

适用于Mac诊断数据收集的思科安全终端连接器

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[使用支持工具生成诊断文件](#)

[使用macOS Finder启动支持工具](#)

[使用macOS终端启动支持工具](#)

[故障排除](#)

[启用调试模式](#)

[启用单心跳调试模式](#)

[禁用调试模式](#)

简介

本文档介绍通过Cisco安全终端Mac连接器上提供的支持工具应用程序生成诊断文件的过程，以及如何解决性能问题。

先决条件

要求

Cisco 建议您了解以下主题：

- 安全终端Mac连接器
- macOS

使用的组件

本文档中的信息基于安全终端Mac连接器。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

安全终端Mac连接器封装了一个称为“支持工具”的应用程序，用于生成有关安装在Mac上的连接器的诊断信息。诊断数据包括有关Mac的信息，例如：

- 资源利用率（磁盘、CPU和内存）
- 特定于连接器的日志

- 连接器配置信息

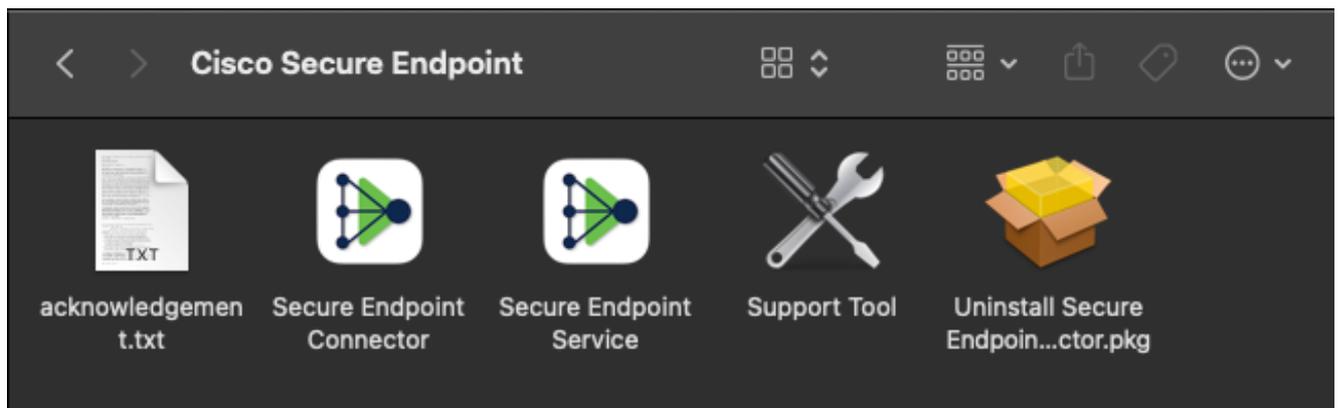
使用支持工具生成诊断文件

本节介绍如何从GUI或CLI启动支持工具应用程序以生成诊断文件。

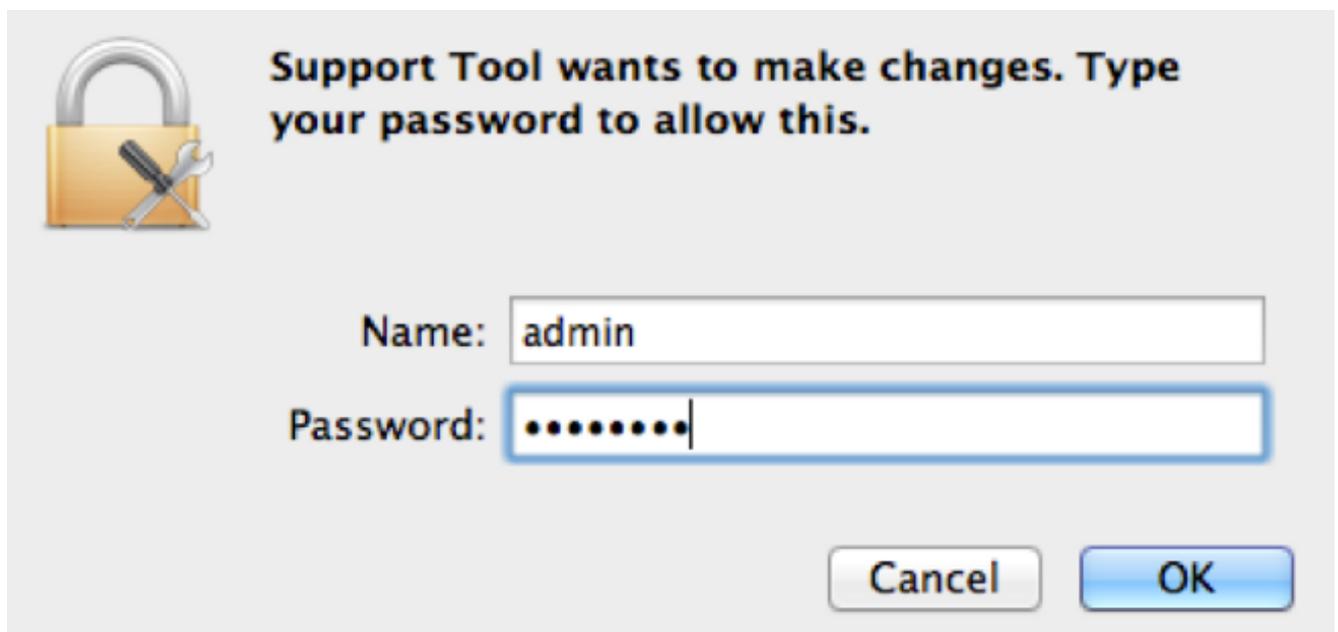
使用macOS Finder启动支持工具

要使用macOS Finder启动安全终端Mac连接器支持工具，请完成以下步骤：

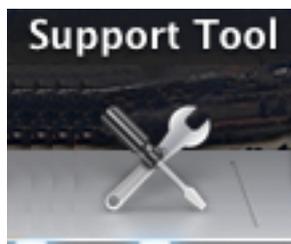
1. 导航到Applications文件夹中的Cisco Secure Endpoint目录，并找到Support Tool启动程序：



