Konfigurieren der Windows-Richtlinie in AMP für Endgeräte

Inhalt

Einführung

Dieses Dokument beschreibt Komponenten, die in der Windows-Richtlinie Advanced Malware Protection (AMP) für Endgeräte konfigurierbar sind.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- AMP für Endgeräte-Benutzer mit Administratorrechten

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der AMP-Konsole für Endgeräte.

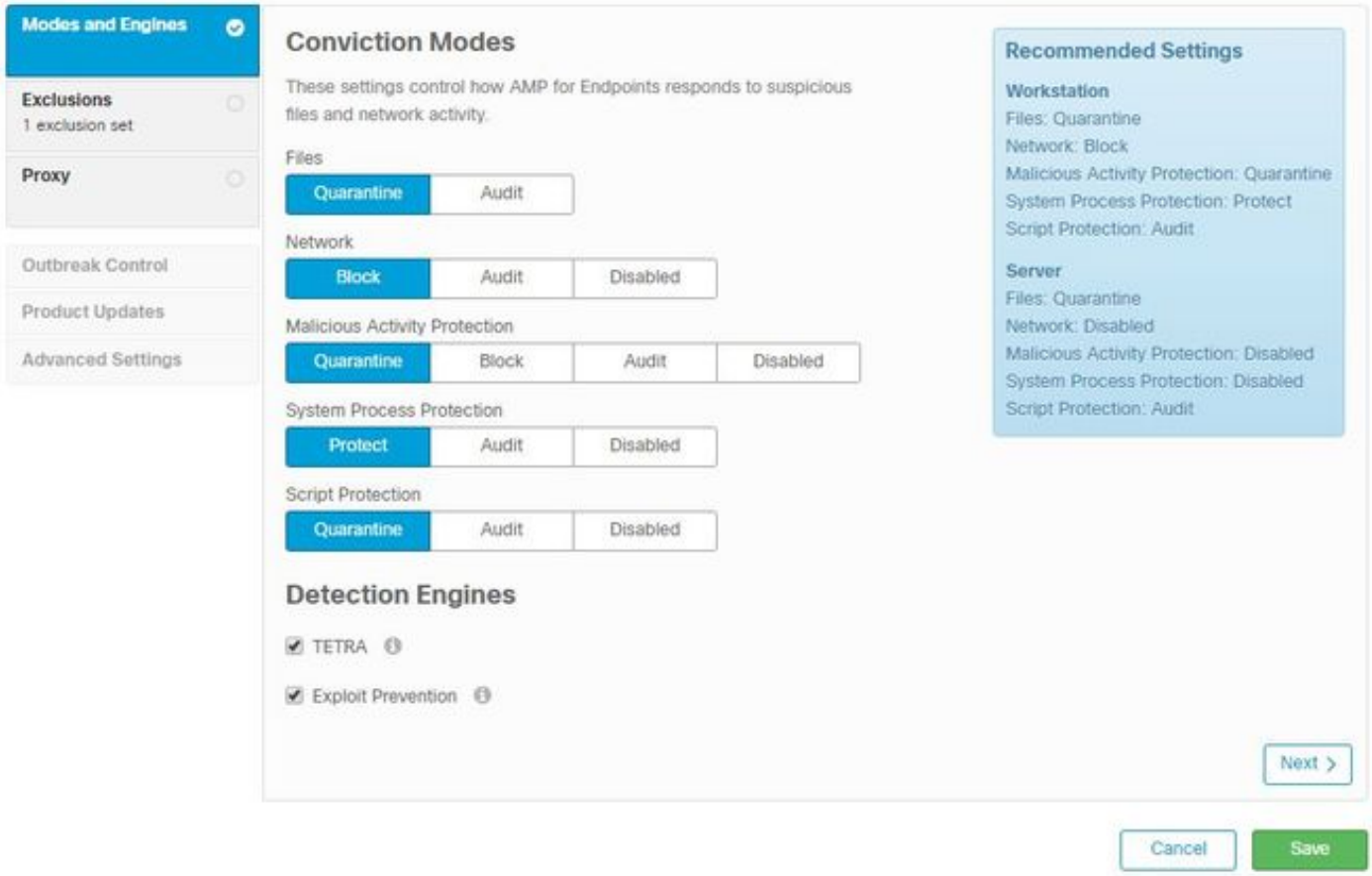
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Um eine neue Windows-Richtlinie zu erstellen, navigieren Sie zur Registerkarte Verwaltung, und

wählen Sie Richtlinien aus. Erstellen Sie im Richtlinienabschnitt eine neue Windows-Richtlinie.

