在面向終端的AMP中配置Windows策略

目錄

簡介

本檔案介紹在面向終端的高級惡意軟體防護(AMP)Windows策略中可配置的元件。

必要條件

需求

思科建議您瞭解以下主題：

- 具有管理員許可權的AMP for Endpoints使用者

採用元件

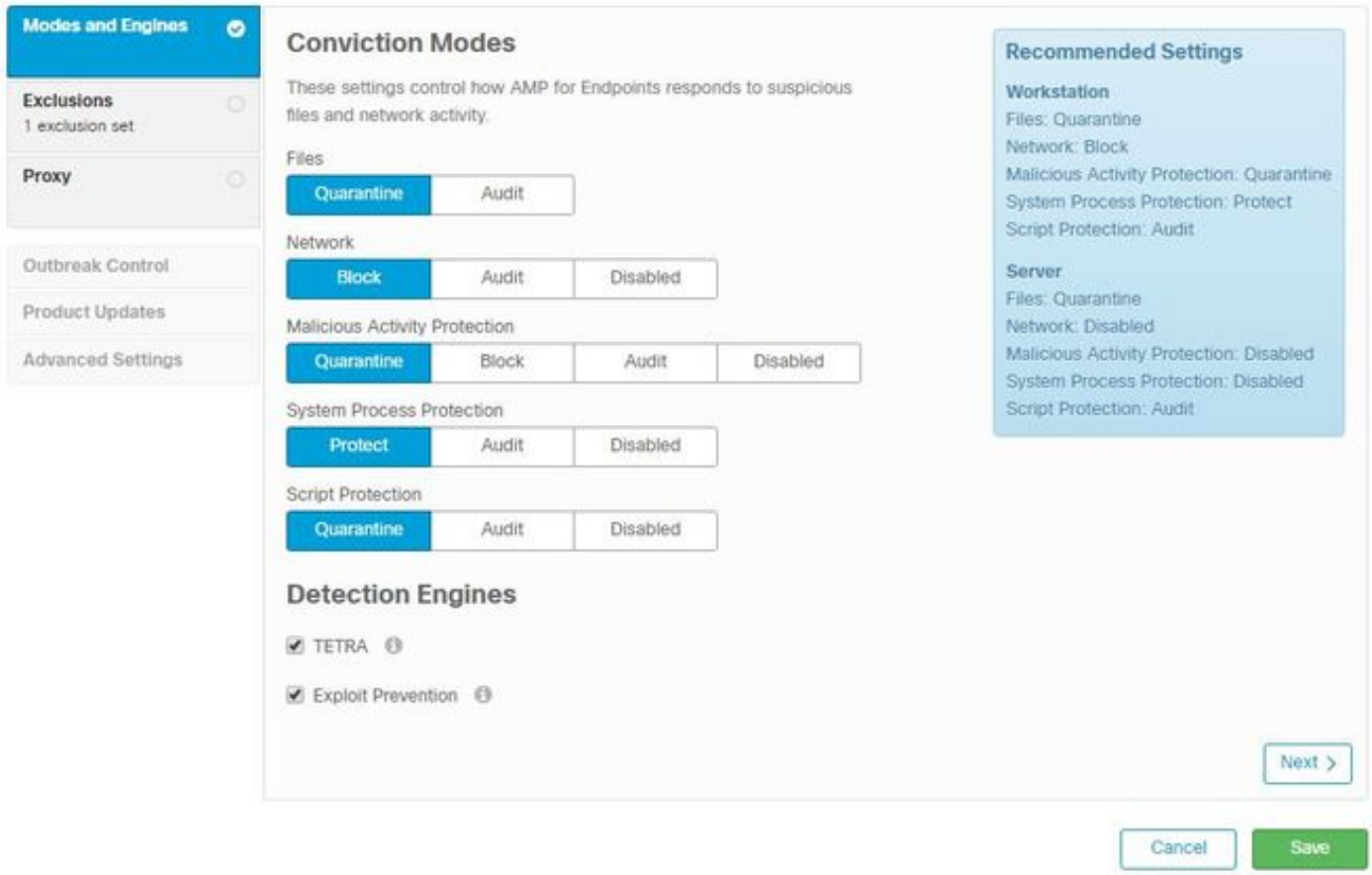
本檔案中的資訊是根據面向終端的AMP主控台。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

