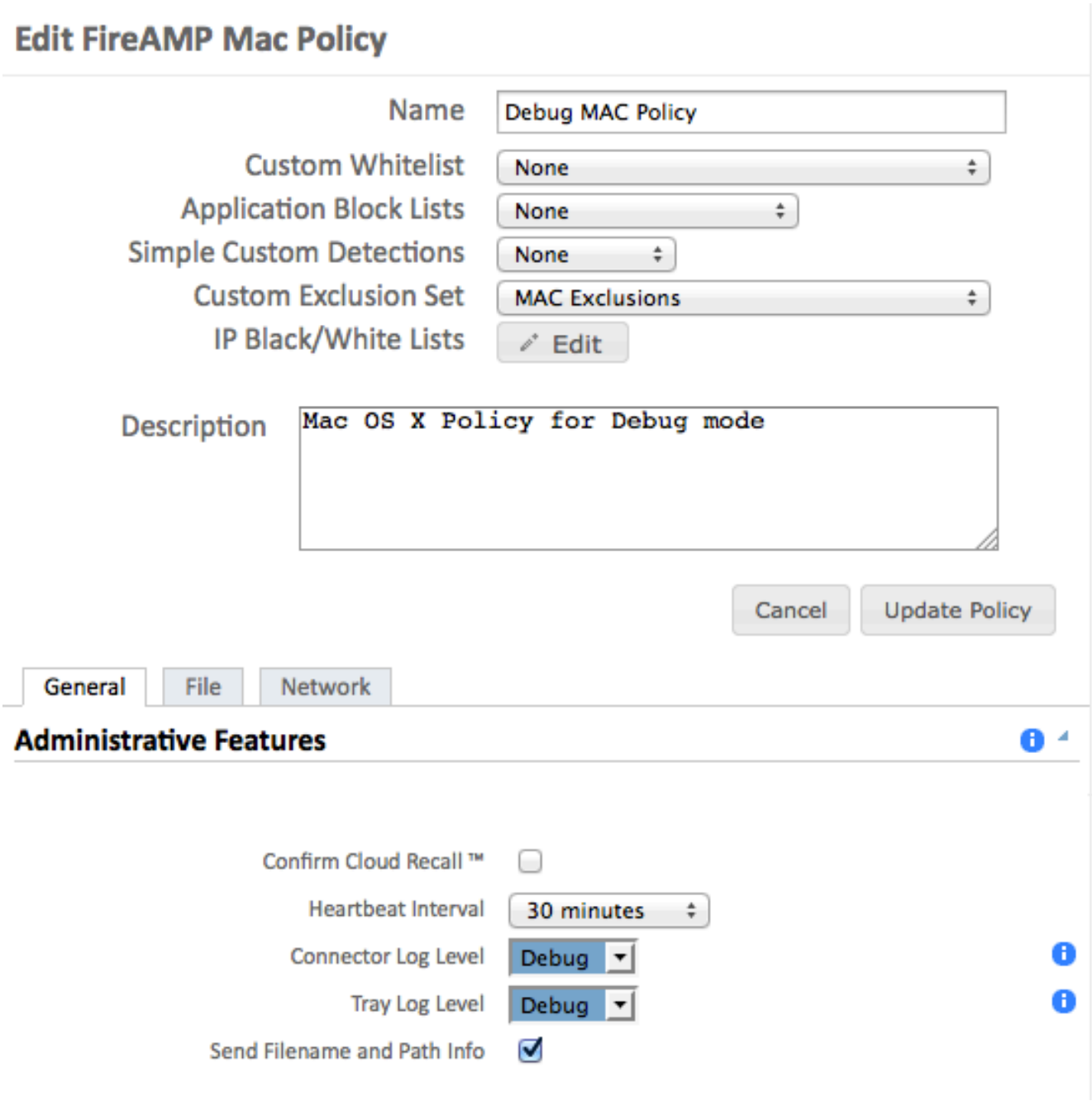
警告： デバッグ モードは、シスコ テクニカル サポートのエンジニアがこのデータを要求した場合にのみ有効にする必要があります。 デバッグ モードを長時間にわたって有効にしておくと、ディスク スペースがすぐに占有され、ファイル サイズの超過が原因で Connector Log データと Tray Log データをサポート診断ファイルに収集できなくなる可能性があります。

デバッグ モードは、FireAMP Connector でパフォーマンス上の問題をトラブルシューティングする際に役立ちます。 デバッグ モードを有効にして、診断データを取得するには、次の手順を実行してください。

