エンドポイント向けAMPとThreat GridのWSAとの統合

内容

概要

このドキュメントでは、エンドポイント用のAdvanced Malware Protection(AMP)とThreat Grid(TG)をWebセキュリティアプライアンス(WSA)と統合する手順について説明します。

著者：Cisco TACエンジニア、Uriel Montero、編集：Yeraldin Sanchez

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。

- エンドポイントアクセス用AMP
- TGプレミアムアクセス
- ファイル分析とファイルレピュテーション機能キーを使用したWSA

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- AMPパブリッククラウドコンソール
- WSA GUI
- TGコンソール

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。

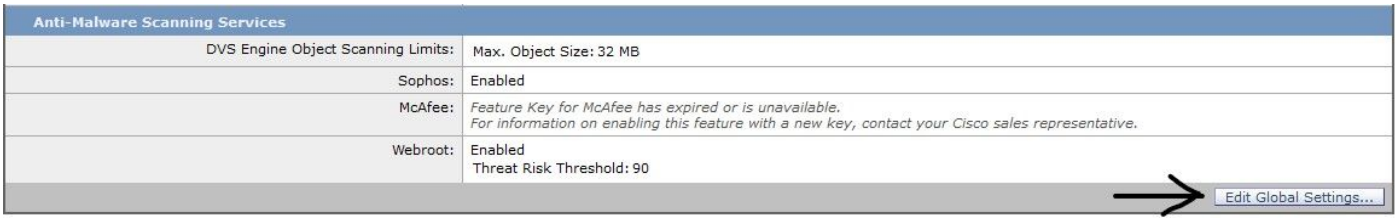
設定

WSAコンソールにログインします。

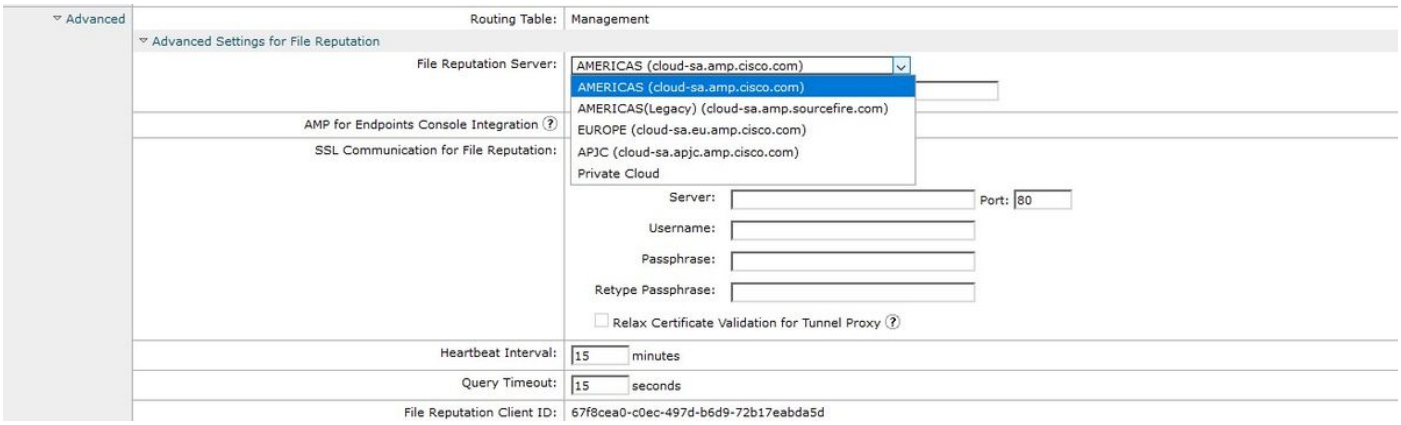
ログインしたら、[Security Services] > [Anti-Malware and Reputation]に移動します。このセクションでは、AMPとTGを統合するオプションを見つけることができます。

