



思科 Cisco Secure Firewall Management Center 与 Security Analytics and Logging (SaaS) 集成指南

上次修改日期: 2024 年 12 月 3 日

集成 Cisco Secure Firewall Management Center 和 Cisco Security Analytics and Logging (SaaS)

如果需要更多空间来存储 Cisco Secure Firewall Threat Defense 事件，则可以使用 Cisco Security Analytics and Logging (SaaS) 将其发送到 Cisco Secure Cloud Analytics 进行存储，并可以选择使用 Cisco Secure Cloud Analytics 使威胁防御事件数据可用于安全分析。根据许可证的不同，您可以在思科防御协调器 (CDO) 或 Cisco Secure Cloud Analytics 中查看事件。

此集成专门用于管理中心管理的威胁防御设备。本文档不适用于未运行威胁防御软件的设备、由设备管理器管理的设备或由管理中心管理的非威胁防御设备。

有关 Cisco Security Analytics and Logging (SaaS) 的详细信息，请参阅[思科安全分析和日志记录产品页面](#)。

Cisco Security Analytics and Logging 远程事件存储选项的比较

将事件数据存储到管理中心外部的类似但不同的选项：

本地	SaaS
您购买、获得许可并在防火墙后设置存储系统。	您可以购买许可证和数据存储计划，并将数据发送到思科安全云。
支持的事件类型： <ul style="list-style-type: none">• 连接• 安全相关的连接• 入侵• 文件和恶意软件• LINA	支持的事件类型： <ul style="list-style-type: none">• 连接• 安全相关的连接• 入侵• 文件和恶意软件
支持系统日志和直接集成。	支持系统日志和直接集成。请参阅 将事件发送到云的方法的比较 ，第 2 页。

本地	SaaS
<ul style="list-style-type: none"> 查看 Cisco Secure Network Analytics 管理器上的所有事件。 从管理中心事件查看器交叉启动，以查看 Cisco Secure Network Analytics 管理器上的事件。 查看远程存储的连接和管理中心中与安全相关的连接事件 	<p>在 CDO 中查看事件，或者 Cisco Secure Network Analytics，具体取决于您的许可证。从管理中心事件查看器交叉启动。</p>
<p>有关详细信息，请参阅《Cisco Secure Firewall Management Center 管理指南》或联机帮助中“数据存储”一章中的链接。</p>	

将事件发送到云的方法的比较

通过系统日志发送	直接发送
<ul style="list-style-type: none"> 需要安全事件连接器 (SEC)。 有利于防火墙设备的高日志发射率，因为每个 SEC 每秒最多可支持 100,000 个事件 可以为 CDO 或非 CDO 管理的设备设置 SEC。 减少防火墙的事件处理压力，从而为防火墙功能释放资源。 集中化并不总是可行或可取的，尤其是对于地理位置分散的环境。 需要单独安装。 	<ul style="list-style-type: none"> 非常适合分支机构，因为它支持地理位置分散的环境。 需要智能许可。 <p>如果您使用的是思科智能软件管理器本地服务器（以前称为智能软件卫星服务器）或气隙部署，则不受支持。</p> <ul style="list-style-type: none"> 无需单独安装或服务。 防火墙资源的压力相对较高。

SAL (SaaS) 集成的要求和前提条件

以下要求适用于将事件发送到 SAL (SaaS) 的两种方法。

要求或前提条件类型	要求
设备和管理器	<p>管理中心 管理 威胁防御 设备</p> <p>通过系统日志发送： 6.4 或更高版本</p> <p>直接发送： 版本 7.0</p> <p>所需版本适用于 管理中心 和所有托管 威胁防御 设备。</p> <p>必须部署系统并成功生成事件。</p>
区域云	<ul style="list-style-type: none"> • 确定要用于发送防火墙事件的思科区域云。 • 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。 <p>无法在不同的区域云之间查看或移动事件。</p> <ul style="list-style-type: none"> • 如果您使用直接连接将事件发送到 思科安全云 以与 思科 XDR 集成，则必须使用相同的区域 CDO 云来进行此集成。
数据计划	<p>确定系统所需的云存储量。有关详细信息，请参阅计算存储要求并购买流量计划，第 4 页。</p>
许可	<ul style="list-style-type: none"> • 思科安全分析和日志许可证：任何 <p>有关许可选项和说明，请参阅SAL (SaaS)许可证，第 4 页。</p> <ul style="list-style-type: none"> • CDO 许可证：无需额外的 CDO 许可。 • Cisco Secure Cloud Analytics 许可证：无需额外的许可。 • 管理中心 许可证：无需额外的许可。
帐户	<p>当您购买该集成的许可证时，您将获得一个 CDO 租户帐户以支持该功能。</p>
支持的事件类型	<p>入侵、连接、安全相关的连接、文件和恶意软件事件。</p>
用户角色	<p>在 管理中心 中：</p> <ul style="list-style-type: none"> • 管理 • 访问管理员 • 网络管理员 • 安全审批人
直接发送事件时的其他要求	<p>请参阅直接集成的前提条件，第 12 页。</p>
其他前提条件	<p>请参阅每个程序的开始之前或前提条件部分。</p>

SAL (SaaS)许可证

许可证	详细信息
免费试用	要获取 30 天免费试用许可证，请访问 https://www.defenseorchestrator.com/provision 。
日志记录故障排除	将事件存储在思科云中，然后使用 CDO Web 界面查看和过滤存储的事件。
(可选) 日志记录分析和检测	<p>系统可以将 Cisco Secure Cloud Analytics 动态实体建模应用于 威胁防御 事件，并使用行为建模分析生成 Cisco Secure Cloud Analytics 观察结果和警报。您可以使用思科单点登录从 CDO 交叉启动为您调配的 Cisco Secure Cloud Analytics 门户。</p> <p>购买 SAL 许可证时，您将获得 CDO 租户的访问权限（用于日志查看）和 Cisco Secure Cloud Analytics 实例的访问权限（用于威胁检测）。SAL 用户无需单独的 CDO 或 Cisco Secure Cloud Analytics 许可证即可访问这两个门户以获取 SAL 提供的结果。</p>
(可选) 全面网络分析和检测	<p>该系统对 威胁防御 事件和网络流量进行动态实体建模，并生成观察结果和警报。您可以使用思科单点登录从 CDO 交叉启动为您调配的 Cisco Secure Cloud Analytics 门户。</p> <p>购买 SAL 许可证时，您将获得 CDO 租户的访问权限（用于日志查看）和 Cisco Secure Cloud Analytics 实例的访问权限（用于威胁检测）。SAL 用户无需单独的 CDO 或 Cisco Secure Cloud Analytics 许可证即可访问这两个门户以获取 SAL 提供的结果。</p>

