# 在面向终端的AMP中配置Windows策略

## 目录



## 简介

本文档介绍在面向终端的高级恶意软件防护(AMP)Windows策略中可配置的组件。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 具有管理员权限的面向终端的AMP用户

### 使用的组件

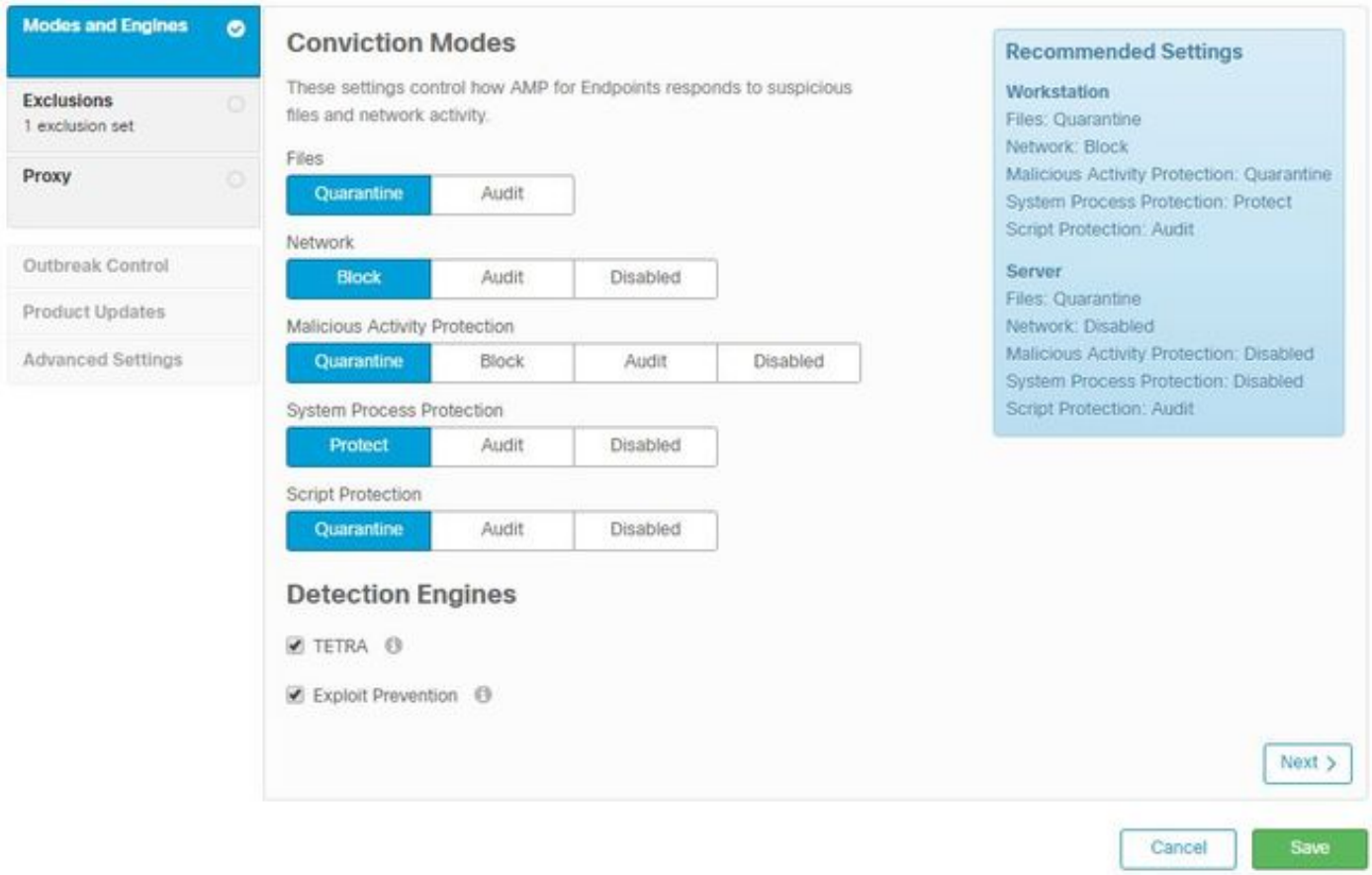
本文档中的信息基于面向终端的AMP控制台。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 配置