AMP統合

[Anti-Malware Scanning Services]セクションで、図に示すように[Edit Global Settings]をクリックします。

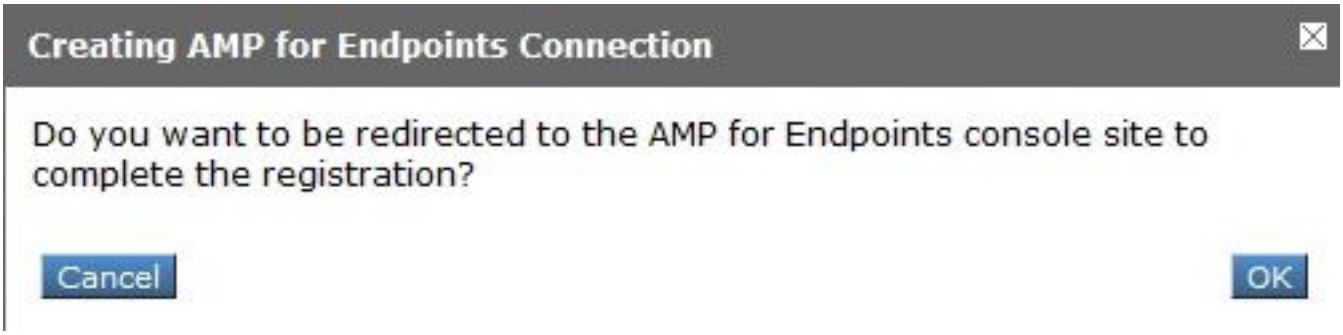


[Advanced] > [Advanced Settings for File Reputation]セクションを検索して、展開すると、一連のクラウドサーバオプションが表示され、最寄りのロケーションを選択します。

