

# AMP for Endpoints에서 Windows 정책 구성

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[모드 및 엔진](#)

[제외](#)

[프록시](#)

[보안 침해 제어](#)

[제품 업데이트](#)

[고급 설정](#)

[변경 내용 저장](#)

[관련 정보](#)

## 소개

이 문서에서는 AMP(Advanced Malware Protection) for Endpoints Windows 정책에서 구성 가능한 구성 요소에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 관리자 권한이 있는 AMP for Endpoints 사용자

### 사용되는 구성 요소

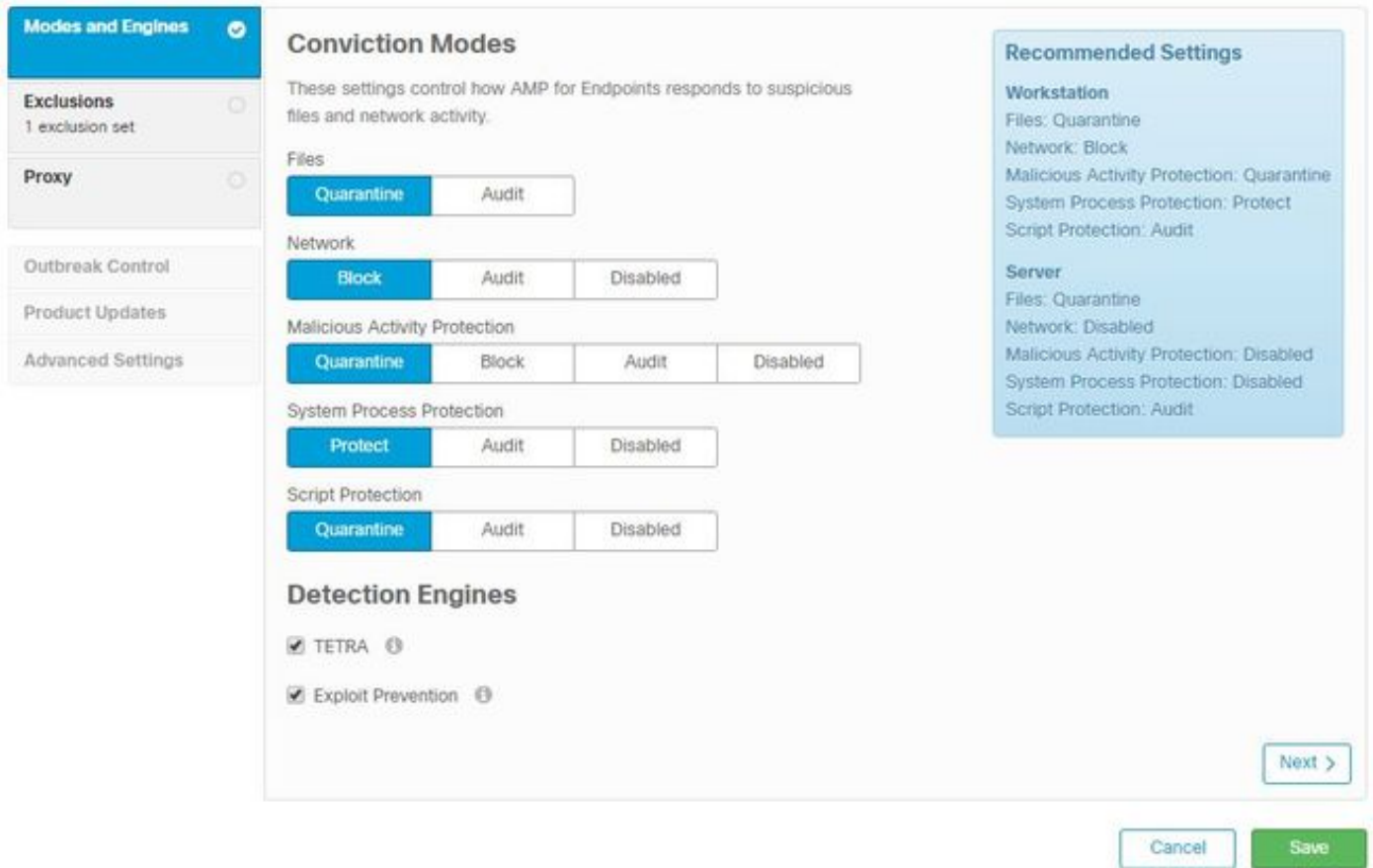
이 문서의 정보는 AMP for Endpoints Console을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 구성