1. FireAMP Cloud Console 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、[Copy] をクリックします。 コピーされたポリシーによって、FireAMP Console が次のように更新されます。



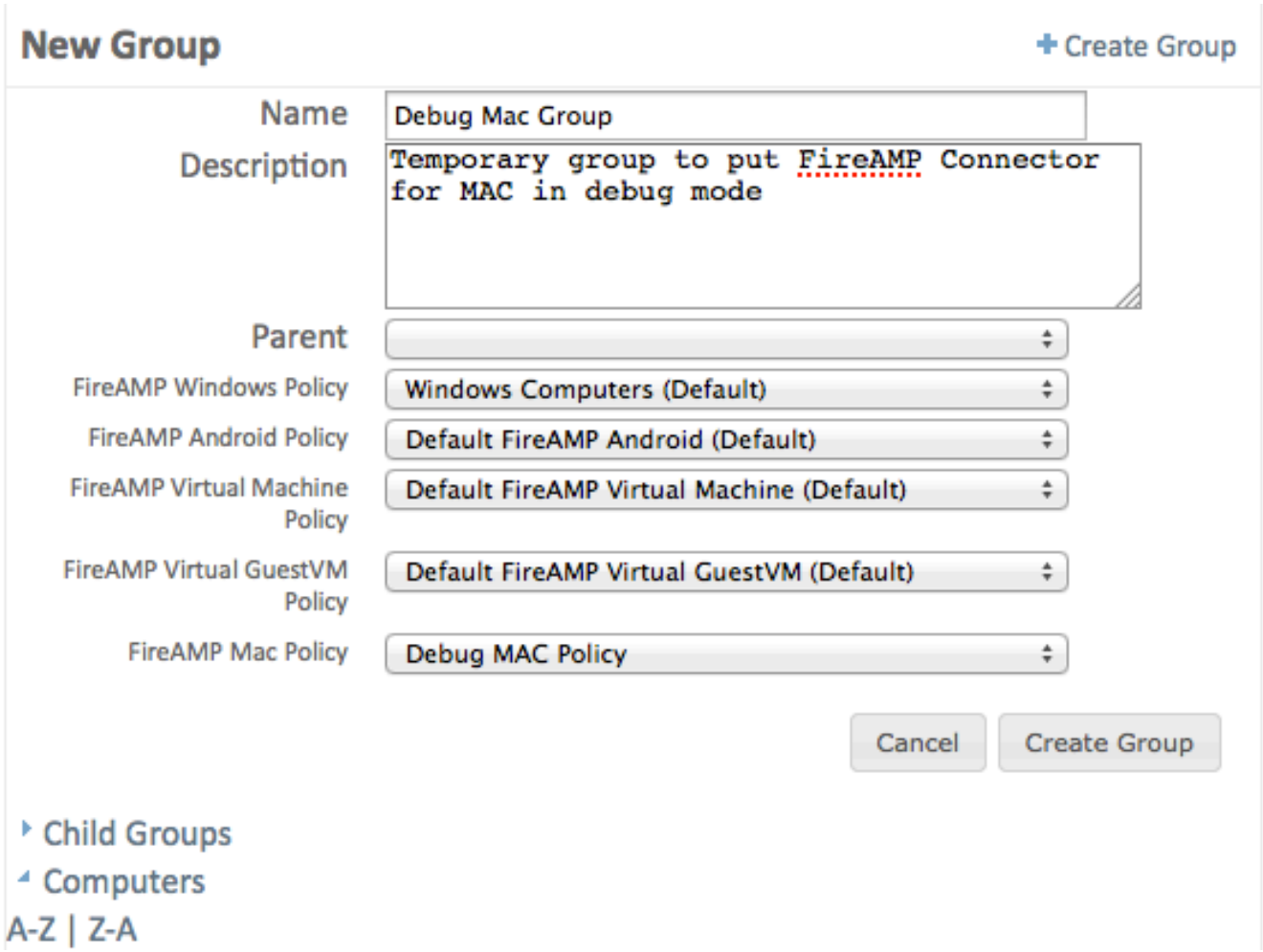
4. [Edit] をクリックし、ポリシーの名前を変更します。 たとえば、*Debug MAC Policy* という名前を付けます。
5. [Administrative Features] をクリックし、[Tray Log Level] と [Connector Log Level] の両方のドロップダウン メニューから [Debug] を選択します。



