



## 使用外部工具的事件分析

- [与思科 SecureX集成](#)，第 1 页
- [使用的事件分析 SecureX 威胁响应](#)，第 9 页
- [使用基于 Web 的资源的事件调查](#)，第 9 页
- [配置交叉启动链接 Secure Network Analytics](#)，第 12 页
- [关于发送 安全事件的系统日志消息](#)，第 13 页
- [eStreamer 服务器流传输](#)，第 26 页
- [Splunk 中的事件分析](#)，第 29 页
- [IBM QRadar 中的事件分析](#)，第 30 页
- [使用外部工具分析事件数据的历史记录](#)，第 30 页

## 与思科 SecureX集成

通过单一管理平台（SecureX 云门户）查看和处理所有思科安全产品及其他产品的数据。使用 SecureX 可用的工具来丰富您的威胁追踪和调查。SecureX 还可以提供有用的设备和设备信息，例如每个设备和设备是否正在运行最佳软件版本。

有关 SecureX 的详细信息，请参阅[思科 SecureX \(Cisco SecureX\)](#) 页面。

## 启用 SecureX 集成

思科 SecureX 结合了思科的集成安全产品组合以及您的基础设施的优势，旨在提供可统一可视性、实现自动化并增强网络、终端、云和应用安全性的一致体验。有关 SecureX 的详细信息，请参阅[思科 SecureX \(Cisco SecureX\)](#) 产品页面。

通过将 SecureX 与管理中心集成，您可以全面了解管理中心中的所有数据。有关将管理中心与 SecureX 集成的更多信息，请参阅[Cisco Secure Firewall Management Center \(版本 7.2 或更高\)](#) 和 [SecureX 集成指南](#)。

### 开始之前

您需要一个属于组织的 SecureX 帐户。

## 过程

**步骤 1** 在管理中心中，选择集成 (Integration) > SecureX。

**步骤 2** (可选) 对于云区域 (Cloud Region)，请选择您的当前区域 (Current Region)。

默认情况下，选择的区域与您的智能许可区域匹配，因此您可能无需更改区域。

**步骤 3** 在 SecureX 启用中，执行以下步骤。

a) 点击启用 SecureX (Enable SecureX)。

图 1: 启用 SecureX

### SecureX Setup

This feature allows Secure Firewall Management Center to integrate with other SecureX services via SecureX ribbon. [Learn more](#)

① Cloud Region

This setting determines where events are sent to, if configured to send to the cloud, as well as data generated by the Cisco Success Network and Cisco Support Diagnostics tools.

Current Region

② SecureX Enablement

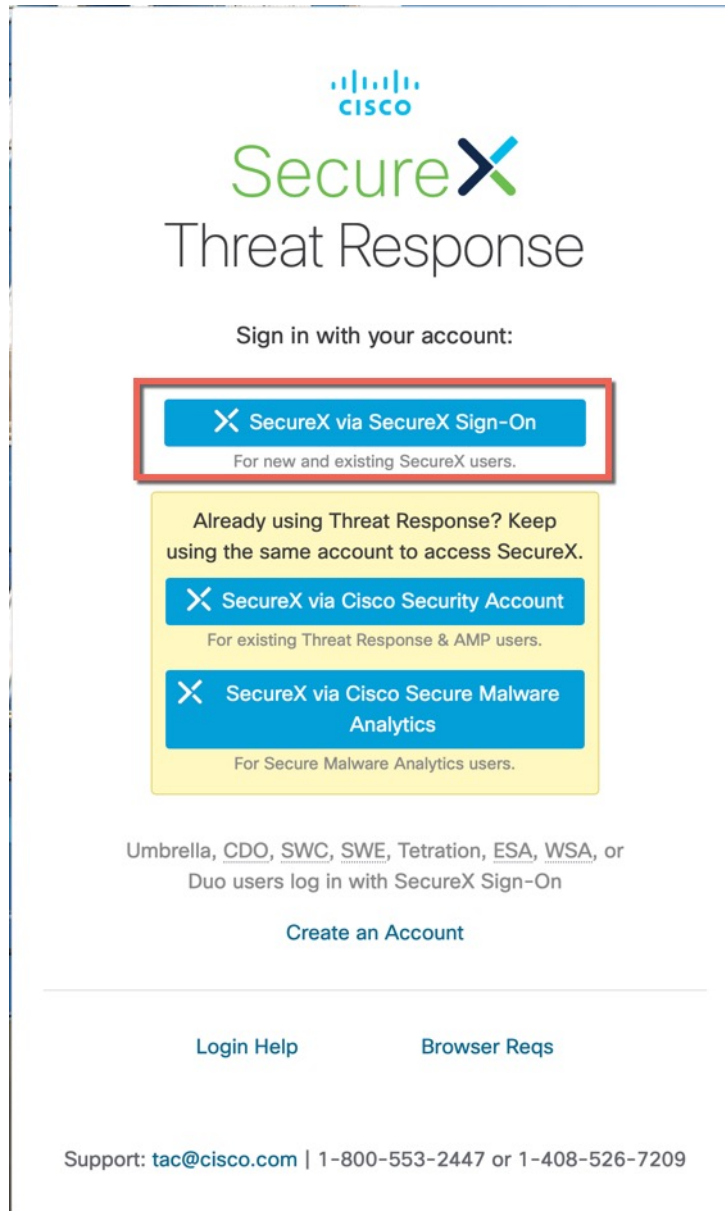
After completing this configuration, the SecureX ribbon will show up at the bottom of each page. [Learn more](#)

[Enable SecureX](#)

