エンドポイントコンソールのAMPからエンドポイントのデバッグを有効にする

内容

はじめに

このドキュメントでは、Cisco Secure Endpoint Consoleからエンドポイントのデバッグを有効にする方法について説明します。

前提条件

要件

開始する前に、次のことを確認してください。

- Cisco Secure Endpoint for Endpointsコンソールへの管理アクセス。
- デバッグ対象のエンドポイントはCisco Secure Endpointにすでに登録されています

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、次のソフトウェアのバージョンに基づくものです。

- Cisco Secure Endpoint Consoleバージョン5.4.20240718
- Cisco Secure Endpoint Connector 6.3.7以降
- Microsoft Windowsオペレーティングシステム

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

生成された診断データは、さらに分析するためにCisco Technical Assistance Center(TAC)に提供できます。

診断データには、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
- コネクタの設定情報

問題

次のいずれかのシナリオでは、Cisco Secure Endpoint Consoleからエンドポイントのデバッグを有効にする必要があります。

シナリオ1:デバイスをリブートする場合は、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ます。そうしないと、リブート後の動作に影響します。ブートアップデバッグログが必要な場合は、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。

シナリオ2：デバイス上のCisco Secure Endpoint Connectorでパフォーマンスの問題が発生した場合、デバッグモードを有効にすると、分析のために詳細なログを収集できます。

シナリオ3:Secure Endpoint Connectorで特定の問題のトラブルシューティングを行う際には、詳細なログから問題の根本原因を把握できます。

設定

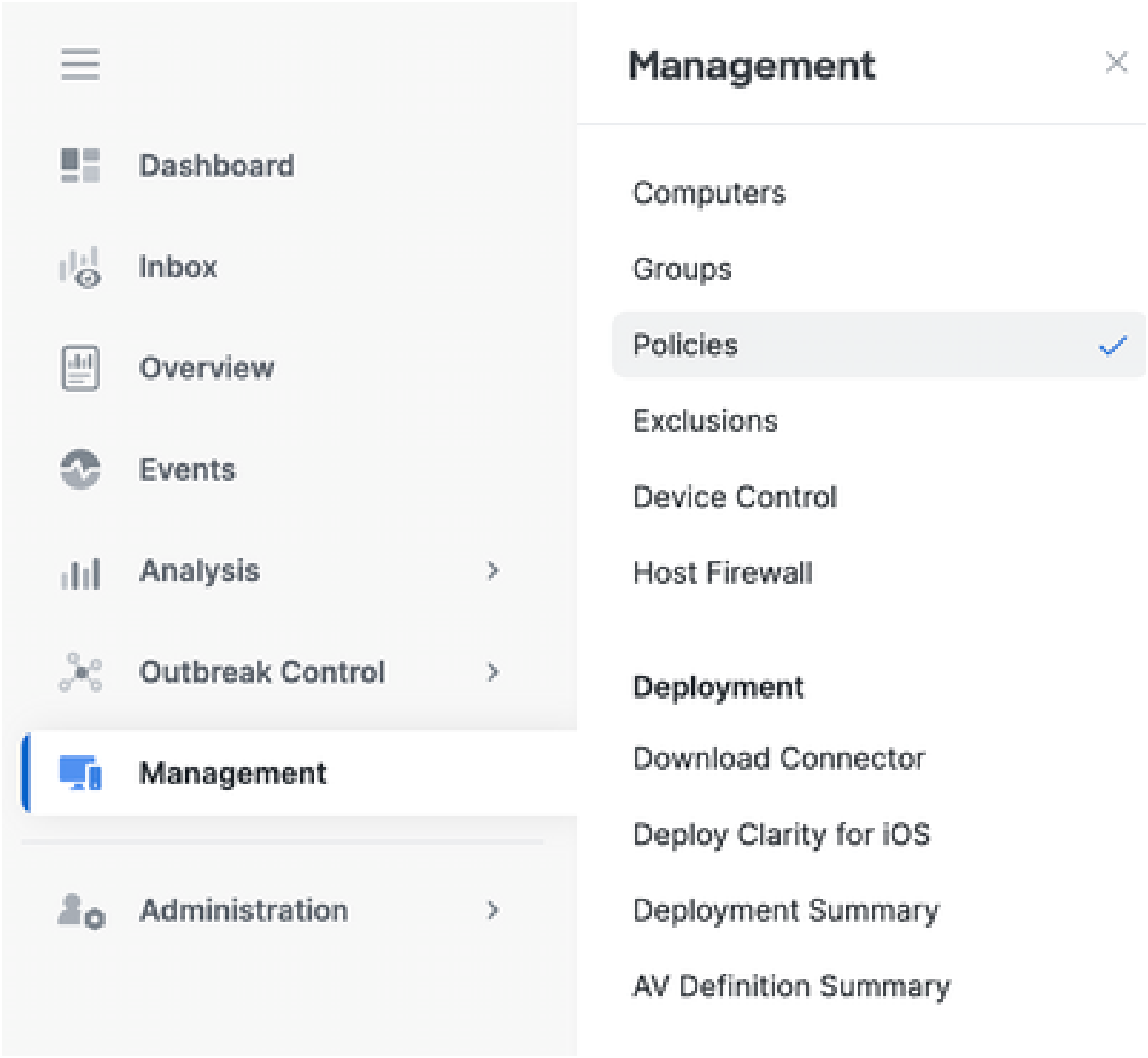
セキュアエンドポイントコンソールを使用して、指定したエンドポイントのデバッグモードを正常に有効にするには、次の手順を実行します。

