Cisco-Maintained Exclusion List Changes for Cisco Secure Endpoint Console

Contents

- **Introduction**
- **Prerequisites**
  - Requirements
  - Components Used
- **Expectations When You Update**
- **Changes**
  - December 18th - 2024
    - VEEAM
    - Cisco WebEx
  - June 4th - 2025
    - Microsoft Windows Default
    - Apple macOS Default
  - September 17th - 2025
    - Microsoft Windows Default
    - Apple macOS Default
  - December 17th - 2025
    - Microsoft Teams
  - February 4th - 2026
    - Microsoft Windows Default
    - Microsoft Exchange Server
    - Appsense
  - September 23 - 2026
    - Windows Default
    - Splunk - Windows
    - Hyper-V - Windows

Introduction

This document describes the changes added to the Cisco-Maintained Exclusions.

Cisco-Maintained Exclusions are created and maintained by Cisco to provide better compatibility between the Advanced Malware Protection (AMP) for Endpoints Connector and antivirus, security or other software, these exclusions can be added to new versions of an application.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Exclusions in AMP for Endpoints
- AMP console

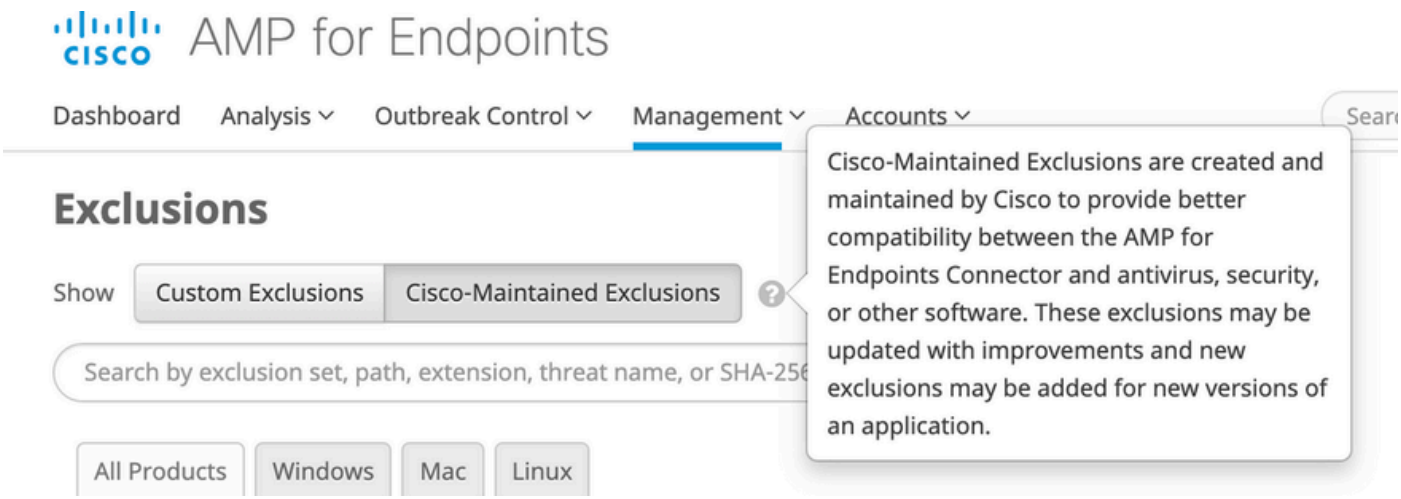
Components Used

The information in this document is based on these software and hardware versions:

- AMP for Endpoints console 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. If your network is live, ensure that you understand the potential impact of any command.

Expectations When You Update



When the Cisco-Maintained lists are changed, a policy update occurs on the backend to reflect that change. As each of the Endpoints use that list check in on their heartbeat, they pull the updated policy. These policy changes are not reflected in the audit log as it is technically a change to the exclusion list, not the policy itself, and Cisco-maintained exclusion lists do not exist within the normal audit log on individual consoles. For large scale environments, this looks like a flood of policy updates and the end result will be better performance on each of the Endpoints.

The update period depends on each endpoint. If all the machines are online, the updates would take place within 1-2 heartbeats. If this is a global environment, updates continue to occur as machines come online so don't be surprised to see additional policy updates 24-48 hours after the maintained list is pushed.

Changes

December 18th - 2024

VEEAM

Addition of:

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

Cisco WebEx

Addition of:

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

Microsoft Windows Default

Small adjustment of existing process **omadmclient.exe** to include child processes.

June 4th - 2025

Microsoft Windows Default

addition of:

- **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 Default

addition of:

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

September 17th - 2025

Microsoft Windows Default

addition of:

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

Apple macOS Default

addition of:

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

Note: Windows Secure Endpoint Versions 8.4.0+ resolves pathing for all CSIDL exclusions.

December 17th - 2025

Microsoft Teams

addition of:

- **CSIDL_PROGRAM_FILES\WindowsApps\MSTeams_***

February 4th - 2026

Microsoft Windows Default

addition of:

- **CSIDL_PROGRAM_FILESX86\Cisco\Cisco Secure Client****

Microsoft Exchange Server

addition of:

- **CSIDL_PROGRAM_FILES\Microsoft\Exchange Server****

Appsense

addition of:

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

September 23 - 2026

Windows Default

addition of:

- **CSIDL_PROGRAM_FILES\Orbital**

Splunk - Windows

addition of:

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

Hyper-V - Windows

addition of:

- **C:\ClusterStorage**
- **CSIDL_WINDOWS\Cluster**

- **CSIDL_WINDOWS\Cluster\clussvc.exe**
- **CSIDL_WINDOWS\Cluster\rhs.exe**