要建立新的Windows策略，請導航到管理頁籤並選擇策略。在策略部分，建立新的Windows策略。

模式和引擎



檔案：AMP的主要SHA引擎和核心功能。此選項允許檔案掃描和隔離。

網路：監控連線的裝置流關聯引擎。

惡意活動保護：保護端點免受勒索軟體攻擊的引擎。

系統進程保護：通過記憶體注入攻擊保護關鍵Windows系統進程免受危害的引擎。

指令碼保護：提供對基於指令碼的攻擊的可視性。

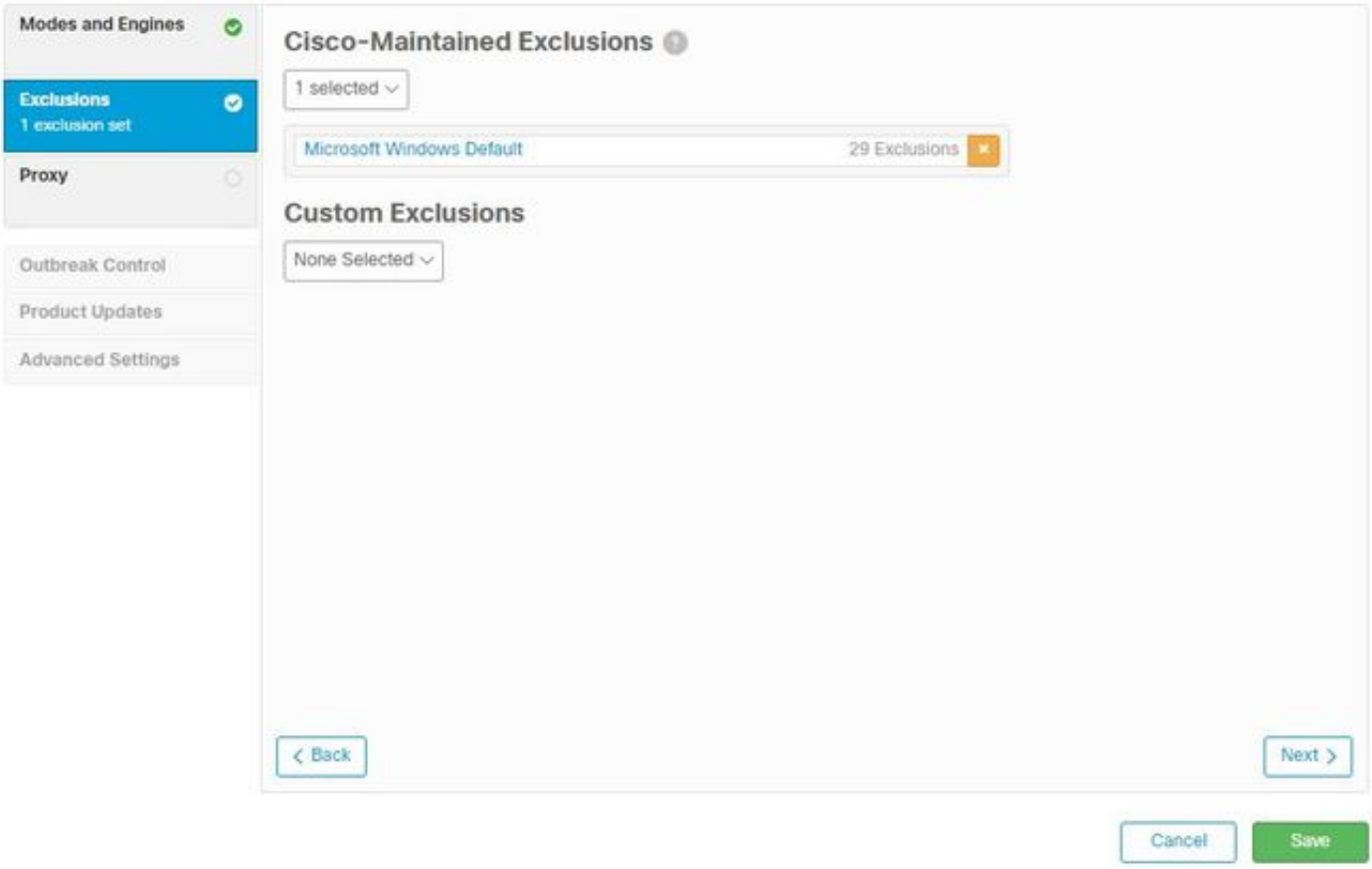
