Configurar a política do Windows na AMP para endpoints

Contents

Introduction

Este documento descreve componentes configuráveis na AMP (Advanced Malware Protection, Proteção avançada contra malware) para a política de Windows de endpoints.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Usuário da AMP para endpoints com privilégios de administrador

Componentes Utilizados

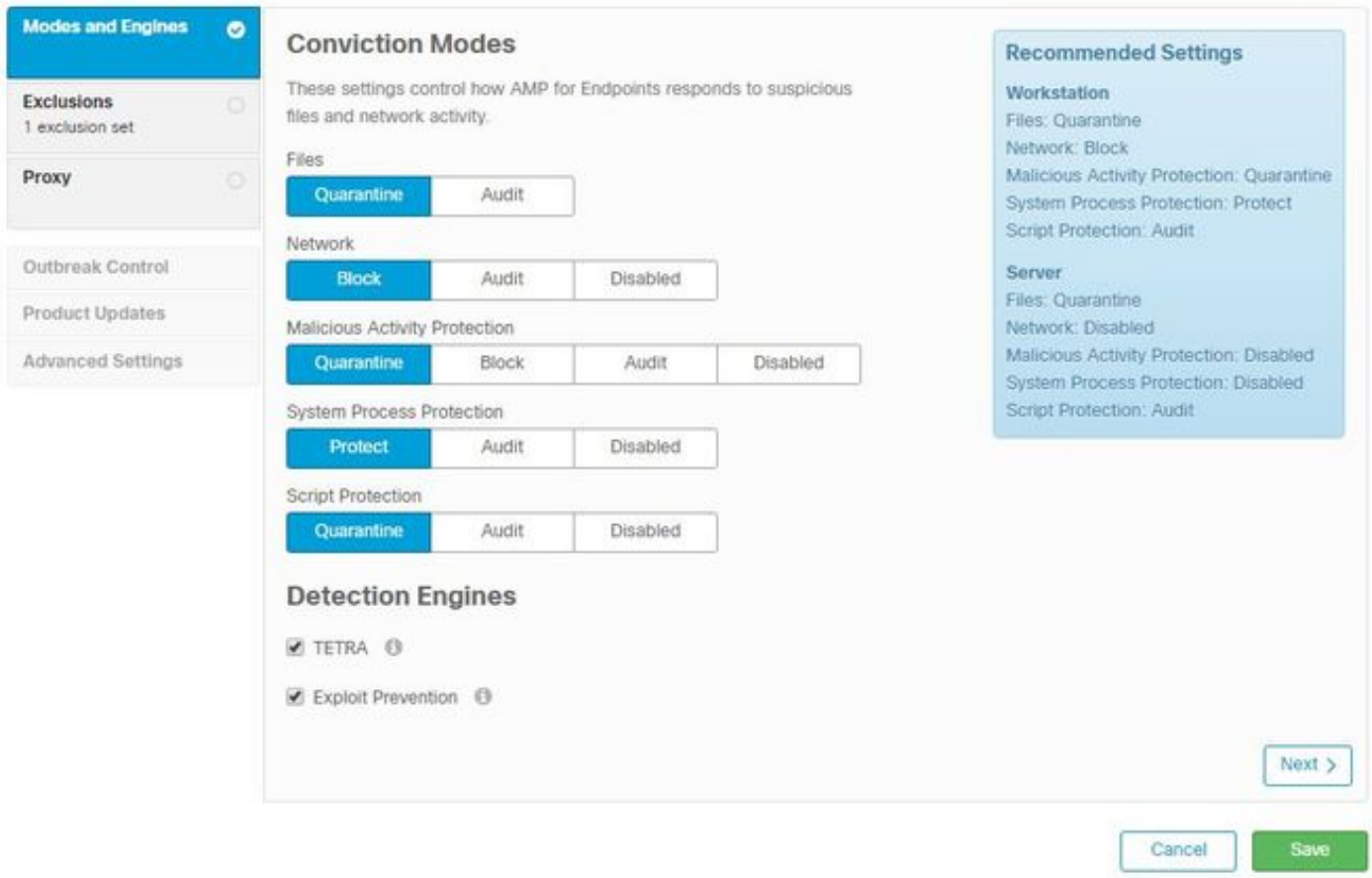
As informações neste documento são baseadas no console do AMP for Endpoints.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Para criar uma nova política do Windows, navegue até a guia Gerenciamento e selecione Políticas. Na seção de política, crie uma nova política do Windows.

