# 思科安全终端：命令行开关介绍

## 目录



## 简介

本文档介绍可用于思科安全终端的命令行(CLI)交换机。

## 背景信息

思科安全终端包含许多可自定义的功能和操作，可使用命令行开关在终端本地执行这些功能和操作。本文档展示了它们。

## 思科安全终端命令行交换机

### 安全终端安装程序交换机

amp_installer.exe

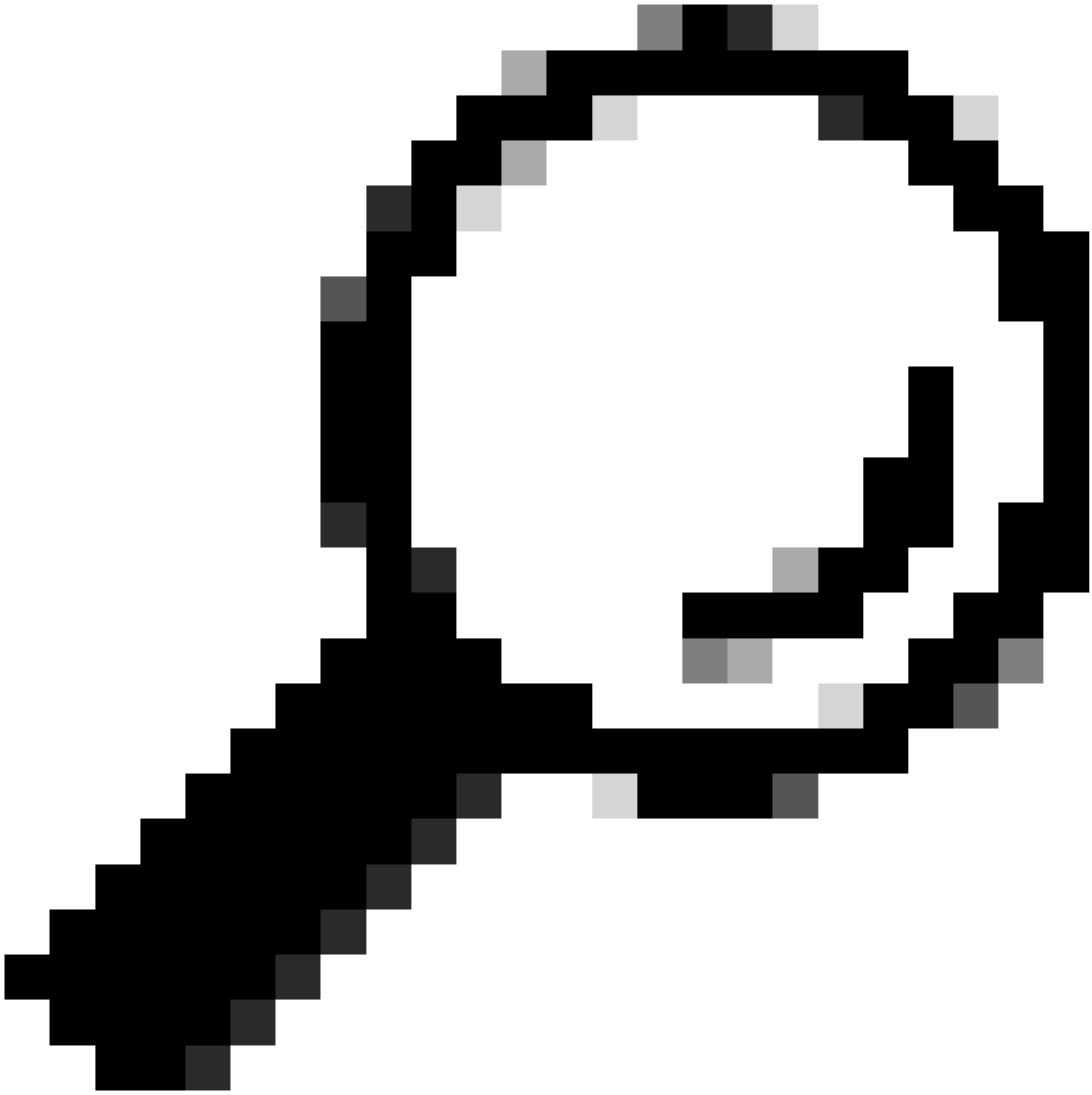
1. 在Windows上打开命令提示符。
2. 在命令提示符下导航到安装程序所在的文件夹（Downloads文件夹用作以下示例）。

   cd C:\Users\sysadmin\Downloads

   - 执行提供的可用交换机。

   amp_protect.exe <switch>

**注意**：执行命令后不会返回任何输出。



**提示**：一次可以使用多个交换机。

| 命令行开关 | 命令说明 | 特殊说明 |
| --- | --- | --- |
| /S | 用于将安装程序置于静默模式。 | |

| | | |
|---|---|---|
| /temppath | 用于指定要提取和执行的安装文件的自定义临时位置。 | /temppath C:\ |
| /desktopicon 0 | 用于指定不创建桌面图标。 | 这是默认配置，不需要提供。 |
| /desktopicon 1 | 用于指定创建桌面图标。 | |
| /startmenu 0 | 未创建“开始”菜单快捷方式。 | |
| /startmenu 1 | “开始”菜单快捷方式已创建。 | 这是默认配置，不需要提供。 |
| /contextmenu 0 | 从右键单击上下文菜单禁用“立即扫描”。 | |
| /contextmenu 1 | 在右键单击上下文菜单中启用“立即扫描”。 | 这是默认配置，不需要提供。 |
| /remove 0 | 卸载连接器并保留文件以供以后重新安装。 | 在重新安装连接器时，保留带有UUID的XML文件并允许重复使用现有的计算机对象。日志文件也会保留。如果正在使用连接器保护密码，则必须使用/uninstallpassword标志指定该密码。 |
| /remove 1 | 卸载连接器并删除所有相关文件。 | 如果正在使用连接器保护密码，则必须使用/uninstallpassword标志指定该密码。 |
| /uninstallpassword | 指定使用/remove标志时的卸载密码 | 在标志后指定卸载密码。 |

| | | |
|---|---|---|
| | 。如果启用了连接器保护功能，则必须指定 | |
| /skipdfc 1 | 跳过DFC驱动程序的安装。 | 所有安装有此标志的连接器必须位于禁用了网络引擎的策略的组中。 |
| /skiptetra 1 | 跳过TETRA驱动程序的安装。 | 所有安装有此标志的连接器必须位于未选中Tetra标志的策略的组中。 |
| /D=[路径] | 用于指定要执行安装的目录。例如，/D=C:\ | 必须将此参数指定为最后一个参数。<br><br>对于/D=命令行开关，默认安装目录因操作系统而异。以下是Microsoft Windows XP Service Pack 3或更高版本上的默认安装目录：<br><br>对于x86平台：<br><br>C:\Program Files (x86)\Cisco\AMP<br><br>x64平台：<br><br>C:\Program Files\Cisco\AMP |
| /goldenimage 1 | 安装连接器以准备金色图像 | 此标志旨在帮助在虚拟环境中准备黄金映像。使用此标志可防止连接器在创建金色图像期间启动和注册。有关更多信息，请参阅：<br>如何使用安全终端准备黄金映像<br>https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214462-how-to-prepare-a-golden-image-with-amp-f.html |
| /skiposccheck 1 | 在安装过程中跳过操作系统检查。 | 此标志可用于在其不兼容的操作系统上安装安全终端。 |

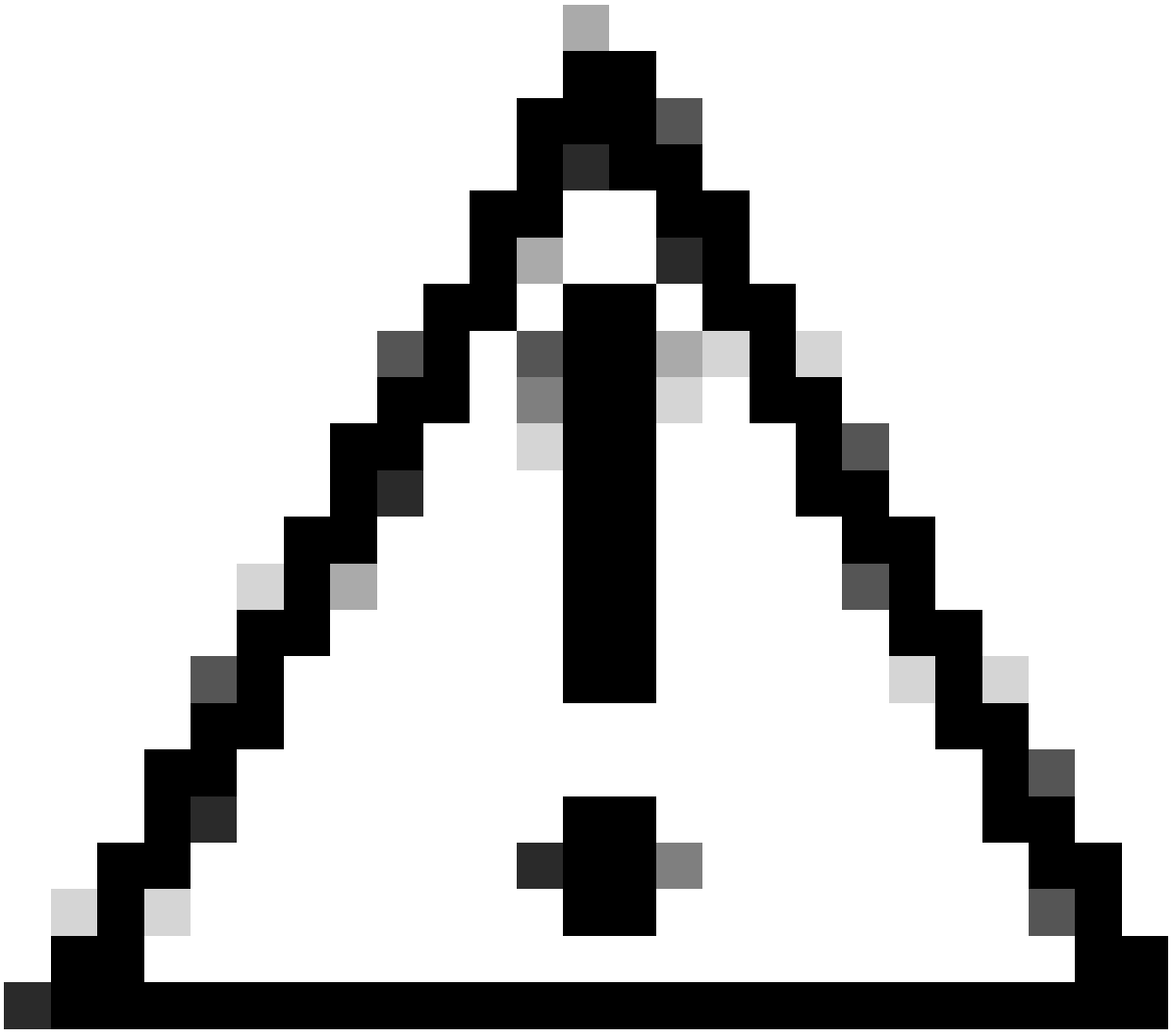
ipsupporttool.exe

- 在Windows上打开命令提示符。

- 在命令提示符下导航至文件夹。 默认路径：**C:\Program Files\Cisco\AMP\X.X.X**，X.X.X表示版本号)。
cd C:\Program Files\Cisco\AMP\8.2.1.21612\

- 执行提供的可用交换机。
ipsupporttool.exe <switch>

**注意**：执行交换机时，不会返回任何输出。

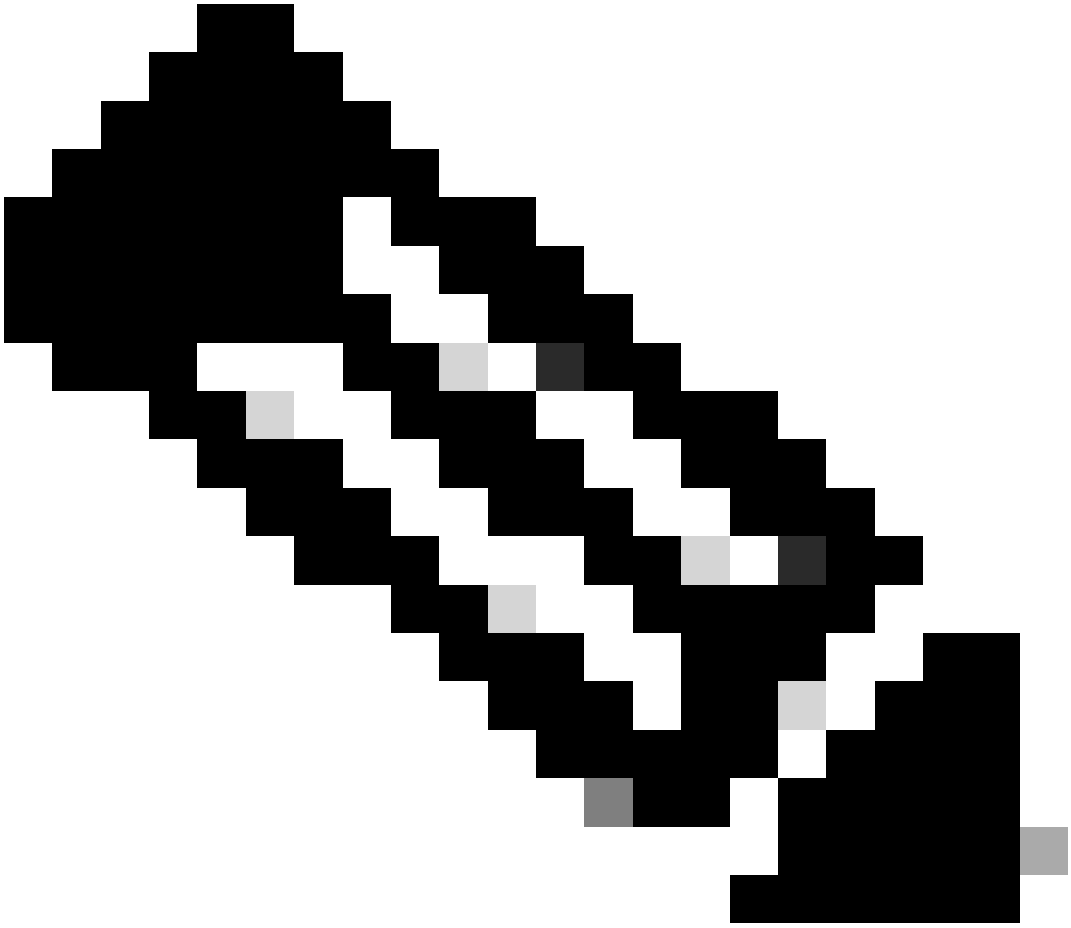


**注意**：任何引用文件夹选择的交换机都要求文件夹已存在

| 命令行开关 | 命令说明 | 特殊说明 |
| --- | --- | --- |
| -o <路径> | 指定支持工具的输出文件夹。 | 如果未指定此选项，则默认为桌面。 |
| -d <安装路径> | 指定Windows支持工具可以从中检索文件的文件夹。 | 如果未指定，则默认为安全终端的默认安装目录。 |
| -t <分钟> | 从Windows支持工具运行指定时间的Timed调试级别诊断。 以分钟为单位指定持续时间。 | |

安全终端UI交换机

iptraytool.exe



**注意**：iptraytool.exe仅在旧版安全终端上可用。

- 在Windows上打开命令提示符。

- 在命令提示符下导航至文件夹。 默认路径：**C:\Program Files\Cisco\AMP\X.X.X**，X.X.X表示版本号)。

```
cd C:\Program Files\Cisco\AMP\7.5.3.20938\
```

- 执行提供的可用交换机。

```
iptray.exe <switch>
```

| 命令行开关 | 命令说明 | 特殊说明 |
| --- | --- | --- |
| -f | 允许从命令行激活客户端用户界面。 | 仅当终端通过Policy关闭了GUI并且未选中Start Client User Interface时，才需要执行此操作。 |

安全终端SFC交换机

sfc.exe

- 在Windows上打开命令提示符。

- 在命令提示符下导航至文件夹。 默认路径：**C:\Program Files\Cisco\AMP\X.X.X**，X.X.X表示版本号)。
cd C:\Program Files\Cisco\AMP\8.2.1.21612\

- 执行提供的可用交换机
sfc.exe <switch>

| 命令行开关 | 命令说明 | 特殊说明 |
| --- | --- | --- |
| -s | 启动Immunet保护（Windows连接器）服务。服务必须已经向SCM注册后才能启动。 | |
| -k | 停止Immunet保护（Windows连接器）服务。 | 如果启用了连接器保护，请在-k之后输入密码，以便成功停止服务。 |
| -u | 卸载Immunet保护（Windows连接器）服务。 向Windows服务控制管理器(SCM)注销服务。 卸载程序使用此选项卸载Windows连接器服务。 | |
| -r | 重置Immunet保护（Windows连接器）服务。这与-i选项非常相似，但不安装服务。这对于修复local.xml损坏非常有用。 | |

| | | |
|---|---|---|
| -l开始 | 动态切换调试和内核日志记录（触发器为小写L）。 | 此状态将一直保持到关闭、服务重新启动或配置新策略以更改日志记录级别。 |
| -l停止 | 动态关闭调试和内核日志记录（触发器为低位L）。 | |
| -unblock SHA_of_file | 此选项可取消阻止进程执行。 运行此命令交换机后，可以从应用程序阻止列表的本地内核缓存中删除该应用程序。 | 当应用程序由于误报或错误而被阻止，并且您希望快速取消阻止应用程序，而不等待30分钟或重新启动计算机时，可以使用此命令。 |
| -reregister | 此选项可以在服务运行时从local.xml和注册表清除uuid和证书，并触发重新注册。将使用新值更新Local.xml和注册表。但是，如果启用ID同步，并且连接器再次获取现有UUID，则会阻止此操作。 如果用于初始安装的安装包已修改，则可以在重新注册之后将连接器置于默认组/策略中。 | 如果启用了连接器保护，您需要输入以下信息：sfc.exe -reregister _password_ |
| -forceupdate | 此选项强制连接器更新TETRA定义。 | |
| -forceapdeupdate | 此选项强制连接器更新行为保护定义。 | 您可以在安全终端控制面板中的device trajectory中检查终端上安装的当前行为保护定义。 |

相关信息

- 技术支持和文档 - Cisco Systems
- 思科安全终端- TechNotes
- 思科安全终端-用户指南
- 使用安全终端Mac/Linux CLI

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）。