ステップ1：デバッグに移動するエンドポイントの特定

1. Cisco Secure Endpointコンソールにログインします。メインダッシュボードから、管理セクションに移動します。
2. Management > Computersの順に移動します。
3. デバッグモードが必要なエンドポイントを特定し、メモします。

ステップ2：既存のポリシーを複製する

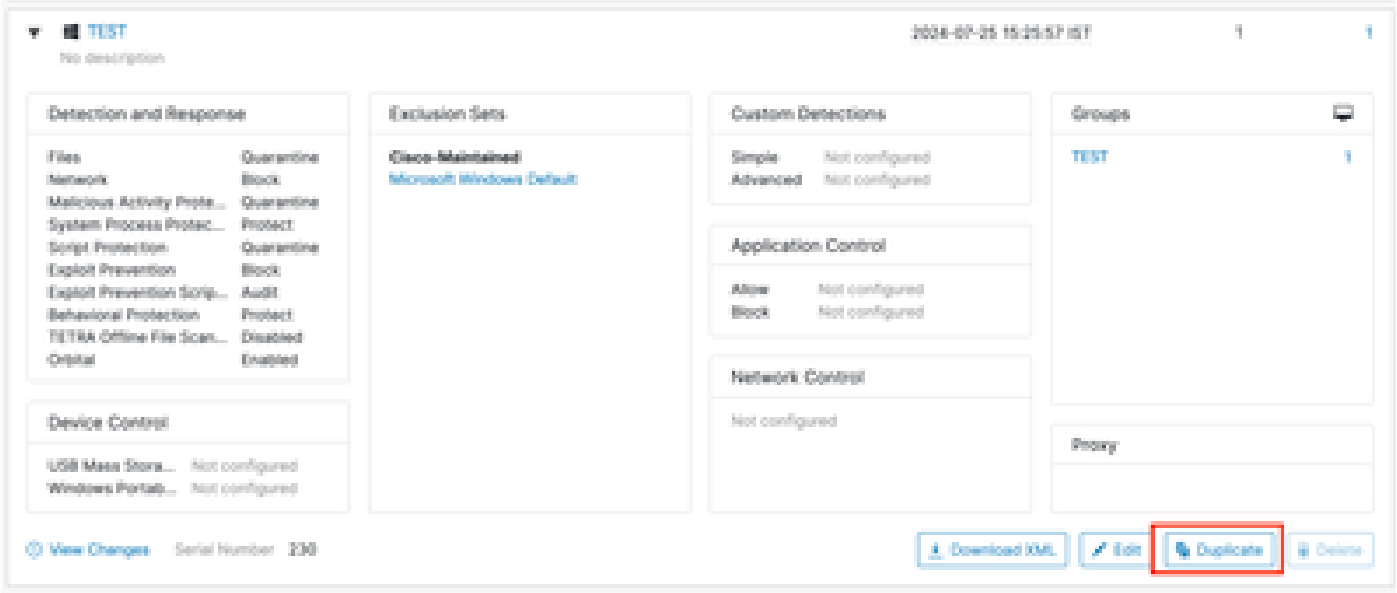
1. [Management] > [Policies] に移動します。



2. 識別されたエンドポイントに現在適用されているポリシーを見つけます。

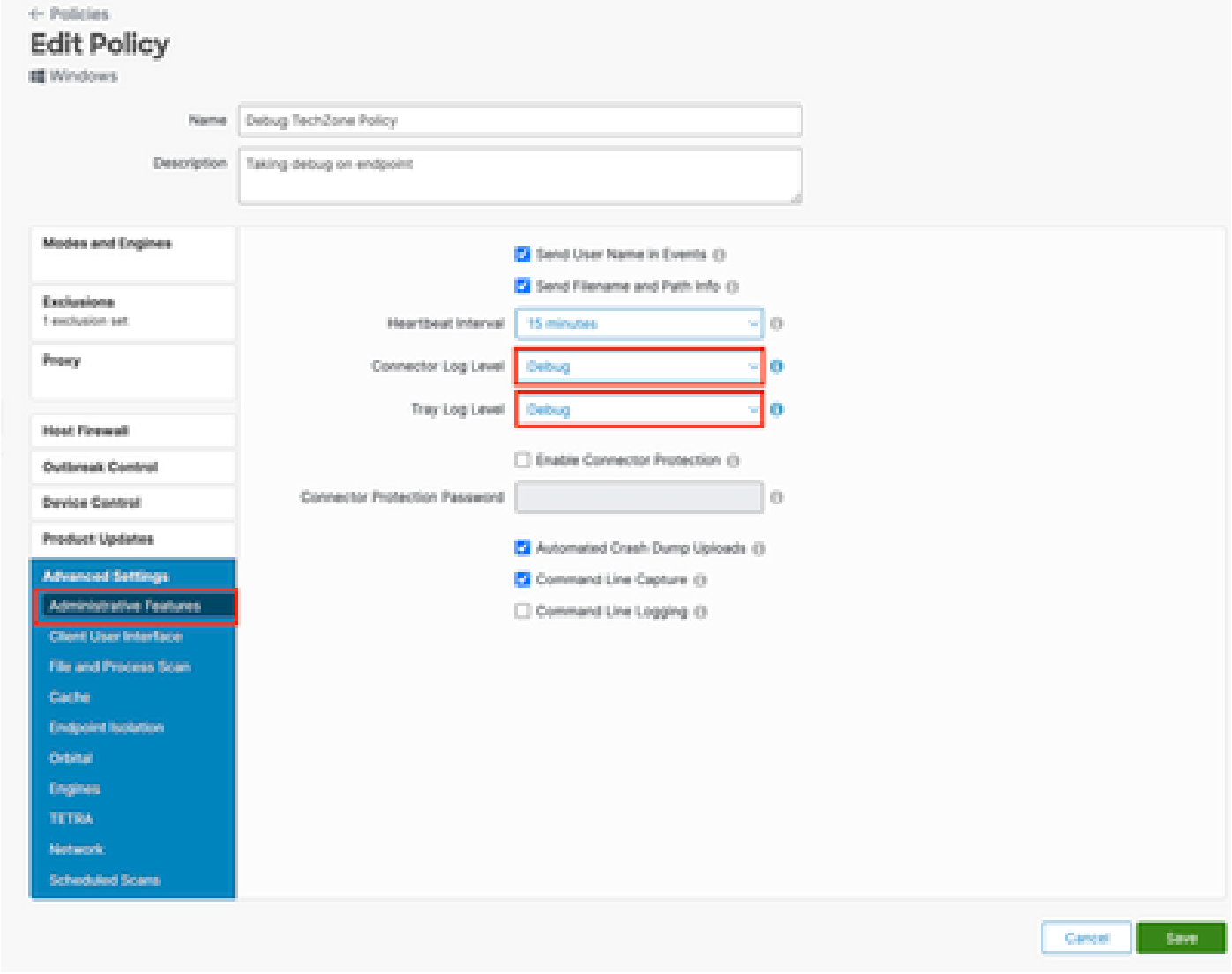
3. policyをクリックして、policyウィンドウを展開します。

