安全终端Mac连接器诊断数据故障排除

目录

简介

环境

- 要求
- 使用的组件

问题

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

本文档介绍如何使用Cisco安全终端Mac连接器上的支持工具应用程序生成诊断文件。

环境

要求

Cisco 建议您了解以下主题：

- macOS
- 安全终端Mac连接器

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

安全终端Mac连接器包括称为支持工具的应用。这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

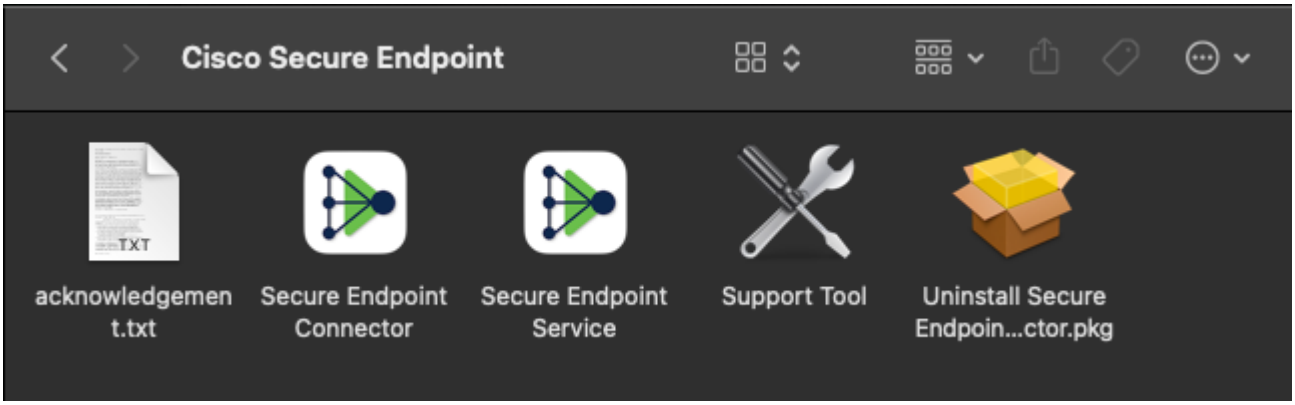
使用支持工具生成诊断文件