b) 登录 SecureX。

系统将打开一个单独的浏览器选项卡或窗口，以供您登录 SecureX 帐户。确保此页面未被弹出窗口阻止程序阻止。

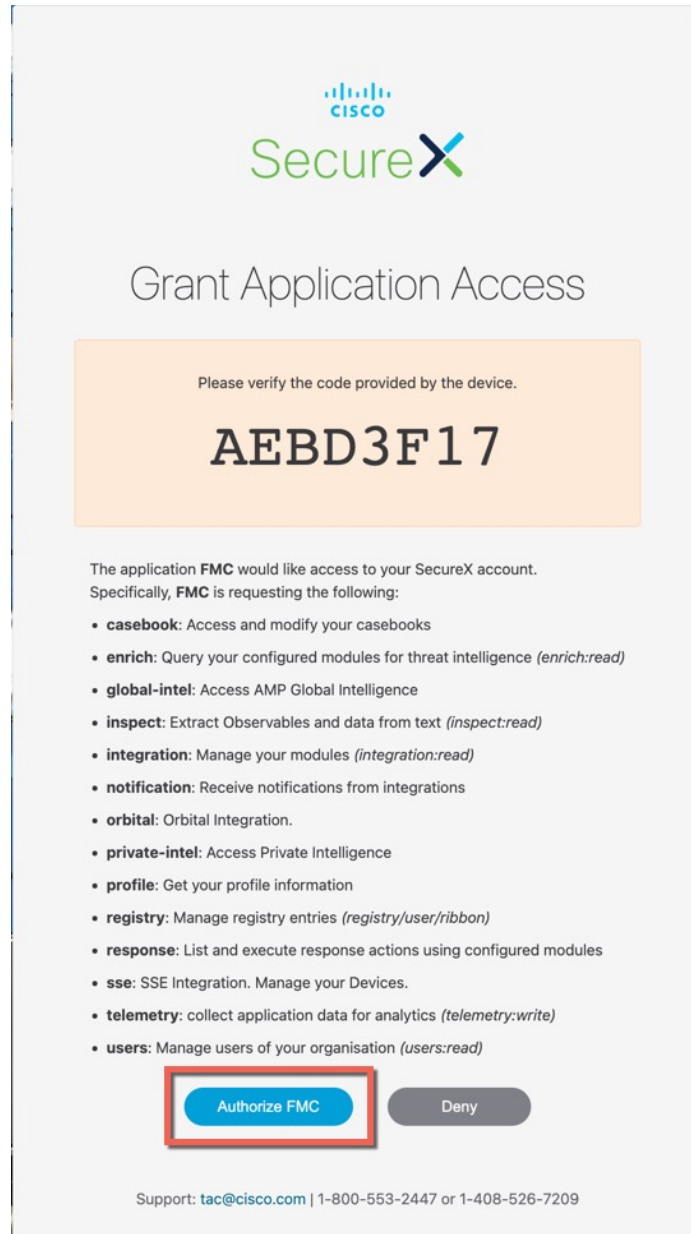
图 2: SecureX 登录



c) 点击授权 **FMC (Authorize FMC)**。

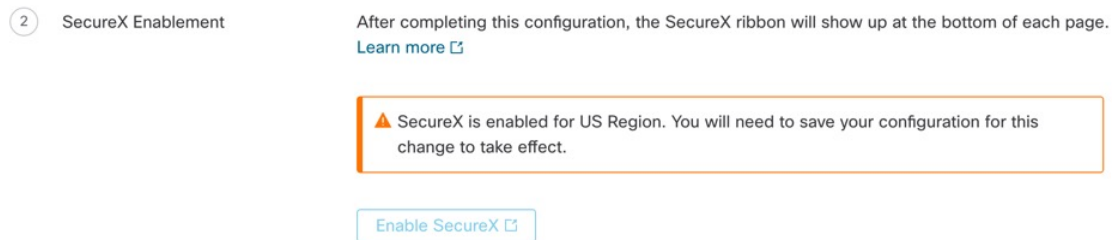
您将看到一个代码，该代码应与管理中心中显示的代码匹配。

图 3: 授予应用访问权限



d) 在管理中心与 SecureX 集成后，您会看到一条成功消息。点击**保存 (Save)**。

图 4: 成功消息



## 配置 管理中心 设备以将事件发送到思科云

将 管理中心 配置为受管 威胁防御 设备直接将事件发送至云。在适用和启用的情况下，您在此页面中配置的云区域和事件类型可用于多个集成。

### 开始之前

- 在 管理中心 中：
  - 转至 **系统 > 配置** 页面并为 管理中心 提供唯一名称，以便其可在云中的“设备”列表中明确识别。
  - 将您的 威胁防御 设备添加到 管理中心，向其分配许可证，并确保系统正常运行。确保您已创建必要的策略，生成的事件如在 管理中心 web 接口中的 **分析** 选项卡下如预期那样显示。
- 请确保您拥有云凭证，并且可以登录到创建您的账户的 SecureX 区域云。  
有关 SecureX 区域云 URL 和支持的设备版本的详细信息，请参阅 [思科 Cisco Secure Firewall Management Center](#) 和 [SecureX集成指南](#)。
- 如果您当前使用系统日志将事件发送到云，请禁用这些发送以避免重复。

### 过程

**步骤 1** 确定要用于发送防火墙事件的思科区域云。有关选择区域云的详细信息，请参阅 [思科 Cisco Secure Firewall Management Center](#) 和 [SecureX 集成指南](#)。

**注释** 如果 SecureX 已启用，并且 管理中心 已注册到所选区域云，则更改区域云会禁用 SecureX。您可以在更改区域云后再次启用 SecureX。

**步骤 2** 在您的 管理中心，转至 **集成 > SecureX**。

**步骤 3** 从 **当前区域** 下拉列表中选择区域云。

**步骤 4** 启用思科云事件配置，并选择要发送到云的事件类型。

1. 选中 **将事件发送到云** 复选框以启用配置。
2. 选择要发送至云的事件类型。

注释 发送到云的事件可用于多个集成。请参阅下表：

集成	受支持的事件选项	备注
思科安全分析和日志记录 (SaaS)	全部	高优先级连接事件包括： <ul style="list-style-type: none"> <li>• 安全相关 连接事件</li> <li>• 与文件和恶意软件事件相关的连接事件</li> <li>• 与入侵事件相关的连接事件</li> </ul>
思科 SecureX 和 思科 SecureX 威胁响应	取决于您的版本： <ul style="list-style-type: none"> <li>• 一些连接事件</li> <li>• 入侵</li> <li>• 文件和恶意软件事件</li> </ul>	如果发送所有连接事件，思科 SecureX 和 思科 SecureX 威胁响应 仅支持安全事件。

- 注释
- 如果 启用入侵事件， 管理中心 设备会随影响标志一起发送事件。
  - 如果启用 文件和恶意软件事件，除了从 威胁防御 设备发送的事件外， 管理中心 设备还会发送追溯性事件。

**步骤 5** 单击保存。

## 配置思科成功网络注册

思科成功网络是一项用户启用的云服务。启用思科成功网络时，管理中心与思科云之间会建立安全连接以传输使用情况信息和统计信息。此数据流遥测提供一种机制，可从威胁防御选择相关数据，并以结构化的格式将其传输至远程管理站，从而获得以下优势：

- 通知您在网络中可用来改进产品效果的未使用功能。
- 通知您适用于您产品的其他技术支持服务和监控。
- （如果与 SecureX 集成）在 SecureX 磁贴中汇总设备和设备状态，并了解所有设备是否都在运行最佳软件版本。
- 帮助思科改善我们的产品。

要了解有关思科收集的遥测数据的更多信息，请参阅 [从 Cisco Secure Firewall Management Center 设备收集的 Cisco 成功网络遥测数据](#)。

当您启用思科支持诊断或思科成功网络时，管理中心会始终建立并维护与思科云的安全连接。您可以随时通过禁用思科成功网络和思科支持诊断功能来关闭该连接，这样会将管理中心与思科云断开。但是，当您启用思科支持诊断时，管理中心和威胁防御都会建立并维护与思科云的安全连接。

将管理中心注册到智能软件管理器时，可启用思科成功网络。使用以下程序查看或更改注册状态。



注释 思科成功网络在评估模式下无法工作。



注释 如果管理中心具有有效的智能软件管理器本地版（之前称为智能软件卫星服务器）配置，或者使用特定许可证预留，则思科成功网络功能将被禁用。

## 过程

**步骤 1** 点击**集成 (Integration) > SecureX**。

**步骤 2** 在**思科云支持 (Cisco Cloud Support)** 下，选中**启用思科成功网络 (Enable Cisco Success Network)** 复选框以启用此服务。

注释 在继续之前，请阅读**启用思科成功网络 (Enable Cisco Success Network)** 复选框旁边提供的信息。

**步骤 3** 单击**保存**。

## 下一步做什么

如果您已启用思科支持诊断，请点击**集成 (Integration) > SecureX** 并验证**云区域 (Cloud Region)** 下的区域云设置。

# 配置思科支持诊断注册

思科支持诊断是一项用户启用的基于云的 TAC 支持服务。启用后，管理中心和托管设备会与思科云建立安全连接，以传输与系统运行状况相关的信息。

思科支持诊断通过允许思科 TAC 在 TAC 案例期间从您的设备安全地收集重要数据，在故障排除期间提供增强的用户体验。此外，思科会定期收集运行状况数据，并使用自动问题检测系统处理数据，以通知您任何问题。虽然 TAC 案例期间的数据收集服务适用于拥有支持合同的所有用户，但通知服务仅适用于拥有特定服务合同的用户。

当您启用思科支持诊断或思科成功网络时，管理中心会建立并维护与思科云的安全连接。您可以随时通过禁用思科成功网络和思科支持诊断功能来关闭该连接，这样会将这些功能与思科云断开。但是，当您启用思科支持诊断时，和会建立并维护与思科云的安全连接。威胁防御管理中心

管理员可以按照 [为特定系统功能生成故障排除文件](#) 中的步骤来查看从管理中心收集的简单数据集。

管理中心 将收集的数据发送到 **集成 > SecureX** 页面上的 **当前区域** 下拉列表下选择的区域云。

将管理中心注册到智能软件管理器时，您就会启用思科成功网络。可以使用以下程序来查看或更改思科支持诊断注册状态。

### 过程

---

**步骤 1** 点击 **集成 > SecureX**。

**步骤 2** 在 思科云支持下，选中 **启用思科支持诊断** 复选框以启用此服务。

**注释** 在继续之前，请参阅 **启用思科支持诊断** 复选框旁边提供的信息。

**步骤 3** 单击保存。

---

### 下一步做什么

如果您已启用思科支持诊断，请点击**集成 (Integration) > SecureX** 并验证云区域 (**Cloud Region**) 下的区域云设置。

## 使用 Ribbon 访问 SecureX

功能区显示在管理中心 Web 界面中每个页面的底部。您可以使用功能区快速跳转到其他思科安全产品，并处理来自多个来源的威胁数据。

### 开始之前

- 如果在 管理中心 Web 界面页面的底部没有看到 SecureX 功能区，请不要使用此程序。相反，请参阅 [Cisco Secure Firewall Threat Defense](#) 和 [SecureX 集成指南](#)。
- 如果您还没有 SecureX 账户，请从您的 IT 部门获取一个。