4. Duplicateをクリックして、既存のポリシーのコピーを作成します。



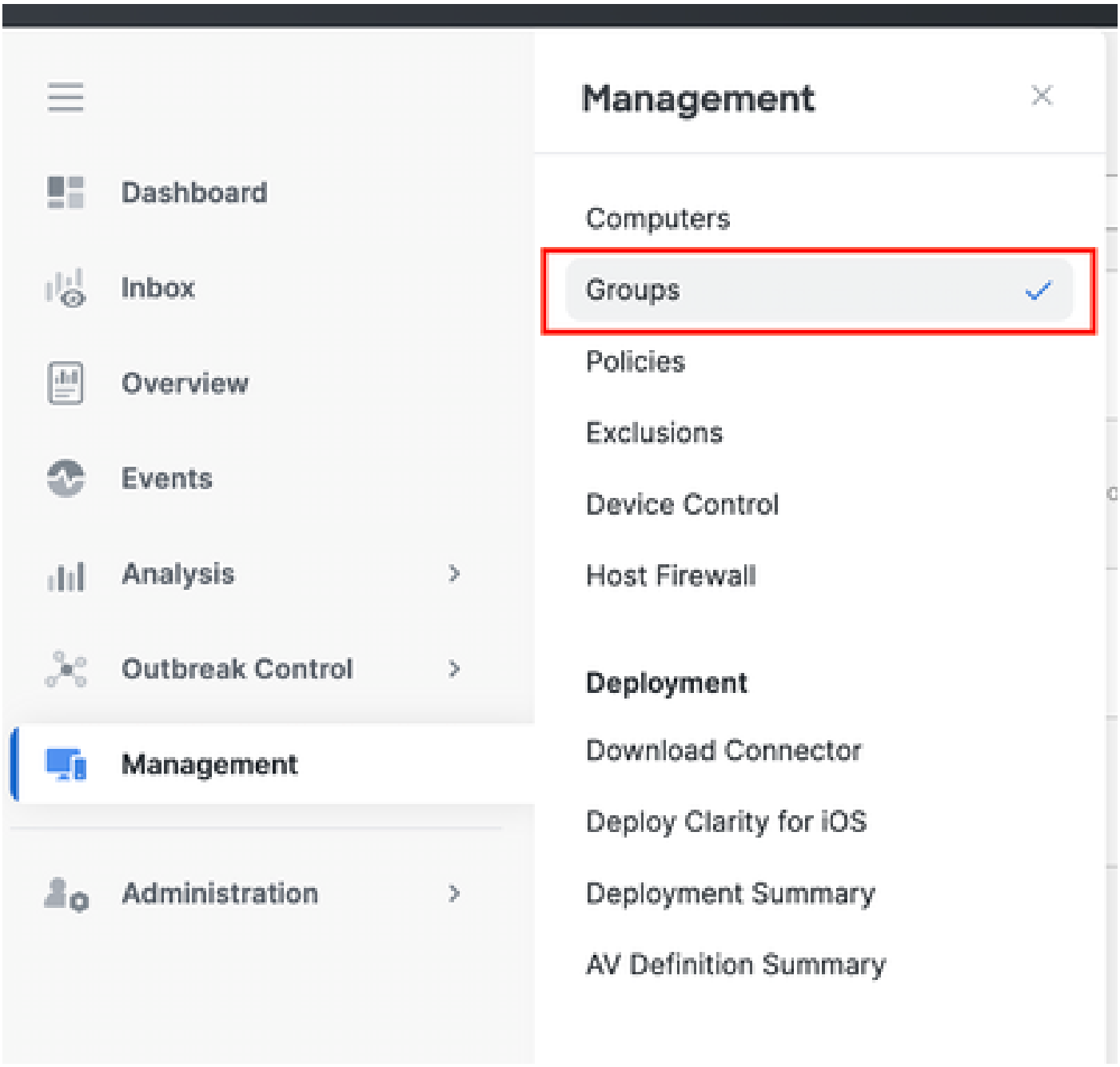
ステップ3：このポリシーをデバッグするためのログレベルの設定

1. duplicated policyウィンドウを選択して展開します。
2. Editをクリックして、ポリシーの名前を変更します（Debug TechZone Policyなど）。
3. [Advanced settings] をクリックします。
4. サイドバーからAdministrative Featuresを選択します。
5. コネクタログレベルとトレイログレベルの両方をデバッグに設定します。
6. Saveをクリックして、変更を保存します。



