使用 Cisco Defense Orchestrator 管理 FDM 设备

首次发布日期: 2021 年 3 月 29 日

上次修改日期: 2022 年 2 月 3 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

目录

使用 Cisco Defense Orchestrator 管理 FDM 管理 设备

使用 Cisco Defense Orchestrator 管理 FDM 管理 设备

重要事项 Firepower 设备管理器 (FDM) 支持和功能仅应要求提供。如果您的租户上尚未启用 防火墙设备管理器 支持，则无法管理或部署到 FDM 管理 设备。向支持团队发送请求以启用此平台。通过 TAC 打开提交支持请求， 第 752 页

思科防御协调器 CDO 提供对 Firepower 设备管理器 设备的简化管理接口和云访问。FDM 管理 管理员会注意到 FDM 接口和 CDO 接口之间的许多相似之处。我们建立 CDO 的理念是让经理之间尽可能保持一致。

使用 CDO 管理物理或虚拟 FDM 管理 设备的以下方面：

- 载入 威胁防御 设备
- 设备管理
- 设备升级
- ASA 到 威胁防御 迁移
- 接口管理
- 路由
- 高可用性
- 安全策略
- 提升策略和配置一致性
- 站点间 VPN

使用 Cisco Defense Orchestrator 管理 FDM 管理 设备

- 远程接入 VPN
- 监控网络
- 思科安全分析和日志记录

软件和硬件支持

CDO 支持版本 6.4 及更高版本，可安装在许多不同的设备或虚拟机上。有关详细信息，请参阅 Secure Firewall Threat Defense 设备支持详情。

管理智能许可证

您可以在载入期间或将设备载入到 CDO 后，使用思科智能许可证来许可 FDM 管理 设备。智能许可内置于我们的工作流程中，可从 CDO 接口轻松访问。有关详细信息，请参阅 应用或更新智能许可证。

注释 如果要载入的设备运行的是软件版本 6.4 或 6.5，并且已获得智能许可，则该设备可能已向思科智能软件管理器注册。**您必须先从智能软件管理器取消注册该设备，然后再使用注册密钥将其载入 CDO**。取消注册时，与设备关联的许可证和所有可选许可证将在您的虚拟帐户中释放。

如果要载入的设备运行的是软件版本 6.6 及更高版本，并且已向思科云注册，**则必须先从思科云服务取消注册设备，然后再使用注册密钥将其载入 CDO**。

CDO 用户接口

CDO GUI 和 CLI 接口

CDO 是一种基于 Web 的管理产品，为您提供图形用户界面 (GUI) 和命令行接口 (CLI)，以便一次管理一个或多个设备。

使用 CLI 接口，您可以直接从 CDO 向 FDM 管理 设备发送命令。使用 CLI 宏保存和运行常用命令。有关详细信息，请参阅命令行接口文档和CDO 命令行接口 ， 第 96 页。

API 支持

CDO 提供可使用设备的 REST API 在 FDM 管理 设备上执行高级操作的 API 工具接口。此外，此接口还提供以下功能：

- 记录已执行的 API 命令的历史记录。
- 提供可重复使用的系统定义的 API 宏。
- 允许使用标准 API 宏、已执行的命令或其他用户定义的宏创建用户定义的 API 宏。

有关 API 工具的详细信息，请参阅使用 API 工具 ， 第 544 页。

使用 Cisco Defense Orchestrator 管理 FDM 管理 设备

载入 FDM 管理 设备

在载入 威胁防御 设备之前，请查看一般设备要求和载入必备条件。

最佳实践是使用注册令牌来载入 FDM 管理 设备。有关详细信息，请参阅使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+。

您还可以使用以下其他方法将 FDM 管理 设备载入 CDO：

- 使用用户名、密码和 IP 地址载入 FDM 管理 设备 ， 第 168 页
- 使用低接触调配载入 FDM 管理 设备的工作流程和必备条件
- 使用低接触调配载入 FDM 管理 设备的工作流程和必备条件 ， 第 179 页

设备管理

使用 CDO 为 FDM 管理 设备升级软件、配置高可用性并配置设备设置和网络资源。

- **系统设置**。获得 FDM 管理 设备的许可并将其载入后，即可FDM 管理 设备设置。您将能够配置管理访问协议、日志记录设置、DHCP 和 DNS 服务器交互、设备的主机名、设备使用的时间服务器以及 URL 过滤首选项。
- **安全数据库更新**。让您的设备保持最新状态并符合当前的更新FDM管理 设备安全数据库要求，以便在必要时检查和更新您的设备。
- **高可用性**。使用 升级 FDM 管理 高可用性对管理 HA 配置和操作。

设备升级

使用以下方法之一对 FDM 管理 设备执行即时升级或安排升级：

- 升级单个 FTD 设备。
- 批量 FDM 管理 设备升级。
- 升级 FDM 管理 高可用性对。

ASA 到 威胁防御 迁移

CDO 可帮助您将自适应安全设备 (ASA) 迁移到 FDM 管理 设备。CDO 提供了一个向导来帮助您将 ASA 的运行配置的这些元素迁移到 防火墙设备管理器 模板：

以下元素支持此迁移：

- 访问控制规则 (ACL)
- 接口
- 网络地址转换 (NAT) 规则
- 网络对象和网络组对象
- 路由

使用 Cisco Defense Orchestrator 管理 FDM 管理 设备

- 服务对象和服务组对象
- 站点间 VPN

有关详细信息，请参阅将 ASA 配置迁移到 FDM 管理 设备模板。

接口管理

您可以使用 CDO 配置 Firepower 接口。

路由

所谓路由是指通过网络将信息从源发送到目标的活动。路由涉及两个基本活动：确定最佳路由路径和通过网络传输数据包。使用 CDO 配置路由的以下方面：

- **配置静态路由和默认路由**。使用 CDO，您可以为 FDM 管理 设备默认路由。
- **网桥组支持**。网桥组是将一个或多个接口分组的虚拟接口。对接口分组的主要原因是创建一组交换接口。使用 CDO，您可以在设备上配置网桥组。
- **NAT（网络地址转换）**。NAT 规则有助于将流量从内部（专用）网络路由到互联网。NAT 规则还可以对网络外部的环境隐藏内部 IP 地址，从而发挥安全作用。您可以使用 CDO 创建和编辑设备的 NAT 规则。有关详细信息，请参阅网络地址转换 ， 第 399 页。

安全策略

安全策略检查网络流量，最终目标是允许网络流量到达或阻止网络流量到达其预定目的地。使用 CDO 管理设备的所有组件：

- **复制并粘贴规则**。通过将规则从策略复制并粘贴到另一个策略，可以轻松地跨策略共享规则。有关详细信息，请参阅复制 FDM 管理 访问控制规则。
- **SSL 解密策略**。某些协议（如 HTTPS）使用安全套接字层 (SSL) 或其后续版本传输层安全性 (TLS) 来加密流量以进行安全传输。由于系统无法检查加密连接，因此，如果要应用可考虑借助更高层流量特性进行访问决策的访问规则，则必须应用 SSL 解密策略将其解密。有关详细信息，请参阅 SSL 解密策略。
- **身份策略**。使用操作步骤从连接中收集用户身份信息。然后，可以在控制面板中基于用户身份查看使用情况，并根据用户或用户组配置访问控制。
- **安全情报策略**。通过 安全情报策略能够根据源/目标 IP 地址或目标 URL 提前丢弃非必要流量。在使用访问控制策略评估列入受阻列表的流量前，系统会将其丢弃，从而减少系统资源的使用量。
- **访问控制策略**。访问控制策略通过根据访问控制规则评估网络流量来控制对网络资源的访问。Firepower 设备管理器 会按照访问控制规则在访问控制策略中的显示顺序，将其与网络流量进行比较。当访问控制规则中的所有流量条件都匹配时，Firepower 设备管理器 将执行规则定义的操作。您可以使用 CDO 来配置 FDM 访问控制策略。
- TLS 1.3 安全身份发现。此功能在版本 6.7 中引入，允许您对使用 TLS 1.3 加密的流量执行 URL 过滤和应用控制。有关详细信息，请参阅 操作步骤。

使用 Cisco Defense Orchestrator 管理 FDM 管理 设备

- **入侵策略**。思科通过 Firepower 系统提供多种入侵策略。这些策略由思科 Talos 安全情报和研究小组设计，他们设定了入侵和预处理器规则的状态和高级设置。入侵策略是访问控制规则的方面。有关详细信息，请参阅 在 FDM 管理 访问控制规则中选择入侵策略。

注释 Snort 3 适用于运行版本 6.7 及更高版本的 FDM 管理 设备。请注意，您可以随意在 Snort 2 和 Snort 3 之间切换，但存在配置不兼容的风险。有关 Snort 3、支持的设备和软件以及任何限制的详细信息，请参阅升级到 Snort 3.0，第 219 页。

- **威胁事件**。威胁事件是在匹配思科 Talos 的入侵策略后已丢弃或已生成警报的流量的报告。在大多数情况下，无需调整 IPS 规则。如有必要，您可以选择通过更改 CDO 中的匹配规则操作来覆盖事件的处理方式。CDO 支持 6.4 和 6.6.1 的所有版本上的 IPS 规则调整。CDO 不支持任何版本 6.5、除 6.6.1 以外的任何 6.6 版本或任何 6.7 版本上的 IPS 规则调整。
- **NAT（网络地址转换）**。NAT 规则的处理顺序有助于将流量从内部（专用）网络路由到互联网。NAT 规则还可以对网络外部的环境隐藏内部 IP 地址，从而发挥安全作用。您可以使用 CDO 来创建和编辑 Firepower 威胁防御的 NAT 规则。

提升策略和配置一致性

对象管理

对象是可在一个或多个安全策略中使用的信息容器。对象使保持策略一致性变得容易，因为您可以修改对象，而该更改会影响使用该对象的所有其他策略。如果没有对象，则需要单独修改需要进行相同更改的所有策略。

使用 CDO 创建和管理以下对象类型：

- 创建或编辑 Active Directory 领域对象
- 上传 RA AnyConnect 客户端配置文件
- 应用过滤器对象
- 证书对象
- DNS 服务器组对象
- 地理位置对象
- 为 FDM 管理 设备配置身份源
- 管理 IKEv1 策略
- 管理 IKEv1 IPsec 提议对象
- 管理 IKEv2 策略
- 管理 IKEv2 IPsec 提议对象

使用 Cisco Defense Orchestrator 管理 FDM 管理 设备

- 创建或编辑 Firepower 网络对象或网络组
- 创建新的 RA VPN 组策略
- 安全区域对象
- 服务对象
- 安全组标记
- 创建和编辑系统日志服务器对象
- 创建或编辑 FDM 管理 URL 对象

解决对象问题

CDO 将多台设备上使用的对象称为“共享对象”，并在“对象”页面中使用此标记 进行标识。有时，共享对象会产生一些“问题”，并且不再在多个策略或设备之间完美共享。通过CDO，您可以轻松 解决重复对象问题、解决未使用的对象问题和 解决不一致的对象问题，从而管理您的设备和对象存储库。

模板

Firepower 设备管理器 模板是已载入的 FDM 管理 设备配置的完整副本。然后，您可以修改该模板并使用它来配置您管理的其他 FDM 管理 设备。Firepower 设备管理器 模板可促进设备之间的策略一致性。有关详细信息，请参阅 FDM 管理 设备模板。

高可用性

通过 CDO，可以轻松配置和管理创建 FDM 管理 高可用性对。您可以载入现有的 HA 对，也可以在 CDO 中创建 HA 对。HA 配置使得在设备可能不可用的情况下（例如在升级期间或设备意外故障期间）维护网络安全成为可能；在故障切换模式下，备用设备已配置为主用设备，这意味着即使其中一台 HA 设备不可用，另一台设备也会继续处理流量。

您可以在 CDO 中升级 FDM 管理 高可用性对。有关详细信息，请参阅升级 FDM 管理 高可用性对。

配置虚拟专用网络

站点间 VPN

虚拟专用网络 (VPN) 由多个远程对等体组成，这些对等体通过不安全的网络相互传输私有数据，从而实现网络到网络的连接。CDO 使用隧道将数据包封装在正常 IP 数据包中，以便通过基于 IP 的网络转发，使用加密来确保隐私，并使用身份验证来确保数据完整性。有关详细信息，请参阅站点间虚拟专用网络。

有关虚拟专用网络的其他信息，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》。

使用 Cisco Defense Orchestrator 管理 FDM 管理 设备

远程接入 VPN

远程访问 (RA) VPN 允许个人使用受支持的笔记本电脑、台式机和移动设备与您的网络建立安全连接。CDO 提供直观的用户界面，供您在 FDM 管理 设备上设置 RA VPN。AnyConnect 是终端设备上通过 RA VPN 连接 FDM 管理 设备的唯一受支持客户端。

CDO 支持 FDM 管理 设备上的 RA VPN 功能的以下方面：

- 传输层安全 (TLS) 或数据报传输层安全 (DTLS)，用于实现隐私、认证和数据完整性
- 基于 SSL 客户端的远程访问
- IPv4 和 IPv6 寻址
- 跨多台 FDM 管理 设备共享 RA VPN 配置

有关详细信息，请参阅监控远程访问虚拟专用网络会话。有关虚拟专用网络的其他信息，请参阅适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南。

监控网络

CDO 提供总结安全策略的影响的报告，以及查看这些安全策略触发的显着事件的方法。CDO 还会记录您对设备所做的更改，并为您提供一种标记这些更改的方法，以便您可以将您在CDO中所做的工作与帮助请求或其他操作请求相关联。

“执行摘要”报告

执行摘要报告显示操作统计信息的集合，例如加密流量、拦截的威胁、检测到的 Web 类别等。当网络流量触发 FDM 管理 设备上的访问规则或策略时，会生成报告中的数据。我们建议启用恶意软件和 许可证，并为访问规则启用文件日志记录，以允许设备生成反映在报告中的事件。

阅读 FDM 管理 设备执行摘要报告，了解有关报告内容以及如何使用它来改进网络基础设施的详细信息。要创建和管理报告，请参阅监控和报告。

思科安全分析和日志记录

思科安全分析和日志记录允许您从所有 FDM 管理 设备捕获连接、入侵、文件、恶意软件和安全情报事件，并在 CDO 中的一个位置进行查看。

事件存储在思科云中，可从CDO中的“事件日志记录”页面查看，您可以在其中过滤和查看事件，以便清楚地了解在网络中触发的安全规则。**日志记录和故障排除** 软件包为您提供这些功能。

使用 **防火墙分析和监控** 软件包，系统可以将安全云分析动态实体建模应用于 FDM 管理 设备事件，并使用行为建模分析生成安全云分析观察结果和警报。如果您获取**全部网络分析和监控** 软件包，则系统会对 FDM 管理 设备事件和网络流量应用动态实体建模，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安全云分析门户。有关详细信息，请参阅关于安全分析和日志记录 (SaaS)。

变更日志

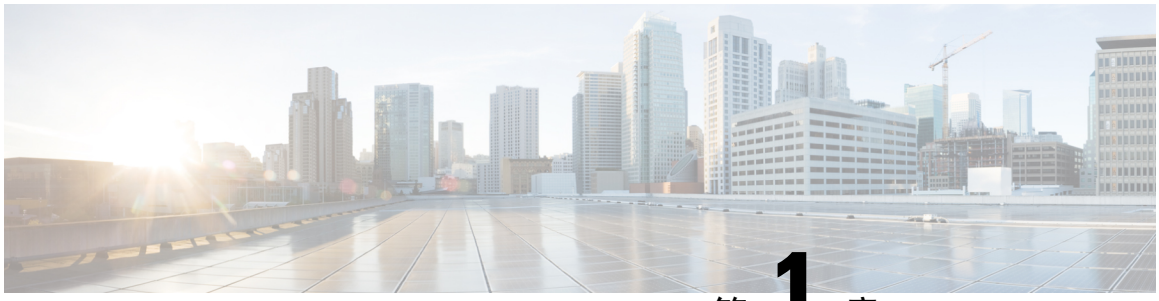
变更日志，第 573 页 会持续捕获在 CDO 中进行的配置更改。此单一视图包括所有受支持设备和服务的更改。以下是更改日志的一些功能：

使用 Cisco Defense Orchestrator 管理 FDM 管理 设备

- 并排比较对设备配置所做的更改
- 所有更改日志条目的纯英文标签。
- 记录设备的自行激活和删除。
- 检测在 CDO 之外发生的策略更改冲突。
- 回答事件调查或故障排除期间的人员、内容和时间。
- 可以将完整更改日志或仅一部分下载为 CSV 文件。

更改请求管理

更改请求管理允许您将在第三方故障单系统中打开的变更请求及其业务理由与变更日志中的事件相关联。使用更改请求管理在CDO中创建更改请求，使用唯一名称进行标识，输入更改说明，并将更改请求与更改日志事件相关联。您可以稍后在更改日志中搜索更改请求名称。



第 1 章

Cisco Defense Orchestrator 基础知识

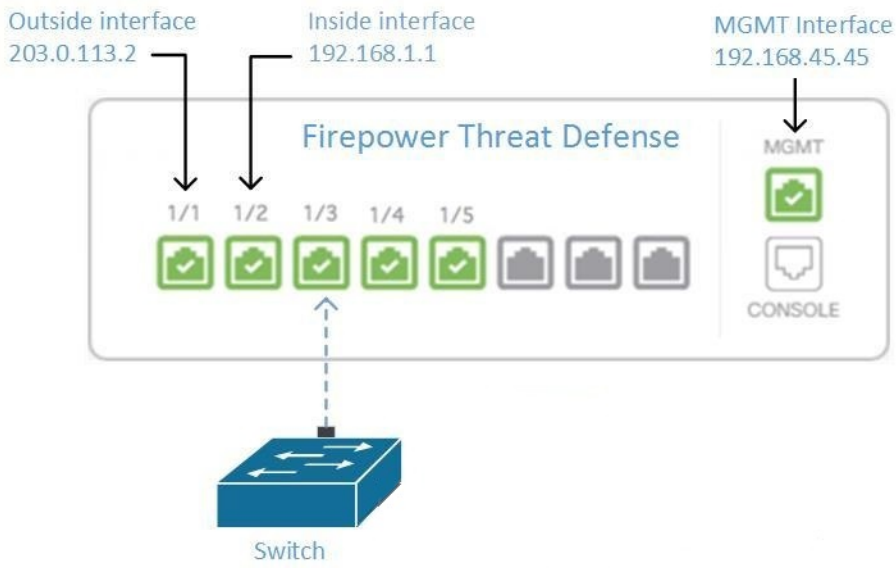
( ) 通过清晰简洁的界面提供策略管理的独特视图。思科防御协调器CDO以下主题介绍了首次使用的基础知识。CDO

联网要求

从内部接口管理设备FDM 管理

如果为专用MGMT接口分配了在您的组织内不可路由的地址，则可能需要使用内部接口管理设备；例如，它可能只能从您的数据中心或实验中访问。FDM 管理

Figure 1: 接口地址



远程接入 VPN 要求

如果您使用 CDO 管理的设备将管理远程接入 VPN (RA VPN) 连接，则 CDO 必须使用内部接口管理设备。FDM 管理

后续操作：

继续，了解配置设备的程序。从内部接口管理设备FDM 管理, on page 3FDM 管理

从内部接口管理设备FDM 管理

此配置方法：

- 假定设备尚未自行激活。FDM 管理CDO
- 将数据接口配置为内部接口。
- 配置内部接口以接收 MGMT 流量 (HTTPS)。
- 允许云连接器的地址到达设备的内部接口。

Before you begin

在以下主题中查看此配置的前提条件：

- 从内部接口管理设备FDM 管理, on page 2
- 将 思科防御协调器 连接到托管设备, on page 11

Procedure

步骤 1 登录Firepower 设备管理器。

步骤 2 在系统设置菜单中，点击管理访问。

步骤 3 点击数据接口选项卡，然后点击创建数据接口。

a. 在接口字段中，从接口列表中选择预先命名为“内部”的接口。

b. 在协议字段中，选择 HTTPS（如果尚未选择）。

c. 在允许的网络 (Allowed Networks) 字段中，选择代表将允许访问设备内部地址的组织内部网络的网络对象。FDM 管理SDC 或云连接器的 IP 地址应在允许访问设备内部地址的地址中。

在接口地址图中，SDC 的 IP 地址 192.168.1.10 应该能够到达 192.168.1.1。#unique_67 unique_67_Connect_42_ftd-interf-addrss, on page 3

步骤 4 部署更改。您现在可以使用内部接口管理设备。

What to do next

如果您使用的是云连接器，该怎么办？

使用上述程序并添加以下步骤：

- 将外部接口 (203.0.113.2)“NAT”添加到内部接口 (192.168.1.1)。
- 在上述程序的步骤 3c 中，“允许的网络”是包含云连接器的公共 IP 地址的网络组对象。
- 添加创建访问控制规则的步骤，允许从云连接器的公共 IP 地址访问外部接口 (203.0.113.2)。

如果您是欧洲、中东或非洲 (EMEA) 的客户，并且连接到 ，则这些是云连接器的公共 IP 地址：CDOhttps://defenseorchestrator.eu/

- 35.157.12.126
- 35.157.12.15

如果您是美国的客户，并且连接到，云连接器的这些公共 IP 地址：CDOhttps://defenseorchestrator.com/

- 52.34.234.2
- 52.36.70.147

如果您是**亚太地区-日本-中国 (AJPC)** 地区的客户，并且您通过 https://www.apj.cdo.cisco.com/ 连接到 CDO，请允许来自以下 IP 地址的入站访问：

- 54.199.195.111
- 52.199.243.0

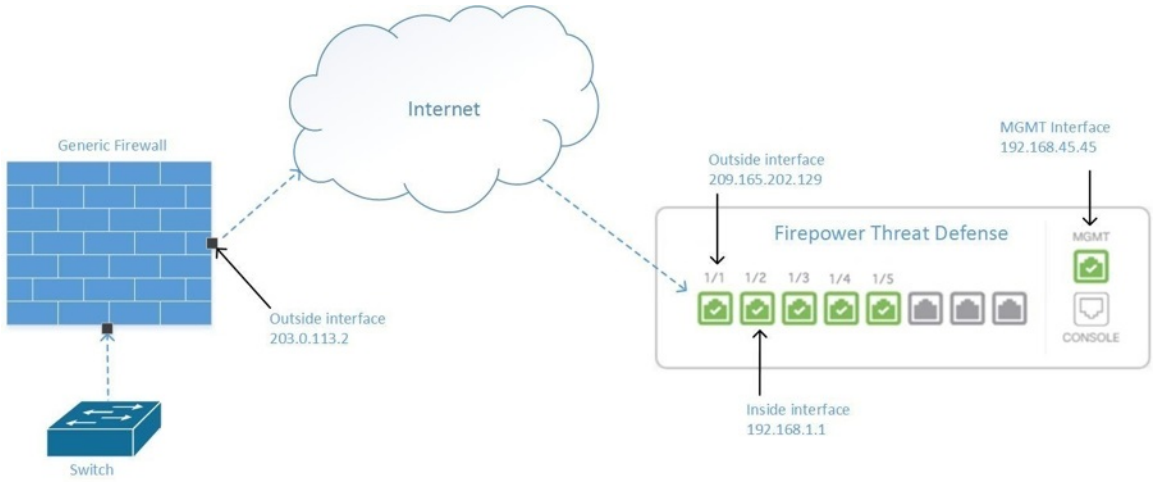
载入 FDM 管理 设备

推荐的自行激活设备的方法是使用注册令牌自行激活方法。FDM 管理CDO将内部接口配置为允许从云连接器对设备进行管理访问后，使用用户名和密码载入设备。FDM 管理FDM 管理有关详细信息，请参阅载入 威胁防御 设备。您将使用内部接口的 IP 地址进行连接。在上面的场景中，该地址是 192.168.1.1。

从外部接口管理设备FDM 管理

如果您有一个分配给分支机构的公共 IP 地址，并使用另一个位置的云连接器进行管理，则可能需要从外部接口管理设备。云交付的防火墙管理中心思科防御协调器

Figure 2: 外部接口上的设备管理



此配置并不意味着物理 MGMT 接口不再是设备的管理接口。如果您在设备所在的办公室，您将能够连接到 MGMT 接口的地址并直接管理设备。云交付的防火墙管理中心

远程接入 VPN 要求

如果您管理的设备将管理远程接入 VPN (RA VPN) 连接， 将无法使用外部接口管理设备。云交付的防火墙管理中心云交付的防火墙管理中心云交付的防火墙管理中心请参阅从内部接口管理设备。从内部接口管理设备FDM 管理

后续操作：

继续，了解配置设备的程序。管理设备的外部接口FDM 管理, on page 5云交付的防火墙管理中心

管理设备的外部接口FDM 管理

此配置方法：

1. 假定设备尚未自行激活。FDM 管理CDO
2. 将数据接口配置为外部接口。

3. 在外部接口上配置管理访问。
4. 允许云连接器的公共 IP 地址（通过防火墙进行 NAT 后）到达外部接口。

Before you begin

在以下主题中查看此配置的前提条件：

- 管理设备的外部接口FDM 管理, on page 5
- 将 思科防御协调器 连接到托管设备, on page 11

Procedure

步骤 1 登录Firepower 设备管理器。

步骤 2 在系统设置菜单中，点击管理访问。

步骤 3 点击数据接口选项卡，然后点击创建数据接口。

a. 在接口字段中，从接口列表中选择预先命名为“外部”的接口。

b. 在协议字段中，选择 HTTPS（如果尚未选择）。只需要 HTTPS 访问。CDO

c. 在允许的网络 (Allowed Networks) 字段中，创建一个主机网络对象，其中包含云连接器通过防火墙的 NAT 后面向公众的 IP 地址。

在从外部接口进行设备管理的网络图中，云连接器的 IP 地址 10.10.10.55 将通过 NAT 转换为 203.0.113.2。#unique_71 unique_71_Connect_42_ftd-mgmt-out-addrss, on page 5对于允许的网络，您将创建一个值为 203.0.113.2 的主机网络对象。

步骤 4 在 中创建访问控制策略，允许从SDC或云连接器的公共IP地址到设备外部接口的管理流量(HTTPS)。Firepower 设备管理器FDM 管理在此场景中，源地址为 203.0.113.2，源协议为 HTTPS；目的地址为 209.165.202.129，协议为 HTTPS。

步骤 5 部署更改。您现在可以使用外部接口管理设备。

What to do next

如果您使用的是云连接器，该怎么办？

该过程非常相似，但有两点不同：

- 在上述程序的步骤 3c 中，“允许的网络”是包含云连接器的公共 IP 地址的网络组对象。
  - 如果您是欧洲、中东或非洲 (EMEA) 的客户，并且连接到，则这些是云连接器的公共 IP 地址：CDOhttps://defenseorchestrator.eu/
    - 35.157.12.126
    - 35.157.12.15

- 如果您是美国的客户，并且连接到 ，则这些是云连接器的公共 IP 地址：CDOhttps://defenseorchestrator.com/
  - 52.34.234.2
  - 52.36.70.147
- 如果您是**亚太地区-日本-中国 (AJPC)** 地区的客户，并且您通过 https://www.apj.cdo.cisco.com/ 连接到 CDO，请允许来自以下 IP 地址的入站访问：
  - 54.199.195.111
  - 52.199.243.0

- 在上述程序的第 4 步中，创建一个允许从云连接器的公共 IP 地址访问外部接口的访问控制规则。

注册令牌自行激活方法是将设备自行激活到的推荐方法。使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+, on page 175FDM 管理CDO将外部接口配置为允许从云连接器进行管理访问后，载入设备。FDM 管理您将使用外部接口的 IP 地址进行连接。在我们的场景中，该地址是 209.165.202.129。

请求 CDO 租户

您可以申请 CDO 租户的 30 天免费试用，以自行激活和管理您的设备。然后，您可以联系思科客户团队将您的租户升级到许可的租户。

准备工作

如果尚未创建 SecureX 帐户，请创建一个。请参阅创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证。

操作步骤

1. 转至https://www.defenseorchestrator.com/new。
2. 选择要调配 CDO 租户的区域。
3. 点击 Sign Up with SecureX。
4. 使用您的 SecureX 账户登录。

   成功登录后，您将收到一封电子邮件，其中包含您注册的电子邮件 ID 上的租户详细信息。系统将在您选择的区域中创建一个新的 CDO 租户。按照邮件中的说明访问新的 CDO 租户。

   有关首次登录 CDO 租户的信息，请参阅新 CDO 租户的初始登录。

   有关管理 CDO 租户和各种租户设置的信息，请参阅新 CDO 租户的初始登录。

请求额外的 CDO 租户

如果要为现有租户创建其他租户，请联系您的客户经理。

许可证

要从 自行激活和管理设备，您需要根据要管理的设备购买基本订用和设备特定的期限订用。思科防御协调器

关于许可证

CDO需要基本订用租户授权和设备许可证来管理设备。您可以根据所需的租户数量购买一个或多个基本订用，并根据设备型号和数量购买设备许可证。CDO换句话说，购买基本订用会为您提供一个租户，对于您选择使用的每台设备，您都需要单独的设备许可证。CDOCDO出于规划部署的目的，请注意，每个租户可以通过安全设备连接器 (SDC) 管理大约 500 台设备，并使用云连接器管理任意数量的设备。CDO有关详细信息，请参阅安全设备连接器 (SDC)。https://www.cisco.com/c/en/us/td/docs/security/cdo/managing-asa-with-cdo/managing-asa-with-cisco-defense-orchestrator/basics-of-cisco-defense-orchestrator.html#Cisco_Concept.dita_e19faf6e-4e1b-4bb3-ad82-48a080430e8c

订用

思科防御协调器 订用是基于期限的：

- 基本 - 提供一年、三年和五年订用，并提供访问租户和自行激活充分许可设备的权利。CDO
- 设备许可证 - 为您选择管理的任何受支持设备提供一年、三年和五年的订用。例如，如果您购买了思科 Firepower 1010 设备的三年软件订用，则可以选择使用 管理思科 Firepower 1010 设备三年。云交付的防火墙管理中心CDO

有关 支持的思科安全设备的详细信息，请参阅 CDO 支持的软件和硬件。https://docs.defenseorchestrator.com/#!c-software-and-hardware-supported-by-cdo.htmlCDO

重要事项 您不需要两个单独的设备许可证来管理高可用性设备对。CDO如果您有安全防火墙 ASA (ASA) 或安全防火墙威胁防御 (FTD) 高可用性对，则购买一个 ASA 或 FTD 设备许可证就足够了，因为会将高可用性设备对视为一台设备。CDO

注释 您无法通过思科智能许可门户管理许可。CDO

软件订用支持

基本订用包括在订用期限内有效的软件订用支持，并可免费访问软件更新、主要升级和思科技术支持中心 (TAC)。CDO虽然默认选择软件支持，但您也可以根据自己的要求利用解决方案支持。CDO

评估许可证

思科防御协调器 试用期许可证

您可以从您的 SecureX 账户申请 30 天试用。思科防御协调器 有关详细信息，请参阅请求 CDO 租户。https://docs.defenseorchestrator.com/#!c-provision-cdo-tenant-securex.html

云交付的防火墙管理中心 评估许可证

提供 90 天的评估许可证，在此之后，服务将被阻止。云交付的防火墙管理中心威胁防御

要了解如何在租户上调配，请参阅为租户请求 。云交付的防火墙管理中心CDO云交付的防火墙管理中心CDO

云交付防火墙管理中心和威胁防御许可证

您无需购买单独的许可证即可在 中使用 ；租户的基本订用包括的成本。云交付的防火墙管理中心CDOCDO云交付的防火墙管理中心

注释 不支持气隙网络中的设备的特定许可证预留 (SLR)。云交付的防火墙管理中心

云交付防火墙管理中心的威胁防御许可证

您需要为 管理的每台设备购买单独的许可证。Secure Firewall Threat Defense云交付的防火墙管理中心有关详细信息，请参阅使用 *Cisco* 防御协调器中的云交付防火墙管理中心管理防火墙威胁防御中的许可证。

要了解如何处理迁移到的设备的许可，请参阅将威胁防御从管理中心迁移到云。CDO云交付的防火墙管理中心https://www.cisco.com/c/en/us/td/docs/security/cdo/cloud-delivered-firewall-management-center-in-cdo/managing-firewall-threat-defense-services-with-cisco-defense-orchestrator/m-change-firewall-threat-defense-device-management-from-secure-firewall-management-center-to-cdo.html#Cisco_Concept.dita_f7a16928-88d3-420a-9dc6-84c35fdd406b

更多支持的设备和许可证

除了通过Secure Firewall Threat Defense支持云交付的防火墙管理中心设备外，CDO 还管理以下设备：

- Cisco Secure Firewall ASA
- Cisco Secure Firewall Cloud Native
- 本地 Cisco Secure Firewall Management Center
- 思科 Meraki MX 安全设备
- 思科 IOS 设备

- 可使用 SSH 访问的设备
- Amazon Web 服务 (AWS) 虚拟私有云 (VPC)
- Duo 管理面板
- Umbrella 组织

您将需要CDO基本授权许可证和特定于要管理的设备的许可证。

安全设备连接器 (SDC)

使用设备凭证将设备载入CDO时，CDO认为最佳实践是在网络中下载并部署安全设备连接器(SDC)，以代理设备与 CDO 之间的通信。但是，如果您愿意，可以使设备通过其外部接口从 CDO 接收直接通信。自适应安全设备 (ASA)、FDM 管理 设备、Firepower 管理中心 (FMC)、安全防火墙云原生设备以及 SSH 和 IOS 设备都可以使用 SDC 载入 CDO。

SDC 监控需要在受管设备上执行的命令，以及需要发送到受管设备的消息。SDC 代表 CDO 执行命令，代表受管设备向 CDO 发送消息，并将受管设备的应答返回给 CDO。

SDC 使用通过 HTTPS (TLS 1.2) 的 AES-128-GCM 签名和加密的安全通信消息与 CDO 通信。载入的设备和服务的所有凭证都会直接从浏览器加密到 SDC，并使用 AES-128-GCM 进行静态加密。只有 SDC 可以访问设备凭证。其他 CDO 服务均无权访问凭证。有关如何允许在 SDC 和 CDO 之间通信的信息，请参阅将 思科防御协调器 连接到托管设备 ， 第 11 页。

SDC 可以安装在设备上，作为虚拟机监控程序上的虚拟机，也可以安装在 AWS 或 Azure 等云环境中。您可以使用 CDO 提供的组合虚拟机和 SDC 映像安装 SDC，也可以创建自己的虚拟机并在其上安装 SDC。SDC 虚拟设备包括 CentOS 操作系统，并在 Docker 容器中运行。

每个 CDO 租户可以拥有无限数量的 SDC。这些 SDC 不会在租户之间共享，而是专用于单个租户。单个SDC可以管理的设备数量取决于这些设备上实施的功能及其配置文件的大小。但是，出于规划部署的目的，预计一个 SDC 可支持大约 500 台设备。

为租户部署多个 SDC 还具有以下优势：

- 您可以使用 CDO 租户管理更多设备，而不会降低性能。
- 您可以将SDC部署到网络中的隔离网段，并且仍然使用相同的CDO租户管理该网段中的设备。如果没有多个 SDC，您将需要使用不同的 CDO 租户管理这些隔离网段中的设备。

部署第二个或后续 SDC 的程序与部署第一个 SDC 的程序相同。租户上的初始 SDC 包含租户的名称和数字 1，并显示在 CDO 的“安全连接器” 页面上。每个额外的 SDC 都按顺序编号。请参阅使用 CDO 的 VM 映像部署安全设备连接器 ， 第 13 页和在您自己的虚拟机上部署安全设备连接器 ， 第 17 页

相关信息：

- 将 思科防御协调器 连接到托管设备
- 对安全设备连接器进行故障排除 ， 第 699 页

• 更新您的安全设备连接器，第 27 页
• 删除安全设备连接器，第 24 页

将 思科防御协调器 连接到托管设备

CDO 通过云连接器或安全设备连接器 (SDC) 连接到其管理的设备。

如果可以直接从互联网访问您的设备，则应使用云连接器连接到您的设备。如果可以将设备配置为，则允许从云区域中的 CDO IP 地址对端口 443 进行入站访问。

如果无法从互联网访问您的设备，您可以在网络中部署本地 SDC，以允许 CDO 与您的设备进行通信。如果您可以将设备配置为，则允许端口 443（或您为设备管理配置的任何端口）上的完全入站访问。

无论 FDM 管理 设是否可直接从互联网访问，都可以使用其设备凭证、注册密钥或其序列号载入 CDO。如果 FDM 管理 设备没有直接访问互联网的权限，但它驻留在有互联网访问权限的网络上，则作为设备一部分提供的 安全服务交换 连接器可以访问 安全服务交换 云，从而允许 FDM 管理 设备载入。有关不同自行激活方法的详细信息，请参阅载入 威胁防御 设备, on page 161。

您的网络中需要有本地 SDC 才能载入：

- 无法从云访问的 ASA 设备。
- 使用无法从云和“凭证载入”方法访问的 FDM 管理 设备。
- Cisco IOS 设备。
- 具有 SSH 访问权限的设备。

所有其他设备和服务都不需要本地 SDC。CDO 将使用其“云连接器”进行连接。请参阅下一部分，了解入站访问必须允许的 IP 地址。

通过云连接器将设备连接到 CDO

通过云连接器将 CDO 直接连接到您的设备时，您应允许 EMEA、美国或 APJC 区域中的各种 IP 地址在端口 443（或您为设备管理配置的任何端口）上进行入站访问。

如果您是**欧洲、中东或非洲 (EMEA)** 地区的客户，并且您在 https://defenseorchestrator.eu/ 连接到 CDO，请允许从以下 IP 地址进行入站访问：

- 35.157.12.126
- 35.157.12.15

如果您是**美国**地区的客户，并且您通过 https://defenseorchestrator.com 连接到 CDO，请允许从以下 IP 地址进行入站访问：

- 52.34.234.2
- 52.36.70.147

如果您是**亚太地区-日本-中国 (APJC)** 地区的客户，并且您通过 https://www.apj.cdo.cisco.com/ 连接到 CDO，请允许来自以下 IP 地址的入站访问：

- 54.199.195.111
- 52.199.243.0

使用 SDC 将设备连接到 CDO

当通过 SDC 将 CDO 连接到您的设备时，您希望 CDO 管理的设备必须允许在端口 443（或您为设备管理配置的任何端口）上进行完全入站访问。这是使用管理访问控制规则配置的。

您还必须确保部署了 SDC 的虚拟机与受管设备的管理接口建立了网络连接。

将 ASA 或 Cisco Secure Firewall Cloud Native 连接到 SDC 的特殊注意事项

具体而言，对于 ASA 或 Cisco Secure Firewall Cloud Native，SDC 使用与 ASDM 相同的安全通信通道。

如果管理的 ASA 或 Cisco Secure Firewall Cloud Native 也配置为接受 AnyConnect VPN 客户端连接，则必须将 ASDM HTTP 服务器端口更改为 1024 或更高的值。请注意，此端口号将与将 ASA 或 Cisco Secure Firewall Cloud Native 设备载入 CDO 时使用的端口号相同。

ASA 或 Cisco Secure Firewall Cloud Native 命令示例

以下示例假定 ASA 或 Cisco Secure Firewall Cloud Native 外部接口名为“outside”，并且在 ASA 或 Cisco Secure Firewall Cloud Native 上配置了 AnyConnect 客户端，因此 ASDM HTTP 服务器正在侦听端口 8443。

要启用外部接口，请输入以下命令：

欧洲、中东和非洲地区：

http 35.157.12.126 255.255.255.255 outside

http 35.157.12.15 255.255.255.255 outside

美国：

http 52.34.234.2 255.255.255.255 outside

http 52.36.70.147 255.255.255.255 outside

亚太地区-日本-中国地区：

http 54.199.195.111 255.255.255.255 outside

http 52.199.243.0 255.255.255.255 outside

要启用 ASDM HTTP 服务器端口，在使用 AnyConnect VPN 客户端的情况下，请输入以下命令：

http server enable 8443

使用 CDO 的 VM 映像部署安全设备连接器

使用设备凭证将 CDO 连接到设备时，最佳做法是在网络中下载并部署 SDC，以管理 CDO 与设备之间的通信。通常，这些设备不是基于边界的，没有公共 IP 地址，或者具有通往外部接口的开放端口。自适应安全设备 (ASA)、FDM 管理 设备、Firepower 管理中心 (FMC)、安全防火墙云原生设备以及 SSH 和 IOS 设备都可以使用 SDC 载入 CDO。

SDC 监控需要在受管设备上执行的命令，以及需要发送到受管设备的消息。SDC 代表 CDO 执行命令，代表受管设备向 CDO 发送消息，并将受管设备的应答返回给 CDO。

单个SDC可以管理的设备数量取决于这些设备上实施的功能及其配置文件的大小。但是，出于规划部署的目的，我们预计一个 SDC 可支持大约 500 台设备。有关详细信息，请参阅在单个 CDO 租户上使用多个 SDC，第 27 页。

此程序介绍如何使用 CDO 的 VM 映像在网络中安装 SDC。这是创建 SDC 的首选、最简单、最可靠的方法。如果需要使用您创建的 VM 创建 SDC，请执行 在您自己的虚拟机上部署安全设备连接器，第 17 页。

开始之前

在部署 SDC 之前，请查看以下前提条件：

- CDO 需要严格的证书检查，并且不支持 SDC 和互联网之间的 Web/内容代理。如果使用代理服务器，请禁用对安全设备连接器 (SDC) 和 CDO 之间的流量进行检查。
- SDC 必须在 TCP 端口 443 或您为设备管理配置的端口上具有对互联网的完全出站访问权限。CDO 管理的设备还必须允许来自此端口的入站流量。
- 查看 将 思科防御协调器 连接到托管设备 以确保适当的网络访问。
- CDO 支持使用 vSphere Web 客户端或 ESXi Web 客户端安装其 SDC VM OVF 映像。
- CDO 不支持使用 vSphere 桌面客户端安装 SDC VM OVF 映像。
- ESXi 5.1 虚拟机监控程序。
- Cent OS 7 访客操作系统。
- 仅具有一个 SDC 的 VMware ESXi 主机的系统要求：
  - VMware ESXi 主机需要 2 个 CPU。
  - VMware ESXi 主机至少需要 2 GB 内存。
  - VMware ESXi 需要 64 GB 磁盘空间来支持虚拟机，具体取决于您的调配选择。
- 具有 SDC 和租户的**单个**安全事件连接器 (SEC) 的 VM 的系统要求。（SEC 是关于安全分析和日志记录 (SaaS)中使用的组件）。

  添加到 VMware ESXi 主机的每个 SEC 都需要额外的 4 个 CPU 以及额外的 8 GB 内存。

  因此，以下是对具有一个 SDC 和一个 SEC 的 VMware ESXi 主机的要求：
  - VMware ESXi 主机需要 6 个 CPU。

- VMware ESXi 主机至少需要 10 GB 内存。
- VMware ESXi 需要 64 GB 磁盘空间来支持虚拟机，具体取决于您的调配选择。

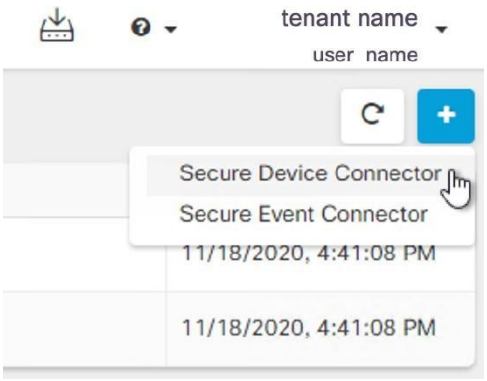
- Docker 的 IP 必须与 SDC 的 IP 范围和设备 IP 范围位于不同的子网中。
- 在开始安装之前收集以下信息：
  - 要用于 SDC 的静态 IP 地址。
  - 您在安装过程中创建的 `root` 和 `cdo` 用户的密码。
  - 您的组织使用的 DNS 服务器的 IP 地址。
  - SDC 地址所在网络的网关 IP 地址。
  - 时间服务器的 FQDN 或 IP 地址。
- SDC 虚拟机配置为定期安装安全补丁，为此，需要打开端口 80 出站。

过程

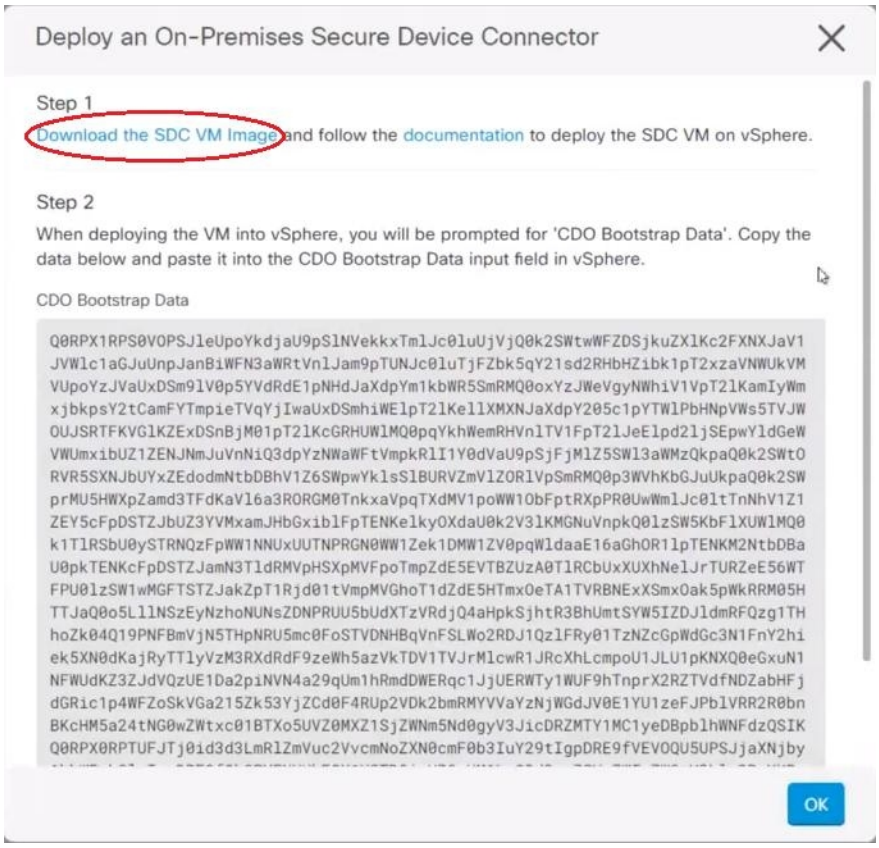
步骤 1 登录到要为其创建 SDC 的 CDO 租户。

步骤 2 从 CDO 菜单中，选择**工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

步骤 3 在安全连接器 页面上，点击蓝色加号按钮，然后选择**安全设备连接器 (Secure Device Connector)**。



步骤 4 在步骤 1 中，点击**下载 SDC VM 映像 (Download the SDC VM image)**。这将在单独的选项卡中打开。



步骤 5 从 zip 文件中提取所有文件。它们看起来和下面有些相似：

- CDO-SDC-VM-ddd50fa.ovf
- CDO-SDC-VM-ddd50fa.mf
- CDO-SDC-VM-ddd50fa-disk1.vmdk

步骤 6 使用 vSphere Web 客户端以管理员身份登录 VMware 服务器。

注释 请勿使用 ESXi Web 客户端。

步骤 7 按照提示从 OVF 模板部署安全设备连接器虚拟机。

步骤 8 设置完成后，打开 SDC VM。

步骤 9 打开新 SDC VM 的控制台。

步骤 10 使用用户名 **cdo** 登录。默认密码为 **adm123**。

步骤 11 在提示符后，键入 `sudo sdc-onboard setup`。

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

步骤 12 出现密码提示时，输入 `adm123`。

步骤 13 按照提示为用户 `root`创建新密码。输入 root 用户的密码。

步骤 14 按照提示为 **cdo** 用户创建新密码。输入 cdo 用户的密码。

步骤 15 当系统提示**请选择要连接的 CDO 域 (Please choose the CDO domain you connect to)** 时，请输入您的 Cisco Defense Orchestrator 域信息。

步骤 16 系统提示时，输入以下的 SDC 的域信息：

a) IP 地址/CIDR
b) 网关
c) DNS 服务器
d) NTP 服务器或 FQDN
e) Docker 网桥

如果 Docker 网桥不适用，请按 Enter 键。

步骤 17 当系统提示 **这些值是否正确时？（是/否）(Are these values correct? [y/n])**， 使用 **y确认您的输入**。

步骤 18 确认您的输入内容。

步骤 19 当系统提示 **您是否要设置 SDC 时？（是/否）(Would you like to setup the SDC now? [y/n])**，输入 `n`。

步骤 20 VM 控制台会自动将您注销。

步骤 21 创建与 SDC 的 SSH 连接。以 **cdo** 身份登录并输入密码。

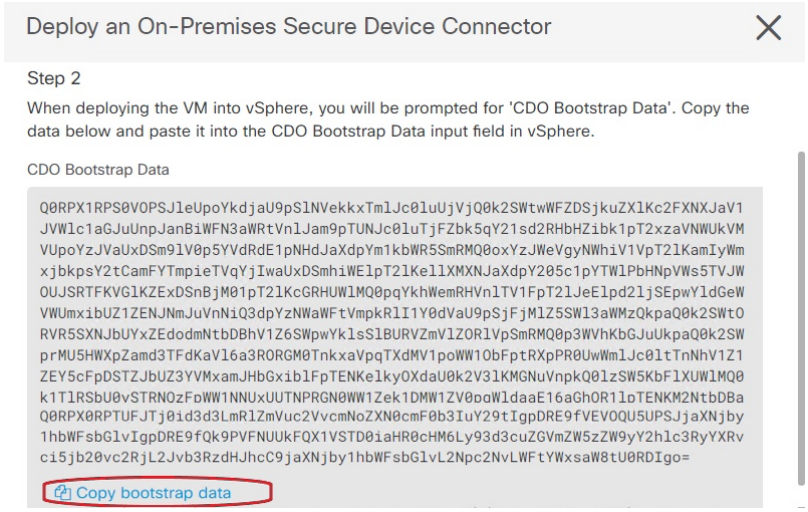
步骤 22 在提示符后，键入 `sudo sdc-onboard bootstrap`。

```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

步骤 23 当系统提示输入 **[sudo] 密码**时，请输入您在步骤 14 中创建的 cdo 密码。

步骤 24 当系统提示**请从 CDO 的安全连接器页面复制引导程序数据 (Please copy the bootstrap data form the Secure Connector Page of CDO)** 时，请执行以下程序：

1. 登录 CDO。
2. 从 CDO 菜单中选择 **管理** > **安全连接器**。
3. 在操作窗格中，点击**部署现场安全设备连接器 (Deploy an On-Premises Secure Device Connector)**。
4. 点击对话框第 2 步中的**复制引导程序数据 (Copy the bootstrap data)**，然后粘贴到 SSH 窗口中。



步骤 25 当系统提示 您是否想更新这些设置？（是/否）**(Do you want to update these setting? [y/n])**，输入 `n`。

步骤 26 返回“安全设备连接器”(Secure Device Connector) 页面。刷新屏幕，直到您看到新 SDC 的状态更改为活动 **(Active)**。

相关信息：

- 对安全设备连接器进行故障排除，第 699 页
- 排除设备与 SDC 的连接故障，第 700 页

在您自己的虚拟机上部署安全设备连接器

使用设备凭证将 CDO 连接到设备时，最佳做法是在网络中下载并部署安全设备连接器 (SDC)，以管理 CDO 与设备之间的通信。通常，这些设备不是基于边界的，没有公共 IP 地址，或者具有通往外部接口的开放端口。自适应安全设备 (ASA)、FDM 管理 设备、Firepower 管理中心 (FMC) 和安全防火墙云原生设备均可使用设备凭证载入 CDO。

SDC 监控需要在受管设备上执行的命令，以及需要发送到受管设备的消息。SDC 代表 CDO 执行命令，代表受管设备向 CDO 发送消息，并将受管设备的应答返回给 CDO。

单个 SDC 可以管理的设备数量取决于这些设备上实施的功能及其配置文件的大小。但是，出于规划部署的目的，我们预计一个 SDC 可支持大约 500 台设备。有关详细信息，请参阅在单个 CDO 租户上使用多个 SDC，第 27 页。

此程序介绍如何使用您自己的虚拟机映像在网络中安装 SDC。

注释 安装 SDC 的首选、最简单、最可靠的方法是下载 CDO 的 SDC OVA 映像并进行安装。对于说明，请参阅 使用 CDO 的 VM 映像部署安全设备连接器，第 13 页 。

开始之前

- CDO 需要严格的证书检查，并且不支持 SDC 和互联网之间的 Web/内容代理。
- SDC 必须在 TCP 端口 443 上具有对互联网的完全出站访问权限。
- 关于网络指南，请查看将 思科防御协调器 连接到托管设备。
- 安装了 vCenter Web 客户端或 ESXi Web 客户端的 VMware ESXi 主机。

注释 我们不支持使用 vSphere 桌面客户端进行安装。

- ESXi 5.1 虚拟机监控程序。
- Cent OS 7 访客操作系统。
- 仅具有 SDC 的 VM 的系统要求：
  - VMware ESXi 主机需要 2 个 CPU。
  - VMware ESXi 主机至少需要 2 GB 内存。
  - VMware ESXi 需要 64 GB 磁盘空间来支持虚拟机，具体取决于您的调配选择。此值假定您对分区使用逻辑卷管理 (LVM)，因此您可以根据需要扩展所需的磁盘空间。
- 具有 SDC 和租户的**单个**安全事件连接器 (SEC) 的 VM 的系统要求。（SEC 是关于安全分析和日志记录 (SaaS)中使用的组件）。

  添加到 VMware ESXi 主机的每个 SEC 都需要额外的 4 个 CPU 以及额外的 8 GB 内存。

  因此，以下是对具有一个 SDC 和一个 SEC 的 VMware ESXi 主机的要求：
  - VMware ESXi 主机需要 6 个 CPU。
  - VMware ESXi 主机至少需要 10 GB 内存。
  - VMware ESXi 需要 64 GB 磁盘空间来支持虚拟机，具体取决于您的调配选择。
- 更新 VM 上的 CPU 和内存后，打开 VM 并确保“安全连接器”页面指示 SDC 处于“活动”状态。
- 执行此过程的用户应该能够轻松地在 Linux 环境中使用 vi 可视化编辑器编辑文件。
- 如果您在 CentOS 虚拟机上安装本地 SDC，我们建议您定期安装 Yum 安全补丁。根据您的 Yum 配置，要获取 Yum 更新，您可能需要在端口 80 和 443 上打开出站访问。您还需要配置 yum-cron 或 crontab 来安排更新。与您的安全运营团队合作，确定是否需要更改任何安全策略以允许您获取 Yum 更新。

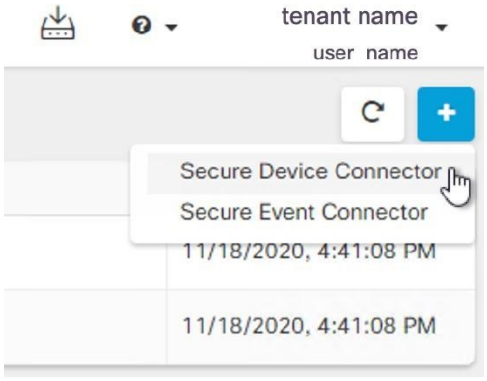
注释 **开始之前**：不要将程序中的命令复制并粘贴到终端窗口中，而应键入这些命令。某些命令包括“n-dash”，在剪切和粘贴过程中，这些命令可以作为 “m-dash” 应用，这可能会导致命令失败。

过程

步骤 1 登录到要为其创建 SDC 的 CDO 租户。

步骤 2 从 CDO 菜单中，选择**工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

步骤 3 在安全连接器 页面上，点击蓝色加号按钮，然后选择**安全设备连接器 (Secure Device Connector)**。



步骤 4 将窗口中步骤 2 中的引导程序数据复制到记事本。

步骤 5 安装 **CentOS 7 虚拟机**，至少为 SDC 分配以下 RAM 和磁盘空间：

- 8 GB RAM
- 10GB 磁盘空间

步骤 6 安装后，配置基本网络，例如指定 SDC 的 IP 地址、子网掩码和网关。

步骤 7 配置 DNS（域名服务器）服务器。

步骤 8 配置 NTP（网络时间协议）服务器。

步骤 9 在 CentOS 上安装 SSH 服务器，以便与 SDC 的 CLI 轻松交互。

步骤 10 运行 yum 更新，然后安装软件包： **open-vm-tools**、 **nettools** 和 **bind-utils**

```
[root@sdc-vm ~]# yum update -y
[root@sdc-vm ~]# yum install -y open-vm-tools net-tools bind-utils
```

步骤 11 安装 AWS CLI 软件包；请参阅https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html。

注释 请勿使用 **--user** 标志。

步骤 12 安装 Docker CE 软件包；请参阅https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce

注释 使用“使用存储库安装”方法。

步骤 13 启动 Docker 服务并使其在启动时启动：

```
[root@sdc-vm ~]# systemctl start docker
[root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service to
    /usr/lib/systemd/system/docker.service.
```

步骤 14 创建两个用户：“cdo”和“sdc”。cdo用户将是您登录以运行管理功能的用户（因此您无需直接使用 root 用户），sdc 用户将是运行 SDC docker 容器的用户。

```
[root@sdc-vm ~]# useradd cdo
[root@sdc-vm ~]# useradd sdc -d /usr/local/cdo
```

步骤 15 为 cdo 用户设置密码。

```
[root@sdc-vm ~]# passwd cdo
Changing password for user cdo.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```

步骤 16 将 cdo 用户添加到“wheel”组，为其提供管理 (sudo) 权限。

```
[root@sdc-vm ~]# usermod -aG wheel cdo
[root@sdc-vm ~]#
```

步骤 17 安装 Docker 时，会创建一个用户组。根据 CentOS/Docker 的版本，它可能被称为 “docker” 或 “dockerroot”。检查 /etc/group 文件以查看创建的组，然后将 sdc 用户添加到此组。

```
[root@sdc-vm ~]# grep docker /etc/group
 docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

步骤 18 如果 /etc/docker/daemon.json 文件不存在，请创建该文件，并使用以下内容填充。创建后，重新启动 Docker 后台守护程序。

注释 确保在 "group" 项中输入的组名称与您在上一步中在 /etc/group 文件中找到的组匹配。

```
[root@sdc-vm ~]# cat /etc/docker/daemon.json
        {
           "live-restore": true,
           "group": "docker"
        }
        [root@sdc-vm ~]# systemctl restart docker
        [root@sdc-vm ~]#
```

步骤 19 如果您当前使用的是 vSphere 控制台会话，请切换到 SSH 并使用 “cdo” 用户登录。登录后，更改为“sdc”用户。当系统提示输入密码时，请输入 “cdo” 用户的密码。

```
[cdo@sdc-vm ~]$ sudo su sdc
              [sudo] password for cdo: <type password for cdo user>
              [sdc@sdc-vm ~]$
```

步骤 20 将目录更改为 **/usr/local/cdo**。

步骤 21 创建一个名为 `bootstrapdata` 的新文件，并将**部署现场安全设备连接器**向导的步骤 2 中的引导程序数据粘贴到此文件中。**保存**文件。您可以使用 `vi` 或 `nano` 创建该文件。

步骤 22 引导程序数据采用 base64 编码。对其进行解码并将其导出到名为 `extractedbootstrapdata` 的文件

```
[sdc@sdc-vm ~]$ base64 -d /usr/local/cdo/bootstrapdata > /usr/local/cdo/extractedbootstrapdata

              [sdc@sdc-vm ~]$
```

运行 cat 命令以查看解码后的数据。命令和解码后的数据应如下所示：

```
[sdc@sdc-vm ~]$ cat /usr/local/cdo/extractedbootstrapdata
                CDO_TOKEN="<token string>"
                CDO_DOMAIN="www.defenseorchestrator.com"
                CDO_TENANT="<tenant-name>"

CDO_BOOTSTRAP_URL="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"
```

步骤 23 运行以下命令，将解码的引导程序数据部分导出到环境变量。

```
[sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > sdcenv && source sdcenv
              [sdc@sdc-vm ~]$
```

步骤 24 从 CDO 下载引导程序捆绑包。

```
[sdc@sdc-vm ~]$ curl -O -H "Authorization: Bearer $CDO_TOKEN" "$CDO_BOOTSTRAP_URL"
                100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
                [sdc@sdc-vm ~]$ ls -l /usr/local/cdo/*SDC
                -rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/cdo/tenant-name-SDC
```

步骤 25 解压缩 SDC tar 包，并运行 `bootstrap.sh` 文件以安装 SDC 软件包。

```
[sdc@sdc-vm ~]$ tar xzvf /usr/local/cdo/tenant-name-SDC
                <snipped - extracted files>
                [sdc@sdc-vm ~]$
                [sdc@sdc-vm ~]$ /usr/local/cdo/bootstrap/bootstrap.sh
                [2018-07-23 13:54:02] environment properly configured
                download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
                toolkit.sh
                common.sh
                [2018-07-23 13:54:04] startup new container
                Unable to find image 'ciscodefenseorchestrator/sdc_prod:latest' locally
                sha256:d98f17101db10e66db5b5d6afda1c95c29ea0004d9e4315508fd30579b275458:
Pulling from
                ciscodefenseorchestrator/sdc_prod
                08d48e6f1cff: Pull complete
                ebbd10b629b1: Pull complete
                d14d580ef2ed: Pull complete
                45421d451ab8: Pull complete
                <snipped - downloads>
                no crontab for sdc
```

SDC 现在应在 CDO 中显示“活动”。

下一步做什么

- 转到载入设备和服务 以载入要使用 CDO 管理的设备。
- 如果要安装安全事件连接器，请返回 在 SDC 虚拟机上安装安全事件连接器 ， 第 600 页。

- 如果要在租户上安装**第二个或多个**安全事件连接器，请返回使用 CDO 映像安装 SEC。

使用 Terraform 模块在 AWS VPC 上部署安全设备连接器

开始之前

在尝试在 AWS VPC 上部署 SDC 之前，请查看以下前提条件：

- CDO 需要严格的证书检查，并且不支持 SDC 和互联网之间的 Web/内容代理。如果使用代理服务器，请禁用对安全设备连接器 (SDC) 和 CDO 之间的流量进行检查。
- 查看 将 思科防御协调器 连接到托管设备 以确保适当的网络访问。
- 您需要一个 AWS 账户、一个至少具有一个子网的 AWS VPC 和一个 AWS Route53 托管区域。
- 确保您有 CDO 引导程序数据、AWS VPC ID 及其子网 ID。
- 确保您部署 SDC 的私有子网连接了 NAT 网关。
- 在运行防火墙管理 HTTP 接口的端口上打开从防火墙到连接到 NAT 网关的弹性 IP 的流量。

过程

步骤 1 在 Terraform 文件中添加以下代码行；请确保手动输入变量：

```
module "example-sdc" {
  source              =
"git::https://github.com/cisco-lockhart/terraform-aws-cdo-sdc.git?ref=v0.0.1"
  env                 = "example-env-ci"
  instance_name       = "example-instance-name"
  instance_size       = "r5a.xlarge"
  cdo_bootstrap_data = "<replace-with-cdo-bootstrap-data>"
  vpc_id              = <replace-with-vpc-id>
  subnet_id           = <replace-with-private-subnet-id>
}
```

有关输入变量和说明的列表，请参阅安全设备连接器 Terraform 模块。

步骤 2 将 `instance_id` 注册为 Terraform 代码中的输出：

```
output "example_sdc_instance_id" {
  value = module. example-sdc.instance_id
}
```

您可以使用 `instance_id` 连接到 SDC 实例，以便使用 AWS 系统管理器会话管理器 (SSM) 进行故障排除。有关可用输出的列表，请参阅安全设备连接器 Terraform 模块中的输出。

下一步做什么

要对 SDC 进行任何故障排除，您需要使用 AWS SSM 连接到 SDC 实例。请参阅 AWS 系统管理器会话管理器，了解有关如何连接到实例的更多信息。请注意，出于安全原因，使用 SSH 连接到 SDC 实例的端口不会被公开。

更改安全设备连接器的 IP 地址

开始之前

- 您必须是管理员才能执行此任务。
- SDC 必须在 TCP 端口 443 或您为设备管理配置的端口上具有对互联网的完全出站访问权限。

注释 更改 SDC 的 IP 地址后，您无需将任何设备重新载入 CDO。

过程

步骤 1 创建与 SDC 的 SSH 连接或打开虚拟机的控制台，并以 CDO 用户身份登录。

步骤 2 如果您希望在更改 IP 地址之前查看 SDC VM 的网络接口配置信息，请使用 ifconfig 命令。

```
[cdo@localhost ~]$ ifconfig
```

步骤 3 要更改接口的 IP 地址，请键入 sudo sdc-onboard setup 命令。

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

步骤 4 出现提示时，请输入密码。

```
[sudo] password for cdo:
```

步骤 5 在提示符后键入 n 以重置 root 和 CDO 密码。

```
Would you like to reset the root and cdo passwords? (y/n):
```

步骤 6 在提示符后键入 y 以重新配置网络。

```
Would you like to re-configure the network? (y/n):
```

步骤 7 出现提示时，输入要分配给 SDC 的新 IP 地址和 SDC VM 的其他域信息：

a) IP 地址
b) 网关
c) DNS 服务器
d) NTP 服务器或 FQDN

   如果 NTP 服务器或 FQDN 不适用，请按 Enter 键。

e) Docker 网桥

如果 Docker 网桥不适用，请按 Enter 键。

步骤 8 当系统提示输入值是否正确时，请使用 y 确认输入。

```
Are these values correct? (y/n):
```

注释 在键入 y 之前，请确保您的值准确无误，因为在此命令后，您与旧 IP 地址的 SSH 连接将丢失。

步骤 9 使用分配给 SDC 的新 IP 地址创建 SSH 连接并登录。

步骤 10 您可以运行连接状态测试命令，以确保 SDC 正常运行。

```
[cdo@localhost ~]$ sudo sdc-onboard status
```

所有检查都必须以绿色显示 [OK]。

注释 如果在 VM 的控制台中执行此程序，则在确认值正确后，连接状态测试将自动运行并显示状态。

步骤 11 您还可以通过 CDO 用户界面检查 SDC 的连接。要执行此操作，请打开 CDO 应用并导航至“工具和服务安全连接器”页面。 >

步骤 12 刷新页面并选择已更改 IP 地址的安全连接器。

步骤 13 在操作窗格中，点击请求检测信号。

您应该会看到已成功请求心跳消息，并且上次心跳应显示当前日期和时间。

重要事项 您所做的 IP 地址更改仅在格林威治标准时间上午 3:00 后反映在 SDC 的“详细信息”窗格中。

有关在 VM 上部署 SDC 的信息，请参阅。在您自己的虚拟机上部署安全设备连接器 ， 第 17 页

删除安全设备连接器

Warning 此程序会删除您的安全设备连接器 (SDC)。这一操作不可逆。在执行此操作后，您将无法管理连接到该 SDC 的设备，直到安装新的 SDC 并重新连接设备。重新连接设备可能需要您为要重新连接的每个设备重新输入管理员凭证。

要从租户中删除 SDC，请遵循以下程序：

Procedure

步骤 1 删除连接到您要删除的 SDC 的任何设备。

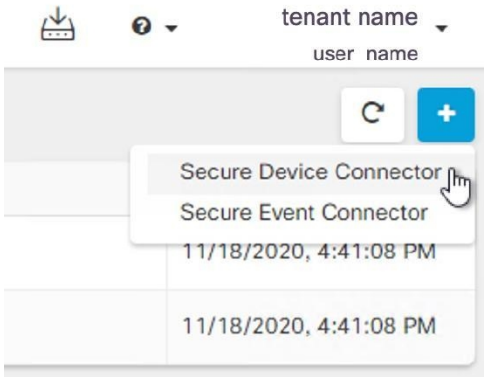
- **a.** 请参阅查找所有使用相同 SDC 连接到 CDO 的设备，以便确定 SDC 使用的所有设备。

b. 在**清单 (Inventory)** 页面中，选择您确定的所有设备。

c. 在“设备操作”(Device Actions) 窗格中，点击**删除 (Remove)**，然后点击**确定 (OK)** 以确认您的操作。

步骤 2 从 CDO 菜单中，选择**工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

步骤 3 在“安全连接器”(Secure Connectors) 页面上，点击蓝色加号按钮，然后选择**安全设备连接器 (Secure Device Connector)**。



步骤 4 在“安全连接器”(Secure Device Connector) 表中，选择要删除的 SDC。其设备计数现在应为零。

步骤 5 在“操作”(Actions) 窗格中，点击 **删除 (Remove)**。您会收到以下警告：

Warning 您即将删除 <sdc_name>。删除 SDC 的操作不可逆。删除 SDC 需要先创建并载入新的 SDC，然后才能载入或重新载入设备。

由于您当前有已载入的设备，因此删除 SDC 将要求您在设置新的 SDC 后重新连接这些设备并再次提供凭证。

- 如果您有任何问题或疑虑，请点击**取消 (Cancel)** 并联系 CDO 支持。
- 如果要继续，请输入 <sdc_name> 在下面的文本框中，然后点击**确定 (OK)**。

步骤 6 在确认对话框中，如果您想继续，请输入警告消息中所述的 SDC 名称。

步骤 7 点击**确定 (OK)** 以确认删除 SDC。

将 ASA 从一个 SDC 移至另一个 SDC

CDO 支持每个租户使用多个 SDC。在单个 CDO 租户上使用多个 SDC，第 27 页您可以使用以下程序将受管 ASA 从一个 SDC 移至另一个 SDC：

过程

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备 (Devices)** 选项卡，然后点击 **ASA** 选项卡。

步骤 3 选择要移动到其他 SDC 的 ASA。

步骤 4 在**设备操作 (Device Actions)** 窗格中，点击**更新凭证 (Update Credentials)**。

步骤 5 点击 Secure Device Connector 按钮，然后选择要将设备移动到的 SDC。

步骤 6 输入用于登录设备的管理员用户名和密码，然后点击**更新 (Update)**。除非已更改，否则管理员用户名和密码与您用于载入 ASA 的凭证相同。您不必将这些更改部署到设备。

注释 如果所有 ASA 都使用相同的凭证，则可以将 ASA 从一个 SDC 批量移至另一个 SDC。如果 ASA 具有不同的凭证，则必须一次将其从一个 SDC 移至另一个 SDC。

更新 Meraki MX 连接凭证

如果您从 Meraki 控制面板生成新的 API 密钥，则必须在 CDO 中更新连接凭证。要生成新密钥，请参阅 生成和检索 Meraki API 密钥 以获取更多信息。CDO 不允许您更新设备本身的连接凭证；如有必要，您可以在 Meraki 控制面板中手动刷新 API 密钥。您必须在 CDO UI 中手动更新 API 密钥，以更新凭证并重新建立通信。

Note 如果 CDO 无法同步设备，CDO 中的连接状态可能会显示“凭证无效”。如果是这种情况，您可能已尝试使用 API 密钥。确认所选 Meraki MX 的 API 密钥正确无误。

使用以下程序更新 Meraki MX 设备的凭证：

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备 (Devices)** 选项卡，然后点击 **Meraki** 选项卡。

步骤 3 选择要更新其连接凭证的 Meraki MX。

步骤 4 在**设备操作 (Device Actions)** 窗格中，点击**更新凭证 (Update Credentials)**。

步骤 5 输入 CDO 用于登录设备的 **API 密钥 (API key)**，然后点击**更新 (Update)**。除非已更改，否则此 API 密钥与您用于载入 Meraki MX 的凭证相同。您不必将这些更改部署到设备。

重命名安全设备连接器

过程

步骤 1 从 CDO 菜单中，选择**工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

步骤 2 选择要重命名的 SDC。

步骤 3 在详细信息窗格中，点击 SDC 名称旁边的编辑图标。

步骤 4 重命名 SDC。

此新名称将显示在CDO界面中出现SDC名称的任何位置，包括“资产”窗格的“安全设备连接器”过滤器。

更新您的安全设备连接器

使用此程序作为故障排除工具。通常，SDC 会自动更新，您不必使用此程序。但是，如果 VM 上的时间配置不正确，则 SDC 无法与 AWS 建立用于接收更新的连接。此程序将启动 SDC 更新，并应解决由于时间同步问题而导致的错误。

Procedure

步骤 1 连接到 SDC。您可以使用 SSH 进行连接，也可以使用 VMware 虚拟机监控程序中的控制台视图。）

步骤 2 以 **cdo** 用户身份登录 SDC。

步骤 3 切换到 SDC 用户以更新 SDC Docker 容器：

```
[cdo@sdc-vm ~]$ sudo su sdc
                [sudo] password for cdo: <type password for cdo user>
                [sdc@sdc-vm ~]$
```

步骤 4 升级 SDC 工具包：

```
[cdo@sdc-vm ~]$ /usr/local/cdo/toolkit/toolkit.sh upgradeToolkit
                [sdc@sdc-vm ~]$
```

步骤 5 升级 SDC：

```
[cdo@sdc-vm ~]$ /usr/local/cdo/toolkit/toolkit.sh upgradeSDC
                [sdc@sdc-vm ~]$
```

在单个 CDO 租户上使用多个 SDC

通过为租户部署多个SDC，您可以管理更多设备，而不会出现性能下降。单个SDC可以管理的设备数量取决于这些设备上实施的功能及其配置文件的大小。

您可以在租户上安装无限数量的 SDC。每个 SDC 可以管理一个网段。这些 SDC 会将这些网段中的设备连接到同一个 CDO 租户。如果没有多个 SDC，您将需要使用不同的 CDO 租户管理隔离网段中的设备。

部署第二个或后续 SDC 的程序与部署第一个 SDC 的程序相同。使用 CDO 的 VM 映像部署安全设备连接器，也可以在您自己的虚拟机上部署安全设备连接器。租户的初始 SDC 包含租户的名称和数字 1。每个额外的 SDC 都按顺序编号。

查找所有使用相同 SDC 连接到 CDO 的设备

请按照以下程序识别所有使用相同 SDC 连接到 CDO 的设备：

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击设备类型选项卡。

步骤 4 如果已指定任何过滤条件，请点击“清单”(Inventory) 表顶部的**清除**按钮，以显示您使用 CDO 管理的所有设备和服务。

步骤 5 点击过滤器按钮  以展开过滤器菜单。

步骤 6 在过滤器的“安全设备连接器”(Secure Device Connectors) 部分中，选中您感兴趣的 SDC 的名称。“清单”(Inventory) 表仅显示通过您在过滤器中选中的 SDC 连接到 CDO 的设备。

步骤 7 （可选）检查过滤器菜单中的其他过滤器，以便进一步细化搜索。

步骤 8 （可选）完成后，点击清单表顶部的**清除**按钮，以便显示您使用 CDO 管理的所有设备和服务。

安全设备连接器开源和第三方许可证归属

==========

*** amqplib ***

amqplib 版权所有 (c) 2013, 2014

米歇尔·布里根<mikeb@squaremobius.net>

此软件包“amqplib”根据 MIT 许可证获得许可。可以在此目录中的文件 LICENSE-MIT 中找到副本，或从以下位置下载

http://opensource.org/licenses/MIT

==========

*** async ***

版权所有 (c) 2010-2016 Caolan McMaho

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

*** bluebird ***

MIT 许可证 (MIT)

版权所有 **(c) 2013-2015 Petka Antonov**

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

***cheerio ***

版权所有 **(c) 2012** 马特穆勒**<mattmuelle@gmail.com>**

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

*** command-line-args ***

MIT 许可证 (MIT)

版权所有 **(c) 2015 Lloyd Brookes <75镑@gmail.com>**

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

*** ip ***

此软件根据 **MIT** 许可证获得许可。

Fedor Indutny, 2012 版权所有。

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

*** json-buffer ***

版权所有 **(c) 2013 Dominic Tarr**

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

*** json-stable-stringify ***

此软件在 **MIT** 许可证下发布：

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

*** json-stringify-safe ***

ISC 许可证

版权所有 **(c) Isaac Z. Schlueter** 和贡献者

特此授予出于任何目的使用、复制、修改和/或分发本软件的权限，前提是所有副本中均包含上述版权声明和本许可声明。

本软件按“原样”提供，作者否认与本软件相关的所有担保，包括对适销性和适用性的所有暗示担保。在任何情况下，作者均不对因使用、数据或利润损失而导致的任何特殊、直接、间接或后果性损害负责，无论是因合同、过失或其他原因造成的与本软件的使用或性能相关。

==========

*** lodash ***

版权所有 JS 基金会和其他贡献者 < https://js.foundation/ >https://js.foundation/

基于 **Underscore.js**，版权所有，

DocumentCloud 和 Investigative Reporters & Editors < >http://underscorejs.org/

该软件由许多个人自愿提供。有关确切的贡献历史记录，请参阅以下位置的修订历史记录：https://github.com/lodash/lodash

以下许可证适用于本软件的所有部分，但作为

记录如下：

====

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

====

通过 **CC0** 放弃示例代码的版权和相关权利。示例代码定义为文档中显示的所有源代码。

CC0: http://creativecommons.org/publicdomain/zero/1.0/

====

位于 node_modules 和 vendor 目录中的文件是此软件使用的外部维护的库，它们有自己的许可证；我们建议您阅读它们，因为它们的术语可能与上述术语不同。

==========

*** log4js ***

版权所有 **2015 Gareth Jones**（许多其他人的贡献）

根据 **Apache** 许可证 **2.0** 版本 **(**\“许可\”**)** 授权； 除非遵守本许可的规定，否则不得使用此文件。 您可以通过以下网址获取许可证副本：

http://www.apache.org/licenses/LICENSE-2.0

除非适用法律要求或达成书面协议， 根据许可证分发的软件均\“按原样\”分发， 且不附带任何明示或默示的保证或条件。 请参阅许可证，了解许可证中有关语言管理权限和限制的特定规定。

==========

*** mkdirp ***

版权所有 **2010 James Galliday (mail@substack.net)**

此项目是在 **MIT/X11** 许可证下发布的免费软件：

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

*** node-forge ***

新 **BSD** 许可证（**3** 个子句）

版权所有 **(c) 2010, Digital Bazaar, Inc.**

版权所有。

对源代码或二进制形式代码的重新发行和使用（包含或不含修改）需要符合下列条件：

***** 源代码的重新分发必须保留上述版权声明、本条件列表及以下免责声明。

***** 以二进制形式重新发行时，必须通过文档和/或在发行时一并提供的其它材料复制上述版权声明、此条件清单和下面的免责声明。

***** 未经事先明确书面许可，不得使用 **Digital Bazaar, Inc.** 及其参与者姓名宣传或推广本软件的衍生产品。

该软件由版权所有者和贡献者按“原样”提供，不承担任何明示或暗示的担保，包括但不限于用于特定用途的适销性和适用性的暗示担保。在任何情况下，**DIGITAL BAZAAR** 对于以任何方式使用

该软件造成的任何直接、间接、意外、特殊、惩罚性或后果性损害（包括但不限于替代货物或服务的采购；用途丧失、数据丢失或利润损失；或业务中断），均不承担任何责任，无论导致前述损害的原因与责任推断如何，也无论是否因合同、严格责任或侵权（包括疏忽或其他原因）造成该等损害，即使已被告知发生此类损害的可能性。

==========

*** request ***

Apache 许可证

版本 **2.0**，**2004** 年 **1** 月

http://www.apache.org/licenses/

使用、复制和分发条款和条件

1. 定义。

“许可”是指本文档第 **1- 9** 节规定的使用、复制和分发的条款和条件。

“许可方”是指版权所有者或由版权所有者授权进行许可授予的实体。

“法律实体”是指实施实体以及所有其他控制该实体、由该实体控制或与该实体共同受控制的实体的联合整体。在此定义中，“控制”是指 **(i)** 通过合同或其他方式，有权直接或间接决定此类实体的方向或管理，或 **(ii)** 拥有此类实体百分之五十 **(50%)** 或以上已发行股份的所有权，或 **(iii)** 拥有此类实体的受益所有权。

“您”（或“您的”）是指行使此许可证所授权限的个人或法律实体。

“源”形式是指用于进行修改的首选形式，包括但不限于软件源代码、文档源和配置文件。

“目标”形式是指任何通过对源形式进行机械转换或翻译所获得的形式，包括但不限于经过编译的对象代码、生成的文档以及转换为其他媒体类型。

“作品”是指根据许可（如作品包含或随附的版权声明所示）提供的源形式或目标形式的著作（下面的附录中提供了一个示例）。

“衍生作品”是指任何基于作品创作（或从作品衍生而来）的，其编辑修订、注释、详细描述或其他修改等从整体上构成原创作品的源形式或目标形式的作品。根据此项许可，衍生作品不包括与作品及其衍生作品分离之作品，或仅与作品及其衍生作品的接口相链接（或以名称绑定）之作品。

“投稿”是指任何创作作品，包括作品的原始版本和对该作品或衍生作品所做的任何修改或增补，由版权所有者或经授权可代表版权所有者进行提交的个人或法律实体特意提交给许可方以纳入其作品中。在此定义中，“提交”是指发送给许可方或其代表的任何电子、口头或书面形式的通信，包括但不限于通过许可方管理的或代表许可方管理的电邮清单、源代码控制系统以及发布跟踪系统为讨论和改善作品而进行的通信，但不包括由版权所有者以书面形式明显标注或指定为“非投稿”的通信。“投稿者”是指许可方，以及许可方已收到其投稿并随后纳入作品中的任何个人或代表该个人的法律实体。

“贡献者”是指许可方以及代表许可方收到文稿并随后纳入作品的任何个人或法人实体。

2. 版权许可的授予。根据此项许可的条款和条件，每位投稿者特此授予您一项永久的、全球性的、非专有的、免费且无版权费的、不可撤销的版权许可，准许您对作品和衍生作品的源形式或目标形式进行复制、制备衍生作品、公开陈列、公开演示、授予分许可，以及分发。

3. 专利许可的授予。根据此项许可的条款和条件，每位投稿者特此授予您一项永久的、全球性的、非专有的、免费且无版权费的、不可撤销的（除非本节另有规定）专利许可，准许您制作、已经制作、使用、邀约销售、销售、进口和以其他方式转让作品，此类许可仅适用于投稿者可予许可的专利权利要求，并且如不授予许可，则单独使用其投稿或将其投稿与提交以供纳入其中的作品组合使用必定构成对前述要求的侵权。如果您对任何实体提起专利法律诉讼（包括交叉诉讼或反诉），主张作品或作品中所含投稿构成直接或共同专利侵权，则根据此项许可授予您的针对该作品的任何专利许可都将在提起上述诉讼之日起终止。

4. 再分发。您可以在任何介质中以源或对象形式复制和分发作品或其衍生作品的副本，无论是否进行修改，前提是您满足以下条件：

您必须向作品或衍生作品的任何其他接收者提供本许可证的副本；和

您必须在任何已修改的文件上放置醒目的通知，说明您更改了文件；和

您必须在您分发的任何衍生作品的源形式中保留作品的源形式的所有版权、专利、商标和归属声明，不包括与衍生作品任何部分无关的声明；和

如果作品包含“通知”文本文件作为其分发的一部分，则您分发的任何衍生作品必须包括该通知文件中包含的归属通知的可读副本，不包括不属于任何部分的通知衍生作品，至少在以下位置：作为衍生作品的一部分分发的通知文本文件；在源表单或文档中（如果与衍生作品一起提供）；或者，在衍生作品生成的显示中，如果以及通常出现此类第三方通知。声明文件的内容仅供参考，并不构成对许可的修改。您可在您分发的衍生作品中随同作品的声明文本或以附录形式添加自己的归属声明，前提是附加的归属声明不得构成对许可的修改。只要您对作品的使用、复制和分发符合此项许可规定的条件，您可以为自身所做的修改添加自己的版权声明并可就自身所修改内容或任何此类衍生作品作为整体的使用、复制或分发提供附加或不同的许可条款和条件。

5. 投稿的提交。除非您明确作出不同声明，否则您向许可方提交的旨在纳入作品中的任何投稿均受此项许可的条款和条件的约束，无任何附加条款或条件。尽管有上述规定，如您与许可方就该等投稿签订了任何单独许可协议，此项许可的条款不得取代或修改该单独许可协议的条款。

6. 商标。此项许可并未授予您使用许可方的商号、商标、服务标记或产品名称的权限，除非此类使用是合理和惯例性描述作品来源和复制声明文件内容之所必需。

7. 免责声明。除非适用法律要求或达成书面协议，否则许可方均“按原样”提供作品（且每位投稿者均“按原样”提供其投稿），不附带任何明示或默示的保证或条件，包括但不限于关于所有权、非侵权、适销性或适用性的保证或条件。您应全权负责确定使用或再分发作品的适当性，并且承担行使此项许可项下权限的所有风险。

8. 责任限制。在任何情况下，在任何法律理论下，无论是侵权（包括过失）、合同或其他理论，除非适用法律要求（例如故意和重大过失行为）或达成书面协议，否则对于您所遭受的损害，包括因此项许可或者因使用或无法使用作品而产生的任何性质的直接、间接、特殊、附带或后果性损害（包括但不限于商誉损失、停工、计算机失效或故障等损害，或任何及所有其他商业损害或损失），任何投稿者概不负责，即使投稿者已被告知发生此类损害的可能性，也是如此。

9.接受担保或附加责任。再分发作品或衍生作品时，您可以选择接受与此项许可一致的支持、担保、赔偿或其他责任义务和/或权利，并就此收取费用。但是，在接受上述义务时，您只可代表您自己并对此全权负责，不得代表任何其他投稿者，除非您同意，如因您接受任何此类担保或附加责任，致使此等投稿者承担任何责任或遭受任何索赔，您将对其作出赔偿、为其辩护并保护其免受损害。

条款和条件结束

==========

*** rimraf ***

ISC 许可证

版权所有 **(c) Isaac Z. Schlueter** 和贡献者

特此授予出于任何目的使用、复制、修改和/或分发本软件的权限，前提是所有副本中均包含上述版权声明和本许可声明。

本软件按“原样”提供，作者否认与本软件相关的所有担保，包括对适销性和适用性的所有暗示担保。在任何情况下，作者均不对因使用、数据或利润损失而导致的任何特殊、直接、间接或后果性损害负责，无论是因合同、过失或其他原因造成的与本软件的使用或性能相关。

==========

*** uuid ***

版权所有 **(c) 2010-2012 Robert Kieffer**

MIT 许可证 - http://opensource.org/licenses/mit-license.php

==========

***** 验证器 *****

版权所有 **(c) 2016 Chris O'Hara<cohara87@gmail.com>**

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。

==========

***** 何时 *****

开源计划 **OSI - MIT** 许可证

http://www.opensource.org/licenses/mit-license.php

版权所有 **(c) 2011** 布赖恩·卡瓦利埃

特此授予获得本软件和相关文档文件（“软件”）副本的任何人无限制地处理本软件的权限，包括但不限于使用、复制、修改、合并的权利发布、分发、再许可和/或销售软件的副本，并允许获得本软件的人员这样做，但须遵守以下条件：

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

所述软件“按原样”提供且不附带任何明示或默示保证，包括但不限于关于适销性、适用特定用途以及不侵权的保证。在任何情况下，作者或版权持有人对软件或软件的使用或其他处理所导致、产

生或与之相关的任何索赔、损害赔偿或其他责任概不负责，无论是出于合同、侵权行为还是其他原因皆是如此。
==========

登录到 CDO

要登录 思科防御协调器 (CDO)，客户需要具有符合 SAML 2.0 标准的身份提供程序 (IdP)、多因素身份验证提供程序以及 用户管理。

IdP 账户包含用户的凭证，IdP 根据这些凭证对用户进行身份验证。多因素身份验证提供了额外的身份安全层。CDO 用户记录主要包含用户名、与其关联的 CDO 租户以及用户的角色。当用户登录时，CDO 会尝试将 IdP 的用户 ID 映射到 CDO 中租户的现有用户记录。当 CDO 找到匹配项时，用户已登录到该租户。

除非您的企业有自己的单点登录身份提供程序，否则身份提供程序是思科安全云登录。Cisco Security Cloud Sign On 使用 Duo 进行多因素身份验证。客户可以选择将 SAML 单点登录与 Cisco Defense Orchestrator 集成。

要登录 CDO，您必须首先在 Cisco Security Cloud Sign On 中创建一个账户，使用 Duo Security 来配置多因素身份验证 (MFA)，并让租户超级管理员创建 CDO 记录。

2019 年 10 月 14 日，CDO 将所有先前存在的租户转换为使用 Cisco Security Cloud Sign On 作为其身份提供程序和 Duo for MFA。

注释

- 如果您使用自己的单点登录身份提供程序登录 CDO，则转换到 Cisco Security Cloud Sign On 不会影响您。您可以继续使用自己的登录解决方案。
- 如果您正在免费试用 CDO，则此过渡确实会影响您。

如果您的 CDO 租户是在 2019 年 10 月 14 日或之后创建的，请参阅新 CDO 租户的初始登录，第 36 页。

如果您的 CDO 租户在 2019 年 10 月 14 日之前就已存在，请参阅迁移到 Cisco Security Cloud Sign On 身份提供程序，第 37 页。

新 CDO 租户的初始登录

思科防御协调器 (CDO) 使用 Cisco Security Cloud Sign On 作为身份提供程序，并使用 Duo 进行多重身份验证 (MFA)。**要登录 CDO，必须先在 Cisco Secure Sign-On 中创建账户，然后再使用 Duo 配置 MFA**。

v 需要 MFA，它为保护您的用户身份提供额外的一重保障。双因素身份验证（一种 MFA）需要两个部分或因素来确保登录 CDO 的用户身份真实。第一个因素是用户名和密码，第二个是按需生成的一次性密码 (OTP)。

重要事项 **如果您的 CDO 租户在 2019 年 10 月 14 日之前就已存在**，请使用 迁移到 Cisco Security Cloud Sign On 身份提供程序，第 37 页 登录说明，而不是本文。

准备工作

安装 DUO Security。我们建议您在手机上安装 Duo Security 应用。如果您对于如何安装 Duo 有疑问，请查看 Duo 双因素身份验证指南：注册指南。

时间同步。您要使用移动设备生成一次性密码。由于 OTP 是基于时间的，所以您的设备时钟与实时同步是非常重要的。请确保您的设备时钟自动或手动设置为正确的时间。

后续操作？

请继续 创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证，第 66 页。这是 4 步流程。您需要完成所有四个步骤。

登录失败故障排除

登录失败，因为您无意中登录到错误的 CDO 区域

请确保您登录的是适当的 CDO 区域。登录 https://sign-on.security.cisco.com 后，您可以选择要访问的区域。点击 **CDO** 磁贴访问 Defenseorchestrator.com 或点击 **CDO (EU)** 访问 Defenseorchestrator.eu。

迁移到 Cisco Security Cloud Sign On 身份提供程序

在 2019 年 10 月 14 日，思科防御协调器(CDO) 会将租户转换为 Cisco Security Cloud Sign On 作为身份提供程序，并使用 Duo 进行多因素身份验证 (MFA)。**要登录 CDO，必须先在 Cisco Secure Sign-On 中激活帐户，然后再使用 Duo 配置 MFA**。

CDO 需要 MFA，它为保护您的用户身份提供额外的一重保障。双因素身份验证（一种 MFA）需要两个部分或因素来确保登录 CDO 的用户身份真实。第一个因素是用户名和密码，第二个是按需生成的一次性密码 (OTP)。

注释

- 如果您使用自己的单点登录身份提供程序登录 CDO，则转换到 Cisco Security Cloud Sign On 和 Duo 不会影响您。您可以继续使用自己的登录解决方案。
- 如果您正在免费试用 CDO，则此过渡适用于您。
- **如果您的 CDO 租户是在 2019 年 10 月 14 日或之后创建的**，请参阅新 CDO 租户的初始登录，第 36 页，而不是本文。

准备工作

我们强烈建议在迁移之前执行以下步骤：

- **安装 DUO Security**。我们建议您在手机上安装 Duo Security 应用。如果您对于如何安装 Duo 有疑问，请查看 Duo 双因素身份验证指南：注册指南。
- **时间同步**。您要使用移动设备生成一次性密码。由于 OTP 是基于时间的，所以您的设备时钟与实时同步是非常重要的。请确保您的设备时钟自动或手动设置为正确的时间。
- 创建新的思科 Secure Sign-On 账户并配置 Duo 多因素身份验证。这是 4 步流程。您需要完成所有四个步骤。

迁移后的登录失败故障排除

由于用户名或密码不正确，CDO 登录失败

解决方法 如果您尝试登录 CDO，并且知道您使用的是正确的用户名和密码，但登录失败，或者您尝试“忘记密码”无法恢复有效的密码，则您可能已尝试在未创建新 Cisco Security Cloud Sign On 帐户的情况下进行登录，则您需要按照创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证，第 66 页中的说明注册新的 Cisco Security Cloud Sign On 帐户。

登录到 Cisco Security Cloud Sign On 控制面板成功，但您无法启动 CDO

解决方法 您可能使用与 CDO 租户不同的用户名创建了 Cisco Security Cloud Sign On 账户。请联系思科技术支持中心 (TAC)，以规范 CDO 和 Cisco Secure Sign-On 之间的用户信息。

使用保存的书签登录失败

解决方法 您可能正在尝试使用浏览器中保存的旧书签登录。书签可能指向 https://cdo.onelogin.com。https://cdo.onelogin.com/

解决方法 登录 https://sign-on.security.cisco.com。

- **解决方法** 如果您尚未创建 Cisco Secure Sign-On 账户，请创建一个账户。创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证，第 66 页
- **解决方法** 如果您已创建新账户，请点击控制面板上与 思科防御协调器（美国）、思科防御协调器（欧盟）或 思科防御协调器（亚太地区）对应的 CDO 磁贴
- **解决方法** 将书签更新为指向 https://sign-on.security.cisco.com。https://sign-on.security.cisco.com/

从 Cisco Security Cloud Sign On 控制面板启动 CDO

Procedure

步骤 1 在 Cisco Security Cloud Sign On 控制板上点击适当的 CDO 按钮。CDO 磁贴会将您导向 https://defenseorchestrator.com，而 CDO (EU) 磁贴会将您导向 https://defenseorchestrator.eu

步骤 2 请点击身份验证器徽标以选择 Duo Security 或 Google Authenticator， 如果您已设置这两个身份验证器。

- 如果您在现有租户上已有用户记录，则将登录该租户。
- 如果您在多个门户上已有用户记录，您将能够选择要连接的门户。
- 如果您在若干租户上已有用户记录，则将能够选择要连接的 CDO 租户。
- 如果您在现有租户上尚无用户记录，将能够了解有关 CDO 的详细信息或申请试用租户。

门户视图检索并显示来自多个租户的整合信息。有关详细信息，请参阅 管理多租户门户, on page 56。

租户视图显示您拥有用户记录的多个租户。

管理租户的超级管理员

最佳做法是限制租户上的超级管理员数量。确定哪些用户应具有超级管理员权限，查看用户管理，并将其他用户的角色更改为“管理员”。用户管理, on page 60

CDO 支持的软件和硬件

CDO 文档介绍其支持的软件和设备。它不会指出 CDO 不支持的软件和设备。如果我们未明确声明对软件版本或设备类型的支持，则表示不支持。

相关信息：

Secure Firewall Threat Defense 设备支持详情

Note Firepower 设备管理器 (FDM) 支持和功能仅应要求提供。如果您的租户上尚未启用 防火墙设备管理器 支持，则无法管理或部署到 FDM 管理 设备。向支持团队发送请求以启用此平台。通过 TAC 打开提交支持请求, on page 752

Secure Firewall Threat Defense 防火墙是思科的下一代防火墙。它力求将下一代防火墙服务与 ASA 平台的精华相结合。它可以安装在许多不同的 ASA 和 Firepower 硬件设备或虚拟机上。

要查看我们支持的功能，请查看使用 Cisco Defense Orchestrator 管理 FDM 管理 设备。有关载入必备条件和要求的完整讨论，请参阅 载入 威胁防御 设备 。

Note Snort 3 适用于运行版本 6.7 及更高版本的 FDM 管理 设备。请注意，您可以随意在 Snort 2 和 Snort 3 之间切换，但存在配置不兼容的风险。有关 Snort 3、支持的设备和软件以及任何限制的详细信息，请参阅升级到 Snort 3.0, on page 219。

CDO 支持的硬件和软件映像

下表的 CDO 列指示了 CDO 在哪个硬件平台上支持的 Firepower Threat Defense 软件版本。

***Table 1: Secure Firewall Threat Defense* 按管理器和版本划分的硬件**

设备平台	设备版本：使用管理中心		设备版本：使用设备管理器	
	客户部署的管理中心	云交付的防火墙管理中心 *	仅设备管理器	设备管理器 + CDO
Firepower 1010、1120 和 1140	6.4+	7.0.3+	6.4+	6.4+
Firepower 1010E	7.2.3+ 7.3 中不支持	7.2.3+ 7.3 中不支持	7.2.3+ 7.3 中不支持	7.2.3+ 7.3 中不支持
Firepower 1150	6.5+	7.0.3+	6.5+	6.5+
Firepower 2110、2120、2130、2140	6.2.1+	7.0.3+	6.2.1+	6.4+
Firepower 4110, 4120, 4140	6.0.1 至 7.2	7.2+	6.5 到 7.2	6.5 到 7.2

设备平台	设备版本：使用管理中心		设备版本：使用设备管理器	
	客户部署的管理中心	云交付的防火墙管理中心 *	仅设备管理器	设备管理器 + CDO
Firepower 4150	6.1 到 7.2	7.2+	6.5 到 7.2	6.5 到 7.2
Firepower 4115、4125、4145	6.4+	7.0.3+	6.5+	6.5+
Firepower 4112	6.6+	7.0.3+	6.6+	6.6+
Firepower 9300: SM-24, SM-36, SM-44	6.0.1 至 7.2	7.0.3+	6.5 到 7.2	6.5 到 7.2
Firepower 9300: SM-40, SM-48, SM-56	6.4+	7.0.3+	6.5+	6.5+
ISA 3000	6.2.3+	7.0.3+	6.2.3+	6.4+
ASA 5506-X、5506H-X、5506W-X	6.0.1 至 6.2.3	-	6.1 至 6.2.3	-
ASA 5508-X、5516-X	6.0.1 至 7.0	7.0.3 至 7.0.x	6.1 至 7.0	6.4 至 7.0
ASA 5512-X	6.0.1 至 6.2.3	-	6.1 至 6.2.3	-
ASA 5515-X	6.0.1 至 6.4	-	6.1 至 6.4	6.4
ASA 5525-X、5545-X、5555-X	6.0.1 至 6.6	-	6.1 至 6.6	6.4 至 6.6

* 云交付的防火墙管理中心 无法管理运行版本 7.1的 FTD 设备或运行任何版本的经典设备。您无法将云管理的设备从 7.0.x 版本升级到7.1版本，除非您取消注册并禁用云管理。我们建议您将设备直接升级到版本 7.2+。

CDO 支持的虚拟机平台和软件映像

下表的 CDO 列指示 CDO 在哪个虚拟设备平台上支持的 Firepower 威胁防御软件版本。

Table 2: 按管理器和版本***FTDv***

设备平台	设备版本：使用管理中心		设备版本：使用设备管理器	
	客户部署的管理中心	云交付的防火墙管理中心 *	仅设备管理器	设备管理器 + CDO
公共云				
Alibaba（阿里巴巴）	7.2+	7.2+	-	—
AWS	6.0.1+	7.0.3+	6.6+	6.6+

设备平台	设备版本：使用管理中心		设备版本：使用设备管理器	
	客户部署的管理中心	云交付的防火墙管理中心 *	仅设备管理器	设备管理器 + CDO
Azure	6.2+	7.0.3+	6.5+	6.5+
GCP	6.7+	7.0.3+	7.2+	7.2+
OCI	6.7+	7.0.3+	-	—
本地/私有云				
HyperFlex	7.0+	7.0.3+	7.0+	7.0+
KVM	6.1+	7.0.3+	6.2.3+	6.4+
Nutanix	7.0+	7.0.3+	7.0+	7.0+
OpenStack	7.0+	7.0.3+	-	—
VMware 7.0	7.0+	7.0.3+	7.0+	7.0+
VMware 6.7	6.5+	7.0.3+	6.5+	6.5+
VMware 6.5	6.2.3+	7.0.3+	6.2.3+	6.4+
VMware 6.0	6.0 至 6.7	-	6.2.2 至 6.7	6.4 至 6.7
VMware 5.5	6.0.1 至 6.2.3	-	6.2.2 至 6.2.3	-
VMware 5.1	仅 6.0.1	-	—	—

* 云交付的防火墙管理中心 无法管理运行版本 7.1的 FTD 设备或运行任何版本的经典设备。您无法将云管理的设备从 7.0.x 版本升级到7.1版本，除非您取消注册并禁用云管理。我们建议您将设备直接升级到版本 7.2+。

有关使用 CDO 管理 Firepower 设备接口的详细信息，请参阅 Firepower 接口配置的指南和限制。

ASA FirePOWER 服务模块

CDO 不支持 ASA FirePOWER 服务模块。

浏览器支持

CDO 支持以下浏览器的最新版本：

- Google Chrome
- Mozilla Firefox

思科防御协调器平台维护计划

Cisco Defense Orchestrator 维护计划

CDO 会每周更新其平台，提供新功能和质量改进。根据此计划，更新可在 3 小时内完成。

大多数情况下，更新会在星期四完成，但如有必要，也可以安排在星期五和星期日进行维护。

表 *3: CDO* 维护时间表

星期	时间 （24 小时制）
星期四	09:00 UTC - 12:00 UTC
星期五	09:00 UTC - 12:00 UTC
星期日	09:00 UTC - 12:00 UTC

在此维护期间，您仍然可以访问您的租户，并且如果您有 云交付的防火墙管理中心，也可以访问该平台。此外，您已载入CDO的设备将继续执行其安全策略。

注释 我们建议您在维护期间不要使用 CDO 来在其管理的设备上部署配置更改。

如果发生阻止 CDO 或 云交付的防火墙管理中心 进行通信的故障，则会尽快在所有受影响的租户上解决该故障，即使并非是在维护时间窗口之内。

云交付的防火墙管理中心维护时间表

在CDO更新云交付的防火墙管理中心环境前大约1周通知在租户上部署了云交付的防火墙管理中心的客户。通过邮件通知租户的超级管理员和管理员用户。CDO还会在其主页上显示一个横幅，通知所有用户即将发布的更新。

在分配给租户区域的维护日的 3 小时维护期内，对租户进行更新最多可能需要 1 小时。在更新租户时，您将无法访问云交付的防火墙管理中心环境，但仍可访问 CDO 的其余部分。

表 *4:* 云交付的防火墙管理中心维护时间表

星期	时间 （24 小时制）	地区
星期三	04:00 UTC - 07:00 UTC	欧洲、中东或非洲 (EMEA)
星期三	17:00 UTC - 20:00 UTC	亚太地区-日本 (APJ)
星期四	09:00 UTC - 12:00 UTC	美洲地区

租户管理

Cisco Defense Orchestrator (CDO) 使您能够在“设置”页面上自定义租户和个人用户帐户的某些方面。在 CDO 菜单栏中，点击左侧导航面板中的**设置 (Settings)**。

相关信息：

- 常规设置，第 44 页
- 用户管理
- 日志记录设置
- 通知设置，第 48 页

常规设置

在右上角的“管理”下拉列表中，点击 **设置**。

请参阅以下有关常规 CDO 设置的主题：

- 用户设置, on page 44
- 对于我的令牌，请参阅 API 令牌, on page 53
- 有关租户设置，请参阅：
  - 启用更改请求跟踪, on page 45
  - 阻止思科支持人员查看您的租户, on page 45
  - 启用计划自动部署的选项, on page 46
  - 默认冲突检测间隔, on page 46
  - Web 分析, on page 47
  - 配置默认定期备份计划, on page 47
  - 租户 ID, on page 47
  - 租户名称, on page 47

用户设置

选择所需的 CDO UI 显示语言。此选择仅影响进行此更改的用户。

我的令牌

有关详细信息，请参阅 API 令牌。API 令牌, on page 53

租户设置

启用更改请求跟踪

启用更改请求跟踪会影响租户的所有用户。要启用更改请求跟踪，请执行以下程序：

Procedure

步骤 1 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 2 点击**常规**选项卡。

步骤 3 点击**更改请求跟踪 (Change Request Tracking)** 下的滑块。

确认后，您会在界面的左下角看到“更改请求”(Change Request) 工具栏，并在“更改日志”(Change Log) 中看到“更改请求”(Change Request) 下拉菜单。

阻止思科支持人员查看您的租户

思科支持将其用户与您的租户相关联，以解决支持请求或主动修复影响多个客户的问题。但是，如果您愿意，可以通过更改帐户设置来阻止思科支持人员访问您的租户。为此，请滑动“防止思科支持人员查看此租户”下的按钮，以显示绿色复选标记。

要防止思科支持人员查看您的租户，请执行以下程序：

Procedure

步骤 1 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 2 点击**常规**选项卡。

步骤 3 点击**阻止思科支持人员查看此租户 (Prevent Cisco support from viewing this tenant)** 下的滑块。

启用自动接受设备更改的选项

启用设备更改自动接受后， Defense Orchestrator 可以自动接受直接在设备上进行的任何更改。如果禁用或稍后禁用此选项，则需要先查看每个设备冲突，然后才能接受它。

要启用设备更改自动接受，请执行以下程序：

Procedure

步骤 1 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 2 点击**常规**选项卡。

步骤 3 点击**启用自动接受设备更改的选项 (Enable the option to auto-accept device changes)** 下的滑块。

默认冲突检测间隔

此时间间隔将确定CDO轮询已载入的设备以了解更改的频率。此选择会影响使用此租户管理的所有设备，并且可以随时更改。

Note 选择一个或多个设备后，可以通过**清单 (Inventory)** 页面中的**冲突检测 (Conflict Detection)** 选项覆盖此选择。

要配置此选项并选择新的冲突检测间隔，请执行以下程序：

Procedure

步骤 1 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 2 点击**常规设置 (General Settings)** 选项卡。

步骤 3 点击**默认冲突检测间隔 (Default Conflict Detection Interval)** 下拉菜单，然后选择一个时间值。

启用计划自动部署的选项

如果启用计划自动部署选项，您就可以计划在方便的未来日期和时间进行部署。启用后，您可以计划单次或定期自动部署。要计划自动部署，请参阅计划自动部署。

请注意，如果其本身的  有待处理的更改，则在CDO上对设备所做的更改不会自动部署到该设备。如果设备未处于**已同步 (Synced)** 状态（例如**检测到冲突 (Conflict Detected)** 或**未同步 (Not Synced)**），则不会执行计划部署。作业页面会列出计划部署失败的所有实例。

如果**启用计划自动部署的选项 (Enable the Option to Schedule Automatic Deployments)** 被关闭，则所有计划的部署都将被删除。

Important 如果使用CDO为一台设备创建多个计划部署，则新部署会覆盖现有部署。如果使用 API 创建多个计划部署，则**必须**首先删除现有部署，然后才能计划新的部署。

要启用该选项以计划自动部署，请执行以下程序：

Procedure

步骤 1 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 2 点击**常规设置 (General Settings)** 选项卡。

步骤 3 点击**启用计划自动部署的选项 (Enable the option to schedule automatic deployments)** 下的滑块。

Web 分析

网络分析可根据页面点击量向思科提供匿名产品使用情况信息。这类信息包括查看的页面、在页面上花费的时间、浏览器版本、产品版本、设备主机名等。此信息可帮助思科确定功能使用模式，帮助思科改进产品。所有使用情况数据均为匿名数据，且不会传输敏感数据。

默认启用网络分析。要禁用 Web 分析或在将来启用，请执行以下程序：

Procedure

步骤 1 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 2 点击**常规设置 (General Settings)** 选项卡。

步骤 3 点击**网络分析 (Web Analytics)** 下的滑块。

配置默认定期备份计划

要使设备之间的备份计划保持一致，请使用此设置配置您自己的默认定期备份计划。为特定设备安排备份时，可以使用默认设置或对其进行更改。更改默认定期备份计划不会更改任何现有的计划备份或定期备份计划。

Procedure

步骤 1 在**频率 (Frequency)** 字段中，选择每日、每周或每月备份。

步骤 2 选择一天中要进行备份的时间（24 小时制）。请注意，以协调世界时 (UTC) 安排时间。

- 对于每周备份：选中要在星期几进行备份。
- 对于每月备份：点击**当月的天数 (Days of Month)** 字段，然后添加要计划备份的每月日期。注意：如果输入第 31 天，但一个月中没有 31 天，则不会进行备份。为计划的备份时间指定名称和说明。

步骤 3 点击**保存 (Save)**。

有关其他信息，请参阅配置单个 FTD 的定期备份计划。为单个设备配置定期备份计划FDM 管理, on page 205

租户 ID

租户 ID 标识租户。如果您需要联系思科技术支持中心 (TAC)，此信息将非常有用。

租户名称

您的租户名称还标识您的租户。请注意，租户名称不是组织名称。如果您需要联系思科技术支持中心 (TAC)，此信息将非常有用。

通知设置

您可以订用电子邮件通知，以便在与您的租户关联的设备遇到特定操作时从CDO接收通知。虽然这些通知适用于与您的租户关联的所有设备，但并非所有设备类型都支持所有可用的选项。另请注意，对下面列出的 CDO 通知所做的更改会实时自动更新，不需要部署。

来自CDO的邮件通知会指明操作类型和受影响的设备。有关设备当前状态和操作内容的更多信息，我们建议您登录 CDO 并检查受影响设备的变更日志。

在左侧的导航栏中，点击**设置 (Settings)** > **通知设置 (Notification Settings)**。

发送设备工作流程警报

Note 您必须具有**超级管理员**用户角色才能更改这些设置或手动订用通知。有关详细信息，请参阅思科防御协调器中的用户角色。

请务必检查您想要通知的所有设备工作流程场景。手动检查以下任何操作：

- **部署 (Deployments)** - 此操作不包括 SSH 或 IOS 设备的集成实例。
- **备份 (Backups)** - 此操作仅适用于 FDM 管理 设备。
- **升级 (Upgrades)** - 此操作仅适用于 ASA 和 FDM 管理 设备。
- **将 FTD 迁移到云** - 此操作适用于更改 FTD

  从 FMC 到 CDO 的设备管理器。

发送设备事件警报

Note 您必须具有**超级管理员**用户角色才能更改这些设置或手动订用通知。有关详细信息，请参阅思科防御协调器中的用户角色。

请务必检查您想要通知的所有设备工作流程场景。手动检查以下任何操作：

- **离线 (Went offline)** - 此操作适用于与您的租户关联的所有设备。
- **恢复在线 (Back online)** - 此操作适用于与您的租户关联的所有设备。
- **检测到冲突 (Conflict detected)** - 此操作适用于与您的租户关联的所有设备。
- **HA 状态已更改 (HA state changed)** - 此操作指示 HA 或故障转移对中的设备、当前状态及其更改后的状态。此操作适用于与您的租户关联的所有 HA 和故障转移配置。
- **站点间会话已断开连接 (Site-to-Site session disconnected)** - 此操作适用于租户中配置的所有站点间 VPN 配置。

发送后台日志搜索警报

您必须具有**超级管理员**用户角色才能更改这些设置或手动订用通知。有关详细信息，请参阅思科防御协调器中的用户角色。

当任何人登录到租户创建后台搜索时，向您发送警报。请务必检查您想要通知的所有设备工作流程场景。手动检查以下任何操作：

- **搜索已开始 (Search started)** - 搜索开始时收到通知。这适用于立即搜索和计划搜索。
- **搜索完成 (Search completed)** - 搜索结束时收到通知。这适用于立即搜索和计划搜索。
- **搜索失败 (Search failed)** - 搜索失败时收到通知。这适用于立即搜索和计划搜索。请检查参数或查询，然后重试。

用户

启用**订用以接收警报 (Subscribe to receive alerts)** 切换按钮，以便将与您的租户登录关联的邮件添加到通知列表。要从邮件程序列表中删除您的邮件，请取消选择切换按钮，使其呈灰色显示。

请注意，某些用户角色对此设置页面的订用操作具有有限的访问权限；具有**超级管理员**用户角色的用户可以添加或删除邮件条目。要将除您自己以外的其他人或备用邮箱联系人添加到订用用户列表，请点击  并手动输入邮箱。

Warning 如果要手动添加用户，请务必输入正确的邮箱。CDO 不会检查与您的租户关联的已知用户的邮件地址。

查看 CDO 通知

点击通知图标  可查看租户上发生的最新警报。CDO 中的通知将在 30 天后从通知列表中删除。

Note 您在**发送警报 (Send Alerts When)** 部分中所做的选择会影响 CDO 中显示的通知类型。

服务集成

在您的消息传递应用上启用传入 Webhook，并直接将 CDO 通知接收到您的应用控制面板。您必须手动允许所选应用上的传入 Webhook 并检索 Webhook URL，以便在 CDO 中启用此选项。有关详细信息，请参阅为 CDO 通知启用服务集成。

为 CDO 通知启用服务集成

启用服务集成，以便通过指定的消息传送应用或服务来转发CDO通知。您需要从消息传递应用生成Webhook URL，并将 CDO 指向 CDO 的**通知设置 (Notification Settings)** 页面中的 Webhook 以接收通知。

CDO 本身支持 Cisco Webex 和 Slack 作为服务集成。发送到这些服务的邮件会经过专门的格式化，可用于通道和自动化机器人。

注释 在**通知设置 (Notification Settings)** 页面中选择的通知是转发到消息传送应用的事件。

Webex Teams 的传入 Webhook

开始之前

CDO 通知显示在指定的工作空间中，或显示为私人邮件中的自动化机器人。有关 Webex Teams 如何处理 Webhook 的更多信息，请参阅面向开发人员的 Webex。https://developer.webex.com/docs/api/guides/webhooks

使用以下程序为 Webex Teams 允许传入 Webhook：

过程

步骤 1 打开 Webex Teams 应用。

步骤 2 在窗口的左下角，点击应用图标。此操作将在您的首选浏览器中的新选项卡中打开思科 Webex 应用中心。

步骤 3 使用搜索栏查找传入 Webhook。

步骤 4 选择**连接 (Connect)**。此操作会在新选项卡中打开 OAuth 授权以允许应用。

步骤 5 选择**接受 (Accept)**。该选项卡会自动重定向到应用的配置页面。

步骤 6 进行以下配置：

- Webhook 名称 - 提供用于标识此应用提供的消息的名称。
- 选择空间 - 使用下拉菜单选择空间。空间必须已存在于 Webex 团队中。如果空间不存在，您可以在 Webex Teams 中创建新空间并刷新应用的配置页面以显示新空间。

步骤 7 选择**添加**。您选择的 Webex Space 将收到添加应用的通知。

步骤 8 复制 Webhook URL。

步骤 9 登录至 CDO。

步骤 10 在左侧的导航栏中，点击**设置 (Settings)** > **通知设置 (Notification Settings)**。

步骤 11 滚动到服务集成。

步骤 12 点击蓝色加号按钮。

步骤 13 输入 **Name**。此名称在 CDO 中显示为已配置的服务集成。它不会出现在转发到已配置服务的任何事件中。

步骤 14 展开下拉菜单并选择 Webex 作为服务类型。

步骤 15 粘贴从服务生成的 Webhook URL。

步骤 16 点击“确定”。

Slack 的传入 Webhook

CDO 通知显示在指定渠道中，或显示为私人邮件中的自动机器人。有关 Slack 如何处理传入 Webhook 的详细信息，请参阅 Slack 应用。https://api.slack.com/tutorials/slack-apps-hello-world

使用以下程序允许 Slack 的传入 Webhook：

过程

步骤 1 登录您的 Slack 帐户。

步骤 2 在左侧的面板中，滚动到底部并选择添加应用。

步骤 3 在应用目录中搜索传入 Webhook 并找到该应用。选择**添加**。

步骤 4 如果您不是 Slack 工作空间的管理员，则必须向组织的管理员发送请求，并等待应用添加到您的账户。选择请求配置。输入可选消息，然后选择提交请求。

步骤 5 为工作空间启用传入 Webhook 应用后，刷新 Slack 设置页面，然后选择将新 Webhook 添加到工作空间。

步骤 6 使用下拉菜单选择要在其中显示 CDO 通知的 Slack 通道。选择**授权 (Authorize)**。如果您在等待请求启用时离开此页面，只需登录 Slack 并在左上角选择工作空间名称即可。从下拉菜单中选择自定义工作空间，然后选择配置应用。导航至管理自定义集成。> 选择传入 Webhook 以打开应用的登录页面，然后从选项卡中选择配置。这将列出您的工作空间中启用了此应用的所有用户。您只能查看和编辑账户的配置。选择您的工作空间名称以编辑配置并继续。

步骤 7 “Slack 设置”页面会将您重定向到应用的配置页面。找到并复制 Webhook URL。

步骤 8 登录至 CDO。

步骤 9 在左侧的导航栏中，点击**设置 (Settings)** > **通知设置 (Notification Settings)**。

步骤 10 滚动到服务集成。

步骤 11 点击蓝色加号按钮。

步骤 12 输入 **Name**。此名称在 CDO 中显示为已配置的服务集成。它不会出现在转发到已配置服务的任何事件中。

步骤 13 展开下拉菜单并选择 Slack 作为服务类型。

步骤 14 粘贴从服务生成的 Webhook URL。

步骤 15 点击“确定”。

自定义集成的传入 Webhook

开始之前

CDO 不会为自定义集成设置消息格式。如果您选择集成自定义服务或应用，CDO 会发送 JSON 消息。

有关如何启用传入 Webhook 和生成 Webhook URL 的信息，请参阅服务文档。获得 Webhook URL 后，请使用以下程序启用 Webhook：

过程

步骤 1 从您选择的自定义服务或应用生成并复制 Webhook URL。

步骤 2 登录至 CDO。

步骤 3 在左侧的导航栏中，点击**设置 (Settings)** > **通知设置 (Notification Settings)**。

步骤 4 滚动到服务集成。

步骤 5 点击蓝色加号按钮。

步骤 6 输入 **Name**。此名称在 CDO 中显示为已配置的服务集成。它不会出现在转发到已配置服务的任何事件中。

步骤 7 展开下拉菜单并选择自定义作为服务类型。

步骤 8 粘贴从服务生成的 Webhook URL。

步骤 9 点击“确定”。

日志记录设置

查看每月事件日志记录限制以及限制重置前剩余的天数。请注意，存储的日志记录表示思科云接收的压缩事件数据。

点击“查看历史使用情况”可查看租户在过去 12 个月内收到的所有日志记录。

您还可以使用链接请求额外的存储空间。

将 SAML 单点登录与 Cisco Defense Orchestrator 集成

思科防御协调器 (CDO) 使用 Cisco Secure Sign-On 作为 SAML 单点登录身份提供商 (Idp)，并使用 Duo Security 进行多因素身份验证 (MFA)。这是 CDO 的首选身份验证方法。

但是，如果客户希望将自己的 SAML 单点登录 IdP 解决方案与 CDO 集成，只要他们的 IdP 支持 SAML 2.0 和身份提供程序启动的工作流程，就可以。

要将您自己的 SAML 解决方案与 CDO 集成，您必须联系支持人员并创建案例。有关说明，请参阅《思Cisco Security Cloud Sign On 第三方身份提供程序集成指南》。

Attention 提交支持案例时，请确保为您的请求选择**手动选择技术 (Manually Select A Technology)**，然后选择 **SecureX - 登录和管理 (SecureX - Sign-on and Administration)**，以便与正确的团队联系。

更新 SSO 证书

您的身份提供程序 (IdP) 通常与 SecureX SSO 集成。创建思科 TAC 支持案例并提供 metadata.xml 文件。https://www.cisco.com/c/en/us/support/index.html有关更多信息，请参阅《思科 SecureX 登录第三方身份提供程序集成指南》。

注意 当您提交支持案例时，请确保为您的请求选择手动选择技术，然后选择 SecureX - 登录和管理，以便联系正确的团队。

（仅限旧版）如果您的身份提供程序 (IdP) 直接与 CDO 集成，请向 CDO TAC 提交支持请求，并提供 metadata.xml 文件。CDO 客户如何通过 TAC 提交支持请求，第 753 页

注释 我们强烈建议您将 IdP 与 SecureX SSO 集成，而不是直接将其与 CDO 集成。

API 令牌

开发人员在进行 CDO REST API 调用时使用 CDO API 令牌。必须在 REST API 授权报头中插入 API 令牌，调用才能成功。API 令牌是“长期”访问令牌，不会过期；但是，您可以续订和撤销它们。

您可以从 CDO 中生成 API 令牌。这些令牌仅在生成后立即可见，并且只要“常规设置”页面处于打开状态。如果您在 CDO 中打开另一个页面并返回到**常规设置 (General Settings)** 页面，则该令牌不再可见，但很明显已发出令牌。

个人用户可以为特定租户创建自己的令牌。一个用户不能代表另一个用户生成令牌。令牌特定于账户-租户对，不能用于其他用户-租户组合。

API 令牌格式和声明

API 令牌是 JSON Web 令牌 (JWT)。要了解有关 JWT 令牌格式的更多信息，请阅读 JSON Web 令牌简介。https://jwt.io/introduction/

CDO API 令牌提供以下一组声明：

- id - 用户/设备 uid
- parentId - 租户 uid
- ver - 公钥的版本（初始版本为 0，例如 cdo_jwt_sig_pub_key.0）
- 订用 - 订用（可选）安全服务交换

- client_id - " api-client "
- jti - 令牌 ID

令牌管理

生成 API 令牌

Procedure

步骤 1 在左侧的导航栏中，点击**设置 (Settings)** > **常规设置 (General Settings)**。

步骤 2 在我的令牌中，点击生成 API 令牌。

步骤 3 根据企业维护敏感数据的最佳实践，将令牌保存在安全位置。

续订 API 令牌

API 令牌不会过期。但是，如果令牌丢失、遭到破坏或符合其企业的安全准则，用户可以选择更新其 API 令牌。

Procedure

步骤 1 在左侧导航栏中，点击 **设置 (Settings)** > **常规设置 (General Settings)**。

步骤 2 在“我的令牌”(My Tokens) 中，点击**续约 (Renew)**。CDO 会生成新的令牌。

步骤 3 根据企业维护敏感数据的最佳实践，将新令牌保存在安全位置。

撤销 API 令牌

Procedure

步骤 1 在左侧导航栏中，点击 **设置 (Settings)** > **常规设置 (General Settings)**。

步骤 2 在“我的令牌”(My Tokens) 中，点击**撤销 (Revoke)**。CDO 将撤销令牌。

身份提供程序账户与思科防御协调器用户记录之间的关系

要登录思科防御协调器 (CDO)，客户需要具有符合 SAML 2.0 标准的身份提供程序 (IdP)、多因素身份验证提供程序以及 CDO 中的用户记录。IdP 账户包含用户的凭证，IdP 根据这些凭证对用户进行身份验证。多因素身份验证提供了额外的身份安全层。CDO 用户记录主要包含用户名、与其关联的

CDO 租户以及用户的角色。当用户登录时，CDO 会尝试将 IdP 的用户 ID 映射到 CDO 中租户的现有用户记录。当 CDO 找到匹配项时，用户将登录到该租户。

除非您的企业有自己的单点登录身份提供程序，否则身份提供程序是思科安全云登录。Cisco Security Cloud Sign On 使用 Duo 进行多因素身份验证。客户可以选择将 SAML 单点登录与 Cisco Defense Orchestrator 集成。

登录工作流程

以下是 IdP 账户如何与 CDO 用户记录交互以登录 CDO 用户的简化说明：

Procedure

步骤 1 用户通过登录到符合 SAML 2.0 标准的身份提供程序 (IdP)（例如 Cisco Security Cloud Sign On (https://sign-on.security.cisco.com)）来请求访问 CDO，以进行身份验证。

步骤 2 IdP 发出用户真实可信的 SAML 断言，门户显示用户可以访问的应用，例如表示 https://defenseorchestrator.com 或 https://defenseorchestrator.eu 或 https://www.apj.cdo 的磁贴.cisco.com/。https://defenseorchestrator.com/https://defenseorchestrator.eu/https://www.apj.cdo.cisco.com/

步骤 3 CDO 验证 SAML 断言，提取用户名并尝试在其租户中查找与该用户名对应的用户记录。

- 如果用户在 CDO 上的单个租户上有用户记录，则 CDO 会向用户授予对租户的访问权限，并且用户的角色决定了他们可以执行的操作。
- 如果用户在多个租户上有用户记录，则CDO会向经过身份验证的用户显示可供他们选择的租户列表。用户选择一个租户并允许访问该租户。用户在该特定租户上的角色决定了他们可以执行的操作。
- 如果 CDO 没有将经过身份验证的用户映射到租户上的用户记录，则 CDO 会显示一个登录页面，让用户有机会了解有关 CDO 的更多信息或请求免费试用。

在 CDO 中创建用户记录不会在 IdP 中创建账户，在 IdP 中创建账户不会在 CDO 中创建用户记录。

同样，删除 IdP 上的账户并不意味着您已从 CDO 中删除用户记录；但是，如果没有 IdP 账户，则无法向 CDO 对用户进行身份验证。删除 CDO用户记录并不意味着您已删除 IdP 账户；但是，如果没有 CDO用户记录，经过身份验证的用户将无法访问 CDO 租户。

此架构的含义

使用 Cisco Security Cloud Sign On 的客户

对于使用 CDO 的 Cisco Security Cloud Sign On 身份提供程序的客户，超级管理员可以在 CDO 中创建用户记录，并且用户可以向 CDO 自行注册。如果两个用户名匹配，并且用户已正确进行身份验证，则用户可以登录 CDO。

如果超级管理员需要阻止用户访问 CDO，他们只需删除 CDO 用户的用户记录即可。Cisco Security Cloud Sign On 账户仍然存在，如果超级管理员想要恢复用户，他们可以使用与 Cisco Security Cloud Sign On 相同的用户名创建新的 CDO 用户记录。

如果客户遇到需要致电我们的技术支持中心 (TAC) 的 CDO 问题，客户可以为 TAC 工程师创建用户记录，以便他们可以调查租户并向客户报告信息和建议。

拥有自己的身份提供程序的客户

对于将 SAML 单点登录与 Cisco Defense Orchestrator 集成，他们可以控制身份提供程序账户和 CDO 租户。这些客户可以在 CDO 中创建和管理身份提供程序账户和用户记录。

如果他们需要阻止用户访问 CDO，他们可以删除 IdP 账户和/或 CDO 用户记录。

如果他们需要思科 TAC 的帮助，他们可以为其 TAC 工程师创建具有只读角色的身份提供程序账户和 CDO 用户记录。然后，TAC 工程师将能够访问客户的 CDO 租户，进行调查，并向客户报告信息和建议。

思科托管服务提供商

如果思科托管服务提供商 (MSP) 使用 CDO 的 Cisco Security Cloud Sign On IdP，则他们可以自行注册 Cisco Security Cloud Sign On，他们的客户可以在 CDO 中为其创建用户记录，以便 MSP 可以管理客户的租户。当然，客户可以在选择时完全控制删除 MSP 的记录。

相关主题

- 常规设置
- 用户管理
- 思科防御协调器中的用户角色

管理多租户门户

CDO 多租户门户视图检索并显示来自多个租户的所有设备的信息。此多租户门户显示设备状态、设备上运行的软件版本等。

Note 在多租户门户中，您可以跨多个区域添加租户，并查看这些租户管理的设备。您无法从多租户门户编辑任何租户或配置任何设备。

准备工作

多租户门户仅在您的租户上启用该功能时可用。要为租户启用多租户门户，请向思科 TAC 提交支持请求。解决支持请求并创建门户后，门户上具有“超级管理员”(Super Admin) 角色的用户就可以向其添加租户。

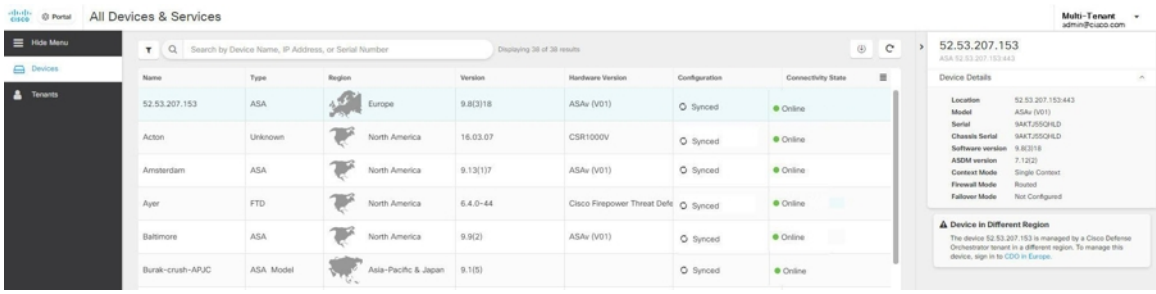
我们建议您从 Web 浏览器清除缓存和 Cookie，以避免可能发生的某些浏览器相关问题。

多租户门户

门户提供以下菜单：

- **设备**：
  - 显示驻留在添加到门户的租户中的所有设备。使用过滤器和搜索字段搜索要查看的设备。您可以点击设备以查看其状态、自行激活方法、防火墙模式、故障切换模式、软件版本等。
  - 该界面提供了一个列选择器，允许您选择或清除要在表中查看的设备属性。除“AnyConnect 远程访问 VPN”外，默认情况下会选择所有其他设备属性。如果您自定义表，CDO 会在您下次登录 CDO 时记住您的选择。
  - 您可以点击设备以在右侧查看其详细信息。
  - 您可以将 门户信息导出为逗号分隔值 (.csv) 文件。此信息可帮助您分析设备或将其发送给无权访问的人员。每次导出数据时，CDO 都会创建一个新的 .csv 文件，其中创建的文件会在名称中包含日期和时间。
  - 您只能从管理设备的 CDO 租户管理设备。多租户门户提供**管理设备 (Manage devices)** 链接，可将您定向到CDO租户页面。如果您在该租户上有账户，并且该租户与门户位于同一区域，您将在设备上看到此链接。如果您没有访问租户的权限，您将看不到管理设备链接。您可以联系组织中的超级管理员获取权限。

Note 如果管理设备的租户位于其他区域，您将在该区域看到用于登录 CDO 的链接。如果您无权访问该区域中的 CDO 或该区域中的租户，您将无法管理设备。



- **租户**：
  - 显示添加到门户的租户。
  - 它允许超级管理员用户将租户添加到门户。
  - 您可以点击 查看 CDO 租户的主页。

将租户添加到多租户门户

具有超级管理员角色的用户可以向门户添加租户。您可以跨多个区域添加租户。例如，您可以将欧洲区域的租户添加到美国区域，反之亦然。

Important 我们建议您为租户创建仅 API 用户，并生成用于向 CDO 进行身份验证的 API 令牌。

Note 如果要将多个租户添加到门户，请从每个租户生成 API 令牌并将其粘贴到文本文件中。然后，您可以轻松地将租户逐个添加到门户，而无需每次都切换到租户以生成令牌。

Procedure

步骤 1 在左侧的导航栏中，点击**设置 (Settings)** > **常规设置 (General Settings)** > **我的令牌 (My Tokens)**。

步骤 2 点击生成 API 令牌，然后复制它。

步骤 3 转到门户，然后点击租户选项卡。

步骤 4 点击右侧的添加租户按钮。 

步骤 5 粘贴令牌，然后点击保存。

从多租户门户删除租户

Procedure

步骤 1 转到门户，然后点击租户选项卡。

步骤 2 点击右侧显示的相应删除图标，删除所需的租户。

步骤 3 点击**删除 (Remove)**。关联的设备也会从门户中删除。

管理租户门户设置

Cisco Defense Orchestrator （ Defense Orchestrator ）使您能够在“设置”页面上自定义多租户门户和个人用户帐户的某些方面。点击左侧导航栏中的设置，访问**设置 (Settings)** 页面。

设置

常规设置

网络分析可根据页面点击量向思科提供匿名产品使用情况信息。这类信息包括查看的页面、在页面上花费的时间、浏览器版本、产品版本、设备主机名等。此信息可帮助思科确定功能使用模式，帮助思科改进产品。所有使用情况数据均为匿名数据，且不会传输敏感数据。

默认启用网络分析。要禁用 Web 分析或在将来启用，请执行以下程序：

1. 在 CDO 控制面板中，点击左侧导航栏中的**设置 (Settings)**。
2. 点击 **General Settings**。
3. 点击**网络分析 (Web Analytics)** 下的滑块。

用户管理

您可以在**用户管理 (User Management)** 屏幕上查看与多租户门户关联的所有用户记录。您可以添加、编辑或删除用户帐户。有关详细信息，请参阅用户管理。

切换租户

如果您有多个门户租户，则可以在不同的门户或租户之间切换，而无需注销 CDO。

Procedure

步骤 1 在多租户门户上，点击右上角显示的租户菜单。
步骤 2 点击**切换租户 (Switch tenant)**。
步骤 3 选择要查看的门户或租户。

思科成功网络

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，设备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。数据流遥测提供一种机制，可从设备选择相关数据，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。
- 帮助思科改善我们的产品。

设备将建立并始终维护该安全连接，使您能够注册思科成功网络。注册设备后，可以更改思科成功网络设置。

注释

- 对于 威胁防御可用性对，主用设备的选择会覆盖备用设备上的思科成功网络设置。
- CDO 不会管理思科成功网络设置。通过 防火墙设备管理器用户界面管理的设置和遥测信息。

启用或禁用思科成功网络

在初始系统设置期间，系统会提示您将设备注册到思科智能软件管理器。如果您选择使用90天的评估许可证，必须在评估期结束前注册设备。要注册该设备，请使用思科智能软件管理器（在“智能许可”页面上）注册该设备，或者通过输入注册密钥使用CDO进行注册。

注册设备时，您的虚拟帐户会向设备分配许可证。注册设备也会注册已启用的任何可选许可证。

您可以通过禁用思科成功网络随时关闭此连接，但只能通过 防火墙设备管理器 UI 禁用此选项。禁用上述功能将断开设备与云的连接。断开连接不会影响接收更新或运行智能许可功能，该功能将继续正常运行。有关详细信息，请参阅《Firepower 设备管理器配置指南》（6.4.0 版或更高版本）**系统管理**一章的“连接到思科成功网络”部分。

用户管理

在CDO中创建或编辑用户记录之前，请阅读身份提供程序账户与思科防御协调器用户记录之间的关系以了解身份提供程序 (IdP) 账户与用户记录的交互方式。CDO 用户需要 CDO 记录和相应的 IdP 账户，这样他们才能通过身份验证并访问您的 CDO 租户。

除非您的企业有自己的 IdP，否则思科安全登录是所有 CDO 租户的身份提供程序。本文的其余部分假设您使用思科安全登录作为身份提供程序。

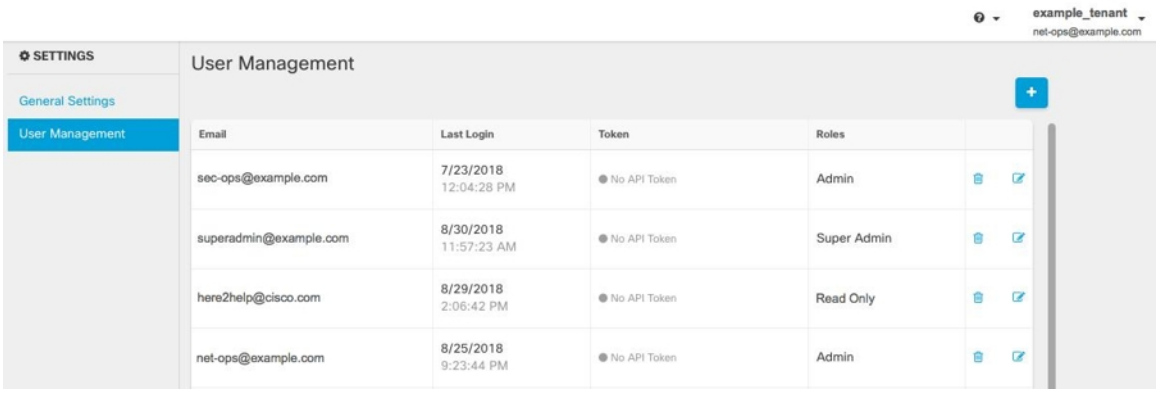
您可以在**用户管理 (User Management)** 屏幕上查看与您的租户关联的所有用户记录。这包括临时与您的账户关联以解决支持请求的任何思科支持工程师。

查看与您的租户关联的用户记录

过程

步骤 1 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 2 点击**用户管理**。



注释 要防止思科支持人员访问您的租户，请在“常规设置”页面中配置您的账户设置。常规设置，第 44 页

用户管理中的 Active Directory 组

对于大量用户的高周转率的租户，您可以将 CDO 映射到 Active Directory (AD) 组，而不是将个人用户添加到CDO，以便更轻松地管理用户列表和用户角色。任何用户更改（例如添加新用户或删除现有用户）现在都可以在 Active Directory 中完成，而不再需要在 CDO 中完成。

您必须具有超级管理员用户角色，才能从“用户管理”页面添加、编辑或删除 AD 组。有关详细信息，请参阅思科防御协调器中的用户角色。

“Active Directory 组”选项卡

设置 (Settings) 页面的“用户管理”(User Management) 部分具有当前映射到 CDO 的 Active Directory 组的选项卡。最重要的是，此页面显示 AD 管理器中分配的 AD 组的角色。

AD 组中的用户不会在 Active Directory Groups 选项卡或 Users 选项卡中单独列出。

“审核日志”选项卡

“设置”(Settings) 页面的“用户管理”(User Management) 部分有一个用于审核日志的选项卡。此新部分显示访问 CDO 租户的所有用户的最后登录时间，以及每个用户在上次登录时的角色。这包括显式用户登录和 AD 组登录。

多角色用户

作为 CDO 中 IAM 功能的扩展，用户现在可以拥有多个角色。

一个用户可以属于 AD 中的多个组，并且每个组都可以在 CDO 中定义为不同的 CDO 角色。用户在登录时获得的最终权限是用户所属的 CDO 中定义的所有 AD 组的角色的组合。例如，如果用户属于两个 AD 组，并且这两个组都以两个不同的角色（例如仅编辑和仅部署）添加到 CDO 中，则该用户将同时具有仅编辑和仅部署权限。这适用于任意数量的组和角色。

AD 组映射只需在 CDO 中定义一次，然后通过在不同组之间添加、删除或移动用户，即可在 AD 中实现对用户的访问和权限管理。

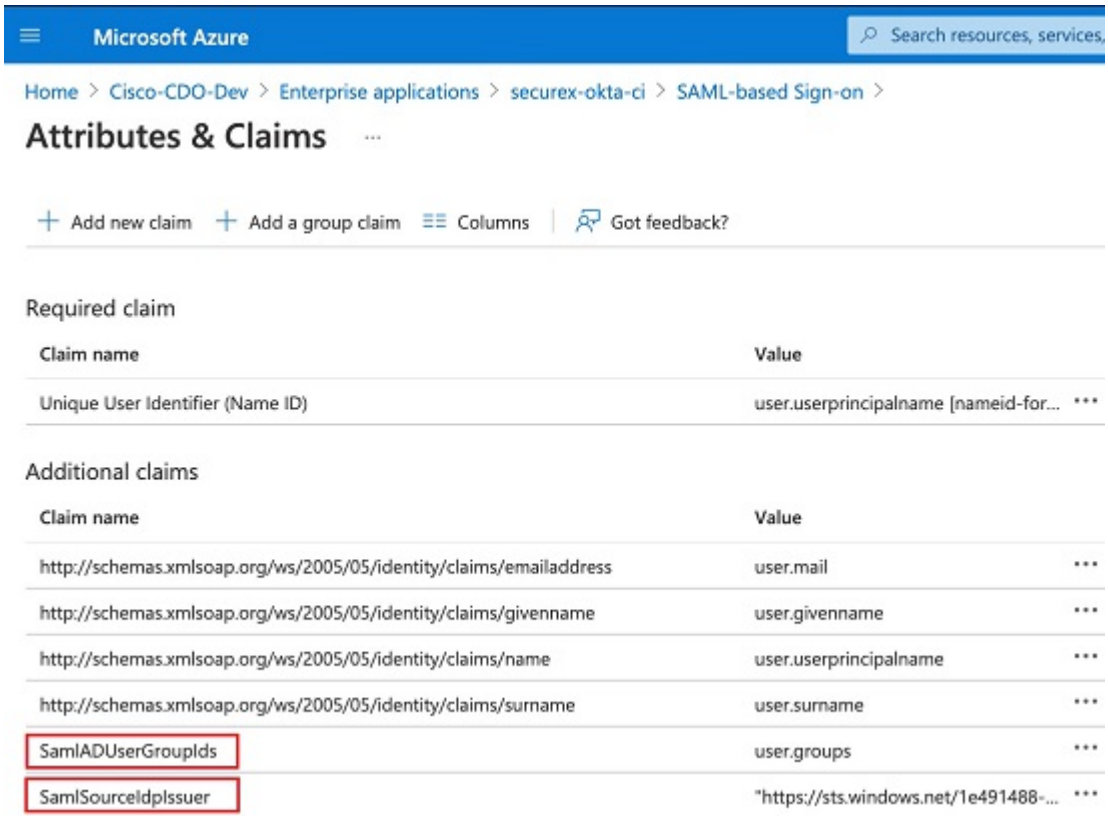
注释 如果用户既是单个用户又是同一租户上的 AD 组的一部分，则单个用户的用户角色将覆盖 AD 组的用户角色。

准备工作

在将 AD 组映射作为用户管理形式添加到 CDO 之前，您必须将 AD 与 SecureX 集成。如果您的 AD 身份提供程序 (IdP) 尚未集成，则必须执行以下操作：

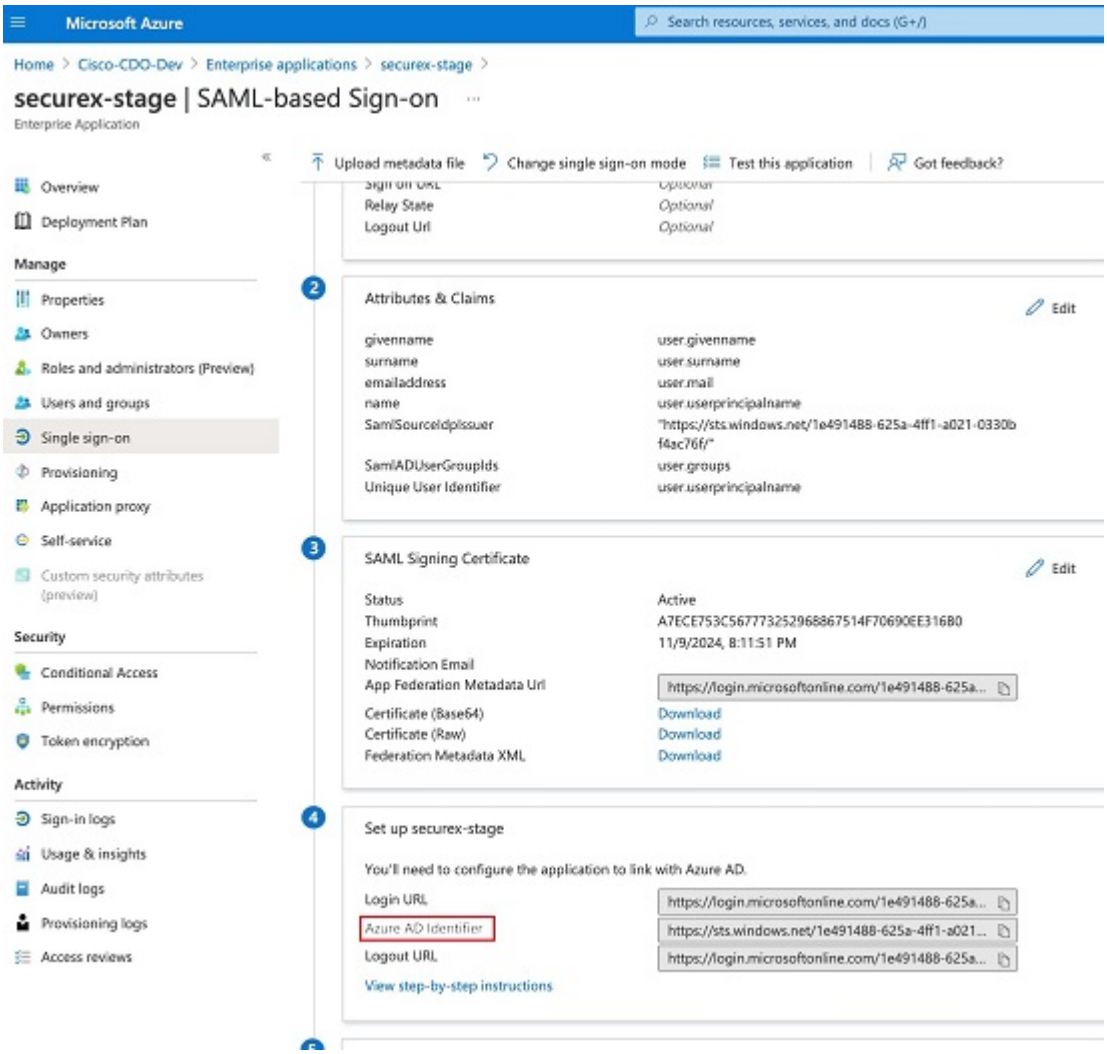
1. 向思科 TAC 提交支持案例，并请求使用以下信息进行自定义 AD IdP 集成：
   https://mycase.cloudapps.cisco.com/case
   - 您的 CDO 租户名称和区域。
   - 定义自定义路由的域（例如：@cisco.com、@myenterprise.com）。
   - XML 格式的证书和联合元数据。
2. 在 AD 中添加以下自定义 SAML 声明。请注意，这些值区分大小写。
   - SamlADUserGroupIds - 此属性描述用户在 AD 上的所有组关联。例如，在 Azure 中选择 + 添加组申领，如下面的屏幕截图所示：

     图 *3: Active Directory* 中定义的自定义声明



   - SamlSourceIdpIssuer - 此属性唯一标识 AD 实例。例如，在 Azure 中选择 + 添加组申领，然后滚动查找 Azure AD 标识符，如下面的屏幕截图所示：

图 *4:* 找到 ***Azure Active Directory*** 标识符



添加用于用户管理的 Active Directory 组

过程

步骤 1 登录 CDO。

步骤 2 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 3 点击 **用户管理** 选项卡。

步骤 4 选择表顶部的 Active Directory 组选项卡。

步骤 5 如果当前没有 AD 组，请点击添加 AD 组。如果有现有条目，请点击添加按钮。

步骤 6 输入以下信息：

- **组名称 (Group Name)** - 输入唯一的名称。此名称不必与 AD 中的组名称匹配。CDO 不支持此字段的特殊字符。
- 组标识符 - 从您的 AD 手动输入组标识符。组标识符的值应与自定义声明定义中的组标识符相同。它可以是与组的唯一标识对应的任何值，例如，my-f Favorite-group、12345 等。
- AD 颁发者 - 手动输入 AD 中的 AD 颁发者值。
- 角色 - 确定此 AD 组中包含的所有用户的角色。有关详细信息，请参阅用户角色。
- （可选）备注 - 添加适用于此 AD 组的任何备注。

步骤 7 点击**确定**。

编辑用于用户管理的 Active Directory 组

开始之前

请注意，在 CDO 中编辑 AD 组的用户管理仅允许修改 CDO 如何限制 AD 组。您无法在 CDO 中编辑 AD 组本身。必须使用 AD 编辑 AD 组中的用户列表。

过程

步骤 1 登录 CDO。

步骤 2 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 3 点击 **用户管理** 选项卡。

步骤 4 选择表顶部的 Active Directory 组选项卡。

步骤 5 确定要编辑的 AD 组，然后选择编辑图标。

步骤 6 修改以下值：

- **组名称 (Group Name)** - 输入唯一的名称。CDO 不支持此字段的特殊字符。
- 组标识符 - 从您的 AD 手动输入组标识符。组标识符的值应与自定义声明定义中的组标识符相同。它可以是与组的唯一标识对应的任何值，例如，my-f Favorite-group、12345 等。
- AD 颁发者 - 手动输入 AD 中的 AD 颁发者值。
- 角色 - 确定此 AD 组中包含的所有用户的角色。有关详细信息，请参阅用户角色。
- 备注 - 添加适用于此 AD 组的任何备注。

删除用于用户管理的 Active Directory 组

过程

步骤 1 登录 CDO。
步骤 2 在右上角的“管理”下拉列表中，点击 **设置**。
步骤 3 点击 **用户管理** 选项卡。
步骤 4 选择表顶部的 Active Directory 组选项卡。
步骤 5 确定要删除的 AD 组。
步骤 6 选择删除图标。
步骤 7 点击确定以确认要删除 AD 组。

创建新的 CDO 用户

要创建新的 CDO 用户，需要执行这两项任务。它们不需要按顺序执行：

- 为新用户创建 Cisco Security Cloud Sign On 账户
- 使用您的 CDO 用户名创建 CDO 用户记录

完成这些任务后，用户可以新用户从思科安全登录控制面板打开 CDO。

为新用户创建 Cisco Security Cloud Sign On 账户

新用户可以随时自行创建 Cisco Security Cloud Sign On 账户。他们不需要知道他们将被分配到的租户的名称。

关于登录 CDO

思科防御协调器 (CDO) 使用 Cisco Security Sign On 作为身份提供程序，并使用 Duo 进行多重身份验证 (MFA)。**要登录 CDO，必须先在 Cisco Security Cloud Sign On 中创建账户，然后再使用 Duo 配置 MFA**。

CDO 需要 MFA，它为保护您的用户身份提供额外的一重保障。双因素身份验证（一种 MFA）需要两个部分或因素来确保登录CDO的用户身份真实。第一个因素是用户名和密码，第二个是按需生成的一次性密码 (OTP)。

Important 如果您的 **CDO 租户在 2019 年 10 月 14 日之前就已存在**，请使用 迁移到 Cisco Security Cloud Sign On 身份提供程序, on page 37 登录说明，而不是本文。

登录前

安装 DUO Security。我们建议您在手机上安装 Duo Security 应用。如果您对于如何安装 Duo 有疑问，请查看 Duo 双因素身份验证指南：注册指南。

时间同步。您要使用移动设备生成一次性密码。由于 OTP 是基于时间的，所以您的设备时钟与实时同步是非常重要的。请确保您的设备时钟自动或手动设置为正确的时间。

创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证

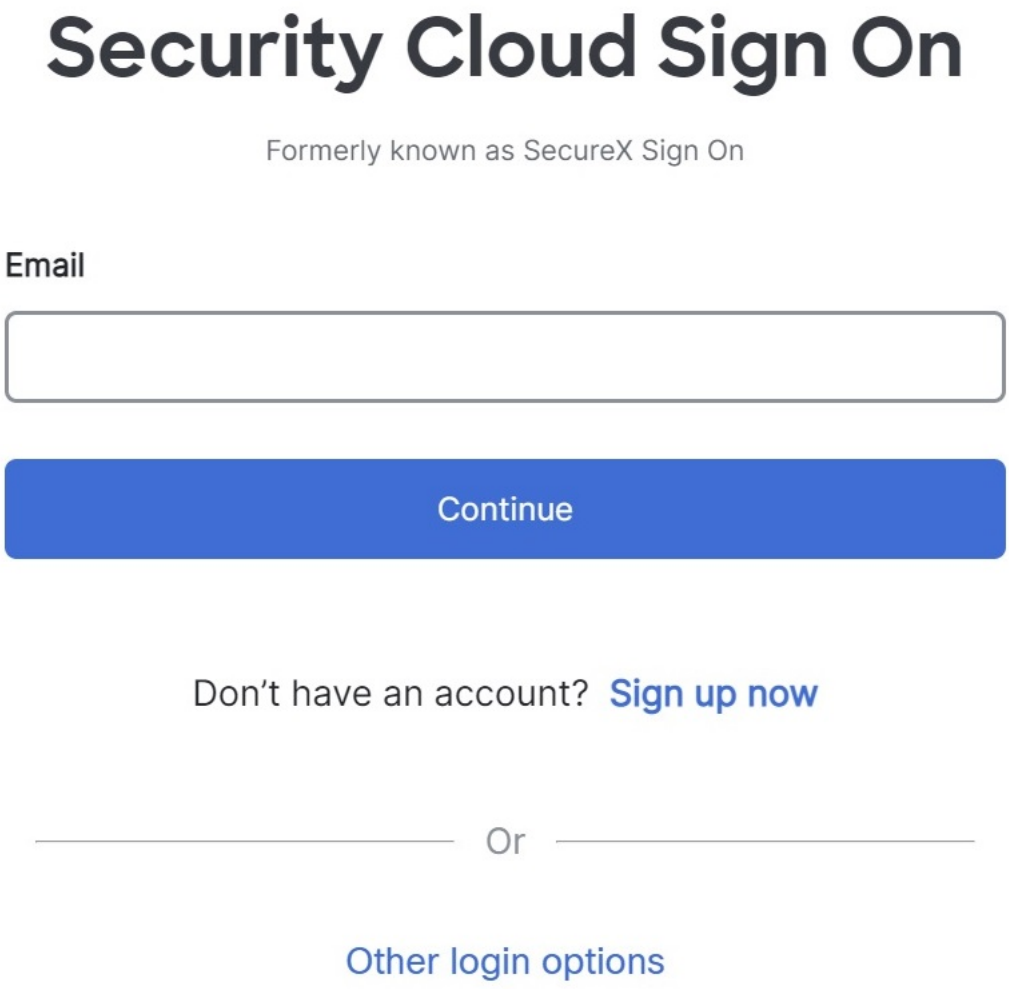
初始登录工作流程分为四步。您需要完成所有四个步骤。

Procedure

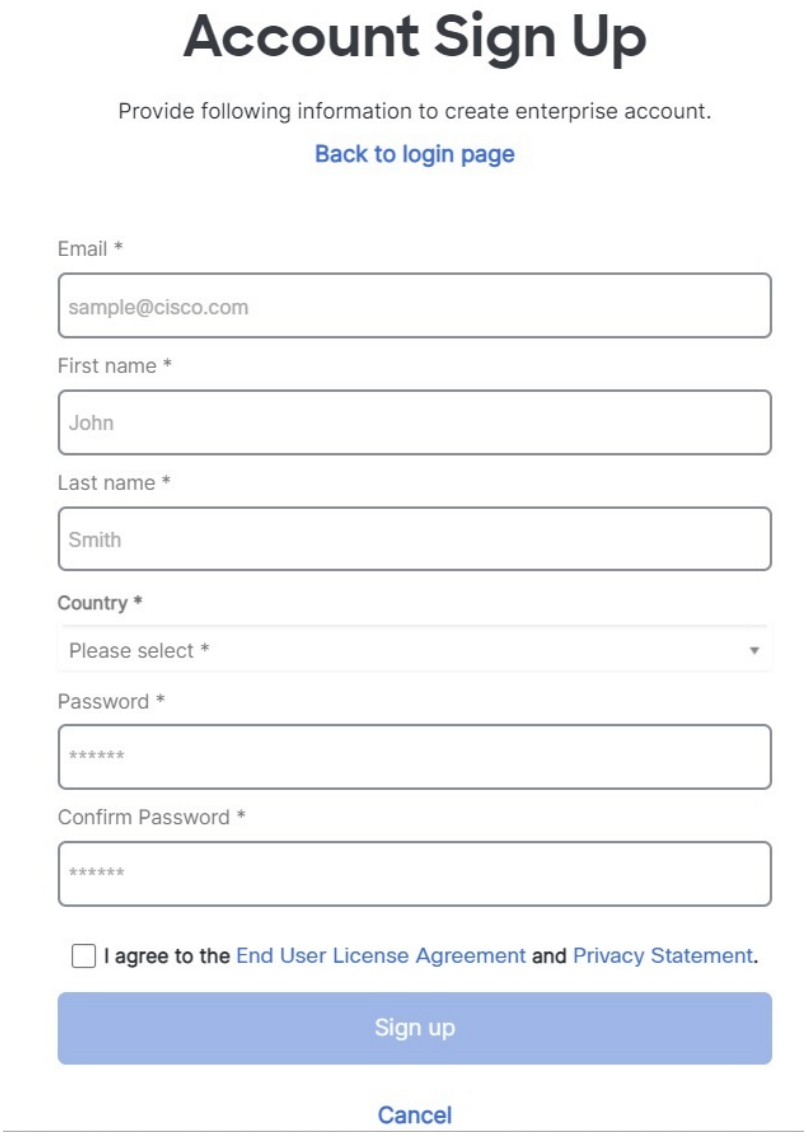
步骤 1 注册新的 **Cisco Security Cloud Sign On** 账户

a. 浏览到 https://sign-on.security.cisco.com。

b. 在“登录”屏幕的底部，点击**注册**。



c. 填写“创建帐户”(Create Account) 对话框中的字段。



我们为您提供了以下提示：

- **电子邮件 (Email)** - 输入您最终将用于登录 CDO 的邮箱地址。
- **密码 (Password)** - 输入强密码。

d. 在您点击**创建帐户 (Create Account)** 之后。

Cisco 会将验证电子邮件发送到您注册的地址。打开电子邮件，然后点击**激活帐户 (Activate Account)**。

步骤 2 使用 Duo 设置多因素身份验证

我们建议在设置多因素身份验证时使用移动设备。

a. 在**设置多因素身份验证 (Set up multi-factor authentication)** 屏幕中，点击**配置因素 (Configure factor)**。

b. 点击**开始设置 (Start setup)**，按照提示选择移动设备，然后验证该移动设备与您的账户是否配对。

有关详细信息，请参阅 Duo 双因素身份验证指南：注册指南。如果您的设备上已经有 Duo 应用，您将收到此帐户的激活代码。Duo 支持一个设备上的多个帐户。

c. 在向导结束时，点击**继续登录**。

d. 通过双因素身份验证登录 Cisco Security Cloud Sign On。

步骤 3 （可选）将 **Google 身份验证器设置为附加身份验证器**

a. 选择要与 Google Authenticator 配对的移动设备，然后点击**下一步**。

b. 按照安装向导中的提示设置 Google Authenticator。

步骤 4 **配置思科安全登录账户的账户恢复选项**

a. 选择恢复电话号码以使用 SMS 重置帐户。

b. 选择安全图像。

c. 点击**创建帐户**。现在，您会看到包含 CDO 应用图块的 Cisco Security Sign-On 控制板。您还可以看到其他应用图块。

Tip

您可以在控制板上拖动图块以按您喜欢的顺序进行排序，创建选项卡对图块分组并重命名选

使用您的 CDO 用户名创建 CDO 用户记录

只有具有“超级管理员”权限的 CDO 用户才能创建 CDO 用户记录。超级管理员应使用上述 **创建您的 CDO 用户名** 任务中指定的相同邮箱地址创建用户记录。

使用以下程序创建具有适当用户角色的用户记录：

Procedure

步骤 1 登录 CDO。

步骤 2 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 3 点击 **用户管理** 选项卡。

步骤 4 点击蓝色加号按钮  ，将新用户添加到租户。

步骤 5 提供用户的邮件地址。

Note 用户的邮箱地址必须与 Cisco Secure Log-On 账户的邮箱地址相对应。

步骤 6 从下拉菜单中选择用户的 思科防御协调器中的用户角色 。

步骤 7 点击**确定 (OK)**。

新用户从思科安全登录控制面板打开 CDO

Procedure

步骤 1 在 Cisco Secure Sign-On 控制板上点击适当的 **CDO** 磁贴。**CDO** 磁贴会将您导向 https://defenseorchestrator.com，而**CDO (EU)** 磁贴会将您导向 https://defenseorchestrator.eu。

步骤 2 请点击身份验证器徽标以选择 Duo Security 或 Google Authenticator， 如果您已设置这两个身份验证器。

- 如果您在现有租户上已有用户记录，则将登录该租户。
- 如果您在多个门户上已有用户记录，您将能够选择要连接的门户。
- 如果您在若干租户上已有用户记录，则将能够选择要连接的 CDO 租户。
- 如果您在现有租户上尚无用户记录，将能够了解有关 CDO 的详细信息或申请试用租户。

门户视图检索并显示来自多个租户的整合信息。有关详细信息，请参阅管理多个CDO租户。管理多租户门户, on page 56

租户视图显示您拥有用户记录的多个租户。

思科防御协调器中的用户角色

思科防御协调器 (CDO) 中有多种用户角色：只读、仅编辑、仅部署、管理员和超级管理员。为每个租户上的每个用户配置用户角色。如果 CDO 用户可以访问多个租户，则他们可能具有相同的用户 ID，但在不同的租户中具有不同的角色。用户可能在一个租户上具有只读角色，在另一个租户上具有超级管理员角色。当接口或文档提及只读用户、管理员用户或超级管理员用户时，我们描述的是该用户对特定租户的权限级别。

只读角色

分配了只读角色的用户会在每个页面上看到此蓝色横幅：

Read Only User. You cannot make configuration changes.

。

具有只读角色的用户可以执行以下操作：

- 查看 CDO 中的任何页面或任何设置。
- 搜索和过滤任何页面的内容。
- 比较设备配置，查看更改日志，并查看 VPN 映射。
- 查看有关任何页面上的任何设置或对象的每个警告。

- 生成、刷新和撤销自己的 API 令牌。请注意，如果只读用户撤销自己的令牌，则无法重新创建令牌。
- 通过我们的界面联系支持人员，并可以导出更改日志。

只读用户不能执行以下操作：

- 创建、更新、配置或删除任何页面上的任何内容。
- 载入设备。
- 逐步完成创建对象或策略等内容所需的任务，但无法保存。
- 创建 CDO 用户记录。
- 更改用户角色。
- 将访问规则附加或分离到策略。

仅编辑角色

具有“仅编辑”角色的用户可以执行以下操作：

- 编辑和保存设备配置，包括但不限于对象、策略、规则集、接口、VPN 等。
- 允许通过读取配置操作进行配置更改。
- 利用“变更请求管理”操作。

仅编辑用户不能执行以下操作：

- 将更改部署到一台设备或多台设备。
- 丢弃暂存的更改或通过 OOB 检测到的更改。
- 上传 AnyConnect 软件包，或配置这些设置。
- 为设备安排或手动启动映像升级。
- 计划或手动启动安全数据库升级。
- 在 Snort 2 和 Snort 3 版本之间手动切换。
- 创建模板。
- 更改现有的 OOB Change 设置。
- 编辑系统管理设置。
- 载入设备。
- 删除设备。
- 删除 VPN 会话或用户会话。

- 创建 CDO 用户记录。
- 更改用户角色。

仅部署角色

具有“仅部署”角色的用户可以执行以下操作：

- 将暂存更改部署到一台设备或多台设备。
- 恢复或恢复 ASA 设备的配置更改。
- 为设备安排或手动启动映像升级。
- 计划或手动启动安全数据库升级。
- 利用“变更请求管理”操作。

仅部署用户不能执行以下操作：

- 在 Snort 2 和 Snort 3 版本之间手动切换。
- 创建模板。
- 更改现有的 OOB Change 设置。
- 编辑系统管理设置。
- 载入设备。
- 删除设备。
- 删除 VPN 会话或用户会话。
- 创建、更新、配置或删除任何页面上的任何内容。
- 载入设备。
- 逐步完成创建对象或策略等内容所需的任务，但无法保存。
- 创建 CDO 用户记录。
- 更改用户角色。
- 将访问规则附加或分离到策略。

VPN 会话管理器角色

“VPN 会话管理器”(Sessions Manager) 角色专为监控远程接入 VPN 连接而非站点间 VPN 连接的管理员而设计。

具有 VPN 会话管理器角色的用户可以执行以下操作：

- 查看 CDO 中的任何页面或任何设置。
- 搜索和过滤任何页面的内容。
- 比较设备配置，查看更改日志，并查看 RA VPN 映射。
- 查看有关任何页面上的任何设置或对象的每个警告。
- 生成、刷新和撤销自己的 API 令牌。请注意，如果 VPN 会话管理器用户撤销其自己的令牌，则无法重新创建该令牌。
- 通过我们的界面联系支持人员并导出更改日志。
- 终止现有的 RA VPN 会话。

VPN 会话管理器用户不能执行以下操作：

- 创建、更新、配置或删除任何页面上的任何内容。
- 载入设备。
- 逐步完成创建对象或策略等内容所需的任务，但无法保存。
- 创建 CDO 用户记录。
- 更改用户角色。
- 将访问规则附加或分离到策略。

管理角色

管理员用户对 CDO 的大多数方面具有完全访问权限。管理员用户可以执行以下操作：

- 在 CDO 中创建、读取、更新和删除任何对象或策略，并配置任何设置。
- 载入设备。
- 查看 CDO 中的任何页面或任何设置。
- 搜索和过滤任何页面的内容。
- 比较设备配置，查看更改日志，并查看 VPN 映射。
- 查看有关任何页面上的任何设置或对象的每个警告。
- 生成、刷新和撤销自己的 API 令牌。如果他们的令牌被撤销，他们可以通过我们的界面联系支持人员，并可以导出更改日志。

管理员用户不能执行以下操作：

- 创建 CDO 用户记录。
- 更改用户角色。

超级管理员角色

超级管理员用户可以完全访问 CDO 的所有方面。超级管理员可以执行以下操作：

- 更改用户角色。
- 创建用户记录。

Note 虽然超级管理员可以创建CDO用户记录，但该用户记录并不是用户登录租户所需的全部内容。用户还需要具有租户使用的身份提供程序的账户。除非您的企业有自己的单点登录身份提供程序，否则身份提供程序是思科安全云登录。用户可以自行注册 Cisco Security Cloud Sign On 账户；有关详细信息，请参阅新 CDO 租户的初始登录, on page 36。

- 在 CDO 中创建、读取、更新和删除任何对象或策略，并配置任何设置。
- 载入设备。
- 查看 CDO 中的任何页面或任何设置。
- 搜索和过滤任何页面的内容。
- 比较设备配置，查看更改日志，并查看 VPN 映射。
- 查看有关任何页面上的任何设置或对象的每个警告。
- 生成、刷新和撤销自己的 API 令牌。如果他们的令牌被撤销，他们可以
- 通过我们的界面联系支持人员，并可以导出更改日志。

更改用户角色的记录

用户记录是当前记录的用户角色。通过查看与您的租户关联的用户，您可以确定每个用户的记录。通过更改用户角色，您可以更改用户记录。用户的角色通过其在“用户管理”表中的角色进行标识。有关详细信息，请参阅用户管理。

您必须是超级管理员才能更改用户记录。如果您的租户没有超级管理员，请联系CDO客户如何通过 TAC 提交支持请求。

为用户角色创建用户记录

CDO 用户需要 CDO 记录和相应的 IdP 账户，以便他们可以进行身份验证并访问您的 CDO 租户。此程序会在 Cisco Security Cloud Sign On 中创建用户的 CDO 用户记录，而不是用户的账户。如果用户在 Cisco Security Cloud Sign On 中没有账户，则可以通过导航到 https://sign-on.security.cisco.com 并点击**登录 (Sign up)** 屏幕底部的“注册”来自行注册。

Note 您需要在 CDO 上具有超级管理员角色角色才能执行此任务。

创建用户记录

使用以下程序创建具有适当用户角色的用户记录：

Procedure

步骤 1 登录 CDO。
步骤 2 在右上角的“管理”下拉列表中，点击 **设置**。
步骤 3 点击 **用户管理** 选项卡。
步骤 4 点击蓝色加号按钮  ，将新用户添加到租户。
步骤 5 提供用户的邮件地址。

Note 用户的邮箱地址必须与 Cisco Secure Log-On 账户的邮箱地址相对应。

步骤 6 从下拉菜单中选择用户的 思科防御协调器中的用户角色 。
步骤 7 点击 v。

Note 虽然超级管理员可以创建CDO用户记录，但该用户记录并不是用户登录租户所需的全部内容。用户还需要具有租户使用的身份提供程序的账户。除非您的企业有自己的单点登录身份提供程序，否则身份提供程序是思科安全登录。用户可以自行注册 Cisco Secure Sign-On 账户；有关详细信息，请参阅新 CDO 租户的初始登录, on page 36。

创建仅 API 用户

过程

步骤 1 登录 CDO。
步骤 2 在右上角的“管理”下拉列表中，点击 **设置**。
步骤 3 点击 **用户管理** 选项卡。
步骤 4 点击蓝色加号按钮  ，将新用户添加到租户。
步骤 5 选择**仅 API 用户 (API Only User)** 复选框。
步骤 6 在用户名字段中，输入用户的名称，然后点击确定。

重要事项 用户名不能是邮件地址或包含“@”字符，因为“@yourtenant”后缀将自动附加到用户名。

步骤 7 从下拉菜单中选择用户的 思科防御协调器中的用户角色 。

步骤 8 点击**确定**。

步骤 9 点击 **用户管理** 选项卡。

步骤 10 在新的仅 API 用户的令牌列中，点击生成 API 令牌以获取 API 令牌。

编辑用户角色的用户记录

您需要具有超级管理员的角色才能执行此任务。如果超级管理员更改已登录的CDO用户的角色，则在其角色更改后，该用户将自动从其会话中注销。用户重新登录后，他们将承担新角色。

Note 您需要在 CDO 上具有超级管理员角色角色才能执行此任务。

Caution 更改用户记录的角色将删除与用户记录关联的 API 令牌（如果有）。API 令牌, on page 53用户角色更改后，用户必须生成新的 API 令牌。

编辑用户角色

Note 如果 CDO 用户已登录，并且超级管理员更改其角色，则该用户必须注销并重新登录，更改才会生效。

要编辑用户记录中定义的角色，请执行以下程序：

Procedure

步骤 1 登录 CDO。

步骤 2 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 3 点击 **用户管理** 选项卡。

步骤 4 点击用户行中的编辑图标。

步骤 5 从“角色”(Role) 下拉菜单中选择用户的新思科防御协调器中的用户角色。

步骤 6 如果用户记录显示有与用户关联的 API 令牌，则需要确认要更改用户的角色并删除 API 令牌。

步骤 7 点击 v。

步骤 8 如果 CDO 删除了 API 令牌，请联系用户，以便他们可以创建新的 API 令牌。

删除用户角色的用户记录

删除 CDO 中的用户记录会破坏用户记录与 Cisco Security Cloud Sign On 账户的映射，从而防止关联用户登录 CDO。删除用户记录时，也会删除与该用户记录关联的 API 令牌（如果有）。删除 CDO 中的用户记录不会删除 Cisco Security Cloud Sign On 中的用户 IdP 账户。

Note 您需要在 CDO 上具有超级管理员角色角色才能执行此任务。

删除用户记录

要删除用户记录中定义的角色，请参阅以下程序：

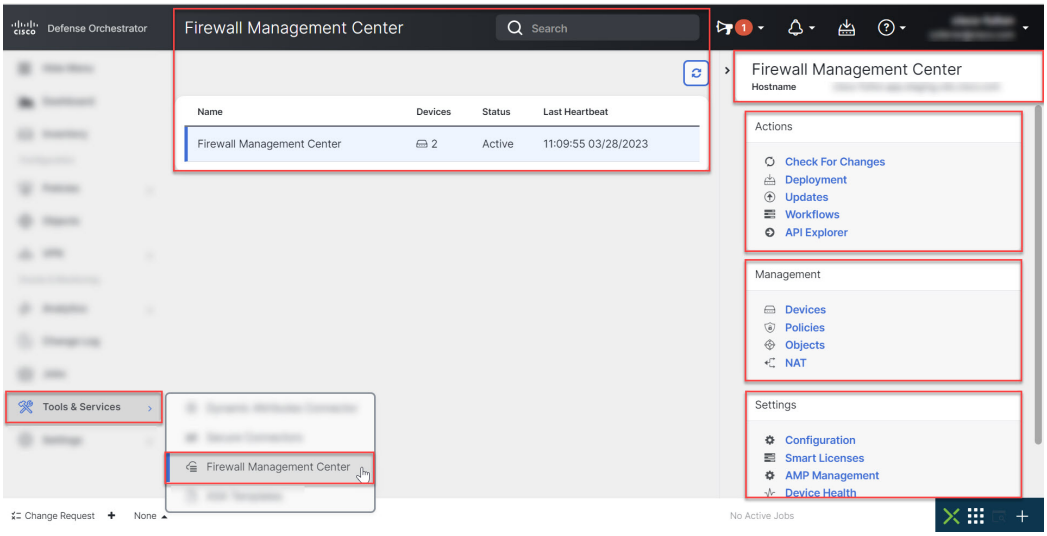
Procedure

步骤 1 登录 CDO。
步骤 2 在右上角的“管理”下拉列表中，点击 **设置**。
步骤 3 点击 **用户管理** 选项卡。
步骤 4 点击要删除的用户所在行的垃圾桶图标。
步骤 5 点击**确定 (OK)**。
步骤 6 点击确定，确认要从租户中删除帐户。

云交付的防火墙管理中心 应用页面

从 CDO 的主菜单打开 云交付的防火墙管理中心 应用页面。

导航至 **工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。



“防火墙管理中心”页面显示以下信息：

- 如果您的租户上没有部署 云交付的防火墙管理中心 ，请点击 **请求 FMC**。
- 上部署的设备数量。Secure Firewall Threat Defense云交付的防火墙管理中心
- 与页面之间的连接状态。CDO云交付的防火墙管理中心
- 的最后一次心跳。云交付的防火墙管理中心这表示上次将 本身的状态及其管理的设备数量与此页面上的表同步。云交付的防火墙管理中心
- 所选对象的主机名。云交付的防火墙管理中心

使用“操作”、“管理”或“设置”窗格中的链接，打开页面以执行与所点击的链接关联的配置任务。云交付的防火墙管理中心

打开 云交付的防火墙管理中心 页面后，点击蓝色问号按钮，然后选择 **页面级帮助** 以了解有关您所在页面的详细信息，以及您可以采取的进一步操作。

更新 云交付的防火墙管理中心 设备计数和状态

在操作窗格中，点击检查更改。表中的设备计数和状态信息将使用上次此页面和 同步时可用的信息进行更新。云交付的防火墙管理中心每 10 分钟进行一次同步。

支持在不同的选项卡上打开 CDO 和 云交付的防火墙管理中心 应用

在 云交付的防火墙管理中心中配置 威胁防御 设备或对象时，您可以在其他浏览器选项卡中打开相应的配置页面，以便在 CDO 和 云交付的防火墙管理中心 门户中同时工作，而无需注销。例如，您可以在 云交付的防火墙管理中心 上创建对象，同时监控从安全策略生成的 CDO 上的事件日志。

此功能适用于导航到 云交付的防火墙管理中心 门户的所有 CDO 链接。要在新选项卡中打开 云交付的防火墙管理中心 门户，请执行以下操作：

在 CDO 门户上，按住 **Ctrl** (Windows) 或 **Command** (Mac) 按钮，然后点击相应的链接。

注释 点击一下即可在同一选项卡中打开 云交付的防火墙管理中心 页面。

以下是在新选项卡中打开 云交付的防火墙管理中心 门户页面的一些示例：

- 选择 **工具和服务** > **防火墙管理中心**。

  在右侧窗格中，按住 **Ctrl** (Windows) 或 **Command** (Mac) 按钮，然后点击要访问的页面。

- 选择 **对象** > **其他 FTD 对象**。
- 点击 CDO 页面右上角的搜索图标，然后在显示的搜索字段中输入搜索字符串。

  在搜索结果中，按住 **Ctrl** (Windows) 或 **Command** (Mac) 按钮，然后点击箭头图标。

- 选择 **控制面板** > **快速操作**。

  按住 **Ctrl** (Windows) 或 **Command** (Mac) 按钮，然后点击 **管理 FTD 策略** 或 **管理 FTD 对象**。

注释 当您切换到新的 CDO 租户时，已在新选项卡中打开的相应 云交付的防火墙管理中心 门户将注销。

设备和服务管理

Cisco Defense Orchestrator (CDO) 提供查看、管理、过滤和评估支持的设备和服务的功能。https://docs.defenseorchestrator.com/Configuration_Guides/Devices_and_Services/Software_and_Hardware_Supported_by_CDO在“资产”页面中，您可以：

- 用于 CDO 管理的载入设备和服务。
- 查看受管设备和服务的配置状态和连接状态。
- 在单独的选项卡中查看已自行激活的设备和模板。请参阅查看资产页面信息，第 89 页。
- 评估各个设备和服务并采取措施。
- 查看设备和服务特定信息并解决问题。
- 查看由以下人员管理的威胁防御设备的设备运行状况：
  - 云交付的防火墙管理中心
  - 本地管理中心

  对于 云交付的防火墙管理中心 管理的威胁防御设备，您还可以查看集群中设备的节点状态。

- 按名称、类型、IP 地址、型号名称、序列号或标签搜索设备或模板。搜索不区分大小写。提供多个搜索词会调出至少与其中一个搜索词匹配的设备和服务。请参阅搜索，第 93 页。

- 设备或模板过滤器可按设备类型、硬件和软件版本、Snort 版本、配置状态、连接状态、冲突检测以及保护设备连接器和标签进行过滤。请参阅过滤器。过滤器， 第 90 页

在 CDO 中更改设备的 IP 地址

在使用 IP 地址将设备载入 Cisco Defense Orchestrator (CDO) 时，CDO 会将该 IP 地址存储在其数据库中，并使用该 IP 地址与设备通信。如果设备的 IP 地址发生更改，您可以更新 CDO 中存储的 IP 地址以匹配新地址。在 CDO 上更改设备的 IP 地址不会更改设备的配置。

要更改 CDO 用于与设备通信的 IP 地址，请执行以下程序：

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击设备类型选项卡。

您可以使用 过滤器 和 搜索 功能查找所需的设备。

步骤 4 选择要更改其 IP 地址的设备。

步骤 5 在**设备详细信息 (Device Details)** 窗格上方，点击设备 IP 地址旁边的编辑按钮。

步骤 6 在字段中输入新的 IP 地址，然后点击蓝色的复选按钮。

设备本身不会发生更改，因此设备的配置状态将继续显示已同步。

相关信息：

- 在租户之间移动设备, on page 89
- 将设备批量重新连接到 CDO, on page 88

在 CDO 中更改设备的名称

所有设备、型号、模板和服务在自行激活或在 CDO 中创建时都会获得一个名称。您可以更改该名称，而无需更改设备本身的配置。

Procedure

步骤 1 在导航栏中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击**设备 (Device)** 选项卡以找到设备。

步骤 3 选择要更改其名称的设备。

步骤 4 在**设备详细信息 (Device Details)** 窗格上方，点击设备名称旁边的编辑按钮。

步骤 5 在字段中输入新的名称，然后点击蓝色的复选按钮。

设备本身不会发生更改，因此设备的配置状态将继续显示已同步。

导出设备和服务列表

本文介绍如何将设备和服务列表导出为逗号分隔值 (.csv) 文件。转换为该格式后，您可以在电子表格应用（例如 Microsoft Excel）中打开该文件，以对列表中的项目进行排序和过滤。

导出按钮在设备和模板选项卡中可用。您还可以从所选设备类型选项卡下的设备导出详细信息。

在导出设备和服务列表之前，请查看过滤器窗格并确定清单表是否显示要导出的信息。清除所有过滤器以查看所有受管设备和服务，或过滤信息以显示所有设备和服务的子集。导出功能会导出您在清单表中看到的内容。

Procedure

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击相应的设备类型选项卡以从该选项卡下的设备导出详细信息，或点击**全部 (All)** 以从所有设备导出详细信息。

您可以使用 过滤器 和 搜索 功能查找所需的设备。

步骤 4 点击**将列表导出到 CSV (Export list to CSV)**：

步骤 5 如果出现提示，请保存 .csv 文件。

步骤 6 在电子表格应用中打开 .csv 文件，对结果进行排序和过滤。

导出设备配置

一次只能导出一个设备配置。使用以下程序将设备的配置导出到 JSON 文件：

过程

步骤 1 在导航栏中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

您可以使用 过滤器 和 搜索 功能查找所需的设备。

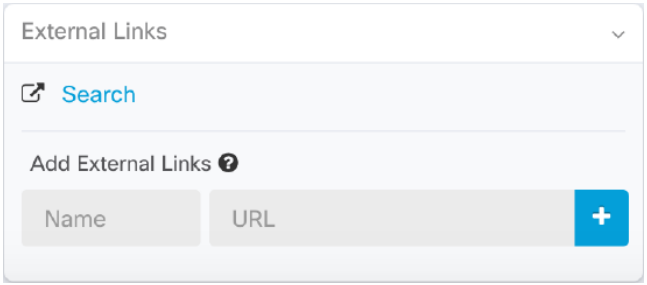
步骤 4 选择所需的设备以便将其突出显示。

步骤 5 在操作窗格中，选择导出配置。

步骤 6 选择确认以将配置另存为 JSON 文件。

设备的外部链接

您可以创建指向外部资源的超链接，并将其与您使用CDO管理的设备相关联。您可以使用此功能创建指向其中一个设备的本地管理器的便捷链接（ 适用于 FTD 的 Firepower 设备管理器 (FDM)）。您还可以使用它来链接到搜索引擎、文档资源、公司 Wiki 或您选择的任何其他 URL。您可以根据需要将任意数量的外部链路与设备关联。您还可以同时将同一链路与多个设备关联。



您创建的链路可以到达任何地方，但您公司的安全要求不会改变。例如，如果您通常需要通过本地部署或通过 VPN 连接来访问特定 URL，则这些要求仍然存在。如果您的公司阻止特定 URL，这些 URL 将继续被阻止。不受限制的 URL 将继续不受限制。

位置变量

我们已创建 {location} 变量，您可以将其合并到您的 URL 中。此变量将填充设备的 IP 地址。例如，