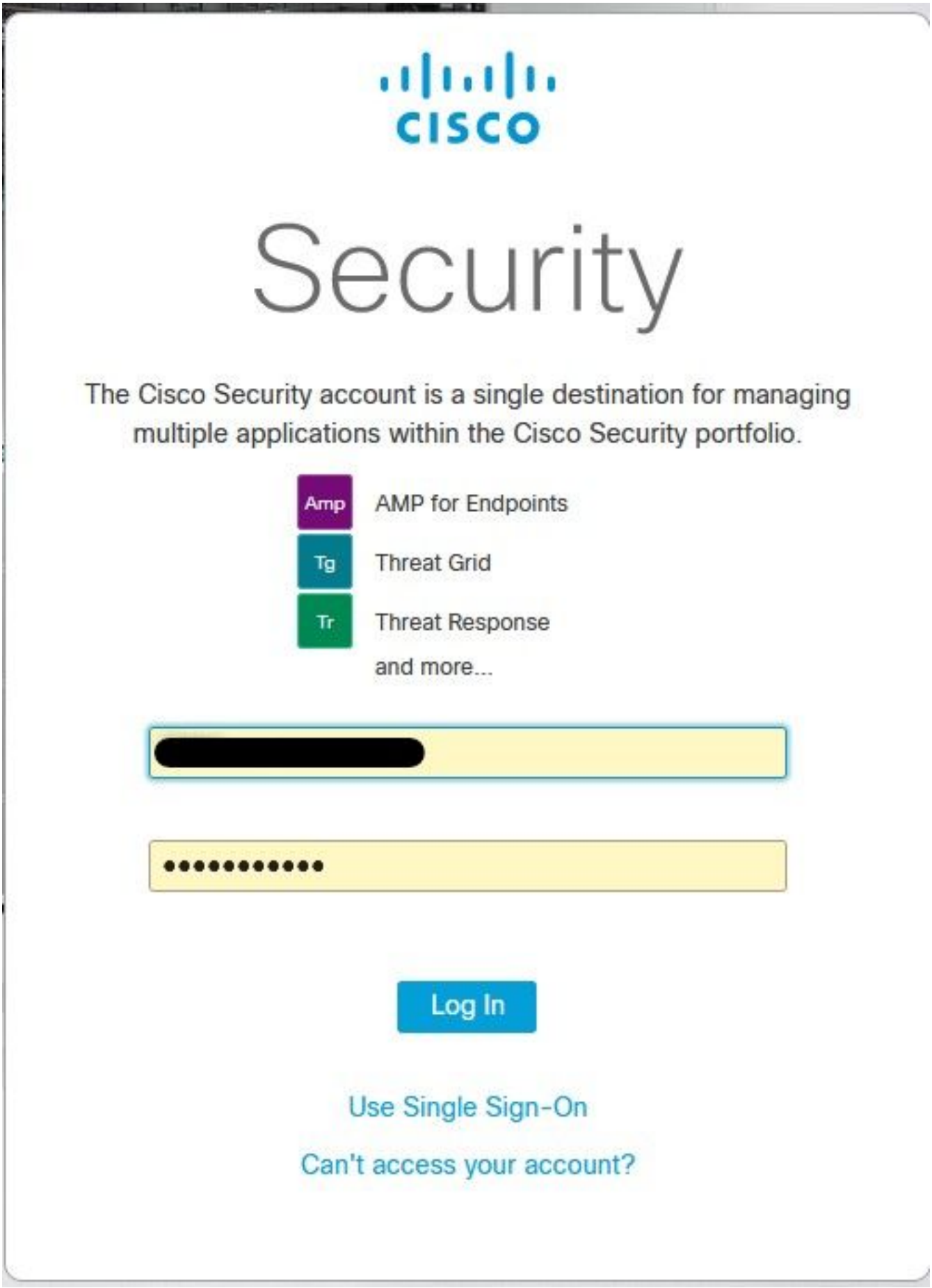


クラウドを選択したら、[Register Appliance with **AMP for Endpoints]ボタンをクリック**します。

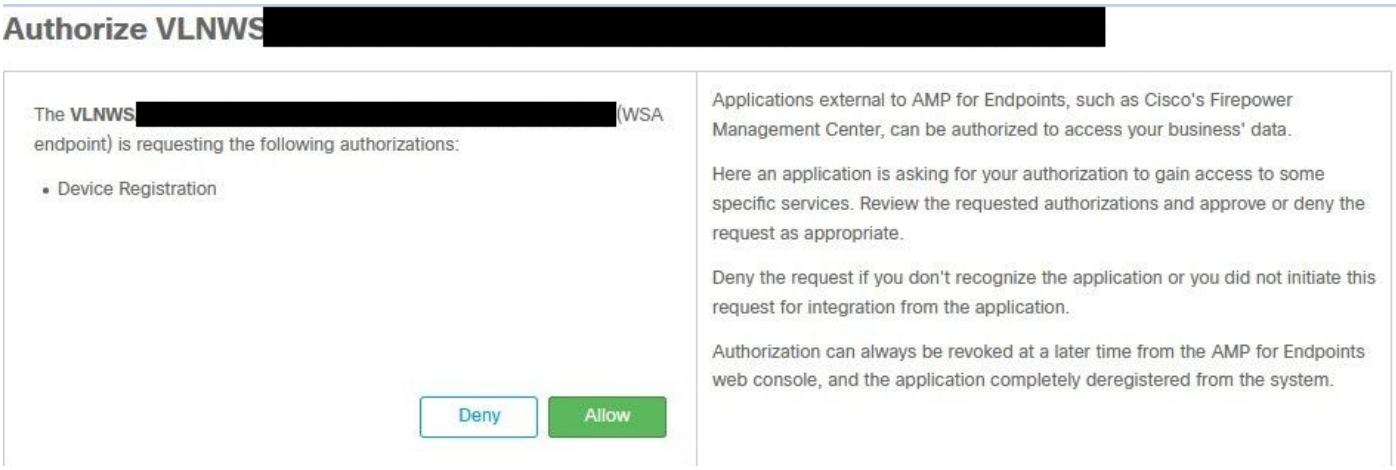
図に示すように、AMPコンソールにリダイレクトするポップアップが表示さ**れ**、[Ok]ボ**タンをク**リックします。