ステップ4：新しいグループを作成し、その新しいポリシーをリンクする

1. [Management] > [Groups] に移動します。

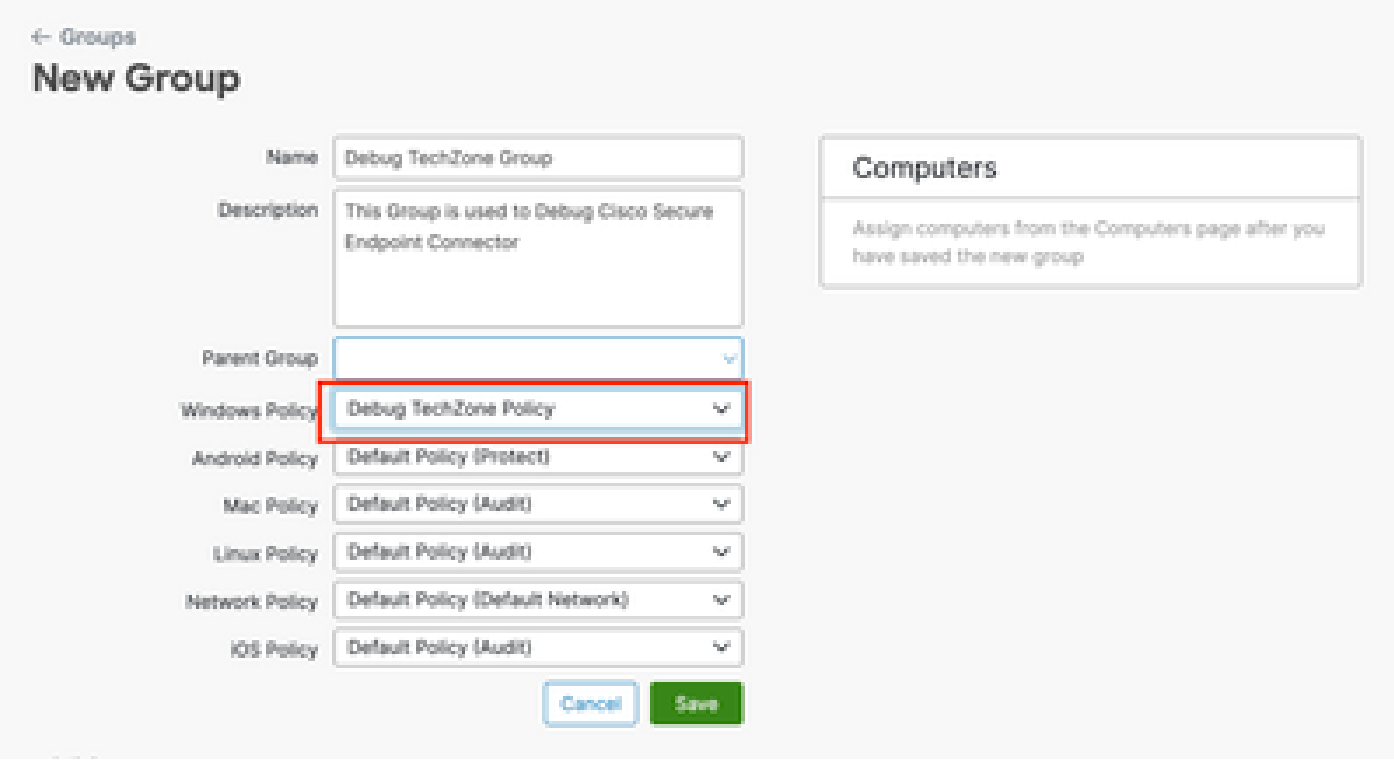


2. 画面右上にあるCreate Groupをクリックします。

