エンドポイント用AMPでのWindowsポリシーの設定

内容

概要

このドキュメントでは、Advanced Malware Protection(AMP)for Endpoints Windowsポリシーで設定可能なコンポーネント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。

- 管理者権限を持つAMP for Endpointsユーザ

使用するコンポーネント

このドキュメントの情報は、AMP for Endpointsコンソールに基づくものです。

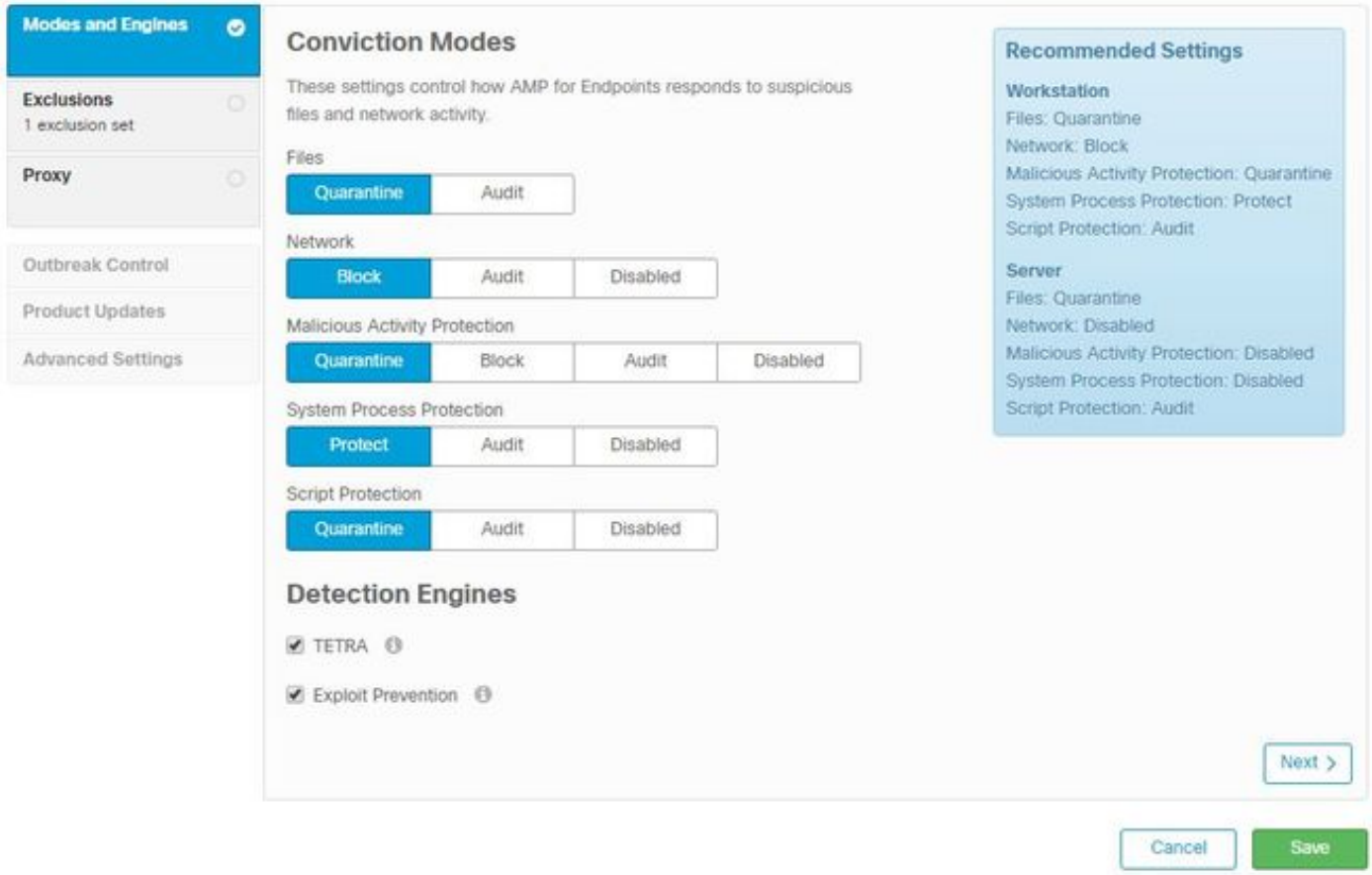
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