6. 変更を保存するため、[Update Policy] ボタンをクリックします。

7. [Management] > [Groups] に移動し、画面の右上付近にある [+Create Group] をクリックします。

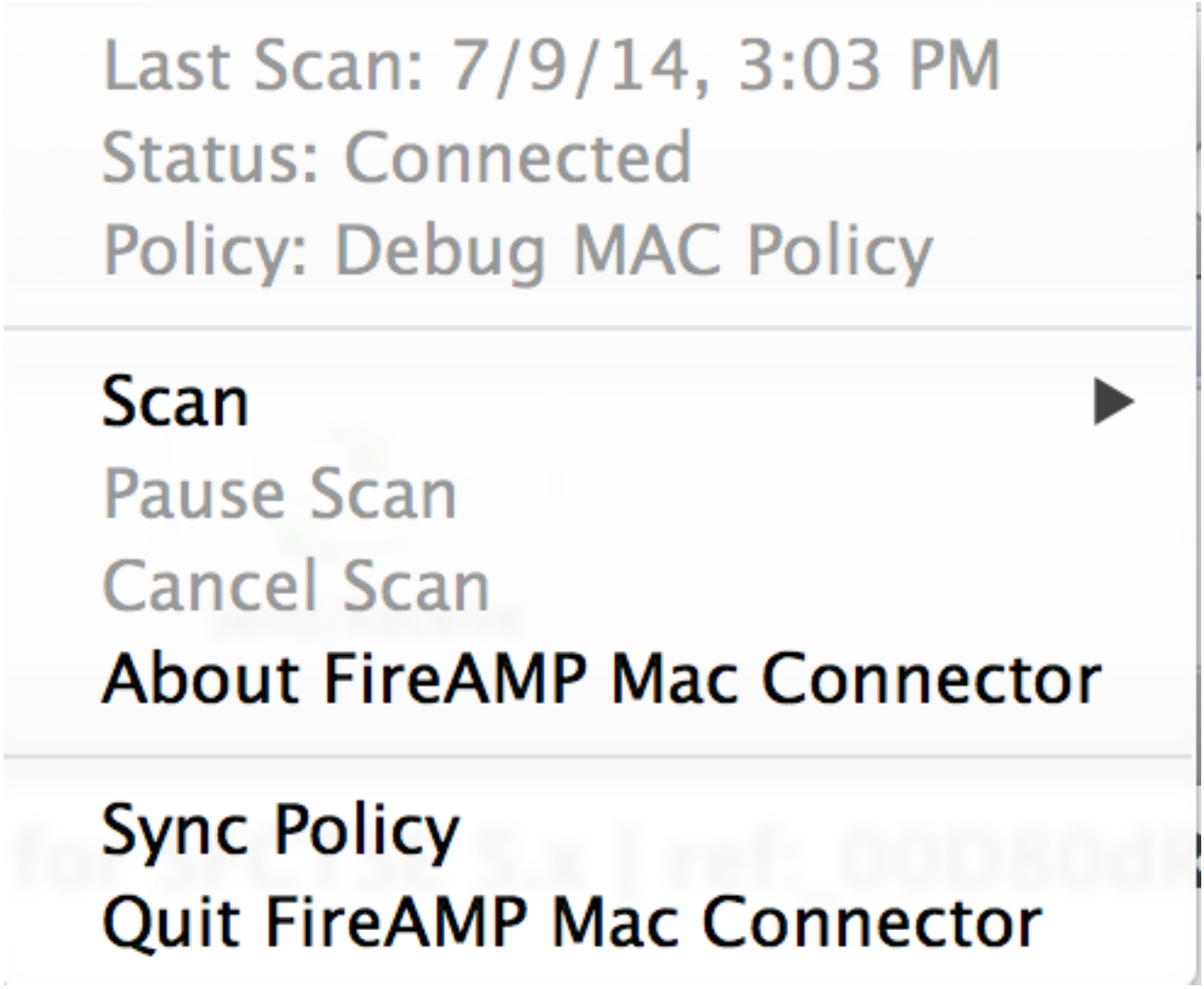
8. グループの名前を入力します。 たとえば、*Debug Mac Group* という名前を付けます。



9. FireAMP MAC ポリシーを、*Default MAC Policy* から、コピーして作成したばかりの新しいポリシー（この例では **Debug MAC Policy**）に変更します。

10. [Computers] をクリックし、リストでご使用のコンピュータを指定します。 コンピュータを選択し、[add selected] をクリックします。

11. [create group] をクリックします。 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 FireAMP アイコンを選択すると、新しいポリシーが適用されていることを確認できます。

