

# エンドポイント用AMPでのWindowsポリシーの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[モードとエンジン](#)

[除外](#)

[プロキシ](#)

[アウトブレイク制御](#)

[製品の更新](#)

[高度な設定](#)

[変更の保存](#)

[関連情報](#)

## 概要

このドキュメントでは、Advanced Malware Protection(AMP)for Endpoints Windowsポリシーで設定可能なコンポーネントについて説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- 管理者権限を持つAMP for Endpointsユーザ

### 使用するコンポーネント

このドキュメントの情報は、AMP for Endpointsコンソールに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 設定

新しいWindowsポリシーを作成するには、[management]タブに移動し、[Policies]を選択します。

[ポリシー]セクションで、新しいWindowsポリシーを作成します。

## モードとエンジン

**Modes and Engines**

**Exclusions**   
1 exclusion set

**Proxy**

**Outbreak Control**

**Product Updates**

**Advanced Settings**

### 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

Next >

Cancel Save

files:AMPの主要なSHAエンジンおよびコア機能。このオプションを使用すると、ファイルスキャンと検疫を実行できます。

ネットワーク：接続を監視するデバイスフロー関連エンジン。

悪意のあるアクティビティの保護：エンドポイントをランサムウェア攻撃から保護するエンジン。

システムプロセス保護：メモリーインジェクション攻撃によって、重要なWindowsシステムプロセスを妥協から保護するエンジン。

スクリプトの保護：スクリプトベースの攻撃を可視化します。

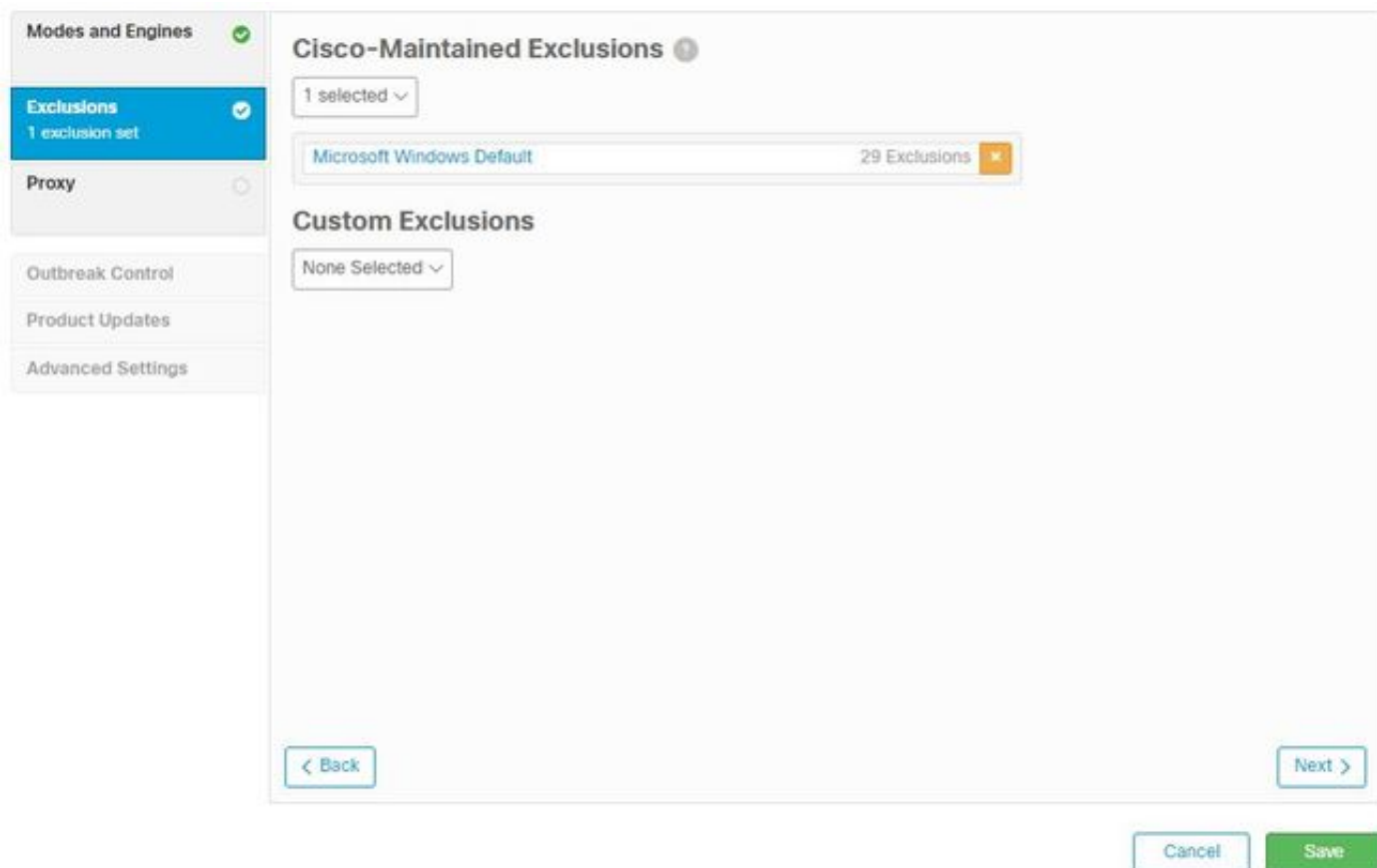
検出エンジン：

- Tetra：エンドポイントを保護するために定義をダウンロードするオフラインウイルス対策
- エクスプロイト防止：コネクタをメモリーインジェクション攻撃から保護

