

# Configurer la stratégie Windows dans AMP pour les terminaux

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Modes et moteurs](#)

[Exclusions](#)

[Proxy](#)

[Contrôle des attaques](#)

[Mises à jour des produits](#)

[Paramètres avancés](#)

[Sauvegardez les modifications](#)

[Informations connexes](#)

## Introduction

Ce document décrit les composants configurables dans la stratégie Windows Advanced Malware Protection (AMP) for Endpoints.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Utilisateur AMP for Endpoints avec privilèges d'administrateur

### Components Used

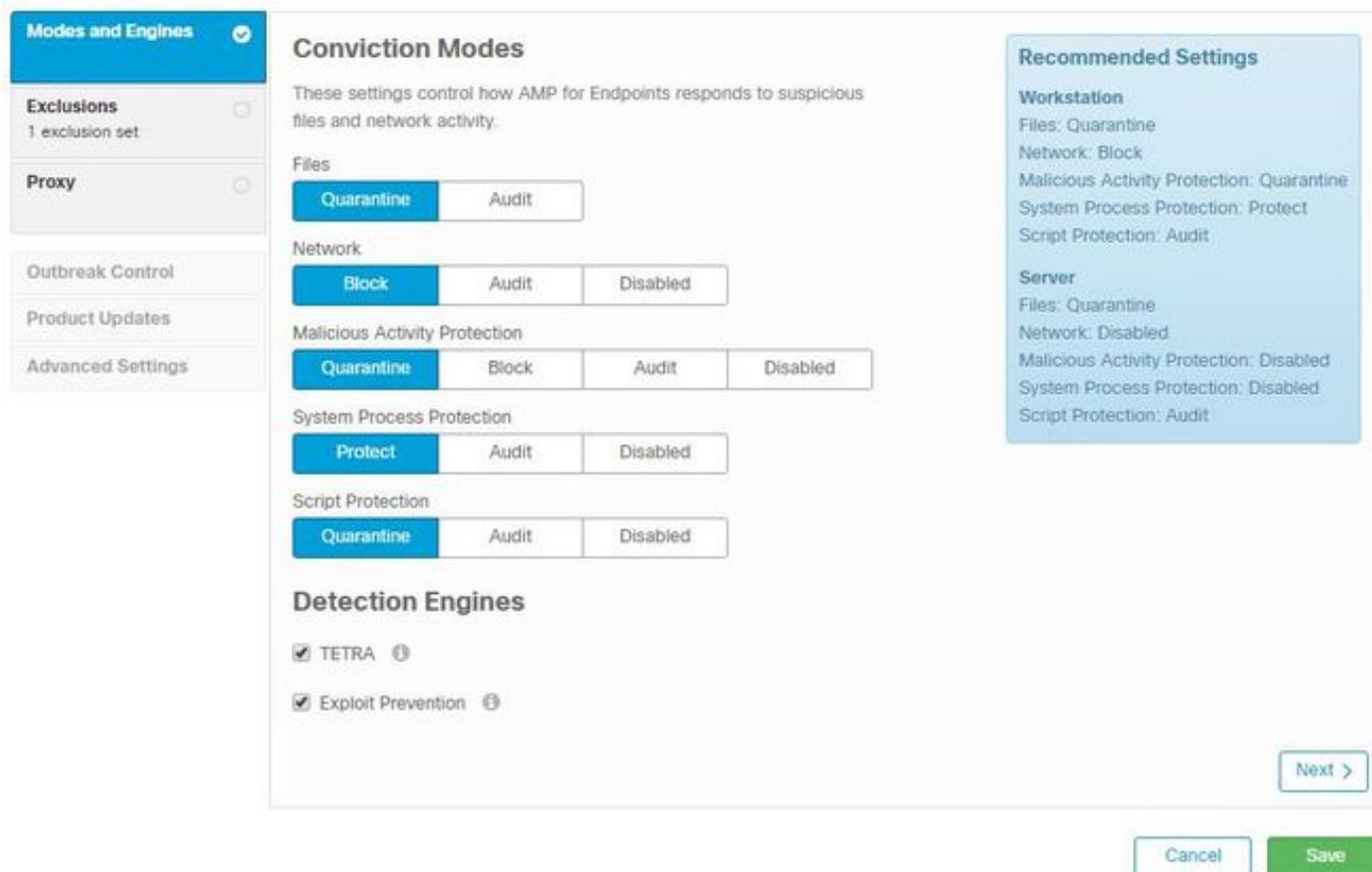
Les informations de ce document sont basées sur AMP for Endpoints Console.

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.

## Configuration

Afin de créer une nouvelle stratégie Windows, accédez à l'onglet de gestion et sélectionnez Stratégies. Dans la section Stratégie, créez une nouvelle stratégie Windows.