Modos e mecanismos



Arquivos: O principal mecanismo SHA e a funcionalidade principal do AMP. Esta opção permite a pesquisa de arquivos e a quarentena.

Rede: O mecanismo de correlação de fluxo de dispositivo que monitora as conexões.

Proteção de atividade mal-intencionada: Mecanismo que protege o endpoint contra ataques de ransomware.

Proteção do processo do sistema: Mecanismo que protege os processos críticos do sistema Windows contra comprometimentos através de ataques de injeção de memória.

Proteção de script: Fornece visibilidade dos ataques baseados em scripts.

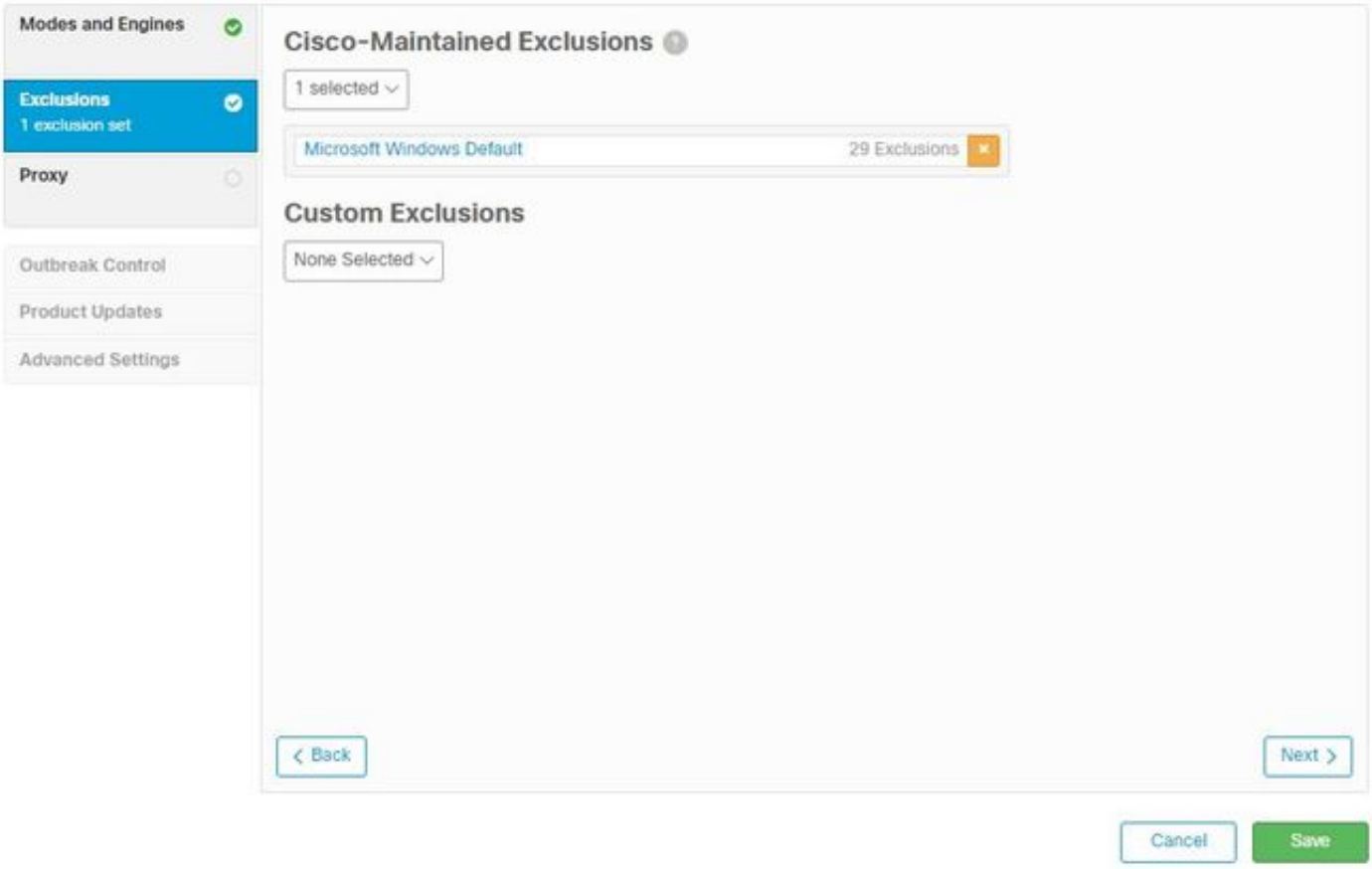
Mecanismos de detecção:

- Tetra: Antivírus off-line que baixa definições para proteger o endpoint
- Prevenção de exploração: Protege os conectores contra ataques de injeção de memória

Note: Uma janela de configurações recomendadas para estações de trabalho e servidores é exibida na seção à direita.

Após a configuração da seção Modos e Mecanismo, clique em **Avançar**, como mostrado na imagem.

Exclusões



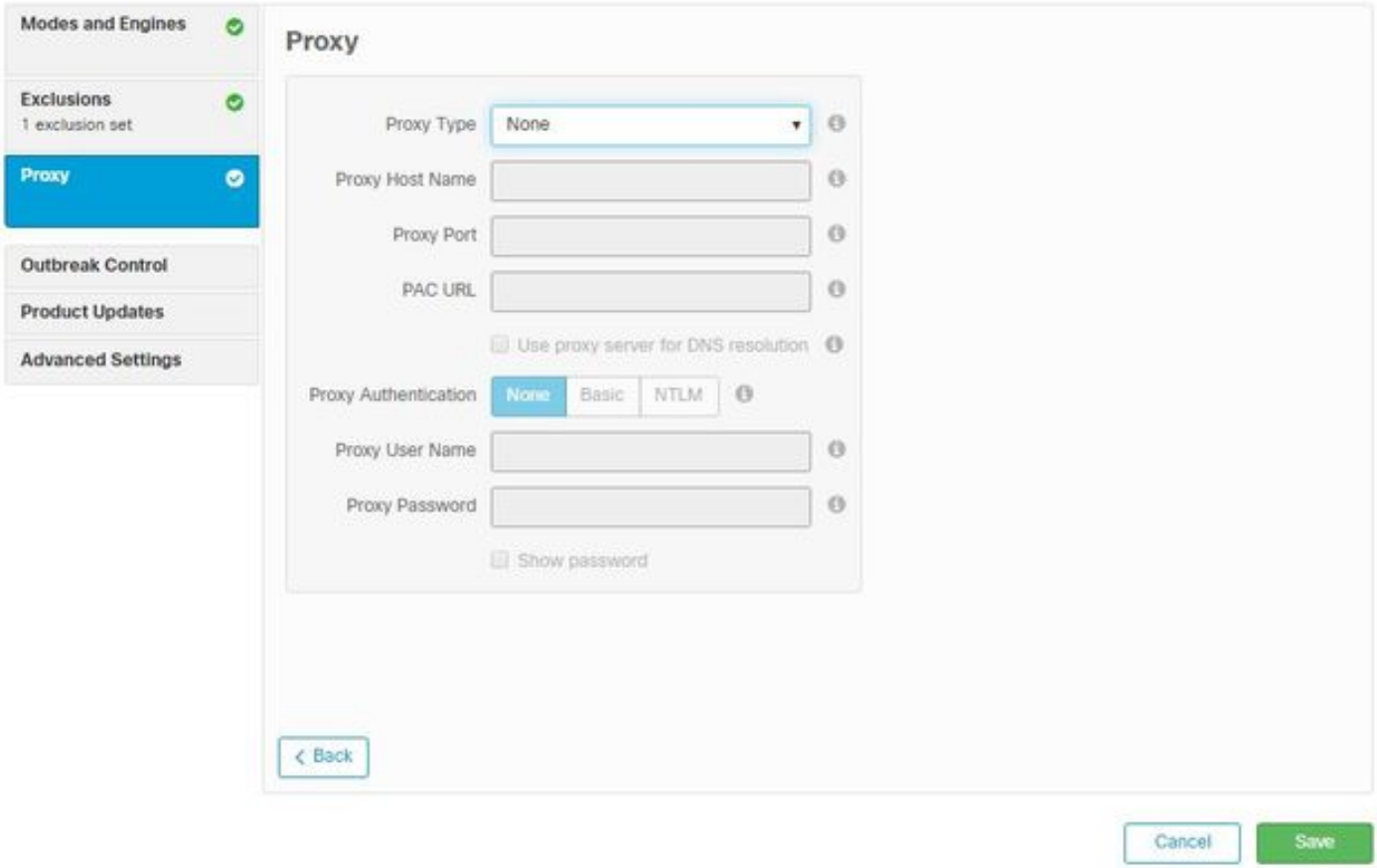
A seção de exclusões contém exclusões mantidas pela Cisco e exclusões personalizadas:

- As exclusões mantidas pela Cisco são criadas e mantidas pela Cisco e permitem que você exclua aplicativos comuns das verificações da AMP para evitar problemas de incompatibilidade
- As exclusões personalizadas são criadas e mantidas pelo administrador do usuário

Se quiser saber mais sobre exclusões, você pode encontrar mais informações neste vídeo.

Depois de concluir a configuração de Exclusões, clique em **Avançar**, como mostrado na imagem.

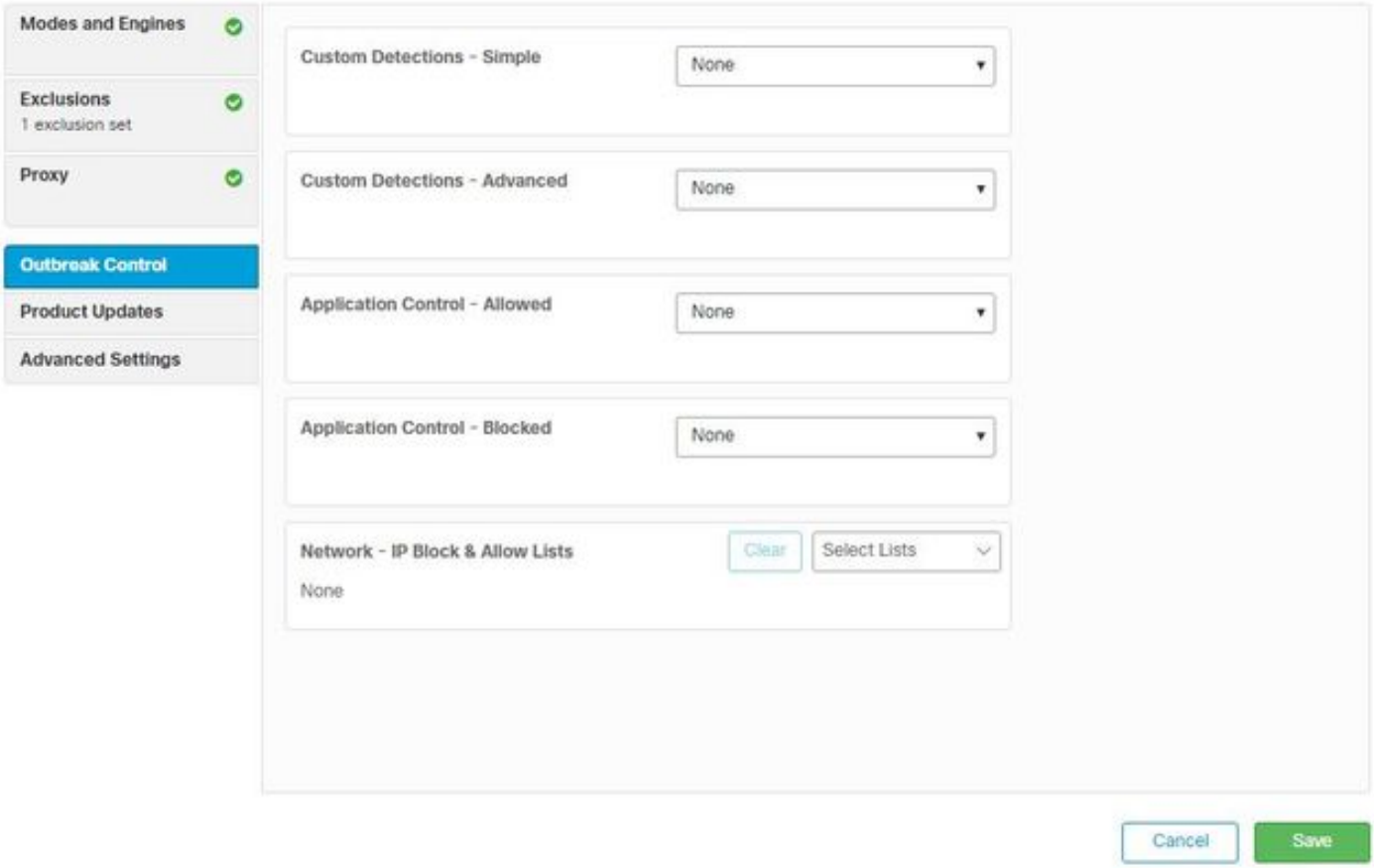
Proxy



Nesta seção, você pode definir as configurações de proxy por ambiente para permitir que o conector consulte a nuvem AMP.

Depois de configurar as definições de Proxy, clique em **Salvar**, como mostrado na imagem.

