Configure Windows Policy in AMP for Endpoints

Contents

Introduction

This document describes components configurable in the Advanced Malware Protection (AMP) for Endpoints Windows Policy.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- AMP for Endpoints user with Administrator privileges

Components Used

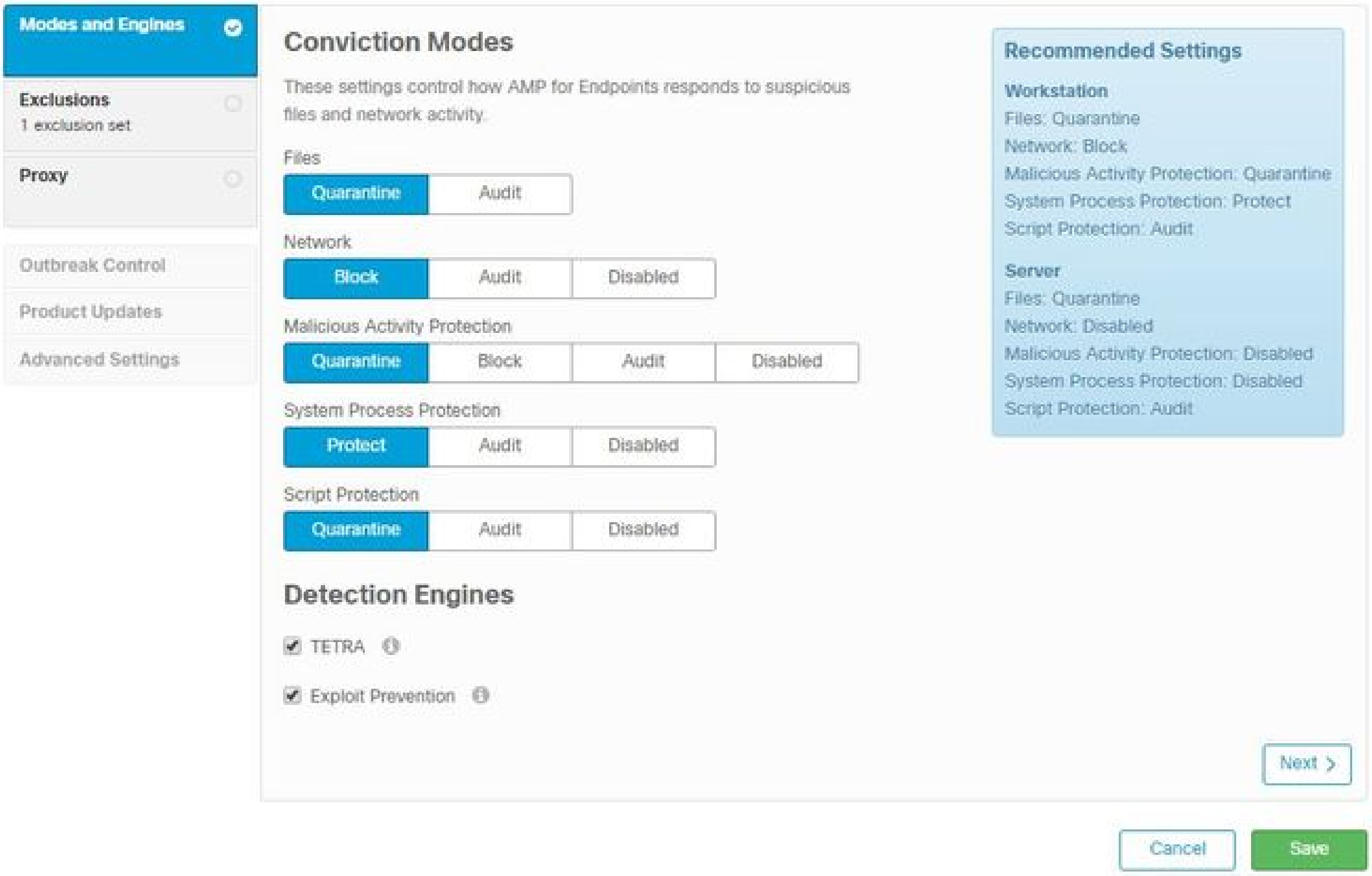
The information in this document is based on AMP for Endpoints Console.