要创建新的Windows策略，请导航至管理选项卡并选择策略。在策略部分，创建新的Windows策略。

### 模式和引擎




文件：AMP的主要SHA引擎和核心功能。此选项允许文件扫描和隔离。

网络:监控连接的设备流关联引擎。

恶意活动保护：用于保护终端免受勒索软件攻击的引擎。

系统进程保护：用于保护关键Windows系统进程免受内存注入攻击危害的引擎。

脚本保护：提供对基于脚本的攻击的可视性。

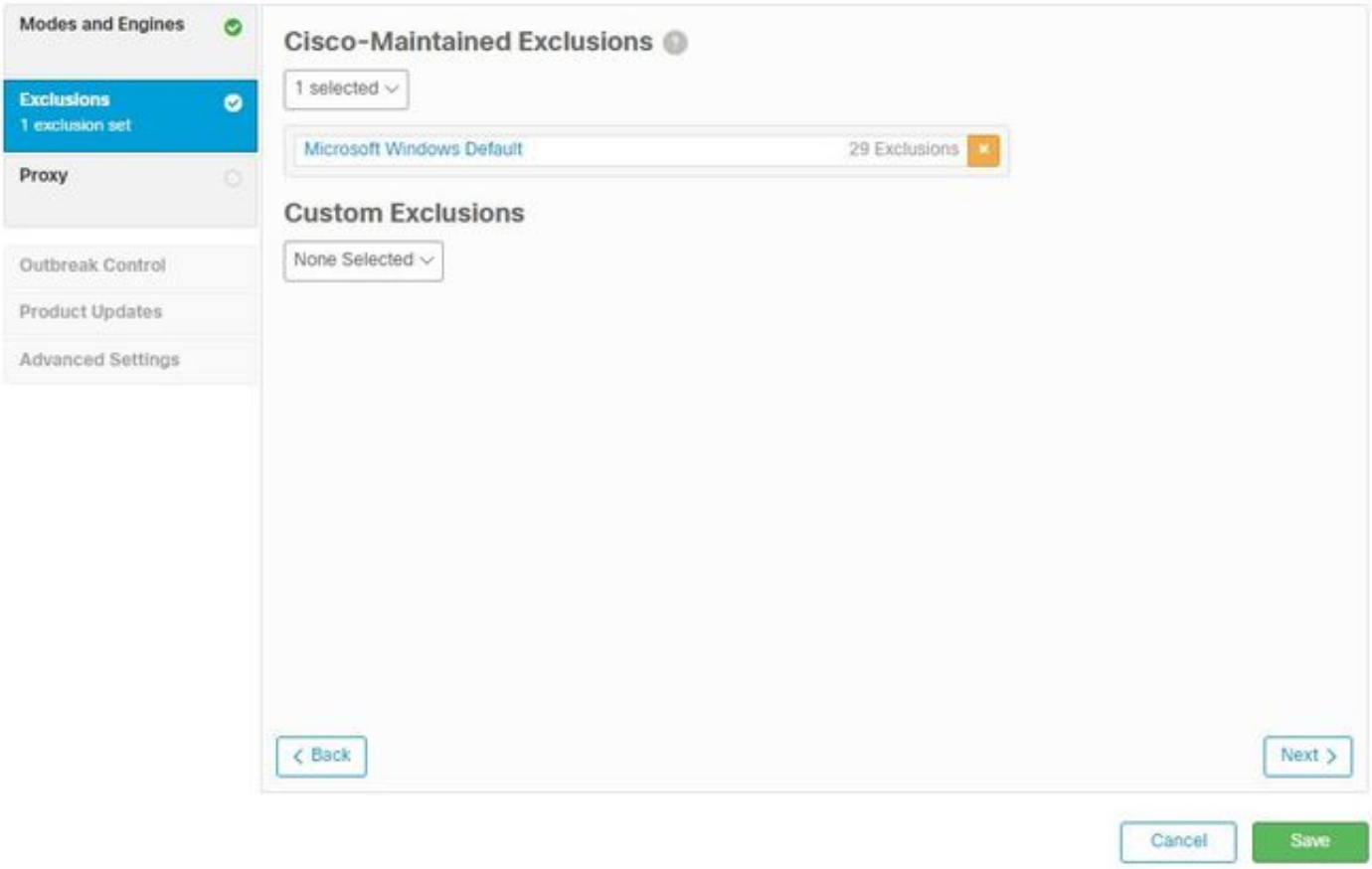
检测引擎：

- TETRA：下载定义以保护终端的脱机防病毒软件