檢測引擎：

- Tetra：下載定義以保護終端的離線防病毒軟體
- 惡意探索防護保護聯結器免受記憶體注入攻擊

附註：工作站和伺服器的建議設定視窗顯示在右側。

設定「模式和引擎」部分後，按一下「**Next**」，如下圖所示。

排除



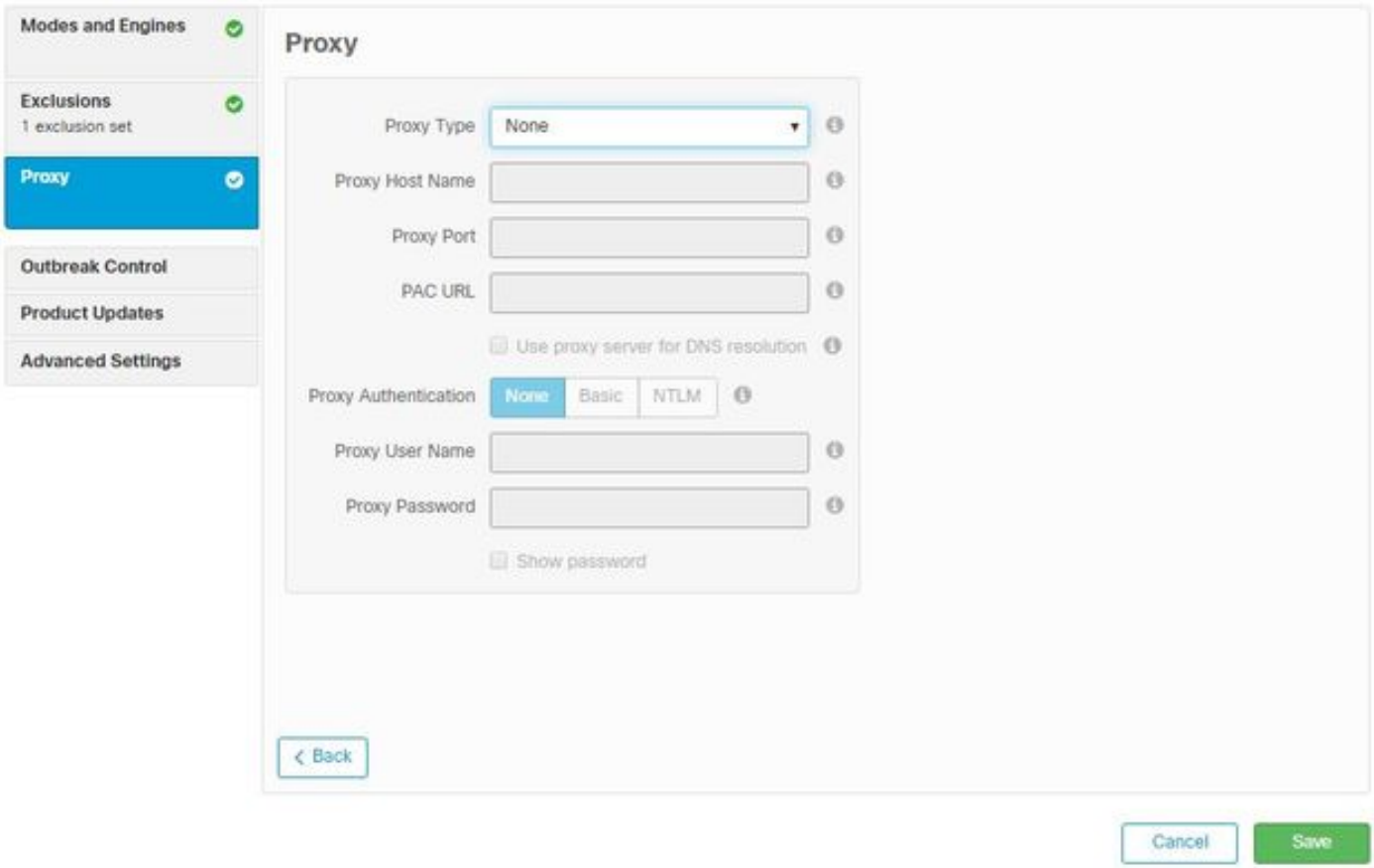
排除部分包含思科維護的排除和自定義排除：

- 思科維護的排除項由思科建立並維護，允許您從AMP的掃描中排除常見應用，以避免不相容問題
