

Cisco Secure Endpoint Connector for Mac Diagnostic Data Collection

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Generate a Diagnostic File with the Support Tool](#)

[Launch the Support Tool Using macOS Finder](#)

[Launch the Support Tool Using macOS Terminal](#)

[Troubleshooting](#)

[Enable Debug Mode](#)

[Enable Single Heartbeat Debug Mode](#)

[Disable Debug Mode](#)

Introduction

This document describes the process that is used in order to generate a diagnostic file via the Support Tool application that is available on the Cisco Secure Endpoint Mac connector and how to troubleshoot performance issues.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Endpoint Mac connector
- macOS

Components Used

The information in this document is based on the Secure Endpoint Mac connector.

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.

Background Information

The Secure Endpoint Mac connector packages an application called Support Tool, which is used

in order to generate diagnostic information about the connector that is installed on your Mac. The diagnostic data includes information about your Mac such as:

- Resource utilization (disk, CPU, and memory)
- connector-specific logs
- connector configuration information

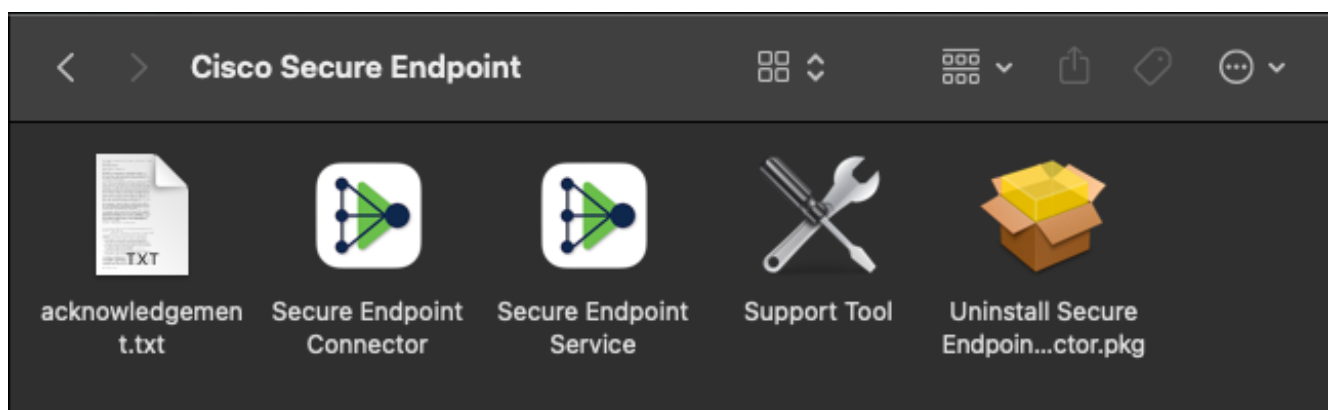
Generate a Diagnostic File with the Support Tool

This section describes how to launch the Support Tool application from the GUI or the CLI in order to generate a diagnostic file.

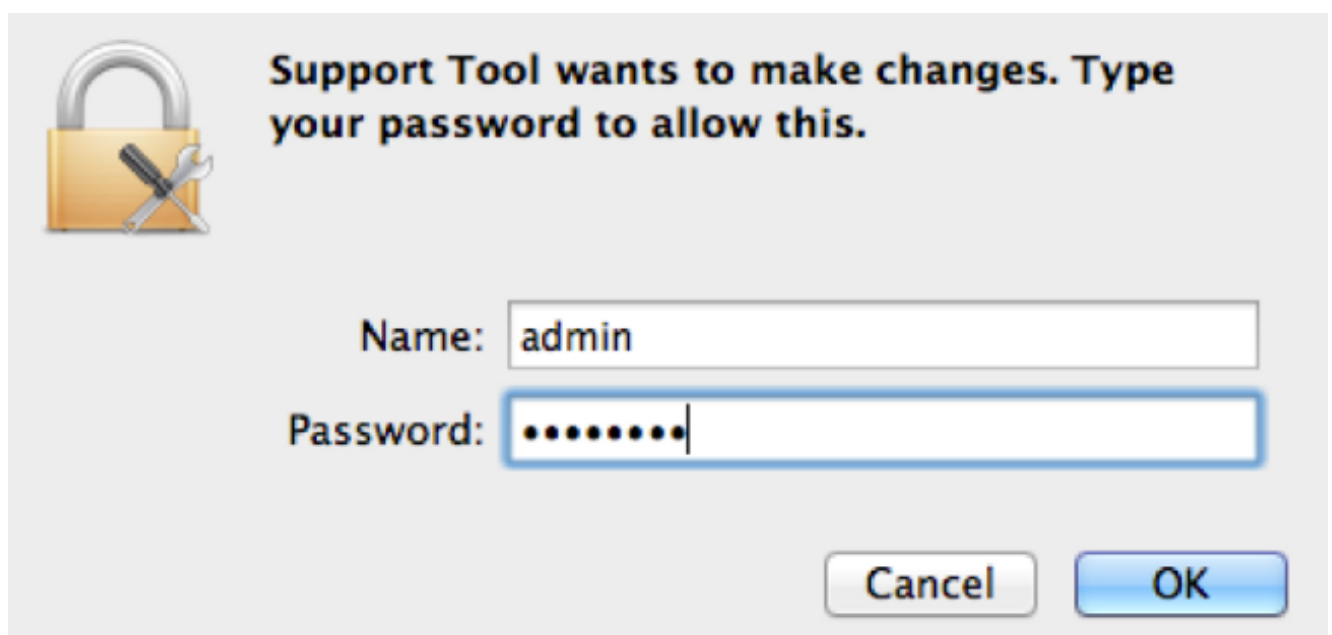
Launch the Support Tool Using macOS Finder

