Configuración de la política de Windows en AMP para terminales

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Configurar](#)
[Modos y motores](#)
[Exclusiones](#)
[Proxy](#)
[Control de brotes](#)
[Actualizaciones de productos](#)
[Parámetros avanzados](#)
[Guardar cambios](#)
[Información Relacionada](#)

Introducción

Este documento describe los componentes configurables en la política de Windows de protección frente a malware avanzado (AMP) para terminales.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Usuario de AMP para terminales con privilegios de administrador

Componentes Utilizados

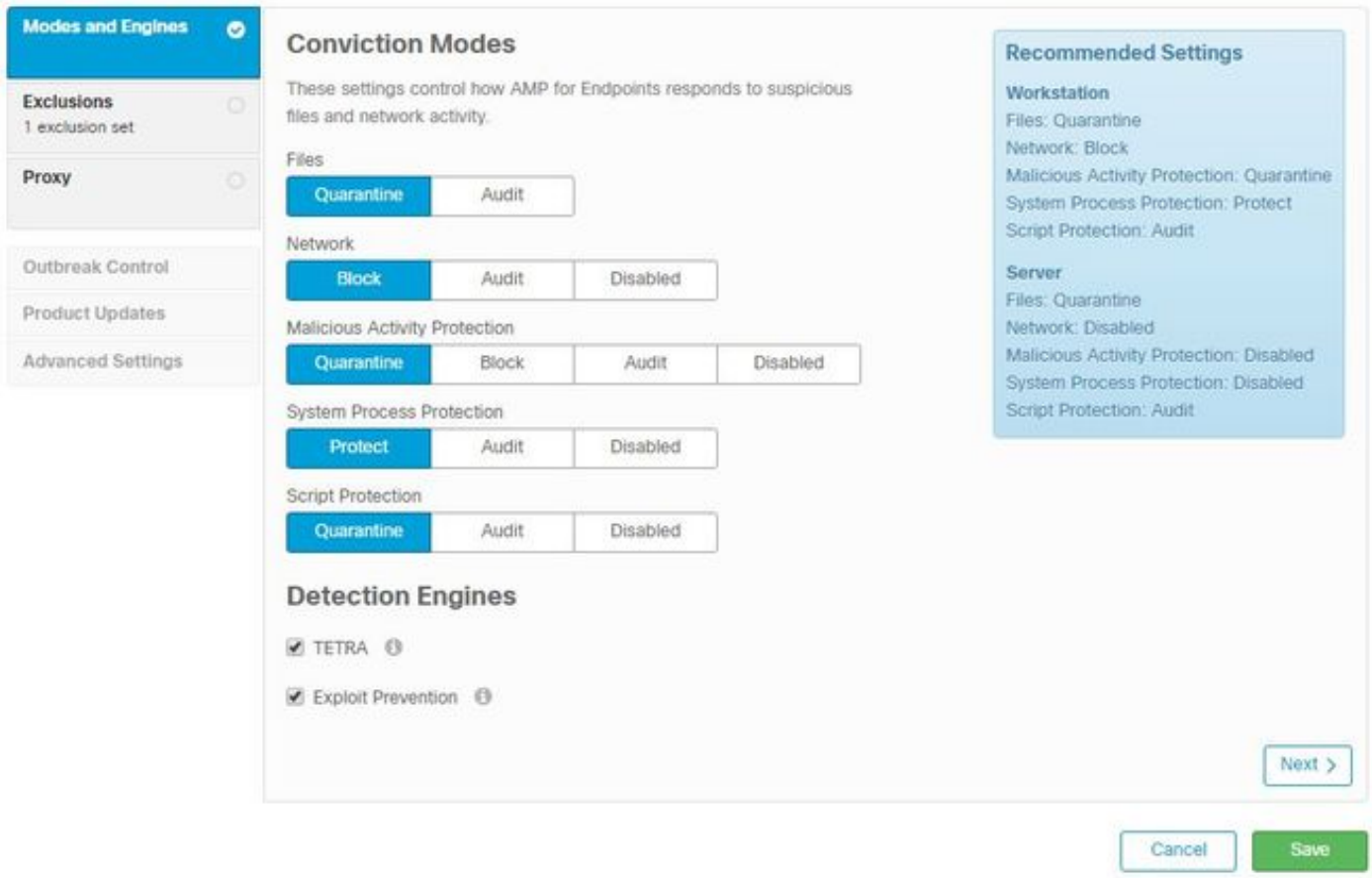
La información de este documento se basa en AMP para la consola de terminales.