注：ワークステーションとサーバの推奨設定ウィンドウが右側のセクションに表示されます。

[モードとエンジン]セクションの設定が完了したら、図に示すように[次へ]をクリックします。

## 除外



除外セクションには、シスコが管理する除外とカスタム除外が含まれます。

- シスコが提供する除外はシスコが作成および維持し、AMPによるスキャンから一般的なアプリケーションを除外して、非互換性の問題を回避できます
- カスタム除外は、ユーザ管理者が作成し、維持します

除外について詳しく知りたい場合は、このビデオで詳細な情報を見つけることが[できます](#)。

除外の設定が完了したら、図に示すように[Next]をクリックします。

## プロキシ

Modes and Engines ✓

Exclusions ✓  
1 exclusion set

**Proxy** ✓

Outbreak Control

Product Updates

Advanced Settings

### 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

< Back

Cancel Save

このセクションでは、コネクタがAMPクラウドを照会できるように、環境ごとにプロキシ設定を構成できます。

プロキシ設定を構成したら、図に示すように[Save]をクリックします。

## アウトブレイク制御

Modes and Engines ✓

Exclusions ✓  
1 exclusion set

Proxy ✓

**Outbreak Control**

Product Updates

Advanced Settings

Custom Detections - Simple None ▼

Custom Detections - Advanced None ▼

Application Control - Allowed None ▼

Application Control - Blocked None ▼

Network - IP Block & Allow Lists  
None Clear Select Lists ▼

Cancel Save

[Outbreak Control]セクションでは、カスタム検出を設定できます。

- カスタム検出：シンプル：SHAに基づいて特定のファイルをブロックできます
- カスタム検出 – 詳細：単純なSHAが不十分な場合の検出のために、シグニチャに基づいてファイルをブロックします
- [Application Allowed]および[Blocked]リスト：SHAを使用してアプリケーションを許可またはブロックする
- ネットワーク – IPブロックと許可リスト：カスタムIPアドレス検出を定義するためにデバイスフロー相関(DFC)とともに使用される

## 製品の更新

Modes and Engines <span>✔</span>	Product Version <input type="text" value="None"/> ⓘ
Exclusions <span>✔</span> 1 exclusion set	Update Server None
Proxy <span>✔</span>	Date Range <input type="text" value="2020-04-11 16:31"/> <input type="text" value="2020-10-12 16:31"/> ⓘ
Outbreak Control	Update Interval <input type="text" value="1 hour"/> ⓘ
<b>Product Updates</b>	<input type="checkbox"/> Block Update if Reboot Required ⓘ
Advanced Settings	Reboot <input type="text" value="Do not reboot"/> ⓘ
	Reboot Delay <input type="text" value="2 minutes"/> ⓘ

[Product Update (製品の更新)]セクションで、新しい更新のオプションを設定します。バージョン、日付範囲を選択して、更新を実行したり、再起動のオプションを選択できます。

## 高度な設定

Modes and Engines <span>✔</span>	<input checked="" type="checkbox"/> Send User Name in Events ⓘ
Exclusions <span>✔</span> 1 exclusion set	<input checked="" type="checkbox"/> Send Filename and Path Info ⓘ
Proxy <span>✔</span>	Heartbeat Interval <input type="text" value="15 minutes"/> ⓘ
Outbreak Control	Connector Log Level <input type="text" value="Default"/> ⓘ
Product Updates	Tray Log Level <input type="text" value="Default"/> ⓘ
<b>Advanced Settings</b>	<input type="checkbox"/> Enable Connector Protection ⓘ
<b>Administrative Features</b>	Connector Protection Password <input type="text"/> ⓘ
Client User Interface	<input checked="" type="checkbox"/> Automated Crash Dump Uploads ⓘ
File and Process Scan	<input checked="" type="checkbox"/> Command Line Capture ⓘ
Cache	<input type="checkbox"/> Command Line Logging ⓘ
Endpoint Isolation	
Orbital	
Engines	
TETRA	
Network	
Scheduled Scans	

管理機能：コネクタがクラウドにポリシーの変更を照会する頻度を設定します。

クライアントユーザインターフェイス：AMPがインストールされているデバイスでの通知の表示を制御できます。

ファイルおよびプロセススキャン：リアルタイム保護オプション、コネクタによるファイルの配置の確認方法、および許可される最大ファイルサイズを設定します。

Cache: キャッシュの存続可能時間(TTL)設定。

エンドポイントの分離では、AMPコネクタがインストールされているデバイスを分離する機能を有効にして設定できます。

軌道オプションは、軌道の高度な検索を有効にします。

エンジン：ETHOSの設定ファイル・グループ化エンジン、SPEROマシンベースの学習システム。

オフラインエンジンのTETRA設定。

[Network]:[Device Flow Correlation]オプションを有効にします。

「スケジュールされたスキャン」セクションでは、コネクタで実行するスキャンのタイミングと種類を設定できます。

## 変更の保存

変更を実行した後、[Save]をクリックしてポリシーに適用されていることを確認します。

このドキュメントに含まれている情報は、『[AMP for Endpointsの](#)』ビデオの「[Windowsポリシーの設定](#)」にも記載されています。

## 関連情報

- [ポリシー設定の詳細については、『ユーザガイド』を参照してください](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)