Complete these steps in order to launch the Secure Endpoint Mac connector Support Tool using the macOS Finder:

1. Navigate to the Cisco Secure Endpoint directory in your Applications folder and locate the Support Tool launcher:



2. Double-click the Support Tool launcher, and you are prompted for administrative credentials:

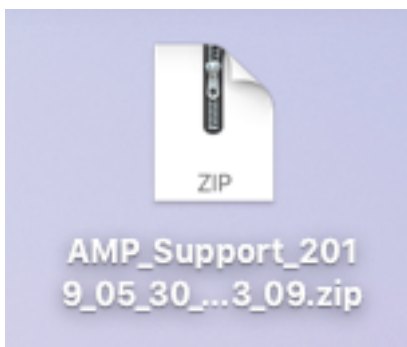


3. After you enter your credentials, the Support Tool icon should appear in your dock:

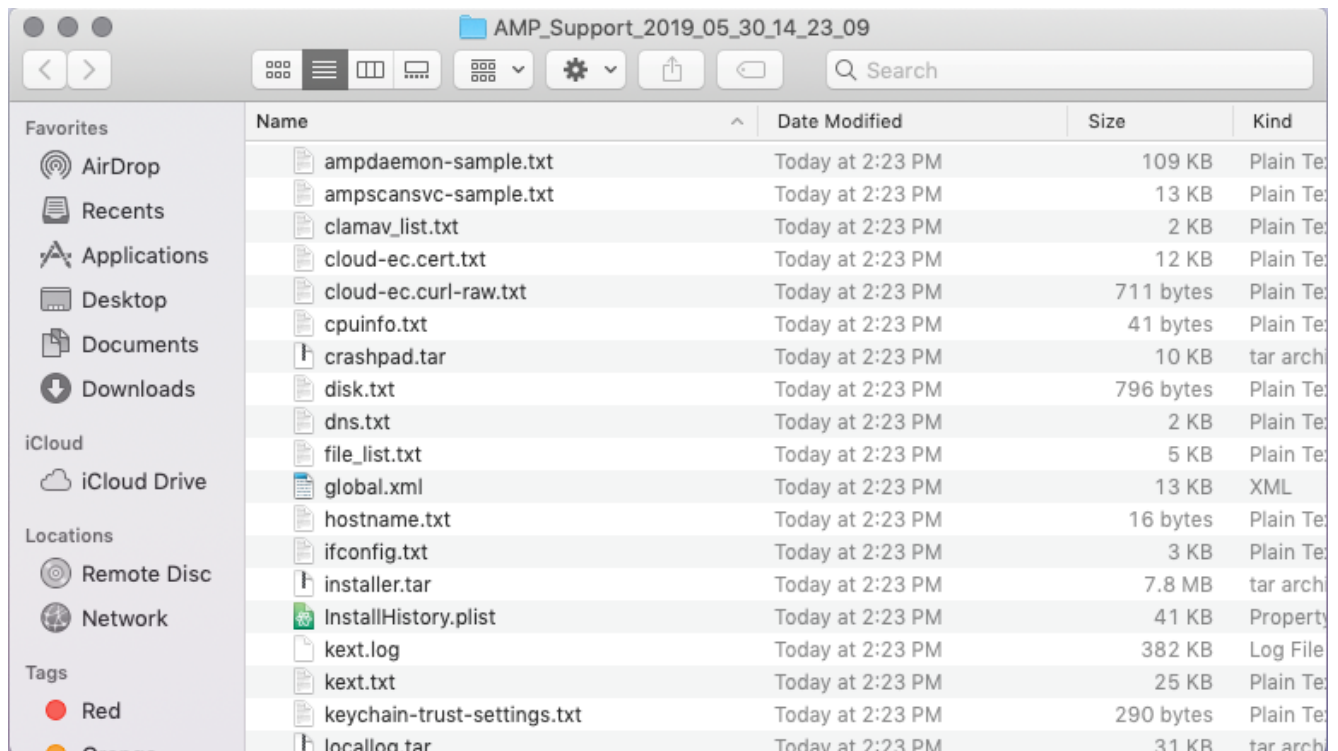


Note: The Support Tool application runs in the background and takes some time to complete (approximately 20-30 minutes).

4. When the Support Tool application completes, a file is generated and placed onto your desktop:



Here is an example of the uncompressed output:



Name	Date Modified	Size	Kind
ampdaemon-sample.txt	Today at 2:23 PM	109 KB	Plain Te
ampscansvc-sample.txt	Today at 2:23 PM	13 KB	Plain Te
clamav_list.txt	Today at 2:23 PM	2 KB	Plain Te
cloud-ec.cert.txt	Today at 2:23 PM	12 KB	Plain Te
cloud-ec.curl-raw.txt	Today at 2:23 PM	711 bytes	Plain Te
cpuinfo.txt	Today at 2:23 PM	41 bytes	Plain Te
crashpad.tar	Today at 2:23 PM	10 KB	tar arch
disk.txt	Today at 2:23 PM	796 bytes	Plain Te
dns.txt	Today at 2:23 PM	2 KB	Plain Te
file_list.txt	Today at 2:23 PM	5 KB	Plain Te
global.xml	Today at 2:23 PM	13 KB	XML
hostname.txt	Today at 2:23 PM	16 bytes	Plain Te
ifconfig.txt	Today at 2:23 PM	3 KB	Plain Te
installer.tar	Today at 2:23 PM	7.8 MB	tar arch
InstallHistory.plist	Today at 2:23 PM	41 KB	Property
kext.log	Today at 2:23 PM	382 KB	Log File
kext.txt	Today at 2:23 PM	25 KB	Plain Te
keychain-trust-settings.txt	Today at 2:23 PM	290 bytes	Plain Te
locallog.tar	Today at 2:23 PM	31 KB	tar arch