3.グループの名前を入力します（例：Debug TechZone Group）。

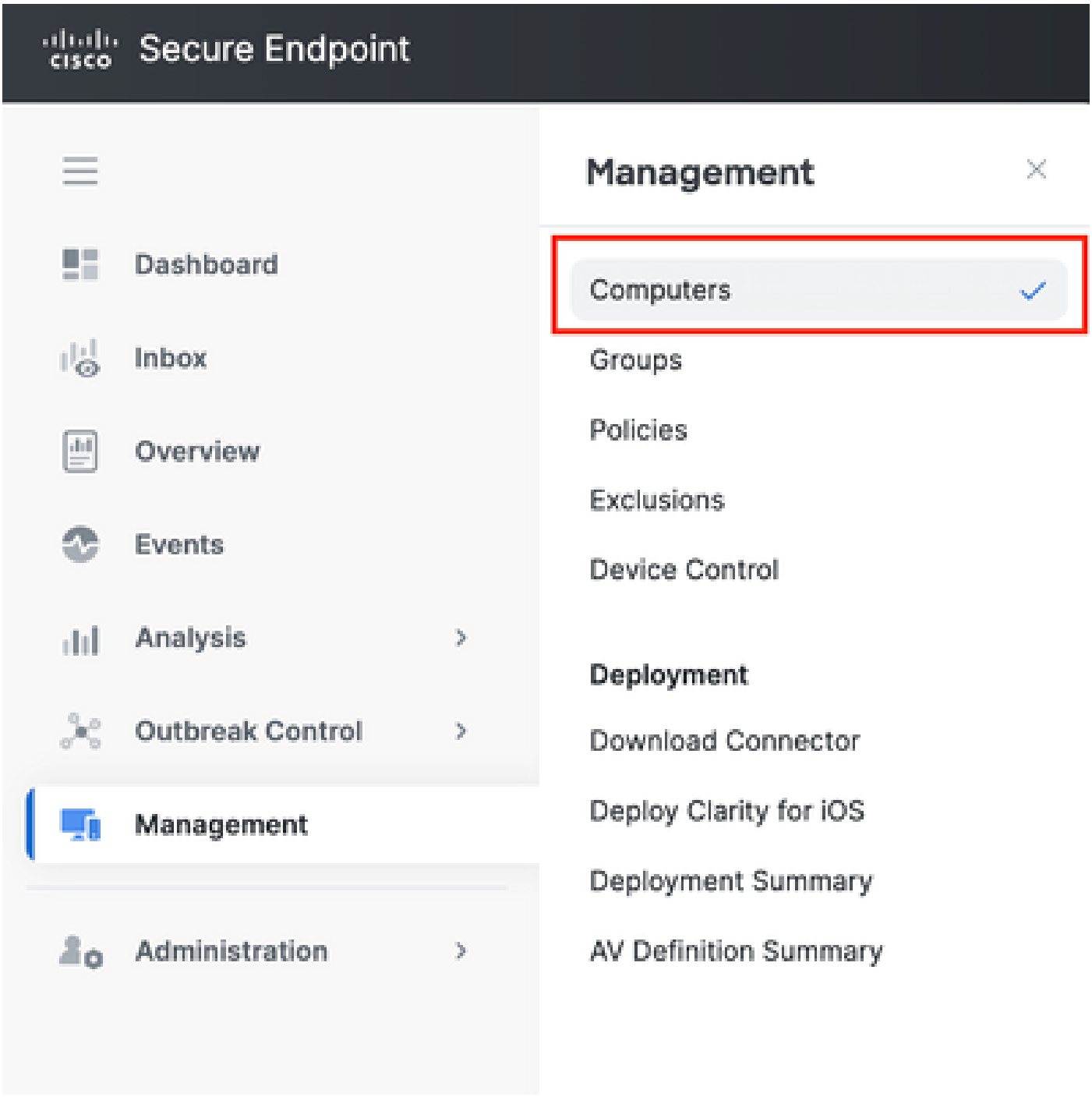
4. ポリシーをデフォルトから新しく作成したデバッグポリシーに変更します。

5. Saveをクリックします。