새 Windows 정책을 생성하려면 관리 탭으로 이동하여 Policies를 선택합니다. 정책 섹션에서 새 Windows 정책을 만듭니다.

### 모드 및 엔진



파일:AMP의 주요 SHA 엔진 및 핵심 기능.이 옵션은 파일 스캔 및 격리를 허용합니다.

네트워크:연결을 모니터링하는 Device Flow Correlation 엔진입니다.

악의적인 활동 보호:엔드포인트를 랜섬웨어 공격으로부터 보호하는 엔진입니다.

시스템 프로세스 보호:메모리 주입 공격을 통해 중요한 Windows 시스템 프로세스를 보안하는 엔진입니다.

스크립트 보호:스크립트 기반 공격에 대한 가시성을 제공합니다.

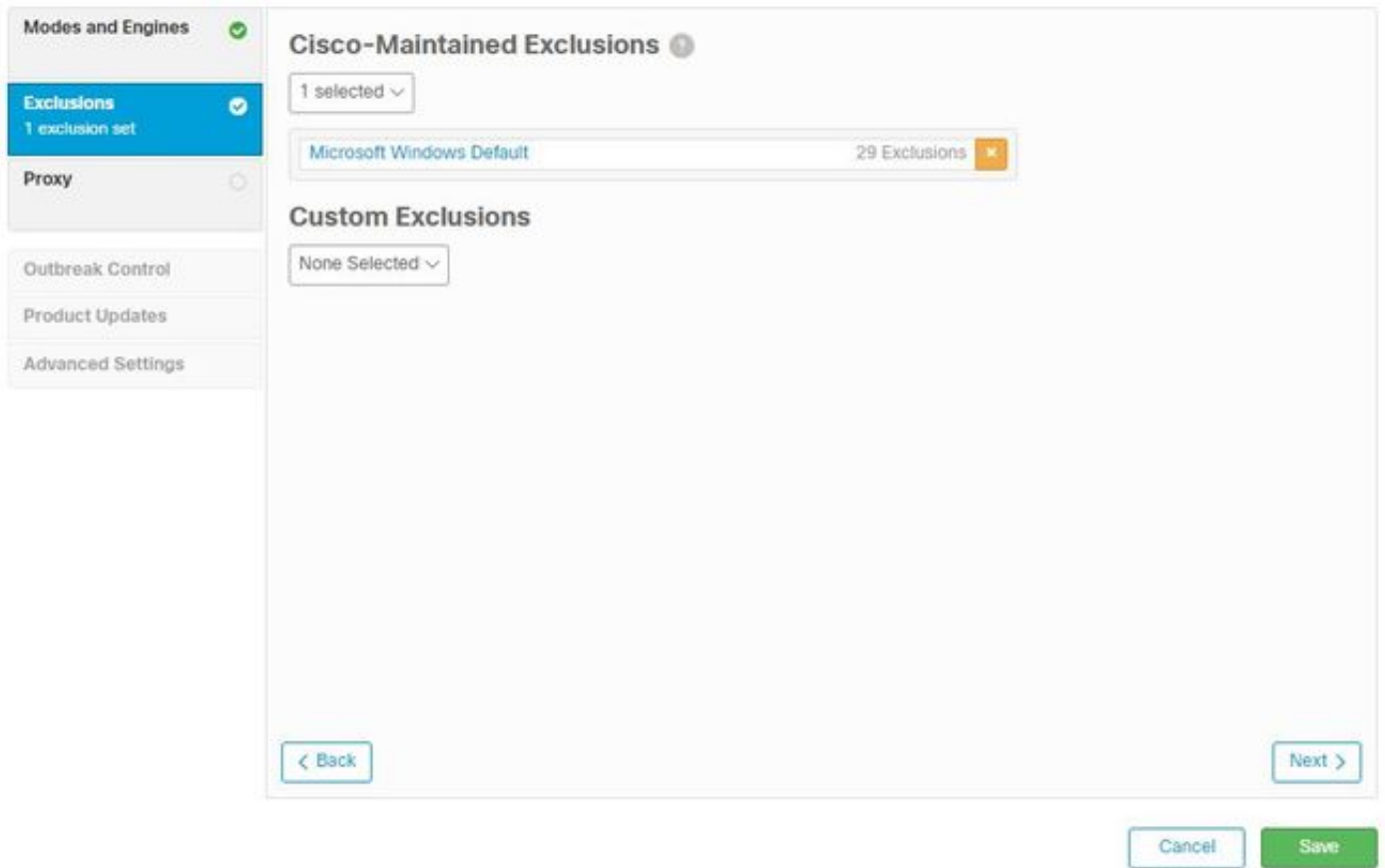
탐지 엔진:

- 텍스트:엔드포인트를 보호하기 위해 정의를 다운로드하는 오프라인 안티바이러스
- 익스플로잇 방지:메모리 주입 공격으로부터 커넥터 보호

참고:워크스테이션 및 서버에 대한 권장 설정 창이 오른쪽 섹션에 표시됩니다.

모드 및 엔진 섹션의 컨피그레이션 후 이미지에 표시된 대로 다음을 클릭합니다.

제외



제외 섹션에는 Cisco에서 유지 관리하는 제외 및 사용자 지정 제외가 포함되어 있습니다.

- Cisco에서 Cisco 유지 관리 제외를 생성하고 유지 관리하며, 비호환성 문제를 방지하기 위해 AMP의 검사에서 공통 애플리케이션을 제외할 수 있습니다.
- 사용자 지정 제외는 사용자 관리자가 생성하고 유지 관리합니다.

제외에 대해 자세히 알아보려면 이 [비디오](#)에서 자세한 정보를 확인할 수 있습니다.

제외 컨피그레이션을 완료했으면 이미지에 표시된 대로 **다음**을 클릭합니다.

## 프록시

The image shows a web interface for configuring proxy settings. On the left, a sidebar lists several sections: 'Modes and Engines' (checked), 'Exclusions' (1 exclusion set, checked), 'Proxy' (selected and highlighted in blue), 'Outbreak Control', 'Product Updates', and 'Advanced Settings'. The main area is titled 'Proxy' and contains the following configuration options:

- Proxy Type:** A dropdown menu currently set to 'None'.
- Proxy Host Name:** An empty text input field.
- Proxy Port:** An empty text input field.
- PAC URL:** An empty text input field.
- Use proxy server for DNS resolution:** An unchecked checkbox.
- Proxy Authentication:** Three tabs labeled 'None', 'Basic', and 'NTLM', with 'None' selected.
- Proxy User Name:** An empty text input field.
- Proxy Password:** An empty text input field.
- Show password:** An unchecked checkbox.

At the bottom left of the main area is a '< Back' button. At the bottom right are 'Cancel' and 'Save' buttons.

이 섹션에서는 커넥터가 AMP 클라우드를 쿼리할 수 있도록 환경별로 프록시 설정을 구성할 수 있습니다.

프록시 설정을 구성한 후 이미지에 표시된 대로 **저장**을 클릭합니다.