SAL (SaaS) 许可证提供使用 CDO 租户的权限来查看防火墙日志和 Cisco Secure Cloud Analytics 分析实例，而无需为这些产品单独持有许可证。

要购买 SAL (SaaS) 许可证，请联系您的授权思科销售代表，或参阅订购指南（上面的链接）并查找以 **SAL-SUB** 开头的 PID。

计算存储要求并购买流量计划

您需要购买一个数据计划，以反映思科云每天从注册的威胁防御接收的事件数量。这称为“每日注入速率”。

要估计您的数据存储要求，请执行以下操作：

- （推荐）在购买前参与 Cisco Security Analytics and Logging (SaaS) 的免费试用。请参阅 [SAL \(SaaS\) 许可证，第 4 页](#)。
- 使用位于 <https://ngfwpe.cisco.com/ftd-logging-estimator> 的日志记录卷估计器工具。

数据计划有不同的日数据量和不同的年数据量。有关数据计划的信息，请参阅《*Cisco Security Analytics and Logging 订购指南*》，网址为：<https://www.cisco.com/c/en/us/products/collateral/security/security-analytics-logging/guide-c07-742707.html>。



注释 如果您有 SAL (SaaS) 许可证和数据计划，则在以后获取不同的许可证，这不需要您获取不同的数据计划。如果您的网络流量吞吐量发生变化，并且您获得了不同的数据计划，则不需要您获得不同的 SAL (SaaS) 许可证。

如何将事件从 管理中心 发送到 SAL SaaS

要成功部署此集成，请执行以下任一主题中的所有步骤：

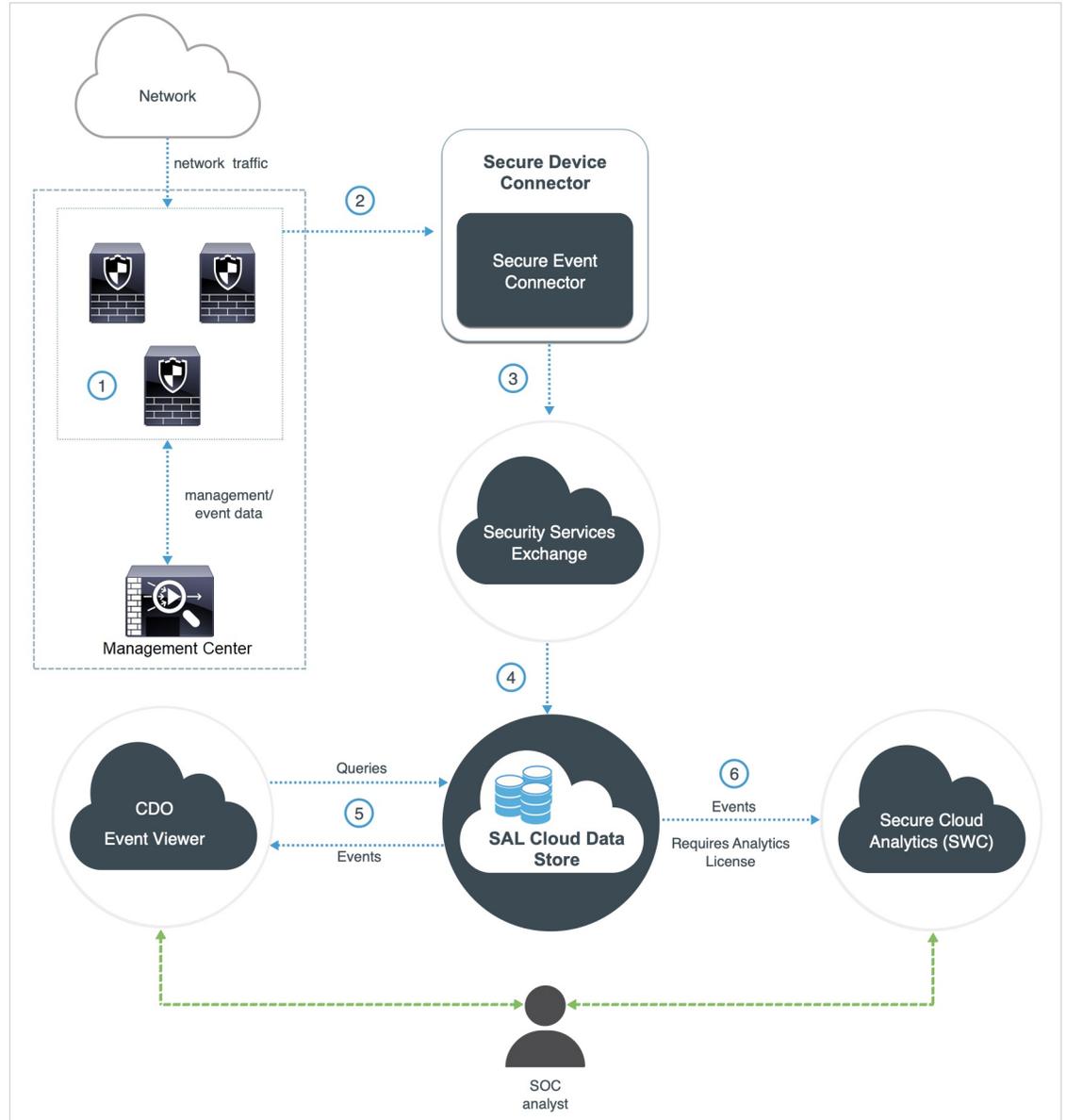
- [如何使用直接连接在 SAL \(SaaS\) 中设置事件数据存储，第 10 页](#)
- [如何使用系统日志在 SAL \(SaaS\) 中设置事件数据存储，第 5 页](#)