## Modes et moteurs



Fichiers : Le moteur SHA principal et la fonctionnalité principale d'AMP. Cette option permet d'effectuer des analyses de fichiers et de mettre en quarantaine.

Réseau: Moteur de corrélation de flux de périphérique qui surveille les connexions.

Protection contre les activités malveillantes : Moteur qui protège le terminal des attaques de ransomwares.

Protection des processus système : Moteur qui protège les processus système Windows critiques contre les attaques par injection de mémoire.

Protection des scripts : Offre une visibilité sur les attaques basées sur des scripts.

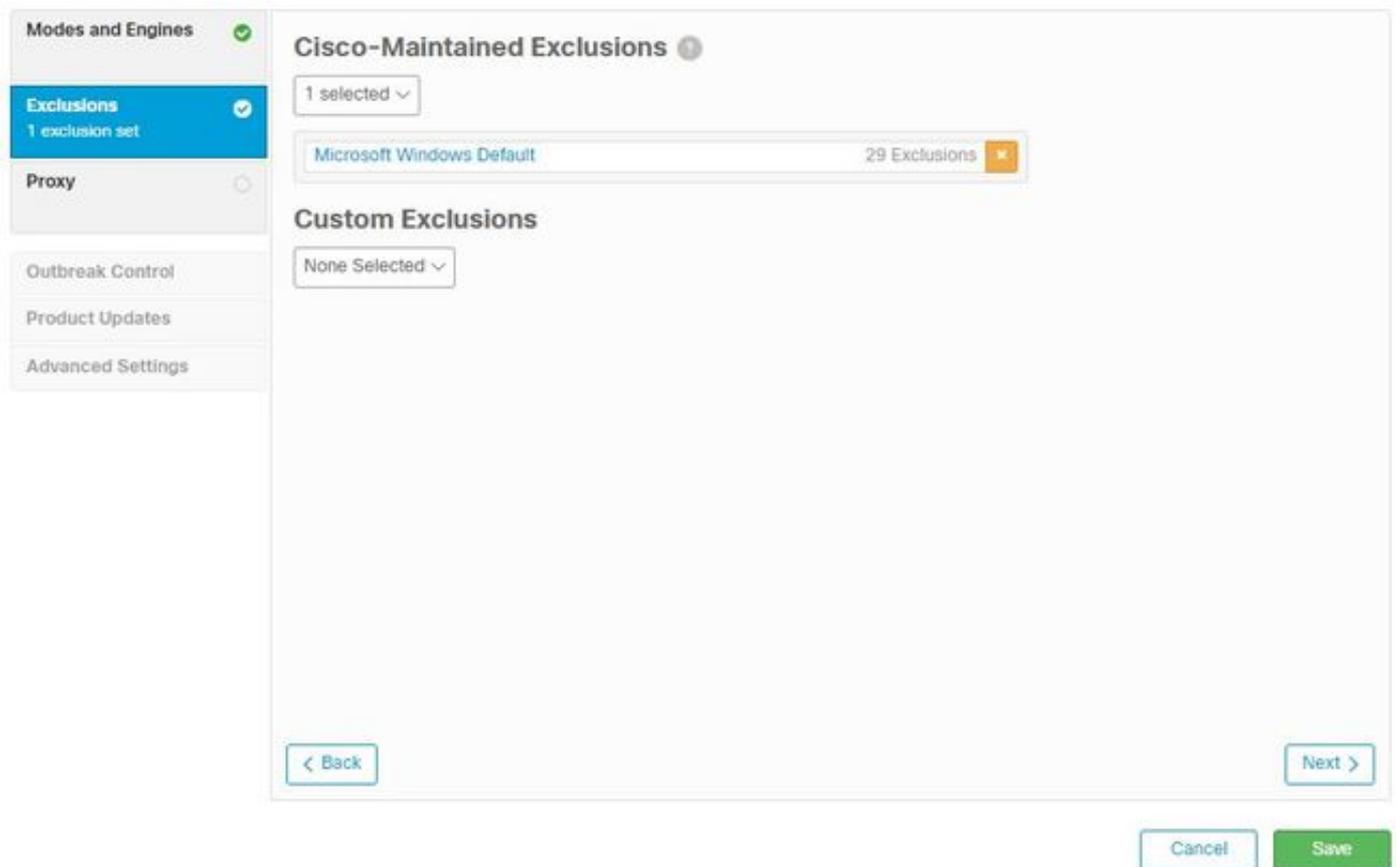
Moteurs de détection :

- Tetra : antivirus hors ligne qui télécharge les définitions pour protéger le terminal
- Prévention des attaques : Protection des connecteurs contre les attaques par injection de mémoire

**Note:** Une fenêtre contenant les paramètres recommandés pour les stations de travail et les serveurs s'affiche dans la section de droite.

