使用外部工具的事件分析

思科云事件设置

通过将防火墙事件发送到云，您可以使用外部工具来调查防火墙事件。设备会将防火墙事件发送到安全服务交换 (SSE)，然后将其转发到各种云服务，以统一可见性并加强威胁调查。

要允许设备将防火墙事件发送到，您必须使用智能许可证（**系统 (⚙) > 智能许可证**）来注册 防火墙管理中心 或启用 集成。 集成将 防火墙管理中心 与您的 安全云控制 账户相关联，并将您的 Cisco Secure Firewall 部署纳入思科云租户，使其能够连接到思科的集成安全云服务。

有关将 防火墙管理中心 与 集成的更多信息，请参阅启用 集成。

安全服务交换 事件整合

安全服务交换不会显示防火墙管理中心中的事件的完整列表。相反，它会关联并整合事件，仅显示唯一事件。此方法可减少事件的冗余并提高透明度。此整合使用的当前分类参数的详细信息，如下所示：

- 在识别入侵事件重复时，会考虑以下元素：发起方 IP、发起方 IP、SID 和 GID。
- 在识别连接事件和安全相关连接事件的重复时，会考虑以下元素：发起方 IP、发起方 IP 和安全情报类别。
- 识别重复的文件和恶意软件事件时，会考虑除 Event Second 以外的所有元素。

启用将事件发送至云

将 防火墙管理中心 配置为托管 防火墙威胁防御 设备直接将事件发送至 。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

- 确定要用于发送防火墙事件的思科区域云。在选择区域云时，请记住：
  - 您选择的区域也可用于思科支持诊断和思科支持网络功能。此设置还使用 Security Analytics and Logging (SaaS)管理 Cisco Secure Network Analytics 云的云区域。
  - 您无法合并或汇聚不同区域云中的数据。要汇聚来自多个区域的数据，则所有区域中的设备都必须将数据发送至同一区域云。
- 确保使用智能许可证（**系统 (⚙) > 智能许可证**）注册管理中心或启用 集成，以便让设备能够将防火墙事件发送到思科云。

注释 如果您已使用版本 7.6 之前的 SecureX 订用将事件发送到 ，则可以继续将事件发送到 服务，例如 思科 XDR。但是，如果您现在使用 安全云控制 帐户将管理中心注册到云租赁，则您的 安全云控制 帐户必须具有 Security Analytics and Logging 许可证才能将事件转发到 服务，例如 思科 XDR。

- 在 防火墙管理中心 中：
  - 转至**系统 (System) > 配置 (Configuration)** 页面并为 防火墙管理中心 提供唯一名称，以便其可在云中的**设备 (Devices)** 列表中明确识别。
  - 将您的 防火墙威胁防御 设备添加到 防火墙管理中心，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 防火墙管理中心 UI 中的**分析 (Analysis)** 菜单下如预期那样显示。
- 请确保您拥有思科安全云登录凭证，并且可以登录到创建您的帐户的区域云。

  有关区域云 URL 和支持的设备版本的更多信息，请参阅区域云。
- 请确保将智能帐户或 安全云控制 租户关联到 SSE 帐户。
- 如果您当前使用系统日志将事件发送到云，请禁用这以避免重复。

过程

步骤 1 确定要用于发送防火墙事件的区域云。有关选择区域云的详细信息，请参阅《Cisco Secure Firewall Threat Defense 和思科 XDR 集成指南》。