## 보안 침해 제어

The screenshot displays the 'Outbreak Control' configuration page. On the left, a navigation menu includes 'Modes and Engines', 'Exclusions', 'Proxy', 'Outbreak Control' (selected), 'Product Updates', and 'Advanced Settings'. The main content area is divided into several sections, each with a dropdown menu currently set to 'None':

- Custom Detections - Simple
- Custom Detections - Advanced
- Application Control - Allowed
- Application Control - Blocked
- Network - IP Block & Allow Lists (includes a 'Clear' button and a 'Select Lists' dropdown)

At the bottom right of the interface, there are 'Cancel' and 'Save' buttons.

Outbreak Control 섹션에서 맞춤형 탐지를 구성할 수 있습니다.

- 맞춤형 탐지 - 단순:SHA를 기반으로 특정 파일을 차단할 수 있습니다.
- 맞춤형 탐지 - 고급:단순 SHA가 충분하지 않을 경우 시그니처를 기반으로 파일을 차단합니다.
- 애플리케이션 허용 및 차단 목록:SHA가 있는 애플리케이션을 허용하거나 차단합니다.
- 네트워크 - IP 차단 및 허용 목록:사용자 지정 IP 주소 탐지를 정의하기 위해 DFC(Device Flow Correlation)와 함께 사용

## 제품 업데이트

- Modes and Engines ✔
- Exclusions ✔  
1 exclusion set
- Proxy ✔
- Outbreak Control
- Product Updates
- Advanced Settings

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 ?

Cancel
Save

제품 업데이트 섹션에서 새 업데이트에 대한 옵션이 설정됩니다. 버전, 날짜 범위를 선택하여 업데이트를 롤하고 재부팅할 옵션을 선택할 수 있습니다.

## 고급 설정

- Modes and Engines ✔
- Exclusions ✔  
1 exclusion set
- Proxy ✔
- Outbreak Control
- Product Updates
- Advanced Settings
- Administrative Features
- Client User Interface
- File and Process Scan
- Cache
- Endpoint Isolation
- Orbital
- Engines
- TETRA
- Network
- Scheduled Scans

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 ?

Cancel
Save

관리 기능: 커넥터가 클라우드에서 정책 변경 사항을 쿼리하는 빈도를 구성합니다.

클라이언트 사용자 인터페이스: AMP가 설치된 디바이스에서 알림 표시를 제어할 수 있습니다.

파일 및 프로세스 스캔: 실시간 보호 옵션, 커넥터에서 파일 속성을 확인하는 방법, 허용되는 최대 파일 크기를 구성합니다.

캐시: 캐시에 대한 Time To Live 컨피그레이션입니다.

엔드포인트 격리를 사용하면 AMP 커넥터가 설치된 디바이스를 격리하도록 기능을 활성화하고 구성할 수 있습니다.

쿼드 옵션은 쿼드 고급 검색을 활성화합니다.

엔진: ETHOS 설정; 파일 그룹화 엔진 및 SPERO, 기계 기반 학습 시스템.

오프라인 엔진의 TETRA 컨피그레이션입니다.

Network(네트워크)는 Device Flow Correlation(디바이스 플로우 상관관계) 옵션을 활성화합니다.

Scheduled Scans(예약된 스캔) 섹션에서 커넥터에서 실행할 스캔 시간 및 유형에 대한 옵션을 구성할 수 있습니다.

## 변경 내용 저장

변경 사항을 수행한 후 **Save(저장)**를 클릭하여 정책이 적용되는지 확인합니다.

[AMP for Endpoints](#) 비디오의 [Windows Policy Configuration\(Windows 정책 컨피그레이션\)](#)에서 이 문서에 포함된 정보를 찾을 수도 있습니다.

## 관련 정보

- [정책 컨피그레이션에 대한 자세한 내용은 사용 설명서를 참조하십시오.](#)
- [기술 지원 및 문서 - Cisco Systems](#)