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 crear una nueva política de Windows, navegue hasta la ficha de administración y seleccione Políticas. En la sección de directivas, cree una nueva directiva de Windows.

Modos y motores



Archivos: El principal motor SHA y la funcionalidad principal de AMP. Esta opción permite escanear archivos y poner en cuarentena.

Red: El motor de correlación de flujo de dispositivos que supervisa las conexiones.

Protección de la actividad maliciosa: Motor que protege el terminal de ataques de ransomware.

Protección del proceso del sistema: Motor que protege los procesos críticos del sistema de Windows de los riesgos a través de ataques de inyección de memoria.

Protección de secuencias de comandos: Proporciona visibilidad de los ataques basados en secuencias de comandos.

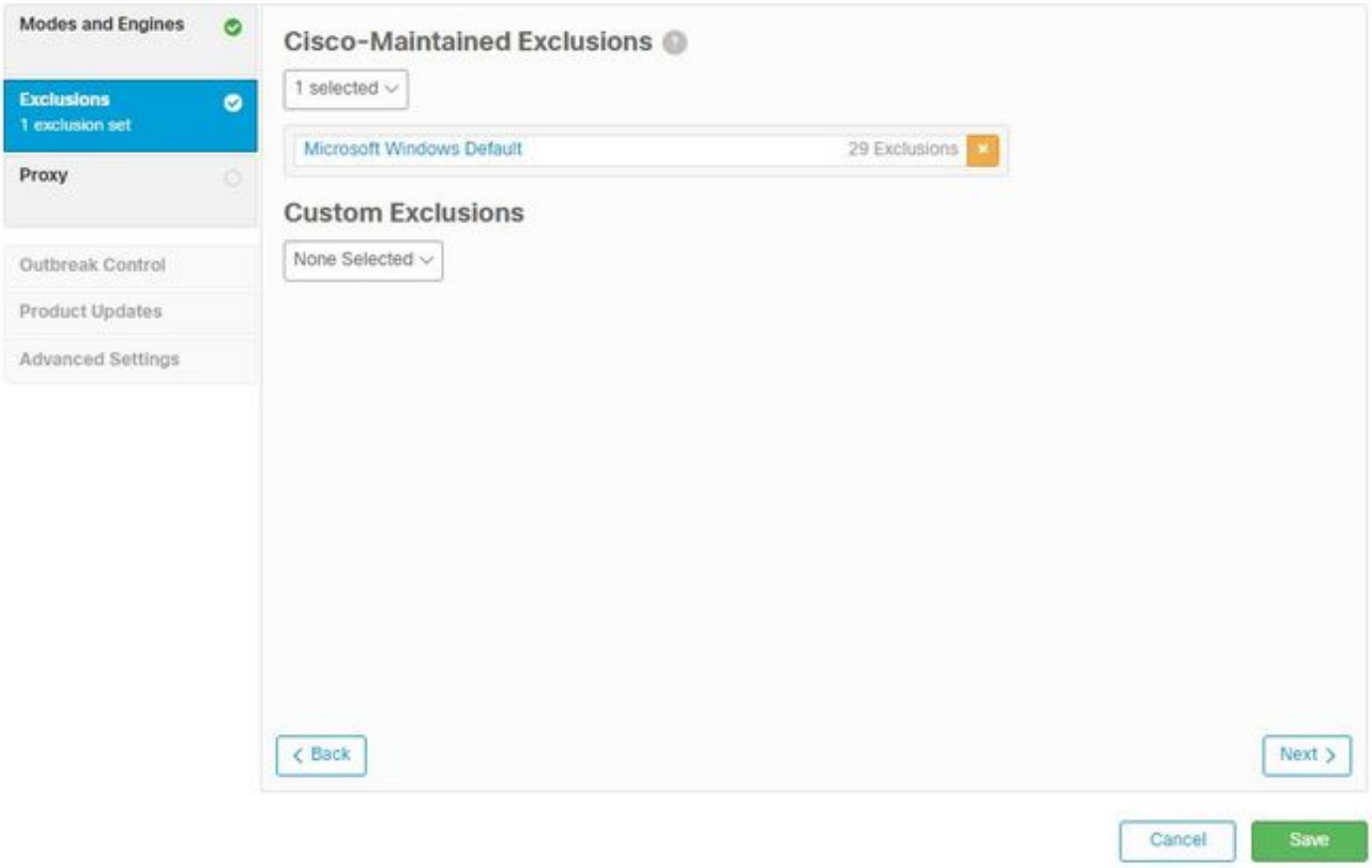
Motores de detección:

- Tetra: antivirus sin conexión que descarga definiciones para proteger el terminal
- Prevención de ataques: Protege los conectores de ataques de inyección de memoria

Nota: En la sección derecha se muestra una ventana con la configuración recomendada para estaciones de trabajo y servidores.

Después de la configuración de la sección Modos y Motor, haga clic en **Siguiente**, como se muestra en la imagen.

Exclusiones



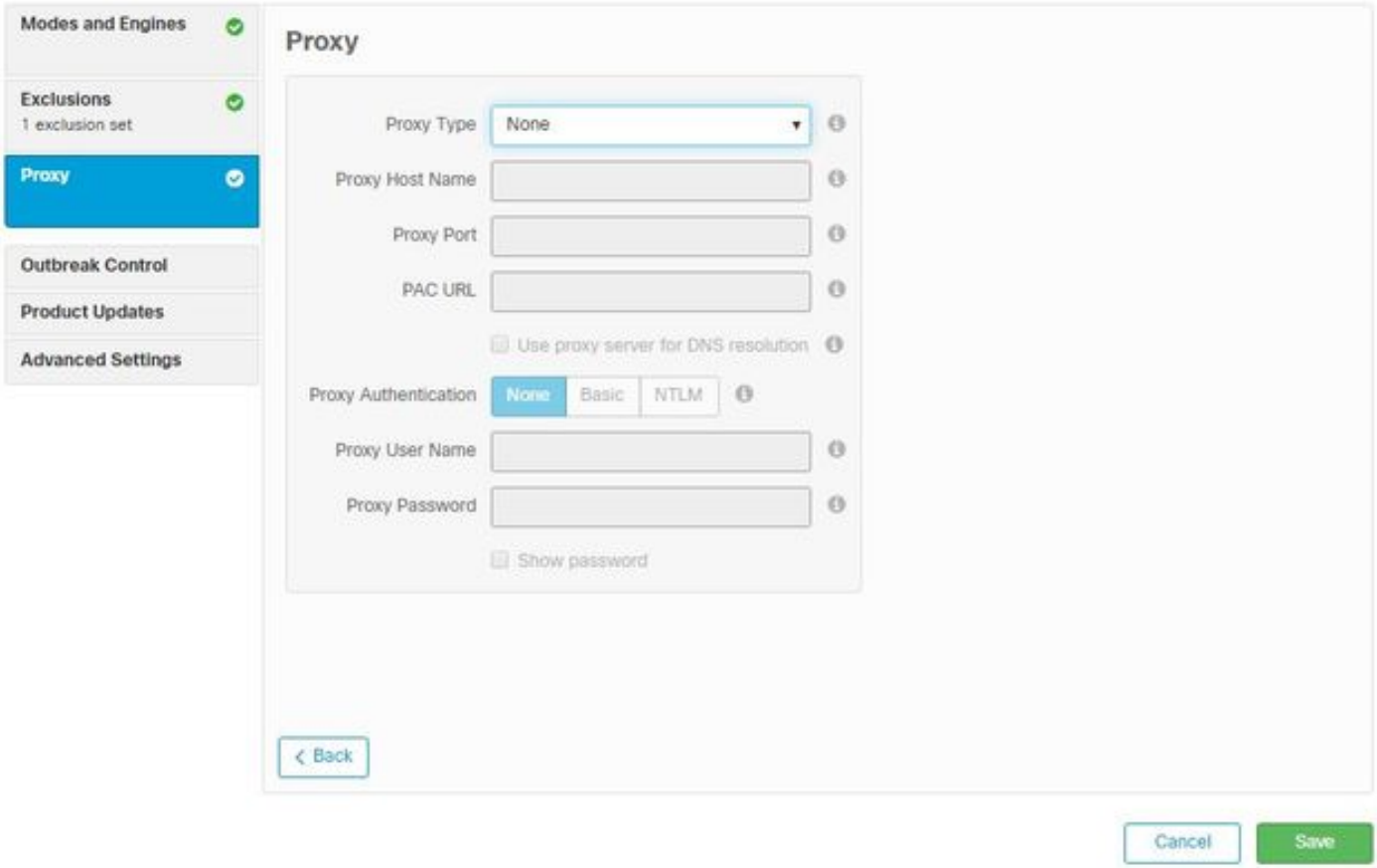
La sección de exclusiones contiene exclusiones y exclusiones personalizadas mantenidas por Cisco:

- Cisco crea y mantiene exclusiones mantenidas por Cisco que le permiten excluir aplicaciones comunes de los análisis realizados por AMP para evitar problemas de incompatibilidad
- El administrador de usuarios crea y mantiene las exclusiones personalizadas

Si desea obtener más información sobre exclusiones, puede encontrar más información en este vídeo.

Una vez finalizada la configuración de Exclusions, haga clic en **Next**, como se muestra en la imagen.

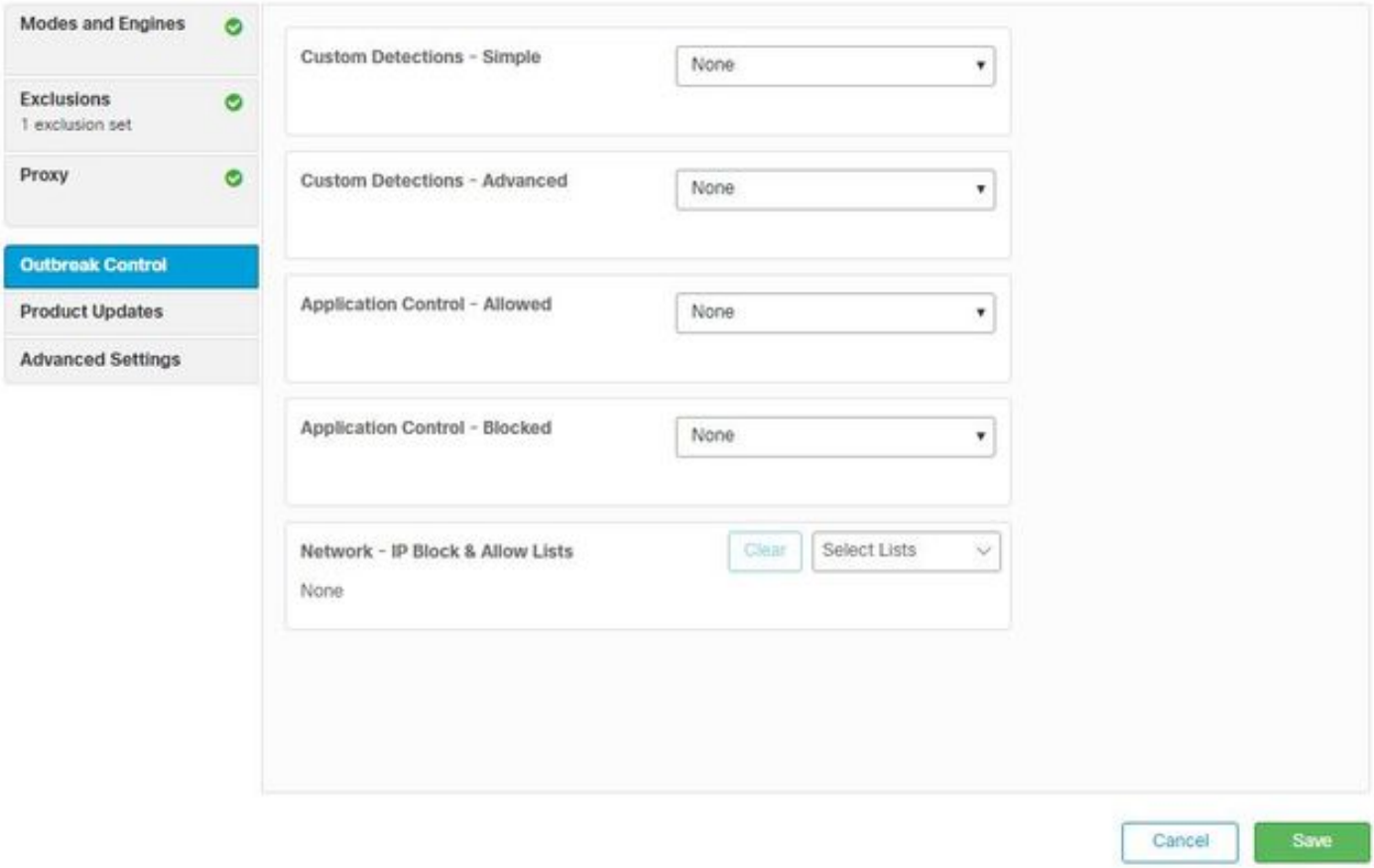
Proxy



En esta sección, puede configurar los parámetros de proxy por su entorno para permitir que el conector consulte la nube de AMP.

Después de configurar los parámetros de Proxy, haga clic en **Guardar**, como se muestra en la imagen.