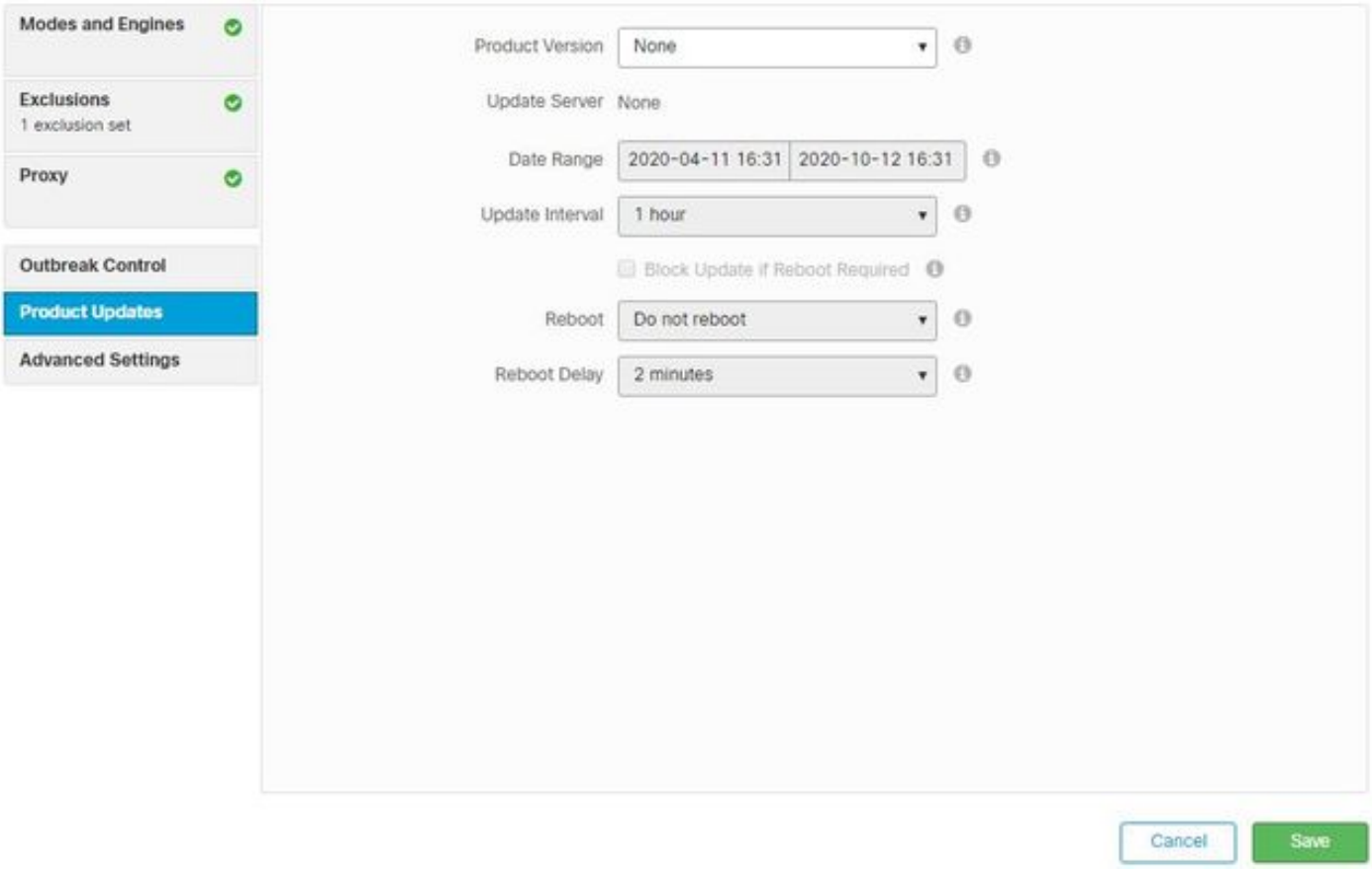
Controle de epidemia



Na seção Controle de epidemia, você pode configurar detecções personalizadas:

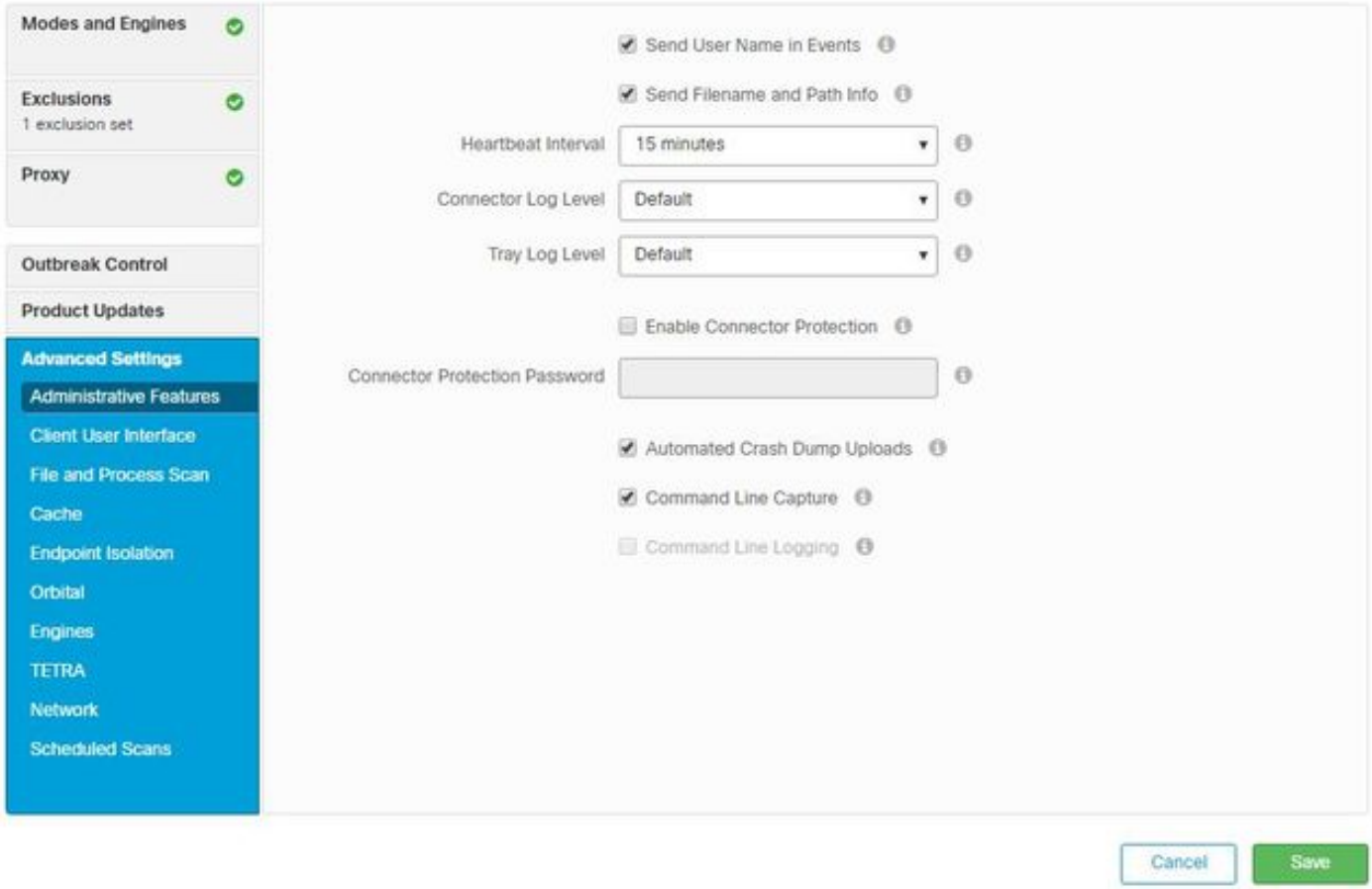
- Detecções personalizadas - Simples: Permite bloquear arquivos específicos com base em seu SHA
- Detecções personalizadas - Avançadas: Bloqueia arquivos com base em assinaturas, para detecções quando um SHA simples não é suficiente
- Aplicativo permitido e listas bloqueadas: Permite ou bloqueia aplicativos com SHAs
- Rede - Bloqueio IP e Listas de permissão: usado com Device Flow Correlation (DFC) para definir detecções de endereços IP personalizados

Atualizações de produtos



Na seção Atualização do produto, são definidas opções para novas atualizações. Você pode escolher uma versão, um intervalo de datas para a rolagem de atualizações e opções para uma reinicialização.

Configurações avançadas



Recursos administrativos: Configura a frequência com que o conector consulta a nuvem para alterações na política.

Interface do usuário cliente: Permite controlar a exibição de notificações em seus dispositivos onde o AMP está instalado.

Verificação de arquivos e processos: configura opções de proteção em tempo real, como os conectores verificam a disposição dos arquivos e o tamanho máximo permitido para esses arquivos.

Cache: configuração de tempo de vida útil para cache.

O isolamento do endpoint permite habilitar e configurar o recurso para isolar dispositivos com o conector AMP instalado.

A opção Orbital permite a pesquisa avançada orbital.

Motores: Configurações para ETHOS; um mecanismo de agrupamento de arquivos e SPERO; um sistema de aprendizagem baseado em máquina.

Configuração de TETRA para o mecanismo off-line.

Rede Ativa as opções de Correlação de Fluxo de Dispositivo.

Na seção Scheduled Scans, você pode configurar as opções para quando e para que tipos de digitalizações deseja executar nos conectores.

Salvar alterações

Depois de efetuar as alterações, clique em **Salvar** para garantir que elas sejam aplicadas à diretiva.

Você também pode encontrar as informações contidas neste documento no vídeo Configuração de política do Windows na AMP para endpoints.

Informações Relacionadas

- Para obter mais informações sobre a configuração da política, navegue até o Guia do usuário
- **Suporte Técnico e Documentação - Cisco Systems**