如何使用系统日志在 SAL (SaaS) 中设置事件数据存储

	相应操作	更多信息
步骤	查看要求和前提条件	请参阅 SAL (SaaS) 集成的要求和前提条件，第 2 页 。
步骤	获取所需的许可证、帐户和数据存储计划	联系您的授权思科销售代表。
步骤	使用多重身份验证来设置 CDO 访问权限	有关 登录 CDO ，请参阅 CDO 在线帮助中的说明。
步骤	在 VMWare 虚拟机上设置本地安全设备连接器 (SDC)	<p>此组件仅用于启用 SEC 的安装，这是设备将向其发送事件的组件。</p> <p>如 CDO 在线帮助中所述，使用以下方法之一：</p> <ul style="list-style-type: none"> • （首选）使用 CDO 提供的 VM 映像。 • 在不使用 CDO 提供的映像的情况下创建 SDC。 <p>重要提示！ 不要跳过程序前提条件。但是，请忽略有关载入的任何信息，这些信息不适用于此集成。</p>

	相应操作	更多信息
步骤	在您刚刚创建的 SDC 虚拟机上安装安全事件连接器 (SEC)。	这是设备将向其发送事件的组件。 有关 安装安全事件连接器 的说明，请参阅 CDO 在线帮助。 重要提示！ 不要跳过程序前提条件。但是，请忽略有关载入的任何信息，这些信息不适用于此集成。
步骤	配置管理中心，以便让托管设备向 SEC 发送系统日志事件。	从威胁防御设备发送安全事件系统日志消息 ，第 8 页
步骤	验证您的事件是否已成功发送	请参阅 查看和处理事件 ，第 24 页。
步骤	(可选) 如果要将连接事件发送到云，并且不想将其存储在管理中心上，请在管理中心上禁用该存储。	在管理中心联机帮助中，请参阅“数据库事件限制”主题中有关连接事件的信息。
步骤	(可选) 配置从管理中心到 CDO 的交叉启动，以便您可以轻松地从管理中心中显示的事件切换到云中的相关事件。	请参阅管理中心中的联机帮助。
步骤	(可选) 在 CDO 中配置常规设置	例如，您可以使思科支持人员无法使用您的数据。 在 CDO 联机帮助中，请参阅 常规设置 。
步骤	(可选) 创建 CDO 用户帐户，供同事查看和处理您的事件。	在 CDO 联机帮助中，请参阅 创建新的 CDO 用户 。

使用系统日志将事件发送到 SAL (SaaS) 概述



①	管理中心 托管设备会生成事件。
②	威胁防御 设备将支持的事件作为系统日志消息发送到安装在网络中虚拟机上的 安全事件连接器 (SEC)。
③	SEC 将事件转发到 安全服务交换 (SSE)，这是一种安全的中间云服务，用于处理思科云安全产品中使用的云到云和场所到云的标识、身份验证和数据存储。
④	SSE 将事件转发到 Cisco Security Analytics and Logging (SAL) 云数据存储。

5	CDO 事件查看器查询 SAL 云数据存储中的事件，并为 SOC 分析师提供其他背景信息。
6	(仅具有分析许可证) Cisco Secure Cloud Analytics (以前称为 SWC) 从 SAL 云数据存储库接收事件，并为 SOC 分析师提供对产品分析功能的访问权限。



注释 CDO 门户中的大多数功能不适用于此集成。例如，CDO 不会管理您的设备，因此您的设备不会载入到 CDO。

从威胁防御设备发送安全事件系统日志消息

此程序记录从管理中心管理的威胁防御设备发送安全事件（连接、安全相关的连接、入侵、文件和恶意软件事件）的系统日志消息的最佳实践配置 devices。



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

- 在管理中心中，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）：
登录到 CDO。然后，从 CDO 浏览器窗口右上角的用户菜单中选择**安全连接器 (Secure Connectors)**。点击**安全事件连接器**，您将在右侧看到所需信息。
- 确保您的设备可以访问系统日志服务器。
- 请参阅管理中心 联机帮助中“连接日志记录”一章中的其他信息。

过程

步骤 1 登录到您的管理中心 Web 接口。

步骤 2 为威胁防御设备配置系统日志设置：

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

使用您从上面的 CDO 收集的 IP 地址、端口和协议。

此集成不支持 EMBLEM 格式和安全系统日志。

如果您对此页面上的选项有任何疑问，请参阅 管理中心 联机帮助中的“配置系统日志服务器”主题。

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) 确保未选择 **发送 EMBLEM 格式的系统日志**。

h) **保存** 您的设置。

步骤 3 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 **日志记录 (Logging)**。

d) 选择 **FTD 6.3 及更高版本**：使用在设备上部署的 FTD 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**。

g) 点击 **保存 (Save)**。

步骤 4 为访问控制策略启用安全相关的连接事件日志记录：

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 (Save)**。

步骤 5 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 **规则** 选项卡。

b) 点击要编辑的规则。

c) 点击规则中的 **日志记录 (Logging)** 选项卡。

d) 在连接开始和结束时启用。

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”。

请勿配置覆盖。

h) 点击 **添加 (Add)**。

i) 对策略中的每个规则重复上述步骤。

步骤 6 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**。
验证策略是否使用为访问控制日志记录配置的默认设置。
 - c) 点击 **Back**（返回）。
 - d) 点击左侧导航窗格中 **策略信息**。
 - e) 点击**确认更改 (Commit Changes)**。
-