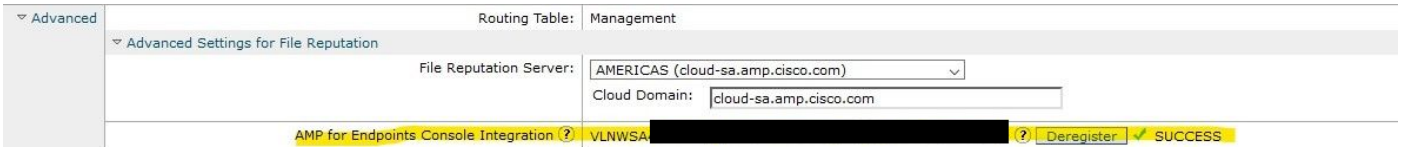
図に示すように、有効なAMPクレデンシャルを入力し、[ログイン]**をクリック**する必要があります。



デバイス登録を受け入れ、クライアントIDをメモします。これは、後でコンソールでWSAを見つけるのに役立ちます。



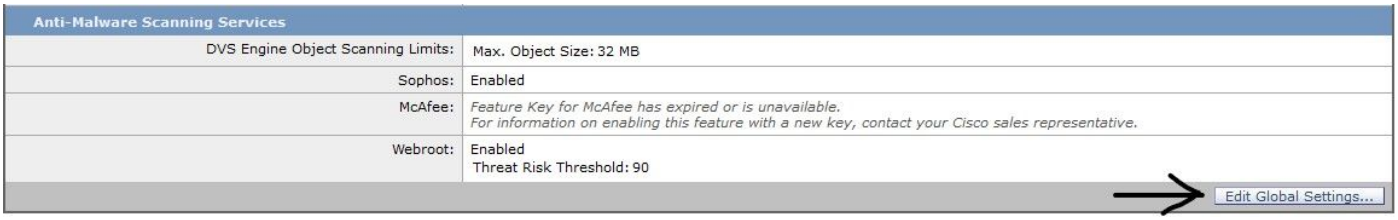
WSAコンソールに戻り、図に示すように、[Amp for Endpoints Console Integration]セクションにチェックが表示されます。



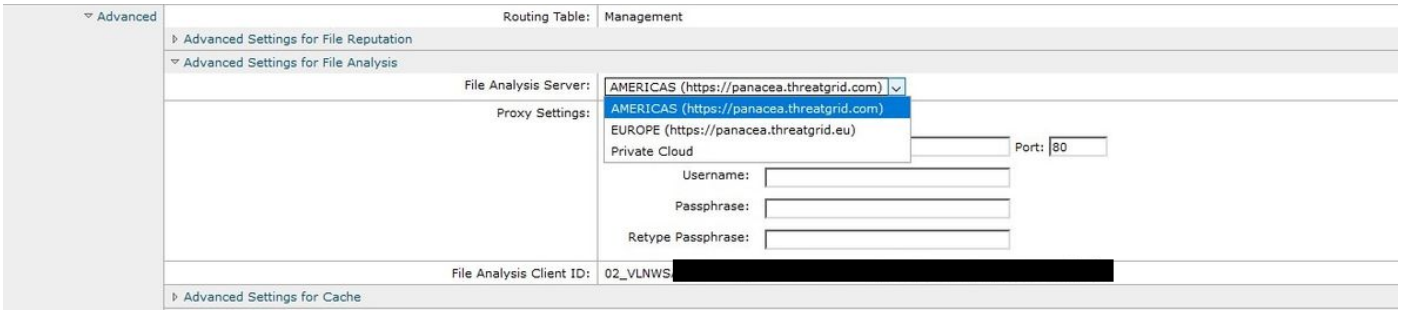
注:[送信]をクリックし**て変更を確定する**ことを忘れないでください（プロンプトが表示された場合）。そうしないと、もう一度プロセスを実行する必要があります。

Threat Gridの統合

[セキュリ**ティサービス] > [マルウェアとレピュテーションの対策]に移動**し、Anti-Malware Protection Servicesで[グローバル設定の編**集]ボタンをクリックします**（図を参照）。