注释

如果 集成已启用，并且 防火墙管理中心 已注册到所选区域云，则更改区域云会禁用 集成。您可以在更改区域云后再次启用 集成。

步骤 2 在 防火墙管理中心中，选择 **集成** > **Cisco 安全云**。

步骤 3 从**当前区域 (Current Region)** 下拉列表中选择区域云。

步骤 4 选中**将事件发送到云 (Send events to the cloud)** 复选框以启用云事件配置。

步骤 5 选择要发送至云的事件类型。

注释
您发送到云端的事件可用于多个集成，如下表所示。

集成	受支持的事件选项	备注
Cisco Security Analytics and Logging (SaaS)	全部	高优先级连接事件包括： • 安全相关 连接事件 • 与文件和恶意软件事件相关的连接事件 • 与入侵事件相关的连接事件
思科扩展检测和响应 (思科 XDR)	取决于您的版本： • 安全相关的连接事件 • 入侵事件 • 文件和恶意软件事件	即使您发送所有连接事件，思科 XDR 仅支持安全相关的连接事件。 **注释** 思科 XDR 是单独许可的产品。除 Cisco Secure Firewall 产品所需的许可证外，还需要额外订用。有关详细信息，请参阅思科 XDR 许可证。

注释

- 如果 **启用入侵事件**， 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 (File and Malware Events)**，除了从 防火墙威胁防御 设备发送的事件外，防火墙管理中心 还会发送追溯性事件。

步骤 6 点击**保存**。

使用思科 XDR 分析事件

思科扩展检测和响应 (思科 XDR) 是基于云的解决方案，通过关联多个遥测源的检测来统一可视性，并使安全团队能够检测、确定优先级和响应最复杂的威胁。将 与 思科 XDR 集成，以便将思科的集成安全产品组合与您的防火墙部署连接起来，提供一致的体验，统一可见性、实现自动化并加强整个网络的安全性。

有关 思科 XDR的详细信息，请参阅 思科 XDR 帮助中心。

重要事项

- 思科 XDR 是单独许可的产品。除 Cisco Secure Firewall 产品所需的许可证外，还需要额外订用。有关详细信息，请参阅思科 XDR 许可证。
- 如果您在 7.6 版本之前已经通过 SecureX 订阅将事件发送到 ，则可以继续将事件发送到 思科 XDR。但是，如果您现在使用 安全云控制 帐户将 防火墙管理中心 注册到云租赁，以便将防火墙事件发送到 思科 XDR，则您的 安全云控制 帐户必须具有 Security Analytics and Logging 许可证才能将事件转发到 思科 XDR。

要将 与 思科 XDR 集成，请参阅《Cisco Secure Firewall Management Center 和 Cisco XDR 集成指南》。

注释 截至 2024 年 7 月 31 日，思科 SecureX 已被淘汰，不再提供。无法为用户调配 Cisco SecureX，并且在购买 Cisco Secure Firewall 产品时不提供对 Cisco SecureX 的访问。此外，所有现有的思科 SecureX 环境都会被禁用，所有功能都不可用。如果您使用 Firefox，您应该移除 Cisco SecureX Ribbon 浏览器扩展。有关更多信息，请参阅常见问题解答。

使用 思科 XDR 自动化功能分析和响应威胁

启用此设置可允许 思科扩展检测和响应 (思科 XDR) 用户创建的自动化工作流程与您的 防火墙管理中心 资源进行交互。

思科 XDR 自动化为构建自动化工作流程提供了一种无到低代码方法。您可以使用拖放界面设计自己的工作流程，并且可以将其设置为响应不同的计划和事件。思科 XDR 自动化帮助您使用自动化功能和有关威胁响应的指导建议，信心十足地在所有相关控制点消除威胁。

注释 思科 XDR 是单独许可的产品。除 Cisco Secure Firewall 产品的许可证外，还需要额外订用。有关详细信息，请参阅思科 XDR 许可证。

有关 思科 XDR 自动化功能的详细信息，请参阅思科 XDR 文档。

开始之前

启用思科安全云并将您的管理中心注册到云。请参阅启用 集成。

过程

步骤 1 请点击 **集成** > **Cisco 安全云**。

步骤 2 选中 **启用思科 XDR 自动化** 复选框。

步骤 3 选择要分配给思科 XDR 自动化工作流程的 防火墙管理中心 用户角色。

访问管理员角色会被设置为默认角色，从而允许访问**策略 (Policies)** 菜单中的访问控制策略和相关功能。

步骤 4 点击**保存**。

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 Cisco Secure Endpoint。

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 Cisco Secure Network Analytics，第 8 页中的程序管理 Cisco 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 6 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，例如威胁智能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 Cisco Secure Network Analytics 设备添加链路， 请检查所需的链路是否已存在；配置 Security Analytics and Logging（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 6 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 (New Cross-launch)**。