```
https://{location}
```

或 FTD 托管设备的 FDM。

相关信息：

- 编写设备说明, on page 89
- 导出设备和服务列表, on page 84

从您的设备创建外部链路

Procedure

步骤 1 在导航栏中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择设备或型号。

您可以使用 过滤器 和 搜索 功能查找所需的设备。

步骤 5 在右侧的详细信息窗格中，转到**外部链接**部分。

步骤 6 输入链接的名称。

步骤 7 在 URL 字段中输入链接的 URL。您需要指定完整的 URL，例如，对于思科，请输入 http://www.cisco.com。

步骤 8 点击 + 将链接与设备关联。

创建到 ASDM FDM 的外部链路

以下是直接从 CDO 打开 ASA 的自适应安全设备管理器 (ASDM) 和 FTD 的 Firepower 设备管理器 (FDM) 的便捷方法。

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

您可以使用 过滤器 和 搜索 功能查找所需的设备。

步骤 4 选择设备或型号。

步骤 5 在右侧的详细信息窗格中，转到“外部链接”部分。

步骤 6 输入链路的名称，例如 ASDM FDM。

步骤 7 在 URL 字段中输入 https://{location}。{location} 变量将填充设备的 IP 地址。

步骤 8 点击 + 框。

为多个设备创建外部链路

Procedure

步骤 1 在导航栏中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

您可以使用过滤器和搜索功能来查找所需的设备。

步骤 4 请选择多个设备或型号。

步骤 5 在右侧的详细信息窗格中，转到“外部链接”部分。

步骤 6 输入链接的名称。

步骤 7 使用以下方法之一输入要访问的 URL：

- 输入

  ```
  https://{location}
  ```

  在 URL 字段中。{location} 变量将填充设备的 IP 地址。这会为您的设备创建指向 ASDM 的自动链接。

- 在 URL 字段中输入链接的 URL。您需要指定完整的 URL，例如，对于思科，请输入 http://www.cisco.com。http://www.cisco.com/

步骤 8 点击 + 将链接与设备关联。

编辑或删除外部链接

Procedure

步骤 1 在导航栏中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

您可以使用 过滤器 和 搜索 功能查找所需的设备。

步骤 4 选择设备或型号。

步骤 5 在右侧的详细信息窗格中，转到“外部链接”部分。

步骤 6 将鼠标悬停在链接名称上可显示编辑和删除图标。

步骤 7 点击相应的图标可编辑或删除外部链接，并确认您的操作。

编辑或删除多台设备的外部链接

Procedure

步骤 1 在导航栏中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

您可以使用过滤器和搜索功能来查找所需的设备。

步骤 4 请选择多个设备或型号。

步骤 5 在右侧的详细信息窗格中，转到**外部链接**部分。

步骤 6 将鼠标悬停在链接名称上可显示编辑和删除图标。

步骤 7 点击相应的图标可编辑或删除外部链接，并确认您的操作。

将设备批量重新连接到 CDO

CDO 允许管理员同时尝试将多个受管设备重新连接到 CDO。当设备 CDO 管理的 标记为“无法访问”时，CDO 无法再检测到带外配置更改或管理设备。断开连接可能有许多不同的原因。尝试重新连接设备是恢复 CDO 对设备的管理的简单第一步。

Note 如果您要重新连接具有新证书的设备，CDO 会自动审核并接受设备上的新证书，并继续与其重新连接。但是，如果您仅与一台设备重新连接，CDO 会提示您手动查看并接受证书，以继续与其重新连接。

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击设备类型选项卡。

使用过滤器查找连接状态为“无法访问”的设备。

步骤 4 从过滤结果中，选择要尝试重新连接的设备。

步骤 5 点击**重新连接 (Reconnect)** 。请注意，CDO 仅提供可应用于所有选定设备的操作的命令按钮。

步骤 6 查看**通知 (notifications)** 选项卡，了解批量设备重新连接操作的进度。如果您想了解有关批量设备重新连接作业中的操作是如何成功或失败的更多信息，请点击蓝色查看链接，您将被定向到作业页面, on page 584。

Tip 如果由于设备的证书或凭证已更改而导致重新连接失败，则必须单独重新连接到这些设备，以添加新凭证并接受新证书。

在租户之间移动设备

在将设备载入 CDO 租户后，无法将设备从一个 CDO 租户迁移到另一个租户。如果要将设备移至新租户，您需要从旧租户中删除设备并将其重新载入新租户。

编写设备说明

使用此程序为设备创建单个纯文本注释文件。

Procedure

步骤 1 在导航栏中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要为其创建备注的设备或型号。

步骤 5 在左侧的**管理 (Management)** 窗格中，点击**备注 (Notes)**。 Notes 。

步骤 6 点击右侧的编辑器按钮，然后选择默认文本编辑器、Vim 或 Emacs 文本编辑器。

步骤 7 编辑“备注”(Notes) 页面。

步骤 8 点击**保存 (Save)**。
注释会被保存在选项卡中。

查看资产页面信息

资产页面显示所有已自行激活的物理和虚拟设备以及从已激活设备创建的模板。该页面根据设备和模板的类型对其进行分类，并在专用于每种设备类型的相应选项卡中显示它们。您可以使用搜索功能或应用过滤器在所选设备类型选项卡中查找设备。

您可以在此页面上查看以下详细信息：

- 设备选项卡显示载入 CDO 的所有实时设备。
- 模板显示从实时设备或导入到 CDO 的配置文件创建的所有模板设备。

标签和过滤

标签用于对设备或对象进行分组。您可以在载入期间或在载入之后随时将标签应用于一台或多台设备。您可以在创建对象后对其应用标签。将标签应用于设备或对象后，即可按该标签过滤设备表或对象表的内容。

注释 应用于设备的标签不会扩展到其关联对象，应用于共享对象的标签不会扩展到其关联对象。

可以使用以下语法“group name:label”创建标签组。例如，Region: East 或 Region:West。如果您要创建这两个标签，则组标签将为区域，您可以在该组中选择 East 或 West。

将标签应用于设备和对象

要将标签应用于设备，请执行以下步骤：

过程

步骤 1 要向设备添加标签，请点击左侧导航窗格中的设备和服务。要向对象添加标签，请点击左侧导航窗格中的对象。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 在生成的表中选择一个或多个设备或型号。

步骤 5 在右侧的添加组和标签字段中，指定设备的标签。

步骤 6 点击蓝色 + 图标。

过滤器

您可以在**清单 (Inventory)** 和**对象 (Objects)** 页面上使用许多不同的过滤器来查找要查找的设备和对象。

要过滤，请点击设备和服务、策略和对象选项卡的左侧窗格中的 ：

清单过滤器允许您按设备类型、硬件和软件版本、Snort 版本、配置状态、连接状态、冲突检测以及保护设备连接器和标签进行过滤。您可以应用过滤器在所选设备类型选项卡中查找设备。您可以使用过滤器在所选设备类型选项卡中查找设备。

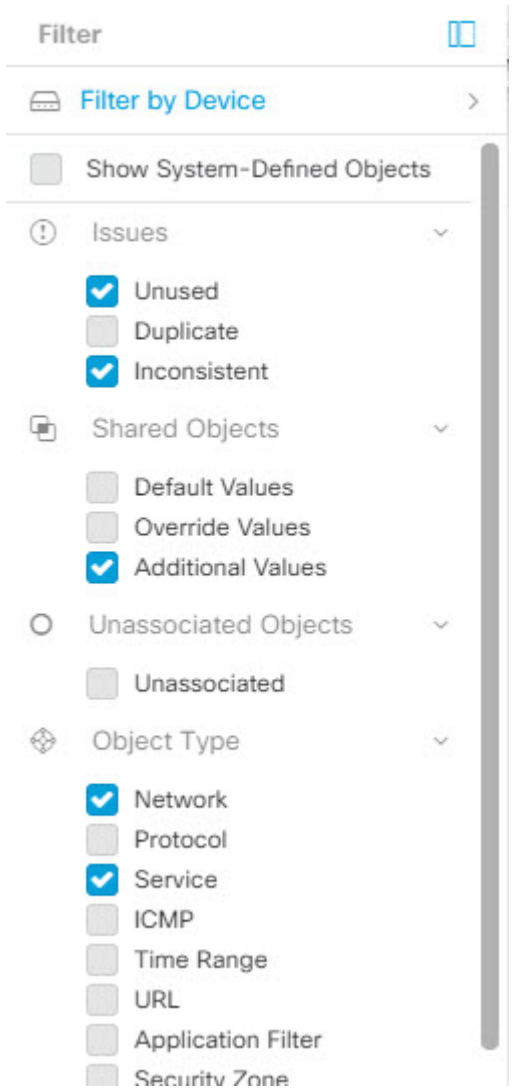
注释 打开 **FTD** 选项卡时，过滤器窗格将提供过滤器，以根据从 CDO 访问设备的管理应用来显示 FDM 管理 设备。

- FDM：使用 FTD API 或 FDM 管理的设备。
- FMC-FTD：通过使用 Firepower 管理中心管理的设备。
- FTD：使用 FTD 管理来管理的设备。

对象过滤器允许您按设备、问题类型、共享对象、未关联的对象和对象类型进行过滤。您可以在结果中包含或不包含系统对象。您还可以使用搜索字段在过滤器结果中搜索包含特定名称、IP 地址或端口号的对象。

过滤设备和对象时，您可以组合搜索词来创建多个潜在的搜索策略来查找相关结果。

在以下示例中，过滤器应用于“问题（已使用或不一致）AND 具有其他值的共享对象 AND 类型为网络 OR 服务的对象”。



查找所有使用相同 SDC 连接到 CDO 的设备

请按照以下程序识别所有使用相同 SDC 连接到 CDO 的设备：

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击设备类型选项卡。

步骤 4 如果已指定任何过滤条件，请点击“清单”(Inventory) 表顶部的**清除**按钮，以显示您使用 CDO 管理的所有设备和服务。

步骤 5 点击过滤器按钮 以展开过滤器菜单。

步骤 6 在过滤器的“安全设备连接器”(Secure Device Connectors) 部分中，选中您感兴趣的 SDC 的名称。“清单”(Inventory) 表仅显示通过您在过滤器中选中的 SDC 连接到 CDO 的设备。

步骤 7 （可选）检查过滤器菜单中的其他过滤器，以便进一步细化搜索。

步骤 8 （可选）完成后，点击清单表顶部的**清除**按钮，以便显示您使用 CDO 管理的所有设备和服务。

搜索

CDO 提供强大的搜索功能，可以轻松查找设备、对象和访问组。在**设备和服务 (Devices & Service)** 空间中，您只需在搜索栏中开始键入，就会显示符合搜索条件的设备。您可以键入设备的任何部分名称、IP 地址或物理设备的序列号来查找设备。

同样，您可以使用**对象 (Objects)** 空间中的搜索栏通过键入对象名称的任何部分或部分 IP 地址、端口、命名地址、协议来查找对象。

Procedure

步骤 1 导航到界面顶部附近的搜索栏。

步骤 2 在搜索栏中键入搜索条件，系统将显示相应的结果。

Global Search

通过全局搜索功能，您可以快速查找并导航至 管理的设备。CDO

所有搜索结果都基于您选择的索引选项。索引选项如下：

- 完整索引 - 要求调用完整索引过程。此过程会扫描系统中的所有设备和对象，并仅在调用索引后将其显示在搜索索引中。要调用完全索引，您必须具有管理权限。

  有关详细信息，请参阅启动完全索引，第 94 页。

- 增量索引 - 一种基于事件的索引过程，每次添加、修改或删除设备或对象时，搜索索引都会自动更新。

您在搜索字段中输入的信息不区分大小写。您可以使用以下实体执行全局搜索：

- 设备名称 - 支持部分设备名称、URL、IP 地址或范围。
- 对象类型 - 支持对象名称、对象说明和配置的值。
- 策略类型 - 支持策略名称、策略说明、规则名称和规则注释。

  在 CDO 中管理的云交付防火墙管理中心和本地 FMC 支持以下策略类型：

- 访问控制策略
- 预过滤器策略
- 威胁防御 NAT 策略

键入搜索表达式时，界面开始显示搜索结果，您无需按 Enter 键即可执行搜索。

搜索结果将显示与您的搜索字符串匹配的所有设备和对象。如果搜索字符串与多个设备或对象匹配，则结果将显示在类别（设备、对象和 connected_fmc）下。

默认情况下，搜索结果中的第一个项目会突出显示，并且该项目的相关信息显示在右侧窗格中。您可以滚动浏览搜索结果，然后点击任何项目以查看相应的信息。您可以点击项目旁边的箭头图标以导航到相应的页面。

注释

- 全局搜索不显示重复的搜索结果。对于对象，共享对象的 UID 用于导航到对象视图。
- 如果从 中删除设备，则会从全局搜索索引中删除所有关联对象。CDO
- 如果在启动完全索引之前从策略中删除对象并保留设备，则该对象将保留在全局搜索索引中，因为它与设备关联。

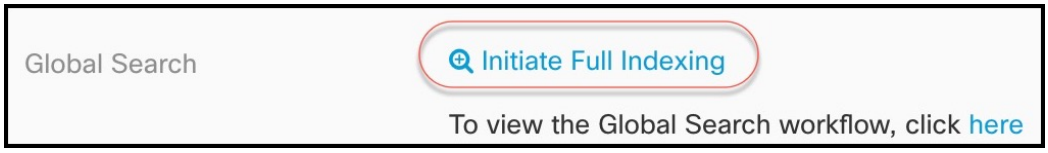
启动完全索引

过程

步骤 1 使用具有管理员或超级管理员权限的帐户登录 CDO。

步骤 2 从菜单栏中，导航至 **设置 (Settings)** > **常规设置 (General Settings)**。

步骤 3 在全局搜索中，点击启动完整索引以触发索引。



注释 启动完整索引会清除 CDO 租户的现有索引。

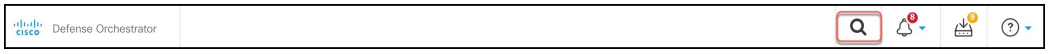
步骤 4 点击此处查看全局搜索工作流程。

执行全局搜索

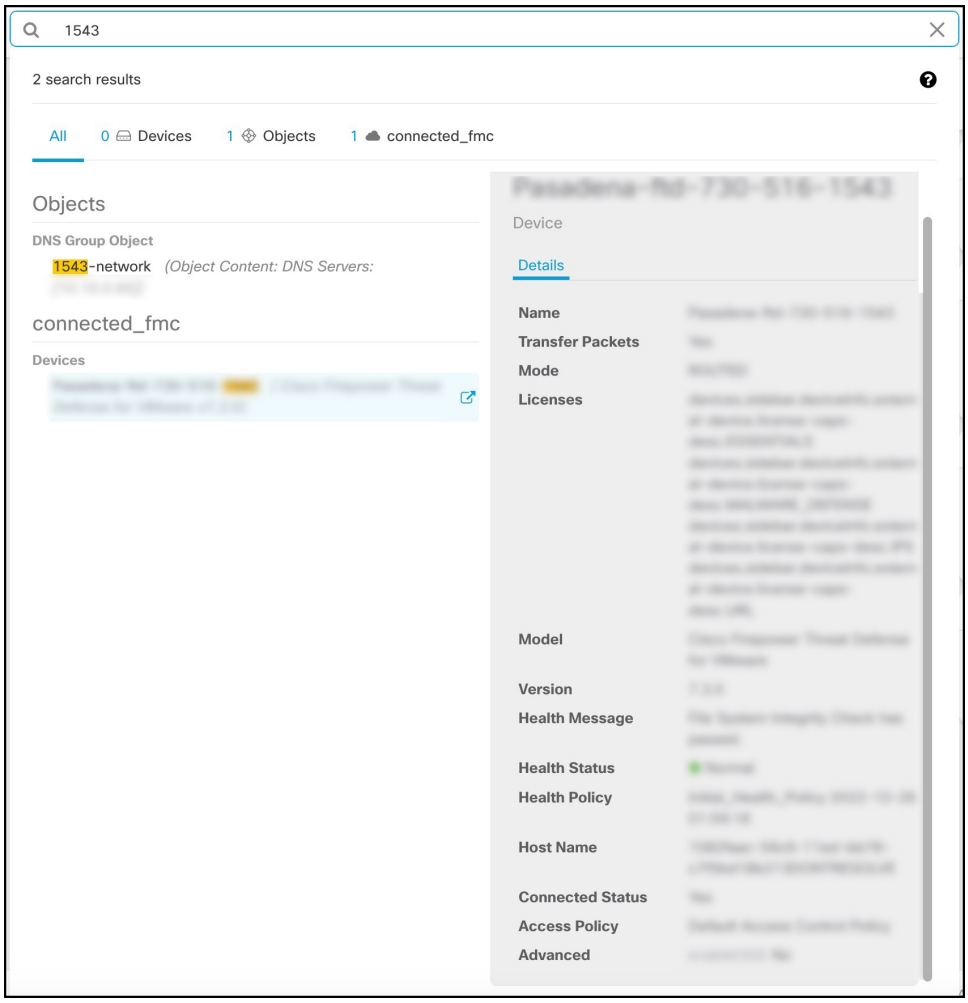
过程

步骤 1 登录至 CDO。

步骤 2 点击CDO页面右上角的搜索图标，然后在显示的搜索字段中输入搜索字符串。



当您开始输入搜索字符串时，搜索结果会显示可能的项目列表。搜索结果显示在四个类别下：All、Devices、Objects 和 connected_fmc。右侧窗格显示所选搜索结果的信息。



步骤 3 从搜索结果中选择设备或对象，然后点击箭头图标从搜索结果导航到相应的设备和对象页面。从搜索结果中选择一个项目，然后点击箭头图标从搜索结果导航到相应的页面。

注释 在云交付的防火墙管理中心中选择设备的搜索结果，可以导航到CDO中的云交付的防火墙管理中心用户界面。

有关 云交付的防火墙管理中心 的信息，请参阅使用 Cisco 防御协调器中的云交付防火墙管理中心管理防火墙威胁防御。

步骤 4 点击 **X** 关闭搜索栏。

CDO 命令行接口

CDO 为用户提供命令行界面 (CLI)，用于管理 、FDM 管理 威胁防御 设备。用户可以将命令发送到单个设备或同时发送到多个设备。

相关信息：

- 有关 FTD CLI 文档，请参阅思科 Firepower 威胁防御命令参考。请注意，FDM 管理 设备的 CLI 功能有限。这些设备只有以下命令：`show`、`ping`、`traceroute`、`packet-tracer`、`failover` 和 `shutdown`。

使用命令行接口

Procedure

步骤 1 打开**资产 (Inventory)** 页面。

步骤 2 点击资产表上方的设备按钮。

步骤 3 使用设备选项卡和过滤器按钮查找要使用命令行界面 (CLI) 管理的设备。

步骤 4 选择设备。

步骤 5 在**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。

步骤 6 点击 **命令行接口 (Command Line Interface)**。

步骤 7 在命令窗格中输入一个或多个命令，然后点击发送。 设备对命令的响应显示在下面的“响应窗格”中。

Note 如果可以运行的命令有限制，则会在命令窗格上方列出这些限制。

Related Topics

在命令行接口中输入命令 ， 第 97 页

在命令行接口中输入命令

可以在一行中输入单个命令，也可以在多行中依次输入多个命令，CDO将按顺序执行这些命令。以下示例发送创建三个网络对象和包含这些网络对象的网络对象组的一批命令。ASA

输入设备命令：CLI 控制台使用基本 CLI。**FDM 管理**威胁防御不能使用 CLI 控制台进入诊断 CLI、专家模式、FXOS CLI（在使用 FXOS 的型号上）。如果需要进入其他 CLI 模式，请使用 SSH。

使用命令历史记录

发送 CLI 命令后，CDO 会在“命令行界面”(Command Line Interface) 页面的历史记录窗格中记录该命令。您可以重新运行历史记录窗格中保存的命令，或将这些命令用作模板：

Procedure

步骤 1 在资产页面上，选择要配置的设备。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击设备类型选项卡。

步骤 4 点击 **>_命令行接口 (>_Command Line Interface)**。

步骤 5 点击时钟图标可展开历史记录窗格（如果尚未展开）。

步骤 6 在历史记录窗格中选择要修改或重新发送的命令。

步骤 7 按原样重新使用命令，或在命令窗格中对其进行编辑，然后点击发送。CDO 在响应窗格中显示命令的结果。

Note CDO 显示 Done!两种情况下响应窗格中的消息：

- 成功执行命令后。
- 当命令没有要返回的结果时。例如，您可以发出带有正则表达式的show命令，用于搜索配置条目。如果没有符合正则表达式条件的配置条目，CDO 将返回 Done!。

批量命令行接口

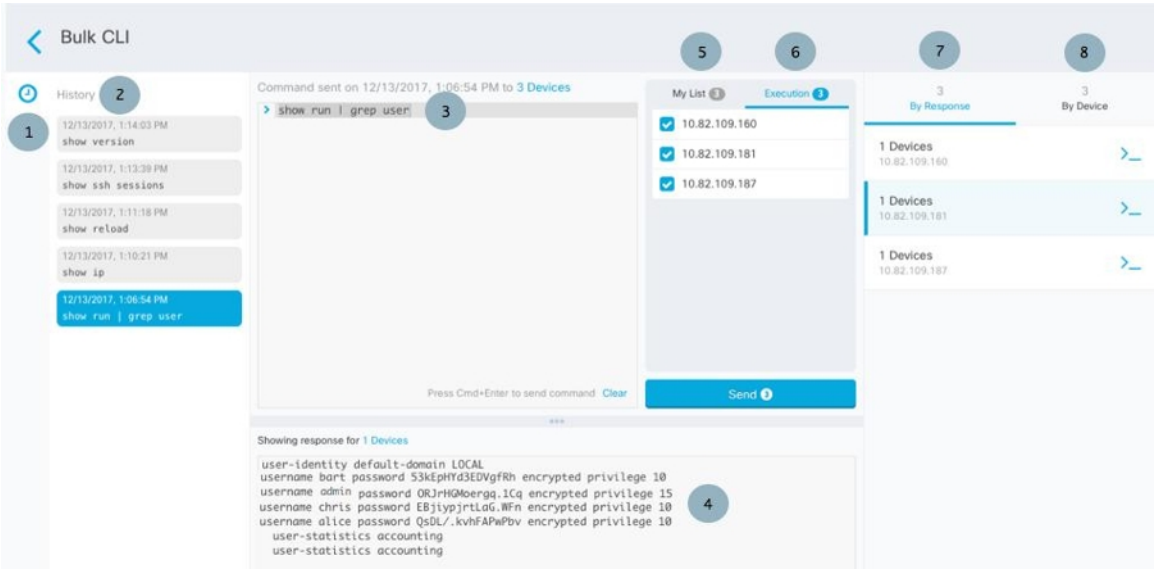
CDO 为用户提供使用命令行接口 (CLI) 管理 Secure Firewall ASA、FDM 管理 威胁防御、SSH、Cisco IOS 和 Cisco Secure Firewall Cloud Native设备。用户可以将命令发送到单个设备或同时发送到多个同类设备。本节介绍一次向多台设备发送 CLI 命令。

相关信息：

- 对于设备文档，CDO 仅支持基本 FTD CLI。FDM 管理这些设备只有以下命令：`show`、`ping`、`traceroute`、`packet-tracer`、`failover` 和 `shutdown`。

  有关 威胁防御 CLI 文档，请参阅思科 Firepower 威胁防御命令参考。

批量 **CLI** 接口



Note CDO 显示 Done!两种情况下的消息：

- 成功执行命令且无错误后。
- 当命令没有要返回的结果时。例如，您可以发出带有正则表达式的show命令，用于搜索某个配置条目。如果没有符合正则表达式条件的配置条目，CDO 将返回 Done!。

编号	说明
1	点击时钟可展开或折叠命令历史记录窗格。

编号	说明
2	命令历史记录。发送命令后，CDO 会在此历史记录窗格中记录该命令，以便您可以返回到该窗格，选择并再次运行该命令。
3	命令窗格。在此窗格的提示符后输入命令。
4	响应窗格。CDO 显示设备对命令的响应以及 CDO 消息。如果多个设备的响应相同，则响应窗格会显示消息“显示 X 台设备的响应”(Showing Responses for X devices)。点击 X 设备，CDO 将显示对命令返回相同响应的所有设备。 **Note** CDO 显示 Done!两种情况下的消息： • 成功执行命令且无错误后。 • 当命令没有要返回的结果时。例如，您可以发出带有正则表达式的 show 命令，用于搜索某个配置条目。如果没有符合正则表达式条件的配置条目，CDO 将返回 Done!。
5	我的列表选项卡显示您从资产表中选择的设备，并允许您包含或排除要向其发送命令的设备。
6	上图中突出显示的“执行”选项卡显示在历史记录窗格中选择的命令中的设备。在本例中，show run |在历史记录窗格中选择了 grep 用户命令，执行选项卡显示它已发送到 10.82.109.160、10.82.109.181 和 10.82.10.9.187。
7	点击“By Response”（按响应）选项卡将显示命令生成的响应列表。相同的响应组合在一行中。当您在“按响应”选项卡中选择一行时，CDO 会在响应窗格中显示对该命令的响应。
8	点击“按设备”选项卡会显示每个设备的单独响应。点击列表中的其中一个设备，即可查看特定设备对命令的响应。

批量发送命令

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 选择相应的设备选项卡，然后使用过滤器按钮查找要使用命令行界面配置的设备。

步骤 4 选择设备。

步骤 5 在**设备操作 (Device Actions)** 窗格中，点击**>_命令行接口 (>_Command Line Interface)**。

步骤 6 您可以在“我的列表”字段中选中或取消选中要向其发送命令的设备。

步骤 7 在命令窗格中输入命令，然后点击发送。命令输出显示在响应窗格中，命令记录在更改日志中，命令 CDO 在批量 CLI 窗口的历史记录窗格中记录您的命令。

使用批量命令历史记录

发送批量 CLI 命令后，CDO 会在“批量 CLI”页面历史记录页面中记录该命令。批量 CLI 接口, on page 98您可以重新运行历史记录窗格中保存的命令，也可以将这些命令用作模板。历史记录窗格中的命令与运行这些命令的原始设备相关联。

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击相应的设备类型选项卡，然后点击过滤器图标以查找要配置的设备。

步骤 4 选择设备。

步骤 5 点击 **命令行接口 (Command Line Interface)**。

步骤 6 在“历史记录”窗格中选择要修改或重新发送的命令。请注意，您选择的命令与特定设备相关联，而不一定是您在第一步中选择的设备。

步骤 7 查看我的列表选项卡，确保您要发送的命令将发送到您期望的设备。

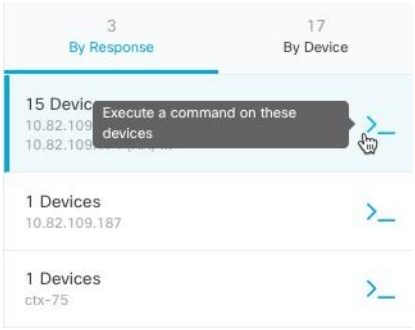
步骤 8 在命令窗格中编辑命令，然后点击发送。CDO 在响应窗格中显示命令的结果。

使用批量命令过滤器

运行批量 CLI 命令后，您可以使用“按响应”过滤器和“按设备”过滤器继续配置设备。

按响应过滤器

运行批量命令后，CDO 会使用发送该命令的设备返回的响应列表填充“按响应”选项卡。具有相同响应的设备会合并到一行中。点击“按响应”(By Response) 选项卡中的行会在响应窗格中显示设备的响应。如果响应窗格显示多个设备的响应，则会显示消息“显示 X 台设备的响应”。点击 X 设备，CDO 将显示对命令返回相同响应的所有设备。



要将命令发送到与命令响应关联的设备列表，请执行以下程序：

Procedure

步骤 1 点击 By Response 选项卡中一行中的命令符号。

步骤 2 查看命令窗格中的命令，然后点击发送以重新发送命令，或点击清除以清除命令窗格并输入要发送到设备的新命令，然后点击发送。

步骤 3 查看从命令收到的响应。

步骤 4 如果您确信所选设备上的运行配置文件反映了您的更改，请在命令窗格中键入 write memory，然后点击 Send。这样会将运行配置保存至启动配置。

按设备过滤器

运行批量命令后，CDO 会使用已发送命令的设备列表填充“执行”选项卡和“按设备”选项卡。点击“按设备”(By Device) 选项卡中的行会显示每个设备的响应。

要在同一设备列表上运行命令，请执行以下程序：

Procedure

步骤 1 点击**按设备 (By Device)** 选项卡。

步骤 2 点击 >_在这些设备上执行命令。

步骤 3 点击清除以清除命令窗格并输入新命令。

步骤 4 在我的列表窗格中，通过选中或取消选中列表中的单个设备来指定要向其发送命令的设备列表。

步骤 5 点击**发送 (Send)**。命令的响应会显示在响应窗格中。如果响应窗格显示多个设备的响应，则会显示消息“显示 X 台设备的响应”。点击 X 设备，CDO 将显示对命令返回相同响应的所有设备。

步骤 6 如果您确信所选设备上的运行配置文件反映了您的更改，请在命令窗格中键入 write memory，然后点击 Send。

用于管理设备的 CLI 宏

CLI 宏是可以使用的完整形式的 CLI 命令，或者是可以在运行之前修改的 CLI 命令的模板。所有宏都可以在一个或多个 FTD 设备上同时运行。

使用类似模板的 CLI 宏可同时在多台设备上运行相同的命令。CLI 宏可促进设备配置和管理的一致性。使用完全格式的 CLI 宏获取有关设备的信息。您可以立即在 FTD 设备上使用不同的 CLI 宏。

您可以创建 CLI 宏来监控您经常执行的任务。有关详细信息，请参阅从新命令创建 CLI 宏。

CLI 宏是系统定义的或用户定义的。系统定义的宏由 CDO 提供，无法编辑或删除。用户定义的宏由您创建，可以编辑或删除。

Note 只有在设备载入 CDO 后，才能为设备创建宏。

以 ASA 为例，如果要查找其中一个 ASA 上的特定用户，可以运行以下命令：

```
show running-config | grep username
```

运行命令时，您要将 *username* 替换为要搜索的用户的用户名。要使用此命令来创建宏，请使用相同的命令并在用户名周围加上大括号。

```
> show running-config | grep {{username}}
```

您可以随意命名参数。您还可以使用此参数名称创建相同的宏：

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

参数名称可以是描述性的，并且必须使用字母数字字符和下划线。命令语法，在本例中为

```
show running-config | grep
```

命令的一部分，必须对要向其发送命令的设备使用正确的 CLI 语法。

从新命令创建 CLI 宏

Procedure

步骤 1 在创建 CLI 宏之前，请在 CDO 的命令行界面中测试命令，以便确保命令语法正确并返回可靠的结果。

Note
- 对于 FTD 设备，CDO 仅支持可在 FDM 的 CLI 控制台中运行的命令：`show`、`ping`、`traceroute`、`packet-tracer`、`failover`、`reboot` 和 `shutdown`。有关这些命令的语法的完整说明，请参阅《思科 Firepower 威胁防御命令参考》。

步骤 2 在导航栏中，点击**清单 (Inventory)**。

步骤 3 点击 **设备 (Devices)**选项卡以找到设备。

步骤 4 点击相应的设备类型选项卡，然后选择在线和同步的设备。

步骤 5 点击 **>_Command Line Interface**。

步骤 6 点击 CLI 宏收藏夹星标 ★，以查看已经存在的宏。

步骤 7 点击加号按钮  。

步骤 8 请为宏指定唯一的名称。如果需要，请为 CLI 宏提供说明和注释。

步骤 9 在**命令 (Command)** 字段中输入完整命令。

步骤 10 运行命令时，将要修改的命令部分替换为用大括号括起来的参数名称。

步骤 11 点击**创建**。您创建的宏可用于该类型的所有设备，而不只是您最初指定的设备。

要运行命令，请参阅运行 CLI 宏。

从 CLI 历史记录或现有 CLI 宏创建 CLI 宏

在此程序中，您将从已运行的命令、另一个用户定义的宏或从系统定义的宏创建用户定义的宏。

过程

步骤 1 在导航栏中，点击 **设备和服务**。

注释 如果要从 CLI 历史记录创建用户定义的宏，请选择运行命令的设备。CLI 宏在同一账户上的设备之间共享，但不是 CLI 历史记录。

步骤 2 点击**设备**选项卡。

步骤 3 点击相应的设备类型选项卡，然后选择在线和同步的设备。

步骤 4 点击 **>_命令行接口**。

步骤 5 查找要生成 CLI 宏的命令，然后选择该命令。使用以下方法之一：

- 点击时钟可查看您在该设备上运行的命令。选择要转换为宏的命令，命令将显示在命令窗格中。
- 点击 CLI 宏收藏夹星标 ★，以查看已经存在的宏。选择要更改的用户定义或系统定义的 CLI 宏。命令显示在命令窗格中。

步骤 6 使用 命令窗格中的 命令，点击 CLI 宏金色星标。  命令现在是新 CLI 宏的基础。

步骤 7 请为宏指定唯一的名称。如果需要，请为 CLI 宏提供说明和注释。

步骤 8 查看命令字段中的命令，并进行所需的更改。

步骤 9 运行命令时，将要修改的命令部分替换为用大括号括起来的参数名称。

步骤 10 点击**创建**。您创建的宏可用于该类型的所有设备，而不只是您最初指定的设备。

要运行命令，请参阅运行 CLI 宏。

运行 CLI 宏

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击相应的设备类型选项卡，然后选择一个或多个设备。

步骤 4 点击 **>_命令行接口**。

步骤 5 在命令面板中，点击星号 ★。

步骤 6 从命令面板中选择 CLI 宏。

步骤 7 使用以下两种方式之一运行宏：

- 如果宏没有要定义的参数，请点击**发送 (Send)**。命令的响应显示在响应窗格中。就行了。
- 如果宏包含参数，例如下面的配置 DNS 宏，请点击 **>_ 查看参数**。

步骤 8 在“参数”(Parameters) 窗格中，在“参数”(Parameters) 字段中填写参数的值。

步骤 9 点击 **Send**。在 CDO 成功发送命令并更新设备配置后，您会收到消息完成！

- 对于 FTD，会更新设备的活动配置。

步骤 10 发送命令后，您可能会看到消息“某些命令可能已对运行配置进行了更改”(Some commands may have made changes to the running config) 以及两个链接。

- 点击**写入磁盘 (Write to Disk)** 会将此命令所做的更改以及运行配置中的任何其他更改保存到设备的启动配置中。
- 点击**消除 (Dismiss)**，可关闭消息。

编辑 CLI 宏

您可以编辑用户定义的 CLI 宏，但不能编辑系统定义的宏。编辑 CLI 宏会更改所有 FTD 设备。宏并非特定于特定设备。

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。
步骤 2 点击**设备**选项卡。
步骤 3 点击适当的设备类型选项卡。
步骤 4 请选择您的设备。
步骤 5 点击 **命令行接口 (Command Line Interface)**。
步骤 6 选择要编辑的用户定义的宏。
步骤 7 点击宏标签中的编辑图标。
步骤 8 在编辑宏对话框中编辑 CLI 宏。
步骤 9 点击**保存 (Save)**。

有关如何运行 CLI 宏的说明，请参阅运行 CLI 宏。

删除 CLI 宏

您可以删除用户定义的 CLI 宏，但不能删除系统定义的宏。删除 CLI 宏会删除所有设备的宏。宏并非特定于特定设备。

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。
步骤 2 点击**设备**选项卡。
步骤 3 点击适当的设备类型选项卡。
步骤 4 请选择您的设备。

步骤 5 点击 >_**命令行接口 (Command Line Interface)**。

步骤 6 选择要删除的用户定义的 CLI 宏。

步骤 7 点击 CLI 宏标签中的垃圾桶图标 。

步骤 8 确认要删除 CLI 宏。

命令行接口文档

CDO 部分支持 FDM 管理 设备的命令行界面。我们在 CDO 中提供类似终端的接口，供用户以命令和响应形式同时向单个设备和多个设备发送命令。对于 CDO 中不支持的命令，请使用设备 GUI 终端（例如 PuTTy 或 SSH 客户端）访问设备，并参阅 CLI 文档以了解更多命令。

导出 CLI 命令结果

您可以将向独立设备或多个设备发出的CLI命令结果导出为逗号分隔值（.csv）文件，以便您可以随意过滤和排序其中的信息。您可以导出单个设备或多个设备的CLI结果。导出的信息包含以下内容：

- 设备
- 日期
- 用户
- 命令
- 输出

导出 CLI 命令结果

您可以将刚刚在命令窗口中执行的命令的结果导出到 .csv 文件：

Procedure

步骤 1 在导航栏中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备，使其突出显示。

步骤 5 在设备的**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。

步骤 6 在命令行界面窗格中，输入命令并点击发送以向设备发出命令。

步骤 7 在已输入命令的窗口右侧，点击导出图标。

步骤 8 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。读取 .csv 文件上的命令输出时，展开所有单元格以查看命令的所有结果。

导出 CLI 宏的结果

您可以导出已在命令窗口中执行的宏的结果。使用以下程序可将在一台或多台设备上执行的 CLI 宏的结果导出到 .csv 文件：

Procedure

步骤 1 打开 **设备和服务** 页面。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备，使其突出显示。

步骤 5 在设备的**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。

步骤 6 在 CLI 窗口的左侧窗格中，选择 CLI 宏收藏夹星型。

步骤 7 点击要导出的宏命令。填写任何适当的参数，然后点击发送。

步骤 8 在已输入命令的窗口右侧，点击导出图标。

步骤 9 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。读取 .csv 文件上的命令输出时，展开所有单元格以查看命令的所有结果。

导出 CLI 命令历史记录

使用以下程序将一个或多个设备的 CLI 历史记录导出到 .csv 文件：

Procedure

步骤 1 在导航窗格中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备，使其突出显示。

步骤 5 在设备的“设备操作”(Device Actions) 窗格中，点击**命令行接口 (Command Line Interface)**。

步骤 6 如果历史记录窗格尚未展开，请点击时钟图标将其展开。

步骤 7 在已输入命令的窗口右侧，点击导出图标。

步骤 8 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。读取 .csv 文件上的命令输出时，展开所有单元格以查看命令的所有结果。

相关信息：

- CDO 命令行接口, on page 96
- 从新命令创建 CLI 宏
- 删除 CLI 宏
- 编辑 CLI 宏
- 运行 CLI 宏
- 命令行接口文档
- 批量命令行接口

导出 CLI 宏列表

您只能导出已在命令窗口中执行的宏。使用以下程序将一个或多个设备的 CLI 宏导出到 .csv 文件：

过程

步骤 1 在导航窗格中，点击 **设备和服务**。
步骤 2 点击**设备**选项卡。
步骤 3 点击适当的设备类型选项卡。
步骤 4 选择一个或多个设备，使其突出显示。
步骤 5 在设备的“设备操作”(Device Actions) 窗格中，点击**>_命令行接口 (>_Command Line Interface)**。
步骤 6 在 CLI 窗口的左侧窗格中，选择 CLI 宏收藏夹星型。
步骤 7 点击要导出的宏命令。填写任何适当的参数，然后点击发送。
步骤 8 在已输入命令的窗口右侧，点击导出图标。
步骤 9 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。

对象

对象是可在一个或多个安全策略中使用的信息容器。使用对象可以轻松维护策略一致性。您可以创建单个对象，使用不同的策略，修改对象，然后将该更改传播到使用该对象的每个策略。如果没有对象，则需要单独修改需要进行相同更改的所有策略。

当您载入设备时， 会识别该设备使用的所有对象，保存它们，并在“对象”(Objects) 页面上列出它们。CDO在“对象”(Objects) 页面中，可以编辑现有对象并创建要在安全策略中使用的新对象。

CDO 将多台设备上使用的对象称为**共享对象**，并在**对象 (Objects)** 页面中使用此标记 进行标识。

有时，共享对象会产生一些“问题”，并且不再在多个策略或设备之间完美共享：

- **重复对象**是指同一设备上具有不同名称但值相同的两个或多个对象。这些对象通常可用于类似的目的，并供不同的策略使用。重复的对象由此问题图标标识：
- **不一致对象**是指两台或多台设备上具有相同名称但值不同的对象。有时，用户会在不同的配置中创建具有相同名称和内容的对象，但随着时间的推移，这些对象的值会出现分歧，从而造成不一致。不一致的对象由此问题图标标识：
- **未使用的对象**是设备配置中存在但未被其他对象、访问列表或NAT规则引用的对象。未使用的对象由此问题图标标识：

您还可以创建在规则或策略中立即使用的对象。您可以创建不与任何规则或策略关联的对象。在规则或策略中使用该未关联的对象时，会创建该对象的副本并使用该副本。CDO

您可以通过导航至对象菜单或在网络策略的详细信息中查看对象来查看对象。CDO

CDO 允许您从一个位置跨受支持的设备管理网络和服务对象。使用 ，您可以通过以下方式管理对象：CDO

- 根据各种条件搜索和过滤所有对象。对象过滤器, on page 115
- 查找设备上的重复、未使用和不一致的对象，并合并、删除或解决这些对象问题。
- 查找未关联的对象，如果未使用，请将其删除。
- 发现跨设备通用的共享对象。
- 在提交更改之前，评估对象更改对一组策略和设备的影响。
- 比较一组对象及其与不同策略和设备的关系。
- 捕获设备在自行激活后使用的对象。CDO

如果您在创建、编辑或读取已载入设备的对象时遇到问题，请参阅以了解详细信息。对思科防御协调器进行故障排除, on page 715

对象类型

下表介绍您可以为设备创建和使用 CDO 管理的对象。

Table 5: FDM 托管设备对象类型

对象	说明
应用过滤器对象	应用过滤器对象定义 IP 连接中使用的应用，或按类型、类别、标记、风险或业务相关性定义应用的过滤器。您可以在策略中使用这些对象而不是使用端口规格来控制流量。
上传 RA AnyConnect 客户端配置文件	AnyConnect 客户端文件对象是文件对象，表示配置中使用的文件，通常适用于远程接入 VPN 策略。可以包含 AnyConnect 客户端配置文件和 AnyConnect 客户端映像文件。
证书对象	数字证书是一种用于身份验证的数字识别方式。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。
DNS 服务器组对象	需要使用 DNS 服务器将完全限定域名 (FQDN) 解析为 IP 地址，例如 www.example.com。您可以为管理和数据接口配置不同的 DNS 组对象。
创建和编辑 Firepower 地理位置过滤器对象	地理位置对象定义托管设备（流量的源或目的）的国家/地区和大洲。您可以在策略中使用这些对象而不是使用 IP 地址来控制流量。
创建或编辑 IKEv1 策略	当定义 VPN 连接时， IKEv1 策略对象包含定义 VPN 连接时 IKEv1 策略所需的参数。
IKEv2 策略	当定义 VPN 连接时， IKEv2 策略对象包含定义 VPN 连接时 IKEv2 策略所需的参数。
IKEv1 IPSEC 提议	IPsec 提议对象配置 IKE 第 1 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。
IKEv2 IPSEC 提议	IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。
网络对象	网络组和网络对象（统称为“网络对象”）定义主机或网络的地址。
安全区域对象	安全区是一组接口。区域将网络划分成网段，帮助您管理流量以及对流量进行分类。
服务对象	服务对象、服务组和端口组是包含被视为 TCP/IP 协议簇一部分的协议或端口的可重用组件。

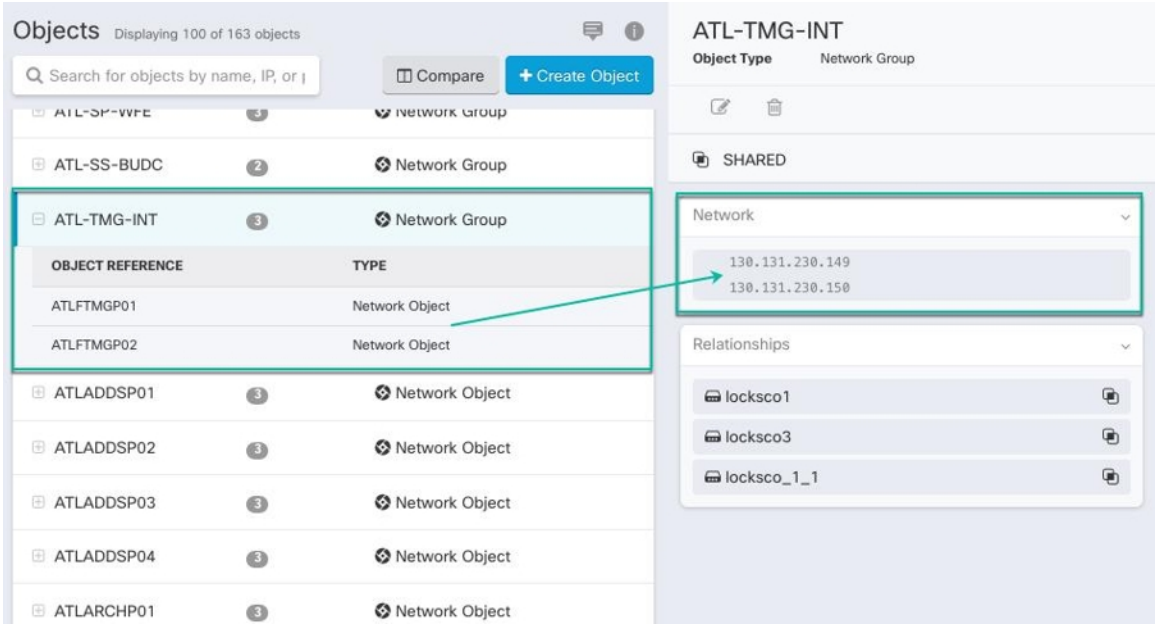
对象	说明
创建 SGT 组	SGT 动态对象根据 ISE 分配的 SGT 识别源或目标地址，然后可以与传入流量进行匹配。
系统日志服务器对象	系统日志服务器对象标识可接收面向连接的消息或诊断系统日志（系统日志）消息的服务器。
URL 对象	使用 URL 对象和组（统称为“URL 对象”）可定义 Web 请求的 URL 或 IP 地址。可以使用这些对象在访问控制策略中执行手动URL过滤，或在安全情报策略中进行阻止。

共享对象

Cisco Defense Orchestrator (CDO) 会调用多个设备上具有相同名称和相同内容的对象，即**共享对象**。共享对象由此图标标识

在**对象 (Objects)** 页面上。使用共享对象可以轻松维护策略，因为您可以在一个位置修改对象，并且该更改会影响使用该对象的所有其他策略。如果没有共享对象，则需要单独修改需要进行相同更改的所有策略。

查看共享对象时，CDO 会在对象表中显示该对象的内容。共享对象具有完全相同的内容。CDO 在详细信息窗格中显示对象元素的组合视图或“平面化”视图。请注意，在详细信息窗格中，网络元素被展平为一个简单的列表，而不是直接与命名对象关联。

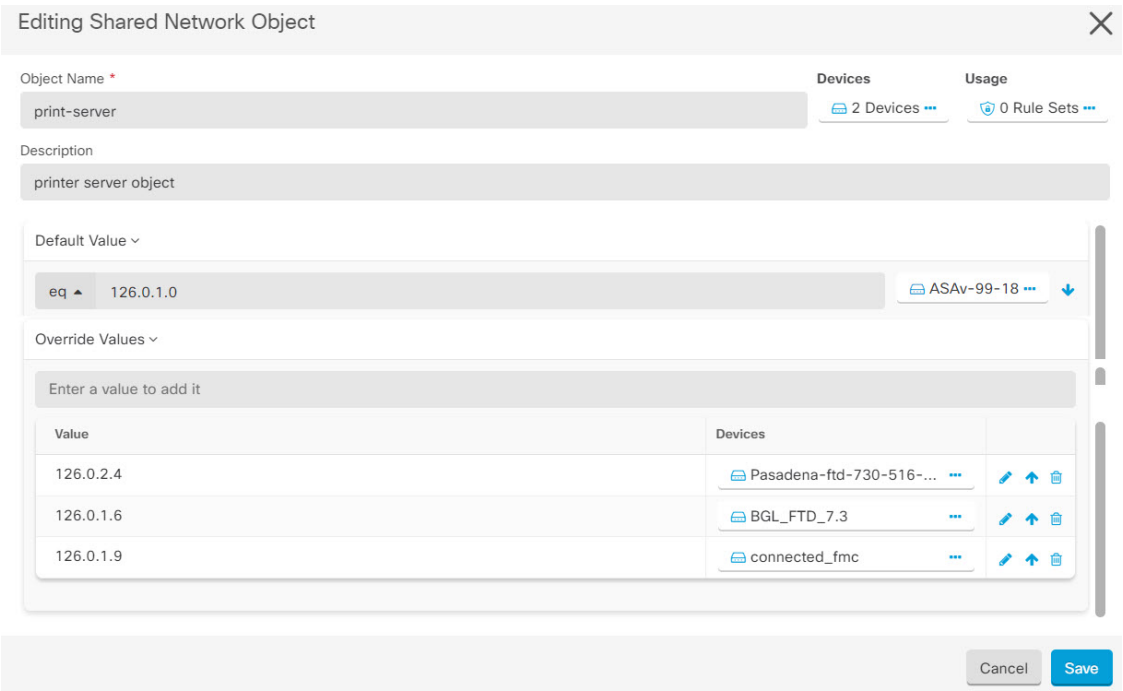


对象覆盖

对象覆盖允许您覆盖特定设备上共享网络对象的值。CDO 会使用您在配置覆盖时指定的设备的相应值。虽然对象位于两个或多个名称相同但值不同的设备上，但 CDO 不会将其识别为**不一致对象**，因为这些值是作为覆盖值添加的。

您可以创建其定义适用于大多数设备的对象，然后使用覆盖为需要不同定义的几个设备指定对象的修改。您还可以创建需要为所有设备覆盖的对象，但其使用使您能够为所有设备创建单个策略。对象覆盖允许您创建较小的一组在设备间使用的共享策略，而不会失去在各个设备需要时修改策略的能力。

例如，假设您的每个办公室都有一台打印机服务器，并且您创建了一个打印机服务器对象 `print-server`。您的 ACL 中有一条规则，用于拒绝打印机服务器访问互联网。打印机服务器对象有一个您想在办公室之间更改的默认值。您可以使用对象覆盖来实现此目的，并在所有位置保持规则和“printer-server”对象的一致性，但它们的值可能不同。



Note CDO 允许您覆盖与规则集中的规则关联的对象。在将新对象添加到规则时，只有在将设备附加到规则集并保存更改后，才能覆盖该对象。有关详细信息，请参阅为设备配置规则集。

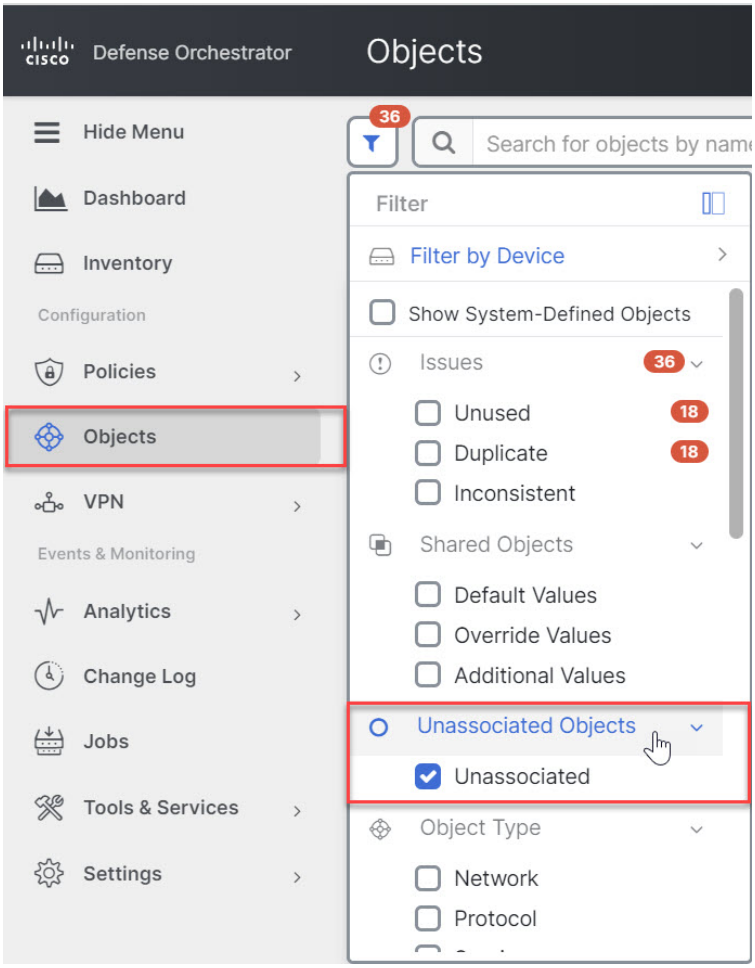
Note 如果存在不一致的对象，您可以将它们合并为一个具有覆盖的共享对象。有关详细信息，请参阅解决不一致的对象问题, on page 721。

未关联的对象

您可以创建对象以立即在规则或策略中使用。您还可以创建不与任何规则或策略关联的对象。当您在规则或策略中使用该未关联的对象时，CDO 会创建该对象的副本并使用该副本。原始未关联对象仍保留在可用对象列表中，直到被夜间维护作业删除或您将其删除。

未关联的对象作为副本保留在 CDO 中，以确保在意外删除与对象关联的规则或策略时不会丢失所有配置。

要查看未关联的对象，请点击对象选项卡的左侧窗格，然后选中未关联的复选框。

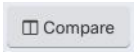


比较对象

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

步骤 2 过滤页面上的对象以查找要比较的对象。

步骤 3 点击**比较**按钮 

。

步骤 4 最多选择三个要比较的对象。

步骤 5 并排查看屏幕底部的对象。

- 点击“对象详细信息”(Object Details) 标题栏中的向上和向下箭头，可查看更多或更少的对象详细信息。
- 展开或折叠详细信息和关系框以查看更多或更少的信息。

步骤 6 （可选）“关系”框显示对象的使用方式。它可能与设备或策略相关联。如果对象与设备关联，您可以点击设备名称，然后点击**查看配置**以查看设备的配置。CDO 显示设备的配置文件，并突出显示该对象的条目。

过滤器

您可以在**清单 (Inventory)** 和**对象 (Objects)** 页面上使用许多不同的过滤器来查找要查找的设备和对象。

要过滤，请点击设备和服务、策略和对象选项卡的左侧窗格中的  ：

清单过滤器允许您按设备类型、硬件和软件版本、Snort 版本、配置状态、连接状态、冲突检测以及保护设备连接器和标签进行过滤。您可以应用过滤器在所选设备类型选项卡中查找设备。您可以使用过滤器在所选设备类型选项卡中查找设备。

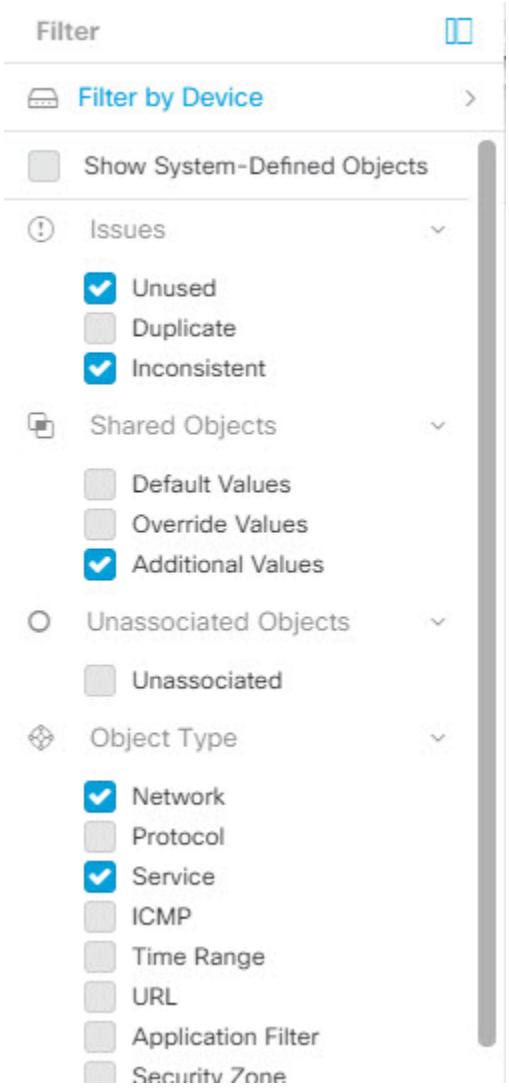
注释 打开 **FTD** 选项卡时，过滤器窗格将提供过滤器，以根据从 CDO 访问设备的管理应用来显示 FDM 管理 设备。

- FDM：使用 FTD API 或 FDM 管理的设备。
- FMC-FTD：通过使用 Firepower 管理中心管理的设备。
- FTD：使用 FTD 管理来管理的设备。

对象过滤器允许您按设备、问题类型、共享对象、未关联的对象和对象类型进行过滤。您可以在结果中包含或不包含系统对象。您还可以使用搜索字段在过滤器结果中搜索包含特定名称、IP 地址或端口号的对象。

过滤设备和对象时，您可以组合搜索词来创建多个潜在的搜索策略来查找相关结果。

在以下示例中，过滤器应用于“问题（已使用或不一致）AND 具有其他值的共享对象 AND 类型为网络 OR 服务的对象”。



对象过滤器

要过滤，请点击“对象”(Objects) 选项卡的左侧窗格的 ：

- **所有对象 (All Objects)** - 此过滤器提供您在 CDO 中注册的所有设备中可用的所有对象。此过滤器可用于浏览所有对象，或作为搜索或进一步应用子过滤器的起点。
- **共享对象 (Shared Objects)** - 此快速过滤器显示 CDO 发现的在多台设备上共享的所有对象。
- **按设备排列的对象 (Objects By Device)** - 允许您选择特定设备，以便可以查看在所选设备上找到的对象。

子过滤器 (Sub filters) - 在每个主过滤器中，您可以应用子过滤器以进一步缩小选择范围。这些子过滤器基于对象类型 - 网络、服务、协议等。

此过滤器栏中的选定过滤器将返回与以下条件匹配的对象：

***** 位于两台设备之一上的对象。（点击**按设备过滤 (Filter by Device)** 以指定设备。）AND 是

*** 不一致** 对象 AND 是

*** 网络 (Network)** 对象 OR **服务 (Service)** 对象 AND

***** 包含**"组"** 在对象命名约定中

由于选中了**显示系统对象 (Show System Objects)**，因此结果将包括系统对象和用户定义的对象。

显示系统对象过滤器

某些设备随附常见服务的预定义对象。这些系统对象很方便，因为它们已经为您创建，您可以在规则和策略中使用它们。对象表中可以有许多系统对象。系统对象无法编辑或删除。

默认情况下，**显示系统对象**处于**关闭**状态。要在对象表中显示系统对象，请选中过滤器栏中的**显示系统对象 (Show System Objects)**。要隐藏对象表中的系统对象，请在过滤器栏中保持未选中状态。

如果隐藏系统对象，它们将不会包含在搜索和过滤结果中。如果显示系统对象，它们将包含在对象搜索和过滤结果中。

配置对象过滤器

您可以根据需要过滤任意数量的条件。过滤所依据的类别越多，预期的结果就越少。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

步骤 2 点击页面顶部的过滤器图标，打开过滤器面板。取消选中任何已选中的过滤器，以确保不会无意中过滤掉任何对象。此外，查看搜索字段并删除可能已在搜索字段中输入的任何文本。

步骤 3 如果要将结果限制为在特定设备上找到的结果，请执行以下操作：

a. 点击**按设备过滤 (Filter By Device)**。

b. 搜索所有设备或点击设备选项卡以仅搜索特定类型的设备。

c. 选中要包含在过滤条件中的设备。

d. 点击**确定 (OK)**。

步骤 4 选中**显示系统对象 (Show System Objects)** 以在搜索结果中包含系统对象。取消选中**显示系统对象 (Show System Objects)** 可从搜索结果中排除系统对象。

步骤 5 选中要作为过滤依据的对象**问题**。如果选中多个问题，则选中的任何类别的对象都将包含在过滤器结果中。

步骤 6 如果要查看存在问题但被管理员忽略的对象，请选中**已忽略 (Ignored)** 的问题。

步骤 7 如果要过滤两台或多台设备之间共享的对象，请在**共享对象 (Shared Objects)** 中选中所需的过滤器。

- **默认值 (Default Values)**：过滤仅具有默认值的对象。
- **覆盖值 (Override Values)**：过滤具有覆盖值的对象。

- **其他值 (Additional Values)**：过滤具有其他值的对象。

步骤 8 如果要过滤不属于任何规则或策略的对象，请选中**未关联 (Unassociated)** 。

步骤 9 选中要作为过滤依据的**对象类型 (Object Types)**。

步骤 10 您还可以将对象名称、IP 地址或端口号添加到对象搜索字段，以在过滤结果中查找符合搜索条件的对象。

何时从过滤条件中排除设备

将设备添加到过滤条件时，结果会显示设备上的对象，但不会显示这些对象与其他设备的关系。例如，假设 ObjectA 在 ASA1 和 ASA2 之间共享。如果要过滤对象以查找 ASA1 上的共享对象，则会找到 ObjectA，但“关系”窗格只会显示该对象位于 ASA1 上。

要查看与对象相关的所有设备，请不要在搜索条件中指定设备。按其他条件过滤并添加搜索条件（如果您愿意）。选择CDO识别的对象，然后在“关系”窗格中进行查看。您将看到与对象相关的所有设备和策略。

忽略对象

解决具有未使用、重复或不一致问题对象的方法之一是忽略它们。您可以决定，尽管对象未使用、重复或不一致，但该状态存在正当理由，并且您选择不解决对象问题。解决未使用的对象问题, on page 720解决重复对象问题, on page 719解决不一致的对象问题, on page 721在未来的某个时候，您可能希望解析这些被忽略的对象。由于CDO在搜索对象问题时不显示已忽略的对象，因此您需要过滤已忽略对象的对象列表，然后对结果执行操作。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

步骤 2 过滤和搜索被忽略的对象。对象过滤器, on page 115

步骤 3 在**对象 (Object)** 表中，选择要取消忽略的对象。一次可以取消忽略一个对象。

步骤 4 点击详细信息窗格中的取消忽略。

步骤 5 确认您的请求。现在，当您按问题过滤对象时，您应该会找到以前忽略的对象。

删除对象

可以删除单个对象或多个对象。

删除单个对象

Caution 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure

步骤 1 在左侧的 CDO 导航栏中，选择**对象 (Objects)**并选择一个选项。

步骤 2 使用对象过滤器和搜索字段找到要删除的对象，然后将其选中。

步骤 3 查看关系窗格。如果在策略或对象组中使用了对象，则在将其从该策略或组中删除之前，无法删除该对象。

步骤 4 点击“操作”(Actions) 窗格中，点击**编辑**图标 。

步骤 5 点击确定，确认要删除对象。

步骤 6 预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

删除一组未使用的对象

当您载入设备并开始解决对象问题时，您会发现许多未使用的对象。一次最多可以删除50个未使用的对象。

过程

步骤 1 使用问题过滤器查找未使用的对象。您还可以使用设备过滤器通过选择无设备来查找未与设备关联的对象。过滤对象列表后，系统将显示对象复选框。

步骤 2 选中对象表标题中的全选复选框，以选择过滤器找到的显示在对象表中的所有对象；或者，选中要删除的各个对象的各个复选框。

步骤 3 点击“操作”(Actions) 窗格中，点击**编辑**图标 。

步骤 4 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

网络对象

网络对象 可以包含主机、网络 IP 地址、IP 地址范围、完全限定域名 (FQDN)或用 CIDR 符号表示的子网 。**网络组**是添加到组中的网络对象和其他单个地址或子网络的集合。网络对象和网络组用于访问规则、网络策略和 NAT 规则。您可以使用 CDO 创建、更新和删除网络对象和网络组。

Table 6: 网络对象的允许值

设备类型	**IPv4 / IPv6**	单个地址	地址范围	域名名称	使用 **CIDR** 表示法的子网。
FTD	IPv4 和 IPv6	是	是	是	是

Table 7: 网络组允许的内容

设备类型	**IP** 值	网络对象	网络组
FTD	不支持	是	是

跨产品重用网络对象

如果您的 思科防御协调器 租户具有云交付的防火墙管理中心：

在创建 Secure Firewall Threat Defense、FDM 管理 威胁防御、ASA 或 Meraki 网络对象或组时，对象的副本也会被添加到在配置 云交付的防火墙管理中心 时使用的**对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的对象列表中。

对任一页面上的网络对象或组所做的更改适用于两个页面上的对象或组实例。从一个页面删除对象也会从另一个页面删除该对象的相应副本。

例外情况：

- 如果 云交付的防火墙管理中心 已存在同名的网络对象，则不会在 思科防御协调器 的**对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上复制新的 Secure Firewall Threat Defense、FDM 管理 威胁防御、ASA 或 Meraki 网络对象
- 由本地 Cisco Secure Firewall Management Center 管理的载入 威胁防御 设备中的网络对象和组不会复制到**对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面，因此无法在 云交付的防火墙管理中心 中使用。

  请注意，对于已迁移到 云交付的防火墙管理中心 的本地 Cisco Secure Firewall Management Center 实例，如果在部署到 FTD 设备的策略中使用网络对象和组，它们将被复制到 CDO 对象页面。
- 新租户上会自动启用在 CDO 和 云交付的防火墙管理中心 之间共享网络对象，但现有租户必须另行请求。如果您的网络对象未与 云交付的防火墙管理中心 共享，请CDO 客户如何通过 TAC 提交支持请求 以在您的租户上启用这些功能。

查看网络对象

使用 CDO 创建的网络对象以及已载入的设备配置中的 CDO 识别的网络对象会显示在对象页面上。它们标有对象类型。这使您可以按对象类型进行过滤，以快速找到要查找的对象。

在“对象”(Objects) 页面上选择网络对象时，您可在“详细信息”(Details) 窗格中看到该对象的值。“关系”(Relationships) 窗格显示对象是否用于策略中，以及对象存储在什么设备上。

在点击网络组时，您会看到该组的内容。网络组是网络对象为其提供的所有值的综合体。

相关信息：

- 创建或编辑 Firepower 网络对象或网络组

创建或编辑 Firepower 网络对象或网络组

Firepower 网络对象可以包含以 CIDR 表示法表示的主机名、IP 地址或子网地址。**网络组**是在访问规则、网络策略和NAT规则中使用的网络对象和网络组的集合。您可以使用 思科防御协调器(CDO)来创建、读取、更新和删除网络对象和网络组。

Firepower 网络对象和组可供 ASA、威胁防御、FDM 管理 和 Meraki 设备使用。请参阅跨产品重用网络对象, on page 119。

Note 如果 云交付的防火墙管理中心 被部署在您的租户上：

在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上创建网络对象或组时，对象的副本会自动添加到 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面，反之亦然。

Caution 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Table 8: 可以添加到网络对象的 ***IP*** 地址

设备类型	IPv4 / IPv6	单个地址	地址范围	部分限定域名 (PQDN)	使用 CIDR 表示法的子网。
FirePower	IPv4 / IPv6	是	是	是	是

相关信息：

- 编辑 Firepower 网络对象, on page 121
- 编辑 Firepower 网络对象, on page 123

- 向共享网络组添加其他值, on page 125
- 编辑共享网络组中的其他值, on page 127

编辑 Firepower 网络对象

Note 如果 云交付的防火墙管理中心 被部署在您的租户上：

在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上创建网络对象或组时，对象的副本会自动添加到 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面，反之亦然。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮  以创建新的对象。

步骤 3 点击**FTD** > **网络 (Network)**。

步骤 4 输入 **对象名称**。

步骤 5 选择 **创建网络对象**。

步骤 6 在**值 (Value)** 部分中：

- 选择 **eq** 并输入以 CIDR 表示法表示的单个 IP 地址、子网地址或部分限定域名 (PQDN)。
- 选择**范围**并输入 IP 地址范围。

Note 请勿设置主机位值。如果输入的主机位值不是 0，CDO 会在创建对象时取消设置，因为云交付的防火墙管理中心 仅接受未设置主机位的 IPv6 对象。

步骤 7 点击**添加 (Add)**。

注意：新创建的网络对象不与任何 FDM 管理 设备关联，因为它们不属于任何规则或策略。要查看这些对象，请在对象过滤器中选择**未关联**的对象类别。有关详细信息，请参阅配置对象过滤器。在设备的规则或策略中使用未关联的对象后，此类对象将与该设备关联。

创建 Firepower 网络组

网络组可以包含网络对象和网络组。创建新的网络组时，可以按名称、IP 地址、IP 地址范围或 FQDN 搜索现有对象，并将其添加到网络组。如果对象不存在，您可以立即在同一接口中创建该对象并将其添加到网络组。

Note 如果 云交付的防火墙管理中心 被部署在您的租户上：

在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上创建网络对象或组时，对象的副本会自动添加到 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面，反之亦然。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮 以创建新的对象。

步骤 3 点击**FTD** > **网络 (Network)**。

步骤 4 输入 **对象名称**。

步骤 5 选择创建网络组。

步骤 6 在**值 (Values)** 字段中输入值或名称。当您开始输入时，CDO 会提供与您的条目匹配的对象名称或值。

步骤 7 您可以选择一个显示的现有对象，也可以根据输入的名称或值创建一个新对象。

步骤 8 如果 CDO 找到了匹配项，要选择现有对象，请点击**添加 (Add)** 将网络对象或网络组添加到新网络组。

步骤 9 如果输入的值或对象不存在，则可以执行以下操作之一：

- 点击**添加为此名称的新对象 (Add as New Object With This Name)**，以创建具有该名称的新对象。输入一个值，然后点击复选标记将其保存。
- 点击**添加为新对象 (Add as New Object)** 以创建一个新对象。对象名称和值相同。输入名称，然后点击复选标记将其保存。

即使该值已存在，也可以创建一个新对象。您可以对这些对象进行更改并将它们保存。

注意：您可以点击编辑图标修改详细信息。点击“删除”按钮不会删除对象本身；相反，它会将其从网络组中删除。

步骤 10 添加所需的对象后，点击保存以创建新的网络组。

步骤 11 预览和部署所有设备的配置更改。

编辑 Firepower 网络对象

Caution 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的对象。

步骤 3 选择网络对象，然后点击**操作 (Actions)** 窗格中的编辑图标 。

步骤 4 以在“创建 Firepower 网络组”(Create a Firepower Network Group) 中创建值的相同方式编辑对话框中的值。

Note 点击旁边的删除图标，从网络组中删除对象。

步骤 5 点击**保存 (Save)**。CDO 会显示将受更改影响的设备。

步骤 6 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

编辑 Firepower 网络组

Caution 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到您要编辑的网络组。

步骤 3 选择网络组，然后点击**操作 (Actions)** 窗格中的编辑图标 。

步骤 4 如有必要，更改对象名称和说明。

步骤 5 如果要更改已添加到网络组的对象或网络组，请执行以下步骤：

a. 点击对象名称或网络组旁边的编辑图标可对其进行修改。

b. 点击复选标记以保存更改。**注意**：您可以点击删除图标从网络组中删除该值。

步骤 6 如果要向此网络组添加新的网络对象或网络组，必须执行以下步骤：

a. 在值字段中，输入新值或现有网络对象的名称。当您开始输入时，CDO 会提供与您的条目匹配的对象名称或值。您可以选择一个显示的现有对象，也可以根据输入的名称或值创建一个新对象。

b. 如果 CDO 找到了匹配项，要选择现有对象，请点击**添加 (Add)** 将网络对象或网络组添加到新网络组。

c. 如果输入的值或对象不存在，则可以执行以下操作之一：

- 点击**添加为此名称的新对象 (Add as New Object With This Name)**，以创建具有该名称的新对象。输入一个值，然后点击复选标记将其保存。
- 点击**添加为新对象 (Add as New Object)** 以创建一个新对象。对象名称和值相同。输入名称，然后点击复选标记将其保存。

即使该值已存在，也可以创建一个新对象。您可以对这些对象进行更改并将它们保存。

步骤 7 点击**保存 (Save)**。CDO 显示将受更改影响的策略。

步骤 8 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

步骤 9 预览和部署所有设备的配置更改。

添加对象覆盖

⚠

注意 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

过程

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到具有要编辑的覆盖的对象。

步骤 3 选择网络对象，然后点击**操作 (Actions)** 窗格中的编辑图标 。

步骤 4 在**覆盖值 (Override Values)** 对话框中输入值，然后点击 **+ 添加值 (+ Add Value)**。

重要事项 要添加的覆盖必须具有与对象所包含的值类型相同。例如，对于网络对象，只能使用网络值而不是主机值来配置覆盖。

步骤 5 看到添加的值后，点击**覆盖值 (Override Values)** 的**设备 (Devices)** 列中的单元格。

步骤 6 点击**添加设备 (Add Devices)**，然后选择要向其添加覆盖的设备。您选择的设备必须包含要向其添加覆盖的对象。

步骤 7 点击**保存 (Save)**。CDO 会显示将受更改影响的设备。

步骤 8 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的覆盖添加。

注释 您可以向一个对象添加多个覆盖。但每次添加覆盖时，都必须选择包含对象的不同设备。

步骤 9 请参阅对象覆盖，第 112 页，了解有关对象覆盖和编辑对象覆盖，第 125 页的详细信息以编辑现有覆盖。

编辑对象覆盖

只要设备上存在对象，您就可以修改现有覆盖的值。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到具有要编辑的覆盖的对象。

步骤 3 选择带有覆盖的对象，然后点击“操作”(Actions) 窗格中的编辑图标  。

步骤 4 修改覆盖值：

- 点击编辑图标以修改值。
- 在**覆盖值 (Override Values)** 中点击**设备 (Devices)** 列，以便分配新设备。您可以选择已分配的设备，然后点击**删除覆盖 (Remove Overrides)** 以删除该设备上的覆盖。
- 点击**覆盖值 (Override Values)** 中的 箭头，将其推送并设置为共享对象的默认值。
- 点击要删除的覆盖旁边的删除图标。

步骤 5 点击**保存 (Save)**。CDO 会显示将受更改影响的设备。

步骤 6 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

步骤 7 预览和部署所有设备的配置更改。

向共享网络组添加其他值

共享网络组中与其关联的所有设备上都存在的值被称为“默认值”。CDO 允许您向共享网络组添加“其他值”，并将这些值分配给与该共享网络组关联的某些设备。当CDO将更改部署到设备时，它

会确定内容并将“默认值”推送到与共享网络组关联的所有设备，而“其他值”只会被推送到指定的设备。

例如，假设您的总部有四台 AD 主服务器，那么这些服务器应可从您的所有站点进行访问。因此，您创建了一个名为“Active-Directory”的对象组，以便用于所有站点。现在，您要为其中一个分支机构再添加两台 AD 服务器。为此，您可以通过将其详细信息添加为对象组“Active-Directory”上该分支机构的特定附加值来执行此操作。这两台服务器不参与确定对象“Active-Directory”是一致的还是共享的。因此，您可从所有站点访问四台 AD 主服务器，但分支机构（具有两台附加服务器）可以访问两台 AD 服务器和四台 AD 主服务器。

Note 如果存在不一致的共享网络组，则您可以将它们合并为具有其他值的单个共享网络组。有关详细信息，请参阅解决不一致的对象问题, on page 721。

Caution 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到您要编辑的共享网络组。

步骤 3 点击**操作 (Actions)** 窗格中的编辑图标 。

- **设备 (Devices)** 字段会显示共享网络组所在的设备。
- **使用情况 (Usage)** 字段会显示与共享网络组关联的规则集。
- **默认值 (Default Values)** 字段将指定默认网络对象及其与创建期间提供的共享网络组关联的值。在此字段旁边，您可以看到包含此默认值的设备数量，您可以点击查看其名称和设备类型。您还可以查看与此值关联的规则集。

步骤 4 在**其他值 (Additional Values)** 字段中输入值或名称。当您开始输入时，CDO 会提供与您的条目匹配的对象名称或值。

步骤 5 您可以选择一个显示的现有对象，也可以根据输入的名称或值创建一个新对象。

步骤 6 如果 CDO 找到了匹配项，要选择现有对象，请点击**添加 (Add)** 将网络对象或网络组添加到新网络组。

步骤 7 如果输入的值或对象不存在，则可以执行以下操作之一：

- 点击**添加为此名称的新对象 (Add as New Object With This Name)**，以创建具有该名称的新对象。输入一个值，然后点击复选标记将其保存。
- 点击**添加为新对象 (Add as New Object)** 以创建一个新对象。对象名称和值相同。输入名称，然后点击复选标记将其保存。

即使该值已存在，也可以创建一个新对象。您可以对这些对象进行更改并将它们保存。

步骤 8 在**设备 (Devices)** 列中，点击与新添加的对象关联的单元格，然后点击**添加设备 (Add Devices)**。

步骤 9 选择所需的设备，然后点击**确定 (OK)**。

步骤 10 点击**保存 (Save)**。CDO 会显示将受更改影响的设备。

步骤 11 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

步骤 12 预览和部署所有设备的配置更改。

编辑共享网络组中的其他值

Caution

如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到具有要编辑的覆盖的对象。

步骤 3 点击 **操作** 窗格中的编辑图标 。

步骤 4 修改覆盖值：

- 点击编辑图标以修改值。
- 点击**设备 (Devices)** 列中的单元格以分配新设备。您可以选择已分配的设备，然后点击**删除覆盖 (Remove Overrides)** 以删除该设备上的覆盖。
- 点击**默认值 (Default Values)** 中的 箭头，将其设置为共享网络组的其他值。与共享网络组关联的所有设备都会自动分配到该共享网络组。
- 点击**覆盖值 (Override Values)** 中的 箭头，将其推送并设置为共享网络组的默认对象。
- 点击旁边的删除图标，从网络组中删除对象。

步骤 5 点击**保存 (Save)**。CDO 会显示将受更改影响的设备。

步骤 6 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

步骤 7 预览和部署所有设备的配置更改。

删除网络对象和组

如果 云交付的防火墙管理中心 被部署在您的租户上：

从 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面删除网络对象或组都会从 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面中删除复制的对象或组，反之亦然。

应用过滤器对象

应用过滤器对象由 Firepower 设备使用。应用过滤器对象定义 IP 连接中使用的应用，或按类型、类别、标记、风险或业务相关性定义应用的过滤器。您可以在策略中使用这些对象而不是使用端口规格来控制流量。

虽然您可以指定个别应用，但应用过滤器可简化策略创建和管理。例如，您可以创建一条访问控制规则，用于识别并阻止所有业务相关性较低的高风险应用。如果用户尝试使用这些应用中的任何一个，系统会阻止会话。

您可以直接在策略中选择应用和应用过滤器，而不使用应用过滤器对象。但是，如果要为同一组应用或过滤器创建多个策略，使用对象则非常方便。该系统包括多个预定义的应用过滤器，您不能编辑或删除它们。

Note 思科会通过系统和漏洞数据库 (VDB) 更新频繁更改并添加其他应用检测器。因此，阻止高风险应用的规则可自动应用到新应用中，而无需您手动更新规则。

Note 当 FDM 托管的 FTD 设备被载入 CDO 时，它会将应用过滤器转换为应用过滤器对象，而不会更改访问规则或 SSL 解密中定义的规则。由于配置更改，设备的配置状态更改为“未同步”，需要从 CDO 进行配置部署。通常，在您手动保存过滤器之前，FDM 不会将应用过滤器转换为应用过滤器对象。

相关信息：

- 创建和编辑 Firepower 应用过滤器对象
- 删除对象

创建和编辑 Firepower 应用过滤器对象

应用过滤器对象允许您以精选应用或由过滤器识别的一组应用为目标。此应用过滤器对象可用于策略中。

创建 Firepower 应用过滤器对象

要创建应用过滤器对象，请执行以下程序：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

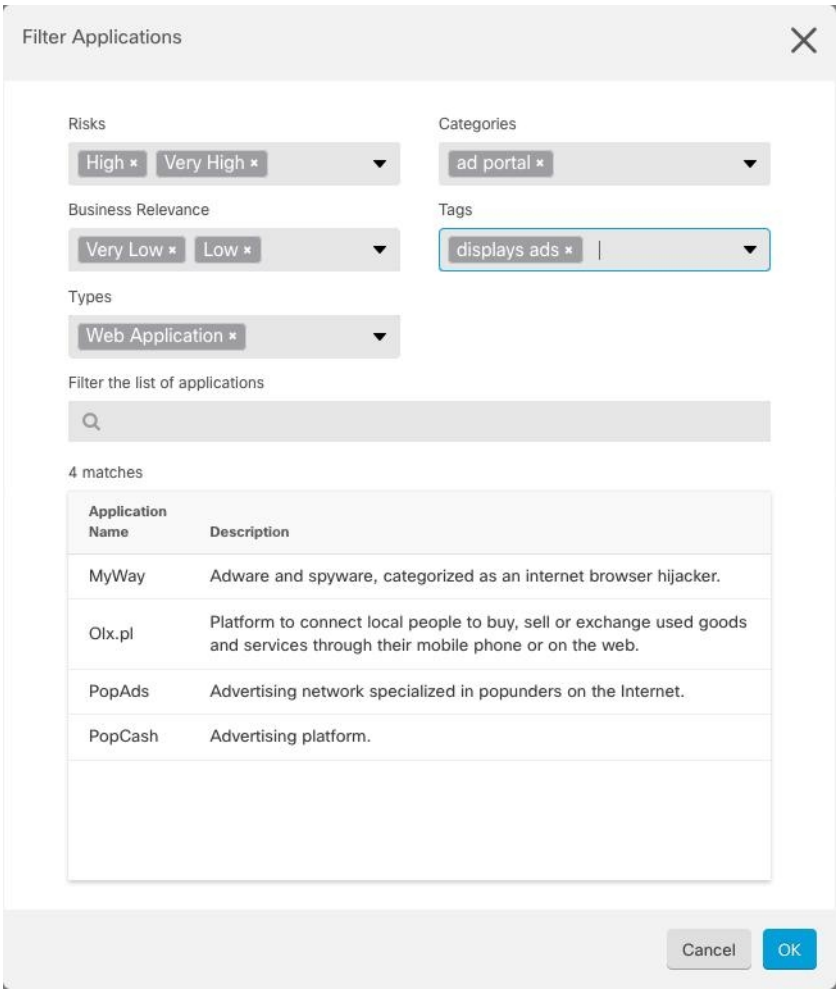
步骤 2 点击创建对象 > FTD > 应用服务。

步骤 3 输入对象的 **对象名称** 和 **说明**（后者为可选项）。

步骤 4 点击**添加过滤器 (Add Filter)**，然后选择要添加到对象的应用程序和过滤器。

初始列表将在连续滚动的列表中显示应用。点击**高级过滤器 (Advanced Filter)** 可查看过滤器选项，可更加方便地查看和选择应用。完成选择后，点击**添加 (Add)**。您可以重复该过程，以添加更多应用或过滤器。

Note 单个过滤器条件中的多个选项具有 OR 关系。例如，风险高 OR 非常高。过滤器之间的关系是 AND，因此是风险高 OR 非常高，AND 业务相关性低 OR 非常低。在选择过滤器时，显示屏中的应用列表更新，只显示符合条件的应用。您可以使用这些过滤器来帮助查找要单独添加的应用，或确认是否要选择所需的过滤器以添加到规则中。



风险 (Risks)：应用所用的用途可能违反组织安全策略的可能性，从非常低到非常高。

业务相关性 (Business Relevance)：在组织的业务运营环境（非娱乐性）下使用应用的可能性，从非常低到非常高。

类型 (Types)：应用类型。

- **应用协议 (Application Protocol)**：应用协议（例如 HTTP 和 SSH），代表主机之间的通信。
- **客户端协议 (Client Protocol)**：客户端（例如 Web 浏览器和邮件客户端），代表主机上运行的软件。
- **Web 应用 (Web Application)**：Web 应用（例如 MPEG 视频和 Facebook），代表 HTTP 流量的内容或请求的 URL。

类别 (Categories)：对应用的一般分类，说明其最基本的功能。

标记 (Tags)：关于应用的其他信息，与类别类似。

对于加密流量，系统可以仅使用标记有 SSL 协议的应用识别和过滤流量。只有在未加密或已解密的流量中才能检测到没有此标记的应用。此外，系统仅将已解密的流量标记分配给可在已解密的流量中检测到的应用，而不会将它们分配给加密或未加密的流量中检测到的应用。

应用列表 (Applications List)（显示底部）：在从列表上方的选项中选择过滤器时，此列表将进行更新，所以您可查看当前符合过滤器的应用。在计划将过滤器条件添加到规则中时，使用此列表可确认您的过滤器是否针对所需的应用。要将特定应用添加到对象，请从过滤列表中选择它们。选择应用后，过滤器将不再适用。如果您希望过滤器本身作为对象，请勿从列表中选择应用。然后，该对象将代表过滤器识别的应用。

步骤 5 点击**确定 (OK)**，保存更改。

编辑 Firepower 应用过滤器对象

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的对象。

步骤 3 选择要编辑的对象。

步骤 4 点击“操作”(Actions) 窗格中的编辑图标  。

步骤 5 以在上述过程中创建值的相同方式编辑对话框中的值。

步骤 6 点击**保存 (Save)**。

步骤 7 CDO 显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

相关信息：

- 对象
- 对象过滤器
- 删除对象

地理位置对象

地理位置对象定义托管设备（流量的源或目的）的国家/地区和大洲。您可以在策略中使用这些对象而不是使用 IP 地址来控制流量。例如，使用地理位置可以很容易地将访问权限限制为特定国家/地区，而无需知道此处使用的所有潜在 IP 地址。

通常，可以直接在策略中选择地理位置，而无需使用地理位置对象。但是，如果要为同一组国家/地区或大洲创建多个策略，使用对象则非常方便。

更新地理定位数据库

为了确保使用最新的地理位置数据来过滤流量，思科强烈建议您定期更新地理位置数据库(GeoDB)。目前，这不是您可以使用 Cisco Defense Orchestrator 执行的任务。请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》的以下部分，了解您的设备正在运行的版本，以了解有关 GeoDB 及其更新方式的详细信息。

- 更新系统数据库和源
- 更新系统数据库

创建和编辑 Firepower 地理位置过滤器对象

您可以在对象页面上或在创建安全策略时单独创建地理位置对象。此程序从对象页面创建地理位置对象。

要创建地理位置对象，请执行以下步骤：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
步骤 2 点击**创建对象 (Create Object)** > **FTD** > **地理位置 (Geolocation)**。
步骤 3 输入对象的 **对象名称** 和 **说明**（后者为可选项）。
步骤 4 在过滤器栏中，开始键入国家/地区或地区的名称，系统会显示可能的匹配项列表。
步骤 5 选中要添加到对象的国家/地区或地区。
步骤 6 点击**添加**。

编辑地理位置对象

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
步骤 2 使用过滤器窗格和搜索字段查找对象。
步骤 3 在“操作”(Actions) 窗格中，点击**编辑 (Edit)**。
步骤 4 您可以更改对象的名称，并向对象添加或删除国家/地区和地区。
步骤 5 点击**保存 (Save)**。
步骤 6 如果有任何设备受到影响，您会收到通知。点击 **Confirm**。
步骤 7 如果设备或策略受到影响，请打开资产页面并预览并将更改部署到设备。

DNS 服务器组对象

域名系统 (DNS) 组定义 DNS 服务器列表和某些相关联的属性。需要使用 DNS 服务器将完全限定域名 (FQDN) 解析为 IP 地址，例如 www.example.com。您可以为管理和数据接口配置不同的 DNS 组对象。

FDM 管理 设备必须先配置 DNS 服务器，然后才能创建新的 DNS 组对象。您可以将 DNS 服务器添加到 思科防御协调器 (CDO) 中的 配置 DNS 服务器，也可以在 防火墙设备管理器 中创建 DNS 服务器，然后将 FDM 管理 配置同步到 CDO。要在 防火墙设备管理器 中创建或修改 DNS 服务器设置，请参阅《思科 Firepower 设备管理器配置指南》，版本 6.4 或更高版本中的**为数据和管理接口配置 DNS**。

创建 DNS 组对象

使用以下程序在 CDO 中创建新的 DNS 组对象：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮  以创建新的对象。

步骤 3 点击 FTD DNS 组。 >

步骤 4 输入 **对象名称 (Object Name)**。

步骤 5 （可选）添加说明。

步骤 6 输入 **DNS 服务器**的 IP 地址。您最多可以添加六个 DNS 服务器；点击添加 DNS 服务器。如果您想要删除服务器地址，请点击删除图标。

Note 列表采用优先顺序：始终使用列表中的第一个服务器，只有当从前面的服务器收不到响应时，才使用后面的服务器。虽然最多可以添加六台服务器，但只有列出的前 3 台服务器将用于管理接口。

步骤 7 输入**域搜索名称 (Domain Search Name)**。此域将被添加到非完全限定的主机名，例如 serverA 而不是 serverA.example.com。

步骤 8 输入重试次数。系统接收不到响应时，重试 DNS 服务器列表的次数，介于 0 和 10 次之间。默认值为 2。此设置仅适用于数据接口上使用的 DNS 组。

步骤 9 输入**超时**值。尝试下一个 DNS 服务器之前要等待的秒数，介于 1 和 30 秒之间。默认值为 2 秒。每次系统重试服务器列表，此超时将加倍。此设置仅适用于数据接口上使用的 DNS 组。

步骤 10 点击**添加**。

编辑 DNS 组对象

您可以编辑在 思科防御协调器 或 防火墙设备管理器 中创建的 DNS 组对象。使用以下程序编辑现有的 DNS 组对象：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的 **DNS 组对象**。

步骤 3 选择对象，然后点击**操作 (Actions)** 窗格中的编辑图标 。

步骤 4 编辑以下任何条目：

- 对象名称。
- 说明。
- DNS 服务器。您可以在此列表中编辑、添加或删除 DNS 服务器。
- 域搜索名称。
- 重试。
- 超时。

步骤 5 点击**保存 (Save)**。

步骤 6 预览和部署所有设备的配置更改。

删除 DNS 组对象

使用以下程序从 CDO 中删除 DNS 组对象：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的 **DNS 组对象**。

步骤 3 选择对象，然后点击删除图标。

步骤 4 确认要删除 DNS 组对象，然后点击确定。

步骤 5 预览和部署所有设备的配置更改。

将 DNS 组对象添加为 DNS 服务器FDM 管理

您可以将 DNS 组对象添加为数据接口或管理接口的首选 DNS 组。有关详细信息，请参阅 FDM 托管设备设置。FDM 管理 设备设置, on page 521

证书对象

数字证书是一种用于身份验证的数字识别方式。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。

请参阅适用于您的设备的版本的《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》中可恢复对象一章的**关于证书**和**配置证书**部分。

关于证书

数字证书是一种用于身份验证的数字识别方式。数字证书包括用于识别设备或用户的信息，例如名称、序列号、公司、部门或 IP 地址。数字证书还包括用户或设备的公钥副本。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。

您可以创建以下类型的证书：

- **内部证书 (Internal certificates)** - 内部身份证书是用于特定系统或主机的证书。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名证书。

  系统提供以下预定义内部证书（您可以按原样使用或替换它们）：**DefaultInternalCertificate** 和 **DefaultWebServerCertificate**

- **内部证书颁发机构 (CA)** 证书 - 内部 CA 证书是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名的内部 CA 证书。如果配置自签名的内部 CA 证书，该 CA 将在设备自身上运行。

  系统提供以下预定义内部CA证书（您可以按原样使用或替换它们）：**NGFW-Default-InternalCA**

- **可信证书颁发机构 (CA)** 证书 - 可信的 CA 证书可用于签署其他证书。它是自签名证书，也称为根证书。由另一个 CA 证书颁发的证书称为从属证书。

  证书颁发机构 (CA) 是指“签署”证书以确认其真实性，从而确保设备或用户的身份的可信颁发机构。CA 在 PKI（使用公钥或私钥加密以确保安全性）的情景下颁发数字证书。CA 可以是可信的第三方（例如 VeriSign），也可以是组织内建立的私有（内部）CA。CA 负责管理证书请求和颁发数字证书。

  系统包括许多从第三方证书颁发机构获取的受信任的 CA 证书。SSL 解密策略可使用这些证书执行解密重新签署操作。

有关详细信息，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》中“可重用对象”一章的**功能使用的证书类型**部分。

功能使用的证书类型

您需要为每个功能创建正确类型的证书。以下功能需要证书。

身份策略（强制网络门户）- 内部证书

（可选。）强制网络门户用于身份策略中。在向设备进行身份验证时，为了标识自己的身份并接收与其用户名关联的 IP 地址，用户必须接受此证书。如果不提供证书，设备将使用自动生成的证书。

SSL 解密策略 - 内部、内部 CA 和受信任 CA 证书。

（必需。）SSL 解密策略将证书用于以下目的：

- 内部证书用于已知的密钥解密规则。
- 在客户端和 FTD 设备之间创建会话时，内部 CA 证书用于解密重签名规则。
- 受信任 CA 证书
  - 在 FTD 设备和服务器之间创建会话时，它们可直接用于解密重签名规则。与其他证书不同，这些证书不能直接在 SSL 解密策略中配置，而是需要上传到系统。系统包括大量受信任 CA 证书，因此，您无需上传任何其他证书。
  - 创建 Active Directory 领域对象并将目录服务器配置为使用加密时。

配置证书

身份策略或 SSL 解密策略中使用的证书必须是 PEM 或 DER 格式的 X509 证书。如果需要，您可以使用 OpenSSL 生成证书、从受信任的证书颁发机构获取证书或创建自签名证书。

使用以下程序配置证书对象：

- 上传内部证书和内部 CA 证书
- 上传受信任的 CA 证书
- 生成自签名的内部证书和内部 CA 证书
- 要查看或编辑证书，请点击证书的编辑图标或视图图标。
- 要删除未引用的证书，请点击证书的垃圾桶图标（删除图标）。请参阅删除对象。

上传内部证书和内部 CA 证书

内部身份证书是特定系统或主机的证书。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名证书。

内部证书颁发机构 (CA) 证书（内部 CA 证书）是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些

证书。此外，您还可以生成自签名的内部CA证书。如果配置自签名的内部CA证书，该CA将在设备自身上运行。

有关使用这些证书的功能的信息，请参阅功能使用的证书类型。

操作步骤

此程序通过上传证书文件或将现有证书文本粘贴到文本框中来创建内部证书身份或内部 CA 证书。如果要生成自签名证书，请参阅生成自签名内部证书和内部 CA 证书。生成自签名的内部证书和内部 CA 证书, on page 139

要创建内部或内部 CA 证书对象，或者在向策略添加新证书对象时，请执行以下程序：

Procedure

步骤 1 执行以下操作之一：

- 在对象页面中创建证书对象：
  a. 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
  b. 点击加号按钮，然后选择 FTD 证书 >
- 将新证书对象添加到策略时，点击创建新对象。

步骤 2 键入证书的**名称**。该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 3 在步骤 1 中，选择内部证书或内部 CA。

步骤 4 在步骤 2 中，选择**上传 (Upload)** 以上传证书文件。

步骤 5 在步骤 3 的**服务器证书 (Server Certificate)** 区域中，将证书内容粘贴到文本框中，或按照向导中的说明上传证书文件。如果将证书粘贴到文本框中，则证书必须包括 BEGIN CERTIFICATE 和 END CERTIFICATE 两行。例如：

```
-----BEGIN CERTIFICATE-----
 MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0
(...5 lines removed...)
shGJDReRYJQqilhHZrYTWZAYTrD7NQPHutK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZlzJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfxwCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjqy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
vlk3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

步骤 6 在步骤 3 的**证书密钥 (Certificate Key)** 区域中，将密钥内容粘贴到证书密钥文本框中，或者按照向导中的说明上传密钥文件。如果将密钥粘贴到文本框中，则密钥必须包含 BEGIN PRIVATE KEY 或 BEGIN RSA PRIVATE KEY 和 END PRIVATE KEY 或 END PRIVATE KEY 行。

Note 密钥不能加密。

步骤 7 点击**添加**。

上传受信任的 CA 证书

受信任证书颁发机构 (CA) 证书用于签署其他证书。它是自签名证书，也称为根证书。由另一个 CA 证书颁发的证书称为从属证书。

有关使用这些证书的功能的信息，请参阅功能使用的证书类型。

受信任 CA 证书可从外部证书颁发机构获取，也可以使用自己的内部 CA 创建（例如通过 OpenSSL 工具生成证书）。然后，使用以下步骤程序上传证书。

操作步骤

Procedure

步骤 1 执行以下操作之一：

- 在对象页面中创建证书对象：
  a. 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
  b. 点击加号按钮，然后选择 FTD 证书。 >
- 将新证书对象添加到策略时，点击创建新对象。

步骤 2 键入证书的**名称**。该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 3 在步骤 1 中，选择外部 CA 证书，然后点击继续。向导前进到步骤 3。

步骤 4 在步骤 3 的**证书内容 (Certificate Contents)** 区域中，将证书内容粘贴到文本框中，或按照向导中的说明上传证书文件。

证书必须遵循以下准则：

- 证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 10.10.10.250 作为 IP 地址，但证书中的地址为 ad.example.com，则连接失败。
- 该证书必须为 PEM 或 DER 格式的 X509 证书。
- 您粘贴的证书必须包括 BEGIN CERTIFICATE 和 END CERTIFICATE 行。例如：

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
```

```
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

步骤 5 点击**添加**。

生成自签名的内部证书和内部 CA 证书

内部身份证书是特定系统或主机的证书。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名证书。

内部证书颁发机构 (CA) 证书（内部 CA 证书）是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名的内部 CA 证书。如果配置自签名的内部 CA 证书，该 CA 将在设备自身上运行。

此外，还可以使用 OpenSSL 创建证书或从受信任的 CA 获取证书，再上传它们。有关详细信息，请参阅上传内部证书和内部 CA 证书。

有关使用这些证书的功能的信息，请参阅功能使用的证书类型。

Note 新的自签名证书生成的有效期为 5 年。请务必在证书过期前进行更换。

Warning 升级具有自签名证书的设备可能会遇到问题；有关详细信息，请参阅检测到新证书。

操作步骤

此程序可通过在向导中输入相应的证书字段值来生成自签名证书。如果要通过上传证书文件来创建内部或内部 CA 证书，请参阅上传内部和内部 CA 证书。上传内部证书和内部 CA 证书, on page 136

要生成自签名证书，请执行以下程序：

Procedure

步骤 1 执行以下操作之一：

- 在对象页面中创建证书对象：
  a. 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
  b. 点击加号按钮，然后选择 FTD 证书。 >

- 将新证书对象添加到策略时，点击创建新对象。

步骤 2 键入证书的**名称**。该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 3 在步骤 1 中，选择内部证书或内部 CA。

步骤 4 在步骤 2 中，选择自签名以在此步骤中创建自签名证书。

步骤 5 为证书主题和颁发者信息至少配置以下一项。

- 国家/地区 (Country [C]) - 从下拉列表中选择国家/地区代码。
- 州或省 (ST) (State or Province [ST]) - 证书中包括的州或省。
- 地区或城市 (Locality or City) (L) - 证书中包括的地区，例如城市名称。
- 组织 (O) (Organization [O]) - 要包含在证书中的组织或公司名称。
- 组织单位（部门）(Organizational Unit [Department]) (OU) - 证书中包含的组织单位名称（例如部门名称）。
- 公用名 (CN)(Common Name [CN]) - 要包含在证书中的 X.500 公用名。它们可能是设备、网站或其他文本字符串的名称。通常需要有此元素，才能成功进行连接。例如，用于远程访问 VPN 的内部证书中必须包括 CN。

步骤 6 点击**添加**。

配置 IPsec 提议

IPsec 是设置 VPN 的最安全方法之一。IPsec 在 IP 数据包级别提供数据加密，提供一种基于标准的强大的安全解决方案。使用 IPsec，数据通过隧道在公共网络上传输。隧道是两个对等体之间安全的逻辑通信路径。进入 IPsec 隧道的流量由称为转换集的安全协议和算法组合保护。在 IPsec 安全关联 (SA) 协商期间，对等体搜索在两个对等体处相同的转换集。

根据 IKE 版本（IKEv1 或 IKEv2），存在不同的 IPsec 提议对象：

- 当创建 IKEv1 IPsec 提议时，可以选择 IPsec 运行的模式，并定义所需的加密和身份验证类型。您可以为算法选择单一选项。如果要在 VPN 中支持多个组合，请创建和选择多个 IKEv1 IPsec 提议对象。
- 当创建 IKEv2 IPsec 提议时，可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序，并与对等体进行协商，直到找到匹配。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

Note 我们建议对 IPsec 隧道使用加密和身份验证。

以下主题介绍如何为每个 IKE 版本配置 IPsec 提议：

- 管理 IKEv1 IPsec 提议对象
- 管理 IKEv2 IPsec 提议对象

管理 IKEv1 IPsec 提议对象

IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。IKEv1 和 IKEv2 有单独的对象。目前， Cisco Defense Orchestrator (CDO) 支持 IKEv1 IPsec 提议对象。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

Note 我们建议对 IPsec 隧道使用加密和身份验证。

Related Topics

创建或编辑 IKEv1 IPsec 提议对象 ， 第 433 页

创建或编辑 IKEv1 IPsec 提议对象

有几个预定义的IKEv1 IPsec提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑站点间 VPN 连接中的 IKEv1 IPsec 设置时，点击对象列表中所示的**创建新 IKEv1 提议 (Create New IKEv1 Proposal)** 链接来创建 IKEv1 IPsec 提议对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FTD > IKEv1 IPsec 提议 (IKEv1 IPsec Proposal)** 以创建新对象。
- 在对象页面中，选择要编辑的IPsec方案，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

步骤 3 为新对象输入**对象名称**。

步骤 4 选择 IKEv1 IPsec 提议对象的运行模式。

- **隧道**模式会封装整个 IP 数据包。IPSec 报头被添加到原始 IP 报头和新的 IP 报头之间。这是默认值。当防火墙对出入位于防火墙后的主机的流量进行保护时，请使用隧道模式。在通过不可

信网络（例如互联网）连接的两个防火墙（或其他安全网关）之间，通常采用隧道模式实施常规 IPSec。

- **传输**模式只封装 IP 数据包的上层协议。IPSec 报头被插入到 IP 报头和上层协议报头（例如 TCP）之间。传输模式要求源和目的主机都支持 IPSec，并且只有在隧道的目的对等体是 IP 数据包的最终目的时才可使用。通常只有在保护第 2 层或第 3 层隧道协议（例如 GRE、L2TP 和 DLSW）时，才会使用传输模式。

步骤 5 选择**加密 (Encryption)**提议的（封装安全协议加密）算法。有关选项的说明，请参阅决定使用哪个加密算法, on page 421。

步骤 6 选择要用于身份验证的 **ESP 散列 (ESP Hash)** 或完整性算法。有关选项的说明，请参阅决定使用哪些散列算法, on page 421。

步骤 7 点击**添加**。

管理 IKEv2 IPsec 提议对象

IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。

当创建 IKEv2 IPsec 提议时，可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序，并与对等体进行协商，直到找到匹配。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

Related Topics

创建或编辑 IKEv2 IPsec 提议对象 ，第 434 页

创建或编辑 IKEv2 IPsec 提议对象

有几个预定义的IKEv2 IPsec提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑 VPN 连接中的 IKEv2 IPsec 设置时，点击对象列表中所示的创建新 IPsec 提议链接来创建 IKEv2 IPsec 提议对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FTD > IKEv2 IPsec 提议 (IKEv2 IPsec Proposal)** 以创建新对象。
- 在对象页面中，选择要编辑的IPsec方案，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

步骤 3 为新对象输入**对象名称**。

步骤 4 配置 IKEv2 IPsec 方案对象：

- **加密** - 此提议的封装安全协议 (ESP) 加密算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪个加密算法, on page 421。
- **完整性散列** - 要用于身份验证的散列或完整性算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪些散列算法, on page 421。

步骤 5 点击**添加**。

配置全局 IKE 策略

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。

IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用提议。IKE 提议是一组两个对等体用于保护其之间的协商的算法。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数用于保护后续 IKE 协商。

IKE 策略对象为这些协商定义 IKE 提议。您启用的对象是对等体协商 VPN 连接时使用的对象：不能为每个连接指定不同的 IKE 策略。每个对象的相对优先级确定首先尝试这些策略中的哪一个，数字越小优先级越高。如果协商无法找到两个对等体全都支持的策略，则不建立连接。

要定义全局 IKE 策略，需要为每个 IKE 版本选择启用哪些对象。如果预定义的对象不能满足您的要求，请创建新的策略来执行您的安全策略。

以下步骤说明如何通过“对象”(Objects) 页面配置全局策略。在编辑 VPN 连接时，您还可以点击 IKE 策略设置的编辑，来启用、禁用和创建策略。

以下主题介绍如何为每个 IKE 策略版本配置 IPsec 提议：

- 管理 IKEv1 策略
- 管理 IKEv2 策略

管理 IKEv1 策略

介绍如何创建和编辑 IKEv1 策略。

关于 IKEv1 策略

互联网密钥交换 (IKE) 版本 1 策略对象包含定义 VPN 连接时 IKEv1 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义 IKEv1 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

Related Topics

创建或编辑 IKEv1 策略，第 429 页

创建或编辑 IKEv1 策略

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。您还可以点击对象列表中所示的**创建新 IKE 策略 (Create New IKEv1 Policy)** 链接，以便在站点间 VPN 连接中编辑 IKEv1 设置时创建 IKEv1 策略对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FTD > IKEv1 Policy** 策略以创建新的 IKEv1 策略。
- 在对象页面中，选择要编辑的 IKEv1 策略，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

步骤 3 输入**对象名称**，最多 128 个字符。

步骤 4 配置 IKEv1 属性。

- **优先级 (Priority)** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **加密** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。有关选项的说明，请参阅“决定使用哪种加密算法”。
- **Diffie-Hellman 组** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。有关选项的解释，请看“决定要使用的 Diffie-Hellman 模数组”。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。

- **身份验证** - 在两个对等体之间使用的身份验证方法。有关详细信息，请参阅确定使用哪种身份验证方法, on page 423。
  - **预共享密钥** - 使用在每个设备上定义的预共享密钥。在身份验证阶段，此类密钥允许密钥在两个对等体之间共享并由 IKE 使用。如果未使用同一预共享密钥配置对等体，则无法建立 IKE SA。
  - **证书** - 使用对等体的设备身份证书来识别彼此。必须通过在证书颁发机构中注册每个对等体来获取这些证书。还须上传用于签署每个对等体的身份证书的受信任 CA 根证书和中间 CA 证书。对等体可以注册到相同或不同的 CA 中。对于任一对等体，都不能使用自签证书。
- **散列** - 用于创建消息摘要的散列算法，以确保消息的完整性。有关选项的说明，请参阅VPN 中使用的加密和散列算法, on page 420。

步骤 5 点击**添加**。

管理 IKEv2 策略

介绍如何创建和编辑 IKEv2 策略。

关于 IKEv2 策略

互联网密钥交换 (IKE) 版本 2 策略对象包含定义 VPN 连接时 IKEv2 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv2 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

Related Topics

创建或编辑 IKEv2 策略，第 430 页

创建或编辑 IKEv2 策略

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。您还可以点击对象列表中所示的 **创建新的 IKE 策略** 链接，以便在站点间 VPN 连接中编辑 IKEv1 设置时创建 IKEv1 策略对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FTD > IKEv2 策略 (IKEv2 Policy)** 以创建新的 IKEv2 策略。
- 在对象页面中，选择要编辑的 IKEv2 策略，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

步骤 3 输入**对象名称 (object name)**，最多 128 个字符。

步骤 4 配置 IKEv2 属性。

- **优先级 (Priority)** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **状态 (State)** - IKE 策略是启用还是禁用状态。点击开关以更改状态。在 IKE 协商期间仅使用启用的策略。
- **加密** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。选择要允许的所有算法，但不能在同一策略中同时包括混合模式 (AES-GCM) 和正常模式选项。（正常模式要求选择完整性散列，而混合模式禁止选择单独的完整性散列。) 系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪个加密算法, on page 421。
- **Diffie-Hellman 组** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。选择要允许的所有算法。系统与对等体协商，从最强到最弱组，直到达成匹配。有关选项的说明，请参阅决定要使用的 Diffie-Hellman 模数组, on page 422。
- **完整性散列** - 用于创建消息摘要的散列算法的完整性部分，用于确保消息完整性。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。完整性散列不与 AES-GCM 加密选项一起使用。有关选项的说明，请参阅VPN 中使用的加密和散列算法, on page 420。
- **伪随机函数 (PRF) 散列 (Pseudo-Random Function [PRF] Hash)** - 散列算法中用作派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法的伪随机函数 (PRF) 部分。在 IKEv1 中，完整性和 PRF 算法不分开，但在 IKEv2 中，可以为这些元素指定不同的算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅VPN 中使用的加密和散列算法, on page 420。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。

步骤 5 点击**添加**。

RA VPN 对象

安全区域对象

安全区是一组接口。区域将网络划分成网段，帮助您管理流量以及对流量进行分类。您可以定义多个区域，但一个给定接口只能位于一个区域中。

Firepower 系统会在初始配置期间创建以下区域，这些区域显示在 Defense Orchestrator 的对象页面中。您可以编辑区域以添加或移除接口；如果不再使用这些区域，也可以删除它们。

- **inside_zone** - 包括内部接口。此区域用于表示内部网络。
- **outside_zone** - 包括外部接口。此区域用于表示在您控制之外的网络，例如互联网。

通常，按接口在网络中扮演的角色对它们分组。例如，可将连接至互联网的接口放在 **outside_zone** 安全区，并将内部网络的所有接口放在 **inside_zone** 安全区。然后，可以对来自外部区域和传至内部区域的流量应用访问控制规则。

在创建区域之前，请考虑要应用至网络的访问规则和其他策略。例如，无需将所有内部接口都放到同一个区域。如果您有 4 个内部网络，并希望将其中一个与另外三个区别对待，则可以创建两个区域（而不是一个区域）。如果有一个接口需允许外部访问公共 Web 服务器，您可能希望对该接口使用单独的区域。

相关信息：

- 创建或编辑 Firepower 安全区域对象
- 将 Firepower 接口分配给安全区域
- 删除对象

创建或编辑 Firepower 安全区域对象

安全区是一组接口。区域将网络划分成网段，帮助您管理流量以及对流量进行分类。您可以定义多个区域，但一个给定接口只能位于一个区域中。有关详细信息，请参阅安全区域对象。

安全区域对象不与设备关联，除非在该设备的规则中使用该对象。

创建安全区域对象

要创建安全区域对象，请按照以下说明操作：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮  ，然后选择 **FTD** > **安全区域 (Security Zone)** 以创建对象。

步骤 3 为对象命名，也可输入说明（可选）。

步骤 4 选择要加入安全区域的的接口。

步骤 5 点击**添加**。

编辑安全区域对象

自行激活设备后，您会发现至少有两个安全区域，一个是 inside_zone，另一个是 outside_zone。FDM 管理可以编辑或删除这些区域。要编辑任何安全区域对象，请按照以下说明操作：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects)** > **FDM 对象 (FDM Objects)**。

步骤 2 查找要编辑的对象：

- 如果您知道对象的名称，则可以在“对象”页面中进行搜索：
  - 按安全区域过滤列表。
  - 在搜索字段中输入对象名称。
  - 选择对象。
- 如果您知道对象与设备关联，则可以从“资产”页面开始搜索。
  - 在导航窗格中，点击**清单 (Inventory)**。
  - 点击**设备**选项卡。
  - 点击相应的选项卡。
  - 使用设备过滤器和搜索栏查找您的设备。过滤器, on page 90搜索, on page 93
  - 选择设备。
  - 在右侧的“管理”(Management) 窗格中，点击  **对象 (Objects)**。
  - 使用对象过滤器和搜索栏查找要查找的对象。 

Note 如果您创建的安全区域对象未与设备策略中的规则关联，则该对象将被视为“未关联”，您将不会在设备的搜索结果中看到该对象。

步骤 3 选择对象。

步骤 4 点击右侧“操作”(Actions) 窗格中的**编辑**图标  。

步骤 5 编辑对象的任何属性后。点击**保存 (Save)**。

步骤 6 点击保存后，您会收到一条消息，说明这些更改将如何影响其他设备。点击**确认 (Confirm)** 以保存更改或点击取消。

服务对象

FirePOWER 服务对象

FTD 服务对象、服务组和端口组是包含被视为 IP 协议簇一部分的协议或端口的可重用组件。

FTD 服务组是服务对象的集合。服务组可能包含一个或多个协议的对象。您可以在安全策略中使用这些对象和组来定义网络流量匹配条件，例如使用访问规则来允许流量传送至特定 TCP 端口。该系统中包括多个针对通用服务的预定义对象。您可以使用策略中的这些对象；但无法编辑或删除系统定义的对象。

Firepower 设备管理器和 Firepower 管理中心将服务对象称为端口对象以及服务组和端口组。

有关详细信息，请参阅创建和编辑 Firepower 服务对象。

协议对象

协议对象是一种包含不太常用或传统协议的服务对象。协议对象由名称和协议编号来标识。CDO 可识别 ASA 和 Firepower（FDM 管理 设备）配置中的这些对象，并为其提供自己的“协议”过滤器，以便您可以轻松找到它们。

有关详细信息，请参阅创建和编辑 Firepower 服务对象。

ICMP 对象

互联网控制消息协议 (ICMP) 对象是专门用于 ICMP 和 IPv6-ICMP 消息的服务对象。当 ASA 和 Firepower配置中的这些设备已载入时，CDO 会识别这些对象，并且CDO 会为其提供自己的“ICMP”过滤器，以便您轻松找到这些对象。

使用 CDO，您可以从 ASA 配置中重命名或删除 ICMP 对象。您可以使用 CDO 在 Firepower 配置中创建、更新和删除 ICMP 和 ICMPv6 对象。

Note 对于 ICMPv6 协议，AWS 不支持选择特定参数。仅支持允许所有 ICMPv6 消息的规则。

有关详细信息，请参阅创建和编辑 Firepower 服务对象。

相关信息：

- 删除对象, on page 117

创建和编辑 Firepower 服务对象

要创建 Firepower 服务对象，请执行以下步骤：

防火墙设备管理器 (FDM 管理) 服务对象是可重用组件，可指定 TCP/IP 协议和端口。防火墙设备管理器、本地防火墙管理中心 和 云交付的防火墙管理中心 将这些对象称为“端口对象”。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击右侧的蓝色按钮  以创建对象，然后选择 **FTD** > **服务 (Service)**。

步骤 3 输入对象名称和说明。

步骤 4 选择**创建服务对象 (Create a service object)**。

步骤 5 点击**服务类型 (Service Type)** 按钮，然后选择要为其创建对象的协议。

步骤 6 按如下方式配置协议：

- **TCP**、 **UDP**
  - 选择 **eq**，然后输入端口号或协议名称。例如，您可以输入 80 作为端口号或 HTTP 作为协议名称。
  - 您还可以选择**范围**，然后输入端口号范围，例如 **1 65535**（以涵盖所有端口）。
- **ICMP**、 **IPv6-ICMP**-选择 ICMP **类型**。选择 **Any** 类型可应用于所有 ICMP 消息。有关类型和代码的信息，请参阅以下页面：
  - ICMP-http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - ICMPv6-http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- **其他 (Other)** - 选择所需协议。

步骤 7 点击**添加 (Add)**。

步骤 8 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

创建 Firepower 服务组

服务组可以由代表一个或多个协议的一个或多个服务对象组成。需要先创建服务对象，然后才能将其添加到组。Firepower 设备管理器和 Firepower 管理中心将这些对象称为“端口对象”。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击右侧的蓝色按钮  以创建对象，然后选择 **FTD > 服务 (Service)**。

步骤 3 输入对象名称和说明。

步骤 4 选择**创建服务组 (Create a service group)**。

步骤 5 通过点击添加对象 (Add Object) 将对象添加到组。

- 点击创建以创建新对象，就像上面创建 Firepower 服务对象中的操作一样。创建和编辑 Firepower 服务对象, on page 150
- 点击选择 (Choose) 以将现有服务对象添加到组。重复此步骤以添加更多对象。

步骤 6 将服务对象添加到服务组后，点击添加。

步骤 7 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

编辑 Firepower 服务对象或服务组

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 过滤对象以查找要编辑的对象，然后在对象表中选择该对象。

步骤 3 在“操作”(Actions) 窗格中，点击**编辑 (Edit)**  。

步骤 4 以在上述过程中创建值的相同方式编辑对话框中的值。

步骤 5 点击**保存 (Save)**。

步骤 6 CDO 显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

步骤 7 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

安全组标记组

安全组标记

关于安全组标记

如果使用思科身份服务引擎 (ISE) 定义并使用**安全组标记** (SGT) 来对 Cisco TrustSec 网络中的流量进行分类，则可以编写使用 SGT 作为匹配条件的访问控制规则。因此，可以基于安全组成员身份阻止或允许访问，而不是使用 IP 地址。

在 ISE 中，您可以创建 SGT，并将主机或网络 IP 地址分配至各标记。如果您将 SGT 分配给用户帐户，SGT 就会被分配给用户流量。将 FDM 管理 设备配置为连接到 ISE 服务器并创建 SGT 后，您可

以在 思科防御协调器 中创建 SGT 组并围绕它们构建访问控制规则。请注意，您必须先配置 ISE 的 SGT 交换协议 (SXP) 映射，然后才能将 SGT 关联到 FDM 管理 设备。有关详细信息，请参阅您当前运行的版本的《思科身份服务引擎管理员指南》中的**安全组标记交换协议**。

FDM 管理 设备评估 SGT 作为访问控制规则的流量匹配条件时，会使用以下优先级：

1. 数据包中定义的源 SGT（如有）。使用此技术无法进行目的地匹配。对于数据包中的 SGT，必须配置网络中的交换机和路由器以添加它们。有关如何实施此方法的信息，请参阅 ISE 文档。
2. 分配给用户会话的 SGT，从 ISE 会话目录下载。您需要启用此选项才能侦听此类 SGT 匹配的会话目录信息，但是，当您首次创建 ISE 身份源时，此选项会默认打开。SGT 可以与源或目标相匹配。尽管非必需，但您通常还会使用 ISE 身份源和 AD 域来设置被动身份验证身份规则，以收集用户身份信息。
3. 使用 SXP 下载的 SGT-IP 地址映射。如果 IP 地址在 SGT 范围内，则流量与使用 SGT 的访问控制规则相匹配。SGT 可以与源或目标相匹配。

Note 您无法直接在访问控制规则中使用从 ISE 检索到的信息。相反，您需要创建引用已下载 SGT 信息的 SGT 组。您的 SGT 组可以引用多个 SGT，因此您可以在适当的情况下根据相关的标记集合应用策略。

版本支持

CDO 当前在运行 6.5 和更高版本的 FDM 管理 设备上支持 SGT 和 SGT 组。FDM 管理 设备允许您在版本 6.5 及更高版本中配置并连接到 ISE 服务器，但在 6.7 之前版本中不支持在 UI 中配置 SGT。

从 FDM 管理 UI 中，这意味着运行版本 6.5 或更高版本的 FDM 管理 设备可以下载 SGT 的 SXP 映射，但不能手动添加到对象或访问控制规则。要更改运行版本 6.5 或版本 6.6 的设备的 SGT，您必须使用 ISE UI。但是，如果运行版本 6.5 的设备已被载入 思科防御协调器，则可以查看与设备关联的当前 SGT 并创建 SGT 组。

CDO 中的 SGT

安全组标记

SGT 在 CDO 中为只读。您无法在 CDO 中创建或编辑 SGT。要创建 SGT，请参阅当前运行版本的《思科身份服务引擎管理员指南》。

SGT 组

Note FDM 管理 设备将 SGT 组称作 SGT 动态对象。在 CDO 中，这些标签列表当前被称作 SGT 组。您可以在 CDO 中创建 SGT 组，而无需参考 FDM 管理 设备或 ISE UI。

使用 SGT 组可以根据 ISE 分配的 SGT 来识别源或目标地址。然后，可以将访问控制规则中的对象用于定义流量匹配条件。您无法直接在访问控制规则中使用从 ISE 检索到的信息。相反，您需要创建引用已下载 SGT 信息的 SGT 组。

您的 SGT 组可以引用多个 SGT，因此您可以在适当的情况下根据相关的标记集合应用策略。

要在 CDO 中创建 SGT 组，必须至少已经配置一个 SGT，并为要使用的设备的 FDM 管理 控制台配置来自 ISE 服务器的 SGT 映射。请注意，如果多个 FDM 管理 设备与同一 ISE 服务器关联，则可以将 SGT 或 SGT 组应用于多个设备。如果设备未与 ISE 服务器关联，则不能在访问控制规则中包含 SGT 对象，也不能将 SGT 组应用于该设备配置。

规则中的 SGT 组

SGT 组可被添加到访问控制规则；它们会显示为源或目标网络对象。有关网络如何在规则中工作的详细信息，请参阅 FDM 管理 访问控制规则中的源和目标条件。

您可以从“对象”(Objects) 页面创建 SGT 组。有关详细信息，请参阅创建 SGT 组, on page 153。

创建 SGT 组

要创建可用于访问控制规则的 SGT 组，请使用以下程序：

Before you begin

在创建安全组标记 (SGT) 组之前，必须配置以下配置或环境：

- FDM 管理 设备必须至少运行版本 6.5。
- 必须配置 ISE 身份源以订用 SXP 映射并启用部署更改。要管理 SXP 映射，请参阅所用版本（版本 6.7 及更高版本）的 Firepower 设备管理器配置指南中的**在 ISE 中配置安全组和 SXP 发布**。
- 所有 SGT 都必须在 ISE 中创建。要创建 SGT，请参阅当前运行版本的《思科身份服务引擎配置指南》。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮  以创建新的对象。

步骤 3 点击 **FTD > 网络 (Network)**。

步骤 4 输入 **对象名称 (Object Name)**。

步骤 5 （可选）添加说明。

步骤 6 点击 **SGT** 并使用下拉菜单选中要包含在组中的所有适用 SGT。您可以按 SGT 名称对列表进行排序。

步骤 7 点击**保存 (Save)**。

Note 您无法在 CDO 中创建或编辑 SGT，只能在 SGT 组中添加或删除它们。要创建或编辑 SGT，请参阅当前运行版本的《思科身份服务引擎配置指南》。

编辑 SGT 组

要编辑 SGT 组，请使用以下程序：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到您要编辑的 SGT 组。

步骤 3 选择 SGT 组，然后点击**操作 (Actions)** 窗格中的编辑图标  。

步骤 4 修改 SGT 组。编辑与该组关联的名称、说明或 SGT。

步骤 5 点击**保存 (Save)**。

Note 您无法在 CDO 中创建或编辑 SGT，只能在 SGT 组中添加或删除它们。要创建或编辑 SGT，请参阅当前运行版本的《思科身份服务引擎配置指南》。

将 SGT 组添加到访问控制规则

要将 SGT 组添加到访问控制规则，请使用以下程序：

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 FTD 选项卡，然后选择要向其添加 SGT 组的设备。

步骤 4 在**管理 (Management)** 窗格中，选择**策略 (Policy)**。

步骤 5 点击源或目标对象的蓝色加号按钮，然后选择 SGT 组。 

步骤 6 使用对象过滤器和搜索字段找到您要编辑的 SGT 组。

步骤 7 点击**保存 (Save)**。

步骤 8 预览和部署所有设备的配置更改。

Note 如果需要创建其他 SGT 组，请点击创建新对象。填写创建 FTD SGT 组并将 SGT 组添加到规则中提到的必填信息。创建 SGT 组, on page 153

系统日志服务器对象

FDM管理设备用来存储事件的容量有限。要尽可能提高事件存储量，您可以配置外部服务器。系统日志 (syslog) 服务器对象标识可接收面向连接的消息或诊断 syslog 消息的服务器。如果已为日志收集和分析设置一台系统日志服务器，您可以使用思科防御协调器来创建对象以进行定义并在相关策略中使用这些对象。

创建和编辑系统日志服务器对象

要创建新的系统日志服务器对象，请执行以下步骤：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击**创建对象 (Create Object)** 按钮  。

步骤 3 选择 FDM 管理 设备对象类型下方的**系统日志服务器 (Syslog Server)**

步骤 4 配置系统日志服务器对象属性：

- **IP 地址** - 输入系统日志服务器的 IP 地址。
- **协议类型 (Protocol Type)** - 选择系统日志服务器用于接收消息的协议。如果您选择 TCP，系统可以识别何时系统日志服务器不可用，并停止发送事件，直至服务器再次可用。
- **端口号 (Port Number)** - 输入要用于系统日志的有效端口号。如果系统日志服务器使用默认端口，请输入 514 作为默认 UDP 端口或 1470 作为默认 TCP 端口。如果服务器不使用默认端口，请输入正确的端口号。端口范围必须介于 1025 至 65535 之间。
- **选择接口**-选择应使用哪个接口发送诊断系统日志消息。连接和入侵事件始终使用管理接口。接口选择决定与系统日志消息关联的 IP 地址。请注意，您只能选择下面列出的选项**之一**。不能同时选择两者。选择以下选项之一：
  - **数据接口** - 选择用于诊断系统日志消息的数据接口。从生成列表中选择一个接口。如果可以通过网桥组成员接口访问该服务器，请选择该网桥组接口 (BVI)。如果通过诊断接口（物理管理接口）访问，我们建议您选择管理接口，而不是此选项。您不能选择被动接口。对于连接和入侵系统日志消息，源 IP 地址是管理接口的地址；如果您通过数据接口进行路由，则是网关接口的地址。
  - **管理接口** - 对所有类型的系统日志消息使用虚拟管理接口。源 IP 地址是管理接口的地址；如果您通过数据接口进行路由，则是网关接口的地址。

步骤 5 点击添加 **(Add)**。

步骤 6 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

编辑系统日志服务器对象

要编辑现有的系统日志服务器对象，请执行以下步骤：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 找到所需的系统日志服务器对象并选择它。您可以按系统日志服务器对象类型过滤对象列表。

步骤 3 在“操作”(Actions) 窗格中，点击**编辑 (Edit)**。

步骤 4 进行所需的编辑，然后点击**保存 (Save)**。

步骤 5 确认您所做的更改。

步骤 6 立即 预览和部署所有设备的配置更改 您所做的更改，或等待并一次部署多个更改。

相关信息：

- 删除对象

为安全日志记录分析 (SaaS) 创建系统日志服务器对象

使用要向其发送事件的安全事件连接器 (SEC) 的 IP 地址、TCP 端口或 UDP 端口创建系统日志服务器对象。您将为已载入租户的每个 SEC 创建一个系统日志对象，但您只能将来自一个规则的事件发送到一个代表一个 SEC 的系统日志对象。

前提条件

此任务是更大工作流程的一部分。开始前，请参阅 为 FDM 管理 设备实施安全日志记录分析 (SaaS), on page 594 。

操作步骤

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击**创建对象 (Create Object)** 按钮  。

步骤 3 选择 FDM 管理 设备对象类型下方的**系统日志服务器 (Syslog Server)**。

步骤 4 配置系统日志服务器对象属性。要查找 SEC 的这些属性，请从 CDO 菜单中选择**管理 (Admin)** > **安全连接器 (Secure Connectors)**。然后，选择要为其配置系统日志对象的安全事件连接器，并查看右侧的“详细信息”窗格。

- **IP 地址 (IP Address)** - 输入 SEC 的 IP 地址。
- 协议类型 - 选择 TCP 或 UDP。
- 端口号 - 如果您选择了 TCP，请输入端口 10125；如果您选择了 UDP，请输入 10025。
- 选择接口 - 选择配置用于访问 SEC 的接口。

Note FDM 管理 设备支持每个 IP 地址一个系统日志对象，因此您必须在使用 TCP 和 UDP 之间进行选择。

步骤 5 点击**添加 (Add)**。

What to do next

继续步骤 3 实施安全日志记录分析 (SaaS) 并通过安全事件连接器将事件发送到思科云的现有 CDO 客户工作流程。

URL 对象

URL 对象和 URL 组由 Firepower 设备使用。使用 URL 对象和组（统称为“URL 对象”）可定义 Web 请求的 URL 或 IP 地址。可以使用这些对象在访问控制策略中执行手动 URL 过滤，或在安全情报策略中进行阻止。URL 对象定义单个 URL 或 IP 地址，而 URL 组可以定义多个 URL 或地址。

准备工作

在创建 URL 对象时，请记住以下要点：

- 如果不包含路径（即 URL 中无 / 字符），则匹配仅基于服务器主机名。如果主机名位于 :// 分隔符之后，或在主机名中的任何点之后，则认为该主机名匹配。例如，ign.com 匹配 ign.com 和 www.ign.com，但不匹配 verisign.com。
- 如果包含一个或多个 / 字符，则整个 URL 字符串将用于子字符串匹配，其中包括服务器名称、路径和任何查询参数。但是，我们建议您不要使用手动URL过滤阻止或允许个别网页或部分网站，因为这样可能会重组服务器并将页面移至新路径。子字符串匹配还可能导致意外匹配，其中 URL 对象中包含的字符串也与非预期服务器上的路径或查询参数中的字符串匹配。
- 系统忽略加密协议（HTTP 与 HTTPS）。换句话说，如果阻止网站，系统将阻止发往该网站的 HTTP 和 HTTPS 流量，除非您使用一个应用条件指定特定协议。在创建 URL 对象时，您不需要指定创建对象时的协议。例如，使用 example.com 而不是 http://example.com。

- 如果您计划使用 URL 对象匹配访问控制规则中的 HTTPS 流量，请使用加密流量时所使用的公钥中的使用者公用名创建该对象。此外，系统会忽略使用者公用名中的子域，因此，不包括子域信息。例如，使用 example.com 而不是 www.example.com。

  但请注意，证书中的使用者公用名可能与网站的域名完全无关。例如，youtube.com 证书中的使用者公用名是 *.google.com（当然，这可能会随时更改）。如果使用 SSL 解密策略解密 HTTPS 流量以便 URL 过滤规则可用于解密策略，则可能获得更一致的结果。

注释 如果由于证书信息不再可用，浏览器恢复 TLS 会话，则 URL 对象将不匹配 HTTPS 流量。因此，即使精心配置 URL 对象，也可能会得到不一致的 HTTPS 连接结果。

创建或编辑 FDM 管理 URL 对象

URL 对象是指定 URL 或 IP 地址的可重用组件。

要创建 URL 对象，请执行以下步骤：

Procedure

步骤 1 在左侧的 思科防御协调器 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击创建对象**创建对象 (Create Object)** > **FTD** > **URL**。

步骤 3 输入对象名称和说明。

步骤 4 选择**创建 URL 对象 (Create a URL object)**。

步骤 5 为对象输入特定 URL 或 IP 地址。

步骤 6 点击**添加**。

创建 Firepower URL 组

URL 组可以由表示一个或多个 URL 或 IP 地址的一个或多个 URL 对象组成。Firepower 设备管理器和 Firepower 管理中心也将这些对象称为“URL 对象”。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击创建对象**创建对象 (Create Object)** > **FTD** > **URL**。

步骤 3 输入对象名称和说明。

步骤 4 选择**创建 URL 组 (Create a URL group)**。

步骤 5 通过点击**添加对象 (Add Object)**，选择一个对象，然后点击**选择 (Select)**，添加现有对象。重复此步骤以添加更多对象。

步骤 6 将 URL 对象添加到 URL 组后，点击**添加**。

编辑 Firepower URL 对象或 URL 组

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

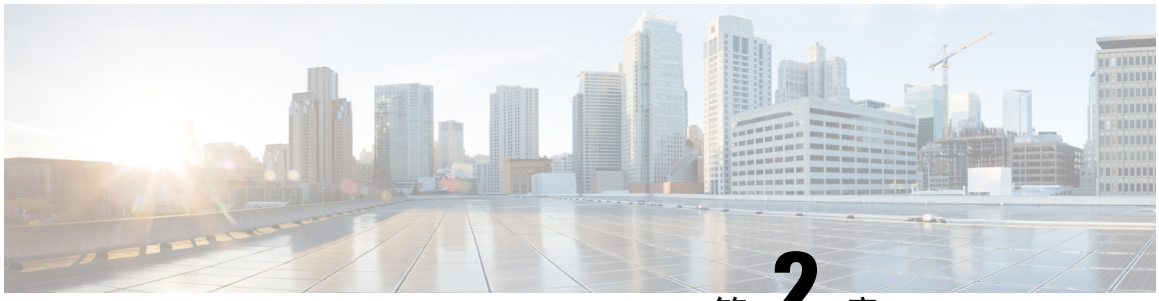
步骤 2 过滤对象以查找要编辑的对象，然后在对象表中选择该对象。

步骤 3 在详细信息窗格中，点击以进行编辑。

步骤 4 以在上述过程中创建值的相同方式编辑对话框中的值。

步骤 5 点击**保存 (Save)**。

步骤 6 CDO 显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。



第 2 章

载入设备和服务

您可以将实时设备和模型设备载入 CDO。模型设备是您可以使用 CDO 查看和编辑的已上传配置文件。

大多数实时设备和服务都需要开放的 HTTPS 连接，以便安全设备连接器可以将 CDO 连接到设备或服务。

有关 SDC 及其状态的详细信息，请参阅安全设备连接器 (SDC)，第 10 页。

本章涵盖以下部分：

载入 威胁防御 设备

Attention Firepower 设备管理器 (FDM) 支持和功能仅应要求提供。如果您的租户上尚未启用 防火墙设备管理器 支持，则无法管理或部署到 FDM 管理 设备。向支持团队发送请求以启用此平台。通过 TAC 打开提交支持请求, on page 752

有多种方法可以载入 威胁防御 设备。我们建议使用注册密钥方法。

如果您在载入设备时遇到问题，请参阅对使用序列号载入 FDM 管理 设备进行故障排除, on page 694或由于许可证不足而失败 , on page 690了解详细信息。

将 威胁防御 设备载入 云交付的防火墙管理中心

您可以将运行版本 7.2 及更高版本的 威胁防御 设备载入 云交付的防火墙管理中心。有关详细信息，请参阅将 FTD 载入云交付的防火墙管理中心。

通过序列号载入 威胁防御 设备

此程序是对运行受支持软件版本的 Firepower 1000、Firepower 2100 或 Secure Firewall 3100 系列物理设备进行载入的简化方法。要载入设备，您需要设备的机箱序列号或PCA序列号，并确保将设备添加到可以访问互联网的网络中。

您可以将新出厂的设备或已配置的设备载入 CDO。

有关详细信息，请参阅 使用设备的序列号载入 FDM 管理 设备, on page 179。

使用注册密钥载入 威胁防御 设备。

建议使用注册密钥来载入 威胁防御 设备。如果使用 DHCP 为您的设备分配 IP 地址，这将非常有用。如果该 IP 地址由于某种原因发生变化，则您的 威胁防御 设备将保持连接到 CDO（如果您已使用注册密钥载入设备）。

- 使用注册密钥载入 FDM 管理 设备运行软件版本 6.4 或 6.5, on page 171
- 使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+, on page 175

使用凭证载入 威胁防御 设备

您可以使用设备凭证和设备的外部、内部或管理接口的 IP 地址来载入 威胁防御 设备，具体取决于设备在网络中是如何配置的。要使用凭证载入设备，请参阅 使用用户名、密码和 IP 地址载入 FDM 管理 设备, on page 168。要使用接口地址来载入，请参阅本文后面的载入 威胁防御 设备。

CDO 需要通过 HTTPS 访问设备才能管理它。如何允许 HTTPS 访问设备要取决于您的设备在网络中是如何配置的，以及您是使用安全设备连接器 (SDC)还是云连接器来载入设备。

Note 如果您连接到 https://www.defenseorchestrator.eu 并且使用的软件版本 6.4，则必须使用此方法来载入 威胁防御 设备。您不能使用注册密钥方法。

使用设备凭证连接 CDO 到设备时，最佳做法是在网络中下载并部署安全设备连接器 (SDC)，以管理 CDO 和设备之间的通信。通常，这些设备不是基于边界的，没有公共 IP 地址，或者具有通往外部接口的开放端口。在使用凭证载入后，威胁防御 设备就可以使用 SDC 载入 CDO。

请注意，当使用 威胁防御 设备作为 VPN 连接的前端时，客户将无法使用外部接口来管理设备。

载入 威胁防御 集群

您可以在载入 CDO 之前载入已加入集群的 威胁防御 设备。集群允许您将多个防火墙 威胁防御 单元集合在一起，作为单个逻辑设备来提供全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。

请参阅 载入集群的 设备, on page 192。

载入的 FDM 管理 设备配置和必备条件

FDM 管理 设备管理

您只能载入由 Firepower 设备管理器 (FDM) 管理的 威胁防御 设备。由 Firepower 管理中心 管理的 威胁防御 设备无法由 云交付的防火墙管理中心 管理。

如果设备未配置为本地管理，则必须在载入设备之前切换到本地管理。请参阅《适用于 Firepower 设备管理器的 配置指南》的 **在本地管理和远程管理之间切换**一章。

许可

设备**必须**至少安装一个许可证才能载入到 CDO，但在某些情况下可以应用智能许可证。

载入方法	Firepower 设备管理器 软件版本	90 天评估许可证是否允许？	在载入之前，设备是否可以先获得智能许可？	在载入之前，设备是否可以先在思科云服务中注册？
凭证（用户名和密码）	全部	是	是	是
注册密钥	6.4 或 6.5	是	不行。请取消注册智能许可证，然后载入设备。	不适用
注册密钥	6.6 或更高版本	是	是	不行。请从思科云服务取消注册设备，然后载入设备。
低接触调配	6.7 或更高版本	是	是	是
通过序列号载入设备	6.7 或更高版本	是	是	是

请参阅思科 FirePOWER 系统功能许可证。

设备编址

最佳实践是使用静态地址来载入 FDM 管理 设备。如果设备的 IP 地址由 DHCP 分配，则最好使用 DDNS（动态域名系统）在设备的新 IP 地址更改时自动使用设备的域名条目进行更新。

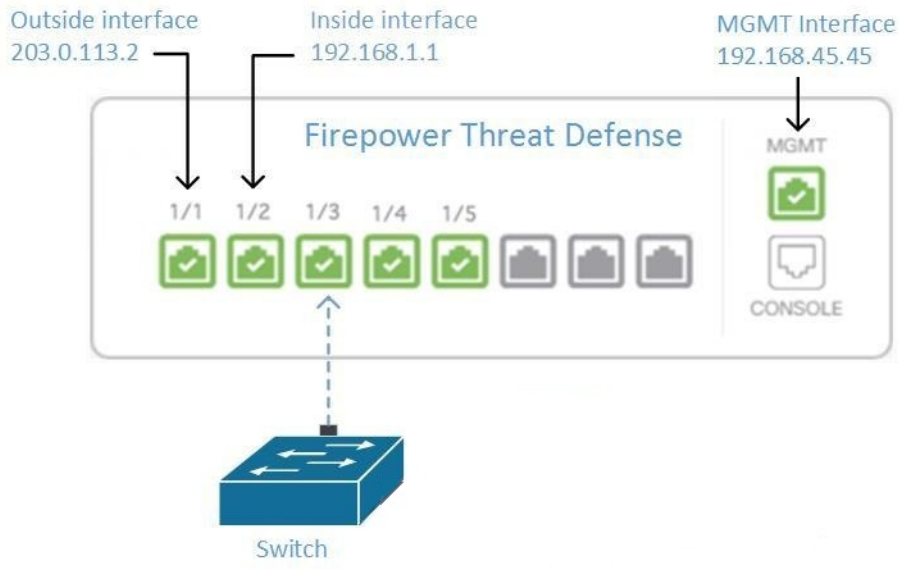
Note FDM 管理 设备本身不支持 DDNS；您必须配置自己的 DDNS。

Important 如果您的设备从 DHCP 服务器获取 IP 地址，并且您没有使用任何新 IP 地址更新 FDM 管理 设备域名条目的 DDNS 服务器，或者您的设备收到了新地址，您可以在 CDO 中更改设备的 IP 地址，然后再将设备批量重新连接到 CDO。更好的方法是使用注册密钥来载入设备。

从内部接口管理设备FDM 管理

如果为专用MGMT接口分配了在您的组织内不可路由的地址，则可能需要使用内部接口管理设备；例如，它可能只能从您的数据中心或实验中访问。FDM 管理

Figure 5: 接口地址



远程接入 VPN 要求

如果您使用 CDO 管理的设备将管理远程接入 VPN (RA VPN) 连接，则 CDO 必须使用内部接口管理设备。FDM 管理

后续操作：

继续，了解配置设备的程序。从内部接口管理设备FDM 管理, on page 3FDM 管理

从内部接口管理设备FDM 管理

此配置方法：

- 假定设备尚未自行激活。FDM 管理CDO
- 将数据接口配置为内部接口。
- 配置内部接口以接收 MGMT 流量 (HTTPS)。
- 允许云连接器的地址到达设备的内部接口。

Before you begin

在以下主题中查看此配置的前提条件：

- 从内部接口管理设备FDM 管理, on page 2
- 将 思科防御协调器 连接到托管设备, on page 11

Procedure

步骤 1 登录Firepower 设备管理器。

步骤 2 在系统设置菜单中，点击管理访问。

步骤 3 点击数据接口选项卡，然后点击创建数据接口。

a. 在接口字段中，从接口列表中选择预先命名为“内部”的接口。

b. 在协议字段中，选择 HTTPS（如果尚未选择）。

c. 在允许的网络 (Allowed Networks) 字段中，选择代表将允许访问设备内部地址的组织内部网络的网络对象。FDM 管理SDC 或云连接器的 IP 地址应在允许访问设备内部地址的地址中。

在接口地址图中，SDC 的 IP 地址 192.168.1.10 应该能够到达 192.168.1.1。#unique_67 unique_67_Connect_42_ftd-interf-addrss, on page 3

步骤 4 部署更改。您现在可以使用内部接口管理设备。

What to do next

如果您使用的是云连接器，该怎么办？

使用上述程序并添加以下步骤：

- 将外部接口 (203.0.113.2)“NAT”添加到内部接口 (192.168.1.1)。
- 在上述程序的步骤 3c 中，“允许的网络”是包含云连接器的公共 IP 地址的网络组对象。
- 添加创建访问控制规则的步骤，允许从云连接器的公共 IP 地址访问外部接口 (203.0.113.2)。

如果您是欧洲、中东或非洲 (EMEA) 的客户，并且连接到 ，则这些是云连接器的公共 IP 地址：CDOhttps://defenseorchestrator.eu/

- 35.157.12.126

- 35.157.12.15

如果您是美国的客户，并且连接到，云连接器的这些公共 IP 地址：CDOhttps://defenseorchestrator.com/

- 52.34.234.2
- 52.36.70.147

如果您是**亚太地区-日本-中国 (AJPC)** 地区的客户，并且您通过 https://www.apj.cdo.cisco.com/ 连接到 CDO，请允许来自以下 IP 地址的入站访问：

- 54.199.195.111
- 52.199.243.0

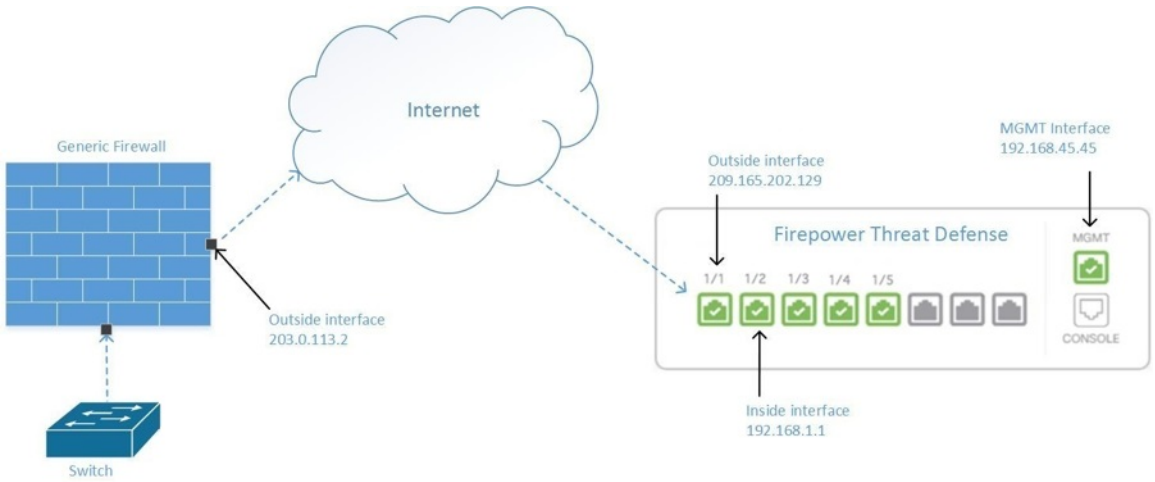
载入 FDM 管理 设备

推荐的自行激活设备的方法是使用注册令牌自行激活方法。FDM 管理CDO将内部接口配置为允许从云连接器对设备进行管理访问后，使用用户名和密码载入设备。FDM 管理FDM 管理有关详细信息，请参阅载入 威胁防御 设备。您将使用内部接口的 IP 地址进行连接。在上面的场景中，该地址是 192.168.1.1。

从外部接口管理设备FDM 管理

如果您有一个分配给分支机构的公共 IP 地址，并使用另一个位置的云连接器进行管理，则可能需要从外部接口管理设备。云交付的防火墙管理中心思科防御协调器

Figure 6: 外部接口上的设备管理



此配置并不意味着物理 MGMT 接口不再是设备的管理接口。如果您在设备所在的办公室，您将能够连接到 MGMT 接口的地址并直接管理设备。云交付的防火墙管理中心

远程接入 VPN 要求

如果您管理的设备将管理远程接入 VPN (RA VPN) 连接， 将无法使用外部接口管理设备。云交付的防火墙管理中心云交付的防火墙管理中心云交付的防火墙管理中心请参阅从内部接口管理设备。从内部接口管理设备FDM 管理

后续操作：

继续，了解配置设备的程序。管理设备的外部接口FDM 管理, on page 5云交付的防火墙管理中心

管理设备的外部接口FDM 管理

此配置方法：

1. 假定设备尚未自行激活。FDM 管理CDO
2. 将数据接口配置为外部接口。
3. 在外部接口上配置管理访问。
4. 允许云连接器的公共 IP 地址（通过防火墙进行 NAT 后）到达外部接口。

Before you begin

在以下主题中查看此配置的前提条件：

- 管理设备的外部接口FDM 管理, on page 5
- 将 思科防御协调器 连接到托管设备, on page 11

Procedure

步骤 1 登录Firepower 设备管理器。

步骤 2 在系统设置菜单中，点击管理访问。

步骤 3 点击数据接口选项卡，然后点击创建数据接口。

a. 在接口字段中，从接口列表中选择预先命名为“外部”的接口。

b. 在协议字段中，选择 HTTPS（如果尚未选择）。只需要 HTTPS 访问。CDO

c. 在允许的网络 (Allowed Networks) 字段中，创建一个主机网络对象，其中包含云连接器通过防火墙的 NAT 后面向公众的 IP 地址。

在从外部接口进行设备管理的网络图中，云连接器的 IP 地址 10.10.10.55 将通过 NAT 转换为 203.0.113.2。#unique_71 unique_71_Connect_42_ftd-mgmt-out-addrss, on page 5对于允许的网络，您将创建一个值为 203.0.113.2 的主机网络对象。

步骤 4 在中创建访问控制策略，允许从SDC或云连接器的公共IP地址到设备外部接口的管理流量(HTTPS)。Firepower 设备管理器FDM 管理在此场景中，源地址为 203.0.113.2，源协议为 HTTPS；目的地址为 209.165.202.129，协议为 HTTPS。

步骤 5 部署更改。您现在可以使用外部接口管理设备。

What to do next

如果您使用的是云连接器，该怎么办？

该过程非常相似，但有两点不同：

- 在上述程序的步骤 3c 中，“允许的网络”是包含云连接器的公共 IP 地址的网络组对象。
  - 如果您是欧洲、中东或非洲 (EMEA) 的客户，并且连接到，则这些是云连接器的公共 IP 地址：CDOhttps://defenseorchestrator.eu/
    - 35.157.12.126
    - 35.157.12.15
  - 如果您是美国的客户，并且连接到，则这些是云连接器的公共 IP 地址：CDOhttps://defenseorchestrator.com/
    - 52.34.234.2
    - 52.36.70.147
  - 如果您是**亚太地区-日本-中国 (AJPC)** 地区的客户，并且您通过 https://www.apj.cdo.cisco.com/ 连接到 CDO，请允许来自以下 IP 地址的入站访问：
    - 54.199.195.111
    - 52.199.243.0
- 在上述程序的第 4 步中，创建一个允许从云连接器的公共 IP 地址访问外部接口的访问控制规则。

注册令牌自行激活方法是将设备自行激活到的推荐方法。使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+, on page 175FDM 管理CDO将外部接口配置为允许从云连接器进行管理访问后，载入设备。FDM 管理您将使用外部接口的 IP 地址进行连接。在我们的场景中，该地址是 209.165.202.129。

将 FDM 管理 设备载入 CDO

使用以下程序按照以下方法将 FDM 管理 载入 CDO。

使用用户名、密码和 IP 地址载入 FDM 管理 设备

按照此程序仅使用设备凭证和设备的管理 IP 地址载入 FDM 管理 设备。这是载入 FDM 管理 设备最简单的方法。但是，建议使用使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+将 FDM 管理 设备载入 CDO。

Before you begin

Important 在将 FDM 管理 设备载入 思科防御协调器 之前，请阅读载入 威胁防御 设备和 将 思科防御协调器 连接到托管设备, on page 11。它们提供了载入设备所需的一般设备要求和载入必备条件。

- 使用凭证方法载入 FDM 管理 设备需要以下信息：
  - CDO 将用于连接到设备的设备凭证。
  - 用来管理设备的设备接口的 IP 地址。它可以是管理接口、内部接口或外部接口，具体取决于您的网络配置。
  - 设备必须由 Firepower 设备管理器 管理，并针对本地管理而配置，以便将其载入 CDO。无法由 Firepower 管理中心 管理。

Note 如果您连接到 https://www.defenseorchestrator.eu ，并且 FDM 管理 设备运行的是 6.4 版本的软件，则必须使用此方法。您只能载入运行 6.5 及更高版本软件的 FDM 管理 设备。

Procedure

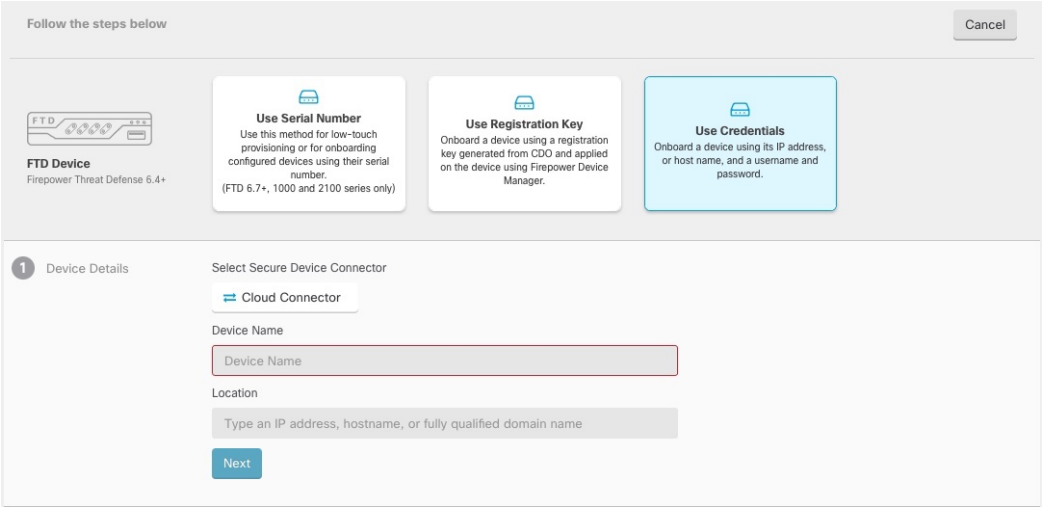
步骤 1 登录 CDO。

步骤 2 在导航窗格中，点击 **清单 (Inventory)** ，然后点击蓝色加号按钮  以便**载入**设备。

步骤 3 点击 **FTD**。

Important 在尝试载入 FDM 管理 设备时，CDO 会提示您阅读并接受 Secure Firewall Threat Defense 最终用户许可协议 (EULA)，这是面向租户的一次性活动。接受 EULA 后，CDO 不会再次提示您接受 EULA，除非 EULA 发生更改。

步骤 4 在载入向导中，点击**使用凭证 (Use Credentials)**。



步骤 5 在设备详细信息步骤中：

- 点击**安全设备连接器 (Secure Device Connector)** 按钮，然后选择网络中安装的安全设备连接器 (SDC)。如果您不想使用 SDC，CDO 可以使用云连接器连接到 FDM 管理 设备。您的选择取决于您如何将 思科防御协调器 连接到托管设备。
- 在**设备名称 (Device Name)** 字段中输入设备名称。它可以是设备的主机名或您选择的任何其他名称。
- 在**位置 (Location)** 字段中，输入设备的管理接口 IP 地址、主机名或设备的完全限定设备名称。默认端口为 443。

Important 如果您已有 SecureX 或思科威胁响应 (CTR) 账户，则需要合并 CDO 租户和 SecureX/CTR 账户，以便您的设备能够注册 SecureX。您的账户可以通过 SecureX 门户合并。有关说明，请参阅合并您的 CDO 和 SecureX 账户。在您的账户合并之前，您将无法在 SecureX 中查看设备的事件或受益于其他 SecureX 功能。

步骤 6 在**数据库更新**区域中，**立即执行安全更新并启用定期更新**默认启用。此选项立即触发安全更新并自动安排设备在每周一凌晨 2 点检查是否有额外更新。有关详细信息，请参阅更新 FDM 管理 设备安全数据库和安排安全数据库更新。

禁用此选项不会影响您通过 FDM 配置的以前计划的任何更新。

点击**下一步 (Next)**。

步骤 7 输入设备管理员的用户名和密码，然后点击**下一步 (Next)**。

步骤 8 如果设备的 Firepower 设备管理器 上有待处理的更改，您将收到通知，您可以恢复更改或登录管理器并部署待处理的更改。如果 Firepower 设备管理器 上没有待处理的更改，您将不会看到提示。

步骤 9 （可选）添加设备的标签。有关详细信息，请参阅标签和过滤。

使用注册密钥载入 FDM 管理 设备运行软件版本 6.4 或 6.5

此程序介绍了如何使用注册码载入 FDM 管理 设备。此方法是将 FDM 管理 设备载入到 思科防御协调器 的推荐方法，如果使用 DHCP 为您的 FDM 管理 设备分配 IP 地址，则此方法非常有用。如果该 IP 地址由于任何原因发生变化，则您的 FDM 管理 设备仍会连接到 CDO。此外，您的 FDM 管理 设备可以在您的局域网上有一个地址，只要它可以访问外部网络，就可以使用此方法载入 CDO。

Warning 如果您已有 SecureX 或思科威胁响应 (CTR) 账户，则需要合并 CDO 租户和 SecureX/CTR 账户，以便您的设备能够注册 SecureX。在您的账户合并之前，您将无法在 SecureX 中查看设备的事件或受益于其他 SecureX 功能。我们强烈建议在 SecureX 中创建 CDO 模块之前合并您的账户。您的账户可以通过 SecureX 门户合并。有关说明，请参阅合并账户。

载入之前

- 对于运行版本 6.4 的客户，仅美国区域 (defenseorchestrator.com) 支持此载入方法。
- 对于运行版本 6.4 并连接到 EU 区域 (defenseorchestrator.eu) 的客户，他们必须使用使用用户名、密码和 IP 地址载入 FDM 管理 设备。
- 运行版本 6.5 或更高版本并连接到美国、欧盟或 APJC 区域 (apj.cdo.cisco.com) 的客户可以使用此载入方法。
- 查看 将 思科防御协调器 连接到托管设备, on page 11 以了解将 CDO 连接到 FDM 管理 设备所需的网络要求。
- 请确保您的设备由 Firepower 设备管理器 管理，而不是由 Firepower 管理中心 管理。
- 运行版本 6.4 和 6.5 的设备在使用注册密钥载入之前，不得向思科智能软件管理器注册。您需要先取消注册这些 FDM 管理 设备的智能许可证，然后再将其载入 CDO。请参阅下面的“取消注册智能许可 防火墙设备管理器”。
- 设备可能正在使用 90 天的评估许可证。
- 登录 FDM 管理 设备并确保设备上没有等待处理的更改。
- 确保在您的 FDM 管理 设备上正确配置 DNS。
- 请确保在 FDM 管理 设备上正确配置时间服务。
- 请确保 FDM 管理 设备显示正确的日期和时间，否则载入将失败。

后续操作

执行以下两项操作之一：

- 从思科智能软件管理器取消注册您的 FDM 管理 设备（如果它已获得智能许可）。**您必须先从智能软件管理器取消注册该设备，然后再使用注册密钥将其载入 CDO**。请继续取消注册智能许可的 FDM 管理 设备, on page 172。

- 如果您的设备尚未获得智能许可，请继续使用注册密钥载入运行软件版本 6.4 或 6.5 的 FDM 管理 设备的程序, on page 173。

取消注册智能许可的 FDM 管理 设备

如果要载入的设备运行的是版本 6.4 或 6.5，并且已获得智能许可，则该设备可能已向思科智能软件管理器注册。**您必须先从智能软件管理器取消注册该设备，然后再使用注册密钥将其载入 CDO**。取消注销时，与设备关联的基本许可证和所有可选许可证将在您的虚拟帐户中释放。

注销设备后，该设备中的当前配置和策略将继续按原样运行，但无法进行或部署任何更改。

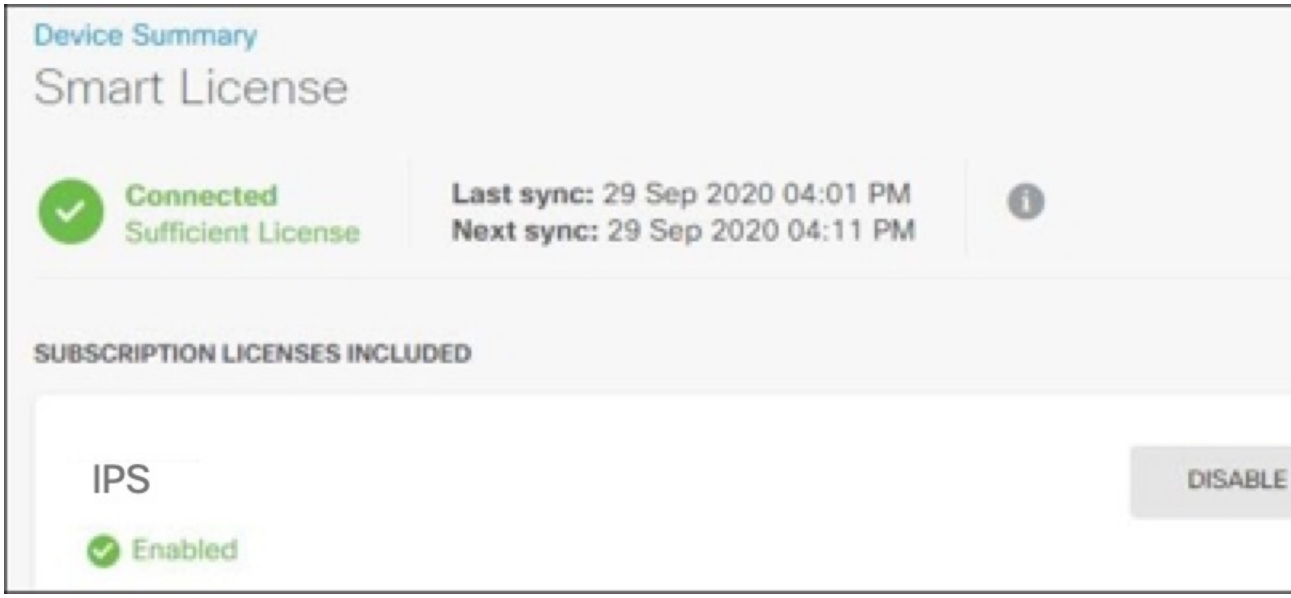
Procedure

步骤 1 使用 Firepower 设备管理器 登录设备。

步骤 2 点击上方选项卡中的设备图标。

步骤 3 点击**智能许可证 (Smart License)** 区域中的 **查看配置 (View Configuration)**。

步骤 4 点击**转到云服务 (Go to Cloud Services)** 齿轮菜单，然后选择**注销设备 (Unregister Device)**。



步骤 5 阅读警告并点击**取消注册 (Unregister)**，以取消注册该设备。

What to do next

如果您已取消注册以便将其载入 CDO，请继续使用注册密钥载入运行软件版本 6.4 或 6.5 的 FDM 管理 设备的程序, on page 173

使用注册密钥载入运行软件版本 6.4 或 6.5 的 FDM 管理 设备的程序

要使用注册密钥载入 FDM 管理，请遵循此程序：

Before you begin

查看先决条件，如 使用注册密钥载入 FDM 管理 设备运行软件版本 6.4 或 6.5, on page 171中所讨论。

Procedure

步骤 1 登录 CDO。

步骤 2 在导航窗格中，点击 **清单 (Inventory)**，然后点击蓝色加号按钮  以便**载入**设备。

步骤 3 点击 **FTD**。

Important 在尝试载入 FDM 管理 设备时，思科防御协调器 会提示您阅读并接受 Firepower 威胁防御最终用户许可协议 (EULA)，这是面向租户的一次性活动。接受本协议后，CDO 不会在后续的 FDM 管理 载入中再次提示您接受协议。如果 EULA 协议未来发生变化，则您必须在收到提示时再次接受它。

步骤 4 在**载入 FTD 设备 (Onboard FTD Device)** 屏幕上，点击**使用注册密钥 (Use Registration Key)**。

步骤 5 在**设备名称 (Device Name)** 字段中输入设备名称。它可以是设备的主机名或您选择的任何其他名称。

步骤 6 在**数据库更新 (Database Updates)** 区域中，**立即执行安全更新并启用定期更新 (Immediately perform security updates, and enable recurring updates)** 选项会被默认启用。此选项立即触发安全更新并自动安排设备在每周一凌晨 2 点检查是否有额外更新。有关详细信息，请参阅更新 FDM 管理 设备安全数据库和安排安全数据库更新。

Note 禁用此选项不会影响您通过 Firepower 设备管理器 配置的以前计划的任何更新。

步骤 7 在**创建注册密钥 (Create Registration Key)** 区域中，CDO 将生成注册密钥。

Note 在生成密钥后，如果您在设备完全载入之前离开了载入屏幕，您将无法返回载入屏幕；但是，CDO 会在**清单 (Inventory)** 页面为该设备创建一个占位符。当您选择设备的占位符时，您将能够在位于右侧的操作窗格中看到该设备的密钥。

步骤 8 点击复制图标 以复制注册密钥。

Note 您可以跳过复制注册密钥的步骤，然后点击**下一步 (Next)** 完成设备的占位符输入，稍后注册设备。如果您尝试先创建设备后注册，或者您是在客户网络中安装价值证明 (POV) 设备的 Cisco 合作伙伴，则此选项很有用。

在**清单 (Inventory)** 页面中，您会看到设备现在处于连接状态“未提供”(Unprovisioned)。将**未调配 (Unprovisioned)** 下出现的注册密钥复制到 防火墙设备管理器，以完成载入过程。

步骤 9 在要载入到 CDO 的设备上登录 Firepower 设备管理器。

步骤 10 在**系统设置 (System Settings)**中，点击**云服务 (Cloud Services)**。

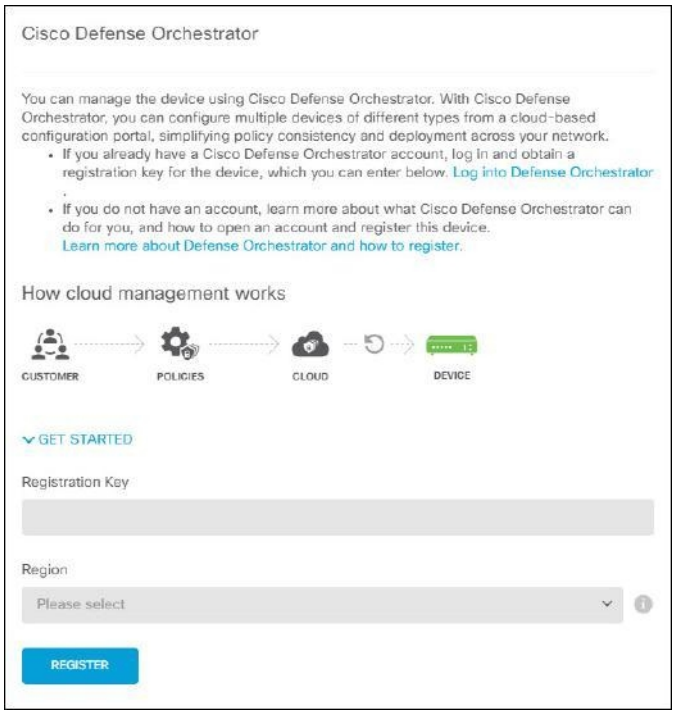
步骤 11 在 CDO 磁贴中，点击**开始 (Get Started)**。

步骤 12 在**区域 (Region)** 字段中，选择您的租户要分配到的 思科云区域：

- 如果您登录到 defenseorchestrator.com，请选择美国。
- 如果您登录到 defenseorchestrator.eu，请选择欧盟。
- 如果您登录到 apj.cdo.cisco.com，请选择亚太及日本地区。

Note 此步骤不适用于运行版本 6.4 的 FDM 管理 设备。

步骤 13 在**注册密钥 (Registration Key)**字段中，粘贴您在 CDO 中生成的注册密钥。



步骤 14 点击**注册 (Register)**，然后**接受** Cisco 披露声明。

步骤 15 返回至 CDO。选择所有要应用于设备的许可证。

有关详细信息，请参阅 应用或更新智能许可证。您也可以点击**跳过 (Skip)** 以使用 90 天评估许可证继续载入。

步骤 16 返回 CDO，打开**清单 (Inventory)** 页面，观察设备状态从“未提供”(Unprovisioned) 到“正在定位”(Locating) 到“正在同步”(Syncing) 再到“已同步”(Synced) 的发展过程。

使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+

此程序介绍了如何使用注册码载入运行 6.6+ 版本的 FDM 管理 设备。此方法是将 FDM 管理 设备载入到 思科防御协调器 的推荐方法，如果使用 DHCP 为您的 FDM 托管设备分配 IP 地址，则此方法非常有用。如果该 IP 地址由于任何原因发生变化，则您的 FDM 管理 设备仍会连接到 CDO。此外，您的 FDM 管理 设备可以在您的局域网上有一个地址，只要它可以访问外部网络，就可以使用此方法载入 CDO。

Warning 如果您已有 SecureX 或思科威胁响应 (CTR) 账户，则需要合并 CDO 租户和 SecureX/CTR 账户，以便您的设备能够注册 SecureX。在您的账户合并之前，您将无法在 SecureX 中查看设备的事件或受益于其他 SecureX 功能。我们强烈建议在 SecureX 中创建 CDO 模块之前合并您的账户。您的账户可以通过 SecureX 门户合并。有关说明，请参阅合并账户。

如果要载入运行软件版本 6.4 或 6.5 的 FDM 管理 设备，请参阅使用注册密钥载入 FDM 管理 设备运行软件版本 6.4 或 6.5。

载入之前

- 此载入方法目前适用于 6.6+ 版本以及连接到 defenseorchestrator.com、defenseorchestrator.eu 和 apj.cdo.cisco.com 的客户。
- 查看 将 思科防御协调器 连接到托管设备, on page 11 以了解将 CDO 连接到 FDM 管理 设备所需的网络要求。
- 请确保您的设备由 Firepower 设备管理器 管理，而不是由 Firepower 管理中心 管理。
- 设备可以使用 90 天评估许可证，也可以使用智能许可。运行版本 6.6+ 的设备可以使用注册密钥载入到 CDO，而无需取消注册任何已安装的智能许可证。
- 设备不能已注册到 Cisco 云服务。在载入之前，请参阅下面的“从思科云服务取消注册 FDM 管理 设备”。
- 登录设备的 Firepower 设备管理器 UI 并确保设备上没有等待处理的更改。
- 确保在您的 FDM 管理 设备上正确配置 DNS。
- 请确保在 FDM 管理 设备上正确配置时间服务。
- 请确保 FDM 管理 设备显示正确的日期和时间，否则载入将失败。

后续操作：

执行以下操作之一：

- 如果运行版本 6.6+ 的 FDM 管理 设备已注册到思科云服务，则需要先取消注册设备，然后再载入。请继续从思科云服务取消注册 FDM 管理 设备, on page 176。
- 如果您的设备未注册到思科云服务，请继续 使用注册密钥载入运行软件版本 6.6+ 的 FDM 管理设备的程序, on page 177。

从思科云服务取消注册 FDM 管理 设备

以下程序是如何从思科云服务取消注册设备的程序。在使用注册密钥载入和 FDM 管理 设备以 CDO 之前，请使用此方法。

Note 如果您载入运行 7.0 或更高版本的虚拟 FDM 管理 设备，将虚拟 FDM 管理 设备注册到 CDO 会自动将性能分层智能许可选项重置为 **变量**，这是默认级别。在载入后，您 **必须** 通过 Firepower 设备管理器 UI 手动重新选择与设备关联的许可证匹配的层。

使用此程序检查并确保它未注册到思科云服务：

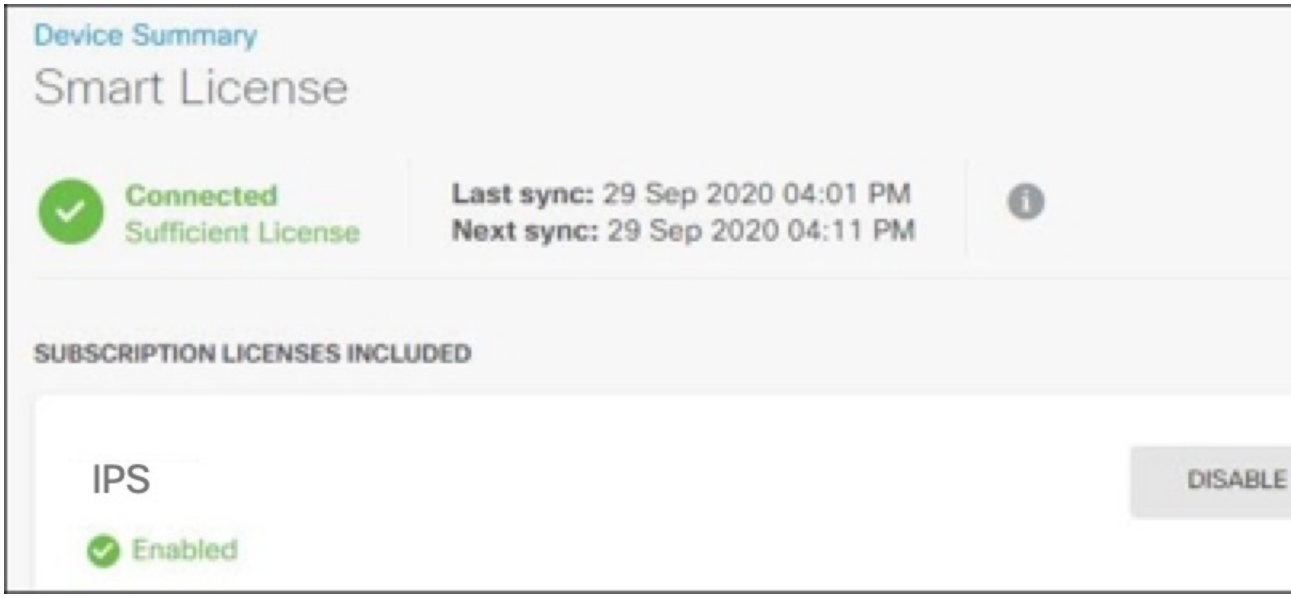
Procedure

步骤 1 使用 Firepower 设备管理器 登录设备。

步骤 2 点击上方选项卡中的设备图标。

步骤 3 展开**系统设置 (System Settings)** 菜单，然后点击**云服务 (Cloud Services)**。

步骤 4 在**云服务 (Cloud Services)** 页面中，点击齿轮菜单，然后选择**取消注册云服务 (Unregister Cloud Services)**。



步骤 5 阅读警告并点击**取消注册 (Unregister)**，以取消注册该设备。

What to do next

如果您尝试载入运行 6.6 或更高版本的 FDM 管理 设备，请继续使用注册密钥载入运行软件版本 6.6+ 的 FDM 管理 设备的程序, on page 177。

使用注册密钥载入运行软件版本 6.6+ 的 FDM 管理 设备的程序

要使用注册密钥载入 FDM 管理 设备，请遵循此程序：

Procedure

步骤 1 登录 CDO。

步骤 2 在导航窗格中，点击 **清单 (Inventory)**，然后点击蓝色加号按钮  以便**载入**设备。

步骤 3 点击 **FTD**。

Important 在尝试载入 FDM 管理 设备时，思科防御协调器 会提示您阅读并接受最终用户许可协议 (EULA)，这是租户中的一次性活动。接受本协议后，CDO 不会在后续的载入中再次提示您接受协议。如果 EULA 协议未来发生变化，则您必须在收到提示时再次接受它。

步骤 4 在**载入 FTD 设备 (Onboard FTD Device)** 屏幕上，点击**使用注册密钥 (Use Registration Key)**。

步骤 5 在**设备名称 (Device Name)** 字段中输入设备名称。它可以是设备的主机名或您选择的任何其他名称。

步骤 6 在**数据库更新 (Database Updates)** 区域中，**立即执行安全更新并启用定期更新 (Immediately perform security updates, and enable recurring updates)** 会被默认启用。此选项立即触发安全更新并自动安排设备在每周一凌晨 2 点检查是否有额外更新。有关详细信息，请参阅更新 FDM 管理 设备安全数据库和安排安全数据库更新。

Note 禁用此选项不会影响您通过 Firepower 设备管理器 配置的以前计划的任何更新。

步骤 7 在**创建注册密钥**步骤中，CDO 将生成注册密钥。

Note 在生成密钥后，如果您在设备完全载入之前离开了载入屏幕，您将无法返回载入屏幕；但是，CDO 会在**清单 (Inventory)** 页面为该设备创建一个占位符。当您选择设备的占位符时，您将能够在该页面上看到该设备的密钥。

步骤 8 点击复制图标 以复制注册密钥。

Note 您可以跳过复制注册密钥的步骤，然后点击**下一步 (Next)** 完成设备的占位符输入，稍后注册设备。如果您尝试先创建设备后注册，或者您是在客户网络中安装价值证明 (POV) 设备的 Cisco 合作伙伴，则此选项很有用。

在**清单 (Inventory)** 页面，您会看到设备现在处于连接状态“未提供”。将**未调配 (Unprovisioned)** 下出现的注册密钥复制到 防火墙设备管理器，以完成 载入过程。

步骤 9 登录到您要载入的设备的 Firepower 设备管理器。

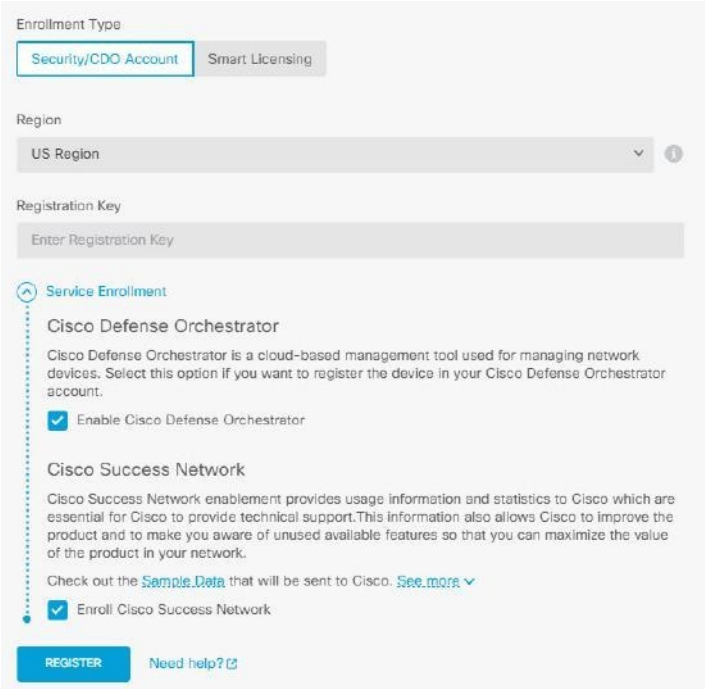
步骤 10 在 **系统设置**下，点击 **云服务**。

步骤 11 在**区域 (Region)** 字段中，选择您的租户要分配到的 思科云区域：

- 如果您登录到 defenseorchestrator.com，请选择美国。
- 如果您登录到 defenseorchestrator.eu，请选择欧盟。
- 如果您登录到 apj.cdo.cisco.com，请选择亚太及日本地区。