5. In order to analyze the data, provide this file to the Cisco Technical Support Team.

Launch the Support Tool Using macOS Terminal

The Support Tool launcher is located in this directory:

```
/Library/Application Support/Cisco/AMP for Endpoints Connector/
```

In order to launch the Support Tool application, enter the following command:

Note: You must run this command as root, so ensure that you switch to root or preface the command with **sudo**.

```
root@mac# cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector root@mac#  
./SupportTool
```

Note: This command runs verbosely. Once it is complete, a diagnostic file is generated and placed onto your desktop.

Troubleshooting

This section describes how to enable and disable debug mode on the Secure Endpoint Mac connector in order to troubleshoot performance issues.

Enable Debug Mode

Warning: Debug mode should be enabled only if a Cisco Technical Support Engineer makes a request for this data. If you keep debug mode enabled for an extended period of time, it can fill up the disk space very quickly and might prevent the connector Log and Tray Log data from being gathered in the Support Diagnostic file due to excessive file size.

Debug mode is useful with attempts to troubleshoot performance issues on a Secure Endpoint connector. Complete these steps in order to enable debug mode and collect diagnostic data;

1. Log in to the Secure Endpoint Console.
2. Navigate to **Management > Policies**.
3. Locate a policy that is applied to a computer, click on the policy which will expand the policy window, and click **Duplicate**. The Secure Endpoint Console updates with the duplicated policy:

Policies

[View All Changes](#)

TechZone

All Products Windows Android Mac Linux Network iOS

+ New Policy...