2. 双击Support Tool启动程序，系统将提示您输入管理凭据：

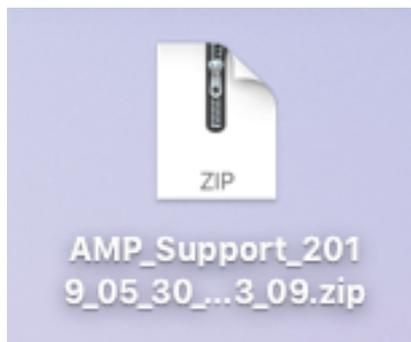


3. 输入凭证后，支持工具图标应显示在坞站中：

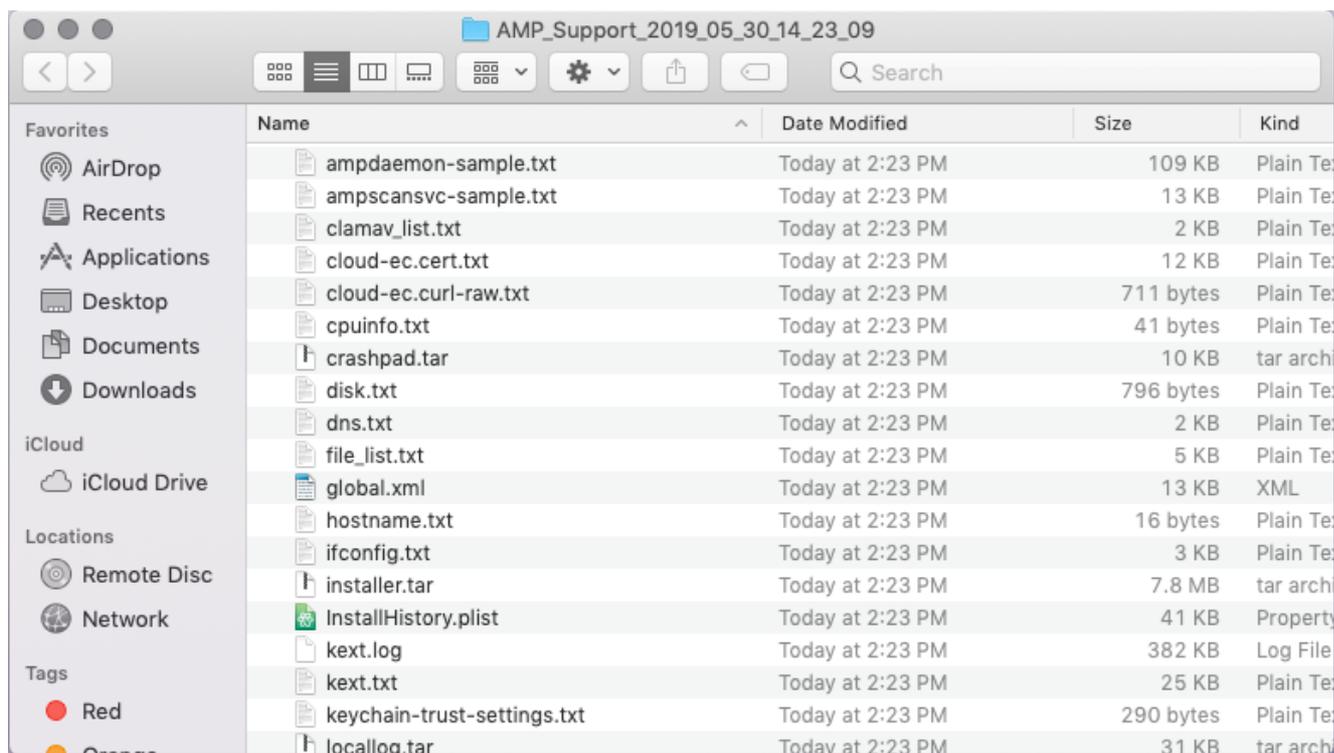


注意：支持工具应用程序在后台运行，需要一些时间才能完成（大约20-30分钟）。

4. 当“支持工具”应用程序完成时，会生成一个文件并将其放置在桌面上：



以下是未压缩输出的示例：



5. 为了分析数据，请将此文件提供给思科技术支持团队。

使用macOS终端启动支持工具

支持工具启动程序位于以下目录中：

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

要启动支持工具应用程序，请输入以下命令：

注意：您必须以root用户身份运行此命令，确保切换到root或使用sudo作为命令前言操作。

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

注意：此命令运行反向。完成后，会生成诊断文件并将其放到桌面上。

故障排除

本节介绍如何在安全终端Mac连接器上启用和禁用调试模式，以便解决性能问题。

启用调试模式

警告：只有当Cisco技术支持工程师请求此数据时，才应启用调试模式。如果长时间保持启用调试模式，则它可能会很快地填充磁盘空间，并且可能会由于文件大小过大而阻止将连接器日志和托盘日志数据收集到支持诊断文件中。

调试模式对于尝试解决安全终端连接器的性能问题非常有用。完成以下步骤以启用调试模式并收集诊断数据；

1. 登录到安全终端控制台。
2. 导航到**管理>策略**。
3. 找到应用于计算机的策略，点击将展开策略窗口的策略，然后单击 **重复**.安全终端控制台使用重复的策略进行更新：

The screenshot shows the 'Policies' page in the Cisco AMP console for the 'TechZone' environment. The page title is 'Policies' and there is a 'View All Changes' link. Below the title is a search bar containing 'TechZone'. There are tabs for 'All Products', 'Windows', 'Android', 'Mac', 'Linux', 'Network', and 'IOS'. A '+ New Policy...' button is visible. The main content area shows a table of policies for 'TechZone MAC Policy'. The table has columns for 'Modes and Engines', 'Exclusions', 'Proxy', and 'Groups'. The 'Exclusions' column shows 'Apple macOS Default'. Below the table is an 'Outbreak Control' section with columns for 'Custom Detections - Simple', 'Custom Detections - Advanced', 'Application Control', and 'Network'. At the bottom of the policy card, there are buttons for 'View Changes', 'Download XML', 'Duplicate', 'Edit', and 'Delete'. The 'Duplicate' button is circled in red.