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。

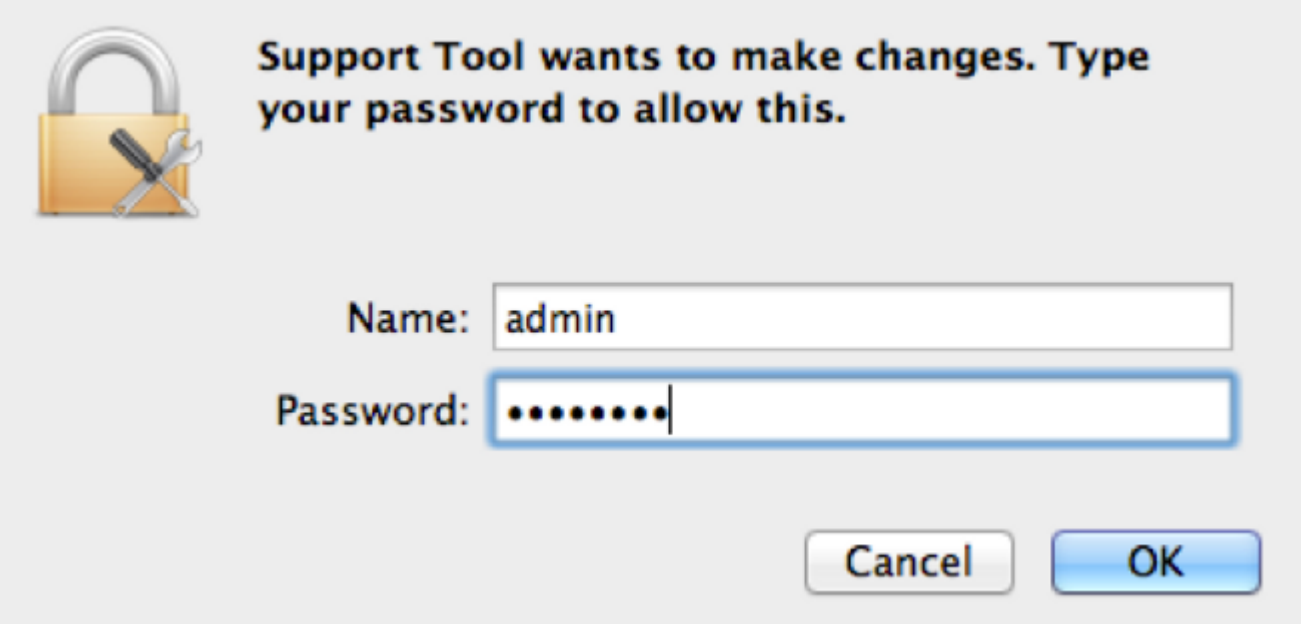
使用macOS Finder启动支持工具

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

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“支持工具”启动程序。系统提示输入管理凭据：

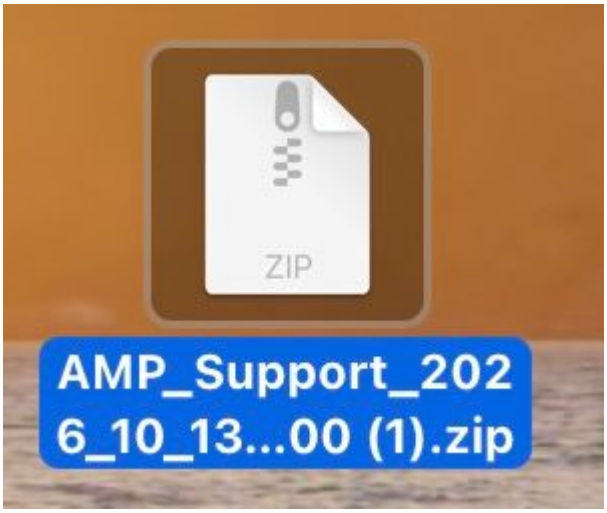


3.输入凭证后，坞站中会出现“Support Tool（支持工具）”图标：



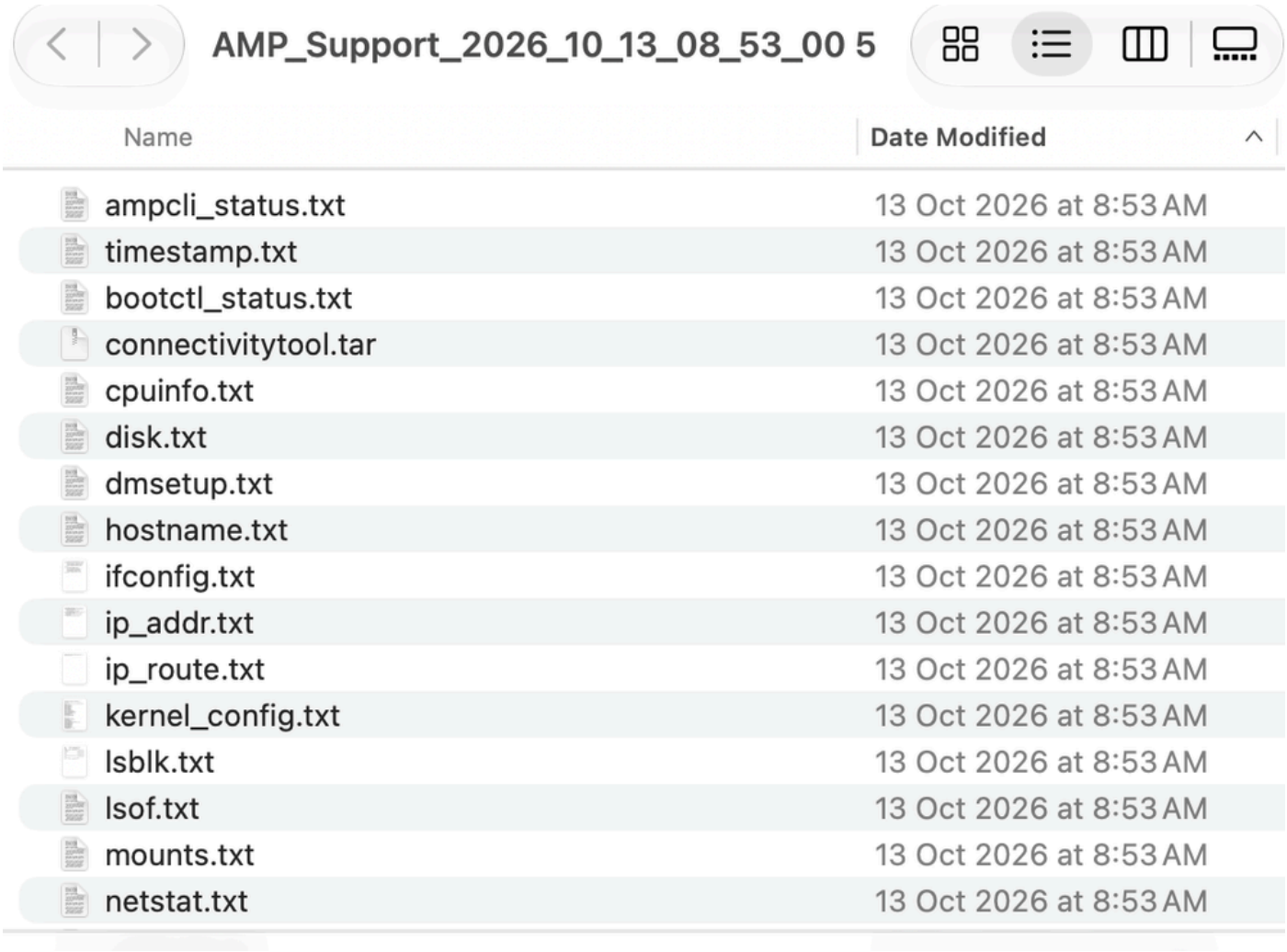
注意：“支持工具”应用程序在后台运行，需要一定时间才能完成（大约20-30分钟）。