Modi und Motoren



Dateien: Die wichtigste SHA-Engine und die Kernfunktionalität von AMP. Diese Option ermöglicht Dateiprüfungen und Quarantäne.

Netzwerk: Die Device Flow Correlation-Engine, die Verbindungen überwacht.

Schutz vor bösartigen Aktivitäten: Eine Engine, die den Endpunkt vor Ransomware-Angriffen schützt.

Schutz von Systemprozessen: Engine, die kritische Windows-Systemprozesse vor Kompromittierungen und Angriffen auf die Speicherinjektion schützt.

Skriptschutz: Bietet Transparenz für skriptbasierte Angriffe.

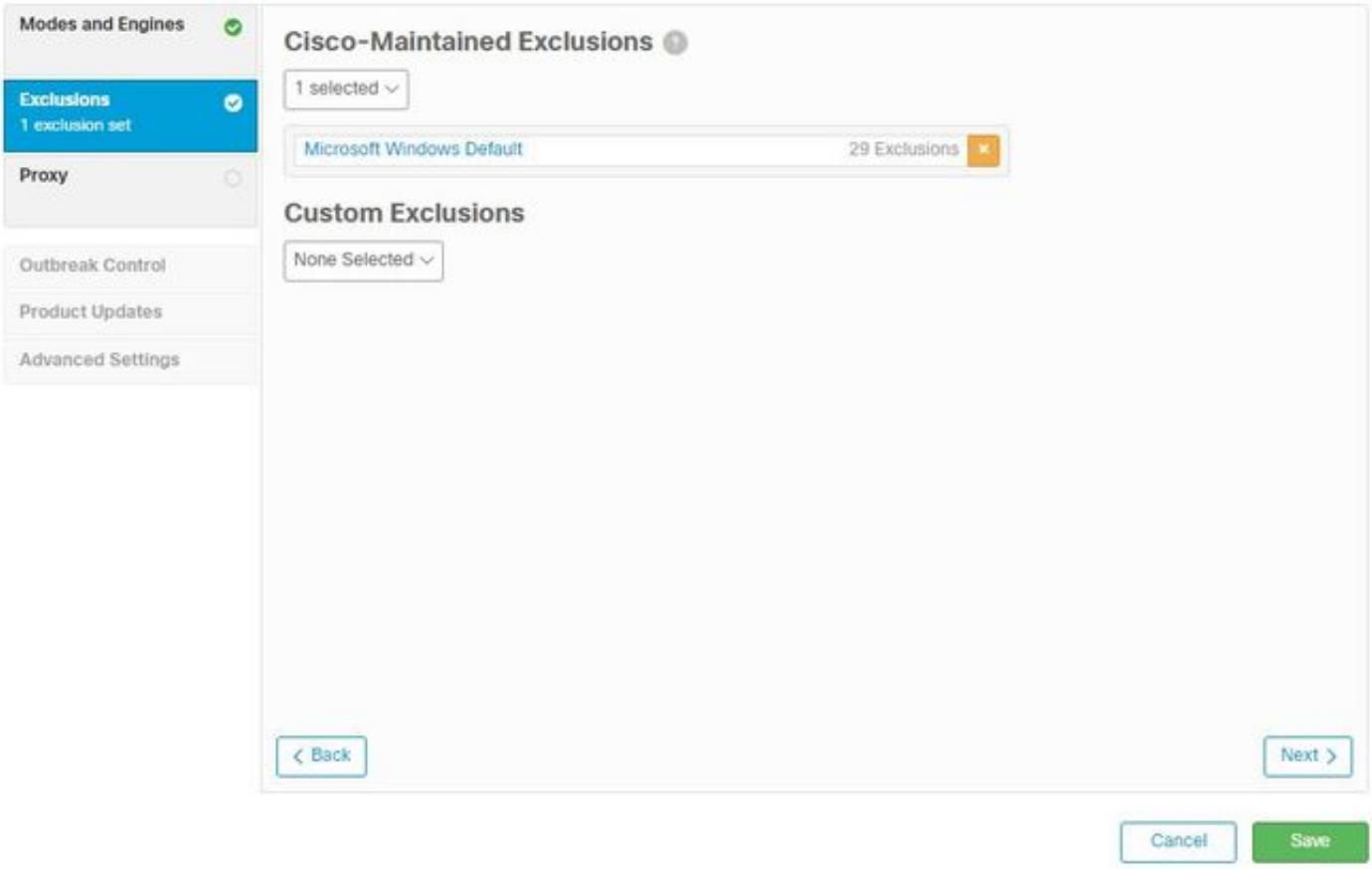
Erkennungs-Engines:

- Tetra: Offline-Antivirus zum Schutz des Endgeräts, das Definitionen herunterlädt
- Exploit-Prävention: Schützt Anschlüsse vor Angriffen durch die Speicherinjektion

Hinweis: Im rechten Bereich wird ein Fenster mit empfohlenen Einstellungen für Workstations und Server angezeigt.

Klicken Sie nach der Konfiguration des Bereichs Modi und Engine auf **Weiter**, wie im Bild gezeigt.

Ausschlüsse



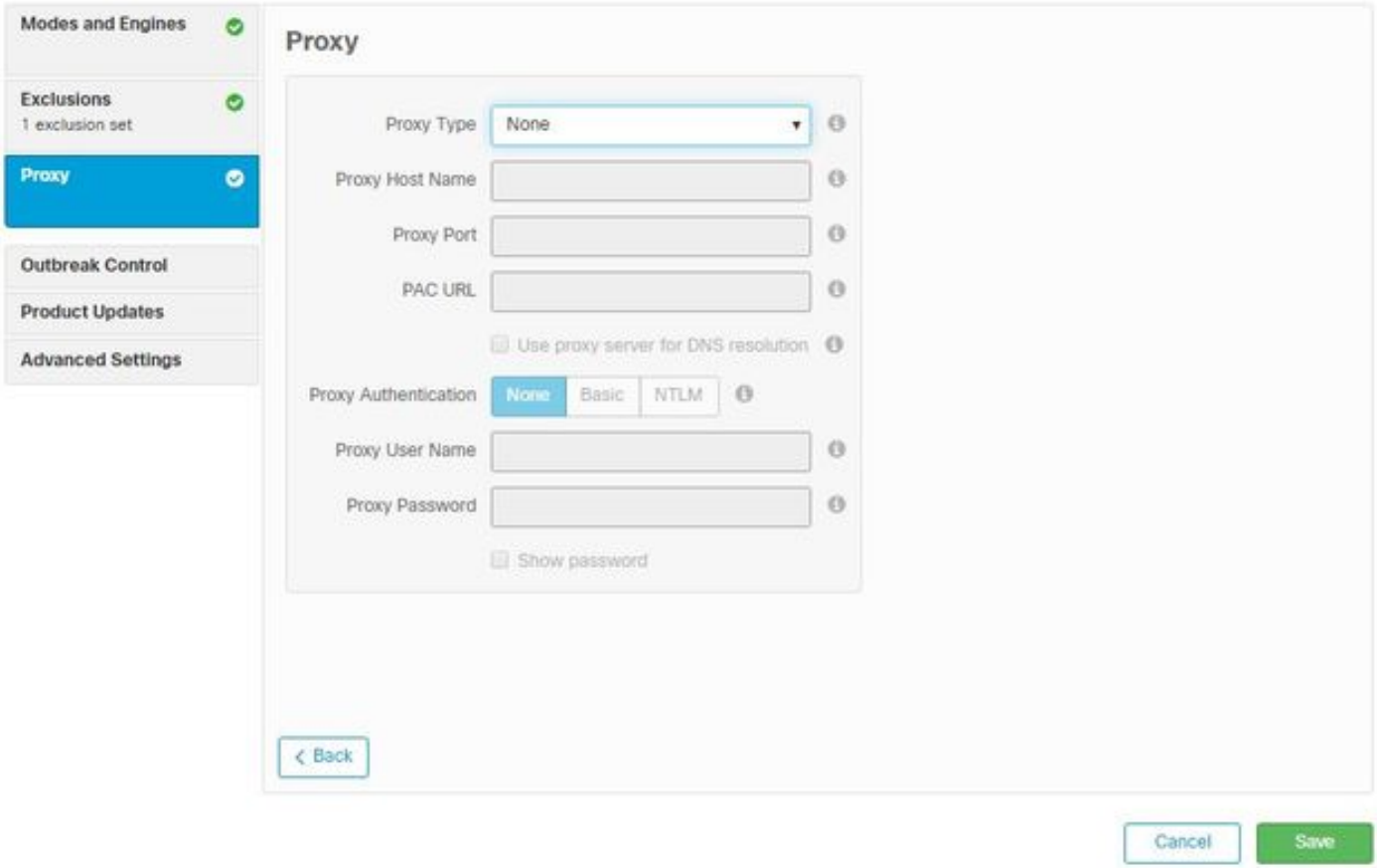
Der Abschnitt "Ausschlüsse" enthält von Cisco verwaltete Ausschlüsse und benutzerdefinierte Ausschlüsse:

- Von Cisco gepflegte Ausschlüsse werden von Cisco erstellt und verwaltet. Sie können gängige Anwendungen von AMP aus den Prüfungen ausschließen, um Kompatibilitätsprobleme zu vermeiden.
- Benutzerdefinierte Ausschlüsse werden vom Benutzeradministrator erstellt und verwaltet.

Weitere Informationen zu Ausschlüssen finden Sie in diesem Video.

Wenn Sie die Konfiguration der Ausschlüsse abgeschlossen haben, klicken Sie auf **Weiter**, wie im Bild gezeigt.

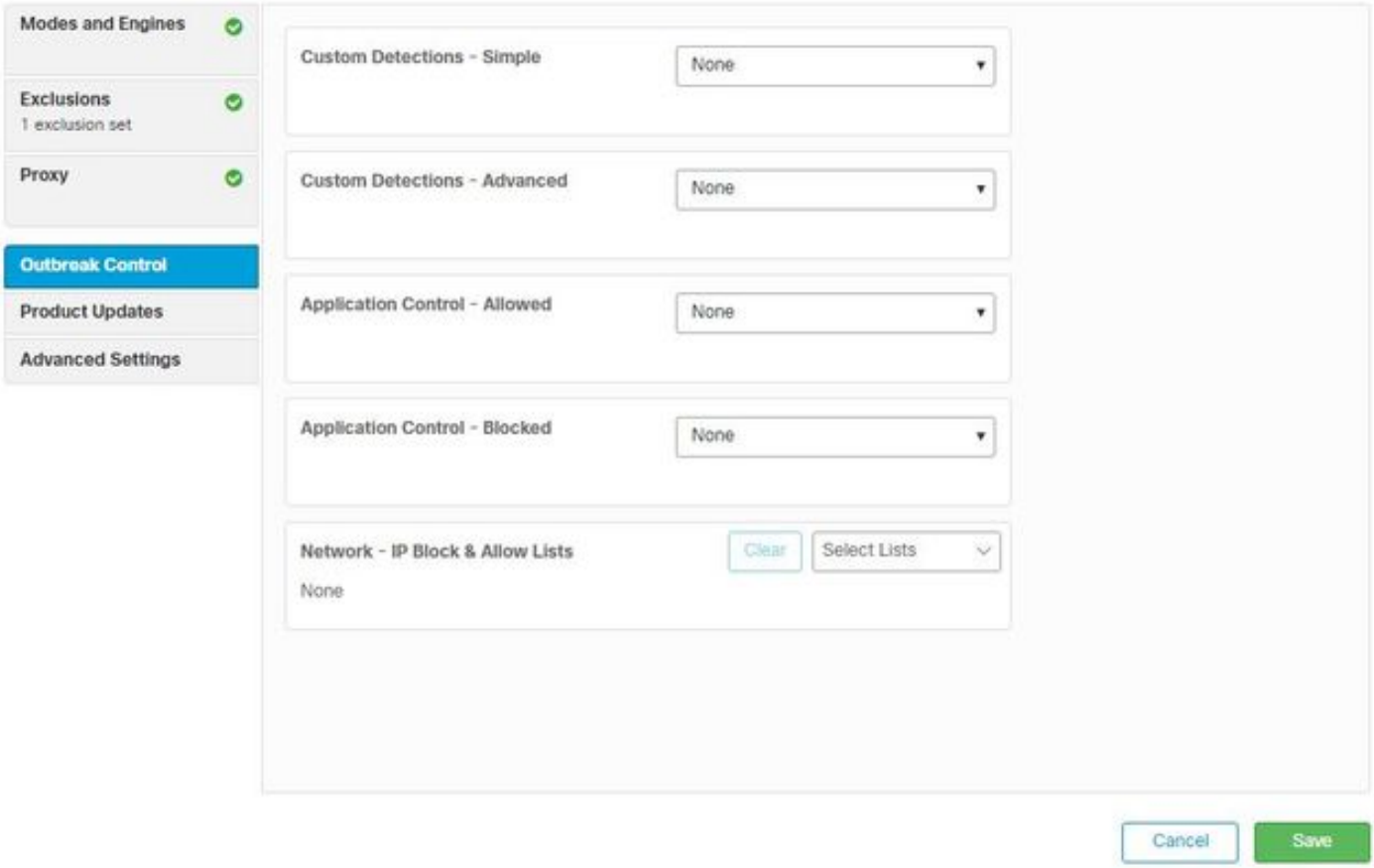
Proxy



In diesem Abschnitt können Sie die Proxyeinstellungen für Ihre Umgebung konfigurieren, damit der Connector die AMP-Cloud abfragen kann.

Nachdem Sie die Proxy-Einstellungen konfiguriert haben, klicken Sie auf **Speichern**, wie im Bild gezeigt.