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.

Configure

In order to create a new Windows policy, navigate to the management tab and select Policies. In the policy section, create a new Windows policy.

Modes and Engines



Conviction Modes

These settings control how AMP for Endpoints responds to suspicious files and network activity.

Files: [✓ Quarantine] Audit

Network: [✓ Block] Audit Disabled

Malicious Activity Protection: [✓ Quarantine] Block Audit Disabled

System Process Protection: [✓ Protect] Audit Disabled

Script Protection: [✓ Quarantine] Audit Disabled

Detection Engines

☑ TETRA

☑ Exploit Prevention

Recommended Settings

Workstation
Files: Quarantine
Network: Block
Malicious Activity Protection: Quarantine
System Process Protection: Protect
Script Protection: Audit

Server
Files: Quarantine
Network: Disabled
Malicious Activity Protection: Disabled
System Process Protection: Disabled
Script Protection: Audit

Files: The main SHA engine and core functionality of AMP. This option allows for file scans and quarantine.

Network: The Device Flow Correlation engine that monitors connections.

Malicious Activity Protection: Engine that protects the endpoint from ransomware attacks.

System Process Protection: Engine that protects critical Windows system processes from compromises through memory injection attacks.

Script protection: Provides visibility into script-based attacks.

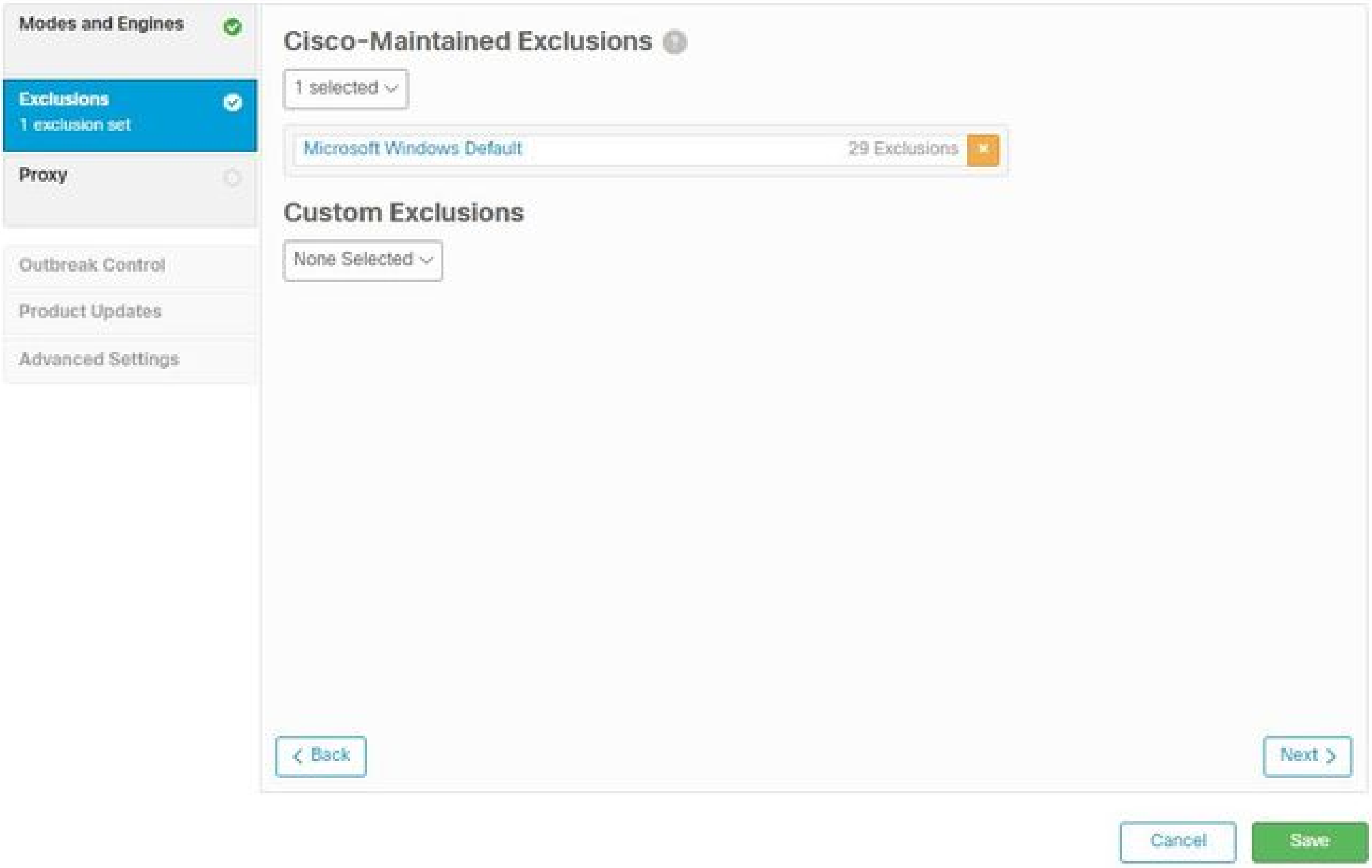
Detection engines:

- Tetra: Offline antivirus that downloads definitions to protect the endpoint
- Exploit Prevention: Protects connectors from memory injection attacks

> **Note**: A window of recommended settings for Workstations and Servers is displayed in the right section.

After the configuration of the Modes and Engine section, click **Next**, as shown in the image.

Exclusions



Cisco-Maintained Exclusions

1 selected

Microsoft Windows Default 29 Exclusions

Custom Exclusions

None Selected

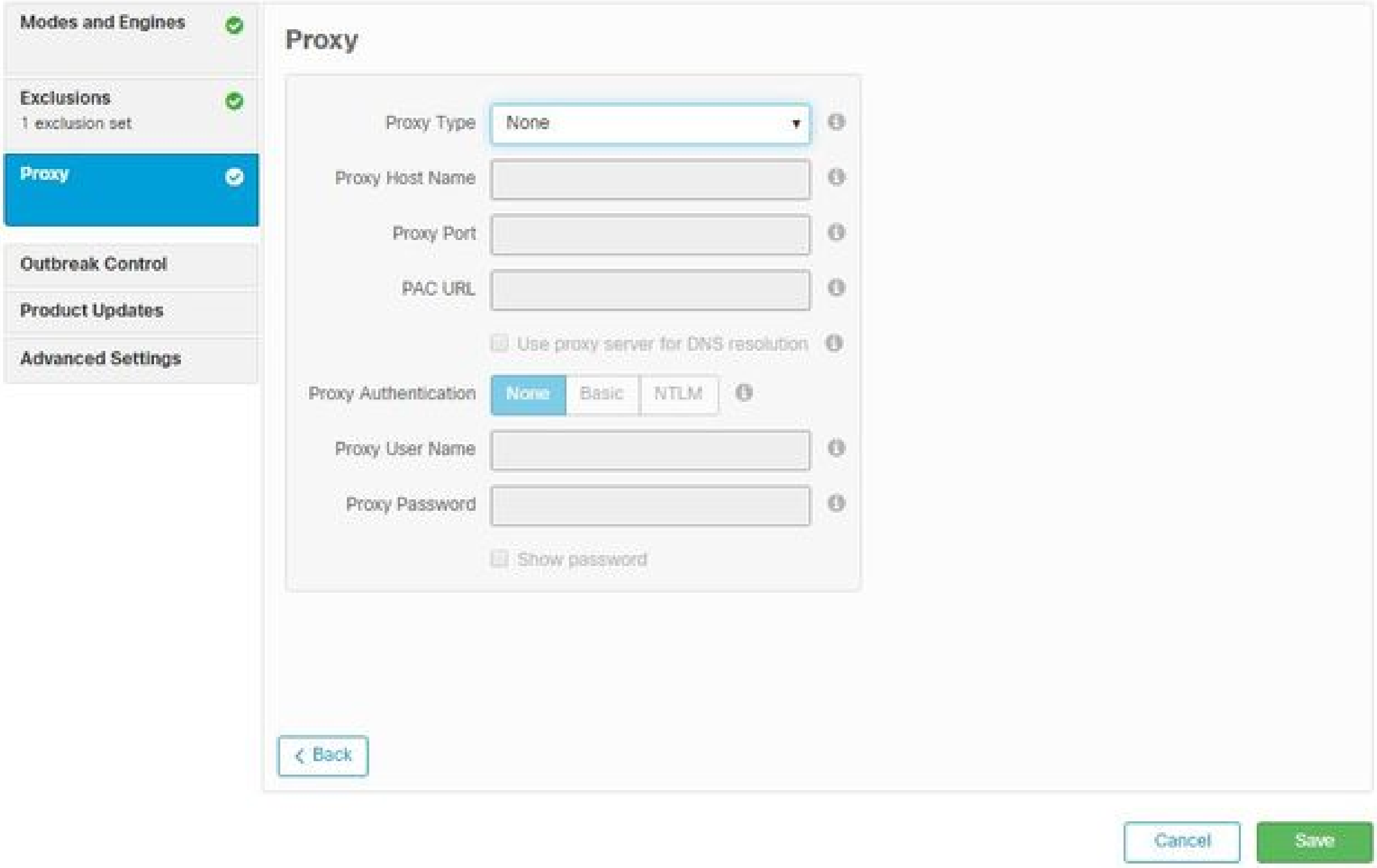
The exclusions section contains Cisco-Maintained Exclusions and Custom exclusions:

- Cisco-Maintained Exclusions are created and maintained by Cisco and allow you to exclude common applications from scans by AMP to avoid incompatibility issues
- Custom Exclusions are created and maintained by the user administrator

If you want to know more about exclusions, you can find more information in this video.

Once you finish your Exclusions configuration, click **Next**, as shown in the image.

Proxy



Proxy

Proxy Type: None

Proxy Host Name:

Proxy Port:

PAC URL:

□ Use proxy server for DNS resolution

Proxy Authentication: [✓ None] Basic NTLM

Proxy User Name:

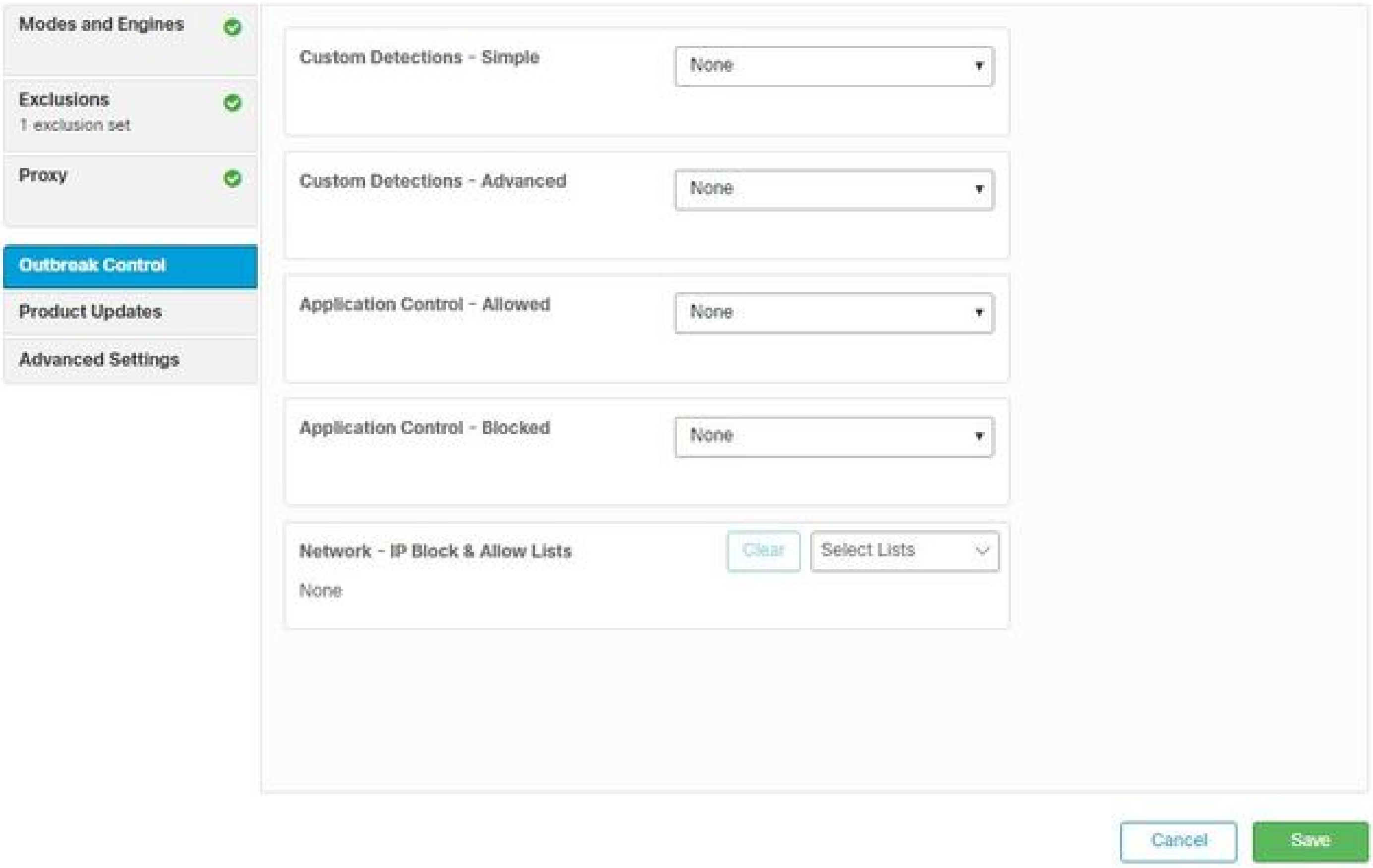
Proxy Password:

□ Show password

In this section, you can configure the proxy settings per your environment to allow the connector to query the AMP cloud.

After you configure your Proxy settings, click **Save**, as shown in the image.

Outbreak Control



Custom Detections - Simple: None

Custom Detections - Advanced: None

Application Control - Allowed: None

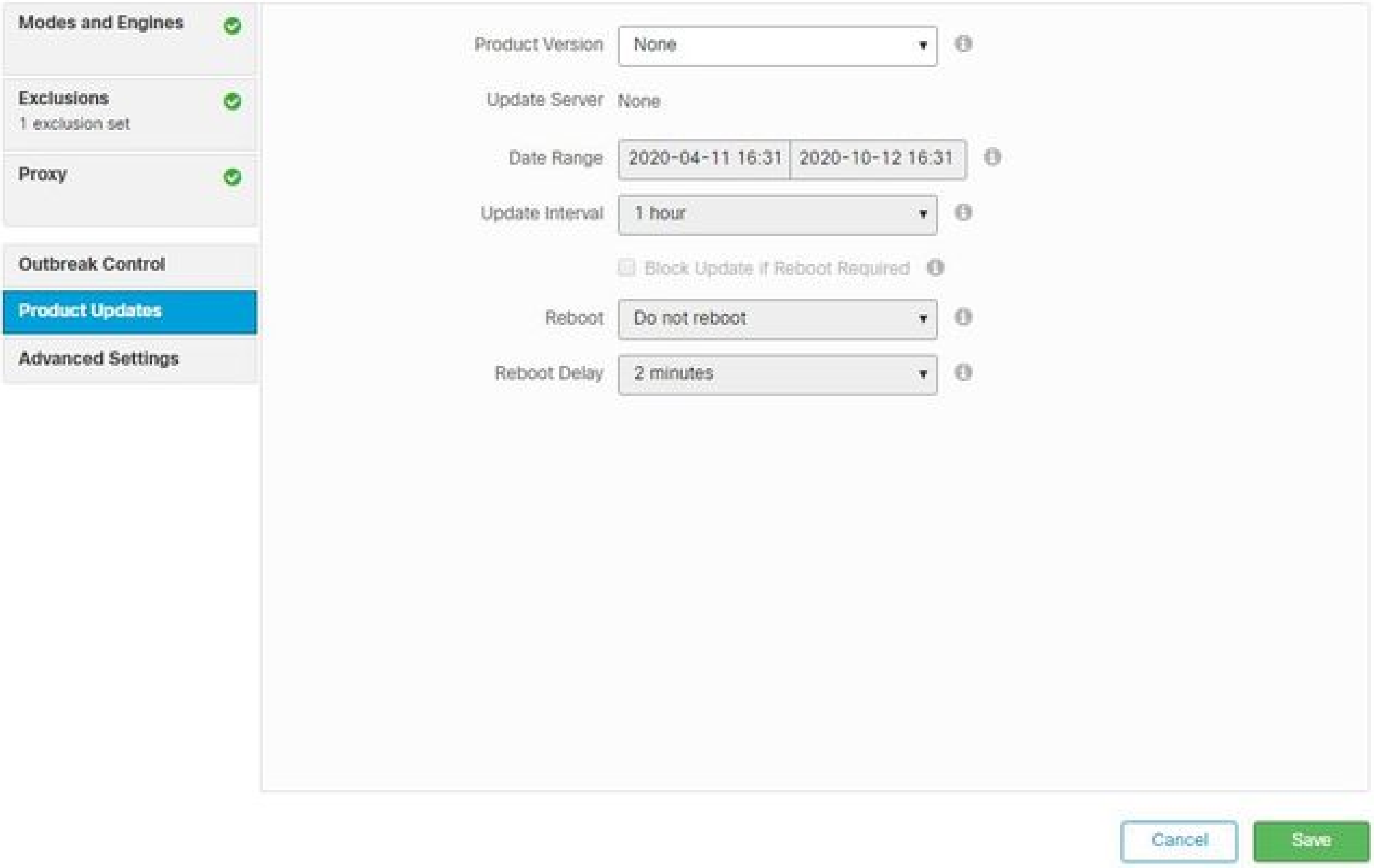
Application Control - Blocked: None

Network - IP Block & Allow Lists: None

In the Outbreak Control section, you can configure custom detections:

- Custom detections - Simple: Allows you to block specific files based on their SHA
- Custom detections - Advanced: Blocks files based on signatures, for detections when a simple SHA is not sufficient
- Application Allowed and Blocked lists: Allows or blocks applications with SHAs
- Network - IP Block & Allow Lists: used with Device Flow Correlation (DFC) to define custom IP address detections