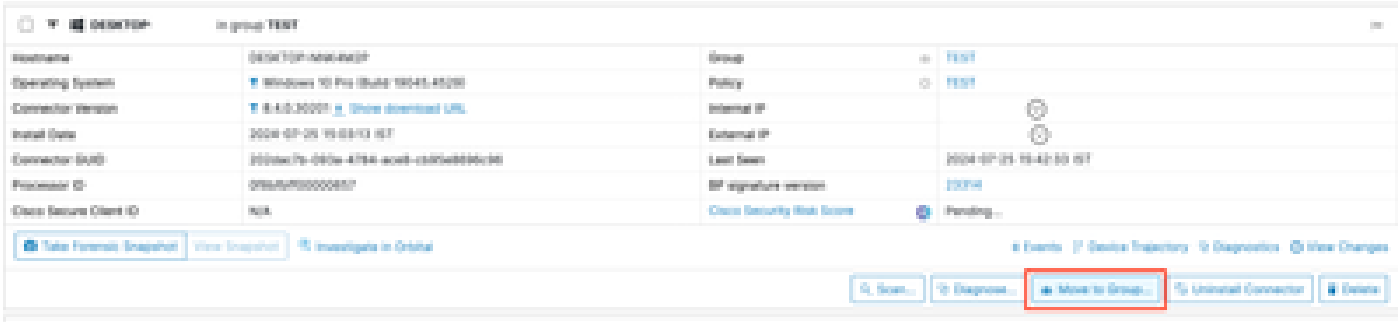
ステップ5：特定したエンドポイントをこの新しいグループに移動する

1. 「管理」>「コンピュータ」に戻ります。



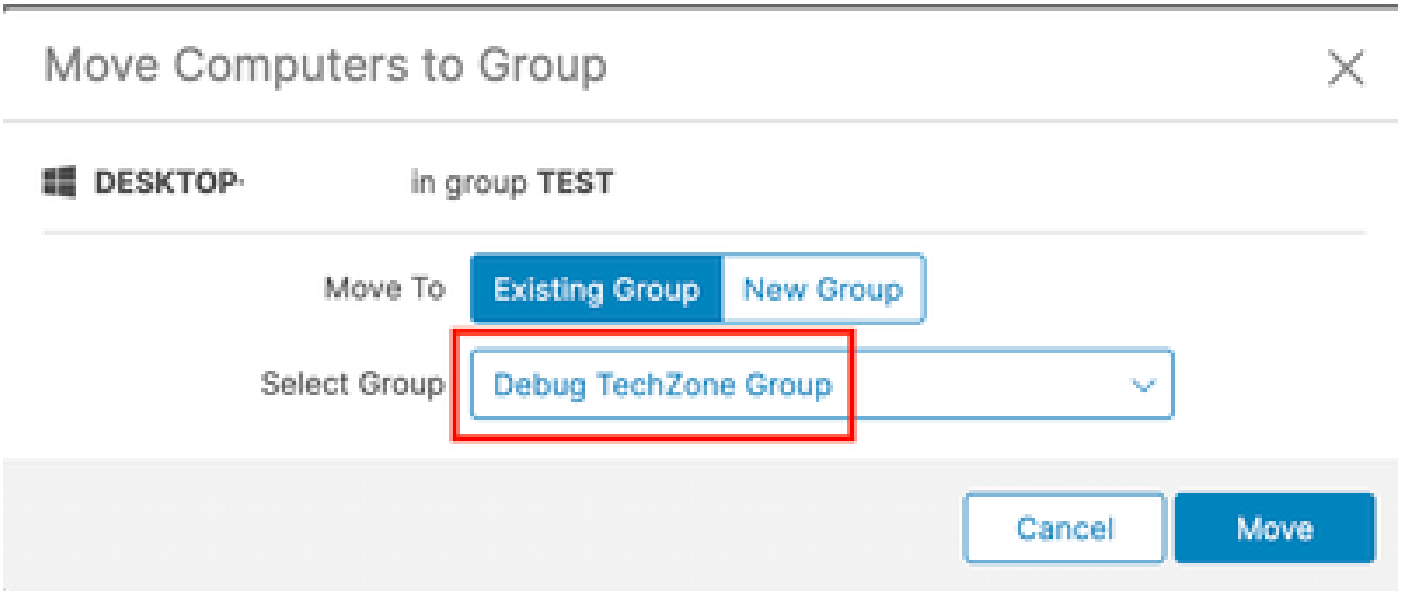