下一步做什么

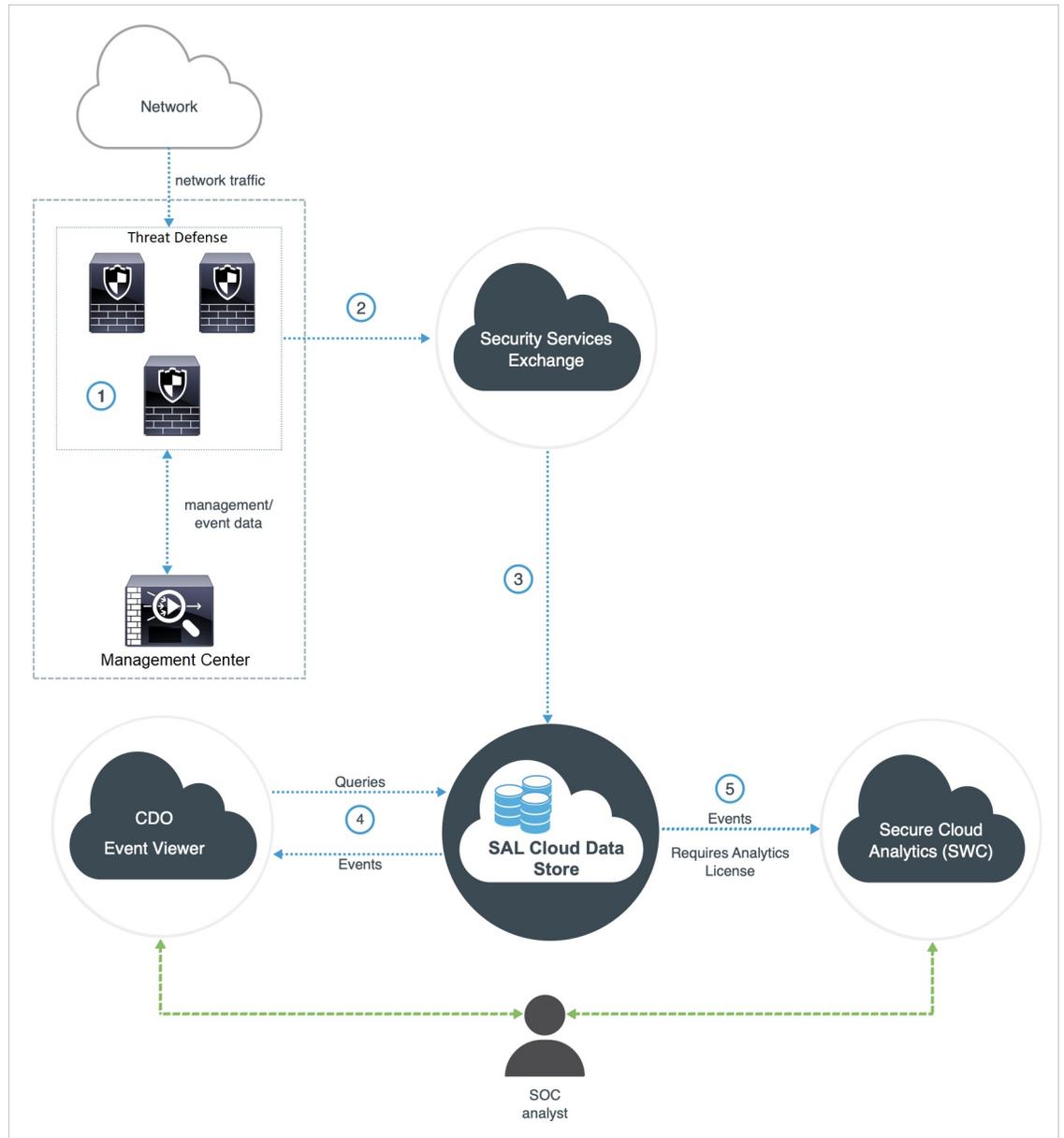
- 如果完成更改，请将更改部署到受管设备。

如何使用直接连接在 SAL (SaaS) 中设置事件数据存储

本部分介绍如何使用直接连接在 SAL (SaaS) 中设置事件数据存储。

工作原理

下图显示了直接集成的工作方式。



①	管理中心 托管设备会生成事件。
②	威胁防御 设备将支持的事件发送到 安全服务交换 (SSE)，这是一种安全的中间云服务，用于处理思科云安全产品中使用的云到云和场所到云的标识、身份验证和数据存储。
③	SSE 将事件转发到 Cisco Security Analytics and Logging (SAL) 云数据存储。
④	CDO 事件查看器查询 SAL 云数据存储中的事件，并为 SOC 分析师提供其他背景信息。

5	(仅具有分析许可证) Cisco Secure Cloud Analytics (以前称为 SWC) 从 SAL 云数据存储库接收事件, 并为 SOC 分析师提供对产品分析功能的访问权限。
---	--

此集成的关键组件

组件	说明
威胁防御	下一代防火墙, 具有防止恶意软件和应用层攻击、集成入侵防御和云提供的威胁情报等功能。
管理中心	在多个平台上运行的精选思科安全产品的管理神经中枢。它为端口和协议控制、应用程序控制、IPS、URL 过滤和恶意软件保护功能提供统一的威胁防御软件管理。
安全服务交换	一种安全的中间云服务, 用于处理思科云安全产品中使用的云到云和场所到云的标识、身份验证和数据存储。
CDO	<p>基于云的多设备管理器, 可用于管理各种安全产品的安全策略变更。此平台可在分支机构和其他高度分散的环境中高效管理策略, 以实现一致的安全实施。</p> <p>在直接集成中, 管理中心及其托管设备都会载入到 CDO 租户。此集成将管理中心连接到一套思科云服务。当管理中心载入 CDO 时, 您可以查看其托管设备, 查看管理网络对象, 并交叉启动到管理中心 UI 以管理关联的设备和对象。</p>
Cisco Secure Cloud Analytics (以前称为 Cisco Secure Network Analytics Cloud)	一个云平台, 可对威胁防御事件进行动态实体建模, 并根据这些信息生成检测结果。这提供了对从网络收集的遥测数据的更深入分析, 使您能够识别趋势并检查网络流量中的异常行为。

直接集成的前提条件

前提条件类型	要求
向 SAL (SaaS) 发送事件的一般要求	除了此表中的要求, 您还必须满足 SAL (SaaS) 集成的要求和前提条件, 第 2 页 和子主题中的项目。