4.当“支持工具”应用程序完成时，它会生成一个文件并将其放在桌面上：



粘贴于11.38.59.jpeg的18-10-2026

5.下图显示未压缩输出的示例：



屏幕截图2026-10-18(11.39.51 AM.png)

6.要分析数据，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，请运行以下命令：

注意：以root用户身份运行此命令。切换到root或使用sudo前缀命令。

```
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置在桌面上。

故障排除

本节介绍如何启用和禁用安全终端Mac连接器上的调试模式以排除性能问题。

启用调试模式

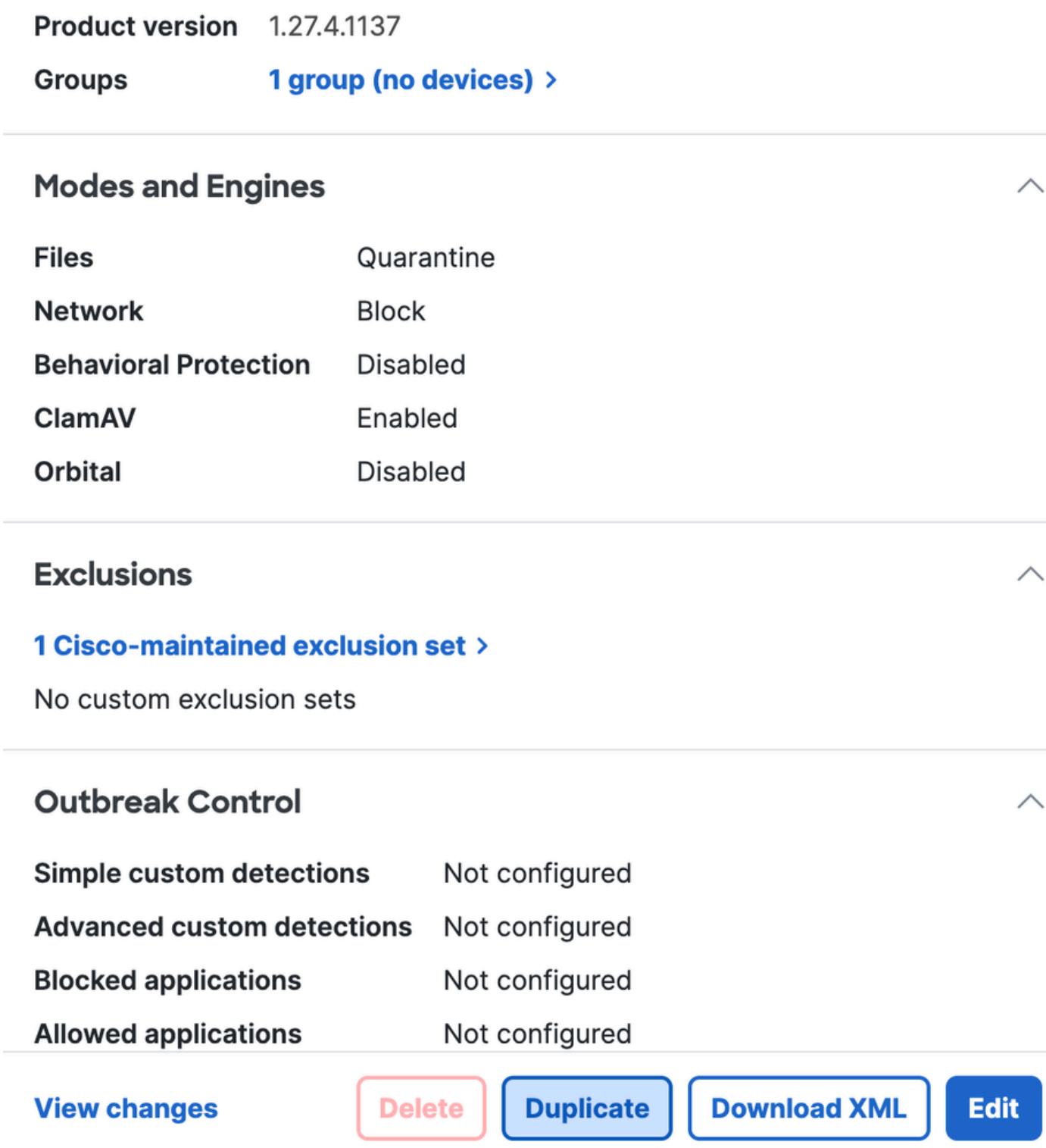