步骤 12 在**注册类型 (Enrollment Type)** 区域中，点击**安全账户 (Security Account)**。

Note 对于运行版本 6.6 的设备，请注意，CDO 的“租户”(Tenancy) 选项卡标题为 **安全账户 (Security Account)**，您必须在 Firepower 设备管理器 中手动启用 CDO。



步骤 13 在**注册密钥 (Registration Key)**字段中，粘贴您在 CDO 中生成的注册密钥。

步骤 14 对于在“服务注册”(Service Enrollment) 区域运行版本 6.7 或更高版本的设备，请选中**启用 Cisco Defense Orchestrator (Enable Cisco Defense Orchestrator)**。

步骤 15 查看有关思科成功网络注册的信息。如果您不想参与，请取消选中**注册思科成功网络 (Enroll Cisco Success Network)** 复选框。

步骤 16 点击**注册 (Register)**，然后点击**接受 (Accept)** 以接受思科披露声明。Firepower 设备管理器 会将注册请求发送至 CDO。

步骤 17 返回到 CDO，在**创建注册密钥 (Create Registration Key)** 区域中，点击**下一步 (Next)**。

步骤 18 选择所有要应用于设备的许可证。点击**下一步**。

步骤 19 返回 CDO，打开**清单 (Inventory)** 页面，观察设备状态从“未提供”(Unprovisioned) 到“正在定位”(Locating) 到“正在同步”(Syncing) 再到“已同步”(Synced) 的发展过程。

使用设备的序列号载入 FDM 管理 设备

此程序是设置 FDM 管理 设备并将其载入到 思科防御协调器 的简化方法。您只需要设备的机箱序列号或 PCA 序列号。在载入设备时，您可以申请智能许可证或使用 90 天评估许可证。

在执行使用低接触调配载入 FDM 管理 设备的工作流程和必备条件之前，请确保通读使用案例以了解概念。

Important 这些载入 FDM 管理 设备的方法仅适用于运行版本 6.7 或更高版本的设备。

使用案例

- 使用设备的序列号载入 FDM 管理 设备, on page 179：载入被添加到网络并从互联网访问的新出厂 FDM 管理 设备。在设备上未完成初始安装向导。
- 使用设备的序列号载入已配置的 FDM 管理 设备, on page 185：载入已配置的 FDM 管理 设备或已添加到网络并从互联网访问的已升级设备。在设备上完成初始设置向导。

Important 如果要使用此方法载入在设备支持的较旧软件版本上运行的设备，则需要在该设备上执行软件的全新安装（重新映像），而不是升级。

相关信息：

- 低接触调配中使用的术语和定义
- 对使用序列号载入 FDM 管理 设备进行故障排除

使用低接触调配载入 FDM 管理 设备的工作流程和必备条件

低接触调配功能允许自动调配和配置新出厂的 Firepower 1000、Firepower 2100 或 Secure Firewall 3100 系列设备，从而消除将设备载入到 CDO 所涉及的大多数手动任务。低接触调配适用于远程办公室或员工不太熟悉网络设备的其他位置。

要使用低接触调配流程，您必须将设备载入 CDO，将其连接到可以访问互联网的网络，然后打开设备电源。有关详细信息，请参阅 使用设备的序列号载入已配置的 FDM 管理 设备, on page 185。

Note 您可以在将设备载入 CDO 之前或之后启动设备。**我们建议您先将设备载入 CDO，然后再启动设备，再将其连接到分支机构网络**。当您在 CDO 中载入设备时，该设备将与思科云中的 CDO 租户关联，并且 CDO 会自动同步设备。

您还可以使用此程序载入从外部供应商处购买的设备，或者载入已由其他区域中的其他云租户管理的设备。但是，如果设备已注册到外部供应商的云租户或其他区域的云租户，则 CDO 不会载入设备，但会显示 “设备序列号已申领 *(Device serial number already claimed)*” 错误消息。在这种情况

下，CDO 管理员必须从其先前的云租户中取消注册设备的序列号，然后在自己的租户中申领 CDO 设备。请参阅故障排除一章中的设备序列号已被申领。

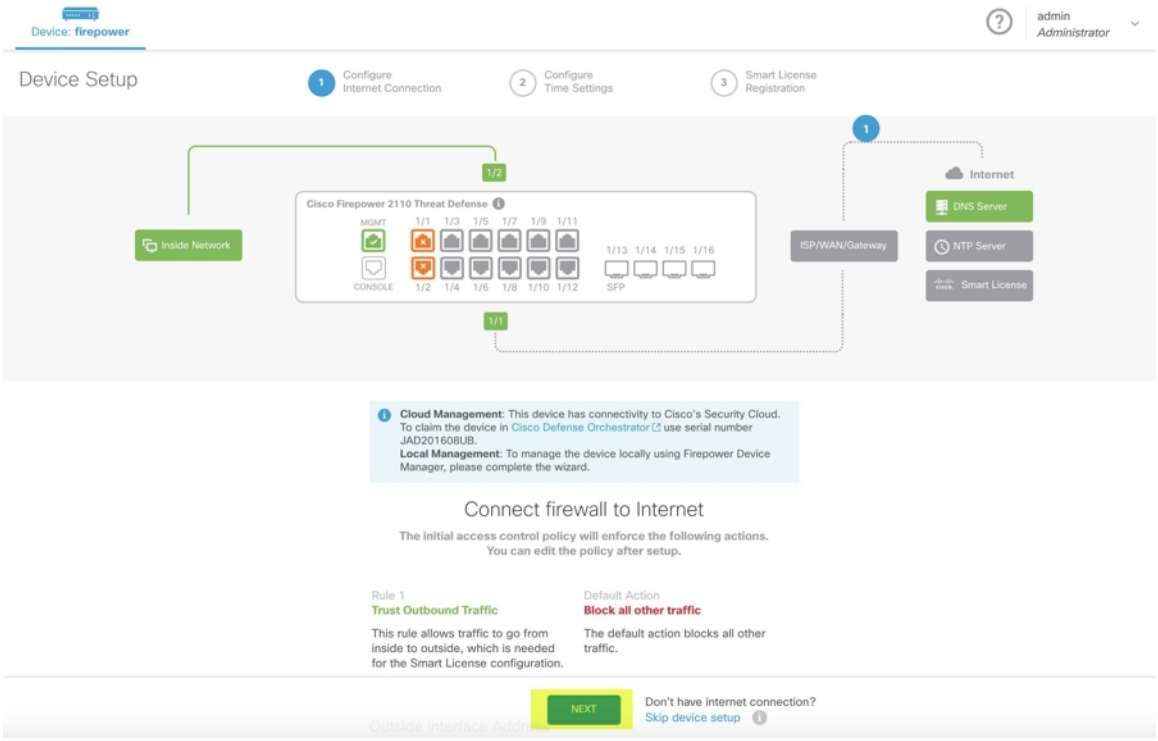
设备**连接 (Connectivity)** 状态更改为“在线”(Online)， **配置 (Configuration)** 状态更改为“已同步”(Synced)。FDM 管理 设备已被载入 CDO。

您可以看到硬件后面板上的状态 LED (Firepower 1010)、SYS LED (Firepower 2100) 或 S LED (Secure Firewall 3100) 呈绿色闪烁。连接到云时，设备 LED 会继续闪烁绿色。如果设备无法连接到思科云或在连接后失去连接，您可以看到状态 LED (Firepower 1010)、SYS LED (Firepower 2100) 或 M LED (Secure Firewall 3100) 交替闪烁绿色和琥珀色。

请参阅此视频：使用低接触调配安装思科 Firepower 防火墙视频，以便了解 LED 指示灯。

Important 如果您已登录 FDM 管理 设备控制台、SSH 或 Firepower Threat Defense，您将在首次登录时更改设备的密码。您仍然可以使用低接触调配流程来使用 CDO 载入设备。登录 Firepower Threat Defense 后，请勿完成配置外部接口的设备安装向导步骤。如果完成此步骤，则设备将从云中注销，并且您无法使用低接触调配。

当您登录 Firepower Threat Defense 时，您将在控制面板上看到以下屏幕。



无需在 Firepower Threat Defense UI 上继续操作，转至序列号载入向导并载入设备。在这里，您必须选择**默认密码已更改 (Default Password Changed)**，因为设备密码已更改。

前提条件

软件和硬件要求

FDM 管理 设备必须运行支持序列号载入的软件。使用下表作为指南：

Table 9: 硬件和软件支持

支持低接触调配的防火墙型号	支持的防火墙软件版本	软件包
Firepower 1000 系列设备型号：1010、1120、1140、1150	6.7 或更高版本	SF-F1K-TDx.x-K9
Firepower 2100 系列设备型号：2110、2120、2130、2140	6.7 或更高版本	SF-F2K-TDx.x-K9
Secure Firewall 3100 系列设备型号：3110、3120、3130、3140	7.1 或更高版本	SF-F3K-TDx.x-K9

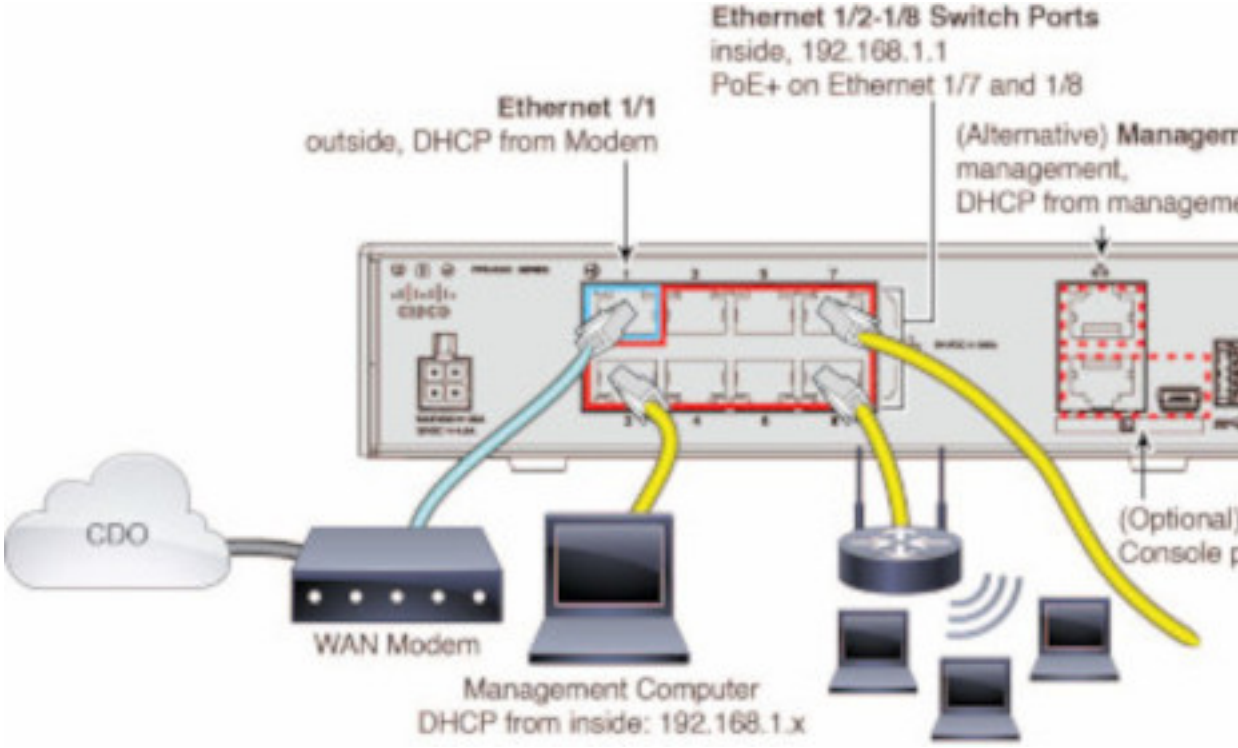
确认管理平台运行的是正确的版本。

Table 10: 支持 ***FTD*** 管理器版本

管理器	支持的版本
Firepower 设备管理器	7.0 或更高版本
本地防火墙管理中心	7.2 或更高版本
云交付的防火墙管理中心	不适用

硬件安装的配置前提条件

- **分支机构的网络无法使用 192.168.1.0/24 地址空间**。以太网 1/1（外部）上的网络无法使用 192.168.1.0/24 地址空间。运行 FDM 6.7 的 1000 和 2100 系列设备上的以太网 1/2“内部”接口的默认 IP 地址为 192.168.1.1，如果它在该子网上，则可能与 WAN 调制解调器分配的 DHCP 地址冲突。
  - **内部** - 以太网 1/2，IP 地址 192.168.1.1
  - **外部** - 以太网 1/1、来自 DHCP 的 IP 地址或在设置过程中指定的地址



如果无法更改外部接口设置，请使用 Firepower 设备管理器 更改以太网 1/2“内部”接口设置上的子网，以避免冲突。例如，您可以更改为以下子网设置：

- IP 地址：192.168.95.1
- DHCP 服务器范围：192.168.95.5-192.168.95.254

要了解配置物理接口的步骤，请参阅 《思科防火墙设备管理器配置指南》。在“接口”一章中，请参阅“配置物理接口”部分。

- 威胁防御 设备必须已安装并连接到思科云。
- 设备的外部或管理接口必须连接到提供 DHCP 寻址的网络。通常，设备在外部或管理接口上有一个默认的 DHCP 客户端。

Note 如果管理接口连接到具有 DHCP 服务器的网络，则它优先于 Linux 堆栈发起的流量的外部接口。

- 需要访问您的外部或管理接口才能访问以下 安全服务交换 域以便使用串行载入方法。
  - 美国地区
    - api-sse.cisco.com
    - est.sco.cisco.com（跨地域通用）

- mx*.sse.itd.cisco.com（目前仅 mx01.sse.itd.cisco.com）
- dex.sse.itd.cisco.com（客户成功案例）
- eventing-ingest.sse.itd.cisco.com （CTR 和 CDO）
- registration.us.sse.itd.cisco.com（允许设备注册到思科区域云）

- 欧盟地区
  - api.eu.sse.itd.cisco.com
  - est.sco.cisco.com（跨地域通用）
  - mx*.eu.sse.itd.cisco.com（目前仅 mx01.eu.sse.itd.cisco.com）
  - dex.eu.sse.itd.cisco.com（客户成功案例）
  - eventing-ingest.eu.sse.itd.cisco.com（CTR 和 CDO）
  - registration.eu.sse.itd.cisco.com（允许设备注册到思科区域云）

- 亚太地区
  - api.apj.sse.itd.cisco.com
  - est.sco.cisco.com（跨地域通用）
  - mx*.apj.sse.itd.cisco.com（目前仅 mx01.apj.sse.itd.cisco.com）
  - dex.apj.sse.itd.cisco.com（客户成功案例）
  - eventing-ingest.apj.sse.itd.cisco.com（CTR 和 CDO）
  - http://registration.apj.sse.itd.cisco.com（允许设备注册到思科区域云）
    http://registration.apj.sse.itd.cisco.com/

- 设备的外部接口必须具有对思科 Umbrella DNS 的 DNS 访问权限。

在 CDO 中申领设备之前

在 CDO 中申领设备之前，请确保您拥有以下信息：

- 威胁防御 设备的机箱序列号或PCA编号。您可以在硬件机箱的底部或装运设备的包装箱上找到此信息。在下面的示例图片中，您可以看到Firepower 1010机箱底部的序列号“*******X0R9”。

- 设备的默认密码。
- 从思科智能软件管理器生成以用于其他功能的智能许可证。但是，您可以使用90天评估许可证来完成设备载入，然后再申请智能许可证。

通过低接触调配载入*FDM* 管理设备

Caution 在 思科防御协调器 中载入设备时，我们建议您不要使用 Firepower 设备管理器 来执行设备简易设置。这会导致 CDO 出现临时错误。

Before you begin

如果您载入设备并打算使用 本地管理中心 对其进行管理，则 本地管理中心 **必须**运行 7.4 及更高版本。较早的版本不支持低接触调配。

Procedure

步骤 1 如果要载入从外部供应商处购买的设备，则必须先重新映像设备。有关更多信息，请参阅《思科 FXOS 故障排除指南》中的“重新映像程序”一章。

步骤 2 登录 CDO。

步骤 3 在导航窗格中，点击 **清单 (Inventory)**，然后点击蓝色加号按钮 以便**载入**设备。

步骤 4 点击 **FTD** 磁贴。

Important 在尝试载入设备时，CDO 会提示您阅读并接受最终用户许可协议 (EULA)，这是租户中的一次性活动。接受本协议后，CDO 不会在后续的载入中再次提示您接受协议。如果 EULA 协议未来发生变化，则您必须在收到提示时再次接受它。

步骤 5 在**载入 FTD 设备 (Onboard FTD Device)** 屏幕上，点击**使用序列号 (Use Serial Number)**。

步骤 6 在**选择 FMC** 步骤中，使用下拉菜单选择已被载入 CDO 的 本地管理中心。点击**下一步**。

本地管理中心 必须运行 7.4 或更高版本。如果您没有载入的 本地管理中心，请点击“+ 载入本地 FMC”(+Onboard On-Prem FMC) 以查看载入向导。

步骤 7 在**连接 (Connection)** 步骤中，输入设备的序列号和设备名称。点击**下一步**。

步骤 8 对于低接触调配，设备必须是全新的或已重新映像。对于**密码重置 (Password Reset)**，确保选择**是，此新设备从未登录或配置管理器 (Yes, this new device has never been logged into or configured for a manager)**。输入设备的新密码并确认新密码，，然后点击**下一步 (Next)**。

步骤 9 对于**策略分配 (Policy Assignment)**，使用下拉菜单选择在设备载入后要部署的访问控制策略。如果没有自定义策略，CDO 会自动选择默认访问控制策略。点击**下一步**。

步骤 10 选择所有要应用于设备的许可证。点击**下一步**。

步骤 11 （可选）为设备添加标签。CDO 会在设备成功载入后应用这些标签。

What to do next

CDO 会开始申领设备，您将在右侧看到**正在申领 (Claiming)** 消息。CDO 会持续轮询一小时，以确定设备是否在线并已注册到云。注册到云后，CDO 将开始初始调配并成功载入设备。当设备上的 LED 状态呈绿色闪烁时，可以确认设备注册。如果设备在连接后无法连接到思科云或失去连接，您可以看到状态 LED (Firepower 1000) 或 SYS LED (Firepower 2100) 交替闪烁绿色和琥珀色。

如果设备在前一小时内仍未注册到云，则会发生超时，现在 CDO 会每隔 10 分钟定期轮询一次，以确定设备状态并保持**正在申领 (Claiming)** 状态。当设备打开并连接到云时，您无需等待 10 分钟即可了解其载入状态。您可以随时点击**检查状态 (Check Status)** 链接查看状态。CDO 会开始初始调配并成功载入设备。

Important 假设您已完成设备安装向导（请参阅 使用设备的序列号载入已配置的 FDM 管理 设备），设备已从云中取消注册，在这种情况下，CDO 仍处于**正在申领 (Claiming)** 状态。您需要从 Firepower 设备管理器 完成手动注册，才能将其添加到 CDO。（在 Firepower 设备管理器 中，转至**系统设置 (System Settings)** > **云服务 (Cloud Services)**，然后选择**通过思科防御协调器自动注册租用 (Auto-enroll with Tenancy from Cisco Defense Orchestrator)** 选项并点击**注册 (Register)**）。然后，点击**检查状态 (Check Status)**。

使用设备的序列号载入已配置的 FDM 管理 设备

此程序适用于已配置为进行管理的设备。由于设备安装向导是在已配置的FDM管理 设备上完成的，因此设备将从云中取消注册，并且您无法使用低接触调配过程将此类设备载入 CDO。

如果您的设备是全新的，并且从未进行过管理或配置，您可以通过低接触调配来载入设备。有关详细信息，请参阅 通过低接触调配载入FDM 管理设备, on page 184。

Note 当设备未连接到思科云时，您可以看到状态 LED（Firepower 1000）、SYS LED（Firepower 2100）或 M LED（Secure Firewall 3100）交替闪烁绿色和琥珀色。

您可能已完成设备安装向导以执行以下任务：

- 设备必须运行版本 6.7 或更高版本。
- 在设备的管理接口上配置静态 IP 地址。如果接口无法获取必要的动态 IP 地址，或者 DHCP 服务器不提供网关路由，则需要配置静态 IP 地址。
- 使用 PPPoE 获取地址并配置外部接口。
- 使用 Firepower 设备管理器 或 Firepower 管理中心 来管理运行 6.7 或更高版本的设备。

Important 您可以将 Secure Firewall Threat Defense 设备的管理器从 Firepower 设备管理器 切换为 Firepower 管理中心，也可以切换为其他方式。对于设备运行的版本，执行《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》的“系统管理”一章的**在本地管理和远程管理之间切换**部分中介绍的步骤。

如果要载入设备，请执行以下操作：

Procedure

步骤 1 有关载入的前提条件，请查看此处的使用低接触调配载入 FDM 管理 设备的工作流程和必备条件。

步骤 2 在 Firepower 设备管理器 UI 中，请转至 **系统设置** > **云服务** ，然后选 **通过 Cisco 防御协调器自动注册租用** 选项并点击 **注册**。

步骤 3 登录 CDO。

步骤 4 在导航窗格中，点击 **清单 (Inventory)** ，然后点击蓝色加号按钮 以便**载入**设备。

步骤 5 点击 **FTD 磁贴**。

步骤 6 在**载入 FTD 设备 (Onboard FTD Device)** 屏幕上，点击**使用序列号 (Use Serial Number)**。

步骤 7 在**选择 FMC** 步骤中，使用下拉菜单选择已被载入 CDO 的 本地管理中心。点击**下一步**。

本地管理中心 必须运行 7.4 或更高版本。如果您没有载入的 本地管理中心，请点击“+ 载入本地 FMC”(+Onboard On-Prem FMC) 以查看载入向导。

步骤 8 在**连接 (Connection)** 步骤中，输入设备的序列号和设备名称。点击**下一步**。

步骤 9 如果设备**并非**全新的，并且已配置为进行管理，请选择**是，此新设备从未登录或为管理器配置 (Yes, this new device has never been logged into or configured for a manager)** 以进行**密码重置**。点击**下一步**。

步骤 10 对于**策略分配 (Policy Assignment)**，使用下拉菜单选择在设备载入后要部署的访问控制策略。如果没有自定义策略，CDO 会自动选择默认访问控制策略。点击**下一步**。

步骤 11 选择所有要应用于设备的许可证。点击**下一步**。

CDO 将设备**连接 (Connectivity)** 状态更改为“在线”(Online)，并将**配置 (Configuration)** 状态更改为“已同步”(Synced) 状态。FDM 管理 设备已被载入 CDO。您可以看到硬件后面板上的状态 LED (Firepower 1000)、SYS LED (Firepower 2100) 或 M LED 呈绿色闪烁。当设备连接到思科云时，设备 LED 会继续闪烁绿色。如果设备无法连接到思科云或在连接后失去连接，您可以看到相同的状态 LED 交替闪烁绿色和琥珀色。

相关信息：

- 低接触调配中使用的术语和定义

载入 FDM 管理 高可用性对

要将 Secure Firewall Threat Defense HA 对载入 CDO，必须单独载入该对中的每台设备。一对设备中的两个对等设备均已被载入后，CDO 会自动将其合并为**清单 (Inventory)** 页面中的单个条目。使用设备登录凭证或注册密钥载入设备。我们建议使用相同的方法载入**两台**设备。另请注意，如果您首先载入处于备用模式的设备，则CDO会禁用从该设备进行部署或读取的功能。您只能读取或部署到 HA 对中的主用设备。

注释 CDO 强烈建议使用注册密钥来载入设备。对于运行特定版本的 FTD 设备，使用注册密钥载入略有不同。有关详细信息，请参阅载入运行版本 6.4 或版本 6.5 的 FDM 管理 HA 对，第 188 页和载入运行版本 6.6 或版本 6.7 及更高版本的 FDM 管理 HA 对，第 189 页。

在将 FTD HA 对载入 CDO 之前，请查看以下内容：

- 您的 HA 对会在载入到 CDO 之前形成。
- 两台设备均处于正常状态。该对可以是主/主用和辅助/备用模式，**或** 主/备用和辅助/主用模式。运行状况不佳的设备将无法成功同步到 CDO。
- 您的 HA 对由 Firepower 设备管理器 管理，而不是由 Firepower 管理中心 管理。
- 您的云连接器连接到 CDO，https://www.defenseorchestrator.com。

使用注册密钥载入 FDM 管理高可用性对

在使用注册密钥载入 FDM 管理高可用性 (HA) 对之前，请注意以下前提条件：

- 仅美国区域 (defenseorchestrator.com) 支持使用注册密钥载入 6.4 版本的设备。要连接到欧盟区域 (defenseorchestrator.eu)，则必须使用用户名、密码和 IP 地址载入其 HA 对。
- 运行版本 6.5 或更高版本并连接到美国、欧盟或 APJC 的客户可以使用此载入方法。

- 运行版本 6.4 和 6.5 的设备在使用注册密钥载入之前，不得向思科智能软件管理器注册。您需要先取消注册这些 FDM 管理 设备的智能许可证，然后再将其载入 CDO。有关详细信息，请参阅取消注册智能许可的 FDM 管理 设备, on page 172。

载入运行版本 *6.4* 或版本 *6.5* 的 *FDM* 管理 *HA* 对

要载入运行软件版本 6.4 或 6.5 的 FDM 管理 HA 对，您必须一次载入一个设备。载入的设备是主设备还是辅助设备并不重要。

Note 如果使用注册密钥载入 HA 对的任一台设备，则必须以相同的方法载入另一台对等设备。

使用以下步骤来载入运行版本 6.4 或 6.5 的 HA 对：

Procedure

步骤 1 载入对等设备。请参阅使用注册密钥载入 FDM 管理 设备运行软件版本 6.4 或 6.5以载入对中的第一台设备。

步骤 2 在导航窗格中，点击**清单 (Inventory)**。

步骤 3 点击 **设备** 选项卡，找到您的设备。

步骤 4 点击 **FTD** 选项卡。设备同步后，请选择设备，使其突出显示。在**设备详细信息 (Device Details)** 正下方的操作窗格中，点击**载入设备 (Onboard Device)**。

步骤 5 输入已载入的对等设备的 **HA 对等体设备名称**。点击**下一步**。

步骤 6 如果您为第一台设备提供了智能许可证，CDO 会重新填充该许可证，以便您可以使用它来载入此当前设备。点击**下一步**。

Note 如果您取消注册设备的智能许可证以载入 FDM 管理 设备，您可以在此处重新应用智能许可证。

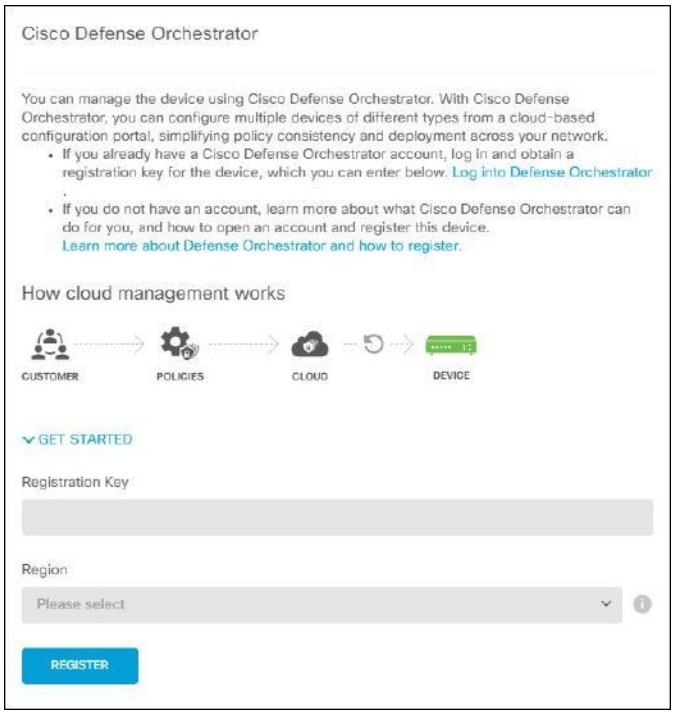
步骤 7 CDO 会自动为您准备载入的设备生成该注册密钥。点击**复制**图标 以复制注册密钥。

步骤 8 登录到您要载入的设备的 Firepower 设备管理器 UI。

步骤 9 在**系统设置 (System Settings)**中，点击**云服务 (Cloud Services)**。

步骤 10 在 CDO 磁贴中，点击**开始 (Get Started)**。

步骤 11 在**注册密钥 (Registration Key)**字段中，粘贴您在 CDO 中生成的注册密钥。



步骤 12 在**区域 (Region)** 字段中，选择您的租户要分配到的 思科云区域：

- 如果您登录到 defenseorchestrator.com，请选择美国。
- 如果您登录到 defenseorchestrator.eu，请选择欧盟。
- 如果您登录到 apj.cdo.cisco.com，请选择亚太及日本地区。

Note 此步骤不适用于在版本 6.4 上运行的 FDM 管理 设备。

步骤 13 点击**注册 (Register)**，然后**接受** Cisco 披露声明。

步骤 14 返回到 CDO，然后在**创建注册密钥 (Create Registration Key)** 区域中，点击**下一步 (Next)**。

步骤 15 点击**转至清单 (Go to Inventory)**。CDO 会自动载入设备并将其合并为一个条目。与您载入的第一个对等设备类似，设备状态会从“未调配”(Unprovisioned) 依次变为“正在查找”(Locating)、“正在同步”(Syncing)、“已同步”(Synced)。

载入运行版本 *6.6* 或版本 *6.7* 及更高版本的 *FDM* 管理 *HA* 对

要载入运行版本 6.6 或 6.7 的 FDM 管理 HA 对，必须一次载入一个设备。载入的设备是主设备还是辅助设备并不重要。

Note 如果使用注册密钥载入 HA 对的任一台设备，则必须以相同的方法载入另一台对等设备。

使用以下步骤载入运行版本 6.6 或 6.7 的 HA 对：

Procedure

步骤 1 载入对等设备。有关详细信息，请参阅使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+。

步骤 2 在导航窗格中，点击**清单 (Inventory)**。

步骤 3 点击 **设备** 选项卡，找到您的设备。

步骤 4 点击 **FTD** 选项卡。设备同步后，请选择设备，使其突出显示。在**设备详细信息 (Device Details)** 正下方的操作窗格中，点击**载入设备 (Onboard Device)**。

步骤 5 输入已被载入的对等设备的 HA 对等设备名称。点击**下一步**。

步骤 6 如果您为第一台设备提供了智能许可证，CDO 会重新填充该许可证，以便您可以使用它来载入此当前设备。点击**下一步**。

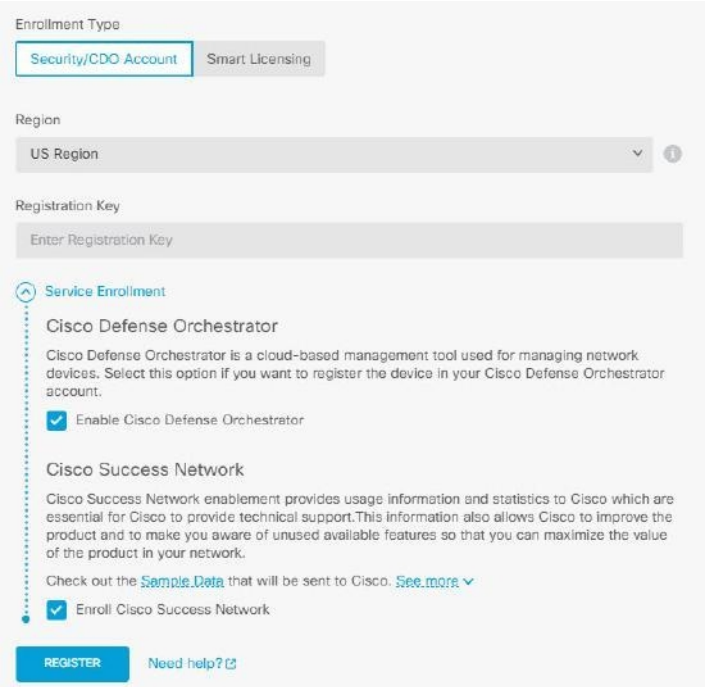
步骤 7 CDO 会自动为您准备载入的设备生成该注册密钥。点击复制图标 以复制注册密钥。

步骤 8 在要载入到 CDO 的设备上登录 Firepower 设备管理器。

步骤 9 在**系统设置 (System Settings)** 下，点击**云服务 (Cloud Services)**。

步骤 10 在**注册类型 (Enrollment Type)** 区域中，点击**安全/CDO 账户 (Security/CDO Account)**。

Note 对于运行版本 6.6 的设备，请注意，CDO 的“租户”(Tenancy) 选项卡标题为 **安全账户 (Security Account)**，您必须在 Firepower 设备管理器 UI 中手动启用 CDO。



步骤 11 在**区域 (Region)** 字段中，选择您的租户要分配到的 思科云区域：

- 如果您登录到 defenseorchestrator.com，请选择美国。
- 如果您登录到 defenseorchestrator.eu，请选择欧盟。
- 如果您登录到 apj.cdo.cisco.com，请选择亚太及日本地区。

步骤 12 在**注册密钥 (Registration Key)**字段中，粘贴您在 CDO 中生成的注册密钥。

步骤 13 对于在“服务注册”(Service Enrollment) 区域运行版本 6.7 或更高版本的设备，请选中**启用思科防御协调器 (Enable Cisco Defense Orchestrator)**。

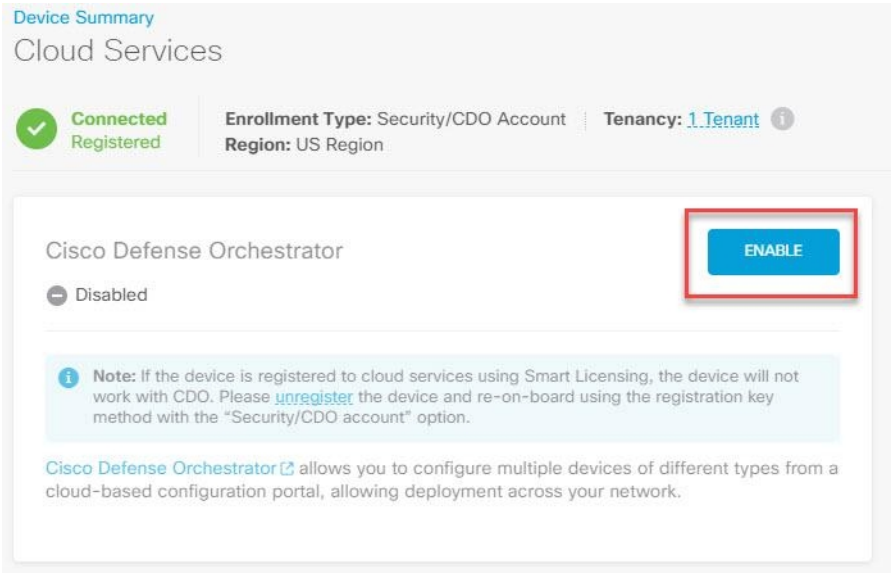
步骤 14 查看有关思科成功网络注册的信息。如果您不想参与，请取消选中**注册思科成功网络 (Enroll Cisco Success Network)** 复选框。

步骤 15 点击**注册 (Register)**，然后**接受** Cisco 披露声明。FDM 将注册请求发送到 CDO。

步骤 16 返回到 CDO，在**创建注册密钥 (Create Registration Key)** 区域中，点击**下一步 (Next)**。

步骤 17 在**智能许可证 (Smart License)** 区域中，您可以将智能许可证应用于 FDM 管理 设备，然后点击**下一步 (Next)**，也可以点击**跳过 (Next)** 以使用 90 天评估许可证继续载入，或者如果设备已获得智能许可。有关详细信息，请参阅 更新 FTD 设备的现有智能许可证。

Note 如果您的设备运行的是版本 6.6，则需要手动启用与 CDO 的通信。在设备的 FDM 管理 UI 中，导航至 **系统设置 (System Settings)** > **云服务 (Cloud Services)** ，然后在**思科防御协调器 (Cisco Defense Orchestrator)** 磁贴中点击**启用 (Enable)**。



步骤 18 返回到 CDO，点击**转至清单 (Go to Inventory)**。CDO 会自动载入设备并将其合并为一个条目。与您载入的第一个对等设备类似，设备状态会从“未调配”(Unprovisioned) 依次变为“正在查找”(Locating)、“正在同步”(Syncing)、“已同步”(Synced)。

载入 FDM 管理 高可用性对

注释 无论您使用什么方法来载入 HA 对的第一台设备，都必须以相同的方法载入另一台对等设备。

要载入在 CDO 外部创建的 FDM 管理 HA 对，请执行以下程序：

过程

步骤 1 载入 HA 对中的一个对等设备。使用设备的使用用户名、密码和 IP 地址载入 FDM 管理 设备、使用注册密钥载入运行软件版本 6.6+ 的 FDM 管理 设备的程序或使用设备的序列号载入已配置的 FDM 管理 设备来载入设备。

步骤 2 在设备同步后，在**清单 (Inventory)** 页面中，点击**设备 (Devices)** 选项卡。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择设备。在**设备详细信息 (Device Details)** 正下方的操作窗格中，点击**载入设备 (Onboard Device)**。

步骤 5 在弹出窗口中，输入 HA 对等体的设备名称和位置。

步骤 6 点击**载入设备 (Onboard Device)**。两台设备成功同步到 CDO 后，HA 对在**清单 (Inventory)** 页面中显示为单个实体。

载入 FTD 集群

-

载入集群的 设备

按照以下程序载入已加入集群的 威胁防御 设备：

开始之前

以下设备支持集群：

- Secure Firewall 3100 设备
- Firepower 4100 设备
- Firepower 9300 设备
- FTDv 设备（AWS、Azure、VMware、KVM、GCP）

请注意集群设备的以下限制：

- 设备必须至少运行 6.4 版本。
- 设备必须由物理或虚拟 Firepower 管理中心 管理。
- Firepower 4100 和 Firepower 9300 设备都必须通过设备的机箱管理器进行集群。
- Secure Firewall 3100 设备、KVM 和 VMware 环境必须通过 UI 进行集群。
- Azure、AWS 和 GCP 环境集群必须通过各自的环境创建并载入 Cisco Secure Firewall Management Center。

过程

步骤 1 登录 CDO。

步骤 2 在导航窗格中，点击 **清单 (Inventory)**，然后点击蓝色加号按钮  以便**载入**设备。

步骤 3 点击 **FTD**。

步骤 4 在 **管理模式**下，确保选择 **FTD** 。

通过选择 **FTD**，您将保留 作为管理平台。如果选择 **FDM**，这会将管理器从 切换到本地管理器，例如 防火墙设备管理器 或 云交付的防火墙管理中心。请注意，交换管理器会重置除接口配置以外的所有现有策略配置，并且您必须在载入设备后重新配置策略。

步骤 5 在**载入 FTD 设备 (Onboard FTD Device)** 屏幕上，点击**使用 CLI 注册密钥 (Use Registration Key)**。

步骤 6 在**设备名称 (Device Name)** 字段中输入设备名称。它可以是设备的主机名或您选择的任何其他名称。

步骤 7 在策略分配步骤中，使用下拉菜单选择在设备载入后要部署的访问控制策略。如果未配置策略，请选择**默认访问控制策略 (Default Access Control Policy)**。

步骤 8 指定要载入的设备是物理设备还是虚拟设备。如果要载入虚拟设备，则必须从下拉菜单中选择设备的性能级别。

步骤 9 选择要应用于设备的基础版许可证。点击**下一步**。

步骤 10 CDO 使用注册密钥生成命令。将整个注册密钥按原样粘贴到设备的 CLI 中。

步骤 11 设备开始载入。作为可选步骤，您可以向设备添加标签，以帮助对“清单”(Inventory) 页面进行排序和过滤。输入标签，然后选择蓝色加号按钮。。

下一步做什么

设备同步后，CDO 会自动检测到设备已加入集群。在这里，请从“清单”(Inventory) 页面选择您刚刚载入的设备，然后选择位于右侧的“管理”(Management) 窗格下列出的任何选项。我们强烈建议您执行以下操作：

- 如果还没有创建，请创建自定义访问控制策略，以自定义环境的安全性。有关详细信息，请参阅FDM 管理 访问控制策略，第 323 页。
- 启用思科安全分析和日志记录 (SAL) 以在 CDO 控制面板中查看事件， **或**将设备注册到 Cisco Secure Firewall Management Center 以进行安全分析。

应用或更新智能许可证

将新的智能许可证应用于 FDM 管理 设备

执行以下程序之一，以智能许可 Firepower 威胁防御 (FTD) 设备：

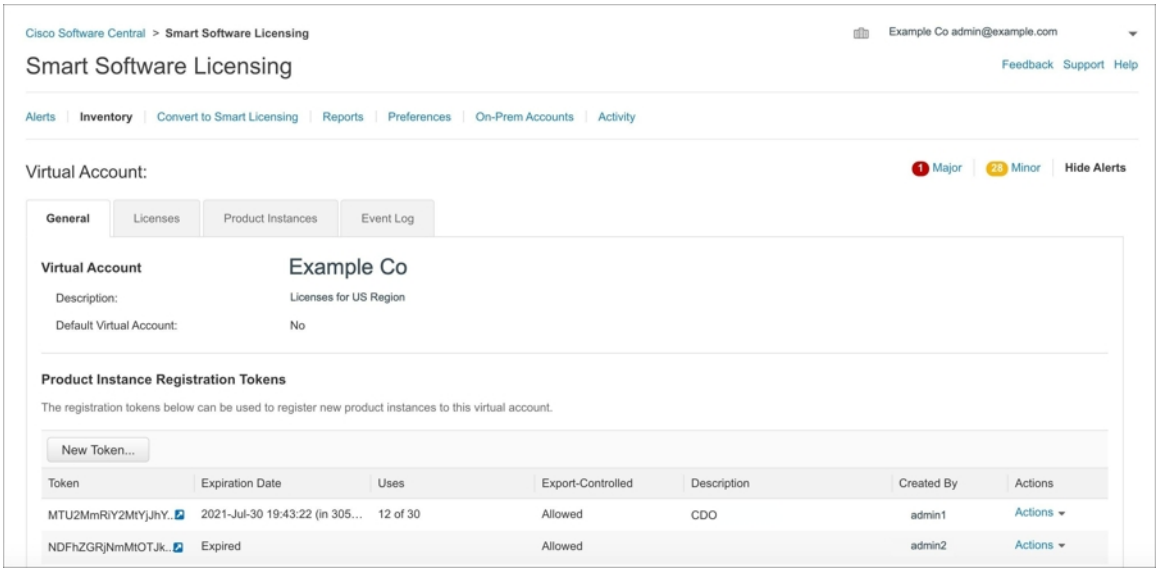
- 使用注册密钥载入 FDM 管理 设备时为设备提供智能许可证。
- 在使用注册密钥或管理员凭证载入设备后，为 FDM 管理 设备授予智能许可证。

Note FDM 管理 设备可能使用的是 90 天评估许可证，也可能是未注册的许可证。

在使用注册密钥载入时为 FDM 管理设备提供智能许可

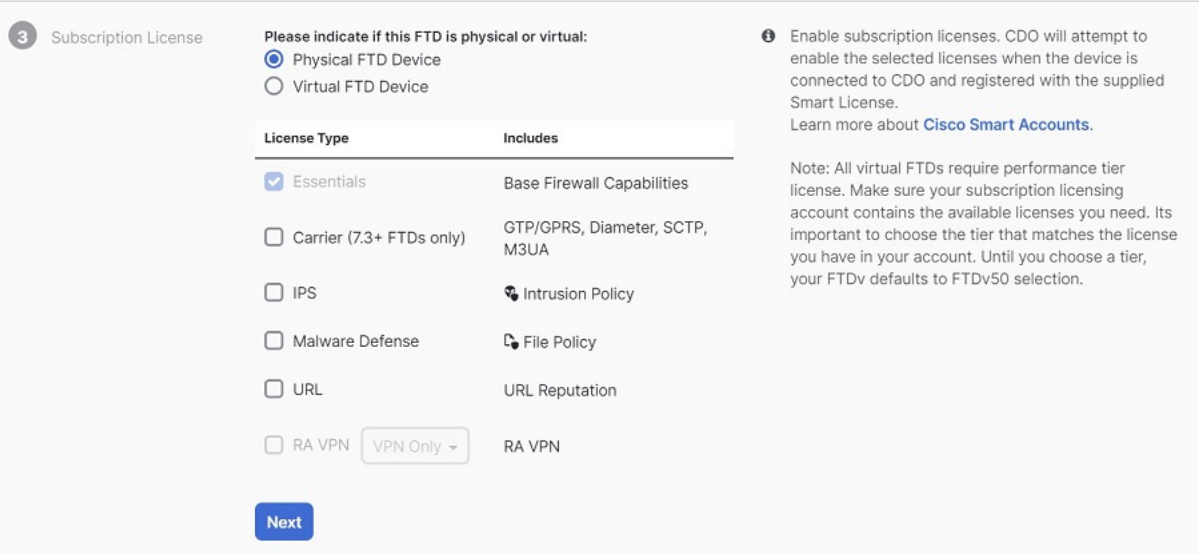
Procedure

步骤 1 登录思科智能软件管理器并生成新的智能许可证密钥。https://software.cisco.com/software/csws/ws/platform/home?locale=en_US#SmartLicensing-Inventory复制新生成的密钥。您可以观看生成智能许可视频了解详细信息。



步骤 2 使用注册密钥开始载入 FDM 管理设备。有关详细信息，请参阅使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+或使用注册密钥载入 FDM 管理 设备运行软件版本 6.4 或 6.5。

步骤 3 在自行激活向导的第 4 步中，在此处的智能许可证框中，将智能许可证粘贴到激活字段中，然后点击下一步。

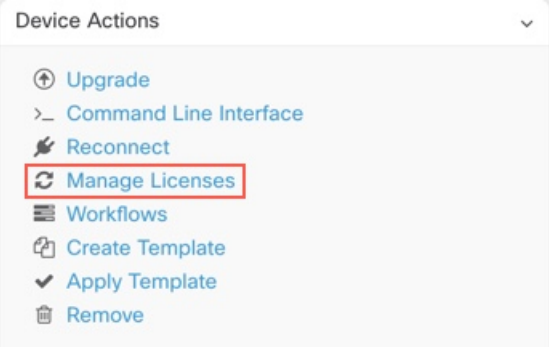


步骤 4 点击**转到清单页面 (Go to Inventory page)**。

步骤 5 点击 FTD 选项卡，查看自行激活过程的进度。设备开始同步并应用智能许可证。

您应该会看到设备现在处于在线连接状态。如果设备未处于在线连接状态，请查看右侧的设备操作窗格，然后点击管理许可证刷新许可证以更新连接状态。 >

步骤 6 将智能许可证成功应用于设备后，点击管理许可证。FDM 管理设备状态显示“已连接，许可证充足”。您可以启用或禁用可选许可证。有关详细信息，请参阅设备智能许可类型。FDM管理 设备许可类型



使用注册密钥或凭据载入设备后，为 FDM 管理设备授予智能许可证

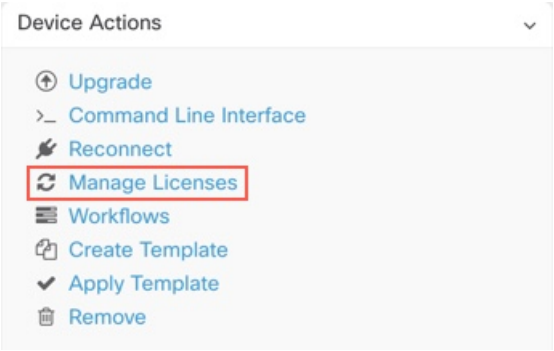
Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡，然后选择要许可的设备。

步骤 4 在右侧的设备操作窗格中，点击管理许可证。



步骤 5 按照屏幕说明输入从思科智能软件管理器生成的智能许可证。

步骤 6 将新的许可证密钥粘贴到框中，然后点击**注册设备 (Register Device)**。与设备同步后，连接状态变为“在线”。成功将智能许可证应用到 FDM 管理设备后，设备状态将显示“**已连接，许可证足够 (Connected, Sufficient License)**”。您可以启用或禁用可选许可证。有关详细信息，请参阅设备智能许可类型。FDM 管理 设备许可类型

更新 FTD 设备的现有智能许可证

您可以将新的智能许可证应用于智能许可的 FTD 设备。根据您选择的设备载入方法，选择适当的程序：

更改应用于使用注册密钥载入的 FDM 管理设备的智能许可证

Procedure

步骤 1 从 思科防御协调器 中删除相应的 FDM 管理设备。

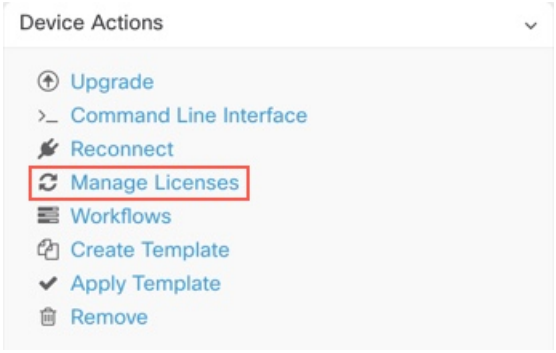
步骤 2 登录到该设备的 Firepower 设备管理器 并注销智能许可证。有关详细信息，请参阅取消注册智能许可的 FDM 管理 设备。

步骤 3 在 CDO 中，使用注册密钥再次载入 FDM 管理设备。有关详细信息，请参阅使用注册密钥载入 FDM 托管设备。使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+, on page 175

步骤 4 点击**设备 (Devices)** 选项卡以找到设备。

步骤 5 点击选项卡。

步骤 6 在载入过程中或通过查看右侧的**设备操作 (Device Actions)** 窗格并点击**管理许可证 (Manage Licenses)** 来应用新的智能许可证。



更改应用于使用其凭证载入的 FDM 管理 设备的智能许可证

Procedure

步骤 1 登录到该设备的 Firepower 设备管理器 并注销智能许可证。有关详细信息，请参阅使用注册密钥载入 FDM 管理 设备运行软件版本 6.6+。

步骤 2 将新的智能许可证应用于 Firepower 设备管理器 中的 FDM 管理 设备。

a. 点击**智能许可证 (Smart License)** 区域中的 **查看配置 (View Configuration)**。

b. 点击**立即注册 (Register Now)**，并按照屏幕上的说明执行操作。

步骤 3 在 CDO 中的**清单 (Inventory)** 页面上，点击**设备 (Devices)** 选项卡。

步骤 4 点击 **FTD** 设备。检查 FDM 管理 设备配置是否有更改，以便 CDO 可以复制 FDM 管理 设备的已部署配置并将其保存到 CDO 数据库。有关详细信息，请参阅读取、丢弃、检查和部署更改。

对 FDM 管理设备的 DHCP 寻址的 CDO 支持

如果我的 FDM 管理设备使用的 IP 地址发生更改会怎样？

Cisco Defense Orchestrator (CDO) 有许多自适应安全设备 (ASA) 和 FDM 管理设备客户，这些客户会使用其服务提供商使用 DHCP 提供的 IP 地址载入设备。

如果设备的 IP 地址因任何原因发生更改，无论是静态 IP 地址更改还是 DHCP 导致的 IP 地址更改，您都可以在 CDO 中更改设备的 IP 地址，然后重新连接设备。

该字段表达了对由 CDO 管理的分支机构部署 FDM 管理设备的情况的担忧，FDM 管理设备的外部接口上需要静态 IP，在某些 SE 看来，当 FDM 管理设备具有为外部接口配置的 DHCP 地址。

但是，这种情况不会影响拥有通往远程分支机构防火墙的 VPN 隧道的客户，并且我们知道，绝大多数客户都拥有从分支机构到数据中心的站点到站点隧道。在使用站点间 VPN 从设备连接到中心站点的情况下，外部接口上的 DHCP 不是问题，因为 CDO（和任何管理平台）可以通过其内部静态寻址

的接口（如已配置）连接到 FW。这是建议的做法，我们的 CDO 客户有许多（+1000）设备都采用此部署模式。

此外，通过 DHCP 发布接口 IP 地址这一事实并不妨碍客户使用该 IP 来管理设备。同样，这并非最佳选择，但在 CDO 中必须定期更改 IP 地址的体验并未被视为对客户的障碍。这种情况并非 CDO 独有，任何使用外部接口（包括 ASDM、FDM 或 SSH）的管理器都存在这种情况。

FDM 管理 设备许可类型

智能许可证类型

下表介绍了 FDM 管理 设备可用的许可证。

购买 FDM 管理 设备会自动附带基本许可证。其他所有许可证均是可选的。

许可证	持续时间	授予的功能
许可证（自动包含）	永久	订用期限的许可证中未包括的所有功能。 您还必须还指定是否在使用此令牌注册的产品上允许出口控制功能。仅在您的国家/地区满足出口控制标准时，才可以选择此选项。此选项控制您对高级加密和需要高级加密的功能的使用。
	基于期限	**入侵检测和防御 (Intrusion detection and prevention)** - 入侵策略用于分析网络流量是否存在入侵和漏洞利用，或者丢弃攻击性数据包。 **文件控制 (File control)** - 文件策略用于检测和选择性地阻止用户上传（发送）或下载（接收）特定类型的文件。通过面向 Firepower 的 AMP（需要恶意软件许可证），您可以检查和阻止包含恶意软件的文件。必须拥有许可证才可使用任何类型的文件策略。 **安全情报过滤 (Security Intelligence filtering)** - 将选定流量丢弃后，通过访问控制规则对流量进行分析。动态源可用于根据最新情报立即丢弃连接。

许可证	持续时间	授予的功能
恶意软件	基于期限	检查恶意软件的文件策略，将思科高级恶意软件保护 (AMP) 与适用于 Firepower 的 AMP（基于网络的高级恶意软件保护）和思科 Threat Grid 结合使用。 文件策略可以检测和阻止通过网络传输的文件中的恶意软件。
URL 许可证	基于期限	基于类别和信誉的 URL 过滤。 您可以对单个 URL 执行 URL 过滤，而不使用此许可证。
	基于期限或永久，取决于许可证类型	远程接入 VPN 配置。您的基础版许可证必须允许出口控制功能，以便配置远程接入 RA VPN。在注册设备时，您需要选择是否满足出口要求。 Firepower 设备管理器可以使用任何有效的 AnyConnect 许可证。可用功能不因许可证类型不同而不同。如果尚未购买，请参阅《远程访问 VPN 的许可要求》。 此外，请参阅《思科 AnyConnect 订购指南》 http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf。

虚拟 FDM 管理设备分层许可证

7.0 版引入了基于吞吐量要求和 RA VPN 会话限制的虚拟 FDM 管理设备性能分层智能许可支持。当虚拟 FDM 管理设备获得其中一个可用性能许可证的许可时，会出现两种情况：RA VPN 的会话限制由安装的虚拟 FDM 管理设备平台授权层确定，并通过速率限制器实施。

CDO 目前**不**完全支持分层智能许可；请参阅以下限制：

- 您无法通过 CDO 来修改分层许可证。您必须在 Firepower 设备管理器 UI 中进行更改。
- 如果注册由 云交付的防火墙管理中心 管理的虚拟 FDM 管理设备，则分层许可证选择会自动重置为**可变**，这是默认级别。
- 如果上载运行 7.0 或更高版本的虚拟 FDM 管理设备，并在上载过程中选择了**非**默认许可证的许可证，则分层许可证选择会自动重置为默认层级**可变**。

我们强烈建议您在载入设备后选择虚拟 FDM 管理设备许可证级别，以避免上述问题。有关详细信息，请参阅管理智能许可证。

查看设备的智能许可证

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择 FDM 管理设备以查看其当前许可证状态。

步骤 5 在右侧的设备操作窗格中，点击管理许可证。**管理许可证 (Manage Licenses)** 屏幕提供以下信息：

- **只能许可证代理状态 (Smart License Agent status)**：显示您使用的是 90 天评估许可证，还是已注册到思科智能软件管理器。. 智能许可证代理状态可能如下：
  - **“已连接”(Connected)**、**“足够的许可证”(Sufficient Licenses)** - 设备已成功联系许可证颁发机构并向其注册，该机构已向设备授予许可证授权。设备现在处于合规状态。
  - **不合规 (Out-of-Compliance)** - 设备没有可用的许可证授权。许可功能可继续工作。但您可以购买或释放其他授权，以便变为合规状态。
  - **授权已过期 (Authorization Expired)** - 设备已连续 90 天或更长时间未与许可颁发机构通信。许可功能可继续工作。在此状态下，智能许可证代理将重试其授权申请。如果重试成功，代理会进入“不合规”(Out-of-Compliance) 或“已授权”(Authorized) 状态，并开始新的授权周期。尝试手动同步设备。
- **许可证注册 (License Registration)**：允许您将智能许可证应用于已载入的 FDM 管理设备。注册后，您可以查看与思科智能软件管理器的连接状态，以及各类许可证的状态。
- **许可证状态 (License Status)**：显示可用于您的 FDM 管理设备的可选许可证的状态。您可以启用许可证以便使用该许可证控制的功能。

启用或禁用可选许可证

您可以在使用 90 天评估许可证或完整许可证的 FDM 管理设备上启用（注册）可选许可证。只有启用许可证后，才能使用该许可证控制的功能。

如果您不想再使用某个可选期限许可证包含的功能，可以禁用（解除）该许可证。禁用许可证会在思科智能软件管理器账户中将其释放，以便可将其应用到其他设备。

在评估模式下，您还可以启用可选许可证的评估版本并执行所有操作。在该模式下，只有注册设备，许可证才会注册到思科智能软件管理器。

Note 您无法在评估模式下启用许可证。

Before you begin

在禁用许可证之前，请确保它不在使用中。重写或删除需要该许可证的任何策略。

对于在高可用性配置中运行的设备，只需在主用设备上上启用或禁用许可证。当备用设备请求（或释放）必要许可证时，更改会在下一次部署配置时反映在备用设备上。启用许可证时，必须确保思科智能软件管理器账户具有足够的许可证，否则可能会造成一台设备合规，而另一台设备不合规。

要启用或禁用可选许可证，请执行以下程序：

Procedure

步骤 1 在**清单 (Inventory)**页面中，选择所需的 FDM 管理设备，然后点击**设备操作 (Device Actions)** 窗格中的**管理许可证 (Manage Licenses)**，系统将显示**管理许可证 (Manage Licenses)** 屏幕。

步骤 2 根据需要，点击每个可选许可证的滑块控件。一旦启用，许可证的状态显示为“正常”(OK)。

- **已启用 (Enabled)**：将许可证注册到您的思科智能软件管理器帐户，并启用控制的功能。现在，您可以配置和部署该许可证控制的策略了。
- **已禁用 (Disabled)**：取消许可证向思科智能软件管理器帐户的注册，并禁用控制的功能。新策略中无法配置这些功能，也不能再部署使用该功能的策略。

步骤 3 点击 **Save** 保存所做的更改。

可选许可证过期或被禁用的影响

如果可选许可证过期，您可以继续使用需要该许可证的功能。但是，该许可证将被标记为不合规，您需要购买许可证并将其添加到您的账户，才能使该许可证恢复合规状态。

如果禁用了某个可选许可证，系统将做出如下反应：

- **恶意软件许可证 (Malware license)**：系统会停止查询 AMP 云，还会停止确认从 AMP 云发送的追溯性事件。如果现有访问控制策略包括的文件策略会应用恶意软件检测，则无法重新部署现有访问控制策略。请注意，在禁用恶意软件许可证后的很短时间内，系统可以使用现有缓存文件处置情况。在时间窗过期后，系统将向这些文件分配不可用的处置情况。
- ：系统将不再应用入侵或文件控制策略。对于安全情报策略，系统不再应用策略并停止下载情报源更新。您无法重新部署需要该许可证的现有策略。
- **URL**：带有 URL 类别条件的访问控制规则会立即停止过滤 URL，且系统不会再下载对 URL 数据的更新。如果现有访问控制策略包括的规则带有基于类别和信誉的URL条件，则不能重新部署现有的访问控制策略。

- ：您不能编辑远程访问 VPN 配置，但可以将其删除。用户仍可使用 RA VPN 配置进行连接。但是，如果您更改设备注册，致使系统不再符合导出规定，则远程访问 VPN 配置会立即停止，且所有远程用户都无法通过 VPN 进行连接。

创建和导入 防火墙设备管理器 模型

思科防御协调器 提供将 CDO 租户上 FDM 管理设备的完整配置导出为 JSON 文件格式的功能。然后，您可以将此文件作为一个防火墙设备管理器模型导入到另一个租户，并将其应用于该租户上的新设备。当您想要在您管理的不同租户上使用 FDM 管理设备的配置时，此功能非常有用。

Note 如果 FDM 管理设备包含规则集，则在导出配置时，与规则集关联的共享规则将被修改为本地规则。稍后，当模型导入到另一个租户并应用于 FDM 管理设备时，您将在设备中看到本地规则。

导出 FDM 管理设备配置

如果您的 FDM 管理设备具有以下配置，则导出配置功能不可用：

- 高可用性
- Snort 3 已启用

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

步骤 2 点击 **设备 (Devices)** 选项卡以查找设备，或点击 **模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择一个 FDM 管理设备，然后在右侧窗格的**设备操作 (Device Actions)** 中，点击**导出配置 (Export Configuration)**。

导入 FDM 管理 设备配置

Procedure

步骤 1 在**清单 (Inventory)** 页面中，点击蓝色加号 (+) 按钮以导入配置。

步骤 2 点击**导入 (Import)** 以便导入配置进行离线管理。

步骤 3 选择设备类型作为 FTD。

步骤 4 点击**浏览 (Browse)** 并选择要上传的配置文件（JSON 格式）。

步骤 5 验证配置后，系统会提示您为设备或服务添加标签。有关详细信息，请参阅标签和过滤。

步骤 6 标记型号设备后，您可以在**清单 (Inventory)** 列表中查看它。

Note 根据配置的大小和其他设备或服务的数量，可能需要一些时间来分析配置。

从CDO删除设备

使用以下程序可从 中删除设备：CDO

过程

步骤 1 登录至 CDO。

步骤 2 导航至**清单 (Inventory)** 页面。

步骤 3 找到要删除的设备，然后选中设备行中的设备以将其选中。

步骤 4 在右侧的“设备操作”(Device Actions) 面板中，选择**删除 (Remove)**。

步骤 5 出现提示时，选择**确定 (OK)** 以确认删除所选设备。选择**取消 (Cancel)** 以使设备保持已载入状态。

请注意，必须同时删除 HA 对中的两台设备。FDM 管理点击 HA 对名称，而不是单个对等体。FDM 管理

导入设备的配置以进行离线管理

通过导入设备的配置以进行离线管理，您可以查看和优化设备的配置，而无需在网络中的实时设备上进行操作。CDO 还将这些上传的配置文件称为“模型”。

您可以将这些设备的配置导入到 CDO：

- 自适应安全设备 (ASA)。
- Firepower 威胁防御 (FTD)。请参阅创建和导入 FTD 模型。
- 像汇聚服务路由器 (ASR) 和集成服务路由器 (ISR) 的 Cisco IOS 设备。

备份 FDM 管理 设备

您可以使用 备份设备的系统配置，以便可以将设备恢复到以前的状态。思科防御协调器FDM管理备份仅包括配置，而不是系统软件。如果需要完全重新映像设备，您需要重新安装软件，然后才能上传备份和恢复配置。CDO 会保存设备的最近 5 次备份。进行新的备份时，会删除最早的备份，以便存储最新的备份。

Note 备份不包括管理 IP 地址配置。因此，恢复备份文件时，不会从备份副本中替换管理地址。这可以确保保存对地址所做的任何更改，并且还可以在其他网段的其他设备上恢复配置。

在备份期间将锁定配置数据库。在备份期间不能更改配置，但可以查看策略、控制面板等。在恢复期间，系统完全不可用。

要使设备之间的备份计划一致，您可以配置自己的默认备份计划。为特定设备安排备份时，可以使用自己的默认设置或进行更改。您可以安排定期备份，频率从每天到每月一次，并且可以执行按需备份。您还可以下载备份，然后使用设备管理器进行恢复。威胁防御

使用 CDO 备份和恢复 FDM 管理 设备的要求和最佳实践

- 可以备份运行 6.5 及更高版本软件的设备。CDOFDM 管理
- 设备必须使用注册密钥自行激活。FDM 管理CDO
- 仅当两台设备的型号相同且运行相同版本的软件（包括内部版本号，而不仅仅是相同的发布版）时，才可将备份恢复到替换设备上。例如，运行软件版本 6.6.0-90 的设备的备份只能恢复到运行 6.6.0-90 的设备。FDM 管理FDM 管理请勿使用备份和恢复过程在设备之间复制配置。备份文件包含唯一标识设备的信息，所以不能按此方式进行共享。
- 要在 CDO 中使用 Secure Firewall Threat Defense 备份功能，威胁防御 需要根据您的租户区域访问这些 CDO URL 之一。
  - edge.us.cdo.cisco.com
  - edge.eu.cdo.cisco.com
  - edge.apj.cdo.cisco.com
- 确保端口 443 具有 HTTPS 协议的外部和出站访问权限。如果端口被防火墙阻止，备份和恢复过程可能会失败。

最佳实践

您要备份的设备应处于已同步状态。 会从 设备备份设备的配置，而不是从中备份设备的配置。CDOCDOCDO因此，如果设备处于“未同步”状态，则不会备份上的更改。CDO如果设备处于“检测到冲突”状态，系统将备份这些更改。

相关信息：

- 配置默认定期备份计划
- 为单个设备配置定期备份计划FDM 管理
- 按需备份设备FDM 管理
- 下载设备备份
- 编辑备份
- 将备份恢复到设备FDM 管理, on page 208

按需备份设备FDM 管理

此程序介绍如何备份设备，以便在需要时可以将其恢复。FDM 管理

准备工作

在备份设备之前，请查看这些要求和最佳实践。备份 FDM 管理 设备, on page 203FDM 管理

操作步骤

Procedure

步骤 1 （可选）为备份创建更改请求管理。

步骤 2 在导航栏中，点击**清单 (Inventory)**。

步骤 3 点击**设备**选项卡。

步骤 4 点击 **FTD** 选项卡，然后选择要备份的设备。

步骤 5 在右侧的设备操作窗格中，点击管理备份。

步骤 6 单击**立即备份 (Backup Now)**。设备进入“备份配置”状态。

在备份完成后，思科防御协调器 会显示备份开始前的设备配置状态。您还可以打开更改日志页面，查找描述为“备份已成功完成”(Backup completed successfully) 的最新更改日志记录。

如果在步骤 1 中创建了更改请求，则您还可以按该值进行过滤以查找更改日志条目。

步骤 7 如果在步骤 1 中创建了更改请求，请清除更改请求值，以免在无意中将更多更改与更改请求关联。

为单个设备配置定期备份计划FDM 管理

准备工作

在备份设备之前，请查看这些要求和最佳实践。备份 FDM 管理 设备, on page 203FDM 管理

操作步骤

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **FTD** 选项卡，然后选择要备份的设备。

步骤 4 在右侧的设备操作窗格中，点击管理备份。

步骤 5 在**设备备份 (Device Backups)** 页面中，点击**设置定期备份 (Set Recurring Backup)** 或点击定期备份字段中的计划。CDO 显示租户上所有 FDM 管理设备的默认备份计划。有关详细信息，请参阅配置默认定期备份计划。

步骤 6 选择一天中要进行备份的时间（24 小时制）。请注意，以协调世界时 (UTC) 来安排时间。

步骤 7 在频率 (Frequency) 字段中，选择每日、每周或每月备份。

- 每日备份 (Daily backups)：为计划的备份时间指定名称和说明。
- 每周备份 (Weekly backups)：选中要在星期几进行备份。为计划的备份时间指定名称和说明。
- 每月备份 (Monthly backups)：点击“当月的天数”(Days of Month) 字段，然后添加要计划备份的每月日期。注意：如果输入第 31 天，但一个月中没有 31 天，则不会进行备份。为计划的备份时间指定名称和说明。

步骤 8 点击**保存 (Save)**。请注意，在“设备备份”(Device Backup) 页面上，定期备份字段将替换为您设置的备份计划，并反映您的本地时间。

下载设备备份

此程序介绍如何下载包含设备备份的 .tar 文件。FDM 管理

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 FTD 选项卡和要下载其备份的设备。

步骤 4 在右侧的操作窗格中，点击管理备份。

步骤 5 选择要下载的备份，然后在其行中点击生成下载链接 (Generate Download Link) 按钮。按钮更改为“下载备份映像”。

步骤 6 该按钮现在显示为“下载备份映像”。执行以下操作之一：

- 如果您使用的设备也可以访问要恢复的设备的防火墙设备管理器，请点击**下载备份映像 (Download Backup Image)** 按钮并保存下载的文件。使用您会记住的名称保存它。
- 如果您不在可以访问要恢复的设备的 FDM 的设备上：

  a. 右键点击 Download Backup Image（下载备份映像）按钮，然后复制链接地址。

  Important 点击“生成下载链接”(Generate Download Link) 按钮 15 分钟后，链接地址将到期。

  b. 在也将访问要将映像恢复到的 Secure Firewall Threat Defense 的 防火墙设备管理器 设备上打开浏览器。

c. 在浏览器地址栏中输入下载链接，并将备份文件下载到该设备。使用您会记住的名称保存它。

编辑备份

此程序允许您编辑成功下载设备的名称或说明。FDM 管理

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **FTD** 选项卡，然后选择要编辑的设备。

步骤 4 在右侧的操作窗格中，点击管理备份。

步骤 5 选择要编辑的备份及其所在的行，点击编辑图标。

步骤 6 更改备份的名称或说明。您可以在“设备备份”页面中查看新信息。

删除备份

CDO 会保存为设备所进行的最后 5 次备份。进行新的备份时，会删除最早的备份，以便存储最新的备份。删除现有备份可帮助您管理保留和删除的备份。

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **FTD** 选项卡，然后选择要删除的设备。

步骤 4 在右侧的操作窗格中，点击管理备份。

步骤 5 选择要删除的备份及其所在的行，点击垃圾箱图标 。

步骤 6 点击**确定 (OK)** 以进行确认。

管理设备备份

可以在“设备备份”(Device Backups) 页面中查看您使用 思科防御协调器 的 FDM 管理设备的备份：

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **FTD** 选项卡。

步骤 4 点击过滤器图标并选中设备/服务下的 FDM，以仅查看设备表中的 FDM 管理设备。

步骤 5 选择所需的设备。

步骤 6 在**设备操作 (Device Actions)** 窗格中，点击**管理备份 (Manage Backups)**。您最多将看到该设备的 5 个最新备份。

What to do next

如果要恢复备份，请参阅将备份恢复到设备FDM 管理, on page 208。

将备份恢复到设备FDM 管理

在恢复受管设备的备份之前，请查看此信息。FDM 管理威胁防御

- 在将备份恢复到设备之前，请查看这些要求和最佳实践。备份 FDM 管理 设备, on page 203FDM 管理 威胁防御
- 如果设备中没有要恢复的备份副本，必须先**上传**该备份，才能进行恢复。
- 在恢复期间，系统完全不可用。恢复备份后，设备会重新启动。
- 此程序假定您已准备好将设备备份到 设备。
- 当设备属于高可用性对的一部分时，您无法恢复备份。您必须首先从“设备”(Device)>“高可用性”(High Availability) 页面中断高可用性，然后才能恢复备份。如果备份包括高可用性配置，设备将重新加入高可用性组。不要在两台设备上恢复相同备份，因为这两台设备都会变成活动状态。相反，您要在想要首先恢复活动状态的设备上恢复备份，然后在另一台设备上恢复等效备份。

Note 备份不包括管理 IP 地址配置。因此，恢复备份文件时，不会从备份副本中替换管理地址。这可以确保保存对地址所做的任何更改，并且还可以在其他网段的其他设备上恢复配置。

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **FTD** 选项卡，然后选择要恢复的设备。

步骤 4 在右侧的设备操作窗格中，点击管理备份。

步骤 5 选择您要恢复的备份。在相应行中，点击生成下载链接 (Generate Download Link) 按钮。

Note 点击“生成下载链接”(Generate Download Link) 按钮 15 分钟后，链接地址将到期。

步骤 6 该按钮现在显示为“下载备份映像”。执行以下操作之一：

- 如果您使用的设备也可以访问要恢复的设备的防火墙设备管理器，请点击**下载备份映像 (Download Backup Image)** 按钮并保存下载的文件。使用您会记住的名称保存它。
- 如果您不在可以访问要恢复的设备的 防火墙设备管理器 的设备上：
  a. 右键点击 Download Backup Image（下载备份映像）按钮，然后复制链接地址。
  b. 在也将访问要将映像恢复到的 防火墙设备管理器 的设备上打开浏览器。
  c. 在浏览器地址栏中输入下载链接，并将备份文件下载到该设备。使用您会记住的名称保存它。

步骤 7 登录您要恢复的设备的 防火墙设备管理器。

步骤 8 打开 6.5 或更高版本的《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》。导航至“系统管理”一章，然后搜索恢复备份。按照这些说明恢复您刚下载到设备的映像。FDM 管理

Tip 您需要将映像上传到 防火墙设备管理器 才能恢复映像。

步骤 9 按照 防火墙设备管理器 中的提示操作。恢复开始时，浏览器会断开与 防火墙设备管理器 的连接。恢复完成后，设备将重新启动。

相关信息：

- 备份 FDM 管理 设备
- 按需备份设备FDM 管理
- 为单个设备配置定期备份计划FDM 管理
- 下载设备备份
- 编辑备份

FDM 软件升级路径

升级 FDM 版本

如果您使用 CDO 升级您的 FDM 管理 防火墙，CDO 会确定您可以升级到哪个版本，您将不需要本主题。如果您维护自己的 FDM 映像存储库并使用自己的映像升级 FDM 托管的设备，则本主题将介绍可用的升级路径。

您可以将 FDM 托管的设备直接从一个主要版本或维护版本升级到另一个版本；例如，版本 6.4.0 > 6.5.0 或版本 6.4.0 > 7.0.1。您不需要运行任何特定级别的补丁。

如果无法直接升级，则升级路径必须包括中间版本，例如版本 6.4.0 > 7.0.0 > 7.1.0。

Table 11: 主要版本的升级路径

目标版本	可以升级到目标版本的最旧版本
7.3.x	7.0.0
7.2.x	6.6.0
7.1.x	6.5.0
7.0.x	6.4.0
6.7.x	6.4.0
6.6.x	6.4.0
6.5.0	6.4.0

修补 FDM 托管的设备

您无法直接从一个版本的修补程序升级到另一个版本的修补程序，例如从版本 6.4.0.1 > 6.5.0.1。您必须先升级到主要版本，然后再修补该版本。例如，您必须从版本 6.4.0.1 升级 > 6.5.0 > 6.5.0.1。

Firepower 热补丁

CDO 不支持修补程序更新或安装。如果有适用于您的设备型号或软件版本的热补丁，我们强烈建议使用已配置的管理器控制面板或 UI。在设备上安装热补丁后，CDO 会检测到带外配置更改。

删除 FDM 升级

您不能使用 CDO 删除或降级任何版本类型，无论是主版本、维护版本还是补丁。

从 Secure Firewall Threat Defense 版本 6.7.0 开始，您可以使用 Firepower 设备管理器或 FTD CLI 将成功升级的设备恢复到上次主要或维护升级之前的状态（也称为快照）。修补后恢复必然也会删除修补程序。恢复后，您必须重新应用在**升级**和恢复之间所做的任何配置更改。**请注意，要将主要或维护升级恢复到 FDM 版本 6.5.0 至 6.6.x，必须重新映像**。有关更多信息，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》中的“系统许可”一章。

删除 FDM 补丁

您无法使用 CDO 或 FDM 删除 FDM 补丁。要删除修补程序，必须重新映像到主版本或维护版本。

Snort 升级

Snort 是产品的主要检测引擎，为了您的方便，它已打包到 Secure Firewall Threat Defense 软件中。版本 6.7 引入了可随时升级或恢复的软件包更新。虽然可以自由切换 Snort 版本，但 Snort 2.0 中的某些

入侵规则未在 Snort 3.0 中提供，反之亦然。我们强烈建议阅读《适用于版本 6.7.0 的 Firepower 设备管理器配置指南》中的差异，以了解详细信息。

要继续升级 FDM 管理 设备以使用 Snort 3 或从 CDO UI 从 Snort 3 恢复到 Snort 2，请分别参阅 升级到 Snort 3.0 和从 Snort 3.0 恢复 FDM 管理 设备。

其他升级限制

2100 系列设备

仅当运行设备模式时，CDO 才能升级 Firepower 2100 系列设备。

- Firepower 威胁防御设备始终处于设备模式。

下一步做什么

有关这些命令的更详细讨论，请参阅《思科 Firepower 2100 入门指南》。https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp2100/firepower-2100-gsg/asa-platform.html

4100 和 9300 系列设备

CDO 不支持 4100 或 9300 系列设备的升级。您必须在 CDO 之外升级这些设备。

相关信息：

- FDM 管理 设备升级前提条件
- 升级单个 FTD 设备
- 批量 FDM 管理 设备升级
- 升级 FDM 管理 高可用性对

FDM 管理 设备升级前提条件

思科防御协调器 (CDO) 提供了一个向导，可帮助您升级单个设备或 HA 对上安装的 防火墙设备管理器 (FDM) 映像。

该向导将指导您选择兼容的映像，安装这些映像，然后重新启动设备以完成升级。我们会验证您在 CDO 上选择的映像是否是复制到并安装在您的 FDM 管理 设备上的映像，从而确保升级过程的安全。我们强烈建议您要升级的 FDM 管理 设备具有对互联网的出站访问权限。

如果您的FDM 管理 设备没有互联网出站访问权限，您可以从Cisco.com 下载所需的映像，将其存储在您自己的存储库中，为升级向导提供这些映像的自定义URL，然后CDO 使用这些映像执行升级。但是，在这种情况下，您需要确定要升级到的映像。CDO 不会执行映像完整性检查或磁盘空间检查。

配置必备条件

- 需要在 FDM 管理 设备上启用 DNS。有关详细信息，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》中**系统管理**一章的“配置 DNS”部分。
- 如果您使用 CDO 的映像存储库中的升级映像， FDM 管理 设备应该能够访问互联网。
- FDM 管理 设备已被成功载入 CDO。
- FDM 管理 设备无法访问。
- FDM 管理 设备已同步。
  - 如果您更新的设备在CDO中有待处理的更改，并且您不接受更改，则在升级完成后，待处理的更改将会丢失。最佳实践是在升级之前部署所有待处理的更改。
  - 如果您在 防火墙设备管理器 中暂存了更改，并且设备未同步，则 CDO 中的升级将在资格检查时失败。

运行 FTD 的 4100 和 9300 系列

CDO 不支持 4100 或 9300 系列设备的升级。您必须在 CDO 外部升级这些设备。

软件和硬件要求

CDO 云管理平台。软件更新随时间推移而发布，通常不依赖于硬件。有关支持的硬件类型的信息，请参阅 CDO 支持的软件和硬件。

运行防火墙设备管理器软件的设备具有推荐的升级路径，以实现最佳性能。有关详细信息，请参阅 FDM 软件升级路径。

升级说明

您无法在设备升级时将更改部署到设备。

相关信息：

- FDM 软件升级路径
- 升级单个 FTD 设备
- 批量 FDM 管理 设备升级
- 升级 FDM 管理 高可用性对

升级单个 FTD 设备

准备工作

在升级之前，请务必仔细阅读 FDM 管理 设备升级前提条件、FDM 软件升级路径以及 CDO 支持的软件和硬件。本文档介绍了在升级到所需的 Firepower 软件版本之前应了解的所有要求和警告。

使用 思科防御协调器 存储库中的映像升级单个 FDM 管理 设备

按照以下程序使用存储在 CDO 存储库中的软件映像升级独立 FDM 管理 设备

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择想要升级的设备。

步骤 5 在**设备操作 (Device Actions)** 窗格中，点击**升级 (Upgrade)**。

步骤 6 在步骤 1 中，点击**使用 CDO 映像存储库 (Use CDO Image Repository)** 以选择要升级到的软件映像，然后点击**继续 (Continue)**。系统只会显示与您可以升级的设备兼容的选项。

步骤 7 在步骤2中，确认您的选择，并决定是仅将映像下载到设备，还是复制映像、安装并重新启动设备。

步骤 8 准备就绪后，点击**执行升级 (Perform Upgrade)**。在“资产”页面中，正在升级的设备具有“正在进行升级”配置状态。

Warning 如果您决定在升级过程中取消升级，请点击“升级”页面中的中止升级。如果在升级开始后取消升级，CDO 不会部署或检查设备中的更改，设备也不会回滚到之前的配置。这可能会导致设备进入不正常状态。如果您在升级过程中遇到任何问题，请联系思科 TAC。

步骤 9 或者，如果您希望 CDO 稍后执行升级，请选中计划升级复选框。点击该字段可选择未来的日期和时间。完成后，点击“计划升级”(Schedule Upgrade) 按钮。

步骤 10 查看通知选项卡，了解批量升级操作的进度。如果您想了解有关批量升级作业中操作成功与否的详细信息，请点击蓝色查看链接，系统会将您定向到作业页面。

步骤 11 升级系统数据库。您必须在 防火墙设备管理器 中执行此步骤。有关详细信息，请参阅《适用于 Firepower 设备管理器版本 6.4 的 Cisco Firepower Threat Defense 配置指南》中的“更新系统数据库”。

使用您自己的存储库中的映像升级单个设备FDM 管理

按照以下程序升级使用 URL 协议的独立设备以查找软件映像：FDM 管理

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择想要升级的设备。

步骤 5 在**设备操作 (Device Actions)** 窗格中，点击**升级 (Upgrade)**。

步骤 6 在步骤 1 中，点击**指定映像 URL (Specify Image URL)** 以选择要升级到的软件映像，然后点击**继续 (Continue)**。系统只会显示与您可以升级的设备兼容的选项。

步骤 7 在步骤2中，确认您的选择，并决定是仅将映像下载到设备，还是复制映像、安装并重新启动设备。

步骤 8 准备就绪后，点击**执行升级 (Perform Upgrade)**。在“资产”页面中，正在升级的设备具有“正在进行升级”配置状态。

Warning 如果您决定在升级过程中取消升级，请点击“升级”页面中的中止升级。如果在升级开始后取消升级，思科防御协调器 不会部署或检查设备中的更改，设备也不会回滚到之前的配置。这可能会导致设备进入不正常状态。如果您在升级过程中遇到任何问题，请联系思科 TAC。

步骤 9 或者，如果您希望CDO稍后执行升级，请选中计划升级复选框。点击该字段可选择未来的日期和时间。完成后，点击“计划升级”(Schedule Upgrade) 按钮。

步骤 10 查看通知选项卡，了解批量升级操作的进度。如果您想了解有关批量升级作业中操作成功与否的详细信息，请点击蓝色查看链接，系统会将您定向到作业页面。

步骤 11 升级系统数据库。您必须在 防火墙设备管理器 中执行此步骤。有关详细信息，请参阅《适用于 Firepower 设备管理器版本 6.4 的 Cisco Firepower Threat Defense 配置指南》中的“更新系统数据库”。

监控升级过程

您可以通过在“资产”页面上选择该设备并点击升级按钮来查看单个设备的进度。CDO会将您引导至该设备的“设备升级”页面。

只要升级失败，CDO 就会显示一条消息。CDO 不会自动重新启动升级过程。

Warning 升级具有自签名证书的设备可能会遇到问题；有关详细信息，请参阅检测到新证书

批量 FDM 管理 设备升级

准备工作

在升级之前，请务必仔细阅读 FDM 管理 设备升级前提条件、FDM 软件升级路径以及 CDO 支持的软件和硬件。本文档介绍在升级到所需的 Firepower 软件版本之前应了解的所有要求和警告。

Note 仅当设备都升级到同一软件版本时，才能批量升级 FDM 管理 设备。

使用 思科防御协调器 存储库中的映像升级批量 FDM 管理 设备

按照以下程序使用存储在 CDO 存储库中的软件映像升级多个 FDM 管理 设备：

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 使用过滤器缩小可能要包含在批量升级中的设备列表。

步骤 5 从过滤后的设备列表中，选择要升级的设备。

步骤 6 在**设备操作 (Device Actions)** 窗格中，点击**升级 (Upgrade)**。

步骤 7 在“批量设备升级”(Bulk Device Upgrade) 页面上，您会看到可升级的设备。如果您选择的任何设备不可升级，CDO 会为您提供一个链接，供您查看不可升级的设备。

步骤 8 或者，如果您希望CDO稍后执行升级，请选中计划升级复选框。点击该字段可选择未来的日期和时间。完成后，点击“计划升级”(Schedule Upgrade) 按钮。

步骤 9 在步骤 1 中，点击**使用 CDO 映像存储库 (Use CDO Image Repository)** 以选择要升级到的软件映像。系统只会显示与您可以升级的设备兼容的选项。点击**继续 (Continue)**。

步骤 10 在步骤2中，确认您的选择，并决定是仅将映像下载到设备，还是复制映像、安装并重新启动设备。

步骤 11 准备就绪后，点击**执行升级 (Perform Upgrade)**。在“资产”页面中，正在升级的设备具有“正在进行升级”配置状态。

Warning 如果您决定在升级过程中取消升级，请点击“升级”页面中的中止升级。如果您在升级开始后取消升级，CDO不会部署或轮询设备中的更改。取消升级后，设备也不会回滚到之前的配置。这可能会导致设备进入不正常状态。如果您在升级过程中遇到任何问题，请联系思科 TAC。

步骤 12 查看通知选项卡，了解批量升级操作的进度。如果您想了解有关批量升级作业中操作成功与否的详细信息，请点击蓝色查看链接，系统会将您定向到作业页面。

步骤 13 升级系统数据库。您必须在防火墙设备管理器中执行此步骤。有关设备运行的版本，请参阅《适用于 Firepower 设备管理器的 Cisco Firepower Threat Defense 配置指南》中的**更新系统数据库**。

使用您自己的存储库中的映像升级批量 FDM 管理 设备

按照以下程序使用 URL 协议升级多个 FDM 管理 设备以查找软件映像：

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 使用过滤器缩小可能要包含在批量升级中的设备列表。

步骤 5 从过滤后的设备列表中，选择要升级的设备。

步骤 6 在**设备操作 (Device Actions)** 窗格中，点击**升级 (Upgrade)**。

步骤 7 在“批量设备升级”(Bulk Device Upgrade) 页面上，您会看到可升级的设备。如果您选择的任何设备不可升级，思科防御协调器 会为您提供一个链接，供您查看不可升级的设备。

步骤 8 或者，如果您希望CDO稍后执行升级，请选中计划升级复选框。点击该字段可选择未来的日期和时间。完成后，点击“计划升级”(Schedule Upgrade) 按钮。

步骤 9 在步骤 1 中，点击**指定映像 URL (Specify Image URL)** 以选择要升级到的软件映像，然后点击**继续 (Continue)**。

步骤 10 在步骤2中，确认您的选择，并决定是仅将映像下载到设备，还是复制映像、安装并重新启动设备。

步骤 11 准备就绪后，点击**执行升级 (Perform Upgrade)**。在**资产**页面中，正在升级的设备具有“正在进行升级”配置状态。

Warning 如果您决定在升级过程中取消升级，请点击“升级”页面中的**中止升级**。如果在升级开始后取消升级，CDO不会部署或轮询设备中的更改，设备也不会回滚到之前的配置。这可能会导致设备进入不正常状态。如果您在升级过程中遇到任何问题，请联系思科TAC。

步骤 12 查看通知选项卡，了解批量升级操作的进度。如果您想了解有关批量升级作业中操作成功与否的详细信息，请点击蓝色查看链接，系统会将您定向到作业页面。

步骤 13 升级系统数据库。您必须在 防火墙设备管理器 中执行此步骤。有关详细信息，请参阅《适用于 Firepower 设备管理器版本 6.4 的 Cisco Firepower Threat Defense 配置指南》中的“更新系统数据库”。

监控批量升级过程

您可以通过在**资产**页面上选择该设备并点击升级按钮来查看批量升级中包含的单个设备的进度。您还可以通过点击导航窗格中的**作业**并展开批量操作来查看进度详细信息。

只要升级失败，CDO 就会显示一条消息。CDO 不会自动重新启动升级过程。

升级 FDM 管理 高可用性对

在不中断流量的情况下升级 HA 对；备用设备在升级辅助设备时继续处理流量检测。

升级 HA 对时，CDO 会执行资格检查并在开始升级之前复制或识别映像位置。高可用性对中的辅助设备首先升级，即使它当前是主用设备；如果辅助设备是主用设备，则配对的设备会自动切换升级过程的角色。辅助设备成功升级后，设备会切换角色，然后新的备用设备会升级。升级完成后，设备会自动配置，因此主用设备处于活动状态，辅助设备处于备用状态。

我们不建议在升级过程中部署到 HA 对。

准备工作

- 在升级之前，将所有待处理的更改部署到主用设备。
- 确保在升级期间没有正在运行的任务。
- 高可用性对中的两台设备都运行正常。
- 确认您已准备好升级；您无法在 CDO 中回滚到以前的版本。
- 仔细阅读 FDM 管理 设备升级前提条件、FDM 软件升级路径以及 CDO 支持的软件和硬件以查看在升级过程中可能出现的任何要求和警告。

使用 思科防御协调器 存储库中的映像升级 FDM 管理 HA 对

按照以下程序使用存储在 CDO 存储库中的软件映像升级 FDM 管理 HA 对：

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择要升级的 HA 对。

步骤 5 在**设备操作 (Device Actions)** 窗格中，点击**升级 (Upgrade)**。

步骤 6 在步骤 1 中，点击**使用 CDO 映像存储库 (Use CDO Image Repository)** 以选择要升级到的软件映像，然后点击**继续 (Continue)**。系统只会显示与您可以升级的设备兼容的选项。

步骤 7 在步骤2中，确认您的选择，并决定是仅将映像下载到设备，还是复制映像、安装并重新启动设备。

步骤 8 准备就绪后，点击**执行升级 (Perform Upgrade)**。在“资产”页面中，正在升级的设备具有“正在进行升级”配置状态。

Warning 如果您决定在升级过程中取消升级，请点击“升级”页面中的中止升级。如果在升级开始后取消升级，CDO不会从设备部署或轮询更改，并且设备不会回滚到之前的配置。这可能会导致设备进入不正常状态。如果您在升级过程中遇到任何问题，请联系思科TAC。

步骤 9 或者，如果您希望CDO稍后执行升级，请选中计划升级复选框。点击该字段可选择未来的日期和时间。完成后，点击“计划升级”(Schedule Upgrade) 按钮。

步骤 10 查看通知选项卡，了解批量升级操作的进度。如果您想了解有关批量升级作业中操作成功与否的详细信息，请点击蓝色查看链接，系统会将您定向到作业页面。

步骤 11 升级系统数据库。您必须在 FDM 中执行此步骤。有关详细信息，请参阅《适用于 Firepower 设备管理器版本 6.4 的 Cisco Firepower Threat Defense 配置指南》中的“更新系统数据库”。

使用您自己的存储库中的映像升级 HA 对FDM 管理

按照以下程序使用 URL 协议升级 HA 对以查找软件映像：FDM 管理

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择要升级的 HA 对。

步骤 5 在**设备操作 (Device Actions)** 窗格中，点击**升级 (Upgrade)**。

步骤 6 在步骤 1 中，点击**指定映像 URL (Specify Image URL)** 以选择要升级到的软件映像，然后点击**继续 (Continue)**。系统只会显示与您可以升级的设备兼容的选项。

步骤 7 在步骤2中，确认您的选择，并决定是仅将映像下载到设备，还是复制映像、安装并重新启动设备。

步骤 8 准备就绪后，点击**执行升级 (Perform Upgrade)**。在“资产”页面中，正在升级的设备具有“正在进行升级”配置状态。

Warning 如果您决定在升级过程中取消升级，请点击“升级”页面中的中止升级。如果在升级开始后取消升级，思科防御协调器 不会从设备部署或轮询更改，并且设备不会回滚到之前的配置。这可能会导致设备进入不正常状态。如果您在升级过程中遇到任何问题，请联系思科 TAC。

步骤 9 或者，如果您希望CDO稍后执行升级，请选中计划升级复选框。点击该字段可选择未来的日期和时间。完成后，点击“计划升级”(Schedule Upgrade) 按钮。

步骤 10 查看通知选项卡，了解批量升级操作的进度。如果您想了解有关批量升级作业中操作成功与否的详细信息，请点击蓝色查看链接，系统会将您定向到作业页面。

步骤 11 升级系统数据库。您必须在 防火墙设备管理器 中执行此步骤。有关详细信息，请参阅《适用于 Firepower 设备管理器版本 6.4 的 Cisco Firepower Threat Defense 配置指南》中的“更新系统数据库”。

监控升级过程

您可以通过在**清单 (Inventory)** 页面上选择该设备并点击升级按钮来查看单个设备的进度。思科防御协调器 会带您前往该设备的**设备升级 (Device Upgrade)** 页面。

升级期间，系统在更新系统库时挂起HA，其中包括自动部署，而且在整个升级过程中可能都不会处于正常运行状态。这是预期行为。在此过程的最后部分中，设备可用于SSH连接，因此，如果在应用升级后不久登录，则可能会看见挂起状态的HA。如果系统在升级过程中遇到问题，并且HA对似乎已暂停，请从主用设备的 防火墙设备管理器 控制台手动恢复 HA。

Note 如果升级在任何时候失败，CDO 会显示一条消息。CDO 不会自动重新启动升级过程。

Warning 升级具有自签名证书的设备可能会遇到问题；有关详细信息，请参阅检测到新证书。

升级到 Snort 3.0

Snort 3 是使用开源入侵防御系统 (IPS) 的最新 snort 引擎或强大的预处理器，适用于 Firepower 版本 6.7 及更高版本。Snort 引擎使用一系列规则来帮助定义恶意网络活动，并使用这些规则查找与其匹配的数据包，并为用户生成警报，理想情况下用作数据包嗅探器、数据包记录器或更传统的 aa独立网络 IPS。

使用 Snort 3，您现在可以创建自定义入侵策略；每个运行 Snort 3 的 FDM 管理 设备都有一组从思科 Talos 情报组 (Talos) 预定义的入侵策略。Snort 3 可以更改这些默认策略，但我们强烈建议在基本策略的基础上进行构建，以获得更强大的策略。

您无法使用 Snort 2 创建自定义策略。

从 Snort 2 切换到 Snort 3

您可以自由切换 Snort 版本，虽然 Snort 2.0 中的某些入侵规则未在 Snort 3.0 中提供，反之亦然。如果对现有规则更改了规则操作，则在从 Snort 3 切换到 Snort 2 或再次切换回 Snort 3 时，不会保留该更改。您对两个版本中现有规则的规则操作更改都将被保留。请注意，Snort 3 与 Snort 2 中的规则之间的映射可以是一对一或一对多的，因此系统将尽可能保留更改。

如果您选择从 Snort 2 升级到 Snort 3，请注意，升级 Snort 引擎相当于系统升级。我们强烈建议在维护窗口期间进行升级，以最大限度地减少网络流量监控的中断。有关切换snort版本将如何影响规则处理流量的方式，请参阅《*Firepower* 设备管理器配置指南》中的管理入侵策略 (Snort3) 。

Tip 您可以在**清单 (Inventory)** 页面上按 Snort 版本进行过滤，所选设备的详细信息窗口将显示设备上运行的当前版本。

Snort 3 限制

许可证要求

要允许 Snort 引擎处理流量以进行入侵和恶意软件分析，必须为 FDM 管理 设备启用 **许可证**。要通过 防火墙设备管理器 启用此许可证，请登录 防火墙设备管理器 UI 并导航至 **设备 (Device)** > **视图配置 (View Configuration)** > **启用/禁用 (Enable/Disable)**，然后启用 许可证。

硬件支持

以下设备支持 Snort 3：

- FTD 1000 系列
- FTD 2100 系列
- FTD 4100 系列
- FTD 虚拟与 AWS
- FTD 虚拟与 Azure
- 具备 FTD 的 ASA 5500-X 系列

软件支持

设备**必须**至少运行 防火墙设备管理器 版本 6.7。思科防御协调器 支持运行版本 6.7 及更高版本的设备的 Snort 3 功能。

对于 FTD 1000 和 2000 系列，请参阅 FXOS 捆绑支持，了解有关 FXOS 补丁支持的详细信息。

配置限制

如果您的设备具有以下配置，CDO 不支持升级到 Snort 3：

- 设备未运行至少版本 6.7。
- 如果设备有待处理的更改。在升级之前部署任何更改。
- 如果设备当前正在升级。在设备同步之前，请勿尝试升级或部署到设备。
- 如果设备配置了虚拟路由器。

Note 如果升级或恢复 Snort 版本，系统会自动部署以实施 Snort 2 入侵策略和 Snort 3 入侵策略之间的更改。

规则集和 Snort 3

请注意，Snort 3 目前没有完整的功能支持。CDO 规则集在 Snort 3 设备上不支持。如果您同时将设备升级到 防火墙设备管理器 6.7 或更高版本，并从 Snort 2 升级到 Snort 3，则在升级之前配置的任何规则集都将被分解，其中的规则将另存为单独的规则。

有关为 Snort 3 配置的设备的完整规则集支持列表，请参阅规则集, on page 385。

同时升级设备和入侵防御引擎

CDO 允许您将设备升级到版本 6.7 和 Snort 3。使用以下程序升级 FTD 系统：

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **FTD** 选项卡，然后选择要升级的设备。

步骤 4 在右侧的**设备操作 (Devices Actions)** 窗格中，点击**升级 (Upgrade)**。

步骤 5 将升级切换开关设置为 FTD 系统升级。

步骤 6 （可选）如果您希望 CDO 稍后执行升级，请选中**计划升级 (Schedule Upgrade)** 复选框。点击该字段以选择未来的日期和时间。

步骤 7 在步骤 1 中，选择升级方法。使用 CDO 映像存储库和您自己的存储库中的映像：

- **使用 CDO 映像存储库 (Use CDO Image Repository)** - 点击此选项可选择要升级到的软件映像，然后点击**继续 (Continue)**。系统只会显示与您可以升级的设备兼容的选项。
- 指定映像 URL - 点击此选项可选择当前存储在您自己的存储库中的软件映像，然后点击继续。系统只会显示与您可以升级的设备兼容的选项。

步骤 8 在步骤2中，确认您的选择，并决定是仅将映像下载到设备，还是复制映像、安装并重新启动设备。

步骤 9 选中升级到 Snort 3 引擎。

步骤 10 准备就绪后，点击**执行升级 (Perform Upgrade)**。在“资产”页面中，正在升级的设备具有“正在进行升级”配置状态。

Warning 如果您决定在升级过程中取消升级，请点击“升级”页面中的中止升级。如果在升级开始后取消升级，CDO不会部署或检查设备中的更改，设备也不会回滚到之前的配置。这可能会导致设备进入不正常状态。如果您在升级过程中遇到任何问题，请联系思科TAC。

升级入侵防御引擎

对于已运行版本 6.7 和 Snort 2 的设备，请使用以下程序将 Snort 引擎更新为版本 3：

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

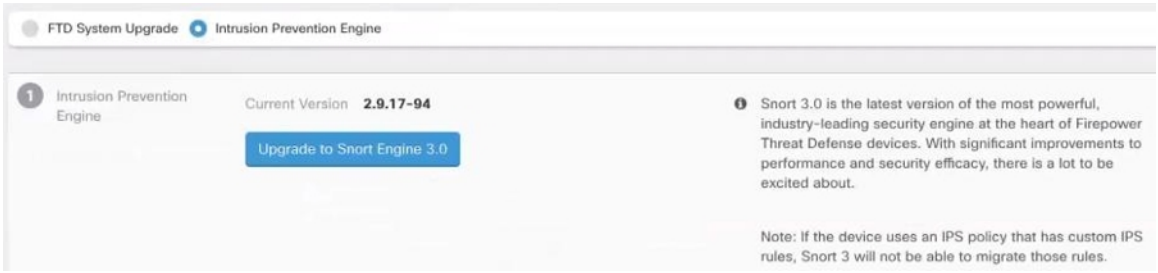
步骤 2 点击**设备**选项卡。

步骤 3 点击 **FTD** 选项卡，然后选择要升级的设备。

步骤 4 在右侧的**设备操作 (Device Actions)** 窗格中，点击**升级 (Upgrade)**。

步骤 5 将升级切换开关设置为入侵防御引擎。

步骤 6 点击 **升级到 Snort Engine 3.0 (Upgrade to Snort Engine 3.0)**。



步骤 7 在“资产”页面中，正在升级的设备具有“正在进行升级”配置状态。

监控升级过程

警告 如果您决定在升级过程中取消升级，请点击“升级”页面中的中止升级。如果在升级开始后取消升级，CDO 不会部署或检查设备中的更改，设备也不会回滚到之前的配置。这可能会导致设备进入不正常状态。如果您在升级过程中遇到任何问题，请联系思科 TAC。

您可以通过在“资产”页面上选择该设备并点击升级按钮来查看单个设备的进度。CDO 会将您引导至该设备的“设备升级”页面。

只要升级失败，CDO 就会显示一条消息。CDO 不会自动重新启动升级过程。

警告 升级具有自签名证书的设备可能会遇到问题；有关详细信息，请参阅检测到新证书

从 Snort 3.0 恢复 FDM 管理 设备

Snort 3.0 中可能不存在 Snort 2.0 中的某些入侵规则。如果降级到 2.0，您创建的所有自定义入侵策略都将转换为自定义策略中使用的基本策略。尽可能保留“覆盖”规则操作。如果多个自定义策略使用相同的基本策略，则系统将保留大多数访问控制策略中使用的自定义策略“覆盖”操作，而其他自定义策略的“覆盖”操作将丢失。现在，使用这些“重复”策略的访问控制规则将使用根据最常用自定义策略创建的基本策略。所有自定义策略都将被删除。

在您选择从 Snort 3.0 恢复之前，请阅读《 *Firepower* 设备管理器配置指南》中的管理入侵策略 (Snort2)，同时了解切换 Snort 引擎版本将如何影响您当前的规则和策略。

Note 恢复为版本 2 不会卸载 Firepower 软件版本。

从 Snort 3.0 恢复

如果更改 Snort 版本，系统将执行自动部署以实施更改。请注意，您只能将单个设备从 Snort 3.0 恢复到版本 2。

使用以下程序恢复入侵防御引擎：

Procedure

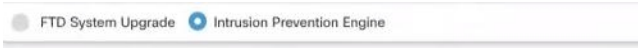
步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

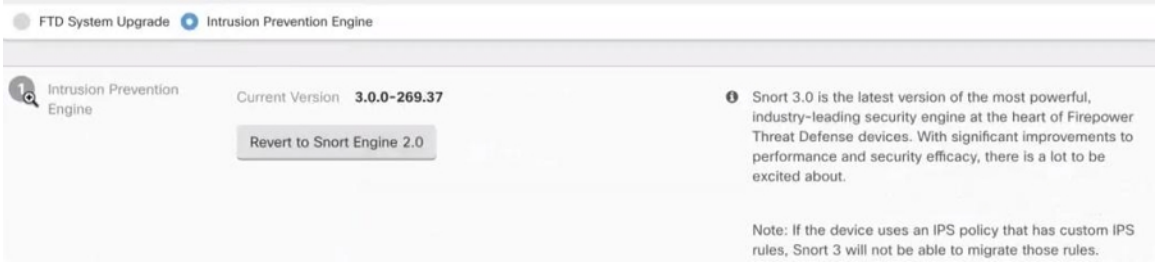
步骤 3 点击 **FTD** 选项卡，然后点击要恢复的设备。

步骤 4 在右侧的**设备操作 (Device Actions)** 窗格中，点击**升级 (Upgrade)**。

步骤 5 将升级切换开关设置为**入侵防御引擎**。



步骤 6 在步骤 1 中，确认要从 Snort 版本 3 恢复，然后点击**恢复到 Snort 引擎 2**。



步骤 7 在**资产**页面中，正在升级的设备具有“正在进行升级”配置状态。

安排安全数据库更新

使用以下程序创建一个计划的任务，以检查和更新 FTD 设备的安全数据库：

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **FTD** 选项卡，然后选择所需的 FTD 设备。

步骤 4 在操作窗格中，找到**安全数据库更新 (Security Database Updates)** 部分，然后点击添加 **+** 按钮。

Note 如果所选设备已存在计划任务，请点击编辑图标创建新任务。创建新任务将覆盖现有任务。

步骤 5 使用以下内容配置计划任务：

- **频率 (Frequency)** - 选择每天、每周或每月进行更新。
- **时间 (Time)** - 选择每天的某个时间。请注意，显示的时间为 UTC。
- **选择天数 (Select Days)** - 选择您希望在一周内的哪一天进行更新。

步骤 6 点击**保存 (Save)**。

步骤 7 设备的配置状态将更改为“正在更新数据库”(Updating Databases)。

编辑计划安全数据库更新

使用以下程序编辑现有的计划任务，以检查和更新 FTD 设备的安全数据库

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **FTD** 选项卡，然后选择所需的 FTD 设备。

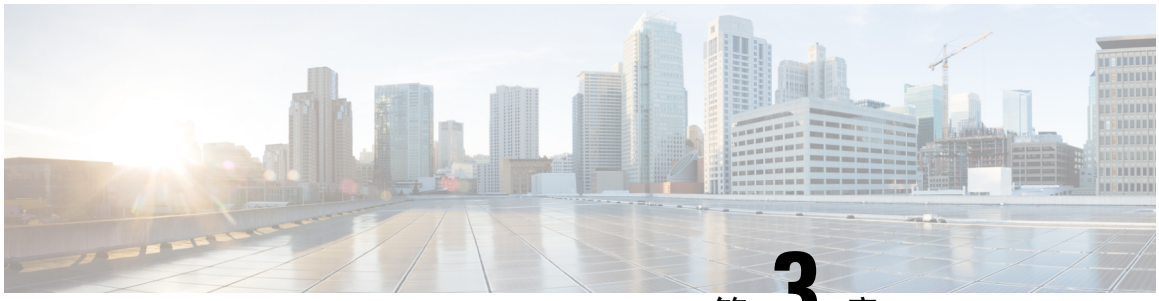
步骤 4 在“操作”(Actions) 窗格中，找到**数据库更新 (Database Updates)** 部分，然后点击编辑图标。

步骤 5 使用以下命令编辑计划任务：

- **频率 (Frequency)** - 选择每天、每周或每月进行更新。
- **时间 (Time)** - 选择每天的某个时间。请注意，显示的时间为 UTC。
- **选择天数 (Select Days)** - 选择您希望在一周内的哪一天进行更新。

步骤 6 点击**保存 (Save)**。

步骤 7 设备的配置状态将更改为“正在更新数据库”(Updating Databases)。



第 3 章

配置 FTD 设备

接口

您可以使用 Cisco Defense Orchestrator (CDO) 配置和编辑 Firepower 威胁防御 (FTD) 设备上的数据接口或管理/诊断接口。

目前，CDO 只能配置路由接口和网桥组。它不支持配置被动接口。

Firepower 接口配置的指南和限制

使用 思科防御协调器 (CDO) 配置设备时，接口配置存在许多局限性。如果您需要以下任意功能，则必须使用 Firepower 管理中心来配置设备。

防火墙

- 仅支持路由防火墙模式。无法配置透明防火墙模式的接口。
- 只有物理 Firepower 1010 设备支持为交换机端口模式配置的接口。有关详细信息，请参阅 FDM 管理 设备的交换机端口模式接口。

被动

- 目前，思科防御协调器 (CDO) 未在接口表中识别被动接口模式，并且您无法配置被动或 ERSPAN 接口。您必须使用 FDM 管理 UI 配置和识别被动接口。

仅 IPS 模式

- 不能将接口配置为内联（在内联集内）或内联分路，用于仅 IPS 的处理。仅 IPS 模式的接口将绕过许多防火墙检查，仅支持 IPS 安全策略。相比之下，防火墙模式接口需要对流量执行防火墙功能，例如维持流量、跟踪 IP 和 TCP 层的流量状态、IP 分片重组和 TCP 规范化。
- 可选，您可以根据安全策略，选择配置该防火墙模式接口的 IPS 功能。

EtherChannel

CDO 支持运行版本 6.5 及更高版本的设备的读取、创建和功能。要创建 Etherchannel 接口，请参阅为 FDM 管理 设备添加 EtherChannel 接口。要创建

- 您最多可以在物理 Firepower 设备上配置 48 个 EtherChannel，但一次可以活动的接口数量取决于您的设备型号。有关设备特定的限制，请参阅设备特定限制。

- 通道组中的所有接口都必须具有相同的介质类型和容量，并且必须设置为相同的速度和双工模式。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。
- EtherChannel 连接到的设备还必须支持 802.3ad EtherChannel。
- FDM 托管设备不支持带有 VLAN 标记的 LACPDU。如果使用 Cisco IOS vlan dot1Q tag native 命令在相邻交换机上启用本地 VLAN 标记，则 FDM 管理 设备将会丢弃已标记的 LACPDU。请务必禁用相邻交换机上的本地 VLAN 标记。
- 所有 FDM 管理 设备配置均引用 EtherChannel 接口，而不是成员物理接口。

Note 设置为 portchannels 的接口仅支持物理接口、冗余接口和子接口作为网桥组成员接口。

网桥组

目前，CDO 支持一个网桥组的配置。要确定您的设备是否支持网桥组，请参阅 FDM 管理 配置中的网桥组兼容性以了解详细信息。

将接口添加到桥接组时，请记住以下几点：

- 该接口必须具有名称。
- 该接口不能有任何已定义的 IPv4 或 IPv6 地址，无论是静态分配的还是通过 DHCP 获得的。
- BVI 可以将 VLAN 接口或其他路由接口作为成员接口，但不能将两个接口作为单个 BVI 上的成员接口。
- BVI 可以将 VLAN 接口或其他路由接口作为成员接口，但不能将两个接口作为单个 BVI 上的成员接口。
- 接口不能是以太网的点对点协议 (PPPoE)
- 接口不能与安全区域关联（如果它在区域中）。您必须删除该接口的所有 NAT 规则，然后才能将其添加到网桥组。
- 单独启用和禁用成员接口。这样就可以禁用任何未使用的接口，而无需将其从网桥组删除。网桥组本身始终处于启用状态。
- 您可以配置成为网桥组 **成员** 的接口。有关接口要求和创建，请参阅配置网桥组。

以太网的点对点协议

- 不能为 IPv4 配置以太网点对点协议 (PPPoE)。如果将互联网接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，且 ISP 使用 PPPoE 为您提供 IP 地址，则您必须使用 FDM 来配置这些设置。

VLAN

要配置 VLAN 接口和 VLAN 成员，请参阅配置 FDM 管理设备 VLAN 以了解详细信息。要为交换机端口模式配置 VLAN，请参阅为交换机端口模式配置 FDM 管理 设备 VLAN 以了解详细信息。

- 接口必须是物理接口。
- 接口不能是仅管理接口。
- 接口不能与任何其他类型的接口关联，包括 BVI、子接口、另一个 VLAN 接口、EtherChannel 等。
- 接口不能是 BVI 成员或 etherchannel 成员。
- 设备型号支持不同数量的 VLAN 成员。有关详细信息，请参阅各设备型号的最大 VLAN 成员数量。

Note 要为环境配置 VLAN，请参阅配置 Firepower VLAN 子接口和 802.1Q 中继。

网络模块卡

可选的网络模块安装仅限于 ASA 5515-X、5525-X、5545-X 和 5555-X 以及 Firepower 2100 系列设备。

- 仅在引导程序期间（即初始安装或重新映像，或在本地/删除管理之间切换时），才会发现网络接口卡。CDO会为这些接口设置正确的速度和复用默认值。如果将可选网络接口卡替换为更改接口速度/双工选项的卡，而不更改可用接口的总数，则重新启动设备，以便系统识别替换接口的正确速度/双工值。在与设备的 SSH 或控制台会话中，输入 reboot 命令。然后，使用 CDO，编辑能够更改的各物理接口，并选择有效的速度和双工选项，因为系统不会自动更正您的原始设置。立即部署更改，确保系统行为正确无误。
- 您无法在 FDM 管理 Secure Firewall 3100 系列设备上启用或禁用网络模块或执行接口的分支在线插入和删除 (OIR)。

Note 将卡更换为接口总数更改的卡，或移除其他对象引用的接口，均可能导致意外问题。如果需要进行此类更改，请先删除待移除接口的所有引用，如安全区成员资格、VPN 连接等。此外，建议您在更改前进行备份。

虚拟 FDM 管理 设备上的接口

- 如果不重新初始化虚拟 FDM 管理 设备，则无法添加或删除接口。您必须在 FDM 管理 设备中执行这些操作。

Note 如果更换的接口具有不同的速率/双工能力，需要重启设备，使系统能够识别新的速率/双工值，步骤如下：在设备的CLI控制台中，输入“重新引导”命令。然后，在 CDO 中，编辑能够更改的各接口，并选择有效的速度和复用选项，因为系统不会自动更正您的原始设置。立即部署更改，确保系统行为正确无误。

各设备型号的最大 VLAN 成员数量

设备型号限制可配置的最大 VLAN 子接口数量。请注意，仅可在数据接口上而不可在管理接口上配置子接口。下表介绍各设备型号的限制。

型号	最大 VLAN 子接口数量
Firepower 1010	60
Firepower 1120	512
Firepower 1140、Firepower 1150	1024
Firepower 2100	1024
Firepower 4100	1024
Firepower 9300	1024
ASA 5508-X	50
ASA 5515-X	100
ASA 5516-X	100
ASA 5525-X	200
ASA 5545-X	300
ASA 5555-X	500
ISA 3000	100

Firepower 数据接口

Cisco Defense Orchestrator (CDO) 支持在 FDM 管理 设备上配置路由接口和桥接虚拟接口。

路由接口

每个第 3 层路由接口（或子接口）都需要唯一子网上的一个 IP 地址。通常会将这些接口与交换机、另一个路由器上的端口或 ISP/WAN 网关连接。

您可以分配静态地址，也可以从 DHCP 服务器获取静态地址。但是，如果 DHCP 服务器提供与设备上的静态定义接口相同的子网地址，系统会禁用 DHCP 接口。如果使用 DHCP 获取地址的接口停止传递流量，请检查该地址是否与设备上其他接口的子网重叠。

可以在路由接口上同时配置 IPv4 和 IPv6 地址。请确保配置一条同时适用于 IPv4 和 IPv6 的默认路由。需要使用 Firepower 设备管理器在 FDM 管理 设备上执行此任务。有关配置默认路由的信息，请参阅“适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南，版本 xxx”中的**基础知识 > 路由**。

网桥组和网桥虚拟接口

网桥组是FDM管理设备用于桥接而非路由的一组接口。桥接接口属于桥接组，且所有接口都在同一网络上。桥接组由在网桥网络上有 IP 地址的桥接虚拟接口 (BVI) 表示。包含在网桥组中的接口称为“成员”。

如果指定 BVI，您可以在路由接口和 BVI 之间路由。在这种情况下，BVI 充当成员接口和路由接口之间的网关。如果不指定 BVI，网桥组成员接口上的流量不能离开网桥组。通常，您可以指定该接口，以便将成员接口路由到互联网。

FDM 管理 设备仅支持一个网桥组；因此，CDO 只能管理该网桥组，而无法在设备上创建其他网桥组。CDO 只能管理直接安装在硬件上的 FDM 管理 设备上的 BVI，而不能管理虚拟 FDM 管理 设备实例上的 BVI。

路由模式下网桥组的一种用途是在 FDM 管理 设备上而非外部交换机上使用额外接口。您可以将终端直接连接到网桥组成员接口。您还可以连接交换机，以将更多终端添加到与 BVI 相同的网络。

被动接口

被动接口使用交换机SPAN（交换端口分析器）或镜像端口监控在网络中传输的流量。SPAN或镜像端口允许从交换机的其他端口复制流量。此功能可以提供网络内的系统可视性，而不会影响网络流量。如果在被动部署中配置系统，系统将不能执行某些操作，例如，阻止流量或流量整形。被动接口无条件接收所有流量，这些接口不会重传接收到的流量。

目前，CDO 对管理 FDM 管理 设备上的被动接口提供有限的支持：

- 必须在 FDM 管理 设备上配置被动接口。
- 路由接口无法使用 CDO 来更改为被动接口，而被动接口也无法更改为路由接口。
- CDO 不会标识接口表中的被动接口。

相关信息：

- Firepower 接口的 IPv6 寻址
- Firepower 接口配置的指南和限制
- 配置物理 Firepower 接口

管理/诊断接口

标记为“管理”(Management) 的物理端口（对于 FDM 管理设备虚拟，则为 Management 0/0 虚拟接口）实际上有两个与其关联的单独接口。

- **管理虚拟接口 (Management virtual interface)** - 此 IP 地址用于系统通信。这是系统用于进行智能许可和检索数据库更新的地址。您可以打开它的管理会话（Firepower 设备管理器和 CLI）。您必须配置一个管理地址，该地址在**系统设置** > **管理接口**上定义。
- **诊断物理接口 (Diagnostic physical interface)** - 此物理管理端口的实际名称为“诊断”(Diagnostic)。您可以使用此接口将系统日志消息发送到外部系统日志服务器。为诊断物理接口配置 IP 地址是可选项。配置该接口的唯一原因是您需要将它用于系统日志。此接口显示在**清单 (Inventory)** > **接口 (Interfaces)** 页面上，并可在此页面上进行配置。诊断物理接口只允许管理流量，而不允许穿越流量。

（硬件设备。）建议配置管理/诊断接口时，不要将物理端口连接到网络。而是仅配置管理 IP 地址，并把它配置为将数据接口用作从互联网获取更新的网关。然后，打开 HTTPS/SSH 流量（默认情况下启用 HTTPS）的内部接口，并使用内部 IP 地址打开 Firepower 设备管理器。您必须直接在 Firepower 设备管理器上执行此任务。有关说明，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》中的“配置管理访问列表”。

对于 FDM 管理设备虚拟，建议的配置是将 Management0/0 连接到与内部接口相同的网络，并将内部接口用作网关。不要为诊断接口配置单独的地址。

Note 有关如何编辑管理接口的特殊说明，请参阅适用于 **Firepower 版本 6.4 或更高版本的** 《 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》。打开指南并导航至**基础知识** > **接口** > **管理/诊断接口**。管理接口配置应在 Firepower 设备管理器上完成。

接口设置

使用这些主题来配置接口设置。

在 Firepower 接口设置中使用安全区域

可为每个接口分配一个安全区。然后根据区域应用您的安全策略。例如，您可以将内部接口分配到内部区域，而将外部接口分配到外部区域。例如，可以配置访问控制策略，允许流量从内部传到外部，但不允许从外部传入内部。

每个区域都有一个模式，路由或被动模式。该模式与接口模式直接关联。您可以仅向同一模式安全区添加路由和被动接口。

桥接虚拟接口 (BVI) 不会添加到安全区域。仅将成员接口添加到安全区域。

不能将诊断或管理接口包括在区域中。区域只适用于数据接口。

CDO 当前不支持在 ASA 或 FTD 设备上管理、监控或使用虚拟隧道接口 (VTI) 隧道。已配置 VTI 隧道的设备可以被载入 CDO，但它会忽略 VTI 接口。如果安全区域或静态路由引用 VTI，则 CDO 会读取不带 VTI 引用的安全区域和静态路由。即将推出对 VTI 隧道的 CDO 支持。

有关安全区域的详细信息，请参阅安全区域对象。

将 FDM 管理设备接口分配给安全区域

准备工作

在添加安全区域时，接口存在以下限制：

- 该接口必须具有名称。
- 接口不能是仅管理接口。此选项可在界面的“高级”(Advanced) 选项卡中启用和禁用。
- 不能将安全区域分配给网桥组接口。
- 不能将安全区域分配给为交换机端口模式配置的接口。
- CDO 当前不支持在 ASA 或 FDM 管理 设备上管理、监控或使用虚拟隧道接口 (VTI) 隧道。已配置 VTI 隧道的设备可以被载入 CDO，但它会忽略 VTI 接口。如果安全区域或静态路由引用 VTI，则CDO会读取不带VTI引用的安全区域和静态路由。即将推出对VTI隧道的CDO支持。

将 Firepower 接口分配给安全区域

使用以下程序将安全区域关联到现有接口：

Procedure

步骤 1 登录 CDO。

步骤 2 在导航窗格中，点击**清单 (Inventory)**。

步骤 3 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 4 点击 **FTD** 设备，然后选择要修改的 FDM 管理 设备。

步骤 5 在右侧的**管理 (Management)** 窗格中，点击 **接口 (Interfaces)**。

步骤 6 选择要向其添加安全区域的接口，然后点击 **编辑 (Edit)**。

步骤 7 使用**安全区 (Security Zone)** 下拉菜单并选择要与此接口关联的安全区域。

Note 如果需要，请点击**新建 (Create New)**，从此下拉菜单中创建新的安全区域。

步骤 8 点击**保存 (Save)**。

步骤 9 将配置更改从 CDO 部署到 FDM 管理 设备。

相关信息：

- 安全区域对象

- 创建或编辑 Firepower 安全区域对象
- Firepower 接口配置的指南和限制

在 Firepower 接口设置中使用 Auto-MDI/MDX

对于 RJ-45 接口，默认的自动协商设置还包括 Auto-MDI/MDIX 功能。Auto-MDI/MDIX 在自动协商阶段检测直通电缆时执行内部交叉，从而消除交叉布线的需要。如要启用接口的 Auto-MDI/MDIX，必须将速度或双工设置为自动协商。如果将速度和双工明确设置为固定值，从而禁用了两种设置的自动协商，则 Auto-MDI/MDIX 也将被禁用。对于千兆以太网，当速度和双工被设置为 1000 和全值时，接口始终会自动协商；因此，Auto-MDI/MDIX 始终会启用，且您无法禁用它。

在编辑接口时，可在“高级”(Advanced) 选项卡上配置这些设置。

在 Firepower 接口设置中使用 MAC 地址

您可以手动配置介质访问控制 (MAC) 地址来覆盖默认值。

对于高可用性配置，您可以同时配置接口的主用和备用 MAC 地址。如果主用设备进行故障切换，并且备用设备成为主用设备，则新的主用设备会开始使用主用 MAC 地址，以最大限度地减少网络中断。

在配置接口时，在“高级”(Advanced) 选项卡上配置主用和备用 MAC 地址。

默认 MAC 地址

默认 MAC 地址分配取决于接口类型。

- **物理接口 (Physical interfaces)** - 物理接口使用已刻录的 MAC 地址。
- **子接口 (Subinterfaces)** - 物理接口的所有子接口都使用相同的刻录的 MAC 地址。您可能想为子接口分配唯一的 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一的 MAC 地址分配给子接口会允许唯一的 IPv6 链路本地地址。

在 Firepower 接口设置中使用 MTU 设置

关于 MTU

MTU 会指定 FDM 管理 设备可在给定以太网接口上传输的最大帧负载大小。MTU 值是没有以太网报头、VLAN 标记或其他系统开销情况下的帧大小。例如，将 MTU 设置为 1500 时，预期帧大小为 1518 字节（含报头）或 1522 字节（使用 VLAN）。请勿为容纳这些报头而将 MTU 的值设得过高。

路径 MTU 发现

FDM 管理 设备支持路径 MTU 发现（如 RFC 1191 中所定义），从而使两个主机之间的网络路径中的所有设备均可协调 MTU，以便它们可以标准化路径中的最低 MTU。

MTU 和分段

对于IPv4，如果传出IP数据包大于指定MTU，则该数据包将分为2帧或更多帧。片段在目标处（有时在中间跃点处）重组，而分片可能会导致性能下降。对于 IPv6，通常不允许对数据包进行分段。因此，IP 数据包大小应在 MTU 大小范围内，以避免分片。

对于 UDP 或 ICMP，应用应将 MTU 考虑在内，以避免分段。

Note 只要有内存空间，FDM 管理 设备就可接收大于所配置的 MTU 的帧。

MTU 和巨型帧

MTU 越大，您能发送的数据包越大。加大数据包可能有利于提高网络效率。请参阅以下准则：

- 与流量路径上的MTU相匹配：我们建议将所有FDM管理 设备接口以及流量路径的其他设备接口上的 MTU 设为相同。匹配 MTU 可防止中间设备对数据包进行分片。
- 容纳巨型帧：巨型帧是指大于标准最大值 1522 字节（包括第 2 层报头和 VLAN 报头）的以太网数据包，最大为 9216 字节。MTU 最大可设置为 9198 字节，以容纳巨帧。FDM 管理 虚拟的最大值为 9000。

Note 加大 MTU 会为巨型帧分配更多内存，这样可能会限制其他功能（例如访问规则）的最大使用量。如果在 ASA 5500-X 系列设备或 FDM 管理 虚拟上将 MTU 增加到默认值 1500 以上，则必须重新启动系统。无需重启 Firepower 2100 系列设备，因为巨帧支持在该设备上始终启用。

默认情况下，在 Firepower 3100 设备上启用巨帧支持。

Firepower 接口的 IPv6 寻址

您可以为 Firepower 物理接口配置两种类型的单播 IPv6 地址。

- **全局 (Global)** - 全局地址是可在公用网络上使用的公用地址。对于桥接组，需要在桥接虚拟接口 (BVI) 上而非每个成员接口上配置全局地址。不能将以下任何地址指定为全局地址。
  - 内部保留的 IPv6 地址：fd00::/56（fd00:: 至 fd00:0000:0000:00ff:ffff:ffff:ffff:ffff）
  - 未指定的地址，例如 ::/128
  - 环回地址 ::1/128
  - 组播地址，ff00::/8
  - 链路本地地址 fe80::/10

- **链路本地 (Link-local)** - 链路本地地址是只能在直连网络上使用的专用地址。路由器不使用链路本地地址转发数据包；它们仅用于在特定物理网段上通信。链路本地地址可用于地址配置或网络发现功能，例如地址解析和邻居发现。每个接口必须有自己的地址，因为链路本地地址仅在网段中可用，并且会与接口 MAC 地址绑定。

至少需要配置链路本地地址，IPv6 才会起作用。如果配置全局地址，则接口上会自动配置链路本地地址，因此无需另外专门配置链路本地地址。如果不配置全局地址，则需要自动或手动配置链路本地地址。

配置 Firepower 接口

将电缆（以物理方式或虚拟方式）连接到接口接头时，您需要配置该接口。至少需要命名并启用该接口，流量才会通过该接口。如果该接口是网桥组的成员，则只用为接口命名。如果接口是桥接虚拟接口 (BVI)，则需要为 BVI 分配一个 IP 地址。如果要在特定端口上创建 VLAN 子接口（而非单一物理接口），通常要在该子接口（而不是物理接口）上配置 IP 地址。通过 VLAN 子接口，可将一个物理接口划分成多个标记有不同 VLAN ID 的逻辑接口。

接口列表将显示可用的接口及其名称、地址和状态。您可以通过选择接口行并点击“操作”(Actions) 窗格中的**编辑 (Edit)** 来更改接口的状态（打开或关闭）或编辑接口。列表将基于您的配置显示接口特征。展开接口行以查看子接口或桥接组成员。

相关信息：

- 接口
- 配置物理 Firepower 接口
- 配置高级 Firepower 接口选项, on page 242
- 配置 Firepower VLAN 子接口和 802.1Q 中继
- 为交换机端口模式配置 FDM 管理 设备 VLAN

配置物理 Firepower 接口

要启用物理接口，至少必须启用它。您可以常规命名它和配置 IP 地址；然而，如果要创建 VLAN 子接口，或者配置被动模式接口，或者要将接口添加到网桥组，无需配置 IP 寻址。

Note 您不能在桥接组成员接口或被动接口上配置 IP 地址，但是可以根据需要修改高级设置。

您可以禁用接口，以临时阻止在相连网络中的传输。无需删除该接口的配置。目前，思科防御协调器 (CDO) 只能配置路由接口和网桥组。CDO 会列出被动接口，但不能将其从 CDO 重新配置为主动接口。

Note 注意：CDO 不支持 IPv4 的点对点以太网协议 (PPPoE) 配置。在 FDM 管理 设备中配置此选项可能会导致 CDO UI 出现问题；如果必须为设备配置 PPPoE，则必须在 FDM 管理 设备中进行适当的更改。

操作步骤

Procedure

步骤 1 在**设备和服务 (Devices & Services)** 页面上，点击要配置其接口的设备，然后点击右侧管理窗格中的**接口 (Interfaces)**。

步骤 2 在“接口”(Interfaces) 页面上，选择要配置的物理接口。

步骤 3 在右侧的“操作”(Actions) 窗格中，点击**编辑 (Edit)**。

步骤 4 为物理接口指定**逻辑名称 (Logical Name)**和**说明 (Description)**（可选）。除非配置子接口，否则接口应有名称。

Note 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

步骤 5 选择这两个选项之一：

- 如果要添加子接口：

如果要为此物理接口配置子接口，则可能已完成。点击**保存 (Save)** 并继续配置 Firepower VLAN 子接口和 802.1Q 中继；否则，请继续。

Note 即使在配置子接口时，为接口命名和提供 IP 地址也有效。这不是常规设置，但如果确定符合您的需求，则可以进行配置。

- 如果您不打算添加子接口，请继续为物理接口配置 IPv4 地址和为物理接口配置 IPv6 地址中的一个或两个。

为物理接口配置 IPv4 地址

Warning 在配置并保存 DHCP 地址池后，DHCP 地址池将绑定到接口的已配置 IP 地址。如果在配置 DHCP 地址池后编辑接口的子网掩码，则部署到 FDM 管理设备会失败。此外，如果在 FDM 管理 控制台中编辑 DHCP 地址池并从 FDM 管理设备读取配置到 思科防御协调器 中，则读取操作会失败。

Procedure

步骤 1 在“编辑物理接口”(Editing Physical Interface) 对话框中，点击 **IPv4 地址 (IPv4 Address)** 选项卡。

步骤 2 从类型字段中选择以下任一选项：

- **静态 (Static)** - 如果希望分配固定的地址，请选择此选项。对于连接到接口的网络，输入接口的 IP 地址和子网掩码。例如，如果您连接的是 10.100.10.0/24 网络，则可以输入 10.100.10.1/24。确保您输入的地址不是网络 ID 或网络的广播地址，并且该地址尚未在网络上使用。
  - **备用 IP 地址和子网掩码 (Standby IP Address and Subnet Mask)** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。
  - 可选）**DHCP 地址池 ([Optional] DHCP Address Pool)** - 输入单个 DHCP 服务器 IP 地址或 IP 地址范围。该 IP 地址范围必须与所选接口位于同一子网上，并且不能包括接口本身的 IP 地址、广播地址或子网地址。指定该池的开始和结束地址，用连字符隔开。要暂时禁用此 DHCP 服务器，请在 配置 DHCP 服务器 页面的 **DHCP 服务器 (DHCP Servers)** 部分编辑该服务器。
- **动态 (DHCP) (Dynamic [DHCP])** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。如有需要，更改以下选项：
  - **获取默认路由 (Obtain Default Route)** - 是否从 DHCP 服务器获取默认路由。您通常都要选中此选项。
  - **DHCP 路由指标 (DHCP Route Metric)** - 如果从 DHCP 服务器获取默认路由，请输入与获知路由的管理距离，其值介于 1 到 255 之间。

  Note 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。

步骤 3 完成后点击**保存 (Save)**，或者继续执行其中一个程序：

- 如果要为此接口分配 IPv6 地址和 IPv4 地址，请“为物理接口配置 IPv6 地址”。
- 配置高级 Firepower 接口选项, on page 242。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。
- 如果您保存了接口并且不想继续使用高级接口选项，请继续启用物理接口。

为物理接口配置 IPv6 地址

Procedure

步骤 1 在“编辑物理接口”(Editing Physical Interface) 对话框中，点击“IPv6 地址”(IPv6 Address) 选项卡。

步骤 2 **状态 (State)** - 在您未配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请点击**状态 (State)** 滑块将其启用。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

Note 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

步骤 3 **地址自动配置 (Address Auto Configuration)** - 选中此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

虽然 RFC 4862 规定为无状态自动配置所配置的主机不发送路由器通告消息，但 FDM 管理 设备在这种情况下确实会发送路由器通告消息。选择**抑制 RA** 可抑制消息，遵从 RFC 要求。

步骤 4 **抑制 RA (Suppress RA)** - 如果要抑制路由器通告，请选中此复选框。Firepower 威胁防御设备可参与路由器通告，以便相邻设备可动态获知默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

也会发送路由器通告，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

对于不希望 Firepower 防御设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望在接口上抑制这些消息。

步骤 5 **本地链路地址 (Link-Local Address)** - 如果要仅将地址用作链路本地地址，请在链路本地地址字段中输入该地址。本地链路地址在本地网络之外无法访问。在网桥组接口上无法配置本地链路地址。

Note 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feee:6a82。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

步骤 6 **备用链路本地地址 (Standby Link-Local Address)** - 如果接口连接高可用性设备，请配置此地址。输入此接口所连接的另一台 FDM 管理 设备上的接口本地链路地址。

步骤 7 **静态地址/前缀 (Static Address/Prefix)** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅 Firepower 接口的 IPv6 寻址。

步骤 8 **备用 IP 地址 (Standby IP Address)** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

步骤 9 完成后点击**保存 (Save)**，或者继续执行其中一个程序：

- 配置高级 Firepower 接口选项, on page 242。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。

- 如果您保存了接口并且不想继续使用高级接口选项，请继续启用物理接口。

启用物理接口

Procedure

步骤 1 选择要启用的接口。

步骤 2 将与接口逻辑名称关联的窗口右上角的**状态 (State)** 滑块滑动到蓝色。

步骤 3 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

配置 Firepower VLAN 子接口和 802.1Q 中继

通过 VLAN 子接口，可将一个物理接口划分成多个标记有不同 VLAN ID 的逻辑接口。带有一个或多个 VLAN 子接口的接口将自动配置为 802.1Q 中继。由于 VLAN 允许您在特定物理接口上将流量分开，所以您可以增加网络中可用的接口数量，而无需增加物理接口或设备。

如果您将物理接口连接到交换机的中继端口，请创建子接口。为交换机中继端口上显示的每个VLAN创建子接口。如果您将物理接口连接到交换机的接入端口，创建子接口将没有意义。

Note 您不能在桥接组成员接口上配置 IP 地址，但是可以根据需要修改高级设置。

准备工作

阻止物理接口上的未标记数据包。如果使用子接口，您通常不想让物理接口传递流量，因为物理接口会传递未标记的数据包。由于必须启用物理接口，才能允许子接口传递流量，所以请确保物理接口不会通过未命名接口传递流量。如果要允许物理接口传递未标记数据包，可以照常命名接口。

操作步骤

Procedure

步骤 1 在导航窗格中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后点击要配置其接口的设备。

步骤 4 点击右侧**管理 (Management)** 窗格中的 **接口 (Interfaces)** 。

步骤 5 在“接口”(Interfaces) 页面上，选择要配置的物理接口，然后在右侧的“操作”(Actions) 窗格中，点击**+ 新建子接口 (+ New Subinterface)**。

请注意，**父接口 (Parent Interface)** 字段显示要为其创建此子接口的物理接口的名称。创建子接口后，父接口则无法更改。

步骤 6 为子接口提供**逻辑名称**和**说明**（可选）。如果没有逻辑名称，将忽略其余的接口配置。

Note 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

步骤 7 配置 VLAN ID 和子接口 ID：

- **VLAN ID** - 输入 VLAN ID，介于 1 和 4094 之间，用于标记该子接口上的数据包。
- **子接口 ID (Subinterface ID)** - 以整数形式输入介于 1 和 4294967295 之间的子接口 ID。允许的子接口数各设备型号的最大 VLAN 成员数量。在创建子接口后，您无法更改子接口 ID。

继续为子接口配置 IPv4 地址 和为子接口配置 IPv6 地址 。

为子接口配置 IPv4 地址

Procedure

步骤 1 在“添加子接口”(Adding Subinterface) 对话框中，点击 **IPv4 地址 (IPv4 Address)** 选项卡。

步骤 2 从类型字段中选择以下任一选项：

- **静态 (Static)** - 如果希望分配固定的地址，请选择此选项。

  对于连接到接口的网络，输入接口的**IP 地址和子网掩码**。例如，如果您连接的是 10.100.10.0/24 网络，则可以输入 10.100.10.1/24。确保您输入的地址不是网络 ID 或网络的广播地址，并且该地址尚未在网络上使用。

- 仅当在高可用性设备对中使用此接口时，才输入**备用 IP 地址**和子网掩码。
- **动态 (DHCP) (Dynamic [DHCP])** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。如有需要，更改以下选项：
  - **获取默认路由 (Obtain Default Route)** - 是否从 DHCP 服务器获取默认路由。您通常都要选中此选项。
  - **DHCP 路由指标 (DHCP Route Metric)** - 如果从 DHCP 服务器获取默认路由，请输入与获知路由的管理距离，其值介于 1 到 255 之间。

    请参阅配置 DHCP 服务器。

    Note 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。

步骤 3 完成后点击**创建 (Create)**，或者继续执行以下程序之一：

- 如果要为此接口分配 IPv6 地址和 IPv4 地址，请继续执行“为物理接口配置 IPv6 地址”。
- 配置高级 Firepower 接口选项, on page 242。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。
- 如果已创建子接口，请转至启用物理接口 。

为子接口配置 IPv6 地址

Procedure

步骤 1 点击“IPv6 地址”(IPv6 Address) 选项卡。

步骤 2 **启用 IPv6 处理 (Enable IPv6 processing)** - 在不想配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请将**状态**滑块移至蓝色。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

Note 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

步骤 3 **地址自动配置 (Address Auto Configuration)** - 选中此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

步骤 4 **抑制 RA (Suppress RA)** - 如果要抑制路由器通告，请选中此复选框。Firepower 威胁防御设备可参与路由器通告，以便相邻设备可动态获知默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

也会发送路由器通告，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

对于不希望 Firepower 防御设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望在接口上抑制这些消息。

步骤 5 **本地链路地址 (Link-Local Address)** - 如果要仅将地址用作链路本地地址，请在链路本地地址字段中输入该地址。本地链路地址在本地网络之外无法访问。

Note 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feee:6a82。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

步骤 6 **备用链路本地地址 (Standby Link-Local Address)** - 如果接口连接高可用性设备，请配置此地址。

步骤 7 **静态地址/前缀 (Static Address/Prefix)** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅第 136 页上的“IPv6 地址”。

步骤 8 **备用 IP 地址 (Standby IP Address)** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

步骤 9 完成后点击**创建 (Create)**，或者继续执行以下程序之一：

- 点击“高级”(Advanced) 选项卡转到配置高级 Firepower 接口选项, on page 242。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。
- 如果已创建子接口，请转至启用物理接口 。

启用物理接口

Procedure

步骤 1 要启用子接口，请将与子接口的逻辑名称关联的状态滑块滑动到蓝色。

步骤 2 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

配置高级 Firepower 接口选项

高级接口选项的默认设置适用于大多数网络。只有在需要解决网络问题时，再配置它们。

以下步骤程序假定已定义接口。另外，您还可以在初始编辑或创建接口时编辑这些设置。

此程序及其中的所有步骤都是可选的。

限制：

- 您无法在 Firepower 2100 系列设备上设置管理接口的 MTU、复用或速度。
- 在未命名接口上，MTU **必须** 设置为 1500。

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后点击要配置其接口的设备。

步骤 4 点击右侧**管理 (Management)** 窗格中的 **接口 (Interfaces)** 。

步骤 5 在“接口”(Interfaces) 页面上，选择要配置的物理接口，然后在右侧的“操作”(Actions) 窗格中，点击**编辑 (Edit)**。

步骤 6 点击**高级**选项卡。

步骤 7 **启用高可用性监控 (Enable for HA Monitoring)** 会被自动启用。如果将其启用，当 HA 对决定是否在高可用性配置中故障转移到对等设备时，设备会考虑接口的运行状况。如果不配置高可用性，可忽略此选项。如果不配置接口的名称，也可以忽略此选项。

步骤 8 要将数据接口仅用于管理，请选中**仅管理 (Management Only)**。

仅管理接口不允许直通流量，所以将数据接口设置为**仅管理 (Management Only)** 接口的价值微乎其微。不能更改管理/诊断接口的此项设置，它们始终为仅管理。

步骤 9 修改 IPv6 DHCP 设置。

- **启用 DHCP 以获取 IPv6 地址配置** - 是否在 IPv6 路由器通告数据包中设置“托管地址配置”(Managed Address Configuration) 标志。此标志通知 IPv6 自动配置客户端应使用 DHCPv6 来获取相关地址以及派生的无状态自动配置地址。
- **启用 DHCP 以获取 IPv6 非地址配置** - 是否在 IPv6 路由器通告数据包中设置“其他地址配置”(Other Address Configuration) 标志。此标志通知 IPv6 自动配置客户端应使用 DHCPv6 从 DHCPv6 获取其他信息，如 DNS 服务器地址。

步骤 10 配置 **DAD 尝试 (DAD Attempts)** - 接口执行重复地址检测 (DAD) 的频率，介于 0 - 600 之间。默认值为 1。在无状态自动配置过程中，DAD 会验证新单播 IPv6 地址的唯一性，再将地址分配给接口。如果重复地址是接口的链路本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。接口将使用邻居的询求消息来执行重复地址检测。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。

步骤 11 将 MTU（最大传输单位）更改为所需的值。

默认 MTU 为 1500 字节。您可以指定介于 64 - 9198（或为 Firepower 威胁防御虚拟指定 9000）之间的值。如果通常在网络中使用巨帧，请设置一个较大的值。有关详细信息，请参阅在Firepower接口设置中使用 MTU 设置。

Note 如果在 ASA 5500-X 系列设备、ISA 3000 系列设备或 Firepower 威胁防御虚拟上将 MTU 提高到 1500 以上，则必须重新启动设备。登录 CLI 并使用 reboot 命令。您无需重启 Firepower 2100 或 Secure Firewall 3100 系列设备，因为在这些设备上会始终启用巨帧支持。

步骤 12 （仅限物理接口）。修改**速度**和**复用**设置。

默认设置为该接口与线路另一端的接口协商最佳复用和速度，但如有必要，您可以强制实施特定的复用或速度。所列的选项仅为接口支持的设置。在网络模块上设置这些选项之前，请阅读Firepower接口配置的指南和限制。

- **复用 (Duplex)** - 选择自动、半复用、全复用或默认。当接口支持时，自动为默认值。例如，您不能为 Firepower 2100 或 Secure Firewall 3100 系列设备上的 SFP 接口选择“自动”(Auto)。选择默认表示 Firepower 设备管理器不应尝试配置设置。

  任何现有配置将保持不变。

- **速度 (Speed)** - 选择自动可使接口协商速度（默认值）或选取特定速度：10 Mbps、100 Mbps、1000 Mbps、10000 Mbps。此外，您还可以选择以下特殊选项：

  任何现有配置将保持不变。

接口类型限制了您可以选择的选项。例如， Firepower 2100 系列设备上的 SFP+ 接口仅支持 1000 (1 Gbps) 和 10000 (10 Gpbs)，SFP 接口仅支持 1000 (1 Gbps)，而千兆以太网端口不支持 10000 (10 Gpbs)。其他设备上的 SPF 接口可能需要设置“不协商”(No Negotiate)。有关接口所支持的选项的信息，请参阅硬件文档。

步骤 13 （可选，建议为子接口和高可用性设备配置。）配置 MAC 地址。

MAC 地址 (MAC Address) - 采用 H.H.H 格式的介质访问控制，其中 H 是 16 位十六进制数字。例如，您可以将 MAC 地址 00-0C-F1-42-4C-DE 输入为 000C.F142.4CDE。MAC 地址不能设置组播位，即左起第二个十六进制数字不能是奇数。

备用 MAC 地址 (Standby MAC Address) - 用于高可用性。如果主用设备发生故障切换，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

步骤 14 点击**创建**。

配置网桥组

网桥组是将一个或多个接口分组的虚拟接口。对接口分组的主要原因是创建一组交换接口。如此，就可以将工作站或其他终端设备直接连接到网桥组中所包含的接口。您不需要通过单独的物理交换机来连接这些设备，尽管您也可以将一台交换机连接到某个网桥组成员。

组成员没有 IP 地址。相反，所有成员接口共用桥接虚拟接口 (BVI) 的 IP 地址。如果在 BVI 上启用 IPv6，系统会自动为成员接口分配唯一的链路本地地址。

通常会在网桥组接口 (BVI) 上配置 DHCP 服务器，为通过成员接口连接的任何终端提供 IP 地址。不过，如果愿意的话，您也可以在连接到成员接口的终端上配置静态地址。网桥组中的所有终端都必须具有与网桥组 IP 地址位于同一子网的 IP 地址。

Note ISA 3000 设备预配置了名为 inside 的桥接组，其中包括除 outside 接口以外的所有数据接口。因此，设备已经预配置了一个端口用于连接到互联网或其他上游网络，而所有其他端口已启用并可用于直接连接终端。如果要将某个内部接口用于新的子网，必须先从 BVI 删除所需接口。

FDM 管理 设备仅支持一个网桥组；因此，思科防御协调器 只能管理该网桥组，而无法在设备上创建其他网桥组。

在 CDO 上创建网桥组后，在将配置部署到 FDM 管理 设备之前，您将不知道网桥组 ID。FDM 管理会分配网桥组 ID，例如 BVI1。如果删除了接口并创建了新的桥接组，则新桥接组的编号会递增，例如 BVI2。

准备工作

指定将成为网桥组 **成员** 的接口。具体而言，每个 **成员** 接口都必须满足以下要求：

- 该接口必须具有名称。

- 接口不能配置为**管理专用**接口。
- 该接口无法被配置为被动模式。
- 接口不能是 EtherChannel 接口或 EtherChannel 子接口。
- 该接口不能有任何已定义的 IPv4 或 IPv6 地址，无论是静态分配的还是通过 DHCP 获得的。如果需要从当前正在使用的某个接口删除地址，则可能还需要删除该接口的其他配置，例如静态路由、DHCP 服务器或 NAT 规则，具体视具有地址的接口而定。如果您尝试将具有 IP 地址的接口添加到网桥组，CDO 将向您发出警告。如果继续将接口添加到网桥组，CDO 将从接口配置中删除 IP 地址。
- BVI 可以将 VLAN 接口或其他路由接口作为成员接口，但不能将两个接口作为单个 BVI 上的成员接口。
- 接口不能是以太网的点对点协议 (PPPoE)
- 接口不能与安全区域关联（如果它在区域中）。您必须删除该接口的所有NAT规则，然后才能将其添加到网桥组。
- 单独启用和禁用成员接口。这样就可以禁用任何未使用的接口，而无需将其从网桥组删除。网桥组本身始终处于启用状态。
- 集群中不支持网桥组。

Note 在路由模式的 Firepower 2100 设备上，或在具有桥接 ixgbevf 接口的 VMware 上，网桥组不受支持。

配置桥接组接口的名称并选择桥接组成员

在此程序中，您将为网桥组接口 (BVI) 指定名称，并选择要添加到网桥组的接口：

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

步骤 2 点击 **设备 (Devices)** 选项卡以查找设备，或点击 **模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择要为其创建网桥组的设备。

步骤 4 执行以下操作之一：

- 选择 BVI 网桥组，然后在“操作”(Actions) 窗格中点击**编辑 (Edit)**。
- 点击加号按钮，然后选择网桥组接口。

Note 您可以创建并配置一个网桥组。如果已经定义了一个网桥组，则应编辑该组而非尝试创建新组。如果需要创建新的网桥组，则必须先删除现有网桥组。

步骤 5 进行以下配置：

- **逻辑名称 (Logical Name)** - 必须为网桥组指定名称。最多可以包含 48 个字符。字母字符必须为小写。例如 inside 或 outside。如果没有名称，将忽略其余的接口配置。

Note 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

- （可选）**说明 (Description)** - 说明最多为 200 个字符，单行，不能使用回车。

步骤 6 点击**网桥组成员 (Bridge Group Member)** 选项卡。一个网桥组最多可以包含 64 个接口或子接口。

- 选中接口以将其添加到网桥组。
- 取消选中要从网桥组中删除的接口。

步骤 7 点击**保存 (Save)**。

BVI 现在具有名称和成员接口。继续执行以下任务以配置网桥组接口。您不会为成员接口本身执行以下任务：

- 如果要为 BVI 分配 IPv4 地址，请为 BVI 配置 IPv4 地址。
- 如果要为 BVI 分配 IPv6 地址，请为 BVI 配置 IPv6 地址。
- 为网桥组接口配置高级接口选项。

为 BVI 配置 IPv4 地址

Procedure

步骤 1 选择要为其创建网桥组的设备。

步骤 2 在接口列表中选择 BVI，然后点击操作窗格中的**编辑 (Edit)**。

步骤 3 点击“IPv4 地址”(IPv4 Address) 选项卡以配置 IPv4 地址。

步骤 4 从类型字段中选择以下任一选项：

- **静态 (Static)** - 如果希望分配固定的地址，请选择此选项。键入网桥组的 IP 地址和子网掩码。所有连接的终端都将位于此网络中。对于预配置了网桥组的型号而言，BVI“inside”网络的默认值为 192.168.1.1/24（如 255.255.255.0）。确保该地址尚未在网络中使用。

  如果您配置了高可用性，并要监控此接口的高可用性，则还要在同一子网上配置一个备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

  Note 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。请参阅配置 DHCP 服务器。

- **动态 (DHCP) (Dynamic [DHCP])** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。网桥组通常不会使用此选项，但是您可以根据需要如此配置。如果您配置高可用性，将不能使用此选项。如有需要，更改以下选项：
  - “路由指标”(Route Metric) - 如果从 DHCP 服务器获取默认路由，则此选项是指与获知路由的管理距离，其值介于 1 到 255 之间。默认值为 1。
  - “获取默认路由”(Obtain Default Route) - 选中此选项以便从 DHCP 服务器获取默认路由。您通常会选择此选项，该选项是默认值。

步骤 5 继续执行以下程序之一：

- 如果要为 BVI 分配 IPv4 地址，请为 BVI 配置 IPv6 地址。
- 配置高级接口选项。
- 点击**保存 (Save)** 并将更改部署到 Firepower 设备。有关详细信息，请参阅将配置更改从 CDO 部署到 FDM 管理 设备。

为 BVI 配置 IPv6 地址

Procedure

步骤 1 点击“IPv6 地址” (IPv6 Address) 选项卡，然后为 BVI 配置 IPv6 地址。

步骤 2 配置 IPv6 地址的以下选项：

步骤 3 **启用 IPv6 处理 (Enable IPv6 processing)** - 在不想配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请将**状态**滑块滑至蓝色。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

Note 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

步骤 4 **抑制 RA (Suppress RA)** - 是否抑制路由器通告。Firepower 威胁防御设备可参与路由器通告，以便相邻设备可动态获知默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

也会发送路由器通告，以响应路由器请求消息（ICMPv6类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

对于不希望 FTD 设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

步骤 5 **静态地址/前缀 (Static Address/Prefix)** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅“IPv6 地址”。

步骤 6 **备用 IP 地址 (Standby IP Address)** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

步骤 7 继续执行以下程序之一：

- 配置高级接口选项。
- 点击**保存 (Save)** 并将更改部署到 Firepower 设备。有关详细信息，请参阅将配置更改从 CDO 部署到 FDM 管理 设备。

配置高级接口选项

请对网桥组 **成员** 接口配置大多数高级选项，不过其中一些选项可用于网桥组接口本身。

Procedure

步骤 1 高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。

步骤 2 点击**确定 (OK)**。

步骤 3 点击**保存 (Save)** 并将更改部署到 Firepower 设备。有关详细信息，请参阅将配置更改从 CDO 部署到 FDM 管理 设备。

What to do next

- 确保已启用您打算使用的所有成员接口。
- 为网桥组配置 DHCP 服务器。请参阅配置 DHCP 服务器。
- 将成员接口添加到相应的安全区。
- 确保各项策略（例如身份、NAT 和访问策略）可为网桥组和成员接口提供所需的服务。

FDM 管理 配置中的网桥组兼容性

在各种配置中，您可以指定接口，有时您将能够指定网桥虚拟接口 (BVI)，而有时您将能够指定网桥组的成员。此表阐述了何时可以使用 BVI，以及何时可以使用成员接口。

Firepower 威胁防御配置类型	可以使用 BVI	可以使用 BVI 成员
DHCP 服务器	是	否
DNS 服务器	是	是
管理访问	是	否
NAT（网络地址转换）	不支持	是

Firepower 威胁防御配置类型	可以使用 BVI	可以使用 BVI 成员
安全区	不支持	是
站点间 VPN 接入点	不支持	是
系统日志服务器	是	否

删除网桥组

删除网桥组时，其成员将变成标准路由接口，并且所有NAT规则或安全区成员身份保持不变。可以编辑这些接口为其提供 IP 地址。如果需要创建新的网桥组，则必须先删除现有网桥组。

Procedure

步骤 1 在导航窗格中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **FTD** 选项卡，然后选择要从中删除网桥组的设备。

步骤 4 选择 BVI 网桥组，然后在“操作”(Actions) 窗格中点击**删除 (Remove)**。

步骤 5 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

为 FDM 管理 设备添加 EtherChannel 接口

EtherChannel 接口限制

根据设备型号，EtherChannel可以包含多个同一介质类型和容量的成员接口，并且必须设置为相同的速度和双工模式。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如1GB和10GB接口）。链路汇聚控制协议 (LACP) 将在两个网络设备之间交换链路汇聚控制协议数据单元 (LACPDU)，进而汇聚接口。

根据物理配置和软件版本，EtherChannel 接口存在诸多限制。有关详细信息，请参阅以下部分。

一般接口限制

- EtherChannel 仅在运行 FDM 管理 版本 6.5 及更高版本的设备上可用。
- 思科防御协调器 支持以下 Firepower 设备上的 EtherChannel 接口配置：1010、1120、1140、1150、2110、2120、2130、2140、3110、3120、3130 和 3140。有关每个设备型号的接口限制，请参阅设备特定限制。
- 通道组中的所有接口都必须具有相同的介质类型和容量，并且必须设置为相同的速度和双工模式。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。
- EtherChannel 连接到的设备还必须支持 802.3ad EtherChannel。

- FDM 管理 设备不支持带有 VLAN 标记的 LACPDU。如果使用 Cisco IOS vlan dot1Q tag native 命令在相邻交换机上启用本地 VLAN 标记，则 FDM 管理 设备将会丢弃已标记的 LACPDU。请务必禁用相邻交换机上的本地 VLAN 标记。
- 所有 FDM 管理 设备配置均引用 EtherChannel 接口，而不是成员物理接口。
- 端口通道接口会被显示为物理接口。

设备特定限制

以下设备具有特定的接口限制：

1000 系列

- Firepower 1010 最多支持 8 个 EtherChannel 接口。
- Firepower 1120、1140、1150 最多支持 12 个 EtherChannel 接口。
- 1000 系列不支持 LACP 快速速率； LACP 始终使用正常速率。此设置不可配置。

2100 系列

- Firepower 2110 和 2120 型号最多支持 12 个 EtherChannel 接口。
- Firepower 2130 和 2140 型号最多支持 16 个 EtherChannel 接口。
- 2100 系列不支持 LACP 快速速率； LACP 始终使用正常速率。此设置不可配置。

Secure Firewall 3100 系列

- 所有 Secure Firewall 3100 型号最多支持 16 个 EtherChannel 接口。
- Secure Firewall 3100 型号支持 LACP 快速速率。
- Secure Firewall 3100 系列型号不支持启用或禁用网络模块，以及接口的分支在线插入和删除 (OIR)。

4100 系列和 9300 系列

- 您无法在 4100 和 9300 系列上创建或配置 EtherChannel。必须在 FXOS 机箱中配置这些设备的 Etherchannel。
- 4100 和 9300 系列上的以太网通道会在 思科防御协调器 中显示为物理接口。

添加 EtherChannel 接口

使用以下程序将 EtherChannel 添加到 FDM 托管设备：

Note 如果要立即创建另一个 EtherChannel，请选中**创建另一个 (Create another)** 复选框，然后点击**创建 (Create)**。

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **FTD** 选项卡，然后选择要将 Etherchannel 添加到的设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击**接口 (Interfaces)**。

步骤 5 点击蓝色加号按钮  ，然后选择 **EtherChannel**。

步骤 6 （可选）输入**逻辑名称 (Logical Name)**。

步骤 7 （可选）输入说明。

步骤 8 输入 **EtherChannel ID**。

对于 Firepower 1010 系列，请输入一个介于 1 和 8 之间的值。

对于 Firepower 2100、3100、4100 和 9300 系列，请输入一个介于 1 和 48 之间的值。

步骤 9 点击**链路汇聚控制协议 (Link Aggregation Control Protocol)** 的下拉按钮，然后选择以下两个选项之一：

- **Active (活动)** - 发送和接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。
- **开 (On)** - EtherChannel 始终开启，并且不使用 LACP。**开启**的 EtherChannel 只能与另一个**开启**的 EtherChannel 建立连接。

步骤 10 搜索并选择要作为成员包含在 EtherChannel 中的接口。您**必须**包含至少一个接口。

警告：如果您将 EtherChannel 接口添加为成员，并且该接口已配置了 IP 地址，则 CDO 会删除该成员的 IP 地址。

步骤 11 点击**创建**。

相关信息：

- 编辑或删除 FDM 管理 设备的 EtherChannel 接口
- 将子接口添加到 EtherChannel 接口
- 从 EtherChannel 编辑或删除子接口
- Firepower 接口配置的指南和限制
- 将 FDM 管理设备接口分配给安全区域
- 为 FDM 管理 设备添加 EtherChannel 接口, on page 249

编辑或删除 FDM 管理 设备的 EtherChannel 接口

使用以下程序修改现有 EtherChannel 接口，或从 FDM 管理 设备中删除 EtherChannel 接口。

编辑 EtherChannel

请注意，EtherChannel有几个限制，您在修改时必须加以注意。有关详细信息，请参阅EtherChannel。

Note EtherChannel 必须至少有一个成员。

使用以下程序可编辑现有 EtherChannel：

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **FTD** 选项卡，然后选择与要修改的 Etherchannel 关联的 威胁防御。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击 **接口 (Interfaces)**。

步骤 5 在**接口 (Interfaces)** 页面上，选择要编辑的 EtherChannel 接口。在位于右侧的“操作”(Actions) 窗格中，点击编辑图标 。

步骤 6 修改以下任何项目：

- 逻辑名称。
- 州/省/自治区。
- 说明。
- 安全区域分配。
- 链路汇聚控制协议状态。
- **IPv4**、**IPv6** 或**高级 (Advanced)** 选项卡中的 IP 地址配置。
- EtherChannel 成员。

Warning **警告**：如果您将 EtherChannel 接口添加为成员，并且该接口已配置了 IP 地址，则 CDO 会删除该成员的 IP 地址。

步骤 7 点击**保存 (Save)**。

删除 ASA EtherChannel 接口

Note 与高可用性 (HA) 或任何其他配置关联的 EtherChannel 接口。您必须先从所有配置中手动删除 EtherChannel 接口，然后再将其从 CDO 中删除。

使用以下程序从 FDM 管理设备中删除 EtherChannel 接口：

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **FTD** 选项卡以及与要删除的 Etherchannel 关联的 威胁防御。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击**接口 (Interfaces)**。

步骤 5 在**接口 (Interfaces)** 页面上，选择要编辑的 EtherChannel 接口。在右侧的“操作”(Actions) 窗格中，点击**删除 (Remove)**。

步骤 6 确认要删除 EtherChannel 接口，然后点击**确定 (OK)**。

将子接口添加到 EtherChannel 接口

EtherChannel 子接口

通过**接口 (Interfaces)** 页面，您可以通过展开每个接口来查看设备的哪些接口具有子接口。这个展开的视图还会显示子接口的唯一逻辑名称、启用/禁用状态、任何关联的安全区域和模式。子接口的接口类型和模式由父接口确定。

一般限制

CDO 不支持以下接口类型的子接口：

- 配置为仅用于管理的接口。
- 为交换机端口模式配置的接口。
- 被动接口。
- VLAN 接口。
- 网桥虚拟接口 (BVI)。
- 已经是另一个 EtherChannel 接口的成员的接口。

您**可以**为以下对象创建子接口：

- 网桥组成员。
- EtherChannel 接口。
- 物理接口。

将子接口添加到 EtherChannel 接口

使用以下程序将子接口添加到现有接口：

Note 如果要立即创建另一个子接口，请选中**创建另一个 (Create another)** 复选框，然后点击**创建 (Create)**。

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **FTD** 选项卡，然后选择要将 Etherchannel 添加到的 威胁防御。在右侧的“管理”(Management) 窗格中，点击**接口 (Interfaces)**。

步骤 4 选择要为其分组子接口的接口。在位于右侧的“操作”(Action) 窗格中，点击 + New Subinterface 按钮。

步骤 5 （可选）输入**逻辑名称 (Logical Name)**。

步骤 6 （可选）输入说明。

步骤 7 （可选）为子接口分配安全区域。请注意，如果子接口没有逻辑名称，则您无法分配安全区域。

步骤 8 输入 VLAN ID。

步骤 9 输入 **EtherChannel ID**。使用 1 到 48 之间的值；对于 Firepower 1010 系列，请使用 1 到 8 之间的值。

步骤 10 选择 **IPv4**、**IPv6** 或**高级 (Advanced)** 选项卡以配置子接口的 IP 地址。

步骤 11 点击**创建**。

从 EtherChannel 编辑或删除子接口

使用以下程序修改现有子接口，或从 Etherchannel 接口删除子接口。

Note 子接口和 EtherChannel 接口具有一系列可能会影响配置的准则和限制。有关详细信息，请参阅一般限制。

编辑子接口

使用以下程序编辑与 EtherChannel 接口关联的现有子接口：

Procedure

步骤 1 登录 CDO。

步骤 2 在导航窗格中，点击**清单 (Inventory)**。

步骤 3 点击**设备**选项卡。

步骤 4 点击 **FTD** 选项卡，然后选择与要编辑的 EtherChannel 和子接口关联的 威胁防御。

步骤 5 在右侧的**管理 (Management)** 窗格中，点击**接口 (Interfaces)**。

步骤 6 找到并展开子接口所属的 Etherchannel 接口。

步骤 7 选择要编辑的子接口。在位于右侧的“操作”(Action) 窗格中，点击编辑图标 。

步骤 8 修改以下任何项目：

- 逻辑名称。
- 州/省/自治区。
- 说明。
- 安全区域分配。
- VLAN ID
- IPv4、IPv6 或高级 (Advanced) 选项卡中的 IP 地址配置。

步骤 9 点击**保存 (Save)**。

从 EtherChannel 中删除子接口

使用以下程序从 EtherChannel 接口删除现有子接口：

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **FTD** 选项卡，然后选择与要编辑的 EtherChannel 和子接口关联的 威胁防御。在右侧的“管理”(Management) 窗格中，点击**接口 (Interfaces)**。

步骤 4 找到并展开子接口所属的 Etherchannel 接口。

步骤 5 选择要删除的子接口。

步骤 6 在右侧的“操作”(Actions) 窗格中，点击**删除 (Remove)**。

步骤 7 确认要删除子接口，然后点击**确定 (OK)**。

将接口添加到虚拟 FDM 管理设备

在部署虚拟 FDM 管理设备时，可以将接口分配给虚拟机。然后，在 FDM 管理设备中，使用与配置硬件设备相同的方法配置这些接口。

但是，您无法给虚拟机添加更多虚拟接口，然后让 FDM 来自动识别它们。如果您需要为虚拟 FDM 管理设备配置更多物理接口对等体，那基本上需要重新执行该流程。您可以部署新的虚拟机，也可以使用以下程序。

Caution 要给虚拟机添加接口，您需要完全清除虚拟FDM管理配置。配置中唯一保留不变的部分是管理地址和网关设置。

准备工作

在 FDM 管理设备中执行以下操作：

- 检查虚拟 FDM 管理设备配置并记下要在新虚拟机中复制的设置。
- 选择**设备 (Devices) > 智能许可证 (Smart License) > 查看配置 (View Configuration)** 并禁用所有功能许可证。

Procedure

步骤 1 关闭虚拟 FDM 管理设备。

步骤 2 使用虚拟机软件，将接口添加到虚拟 FDM 管理设备。对于 VMware，默认情况下，虚拟设备使用 e1000（1 千兆位/秒）接口。您还可以使用 vmxnet3 或 ixgbe（10 千兆位/秒）接口

步骤 3 打开虚拟 FDM 管理设备电源。

步骤 4 打开虚拟FDM管理设备控制台，删除本地管理器，然后启用本地管理器。删除本地管理器，然后启用本地管理器，重置设备配置，并让系统识别新接口。管理接口配置不会重置。以下 SSH 会话会显示相应命令。

```
> show managers
Managed locally.
> configure manager delete
If you enabled any feature licenses, you must disable them in Firepower Device Manager
before deleting the local manager. Otherwise, those licenses remain assigned to the device
 in Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
DCHP Server Disabled
> show managers
No managers configured.
> configure manager local
>
```

步骤 5 打开浏览器并连接到FDM管理设备，完成设备安装向导，并配置设备。有关详细说明，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南，版本 xxx》指南中的“完成初始配置”部分。

FDM 管理 设备的交换机端口模式接口

对于各物理 Firepower 1010 接口，可以将其操作设置为防火墙接口或交换机端口。交换机端口使用硬件中的交换功能在第 2 层转发流量。同一 VLAN 上的交换机端口可使用硬件交换互相通信，且流量不受FDM管理 设备安全策略的限制。接入端口仅接受未标记流量，可以将其分配给单个VLAN。中继端口接受未标记和已标记流量，且可以属于多个 VLAN。对于已重新映像到版本 6.4 的设备，以太网 1/2 至 1/8 配置为 VLAN 1 上的接入交换机端口；手动升级到版本 6.4（及更高版本）的设备，

以太网配置会在升级之前保留配置。请注意，同一 VLAN 上的交换机端口可使用硬件交换互相通信，且流量不受 FDM 管理 设备安全策略的限制。

访问或中继

配置为交换机端口的物理接口可以分配为接入端口或中继端口。

接入端口仅将流量转发到一个 VLAN，并且仅接受未标记的流量。如果您打算将流量转发到单个主机或设备，我们强烈建议使用此选项。您还必须指定要与接口关联的 VLAN，否则将默认为 VLAN 1。

中继端口将流量转发到多个 VLAN。您必须分配一个 VLAN 接口作为本地中继端口，并至少分配一个 VLAN 作为关联中继端口。最多可以选择 20 个接口与交换机端口接口关联，这使来自不同 VLAN ID 的流量能够通过交换机端口接口。如果未标记流量通过交换机端口，则使用本征 VLAN 接口的 VLAN ID 标记流量。请注意，1002 和 1005 之间的默认光纤分布式数据接口 (FDDI) 和令牌环 ID 不能用于 VLAN ID。

更改端口模式

如果选择为路由模式配置的接口作为 VLAN 成员，CDO 会自动将该接口转换为交换机端口模式，并将该接口默认配置为接入端口。因此，逻辑名称和关联的静态 IP 地址将从接口中删除。

配置限制

请注意以下限制：

- 只有物理 Firepower 1010 设备支持交换机端口模式配置。虚拟 FDM 管理 设备不支持交换机端口模式。
- Firepower 1010 设备最多允许 60 个 VLAN。
- 为交换机端口模式配置的 VLAN 接口必须是未命名的。这意味着 MTU **必须**被配置为 1500 字节。
- 您 **不能** 将配置为交换机端口模式的接口删除。您必须手动将接口模式从**交换机端口**模式更改为**已路由**模式。
- 为交换机端口模式配置的接口不支持 IP 地址。如果接口当前已在 VPN、DHCP 中引用或配置，或者已与静态路由关联，则**必须**手动删除 IP 地址。
- 不能将桥接组接口的任何成员用作交换机端口。
- VLAN 接口的 MTU **必须**为 1500 字节。未命名的 VLAN 接口不支持任何其他配置。
- 交换机端口模式不支持以下选项：
  - 诊断接口。
  - 动态、组播、等价多路径 (ECMP) 路由。
  - 被动接口。
  - 端口 etherchannel，或使用作为 etherchannel 成员的接口。

- 子接口。
- 故障切换和状态链路。

高可用性和交换机端口接口

使用高可用性时，不应使用交换机端口功能。由于交换机端口在硬件中运行，因此它们会继续在主用和备用设备上传递流量。高可用性旨在防止流量通过备用设备，但此功能不会扩展到交换机端口。在正常高可用性网络设置中，两台设备上的活动交换机端口将导致网络环路。建议将外部交换机用于任何交换功能。请注意，VLAN接口可通过故障转移监控，而交换机端口无法通过故障转移监控。

Note 仅可使用防火墙接口作为故障切换链路。

模板中的交换机端口模式配置

您可以使用为交换机端口模式配置的接口创建设备模板。将接口从模板映射到设备时，请注意以下情况：

- 如果模板接口在应用模板之前不包含任何 VLAN 成员，则 CDO 会自动将其映射到具有相同属性的可用设备接口。
- 如果不包含 VLAN 成员的模板接口映射到配置为 **N/A** 的设备接口，则 CDO 会自动在要应用模板的设备上创建接口
- 如果包含 VLAN 成员的模板接口映射到不存在的设备接口，则应用模板将**失败**。
- 模板不支持将多个模板接口映射到同一设备接口。
- 模板的管理接口必须映射到设备的管理接口。

配置 FDM 管理设备 VLAN

如果要配置子接口或交换机端口，您必须先配置 VLAN 接口。

Note 一个 FDM 管理 设备最多支持 60 个 VLAN 接口。

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择要在其上创建 VLAN 的所需设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击**接口 (Interfaces)**。

步骤 5 在**接口 (Interfaces)** 页面上，点击  按钮。

步骤 6 进行以下配置：

- **父接口 (Parent Interface)** - 父接口是将子接口添加至其中的物理接口。创建子接口后，父接口则无法更改。
- （可选）**逻辑名称 (Logical Name)** - 设置 VLAN 名称，最多 48 个字符。字母字符必须为小写。如果不希望在 VLAN 和其他 VLAN 或防火墙接口之间进行路由，则将 VLAN 接口名称留空。

  Note 如果未输入名称，则必须将**高级选项 (Advanced Options)** 中的 MTU 设为 1500。如果将 MTU 更改为 1500 以外的值，则不得为 VLAN 命名。

- （可选）**说明 (Description)** - 说明最多为 200 个字符，单行，不能使用回车。
- （可选）**安全区域 (Security Zone)** - 将子接口分配给安全区域。请注意，如果子接口没有逻辑名称，则您无法分配该子接口。您还可以在创建子接口后分配安全区域。有关详细信息，请参阅在 Firepower 接口设置中使用安全区域。
- （可选）**VLAN ID** - 输入 VLAN ID，介于 1 和 4070 之间，用于标记该子接口上的数据包。

  Note 默认情况下会路由 VLAN 接口。如果将此 VLAN 接口添加至网桥组，则 思科防御协调器 (CDO) 会将模式自动更改为 **BridgeGroupMember**。同样，如果将此 VLAN 接口更改为交换机端口模式，则CDO会自动将模式更改为**交换机端口 (Switch Port)**。

- （可选）**子接口 ID (Subinterface ID)** - 以整数形式输入介于 1 和 4294967295 之间的子接口 ID。此 ID 附加至接口 ID；例如 Ethernet1/1.100。方便起见，您可以匹配 VLAN ID，但这不是必需的。创建子接口后，则无法更改该 ID。

步骤 7 点击 **IPv4 地址 (IPv4 Address)** 选项卡，然后从类型字段中选择以下选项之一：

- **静态 (Static)** - 如果希望分配固定的地址，请选择此选项。对于连接到接口的网络，键入接口的 IP 地址和子网掩码。例如，如果您连接的是 10.100.10.0/24 网络，则可以输入 10.100.10.1/24。确保该地址尚未在网络中使用。

  如果您配置了高可用性，并要监控此接口的高可用性，则还要在同一子网上配置一个备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

  Note 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。有关详细信息，请参阅配置 DHCP 服务器。

- **动态 (DHCP) (Dynamic [DHCP])** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。如果您配置高可用性，将不能使用此选项。如有需要，更改以下选项：
  - **路由指标 (Route Metric)** - 如果从 DHCP 服务器获取默认路由，则此选项是指与获知路由的管理距离，其值介于 1 到 255 之间。默认值为 1。
  - **获取默认路由 (Obtain Default Route)** - 选中此选项以便从 DHCP 服务器获取默认路由。您通常会选择此选项，该选项是默认值。

- **DHCP 地址池 (DHCP Address Pool)** - 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。

步骤 8 （可选）点击 **IPv6 地址 (IPv6 Address)** 选项卡并配置以下内容：

- **状态 (State)** - 在不想配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请将状态滑块滑至蓝色。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

  Note 禁用 IPv6 不会禁用接口上使用显式 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **地址自动配置 (Address Auto Configuration)** - 选中此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

- **抑制 RA (Suppress RA)** - 是否抑制路由器通告。威胁防御 可以参与路由器通告，以便邻居设备可以动态获悉默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）。

  也会发送路由器通告，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

  对于不希望 FDM 管理 设备提供 IPv6 前缀的任何接口（例如外部接口），我们建议抑制接口上的这些消息。

- **静态地址/前缀 (Static Address/Prefix)** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅 Firepower 接口的 IPv6 寻址。

- **备用 IP 地址 (Standby IP Address)** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

步骤 9 （可选）点击**高级 (Advanced)** 选项卡。

- 如果您想让系统在决定是否故障切换到高可用性配置中的对等设备时考虑接口的运行状况，请选择**启用高可用性监控**。

  如果不配置高可用性，可忽略此选项。如果不配置接口的名称，也可以忽略此选项。

- 选择**仅管理 (Management Only)** 以便将数据接口仅用于管理。

  仅管理接口不允许直通流量，所以将数据接口设置为仅管理的价值微乎其微。不能更改管理/诊断接口的此项设置，它们始终为仅管理。

- 修改 IPv6 配置设置。

  - **启用 DHCP 以获取 IPv6 地址配置 (Enable DHCP for IPv6 address configuration)** - 是否在 IPv6 路由器通告数据包中设置“托管地址配置”标志。此标志通知 IPv6 自动配置客户端应使用 DHCPv6 来获取相关地址以及派生的无状态自动配置地址。

- **启用 DHCP 以获取 IPv6 非地址配置 (Enable DHCP for IPv6 non-address configuration)** - 是否在 IPv6 路由器通告数据包中设置“其他地址配置”标志。此标志通知 IPv6 自动配置客户端应使用 DHCPv6 从 DHCPv6 获取其他信息，如 DNS 服务器地址。
- **DAD 尝试 (DAD Attempts)** - 接口执行重复地址检测 (DAD) 的频率，介于 0 - 600 之间。默认值为 1。在无状态自动配置过程中，DAD 会验证新单播 IPv6 地址的唯一性，再将地址分配给接口。如果重复地址是接口的链路本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。接口将使用邻居的询求消息来执行重复地址检测。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。

- 将 **MTU**（最大传输单位）更改为所需的值。

  默认 MTU 为 1500 字节。您可以指定介于 64 - 9198（或为虚拟 FDM 管理 设备指定 9000，并为 Firepower 4100/9300 指定 9184）之间的值。如果通常在网络中使用巨帧，请设置一个较大的值。

  Note 如果在 ASA 5500-X 系列设备、ISA 3000 系列设备或虚拟 FDM 管理 设备上将 MTU 提高到 1500 以上，则必须重命名 VLAN **并**重新启动设备。登录 CLI 并使用 reboot 命令。如果设备已为 HA，还须重新启动备用设备。无需重新启动 Firepower 型号，因为巨帧支持在该型号上始终启用。

- （对于子接口和 HA 对为可选）配置 **MAC 地址 (MAC address)**。

  默认情况下，系统对接口使用预烧到网络接口卡 (NIC) 的 MAC 地址。因此，该接口上的所有子接口都使用相同的 MAC 地址，也因此您可能想要为每个子接口创建唯一地址。如果您配置高可用性，建议手动配置主用/备用 MAC 地址。定义 MAC 地址有助于在故障转移时保持网络中的一致性。

  - **MAC 地址 (MAC Address)** - 采用 H.H.H 格式的介质访问控制，其中 H 是 16 位十六进制数字。例如，您可以将 MAC 地址 00-0C-F1-42-4C-DE 输入为 000C.F142.4CDE。MAC 地址不能设置组播位，即左起第二个十六进制数字不能是奇数。
  - **备用 MAC 地址 (Standby MAC Address)** - 用于 HA 对。如果主用设备发生故障切换，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

步骤 10 如果要为此设备创建另一个子接口，请在完成子接口配置之前选中**创建另一个 (Create another)**。

步骤 11 （可选）将弹出窗口右上角的**状态**滑块从灰色切换为蓝色，以便在创建时激活子接口。

步骤 12 点击**确定 (OK)**。

步骤 13 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

为交换机端口模式配置 FDM 管理 设备 VLAN

在配置之前，请务必阅读交换机端口模式的限制；有关详细信息，请参阅 FDM 管理 设备的交换机端口模式接口。

Note 您可以随时为物理接口分配或编辑 VLAN 成员。请务必在确认新配置后将更改部署到设备。

为交换机端口模式创建 VLAN 接口

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择要为其配置接口的设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击**接口 (Interfaces)**。

步骤 5 在**接口 (Interfaces)** 页面上，点击  按钮并选择 **VLAN 接口 (VLAN Interface)**。

步骤 6 查看 **VLAN 成员 (VLAN Members)** 选项卡并选择所需的物理接口。

Note 如果您选择添加引用为接入或本地中继配置的VLAN接口的成员，则只能选择一个VLAN作为成员。引用为关联中继配置的VLAN接口的物理接口最多支持20个接口作为成员。

步骤 7 配置 VLAN 接口的其余部分，如配置 FDM 管理设备 VLAN 中所述。

步骤 8 点击**保存 (Save)**。确认要重置 VLAN 配置并为接口重新分配 IP 地址。

步骤 9 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

为交换机端口模式配置现有物理接口

Procedure

步骤 1 在导航窗格中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击 **设备 (Devices)** 选项卡以查找设备，或点击 **模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择要为其配置接口的设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击**接口 (Interfaces)**。

步骤 5 在**接口 (Interfaces)** 页面上，选择要修改的物理接口。在右侧的“操作”(Actions) 窗格中，点击编辑图标  。

步骤 6 为交换机端口模式配置的接口不支持逻辑名称。如果接口具有逻辑名称，请将其删除。

步骤 7 找到**模式 (Mode)** 并使用下拉菜单选择**交换机端口 (Switch Port)**。

步骤 8 为交换机端口模式配置物理接口：

- （可选）选中**受保护端口 (Protected Port)** 复选框以将此交换机端口设置为受保护端口，因此您可以阻止交换机端口与同一 VLAN 上的其他受保护交换机端口进行通信。在以下情况下，您可能想要防止交换机端口相互之间进行通信：主要从其他 VLAN 访问这些交换机端口上的设备；

您不需要允许 VLAN 间访问；由于病毒感染或其他安全漏洞，您想要将设备相互隔离开。例如，如果具有托管 3 台 Web 服务器的 DMZ，则在您将此选项应用于各交换机端口后，则可以将 Web 服务器相互隔离。内部网络和外部网络均可以与这 3 台网络服务器进行通信，反之亦然，但这些网络服务器相互之间无法进行通信。