### 过程

---

**步骤 1** 在 管理中心中，点击任何 管理中心 页面底部的功能区。

**步骤 2** 点击 **获取 SecureX**。

**步骤 3** 登录到 SecureX。

**步骤 4** 点击链接以授权访问。

**步骤 5** 点击功能区以展开并使用它。

---



### 下一步做什么

有关功能区功能及其使用方法的信息，请参阅 SecureX 中的在线帮助。

## 使用的事件分析 **SecureX** 威胁响应

SecureX 威胁响应 以前称为思科威胁响应 (CTR)。

使用思科云中的集成平台 SecureX 威胁响应可快速检测、调查和响应威胁，让您可以使用从多个产品汇聚的数据分析事件，包括 Cisco Secure Firewall。

- 有关 SecureX 威胁响应的一般信息，请参阅：  
[思科 SecureX 威胁响应产品页面](#)。
- 有关将 SecureX 威胁响应到集成 Firepower 的详细说明，请参阅：
- 请参阅 [Cisco Secure Firewall Threat Defense](#) 和 [思科 SecureX 集成指南](#)。

## 查看 **SecureX** 威胁响应中的事件数据

### 开始之前

- 按照 [Cisco Secure Firewall Threat Defense](#) 和 [思科 SecureX 威胁响应集成指南](#) 中的说明设置集成。
- 查看 SecureX 威胁响应 中的联机帮助，了解如何查找、调查威胁并对其采取措施。
- 您将需要您的凭证才能访问 SecureX 威胁响应。

### 过程

---

**步骤 1** 在 Cisco Secure Firewall Management Center 中，执行以下操作：

- 要从特定事件跳转到 SecureX 威胁响应，请执行以下操作：
  - a. 导航到分析 > 入侵菜单下列出受支持事件的页面。
  - b. 右键单击源或目标 IP 地址，然后选择在 **SecureX** 中查看。

**步骤 2** 按提示登录到 SecureX 威胁响应。

---

## 使用基于 **Web** 的资源的事件调查

使用上下文交叉启动功能可在 Cisco Secure Firewall Management Center 以外快速查找有关基于 Web 的资源中的潜在威胁的更多信息。例如，您可以：

- 在思科或第三方云托管服务中查找可疑源 IP 地址，所述服务发布有关已知和可疑威胁的信息；或
- 在您组织的历史日志中查找特定威胁的以往实例，前提是您的组织将这些数据存储在安全信息和事件管理 (SIEM) 应用中。
- 查找有关特定文件的信息（包括文件轨迹信息），前提是您的组织已部署思科面向终端的 AMP。

调查事件时，您可以直接从 Cisco Secure Firewall Management Center 中的事件查看器或控制面板中点击某个事件以转到外部资源中的相关信息。这样，您可以根据 IP 地址、端口、协议、域和/或 SHA 256 散列值快速收集有关特定事件的背景信息。

例如，假设您正在查看“排名靠前的攻击者”控制面板构件，并希望查找有关其中一个所列源 IP 地址的更多信息。您想要查看 Talos 发布了哪些有关此 IP 地址的信息，因此您选择“Talos IP”资源。Talos 网站将打开一个页面，其中包含有关此特定 IP 地址的信息。

您可以从一组预定义的常用思科和第三方威胁情报服务的链接中进行选择，并可以添加指向其他基于 Web 的服务的自定义链接，以及指向 SIEM 或其他具有 Web 界面的产品的自定义链接。请注意，某些资源可能需要拥有账户或购买产品。

## 关于管理上下文交叉启动资源

使用分析 > 高级 > 上下文交叉启动页面管理基于 Web 的外部资源。

**例外：**按照 [配置交叉启动链接 Secure Network Analytics](#)，第 12 页中的程序管理 Secure Network Analytics 设备的交叉启动链路。

思科提供的预定义资源标注有思科徽标。其余链接是第三方资源。

您可以禁用或删除任何不需要的资源，也可以重命名这些资源，例如通过在名称前面加上小写“z”，这样这些资源便排序在列表底部。禁用交叉启动资源将对所有用户禁用。您无法恢复已删除的资源，但可以重新创建这些资源。

要添加资源，请参阅[添加上下文交叉启动资源](#)，第 11 页。

## 自定义上下文交叉启动资源的要求

添加自定义上下文交叉启动资源时：

- 资源必须可通过网络浏览器访问。
- 仅支持 http 和 https 协议。
- 仅支持 GET 请求；不支持 POST 请求。
- 不支持在 URL 中编码变量。虽然 IPv6 地址可能需要编码冒号分隔符，但大多数服务都不需要这种编码。
- 最多可以配置 100 个资源，包括预定义的资源。
- 您必须是 管理员 或 安全分析师 用户才能创建交叉启动，但也可以是只读 安全分析师 才能使用它们。

## 添加上下文交叉启动资源

您可以添加上下文交叉启动资源，例如威胁情报服务以及安全信息和事件管理 (SIEM) 工具。

在多域部署中，您可以在父域中查看和使用资源，但您只能在当前域中创建和编辑资源。所有域中的资源总数限制为 100。

### 开始之前

- 如果要向 Secure Network Analytics 设备添加链路，请检查所需的链路是否已存在；配置安全分析和日志记录（本地部署）时，系统会自动为您创建大多数链路。
- 请参阅[自定义上下文交叉启动资源的要求](#)，第 10 页。
- 如果将链接到的资源需要，请创建或获取账户以及访问所需的凭证。或者，为每个需要访问权限的用户分配和分发凭证。
- 确定您将链接到的资源的查询链接的语法：

通过浏览器访问资源，并根据需要使用该资源的文档来编制查询链接，搜索您希望查询链接查找的信息类型的特定示例需要此查询链接，例如 IP 地址。

运行查询，然后从浏览器的位置栏复制生成的 URL。

例如，查询的 URL 可能为：

```
https://www.talosintelligence.com/reputation_center/lookup?search=10.10.10.10。
```

### 过程

**步骤 1** 选择分析 > 高级 > 上下文交叉启动。

**步骤 2** 点击新建交叉启动。

在显示的表单中，所有标记星号的字段必须填写值。

**步骤 3** 输入唯一的资源名称。

**步骤 4** 将资源中的有效 URL 字符串粘贴到 **URL 模板** 字段中。

**步骤 5** 使用适当的变量替换查询字符串中的特定数据（例如 IP 地址）：将光标置于相应位置，然后点击变量（例如，**ip**）一次以插入变量。

在上方“开始之前”部分中的示例中，生成的 URL 可能是：

```
https://www.talosintelligence.com/reputation_center/lookup?search={ip}。
```

使用上下文交叉启动链接时，URL 中的 {ip} 变量将替换为用户在事件查看器或控制面板中右键单击的 IP 地址。

要查看每个变量的说明，请将鼠标悬停在变量上。

您可以为单个工具或服务创建多个上下文交叉启动链接，为每个链接使用不同的变量。

**步骤 6** 点击 **使用示例数据测试** (🔄) 以使用示例数据测试您的链接。

步骤 7 修复任何问题。

步骤 8 单击保存。

---

## 使用上下文交叉启动调查事件

### 开始之前

如果您将访问的资源需要凭证，请确保您具有这些凭证。

### 过程

---

步骤 1 导航到 Cisco Secure Firewall Management Center 中显示事件的以下其中一个页面：

- 控制面板（概述 > 控制面板），或
- 事件查看器页面（分析菜单下包括事件表的任何菜单选项。）

步骤 2 右键单击感兴趣的事件，然后选择要使用的上下文交叉启动资源。

如有必要，在上下文菜单中向下滚动以查看所有可用选项。

右键单击的数据类型决定了您可看到的选项；例如，如果您右键单击 IP 地址，则只能看到与 IP 地址相关的上下文交叉启动选项。

因此，例如，要从思科 Talos 获取有关“排名靠前的攻击者”控制面板构件中的源 IP 地址的威胁情报，请选择 **Talos SrcIP** 或 **Talos IP**。