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

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

4. 选择并展开复制策略窗口，单击 **编辑** 并更改策略的名称。例如，您可以使用 *Debug TechZone MAC Policy*。

5. 点击 **高级设置**,选择 **管理功能** 从侧边栏中选择 **调试** 对于连接器日志级别和托盘日志级别下拉菜单 :

Mac

Name: Debug TechZone MAC Policy

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: 15 minutes

Connector Log Level: Debug

Tray Log Level: Debug

Automated Crash Dump Uploads

Command Line Capture

Command Line Logging

6. 单击 **保存** 按钮以保存更改。
7. 导航至 **Management > Groups** 并单击 **创建组** 靠近屏幕右上角。
8. 输入组的名称。例如, 您可以使用 *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)

Cancel Save

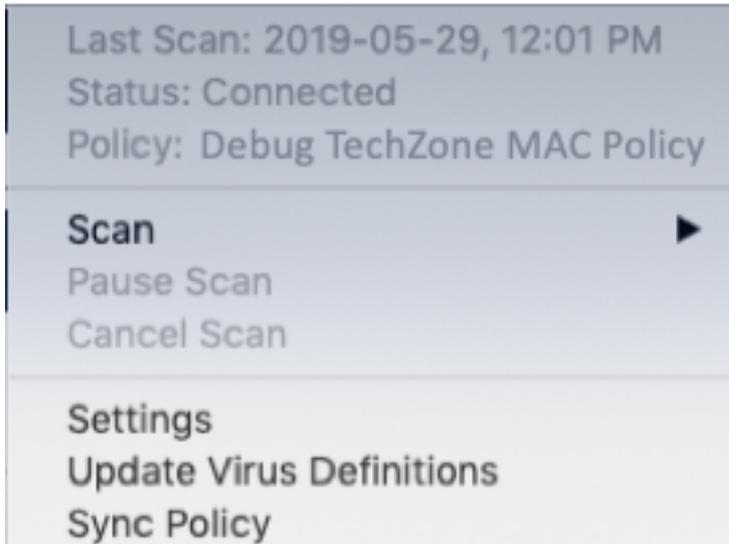
Computers

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

9. 更改Mac策略 **默认Mac策略** 您刚刚创建的新策略复制到 **Debug TechZone Mac Policy** 在本例

中。点击 **保存**。

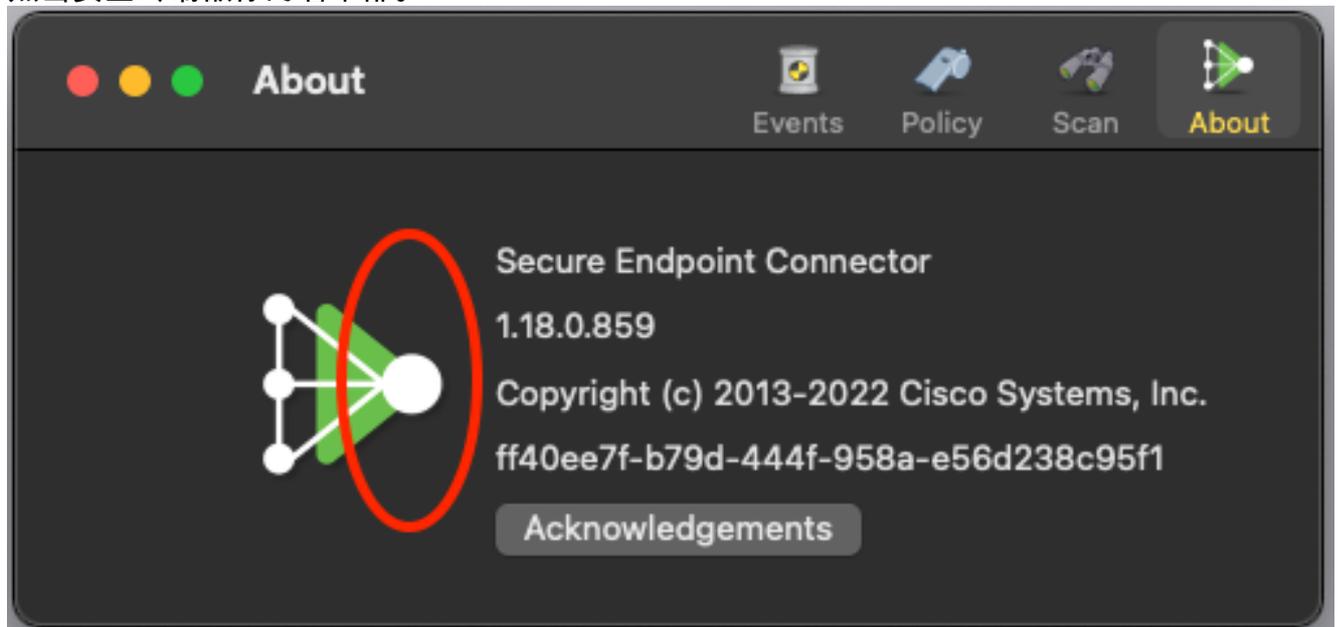
10. 导航至 **Management > Computers** 并在列表中识别您的计算机。选择它并单击 **移动到组....**
11. 从 **选择组** 下拉菜单。点击 **移动** 将所选计算机移动到新组中。您的Mac现在应该具有功能调试策略。您可以选择显示在菜单栏上的安全终端图标，并确保应用新策略：