2. リストから識別されたエンドポイントを選択します。

3. Move to Groupをクリックします。



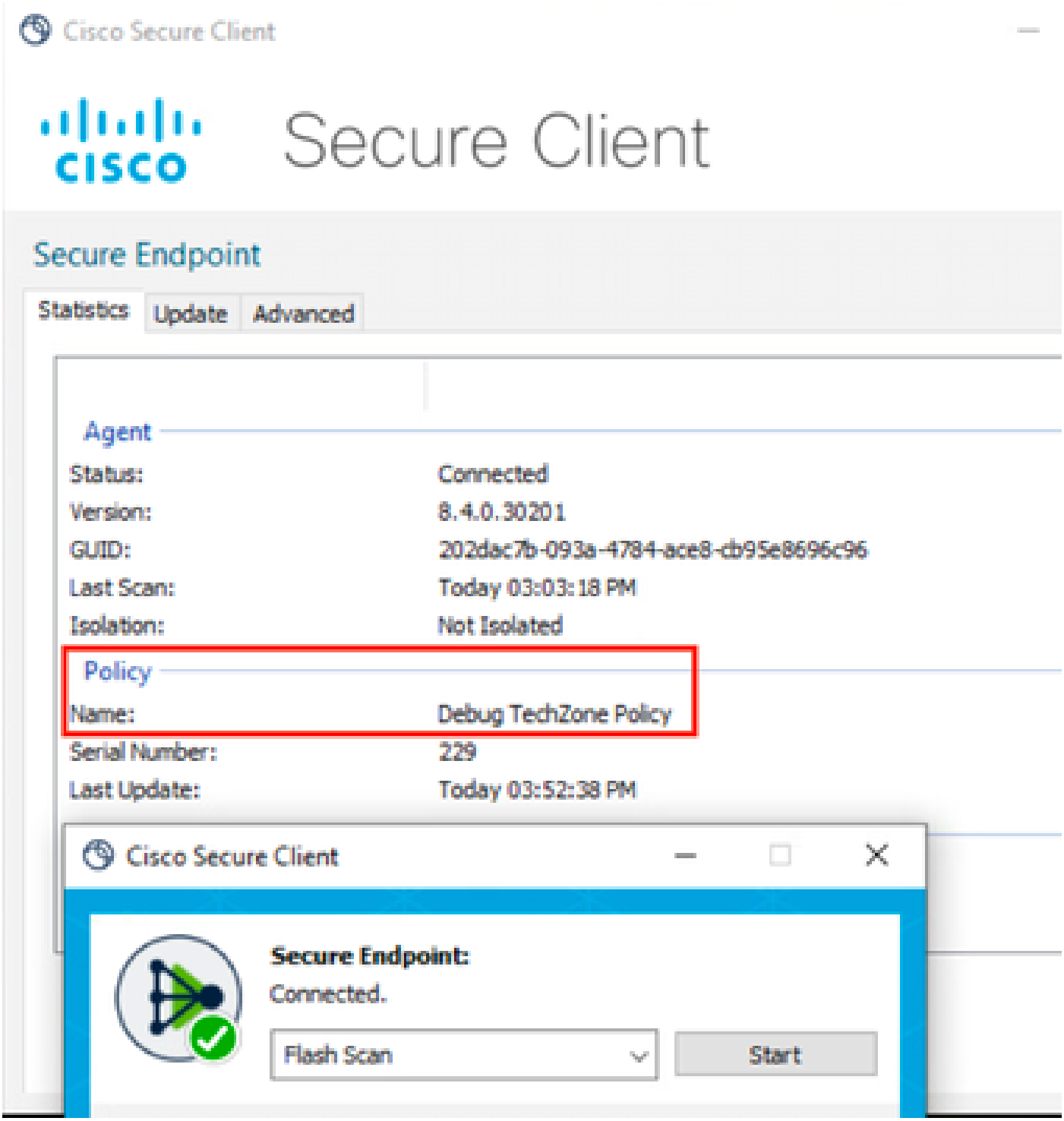
4. 「グループの選択」ドロップダウン・メニューから、新しく作成したグループを選択します。