新しいWindowsポリシーを作成するには、[management]タブに移動し、[Policies]を選択します。

[ポリシー]セクションで、新しいWindowsポリシーを作成します。

モードとエンジン



files:AMPの主要なSHAエンジンおよびコア機能。このオプションを使用すると、ファイルスキャンと検疫を実行できます。

ネットワーク：接続を監視するデバイスフロー相関エンジン。

悪意のあるアクティビティの保護：エンドポイントをランサムウェア攻撃から保護するエンジン。

システムプロセス保護：メモリインジェクション攻撃によって、重要なWindowsシステムプロセスを妥協から保護するエンジン。

スクリプトの保護：スクリプトベースの攻撃を可視化します。

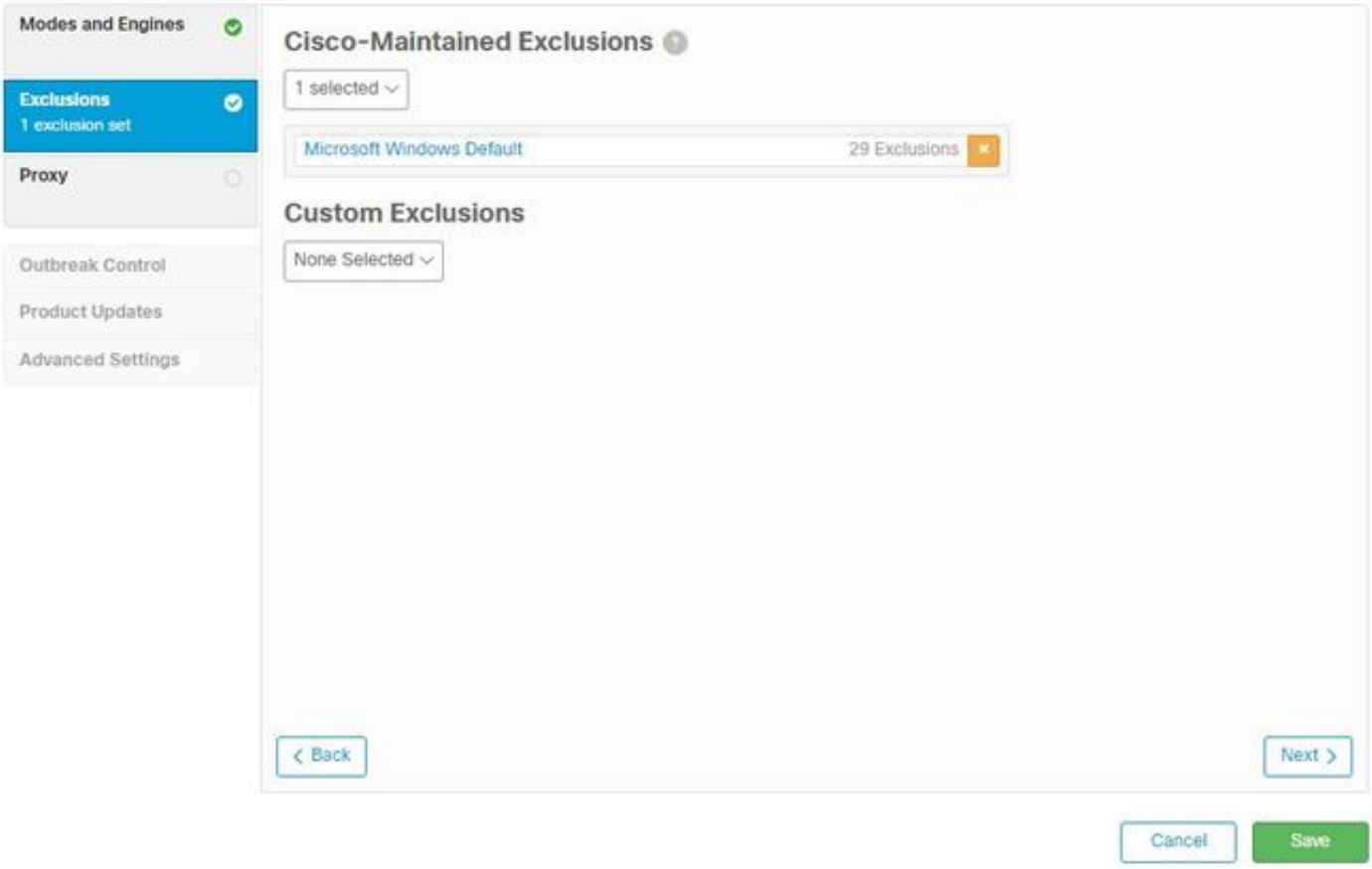