- 对于使用类型，请选择**访问 (Access)** 或**中继 (Trunk)**。请参阅FDM 管理 设备的交换机端口模式接口，以确定所需的端口类型。
  - 如果选择**中继 (Trunk)**，则您必须选择一个 VLAN 接口作为**本地中继 (Native Trunk) VLAN** 以转发未标记流量，并至少选择一个**关联 VLAN (Associated VLAN)** 以转发标记流量。点击  图标以查看现有物理接口。最多可以选择 20 个 VLAN 接口作为关联的 VLAN。
  - 您可以通过点击**新建 VLAN (C reate new VLAN)** 来创建被设为访问模式的新 VLAN 接口。

步骤 9 点击**保存 (Save)**。确认要重置 VLAN 配置并为接口重新分配 IP 地址。

步骤 10 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

查看和监控 Firepower 接口

要查看 Firepower 接口，请执行以下步骤：

Procedure

步骤 1 在导航窗格中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击 **设备 (Devices)** 选项卡以查找设备，或点击 **模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后点击要查看其接口的设备。

步骤 4 在右侧的“管理”(Management) 窗格中选择**接口 (Interfaces)** ⌂。

步骤 5 在“接口”(Interfaces) 表中选择一个接口

- 如果展开接口行，您就会看到子接口信息。
- 在右侧，您将看到详细的接口信息。

在 CLI 中监控接口

您可以通过使用 SSH 连接到设备并运行下面的命令来查看有关接口的一些基本信息、行为和统计信息。

要使用 SSH 轻松连接到设备，请将要监控的 FDM 管理设备作为 SSH 设备载入，然后使用 CDO 中的 >_ 命令行接口。

- **show interface** 显示接口统计信息和配置信息。此命令有许多关键字，可用于获取所需的信息。使用 ? 作为关键字可查看可用选项。
- **show ipv6 interface** 显示有关接口的 IPv6 配置信息。
- **show bridge-group** 显示有关桥接虚拟接口 (BVI) 的信息，包括成员信息和 IP 地址。
- **show conn** 显示有关当前通过接口建立的连接的信息。
- **show traffic** 显示有关流经每个接口的流量的统计信息。
- **show ipv6 traffic** 显示有关流经设备的 IPv6 流量的统计信息。
- **show dhcpd** 显示有关接口上的 DHCP 使用情况的统计信息和其他信息，特别是有关接口上配置的 DHCP 服务器的信息。

使用 FXOS 同步添加到 Firepower 设备的接口

在 Firepower 4100 系列或 9300 系列设备上，如果使用 Firepower 可扩展操作系统 (FXOS) 机箱管理器将接口添加到 Firepower 设备，则 思科防御协调器 不会识别该配置更改并报告配置冲突。

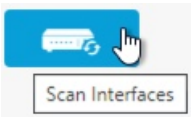
要在 CDO 中查看新添加的接口，请执行以下程序：

过程

步骤 1 登录至 FDM 管理 设备。

步骤 2 在 FDM 管理 主页中，点击“接口”(Interfaces) 面板中的**查看所有接口 (View All Interfaces)**。

步骤 3 点击**扫描接口 (Scan Interfaces)** 按钮：



步骤 4 等待接口扫描，然后点击**确定 (OK)**。

步骤 5 将更改部署到 FDM 管理 设备。

步骤 6 以管理员或超级管理员身份登录到 CDO。

步骤 7 在导航窗格中，点击**清单 (Inventory)**。

步骤 8 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 9 点击 **FTD** 选项卡，然后选择具有预期新接口配置的设备。

步骤 10 点击**检查更改 (Check for Changes)**，立即将设备上的配置副本与 CDO 上存储的配置副本进行比较。CDO 将检测接口更改，并在设备的**清单 (Inventory)** 页面上报告“检测到冲突”(Conflict Detected) 状态。

步骤 11 点击**查看冲突 (Review Conflict)**，然后接受带外更改，以便解决检测到的冲突。

路由

所谓路由是指通过网络将信息从源发送到目标的活动。在途中通常会经过至少一个中间节点。路由涉及两个基本活动：确定最佳路由路径和通过网络传输数据包。

通过使用 Cisco Defense Orchestrator (CDO)，您可以为 Firepower 威胁防御 (FTD) 设备定义默认路由和其他静态路由。以下主题介绍路由的基本信息以及如何使用 CDO 在 FDM 管理 设备上配置静态路由。

- 关于静态路由和默认路由
- 路由表和路由选择
- 为 FDM 管理 设备配置静态路由和默认路由
- 监控路由

关于静态路由和默认路由

要将流量路由到非连接的主机或网络，您必须定义到主机或网络的路由。该定义的路由是静态路由。还要考虑配置一个默认路由。所有流量的默认路由（不是通过其他方式路由到默认网络网关），通常是指下一跳路由器。

相关信息：

- 默认路由
- 静态路由

默认路由

如果您不知道通往某个特定网络的路由，最简单的方法是配置一个默认路由，将所有流量都发送到上游路由器，从而依靠该路由器来为您路由流量。默认路由对网关 IP 地址进行标识，FTD 设备会将您没有定义静态路由的 IP 数据包发送到该地址。默认路由是以 0.0.0.0/0 (IPv4) 或 ::/0 (IPv6) 作为目标 IP 地址的静态路由。

静态路由

静态路由是从一个网络到另一个网络的路由，您可以手动定义并输入到路由表中。在以下情况下，您可能希望使用静态路由：

- 您的网络规模小且稳定，可以轻松管理设备之间的手动添加和更改路由。
- 您的网络使用不受支持的路由器发现协议。
- 不希望流量或 CPU 开销与路由协议相关联。

- 在某些情况下，仅使用默认路由并不足够。默认网关可能无法到达目标网络，因此还必须配置更具体的静态路由。例如，如果默认网关在外部，则默认路由无法将直接流量定向到未直接与 FDM 管理设备连接的任何内部网络。
- 您使用的是不支持动态路由协议的功能。

限制：

- CDO 当前不支持在 ASA 或 FDM 管理 设备上管理、监控或使用虚拟隧道接口 (VTI) 隧道。已配置 VTI 隧道的设备可以载入 CDO，但它会忽略 VTI 接口。如果安全区域或静态路由引用 VTI，则 CDO 会读取不带 VTI 引用的安全区域和静态路由。即将推出对 VTI 隧道的 CDO 支持。
- FDM 管理 在软件版本 7.0 或更高版本上运行的设备允许配置等价多路径 (ECMP) 流量区域。当 FDM 管理设备载入 CDO 时，它可以读取但不能修改全局 VRF 路由中可用的 ECMP 配置，因为它不允许具有相同指标值的同一目标网络的路由。您可以通过 FDM 创建和修改 ECMP 流量区域，然后再将其读入 CDO。有关 ECMP 的详细信息，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南，版本 7.0 或更高版本》的“路由基础知识和静态路由”一章中的“等价多路径 (ECMP) 路由”部分。

路由表和路由选择

如果 NAT 转换 (xlates) 和规则无法确定传出接口，系统将使用路由表来确定数据包的路径。

路由表中的路由包括一个名为“管理距离”的指标，提供相对于既定路由的优先级。如果某个数据包与多个路由条目匹配，则使用距离最短的路由。直连网络（在接口上定义的网络）的距离为 0，因此始终首选使用此网络。静态路由的默认距离为 1，但您可以使用 1-254 之间的任意距离创建默认距离。

标识具体目标的路由优先于默认路由（即目标为 0.0.0.0/0 或 ::/0 的路由）。

如何填充路由表

可以使用静态定义的路由和直连路由来填充 FDM 管理设备路由表。可以通过多种方式来输入相同的路由。当在路由表中放入同一目标的两条路由时，将按如下确定保留在路由表中的路由：

- 如果两个路由具有不同的网络前缀长度（网络掩码），则会将两个路由都视为唯一并输入到路由表中。然后，由数据包转发逻辑确定使用哪一条路由。

例如，假设在路由表中输入了以下路由：

- 192.168.32.0/24
- 192.168.32.0/19

即使 192.168.32.0/24 路由具有更长的网络前缀，但由于两条路由具有不同的前缀长度（子网掩码），因此均会安装在路由表中。这两条路由被视为不同目标，数据包转发逻辑会确定使用哪条路由。

- 如果在路由表中输入了通向同一目的地的多条路径，则与静态路由一起输入的具有更好度量的路由将被输入到路由表中。

度量是与特定路由关联的值，从最高优先到最低优先进行排序。用于确定度量的参数根据路由协议而异。具有最低指标的路径选择作为最佳路径并安装在路由表中。如果有多个度量相等的通向同一目的地的路径，则会在这些等价路径上进行负载均衡。

相关信息：

- 如何制定转发决策

如何制定转发决策

按以下顺序做出转发决策：

- 使用 NAT 转换 (xlate) 和规则来确定出口接口。如果 NAT 规则无法确定传出接口，系统将使用路由表来确定数据包的路径。
- 如果目的不匹配路由表中的条目，则通过为默认路由指定的接口转发数据包。如果尚未配置默认路由，则会丢弃数据包。
- 如果目的匹配路由表中的单个条目，则通过与该路由关联的接口转发数据包。
- 如果目的匹配路由表中的多个条目，则通过与具有较长网络前缀的路由相关联的接口转发数据包。例如，发往 192.168.32.1 的数据包到达在路由表中拥有以下路由的接口：
- 192.168.32.0/24 网关 10.1.1.2
- 192.168.32.0/19 网关 10.1.1.3

在这种情况下，发往 192.168.32.1 的数据包直接发送到 10.1.1.2，因为 192.168.32.1 属于 192.168.32.0/24 网络。它也属于路由表中的其他路由，但 192.168.32.0/24 在路由表中的前缀更长（24 位对比 19 位）。在转发数据包时，较长前缀始终优先于较短的前缀。

Note 即便新的相似连接将因路由中的变化而导致不同行为，现有连接也将继续使用其已建立的接口。

为 FDM 管理 设备配置静态路由和默认路由

在 Firepower 威胁防御 (FTD) 设备上定义静态路由，以告知系统从何处发送的数据包不会绑定至直连到系统接口的网络。

考虑创建默认路由。这是网络 0.0.0.0/0 的路由。如果数据包的传出接口无法由现有 NAT 转换、静态 NAT 规则或其他静态路由确定，则此路由为所发送的数据包定义目的。

如果无法使用默认网关到达所有网络，则可能需要其他静态路由。例如，默认路由通常是外部接口上的上游路由器。如果还有其他未直连到设备的内部网络，并且通过默认网关无法访问它们，则需要对每个此类内部网络使用静态路由。

对于直连到系统接口的网络，无法定义静态路由。系统自动创建这些路由。

操作步骤

Procedure

步骤 1 在导航窗格中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击 **设备 (Devices)** 选项卡以查找设备，或点击 **模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 设备，然后选择要定义静态路由的设备。

步骤 4 在左侧的**管理 (Management)** 窗格中，点击 **路由 (Routing)**。

步骤 5 在静态路由页中，执行以下某项操作：

- 要添加新的静态路由，请点击加号按钮  。
- 点击要编辑的路由的编辑图标。

如果不再需要路由，请点击该路由的垃圾桶图标将其删除。

步骤 6 配置路由属性。

- **协议** - 选择路由是用于 IPv4 还是 IPv6 地址。
- **接口 (Interface)** - 选择要通过其发送流量的接口。通过此接口需能够访问网关地址。
- **网关 (Gateway)** - 选择标识网关 IP 地址的主机网络对象至目标网络。流量将发送至此地址。
- **度量 (Metric)** - 路由的管理距离，该值介于 1 和 254 之间。静态路由的默认值为 1。如果接口和网关之间还有其他路由器，请输入跳数作为管理距离。

  管理距离是用于比较路由的参数。数字越小，为该路由指定的优先级越高。连接的路由（直连到设备接口的网络）始终优先于静态路由。
- **目标网络 (Destination Network)** - 选择标识目标网络的网络对象，该目标网络包含在此路由中使用网关的主机。

  要定义默认路由，请使用预定义的 any-ipv4 或 any-ipv6 网络对象，或创建一个适用于 0.0.0.0/0 (IPv4) 或 ::/0 (IPv6) 网络的对象。

步骤 7 点击**确定 (OK)**。

步骤 8 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

静态路由示例

有关此示例中使用的地址，请参阅静态路由网络图。

目标是创建一个静态路由，它允许将流量返回到目的网络 20.30.1.0/24 中位于 20.30.1.2 的主机。

数据包可以通过任何路径到达目标。当网络接收到接口上的数据包时，它会决定将数据包转发到哪里，以获得到达目标的最佳路由。

Note DMZ 没有静态路由，因为它直接连接到接口。

例如，请考虑以下两个到达目标的路由。

路由 1：

Procedure

步骤 1 数据包返回到外部接口 **209.165.201.0/27**，查找 **20.30.1.2**。

步骤 2 我们将数据包定向到使用**内部**接口到达与目标位于同一网络的网关 192.168.1.2。

步骤 3 然后，通过网络的**网关地址** 20.30.1.1 识别目的网络。

步骤 4 IP 地址 20.30.1.2 与 20.30.1.1 位于同一子网。路由器会将数据包转发到交换机，而交换机会将数据包转发到 20.30.1.2。

Interface:Inside Destination_N/W:20.30.1.0/24 Gateway: 192.168.1.2 Metric: 1

路由 2：

Procedure

步骤 1 数据包返回到外部接口 **209.165.201.0/27**，查找 **20.30.1.2**。

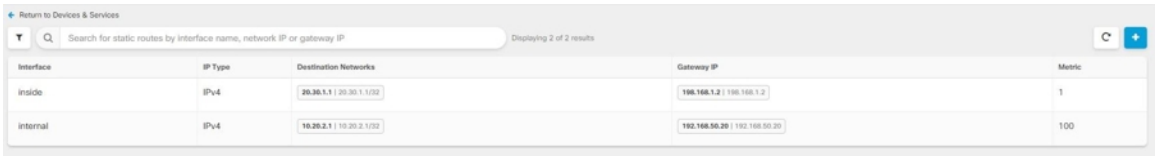
步骤 2 我们将数据包定向为使用**内部**接口到达网关 192.168.50.20，该地址距离目标网络有多跳。

步骤 3 然后，通过网络的**网关地址** 20.30.1.1 识别目的网络。

步骤 4 IP 地址 20.30.1.2 与 20.30.1.0 位于同一子网。路由器会将数据包转发到交换机，而交换机会将数据包转发到 20.30.1.2。

Interface:Inside Destination_N/W:20.30.1.0/24 Gateway: 192.168.50.20 Metric: 100

以下是这些路由的完整添加静态路由表。



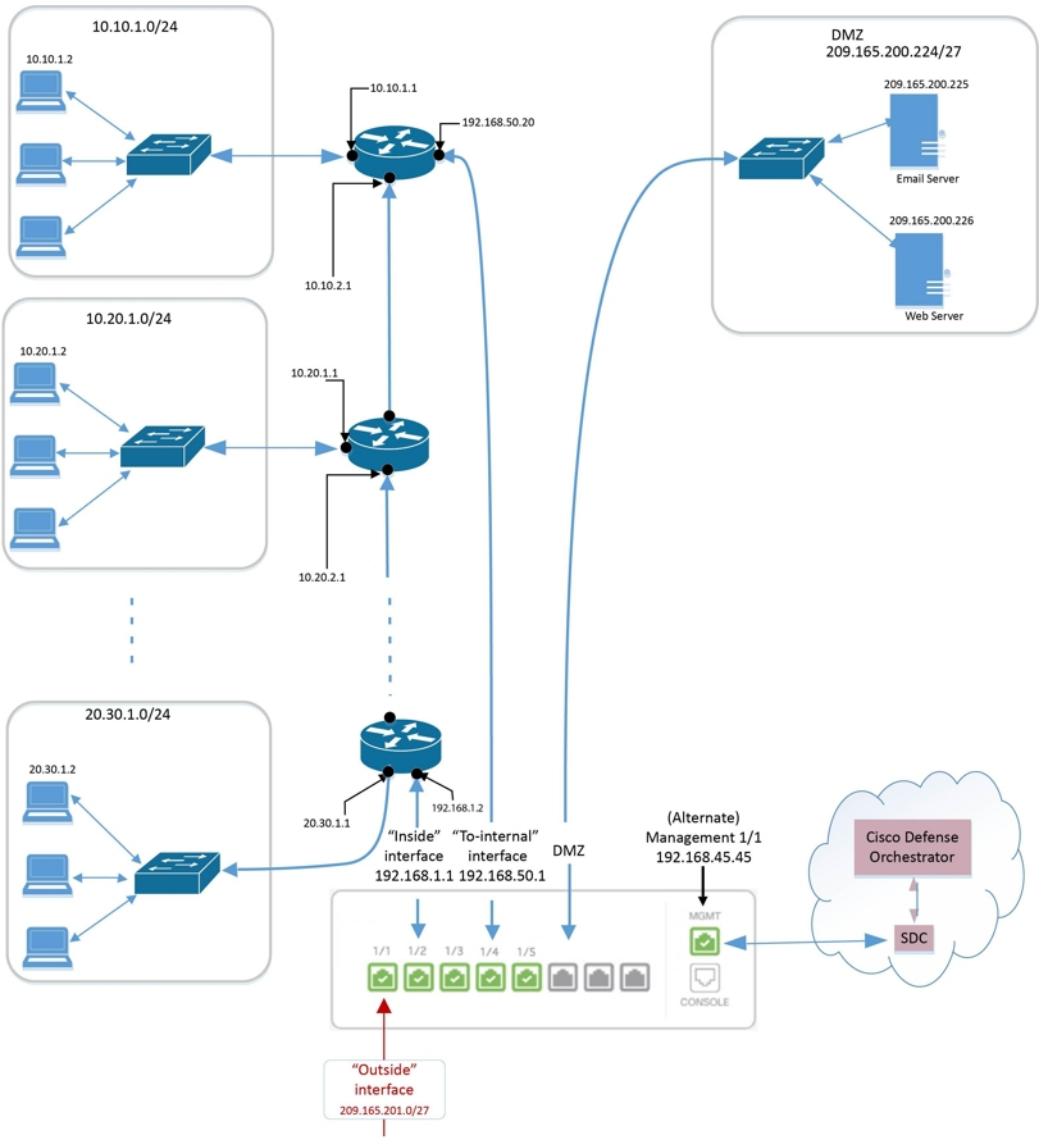
监控路由

要对路由进行监控和故障排除，请打开设备的 防火墙设备管理器 并打开 CLI 控制台，或使用 SSH 登录设备 CLI 并使用以下命令：

- `show route` 显示数据接口的路由表，包括直连网络的路由。
- `show ipv6 route` 显示数据接口的 IPv6 路由表，包括直连网络的路由。
- `show network` 显示虚拟管理接口的配置，包括管理网关。通过虚拟接口路由不由数据接口路由表处理，除非您指定数据接口作为管理网关。
- `show network-static-routes` 显示使用 `configure network static-routes` 命令为虚拟管理接口配置的静态路由。通常不会有任何静态路由，因为在大多数情况下，管理网关足以支持管理路由。这些路由不可用于数据接口上的流量。该命令在 CLI 控制台中不可用。

静态路由网络图

在讨论为 FDM 管理 设备配置静态路由和默认路由时，我们会参考此网络图：



关于虚拟路由和转发

关于 VRF

虚拟路由和转发 (VRF) 允许一个路由器中存在多个路由表实例。Firepower 版本 6.6 引入了具有默认 VRF 表和用户创建的 VRF 表的功能。单个 VRF 表可以处理多种不同的路由协议，例如 EX、OSPF、BGP、IGRP 等。VRF 表中的每个路由协议都作为一个条目列出。除了处理多种类型的常见路由协议之外，您还可以配置路由协议以引用另一个 VRF 的接口。这使得您可以在不使用多个设备的情况下对网络路径进行分段。

有关详细信息，请参阅关于虚拟路由器和虚拟路由与转发 (VRF)。

思科防御协调器 中的 VRF

此功能是 Firepower 版本 6.6 的新增功能。在将 FDM 管理设备载入 CDO 时，FDM 管理设备的路由页面只会读取并支持设备的全局路由器上定义的 VRF。要在 CDO 中查看全局 VRF，请从**清单 (Inventory)** 页面中选择设备，然后从窗口右侧的**管理 (Management)** 窗格中选择**路由 (Routing)**。您可以在此处查看、修改和删除全局 VRF；请注意，在从 FDM 读取配置时，CDO 会保留 VRF 的名称。

CDO防火墙设备管理器 不会读取用户定义的虚拟路由器中配置的 VRF。您必须通过 防火墙设备管理器 来创建和管理 VRF 表。

有关全局和用户定义的路由的信息，请参阅《适用于 Firepower 设备管理器版本 7.0 或更高版本的思科 Firepower 威胁防御配置指南》的“虚拟路由器”一章中的“管理虚拟路由器”部分。

对象

对象是可在一个或多个安全策略中使用的信息容器。使用对象可以轻松维护策略一致性。您可以创建单个对象，使用不同的策略，修改对象，然后将该更改传播到使用该对象的每个策略。如果没有对象，则需要单独修改需要进行相同更改的所有策略。

当您载入设备时， 会识别该设备使用的所有对象，保存它们，并在“对象”(Objects) 页面上列出它们。CDO在“对象”(Objects) 页面中，可以编辑现有对象并创建要在安全策略中使用的新对象。

CDO 将多台设备上使用的对象称为**共享对象**，并在**对象 (Objects)** 页面中使用此标记 进行标识。

有时，共享对象会产生一些“问题”，并且不再在多个策略或设备之间完美共享：

- **重复对象**是指同一设备上具有不同名称但值相同的两个或多个对象。这些对象通常可用于类似的目的，并供不同的策略使用。重复的对象由此问题图标标识：
- **不一致对象**是指两台或多台设备上具有相同名称但值不同的对象。有时，用户会在不同的配置中创建具有相同名称和内容的对象，但随着时间的推移，这些对象的值会出现分歧，从而造成不一致。不一致的对象由此问题图标标识：
- **未使用的对象**是设备配置中存在但未被其他对象、访问列表或NAT规则引用的对象。未使用的对象由此问题图标标识：

您还可以创建在规则或策略中立即使用的对象。您可以创建不与任何规则或策略关联的对象。在规则或策略中使用该未关联的对象时，会创建该对象的副本并使用该副本。CDO

您可以通过导航至对象菜单或在网络策略的详细信息中查看对象来查看对象。CDO

CDO 允许您从一个位置跨受支持的设备管理网络和服务对象。使用 ，您可以通过以下方式管理对象：CDO

- 根据各种条件搜索和过滤所有对象。对象过滤器, on page 115
- 查找设备上的重复、未使用和不一致的对象，并合并、删除或解决这些对象问题。
- 查找未关联的对象，如果未使用，请将其删除。
- 发现跨设备通用的共享对象。

- 在提交更改之前，评估对象更改对一组策略和设备的影响。
- 比较一组对象及其与不同策略和设备的关系。
- 捕获设备在自行激活后使用的对象。CDO

如果您在创建、编辑或读取已载入设备的对象时遇到问题，请参阅以了解详细信息。对思科防御协调器进行故障排除, on page 715

对象

对象是可在一个或多个安全策略中使用的信息容器。使用对象可以轻松维护策略一致性。您可以创建单个对象，使用不同的策略，修改对象，然后将该更改传播到使用该对象的每个策略。如果没有对象，则需要单独修改需要进行相同更改的所有策略。

当您载入设备时， 会识别该设备使用的所有对象，保存它们，并在“对象”(Objects) 页面上列出它们。CDO在“对象”(Objects) 页面中，可以编辑现有对象并创建要在安全策略中使用的新对象。

CDO 将多台设备上使用的对象称为**共享对象**，并在**对象 (Objects)** 页面中使用此标记 进行标识。

有时，共享对象会产生一些“问题”，并且不再在多个策略或设备之间完美共享：

- **重复对象**是指同一设备上具有不同名称但值相同的两个或多个对象。这些对象通常可用于类似的目的，并供不同的策略使用。重复的对象由此问题图标标识：
- **不一致对象**是指两台或多台设备上具有相同名称但值不同的对象。有时，用户会在不同的配置中创建具有相同名称和内容的对象，但随着时间的推移，这些对象的值会出现分歧，从而造成不一致。不一致的对象由此问题图标标识：
- **未使用的对象**是设备配置中存在但未被其他对象、访问列表或NAT 规则引用的对象。未使用的对象由此问题图标标识：

您还可以创建在规则或策略中立即使用的对象。您可以创建不与任何规则或策略关联的对象。在规则或策略中使用该未关联的对象时，会创建该对象的副本并使用该副本。CDO

您可以通过导航至对象菜单或在网络策略的详细信息中查看对象来查看对象。CDO

CDO 允许您从一个位置跨受支持的设备管理网络和服务对象。使用 ，您可以通过以下方式管理对象：CDO

- 根据各种条件搜索和过滤所有对象。对象过滤器, on page 115
- 查找设备上的重复、未使用和不一致的对象，并合并、删除或解决这些对象问题。
- 查找未关联的对象，如果未使用，请将其删除。
- 发现跨设备通用的共享对象。
- 在提交更改之前，评估对象更改对一组策略和设备的影响。
- 比较一组对象及其与不同策略和设备的关系。
- 捕获设备在自行激活后使用的对象。CDO

如果您在创建、编辑或读取已载入设备的对象时遇到问题，请参阅以了解详细信息。对思科防御协调器进行故障排除, on page 715

对象类型

下表介绍您可以为设备创建和使用 CDO 管理的对象。

***Table 12: FDM* 托管设备对象类型**

对象	说明
应用过滤器对象	应用过滤器对象定义IP连接中使用的应用，或按类型、类别、标记、风险或业务相关性定义应用的过滤器。您可以在策略中使用这些对象而不是使用端口规格来控制流量。
上传 RA AnyConnect 客户端配置文件	AnyConnect客户端文件对象是文件对象，表示配置中使用的文件，通常适用于远程接入 VPN 策略。可以包含 AnyConnect 客户端配置文件和 AnyConnect 客户端映像文件。
证书对象	数字证书是一种用于身份验证的数字识别方式。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。
DNS 服务器组对象	需要使用 DNS 服务器将完全限定域名 (FQDN) 解析为 IP 地址，例如 www.example.com。您可以为管理和数据接口配置不同的 DNS 组对象。
创建和编辑 Firepower 地理位置过滤器对象	地理位置对象定义托管设备（流量的源或目的）的国家/地区和大洲。您可以在策略中使用这些对象而不是使用 IP 地址来控制流量。
创建或编辑 IKEv1 策略	当定义 VPN 连接时， IKEv1 策略对象包含定义 VPN 连接时 IKEv1 策略所需的参数。
IKEv2 策略	当定义 VPN 连接时， IKEv2 策略对象包含定义 VPN 连接时 IKEv2 策略所需的参数。
IKEv1 IPSEC 提议	IPsec 提议对象配置 IKE 第 1 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。
IKEv2 IPSEC 提议	IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。

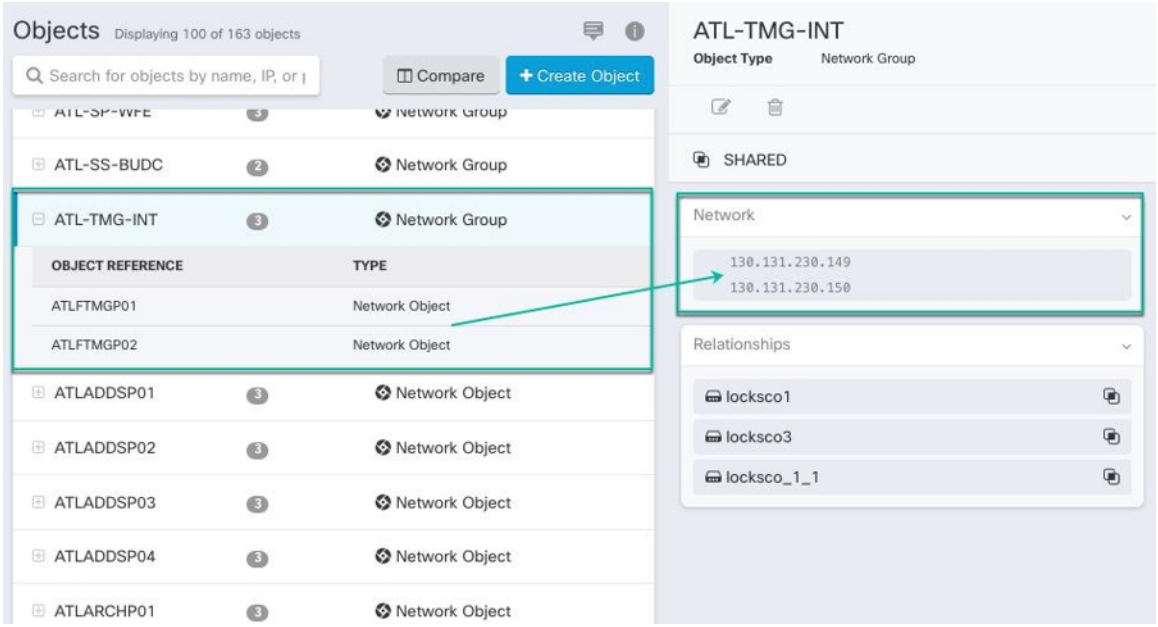
对象	说明
网络对象	网络组和网络对象（统称为“网络对象”）定义主机或网络的地址。
安全区域对象	安全区是一组接口。区域将网络划分成网段，帮助您管理流量以及对流量进行分类。
服务对象	服务对象、服务组和端口组是包含被视为 TCP/IP 协议簇一部分的协议或端口的可重用组件。
创建 SGT 组	SGT 动态对象根据 ISE 分配的 SGT 识别源或目标地址，然后可以与传入流量进行匹配。
系统日志服务器对象	系统日志服务器对象标识可接收面向连接的消息或诊断系统日志（系统日志）消息的服务器。
URL 对象	使用 URL 对象和组（统称为“URL 对象”）可定义 Web 请求的 URL 或 IP 地址。可以使用这些对象在访问控制策略中执行手动 URL 过滤，或在安全情报策略中进行阻止。

共享对象

Cisco Defense Orchestrator (CDO) 会调用多个设备上具有相同名称和相同内容的对象，即**共享对象**。共享对象由此图标标识

在**对象 (Objects)** 页面上。使用共享对象可以轻松维护策略，因为您可以在一个位置修改对象，并且该更改会影响使用该对象的所有其他策略。如果没有共享对象，则需要单独修改需要进行相同更改的所有策略。

查看共享对象时，CDO 会在对象表中显示该对象的内容。共享对象具有完全相同的内容。CDO 在详细信息窗格中显示对象元素的组合视图或“平面化”视图。请注意，在详细信息窗格中，网络元素被展平为一个简单的列表，而不是直接与命名对象关联。

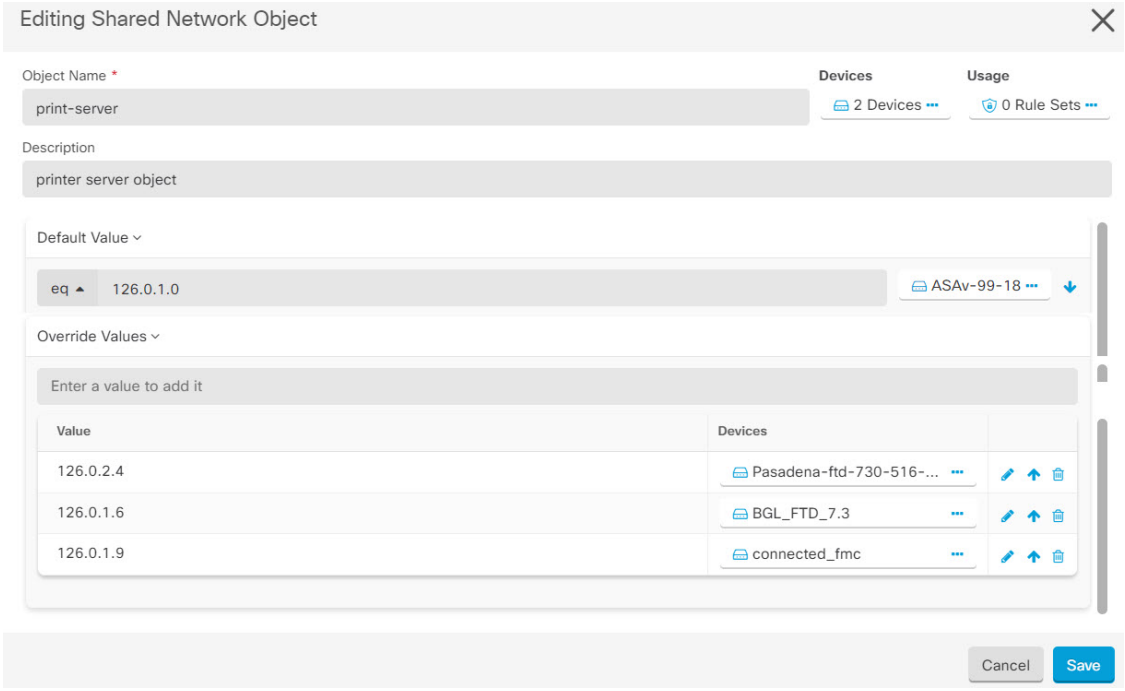


对象覆盖

对象覆盖允许您覆盖特定设备上共享网络对象的值。CDO 会使用您在配置覆盖时指定的设备的相应值。虽然对象位于两个或多个名称相同但值不同的设备上，但 CDO 不会将其识别为**不一致对象**，因为这些值是作为覆盖值添加的。

您可以创建其定义适用于大多数设备的对象，然后使用覆盖为需要不同定义的几个设备指定对象的修改。您还可以创建需要为所有设备覆盖的对象，但其使用使您能够为所有设备创建单个策略。对象覆盖允许您创建较小的一组在设备间使用的共享策略，而不会失去在各个设备需要时修改策略的能力。

例如，假设您的每个办公室都有一台打印机服务器，并且您创建了一个打印机服务器对象 `print-server`。您的 ACL 中有一条规则，用于拒绝打印机服务器访问互联网。打印机服务器对象有一个您想在办公室之间更改的默认值。您可以使用对象覆盖来实现此目的，并在所有位置保持规则和“printer-server”对象的一致性，但它们的值可能不同。



Note CDO 允许您覆盖与规则集中的规则关联的对象。在将新对象添加到规则时，只有在将设备附加到规则集并保存更改后，才能覆盖该对象。有关详细信息，请参阅为设备配置规则集。

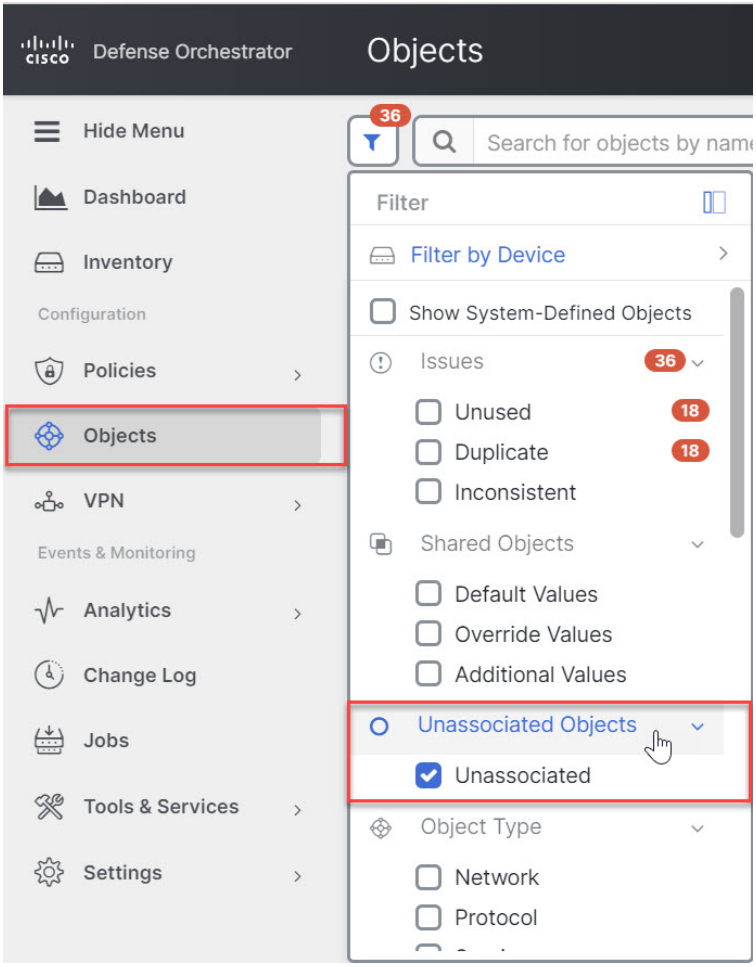
Note 如果存在不一致的对象，您可以将它们合并为一个具有覆盖的共享对象。有关详细信息，请参阅解决不一致的对象问题, on page 721。

未关联的对象

您可以创建对象以立即在规则或策略中使用。您还可以创建不与任何规则或策略关联的对象。当您在规则或策略中使用该未关联的对象时，CDO 会创建该对象的副本并使用该副本。原始未关联对象仍保留在可用对象列表中，直到被夜间维护作业删除或您将其删除。

未关联的对象作为副本保留在 CDO 中，以确保在意外删除与对象关联的规则或策略时不会丢失所有配置。

要查看未关联的对象，请点击对象选项卡的左侧窗格，然后选中未关联的复选框。

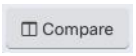


比较对象

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

步骤 2 过滤页面上的对象以查找要比较的对象。

步骤 3 点击**比较**按钮 

。

步骤 4 最多选择三个要比较的对象。

步骤 5 并排查看屏幕底部的对象。

- 点击“对象详细信息”(Object Details) 标题栏中的向上和向下箭头，可查看更多或更少的对象详细信息。
- 展开或折叠详细信息和关系框以查看更多或更少的信息。

步骤 6 （可选）“关系”框显示对象的使用方式。它可能与设备或策略相关联。如果对象与设备关联，您可以点击设备名称，然后点击**查看配置**以查看设备的配置。CDO 显示设备的配置文件，并突出显示该对象的条目。

过滤器

您可以在**清单 (Inventory)** 和**对象 (Objects)** 页面上使用许多不同的过滤器来查找要查找的设备和对象。

要过滤，请点击设备和服务、策略和对象选项卡的左侧窗格中的 ：

清单过滤器允许您按设备类型、硬件和软件版本、Snort版本、配置状态、连接状态、冲突检测以及保护设备连接器和标签进行过滤。您可以应用过滤器在所选设备类型选项卡中查找设备。您可以使用过滤器在所选设备类型选项卡中查找设备。

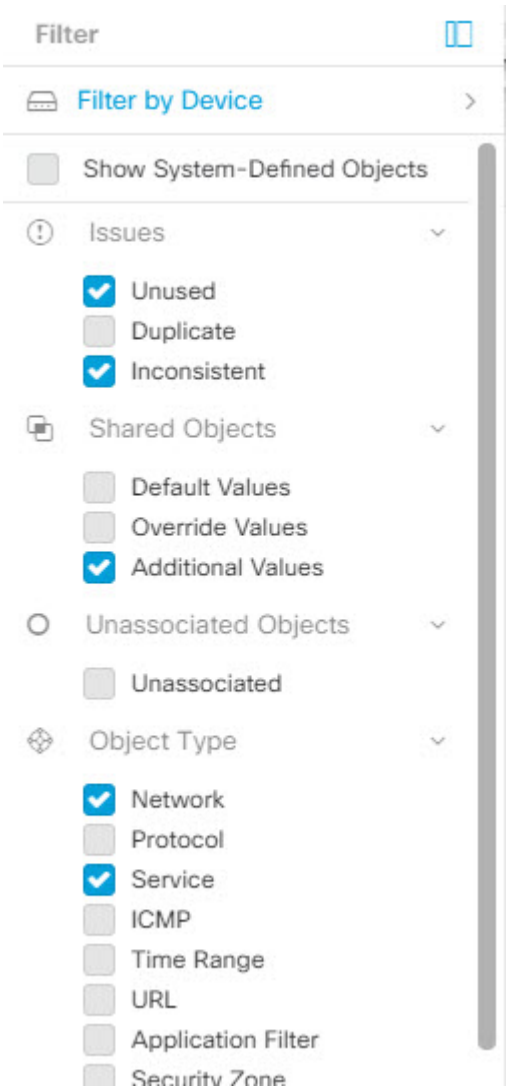
注释 打开 **FTD** 选项卡时，过滤器窗格将提供过滤器，以根据从 CDO 访问设备的管理应用来显示 FDM 管理 设备。

- FDM：使用 FTD API 或 FDM 管理的设备。
- FMC-FTD：通过使用 Firepower 管理中心管理的设备。
- FTD：使用 FTD 管理来管理的设备。

对象过滤器允许您按设备、问题类型、共享对象、未关联的对象和对象类型进行过滤。您可以在结果中包含或不包含系统对象。您还可以使用搜索字段在过滤器结果中搜索包含特定名称、IP 地址或端口号的对象。

过滤设备和对象时，您可以组合搜索词来创建多个潜在的搜索策略来查找相关结果。

在以下示例中，过滤器应用于“问题（已使用或不一致）AND 具有其他值的共享对象 AND 类型为网络 OR 服务的对象”。



对象过滤器

要过滤，请点击“对象”(Objects) 选项卡的左侧窗格的 ：

- **所有对象 (All Objects)** - 此过滤器提供您在 CDO 中注册的所有设备中可用的所有对象。此过滤器可用于浏览所有对象，或作为搜索或进一步应用子过滤器的起点。
- **共享对象 (Shared Objects)** - 此快速过滤器显示 CDO 发现的在多台设备上共享的所有对象。
- **按设备排列的对象 (Objects By Device)** - 允许您选择特定设备，以便可以查看在所选设备上找到的对象。

子过滤器 (Sub filters) - 在每个主过滤器中，您可以应用子过滤器以进一步缩小选择范围。这些子过滤器基于对象类型 - 网络、服务、协议等。

此过滤器栏中的选定过滤器将返回与以下条件匹配的对象：

***** 位于两台设备之一上的对象。（点击**按设备过滤 (Filter by Device)** 以指定设备。）AND 是

*** 不一致** 对象 AND 是

*** 网络 (Network)** 对象 OR **服务 (Service)** 对象 AND

***** 包含**"组"** 在对象命名约定中

由于选中了**显示系统对象 (Show System Objects)**，因此结果将包括系统对象和用户定义的对象。

显示系统对象过滤器

某些设备随附常见服务的预定义对象。这些系统对象很方便，因为它们已经为您创建，您可以在规则和策略中使用它们。对象表中可以有许多系统对象。系统对象无法编辑或删除。

默认情况下，**显示系统对象**处于**关闭**状态。要在对象表中显示系统对象，请选中过滤器栏中的**显示系统对象 (Show System Objects)**。要隐藏对象表中的系统对象，请在过滤器栏中保持未选中状态。

如果隐藏系统对象，它们将不会包含在搜索和过滤结果中。如果显示系统对象，它们将包含在对象搜索和过滤结果中。

配置对象过滤器

您可以根据需要过滤任意数量的条件。过滤所依据的类别越多，预期的结果就越少。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

步骤 2 点击页面顶部的过滤器图标，打开过滤器面板。取消选中任何已选中的过滤器，以确保不会无意中过滤掉任何对象。此外，查看搜索字段并删除可能已在搜索字段中输入的任何文本。

步骤 3 如果要将结果限制为在特定设备上找到的结果，请执行以下操作：

a. 点击**按设备过滤 (Filter By Device)**。

b. 搜索所有设备或点击设备选项卡以仅搜索特定类型的设备。

c. 选中要包含在过滤条件中的设备。

d. 点击**确定 (OK)**。

步骤 4 选中**显示系统对象 (Show System Objects)** 以在搜索结果中包含系统对象。取消选中**显示系统对象 (Show System Objects)** 可从搜索结果中排除系统对象。

步骤 5 选中要作为过滤依据的对象**问题**。如果选中多个问题，则选中的任何类别的对象都将包含在过滤器结果中。

步骤 6 如果要查看存在问题但被管理员忽略的对象，请选中**已忽略 (Ignored)** 的问题。

步骤 7 如果要过滤两台或多台设备之间共享的对象，请在**共享对象 (Shared Objects)** 中选中所需的过滤器。

- **默认值 (Default Values)**：过滤仅具有默认值的对象。
- **覆盖值 (Override Values)**：过滤具有覆盖值的对象。

- **其他值 (Additional Values)**：过滤具有其他值的对象。

步骤 8 如果要过滤不属于任何规则或策略的对象，请选中**未关联 (Unassociated)** 。

步骤 9 选中要作为过滤依据的**对象类型 (Object Types)**。

步骤 10 您还可以将对象名称、IP 地址或端口号添加到对象搜索字段，以在过滤结果中查找符合搜索条件的对象。

何时从过滤条件中排除设备

将设备添加到过滤条件时，结果会显示设备上的对象，但不会显示这些对象与其他设备的关系。例如，假设 ObjectA 在 ASA1 和 ASA2 之间共享。如果要过滤对象以查找 ASA1 上的共享对象，则会找到 ObjectA，但“关系”窗格只会显示该对象位于 ASA1 上。

要查看与对象相关的所有设备，请不要在搜索条件中指定设备。按其他条件过滤并添加搜索条件（如果您愿意）。选择CDO识别的对象，然后在“关系”窗格中进行查看。您将看到与对象相关的所有设备和策略。

忽略对象

解决具有未使用、重复或不一致问题对象的方法之一是忽略它们。您可以决定，尽管对象未使用、重复或不一致，但该状态存在正当理由，并且您选择不解决对象问题。解决未使用的对象问题, on page 720解决重复对象问题, on page 719解决不一致的对象问题, on page 721在未来的某个时候，您可能希望解析这些被忽略的对象。由于CDO在搜索对象问题时不显示已忽略的对象，因此您需要过滤已忽略对象的对象列表，然后对结果执行操作。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

步骤 2 过滤和搜索被忽略的对象。对象过滤器, on page 115

步骤 3 在**对象 (Object)** 表中，选择要取消忽略的对象。一次可以取消忽略一个对象。

步骤 4 点击详细信息窗格中的取消忽略。

步骤 5 确认您的请求。现在，当您按问题过滤对象时，您应该会找到以前忽略的对象。

删除对象

可以删除单个对象或多个对象。

删除单个对象

Caution 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure

步骤 1 在左侧的 CDO 导航栏中，选择**对象 (Objects)**并选择一个选项。

步骤 2 使用对象过滤器和搜索字段找到要删除的对象，然后将其选中。

步骤 3 查看关系窗格。如果在策略或对象组中使用了对象，则在将其从该策略或组中删除之前，无法删除该对象。

步骤 4 点击“操作”(Actions) 窗格中，点击**编辑**图标 。

步骤 5 点击确定，确认要删除对象。

步骤 6 预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

删除一组未使用的对象

当您载入设备并开始解决对象问题时，您会发现许多未使用的对象。一次最多可以删除 50 个未使用的对象。

过程

步骤 1 使用问题过滤器查找未使用的对象。您还可以使用设备过滤器通过选择无设备来查找未与设备关联的对象。过滤对象列表后，系统将显示对象复选框。

步骤 2 选中对象表标题中的全选复选框，以选择过滤器找到的显示在对象表中的所有对象；或者，选中要删除的各个对象的各个复选框。

步骤 3 点击“操作”(Actions) 窗格中，点击**编辑**图标 。

步骤 4 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

网络对象

网络对象 可以包含主机、网络 IP 地址、IP 地址范围、完全限定域名 (FQDN)或用 CIDR 符号表示的子网 。**网络组**是添加到组中的网络对象和其他单个地址或子网络的集合。网络对象和网络组用于访问规则、网络策略和 NAT 规则。您可以使用 CDO 创建、更新和删除网络对象和网络组。

Table 13: 网络对象的允许值

设备类型	IPv4 / IPv6	单个地址	地址范围	域名名称	使用 CIDR 表示法的子网。
FTD	IPv4 和 IPv6	是	是	是	是

Table 14: 网络组允许的内容

设备类型	IP 值	网络对象	网络组
FTD	不支持	是	是

跨产品重用网络对象

如果您的 思科防御协调器 租户具有云交付的防火墙管理中心：

在创建 Secure Firewall Threat Defense、FDM 管理 威胁防御、ASA 或 Meraki 网络对象或组时，对象的副本也会被添加到在配置 云交付的防火墙管理中心 时使用的**对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的对象列表中。

对任一页面上的网络对象或组所做的更改适用于两个页面上的对象或组实例。从一个页面删除对象也会从另一个页面删除该对象的相应副本。

例外情况：

- 如果 云交付的防火墙管理中心 已存在同名的网络对象，则不会在 思科防御协调器 的**对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上复制新的 Secure Firewall Threat Defense、FDM 管理 威胁防御、ASA 或 Meraki 网络对象
- 由本地 Cisco Secure Firewall Management Center 管理的载入 威胁防御 设备中的网络对象和组不会复制到**对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面，因此无法在 云交付的防火墙管理中心 中使用。

  请注意，对于已迁移到 云交付的防火墙管理中心 的本地 Cisco Secure Firewall Management Center 实例，如果在部署到 FTD 设备的策略中使用网络对象和组，它们将被复制到 CDO 对象页面。
- 新租户上会自动启用在 CDO 和 云交付的防火墙管理中心 之间共享网络对象，但现有租户必须另行请求。如果您的网络对象未与 云交付的防火墙管理中心 共享，请CDO 客户如何通过 TAC 提交支持请求 以在您的租户上启用这些功能。

查看网络对象

使用 CDO 创建的网络对象以及已载入的设备配置中的 CDO 识别的网络对象会显示在对象页面上。它们标有对象类型。这使您可以按对象类型进行过滤，以快速找到要查找的对象。

在“对象”(Objects) 页面上选择网络对象时，您可在“详细信息”(Details) 窗格中看到该对象的值。“关系”(Relationships) 窗格显示对象是否用于策略中，以及对象存储在什么设备上。

在点击网络组时，您会看到该组的内容。网络组是网络对象为其提供的所有值的综合体。

相关信息：

- 创建或编辑 Firepower 网络对象或网络组

创建或编辑 Firepower 网络对象或网络组

Firepower 网络对象可以包含以 CIDR 表示法表示的主机名、IP 地址或子网地址。**网络组**是在访问规则、网络策略和NAT规则中使用的网络对象和网络组的集合。您可以使用 思科防御协调器(CDO)来创建、读取、更新和删除网络对象和网络组。

Firepower 网络对象和组可供 ASA、威胁防御、FDM 管理 和 Meraki 设备使用。请参阅跨产品重用网络对象, on page 119。

Note 如果 云交付的防火墙管理中心 被部署在您的租户上：

在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上创建网络对象或组时，对象的副本会自动添加到 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面，反之亦然。

Caution 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Table 15: 可以添加到网络对象的 ***IP*** 地址

设备类型	**IPv4 / IPv6**	单个地址	地址范围	部分限定域名 **(PQDN)**	使用 **CIDR** 表示法的子网。
FirePower	IPv4 / IPv6	是	是	是	是

相关信息：

- 编辑 Firepower 网络对象, on page 121
- 编辑 Firepower 网络对象, on page 123
- 向共享网络组添加其他值, on page 125
- 编辑共享网络组中的其他值, on page 127

编辑 Firepower 网络对象

Note 如果 云交付的防火墙管理中心 被部署在您的租户上：

在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上创建网络对象或组时，对象的副本会自动添加到 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面，反之亦然。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮 以创建新的对象。

步骤 3 点击**FTD** > **网络 (Network)**。

步骤 4 输入 **对象名称**。

步骤 5 选择 **创建网络对象**。

步骤 6 在**值 (Value)** 部分中：

- 选择 **eq** 并输入以 CIDR 表示法表示的单个 IP 地址、子网地址或部分限定域名 (PQDN)。
- 选择**范围**并输入 IP 地址范围。

Note 请勿设置主机位值。如果输入的主机位值不是 0，CDO 会在创建对象时取消设置，因为云交付的防火墙管理中心 仅接受未设置主机位的 IPv6 对象。

步骤 7 点击**添加 (Add)**。

注意：新创建的网络对象不与任何 FDM 管理 设备关联，因为它们不属于任何规则或策略。要查看这些对象，请在对象过滤器中选择**未关联**的对象类别。有关详细信息，请参阅配置对象过滤器。在设备的规则或策略中使用未关联的对象后，此类对象将与该设备关联。

创建 Firepower 网络组

网络组可以包含网络对象和网络组。创建新的网络组时，可以按名称、IP地址、IP地址范围或FQDN搜索现有对象，并将其添加到网络组。如果对象不存在，您可以立即在同一接口中创建该对象并将其添加到网络组。

Note 如果 云交付的防火墙管理中心 被部署在您的租户上：

在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上创建网络对象或组时，对象的副本会自动添加到 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面，反之亦然。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮  以创建新的对象。

步骤 3 点击**FTD > 网络 (Network)**。

步骤 4 输入 **对象名称**。

步骤 5 选择创建网络组。

步骤 6 在**值 (Values)** 字段中输入值或名称。当您开始输入时，CDO 会提供与您的条目匹配的对象名称或值。

步骤 7 您可以选择一个显示的现有对象，也可以根据输入的名称或值创建一个新对象。

步骤 8 如果 CDO 找到了匹配项，要选择现有对象，请点击**添加 (Add)** 将网络对象或网络组添加到新网络组。

步骤 9 如果输入的值或对象不存在，则可以执行以下操作之一：

- 点击**添加为此名称的新对象 (Add as New Object With This Name)**，以创建具有该名称的新对象。输入一个值，然后点击复选标记将其保存。
- 点击**添加为新对象 (Add as New Object)** 以创建一个新对象。对象名称和值相同。输入名称，然后点击复选标记将其保存。

即使该值已存在，也可以创建一个新对象。您可以对这些对象进行更改并将它们保存。

注意：您可以点击编辑图标修改详细信息。点击“删除”按钮不会删除对象本身；相反，它会将其从网络组中删除。

步骤 10 添加所需的对象后，点击保存以创建新的网络组。

步骤 11 预览和部署所有设备的配置更改。

编辑 Firepower 网络对象

Caution 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的对象。

步骤 3 选择网络对象，然后点击**操作 (Actions)** 窗格中的编辑图标 。

步骤 4 以在“创建 Firepower 网络组”(Create a Firepower Network Group) 中创建值的相同方式编辑对话框中的值。

Note 点击旁边的删除图标，从网络组中删除对象。

步骤 5 点击**保存 (Save)**。CDO 会显示将受更改影响的设备。

步骤 6 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

编辑 Firepower 网络组

⚠

Caution 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到您要编辑的网络组。

步骤 3 选择网络组，然后点击**操作 (Actions)** 窗格中的编辑图标 。

步骤 4 如有必要，更改对象名称和说明。

步骤 5 如果要更改已添加到网络组的对象或网络组，请执行以下步骤：

a. 点击对象名称或网络组旁边的编辑图标可对其进行修改。

b. 点击复选标记以保存更改。**注意**：您可以点击删除图标从网络组中删除该值。

步骤 6 如果要向此网络组添加新的网络对象或网络组，必须执行以下步骤：

a. 在值字段中，输入新值或现有网络对象的名称。当您开始输入时，CDO 会提供与您的条目匹配的对象名称或值。您可以选择一个显示的现有对象，也可以根据输入的名称或值创建一个新对象。

b. 如果 CDO 找到了匹配项，要选择现有对象，请点击**添加 (Add)** 将网络对象或网络组添加到新网络组。

c. 如果输入的值或对象不存在，则可以执行以下操作之一：

- 点击**添加为此名称的新对象 (Add as New Object With This Name)**，以创建具有该名称的新对象。输入一个值，然后点击复选标记将其保存。
- 点击**添加为新对象 (Add as New Object)** 以创建一个新对象。对象名称和值相同。输入名称，然后点击复选标记将其保存。

即使该值已存在，也可以创建一个新对象。您可以对这些对象进行更改并将它们保存。

步骤 7 点击**保存 (Save)**。CDO 显示将受更改影响的策略。

步骤 8 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

步骤 9 预览和部署所有设备的配置更改。

添加对象覆盖

注意 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

过程

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到具有要编辑的覆盖的对象。

步骤 3 选择网络对象，然后点击**操作 (Actions)** 窗格中的编辑图标  。

步骤 4 在**覆盖值 (Override Values)** 对话框中输入值，然后点击 **+ 添加值 (+ Add Value)**。

重要事项 要添加的覆盖必须具有与对象所包含的值类型相同。例如，对于网络对象，只能使用网络值而不是主机值来配置覆盖。

步骤 5 看到添加的值后，点击**覆盖值 (Override Values)** 的**设备 (Devices)** 列中的单元格。

步骤 6 点击**添加设备 (Add Devices)**，然后选择要向其添加覆盖的设备。您选择的设备必须包含要向其添加覆盖的对象。

步骤 7 点击**保存 (Save)**。CDO 会显示将受更改影响的设备。

步骤 8 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的覆盖添加。

注释 您可以向一个对象添加多个覆盖。但每次添加覆盖时，都必须选择包含对象的不同设备。

步骤 9 请参阅对象覆盖，第 112 页，了解有关对象覆盖和编辑对象覆盖，第 125 页的详细信息以编辑现有覆盖。

编辑对象覆盖

只要设备上存在对象，您就可以修改现有覆盖的值。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到具有要编辑的覆盖的对象。

步骤 3 选择带有覆盖的对象，然后点击“操作”(Actions) 窗格中的编辑图标  。

步骤 4 修改覆盖值：

- 点击编辑图标以修改值。
- 在**覆盖值 (Override Values)** 中点击**设备 (Devices)** 列，以便分配新设备。您可以选择已分配的设备，然后点击**删除覆盖 (Remove Overrides)** 以删除该设备上的覆盖。
- 点击**覆盖值 (Override Values)** 中的 箭头，将其推送并设置为共享对象的默认值。
- 点击要删除的覆盖旁边的删除图标。

步骤 5 点击**保存 (Save)**。CDO 会显示将受更改影响的设备。

步骤 6 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

步骤 7 预览和部署所有设备的配置更改。

向共享网络组添加其他值

共享网络组中与其关联的所有设备上都存在的值被称为“默认值”。CDO 允许您向共享网络组添加“其他值”，并将这些值分配给与该共享网络组关联的某些设备。当CDO将更改部署到设备时，它会确定内容并将“默认值”推送到与共享网络组关联的所有设备，而“其他值”只会被推送到指定的设备。

例如，假设您的总部有四台 AD 主服务器，那么这些服务器应可从您的所有站点进行访问。因此，您创建了一个名为“Active-Directory”的对象组，以便用于所有站点。现在，您要为其中一个分支机构再添加两台 AD 服务器。为此，您可以通过将其详细信息添加为对象组“Active-Directory”上该分支机构的特定附加值来执行此操作。这两台服务器不参与确定对象“Active-Directory”是一致的还是共享的。因此，您可从所有站点访问四台AD主服务器，但分支机构（具有两台附加服务器）可以访问两台 AD 服务器和四台 AD 主服务器。

Note 如果存在不一致的共享网络组，则您可以将它们合并为具有其他值的单个共享网络组。有关详细信息，请参阅解决不一致的对象问题, on page 721。

Caution 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到您要编辑的共享网络组。

步骤 3 点击**操作 (Actions)** 窗格中的编辑图标 。

- **设备 (Devices)** 字段会显示共享网络组所在的设备。
- **使用情况 (Usage)** 字段会显示与共享网络组关联的规则集。
- **默认值 (Default Values)** 字段将指定默认网络对象及其与创建期间提供的共享网络组关联的值。在此字段旁边，您可以看到包含此默认值的设备数量，您可以点击查看其名称和设备类型。您还可以查看与此值关联的规则集。

步骤 4 在**其他值 (Additional Values)** 字段中输入值或名称。当您开始输入时，CDO 会提供与您的条目匹配的对象名称或值。

步骤 5 您可以选择一个显示的现有对象，也可以根据输入的名称或值创建一个新对象。

步骤 6 如果 CDO 找到了匹配项，要选择现有对象，请点击**添加 (Add)** 将网络对象或网络组添加到新网络组。

步骤 7 如果输入的值或对象不存在，则可以执行以下操作之一：

- 点击**添加为此名称的新对象 (Add as New Object With This Name)**，以创建具有该名称的新对象。输入一个值，然后点击复选标记将其保存。
- 点击**添加为新对象 (Add as New Object)** 以创建一个新对象。对象名称和值相同。输入名称，然后点击复选标记将其保存。

即使该值已存在，也可以创建一个新对象。您可以对这些对象进行更改并将它们保存。

步骤 8 在**设备 (Devices)** 列中，点击与新添加的对象关联的单元格，然后点击**添加设备 (Add Devices)**。

步骤 9 选择所需的设备，然后点击**确定 (OK)**。

步骤 10 点击**保存 (Save)**。CDO 会显示将受更改影响的设备。

步骤 11 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

步骤 12 预览和部署所有设备的配置更改。

编辑共享网络组中的其他值

Caution 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到具有要编辑的覆盖的对象。

步骤 3 点击 **操作** 窗格中的编辑图标 。

步骤 4 修改覆盖值：

- 点击编辑图标以修改值。
- 点击**设备 (Devices)** 列中的单元格以分配新设备。您可以选择已分配的设备，然后点击**删除覆盖 (Remove Overrides)** 以删除该设备上的覆盖。
- 点击**默认值 (Default Values)** 中的 箭头，将其设置为共享网络组的其他值。与共享网络组关联的所有设备都会自动分配到该共享网络组。
- 点击**覆盖值 (Override Values)** 中的 箭头，将其推送并设置为共享网络组的默认对象。
- 点击旁边的删除图标，从网络组中删除对象。

步骤 5 点击**保存 (Save)**。CDO 会显示将受更改影响的设备。

步骤 6 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

步骤 7 预览和部署所有设备的配置更改。

删除网络对象和组

如果 云交付的防火墙管理中心 被部署在您的租户上：

从 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面删除网络对象或组都会从 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面中删除复制的对象或组，反之亦然。

应用过滤器对象

应用过滤器对象由 Firepower 设备使用。应用过滤器对象定义 IP 连接中使用的应用，或按类型、类别、标记、风险或业务相关性定义应用的过滤器。您可以在策略中使用这些对象而不是使用端口规格来控制流量。

虽然您可以指定个别应用，但应用过滤器可简化策略创建和管理。例如，您可以创建一条访问控制规则，用于识别并阻止所有业务相关性较低的高风险应用。如果用户尝试使用这些应用中的任何一个，系统会阻止会话。

您可以直接在策略中选择应用和应用过滤器，而不使用应用过滤器对象。但是，如果要为同一组应用或过滤器创建多个策略，使用对象则非常方便。该系统包括多个预定义的应用过滤器，您不能编辑或删除它们。

Note 思科会通过系统和漏洞数据库 (VDB) 更新频繁更改并添加其他应用检测器。因此，阻止高风险应用的规则可自动应用到新应用中，而无需您手动更新规则。

Note 当 FDM 托管的 FTD 设备被载入 CDO 时，它会将应用过滤器转换为应用过滤器对象，而不会更改访问规则或 SSL 解密中定义的规则。由于配置更改，设备的配置状态更改为“未同步”，需要从 CDO 进行配置部署。通常，在您手动保存过滤器之前，FDM 不会将应用过滤器转换为应用过滤器对象。

相关信息：

- 创建和编辑 Firepower 应用过滤器对象
- 删除对象

创建和编辑 Firepower 应用过滤器对象

应用过滤器对象允许您以精选应用或由过滤器识别的一组应用为目标。此应用过滤器对象可用于策略中。

创建 Firepower 应用过滤器对象

要创建应用过滤器对象，请执行以下程序：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

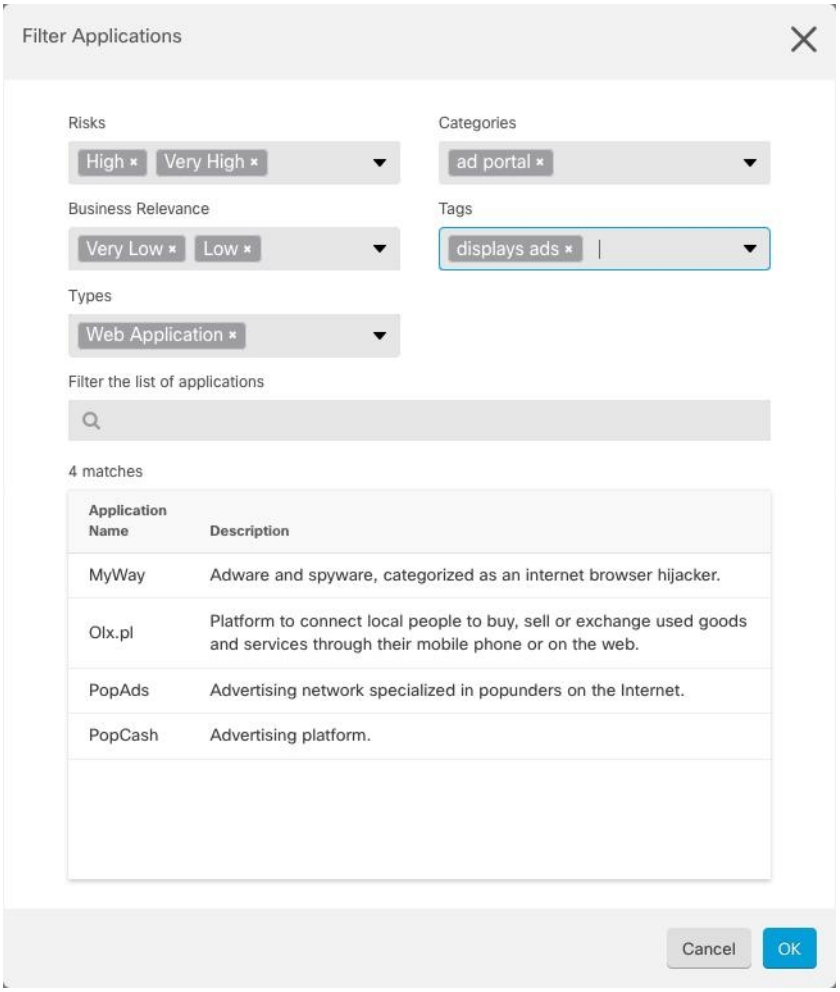
步骤 2 点击创建对象 > FTD > 应用服务。

步骤 3 输入对象的 **对象名称** 和 **说明**（后者为可选项）。

步骤 4 点击**添加过滤器 (Add Filter)**，然后选择要添加到对象的应用程序和过滤器。

初始列表将在连续滚动的列表中显示应用。点击**高级过滤器 (Advanced Filter)** 可查看过滤器选项，可更加方便地查看和选择应用。完成选择后，点击**添加 (Add)**。您可以重复该过程，以添加更多应用或过滤器。

Note 单个过滤器条件中的多个选项具有 OR 关系。例如，风险高 OR 非常高。过滤器之间的关系是 AND，因此是风险高 OR 非常高，AND 业务相关性低 OR 非常低。在选择过滤器时，显示屏中的应用列表更新，只显示符合条件的应用。您可以使用这些过滤器来帮助查找要单独添加的应用，或确认是否要选择所需的过滤器以添加到规则中。



风险 (Risks)：应用所用的用途可能违反组织安全策略的可能性，从非常低到非常高。

业务相关性 (Business Relevance)：在组织的业务运营环境（非娱乐性）下使用应用的可能性，从非常低到非常高。

类型 (Types)：应用类型。

- **应用协议 (Application Protocol)**：应用协议（例如 HTTP 和 SSH），代表主机之间的通信。
- **客户端协议 (Client Protocol)**：客户端（例如 Web 浏览器和邮件客户端），代表主机上运行的软件。

- **Web 应用 (Web Application)**：Web 应用（例如 MPEG 视频和 Facebook），代表 HTTP 流量的内容或请求的 URL。

类别 (Categories)：对应用的一般分类，说明其最基本的功能。

标记 (Tags)：关于应用的其他信息，与类别类似。

对于加密流量，系统可以仅使用标记有 SSL 协议的应用识别和过滤流量。只有在未加密或已解密的流量中才能检测到没有此标记的应用。此外，系统仅将已解密的流量标记分配给可在已解密的流量中检测到的应用，而不会将它们分配给加密或未加密的流量中检测到的应用。

应用列表 (Applications List)（显示底部）：在从列表上方的选项中选择过滤器时，此列表将进行更新，所以您可查看当前符合过滤器的应用。在计划将过滤器条件添加到规则中时，使用此列表可确认您的过滤器是否针对所需的应用。要将特定应用添加到对象，请从过滤列表中选择它们。选择应用后，过滤器将不再适用。如果您希望过滤器本身作为对象，请勿从列表中选择应用。然后，该对象将代表过滤器识别的应用。

步骤 5 点击**确定 (OK)**，保存更改。

编辑 Firepower 应用过滤器对象

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的对象。

步骤 3 选择要编辑的对象。

步骤 4 点击“操作”(Actions) 窗格中的编辑图标  。

步骤 5 以在上述过程中创建值的相同方式编辑对话框中的值。

步骤 6 点击**保存 (Save)**。

步骤 7 CDO 显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

相关信息：

- 对象
- 对象过滤器
- 删除对象

地理位置对象

地理位置对象定义托管设备（流量的源或目的）的国家/地区和大洲。您可以在策略中使用这些对象而不是使用 IP 地址来控制流量。例如，使用地理位置可以很容易地将访问权限限制为特定国家/地区，而无需知道此处使用的所有潜在 IP 地址。

通常，可以直接在策略中选择地理位置，而无需使用地理位置对象。但是，如果要为同一组国家/地区或大洲创建多个策略，使用对象则非常方便。

更新地理定位数据库

为了确保使用最新的地理位置数据来过滤流量，思科强烈建议您定期更新地理位置数据库(GeoDB)。目前，这不是您可以使用 Cisco Defense Orchestrator 执行的任务。请参阅《适用于 Firepower 设备管理器的思科Firepower威胁防御配置指南》的以下部分，了解您的设备正在运行的版本，以了解有关 GeoDB 及其更新方式的详细信息。

- 更新系统数据库和源
- 更新系统数据库

创建和编辑 Firepower 地理位置过滤器对象

您可以在对象页面上或在创建安全策略时单独创建地理位置对象。此程序从对象页面创建地理位置对象。

要创建地理位置对象，请执行以下步骤：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
步骤 2 点击**创建对象 (Create Object) > FTD > 地理位置 (Geolocation)**。
步骤 3 输入对象的 **对象名称** 和 **说明**（后者为可选项）。
步骤 4 在过滤器栏中，开始键入国家/地区或地区的名称，系统会显示可能的匹配项列表。
步骤 5 选中要添加到对象的国家/地区或地区。
步骤 6 点击**添加**。

编辑地理位置对象

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
步骤 2 使用过滤器窗格和搜索字段查找对象。
步骤 3 在“操作”(Actions) 窗格中，点击**编辑 (Edit)**。
步骤 4 您可以更改对象的名称，并向对象添加或删除国家/地区和地区。
步骤 5 点击**保存 (Save)**。
步骤 6 如果有任何设备受到影响，您会收到通知。点击 **Confirm**。
步骤 7 如果设备或策略受到影响，请打开资产页面并预览并将更改部署到设备。

DNS 服务器组对象

域名系统 (DNS) 组定义 DNS 服务器列表和某些相关联的属性。需要使用 DNS 服务器将完全限定域名 (FQDN) 解析为 IP 地址，例如 www.example.com。您可以为管理和数据接口配置不同的 DNS 组对象。

FDM 管理 设备必须先配置 DNS 服务器，然后才能创建新的 DNS 组对象。您可以将 DNS 服务器添加到 思科防御协调器 (CDO) 中的 配置 DNS 服务器，也可以在 防火墙设备管理器 中创建 DNS 服务器，然后将 FDM 管理 配置同步到 CDO。要在 防火墙设备管理器 中创建或修改 DNS 服务器设置，请参阅《思科 Firepower 设备管理器配置指南》，版本 6.4 或更高版本中的**为数据和管理接口配置 DNS**。

创建 DNS 组对象

使用以下程序在 CDO 中创建新的 DNS 组对象：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮  以创建新的对象。

步骤 3 点击 FTD DNS 组。 >

步骤 4 输入 **对象名称 (Object Name)**。

步骤 5 （可选）添加说明。

步骤 6 输入 **DNS 服务器**的 IP 地址。您最多可以添加六个 DNS 服务器；点击添加 DNS 服务器。如果您想要删除服务器地址，请点击删除图标。

Note 列表采用优先顺序：始终使用列表中的第一个服务器，只有当从前面的服务器收不到响应时，才使用后面的服务器。虽然最多可以添加六台服务器，但只有列出的前 3 台服务器将用于管理接口。

步骤 7 输入**域搜索名称 (Domain Search Name)**。此域将被添加到非完全限定的主机名，例如 serverA 而不是 serverA.example.com。

步骤 8 输入重试次数。系统接收不到响应时，重试 DNS 服务器列表的次数，介于 0 和 10 次之间。默认值为 2。此设置仅适用于数据接口上使用的 DNS 组。

步骤 9 输入**超时**值。尝试下一个 DNS 服务器之前要等待的秒数，介于 1 和 30 秒之间。默认值为 2 秒。每次系统重试服务器列表，此超时将加倍。此设置仅适用于数据接口上使用的 DNS 组。

步骤 10 点击**添加**。

编辑 DNS 组对象

您可以编辑在 思科防御协调器 或 防火墙设备管理器 中创建的 DNS 组对象。使用以下程序编辑现有的 DNS 组对象：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
步骤 2 使用对象过滤器和搜索字段找到要编辑的 **DNS 组对象**。
步骤 3 选择对象，然后点击**操作 (Actions)** 窗格中的编辑图标 。
步骤 4 编辑以下任何条目：

- 对象名称。
- 说明。
- DNS 服务器。您可以在此列表中编辑、添加或删除 DNS 服务器。
- 域搜索名称。
- 重试。
- 超时。

步骤 5 点击**保存 (Save)**。
步骤 6 预览和部署所有设备的配置更改。

删除 DNS 组对象

使用以下程序从 CDO 中删除 DNS 组对象：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
步骤 2 使用对象过滤器和搜索字段找到要编辑的 **DNS 组对象**。
步骤 3 选择对象，然后点击删除图标。
步骤 4 确认要删除 DNS 组对象，然后点击确定。
步骤 5 预览和部署所有设备的配置更改。

将 DNS 组对象添加为 DNS 服务器FDM 管理

您可以将 DNS 组对象添加为数据接口或管理接口的首选 DNS 组。有关详细信息，请参阅 FDM 托管设备设置。FDM 管理 设备设置, on page 521

证书对象

数字证书是一种用于身份验证的数字识别方式。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。

请参阅适用于您的设备的版本的《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》中可恢复对象一章的**关于证书**和**配置证书**部分。

关于证书

数字证书是一种用于身份验证的数字识别方式。数字证书包括用于识别设备或用户的信息，例如名称、序列号、公司、部门或 IP 地址。数字证书还包括用户或设备的公钥副本。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。

您可以创建以下类型的证书：

- **内部证书 (Internal certificates)** - 内部身份证书是用于特定系统或主机的证书。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名证书。

  系统提供以下预定义内部证书（您可以按原样使用或替换它们）：**DefaultInternalCertificate** 和 **DefaultWebServerCertificate**

- **内部证书颁发机构 (CA)** 证书 - 内部 CA 证书是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名的内部 CA 证书。如果配置自签名的内部 CA 证书，该 CA 将在设备自身上运行。

  系统提供以下预定义内部CA证书（您可以按原样使用或替换它们）：**NGFW-Default-InternalCA**

- **可信证书颁发机构 (CA)** 证书 - 可信的 CA 证书可用于签署其他证书。它是自签名证书，也称为根证书。由另一个 CA 证书颁发的证书称为从属证书。

  证书颁发机构 (CA) 是指“签署”证书以确认其真实性，从而确保设备或用户的身份的可信颁发机构。CA 在 PKI（使用公钥或私钥加密以确保安全性）的情景下颁发数字证书。CA 可以是可信的第三方（例如 VeriSign），也可以是组织内建立的私有（内部）CA。CA 负责管理证书请求和颁发数字证书。

  系统包括许多从第三方证书颁发机构获取的受信任的 CA 证书。SSL 解密策略可使用这些证书执行解密重新签署操作。

有关详细信息，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》中“可重用对象”一章的**功能使用的证书类型**部分。

功能使用的证书类型

您需要为每个功能创建正确类型的证书。以下功能需要证书。

身份策略（强制网络门户）- 内部证书

（可选。）强制网络门户用于身份策略中。在向设备进行身份验证时，为了标识自己的身份并接收与其用户名关联的 IP 地址，用户必须接受此证书。如果不提供证书，设备将使用自动生成的证书。

SSL 解密策略 - 内部、内部 CA 和受信任 CA 证书。

（必需。）SSL 解密策略将证书用于以下目的：

- 内部证书用于已知的密钥解密规则。
- 在客户端和 FTD 设备之间创建会话时，内部 CA 证书用于解密重签名规则。
- 受信任 CA 证书
  - 在 FTD 设备和服务器之间创建会话时，它们可直接用于解密重签名规则。与其他证书不同，这些证书不能直接在 SSL 解密策略中配置，而是需要上传到系统。系统包括大量受信任 CA 证书，因此，您无需上传任何其他证书。
  - 创建 Active Directory 领域对象并将目录服务器配置为使用加密时。

配置证书

身份策略或 SSL 解密策略中使用的证书必须是 PEM 或 DER 格式的 X509 证书。如果需要，您可以使用 OpenSSL 生成证书、从受信任的证书颁发机构获取证书或创建自签名证书。

使用以下程序配置证书对象：

- 上传内部证书和内部 CA 证书
- 上传受信任的 CA 证书
- 生成自签名的内部证书和内部 CA 证书
- 要查看或编辑证书，请点击证书的编辑图标或视图图标。
- 要删除未引用的证书，请点击证书的垃圾桶图标（删除图标）。请参阅删除对象。

上传内部证书和内部 CA 证书

内部身份证书是特定系统或主机的证书。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名证书。

内部证书颁发机构 (CA) 证书（内部 CA 证书）是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名的内部 CA 证书。如果配置自签名的内部 CA 证书，该 CA 将在设备自身上运行。

有关使用这些证书的功能的信息，请参阅功能使用的证书类型。

操作步骤

此程序通过上传证书文件或将现有证书文本粘贴到文本框中来创建内部证书身份或内部 CA 证书。如果要生成自签名证书，请参阅生成自签名内部证书和内部 CA 证书。生成自签名的内部证书和内部 CA 证书, on page 139

要创建内部或内部 CA 证书对象，或者在向策略添加新证书对象时，请执行以下程序：

Procedure

步骤 1 执行以下操作之一：

- 在对象页面中创建证书对象：
  a. 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
  b. 点击加号按钮，然后选择 FTD 证书 >
- 将新证书对象添加到策略时，点击创建新对象。

步骤 2 键入证书的**名称**。该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 3 在步骤 1 中，选择内部证书或内部 CA。