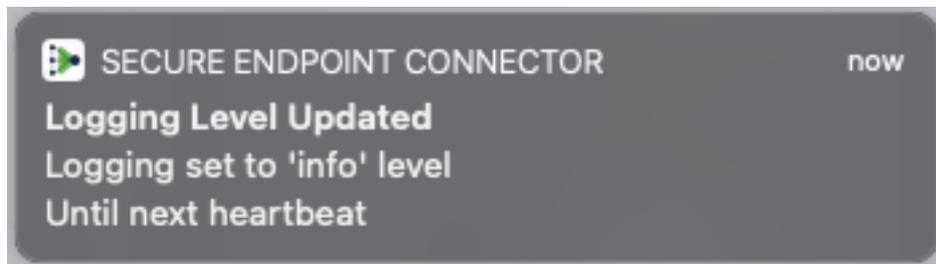
启用单心跳调试模式

此步骤仅适用于1.0.4及以上连接器。这允许单个连接器进入调试模式，直到下一个心跳。根据具体情况，这可能为我们的开发人员提供足够的信息，但取决于心跳长度，可能会不捕获进行完整诊断分析所需的所有流程。以下是启用单个心跳调试的步骤：

1. 访问连接器菜单栏并转至 **设置**。
2. 点击 **关于**。
3. 点击安全终端徽标的右半部。



4. 如果操作正确，屏幕右侧将弹出以下通知：

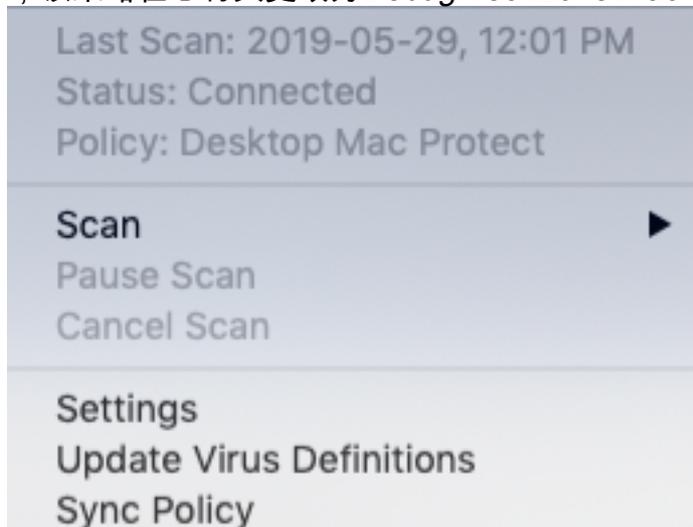


调试将在下次心跳后自动禁用。

禁用调试模式

获得调试模式下的诊断数据后，必须将安全终端连接器恢复为正常模式。要禁用调试模式，请完成以下步骤：

1. 登录安全终端控制台。
2. 导航到**管理>组**。
3. 找到在调试模式下创建的新组 *Debug TechZone Mac Group*。
4. 单击 **Edit**。
5. 在屏幕右上角的“计算机”窗口中，在列表中找到您的计算机。选择它，它将带您进入 Computerspace。再次从列表中选择您的计算机，然后单击**移动到组**.....
6. 从选择组下拉**菜单**中选择上一组。单击移动将所选计算机移动到上一组。
7. 单击菜单栏中的 Secure Endpoint 图标。从**菜单**中选择 **Sync Policy**。
8. 验证策略现在是否返回到上一个默认值。在菜单栏上选中此项。策略现在应已恢复为原始策略，该策略在您将其更改为 *Debug TechZone Mac Group* 之前使用:



关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。