# 代理设备上传



# 代理设备上传

将日志文件中的遥测数据从思科网络安全设备 (WSA) 和 Blue Coat ProxySG 等代理设备上传到全局威胁警报系统以进行分析。

**步骤 1** 点击页面右上角的齿轮图标，然后选择**设备帐户**以打开设置向导。

**注释** 如果已有至少一个现有设备帐户，则跳过设置并显示设备帐户页面。

**步骤 2** 当您准备启动安装向导以添加设备帐户时，请点击**让我们开始吧**。

**步骤 3** 通过从下拉列表中选择自动或手动上传，选择如何从设备上传遥测数据。全局威胁警报系统一次仅支持一种上传方法；不能一起使用这两种方法。

**注释** 要从自动上传切换到手动上传，必须先从自动上传配置中删除所有代理设备。

**步骤 4** 如果选择了自动上传方法，请通过选择 **SCP** 或 **HTTPS** 选择用于传输日志文件的协议。

a) 输入此设备的名称，然后点击**添加帐户**。

b) 如果选择了 SCP：

- 复制信息（主机、端口、目录、用户名），以粘贴到您的思科 WSA 配置中。出于安全原因，信息仅显示一次。
- 有关如何配置思科 WSA 的详细信息，请参阅其配置指南。
- 思科 WSA 管理控制台返回公钥 SSH 后，请将公钥 SSH 复制并粘贴到设备帐户中。
- 点击**完成**。
- 或者，您可以稍后通过导航到设备帐户页面并点击该设备来输入公共 SSH 密钥。

c) 如果选择了 HTTPS：

代理设备上传

- 复制信息（主机、端口、路径、用户名、密码）以粘贴到 Blue Coat ProxySG 配置中。
- 有关如何配置 Blue Coat ProxySG 的详细信息，请参阅其配置指南。
- 点击**完成**。

**步骤 5** 如果您选择手动上传方法：

a) 验证日志文件的格式。遵循这些准备指南：

- 支持由思科 WSA 和 Blue Coat 代理创建的 W3C 日志文件。
- 所有日志文件必须以 GZip (*.gz) 格式压缩。
- 每个日志文件必须小于 1 GB。大于 1 GB 的日志文件应分为多个较小的文件。确保单独的时间间隔不重叠，并且每个文件都包含相同的正确信头。
- 日志文件涵盖的总时间间隔应大于两天。
- 每个日志文件必须具有特定的非重叠时间间隔。
- 每个日志文件必须按升序包含日志条目；较早的条目在较新的条目之前。
- 日志文件应按字母/数字排序，并根据时间顺序上传；较旧的文件应在较新的文件之前上传。在单次上传中，上传组件会自动对文件进行排序。如果上传多次，请确保始终上传比以前更新的数据。如果保留代理日志文件中默认使用的命名约定，则文件名已正确排序。
- 将不会处理早于之前上传的数据的数据。
- 日志文件的内容必须与某些条件匹配才能有效上传。
  - 我们为您提供日志验证工具，用于在上传之前检查您的日志文件。
  - 将日志文件的前 20 行复制并粘贴到日志验证工具中，以检查是否存在错误。
  - 系统会显示任何错误，并且在您纠正错误后，该工具将自动继续检查是否存在错误。

b) 点击**添加文件**以选择要上传的日志文件，或将日志文件拖放到上传框中。

**注释** 点击**清除文件**以清除添加到上传框中的所有文件。

c) 点击**开始上传**会将所选日志文件上传到全局威胁警报系统以进行分析。允许全局威胁警报系统在查看到结果之前等待一段时间。

**注释** 为了最大限度地降低数据丢失的风险，全局威胁警报系统会在 5 小时后开始处理上传的数据。这使您有时间完成所有上传操作，并确保在数据处理开始之前一切就绪且顺序正确。

**注意** 尝试从手动上传切换到自动上传会立即中止所有上传并停止处理已上传的数据。所有上传的数据都将被丢弃。

**注释** 关闭页面或导航离开页面将停止任何当前文件上传。

**注释** 除非先停止所有手动上传，否则您无法使用自动上传。如果在处理完所有数据之前便进行切换，则转换过程中可能会丢失一些分析数据。为确保系统不丢失任何数据，请在上次手动上传 24 小时后执行切换。

### 下一步做什么

“设备帐户”页面列出代理设备及其信息。“状态”列显示每个设备的状态：

- 新建—SCP 的配置不完整，可能缺少公共 SSH 密钥
- 调配—正在调配的帐户，尚未准备就绪
- 就绪—已成功创建帐户
- 错误—将光标悬停在状态上以显示解释错误的弹出消息

在此概述页面中，您可以添加更多设备帐户，或者点击任意设备将其删除，输入公共 SSH 密钥或进行故障排除。

虽然可以在多个设备或上传流程之间共享帐户，但我们建议您为每个设备使用单独的帐户，以最大程度地减少文件名冲突的可能性，并简化上传问题的故障排除。

一旦您的设备帐户准备就绪，点击以查看**已确认**或**已检测**页面，以了解网络中的任何可疑活动。

**注释** 数据通常在调配完成后两到三天内可用。

代理设备上传