検出エンジン：

- Tetra：エンドポイントを保護するために定義をダウンロードするオフラインウイルス対策
- エクスプロイト防止：コネクタをメモリインジェクション攻撃から保護

注：ワークステーションとサーバの推奨設定ウィンドウが右側のセクションに表示されます。

[モードとエンジン]セクションの設定が完了したら、図に示すように[**次へ**]をクリックします。

除外



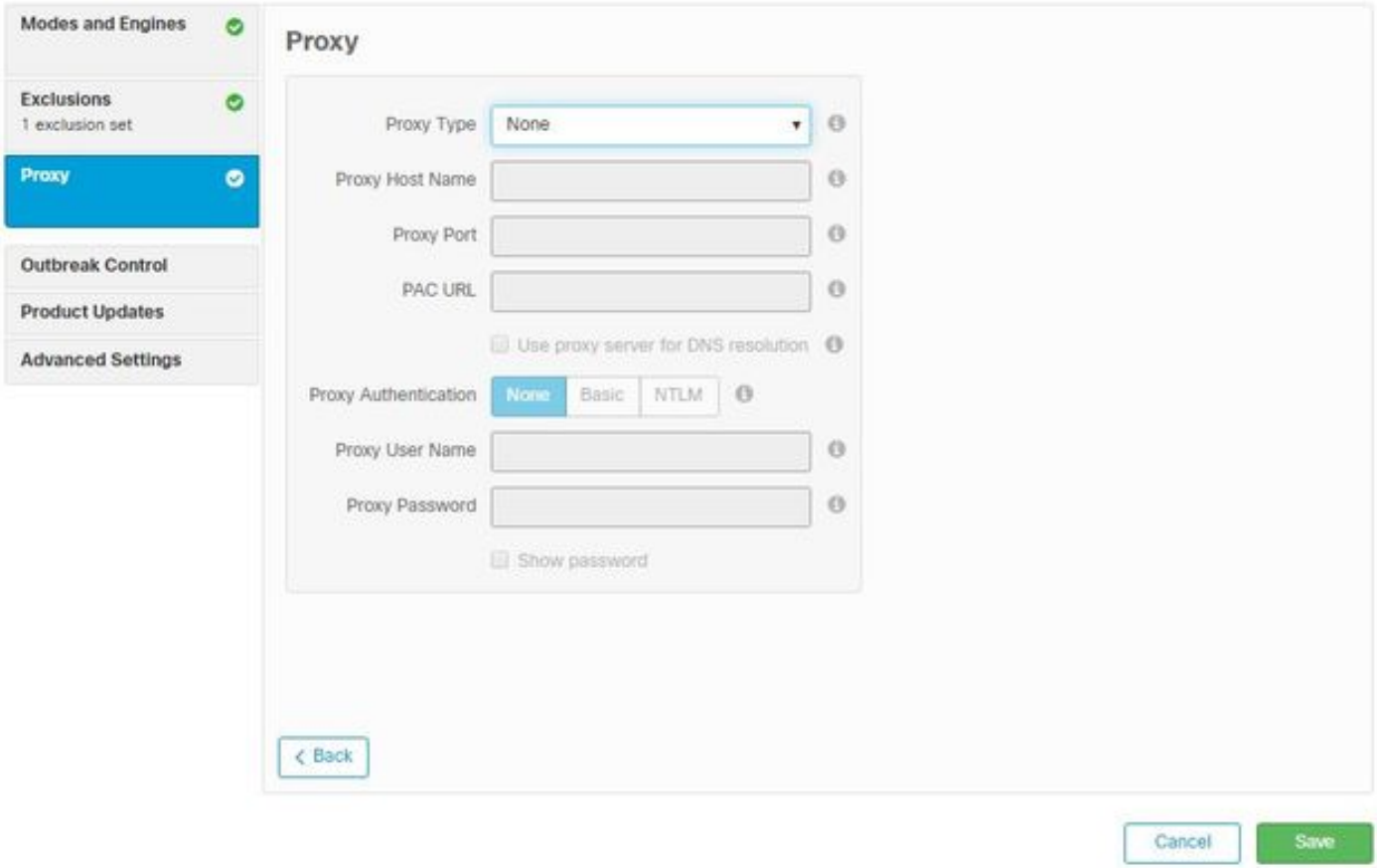
除外セクションには、シスコが管理する除外とカスタム除外が含まれます。

- シスコが提供する除外はシスコが作成および維持し、AMPによるスキャンから一般的なアプリケーションを除外して、非互換性の問題を回避できます
- カスタム除外は、ユーザ管理者が作成し、維持します

