Windows-beleid in Advanced Malware Protection voor endpoints

Inhoud

Inleiding

Dit document beschrijft onderdelen die te configureren zijn in het Advanced Malware Protection (AMP) voor endpoints en Windows-beleid.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Advanced Malware Protection voor endpoints voor gebruikers met Administrator-rechten

Gebruikte componenten

De informatie in dit document is gebaseerd op Advanced Malware Protection voor endpoints.

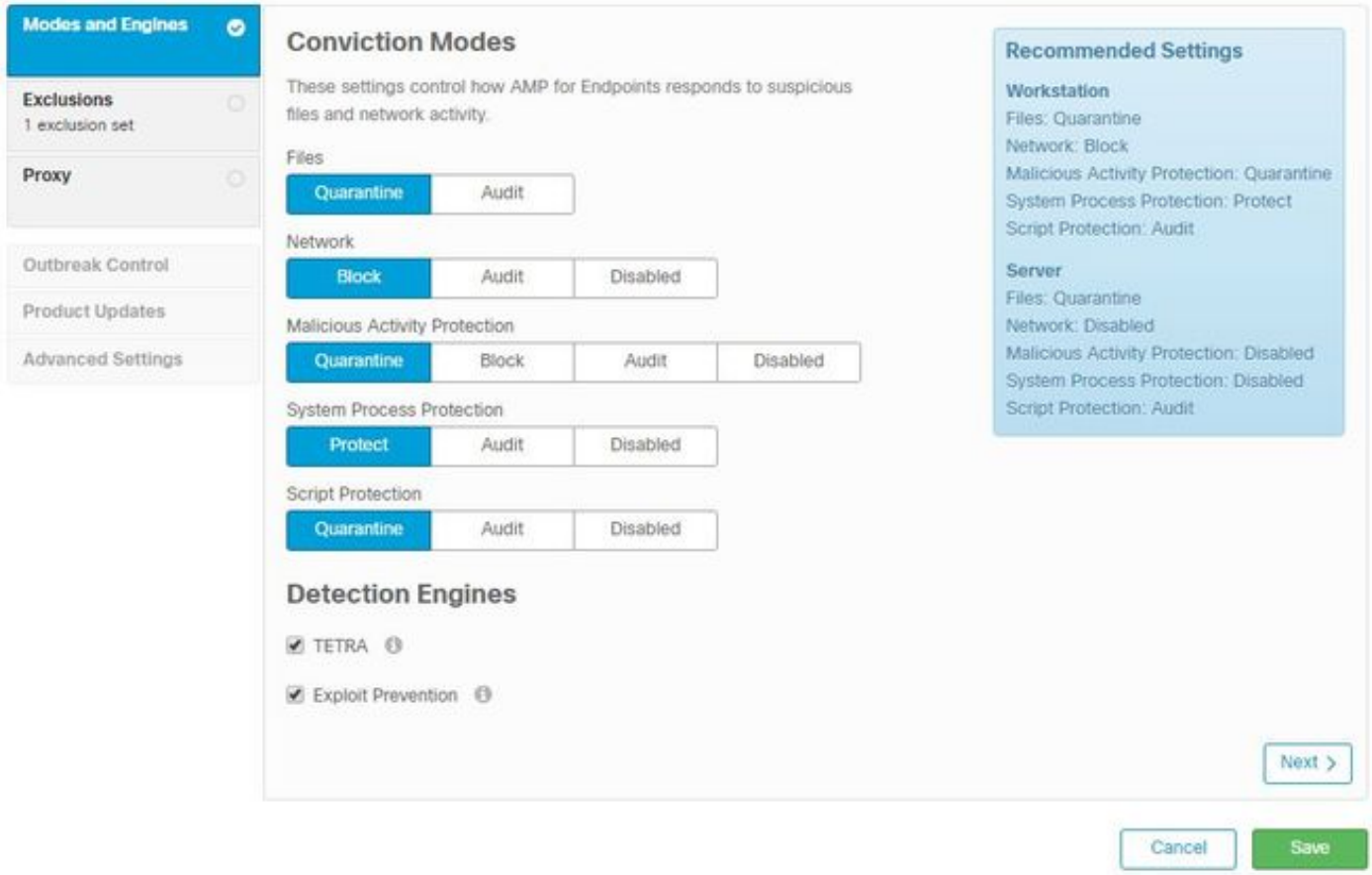
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Als u een nieuw Windows-beleid wilt maken, navigeer dan naar het tabblad Beheer en selecteer

Beleid. Maak in het beleidsgedeelte een nieuw Windows-beleid.