如果资源包括多个变量，则用于选择该资源的选项仅适用于对于每个包含的变量只有单个可能值的事件。

上下文交叉启动资源将在单独的浏览器窗口中打开。

处理查询可能需要一些时间，具体取决于待查询的数据量、资源的速度和需求等。

步骤 3 必要时登录资源。

---

## 配置交叉启动链接 Secure Network Analytics

您还可以从 Firepower 中的事件交叉启动，以查看 Secure Network Analytics 设备上的相关数据。有关 Secure Network Analytics 产品的详细信息，请参阅 <https://www.cisco.com/c/en/us/products/security/security-analytics-logging/index.html>。

有关上下文交叉启动的一般信息，请参阅 [使用上下文交叉启动调查事件](#)，第 12 页。

使用此程序可快速配置一组指向 Secure Network Analytics 设备的交叉启动链路。

**注释**

- 如果稍后需要对这些链接进行更改，请返回到此程序；您无法直接在上下文交叉启动列表页面上进行更改。
- 您可以使用 [添加上下文交叉启动资源](#)，第 11 页中的程序手动创建其他链接以交叉启动到 Secure Network Analytics 设备中，但这些链接将独立于自动创建的资源，因此需要手动管理（删除、更新等）

**开始之前**

您必须部署并运行 Secure Network Analytics 设备。

如果要使用 安全分析和日志记录（本地部署）将 Firepower 数据发送到 Secure Network Analytics 设备，请参阅 [Secure Network Analytics 设备上的远程数据存储](#)。

**过程**

**步骤 1** 选择 系统 > 日志记录 > 安全分析和日志记录。

**步骤 2** 启用此功能。

**步骤 3** 输入 Secure Network Analytics 设备的主机名或 IP 地址和端口。

默认端口为 443。

**步骤 4** 单击保存 (Save)。

**步骤 5** 验证新的交叉启动链接：选择 分析 > 高级 > 上下文交叉启动。

如果需要进行更改，请返回此程序；您无法直接在上下文交叉启动列表页面上进行更改。

**下一步做什么**

要从事件交叉启动到 Secure Network Analytics 事件查看器，您将需要 Secure Network Analytics 凭证。

要从管理中心事件查看器或控制面板中的事件交叉启动，请右键单击相关事件的表格单元格，然后选择相应的选项。

处理查询可能需要一些时间，具体取决于 Cisco Secure Network Analytics 管理器上的待查询的数据量、资源的速度和需求等。

## 关于发送 安全事件的系统日志消息

您可以通过系统日志将与连接、安全情报、入侵以及文件和恶意软件事件相关的数据发送到安全信息和事件管理 (SIEM) 工具或其他外部事件存储和管理解决方案，例如。

这些事件有时也称为 Snort® 事件。

## 关于配置系统以向系统日志发送安全事件数据

为了配置系统以发送安全事件系统日志，您需要了解以下内容：

- [配置安全事件系统日志消息的最佳实践，第 14 页](#)
- [安全事件系统日志的配置位置，第 18 页](#)
- 在《[Cisco Secure Firewall Management Center 设备配置指南](#)》中的适用于安全事件系统日志消息的 *FTD* 平台设置
- 如果在任何策略中更改系统日志设置，则必须重新部署才能使更改生效。

### 配置安全事件系统日志消息的最佳实践

设备和版本	配置位置
所有 (All)	如果您要使用 <code>syslog</code> 或在外部存储事件，请避免在对象名称（例如策略和规则名称）中使用特殊字符。对象名称不应包含特殊字符（例如逗号），接收名称的应用可能将其用作分隔符。
Cisco Secure Firewall Threat Defense	<ol style="list-style-type: none"> <li>1. 配置 FTD 平台设置（设备 &gt; 平台设置 &gt; 威胁防御设置 &gt; 系统日志。） 也请参阅《<a href="#">Cisco Secure Firewall Management Center 设备配置指南</a>》中的适用于安全事件系统日志消息的 <i>FTD</i> 平台设置。</li> <li>2. 在访问控制策略“日志记录”选项卡中，选择使用 FTD 平台设置。</li> <li>3. （对于入侵事件）将入侵策略配置为使用访问控制策略“日志记录”选项卡中的设置。（这是默认。）</li> </ol> <p>不建议覆盖其中任何设置。</p> <p>有关基本信息，请参阅 <a href="#">从威胁防御设备发送安全事件系统日志消息，第 14 页</a>。</p>
所有其他设备	<ol style="list-style-type: none"> <li>1. 创建警报响应</li> <li>2. 配置访问控制策略日志记录以使用警报响应。</li> <li>3. （对于入侵事件）在入侵策略中配置系统日志设置。</li> </ol> <p>有关完整的详细信息，请参阅 <a href="#">从经典设备发送安全事件系统日志消息，第 17 页</a>。</p>

### 从威胁防御设备发送安全事件系统日志消息

此程序记录从威胁防御管理的 Cisco Secure Firewall Management Center 设备。



注释 许多威胁防御系统日志设置不适用于安全事件。仅配置此程序中所述的选项。

### 开始之前

- 在 Cisco Secure Firewall Management Center 中，配置策略以生成安全事件，并验证您希望看到的事件显示在“分析”菜单下的适用表中。
- 收集系统日志服务器 IP 地址，端口和协议（UDP 或 TCP）：
- 确保您的设备可以访问系统日志服务器。
- 确认系统日志服务器可接受远程消息。
- 有关连接日志的重要信息，请参阅 [连接日志记录](#) 的章节。

### 过程

**步骤 1** 为威胁防御设备配置系统日志设置：

- a) 点击 **设备 > 平台设置**。
- b) **编辑** 与威胁防御设备关联的平台设置策略。
- c) 在左侧导航窗格中，点击 **系统日志**。
- d) 点击 **系统日志服务器 (Syslog Servers)**，然后点击 **添加 (+)** 以输入服务器、协议、接口和相关信息。

如果您对此页面上的选项有任何疑问，请参阅 [《Cisco Secure Firewall Management Center 设备配置指南》](#)。


- e) 点击 **系统日志设置** 并配置以下设置：
  - 在系统日志消息中启用时间戳
  - 时间戳格式
  - 启用系统日志设备 ID
- f) 点击 **日志记录设置**。
- g) 在 **基本日志记录设置 (Basic Logging Settings)** 中，选择是否要以 **EMBLEM** 格式发送系统日志 (**Send syslogs in EMBLEM format**)。
- h) 点击 **保存 (Save)** 以保存您的设置。

**步骤 2** 配置访问控制策略的常规日志记录设置（包括文件和恶意软件日志记录）：

- a) 点击 **策略 (Policies) > 访问控制 (Access Control)**。
- b) 编辑适用的访问控制策略。
- c) 点击 **更多 (More) > 日志记录 (Logging)**。

- d) 威胁防御 6.3 及更高版本：选择使用在设备上部署的威胁防御平台设置策略中配置的系统日志设置。
- e) （可选）选择 **系统日志严重性**。
- f) 如果要发送文件和恶意软件事件，选择为文件和恶意软件事件发送系统日志消息 (**Send Syslog messages for File and Malware events**)。
- g) 点击 **保存 (Save)**。

**步骤 3** 为访问控制策略启用安全情报事件日志记录：

- a) 在同一访问控制策略中，点击 **安全情报** 选项卡。
- b) 在以下每个位置，点击 **日志记录** (  ) 并启用连接的开始和结束和 **系统日志服务器**：
  - 在 **DNS 策略** 旁边。
  - 在 **阻止列表** 框中，对于 **网络** 和对于 **URL**。
- c) 点击 **保存 (Save)**。

**步骤 4** 为访问控制策略中的每个规则启用系统日志记录：

- a) 在同一访问控制策略中，点击 **访问控制 (Access Control) > 添加规则 (Add Rule)**。
- b) 选择一条规则进行编辑。
- c) 点击规则中的 **日志记录 (Logging)** 选项卡。
- d) 选择是记录连接的开始还是结束，或者同时选择两者。  
(连接日志记录会生成大量数据；记录开始和结束时会生成大约两倍的数据。并非在开始和结束时都可以记录每个连接。)
- e) 如果要记录文件事件，请选择 **日志文件 (Log Files)**。
- f) 启用 **系统日志服务器**。
- g) 验证规则是“在访问控制日志记录中使用默认系统日志配置”。
- h) 点击 **Confirm**。
- i) 对策略中的每个规则重复上述步骤。

