



# 故障排除

---

本章包含以下部分：

- [收集系统信息](#) , on page 1
- [对硬件问题进行故障排除](#) , on page 1
- [功能设置问题故障排除](#) , on page 2
- [一般故障排除资源](#) , on page 2
- [特定功能问题的故障排除](#) , on page 2
- [使用技术支持](#) , on page 4
- [运行数据包捕获](#) , on page 7
- [远程重置设备电源](#) , on page 8

## 收集系统信息

您可以获得有关设备及其状态的信息，包括序列号。参考 [监控系统状态](#)

## 对硬件问题进行故障排除

硬件设备前面板和/或后面板上的指示灯指示设备的运行状况和状态。有关这些指示灯的说明，请参阅硬件指南，例如，中指定位置提供的《思科 x90 系列内容安全设备安装和维护指南》。

这些文档中还会介绍设备规格，例如温度范围。



---

**Note** 如果您需要重启 x80 或 x90 设备，请等待至少 20 分钟以便设备完成启动准备（所有 LED 均呈绿色亮起），然后再按电源按钮。

---

## 功能设置问题故障排除

如果您在成功配置功能方面遇到困难，请参阅您必须为每项功能完成的任务的摘要。这些摘要包括每项任务的特定信息的链接。

- [设置集中 Web 报告和跟踪](#)
- [设置集中邮件报告](#)
- [设置集中邮件跟踪](#)
- [设置集中垃圾邮件隔离区](#)
- [集中策略、病毒和病毒爆发隔离区](#)
- [使用主配置以集中管理网络安全设备](#)

## 一般故障排除资源

一般故障排除资源包括：

- 最近的警报。请参阅[查看最近的警报](#)。
- 日志文件。请参阅[日志记录](#)
- 版本说明，包括“文档更新”部分。请参阅[文档](#)。
- 思科漏洞搜索工具（有关访问说明，请参阅版本说明）
- [知识库文章（技术说明）](#)
- 这种[思科支持社区](#)

## 特定功能问题的故障排除

另请参阅[功能设置问题故障排除](#) , on page 2。

### 网络安全相关问题

- [对所有报告进行故障排除](#)
- [解决 Web 报告和跟踪问题](#)
- [对配置管理问题进行故障排除](#)
- 网络安全设备上的设置也会导致功能相关的问题。请参阅[文档](#)中指定位置处您所用版本的版本说明和在线帮助或用户指南。

### 邮件安全相关问题

- [对所有报告进行故障排除](#)

- [邮件跟踪故障排除](#)
- [垃圾邮件隔离区功能故障排除](#)
- [排除集中策略隔离区故障](#)
- 邮件安全设备上的设置也会导致功能相关的问题。请参阅[文档](#)中指定位置处您所用版本的版本说明和在线帮助或用户指南。

#### 一般问题

- 如果无法加载配置文件，请确保您的磁盘空间配额超过[管理设备 > 系统管理 > 磁盘管理](#)页面上的表中每项功能的当前大小。
- 如果您最近已升级，并且联机帮助似乎已过时，或者您无法找到有关某项新功能的信息，请清除浏览器缓存，然后重新打开浏览器窗口。
- 在使用网络界面配置设置时，如果您同时使用多个浏览器窗口或选项卡，可能会发生意外行为。
- 请参阅[回应警报 , on page 3](#)。
- 请参阅[管理用户访问故障排除](#)。

## 回应警报

- [警报：380 或 680 硬件上的电池再记忆超时（RAID 活动） , on page 3](#)
- [其他警报说明 , on page 3](#)

### 警报：380 或 680 硬件上的电池再记忆超时（RAID 活动）

问题：您收到关于 380 或 680 硬件的主题为“电池再学习已超时”的警报。

解决方案：此警报可能表示存在问题，也可能不表示存在问题。电池再记忆超时并不意味着 RAID 控制器存在问题。控制器可以在后续的再记忆中恢复。请在接下来的48小时内监控您的邮件是否出现任何其他 RAID 警报，以确保此问题不是其他问题的副作用所致。如果系统中未出现任何其他 RAID 相关的警报，则可以安全地忽略此警报。

### 其他警报说明

有关其他警报的说明，请参阅

- [硬件警报说明](#)
- [系统警报说明](#)

后续操作

- [管理警报](#)

## 使用技术支持

- 从设备提交或更新支持请求, on page 4
- 获取虚拟设备技术支持, on page 4
- 启用思科技术支持人员远程访问, on page 5

## 从设备提交或更新支持请求

您可以使用此方法与思科 TAC 或您自己的支持服务人员联系。

### Before you begin

如果想要联系思科 TAC:

- 如果问题紧急, 请勿使用此方法。请改为使用[客户支持](#)中列出的方法之一与支持人员联系。
- 考虑获取帮助的其他选项:
- 使用此过程创建支持请求时, 系统会将设备配置文件发送给思科客户支持人员。如果您不希望发送设备配置, 可以使用另一种方法联系客户支持部门。
- 设备必须联网并且能够发送邮件。
- 如果您要发送某个现有案例的相关信息, 确保您有案例编号。

**步骤 1** 登录到设备。

**步骤 2** 依次选择帮助和支持 (Help and Support) > 联系技术支持 (Contact Technical Support)。

**步骤 3** 确定支持请求的收件人:

要将发送请求给思科 TAC	选中思科技术支持 (Cisco Technical Support) 复选框。
要仅将请求发送给您的内部支持部门	<ul style="list-style-type: none"> <li>• 取消选中思科技术支持 (Cisco Technical Support) 复选框。</li> <li>• 输入您的支持部门邮件地址。</li> </ul>
(可选) 要包括其他收件人	输入邮件地址。

**步骤 4** 完成表格。

**步骤 5** 点击发送 (Send)。

## 获取虚拟设备技术支持

如果您为思科内容安全虚拟设备提交一个支持请求, 则必须提供您的虚拟许可证号 (VLN)、合同编号和产品标识符代码 (PID)。

您可以根据虚拟设备上运行的软件许可证, 通过参考采购订单或从下表识别 PID。

功能	PID	说明
所有集中网络安全功能	SMA-WMGT-LIC=	—
所有集中邮件安全功能	SMA-EMGT-LIC=	

## 启用思科技术支持人员远程访问

只有思科客户帮助部门才能使用这些方法访问您的设备。

- [启用思科技术支持人员远程访问](#) , on page 5
- [启用对无直接网络连接设备的远程访问](#) , on page 5
- [禁用技术支持隧道](#) , on page 6
- [禁用远程访问](#) , on page 6
- [检查支持连接的状态](#) , on page 6

## 启用对网络连接设备的远程访问

支持部门可通过此过程在设备与 [upgrades.ironport.com](http://upgrades.ironport.com) 服务器之间创建的 SSH 隧道访问设备。

### Before you begin

确定一个可以从互联网访问的端口。默认端口为 [22](#)。大多数防火墙配置都允许通过此端口进行的连接。

---

**步骤 1** 登录到设备。

**步骤 2** 从 GUI 窗口的右上角，依次选择帮助和支持 (**Help and Support**) > 远程访问 (**Remote Access**)。

**步骤 3** 点击启用 (**Enable**)。

**步骤 4** 输入信息。

**步骤 5** 点击提交 (**Submit**)。

---

### What to do next

当不再需要远程访问支持人员时，请参阅[禁用技术支持隧道](#) , on page 6。

## 启用对无直接网络连接设备的远程访问

对于没有直接互联网连接的设备，可以通过连接至互联网的第三台设备进行访问。

### Before you begin

- 设备必须能够通过端口 22 连接到第三台连网设备。

- 在已连接互联网的设备上，按照[启用对网络连接设备的远程访问](#)，on page 5中的程序创建通往该设备的支持隧道。

---

**步骤 1** 在请求支持的设备的命令行界面中，输入 `techsupport` 命令。

**步骤 2** 输入 `sshaccess`。

**步骤 3** 按照提示操作。

---

### What to do next

当不再需要支持人员的远程访问时，请参阅以下内容：

- [禁用远程访问](#)，on page 6
- [禁用技术支持隧道](#)，on page 6

## 禁用技术支持隧道

已启用的 `techsupport` 隧道连续 7 天保持连接到 `upgrades.ironport.com`。7 天之后，建立的连接虽然不会断开，但一旦断开就无法重新连接至该隧道。