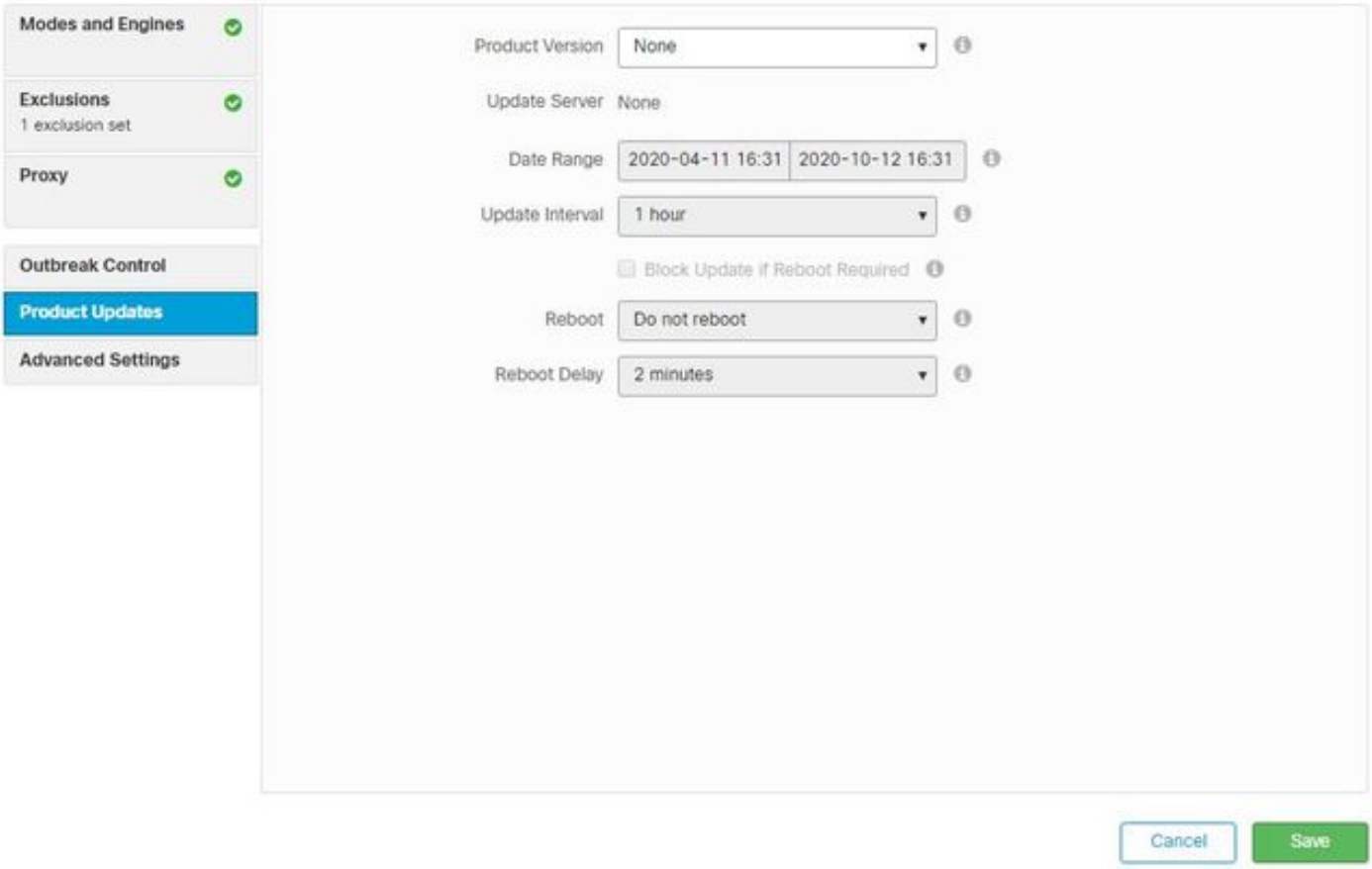
Outbreak-Kontrolle



Im Abschnitt Outbreak-Steuerelement können Sie benutzerdefinierte Erkennungen konfigurieren:

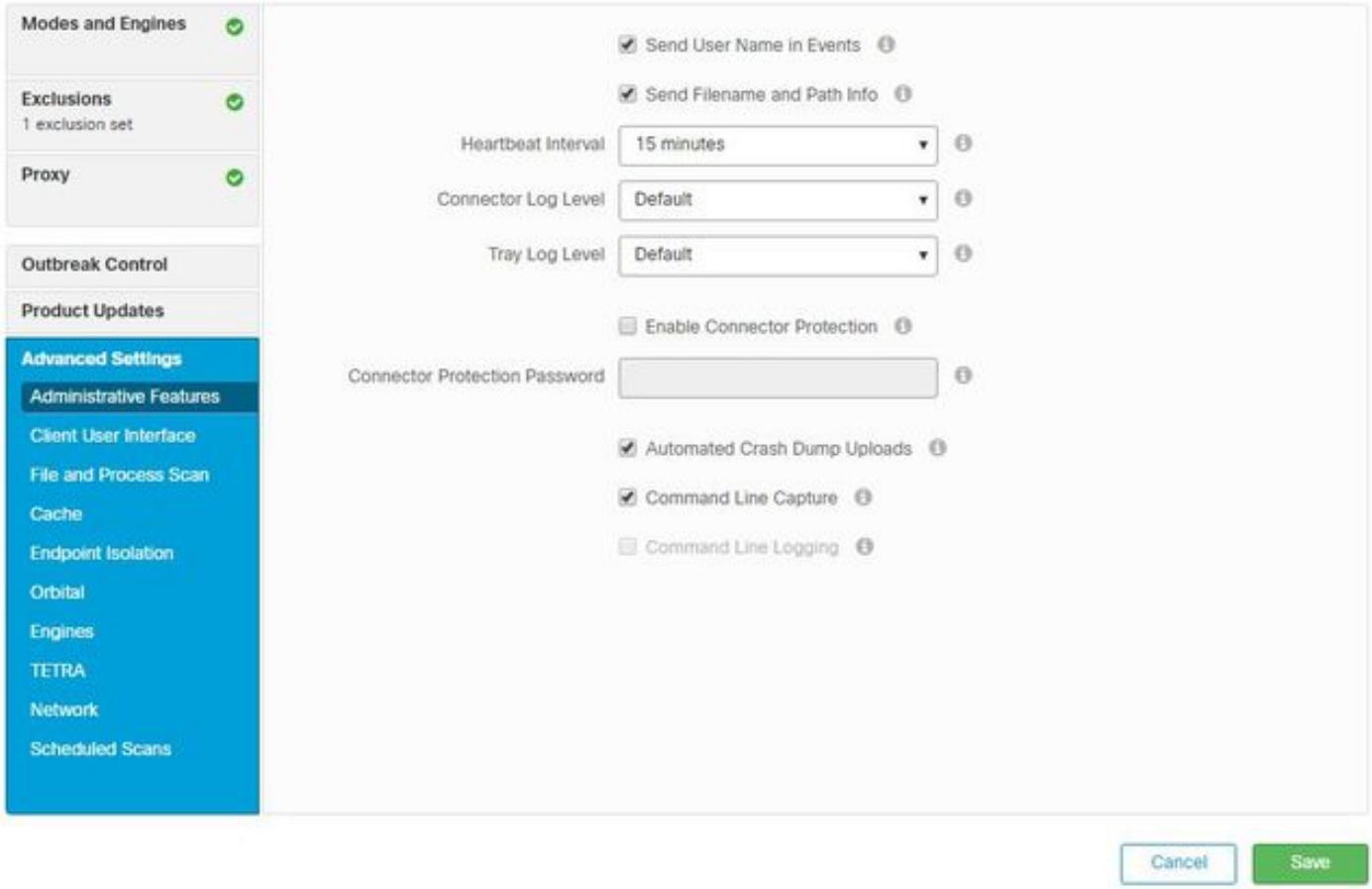
- Benutzerdefinierte Erkennung - Einfach: Ermöglicht Ihnen das Blockieren bestimmter Dateien basierend auf deren SHA.
- Benutzerdefinierte Erkennung - Erweitert: Blockiert Dateien auf der Grundlage von Signaturen für Erkennungen, wenn ein einfaches SHA nicht ausreicht
- Zulässige und gesperrte Anwendungslisten: Ermöglicht oder blockiert Anwendungen mit SHAs
- Netzwerk - IP-Sperrlisten und Listen zulassen: Verwendung mit Device Flow Correlation (DFC) zur Definition benutzerdefinierter IP-Adresserkennungen

