Modifications apportées à la liste d'exclusion de Cisco pour Cisco Secure Endpoint Console

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Attentes lors de la mise à jour
- Modifications
  - 18 décembre - 2024
    - VEEAM
    - Cisco WebEx
  - 4 juin - 2025
    - Microsoft Windows par défaut
    - Apple macOS par défaut
  - 17 septembre - 2025
    - Microsoft Windows par défaut
    - Apple macOS par défaut
  - 17 décembre - 2025
    - Microsoft Teams
  - 4 février - 2026
    - Microsoft Windows par défaut
    - Serveur Microsoft Exchange
    - Apsense
  - 23 septembre - 2026
    - Windows par défaut
    - Splunk - Windows
    - Hyper-V - Windows

Introduction

Ce document décrit les modifications apportées aux exclusions maintenues par Cisco.

Les exclusions maintenues par Cisco sont créées et maintenues par Cisco afin d'assurer une meilleure compatibilité entre Advanced Malware Protection (AMP) for Endpoints Connector et les logiciels antivirus, de sécurité ou autres. Ces exclusions peuvent être ajoutées aux nouvelles versions d'une application.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Exclusions dans AMP for Endpoints
- console AMP

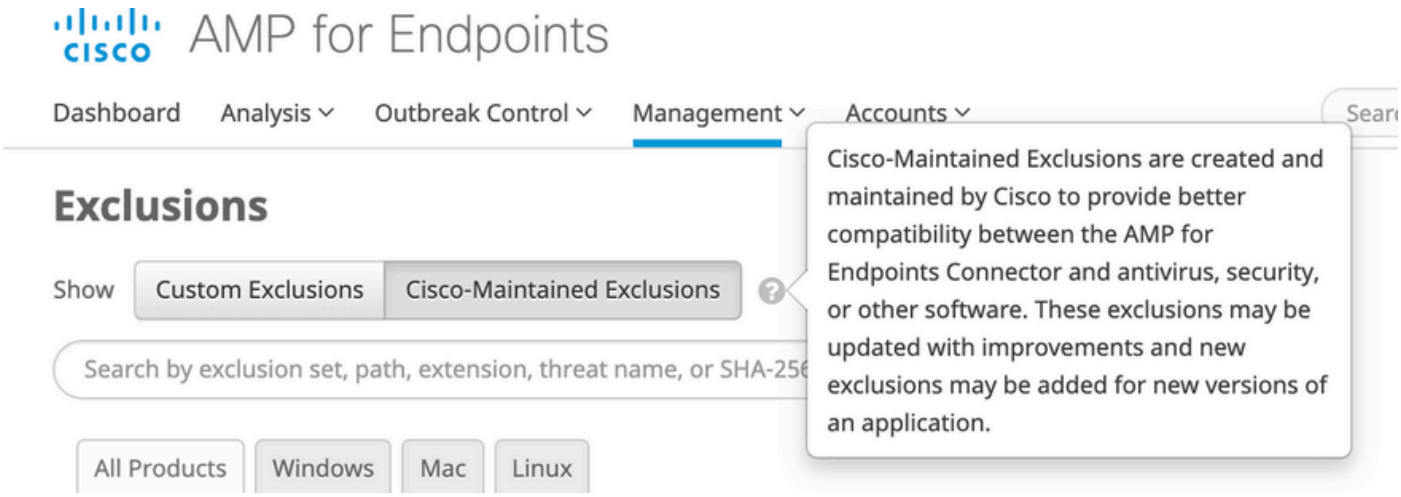
Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Console AMP for Endpoints version 5.4.20190820

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Attentes lors de la mise à jour



Lorsque les listes gérées par Cisco sont modifiées, une mise à jour de la stratégie est effectuée sur le serveur principal pour refléter cette modification. Lorsque chacun des terminaux utilise cette liste pour s'archiver sur leur pulsation, ils extraient la stratégie mise à jour. Ces modifications de stratégie ne sont pas reflétées dans le journal d'audit, car il s'agit techniquement d'une modification de la liste d'exclusion, et non de la stratégie elle-même, et les listes d'exclusion gérées

par Cisco n'existent pas dans le journal d'audit normal sur les consoles individuelles. Pour les environnements à grande échelle, cela ressemble à un déluge de mises à jour de politiques et le résultat final sera de meilleures performances sur chacun des terminaux.