**步骤 5** 如果发送入侵事件：

- a) 导航至与访问控制策略关联的入侵策略。
- b) 在入侵策略中，点击 **高级设置 > 系统日志警报 > 已启用**。
- c) 如有必要，请点击 **编辑**
- d) 输入选项：

选项	值
日志记录主机	除非将入侵事件系统日志消息发送到与其他系统日志消息不同的系统日志服务器，否则将此字段留空以使用您在上一步配置的设置。
设施	仅当您在此页面上指定日志记录主机时，此设置才适用。 有关说明，请参阅 <a href="#">系统日志警报设施</a> 。



选项	值
严重性	仅当您在此页面上指定日志记录主机时，此设置才适用。 有关说明，请参阅 <a href="#">系统日志严重性级别</a> 。

- e) 点击 **Back**（返回）。
- f) 点击左侧导航窗格中 **策略信息**。
- g) 点击**确认更改 (Commit Changes)**。

### 下一步做什么

- （可选）为单个策略和规则配置不同的日志记录设置。

请参阅 管理中心 联机帮助中 [连接和安全情报事件系统日志的配置位置（所有设备）](#)，第 19 页。

这些设置需要系统日志警报响应，其配置如 [创建系统日志警报响应](#)中所述。它们不使用您在此程序中配置的平台设置。

- 要配置典型设备的安全事件系统日志记录，请参阅 [从经典设备发送安全事件系统日志消息](#)，第 17 页。
- 如果完成更改，请将更改部署到受管设备。

## 从经典设备发送安全事件系统日志消息

### 开始之前

- 配置策略以生成安全事件。
- 确保您的设备可以访问系统日志服务器。
- 确认系统日志服务器可接受远程消息。
- 有关连接日志的重要信息，请参阅 [连接日志记录](#)的章节。

### 过程

**步骤 1** 为经典设备配置警报响应：

请参阅[创建系统日志警报响应](#)。

**步骤 2** 在访问控制策略中配置系统日志设置：

- a) 点击 **策略 (Policies) > 访问控制 (Access Control)**。
- b) 编辑适用的访问控制策略。
- c) 点击 **日志记录**。

- d) 选择 **使用特定系统日志警报发送**。
- e) 选择您在上面创建的 **系统日志警报**。
- f) 点击 **保存 (Save)**。

**步骤 3** 如果您将发送文件和恶意软件事件：

- a) 选择 **发送文件和恶意软件事件**的系统日志消息。
- b) 点击 **保存 (Save)**。

**步骤 4** 如果您将发送入侵事件：

- a) 导航至与访问控制策略关联的入侵策略。
- b) 在入侵策略中，点击 **高级设置 > 系统日志警报 > 已启用**。
- c) 如有必要，请点击 **编辑**
- d) 输入选项：

选项	值
日志记录主机	除非将入侵事件系统日志消息发送到与其他系统日志消息不同的系统日志服务器，否则将此字段留空以使用您在上一步配置的设置。
设施	仅当您在此页面上指定日志记录主机时，此设置才适用。 请参阅 <a href="#">系统日志警报设施</a> 。
严重性	仅当您在此页面上指定日志记录主机时，此设置才适用。 请参阅 <a href="#">系统日志严重性级别</a> 。

- e) 点击 **Back (返回)**。
- f) 点击左侧导航窗格中 **策略信息**。
- g) 点击 **确认更改 (Commit Changes)**。

#### 下一步做什么

- (可选) 为各个访问控制规则配置不同的日志记录设置。请参阅 [连接和安全情报事件系统日志的配置位置 \(所有设备\)](#)，第 19 页中适用的表行。这些设置需要系统日志警报响应，其配置如 [创建系统日志警报响应](#) 中所述。它们不使用您上面配置的设置。
- 要为 FTD 设备配置安全事件系统日志记录，请参阅 [从威胁防御设备发送安全事件系统日志消息](#)，第 14 页。

## 安全事件系统日志的配置位置

- [连接和安全情报事件系统日志的配置位置 \(所有设备\)](#)，第 19 页
- [入侵事件系统日志的配置位置 \(FTD 设备\)](#)，第 20 页
- [入侵事件系统日志的配置位置 \(非 FTD 设备\)](#)，第 21 页

- [文件和恶意软件事件系统日志的配置位置，第 21 页](#)

## 连接和安全情报事件系统日志的配置位置（所有设备）

有许多位置可配置日志记录设置。使用下表来确保设置所需的选项。



### 重要事项

- 配置系统日志设置时，尤其是在使用其他配置的继承默认设置时要特别注意。某些选项可能无法用于所有受管设备型号和软件版本，如下表所示。
- 有关配置连接日志记录的重要信息，请参阅[连接日志记录](#)一章。

配置位置	说明和更多信息
设备 > 平台设置，威胁防御设置策略，系统日志	<p>此选项仅适用于 威胁防御 设备。</p> <p>您在此处配置的设置可以在访问控制策略的日志记录设置中指定，然后在此表的其余策略和规则中使用或覆盖。</p> <p>请参阅 <a href="#">《Cisco Secure Firewall Management Center 设备配置指南》</a>。</p>
策略 > 访问控制，<每个策略>，日志记录	<p>您在此处配置的设置是所有连接和安全情报事件的系统日志的默认设置，除非您在此表的其余行中指定的位置处覆盖后代策略和规则中的默认设置。</p> <p>威胁防御设备的建议设置：使用威胁防御平台设置。有关信息，请参阅 <a href="#">《Cisco Secure Firewall Management Center 设备配置指南》</a>。</p> <p>所有其他设备的必需设置：使用系统日志警报。</p> <p>如果您指定系统日志警报，请参阅<a href="#">创建系统日志警报响应</a>。</p> <p>有关“日志记录”选项卡上的设置的详细信息，请参阅 <a href="#">《Cisco Secure Firewall Management Center 设备配置指南》</a>。</p>
策略 > 访问控制，<每个策略>，规则，默认操作 行，日志记录 ( )	<p>与访问控制策略关联的默认操作的日志记录设置。</p> <p>请参阅有关登录 <a href="#">《Cisco Secure Firewall Management Center 设备配置指南》</a> 和 <a href="#">使用策略默认操作记录连接</a> 的信息。</p>
策略 > 访问控制，<每个策略>，规则，<每个规则>，登录	<p>访问控制策略中特定规则的日志记录设置。</p> <p>请参阅有关登录到 <a href="#">《Cisco Secure Firewall Management Center 设备配置指南》</a> 的信息。</p>

配置位置	说明和更多信息
策略 > 访问控制, <每个策略>, 安全情报, 日志记录 (  )	安全情报阻止列表的日志记录设置。 点击这些按钮可配置： <ul style="list-style-type: none"> <li>• DNS 阻止列表日志记录选项</li> <li>• URL 阻止列表日志记录选项</li> <li>• 网络阻止列表日志记录选项（对于受阻列表中的 IP 地址）</li> </ul> 请参阅 <a href="#">《Cisco Secure Firewall Management Center 设备配置指南》</a>
策略 > 访问控制, <每个策略>, 默认操作 行, 日志记录 (  )	与 SSL 策略关联的默认操作的日志记录设置。 请参阅 <a href="#">使用策略默认操作记录连接</a> 。
策略 > SSL, <每个策略>, <每个规则>, 日志记录	SSL 规则的日志记录设置。 请参阅 <a href="#">《Cisco Secure Firewall Management Center 设备配置指南》</a> 。
策略 > 预过滤器, <每个策略>, 默认操作 行, 日志记录 (  )	与预过滤器策略关联的默认操作的日志记录设置。 请参阅 <a href="#">使用策略默认操作记录连接</a> 。
策略 > 预过滤器, <每个策略>, <每个预过滤器规则>, 日志记录	预过滤器策略中每个预过滤器规则的日志记录设置。 请参阅 <a href="#">《Cisco Secure Firewall Management Center 设备配置指南》</a>
策略 > 预过滤器, <每个策略>, <每个隧道规则>, 日志记录	预过滤器策略中每个隧道规则的日志记录设置。 请参阅 <a href="#">《Cisco Secure Firewall Management Center 设备配置指南》</a>
威胁防御 集群配置的其他系统日志设置:	<a href="#">《Cisco Secure Firewall Management Center 设备配置指南》</a> 多次提到了系统日志; 在该章中搜索“系统日志。”