前提条件类型	要求
许可	<p>将管理中心注册到思科智能软件管理器。</p> <p>在管理中心 Web 界面中，点击系统 (System) (⚙️) > 智能许可证 (Smart Licenses)，并验证：</p> <ul style="list-style-type: none"> • 使用授权 (Usage Authorization) 状态为已授权 (Authorized)。 • 产品注册 (Product Registration) 状态为已注册 (Registered)。 <p>请记住：</p> <ul style="list-style-type: none"> • 评估许可证不支持此集成。 • 您的环境不能使用思科智能软件管理器本地服务器（以前称为 Smart Software Satellite Server），也不能部署在气隙环境中。
账户	<ul style="list-style-type: none"> • 您必须具有已获得许可产品思科智能账户的管理员权限。 <p>要确定智能帐户用户角色，请执行以下操作：</p> <ol style="list-style-type: none"> 1. 转至 https://software.cisco.com。 2. 点击管理职能帐户 (Manage Smart Account)。 3. 在页面的右上角区域（“帮助”链接上方）选择智能帐户。 4. 点击用户 (Users) 选项卡。 5. 搜索您的用户 ID。 <ul style="list-style-type: none"> • 您的管理中心帐户必须具有以下用户角色之一： <ul style="list-style-type: none"> • 管理员 • 访问管理员 • 网络管理员 • 安全审批人 <p>要确定您的用户角色，请在管理中心 Web 界面中依次点击 系统 (System) (⚙️) > 用户 (Users)。</p> <ul style="list-style-type: none"> • 您的 CDO 帐户必须具有以下用户角色之一： <ul style="list-style-type: none"> • 管理员 • 超级管理员

直接集成的前提条件

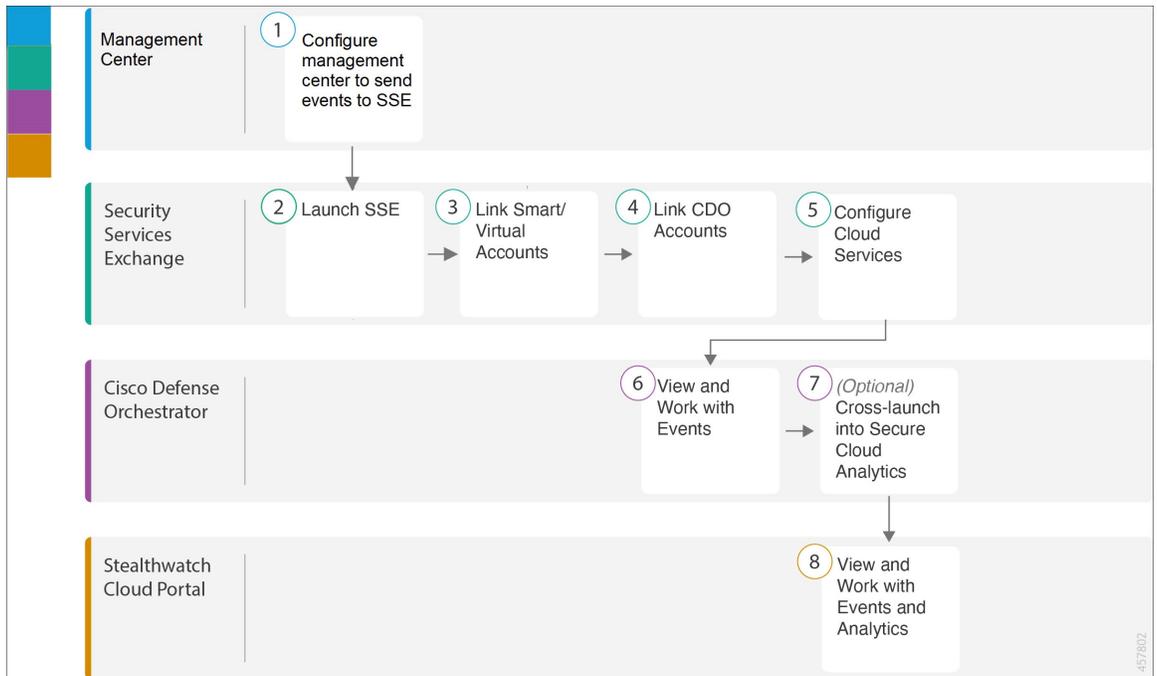
前提条件类型	要求
连接	

前提条件类型	要求
	<p>管理中心 和托管设备必须能够通过 443 端口向外连接以下地址的思科云：</p> <ul style="list-style-type: none"> • 北美洲云： <ul style="list-style-type: none"> • api-sse.cisco.com • mx*.sse.itd.cisco.com • eventing-ingest.sse.itd.cisco.com • defenseorchestrator.com • edge.us.cdo.cisco.com • 欧盟云： <ul style="list-style-type: none"> • api.eu.sse.itd.cisco.com • mx*.eu.sse.itd.cisco.com • eventing-ingest.eu.sse.itd.cisco.com • defenseorchestrator.eu • edge.eu.cdo.cisco.com • 亚洲 (APJC) 云： <ul style="list-style-type: none"> • api.apj.sse.itd.cisco.com • mx*.apj.sse.itd.cisco.com • eventing-ingest.apj.sse.itd.cisco.com • apj.cdo.cisco.com • edge.apj.cdo.cisco.com • 澳大利亚 <ul style="list-style-type: none"> • api.aus.sse.itd.cisco.com • mx*.aus.sse.itd.cisco.com • eventing-ingest.aus.sse.itd.cisco.com • aus.cdo.cisco.com • 印度 <ul style="list-style-type: none"> • api.in.sse.itd.cisco.com • mx*.in.sse.itd.cisco.com

前提条件类型	要求
	<ul style="list-style-type: none"> • eventing-ingest.in.sse.itd.cisco.com • in.cdo.cisco.com

使用直接连接设置 SAL (SaaS) 中的事件数据存储

执行以下任务，以使用直接集成在 SAL (SaaS) 中设置事件数据存储。



		工作空间
①	管理中心	<ul style="list-style-type: none"> • 将管理中心（版本 7.1 及更低版本）配置为将事件发送到安全服务交换，第 17 页。 • 配置，管理中心（7.2 和更高版本）以将事件发送至安全服务交换，第 18 页。
②	安全服务交换	启动安全服务交换，第 20 页
③	安全服务交换	在安全服务交换上关联智能帐户或虚拟帐户，第 20 页
④	安全服务交换	在安全服务交换上链接 CDO 帐户，第 22 页
⑤	安全服务交换	在安全服务交换上配置云服务，第 24 页