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“准备工作”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点击的 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 点击**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**)，或者
- 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 右键点击感兴趣的事件，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。

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

例如，要从思科 Talos 获取有关入侵事件中的源 IP 地址的威胁智能，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 Cisco Secure Network Analytics

您还可以从 中的事件交叉启动，以查看 Cisco Secure Network Analytics 设备上的相关数据。有关 Cisco Secure Network Analytics 产品的详细信息，请参阅思科安全分析和日志记录产品页面。

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 7 页。

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

注释

- 如果稍后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 6 页中的程序手动创建其他链接以交叉启动到 Cisco Secure Network Analytics 设备中，但这些链接仍独立于自动创建的资源，您必须手动管理它们。

开始之前

- 您必须部署并运行 Cisco Secure Network Analytics 设备。
- 如果您当前使用系统日志将事件从支持直接发送事件的设备版本发送到 Cisco Secure Network Analytics，请禁用这些设备的系统日志（或为这些设备分配不包含系统日志配置的访问控制策略），以避免在远程卷上复制事件。
- 您必须具备以下条件：
  - 管理器的主机名或 IP 地址。
  - Cisco Secure Network Analytics 设备上具有管理员权限的帐户的凭证。

如果要使用 Security Analytics and Logging（本地部署） 将 数据发送到 Cisco Secure Network Analytics 设备，请参阅 Cisco Secure Network Analytics 设备上的远程数据存储。

过程

步骤 1 选择**集成** > **安全性分析和日志**。

步骤 2 您的 Cisco Secure Network Analytics 部署有两个选项：

- 仅管理器 (Manager Only) - 部署独立管理器以接收和存储事件，您可以从中查看和查询事件。

- 数据存储 (Data Store) - 部署用于接收事件的思科 Cisco Secure Network Analytics 流量收集器、用于存储事件的 Cisco Secure Network Analytics 数据存储以及用于查看和查询事件的管理器。

选择部署选项，然后点击**开始 (Start)**。

步骤 3 完成向导。有关详细信息，请参阅《思科安全分析和日志记录防火墙集成指南》中的 防火墙管理中心 配置部分。

步骤 4 选择 **分析** > **高级** > **上下文交叉启动** 以验证新的交叉启动链接。

如果要进行更改，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

使用 Cisco Secure Network Analytics 凭证从事件交叉启动到 Cisco Secure Network Analytics 事件查看器。

要从 防火墙管理中心 事件查看器或控制面板中的事件交叉启动，请右键点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，具体取决于需要处理的数据量、Cisco Secure Network Analytics 管理器上的速度和需求等。

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、 安全智能、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。

注释 在 7.2.1 版中，允许使用路由查找转发系统日志流量。这样，无论日志主机配置中指定了哪个接口，流量都能被转发。但是，在 7.2.5.1 及更高版本中，7.2.1 中引入的更改已被删除。

因此，从 7.2.5.1 及更高版本开始，日志主机配置中指定的配置将优先于路由查找，系统日志流量将从指定接口转发。

关于配置系统以向系统日志发送安全事件数据

要了解适用于安全事件系统日志消息的平台设置，请参阅《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威胁防御平台设置。

请注意，如果在任何策略中更改系统日志设置，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 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。
Cisco Secure Firewall Threat Defense	1. 执行以下操作，以在 平台设置中配置系统日志： 1. 请点击 **设备** > **平台设置**。 2. 编辑威胁防御设置策略。 3. 在左侧导航窗格中，点击 **系统日志**。 另请参阅《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威胁防御平台设置。 2. 在访问控制策略**日志记录**选项卡中，选择使用 平台设置。 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。） 不建议覆盖其中任何设置。 有关基本信息，请参阅 从 设备发送安全事件系统日志消息，第 10 页。
所有其他设备	1. 创建警报响应 2. 配置访问控制策略日志记录以使用警报响应。 3. （对于入侵事件）在入侵策略中配置系统日志设置。 有关完整的详细信息，请参阅 从经典设备发送安全事件系统日志消息，第 13 页。