### 入侵事件系统日志的配置位置（FTD 设备）

您可以在各个位置指定入侵策略的系统日志设置，也可以从访问控制策略或 FTD 平台设置或者从这两者继承设置。

配置位置	说明和更多信息
设备 > 平台设置，威胁防御设置策略，系统日志	您在此处配置的系统日志目标可以在访问控制策略的“日志记录”选项卡中指定，该策略可以是入侵策略的默认策略。  请参阅 <a href="#">《Cisco Secure Firewall Management Center 设备配置指南》</a> 。
策略 > 访问控制，<每个策略>，日志记录	入侵事件的系统日志目标的默认设置（在入侵策略未指定其他日志记录主机的情况下）。  请参阅 <a href="#">《Cisco Secure Firewall Management Center 设备配置指南》</a> 。
策略 > 入侵，<每个策略>，高级设置，启用系统日志警报，点击编辑	要指定访问控制策略“日志记录”选项卡中指定的目标之外的系统日志收集器，并指定设施和严重性，请参阅 <a href="#">为入侵事件配置系统日志警报</a> 。  如果您要使用入侵策略中配置的严重性或设施或两者，则还必须在策略中配置日志记录主机。如果您使用访问控制策略中指定的日志记录主机，则不会使用入侵策略中指定的严重性和设施。
策略 > 访问控制 > 日志记录 > IPS 设置	如果您想要发送 IPS 事件的系统日志消息。配置的默认系统日志设置用于 IPS 事件的系统日志目标

#### 入侵事件系统日志的配置位置（非 FTD 设备）

- （默认）访问控制策略 [《Cisco Secure Firewall Management Center 设备配置指南》](#)，如果您指定系统日志警报（请参阅[创建系统日志警报响应](#)。）
- 或者参阅[为入侵事件配置系统日志警报](#)。

默认情况下，入侵策略使用访问控制策略的“日志记录”选项卡中的设置。如果未在此处配置适用于 FTD 以外设备的设置，则不会为 FTD 以外的设备发送系统日志，也不会显示警告。

#### 文件和恶意软件事件系统日志的配置位置

配置位置	说明和更多信息
在访问控制策略中： 策略 > 访问控制，<每个策略>，日志记录	这是将系统配置为发送文件和恶意软件事件系统日志的主要位置。  如果您不使用 FTD 平台设置中的系统日志设置，则还必须创建警报响应。请参阅 <a href="#">创建系统日志警报响应</a> 。

配置位置	说明和更多信息
在 Firepower 威胁防御平台设置中： 设备 > 平台设置，威胁防御设置策略，系统日志	这些设置仅适用于运行受支持版本的 Firepower 威胁防御设备，并且仅当您将访问控制策略中的“日志记录”选项卡配置为使用 FTD 平台设置时才适用。  请参阅 <a href="#">《Cisco Secure Firewall Management Center 设备配置指南》</a> 。
在访问控制规则中： 策略 > 访问控制，<每个策略>，规则，<每个规则>，日志记录	如果您不使用 FTD 平台设置中的系统日志设置，则还必须创建警报响应。请参阅 <a href="#">创建系统日志警报响应</a> 。

## 安全事件系统日志消息剖析

FTD 中的示例安全事件消息（入侵事件）

```

0           1           2           3           4 5 6
-----
<37>2018-06-27 192.168.0.81 SFIMS : %FTD-5-430001:
192.168.1.10, DstIP: 192.168.1.102, SrcPort: 33994
Protocol: tcp, Priority: 2, GID: 133, SID: 17, Rev
Message: "DCE2_EVENT SMB_INVALID_DSIZE", Classifi
Potentially Bad Traffic, User: No Authentication R
Client: NetBIOS-ssn (SMB) client, ApplicationProto
(SMB), ACPolicy: test, NAPPolicy: Balanced Securit
Connectivity, InlineResult: Blocked

```

表 1: 安全事件系统日志消息的组件

示例消息中的项目编号	报头元素	说明
0	PRI	优先级值代表警报的设施和严重性。仅当您使用 FMC 平台设置以 EMBLEM 格式启用日志记录时，系统日志消息中才会显示该值。如果通过访问控制策略的日志记录选项卡启用入侵事件日志记录，则系统日志消息中会自动显示 PRI 值。有关如何启用 EMBLEM 格式的信息，请参阅 <a href="#">《Cisco Secure Firewall Management Center 设备配置指南》</a> 。有关 PRI 的详细信息，请参阅 <a href="#">RFC5424</a> 。
1	时间戳	<p>从设备发送系统日志消息的日期和时间。</p> <ul style="list-style-type: none"> <li>（从 FTD 设备发送的系统日志）对于使用访问控制策略及其后代中的设置发送的系统日志，或者如果在 FTD 平台设置中指定使用此格式，日期格式是 ISO 8601 中定义的格式，时间戳是 RFC 5424 中指定的格式 (yyyy-MM-ddTHH:mm:ssZ)，其中字母 Z 表示 UTC 时区。</li> <li>（从所有其他设备发送的系统日志）对于使用访问控制策略及其后代中的设置发送的系统日志，日期格式是 ISO 8601 中定义的格式，时间戳是 RFC 5424 中指定的格式 (yyyy-MM-ddTHH:mm:ssZ)，其中字母 Z 表示 UTC 时区。</li> <li>否则，即使未指示时区，仍采用 UTC 时区格式的月、日和时区。</li> </ul> <p>要在 FTD 平台设置中配置时间戳设置，请参阅 <a href="#">《Cisco Secure Firewall Management Center 设备配置指南》</a>。</p>
2	<p>发送消息的设备或接口。</p> <p>该字段可以是：</p> <ul style="list-style-type: none"> <li>接口的 IP 地址</li> <li>设备主机名</li> <li>自定义设备标识符</li> </ul>	<p>（对于从 FTD 设备发送的系统日志）</p> <p>如果使用 FTD 平台设置发送了系统日志消息，则这是在 <a href="#">系统日志设置</a> 中为 <a href="#">启用系统日志设备 ID</a> 选项配置的值（如果已指定）。</p> <p>否则，报头中不存在此元素。</p> <p>要在 FTD 平台设置中配置此设置，请参阅 <a href="#">《Cisco Secure Firewall Management Center 设备配置指南》</a>。</p>
3	自定义值	<p>如果使用警报响应发送了消息，则这是在发送消息的警报响应中配置的标记值（如果已配置）。（请参阅<a href="#">创建系统日志警报响应</a>。）</p> <p>否则，报头中不存在此元素。</p>
4	%FTD	发送消息的设备的类型。%FTD 是 Firepower 威胁防御

示例消息中的项目编号	报头元素	说明
5	严重性	在系统日志设置中为触发消息的策略指定的严重性。 有关严重性的说明，请参阅《 <a href="#">Cisco Secure Firewall Management Center 设备配置指南</a> 》中的严重性级别或 <a href="#">系统日志严重性级别</a> 。
6	事件类型标识符	<ul style="list-style-type: none"> <li>• 430001: 入侵事件</li> <li>• 430002: 连接开始时记录的连接事件</li> <li>• 430003: 连接结束时记录的连接事件</li> <li>• 430004: 文件事件</li> <li>• 430005: 文件恶意软件事件</li> </ul>
--	设施	请参阅 <a href="#">安全事件系统日志消息中的设施</a> ，第 24 页。
--	消息的其余部分	<p>用冒号分隔的字段和值。</p> <p>具有空值或未知值的字段在消息中会被省略。</p> <p>有关字段说明，请参阅：</p> <ul style="list-style-type: none"> <li>• <a href="#">连接和 安全相关连接 事件字段</a>。</li> <li>• <a href="#">入侵事件字段</a></li> <li>• <a href="#">文件和恶意软件事件字段</a></li> </ul> <p><b>注释</b></p> <p>字段说明列表包括系统日志字段和事件查看器中显示的字段（Firepower 管理中心 Web 界面中“分析”菜单下的菜单选项。）通过系统日志提供的字段这样标记。</p> <p>在事件查看器中显示的某些字段无法通过系统日志获得。此外，某些系统日志字段不包括在事件查看器中（但可以通过搜索获得），某些字段被组合在一起或被分开。</p>