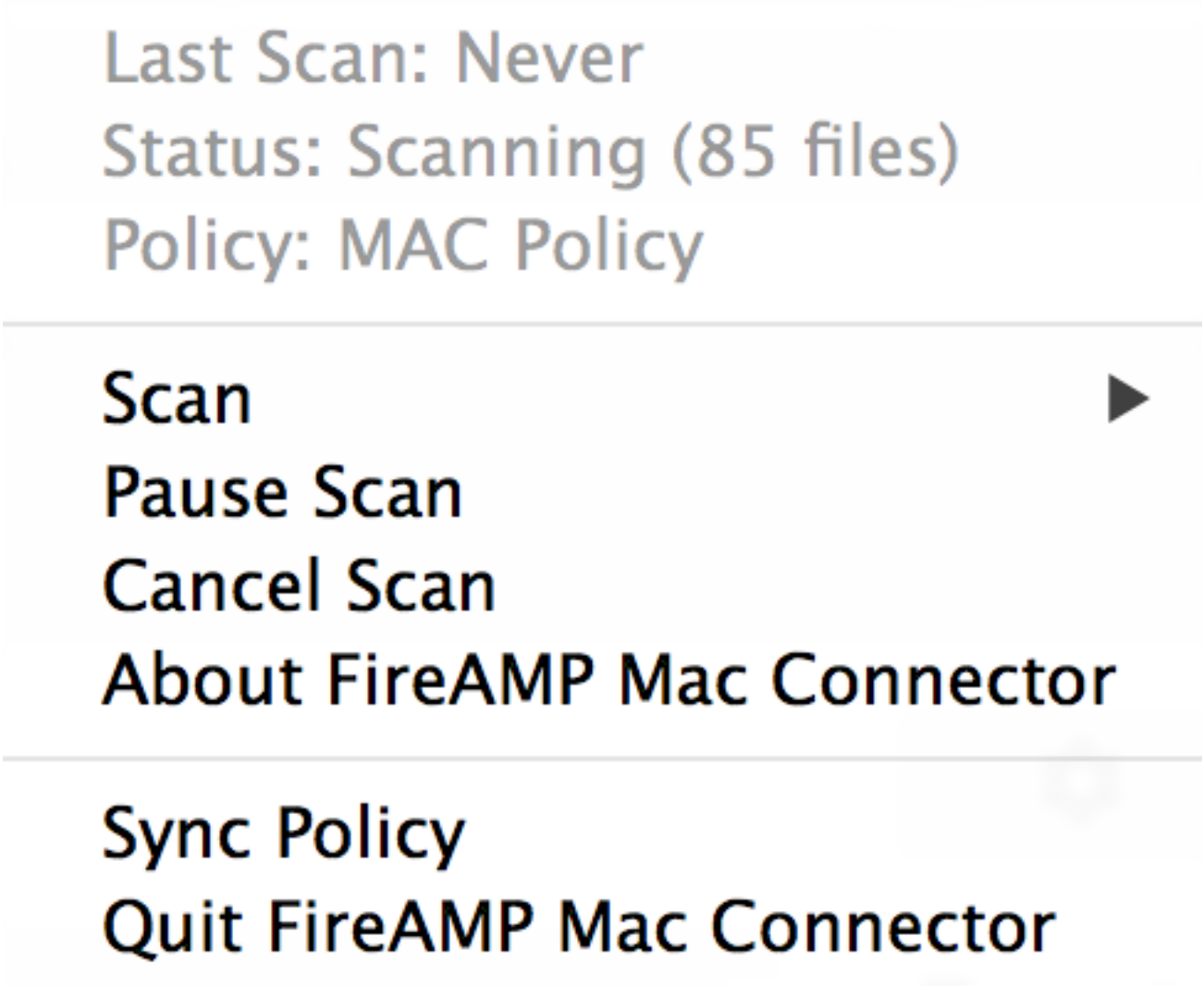


デバッグ モードの無効化

デバッグ モードで診断データを取得した後、FireAMP Connector 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. FireAMP Cloud Console 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 MAC Group* を見つけます。
4. [Edit] をクリックします。
5. [Computers] をクリックして、リストからご使用のコンピュータを見つけます。 コンピュータを選択し、[remove selected] をクリックします。
6. [update group] をクリックします。
7. FireAMP アイコンが表示されているメニュー バーの [Sync Policy] をクリックします。
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。 ポリシーが、*Debug MAC Policy* に変更する前に使用していた元のポリシーに戻ります

。



デバッグ モードが無効になり、FireAMP Connector が正常に機能するようになります。