警告： 只有在思科技术支持工程师请求此数据时，才能启用调试模式。如果长时间保持启用调试模式，则它可能会快速填充磁盘空间，并且可能会由于文件过大而阻止将连接器日志和托盘日志数据收集到支持诊断文件中。

对安全终端连接器的性能问题进行故障排除时，调试模式非常有用。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.定位至管理>策略。

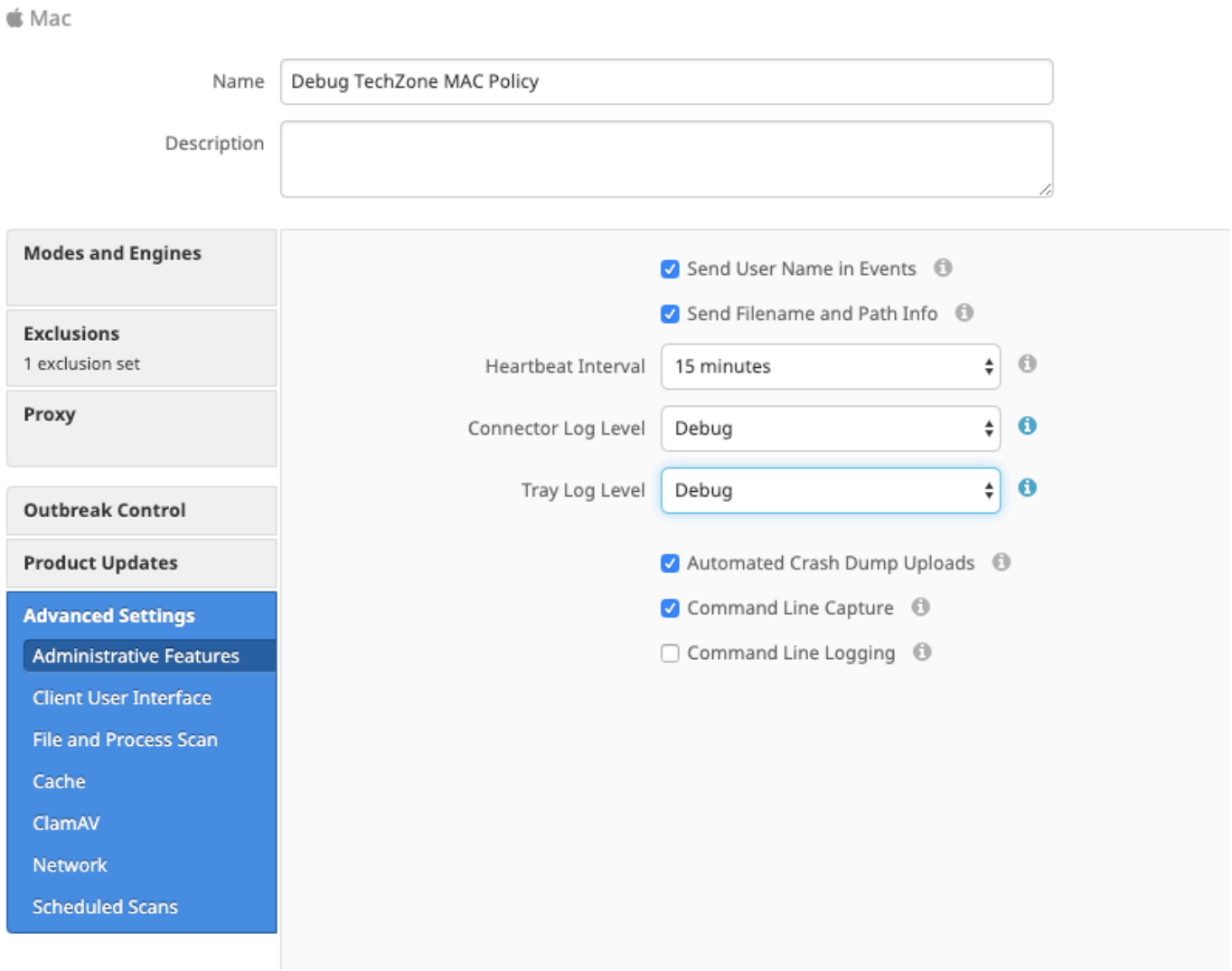
1.找到应用于计算机的策略，单击展开策略窗口的策略，然后单击复制。安全终端控制台使用重复的策略进行更新：



屏幕截图2026-10-18(11.50.48 AM.png)