		工作空间
⑥	CDO	查看和处理事件，第 24 页
⑦	CDO	查看和处理思科安全云分析中的事件，第 25 页：交叉启动到 Cisco Secure Cloud Analytics
⑧	Cisco Secure Cloud Analytics	查看和处理思科安全云分析中的事件，第 25 页

将管理中心（版本 7.1 及更低版本）配置为将事件发送到 安全服务交换

如果您的管理中心版本为 7.1 或更早版本（版本 7.0.2 至 7.0.X 除外），请按照此程序将管理中心配置为让托管威胁防御设备直接向 SSE 发送事件。如果您的管理中心版本是 7.0.2 到 7.0.X，请按照[配置，管理中心（7.2 和更高版本）](#)以将事件发送至[安全服务交换](#)中的步骤操作。

开始之前

在管理中心 Web 界面中，执行以下操作：

- 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。创建必要的策略，并确保生成的事件如在管理中心 web 接口中的[分析 \(Analysis\)](#) 选项卡下如预期那样显示。

过程

步骤 1 在管理中心 Web 界面中，点击**系统 (System) > 集成 (Integration)**。

步骤 2 在**思科云区域 (Cisco Cloud Region)** 构件中，从**区域 (Region)** 下拉列表中选择区域云，然后点击**保存 (Save)**。

注释

如果管理中心已注册到所选区域云，则**保存 (Save)** 按钮将显示为非活动。

在此步骤中选择的区域也用于思科支持诊断和思科支持网络功能（如果适用并已启用）。

在选择区域云时，请考虑以下几点：

- 如果可能，请使用离您的部署最近的区域云。
- 不能汇聚或合并不同云中的数据。
- 如果需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。
- 您可以在每个区域云上创建一个帐户，并且每个云上的数据都保持独立。

步骤 3 在**思科云事件配置 (Cisco Cloud Event Configuration)** 构件中，将管理中心配置为将事件发送到 SSE。

1. 点击思科云事件配置 (Cisco Cloud Event Configuration) 滑块以启用整个配置。
2. 启用或禁用要发送到 SSE 的事件类型。

注释

多个集成可以使用您发送到云端的事件。请参阅下表：

集成	受支持的事件选项	备注
Security Analytics and Logging	全部	高优先级连接事件包括： <ul style="list-style-type: none"> • 安全相关的连接事件。 • 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 XDR	取决于您的版本： <ul style="list-style-type: none"> • 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 。

3. 点击保存 (Save)。

步骤 4 点击保存 (Save)。

下一步做什么

[启动安全服务交换，第 20 页](#)

配置，管理中心（7.2 和更高版本）以将事件发送至 安全服务交换

如果您的 管理中心 版本为 7.0.2 至 7.0.X 或 7.2 及更高版本，请按照此程序将 管理中心 配置为让受管设备将事件直接发送到 SSE。

开始之前

在 管理中心 Web 界面中，执行以下操作：

- 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。创建必要的策略，并确保生成的事件如在 管理中心 web 接口中的 **分析 (Analysis)** 选项卡下如预期那样显示。
- 启用 SecureX 或 思科安全云 集成，以便允许您的设备将防火墙事件发送到云。

过程

步骤 1 在管理中心中，导航至**集成 (Integration) > SecureX**（适用于管理中心版本 7.2.0 至 7.4.X），或导航至 **集成 (Integration) > 思科安全云 (Cisco Security Cloud)**（适用于管理中心版本 7.6.0 及更高版本）。

步骤 2（可选）从**当前区域 (Current Region)** 下拉列表中选择区域云。

在选择区域云时，请考虑以下几点：

- 如果可能，请使用离您的部署最近的区域云。
- 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。
- 您可以在每个区域云上创建一个帐户，并且每个云上的数据都保持独立。

步骤 3 选中**将事件发送到云 (Send events to the cloud)** 复选框。

步骤 4 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
Security Analytics and Logging	全部	高优先级连接事件包括： <ul style="list-style-type: none"> • 安全相关的连接事件。 • 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 XDR	取决于您的版本： <ul style="list-style-type: none"> • 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，还需要额外订购。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 (Intrusion Events)**，管理中心 设备会随影响标志一起发送事件数据。
- 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 点击保存 (Save)。

下一步做什么

[启动安全服务交换](#)，第 20 页

启动安全服务交换

过程

步骤 1 导航至 <https://admin.sse.itd.cisco.com/login>，然后点击登录 (Login)。

步骤 2 点击通过安全云登录 (Login via Security Cloud Sign On)，然后使用您的安全云登录帐户登录。

步骤 3 在出现提示时使用 Duo Security 完成身份验证，以获取对安全服务交换门户的访问权限。

下一步做什么

[在安全服务交换上关联智能帐户或虚拟帐户](#)，第 20 页

在安全服务交换上关联智能帐户或虚拟帐户

要将不同许可智能帐户（或虚拟帐户）下注册的产品整合到云中的单一视图中，必须将这些许可帐户链接到用于访问 SSE 的帐户。

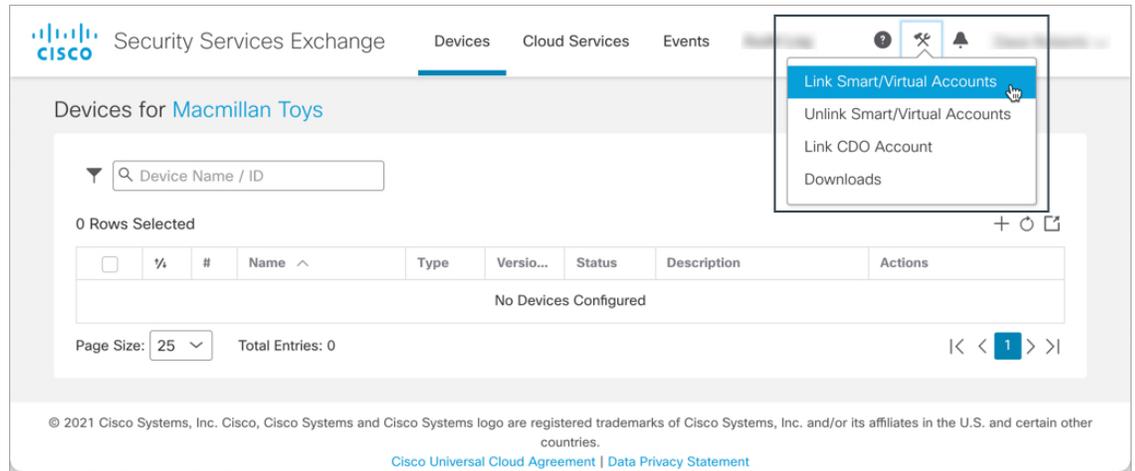
开始之前

- 要链接许可帐户，您必须为所有许可帐户（您的产品通过这些帐户获得许可）和您用来访问 SSE 的帐户拥有管理员级别的智能帐户或虚拟帐户权限。
- 如果您已关联用于思科 XDR 的帐户，则无需再次为 SAL (SaaS) 关联这些帐户。

过程

步骤 1 [启动安全服务交换](#)，第 20 页。

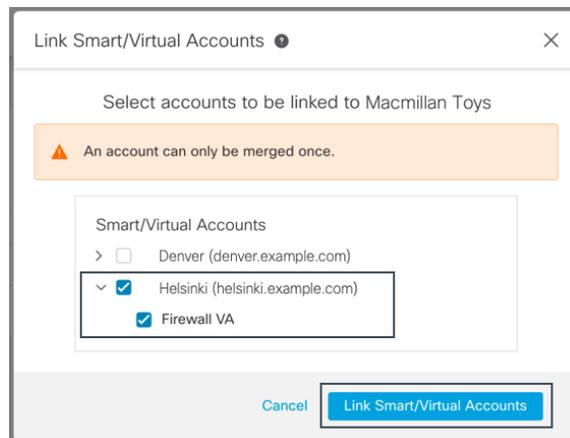
步骤 2 点击右上角的工具 (⚙) 按钮，然后选择关联智能/虚拟帐户 (Link Smart/Virtual Accounts)。



步骤 3 点击链接更多帐户 (**Link more accounts**)。

步骤 4 如果出现提示，请使用 Cisco.com 凭证登录。

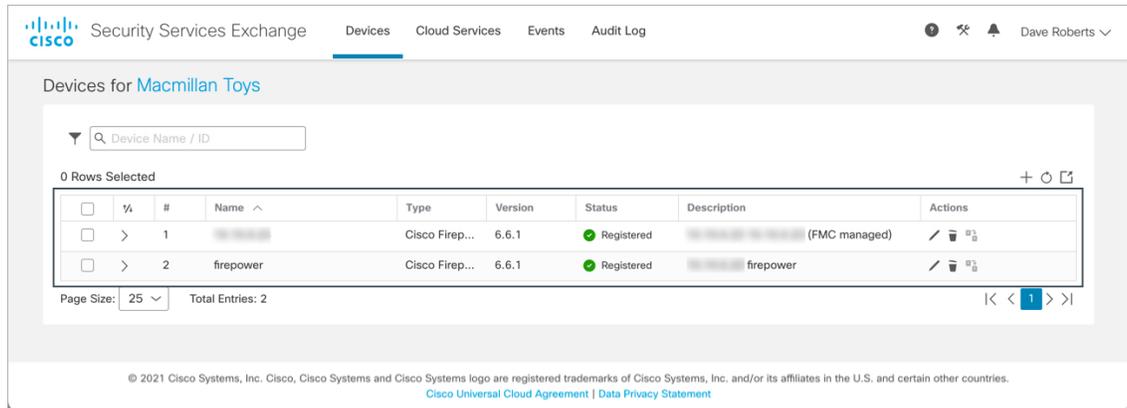
步骤 5 选择要与此云帐户集成的帐户。



步骤 6 点击链接智能/虚拟帐户 (**Link Smart/Virtual Accounts**)。

步骤 7 点击 **OK** 继续操作。

步骤 8 验证 管理中心 及其托管设备是否显示在设备 (**Devices**) 选项卡下。



下一步做什么

在安全服务交换上链接 CDO 帐户，第 22 页

在安全服务交换上链接 CDO 帐户

您必须将 CDO 帐户与 [SSE中与设备关联的帐户合并。请记住，如果您在多个区域云上有帐户，则必须为每个区域云单独合并帐户。

开始之前

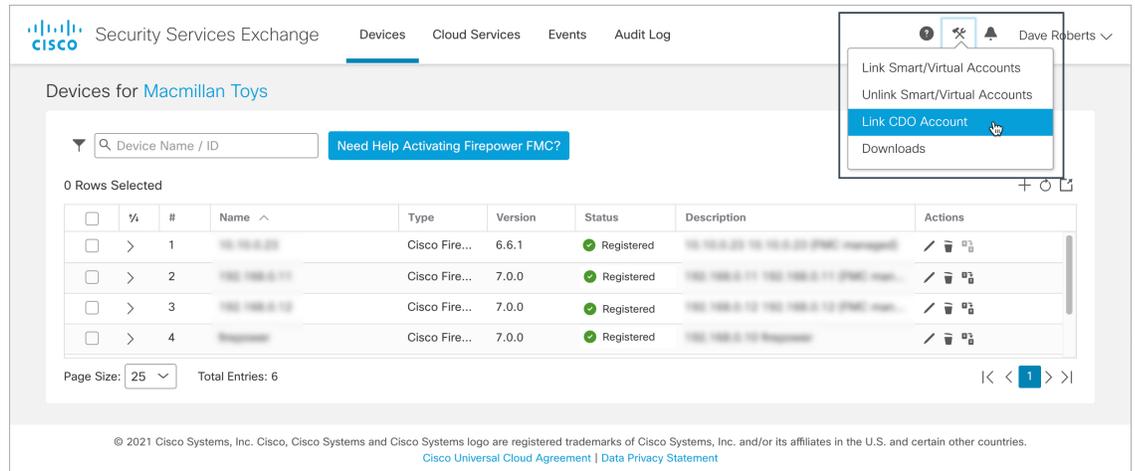
- 确保您的 CDO 帐户具有**管理员或超级管理员**权限。
- 在 CDO 中，执行以下操作为您的帐户生成新的 API 令牌：
 1. 登录到要合并的 CDO 帐户。
 2. 选择要合并的租户帐户。
 3. 从窗口右上角的用户菜单中选择**设置 (Settings)**。
 4. 在我的令牌 (**My Tokens**) 部分中，点击**生成 API 令牌 (Generate API Token)**或**刷新 (Refresh)**。
 5. 复制该令牌。