Après la configuration de la section Modes and Engine, cliquez sur **Next**, comme illustré dans l'image.

## Exclusions



La section Exclusions contient les exclusions et les exclusions personnalisées gérées par Cisco :

- Les exclusions gérées par Cisco sont créées et gérées par Cisco et vous permettent d'exclure les applications courantes des analyses par AMP afin d'éviter les problèmes d'incompatibilité
- Les exclusions personnalisées sont créées et gérées par l'administrateur utilisateur

Si vous voulez en savoir plus sur les exclusions, vous pouvez trouver plus d'informations dans cette [vidéo](#).

Une fois la configuration Exclusions terminée, cliquez sur **Suivant**, comme l'illustre l'image.

## Proxy

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

Dans cette section, vous pouvez configurer les paramètres de proxy par environnement pour permettre au connecteur d'interroger le cloud AMP.

Après avoir configuré vos paramètres de proxy, cliquez sur **Enregistrer**, comme indiqué dans l'image.

## Contrôle des attaques

The screenshot displays the 'Outbreak Control' configuration page. On the left, a sidebar lists various settings: 'Modes and Engines' (checked), 'Exclusions' (1 exclusion set, checked), 'Proxy' (checked), 'Outbreak Control' (selected), 'Product Updates', and 'Advanced Settings'. The main content area is divided into five 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 main area, there are two buttons: 'Cancel' and 'Save'.

Dans la section Contrôle des attaques, vous pouvez configurer des détections personnalisées :

- Détections personnalisées - Simple : Vous permet de bloquer des fichiers spécifiques en fonction de leur SHA
- Détections personnalisées - Avancé : Bloque les fichiers basés sur des signatures, pour les détections lorsqu'un SHA simple n'est pas suffisant
- Listes d'applications autorisées et bloquées : Autorise ou bloque les applications avec des SHA
- Réseau - Listes de blocage et d'autorisation IP : Utilisé avec la corrélation de flux de périphériques (DFC) pour définir des détections d'adresses IP personnalisées

## Mises à jour des produits

The screenshot displays the 'Product Updates' configuration page. On the left, a sidebar lists several settings categories: 'Modes and Engines', 'Exclusions', 'Proxy', 'Outbreak Control', 'Product Updates' (highlighted in blue), and 'Advanced Settings'. The main content area is divided into several sections:

- Product Version:** A dropdown menu set to 'None'.
- Update Server:** A text field containing 'None'.
- Date Range:** Two date-time pickers showing '2020-04-11 16:31' and '2020-10-12 16:31'.
- Update Interval:** A dropdown menu set to '1 hour'.
- Block Update if Reboot Required:** An unchecked checkbox.
- Reboot:** A dropdown menu set to 'Do not reboot'.
- Reboot Delay:** A dropdown menu set to '2 minutes'.

At the bottom right of the main area, there are two buttons: 'Cancel' and 'Save'.

Dans la section Mise à jour du produit, les options pour les nouvelles mises à jour sont définies. Vous pouvez choisir une version, une plage de dates pour lancer les mises à jour et des options pour un redémarrage.

## Paramètres avancés

Fonctions administratives : Configure la fréquence à laquelle le connecteur interroge le cloud pour les modifications apportées à la stratégie.

Interface utilisateur client : Vous permet de contrôler l'affichage des notifications sur vos périphériques où AMP est installé.

Analyse des fichiers et des processus : configure les options de protection en temps réel, la manière dont les connecteurs vérifient la disposition des fichiers et la taille maximale des fichiers autorisée.

Cache : Configuration Time To Live pour le cache.

L'isolation des points de terminaison vous permet d'activer et de configurer la fonctionnalité pour isoler les périphériques avec le connecteur AMP installé.

L'option Orbital permet la recherche avancée orbitale.

Moteurs : Paramètres pour ETHOS ; un moteur de regroupement de fichiers et SPERO ; un système d'apprentissage automatique.

Configuration TETRA pour le moteur hors connexion.

Network (Réseau) : active les options de corrélation de flux de périphériques.

Dans la section Analyses planifiées, vous pouvez configurer les options pour le moment et le type d'analyses à exécuter dans les connecteurs.

## Sauvegardez les modifications

Après avoir effectué les modifications, cliquez sur **Enregistrer** pour vous assurer qu'elles sont appliquées à la stratégie.

Vous pouvez également trouver les informations contenues dans ce document dans la vidéo [Configuration de stratégie Windows dans AMP for Endpoints](#).

## Informations connexes

- [Pour plus d'informations sur la configuration de la stratégie, accédez au Guide de l'utilisateur](#)
- [Support et documentation techniques - Cisco Systems](#)