步骤 4 在步骤 2 中，选择**上传 (Upload)** 以上传证书文件。

步骤 5 在步骤 3 的**服务器证书 (Server Certificate)** 区域中，将证书内容粘贴到文本框中，或按照向导中的说明上传证书文件。如果将证书粘贴到文本框中，则证书必须包括 BEGIN CERTIFICATE 和 END CERTIFICATE 两行。例如：

```
-----BEGIN CERTIFICATE-----
 MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0
(...5 lines removed...)
shGJDReRYJQqilhHZrYTWZAYTrD7NQPHutK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZlzJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfxwCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjqy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
vlk3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

步骤 6 在步骤 3 的**证书密钥 (Certificate Key)** 区域中，将密钥内容粘贴到证书密钥文本框中，或者按照向导中的说明上传密钥文件。如果将密钥粘贴到文本框中，则密钥必须包含 BEGIN PRIVATE KEY 或 BEGIN RSA PRIVATE KEY 和 END PRIVATE KEY 或 END PRIVATE KEY 行。

Note 密钥不能加密。

步骤 7 点击**添加**。

上传受信任的 CA 证书

受信任证书颁发机构 (CA) 证书用于签署其他证书。它是自签名证书，也称为根证书。由另一个 CA 证书颁发的证书称为从属证书。

有关使用这些证书的功能的信息，请参阅功能使用的证书类型。

受信任 CA 证书可从外部证书颁发机构获取，也可以使用自己的内部 CA 创建（例如通过 OpenSSL 工具生成证书）。然后，使用以下步骤程序上传证书。

操作步骤

Procedure

步骤 1 执行以下操作之一：

- 在对象页面中创建证书对象：
  a. 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
  b. 点击加号按钮，然后选择 FTD 证书。 >
- 将新证书对象添加到策略时，点击创建新对象。

步骤 2 键入证书的**名称**。该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 3 在步骤 1 中，选择外部 CA 证书，然后点击继续。向导前进到步骤 3。

步骤 4 在步骤 3 的**证书内容 (Certificate Contents)** 区域中，将证书内容粘贴到文本框中，或按照向导中的说明上传证书文件。

证书必须遵循以下准则：

- 证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 10.10.10.250 作为 IP 地址，但证书中的地址为 ad.example.com，则连接失败。
- 该证书必须为 PEM 或 DER 格式的 X509 证书。
- 您粘贴的证书必须包括 BEGIN CERTIFICATE 和 END CERTIFICATE 行。例如：

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

步骤 5 点击**添加**。

生成自签名的内部证书和内部 CA 证书

内部身份证书是特定系统或主机的证书。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名证书。

内部证书颁发机构 (CA) 证书（内部 CA 证书）是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名的内部 CA 证书。如果配置自签名的内部 CA 证书，该 CA 将在设备自身上运行。

此外，还可以使用 OpenSSL 创建证书或从受信任的 CA 获取证书，再上传它们。有关详细信息，请参阅上传内部证书和内部 CA 证书。

有关使用这些证书的功能的信息，请参阅功能使用的证书类型。

Note 新的自签名证书生成的有效期为 5 年。请务必在证书过期前进行更换。

Warning 升级具有自签名证书的设备可能会遇到问题；有关详细信息，请参阅检测到新证书。

操作步骤

此程序可通过在向导中输入相应的证书字段值来生成自签名证书。如果要通过上传证书文件来创建内部或内部 CA 证书，请参阅上传内部和内部 CA 证书。上传内部证书和内部 CA 证书, on page 136

要生成自签名证书，请执行以下程序：

Procedure

步骤 1 执行以下操作之一：

- 在对象页面中创建证书对象：
  a. 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
  b. 点击加号按钮，然后选择 FTD 证书。 >
- 将新证书对象添加到策略时，点击创建新对象。

步骤 2 键入证书的**名称**。该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 3 在步骤 1 中，选择内部证书或内部 CA。

步骤 4 在步骤 2 中，选择自签名以在此步骤中创建自签名证书。

步骤 5 为证书主题和颁发者信息至少配置以下一项。

- 国家/地区 (Country [C]) - 从下拉列表中选择国家/地区代码。
- 州或省 (ST) (State or Province [ST]) - 证书中包括的州或省。
- 地区或城市 (Locality or City) (L) - 证书中包括的地区，例如城市名称。
- 组织 (O) (Organization [O]) - 要包含在证书中的组织或公司名称。
- 组织单位（部门）(Organizational Unit [Department]) (OU) - 证书中包含的组织单位名称（例如部门名称）。
- 公用名 (CN)(Common Name [CN]) - 要包含在证书中的 X.500 公用名。它们可能是设备、网站或其他文本字符串的名称。通常需要有此元素，才能成功进行连接。例如，用于远程访问 VPN 的内部证书中必须包括 CN。

步骤 6 点击**添加**。

配置 IPsec 提议

IPsec 是设置 VPN 的最安全方法之一。IPsec 在 IP 数据包级别提供数据加密，提供一种基于标准的强大的安全解决方案。使用 IPsec，数据通过隧道在公共网络上传输。隧道是两个对等体之间安全的逻辑通信路径。进入 IPsec 隧道的流量由称为转换集的安全协议和算法组合保护。在 IPsec 安全关联 (SA) 协商期间，对等体搜索在两个对等体处相同的转换集。

根据 IKE 版本（IKEv1 或 IKEv2），存在不同的 IPsec 提议对象：

- 当创建 IKEv1 IPsec 提议时，可以选择 IPsec 运行的模式，并定义所需的加密和身份验证类型。您可以为算法选择单一选项。如果要在 VPN 中支持多个组合，请创建和选择多个 IKEv1 IPsec 提议对象。
- 当创建 IKEv2 IPsec 提议时，可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序，并与对等体进行协商，直到找到匹配。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

Note 我们建议对 IPsec 隧道使用加密和身份验证。

以下主题介绍如何为每个 IKE 版本配置 IPsec 提议：

- 管理 IKEv1 IPsec 提议对象
- 管理 IKEv2 IPsec 提议对象

管理 IKEv1 IPsec 提议对象

IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。IKEv1 和 IKEv2 有单独的对象。目前， Cisco Defense Orchestrator (CDO) 支持 IKEv1 IPsec 提议对象。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

Note 我们建议对 IPsec 隧道使用加密和身份验证。

Related Topics

创建或编辑 IKEv1 IPsec 提议对象 ， 第 433 页

创建或编辑 IKEv1 IPsec 提议对象

有几个预定义的IKEv1 IPsec提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑站点间 VPN 连接中的 IKEv1 IPsec 设置时，点击对象列表中所示的**创建新 IKEv1 提议 (Create New IKEv1 Proposal)** 链接来创建 IKEv1 IPsec 提议对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FTD > IKEv1 IPsec 提议 (IKEv1 IPsec Proposal)** 以创建新对象。
- 在对象页面中，选择要编辑的IPsec方案，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

步骤 3 为新对象输入**对象名称**。

步骤 4 选择 IKEv1 IPsec 提议对象的运行模式。

- **隧道**模式会封装整个 IP 数据包。IPSec 报头被添加到原始 IP 报头和新的 IP 报头之间。这是默认值。当防火墙对出入位于防火墙后的主机的流量进行保护时，请使用隧道模式。在通过不可信网络（例如互联网）连接的两个防火墙（或其他安全网关）之间，通常采用隧道模式实施常规 IPSec。
- **传输**模式只封装IP数据包的上层协议。IPSec报头被插入到IP报头和上层协议报头（例如TCP）之间。传输模式要求源和目的主机都支持 IPSec，并且只有在隧道的目的对等体是 IP 数据包的最终目的时才可使用。通常只有在保护第2层或第3层隧道协议（例如GRE、L2TP和DLSW）时，才会使用传输模式。

步骤 5 选择**加密 (Encryption)**提议的（封装安全协议加密）算法。有关选项的说明，请参阅决定使用哪个加密算法, on page 421。

步骤 6 选择要用于身份验证的 **ESP 散列 (ESP Hash)** 或完整性算法。有关选项的说明，请参阅决定使用哪些散列算法, on page 421。

步骤 7 点击**添加**。

管理 IKEv2 IPsec 提议对象

IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。

当创建 IKEv2 IPsec 提议时，可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序，并与对等体进行协商，直到找到匹配。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

Related Topics

创建或编辑 IKEv2 IPsec 提议对象 ， 第 434 页

创建或编辑 IKEv2 IPsec 提议对象

有几个预定义的IKEv2 IPsec提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑 VPN 连接中的 IKEv2 IPsec 设置时，点击对象列表中所示的创建新 IPsec 提议链接来创建 IKEv2 IPsec 提议对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FTD > IKEv2 IPsec 提议 (IKEv2 IPsec Proposal)** 以创建新对象。
- 在对象页面中，选择要编辑的IPsec方案，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

步骤 3 为新对象输入**对象名称**。

步骤 4 配置 IKEv2 IPsec 方案对象：

- **加密** - 此提议的封装安全协议 (ESP) 加密算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪个加密算法, on page 421。

- **完整性散列** - 要用于身份验证的散列或完整性算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪些散列算法, on page 421。

步骤 5 点击**添加**。

配置全局 IKE 策略

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。

IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用提议。IKE 提议是一组两个对等体用于保护其之间的协商的算法。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数用于保护后续 IKE 协商。

IKE 策略对象为这些协商定义 IKE 提议。您启用的对象是对等体协商 VPN 连接时使用的对象：不能为每个连接指定不同的 IKE 策略。每个对象的相对优先级确定首先尝试这些策略中的哪一个，数字越小优先级越高。如果协商无法找到两个对等体全都支持的策略，则不建立连接。

要定义全局 IKE 策略，需要为每个 IKE 版本选择启用哪些对象。如果预定义的对象不能满足您的要求，请创建新的策略来执行您的安全策略。

以下步骤说明如何通过“对象”(Objects) 页面配置全局策略。在编辑 VPN 连接时，您还可以点击 IKE 策略设置的编辑，来启用、禁用和创建策略。

以下主题介绍如何为每个 IKE 策略版本配置 IPsec 提议：

- 管理 IKEv1 策略
- 管理 IKEv2 策略

管理 IKEv1 策略

介绍如何创建和编辑 IKEv1 策略。

关于 IKEv1 策略

互联网密钥交换 (IKE) 版本 1 策略对象包含定义 VPN 连接时 IKEv1 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义 IKEv1 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

Related Topics

创建或编辑 IKEv1 策略 ，第 429 页

创建或编辑 IKEv1 策略

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。您还可以点击对象列表中所示的**创建新 IKE 策略 (Create New IKEv1 Policy)** 链接，以便在站点间 VPN 连接中编辑 IKEv1 设置时创建 IKEv1 策略对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FTD > IKEv1 Policy** 策略以创建新的 IKEv1 策略。
- 在对象页面中，选择要编辑的IKEv1策略，然后点击右侧“操作”(Actions)窗格中的**编辑 (Edit)**。

步骤 3 输入**对象名称**，最多 128 个字符。

步骤 4 配置 IKEv1 属性。

- **优先级 (Priority)** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **加密** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。有关选项的说明，请参阅“决定使用哪种加密算法”。
- **Diffie-Hellman 组** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。有关选项的解释，请看“决定要使用的 Diffie-Hellman 模数组”。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。
- **身份验证** - 在两个对等体之间使用的身份验证方法。有关详细信息，请参阅确定使用哪种身份验证方法, on page 423。
  - **预共享密钥** - 使用在每个设备上定义的预共享密钥。在身份验证阶段，此类密钥允许密钥在两个对等体之间共享并由 IKE 使用。如果未使用同一预共享密钥配置对等体，则无法建立 IKE SA。
  - **证书** - 使用对等体的设备身份证书来识别彼此。必须通过在证书颁发机构中注册每个对等体来获取这些证书。还须上传用于签署每个对等体的身份证书的受信任 CA 根证书和中间 CA 证书。对等体可以注册到相同或不同的 CA 中。对于任一对等体，都不能使用自签证书。

- **散列** - 用于创建消息摘要的散列算法，以确保消息的完整性。有关选项的说明，请参阅VPN 中使用的加密和散列算法, on page 420。

步骤 5 点击**添加**。

管理 IKEv2 策略

介绍如何创建和编辑 IKEv2 策略。

关于 IKEv2 策略

互联网密钥交换 (IKE) 版本 2 策略对象包含定义 VPN 连接时 IKEv2 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv2 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

Related Topics

创建或编辑 IKEv2 策略 ， 第 430 页

创建或编辑 IKEv2 策略

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。您还可以点击对象列表中所示的 **创建新的 IKE 策略** 链接，以便在站点间 VPN 连接中编辑 IKEv1 设置时创建 IKEv1 策略对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FTD > IKEv2 策略 (IKEv2 Policy)** 以创建新的 IKEv2 策略。
- 在对象页面中，选择要编辑的 IKEv2 策略，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

步骤 3 输入**对象名称 (object name)**，最多 128 个字符。

步骤 4 配置 IKEv2 属性。

- **优先级 (Priority)** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **状态 (State)** - IKE 策略是启用还是禁用状态。点击开关以更改状态。在 IKE 协商期间仅使用启用的策略。
- **加密** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。选择要允许的所有算法，但不能在同一策略中同时包括混合模式 (AES-GCM) 和正常模式选项。（正常模式要

求选择完整性散列，而混合模式禁止选择单独的完整性散列。)系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪个加密算法, on page 421。

- **Diffie-Hellman 组** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。选择要允许的所有算法。系统与对等体协商，从最强到最弱组，直到达成匹配。有关选项的说明，请参阅决定要使用的 Diffie-Hellman 模数组, on page 422。
- **完整性散列** - 用于创建消息摘要的散列算法的完整性部分，用于确保消息完整性。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。完整性散列不与 AES-GCM 加密选项一起使用。有关选项的说明，请参阅VPN 中使用的加密和散列算法, on page 420。
- **伪随机函数 (PRF) 散列 (Pseudo-Random Function [PRF] Hash)** - 散列算法中用作派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法的伪随机函数 (PRF) 部分。在 IKEv1 中，完整性和 PRF 算法不分开，但在 IKEv2 中，可以为这些元素指定不同的算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅VPN 中使用的加密和散列算法, on page 420。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。

步骤 5 点击**添加**。

RA VPN 对象

安全区域对象

安全区是一组接口。区域将网络划分成网段，帮助您管理流量以及对流量进行分类。您可以定义多个区域，但一个给定接口只能位于一个区域中。

Firepower 系统会在初始配置期间创建以下区域，这些区域显示在 Defense Orchestrator 的对象页面中。您可以编辑区域以添加或移除接口；如果不再使用这些区域，也可以删除它们。

- **inside_zone** - 包括内部接口。此区域用于表示内部网络。
- **outside_zone** - 包括外部接口。此区域用于表示在您控制之外的网络，例如互联网。

通常，按接口在网络中扮演的角色对它们分组。例如，可将连接至互联网的接口放在 **outside_zone** 安全区，并将内部网络的所有接口放在 **inside_zone** 安全区。然后，可以对来自外部区域和传至内部区域的流量应用访问控制规则。

在创建区域之前，请考虑要应用至网络的访问规则和其他策略。例如，无需将所有内部接口都放到同一个区域。如果您有 4 个内部网络，并希望将其中一个与另外三个区别对待，则可以创建两个区域（而不是一个区域）。如果有一个接口需允许外部访问公共 Web 服务器，您可能希望对该接口使用单独的区域。

相关信息：

- 创建或编辑 Firepower 安全区域对象
- 将 Firepower 接口分配给安全区域
- 删除对象

创建或编辑 Firepower 安全区域对象

安全区是一组接口。区域将网络划分成网段，帮助您管理流量以及对流量进行分类。您可以定义多个区域，但一个给定接口只能位于一个区域中。有关详细信息，请参阅安全区域对象。

安全区域对象不与设备关联，除非在该设备的规则中使用该对象。

创建安全区域对象

要创建安全区域对象，请按照以下说明操作：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮  ，然后选择 **FTD > 安全区域 (Security Zone)** 以创建对象。

步骤 3 为对象命名，也可输入说明（可选）。

步骤 4 选择要加入安全区域的的接口。

步骤 5 点击**添加**。

编辑安全区域对象

自行激活设备后，您会发现至少有两个安全区域，一个是 inside_zone，另一个是 outside_zone。FDM 管理可以编辑或删除这些区域。要编辑任何安全区域对象，请按照以下说明操作：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 查找要编辑的对象：

- 如果您知道对象的名称，则可以在“对象”页面中进行搜索：
  - 按安全区域过滤列表。

- 在搜索字段中输入对象名称。
- 选择对象。

- 如果您知道对象与设备关联，则可以从“资产”页面开始搜索。
  - 在导航窗格中，点击**清单 (Inventory)**。
  - 点击**设备**选项卡。
  - 点击相应的选项卡。
  - 使用设备过滤器和搜索栏查找您的设备。过滤器, on page 90搜索, on page 93
  - 选择设备。
  - 在右侧的“管理”(Management) 窗格中，点击  **对象 (Objects)**。
  - 使用对象过滤器和搜索栏查找要查找的对象。

Note 如果您创建的安全区域对象未与设备策略中的规则关联，则该对象将被视为“未关联”，您将不会在设备的搜索结果中看到该对象。

步骤 3 选择对象。

步骤 4 点击右侧“操作”(Actions) 窗格中的**编辑**图标 。

步骤 5 编辑对象的任何属性后。点击**保存 (Save)**。

步骤 6 点击保存后，您会收到一条消息，说明这些更改将如何影响其他设备。点击**确认 (Confirm)** 以保存更改或点击取消。

服务对象

FirePOWER 服务对象

FTD 服务对象、服务组和端口组是包含被视为 IP 协议簇一部分的协议或端口的可重用组件。

FTD 服务组是服务对象的集合。服务组可能包含一个或多个协议的对象。您可以在安全策略中使用这些对象和组来定义网络流量匹配条件，例如使用访问规则来允许流量传送至特定 TCP 端口。该系统中包括多个针对通用服务的预定义对象。您可以使用策略中的这些对象；但无法编辑或删除系统定义的对象。

Firepower 设备管理器和 Firepower 管理中心将服务对象称为端口对象以及服务组和端口组。

有关详细信息，请参阅创建和编辑 Firepower 服务对象。

协议对象

协议对象是一种包含不太常用或传统协议的服务对象。协议对象由名称和协议编号来标识。CDO 可识别 ASA 和 Firepower（FDM 管理 设备）配置中的这些对象，并为其提供自己的“协议”过滤器，以便您可以轻松找到它们。

有关详细信息，请参阅创建和编辑 Firepower 服务对象。

ICMP 对象

互联网控制消息协议 (ICMP) 对象是专门用于 ICMP 和 IPv6-ICMP 消息的服务对象。当 ASA 和 Firepower配置中的这些设备已载入时，CDO 会识别这些对象，并且CDO 会为其提供自己的“ICMP”过滤器，以便您轻松找到这些对象。

使用 CDO，您可以从 ASA 配置中重命名或删除 ICMP 对象。您可以使用 CDO 在 Firepower 配置中创建、更新和删除 ICMP 和 ICMPv6 对象。

Note 对于 ICMPv6 协议，AWS 不支持选择特定参数。仅支持允许所有 ICMPv6 消息的规则。

有关详细信息，请参阅创建和编辑 Firepower 服务对象。

相关信息：

- 删除对象, on page 117

创建和编辑 Firepower 服务对象

要创建 Firepower 服务对象，请执行以下步骤：

防火墙设备管理器 (FDM 管理) 服务对象是可重用组件，可指定 TCP/IP 协议和端口。防火墙设备管理器、本地防火墙管理中心 和 云交付的防火墙管理中心 将这些对象称为“端口对象”。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击右侧的蓝色按钮  以创建对象，然后选择 **FTD** > **服务 (Service)**。

步骤 3 输入对象名称和说明。

步骤 4 选择**创建服务对象 (Create a service object)**。

步骤 5 点击**服务类型 (Service Type)** 按钮，然后选择要为其创建对象的协议。

步骤 6 按如下方式配置协议：

- **TCP**、 **UDP**
  - 选择 **eq**，然后输入端口号或协议名称。例如，您可以输入 80 作为端口号或 HTTP 作为协议名称。

- 您还可以选择**范围**，然后输入端口号范围，例如 **1 65535**（以涵盖所有端口）。

- **ICMP**、 **IPv6-ICMP**-选择 ICMP **类型**。选择 **Any** 类型可应用于所有 ICMP 消息。有关类型和代码的信息，请参阅以下页面：
  - ICMP-http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - ICMPv6-http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml

- **其他 (Other)** - 选择所需协议。

步骤 7 点击**添加 (Add)**。

步骤 8 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

创建 Firepower 服务组

服务组可以由代表一个或多个协议的一个或多个服务对象组成。需要先创建服务对象，然后才能将其添加到组。Firepower 设备管理器和 Firepower 管理中心将这些对象称为“端口对象”。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击右侧的蓝色按钮  以创建对象，然后选择 **FTD > 服务 (Service)**。

步骤 3 输入对象名称和说明。

步骤 4 选择**创建服务组 (Create a service group)**。

步骤 5 通过点击添加对象 (Add Object) 将对象添加到组。

- 点击创建以创建新对象，就像上面创建 Firepower 服务对象中的操作一样。创建和编辑 Firepower 服务对象, on page 150
- 点击选择 (Choose) 以将现有服务对象添加到组。重复此步骤以添加更多对象。

步骤 6 将服务对象添加到服务组后，点击添加。

步骤 7 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

编辑 Firepower 服务对象或服务组

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 过滤对象以查找要编辑的对象，然后在对象表中选择该对象。

步骤 3 在“操作”(Actions) 窗格中，点击**编辑 (Edit)**  。

步骤 4 以在上述过程中创建值的相同方式编辑对话框中的值。

步骤 5 点击**保存 (Save)**。

步骤 6 CDO 显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

步骤 7 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

安全组标记组

安全组标记

关于安全组标记

如果使用思科身份服务引擎 (ISE) 定义并使用**安全组标记** (SGT) 来对 Cisco TrustSec 网络中的流量进行分类，则可以编写使用 SGT 作为匹配条件的访问控制规则。因此，可以基于安全组成员身份阻止或允许访问，而不是使用 IP 地址。

在 ISE 中，您可以创建 SGT，并将主机或网络 IP 地址分配至各标记。如果您将 SGT 分配给用户帐户，SGT 就会被分配给用户流量。将 FDM 管理 设备配置为连接到 ISE 服务器并创建 SGT 后，您可以在 思科防御协调器 中创建 SGT 组并围绕它们构建访问控制规则。请注意，您必须先配置 ISE 的 SGT 交换协议 (SXP) 映射，然后才能将 SGT 关联到 FDM 管理 设备。有关详细信息，请参阅您当前运行的版本的《思科身份服务引擎管理员指南》中的**安全组标记交换协议**。

FDM 管理 设备评估 SGT 作为访问控制规则的流量匹配条件时，会使用以下优先级：

1. 数据包中定义的源 SGT（如有）。使用此技术无法进行目的地匹配。对于数据包中的 SGT，必须配置网络中的交换机和路由器以添加它们。有关如何实施此方法的信息，请参阅 ISE 文档。
2. 分配给用户会话的 SGT，从 ISE 会话目录下载。您需要启用此选项才能侦听此类 SGT 匹配的会话目录信息，但是，当您首次创建 ISE 身份源时，此选项会默认打开。SGT 可以与源或目标相匹配。尽管非必需，但您通常还会使用 ISE 身份源和 AD 域来设置被动身份验证身份规则，以收集用户身份信息。
3. 使用 SXP 下载的 SGT-IP 地址映射。如果 IP 地址在 SGT 范围内，则流量与使用 SGT 的访问控制规则相匹配。SGT 可以与源或目标相匹配。

Note 您无法直接在访问控制规则中使用从 ISE 检索到的信息。相反，您需要创建引用已下载 SGT 信息的 SGT 组。您的 SGT 组可以引用多个 SGT，因此您可以在适当的情况下根据相关的标记集合应用策略。

版本支持

CDO 当前在运行 6.5 和更高版本的 FDM 管理 设备上支持 SGT 和 SGT 组。FDM 管理 设备允许您在版本 6.5 及更高版本中配置并连接到 ISE 服务器，但在 6.7 之前版本中不支持在 UI 中配置 SGT。

从 FDM 管理 UI 中，这意味着运行版本 6.5 或更高版本的 FDM 管理 设备可以下载 SGT 的 SXP 映射，但不能手动添加到对象或访问控制规则。要更改运行版本 6.5 或版本 6.6 的设备的 SGT，您必须使用 ISE UI。但是，如果运行版本 6.5 的设备已被载入 思科防御协调器，则可以查看与设备关联的当前 SGT 并创建 SGT 组。

CDO 中的 SGT

安全组标记

SGT 在 CDO 中为只读。您无法在 CDO 中创建或编辑 SGT。要创建 SGT，请参阅当前运行版本的《思科身份服务引擎管理员指南》。

SGT 组

Note FDM 管理 设备将 SGT 组称作 SGT 动态对象。在 CDO 中，这些标签列表当前被称作 SGT 组。您可以在 CDO 中创建 SGT 组，而无需参考 FDM 管理 设备或 ISE UI。

使用 SGT 组可以根据 ISE 分配的 SGT 来识别源或目标地址。然后，可以将访问控制规则中的对象用于定义流量匹配条件。您无法直接在访问控制规则中使用从 ISE 检索到的信息。相反，您需要创建引用已下载 SGT 信息的 SGT 组。

您的 SGT 组可以引用多个 SGT，因此您可以在适当的情况下根据相关的标记集合应用策略。

要在 CDO 中创建 SGT 组，必须至少已经配置一个 SGT，并为要使用的设备的 FDM 管理 控制台配置来自 ISE 服务器的 SGT 映射。请注意，如果多个 FDM 管理 设备与同一 ISE 服务器关联，则可以将 SGT 或 SGT 组应用于多个设备。如果设备未与 ISE 服务器关联，则不能在访问控制规则中包含 SGT 对象，也不能将 SGT 组应用于该设备配置。

规则中的 SGT 组

SGT 组可被添加到访问控制规则；它们会显示为源或目标网络对象。有关网络如何在规则中工作的详细信息，请参阅 FDM 管理 访问控制规则中的源和目标条件。

您可以从“对象”(Objects) 页面创建 SGT 组。有关详细信息，请参阅创建 SGT 组, on page 153。

创建 SGT 组

要创建可用于访问控制规则的 SGT 组，请使用以下程序：

Before you begin

在创建安全组标记 (SGT) 组之前，必须配置以下配置或环境：

- FDM 管理 设备必须至少运行版本 6.5。

- 必须配置 ISE 身份源以订用 SXP 映射并启用部署更改。要管理 SXP 映射，请参阅所用版本（版本 6.7 及更高版本）的 Firepower 设备管理器配置指南中的**在 ISE 中配置安全组和 SXP 发布**。
- 所有 SGT 都必须在 ISE 中创建。要创建 SGT，请参阅当前运行版本的《思科身份服务引擎配置指南》。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮  以创建新的对象。

步骤 3 点击 **FTD > 网络 (Network)**。

步骤 4 输入 **对象名称 (Object Name)**。

步骤 5 （可选）添加说明。

步骤 6 点击 **SGT** 并使用下拉菜单选中要包含在组中的所有适用 SGT。您可以按 SGT 名称对列表进行排序。

步骤 7 点击**保存 (Save)**。

Note 您无法在 CDO 中创建或编辑 SGT，只能在 SGT 组中添加或删除它们。要创建或编辑 SGT，请参阅当前运行版本的《思科身份服务引擎配置指南》。

编辑 SGT 组

要编辑 SGT 组，请使用以下程序：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到您要编辑的 SGT 组。

步骤 3 选择 SGT 组，然后点击**操作 (Actions)** 窗格中的编辑图标  。

步骤 4 修改 SGT 组。编辑与该组关联的名称、说明或 SGT。

步骤 5 点击**保存 (Save)**。

Note 您无法在 CDO 中创建或编辑 SGT，只能在 SGT 组中添加或删除它们。要创建或编辑 SGT，请参阅当前运行版本的《思科身份服务引擎配置指南》。

将 SGT 组添加到访问控制规则

要将 SGT 组添加到访问控制规则，请使用以下程序：

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 FTD 选项卡，然后选择要向其添加 SGT 组的设备。

步骤 4 在**管理 (Management)** 窗格中，选择**策略 (Policy)**。

步骤 5 点击源或目标对象的蓝色加号按钮，然后选择 SGT 组。 

步骤 6 使用对象过滤器和搜索字段找到您要编辑的 SGT 组。

步骤 7 点击**保存 (Save)**。

步骤 8 预览和部署所有设备的配置更改。

Note 如果需要创建其他 SGT 组，请点击创建新对象。填写创建 FTD SGT 组并将 SGT 组添加到规则中提到的必填信息。创建 SGT 组, on page 153

系统日志服务器对象

FDM管理 设备用来存储事件的容量有限。要尽可能提高事件存储量，您可以配置外部服务器。系统日志 (syslog) 服务器对象标识可接收面向连接的消息或诊断 syslog 消息的服务器。如果已为日志收集和分析设置一台系统日志服务器，您可以使用 思科防御协调器 来创建对象以进行定义并在相关策略中使用这些对象。

创建和编辑系统日志服务器对象

要创建新的系统日志服务器对象，请执行以下步骤：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击**创建对象 (Create Object)** 按钮  。

步骤 3 选择 FDM 管理 设备对象类型下方的**系统日志服务器 (Syslog Server)**

步骤 4 配置系统日志服务器对象属性：

- **IP 地址** - 输入系统日志服务器的 IP 地址。
- **协议类型 (Protocol Type)** - 选择系统日志服务器用于接收消息的协议。如果您选择 TCP，系统可以识别何时系统日志服务器不可用，并停止发送事件，直至服务器再次可用。
- **端口号 (Port Number)** - 输入要用于系统日志的有效端口号。如果系统日志服务器使用默认端口，请输入 514 作为默认 UDP 端口或 1470 作为默认 TCP 端口。如果服务器不使用默认端口，请输入正确的端口号。端口范围必须介于 1025 至 65535 之间。

- **选择接口**-选择应使用哪个接口发送诊断系统日志消息。连接和入侵事件始终使用管理接口。接口选择决定与系统日志消息关联的 IP 地址。请注意，您只能选择下面列出的选项**之一**。不能同时选择两者。选择以下选项之一：
  - **数据接口** - 选择用于诊断系统日志消息的数据接口。从生成列表中选择一个接口。如果可以通过网桥组成员接口访问该服务器，请选择该网桥组接口 (BVI)。如果通过诊断接口（物理管理接口）访问，我们建议您选择管理接口，而不是此选项。您不能选择被动接口。对于连接和入侵系统日志消息，源 IP 地址是管理接口的地址；如果您通过数据接口进行路由，则是网关接口的地址。
  - **管理接口** - 对所有类型的系统日志消息使用虚拟管理接口。源 IP 地址是管理接口的地址；如果您通过数据接口进行路由，则是网关接口的地址。

步骤 5 点击**添加 (Add)**。

步骤 6 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

编辑系统日志服务器对象

要编辑现有的系统日志服务器对象，请执行以下步骤：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 找到所需的系统日志服务器对象并选择它。您可以按系统日志服务器对象类型过滤对象列表。

步骤 3 在“操作”(Actions) 窗格中，点击**编辑 (Edit)**。

步骤 4 进行所需的编辑，然后点击**保存 (Save)**。

步骤 5 确认您所做的更改。

步骤 6 立即 预览和部署所有设备的配置更改 您所做的更改，或等待并一次部署多个更改。

相关信息：

- 删除对象

为安全日志记录分析 (SaaS) 创建系统日志服务器对象

使用要向其发送事件的安全事件连接器 (SEC) 的 IP 地址、TCP 端口或 UDP 端口创建系统日志服务器对象。您将为已载入租户的每个 SEC 创建一个系统日志对象，但您只能将来自一个规则的事件发送到一个代表一个 SEC 的系统日志对象。

前提条件

此任务是更大工作流程的一部分。开始前，请参阅 为 FDM 管理 设备实施安全日志记录分析 (SaaS), on page 594 。

操作步骤

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击**创建对象 (Create Object)** 按钮  。

步骤 3 选择 FDM 管理 设备对象类型下方的**系统日志服务器 (Syslog Server)**。

步骤 4 配置系统日志服务器对象属性。要查找 SEC 的这些属性，请从 CDO 菜单中选择**管理 (Admin)** > **安全连接器 (Secure Connectors)**。然后，选择要为其配置系统日志对象的安全事件连接器，并查看右侧的“详细信息”窗格。

- **IP 地址 (IP Address)** - 输入 SEC 的 IP 地址。
- 协议类型 - 选择 TCP 或 UDP。
- 端口号 - 如果您选择了 TCP，请输入端口 10125；如果您选择了 UDP，请输入 10025。
- 选择接口 - 选择配置用于访问 SEC 的接口。

Note FDM 管理 设备支持每个 IP 地址一个系统日志对象，因此您必须在使用 TCP 和 UDP 之间进行选择。

步骤 5 点击**添加 (Add)**。

What to do next

继续步骤 3 实施安全日志记录分析 (SaaS) 并通过安全事件连接器将事件发送到思科云的现有 CDO 客户工作流程。

URL 对象

URL 对象和 URL 组由 Firepower 设备使用。使用 URL 对象和组（统称为“URL 对象”）可定义 Web 请求的 URL 或 IP 地址。可以使用这些对象在访问控制策略中执行手动 URL 过滤，或在安全情报策略中进行阻止。URL 对象定义单个 URL 或 IP 地址，而 URL 组可以定义多个 URL 或地址。

准备工作

在创建 URL 对象时，请记住以下要点：

- 如果不包含路径（即 URL 中无 / 字符），则匹配仅基于服务器主机名。如果主机名位于 :// 分隔符之后，或在主机名中的任何点之后，则认为该主机名匹配。例如，ign.com 匹配 ign.com 和 www.ign.com，但不匹配 verisign.com。
- 如果包含一个或多个 / 字符，则整个 URL 字符串将用于子字符串匹配，其中包括服务器名称、路径和任何查询参数。但是，我们建议您不要使用手动URL过滤阻止或允许个别网页或部分网

站，因为这样可能会重组服务器并将页面移至新路径。子字符串匹配还可能导致意外匹配，其中 URL 对象中包含的字符串也与非预期服务器上的路径或查询参数中的字符串匹配。

- 系统忽略加密协议（HTTP 与 HTTPS）。换句话说，如果阻止网站，系统将阻止发往该网站的 HTTP 和 HTTPS 流量，除非您使用一个应用条件指定特定协议。在创建 URL 对象时，您不需要指定创建对象时的协议。例如，使用 example.com 而不是 http://example.com。
- 如果您计划使用 URL 对象匹配访问控制规则中的 HTTPS 流量，请使用加密流量时所使用的公钥中的使用者公用名创建该对象。此外，系统会忽略使用者公用名中的子域，因此，不包括子域信息。例如，使用 example.com 而不是 www.example.com。

  但请注意，证书中的使用者公用名可能与网站的域名完全无关。例如，youtube.com 证书中的使用者公用名是 *.google.com（当然，这可能会随时更改）。如果使用 SSL 解密策略解密 HTTPS 流量以便 URL 过滤规则可用于解密策略，则可能获得更一致的结果。

注释 如果由于证书信息不再可用，浏览器恢复 TLS 会话，则 URL 对象将不匹配 HTTPS 流量。因此，即使精心配置 URL 对象，也可能会得到不一致的 HTTPS 连接结果。

创建或编辑 FDM 管理 URL 对象

URL 对象是指定 URL 或 IP 地址的可重用组件。

要创建 URL 对象，请执行以下步骤：

Procedure

步骤 1 在左侧的 思科防御协调器 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击创建对象**创建对象 (Create Object) > FTD > URL**。

步骤 3 输入对象名称和说明。

步骤 4 选择**创建 URL 对象 (Create a URL object)**。

步骤 5 为对象输入特定 URL 或 IP 地址。

步骤 6 点击**添加**。

创建 Firepower URL 组

URL 组可以由表示一个或多个 URL 或 IP 地址的一个或多个 URL 对象组成。Firepower 设备管理器和 Firepower 管理中心也将这些对象称为“URL 对象”。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击创建对象**创建对象 (Create Object) > FTD > URL**。

步骤 3 输入对象名称和说明。

步骤 4 选择**创建 URL 组 (Create a URL group)**。

步骤 5 通过点击**添加对象 (Add Object)**，选择一个对象，然后点击**选择 (Select)**，添加现有对象。重复此步骤以添加更多对象。

步骤 6 将 URL 对象添加到 URL 组后，点击**添加**。

编辑 Firepower URL 对象或 URL 组

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 过滤对象以查找要编辑的对象，然后在对象表中选择该对象。

步骤 3 在详细信息窗格中，点击以进行编辑。

步骤 4 以在上述过程中创建值的相同方式编辑对话框中的值。

步骤 5 点击**保存 (Save)**。

步骤 6 CDO 显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

安全策略管理

安全策略检查网络流量，最终目标是允许流量到达其预定目的地，或者在识别出安全威胁时丢弃该流量。您可以使用 CDO 在许多不同类型的设备上配置安全策略。

- FDM 策略配置， 第 322 页
- 网络地址转换， 第 399 页

FDM 策略配置

安全策略检查网络流量，最终目标是允许流量到达其预定目的地，或者在识别出安全威胁时丢弃该流量。使用 CDO 来管理 FDM 管理 设备的所有安全策略组件：

FDM 管理 访问控制策略

您可以使用 思科防御协调器 来管理 FDM 管理 设备的访问控制策略。访问控制策略通过根据访问控制规则评估网络流量来控制对网络资源的访问。FDM管理 设备会按照访问控制规则在访问控制策略中的显示顺序，将其与网络流量进行比较。当访问控制规则中的所有流量条件均为

- **信任** - 允许流量，而无需进行任何类型的进一步检测。
- **允许** - 允许流量，不受策略中的入侵及其他检测设置约束。
- **阻止** - 无条件地丢弃流量。不检测流量。

如果访问控制策略中的任何规则都与网络流量不匹配，则 FDM 管理 设备将采取访问控制规则下面列出的默认操作。

读取 FDM 管理 访问控制策略

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

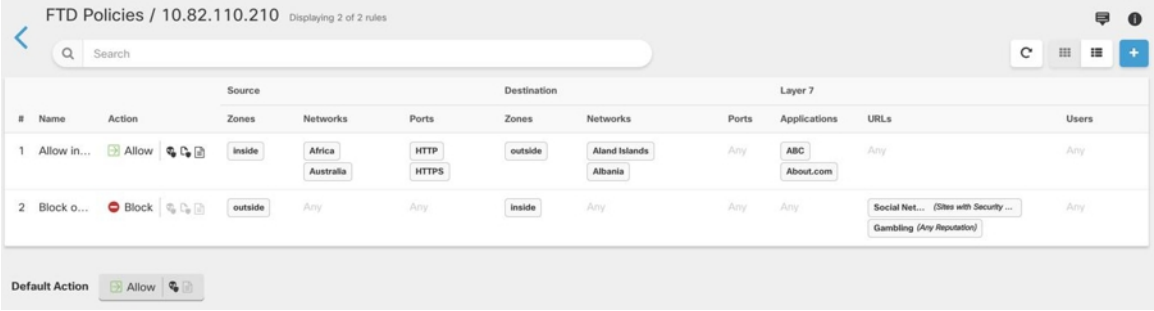
步骤 3 点击 **FTD** 选项卡，然后选择要读取其策略的设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，选择 **策略 (Policy)**。

步骤 5 要确保您看到整个策略，请点击“过滤器”(Filter) 面板中的**全部显示 (Show All)**。

步骤 6 将显示切换规则列，以便查看具有更多或更少列的规则。如果您习惯于查看FDM管理设备中的访问控制规则，请切换规则列显示以显示更多列。

以下是如何读取策略中的规则的示例。首先根据规则 1 评估所有流量是否匹配。如果流量与规则 1 匹配，则该规则的操作将应用于流量。源自内部区域的流量，AND 源自非洲或澳大利亚，AND 源自 HTTP 或 HTTPS 端口，AND 到达外部区域，AND 到达奥兰群岛或阿尔巴尼亚，AND 到达任何端口，AND 到达 ABC OR允许 About.com 从源流向目的地。我们还可以看到，入侵策略和文件策略已应用于规则，并且正在记录规则中的事件。



相关信息：

- 配置 FDM 访问控制策略

配置 FDM 访问控制策略

FDM管理 设备有一个策略。该策略的一部分具有访问控制规则。为便于讨论，我们将具有访问控制规则的策略部分称为访问控制策略。载入 FDM 管理 设备后，您可以向访问控制策略添加规则或在其中编辑规则。

如果您要载入新的 FDM 管理 设备，则导入的策略中可能没有任何规则。在这种情况下，当您打开 FDM 策略页面时，您将看到消息“未找到结果”(No results found)。如果看到该消息，则可以开始将规则添加到 FDM 托管设备策略，然后从 CDO 将其部署到设备。

开始之前的提示

向访问控制规则中添加条件时，请考虑以下提示：

- 您可以在将某些条件添加到规则时为其创建自定义对象。在对话框中查找用于创建自定义对象的链接。
- 您可以为每个规则配置多个条件。要使规则应用于流量，流量必须匹配该规则中的所有条件。例如，可以使用单一规则对特定主机或网络执行 URL 过滤。
- 最多可以为规则中的每个条件添加50个标准。匹配某个条件所有条件标准的流量满足该条件。例如，您可以使用单一规则为最多50个应用或应用过滤器执行应用控制。因此，单一条件中的项目之间为 OR 关系，但不同条件类型之间（例如，源/目的和应用之间）为 AND 关系。
- 有些功能需要您启用适当的 Firepower 许可证。
- 某些编辑任务可能不需要您进入编辑模式。从策略页面，您可修改规则中的条件，通过点击该条件栏内的 + 按钮，选择弹出对话框中的所需的对象或元素。您也可以点击对象或元素对应的 **x**，可将其从规则中移除。

创建或编辑 FDM 管理 访问控制策略

按照以下程序使用 思科防御协调器 编辑 FDM 管理 访问控制策略：

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择要编辑其策略的访问控制。

步骤 4 在右侧的**管理 (Management)** 窗格中，选择 **策略 (Policy)**。

步骤 5 执行以下任一操作：

- 要创建新规则，请点击蓝色加号按钮  。
- 要编辑现有规则，请选择该规则，然后点击**操作 (Actions)** 窗格中的编辑图标 。（也可以在不进入编辑模式的情况下内联执行简单编辑。）
- 要删除不再需要的规则，请选择该规则，然后点击“操作”(Actions) 窗格中的删除图标 。
- 要移动策略中的规则，请在访问控制表中选择该规则，然后点击规则行末尾的向上或向下箭头以移动该规则。

在编辑或添加规则时，请继续执行此程序中的其他步骤。

步骤 6 在**顺序 (Order)** 字段中，选择规则在策略中的位置。根据规则列表（按数字顺序从 1 到“最后”(last)）评估网络流量。

先匹配的规则先应用，所以您必须确保流量匹配条件标准较具体的规则显示在次之用来匹配流量的较通用条件标准的策略上方。

默认将规则添加到列表的末尾。如果以后要更改规则的位置，请编辑此选项。

步骤 7 输入规则名称。可以使用字母数字字符和以下特殊字符：+ . _ -

步骤 8 选择规则匹配网络流量时要应用的操作：

- **信任** - 允许流量，而无需进行任何类型的进一步检测。
- **允许** - 允许流量，不受策略中的入侵及其他检测设置约束。
- **阻止** - 无条件地丢弃流量。不检测流量。

步骤 9 通过使用以下选项卡的任意属性组合，定义流量匹配标准：

- **源 (Source)** - 点击**源 (Source)** 并添加或删除安全区域（接口）、网络（包括网络、大洲和自定义地理位置）或网络流量来源的端口。默认值为“任意”(Any)。
- **目标 (Destination)** - 点击**目标 (Destination)** 选项卡，然后添加或删除流量到达的安全区域（接口）、网络（包括网络、大洲和自定义地理位置）或端口。默认值为“任意”(Any)。请参阅 FDM 管理 访问控制规则中的源和目标条件。
- **应用 (Application)** - 点击**应用 (Application)**，然后添加或删除网络应用，或根据类型、类别、标签、风险或业务相关性定义应用的过滤器。默认设置为任何应用。请参阅 FDM 管理 访问控制规则中的应用条件

- **URL** - 点击 **URL** 选项卡，然后添加或删除 Web 请求的 URL 或 URL 类别。默认设置为任何 URL。请参阅 FDM 管理 访问控制规则中的 URL 条件，了解如何使用 URL 类别和信誉过滤器来调整该条件。
- **用户 (Users)** - 在规则行中可以看到从 防火墙设备管理器 添加到规则中的 Active Directory 领域对象、特殊身份（身份验证失败、访客、无需身份验证、未知）和用户组，但在CDO中尚不可编辑。

  Caution 单个用户对象在 CDO 中的访问控制策略规则中不可见。登录到 FDM 管理设备以查看单个用户对象会如何影响访问控制策略规则。

步骤 10 （可选，对于具有“允许”(Allow) 操作的规则）点击入**侵策略 (Intrusion Policy)** 选项卡，分配入侵检测策略，以检测流量是否存在入侵和漏洞。请参阅在 FDM 管理 访问控制规则中选择入侵策略。

a. **要记录入侵策略规则生成的入侵事件**，请参阅设备的“FDM 管理 设备设置”。

步骤 11 （可选，对于具有“允许”(Allow) 操作的规则）点击**文件策略 (File Policy)** 选项卡，以分配检查包含恶意软件的文件和应阻止的文件的流量的文件策略。请参阅 FDM 管理 访问控制规则中的文件策略设置。

a. **要记录入侵策略规则生成的文件事件**，请参阅设备的“FDM 管理 设备设置”。

步骤 12 （可选）点击日志记录选项卡以启用日志记录，并收集访问控制规则报告的**连接事件**。

有关日志记录设置的详细信息，请参阅 FDM 管理 访问控制规则中的日志记录设置。

如果您订用了思科安全分析和日志记录，则可以通过为安全日志记录分析 (SaaS) 创建系统日志服务器对象，在 CDO 中配置连接事件并将其发送到安全事件连接器 (SEC)。有关此功能的详细信息，请参阅FDM 管理 设备的安全日志记录分析。您将为已载入租户的每个 SEC 创建一个系统日志对象，但您只能将由一个规则生成的事件发送到一个代表一个 SEC 的系统日志对象。

步骤 13 点击**保存 (Save)**。您现在已在安全策略中配置了特定的规则。

步骤 14 您现在可以配置整个安全策略的**默认操作**。“默认操作”定义了网络流量与访问控制策略、入侵策略或文件/恶意软件策略中的任何规则都不匹配时会发生的情况。

步骤 15 点击策略的默认操作。

步骤 16 按照上面的步骤 9 配置入侵策略。

步骤 17 配置默认操作生成的日志记录连接事件。

如果您订用了思科安全分析和日志记录，则可以通过为安全日志记录分析 (SaaS) 创建系统日志服务器对象，将默认操作生成的事件发送到安全事件连接器(SEC)。有关此功能的详细信息，请参阅FDM 管理 设备的安全日志记录分析。您将为已载入租户的每个SEC创建一个系统日志对象，但您只能将由规则生成的事件发送到一个代表一个 SEC 的系统日志对象。

步骤 18 （可选）对于您创建的任何规则，您可以选择它并在“添加注释”(Add Comments) 字段中添加注释。要了解有关规则注释的详细信息，请参阅向策略和规则集中的规则添加注释。

步骤 19 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

配置访问策略设置

您可以配置应用于访问策略而不是策略中特定规则的设置。

操作步骤

这些设置适用于整个访问策略，而不是策略中的特定规则。

过程

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择要编辑其策略的访问控制。

步骤 4 在右侧的**管理 (Management)** 窗格中，选择 **策略 (Policy)**。

步骤 5 点击**设置 (Settings)** 图标并配置以下设置：

- **TLS 服务器身份发现 (TLS Server Identity Discovery)** - TLS 1.3 证书已加密。对于使用 TLS 1.3 加密的流量，要匹配使用应用或 URL 过滤的访问规则，系统必须对 TLS 1.3 证书进行解密。建议您启用此选项，以确保将加密连接与正确的访问控制规则进行匹配。此设置仅解密证书；连接保持加密状态。启用此选项即可解密 TLS 1.3 证书；您无需创建相应的 SSL 解密规则。可用于运行 6.7 或更高版本软件的 FDM 管理设备。
- **DNS 流量的信誉实施 (Reputation Enforcement on DNS Traffic)** - 启用此选项可将 URL 过滤类别和信誉规则应用于 DNS 查找请求。如果查找请求中的完全限定域名 (FQDN) 具有要阻止的类别和信誉，系统会阻止 DNS 回复。由于用户未收到 DNS 解析，因此用户无法完成连接。使用此选项可将 URL 类别和信誉过滤应用于非 Web 流量。有关详细信息，请参阅 DNS 请求过滤。适用于运行 7.0 及更高版本软件的 FDM 管理设备。

步骤 6 点击**保存 (Save)**。

关于 TLS 服务器身份发现

通常情况下，TLS 1.3 证书已加密。对于使用 TLS 1.3 加密的流量，要匹配使用应用或 URL 过滤的访问规则，系统必须对 TLS 1.3 证书进行解密。我们建议您启用早期应用检测和 URL 分类，以确保将加密连接与正确的访问控制规则进行匹配。该设置仅解密证书；连接保持加密状态。

Note 此功能当前可用于运行 6.7 或更高版本软件的 FDM 管理 设备。

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择要编辑其策略的访问控制。

步骤 4 在右侧的**管理 (Management)** 窗格中，选择 **策略 (Policy)**。

步骤 5 点击设置 按钮。

步骤 6 点击 **TLS 服务器身份发现 (TLS Server Identity Discovery)** 旁边的滑块，为加密连接启用早期应用检测和 URL 分类。

步骤 7 点击**保存 (Save)**。

复制 FDM 管理 访问控制规则

使用此程序复制访问控制规则，方法是将其从当前位置复制并粘贴到同一策略中的新位置，或者将其粘贴到不同 FDM 管理 设备的策略。您可以将规则粘贴在策略中的其他规则之前或之后，以便规则按其在策略中的正确顺序评估该网络流量。

在设备中复制规则

要复制 FDM 管理 设备中的规则，请执行以下程序：

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择要编辑其策略的 FDM 管理 设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。

步骤 5 选择要复制的一个或多个访问控制规则，然后点击右侧**操作 (Actions)** 窗格中的**复制 (Copy)**。

步骤 6 在要粘贴规则的策略中，选择复制的规则应在其前面或后面的规则，然后在**操作 (Actions)** 窗格中，点击以下选项之一：

- **粘贴前 (Paste Before)** 会自动将一个或多个复制的规则粘贴到所选规则上方，以便复制的规则排在其上方。
- **粘贴后 (Paste After)** 会自动将一个或多个复制的规则粘贴到所选规则的下方，以便复制的规则排在其下方。

可以在任何所需位置多次执行粘贴操作。

Note 在 FDM 管理 设备中粘贴规则时，如果存在具有相同名称的规则，则会将“- Copy”附加到原始名称。如果重命名的名称也存在，则会将“- Copy n”附加到原始名称。例如，“rule name - Copy 2”。

步骤 7 立即查看您的更改并将配置更改从 CDO 部署到 FDM 管理 设备，或者等待并一次部署多个更改。

将规则从一个 FDM 管理设备策略复制到另一个 FDM 管理设备策略

将规则从一个 FDM 管理设备策略复制到另一个 FDM 管理设备策略时，与这些规则关联的对象也会被复制到新的 FDM 管理设备。

在粘贴规则时，CDO 会验证某些条件。有关详细信息，请参阅将规则粘贴到另一个设备时的对象行为。

Important **重要提示**：仅当两台设备上的相同软件版本相同时，CDO 才允许您将规则从一台 FDM 管理设备复制到另一台 FDM 管理设备。如果软件版本不同，当您尝试粘贴规则时，系统会显示“规则无法粘贴，因为它们与此设备的版本不兼容”(Rules could not be pasted because they are not compatible with the version of this device)。您可以点击**详细信息 (Details)** 链接以了解详细信息。

要将规则复制到另一台 FDM 管理设备，请执行以下程序：

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择要从中复制规则的设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。

步骤 5 选择要复制的一个或多个访问控制规则，然后点击右侧**操作 (Actions)** 窗格中的**复制 (Copy)**。

步骤 6 点击**清单 (Inventory)** 并导航至要将规则复制到的 FDM 管理设备。

步骤 7 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。

步骤 8 在要粘贴刚才所复制规则的策略中，选择复制的规则应在其前面或后面的规则，然后在**操作 (Actions)** 窗格中，点击**粘贴在前 (Paste Before)** 或**粘贴在后 (Paste After)**。

步骤 9 选择要在其周围粘贴复制的规则的任何访问控制规则，然后在**操作 (Actions)** 窗格中点击以下选项之一：

- **粘贴在前 (Paste Before)** 会自动将一个或多个规则置于所选规则之上，以便复制的规则在所选规则之前评估网络流量。
- **粘贴在后 (Paste After)** 会在选定规则下自动粘贴一个或多个规则，以便复制的规则在选定规则之后评估网络流量。

可以在任何所需位置多次执行粘贴操作。

Note 在将规则粘贴到另一台 FDM 管理设备时，如果存在具有相同名称的规则，则会将“- Copy”附加到原始名称。如果重命名的名称也存在，则会将“- Copy n”附加到原始名称。例如，“rule name-Copy 2”。

步骤 10 在将规则从一台 FDM 管理设备复制到另一台设备时，目标设备的**配置状态 (Configuration Status)** 将处于“未同步”(Not Synced) 状态。立即查看您的更改并将配置更改从 CDO 部署到 FDM 管理 设备，或者等待并一次部署多个更改。

相关信息：

- 移动 FDM 管理 访问控制规则
- 将规则粘贴到另一个设备时的对象行为

移动 FDM 管理 访问控制规则

使用此功能可移动访问控制规则，方法是将其从策略中的当前位置剪切，并将其粘贴到同一策略中的新位置或不同 FDM 管理 设备的策略中。您可以将规则粘贴在策略中的其他规则之前或之后，以便规则在策略中按其适当的顺序评估该网络流量。

在设备内移动规则

要在 FDM 管理设备内移动规则，请执行以下程序：

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择您要编辑其策略的 FDM 管理 设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。

步骤 5 选择要移动的一个或多个访问控制规则，然后点击右侧“操作”(Actions) 窗格中的**剪切 (Cut)**。您选择的规则将以黄色突出显示。**注意**：如果要取消选择，请选择任何规则，然后点击**复制 (Copy)**。

步骤 6 在要粘贴刚才所剪切规则的策略中，选择剪切的规则应在其前面或后面的规则，然后在**操作 (Actions)** 窗格中，点击以下选项之一：

- **粘贴在前 (Paste Before)** 会自动将一个或多个规则粘贴在所选规则之上，以便剪切的规则在所选规则之前评估网络流量。
- **粘贴在后 (Paste After)** 会在选定规则下自动粘贴一个或多个规则，以便剪切规则在选定规则之后评估网络流量。

可以在任何所需位置多次执行粘贴操作。

Note 在FDM管理 设备中粘贴规则时，如果存在具有相同名称的规则，则会将“- Copy”附加到原始名称。如果重命名的名称也存在，则会将“- Copy n”附加到原始名称。例如，“rule name - Copy 2”。

步骤 7 立即查看您的更改并将配置更改从 CDO 部署到 FDM 管理 设备，或者等待并一次部署多个更改。

将规则从一个 FDM 管理设备策略移至另一个 FDM 管理设备策略

将规则从一个 FDM 管理设备策略移动到另一个 FDM 管理设备策略时，与这些规则关联的对象也会被复制到新的 FDM 管理设备。

在粘贴规则时，CDO 会验证某些条件。有关这些条件的详细信息，请参阅将规则粘贴到另一个设备时的对象行为。

要将规则移至另一台 FDM 管理设备，请执行以下程序：

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择要从中复制规则的 FDM 管理设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。

步骤 5 选择要移动的一个或多个访问控制规则，然后点击右侧**操作 (Actions)** 窗格中的**剪切 (Cut)**。

步骤 6 点击**清单 (Inventory)** 并导航至要将一个或多个选定规则移动到的 FDM 管理设备。

步骤 7 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。

步骤 8 在要粘贴刚才所剪切规则的策略中，选择剪切的规则应在其前面或后面的规则，然后在**操作 (Actions)** 窗格中，点击**粘贴在前 (Paste Before)** 或**粘贴在后 (Paste After)**。

- **粘贴在前 (Paste Before)** 会自动将一个或多个规则置于所选规则之上，以便剪切的规则在所选规则之前评估网络流量。
- **粘贴在后 (Paste After)** 会在选定规则下自动粘贴一个或多个规则，以便剪切规则在选定规则之后评估网络流量。

可以在任何所需位置多次执行粘贴操作。

Note 在 FDM 管理设备中粘贴规则时，如果存在具有相同名称的规则，则会将“- Copy”附加到原始名称。如果重命名的名称也存在，则会将“- Copy n”附加到原始名称。例如，“rule name - Copy 2”。

步骤 9 在将规则从一台 FDM 管理设备复制到另一台设备时，源设备和目标设备的**配置状态 (Configuration Status)** 将处于“未同步”(Not Synced) 状态。立即查看您的更改并将配置更改从 CDO 部署到 FDM 管理 设备，或者等待并一次部署多个更改。

相关信息：

- 复制 FDM 管理 访问控制规则
- 将规则粘贴到另一个设备时的对象行为

将规则粘贴到另一个设备时的对象行为

如果您剪切或复制的规则包含对象，并且您将这些规则粘贴到另一个FDM管理设备策略中，则当满足以下任何条件时，CDO 会将这些规则中的对象复制到目标 FDM 管理设备：

适用于所有类型的对象（安全区域除外）

- 目的设备不包含对象；在这种情况下，CDO 首先在目标设备中创建对象，然后再粘贴规则。
- 目标设备包含与源设备具有相同名称和相同值的对象。

对于安全区域对象

- 目的设备包含与源设备具有相同名称和相同接口的安全区域对象。
- 目的设备不包含相同的安全区域对象，并且具有在目的设备上使用的接口。
- 目的设备包含安全区域对象，则该对象为空，并且具有在目的设备上使用的接口。

对于具有 Active Directory (AD) 领域的对象

- 仅当目标设备上已存在具有相同名称的领域时，CDO 才会使用 Active Directory (AD) 领域对象来粘贴规则。

Important 在以下情况下，粘贴操作会失败：

- 如果两个设备版本之间的漏洞、地理位置、入侵或 URL 数据库存在差异，则 CDO 无法将规则粘贴到目标设备中。您需要在新设备中手动重新创建规则。
- 如果要添加的规则具有包含“仅管理”(management-only) 类型接口的安全区域。

相关信息：

- 复制 FDM 管理 访问控制规则
- 移动 FDM 管理 访问控制规则

FDM 管理 访问控制规则中的源和目标条件

访问规则的“源和目标”标准定义通过其传递流量的安全区（接口）、IP 地址或 IP 地址的国家/地区或大洲（地理位置）或流量中使用的协议和端口。默认设置为任何区域、地址、地理位置、协议和端口。

要修改访问控制规则中的源或目标条件，可以使用 配置 FDM 访问控制策略中的程序编辑规则。无需进入编辑模式即可执行简单编辑。在策略页面中，您可以修改规则中的条件，方法是选择规则并点击源或目标条件列中的 + 按钮，然后在弹出对话框中选择新的对象或元素。您也可以点击对象或元素对应的 **x**，可将其从规则中移除。

您可以通过以下标准来标识规则中要匹配的源和目标。

源区域、目标区域

安全区对象，定义通过其传递流量的接口。可以定义一个或两个条件，也可以不定义任何条件：未指定的任何条件都将应用到任何接口上的流量。

- 要匹配从区域中的接口离开设备的流量，请将该区域添加至目标区域。
- 要匹配从区域中的接口进入设备的流量，请将该区域添加至源区域。
- 如果同时向一条规则添加源区域和目标区域条件，匹配流量必须源自其中一个指定源区域并通过其中一个目标区域流出。

如果应基于流量进入或离开设备的位置来应用规则，请使用此条件。例如，如果要确保到达内部主机的所有流量均进行入侵检测，则应将内部区域选为目标区域，同时将源区域保留为空。要在规则中实施入侵过滤，则规则操作必须为允许，并且必须在该规则中选择入侵策略。

Note 不能在同一规则中搭配使用被动和路由安全区域。此外，被动安全区域只能被指定为源区域，不能作为目标区域。

源网络、目标网络

定义流量的网络地址或位置的网络对象或地理位置。

- 要匹配来自某个 IP 地址或地理位置的流量，请配置源网络。
- 要匹配流向 IP 地址或地理位置的流量，请配置目标网络。
- 如果同时向一条规则添加源网络条件和目标网络条件，匹配流量必须源自其中一个指定 IP 地址并流向其中一个目标 IP 地址。

添加此条件时，可从以下选项卡中进行选择：

- 网络 - 为您要控制的流量选择定义源或目标 IP 地址的网络对象或组。您可以使用通过完全限定域名 (FQDN) 定义地址的对象；通过 DNS 查询确定地址。
- 地理位置 - 选择要基于流量的源或目的国家/地区或大洲控制流量的地理位置。选择大洲将会选择该大洲内的所有国家/地区。除了直接在规则中选择地理位置外，也可以选择您创建的地理位置对象来定义位置。使用地理位置，可以便捷地限制对特定国家/地区的访问，而不需要知道此位置所用的全部潜在 IP 地址。

Note 为了确保使用最新的地理位置数据来过滤流量，思科强烈建议您定期更新地理位置数据库 (GeoDB)。

源端口、目标端口/协议

定义流量中所用协议的端口对象。对于 TCP/UDP，这可能包括端口。对于 ICMP，可包括代码和类型。

- 要匹配来自协议或端口的流量，请配置**源端口**。源端口只能为 TCP/UDP。
- 要匹配流向协议或端口的流量，请配置**目标端口/协议**。如果仅将目标端口添加至条件，则可以添加使用不同传输协议的端口。ICMP 和其他非 TCP/UDP 规格仅可用于目标端口，不允许用于源端口。
- 要同时匹配来自特定 TCP/UDP 端口的流量和流向特定 TCP/UDP 端口的流量，请配置源端口和目标端口。如果同时将源和目标端口添加至条件，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，您可以匹配从端口 TCP/80 流至端口 TCP/8080 的流量。

FDM 管理 访问控制规则中的 URL 条件

访问控制规则中的 URL 条件对 Web 请求中使用的 URL 或请求的 URL 所属的类别进行定义。对于类别匹配，您还可以指定要允许或阻止的站点的相对信誉。默认设置为允许所有 URL。

URL 类别和信誉可供您快速创建访问控制规则的 URL 标准。例如，您可以阻止所有游戏站点或所有高风险社交网站。如果用户尝试浏览至任何包含该类别和信誉组合的 URL，会话将被阻止。

使用类别和信誉数据还会简化策略创建和管理。此方法可保证系统将按预期控制网络流量。最后，由于思科的威胁智能会不断更新有关新 URL 以及现有 URL 的新类别和新风险的信息，因此可以确保系统使用最新信息来过滤所请求的 URL。代表安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的恶意站点出现和消失的速度可能比您更新和部署新策略的速度要快。

要修改访问控制规则中的 URL 和 URL 类别条件，您可以使用配置 FDM 访问控制策略中的程序编辑规则。无需进入编辑模式即可执行简单编辑。在策略页面中，您可以修改规则中的 URL 条件，方法是选择规则并点击 URL 条件列中的 + 按钮，然后在弹出对话框中选择新的对象、元素、URL 声誉或 URL 类别。您也可以点击对象或元素对应的 **x**，可将其从规则中移除。

点击蓝色加号图标  ，选择 URL 对象、组或 URL 类别，然后点击**保存 (Save)**。如果所需的 URL 对象不存在，可以点击“创建新对象”(Create New Object)。有关 URL 对象的详细信息，请参阅创建或编辑 FDM 管理 URL 对象。

URL 过滤的许可证要求

要使用 URL 过滤，您需要在 FDM 管理设备上启用 **URL** 许可证。

为规则中使用的 URL 类别指定信誉

默认情况下，规则会以相同的方式处理 URL 类别中的所有 URL。例如，如果您有阻止社交网络 URL 的规则，则无论信誉如何，都将阻止所有这些 URL。您可以调整该设置，以便只阻止高风险社交网络站点。同样，您可以允许 URL 类别中的所有 URL，但高风险站点除外。

使用此程序可对访问控制规则中的 URL 类别使用信誉过滤器：

Procedure

步骤 1 在“FTD 策略”(FTD Policy) 页面中，选择要编辑的规则。

步骤 2 点击**编辑 (Edit)**。

步骤 3 点击 **URL** 选项卡。

步骤 4 点击蓝色加号按钮  ，然后选择 URL 类别。

步骤 5 点击**将信誉应用于所选的类别 (Apply Reputation to Selected Categories)** 或您刚刚选择的 URL 类别上的**任何信誉 (Any Reputation)** 链接。

步骤 6 取消选中**任何信誉 (Any Reputation)** 复选框。

步骤 7 按信誉过滤 URL：

- 如果规则具有阻止操作，请将信誉滑块滑动到右侧，以便仅阻止信誉标记为红色的站点。例如，如果将滑块滑动到“具有安全风险的站点”(Sites with Security Risks)，则阻止规则将阻止“具有安全风险的站点”(Sites with Security Risks)、“可疑站点”(Suspicious Sites) 和“高风险站点”(High-Risk sites)，但它会允许来自“公认站点”(Well-known Sites)和“良性站点”(Benign Sites) 的流量站点。
- 如果规则具有允许操作，请将信誉滑块滑动到右侧，以便仅允许信誉标记为绿色的站点。例如，如果将滑块滑动到“良性站点”(Benign Sites)，规则将允许来自“公认站点”(Well-Known Sites) 和“良性站点”(Benign Sites) 的流量，但不允许来自“具有安全风险的站点”(Sites with Security Risks)、“可疑站点”(Suspicious Sites) 和“高风险站点”(High-Risk sites).

步骤 8 点击**保存 (Save)**。

步骤 9 点击 **Select**。

步骤 10 点击**保存 (Save)**。

步骤 11 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

在 FDM 管理 访问控制规则中选择入侵策略

思科通过 Firepower 系统提供多种入侵策略。这些策略由思科 Talos 安全情报和研究小组设计，他们设定了入侵和预处理器规则的状态和高级设置。

入侵策略的许可证和操作要求

- **许可证 (Licenses)** - 要将入侵策略添加到规则，您需要在 FDM 管理 设备上启用 许可证
- **规则操作 (Rule action)** - 您只能对**允许**流量的规则配置入侵策略和文件策略。对于设置为**信任**或**阻止**流量的规则，系统不会执行检测。此外，如果访问控制策略的默认操作是**允许**，则您可以配置入侵策略，但不能配置文件策略。

访问控制规则的可用入侵策略

对于允许流量的访问控制规则，您可以选择以下任一入侵策略来检测流量中是否存在入侵和攻击程序。入侵策略根据模式检查已解码数据包中是否存在攻击，并且可以阻止或修改恶意流量。

策略将按安全性由低到高列出：

- **连接优先于安全** - 此策略适用于连接（即确保能够获取所有资源）优先于网络基础设施安全的组织。此入侵策略启用的规则远远少于“安全优先于连接”策略中启用的规则。仅会启用阻止流量的最重要规则。如果要应用某些入侵保护，但对网络的安全性相当自信，可选择此策略。
- **平衡安全和连接** - 此策略用于平衡整体网络性能和网络基础设施安全性。此策略适合大多数网络。对于要应用入侵防御的大多数情况，可选择此策略。
- **安全性优先于连接** - 此策略适用于网络基础设施安全优先于用户便利性的组织。此入侵策略将启用许多可能会提醒或丢弃合法流量的网络异常入侵规则。如果安全性至上或针对高风险流量，可选择此策略。
- **最大检测** - 此策略适用于网络基础设施安全性比在“安全优先于连接”策略中还要重要、有可能产生更大运营影响的组织。例如，入侵策略将启用大量威胁类别中的规则，包括恶意软件、攻击程序包、旧漏洞和常见漏洞及已知外部攻击程序。如果选择此策略，请仔细评估是否要丢弃过多的合法流量。

相关信息

- FDM 管理 访问控制策略中的入侵、文件和恶意软件检测

FDM 管理 访问控制规则中的文件策略设置

借助适用于 Firepower 的高级恶意软件保护（适用于 Firepower 的 AMP），可使用文件策略检测恶意软件（或恶意软件）。另外，您还可以使用文件策略执行文件控制，以允许控制特定类型的所有文件，而不考虑文件中是否包含恶意软件。

适用于 Firepower 的 AMP 使用 AMP 云检索网络流量中检测到的潜在恶意软件的处置，并获取本地恶意软件分析和文件预分类更新。管理接口必须可连接互联网，以便访问 AMP 云并搜索恶意软件。当设备检测到符合条件的文件时，它将使用该文件的 SHA-256 散列值来查询 AMP 云中是否存在该文件的处置。可能的处置包括：

- 恶意软件 - AMP 云将文件归类为恶意软件。如果其中的任何文件为恶意软件，存档文件（例如 zip 文件）会被标记为恶意软件。
- 安全 - AMP 云将文件归类为安全，不含恶意软件。如果其中的所有文件都安全，存档文件将会标记为安全。
- 未知 - AMP 云尚未指定该文件的处置。如果其中的任何文件属于未知状态，存档文件会被标记为未知。
- 不可用 - 系统无法通过查询 AMP 云来确定文件的处置。您可能看到很少一部分事件为此处置；这是预期行为。如果您连续看到许多“不可用”事件，请确保管理地址的互联网连接正常运行。

文件策略的许可证和操作要求

许可证 - 要将文件策略添加到规则，您需要在 Firepower 设备管理器上启用两个许可证：

- 许可证
- 恶意软件许可证

规则操作 - 您只能对允许流量的规则配置文件策略。对于设置为信任或阻止流量的规则，系统不会执行检测。此外，如果访问控制策略的默认操作是允许，则您可以配置入侵策略，但不能配置文件策略。

访问控制规则的可用文件策略

- **无** - 不评估传输的文件中是否存在恶意软件，且不阻止特定的文件。对于文件传输受信任或不可能传输文件的规则或您相信自己的应用或URL过滤可适当保护网络的规则，请选择此选项。
- **阻止所有恶意软件** - 查询 AMP 云以确定通过网络传输的文件是否包含恶意软件，然后阻止存在威胁的文件。
- **全部执行云查找** - 查询 AMP 云以获取和记录通过网络传输的文件的处置，同时仍允许文件传输。
- **阻止 Office 文档和 PDF 上传、阻止其他恶意软件** - 阻止用户上传 Microsoft Office 文档和 PDF。此外，查询 AMP 云以确定遍历网络的文件是否包含恶意软件，然后阻止存在威胁的文件。
- **阻止 Office 文档上传、阻止其他恶意软件** - 阻止用户上传 Microsoft Office 文档。此外，查询 AMP 云以确定遍历网络的文件是否包含恶意软件，然后阻止存在威胁的文件。

相关信息：

- 在 FDM 管理 访问控制规则中选择入侵策略

FDM 管理 访问控制规则中的日志记录设置

访问控制规则的日志记录设置

访问规则的日志记录设置确定是否对匹配规则的流量发出连接事件。

您应该根据您组织的安全和合规性需求记录连接。如果您的目标是限制所生成事件的数量和提高性能，则只能启用对分析至关重要的连接的日志记录。然而，如果出于分析目的，您想要广泛了解网络流量，则可启用其他连接的日志记录。

Caution 在拒绝服务 (DoS) 攻击期间记录被阻止的 TCP 连接会影响系统性能并因多个相似事件使数据库不堪重负。在对“阻止”规则启用日志记录之前，请考虑该规则是否监控面向互联网的接口或其他易受 DoS 攻击的接口。

操作步骤

Procedure

步骤 1 配置 FDM 访问控制策略，然后点击**日志记录**选项卡。

步骤 2 指定日志操作：

- **在连接开始和结束时记录** - 在连接开始和结束时发出事件。由于连接结束事件包含连接开始事件所含的一切，以及连接期间可能收集的所有信息，所以思科建议不要对允许的流量选择此选项。记录两种事件可能会影响系统性能。但是，这是针对阻止的流量唯一允许的选项。
- **在连接结束时记录** - 如果要在连接结束时启用连接日志记录（建议对允许或受信任的流量执行此操作），请选择此选项。
- **不记录 (Log None)** - 选择此选项，可对规则禁用日志记录。这是默认值。

Note 当访问控制规则调用的入侵策略检测到入侵并生成入侵事件时，系统会在发生入侵的位置自动记录连接终止，无论该规则的日志记录配置如何。对于入侵受阻的连接，连接日志中的连接操作为**阻止**，原因为**入侵阻止**，即使执行入侵检测，也必须使用“允许”规则。

步骤 3 指定将连接事件发送至何处：

如果要将事件副本发送到外部系统日志服务器，请选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，则需要创建一个。有关详细信息，请参阅创建和编辑系统日志服务器对象。

由于设备中的事件存储受限，所以将事件发送至外部系统日志服务器可供长期存储，并增强您的事件分析。

对于FDM 管理 设备的安全日志记录分析用户：

- 如果通过安全事件连接器 (SEC) 将事件发送到思科云，请为安全日志记录分析 (SaaS) 创建系统日志服务器对象。然后，您将能够在文件策略和恶意软件策略连接事件旁边看到这些事件。
- 如果不使用 SEC 将事件直接发送到思科云，请指定记录事件的时间（在连接开始或结束时），但不要将 SEC 指定为系统日志服务器。

步骤 4 文件事件

如果要对禁止文件或恶意软件事件启用日志记录，请选中**日志文件 (Log Files)**。只有在规则中选择了文件策略，才能配置此选项。如果对规则选择了文件策略，则该选项默认处于启用状态。我们建议您将此选项保留为已启用。

当系统检测到受禁文件时，它会将以下类型事件之一自动记录到 FDM 管理 内部缓冲区：

- 文件事件，代表检测到或阻止的文件，包括恶意软件文件。
- 恶意软件事件，仅代表检测到或阻止的恶意软件文件。
- 可追溯的恶意软件事件，在之前检测到的文件的恶意软件处置变更时生成。

对于文件受阻的连接，连接记录中的连接操作为阻止，即便要执行文件和恶意软件检测，也必须使用“允许”规则。连接原因是“文件监控”（检测到某种文件类型或恶意软件）或者是“恶意软件阻止”或“文件阻止”（文件被阻止）

步骤 5 点击**保存 (Save)**。

步骤 6 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

安全组标记

关于安全组标记

如果使用思科身份服务引擎 (ISE) 定义并使用**安全组标记** (SGT) 来对 Cisco TrustSec 网络中的流量进行分类，则可以编写使用 SGT 作为匹配条件的访问控制规则。因此，可以基于安全组成员身份阻止或允许访问，而不是使用 IP 地址。

在 ISE 中，您可以创建 SGT，并将主机或网络 IP 地址分配至各标记。如果您将 SGT 分配给用户帐户，SGT 就会被分配给用户流量。将 FDM 管理 设备配置为连接到 ISE 服务器并创建 SGT 后，您可以在 思科防御协调器 中创建 SGT 组并围绕它们构建访问控制规则。请注意，您必须先配置 ISE 的 SGT 交换协议 (SXP) 映射，然后才能将 SGT 关联到 FDM 管理 设备。有关详细信息，请参阅您当前运行的版本的《思科身份服务引擎管理员指南》中的**安全组标记交换协议**。

FDM 管理 设备评估 SGT 作为访问控制规则的流量匹配条件时，会使用以下优先级：

1. 数据包中定义的源 SGT（如有）。使用此技术无法进行目的地匹配。对于数据包中的 SGT，必须配置网络中的交换机和路由器以添加它们。有关如何实施此方法的信息，请参阅 ISE 文档。
2. 分配给用户会话的 SGT，从 ISE 会话目录下载。您需要启用此选项才能侦听此类 SGT 匹配的会话目录信息，但是，当您首次创建 ISE 身份源时，此选项会默认打开。SGT 可以与源或目标相匹配。尽管非必需，但您通常还会使用 ISE 身份源和 AD 域来设置被动身份验证身份规则，以收集用户身份信息。
3. 使用 SXP 下载的 SGT-IP 地址映射。如果 IP 地址在 SGT 范围内，则流量与使用 SGT 的访问控制规则相匹配。SGT 可以与源或目标相匹配。

Note 您无法直接在访问控制规则中使用从 ISE 检索到的信息。相反，您需要创建引用已下载 SGT 信息的 SGT 组。您的 SGT 组可以引用多个 SGT，因此您可以在适当的情况下根据相关的标记集合应用策略。

版本支持

CDO 当前在运行 6.5 和更高版本的 FDM 管理 设备上支持 SGT 和 SGT 组。FDM 管理 设备允许您在版本 6.5 及更高版本中配置并连接到 ISE 服务器，但在 6.7 之前版本中不支持在 UI 中配置 SGT。

从 FDM 管理 UI 中，这意味着运行版本 6.5 或更高版本的 FDM 管理 设备可以下载 SGT 的 SXP 映射，但不能手动添加到对象或访问控制规则。要更改运行版本 6.5 或版本 6.6 的设备的 SGT，您必须使用 ISE UI。但是，如果运行版本 6.5 的设备已被载入 思科防御协调器，则可以查看与设备关联的当前 SGT 并创建 SGT 组。

CDO 中的 SGT

安全组标记

SGT 在 CDO 中为只读。您无法在 CDO 中创建或编辑 SGT。要创建 SGT，请参阅当前运行版本的《思科身份服务引擎管理员指南》。

SGT 组

Note FDM 管理 设备将 SGT 组称作 SGT 动态对象。在 CDO 中，这些标签列表当前被称作 SGT 组。您可以在 CDO 中创建 SGT 组，而无需参考 FDM 管理 设备或 ISE UI。

使用 SGT 组可以根据 ISE 分配的 SGT 来识别源或目标地址。然后，可以将访问控制规则中的对象用于定义流量匹配条件。您无法直接在访问控制规则中使用从 ISE 检索到的信息。相反，您需要创建引用已下载 SGT 信息的 SGT 组。

您的 SGT 组可以引用多个 SGT，因此您可以在适当的情况下根据相关的标记集合应用策略。

要在 CDO 中创建 SGT 组，必须至少已经配置一个 SGT，并为要使用的设备的 FDM 管理 控制台配置来自 ISE 服务器的 SGT 映射。请注意，如果多个 FDM 管理 设备与同一 ISE 服务器关联，则可以将 SGT 或 SGT 组应用于多个设备。如果设备未与 ISE 服务器关联，则不能在访问控制规则中包含 SGT 对象，也不能将 SGT 组应用于该设备配置。

规则中的 SGT 组

SGT 组可被添加到访问控制规则；它们会显示为源或目标网络对象。有关网络如何在规则中工作的详细信息，请参阅 FDM 管理 访问控制规则中的源和目标条件。

您可以从“对象”(Objects) 页面创建 SGT 组。有关详细信息，请参阅创建 SGT 组, on page 153。

创建 SGT 组

要创建可用于访问控制规则的 SGT 组，请使用以下程序：

Before you begin

在创建安全组标记 (SGT) 组之前，必须配置以下配置或环境：

- FDM 管理 设备必须至少运行版本 6.5。
- 必须配置 ISE 身份源以订用 SXP 映射并启用部署更改。要管理 SXP 映射，请参阅所用版本（版本 6.7 及更高版本）的 Firepower 设备管理器配置指南中的**在 ISE 中配置安全组和 SXP 发布**。
- 所有 SGT 都必须在 ISE 中创建。要创建 SGT，请参阅当前运行版本的《思科身份服务引擎配置指南》。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮  以创建新的对象。

步骤 3 点击 **FTD > 网络 (Network)**。

步骤 4 输入 **对象名称 (Object Name)**。

步骤 5 （可选）添加说明。

步骤 6 点击**SGT**并使用下拉菜单选中要包含在组中的所有适用SGT。您可以按SGT名称对列表进行排序。

步骤 7 点击**保存 (Save)**。

Note 您无法在 CDO 中创建或编辑 SGT，只能在 SGT 组中添加或删除它们。要创建或编辑 SGT，请参阅当前运行版本的《思科身份服务引擎配置指南》。

编辑 SGT 组

要编辑 SGT 组，请使用以下程序：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到您要编辑的 SGT 组。

步骤 3 选择 SGT 组，然后点击**操作 (Actions)** 窗格中的编辑图标  。

步骤 4 修改 SGT 组。编辑与该组关联的名称、说明或 SGT。

步骤 5 点击**保存 (Save)**。

Note 您无法在 CDO 中创建或编辑 SGT，只能在 SGT 组中添加或删除它们。要创建或编辑 SGT，请参阅当前运行版本的《思科身份服务引擎配置指南》。

将 SGT 组添加到访问控制规则

要将 SGT 组添加到访问控制规则，请使用以下程序：

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 FTD 选项卡，然后选择要向其添加 SGT 组的设备。

步骤 4 在**管理 (Management)** 窗格中，选择**策略 (Policy)**。

步骤 5 点击源或目标对象的蓝色加号按钮，然后选择 SGT 组。 

步骤 6 使用对象过滤器和搜索字段找到您要编辑的 SGT 组。

步骤 7 点击**保存 (Save)**。

步骤 8 预览和部署所有设备的配置更改。

Note 如果需要创建其他 SGT 组，请点击创建新对象。填写创建 FTD SGT 组并将 SGT 组添加到规则中提到的必填信息。创建 SGT 组, on page 153

FDM 管理 访问控制规则中的应用条件

访问规则的“应用”条件对 IP 连接中使用的应用进行定义，或按类型、类别、标记、风险或业务相关性定义应用的过滤器。默认设置为任何应用。

虽然您可以在规则中指定个别应用，但应用过滤器可简化策略创建和管理。例如，您可以创建一条访问控制规则，用于识别并阻止所有业务相关性较低的高风险应用。如果用户尝试使用这些应用中的任何一个，系统会阻止会话。

另外，思科会通过系统和漏洞数据库 (VDB) 更新频繁更新和添加其他应用检测器。因此，阻止高风险应用的规则可自动应用到新应用中，而无需您手动更新规则。

您可以直接在规则指定应用和过滤器，也可以创建定义这些特征的应用过滤器对象。规格相当，尽管如果要创建复杂规则，使用对象可便于遵守每个条件50个项目的系统限制。有关创建应用过滤器对象的详细信息，请参阅创建和编辑 Firepower 应用过滤器对象。

要修改规则中使用的应用和应用过滤器，可以使用FDM 管理 访问控制策略中的程序编辑规则。无需进入编辑模式即可执行简单编辑。在策略页面中，您可以修改规则中的应用条件，方法是选择规则并点击应用条件列中的 + 按钮，然后在弹出对话框中选择新的对象或元素。您也可以点击对象或元素对应的 **x**，可将其从规则中移除。

FDM 管理 访问控制策略中的入侵、文件和恶意软件检测

入侵策略和文件策略共同发挥作用，作为允许流量到达其目标之前的最后一道防线。

- 入侵策略监管系统的入侵防御功能。
- 文件策略监管系统的文件控制和适用于 Firepower 的 AMP 功能。

处理所有其他流量后，才会检验网络流量中是否存在入侵、禁止文件和恶意软件。通过将入侵策略或文件策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要使用入侵策略和/或文件策略检测流量。

您只能对允许流量的规则配置入侵策略和文件策略。对于设置为信任或阻止流量的规则，系统不会执行检测。此外，如果访问控制策略的默认操作是允许，则您可以配置入侵策略，但不能配置文件策略。

对由访问控制规则处理的任何单个连接，文件检测均发生在入侵检测之前。也就是说，系统不检测文件策略所阻止的文件是否存在入侵。在文件检测中，基于类型的简单阻止优先于恶意软件检测和阻止。文件在会话中得以检测和阻止之前，来自该会话的数据包均可能接受入侵检测。

Note 默认情况下，系统禁用对已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。检测仅适用于未加密的流量。

相关信息：

- 在 FDM 管理 访问控制规则中选择入侵策略
- FDM 管理 访问控制规则中的文件策略设置

FDM 管理 访问控制规则中的自定义 IPS 策略

不能将同一自定义 IPS 策略的多个实例与单个设备关联。

Note 将 IPS 策略与访问控制规则相关联意味着传递的流量将被提交到深度数据包检查。具有 IPS 策略的访问控制规则唯一受支持的规则操作是**允许 (Allow)**。

使用以下程序将自定义 IPS 策略关联到 FDM 管理 设备：

Procedure

步骤 1 创建自定义 IPS 策略。有关详细信息，请参阅配置 Firepower 自定义 IPS 策略。

步骤 2 在 思科防御协调器 导航窗格中，选择**策略 (Policies)**。点击 **FTD/Meraki/AWS 策略 (FTD / Meraki / AWS Policies)**。

步骤 3 滚动或过滤 FDM 管理 设备策略列表，然后选择要与自定义 IPS 策略关联的策略。

步骤 4 点击蓝色加号按钮  。

步骤 5 在**顺序 (Order)** 字段中，选择规则在策略中的位置。根据规则列表（按数字顺序从 1 到“最后”(last)）评估网络流量。

步骤 6 输入规则名称。可以使用字母数字字符和以下特殊字符：+ . _ -

步骤 7 选择**入侵策略 (Intrusion Policy)** 选项卡。展开下拉菜单以查看所有可用的入侵策略，然后选择所需的自定义 IPS 策略。

步骤 8 使用以下选项卡中的任意属性组合定义流量匹配条件：**源/目标 (Source/Destination)**、**URLs**, **应用 (Applications)** 和**文件策略 (File Policy)**。

步骤 9 （可选）点击日志记录选项卡以启用日志记录，并收集访问控制规则报告的**连接事件**。

步骤 10 点击**保存 (Save)**。

步骤 11 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

Firepower 威胁防御中的 TLS 服务器身份发现

现在，您可以使用 威胁防御 的独特 TLS 服务器身份发现来对流量执行改进的 URL 过滤和应用控制，从而在环境中实现可控性和精确性。您没有解密流量才能使此功能正常工作。

Note 对服务器身份发现功能的支持仅限于版本 6.7 及更高版本。

启用 TLS 服务器身份发现

使用以下程序为 FDM 管理访问控制策略启用或禁用 TLS 服务器身份发现功能：

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡并选择设备。

步骤 4 在位于右侧的**管理 (Management)** 窗格中，选择**策略 (Policy)**。

步骤 5 点击表右上角的访问策略设置齿轮图标 。

步骤 6 滑动开关以启用 TLS 服务器身份发现。

步骤 7 点击**保存 (Save)**。

入侵防御系统

思科 Talos 情报组 (Talos) 实时检测和关联威胁，并维护数十亿个文件的信誉处理情况。思科 IOS 入侵防御系统 (IPS) 是一种内联深度数据包检测功能，通过使用来自 Talos 的威胁情报数据来实时准确识别、分类和丢弃恶意流量，从而缓解网络上的攻击。

思科防御协调器 (CDO) Cisco Defense Orchestrator (CDO) 能够激活并调整运行软件版本 6.4.xx 至 6.6.0.x 和 6.6.1.x 的 FDM 管理 设备上的 IPS 功能。

Note CDO 当前不支持版本 6.7 上的 IPS 规则调整。

在 CDO 菜单栏上，导航到**策略 (Policies) > 前面覆盖 (Signature Overrides)** 以执行以下任务：

- 解决跨设备覆盖的不一致问题。
- 查看和隐藏威胁事件。
- 通过更改规则操作来覆盖威胁事件的处理方式。

相关信息：

- Firepower 入侵策略签名覆盖
- 威胁事件
- 入侵防御系统故障排除

威胁事件

威胁事件报告是在匹配思科 Talos 的入侵策略后已丢弃或已生成警报的流量的报告。在大多数情况下，无需调整 IPS 规则。如有必要，您可以选择通过更改 思科防御协调器 中的匹配规则操作来覆盖事件的处理方式。

请注意“威胁”(Threats) 页面的以下行为：

- 显示的威胁事件不是实时的。设备每小时轮询一次，以查找其他威胁事件。
- 未包含在查看实时事件 视图中的威胁事件不属于思科安全分析和日志记录。
- 要查看已隐藏的威胁事件，请点击过滤器图标并选中**查看隐藏 (view hidden)** 选项。
- 如果您是FDM 管理 设备的安全日志记录分析的订户，则您在“威胁事件”(Threat Events) 表中看到的事件不包含发送到安全事件连接器的事件。

Procedure

步骤 1 从导航窗格中，选择 **监控 (Monitoring)** > **威胁 (Threats)**。您可以对象过滤器显示的事件，并按源 IP 地址进行搜索。

步骤 2 点击威胁事件可展开右侧的详细信息面板。

a) 有关规则的详细信息，请点击**规则详细信息 (Rule Details)** 部分中的 **规则文档 (Rule Document)** URL。

b) 要隐藏此事件，请选中**隐藏事件 (Hide Events)** 的切换开关。事件处理将按原样继续，但您不会在此处看到它，除非您点击**查看隐藏 (View Hidden)** 或取消隐藏此事件。

c) 要编辑规则覆盖，请点击**调整规则 (Tune Rule)**。当您在 CDO 中更改规则操作时，覆盖将应用于所有预定义策略。这与 FDM 不同，在 FDM 管理 设备中，每个规则可能因政策而异。

Note CDO 提供在运行软件版本 6.4.xx 至 6.6.0.x 和 6.6.1.x 的 FDM 管理 设备上调整规则的功能。CDO 当前不支持 FDM 管理 版本 6.7 上的规则调整。

- 在**覆盖所有 (Override All)** 设备下拉列表中，选择一个操作，然后点击**保存 (Save)**。
  - **丢弃 (Drop)** - 当此规则与流量匹配时，此选择规则创建一个事件同时丢弃连接。使用此操作可加强某些规则的安全性。例如，当 Talos 规则匹配时，即使为访问控制规则指定了“连接优先于安全”策略，指定 Drop 也会提高安全性。
  - **警报 (Alert)** - 当此规则与流量匹配时，此选择创建一个事件但不丢弃连接。“警报”的一个使用案例是流量被阻止，但客户希望允许，并在禁用规则之前查看警报。
  - **已禁用 (Disabled)** - 此选项可防止流量与规则匹配。不生成事件。“禁用”的使用案例是停止报告中的误报，或删除不适用于您的环境的规则，例如，如果您不使用 httpd，则禁用 Apache httpd 规则。
  - **默认 (Default)** - 对于在其中列出的入侵策略，此选项将规则恢复为 Talos 为其分配的默认操作。例如，当您将入侵规则恢复为“默认”时，这可能意味着其操作在“连接优先于安全”策略和“平衡安全性和连接”策略中的“阻止”。

- 要按设备编辑规则覆盖，请选中**高级选项 (Advanced Options)**滑块。此部分显示为每个设备配置的规则操作，您可以通过选中受影响的设备，选择覆盖操作，然后点击**保存 (Save)** 来更改规则操作。
- **受影响的设备**不表示源设备。相反，它会显示报告事件的 FDM 管理 设备。

Note

- 点击刷新 ( ) 按钮可刷新根据当前搜索过滤器显示威胁的表。
- 点击导出 ( ) 按钮，将威胁的当前摘要下载到逗号分隔值 (.csv) 文件。您可以在电子表格应用（例如 Microsoft Excel）中打开 .csv 文件，对列表中的项目进行排序和过滤。CDO 会将基本威胁详细信息导出到文件，但时间、来源和设备等附加信息除外。

步骤 3 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

Firepower 入侵策略签名覆盖

在大多数情况下，无需调整任何 IPS 规则。如有必要，您可以选择通过更改 CDO 中的匹配规则操作来覆盖事件的处理方式。CDO 为您提供解决覆盖问题的选项。

管理签名覆盖

Procedure

步骤 1 在主导航栏中，点击**策略 (Policies) > 签名覆盖 (Signature Overrides)**。您可以对象过滤器显示的设备和策略覆盖策略。您还可以按名称或入侵规则 SID 来搜索入侵策略。

步骤 2 点击策略覆盖策略的名称，以便展开右侧的详细信息面板。

步骤 3 在**问题 (Issues)** 窗格中， 标记表示设备之间的覆盖不一致。您可以看到包含受影响设备数量的“不一致”(INCONSISTENT) 字段： INCONSISTENT 2 Resolve | Ignore

a) **要忽略问题**，请点击**忽略 (Ignore)**。这不会更改问题，但会从**问题 (Issues)** 列中删除指示器标记。

b) **要解决此问题**，请点击**解决 (Resolve)**。在左侧面板中，选择要比较的策略，然后显示其一致和不一致的覆盖。

- 要合并策略，请执行以下操作：
  1. 点击**通过合并解决 (Resolve by Merging)** 以便将其合并为一个策略，在其所有设备上采用相同的覆盖。
  2. 点击 **Confirm**。
- 要重命名策略：
  1. 在策略的部分中，点击**重命名 (Rename)** 并为其指定其他名称。
  2. 点击 **Confirm**。

- 要忽略策略，请执行以下操作：
  1. 在策略的部分中，点击**忽略 (Ignore)**。
  2. 点击 **Confirm**。
- 要忽略所有不一致，请点击**全部忽略 (Ignore All)**。

步骤 4 如果使用 FDM 管理 设备在设备上更改了单个 Talos 入侵规则，您将在**覆盖 (Overrides)** 窗格中看到这些规则。您可以通过点击**调整 (Tune)** 链接并选择覆盖操作来更改入侵规则的覆盖操作。此操作将应用于使用它的所有 Talos 入侵策略中的该规则。请注意，如果您选择恢复默认操作规则（**默认值**），则在环境触发入侵规则之前，您将无法再次调整该规则。

- 连接优先于安全
- 平衡安全和连接
- 安全优先于连接
- 最大检测数

为了在设备之间保持一致，覆盖操作将保存到与入侵覆盖策略关联的每个设备。

以下是覆盖操作的效果：

- **丢弃 (Drop)** - 当此规则与流量匹配时，此选择规则创建一个事件同时丢弃连接。使用此操作可加强某些规则的安全性。例如，当 Talos 规则匹配时，即使为访问控制规则指定了“连接优先于安全”策略，指定 Drop 也会提高安全性。
- **警报 (Alert)** - 当此规则与流量匹配时，此选择创建一个事件但不丢弃连接。“警报”的一个使用案例是流量被阻止，但客户希望允许，并在禁用规则之前查看警报。
- **已禁用 (Disabled)** - 此选项可防止流量与规则匹配。不生成事件。“禁用”的使用案例是停止报告中的误报，或删除不适用于您的环境的规则，例如，如果您不使用 httpd，则禁用 Apache httpd 规则。
- **默认 (Default)** - 此选项仅适用于 Talos 入侵策略级别中的规则默认操作。例如，当您将入侵规则恢复为“默认”时，这可能意味着其操作在“连接优先于安全”策略和“平衡安全性和连接”策略中的“阻止”。
- 使用以下选项编辑规则覆盖：
  - **覆盖所有设备 (Override for all devices)** - 此选项可为 CDO 管理的所有设备设置所需的操作。从下拉菜单中选择一个选项。如果规则对于不同的入侵覆盖策略具有不同的覆盖值，则默认情况下，下拉选项为“多个”(Multiple)。
  - **按设备编辑规则覆盖 (Edit rule overrides by device)** - 选中**高级选项 (Advanced Options)** 滑块，然后选择**按设备覆盖 (Overrides by Devices)** 选项卡。此选项显示为每个设备配置的规则操作，您可以通过选中受影响的设备，选择覆盖操作，然后点击**保存 (Save)** 来更改规则操作。

- **按策略编辑规则覆盖 (Edit rule overrides by policy)** - 选中**高级选项 (Advanced Options)** 滑块，然后选择**全部覆盖 (All Overrides)** 选项卡。仅当您的租户配置了多个 IPS 策略时，此部分才适用。您可以从此页面管理所有 IP 策略，包括与多个设备关联的策略。

步骤 5 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

创建签名覆盖

您只能为已在 FTD 设备上触发的 IPS 规则创建签名覆盖。在 CDO 中创建签名覆盖时，覆盖会自动将配置的操作（**丢弃**、**警报**、**禁用**、**默认**）应用于所有策略级别。

Procedure

步骤 1 在主导航栏中，点击**监控 (Monitoring)** > **威胁 (Threats)**。

步骤 2 从表中选择一个威胁并将其展开。在“调整操作”(Tune Actions) 窗格中，点击**调整 (Tune)**。

步骤 3 按照 Firepower 入侵策略签名覆盖程序的**步骤 4** 中的说明调整规则。

步骤 4 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

删除签名覆盖

Procedure

步骤 1 在主导航栏中，点击**策略 (Policies)** > **签名覆盖 (Signature Overrides)**。

步骤 2 点击覆盖的名称，以便展开右侧的详细信息面板。

步骤 3 展开覆盖窗格并选择要删除的覆盖，然后点击**调整 (Tune)**。

步骤 4 将默认操作设置为**默认 (Default)**。

步骤 5 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

自定义 Firepower 入侵防御系统策略

关于自定义 IPS 策略

随着版本 6.7 的推出，改进的 Snort 3 处理引擎允许您使用思科 Talos 情报组 (Talos) 提供的规则来创建和自定义入侵防御系统 (IPS) 策略。最佳实践是根据提供的 Talos 策略模板创建您自己的策略，并在需要调整规则操作时进行更改。

Note 目前，CDO 不支持自定义 IPS 规则。您可以使用 Talos 提供的规则创建和修改自定义 IPS 策略，但不能创建自己的 IPS 规则并将其应用于自定义 IPS 策略。

这些基本模板包含相同的入侵规则（也称为签名）列表，但针对每个规则所采取的操作有所不同。比如，某个规则可能在某个策略中启用，但在另一个策略中却被禁用。又比如，如果您发现某个特定规则为您提供的误报过多，在这种情况下该规则会阻止您不希望阻止的流量，可以禁用该规则而不必切换到安全性较低的入侵策略。也可将其更改为匹配警告，而不丢弃流量。

IPS 策略库模板

这些基本模板包含相同的入侵规则（也称为签名）列表，但针对每个规则所采取的操作有所不同。例如，一条规则在某个策略中可能处于启用状态，但在另一个策略中可能被禁用。有比如，如果您发现某个特定规则为您提供的误报过多，在这种情况下该规则会阻止您不希望阻止的流量，可以禁用该规则而不必切换到安全性较低的入侵策略。也可将其更改为匹配警告，而不丢弃流量。

提供的基本模板是根据您的网络可能需要的保护类型而建议采用的配置。在创建新策略时，您可以使用以下任何模板作为基础：

Caution 请勿修改启用了 Snort 3 的 FDM 管理设备随附的默认 IPS 策略。我们强烈建议根据以下模板来创建新的自定义 IPS 策略，并为新策略使用不同于下面列出的默认 IPS 策略名称的唯一名称。如果您需要对策略进行故障排除，思科 TAC 可以轻松找到自定义策略并恢复为默认策略；这样可以保护您的网络，而不会丢失您的自定义更改。

提供的基本模板是根据您的网络可能需要的保护类型而建议采用的配置。在创建新策略时，您可以使用以下任何模板作为基础：

- **最大检测 (Maximum Detection)** - 此类策略适用于网络基础设施安全比在“安全优先于连接”策略中还要重要、且有可能产生更大运行影响的网络。
- **安全优先于连接 (Security Over Connectivity)** - 这些策略专为网络基础设施安全优先于用户便利性的网络而构建。此入侵策略将启用许多可能会提醒或丢弃合法流量的网络异常入侵规则。
- **平衡安全和连接 (Balanced Security and Connectivity)** - 这些策略专为速度和检测而构建。共同使用时，这些策略充当大多数网络和部署类型的良好起点。
- **连接优先于安全 (Connectivity Over Security)** - 这些策略专为连接（即能够获取所有资源）优先于网络基础设施安全的网络而构建。仅会启用阻止流量的最重要规则。
- **无活动规则 (No Rules Active)** - 默认情况下禁用策略中包含的规则。

Tip **最大检测 (Maximum Detection)** 基础模板需要大量内存和 CPU 才能有效工作。CDO 建议使用此模板将 IPS 策略部署到 2100、4100 或虚拟设备等型号。

随着新的漏洞被发现，Talos 会发布入侵规则更新。这些规则更新可以修改任何思科提供的网络分析或入侵策略，并可提供自动应用于现有规则和策略设置的新的和更新的入侵规则和预处理器规则。规则更新还可能删除现有模板库中的规则，提供新的规则类别，以及修改默认变量集。

IPS 策略模式

默认情况下，所有入侵策略在**防御**模式下运行，以实施 IPS。在防御检测模式下，如果连接与实施流量丢弃操作的入侵规则匹配，则该连接会被主动阻止。

如果想要测试入侵策略对网络的影响，则可以更改为**检测**模式，从而实施入侵检测系统 (IDS) 。在此检测模式下，丢弃规则的处理方式类似于报警规则，在这种情况下，系统会通知您匹配的连接，但操作结果变为**将被阻止**，而事实上绝不会阻止连接。

IPS 规则组安全级别

CDO 允许您修改策略中包含的规则组的安全级别。请注意，此安全级别适用于规则组中的所有规则，而不是单个规则。

Note 对规则组的安全级别所做的更改将自动提交，并且无法恢复。您不必点击**保存 (Save)** 即可提交安全级别修改。您必须手动更改安全级别。

IPS 规则操作

随时修改规则组中单个规则或多个规则的操作。IPS 规则可以设置为以下选项：

- **禁用** - 不针对此规则匹配流量。不生成事件。
- **警报** - 当此规则与流量匹配时，创建一个事件但不丢弃连接。
- **丢弃** - 当此规则与流量匹配时，创建一个事件同时丢弃连接。

FDM 模板和自定义 IPS 策略

从启用了 Snort 3 的设备派生的模板只能应用于也启用了 Snort 3 的设备。由于 Snort 2 和 Snort 3 支持和处理的规则存在差异，配置了 Snort 3 的模板无法完全支持和保护配置了 Snort 2 的设备。有关详细信息，请参阅升级到 Snort 3.0。

如果您碰巧使用 ASA 迁移工具从 ASA 配置创建 FDM 模板，我们**强烈**建议不要配置或取消配置任何 IPS 策略。ASA 设备不支持 Snort 引擎，将 IPS 策略从 ASA 配置迁移到 FDM 管理设备配置可能会导致问题。如果您使用 ASA 迁移工具，我们建议在创建和部署模板后为设备创建自定义 IPS 策略。

有关模板的详细信息，请参阅 FDM 管理 设备模板。

规则集和自定义 IPS 策略

为 Snort 3 配置的设备尚不支持规则集。以下限制适用：

- 不能将规则集附加到支持 Snort 3 的设备。
- 您无法从已安装 Snort 3 的现有设备创建规则集。
- 不能将自定义 IPS 策略与规则集关联。

前提条件

您可以从**入侵策略 (Intrusion policies)** 页面查看可用的 IPS 策略，但如果不满足以下前提条件，则无法创建或修改自定义 IPS 策略：

设备支持

- Firepower 1000 系列
- Firepower 2100 系列
- Firepower 4100 系列
- 带有 AWS 的 威胁防御 virtual
- 带有 Azure 的 威胁防御 virtual

软件支持

s

设备**必须**至少运行版本 6.7 和 Snort 3。

如果您的设备运行的是 6.7 之前的版本，请升级设备。有关详细信息，请参阅升级单个 FTD 设备。

如果您的设备运行的是 Snort 2 版本 6.7，请注意，Snort 3.0 中可能不存在 Snort 2.0 中的某些入侵规则。有关详细信息，请参阅升级到 Snort 3.0。

Note 要了解设备正在运行的软件版本和 Snort 引擎，只需在**清单 (Inventory)** 页面上找到并选择设备，然后查看**设备详细信息 (Device Details)**

相关信息：

- 配置 Firepower 自定义 IPS 策略
- FDM 管理 访问控制规则中的自定义 IPS 策略

配置 Firepower 自定义 IPS 策略

在 CDO 中为 FTD 设备创建或修改自定义 IPS 策略之前，请务必阅读 自定义 Firepower 入侵防御系统策略。

目前，CDO 不支持自定义 IPS 规则。您可以使用 Talos 提供的规则创建和修改自定义 IPS 策略，但不能创建自己的 IPS 规则并将其应用于自定义 IPS 策略。

如果您在 CDO 中创建或编辑 IPS 策略时遇到问题，请参阅入侵防御系统故障排除, on page 693以了解详细信息。

Note 您无法删除自定义 IPS 策略的规则组中的规则或对其重新排序。

创建自定义 *IPS* 策略

按照以下程序使用 Talos 提供的 IPS 规则创建新的自定义 IPS 策略：

Procedure

步骤 1 在 CDO 导航窗格中，点击**策略 (Policies)**。

步骤 2 选择**入侵策略 (Intrusion Policies)**。

步骤 3 点击蓝色加号按钮  。

步骤 4 展开**基本模板 (Base Template)** 的下拉菜单。如果您的设备运行的是版本 7.2 和 Snort 3，则必须展开下拉列表，然后点击**选择 (Choose)** 以选择模板。如果设备运行的是版本 7.1.x 及更早版本，只需展开下拉菜单并选择以下选项之一即可。以下模板：

- **最大检测 (Maximum Detection)** - 此类策略适用于网络基础设施安全比在“安全优先于连接”策略中还要重要、且有可能产生更大运行影响的网络。

  Tip **最大检测 (Maximum Detection)** 基础模板需要大量内存和 CPU 才能有效工作。CDO 建议使用此模板将 IPS 策略部署到 2100、3100、4100 或 威胁防御 virtual 等型号。

- **安全优先于连接 (Security Over Connectivity)** - 这些策略专为网络基础设施安全优先于用户便利性的网络而构建。此入侵策略将启用许多可能会提醒或丢弃合法流量的网络异常入侵规则。
- **平衡安全和连接 (Balanced Security and Connectivity)** - 这些策略专为速度和检测而构建。共同使用时，这些策略充当大多数网络和部署类型的良好起点。
- **连接优先于安全 (Connectivity Over Security)** - 这些策略专为连接（即能够获取所有资源）优先于网络基础设施安全的网络而构建。仅会启用阻止流量的最重要规则。
- **无活动规则 (No Rules Active)** - 默认情况下禁用策略中包含的规则。

步骤 5 输入策略的**名称**。

我们**强烈**建议使用与默认基本模板不同的唯一名称。如果您需要对 IPS 策略进行故障排除，思科 TAC 可以轻松找到自定义策略并恢复为默认策略；这样可以保护您的网络，而不会丢失您的自定义更改。

步骤 6 （可选）输入策略**说明**。

步骤 7 选择 **IPS 模式 (IPS Mode)**。

- **防御 (Prevention)** - 如果连接与实施流量丢弃操作的入侵规则匹配，则该连接会被主动阻止。
- **检测 (Detection)** - 如果连接匹配其操作为丢弃流量的入侵规则，操作结果将变为**将被阻止 (Would Have Blocked)**，并且不执行任何操作。

步骤 8 点击**保存 (Save)**。

后续步骤

将 IPS 策略添加到 FDM 管理 设备访问控制规则。有关详细信息，请参阅 FDM 管理 访问控制规则中的自定义 IPS 策略。

编辑自定义 *IPS* 策略

如果您已载入具有 IPS 策略的 FDM 管理设备，如果您在 FDM 中创建了 IPS 策略并且 CDO 从已部署的配置中读取该策略，或者您刚刚创建了新的 IPS 策略，则可以编辑现有 IPS 策略。

使用以下程序修改现有自定义 IPS 策略：

Procedure

步骤 1 在 CDO 导航窗格中，点击**策略 (Policies)**。

步骤 2 选择**入侵策略 (Intrusion Policies)**。

步骤 3 确定要编辑的 IPS 策略。点击**编辑 (Edit)**。

步骤 4 从页面顶部，点击编辑图标  。

步骤 5 编辑以下所需的字段：

- 基本模板。
- 名称。
- 说明。
- IPS 模式。

步骤 6 点击**保存 (Save)**。

步骤 7 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

编辑自定义 *IPS* 策略中的规则组

您可以覆盖规则组中规则的默认操作。使用以下程序编辑规则组中包含的规则

Procedure

步骤 1 在 CDO 导航窗格中，点击策略。

步骤 2 选择**入侵策略 (Intrusion Policies)**。

步骤 3 确定要编辑的 IPS 策略。点击**编辑 (Edit)**。

步骤 4 从左侧的规则组选项卡中，展开所需的规则组。从展开的列表中选择组。

步骤 5 编辑规则组：

a) 通过选择安全级别栏来编辑整个规则组的安全级别。手动将安全级别拖至要应用于整个规则组的安全类型。点击**提交**

b) 通过展开位于右侧的规则下拉菜单，编辑单个规则的规则操作。

c) 通过选中所需规则的复选框并展开位于规则表上方的下拉菜单，编辑多个规则的规则操作。此选择会影响所有选定的规则。

d) 通过选中表的标题行中的复选框并展开位于规则表上方的下拉菜单，编辑所有规则的规则操作。此选择会影响规则组中的所有规则。

步骤 6 点击策略页面顶部的**保存 (Save)**。

步骤 7 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

删除自定义 *IPS* 策略

使用以下程序从 CDO 中删除自定义 IPS 策略：

Procedure

步骤 1 在 CDO 导航窗格中，点击**策略**。

步骤 2 选择**入侵策略 (Intrusion Policies)**。

步骤 3 确定要编辑的 IPS 策略。点击**删除**。

步骤 4 点击**确定 (OK)** 以删除策略。

步骤 5 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

安全情报策略

关于安全智能

通过安全智能策略能够根据源/目标 IP 地址或目标 URL 提前丢弃非必要流量。在使用访问控制策略评估列入受阻列表的流量前，系统会将其丢弃，从而减少系统资源的使用量。

您可以根据以下条件阻止流量：

- **思科 Talos 情报源 (Cisco Talos feeds)** - 思科 Talos 提供对定期更新的安全情报源的访问权限。具有安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的站点出现和消失的速度可能比您更新和部署自定义配置的速度要快。系统定期下载智能源更新，从而提供新的威胁智能，而无需重新部署配置。

Note 默认情况下，思科 Talos 情报源每小时更新一次。您可以更改更新频率，甚至可以根据需要更新源，方法是登录 Firepower 设备管理器并从主页导航：设备 (Device) > 更新 (Updates) > 查看配置 (View Configuration)。

- **网络和 URL 对象 (Network and URL objects)** - 如果您知道要阻止的特定 IP 地址或 URL，则可为其创建对象并将其添加到阻止列表或允许列表。

创建用于 IP 地址（网络）和 URL 的单独阻止和允许列表。

安全情报许可证要求

您必须在 FDM 管理 设备上启用 许可证才能使用安全智能。

有关详细信息，请参阅《适用于 Firepower 设备管理器的思科 FTD 配置指南》的“安全策略”一章的**安全情报源类别**部分。

配置 Firepower 安全情报策略

通过安全智能策略能够根据源/目标 IP 地址或目标 URL 提前丢弃非必要流量。所有允许的连接仍会通过访问控制策略进行评估，并且最终可能会被丢弃。您必须启用 许可证，才能使用安全智能。

配置 Firepower 安全情报策略

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择要为其创建或编辑安全情报策略的 FDM 管理 设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击 **策略**。

步骤 5 在 FDM 管理 设备策略页面中，点击策略栏中的 **安全情报** 。

步骤 6 如果策略未启用，请点击安全情报滑块将其启用，或点击关于安全情报信息框中的**启用 (Enable)** 。

Note 您可以通过点击安全情报开关切换到关闭随时禁用策略。配置将被保留，因此，当您再次启用该策略时，无需重新配置。

步骤 7 选择**阻止列表 (Blocked List)** 行。请注意，根据您的表视图，在“网络”、“网络对象”、“网络源”、“URL”、“URL 对象”和“URL 源”列中有加号 。

- 在**将网络添加到阻止列表 (Add Networks to Blocked List)** 对话框和**将 URL 对象添加到阻止列表 (Add URL Object to Blocked List)** 对话框中，可以搜索现有对象或根据需要创建对象。选中要阻止的对象，然后点击**选择 (Select)**。

  Note 安全智能会忽略使用 /0 掩码的 IP 地址块。这包括 any-ipv4 和 any-ipv6 网络对象。不得选择将这些对象用于网络阻止操作。

- 在**将 URL 对象添加到阻止列表 (Add URL Objects to Blocked List)** 和**将网络源添加到阻止列表 (Add Network Feeds to Blocked List)** 对话框中，选中要阻止的源，然后点击**选择 (Select)**。您可以通过点击源行末尾的向下箭头来阅读源的说明。如Firepower安全情报策略的安全情报源中所描述。

步骤 8 如果您知道在上一步中指定的任何网络组、网络源、URL 对象或 URL 源中包含要对其设置例外的网络、IP 地址或 URL，请点击**允许列表 (Allowed List)** 行。

步骤 9 为要设置例外的网络、IP 地址和 URL 选择或创建对象。当您点击**选择 (Select)** 或**添加 (Add)** 时，它们将被添加到“允许列表”(Allowed List) 行中。

步骤 10 （可选）要记录安全情报策略生成的事件，请执行以下操作：

a) 点击 日志记录设置 图标来配置日志记录。如果启用了日志记录，系统会记录与阻止列表条目匹配的任意项。系统不记录例外条目的匹配项，但如果被免除的连接与启用日志记录的访问控制规则匹配，您会收到日志消息。

b) 通过点击**连接事件日志记录 (Connection Events Logging)** 开关启用事件日志记录。

c) 选择发送事件的位置：

- 点击**无 (None)** 会将事件保存到 FDM 管理 设备。它们在 FDM 事件查看器中显示。FDM 管理 设备上的存储空间非常有限。最好通过定义系统日志服务器对象（而不是选择无）将连接事件存储在系统日志服务器上。
- 点击**创建 (Create)** 或**选择 (Choose)** 可创建或选择由系统日志服务器对象表示的系统日志服务器，以向其发送日志记录事件。由于设备中的事件存储受限，所以将事件发送至外部系统日志服务器可供长期存储，并增强您的事件分析。

如果您订用了思科安全分析和日志记录，请使用 为安全日志记录分析 (SaaS) 创建系统日志服务器对象，将事件发送到安全事件连接器。有关此功能的详细信息，请参阅FDM 管理 设备的安全日志记录分析。

步骤 11 （可选）对于您创建的任何规则，您可以选择它并在“添加注释”(Add Comments) 字段中添加注释。要了解有关规则注释的详细信息，请参阅向策略和规则集中的规则添加注释。

步骤 12 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

对 Firepower 安全情报策略阻止列表进行例外处理

对于在 配置 Firepower 安全情报策略中创建的每个阻止列表，您可以创建关联的允许列表。允许列表的唯一目的是豁免阻止出现在阻止列表中的IP地址或URL。也就是说，如果发现需使用且已知安

全的地址或 URL 位于在阻止列表上配置的智能源中，则可以将该地址或 URL 添加到允许列表中，使其免于访问。这样，您就不用为了一个地址或 URL 而从阻止列表中删除整个源。

通过安全情报策略后，允许的流量随后会由访问控制策略进行评估。有关允许或丢弃连接的最终决定基于连接匹配的访问控制规则。访问规则还会决定恶意软件检查是否应用于连接。

Firepower 安全情报策略的安全情报源

下表介绍了思科 Talos 源中的可用类别。可以在网络和 URL 阻止列表中输入这些类别。

类别	说明
攻击者	出站恶意活动已知的活动扫描工具和列入组织名单的主机
bogon	Bogon 网络和未分配的 IP 地址。
僵尸	托管二进制恶意软件丢弃程序的站点。
CnC	托管僵尸网络的命令和控制服务器的站点。
dga	用于生成作为与命令和控制服务器的交汇点的大量域名的恶意软件算法。
exploitkit	指定用于识别客户端中的软件漏洞的软件包。
恶意软件	托管恶意软件二进制或漏洞包的站点。
open_proxy	允许匿名 Web 浏览的开放代理。
open_relay	已知用于垃圾邮件的开放邮件中继。
网络钓鱼	托管网络钓鱼页面的站点。
效率低下	主动参与恶意或可疑活动的 IP 地址和 URL。
垃圾邮件	已知用于发送垃圾邮件的邮件主机。
可疑	看似可疑并具有类似于已知恶意软件的特征的文件。
tor_exit_node	Tor 出口节点。

FDM 托管设备身份策略

身份策略概述

使用身份策略从连接中收集用户身份信息。然后，可以在控制面板中基于用户身份查看使用情况，并根据用户或用户组配置访问控制。通过将网络行为、流量和事件直接与单个用户和组相关联，系统可帮助您确定策略违规、攻击或网络漏洞的来源。

例如，可以确定入侵事件所攻击的主机的所有人是谁，并确定是谁发起了内部攻击或端口扫描。此外，还可以确定高带宽用户，以及正在访问不良网站或应用的用户。

然后，您可以根据控制面板中的用户身份来查看使用情况，并根据 Active Directory (AD) 领域对象（与该AD上的所有用户匹配）、特殊身份（例如身份验证失败、访客、无需身份验证或未知身份）或用户组。

可以使用以下方法获取用户身份：

- 被动身份验证 - 对所有类型的连接，从其他身份验证服务获取用户身份而不提示输入用户名和密码。
- 主动身份验证 - 提示输入用户名和密码，并根据指定身份源进行身份验证，获取源 IP 地址的用户身份（仅限于 HTTP 连接）。

通过被动身份验证确定用户身份

被动身份验证在收集用户身份信息时不提示用户输入用户名和密码。系统会从您指定的身份源获取映射。

您可以从以下源被动获取用户到 IP 地址的映射：

- 远程访问 VPN 登录。被动身份支持以下用户类型：
  - 在外部验证服务器中定义的用户账户。
  - 在 FDM 管理设备中定义的本地用户账户。
- 思科身份服务引擎 (ISE)；思科身份服务引擎被动身份连接器 (ISE-PIC)。

如果给定用户是通过多个源所识别，则远程访问 VPN 登录身份占优先地位。

通过主动身份验证确定用户身份

身份验证是确认用户身份的行为。

如果 HTTP 流量来自系统没有其用户身份映射的 IP 地址，通过主动身份验证，您可以决定是否针对为系统配置的目录对发起该流量的用户进行身份验证。如果身份验证成功，该 IP 地址则被视为具有该通过身份验证的用户的身份。

如身份验证不成功，用户对网络的访问并不会受阻。为这些用户提供哪些访问权限最终由访问规则决定。

处理未知用户

当您使用 FDM 管理为身份策略配置目录服务器后，FDM 管理会从目录服务器下载用户和组成员信息。Active Directory 信息每 24 小时在午夜刷新一次，或在每次您编辑和保存目录配置时刷新（即使您未进行任何更改）。

如果某用户在活动身份验证身份规则提示时成功进行了身份验证，但该用户的名称不在下载的用户身份信息中，则该用户会被标记为“未知”。您不会在与身份相关的控制面板中看到该用户的 ID，该用户也不会匹配组规则。

但是，系统将应用面向未知用户的任何访问控制规则。例如，如果您阻止未知用户的连接，那么即使这些用户成功进行了身份验证（即目录服务器可识别用户并且密码有效），他们也会被阻止。

因此，当您对目录服务器进行更改（例如添加或删除用户，或更改组成员身份）时，直到系统从目录下载更新之后这些更改才会反映在策略实施中。

如果您不希望每天都等到午夜进行更新，可以通过编辑目录领域信息（登录到FDM管理设备并导航至“对象”(Objects)>“身份源”(Identity Sources)，然后编辑领域）。点击**确定 (OK)**，然后部署更改。系统随即会下载更新。

Note 您可以登录 FDM 管理设备并导航至**策略 (Policies) > 访问控制 (Access Control)**，点击**添加规则 (Add Rule)** (+) 按钮，并在“用户”(Users) 选项卡上查看用户列表，从而检查 FDM 管理 系统上是否有新的或已删除的用户信息。如果找不到新用户，或者还是可以找到已删除的用户，则系统的信息未更新。

如何实施 Firepower 身份策略

如果要使用 Cisco Defense Orchestrator (CDO) 管理 FDM 管理 设备的身份策略，则需要先创建身份源。您可以使用 Defense Orchestrator 配置其余设置。

正确配置后，您将能够看到FDM中监控控制面板和事件中的用户名。您还将能够在访问控制和SSL解密规则中使用用户身份作为流量匹配条件。

Note 目前，CDO 无法配置实施身份策略所需的某些组件，例如远程接入 VPN 和思科身份服务引擎。这些组件必须在 FDM（设备的本地管理器）中进行配置。以下程序中的某些步骤表明，您必须使用 FDM 配置某些身份组件以实施身份策略。

操作步骤

以下过程概述您必须配置哪些内容才能正常使用身份策略：

Procedure

步骤 1 创建 AD 身份领域。不论您是主动使用用户身份，还是被动使用，都需要配置包含用户身份信息的 Active Directory (AD) 服务器。有关详细信息，请参阅创建 FTD Active Directory 领域对象。

步骤 2 如果您想要使用被动身份验证身份规则，请**使用 FDM** 来配置被动身份源。

根据您要在设备中实现的服务和网络中可用的服务，您可以配置任何以下内容。

- 远程访问 VPN - 如果您要支持到设备的远程访问 VPN 连接，用户登录可以提供基于 AD 服务器或本地用户（FDM 管理 设备中定义的用户）的身份。有关配置远程访问 VPN 的详细信息，请参阅适用于您的设备的版本的《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》中的“配置远程访问 VPN”一章。

- 思科身份服务引擎 (ISE) 或思科身份服务引擎被动身份连接器 (ISE PIC) - 如果您使用这些产品，您可以将设备配置为 pxGrid 订阅方，并从 ISE 获取用户身份。有关说明，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》的“配置身份服务引擎”一章。

步骤 3 **使用 防御协调器**，启用身份策略并配置被动或主动身份验证。有关详细信息，请参阅配置身份策略设置。

步骤 4 **使用 防御协调器**，配置 Firepower 身份策略默认操作。如果您打算仅使用被动身份验证，您可以将默认操作设置为被动身份验证，无需创建特定规则。

步骤 5 **使用 防御协调器**，配置身份规则。创建将从相关网络收集被动或主动用户身份的规则。

步骤 6 （可选）对于您创建的任何规则，您可以选择它并在“添加注释”(Add Comments) 字段中添加注释。要了解有关规则注释的详细信息，请参阅向策略和规则集中的规则添加注释。

步骤 7 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

配置身份策略

您可以使用身份策略从连接中收集用户身份信息。然后，可以在FDM控制面板中基于用户身份查看使用情况，并根据用户或用户组配置访问控制。

下文概述了如何配置通过身份策略获取用户身份所需的元素：

操作步骤

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，选择要为其配置身份策略的设备，然后点击右侧**管理 (Management)** 窗格中的 **策略 (Policy)**。

步骤 4 点击策略栏中的**身份 (Identity)**。

步骤 5 如果尚未启用身份策略，请参阅被动和主动身份验证，然后点击**启用 (Enable)**。您正在启用身份策略，而不是被动身份验证策略或主动身份验证策略。策略中的规则将指定主动或被动身份验证。

步骤 6 管理身份策略：

在配置身份设置后，此页面将按顺序列出所有规则。规则依据流量按照从上到下的顺序进行匹配，由第一个匹配项确定要应用的操作。从此页面中可以执行以下操作：

- **要启用或禁用身份策略**，请点击身份策略开关。有关详细信息，请参阅配置身份策略设置。
- **要读取被动身份验证设置**，请点击身份栏上**被动身份验证 (Passive Auth)** 标签旁边的按钮。有关详细信息，请参阅配置身份策略设置。
- **要启用主动身份验证**，请点击身份栏上**主动身份验证 (Active Auth)** 标签旁边的按钮。有关详细信息，请参阅配置身份策略设置。

- **要更改默认操作**，请点击默认操作按钮并选择所需的操作。请参阅配置 Firepower 身份策略默认操作。
- **要移动表中的规则**，请选择该规则，然后点击规则表中该规则行末尾的向上或向下箭头。
- **要移动表中的规则**，请选择该规则，然后点击规则表中该规则行末尾的向上或向下箭头。
- **要配置规则**，请执行以下操作：
  - 要创建新规则，请点击加号  按钮。
  - 要编辑现有规则，请选择该规则，然后点击操作窗格中的**编辑 (Edit)**。也可以选择在表中点击某规则属性来编辑该属性。
  - 要删除不再需要的规则，请选择该规则，然后在“操作”窗格中点击**删除 (Remove)**。

有关创建和编辑身份策略的更多信息，请参阅 配置身份规则。

步骤 7 （可选）对于您创建的任何规则，您可以选择它并在“添加注释”(Add Comments) 字段中添加注释。要了解有关规则注释的详细信息，请参阅向策略和规则集中的规则添加注释。

步骤 8 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

配置身份策略设置

要正常使用身份策略，必须配置提供用户身份信息的源。必须配置的设置因配置的规则类型而异，而规则类型可以是被动和/或主动的。

Note 目前，CDO 无法配置实施身份策略所需的某些组件，例如 Active Directory 身份领域、远程访问 VPN 和思科身份服务引擎。这些组件必须在 FDM 中配置，FDM 是 FTD 设备的本地管理器。以下程序中的某些步骤表明，您必须使用 FDM 配置某些身份组件以实施身份策略。

操作步骤

Before you begin

确保目录服务器、FDM 管理设备和客户端之间的时间设置一致。这些设备间的时间偏差可能会导致用户身份验证操作失败。“一致”说明您可以使用不同的时区，但时间相对于这些时区应是相同的；例如，10 AM PST = 1 PM EST。

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，选择要为其配置身份策略的设备，然后点击右侧**管理 (Management)** 窗格中的 **策略 (Policy)**。

步骤 4 通过点击身份切换**启用身份策略** 。或者，您可以点击 按钮，查看被动和主动身份验证的说明，然后点击对话框中的**启用 (Enable)**。

步骤 5 读取**被动身份验证**设置。点击身份栏上的**被动身份验证 (Passive Auth)** 按钮。

如果您已使用 Firepower 设备管理器配置远程访问 VPN 或思科身份服务引擎，则被动身份验证按钮显示**已启用 (Enabled)**。

必须配置至少一个被动身份源，才能创建被动身份验证规则。

步骤 6 **配置主动身份验证**。如果身份规则要求对用户进行主动身份验证，则该用户将重定向到连接该用户所通过的界面上的强制网络门户，然后系统会提示用户进行身份验证。

a) 点击身份栏上的**主动身份验证 (Active Auth)** 按钮。

b) 如果尚未启用 SSL 说明，请点击**启用 (Enable)** 链接。如果您没有看到“启用”链接，请跳至步骤 "c"。

1. 从**选择解密重签名证书 (Select Decrypt Re-Sign Certificate)** 菜单，选择内部 CA 证书，以用于使用重签名证书实施解密的规则。

   您可以使用预定义的 **NGFW-Default-InternalCA** 证书，或者点击菜单并选择创建或选择以创建新证书，或者选择已上传到 FDM 管理 设备的证书。

   如果尚未在客户端浏览器中安装证书，请点击下载按钮 获取副本。有关如何安装证书的信息，请参阅各浏览器文档。另请参阅为解密重签名规则下载 CA 证书。

   Note 只有在未配置 SSL 解密策略的情况下，系统才会提示您进行 SSL 解密设置。要在启用身份策略之后更改这些设置，请编辑 SSL 解密策略设置。

2. 点击**保存 (Save)**。

c) 点击**服务器证书 (Server Certificate)** 菜单以选择在主动身份验证期间提供给用户的内部证书。如果尚未创建所需的证书，请点击**创建 (Create)**。如果用户不上传其浏览器已经信任的证书，则必须接受该证书。

d) 在**端口 (Port)** 字段中，输入适用于强制网络门户的端口号。默认端口是 885 (TCP)。如果配置了其他端口，则该端口必须在 1025-65535 的范围内。

Note 对于 HTTP Basic、HTTP Response Page 和 NTLM 身份验证方法，通过接口的 IP 地址可将用户重定向到强制网络门户。但对于 HTTP 协商，用户将使用完全限定 DNS 名称 firewall-hostname.AD-domain-name 进行重定向。如果想要使用 HTTP Negotiate，还必须更新 DNS 服务器以将此名称映射到您需要进行主动身份验证的所有内部接口的 IP 地址。否则，将无法进行重定向，用户也无法进行身份验证。

e) 点击**保存 (Save)**。

步骤 7 继续 配置 Firepower 身份策略默认操作。

配置 Firepower 身份策略默认操作

身份策略会对不匹配任何身份规则的连接实施默认操作。

实际上，不设置规则是策略的有效配置。如果想在所有流量源上使用被动身份验证，只需将被动身份验证配置为默认操作。

操作步骤

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，选择要为其配置身份策略的设备，然后点击右侧**管理 (Management)** 窗格中的 **策略 (Policy)**。

步骤 4 点击策略栏中的**身份 (Identity)**。

步骤 5 如果尚未配置身份策略设置，请配置身份策略设置。

步骤 6 在屏幕底部，点击“默认操作”(Default Action) 按钮，并从以下选项中选择一个：

- **被动身份验证 (Passive Auth)** - 对与任何身份规则都不匹配的连接，将使用所有已配置的被动身份源来确定用户身份。如果不配置任何被动身份源，使用被动身份验证作为默认选择等同于使用“无身份验证”。
- **无身份验证 (No Auth)** - 对与任何身份规则都不匹配的连接，不会确定用户身份。

步骤 7 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

配置身份规则

身份规则确定是否应收集用户身份信息以匹配流量。如果您不想收集用户身份信息以匹配流量，则可以配置“无身份验证”。

请记住，无论规则配置如何，都仅对 HTTP 流量进行主动身份验证。因此，无需创建规则将非 HTTP 流量从主动身份验证中排除。如果您希望获取所有 HTTP 流量的用户身份信息，只需将主动身份验证规则应用于所有源和目的。

Note 而且请记住，身份验证失败对网络访问没有影响。身份策略仅收集用户身份信息。如果要阻止无法进行身份验证的用户访问网络，则必须使用访问规则。

操作步骤

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，选择要为其配置身份策略的设备，然后点击右侧**管理 (Management)** 窗格中的 **策略 (Policy)**。

步骤 4 点击策略栏中的**身份 (Identity)**。

步骤 5 执行以下任一操作：

- 要创建新规则，请点击加号  按钮。要了解身份源对象及其对规则的影响，请参阅为 FDM 管理 设备配置身份源以了解详细信息。
- 要编辑现有规则，请点击要编辑的规则，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。
- 要删除不再需要的规则，请点击要删除的规则，然后在右侧“操作”窗格中点击**删除 (Remove)**。

步骤 6 在**顺序**中，选择要将该规则插入在已排序有序规则列表插入该规则的位置。

先匹配的规则先应用，所以您必须确保流量匹配条件标准较具体的规则显示在次之用来匹配流量的较通用条件标准的策略上方。

默认将规则添加到列表的末尾。如果以后要更改规则的位置，请编辑此选项。

步骤 7 在**名称 (Name)** 中输入规则的名称。

步骤 8 选择 FDM 管理 设备应对匹配项应用的**操作**，如有必要，还可以选择 Active Directory (AD) 身份源。

您必须选择包括用于被动和主动身份验证规则的用户账户的 AD 身份领域。选择以下之一：

- **被动身份验证** - 使用被动身份验证确定用户身份。系统将会显示所有已配置的身份源。此规则会自动使用所有已配置的源。
- **主动身份验证 (Active Auth)**使用主动身份验证确定用户身份。主动身份验证仅适用于 HTTP 流量。如果任何其他类型的流量与要求或允许主动身份验证的身份策略匹配，则不会尝试进行主动身份验证。
- **无身份验证** - 不获取用户身份。基于身份的访问规则不会应用于此流量。这些用户将标记为无需身份验证。

Note 对于**被动身份验证 (Passive Auth)** 和**主动身份验证 (Active Auth)**，您可以选择 AD 领域身份源。如果您没有准备好任何身份源对象，请点击**新建对象 (Create new object)** 以启动身份源对象向导。有关详细信息，请参阅创建或编辑 Active Directory 领域对象。

步骤 9 （仅主动身份验证。）点击**主动身份验证 (Active authentication)** 选项卡，然后选择您的目录服务器支持的身份验证方法（类型）。

- **HTTP 基本身份验证 (HTTP Basic)** - 使用未加密的 HTTP 基本身份验证连接对用户进行身份验证。用户通过其浏览器的默认身份验证弹出窗口登录网络。这是默认值。
- **NTLM** - 使用 NT LAN Manager (NTLM) 连接对用户进行身份验证。仅当选择了一个 AD 领域时，此选项才可用。用户使用其浏览器的默认身份验证弹出窗口登录网络，不过您可以将 Internet Explorer 和 Firefox 浏览器配置为使用其 Windows 登录域信息以透明方式进行身份验证。该任务在 FDM 中完成，有关说明，请参阅适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南 > 安全策略 > 身份策略 > **启用透明用户身份验证**。
- **HTTP 协商** - 允许设备协商用于用户代理（用户发起流量流所用的应用）和 Active Directory 服务器之间的方法。协商有助于使用广受支持的最强方法，顺序为先 NTLM，然后是 Basic 方法。用户通过其浏览器的默认身份验证弹出窗口登录网络。
- **HTTP 响应页面 (HTTP Response Page)**提示用户使用系统提供的网页进行身份验证。这是一种 HTTP Basic 身份验证方法。

Note 对于 HTTP Basic、HTTP Response Page 和 NTLM 身份验证方法，通过接口的 IP 地址可将用户重定向到强制网络门户。但对于 HTTP 协商，用户将使用完全限定 DNS 名称 *firewall-hostname.AD-domain-name* 进行重定向。如果想要使用 HTTP Negotiate，还必须更新 DNS 服务器以将此名称映射到您需要进行主动身份验证的所有内部接口的 IP 地址。否则，将无法进行重定向，用户也无法进行身份验证。

步骤 10 （仅主动身份验证。）选择**以访客身份回退 (Fall Back as Guest) > 开/关 (On/Off)**，确定是否将未通过主动身份验证的用户标记为访客用户。

用户有三次机会成功进行身份验证。如果仍不成功，选择此选项可以确定是否标记用户。您可以根据这些值部署访问规则。

- 以访客身份回退 (Fall Back as Guest) > **开 (On)** - 系统将用户标记为“访客”(Guest)。
- 以访客身份回退 (Fall Back as Guest) > **关 (Off)** - 用户标记为“访客”(Guest)。

步骤 11 在**源 (Source)** 和**目标 (Destination)** 选项卡上为被动身份验证、主动身份验证或无身份验证规则操作定义流量匹配条件。

请记住，仅在使用 HTTP 流量时才会尝试进行主动身份验证。因此，无需为非 HTTP 流量配置无身份验证规则，也无需为任何非 HTTP 流量创建主动身份验证规则。但是，被动身份验证适用于任何类型的流量。

身份规则的源/目标条件定义了流量通过的安全区（接口）、IP 地址或该 IP 地址所在的国家/地区或大洲（地理位置）或是流量中所用的协议和端口。默认设置为任何区域、地址、地理位置、协议和端口。

要修改条件，请点击该条件内的  按钮，选择所需的对象或元素，然后在弹出对话框中点击“确定”(OK)。如果条件需要对象，而所需的对象不存在，您可以点击**创建新对象 (Create New Object)**。

要从条件中删除对象，请将鼠标悬停在对象上，然后点击 X。

可以配置以下流量匹配条件。

源区域、目标区域

安全区对象，定义通过其传递流量的接口。可以定义一个或两个条件，也可以不定义任何条件：未指定的任何条件都将应用到任何接口上的流量。

- 要匹配从区域中的接口离开设备的流量，请将该区域添加至目标区域。
- 要匹配从区域中的接口进入设备的流量，请将该区域添加至源区域。
- 如果同时向一条规则添加源区域和目标区域条件，匹配流量必须源自其中一个指定源区域并通过其中一个目标区域流出。

如果应基于流量进入或离开设备的位置来应用规则，请使用此条件。例如，如果要确保从源自内部网络的所有流量收集用户身份，请选择内部区域作为源区域，同时将目标区域留空。

Note 不能在同一规则中搭配使用被动和路由安全区域。此外，被动安全区域只能被指定为源区域，不能作为目标区域。

源网络、目标网络

定义流量的网络地址或位置的网络对象或地理位置。

- 要匹配来自某个 IP 地址或地理位置的流量，请配置源网络。
- 要匹配流向 IP 地址或地理位置的流量，请配置目标网络。
- 如果同时向一条规则添加源网络条件和目标网络条件，匹配流量必须源自其中一个指定 IP 地址并流向其中一个目标 IP 地址。

添加此条件时，可从以下选项卡中进行选择：

- **网络 (Network)** - 为您要控制的流量选择定义源或目标 IP 地址的网络对象或组。
- **国家/地区/大洲 (Country/Continent)** - 选择要基于流量的源或目的国家/地区或大洲控制流量的地理位置。选择大洲将会选择该大洲内的所有国家/地区。除了直接在规则中选择地理位置外，也可以选择您创建的地理位置对象来定义位置。使用地理位置，可以便捷地限制对特定国家/地区的访问，而不需要知道此位置所用的全部潜在 IP 地址。
- **自定义地理位置 (Custom Geolocation)** - 选择（或创建）具有您指定的国家/地区和大洲的地理位置对象。

Note 为了确保使用最新地理位置数据过滤流量，思科强烈建议您定期更新地理位置数据库 (GeoDB)。有关详细信息，请参阅创建和编辑 Firepower 地理位置过滤器对象。

源端口、目标端口/协议

定义流量中所用协议的端口对象。对于 TCP/UDP，这可能包括端口。

- 要匹配来自协议或端口的流量，请配置源端口。源端口只能为 TCP/UDP。
- 要匹配流向协议或端口的流量，请配置目标端口/协议。
- 要同时匹配来自特定 TCP/UDP 端口的流量和流向特定 TCP/UDP 端口的流量，请配置源端口和目标端口。如果同时将源和目标端口添加至条件，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，您可以匹配从端口 TCP/80 流至端口 TCP/8080 的流量。

步骤 12 点击**保存 (Save)**。

步骤 13 返回**清单 (Inventory)** 页面。

步骤 14 选择已将这些规则添加到身份策略的设备。

步骤 15 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

SSL 解密策略

某些协议（如 HTTPS）使用安全套接字层 (SSL) 或其后续版本传输层安全性 (TLS) 来加密流量以进行安全传输。由于系统无法检查加密连接，因此，如果要应用可考虑借助更高层流量特性进行访问决策的访问规则，则必须应用 SSL 解密策略将其解密。

Caution 请记住，解密并重新加密流量会增加设备的处理负载，从而降低整体系统性能。

继续讨论以下主题：

- 关于 SSL 解密
- 如何实施和维护 SSL 解密策略
- 配置 SSL 解密策略
- 为已知密钥和重签解密配置证书
- 为解密重签名规则下载 CA 证书
- SSL 解密问题故障排除

如何实施和维护 SSL 解密策略

您可以使用 SSL 解密策略将加密流量转换为纯文本流量，以便可应用 URL 过滤、入侵和恶意软件控制以及其他需要深度数据包检测的服务。如果策略允许流量通过，则流量在离开设备前会被重新加密。

SSL 解密策略仅适用于加密流量。系统不会根据 SSL 解密规则评估未加密连接。

与其他一些安全策略不同的是，您需要监控并积极维护 SSL 解密策略，这是因为目标服务器上的证书可能会过期甚至发生变更。此外，客户端软件的变更可能会改变解密某些连接的能力，这是因为解密重签名操作无法与中间人攻击区分开来。

以下程序介绍了实施和维护 SSL 解密策略的端到端流程。

操作步骤

Procedure

步骤 1 如果要实施解密重签名规则，请创建所需的内部 CA 证书。

必须使用内部证书颁发机构(CA)证书。您有以下选择：由于用户必须信任证书，因此应上传客户端浏览器已配置为可信任的证书，或确保所上传的证书已添加到浏览器信任存储区。

- 创建由设备自身签署的自签名内部 CA 证书。请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》> 可重用对象 > 证书 > 生成自签名内部和内部 CA 证书。
- 上传由外部受信任 CA 或组织内部 CA 签署的内部 CA 证书和密钥。请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》> 可重用对象 > 证书 > 上传内部和内部 CA 证书。

步骤 2 如果要实施解密已知密钥规则，请从各内部服务器收集证书和密钥。

只可将解密已知密钥用于您所控制的服务器，这是因为必须从服务器中获取证书和密钥。上传这些证书和密钥，作为内部证书（而不是内部 CA 证书）。请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》> 可重用对象 > 证书 > 上传内部和内部 CA 证书。

步骤 3 配置 SSL 解密策略。

启用该策略时，还需要配置一些基本设置。

步骤 4 配置默认 SSL 解密操作

如有疑问，请选择不解密作为默认操作。在适当的情况下，访问控制策略仍然可以丢弃与默认 SSL 解密规则匹配的流量。

步骤 5 配置 SSL 解密规则。

标识要解密的流量以及要应用的解密类型。

步骤 6 如要配置已知密钥解密，请编辑 SSL 解密策略设置，以加入这些证书。请参阅为已知密钥和重签解密配置证书。

步骤 7 如有需要，下载用于解密重签名规则的 CA 证书并将其上传到客户端工作站上的浏览器。

有关下载证书并将其分发给客户端的信息，请参阅为解密重签名规则下载 CA 证书。

步骤 8 定期更新重新签名已知密钥证书。

- 重签名证书 - 在证书过期之前更新此证书。如果通过 Firepower 设备管理器生成证书，则有效期为 5 年。要确定证书何时到期，请从“对象”(Objects) 页面点击证书的查看图标。
- 已知密钥证书 - 对于任何已知密钥解密规则，需要确保已上传目标服务器的当前证书和密钥。只要所支持的服务器上的证书和密钥发生更改，就必须上传新的证书和密钥（作为内部证书）并更新 SSL 解密设置，以使用新证书。

步骤 9 上传外部服务器缺失的受信任 CA 证书。

系统包含各种由第三方颁发的受信任根证书和中间证书。为解密重签名规则协商 FDM 管理 设备和目标服务器之间的连接时，需要这些证书。

将根 CA 的信任链链中的所有证书都上传到受信任 CA 证书列表中，包括根 CA 证书和所有中间 CA 证书。否则，更难以检测由中间 CA 颁发的受信任证书。在“对象”(Objects)>“证书”(Certificates)页面上上传证书。请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》> 可重用对象 > 证书 > 上传受信任的 CA 证书。

关于 SSL 解密

通常情况下，访问控制策略会确定是允许还是阻止网络连接。但是，如果启用 SSL 解密策略，则连接将首先被发送至 SSL 解密策略，以确定应将其解密还是阻止。然后，访问控制策略评估任何未被阻止的连接（无论是否解密），作出最终的允许/阻止决策。

Note 您必须启用 SSL 解密策略，才能在身份策略中实施有效的身份验证规则。如果您启用 SSL 解密来启用身份策略，但不想另外实施 SSL 解密，请在“SSL 解密”(SSL Decryption) 页面中选择“不解密”(Do Not Decrypt) 作为默认操作，并且不要创建其他 SSL 解密规则。身份策略会自动生成所需的任何规则。

以下主题更详细地介绍了加密流量管理和解密。

- 为什么要实施 SSL 解密？
- 自动生成的 SSL 解密规则
- 处理不可解密流量

为什么要实施 SSL 解密？

无法检查 HTTPS 连接等加密流量。许多连接均是合法加密的连接，比如与银行和其他金融机构的连接。许多网站使用加密保护隐私或敏感数据。例如，加密与 Firepower 设备管理器的连接。但是，用户也可能会隐藏加密连接中的不良流量。

通过实施 SSL 解密，可解密和检查连接，确保不含威胁或其他不良流量，然后重新加密后再允许继续连接。（解密流量通过访问控制策略，并根据检查的加密连接特征而不是加密特征匹配规则。）这平衡了应用访问控制策略的需求与用户保护敏感信息的需求。

还可以配置 SSL 解密规则，阻止明确不想要允许其进入网络的加密流量类型。

Caution 请记住，解密并重新加密流量会增加设备的处理负载，从而降低整体系统性能。

可应用于加密流量的操作

配置 SSL 解密规则时，可应用以下主题中所述的操作。这些操作也可用于默认操作（适用于与显示规则不匹配的任何流量）。

- 解密重签名
- 解密已知密钥
- 不解密
- 阻止

Note 通过 SSL 解密策略的任何流量均必须通过访问控制策略。除了 SSL 解密策略中丢弃的流量外，最终的允许或丢弃决定还取决于访问控制策略。

解密重签名

如果选择解密或重签流量，系统将扮演中间人的角色。

例如，用户在浏览器中键入 https://www.cisco.com。流量到达 FTD 设备，然后设备使用规则中指定的 CA 证书与用户进行协商，并在用户和 FTD 设备之间建立 SSL 隧道。同时，设备连接至 https://www.cisco.com，并在服务器和 FTD 设备之间建立 SSL 隧道。

因此，用户将看到配置用于 SSL 解密规则的 CA 证书，而不是来自 www.cisco.com 的证书。用户必须信任该证书才能完成连接。FTD 设备随后对用户和目标服务器之间的流量执行双向解密/重新加密。

Note 如果客户端不信任用于对服务器证书重新签名的CA，则会警告用户不应信任该证书。为了避免此情况，请将 CA 证书导入到客户端信任的 CA 库。或者，如果组织拥有专用 PKI，则可以颁发由根 CA（自动受组织中的所有客户端信任）签名的中级 CA 证书，然后将该 CA 证书上传到设备。

如果配置具有“解密重签名”(Decrypt Re-Sign) 操作的规则，则除任何已配置的规则条件外，该规则会根据所引用的内部 CA 证书的签名算法类型来匹配流量。由于您可以选择用于 SSL 解密策略的单个重签名证书，因此可以限制匹配重签规则的流量。

例如，仅当重签名证书是基于 EC 的 CA 证书时，使用椭圆曲线 (EC) 算法加密的出站流量才能匹配解密重签名规则。同样，仅当全局重签名证书为 RSA 时，使用 RSA 算法加密的流量才可与解密重签名规则匹配；即使所有其他配置的规则条件匹配，使用 EC 算法加密的出站流量也与规则不匹配。

解密已知密钥

如果您拥有目标服务器，则可使用已知密钥实现解密。在这种情况下，用户打开https://www.cisco.com的连接后，用户会看到 www.cisco.com 的实际证书，即使出示证书的是 FTD 设备。

您的组织必须是域和证书的所有者。以 cisco.com 为例，让最终用户查看思科证书的唯一可能方式是，您实际拥有域 cisco.com（即您是思科系统公司）并拥有由公共 CA 签名的 cisco.com 证书。您仅可使用已知密钥对您的组织拥有的站点进行解密。

使用已知密钥进行解密的主要目的是对通往 HTTPS 服务器的流量进行解密，以保护服务器免受外部攻击。如要检查流向外部 HTTPS 站点的客户端流量，由于您不是服务器所有者，所以必须使用解密重签名。

Note 要使用已知密钥解密，必须将服务器证书和密钥上传为内部身份证书，再在 SSL 解密策略设置中将其添加至已知密钥证书。然后，可部署已知密钥解密规则，其中服务器地址为目标地址。有关将证书添加到 SSL 解密策略的信息，请参阅配置 SSL 解密策略。

不解密

如果选择绕行某些类型的流量的解密，则不会对流量进行任何处理。系统会使加密流量继续进入访问控制策略，根据流量所匹配的访问控制规则对其执行允许或丢弃操作。

阻止

您可以简单地阻止匹配 SSL 解密规则的加密流量。阻止 SSL 解密策略可防止连接到访问控制策略。

阻止 HTTPS 连接后，用户看不到系统默认阻止响应页面。相反，用户会看到浏览器显示安全连接故障的默认页面。错误消息不会指明该站点由于策略而被阻止。相反，错误可能显示为没有通用的加密算法。据此消息，无法明确看出是您有意阻止了该连接。

自动生成的 SSL 解密规则

无论您是否启用 SSL 解密策略，FDM 管理 设备都会自动为实施主动身份验证的各身份策略规则生成解密重签名规则。这是为 HTTPS 连接启用主动身份验证的必然要求。

启用 SSL 解密策略后，您可以在“身份策略主动身份验证规则”标题下看到这些规则。这些规则归入 SSL 解密策略顶部。这些规则为只读格式。仅可通过更改身份策略进行更改

处理不可解密流量

有几个特点使得连接不可解密。如果连接具有以下任何特征，则默认操作将应用于该连接，而不管该连接本可能会与哪个规则匹配。如果将“阻止”选作默认操作（而不是“不解密”），则可能会出问题，包括过度丢弃合法流量的问题。

- 压缩会话 - 数据压缩应用于连接。
- SSLv2 会话 - 支持的最低 SSL 版本是 SSLv3。
- 未知密码套件 - 系统无法识别连接的密码套件。
- 不受支持的密码套件 - 系统不支持根据检测到的密码套件进行解密。
- 会话未缓存 - SSL 会话已启用会话重复使用，客户端和服务器使用会话标识符重新建立了该会话，并且系统未缓存该会话标识符。
- 握手错误 - SSL 握手协商期间出错。
- 解密错误 - 解密操作期间出错。
- 被动接口流量 - 被动接口（被动安全区）上的所有流量均无法解密。

SSL 解密策略的许可证要求

使用 SSL 解密策略无需特殊许可证。

但需要 URL 许可证创建将 URL 类别和信誉作为匹配标准的规则。有关配置许可的详细信息，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》> 许可系统 > 启用或禁用可选许可证。

SSL 解密准则

配置和监控 SSL 解密策略时，请注意以下事项：

- 对于与设置为信任或阻止的访问控制规则匹配的任何连接，如果这些规则满足以下条件，则绕过 SSL 解密策略：
  - 将安全区、网络、地理位置和端口仅用作流量匹配条件。
  - 排在任何要求检测的其他规则之前，例如，基于应用或URL匹配连接的规则，或允许应用入侵或文件检测的规则。
- 使用URL类别匹配时，请注意，有时候站点登录页的类别与站点本身的类别不同。例如，Gmail 的类别是“基于网页的邮件”，而登录页的类别是“互联网门户网站”。要对到这些站点的连接解密，必须在规则中添加这两个类别。
- 如果您有任何主动身份验证规则，将无法禁用 SSL 解密策略。要禁用 SSL 解密策略，您必须禁用身份策略，或者删除任何使用主动身份验证的身份规则。

配置 SSL 解密策略

您可以使用 SSL 解密策略将加密流量转换为纯文本流量，以便可应用 URL 过滤、入侵和恶意软件控制以及其他需要深度数据包检测的服务。如果策略允许流量通过，则流量在离开设备前会被重新加密。

SSL 解密策略仅适用于加密流量。系统不会根据 SSL 解密规则评估未加密连接。

Caution 请记住，解密并重新加密流量会增加设备的处理负载，从而降低整体系统性能。

Note VPN 隧道在 SSL 解密策略评估之前已解密，因此该策略永远不适用于隧道本身。但是，隧道内的任何加密连接都要通过 SSL 解密策略进行评估。

以下程序介绍了如何配置 SSL 解密策略。有关创建和管理 SSL 解密的端到端流程说明，请参阅 如何实施和维护 SSL 解密策略。

操作步骤

Before you begin

SSL 解密规则表包含两个部分：

- **身份策略主动身份验证规则** - 如果启用身份策略并创建使用主动身份验证的规则，系统将自动创建使这些策略生效所需的 SSL 解密规则。这些规则始终在您自己创建的 SSL 解密规则之前进行评估。只可通过更改身份策略来间接更改这些规则。
- **SSL 本机规则** - 这些是已经配置的规则。只能将规则添加到此部分。

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择要创建 SSL 策略的设备。

步骤 4 点击右侧**管理 (Management)** 窗格中的 **策略 (Policy)** 。

步骤 5 点击策略栏中的 **SSL 解密 (SSL Decryption)**。

步骤 6 如果尚未启用该策略，请点击**启用 SSL 解密 (Enable SSL Decryption)** 并按照启用 SSL 解密策略中的说明来配置策略设置。

步骤 7 配置策略的默认操作。最安全的选择是不解密。有关详细信息，请参阅适用于您的设备的版本的《适用于 Firepower 设备管理器的 Cisco Firepower 威胁防御配置指南》中“安全策略”一章的**配置默认 SSL 解密操作**部分。

步骤 8 管理 SSL 解密策略。

在配置 SSL 解密设置后，此页面将按顺序列出所有规则。规则依据流量按照从上到下的顺序进行匹配，由第一个匹配项确定要应用的操作。从此页面中可以执行以下操作：

- 要禁用该策略，请点击 SSL 解密策略开关。可以通过点击启用 SSL 解密重新启用该策略。
- 要编辑策略设置（包括策略中使用的证书列表），请点击 SSL 工具栏上的配置按钮： 

。此外，还可以下载与解密重签名规则一起使用的证书，以便将

其分发给客户端。请参阅适用于您的设备的版本的《适用于 Firepower 设备管理器的 Cisco Firepower 威胁防御配置指南》中“安全策 略”一章的以下部分：

- 为已知密钥和重签解密配置证书
- 为解密重签名规则下载 CA 证书

- 要配置规则，请执行以下操作：
  - 要创建新规则并记录它生成的事件，请点击蓝色加号按钮  。请参阅配置 SSL 解密规则。
  - 要编辑现有规则，请在规则表中点击该规则，然后点击“操作”(Actions) 窗格中的**编辑 (Edit)**。也可以选择在表中点击某规则属性来编辑该属性。
  - 要删除不再需要的规则，请在规则表中点击该规则，然后在“操作”窗格中点击**删除 (Remove)**。
  - 要移动规则，请将鼠标光标悬停在规则表中。在行的最后，使用向上和向下箭头移动其与规则表的位置。
  - （可选）对于您创建的任何规则，您可以选择它并在“添加注释”(Add Comments) 字段中添加注释。要了解有关规则注释的详细信息，请参阅向策略和规则集中的规则添加注释。

步骤 9 继续启用 SSL 解密策略。

启用 SSL 解密策略

在可以配置 SSL 解密规则之前，必须启用该策略并配置一些基本设置。以下程序介绍了如何直接启用该策略。此外，还可在启用身份策略时启用该策略。身份策略要求启用 SSL 解密策略。

操作步骤

Before you begin

如果从未设置 SSL 解密策略的版本进行升级，但已使用主动身份验证规则配置身份策略，则 SSL 解密策略已启用。确保已选择要使用的解密重签名证书，并且可以选择启用预定义规则。

查看配置 SSL 解密策略（如果尚未配置）。

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡和要为其启用 SSL 解密策略的设备。

步骤 4 点击右侧**管理 (Management)** 窗格中的 **策略 (Policy)** 。

步骤 5 点击策略栏中的 **SSL 解密 (SSL Decryption)**。

步骤 6 点击 SSL 栏中的 **SSL 解密 (SSL Decryption)** 开关以启用 SSL 解密策略。

- 如果这是您首次启用该策略，请阅读解密已知密钥和解密重签 SSL 解密的说明，然后点击启用。
- 如果已对策略进行过一次配置然后禁用了策略，则只需使用之前的设置和规则即可再次启动该策略。您可以点击 SSL 解密配置按钮 

为已知密钥和重签解密配置证书，并如中所述配置设置。

步骤 7 对于**选择解密重签名证书**，请选择内部 CA 证书，以用于使用重签名证书实施解密的规则。

您可以使用预定义的 NGFW-Default-InternalCA 证书，也可以使用您创建或上传的证书。如果尚无证书，请点击**创建 (Create)** 以添加 FDM 管理设备内部 CA 证书。

如果尚未在客户端浏览器中安装证书，请点击下载按钮  获取副本。有关如何安装证书的信息，请参阅各浏览器文档。另请参阅为解密重签名规则下载 CA 证书。

步骤 8 点击**保存 (Save)**。

步骤 9 继续配置默认 SSL 解密操作，以便为策略设置默认操作。

配置默认 SSL 解密操作

如果加密连接没有匹配特定 SSL 解密规则，则由 SSL 解密策略的默认操作来处理。

操作步骤

Before you begin

如果还没有，请查看这些程序并按照其中的程序进行操作：

1. 配置 SSL 解密策略
2. 启用 SSL 解密策略

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择要为其配置默认 SSL 解密操作的设备。

步骤 4 点击右侧**管理 (Management)** 窗格中的 **策略 (Policy)** 。

步骤 5 点击策略栏中的 **SSL 解密 (SSL Decryption)**。

步骤 6 点击**默认操作 (Default Action)** 按钮。

步骤 7 选择应用于匹配流量的操作：

- **不解密** - 允许加密连接。然后，访问控制策略将评估加密连接，并根据访问控制规则丢弃或允许该连接。
- **阻止** - 立即丢弃连接。连接将不传递到访问控制策略。

步骤 8 （可选。）针对默认操作配置日志记录。您必须启用日志记录以便从 SSL 解密策略捕获事件。从以下选项中选择：

- **连接结束时** - 在连接结束时生成事件。
  - 将连接事件发送到 (Send Connection Events To) - 如果要将事件副本发送至外部系统日志服务器，请选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，请点击创建新系统日志服务器，并创建对象。（要对系统日志服务器禁用日志记录，请从服务器列表中选择“任何”）。

    由于设备中的事件存储受限，所以将事件发送至外部系统日志服务器可供长期存储，并增强您的事件分析。

    如果订用了思科安全分析和日志记录，请将 FDM 事件发送到 思科防御协调器 事件日志记录。有关此功能的详细信息，请参阅FDM 管理 设备的安全日志记录分析。

- **无日志记录 (No logging)** - 不生成任何事件。

步骤 9 点击**保存 (Save)**。

步骤 10 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

配置 SSL 解密规则

使用 SSL 解密规则确定如何处理加密连接。SSL 解密策略中的规则按从上到下的顺序进行评估。对流量应用的规则是符合所有流量条件标准的第一个规则。

只可在“SSL 本机规则”部分创建和编辑规则。

Caution 请记住，解密并重新加密流量会增加设备的处理负载，从而降低整体系统性能。

Note 在 SSL 解密策略评估连接之前，系统将对 VPN 连接（站点间和远程访问）流量进行解密。因此，SSL 解密规则永远不会应用于 VPN 连接，且在创建这些规则时不需要考虑 VPN 连接。但是，系统会对 VPN 隧道中使用的所有加密连接进行评估。例如，SSL 解密规则将对通过 RA VPN 连接到内部服务器的 HTTPS 连接进行评估，即使 RA VPN 隧道本身没有接受评估（原因在于其已解密）

操作步骤

Before you begin

如果还没有，请查看配置 SSL 解密策略、启用 SSL 解密策略和配置默认 SSL 解密操作，以配置将向其添加规则的 SSL 解密策略。

如要创建解密已知密钥规则，请确保上传目标服务器的证书和密钥（作为内部证书），并编辑 SSL 解密策略设置，以使用该证书。已知密钥规则通常在该规则目标网络条件中指定目标服务器。有关详细信息，请参阅为已知密钥和重签解密配置证书。

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择要为其启用 SSL 解密策略的设备。

步骤 4 点击右侧“管理”(Management) 窗格中的 **策略 (Policy)** 。

步骤 5 点击策略栏中的 **SSL 解密 (SSL Decryption)**。

步骤 6 执行以下任一操作：

- 要创建新规则，请点击蓝色加号  按钮。
- 要编辑现有规则，请点击规则的编辑图标 。
- 要删除不再需要的规则，请点击该规则的删除图标 。

步骤 7 在**顺序 (Order)** 中，选择要在规则编号列表中插入规则的位置。

只可将规则插入 SSL 本机规则部分。身份策略主动身份验证规则将根据身份策略自动生成并且为只读形式。

先匹配的规则先应用，所以您必须确保流量匹配条件标准较具体的规则显示在次之用来匹配流量的较通用条件标准的策略上方。

默认将规则添加到列表的末尾。如果以后要更改规则的位置，请编辑此选项。

步骤 8 在**名称 (Name)** 中输入规则的名称。

名称不能包含空格。可以使用字母数字字符和以下特殊字符：+ . _ -

步骤 9 选择应用于匹配流量的操作。有关每个选项的详细讨论，请参阅下列内容：

- 解密重签名
- 解密已知密钥
- 不解密
- 阻止

步骤 10 使用以下选项卡的任意组合，定义流量匹配标准：

- **源/目标** - 流量通过的安全区（接口）、IP 地址或该 IP 地址的国家/地区或大洲（地理位置）或者流量中使用的 TCP 端口。默认设置为任何区域、地址、地理位置和 TCP 端口。请参阅 SSL 解密规则的源/目标条件。
- **URL** - Web 请求的 URL 类别。默认情况下，进行匹配时不考虑 URL 类别和信誉。请参阅 SSL 解密规则的 URL 标准。
- **应用** - 应用或按类型、类别、标记、风险或业务相关性定义应用的过滤器。默认设置为任何加密应用。请参阅 SSL 解密规则的应用标准。
- **用户** - 用户或用户组。身份策略决定了用户和组的信息是否可用于流量匹配。只有配置身份策略，才能使用此条件标准。请参阅 SSL 解密规则的用户条件。
- **高级** - 从连接中使用的证书派生的特性，例如 SSL/TLS 版本和证书状态。请参阅 SSL 解密规则的高级条件。

要修改条件，请点击该条件内的蓝色加号按钮  ，选择所需的对象或元素，然后在弹出对话框中点击**选择 (Select)**。如果条件需要对象，而所需的对象不存在，您可以点击**创建新对象 (Create New Object)**。点击对象或元素对应的 x，可将其从策略中移除。

向 SSL 解密规则中添加条件时，请考虑以下提示：

- 您可以为每个规则配置多个条件。要使规则应用于流量，流量必须匹配该规则中的所有条件。例如，可以使用单一规则来基于 URL 类别对流量进行解密。
- 最多可以为规则中的每个条件添加 50 个标准。匹配某个条件所有条件标准的流量满足该条件。例如，您可以使用单一规则为最多 50 个应用或应用过滤器执行应用控制。因此，单一条件中的项目之间为 OR 关系，但不同条件类型之间（例如，源/目的和应用之间）为 AND 关系。
- 匹配 URL 类别需要 URL 许可证。

步骤 11 （可选。）针对规则配置日志记录。

对于与控制面板或事件查看器中包括的规则匹配的流量，必须为其启用日志记录。从以下选项中选择：

- **无日志记录 (No logging)** - 不生成任何事件。
- **将连接事件发送到** - 如果要将事件副本发送至外部系统日志服务器，请选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，请点击**创建 (Create)** 并创建对象。（要对系统日志服务器禁用日志记录，请从服务器列表中选择“任何”）。
- **连接结束时** - 在连接结束时生成事件。由于设备中的事件存储受限，所以将事件发送至外部系统日志服务器可供长期存储，并增强您的事件分析。

如果订用了思科安全分析和日志记录，请使用安全事件连接器的 IP 地址和端口来指定或为安全日志记录分析 (SaaS) 创建系统日志服务器对象。有关详细信息，请参阅思科安全分析和日志记录。

步骤 12 点击**保存 (Save)**。

步骤 13 （可选）对于您创建的任何规则，您可以选择它并在“添加注释”(Add Comments) 字段中添加注释。要了解有关规则注释的详细信息，请参阅向策略和规则集中的规则添加注释。

步骤 14 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

SSL 解密规则的源/目标条件

SSL 解密规则的源/目标条件定义了流量通过的安全区（接口）、IP 地址或该 IP 地址所在的国家/地区或大洲（地理位置）或是流量中所用的 TCP 端口。默认设置为任何区域、地址、地理位置、协议和任何 TCP 端口。TCP 是与 SSL 解密规则匹配的唯一协议。

要修改条件，请点击该条件内的蓝色按钮  ，选择所需的对象或元素，然后点击**选择 (Select)**。如果条件需要对象，而所需的对象不存在，您可以点击**创建新对象 (Create New Object)**。点击对象或元素对应的 **x**，可将其从策略中移除。

源区域、目标区域

安全区对象，定义通过其传递流量的接口。可以定义一个或两个条件，也可以不定义任何条件：未指定的任何条件都将应用到任何接口上的流量。

- 要匹配从区域中的接口离开设备的流量，请将该区域添加至目标区域。
- 要匹配从区域中的接口进入设备的流量，请将该区域添加至源区域。
- 如果同时向一条规则添加源区域和目标区域条件，匹配流量必须源自其中一个指定源区域并通过其中一个目标区域流出。

如果应基于流量进入或离开设备的位置来应用规则，请使用此条件。例如，如果要确保从外部主机到内部主机的所有流量均被解密，则应将外部区域选为源区域，并将内部区域选为目标区域。

源网络、目标网络

定义流量的网络地址或位置的网络对象或地理位置。

- 要匹配来自某个 IP 地址或地理位置的流量，请配置源网络。
- 要匹配流向 IP 地址或地理位置的流量，请配置目标网络。

如果同时向一条规则添加源网络条件和目标网络条件，匹配流量必须源自其中一个指定 IP 地址并流向其中一个目标 IP 地址。

添加此条件时，可从以下菜单选项中进行选择：

- **网络** - 为您要控制的流量选择定义源或目标 IP 地址的网络对象或组。

Note 对于解密已知密钥规则，请选择使用目标服务器 IP 地址的对象（该对象使用您上传的证书和密钥）。

- **国家/地区/大洲 (Country/Continent)** - 选择要基于流量的源或目的国家/地区或大洲控制流量的地理位置。选择大洲将会选择该大洲内的所有国家/地区。

- **自定义地理位置 (Custom Geolocation)** - 您可以选择您创建的地理位置对象来定义位置。使用地理位置，可以便捷地限制对特定国家/地区的访问，而不需要知道此位置所用的全部潜在 IP 地址。

源端口、目标端口/协议

定义流量中所用协议的端口对象。仅可指定用于 SSL 解密规则的 TCP 协议和端口。

- 要匹配来自 TCP 端口的流量，请配置源端口。
- 要匹配流向 TCP 端口的流量，请配置目标端口/协议。

要同时匹配来自特定 TCP 端口的流量和流向特定 TCP 端口的流量，请配置源端口和目标端口。例如，您可以匹配从端口 TCP/80 流至端口 TCP/8080 的流量。

步骤 10

SSL 解密规则的应用标准

SSL 解密规则的应用标准定义 IP 连接中使用的应用，或定义按类型、类别、标记、风险或业务相关性定义应用的过滤器。默认为任何具有 SSL 协议标记的应用。您无法将 SSL 解密规则与任何未加密应用相匹配。

虽然您可以在规则中指定个别应用，但应用过滤器可简化策略创建和管理。例如，您可以创建一条 SSL 解密规则，用于解密或阻止所有业务相关性较低的高风险应用。如果用户尝试使用这些应用中的任意一个，系统会解密或阻止会话。

另外，思科会通过系统和漏洞数据库 (VDB) 更新频繁更新和添加其他应用检测器。因此，高风险应用规则可自动应用到新应用中，而无需您手动更新规则。

您可以直接在规则指定应用和过滤器，也可以创建定义这些特征的应用过滤器对象。规格相当，尽管如果要创建复杂规则，使用对象可便于遵守每个条件 50 个项目的系统限制。

要修改应用和过滤器列表，请点击该条件内的  按钮，选择所需的应用程序或应用程序筛选器对象，在弹出的对话框中点击“选择”(Select)，然后点击“保存”(Save)。点击应用、过滤器或对象的 x，可将其从策略中移除。点击另存为过滤器链接，可将尚不是对象的组合条件另存为新应用过滤器对象。

有关应用标准以及如何配置高级过滤器和选择应用的更多信息，请参阅创建和编辑 Firepower 应用过滤器对象。

在 SSL 解密规则中使用应用标准时，请考虑以下提示：

- 系统可以识别使用 StartTLS 进行加密的未加密应用。这包括诸如 SMTPS、POPS、FTPS、TelnetS 和 IMAPS 之类的应用。此外，系统还可以根据 TLS ClientHello 消息中的服务器名称指示或服务器证书使用者可分辨名称值来识别某些加密应用。
- 仅在服务器证书交换后，系统才可识别使用。如果在 SSL 握手期间交换的流量与包含应用条件的 SSL 规则中的所有其他条件相匹配，但是识别未完成，则 SSL 策略允许数据包通过。此行为允许完成握手，以便可以识别应用。在系统完成其识别后，系统将 SSL 规则操作应用于与其应用条件相匹配的剩余会话流量。

步骤 10

SSL 解密规则的 URL 标准

SSL 解密规则的 URL 标准定义了 Web 请求中的 URL 所属的类别。还可以指定要解密、阻止或允许不解密的站点的相对信誉。默认不基于 URL 类别匹配连接。

例如，您可以阻止所有加密的游戏站点或解密所有高风险社交网站。如果用户尝试浏览至任何包含该类别和信誉组合的 URL，会话将被阻止或解密。

要向 SSL 解密规则添加 URL 条件，请执行以下操作：

Procedure

步骤 1 点击 URL 选项卡，将 URL 类别添加到 SSL 解密规则。

步骤 2 搜索并选择要阻止的 URL 类别。

步骤 3 默认情况下，来自您选择的类别的 URL 的流量将由 SSL 解密规则解密，而无论其安全信誉如何。但是，您可以微调规则中的 URL 类别或所有 URL 类别，以便根据信誉从解密中排除某些站点。

- 要微调 URL 中单个类别的信誉，请执行以下操作：
  1. **a.** 在选择 URL 类别后，点击该类别。
  2. **b.** 取消选中**任何信誉 (Any Reputation)**。
  3. **c.** 将绿色滑块向右滑动，选择要从规则中排除的 URL 信誉设置，然后点击**保存 (Save)**。

     滑块所覆盖的信誉不受规则影响。例如，如果将绿色滑块滑动到“良性站点”，那么“知名站点”和“良性站点”不会受到所选类别的 SSL 解密规则的影响。被视为具有安全风险、可疑站点和高风险站点的 URL 仍会受到该 URL 类别的规则影响。

- 要微调添加到规则中的所有 URL 类别的信誉，请执行以下操作：
  1. **a.** 选择要包含在SSL解密规则中的所有类别后，点击**将信誉应用于所选类别 (Apply Reputation to Selected Categories)**。
  2. **b.** 取消选中**任何信誉 (Any Reputation)**。
  3. **c.** 将绿色滑块向右滑动，选择要从规则中排除的 URL 信誉设置，然后点击**保存 (Save)**。

     滑块所覆盖的信誉不受规则影响。例如，如果将绿色滑块滑动到“良性站点”，那么“知名站点”和“良性站点”不会受到全部所选类别的 SSL 解密规则的影响。被视为具有安全风险、可疑站点和高风险站点的 URL 仍会受到全部 URL 类别的规则影响。

步骤 4 点击 **Select**。

步骤 5 点击**保存 (Save)**。

步骤 10

SSL 解密规则的用户条件

SSL 解密规则的“用户”条件对 IP 连接的用户或用户组进行了定义。只有配置身份策略和相关联的目录服务器，才能在规则中包括用户或用户组条件。

您的身份策略决定是否收集某个特定连接的用户身份。如果建立了身份，则主机的 IP 地址与所识别的用户相关联。因此，源 IP 地址映射到用户的流量将被视为来自该用户。IP 数据包本身不包含用户身份信息，所以此 IP 地址到用户的映射是最接近的近似值。

由于最多可以向规则中添加 50 个用户或组，所以选择组比选择单个用户通常更有意义。例如，您可以创建规则，对从外部网络发往工程组的流量进行解密，并单独创建一个不会对从该组传出的流量进行解密的规则。然后，要将该规则应用于新工程师，您只需添加将工程师添加到目录服务器的“工程”组即可。

要修改用户列表，请点击该条件内的 + 按钮，并选择所需的用户组，然后点击“选择”(Select)。

步骤 10

SSL 解密规则的高级条件

高级流量匹配标准与根据连接中使用的证书派生的属性有关。您可以配置以下任何或全部选项。

证书属性

如果流量与任何选定属性匹配，则它与相应规则的证书属性选项匹配。您可以配置以下内容：

- **证书状态 (Certificate Status)**：证书无效还是有效。如果您不关心证书状态，请选择任意（默认）。如果满足以下所有条件，证书即视为有效，否则视为无效：
  - 策略信任颁发证书的 CA。
  - 可根据证书的内容对证书的签名进行适当的验证。
  - 颁发者 CA 证书存储在策略的受信任 CA 证书列表中。
  - 策略的受信任 CA 未撤销证书。
  - 当前日期介于证书的有效期开始日期和有效期结束日期之间。
- **自签名 (Self-Signed)**：服务器证书是否包含相同的使用者和颁发者可分辨名称。选择以下一个选项：
- 自签名 - 服务器证书自签名。
  - CA 签名 - 服务器证书由证书颁发机构签名。也就是说，颁发者和使用者不同。
  - 任意 - 不考虑按照匹配标准，证书是否为自签名。

支持的版本

要匹配的 SSL/TLS 版本。该规则适用于仅使用任何选定版本的流量。默认设置是所有版本。可以选择以下版本：SSLv3.0、TLSv1.0、TLSv1.1 和 TLSv1.2。

例如，如果仅希望允许 TLSv1.2 连接，则可创建用于非 TLSv1.2 版本的阻止规则。使用任何未列出版本（例如 SSL v2.0）的流量均由 SSL 解密策略的默认操作处理。

步骤 10

为已知密钥和重签解密配置证书

如果通过重签或使用已知密钥实施解密，则需要确定 SSL 解密规则可以使用的证书。确保所有证书均有效且未过期。

特别是对于已知密钥的解密，需要确保系统拥有要解密连接的各目标服务器的当前证书和密钥。通过解密已知密钥规则，可以使用目标服务器的实际证书和密钥进行解密。因此，必须确保FDM管理设备始终拥有当前证书和密钥，否则将无法成功解密。

只要在已知密钥规则中更改目标服务器上的证书或密钥，就要上传新的内部证书和密钥。将上述证书作为内部证书（而不是内部CA证书）上传。可以在下列程序中上传证书，也可以转到**对象 (Objects)** 页面并在此页面中点击  按钮并选择 **FTD > 证书 (Certificate)** 上传。

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，选择要为其创建 SSL 策略的设备，然后点击右侧管理窗格中的**策略 (Policy)**。

步骤 4 点击策略栏中的 **SSL 解密 (SSL Decryption)**。

步骤 5 点击 SSL 解密策略栏中的证书按钮 

。

步骤 6 在 SSL 解密配置对话框中，点击**选择解密重新签名证书 (Select Decrypt Re-Sign Certificate)**菜单，然后选择或创建内部 CA 证书，以用于利用重签名证书实施解密的规则。您可以使用预定义的 **NGFW-Default-InternalCA** 证书，也可以使用您创建或上传的证书。

如果尚未在客户端浏览器中安装证书，请点击下载按钮  获取副本。有关如何安装证书的信息，请参阅各浏览器文档。另请参阅适用于运行设备的版本的《适用于 Firepower 设备管理器的 Cisco Firepower 威胁防御配置指南》“安全策略”一章的**下载 CA 证书以进行解密重签名规则**部分。

步骤 7 对于使用已知密钥解密的每条规则，上传目标服务器的内部证书和密钥。

步骤 8 点击**解密已知密钥证书 (Decrypt Known-Key Certificates)** 下的  。

步骤 9 选择内部身份证书，或点击**创建新的内部证书**以便立即上传。

步骤 10 点击**保存 (Save)**。

步骤 11 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

为解密重签名规则下载 CA 证书

如果决定对流量进行解密，则用户必须拥有加密流程中使用的内部CA证书，该证书由使用TLS/SSL的应用中被定义为受信任根证书颁发机构所颁发。通常，当生成证书或即使导入证书后，证书不会立即在这些应用中定义为受信任。默认情况下，在大多数网络浏览器中，当用户发送 HTTPS 请求时，他们将看到一条来自客户端应用的警告消息，告知他们网站的安全证书有问题。通常，错误消

息表明网站的安全证书并非由受信任证书颁发机构所颁发或网站由未知机构所认证，但该警告可能还表明可能存在中间人攻击。一些其他客户端应用不会向用户显示此警告消息，也不允许用户接受无法识别的证书。

可以通过以下方式为用户提供所需的证书：

通知用户接受根证书

可以通知您组织中的用户，告知其公司的新策略并指示其接受组织提供的根证书作为受信任来源。用户应接受该证书并将其保存在受信任根证书颁发机构存储区，以确保在下次访问该站点时系统不会再次提示。

Note 用户需要接受并信任创建替换证书的 CA 证书。如果仅信任替换服务器证书，用户访问各个不同 HTTPS 站点时将继续看到警告。

将根证书添加到客户端设备

能够以受信任根证书颁发机构身份将根证书添加到网络上的所有客户端设备。这样，客户端应用将自动接受包含根证书的事务。

可以通过以下方式向用户提供证书：通过邮件发送或将其放在共享站点上，将证书整合到企业工作站映像中并使用应用更新工具将其自动分发给用户。

以下程序介绍了如何下载内部 CA 证书并将其安装在 Windows 客户端上。

操作步骤

该流程因操作系统和浏览器类型的不同而不同。例如，对于 Windows 上运行的 Internet Explorer 和 Chrome 浏览器，可以采用以下流程。（对于 Firefox，请选择**工具 (Tools)** > **选项 (Options)** > **高级 (Advanced)** 页面，进行安装。）

系统应显示消息，指示已成功导入。您可能会看到一个中间对话框，警告：如果生成自签名证书而不是从知名第三方证书颁发机构获取证书，则 Windows 无法验证该证书。

此时，可以关闭“证书”和“Internet 选项”对话框。

Procedure

步骤 1 从 Firepower 设备管理器中下载证书。

a) 在导航窗格中，点击**清单 (Inventory)**。
b) 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
c) 点击 **FTD** 选项卡，然后选择存储证书的设备。
d) 点击右侧“管理”(Management) 窗格中的 **策略 (Policy)** 。
e) 点击策略栏中的 **SSL 解密 (SSL Decryption)**。
f) 点击 SSL 解密策略栏中的 SSL 解密配置按钮 

。
g) 点击下载按钮 

h) 选择一个下载位置，或者更改文件名（但是不要更改扩展名），然后点击保存 (Save)。

i) 此时可以取消“SSL 解密设置”对话框。

步骤 2 在客户端系统上，在网络浏览器的受信任根证书颁发机构存储区安装证书，或向客户端提供证书，以便用户自行安装。对于不同的浏览器和操作系统，此过程会有所不同。

警告

通过 FDM 管理设备配置的 CA 证书

思科防御协调器 可以管理多个设备，但在保存设备配置时保存的其他信息受到限制，这可能会在处理内部 CA 证书时产生一些问题。CDO **不会**保存通过 FDM 管理 控制台配置的 CA 证书的证书或密钥信息；如果您尝试使用 FDM 管理设备中配置的 CA 证书并将其应用于部署到辅助设备的 SSL 策略，则 CDO 会创建 CA 证书的本地副本，但不会也无法复制密钥信息。因此， CDO 或辅助设备都没有密钥信息，并且无法成功部署 CA 证书。这也意味着 CA 证书的本地副本的下载链接不可用。

我们强烈建议通过 FDM 管理设备为任何其他设备配置单独的 CA 证书，或通过 CDO UI 创建 CA 证书。

规则集

关于规则集

规则集是可与多个 FDM 管理 设备共享的访问控制规则的集合。对规则集的规则所做的任何更改都会影响使用此规则集的其他受管设备。FDM管理 设备可以具有设备特定（本地）和共享（规则集）规则。您还可以从 FDM 管理 设备中的现有规则创建规则集。

Important “规则集”功能当前可用于运行 FDM 管理 设备升级单个 FTD 设备和更高版本。另请注意，规则集不支持启用 Snort 3 的设备。

以下限制适用：

- 不能将规则集附加到支持 Snort 3 的设备。
- 您无法从已安装 Snort 3 的现有设备创建规则集。
- 不能将自定义 IPS 策略与规则集关联。

复制或移动与规则集关联的规则

可以在规则集中或跨不同规则集复制或移动访问控制规则。此外，您还可以在本地和规则集之间复制或移动规则。有关详细信息，请参阅复制 FDM 管理 访问控制规则和移动 FDM 管理 访问控制规则。

自动检测现有规则集

当您载入设备时，思科防御协调器 会自动检测设备上的现有规则集，并尝试将其与设备上的规则进行匹配。成功匹配后，CDO 会自动将规则集附加到新载入的设备。但是，如果设备上的同一组规则有多个规则集匹配项，则不会附加任何规则集，您必须手动分配它们。

为设备配置规则集

按照以下部分来创建和部署规则集：

Procedure

步骤 1 为设备配置规则集。

a) 创建新的规则集并为其分配规则。
b) 将对象分配给规则。
c) 设置规则集的优先级。
d) 如果需要，更改规则的顺序。

步骤 2 为设备配置规则集。

a) 将多个设备附加到规则集。
b) 查看规则集并将其部署到设备。

创建或编辑规则集

您可以创建规则集并向其添加新的访问控制规则。

按照以下程序为多个 FDM 管理设备创建规则集：

Procedure

步骤 1 在导航窗格中，点击**策略 (Policies) > FTD 规则集 (FTD Rulesets)**。

步骤 2 点击加号  按钮创建新的规则集。

Note 要编辑现有规则集，请选择该规则集，然后点击编辑图标 。

步骤 3 为该规则集输入一个名称，然后点击**创建 (Create)**。

步骤 4 创建访问控制规则以将其添加到规则集中。有关说明，请参阅配置 FDM 访问控制策略。

Note 规则集中的访问控制规则不支持用户条件。

步骤 5 在窗口的右上角，选择规则集的优先级 

。如果设备未连接到规则集，则可以设置优先级。该选择会影响此规则集中包含的所有规则及其在设备上的处理方式：

- **排名靠前 (Top)** - 在设备上的所有其他规则之前处理规则集。规则排列在规则列表的顶部，并首先进行处理。任何其他规则集都不能优先于此策略中的规则。每个设备只能有一个排名靠前的规则集。
- **排名靠后 (Bottom)** - 规则集在设备上的所有其他规则之后处理。除策略的默认操作外，没有其他规则集可以继承此策略中的规则。每个设备只能有一个排名靠后规则集。默认情况下，优先级会被设为**排名靠后 (Bottom)**。

本地规则 (Local Rules) 显示设备的所有设备特定规则。

Note 当规则集连接到设备时，无法更改优先级。您必须断开设备并更改优先级。

步骤 6 点击**保存 (Save)**。您可以根据需要创建任意数量的规则。

步骤 7 （可选）对于您创建的任何规则，您可以选择它并在“添加注释”(Add Comments) 字段中添加注释。要了解有关规则注释的详细信息，请参阅向策略和规则集中的规则添加注释。

Note

- 即使将设备连接到规则集中，也可以更改规则集中的规则顺序。按照以下程序来更改规则集的优先级：
  a. 在导航窗格中，点击**策略 (Policies) > 规则集 (Rulesets)**，然后选择要删除的规则集。
  b. 选择要移动的规则。
  c. 将光标悬停在规则行内，然后使用**上移** 或**下移** 箭头将规则移至所需的顺序。
- CDO 允许您对象覆盖。在将新对象添加到规则时，只有在将设备附加到规则集并保存更改后，才能覆盖该对象。

将规则集部署到多个 FDM 管理 的设备或模板

您必须将规则集附加到要实施的设备或模板。在查看更改后，您可以在设备上部署配置。在将模板应用于新的 FDM 管理 设备时，模板中包含的规则集将被推送到设备。

有关详细信息，请参阅使用 FDM 管理 模板的规则集。

在开始之前，请考虑以下信息：

- 您只能将规则集附加到已载入 思科防御协调器 的 FDM 管理 设备。
- 设备只能有一个底部或顶部规则集。
- 从规则集中连接或删除设备后，更改会在CDO中暂存但不会部署，并且设备将变为**未同步 (Not Synced)**，表示未与 CDO 同步。点击屏幕右上角的 图标，将更改部署到设备。
- 在连接设备后，与规则集关联的新规则不会覆盖与设备关联的现有规则。

您可以通过两种方式将规则集与设备关联：

- 从“规则集”(Ruleset) 页面将设备添加到规则集。
- 从“设备策略”(Device Policy) 页面向设备添加规则集。

从“规则集”(Ruleset) 页面将设备添加到规则集

Procedure

步骤 1 在导航窗格中，点击**策略 (Policies) > FTD 规则集 (FTD Rulesets)**。

步骤 2 选择要分配给 FTD 设备的规则集，然后在**操作 (Actions)** 窗格中点击**编辑 (Edit)**。

步骤 3 在右上角，点击**规则集 (Ruleset for)**旁边显示的**设备 (Device)** 按钮 

。

步骤 4 从符合条件的 FTD 设备列表中选择。

步骤 5 当系统确定规则集中的规则与设备特定的规则之间存在重复名称时，在齿轮图标中选择系统要执行的以下操作之一：

- **规则冲突时失败 (Fail on conflicting rules)**（默认选项）：CDO 不会将规则集添加到设备。您需要手动重命名重复的规则，然后添加规则集。
- **重命名冲突规则 (Rename conflicting rules)**：CDO 重命名设备上存在的冲突规则（本地规则）。

步骤 6 点击**保存 (Save)**。**将规则集附加到设备 (Attached Ruleset to Devices)** 向导将关闭。

步骤 7 点击右上角的**保存 (Save)** 以保存对规则集所做的更改。保存规则集会将更改暂存到 CDO。

Note 每次修改规则集时，都必须点击**保存 (Save)**。通过执行此操作，所有更改都将被暂存到 CDO。您必须手动部署更改。

步骤 8 点击 **Confirm**。保存规则集会将更改暂存到 CDO。

步骤 9 预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。如果您放弃更改设备上的暂存规则集更改，请参阅放弃暂存规则集更改的影响。

从“设备策略”(Device Policy) 页面向设备添加规则集

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后从列表中选择所需的设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。

步骤 5 点击窗口右上角出现的  按钮。

步骤 6 选择所需的规则集。

步骤 7 当系统确定规则集中的规则与设备特定的规则之间存在重复名称时，在齿轮图标中选择系统要执行的以下操作之一：

- **规则冲突时失败 (Fail on conflicting rules)**（默认选项）：CDO 不会将规则集添加到设备。您需要手动重命名重复的规则，然后添加规则集。
- **重命名冲突规则 (Rename conflicting rules)**：CDO 重命名设备上存在的冲突规则（本地规则）。

Note 如果所选设备上没有冲突规则，CDO 会将规则集附加到设备，而不进行任何更改。

步骤 8 点击**附加规则集 (Attach Ruleset)**。规则集会根据规则集的优先级被添加到设备。

步骤 9 预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。如果您放弃更改设备上的暂存规则集更改，请参阅放弃暂存规则集更改的影响。

相关信息：

- 规则集
- 使用 FDM 管理 模板的规则集
- 从所选规则集中分离 FTD 设备
- 删除规则和规则集
- 带外更改对规则集的影响
- 查看规则和规则集
- 创建规则集后更改日志条目
- 从现有设备规则创建规则集

使用 FDM 管理 模板的规则集

思科防御协调器 允许您将规则集分配给 FDM 管理 模板。

- 从具有规则集的 FDM 管理设备创建模板时，CDO 会自动将模板添加到源设备上存在的规则集中。您可以从规则集中管理模板。
- 将包含规则集的模板应用于目标 FDM 管理设备时，CDO 会自动将目标设备添加到规则集，从而从规则集中管理目标设备。
- 将包含规则集的模板应用于已具有不同规则集的目标 FDM 管理设备时，CDO 会从目标设备中删除现有规则集，并添加与该模板关联的新规则集。

有关详细信息，请参阅将规则集部署到多个 FDM 管理 的设备或模板。

相关信息：

- 规则集

从现有设备规则创建规则集

您可以通过选择 FDM 管理设备中的现有规则来创建规则集。

按照以下程序从现有设备规则创建规则集：

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后从列表中选择所需的设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。系统将显示设备的现有规则。

步骤 5 根据您的要求执行以下操作：

a) 要创建**排名靠前**的规则，请从顶部的第一个规则开始选择连续规则。

b) 要创建**排名靠后**规的则，请选择包含底部最后一条规则的连续规则。

步骤 6 在右侧的**操作 (Actions)** 窗格中，点击**创建规则集 (Create Ruleset)**。

Note 您的选择必须包含第一个或最后一个规则，**创建规则集 (Create Ruleset)** 链接才能点击。

步骤 7 在**规则集名称 (Ruleset Name)** 字段中指定名称，然后点击**创建 (Create)**。在设备中创建相应的规则集。

您可以使用设备中的其余规则继续创建规则集。

带外更改对规则集的影响

当您使用 FDM 管理设备添加新规则或对现有规则进行更改，并且您已在 思科防御协调器 中为 FDM 管理设备启用冲突检测时，CDO 会检测到带外更改，并且设备的配置状态显示为**检测到冲突 (Conflict Detected)**。解决配置冲突。

如果您接受设备更改，CDO 会使用在设备上进行的新更改覆盖最新的配置。将发生以下变化：

- 受更改影响的规则集会失去与设备的关系。

- 与这些规则集关联的规则将转换为本地规则。

如果您拒绝设备更改，CDO 会拒绝新的更改，并将设备上的配置替换为 CDO 中的上次同步配置。

相关信息：

- 规则集
- 为设备配置规则集
- 从现有设备规则创建规则集
- 放弃暂存规则集更改的影响
- 查看规则和规则集
- 创建规则集后更改日志条目
- 从所选规则集中分离 FTD 设备
- 删除规则和规则集

放弃暂存规则集更改的影响

在向规则集添加新规则或使用CDO更改与规则集关联的现有规则时，它会将您所做的更改保存到其自己的配置文件副本中。在“部署”到设备之前，这些更改将被视为已在 CDO 上“待处理”。

如果放弃更改设备上的待定规则集更改，则CDO会用存储在设备上的配置**完全覆盖**设备配置的本地副本。

规则集和关联设备上发生以下更改：

- 受更改影响的规则集会失去与设备的关系。
- 与这些规则集关联的规则将转换为本地规则。
- CDO 会丢弃新的暂存更改并保留设备上的配置。

相关信息：

- 规则集
- 为设备配置规则集
- 从现有设备规则创建规则集
- 带外更改对规则集的影响
- 查看规则和规则集
- 创建规则集后更改日志条目
- 从所选规则集中分离 FTD 设备
- 删除规则和规则集

查看规则和规则集

从设备策略页面查看规则

FDM 管理设备策略页面会显示单个（本地）和共享规则（与规则集关联）。

使用以下程序从策略页面查看 FDM 管理设备规则集：

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后选择所需的设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。根据所做的配置，您会看到以下规则：

- **排名靠前的规则 (Top Rules)**：显示将在设备上的所有其他规则之前处理的强制共享规则。
- **本地规则 (Local Rules)**：显示将在设备上的强制性规则之后处理的设备特定规则。
- **排名靠后 (Bottom)**：显示将在设备上的所有其他规则之后处理的默认共享规则。

Note 您可以通过转至相应的规则集页面来编辑规则集。

a) 在规则集标题的右上角，点击**转到规则集**  。

b) 对规则进行所需的更改，然后点击**保存 (Save)**。新的更改会在与规则集关联的所有设备上更新。

查看规则集

规则集 (Rulesets) 页面会显示租户中可用的所有规则集。它还会提供有关与规则集关联的设备的信息。

使用以下程序可从“规则集”(Rulesets) 页面查看所有规则集：

Procedure

步骤 1 在导航窗格中，点击**策略 (Policies)** > **规则集 (Rulesets)**。系统将显示租户中可用的规则。

步骤 2 点击规则集可查看其详细信息。**设备 (Devices)** 列将显示连接到每个规则集的 FTD 设备的数量。

步骤 3 在**管理 (Management)** 窗格中，点击**工作流程 (Workflows)**。此页面将显示您在设备上执行的所有操作。您可以点击**图表 (Diagram)** 以查看工作流程的图示。

搜索规则集

您可以使用**按设备过滤 (Filter by Device)** 过滤器来选择设备，以便查看分配给它们的规则集。

Procedure

步骤 1 在导航窗格中，点击**策略 (Policies)** > **规则集 (Rulesets)**。

步骤 2 点击过滤器图标，然后点击**按设备过滤 (Filter by Device)**。

步骤 3 从列表选择一个或多个设备，然后点击**确定 (OK)**。

您可以根据所选的设备来查看规则集。

查看与规则集关联的作业

当您将规则集应用于 FTD 设备或从 FTD 设备中删除它们时，**作业 (Jobs)** 页面会记录操作。它还会确定操作是成功还是失败。

Procedure

步骤 1 在导航窗格中，点击**策略 (Policies)** > **规则集 (Rulesets)**。

步骤 2 点击规则集可查看其详细信息。

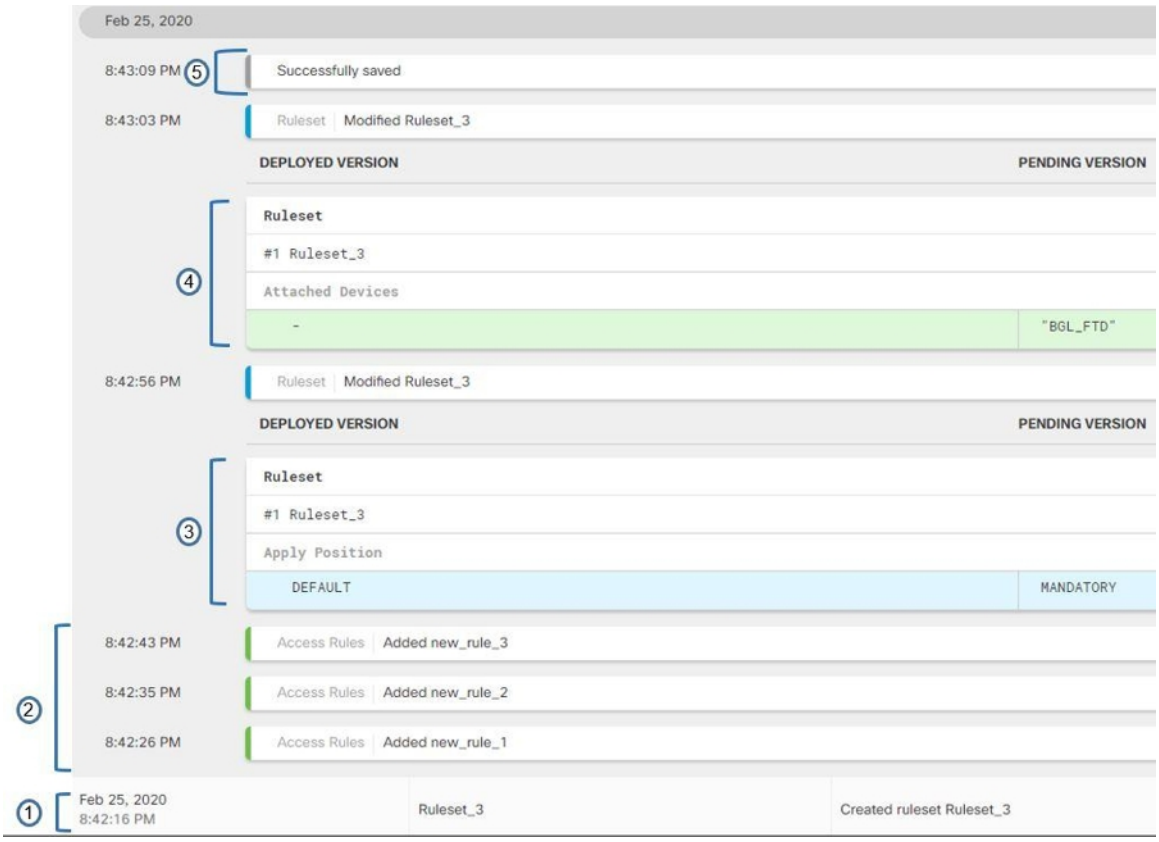
步骤 3 在**管理 (Management)** 窗格中，点击**作业 (Jobs)**。此页面将显示您在规则集上执行的操作。

创建规则集后更改日志条目

当 CDO 检测到规则集发生更改时，它会为在规则集上执行的每个操作创建一个更改日志条目。

如果点击更改日志条目行中的蓝色查看更改日志差异 链接，则会在运行配置文件的上下文中并排对比显示更改。

在下面的示例中，更改日志将显示新规则集的条目，其中三个规则已添加到规则集中。它还会显示有关设置规则集的优先级以及连接到规则集的 FTD 设备的信息。



图中的数字	说明
1	新规则集“Ruleset_3”创建于 2020 年 2 月 25 日上午 11:03:18。
2	在规则集中创建了新的访问规则“new_rule_1”、“new_rule_3”和“new_rule_3”。
3	规则集的优先级被设置为“强制”。
4	规则集被附加到“BGL_FTD”设备。
5	规则集更改已保存。

从所选规则集中分离 FTD 设备

使用以下程序从规则集分离设备：

Procedure

步骤 1 在导航窗格中，点击**策略 (Policies) > 规则集 (Rulesets)**。

步骤 2 选择您要编辑的规则集，然后点击**操作 (Actions)** 窗格中的**编辑 (Edit)** 链接。

步骤 3 在右上角，点击**规则集 (Ruleset for)**旁边显示的**设备 (Device)** 按钮。

步骤 4 取消选中当前连接到规则集的设备，或点击**清除 (Clear)** 以立即删除所有设备。

步骤 5 点击**保存 (Save)**。

步骤 6 点击右上角窗口中的**保存 (Save)** 以保存规则集。保存策略会将更改暂存到 CDO。

步骤 7 预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

相关信息：

- 规则集
- 为设备配置规则集
- 从现有设备规则创建规则集
- 带外更改对规则集的影响
- 查看规则和规则集
- 创建规则集后更改日志条目
- 删除规则和规则集

删除规则和规则集

从规则集中删除规则

可以删除规则集中不再需要的规则。

使用以下程序删除规则：

Procedure

步骤 1 在导航窗格中，点击**策略 (Policies) > 规则集 (Rulesets)**，然后选择规则集。

步骤 2 点击**操作 (Actions)** 窗格中的**编辑 (Edit)**。

步骤 3 选择要删除的规则，然后点击**操作 (Actions)** 下的**删除 (Remove)**。

步骤 4 点击**确定**，确认删除。

步骤 5 点击右上角的**保存 (Save)** 以保存对规则集所做的更改。保存规则集会将更改暂存到 CDO。

步骤 6 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

删除规则集

只有在分离与其关联的所有设备后，才能删除规则集。请参阅从规则集中分离 FTD 设备。删除规则和规则集, on page 395

使用以下程序删除规则集：

Procedure

步骤 1 在导航窗格中，点击策略 > 规则集，然后选择要删除的规则集。
步骤 2 点击规则集行内的删除 (Remove)。
步骤 3 点击确认以永久删除规则集。
步骤 4 立即预览和部署所有设备的配置更改您的更改，或等待并一次部署多个更改。

- 规则集
- 为设备配置规则集
- 从所选规则集中分离 FTD 设备

从所选 FDM 的设备中删除规则集

有两种方法可从所选 FTD 设备中删除规则集，但它们的行为略有不同。

- 从所选 FDM 管理设备删除规则集：此功能从所选 FTD 设备删除规则集及其关联的共享规则。
- 取消规则集与所选 FDM 管理设备的关联：此功能不会删除共享规则。相反，它会将共享规则转换为本地规则。

从所选 FDM 管理设备删除规则集

您可以从所选 FDM 管理设备中删除规则集及其关联的共享规则。规则集也可以从规则集页面从所选规则集中分离 FTD 设备。

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。
步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。
步骤 3 点击 **FTD** 选项卡，然后从列表中选择所需的设备。
步骤 4 点击规则集右上角显示的删除图标。
步骤 5 点击 **Confirm**。
步骤 6 预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

取消规则集与所选 FDM 管理设备的关联

如果要将新的设备特定规则添加到 FDM 管理设备中的规则集，则需要将该规则集与 FDM 管理设备取消关联，这会将其关联的共享规则转换为本地规则。然后，您可以将所需的规则添加到本地规则。

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以查找设备，或点击**模板 (Templates)** 选项卡以查找型号设备。

步骤 3 点击 **FTD** 选项卡，然后从列表中选择所需的设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击**策略 (Policy)**。

步骤 5 点击规则集右上角显示的 图标。

步骤 6 点击 **Confirm**。

步骤 7 预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

向策略和规则集中的规则添加注释

您可以向 FDM 管理 设备策略中的规则和规则集中的规则添加注释，以记录规则的某些特征。规则注释仅在 思科防御协调器 上可见；它们永远不会写入 FDM 管理 设备，也不会在 FDM 中可见。

在 CDO 中创建并保存注释后，注释会被添加到规则中。由于规则注释只是 CDO 的一项功能，因此创建、更改或删除规则注释并不会将 CDO 中设备的配置状态更改为“未同步”(Not Synced)。您无需将更改从 CDO 写入 FDM 管理 设备即可保存规则注释。

可以在设备的策略页面上查看和编辑与 FDM 管理 设备策略中的规则关联的注释。可以在规则集页面上查看和编辑与 FDM 管理 设备规则集中的规则关联的注释。如果规则集被用于策略中，则与规则集中的任何规则关联的任何注释都显示在策略的注释区域中。注释为只读。

如果您在策略、规则集或更改日志中搜索字符串，CDO 将搜索与该字符串的规则关联的注释以及规则的其他属性和值。

在添加或编辑规则的注释时，该操作会记录在更改日志中。由于规则注释只在 CDO 中记录和维护，因此它们会在更改日志中被标记（仅限 CDO 更改）。

Caution 如果 FDM 管理 设备配置发生带外更改，并且 CDO 将该配置读入其数据库，则与任何规则关联的注释都将被清除。

向规则添加注释

Procedure

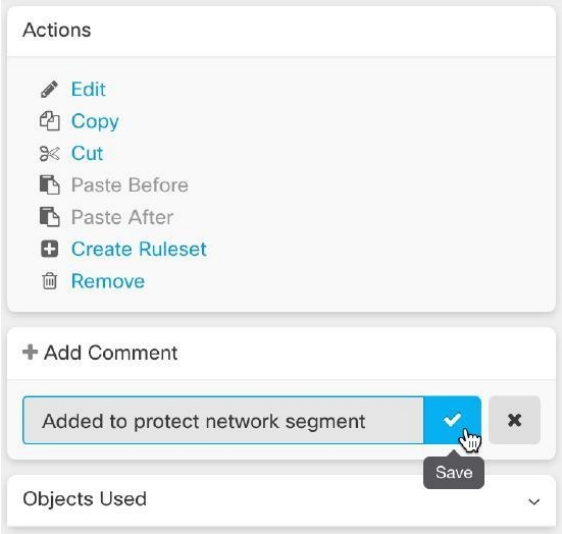
步骤 1 打开包含您要注释的规则的策略或规则集。

步骤 2 选择规则。

步骤 3 在规则的“添加注释”(Add Comment) 区域中点击**添加注释 (Add Comment)**。

步骤 4 在文本框中添加注释。

步骤 5 点击保存 (Save)。



编辑政策和规则集中有关规则的注释

编辑策略中的规则注释

使用此程序可编辑 FDM 管理 设备策略中的规则注释。

Procedure

步骤 1 从 CDO 菜单栏中，选择策略 (Policies) > FTD/Meraki/AWS 策略 (FTD/Meraki/AWS Policies)。

步骤 2 选择包含要添加注释的本地规则的 FDM 管理 设备策略。您无法为策略内的规则集中的规则添加注释。

步骤 3 在“注释”(Comment) 窗格中，点击编辑图标 。

步骤 4 编辑注释并点击“保存”(Save)。您会马上在“注释”(Comment) 区域中看到注释更改。

编辑规则集中规则的注释

要查看规则集中规则的注释更改（反映在策略页面上），则必须按特定顺序对注释和规则进行更改。

Procedure

步骤 1 从 CDO 导航面板中，选择策略 (Policies) > FTD 规则集 (FTD Rulesets)。

步骤 2 选择要为其添加注释的规则。

步骤 3 在“操作”(Actions) 窗格中，点击**编辑 (Edit)**。

步骤 4 选择规则。

步骤 5 在“注释”(Comment) 窗格中，点击编辑图标 。

步骤 6 编辑注释并点击“保存”(Save)。您会马上在规则集页面的“注释”(Comment) 区域中看到注释更改。

步骤 7 选择要更改的规则，然后在操作窗格中点击**编辑 (Edit)**。

步骤 8 编辑规则，然后点击蓝色复选按钮以保存更改。

步骤 9 在规则集页面的顶部，点击**保存 (Save)** 以保存规则集。规则集中该规则的新注释现在将显示在策略页面上。

步骤 10 要查看策略页面中的注释更改，请执行以下操作：

a) 从 CDO 菜单栏中，选择**策略 (Policies) > FTD/Meraki/AWS 策略 (FTD/Meraki/AWS Policies)**。

b) 选择包含您刚刚编辑的规则集的 FDM 管理设备策略。

c) 选择包含您刚刚编辑的注释的规则。您应该会在“注释”(Comment) 窗格中看到新的注释。

网络地址转换

IP 网络中的每台计算机和设备都分配了标识主机的唯一 IP 地址。因为缺乏公用 IPv4 地址，所以这些 IP 地址中的大多数都是专用地址，在专用公司网络以外的任何地方都不可路由。RFC 1918 定义可以在内部使用但不应通告的专用 IP 地址：

- 10.0.0.0 到 10.255.255.255
- 172.16.0.0 至 172.31.255.255
- 192.168.0.0 到 192.168.255.255

网络地址转换 (NAT) 的主要功能之一是使专用 IP 网络可以连接到互联网。NAT 用公用 IP 地址替换专用 IP 地址，将内部专用网络中的专用地址转换为可在公用互联网上使用的合法可路由地址。NAT 以此方式保存公用地址，因为它可配置为至少仅将整个网络的一个公用地址向外界通告。

NAT 的其他功能包括：

- 安全-隐藏内部 IP 地址可以阻止直接攻击。
- IP 路由解决方案-使用 NAT 时不会出现重叠 IP 地址。
- 灵活性-可以更改内部 IP 寻址方案，而不影响外部的可用公用地址；例如，对于可以访问互联网的服务器，可以维护供互联网使用的固定 IP 地址，但在内部，可以更改服务器地址。
- 在 IPv4 和 IPv6 之间转换（仅路由模式）- 如果想将 IPv6 网络连接到 IPv4 网络，可以利用 NAT 在两种类型的地址之间转换。

您可以使用 Cisco Defense Orchestrator 为许多不同的使用案例创建 NAT 规则。使用 NAT 规则向导或以下主题创建不同的 NAT 规则：

NAT 规则的处理顺序

网络对象 NAT 和两次 NAT 规则存储在划分为三部分的单个表中。首先应用第一部分规则，其次是第二部分，最后是第三部分，直到找到匹配项为止。例如，如果在第一部分找到匹配项，则不评估第二部分和第三部分。下表显示每个部分的规则顺序。

***Table 16: NAT* 规则表**

表部分	规则类型	部分中的规则顺序
第 1 部分	两次 NAT (ASA) 手动 NAT (FTD)	系统按照在配置中出现的顺序应用第一个匹配的规则。因为会应用第一个匹配规则，所以必须确保具体规则位于更加通用的规则前面，否则无法按预期应用特定规则。默认情况下，两次 NAT 规则会添加到第 1 部分。
第 2 部分	网络对象 NAT (ASA) 自动 NAT (FTD)	如果在第 1 部分未找到匹配项，则会按照以下顺序应用第 2 部分的规则： **1.** 静态规则。 **2.** 动态规则。 **在每个规则类型中，遵循以下排序准则：** **1.** 实际IP地址数量â€”从最小到最大。例如，带一个地址的对象将在带 10 个地址的对象之前进行评估。 **2.** 如果数量相同，则按从最低到最高的顺序使用 IP 地址编号。例如，10.1.1.0 在 11.1.1.0 之前进行评估。 **3.** 如果使用同一 IP 地址，则按字母数字顺序使用网络对象名称。例如，先评估对象“Arlington”，然后再评估对象“Detroit”。
第 3 部分	两次 NAT (ASA) 手动 NAT (FTD)	如果仍未找到匹配项，则按照在配置中出现的顺序，应用第三部分规则的第一个匹配项。此部分应当包含最通用的规则。还必须确保此部分的特定规则位于通用规则之前，否则会应用通用规则。

例如，对于第二部分规则，在网络对象中定义以下 IP 地址：

- 192.168.1.0/24（静态）
- 192.168.1.0/24（动态）
- 10.1.1.0/24（静态）

- 192.168.1.1/32（静态）
- 172.16.1.0/24（动态）（对象 Drtroit）
- 172.16.1.0/24（动态）（对象 Arlington）

结果排序可能是：

- 192.168.1.1/32（静态）
- 10.1.1.0/24（静态）
- 192.168.1.0/24（静态）
- 172.16.1.0/24（动态）（对象 Arlington）
- 172.16.1.0/24（动态）（对象 Drtroit）
- 192.168.1.0/24（动态）

网络地址转换向导

网络地址转换 (NAT) 向导可帮助您在设备上为以下类型的访问创建 NAT 规则：

- 为内部用户启用互联网访问。您可以使用此 NAT 规则允许内部网络上的用户访问互联网。
- 向互联网公开内部服务器。您可以使用此 NAT 规则允许网络外部的人员访问内部 Web 或邮件服务器。

“为内部用户启用互联网访问”的前提条件

在创建 NAT 规则之前，请收集以下信息：

- 最接近用户的接口；这通常称为“内部”接口。
- 离您的互联网连接最近的接口；这通常称为“外部”接口。
- 如果您只想允许特定用户访问互联网，则需要这些用户的子网地址。

“将内部服务器暴露给互联网”的必备条件

在创建 NAT 规则之前，请收集以下信息：

- 最接近用户的接口；这通常称为“内部”接口。
- 离您的互联网连接最近的接口；这通常称为“外部”接口。
- 要转换为面向互联网的 IP 地址的网络内服务器的 IP 地址。
- 您希望服务器使用的公共 IP 地址。

后续操作

请参阅使用 NAT 向导创建 NAT 规则, on page 402。

使用 NAT 向导创建 NAT 规则

Before you begin

有关使用 NAT 向导创建 NAT 规则所需的必备条件，请参阅。网络地址转换向导, on page 401

Procedure

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 使用过滤器和搜索字段查找要为其创建 NAT 规则的设备。

步骤 5 在详细信息面板的**管理 (Management)** 区域中，点击 **NAT** NAT。

步骤 6 点击 > NAT 向导。 

步骤 7 回答 NAT 向导问题并按照屏幕上的说明进行操作。

- NAT 向导创建规则。网络对象, on page 119从下拉菜单中选择现有对象，或使用创建按钮创建新对象。 + Create...
- 在保存 NAT 规则之前，需要将所有 IP 地址定义为网络对象。

步骤 8 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

NAT 常见使用案例

两次 NAT 和手动 NAT

以下是使用“网络对象 NAT”（也称为“自动 NAT”）可以实现的一些常见任务：

- 启用内部网络上的服务器以使用公共 IP 地址访问互联网， 第 403 页
- 使内部网络上的用户能够使用外部接口的公共 IP 地址访问互联网， 第 404 页
- 使内部网络上的服务器在公共 IP 地址的特定端口上可用， 第 405 页
- 将专用 IP 地址范围转换为公用 IP 地址范围， 第 408 页

网络对象 NAT 和自动 NAT

以下是使用“两次 NAT”（也称为“手动 NAT”）可以实现的常见任务：

• 防止在遍历外部接口时转换某个范围的 IP 地址 ， 第 409 页

启用内部网络上的服务器以使用公共 IP 地址访问互联网

使用案例

当您的服务器具有需要从互联网访问的私有 IP 地址，并且您有足够的公共 IP 地址将一个公共 IP 地址转换为私有 IP 地址时，请使用此 NAT 策略。如果您的公共 IP 地址数量有限，请参阅使内部网络上的服务器可供公共 IP 地址的特定端口上的用户使用（该解决方案可能更合适）。使内部网络上的服务器在公共 IP 地址的特定端口上可用, on page 405

战略

您的服务器具有静态专用 IP 地址，网络外部的用户必须能够访问您的服务器。创建将静态私有 IP 地址转换为静态公共 IP 地址的网络对象 NAT 规则。之后，创建允许来自该公共 IP 地址的流量到达专用 IP 地址的访问策略。最后，将这些更改部署到您的设备。

Before you begin

在开始之前，请创建两个网络对象。将一个对象命名为 servername _inside，将另一个对象命名为 _outside。servername _inside 网络对象应包含服务器的专用 IP 地址。servername _outside 网络对象应包含服务器的公共 IP 地址。有关说明，请参阅创建网络对象。网络对象, on page 119

Procedure

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要为其创建 NAT 规则的设备。

步骤 5 点击右侧**管理 (Management)** 窗格中的 **NAT**。

步骤 6 点击 > 网络对象 NAT。 

步骤 7 在第 1 部分中，**键入**选择**静态 (Static)**。点击**继续 (Continue)**。

步骤 8 在部分 2 中，为源接口选择内部，为目标接口选择外部。点击**继续 (Continue)**。

步骤 9 在第 3 部分“数据包”中，执行以下操作：

a. 展开 Original Address 菜单，点击 Choose，然后选择 servername_inside 对象。

b. 展开 Translated Address 菜单，点击 Choose，然后选择 servername_outside 对象。

步骤 10 跳过第 4 节“高级”。

步骤 11 对于 FDM 管理的设备，在部分 5 (Name) 中，为 NAT 规则指定名称。

步骤 12 点击**保存 (Save)**。

步骤 13 对于，部署网络策略规则，或者对于设备，部署访问控制策略规则，以允许流量从servername _inside 流向 servername _outside。ASAFDM 管理

步骤 14 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

使内部网络上的用户能够使用外部接口的公共 IP 地址访问互联网

使用案例

通过共享外部接口的公共地址，允许专用网络中的用户和计算机连接到互联网。

战略

创建端口地址转换 (PAT) 规则，允许专用网络上的所有用户共享设备的外部接口公共 IP 地址。

将私有地址映射到公有地址和端口号后，设备会记录该映射。当收到发往该公共 IP 地址和端口的传入流量时，设备会将其发送回请求它的私有 IP 地址。

Procedure

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要为其创建 NAT 规则的设备。

步骤 5 点击右侧**管理 (Management)** 窗格中的 **NAT**。

步骤 6 点击网络对象 NAT。 

步骤 7 在第 1 部分中，**键入**选择**动态 (Dynamic)**。点击**继续 (Continue)**。

步骤 8 在部分 2 中，为源接口选择 any，为目标接口选择 outside。点击**继续 (Continue)**。

步骤 9 在第 3 部分“数据包”中，执行以下操作：

a. 展开 Original Address 菜单，点击 Choose 并根据您的网络配置选择 any-ipv4 或 any-ipv6 对象。

b. 展开 Translated Address 菜单，然后从可用列表中选择 interface。接口指示使用外部接口的公共地址。

步骤 10 对于 Firepower 威胁防御 (FTD)，在部分 5 中，输入 NAT 规则的名称。

步骤 11 点击**保存 (Save)**。

步骤 12 立即 预览和部署所有设备的配置更改 您所做的更改，或等待并一次部署多个更改。

的已保存配置文件中的条目 **ASA**

以下是由于此程序而创建并显示在 的已保存配置文件中的条目。ASA

Note 这不适用于设备。FDM 管理

通过此程序创建的对象：

```
object network any_network
subnet 0.0.0.0 0.0.0.0
```

此程序创建的 *NAT* 规则：

```
object network any_network
nat (any,outside) dynamic interface
```

使内部网络上的服务器在公共 IP 地址的特定端口上可用

使用案例

如果您只有一个或非常有限的公共 IP 地址，则可以创建一个网络对象 NAT 规则，将绑定到静态 IP 地址和端口的入站流量转换为内部地址。我们提供了适用于特定情况的程序，但您可以将其用作其他受支持应用的模型。

前提条件

在开始之前，请创建三个单独的网络对象，分别用于 FTP、HTTP 和 SMTP 服务器。出于以下程序的考虑，我们将这些对象称为 ftp-server-object、http-server-object 和 smtp-server-object。有关说明，请参阅创建网络对象创建网络对象。创建或编辑 Firepower 网络对象或网络组, on page 120

到 FTP 服务器的 NAT 传入 FTP 流量

Procedure

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要为其创建 NAT 规则的设备。

步骤 5 点击右侧**管理 (Management)** 窗格中的 **NAT**。

步骤 6 点击 > 网络对象 NAT。 

步骤 7 在第 1 部分中，**键入**选择**静态 (Static)**。点击**继续 (Continue)**。

步骤 8 在部分 2 中（**接口**），为源接口选择**内部**，为目标接口选择**外部**。点击**继续 (Continue)**。

步骤 9 在第 3 部分**数据包**中，执行以下操作：

- 展开 Original Address 菜单，点击 **Choose**，然后选择 **ftp-server-object**。
- 展开 Translated Address 菜单，点击 **Choose**，然后选择 **Interface**。
- 选中**使用端口转换 (Use Port Translation)**。
- 选择 **tcp**、**ftp, ftp**。

步骤 10 跳过第 4 节**高级**。

步骤 11 对于 Firepower 威胁防御 (FTD)，请在第 5 部分**名称**中为 NAT 规则命名。

步骤 12 点击**保存 (Save)**。新规则在 NAT 表的NAT 规则的处理顺序中创建。

步骤 13 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

流向 HTTP 服务器的 NAT 传入 HTTP 流量

如果您只有一个或非常有限的公共 IP 地址，则可以创建一个网络对象 NAT 规则，将绑定到静态 IP 地址和端口的入站流量转换为内部地址。我们提供了适用于特定情况的程序，但您可以将其用作其他受支持应用的模型。

Before you begin

在开始之前，为 http 服务器创建网络对象。在本程序中，我们将调用对象 **http-object**。有关说明，请参阅创建或编辑 Firepower 网络对象或网络组。

Procedure

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要为其创建 NAT 规则的设备。

步骤 5 点击右侧**管理 (Management)** 窗格中的 **NAT**。

步骤 6 点击 + > **网络对象 NAT**。

步骤 7 在第 1 部分中，**键入**选择**静态 (Static)**。点击**继续 (Continue)**。

步骤 8 在部分 2 中（**接口**），为源接口选择**内部**，为目标接口选择**外部**。点击**继续 (Continue)**。

步骤 9 在第 3 部分**数据包**中，执行以下操作：

- 展开 Original Address 菜单，点击 **Choose**，然后选择 **http** 对象。
- 展开 Translated Address 菜单，点击 **Choose**，然后选择 **Interface**。
- 选中**使用端口转换 (Use Port Translation)**。
- 选择 **tcp**、**http**、http。

步骤 10 跳过第 4 节高级。

步骤 11 对于 Firepower 威胁防御 (FTD)，请在第 5 部分名称中为 NAT 规则命名。

步骤 12 点击保存 (Save)。新规则在 NAT 表的NAT 规则的处理顺序中创建。

步骤 13 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

到 SMTP 服务器的 NAT 传入 SMTP 流量

如果您只有一个或非常有限的公共 IP 地址，则可以创建一个网络对象 NAT 规则，将绑定到静态 IP 地址和端口的入站流量转换为内部地址。我们提供了适用于特定情况的程序，但您可以将其用作其他受支持应用的模型。

Before you begin

在开始之前，为 SMTP 服务器创建网络对象。在本程序中，我们将调用对象 **smtp-object**。有关说明，请参阅创建或编辑 Firepower 网络对象或网络组。

Procedure

步骤 1 在 CDO 导航栏中，点击清单 (Inventory)。

步骤 2 点击 设备 选项卡以查找设备，或点击 模板 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要为其创建 NAT 规则的设备。

步骤 5 点击右侧管理 (Management) 窗格中的 **NAT**。

步骤 6 点击  > 网络对象 NAT。

步骤 7 在第 1 部分中，键入选择静态 (Static)。点击继续 (Continue)。

步骤 8 在部分 2 中（接口），为源接口选择内部，为目标接口选择外部。点击继续 (Continue)。

步骤 9 在第 3 部分数据包中，执行以下操作：

- 展开 Original Address 菜单，点击 **Choose**，然后选择 smtp-server-object。
- 展开 Translated Address 菜单，点击 **Choose**，然后选择 **Interface**。
- 选中使用端口转换 (Use Port Translation)。
- 选择 **tcp**、**smtp**、**smtp**。

步骤 10 跳过第 4 节高级。

步骤 11 对于 Firepower 威胁防御 (FTD)，请在第 5 部分名称中为 NAT 规则命名。

步骤 12 点击保存 (Save)。新规则在 NAT 表的NAT 规则的处理顺序中创建。

步骤 13 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

将专用 IP 地址范围转换为公用 IP 地址范围

使用案例

如果您有一组特定设备类型或用户类型，需要将其 IP 地址转换为特定范围，以便接收设备（事务另一端的设备）允许流量传入。

将内部地址池转换为外部地址池

Before you begin

为要转换的私有 IP 地址池创建网络对象，并为要将这些私有 IP 地址转换为的公有地址池创建网络对象。

Note 对于 FTD，定义“转换后的地址”池的网络组不能是定义子网的网络对象。ASA

创建这些地址池时，请使用 Create or Edit ASA Network Objects and Network Groups use Create or Edit a Firepower Network Object or Network Groups 了解相关说明。创建或编辑 Firepower 网络对象或网络组, on page 120

出于以下程序的考虑，我们将私有地址池命名为 inside_pool，将公共地址池命名为 outside_pool。

Procedure

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要为其创建 NAT 规则的设备。

步骤 5 点击右侧**管理 (Management)** 窗格中的 **NAT**。

步骤 6 点击 > 网络对象 NAT。 

步骤 7 在第 1 部分“类型”中，选择“动态”，然后点击“继续”。

步骤 8 在第 2 部分**接口 (Interfaces)** 中，为源接口选择**内部**内部，为目标接口选择**外部**。点击**继续 (Continue)**。

步骤 9 在部分 3 数据包中，执行以下任务：

- 对于 Original Address，请点击 Choose，然后选择您在上述前提条件部分中创建的 inside_pool 网络对象（或网络组）。
- 对于 Translated Address，点击 Choose，然后选择您在上述前提条件部分中创建的 outside_pool 网络对象（或网络组）。

步骤 10 跳过第 4 节“高级”。

步骤 11 对于 Firepower 威胁防御 (FTD)，请在第 5 部分“名称”中为 NAT 规则命名。

步骤 12 点击**保存 (Save)**。

步骤 13 立即 预览和部署所有设备的配置更改 您所做的更改，或等待并一次部署多个更改。

防止在遍历外部接口时转换某个范围的 IP 地址

使用案例

使用此两次 NAT 使用案例启用站点间 VPN。

策略

您将 IP 地址池转换为自身，以便网络上一个位置的 IP 地址到达另一个位置时保持不变。

创建两次 NAT 规则

Before you begin

创建定义要转换为自身的IP地址池的网络对象或网络组。对于FTD，地址范围可以通过定义子网的网络对象或包含该范围内所有地址的网络组对象来定义。

创建网络对象或网络组时，请使用创建或编辑 Firepower 网络对象或网络组获取说明。

在以下程序中，我们将调用网络对象或网络组，即站点间 PC 池。

Procedure

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要为其创建 NAT 规则的设备。

步骤 5 点击右侧**管理 (Management)** 窗格中的 **NAT**。

步骤 6 点击  > **两次 NAT (Twice NAT)**。。

步骤 7 在第 1 部分中，**键入**选择**静态 (Static)**。点击**继续 (Continue)**。

步骤 8 在部分 2 中（**接口**），为源接口选择**内部**，为目标接口选择**外部**。点击**继续 (Continue)**。

步骤 9 在第 3 部分**数据包**中，进行以下更改：

- 展开原始地址菜单，点击**Choose**，然后选择您在先决条件部分中创建的站点到站点PC池对象。
- 展开 Translated Address 菜单，点击 **Choose**，然后选择您在前提条件部分中创建的 Site-to-Site-PC-Pool 对象。

步骤 10 跳过第 4 节**高级**。

步骤 11 对于 Firepower 威胁防御 (FTD)，请在第 5 部分**名称**中为 NAT 规则命名。

步骤 12 点击**保存 (Save)**。

步骤 13 为 ASA 创建一个加密映射。有关创建加密映射的详细信息，请参阅 CLI 手册 3：思科 ASA 系列 VPN CLI 配置指南并查看 LAN 到 LAN IPsec VPN 一章。https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

步骤 14 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

虚拟专用网络管理

虚拟专用网络 (VPN) 连接在使用公共网络（如互联网）的终端之间建立安全隧道。

本节适用于 FDM 托管设备上的远程访问和站点间 VPN。它介绍了在 FTD 上构建站点间 VPN 连接的互联网协议安全 (IPsec) 标准。它还介绍了用于在 ASA FTD 上构建和远程访问 VPN 连接的 SSL 标准。

CDO 支持以下几种类型的 VPN 配置：

- 站点间虚拟专用网络 ， 第 410 页
- 远程访问虚拟专用网络

有关虚拟专用网络的其他信息，请参阅适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南。

站点间虚拟专用网络

站点间 VPN 隧道可连接不同地理位置的网络。您可以在托管设备之间以及托管设备与其他符合所有相关标准的思科或第三方对等体之间创建站点间的 IPsec 连接。这些对等体可以采用内部和外部 IPv4 和 IPv6 地址的任意组合。站点间隧道使用 Internet Protocol Security (IPsec) 协议套件或网络密钥交换版本 2 (IKEv2) 构建。建立 VPN 连接之后，本地网关后台的主机可通过安全 VPN 隧道连接至远程网关后台的主机。

VPN 拓扑

要创建一个新的站点间 VPN 拓扑，至少必须为其指定一个唯一名称，指定拓扑类型，选择用于 IPsec IKEv1 和/或 IKEv2 的 IKE 版本。配置完毕后，可以将拓扑部署到 FTD。

IPsec 和 IKE

在 CDO 中，站点间 VPN 是根据分配给 VPN 拓扑的 IKE 策略和 IPsec 建议配置的。策略和建议是定义站点到站点 VPN 的特性的参数集，例如用于在 IPsec 隧道中保护流量安全的安全协议和算法。可能需要多种策略类型来定义可以分配给 VPN 拓扑的完整配置映像。

身份验证

要对VPN连接进行身份验证，请在每个设备上拓扑中配置预共享密钥。预共享密钥允许在两个对等体之间共享安全密钥，该共享密钥在 IKE 身份验证阶段使用。

虚拟隧道接口 (VTI)

CDO 当前不支持在 FTD 上管理、监控或使用虚拟隧道接口 (VTI) 隧道。已配置 VTI 隧道的设备可以载入 CDO，但它会忽略 VTI 接口。如果安全区域或静态路由引用 VTI，则 CDO 会读取不带 VTI 引用的安全区域和静态路由。即将推出对 VTI 隧道的 CDO 支持。

相关信息：

- 为 FDM 管理 设备配置站点间 VPN, on page 411
- 监控 FDM 管理 设备 站点间虚拟专用网络

为 FDM 管理 设备配置站点间 VPN

思科防御协调器 (CDO) 支持 FDM 管理 设备上的站点间 VPN 功能：

- 支持 IPsec IKEv1 和 IKEv2 协议。
- 用于身份验证的自动或手动预共享密钥。
- IPv4 和 IPv6。支持内部和外部的所有组合。
- IPsec IKEv2 站点间 VPN 拓扑提供符合安全认证的配置设置。
- 静态和动态接口。
- 支持作为终端的外联网设备的动态 IP 地址。

外部网设备

每种拓扑类型都可以包括外部网设备，即不在 CDO 中管理的设备。其中包括：

- CDO支持但您的组织不负责的思科设备。例如，由您公司内的其他部门管理的网络中的分支，或者与服务提供商或合作伙伴的网络的连接。
- 非托管设备。不能使用CDO创建配置以及将配置部署到非托管设备。将非托管设备作为“外联网”设备添加到 VPN 拓扑。此外，还指定每个远程设备的 IP 地址。

配置与动态寻址对等体的站点间 VPN 连接

如果其中一个对等体的 VPN 接口 IP 地址未知或接口从 DHCP 服务器获取其地址，CDO 允许您在对等体之间创建站点间 VPN 连接。预共享密钥、IKE 设置和 IPsec 配置与另一个对等体匹配的任何动态对等体都可以建立站点间 VPN 连接。

假设有两个对等体 A 和 B。静态对等体是其 VPN 接口为固定 IP 地址的设备，而动态对等体是其 VPN 接口为未知 IP 地址或具有临时 IP 地址的设备。

以下使用案例介绍了与动态寻址对等体建立安全站点间 VPN 连接的不同场景：

- A 是静态对等体，而 B 是动态对等体，反之亦然。
- A 是静态对等体，而 B 是具有来自 DHCP 服务器的已解析 IP 地址的动态对等体，反之亦然。您可以选择**将 VPN 绑定到分配的 IP (Bind VPN to the assigned IP)**，以便在静态对等体的 IP 地址和动态对等体的 DHCP 分配的 IP 地址之间建立 VPN 连接。
- A 和 B 是动态的，具有来自 DHCP 服务器的已解析 IP 地址。在这种情况下，必须为至少一个对等体选择**将 VPN 绑定到分配的 IP (Bind VPN to the assigned IP)**，以便在静态对等体的 IP 地址和动态对等体的 DHCP 分配 IP 地址之间建立 VPN 连接。
- A 是动态对等体，而 B 是具有静态或动态 IP 地址的外联网设备。
- A 是具有来自 DHCP 服务器的已解析 IP 地址的动态对等体，而 B 是具有静态或动态 IP 地址的外联网设备。您可以选择**将 VPN 绑定到分配的 IP (Bind VPN to the assigned IP)**，以便在静态对等体的 IP 地址和动态对等体的 DHCP 分配的 IP 地址之间建立 VPN 连接。

Important 如果选择**将 VPN 绑定到分配的 IP (Bind VPN to the assigned IP)**，则 VPN 会静态绑定到 DHCP 分配的 IP 地址。但是，在对等体重新启动后，该动态接口就可以接收许多新的 IP 地址。虽然 VPN 隧道会更新新的 IP 地址，但另一个对等体不会使用新的配置来更新。您必须再次部署站点间配置，以便在另一个对等体上实现带外更改。

Note 如果使用 防火墙设备管理器 等本地管理器更改了接口的 IP 地址，则 CDO 中该对等体的**配置状态**会显示“检测到冲突”。当您解决配置冲突时，其他对等体的**配置状态 (Configuration Status)** 会变成“未同步”(Not Synced) 状态。您必须将 CDO 配置部署到处于“未同步”(Not Synced) 状态的设备。

通常，连接必须由动态对等体发起，因为另一个对等体不知道动态对等体的 IP 地址。当远程对等体尝试建立连接时，另一个对等体会使用预共享密钥、IKE 设置和 IPsec 配置来验证连接。

由于只有在远程对等体发起连接之后才会建立VPN连接，因此在连接建立之前，系统会丢弃与允许流量通过 VPN 隧道的访问控制规则匹配的出站流量。这可确保数据不会在未采取适当加密和 VPN 保护措施的情况下离开您的网络。

Note 在以下情况下，无法配置站点间 VPN 连接：

- 如果两个对等体都有 DHCP 分配的 IP 地址。
  - **解决方法**：如果其中一个对等体有从 DHCP 服务器获取的已解析 IP 地址，则可以配置站点间 VPN。在这种情况下，您必须选择**将 VPN 绑定到分配的 IP (Bind VPN to the assigned IP)** 以配置站点间 VPN。
- 如果设备有多个动态对等体连接。

- **解决方法**：您可以通过执行以下步骤来配置站点间 VPN：
  - 考虑三台设备 A、B 和 C。
  - 配置 A（静态对等体）和 B（动态对等体）之间的站点间 VPN 连接。
  - 通过创建外联网设备来配置 A 和 C（动态对等体）之间的 VPN 连接。将 A 的静态 VPN 接口 IP 地址分配给外联网设备，并与 C 建立连接。

FDM 管理站点间 VPN 准则和限制

- CDO 不支持使用 crypto-acl 来设计 S2S VPN 需要关注的流量。它仅支持受保护的网络。
- CDO 当前不支持在 ASA 或 FDM 管理 设备上管理、监控或使用虚拟隧道接口 (VTI) 隧道。已配置 VTI 隧道的设备可以载入 CDO，但它会忽略 VTI 接口。如果安全区域或静态路由引用 VTI，则 CDO 会读取不带 VTI 引用的安全区域和静态路由。VTI 隧道的 CDO 支持即将推出。
- 只要使用的是 IKE 端口 500/4500，或者有一些 PAT 转换处于活动状态，则无法在同一端口上配置站点间 VPN，因为无法在这些端口上启动服务。
- 不支持传输模式，仅支持隧道模式。IPsec 隧道模式对整个原始 IP 数据报进行加密，使其成为新 IP 数据包中的负载。当防火墙对出入位于防火墙后的主机的流量进行保护时，请使用隧道模式。在通过不可信网络（例如互联网）连接的两个防火墙（或其他安全网关）之间，通常采用隧道模式实施常规 IPsec。
- 对于此版本，仅支持包含一个或多个 VPN 隧道的 PTP 拓扑。点对点 (PTP) 部署在两个终端之间建立 VPN 隧道。

相关信息：

- 创建站点间 VPN
- 编辑现有 CDO 站点间 VPN
- VPN 中使用的加密和散列算法
- 使站点间 VPN 流量豁免 NAT

创建站点间 VPN

您可以通过以下两种方法之一创建站点间 VPN：简单配置和高级配置。在简单配置中，默认配置用于建立站点间 VPN 连接。您可以在**高级 (Advanced)** 模式下修改配置。

每种站点间 VPN 拓扑类型都可以包括外部网设备，即不在 CDO 中管理的设备。外部网设备可以是任何设备（思科或第三方设备），并非由 CDO 管理。

对于此版本，仅支持 PTP 拓扑，每个站点间连接包含一个隧道。点对点 (PTP) 部署在两个终端之间建立 VPN 隧道。

相关信息：

- 使用简单配置创建站点间 VPN, on page 414

- 使用高级配置创建站点间 VPN, on page 415
- 为站点间对等体之间的受保护流量配置网络, on page 417

使用简单配置创建站点间 *VPN*

Procedure

步骤 1 在导航窗格中，选择 **VPN** > **站点间 VPN**。

步骤 2 点击蓝色加号  按钮以创建 VPN 隧道。

Note 或者，您可以从**清单 (Inventory)** 页面创建站点间 VPN 连接。

a. 在导航栏中，点击**清单 (Inventory)**。

b. 选择要配置的两个 FDM 管理 设备。如果选择外联网设备，请指定外联网设备的 IP 地址。

c. 在右侧页面的**设备操作 (Device Actions)** 下，点击**创建站点间 VPN (Create Site-to-Site VPN)**。

步骤 3 输入唯一的拓扑**配置名称**。我们建议命名您的拓扑以指示它是一个 FDM 管理 设备 VPN，并指定其拓扑类型。

步骤 4 从“设备”(Devices) 中选择此 VPN 部署的终端设备。

步骤 5 如果您在**对等体 2 (Peer 2)** 中选择了一个外联网设备，请选择**静态 (Static)** 并指定 IP 地址，或者为使用 DHCP 分配 IP 的外联网设备选择**动态 (Dynamic)**。**IP 地址 (IP Address)** 显示静态接口的 IP 地址或为动态接口**分配的 DHCP** 。

步骤 6 为终端设备选择 **VPN 访问接口 (VPN Access Interface)** 。

Note 如果一个或两个终端设备具有动态 IP 地址，请参阅配置与动态寻址对等体的站点间 VPN 连接以获取额外说明。

步骤 7 点击蓝色加号按钮  ，为参与的设备添加**受保护的网络**。

步骤 8 （可选）选择 **NAT 免除 (NAT Exempt)** 以便从本地 VPN 访问接口的 NAT 策略中免除 VPN 流量。必须为单个对等体手动配置。如果不想将 NAT 规则应用于本地网络，请选择托管本地网络的接口。此选项仅在本地网络驻留在单个路由接口（而非网桥组成员）后时有用。如果本地网络位于多个路由接口或一个或多个网桥组成员之后，则必须手动创建 NAT 豁免规则。有关手动创建所需规则的信息，请参阅 使站点间 VPN 流量豁免 NAT 。

步骤 9 点击**创建 VPN (Create VPN)**，然后点击**完成 (Finish)**。

步骤 10 执行其他强制性配置。请参阅为站点间对等体之间的受保护流量配置网络。

已配置站点间 VPN。

使用高级配置创建站点间 *VPN*

Procedure

步骤 1 在导航栏上，选择 **VPN**。

步骤 2 点击蓝色加号  按钮以创建 VPN 隧道。

步骤 3 在**对等设备**部分中，指定以下设备配置：

a. 输入唯一的拓扑**配置名称**。我们建议命名您的拓扑以指示它是一个 FDM 管理 设备 VPN，并指定其拓扑类型。

b. 从“设备”(Devices) 中选择此 VPN 部署的终端设备。

c. 如果您选择了一个外联网设备，请选择**静态 (Static)** 并指定 IP 地址，或者为使用 DHCP 分配 IP 的外联网设备选择**动态 (Dynamic)**。**IP 地址 (IP Address)** 显示静态接口的 IP 地址或为动态接口**分配的 DHCP** 。

d. 为终端设备选择 **VPN 访问接口 (VPN Access Interface)**。

Note 如果一个或两个终端设备具有动态IP地址，请参阅配置与动态寻址对等体的站点间VPN连接以获取额外说明。

步骤 4 点击蓝色加号按钮  ，为参与的设备添加**受保护的网络**。

步骤 5 点击 **Advanced**。

步骤 6 在 **IKE 设置 (IKE Settings)** 部分中，选择要在互联网密钥交换 (IKE) 协商期间使用的 IKE 版本，并指定隐私配置：有关 IKE 策略的详细信息，请参阅配置全局 IKE 策略, on page 143。

Note IKE 策略对设备是全局的，并应用于与其关联的所有 VPN 隧道。因此，添加或删除策略会影响此设备参与的所有 VPN 隧道。

a. 根据需要选择一个或两个选项。

Note 默认情况下，**IKEV 版本 2** 和 **IKEV2 POLICIES** 出于启用状态。

b. 点击蓝色加号  按钮，然后选择 IKEv2 策略。

点击**创建新的 IKEv2 策略 (Create New IKEv2 Policy)** 以创建新的 IKEv2 策略。或者，您可以转到 CDO 导航栏并点击 **对象 (Objects) > FDM 对象 (FDM Objects)**，然后点击  > **IKEv2 策略 (IKEv2 Policy)**。有关创建新 IKEv2 策略的详细信息，请参阅管理 IKEv2 策略。要删除现有 IKEv2 策略，请将鼠标悬停在所选的策略上，然后点击 **x** 图标。

c. 点击 **IKE 版本 1 (IKE Version 1)** 将其启用。

d. 点击蓝色加号  按钮，然后选择 IKEv1 策略。点击**创建新的 IKEv1 策略 (Create New IKEv1 Policy)** 以创建新的 IKEv1 策略。或者，您可以转到 CDO 导航栏并点击 **对象 (Objects) > FDM 对**

象 (FDM Objects)，然后点击  > **IKEv1 策略 (IKEv1 Policy)**。有关创建新 IKEv1 策略的详细信息，请参阅管理 IKEv1 策略。要删除现有 IKEv1 策略，请将鼠标悬停在所选策略上，然后点击 **x** 图标。

e. 输入参与设备的**预共享密钥**。预共享密钥是在连接中的每个对等体上配置的加密密钥字符串。这些密钥由 IKE 在身份验证阶段使用。

- (IKEv2) **对等体 1 预共享密钥、对等体 2 预共享密钥**：对于 IKEv2，您可以在每个对等体上配置唯一的密钥。输入**预共享密钥 (Pre-shared Key)**。您可以点击**显示覆盖 (Show Override)** 按钮，并为对等体输入适当的预共享。该密钥可以有 1 至 127 个字母数字字符。下表介绍了两个对等体的预共享密钥的用途。

	本地预共享密钥	远程对等预共享密钥
对等体 1	对等体 1 预共享密钥	对等体 2 预共享密钥
对等体 2	对等体 2 预共享密钥	对等体 1 预共享密钥

- (IKEv1) **预共享密钥**：对于 IKEv1，您必须在每个对等体上配置相同的预共享密钥。该密钥可以有 1 至 127 个字母数字字符。在此场景中，对等体 1 和对等体 2 使用相同的预共享密钥加密和解密数据。

f. 点击**下一步**。

步骤 7 在 **IPSec 设置 (IPSec Settings)** 部分中，指定 IPSec 配置。相应的 IKEV 提议是否可用，具体取决于在 **IKE 设置**步骤中所做的选择。

有关 IPSec 设置的详细信息，请参阅配置 IPsec 提议, on page 140。

a. 点击蓝色加号  按钮，然后选择 IKEv2 提议。要删除现有的 IKEv2 提议，请将鼠标悬停在所选提议上，然后点击 **x** 图标。

Note 点击“创建新的 IKEv2 提议”(Create New IKEv2 Proposal) 以创建新的 IKEv2 提议。或者，您可以转到 CDO 导航栏并点击 **对象 (Objects) > FDM 对象 (FDM Objects)**，然后点击  > **IKEv2 IPSec 提议 (IKEv2 IPSec Proposal)**。

有关创建新 IKEv2 策略的详细信息，请参阅管理 IKEv2 IPsec 提议对象。

b. 选择**适用于完全向前保密的 Diffie-Hellman 组 (Diffie-Hellman Group for Perfect Forward Secrecy)**。有关详细信息，请参阅决定要使用的 Diffie-Hellman 模数组。

c. 点击**创建 VPN**。

d. 阅读配置，如果满意，请点击**完成 (Finish)**。

e. 执行其他强制性配置。请参阅为站点间对等体之间的受保护流量配置网络。

为站点间对等体之间的受保护流量配置网络

完成站点间连接的配置后，请确保对 VPN 执行以下配置，以便在所有目标设备上运行。

Procedure

步骤 1 配置 AC 策略：

配置 AC 策略，用于允许两个对等体后面的受保护网络之间的双向流量。这些策略可帮助数据包到达预期目的地而不会被丢弃。

Note 您必须为两个对等体上的传入和传出流量创建 AC 策略。

a. 在左侧的 思科防御协调器 导航栏中，点击**策略 (Policies)** 并选择所需的选项。

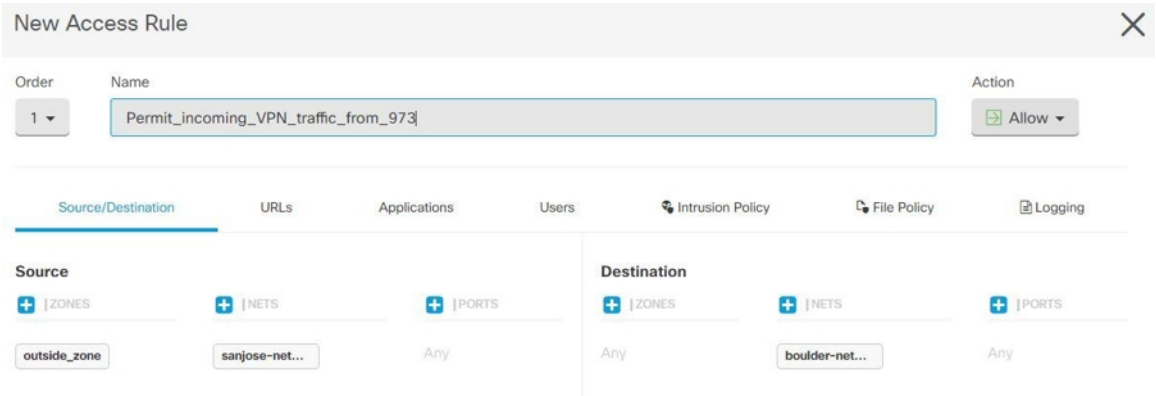
b. 为两个对等体上的传入和传出流量创建策略。有关创建 AC 策略的详细信息，请参阅配置 FDM 访问控制策略。

以下示例显示了在两个对等体上创建 AC 策略的步骤。

考虑两个 FDM 管理 设备“FTD_BGL_972”和“FTD_BGL_973”，它们分别在两个受保护的网络“boulder-network”和“sanjose-network”之间建立了站点间 VPN 连接。

创建允许传入流量的 *AC* 策略：

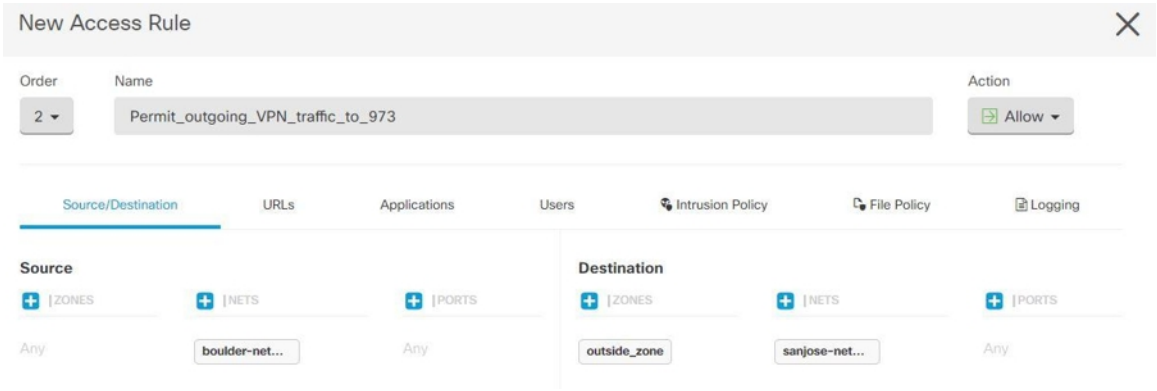
策略“Permit_incoming_VPN_traffic_from_973”是在“FTD_BGL_972”设备上创建的，用于允许来自对等体 (“FTD_BGL_973”) 的传入流量。



- **源区域 (Source Zone)**：设置产生网络流量的对等设备的区域。在本示例中，流量源自 FTD_BGL_973 并到达 FTD_BGL_972。
- **源网络 (Source Network)**：设置发起网络流量的对等设备的受保护网络。在本例中，流量源自“sanjose-network”，这是对等设备 (FTD_BGL_973) 背后的受保护网络。
- **目标网络**：设置网络流量到达的设备的受保护网络。在本例中，流量到达“boulder-network”，这是对等设备 (FTD_BGL_972) 背后的受保护网络。**注意**：其余字段可以使用默认值（“任意”）。
- 将**操作 (Action)** 设置为**允许 (Allow)** 以便流量不受策略中的入侵及其他检测设置约束。

创建允许传出流量的 *AC* 策略：

策略“Permit_outgoing_VPN_traffic_to_973”是在“FTD_BGL_972”设备上创建的，用于允许向对等体 (“FTD_BGL_973”) 传出流量。



- **源网络 (Source Network)**：设置发起网络流量的对等设备的受保护网络。在本例中，流量源自“boulder-network”，这是对等设备 (FTD_BGL_972) 背后的受保护网络。
- **目标区域 (Destination Zone)**：设置网络流量到达的对等设备的区域。在本示例中，流量从 FTD_BGL_972 到达并到达 FTD_BGL_973。
- **目标网络 (Destination Network)**：设置网络流量到达的对等体的受保护网络。在本例中，流量到达“sanjose-network”，这是对等设备 (FTD_BGL_972) 背后的受保护网络。**注意**：其余字段可以使用默认值（“任意”）。
- 将**操作 (Action)** 设置为**允许 (Allow)** 以便流量不受策略中的入侵及其他检测设置约束。

在一台设备上创建 AC 策略后，您必须在其对等设备上创建类似的策略。

步骤 2 如果在任一对等设备上配置了 NAT，则您需要手动配置 NAT 豁免规则。请参阅使站点间 VPN 流量豁免 NAT 。

步骤 3 配置每个对等体上接收返回 VPN 流量的路由。有关详细信息，请参阅为 FDM 管理 设备配置静态路由和默认路由。

a. **网关 (Gateway)** - 选择标识网关 IP 地址的主机网络对象至目标网络。流量将发送至此地址。

b. **接口 (Interface)** - 选择要通过其发送流量的接口。在本例中，流量通过“外部”接口发送。

c. **目标网络 (Destination Networks)** - 选择一个或多个标识目标网络的网络对象。在本例中，目的地是对等设备 (FTD_BGL_973) 后面的“sanjose-network”。

在一台设备上配置路由设置后，您必须在其对等设备上配置类似的设置。

编辑现有 CDO 站点间 VPN

默认情况下，使用高级配置向导修改现有站点间 VPN 配置。

Procedure

步骤 1 在导航栏上，选择 **VPN** > **站点间 VPN (Site-to-Site VPN)**。

步骤 2 选择要编辑的所需站点间 VPN 隧道。

步骤 3 在**操作 (Actions)** 窗格中，点击 **编辑 (Edit)**。

Note 或者，您可以执行以下操作来编辑配置：

a. 打开 VPN 页面，然后点击过滤器面板中的**全局视图 (Global View)** 按钮（有关详细信息，请参阅搜索和过滤器站点间 VPN 隧道）。

系统将显示所有设备上可用的所有站点间 VPN 隧道。

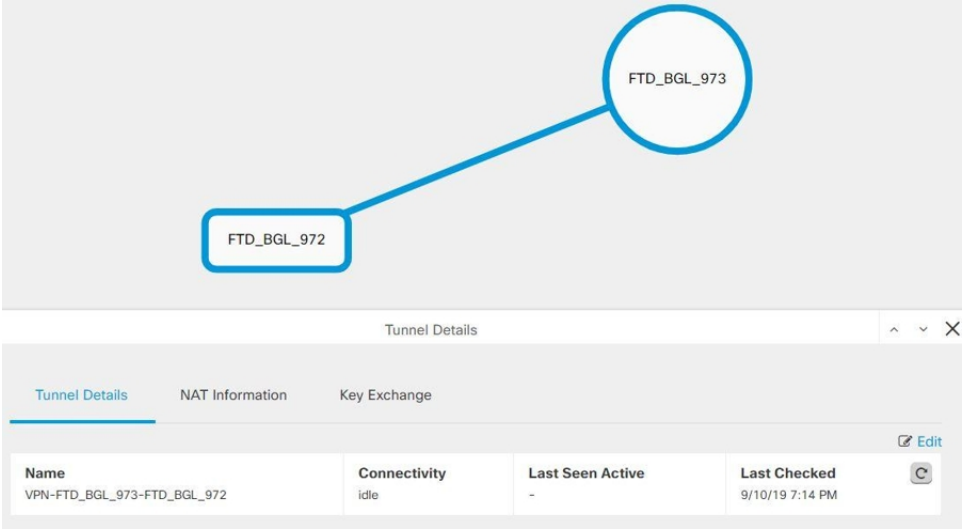
要编辑配置，其中一个对等体必须是 FDM 管理 设备。

b. 通过点击框选择设备。

c. 点击**查看详细信息 (View details)** 以查看其对等体。

d. 点击对等设备以查看隧道详细信息。

您可以查看与设备相关的隧道详细信息、NAT 信息和密钥交换信息。



e. 点击**隧道详细信息 (Tunnel Details)** 中的**编辑 (Edit)** 。

步骤 4 在**对等设备 (Peer Devices)** 部分中，您可以修改以下设备配置：配置名称、VPN 访问接口和受保护的网络。

Note 您无法更改参与设备。

步骤 5 在 **IKE 设置 (IKE Settings)** 部分中，您可以修改以下 IKEv2 策略配置：

a. 点击相应设备的蓝色加号  按钮，然后选择新的 IKEv2 策略。要删除现有 IKEv2 策略，请将鼠标悬停在所选策略上，然后点击 **x** 图标。

b. 修改参与设备的**预共享密钥 (Pre-Shared Key)**。如果终端设备的预共享密钥不同，请点击蓝色设置  按钮，然后输入设备的相应预共享密钥。

c. 点击**下一步**。

步骤 6 在 **IPSec 设置 (IPSec Settings)** 部分中，您可以修改以下 IPSec 配置：

a. 点击蓝色加号  按钮以选择新的 IKEv2 提议。要删除现有的 IKEv2 提议，请将鼠标悬停在所选提议上，然后点击 **x** 图标。

b. 选择 **适用于完全向前保密的 Diffie-Hellman 组**。

c. 点击**编辑 VPN (Edit VPN)**，然后点击**完成 (Finish)**。

点对点 VPN 将使用您所做的所有更改进行修改和更新。

删除现有 *CDO* 站点间 *VPN*

Procedure

步骤 1 在导航栏上，选择 **VPN> ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

步骤 2 选择要删除的所需站点间 VPN 隧道。

步骤 3 在**操作 (Actions)** 窗格中，点击**删除 (Delete)**。

所选站点间 VPN 隧道将被删除。

VPN 中使用的加密和散列算法

由于VPN隧道通常流经公共网络（最可能是互联网），因此您需要对连接进行加密以保护流量。可以使用 IKE 策略和 IPsec 提议定义要应用的加密和其他安全技术。

如果您的设备许可证允许应用较强的加密，则有大量的加密和散列算法以及Diffie-Hellman组供您选择。然而，通常情况下，应用于隧道的加密越强，系统性能越差。您要在安全性和性能之间实现平衡，在提供充分保护的同时不牺牲效率。

我们无法就选择哪些选项提供具体指导。如果您在大型公司或其他组织执行运营，可能已有需要满足的指定标准。如果没有，请花些时间研究各个选项。

下面的主题介绍了几个可用选项：

决定使用哪个加密算法

在决定用于 IKE 策略或 IPsec 提议的加密算法时，您的选择仅限于 VPN 中的设备所支持的算法。

对于 IKEv2，您可以配置多个加密算法。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

对于 IPsec 提议，该算法用于封装安全协议 (ESP)，该协议提供身份验证、加密和防重放服务。ESP 为 IP 协议类型 50。在 IKEv1 IPsec 提议中，算法名称以 ESP 为前缀。

如果设备许可证符合强加密要求，可以从以下加密算法中选择。如果不符合强加密要求，则只能选择 DES。

- AES-GCM -（仅限 IKEv2。）Galois/Counter 模式中的高级加密标准是提供机密性和数据源身份验证的分组加密操作模式，并且提供比 AES 更高的安全性。AES-GCM 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。密钥越长，其提供的安全性就越高，但性能会随之降低。GCM 是支持 NSA Suite B 所需的 AES 模式。NSA Suite B 是一套加密算法，设备必须支持这套算法才能满足密码强度的联邦标准。
- AES-GMAC -（仅限 IKEv2 IPsec 提议。）高级加密标准 Galois 消息身份验证代码是仅提供数据源身份验证的分组加密操作模式。它是 AES-GCM 的一个变体，允许在不加密数据的情况下进行数据身份验证。AES-GMAC 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。
- AES - 高级加密标准是一种对称密码算法，提供比 DES 更高的安全性，在计算上比 3DES 更高效。AES 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。密钥越长，其提供的安全性就越高，但性能会随之降低。
- DES - 数据加密标准，使用 56 位密钥进行加密，是一种对称密钥块算法。如果您的许可证账户不符合导出控制要求，这将是您唯一的选择。此算法比 3DES 快且使用的系统资源更少，但安全性也较低。如果不需要很强的数据保密性，并且系统资源或速度存在问题，请选择 DES。
- 3DES - 三重 DES，使用 56 位密钥加密三次，比 DES 更加安全，因其使用不同密钥对每个数据块处理三次。不过，此算法比 DES 使用的系统资源更多且速度更慢。
- NULL - 空加密算法提供不加密的身份验证。这通常仅用于测试目的。

决定使用哪些散列算法

在 IKE 策略中，散列算法创建消息摘要，用于确保消息的完整性。在 IKEv2 中，散列算法分成两个选项，一个用于完整性算法，一个用于伪随机函数 (PRF)。

在 IPsec 提议中，散列算法由封装安全协议 (ESP) 用于身份验证。在 IKEv2 IPsec 提议中，这称为完整性散列。在 IKEv1 IPsec 提议中，算法名称以 ESP- 为前缀，并且还有 -HMAC 后缀（代表“散列方法身份验证代码”）。

对于 IKEv2，您可以配置多个散列算法。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

您可以选择以下散列算法：

- SHA （安全散列算法）- 生成 160 位摘要的标准 SHA (SHA-1)。SHA 抗暴力攻击的能力高于 MD5。但是，它也比 MD5 占用更多资源。对于需要最高级别安全性的实施，请使用 SHA 散列算法。
- 以下 SHA-2 选项更加安全，可用于 IKEv2 配置。如果要实施 NSA Suite B 加密规范，请选择以下选项之一。
  - SHA-256 - 指定具有 256 位摘要的安全散列算法 SHA-2。
  - SHA-384 - 指定具有 384 位摘要的安全散列算法 SHA-2。
  - SHA-512 - 指定具有 512 位摘要的安全散列算法 SHA-2。
- MD5（消息摘要 5）- 生成 128 位的摘要。MD5 能使用更少的处理时间实现比 SHA 更快的整体性能，但 MD5 被认为安全性低于 SHA。
- 空或无（NULL、ESP-NONE） -（仅限 IPsec 提议。）空散列算法；这通常仅用于测试目的。但是，如果选择 AES-GCM/GMAC 选项之一作为加密算法，则应选择空完整性算法。即使选择非空选项，这些加密标准也会忽略完整性散列。

决定要使用的 Diffie-Hellman 模数组

您可以使用以下 Diffie-Hellman 密钥导出算法生成 IPsec 安全关联 (SA) 密钥。每组具有不同的长度模数。模数更大则安全性越高，但需要更多的处理时间。两个对等体上必须具有一个匹配的模数组。

如果选择 AES 加密，要支持 AES 所需的大型密钥长度，应使用 Diffie-Hellman (DH) 组 5 或更高组。IKEv1 策略不支持下面列出的所有组。

要实施 NSA Suite B 加密规范，请使用 IKEv2 并选择椭圆曲线 Diffie-Hellman (ECDH) 的一个选项：19、20 或 21。使用 2048 位模数的椭圆曲线选项和组较少遭受 Logjam 等攻击。

对于 IKEv2，您可以配置多个组。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

- 2 - Diffie-Hellman 组 2：1024 位模幂算法 (MODP) 组。此选项不再是一种良好的保护措施。
- 5 - Diffie-Hellman 组 5：1536 位 MODP 组。曾经被认为可以良好地保护 128 位密钥，如今却不再是一种良好的保护措施。
- 14 - Diffie-Hellman 组 14：2048 位模幂算法 (MODP) 组。被认为可以良好地保护 192 位密钥。
- 19 - Diffie-Hellman 组 19：美国国家标准与技术研究所 (NIST) 256 位椭圆曲线取素数 (ECP) 组。
- 20 - Diffie-Hellman 组 20： NIST 384 位 ECP 组。
- 21 - Diffie-Hellman 组 21： NIST 521 位 ECP 组。
- 24 - Diffie-Hellman 组 24：带 256 位素数阶子组的 2048 位 MODP 组。我们不再建议采用此选项。

确定使用哪种身份验证方法

您可以使用以下方法对站点间 VPN 连接中的对等体进行身份验证。

预共享密钥

预共享密钥是在连接中的每个对等体上配置的加密密钥字符串。这些密钥由 IKE 在身份验证阶段使用。对于 IKEv1，您必须在每个对等体上配置相同的预共享密钥。对于 IKEv2，您可以在每个对等体上配置唯一密钥。

与证书相比，预共享密钥的扩展性相对逊色。如果需要配置大量的站点间VPN连接，请使用证书而非预共享密钥。

使站点间 VPN 流量豁免 NAT

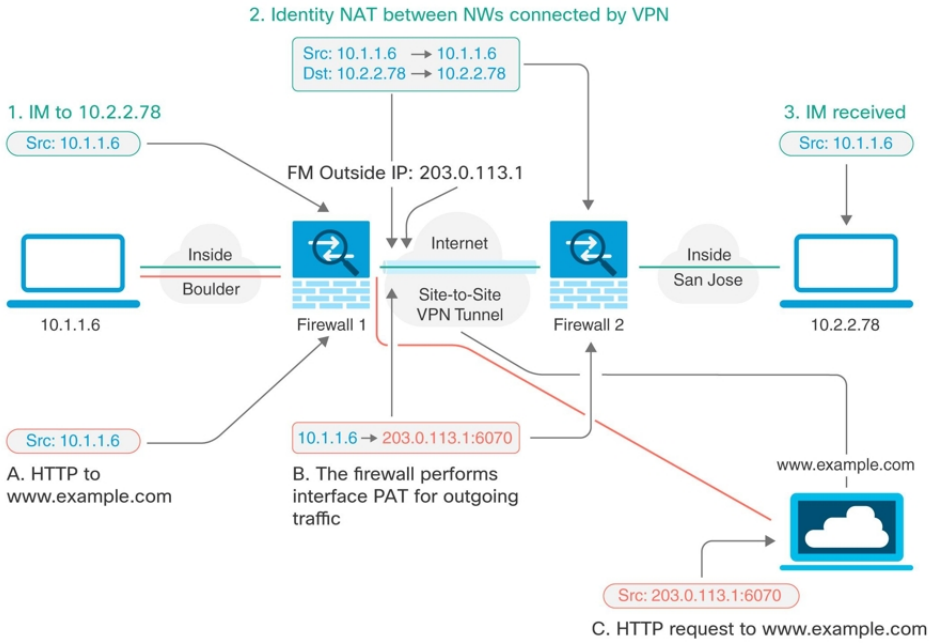
当您在某个接口上定义了站点间 VPN 连接并且还对该接口实施了 NAT 规则时，可以选择使该 VPN 上的流量豁免 NAT 规则。如果 VPN 连接的远端可以处理您的内部地址，则可能要执行此操作。

创建 VPN 连接时，可以选择 **NAT 豁免**选项自动创建 NAT 豁免规则。不过，此操作仅在通过单个路由接口（而非网桥组成员）连接本地受保护网络时才奏效。相反，如果该连接中的本地网络位于两个或多个路由接口之后或者一个或多个网桥组成员之后，则需要手动配置 NAT 豁免规则。

要使 VPN 流量豁免 NAT 规则，需要为目的是远程网络时的本地流量创建身份手动 NAT 规则。然后，将NAT应用于目的是其他网络（例如互联网）时的流量。如果本地网络有多个接口，请为每个接口分别创建规则。也可以考虑以下建议：

- 如果连接中有多个本地网络，请创建一个网络对象组用于容纳定义这些网络的对象。
- 如果 VPN 中同时包括 IPv4 和 IPv6 网络，请为其各创建一个单独的身份 NAT 规则。

下例显示连接博尔德办公室和圣荷西办公室的站点间隧道。对于要发送到互联网的流量（例如，从博尔德办公室中的 10.1.1.6 到 www.example.com），需要利用 NAT 提供的公用 IP 地址访问互联网。以下示例使用接口端口地址转换 (PAT) 规则。然而，对于要穿过 VPN 隧道的流量（例如，从博尔德办公室中的 10.1.1.6 到圣荷西办公室中的 10.2.2.78），您不想执行 NAT；您需要通过创建身份 NAT 规则来豁免此流量。身份 NAT 将地址转换为其相同的地址。



以下示例说明 Firewall1（博尔德办公室）的配置。该示例假定内部接口是网桥组，因此需要为每个成员接口编写规则。如果有一个或多个路由内部接口，其过程相同。

Note 此示例假定只包括 IPv4 网络。如果该 VPN 还包括 IPv6 网络，请为 IPv6 创建并行规则。请注意，由于无法实施 IPv6 接口 PAT，因此需要使用唯一 IPv6 地址创建主机对象用于 PAT。

Procedure

步骤 1 创建对象来定义各种网络。

a. 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

b. 点击蓝色加号按钮  以创建新的对象。

c. 点击**FTD > 网络 (Network)**。

d. 找到博尔德办公室内部网络。

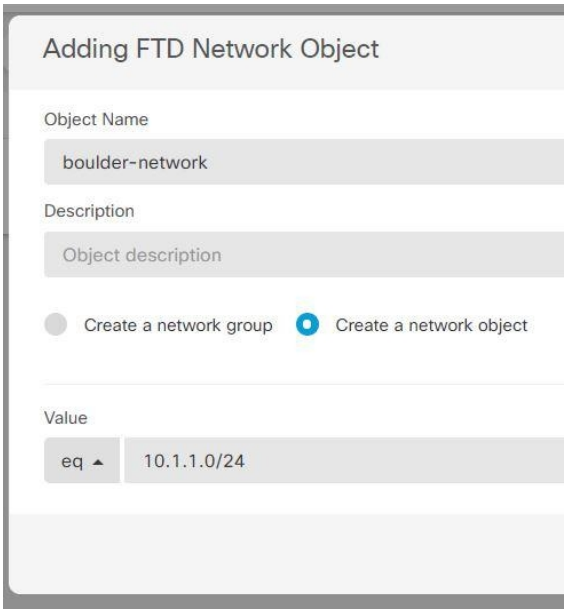
e. 输入对象名称（例如，boulder-network）。

f. 选择 **创建网络对象**。

g. 在“值”部分：

- 选择 **eq** 并输入以 CIDR 表示法表示的单个 IP 地址或子网地址。

- 选择 **范围** 并输入 IP 地址范围。例如，输入网络地址 10.1.1.0/24。



h. 点击**添加 (Add)**。

i. 点击蓝色加号按钮  以创建新的对象。

j. 定义内部圣荷西办公室网络。

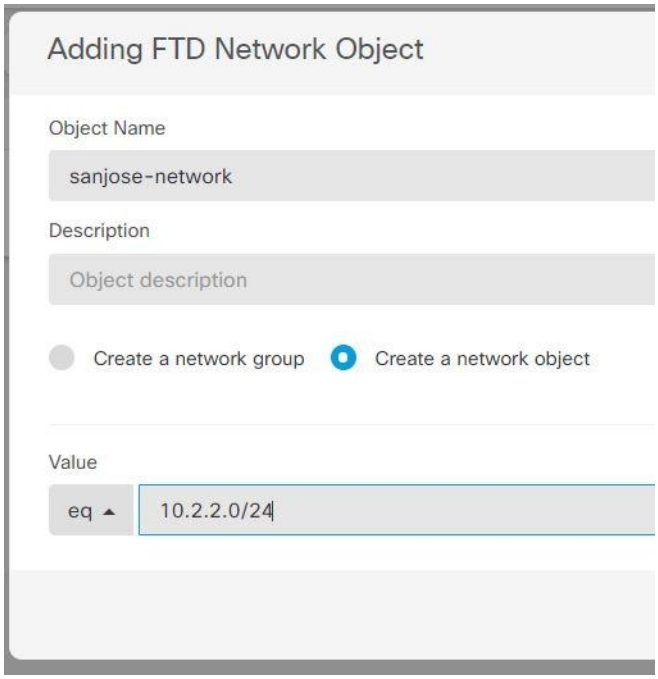
k. 输入对象名称（例如，san-jose）。

l. 选择 **创建网络对象**。

m. 在“值”部分：

- 选择 **eq** 并输入以 CIDR 表示法表示的单个 IP 地址或子网地址。

- 选择 **范围** 并输入 IP 地址范围。例如，输入网络地址 10.1.1.0/24。



n. 点击**添加 (Add)**。

步骤 2 在Firewall1（博尔德办公室）上，为博尔德办公室网络配置经过VPN连接到圣荷西办公室时的手动身份 NAT。

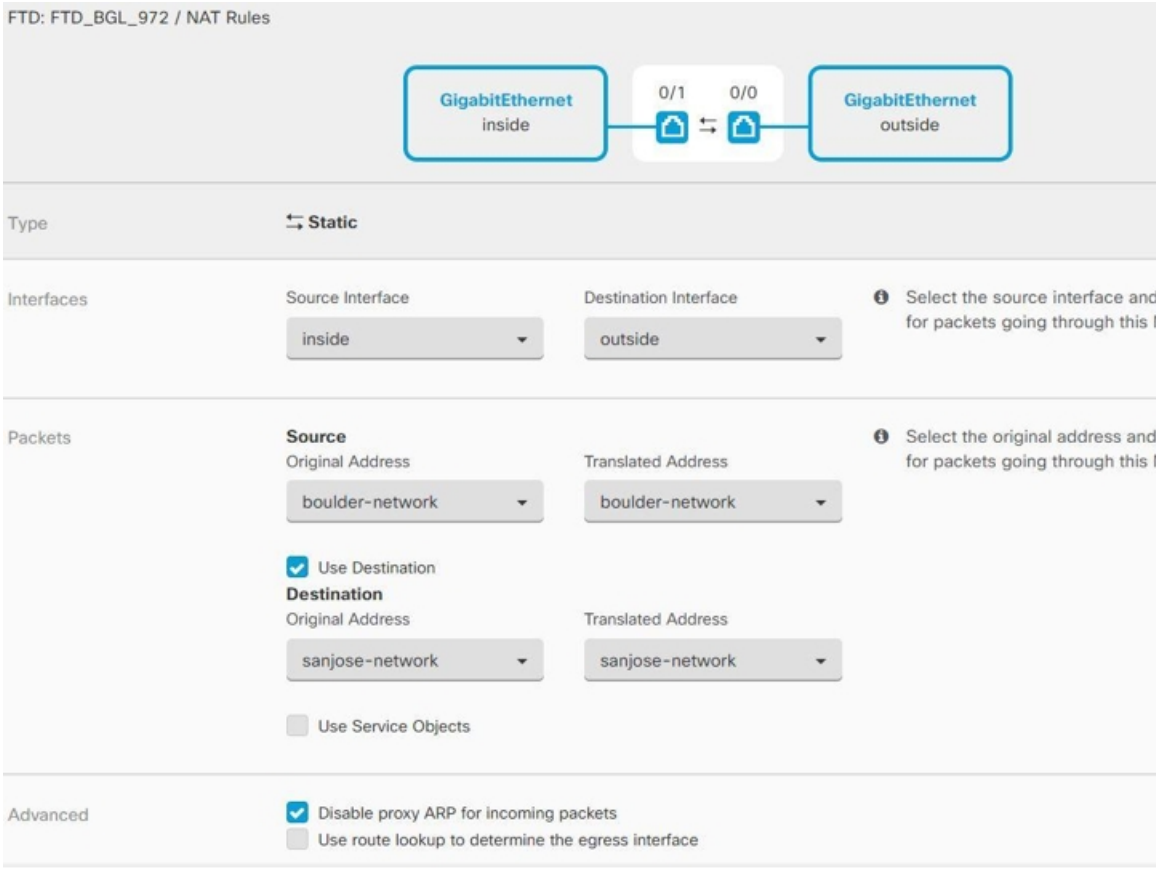
a. 在 CDO 导航栏中，点击**清单 (Inventory)**。

b. 使用过滤器查找要为其创建 NAT 规则的设备。

c. 在详细信息面板的管理区域中，点击 **NAT** NAT。

d. 点击 + > **两次 NAT**。

- 在第 1 部分中，选择**静态 (Static)**。点击**继续**。
- 在部分 2 中，选择**源接口 (Source Interface)** = **inside** 和**目标接口 (Destination Interface)** = **outside**。点击**继续**。
- 在第 3 部分中，选择**原始源地址 (Source Original Address)** = 'boulder-network' 和 **转换后的源地址 (Source Translated Address)** = 'boulder-network'。
- 选择 **使用目的**。
- 选择**原始目标地址 (Destination Original Address)** = 'sanjose-network' 和**转换后的源地址 (Source Translated Address)** = 'sanjose-network'。**注意**：由于您不需要转换目的地址，因此需要通过为原始目的地址和转换后的目的地址指定相同的地址，从而为其配置身份 NAT。将所有端口字段留空。此规则为源和目标配置身份 NAT。



- 选择为传入数据包禁用代理 **ARP (Disable proxy ARP for incoming packets)**。
- 点击保存 **(Save)**。
- 重复此过程，为每个其他内部接口创建相应规则。

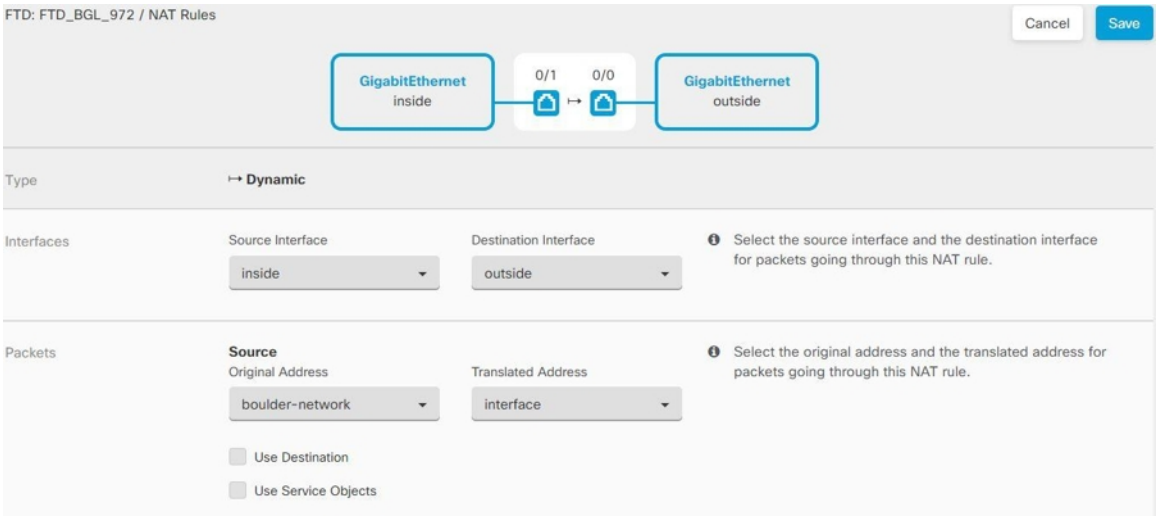
步骤 3 在Firewall1（博尔德办公室）上，为内部博尔德办公室网络配置接入互联网时的手动动态接口PAT。
注意：内部接口可能已经配置了将所有 IPv4 流量包括在内的动态接口 PAT 规则，因为初始配置过程中会默认创建这些规则。不过，为完整起见，此处仍显示了这些配置。完成这些步骤之前，请检查是否已经存在将内部接口和网络包括在内的规则，如有则跳过此步骤。

a. 点击 + > **两次 NAT**。

b. 在第 1 部分中，选择**动态 (Dynamic)**。点击**继续**。

c. 在部分 2 中，选择**源接口 (Source Interface)** = **inside** 和**目标接口 (Destination Interface)** = **outside**。点击**继续**。

d. 在第 3 部分中，选择**原始源地址 (Source Original Address)** = 'boulder-network' 和**转换后的源地址 (Source Translated Address)** = 'interface'。



e. 点击**保存 (Save)**。

f. 重复此过程，为每个其他内部接口创建相应规则。

步骤 4 将配置更改部署到 CDO。有关详细信息，请参阅将配置更改从 CDO 部署到 FDM 管理 设备。

步骤 5 如果您也管理着 Firewall2（圣荷西办公室），您可以为该设备配置类似的规则。

- 当目标是 boulder-network 时，手动身份 NAT 规则将用于 'sanjose-network'。为 Firewall2 内部和外部网络创建新的接口对象。
- 当目标是“任何”时，手动动态接口 PAT 规则将用于 'sanjose-network'。

配置全局 IKE 策略

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。

IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用提议。IKE 提议是一组两个对等体用于保护其之间的协商的算法。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数用于保护后续 IKE 协商。

IKE 策略对象为这些协商定义 IKE 提议。您启用的对象是对等体协商 VPN 连接时使用的对象：不能为每个连接指定不同的 IKE 策略。每个对象的相对优先级确定首先尝试这些策略中的哪一个，数字越小优先级越高。如果协商无法找到两个对等体全都支持的策略，则不建立连接。

要定义全局 IKE 策略，需要为每个 IKE 版本选择启用哪些对象。如果预定义的对象不能满足您的要求，请创建新的策略来执行您的安全策略。

以下步骤说明如何通过“对象”(Objects) 页面配置全局策略。在编辑 VPN 连接时，您还可以点击 IKE 策略设置的编辑，来启用、禁用和创建策略。

以下主题介绍如何为每个 IKE 策略版本配置 IPsec 提议：

- 管理 IKEv1 策略
- 管理 IKEv2 策略

管理 IKEv1 策略

介绍如何创建和编辑 IKEv1 策略。

关于 IKEv1 策略

互联网密钥交换 (IKE) 版本 1 策略对象包含定义 VPN 连接时 IKEv1 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义 IKEv1 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

Related Topics

创建或编辑 IKEv1 策略 ，第 429 页

创建或编辑 *IKEv1* 策略

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。您还可以点击对象列表中所示的**创建新 IKE 策略 (Create New IKEv1 Policy)** 链接，以便在站点间 VPN 连接中编辑 IKEv1 设置时创建 IKEv1 策略对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择**FDM > IKEv1 策略 (IKEv1 Policy)** 以创建新的 IKEv1 策略。
- 在对象页面中，选择要编辑的 IKEv1 策略，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

步骤 3 输入**对象名称**，最多 128 个字符。

步骤 4 配置 IKEv1 属性。

- **优先级** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **加密** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。有关选项的说明，请参阅“决定使用哪种加密算法”。

- **Diffie-Hellman 组 (Diffie-Hellman Group)** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。有关选项的解释，请看“决定要使用的 Diffie-Hellman 模数组”。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。
- **身份验证 (Authentication)** - 在两个对等体之间使用的身份验证方法。关于更多信息，请参阅 确定使用哪种身份验证方法。
  - **预共享密钥** - 使用在每个设备上定义的预共享密钥。在身份验证阶段，此类密钥允许密钥在两个对等体之间共享并由 IKE 使用。如果未使用同一预共享密钥配置对等体，则无法建立 IKE SA。
  - **证书 (Certificate)** - 使用对等体的设备身份证书来识别彼此。必须通过在证书颁发机构中注册每个对等体来获取这些证书。还须上传用于签署每个对等体的身份证书的受信任 CA 根证书和中间 CA 证书。对等体可以注册到相同或不同的 CA 中。对于任一对等体，都不能使用自签证书。
- **散列** - 用于创建消息摘要的散列算法，以确保消息的完整性。有关选项的说明，请参阅决定要使用的 Diffie-Hellman 模数组。

步骤 5 点击**添加**。

管理 IKEv2 策略

介绍如何创建和编辑 IKEv2 策略。

关于 IKEv2 策略

互联网密钥交换 (IKE) 版本 2 策略对象包含定义 VPN 连接时 IKEv2 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv2 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

Related Topics

创建或编辑 IKEv2 策略 ， 第 430 页

创建或编辑 *IKEv2* 策略

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。您还可以点击对象列表中所示的 **创建新的 IKE 策略** 链接，以便在站点间 VPN 连接中编辑 IKEv1 设置时创建 IKEv1 策略对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FDM > IKEv2 策略 (IKEv2 Policy)** 以创建新的 IKEv2 策略。
- 在对象页面中，选择要编辑的 IKEv2 策略，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

步骤 3 输入**对象名称 (object name)**，最多 128 个字符。

步骤 4 配置 IKEv2 属性。

- **优先级** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **状态** - IKE 策略是启用还是禁用状态。点击开关以更改状态。在 IKE 协商期间仅使用启用的策略。
- **加密 (Encryption)** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。选择要允许的所有算法，但不能在同一策略中同时包括混合模式 (AES-GCM) 和正常模式选项。（正常模式要求选择完整性散列，而混合模式禁止选择单独的完整性散列。) 系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定决定使用哪个加密算法.
- **Diffie-Hellman 组 (Diffie-Hellman Group)** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。选择要允许的所有算法。系统与对等体协商，从最强到最弱组，直到达成匹配。有关选项的解释，请参阅决定要使用的 Diffie-Hellman 模数组。
- **完整性散列 (Integrity Hash)** - 用于创建消息摘要的散列算法的完整性部分，用于确保消息完整性。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。完整性散列不与 AES-GCM 加密选项一起使用。有关选项的说明，请参阅 决定使用哪些散列算法。
- **伪随机函数 (PRF) 散列 (Pseudo-Random Function [PRF] Hash)** - 散列算法中用作派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法的伪随机函数 (PRF) 部分。在 IKEv1 中，完整性和 PRF 算法不分开，但在 IKEv2 中，可以为这些元素指定不同的算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪些散列算法。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。

步骤 5 点击添加。

配置 IPsec 提议

IPsec 是设置 VPN 的最安全方法之一。IPsec 在 IP 数据包级别提供数据加密，提供一种基于标准的强大的安全解决方案。使用 IPsec，数据通过隧道在公共网络上传输。隧道是两个对等体之间安全的逻辑通信路径。进入 IPsec 隧道的流量由称为转换集的安全协议和算法组合保护。在 IPsec 安全关联 (SA) 协商期间，对等体搜索在两个对等体处相同的转换集。

根据 IKE 版本（IKEv1 或 IKEv2），存在不同的 IPsec 提议对象：

- 当创建 IKEv1 IPsec 提议时，可以选择 IPsec 运行的模式，并定义所需的加密和身份验证类型。您可以为算法选择单一选项。如果要在 VPN 中支持多个组合，请创建和选择多个 IKEv1 IPsec 提议对象。
- 当创建 IKEv2 IPsec 提议时，可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序，并与对等体进行协商，直到找到匹配。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

Note 我们建议对 IPsec 隧道使用加密和身份验证。

以下主题介绍如何为每个 IKE 版本配置 IPsec 提议：

- 管理 IKEv1 IPsec 提议对象
- 管理 IKEv2 IPsec 提议对象

管理 IKEv1 IPsec 提议对象

IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。IKEv1 和 IKEv2 有单独的对象。目前， Cisco Defense Orchestrator (CDO) 支持 IKEv1 IPsec 提议对象。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

Note 我们建议对 IPsec 隧道使用加密和身份验证。

Related Topics

创建或编辑 IKEv1 IPsec 提议对象 ， 第 433 页

创建或编辑 *IKEv1 IPsec* 提议对象

有几个预定义的IKEv1 IPsec提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑站点间 VPN 连接中的 IKEv1 IPsec 设置时，点击对象列表中所示的**创建新 IKEv1 提议 (Create New IKEv1 Proposal)** 链接来创建 IKEv1 IPsec 提议对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FDM > IKEv1 IPsec 提议 (IKEv1 IPsec Proposal)** 以创建新对象。
- 在对象页面中，选择要编辑的IPsec方案，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

步骤 3 为新对象输入**对象名称**。

步骤 4 选择 IKEv1 IPsec 提议对象的运行模式。

- **隧道**模式会封装整个 IP 数据包。IPSec 报头被添加到原始 IP 报头和新的 IP 报头之间。这是默认值。当防火墙对出入位于防火墙后的主机的流量进行保护时，请使用隧道模式。在通过不可信网络（例如互联网）连接的两个防火墙（或其他安全网关）之间，通常采用隧道模式实施常规 IPSec。
- **传输**模式只封装IP数据包的上层协议。IPSec报头被插入到IP报头和上层协议报头（例如TCP）之间。传输模式要求源和目的主机都支持 IPSec，并且只有在隧道的目的对等体是 IP 数据包的最终目的时才可使用。通常只有在保护第2层或第3层隧道协议（例如GRE、L2TP和DLSW）时，才会使用传输模式。

步骤 5 选择**加密 (Encryption)**提议的（封装安全协议加密）算法。有关选项的说明，请参阅 决定使用哪个加密算法。

步骤 6 选择要用于身份验证的 **ESP 散列 (ESP Hash)** 或完整性算法。有关选项的说明，请参阅决定使用哪些散列算法。

步骤 7 点击**添加**。

管理 IKEv2 IPsec 提议对象

IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。

当创建 IKEv2 IPsec 提议时，可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序，并与对等体进行协商，直到找到匹配。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

Related Topics

创建或编辑 IKEv2 IPsec 提议对象 ， 第 434 页

创建或编辑 *IKEv2 IPsec* 提议对象

有几个预定义的IKEv2 IPsec提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑 VPN 连接中的 IKEv2 IPsec 设置时，点击对象列表中所示的创建新 IPsec 提议链接来创建 IKEv2 IPsec 提议对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FDM > IKEv2 IPsec 提议 (IKEv2 IPsec Proposal)** 以创建新对象。
- 在对象页面中，选择要编辑的IPsec方案，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

步骤 3 为新对象输入**对象名称**。

步骤 4 配置 IKEv2 IPsec 方案对象：

- **加密 (Encryption)** - 此提议的封装安全协议 (ESP) 加密算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定决定使用哪个加密算法.
- **完整性散列 (Integrity Hash)** - 要用于身份验证的散列或完整性算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪些散列算法。

步骤 5 点击**添加**。

监控 FDM 管理 设备 站点间虚拟专用网络

CDO 允许您在载入的 FDM 管理 设备上监控、修改和删除现有或新创建的站点间 VPN 配置。

检查站点间 VPN 隧道连接

使用 **Check Connectivity** 按钮触发对隧道的实时连接检查，以确定隧道当前处于搜索和过滤器站点间VPN隧道。除非您点击“按需连接检查”按钮，否则将每小时检查一次所有已自行激活设备上可用的所有隧道。

Note

- CDO 在 FTD 上运行此连接检查命令，以确定隧道处于活动状态还是空闲状态：