2.选择并展开复制策略窗口，单击Edit，然后更改策略的名称。例如，您可以使用Debug TechZone MAC Policy。

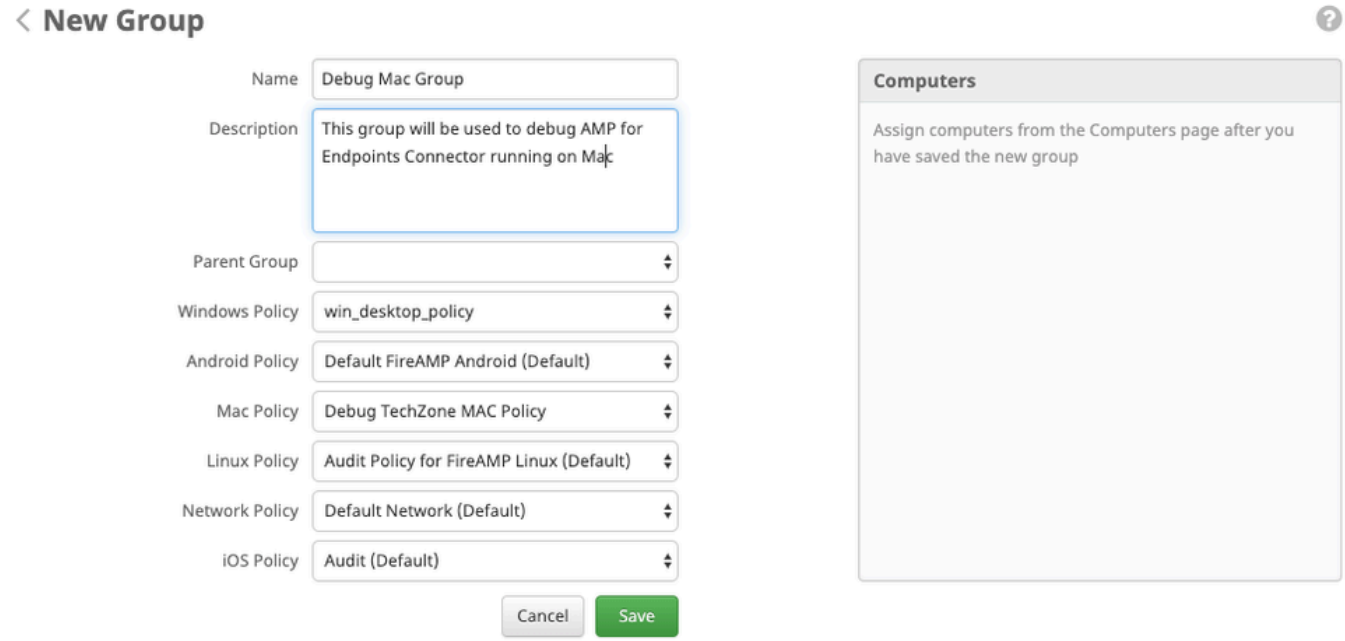
3.单击Advanced Settings，从边栏中选择Administrative Features，然后为连接器“日志级别”和“托盘日志级别”下拉菜单选择Debug:



4.单击保存。

5.定位至管理>组，然后单击屏幕右上角附近的创建组。

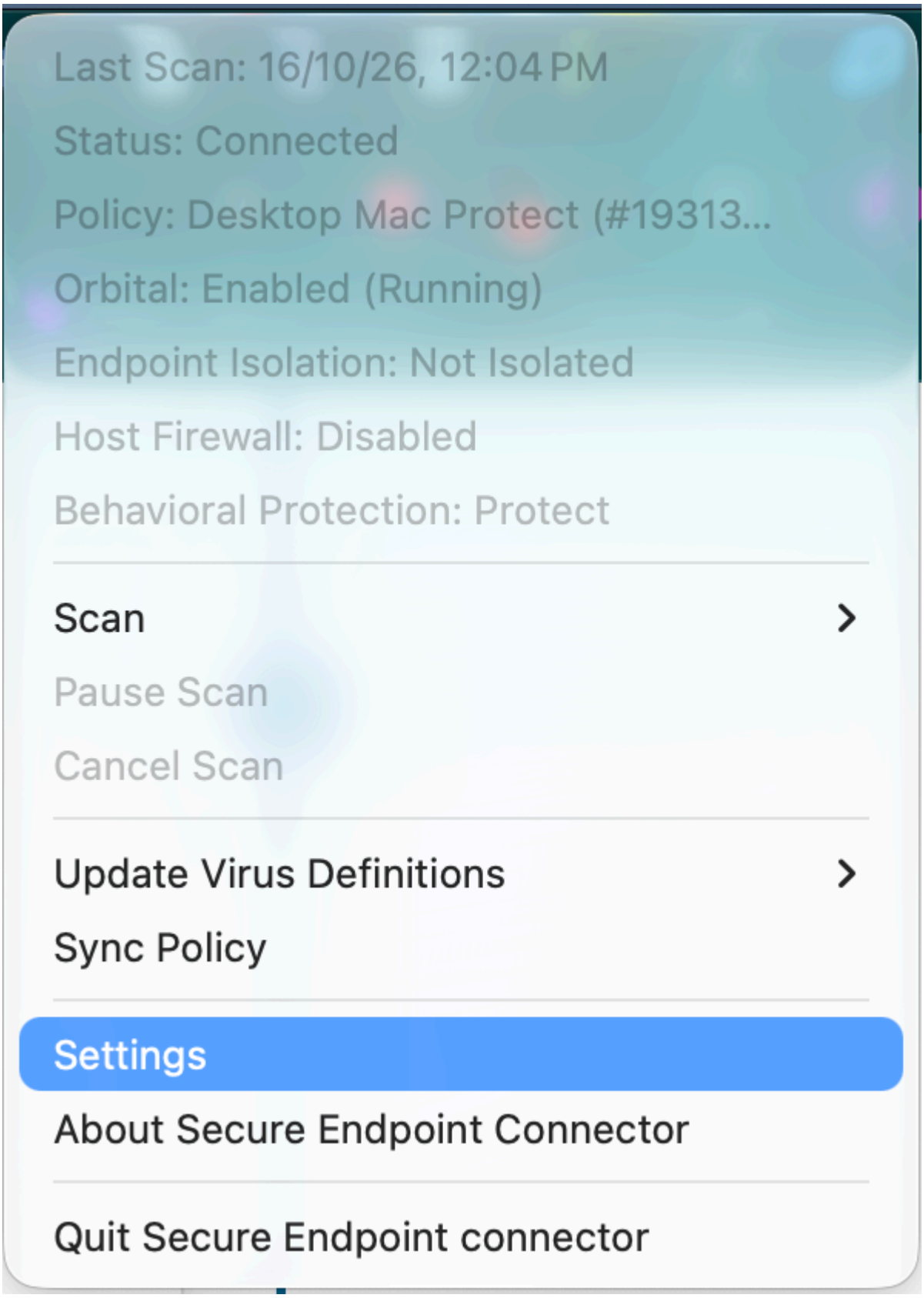
6.输入组的名称。例如，您可以使用Debug TechZone Mac Group。



7.将Mac策略从默认Mac策略更改为您刚刚创建的重复的新策略，即本示例中的Debug TechZone Mac Policy。Click Save.