除外について詳しく知りたい場合は、このビデオで詳細な情報を見つけることができます。

除外の設定が完了したら、図に示すように[Next]をクリックします。

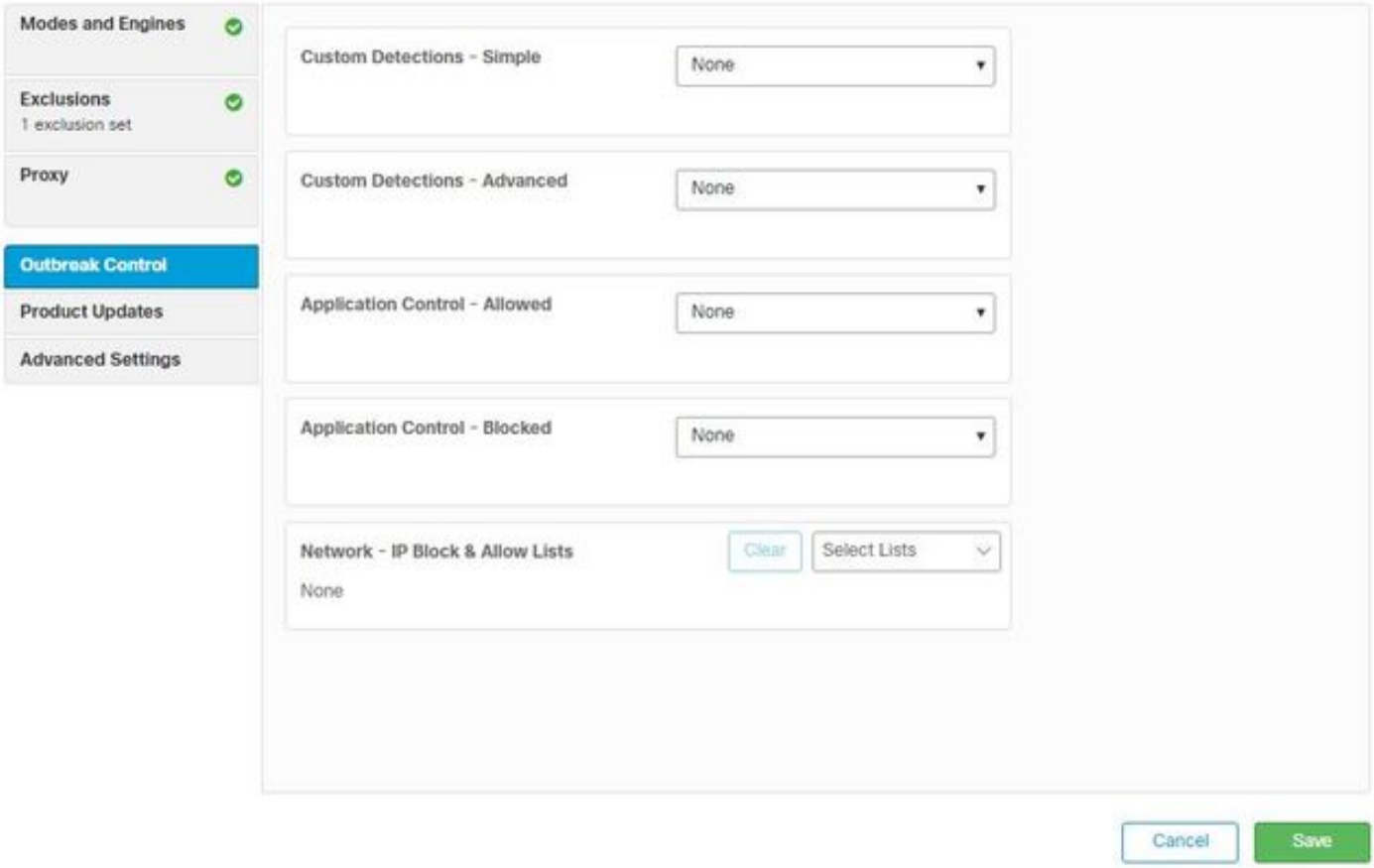
プロキシ



このセクションでは、コネクタがAMPクラウドを照会できるように、環境ごとにプロキシ設定を構成できます。

プロキシ設定を構成したら、図に示すように[Save]をクリックします。

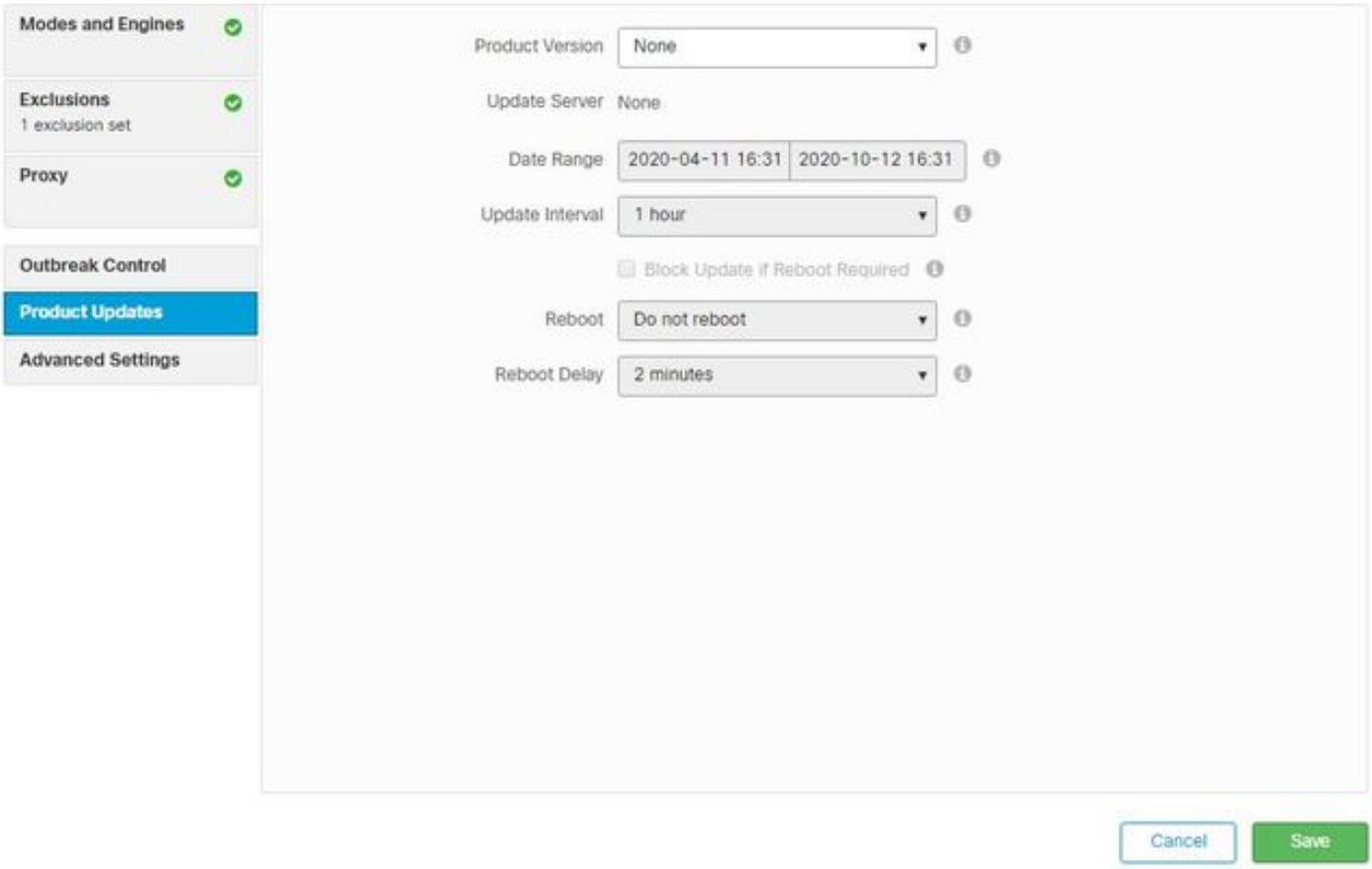
アウトブレイク制御



[Outbreak Control]セクションでは、カスタム検出を設定できます。

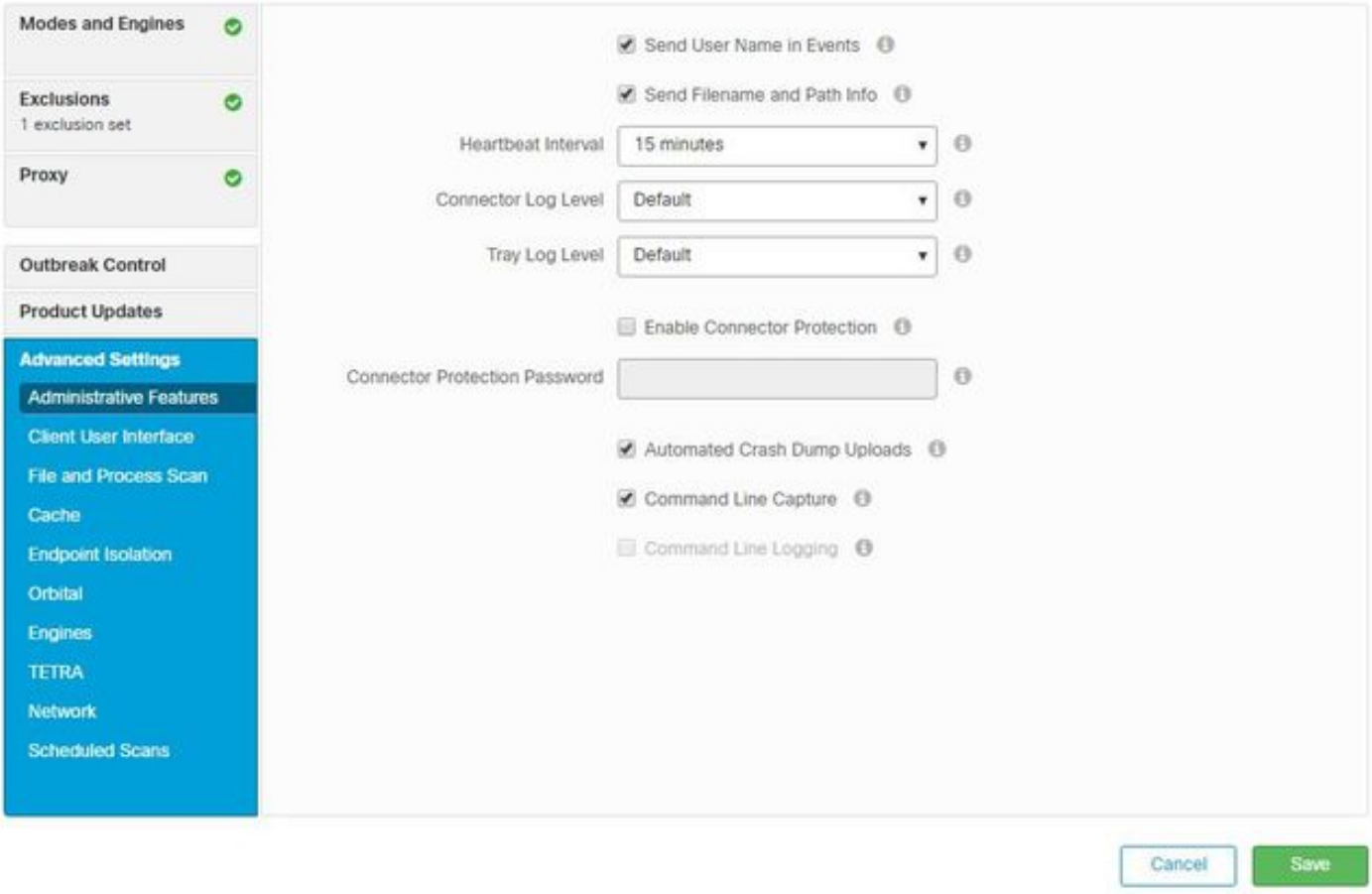