  ```
  show vpn-sessiondb l2l sort ipaddress
  ```

- 建模 ASA 设备将始终显示为**空闲**。

要从 VPN 页面检查隧道连接，请执行以下操作：

Procedure

步骤 1 在主导航栏中，点击 VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)。

步骤 2 搜索和过滤器站点间 VPN 隧道站点间 VPN 隧道的隧道列表，然后选择该列表。

步骤 3 在右侧的操作窗格中，点击**检查连接**。

确定 VPN 问题

CDO 可以识别 ASA FTD 上的 VPN 问题。（此功能尚不适用于 AWS VPC 站点间 VPN 隧道。）本文将介绍以下内容：

- 查找缺少对等体的 VPN 隧道
- 查找存在加密密钥问题的 VPN 对等体
- 查找为隧道定义的不完整或配置错误的访问列表
- 查找隧道配置中的问题

解决隧道配置问题, on page 437

查找缺少对等体的 *VPN* 隧道

“缺少 IP 对等体”情况在 ASA 设备上比FDM 管理设备上更可能发生。

Procedure

步骤 1 在 CDO 导航窗格中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

步骤 2 选择**表视图 (Table View)**。

步骤 3 通过点击过滤器图标 打开过滤器面板。

步骤 4 检查**检测到的问题**。

步骤 5 选择每个报告问题的设备，然后查看右侧的“对等体”窗格。系统将列出一个对等体名称。CDO 报告另一个对等体名称为“[缺少对等体 IP.]”。

查找存在加密密钥问题的 *VPN* 对等体

使用此方法查找存在加密密钥问题的 VPN 对等体，例如：

- IKEv1 或 IKEv2 密钥无效、缺失或不匹配
- 过时或低加密隧道

Procedure

步骤 1 在 CDO 导航栏中，点击 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

步骤 2 选择**表视图 (Table View)**。

步骤 3 通过点击过滤器图标 打开过滤器面板。

步骤 4 选择每个报告问题的设备，然后查看右侧的“对等体”窗格。⚠对等体信息将显示两个对等体。

步骤 5 点击其中一台设备的查看对等体。

步骤 6 双击图表视图中报告问题的设备。

步骤 7 点击底部隧道详细信息面板中的密钥交换。您将能够查看两台设备并从该点诊断关键问题。

查找为隧道定义的不完整或配置错误的访问列表

“不完整或配置错误的访问列表”条件只能出现在 ASA 设备上。

Procedure

步骤 1 在 CDO 导航栏中，点击 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

步骤 2 选择**表视图 (Table View)**。

步骤 3 通过点击过滤器图标 打开过滤器面板。

步骤 4 选择每个报告问题的设备，然后查看右侧的“对等体”窗格。⚠对等体信息显示两个对等体。

步骤 5 点击其中一台设备的查看对等体。

步骤 6 双击图表视图中报告问题的设备。

步骤 7 点击底部隧道详细信息面板中的隧道详细信息。您将看到消息“网络策略：不完整”

查找隧道配置中的问题

在以下情况下可能会发生隧道配置错误：

- 当站点间 VPN 接口的 IP 地址更改时，“对等 IP 地址值已更改”。
- 当 VPN 隧道的 IKE 值与另一个 VPN 隧道不匹配时，系统将显示“IKE 值不匹配”消息。

Procedure

步骤 1 在 CDO 导航栏中，点击 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

步骤 2 选择**表视图 (Table View)**。

步骤 3 通过点击过滤器图标 打开过滤器面板。

步骤 4 在**隧道问题 (Tunnel Issues)** 中，点击**检测到的问题 (Detected Issues)** 以查看 VPN 配置报告错误。您可以查看配置报告问题 。

步骤 5 选择 VPN 配置报告问题。

步骤 6 在右侧的**对等体**窗格中，会显示存在问题的对等体的 图标。将鼠标悬停在 图标上可查看问题和解决方案。

下一步：解决隧道配置问题。

解决隧道配置问题

此程序尝试解决以下隧道配置问题：

- 当站点间 VPN 接口的 IP 地址更改时，“对等 IP 地址值已更改”。
- 当 VPN 隧道的 IKE 值与另一个 VPN 隧道不匹配时，系统将显示“IKE 值不匹配”消息。

有关详细信息，请参阅查找隧道配置中的问题。

过程

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击相应的设备类型选项卡，然后选择与报告问题的 VPN 配置关联的设备。

步骤 4 接受设备更改。解决“检测到冲突”状态，第 566 页

步骤 5 在 CDO 导航窗格中，点击 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

步骤 6 选择报告此问题的 VPN 配置。

步骤 7 点击**操作 (Actions)** 窗格中的**编辑** 图标 。

步骤 8 在每个步骤中点击下一步，直到您在步骤 4 中点击完成按钮。

步骤 9 预览和部署所有设备的配置更改，第 556 页。

搜索和过滤器站点间 VPN 隧道

将过滤器边栏 与搜索字段结合使用，可重点搜索 VPN 隧道图中显示的 VPN 隧道。

Procedure

步骤 1 在主导航栏中，导航至 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

步骤 2 点击过滤器图标 可打开过滤器窗格。

步骤 3 使用以下过滤器细化搜索：

- **按设备过滤 (Filter by Device)** - 点击**按设备过滤 (Filter by Device)**，选择设备类型选项卡，然后选中要通过过滤查找的设备。
- **隧道问题 (Tunnel Issues)** - 我们是否检测到隧道的任一端存在问题。存在问题的设备的一些示例可能包括（但不限于）：缺少关联的接口或对等体 IP 地址或访问列表、IKEv1 提议不匹配等。（检测隧道问题尚不适用于 AWS VPC VPN 隧道。）
- **设备/服务 (Devices/Services)** - 按设备类型过滤。
- **状态 (Status)** - 隧道状态可以是活动或空闲。
  - **活动 (Active)** - 存在网络数据包通过 VPN 隧道的开放会话，或者已成功建立会话且尚未超时的会话。活动可以帮助指示隧道处于活动状态和相关性。
  - **空闲 (Idle)** - CDO 无法发现此隧道的开放会话，隧道可能未在使用或此隧道存在问题。
- **已载入 (Onboarded)** - 设备可以由 CDO 管理，也可以不由 CDO 管理（非托管）。
  - **托管 (Managed)** - 按 CDO 管理的设备过滤。
  - **非托管 (Unmanaged)** - 按 CDO 不管理的设备进行过滤。
- **设备类型 (Device Types)** - 隧道的任一端是实时（已连接设备）还是模型设备。

步骤 4 您还可以通过在搜索栏中输入设备名称或 IP 地址来搜索过滤结果。搜索不区分大小写。

载入非托管设备

在载入其中一个对等设备时，CDO 将发现站点间 VPN 隧道。如果第二个对等设备不由 CDO 管理，则您可以过滤 VPN 隧道列表以查找非受管设备并将其载入：

Procedure

步骤 1 在主导航栏中，选择 **VPN** > **ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)** 以打开 VPN 页面。

步骤 2 选择**表视图 (Table View)**。

步骤 3 通过点击 打开过滤器面板。

步骤 4 点击**非托管 (Unmanaged)**。

步骤 5 从表中的结果中选择一个隧道。

步骤 6 在右侧的对等体 (Peers) 窗格中，点击载入设备 (Onboard Device)，然后按照屏幕上的说明进行操作。

相关信息：

- 载入设备和服务, on page 161
- 载入 威胁防御 设备, on page 161

查看站点间 VPN 隧道的 IKE 对象详细信息

您可以查看所选隧道的对等体/设备上配置的 IKE 对象的详细信息。这些详细信息根据 IKE 策略对象的优先级显示在层次结构中的树结构中。

Note 外联网设备不显示 IKE 对象详细信息。

Procedure

步骤 1 在左侧 CDO 导航栏中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

步骤 2 在 VPN Tunnels 页面中，点击连接对等体的 VPN 隧道的名称。

步骤 3 在右侧的“关系”下，展开要查看其详细信息的对象。

查看上次成功建立站点间 VPN 隧道的日期

Procedure

步骤 1 查看站点间 VPN 隧道信息。

步骤 2 点击 **Tunnel Details** 窗格。

步骤 3 查看**上次查看的活动**字段。

查看站点间 VPN 隧道信息

站点间 VPN 表视图是载入 CDO 的所有设备上可用的所有站点间 VPN 隧道的完整列表。隧道在此列表中仅存在一次。点击表中列出的隧道会在右侧栏中提供一个选项，以直接导航到隧道的对等体以进行进一步调查。

如果 CDO 不管理隧道的两端，您可以点击载入非托管设备 以打开主载入页面并载入非托管对等设备。在 CDO 管理隧道两端的情况下，对等体 2 列包含受管设备的名称。但是，对于 AWS VPC，对等体 2 列包含 VPN 网关的 IP 地址。

要在表视图中查看站点间 VPN 连接，请执行以下操作：

Procedure

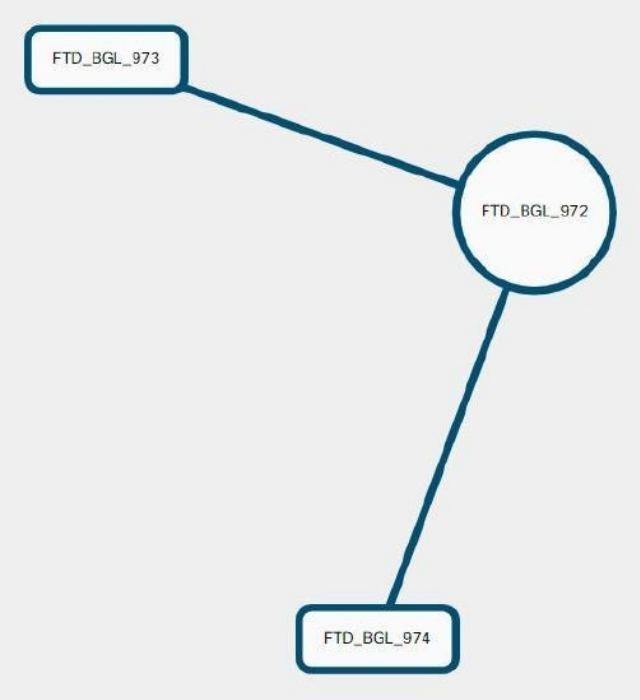
步骤 1 在主导航栏中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

步骤 2 点击**表格视图 (Table view)** 按钮。

步骤 3 使用搜索和过滤器站点间 VPN 隧道 以查找特定隧道，或放大全局视图图形以查找要查找的 VPN 网关及其对等体。

站点间 *VPN* 全局视图

这是全局视图的示例。在图中，“FTD_BGL_972”与 FTD_BGL_973 和 FTD_BGL_974 设备建立了站点间连接。



Procedure

步骤 1 在主导航栏中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

步骤 2 点击**全局视图 (Global view)** 按钮。

步骤 3 使用搜索和过滤器站点间 VPN 隧道 以查找特定隧道，或放大全局视图图形以查找要查找的 VPN 网关及其对等体。

步骤 4 选择全局视图中表示的对等体之一。

步骤 5 点击**查看详细信息**。

步骤 6 点击 VPN 隧道的另一端，CDO 将显示该连接的隧道详细信息、NAT 信息和密钥交换信息：

- 隧道详细信息 - 显示有关隧道的名称和连接信息。点击刷新图标可更新隧道的连接信息。

- 特定于AWS连接的隧道详细信息 - AWS站点到站点连接的隧道详细信息与其他连接略有不同。对于从 AWS VPC 到 VPN 网关的每个连接，AWS 会创建两个 VPN 隧道。这用于高可用性。
  - 隧道的名称代表您的 VPN 网关所连接的 VPC 的名称。隧道中指定的 IP 地址是您的 VPN 网关获知的 VPC 的 IP 地址。
  - 如果 CDO 连接状态显示为“活动”，则 AWS 隧道状态为“运行”。如果 CDO 连接状态为“非活动”，则 AWS 隧道状态为“关闭”。
- NAT 信息 - 显示正在使用的 NAT 规则类型、原始和转换后的数据包信息，并提供指向 NAT 表的链接以查看该隧道的 NAT 规则。（尚不可用于 AWS VPC 站点间 VPN。）
- 密钥交换 - 显示隧道和密钥交换问题正在使用的加密密钥。（尚不可用于 AWS VPC 站点间 VPN。）

隧道窗格

Tunnels 窗格显示与特定 VPN 网关关联的所有隧道的列表。对于 VPN 网关和 AWS VPC 之间的站点间 VPN 连接，隧道窗格显示从 VPN 网关到 VPC 的所有隧道。由于您的 VPN 网关和 AWS VPC 之间的每个站点间 VPN 连接都有两个隧道，因此您会看到通常用于其他设备的隧道数量的两倍。

VPN 网关详细信息

显示连接到VPN网关的对等体的数量以及VPN网关的IP地址。这仅在“VPN隧道”(VPN Tunnels)页面中可见。

对等体窗格

选择站点间VPN对等体后，对等体窗格将列出该对中的两台设备，并允许您点击其中一台设备的查看对等体。通过点击查看对等体，您可以看到与该设备关联的任何其他站点到站点对等体。这在“表”视图和“全局”视图中可见。

远程访问虚拟专用网络

远程访问虚拟专用网络 (RA VPN) 允许个人用户使用连接到互联网的计算机或其他受支持的 iOS 或 Android 设备，从远程位置连接到您的网络。这样，移动员工就可以从家庭网络或公共 Wi-Fi 网络进行连接。

RA VPN 配置包括以下组件：

- 连接配置文件：您可以创建远程访问VPN连接配置文件，允许用户在外部网络（例如其家庭网络）上时连接到您的内部网络。创建单独的配置文件，以适应不同的身份验证方法。连接配置文件由身份源和组策略组成。

相关信息：

-

- 为 FTD 配置远程访问 VPN

监控远程访问虚拟专用网络会话

远程访问虚拟专用网络 (RA VPN) 为远程用户（如移动用户或远程工作者）提供安全连接。监控这些连接可以让连接和用户会话性能的重要指标变得一目了然。Cisco Defense Orchestrator (CDO) RA VPN 监控功能使您能够快速确定远程接入 VPN 问题是否存在及其存在的位置。然后，您可以应用这些知识并使用网络管理工具来减少或消除网络和用户问题。您还可以根据需要断开远程访问 VPN 会话。

“远程访问虚拟专用监控”(Remote Access Virtual Private Monitoring) 页面提供以下信息：

- 至少过去 90 天内的活动会话和历史会话列表。
- 显示直观的图形视觉效果，让 CDO 管理的所有活动 VPN 前端变得一目了然。
- 实时会话屏幕会显示 CDO 租户中最常用的操作系统和 VPN 连接配置文件。它还会显示平均会话持续时间以及上传和下载的数据。
- 过滤功能可根据设备类型、设备名称、会话长度以及传输和接收的数据量等条件来缩小搜索范围。

相关信息：

- 监控实时 AnyConnect RA VPN 会话, on page 442
- 监控历史 AnyConnect RA VPN 会话, on page 444
- 搜索和过滤 RA VPN 会话
- 自定义 RA VPN 监控视图
- 将 RA VPN 会话导出至 CSV 文件
- 断开 FDM 管理 设备上的活动 RA VPN 会话

监控实时 AnyConnect RA VPN 会话

您可以监控设备上活动 AnyConnect RA VPN 会话的实时数据。这些数据每 10 分钟会自动刷新一次。如果要随时检索最新的会话列表，请点击屏幕右上角显示的重新加载图标 。

开始之前

- 将 RA VPN 前端载入 CDO。
- 确保要监控实时数据的设备的连接状态在**清单 (Inventory)** 页面上为“在线”(Online)。

过程

步骤 1 在 CDO 导航窗格中，点击 **VPN** > **远程访问 VPN 监控**。

或者，您可以点击 CDO 主页上的**查看活动远程访问 VPN 会话 (View Active Remote Access VPN Sessions)**，或导航至 **VPN** > **远程访问 VPN (Remote Access VPN)**并点击屏幕右上角的 图标。

步骤 2 点击 **RA VPN**。

步骤 3 点击**实时 (Live)**。

您可以搜索和过滤 RA VPN 会话以根据设备类型、会话长度以及上传和下载数据范围等条件来缩小搜索范围。

注释 **数据 TX** 和**数据 RX** 信息不适用于 FTD。

查看实时数据

实时数据以控制面板和表格形式显示。

面板视图

您必须点击屏幕右上角的**显示图表视图**图标才能查看控制面板。

控制面板提供 CDO 管理的所有活动 VPN 头端的概览视图。

- **明细（所有设备）**：显示实时会话总数。它还显示了一个分为四个弧长的饼形图。它说明会话数最多的前三台设备的 VPN 会话百分比。剩余的弧长表示其他设备的总和。
- 显示 CDO 租户中最常用的操作系统和 VPN 连接配置文件。
- 显示平均会话持续时间以及上传和下载的数据。
- **按国家/地区排列的活动会话 (Active Sessions by Country)**：显示连接到 RA VPN 前端的用户的位置的交互式热度地图。
  - 用户已连接的国家/地区以逐渐变深的蓝色显示，具体取决于从该国家/地区建立的会话的相对比例 - 蓝色越深表示从该国家/地区建立的会话越多。
  - 地图底部的图例提供了一个比例，表示某个国家/地区的会话数与其所用蓝色阴影之间的相关性。
  - 将鼠标指针悬停在地图上，可查看国家/地区名称以及从该国家/地区建立的活动用户会话总数。
  - 将鼠标指针悬停在表格上，可在地图上看到国家/地区的位置和活动用户会话总数。

表格视图

点击屏幕右上角的**显示表格视图**图标，以表格格式查看数据。

表格形式提供当前连接的 VPN 用户的完整列表。

- **位置**列通过对公共 IP 地址进行地理定位来显示连接到 VPN 头端的所有用户的位置。点击一行可查看用户详细信息。点击左侧窗格中的位置链接时，用户的位置会显示在 Google 地图上。

重要事项	CDO 对实时数据应用标准过滤器，并在控制面板上显示这些数据。仅当显示表格数据时，才能应用新过滤器，因为可视化控制面板视图中不支持自定义过滤器。点击**清除**以删除已应用的所有过滤器。您无法删除标准过滤器。

您可以使用搜索和过滤 RA VPN 会话功能根据设备类型、会话长度以及上传和下载数据范围等条件来缩小搜索范围。请注意，一次最多可以显示 10,000 个结果。

状态列中带有**活动**标签的绿点表示活动 VPN 用户的会话。

监控历史 AnyConnect RA VPN 会话

您可以监控过去三个月内记录的 AnyConnect RA VPN 会话的历史数据。

开始之前

- 将 RA VPN 前端载入 CDO。

过程

步骤 1 在 CDO 导航窗格中，点击 **VPN** > **远程访问 VPN 监控**。

或者，您可以点击 CDO 主页上的**查看活动远程访问 VPN 会话 (View Active Remote Access VPN Sessions)**，或导航至 **VPN** > **远程访问 VPN (Remote Access VPN)** 并点击右上角的 图标。

步骤 2 点击 **RA VPN**。

步骤 3 点击**历史 (Historical)**。

CDO 会显示过去三个月内记录的 RA VPN 会话的历史数据。

您可以使用搜索和过滤 RA VPN 会话功能根据设备类型、会话长度以及上传和下载数据范围等条件来缩小搜索范围。

数据 TX 和**数据 RX** 信息不适用于 FTD。

查看历史数据

历史数据以控制面板和表格形式显示。

面板视图

您必须点击屏幕右上角的“显示图表视图”图标才能查看控制面板。您将看到控制面板视图和表格视图。

控制面板提供 CDO 管理的所有活动 VPN 头端的概览视图。它会提供一个条形图，以便显示过去 24 小时、7 天和 30 天内为所有设备记录的 VPN 会话。您可以从下拉列表中选择持续时间。您可以将鼠标悬停在各个条形上，以查看当天的日期和会话总数。

表格视图

您必须点击屏幕右上角显示的“显示表格视图”图标，才能仅查看表格视图。此表格提供了过去三个月内连接的 VPN 用户的完整列表。

“位置”列通过对公共 IP 地址进行地理定位来显示连接到 VPN 头端的所有用户的位置。点击一行可查看用户详细信息。点击左侧窗格中的位置链接时，用户的位置会显示在 Google 地图上。

重要事项 CDO 对历史数据应用标准过滤器，并将其显示在控制面板上。您只能在显示表格数据时应用新过滤器，因为自定义过滤器不支持控制面板。清除新应用的过滤器会重新启动控制面板（在屏幕上，点击清除可删除手动应用的过滤器）。您无法删除标准过滤器。

您可以使用搜索和过滤 RA VPN 会话功能根据会话日期和时间范围、会话长度以及上传和下载数据范围等条件来缩小搜索范围。请注意，一次最多可以显示 10,000 个结果。

状态列中带有活动标签的绿点表示活动 VPN 用户的会话。

搜索和过滤 RA VPN 会话

搜索

使用搜索栏功能查找 RA VPN 会话。开始在搜索栏中键入设备名称、IP 地址或序列号，系统将显示符合搜索条件的 RA VPN 会话。搜索不区分大小写。

过滤

使用过滤器边栏可根据会话时间范围、会话长度以及上传和下载数据范围等条件查找 RA VPN 会话。过滤功能可用于实时视图和历史视图。

- **按设备过滤 (Filter by Devices)**：从**所有类型 (All Types)** 选项卡中选择一个或所有设备以查看所选设备的会话。该窗口还会根据设备的类型来对它们进行分类，并在相应的选项卡下显示它们。
- **会话时间范围 (Sessions Time Range)**（仅适用于历史数据）：查看指定日期和时间范围内的历史会话。请注意，您可以查看过去三个月内记录的数据。
- **会话长度 (Sessions Length)**：根据指定会话的持续时间长度查看会话。设置时间单位（小时、分钟或秒），并通过移动滑块指定最小和最大持续时间。您还可以在提供的字段中指定长度。
- **上传 (TX) (Upload [TX])**：根据上传或传输到安全网络的指定数据量查看会话。设置单位（GB、MB 或 KB），并通过相应地移动滑块来选择范围。您还可以在可用字段中指定值。
- **下载 (RX) (Download [RX])**：根据从安全网络下载或接收的指定数据量查看会话。设置单位（GB、MB 或 KB），并通过相应地移动滑块来选择范围。您还可以在可用字段中指定值。

自定义 RA VPN 监控视图

您可以在实时和历史模式下修改 RA VPN 监控视图，以仅包含适用于所需视图的列标题。点击列右侧的列过滤器图标 ，然后选择或取消选择所需的列。

CDO 会在您下次登录 CDO 时记住您的选择。

将 RA VPN 会话导出至 CSV 文件

您可以将一个或多个设备的 RA VPN 会话导出至以逗号来分隔值的 (.csv) 文件。您可以在电子表格应用（例如 Microsoft Excel）中打开 .csv 文件，对列表中的项目进行排序和过滤。这些信息可帮助您分析 RA VPN 会话。每次导出会话时，CDO 都会创建一个新的 .csv 文件，其中创建的文件会在名称中包含日期和时间。

CDO 最多可以将 100,000 个活动会话导出至 CSV 文件。如果来自所有设备的会话总数超过最大限制，则可以使用**按设备查看 (View By Device)** 过滤器并为各个设备生成报告。

Procedure

步骤 1 在 CDO 导航窗格中，点击 **VPN** > **远程访问 VPN 监控 (Remote Access VPN Monitoring)**。

步骤 2 在**按设备查看 (View By Devices)** 区域中，选择以下选项之一：

- **所有设备 (All Devices)**，可从其下面列出的所有设备导出活动会话。
- 点击要导出其会话的设备。

步骤 3 点击右上角的 图标。CDO 会将您在屏幕上看到的规则导出至 .csv 文件。

步骤 4 在电子表格应用中打开 .csv 文件，对结果进行排序和过滤。

断开 FDM 管理 设备上的活动 RA VPN 会话

目前，无法使用 思科防御协调器 接口在 FDM 管理 设备上终止 RA VPN 会话。相反，您可以使用 SSH 连接到 威胁防御 CLI 并断开所需用户的连接。您可以在载入到 CDO 的在线 FDM 管理 设备上执行此任务。

Procedure

步骤 1 登录到 防火墙设备管理器 并使用设备 CLI，如运行设备版本的《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》的“入门”一章的**登录命令行接口 (CLI)** 部分所述。

步骤 2 执行 `vpn-sessionsdb logoff {name}` 命令并将 **name** 替换为用户名。此命令将终止您指定的用户名的所有会话。

为 FTD 配置远程访问 VPN

CDO 提供直观的用户界面，用于配置新的远程访问虚拟专用网络 (RA VPN)。它还允许您快速轻松地为 CDO 中的多个设备配置 RA VPN 连接。FDM 管理AnyConnect 是终端设备上通过 RA VPN 连接 FDM 管理 设备的唯一受支持客户端。

AnyConnect 客户端与 FDM 管理设备协商 SSL VPN 连接时，会使用传输层安全 (TLS) 或数据报传输层安全 (DTLS) 进行连接。DTLS 可避免与某些 SSL 连接关联的延迟和带宽问题，并可提高对于数据包延迟敏感的实时应用的性能。客户端与 FDM 管理 设备协商要使用的 TLS/DTLS 版本。如果客户端支持 DTLS，则使用 DTLS。

CDO 支持 FDM 管理 设备上的 RA VPN 功能的以下方面：

- 基于 SSL 客户端的远程访问
- IPv4 和 IPv6 寻址
- 跨多台 FDM 管理 设备共享 RA VPN 配置

Important 如果自行激活的设备（在软件版本 6.7 或更高版本上运行）包含使用 SAML 服务器作为身份验证源的 RA VPN 配置，则 CDO 不会在连接配置文件中填充 AAA 详细信息，因为它不管理当前版本中的 SAML 服务器对象。FDM 管理因此，您无法从 CDO 管理此类 RA VPN 配置。但是，CDO 会读取 RA VPN 连接配置文件以及关联的受信任 CA 证书和 SAML 服务器对象。

相关信息：

- 使用 RADIUS 和组策略控制用户权限和属性
- FDM 管理设备的端到端远程接入 VPN 配置过程
  - 下载 AnyConnect 客户端软件包
  - 将 AnyConnect 软件包上传到运行版本 6.4.0 的 FDM 管理设备
  - 将 AnyConnect 软件包上传到运行 FTD 6.5 或更高版本的设备 将 AnyConnect 软件包上传到运行 FDM 管理 6.5 或更高版本的设备
  - 上传 RA AnyConnect 客户端配置文件, on page 493
  - 为 FDM 管理 设备配置身份源
    - 创建或编辑 Active Directory 领域对象
    - 创建或编辑 RADIUS 服务器对象或组
  - 创建新的 RA VPN 组策略
  - 创建 RA VPN 配置
  - 配置 RA VPN 连接配置文件
  - 允许流量通过远程访问 VPN

RA VPN 用户的拆分隧道（Hair Pinning）

本文介绍 RA VPN 的分割隧道。

典型地，在远程接入 VPN 中，您可能希望 VPN 用户通过您的设备访问互联网。但是，您可以允许 VPN 用户在连接到 RA VPN 时访问外部网络。这种技术有时候称为分割隧道或发夹方法。拆分隧道不仅允许 VPN 通过安全隧道连接到远程网络，而且允许连接到 VPN 隧道外的网络。拆分隧道可减少 FTD 设备上的网络负载，并增加外部接口上的带宽。

要配置拆分隧道列表，必须创建标准访问列表或扩展访问列表。按照您的设备版本的《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》中的“虚拟专用网络 (VPN)”一章的**如何在外部接口上为远程访问 VPN 用户提供互联网访问**部分中所述的说明操作正在运行。

使用 RADIUS 和组策略控制用户权限和属性

本文提供有关从外部 RADIUS 服务器或组策略将属性应用于 RA VPN 连接的信息。

您可以将用户授权属性（也称为用户权利或权限）应用于来自外部 RADIUS 服务器或 FTD 设备上定义的组策略的 RA VPN 连接。如果 FTD 设备从与组策略上配置的属性冲突的外部 AAA 服务器接收属性，则来自 AAA 服务器的属性始终优先。

FTD 设备按照以下顺序应用属性：

Procedure

步骤 1 外部 AAA 服务器上的用户属性 - 该服务器在用户身份验证或授权成功后返回这些属性。

步骤 2 在 FTD 设备上配置的组策略 - 如果 RADIUS 服务器为用户返回 RADIUS CLASS 属性 IETF-Class-25 (OU=group-policy) 值，FTD 设备会将该用户放在名称相同的组策略中，并实施组策略中该服务器未返回的所有属性。

步骤 3 连接配置文件分配的组策略 - 连接配置文件包含该连接的初步设置，包括在进行身份验证前应用于用户的默认组策略。连接至 FTD 设备的所有用户最初都属于此组，这可以提供 AAA 服务器返回的用户属性或分配给用户的组策略中缺失的所有属性。

FTD 设备支持供应商 ID 为 3076 的 RADIUS 属性。如果使用的 RADIUS 服务器没有定义这些属性，您必须手动定义它们。要定义属性，请使用属性名称或编号、类型、值和供应商代码 (3076)。

以下主题根据属性值是在 RADIUS 服务器中定义的还是由系统发送到 RADIUS 服务器的来介绍受支持的属性。

发送到 *RADIUS* 服务器的属性

RADIUS 属性 146 和 150 由 FDM 管理 发送到 RADIUS 服务器，用于身份验证请求和授权请求。以下所有属性都是由 FDM 管理设备发送到 RADIUS 服务器，用于记账开始请求、临时更新请求和停止请求。

Table 17: 发送到 ***RADIUS*** 的属性 ***Secure Firewall Threat Defense***

属性	属性	语法、类型	单值或多值	说明或值
客户端类型	150	整数	单值	连接到 VPN 的客户端类型： 2 = AnyConnect 客户端 SSL VPN
会话类型	151	整数	单值	连接类型： 1 = AnyConnect 客户端 SSL VPN
隧道组名称	146	字符串	单值	用于建立会话的连接配置文件名称，如 FDM 管理 设备上的定义。此名称可以包含 1-253 个字符。

从 RADIUS 服务器接收的属性

以下用户授权属性由 RADIUS 服务器发送到 FDM 管理设备。

属性	属性编号	语法、类型	单值或多值	说明或值
Access-List-Inbound	86	字符串	单值	这两个访问列表属性都使用 FDM 管理 设备上配置的 ACL 名称。使用 Smart CLI 扩展访问列表对象类型在防火墙设备管理器中创建 ACL（登录防火墙设备管理器并选择**设备 (Device)** > **高级配置 (Advanced Configuration)** > **Smart CLI** > **对象 (Objects)**）。此类 ACL 用于控制入站流量（流量进入 FDM 管理 设备）或出站流量（流量离开 FDM 管理 设备）。
Access-List-Outbound	87	字符串	单值	
Address-Pools	217	字符串	单值	FDM 管理 设备上定义的网络对象名称，用于识别将作为地址池供客户端连接 RA VPN 时使用的子网。在**对象 (Objects)** 页面上定义网络对象。
Banner1	15	字符串	单值	用户登录时显示的横幅。
Banner2	36	字符串	单值	用户登录时显示的横幅的第二部分。横幅 2 附加到横幅 1。

属性	属性编号	语法、类型	单值或多值	说明或值
Group-Policy	25	字符串	单值	要在连接中使用的组策略。必须在 RA VPN **组策略 (Group Policy)** 页面上创建组策略。您可以使用以下其中一种格式： • 组策略名称 • OU = 组策略名称 • OU = 组策略名称；
Simultaneous-Logins	2	整数	单值	用户可以建立的独立并发连接的数量，0 - 2147483647。
VLAN	140	整数	单值	限制用户连接的 VLAN，0 - 4094。还必须在 FDM 管理设备的子接口上配置此 VLAN。

双因素身份验证

可以为RA VPN配置双因素身份验证。配置了双因素身份验证时，用户必须提供用户名、静态密码，以及一个额外项，如 Duo 密码等。双因素身份验证不同于使用第二个身份验证源，双因素是在单个身份验证源中配置的，其与 Duo 服务器的关系绑定到主身份验证源。例外情况是 Duo LDAP，它将“Duo LDAP 服务器”配置为辅助身份验证源。

- 使用 RADIUS 的 Duo 双因素身份验证，第 451 页
- 使用 LDAP 的 Duo 双因素身份验证，第 456 页

使用 *RADIUS* 的 *Duo* 双因素身份验证

可以将 Duo RADIUS 服务器配置为主要身份验证源。此方法使用 Duo RADIUS 身份验证代理。

有关配置 Duo 的详细步骤，请参阅 https://duo.com/docs/cisco-firepower。

然后，配置Duo，以转发定向到代理服务器的身份验证请求，并将另一台RADIUS服务器或Microsoft Active Directory(AD) 服务器用作第一个身份验证因素，将 Duo 云服务用作第二个因素。

使用此方法时，用户必须使用 Duo 身份验证代理和关联的 RADIUS/AD 服务器上配置的用户名，以及RADIUS/AD服务器中配置的用户名对应的密码进行身份验证，其后紧随以下其中一个Duo代码：

Duo-passcode。例如，my-password,12345。

push。例如，*my-password*,**push**。使用 **push** 告知 Duo 向用户应该已经安装并注册的 Duo 移动应用发送推送身份验证。

sms。例如，*my-password*,**sms**。使用 sms 告知 Duo 向用户的移动设备发送包含新一批密码的 SMS 消息。使用 sms 时，用户的身份验证尝试将会失败。用户必须重新进行身份验证，并输入新密码作为辅助因素。

phone。例如，*my-password*,**phone**。使用 phone 告知 Duo 执行电话回叫身份验证。

如果用户名和密码已经过验证，Duo 身份验证代理会联系 Duo 云服务，后者将核实该请求是来自有效配置的代理设备，然后按照指示将临时密码推送到用户的移动设备。当用户接受此密码时，Duo 会将会话标记为已验证，同时 RA VPN 成功创建。

有关详细说明，请参阅如何使用 Duo RADIUS 配置双因素身份验证，第 452 页

如何使用 Duo RADIUS 配置双因素身份验证

可以将 Duo RADIUS 服务器配置为主要身份验证源。此方法使用 Duo RADIUS 身份验证代理。

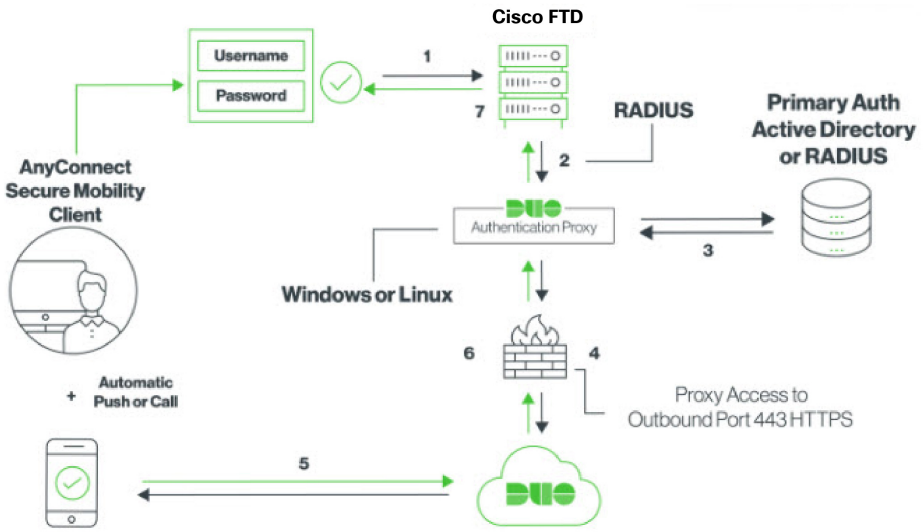
然后，配置 Duo，以转发定向到代理服务器的身份验证请求，并将另一台 RADIUS 服务器或 AD 服务器用作第一个身份验证因素，将 Duo 云服务用作第二个因素。

以下主题详细说明这种类型的高级配置：

- Duo RADIUS 辅助身份验证系统流程，第 452 页
- 使用 CDO 为 Duo RADIUS 配置设备，第 453 页

Duo RADIUS 辅助身份验证系统流程

以下是系统流程的说明：



1. 用户与设备建立远程接入 VPN 连接，并提供与 RADIUS/AD 服务器关联的用户名、RADIUS/AD 服务器中配置的用户名的密码，后跟其中一个 DUO 代码 Duo-password、push、SMS、或电话。FDM 管理有关更多信息，使用 RADIUS 的 Duo 双因素身份验证，第 451 页
2. FDM 管理 设备将身份验证请求发送到 Duo 身份验证代理。
3. Duo Authentication 代理使用主身份验证服务器（可能是 Active Directory 或 RADIUS）对此主要身份验证尝试进行身份验证。
4. 如果凭证已通过身份验证，则会通过 TCP 端口 443 与 Duo Security 建立 Duo 身份验证代理连接。
5. 然后，通过推送通知、带密码的短信消息或电话呼叫单独对用户进行身份验证。用户必须成功完成此身份验证。
6. Duo 身份验证代理接收身份验证响应。
7. 如果辅助身份验证成功，则 FDM 管理 设备会与用户的 AnyConnect 客户端建立远程接入 VPN 连接。

配置 Duo RADIUS 辅助身份验证

Duo Authentication 代理使用主身份验证服务器（可能是 Active Directory 或 RADIUS）对此主要身份验证尝试进行身份验证。

创建 Duo 账户

创建 Duo 账户并获取集成密钥、密钥和 API 主机名。

以下是对此过程的概述。有关详细信息，请参阅 Duo 网站。

过程

步骤 1 注册 Duo 账户。

步骤 2 登录到 Duo 管理面板 (Duo Admin Panel) 并导航至**应用 (Applications)**。

步骤 3 点击**保护应用 (Protect an Application)** 并在应用列表中找到 **Cisco Firepower Threat Defense VPN**。

步骤 4 点击**保护此应用 (Protect this Application)** 以获取您的集成密钥、密钥和 API 主机名。配置代理时，您将需要此信息。如需帮助，请参阅《*Duo* 入门指南》https://duo.com/docs/getting-started。

步骤 5 安装和配置 Duo 身份验证代理。有关说明，请参阅中的“安装 Duo 身份验证代理”部分。https://duo.com/docs/cisco-firepower

步骤 6 启动身份验证代理。有关说明，请参阅中的“启动代理”部分。https://duo.com/docs/cisco-firepower

有关在 Duo 中注册新用户的信息，请参阅 https://duo.com/docs/enrolling-users。https://duo.com/docs/enrolling-users

使用 CDO 为 Duo RADIUS 配置设备

过程

步骤 1 配置 FTD Radius 服务器对象。

a) 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

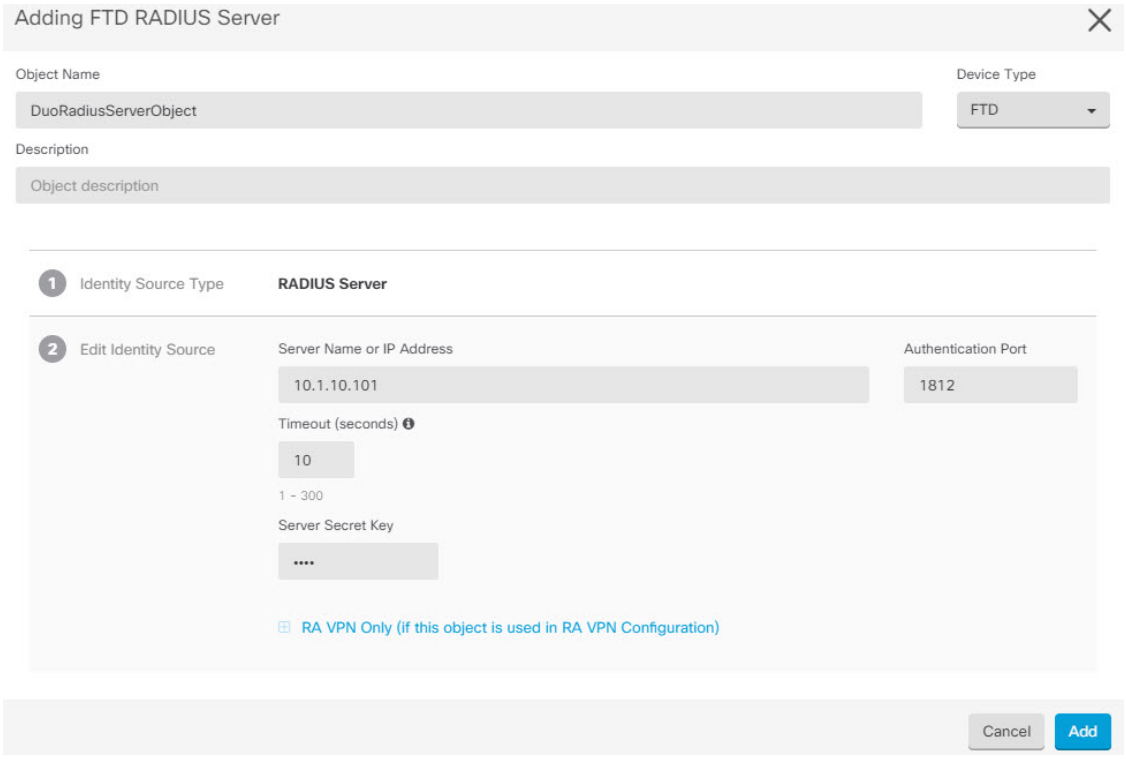
b) 点击 > RA VPN 对象（ASA 和 FTD） > 身份源。 

c) 提供名称并将设备类型设置为 FTD。

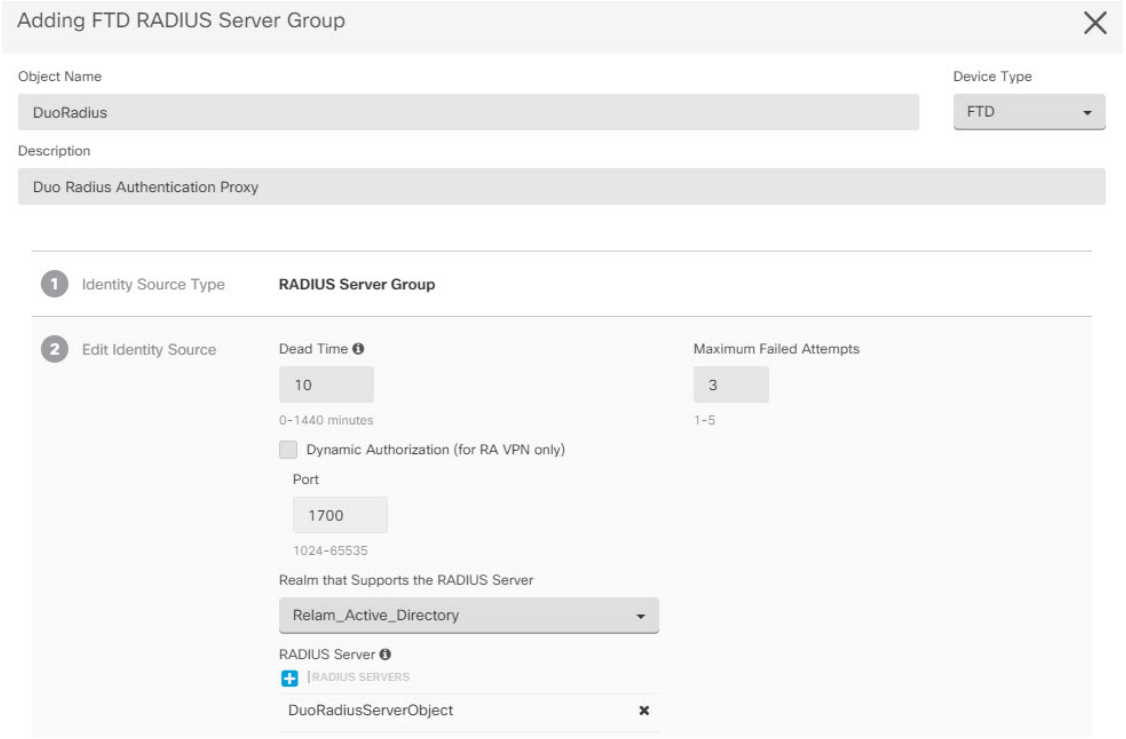
d) 选择 Radius 服务器组，然后点击继续。有关详细信息，请参阅中的步骤 6。创建 RADIUS 服务器组，第 475 页

e) 在 Radius Server 部分，点击 Add 按钮，然后点击 Create New Radius Server。请参阅创建 RADIUS 服务器对象，第 474 页

在服务器名称或 IP 地址字段中，输入 Duo 身份验证代理服务器的完全限定主机名或 IP 地址。



f) 将 Duo RADIUS 服务器添加到组后，点击添加以创建新的 Duo RADIUS 服务器组。



步骤 2 将远程接入 VPN 身份验证方法更改为 Duo RADIUS。

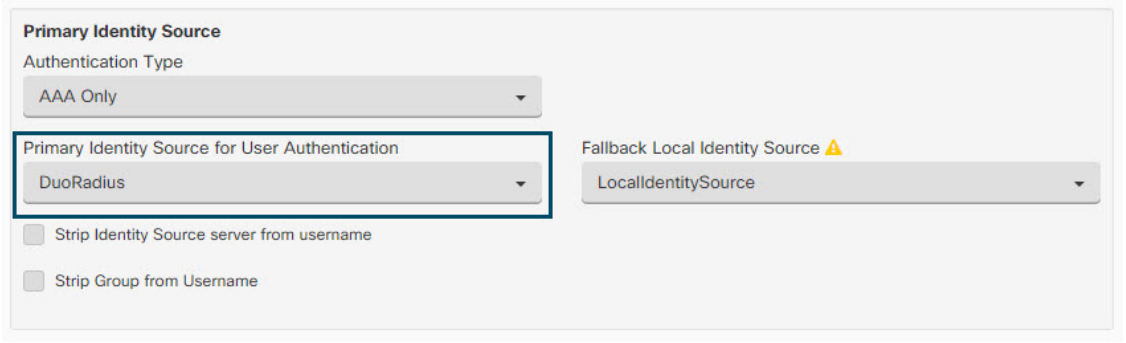
a) 在 CDO 导航菜单中，点击 VPN > 远程接入 VPN 配置。

b) 展开 VPN 配置，然后点击要向其添加 Duo 的连接配置文件。

c) 在右侧的**操作 (Actions)** 窗格中，点击**编辑 (Edit)**。

d) **身份验证类型 (Authentication Type)** 可以选择 **AAA** 或 **AAA 和客户端证书 (AAA and Client Certificate)**。

e) 在“用户身份验证的主身份源”(Primary Identity Source for User Authentication) 列表中，选择您之前创建的服务器组。



f) 您通常不需要选择“授权服务器”或“审计服务器”。

g) 点击**继续 (Continue)**。

h) 在摘要和说明步骤中，点击完成以保存配置。

步骤 3 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

使用 *LDAP* 的 *Duo* 双因素身份验证

您可以将 Duo LDAP 服务器作为辅助身份验证源与作为主要源的 Microsoft Active Directory (AD) 或 RADIUS 服务器结合使用。使用 Duo LDAP 时，辅助身份验证使用 Duo 密码、推送通知或电话呼叫验证主要身份验证。

注释 Duo 双因素身份验证功能在 CDO 中适用于运行 Firepower 威胁版本 6.5 或更高版本的设备。升级单个 FTD 设备，第 213 页

FTD 设备使用通过端口 TCP/636 的 LDAPS 与 Duo LDAP 通信。

使用此方法时，用户必须使用 AD/RADIUS 服务器和 Duo LDAP 服务器上配置的用户名进行身份验证。系统提示通过 AnyConnect 登录时，用户应在主密码字段中提供 AD/RADIUS 密码，对于辅助密码，可以提供以下选项之一来使用 Duo 进行身份验证。有关更多详细信息，请参阅中的“用于选择因素的第二个密码”部分。https://guide.duo.com/anyconnect

- *Duo* 密码 - 使用密码进行身份验证，密码将由 Duo Mobile 生成、通过 SMS 发送、由硬件令牌生成或由管理员提供。例如，1234567。
- **推送** - 如果已安装并激活 Duo Mobile 应用，请将登录请求推送至您的手机。查看请求并点击**批准**以登录。
- **电话** - 使用电话呼叫进行身份验证。
- **短信** - 以短信消息请求 Duo 密码。登录尝试失败。使用新密码重新登录。

有关详细说明，请参阅如何使用 Duo LDAP 配置双因素身份验证，第 456 页。

如何使用 Duo LDAP 配置双因素身份验证

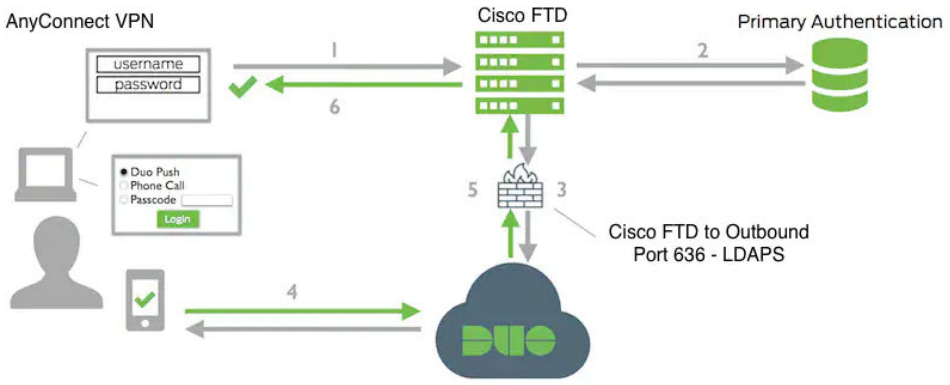
您可以将 Duo LDAP 服务器作为辅助身份验证源与作为主要源的 Microsoft Active Directory (AD) 或 RADIUS 服务器结合使用。使用 Duo LDAP 时，辅助身份验证使用 Duo 密码、推送通知或电话呼叫验证主要身份验证。

以下主题详细说明这种类型的高级配置：

Duo LDAP 辅助身份验证系统流程

下图显示的是 威胁防御 如何和 Duo 共同发挥作用，以使用 LDAP 提供双因素身份验证。

以下是系统流程的说明：



1. 用户对 FDM 管理 设备进行远程访问 VPN 连接，并提供用户名和密码。
2. FDM 管理 设备使用主身份验证服务器（可能是 Active Directory 或 RADIUS）对此主要身份验证尝试进行身份验证。
3. 如果主身份验证正常工作， FDM 管理 设备会将辅助身份验证请求发送至 Duo LDAP 服务器。
4. 然后，通过推送通知、带密码的短信消息或电话呼叫单独对用户进行身份验证。用户必须成功完成此身份验证。
5. Duo 响应 FDM 管理 设备，以指示用户是否已成功进行身份验证。
6. 如果辅助身份验证成功，则 FDM 管理 设备会与用户的 AnyConnect 客户端建立远程接入 VPN 连接。

配置 Duo LDAP 辅助身份验证

以下操作步骤介绍配置双因素身份验证的端到端过程，使用 Duo LDAP 作为辅助身份验证源，用于远程访问 VPN。您必须拥有一个 Duo 账户，并从 Duo 获取一些信息，才能完成此配置。

创建 Duo 账户

创建 Duo 账户并获取集成密钥、密钥和 API 主机名。

以下是对此过程的概述。有关详细信息，请参阅 Duo 网站。

过程

步骤 1 注册 Duo 账户。

步骤 2 登录到 Duo 管理面板 (Duo Admin Panel) 并导航至**应用 (Applications)**。

步骤 3 点击**保护应用 (Protect an Application)** 并在应用列表中找到 **Cisco Firepower Threat Defense VPN**。

步骤 4 点击**保护此应用 (Protect this Application)** 以获取您的**集成密钥**、**密钥**和 **API 主机名**。如需帮助，请参阅《*Duo* 入门指南》https://duo.com/docs/getting-started。

有关在 Duo 中注册新用户的信息，请参阅 https://duo.com/docs/enrolling-users。https://duo.com/docs/enrolling-users

将受信任的 CA 证书上传到设备FDM 管理

FDM 管理 设备必须具有验证与 Duo LDAP 服务器的连接所需的可信 CA 证书。您可以直接转至 https://www.digicert.com/digicert-root-certificates.htm 并下载 **DigiCertSHA2HighAssuranceServerCA** 或 **DigiCert High Assurance EV Root CA**，然后使用 防火墙设备管理器 (FDM) 将其上传。

过程

步骤 1 访问 FDM 管理 设备的 防火墙设备管理器 页面，选择**对象 (Objects)** > **证书 (Certificates)**。

步骤 2 点击 + > **添加受信任 CA 证书 (Add Trusted CA Certificate)**。

步骤 3 输入证书名称，例如，DigiCert_High_Assurance_EV_Root_CA。（不允许使用空格。）

步骤 4 点击**上传证书 (Upload Certificate)**，然后选择下载的文件。

步骤 5 点击**确定 (OK)**。

步骤 6 如果尚未将设备载入 思科防御协调器，请将其载入。

步骤 7 读取所有设备配置。

在 CDO 中为 Duo LDAP 配置 FTD

过程

步骤 1 创建用于 Duo LDAP 服务器的 Duo LDAP 身份源对象。

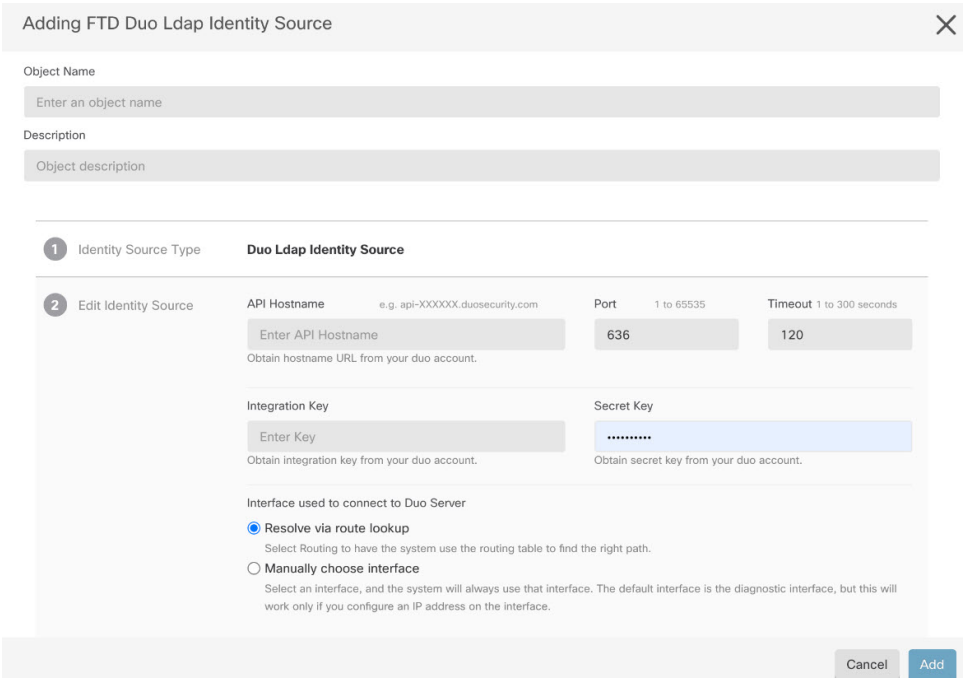
a) 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

b) 点击  以创建一个对象 > **RA VPN 对象 (ASA & FTD) (RA VPN Objects [ASA & FTD])** > **身份源 (Identity Source)**。

c) 为对象输入一个名称，例如 Duo-LDAP-server。

d) 选择**设备类型**作为 **FTD**。

e) 点击 **Duo LDAP 身份源**，然后点击 **Continue**。



f) 在**编辑身份源**区域中，提供以下详细信息：

- **API 主机名 (API Hostname)**：请输入您从 Duo 账户中获取的 API 主机名。主机名应如下所示，X 替换为您的唯一值：API-XXXXXXXX.DUOSECURITY.COM。无需大写。
- **端口 (Port)**：请输入用于 LDAPS 的 TCP 端口。这应该是 636，除非 Duo 通知您使用不同端口。请注意，必须确保访问控制列表允许通过此端口流向 Duo LDAP 服务器的流量。
- **超时 (Timeout)**：请输入连接到 Duo 服务器所采用的超时时间（以秒为单位）。值可以是 1-300 秒。默认值为 120。要使用默认值，请输入 120 或删除该属性行。
- **集成密钥 (Integration Key)**：请输入从您的 Duo 账户获取的集成密钥。
- **密钥 (Secret Key)**：输入从您的 Duo 账户获取的密钥。此密钥随后将被屏蔽。
- **用于连接到 Duo 服务器的接口**：选择用于连接到 Duo 服务器的接口。
  - **通过路由查找解析**：选择此选项可使用路由表查找正确的路径。有关创建路由表的信息，请参阅路由。
  - **手动选择接口**：选择此选项并从列表中选择一个接口。默认接口为诊断接口，但此操作仅当在接口上配置 IP 地址时有效。注意：确保所选接口存在于要连接到 Duo Server 的同一设备上。
  - 点击**添加 (Add)**。

步骤 2 （可选）使用 AnyConnect 配置文件编辑器创建配置文件，将身份验证超时值指定为 60 秒或更长时间。

需要为用户提供额外的时间来获取 Duo 密码并完成辅助身份验证。我们建议将此时间设置为至少 60 秒。以下操作步骤介绍如何仅配置身份验证超时，然后将配置文件上传至 FDM 管理 设备。如果要更改其他设置，现在就可以进行更改。

a) 如果尚未执行此操作，请下载并安装 AnyConnect 配置文件编辑器软件包。可以在思科软件中心 (software.cisco.com) 相应 AnyConnect 版本文件夹内找到此软件包。截至我们编制本文件时，基本路径是**下载主页 (Downloads Home)** > **安全 (Security)** > **VPN 和终端安全客户端 (VPN and Endpoint Security Clients)** > **思科 VPN 客户端 (Cisco VPN Clients)** > **AnyConnect 安全移动客户端 (AnyConnect Secure Mobility Client)**。

b) 打开 AnyConnect **VPN 配置文件编辑器**。

c) 在目录中选择**首选项（第 2 部分）**，滚动至页面末尾，并将**身份验证超时**更改为 60（或更大值）。以下是来自 AnyConnect 4.7 VPN 配置文件编辑器的图像；先前或后续版本可能不同。

d) 选择**文件 (File)** > **保存 (Save)**，将配置文件 XML 文件保存至您的工作站，并使用适当名称（例如，duo-ldap-profile.xml）。

e) 现在，可以关闭 **VPN 配置文件编辑器**应用。

f) 在CDO 中，上传 RA AnyConnect 客户端配置文件。

步骤 3 创建组策略，并在策略中选择 AnyConnect 配置文件。

分配给用户的组策略控制连接的许多方面。以下操作步骤介绍如何将配置文件 XML 文件分配到组。有关详细信息，请参阅创建新的 RA VPN 组策略。

a) 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

b) 要编辑现有组策略，请使用 **RA VPN 组策略**过滤器仅查看现有组策略，修改所需的策略并保存。

c) 要创建新的组策略，请点击 **RA VPN 对象（ASA 和 FTD）(RA VPN Objects [ASA & FTD])** > **RA VPN 组策略 (RA VPN Group Policy)**。

d) 在**常规 (General)** 页面上，配置以下属性：

- **名称 (Name)** - 对于新的配置文件，请输入名称。例如，Duo-LDAP-group。
- **AnyConnect 客户端配置文件 (AnyConnect Client Profiles)** - 选择您创建的 AnyConnect 客户端配置文件对象。

e) 点击**添加 (Add)** 以保存对象。

f) 点击 **VPN** > **远程访问 VPN 配置 (Remote Access VPN Configuration)**。

g) 点击要更新的远程接入 VPN 配置。

h) 在右侧的**操作**窗格中，点击**组策略**。

i) 点击 + 选择要与 VPN 配置关联的组策略。

j) 点击**保存**以保存组策略。

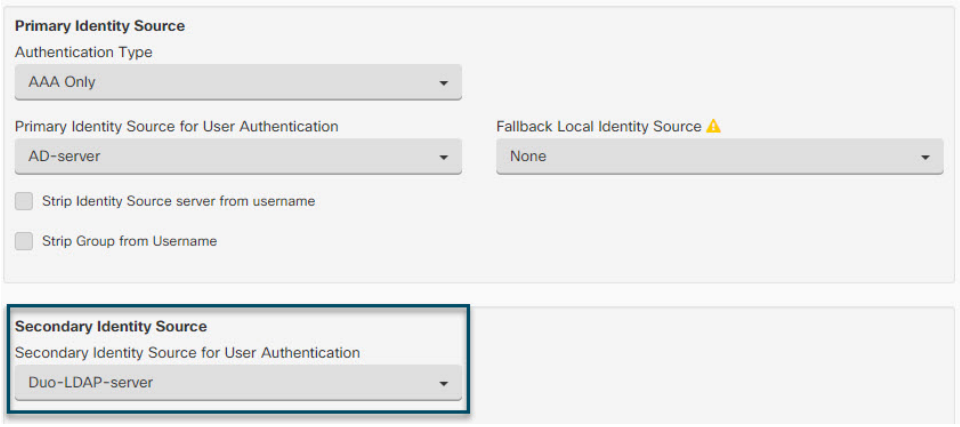
步骤 4 创建或编辑用于 Duo-LDAP 辅助身份验证的远程访问 VPN 连接配置文件。

以下操作过程仅介绍将 Duo-LDAP 启用为辅助身份验证源并应用 AnyConnect 客户端配置文件所需执行的密钥更改。对于新连接配置文件，必须配置其余必填字段。对于此操作过程，我们假设您正在编辑现有连接配置文件，而且您必须更改这两个设置。

a) 在 CDO 导航页面上，点击 **VPN** > **远程接入 VPN 配置**。

b) 展开远程接入 VPN 配置，然后点击要更新的连接配置文件。
c) 在右侧的**操作 (Actions)** 窗格中，点击**编辑 (Edit)**。
d) 在**主身份源 (Primary Identity Source)** 下，配置以下内容：

- **身份验证类型 (Authentication Type)** - 选择“仅 AAA”(AAA Only) 或“AAA 和客户端证书”(AAA and Client Certificate)。除非使用 AAA，否则无法配置双因素身份验证。
- **用于用户身份验证的主要身份源 (Primary Identity Source for User Authentication)** - 选择主 Active Directory 或 RADIUS 服务器。请注意，可以选择一个 Duo-LDAP 身份源作为主要源。然而，Duo-LDAP 仅提供身份验证服务，而不提供身份服务，因此，如果将其作为主要身份验证源，则在任何控制面板中都将看不到与 RA VPN 连接关联的用户名，且将无法为这些用户编写访问控制规则。（如有需要，可将回退配置为本地身份源。）
- **辅助身份源 (Secondary Identity Source)** - 选择 Duo-LDAP 身份源。



注释 如果**主身份源**和**辅助身份源**中的用户名相同，我们建议在连接配置文件的**高级**选项中启用**使用主用户名进行辅助登录**。通过这种方式配置，最终用户可以将单个用户名同时用于主要和辅助身份源。

e) 点击**继续 (Continue)**。
f) 在**组策略 (Group Policy)** 页面中，选择您创建或编辑的组策略。

g) 点击**继续 (Continue)**。
h) 点击**完成 (Done)**，将更改保存至连接配置文件。

步骤 5 预览和部署所有设备的配置更改，第 556 页。

FDM 管理设备的端到端远程接入 VPN 配置过程

本节提供在载入到CDO的FDM 管理设备上配置远程访问虚拟专用网络 (RA VPN) 的端到端程序。

要为客户端启用远程访问 VPN，需要配置多个单独的项目。以下程序介绍了端到端流程。

Procedure

步骤 1 启用两个许可证。

- 注册设备时，必须使用为受到出口管制的功能启用的智能软件管理器帐户执行此操作。许可证必须符合出口控制要求，然后才能配置远程访问 VPN。您也不能使用评估许可证配置该功能。您购买的 FDM 管理 设备会自动附带许可证。许可证涵盖可选许可证未覆盖的所有功能。它是一种永久许可证。设备必须注册到 Firepower 设备管理器。请参阅《思科Firepower Threat Defense 配置指南》的“许可系统”一章中的**注册设备**部分，了解您的设备正在运行的版本。
- 许可证。有关详细信息，请参阅远程访问 VPN 的许可要求。
  - 要启用许可证，请参阅《配置指南》的“许可系统”一章中的**启用或禁用可选许可证**部分。

步骤 2 配置证书。

对客户端与设备之间的 SSL 连接进行身份验证需要使用证书。您可以将预定义的 DefaultInternalCertificate 用于 VPN，也可以自行创建证书。

如果对用于身份验证的目录领域使用加密连接，则必须上传受信任的 CA 证书。有关证书及其上传方法的详细信息，请参阅配置证书。

步骤 3 配置用于对远程用户进行身份验证的身份源。

您可以使用以下来源对尝试使用 RA VPN 连接到您的网络的用户进行身份验证。此外，可以使用客户端证书进行身份验证，可单独使用，也可与身份源配合使用。

- Active Directory 身份领域：作为主要身份验证源。在 Active Directory AD 服务器中定义用户账户。请参阅“配置 AD 身份领域”。请参阅创建或编辑 Active Directory 领域对象。
- RADIUS 服务器组：充当主要或辅助身份验证源，并用于授权和记账。请参阅创建或编辑 RADIUS 服务器对象或组。
- 本地身份源（本地用户数据库）：作为主要或回退源。您可以直接在设备上定义用户，不使用外部服务器。如果您使用本地数据库作为回退源，请确保您定义与外部服务器中描述的相同用户名/密码。

  Note 您只能直接在FDM 管理设备上从Firepower 设备管理器中创建用户账户。请参阅配置本地用户。

步骤 4 （可选。）创建新的 RA VPN 组策略。

组策略定义用户相关的属性。可以配置组策略，根据组成员身份提供差异化的资源访问权限。或者，可以对所有连接使用默认策略。

步骤 5 创建 RA VPN 配置。

步骤 6 配置 RA VPN 连接配置文件。

步骤 7 预览和部署所有设备的配置更改。

步骤 8 允许流量通过远程访问 VPN。

步骤 9 （可选。）启用身份策略并配置被动身份验证规则。如果启用被动用户验证，通过远程访问VPN登录的用户将显示在控制面板上，他们也可以用作策略中的流量匹配条件。如果不启用被动身份验证，只有当远程访问VPN用户匹配主动身份验证策略时，这些用户才可用。必须启用身份策略以在控制面板中获取任何用户名信息，或将其用于流量匹配。请参阅配置身份策略。

Important 如果使用本地管理器（如 Firepower 设备管理器）更改远程访问 VPN 配置，CDO 中该设备**的配置状态 (Configuration Status)** 将显示“检测到冲突”(Conflict Detected)。请参阅设备上的带外更改。您可以解决配置冲突。

What to do next

将 RA VPN 配置下载到设备后，用户可以使用连接到互联网的计算机或其他受支持的 iOS 或 Android 设备从远程位置连接到您的网络。FDM 管理您可以从租户中所有已自行激活的 RA VPN 前端监控实时 AnyConnect 远程访问虚拟专用网络 (RA VPN) 会话。请参阅监控远程访问虚拟专用网络会话。

下载 *AnyConnect* 客户端软件包

在配置远程接入 VPN 之前，必须将 AnyConnect 软件包从 https://software.cisco.com/download/home/283000185 下载到您的工作站。确保为所需的操作系统下载“AnyConnect 前端部署软件包”。稍后，您可以在定义 VPN 时将这些软件包上传到 Firepower 威胁防御 (FTD) 设备。

始终下载最新的 AnyConnect 版本，以确保获得最新的功能、漏洞修复和安全补丁。请定期更新设备上的软件包。

Note 您可以为以下每个操作系统 (OS) 上传一个 AnyConnect 软件包：Windows、Mac 和 Linux。无法为特定操作系统类型上传多个版本。

将 *AnyConnect* 软件包上传到运行版本 *6.4.0* 的 *FDM* 管理设备

您可以使用 防火墙设备管理器 API 资源管理器将 AnyConnect 软件包上传到 FDM 管理 设备版本 6.4.0。设备上必须至少有一个 AnyConnect 软件包才能创建 RA VPN 连接。

Important 该程序仅适用于 防火墙设备管理器 版本 6.4。如果您使用的是 防火墙设备管理器 版本 6.5 或更高版本，请使用 思科防御协调器 界面来将 AnyConnect 软件包上传到运行 FDM 管理 6.5 或更高版本的设备。

使用以下程序将 AnyConnect 软件包上传到 防火墙设备管理器 版本 6.4.0：

Procedure

步骤 1 从 https://software.cisco.com/download/home/283000185 下载 AnyConnect 软件包。

- 确保您接受 EULA 并具有 K9（加密映像）权限。
- 为您的操作系统选择“AnyConnect 前端部署软件包”。软件包名称类似于“anyconnect-win-4.7.04056-webdeploy-k9.pkg”。Windows、macOS 和 Linux 有单独的前端 Web 部署软件包。

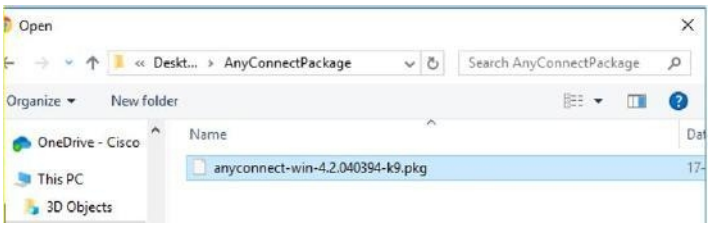
步骤 2 使用浏览器打开系统主页。例如，https://ftd.example.com。

步骤 3 登录至 防火墙设备管理器。

步骤 4 编辑 URL，使其指向 /#/api-explorer，例如 https://ftd.example.com/#/api-explorer。

步骤 5 向下滚动并点击 Upload /action/uploaddiskfile。 >

步骤 6 在 fileToUpload 字段中，点击 Choose File 并选择所需的 AnyConnect 软件包。您可以一次上传一个软件包。



步骤 7 点击**打开 (Open)**。

步骤 8 向下滚动并点击**试用！(TRY IT OUT!)**。等待数据包完全上传。在响应正文中，API 响应按以下格式显示。

{ "version": null, "name": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
"fileName": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
"id": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
"type": "fileuploadstatus",
"links": {
"self":
“https://ftd.example.com:972/api/fdm/...90d111e9-a361-%20cf32937ce0df.pkg”
} }

记录响应中的软件包的 fileName，因为在执行 POST 操作时必须输入相同的字符串。在本例中，fileName 为 691f47e1-90c7-11e9-a361-79e2452f0c57.pkg。

步骤 9 向上滚动到 威胁防御 REST API 页面顶部，然后点击 **AnyConnectPackageFile > POST /object/anyconnectpackagefiles**。对 API 执行 POST 操作，在负载中提供临时磁盘文件名和软件包文件的操作系统类型。此操作会创建 AnyConnect 软件包文件。

步骤 10 在正文字段中，仅按以下格式输入软件包详细信息：

{ "platformType": "WINDOWS",

"diskFileName": "691f47e1-90c7-11e9-a361-79e2452f0c57.pkg",
"type": "anyconnectpackagefile",
"name": "AnyConnectWindowsBGL" }

a. 在 platformType 字段中，输入操作系统平台为 WINDOWS、MACOS 或 LINUX。

b. 在 diskFileName 字段中，输入您在上传磁盘文件后记录的 fileName。

c. 在**名称 (name)** 字段中，输入要用于软件包的名称。

d. 点击试用！。

在“响应正文”字段中，成功执行 POST 操作后，API 响应将按以下格式显示。

{ "version": "ni7xeneslft3p",
"name": "AnyConnectWindowsBGL",
"description": null,
"diskFileName": "41d592e3-90ca-11e9-a361-6d05320a165d.pkg",
"md5Checksum": "9bbe53dcf92e515d3ce5423048212488",
"platformType": "WINDOWS",
"id": "c9c9dfe3-9cd8-11e9-a361-23534f081c43",
"type": "anyconnectpackagefile",
"links": { "self":

" https:/>/ftd.example.com:972...1-cf32937ce0df "https://bglgrp1224-pod.cisco.com:972/api/fdm/v3/object/anyconnectpackagefiles/7f8248c7-90d1-11e9-a361-cf32937ce0df

}
}

在 防火墙设备管理器 上创建 AnyConnect 软件包。

步骤 11 点击 AnyConnectPackageFile GET /object/anyconnectpackagefiles TRY IT OUT!。 > >

响应正文显示所有 AnyConnect 软件包文件。

示例响应如下所示。

{
"items": [
{
"version": "la4nwceqk2sg4",
"name": "AnyConnectWindowsBGL",
"description": null,
"diskFileName": "82f1e362-9cd8-11e9-a361-9758ba07962d.pkg",
"md5Checksum": "9bbe53dcf92e515d3ce5423048212488",
"platformType": "WINDOWS",
"id": "c9c9dfe3-9cd8-11e9-a361-23534f081c43",
"type": "anyconnectpackagefile",
"links": {

"self":
"https://ftd.example.com:972...1-23534f081c43"
}
}
],

步骤 12 为每种操作系统类型上传其他 AnyConnect 软件包。重复步骤 4 到 10。

步骤 13 编辑 URL 以指向网页，例如 https://ftd.example.com https://ftd.example.com/#/api-explorer

步骤 14 点击网页右上角的**部署更改 (Deploy Changes)** 图标。若有未部署的更改，系统会用圆点高亮显示。

步骤 15 如果您对所做的更改比较满意，可以点击**立即部署 (Deploy Now)** 立即启动作业。窗口将显示部署正在进行。您可以关闭窗口，或等待部署完成。

Note 要从设备中删除软件包，请点击 AnyConnectPackageFile Delete。FDM 管理 > 在 objID 字段中，键入软件包 ID，然后点击试用！

要完成 VPN 连接，您的用户必须在他们的工作站上安装 AnyConnect 客户端软件。有关详细信息，请参阅用户如何在 FDM 管理设备上安装 AnyConnect 客户端软件, on page 496。

将 *AnyConnect* 软件包上传到运行 *FDM* 管理 *6.5* 或更高版本的设备

如果您使用运行 升级单个 FTD 设备的 FDM 管理 设备来配置 RA VPN，则可以使用 思科防御协调器 中的 RA VPN 向导将 AnyConnect 软件包上传到设备。在 RA VPN 向导中，必须提供预加载 AnyConnect 软件包的远程 HTTP 或 HTTPS 服务器的 URL。

Note 您也可以使用 FDM API 程序上传 AnyConnect 软件包。将 AnyConnect 软件包上传到运行版本 6.4.0 的 FDM 管理设备, on page 463

从 CDO 存储库上传 AnyConnect 软件包

远程接入 VPN 配置向导显示 CDO 存储库中每个操作系统的 AnyConnect 软件包，您可以从中选择并上传到设备。确保设备可以访问互联网并进行正确的 DNS 配置。

注释 如果所需的软件包在显示的列表中不可用，或者设备无法访问互联网，则可以使用预加载 AnyConnect 软件包的服务器上传软件包。

过程

步骤 1 点击与操作系统对应的字段，然后选择 AnyConnect 软件包。

步骤 2 点击 以上传软件包。如果校验和不匹配，则 AnyConnect 软件包上传失败。您可以查看设备的工作流程选项卡，了解有关故障的更多详细信息。

准备工作

请确保为所需的操作系统下载“AnyConnect 前端部署软件包”。始终下载最新的 AnyConnect 版本，以确保获得最新的功能、漏洞修复和安全补丁。请定期更新设备上的软件包。

Note 您可以为以下每个操作系统 (OS) 上传一个 AnyConnect 软件包：Windows、Mac 和 Linux。无法为特定操作系统类型上传多个版本。

Procedure

步骤 1 从 https://software.cisco.com/download/home/283000185 下载 AnyConnect 软件包。

- 确保您接受 EULA 并具有 K9（加密映像）权限。
- 为您的操作系统选择“AnyConnect 前端部署软件包”。软件包名称类似于“anyconnect-win-4.7.04056-webdeploy-k9.pkg”。有适用于 Windows、macOS 和 Linux 的单独前端软件包。

步骤 2 将 AnyConnect 软件包上传到远程 HTTP 或 HTTPS 服务器。确保存在从 FDM 管理 设备到 HTTP 或 HTTPS 服务器的网络路由。

Note 如果要将 AnyConnect 软件包上传到 HTTPS 服务器，请确保执行以下步骤：

- 从 防火墙设备管理器 上传 FDM 管理 设备上该服务器的受信任 CA 证书。要上传证书，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南，版本 XY》“证书”一章中的“上传受信任 CA 证书”部分https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html#anchor613
- 在 HTTPS 服务器上安装受信任的 CA 证书。

步骤 3 远程服务器的 URL 必须是不提示进行身份验证的直接链接。如果 URL 已进行预身份验证，则可以通过指定 RA VPN 向导的 URL 来下载文件。

步骤 4 如果远程服务器 IP 地址经过 NAT，则必须提供远程服务器位置的 NAT 公共 IP 地址。

上传新的 AnyConnect 软件包

使用以下程序将新的 AnyConnect 软件包上传到运行版本 6.5.0 的 FDM 管理 设备：

Procedure

步骤 1 根据步骤 1-4 创建 RA VPN 配置。创建 RA VPN 配置, on page 483

步骤 2 在**检测到的 AnyConnect 软件包 (AnyConnect Package Detected)** 中，您可以为 Windows、Mac 和 Linux 终端上传单独的软件包。

步骤 3 在相应的平台字段中，指定预上传与 Windows、Mac 和 Linux 兼容的 AnyConnect 软件包的服务器路径。服务器路径示例：'http://<ip_address> :port_number/<folder_name> /anyconnect-win-4.8.01090-webdeploy-k9.pkg', 'https:// :port_number/ /anyconnect-linux64-4.7.03052-webdeploy-k9.pkg'。

步骤 4 点击 以上传软件包。CDO 验证路径是否可访问，以及指定的文件名是否有效。验证成功后，系统将显示 AnyConnect 软件包的名称。当您将更多设备添加到 RA VPN 配置时，您可以将 AnyConnect 软件包上传到这些设备。FDM 管理

步骤 5 点击**确定 (OK)**。AnyConnect 软件包已添加到 RA VPN 配置中。

步骤 6 从第 6 步开始继续创建 RA VPN 配置。创建 RA VPN 配置, on page 483

What to do next

要完成 VPN 连接，您的用户必须在他们的工作站上安装 AnyConnect 客户端软件。有关详细信息，请参阅用户如何在 FTD 上安装 AnyConnect 客户端软件。用户如何在 FDM 管理设备上安装 AnyConnect 客户端软件, on page 496

替换现有的 AnyConnect 软件包

如果设备上已存在 AnyConnect 软件包，您可以在 RA VPN 向导中看到它们。您可以在下拉列表中查看操作系统的所有可用 AnyConnect 软件包。您可以从列表中选择现有软件包并将其替换为新软件包，但不能向列表中添加新软件包。

Note 如果要将现有软件包替换为新软件包，请确保新的 AnyConnect 软件包已上传到设备可访问的网络上的服务器。FDM 管理

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **VPN > 远程访问 VPN (Remote Access VPN)**。

步骤 2 选择要修改的 RA VPN 配置，然后在操作下点击编辑。

步骤 3 在“检测到的 AnyConnect 软件包”中，点击现有 AnyConnect 软件包旁边的图标。如果操作系统有多个版本的 AnyConnect 软件包，请从列表中选择要替换的软件包，然后点击编辑。现有软件包将从相应字段中消失。

步骤 4 指定预加载新 AnyConnect 软件包的服务器路径，然后点击 上传软件包。

步骤 5 点击**确定 (OK)**。新的 AnyConnect 软件包已添加到 RA VPN 配置中。

步骤 6 从第 6 步开始继续创建 RA VPN 配置。创建 RA VPN 配置, on page 483

删除 AnyConnect 软件包

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **VPN** > **远程访问 VPN (Remote Access VPN)**。

步骤 2 选择要修改的 RA VPN 配置，然后在操作下点击编辑。

步骤 3 在“检测到的 AnyConnect 软件包”中，点击要删除的 AnyConnect 软件包旁边的图标。如果某个操作系统有多个版本的AnyConnect软件包，请从列表中选择要删除的软件包。现有软件包将从相应字段中消失。

Note 点击取消以停止删除操作并保留现有软件包，

步骤 4 点击**确定 (OK)**。设备的配置状态处于“未同步”状态。

Note 如果要在此阶段撤消删除操作，请转到设备和服务页面，然后点击放弃更改以保留现有的 AnyConnect 软件包。

步骤 5 预览和部署所有设备的配置更改。

为 *FDM* 管理 设备配置身份源

身份源（例如 Microsoft AD 领域和 RADIUS 服务器）是为组织内的人员定义用户账户的 AAA 服务器和数据库。身份源信息具有多种用途，例如提供与IP地址关联的用户身份，或是对远程访问 VPN 连接或到 思科防御协调器的访问进行身份验证。

点击 **对象 (Objects) > FDM 对象 (FDM Objects)**，然后点击  并选择 **> RA VPN 对象（ASA 和 FTD）(RA VPN Objects [ASA & FTD]) > 身份源 (Identity Source)** 以创建源。后期配置需要使用身份源的服务时，可以使用这些对象。您可以应用适当的过滤器来搜索现有源并对其进行管理。

Active Directory 领域

Active Directory 可提供用户账户和身份验证信息。将包含 AD 领域的配置部署到FDM 管理 设备时，CDO 会从 AD 服务器获取用户和组。

您可以将此源用于以下目的：

- 远程访问 VPN，作为主要身份源。您可以配合使用 AD 和 RADIUS 服务器。
- 身份策略，用于主动身份验证，并作为用户身份源用于被动身份验证。
- 身份规则，适用于用户的主动身份验证。

您可以使用用户身份创建访问控制规则。有关详细信息，请参阅如何实施 Firepower 身份策略。

CDO 每 24 小时请求一次更新的用户组列表。由于最多可以向规则中添加 50 个用户或组，所以选择组比选择单个用户通常更有意义。例如，您可以创建一条规则允许“工程”组访问开发网络，并创建一条后续规则拒绝对该网络的所有其他访问。然后，要将该规则应用于新工程师，您只需添加将工程师添加到目录服务器的“工程”组即可。

CDO 中的 Active Directory 领域

在创建 AD 身份对象时配置 AD 领域。身份源对象向导可帮助确定如何连接到 AD 服务器以及 AD 服务器在网络中的位置。

Note 如果在 CDO 中创建 AD 领域，则在创建附属身份源对象以及将这些对象添加到身份规则时，CDO 会记住 AD 密码。

FDM 中 Active Directory 领域

您可以从 CDO 对象向导指向在 FDM 中创建的 AD 领域对象。请注意，CDO 不会读取在 FDM 中创建的 AD 领域对象的 AD 密码。您必须在 CDO 中手动输入正确的 AD 密码。

要在 防火墙设备管理器 中配置 AD 领域，请参阅适用于运行设备的版本的《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》中可重用对象一章的**配置 AD 身份领域**部分。

支持的目录服务器

可以使用 Windows Server 2008 和 2012 上的 AD。

请注意以下有关服务器配置的信息：

- 如果要对用户组或组内用户执行用户控制，则必须在目录服务器上配置用户组。如果服务器按照基本对象层次结构组织用户，系统无法执行用户组控制。
- 目录服务器必须使用下表中列出的字段名称，以便系统从该域的服务器中检索用户元数据：

元数据	Active Directory 字段
LDAP 用户名	samaccountname
First name	名称
姓氏	sn
邮箱地址	mail Userprincipalname（如果 mail 没有值）
部门	department distinguishedname（如果 department 没有值）
电话号码	telephonenumber

确定目录基准标识名

配置目录属性时，需要为用户和组指定公共基准标识名 (DN)。基准在您的目录服务器中定义，并且会因网络而不同。您必须输入正确的基准，身份策略才能正常使用。如果基准错误，则系统无法确定用户名或组名，进而导致基于身份的策略无法使用。

Note 要获得正确的基准，请咨询目录服务器的管理员。

对于 Active Directory，您可以用域管理员的身份登录 AD 服务器，并按照如下所示在命令提示符后输入 **dsquery** 命令来确定正确的基准：

用户搜索库

输入具有已知用户名（部分或完整）的 **dsquery user** 命令，以确定基准标识名。例如，以下命令使用部分名称“John*”返回以“John.”开头的所有用户的信息。

C:\Users\Administrator>dsquery user -name "John*"

"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"

基准 DN 为“DC=csc-lab,DC=example,DC=com”。

组搜索基准

输入具有已知组名称的 **dsquery group** 命令，以确定基准 DN。例如，以下命令使用组名称 Employees 返回标识名：

C:\>dsquery group -name "Employees"

"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"

组基准 DN 为“DC=csc-lab,DC=example,DC=com”。

此外，您还可以使用 ADSI Edit 程序浏览 AD 结构 (**Start** > **Run** > **adsiedit.msc**)。在 ADSI Edit 中，右键点击任意对象，例如组织单位 (OU)、组或用户，然后选择**属性**查看标识名。然后，可以复制 DC 值的字符串作为基准。

要验证您是否获得了正确的基准，请执行以下操作：

Procedure

步骤 1 点击目录属性中的**测试连接 (Test Connection)** 按钮验证连接。解决所有问题后，保存目录属性。

步骤 2 提交对设备的更改。

步骤 3 创建访问规则，选择**用户**选项卡，并尝试从目录添加已知的用户和组名称。在您键入内容时，系统会自动填充建议，以匹配包含该目录的领域中的用户和组。如果这些建议显示在一个下拉列表中，则说明系统可以成功查询目录。如果您没有看到建议，而且确定您键入的字符串应显示在用户或组名称中，则需要更正相应的搜索基准。

What to do next

有关详细信息，请参阅创建或编辑 Active Directory 领域对象。

RADIUS 服务器和组

您可以使用 RADIUS 服务器对管理用户进行身份验证和授权。

配置要使用 RADIUS 服务器的功能时，您应选择 RADIUS 组而不是单个服务器。RADIUS 组所含 RADIUS 服务器是彼此副本的集合。如果一个组具有多个服务器，这些服务器可构成备份服务器链，在其中一台服务器不可用时提供冗余。但即使只有一台服务器，也必须创建包含一个成员的组，以配置功能的 RADIUS 支持。

您可以将此源用于以下目的：

- 远程访问 VPN 用作身份验证、授权和记账的身份源。您可以配合使用 AD 和 RADIUS 服务器。
- 身份策略，作为被动身份源来从远程访问 VPN 登录收集用户身份信息。

有关详细信息，请参阅创建或编辑 RADIUS 服务器对象或组。

相关信息：

- 创建或编辑 Active Directory 领域对象
- 创建或编辑 RADIUS 服务器对象或组
- 配置身份策略

创建或编辑 Active Directory 领域对象

关于 Active Directory 领域对象

当您创建或编辑身份源对象（例如 AD 领域对象）时，思科防御协调器 通过 SDC 将配置请求发送到 FDM 管理 设备。然后，FDM 管理 设备会与配置的 AD 领域通信。

请注意，CDO 不会读取通过 防火墙设备管理器 控制台配置的 AD 领域的目录密码。如果使用最初在 防火墙设备管理器 中创建的 AD 领域对象，则必须手动输入目录密码。

创建 FTD Active Directory 领域对象

使用以下程序创建对象：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击 ，然后点击 RA VPN 对象（ASA 和 FTD）身份源。 >

步骤 3 为对象输入**对象名称 (Object Name)**。

步骤 4 选择设备类型作为 FTD。

步骤 5 在向导的第一部分中，选择 Active Directory 领域作为身份源类型。点击**继续 (Continue)**。

步骤 6 配置基本领域属性。

- **目录用户名、目录密码 (Directory Username, Directory Password)** - 用户的标识名称和密码，该用户具备访问您要检索的用户信息的适当权限。对于 AD，用户不需要更高的权限。您可以在域中指定任何用户。用户名必须是完全限定的；例如，Administrator@example.com（而不仅仅是 Administrator）。

  Note 系统使用此信息生成 ldap-login-dn 和 ldap-login-password。例如，Administrator@example.com 被转换为 cn=administrator,cn=users,dc=example,dc=com。请注意，cn = users 始终是此转换的一部分，因此您必须在公用名“users”文件夹下配置此处指定的用户。

- **基准区别名称 (Base Distinguished Name)** - 用于搜索或查询用户和组信息的目录树，即用户和组的公共父项。例如，cn=users,dc=example,dc=com。
- **AD 主域 (AD Primary Domain)** - 设备应加入的完全限定 AD 域名。例如 example.com。

步骤 7 配置目录服务器属性。

- **主机名/IP 地址 (Hostname/IP Address)** - 目录服务器的主机名或 IP 地址。如果以加密方式连接到服务器，则必须输入完全限定域名，而非 IP 地址。
- **端口 (Port)** - 用于与服务器通信的端口号。默认值为 389。如果选择 LDAPS 作为加密方法，请使用端口 636。
- **加密 (Encryption)** - 要使用加密连接下载用户和组信息，请选择所需的方法 **STARTTLS** 或 **LDAPS**。系统默认为**无**，也就是说以明文形式下载用户和组信息。
  - **STARTTLS** 将会协商加密方法，并使用目录服务器支持的最强方法。使用端口 389。如果将领域用于远程访问 VPN，则不支持此选项。
  - **LDAPS** 需要基于 SSL 的 LDAP。使用端口 636。
- **受信任 SSL 证书 (Trusted CA Certificate)** - 如果选择加密方法，请上传证书颁发机构 (CA) 证书以便在系统和目录服务器之间启用受信任的连接。如果要使用证书进行身份验证，则证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 10.10.10.250 作为 IP 地址，但证书中的地址为 ad.example.com，则连接失败。

步骤 8 （可选）使用测试按钮验证配置。

步骤 9 （可选）点击添加其他配置，将多个 AD 服务器添加到 AD 领域。AD 服务器需要彼此复制并支持相同的 AD 域。因此，与该 AD 领域关联的所有 AD 服务器的基本领域属性（例如目录名称、目录密码和基本可分辨名称）必须相同。

步骤 10 点击**添加 (Add)**。

步骤 11 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

编辑 FTD Active Directory 领域对象

请注意，在编辑身份源对象时，不能更改身份源类型。您必须创建具有正确类型的新对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的对象。

步骤 3 选择要编辑的对象。

步骤 4 点击**操作 (Actions)** 窗格中的编辑图标 。

步骤 5 以在上述过程中创建值的相同方式编辑对话框中的值。展开下面列出的配置栏，以编辑或测试主机名/IP 地址或加密信息。

步骤 6 点击**保存 (Save)**。

步骤 7 CDO 显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

步骤 8 立即 预览和部署所有设备的配置更改 您所做的更改，或等待并一次部署多个更改。

相关信息：

- 创建或编辑 RADIUS 服务器对象或组
- 配置身份策略
- 配置身份规则
- 配置身份策略设置

创建或编辑 RADIUS 服务器对象或组

关于 RADIUS 服务器对象或组

在创建或编辑 RADIUS 服务器对象或一组 RADIUS 服务器对象等身份源对象时，CDO 会通过 SDC 将配置请求发送到 FDM 管理 设备。然后，FDM 管理 设备会与配置的 AD 领域通信。

创建 RADIUS 服务器对象

RADIUS 服务器提供 AAA（身份验证、授权和记账）服务。

使用以下程序创建对象：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击 ，然后点击**RA VPN 对象 (ASA & FTD) (RA VPN Objects [ASA & FTD]) > 身份源 (Identity Source)**。

步骤 3 为对象输入**对象名称 (Object name)**。

步骤 4 对于**设备类型**，请选择 **FTD**。

步骤 5 对于**身份源**类型，请选择 **RADIUS 服务器**。点击**继续 (Continue)**。

步骤 6 使用以下属性编辑身份源配置：

- **服务器名称或 IP 地址 (Server Name or IP Address)** - 服务器的完全限定主机名 (FQDN) 或 IP 地址。
- **身份验证端口 (Authentication Port)**（可选）- 在其上执行 RADIUS 身份验证和授权的端口。默认值为 1812。
- **超时 (Timeout)** - 系统将请求发送至下一服务器之前等待服务器响应的时长，此为 1-300 秒之间的数值。默认值为 10 秒。
- 输入**服务器密钥 (Server Secret Key)**（可选）- 用于加密 Firepower 威胁防御设备和 RADIUS 服务器之间数据的共享密钥。该密钥是一个区分大小写的字母数字字符串，最多64个字符，且不含空格。密钥必须以字母数字字符或下划线开头，它可以包含特殊字符：$ & - _ . + @。字符串必须匹配 RADIUS 服务器上配置的字符串。如果不配置密钥，则不加密连接。

步骤 7 如果您已经为网络配置了 Cisco Identity Services Engine (ISE)，并使用服务器进行远程访问 VPN 授权更改配置，您可以点击**仅限 RA VPN (RA VPN Only)** 链接并配置以下选项。

- **重定向 ACL (Redirect ACL)** - 选择要用于 RA VPN 重定向 ACL 的扩展访问控制列表 (ACL)。如果没有扩展 ACL，则必须从 FDM 管理 设备控制台中的 Smart CLI 模板创建所需的扩展 ACL 对象。请参阅适用于运行设备的版本的《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》中“高级配置”一章的**配置智能 CLI 对象**部分。重定向 ACL 的目的是向 ISE 发送初始流量，以便评估客户端安全状态。ACL 应向 ISE 发送 HTTPS 流量，而非已设定发往 ISE 的流量或被定向到域名解析 DNS 服务器的流量。请参阅适用于运行设备的版本的《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》中“虚拟专用网络 (VPN)”一章的**配置授权更改**部分。
- **诊断接口** - 启用此选项将允许系统始终使用“诊断”接口与服务器通信。如果禁用此选项，CDO 将默认使用路由表来确定要使用的接口。

步骤 8 点击**添加 (Add)**。

步骤 9 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

创建 RADIUS 服务器组

RADIUS 服务器组中包含一个或多个 RADIUS 服务器对象。组中的服务器必须是彼此的备份。这些服务器构成备份服务器链，因此，如果第一台服务器不可用，系统可以尝试列表中的下一个服务器。

使用以下程序创建对象组：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击，然后点击 FTD 身份源。 >

步骤 3 为对象输入**对象名称 (Object name)**。

步骤 4 选择设备类型作为 FTD。

步骤 5 选择 RADIUS 服务器组作为身份源类型。点击**继续 (Continue)**。

步骤 6 使用以下属性编辑身份源配置：

- **断路时间 (Dead Time)** - 只有当所有服务器均发生故障时，才会重新激活故障服务器。断路时间是指最后一台服务器发生故障后，在重新激活所有服务器之前所等待的时间。
- **最大失败尝试次数 (Maximum Failed Attempts)** - 尝试组中下一个服务器之前发送到 RADIUS 服务器的失败请求（即，未收到响应的请求）数。超过最大失败尝试次数时，系统会将服务器标记为故障。对于给定功能，如果您使用本地数据库配置回退方法，并且组中的所有服务器都无法响应，则会将该组视为无法响应，并将尝试回退方法。该服务器组会在断路时间内保持标记为无响应，以确保该时段内其他 AAA 请求不会尝试联系该服务器组，而是立即使用回退方法。
- **动态授权/端口 (Dynamic Authorization/Port)**（可选）- 如果为此 RADIUS 服务器组启用 RADIUS 动态授权或授权更改 (CoA) 服务，该组会注册 CoA 通知并侦听指定的端口，以便使 CoA 策略从 Cisco Identity Services Engine (ISE) 进行更新。仅当您在远程接入 VPN 中结合 ISE 使用此服务器组时，才能启用动态授权。

步骤 7 从下拉菜单中选择支持 RADIUS 服务器的 AD 领域。如果尚未创建 AD 领域，请从下拉菜单中点击创建。

步骤 8 点击添加按钮以添加现有的 RADIUS 服务器对象。  或者，您可以从此窗口创建新的 RADIUS 服务器对象。

Note 优先级添加这些对象，因为列表中的第一个服务器将被使用，直到它停止响应。然后，设备默认为列表中的下一个服务器。FDM 管理

步骤 9 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

编辑 Radius 服务器对象或组

使用以下程序编辑 Radius 服务器对象或 Radius 服务器组：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的对象。

步骤 3 选择要编辑的对象。

步骤 4 点击**操作 (Actions)** 窗格中的编辑图标  。

步骤 5 以在上述过程中创建值的相同方式编辑对话框中的值。要编辑或测试主机名/IP 地址或加密信息，请展开配置栏。

步骤 6 点击**保存 (Save)**。

步骤 7 CDO 显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

步骤 8 立即预览和部署所有设备的配置更改您所做的更改，或等待并一次部署多个更改。

创建新的 *RA VPN* 组策略

组策略是一组面向用户的远程接入 VPN 的属性/值对。连接配置文件使用组策略在建立隧道后设置用户连接的条款。通过组策略可将整组属性应用于用户或用户组，而不必为每个用户单独指定每个属性。

系统包含名为“DfltGrpPolicy”的默认组策略。您可以创建其他组策略，以提供您所需的服务。

Note 不能将不一致的组策略对象添加到 RA VPN 配置。在将组策略添加到 RA VPN 配置之前，请解决所有不一致问题。

Procedure

步骤 1 在左侧的 思科防御协调器 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击“加号”  按钮。

步骤 3 点击 **RA VPN 对象（ASA 和 FTD）(RA VPN Objects [ASA & FTD]) > RA VPN 组策略 (RA VPN Group Policy)**。

步骤 4 输入组策略的名称。此名称最多可包含 64 个字符，允许使用空格。

步骤 5 在**设备类型 (Device Type)** 下拉列表中，选择 **ASA**。

步骤 6 执行以下任一操作：

- 点击所需的选项卡并配置页面上的属性：
  - RA VPN 组策略属性
  - AnyConnect 客户端配置文件, on page 478
  - 会话设置属性, on page 479
  - 地址分配属性, on page 479
  - 分割隧道属性, on page 480
  - AnyConnect 属性, on page 481
  - 流量过滤器属性, on page 482
  - Windows 浏览器代理属性, on page 482

步骤 7 点击**保存 (Save)** 以保存组策略。

RA VPN 组策略属性

组策略的常规属性定义组名称和一些其他基本设置。“名称”属性是唯一必需的属性。

- **DNS 服务器 (DNS Server)**：选择定义连接到 VPN 时，DNS 服务器客户端应用于域名解析的 DNS 服务器组。如果所需的组尚不存在，请点击**创建 DNS 组**并立即创建组。
- **横幅**：登录时向用户显示的横幅文本或欢迎消息。默认无横幅。最多 496 字符。AnyConnect 客户端支持部分 HTML。为确保向远程用户正确地显示横幅，请使用
 标记表示换行。
- **默认域 (Default Domain)**：RA VPN 中用户的默认域名。例如 example.com。此域将被添加到非完全限定的主机名，例如 serverA 而不是 serverA.example.com。
- **AnyConnect 客户端配置文件 (AnyConnect Client Profiles)**：点击 + 并选择要用于该组的 AnyConnect 客户端配置文件。请参阅上传 RA AnyConnect 客户端配置文件。如果为外部接口（在连接配置文件中）配置的是完全限定域名，则系统将会为您创建默认配置文件。或者，您可上传您的客户端配置文件。使用独立的 AnyConnect 配置文件编辑器创建这些配置文件，您可以从 software.cisco.com 下载和安装该编辑器。如果不选择客户端配置文件，AnyConnect 客户端将为所有选项使用默认值。此列表中的项目是 AnyConnect 客户端配置文件对象，而不是配置文件本身。您可以通过点击下拉列表中的**创建新的 AnyConnect 客户端配置文件 (Create New AnyConnect Client Profile)**，创建（和上传）新配置文件。

AnyConnect 客户端配置文件

运行软件版本 6.7 或更高版本的 防火墙设备管理器 支持此功能。

Cisco AnyConnect VPN 客户端通过各种内置模块提供增强的安全性。这些模块提供网络安全，终端流量的网络可视性和网络外漫游保护等服务。每个客户端模块都包含一个客户端配置文件，其中包含根据您的要求的一组自定义配置。

当 VPN 用户下载 VPN AnyConnect 客户端软件时，您可以选择要下载到客户端的 AnyConnect VPN 配置文件对象和 AnyConnect 模块。

1. 选择或创建 AnyConnect VPN 配置文件对象。请参阅上传 RA AnyConnect 客户端配置文件, on page 493。除 DART 和“登录前启动”模块外，必须选择 AnyConnect VPN 配置文件对象。
2. 点击**添加Any 链接客户端模块 (Add Any Connect Client Module)**。

   以下 AnyConnect 模块是可选的，您可以将这些模块配置为在 VPN AnyConnect 客户端软件时下载：

   - **AMP 启用程序 (AMP Enabler)** - 为终端部署高级恶意软件防护 (AMP) 。
   - **DART** - 捕获系统日志和其他诊断信息的快照并在桌面上创建 .zip 文件，因此您可以便利地将故障排除信息发送到思科 TAC。
   - **反馈 (Feedback)** - 提供有关客户已启用和使用的功能和模块的信息。
   - **ISE 终端安全评估 (ISE Posture)** - 使用 OPSWAT v3 库执行终端安全评估检查，评估终端的合规性。
   - **网络访问管理器 (Network Access Manager)** - 为有线和无线网络访问提供 802.1X（第 2 层）和设备身份验证。

- **网络可视性 (Network Visibility)** - 可提升企业管理员执行容量和服务规划、审计、合规性和安全分析的能力。
- **登录前启动 (Start Before Login)** - 通过在 Windows 登录对话框出现之前启动 AnyConnect，强制用户在登录到 Windows 之前通过 VPN 连接而连接到企业基础设施。
- **Umbrella 漫游安全 (Umbrella Roaming Security)** - 在没有处于活动状态的 VPN 时提供 DNS 层安全。
- **网络安全 (Web Security)** - 根据定义的安全策略分析网页的元素，允许可接受的内容，并阻止恶意或不可接受的内容。

3. 在**客户端模块 (Client Module)** 列表中选择 **AnyConnect 模块 (AnyConnect module)**。
4. 在**配置文件 (Profile)** 列表中，选择或创建包含 AnyConnect 客户端配置文件的配置文件对象。
5. 选择**启用模块下载 (Enable Module Download)** 以下载客户端模块以及配置文件。如果未选择，则终端只能下载客户端配置文件。

会话设置属性

组政策会话设置控制用户可以连接到 VPN 的时长和可以创建的独立连接的数量。

- **最长连接时间 (Maximum Connection Time)**：在不注销和重新连接的情况下，用户可持续连接到 VPN 的最大时间长度（以分钟为单位），范围为 1 到 4473924 或留空。默认值为无限（留空），但空闲超时仍适用。
- **连接时间警报间隔 (Connection Time Alert Interval)**：如果您指定了最大连接时间，则警报间隔定义，在达到最长时间之前，向用户显示即将自动断开连接警告的时间。用户可以选择结束连接并重新连接，以重新启动计时器。默认值为 1 分钟。可以指定 1 到 30 分钟。
- **空闲时间 (Idle Time)**：VPN 连接在自动关闭之前可以闲置的时间长度（以分钟为单位），范围为 1 到 35791394。如果在此时间段内此连接上无通信活动，则系统会终止连接。默认值为 30 分钟。
- **空闲时间警报间隔 (Idle Time Alert Interval)**：在达到空闲时间之前，向用户显示因闲置会话而即将自动断开连接的警报的时间。任何活动都会重置计时器。默认值为 1 分钟。可以指定 1 到 30 分钟。
- **每个用户的同时登录数 (Simultaneous Login Per User)**：允许用户执行的最多同时登录数。默认值为 3。可以指定 1 到 2147483647 个连接。允许许多同时连接可能会危害安全性并影响性能。

地址分配属性

组策略的地址分配属性定义组的 IP 地址池。此处定义的地址池将覆盖使用此组的任何连接配置文件中定义的池。如果您希望使用连接配置文件中定义的池，请将这些设置留空。

- **IPv4 地址池 (IPv4 Address Pool)**、**IPv6 地址池 (IPv6 Address Pool)**：这些选项定义远程终端的地址池。根据客户端用于建立 VPN 连接的 IP 版本，从这些池为客户端分配地址。选择一个网络对象，定义要支持的每个 IP 类型的子网。如果您不想支持该 IP 版本，则可以空着列表。例

如，可以将 IPv4 池定义为 10.100.10.0/24。地址池不能与外部接口的 IP 地址位于同一子网。可以指定包含最多六个地址池的列表，用于本地地址分配。地址池的指定顺序非常重要。系统按照地址池出现的顺序分配这些地址池中的地址。

- **DHCP 范围 (DHCP Scope)**：如果在连接配置文件中为地址池配置了 DHCP 服务器，DHCP 作用域会标识要用于此组的地址池的子网。DHCP 服务器的地址还必须来自此作用域标识的同一个池。作用域允许您选择DHCP服务器中定义的部分地址池，用于此特定组。如未定义网络范围，则 DHCP 服务器将按地址池配置顺序分配 IP 地址。它将检查各个池，直到发现未分配的地址为止。要指定作用域，请选择包含网络号主机地址的网络对象。如果对象尚不存在，请点击**创建新网络**。例如，要告诉DHCP服务器使用192.168.5.0/24子网池中的地址，请选择指定192.168.5.0为主机地址的网络对象。DHCP 仅可用于 IPv4 寻址。

分割隧道属性

组策略的分割隧道属性定义系统如何处理用于内部网络的流量和流向外部的流量。分割隧道引导一些网络流量通过 VPN 隧道（加密），将剩下的网络流量引导至 VPN 隧道外部（未加密或以明文形式）。

- **IPv4 分割隧道 (IPv4 Split Tunneling)**、**IPv6 分割隧道 (IPv6 Split Tunneling)**：可以根据流量是使用 IPv4 寻址还是 IPv6 寻址来指定不同的选项，但每个流量的选项都相同。如果想要启用分割隧道，指定其中一个要求您选择网络对象的选项。
  - **允许所有流量通过隧道 (Allow all traffic over tunnel)**：不分割隧道。一旦用户建立 RA VPN 连接，用户的所有流量都会通过受保护隧道。这是默认值。这也被视为最安全的选项。
  - **允许指定流量通过隧道 (Allow specified traffic over the tunnel)**：选择定义目标网络和主机地址的网络对象。前往这些目标的所有流量都会通过受保护隧道。客户端会将前往其他目标的流量路由至隧道外部（例如，本地 Wi-Fi 或网络连接）。
  - **排除以下指定网络 (Exclude networks specified below)**：选择定义目标网络或主机地址的网络对象。客户端将前往这些目标的所有流量路由至隧道外部的连接。前往其他目标的流量都会通过隧道。
- **分割 DNS (Split DNS)** - 您可以配置系统通过安全连接发送某些 DNS 请求，同时允许客户端将其他 DNS 请求发送到客户端上配置的 DNS 服务器。您可以配置以下 DNS 行为：
  - **根据分割隧道策略发送 DNS 请求 (Send DNS Request as per split tunnel policy)**：使用此选项时，系统将按照与定义分割隧道选项相同的方式处理DNS请求。如果启用分割隧道，则会根据目标地址发送 DNS 请求。如果未启用分割隧道，所有 DNS 请求都会通过受保护的连接。
  - **始终通过隧道发送 DNS 请求 (Always send DNS requests over tunnel)**：如果启用了分割隧道，但想要通过受保护连接将所有 DNS 请求发送到为该组定义的 DNS 服务器上，则可选择此选项。
  - **仅通过隧道发送指定的域 (Send only specified domains over tunnel)**：如果想要让受保护的 DNS 服务器仅解析特定域的地址，则可选择此选项。然后，指定这些域，用逗号分隔域名。例如，example.com, example1.com。如果想要让内部 DNS 服务器解析内部域的名称，同时让外部 DNS 服务器处理所有其他互联网流量，请使用此选项。

AnyConnect 属性

组策略的 AnyConnect 属性定义 AnyConnect 客户端用于远程接入 VPN 连接的某些 SSL 和连接设置。

- **SSL 设置**
  - **启用数据报传输层安全 (DTLS) (Enable Datagram Transport Layer Security [DTLS])**：是否允许 AnyConnect 客户端使用两个同步隧道：SSL 隧道和 DTLS 隧道。使用 DTLS 可避免某些 SSL 连接带来的延迟和带宽问题，并可改进对数据包延迟敏感的实时应用的性能。如果不启用 DTLS，AnyConnect 客户端用户在建立 SSL VPN 连接时仅与 SSL 隧道连接。
  - **DTLS 压缩 (DTLS Compression)**：是否使用 LZS 为此组压缩数据报传输层安全 (DTLS) 连接。默认情况下会禁用 DTLS 压缩。
  - **SSL 压缩 (SSL Compression)**：是否启用数据压缩，如启用，则设置要使用的数据压缩方法：**Deflate** 或 **LZS**。默认情况下会**禁用** SSL 压缩。数据压缩加快了传输速率，但也增加了每个用户会话的内存需求和 CPU 使用率。因此，SSL 压缩会降低设备的整体吞吐量。
  - **SSL 重新生成密钥方法 (SSL Rekey Method)**、**SSL 重新生成密钥间隔 (SSL Rekey Interval)**：客户端能够为 VPN 连接重新生成密钥，重新协商加密密钥和初始化向量，从而提高连接的安全性。选择**无**可禁用重新生成密钥。要启用重新生成密钥，请选择**新隧道**来创建新的隧道。（ **现有隧道 (Existing Tunnel)** 选项导致的操作与 **新隧道 (New Tunnel)** 的相同。）如果启用重新生成密钥，还需设置重新生成密钥间隔，默认间隔为 4 分钟。可以将间隔设置为 4 到 10080 分钟（1 周）。
- **连接设置**
  - **忽略 DF（不分片）位 (Ignore the DF [Don't Fragment] bit)**：是否忽略需要分片的数据包内的“不分片” (DF) 位。选择此选项会允许强制将已设置 DF 位的数据包分片，从而使这些数据包能够通过隧道。
  - **客户端绕行协议 (Client Bypass Protocol)** - 允许您配置安全网关管理 IPv4 流量（安全网关仅允许 IPv6 流量时）或管理 IPv6 流量（安全网关仅允许 IPv4 流量时）的方式。

    当 AnyConnect 客户端建立与头端的 VPN 连接时，头端可以为客户端分配 IPv4 和/或 IPv6 地址。如果头端对 AnyConnect 连接仅分配一个 IPv4 地址或一个 IPv6 地址，则您可以配置 Client Bypass Protocol 以丢弃头端尚未分配 IP 地址（默认、已禁用、未检查）的网络流量，或允许该流量绕过头端并从客户端以未加密或“明文形式”发送（已启用、已检查）。

    例如，假设安全网关只将一个 IPv4 地址分配给 AnyConnect 连接，且终端为双协议栈。当终端尝试访问 IPv6 地址时，如果禁用客户端旁路协议，则会丢弃 IPv6 流量；但是，如果启用客户端旁路协议，则会从客户端以明文形式发送 IPv6 流量。
  - **MTU**：思科 AnyConnect VPN 客户端为 SSL VPN 连接建立的最大传输单位 (MTU) 大小。默认值为 1406 字节。范围为 576 至 1462 字节。
    - **AnyConnect 和 VPN 网关之间的保持连接消息**：是否在对等体之间交换保持连接消息，以证明它们可用于在隧道中发送和接收数据。保持连接消息以设置的时间间隔传输。默认间隔为 20 秒，有效范围为 15 到 600 秒。

- **网关端 DPD 间隔、客户端 DPD 间隔**：启用失效对等体检测 (DPD)，确保 VPN 网关或 VPN 客户端快速检测对等体不再响应的时间。您可以单独启用网关或客户端 DPD。发送 DPD 消息的默认间隔为 30 秒。时间间隔可以是 5 到 3600 秒。

流量过滤器属性

组策略的流量过滤器属性定义您想要对分配到该组的用户设置的限制。您可以使用这些属性（而非创建策略规则）根据主机或子网地址和协议或 VLAN 来限制 RA VPN 用户仅可访问特定资源。默认情况下，RA VPN 用户不会受到组策略的限制，可以访问受保护网络上的任何目标。

- **访问列表过滤器 (Access List Filter)**：使用扩展的访问控制列表 (ACL) 限制访问权限。选择 Smart CLI 扩展 ACL 对象。扩展 ACL 允许您基于源地址、目的地址和协议（例如 IP 或 TCP）进行过滤。ACL 评估遵循自上而下、“先匹配的规则先应用”原则，因此，请确保特定规则放在一般规则之前。ACL 末尾不包含隐式“deny any”语句，因此如果您想要拒绝对几个子网的访问，同时允许其他访问，请确保在 ACL 末尾加上“permit any”规则。由于您无法在编辑扩展的 ACL Smart CLI 对象时创建网络对象，因此您应在编辑组策略之前创建 ACL。否则，您可能需要先创建对象，然后再返回来创建网络对象，最后创建您需要的所有访问控制条目。要创建 ACL，登录 防火墙设备管理器，请转至**设备 (Device)** > **高级配置 (Advanced Configuration)** > **智能 CLI (Smart CLI)** > **对象 (Objects)**，创建对象，并选择**扩展访问列表 (Extended Access List)** 作为对象类型。
- **限制 VPN 到 VLAN (Restrict VPN to VLAN)**：也称为“VLAN 映射”，此属性指定该组策略应用到的会话的出口 VLAN 接口。系统将该组中的所有流量都转发到所选 VLAN。使用此属性向组策略分配 VLAN 以简化访问控制。向此属性赋值是在会话中使用 ACL 过滤流量的替代方法。确保您指定了在设备子接口上定义的 VLAN 编号。值的范围为 1 到 4094。

Windows 浏览器代理属性

组策略的 Windows 浏览器代理属性确定用户浏览器上定义的代理是否运行以及如何运行。

可以为 **VPN 会话期间浏览器代理**选择以下值之一：

- **终端设置无变化 (No change in endpoint settings)**：允许用户配置（或不配置）浏览器代理或 HTTP，并在已配置的情况下使用代理。
- **禁用浏览器代理 (Disable browser proxy)**：不使用为浏览器定义的代理（如有）。浏览器连接不会通过该代理。
- **自动检测设置 (Auto detect settings)**：在客户端设备的浏览器中启用自动代理服务器检测。
- **使用自定义设置 (Use custom settings)**：定义所有客户端设备应对 HTTP 流量使用的代理。配置以下设置：
  - **代理服务器 IP 或主机名 (Proxy Server IP or Hostname)**、**端口 (Port)**：代理服务器的 IP 地址或主机名，以及代理服务器用于代理连接的端口。主机和端口总共不能超过 100 个字符。
  - **浏览器例外列表 (Browser Proxy Exemption List)**：与例外列表中的主机/端口的连接不通过代理。添加不应使用代理的所有目标的主机/端口值。例如，www.example.com 端口 80。点

击**添加代理例外 (Add proxy exemption)** 以将项目添加到列表。点击垃圾桶图标可删除项目。整个代理例外列表（包括所有地址和端口）不能超过 255 个字符。

创建 *RA VPN* 配置

CDO 允许您将一个或多个设备添加到 RA VPN 配置向导，并配置与设备关联的 VPN 接口、访问控制和 NAT 豁免设置。FDM 管理因此，每个 RA VPN 配置都可以在与 RA VPN 配置关联的多个设备之间共享连接配置文件和组策略。FDM管理此外，您可以通过创建连接配置文件和组策略来增强配置。

您可以载入已配置 RA VPN 设置的设备，也可以载入没有 RA VPN 设置的新设备。FDM 管理当您载入已具有 RA VPN 设置的设备时，CDO 会自动创建“默认 RA VPN 配置”并将设备与此配置相关联。FDM 管理FDM 管理此外，此默认配置可以包含设备上定义的所有连接配置文件对象。

Important

- 不允许在同一远程接入 VPN 配置中添加 ASA 和设备。FDM 管理
- 一台设备不能有多个 RA VPN 配置。FDM 管理

前提条件

在将设备添加到 RA VPN 配置之前，必须满足以下前提条件：FDM 管理

- 确保设备具备以下条件：FDM 管理
  - 有效的思科安全客户端许可证。有关详细信息，请参阅远程访问 VPN 的许可要求。
  - 对于 FDM 版本 6.4.0，请确保至少已将一个 AnyConnect 软件包预上传到设备。有关详细信息，请参阅将 AnyConnect 软件包上传到 Firepower 威胁防御设备版本 6.4.0。在运行版本 6.4.0 的 FDM 管理 设备上升级 AnyConnect 软件包, on page 491
  - 对于 FDM 版本 6.5.0 及更高版本，您可以使用 CDO 上传 AnyConnect 软件包。有关详细信息，请参阅将 AnyConnect 软件包上传到 Firepower 威胁防御设备版本 6.5.0。将 AnyConnect 软件包上传到运行 FDM 管理 6.5 或更高版本的设备, on page 466
  - 没有待处理的配置部署。
- FDM 更改同步到 CDO。
  1. 在左侧的 CDO 导航栏中，点击资产并搜索要同步的一个或多个设备。FDM 管理
  2. 选择一个或多个设备，然后点击检查更改。CDO 与一个或多个设备通信以同步更改。FDM 管理
- RA VPN 配置组策略对象一致。
  - 确保解决所有不一致的组策略对象，因为它们无法添加到 RA VPN 配置中。解决问题或从“对象”(Objects) 页面删除不一致的组策略对象。有关详细信息，请参阅解决重复对象问

题和解决不一致对象问题。解决重复对象问题, on page 719解决不一致的对象问题, on page 721

- 设备的 RA VPN 组策略与 RA VPN 配置组策略匹配。FDM 管理

操作步骤

Procedure

步骤 1 在左侧的 思科防御协调器 导航栏中，点击**VPN** > **远程访问 VPN 配置 (Remote Access VPN Configuration)**。

步骤 2 点击蓝色加号  按钮以创建 RA VPN 配置。

步骤 3 输入远程访问 VPN 配置的名称。

步骤 4 点击蓝色加号  按钮将 FDM 管理 设备添加到配置。您可以添加设备详细信息并配置与设备关联的网络流量相关权限。

a. 提供以下设备详细信息：

- **设备**：选择要添加的FDM 管理设备，然后点击**选择**。

  Important 不允许在同一远程接入 VPN 配置中添加 ASA 和 FDM 管理 设备。

- **设备身份证书 (Certificate of Device Identity)** ：选择用于建立设备身份的内部证书。在 AnyConnect 客户端与设备进行连接时确定客户端的设备身份。客户端必须接受此证书才能完成安全的 VPN 连接。如果您还没有证书，请点击下拉列表中的**创建新内部证书 (Create New Internal Certificate)**。请参阅生成自签名的内部证书和内部 CA 证书。

- **外部接口 (Outside Interface)**：用户在进行远程访问 VPN 连接时连接的接口。请选择您使用此连接配置文件支持的设备与最终用户之间的任何接口，虽然这通常是外部（面向互联网的）接口。要创建新的子接口，请参阅配置 Firepower VLAN 子接口和 802.1Q 中继。

- **外部接口的完全限定域名或 IP (Fully Qualified Domain Name or IP for the Outside Interface)**：接口的名称（例如 ravpn.example.com）或必须提供的 IP 地址。如果指定名称，系统可以为您创建一个客户端配置文件。**注意**：您要确保 VPN 中和客户端使用的 DNS 服务器可以将此名称解析为外部接口的 IP 地址。将 FQDN 添加到相关 DNS 服务器。

b. 点击**继续**以配置流量权限。

- **为已解密的流量绕过访问控制策略 (sysopt permit-vpn)**：默认情况下，已解密流量要经过访问控制策略的检查。启用此选项可绕过解密流量选项，绕过访问控制策略检查，但从 AAA 服务器下载的 VPN 筛选 ACL 和授权 ACL 仍会应用于 VPN 流量。请注意，如果选择此选项，系统会配置 sysopt connection permit-vpn 命令，此为全局设置。这也会影响站点间 VPN 连接的行为。如果不选择此选项，外部用户可能会骗取远程访问 VPN 地址池中的 IP 地址，从而获取访问您网络的权限。这种情况可能会发生，因为您创建的访问控制规则需要允许地址池访问内部资源。如果您使用访问控制规则，请考虑使用用户说明来控制访问，而不是只

使用源 IP 地址。选择此选项的弊端在于，VPN 流量将不会被检测，也就是说不会对流量应用入侵和文件保护、URL 过滤或其他高级功能。同时，系统不会生成有关此流量的任何连接事件，且统计控制面板不会反映 VPN 连接。

- **NAT 豁免 (NAT Exempt)**：启用 NAT 豁免，使进出远程访问 VPN 终端的流量免于执行 NAT 转换。如果不豁免 VPN 流量执行 NAT，请确保外部和内部接口的现有 NAT 规则不适用于 RA VPN 地址池。NAT 豁免规则是给定源/目标接口和网络组合的手动静态身份 NAT 规则，但它们不会反映在 NAT 策略中，它们是隐藏起来的。如果启用 NAT 豁免，还必须进行以下配置。
  - **内部接口**：选择远程用户将要访问的内部网络的接口。所创建的 NAT 规则用于这些接口。
  - **内部网络**：选择代表远程用户将访问的内部网络的网络对象。网络列表必须包含与您支持的地址池相同的 IP 类型。

步骤 5 点击**确定 (OK)**。

- 如果您已载入 防火墙设备管理器 版本 6.4.0 设备，则**检测到的 AnyConnect 软件包**会显示设备中可用的 AnyConnect 软件包。
- 如果您已载入 防火墙设备管理器 版本 6.5.0 或更高版本的设备，则必须从预上传 AnyConnect 软件包的服务器添加 AnyConnect 软件包。有关说明，请参阅将 AnyConnect 软件包上传到运行 FDM 管理 6.5 或更高版本的设备。

步骤 6 点击**确定 (OK)**。设备已添加到配置中。

What to do next

Note 选择配置，然后在**操作**下点击相应的操作：

- **Group Policies**，用于添加或删除组策略。
  - 点击 + 选择所需的组策略。要创建新的 RA VPN 组策略，请参阅创建新的 RA VPN 组策略。
- **删除 (Remove)** 以删除所选的 RA VPN 配置。

修改 RA VPN 配置

您可以修改现有 RA VPN 配置的名称和设备详细信息。

Procedure

选择要修改的配置，然后在操作下点击编辑。

- 如果需要，请修改名称。
- 点击蓝色加号按钮  以添加新设备。
- 点击以在设备上执行以下操作。 FDM 管理
  - 点击编辑以修改现有的 RA VPN 配置。
  - 点击删除以从 RA VPN 配置中删除设备。FDM 管理除组策略外，与该设备关联的所有连接配置文件和 RA VPN 设置都将被删除。您可以从对象页面中明确删除组策略。注意：如果该设备是唯一使用该配置的设备，则无法删除该设备。FDM 管理或者，您可以删除 RA VPN 配置。

您还可以通过键入配置或设备的名称来搜索远程接入 VPN 配置。

相关信息：

- 配置 RA VPN 连接配置文件。
- 预览和部署所有设备的配置更改。
- 允许流量通过远程访问 VPN。

配置 *RA VPN* 连接配置文件

RA VPN 连接配置文件定义了一些特征，这些特征允许外部用户使用 AnyConnect 客户端与系统创建 VPN 连接。每个配置文件都定义了用于用户身份验证的 AAA 服务器和证书、分配用户 IP 地址的地址池，以及定义各种面向用户的属性的组策略。

如果需要为不同的用户组提供不同的服务，或者有不同的身份验证源，您可以在 RA VPN 配置中创建多个配置文件。例如，如果您的组织与使用不同身份验证服务器的组织合并，您可以为使用这些身份验证服务器的新组创建配置文件。

远程访问 VPN 连接配置文件让您的用户可在外部网络（例如其家庭网络）上时连接到您的内部网络。创建单独的配置文件，以适应不同的身份验证方法。

准备工作

在配置远程访问 (RA) VPN 连接之前：

- 外部接口（作为远程访问 VPN 连接终端的那个外部接口）也不能具有允许 HTTPS 连接的管理访问列表。在配置 RA VPN 之前，从外部接口删除所有 HTTPS 规则。请参阅《适用于 Firepower

设备管理器版本 X.Y 的思科 Firepower 威胁防御配置指南》的“系统设置”一章中的“配置管理访问列表”部分。

- 创建 RA VPN 配置。请参阅创建 RA VPN 配置。创建 RA VPN 配置, on page 483

操作步骤

Procedure

步骤 1 在 CDO 导航窗格中，点击**VPN > 远程访问 VPN 配置 (Remote Access VPN Configuration)**。您可以点击 VPN 配置以查看当前已配置多少连接配置文件和组策略的摘要信息。

步骤 2 点击连接配置文件，然后在右侧边栏中的**操作**下点击**添加连接配置文件**。

步骤 3 配置基本连接属性。

- **连接配置文件名称 (Connection Profile Name)**：此连接的名称，最多 50 个字符，不能含空格。例如，MainOffice。

  Note 您在此输入的名称将是用户在 AnyConnect 客户端的连接列表中看到的名称。选择一个对您的用户来说有意义的名称。

- **组别名、组 URL (Group Alias, Group URL)**：别名包含特定连接配置文件的备用名称或 URL。在连接到 FDM 管理设备时，VPN 用户可以在连接列表中的 AnyConnect 客户端中选择别名。连接配置文件名称会自动添加为组别名。您还可以配置组 URL 列表，在发起远程访问 VPN 连接时您的终端可以从该列表中进行选择。如果用户使用组 URL 进行连接，系统将自动使用与 URL 匹配的连接配置文件。此 URL 供尚未安装 AnyConnect 客户端的客户使用。按需要添加组别名和 URL。在设备上定义的所有连接配置文件中，这些别名和 URL 必须是唯一的。组 URL 必须以 **https://** 开头。
- 例如，您可能有别名承包商和组 URLhttps://ravpn.example.com/contractor。安装 AnyConnect 客户端后，用户只需在连接的 AnyConnect VPN 下拉列表中选择组别名。

步骤 4 配置主身份源和辅助身份源（可选）。这些选项确定设备如何对远程用户进行身份验证，以启用远程访问 VPN 连接。最简单的方法是仅使用 AAA，然后选择 AD 领域或使用 LocalIdentitySource。根据**身份验证类型**，您可以使用以下方法：

- **仅 AAA (AAA Only)**：根据用户名和密码对用户进行身份验证和授权。有关详细信息，请参阅为连接配置文件配置 AAA。
- **仅客户端证书 (Client Certificate Only)**：根据客户端设备身份证书进行用户身份验证。有关详细信息，请参阅为连接配置文件配置证书身份验证。
- **AAA 和 ClientCertificate (AAA and ClientCertificate)**：同时使用用户名/密码和客户端设备身份证书。

步骤 5 配置客户端的地址池。地址池定义了远程客户端在建立 VPN 连接时，系统可以分配给它们的 IP 地址。有关详细信息，请参阅配置客户端地址池分配。

步骤 6 点击**继续 (Continue)**。

步骤 7 从列表中选择要用于此配置文件的**组策略**，然后点击**选择 (Select)**。组策略在建立隧道后设置用户连接的条款。系统包含名为 DfltGrpPolicy 的默认组策略。您可以创建其他组策略，以提供您所需的服务。

Note 如果所需的组策略尚不存在，请在**对象**页面上创建组策略，然后将该策略与 RA VPN 配置相关联。有关组策略的详细信息，请参阅创建新的 RA VPN 组策略。

步骤 8 点击**继续 (Continue)**。

步骤 9 审核摘要。首先，验证摘要是否正确。您可以查看最终用户初步安装 AnyConnect 软件需要做什么，并测试他们是否可以完成 VPN 连接。点击  将这些说明复制到剪贴板，然后分发给您的用户。

步骤 10 点击**完成 (Done)**。

What to do next

确保 VPN 隧道中允许流量，如允许流量通过远程访问 VPN 中所述。

为连接配置文件配置 AAA

身份验证、授权和记账 (AAA) 服务器使用用户名和密码来确认是否允许用户访问远程访问 VPN。如果使用 RADIUS 服务器，则可以区分已验证用户的授权级别，从而提供对受保护资源的差异化访问权限。还可以使用 RADIUS 记账服务来跟踪使用情况。

在配置 AAA 时，您必须配置主身份源。辅助源和备用源是可选的。如果想要实施双重身份验证，请使用辅助源，例如，RSA 令牌或 DUO。

主身份源选项

- **用户身份验证的主身份源 (Primary Identity Source for User Authentication)**：用于对远程用户进行身份验证的主要身份源。必须在此源或可选的回退源中定义最终用户，才能完成 VPN 连接。选择以下一个选项：
  - Active Directory (AD) 身份领域。如果所需的领域尚不存在，请点击**创建新身份领域**。
  - RADIUS 服务器组。
  - LocalIdentitySource（本地用户数据库）：您可以直接在设备上定义用户，而不使用外部服务器。
- **回退本地身份源 (Fallback Local Identity Source)**：如果主要源是一个外部服务器，您可以选择 LocalIdentitySource 作为回退源，以防主服务器不可用。如果使用本地数据库作为回退源，请确保您定义的本地用户名/密码与外部服务器中的定义的用户名/密码相同。
- **删除选项 (Strip options)**：领域是管理域。启用以下选项将允许仅基于用户名进行身份验证。您可以启用这些选项的任意组合。但是，如果服务器无法分析分隔符，则必须选中这两个复选框。

- **从用户名删除身份源服务器 (Strip Identity Source Server from Username)**：在将用户名传递到AAA服务器之前，是否要从用户名删除身份源名称。例如，如果选择此选项且用户输入域\用户名作为用户名，则该域将从用户名中删除，并发送到AAA服务器进行身份验证。默认情况下，此选项处于取消选中状态。
- **从用户名删除组 (Strip Group from Username)**：在将用户名传递到 AAA 服务器之前，是否要从用户名删除组名称。此选项适用于 username@domain 格式中给定的名称；此选项会剥离域和 @ 符号。默认情况下，此选项处于取消选中状态。

辅助身份源

- **用于用户授权的辅助身份源 (Secondary Identity Source for User Authorization)**：可选的第二个身份源。如果用户成功使用主要源进行身份验证，则系统会提示其使用辅助源进行身份验证。可以选择 AD 领域、RADIUS 服务器组或本地身份源。
- **高级 (Advanced) 选项**：点击**高级 (Advanced)** 链接并配置以下选项：
  - **辅助源的备用本地身份源 (Fallback Local Identity Source for Secondary)**：如果辅助源为外部服务器，您可以选择LocalIdentitySource作为备用源，以防辅助服务器不可用。如果使用本地数据库作为备用源，请确保您定义的本地用户名/密码与辅助外部服务器中定义的用户名/密码相同。
  - **使用主要用户名进行辅助登录 (Use Primary Username for Secondary Login)**：默认情况下，使用辅助身份源时，系统将提示输入辅助源的用户名和密码。如果选择此选项，系统将仅提示您输入辅助密码，并使用与主身份源相同的用户名来进行辅助源身份验证。如果您在主身份源和辅助身份源中配置了相同的用户名，请选择此选项。
    - **会话服务器用户名 (Username for Session Server)**：身份验证成功后，用户名将显示在事件和统计控制面板中，用于确定基于用户或组的 SSL 解密和访问控制规则之间的匹配关系，并用于记账。由于使用了两个身份验证源，因此您需要告诉系统是使用主用户名还是辅助用户名作为用户身份。默认情况下，使用主用户名。
    - **密码类型 (Password Type)**：如何获取辅助服务器的密码。默认值为**提示**，这表明系统将提示用户输入密码。选择**主身份源密码**，自动使用用户在主服务器中进行身份验证时输入的密码。选择**公用密码**，为每个用户使用相同的密码，然后在**公用密码**字段中输入该密码。
  - **授权服务器 (Authorization Server)**：已配置为授权远程访问 VPN 用户的 RADIUS 服务器组。身份验证完成后，授权将控制对每个经过身份验证的用户都可用的服务和命令。授权通过组合一组描述用户被授权执行的操作、其实际功能和限制的属性来工作。如果您不使用授权，则单独的身份验证将为所有经过身份验证的用户提供相同的访问权限。有关配置 RADIUS 进行授权的信息，请参阅使用 RADIUS 和组策略控制用户权限和属性。使用 RADIUS 和组策略控制用户权限和属性, on page 448请注意，如果系统从 RADIUS 服务器获取的授权属性与组策略中定义的属性重叠，则 RADIUS 属性将覆盖组策略属性。
  - **记账服务器 (Accounting Server)**：（可选。）用于为远程访问 VPN 会话记账的 RADIUS 服务器组。记账会跟踪用户正在访问的服务以及他们正在使用的网络资源数量。FTD 设备向 RADIUS 服务器报告用户活动。记账信息包括每个会话的开始和停止时间、用户名、会话

时通过设备的字节数、使用的服务以及每个会话的持续时间。然后，您可分析该数据，以进行网络管理、客户端计费或审核。您可以单独使用记账功能，也可以将其与身份验证和授权功能配合使用。

为连接配置文件配置证书身份验证

Note 此部分不适用于仅作为 AAA 的身份验证类型。

可以使用客户端设备安装的证书对远程接入 VPN 连接进行身份验证。

使用客户端证书时，仍可以配置辅助身份源、备用源，以及授权和记账服务器。这些是AAA选项；有关详细信息，请参阅配置 RA VPN 连接配置文件。配置 RA VPN 连接配置文件, on page 486

以下是证书特定的属性。您可以为主身份源和辅助身份源单独配置这些属性。配置辅助源为可选操作。

- **从证书中获取的用户名 (Username from Certificate)**：选择以下选项之一：
  - **映射特定字段 (Map Specific Field)**：按照**主要字段 (Primary Field)** 和**辅助字段 (Secondary Field)** 的顺序使用证书元素。默认值为 CN（公用名）和 OU（组织单位）。选择适用于您的组织的选项。这些字段组合在一起用于提供用户名，此名称用于事件和控制面板中，并出于匹配的目的，在 SSL 解密和访问控制规则中使用。
  - **使用完整 DN（可分辨名称）作为用户名 (Use entire DN [distinguished name] as username)**：系统自动从 DN 字段派生出用户名。•
- 高级选项（不适用于作为仅客户端证书的身份验证类型）：点击高级链接并配置以下选项：
  - **在用户登录窗口预填证书中的用户名 (Prefill username from certificate on user login window)**：在提示用户进行身份验证时，是否在用户名字段填写检索到的用户名。
  - **在登录窗口隐藏用户名 (Hide username in login window)**：如果选择**预填充 (Prefill)** 选项，则可以隐藏用户名，这意味着用户无法编辑密码提示中的用户名。

配置客户端地址池分配

系统必须可以通过某种方法向连接到远程访问 VPN 的终端提供 IP 地址。AAA 服务器、DHCP 服务器、组策略中配置的 IP 地址池，或连接配置文件中配置的 IP 地址池可以提供这些地址。系统会按照以上顺序尝试使用这些资源，并在获取一个可用地址后停止尝试，然后将此地址分配给客户端。因此，您可以配置多个选项，以便在并发连接数异常多的情况下，可保障系统能获取地址。

使用下列一个或多个方法配置连接配置文件的地址池。

- IPv4 地址池和 IPv4 地址池：首先，创建最多六个指定子网的网络对象。可以为 IPv4 和 IPv6 单独配置池。然后，在组策略或者连接配置文件的 **IPv4 地址池 (IPv4 Address Pool)** 和 **IPv6 地址池 (IPv6 Address Pool)** 选项中，选择这些对象。无需同时配置 IPv4 和 IPv6，配置您想要支持的寻址方案即可。也不需要同时在组策略和连接配置文件中配置池。组策略会覆盖连接配置文件

的设置，因此如果您在组策略中配置了池，则请将连接配置文件中的选项留空。请注意，系统按照您列出的顺序使用地址池。

- **DHCP 服务器 (DHCP Servers)**：首先，使用一个或多个 IPv4 地址范围为 RA VPN 配置 DHCP 服务器（您无法使用 DHCP 配置 IPv6 池）。然后，使用 DHCP 服务器的 IP 地址创建主机网络对象。随后，便可以在连接配置文件的 **DHCP 服务器 (DHCP Servers)** 属性中选择此对象。可以配置多个 DHCP 服务器。如果 DHCP 服务器有多个地址池，则可以在与连接配置文件关联的组策略中使用 **DHCP 作用域 (DHCP Scope)** 属性，选择要使用的池。使用池的网络地址创建主机网络对象。例如，如果 DHCP 池包含 192.168.15.0/24 和 192.168.16.0/24，将 DHCP 范围设置为 192.168.16.0 可确保从 192.168.16.0/24 子网中选择地址。

允许流量通过远程访问 *VPN*

可以使用以下方法之一来启用远程访问 VPN 隧道中的流量。

- 配置 **sysopt connection permit-vpn** 命令，此命令会使匹配 VPN 连接的流量免受访问控制策略的限制。此命令的默认值是 **no sysopt connection permit-vpn**，这意味着 VPN 流量的通过还必须获得访问控制策略的允许。外部用户无法在远程访问 VPN 地址池中伪造 IP 地址，因此这种允许 VPN 流量的方法较为安全。但它的缺点是，VPN 流量得不到检测，也就是说不会对流量应用入侵和文件保护、URL 过滤或其他高级功能。同时，系统不会生成有关此流量的任何连接事件，且统计控制面板不会反映 VPN 连接。要配置此命令，请在 RA VPN 配置中选择**为已解密的流量绕过访问控制策略 (Bypass Access Control policy for decrypted traffic)** 选项。请参阅创建 RA VPN 配置。创建 RA VPN 配置, on page 483
- 创建访问控制规则以允许来自远程访问 VPN 地址池的连接。此方法可确保对 VPN 流量进行检测，并将高级服务应用于连接。但它的缺点是，有可能造成外部用户伪造 IP 地址，进而获得访问　内部网络的权限。请参阅配置 FDM 访问控制策略。

在运行版本 *6.4.0* 的 *FDM* 管理 设备上升级 *AnyConnect* 软件包

您可以使用 思科防御协调器 升级 FDM 管理 设备上可用的 AnyConnect 软件包，以便将其分发给 RA VPN 用户。

以下是升级 AnyConnect 软件包所涉及的主要步骤：

Procedure

步骤 1 使用 防火墙设备管理器 来删除 AnyConnect 软件包并上传该软件包的更高版本。使用其中一种方法来完成此任务。

- 删除旧软件包并从 防火墙设备管理器 UI 上传新软件包。
- 删除旧软件包并从 防火墙设备管理器 API 资源管理器上传新软件包。

步骤 2 将 防火墙设备管理器 更改部署到设备。

步骤 3 将新配置信息读入 CDO。

步骤 4 验证 RA VPN 连接配置文件中的新软件包。

前提条件

- 至少一个具有连接配置文件的 RA VPN 配置已部署到设备。FDM 管理
- 从 https://software.cisco.com/download/home/283000185 下载您想要的 AnyConnect 软件包。思科建议升级到最新的可用软件包。

使用 防火墙设备管理器 将所需的 AnyConnect 软件包上传到 Secure Firewall Threat Defense

Procedure

步骤 1 使用浏览器打开系统主页。例如，https://ftd.example.com。https://ftd.example.com/

步骤 2 登录至 防火墙设备管理器。

步骤 3 在**设备 (Device)** > **远程访问 VPN (Remote Access VPN)** 中点击**查看配置 (View Configuration)**。该组显示有关当前已配置多少连接配置文件和组策略的摘要信息。

步骤 4 点击查看按钮 ( ) 按钮（**查看 (View)** 配置按钮），打开连接配置文件和连接说明的摘要。

Note 您可以编辑任何一个连接配置文件，以将 AnyConnect 软件包上传到 FDM 管理 设备。

步骤 5 点击**编辑 (Edit)** 按钮以进行更改。

步骤 6 点击下一步，直到显示全局设置屏幕。**AnyConnect 软件包**会显示FDM管理 设备上可用的AnyConnect 软件包。

步骤 7 点击“X”按钮删除要替换的 AnyConnect 软件包。

步骤 8 点击上传软件包，然后点击要上传兼容软件包的操作系统。

步骤 9 选择软件包，然后点击**打开 (Open)**。您可以在 防火墙设备管理器 UI 上看到正在上传的软件包。

步骤 10 点击**完成**。配置已保存。

Note 或者，您可以使用 防火墙设备管理器 API 资源管理器删除并上传新的 AnyConnect 软件包。

a. 编辑 URL，使其指向 /#/api-explorer，例如 https://ftd.example.com/#/api-explorer。

b. 从 FDM 管理 设备中删除软件包，点击 **AnyConnectPackageFile** > **删除 (Delete)**。在 objID 字段中，键入软件包 ID，然后点击试用！

c. 通过执行将 AnyConnect 软件包上传到 Firepower 威胁防御设备部分中所述的步骤上传新软件包。将 AnyConnect 软件包上传到运行版本 6.4.0 的 FDM 管理设备, on page 463

步骤 11 点击网页右上角的**部署更改 (Deploy Changes)** 图标。若有未部署的更改，系统会用圆点高亮显示。

步骤 12 如果您对所做的更改比较满意，可以点击**立即部署 (Deploy Now)** 立即启动作业。窗口将显示部署正在进行。您可以关闭窗口，或等待部署完成。

验证 RA VPN 连接配置文件中是否引用了新软件包

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **FTD** 选项卡，然后选择具有升级的 AnyConnect 软件包的 FTD 设备。此设备将报告冲突。

步骤 4 接受带外更改，以便用设备的**运行配置覆盖 CDO 上存储的配置**和任何待定更改。有关详细信息，请参阅解决“检测到冲突”状态。

步骤 5 通过执行以下操作查看新的 AnyConnect 软件包：

- 点击**VPN** > **远程访问 VPN (Remote Access VPN)**。
- 点击与此 FTD 设备关联的 RA VPN 配置。
- 点击**操作**下的**编辑**。新软件包显示在**设备**下。

上传 *RA AnyConnect* 客户端配置文件

远程接入 VPN AnyConnect 客户端配置文件是存储在文件中的一组配置参数。这些不同的 AnyConnect 客户端配置文件包含核心客户端 VPN 功能和可选客户端模块网络访问管理器、AMP 启动器、ISE 终端安全评估、网络可视性、客户体验反馈、Umbrella 漫游安全和网络安全的配置设置。

CDO 允许将这些配置文件作为对象上传，以便稍后在组策略中使用。

- **AnyConnect VPN 配置文件 (AnyConnect VPN Profile)** - AnyConnect 客户端配置文件随 AnyConnect 客户端软件一起下载到客户端。这些配置文件定义与客户端相关的诸多选项，例如启动时自动连接和自动重新连接，以及最终用户是否可以更改 AnyConnect 客户端首选项和高级设置中的选项。CDO 支持 XML 文件格式。
- **AMP 启用程序服务配置文件 (AMP Enabler Service Profile)** - 该配置文件用于 AnyConnect AMP 启用程序。当远程访问 VPN 用户连接到 VPN 时，AMP 启动器和此配置文件会从 FDM 管理 设备推送到终端。CDO 支持 XML 和 ASP 文件格式。

- **反馈配置文件 (Feedback Profile)** - 您可以添加客户体验反馈配置文件并选择此类型，以接收有关客户已启用和使用的功能和模块的信息。CDO 支持 FSP 文件格式。
- **ISE 终端安全评估配置文件 (ISE Posture Profile)** - 如果要为 AnyConnect ISE 终端安全评估模块添加配置文件，请选择此选项。CDO 支持 XML 和 ISP 文件格式。
- **网络访问管理器服务配置文件 (Network Access Manager Service Profile)** - 使用网络访问管理器配置文件编辑器配置和添加 NAM 配置文件。CDO 支持 XML 和 NSP 文件格式。
- **网络可视性服务配置文件 (Network Access Manager Service Profile)** - AnyConnect 网络可视性模块的配置文件。您可以使用 NVM 配置文件编辑器创建配置文件。CDO 支持 XML 和 NVMSP 文件格式。
- **Umbrella 漫游安全配置文件 (Umbrella Roaming Security Profile)** - 如果部署 Umbrella 漫游安全模块，则必须选择此文件类型。CDO 支持 XML 和 JSON 文件格式。
- **网络安全服务配置文件 (Web Security Service Profile)** - 在为网络安全模块添加配置文件时选择此文件类型。CDO 支持 XML、WSO 和 WSP 文件格式。

Before you begin

使用适当的基于 GUI AnyConnect 配置文件编辑器创建所需的配置文件。您可以从思科软件下载中心的 AnyConnect 安全移动客户端类别下载配置文件编辑器，并安装 AnyConnect“配置文件编辑器 - Windows/独立安装程序 (MSI)”(Profile Editor - Windows / Standalone installer [MSI])。配置文件编辑器安装程序包含独立版本的配置文件编辑器。此安装文件仅适用于 Windows，文件名为 anyconnect-profileeditor-win-<version>-k9.msi，其中 <version> 指 AnyConnect 版本。例如，anyconnect-profileeditor-win-4.3.04027-k9.msi。您还必须在安装配置文件编辑器之前安装 Java JRE 1.6（或更高版本）。

除 Umbrella 漫游安全配置文件编辑器外，此软件包包含创建模块所需的所有配置文件编辑器。有关详细信息，请参阅相应版本的《思科 AnyConnect 安全移动客户端管理员指南》中的 *AnyConnect* 配置文件编辑器一章。从 Umbrella 控制面板单独下载 Umbrella 漫游安全配置文件。有关详细信息，请参阅《思科 Umbrella 用户指南》中“Umbrella 漫游安全”一章的“从 Umbrella 控制面板下载 AnyConnect 漫游安全配置文件”部分。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击“加号”  按钮。

步骤 3 点击 **RA VPN 对象（ASA 和 FDM）(RA VPN Objects [ASA & FDM]) > AnyConnect 客户端配置文件 (AnyConnect Client Profile)**。

步骤 4 在**对象名称 (Object Name)** 字段中输入 AnyConnect 客户端配置文件名称。

步骤 5 点击**浏览 (Browse)** 并选择使用配置文件编辑器创建的文件。

步骤 6 点击**打开**上传配置文件。

步骤 7 点击**添加 (Add)** 以添加对象。

相关信息：

- 将客户端模块与 RA VPN 组策略窗口中的 AnyConnect VPN 配置文件关联。请参阅 创建新的 RA VPN 组策略。

Note 所有 ASA 版本和运行软件版本 6.7 或更高版本的 FDM 都支持客户端模块关联。

FDM 管理 设备的远程访问 VPN 准则和限制

配置 RA VPN 时，请时刻注意以下准则和限制。

- 必须使用 防火墙设备管理器 将 AnyConnect 软件包预加载到运行版本 6.4.0 的 FDM 管理设备。

Note 使用 思科防御协调器 中的远程接入 VPN 配置向导将 AnyConnect 软件包单独上传到运行版本 6.5.0 的 FDM 管理 设备。

- 从 CDO 配置 RA VPN 之前：
  - 从 防火墙设备管理器 为 FDM 管理 设备注册许可证。
  - 通过导出控制从 防火墙设备管理器 启用许可证。
- CDO 不支持扩展访问列表对象。在 防火墙设备管理器 中使用 Smart CLI 配置对象，然后在 VPN 过滤器和授权更改 (CoA) 重定向 ACL 中使用。
- 您从设备创建的模板将不包含 RA VPN 配置。FDM 管理
- IP 池对象和 RADIUS 身份源需要设备特定的覆盖。
- 对于同一个 TCP 端口，无法在同一接口上同时配置 防火墙设备管理器 访问（管理访问列表中的 HTTPS 访问）和 AnyConnect 远程访问 SSL VPN。例如，如果在外部接口上配置远程访问 SSL VPN，则也无法在端口 443 上打开 HTTPS 连接的外部接口。因为无法在 防火墙设备管理器中配置这些功能所使用的端口，所以无法在同一接口上配置这两项功能。
- 如果您使用 RADIUS 和 RSA 令牌配置双因素身份验证，则在大多数情况下，12 秒的默认身份验证超时太短，无法实现成功的身份验证。通过创建自定义 AnyConnect 客户端配置文件并将其应用到 RA VPN 连接配置文件，来增加身份验证超时值，如上传 RA AnyConnect 客户端配置文件, on page 493中所述。建议身份验证超时时间最短为 60 秒，以便用户有足够的时间进行身份验证并粘贴 RSA 令牌，以及进行令牌往返验证。

用户如何在 FDM 管理设备上安装 AnyConnect 客户端软件

使用 防火墙设备管理器 API 将 AnyConnect 客户端软件包上传到 FDM 管理 设备以分发给用户。请参阅将 AnyConnect 软件包上传到 Firepower 威胁防御设备。将 AnyConnect 软件包上传到运行版本 6.4.0 的 FDM 管理设备, on page 463

要完成 VPN 连接，您的用户必须安装 AnyConnect 客户端软件。可以使用现有的软件分发方法直接安装该软件。或者，可以让用户直接从 FDM 管理设备安装 AnyConnect 客户端。

Note 用户必须对其工作站具有管理员权限才能安装软件。

如果您决定让用户一开始从 FDM 管理 设备安装软件，请告知用户执行以下步骤。

Note Android 和 iOS 用户应从相应的应用商店下载 AnyConnect。

Procedure

步骤 1 使用 Web 浏览器，打开 **https://***ravpn-address*，其中 *ravpn-address* 是您允许 VPN 连接的外部接口的 IP 地址或主机名。您在配置远程访问 VPN 时确定此接口。系统提示用户登录。

步骤 2 登录到网站。用户使用为远程访问VPN配置的目录服务器进行身份验证。登录成功后可继续操作。如果登录成功，系统将确定用户是否已具有所需的AnyConnect客户端版本。如果用户的计算机上没有 AnyConnect 客户端，或者客户端的版本较低，系统将自动开始安装 AnyConnect 软件。安装后，AnyConnect 会完成远程接入 VPN 连接。

分发新的 *AnyConnect* 客户端软件版本

您可以将新版本的 AnyConnect 客户端软件上传到设备，而不删除旧版本。FDM 管理成功上传 AnyConnect 客户端后，您可以删除旧版本。

AnyConnect 客户端在用户建立的下一个 VPN 连接上检测新版本。系统将自动提示用户下载并安装更新的客户端软件。这种自动化可为您和您的客户端简化软件分发。

下图显示了具有适用于 Windows 操作系统的两个版本 AnyConnect 客户端软件（AnyConnectWindows_3.2_BGL 和 AnyConnectWindows_4.2_BGL）的设备示例。FDM 管理

上传 RA AnyConnect 客户端配置文件

远程接入VPN AnyConnect客户端配置文件是存储在文件中的一组配置参数。这些不同的AnyConnect客户端配置文件包含核心客户端VPN功能和可选客户端模块网络访问管理器、AMP启动器、ISE终端安全评估、网络可视性、客户体验反馈、Umbrella 漫游安全和网络安全的配置设置。

CDO 允许将这些配置文件作为对象上传，以便稍后在组策略中使用。

- **AnyConnect VPN 配置文件 (AnyConnect VPN Profile)** - AnyConnect客户端配置文件随 AnyConnect客户端软件一起下载到客户端。这些配置文件定义与客户端相关的诸多选项，例如启动时自动连接和自动重新连接，以及最终用户是否可以更改AnyConnect客户端首选项和高级设置中的选项。CDO 支持 XML 文件格式。
- **AMP 启用程序服务配置文件 (AMP Enabler Service Profile)** - 该配置文件用于 AnyConnect AMP 启用程序。当远程访问 VPN 用户连接到 VPN 时，AMP 启动器和此配置文件会从 FDM 管理 设备推送到终端。CDO 支持 XML 和 ASP 文件格式。
- **反馈配置文件 (Feedback Profile)** - 您可以添加客户体验反馈配置文件并选择此类型，以接收有关客户已启用和使用的功能和模块的信息。CDO 支持 FSP 文件格式。
- **ISE 终端安全评估配置文件 (ISE Posture Profile)** - 如果要为 AnyConnect ISE 终端安全评估模块添加配置文件，请选择此选项。CDO 支持 XML 和 ISP 文件格式。
- **网络访问管理器服务配置文件 (Network Access Manager Service Profile)** - 使用网络访问管理器配置文件编辑器配置和添加 NAM 配置文件。CDO 支持 XML 和 NSP 文件格式。
- **网络可视性服务配置文件 (Network Access Manager Service Profile)** - AnyConnect 网络可视性模块的配置文件。您可以使用 NVM 配置文件编辑器创建配置文件。CDO 支持 XML 和 NVMSP 文件格式。
- **Umbrella 漫游安全配置文件 (Umbrella Roaming Security Profile)** - 如果部署 Umbrella 漫游安全模块，则必须选择此文件类型。CDO 支持 XML 和 JSON 文件格式。
- **网络安全服务配置文件 (Web Security Service Profile)** - 在为网络安全模块添加配置文件时选择此文件类型。CDO 支持 XML、WSO 和 WSP 文件格式。

Before you begin

使用适当的基于GUI AnyConnect配置文件编辑器创建所需的配置文件。您可以从思科软件下载中心的 AnyConnect 安全移动客户端类别下载配置文件编辑器，并安装 AnyConnect“配置文件编辑器 - Windows/独立安装程序 (MSI)”(Profile Editor - Windows / Standalone installer [MSI])。配置文件编辑器安装程序包含独立版本的配置文件编辑器。此安装文件仅适用于 Windows，文件名为 anyconnect-profileeditor-win-<version>-k9.msi，其中 <version> 指 AnyConnect 版本。例如，anyconnect-profileeditor-win-4.3.04027-k9.msi。您还必须在安装配置文件编辑器之前安装 Java JRE 1.6（或更高版本）。

除 Umbrella 漫游安全配置文件编辑器外，此软件包包含创建模块所需的所有配置文件编辑器。有关详细信息，请参阅相应版本的《思科 AnyConnect 安全移动客户端管理员指南》中的 *AnyConnect* 配置文件编辑器一章。从 Umbrella 控制面板单独下载 Umbrella 漫游安全配置文件。有关详细信息，请参阅《思科 Umbrella 用户指南》中“Umbrella 漫游安全”一章的“从 Umbrella 控制面板下载 AnyConnect 漫游安全配置文件”部分。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击“加号”  按钮。

步骤 3 点击 **RA VPN 对象（ASA 和 FDM）(RA VPN Objects [ASA & FDM])** > **AnyConnect 客户端配置文件 (AnyConnect Client Profile)**。

步骤 4 在**对象名称 (Object Name)** 字段中输入 AnyConnect 客户端配置文件名称。

步骤 5 点击**浏览 (Browse)** 并选择使用配置文件编辑器创建的文件。

步骤 6 点击**打开**上传配置文件。

步骤 7 点击**添加 (Add)** 以添加对象。

相关信息：

- 将客户端模块与 RA VPN 组策略窗口中的 AnyConnect VPN 配置文件关联。请参阅 创建新的 RA VPN 组策略。

Note 所有 ASA 版本和运行软件版本 6.7 或更高版本的 FDM 都支持客户端模块关联。

远程访问 VPN 的许可要求

从 防火墙设备管理器 为 FDM 管理 设备启用（注册）许可证，以配置 RA VPN 连接。注册设备时，必须使用启用了出口控制功能的智能软件管理器(SSM)账户。您也不能使用评估许可证配置该功能。

此外，您必须购买并启用许可证；它可以是以下任何一项：。即使这些许可证被设计为在与基于 ASA 软件的头端一起使用时允许不同的功能集，它们对于 FDM 管理 设备都同等处理。

有关从 防火墙设备管理器 启用许可证的详细信息，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》中“远程访问 VPN”一章中的**远程访问 VPN 的许可要求**部分。

有关详细信息，请参阅《思科 *AnyConnect* 订购指南》。
http://www.cisco.com/c/en/us/product...t-listing.html 上还提供了其他数据表。

要查看许可证状态，请执行以下操作：

Procedure

步骤 1 在左侧的 思科防御协调器 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)**。

步骤 3 点击 **FTD** 选项卡，然后选择所需的设备。

步骤 4 在右侧的**设备操作**窗格中，点击**管理许可证**。如果许可证有效，则**状态**显示为**已启用**。

各设备型号的最大并发 VPN 会话数量

根据设备型号，设备上允许的并发远程接入VPN会话数量有最大值限制。此限制用于确保系统性能不会降低到不可接受的水平。请使用这些限制进行容量规划。

设备型号	最大并发远程接入 VPN 会话数
Firepower 2110	1,500
Firepower 2120	3,500
Firepower 2130	7500
Firepower 2140	10,000
Firepower 威胁防御虚拟	250

RADIUS 授权更改

RADIUS 更改授权 (CoA) 功能提供了一种机制，可在通过身份验证后更改身份验证、授权和记账 (AAA) 会话的属性。RA VPN 的一个主要挑战是保护　内部网络免遭受攻击终端感染，并在终端受病毒或恶意软件感染时，在终端上采取补救措施来保护终端。有必要在所有阶段（即，在 RA VPN 会话之前、过程中和之后）保护终端和内部网络。RADIUS CoA 功能有助于实现此目标。

如果使用思科身份服务引擎 (ISE) RADIUS 服务器，则可以配置授权更改策略实施。当 AAA 中的用户或用户组的策略发生更改时，ISE 会向 FTD 设备发送 CoA 消息，以重新初始化身份验证并应用新策略。不需要内联安全状态实施点 (IPEP) 来为与 FTD 设备建立的每个 VPN 会话应用访问控制列表 (ACL)。

相关信息：

- 在 FTD 设备上配置授权更改

在 *FTD* 设备上配置授权更改

大多数授权更改策略是在 ISE 服务器中配置的。但是，您必须将 FTD 设备配置为正确连接到 ISE。

准备工作

如果在任何对象中使用主机名，请确保配置用于数据接口的 DNS 服务器，如《适用于 Firepower 设备管理器的思科Firepower威胁防御配置指南》“系统设置”一章的“为数据和管理接口配置DNS”部分中所述。您的设备运行的版本。您通常需要配置 DNS 才能拥有功能齐全的系统。
https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html

操作步骤

Procedure

步骤 1 登录至您的 FDM 管理 设备的 防火墙设备管理器。

步骤 2 配置扩展的访问控制列表 (ACL)，用于将初始连接重定向到 ISE。重定向 ACL 的目的是向 ISE 发送初始流量，以便 ISE 可以评估客户端安全状态。ACL 应向 ISE 发送 HTTPS 流量，而非已设定发往 ISE 的流量或被定向到域名解析 DNS 服务器的流量。重定向 ACL 的示例如下所示：

access-list redirect extended deny ip any host<ISE server IP>

access-list redirect extended deny ip any host<DNS server IP>

access-list redirect extended deny icmp any any

access-list redirect extended permit tcp any any eq www

但是，请注意，ACL 包含隐式“deny any any”作为最后一个访问控制条目 (ACE)。在此示例中，与 TCP 端口 www（即端口 80）匹配的最后一个 ACE 将不会匹配与前 3 个 ACE 匹配的任何流量，因此这些 ACE 是冗余的。您只需使用最后一个 ACE 创建 ACL 即可获得相同的结果。请注意，在重定向 ACL 中，允许和拒绝操作只会确定哪些流量与 ACL 匹配，系统会允许匹配的流量并拒绝不匹配的流量。实际上，系统并不会丢弃任何流量，被拒绝的流量只是未重定向至 ISE。要创建重定向 ACL，您需要配置 Smart CLI 对象。

a. 选择**设备 (Device)** > **高级配置 (Advanced Configuration)** > **智能 CLI (Smart CLI)** > **对象 (Objects)**。

b. 点击 + 创建新对象。

c. 输入 ACL 的名称。例如，**重定向**。

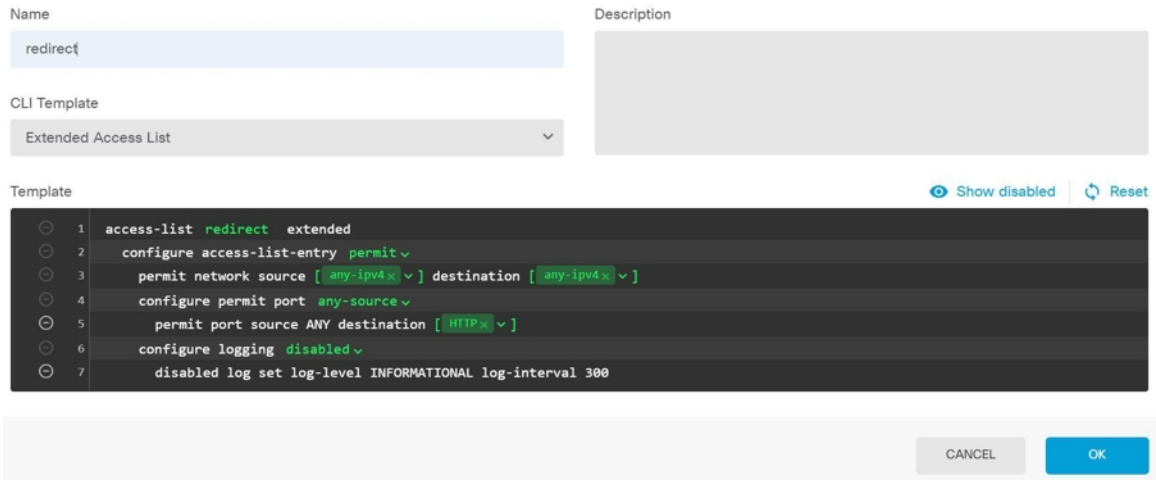
d. 对于 **CLI 模板**，选择**扩展访问列表**。

e. 在**模板**正文中进行以下配置：

- configure access-list-entry action = permit
- source-network = any-ipv4
- destination-network = any-ipv4
- configure permit port = any-source

- destination-port = HTTP
- configure logging = disabled

ACE 应如下所示：



f. 点击**确定 (OK)**。

在下次部署更改时会配置此 ACL。无需在任何其他策略中使用此对象来强制部署。

Note 此 ACL 仅适用于 IPv4。如果您还想要支持 IPv6，除了要为源和目标网络选择 any-ipv6 外，只需再添加一个拥有所有相同属性的 ACE 即可。您还可以添加其他 ACE，以确保前往 ISE 或 DNS 服务器的流量未被重定向。您首先需要创建主机网络对象，以保留这些服务器的 IP 地址。

步骤 3 配置用于动态授权的 RADIUS 服务器组。

按照“创建或编辑 Firepower 威胁防御 RADIUS 服务器对象或组”部分中提供的说明执行以下步骤。创建或编辑 RADIUS 服务器对象或组, on page 474

a. 创建 RADIUS 服务器对象

b. 创建 RADIUS 服务器组

步骤 4 创建使用此 RADIUS 服务器组的连接配置文件。请参阅配置 RA VPN 连接配置文件。使用 **AAA 身份验证**（单独使用或与证书结合使用），并在**用户身份验证主身份源**、**授权**和**记账**选项中选择服务器组。

验证 FDM 管理 设备的远程接入 VPN 配置

在配置远程访问 VPN 并将该配置部署到设备后，请确认是否可以进行远程连接。

Procedure

步骤 1 在外部网络中，使用 AnyConnect 客户端建立 VPN 连接。使用 Web 浏览器，打开 **https://***ravpn-address*，其中 *ravpn-address* 是您允许 VPN 连接的外部接口的 IP 地址或主机名。如有必要，安装客户端软件并完成连接。请参阅用户如何在 FDM 管理设备上安装 AnyConnect 客户端软件。如果配置了组 URL，也可尝试这些 URL。

步骤 2 在资产页面中，选择要验证的设备，然后点击设备操作下的命令行界面。

步骤 3 使用 **show vpn-sessiondb** 命令可查看有关当前 VPN 会话的摘要信息。

步骤 4 统计信息应显示您的活动 AnyConnect 客户端会话以及有关累积会话、峰值并发会话数量和非活动会话的信息。以下是该命令的输出示例。

```
> show vpn-sessiondb
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ------------------------------------------------
AnyConnect Client           :      1 :         49 :           3 :        0
  SSL/TLS/DTLS              :      1 :         49 :           3 :        0
Clientless VPN              :      0 :          1 :           1
  Browser                   :      0 :          1 :           1
--------------------------------------------------------------------------------


  Total Active and Inactive    :      1             Total Cumulative :     50
  Device Total VPN Capacity    :  10000
  Device Load                  :     0%
  --------------------------------------------------------------------------------

  --------------------------------------------------------------------------------
  Tunnels Summary
  --------------------------------------------------------------------------------
                               Active : Cumulative : Peak Concurrent
                              ------------------------------------------------
  Clientless                  :      0 :          1 :               1
  AnyConnect-Parent           :      1 :         49 :               3
  SSL-Tunnel                  :      1 :         46 :               3
  DTLS-Tunnel                 :      1 :         46 :               3
  --------------------------------------------------------------------------------
  Totals                      :      3 :        142
  --------------------------------------------------------------------------------

  --------------------------------------------------------------------------------
  IPv6 Usage Summary
  --------------------------------------------------------------------------------
                               Active : Cumulative : Peak Concurrent
                              ------------------------------------------------
  AnyConnect SSL/TLS/DTLS     :        :           :
    Tunneled IPv6             :      1 :         20 :           2
  --------------------------------------------------------------------------------
```

步骤 5 使用 **show vpn-sessiondb anyconnect** 命令可查看有关当前 AnyConnect VPN 会话的详细信息。详细信息包括使用的加密方式、传输和接收的字节数及其他统计信息。如果使用VPN连接，随着您重新发出命令，您应可看到传输/接收的字节数会变化。

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : User1                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone : 0
```

查看设备的远程接入 VPN 配置详细信息FDM 管理

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 VPN 远程访问 VPN 配置。 >

步骤 2 点击现有的 VPN 配置对象。

该组显示有关当前已配置多少连接配置文件和组策略的摘要信息。

- 展开 RA VPN 配置以查看与其关联的所有连接配置文件。
  - 点击添加 + 按钮可添加新的连接配置文件。
  - 点击查看按钮( )，打开连接配置文件和连接说明的摘要。在操作下，您可以点击编辑以修改更改。
- 您可以点击“操作”下的以下选项之一来执行其他任务：
  - 点击组策略以分配/添加组策略。
  - 点击不再需要的配置对象或连接配置文件，然后点击删除进行删除。

模板

模板提供了开发设备配置文件的首选和通用版本的方法：

- 模板是从现有的基本配置文件创建的。
- 它们支持值参数，以便轻松自定义预期值，包括 IP 地址和端口号。

- 它们可以通过参数替换导出，以便在多个设备之间使用。

相关信息

- FDM 管理 设备模板, on page 504
  - 配置 FDM 模板, on page 505
  - 将模板应用到 FDM 管理设备, on page 509

FDM 管理 设备模板

关于 FDM 管理 设备模板

思科防御协调器 允许您创建已载入 FDM 管理 设备配置的 FDM 管理 模板。创建模板时，请选择要包含在 FDM 管理 设备模板中的部分（对象、策略、设置、接口和 NAT）。然后，您可以修改该模板并使用它来配置您管理的其他 FDM 管理 设备。FDM 管理 设备模板是促进 FDM 管理 设备之间策略一致性的一种方法。

创建 FDM 管理 设备模板时，您可以选择创建完整或自定义模板：

- 完整的模板包括 FDM FDM 管理 设备配置的所有部分，并将所有内容应用于其他 FDM 管理 设备。
- 自定义模板仅包含您选择的 FDM 管理 设备配置的一个或多个部分，并且仅在其他 FDM 管理 设备上应用该部分及其关联的实体。

Important FDM 管理 模板不包括证书、Radius、AD 和 RA VPN 对象。

如何使用 FDM 管理 设备模板

以下是使用 FDM 管理 设备模板的一些方法：

- 通过应用另一台 FDM 管理 设备的配置模板来配置一台 FDM 管理 设备。您应用的模板可能代表了您要在所有 FDM 管理 设备上使用的“最佳实践”配置。
- 将模板用作一种进行设备配置更改的方法，并在实验环境中模拟这些更改，以便在将这些更改应用于实时 FDM 管理 设备之前测试其功能。
- 在创建模板时，对接口和子接口的属性进行参数化。您可以在应用模板时更改接口和子接口的参数化值。

您将在更改日志中看到的内容

在将模板应用于设备时，该设备的整个配置都会被覆盖。CDO 更改日志会记录由此产生的每个更改。因此，将模板应用于设备后，更改日志条目会变得非常长。

相关信息：

配置 FDM 模板

前提条件

在创建 FDM 管理 模板之前，请将您将创建模板的 FDM 管理 载入 思科防御协调器。您只能从已载入的 FDM 管理 设备创建 FDM 管理 设备模板。

我们强烈建议使用模板来配置正被添加到环境中的全新 FDM 管理 设备。

Note 从 FDM 管理 设备创建模板时，RA VPN 对象不会被包含在模板中。

创建 FDM 模板

在创建模板时，如果您选择所有部分，则模板将包括该设备配置的各个方面；管理IP地址、接口配置、策略信息等。

如果选择某些部分，自定义模板将包括以下实体。

模板部件	自定义模板中包含的部分
访问规则	包括访问控制规则和这些规则的任何相关实体。例如，对象和接口（带子接口）。
NAT 规则	包括 NAT 规则以及这些 NAT 规则所需的任何相关实体。例如，对象和接口（带子接口）。
设置	包括系统设置以及这些设置所需的任何相关实体。例如，对象和接口（带子接口）。
接口	包括接口和子接口。
对象	包括对象和这些对象所需的任何相关实体。例如，接口和子接口。

使用此程序创建 FDM 管理 设备模板：

Procedure

步骤 1 在 思科防御协调器 导航栏中，点击 **清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击 **FTD** 选项卡，然后从列表中选择所需的设备。

步骤 4 使用过滤器和搜索字段查找要为其创建模板的 FDM 管理 设备。

步骤 5 在右侧的**设备操作 (Device Actions)** 窗格中，点击**创建模板 (Create Template)**。**名称模板**会提供设备上每个部分的计数。它还会显示子接口（如有）的计数。

步骤 6 选择您要在模板中包含的部分。

步骤 7 输入模板的名称。

步骤 8 点击**创建模板 (Create Template)**。

步骤 9 在**参数化模板 (Parameterize Template)** 区域中，您可以执行以下操作：

- 要参数化接口，请将鼠标悬停在与该接口对应的单元格上（直到您看到花括号）并点击。
- 要参数化子接口，请展开具有子接口的接口，将鼠标悬停在与该子接口对应的单元格上（直到看到花括号）并点击。

您可以参数化以下属性，以便启用每台设备的自定义。

- **逻辑名称**
- **状态**
- **IP 地址/网络掩码**

Note 这些属性仅支持每个参数一个值。

步骤 10 点击**继续 (Continue)**。

步骤 11 查看模板和任何参数化。点击**完成 (Done)** 以创建模板。

清单 (Inventory) 页面现在会显示您刚刚创建的 FDM 管理 设备模板。

Note 创建模板后，在**清单 (Inventory)** 窗格中，CDO 会显示相应的模板部件图标，以显示该模板中包含的部件。当您点击设备或将鼠标指针悬停在图标上时，此信息也会显示在**设备详细信息 (Device Details)** 窗格中。

下图显示了一个部件图标示例，用于显示包括“访问规则”、“NAT 规则”和“对象”在内的模板。

编辑 FDM 管理设备模板

使用以下程序来编辑模板参数：

Procedure

步骤 1 在 思科防御协调器 导航栏中，点击 **清单 (Inventory)**。

步骤 2 点击**模板 (Templates)** 选项卡。

步骤 3 点击 **FTD** 选项卡。

步骤 4 使用模型/模板过滤器查找要修改的模板。

步骤 5 在右侧的**设备操作 (Device Actions)** 窗格中，点击**编辑参数 (Edit Parameters)**。

步骤 6 （可选）通过直接编辑文本框对参数进行任何更改。

步骤 7 点击**保存 (Save)**。

您可以像编辑实时 FDM 管理设备一样编辑 FDM 管理设备模板的其余部分。您可以使用以下配置来编辑 FDM 管理设备模板：

- FDM 管理 设备设置
- 虚拟专用网络管理
- 创建 RA VPN 配置
- FDM 策略配置
- 促进策略和配置的一致性

删除 FDM 模板

您可以像从 思科防御协调器 中删除 FDM 管理 设备一样删除 FDM 管理 设备模板：

Procedure

步骤 1 在 CDO 导航栏中，点击 **清单 (Inventory)**。

步骤 2 点击**模板 (Templates)** 选项卡。

步骤 3 点击 **FTD** 选项卡。

步骤 4 使用过滤器和搜索字段查找要删除的 FDM 管理 设备模板。

步骤 5 在**设备操作 (Device Actions)** 窗格中，点击**删除 (Remove)** 。

步骤 6 阅读警告消息，然后点击**确定 (OK)** 以删除模板。

相关信息：

- FDM 管理 设备模板
- 应用 FDM 模板

应用 FDM 模板

在应用模板之前，您可以通过导航至**清单 (Inventory)** 页面并过滤**模型/模板 (Model/Template)**来识别其内容。思科防御协调器 会显示相应的模板部件图标，以显示该模板中包含的部件。当您点击设备或将鼠标指针悬停在图标上时，此信息也会显示在**设备详细信息 (Device Details)** 窗格中。

您可以通过参数化以下属性来启用每台设备的自定义，这意味着您可以在应用模板时应用设备特定的值：

应用 FDM 管理 设备模板时，可以更改创建模板时配置的接口和子接口的参数化值。

应用整个模板

应用完整的 FDM 管理 设备模板以创建的新 FDM 管理 设备会完全覆盖 FDM 管理 设备上的任何现有配置，包括尚未从 CDO 部署到设备的任何暂存更改。设备上未包含在模板中的任何内容都将丢失。