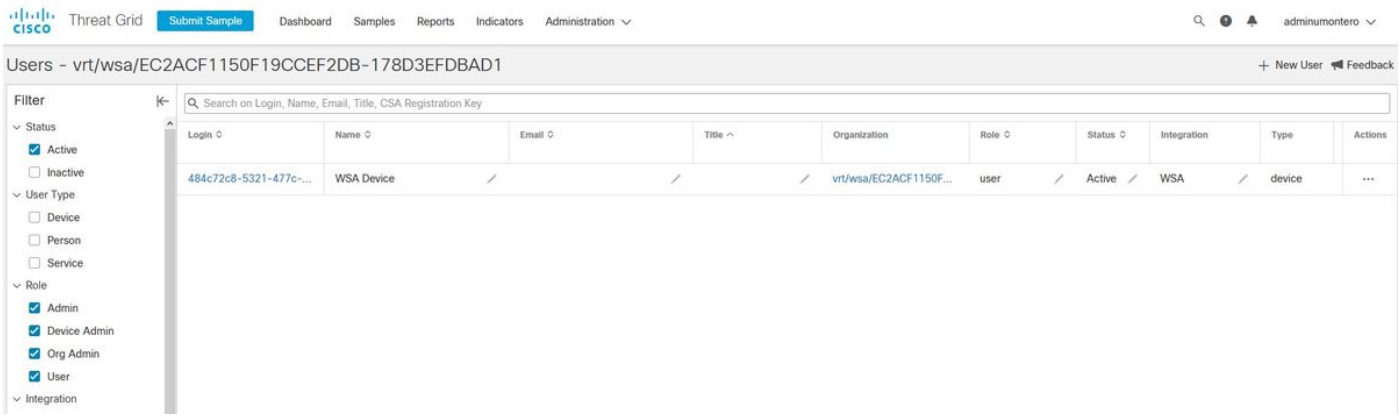


[Advanced] > [Advanced Settings for File Analysis]セクションを検索して展開し、図に示すように、場所に最も近いオプションを選択します。



[Submit]をクリックし、**変更を[Commit]**をクリックします。

アプライアンスがAMP/TGと正常に統合された場合は、TGポータル側で[Users]タブの下でWSAデバイスを検索します。



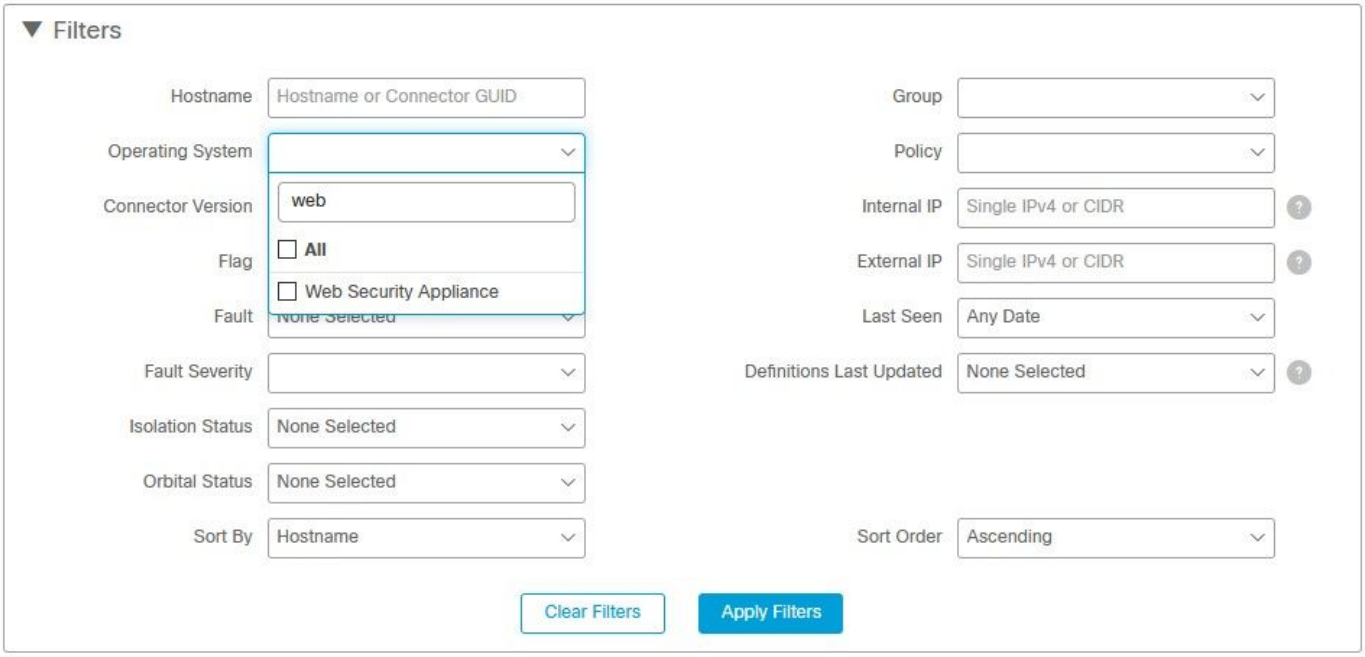
[Login]をクリックすると、該当するアプライアンスの情報にアクセスできます。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