有关 API 令牌的详细信息，请参阅CDO联机帮助中的 [API 令牌](#)部分。

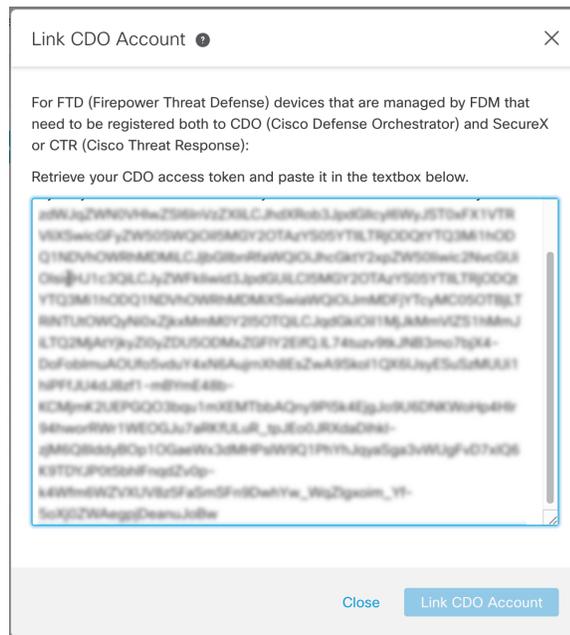
过程

步骤 1 转至安全服务交换 管理员门户。有关详细信息，请参阅[启动安全服务交换](#)，第 20 页。

步骤 2 点击右上角的工具 (🔧) 按钮，然后选择**关联 CDO 帐户 (Link CDO Account)**。



步骤 3 粘贴您从 CDO 复制的令牌。



步骤 4 确认您关联的是要关联的帐户，然后点击关联 CDO 帐户 (Link CDO Account)。

下一步做什么

在安全服务交换上配置云服务，第 24 页

在安全服务交换上配置云服务

过程

- 步骤 1 启动安全服务交换，第 20 页。
 - 步骤 2 点击云服务 (Cloud Services) 选项卡。
 - 步骤 3 验证是否已启用“事件处理服务” (Eventing services) 选项。
 - 步骤 4 验证事件 (Events) 选项卡下是否按预期显示了事件。
-

下一步做什么

- 查看和处理事件，第 24 页
- 查看和处理思科安全云分析中的事件，第 25 页

查看和处理事件

要查看和搜索云中的事件，请执行以下操作：

过程

- 步骤 1 使用浏览器转至您将事件发送到的区域 CDO 云：
 - 北美洲：
<http://www.defenseorchestrator.com>
 - 欧洲：
<http://www.defenseorchestrator.eu>
- 步骤 2 登录 CDO。
- 步骤 3 从导航栏中，选择监控 (Monitoring) > 事件日志记录 (Event Logging)。
- 步骤 4 使用历史 (Historical) 选项卡查看历史事件数据。默认情况下，查看器会显示此选项卡。
- 步骤 5 要查看实时事件，请点击实时 (Live) 选项卡。

有关在此页面上可以做什么的更多信息，请参阅 CDO 在线帮助中有关[查看事件](#)的说明。

下一步做什么

如果您有日志记录分析和检测 (**Logging Analytics and Detection**) 或全部网络分析和检测 (**Total Network Analytics and Detection**) 许可证, 请参阅 [CDO 在线帮助](#) 中的说明, 以交叉启动到 Stealthwatch 云门户。

查看和处理思科安全云分析中的事件

要在 Cisco Secure Cloud Analytics 中查看和搜索您的事件:

过程

步骤 1 使用要合并的帐户的凭证登录到相应的区域 CDO 站点。例如, 美国云为 <https://defenseorchestrator.com>, 欧盟云为 <https://defenseorchestrator.eu>。

步骤 2 从导航栏中点击 **监控 (Monitoring) > 安全分析 (Security Analytics)**。
Stealthwatch 云门户会在新浏览器标签中打开。

步骤 3 (一次性活动) 为确保事件无缝传输, 在使用事件查看器之前, 请在 Stealthwatch 云门户中执行以下操作:

1. 验证 Cisco Secure Cloud Analytics 是否与正确的 CDO 租户集成。要查看 CDO 租户, 请点击 **设置 (Settings) > 传感器 (Sensors)**。
2. 将要监控的子网添加到 Cisco Secure Cloud Analytics。要添加子网, 请点击 **设置 (Settings) > 子网 (Subnets)**。

有关详细信息, 请参阅 Cisco Secure Cloud Analytics 联机帮助。

步骤 4 要查看事件, 请点击 **调查 (Investigate) > 事件查看器 (Event Viewer)**。

有关详细信息, 请参阅 Cisco Secure Cloud Analytics 联机帮助。

常见问题解答

在哪里可以找到有关 **SAL** 的更多信息?

另请参阅 [SAL 入门和常见问题解答](#)。

是否需要将我的设备载入 **CDO**?

如果您使用直接连接发送事件, 管理中心 及其托管设备都会被载入到 CDO 租户。当管理中心 载入 CDO 时, 您可以查看其托管设备, 查看管理网络对象, 并交叉启动到 管理中心 UI 以管理关联的设备和对象。

如果我使用 思科 XDR，是否需要合并我的 CDO 帐户？

仅当您使用[如何使用直接连接](#)在 SAL (SaaS) 中设置事件数据存储，[第 10 页](#)中所述的过程将事件直接发送到云时。

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。