应用自定义模板

将自定义 FDM 管理 模板应用于其他 FDM 管理 设备将根据模板部分保留或删除现有配置。下表提供在其他 FDM 管理 设备上应用自定义模板后发生的更改。

模板部件	应用自定义模板后
访问规则	• 自定义模板中的新访问控制规则会覆盖设备上的任何现有访问控制规则。 • 自定义模板中的新对象和接口（带有子接口）（如有）将应用于设备，而不会删除任何现有对象和接口。
NAT 规则	• 自定义模板中的新 NAT 规则会覆盖设备上的任何现有 NAT 规则。 • 自定义模板中的新对象和接口（带有子接口）（如有）将应用于设备，而不会删除任何现有对象和接口。
设置	• 自定义模板中的新系统设置将应用于设备，而不会删除任何现有系统设置。 • 自定义模板中的新对象和接口（带有子接口）（如有）将应用于设备，而不会删除任何现有对象和接口。
接口	• 自定义模板中的新接口和子接口将应用于设备，而不会删除任何现有接口和子接口。 • CDO 不允许将模板应用于模板中定义的接口数量超过设备上接口数量的设备。
对象	• 自定义模板中的新对象将应用于设备，而不会删除任何现有对象。 • 自定义模板中的新接口和子接口（如有）将应用于设备，而会不删除任何现有接口和子接口。

前提条件

在应用模板之前，必须满足以下条件：

- 使用模板时，请确保您对模板所做的任何更改都已提交，并且模板在**清单 (Inventory)** 页面上处于“已同步”(Synced) 状态。

- 在使用 FDM 管理 设备作为模板时，请确保已部署您打算部署到设备的 CDO 上的任何更改，并且没有尚未部署的防火墙设备管理器 控制台更改。设备必须在**清单 (Inventory)** 页面上显示“已同步”(Synced) 状态。

将模板应用于设备的过程分为三步。

1. 应用整个模板
2. 查看设备和网络设置
3. 将更改部署到设备

将模板应用到 FDM 管理设备

Important 在将更改部署到设备之前，请继续执行下一程序：

查看设备和网络设置

在应用模板之前，您可以使用更改请求跟踪将跟踪标签应用于更改。更改请求管理, on page 577使用以下程序应用 FDM 管理设备模板：

Procedure

步骤 1 （可选）开始之前，请先创建设备模板，然后再向其应用其他模板。FDM 管理这为您提供了一个配置备份，您可以在需要重新应用设备和网络设置时进行参考。

步骤 2 在 CDO 导航栏中，点击 **清单 (Inventory)**。

步骤 3 点击**模板 (Templates)** 选项卡。

步骤 4 点击 **FTD** 选项卡。

步骤 5 使用过滤器和搜索字段查找要应用模板的设备或模板。FDM 管理

Note 如果此时更改模板的名称，则会对 DeviceName 应用完整的设备配置或模板。将此更改部署到 DeviceName 将覆盖该设备上运行的整个配置。

步骤 6 在右侧的设备**操作 (Actions)** 窗格中，点击**应用模板 (Apply Template)**。

步骤 7 点击选择模板并选择所需的模板，然后点击继续。

步骤 8 您可以配置以下内容，然后点击每个屏幕上显示的继续。

a. 映射接口：确认或更改模板和设备之间的接口映射。 请注意，不能将多个模板接口映射到单个设备接口；如果接口配置不受支持，则无法继续并应用模板。

Note CDO 不允许将模板应用于模板中定义的接口数量超过设备上接口数量的设备。

b. 填充参数：自定义要应用模板的设备的接口或子接口参数值。

c. 查看：查看模板配置，并在准备好使用模板中的配置覆盖现有设备配置时点击应用模板。

步骤 9 点击预览和部署所有设备的配置更改 以查看并部署您所做的更改，或等待并一次部署多个更改。

查看设备和网络设置

创建 FDM 管理 模板时，思科防御协调器 会将整个设备配置复制到模板中。因此，模板中包含原始设备的管理 IP 地址等内容。在将模板应用于设备之前，请查看以下设备和网络设置：

Procedure

步骤 1 查看这些 FDM 管理 设备设置，以确保它们反映新 FDM 管理 设备的正确信息：

- FDM 管理 设备设置
- 管理接口
- 主机名

步骤 2 查看 配置 FDM 访问控制策略 ，确保规则在适当的情况下引用新 FDM 管理 设备的 IP 地址。

步骤 3 查看 inside_zone 和 outside_zone 安全对象，确保它们引用新 FDM 管理 设备的正确 IP 地址。

步骤 4 查看 NAT 策略，确保它们引用新 FDM 管理 设备的正确 IP 地址。

步骤 5 查看接口配置，确保它们反映新 FDM 管理 设备的正确配置。

将更改部署到设备

立即 预览和部署所有设备的配置更改 您所做的更改，或等待并一次部署多个更改。

相关信息：

- FDM 管理 设备模板
- 配置 FDM 模板

将 ASA 配置迁移到 FDM 管理 设备模板

Attention Firepower 设备管理器 (FDM) 支持和功能仅应要求提供。如果您的租户上尚未启用 防火墙设备管理器 支持，则无法管理或部署到 FDM 管理 设备。向支持团队发送请求以启用此平台。通过 TAC 打开提交支持请求, on page 752

思科防御协调器 可帮助您将 ASA 迁移到 FDM 管理 设备。CDO 提供了一个向导来帮助您将 ASA 的运行配置的这些元素迁移到 FDM 管理 模板：

- 访问控制规则 (ACL)

- 接口
- 网络地址转换 (NAT) 规则
- 网络对象和网络组对象
- 路由
- 服务对象和服务组对象
- 站点间 VPN

将 ASA 运行配置的这些元素迁移到 FDM 管理 模板后，即可将 FDM 模板应用于由 CDO 管理的新 FDM 管理 设备。FDM 管理 设备采用模板中定义的配置，因此，FDM 管理 设备现在配置了 ASA 运行配置的某些方面。

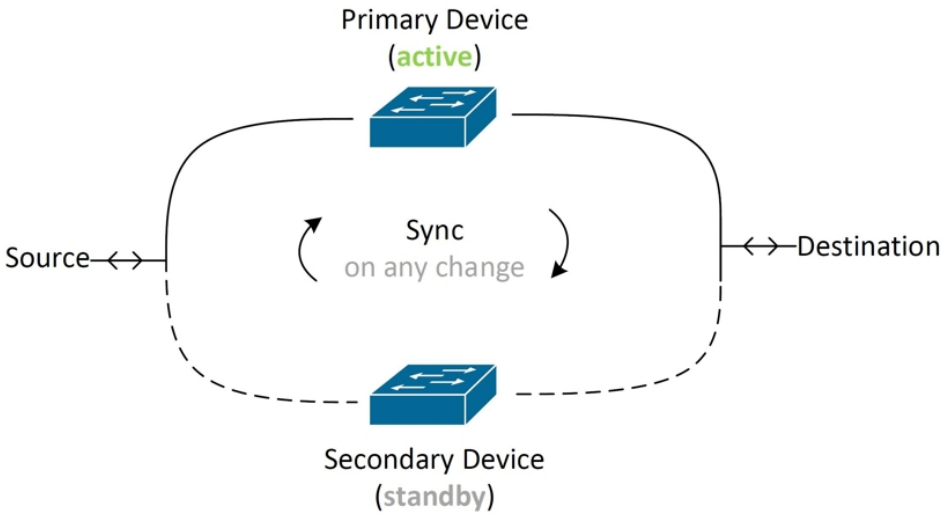
使用此过程不会迁移 ASA 运行配置的其他元素。这些其他元素在 FDM 管理 设备模板中由空值表示。将模板应用于 FDM 管理 设备时，我们会应用迁移到新 FDM 管理 设备的值并忽略空值。无论新 FDM 管理 设备具有哪些其他默认值，它都会保留。我们未迁移的 ASA 运行配置的其他元素将需要在迁移过程之外在 FDM 管理 设备上重新创建。

有关使用 CDO 将 ASA 迁移到 FDM 管理 设备的过程的完整说明，请参阅使用思科防御协调器将 ASA 迁移到 FDM 托管设备。

FDM 管理 高可用性

关于高可用性

高可用性 (HA) 或故障转移配置可将两台设备连接成主/辅助设置，这样，如果主设备发生故障，辅助设备就会自动接管其任务。配置高可用性（也称为故障切换）需要通过专用故障切换链路和状态链路（可选）相互连接的两台相同的FDM管理。系统会对主用设备的运行状况（硬件、接口、软件以及环境状态）进行监控，以便确定是否符合特定的故障切换条件。如果符合这些条件，将执行故障切换。这有助于在设备发生故障的情况下或在设备升级的维护期间让网络保持运行。有关详细信息，请参阅以下相关文章。



这两台设备构成一对主用/备用设备，其中，主设备是主用设备并传递流量。辅助（备用）设备不会主动传递流量，但会使配置和其他状态信息与主用设备同步。这两台设备通过故障转移链路进行通信，以便确定每台设备的运行状态。

Note 当您选择接受 HA 对更改或在部署到 FDM 管理 HA 对时，您将与 HA 对的主用设备通信。这意味着仅从主用设备提取配置和备份。

证书和高可用性对

将证书应用于 FDM 管理 HA 对时，CDO 只会将证书应用于主用设备；只有在部署主用设备时，配置和证书才会与备用设备同步。如果通过 FDM 管理 将新证书应用于主用设备，则主用设备和备用设备可能具有两个不同的证书。这可能会导致故障转移或故障转移历史记录出现问题，以及其他可能的问题。两台设备必须具有相同的证书才能成功运行。如果必须通过 FDM 管理 更改证书，则必须在 HA 对中部署更改并同步证书。

相关信息：

- 用于 FDM 管理 高可用性的故障转移和状态链路
- FDM 管理 高可用性对要求
- 创建 FDM 管理 高可用性对
- “高可用性”(High Availability) 页面中的 FDM 管理设备
- 中断 FDM 管理 高可用性对
- FDM 管理 高可用性故障转移历史记录
- 刷新 FDM 管理 高可用性状态

- 在高可用性对上强制执行故障切换 在高可用性对上强制执行故障切换FDM 管理
- 升级 FDM 管理 高可用性对
- 读取、丢弃、检查和部署更改
- 将配置更改从 FDM 管理 设备读取到 CDO
- 将配置更改从 CDO 部署到 FDM 管理 设备

FDM 管理 高可用性对要求

高可用性要求

在创建高可用性 (HA) 对之前，必须满足几个要求。

高可用性的物理和虚拟设备要求

必须满足以下硬软要求：

- 设备的硬件型号必须相同。
- 设备安装的模块必须相同。例如，如果具有可选的网络接口模块，则必须在另一台设备中安装相同的网络模块。
- 设备接口的数量和类型必须相同。
- 要在 思科防御协调器 中创建 HA 对，两台设备都必须配置管理接口。如果设备配置了数据接口，则必须通过 FDM 管理 UI 创建 HA 对，然后将该对载入 CDO。

Note 您不能在 HA 对中使用 FDM 管理 模板。

高可用性的软件要求

物理和虚拟 FDM 管理 设备必须满足以下软件要求：

- 您有两台已在 Defense Orchestrator 中载入的独立 FDM 管理 设备。
- 设备必须运行完全相同的软件版本，也即，主要版本号（第一个）、次要版本号（第二个）以及维护版本号（第三个）都必须相同。您可以在设备详情窗口的**清单 (Inventory)** 页面，或者可以在 CLI 中使用显示版本命令找到版本。

Note 允许连接具有不同版本的设备，但配置不会导入备用设备且故障切换无法使用，直到您将设备升级到同一软件版本。

- 两台设备必须在本地管理器模式下运行，也即，使用FDM配置设备。如果您可以在两个系统上登录 FDM，则表示这两台设备是本地管理器模式。您还可以在 CLI 中使用 show managers 命令进行验证。
- 您必须在每台设备中完成初始设置向导，然后再载入 CDO。
- 每台设备都必须有自己的管理 IP 地址。管理接口的配置在两台设备之间未同步。
- 设备必须具有相同的 NTP 配置。
- 不能配置任何接口使用 DHCP 获取地址。也就是说，所有接口都必须有静态 IP 地址。

  注意：如果更改任何接口配置，则必须在建立 HA 之前将更改部署到设备。
- 两台设备必须保持**同步**。如果检测到待处理更改或冲突，请参阅解决配置冲突和解决配置冲突以了解详细信息。

Note 当您选择接受 HA 对更改或在部署到 FDM 管理 HA 对时，您将与 HA 对的主用设备通信。这意味着仅从主用设备提取配置和备份。

高可用性的智能许可证要求

物理和虚拟 FDM 管理 设备必须满足以下许可证要求：

- 高可用性对中的两台设备都必须具有注册许可证或评估许可证。如果设备已注册，可以将其注册到不同的思科智能软件管理器账户，但这些账户的出口控制功能设置的状态必须相同，要么都启用这类设置，要么都禁用。但是，如果您已在设备上启用不同的可选许可证，上述设置便不再重要。
- 高可用性对中的两台设备在运行期间必须具有相同的许可证。如果没有足够的许可证，可能会出现一台设备合规，另一台设备不合规的情况。如果您的智能许可证账户不包含足够的购买权利，则您的账户将在您购买正确数量的许可证之前变得不符合要求（即使其中一台设备符合要求）。

请注意，如果设备处于评估模式，您必须确保CDO的注册状态在两台设备上相同。您还必须确保选择的思科 Success Network 参与状态相同。对于已注册设备，设置可以在两台设备上不同，但任何已在主（主用）设备上配置的对象将在辅助设备上注册或注销。同意在主设备上参与思科成功网络意味着辅助设备上也将执行相同操作。

如果将用户注册到存在不同出口控制功能设置的账户，或者尝试创建一个 HA 对，注册其中的一台设备，而将另外一台设备设置为评估模式，则 HA 加入可能会失败。对于出口控制功能，如果您使用不一致的设置配置 IPSec 加密密钥，当您激活 HA 后，两个设备都将变为主用状态。这会影响受支持网段上的路由，且您必须手动断开辅助设备上的 HA 才能消除影响。

HA 的云服务配置

高可用性对中的两台设备都必须启用**将事件发送到思科云 (Send Events to the Cisco Cloud)**。此功能在 FDM UI 中可用。导航至**系统设置 (System Settings)**，然后点击**云服务 (Cloud Services)** 以启用此

功能。如果未启用此选项，则无法在 CDO 中形成 HA 对，并且会发生事件描述错误。有关详细信息，请参阅所运行版本的《Firepower 设备管理器配置指南》的**配置云服务**一章。

创建 FDM 管理 高可用性对

在 Defense Orchestrator 中创建 FDM 管理 HA 对之前，必须首先载入满足FDM 管理 高可用性对要求中所述的两个独立 FDM 管理 设备。

Note 要在 CDO 中创建 HA 对，两台设备都必须配置管理接口。如果设备配置了数据接口，则必须通过 FDM 控制台创建 HA 对，然后将该对载入 CDO。

创建 FDM 管理 高可用性对后，默认情况下，主设备处于**主用状态**，辅助设备处于**备用状态**。所有配置更改或部署都通过主设备进行，辅助设备保持备用模式，直到主设备不可用。

请注意，当您选择接受配置更改或部署到 FDM 管理 HA 对时，您将与 HA 对的主用设备通信。对主设备所做的任何更改都通过主设备和辅助设备之间的链路传输。CDO 会部署到主设备并仅接受来自主设备的更改；因此，**清单 (Inventory)** 页面显示该对的单个条目。部署完成后，主设备会将所有配置更改同步到辅助设备。

类似于 CDO 如何仅与主用设备通信，当您计划或选择备份 FDM 管理 HA 对时，只有主用设备符合备份条件。

Note 如果 HA 设备在创建过程中遇到问题，或者 HA 对未处于正常状态，则必须手动中断 HA 配置，然后才能尝试再次创建该对。

操作步骤

使用以下程序从两个独立 FTD 设备创建 HA 对：

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡并选择要建立为主设备的设备。

Note CDO 不支持使用配置了 DHCP 的设备创建 HA 对。

步骤 4 在“管理”(Management)窗格中，点击**高可用性 (High Availability)**。

步骤 5 找到辅助设备的区域并点击**选择设备 (Select Device)**，然后从符合条件的设备列表中选择一个设备。

步骤 6 配置故障转移链路。

a. 点击**物理接口 (Physical Interface)** 并从下拉菜单中选择接口。

b. 选择适当的 **IP 类型**。

c. 输入**主 IP** 地址。

d. 输入**辅助 IP** 地址。

e. 输入**子网掩码**。默认情况下，该值为 24。

f. 如果适用，请输入有效的 **IPSec 加密密钥**。

步骤 7 配置状态链路。如果要使用与故障转移链路相同的配置，请选中**与故障转移链路相同 (The same as Failover Link)** 复选框。如果要使用其他配置，请使用以下程序：

a. 点击**物理接口 (Physical Interface)** 并从下拉菜单中选择接口。请注意，主设备和辅助设备**必须**具有相同数量的物理接口。

b. 选择适当的 **IP 类型**。

c. 输入**主 IP** 地址。

d. 输入**辅助 IP** 地址。

e. 输入**子网掩码**。默认情况下，该值为 24。

步骤 8 在屏幕的右上角点击**创建 (Create)** 以便完成向导。CDO 会立即将您重定向到“高可用性状态”(High Availability Status) 页面。在此页面中，您可以监控 HA 创建的状态。请注意，创建 HA 对后，**清单 (Inventory)** 页面会将该对显示为单行。

步骤 9 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

“高可用性”(High Availability) 页面中的 FDM 管理设备

高可用性 (HA) 管理页面中的 FDM 管理 是 FDM 管理设备的多用途页面。此页面仅适用于已配置为 HA 对的设备。您可以载入 FDM 管理 HA 对，也可以从两台独立 FDM 管理设备创建 FDM 管理 HA 对。

如果从**清单 (Inventory)** 页面选择独立 FDM 管理设备，则此页面将用作创建 HA 对的向导。此时，您必须将两台 FDM 管理设备载入到 思科防御协调器 才能创建配对。要在 CDO 中创建 FDM 管理 HA 对，请参阅创建 FDM 管理 高可用性对。

如果从**清单 (Inventory)** 页面选择 FDM 管理 HA 对，则此页面将用作概述页面。在这里，您可以查看 HA 配置和故障转移历史记录，以及可操作的项目，例如强制故障转移、编辑故障转移条件以及删除 HA 链路。

高可用性管理页面

要查看“高可用性”(High Availability) 页面，请使用以下程序：

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡，然后选择独立 FDM 管理设备**或** FDM 管理 HA 对的主用 FDM 管理设备。

步骤 4 在**管理 (Management)** 窗格中，点击**高可用性 (High Availability)**。

相关信息：

- FDM 管理 高可用性故障转移历史记录
- 编辑高可用性故障切换条件
- 在高可用性对上强制执行故障切换FDM 管理
- 中断 FDM 管理 高可用性对
- 刷新 FDM 管理 高可用性状态

编辑高可用性故障切换条件

您可以在创建 FTD HA 对后编辑故障转移条件。

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡，然后选择 FTD HA 对的主用设备。

步骤 4 在“管理”(Management)窗格中，点击**高可用性 (High Availability)**。

步骤 5 在“故障转移条件”(Failover Criteria) 窗口中，点击**编辑 (Edit)**。

步骤 6 进行任何必要的更改，然后点击**保存 (Save)**。

步骤 7 预览和部署所有设备的配置更改您现在所做的更改到主用设备，或等待并一次部署多个更改。

中断 FDM 管理 高可用性对

中断高可用性时，备用设备上的已配置接口将自动禁用。在此过程中，设备可能会遇到流量中断。成功删除 HA 对后，您将从状态页面重定向到“高可用性”页面，您可以在其中选择使用相同的主设备创建另一个 HA 对。

Note 在成功删除高可用性对之前，您无法部署到任一设备。

使用管理接口中断高可用性

中断配置了管理接口的 HA 对时，中断可能需要 10 分钟或更长时间才能完成，并且在此过程中两台设备都会离线。成功删除 HA 配置后，CDO 会在“服务和设备”页面中将两台设备显示为独立设备。

使用数据接口中断高可用性

中断已配置数据接口的 HA 时，中断可能需要 20 分钟或更长时间才能完成，并且两台设备都会离线。删除高可用性配置后，您必须手动重新连接主用设备。

但是，备用设备会保留 HA 配置，并且将无法访问，因为它与主用设备具有相同的配置。您必须在 CDO 外部手动重新配置 IP 接口，然后将设备作为独立设备重新载入。

中断高可用性

使用以下程序删除两台 FDM 管理设备的 HA 配对：

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**，然后选择 FDM 管理 HA 对的主用设备。

步骤 2 点击 **设备** 选项卡，找到您的设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 在“管理”(Management)窗格中，点击**高可用性 (High Availability)**。

步骤 5 点击**中断高可用性 (Break High Availability)**。

步骤 6 CDO 将删除 HA 配置，两台设备在**清单 (Inventory)** 页面中显示为独立设备。

步骤 7 将配置更改从 CDO 部署到 FDM 管理 设备，以便将新配置部署到两台设备。

步骤 8 预览和部署所有设备的配置更改您现在所做的更改到主用设备，或等待并一次部署多个更改。

中断带外高可用性

如果使用 FDM 接口中断 FDM 管理 HA 对，则 思科防御协调器 中 HA 对的配置状态会更改为**检测到冲突 (Conflict Detected)**。中断高可用性后，您必须通过 FDM 管理 将更改部署到主设备，然后解决 CDO 中的解决配置冲突 状态。

设备恢复为“已同步”(Synced) 状态后，您可以将 CDO 中所做的配置更改部署到设备。

我们不建议在使用 FDM 管理 接口中断高可用性后从 CDO 恢复更改。

相关信息：

- FDM 管理 高可用性故障转移历史记录
- 刷新 FDM 管理 高可用性状态
- 在高可用性对上强制执行故障切换FDM 管理
- 读取、丢弃、检查和部署更改

在高可用性对上强制执行故障切换FDM 管理

通过强制故障切换来切换 HA 对中的主用设备和备用设备。FDM 管理请注意，如果您最近将新证书应用于主用设备，并且尚未部署更改，则备用设备会保留原始证书，并且故障切换将失败。主用设备和备用设备必须应用相同的证书。使用以下程序手动强制执行故障切换：

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择 HA 对的主用设备。FDM 管理

步骤 5 在“管理”(Management)窗格中，点击**高可用性 (High Availability)**。

步骤 6 点击选项图标。 

步骤 7 点击切换模式。主用设备现在处于备用状态，备用设备现在处于活动状态。

相关信息：

- 中断 FDM 管理 高可用性对
- FDM 管理 高可用性故障转移历史记录
- 刷新 FDM 管理 高可用性状态
- 在高可用性对上强制执行故障切换 在高可用性对上强制执行故障切换FDM 管理

FDM 管理 高可用性故障转移历史记录

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择 HA 对的主用设备。FDM 管理

步骤 5 在“管理”(Management)窗格中，点击**高可用性 (High Availability)**。

步骤 6 点击**故障转移历史 (Failover History)**。CDO 会生成一个窗口，其中详细说明自 HA 对形成以来主设备和辅助设备的故障切换历史记录。

Note 故障切换历史记录也会显示在设备对的更改日志中，可从“资产”页面获取。

相关信息：

- 中断 FDM 管理 高可用性对
- FDM 管理 高可用性故障转移历史记录
- 刷新 FDM 管理 高可用性状态
- 在高可用性对上强制执行故障切换 在高可用性对上强制执行故障切换FDM 管理

刷新 FDM 管理 高可用性状态

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡，然后选择 FDM 管理 设备或 FDM 管理 HA 对。

步骤 4 在 **管理** 窗格中，点击 **高可用性**。

步骤 5 点击选项图标。 

步骤 6 点击获取最新状态。CDO 从主设备请求运行状况。

相关信息：

- 中断 FDM 管理 高可用性对
- FDM 管理 高可用性故障转移历史记录
- 刷新 FDM 管理 高可用性状态
- 在高可用性对上强制执行故障切换 在高可用性对上强制执行故障切换FDM 管理

用于 FDM 管理 高可用性的故障转移和状态链路

故障转移链路和（可选）状态链路

故障转移链路是两台设备之间的专用连接。状态故障转移链路也是专用连接，不过，您可以使用一个故障转移链路作为组合的故障转移/状态链路，也可以创建单独的专用状态链路。如果仅使用故障转移链路，状态信息也会通过该链路：状态故障转移功能不会受到影响。默认情况下，故障转移和状态故障转移链路上的通信是纯文本通信（不加密）。为了增强安全性，您可以通过配置 IPsec 加密密钥对通信加密。

您可以将任何未使用的数据物理接口用作故障转移链路和可选的专用状态链路。但是，您不能选择当前已配置名称或具有子接口的接口。故障转移和状态故障转移链路接口不会被配置为通常的网络接口。这些接口只是为了进行故障转移通信，不能用于直通流量或管理访问。此配置在设备之间是同步的，因此您必须为链路的两端选择相同的端口号。例如，用于故障转移链路的两台设备都使用 GigabitEthernet1/3。

Note FDM 管理 设备用户数据和故障转移链路之间共享接口。

故障转移链路

故障转移对中的两台设备会不断地通过故障转移链路进行通信，以确定每台设备的运行状态和同步配置更改。通过此链接共享以下信息：

- 设备状态（主用或备用）
- Hello 消息 (keep-alives)
- 网络链路状态
- MAC 地址交换
- 配置复制和同步

您可以使用未使用的数据接口（物理接口、冗余接口或 EtherChannel 接口）作为故障转移链路；但不能指定当前配置了名称的接口。请**勿**使用子接口作为故障转移链路。

故障转移链路接口不会配置为常规网络接口；该接口仅会因为故障转移而存在。该接口只能用于故障转移链路（还用于状态链路）。

状态链接

主用设备使用状态链路将连接状态信息传送到备用设备。这意味着，备用设备可以保持某些类型的连接，而不会影响用户。此信息可在发生故障转移时帮助备用设备保留现有连接。

您可以将专用接口（物理、冗余或EtherChannel）用于状态链路。对于用作状态链路的EtherChannel，要阻止无序数据包，仅使用EtherChannel中的一个接口。如果该接口发生故障，则会使用EtherChannel中的下一个接口。

对故障转移和状态故障转移链路使用一条链路能够最大程度地节省接口。但是，如果您有一个大型配置和高流量网络，必须考虑对状态链路和故障转移链路使用专用接口。我们建议状态故障转移链路的带宽应匹配设备上数据接口的最大带宽。

FDM 管理 设备设置

配置 FTD 设备的系统设置

使用此程序在单个 FTD 设备上配置设置：

Procedure

步骤 1 打开**清单 (Inventory)** 页面。

步骤 2 点击 **设备** 选项卡，找到您的设备。

步骤 3 点击 **FTD** 选项卡，然后选择要配置其设置的设备。

步骤 4 在右侧的**管理 (Management)** 窗格中，点击**设置 (Settings)**。

步骤 5 点击**系统设置 (System Settings)** 选项卡。

步骤 6 编辑这些设备设置：

- 配置管理访问
- 配置日志记录设置
- 配置 DHCP 服务器
- 配置 DNS 服务器
- 主机名
- 配置 NTP 服务器
- 配置 URL 过滤
- 云服务
- 启用或禁用网络分析

配置管理访问

默认情况下，您可以从任何 IP 地址访问设备的管理地址。系统访问仅受用户名和密码的保护。但是，您可以配置访问列表以仅允许来自特定 IP 地址或子网的连接，以进一步加强保护。

您还可以开放数据接口以允许 FDM 管理 设备或 SSH 连接至 CLI。然后，无需使用管理地址即可管理设备。例如，您可以允许对外部接口进行管理访问，这样就能远程配置设备。用户名和密码可防止不想要的连接。默认情况下，对数据接口的 HTTPS 管理访问会在内部接口上启用而在外部接口上禁用。对于具有默认“内部”网桥组的设备型号，这意味着可以通过网桥组中的任意数据接口，与网桥组 IP 地址（默认值为 192.168.1.1）建立 FDM 管理 设备连接。您可以只在进入设备所通过的接口上开放管理连接。

⚠

注意 如果只允许访问特定地址，那么您可能很容易将自己锁定在系统之外。如果删除对当前所用 IP 地址的访问，并且没有“任何”地址条目，则在部署策略时将丢失对系统的访问。在配置访问列表时请注意这一点。

为管理接口创建规则

使用以下程序为管理接口创建规则：

过程

步骤 1 点击“管理接口”(Management Interface) 部分中的**新访问权限 (New Access)**。

- **Protocol**。选择规则是用于 HTTPS（端口 443）还是 SSH（端口 22）。
- **允许的网络**。选择定义应该能够访问系统的 IPv4 或 IPv6 网络或主机的网络对象。要指定“任何”地址，请选择 **any-ipv4** (0.0.0.0/0) 和 **any-ipv6**(::/0)。

步骤 2 点击**保存 (Save)**。

为数据接口创建规则

使用以下程序为数据接口创建规则：

过程

步骤 1 点击“数据接口”(Data Interface) 部分中的**新访问权限 (New Access)**。

- **接口**。选择要在其上允许管理访问的接口。
- **Protocol**。选择规则是用于 HTTPS（端口 443）、SSH（端口 22）还是二者。不能为远程访问 VPN 连接配置文件中使用的外部接口配置 HTTPS 规则。
- **允许的网络**。选择定义应该能够访问系统的 IPv4 或 IPv6 网络或主机的网络对象。要指定“任何”地址，请选择 **any-ipv4** (0.0.0.0/0) 和 **any-ipv6** (::/0)。

步骤 2 点击**保存 (Save)**。

步骤 3 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

配置日志记录设置

此程序介绍如何启用数据（诊断）事件、文件事件和恶意软件事件事件、入侵事件事件和控制台事件的日志记录。由于这些设置，连接事件不会被记录。如果在访问规则、安全情报策略或 SSL 解密规则上配置了连接日志记录，则会记录连接事件。

Procedure

步骤 1 配置 FTD 设备的系统设置。

步骤 2 在“系统设置”(System Settings) 页面上，点击设置菜单中的**日志记录 (Logging)**。

步骤 3 **数据日志记录**。将**数据日志记录 (Data Logging)** 滑块滑动到**开 (On)** 以捕获诊断日志记录系统日志消息。点击加号按钮  以指定表示要向其发送事件的系统日志服务器的系统日志服务器对象。（此时您还可以创建系统日志服务器对象。）此外，请选择要记录的最低消息 严重性级别级别。

这会将任何类型的系统日志消息的数据日志记录事件以及您选择的最低严重性级别发送到系统日志服务器。

Note 思科防御协调器 当前不支持为数据日志记录创建自定义日志记录过滤器。为了更好地控制向系统日志服务器发送的消息，我们建议您在 FDM 管理 设备中定义此设置。为此，请登录 FDM 管理 设备，然后导航至**系统设置 (System Settings)** > **日志记录设置 (Logging Settings)**。

Tip 如果您是思科安全分析和日志记录客户，请勿启用数据日志记录，除非您将数据日志记录事件转发到安全事件连接器之外的系统日志服务器。数据事件（诊断事件）不是流量事件。将数据事件发送到不同的系统日志服务器可以消除 SEC 分析和过滤事件的负担。

步骤 4 **文件/恶意软件日志设置**。将滑块滑动到**开 (On)** 以捕获文件事件 和恶意软件事件。指定表示要将事件发送到的系统日志服务器的系统日志服务器对象。如果尚未创建系统日志服务器对象，也可以在此时创建。

生成的文件和恶意软件事件的严重性级别相同。您选择的最低消息 严重性级别级别将分配给所有文件和恶意软件事件。

触发任何访问控制规则中的文件或恶意软件策略时，会报告文件和恶意软件事件。这与连接事件不同。请注意，仅当您应用需要 和恶意软件许可证的文件或恶意软件策略时，文件/恶意软件事件的系统日志设置才具有相关性。

对于思科安全分析和日志记录用户：

- 如果通过安全事件连接器 (SEC) 将事件发送到思科云，请指定 SEC 作为系统日志服务器。然后，您将能够在文件策略和恶意软件策略连接事件旁边看到这些事件。
- 如果您在没有 SEC 的情况下直接将事件发送到思科云，则无需启用此设置。如果访问控制规则配置为发送连接事件，则会发送文件和恶意软件事件。

步骤 5 **入侵日志记录**。通过指定表示要将事件发送到的系统日志服务器的系统日志服务器对象，将入侵事件发送到系统日志服务器。如果尚未创建系统日志服务器对象，也可以在此时创建。

触发任何访问控制规则中的入侵策略时，会报告入侵事件。这与连接事件不同。请注意，仅当您应用需要 许可证的入侵策略时，入侵事件的系统日志设置才有意义。

对于思科安全分析和日志记录用户：

- 如果通过安全事件连接器 (SEC) 将事件发送到思科云，请指定 SEC 作为系统日志服务器。然后，您将能够在文件策略和恶意软件策略连接事件旁边看到这些事件。
- 如果您在没有 SEC 的情况下直接将事件发送到思科云，则无需启用此设置。如果访问控制规则配置为发送连接事件，则将入侵事件发送到思科云。

步骤 6 **控制台过滤器**。将滑块滑动到**开 (On)**，将数据日志记录（诊断日志记录）事件发送到控制台而不是系统日志服务器。此外，请选择要记录的最低事件严重性级别。这将为任何类型的系统日志消息发送数据日志记录事件，其中包含您选择的严重性级别。

当在 FDM 管理 设备的控制台端口上登录 CLI 时，您会看到这些消息。使用 **show console-output** 命令也可以在其他 FDM 管理 设备接口（包括管理接口）的 SSH 会话中看到这些日志。此外，从主 CLI 中输入 **system support diagnostic-cli** 即可在诊断 CLI 中实时查看这些消息。

步骤 7 点击**保存 (Save)**。

步骤 8 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

消息 严重性级别

下表列出系统日志消息严重性级别。

级别号	严重性级别	说明
0	应急	系统不可用。
1	警报	需要立即采取措施。
2	严重	严重情况。
3	错误	错误情况。
4	警告	警告情况。
5	通知	正常但重大的情况。
6	信息性	消息仅供参考。
7	调试	消息仅供调试。
Note	FDM管理 设备不会生成严重性级别为零（紧急）的系统日志消息。	

配置 DHCP 服务器

动态主机配置协议 (DHCP) 服务器可为 DHCP 客户端提供网络配置参数，例如 IP 地址。您可以在接口上配置 DHCP 服务器，为连接的网络上的 DHCP 客户端提供配置参数。

IPv4 DHCP 客户端使用广播而非组播地址到达服务器。DHCP 客户端侦听 UDP 端口 68 上的消息。DHCP 服务器侦听 UDP 端口 67 上的消息。DHCP 服务器不支持 BOOTP 请求。

DHCP客户端必须与启用了服务器的接口位于同一网络内。服务器和客户端之间不能有干预路由器，但可以有交换机。

⚠

Caution 不要在已经有 DHCP 服务器运行的网络上配置 DHCP 服务器。这两个服务器间将发生冲突，结果不可预测。

Procedure

步骤 1 该部分有两个区域。一开始，配置区域显示全局参数。DHCP 服务器区域显示已在其上配置服务器的接口、服务器启用情况以及服务器的地址池。

步骤 2 在**配置 (Configuration)** 部分中，配置自动配置和全局设置。

DHCP 自动配置使 DHCP 服务器能为 DHCP 客户端提供从运行于指定接口上的 DHCP 客户端获得的 DNS 服务器、域名和 WINS 服务器信息。通常，如果您是在使用 DHCP 获取地址，则会使用自动配置，但您可以选择通过 DHCP 获取其地址的任何接口。如果无法使用自动配置，可以手动定义所需的选项。

a. 如果要使用自动配置，请点击**启用自动配置 (Enable Auto Configuration)** 滑块，然后在**从接口 (From Interface)** 下拉列表中选择正在通过 DHCP 获取其地址的接口。

b. 如果不启用自动配置，或者如果要覆盖任何一个自动配置的设置，请配置以下全局选项。这些设置将发送到托管 DHCP 服务器的所有接口上的 DHCP 客户端。

1. **主 WINS IP 地址**、**辅助 WINS IP 地址**。Windows Internet Name Service (WINS) 服务器客户端应该用于 NetBIOS 域名解析的地址。
2. **主 DNS IP 地址**、**辅助 DNS IP 地址**。客户端应该用于域名解析的域名系统 (DNS) 服务器的地址。如果要使用思科 Umbrella DNS 服务器填充 DNS IP 地址字段，请点击**应用 Umbrella 设置 (Apply Umbrella Settings)**。点击该按钮会将正确的 IP 地址载入字段中。

c. 点击**保存 (Save)**。

步骤 3 在“DHCP 服务器”(DHCP Servers) 部分中编辑现有服务器，或者点击**新建 DHCP 服务器 (New DHCP Server)** 以添加和配置新服务器。

a. 配置服务器属性：

1. **启用 DHCP 服务器**。是否启用服务器。您可以配置服务器，但在做好准备开始使用之前，要一直将其禁用。
2. **接口**。选择您为客户端提供 DHCP 地址的接口。接口必须拥有静态 IP 地址；如果要在接口上运行 DHCP 服务器，则不能使用 DHCP 获取接口。对于网桥组，在网桥虚拟接口 (BVI) 上（而不是成员接口上）配置 DHCP 服务器，并且服务器在所有成员接口上运行。您不能在诊断接口上配置 DHCP 服务器，而应在管理接口上配置，它位于**设备 (Device)** > **系统设置 (System Settings)** > **管理接口 (Management Interface)** 页面中。
3. **地址池**。添加 DHCP 服务器的单个 IP 地址或 IP 地址范围。允许服务器为请求地址的客户端提供的 IP 地址的范围（最低至最高）。该 IP 地址范围必须与所选接口位于同一子网上，并且不能包括接口本身的 IP 地址、广播地址或子网地址。指定该池的开始和结束地址，用连字符隔开。例如 10.100.10.12-10.100.10.250。

b. 点击**确定 (OK)**。

步骤 4 点击**保存 (Save)**。

步骤 5 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

配置 DNS 服务器

域名系统 (DNS) 服务器用来将主机名解析到 IP 地址。管理接口用于 DNS 服务器。

Procedure

步骤 1 在**主、辅助、第三 DNS IP 地址 (Primary, Secondary, Tertiary DNS IP Address)** 中，按照首选项顺序输入最多三个 DNS 服务器的 IP 地址。正常情况下，会使用主 DNS 服务器，除非联系不上它，在这种情况下，会尝试使用辅助服务器，最终尝试第三服务器。如果要使用思科 Umbrella DNS 服务器填充 DNS IP 地址字段，请点击**应用 Umbrella 设置 (Apply Umbrella Settings)**。点击该按钮会将正确的 IP 地址载入字段中。

步骤 2 在**域搜索名称 (Domain Search Name)** 中，输入网络的域名，例如 example.com。此域将被附加到非完全限定的主机名，例如 serverA 而不是 serverA.example.com。

步骤 3 点击**保存 (Save)**。

步骤 4 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

管理接口

管理接口是一个连接到物理管理端口的虚拟接口。该物理端口名为诊断接口，可在“接口”页面上使用其他物理端口进行配置。在虚拟 FDM 管理 设备上，即使两个接口都是虚拟接口，这种双重性也保持不变。

管理接口有两种用途：

- 您可以与该 IP 地址建立 Web 连接和 SSH 连接，并通过该接口配置设备。
- 系统通过此 IP 地址获取智能许可和数据库更新。

如果使用 CLI 安装向导，则在初始系统配置期间，为设备配置管理地址和网关。如果使用 FDM 管理 安装向导，管理地址和网关将保留默认值。

如果需要，可以通过 FDM 管理 设备来更改这些地址。您还可以在 CLI 中使用 **configure network ipv4 manual** 和 **configure network ipv6 manual** 命令更改管理地址和网关。

您可以定义静态地址，也可以在管理网络中有另一台设备用作 DHCP 服务器时，通过 DHCP 获取地址。默认情况下，管理地址是静态的，而且 DHCP 服务器通常运行在端口（虚拟 FDM 管理 设备除外，它没有 DHCP 服务器）。因此，您可以将设备直接连接到管理端口并为工作站获取 DHCP 地址。这种方法可以十分方便地连接和配置设备。

Caution 如果更改当前连接的地址，则当保存更改时，由于这些更改会立即应用，您将丢失对 FDM 管理 设备（或 CLI）的访问。您需要重新连接到设备。确保新地址有效且在管理网络中可用。

Procedure

步骤 1 配置管理 IP 地址、网络掩码或 IPv6 前缀，并根据需要配置 IPv4 和/或 IPv6 的网关。必须配置至少一组属性。将一组设置留空将会禁用该寻址方法。

步骤 2 依次选择**类型** > **DHCP**，通过 DHCP 或 IPv6 自动配置功能获取地址和网关。但是，如果使用数据接口作为网关，则不能使用 DHCP。在此情况下，必须使用静态地址。

步骤 3 点击**保存 (Save)**。

步骤 4 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

主机名

可以更改设备主机名。

Procedure

步骤 1 在**防火墙主机名 (Firewall Hostname)** 字段中，输入设备的新主机名。

步骤 2 点击**保存 (Save)**。

步骤 3 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

配置 NTP 服务器

配置网络时间协议 (NTP) 服务器才能在系统上设置时间。

Procedure

步骤 1 选择使用您自己的（手动）时间服务器还是思科的时间服务器。

- **新 NTP 服务器**。输入您要使用的 NTP 服务器的完全限定域名或 IP 地址。例如 ntp1.example.com 或 10.100.10.10。
- **使用默认值**。

步骤 2 点击 **Save**。

步骤 3 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

配置 URL 过滤

系统从思科综合安全情报 (CSI) 获取 URL 类别和信誉数据库。这些首选项控制数据库更新和系统如何处理类别或信誉未知的 URL。必须启用 URL 过滤许可证，才能设置这些首选项。

Caution 如果您没有 URL 智能许可证，则可以配置 URL 过滤首选项，但需要智能许可证才能部署。在添加 URL 智能许可证之前，系统将阻止您进行部署。

Procedure

步骤 1 启用应用选项：

- 点击**启用自动更新 (Enable Automatic Updates)** 滑块开启以允许系统自动检查和下载更新的 URL 数据，这些数据中包括类别和信誉信息。部署后，FDM 管理 设备每 30 分钟检查一次更新。
- 点击**通过 Cisco CSI 查询未知 URL (Query Cisco CSI for Unknown URLs)** 滑块开启以对在本地 URL 过滤数据库中不含类别和信誉数据的 URL，是否通过 Cisco CSI 查询其更新的信息。
- 仅当启用**查询思科 CSI 以获取未知 URL (Query Cisco CSI for Unknown URLs)** 选项时，**URL 生存时间 (URL Time to Live)** 才有效。这决定了为给定 URL 缓存类别和信誉查找值的时间。生存时间到期时，下一个 URL 访问尝试将导致新的类别/信誉查找。更短的时间会产生更准确的 URL 过滤，较长的时间会给未知 URL 带来更好的表现。这是默认选择是**从不 (Never)**。

步骤 2 点击**保存 (Save)**。

步骤 3 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

云服务

使用“云服务”页面管理基于云的服务。

Note 可以在运行软件版本 6.6 及更高版本的 FTD 设备上配置连接到思科成功网络并配置将哪些事件发送到思科云的功能。

连接到思科成功网络

通过启用思科成功网络，可以向思科提供使用信息和统计信息，这对思科为您提供技术支持至关重要。通过此信息，思科还可以改进产品，并使您获悉未使用的可用功能，以便您能够在网络中将产品的价值最大化。

启用连接时，设备将与思科云建立安全连接，以确保设备可以参与思科提供的其他服务（例如技术支持服务、云管理和监控服务）。您的设备将随时建立并维护此安全连接。

准备工作

要启用思科成功网络，必须使用FDM管理设备向云注册设备。要注册该设备，请使用思科智能软件管理器（在“智能许可”页面上）注册该设备，或者通过输入注册密钥使用思科防御协调器进行注册。

Attention 如果您在高可用性组的主用设备上启用思科成功网络，也会在备用设备上启用该连接。

Procedure

步骤 1 点击**云服务 (Cloud Services)** 选项卡。

步骤 2 点击思科成功网络功能的**启用**滑块，以根据需要更改设置。

步骤 3 点击**保存 (Save)**。

步骤 4 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

将事件发送至思科云

可以将事件发送至思科云服务器。各种思科云服务均可从这里访问事件。然后，可以使用这些云应用（例如思科威胁响应）来分析事件并评估设备可能遇到的威胁。

准备工作

您必须先向思科智能软件管理器注册设备，然后才能启用此服务。

在美国地区通过 https://visibility.amp.cisco.com/，在欧盟地区通过 https://visibility.amp.cisco.com/，可以连接至思科威胁响应。您可以在 YouTube 上观看视频 (http://cs.co/CTRvideos)，了解此应用的使用方法和优点。有关思科威胁响应与 FTD 结合使用的更多信息，请参阅 https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html 处提供的《*Firepower* 和 *CTR* 集成指南》。

Procedure

步骤 1 点击**云服务 (Cloud Services)** 选项卡。

步骤 2 点击**发送事件到思科云 (Send Events to the Cisco Cloud)** 选项的**启用 (Enabled)**滑块，以便根据需要更改设置。

步骤 3 当您启用该服务时，系统会提示您选择要发送到云的事件。

- **文件/恶意软件 (File/Malware)** - 适用于在任何访问控制规则中应用的任何文件策略。
- **入侵事件 (Intrusion Events)** - 适用于在任何访问控制规则中应用的任何入侵策略。
- **连接事件 (Connection Events)** - 适用于已启用日志记录的访问控制规则。选择此选项后，您还可以选择发送所有连接事件，或者只发送高优先级连接事件。高优先级连接事件是指与触发入侵、文件或恶意软件事件的连接相关，或与匹配安全智能阻止策略的连接相关。

步骤 4 点击**保存 (Save)**。

步骤 5 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

启用或禁用网络分析

启用网络分析可根据页面点击量向思科提供匿名产品使用情况信息。这类信息包括查看的页面、在页面上花费的时间、浏览器版本、产品版本、设备主机名等。此信息可帮助思科确定功能使用模式，帮助思科改进产品。所有使用情况数据均为匿名数据，且不会传输敏感数据。您可以使用CDO在所有版本的 FDM 管理 设备上配置此功能。

默认启用网络分析。

Procedure

步骤 1 点击 **Web 分析 (Web Analytics)** 选项卡。

步骤 2 点击**Web 分析 (Web Analytics)** 功能的**启用 (Enable)** 滑块，根据需要更改设置。

步骤 3 点击**保存 (Save)**。

步骤 4 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

CDO 命令行接口

CDO 为用户提供命令行界面 (CLI)，用于管理 、FDM 管理 威胁防御 设备。用户可以将命令发送到单个设备或同时发送到多个设备。

相关信息：

- 有关 FTD CLI 文档，请参阅思科 Firepower 威胁防御命令参考。请注意，FDM 管理 设备的 CLI 功能有限。这些设备只有以下命令：`show`、`ping`、`traceroute`、`packet-tracer`、`failover` 和 `shutdown`。

使用命令行接口

Procedure

步骤 1 打开**资产 (Inventory)** 页面。

步骤 2 点击资产表上方的设备按钮。

步骤 3 使用设备选项卡和过滤器按钮查找要使用命令行界面 (CLI) 管理的设备。

步骤 4 选择设备。

步骤 5 在**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。

步骤 6 点击 **命令行接口 (Command Line Interface)**。

步骤 7 在命令窗格中输入一个或多个命令，然后点击发送。 设备对命令的响应显示在下面的“响应窗格”中。

Note 如果可以运行的命令有限制，则会在命令窗格上方列出这些限制。

Related Topics

在命令行接口中输入命令 ，第 97 页

在命令行接口中输入命令

可以在一行中输入单个命令，也可以在多行中依次输入多个命令，CDO将按顺序执行这些命令。以下示例发送创建三个网络对象和包含这些网络对象的网络对象组的一批命令。ASA

输入设备命令：CLI 控制台使用基本 CLI。**FDM 管理**威胁防御不能使用 CLI 控制台进入诊断 CLI、专家模式、FXOS CLI（在使用 FXOS 的型号上）。如果需要进入其他 CLI 模式，请使用 SSH。

使用命令历史记录

发送 CLI 命令后，CDO 会在“命令行界面”(Command Line Interface) 页面的历史记录窗格中记录该命令。您可以重新运行历史记录窗格中保存的命令，或将这些命令用作模板：

Procedure

步骤 1 在资产页面上，选择要配置的设备。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击设备类型选项卡。

步骤 4 点击 **>_命令行接口 (>_Command Line Interface)**。

步骤 5 点击时钟图标可展开历史记录窗格（如果尚未展开）。 

步骤 6 在历史记录窗格中选择要修改或重新发送的命令。

步骤 7 按原样重新使用命令，或在命令窗格中对其进行编辑，然后点击发送。CDO 在响应窗格中显示命令的结果。

Note CDO 显示 Done!两种情况下响应窗格中的消息：

- 成功执行命令后。
- 当命令没有要返回的结果时。例如，您可以发出带有正则表达式的 show 命令，用于搜索配置条目。如果没有符合正则表达式条件的配置条目，CDO 将返回 Done!。

批量命令行接口

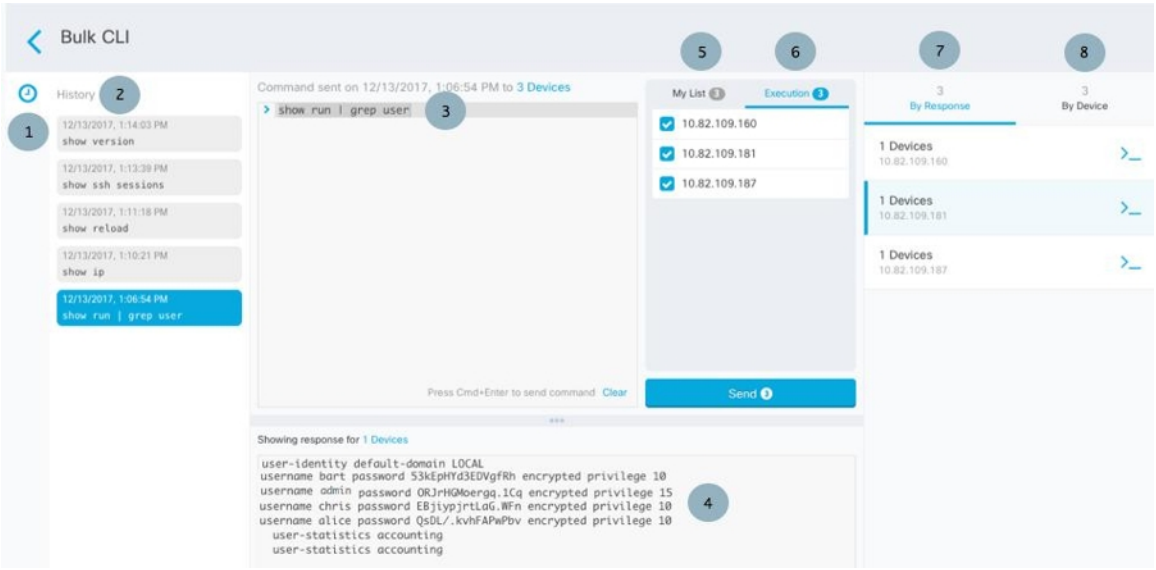
CDO 为用户提供使用命令行接口 (CLI) 管理 Secure Firewall ASA、FDM 管理 威胁防御、SSH、Cisco IOS 和 Cisco Secure Firewall Cloud Native设备。用户可以将命令发送到单个设备或同时发送到多个同类设备。本节介绍一次向多台设备发送 CLI 命令。

相关信息：

- 对于设备文档，CDO 仅支持基本 FTD CLI。FDM 管理这些设备只有以下命令：`show`、`ping`、`traceroute`、`packet-tracer`、`failover` 和 `shutdown`。

  有关 威胁防御 CLI 文档，请参阅思科 Firepower 威胁防御命令参考。

批量 CLI 接口



Note CDO 显示 Done!两种情况下的消息：

- 成功执行命令且无错误后。
- 当命令没有要返回的结果时。例如，您可以发出带有正则表达式的 show 命令，用于搜索某个配置条目。如果没有符合正则表达式条件的配置条目，CDO 将返回 Done!。

编号	说明
1	点击时钟可展开或折叠命令历史记录窗格。
2	命令历史记录。发送命令后，CDO 会在此历史记录窗格中记录该命令，以便您可以返回到该窗格，选择并再次运行该命令。
3	命令窗格。在此窗格的提示符后输入命令。
4	响应窗格。CDO 显示设备对命令的响应以及 CDO 消息。如果多个设备的响应相同，则响应窗格会显示消息“显示 X 台设备的响应”(Showing Responses for X devices)。点击 X 设备，CDO 将显示对命令返回相同响应的所有设备。 **Note** CDO 显示 Done!两种情况下的消息： • 成功执行命令且无错误后。 • 当命令没有要返回的结果时。例如，您可以发出带有正则表达式的 show 命令，用于搜索某个配置条目。如果没有符合正则表达式条件的配置条目，CDO 将返回 Done!。

编号	说明
5	我的列表选项卡显示您从资产表中选择的设备，并允许您包含或排除要向其发送命令的设备。
6	上图中突出显示的“执行”选项卡显示在历史记录窗格中选择的命令中的设备。在本例中，show run |在历史记录窗格中选择了 grep 用户命令，执行选项卡显示它已发送到 10.82.109.160、10.82.109.181 和 10.82.10.9.187。
7	点击“By Response”（按响应）选项卡将显示命令生成的响应列表。相同的响应组合在一行中。当您在“按响应”选项卡中选择一行时，CDO 会在响应窗格中显示对该命令的响应。
8	点击“按设备”选项卡会显示每个设备的单独响应。点击列表中的其中一个设备，即可查看特定设备对命令的响应。

批量发送命令

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 选择相应的设备选项卡，然后使用过滤器按钮查找要使用命令行界面配置的设备。

步骤 4 选择设备。

步骤 5 在**设备操作 (Device Actions)** 窗格中，点击**>_命令行接口 (>_Command Line Interface)**。

步骤 6 您可以在“我的列表”字段中选中或取消选中要向其发送命令的设备。

步骤 7 在命令窗格中输入命令，然后点击发送。命令输出显示在响应窗格中，命令记录在更改日志中，命令 CDO 在批量 CLI 窗口的历史记录窗格中记录您的命令。

使用批量命令历史记录

发送批量 CLI 命令后，CDO 会在“批量 CLI”页面历史记录页面中记录该命令。批量 CLI 接口, on page 98您可以重新运行历史记录窗格中保存的命令，也可以将这些命令用作模板。历史记录窗格中的命令与运行这些命令的原始设备相关联。

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击相应的设备类型选项卡，然后点击过滤器图标以查找要配置的设备。

步骤 4 选择设备。

步骤 5 点击 **命令行接口 (Command Line Interface)**。

步骤 6 在“历史记录”窗格中选择要修改或重新发送的命令。请注意，您选择的命令与特定设备相关联，而不一定是您在第一步中选择的设备。

步骤 7 查看我的列表选项卡，确保您要发送的命令将发送到您期望的设备。

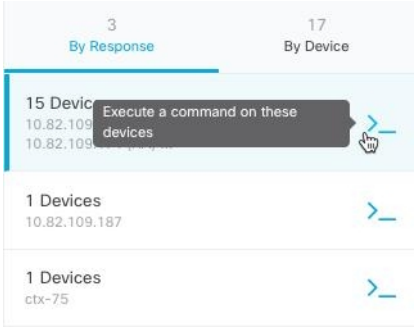
步骤 8 在命令窗格中编辑命令，然后点击发送。CDO 在响应窗格中显示命令的结果。

使用批量命令过滤器

运行批量 CLI 命令后，您可以使用“按响应”过滤器和“按设备”过滤器继续配置设备。

按响应过滤器

运行批量命令后，CDO 会使用发送该命令的设备返回的响应列表填充“按响应”选项卡。具有相同响应的设备会合并到一行中。点击“按响应”(By Response) 选项卡中的行会在响应窗格中显示设备的响应。如果响应窗格显示多个设备的响应，则会显示消息“显示 X 台设备的响应”。点击 X 设备，CDO 将显示对命令返回相同响应的所有设备。



要将命令发送到与命令响应关联的设备列表，请执行以下程序：

Procedure

步骤 1 点击 By Response 选项卡中一行中的命令符号。

步骤 2 查看命令窗格中的命令，然后点击发送以重新发送命令，或点击清除以清除命令窗格并输入要发送到设备的新命令，然后点击发送。

步骤 3 查看从命令收到的响应。

步骤 4 如果您确信所选设备上的运行配置文件反映了您的更改，请在命令窗格中键入 write memory，然后点击 Send。这样会将运行配置保存至启动配置。

按设备过滤器

运行批量命令后，CDO 会使用已发送命令的设备列表填充“执行”选项卡和“按设备”选项卡。点击“按设备”(By Device) 选项卡中的行会显示每个设备的响应。

要在同一设备列表上运行命令，请执行以下程序：

Procedure

步骤 1 点击**按设备 (By Device)** 选项卡。

步骤 2 点击 >_在这些设备上执行命令。

步骤 3 点击清除以清除命令窗格并输入新命令。

步骤 4 在我的列表窗格中，通过选中或取消选中列表中的单个设备来指定要向其发送命令的设备列表。

步骤 5 点击**发送 (Send)**。命令的响应会显示在响应窗格中。如果响应窗格显示多个设备的响应，则会显示消息“显示 X 台设备的响应”。点击 X 设备，CDO 将显示对命令返回相同响应的所有设备。

步骤 6 如果您确信所选设备上的运行配置文件反映了您的更改，请在命令窗格中键入 write memory，然后点击 Send。

用于管理设备的 CLI 宏

CLI 宏是可以使用的完整形式的 CLI 命令，或者是可以在运行之前修改的 CLI 命令的模板。所有宏都可以在一个或多个 FTD 设备上同时运行。

使用类似模板的 CLI 宏可同时在多台设备上运行相同的命令。CLI 宏可促进设备配置和管理的一致性。使用完全格式的 CLI 宏获取有关设备的信息。您可以立即在 FTD 设备上使用不同的 CLI 宏。

您可以创建 CLI 宏来监控您经常执行的任务。有关详细信息，请参阅从新命令创建 CLI 宏。

CLI 宏是系统定义的或用户定义的。系统定义的宏由 CDO 提供，无法编辑或删除。用户定义的宏由您创建，可以编辑或删除。

Note 只有在设备载入 CDO 后，才能为设备创建宏。

以 ASA 为例，如果要查找其中一个 ASA 上的特定用户，可以运行以下命令：

```
show running-config | grep username
```

运行命令时，您要将 *username* 替换为要搜索的用户的用户名。要使用此命令来创建宏，请使用相同的命令并在用户名周围加上大括号。

```
> show running-config | grep {{username}}
```

您可以随意命名参数。您还可以使用此参数名称创建相同的宏：

```
> show running-config | grep {{username_of_local_user_stored_on_asa}}
```

参数名称可以是描述性的，并且必须使用字母数字字符和下划线。命令语法，在本例中为

```
show running-config | grep
```

命令的一部分，必须对要向其发送命令的设备使用正确的 CLI 语法。

从新命令创建 CLI 宏

Procedure

步骤 1 在创建 CLI 宏之前，请在 CDO 的命令行界面中测试命令，以便确保命令语法正确并返回可靠的结果。

Note

- 对于 FTD 设备，CDO 仅支持可在 FDM 的 CLI 控制台中运行的命令：`show`、`ping`、`traceroute`、`packet-tracer`、`failover`、`reboot` 和 `shutdown`。有关这些命令的语法的完整说明，请参阅《思科 Firepower 威胁防御命令参考》。

步骤 2 在导航栏中，点击**清单 (Inventory)**。

步骤 3 点击 **设备 (Devices)**选项卡以找到设备。

步骤 4 点击相应的设备类型选项卡，然后选择在线和同步的设备。

步骤 5 点击 **>_Command Line Interface**。

步骤 6 点击 CLI 宏收藏夹星标 ★，以查看已经存在的宏。

步骤 7 点击加号按钮  。

步骤 8 请为宏指定唯一的名称。如果需要，请为 CLI 宏提供说明和注释。

步骤 9 在**命令 (Command)** 字段中输入完整命令。

步骤 10 运行命令时，将要修改的命令部分替换为用大括号括起来的参数名称。

步骤 11 点击**创建**。您创建的宏可用于该类型的所有设备，而不只是您最初指定的设备。

要运行命令，请参阅运行 CLI 宏。

从 CLI 历史记录或现有 CLI 宏创建 CLI 宏

在此程序中，您将从已运行的命令、另一个用户定义的宏或从系统定义的宏创建用户定义的宏。

过程

步骤 1 在导航栏中，点击 **设备和服务**。

注释 如果要从 CLI 历史记录创建用户定义的宏，请选择运行命令的设备。CLI 宏在同一账户上的设备之间共享，但不是 CLI 历史记录。

步骤 2 点击**设备**选项卡。

步骤 3 点击相应的设备类型选项卡，然后选择在线和同步的设备。

步骤 4 点击 **>_命令行接口**。

步骤 5 查找要生成 CLI 宏的命令，然后选择该命令。使用以下方法之一：

- 点击时钟可查看您在该设备上运行的命令。选择要转换为宏的命令，命令将显示在命令窗格中。
- 点击 CLI 宏收藏夹星标，以查看已经存在的宏。选择要更改的用户定义或系统定义的 CLI 宏。命令显示在命令窗格中。

步骤 6 使用 命令窗格中的 命令，点击 CLI 宏金色星标。命令现在是新 CLI 宏的基础。

步骤 7 请为宏指定唯一的名称。如果需要，请为 CLI 宏提供说明和注释。

步骤 8 查看命令字段中的命令，并进行所需的更改。

步骤 9 运行命令时，将要修改的命令部分替换为用大括号括起来的参数名称。

步骤 10 点击**创建**。您创建的宏可用于该类型的所有设备，而不只是您最初指定的设备。

要运行命令，请参阅运行 CLI 宏。

运行 CLI 宏

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击相应的设备类型选项卡，然后选择一个或多个设备。

步骤 4 点击 **>_命令行接口**。

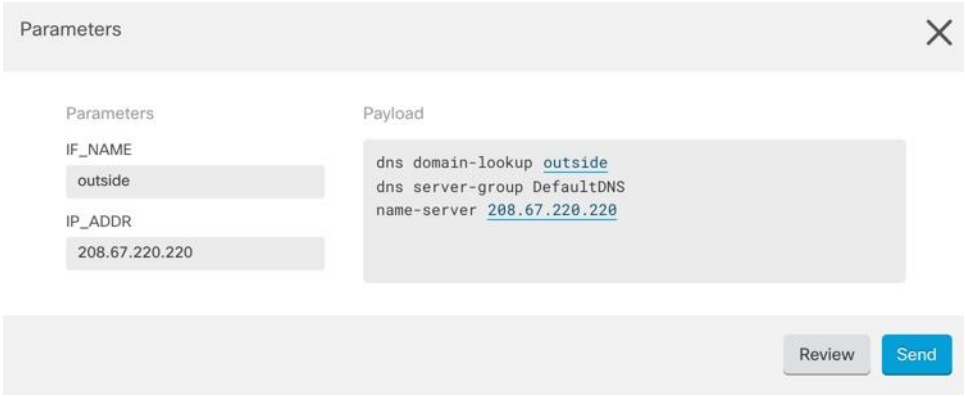
步骤 5 在命令面板中，点击星号。

步骤 6 从命令面板中选择 CLI 宏。

步骤 7 使用以下两种方式之一运行宏：

- 如果宏没有要定义的参数，请点击**发送 (Send)**。命令的响应显示在响应窗格中。就行了。
- 如果宏包含参数，例如下面的配置 DNS 宏，请点击 **>_ 查看参数**。

步骤 8 在“参数”(Parameters) 窗格中，在“参数”(Parameters) 字段中填写参数的值。



步骤 9 点击 **Send**。在 CDO 成功发送命令并更新设备配置后，您会收到消息完成！

- 对于 FTD，会更新设备的活动配置。

步骤 10 发送命令后，您可能会看到消息“某些命令可能已对运行配置进行了更改”(Some commands may have made changes to the running config) 以及两个链接。

- 点击**写入磁盘 (Write to Disk)** 会将此命令所做的更改以及运行配置中的任何其他更改保存到设备的启动配置中。
- 点击**消除 (Dismiss)**，可关闭消息。

编辑 CLI 宏

您可以编辑用户定义的 CLI 宏，但不能编辑系统定义的宏。编辑 CLI 宏会更改所有 FTD 设备。宏并非特定于特定设备。

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。
步骤 2 点击**设备**选项卡。
步骤 3 点击适当的设备类型选项卡。
步骤 4 请选择您的设备。
步骤 5 点击 **命令行接口 (Command Line Interface)**。
步骤 6 选择要编辑的用户定义的宏。
步骤 7 点击宏标签中的编辑图标。
步骤 8 在编辑宏对话框中编辑 CLI 宏。
步骤 9 点击**保存 (Save)**。

有关如何运行 CLI 宏的说明，请参阅运行 CLI 宏。

删除 CLI 宏

您可以删除用户定义的 CLI 宏，但不能删除系统定义的宏。删除 CLI 宏会删除所有设备的宏。宏并非特定于特定设备。

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 请选择您的设备。

步骤 5 点击 >_**命令行接口 (Command Line Interface)**。

步骤 6 选择要删除的用户定义的 CLI 宏。

步骤 7 点击 CLI 宏标签中的垃圾桶图标 。

步骤 8 确认要删除 CLI 宏。

命令行接口文档

CDO 部分支持 FDM 管理 设备的命令行界面。我们在 CDO 中提供类似终端的接口，供用户以命令和响应形式同时向单个设备和多个设备发送命令。对于 CDO 中不支持的命令，请使用设备 GUI 终端（例如 PuTTy 或 SSH 客户端）访问设备，并参阅 CLI 文档以了解更多命令。

导出 CLI 命令结果

您可以将向独立设备或多个设备发出的CLI命令结果导出为逗号分隔值（.csv）文件，以便您可以随意过滤和排序其中的信息。您可以导出单个设备或多个设备的CLI结果。导出的信息包含以下内容：

- 设备
- 日期
- 用户
- 命令
- 输出

导出 CLI 命令结果

您可以将刚刚在命令窗口中执行的命令的结果导出到 .csv 文件：

Procedure

步骤 1 在导航栏中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备，使其突出显示。

步骤 5 在设备的**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。

步骤 6 在命令行界面窗格中，输入命令并点击发送以向设备发出命令。

步骤 7 在已输入命令的窗口右侧，点击导出图标。

步骤 8 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。读取 .csv 文件上的命令输出时，展开所有单元格以查看命令的所有结果。

导出 CLI 宏的结果

您可以导出已在命令窗口中执行的宏的结果。使用以下程序可将在一台或多台设备上执行的 CLI 宏的结果导出到 .csv 文件：

Procedure

步骤 1 打开 **设备和服务** 页面。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备，使其突出显示。

步骤 5 在设备的**设备操作 (Device Actions)** 窗格中，点击**命令行接口 (Command Line Interface)**。

步骤 6 在 CLI 窗口的左侧窗格中，选择 CLI 宏收藏夹星型。

步骤 7 点击要导出的宏命令。填写任何适当的参数，然后点击发送。

步骤 8 在已输入命令的窗口右侧，点击导出图标。

步骤 9 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。读取 .csv 文件上的命令输出时，展开所有单元格以查看命令的所有结果。

导出 CLI 命令历史记录

使用以下程序将一个或多个设备的 CLI 历史记录导出到 .csv 文件：

Procedure

步骤 1 在导航窗格中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备，使其突出显示。

步骤 5 在设备的“设备操作”(Device Actions) 窗格中，点击**命令行接口 (Command Line Interface)**。

步骤 6 如果历史记录窗格尚未展开，请点击时钟图标将其展开。

步骤 7 在已输入命令的窗口右侧，点击导出图标。

步骤 8 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。读取 .csv 文件上的命令输出时，展开所有单元格以查看命令的所有结果。

相关信息：

- CDO 命令行接口, on page 96
- 从新命令创建 CLI 宏
- 删除 CLI 宏
- 编辑 CLI 宏
- 运行 CLI 宏
- 命令行接口文档
- 批量命令行接口

导出 CLI 宏列表

您只能导出已在命令窗口中执行的宏。使用以下程序将一个或多个设备的 CLI 宏导出到 .csv 文件：

过程

步骤 1 在导航窗格中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备，使其突出显示。

步骤 5 在设备的“设备操作”(Device Actions) 窗格中，点击**>_命令行接口 (>_Command Line Interface)**。

步骤 6 在 CLI 窗口的左侧窗格中，选择 CLI 宏收藏夹星型。

步骤 7 点击要导出的宏命令。填写任何适当的参数，然后点击发送。

步骤 8 在已输入命令的窗口右侧，点击导出图标。

步骤 9 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。

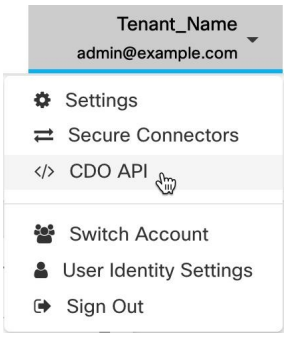
CDO 公共 API

CDO 已发布其公共 API，并为您提供文档、示例和试验场。我们的公共 API 的目标是为您提供一种简单而有效的方法来执行您通常能够在 CDO UI 中执行的许多操作，但在代码中。

要使用此 API，您需要了解 GraphQL。他们的官方指南 () 提供了全面、轻松的阅读。https://graphql.org/learn/

要查找完整的架构文档，请转到 GraphQL Playground，然后点击页面右侧的“文档”选项卡。https://edge.staging.cdo.cisco.com/api-explorer/playground-samples

您可以通过从用户菜单中选择来启动 CDO 公共 API。



创建 REST API 宏

使用 API 工具

CDO 提供 API 工具接口来执行 FDM 管理 设备具象状态传输 (REST) 应用编程 (API) 请求，以便在 FDM 管理 设备上执行高级操作。REST API 使用 JavaScript 对象表示法 (JSON) 格式表示对象。

该接口提供系统定义或用户定义的 API 宏。系统定义的宏由 CDO 提供，无法编辑或删除。用户定义的宏由您创建，可以编辑或删除。您可以使用 Firepower 设备管理器 API Explorer 中支持的所有资源组。

Note CDO 仅支持返回 JSON 的 API 终端。

假定条件

假设您对编程有基本认识并对 REST API 和 JSON 有特定理解。如果您不熟悉这些技术，请首先阅读有关 REST API 的一般指南。

受支持的文档

- 有关详细信息，请参阅《思科 Firepower 威胁防御 REST API 指南》。
- 您还可以在 思科 DevNet 站点上找到参考信息和示例。

支持的 HTTP 方法

仅可使用以下 HTTP 方法。

Important 具有思科防御协调器中的用户角色角色的用户只能执行 GET 操作。

Attribute	说明
GET	从设备读取数据。
POST	为某种资源创建新对象。例如，使用 POST 方法创建新的网络对象。
PUT	更改现有资源的属性。使用 PUT 时，必须包含整个 JSON 对象。无法选择性地更新对象内的个别属性。例如，使用 PUT 方法修改现有网络对象中包含的地址。
DELETE	删除您或其他用户创建的资源。例如，使用 DELETE 方法删除您不再使用的网络对象。

相关信息：

- 如何输入 Secure Firewall Threat Defense REST API 请求
- 关于 FTD REST API 宏
  - 创建 REST API 宏
  - 运行 REST API 宏
  - 编辑 REST API 宏
  - 删除 REST API 宏

如何输入 Secure Firewall Threat Defense REST API 请求

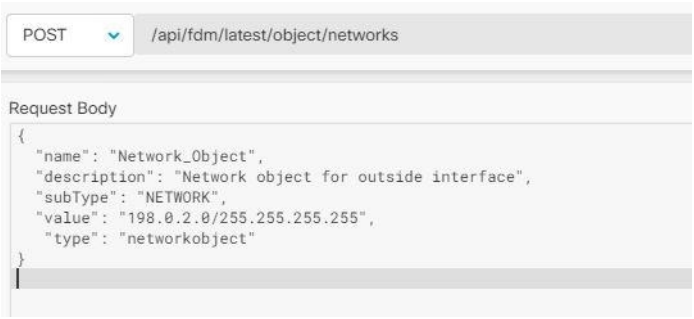
您可以选择 FDM 管理 设备并指定单个命令或执行需要其他参数的命令。

如果要确定 REST API 请求的语法，请登录到设备的 API Explorer 页面，例如 https://ftd.example.com/#/api-explorer，然后点击所需的资源组以查看要执行的命令的语法。例如，https://10.10.5.84/#/api-explorer。

下图显示了 思科防御协调器 中的单个 REST API 请求的示例：

下图显示需要其他参数的 REST API 请求示例。您需要在**请求正文 (Request Body)** 中手动指定数据。如果要确定命令的语法，请登录设备的 API Explorer 页面。

Note 设备必须处于同步状态才能执行 POST 请求。



Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择要使用 REST API 管理的 FDM 管理 设备，然后在右侧的**设备操作 (Device Actions)** 中，点击 **API 工具 (API Tool)**。

步骤 5 从下拉列表中选择请求方法，然后键入**/api/fdm/latest/**，然后键入要执行的命令。如果要执行 POST 或 PUT 命令，请输入请求正文。

步骤 6 点击 **Send**。**响应正文 (Response Body)** 会显示已执行命令的响应。

Important POST 请求通常会更改设备上的暂存配置。点击**在 FDM 中提交更改 (Commit Changes in FDM)**，将更改发送到 FDM 管理 设备。

相关信息：

- 使用 API 工具, on page 544
- 关于 FTD REST API 宏
  - 创建 REST API 宏
  - 运行 REST API 宏
  - 编辑 REST API 宏
  - 删除 REST API 宏

关于 FTD REST API 宏

REST API 宏是可以使用的完全格式的 REST API 命令，或者是可以在运行之前修改的 REST API 命令的模板。所有 REST API 宏都可以在一个或多个 FTD 设备上同时运行。

使用类似于模板的 REST API 宏同时在多个设备上运行相同的命令。REST API 宏可提高设备配置和管理的一致性。使用完全格式的 REST API 宏获取有关设备的信息。您可以立即在 FTD 设备上使用不同的 REST API 宏。

您可以为经常执行的任务创建 REST API 宏。有关详细信息，请参阅创建 REST API 宏。

REST API 宏是系统定义的或用户定义的。系统定义的宏由 CDO 提供，无法编辑或删除。用户定义的宏由您创建，可以编辑或删除。

Note 只有在设备载入 CDO 后，才能为设备创建宏。

相关信息：

- 创建 REST API 宏
- 运行 REST API 宏
- 编辑 REST API 宏
- 删除 REST API 宏

创建 REST API 宏

从新命令创建 REST API 宏

Procedure

步骤 1 在创建 REST API 宏之前，请在 CDO 的 REST API 接口中测试命令，以便确保命令语法正确并返回可靠的结果。

Note 只有在设备载入 CDO 后，才能为设备创建宏。

步骤 2 选择要使用 REST API 管理的 FTD 设备，然后在右侧的**设备操作 (Device Actions)**中，点击 **API 工具 (API Tool)**。

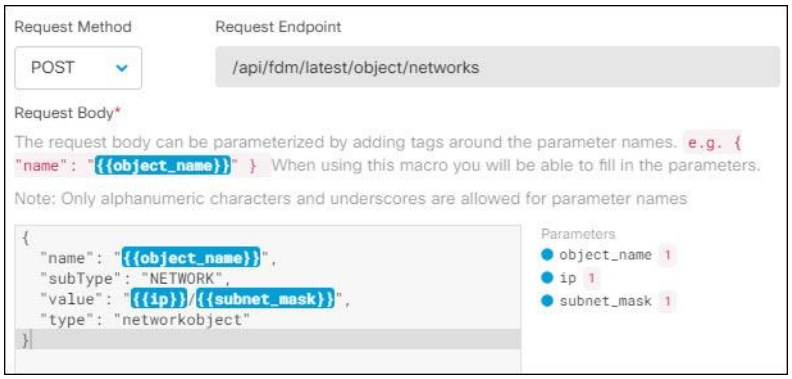
步骤 3 点击 REST API 宏收藏夹星标 ★，以查看已经存在的宏。

步骤 4 点击加号按钮 +。

步骤 5 请为宏指定唯一的名称。如果需要，请为 REST API 宏提供说明和注释。

步骤 6 选择**请求方法 (Request Method)**，然后在**请求终端 (Request Endpoint)** 字段中输入终端 URL。有关详细信息，请参阅《思科 Firepower 威胁防御 REST API 指南》。

步骤 7 运行命令时，将要修改的命令部分替换为用大括号括起来的参数名称。



步骤 8 点击**确定 (OK)**。您创建的宏可用于该类型的所有设备，而不只是您最初指定的设备。

要运行命令，请参阅运行 REST API 宏。

从历史记录或现有 REST API 宏创建 REST API 宏

在此程序中，您将从已执行的命令、另一个用户定义的 REST API 宏或从系统定义的宏创建用户定义的宏。

Procedure

步骤 1 选择要使用 REST API 管理的 FDM 管理 设备，然后在右侧的**设备操作 (Device Actions)** 中，点击 **API 工具 (API Tool)**。

Note 如果要从 REST API 历史记录创建用户定义的宏，请选择运行命令的设备。REST API 宏会在同一账户上的设备之间共享，但不会共享 REST API 历史记录。

步骤 2 查找要生成 REST API 宏的命令，然后选择该命令。使用以下方法之一：

- 点击时钟可查看您在该设备上运行的命令。双击选择要转换为宏的命令，命令将显示在命令窗格中。

- 点击 API 宏收藏夹星标 ★，以查看已经存在的宏。选择要更改的用户定义或系统定义的 API 宏。命令显示在命令窗格中。

步骤 3 使用命令窗格中的命令，点击 API 宏金色星标 ★。命令现在是新 API 宏的基础。

步骤 4 请为宏指定唯一的名称。如果需要，请为 API 宏提供说明和注释。

步骤 5 查看命令字段中的命令，并进行所需的更改。

步骤 6 运行命令时，将要修改的命令部分替换为用大括号括起来的参数名称。

步骤 7 点击**创建**。您创建的宏可用于该类型的所有设备，而不只是您最初指定的设备。

要运行命令，请参阅运行 REST API 宏。

相关信息：

关于 FTD REST API 宏

运行 REST API 宏

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

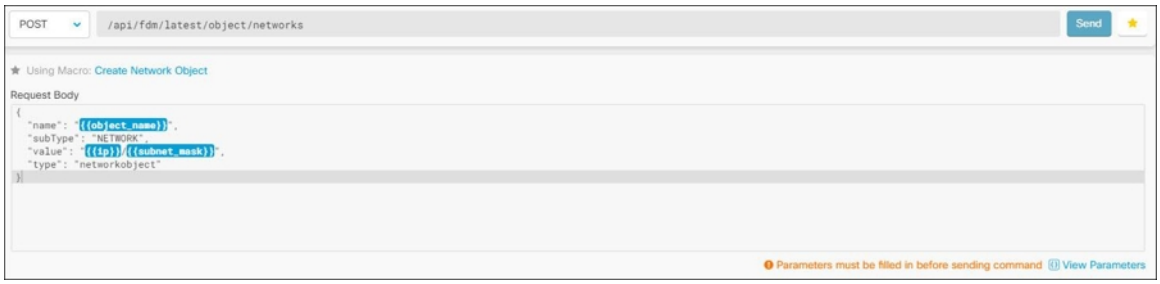
步骤 4 点击右侧**设备操作 (Device Actions)** 窗格中的 **API 工具 (API Tool)** 。

步骤 5 在命令面板中，点击星号 ★ 查看 REST API 宏。

步骤 6 从命令面板中选择 REST API 宏。

步骤 7 使用以下两种方式之一运行宏：

- 如果宏没有要定义的参数，请点击**发送 (Send)**。命令的响应显示在响应窗格中。就行了。
- 如果宏包含参数，例如下面的“创建网络对象”(Create Network Object) 宏，请点击**查看参数 (View Parameters)**。



步骤 8 在**参数 (Parameters)** 窗格中，在“参数”(Parameters) 字段中填写参数的值。

步骤 9 点击 **Send**。

Note FTD 设备的活动配置已更新。

相关信息：

关于 FTD REST API 宏

编辑 REST API 宏

您可以编辑用户定义的 REST API 宏，但不能编辑系统定义的宏。编辑 REST API 宏会更改所有 FDM 管理 设备的宏。宏并非特定于特定设备。

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择要使用 REST API 管理的 FDM 管理 设备，然后在右侧的**设备操作 (Device Actions)** 中，点击 **API 工具 (API Tool)**。

步骤 5 选择要编辑的用户定义的宏。

步骤 6 点击宏标签中的编辑图标。

步骤 7 在编辑宏对话框中编辑 REST API 宏。

步骤 8 点击**保存 (Save)**。

有关如何运行 REST API 宏的说明，请参阅运行 REST API 宏。

相关信息：

关于 FTD REST API 宏

删除 REST API 宏

您可以删除用户定义的 REST API 宏，但不能删除系统定义的宏。删除 REST API 宏会删除所有设备的宏。宏并非特定于特定设备。

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择一个设备，然后在右侧的**设备操作 (Device Actions)** 中，点击 **API 工具 (API Tool)**。

步骤 5 选择要删除的用户定义的 REST API 宏。

步骤 6 点击 REST API 宏标签中的垃圾桶图标 。

步骤 7 确认要删除 REST API 宏。

相关信息：

关于 FTD REST API 宏

读取、丢弃、检查和部署更改

为了管理设备，CDO 必须在其本地数据库中存储自己的设备配置副本。当CDO从其管理的设备“读取”配置时，它会获取设备配置的副本并将其保存。CDO 首次在设备载入时读取并保存设备配置的副本。这些选项描述了出于不同目的而读取配置：

- 当设备的配置状态为“未同步”(Not Synced) 时，可以使用**放弃更改 (Discard Changes)**。在“未同步”状态下，CDO 上的设备配置有待更改。此选项允许您撤消所有待处理的更改。待处理的更改将被删除，并且 CDO 会使用设备上存储的配置副本覆盖其配置副本。
- **检查更改**。如果设备的配置状态为“已同步”(Synced)，则此操作可用。点击“检查更改”(Checking for Changes) 会指示 CDO 将其设备配置副本与设备上存储的配置副本进行比较。如果存在差异，CDO 会立即使用设备上存储的副本覆盖其设备配置副本。
- **审核冲突**并**接受而不审核**。。如果您在设备上启用了冲突检测 (Conflict Detection)，CDO 会每 10 分钟检查一次设备上的配置更改。如果设备上存储的配置副本已更改，CDO 会通过显示“检测到冲突“配置状态来通知您。
  - **查看冲突**。点击查看冲突，您可以查看直接在设备上进行的更改，并接受或拒绝这些更改。
  - **接受而不审核**。此操作会使用设备上存储的最新配置副本来覆盖设备配置的CDO副本。在执行覆盖操作之前，CDO 不会提示您确认配置的两个副本中的差异。

读取所有是一个批处理操作。您可以选择任何状态的多个设备，然后点击**读取全部 (Read All)**，以使用设备上存储的配置覆盖 CDO 上存储的所有设备的配置。

部署更改

当您更改设备的配置时，CDO会将您所做的更改保存到自己的配置副本中。在将这些更改部署到设备之前，这些更改在CDO上“待处理”。当设备的配置发生更改但尚未部署到设备时，该设备将处于“未同步”配置状态。

待处理的配置更改对通过设备运行的网络流量没有影响。只有在CDO将更改部署到设备后，它们才会生效。当CDO将更改部署到设备的配置时，它只会覆盖已更改的配置元素。它不会覆盖设备上存储的整个配置文件。可以为单个设备或同时在多个设备上启动部署。

注释 您可以安排部署或定期部署。有关详细信息，请参阅计划自动部署，第 559 页。

丢弃全部 (Discard All) 选项仅在您点击**预览并部署...(Preview and Deploy...)**。点击“预览并部署”(Preview and Deploy) 后，CDO 会向您显示 CDO 中待处理更改的预览。点击**丢弃全部 (Discard All)** 会从 CDO 中删除所有待处理的更改，并且不会将任何内容部署到所选设备。与上面的“放弃更改”(Discard Changes) 不同，删除待处理的更改是操作的结束。

读取所有设备配置

如果在 Cisco Defense Orchestrator (CDO) 之外对设备进行配置更改，则存储在 CDO 上的设备配置与其配置的本地副本将不再相同。您可能希望使用设备上存储的配置覆盖CDO的设备配置副本，以使配置再次相同。您可以使用**全部读取 (Read All)** 链接在多台设备上同时执行此任务。

有关 CDO 如何管理设备配置的两个副本的详细信息，请参阅读取、丢弃、检查和部署更改。

以下是三种配置状态，其中点击**全部读取 (Read All)** 将使用设备的配置副本覆盖 CDO 的设备配置副本。

- **检测到冲突 (Conflict Detected)** - 如果启用冲突检测，CDO 将每 10 分钟轮询一次其管理的设备，以了解对其配置所做的更改。如果 CDO 发现设备上的配置已更改，则 CDO 会显示设备的“检测到冲突”(Conflict detected) 配置状态。
- **已同步 (Synced)** - 如果设备处于同步状态，并且您点击**全部读取 (Read All)**，CDO 会立即检查设备以确定是否直接对其配置进行了任何更改。点击**读取全部 (Read All)** 后，CDO 会确认您是否打算覆盖其设备配置副本，然后 CDO 会执行覆盖。
- **未同步 (Not Synced)** - 如果设备处于未同步状态，并且您点击**全部读取 (Read All)**，则 CDO 会警告您使用CDO对设备的配置进行了待处理的更改，并且继续执行读取操作将删除这些更改，然后覆盖CDO 的配置副本以及设备上的配置。此读取所有功能，例如放弃更改。

Procedure

步骤 1 从导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 （可选）创建更改请求管理以便在更改日志中轻松识别此批量操作的结果。

步骤 5 选择要保存 CDO 配置的设备。请注意，CDO 仅提供可应用于所有选定设备的操作的命令按钮。

步骤 6 点击**全部读取 (Read All)**。

步骤 7 如果您选择的任何设备的 CDO 上有配置更改，CDO 会发出警告，并询问您是否要继续执行批量读取配置操作。点击**全部读取 (Read All)** 以继续。

步骤 8 查看作业页面以了解“全部读取”(Read All) 配置操作的进度。如果您想了解有关批量操作中各个操作是如何成功或失败的更多信息，请点击蓝色查看链接，您将被定向到作业页面 页面。

步骤 9 如果您创建并激活了更改请求标签，请记住将其清除，以免无意中将其他配置更改与此事件关联。

相关信息

- 读取、丢弃、检查和部署更改
- 放弃更改
- 检查配置更改

将配置更改从 FDM 管理 设备读取到 CDO

为什么 Cisco Defense Orchestrator 会读取设备配置？FDM 管理

为了管理 FDM 管理 设备，CDO 必须拥有自己存储的 FDM 管理 设备配置文件副本。当 CDO 从 FDM 管理 设备读取配置时，它会获取 FDM 管理 设备已部署的配置副本并将其保存到自己的数据库中。CDO 首次读取并保存设备配置文件的副本是在设备载入时。有关详细信息，请参阅读取、丢弃、检查和部署更改。

待处理和已部署的更改

直接通过 Firepower 设备管理器 (FDM) 或其 CLI 对设备进行的配置更改在部署之前称为设备上的暂存更改。FDM 管理FDM 管理可以编辑或删已暂存或除待处理的更改，而不会影响通过 FDM 管理设备的流量。但是，部署待处理的更改后，它们会由 FDM 管理 设备实施并影响通过设备的流量。

检测到冲突

如果您在设备上启用冲突检测，则 CDO 会每 10 分钟检查一次配置更改。如果设备上存储的配置副本已更改，CDO 会通过显示“检测到冲突“(Conflict Detected) 配置状态来通知您。如果您未启用冲突检测，或者在自动轮询之间的 10 分钟间隔内对设备的配置进行了更改，则点击检查更改会提示 CDO 立即比较设备上的配置副本与配置存储在 CDO 上。您可以选择查看冲突以检查设备配置与保存到 CDO 的配置之间的差异，然后选择放弃更改以删除暂存的更改并恢复为已保存的配置或确认更改。您也可以选择接受而不审核；此选项会获取配置并覆盖当前保存到 CDO 的内容。

放弃更改程序

要丢弃设备的配置更改，请执行以下程序：FDM 管理

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择其配置设置为检测到冲突的设备，并为您提供恢复待处理更改的链接。该消息说明您可以点击链接恢复待处理的更改，也可以使用本地管理器FDM登录设备并首先部署更改。您可以使用过滤器查找处于冲突状态的设备。过滤器, on page 90

Caution 点击恢复待处理更改链接会立即删除设备上的待处理更改。FDM管理您没有机会先查看更改。

步骤 5 在点击恢复待处理更改之前，查看 FDM 上的更改：

a. 打开浏览器窗口并输入 https://< IP_address_of_the_FTD >。

b. 在 FDM 中查找部署图标。系统将显示一个橙色圆圈，表示有可供部署的更改。 

c. 点击 图标并查看待处理的更改：

- 如果可以删除更改，请返回 CDO 并点击“恢复待处理更改”。此时，设备上的配置和 CDO 上的配置副本应该相同。FDM 管理大功告成。
- 如果要将更改部署到设备，请点击立即部署。现在，设备上已部署的配置与CDO上存储的配置不同。FDM 管理然后，您可以返回到 CDO 并轮询设备以进行更改。检查配置更改, on page 561CDO 标识设备上已发生更改，并为您提供查看冲突的机会。FDM 管理请参阅检测到冲突 - 查看冲突以解决该状态。冲突检测, on page 563

如果恢复待处理更改失败

CDO 无法恢复对系统数据库和安全源所做的更改。CDO 识别出有待处理的更改，尝试将其恢复，然后失败。要确定恢复失败的原因是数据库更新还是安全源更新，请登录设备的FDM控制台。系统将显示一个橙色圆圈，表示有可供部署的更改。  点击部署按钮以查看待处理的更改，并根据需要部署或丢弃它们。

审核冲突程序

要从设备查看配置更改，请执行以下程序：FDM 管理

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择配置标记为“检测到冲突”的设备，并在右侧的“检测到的冲突”窗格中提供查看冲突的链接。

步骤 5 点击**查看冲突 (Review Conflict)**。

步骤 6 比较呈现给您的两种配置。

步骤 7 采取下列操作之一：

- 点击接受，用设备上找到的配置覆盖 CDO 上的最后一个已知配置。注意：存储在 CDO 上的整个配置将被设备上的配置完全覆盖。
- 点击拒绝以拒绝在设备上进行的更改，并将其替换为 CDO 上的最后一个已知配置。
- 点击**取消 (Cancel)** 以停止操作。

Note 当设备处于同步状态时，您可以通过点击检查更改来提示 CDO 立即检查设备的带外更改。检查配置更改, on page 561

接受而不审核程序

要接受设备的配置更改而不进行审核，请执行以下程序：FDM 管理

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择配置标记为“检测到冲突”(Conflict Detected) 的设备，并在右侧的“检测到冲突”(Conflict Detected) 窗格中显示接受而不审核的链接。

步骤 5 点击**接受而不审核 (Accept Without Review)**。CDO 接受并覆盖当前配置。

相关信息：

- 读取、丢弃、检查和部署更改
- 冲突检测
- 放弃更改

预览和部署所有设备的配置更改

当您对租户上的设备进行了配置更改，但您尚未部署该更改时，CDO 会通过在部署图标上显示一个橙色点来通知您

。受这些更改影响的设备在设备和**服务 (Services)** 页面中显示“未同步”(Not Synced) 状态。通过点击**部署 (Deploy)**，您可以查看哪些设备具有待处理的更改，并将更改部署到这些设备。

此部署方法适用于所有受支持的设备。

您可以将此部署方法用于单个配置更改，也可以等待并一次部署多个更改。

过程

步骤 1 在屏幕的右上角，点击**部署 (Deploy)** 图标  。

步骤 2 选择要部署更改的设备。如果设备有黄色警告三角形，则无法将更改部署到该设备。将鼠标悬停在黄色警告三角形上，了解无法将更改部署到该设备的原因。

步骤 3 选择设备后，您可以在右侧面板中将其展开并预览其特定更改。

步骤 4 （可选）如果要查看有关待处理更改的更多信息，请点击**查看详细更改日志 (View Detailed Changelog)** 链接以打开与该更改关联的更改日志。点击**部署 (Deploy)** 图标可返回**具有待处理更改的设备 (Devices with Pending Changes)** 页面。

步骤 5 （可选）更改请求管理以跟踪更改，而无需离开**具有待处理更改的设备 (Devices with Pending Changes)** 页面。

步骤 6 点击**立即部署 (Deploy Now)**，立即将更改部署到您选择的设备。您将在“作业”(Jobs) 托盘的“活动作业”(Active jobs) 指示器中看到进度。

步骤 7 （可选）部署完成后，点击 CDO 导航栏中的**作业 (Jobs)**。您将看到最近的“部署更改”(Deploy Changes) 作业，其中显示了部署的结果。

步骤 8 如果您创建了更改请求标签，并且没有其他配置更改与之关联，请将其清除。

下一步做什么

- 已计划的自动部署
- 将配置更改从 CDO 部署到 FDM 管理 设备， 第 557 页
- 部署到 FDM 管理 设备后更改日志条目， 第 574 页

将配置更改从 CDO 部署到 FDM 管理 设备

为什么 CDO 会将更改部署到 FDM 管理 设备？

当您使用 CDO 管理和更改设备配置时，CDO 会将您所做的更改保存到自己的配置文件副本中。在部署到设备之前，这些更改将被视为已在 CDO 上暂存。暂存配置更改对通过设备运行的网络流量没有影响。只有在 CDO 将更改部署到设备后，它们才会影响通过设备运行的流量。当 CDO 将更改部署到设备的配置时，它只会覆盖已更改的配置元素。它不会覆盖设备上存储的整个配置文件。

与 CDO 一样，FDM 管理 也有待处理更改和已部署更改的概念。FDM 管理 设备上的待处理更改相当于 CDO 上的分阶段更改。可以编辑或删除待处理的更改，而不会影响通过 FDM 管理 设备的流量。但是，部署待处理的更改后，它们会由 FDM 管理 设备实施并影响通过设备的流量。

由于 FDM 托管设备有两步编辑配置文件，因此 CDO 将更改部署到 FDM 管理 设备的方式与其管理的其他设备略有不同。CDO 首先将更改部署到 FDM 管理 设备，并且更改处于待处理状态。然后，CDO 在设备上部署更改并使其生效。现在，更改已部署，并且会影响通过 FDM 管理 设备运行的流量。这适用于独立设备和高可用性 (HA) 设备。

部署可以为单个设备或同时在多个设备上启动。您可以为单个设备安排单独的部署或定期部署。

有两件事会阻止 CDO 将更改部署到 FDM 管理 设备：

- FDM 管理 设备上是否存在分阶段更改。有关如何解决此状态的详细信息，请参阅冲突检测 。
- 如果部署到 FDM 管理 设备的过程发生更改，CDO 不会部署更改。

计划自动部署

您还可以将租户配置为将部署安排到具有已计划的自动部署的待处理更改。

将更改部署到设备

Procedure

步骤 1 使用 CDO 对设备进行配置更改并保存后，该更改将保存在设备配置的 CDO 实例中。

步骤 2 在导航栏中，点击 **设备和服务**。

步骤 3 点击**设备**选项卡。

步骤 4 点击适当的设备类型选项卡。您应该会看到您所做更改的设备的配置状态现在为“未同步”。

步骤 5 使用以下方法之一部署更改：

- 选择设备，然后在右侧的未同步窗格中，点击预览并部署。 在 Pending Changes 屏幕上，查看更改。如果您对待定版本感到满意，请点击立即部署。成功部署更改后，您可以查看更改日志以确认刚刚发生的情况。变更日志, on page 573

- 点击屏幕右上角的**部署 (Deploy)** 图标  。有关详细信息，请参阅预览和部署所有设备的配置更改, on page 556。

取消更改

如果在将更改从CDO部署到设备时，点击取消，则所做的更改不会部署到设备。进程被取消。您所做的更改在 CDO 上仍处于待处理状态，可以在最终将其部署到设备之前进行进一步编辑。FDM 管理

放弃更改

如果在预览更改时点击**全部弃用 (Discard all)**，则您所做的更改以及任何其他用户所做但未部署到设备的任何其他更改都将被删除。在进行任何更改之前，CDO将其待处理配置恢复为上次读取或部署的配置。

批量部署设备配置

如果您对多个设备进行了更改（例如通过编辑共享对象），则可以一次将这些更改应用到所有受影响的设备：

Procedure

步骤 1 在导航窗格中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择已在 CDO 上进行配置更改的所有设备。这些设备应显示“未同步”(Not Synced) 状态。

步骤 5 使用以下方法之一部署更改：

- 点击屏幕右上角的**部署 (Deploy)** 按钮  。这使您有机会在部署之前查看所选设备上的待处理更改。点击**立即部署 (Deploy Now)** 以部署更改。

  Note 如果在**有待处理更改的设备 (Devices with Pending Changes)** 屏幕上看到某个设备旁边显示黄色警告三角形，则无法将更改部署到该设备。将鼠标悬停在警告三角形上，了解有关无法将更改部署到该设备的信息。

- 点击详细信息窗格中的**全部部署 (Deploy All)** 。查看所有警告，然后点击**确定 (OK)**。批量部署会立即开始，无需审核更改。

步骤 6 （可选）点击导航栏中的“作业”(Jobs) 图标  以查看批量部署的结果。

相关信息：

- 计划自动部署, on page 559

已计划的自动部署

通过使用CDO，您可以对其管理的一个或多个设备进行配置更改，然后安排在您方便的时间将更改部署到这些设备。

只有您在“设置”(Settings) 页面的**租户设置 (Tenant Settings)** 选项卡中 启用计划自动部署的选项, on page 46 才能安排部署。一旦启用此选项，您就可以创建、编辑或删除计划部署。计划的部署会在设置的日期和时间部署在 CDO 上保存的所有暂存更改。您还可以在“作业”(Jobs) 页面中查看和删除计划部署。

如果直接对设备进行了尚未读取、丢弃、检查和部署更改到CDO的更改，则将跳过计划的部署，直到该冲突得以解决。“作业”(Jobs) 页面将列出计划部署失败的所有实例。如果**启用计划自动部署的选项 (Enable the Option to Schedule Automatic Deployments)** 被关闭，则所有计划的部署都将被删除。

Caution 如果您为多台设备安排新的部署，并且其中一些设备已安排了部署，则新的安排部署将覆盖现有的安排部署。

Note 当您创建计划部署时，将按照本地时间来创建计划，而不是设备的时区。计划的部署不会自动调整夏令时。

计划自动部署

部署计划可以是单个事件或周期性事件。您可能会发现定期自动部署是一种将定期部署与维护窗口对齐的便捷方式。请按照以下程序为单个设备安排一次性或周期性部署：

Note 如果为已安排现有部署的设备安排部署，新的安排部署将覆盖现有部署。

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备。

步骤 5 在设备详细信息窗格中，找到计划的部署选项卡，然后点击**计划 (Schedule)**。

步骤 6 选择应进行部署的时间。

- 对于一次性部署，请点击**一旦开启 (Once on)** 选项以从日历中选择日期和时间。
- 对于周期性部署，请点击**每次 (Every)** 选项。您可以选择每天或每周一次部署。选择部署的**日期 (Day)** 和**时间 (Time)**。

步骤 7 点击**保存 (Save)**。

编辑计划部署

请按照以下程序编辑计划部署：

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备。

步骤 5 在**设备详细信息 (Device Details)** 窗格中，找到计划的部署选项卡，然后点击**编辑 (Edit)**。

步骤 6 编辑计划部署的重复周期、日期或时间。

步骤 7 点击**保存 (Save)**。

删除计划部署

请按照以下程序删除计划部署：

Note 如果为多台设备安排部署，然后更改或删除某些设备的安排，则其余设备的原始安排部署将保留。

Procedure

步骤 1 在导航栏中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备。

步骤 5 在**设备详细信息 (Device Details)** 窗格中，找到计划的部署选项卡，然后点击**删除 (Delete)** 。

What to do next

- 读取、丢弃、检查和部署更改
- 读取所有设备配置, on page 552
- 将配置更改从 CDO 部署到 FDM 管理 设备, on page 557
- 预览和部署所有设备的配置更改, on page 556

检查配置更改

检查更改以确定设备的配置是否已直接在设备上更改，并且它不再与CDO上存储的配置副本相同。当设备处于“已同步”(Synced) 状态时，您将看到此选项。

要检查更改，请执行以下操作：

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择您怀疑其配置可能已直接在设备上更改的设备。

步骤 5 点击右侧“已同步”(Synced) 窗格中的**检查更改 (Check for Changes)**。

步骤 6 以下行为因设备而有细微差别：

- 对于 FTD 设备，如果设备的配置发生变化，您将收到以下消息：

  从设备读取策略。如果设备上有活动的部署，则将在完成后开始读取。

  - 点击 **OK** 继续操作。设备上的配置将覆盖 CDO 上存储的配置。
  - 点击**取消 (Cancel)** 以取消操作。

- 对于 设备：

a. 比较呈现给您的两种配置。点击**继续**。标记为**最后已知的设备配置 (Last Known Device Configuration)** 的配置是存储在 CDO 上的配置。标记为**在设备上找到 (Found on Device)** 的配置是保存在 ASA上的配置。

b. 选择以下选项中的一种：

   1. **拒绝**带外更改以保留“最后已知的设备配置”(Last Known Device Configuration)。
   2. **接受**带外更改，以使用设备上找到的配置来覆盖 CDO 中存储的设备配置。

c. 点击**继续**。

放弃更改

如果要“撤消”使用 CDO 对设备配置所做的所有未部署的配置更改，请点击**放弃更改 (Discard Changes)**。在点击**放弃更改 (Discard Changes)** 时，CDO 会使用设备上存储的配置完全覆盖设备配置的本地副本。

点击**放弃更改 (Discard Changes)** 时，设备的配置状态为**未同步 (Not Synced)**。在放弃更改后，CDO 上的配置副本将与设备上的配置副本相同，CDO 中的配置状态将恢复为“已同步”(Synced)。

要放弃或“撤消”设备的所有未部署的配置更改，请执行以下操作：

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择您已对其进行配置更改的设备。

步骤 5 点击右侧未同步窗格中的**放弃更改 (Discard Changes)**。

- 对于 FDM 管理 设备，CDO 会警告您“CDO 上的待处理更改将被丢弃，此设备的 CDO 配置将替换为设备上当前运行的配置”(Pending changes on CDO will be discarded and the CDO configuration for this device will be replaced with the configuration currently running on the device)。点击**继续 (Continue)** 以放弃更改。
- 对于 Meraki 设备 - CDO 会立即删除更改。
- 对于 AWS 设备 - CDO 会显示您要删除的内容。点击**接受 (Accept)** 或**取消 (Cancel)**。

设备上的带外更改

带外更改是指在不使用 CDO 的情况下直接在设备上进行的更改。可以使用设备的命令行界面通过 SSH 连接进行这些更改，也可以使用本地管理器（例如适用于 ASA 的自适应安全设备管理器 (ASDM) 或适用于 FDM 管理 设备的 FDM）进行这些更改。带外更改会导致 CDO 上存储的设备配置与设备本身上存储的配置之间发生冲突。

检测设备上的带外更改

如果为 ASA、FDM 管理 设备或 Cisco IOS 设备启用了冲突检测，CDO 会每 10 分钟检查一次设备，以搜索在 CDO 之外直接对设备配置进行的任何新更改。

如果 CDO 发现未存储在 CDO 上的设备配置更改，则会将该设备的**配置状态**更改为“检测到冲突”状态。

当 Defense Orchestrator 检测到冲突时，可能出现以下两种情况：

- 直接对设备进行的配置更改尚未保存到 CDO 的数据库中。
- 对于 FDM 管理 设备，FDM 管理 设备上可能存在尚未部署的“待处理”配置更改。

同步 Defense Orchestrator 和设备之间的配置

关于配置冲突

在“设备和服务”页面上，您可能会看到设备或服务的状态为“已同步”(Synced)、“未同步”(Not Synced) 或“检测到冲突”(Conflict Detected)。

- 如果设备为**已同步 (Synced)**， Cisco Defense Orchestrator (CDO) 上的配置与设备本地存储的配置相同。
- 如果设备为**未同步 (Not Synced)**，CDO 中存储的配置已更改，现在存储在设备上的配置有所不同。将您的更改从 CDO 部署到设备会更改设备上的配置以匹配 CDO 的版本。
- 在 CDO 之外对设备进行的更改称为**带外更改**。进行带外更改时，如果为设备启用了冲突检测，您会看到设备状态更改为“检测到冲突”(Conflict Detected)。接受带外更改会更改 CDO 上的配置以匹配设备上的配置。

冲突检测

启用冲突检测后， Cisco Defense Orchestrator (CDO) 将按默认间隔轮询设备，以确定是否在 CDO 之外对设备配置进行了更改。如果 CDO 检测到已进行更改，则会将设备的配置状态更改为**检测到冲突 (Conflict Detected)**。在 CDO 之外对设备进行的更改称为“带外”更改。

启用此选项后，您可以配置每台设备检测冲突或OOB更改的频率。有关详细信息，请参阅安排设备更改轮询, on page 567。

启用冲突检测

启用冲突检测会提醒您在 Defense Orchestrator 之外对设备进行更改。

Procedure

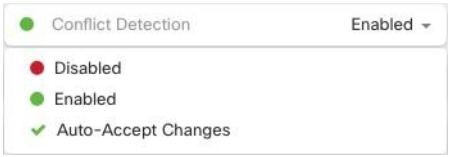
步骤 1 从导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备**选项卡。

步骤 3 选择适当的设备类型选项卡。

步骤 4 选择要启用冲突检测的设备。

步骤 5 在设备表右侧的冲突检测框中，从列表中选择已启用。



自动接受设备的带外更改

您可以通过启用自动接受更改，将 Cisco Defense Orchestrator (CDO) 配置为自动接受直接对受管设备所做的任何更改。不使用 CDO 直接对设备进行的更改称为带外更改。带外更改会在 CDO 上存储的设备配置与设备本身上存储的配置之间产生冲突。

自动接受更改功能是对冲突检测的增强。如果您在设备上启用了自动接受更改，CDO 会每 10 分钟检查一次更改，以确定是否对设备的配置进行了任何带外更改。如果配置发生更改，CDO会自动更新其本地版本的设备配置，而不会提示您。

如果对 CDO 进行的配置更改尚未部署到设备，则 CDO 不会自动接受配置更改。按照屏幕上的提示确定下一步操作。

要使用自动接受更改，请先启用租户，以在**清单 (Inventory)** 菜单中显示自动接受选项；然后，您可以为单个设备启用自动接受更改。

如果您希望 CDO 检测带外更改，但为您提供手动接受或拒绝更改的选项，请改为启用 冲突检测, on page 563。

配置自动接受更改

Procedure

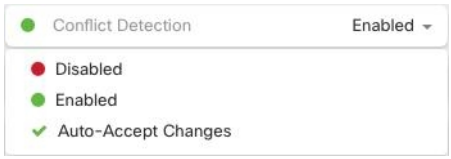
步骤 1 使用具有管理员或超级管理员权限的帐户登录 CDO。

步骤 2 从 CDO 菜单中，导航至 **设置 (Settings)** > **常规设置 (General Settings)**。

步骤 3 在租户设置区域中，点击切换按钮以启用“自动接受设备更改的选项”。这将使“自动接受更改”菜单选项显示在“资产”页面的“冲突检测”菜单中。

步骤 4 打开“资产”页面，然后选择要自动接受带外更改的设备。

步骤 5 在“冲突检测”(Conflict Detection) 菜单中，选择下拉菜单中的“自动接受更改”(Auto-Accept Changes)。



为租户上的所有设备禁用自动接受更改

Procedure

步骤 1 使用具有管理员或超级管理员权限的帐户登录 CDO。

步骤 2 从 CDO 菜单中，导航至 **设置 (Settings)** > **常规设置 (General Settings)**

步骤 3 在“租户设置”区域中，通过将切换开关向左滑动来禁用“启用自动接受设备更改的选项”，使其显示灰色 X。这将禁用“冲突检测”菜单中的“自动接受更改”选项，并为以下项禁用此功能：租户上的每台设备。

Note 禁用“自动接受”将要求您查看每个设备冲突，然后才能将其接受到CDO中。这包括之前配置为自动接受更改的设备。

解决配置冲突

本节提供有关解决设备上发生的配置冲突的信息。

解决“未同步”状态

使用以下程序解决配置状态为“未同步”的设备：

Procedure

步骤 1 在导航栏中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择报告为“未同步”的设备。

步骤 5 在右侧的未同步面板中，选择以下任一选项：

- **预览并部署...** - 如果要将配置更改从 CDO 推送到设备，请预览并部署您现在所做的更改，或者等待并一次部署多个更改。预览和部署所有设备的配置更改, on page 556
- 放弃更改 - 如果您不想将配置更改从 CDO 推送到设备，或者您想要“撤消”您开始在 CDO 上进行的配置更改。此选项使用设备上存储的运行配置覆盖 CDO 中存储的配置。

解决“检测到冲突”状态

CDO 允许您在每个实时设备上启用或禁用冲突检测。如果 冲突检测, on page 563 已启用，并且在未使用 CDO 的情况下对设备的配置进行了更改，则设备的配置状态将显示为**检测到冲突 (Conflict Detected)**。

要解决“检测到冲突”(Conflict Detected) 状态，请执行以下程序：

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择报告冲突的设备，然后点击右侧详细信息窗格中的**查看冲突 (Review Conflict)**。

步骤 5 在**设备同步 (Device Sync)** 页面中，通过查看突出显示的差异来比较两种配置。

- 标记为“最后一次设备配置”(Last Known Device Configuration) 的面板是存储在 CDO 上的设备配置。
- 标记为“在设备上找到”(Found on Device) 的面板是存储在运行 ASA 配置中的配置。

步骤 6 通过选择以下选项之一来解决冲突：

- **接受设备更改 (Accept Device changes)**：这将使用设备的运行配置覆盖 CDO **上存储的配置** 和任何待处理的更改。

  Note 由于 CDO 不支持在命令行界面之外部署对Cisco IOS 设备的更改，因此在解决冲突时，您对Cisco IOS 设备的唯一选择是选择**接受而不查看 (Accept Without Review)**。

- **拒绝设备更改 (Reject Device Changes)**：这将使用存储在 CDO 上的配置覆盖设备上存储的配置。

Note 所有配置更改（拒绝或接受）都记录在更改日志中。

安排设备更改轮询

如果已启用 冲突检测, on page 563 或从“设置”(Settings) 页面 **启用自动接受设备更改的选项 (Enable the option to auto-accept device changes)**，则 CDO 将按默认间隔轮询设备，以确定是否在 CDO 之外对设备配置进行了更改。您可以自定义CDO轮询每台设备更改的频率。这些更改可以应用于多个设备。

如果没有为设备配置选择，则会自动为“租户默认”配置间隔。

Note 从**设备和服务 (Devices & Services)** 页面自定义每台设备的间隔会覆盖从**常规设置 (General Settings)** 页面选择作为默认冲突检测间隔 的轮询间隔。

从**设备和服务 (Devices & Services)** 页面启用**冲突检测 (Conflict Detection)** 或从“设置”(Settings) 页面选择**启用该选项以自动接受设备更改 (Enable the option to auto-accept device changes)** 后，请使用以下程序来安排您希望 CDO 轮询设备的频率：

Procedure

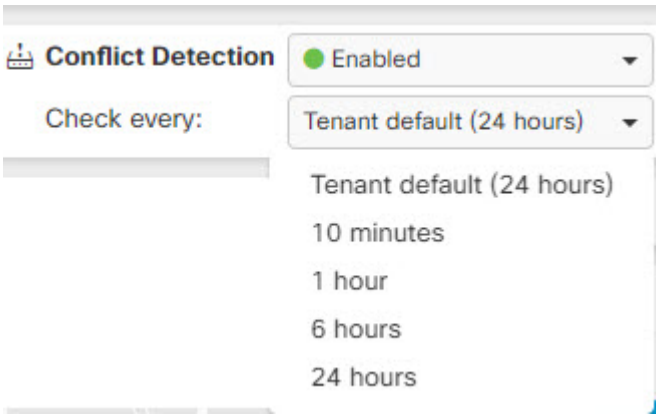
步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击 **设备** 选项卡，找到您的设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择要启用冲突检测的设备。

步骤 5 在与**冲突检测 (Conflict Detection)** 相同的区域中，点击**检查间隔 (Check every)** 下拉菜单，然后选择所需的轮询间隔：



安排安全数据库更新

本节提供有关在设备上安排安全数据库更新的信息。

创建计划安全数据库更新

使用以下程序创建一个计划的任务，以检查和更新 FTD 设备的安全数据库：

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择设备。

步骤 5 在**操作 (Actions)** 窗格中，找到**安全数据库更新 (Security Database Updates)** 部分，然后点击**添加 +** 按钮。

Note 如果所选设备已存在计划任务，请点击编辑图标 以创建新任务。创建新任务将覆盖现有任务。

步骤 6 使用以下内容配置计划任务：

- **频率 (Frequency)**。选择每天、每周或每月进行更新。
- **时间 (Time)**。选择每天的某个时间。请注意，显示的时间为 UTC。
- **选择天数 (Select Days)**。选择您希望在一周内的哪一天进行更新。

步骤 7 点击**保存 (Save)**。

设备的配置状态将更改为“正在更新数据库”(Updating Databases)。

编辑计划安全数据库更新

使用以下程序编辑现有的计划任务，以检查和更新 FTD 设备的安全数据库。

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击 **FTD** 选项卡。

步骤 4 选择设备。

步骤 5 在**操作 (Actions)** 窗格中，找到**安全数据库更新 (Security Database Updates)** 部分，然后点击编辑图标 。

步骤 6 使用以下命令编辑计划任务：

- **频率**。选择每天、每周或每月进行更新。
- **时间 (Time)**。选择每天的某个时间。请注意，显示的时间为 UTC。
- **选择天数 (Select Days)**。选择您希望在一周内的哪一天进行更新。

步骤 7 点击**保存 (Save)**。

步骤 8 设备的配置状态将更改为“正在更新数据库”(Updating Databases)。

更新 FDM 管理 设备安全数据库

通过更新FDM管理 设备上的安全数据库，您将更新以下内容：SRU（入侵规则）、安全情报(SI)、漏洞数据库 (VDB) 以及地理位置数据库。如果您选择通过 思科防御协调器 UI 来更新安全数据库，请注意，**所有**提到的数据库都会更新；您无法选择要更新的数据库。

请注意，安全数据库更新无法恢复。

Note 在更新安全数据库时，某些数据包可能会被丢弃或不经检查通过。我们建议您在维护窗口期间安排安全数据库更新。

载入时更新 FDM 管理 设备安全数据库

当您将 FDM 管理 设备载入 CDO 时，在载入过程中可以**启用计划的数据库定期更新**。默认情况下，会选中此选项。启用后，CDO 会立即检查并应用任何安全更新，并自动安排设备检查是否有额外更新。在设备载入后，您可以修改计划任务的日期和时间。

我们建议在载入过程中启用自动计划程序，以定期检查和应用安全数据库更新。这样，您的设备将始终保持最新状态。要在载入 FDM 管理 设备时更新安全数据库，请参阅使用注册密钥载入 FDM 管理 设备运行软件版本 6.4 或 6.5。

Note 如果使用注册密钥方法载入设备，则**不得**使用智能许可证来注册设备。我们建议注册许可证。作为替代方法，您可以使用设备的使用用户名、密码和 IP 地址载入 FDM 管理 设备来载入设备。

载入后更新 FDM 管理 设备安全数据库

在 FDM 管理 设备被载入 CDO 后，您可以通过安排更新来配置设备，以便检查安全数据库更新。您可以通过选择计划更新的设备来随时修改此计划任务。有关详细信息，请参阅安排安全数据库更新。

工作流程

设备许可证

如果没有许可证，思科防御协调器 将无法更新安全数据库。我们建议您的设备至少具有 Essentials 许可证。FDM 管理

如果您要自行激活没有许可证的设备，这不会阻止CDO 自行激活设备。相反，设备将遇到“许可证不足”的连接状态。要解决此问题，您必须通过 FDM 管理 设备 UI 应用正确的许可证。

Note 如果您载入FDM管理设备并选择计划未来的安全数据库更新，并且设备**没有**注册的许可证，则CDO仍会创建计划任务，但在应用适当的许可证且设备成功同步之前不会触发该任务。

安全数据库更新在 FDM 中待处理

如果您通过 FDM 管理 设备 UI 更新安全数据库，并且您在设备上启用了**冲突检测**，则 CDO 会将待处理的更新检测为冲突。

Note 如果您载入 FDM 管理 设备并选择安排更新，则 CDO 会在下次部署期间自动更新安全数据库以及对已存储配置的任何其他待处理更改。**不必是配置部署**

在安全数据库更新期间，设备具有 OOB 更改或暂存更改

如果为具有带外 (OOB) 更改或尚未部署的暂存更改的 FDM 管理 设备安排安全数据库更新，则 CDO 只会检查和更新安全数据库。CDO 不会部署 OOB 或暂存更改。

设备已有更新安全数据库的计划任务

每台设备只能有一个计划任务。如果设备已有更新安全数据库的计划任务，则创建新任务会覆盖该任务。这适用于在 CDO 或 FDM 管理 设备上创建的任务。

没有可用的安全数据库更新

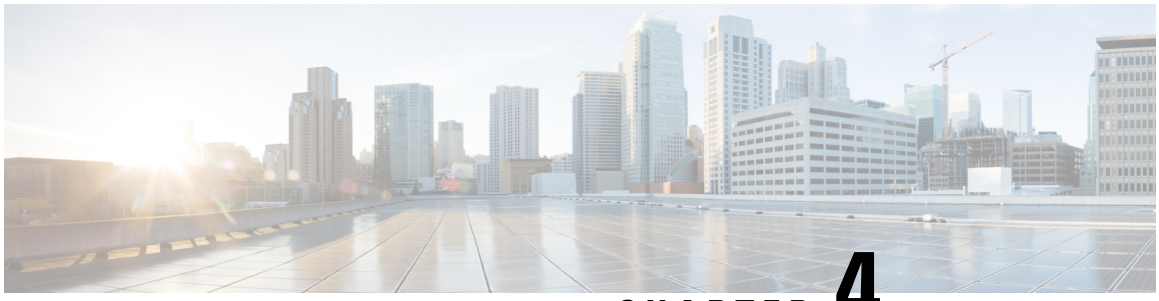
如果没有可用的更新，CDO 不会向设备部署任何内容。

高可用性 (HA) 对的安全数据库更新FDM 管理

安全数据库更新仅应用于 HA 对的主设备。

相关信息：

- 使用注册密钥载入 FDM 管理 设备运行软件版本 6.4 或 6.5
- 使用用户名、密码和 IP 地址载入 FDM 管理 设备, on page 168
- 安排安全数据库更新



CHAPTER 4

监控和报告

CDO 的监控和报告功能可帮助您深入了解现有策略的影响以及由此产生的安全状况。

变更日志

关于更改日志

更改日志 会持续捕获在 CDO 中进行的配置更改。此单一视图包括所有受支持设备和服务的更改。以下是更改日志的一些功能：

- 并排比较对设备配置所做的更改。
- 所有更改日志条目的纯英文标签。
- 记录设备的自行激活和删除。
- 检测在 CDO 之外发生的策略更改冲突。
- 回答事件调查或故障排除期间的人员、内容和时间。
- 可以将完整更改日志或仅一部分下载为 CSV 文件。

更改日志容量

CDO 会将更改日志中的信息保留一年。超过一年的信息将被删除。

CDO 在其数据库中存储的更改日志信息与导出更改日志时看到的信息之间存在差异。有关详细信息，请参阅将更改日志导出到 CSV 文件, on page 576。

“更改日志”(Change Log) 页面上的更改日志条目

更改日志条目反映对单个设备配置的更改、在设备上执行的操作，或者是否在CDO之外对设备进行了更改。

- 对于包含配置更改的更改日志条目，您可以通过点击行中的任意位置来展开更改。
- 对于在 CDO 之外进行的被检测为冲突的带外更改，**系统用户**将被报告为最后一个用户。
- 在CDO 上的设备配置与设备上的配置同步后，或从 CDO 中删除设备时，CDO 会关闭更改日志条目。将配置从设备“读取”到 CDO 或通过将配置从 CDO 部署到设备后，配置会同步。
- CDO在关闭现有条目后立即创建新的更改日志条目。其他配置更改将添加到打开的更改日志条目中。
- 显示针对设备的读取、部署和删除操作的事件。这些操作会关闭设备的更改日志。
- 一旦 CDO 与设备上的配置同步（通过读取或部署），或者当 CDO 不再管理设备时，更改日志就会关闭。
- 如果在 CDO 之外对设备进行了更改，则会在更改日志中写入“检测到冲突”的条目。

活动和已完成的更改日志条目

更改日志的状态为 **活动**或**已完成**。当您使用 CDO 更改设备的配置时，这些更改会记录在**活动**更改日志条目中。将配置从设备读取到CDO、将更改从 CDO 部署到设备、从 CDO 删除设备或运行更新运行配置文件的 CLI 命令都会完成活动更改日志，并为未来的更改创建新的更改日志。

在更改日志中查找条目

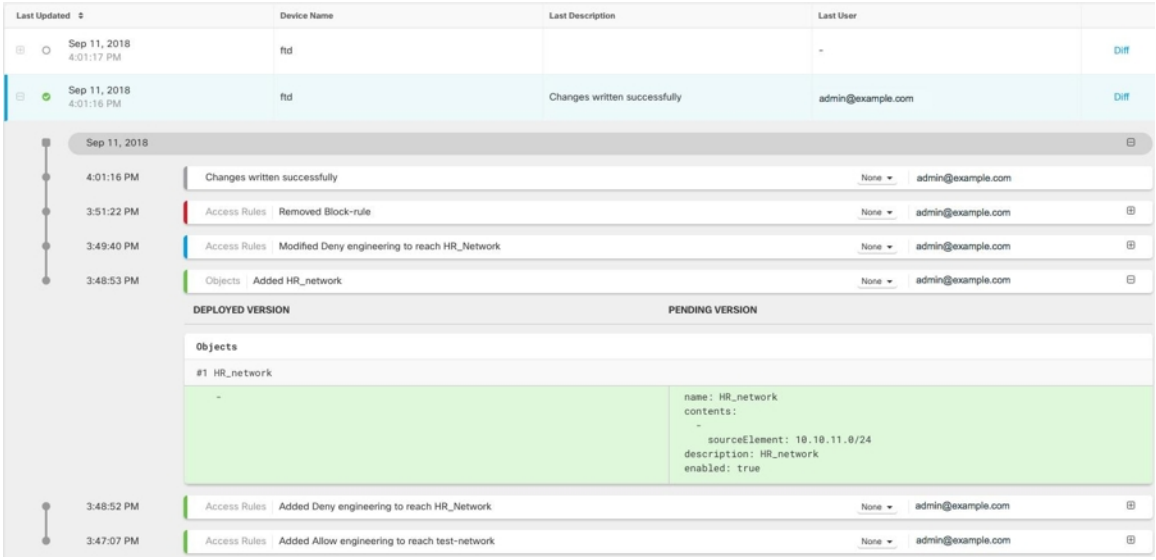
更改日志事件可搜索和过滤。使用搜索栏查找与关键字匹配的事件。使用过滤器 以查找符合您指定的所有条件的条目。您还可以通过过滤更改日志并将关键字添加到搜索字段来组合操作，以在过滤后的结果中查找条目。

部署到 FDM 管理 设备后更改日志条目

FDM管理 设备的更改日志条目中的更改会以简单的英语进行汇总。点击更改日志条目中的更改可将其展开，这样您就能查看到底更改了哪些内容。将更改从CDO 写入 FDM 管理 设备后，更改日志条目已完成， Defense Orchestrator 会为未来的更改创建一个新条目。如果点击更改日志条目行中的蓝色查看更改日志差异 链接，则会在运行配置文件的上下文中并排对比显示更改。

红色部分表示删除，蓝色部分表示修改，绿色部分表示设备配置添加内容，灰色部分表示消息。

查看下图中**已添加的 HR_network** 展开的更改。这是添加的网络对象 HR_network。“已部署版本”列为空，因为在更改之前设备上没有 HR_network 对象。“待定版本”(Pending Version) 列显示了已使用值 10.10.11.0/24 创建 HR_network 对象。



从设备读取更改后的更改日志条目FDM 管理

当 CDO 检测到设备发生更改时，它会在设备的“资产”页面的“配置状态”列中注册“检测到冲突”状态。FDM 管理它不会在更改日志中记录该配置状态。

当您接受在 CDO 之外进行的配置更改时，CDO 会创建一个作业，并在界面的右下角显示作业的处理状态。我们不建议在作业完成之前进行其他操作。否则，更改可能会丢失。

作业成功完成后，点击更改日志条目的“差异”链接。查看更改日志差异, on page 575

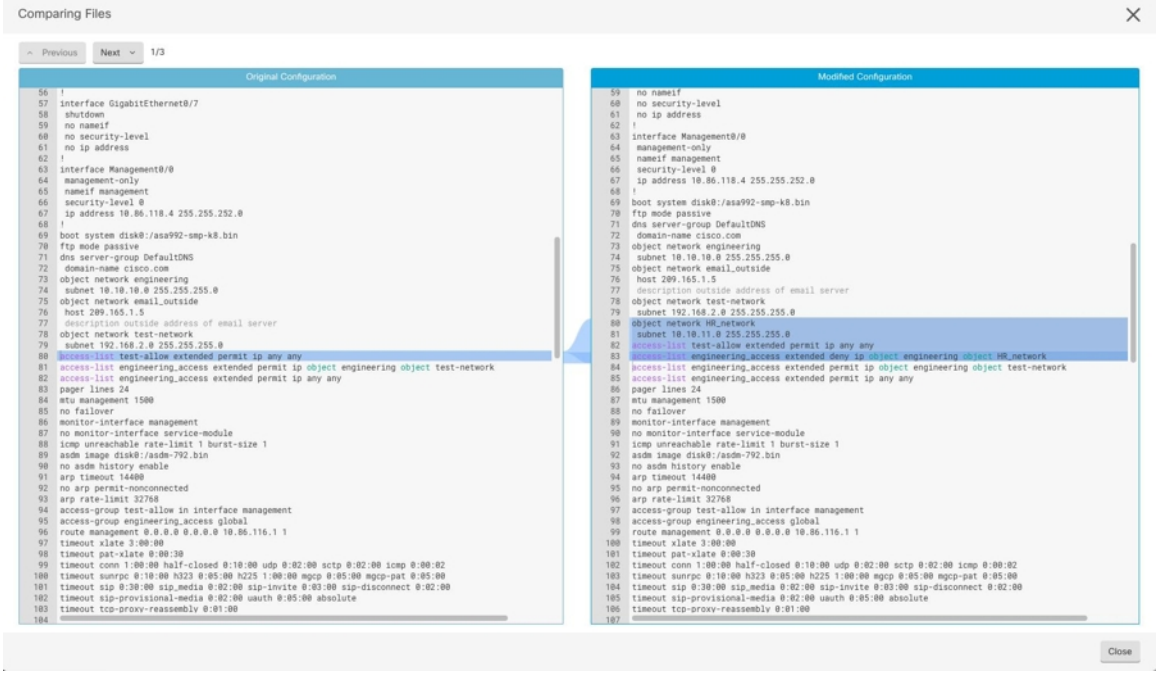
相关信息：

- 读取、丢弃、检查和部署更改, on page 551

查看更改日志差异

点击更改日志中的蓝色“差异”(Diff) 链接，可以并排比较设备的运行配置文件中的更改。您会看到两个版本的差异。

在下图中，“原始配置”(Original Configuration) 是更改写入之前的运行配置文件，“修改后的配置”(Modified Configuration) 列显示更改写入 ASA 后的运行配置文件。在这种情况下，原始配置列会突出显示运行配置文件中实际未更改的行，但会在修改后的配置列中提供参考点。按照从左到右列的行，您会看到添加了 HR_network 对象和访问规则，以防止“工程”网络中的地址访问“HR_network”网络中的地址。点击**上一个 (Previous)** 和**下一个 (Next)** 按钮浏览文件中的更改。



相关主题

- 变更日志, on page 573

将更改日志导出到 CSV 文件

您可以将 CDO 更改日志的全部或子集导出到逗号分隔值 (.csv) 文件，以便您可以随意过滤和排序其中的信息。

要将更改日志导出到 .csv 文件，请执行以下程序：

Procedure

步骤 1 在导航窗格中，点击 **更改日志**。

步骤 2 通过执行以下操作之一查找要导出的更改：

- 使用过滤器字段和搜索字段准确查找要导出的内容。例如，按设备过滤以仅查看所选设备的更改。
- 清除更改日志中的所有过滤器和搜索条件。这允许您导出整个更改日志。

Note 请记住，CDO 会存储 1 年的更改日志数据。最好是过滤更改日志内容并将结果下载到 .csv 文件，而不是下载长达一年的更改日志历史记录。

步骤 3 点击更改日志右上角的蓝色导出按钮。

步骤 4 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。

CDO 中的更改日志容量与导出的更改日志大小之间的差异

您从 CDO 的更改日志页面导出的信息与 CDO 存储在其数据库中的更改日志信息不同。

对于每个更改日志，CDO 会存储设备配置的两个副本，即“开始”配置和“结束”配置（如果更改日志已关闭）；或“当前”配置（如果是打开的更改日志）。这允许 CDO 并排显示配置差异。此外，CDO 会跟踪并存储每个步骤的“更改事件”，包括进行更改的用户名、更改时间以及其他详细信息。

但是，导出更改日志时，导出的内容不包括配置的两个完整副本。它仅包括“更改事件”，这使得导出文件比 CDO 存储的更改日志小得多。

CDO 最多可存储 1 年的更改日志信息，其中包括配置的两个副本。

更改请求管理

变更请求管理 允许您将在第三方故障单系统中打开的变更请求及其业务理由与变更日志中的事件相关联。使用更改请求管理在 CDO 中创建更改请求，使用唯一名称进行标识，输入更改说明，并将更改请求与更改日志事件相关联。您可以稍后在更改日志中搜索更改请求名称。

Note 您可能还会在 CDO 中看到对变更请求跟踪的引用。变更请求跟踪和变更请求管理指的是相同的功能。

启用更改请求管理

启用更改请求跟踪会影响租户的所有用户。要启用更改请求跟踪，请执行以下程序：

Procedure

步骤 1 从用户菜单中，选择“设置”(Settings)。

步骤 2 从用户菜单中，点击常规设置。

步骤 3 点击“更改请求跟踪”下的滑块。

确认后，您会在 Defense Orchestrator 界面的左下角看到 Change Request 工具栏，并在 Change Log 中看到 Change Request 下拉菜单。

创建更改请求

Procedure

步骤 1 在任何 CDO 页面中，点击页面左下角的更改请求工具栏中的蓝色 + 按钮。

步骤 2 为更改请求指定名称和说明。让变更请求名称反映您的组织想要实施的变更请求标识符。使用说明字段描述更改的目的。

Note 更改请求的名称一旦创建便无法更改。

步骤 3 保存更改请求。

Note CDO 保存更改请求并将所有新更改与该更改请求名称关联，直到您禁用更改请求或清除更改请求工具栏中的更改请求信息。

将更改请求与更改日志事件关联

Procedure

步骤 1 在导航窗格中，点击**更改日志 (Change Log)**。

步骤 2 展开更改日志以显示要与更改请求关联的事件。

步骤 3 在“更改请求”列中，点击事件的下拉菜单。请注意，最新的更改请求列在更改请求列表的顶部。

步骤 4 点击更改请求的名称，然后点击选择。

使用更改请求搜索更改日志事件

Procedure

步骤 1 在导航窗格中，点击**更改日志 (Change Log)**。

步骤 2 在更改日志搜索字段中，输入更改请求的确切名称，以便查找与该更改请求关联的更改日志事件。CDO 突出显示具有完全匹配项的更改日志事件。

搜索更改请求

Procedure

步骤 1 点击更改请求工具栏中的更改请求菜单。

步骤 2 开始键入您要搜索的更改请求名称或关键字。您将开始在更改请求列表的名称字段和说明字段中看到部分匹配的结果。

过滤器更改请求

过滤器托盘中有一个“更改请求”过滤器，可用于查找更改日志事件。

Procedure

步骤 1 在“更改日志”页面左侧的过滤器托盘中，找到“更改请求”区域。

步骤 2 展开过滤器并开始在搜索字段中键入更改请求的名称。部分匹配开始显示在搜索字段下方。

步骤 3 选择更改请求名称，选中相应的复选框，然后在“更改日志”表中显示匹配项。CDO突出显示具有完全匹配项的更改日志事件。

清除更改请求工具栏

清除更改请求工具栏可防止更改日志事件与现有更改请求自动关联。

Procedure

步骤 1 选择更改请求工具栏中的更改请求菜单。

步骤 2 点击**清除**。更改请求菜单更改为“无”。

清除与更改日志事件关联的更改请求

Procedure

步骤 1 在导航窗格中，点击 **更改日志**。

步骤 2 展开更改日志以显示要与更改请求取消关联的事件。

步骤 3 在“更改请求”列中，点击事件的下拉菜单。

步骤 4 点击清除。

删除更改请求

删除更改请求时，是将其从更改请求列表中删除，而不是从更改日志中删除。

Procedure

步骤 1 点击更改请求工具栏中的更改请求菜单。
步骤 2 点击更改请求名称。
步骤 3 点击该行中的删除图标。
步骤 4 点击绿色复选标记以确认您要删除更改请求。

禁用更改请求管理

禁用更改请求管理会影响您账户的所有用户。要禁用变更请求管理，请执行以下程序：

Procedure

步骤 1 从用户名菜单中，选择设置。
步骤 2 滑动更改请求跟踪下的按钮以显示灰色 X。

使用案例

这些使用案例假定您之前已按照上述说明启用了变更请求管理。

跟踪为解决外部系统中维护的故障单所做的防火墙更改

在此使用案例中，用户正在更改防火墙以解决在外部系统中维护的故障单。用户希望将这些防火墙更改导致的更改日志事件与更改请求相关联。请按照以下程序创建更改请求，并将更改日志事件与其关联。

1. 创建更改请求, on page 578。使用外部系统中的故障单名称或编号作为更改请求的名称。使用说明字段添加更改理由或其他相关信息。
2. 确保新的更改请求在更改请求工具栏中可见。
3. 进行防火墙更改。
4. 在导航窗格中，点击更改日志并查找与新更改请求关联的更改日志事件。

5. 清除更改请求工具栏, on page 579 完成后。

更改防火墙后手动更新单个更改日志事件

在此使用案例中，用户进行了防火墙更改以解决在外部系统中维护的故障单，但忘记使用更改请求管理功能将更改请求与更改日志事件相关联。用户希望返回更改日志，以使用故障单编号更新更改日志事件。请按照以下程序将更改请求与更改日志事件相关联。

1. 创建更改请求, on page 578。使用外部系统中的故障单名称或编号作为更改请求的名称。使用说明字段添加更改理由或其他相关信息。
2. 在导航窗格中，点击更改日志并搜索与防火墙更改关联的更改日志事件。
3. 将更改请求与更改日志事件关联, on page 578。
4. 完成后，清除更改请求工具栏。

搜索与更改请求关联的更改日志事件

在此使用案例中，用户希望了解由于解决外部系统中维护的故障单而导致的更改日志中记录了哪些更改日志事件。请按照以下程序搜索与更改请求关联的更改日志事件：

1. 在导航窗格中，点击**更改日志 (Change Log)**。
2. 使用以下方法之一搜索与更改请求关联的更改日志事件。
   - 在更改日志搜索字段中，输入更改请求的确切名称，以便查找与该更改请求关联的更改日志事件。CDO 突出显示具有完全匹配项的更改日志事件。
   - 过滤器更改请求, on page 579 查找更改日志事件。
3. 查看每个更改日志，查找显示相关更改请求的突出显示的更改日志事件。

FDM 管理 设备执行摘要报告

执行摘要报告提供所有 FDM 管理 设备的运行统计信息集合。载入设备后，思科防御协调器 最多可能需要两个小时才能从防火墙设备管理器收集此信息；初始报告生成后，每小时编译一次数据。请注意，报告信息不是事件请求的一部分，因此事件和报告不会以相同的节奏提供。

当网络流量触发 FDM 管理 设备上的访问规则或策略时，会生成报告中的数据。我们强烈建议启用恶意软件防御和 IPS 许可证，并为访问规则启用文件日志记录，以允许设备生成反映在报告中的事件。

请注意，报告中显示的所有信息都取决于页面顶部的**时间范围 (Time Range)** 切换。在您选择的时间范围内，策略可能会遇到不同的流量或触发器。

如果您在使用“执行摘要”报告时遇到问题，或者看到意外的流量，请参阅 执行摘要报告故障排除, on page 689 了解更多信息。

生成网络运行数据

在设备被载入 CDO 后，系统会自动收集事件数据。收集的数据取决于设备配置。与所有 FDM 管理设备一起提供的许可证并不支持网络操作报告中的所有选项。对于要从中收集数据的设备，我们建议进行以下配置：

- **日志记录 (Logging)** - 对适用的访问控制规则启用文件日志记录。有关详细信息，请参阅 FDM 管理 访问控制规则中的日志记录设置。
- **恶意软件事件** - 启用恶意软件智能许可证。
- **安全情报** - 启用 智能许可证。
- **IPS 威胁**- 启用 智能许可证。
- **Web 类别 (Web Categories)** - 启用 URL 智能许可证。
- **检测到的文件** - 启用 智能许可证。

有关智能许可证和这些许可证提供的功能的详细信息，请参阅 FDM 管理 设备许可类型。

Note 执行摘要本身并不包括通过 VPN 遇到的流量。

概述

“概述”(Overview) 选项卡显示已触发的规则、威胁和文件类型的视觉对象。这些项目以数字形式显示，首先列出最大或最常命中的规则、事件或文件。

恶意软件事件仅代表检测到或阻止的恶意软件文件。请注意，文件的处置可能发生变化，例如，从安全变为恶意软件或从恶意软件变为安全。我们建议您安排安全数据库更新以使您的设备保持最新的入侵规则 (SRU)。

前十个访问规则命中提供三个不同的选项卡，您可以在它们之间切换，以查看前十个规则传输、连接或阻止数据包的规则。

网络评估

“网络评估”(Network Assessment) 选项卡用于处理网站类别和检测到的文件类型。此显示仅捕获前十个最常遇到的类别和文件类型。除所选时间范围外，您无法使用此选项卡来确定检测到特定 Web 类别或文件类型的时间。

威胁

“威胁”(Threats) 选项卡显示入侵事件生成的统计信息： **排名靠前的攻击者 (Top Attacker)** 捕获事件的源 IP 地址， **排名靠前的目标 (Top Target)** 捕获事件的目的 IP 地址，而 **排名靠前的威胁 (Top Threats)** 捕获已归类为威胁的事件类型。

此选项卡还详细说明检测到的威胁和恶意软件类型。

生成报告

根据您的偏好配置报告后，您可以随时生成报告的 PDF 文件。有关详细信息，请参阅生成 FDM 管理 设备执行摘要报告。

生成 FDM 管理 设备执行摘要报告

CDO 提供多个报告，可用于分析安全策略对通过 FDM 管理 设备的流量的影响。执行摘要报告总结了最具影响力的恶意软件、威胁和受影响的安全情报。CDO 每小时轮询设备以收集事件。要了解有关执行摘要提供的更多信息，请参阅FDM 管理 设备执行摘要报告了解更多信息。

Important FDM 管理 设备报告仅在当前载入租户的 FDM 管理 设备上可用。这些报告会每小时生成一次并且不是事件请求的一部分，因此事件和报告不会以相同的节奏提供。在最初载入 FDM 管理 设备后，CDO 最多可能需要两个小时才能生成报告。在有报告显示之前，**监控 (Monitoring)** 选项下的**报告 (Reports)** 选项卡可能不会显示。

如果您是关于安全分析和日志记录 (SaaS)用户，则网络报告不会反映转发到安全事件连接器 (SEC) 的事件。

Note 流量相关报告中使用的数据是从访问控制规则和其他安全策略触发的事件中收集的。生成的报告不会反映未启用日志记录的规则或尚未触发的规则的流量。请确保配置规则以记录对您重要的信息。

使用以下程序生成执行摘要报告：

Procedure

步骤 1 在导航窗格中，点击 **监控 (Monitoring) > 执行摘要报告 (Executive Summary Report)**。

步骤 2 选择报告的时间范围： **过去 24 小时 (Last 24 Hours)**、**过去 7 天 (Last 7 Day)**、**过去 30 天 (Last 30 Day)**或 **过去 90 天(Last 90 Day)**。

步骤 3 （可选）点击过滤器图标 可生成有关自定义设备列表的报告。

步骤 4 点击**生成报告 (PDF) (Generate Report [PDF])**。

步骤 5 点击**保存 (Save)** 将报告另存为 PDF。浏览保存位置，然后点击**保存 (Save)**。如果您决定不保存报告，请随时点击**取消 (Cancel)**。

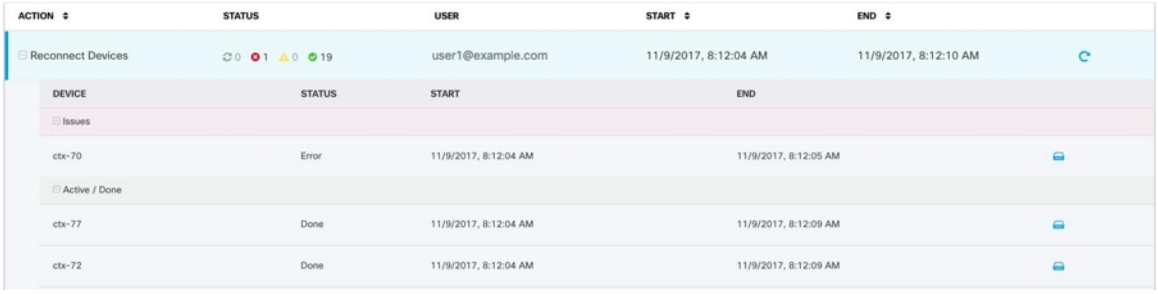
相关信息：

- FDM 管理 设备执行摘要报告
- 执行摘要报告故障排除, on page 689

作业页面

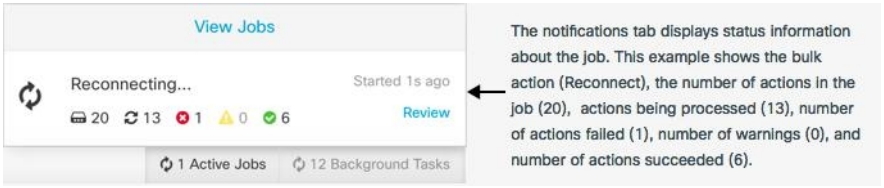
“作业”(Jobs)会页面显示有关批量操作状态的信息。批量操作可能是重新连接多个设备、从多个设备读取配置或同时升级多个设备。作业表中用颜色标记的行表示成功或失败的各个操作。

表中的一行代表一个批量操作。例如，该批量操作可能是尝试重新连接20台设备。展开“作业”(Jobs)页面中的一行，将显示受批量操作影响的每个设备的结果。



您可以通过三种不同的方式访问“作业”(Jobs) 页面：

- 在通知选项卡中，点击通知行中的**查看 (Review)** 链接。您将被重定向到“作业”(Jobs) 页面，并查看该通知所代表的特定作业。



- 在“通知”(Notifications) 选项卡的顶部，点击“查看作业”(View jobs) 链接，您将转到“作业”(Jobs)页面。
- 从 CDO 的菜单中，选择**监控 (Monitoring)** > **作业 (Jobs)**。此表显示了在 CDO 中执行的批量操作的完整列表。

搜索和过滤

进入“作业”(Jobs) 页面后，您可以按操作类型、执行这些操作的用户以及操作状态进行过滤和搜索。

重新启动导致操作失败的批量操作

查看“作业”页面时，如果发现批量操作中的一个或多个操作失败，则可以在进行任何必要的更正后重新运行批量操作。CDO将仅对失败的操作重新运行作业。要重新运行批量操作，请执行以下操作：

Procedure

步骤 1 选择作业页面中指示失败操作的行。

步骤 2 点击重新初始化 图标。

取消批量操作

现在，您可以取消在多台设备上执行的任何活动批量操作。例如，假设您已尝试重新连接四台受管设备，其中三台设备已成功重新连接，但第四台设备既未成功重新连接，也无法重新连接。

要取消批量操作，请执行以下操作：

Procedure

步骤 1 在 CDO 导航菜单上，点击作业。

步骤 2 找到仍在运行的批量操作，然后点击作业行右侧的取消链接。

如果批量操作的任何部分成功，这些操作将不会被撤销。任何仍在运行的操作都将被取消。

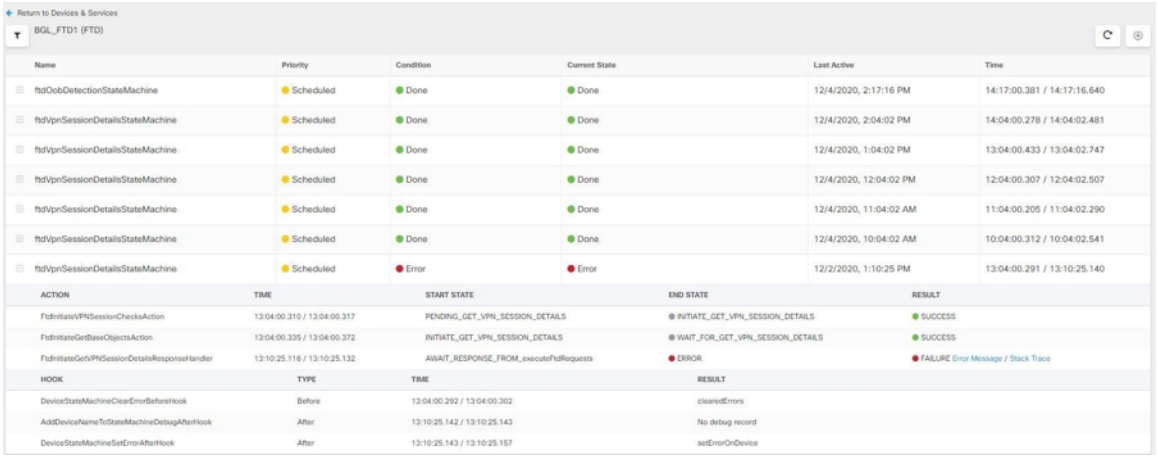
工作流程页面

通过“工作流程”(Workflow) 页面，您可以监控 CDO 在与设备、安全设备连接器 (SDC) 或安全事件连接器 (SEC) 通信时以及在对设备应用规则集更改时运行的每个进程。CDO 会在工作流程表中为每个步骤创建一个条目，并在此页面上显示其结果。该条目只会包含与 CDO 执行的操作相关的信息，而不是与其交互的设备相关的信息。

当 CDO 无法在设备上执行任务时，它会报告错误，您可以导航至“工作流程”(Workflows) 页面查看发生错误的步骤以了解更多详细信息。

您可以访问此页面来确定错误并进行故障排除，或者在 TAC 坚持时与他们共享信息。

要导航至“工作流程”(Workflows) 页面，请在**清单 (Inventory)** 页面上点击**设备 (Devices)** 选项卡。点击相应的设备类型选项卡，以便查找设备并选择所需的设备。在右侧窗格的**设备和操作 (Devices and Actions)** 中，点击**工作流程 (Workflows)**。下图显示了“工作流程”(Workflow) 页面，其中包含“工作流程”(Workflow) 表中的条目。

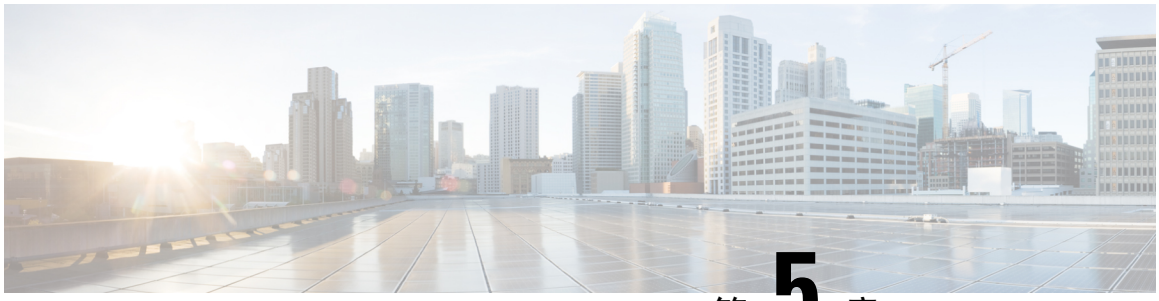


下载工作流程信息

您可以将完整的工作流程信息下载到 JSON 文件，并在 TAC 团队要求进行进一步分析时提供。要下载这些信息，您可以选择设备并导航至其工作流程页面，然后点击右上角显示的导出按钮 。

生成堆栈跟踪

如果您遇到无法解决的错误，TAC 可能会要求您提供堆栈跟踪的副本。要收集错误的堆栈跟踪，请点击**堆栈跟踪 (Stack Trace)** 链接，然后点击**复制堆栈跟踪 (Copy Stacktrace)**，以便将屏幕上显示的堆栈复制到剪贴板。



第 5 章

思科安全分析和日志记录

关于安全分析和日志记录 (SaaS)

思科安全分析和日志记录 (SAL) 允许您从所有 FDM 管理 设备捕获连接、入侵、文件、恶意软件和安全情报事件，以及从 ASA 捕获所有系统日志事件和 Netflow 安全事件日志记录 (NSEL) 事件并在 Cisco Defense Orchestrator (CDO) 中的一个位置进行查看。事件存储在思科云中，可从 CDO 中的“事件日志记录”页面查看，您可以在其中过滤和查看事件，以便清楚地了解在网络中触发的安全规则。

通过额外许可，在捕获这些事件后，您可以从CDO交叉启动为您调配的安全云分析门户。安全云分析是一种软件即服务 (SaaS) 解决方案，通过对事件和网络流数据执行行为分析来跟踪网络状态。通过从源（包括防火墙事件和网络流数据）收集有关网络流量的信息，它会创建有关流量的观察结果，并根据其流量模式自动识别网络实体的角色。使用此信息与其他威胁情报来源（例如 Talos）相结合，安全云分析会生成警报，警告可能存在恶意行为。除警报外，安全云分析还提供网络和主机可视性以及所收集的情景信息，为您研究警报和查找恶意行为的来源提供更好的基础。

术语说明：在本文档中，当思科安全分析和日志记录与安全云分析门户（软件即服务产品）配合使用时，您会看到此集成称为思科安全分析和日志记录 (SaaS) 或 SAL (SaaS) 。

FDM 管理 设备的安全日志记录分析

思科安全分析和日志记录 (SaaS) 允许您从所有 FDM 管理 设备捕获连接、入侵、文件、恶意软件和安全情报事件，并在 思科防御协调器 中的一个位置进行查看。

事件存储在思科云中，可从CDO中的“事件日志记录”页面查看，您可以在其中过滤和查看事件，以便清楚地了解在网络中触发的安全规则。**日志记录和故障排除**软件包为您提供这些功能。

使用**日志记录分析和检测**包（以前称为**防火墙分析和日志记录**包），系统可以将安全云分析动态实体建模应用于 FDM 管理 设备事件，并使用行为建模分析生成安全云分析观察结果和警报。如果您获取**全部网络分析和监控**软件包，则系统会对 FDM 管理 设备事件和网络流量应用动态实体建模，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思科安全云分析门户。

FDM 事件在 CDO 事件查看器中的显示方式

当单个规则配置为记录事件且网络流量与规则条件匹配时，会生成连接、入侵、文件、恶意软件和安全情报事件。将事件存储在思科云中后，您可以在 CDO 中查看它们。有两种方法可以配置 FDM 管理 设备以将事件发送到思科云：

- 您可以安装多个安全事件连接器 (SEC)，并将任何设备上的规则生成的事件发送到任何 SEC，就像它是系统日志服务器一样。然后，SEC 将事件转发到思科云。
- 如果您的 FDM 管理 设备已使用注册密钥载入 CDO，则可以使用 Firepower 设备管理器 中的控件将事件直接发送到思科云。

如何使用安全事件连接器将事件发送到思科云

使用基本**日志记录和故障排除**许可证，Firepower 设备管理器 事件到达思科云的方式如下：

1. 您可以使用用户名和密码或使用注册密钥将 FDM 管理 设备载入 CDO。
2. 配置各个规则（例如访问控制规则、安全情报规则和 SSL 解密规则）以将事件转发到任何一个 SEC，就像它是系统日志服务器一样。在访问控制规则中，您还可以启用文件和恶意软件策略以及入侵策略，并将这些策略生成的事件转发到 SEC。
3. 您可以在文件事件的**系统设置 (System Settings)** > **日志记录 (Logging)** 中配置文件/恶意软件日志记录。
4. 在**系统设置 (System Settings)** > **日志记录 (Logging)** 中为入侵事件配置入侵日志记录。
5. SEC 将事件转发到存储事件的思科云。
6. CDO 根据您设置的过滤器在其事件日志记录页面中显示来自思科云的事件。

使用**日志记录分析和检测**或**全部网络分析和监控**许可证时，还会发生以下情况：

1. 思科安全云分析将分析应用于存储在思科云中的 Firepower 设备管理器 连接事件。
2. 生成的观察结果和警报可从与您的 CDO 门户关联的安全云分析门户访问。
3. 在 CDO 门户中，您可以交叉启动 Cisco Secure Cloud Analytics 门户，以查看这些观察结果和警报。

如何将事件从 Firepower 设备管理器 发送到思科云

通过使用基本**日志记录和故障排除许可证**，Firepower 设备管理器 事件会通过以下方式到达思科云：

1. 您使用注册令牌将 FDM 管理 设备载入 CDO。
2. 配置各个规则（例如访问控制规则、安全情报规则和 SSL 解密规则）以记录事件，但不指定要向其发送事件的系统日志服务器。在访问控制规则中，您还可以启用文件和恶意软件策略以及入侵策略，并将这些策略生成的事件转发到思科云。
3. 如果在访问控制规则中配置了文件和恶意软件策略以及入侵策略来记录连接事件，则将文件事件和入侵事件发送到思科云。
4. 在 Firepower 设备管理器 上载入云日志记录，并将各种规则中记录的事件发送到思科云。
5. CDO 根据您设置的过滤器从思科云提取事件，并将其显示在其事件查看器中。

使用 **日志记录分析和检测** 或 **全部网络分析和监控** 许可证时，还会发生以下情况：

1. 思科安全云分析将分析应用于存储在思科云中的 Firepower 设备管理器 连接事件。
2. 生成的观察结果和警报可从与您的 CDO 门户关联的安全云分析门户访问。
3. 在 CDO 门户中，您可以交叉启动 Cisco Secure Cloud Analytics 门户，以查看这些观察结果和警报。

配置对比

以下是通过 SEC 将事件发送到思科云与直接将事件发送到思科云之间的 CDO 配置差异的摘要。

FDM 管理 设备配置	通过安全事件连接器 (SEC) 发送事件时	将事件直接发送至思科云时
FDM 管理 设备的 CDO 载入方法	凭证（用户名和密码） 注册令牌	注册令牌 序列号
版本支持	版本 6.4+	注册令牌 - 版本 6.5+ 序列号 - 版本 6.7+
思科安全分析和日志记录 (SaaS) 许可证	日志记录故障排除 日志记录分析和检测（可选） 全面的网络分析和监控（可选）	日志记录故障排除 日志记录分析和检测（可选） 全面的网络分析和监控（可选）
许可证	许可证 - 如果要从入侵规则、文件控制规则或安全情报过滤收集连接事件。 恶意软件 - 如果要从文件控制规则收集连接事件。	许可证 - 如果要从入侵规则、文件控制规则或安全情报过滤收集连接事件。 恶意软件 - 如果要从文件控制规则收集连接事件。
安全事件连接器	必要	不适用
数据压缩*	事件已压缩*	事件未压缩*
数据计划	必填	必填

注释 数据订用和您的历史每月使用量基于您使用的未压缩数据量。

解决方案中的组件

思科安全分析和日志记录 (SaaS) 使用以下组件向 CDO 传送事件：

安全设备连接器 (SDC) - SDC 将 CDO 连接到您的 FDM 管理 设备。FDM 管理 设备的登录凭证被存储在 SDC 上。有关详细信息，请参阅 安全设备连接器 (SDC)，第 10 页。

安全事件连接器 (SEC) - SEC 是一种从 FDM 管理 设备接收事件并将其转发到思科云的应用。进入思科云后，您可以在 CDO 的事件日志记录页面上查看事件，或使用思科安全云分析进行分析。您可能有一个或多个 SEC 与您的租户相关联。根据您的环境，在安全设备连接器或 CDO 连接器虚拟机上安装安全事件连接器。

Firepower 设备管理器 - FDM 管理 设备是思科的下一代防火墙。除了对网络流量和访问控制进行状态检查之外，FDM 管理 设备还提供多种功能，例如防御恶意软件和应用层攻击、集成入侵防御以及云提供的威胁情报。

如果您有**日志记录分析和检测**或**全面网络分析和监控**许可证，思科安全分析和日志记录 (SaaS) 将使用 Cisco Secure Cloud Analytics 进一步分析传送给 CDO 的事件。

思科安全云分析 - 安全云分析将动态实体建模应用于事件，并根据此信息生成检测。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。

许可

要配置此解决方案，您需要以下账户和许可证：

思科防御协调器。您必须有 CDO 租户。

安全设备连接器。SDC 没有单独的许可证。

安全事件连接器。SEC 没有单独的许可证。

安全日志记录分析 (SaaS)。您需要购买**日志记录和故障排除**许可证。此软件包的目标是为网络运营团队提供从其载入的 FDM 管理 设备派生的实时和历史事件，以便对其网络中的流量进行故障排除和分析。

您还可以购买**日志记录分析和检测**或**全面网络分析和监控**许可证来应用思科安全云分析。这些软件包的目标是为网络运营团队提供有关事件（以及使用全面网络分析和监控许可证的网络流量）的更多见解，以便更好地识别可能的异常行为并做出响应。

许可证名称	提供的功能	可用许可证持续时间	功能前提条件
日志记录故障排除	在CDO中查看事件和事件详细信息，包括实时源和历史视图	• 1 年 • 3 年 • 提高	• CDO • 运行 6.4 或更高版本的本地部署 。 • 部署一个或多个 SEC 以将事件传递到云
日志记录分析和检测（以前称为**防火墙分析和监控**）	**日志记录和故障排除**功能，以及： • 对 FDM 管理 设备事件应用动态实体建模和行为分析。 • 根据事件数据在 Secure Cloud Analytics 中打开警报，从 CDO 事件查看器交叉启动	• 1 年 • 3 年 • 提高	• CDO • 运行 6.4 或更高版本的本地部署。 • 部署一个或多个 SEC 以将事件传递到云。 • 新调配的或现有的安全云分析门户。

许可证名称	提供的功能	可用许可证持续时间	功能前提条件
全面的网络分析和监控	日志记录分析和检测，以及： • 将动态实体建模和行为分析应用于事件、本地网络流量和基于云的网络流量。 • 根据事件数据、安全云分析传感器收集的本地网络流量数据以及从 CDO 事件查看器交叉启动传递到安全云分析的基于云的网络流量的组合，在安全云分析中打开警报。	• 1 年 • 3 年 • 提高	• CDO • 运行 6.4 或更高版本的本地部署 。 • 部署一个或多个 SEC 以将事件传递到云 。 • 部署至少一个安全云分析传感器版本 4.1 或更高版本，以将网络流量数据传递到云，或者将安全云分析与基于云的部署集成，以将网络流量数据传递到安全云分析。 • 新调配的或现有的安全云分析门户。

FDM 管理 设备。您需要具有以下许可证才能运行 FDM 管理 设备并创建生成安全事件的规则：

许可证	持续时间	授予的功能
基础版（自动包含）	永久	可选期限的许可证中未包括的所有功能。 您还必须指定是否**在使用此令牌注册的产品上允许出口控制功能**。仅在您的国家/地区满足出口控制标准时，才可以选择此选项。此选项控制您对高级加密和需要高级加密的功能的使用。

许可证	持续时间	授予的功能
	基于期限	**入侵检测和防御 (Intrusion detection and prevention)** - 入侵策略用于分析网络流量是否存在入侵和漏洞利用，或者丢弃攻击性数据包。 **文件控制 (File control)** - 文件策略用于检测和选择性地阻止用户上传（发送）或下载（接收）特定类型的文件。通过面向 Firepower 的 AMP（需要恶意软件许可证），您可以检查和阻止包含恶意软件的文件。必须拥有威胁许可证才可使用任何类型的文件策略。 **安全情报过滤 (Security Intelligence filtering)** - 将选定流量丢弃后，通过访问控制规则对流量进行分析。动态源可用于根据最新情报立即丢弃连接。
恶意软件	基于期限	检查恶意软件的文件策略，将思科高级恶意软件保护 (AMP) 与适用于 Firepower 的 AMP（基于网络的高级恶意软件保护）和思科 Threat Grid 结合使用。 文件策略可以检测和阻止通过网络传输的文件中的恶意软件。

数据计划

您需要购买反映思科云每天从您注册的 FDM 管理 设备接收的事件数量的数据存储计划。确定注入速率的最佳方法是在购买之前参加安全日志分析 (SaaS) (SaaS) 的免费试用。这将为您提供对事件数量的一个很好的估计。此外，您还可以使用日志记录量估算器工具。

注意 可以将 FDM 管理 设备配置为直接和通过 SEC 将事件发送到思科云。如果执行此操作，则同一事件将被 "注入" 两次，并根据您的数据计划进行两次计数，但只会在思科云中存储一次。使用一种或另一种方法将事件发送到思科云时，请务必小心，以避免产生不必要的费用。

数据计划有 1 年、3 年或 5 年期限，每日增量为 1 GB。有关数据计划的信息，请参阅《安全日志分析 (SaaS) 订购指南 》。

注释 如果您有安全分析和日志记录许可证和数据计划，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安全分析和日志记录许可证。

30 天免费试用

您可以通过登录 CDO 并导航到 **分析 (Analytics)** > **事件日志记录 (Event Logging)** 来申请 30 天无风险试用。完成30天试用后，您可以按照《安全日志分析(SaaS)订购指南》中的说明，从思科商务工作空间 (CCW) 订购所需的事件数据量，以继续使用该服务。

后续操作？

继续执行为 FDM 管理 设备实施安全日志记录分析 (SaaS)，第 594 页。

为 FDM 管理 设备实施安全日志记录分析 (SaaS)

准备工作

- 查看 FDM 管理 设备的安全日志记录分析, on page 588 以了解以下内容：
  - 如何将事件发送到思科云
  - 应用解决方案
  - 您需要的许可证
  - 您需要的数据计划
- 您已联系托管服务提供商或 思科防御协调器 销售代表，并且您有一个 CDO 租户。
- 您的租户可能会也可能不会使用 CDO 的安全设备连接器 (SDC) 来连接您的 FDM 管理设备。您的租户应为您使用设备凭证载入的那些 FDM 管理设备安装 SDC，安全设备连接器 (SDC)。如果您使用注册密钥或序列号来载入 FDM 管理设备，则不需要 SDC。
- 如果您已为租户安装 SDC，请确保您的 SDC 状态为**活动 (Active)** 并已记录最近的心跳。
- 如果要安装 SDC，请使用以下方法之一进行安装：
  - 使用使用 CDO 的 VM 映像部署安全设备连接器 以使用 CDO 准备的虚拟机映像安装 SDC。这是部署 SDC 的首选且最简单的方法。
  - 使用在您自己的虚拟机上部署安全设备连接器。
- 您可以为租户使用 CDO 映像安装 SEC，并且可以将任何 防火墙设备管理器 中的事件发送至已载入到租户的任何一个 SEC。

- 如果您从 防火墙设备管理器 直接向思科云发送事件，则已在管理接口上的端口 443 上打开出站访问。
- 您已为账户的用户 登录到 CDO 。

用于实施安全日志记录分析 (SaaS) 并通过安全事件连接器将事件发送到思科云的新 CDO 客户工作流程

1. 载入 威胁防御 设备。您可以使用管理员用户名和密码或注册令牌来载入设备。
2. 系统日志服务器对象。
3. FDM 管理 访问控制策略以记录连接事件。
4. 将 FDM 管理设备配置为将 FDM 事件发送到 思科防御协调器 事件日志记录。
5. 确认事件显示在 CDO 中。从导航栏中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。点击“实时”(Live) 选项卡以查看实时事件。
6. 如果您有**日志记录分析和检测**或**全面网络分析和监控**许可证，请继续分析思科安全云分析中的事件。

实施安全日志记录分析 (SaaS) 并将事件直接发送到思科云的新 CDO 客户工作流程

1. 载入 威胁防御 设备。您仅能使用注册密钥。
2. FDM 管理 访问控制策略以记录连接事件。
3. 将 FDM 管理 设备配置为将 FDM 管理 事件直接发送至思科云。
4. 确认事件显示在 CDO 中。从导航栏中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。点击“实时”(Live) 选项卡以查看实时事件。
5. 如果您有**日志记录分析和检测**或**全面网络分析和监控**许可证，请继续分析思科安全云分析中的事件。

实施安全日志记录分析 (SaaS) 并通过安全事件连接器将事件发送到思科云的现有 CDO 客户工作流程

1. 载入 威胁防御 设备。您可以使用管理员用户名和密码或注册令牌来载入设备。
2. 系统日志服务器对象。
3. FDM 管理 访问控制策略以记录连接事件。
4. 将 FDM 事件发送到 思科防御协调器 事件日志记录。
5. 确认事件显示在 CDO 中。从导航栏中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。点击“实时”(Live) 选项卡以查看实时事件。
6. 如果您有 **日志记录分析和检测** 或 **全面网络分析和监控** 许可证，请继续 分析思科安全云分析中的事件。

实施安全日志记录分析 (SaaS) 并将事件直接发送到思科云的现有 CDO 客户工作流程

1. 载入 威胁防御 设备。您仅能使用注册密钥。
2. FDM 管理 访问控制策略以记录连接事件。
3. 将 FDM 管理 设备配置为将 FDM 管理 事件直接发送至思科云。
4. 确认事件显示在 CDO 中。从导航栏中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。点击“实时”(Live) 选项卡以查看实时事件。
5. 如果您有 **日志记录分析和检测** 或 **全面网络分析和监控** 许可证，请继续 分析思科安全云分析中的事件。

分析思科安全云分析中的事件

如果您有**日志记录分析和检测**或**全面网络分析和监控**许可证，除上述步骤外，还应执行以下操作：

1. 调配思科安全云分析门户, on page 620。
2. 如果您购买了**全面网络分析和监控**许可证，请将一个或多个安全云分析传感器部署到您的内部网络。请参阅用于全面网络分析和报告的思科安全云分析传感器部署, on page 622。
3. 邀请用户创建与其思科单点登录凭证相关联的安全云分析用户账户。请参阅从 CDO 查看 Cisco Secure Cloud Analytics 警报, on page 622。
4. 从 CDO 到 Secure Cloud Analytics 的交叉启动，以监控 防火墙设备管理器 事件生成的安全云分析警报。请参阅 从 CDO 查看 Cisco Secure Cloud Analytics 警报, on page 622。

通过从 CDO 交叉启动查看安全云分析警报

使用**日志记录分析和检测**或**全面网络分析和监控**许可证，您可以从CDO交叉启动安全云分析，以查看由安全云分析基于 防火墙设备管理器 事件生成的警报。

有关详细信息，请参阅以下文章：

- 登录到 CDO
- 从 CDO 查看 Cisco Secure Cloud Analytics 警报, on page 622
- 思科安全云分析和动态实体建模, on page 624
- 使用基于防火墙事件的警报

安全分析和日志记录 (SaaS) 工作流程

使用安全和分析日志记录事件排除网络问题介绍了使用从安全日志记录分析 (SaaS) 生成的事件来确定用户无法访问网络资源的原因。

另请参阅使用基于防火墙事件的警报。

将 FDM 事件发送到 思科防御协调器 事件日志记录

要在事件日志记录查看器中查看来自访问控制规则、安全情报规则和 SSL 解密规则的 FDM 管理 事件，首先需要将这些事件发送到思科云。

- **访问控制规则**。您可以在网络连接开始或结束时记录FDM 管理 事件类型。有关配置此规则类型的日志记录的详细信息，请参阅配置 FDM 访问控制策略和 FDM 管理 访问控制规则中的日志记录设置。
- **安全情报规则**。您可以记录安全情报规则生成的 FDM 管理 事件类型。如果启用了日志记录，系统会记录与阻止列表条目匹配的任意项。系统不记录例外条目的匹配项，但如果被免除的连接与启用日志记录的访问控制规则匹配，您会收到日志消息。有关配置日志记录的详细信息，请参阅配置 Firepower 安全情报策略。
- **SSL 解密规则**。您可以记录 SSL 解密规则生成的FDM 管理 事件类型。

如果您将文件和恶意软件事件或入侵事件事件发送到思科云，并且使用的是安全事件连接器，则需要为配置日志记录设置。

相关信息：

- 为安全日志记录分析 (SaaS) 创建系统日志服务器对象

将 FDM 管理 事件直接发送至思科云

从 防火墙设备管理器 版本 6.5 开始，您可以将连接事件、入侵、文件和恶意软件事件直接从您的 FDM 管理 设备发送到思科云。进入思科云后，您可以使用 思科防御协调器 (CDO) 对其进行监控，并使用思科安全云分析器进行分析。此方法不需要在安全设备连接器 (SDC) 虚拟机上安装安全事件连接器 (SEC) 容器。

Before you begin

查看这些主题：

- FDM 管理 设备的安全日志记录分析, on page 588
- 为 FDM 管理 设备实施安全日志记录分析 (SaaS)

Procedure

步骤 1 登录到要从中将事件发送到思科云的设备的 防火墙设备管理器。

步骤 2 依次选择 **设备 (Device)** > **系统设置 (System Settings)** > **云服务 (Cloud Services)**。

步骤 3 在将事件发送到思科云窗格中，点击**启用 (Enable)**。

FDM 管理 事件类型

事件类型

系统可以生成以下类型的事件。只有生成这些事件，才能在监控控制面板中查看相关统计信息。

数据（诊断）事件

数据记录可以为与连接不相关的事件（包括与设备和系统健康状况以及网络配置相关的事件）提供系统日志消息。可以在各个访问控制规则内配置连接日志记录。

数据记录可为在数据平面上运行的功能（即在CLI配置中定义的功能，可以使用**show running-config**命令来查看这些功能）生成消息。这包括诸如路由、VPN、数据接口、DHCP 服务器、NAT 等功能。

连接事件

您可以在用户生成通过系统传递的流量时生成连接事件。启用访问规则连接日志记录以生成这些事件。还可启用安全情报策略和 SSL 解密规则日志记录，以生成连接事件。

连接事件包含关于检测到的会话的数据。任何单个连接事件的可用信息都取决于多种因素，但通常包括：

- 基本连接属性：时间戳、源和目标 IP 地址、入口和出口区域，处理连接的设备等。
- 系统发现或推断的其他连接属性：应用、请求的 URL 或与连接关联的用户等。
- 有关连接记录原因的元数据：哪个配置处理流量，连接是被允许还是被阻止，以及有关已加密和已解密连接的详细信息等。

入侵事件

系统检查网络上传输的数据包是否存在可能影响主机及其数据的可用性、完整性和机密性的恶意活动。如果系统识别出潜在的入侵，会生成入侵事件；入侵事件是有关攻击源和攻击目标的日期、时间、攻击程序类型以及情境信息的记录。无论调用访问控制规则的日志记录配置如何，系统均会生成设为阻止或提醒的入侵规则的入侵事件。

文件事件

文件事件表示系统基于文件策略在网络流量中检测到或者被阻止的文件。只有在应用文件策略的访问规则中启用文件日志记录，才能生成这些事件。

无论调用访问控制规则采用何种日志记录配置，在系统生成文件事件时，都会记录相关连接的终止。

恶意软件事件

作为整体访问控制配置的一部分，系统可在网络流量内检测恶意软件。适用于 Firepower 的 AMP 可以生成恶意软件事件，其中包含生成事件的处置，有关检测该恶意软件的方式、位置和时间的情境数据。只有在应用文件策略的访问规则中启用文件日志记录，才能生成这些事件。

文件的处置可能发生变化，例如，从安全变为恶意软件或从恶意软件变为安全。如果适用于Firepower的 AMP 向 AMP 云查询文件，且云决定在查询一周内更改处置，系统即会生成追溯性恶意软件事件。

安全情报事件

安全情报事件是由安全情报策略为该策略阻止或监控的每个连接生成的一种连接事件。所有安全情报事件都有一个由系统填充的“安全情报类别”字段。

对于各事件，都有一个相应的“常规”连接事件。由于评估安全智能策略后才会评估许多其他安全策略（包括访问控制），所以当安全智能阻止连接时，所生成事件不含系统从后续评估中收集的信息（如用户身份）。

安全事件连接器

安全事件连接器 (SEC) 是安全分析和日志记录 SaaS 解决方案的一个组件。它接收来自 ASA 和 FDM 管理 设备的事件，并将其转发到思科云。CDO 在“事件日志记录”(Event Logging) 页面上显示事件，以便管理员可以在该页面或使用 Cisco Secure Cloud Analytics 进行分析。

SEC 安装在您的网络中部署的安全设备连接器上，安装在您的网络中部署的自己的CDO连接器虚拟机上，或安装在 AWS 虚拟私有云 (VPC) 上。

安全事件连接器 ID

与思科 Technical Assistance Center (TAC) 或其他 CDO 支持人员合作时，您可能会需要 SEC 的 ID。该 ID 可在 CDO 的“安全连接器”(Secure Connectors) 页面上找到。要查找 SEC ID，请执行以下操作：

1. 从左侧 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。
2. 点击您要标识的 SEC。
3. SEC ID 是“详细信息”(Details) 窗格中“租户 ID”(Tenant ID) 上方列出的 ID。

相关信息：

- FDM 管理 设备的安全日志记录分析
- 在 SDC 虚拟机上安装安全事件连接器， 第 600 页
- 使用 VM 映像安装 SEC
- 使用 VM 映像安装 SEC
- 使用 Terraform 模块在 AWS VPC 上安装安全事件连接器， 第 617 页
- 删除安全事件连接器
- 取消调配思科安全分析和日志记录 (SaaS)

安装安全事件连接器

安全事件连接器 (SEC) 可以安装在有或没有 SDC 的租户上。

您可以在与安全设备连接器相同的虚拟机上安装一个 SEC（如果有）；或者，您可以在网络中维护的 SEC 自己的 CDO 连接器虚拟机上安装 SEC。

请参阅以下介绍各种安装情况的主题：

- 使用 VM 映像安装 SEC，第 609 页
- 使用 CDO 映像安装 SEC，第 603 页
- 使用 Terraform 模块在 AWS VPC 上安装安全事件连接器，第 617 页

在 SDC 虚拟机上安装安全事件连接器

安全事件连接器 (SEC) 从 ASA 和 FDM 管理 设备接收事件，并将其转发到思科云。CDO 在“事件日志记录”(Event Logging) 页面上显示事件，以便管理员可以在该页面或使用思科安全云分析进行分析。

您可以在与安全设备连接器相同的虚拟机上安装一个 SEC（如果有）；或者，您可以在网络中维护的 SEC 自己的 CDO 连接器虚拟机上安装 SEC。

本文介绍如何在与 SDC 相同的虚拟机上安装 SEC。如果要安装更多 SEC，请参阅 使用 CDO 映像安装 SEC，第 603 页 或 使用 VM 映像安装 SEC，第 609 页。

开始之前

- 购买思科安全和分析日志记录、**日志记录和故障排除**许可证。或者，如果您想先注销思科安全和分析，请登录 CDO，然后在主导航栏上，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)** 并点击**请求试用 (Request Trial)**。您还可以购买 **日志记录 分析和检测 (Logging Analytics and Detection)** 以及 **全面网络分析和监控 (Total Network Analytics and Monitoring)** 许可证，以将安全云分析应用于事件。
- 确保您的 SDC 已安装。如果需要安装 SDC，请执行以下程序之一：
  - 使用 CDO 的 VM 映像部署安全设备连接器
  - 在您自己的虚拟机上部署安全设备连接器

注释 如果您在自己的虚拟机上安装了本地 SDC，则需要进行您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置才能允许事件到达它。

- 确保 SDC 与 CDO 通信：
  1. 从 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

2. 在安装 SEC 之前，请确保 SDC 的最后一次心跳不超过 10 分钟，并且 SDC 的状态为活动。

- 系统要求 - 为运行 SDC 的虚拟机分配额外的 CPU 和内存：
  - CPU：分配**额外** 4 个 CPU 以容纳 SEC，使 CPU 总数达到 6 个。
  - 内存：为 SEC 分配**额外** 8 GB 内存，使内存总量达到 10 GB。

    更新 VM 上的 CPU 和内存以适应 SEC 后，打开 VM 并确保“安全连接器”页面指示 SDC 处于“活动”状态。

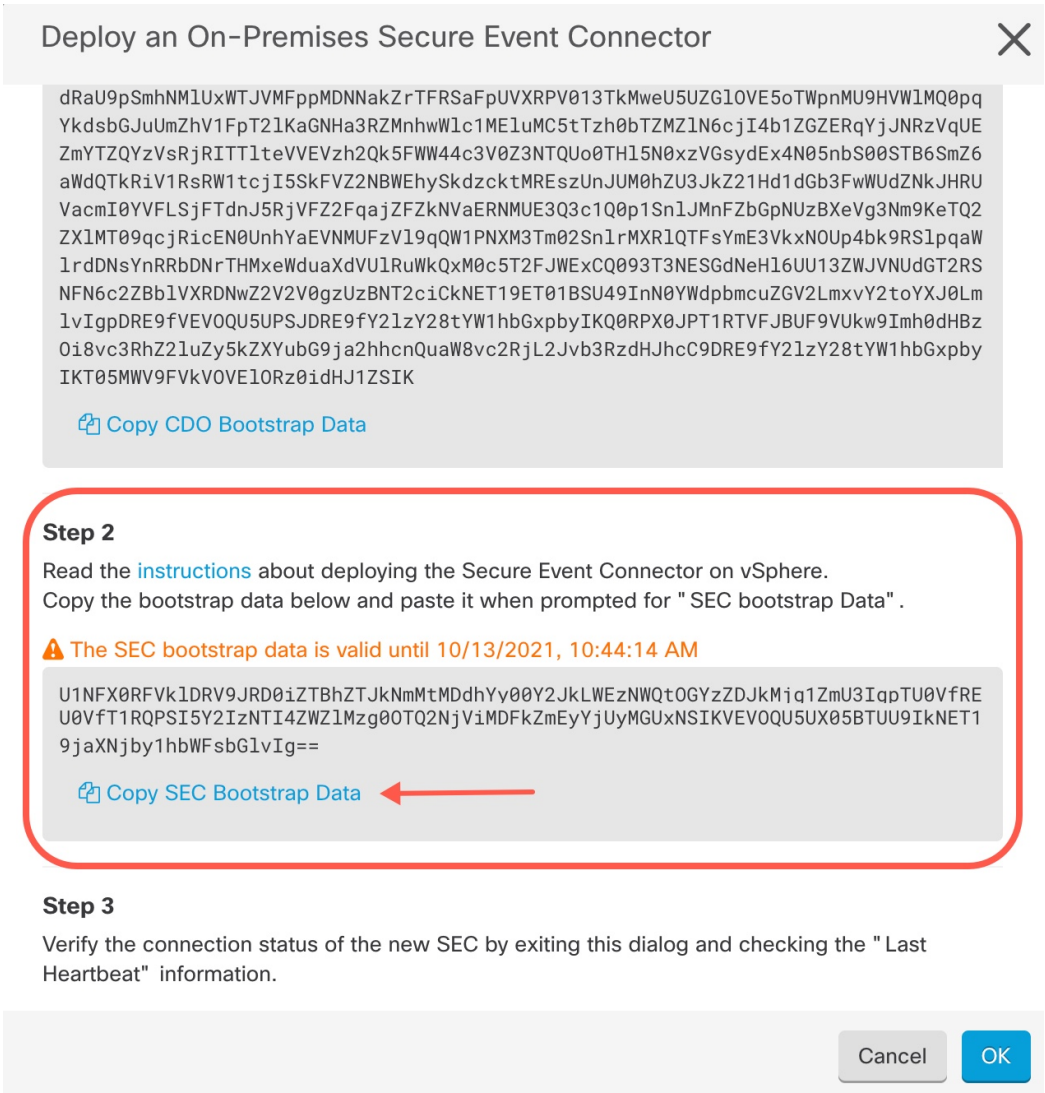
过程

步骤 1 登录 CDO。

步骤 2 从 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

步骤 3 点击蓝色加号按钮，然后点击**安全事件连接器 (Secure Event Connector)**。

步骤 4 跳过向导的步骤 1，转至步骤 2。在向导的步骤 2 中，点击复制 **SEC 引导程序数据 (Copy SEC Bootstrap Data)**的链接。