- カスタム検出：シンプル：SHAに基づいて特定のファイルをブロックできます
- カスタム検出 – 詳細：単純なSHAが不十分な場合の検出のために、シグニチャに基づいてファイルをブロックします
- [Application Allowed]および[Blocked]リスト：SHAを使用してアプリケーションを許可またはブロックする
- ネットワーク – IPブロックと許可リスト：カスタムIPアドレス検出を定義するためにデバイスフロー相関(DFC)とともに使用される

製品の更新



[Product Update（製品の更新）]セクションで、新しい更新のオプションを設定します。バージョン、日付範囲を選択して、更新を実行したり、再起動のオプションを選択できます。

高度な設定



管理機能：コネクタがクラウドにポリシーの変更を照会する頻度を設定します。

クライアントユーザインターフェイス：AMPがインストールされているデバイスでの通知の表示を制御できます。

ファイルおよびプロセススキャン：リアルタイム保護オプション、コネクタによるファイルの配置の確認方法、および許可される最大ファイルサイズを設定します。

Cache:キャッシュの存続可能時間(TTL)設定。

エンドポイントの分離では、AMPコネクタがインストールされているデバイスを分離する機能を有効にして設定できます。

軌道オプションは、軌道の高度な検索を有効にします。

エンジン：ETHOSの設定ファイル・グループ化エンジン、SPEROマシンベースの学習システム。

オフラインエンジンのTETRA設定。

[Network]:[Device Flow Correlation]オプションを有効にします。

「スケジュールされたスキャン」セクションでは、コネクタで実行するスキャンのタイミングと種類を設定できます。

変更の保存

変更を実行した後、[Save]をクリックしてポリシーに適用されていることを確認します。

このドキュメントに含まれている情報は、『AMP for Endpointsの』ビデオの「Windowsポリシーの設定」にも記載されています。

関連情報

- ポリシー設定の詳細については、『ユーザガイド』を参照してください
- テクニカル サポートとドキュメント – Cisco Systems