- 自定義排除項由使用者管理員建立和維護

如果您想瞭解有關排除的詳細資訊，可以在此影片中找到詳細資訊。

完成「排除」配置後，按一下**下一步**，如下圖所示。

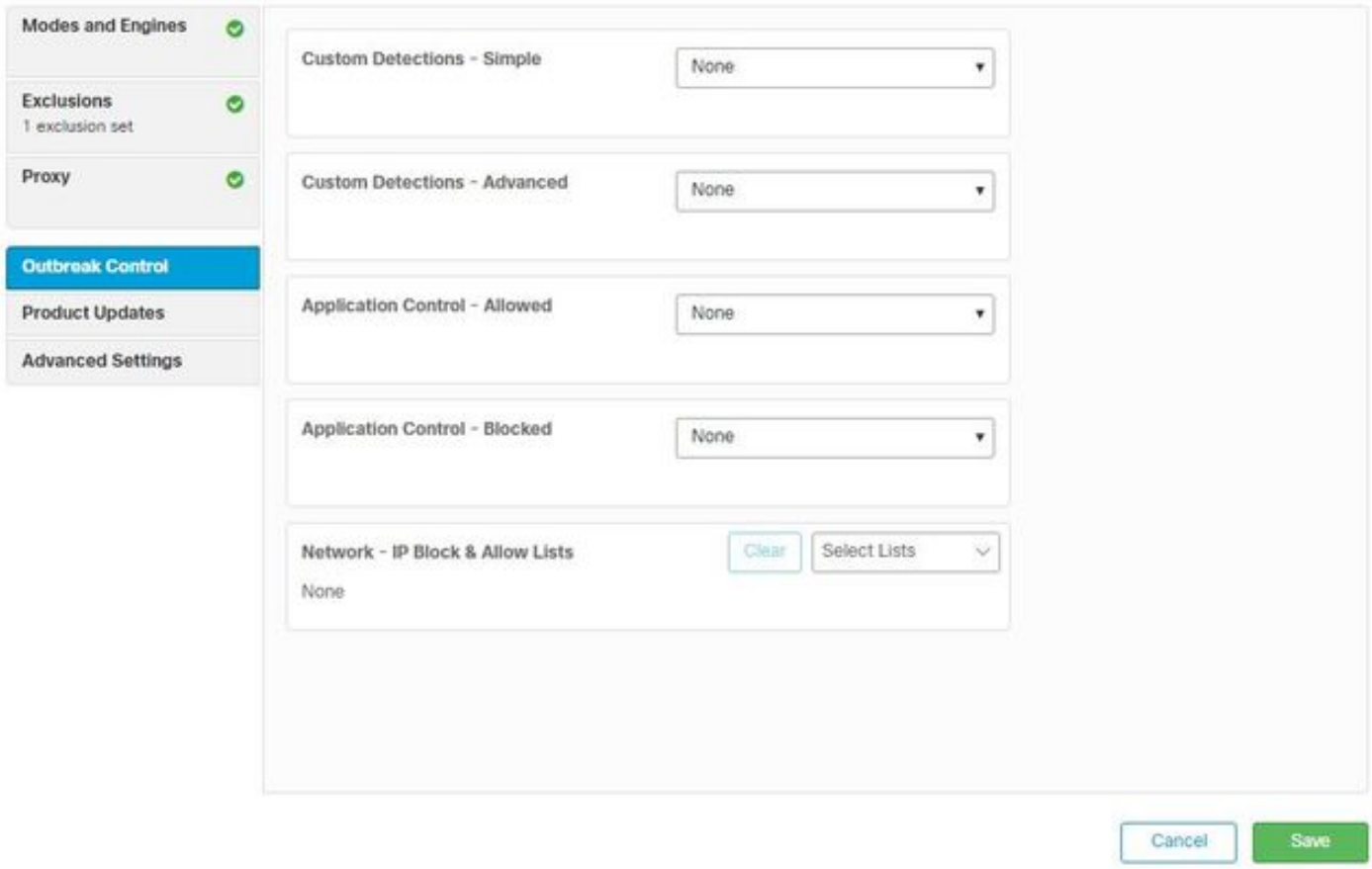
代理



在本節中，您可以根據您的環境配置代理設定，以允許聯結器查詢AMP雲。

設定代理設定後，按一下**Save**，如下圖所示。

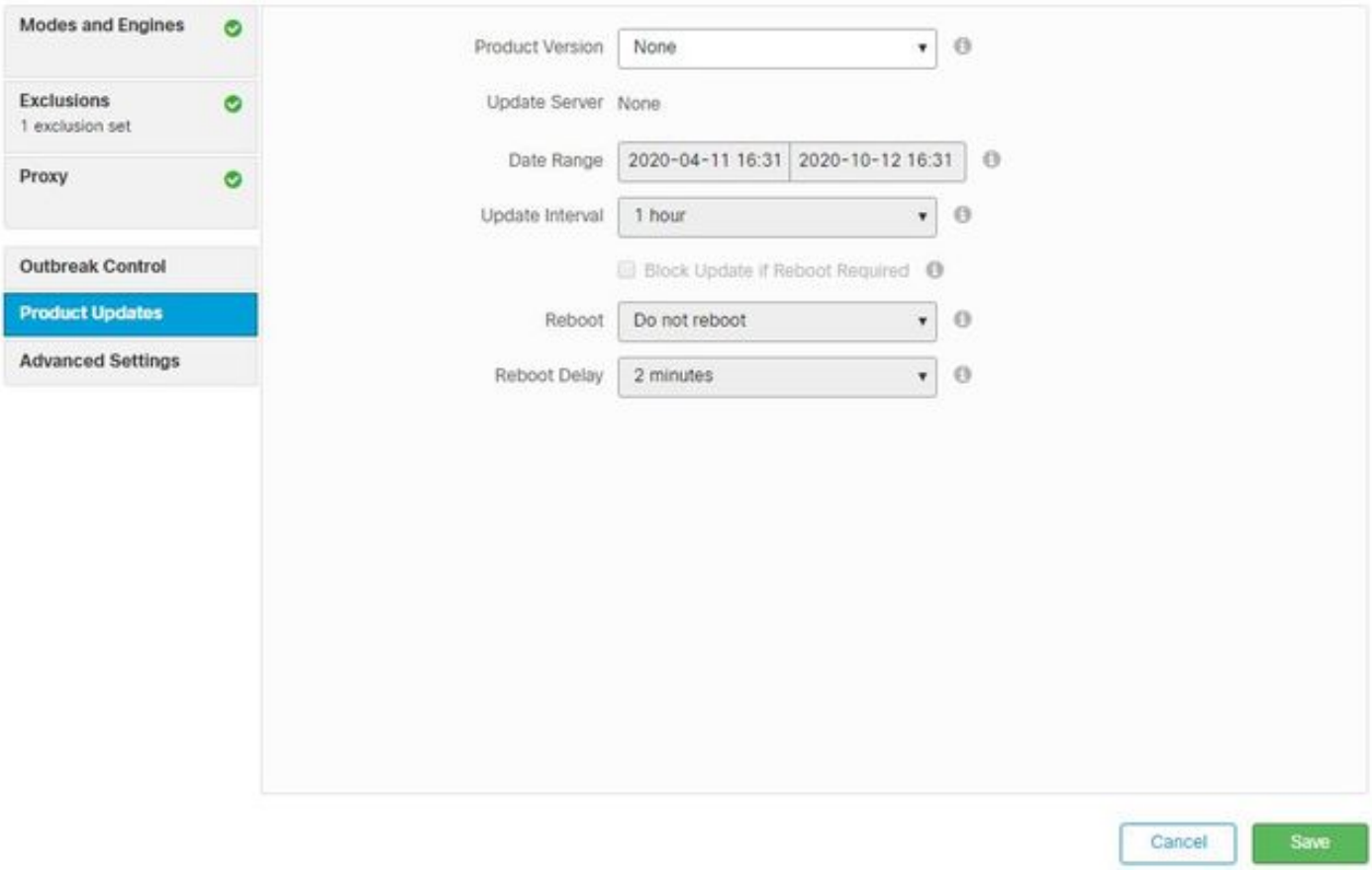