8.定位至管理>计算机，然后在列表中标识您的计算机。选择它并单击移动到组……

9.从“选择组”下拉菜单中选择新创建的组。单击Move将所选计算机移动到新组中。您的Mac现在具有功能调试策略。您可以选择显示在菜单栏上的“安全终端”图标，并确保它有新策略：



屏幕截图2026-10-18(11.55.26 AM.png)

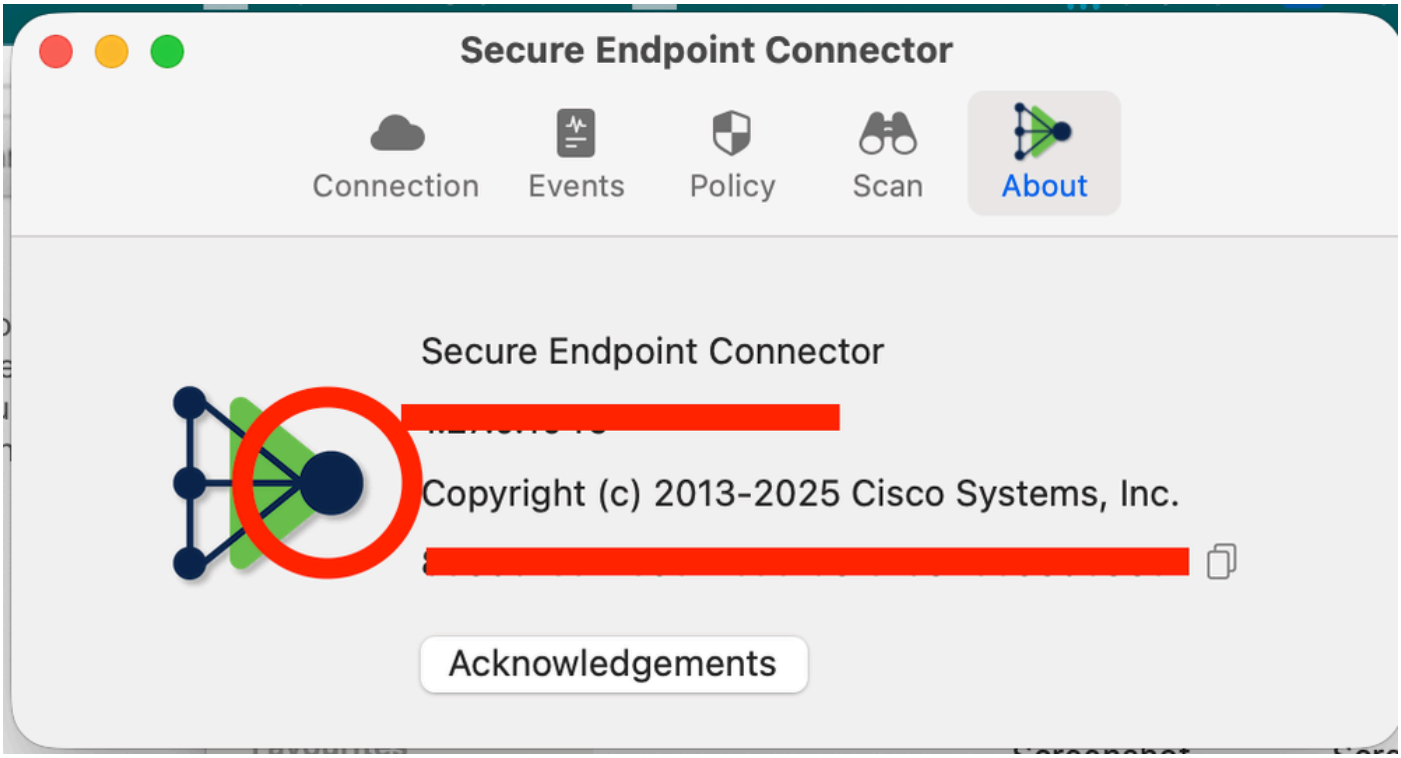
启用单心跳调试模式

此过程仅适用于1.0.4连接器及更高版本。它允许单个连接器进入调试模式，直到下一个心跳为止。心跳是连接器与管理服务的预定签入间隔。根据检测信号间隔，此过程不会捕获进行完整诊断分析所需的所有活动。

1.转到设置。

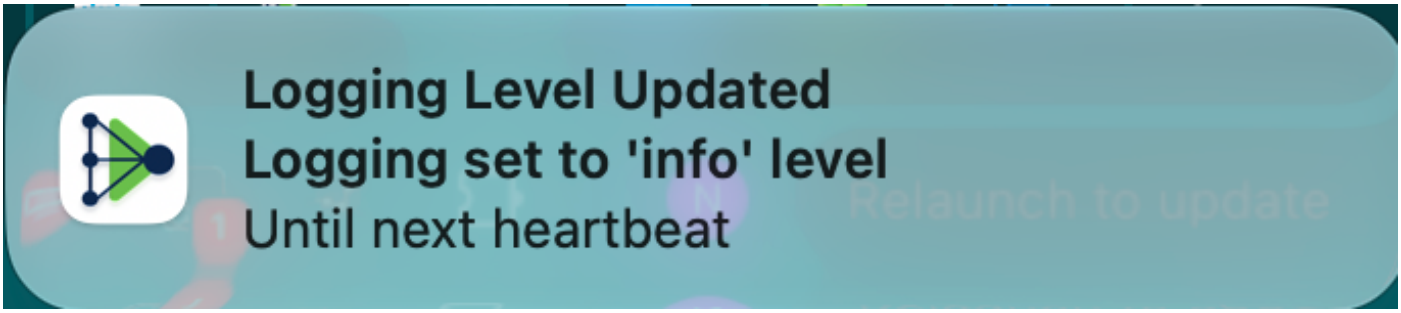
2.单击About。