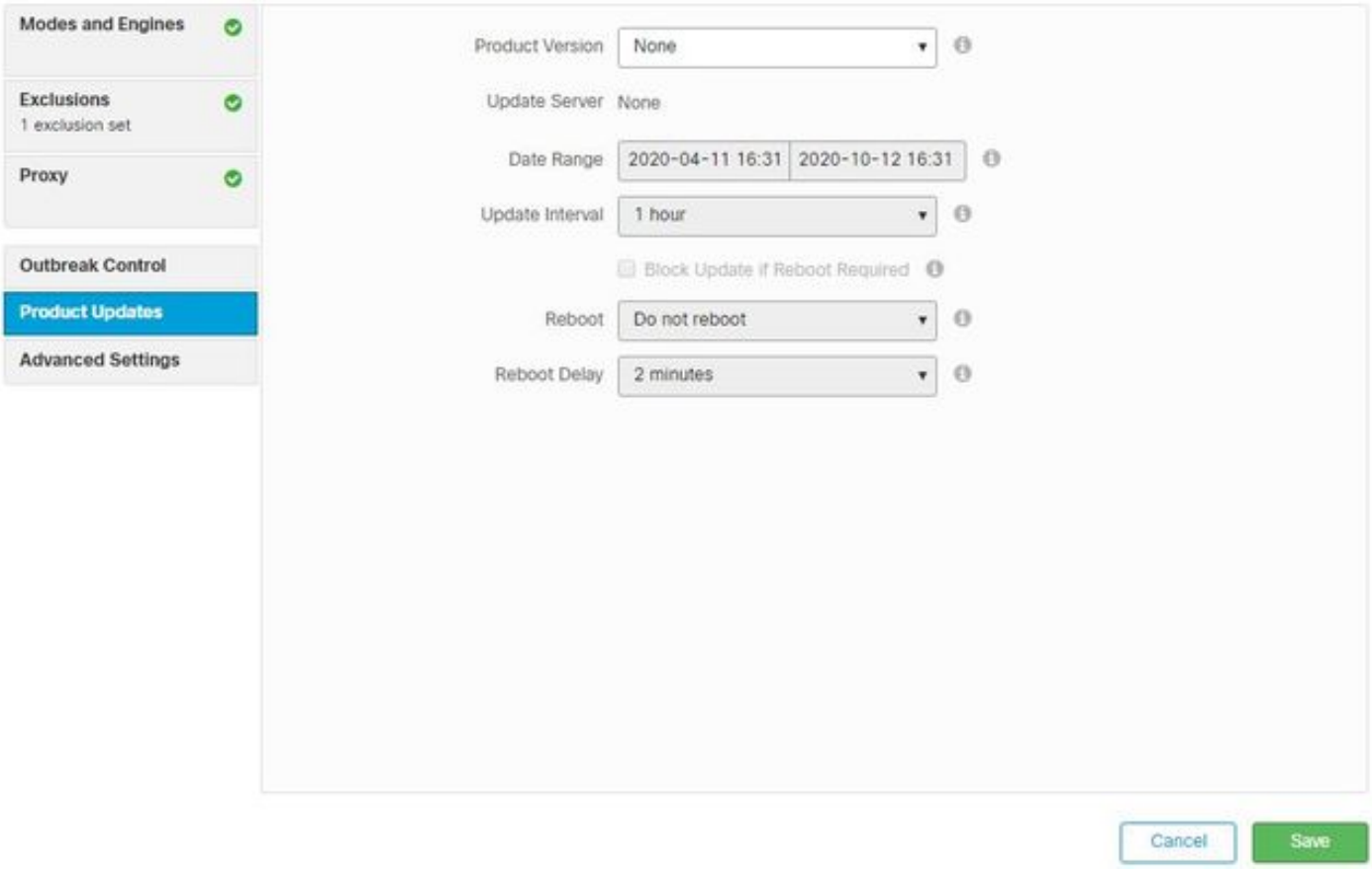
Control de brotes



En la sección Control de brotes, puede configurar detecciones personalizadas:

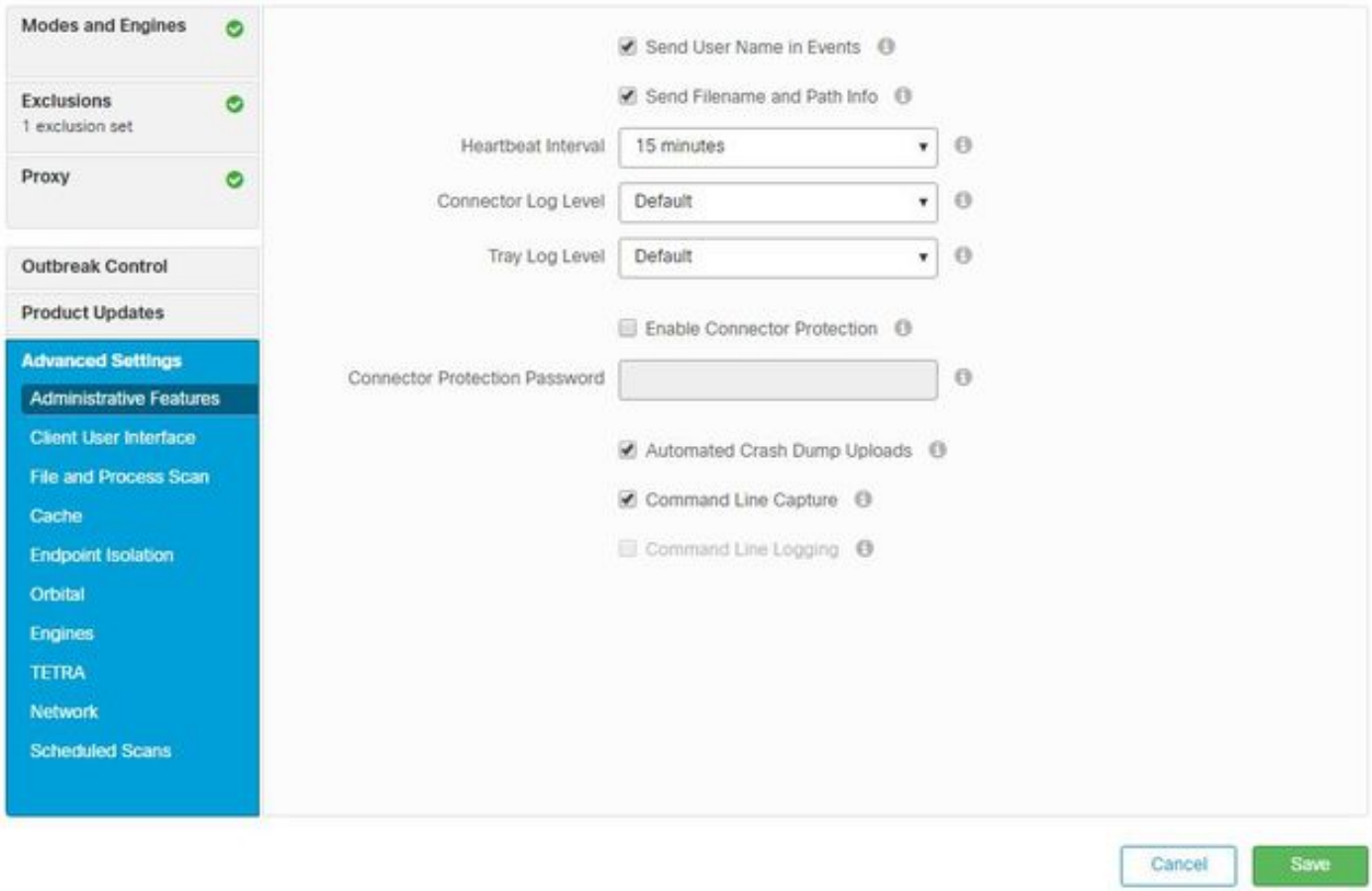
- Detecciones personalizadas: sencillas: Permite bloquear archivos específicos en función de su SHA
- Detecciones personalizadas - Avanzadas: Bloquea archivos basados en firmas para las detecciones cuando un SHA simple no es suficiente
- Listas de aplicaciones permitidas y bloqueadas: Permite o bloquea aplicaciones con SHA
- Red - Bloqueo IP y listas de permitidos: se utiliza con la correlación de flujo de dispositivos (DFC) para definir detecciones de direcciones IP personalizadas

Actualizaciones de productos



En la sección Actualización de producto, se establecen opciones para nuevas actualizaciones. Puede elegir una versión, un intervalo de fechas para implementar actualizaciones y opciones para reiniciar.

Parámetros avanzados



Características administrativas: Configura la frecuencia con la que el conector consulta a la nube los cambios de la política.

Interfaz de usuario cliente: Permite controlar la visualización de notificaciones en los dispositivos en los que está instalado AMP.

Análisis de archivos y procesos: configura las opciones de protección en tiempo real, cómo comprueban los conectores las disposiciones de los archivos y cómo se permiten los tamaños máximos de los archivos.

Caché: Configuración de Time To Live para la memoria caché.

El aislamiento de terminales permite habilitar y configurar la función para aislar dispositivos con el conector de AMP instalado.

La opción orbital habilita la búsqueda orbital avanzada.

Motores: Configuración para ETHOS; un motor de agrupación de archivos y SPERO; un sistema de aprendizaje automatizado.

Configuración de TETRA para el motor sin conexión.

Network Habilita las opciones de Correlación de Flujo del Dispositivo.

En la sección Exploraciones programadas puede configurar las opciones para cuándo y qué tipo de exploraciones desea ejecutar en los conectores.

Guardar cambios

Después de realizar cualquier cambio, haga clic en **Guardar** para asegurarse de que se aplican a la directiva.

También puede encontrar la información contenida en este documento en el vídeo Configuración de políticas de Windows en AMP para terminales.

Información Relacionada

- Para obtener más información sobre la configuración de políticas, vaya a la guía del usuario
- **Soporte Técnico y Documentación - Cisco Systems**