La période de mise à jour dépend de chaque terminal. Si toutes les machines sont en ligne, les mises à jour s'effectueront en 1 à 2 pulsations. S'il s'agit d'un environnement global, les mises à jour continuent à se produire lorsque les machines se mettent en ligne. Ne soyez donc pas surpris de voir des mises à jour de stratégie supplémentaires 24 à 48 heures après la diffusion de la liste mise à jour.

Modifications

18 décembre - 2024

VEEAM

Ajout de :

- CSIDL_PROGRAM_FILES\Veeam\Backup and Replication\Threat Hunter\

Cisco WebEx

Ajout de :

- CSIDL_LOCAL_APPDATA\WebEx\WebEx64\Meetings\webexmta.exe
- CSIDL_PROGRAM_FILES\Cisco Spark\CiscoCollabHost.exe

Microsoft Windows par défaut

Petit ajustement du processus existant omadmclient.exe pour inclure les processus enfants.

4 juin - 2025

Microsoft Windows par défaut

ajout de :

- CSIDL_PROGRAM_FILES\Cisco\Cisco Secure Client\CM*\CMID*\csc_cmid.exe
- CSIDL_PROGRAM_FILES\Cisco\Cisco Secure Client\CM*\CMPM*\csc_pm.exe
- CSIDL_PROGRAM_FILES\Cisco\Cisco Secure Client\EVM\bin\csc_evm.exe
- CSIDL_PROGRAM_FILES\Microsoft Device Inventory Agent\InventoryService\InventoryService.exe
- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client\NVM\acnvmagent.exe
- CSIDL_COMMON_APPDATA\Cisco\Cisco Secure Client\EVM*
- CSIDL_PROGRAM_FILES\Microsoft Device Inventory Agent\InventoryService\

Apple macOS par défaut

ajout de :

- /opt/cisco/secureclient/evm/bin/csc_evm.app/Contents/MacOS/csc_evm
- /Library/Cisco/evm/Log Files
- /Library/Cisco/evm/Upload\ Queue/

17 septembre - 2025

Microsoft Windows par défaut

ajout de :

- CSIDL_PROGRAM_FILES\Cisco\Forensics\AIR**
- CSIDL_PROGRAM_FILES\Cisco\Forensics\AIR\

Apple macOS par défaut

ajout de :

- /opt/cisco/forensics/air/
- /opt/cisco/forensics/air/**



Remarque : Windows Secure Endpoint Versions 8.4.0+ résout le chemin pour toutes les exclusions CSIDL.

17 décembre - 2025

Microsoft Teams

ajout de :

- CSIDL_PROGRAM_FILES\WindowsApps\MSTeams_*\

4 février - 2026

Microsoft Windows par défaut

ajout de :

- CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client**

Serveur Microsoft Exchange

ajout de :

- CSIDL_PROGRAM_FILES\Microsoft\Exchange Server**

Apsense

ajout de :

- CSIDL_PROGRAM_FILES\AppSense\Environment Manager\Agent\EmSystem.exe

23 septembre - 2026

Windows par défaut

ajout de :

- CSIDL_PROGRAM_FILES\Orbital\

Splunk - Windows

ajout de :

- CSIDL_PROGRAM_FILES\SplunkUniversalForwarder\bin\splunk-winevtlog.exe
- CSIDL_PROGRAM_FILES\SplunkUniversalForwarder\bin\splunkd.exe

Hyper-V - Windows

ajout de :

- C:\ClusterStorage\
- CSIDL_WINDOWS\Cluster\
- CSIDL_WINDOWS\Cluster\clussvc.exe
- CSIDL_WINDOWS\Cluster\rhs.exe

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.