---

**步骤 1** 登录到设备。

**步骤 2** 从 GUI 窗口的右上角，依次选择帮助和支持 (**Help and Support**) > 远程访问 (**Remote Access**)。

**步骤 3** 点击禁用 (**Disable**)。

---

## 禁用远程访问

使用 `techsupport` 命令创建的远程访问账户将保持活动状态，直到将其禁用为止。

---

**步骤 1** 在命令行界面中，输入 `techsupport` 命令。

**步骤 2** 输入 `sshaccess`。

**步骤 3** 输入 `disable`。

---

## 检查支持连接的状态

**步骤 1** 在命令行界面中，输入 `techsupport` 命令。

**步骤 2** 输入 `status`。

---

# 运行数据包捕获

数据包捕获允许支持人员查看设备接收和发出的TCP/IP数据及其他数据包。这样，支持人员就可以调试网络设置，并知道哪些网络流量到达该设备或者离开该设备。

**步骤 1** 依次选择帮助和支持 (**Help and Support**) > 数据包捕获 (**Packet Capture**)。

**步骤 2** 指定数据包捕获设置：

- a) 在**数据包捕获设置 (Packet Capture Settings)** 屏幕中，点击**编辑设置 (Edit Settings)**。
- b) (可选) 输入数据包捕获的持续时间、限制和过滤器。

您的支持代表可能会提供这些设置的相关指导。

如果您输入了捕获的持续时间却没有指定时间单位，AsyncOS 默认使用秒。

在“过滤器 (Filters)”部分：

- 自定义过滤器可以使用 UNIX `tcpdump` 命令支持的任何语法，例如 `host 10.10.10.10 && port 80`。
- 客户端 IP 是连接到设备的计算机的 IP 地址，例如通过邮件安全设备发送邮件的邮件客户端。
- 服务器 IP 是指设备连接的计算机（例如设备传送邮件至的 Exchange 服务器）的 IP 地址。

您可以使用客户端和服务器 IP 地址跟踪特定客户端与特定服务器之间的流量，将邮件安全设备置于中间。

- c) 点击**提交 (Submit)**。

**步骤 3** 点击**开始捕获 (Start Capture)**。

- 一次只能运行一个捕获操作。
- 运行数据包捕获时，数据包捕获页面会显示当前统计数据，例如文件大小和逝去的时间，让您能够看到进行中的捕获状态。
- GUI 只显示 GUI 中开始的数据包捕获，而不显示从 CLI 开始的数据包捕获。同样地，CLI 只显示 CLI 中开始的当前数据包捕获的运行状态。
- 数据包捕获文件分为 10 个部分。如果数据包捕获结束前文件到达最大大小限制，那么该文件最早的部分将会被删除（数据丢弃），新的部分从当前的数据包捕获数据开始。一次只能丢弃数据包捕获文件的 1/10。
- 两次会话期间保留 GUI 中开始的正在运行的捕获。（当会话终止时，CLI 中开始的正在运行的捕获会停止。）

**步骤 4** 允许捕获操作运行指定的时间，或者如果您让捕获无限运行，则可以点击**停止捕获 (Stop Capture)**停止捕获。

**步骤 5** 访问数据包捕获文件：

- 在**管理数据包捕获文件 (Manage Packet Capture Files)** 列表中点击该文件，然后点击**下载文件 (Download File)**。
- 使用 FTP 或 SCP 访问设备 `captures` 子目录中的文件。

## What to do next

将该文件提供给支持部门：

- 如果您允许远程访问您的设备，技术人员可以使用 FTP 或 SCP 访问数据包捕获文件。请参阅[启用思科技术支持人员远程访问](#)，on page 5。
- 通过邮件形式将该文件发送给支持部门。

## 远程重置设备电源

如果设备需要硬重置，您可以使用第三方智能平台管理接口 (IPMI) 工具远程重新启动设备机箱。

### 限制

- 远程电源重新启动仅适用于特定硬件。  
有关具体信息，请参阅[启用远程电源循环](#)。
- 如果您希望能够使用此功能，您必须提前启用它。  
有关详细信息，请参阅[启用远程电源循环](#)。
- 仅支持以下 IPMI 命令：

```
status, on, off, cycle, reset, diag, soft
```

发出不支持的命令将导致“权限不足”错误。

### Before you begin

- 使用 IPMI 版本 2.0 获取并设置可用于管理设备的实用程序。
- 了解如何使用受支持的 IPMI 命令。请参阅 IPMI 工具的文档。

---

**步骤 1** 使用 IPMI 向分配到“远程重启”端口（之前配置）的 IP 地址发出支持的电源循环命令，以及所需的凭证。

例如，从支持 IPMI 的 UNIX 类型计算机中可能发出如下命令：

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P passphrase chassis power reset
```

其中，192.0.2.1 是分配到远程电源重新启动端口的 IP 地址，remoteresetuser 和 passphrase 是您在启用此功能时输入的凭证。

**步骤 2** 等待至少十一分钟，以便设备重启。

---



## 当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。