Modus en motor



Bestanden: De belangrijkste SHA-motor en kernfunctionaliteit van AMP. Met deze optie kunt u bestanden scannen en in quarantaine plaatsen.

Netwerk: De machine voor de stroomvergelijking van het apparaat die aansluitingen controleert.

Bescherming tegen schadelijke activiteiten: De motor die het eindpunt tegen ransomware aanvallen beschermt.

Systeemprocesbescherming: Engine die kritische Windows systeemprocessen tegen compromissen beschermt door geheugeninjectieaanvallen.

Script-bescherming: Verstrekt zichtbaarheid in op script gebaseerde aanvallen.

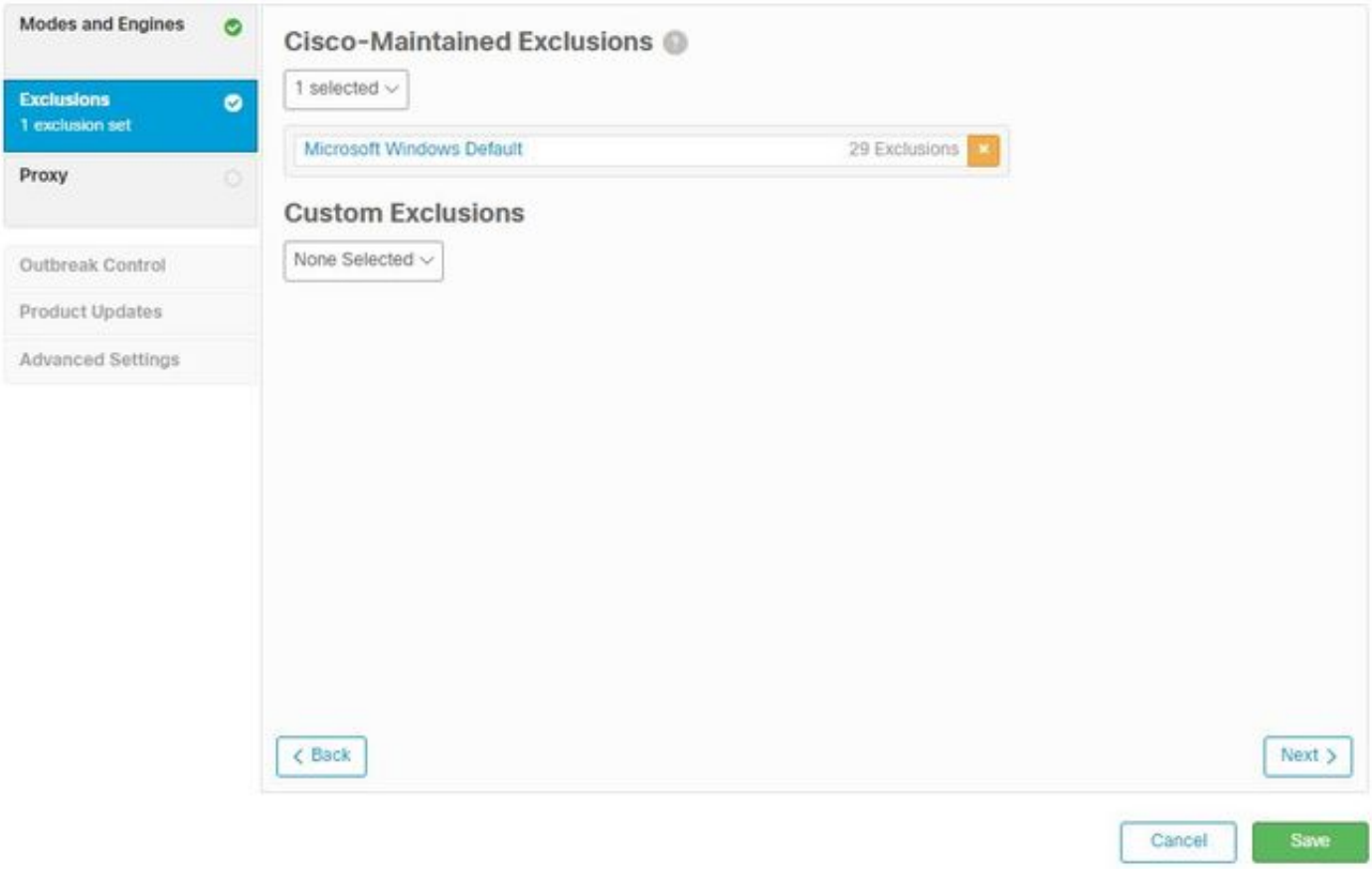
Detectiemotoren:

- Tetra: Offline antivirus dat definities downloads om het eindpunt te beschermen
- Explosiepreventie: Bescherm de connectors tegen aanvallen met een injectie in het geheugen

  Opmerking: Er verschijnt een venster met aanbevolen instellingen voor werkstations en servers in het juiste gedeelte.

Klik na het configureren van het vak Modi en engine op **Volgende**, zoals in de afbeelding.

Uitsluitingen



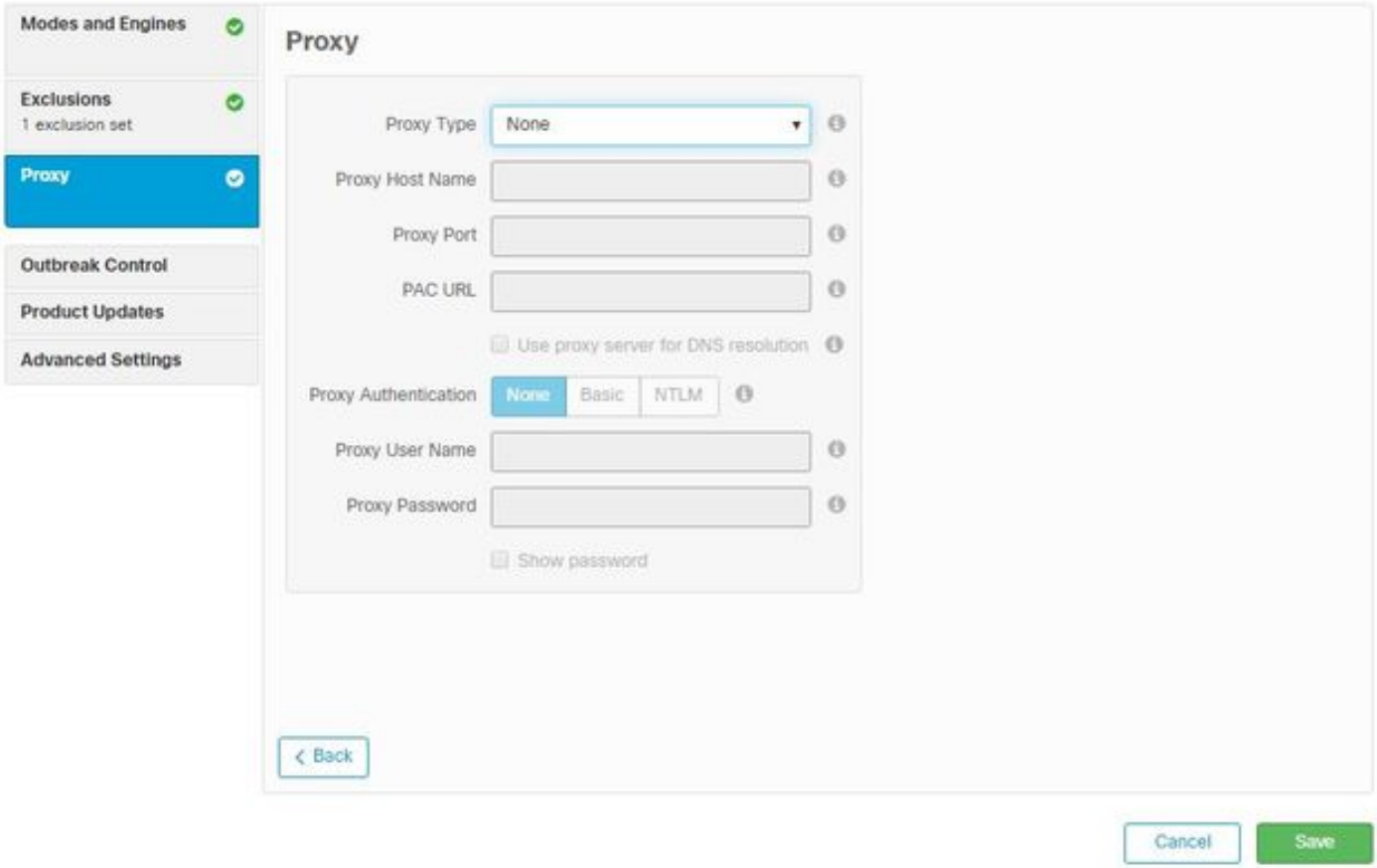
De uitsluitingssectie bevat Cisco-Onderhouden uitsluitingen en Aangepaste uitsluitingen:

- Cisco-onderhouden uitsluitingen worden gecreëerd en onderhouden door Cisco en u kunt gemeenschappelijke toepassingen van scans door AMP uitsluiten om onverenigbaarheidsproblemen te voorkomen
- Aangepaste uitsluitingen worden gecreëerd en onderhouden door de gebruikersbeheerder

Als je meer wilt weten over uitsluitingen, vind je meer informatie in deze video.

Nadat u de configuratie van uw uitsluitingen hebt voltooid, klikt u op **Volgende**, zoals in de afbeelding wordt weergegeven.

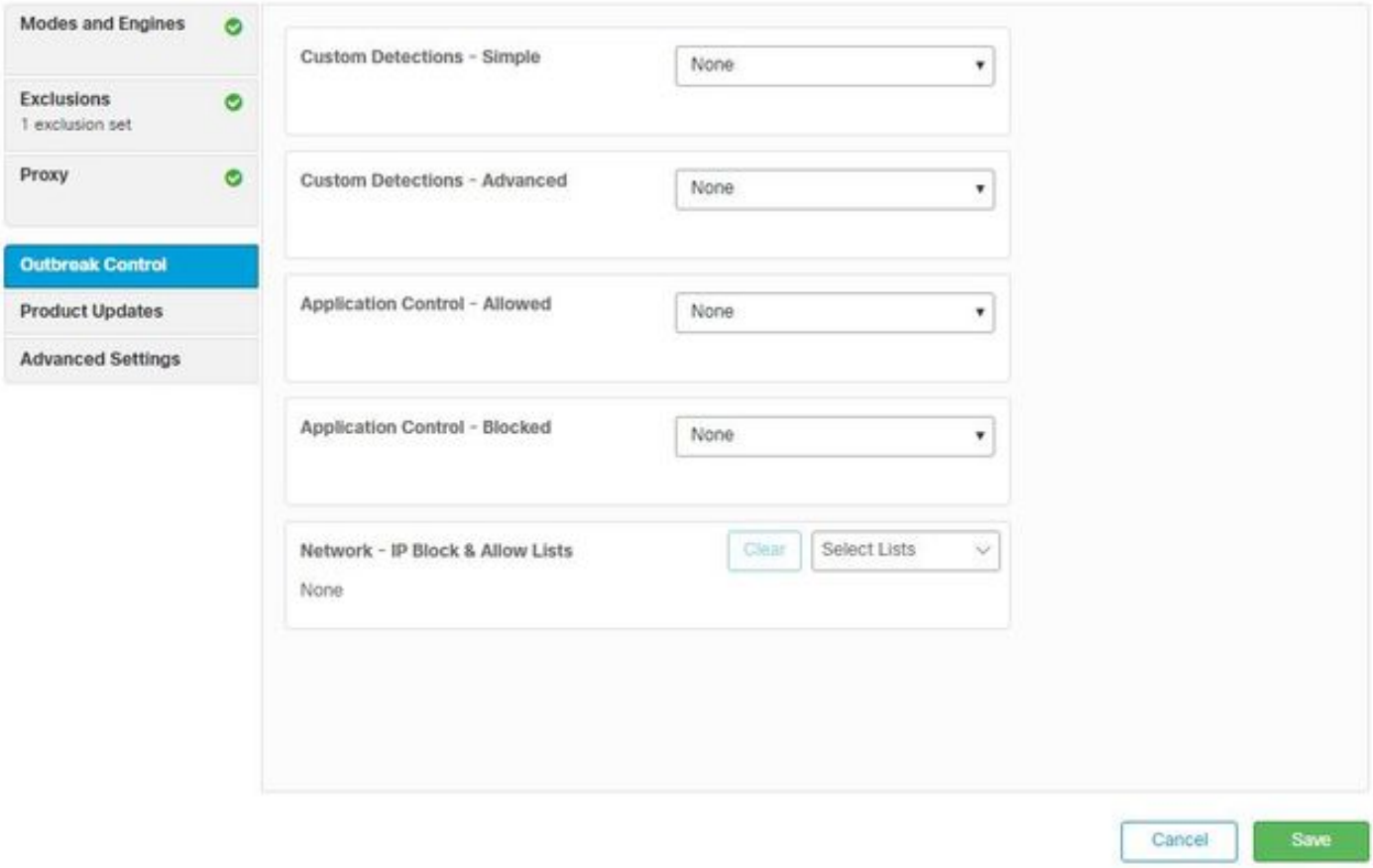
proxy



In deze sectie kunt u de proxy-instellingen per omgeving configureren om de connector in staat te stellen de AMP-cloud aan te vragen.

Nadat u de instellingen voor proxy hebt ingesteld, klikt u op **Opslaan**, zoals in de afbeelding.