TechZone MAC Policy

Modes and Engines	Exclusions	Proxy	Groups
Files Network ClamAV	Quarantine Audit On Apple macOS Default	Not Configured	Not Configured

Outbreak Control

Custom Detections - Simple	Custom Detections - Advanced	Application Control	Network
Not Configured	Not Configured	Not Configured	Not Configured

[View Changes](#) Modified 2019-05-30 14:49:32 UTC Serial Number 10004 [Download XML](#) [Duplicate](#) [Edit](#) [Delete](#)

4. Select and expand the duplicate policy window, click **Edit** and change the name of the policy. For example, you could use *Debug TechZone MAC Policy*.

5. Click **Advanced Settings**, select **Administrative Features** from the sidebar, and select **Debug** for both the connector Log Level and Tray Log Level drop down menus:

Mac

Name

Description

Modes and Engines

Exclusions
1 exclusion set

Proxy

Outbreak Control

Product Updates

Advanced Settings

- Administrative Features**
- Client User Interface
- File and Process Scan
- Cache
- ClamAV
- Network
- Scheduled Scans

Send User Name in Events ⓘ

Send Filename and Path Info ⓘ

Heartbeat Interval ⓘ

Connector Log Level ⓘ

Tray Log Level ⓘ

Automated Crash Dump Uploads ⓘ

Command Line Capture ⓘ

Command Line Logging ⓘ

- Click the **Save** button in order to save the changes.
- Navigate to **Management > Groups** and click **Create Group** near the top-right side of your screen.
- Enter a name for the group. For example, you could use *Debug TechZone Mac Group*.

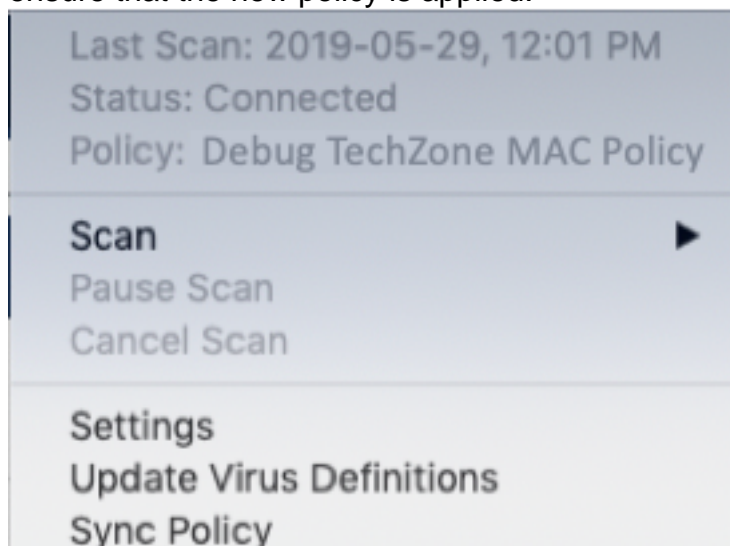
< New Group ?

Name	Debug Mac Group
Description	This group will be used to debug AMP for Endpoints Connector running on Mac
Parent Group	
Windows Policy	win_desktop_policy
Android Policy	Default FireAMP Android (Default)
Mac Policy	Debug TechZone MAC Policy
Linux Policy	Audit Policy for FireAMP Linux (Default)
Network Policy	Default Network (Default)
iOS Policy	Audit (Default)

Computers

Assign computers from the Computers page after you have saved the new group

- Change the Mac Policy from *Default Mac Policy* to the duplicated, new policy that you just created, which is **Debug TechZone Mac Policy** in this example. Click **Save**.
- Navigate to **Management > Computers** and identify your computer in the list. Select it and click **Move to Group...**
- Select your newly created group from the **Select Group** drop down menu. Click **Move** to move the selected computer into your new group. Your Mac should now have a functional debug policy. You can select the Secure Endpoint icon that appears on your menu bar and ensure that the new policy is applied:

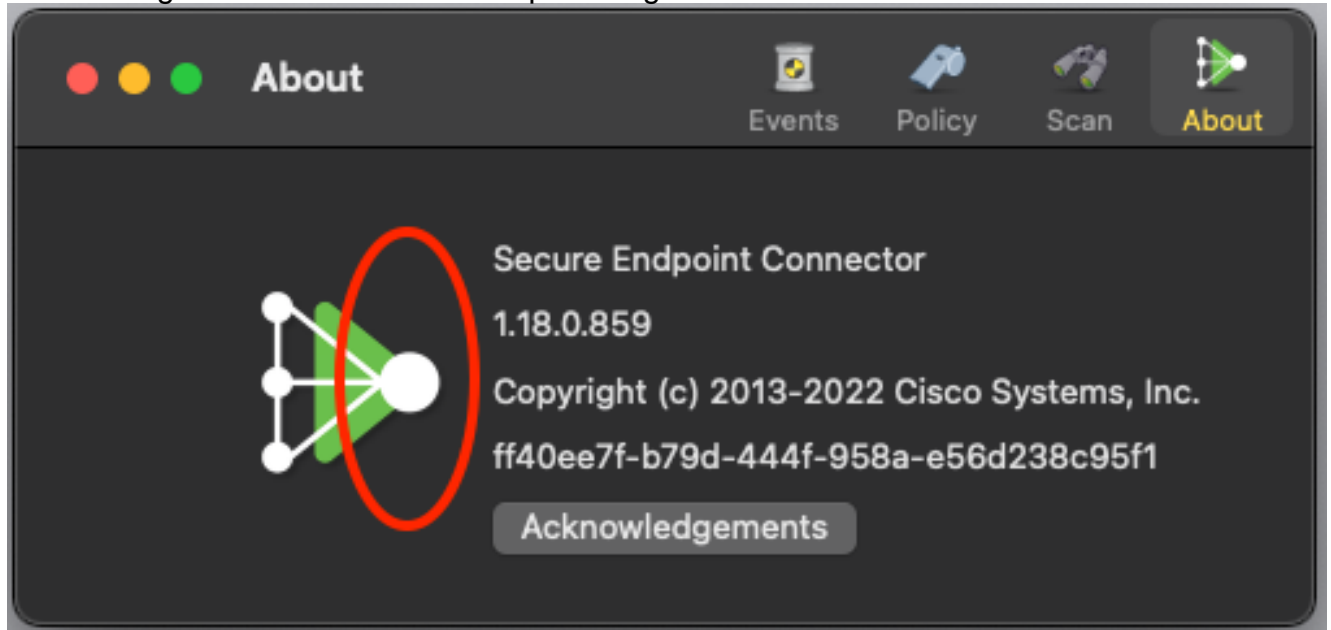


Enable Single Heartbeat Debug Mode

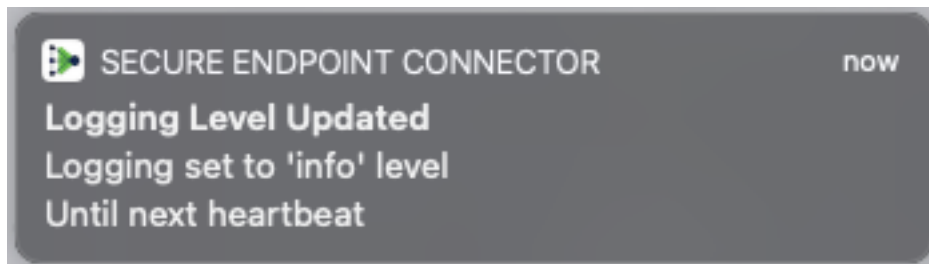
This procedure is only available for the 1.0.4 connector and above. This allows for a single connector to be put into debug mode until the next heartbeat. Depending on the situation, this may provide enough information for our developers but dependent on the length of heartbeat, risks not catching all the processes necessary to make a full diagnostic analysis. Here are the steps to

enable Debug for a single Heartbeat:

1. Access the connector menu bar and go to **Settings**.
2. Click on **About**.
3. Click the right-half of the Secure Endpoint Logo.



4. if it was done correctly, The following notice will pop up on the right side of the screen:



Debug will automatically disable after the next heartbeat.

Disable Debug Mode

After the diagnostic data in debug mode is obtained, you must revert the Secure Endpoint connector back to the normal mode. Complete these steps in order to disable debug mode:

1. Log in to the Secure Endpoint Console.
2. Navigate to **Management > Groups**.
3. Locate the new group, *Debug TechZone Mac Group*, that you created in debug mode.
4. Click **Edit**.
5. In the **Computers** window located towards the top-right of your screen, locate your computer in the list. Select it, which will take you to the **Computers** page. Once again, select your computer from the list, and click **Move to Group...**
6. Select your previous group from the **Select Group** drop down menu. Click **Move** to move the selected computer into the previous group.
7. Click on the Secure Endpoint icon in your menu bar. Select **Sync Policy** from the menu.

8. Verify that the policy is now returned to the previous default value. Check this on the menu bar. The policy should now have reverted back to the original policy that was used before you changed it to the *Debug TechZone Mac Group*:

