使用恢复方法排除陷入隔离的安全终端故障

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[背景信息](#)
[停止隔离](#)
[从控制台停止隔离会话](#)
[从命令行停止隔离会话](#)
[恢复故障排除](#)
[Mac恢复：](#)
[Windows恢复：](#)
[从命令行恢复隔离方法](#)
[不使用命令行的恢复隔离方法](#)
[验证](#)
[相关信息](#)

简介

本文档介绍使用从隔离模式安装的安全终端连接器恢复终端的流程。

先决条件

要求

Cisco 建议您了解以下主题：

- 安全终端连接器
- 安全终端控制台
- 终端隔离功能

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 安全终端控制台版本v5.4.2021092321
- 安全终端Windows连接器版本7.4.5.20701
- 安全终端Mac连接版本v1.21.0

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

在终端设备处于此状态且无法禁用隔离模式的情况下，本文档中介绍的过程会很有用。

终端隔离功能可以阻止计算机上的网络活动（IN和OUT），以防止数据泄露和恶意软件传播等威胁。其网址为：

- 支持7.0.5及更高版本的Windows连接器的64位版本
- 支持Mac连接器版本1.21.0及更高版本的Mac版本。

终端隔离会话不会影响连接器与思科云之间的通信。您的终端具有和会话之前相同的保护和可视性级别。您可以配置IP隔离允许地址列表，以避免在活动终端隔离会话处于活动状态时连接器阻塞有问题的IP地址。您可以在此处查看有关终端隔离功能的更多详细信息。

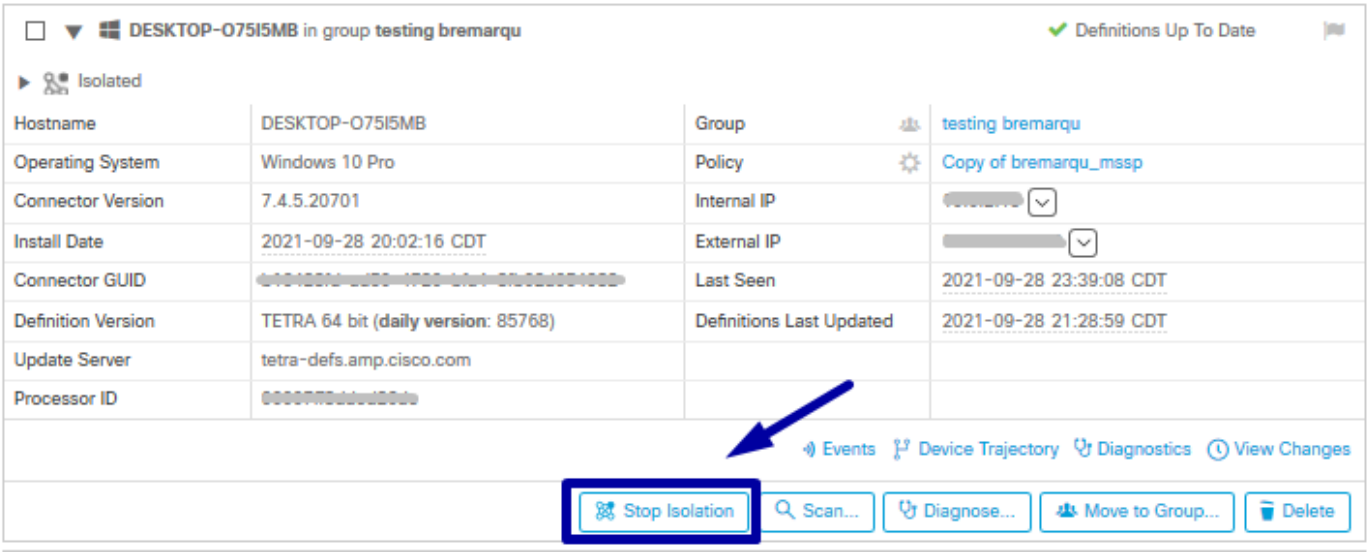
停止隔离

一旦要在计算机上停止终端隔离，请通过安全终端控制台或命令行执行以下快速步骤。

从控制台停止隔离会话

停止隔离会话并将所有网络流量恢复到终端。

步骤1:在控制台中，导航到**管理>计算机**。
第二步：找到要停止隔离的计算机，然后单击以显示详细信息。
第三步：单击**Stop Isolation**按钮，如图所示。



第四步：输入有关停止终端上的隔离功能的原因的注释。

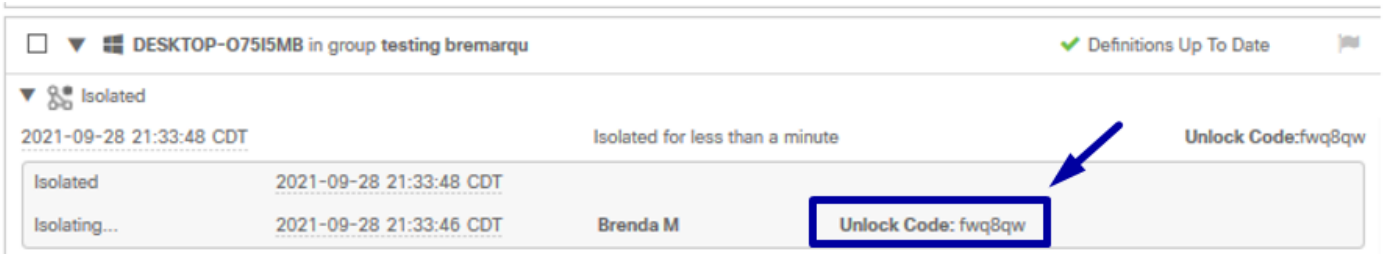
从命令行停止隔离会话

如果隔离终端失去与思科云的连接，并且您无法从控制台停止隔离会话。在这些情况下，您可以使用解锁代码从命令行在本地停止会话。

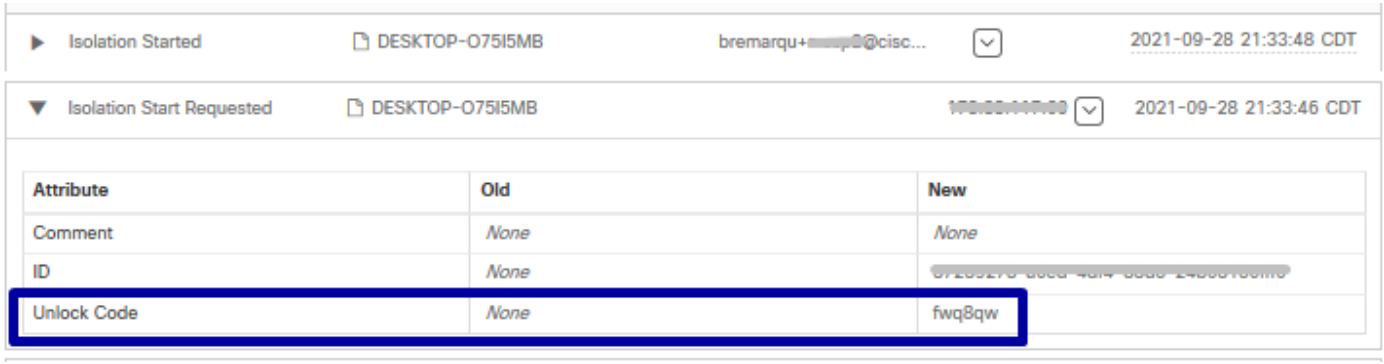
步骤1:在控制台中，导航到**管理>计算机**。

第二步：找到要停止隔离的计算机，然后单击以显示详细信息。

第三步：请注意**解锁代码**，如图所示。



第四步：如果导航到**帐户>审核日志**，也可以找到**解锁代码**，如图所示。



第五步： 在隔离的计算机上，以管理员权限打开命令提示符。

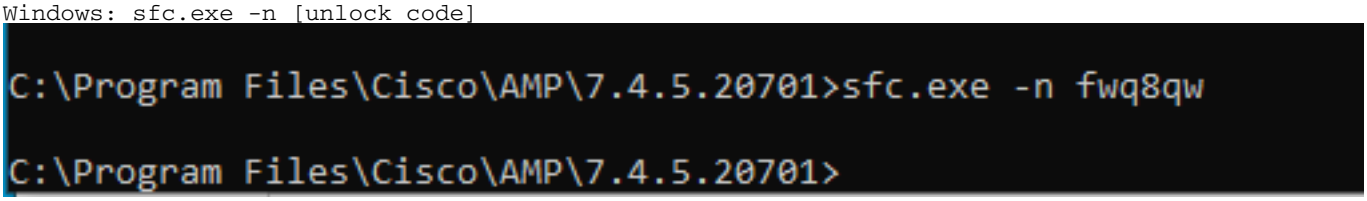
第六步： 导航到安装连接器的目录

Windows: C:\Program Files\Cisco\AMP\[版本号]

Mac:/opt/cisco/amp

步骤 7.运行stop命令

```
Windows: sfc.exe -n [unlock code]
```




```
Mac: ampcli isolate stop [unlock code]
```

注意：如果解锁代码输入错误5次，则必须在等待30分钟后再尝试再次解锁。

恢复故障排除

如果您用尽所有途径，但仍无法从安全终端控制台或本地使用解锁代码恢复孤立的终端；您可以使用紧急恢复方法恢复孤立的终端。

Mac恢复：

删除隔离配置并重新启动安全终端服务

```
sudo rm /Library/Application\ Support/Cisco/Secure\ Endpoint/endpoint_isolation.xml
sudo launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plist
sudo launchctl load /Library/LaunchDaemons/com.cisco.amp.daemon.plist
```

Windows恢复：

从命令行恢复隔离方法

如果终端设备被隔离粘滞，且无法通过安全终端控制台或解锁代码禁用隔离，请执行以下步骤。

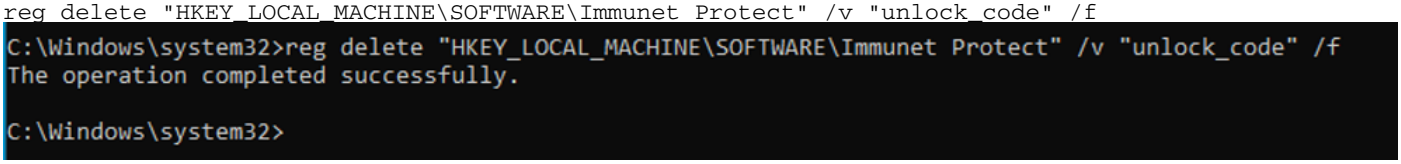
步骤1:通过连接器用户界面或Windows服务停止连接**器服务**。

第二步：找到安全终端连接器服务并停止该服务。

第三步：在隔离的计算机上，以管理员权限打开命令提示符。

第四步：运行命令**reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f**，如图所示。

```
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f
```

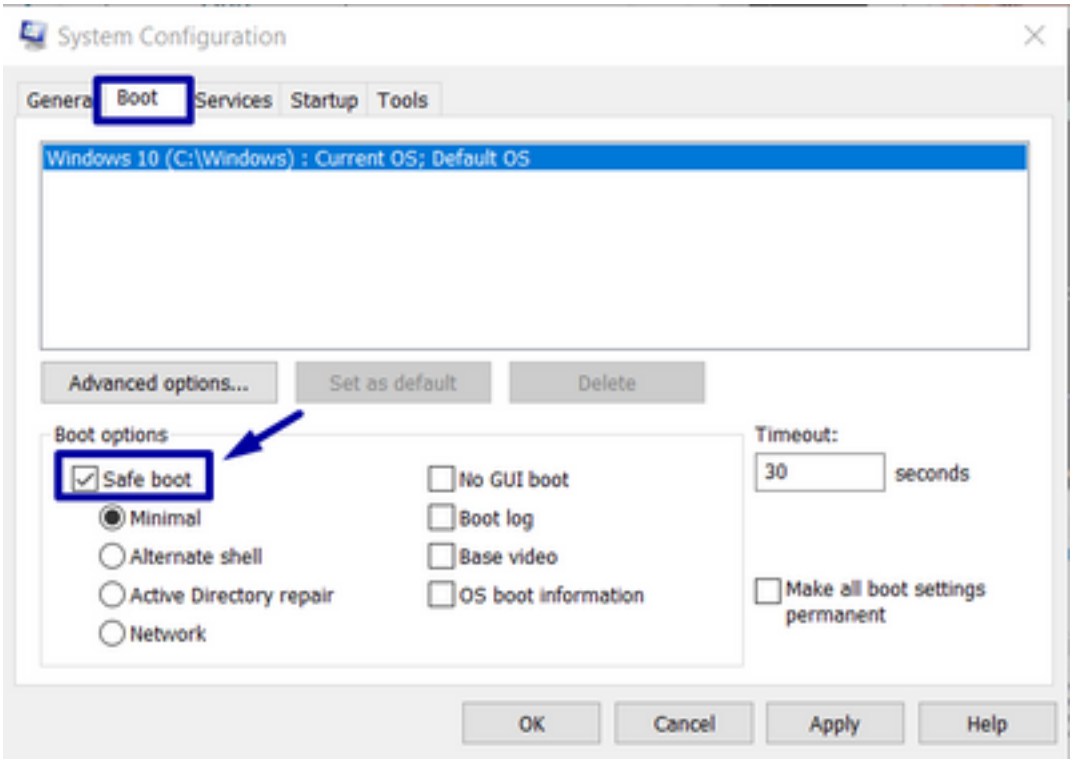


第五步：消息**The operation completed successfully**表示操作已完成。（如果显示另一条消息，如“Error: Access is denied”，则需要在运行命令之前停止安全终端连接器服务）。

第六步：启动安全终端连接器服务。

> **提示**：如果无法从连接器用户界面或Windows服务停止安全终端连接器服务，则可以执行安全启动。

在隔离终端上，导航到**System Configuration > Boot > Boot options**，然后选择**Safe boot**，如映像所示。

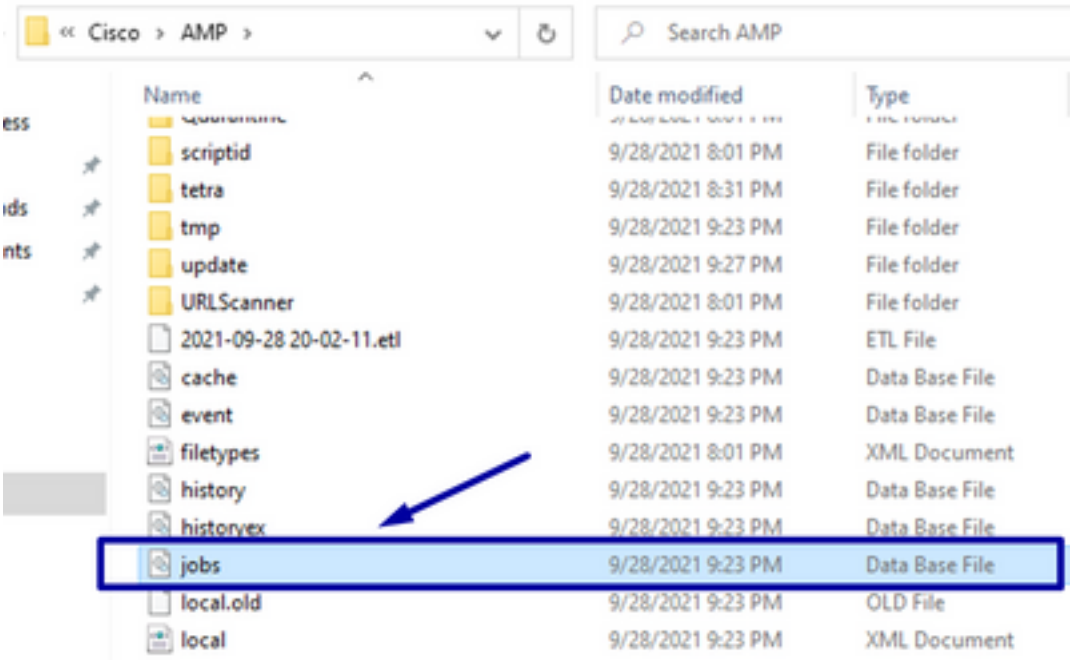


不使用命令行的恢复隔离方法

如果终端设备被隔离卡住，并且无法通过安全终端控制台或解锁代码禁用隔离，或者即使您无法使用命令行也无法禁用隔离，请执行以下步骤：

步骤1:通过连接器用户界面或Windows服务停止连接**器服务**。

第二步：导航到安装连接器的目录(C:\Program Files\Cisco\AMP\)，然后删除文件**jobs.db**，如图所示。



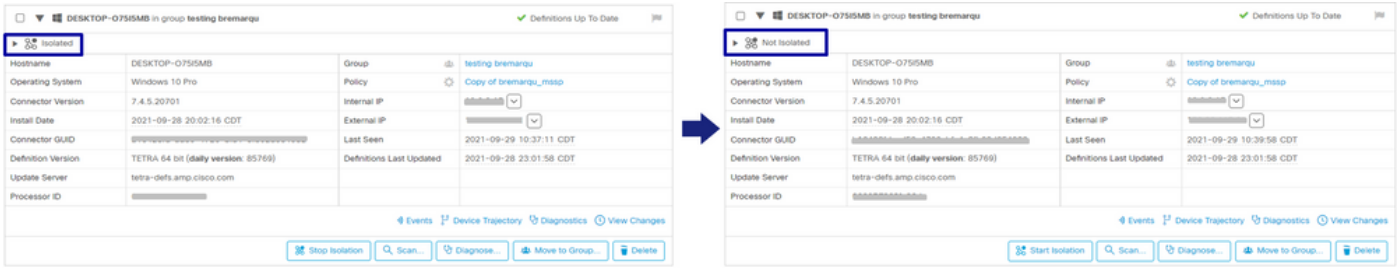
3.重新启动计算机。

此外，如果在控制台中看到Isolation事件，则可以导航到**Error Details**以查看错误代码及其说明，如图所示。

验证

为了验证终端已恢复隔离或不再隔离，您可以看到“安全终端”连接器用户界面将“隔离”状态显示为**未隔离**，如图所示。

在安全终端控制台中，如果导航到**管理>计算机**，然后找到有问题的计算机，则可以单击以显示详细信息。隔离状态显示**Not Isolated**，如图所示。



相关信息

- [安全终端用户指南]
- [技术支持和文档 - Cisco Systems]

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）。