对Windows设备安全终端中的调试日志收集进行故障排除

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

收集适用于Windows的思科安全终端中的调试日志文件

- 7.5.5及更低版本
- 8.0.1及更高版本（Cisco安全客户端）

简介

本文档介绍如何从Windows上的Cisco Secure Endpoint Connector生成调试捆绑文件。

先决条件

要求

所需知识：思科安全终端连接器。

使用的组件

本文档中的信息适用于：

- Microsoft Windows
- 适用于Windows的思科安全终端连接器：
  - 版本7.x.x及更高版本（版本7.5.5及更高版本中的过程）
  - 版本8.x.x及更高版本(Cisco安全客户端；8.0.1版及更高版本（Cisco安全客户端）中的过程。

注意：本文档不涵盖版本7.5.6至8.0.0。如果这些版本正在使用中，请在产品文档中或与Cisco TAC确认正确的工作流程。

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。

背景信息

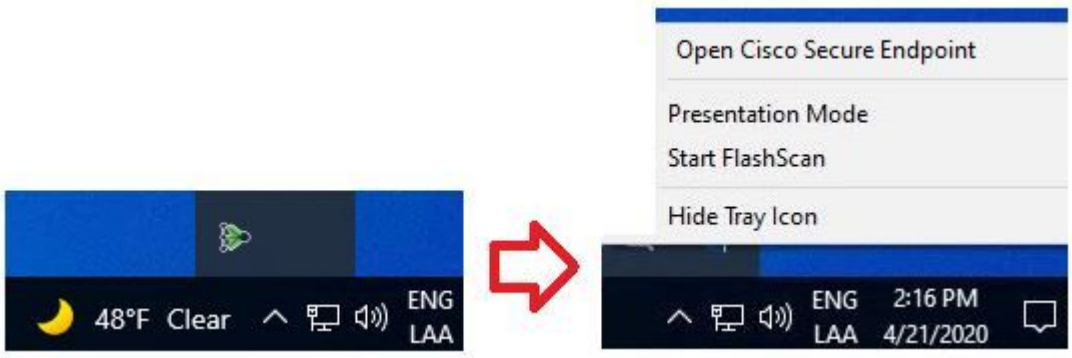
有关Microsoft Windows操作系统上的Cisco Secure Endpoint Connector的性能问题，请联系思科技术支持中心(TAC)。思科技术支持工程师分析调试捆绑包文件中提供的日志，以确定根本原因。

注意：如果从托盘图标菜单启用了Debug模式，则Debug模式在重新启动后不会持续。要在重新启动后保留设置，请通过安全终端控制台中的策略配置启用Debug模式。

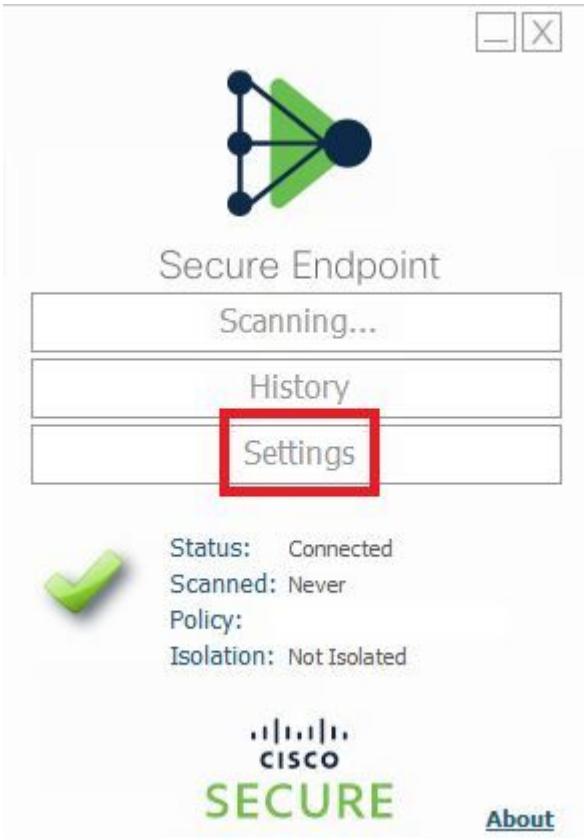
在Cisco Secure Endpoint for Windows中收集调试日志文件

版本7.5.5及更低版本

步骤1.点击任务栏上的Cisco Secure Endpoint托盘图标，然后单击Open Cisco Secure Endpoint，如图所示。



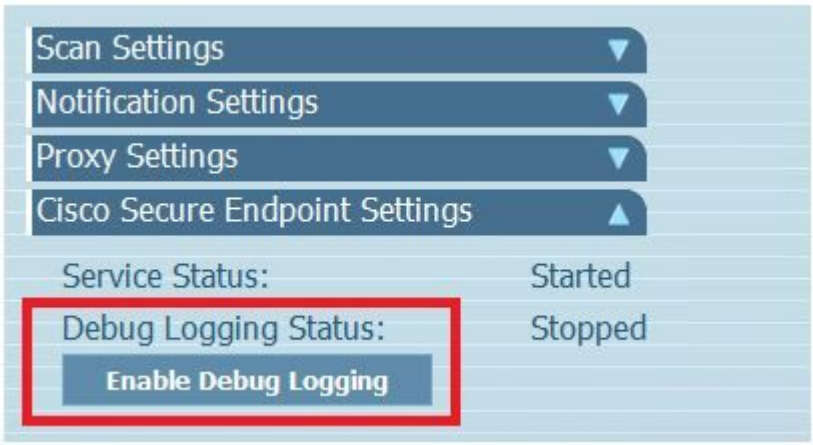
步骤2.单击Secure Endpoint Connector中的Settings，如图所示。



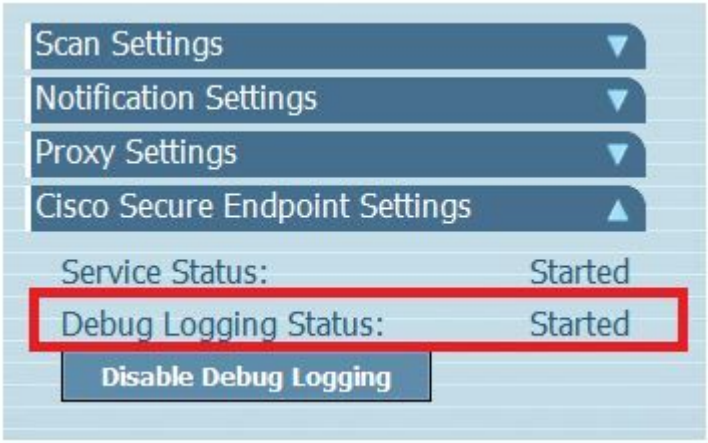
步骤3.选择Settings > Cisco Secure Endpoint Connector Settings，如图所示。



步骤4.单击Enable Debug Logging，如图所示。

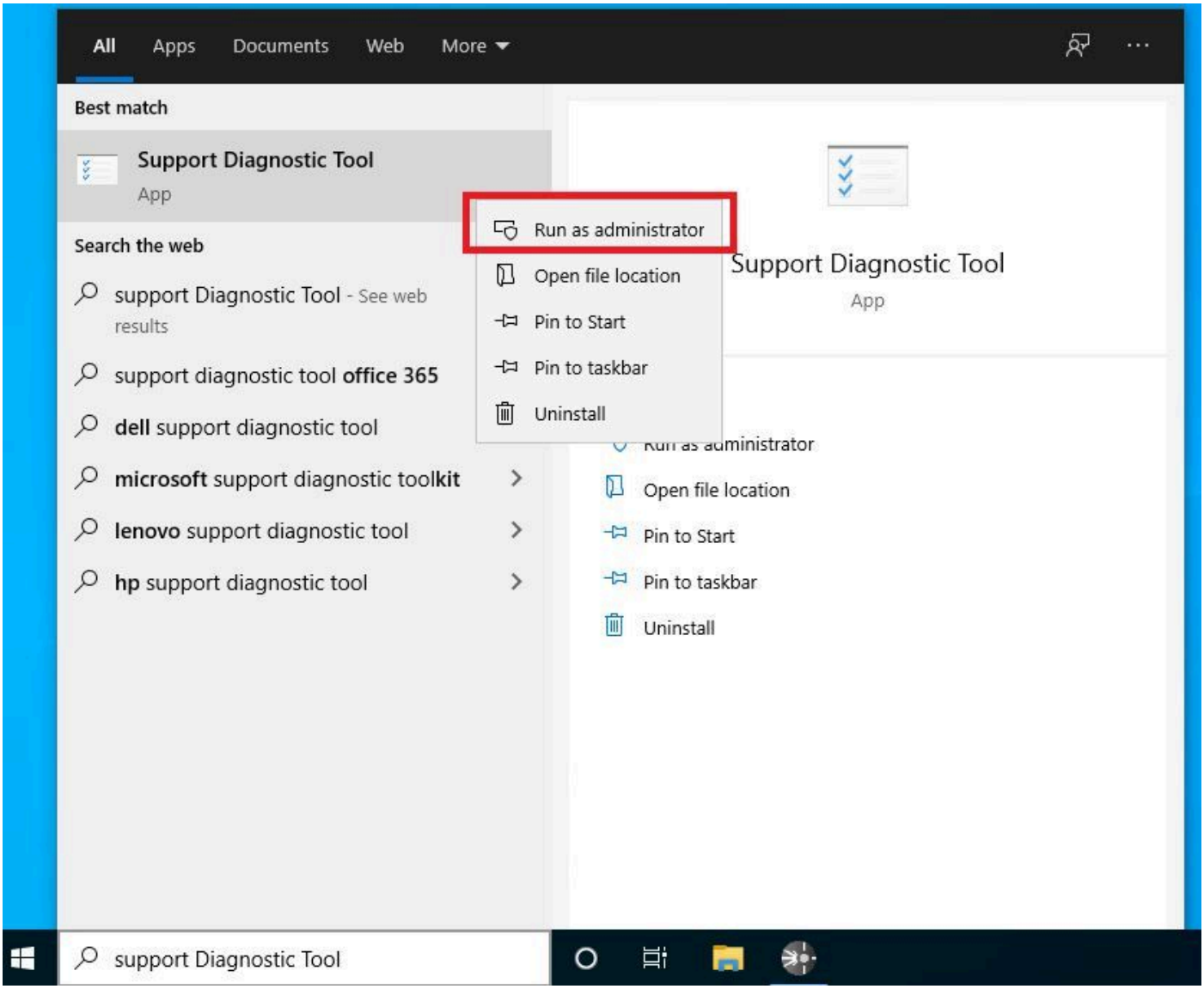


步骤5.按钮名称更改为Disable Debug Logging。调试模式现在已启用，如图所示。



步骤6.重新创建问题并让设备运行至少30分钟。

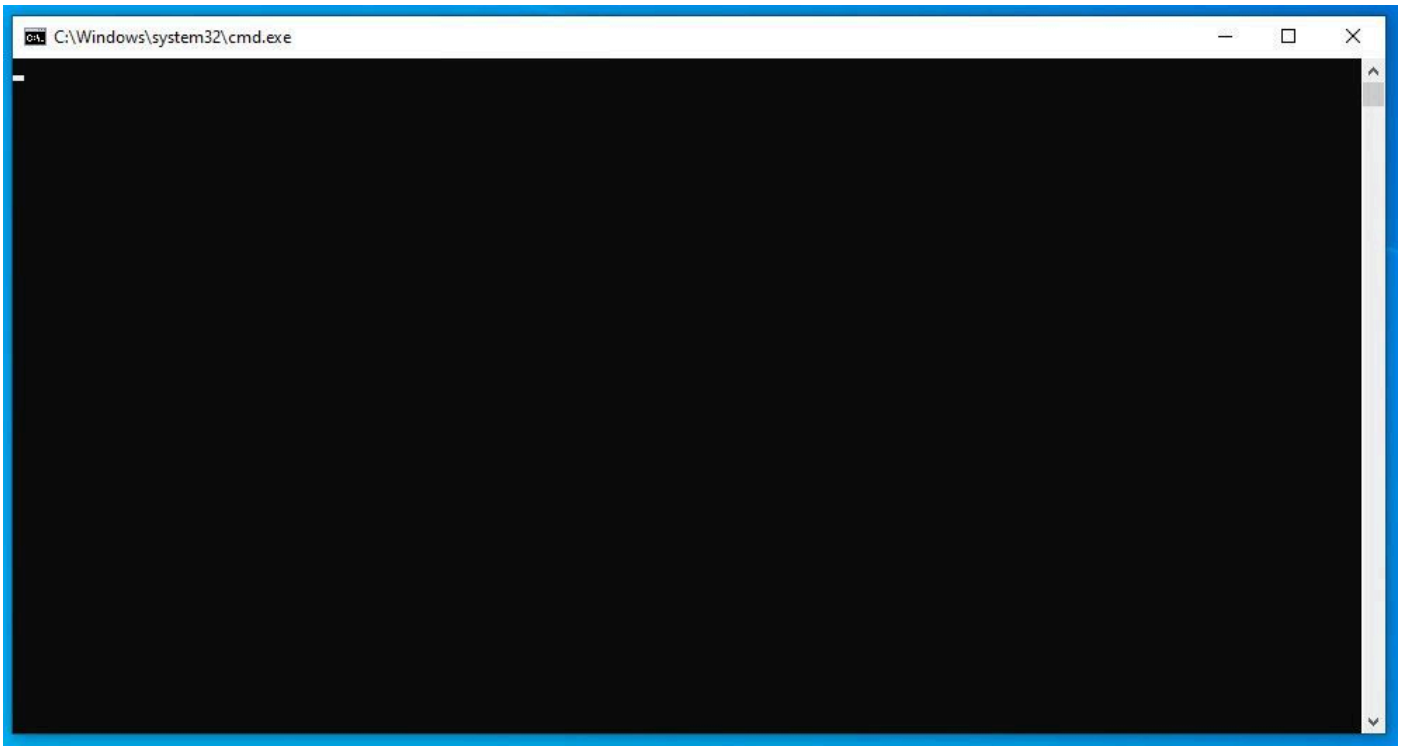
步骤7.在30分钟后，打开Windows搜索并键入Support Diagnostic Tool。以Administrator权限运行工具，如图所示。



注意： 从Secure Endpoint Connector版本7.5.5开始，不需要具有管理员权限的Windows帐户来打开支持诊断工具，以便收集调试日志。发行说明:“更新了支持诊断工具，使其不需要提升的权限”。

步骤8.出现临时Windows黑屏，如图所示。

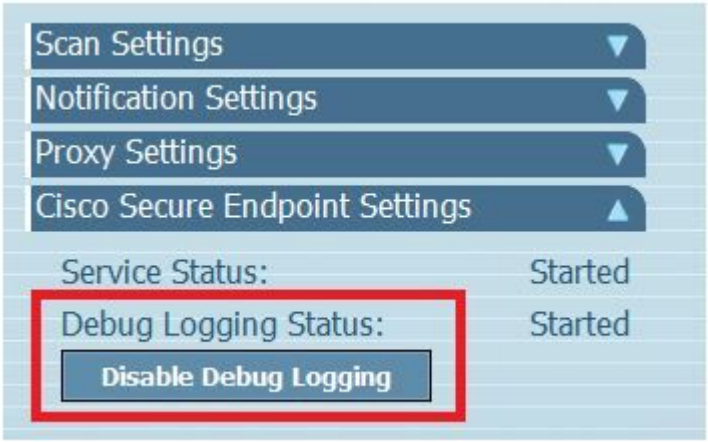
注意：等待几秒钟，让黑色窗口自动关闭。



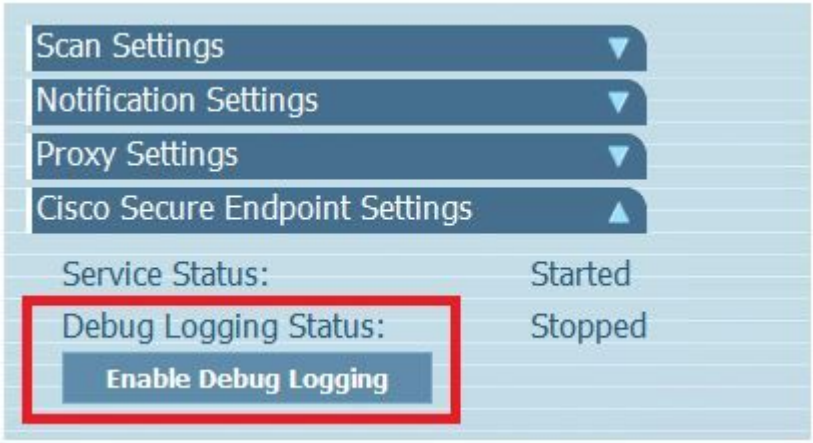
步骤9.几分钟后，调试捆绑文件将显示在桌面上，如图所示。



步骤10.生成调试捆绑文件后，可以禁用调试模式。选择Disable Debug Logging按钮，如图所示。



步骤11.按钮名称更改为Enable Debug Logging，如图所示。



注意： 必须启用调试模式才能收集调试捆绑文件。如果长时间启用调试模式，可能会占用磁盘空间。

步骤12.收集调试捆绑包文件后，将其上传到My Case in Cloud Apps。

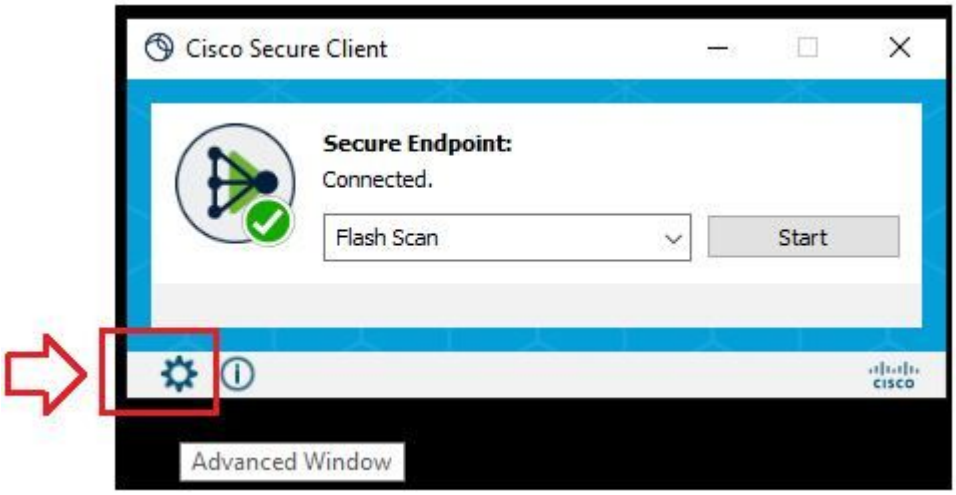
注意： 确保您参考了服务请求编号。

版本8.0.1及更高版本（Cisco安全客户端）

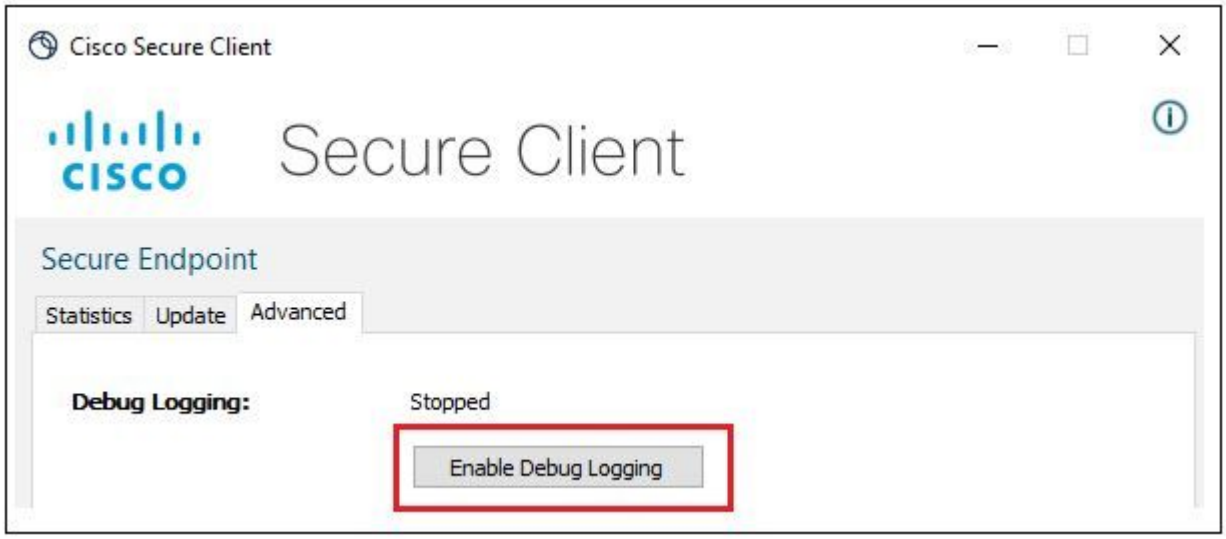
步骤1.点击任务栏上的Cisco Secure Endpoint托盘图标，如图所示。



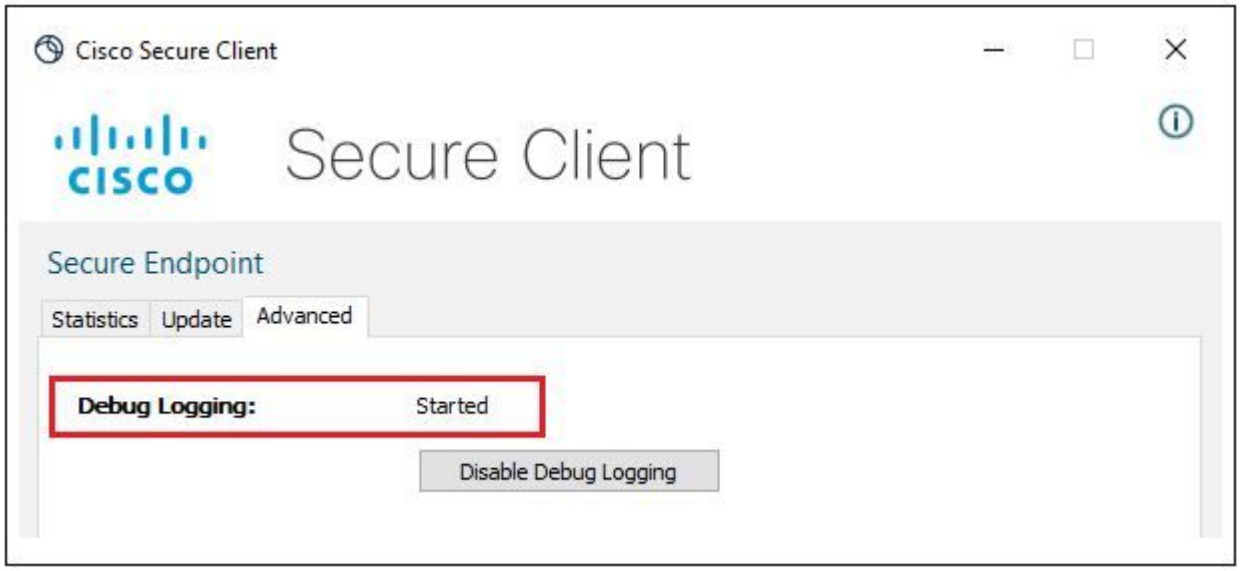
步骤2.在Secure Endpoint Connector中的托盘图标菜单中单击Advanced Window，如图所示。