从 设备发送安全事件系统日志消息

此程序记录从 管理的 Cisco Secure Firewall Management Center设备。

注释 许多 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 设备配置系统日志设置：

a) 请点击 **设备** > **平台设置**。
b) **编辑** 与 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**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) 请点击 **策略** > **访问控制标题** > **访问控制**。
b) 编辑适用的访问控制策略。
c) 点击**更多 (More)** > **日志记录 (Logging)**。
d) 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**。

步骤 3 为访问控制策略启用安全智能事件日志记录：

a) 在同一访问控制策略中，点击 **安全智能** 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**。

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** > **添加规则**。
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**。
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，选择**高级设置** > **系统日志警报**，然后点击**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面配置的设置。
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，请参阅系统日志警报设施。
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，请参阅系统日志严重性级别。

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 防火墙管理中心 联机帮助中 连接和安全智能事件系统日志的配置位置（所有设备），第 14 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 13 页。
- 如果完成更改，请将更改部署到托管设备。

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) 请点击 **策略** > **访问控制标题** > **访问控制**。
b) 编辑适用的访问控制策略。
c) 点击 **日志记录 (Logging)**。
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**。

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**。

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) 在您的入侵策略中，点击**高级设置** > **系统日志警报**，然后点击**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面配置的设置。
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。 请参阅系统日志警报设施。
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。 请参阅系统日志严重性级别。

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 连接和安全智能事件系统日志的配置位置（所有设备），第 14 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。
- 有关为 设备配置安全事件系统日志记录的信息，请参阅从 设备发送安全事件系统日志消息，第 10 页。

安全事件系统日志的配置位置

这些主题介绍如何为安全事件系统日志配置位置：

连接和安全智能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托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**	此选项仅适用于 设备。 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。 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 。
策略 > 访问控制，<每个策略>，**日志记录**	您在此处配置的设置是所有连接和安全智能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。 设备的建议设置：使用威胁防御平台设置。有关信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》 。 所有其他设备的必需设置：使用系统日志警报。 如果您指定系统日志警报，请参阅创建系统日志警报响应。 有关“日志记录”选项卡上的设置的详细信息，请参阅《Cisco Secure Firewall Management Center 设备配置指南》 。
策略> 访问控制，<每个策略>，**规则**， **默认操作** 行， **日志记录**（）	与访问控制策略关联的默认操作的日志记录设置。 请参阅有关登录 《Cisco Secure Firewall Management Center 设备配置指南》 和 使用策略默认操作记录连接 的信息。
策略 > 访问控制，<每个策略>，**规则**，<每个规则>， **登录**	访问控制策略中特定规则的日志记录设置。 请参阅有关登录到 《Cisco Secure Firewall Management Center 设备配置指南》的信息。
策略 > 访问控制，<每个策略>，**安全智能**， **日志记录**（）	安全智能阻止列表的日志记录设置。 点击这些按钮可配置： • DNS 阻止列表日志记录选项 • URL 阻止列表日志记录选项 • 网络阻止列表日志记录选项（对于受阻列表中的 IP 地址） 请参阅 《Cisco Secure Firewall Management Center 设备配置指南》
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。 请参阅使用策略默认操作记录连接。
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《Cisco Secure Firewall Management Center 设备配置指南》 。