## 安全事件系统日志消息中的设施

设施值通常在安全事件系统日志消息中不相关。但是，如果您需要设施，请使用下表：



设备	要在连接事件中包括设施	要在入侵事件中包括设施	在系统日志消息中的位置
FTD	在 FTD 平台设置中使用 EMBLEM 选项。 使用 FTD 平台设置发送系统日志消息时，连接事件的设施值始终为 <b>ALERT</b> 。	在 FTD 平台设置中使用 EMBLEM 选项或使用入侵策略中的系统日志设置配置日志记录。如果您使用入侵策略，则还必须在入侵策略设置中指定日志记录主机。  启用系统日志警报并配置入侵策略的设施和严重性。请参阅 <a href="#">为入侵事件配置系统日志警报</a> 。	虽然设施不会出现在消息报头中，但是系统日志收集器可以根据 RFC 5424 的第 6.2.1 节导出该值。
FTD 以外的设备	使用警报响应。	使用入侵策略高级设置中的系统日志设置或访问控制策略“日志记录”选项卡中标识的警报响应。	

有关详细信息，请参阅[入侵系统日志警报的设施和严重性](#)和[创建系统日志警报响应](#)。

## Firepower 系统日志消息类型

Firepower 可以发送多种系统日志数据类型，如下表所述：

系统日志数据类型	请参阅
来自 FMC 的审核日志	<a href="#">将审核日志流传输到系统日志</a> 和 <a href="#">审核和系统日志</a> 一章
来自 FTD 设备的设备运行状况和网络相关日志	<a href="#">《Cisco Secure Firewall Management Center 设备配置指南》</a>
来自 FTD 设备的连接、安全情报和入侵事件日志	<a href="#">关于配置系统以向系统日志发送安全事件数据</a> ，第 14 页。
来自经典设备的连接、安全情报和入侵事件日志	<a href="#">关于配置系统以向系统日志发送安全事件数据</a> ，第 14 页
文件和恶意软件事件日志	<a href="#">关于配置系统以向系统日志发送安全事件数据</a> ，第 14 页
IPS 设置	发送 IPS 事件的系统日志消息。 <a href="#">入侵事件系统日志的配置位置（FTD 设备）</a> ，第 20 页

## 安全事件的系统日志限制

- 如果您要使用 syslog 或在外部存储事件，请避免在对象名称（例如策略和规则名称）中使用特殊字符。对象名称不应包含特殊字符（例如逗号），接收名称的应用可能将其用作分隔符。

- 可能需要 15 分钟事件才能显示在系统日志收集器上。
- 以下文件和恶意软件事件的数据不可通过系统日志获得：
  - 追溯性事件
  - 由面向终端的 AMP 生成的事件

## eStreamer 服务器流传输

通过 Event Streamer (eStreamer)，您可以将几种事件数据从 Cisco Secure Firewall Management Center 传输到自定义开发的客户端应用。有关详细信息，请参阅 *Firepower 系统 Event Streamer 集成指南*。

您必须将 eStreamer 服务器配置为向客户端发送 eStreamer 事件，提供关于客户端的信息并生成建立通信时要使用的身份验证凭据集，然后，要用作 eStreamer 服务器的设备才能开始向外部客户端流传输 eStreamer 事件。可从设备的用户界面执行所有这些任务。一旦保存设置，收到请求时，您选择的事件将转发至 eStreamer 客户端。

您可以控制 eStreamer 服务器能够向发出请求的客户端传输的事件类型。

表 2: eStreamer 服务器可传输的事件类型

事件类型	说明
入侵事件	受管设备生成的入侵事件
入侵事件数据包数据	与入侵事件关联的数据包
入侵事件额外数据	与入侵事件关联的额外数据，如通过 HTTP 代理或负载均衡器连接至 Web 服务器的客户端的源 IP 地址
发现事件	网络发现事件
关联和允许列表事件	关联和合规性 allow 名单事件
影响标志警报	生成的影响警报 管理中心
用户事件	用户事件
恶意软件事件	恶意软件事件
文件事件	文件事件
连接事件	有关被监控主机与所有其他主机之间的会话流量的信息。

## 系统日志与 eStreamer 在安全事件方面的比较

通常，目前没有对 eStreamer 进行重大投资的组织应使用系统日志而不是 eStreamer 来在外部管理安全事件数据。

系统日志	eStreamer
无需任何自定义	需要执行大量自定义和持续维护来适应每个版本的更改
标准	受限于专有环境
系统日志标准不能防范数据丢失，尤其是在使用 UDP 时	防范数据丢失
直接从设备发送	从 FMC 发送，增加处理开销
仅支持 文件和恶意软件事件、连接事件（包括安全情报事件）和入侵事件。	支持 eStreamer 服务器流传输，第 26 页中所列的所有事件类型。
某些事件数据只能从 FMC 发送。请参阅 <a href="#">仅通过 eStreamer 发送的数据，不通过系统日志发送，第 27 页</a> 。	包括无法直接从设备通过系统日志发送的数据。请参阅 <a href="#">仅通过 eStreamer 发送的数据，不通过系统日志发送，第 27 页</a> 。

### 仅通过 eStreamer 发送的数据，不通过系统日志发送

以下数据仅可从 Cisco Secure Firewall Management Center 获取，因此无法从设备通过系统日志发送：

- 数据包日志
- 入侵事件额外数据事件
  - 有关说明，请参阅 [eStreamer 服务器流传输，第 26 页](#)。
- 统计信息和汇聚事件
- 网络发现事件
- 用户活动和登录事件
- 相关事件
- 对于恶意软件事件：
  - 追溯性判定
  - ThreatName 和 Disposition，除非有关相关 SHA 的信息已同步到设备
- 以下字段：
  - Impact 和 ImpactFlag 字段
  - 有关说明，请参阅 [eStreamer 服务器流传输，第 26 页](#)。

- IOC\_Count 字段
- 大多数原始 ID 和 UUID。  
例外情况：
  - 连接事件的系统日志包括以下内容：FirewallPolicyUUID、FirewallRuleID、TunnelRuleID、MonitorRuleID、SI\_CategoryID、SSL\_PolicyUUID 和 SSL\_RuleID
  - 入侵事件的系统日志包括 IntrusionPolicyUUID、GeneratorID 和 SignatureID
- 拓展元数据包括但不限于：
  - LDAP 提供的用户详细信息，例如全名、部门、电话号码等。  
系统日志仅在事件中提供用户名。
  - 基于状态的信息的详细信息，例如 SSL 证书详细信息。  
系统日志提供证书指纹等基本信息，但不会提供证书 CN 等其他证书详细信息。
  - 详细的应用信息，例如应用标签和类别。  
系统日志仅提供应用名称。某些元数据消息还包括有关对象的额外信息。
- 地理位置信息

## 选择 eStreamer 事件类型

**eStreamer 事件配置 (eStreamer Event Configuration)** 复选框控制 eStreamer 服务器可传输的事件。您的客户端仍必须在发送到 eStreamer 服务器的请求消息中，特别请求您要其接收的事件类型。有关详细信息，请参阅 *Firepower* 系统 *Event Streamer* 集成指南。

在多域部署中，您可以在任何域级别配置 eStreamer 事件配置。但是，如果祖先域已启用特定事件类型，则无法禁用后代域中的事件类型。

为管理中心，您必须是管理员用户才能执行此任务。

### 过程

---

**步骤 1** 选择集成 > 其他集成。

**步骤 2** 点击 **eStreamer**。

**步骤 3** 在 **eStreamer 事件配置 (eStreamer Event Configuration)** 下，选中或清除想要 eStreamer 转发到请求客户端的事件类型旁边的复选框（在 **eStreamer 服务器流传输**，第 26 页中进行了介绍）。

**步骤 4** 单击保存。

---

## 配置 eStreamer 客户端通信

必须先从 eStreamer 页面将客户端添加到 eStreamer 服务器的对等体数据库，然后 eStreamer 才能向该客户端发送 eStreamer 事件。您还必须将 eStreamer 服务器生成的身份验证证书复制到该客户端。完成这些步骤后，无需重新启动 eStreamer 服务即可使客户端能够连接到 eStreamer 服务器。

在多域部署中，可以在任何域中创建 eStreamer 客户端。通过身份验证证书，可以仅从客户端证书的域和任何后代域请求事件。eStreamer 配置页面仅显示与当前域相关联的客户端，因此，如果要下载或吊销证书，请切换到创建了客户端的域。