- 漏洞攻击防护：保护连接器免受内存注入攻击

**注意：**右侧部分显示了建议的工作站和服务器设置窗口。

配置“模式和引擎”部分后，单击**下一步**，如图所示。

## 排除



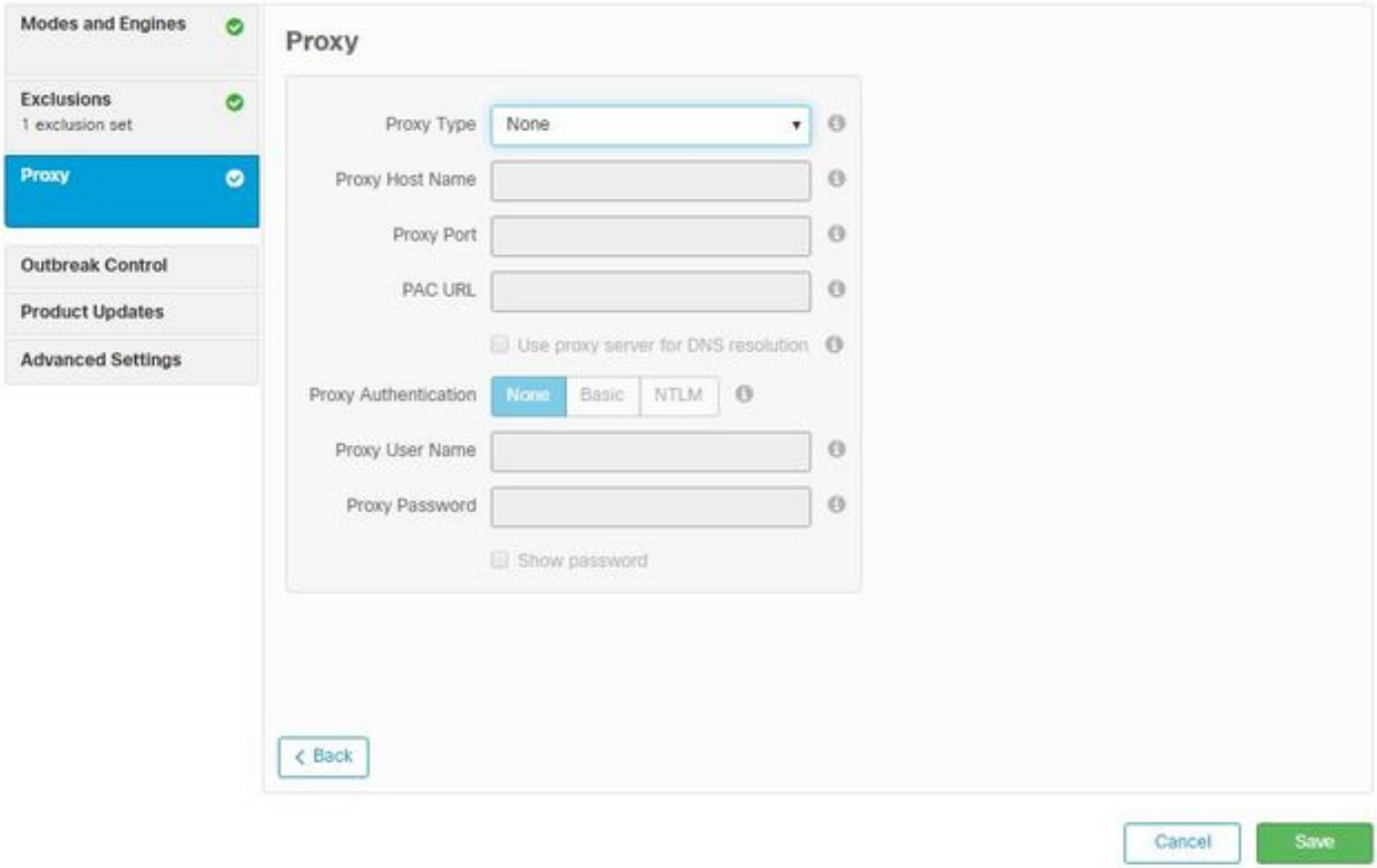

排除部分包含思科维护的排除项和自定义排除项：

- 思科维护的排除项由思科创建和维护，允许您从AMP扫描中排除常见应用，以避免出现不兼容问题
- 自定义例外项由用户管理员创建和维护

如果您想了解有关排除项的更多信息，可以在此视频中找到更多信息。

完成排除配置后，单击**Next**，如图所示。