配置位置	说明和更多信息
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。 请参阅使用策略默认操作记录连接。
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 《Cisco Secure Firewall Management Center 设备配置指南》
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 《Cisco Secure Firewall Management Center 设备配置指南》
集群配置的其他系统日志设置：	《Cisco Secure Firewall Management Center 设备配置指南》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 《Cisco Secure Firewall Management Center 设备配置指南》。
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《Cisco Secure Firewall Management Center 设备配置指南》。
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，请参阅为入侵事件配置系统日志警报。 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。请参阅创建系统日志警报响应。
在 Firepower Threat Defense 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 Threat Defense 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 《Cisco Secure Firewall Management Center 设备配置指南》。
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。请参阅创建系统日志警报响应。

安全事件系统日志消息剖析

中的示例安全事件消息（入侵事件）

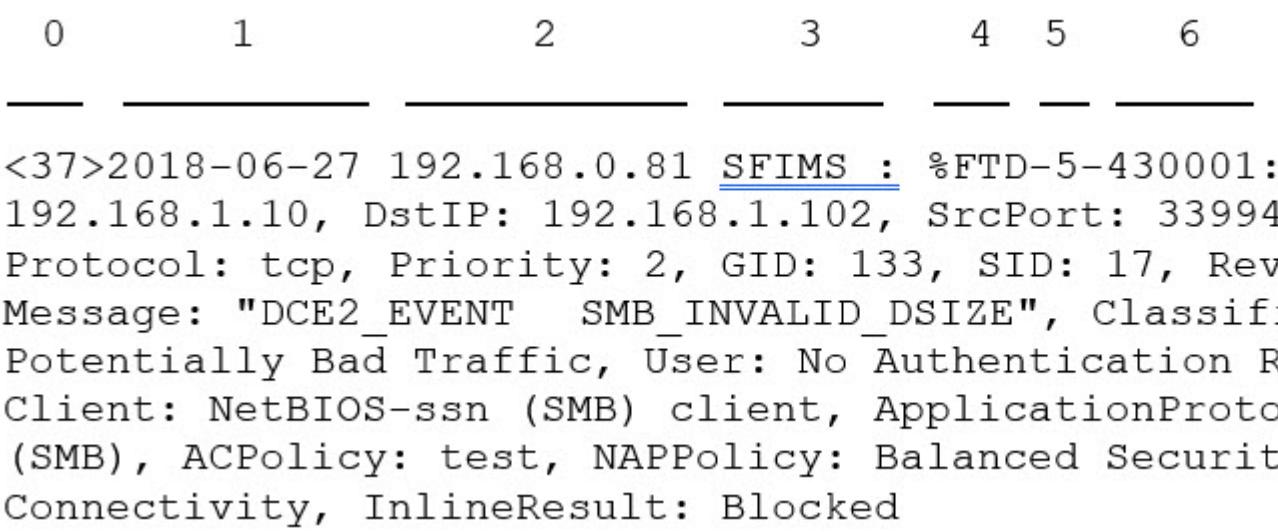

表 *1:* 安全事件系统日志消息的组件

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。仅当您使用防火墙管理中心 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 《Cisco Secure Firewall Management Center 设备配置指南》 。有关 PRI 的详细信息，请参阅 RFC5424。

示例消息中的项目编号	报头元素	说明
1	时间戳	从设备发送系统日志消息的日期和时间。 • （从 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，或者如果在威胁防御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。 • （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。 • 否则，即使未指示时区，仍采用 UTC 时区格式的月、日和时间。 要在威胁防御平台设置中配置时间戳设置，请参阅《Cisco Secure Firewall Management Center 设备配置指南》。
2	发送消息的设备或接口。 该字段可以是： • 接口的 IP 地址 • 设备主机名 • 自定义设备标识符	（对于从 设备发送的系统日志） 如果使用威胁防御平台设置发送了系统日志消息，则这是在**系统日志设置**中为**启用系统日志设备 ID** 选项配置的值（如果已指定）。 否则，报头中不存在此元素。 要在威胁防御平台设置中配置此设置，请参阅《Cisco Secure Firewall Management Center 设备配置指南》。
3	自定义值	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）。（请参阅创建系统日志警报响应。） 否则，报头中不存在此元素。
4	%FTD	发送消息的设备的类型。%FTD 是 Cisco Secure Firewall Threat Defense
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《Cisco Secure Firewall Management Center 设备配置指南》中的 严重性级别 或 系统日志严重性级别。