您必须是管理员或发现管理员用户，才能对管理中心执行此任务。

### 过程

**步骤 1** 选择集成 > 其他集成。

**步骤 2** 点击 eStreamer。

**步骤 3** 点击 **Create Client**。

**步骤 4** 在主机名 (**Hostname**) 字段中，输入运行 eStreamer 客户端的主机的主机名或 IP 地址。

**注释** 如果尚未配置 DNS 解析，请使用 IP 地址。

**步骤 5** 如果要对证书文件进行加密，请在密码 (**Password**) 字段中输入密码。

**步骤 6** 单击保存。

eStreamer 服务器现在允许主机访问 eStreamer 服务器上的端口 8302，并创建要在客户端-服务器身份验证期间使用的身份验证证书。

**步骤 7** 点击客户端主机名称旁边的 **下载** (↓) 以下载证书文件。

**步骤 8** 将证书文件保存至客户端用于 SSL 身份验证的适当目录。

**步骤 9** 要撤消客户端的访问权限，请点击想要移除的主机旁边的 **删除** (🗑️)。

请注意，无需重新启动 eStreamer 服务；系统将立即撤销访问权限。

## Splunk 中的事件分析

您可以使用 Cisco Secure Firewall (f.k.a. 面向 Splunk (以前称为适用于 Splunk 的思科 Firepower 应用) 作为显示和处理 Firepower 事件数据的外部工具，以追踪和调查网络上的威胁。

eStreamer 为必填项。这个是高级功能。请参阅 [eStreamer 服务器流传输](#)，第 26 页。

有关详细信息，请参阅 <https://cisco.com/go/firepower-for-splunk>。

## IBM QRadar 中的事件分析

您可以使用适用于 IBM QRadar 的思科 Firepower 应用作为显示事件数据并帮助您分析、寻找和调查网络威胁的替代方法。

eStreamer 为必填项。这个是高级功能。请参阅 [eStreamer 服务器流传输](#)，第 26 页。

有关详细信息，请参阅 <https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/QRadar/integration-guide-for-the-cisco-firepower-app-for-ibm-qradar.html>。

## 使用外部工具分析事件数据的历史记录

特性	版本	详细信息
SecureX 功能区	7.0	SecureX 功能区将转换为 SecureX，可即时了解思科安全产品中的威胁形势。 要在 FMC 中显示 SecureX 功能区，请参阅 <i>Firepower</i> 和 <i>SecureX</i> 集成指南，网址为 <a href="https://cisco.com/go/firepower-securex-documentation">https://cisco.com/go/firepower-securex-documentation</a> 。 新增/修改的屏幕：新页面：系统 > SecureX
将所有连接事件发送至思科云	7.0	您现在可以将所有连接事件发送到思科云，而不仅仅是发送高优先级连接事件。 新增/经修改的屏幕：系统 > 集成 > 云服务页面上的新选项
交叉启动以查看 Secure Network Analytics 中的数据	6.7	此功能引入了一种在“分析” > “上下文交叉启动”页面上为 Secure Network Analytics 设备创建多个条目的快速方法。 这些条目允许您右键单击相关事件，以交叉启动 Secure Network Analytics 并显示与您交叉启动的数据点相关的信息。 新菜单项：系统 > 日志记录 > 安全分析和日志记录 配置事件发送至 Secure Network Analytics 的新页面。

特性	版本	详细信息
从其他字段类型进行上下文交叉启动	6.7	<p>现在，您可以使用以下其他类型的事件数据交叉启动外部应用：</p> <ul style="list-style-type: none"> <li>• 访问控制策略</li> <li>• 入侵策略</li> <li>• 应用协议</li> <li>• 客户端应用</li> <li>• Web 应用</li> <li>• 用户名（包括领域）</li> </ul> <p>新菜单选项：右键点击“分析”菜单下页面上的“控制面板”构件和事件表中的事件的上述数据类型时，可以使用上下文交叉启动选项。</p> <p>支持的平台： Cisco Secure Firewall Management Center</p>
与 IBM QRadar 集成	6.0 及更高版本	<p>IBM QRadar 用户可以使用新的 Firepower 特定应用来分析其事件数据。</p> <p>可用功能受 Firepower 版本的影响。</p> <p>请参阅<a href="#">IBM QRadar 中的事件分析</a>，第 30 页。</p>
与 SecureX 威胁响应集成的增强功能	6.5	<ul style="list-style-type: none"> <li>• 支持区域云： <ul style="list-style-type: none"> <li>• 美国（北美）</li> <li>• 欧洲</li> </ul> </li> <li>• 支持其他事件类型： <ul style="list-style-type: none"> <li>• 文件和恶意软件事件</li> <li>• 高优先级连接事件</li> </ul> <p>这些是与以下内容相关的连接事件：</p> <ul style="list-style-type: none"> <li>• 入侵事件</li> <li>• 安全情报事件</li> <li>• 文件和恶意软件事件</li> </ul> </li> </ul> <p>经修改的屏幕：系统 &gt; 集成 &gt; 云服务中新的选项。</p> <p>支持的平台：此版本中通过直接集成或系统日志支持的所有设备。</p>
Syslog	6.5	AccessControlRuleName 字段现在在入侵事件系统日志消息中可用。
集成 思科安全数据包分析器	6.5	已删除对此功能的支持。

特性	版本	详细信息
集成 SecureX 威胁响应	6.3（通过系统日志，使用代理收集器） 6.4（直接）	使用 SecureX 威胁响应中功能强大的分析工具，将 Firepower 入侵事件数据与来自其他来源的数据集成，以便统一查看网络上的威胁。 经修改的屏幕（版本 6.4）： <a href="#">系统 &gt; 集成 &gt; 云服务</a> 中新的选项。 支持的平台：运行 6.3 版（通过系统日志）或 6.4 版的 Cisco Secure Firewall Threat Defense 设备。
文件和恶意软件事件的系统日志支持	6.4	现在可以通过系统日志从受管设备发送完全限定的文件和恶意软件事件数据。 修改的屏幕： <a href="#">策略 &gt; 访问控制 &gt; 访问控制 &gt; “日志记录”</a> 。 支持的平台：运行 6.4 版的所有受管设备。
与 Splunk 集成	支持所有 6.x 版本	Splunk 用户可以使用新的独立 Splunk 应用程序 Cisco Secure Firewall (f.k.a. 面向 Splunk 分析事件)。 可用功能受 Firepower 版本的影响。 请参阅 <a href="#">Splunk 中的事件分析</a> ，第 29 页。
集成 思科安全数据包分析器	6.3	引入的功能：立即向思科安全数据包分析器查询与事件相关的数据包，然后单击以检查思科安全数据包分析器中的结果或下载结果以便在另一种外部工具中进行分析。 新屏幕： <a href="#">系统 &gt; 集成 &gt; 数据包分析器</a> <a href="#">分析 &gt; 高级 &gt; 数据包分析器查询</a> 新菜单项： <a href="#">查询数据包分析器</a> 菜单项，在右键单击“控制面板”页面上的事件和“分析”菜单下页面上的事件表时会出现此菜单项。 支持的平台： <a href="#">Cisco Secure Firewall Management Center</a>
上下文交叉启动	6.3	引入的功能：右键单击事件以在基于 URL 的预定义或自定义外部资源中查找相关信息。 新增屏幕： <a href="#">分析 &gt; 高级 &gt; 上下文交叉启动</a> 新菜单项：多个选项，在右键单击“控制面板”页面上的事件和“分析”菜单下页面上的事件表时会出现这些选项。 支持的平台： <a href="#">Cisco Secure Firewall Management Center</a>



特性	版本	详细信息
连接和入侵事件系统日志消息	6.3	<p>能够使用新的统一、简化配置，通过系统日志将完全限定的连接和入侵事件发送到外部存储和工具。现在消息报头进行了标准化，包括事件类型标识符，消息变得更小，因为省略了具有未知值和空值的字段。</p> <p>支持的平台：</p> <ul style="list-style-type: none"><li>• 所有新功能：运行 6.3 版的 FTD 设备。</li><li>• 部分新功能：运行 6.3 版的非 FTD 设备。</li><li>• 更少的新功能：运行 6.3 以下版本的所有设备。</li></ul> <p>有关更多信息，请参阅<a href="#">关于发送安全事件的系统日志消息</a>，第 13 页下的主题以及子主题。</p>
eStreamer	6.3	<p>将 eStreamer 内容从“主机身份源”一章移至本章，并添加了将 eStreamer 与系统日志进行比较的摘要。</p>



## 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。