Produktaktualisierungen



Im Abschnitt "Produktaktualisierung" werden Optionen für neue Updates festgelegt. Sie können eine Version, einen Datumsbereich zum Rollen von Updates und Optionen für einen Neustart auswählen.

Erweiterte Einstellungen



Verwaltungsfunktionen: Konfiguriert, wie oft der Connector die Cloud nach Änderungen an der Richtlinie abfragt.

Client-Benutzeroberfläche: Ermöglicht Ihnen, die Anzeige von Benachrichtigungen auf den Geräten zu steuern, auf denen AMP installiert ist.

Datei- und Prozessprüfung: konfiguriert Echtzeit-Schutzoptionen, wie Connectors nach Dateistatus und zulässigen maximalen Dateigrößen suchen.

Cache: Zeit bis zur Live-Konfiguration für den Cache.

Dank der Endpunktisolierung können Sie die Funktion aktivieren und konfigurieren, um Geräte mit dem installierten AMP-Anschluss zu isolieren.

Die Orbital-Option ermöglicht die erweiterte Orbital-Suche.

Motoren: Einstellungen für ETHOS; eine Datei-Gruppierungsengine und SPERO; ein maschinelles Lernsystem.

TETRA-Konfiguration für die Offline-Engine.

Netzwerk aktiviert die Optionen für die Device Flow Correlation.

Im Abschnitt Geplante Prüfungen können Sie die Optionen für den Zeitpunkt und die Art der Prüfungen konfigurieren, die Sie in den Anschlüssen ausführen möchten.

Änderungen speichern

Wenn Sie Änderungen vorgenommen haben, klicken Sie auf **Speichern**, um sicherzustellen, dass sie auf die Richtlinie angewendet werden.

Die Informationen in diesem Dokument finden Sie auch im Video zur Konfiguration der Windows-Richtlinie in AMP für Endgeräte.

Zugehörige Informationen

- Weitere Informationen zur Richtlinienkonfiguration finden Sie im Benutzerhandbuch.
- **Technischer Support und Dokumentation - Cisco Systems**