示例消息中的项目编号	报头元素	说明
6	事件类型标识符	• 430001：入侵事件 • 430002：连接开始时记录的连接事件 • 430003：连接结束时记录的连接事件 • 430004：文件事件 • 430005：文件恶意软件事件
--	设施	请参阅安全事件系统日志消息中的设施，第 20 页。
--	消息的其余部分	用冒号分隔的字段和值。 具有空值或未知值的字段在消息中会被省略。 有关字段说明，请参阅： • 连接和 安全相关连接 事件字段。 • 入侵事件字段 • 文件和恶意软件事件字段 **注释** 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（防火墙管理中心 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。 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。

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
	在威胁防御平台设置中使用 EMBLEM 选项。 使用威胁防御平台设置发送系统日志消息时，连接事件的设施值始终为 **ALERT**。	在威胁防御平台设置中使用 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。请参阅为入侵事件配置系统日志警报。	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。
之外的设备	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。

Cisco Secure Firewall 系统日志消息类型

Cisco Secure Firewall 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
来自的审核日志 防火墙管理中心	将审核日志流传输到系统日志和审核和系统日志一章
来自 设备的设备运行状况和网络相关日志	《Cisco Secure Firewall Management Center 设备配置指南》
来自 设备的连接、 安全情报和入侵事件日志	关于配置系统以向系统日志发送安全事件数据， 第 9 页。
来自经典设备的连接、安全情报和入侵事件日志	关于配置系统以向系统日志发送安全事件数据， 第 9 页
文件和恶意软件事件日志	关于配置系统以向系统日志发送安全事件数据， 第 9 页
IPS 设置	发送 IPS 事件的系统日志消息。 入侵事件系统日志的配置位置（FTD 设备）， 第 16 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《*Cisco Secure Firewall Management Center* 事件流传输器集成指南》《》。

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	托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 防火墙管理中心
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 22 页中所列的所有事件类型。
某些事件数据只能从 FMC 发送。请参阅仅通过 eStreamer 发送的数据，不通过系统日志发送， 第 23 页。	包括无法直接从设备通过系统日志发送的数据。请参阅仅通过 eStreamer 发送的数据，不通过系统日志发送， 第 23 页。

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 22 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 22 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《*Cisco Secure Firewall Management Center* 事件流传输器集成指南》。

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 防火墙管理中心，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 22 页中进行了介绍）。

步骤 4 点击**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 防火墙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 点击**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 Cisco Firepower 应用）作为显示和处理 Cisco Secure Firewall 事件数据的外部工具，以追踪和调查网络上的威胁。要使用 Splunk 工具，则需要安装 eStreamer。这个是高级功能。请参阅eStreamer 服务器流传输 ， 第 22 页。有关详细信息，请参阅 Cisco Secure Firewall 用户指南 (f.k.a. 面向 Splunk 的 Firepower) App。

IBM QRadar 中的事件分析

您可以使用适用于 IBM QRadar 的 Cisco 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 22 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

功能	防火墙管理中心最低版本	最低版本	详细信息
使用您的 Cisco Security Cloud Sign On 账户向注册您的管理中心。	7.6.0	任意	现在，您可以授权管理中心使用您的思科安全云登录账户和 CDO 租户注册到 。将管理中心注册到 ，即可访问最新的思科云服务，例如思科安全 AI 助手、策略分析器和优化器、零接触调配等。 新增/修改的屏幕：**集成 (Integration)** > **思科安全云 (Cisco Security Cloud)**。 **升级影响**：默认情况下，思科安全云集成设置为禁用。
已弃用：SecureX 功能区	任意	任意	SecureX 功能区已弃用。 如果您已在 Firefox 浏览器中安装**思科 SecureX 功能区**浏览器扩展，并且在使用 防火墙管理中心时遇到兼容性错误，请删除 SecureX 功能区扩展。 要删除扩展，请打开 Firefox，转到浏览器的加载项或扩展管理器，找到**思科 SecureX 功能区**扩展，然后将其删除或禁用。重新启动 Firefox 以应用更改。
已弃用：SecureX 集成	7.6.0	任意	SecureX 集成已弃用。现在，您可以使用思科安全云登录账户和 安全云控制 租户将 防火墙管理中心 及其托管设备注册到 。 新增/修改的屏幕：**集成 (Integration)** > **思科安全云 (Cisco Security Cloud)**。 已弃用的屏幕：**集成** > **SecureX**。