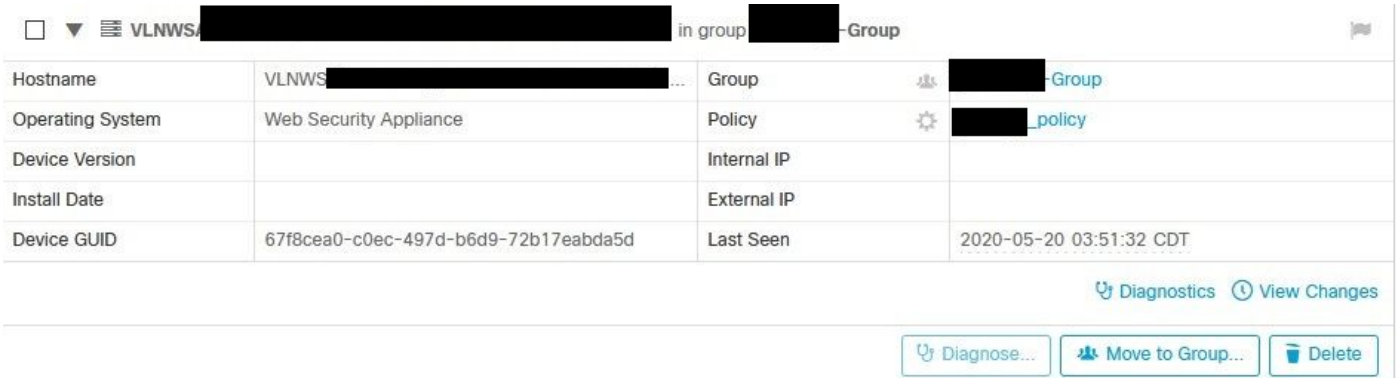
AMPとWSAの統合が成功したことを確認するには、AMPコンソールにログインし、WSAデバイスを検索します。