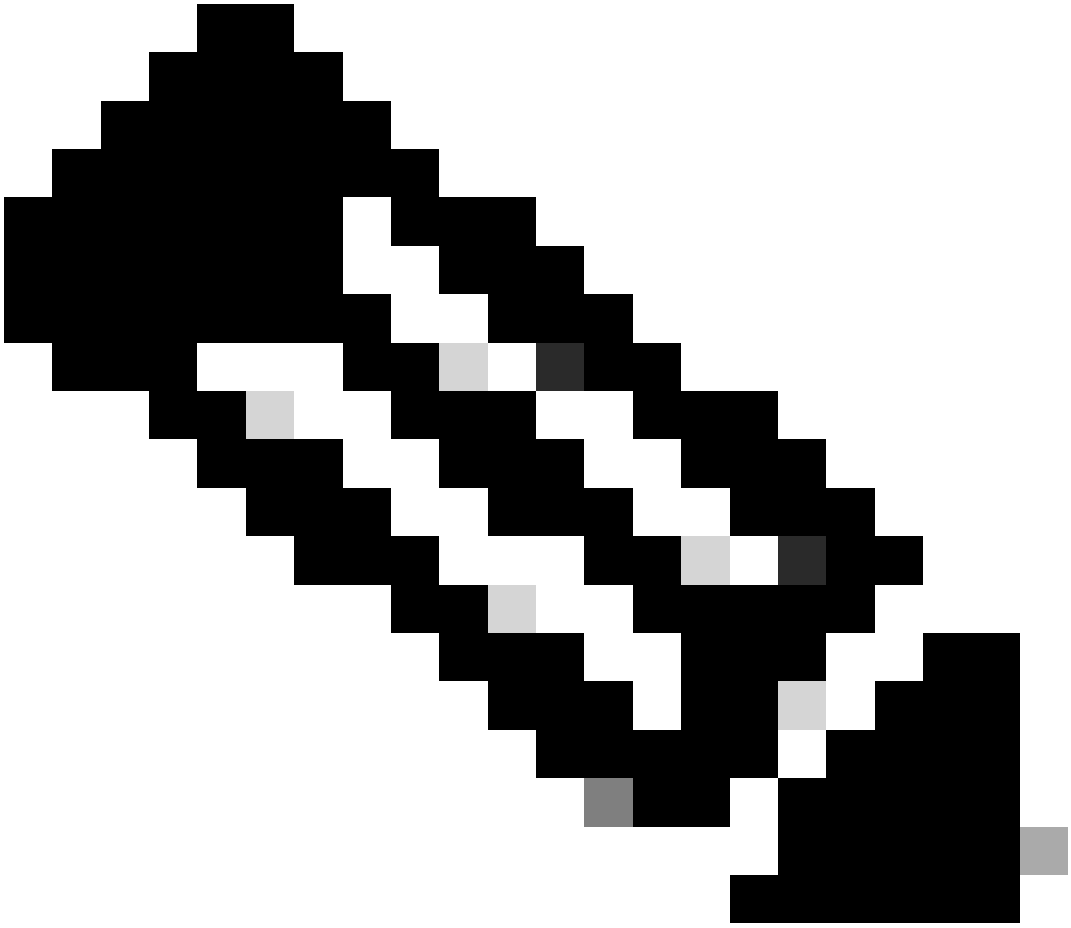
5. Moveをクリックして、選択したエンドポイントを新しいグループに移動します。



手順6：コンピュータのページとコネクタUIでエンドポイントを確認します

1. エンドポイントがComputersページの新しいグループの下にリストされていることを確認します。
2. エンドポイントで、セキュアエンドポイントコネクタUIを開きます。
3. メニューバーのSecure Endpointアイコンをチェックして、新しいデバッグポリシーが適用されていることを確認します。


Cisco Secure Client
Secure Client
Secure Endpoint
Statistics
Update
Advanced
Agent
Status: Connected
Version: 8.4.0.30201
GUID: 202dac7b-093a-4784-ace8-cb95e8696c96
Last Scan: Today 03:03:18 PM
Isolation: Not Isolated
Policy
Name: Debug TechZone Policy
Serial Number: 229
Last Update: Today 03:52:38 PM
Cisco Secure Client
Secure Endpoint:
Connected.
Flash Scan
Start



注：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できます。デバッグモードを長時間にわたって有効にしておくと、ディスク領域がすぐにいっぱいになり、ファイルサイズが大きすぎるためにコネクタのログとトレイログのデータがサポート診断ファイルに収集されるのを防ぐことができます。

さらにサポートが必要な場合は、シスコのサポートに連絡してください。

[各国のシスコ サポートの連絡先]

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。