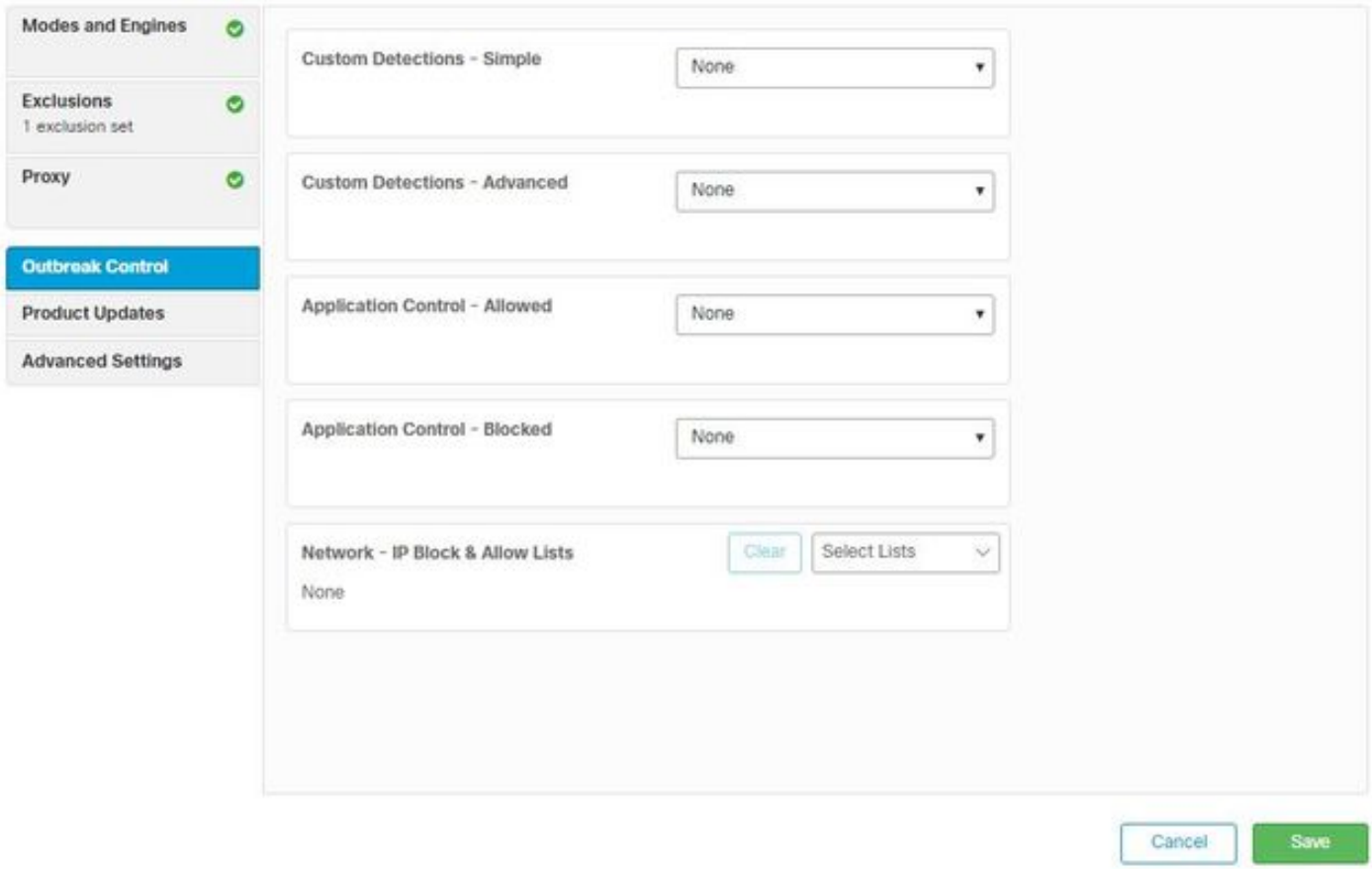
## 代理




在本节中，您可以根据环境配置代理设置，以允许连接器查询AMP云。

配置代理设置后，单击**Save**，如图所示。

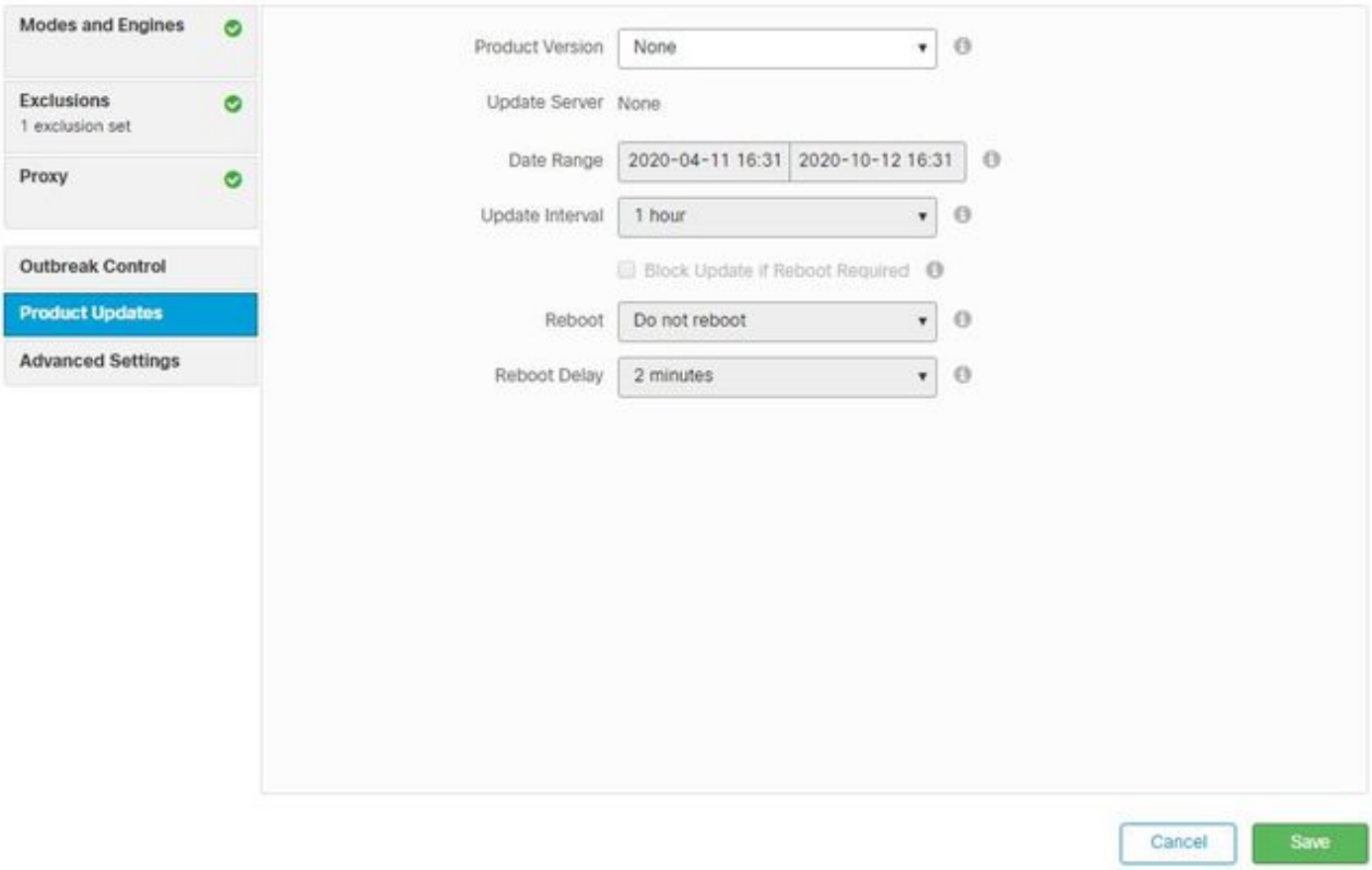
## 爆发控制



在爆发控制部分，可以配置自定义检测：

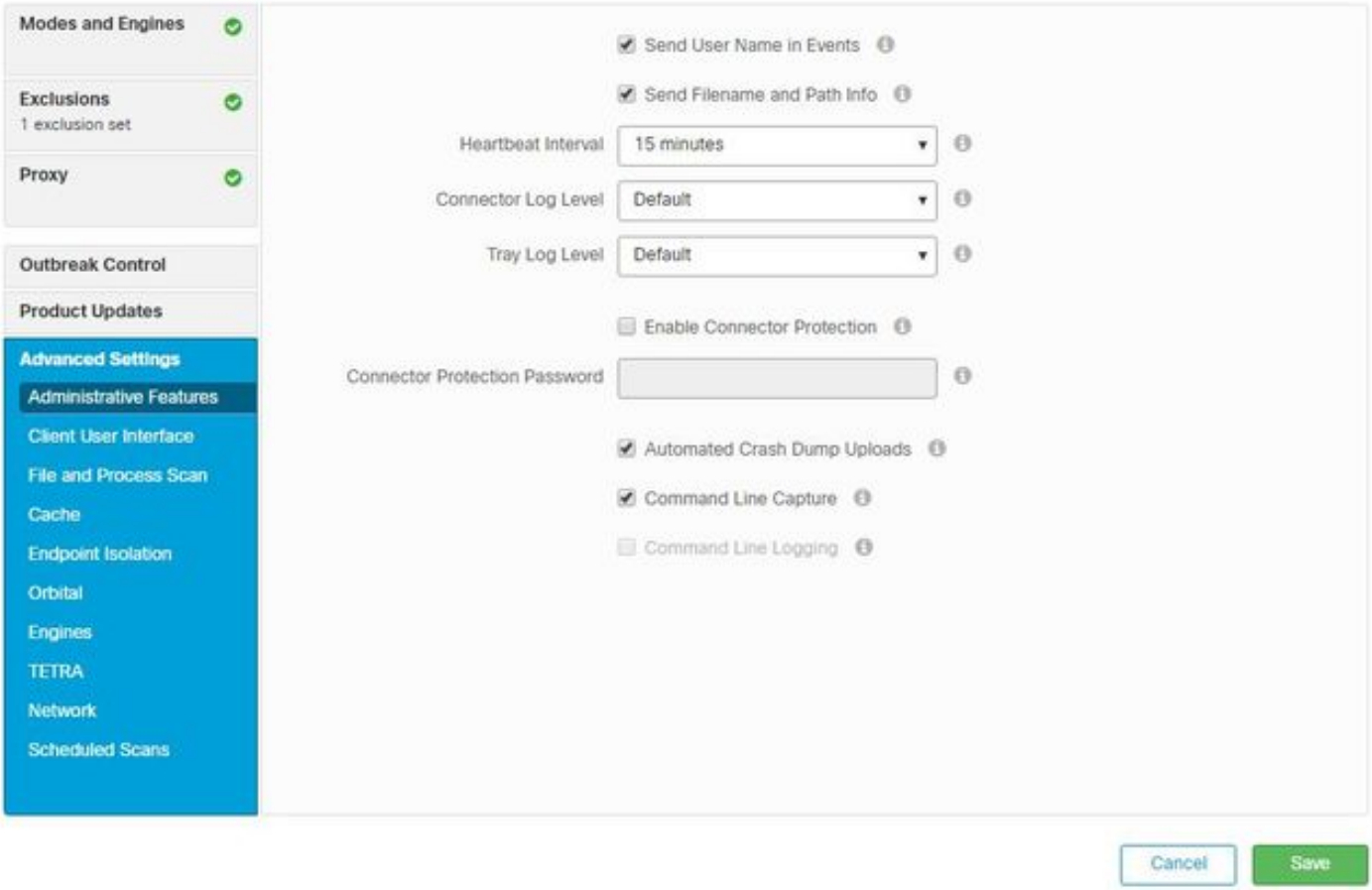
- 自定义检测 — 简单：允许您根据特定文件的SHA阻止特定文件
- 自定义检测 — 高级：根据签名阻止文件，以在简单SHA不足时进行检测
