Cisco Secure Endpoint Mac Connector Faults

Contents

Introduction

The Connector may notify you of a Fault Raised event when it detects a condition that affects the proper functioning of the Connector. Similarly, a Fault Cleared event communicates that the condition is no longer present.

Connector Fault Table

The following table describes faults and corresponding diagnostic steps.

Fault ID	Portal Text	Endpoint Description	Troubleshooting/Resolution
1	Kernel module not authorized	System extension not authorized	The Connector's system extension has been blocked from execution. Open Security and Privacy System Preferences and approve the extension. Alternatively, system extensions can be approved remotely using a mobile device management (MDM) profile .
2	Version mismatch	System extension version mismatch	The installed Connector software is corrupt. Reinstall the Connector. Note: When running Mac Connector versions 1.14.0 and later, some occurances of this fault may be cleared by restarting the computer.
3	Disk access not granted	Full Disk Access not granted	The Connector cannot access user files for scan. Open Security and Privacy System Preferences and grant Full Disk Access to the AMP service. For Mac Connector versions prior to 1.14.0, this process is named */opt/cisco/amp/ampdaemon*. For Mac Connector versions 1.14.0 and later, the following two applications require full disk access depending on the macOS version: • *AMP for Endpoints Service* (needed for all macOS versions) • *AMP Security Extension* (needed on macOS 10.15.5 and newer) For Mac Connector versions 1.14.1 and later, the following two applications require full disk access depending on the macOS version:

			• *AMP for Endpoints Service* (needed for all macOS versions) • *AMP Security Extension* (needed on macOS 11 and newer) Additional details are available in this tech note.
4	Kernel module not loaded	System extension could not be loaded; reinstall the Connector	For Mac Connector versions prior to 1.14.0, or when running on macOS 10.14 or 10.15, this fault indicates that Connector’s system extension is the correct version and has been approved for execution but has still failed to load. Review */Library/Logs/Cisco/ampdaemon.log* for details. Uninstalling and reinstalling the Connector may also clear this fault.
5	Scan service user unavailable	Scan service user unavailable	The Connector failed to create a user to run the file scan process. The Connector works around this by using the root user to perform file scan. This deviates from the intended design and is not expected. If the `cisco-amp-scan-svc` user or group has been deleted, or the configuration of the user and group has been changed, reinstalling the Connector will re-create the user and group with the necessary configuration. Additional details are available in */Library/Logs/Cisco/ampdaemon.log*.
6	Scan service restarting frequently	Scan service restarting frequently	The Connector's file scan process encountered repeated failures and the Connector has restarted in an attempt to clear the failure. It is possible one or more files on the system is causing the scan algorithm to crash when scanned. The Connector continues with scans on a best-effort basis. If this fault is not automatically cleared within 10 minutes after the Connector is started then this is an indication that further user intervention is required and the Connector's ability to perform scans is will be degraded. Review */Library/Logs/Cisco/ampdaemon.log* and */Library/Logs/Cisco/ampscansvc.log* for details.
7	Scan service failed to start	Scan service failed to start	The Connector’s file scan process failed to start and the Connector has restarted in an attempt to clear the failure. File scan functionality is disabled while this fault is raised. This failure can be triggered if an error is encountered when loading a newly installed virus definition files (.cvd files). The Connector performs a number of integrity and stability checks before activating new .cvd files to prevent this failure. Upon restart the Connector will remove any invalid .cvd files so that the Connector can resume. If this fault is not cleared when the Connector is restarted then this is an indication that further user intervention is required. If this failure repeats with each .cvd update then this is an indication that an invalid .cvd file is not being properly detected by the Connector's .cvd file integrity checks. Review */Library/Logs/Cisco/ampdaemon.log* and

			/Library/Logs/Cisco/ampscansvc.log for details.
10	Reboot required to load kernel module or system extension	Reboot required to load system extensions	Reboot the system. For Mac Connector versions 1.11.1 and 1.14.0, this fault can be raised if the system extensions are unable to load. In this case, this fault can be cleared by reinstalling the Connector. Note that Mac Connector 1.14.1 and later may raise this fault if there are too many Network Content Filter system extensions installed on the system. Refer to the fault 13 guidance below for additional details if rebooting the computer does not clear this fault.
12	Network filter not allowed	Network Filter not allowed	The Network Filter is required by the 'Enable Device Flow Correlation' feature in the policy. To clear this fault, allow 'AMP for Endpoints Service' to Filter Network Content on the endpoint. The macOS dialogue to allow the Network Filter can be accessed by clicking on the active fault listed in the Agent menulet and following the guidance provided. Additional details, including MDM profile settings for remote authorization of network filters, are available in this tech note.
13	Too many network content filter system extensions	Too many network content filter system extensions	For Mac Connector 1.14.0, this fault is frequently raised raised due to a macOS bug when starting the network content filter system extension. Rebooting the computer will clear this fault. The 'Enable Device Flow Correlation' feature in the policy requires use of a firewall-grade macOS network content filter. MacOS limits the number of network content filters that can run. If this fault is raised and is not cleared by rebooting the computer, uninstall the firewall-grade network content filters that are no longer needed and restart the Connector.
14	Too many endpoint security system extensions	Too many Endpoint Security system extensions	MacOS limits the number of Endpoint Security system extensions that can be running. The Mac Connector requires one of these Endpoint Security system extensions for 'Monitor File Copies and Moves' and 'Monitor Process Execution' features in the policy . To clear this fault, uninstall Endpoint Security system extensions that are no longer needed and restart the Connector.
15	System Extension requires Full Disk Access	System Extension requires Full Disk Access	The Mac Connector's macOS System Extensions cannot access user files for scan. Open Security & Privacy System Preferences and grant Full Disk Access to the *AMP Security Extension*. Additional details, including MDM profile settings for remote

			authorization of full disk access with system extensions, are available in this tech note. Note that a bug on macOS 11.0.0 can cause the full disk access setting to be spontaneously cleared on a reboot after it has been granted. This bug has been fixed in macOS 11.0.1.
17	Orbital Full Disk Access Not Granted	Orbital Full Disk Access Not Granted	Orbital requires full disk access to access protected files and directories for queries. Open Security & Privacy System Preferences and grant Full Disk Access to *Cisco Orbital*.
18	Connector event monitoring is overloaded	Connector event monitoring is overloaded	This fault is raised when the connector is under heavy load due to an overwhelming number of system events. System protection is limited and the connector monitors a smaller set of system critical events until overall system activity is reduced. This fault could be an indication of malicious system activity or of very active applications on the system. If an active application is benign and trusted by the user, then it can be added to a process exclusion set to reduce the monitoring load on the connector. This action can be enough to clear the fault. If no benign processes cause heavy load, then some investigation is required to determine if the increased activity is due to a malicious process. If the connector is under short periods of heavy load then it is possible that this fault can clear itself. If this fault is raised frequently, there are no benign processes that cause heavy load, and no malicious processes were discovered, then the system needs to be re-provisioned to handle heavier loads.