功能	防火墙管理中心最低版本	最低版本	详细信息
SecureX 功能区	7.0	任意	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 防火墙管理中心中显示 SecureX 功能区，请参阅 *Firepower* 和 *SecureX* 集成指南 ，网址为 https://cisco.com/go/firepower-securex-documentation。 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	任意	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 Cisco Secure Network Analytics中的数据	6.7	任意	此功能引入了一种在“分析”>“上下文交叉启动”页面上为Cisco 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点击相关事件，以交叉启动 Cisco 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 Cisco Secure Network Analytics的新页面。
从其他字段类型进行上下文交叉启动	6.7	任意	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： • 访问控制策略 • 入侵策略 • 应用协议 • 客户端应用 • Web 应用 • 用户名（包括领域） 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。 支持的平台： Cisco Secure Firewall Management Center
与 IBM QRadar 集成	6.0 及更高版本	任意	IBM QRadar 用户可以使用新的 Firepower 特定应用来分析其事件数据。 可用功能受 Firepower 版本的影响。 请参阅IBM QRadar 中的事件分析 ，第 26 页。

功能	防火墙管理中心最低版本	最低版本	详细信息

与 SecureX 威胁响应集成的增强功能	6.5	任意	• 支持区域云：
			  • 美国（北美）
			  • 欧洲
			• 支持其他事件类型：
			  • 文件和恶意软件事件
			  • 高优先级连接事件
			  这些是与以下内容相关的连接事件：
			  • 入侵事件
			  • 安全智能事件
			  • 文件和恶意软件事件
			经修改的屏幕：**系统** > **集成** > **云服务**中的新选项。
			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。

Syslog	6.5	任意	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	任意	已删除对此功能的支持。
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）	任意	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）：**系统** > **集成** > **云服务**中的新选项。 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	任意	现在可以通过系统日志从托管设备发送完全限定的文件和恶意软件事件数据。 经修改的屏幕：**策略** > **访问控制** > **访问控制** > **日志记录**。 支持的平台：运行 6.4 版的所有托管设备。

功能	防火墙管理中心最低版本	最低版本	详细信息
与 Splunk 集成	支持所有 6.x 版本	任意	Splunk 用户可以使用新的独立 Splunk 应用 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Splunk 中的事件分析，第 25 页。
集成思科安全数据包分析器	6.3	任意	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，然后点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： **系统** > **集成** > **数据包分析器** **分析** > **高级** > **数据包分析器查询**。 新菜单选项：**查询** > **数据包分析器**菜单项，在右键点击“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： Cisco Secure Firewall Management Center
上下文交叉启动	6.3	任意	引入的功能：右键点击事件以在基于 URL 的预定义或自定义外部资源中查找相关信息。 新增屏幕：**分析** > **高级** > **情景交叉启动**。 新菜单选项：多个选项，在右键点击“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： Cisco Secure Firewall Management Center
连接和入侵事件系统日志消息	6.3	任意	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。 支持的平台： • 所有新功能：运行 6.3 版的 设备。 • 部分新功能：运行 6.3 版的非 设备。 • 更少的新功能：运行 6.3 以下版本的所有设备。 有关更多信息，请参阅关于发送 安全事件的系统日志消息，第 9 页下的主题以及子主题。
eStreamer	6.3	任意	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。

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。