- 允许和阻止的应用列表：允许或阻止使用SHA的应用
- 网络 — IP阻止和允许列表：与设备流关联(DFC)一起用于定义自定义IP地址检测

## 产品更新




在“产品更新”(Product Update)部分，设置新更新的选项。您可以选择版本、日期范围以滚动更新和重新启动选项。

## 高级设置




管理功能：配置连接器查询云以查找策略更改的频率。

客户端用户界面：允许您控制在安装AMP的设备中显示通知。

文件和进程扫描：配置实时保护选项、连接器如何检查文件性质和允许的最大文件大小。

缓存：缓存的生存时间配置。

终端隔离功能允许您启用和配置该功能，以隔离安装了AMP连接器的设备。

轨道选项支持轨道先进搜索。

引擎：ETHOS设置；文件分组引擎和SPERO;机器学习系统。

离线引擎的TETRA配置。

网络启用设备流关联选项。

在“计划扫描”(Scheduled Scans)部分，可以配置要在连接器中运行的扫描的时间和类型选项。

### 保存更改

执行任何更改后，请单击**Save**以确保这些更改已应用到策略。

您还可以在面向终端的AMP视频的Windows策略配置中找到本文档中包含的信息。

## 相关信息

- 有关策略配置的详细信息，请导航至《用户指南》
- **技术支持和文档 - Cisco Systems**