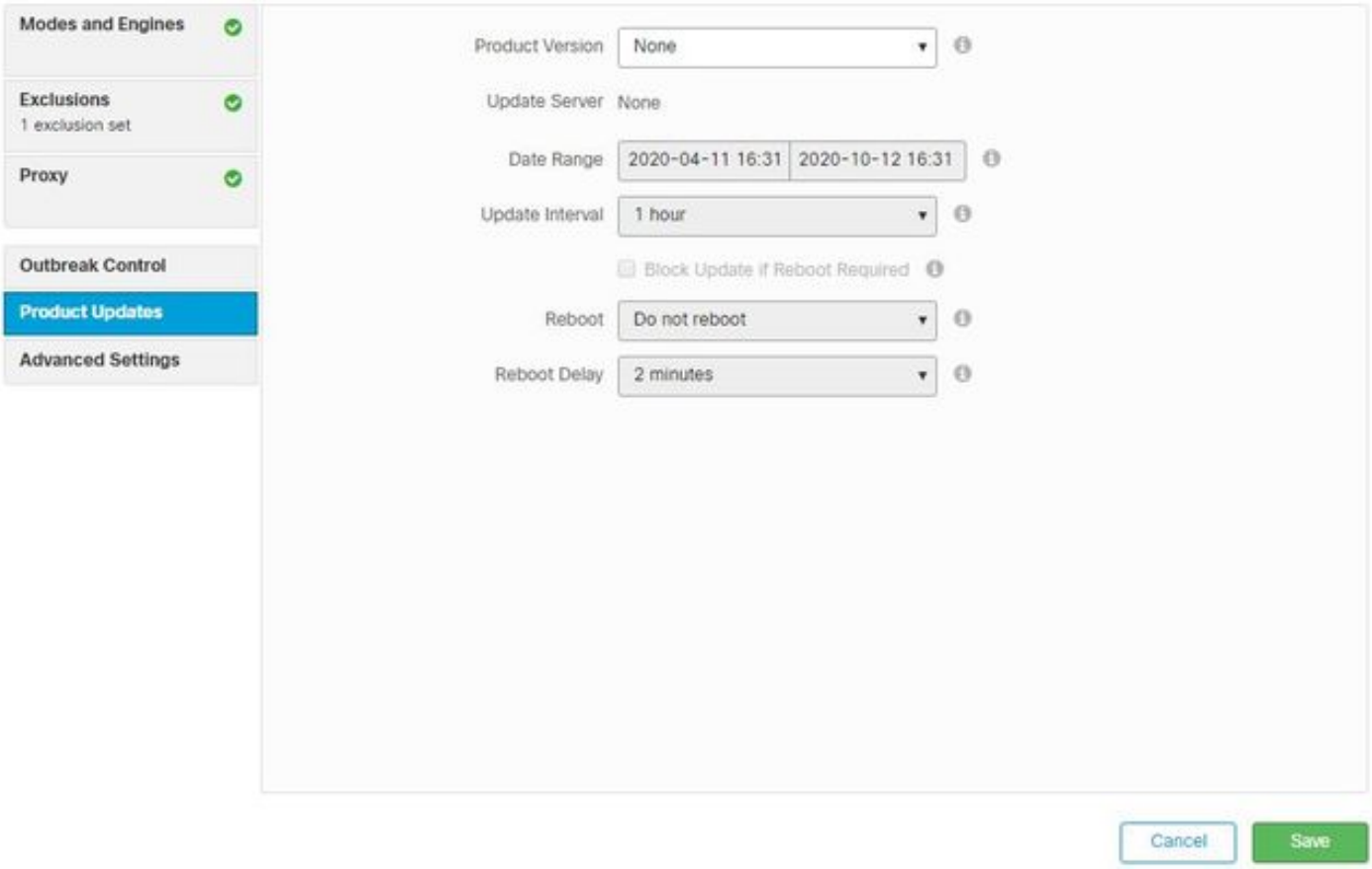
Outdoorcontrole



In het gedeelte Outbreak Control kunt u aangepaste detecties configureren:

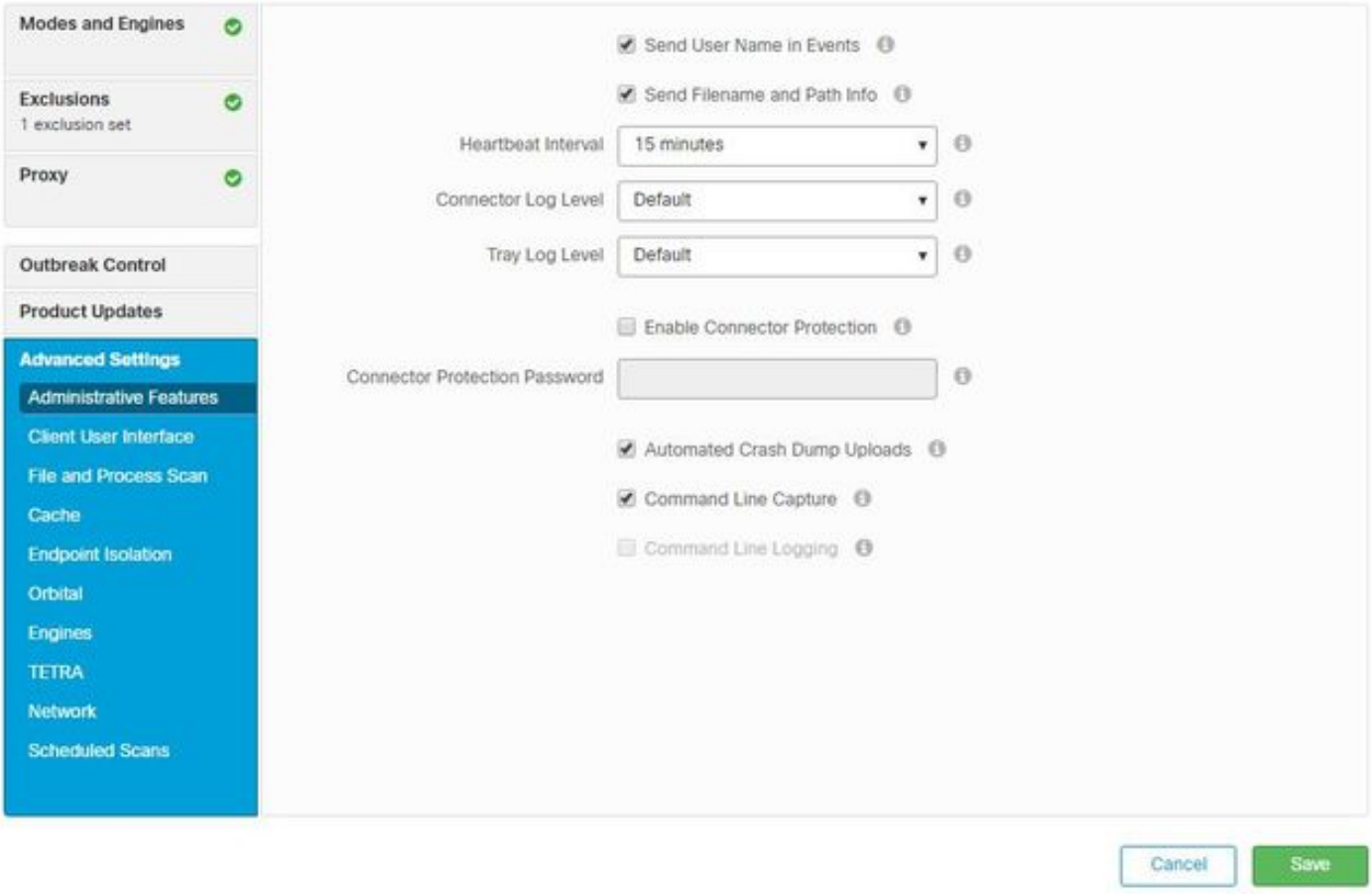
- Aangepaste detecties - Eenvoudig: Hiermee kunt u specifieke bestanden op basis van hun SHA blokkeren
- Aangepaste detecties - Geavanceerd: Blokkeert bestanden op basis van handtekeningen, voor detecties wanneer een eenvoudige SHA niet voldoende is
- Toegestaan en geblokkeerde lijsten: Hiermee kunt u toepassingen met SHA's toestaan of blokkeren
- Netwerk - IP-blokkering en lijst toestaan: gebruikt met apparaatFlow Correlatie (DFC) om aangepaste IP-adresdetectie te definiëren

Productupdates



In het gedeelte Product Update worden de opties voor nieuwe updates ingesteld. U kunt een versie, datumbereik selecteren om updates en opties voor een herstart te rollen.

Geavanceerde instellingen



Administratieve kenmerken: hiermee wordt ingesteld hoe vaak de connector de cloud vraagt voor wijzigingen in het beleid.

Clientgebruikersinterface: Hiermee kunt u de weergave van meldingen in uw apparaten controleren waar AMP is geïnstalleerd.

Scannen bestand en proces: Configureert de opties voor realtime beveiliging, de manier waarop connectors controleren op bestandsindelingen en de maximale grootte van een bestand.

cache: Tijd om te leven configuratie voor cache.

Endpoint isolatie stelt u in staat om deze functie in te schakelen en in te stellen om apparaten te isoleren terwijl de AMP-connector is geïnstalleerd.

Orbital Option maakt het mogelijk om geavanceerd orbitaal te zoeken.

Motoren: Instellingen voor ETHOS; een bestandsgroeperingsmotor en SPERO; een op de machine gebaseerd leersysteem.

TETRA-configuratie voor de offline motor.

Netwerk schakelt de opties voor apparaatFlow in.

In het gedeelte Geplande scans kunt u de opties configureren voor wanneer en welk type scans u in de connectors wilt uitvoeren.

Wijzigingen opslaan

Klik na het uitvoeren van alle wijzigingen op **Opslaan** om er zeker van te zijn dat deze op het beleid worden toegepast.

U kunt de informatie in dit document ook vinden in de video Windows Policy Configuration voor Endpoints.

Gerelateerde informatie

- Raadpleeg de gebruikersgids voor meer informatie over de beleidsconfiguratie
- **Technische ondersteuning en documentatie – Cisco Systems**