3.在About页上，点击Secure Endpoint徽标的右半部。



屏幕截图2026-10-18(11.56.57 AM.png)

1.如果前几个步骤正确完成，则通知将显示在屏幕右侧：



屏幕截图2026-10-18(11.59.09 AM.png)

---

2. Debug会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，将安全终端连接器恢复为正常模式。完成以下步骤以禁用调试模式：

1.登录到安全终端控制台。

2.定位至管理>组。

3.找到在调试模式下创建的新组Debug TechZone Mac Group。

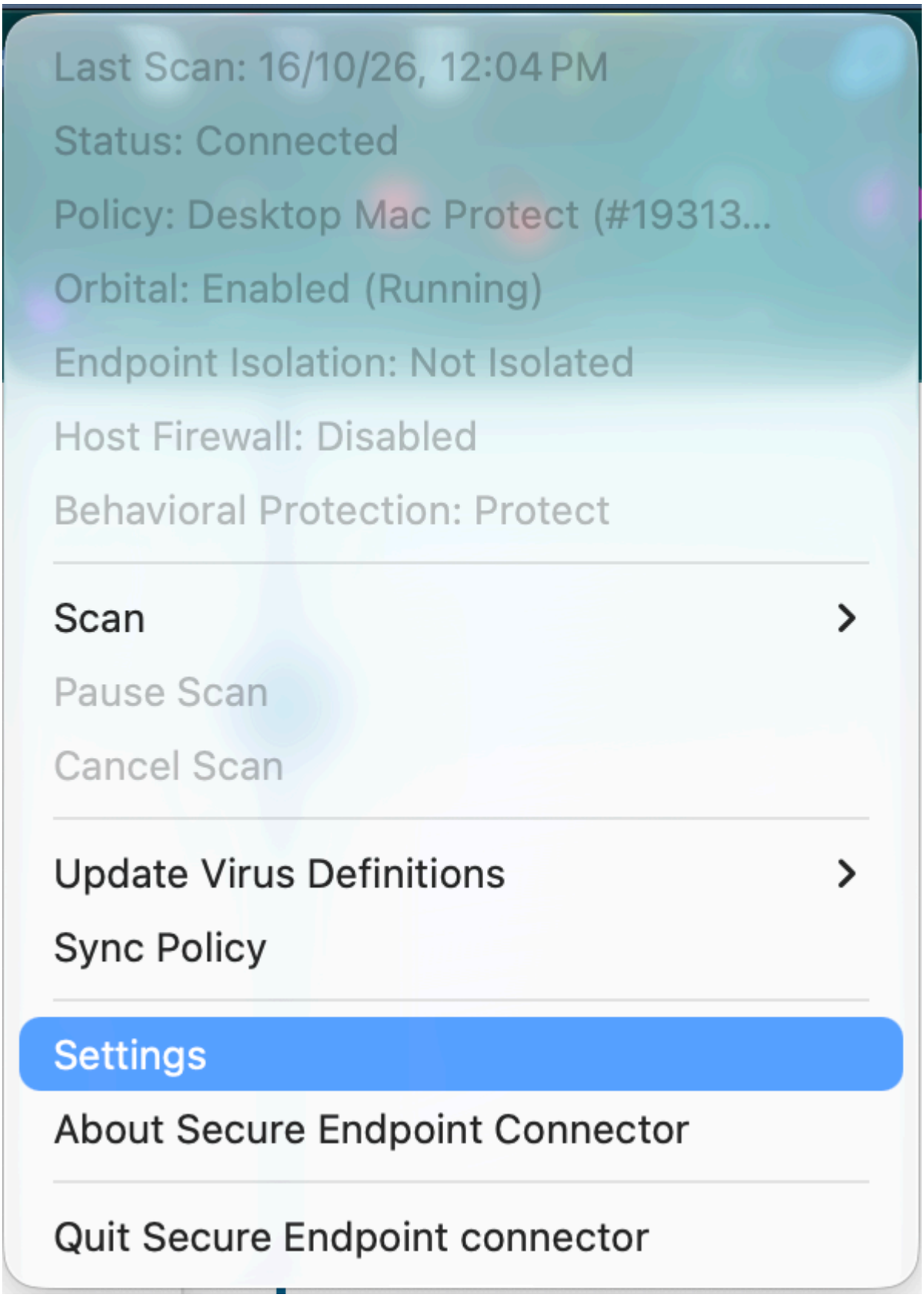
4.单击编辑。

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。选择该选项，您将进入计算机页面。再次从列表中选择您的计算机，然后单击Move to Group...

6.从“选择组”下拉菜单中选择上一个组。单击Move将所选计算机移动到上一组。

7.单击菜单栏中的“安全终端”图标。从菜单中选择Sync Policy。

8.验证策略现在是否恢复为上一个默认值。在菜单栏上选中此项。策略现在已恢复为原始策略，该策略在您将其更改为Debug TechZone Mac Group之前已使用：



屏幕截图2026-10-18(11.55.26 AM.png)

9.调试模式现已禁用，安全终端连接器现在可以正常运行。

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）。