步骤3.单击Advanced选项卡，然后单击Enable Debug Logging，如图所示。



步骤4.调试日志记录按钮名称更改为Started。调试模式现在已启用，如图所示。

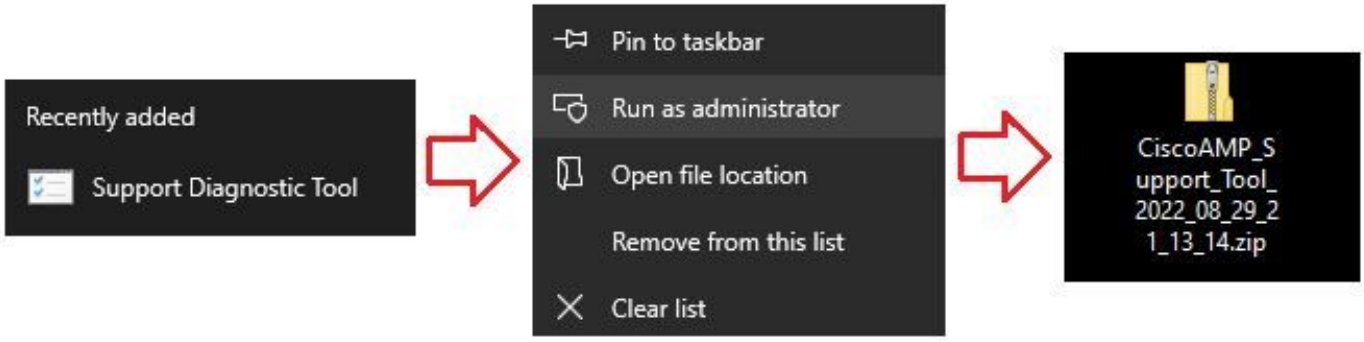


步骤5.重新创建问题并让设备运行至少30分钟。

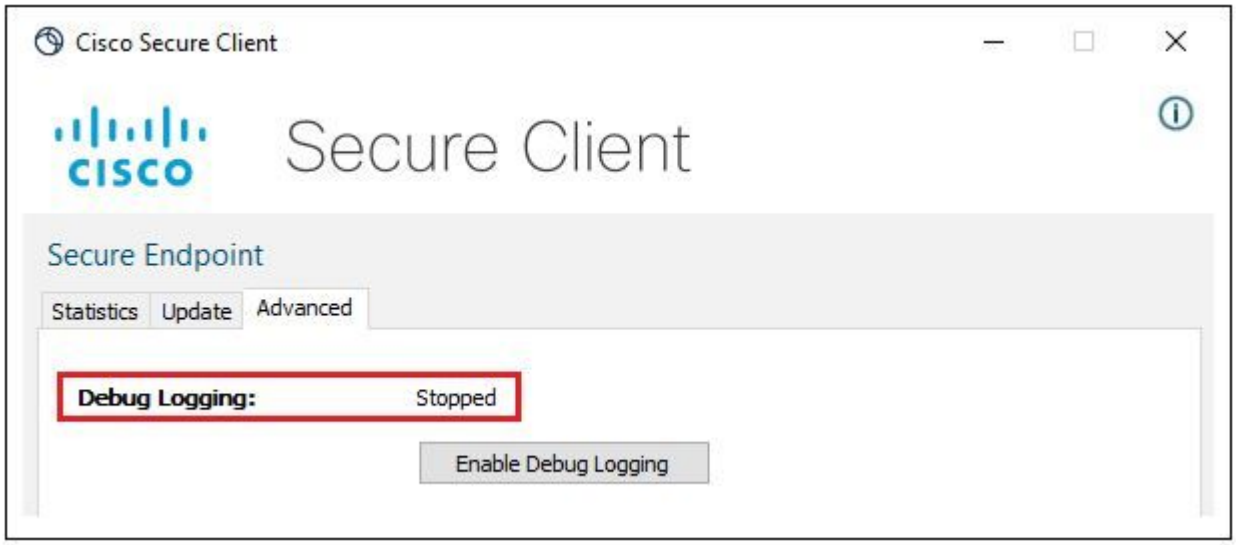
步骤6.打开Windows Search并输入Support Diagnostic Tool。

步骤7.单击Support Diagnostic Tool，然后使用Administrator权限运行该工具。

步骤8.几分钟后，确认Debug Bundle文件显示在桌面上，如图所示。



步骤9.生成调试捆绑文件后，可以禁用调试模式。点击禁用调试日志记录。



注意： 必须启用调试模式才能收集调试捆绑文件。如果长时间启用调试模式，可能会占用磁盘空间。

步骤10.收集调试捆绑包文件后，将其上传到My Case in Cloud Apps。

注意： 确保您参考了服务请求编号。

相关内容

- 思科安全终端连接器版本说明
- 思科安全终端文档
- 我的云应用案例（将文件上传到TAC服务请求）

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）。