[管理] > [コンピュータ]に移動し、[フィルタ]セクションで[Web Security Appliance]を検索し、フィルタを適用します

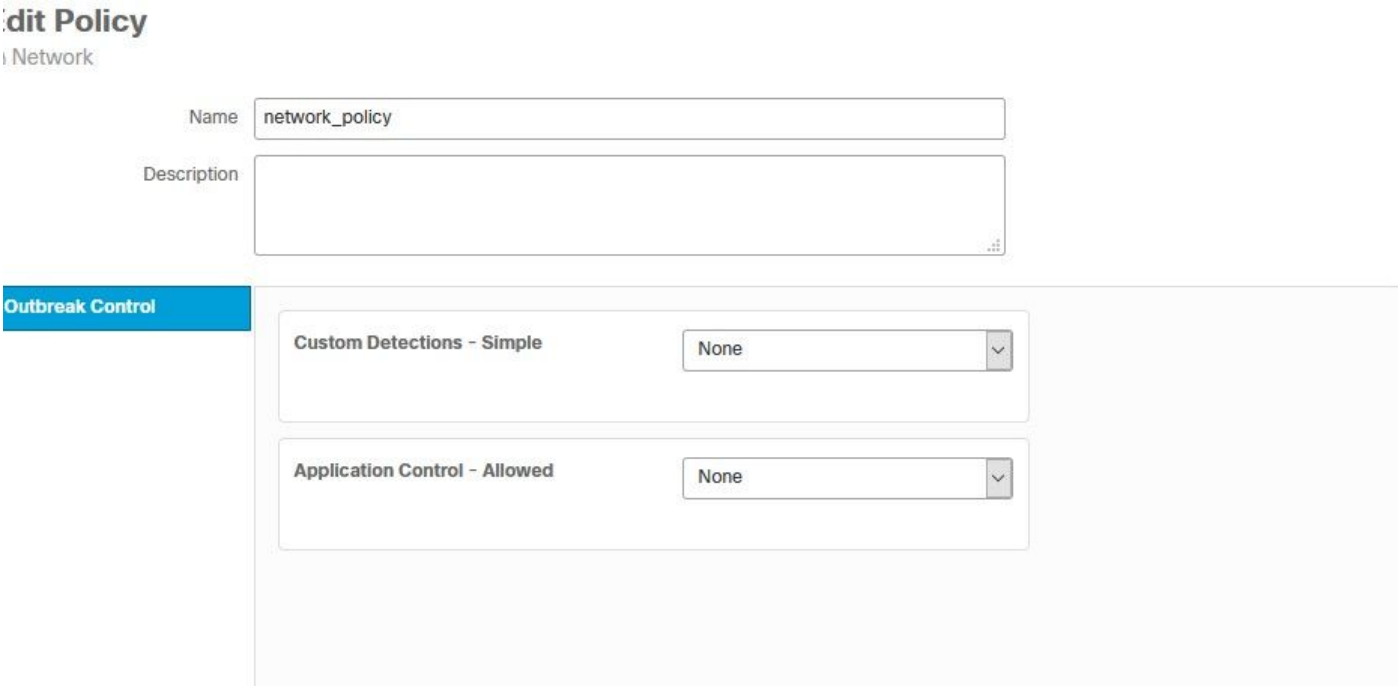


複数のWSAデバイスが登録されている場合は、ファイル分析クライアントIDを使用してそれらを識別できます。

デバイスを展開すると、そのデバイスが属するグループが表示され、適用されたポリシーとデバイスGUIDを使用してデバイストラジェクトリを表示できます。

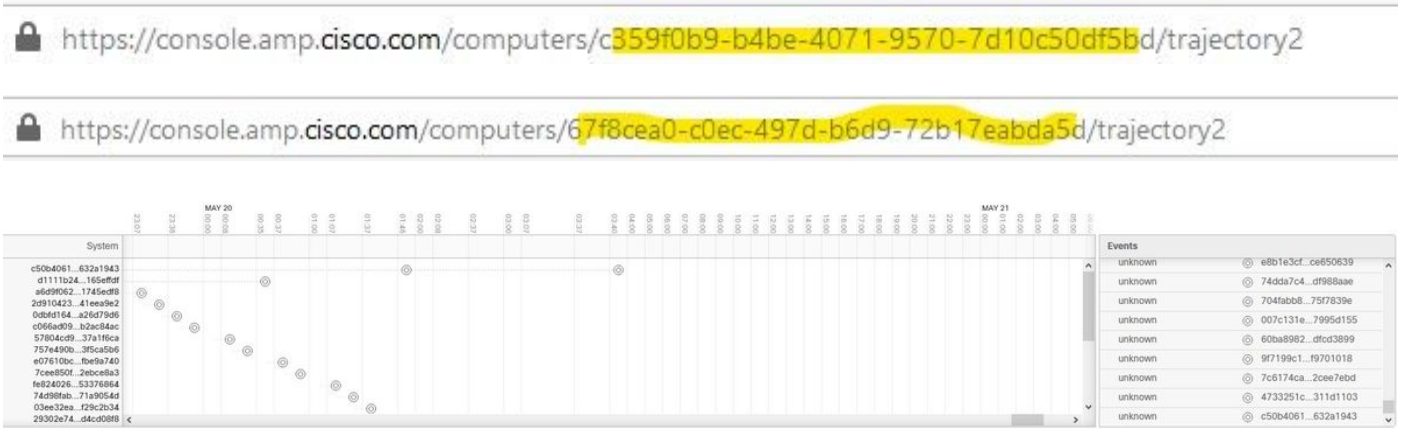


[Policy]セクションでは、デバイスに適用される[Simple Custom Detection]および[Application Control - Allowed]を設定できます。

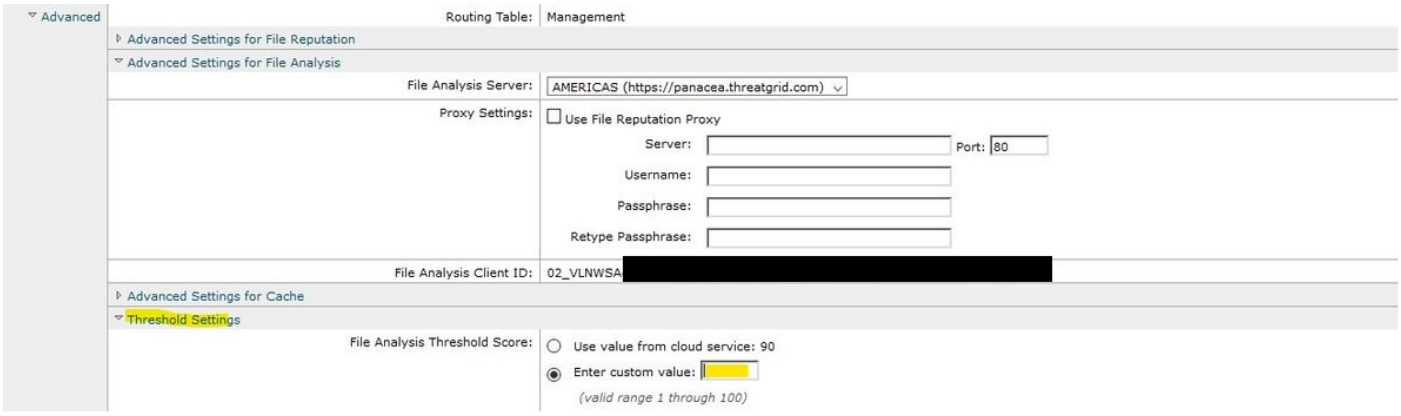


WSAの[Device Trajectory]セクションを表示するには、別のコンピュータの[Device Trajectory]を開いて[Device GUID]を使用する必要があります。

変更は、図に示すようにURLに適用されます。



Threat Gridでは、しきい値は90です。この数値を下回るファイルにスコアが付いた場合、悪意のあるファイルはプッキングされませんが、WSAでカスタムしきい値を設定できます。



トラブルシュート

WSAがAMPページにリダイレクトされない

- AMPに必要なアドレスがファイアウォールで許可されていることを確認します。ここをクリックします。
- 適切なAMPクラウドを選択していることを確認します（レガシークラウドを選択しないでください）。

WSAは指定されたSHAをブロックしません

- WSAが正しいグループにあることを確認します。
- WSAが正しいポリシーを使用していることを確認します。
- SHAがクラウド上でクリーンでないことを確認します。そうでないと、WSAはクラウドをブロックできません。

WSAがTG組織に表示されない

- 適切なTGクラウド（アメリカまたはヨーロッパ）を選択していることを確認します。
- ファイアウォールでTGに必要なアドレスが許可されていることを確認します。
- ファイル分析クライアントIDをメモします。
- [Users]セクションで検索します。
- 見つからない場合は、シスコサポートに連絡して、組織間での移行を支援してください。