Product Updates



Product Version: None

Update Server: None

Date Range: 2020-04-11 16:31 – 2020-10-12 16:31

Update Interval: 1 hour

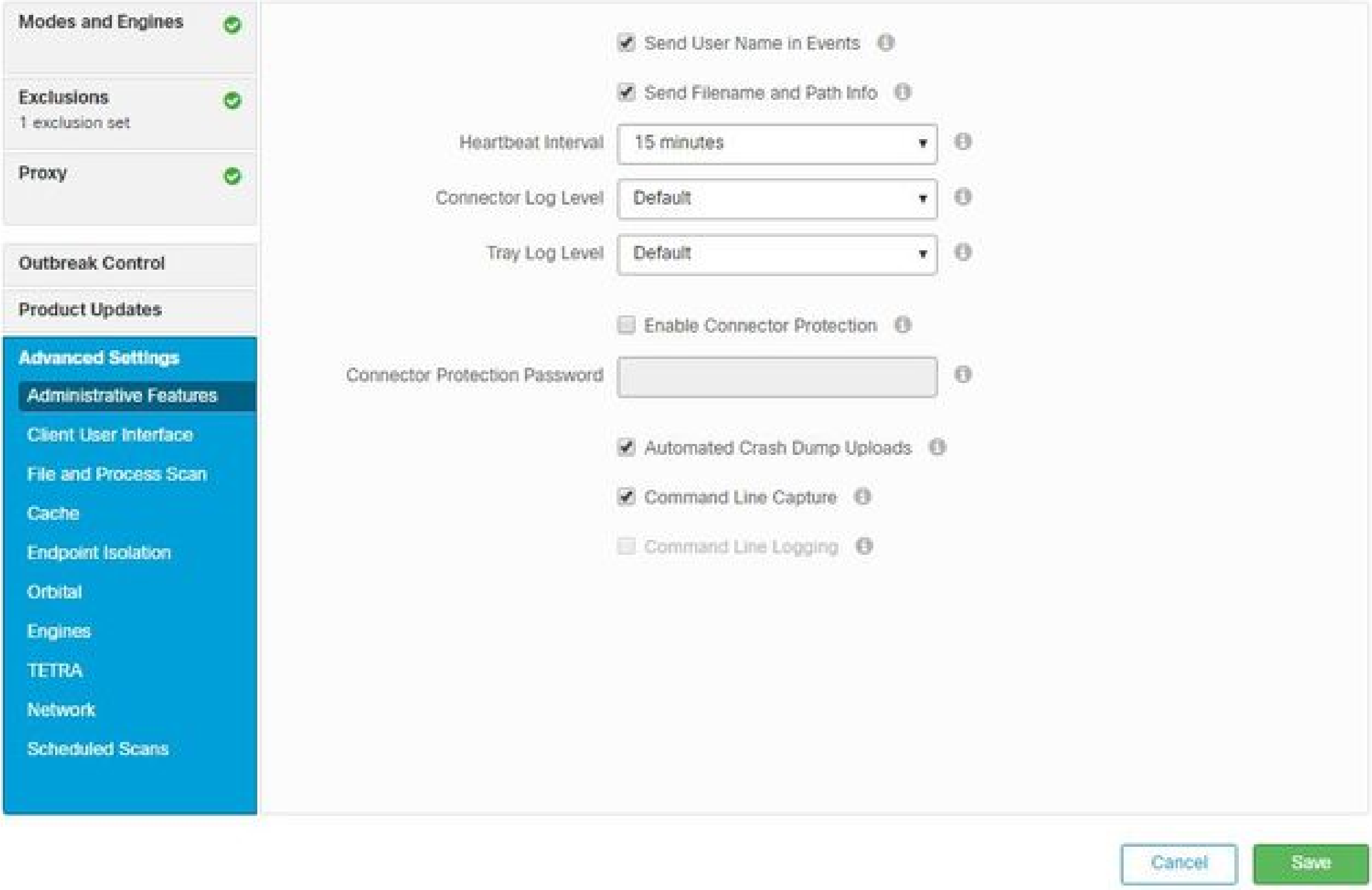
□ Block Update if Reboot Required

Reboot: Do not reboot

Reboot Delay: 2 minutes

In the Product Update section, options for new updates are set. You can choose a version, date range to roll updates and options for a reboot.

Advanced Settings



☑ Send User Name in Events

☑ Send Filename and Path Info

Heartbeat Interval: 15 minutes

Connector Log Level: Default

Tray Log Level: Default

□ Enable Connector Protection

Connector Protection Password:

☑ Automated Crash Dump Uploads

☑ Command Line Capture

□ Command Line Logging

Administrative features: Configures how often the connector queries the cloud for changes to the policy.

Client User interface: Allows you to control the display of notifications in your devices where AMP is installed.

File and Process Scan: configures real-time protection options, how connectors check for file dispositions, and maximum file sizes allowed.

Cache: Time To Live configuration for cache.

Endpoint isolation allows you to enable and configure the feature to isolate devices with the AMP connector installed.

Orbital option enables the orbital advanced search.

Engines: Settings for ETHOS; a file grouping engine, and SPERO; a machine-based learning system.

TETRA configuration for the offline engine.

Network Enables the Device Flow Correlation options.

In the Scheduled Scans section you can configure the options for when and what type of scans you want to run in the connectors.

Save Changes

After you perform any changes, click **Save** to ensure that they are applied to the policy.

You can also find the information contained in this document in the Windows Policy Configuration in AMP for Endpoints video.

Related Information

- For more information on the policy configuration, navigate to the User Guide
- **Technical Support & Documentation - Cisco Systems**