爆發控制



在「爆發控制」部分，可以配置自定義檢測：

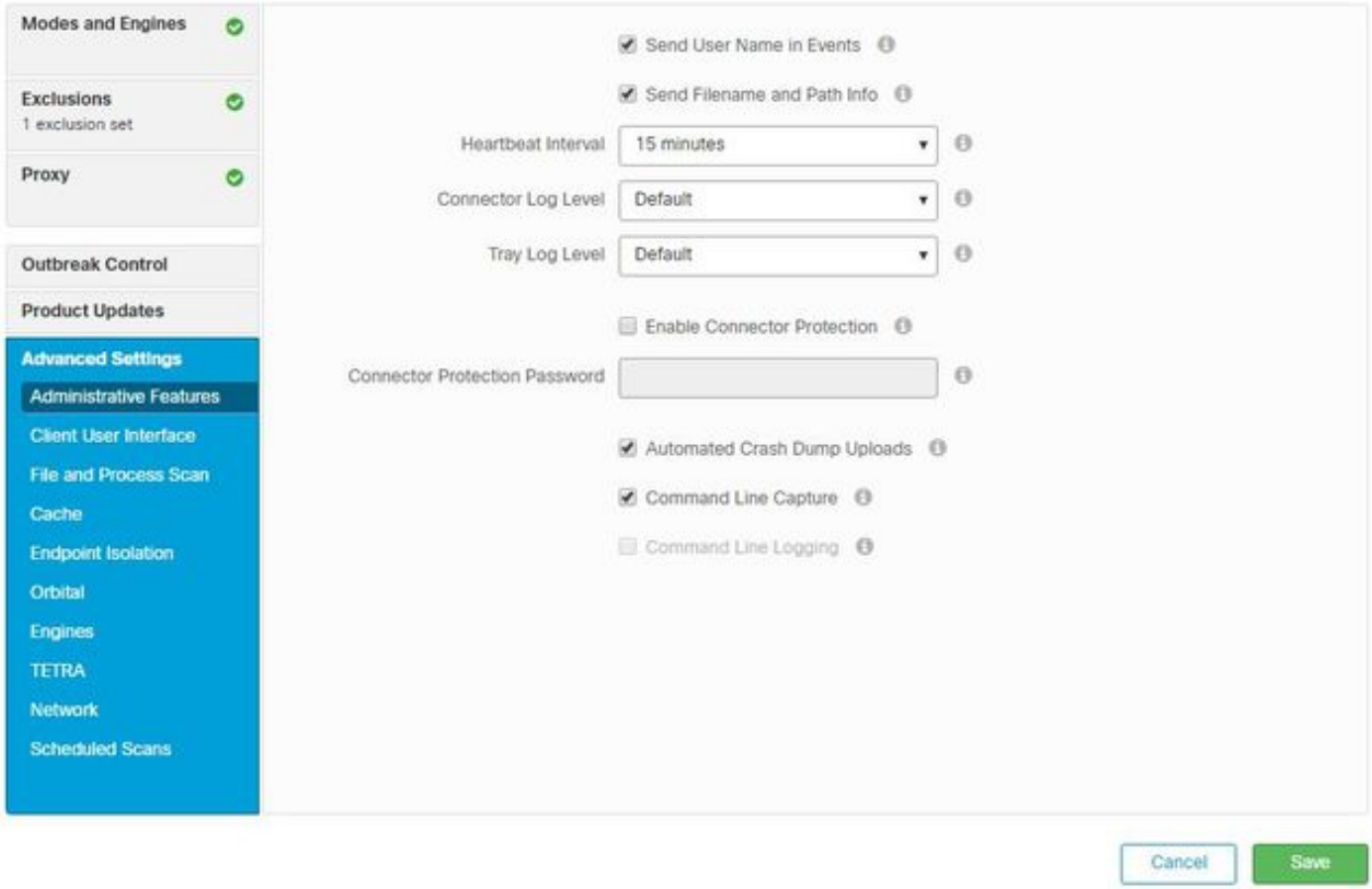
- 自定義檢測 — 簡單：允許您根據特定檔案的SHA阻止這些檔案
- 自定義檢測 — 高級：基於簽名阻止檔案，以便在簡單SHA不足時進行檢測
- 允許的應用和阻止的清單：允許或阻止具有SHA的應用
- 網路 — IP阻止和允許清單：與裝置流關聯(DFC)一起使用，用於定義自定義IP地址檢測

產品更新



在「產品更新」部分中，設定了新更新的選項。您可以選擇版本、用於滾動更新的日期範圍以及重新啟動的選項。

高級設定



管理功能：配置聯結器向雲查詢策略更改的頻率。

客戶端使用者介面：允許您控制安裝AMP的裝置中的通知顯示。

檔案和進程掃描：配置即時保護選項、聯結器檢查檔案性質的方式以及允許的最大檔案大小。

快取：快取的生存時間配置。

終端隔離允許您啟用和配置功能以隔離安裝了AMP聯結器的裝置。

軌道選項使軌道高級搜尋成為可能。

引擎：ETHOS設定；檔案分組引擎和SPERO;基於機器的學習系統。

離線引擎的TETRA配置。

網路啟用裝置流關聯選項。

在「計畫的掃描」部分中，可以配置要在聯結器中運行掃描的時間和型別選項。

儲存更改

執行任何更改後，按一下**Save**以確保將更改應用於策略。

您還可以在AMP for Endpoints影片的Windows策略配置中找到本文檔中包含的資訊。

相關資訊

- 有關策略配置的詳細資訊，請導航至《使用手冊》
- **技術支援與文件 - Cisco Systems**