步骤 5 打开终端窗口并以“cdo”用户身份登录 SDC。

步骤 6 登录后，切换到“sdc”用户。当系统提示输入密码时，请输入“cdo”用户的密码。以下是这些命令的示例：

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

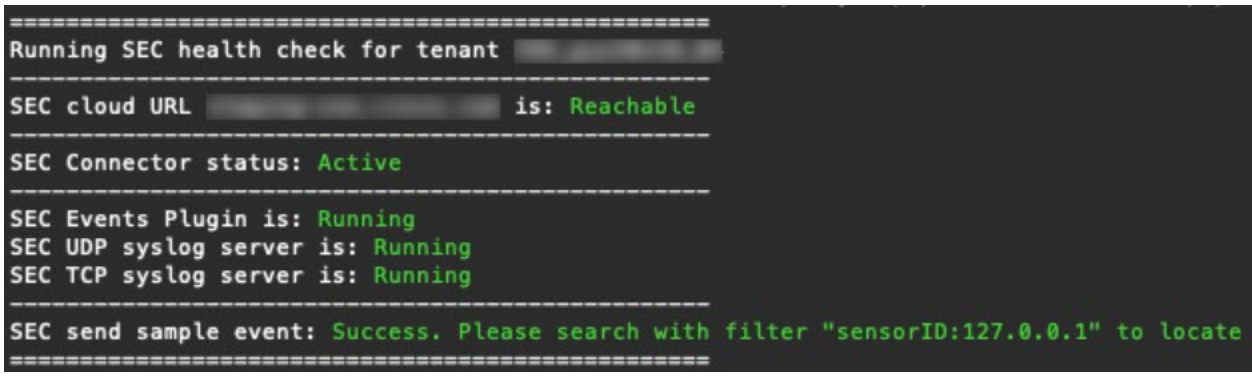
步骤 7 在提示符后，运行 **sec.sh setup** 脚本：

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

步骤 8 在提示符的末尾，粘贴您在步骤 4 中复制的引导程序数据，然后按 **Enter**键。

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

载入 SEC 后，sec.sh 将运行脚本来检查 SEC 的运行状况。如果所有运行状况检查均为“绿色”，则运行状况检查会向事件日志发送示例事件。示例事件在事件日志中显示为名为“sec-health-check”的策略。



如果您收到注册失败或 SEC 载入失败的消息，请转至安全事件连接器载入故障排除。

步骤 9 确定运行 SDC 和 SEC 的虚拟机是否需要额外配置：

- 如果您在自己的虚拟机上安装了 SDC，请继续 您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置，第 614 页。
- 如果您使用 CDO 映像安装了 SDC，请继续执行“下一步”。

下一步做什么

退回至 为 FDM 管理 设备实施安全日志记录分析 (SaaS)，第 594 页。

相关信息：

- 对安全设备连接器进行故障排除，第 699 页
- 安全事件连接器故障排除
- 安全事件连接器载入故障排除
- 安全事件连接器注册失败故障排除，第 707 页

使用 CDO 映像安装 SEC

安全事件连接器 (SEC) 将事件从 ASA 和 FTD 转发到思科云，以便您可以在“事件日志记录”页面中查看它们，并根据您的许可使用安全云分析进行调查。

您可以在租户上安装多个安全事件连接器 (SEC)，并将事件从您的 ASA 和 FDM 托管的设备定向到您安装的任何 SEC。拥有多个 SEC 可让您将 SEC 安装在不同的位置，并将事件发送到思科云的工作分发给他们。

安装 SEC 的过程分为两部分：

1. 使用 CDO VM 映像安装 CDO 连接器，以便支持安全事件连接器，第 604 页 您安装的每个 SEC 都需要一个 CDO 连接器。CDO 连接器不同于安全设备连接器 (SDC)。
2. 在 CDO 连接器虚拟机上安装安全事件连接器，第 615 页。

注释 如果要通过创建自己的 VM 来创建 CDO 连接器，请参阅您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置。

后续操作：

继续执行 使用 CDO VM 映像安装 CDO 连接器，以便支持安全事件连接器，第 604 页

使用 CDO VM 映像安装 CDO 连接器，以便支持安全事件连接器

开始之前

- 购买思科安全和分析日志记录、**日志记录和故障排除**许可证，您还可以购买**日志记录分析和检测**以及**全面网络分析和监控**许可证，以便将安全云分析应用于事件。

  如果愿意，您还可以登录 CDO，然后在主导航栏中选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)** 并点击**请求试用 (Request Trial)**，以便申请获取试用版的安全分析和日志记录。
- CDO 需要进行严格的证书检查，并且不支持 CDO 连接器和互联网之间的 Web/内容代理检查。如果使用代理服务器，请禁用对 CDO 连接器和 CDO 之间的流量进行检查。
- **此进程中安装的 CDO 连接器必须在 TCP 端口 443 上具有对互联网的完全出站访问权限。**
- **查看** 将 思科防御协调器 连接到托管设备，**以便确保 CDO 连接器能够正确访问网络。**
- CDO 支持使用 vSphere Web 客户端或 ESXi Web 客户端来安装其 CDO 连接器 VM OVF 映像。
- CDO 不支持使用 VM vSphere 桌面客户端来安装 CDO 连接器 VM OVF 映像。
- ESXi 5.1 虚拟机监控程序。
- 仅用于托管 CDO 连接器和 SEC 的 VM 的系统要求：
  - VMware ESXi 主机需要 4 个 vCPU。
  - VMware ESXi 主机至少需要 8GB 内存。
  - VMware ESXi 需要 64GB 磁盘空间来支持虚拟机，具体取决于您的调配选择。
- 在开始安装之前收集以下信息：
  - 要用于 CDO 连接器虚拟机的静态 IP 地址。
  - 您在安装过程中创建的 **root** 和 **cdo** 用户的密码。
  - 您的组织使用的 DNS 服务器的 IP 地址。
  - SDC 地址所在网络的网关 IP 地址。

- 时间服务器的 FQDN 或 IP 地址。

- CDO 连接器虚拟机被配置为定期安装安全补丁，为此需要打开出站端口 80。

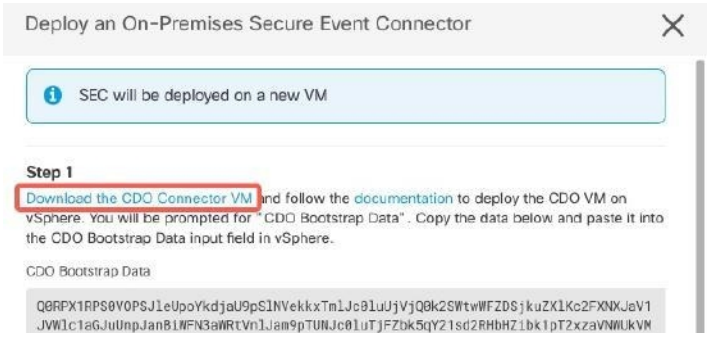
过程

步骤 1 登录到要为其创建 CDO 连接器的 CDO 租户。

步骤 2 从 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

步骤 3 点击蓝色加号按钮，然后点击**安全事件连接器 (Secure Event Connector)**。

步骤 4 在步骤 1 中，点击**下载 CDO 连接器虚拟机映像 (Download the CDO Connector VM image)**。这是您在上面安装 SEC 的特殊映像。始终下载 CDO 连接器虚拟机，以确保使用的是最新映像。



步骤 5 从 zip 文件中提取所有文件。它们看起来和下面有些相似：

- CDO-SDC-VM-ddd50fa.ovf
- CDO-SDC-VM-ddd50fa.mf
- CDO-SDC-VM-ddd50fa-disk1.vmdk

步骤 6 使用 vSphere Web 客户端以管理员身份登录 VMware 服务器。

注释 请勿使用 VM vSphere 桌面客户端。

步骤 7 按照相关提示从 OVF 模板部署本地 CDO 连接器虚拟机。（您将需要 .ovf、.mf 和 .vdk 文件才能部署模板。）

步骤 8 在设置完成后，打开虚拟机电源。

步骤 9 打开新 CDO 连接器虚拟机的控制台。

步骤 10 以 **cdo** 用户的身份登录。默认密码为 `adm123`。

步骤 11 在提示符处键入 `sudo sdc-onboard setup`

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

步骤 12 出现提示时，输入 cdo 用户的默认密码：`adm123`。

步骤 13 按照提示为 **root** 用户创建一个新密码。

步骤 14 按照提示为 **cdo** 用户创建一个新密码。

步骤 15 按照提示输入 Cisco Defense Orchestrator 的域信息。

步骤 16 输入您要用于 CDO 连接器虚拟机的静态 IP 地址。

步骤 17 输入要在上面安装 CDO 连接器虚拟机的网络的网关 IP 地址。

步骤 18 输入 CDO 连接器的 NTP 服务器地址或 FQDN。

步骤 19 出现提示时，输入 Docker 网桥的信息，如果不适用，则可将其留空，然后按 <Enter>。

步骤 20 确认您的输入内容。

步骤 21 当系统提示“您想立即设置 SDC 吗？”(Would you like to setup the SDC now?) 时输入 **n**。

步骤 22 以 **cdo** 用户身份登录，以便创建与 CDO 连接器的 SSH 连接。

步骤 23 在提示符处键入 **`sudo sdc-onboard bootstrap`**

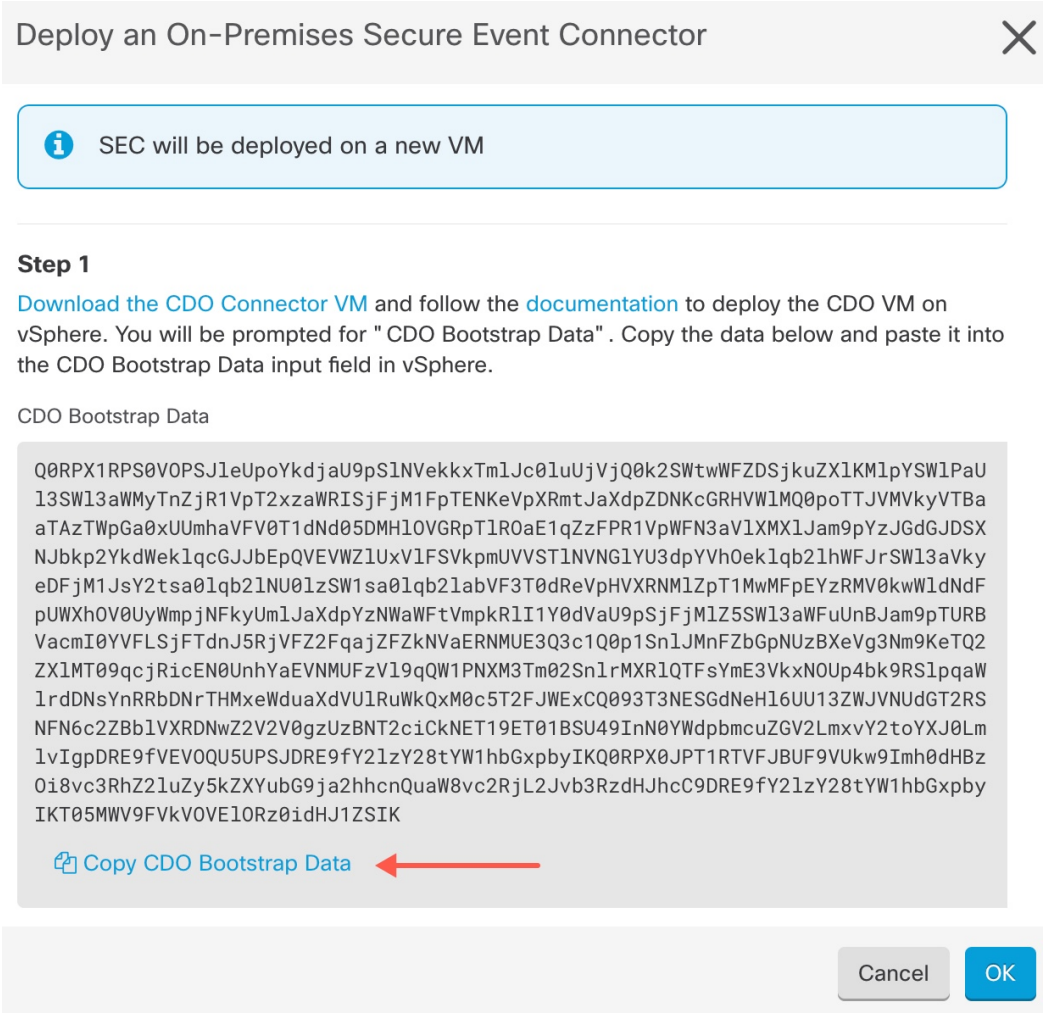
```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

步骤 24 在出现提示时，请输入 cdo 用户的密码。

步骤 25 在出现提示时，返回 CDO 并复制 CDO 引导程序数据，然后将其粘贴到 SSH 会话中。要复制 CDO 引导程序数据，请执行以下操作：

1. 登录 CDO。
2. 从 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。
3. 选择您开始载入的安全事件连接器。状态应显示为“正在载入”(Onboarding)。
4. 在“操作”(Actions) 窗格中，点击**部署本地安全事件连接器 (Deploy an On-Premises Secure Event Connector)**。

5. 复制对话框步骤 1 中的 CDO 引导程序数据。



步骤 26 当系统提示**您是否要更新这些设置时？(Would you like to update these settings?)** 输入 **n**。

步骤 27 返回 CDO 中的“部署本地安全事件连接器对话框”(Deploy an On-Premises Secure Event Connector)，然后点击**确定 (OK)**。在“安全连接器”(Secure Connectors) 页面上，您会看到安全事件连接器处于黄色的正在载入状态。

下一步做什么

请继续在 CDO 连接器虚拟机上安装安全事件连接器，第 608 页。

在 CDO 连接器虚拟机上安装安全事件连接器

开始之前

您应该已安装 CDO 连接器虚拟机，如使用 CDO VM 映像安装 CDO 连接器，以便支持安全事件连接器，第 604 页中所述。

过程

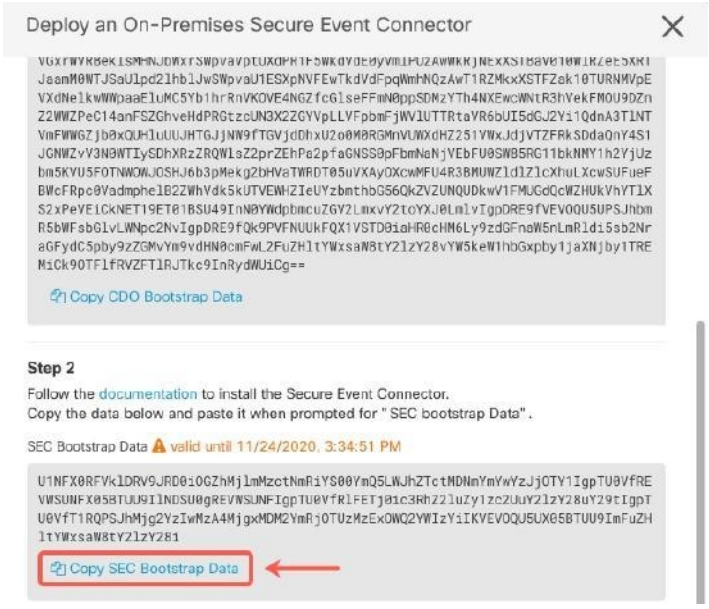
步骤 1 登录 CDO。

步骤 2 从 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

步骤 3 选择您在上面载入的 CDO 连接器。在“安全连接器”(Secure Connectors) 表中，它将被称为“安全事件连接器”，并且应仍处于“正在载入”状态。

步骤 4 点击右侧“操作”(Actions) 窗格中的**部署现场安全事件连接器 (Deploy an On-Premises Secure Event Connector)** 。

步骤 5 在向导的**步骤 2** 中，点击**复制 SEC 引导程序数据 (Copy SEC bootstrap data)** 的链接。



步骤 6 创建与 CDO 连接器的 SSH 连接，并以 **cdo** 用户身份登录。

步骤 7 登录后，切换到 **sdc** 用户。当系统提示输入密码时，请输入“cdo”用户的密码。以下是这些命令的示例：

```
[cdo@sdc-vm ~]$ sudo su sdc
 [sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

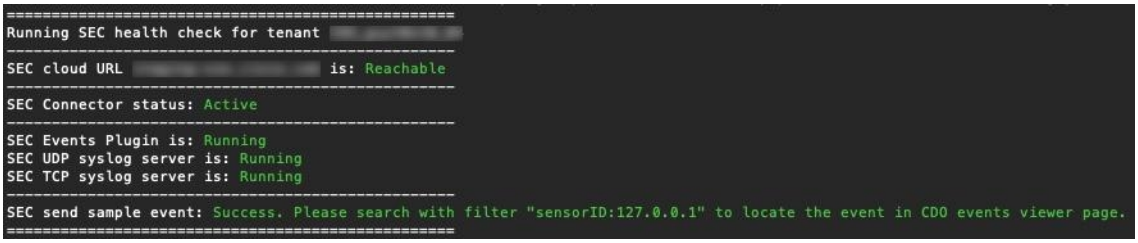
步骤 8 在提示符后，运行 sec.sh 安装脚本：

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

步骤 9 在提示符的末尾，粘贴您在步骤 4 中复制的引导程序数据，然后按 **Enter**键。

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
 RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

载入 SEC 后，sec.sh 将运行脚本来检查 SEC 的运行状况。如果所有运行状况检查均为“绿色”，则运行状况检查会向事件日志发送示例事件。示例事件在事件日志中显示为名为“sec-health-check”的策略。



如果您收到注册失败或 SEC 载入失败的消息，请转至安全事件连接器载入故障排除，第 704 页。

如果您收到成功消息，请返回 CDO 并点击**完成部署现场安全事件连接器 (Done on the Deploy an ON-Premise Secure Event Connector)** 对话框。

步骤 10 继续“下一步做什么。"

下一步做什么

退回至 为 FDM 管理 设备实施安全日志记录分析 (SaaS)，第 594 页。

相关信息：

- 对安全设备连接器进行故障排除，第 699 页
- 安全事件连接器故障排除，第 703 页
- 安全事件连接器载入故障排除，第 704 页

使用 VM 映像安装 SEC

安全事件连接器 (SEC) 将事件从 ASA 和 FTD 转发到思科云，以便您可以在“事件日志记录”页面中查看它们，并根据您的许可使用安全云分析进行调查。

您可以在租户上安装多个安全事件连接器 (SEC)，并将事件从您的 ASA 和 FDM 托管的设备定向到您安装的任何 SEC。拥有多个 SEC 可让您在不同区域安装 SEC，并将事件发送到思科云的工作分发给他们。

使用您自己的 VM 映像安装多个 SEC 的过程分为三部分。您必须执行以下每个步骤：

1. 使用 VM 映像安装 CDO 连接器以支持 SEC，第 610 页
2. 使用 您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置，第 614 页对虚拟机执行一些额外的配置步骤

3. 在 CDO 连接器虚拟机上安装安全事件连接器

注释 将 CDO VM 映像用于 CDO 连接器是安装 CDO 连接器的最简单、最准确和首选的方法。如果要使用该方法，请参阅使用 CDO 映像安装 SEC，第 603 页。

后续操作：

请继续使用 VM 映像安装 CDO 连接器以支持 SEC，第 610 页

使用 VM 映像安装 CDO 连接器以支持 SEC

CDO 连接器 VM 是安装 SEC 的虚拟机。CDO 连接器仅用于为思科安全分析和日志记录 (SaaS) 客户提供 SEC 支持。

开始之前

- 购买思科安全和分析日志记录、**日志记录和故障排除**许可证，您还可以购买**日志记录分析和检测**以及**全面网络分析和监控**许可证，以将安全云分析应用于事件。

  如果愿意，您还可以登录 CDO，然后在主导航栏中选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)** 并点击**请求试用 (Request Trial)**，以便申请获取试用版的安全分析和日志记录。

- CDO 需要严格的证书检查，并且不支持 CDO 连接器和互联网之间的 Web/内容代理。
- **CDO 连接器必须在 TCP 端口 443 上具有对互联网的完全出站访问权限。**
- **查看** 将 思科防御协调器 连接到托管设备**以确保对 CDO 连接器进行适当的网络访问。**
- 安装了 vCenter Web 客户端或 ESXi Web 客户端的 VMware ESXi 主机。

注释 我们不支持使用 vSphere 桌面客户端进行安装。

- ESXi 5.1 虚拟机监控程序。
- Cent OS 7 访客操作系统。
- 仅托管 CDO 连接器和 SEC 的 VM 的系统要求：
  - CPU：分配 4 个 CPU 以容纳 SEC。
  - 内存：为 SEC 分配 8 GB 内存。
  - 磁盘空间：64 GB
- 执行此过程的用户应该能够轻松地在 Linux 环境中使用 **vi** 可视化编辑器编辑文件。
- 如果您在 CentOS 虚拟机上安装 CDO 连接器，我们建议您定期安装 Yum 安全补丁。根据您的 Yum 配置，要获取 Yum 更新，您可能需要在端口 80 和 443 上打开出站访问。您还需要配置

yum-cron 或 crontab 来安排更新。与您的安全运营团队合作，确定是否需要更改任何安全策略以允许您获取 Yum 更新。

- 在开始安装之前收集以下信息：
  - 要用于 CDO 连接器的静态 IP 地址。
  - 您在安装过程中创建的 **root** 和 **cdo** 用户的密码。
  - 您的组织使用的 DNS 服务器的 IP 地址。
  - CDO 连接器地址所在网络的网关 IP 地址。
  - 时间服务器的 FQDN 或 IP 地址。
- CDO 连接器虚拟机被配置为定期安装安全补丁，为此需要打开出站端口 80。
- **开始之前**：不要将本程序中的命令复制并粘贴到终端窗口中，而应键入这些命令。某些命令包括“n-dash”，在剪切和粘贴过程中，这些命令可以作为“m-dash”应用，这可能会导致命令失败。

过程

步骤 1 在安全设备连接器页面中，点击蓝色加号按钮  ，然后点击安全事件连接器。

步骤 2 使用提供的链接，复制“部署现场安全事件连接器”(Deploy an On-Premises Secure Event Connector) 窗口的步骤 2 中的 SEC 引导程序数据。

步骤 3 安装 CentOS 7 虚拟机 (http://isoredirect.centos.org/centos/7/isos/x86_64/CentOS-7-x86_64-Minimal-1804.iso)，其内存、CPU 和磁盘空间至少应符合此程序的要求。

步骤 4 安装后，配置基本网络，例如指定 CDO 连接器的 IP 地址、子网掩码和网关。

步骤 5 配置 DNS（域名服务器）服务器。

步骤 6 配置 NTP（网络时间协议）服务器。

步骤 7 在 CentOS 上安装 SSH 服务器，以便与 CDO 连接器的 CLI 轻松交互。

步骤 8 运行 yum 更新，然后安装软件包： **open-vm-tools**、 **nettools** 和 **bind-utils**

```
[root@sdc-vm ~]# yum update -y
[root@sdc-vm ~]# yum install -y open-vm-tools net-tools bind-utils
```

步骤 9 安装 **AWS CLI 软件包** (https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html)

注释 请勿使用 `--user` 标志。

步骤 10 安装 **Docker CE 软件包** (https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce)

注释 使用“使用存储库安装”方法。

步骤 11 启动 Docker 服务并使其在启动时启动：

```
[root@sdc-vm ~]# systemctl start docker
 [root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service to
/usr/lib/systemd/system/docker.service.
```

步骤 12 创建两个用户： **cdo** 和 **sdc**。cdo 用户将是您登录以运行管理功能的用户（因此您无需直接使用 root 用户），sdc 用户将是运行 CDO 连接器 docker 容器的用户。

```
[root@sdc-vm ~]# useradd cdo
 [root@sdc-vm ~]# useradd sdc -d /usr/local/cdo
```

步骤 13 为 cdo 用户设置密码。

```
[root@sdc-vm ~]# passwd cdo
Changing password for user cdo.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```

步骤 14 将 cdo 用户添加到“wheel”组，为其提供管理 (sudo) 权限。

```
[root@sdc-vm ~]# usermod -aG wheel cdo
 [root@sdc-vm ~]#
```

步骤 15 安装 Docker 时，会创建一个用户组。根据 CentOS/Docker 的版本，它可能被称为 “docker” 或 “dockerroot”。检查 /etc/group 文件以查看创建的组，然后将 sdc 用户添加到此组。

```
 [root@sdc-vm ~]# grep docker /etc/group
docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

步骤 16 如果 `/etc/docker/daemon.json` 文件不存在，请创建该文件，并使用以下内容填充。创建后，重新启动 Docker 后台守护程序。

注释 确保在 "组" 项中输入的组名称与步骤 15匹配。

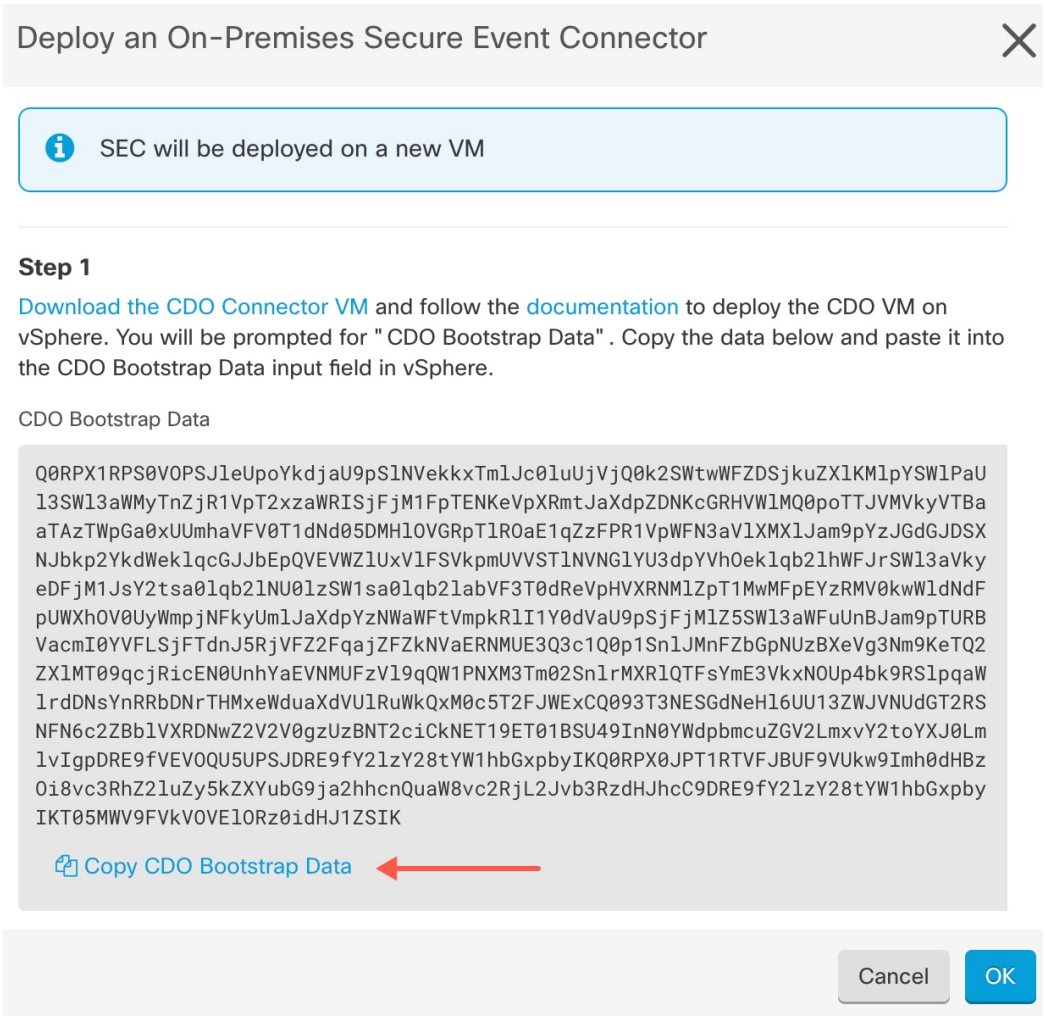
```
 [root@sdc-vm ~]# cat /etc/docker/daemon.json
{
 "live-restore": true,
 "group": "docker"
}
[root@sdc-vm ~]# systemctl restart docker
[root@sdc-vm ~]#
```

步骤 17 如果您当前使用的是 vSphere 控制台会话，请切换到 SSH 并以 **cdo** 用户身份登录。登录后，更改为 **sdc** 用户。当系统提示输入密码时，请输入 **cdo** 用户的密码。

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

步骤 18 将目录更改为 **/usr/local/cdo**。

步骤 19 创建一个名为 **bootstrapdata** 的新文件，并将部署向导步骤 1 中的引导程序数据粘贴到此文件中。保存文件。您可以使用 **vi** 或 **nano** 创建该文件。



步骤 20 引导程序数据采用 base64 编码。对其进行解码并将其导出到名为 **extractedbootstrapdata** 的文件

```
 [sdc@sdc-vm ~]$ base64 -d /usr/local/cdo/bootstrapdata >
/usr/local/cdo/extractedbootstrapdata
[sdc@sdc-vm ~]$
```

运行 cat 命令以查看解码后的数据。命令和解码后的数据应如下所示：

```
[sdc@sdc-vm ~]$ cat /usr/local/cdo/extractedbootstrapdata
CDO_TOKEN="<token string>"
CDO_DOMAIN="www.defenseorchestrator.com"
CDO_TENANT="<tenant-name>"
CDO_BOOTSTRAP_URL="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"

ONLY_EVENTING="true"
```

步骤 21 运行以下命令，将解码的引导程序数据部分导出到环境变量。

```
 [sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > sdcenv && source sdcenv
[sdc@sdc-vm ~]$
```

步骤 22 从 CDO 下载引导程序捆绑包。

```
 [sdc@sdc-vm ~]$ curl -O -H "Authorization: Bearer $CDO_TOKEN" "$CDO_BOOTSTRAP_URL"
100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
[sdc@sdc-vm ~]$ ls -l /usr/local/cdo/*SDC
-rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/cdo/tenant-name-SDC
```

步骤 23 解压缩 CDO 连接器 tarball，并运行 bootstrap_sec_only.sh 文件以安装 CDO 连接器软件包。

```
 [sdc@sdc-vm ~]$ tar xzvf /usr/local/cdo/tenant-name-SDC
<snipped - extracted files>
[sdc@sdc-vm ~]$
[sdc@sdc-vm ~]$ /usr/local/cdo/bootstrap/bootstrap_sec_only.sh
[2018-07-23 13:54:02] environment properly configured
download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
toolkit.sh
common.sh
es_toolkit.sh
sec.sh
healthcheck.sh
troubleshoot.sh
no crontab for sdc
-bash-4.2$ crontab -l
*/5 * * * * /usr/local/cdo/toolkit/es_toolkit.sh upgradeEventing 2>&1 >>
/usr/local/cdo/toolkit/toolkit.log
0 2 * * * sleep 30 && /usr/local/cdo/toolkit/es_toolkit.sh es_maintenance 2>&1 >>
/usr/local/cdo/toolkit/toolkit.log
You have new mail in /var/spool/mail/sdc
```

下一步做什么

请继续 您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置，第 614 页。

您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置

如果您在自己的 CentOS 7 虚拟机上安装了 CDO 连接器，则需要执行以下附加配置程序**之一**，以允许事件到达 SEC。

- 在 CentOS 7 虚拟机上禁用 firewalld 服务。这与思科提供的 SDC VM 的配置相匹配。
- 允许 firewalld 服务运行并添加防火墙规则以允许事件流量到达 SEC，第 615 页。这是一种允许入站事件流量的更精细的方法。

在 CentOS 7 虚拟机上禁用 firewalld 服务

1. 以“cdo”用户身份登录 SDC VM 的 CLI。
2. 停止 firewalld 服务，然后确保该服务在 VM 后续重新启动时保持禁用。如果系统提示，请输入 **cdo** 用户的密码：

   ```
   [cdo@SDC-VM ~]$ sudo systemctl stop firewalld
   cdo@SDC-VM ~]$ sudo systemctl disable firewalld
   ```

3. 重新启动 Docker 服务，以便将 Docker 特定条目重新插入本地防火墙：

   ```
   [cdo@SDC-VM ~]$ sudo systemctl restart docker
   ```

4. 请继续在 CDO 连接器虚拟机上安装安全事件连接器，第 615 页。

允许 firewalld 服务运行并添加防火墙规则以允许事件流量到达 SEC

1. 以“cdo”用户身份登录 SDC VM 的 CLI。
2. 添加本地防火墙规则，以便允许从配置的 TCP、UDP 或 NSEL 端口到 SEC 的传入流量。有关 SEC 使用的端口，请参阅查找用于安全日志记录分析 (SaaS) 的设备 TCP、UDP 和 NSEL 端口。如果系统提示，请输入 **cdo** 用户的密码。以下是命令的示例。您可能需要指定不同的端口值。

```
[cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10125/tcp
cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10025/udp
[cdo@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent --add-port=10425/udp
```

3. 重新启动 firewalld 服务，以便让新的本地防火墙规则始终保持激活：

```
[cdo@SDC-VM ~]$ sudo systemctl restart firewalld
```

4. 请继续在 CDO 连接器虚拟机上安装安全事件连接器，第 615 页。

在 CDO 连接器虚拟机上安装安全事件连接器

开始之前

执行以下两项任务：

- 使用 VM 映像安装 CDO 连接器以支持 SEC，第 610 页
- 您创建的 VM 上安装的 SDC 和 CDO 连接器的其他配置，第 614 页

过程

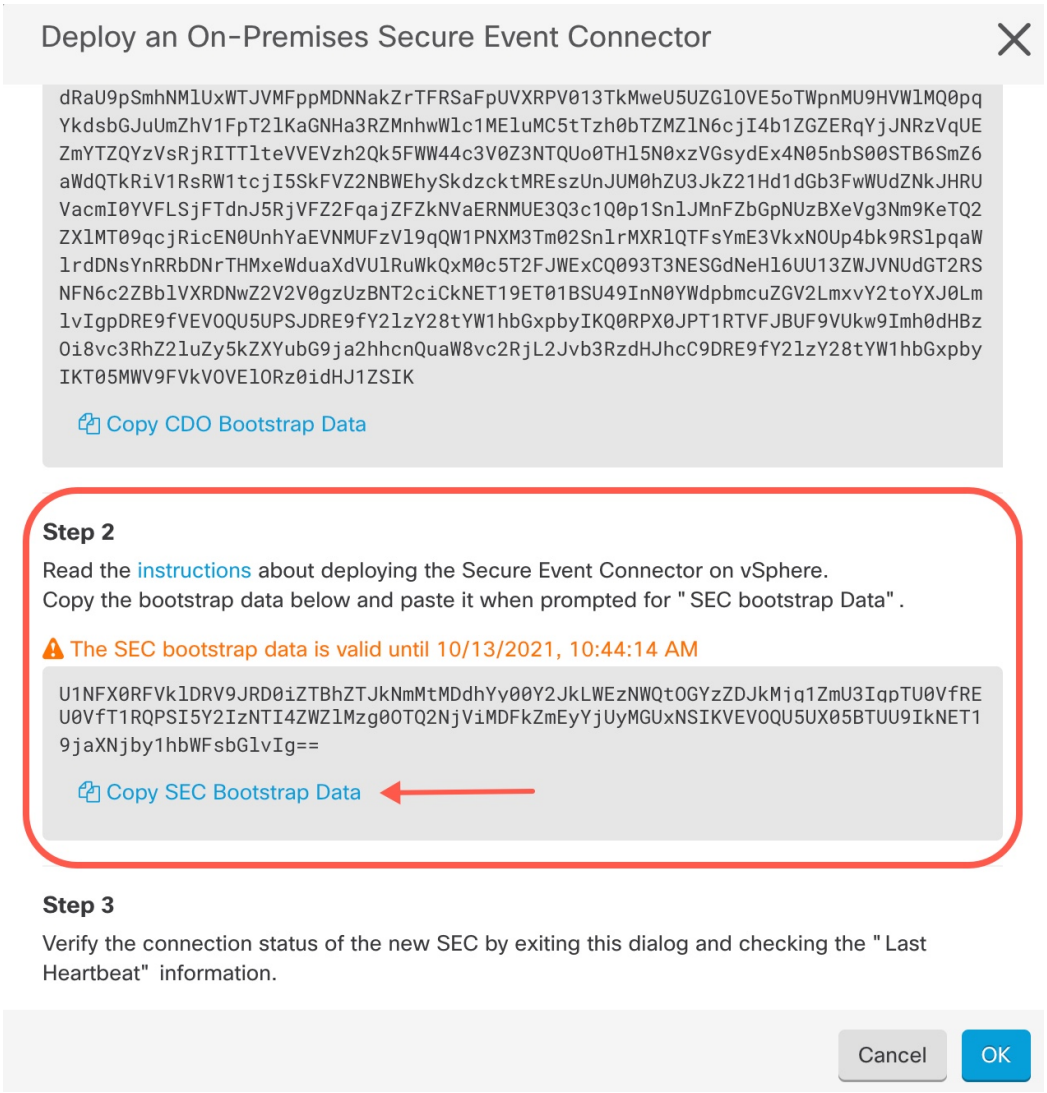
步骤 1 登录 CDO。

步骤 2 从 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

步骤 3 选择您使用上述必备条件中的程序安装的 CDO 连接器。在“安全连接器”(Secure Connectors) 表中，它将被称为“安全事件连接器”(Secure Event Connector)。

步骤 4 点击右侧“操作”窗格中的 **部署现场安全事件连接器** 。

步骤 5 在向导的 步骤 2 中，点击**复制 SEC 引导程序数据 (Copy SEC Bootstrap Data)** 的链接。



步骤 6 使用 SSH 连接到安全连接器并以 **cdo** 用户身份登录。

步骤 7 登录后，切换到 **sdc** 用户。当系统提示输入密码时，请输入“cdo”用户的密码。以下是这些命令的示例：

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

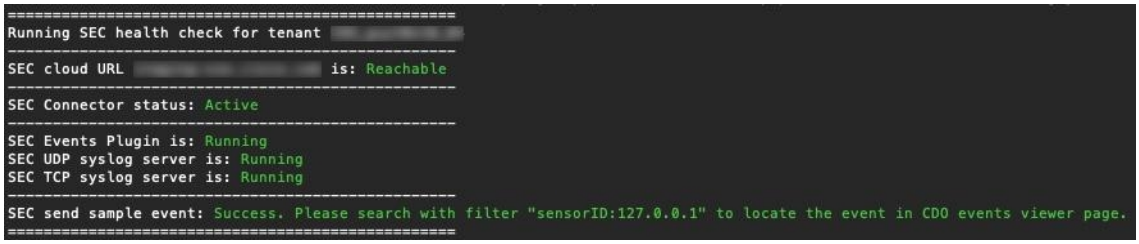
步骤 8 在提示符后，运行 sec.sh 安装脚本：

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

步骤 9 在提示符的末尾，粘贴您在步骤 4 中复制的引导程序数据，然后按 **Enter**键。

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
 KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

载入 SEC 后，sec.sh 将运行脚本来检查 SEC 的运行状况。如果所有运行状况检查均为“绿色”，则运行状况检查会向事件日志发送示例事件。示例事件在事件日志中显示为名为“sec-health-check”的策略。



如果您收到注册失败或 SEC 载入失败的消息，请转至安全事件连接器故障排除。

如果您收到成功消息，请点击**部署现场安全事件连接器 (Deploy an ON-Premise Secure Event Connector)** 对话框中的**完成 (Done)**。您已在虚拟机映像上安装 SEC。

步骤 10 继续执行 “**下一步操作**”。

下一步做什么

返回此程序以继续实施 SAL SaaS： 为 FDM 管理 设备实施安全日志记录分析 (SaaS)，第 594 页。

相关信息：

- 对安全设备连接器进行故障排除，第 699 页
- 安全事件连接器故障排除
- 安全事件连接器载入故障排除
- 安全事件连接器注册失败故障排除

使用 Terraform 模块在 AWS VPC 上安装安全事件连接器

开始之前

- 要执行此任务，您必须在 CDO 租户上启用 SAL。本部分假定您已拥有 SAL 许可证。如果还没有，请购买思科安全和分析日志记录、日志记录和故障排除许可证。
- 确保您已安装新的 SEC。要创建新的 SEC，请参阅在 SDC 虚拟机上安装安全事件连接器，第 600 页。
- 在安装 SEC 时，请确保记下 CDO 引导程序数据和 SEC 引导程序数据。

过程

步骤 1 转到 Terraform 注册表中的安全事件连接器 Terraform 模块，然后按照说明将 SEC Terraform 模块添加到 Terraform 代码。

步骤 2 应用 Terraform 代码。

步骤 3 确保打印 `instance_id` 和 `sec_fqdn` 输出，因为稍后在程序中会用到它们。

注释 要对 SEC 进行故障排除，您必须使用 AWS 系统管理器会话管理器 (SSM) 来连接到 SEC 实例。请参阅 AWS 系统管理器会话管理器文档，了解有关使用 SSM 连接到实例的更多信息。

出于安全原因，使用 SSH 连接到 SDC 实例的端口不会被公开。

步骤 4 要启用从 ASA 向 SEC 发送日志的功能，请使用步骤 3 的输出来运行以下命令，以获取您创建的 SEC 的证书链并删除枝叶证书：

```
rm -f /tmp/cert_chain.pem && openssl s_client -showcerts -verify 5 -connect <FQDN>:10125 <
 /dev/null | awk '/BEGIN CERTIFICATE/,/END CERTIFICATE/{ if(/BEGIN CERTIFICATE/){a++};
out="/tmp/cert_chain.pem"; if(a > 1) print >>out}'
```

步骤 5 将 `/tmp/cert_chain.pem` 的内容复制到剪贴板。

步骤 6 使用以下命令记录 SEC 的 IP 地址：

```
nslookup <FQDN>
```

步骤 7 登录 CDO 并开始添加新的信任点对象。有关详细信息，请参阅添加受信任 CA 证书对象。在点击**添加 (Add)**，请确保取消选中**其他选项 (Other Options)** 中的**在基本限制扩展中启用 CA 标志 (Enable CA flag in basic constraints extension)** 复选框。

步骤 8 点击**添加 (Add)**，复制 CDO 生成的 CLI 命令在**安装证书 (Install Certificate)** 页面中，然后点击**取消 (Cancel)**。

步骤 9 在`注册终端 (enrollment terminal)` 下方，在文本剪贴板中添加 `no ca-check`。

步骤 10 通过 SSH 连接到 ASA 设备或使用 CDO 中的 ASA CLI 选项并执行以下命令：

```
DataCenterFW-1> en
Password: ******************
DataCenterFW-1# conf t
DataCenterFW-1(config)# <paste your modified ASA CLIs here and press Enter>
DataCenterFW-1(config)# wr mem
Building configuration...
Cryptochecksum: 6634f35f 4c5137f1 ab0c5cdc 9784bdb6
```

下一步做什么

您可以使用 AWS SSM 来检查 SEC 是否正在接收数据包：

您现在应该会看到类似于以下内容的日志：

```
time="2023-05-10T17:13:46.135018214Z" level=info msg="[ip-10-100-5-19.ec2.internal][util.go:67
 plugin.createTickers:func1] Events - Processed - 6/s, Dropped - 0/s, Queue size - 0"
```

取消调配思科安全分析和日志记录 (SaaS)

如果允许思科安全分析和日志记录(SaaS)付费许可证失效，则您有90天的宽限期。如果您在此宽限期内续订付费许可证，则服务不会发生中断。

否则，如果您允许90天的宽限期，系统将清除所有的客户数据。您无法再从“事件日志记录”(Event Logging) 页面查看 ASA 或 FTD 事件，也无法将动态实体建模行为分析应用于您的 ASA 或 FTD 事件和网络流数据。

删除安全事件连接器

警告：此程序会从安全设备连接器中删除安全事件连接器。这样做会阻止您使用安全日志分析(SaaS)。这一操作不可逆。如果您有任何问题或疑虑，请在执行此操作之前联系思科威胁防御支持。

从安全设备连接器中删除安全事件连接器的过程可分为两步：

1. 从 CDO 中删除 SEC。
2. 从 SDC 中删除 SEC 文件。

下一步：继续从 CDO 中删除 SEC

从 CDO 中删除 SEC

开始之前

请参阅删除安全事件连接器 ， 第 619 页。

过程

步骤 1 登录 CDO。

步骤 2 从 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

步骤 3 选择设备类型为**安全事件连接器 (Secure Event Connector)** 的行。

警告：要小心。请勿选择您的安全设备连接器。

步骤 4 在“操作”(Actions) 窗格中，点击**删除 (Remove)**。

步骤 5 点击**确定 (OK)** 以确认您删除安全事件连接器的意图。

下一步做什么

请继续从 SDC 中删除 SEC 文件 ， 第 620 页。

从 SDC 中删除 SEC 文件

这是从 SDC 中删除安全事件连接器程序的第二部分。开始前，请参阅删除安全事件连接器，第 619 页。

过程

步骤 1 打开虚拟机监控程序并启动 SDC 的控制台会话。

步骤 2 切换到 SDC 用户。

```
[cdo@tenant toolkit]$sudo su sdc
```

步骤 3 在提示符后键入以下命令之一：

- 如果您仅管理自己的租户：

  ```
  [sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove
  ```

- 如果您管理多个租户，请将 CDO_ 添加到租户名称的开头。例如：

  ```
  [sdc@tenant toolkit]$ /usr/local/cdo/toolkit/sec.sh remove CDO_[tenant_name]
  ```

步骤 4 确认您打算删除 SEC 文件。

调配思科安全云分析门户

所需许可证： 日志记录分析和检测 或 全面网络分析和监控

如果您购买了**日志记录分析和检测**或**全局网络分析和监控**许可证，则在部署和配置安全事件连接器 (SEC) 后，必须将安全云分析门户与 CDO 门户关联，以查看安全云分析警报。购买许可证时，如果您有安全云分析门户，则可以提供安全云分析门户名称，并立即将其链接到您的 CDO 门户。

否则，您可以从 CDO UI 请求新的安全云分析门户。首次访问安全云分析警报时，系统会将您引导至请求安全云分析门户的页面。向请求此门户的用户授予门户中的管理员权限。

Procedure

步骤 1 从 CDO 菜单中，选择 **分析 (Analytics)** > **安全云分析 (Secure Cloud Analytics)** 以在新窗口中打开安全云分析 UI。

步骤 2 点击**开始免费试用 (Start Free Trial)** 以调配安全云分析门户并将其与您的 CDO 门户关联。

Note 请求门户后，调配可能需要几个小时。

在继续下一步之前，请确保您的门户已调配。

1. 从 CDO 菜单中，选择 **分析 (Analytics)** > **安全云分析 (Secure Cloud Analytics)** 以在新窗口中打开安全云分析 UI。
2. 您有以下选择：
   - 如果您请求了安全云分析门户，并且系统指出它仍在调配门户，请稍后再尝试访问警报。
   - 如果已调配安全云分析门户，请输入您的**用户名**和**密码**，然后点击**登录 (Sign in)**。

Note 管理员用户可以邀请其他用户在安全云分析门户中创建账户。有关详细信息，请参阅从 CDO 查看 Cisco Secure Cloud Analytics 警报, on page 622。

What to do next

- 如果您购买了**日志记录分析和检测**许可证，则配置已完成。如果要从安全云分析门户 UI 查看 CDO 集成状态或传感器运行状况，请参阅在安全云分析中查看传感器运行状况和 CDO 集成状态, on page 621了解更多信息。如果要使用安全云分析门户中的警报，请参阅从 CDO 查看 Cisco Secure Cloud Analytics 警报, on page 622和使用基于防火墙事件的警报以了解详细信息。
- 如果您购买了**全面网络分析和监控**许可证，请将一个或多个安全云分析传感器部署到您的内部网络，以将网络流数据传递到云。如果要监控基于云的网络流数据，请将基于云的部署配置为将流数据传递到安全云分析。有关详细信息，请参阅用于全面网络分析和报告的思科安全云分析传感器部署, on page 622。

在安全云分析中查看传感器运行状况和 CDO 集成状态

传感器状态

所需许可证： 日志记录分析和检测 或 全面网络分析和监控

在思科安全云分析 Web UI 中，您可以从“传感器列表”(Sensor List) 页面查看 CDO 集成状态和已配置的传感器。CDO 集成是只读连接事件传感器。Stelathwatch 云在主菜单中提供传感器的整体运行状况：

- 绿色云图标 ( ) - 已与所有传感器和 CDO（如果已配置）建立连接
- 黄色云图标 ( ) - 已与某些传感器或 CDO（如果已配置）建立连接，但一个或多个传感器未正确配置
- 红色云图标 ( ) - 与所有已配置的传感器和 CDO（如果已配置）的连接丢失

每个传感器或 CDO 集成，绿色图标表示连接已建立，红色图标表示连接丢失。

过程

步骤 1 1. 在安全云分析门户 UI 中，选择设置 (⚙) > **传感器 (Sensors)**。

步骤 2 选择**传感器列表 (Sensor List)**。

用于全面网络分析和报告的思科安全云分析传感器部署

安全云分析传感器概述和部署

所需许可证：全面网络分析和监控

如果您获得了**全面网络分析和监控**许可证，则在调配安全云分析门户后，您可以：

- 在本地网络中部署和配置安全云分析传感器，以将网络流数据传递到云进行分析。
- 配置基于云的部署，以将网络流日志数据传递到安全云分析进行分析。

网络边界的防火墙收集有关内部网络和外部网络之间流量的信息，而安全云分析传感器收集有关内部网络流量的信息。

Note FDM 管理Secure Firewall Threat Defense 设备可以配置为传递 NetFlow 数据。部署传感器时，请勿将其配置为从您还配置为将事件信息传递到 CDO 的任何 FDM 管理Secure Firewall Threat Defense 设备传递 NetFlow 数据。

有关传感器部署说明和建议，请参阅《安全云分析传感器安装指南》。

有关基于云的部署配置说明和建议，请参阅《安全云分析公共云监控指南》。

Note 您还可以查看安全云分析门户 UI 中的说明，以配置传感器和基于云的部署。

有关安全云分析的详细信息，请参阅《安全云分析免费试用指南》。

后续步骤

- 继续执行从 CDO 查看 Cisco Secure Cloud Analytics 警报, on page 622。

从 CDO 查看 Cisco Secure Cloud Analytics 警报

所需许可证： 日志记录分析和检测 或 全面网络分析和监控

虽然您可以在“事件日志记录”(Events logging) 页面上查看防火墙事件，但无法从 CDO 门户 UI 中查看 Cisco Secure Cloud Analytics 警报。您可以使用“安全分析”(Security Analytics) 菜单选项从 CDO 交叉启动安全云分析门户，并查看从防火墙事件数据（如果启用了**全面网络分析和监控 (Total Network Analytics and Monitoring)**，则从网络流数据）生成的警报。“安全分析”(Security Analytics) 菜单选项会显示一个标记，其中包含处于打开的工作流程状态的安全云分析警报的数量（如果有一个或多个）。

如果您使用安全分析和日志记录许可证生成安全云分析警报，并且已调配新的安全云分析门户，请登录 CDO，然后使用 Cisco Security Cloud Sign On 来启动安全云分析。您还可以通过其 URL 直接访问安全云分析门户。

有关详细信息，请参阅 Cisco Security Cloud Sign On。

邀请用户加入您的安全云分析门户

请求安全云分析门户调配的初始用户在安全云分析门户中具有管理员权限。该用户可以通过邮件邀请其他用户加入门户。如果这些用户没有 Cisco Security Cloud Sign On 凭证，可以使用邀请邮件中的链接创建这些凭证。然后，用户可以在从 CDO 到 Secure Cloud Analytics 的交叉启动期间使用 Cisco Security Cloud Sign On 凭证登录。

要通过邮件邀请其他用户访问 Secure Cloud Analytics 门户，请执行以下操作：

Procedure

步骤 1 以管理员身份登录 Secure Cloud Analytics 门户。

步骤 2 选择 Settings Account Management User Management。 > >

步骤 3 输入**邮件**地址。

步骤 4 点击**邀请 (Invite)**。

从 CDO 交叉启动到 Cisco Secure Cloud Analytics

要从 CDO 查看安全警报，请执行以下操作：

Procedure

步骤 1 登录到 CDO 门户。

步骤 2 从 CDO 菜单中，选择 **分析 (Analytics)** > **安全云分析 (Secure Cloud Analytics)**。

步骤 3 在 Cisco Secure Cloud Analytics 界面中，选择**监控 (Monitor)** > **警报 (Alerts)**。

思科安全云分析和动态实体建模

所需许可证 (Required License)：日志记录分析和检测 (Logging Analytics and Detection) 或**全面网络分析和监控 (Total Network Analytics and Monitoring)**

安全云分析是一种软件即服务 (SaaS) 解决方案，可用于监控您的本地和基于云的网络部署。通过从源（包括防火墙事件和网络流数据）收集有关网络流量的信息，它会创建有关流量的观察结果，并根据其流量模式自动识别网络实体的角色。使用此信息与其他威胁情报来源（例如 Talos）相结合，安全云分析会生成警报，警告可能存在恶意行为。除警报外，安全云分析还提供网络和主机可视性以及所收集的情景信息，为您研究警报和查找恶意行为的来源提供更好的基础。

动态实体建模

动态实体建模可通过对防火墙事件和网络流数据执行行为分析来跟踪网络状态。在 Cisco Secure Cloud Analytics 环境中，实体是指可以随时间推移进行跟踪的对象，例如网络上的主机或终端。动态实体建模根据实体传输的流量及其在网络上执行的活动，收集实体的相关信息。与**日志记录分析和检测**许可证集成的 Cisco Secure Cloud Analytics 可以从防火墙事件和其他流量信息中进行提取，以便确定实体通常传输的流量类型。如果您购买了**全面网络分析和监控**许可证，则 Cisco Secure Cloud Analytics 还可以在对实体流量进行建模时纳入 NetFlow 和其他流量信息。Cisco Secure Cloud Analytics 会随着时间的推移更新这些模型，因为实体会继续发送流量，并且可能会发送不同的流量，从而保持每个实体的最新模型。根据这些信息，Cisco Secure Cloud Analytics 可以识别：

- 实体的角色，即实体通常执行的操作的描述符。例如，如果实体发送通常与邮件服务器关联的流量，Cisco Secure Cloud Analytics 会为该实体分配邮件服务器角色。角色/实体关系可以是多对一，因为实体可以履行多种角色。
- 对实体的观察结果，即有关实体在网络上的行为的事实，例如与外部 IP 地址建立的心跳连接或与另一个实体建立的远程访问会话。如果与 CDO 集成，则可以从防火墙事件中获取这些事实。如果您还购买了**全面的网络分析和监控**许可证，则系统还可以从 NetFlow 获取事实，并从防火墙事件和 NetFlow 中生成观察结果。观察结果本身并不具有超出其所代表的事实的意义。一个典型的客户可能有数千个观察结果和若干个警报。

警报和分析

Cisco Secure Cloud Analytics 会根据角色、观察结果和其他威胁情报的组合生成警报，这些警报是可操作项目，代表系统标识的可能的恶意行为。请注意，一个警报可能代表多个观察结果。如果防火墙记录了与同一连接和实体相关的多个连接事件，则可能只会生成一个警报。

例如，新的内部设备观察结果本身并不构成可能的恶意行为。但是，随着时间的推移，如果实体传输的流量与域控制器一致，则系统会向该实体分配域控制器角色。如果实体随后使用异常端口与之前未建立连接的外部服务器建立了连接，并且传输了大量的数据，则系统将记录新的大型连接（外部）观察结果和异常域控制器观察结果。如果该外部服务器被识别为一个 Talos 监视列表，则所有这些信息的组合将导致 Cisco Secure Cloud Analytics 生成此实体行为的警报，从而提示您采取进一步措施来研究和补救恶意行为。

在 Cisco Secure Cloud Analytics Web 门户 UI 中打开警报时，您可以查看导致系统生成该警报的支持性观察结果。您还可以从这些观察结果中查看有关所涉实体的其他背景信息，包括它们传输的流量

以及外部威胁情报（如果可用）。您还可以查看实体涉及的其他观察结果和警报，然后确定此行为是否与其他潜在恶意行为相关。

请注意，在 Cisco Secure Cloud Analytics 中查看和关闭警报时，无法允许或阻止来自 Cisco Secure Cloud Analytics UI 的流量。如果在主动模式下部署设备，则必须更新防火墙访问控制规则以允许或阻止流量；如果在被动模式下部署防火墙，则必须更新防火墙访问控制规则。

使用基于防火墙事件的警报

所需许可证： 日志记录分析和检测 或 全面网络分析和监控

警报工作流程

警报的工作流程基于其状态。当系统生成警报时，其默认状态为“待处理”，并且未分配任何用户。当您查看警报总结时，默认情况下会显示所有待处理警报，因为这些是最需要关注的。

注意：如果您拥有**全面网络分析和监控**许可证，则警报可以基于从 NetFlow 生成的观察结果、从防火墙事件生成的观察结果或来自两个数据源的观察结果。

查看警报总结时，可以分配和标记警报，以及将其状态更新为初始分类。您可以使用过滤器和搜索功能查找特定警报，也可以显示不同状态的警报或具有不同标记或负责人的警报。您可以将警报的状态设置为“已暂停”，在这种情况下，警报要等暂停期过后才会重新显示在待处理警报列表中。您也可以移除警报的“已暂停”状态，使其再次显示为待处理警报。查看警报时，您可以将其分配给您自己或系统中的其他用户。用户可以搜索分配给其用户名的所有警报。

在警报摘要中，您可以查看警报详细信息页面。此页面允许您查看有关生成此警报的支持性观察结果的其他背景信息，以及有关此警报中涉及的实体的其他背景信息。这些信息可帮助您查明实际问题，以便进一步研究网络上的问题，并且有可能解决恶意行为。

当您在 CDO 中的 Stealthwatch 云 web 门户 UI 和网络中进行研究时，可以进行备注，描述您对警报的发现。这有助于为您的研究创建记录，供您将来参考。

完成分析后，您可以将状态更新为“已关闭”，使其不再默认显示为待处理警报。如果情况发生变化，您还可以在将来重新打开已关闭的警报。

下面介绍有关如何调查给定警报的一般准则和建议。Stealthwatch 云会在记录警报时提供附加背景信息，因此，您可以使用此信息帮助指导调查工作。

这些步骤既不全面，也非包罗万象。它们仅提供一个总体框架来帮助您开始调查警报。

通常，查看警报时可以采取以下步骤：

1. 对待处理警报进行分类, on page 626
2. 暂停警报以供以后分析, on page 626
3. 更新警报以进行进一步调查, on page 627
4. 查看警报并开始调查, on page 627
5. 检查实体和用户, on page 629

6. 使用安全云分析补救问题, on page 629
7. 更新并关闭警报, on page 630

对待处理警报进行分类

对待处理警报进行分类，特别是如果要调查多个待处理警报：

- 有关从 CDO 交叉启动和查看警报的详细信息，请参阅从 CDO 查看 Cisco Secure Cloud Analytics 警报。

询问以下问题：

- 您是否将此警报类型配置为高优先级？
- 您是否为受影响的子网设置了高灵敏度？
- 这是网络上新实体的异常行为吗？
- 实体的正常角色是什么，此警报中的行为与该角色的匹配度如何？
- 这是否是此实体正常行为的异常偏离？
- 如果用户参与其中，这是用户的预期行为还是异常行为？
- 受保护数据或敏感数据是否有被泄露的风险？
- 如果允许此行为继续下去，会对网络产生多严重的影响？
- 如果与外部实体有通信，这些实体过去是否与您网络上的其他实体建立了连接？

如果这是高优先级警报，请考虑将该实体与互联网隔离，或以其他方式关闭其连接，然后再继续调查。

暂停警报以供以后分析

当警报的优先级较低（与其他警报相比）时，可将其暂停。例如，如果您的组织将邮件服务器重新定位为 FTP 服务器，并且系统生成紧急配置文件警报（表明一个实体的当前流量匹配了它以前没有匹配的行为概要文件），您可以暂停此警报（因为这是预期行为），并在以后重新访问它。已暂停的警报不会与待处理警报一起显示；您必须专门过滤才能查看这些暂停的警报。

暂停警报：

Procedure

步骤 1 点击**关闭警报 (Close Alert)**。

步骤 2 在暂停此警报窗格中，从下拉列表中选择暂停时段。

步骤 3 点击**保存 (Save)**。

What to do next

当您准备好查看这些警报时，可以取消暂停该警报。这会将状态设置为“未处理”(Open)，并在其他“未处理”的警报旁边显示该警报。

取消暂停已暂停的警报：

- 从暂停的警报中，点击**取消暂停警报 (Unsnooze Alert)**。

更新警报以进行进一步调查

打开警报详细信息：

Procedure

步骤 1 选择**监控 (Monitor)** > **警报 (Alerts)**。

步骤 2 点击警报类型名称。

What to do next

根据您的初始分类和优先级，分配警报并标记：

1. 从**被分派人 (Assignee)** 下拉列表中选择用户以分配警报，以便用户可以开始调查。
2. 从下拉列表中选择一个或多个**标签**，以将标签添加到警报，以便更好地对警报进行分类以供将来识别，并尝试在警报中建立长期模式。
3. 输入**为此警报添加注释 (Comment on this alert)**，然后点击**注释 (Comment)** 以根据需要留下注释，以跟踪您的初始发现，并协助分配到警报的人员。警报同时跟踪系统注释和用户注释。

查看警报并开始调查

如果您正在查看已分配的警报，请查看警报详细信息以了解 Stealthwatch 云生成警报的原因。查看支持性观察结果，了解这些观察结果对源实体的意义。

请注意，如果警报是基于防火墙事件生成的，则系统不会注意到您的防火墙部署是此警报的来源。

查看此源实体的所有支持性观察结果，以了解其一般行为和模式，并查看此活动是否可能影响着某个长期趋势：

过程

步骤 1 在观察结果控制面板上，点击观察结果类型旁边的箭头图标 ( )，以查看该类型的所有已记录观察结果。

步骤 2 点击**网络的所有观察结果 (All Observations for Network)** 旁边的箭头图标 ( )，查看此警报的源实体的所有已记录观察结果。

如果要对这些观察结果执行其他分析，请下载逗号分隔值文件中的支持观察结果：

- 在警报详细信息的支持观察结果窗格中，点击 **CSV**。

从观察结果，确定源实体行为是否指示恶意行为。如果源实体与多个外部实体建立了连接，请确定外部实体是否以某种方式相关，例如它们是否都具有相似的地理位置信息，或者它们的 IP 地址是否来自同一子网。

从源实体 IP 地址或主机名称查看有关源实体的其他背景信息，包括它可能涉及的其他警报和观察结果、有关设备本身的信息以及它传输的会话流量类型：

- 从 IP 地址或主机名下拉列表中选择**警报 (Alerts)**，以查看与该实体相关的所有警报。
- 从 IP 地址或主机名下拉列表中选择**观察结果 (Observations)**，以查看与实体相关的所有观察结果。
- 从 IP 地址或主机名下拉列表中选择**设备 (Device)**，以查看有关设备的信息。
- 从 IP 地址或主机名下拉列表中选择**会话流量 (Session Traffic)**，以查看与此实体相关的会话流量。
- 从 IP 地址或主机名下拉列表中选择**复制 (Copy)** 以复制 IP 地址或主机名。

请注意，Stealthwatch 云中的源实体始终位于您的网络内部。将此与防火墙事件中的发起方 IP 进行对比，后者指示发起连接的实体，并且可能位于您的网络内部或外部。

从观察结果中，检查有关其他外部实体的信息。检查地理位置信息，确定是否有任何地理位置数据或 Umbrella 数据标识恶意实体。查看这些实体生成的流量。检查 Talos、AbuseIPDB 或 Google 是否有关于这些实体的任何信息。查找多天的 IP 地址，并查看外部实体与您网络上的实体建立的其他类型的连接。如有必要，请找到这些内部实体，并确定是否有任何证据表明存在攻击活动或意外行为。

查看与源实体建立了连接的外部实体 IP 地址或主机名称的背景信息：

- 从 IP 地址或主机名下拉列表中选择 **IP 流量 (IP Traffic)**，以查看此实体的最近流量信息。
- 从 IP 地址或主机名下拉列表中选择**会话流量 (Session Traffic)**，以查看此实体的最近会话流量信息。
- 从 IP 地址或主机名下拉列表中选择 **AbuseIPDB**，以查看有关 AbuseIPDB 网页实体的信息。
- 从 IP 地址或主机名下拉列表中选择**思科 Umbrella (Cisco Umbrella)**，可在 Cisco Umbrella 网站上查看有关此实体的信息。

- 从 IP 地址或主机名下拉列表中选择 **Google 搜索 (Google Search)**，以在 Google 上搜索此 IP 地址。
- 从 IP 地址或主机名下拉列表中选择 **Talos 智能 (Talos Intelligence)**，以查看有关 Talos 网页的信息。
- 从 IP 地址或主机名下拉列表中选择**将 IP 添加到监视列表 (Add IP to watchlist)**，以将此实体添加到监视列表。
- 从 IP 地址或主机名下拉列表中选择**查找多天的 IP (Find IP on multiple days)**，以搜索此实体上个月的流量。
- 从 IP 地址或主机名下拉列表中选择**复制 (Copy)** 以复制 IP 地址或主机名。

请注意，Stealthwatch 云中的连接实体始终位于您的网络外部。将此与防火墙事件中的响应方 IP 进行对比，后者指示响应连接请求的实体，并且可能位于您的网络的内部或外部。

就您的发现进行备注。

- 在警报详细信息中，输入**对此警报的注释 (Comment on this alert)**，然后点击**注释 (Comment)**。

检查实体和用户

在 Stealthwatch 云门户 UI 中查看警报后，您可以直接对源实体、可能与此警报相关的任何用户以及其他相关实体执行其他检查。

- 确定源实体在网络上的物理位置或云中的位置，并直接访问它。找到此实体的日志文件。如果它是网络上的物理实体，请访问设备以查看日志信息，并查看是否有任何信息表明是什么导致了此行为。如果它是虚拟实体或存储在云中，请访问日志并搜索与此实体相关的条目。检查日志，了解有关未经授权的登录、未经批准的配置更改等活动的更多信息。
- 检查实体。确定您能否识别实体本身上的恶意软件或漏洞。查看是否发生了一些恶意更改，包括设备是否发生了物理更改，例如插入了未经组织批准的 U 盘。
- 确定所涉及的用户来自您的网络内部还是外部。如果可能，询问他们当时在做什么。如果询问未果，请确定他们是否应该具有访问权限，以及是否发生了导致此行为的情况，例如，离职员工在离开公司之前将文件上传到外部服务器。

就您的发现进行备注：

- 在警报详细信息中，输入**对此警报的注释 (Comment on this alert)**，然后点击**注释 (Comment)**。

使用安全云分析补救问题

如果恶意行为导致生成警报，请修复恶意行为。例如：

- 如果恶意实体或用户尝试从网络外部进行登录，请更新防火墙规则和防火墙配置，防止该实体或用户访问您的网络。

- 如果实体尝试访问未经授权或恶意的域，请检查受影响的实体，以确定是否为恶意软件导致的原因。如果存在恶意DNS重定向，请确定网络上的其他实体是否受到影响，或是否是僵尸网络的一部分。如果用户有意这样做，请确定是否存在合法原因，例如测试防火墙设置。更新防火墙规则和防火墙配置，以防止进一步访问该域。
- 如果实体表现出与历史实体模型行为不同的行为，请确定是否有意更改行为。如果不是故意的，请检查网络上的其他授权用户是否应对更改负责。更新防火墙规则和防火墙配置，以解决涉及与网络外部实体的连接的意外行为。
- 如果发现漏洞或漏洞攻击，请更新或修补受影响的实体以消除漏洞，或更新防火墙配置以防止未经授权的访问。确定网络上的其他实体是否可能受到类似影响，并向这些实体应用相同的更新或补丁。如果漏洞或漏洞攻击当前没有修补程序，请联系相应的供应商告知他们。
- 如果发现恶意软件，请隔离实体并删除恶意软件。查看防火墙文件和恶意软件事件，以确定网络上的其他实体是否存在风险，更新实体以防止此恶意软件传播。使用有关此恶意软件或导致此恶意软件的实体的信息更新安全情报。更新您的防火墙访问控制以及文件和恶意软件规则，以防止此恶意软件将来感染您的网络。根据需要向供应商发出警报。
- 如果恶意行为导致数据泄露，请确定发送到未授权源的数据的性质。对于未经授权的数据泄露，请遵循组织协议进行操作。更新您的防火墙配置，以防止此来源未来的数据泄露尝试。

更新并关闭警报

根据您的调查结果添加其他标签：

Procedure

步骤 1 在 Cisco Secure Cloud Analytics 门户 UI 中，选择**监控 (Monitor)** > **警报 (Alerts)**。

步骤 2 从下拉列表中选择一个或多个**标签**。

添加描述调查结果的最终注释，以及所采取的任何补救步骤：

- 在警报的详细信息中，输入**为此警报添加注释 (Comment on this alert)**，然后点击**注释 (Comment)**。

关闭警报，然后将其标记为有用或无用：

1. 在警报的详细信息中，点击**关闭警报 (Close Alert)**。
2. 如果警报有用，请选择**是 (Yes)**；如果警报无用，请点击**否 (No)**。请注意，这并不一定意味着该警报是由恶意行为导致的，而只是表示它对您的组织有所帮助。
3. 点击**保存 (Save)**。

What to do next

重新打开已关闭的警报

如果您发现与已关闭警报相关的其他信息，或者想要添加与该警报相关的更多备注，则可以将其重新打开，并将状态更改为“待处理”。然后，您可以根据需要对警报进行更改，并在其他调查完成后再次将其关闭。

重新打开已关闭的警报：

- 在已关闭警报的详细信息中，点击**重新打开警报 (Reopen Alert)**。

修改警报优先级

所需许可证 (Required License)： 日志记录分析和检测 (Logging Analytics and Detection) 或**全面网络分析和监控 (Total Network Analytics and Monitoring)**

警报类型具有默认优先级，这会影响系统对生成此类警报的敏感程度。根据思科情报和其他因素，警报的优先级默认为低或正常。根据您的网络环境，您可能希望重新确定警报类型的优先级，以强调您关注的某些警报。您可以将任何风险通告类型配置为低、正常或高优先级。

- 选择**监控 (Monitor)** > **警报 (Alerts)**。
- 点击设置下拉图标 ()，然后选择警报类型和优先级。
- 点击警报类型旁边的编辑图标 ()，然后选择低、中或高以更改优先级。

查看实时事件

实时事件页面显示与您输入的在事件日志记录页面中搜索和过滤事件匹配的最新 500 个事件。如果“实时事件”页面最多显示500个事件，并且有更多事件传入，则CDO会显示最新的实时事件，并将最早的实时事件传输到“历史事件”页面，使实时事件总数保持为 500。执行该传输大约需要一分钟。如果未添加过滤条件，您将看到配置为记录事件的规则生成的所有最新实时 500 事件。

事件的时间戳以查看事件的 CDO 管理员的本地时间显示。

更改过滤条件（无论是正在播放还是已暂停的实时事件）会清除事件屏幕并重新启动收集过程。

要在 CDO 事件查看器中查看实时事件，请执行以下操作：

Procedure

步骤 1 在导航窗格中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

步骤 2 点击**实时 (Live)** 选项卡。

What to do next

通过阅读了解如何播放和暂停事件。

相关信息：

播放/暂停实时事件

您可以在实时事件传入时“播放”或“暂停”。如果实时事件正在“播放”，则 CDO 将按接收顺序来显示与事件查看器中指定的过滤条件匹配的事件。如果事件已暂停，则在您重新开始播放实时事件之前，CDO 不会更新“实时事件”(Live events) 页面。当您重新开始播放事件时，CDO 会从您重新开始播放事件的位置开始在“实时”(Live) 页面中填充事件。它不会回填您遗漏的内容。

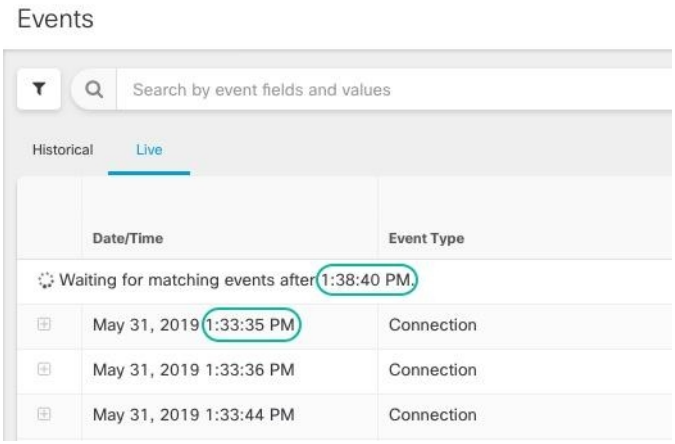
要查看 CDO 收到的所有事件（无论您已播放还是暂停），请点击“历史”(Historical) 选项卡。

自动暂停实时事件

在连续显示事件约 5 分钟后，CDO 会警告您即将暂停实时事件流。届时，您可以点击该链接以继续流传输其他 5 分钟的实时事件，或者允许流停止。在准备就绪后，您可以重新启动实时事件流。

接收和报告事件

在实时事件查看器中，安全事件连接器 (SEC) 接收事件和 CDO 发布事件之间可能会存在一点延迟。您可以在“实时”(Live) 页面上查看差距。事件的时间戳是 SEC 收到的时间。



查看历史事件

实时事件页面会显示与您输入的在事件日志记录页面中搜索和过滤事件匹配的 500 个最新事件。超出最近的 500 个事件将被传输到历史事件表。执行该传输大约需要一分钟。然后，您可以过滤已存储的所有事件，以便找到要查找的事件。

要查看历史事件，请执行以下操作：

Procedure

步骤 1 在导航窗格中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

步骤 2 点击**历史 (Historical)** 选项卡。默认情况下，当您打开历史事件表时，过滤器会被设置为显示最近一小时内收集的事件。

事件属性与 Firepower 设备管理器 (FDM) 或自适应安全设备管理器 (ASDM) 报告的属性基本相同。

- 有关 Firepower 威胁防御事件属性的详尽说明，请参阅思科 FTD 系统日志消息。
- 有关 ASA 事件属性的详尽说明，请参阅思科 ASA 系列系统日志消息。

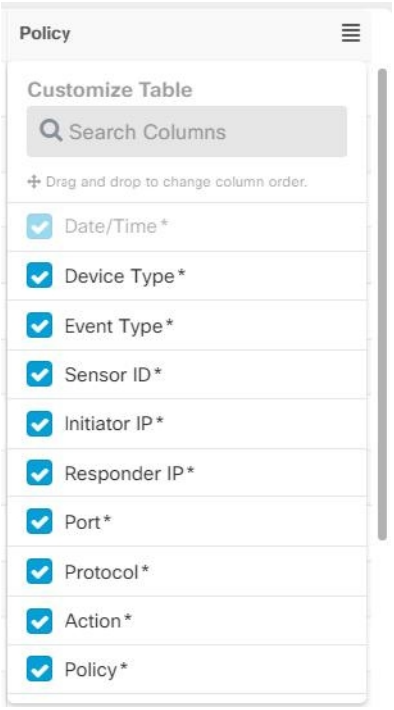
自定义事件视图

当您离开此页面并稍后返回时，系统会自动保存对“事件日志记录”(Event Logging) 页面所做的任何更改。

Note 实时和历史事件视图具有相同的配置。自定义事件视图时，这些更改将同时应用于实时和历史视图。

列

您可以修改实时事件和历史事件的事件视图，以仅包含适用于所需视图的列标题。点击列右侧的列过滤器图标 ，然后选择或取消选择所需的列：



默认情况下，事件表中提供带星号的列，但您可以随时将其删除。使用搜索栏手动搜索可能要包括的其他列的关键字。

订单

您可以对“事件”视图的列重新排序。点击列右侧的列过滤器图标 可展开所选列的列表，并手动将列拖放到所需的顺序，其中下拉菜单中列表顶部的列位于左侧- 事件视图中的大多数列。

相关信息：

- 在事件日志记录页面中搜索和过滤事件
- 安全分析和日志记录中的事件属性

在事件日志记录页面上显示和隐藏列

“事件日志记录”(Event Logging) 页面显示从已配置的 ASA 和 FDM 管理 设备发送到思科云的 ASA 和 FTD 系统日志事件和 ASA NetFlow 安全事件日志记录 (NSEL) 事件。

您可以通过对表使用显示/隐藏构件来显示或隐藏“事件日志记录”页面上的列：

Procedure

步骤 1 从 CDO 导航栏中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

步骤 2 滚动到表格的最右侧，然后点击**显示/隐藏列 (Show/Hide Columns)** 按钮 ≣。

步骤 3 选中要查看的列，并取消选中要隐藏的列。

步骤 4 将鼠标悬停在“显示/隐藏列”(Show/Hide Columns) 下拉菜单中的列名称上，然后抓住灰色十字，重新排列列顺序。

登录到租户的其他用户将看到您选择显示的相同列，直到列再次显示或隐藏。

下表介绍了列标题：

列标题	说明
日期/时间	设备生成事件的时间。时间以计算机的本地时间显示。
设备类型	或 FTD（Firepower 威胁防御）

事件类型	此组合列可以包含以下任何内容：
	• **FTD 事件类型**
	  • 连接 - 显示访问控制规则中的连接事件。
	  • 文件 - 显示访问控制规则中文件策略报告的事件。
	  • 入侵 - 显示访问控制规则中入侵策略报告的事件。
	  • 恶意软件 - 显示访问控制规则中的恶意软件策略报告的事件。
	• ASA **事件类型 (Event Types)** - 这些事件类型表示系统日志或 NetFlow 事件组。有关哪个系统日志 ID 或哪个 NetFlow ID 包含在哪个组中的详细信息，请参阅 ASA 事件类型。
	  • 解析的事件 - 解析的系统日志事件包含比其他系统日志事件更多的事件属性，并且 CDO 能够更快地返回基于这些属性的搜索结果。解析的事件不是过滤类别；但是，解析的事件 ID 以 斜体显示在“事件类型”(Event Types) 列中。不以斜体显示的事件 ID 不会被解析。
	  • ASA NetFlow 事件 ID：此处会显示 ASA 的所有 Netflow (NSEL) 事件 。

列标题	说明
传感器 ID (Sensor ID)	传感器 ID 是将事件发送到安全事件连接器的 IP 地址。这通常是 Firepower 威胁防御或 ASA上的管理接口。
发起方 IP	这是网络流量源的IP地址。发起方地址字段的值对应于事件详细信息中发起方IP字段的值。您可以输入单个地址（例如 10.10.10.100）或以 CIDR 表示法定义的网络（例如 10.10.10.0/24）。
响应方 IP	这是流数据包的目的 IP 地址。“目的地址”(Destination address) 字段的值对应于事件详细信息中 ResponderIP 字段中的值。您可以输入单个地址（例如 10.10.10.100）或以 CIDR 表示法定义的网络（例如 10.10.10.0/24）。
Port	会话**响应方**使用的端口或 ICMP 代码。目标端口的值对应于事件详细信息中的**ResponderPort**值。
协议	它代表事件中的协议。
操作	指定规则定义的安全操作。输入的值必须与要查找的内容完全匹配；但是，大小写无关紧要。为连接、文件、入侵、恶意软件、系统日志和 NetFlow 事件类型输入不同的值： • 对于连接事件类型，过滤器在AC_RuleAction属性中搜索匹配项。这些值可以是“允许”(Allow)、“阻止”(Block)、“信任”(Trust)。 • 对于文件事件类型，过滤器在 FileAction 属性中搜索匹配项。这些值可以是“允许”、“阻止”、“信任”。 • 对于入侵事件类型，过滤器在 InLineResult 属性中搜索匹配项。这些值可以是 “已允许”(Allowed)、“已阻止”(Blocked)、“已信任”(Trusted)。 • 对于恶意软件事件类型，过滤器会在 FileAction 属性中搜索匹配项。这些值可以是“云查找超时”(Cloud Lookup Timeout)。 • 对于系统日志和 NetFlow 事件类型，过滤器在操作属性中搜索匹配项。

列标题	说明
策略	触发事件的策略的名称。ASA 和 FDM 管理 设备的名称不同。

相关信息：

在事件日志记录页面中搜索和过滤事件, on page 669

可自定义的事件过滤器

如果您是安全日志记录分析 (SaaS) 客户，则可以创建并保存您经常使用的自定义过滤器。

过滤器的元素会在您配置时保存到过滤器选项卡中。每当您返回“事件日志记录”(Event Logging) 页面时，这些搜索都可供使用。租户的其他CDO用户将无法使用它们。如果您管理多个租户，它们将无法在其他租户上使用。

Note 请注意，在过滤器选项卡中操作时，如果修改任何过滤器条件，这些更改将自动保存到自定义过滤器选项卡。

Procedure

步骤 1 从主菜单中选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

步骤 2 清除任何值的搜索字段。

步骤 3 在事件表上方，点击蓝色加号按钮以添加视图选项卡。过滤器视图被标记为“视图 1”(View 1)、“视图 2”(View 2)、“视图 3”(View 3) 等，直到您为其指定名称。

步骤 4 选择一个视图选项卡。

步骤 5 打开过滤器栏，然后在自定义过滤器中选择所需的过滤器属性。请参阅在事件日志记录页面中搜索和过滤事件, on page 669。请记住，自定义过滤器中仅保存过滤器属性。

步骤 6 自定义要在事件日志记录表中显示的列。有关显示和隐藏列的讨论，请参阅在事件日志记录页面上显示和隐藏列, on page 634。

步骤 7 双击带有“视图 X”(View X) 标签的过滤器选项卡并将其重命名。

步骤 8 （可选）现在您已创建自定义过滤器，您可以通过向“搜索”(Search) 字段添加搜索条件来微调“事件日志记录”(Event Logging) 页面上显示的结果，而无需更改自定义过滤器。请参阅在事件日志记录页面中搜索和过滤事件, on page 669。

安全分析和日志记录中的事件属性

事件属性说明

CDO 使用的事件属性说明与 Firepower Device Manager (FDM) 和自适应安全设备管理器 (ASDM) 报告的内容基本相同。

- 有关 FDM 托管设备事件属性的完整说明，请参阅思科 FirePower 威胁防御系统日志消息。

某些 ASA 系统日志事件经过“解析”，其他事件具有其他属性，您可以在使用“属性:值”对过滤事件日志记录表的内容时使用这些属性。有关系统日志事件的其他重要属性，请参阅以下附加主题：

- 某些系统日志消息的 EventGroup 和 EventGroupDefinition 属性
- 系统日志事件的 EventName 属性
- 系统日志事件中的时间属性

某些系统日志消息的 EventGroup 和 EventGroupDefinition 属性

某些系统日志事件将具有附加属性“EventGroup”和“EventGroupDefinition”。您将能够通过过滤“属性:值”对来过滤事件表，查找使用这些附加属性的事件。例如，您可以通过在事件日志记录表的搜索字段中输入 `apfw:415*` 来过滤应用防火墙事件。

系统日志消息类和关联的消息 ID 号

事件组	EventGroupDefinition	系统日志消息 ID 号（前 3 数字）
aaa/auth	用户身份验证	109、113
acl/session	访问列表/用户会话	106
apfw	应用防火墙	415
bridge	透明防火墙	110、220
ca	PKI 证书颁发机构	717
citrix	Citrix Client	723
clst	集群	747
cmgr	卡管理	323
config	命令界面	111、112、208、308
csd	安全桌面	724
cts	Cisco TrustSec	776
dap	动态访问策略	734

事件组	EventGroupDefinition	系统日志消息ID号（前3数字）
eap, eapoudp	用于网络准入控制的 EAP 或 EAPoUDP	333、334
eigrp	EIGRP 路由	336
电子邮件	邮件代理	719
ipaa/envmon	环境监控	735
ha	故障切换	101、102、103、104、105、210、311、709
idfw	基于身份认证的防火墙	746
ids	入侵检测系统	733
ids/ips	入侵检测系统/入侵保护系统	400
ikev2	IKEv2 工具包	750、751、752
ip	IP 堆栈	209、215、313、317、408
ipaa	IP 地址分配	735
ips	入侵保护系统	401、420
ipv6	IPv6	325
l4tm	阻止列表、允许列表、灰名单	338
许可证	许可	444
mdm-proxy	MDM 代理	802
nac	网络准入控制	731、732
vpn/nap	IKE 和 IPsec/网络接入点	713
np	网络处理器	319
ospf	OSPF 路由	318、409、503、613
passwd	密码加密	742
pp	电话代理	337
rip	RIP 路由	107、312
rm	资源管理器	321
sch	Smart Call Home	120
session	用户会话	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710

事件组	EventGroupDefinition	系统日志消息 ID 号（前 3 数字）
会话/natpat	用户会话/NAT 和 PAT	305
snmp	SNMP	212
ssafe	ScanSafe	775
ssl/np ssl	SSL 协议栈/NP SSL	725
svc	SSL VPN 客户端	722
sys	System	199、211、214、216、306、307、315、414、604、605，606、610、612、614、615、701、711、741
tre	事务规则引擎	780
ucime	UC-IME	339
标记交换	服务标记交换	779
td	威胁检测	733
vm	VLAN 映射	730
vpdn	PPTP 和 L2TP 会话	213、403、603
vpn	IKE 和 IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN 客户端	611
vpnfo	VPN 故障切换	720
vpnlb	VPN 负载均衡	718
vxlan	VXLAN	778
webfo	WebVPN 故障切换	721
webvpn	WebVPN 和 AnyConnect 客户端	716
会话/natpat	用户会话/NAT 和 PAT	305

系统日志事件的 EventName 属性

某些系统日志事件将具有附加属性“EventName”。您将能够通过过滤“属性:值”对来过滤事件表，查找使用 EventName 属性的事件。例如，您可以通过在事件日志记录表的搜索字段中输入 **EventName:"Denied IP Packet"** 来过滤“被拒绝的 IP 数据包”的事件。

系统日志事件 ID 和事件名称表

- AAA 系统日志事件 ID 和事件名称
- 僵尸网络系统日志事件 ID 和事件名称

- 故障切换系统日志事件 ID 和事件名称
- 防火墙拒绝系统日志事件 ID 和事件名称
- 防火墙流量系统日志事件 ID 和事件名称
- 基于身份的防火墙系统日志事件 ID 和事件名称
- IPSec 系统日志事件 ID 和事件名称
- NAT 系统日志事件 ID 和事件名称
- SSL VPN 系统日志事件 ID 和事件名称

AAA 系统日志事件 ID 和事件名称

EventID	EventName
109001	AAA 开始
109002	AAA 失败
109003	AAA 服务器发生故障
109005	身份验证成功
109006	身份验证失败
109007	授权成功
109008	授权失败
109010	AAA 待处理
109011	AAA 会话已启动
109012	AAA 会话已结束
109013	AAA
109014	AAA 失败
109016	未找到 AAA ACL
109017	AAA 限制到达
109018	AAA ACL 空
109019	AAA ACL 错误
109020	AAA ACL 错误
109021	AAA 错误

EventID	EventName
109022	AAA HTTP 限制已达到
109023	需要 AAA 身份验证
109024	授权失败
109025	授权失败
109026	AAA 错误
109027	AAA 服务器错误
109028	AAA 绕行
109029	AAA ACL 错误
109030	AAA ACL 错误
109031	身份验证失败
109032	AAA ACL 错误
109033	身份验证失败
109034	身份验证失败
109035	AAA 限制到达
113001	AAA 会话限制范围
113003	AAA 已覆盖
113004	AAA 成功
113005	授权被拒绝
113006	AAA 用户已锁定
113007	AAA 用户已解锁
113008	AAA 成功
113009	AAA 已检索
113010	AAA 挑战已收到
113011	AAA 已检索
113012	身份验证成功
113013	AAA 错误

EventID	EventName
113014	AAA 错误
113015	身份验证已被拒绝
113016	AAA 已被拒绝
113017	AAA 已被拒绝
113018	AAA ACL 错误
113019	AAA 已断开
113020	AAA 错误
113021	AAA 日志记录失败
113022	AAA 失败
113023	AAA 已重新激活
113024	AAA 客户端证书
113025	AAA 认证失败
113026	AAA 错误
113027	AAA 错误

僵尸网络系统日志事件 ID 和事件名称

EventID	EventName
338001	僵尸网络源阻止列表
338002	僵尸网络目标阻止列表
338003	僵尸网络源阻止列表
338004	僵尸网络目标阻止列表
338101	僵尸网络源允许列表
338102	僵尸网络目标允许列表
338202	僵尸网络目的地（灰色）
338203	僵尸网络源灰色
338204	僵尸网络目标灰色
338301	僵尸网络 DNS 已拦截

EventID	EventName
338302	僵尸网络 DNS
338303	僵尸网络 DNS
338304	僵尸网络下载成功
338305	僵尸网络下载失败
338306	僵尸网络身份验证失败
338307	僵尸网络解密失败
338308	僵尸网络客户端
338309	僵尸网络客户端
338310	僵尸网络动态过滤器失败

故障切换系统日志事件 ID 和事件名称

EventID	EventName
101001	故障切换电缆 OK
101002	故障切换电缆 BAD
101003	故障切换电缆未连接
101004	故障切换电缆未连接
101005	故障切换电缆读取错误
102001	故障转移电源失败
103001	故障转移伙伴无响应
103002	故障转移配对接口 OK
103003	故障转移伙伴接口 BAD
103004	故障转移伙伴报告失败
103005	故障转移伙伴报告自身失败
103006	故障转移版本不兼容
103007	故障转移版本差异
104001	故障转移角色切换
104002	故障转移角色切换

EventID	EventName
104003	故障转移设备发生故障
104004	故障转移单元 OK
106100	允许/被 ACL 拒绝
210001	状态故障转移错误
210002	状态故障转移错误
210003	状态故障转移错误
210005	状态故障转移错误
210006	状态故障转移错误
210007	状态故障转移错误
210008	状态故障转移错误
210010	状态故障转移错误
210020	状态故障转移错误
210021	状态故障转移错误
210022	状态故障转移错误
311001	状态故障转移更新
311002	状态故障转移更新
311003	状态故障转移更新
311004	状态故障转移更新
418001	被拒绝的向管理发送的数据包
709001	故障转移复制错误
709002	故障转移复制错误
709003	故障转移复制开始
709004	故障转移复制完成
709005	故障转移接收复制开始
709006	故障转移接收复制完成
709007	故障转移复制失败

EventID	EventName
710003	被拒绝的访问设备

防火墙拒绝系统日志事件 ID 和事件名称

EventID	EventName
106001	被安全策略拒绝
106002	出站拒绝
106006	被安全策略拒绝
106007	被拒绝的入站 UDP
106008	被安全策略拒绝
106010	被安全策略拒绝
106011	被拒绝的入站
106012	由于 IP 选项错误而被拒绝
106013	对 PAT IP 的 ping 操作丢弃
106014	被拒绝的入站 ICMP
106015	被安全策略拒绝
106016	被拒绝的 IP 欺骗
106017	由于着陆攻击而被拒绝
106018	被拒绝的出站 ICMP
106020	被拒绝的 IP 数据包
106021	被拒绝的 TCP
106022	被拒的绝欺骗数据包
106023	被拒绝的 IP 数据包
106025	被丢弃的数据包未能检测情景
106026	被丢弃的数据包未能检测情景
106027	被丢弃的数据包未能检测情景
106100	允许/被 ACL 拒绝
418001	被拒绝的向管理发送的数据包

EventID	EventName
710003	被拒绝的访问设备

防火墙流量系统日志事件 ID 和事件名称

EventID	EventName
108001	检查 SMTP
108002	检查 SMTP
108003	检查 ESMTP 已丢弃
108004	检查 ESMTP
108005	检查 ESMTP
108006	检查 ESMTP 违规
108007	检查 ESMTP
110002	找不到路由器
110003	未能找到下一跳
209003	分段限制范围
209004	分段长度无效
209005	分段 IP 丢弃
302003	H245 连接开始
302004	H323 连接开始
302009	重新启动 TCP
302010	连接使用情况
302012	H225 CALL SIGNAL CONN
302013	内置 TCP
302014	拆解 TCP
302015	内置 UDP
302016	拆解 UDP
302017	内置 GRE
302018	拆解 GRE

EventID	EventName
302019	H323 失败
302020	内置 ICMP
302021	拆解 ICMP
302022	内置 TCP 末节
302023	拆解 TCP 末节
302024	内置 UDP 末节
302025	拆解 UDP 末节
302026	内置 ICMP 末节
302027	拆解 ICMP 末节
302033	连接 H323
302034	H323 连接失败
302035	内置 SCTP
302036	拆解 SCTP
303002	FTP 文件下载/上传
303003	检查 FTP 已丢弃
303004	检查 FTP 已丢弃
303005	检查 FTP 重置
313001	ICMP 已拒绝
313004	ICMP 丢弃
313005	ICMP 错误消息丢弃
313008	ICMP ipv6 已拒绝
324000	GTP 数据包丢弃
324001	GTP 数据包错误
324002	内存错误
324003	GTP 数据包丢弃
324004	不支持 GTP 版本

EventID	EventName
324005	GTP 隧道失败
324006	GTP 隧道失败
324007	GTP 隧道失败
337001	电话代理 SRTP 失败
337002	电话代理 SRTP 失败
337003	电话代理 SRTP 身份验证失败
337004	电话代理 SRTP 身份验证失败
337005	电话代理 SRTP 无媒体会话
337006	电话代理 TFTP 无法创建文件
337007	电话代理 TFTP 无法查找文件
337008	电话代理呼叫失败
337009	电话代理无法创建电话条目
400000	IPS IP 选项 - 错误选项列表
400001	IPS IP 选项 - 记录数据包路由
400002	IPS IP 选项 - 时间戳
400003	IPS IP 选项 - 安全
400004	IPS IP 选项 - 松散源路由
400005	IPS IP 选项 - SATNET ID
400006	IPS IP 选项 - 严格源路由
400007	IPS IP 分段攻击
400008	IPS IP 不可能的数据包
400009	IPS IP 分段重叠
400010	IPS ICMP 回应应答
400011	IPS ICMP 主机不可达
400012	IPS ICMP 源抑制
400013	IPS ICMP 重定向

EventID	EventName
400014	IPS ICMP 回应请求
400015	数据报的 IPS ICMP 超时
400017	IPS ICMP 时间戳请求
400018	IPS ICMP 时间戳应答
400019	IPS ICMP 信息请求
400020	IPS ICMP 信息应答
400021	IPS ICMP 地址掩码请求
400022	IPS ICMP 地址掩码应答
400023	IPS 分段的 ICMP 流量
400024	IPS 大 ICMP 流量
400025	死亡之 IPS Ping 攻击
400026	IPS TCP NULL 标志
400027	IPS TCP SYN+FIN 标志
400028	仅 IPS TCP FIN 标志
400029	指定了不正确的 IPS FTP 地址
400030	指定了不正确的 IPS FTP 端口
400031	IPS UDP 炸弹攻击
400032	IPS UDP Snork 攻击
400033	IPS UDP Chargen DoS 攻击
400034	IPS DNS HINFO 请求
400035	IPS DNS 区域传输
400036	来自高端口的 IPS DNS 区域传输
400037	所有记录的 IPS DNS 请求
400038	IPS RPC 端口注册
400039	IPS RPC 端口取消注册
400040	IPS RPC 转储

EventID	EventName
400041	IPS 通过代理发送的 RPC 请求
400042	IPS YP 服务器端口映射请求
400043	IPS YP 绑定端口映射请求
400044	IPS YP 密码端口映射请求
400045	IPS YP 更新端口映射请求
400046	IPS YP 传输端口映射请求
400047	IPS 装载端口映射请求
400048	IPS 远程执行端口映射请求
400049	IPS 远程执行尝试
400050	IPS Statd 缓冲区溢出
406001	检查 FTP 已丢弃
406002	检查 FTP 已丢弃
407001	主机限制到达
407002	初期限制已到达
407003	既定限制已到达
415001	检查 Http 信头字段计数
415002	检查 Http 信头字段长度
415003	检查 Http 正文长度
415004	检查 Http 内容类型
415005	检查 Http URL 长度
415006	检查 Http URL 匹配
415007	检查 Http 正文匹配
415008	检查 Http 信头匹配
415009	检查 Http 方法匹配
415010	检查传输编码匹配
415011	检查 Http 协议违规

EventID	EventName
415012	检查 Http 内容类型
415013	检查 Http 格式错误
415014	检查 Http MIME 类型
415015	检查 Http Transfer-encoding
415016	检查 Http 未应答
415017	检查 Http 参数匹配
415018	检查 Http 信头长度
415019	检查 Http 状态已匹配
415020	检查 Http non-ASCII
416001	检查 SNMP 已丢弃
419001	已丢弃的数据包
419002	重复 TCP SYN
419003	数据包已修改
424001	被拒绝的数据包
424002	已丢弃的数据包
431001	已丢弃的 RTP
431002	已丢弃的 RTCP
500001	检查 ActiveX
500002	检查 Java
500003	检查 TCP 信头
500004	检查 TCP 信头
500005	检查连接已终止
508001	检查 DCERPC 已丢弃
508002	检查 DCERPC 已丢弃
509001	已阻止 No Forward Cmd
607001	检查 SIP

EventID	EventName
607002	检查 SIP
607003	检查 SIP
608001	检查 Skinny
608002	检查 Skinny 已丢弃
608003	检查 Skinny 已丢弃
608004	检查 Skinny 已丢弃
608005	检查 Skinny 已丢弃
609001	内置本地主机
609002	拆解本地主机
703001	H225 不支持的版本
703002	H225 连接
726001	检查即时消息

基于身份的防火墙系统日志事件 ID 和事件名称

EventID	EventName
746001	导入已开始
746002	导入完成
746003	导入失败
746004	超出用户组限制
746005	AD 代理关闭
746006	AD 代理不同步
746007	Netbios 响应失败
746008	Netbios 已启动
746009	Netbios 已停止
746010	导入用户失败
746011	超出用户限制
746012	用户 IP 添加

EventID	EventName
746013	用户 IP 删除
746014	FQDN 过时
746015	FQDN 已解析
746016	DNS 查找失败
746017	导入用户已颁发
746018	导入用户已完成
746019	更新 AD 代理失败

IPSec 系统日志事件 ID 和事件名称

EventID	EventName
402114	收到无效的 SPI
402115	收到意外的协议
402116	数据包与身份不匹配
402117	收到的非 IPSEC 数据包
402118	无效的分段偏移量
402119	防重放检查失败
402120	身份验证失败
402121	数据包已丢弃
426101	cLACP 端口捆绑包
426102	cLACP 端口备用
426103	已将 cLACP 端口从备用端口移至捆绑包
426104	cLACP 非捆绑端口
602103	路径 MTU 已更新
602104	路径 MTU 已超出
602303	新 SA 已创建
602304	SA 已删除
702305	SA 到期 - 序列滚动
702307	SA 到期 - 数据滚动

NAT 系统日志事件 ID 和事件名称

EventID	EventName
201002	超出主机的最大连接数
201003	已超出初期限制
201004	已超出 UDP 连接限制
201005	FTP 连接失败
201006	RCMD 连接失败
201008	不允许新建连接
201009	超出连接限制
201010	已超出初期连接限制
201011	已超出连接限制
201012	已超出每个客户端的初期连接限制
201013	已超出每个客户端连接限制
202001	全局 NAT 已耗尽
202005	初期连接错误
202011	超出连接限制
305005	未找到 NAT 组
305006	转换已失败
305007	连接已断开
305008	NAT 分配问题
305009	NAT 已创建
305010	NAT 拆解
305011	PAT 已创建
305012	PAT 拆解
305013	连接已被拒绝

SSL VPN 系统日志事件 ID 和事件名称

EventID	EventName
716001	WebVPN 会话已启动
716002	WebVPN 会话已终止
716003	WebVPN 用户 URL 访问
716004	WebVPN 用户 URL 访问被拒绝

EventID	EventName
716005	WebVPN ACL 错误
716006	WebVPN 用户已禁用
716007	WebVPN 无法创建
716008	WebVPN 调试
716009	WebVPN ACL 错误
716010	WebVPN 用户接入网络
716011	WebVPN 用户访问
716012	WebVPN 用户目录访问
716013	WebVPN 用户文件访问
716014	WebVPN 用户文件访问
716015	WebVPN 用户文件访问
716016	WebVPN 用户文件访问
716017	WebVPN 用户文件访问
716018	WebVPN 用户文件访问
716019	WebVPN 用户文件访问
716020	WebVPN 用户文件访问
716021	WebVPN 用户访问文件被拒绝
716022	WebVPN 无法连接代理
716023	WebVPN 会话限制已到达
716024	WebVPN 用户访问错误
716025	WebVPN 用户访问错误
716026	WebVPN 用户访问错误
716027	WebVPN 用户访问错误
716028	WebVPN 用户访问错误
716029	WebVPN 用户访问错误
716030	WebVPN 用户访问错误
716031	WebVPN 用户访问错误
716032	WebVPN 用户访问错误
716033	WebVPN 用户访问错误

EventID	EventName
716034	WebVPN 用户访问错误
716035	WebVPN 用户访问错误
716036	WebVPN 用户登录成功
716037	WebVPN 用户登录失败
716038	WebVPN 用户身份验证成功
716039	WebVPN 用户身份验证被拒绝
716040	WebVPN 用户日志记录被拒绝
716041	WebVPN ACL 命中计数
716042	WebVPN ACL 命中
716043	WebVPN 端口转发
716044	WebVPN 错误参数
716045	WebVPN 参数无效
716046	WebVPN 连接已终止
716047	WebVPN ACL 使用情况
716048	WebVPN 内存问题
716049	WebVPN 空 SVC ACL
716050	WebVPN ACL 错误
716051	WebVPN ACL 错误
716052	WebVPN 会话已终止
716053	WebVPN SSO 服务器已添加
716054	WebVPN SSO 服务器已删除
716055	WebVPN 身份验证成功
716056	WebVPN 身份验证失败
716057	WebVPN 会话已终止
716058	WebVPN 会话已丢失
716059	WebVPN 会话已恢复
716060	WebVPN 会话已终止
722001	WebVPN SVC 连接请求错误
722002	WebVPN SVC 连接请求错误

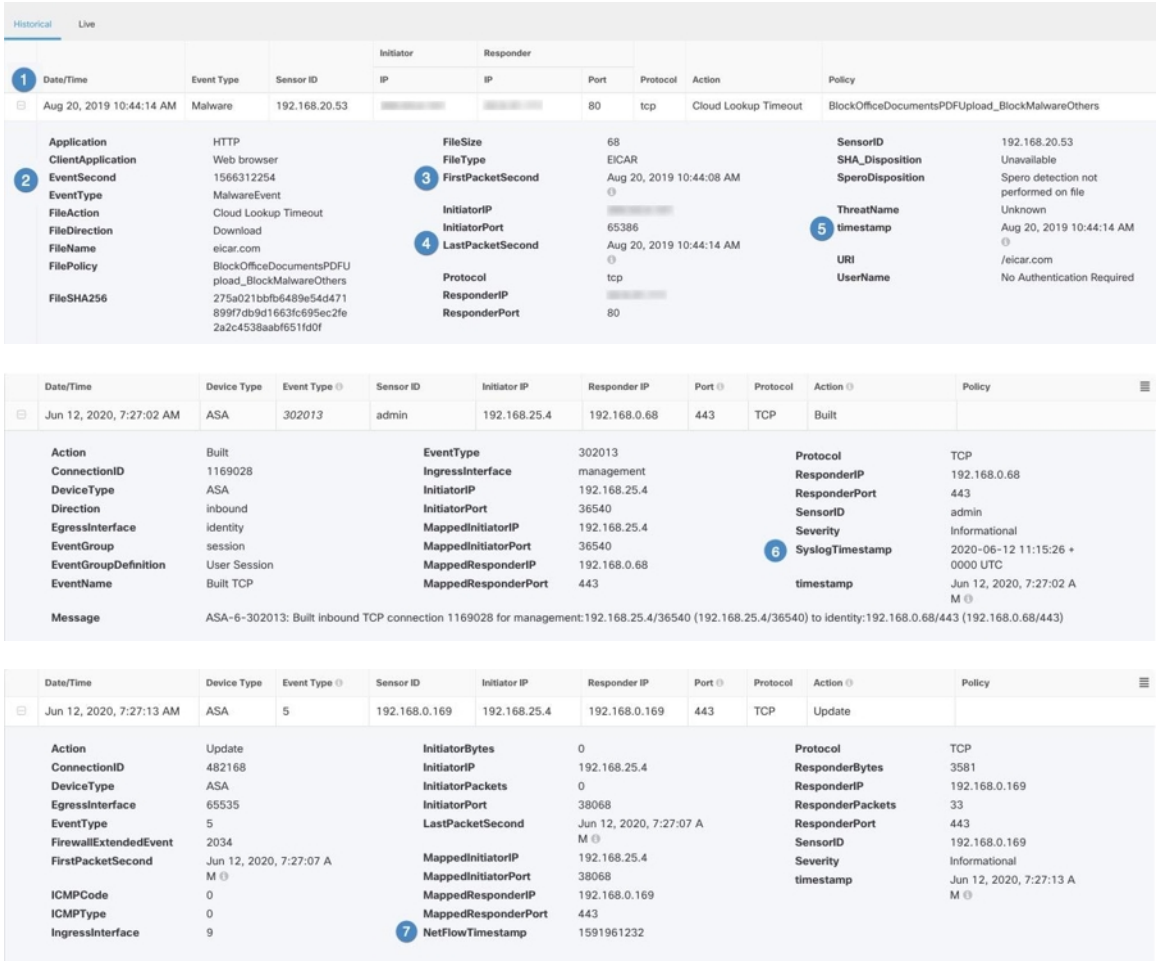
EventID	EventName
722003	WebVPN SVC 连接请求错误
722004	WebVPN SVC 连接请求错误
722005	WebVPN SVC 连接更新问题
722006	WebVPN SVC 地址无效
722007	WebVPN SVC 消息
722008	WebVPN SVC 消息
722009	WebVPN SVC 消息
722010	WebVPN SVC 消息
722011	WebVPN SVC 消息
722012	WebVPN SVC 消息
722013	WebVPN SVC 消息
722014	WebVPN SVC 消息
722015	WebVPN SVC 无效帧
722016	WebVPN SVC 无效帧
722017	WebVPN SVC 无效帧
722018	WebVPN SVC 无效帧
722019	WebVPN SVC 数据不足
722020	WebVPN SVC 无地址
722021	WebVPN 内存问题
722022	WebVPN SVC 连接已建立
722023	WebVPN SVC 连接已终止
722024	WebVPN 压缩已启用
722025	WebVPN 压缩已禁用
722026	WebVPN 压缩重置
722027	WebVPN 解压重置
722028	WebVPN 连接已关闭
722029	WebVPN SVC 会话已终止
722030	WebVPN SVC 会话已终止
722031	WebVPN SVC 会话已终止

EventID	EventName
722032	WebVPN SVC 连接替换
722033	WebVPN SVC 连接已建立
722034	WebVPN SVC 新连接
722035	WebVPN 收到大数据包
722036	WebVPN 传输大型数据包
722037	WebVPN SVC 连接已关闭
722038	WebVPN SVC 会话已终止
722039	WebVPN SVC 无效 ACL
722040	WebVPN SVC 无效 ACL
722041	WebVPN SVC IPv6 不可用
722042	WebVPN 无效协议
722043	WebVPN DTLS 已禁用
722044	WebVPN 无法请求地址
722045	WebVPN 连接已终止
722046	WebVPN 会话已终止
722047	WebVPN 隧道已终止
722048	WebVPN 隧道已终止
722049	WebVPN 会话已终止
722050	WebVPN 会话已终止
722051	分配的 WebVPN 地址
722053	WebVPN 未知客户端
723001	WebVPN Citrix 连接开启
723002	WebVPN Citrix 连接关闭
723003	WebVPN Citrix 无内存问题
723004	WebVPN Citrix 不良流量控制
723005	WebVPN Citrix 无信道
723006	WebVPN Citrix SOCKS 错误
723007	WebVPN Citrix 连接列表已损坏
723008	WebVPN Citrix 无效 SOCKS

EventID	EventName
723009	WebVPN Citrix 无效连接
723010	WebVPN Citrix 无效连接
723011	WebVPN citrix 不良 SOCKS
723012	WebVPN Citrix 不良 SOCKS
723013	WebVPN Citrix 无效连接
723014	WebVPN Citrix 连接到服务器
724001	不允许使用 WebVPN 会话
724002	WebVPN 会话已终止
724003	WebVPN CSD
724004	WebVPN CSD
725001	SSL 握手已开始
725002	SSL 握手已完成
725003	SSL 客户端会话恢复
725004	SSL 客户端请求身份验证
725005	SSL 服务器请求认证
725006	SSL 握手已失败
725007	SSL 会话已终止
725008	SSL 客户端密码
725009	SSL 服务器密码
725010	SSL 密码
725011	SSL 设备选择密码
725012	SSL 设备选择密码
725013	SSL 服务器选择密码
725014	SSL LIB 错误
725015	SSL 客户端证书已失败

系统日志事件中的时间属性

了解“事件日志记录”(Event Logging) 页面中不同时间戳的用途将有助于您过滤并查找感兴趣的事件。



数字	编号	说明
1	日期/时间	安全事件连接器 (SEC) 处理事件的时间。这可能与防火墙检查该流量的时间有所不同。与时间戳相同的值。
2	EventSecond	等于 LastPacketSecond。
3	FirstPacketSecond	连接打开的时间。防火墙会在此时检查数据包。 FirstPacketSecond 的值通过从 LastPacketSecond 中减去 ConnectionDuration 来计算得出。 对于在连接开始时记录的连接事件，FirstPacketSecond、LastPacketSecond 和 EventSecond 的值均相同。

数字	编号	说明
4	LastPacketSecond	连接被关闭的时间。对于在连接结束时记录的连接事件，LastPacketSecond 和 EventSecond 将相等。
5	timestamp	安全事件连接器 (SEC) 处理事件的时间。这可能与防火墙检查该流量的时间有所不同。与日期/时间相同的值。
6	系统日志时间戳	如果使用“日志记录时间戳”，则表示系统日志的发起时间。如果系统日志中没有此信息，则会反映 SEC 收到事件的时间。
7	NetflowTimeStamp	ASA 完成收集足够的流记录/事件以填充 NetFlow 数据包，然后将其发送到流收集器的时间。

思科安全云分析和动态实体建模

所需许可证 (Required License)：日志记录分析和检测 (Logging Analytics and Detection) 或**全面网络分析和监控 (Total Network Analytics and Monitoring)**

安全云分析是一种软件即服务 (SaaS) 解决方案，可用于监控您的本地和基于云的网络部署。通过从源（包括防火墙事件和网络流数据）收集有关网络流量的信息，它会创建有关流量的观察结果，并根据其流量模式自动识别网络实体的角色。使用此信息与其他威胁情报来源（例如 Talos）相结合，安全云分析会生成警报，警告可能存在恶意行为。除警报外，安全云分析还提供网络和主机可视性以及所收集的情景信息，为您研究警报和查找恶意行为的来源提供更好的基础。

动态实体建模

动态实体建模可通过对防火墙事件和网络流数据执行行为分析来跟踪网络状态。在 Cisco Secure Cloud Analytics 环境中，实体是指可以随时间推移进行跟踪的对象，例如网络上的主机或终端。动态实体建模根据实体传输的流量及其在网络上执行的活动，收集实体的相关信息。与**日志记录分析和检测**许可证集成的 Cisco Secure Cloud Analytics 可以从防火墙事件和其他流量信息中进行提取，以便确定实体通常传输的流量类型。如果您购买了**全面网络分析和监控**许可证，则 Cisco Secure Cloud Analytics 还可以在对实体流量进行建模时纳入 NetFlow 和其他流量信息。Cisco Secure Cloud Analytics 会随着时间的推移更新这些模型，因为实体会继续发送流量，并且可能会发送不同的流量，从而保持每个实体的最新模型。根据这些信息，Cisco Secure Cloud Analytics 可以识别：

- 实体的角色，即实体通常执行的操作的描述符。例如，如果实体发送通常与邮件服务器关联的流量，Cisco Secure Cloud Analytics 会为该实体分配邮件服务器角色。角色/实体关系可以是多对一，因为实体可以履行多种角色。

- 对实体的观察结果，即有关实体在网络上的行为的事实，例如与外部 IP 地址建立的心跳连接或与另一个实体建立的远程访问会话。如果与 CDO 集成，则可以从防火墙事件中获取这些事实。如果您还购买了**全面的网络分析和监控**许可证，则系统还可以从 NetFlow 获取事实，并从防火墙事件和 NetFlow 中生成观察结果。观察结果本身并不具有超出其所代表的事实的意义。一个典型的客户可能有数千个观察结果和若干个警报。

警报和分析

Cisco Secure Cloud Analytics 会根据角色、观察结果和其他威胁情报的组合生成警报，这些警报是可操作项目，代表系统标识的可能的恶意行为。请注意，一个警报可能代表多个观察结果。如果防火墙记录了与同一连接和实体相关的多个连接事件，则可能只会生成一个警报。

例如，新的内部设备观察结果本身并不构成可能的恶意行为。但是，随着时间的推移，如果实体传输的流量与域控制器一致，则系统会向该实体分配域控制器角色。如果实体随后使用异常端口与之前未建立连接的外部服务器建立了连接，并且传输了大量的数据，则系统将记录新的大型连接（外部）观察结果和异常域控制器观察结果。如果该外部服务器被识别为一个 Talos 监视列表，则所有这些信息的组合将导致 Cisco Secure Cloud Analytics 生成此实体行为的警报，从而提示您采取进一步措施来研究和补救恶意行为。

在 Cisco Secure Cloud Analytics Web 门户 UI 中打开警报时，您可以查看导致系统生成该警报的支持性观察结果。您还可以从这些观察结果中查看有关所涉实体的其他背景信息，包括它们传输的流量以及外部威胁情报（如果可用）。您还可以查看实体涉及的其他观察结果和警报，然后确定此行为是否与其他潜在恶意行为相关。

请注意，在 Cisco Secure Cloud Analytics 中查看和关闭警报时，无法允许或阻止来自 Cisco Secure Cloud Analytics UI 的流量。如果在主动模式下部署设备，则必须更新防火墙访问控制规则以允许或阻止流量；如果在被动模式下部署防火墙，则必须更新防火墙访问控制规则。

使用基于防火墙事件的警报

所需许可证： 日志记录分析和检测 或 全面网络分析和监控

警报工作流程

警报的工作流程基于其状态。当系统生成警报时，其默认状态为“待处理”，并且未分配任何用户。当您查看警报总结时，默认情况下会显示所有待处理警报，因为这些是最需要关注的。

注意：如果您拥有**全面网络分析和监控**许可证，则警报可以基于从 NetFlow 生成的观察结果、从防火墙事件生成的观察结果或来自两个数据源的观察结果。

查看警报总结时，可以分配和标记警报，以及将其状态更新为初始分类。您可以使用过滤器和搜索功能查找特定警报，也可以显示不同状态的警报或具有不同标记或负责人的警报。您可以将警报的状态设置为“已暂停”，在这种情况下，警报要等暂停期过后才会重新显示在待处理警报列表中。您也可以移除警报的“已暂停”状态，使其再次显示为待处理警报。查看警报时，您可以将其分配给您自己或系统中的其他用户。用户可以搜索分配给其用户名的所有警报。

在警报摘要中，您可以查看警报详细信息页面。此页面允许您查看有关生成此警报的支持性观察结果的其他背景信息，以及有关此警报中涉及的实体的其他背景信息。这些信息可帮助您查明实际问题，以便进一步研究网络上的问题，并且有可能解决恶意行为。

当您在 CDO 中的 Stealthwatch 云 web 门户 UI 和网络中进行研究时，可以进行备注，描述您对警报的发现。这有助于为您的研究创建记录，供您将来参考。

完成分析后，您可以将状态更新为“已关闭”，使其不再默认显示为待处理警报。如果情况发生变化，您还可以在将来重新打开已关闭的警报。

下面介绍有关如何调查给定警报的一般准则和建议。Stealthwatch 云会在记录警报时提供附加背景信息，因此，您可以使用此信息帮助指导调查工作。

这些步骤既不全面，也非包罗万象。它们仅提供一个总体框架来帮助您开始调查警报。

通常，查看警报时可以采取以下步骤：

1. 对待处理警报进行分类, on page 626
2. 暂停警报以供以后分析, on page 626
3. 更新警报以进行进一步调查, on page 627
4. 查看警报并开始调查, on page 627
5. 检查实体和用户, on page 629
6. 使用安全云分析补救问题, on page 629
7. 更新并关闭警报, on page 630

对待处理警报进行分类

对待处理警报进行分类，特别是如果要调查多个待处理警报：

- 有关从 CDO 交叉启动和查看警报的详细信息，请参阅从 CDO 查看 Cisco Secure Cloud Analytics 警报。

询问以下问题：

- 您是否将此警报类型配置为高优先级？
- 您是否为受影响的子网设置了高灵敏度？
- 这是网络上新实体的异常行为吗？
- 实体的正常角色是什么，此警报中的行为与该角色的匹配度如何？
- 这是否是此实体正常行为的异常偏离？
- 如果用户参与其中，这是用户的预期行为还是异常行为？
- 受保护数据或敏感数据是否有被泄露的风险？
- 如果允许此行为继续下去，会对网络产生多严重的影响？
- 如果与外部实体有通信，这些实体过去是否与您网络上的其他实体建立了连接？

如果这是高优先级警报，请考虑将该实体与互联网隔离，或以其他方式关闭其连接，然后再继续调查。

暂停警报以供以后分析

当警报的优先级较低（与其他警报相比）时，可将其暂停。例如，如果您的组织将邮件服务器重新定位为 FTP 服务器，并且系统生成紧急配置文件警报（表明一个实体的当前流量匹配了它以前没有匹配的行为概要文件），您可以暂停此警报（因为这是预期行为），并在以后重新访问它。已暂停的警报不会与待处理警报一起显示；您必须专门过滤才能查看这些暂停的警报。

暂停警报：

Procedure

步骤 1 点击**关闭警报 (Close Alert)**。

步骤 2 在暂停此警报窗格中，从下拉列表中选择暂停时段。

步骤 3 点击**保存 (Save)**。

What to do next

当您准备好查看这些警报时，可以取消暂停该警报。这会将状态设置为“未处理”(Open)，并在其他“未处理”的警报旁边显示该警报。

取消暂停已暂停的警报：

- 从暂停的警报中，点击**取消暂停警报 (Unsnooze Alert)**。

更新警报以进行进一步调查

打开警报详细信息：

Procedure

步骤 1 选择**监控 (Monitor)** > **警报 (Alerts)**。

步骤 2 点击警报类型名称。

What to do next

根据您的初始分类和优先级，分配警报并标记：

1. 从**被分派人 (Assignee)** 下拉列表中选择用户以分配警报，以便用户可以开始调查。
2. 从下拉列表中选择一个或多个**标签**，以将标签添加到警报，以便更好地对警报进行分类以供将来识别，并尝试在警报中建立长期模式。

3. 输入**为此警报添加注释 (Comment on this alert)**，然后点击**注释 (Comment)** 以根据需要留下注释，以跟踪您的初始发现，并协助分配到警报的人员。警报同时跟踪系统注释和用户注释。

查看警报并开始调查

如果您正在查看已分配的警报，请查看警报详细信息以了解 Stealthwatch 云生成警报的原因。查看支持性观察结果，了解这些观察结果对源实体的意义。

请注意，如果警报是基于防火墙事件生成的，则系统不会注意到您的防火墙部署是此警报的来源。

查看此源实体的所有支持性观察结果，以了解其一般行为和模式，并查看此活动是否可能影响着某个长期趋势：

过程

步骤 1 在观察结果控制面板上，点击观察结果类型旁边的箭头图标 ( )，以查看该类型的所有已记录观察结果。

步骤 2 点击**网络的所有观察结果 (All Observations for Network)** 旁边的箭头图标 ( )，查看此警报的源实体的所有已记录观察结果。

如果要对这些观察结果执行其他分析，请下载逗号分隔值文件中的支持观察结果：

- 在警报详细信息的支持观察结果窗格中，点击 **CSV**。

从观察结果，确定源实体行为是否指示恶意行为。如果源实体与多个外部实体建立了连接，请确定外部实体是否以某种方式相关，例如它们是否都具有相似的地理位置信息，或者它们的 IP 地址是否来自同一子网。

从源实体 IP 地址或主机名称查看有关源实体的其他背景信息，包括它可能涉及的其他警报和观察结果、有关设备本身的信息以及它传输的会话流量类型：

- 从 IP 地址或主机名下拉列表中选择**警报 (Alerts)**，以查看与该实体相关的所有警报。
- 从 IP 地址或主机名下拉列表中选择**观察结果 (Observations)**，以查看与实体相关的所有观察结果。
- 从 IP 地址或主机名下拉列表中选择**设备 (Device)**，以查看有关设备的信息。
- 从 IP 地址或主机名下拉列表中选择**会话流量 (Session Traffic)**，以查看与此实体相关的会话流量。
- 从 IP 地址或主机名下拉列表中选择**复制 (Copy)** 以复制 IP 地址或主机名。

请注意，Stealthwatch 云中的源实体始终位于您的网络内部。将此与防火墙事件中的发起方 IP 进行对比，后者指示发起连接的实体，并且可能位于您的网络内部或外部。

从观察结果中，检查有关其他外部实体的信息。检查地理位置信息，确定是否有任何地理位置数据或 Umbrella 数据标识恶意实体。查看这些实体生成的流量。检查 Talos、AbuseIPDB 或 Google 是否

有关于这些实体的任何信息。查找多天的IP地址，并查看外部实体与您网络上的实体建立的其他类型的连接。如有必要，请找到这些内部实体，并确定是否有任何证据表明存在攻击活动或意外行为。

查看与源实体建立了连接的外部实体 IP 地址或主机名称的背景信息：

- 从 IP 地址或主机名下拉列表中选择 **IP 流量 (IP Traffic)**，以查看此实体的最近流量信息。
- 从IP地址或主机名下拉列表中选择**会话流量 (Session Traffic)**，以查看此实体的最近会话流量信息。
- 从 IP 地址或主机名下拉列表中选择 **AbuseIPDB**，以查看有关 AbuseIPDB 网页实体的信息。
- 从 IP 地址或主机名下拉列表中选择**思科 Umbrella (Cisco Umbrella)**，可在 Cisco Umbrella 网站上查看有关此实体的信息。
- 从 IP 地址或主机名下拉列表中选择 **Google 搜索 (Google Search)**，以在 Google 上搜索此 IP 地址。
- 从 IP 地址或主机名下拉列表中选择 **Talos 智能 (Talos Intelligence)**，以查看有关 Talos 网页的信息。
- 从 IP 地址或主机名下拉列表中选择**将 IP 添加到监视列表 (Add IP to watchlist)**，以将此实体添加到监视列表。
- 从 IP 地址或主机名下拉列表中选择**查找多天的 IP (Find IP on multiple days)**，以搜索此实体上个月的流量。
- 从 IP 地址或主机名下拉列表中选择**复制 (Copy)** 以复制 IP 地址或主机名。

请注意，Stealthwatch 云中的连接实体始终位于您的网络外部。将此与防火墙事件中的响应方 IP 进行对比，后者指示响应连接请求的实体，并且可能位于您的网络的内部或外部。

就您的发现进行备注。

- 在警报详细信息中，输入**对此警报的注释 (Comment on this alert)**，然后点击**注释 (Comment)**。

检查实体和用户

在 Stealthwatch 云门户 UI 中查看警报后，您可以直接对源实体、可能与此警报相关的任何用户以及其他相关实体执行其他检查。

- 确定源实体在网络上的物理位置或云中的位置，并直接访问它。找到此实体的日志文件。如果它是网络上的物理实体，请访问设备以查看日志信息，并查看是否有任何信息表明是什么导致了此行为。如果它是虚拟实体或存储在云中，请访问日志并搜索与此实体相关的条目。检查日志，了解有关未经授权的登录、未经批准的配置更改等活动的更多信息。
- 检查实体。确定您能否识别实体本身上的恶意软件或漏洞。查看是否发生了一些恶意更改，包括设备是否发生了物理更改，例如插入了未经组织批准的 U 盘。
- 确定所涉及的用户来自您的网络内部还是外部。如果可能，询问他们当时在做什么。如果询问未果，请确定他们是否应该具有访问权限，以及是否发生了导致此行为的情况，例如，离职员工在离开公司之前将文件上传到外部服务器。

就您的发现进行备注：

- 在警报详细信息中，输入**对此警报的注释 (Comment on this alert)**，然后点击**注释 (Comment)**。

更新并关闭警报

根据您的调查结果添加其他标签：

Procedure

步骤 1 在 Cisco Secure Cloud Analytics 门户 UI 中，选择**监控 (Monitor)** > **警报 (Alerts)**。

步骤 2 从下拉列表中选择一个或多个**标签**。

添加描述调查结果的最终注释，以及所采取的任何补救步骤：

- 在警报的详细信息中，输入**为此警报添加注释 (Comment on this alert)**，然后点击**注释 (Comment)**。

关闭警报，然后将其标记为有用或无用：

1. 在警报的详细信息中，点击**关闭警报 (Close Alert)**。
2. 如果警报有用，请选择**是 (Yes)**；如果警报无用，请点击**否 (No)**。请注意，这并不一定意味着该警报是由恶意行为导致的，而只是表示它对您的组织有所帮助。
3. 点击**保存 (Save)**。

What to do next

重新打开已关闭的警报

如果您发现与已关闭警报相关的其他信息，或者想要添加与该警报相关的更多备注，则可以将其重新打开，并将状态更改为“待处理”。然后，您可以根据需要对警报进行更改，并在其他调查完成后再次将其关闭。

重新打开已关闭的警报：

- 在已关闭警报的详细信息中，点击**重新打开警报 (Reopen Alert)**。

修改警报优先级

所需许可证 (Required License)： 日志记录分析和检测 (Logging Analytics and Detection) 或**全面网络分析和监控 (Total Network Analytics and Monitoring)**

警报类型具有默认优先级，这会影响系统对生成此类警报的敏感程度。根据思科情报和其他因素，警报的优先级默认为低或正常。根据您的网络环境，您可能希望重新确定警报类型的优先级，以强调您关注的某些警报。您可以将任何风险通告类型配置为低、正常或高优先级。

- 选择**监控 (Monitor)** > **警报 (Alerts)**。
- 点击设置下拉图标 ()，然后选择警报类型和优先级。
- 点击警报类型旁边的编辑图标 ()，然后选择低、中或高以更改优先级。

在事件日志记录页面中搜索和过滤事件

搜索和过滤特定事件的历史和实时事件表的方式与在CDO中搜索和过滤其他信息时的方式相同。当您添加过滤条件时，CDO 就会开始限制其在“事件”(Events) 页面上显示的内容。您还可以在搜索字段中输入搜索条件，以便查找具有特定值的事件。如果结合使用过滤和搜索机制，搜索会尝试在过滤事件后从显示的结果中查找您输入的值。

以下是执行搜索事件日志的选项：

- 在事件日志记录页面中搜索事件，第 676 页
- 在后台搜索历史事件，第 676 页

过滤实时事件的方式与过滤历史事件的方式相同，但不能按时间过滤实时事件。

了解这些过滤方法：

- 过滤实时或历史事件，第 669 页
- 仅过滤 NetFlow 事件，第 671 页
- 过滤 ASA 或 FDM 管理 设备系统日志事件，但不过滤 ASA NetFlow 事件，第 671 页
- 组合过滤器元素，第 671 页

过滤实时或历史事件

此程序介绍了如何使用事件过滤查看“事件日志记录”(Event Logging) 页面中的事件子集。如果您发现自己重复使用某些过滤条件，则可以创建自定义过滤器并保存。有关详细信息，请参阅可自定义的事件过滤器。

Procedure

步骤 1 在导航栏中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**

步骤 2 点击“历史”(Historical) 或“实时”(Live) 选项卡。

步骤 3 点击过滤器按钮 。点击固定图标 可固定打开过滤列。

步骤 4 点击没有已保存过滤器元素的视图选项卡。

步骤 5 选择要作为过滤条件的事件详细信息：

- **FTD 事件类型**
  - 连接 - 显示访问控制规则中的连接事件。
  - 文件 - 显示访问控制规则中文件策略报告的事件。
  - 入侵 - 显示访问控制规则中入侵策略报告的事件。
  - 恶意软件 - 显示访问控制规则中的恶意软件策略报告的事件。

  有关这些事件类型的详细信息，请参阅 FDM 管理 事件类型。
- ASA **事件类型 (Event Types)** - 这些事件类型表示系统日志或 NetFlow 事件组。
- **时间范围 (Time Range)** - 点击开始或结束时间字段以选择要显示的时间段的开始和结束时间。时间戳以计算机的本地时间显示。
- **操作 (Action)** - 指定规则定义的安全操作。输入的值必须与要查找的内容完全匹配；但是，大小写无关紧要。为连接、文件、入侵、恶意软件、系统日志和 NetFlow 事件类型输入不同的值：
  - 对于连接事件类型，过滤器在 AC_RuleAction 属性中搜索匹配项。这些值可以是“允许”(Allow)、“阻止”(Block)、“信任”(Trust)。
  - 对于文件事件类型，过滤器在 FileAction 属性中搜索匹配项。这些值可以是“允许”、“阻止”、“信任”。
  - 对于入侵事件类型，过滤器在 InLineResult 属性中搜索匹配项。这些值可以是 “已允许”(Allowed)、“已阻止”(Blocked)、“已信任”(Trusted)。
  - 对于恶意软件事件类型，过滤器会在 FileAction 属性中搜索匹配项。这些值可以是“云查找超时”(Cloud Lookup Timeout)。
  - 对于系统日志和 NetFlow 事件类型，过滤器在操作属性中搜索匹配项。
- **传感器 ID (Sensor ID)** - 传感器 ID 是将事件发送到安全事件连接器的管理 IP 地址。

  对于 FDM 管理 设备，传感器 ID 通常是设备管理接口的 IP 地址。
- **IP 地址**
  - **发起方 (Initiator)** - 这是网络流量源的 IP 地址。发起方地址字段的值对应于事件详细信息中发起方 IP 字段的值。您可以输入单个地址（例如 10.10.10.100）或以 CIDR 表示法定义的网络（例如 10.10.10.0/24）。
  - **响应方 (Responder)** - 这是流数据包的目的 IP 地址。“目的地址”(Destination address) 字段的值对应于事件详细信息中 ResponderIP 字段中的值。您可以输入单个地址（例如 10.10.10.100）或以 CIDR 表示法定义的网络（例如 10.10.10.0/24）。
- 端口
  - **发起方 (Initiator)** - 会话发起方使用的端口或 ICMP 类型。源端口的值对应于事件详细信息中的发起方端口的值。（添加范围 - 起始端口和结束端口之间的空格或发起方和响应方）

- **响应方 (Reponder)** - 会话响应方使用的端口或 ICMP 代码。目标端口的值对应于事件详细信息中的 ResponderPort 值。

步骤 6 （可选）点击查看选项卡，将过滤器另存为自定义过滤器。

仅过滤 NetFlow 事件

此程序仅查找 ASA NetFlow 事件：

Procedure

步骤 1 从 CDO 菜单栏中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

步骤 2 点击过滤器图标 并将过滤器固定为打开状态。

步骤 3 检查 **Netflow** ASA 事件过滤器。

步骤 4 清除所有其他 ASA 事件过滤器。

事件日志记录表中仅显示 ASA NetFlow 事件。

过滤 ASA 或 FDM 管理 设备系统日志事件，但不过滤 ASA NetFlow 事件

此过程仅查找系统日志事件：

Procedure

步骤 1 从 CDO 菜单栏中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

步骤 2 点击过滤器图标 并将过滤器固定为打开状态。

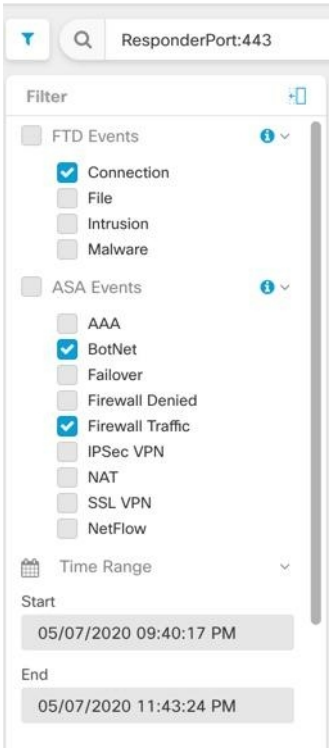
步骤 3 滚动到过滤器栏的底部，并确保**取消选中包括 NetFlow 事件 (Include NetFlow Events)** 过滤器。

步骤 4 向上滚动到 ASA 事件过滤器树，并确保**取消选中 NetFlow** 框。

步骤 5 选择 ASA 其余部分或 FTD 过滤条件。

组合过滤器元素

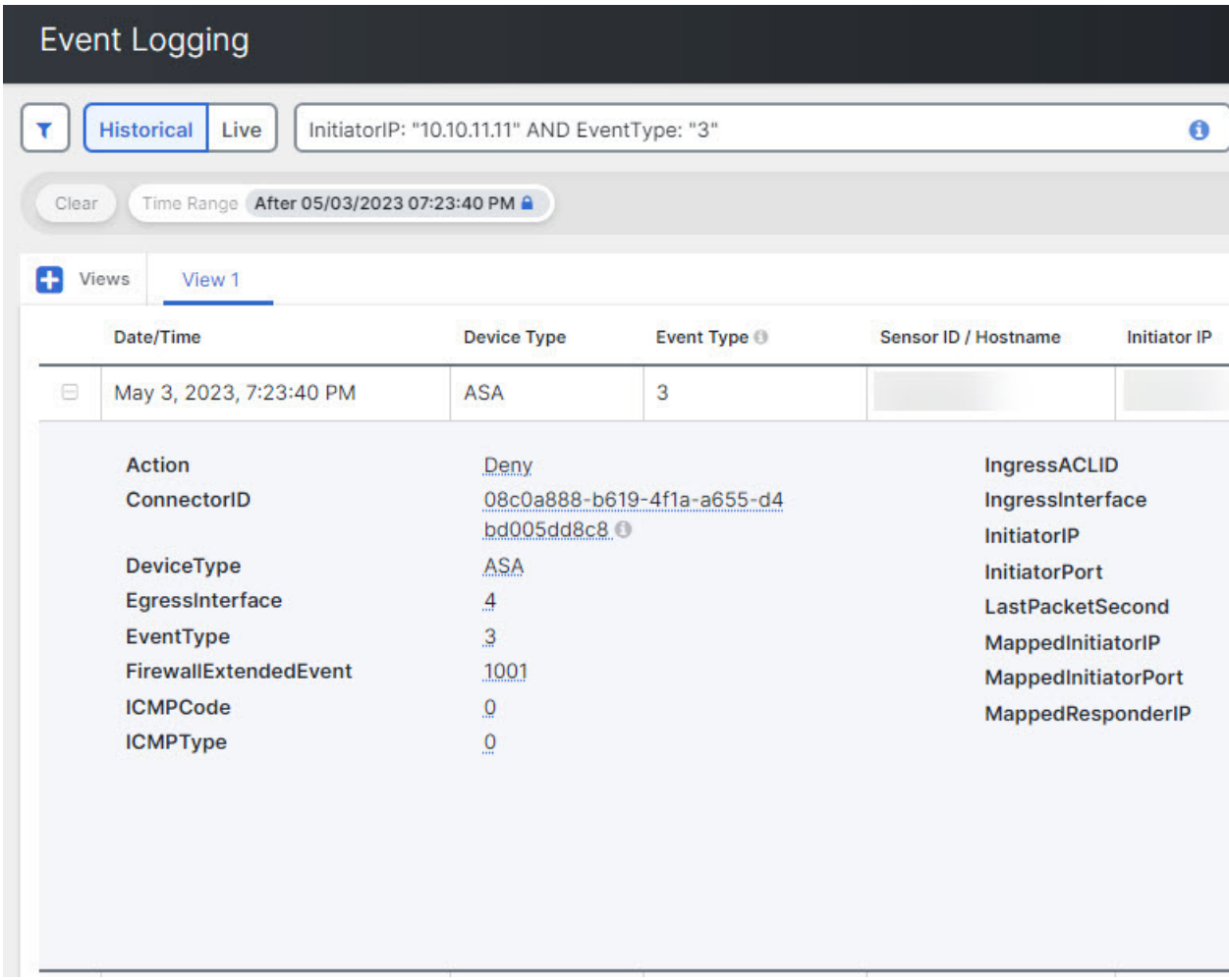
过滤事件通常遵循 CDO 中的标准过滤规则：过滤类别为“AND-ed”，类别中的值“OR-ed”。您还可以将过滤器与您自己的搜索条件配合使用。对于事件过滤器；但是，设备事件过滤器也是“OR-ed”。例如，如果在过滤器中选择了这些值：



使用此过滤器时，CDO 将显示 威胁防御 设备连接事件**或** ASA 僵尸网络**或**防火墙流量事件，**和**时间范围内两个时间之间发生的事件，**以及**还包含响应器端口 443 的事件。您可以按时间范围内的历史事件进行过滤。实时事件页面会始终显示最新事件。

搜索特定属性：值对

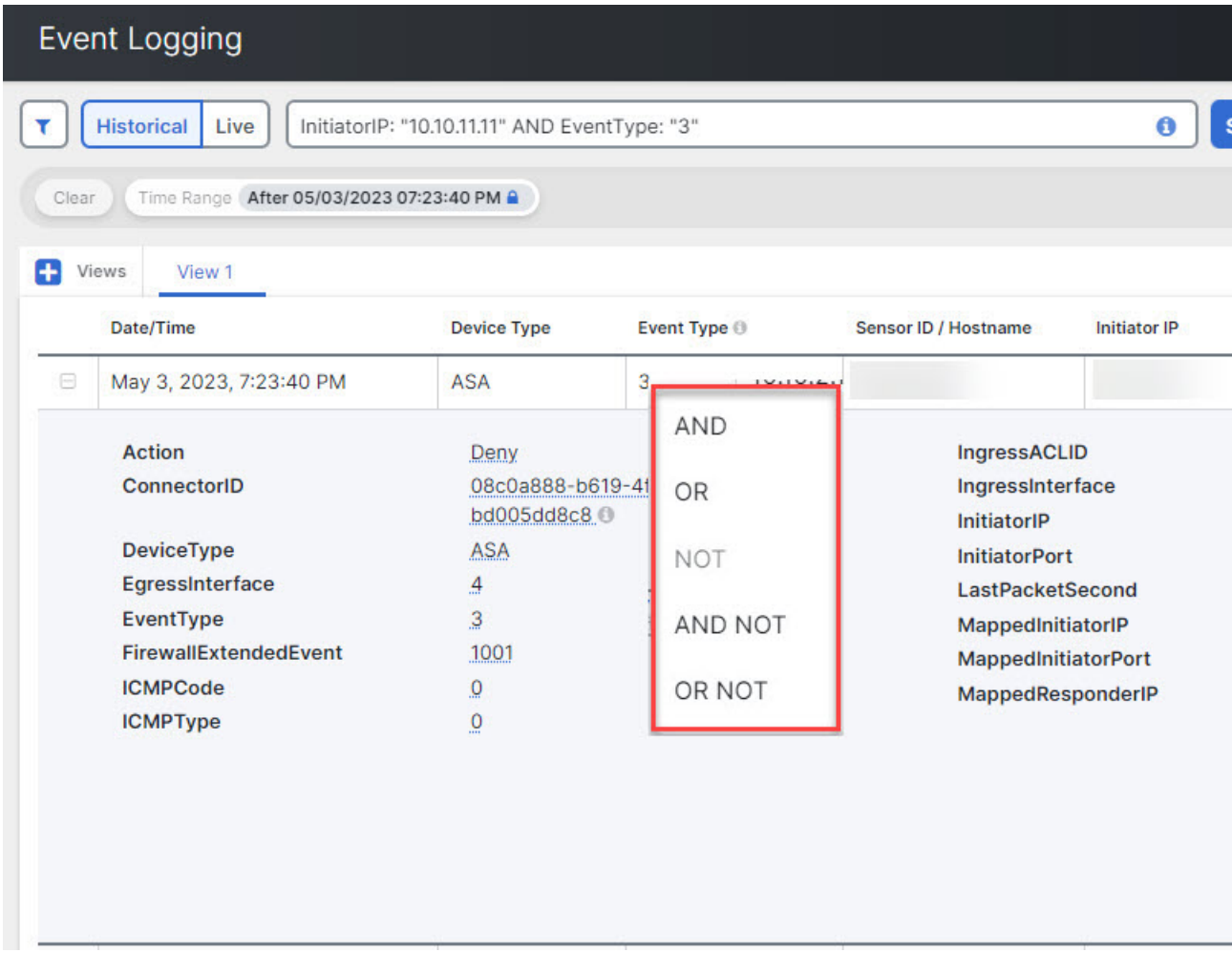
您可以通过在搜索字段中输入事件属性和值来搜索实时或历史事件。执行此操作的最简单方法是在“事件日志记录”(Event Logging) 表中点击要搜索的属性，然后 CDO 会在“搜索”(Search) 字段中输入该属性。在滚动鼠标时，您可以点击的事件会显示为蓝色。以下为输出示例：



在本示例中，通过滚动“InitiatorIP”值 10.10.11.11 并点击它即可开始搜索。发起方 IP 及其值已被添加到搜索字符串中。接下来，滚动并点击事件类型 3，然后将其添加到搜索字符串中，并且 CDO 添加了 AND。因此，此搜索的结果将是从 10.10.11.11 和 3 种事件类型发起的事件列表。

请注意上面示例中值3旁边的放大镜。如果将鼠标悬停在放大镜上，您还可以选择AND、OR、AND NOT 和 OR NOT 运算符来匹配要添加到搜索中的值。

在下面的示例中，选择的是“OR”。此搜索的结果将是从 10.10.11.11 或 106023 种事件类型发起的事件列表。请注意，如果搜索字段为空，并且您右键点击表中的值，则只有NOT可用，因为没有其他值。



只要滚动鼠标指针并将其突出显示为蓝色，您就可以将该值添加到搜索字符串中。

AND、OR、NOT、AND NOT 和 OR NOT 过滤器运算符

以下是在搜索字符串中使用的“AND”、“OR”、“NOT”、“AND NOT”和“OR NOT”的行为：

和

在过滤器字符串中使用 AND 运算符可以查找包含所有属性的事件。AND 运算符不能位于搜索字符串的开头。

例如，下面的搜索字符串将搜索包含 TCP 协议、源自发起方 IP 地址 10.10.10.43 且从发起方端口 59614 发送的事件。正常情况下，每增加一个 AND 语句，符合条件的事件数量就会越来越少。

```
Protocol: "tcp" AND InitiatorIP: "10.10.10.43" AND InitiatorPort: "59614"
```

或

在过滤器字符串中使用OR运算符可以查找包含任何属性的事件。OR运算符不能位于搜索字符串的开头。

例如，下面的搜索字符串将在事件查看器中显示事件，这些事件包括 TCP 协议、源自发起方 IP 地址 10.10.10.43 或从发起方端口 59614 发送的事件。正常情况下，每增加一个 OR 语句，符合条件的事件数量就会越来越多。

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR InitiatorPort: "59614"
```

不

仅在搜索字符串的开头使用此选项，以便排除具有某些属性的事件。例如，此搜索字符串将从结果中排除任何具有 InitiatorIP 192.168.25.3 的事件。

```
NOT InitiatorIP: "192.168.25.3"
```

AND NOT

在过滤器字符串中使用 AND NOT 运算符可以排除包含某些属性的事件。AND NOT 不能用于搜索字符串的开头。

例如，此过滤器字符串将显示发起方 IP 为 192.168.25.3 的事件，但不会显示响应方 IP 地址为 10.10.10.1 的事件。

```
InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

您还可以组合使用 NOT 和 AND NOT，从而排除多个属性。例如，此过滤器字符串将排除具有 InitiatorIP 192.168.25.3 的事件以及具有 ResponderIP 10.10.10.1 的事件

```
NOT InitiatorIP: "192.168.25.3" AND NOT ResponderIP: "10.10.10.1"
```

OR NOT

使用 OR NOT 运算符可包含排除了某些元素的搜索结果。OR NOT 运算符不能用于搜索字符串的开头。

例如，此搜索字符串将查找协议为 TCP 或发起方 IP 为 10.10.10.43 的事件，或者非发起方端口 59614 的事件。

```
Protocol: "tcp" OR InitiatorIP: "10.10.10.43" OR NOT InitiatorPort: "59614"
```

您也可以这样考虑：搜索 (Protocol: "tcp") OR (InitiatorIP: "10.10.10.43") OR (NOT InitiatorPort: "59614")。

通配符搜索

使用星号 (*) 表示属性值字段中的 **attribute:value** 搜索可在事件中查找结果。例如，此过滤器字符串，

```
URL:*feedback*
```

将在事件的 URL 属性字段中查找包含字符串 **feedback** 的字符串。

相关信息：

- 在事件日志记录页面上显示和隐藏列
- 安全分析和日志记录中的事件属性

在后台搜索历史事件

通过CDO，您可以定义搜索条件，并根据任何已定义的搜索条件来搜索事件日志。通过使用后台搜索功能，您还可以在后台执行事件日志搜索，并在后台搜索完成后查看搜索结果。

根据您配置的订用警报和服务集成，当后台搜索完成后，您会收到通知。

您可以直接从“后台搜索”页面查看、下载或删除搜索结果。您还可以安排对一次性事件进行后台搜索，或安排周期性安排。导航至“通知设置”(Notification Settings) 页面以查看或修改订用选项。

在事件日志记录页面中搜索事件

使用搜索和后台搜索功能查看“事件日志记录”(Event Logging) 页面中记录的所有事件。请注意，只能对历史事件执行后台搜索。

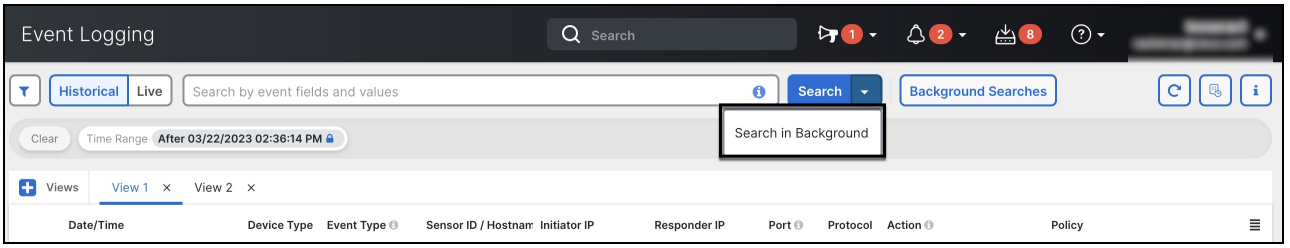
过程

步骤 1 在导航栏中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

步骤 2 点击**历史 (Historical)** 或**实时 (Live)** 选项卡。

步骤 3 导航至搜索栏，键入搜索表达式，然后输入 **搜索 (Search)** 按钮以执行搜索。您可以使用绝对时间范围或相对时间范围来缩小或扩大搜索范围。

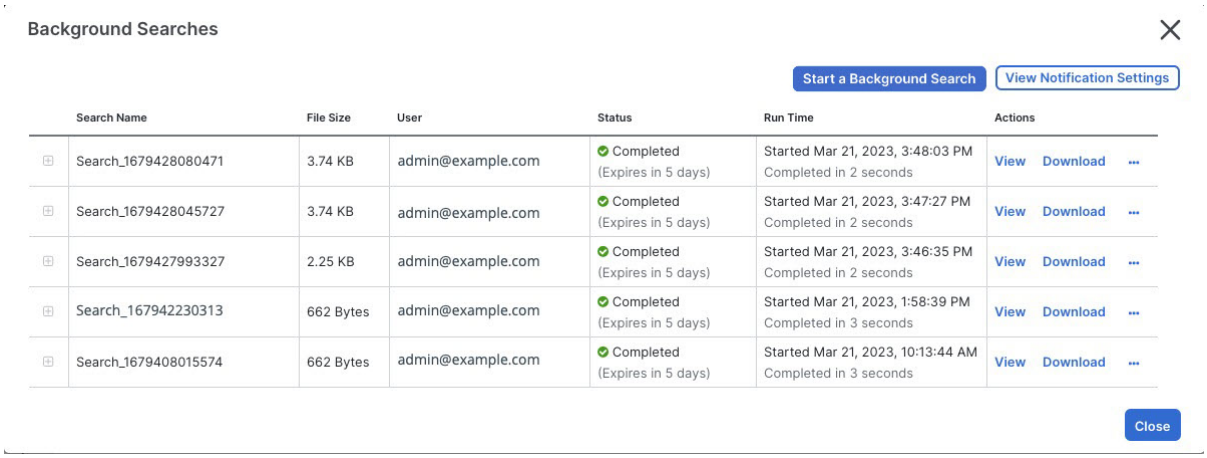
或者，从搜索下拉列表中选择在后台搜索，以便在离开搜索页面时在后台执行搜索。当搜索结果准备就绪时，您会收到通知。



如果点击**搜索 (Search)** 按钮，结果将直接显示在事件日志记录视图中。选择任何特定搜索结果后，搜索条件会显示在搜索栏中，以便于参考。

如果您选择在后台执行搜索，搜索操作会加入队列，并在搜索完成后通知您。您可以在后台执行多个搜索查询。

步骤 4 点击“背景搜索”按钮以查看“背景搜索”页面。



“后台搜索”页面显示搜索结果列表。您可以选择查看、下载或删除搜索结果。您还可以导航至“通知设置”页面以查看或修改订用选项。选择**开始后台搜索 (Start a Background Search)** 按钮可从此页面启动搜索。

有关查看或修改订用选项的信息，请参阅通知设置，第 48 页。

下一步做什么

如果需要重复查询，您可以将任何后台搜索转换为计划后台搜索。有关详细信息，请参阅在事件查看器中计划后台搜索，第 677 页。

在事件查看器中计划后台搜索

在事件查看器页面的后台计划定期查询。只能为历史事件安排搜索。您可以随时修改或取消预定搜索。您还可以将现有查询修改为周期性搜索。

注释 您可以选择获取有关已开始、已完成或已失败的搜索的警报。有关详细信息，请参阅通知设置，第 48 页。

只能为**历史**事件安排后台搜索。使用以下步骤创建计划的后台搜索：

过程

步骤 1 在导航栏中，选择**分析 (Analytics)** > **事件日志记录 (Event Logging)**。

步骤 2 点击**历史 (Historical)** 开关将其选中。您只能为历史事件安排后台搜索。

步骤 3 在搜索栏中，键入要搜索的搜索表达式。点击**搜索 (Search)** 下拉按钮，然后选择**在后台搜索 (Search in background)**。

步骤 4 （可选）重命名搜索。

步骤 5 默认情况下，**立即搜索 (Search Now)** 复选框处于选中状态。如果已选中，将在保存时开始搜索；如果取消选中，则后台查询仅作为未来搜索运行。

步骤 6 检查**设置定期计划 (Setup recurring schedule)** 并配置以下设置：

- **搜索最近日志 (Search Logs for the Last)** - 要搜索多长时间以前的日志。
- **频率 (Frequency)** - 您希望进行预定搜索的频率。

步骤 7 确认窗口底部的计划搜索条件。选择**计划并立即搜索 (Schedule and Search Now)**。或者，如果您没有选择立即开始搜索，则该按钮显示为**计划搜索 (Schedule Search)**

下一步做什么

计划后台搜索的结果最多可查看 7 天，然后 CDO 会自动将其删除。

下载后台搜索

搜索结果和计划查询会在 CDO 自动删除之前存储 7 天。下载对历史事件执行的后台搜索的 CSV 副本。

过程

步骤 1 在导航窗格中，转到**分析 (Analytics)** > **事件日志记录 (Event Logging)**。

步骤 2 点击**后台搜索 (Background Searches)** > **操作 (Actions)** > **下载 (Download)**。

步骤 3 找到您的搜索内容。计划的搜索存储在**查询 (Queries)** 选项卡下。

步骤 4 点击 **Download**。.CSV 文件会自动下载到本地驱动器上的默认存储位置。

数据存储计划

您需要购买反映思科云每天从您载入的 ASA和 FDM 托管设备接收的事件数量的数据存储计划。这称为“每日注入速率”。数据计划有整数 GB/天和 1 年、3 年或 5 年期限。确定注入速率的最佳方法是在购买之前参加安全日志分析 (SaaS) 的免费试用。这将为您提供对事件数量的一个很好的估计。

客户自动获得 90 天的滚动数据存储。这意味着最近 90 天的事件存储在思科云中，第 91 天将被删除。

客户可以升级到超过默认90天的额外事件保留，或通过更改订单对现有订用添加额外的每日量（GB/天），并且只需按比例为剩余的订用期限计费。

有关数据计划的所有详细信息，请参阅《安全日志分析 (SaaS) 订购指南》。

Note 如果您拥有安全分析和日志记录许可证和数据计划，然后在之后获得了不同的安全分析和日志记录许可证，则无需获得不同的数据计划。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安全分析和日志记录许可证。

我的配额会统计哪些数据？

发送到安全事件连接器的所有事件都在安全日志分析 (SaaS) 云中累积，并根据您的数据分配进行计数。

过滤您在事件查看器中看到的内容并不会减少安全日志分析 (SaaS) 云中存储的事件数量，而是会减少您可以在事件查看器中看到的事件数量。

您的事件在安全日志分析 (SaaS) 云中存储 90 天；之后，它们将被清除。

我们的存储配额很快用尽，我们该怎么办？

以下是解决该问题的两种方法：

- 请求更多存储空间。https://www.cisco.com/c/en/us/products/collateral/security/security-analytics-logging/guide-c07-742707.html您可能低估了您的需求。
- 减少记录事件的规则数量。您可以从 SSL 策略规则、安全情报规则、访问控制规则以及入侵策略以及文件和恶意软件策略中记录事件。检查您正在记录的内容。您是否需要记录尽可能多的规则和策略的事件？

延长事件存储持续时间并增加事件存储容量

安全分析和日志记录客户在购买任何这些许可证时都会收到 90 天的事件存储。许可，第 591 页

- **日志记录故障排除**
- **日志记录分析和检测**
- **全面的网络分析和监控**

您可以选择在首次购买许可证时或在许可证有效期内的任何时间将许可证升级为具有 1 年、2 年或 3 年的滚动事件存储。

首次购买安全分析和日志记录许可证时，系统会询问您是否要升级存储容量。如果您回答“是”，系统会在您购买的 PID 列表中添加一个额外的产品标识符 (PID)。

如果您在许可期限中间决定扩展滚动事件存储或增加事件云存储量，您可以：

过程

步骤 1 在思科商务工作空间上登录您的账户。

步骤 2 选择您的 Cisco Defense Orchestrator PID。

步骤 3 按照提示升级存储容量的长度或容量。

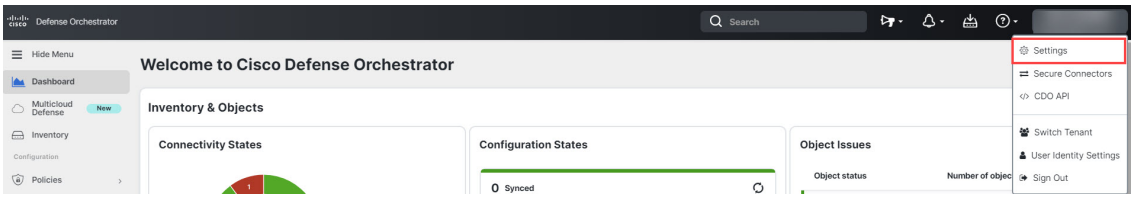
增加的成本将根据现有许可证的剩余期限按比例分配。有关详细说明，请参阅《安全日志分析 (SaaS) 订购指南》。

查看安全分析和日志记录数据计划的使用情况

要查看每月的日志记录限制、已使用的存储量以及使用期何时重置为零，请执行以下操作：

Procedure

步骤 1 点击租户，选择**设置 (Settings)**。



步骤 2 点击**日志记录设置 (Logging Settings)**。

步骤 3 您还可以点击查看历史使用情况，查看最近 12 个月的存储使用情况。

查找用于安全日志记录分析 (SaaS) 的设备 TCP、UDP 和 NSEL 端口

安全日志分析 (SaaS) 允许您将事件从您的 ASA 或 FDM 管理 设备发送到安全事件连接器 (SEC) 上的某些 UDP、TCP 或 NSEL 端口。然后，SEC 会将这些事件转发到思科云。

如果这些端口尚未被占用，SEC 会将其用于接收事件，而安全日志分析 (SaaS) 文档会建议您在配置功能时使用这些端口。

- TCP：10125
- UDP：10025
- NSEL：10425

如果这些端口已被占用，则在配置安全日志记录分析 (SaaS) 之前，请查看 SEC 设备详细信息，以确定其实际用于接收事件的端口。

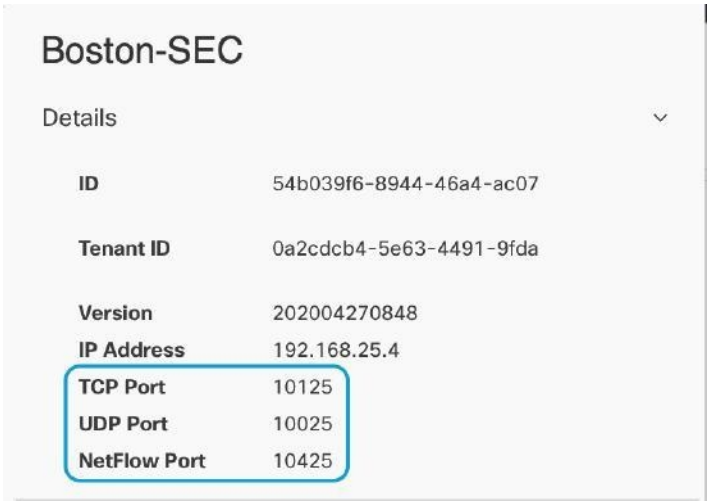
要查找 SEC 使用的端口号，请执行以下操作：

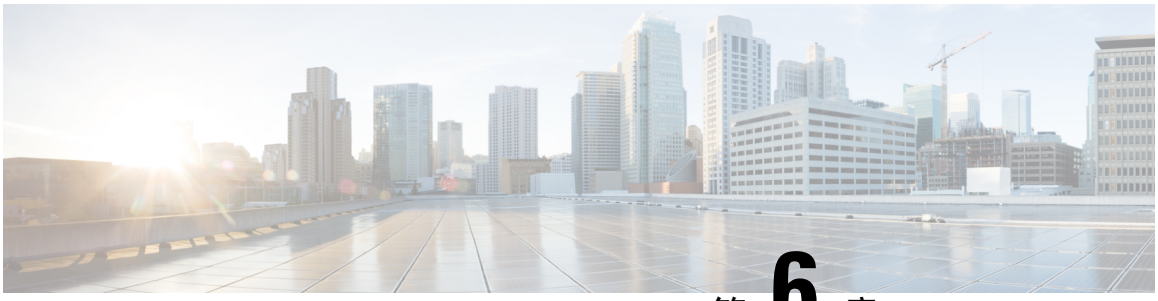
Procedure

步骤 1 从 CDO 菜单中，选择 **工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

步骤 2 在“安全连接器”(Secure Connectors) 页面中，选择要向其发送事件的 SEC。

步骤 3 在“详细信息”(Details) 窗格中，您将看到应向其发送事件的 TCP、UDP 和 NetFlow (NSEL) 端口。





第 6 章

将 CDO 与 Cisco Security Cloud Sign On 集成

SecureX和CDO

思科 SecureX 平台结合了思科的集成安全产品组合以及客户基础设施的优势，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。通过集成平台中的连接技术，SecureX 提供了可衡量的洞察力、预期成果以及无与伦比的跨团队协作。有关 SecureX 是什么以及此平台提供的功能的更多信息，请参阅关于 SecureX。

允许 SecureX 访问您的 CDO 租户会生成设备事件摘要，包括设备总数以及出现错误的设备、存在冲突的设备以及当前可能不同步的设备。事件摘要还提供了第二个窗口，用于记录当前应用的策略以及与这些策略关联的对象。策略按设备类型定义，对象通过对象类型标识。

将 CDO 模块添加到 SecureX 控制面板需要多个步骤。有关详细信息，请参阅将 CDO 添加到 SecureX。

Warning 如果您尚未合并 CDO 和 SecureX 账户，则可能无法查看所有已自行激活设备的事件。我们强烈建议在 SecureX 中创建 CDO 模块之前合并您的账户。有关详细信息，请参阅合并您的 CDO 和 SecureX 帐户。

SecureX 功能区

无论您是否创建 SecureX 账户，CDO 中都可以使用 SecureX 功能区。点击页面底部的 SecureX 选项卡 

以展开功能区。

要使用功能区，您需要验证您的 SecureX 账户。我们强烈建议使用与访问 SecureX 相同的身份验证登录信息。功能区通过身份验证后，您可以直接从 CDO 使用 SecureX 功能。

有关详细信息，请参阅 SecureX 功能区文档。https://visibility.amp.cisco.com/iroh/iroh-auth/login?redirect_after_login=https://securex.us.security.cisco.com/help/ribbon

SecureX 故障排除

此体验涉及两种产品；请参阅以帮助识别、解决或查询您可能遇到的问题。SecureX 故障排除 , on page 737

相关信息：

- 关于 SecureX
- 合并您的 CDO 和 SecureX 帐户
- 在 CDO 中连接 SecureX, on page 685
- 在 CDO 中断开 SecureX 的连接, on page 686
- 将 CDO 添加到 SecureX
- SecureX 故障排除 , on page 737

合并您的 CDO 和 SecureX 帐户

如果您已有 SecureX 或思科威胁响应 (CTR) 账户，则需要合并 CDO 租户和 SecureX/CTR 账户，以便您的设备能够注册 SecureX。您的账户可以合并到 SecureX 门户。我们强烈建议在创建 CDO 模块之前合并您的账户。在您的账户合并之前，您将无法在 SecureX 中查看设备的事件或受益于其他 SecureX 功能。

Note 请注意何时启动此过程。将 CDO 合并到 SecureX 可能需要较长时间。

有关说明，请参阅合并账户。

Note 如果您在多个区域云上有账户，则必须为每个区域云单独合并账户。

相关信息：

- SecureX和CDO
- 将 CDO 添加到 SecureX
- SecureX 故障排除

将 CDO 添加到 SecureX

允许 SecureX 访问您注册的设备，并将 CDO 模块添加到 SecureX 控制面板，以查看您的设备策略和对象的摘要以及安全产品组合中的其他思科平台。

Note 请注意何时启动此过程。将 CDO 合并到 SecureX 可能需要较长时间。

准备工作

在 CDO 中连接 SecureX 之前，我们强烈建议执行以下操作：

- 您必须至少是 SecureX 账户的管理员。
- 您的 CDO 租户必须具有超级管理员用户角色。
- 合并您的租户账户，以促进租户通信。安全服务交换有关详细信息，请参阅合并您的 CDO 和 SecureX 帐户。
- 将 CDO 租户与 安全服务交换 合并后，请确保注销 CDO 租户并重新登录。
- 如果您已经这样做，请将 Cisco Secure Sign-On 配置为 SAML 单点登录身份提供程序 (Idp)，并使用 Duo Security 进行多因素身份验证 (MFA)。CDO 和 SecureX 均使用此身份验证方法。有关详细信息，请参阅将 SAML 单点登录与 Cisco Defense Orchestrator 集成。

Note **注意：**如果您有多个租户，则必须在 SecureX 中为每个租户创建一个模块。每个租户都需要唯一的 API 令牌进行授权。

在 CDO 中连接 SecureX

合并 SecureX 和 CDO 账户后，您必须授权两个平台之间的通信，并手动启用要添加到 SecureX 控制面板的 CDO 模块。通过 CDO UI 连接 SecureX，并查看设备策略、事件类型、对象等的摘要以及安全产品组合中的其他思科平台。

Note 如果您已在 SecureX 控制面板中配置了 CDO 模块，则 Connect Tenant to SecureX 选项将创建重复的 CDO 模块。如果遇到此问题，请参阅 SecureX 故障排除以了解详细信息。SecureX 故障排除 , on page 737

使用以下程序从 CDO 获取 API 令牌并将 CDO 模块添加到 SecureX：

Procedure

步骤 1 登录 CDO。

步骤 2 从右上角的用户菜单中，选择设置。

步骤 3 选择窗口左侧的常规设置选项卡。

步骤 4 找到租户设置部分，然后点击连接 SecureX。浏览器窗口会将您重定向到 SecureX 登录页面。使用您希望与 CDO 租户关联的组织凭证登录 SecureX。

步骤 5 成功登录 SecureX 后，浏览器会自动重定向回 CDO。在“常规设置”(General Settings) 页面的“用户管理”(User Management) 选项卡中，您将看到一个新用户，其中包含您登录 SecureX 的组织的名称。此用户为只读用户，仅用于向 SecureX 发送数据。

在 CDO 中断开 SecureX 的连接

您可以断开 CDO 与 SecureX 组织之间的通信请求。此选项不会从 SecureX 中删除组织，但会从 CDO 中删除只读 API 用户，并且以前与 SecureX 组织关联的租户会停止发送事件报告。

请注意，这不会将租户从 CDO 中的 SecureX 功能区注销，也不会以任何方式禁用功能区。要注销功能区，您必须在支持案例管理器中创建一个案例，以手动重置功能区登录。https://mycase.cloudapps.cisco.com/case此请求将您的租户从功能区注销。

过程

步骤 1 登录至 CDO。

步骤 2 从右上角的用户菜单中，选择设置。

步骤 3 选择窗口左侧的常规设置选项卡。

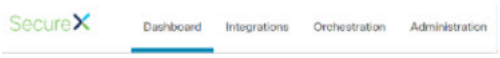
步骤 4 找到**租户设置 (Tenant Settings)** 部分，然后点击**断开 (Disconnect)**SecureX。在**常规设置 (General Settings)** 页面的**用户管理 (User Management)** 选项卡中，删除为向 SecureX 发送数据而创建的只读用户。

将 CDO 磁贴添加到 SecureX

启用 CDO 模块后，您现在可以将 CDO 磁贴添加到 SecureX 控制面板。产品的模块从 CDO 访问状态信息，并通过两个可能的磁贴选择将数据报告给控制面板。

使用以下程序将 CDO 磁贴添加到 SecureX 控制面板：

Procedure

步骤 1 在 SecureX **控制面板 (Dashboard)** 选项卡 

中，点击**新控制面板 (New Dashboard)**。如果这是您第一次访问 SecureX 控制面板，还可以点击**添加磁贴 (Add Tiles)**。

步骤 2 （可选）重命名控制面板。

Tip 如果您有多个租户，请使用此重命名选项来识别与 CDO 磁贴关联的租户。

步骤 3 从**可用磁贴 (Available Tiles)** 列表中选择 CDO，然后展开选项以查看可用磁贴。选中要包含在控制面板中的所有磁贴。

- **CDO 设备摘要 (CDO Device Summary)** - 此磁贴列出当前加入 CDO 租户的所有设备及其状态。

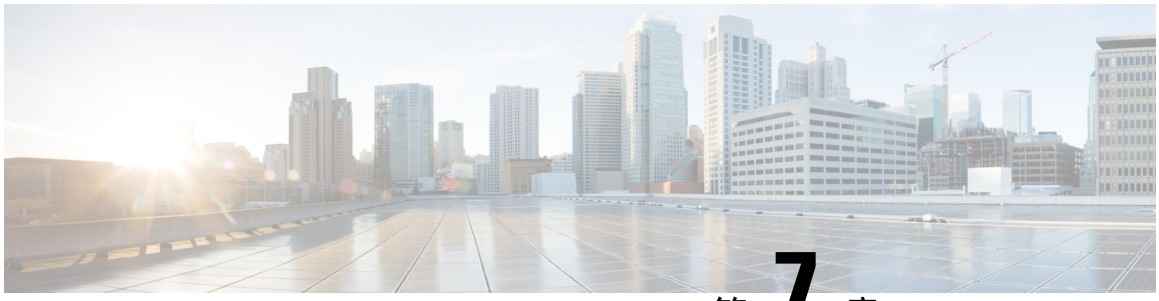
- **CDO 对象和策略 (CDO Objects and Policies)** - 此磁贴列出当前应用于设备的所有策略以及与这些策略关联的对象。

Note 如果未列出 CDO，则 SecureX 未保存来自 CDO 的有效 API 令牌。有关详细信息，请参阅将 CDO 磁贴添加到 SecureX。

步骤 4 点击保存 **(Save)**。

相关信息：

- 合并您的 CDO 和 SecureX 帐户
- SecureX 故障排除



第 7 章

故障排除

本章涵盖以下部分：

对 FDM 管理 设备进行故障排除

使用以下文章对您的设备进行故障排除：FDM 管理

执行摘要报告故障排除

您可能会生成网络运营报告，但看不到预期的结果，也可能根本看不到任何数据。在某些情况下，摘要可能会显示**无可用数据 (No data available)**。请考虑以下情形：

- CDO 从设备载入后每 **小时** 轮询一次事件。某些计划事件可以触发多个作业，这些作业以不同的时间间隔（每 10 分钟、60 分钟、6 小时或 24 小时）进行轮询。如果所选设备刚刚载入，可能没有足够的时间来收集和编译数据。
- 您的智能许可证可能不足。只有拥有足够许可证的设备才能生成数据。请参阅FDM 管理 设备许可类型, on page 198以确定生成所需数据所需的智能许可证。
- 未为访问控制规则启用日志记录。有关详细信息，请参阅FDM 管理 访问控制规则中的日志记录设置, on page 337。
- 您选择的时间范围可能没有足够的数据来显示，或者在选定的时间范围内可能未触发访问控制规则。在**时间范围 (Time Range)** 选项之间切换，并确定不同的时间段是否会影响报告。

FTD 自行激活故障排除

连接

- 使用 ping 检查设备连接。尝试直接从 ASA ping 通 FP 管理 IP 地址。如果 ICMP 阻止来自外部的通信，您将无法从互联网 ping 通 FP 管理接口。 cUrl/wget 有助于检查是否可在已配置的 IP/端口上访问 FP 管理接口。
- 检查 ASA 和/或 ASDM 软件版本的兼容性。有关详细信息，请参阅 CDO 支持的软件和硬件。
- 使用 ASA 日志确定 CDO 流量是否被 ASA 阻止。通过 SSH 连接到 FP HTTP 管理接口的尝试会记录在 /var/log/httpd/httpsd_access_log 中。

模块配置错误

- Unsupported configuration. 如果模块不符合特定要求，CDO 可能无法支持设备的配置。有关配置要求和证书支持的详细信息，请参阅中的 ASA 先决条件。

HTTP 身份验证

- CDO 在自行激活过程中发出基于令牌的 SSO 以对 ASA 设备进行身份验证。如果 ASA 处于多情景模式，则尝试从非管理情景载入 FP 模块可能会导致令牌问题。在 /var/log/mojo/mojo.log 中，无效的令牌被识别为 ASDM SSO 登录

由于许可证不足而失败

如果设备连接状态显示“许可证不足”(Insufficient License)，请执行以下操作：

- 等待一段时间，直到设备获得许可证。通常，思科智能软件管理器需要一些时间才能将新许可证应用于设备。
- 如果设备状态未更改，请从 CDO 注销并重新签名，以刷新 CDO 门户，以解决许可证服务器和设备之间的任何网络通信故障。
- 如果门户刷新未更改设备状态，请执行以下操作：

Procedure

步骤 1 从思科智能软件管理器生成新的注册密钥并进行复制。您可以观看生成智能许可视频了解详细信息。

步骤 2 在 CDO 导航栏中，点击**清单 (Inventory)** 页面。

步骤 3 点击**设备**选项卡。

步骤 4 点击相应的设备类型选项卡，然后选择状态为**许可证不足**的设备。

步骤 5 在**设备详细信息 (Device Details)** 窗格中，点击**许可证不足 (Insufficient Licenses)**中出现的**管理许可证 (Manage Licenses)**。此时将出现**管理许可证 (Manage Licenses)** 窗口。

步骤 6 在**激活 (Activate)** 字段中，粘贴新的注册密钥，然后点击**注册设备 (Register Device)**。

将新的注册密钥成功应用于设备后，其连接状态将变为**在线 (Online)**。

相关信息：

- 载入 威胁防御 设备
- 使用用户名、密码和 IP 地址载入 FDM 管理 设备, on page 168
- 应用或更新智能许可证

排除设备未注册故障

FDM 管理 设备可能已通过 防火墙设备管理器 从云注销。

执行以下操作，在云上重新注册设备：

过程

步骤 1 在**清单 (Inventory)** 页面中，点击**设备 (Devices)** 选项卡。

步骤 2 点击 FTD 选项卡并选择处于“设备未注册”状态的设备，然后查看右侧的错误消息。

步骤 3 如果未注册的设备是使用注册密钥自行激活的，则思科防御协调器会提示您生成新的注册密钥，因为之前应用的密钥已过期。

a) 点击刷新按钮以生成新的注册密钥，然后点击复制图标。
b) 登录到要向其重新注册 CDO 的设备的 防火墙设备管理器。
c) 在 **系统设置**下，点击 **云服务**。
d) 在 思科防御协调器 区域中，展开**入门 (Get Started)**。
e) 在**注册密钥 (Registration Key)**字段中，粘贴您在 CDO 中生成的注册密钥。
f) 点击**注册 (Register)**，然后点击**接受 (Accept)** 以接受思科披露声明。防火墙设备管理器 会将注册请求发送至 CDO。
g) 在 CDO 中刷新**清单 (Inventory)** 页面，直到您看到设备的连接状态更改为“读取错误”(Read Error)。
h) 点击 CDO 的**读取配置 (Read Configuration)** 以从设备读取配置。

步骤 4 如果未注册的设备是使用序列号自行激活的，CDO 会提示您从 防火墙设备管理器 自动注册设备。

a) 登录到要向其重新注册 CDO 的设备的 防火墙设备管理器。
b) 在 **系统设置**下，点击 **云服务**。
c) 选择**通过思科防御协调器自动注册租用 (Auto-enroll with Tenancy from Cisco Defense Orchestrator)** 选项并点击**注册 (Register)**。
d) 在 CDO 中刷新**清单 (Inventory)** 页面，直到您看到设备的连接状态更改为“读取错误”(Read Error)。

e) 点击 CDO 的**读取配置 (Read Configuration)** 以从设备读取配置。

在使用注册密钥自行激活期间对设备注册失败进行故障排除

未能解析云服务 FQDN

如果由于解析云服务 FQDN 失败而导致设备注册失败，请检查网络连接或 DNS 配置，然后尝试重新载入设备。

由于注册密钥无效而失败

如果由于注册密钥无效而导致设备注册失败（在防火墙设备管理器中粘贴不正确的注册密钥时可能会发生这种情况）。

再次从思科防御协调器复制相同的注册密钥，并尝试注册设备。如果设备已获得智能许可，请确保在 防火墙设备管理器 中粘贴注册密钥之前删除智能许可证。

由于许可证不足而失败

如果设备连接状态显示“许可证不足”(Insufficient License)，请执行以下操作：

- 等待一段时间，直到设备获得许可证。通常，思科智能软件管理器需要一些时间才能将新许可证应用于设备。
- 如果设备状态未更改，请从 CDO 注销并重新签名，以刷新 CDO 门户，以解决许可证服务器和设备之间的任何网络通信问题。
- 如果门户刷新未更改设备状态，请执行以下操作：
  1. 从思科智能软件管理器生成新的注册密钥并进行复制。您可以观看生成智能许可视频了解详细信息。
  2. 在 CDO 导航栏中，点击**清单 (Inventory)** 页面。
  3. 选择许可证状态为“不足”的设备。
  4. 在**设备详细信息 (Device Details)** 窗格中，点击“许可证不足”(Insufficient Licenses) 中出现的**管理许可证 (Manage Licenses)**。打开“管理帐户”(Manage Accounts) 窗口。
  5. 在**激活 (Activate)** 字段中，粘贴新的注册密钥，然后点击**注册设备 (Register Device)**。
- 将新的注册密钥成功应用于设备后，其连接状态将变为**在线 (Online)**。

入侵防御系统故障排除

IPS 策略选项有哪些？

每个已自行激活的设备都会自动关联到 思科防御协调器 提供的名为“默认覆盖”的 IPS 策略。CDO 会为每台 FDM 管理 设备生成一个新的 IPS 策略，因此可能有多个具有此名称的策略。如果要使用默认 IP 策略，但要修改签名覆盖选项，请参阅 Firepower 入侵策略签名覆盖了解详细信息。Firepower 入侵策略签名覆盖, on page 346请注意，为每台设备配置不同的签名覆盖可能会导致默认覆盖策略变得不一致。

如何为每台设备设置不同的 IPS 策略？

CDO 为每个 FTD 设备生成一个新的 FDM 管理 策略，因此可能有多个具有此名称的策略。在自行激活每个设备后，您不必重命名 CDO 提供的 IPS 策略。展开策略会显示与其关联的设备，您还可以按设备或策略过滤威胁事件页面和签名覆盖页面。要自定义默认覆盖策略，请按设备配置签名覆盖。这将导致默认覆盖入侵策略变得不一致，但这不会抑制任何功能。

我已从 FDM 管理 设备载入拥有已配置的覆盖的设备。

在 CDO 外部配置的覆盖不会对设备配置或功能造成问题。

如果您载入已配置覆盖的设备，并且此新设备与没有覆盖的设备共享 IP 策略，则 IPS 策略将显示为不一致。请参阅 Firepower 入侵策略签名覆盖中的步骤 3，以解决不一致问题。Firepower 入侵策略签名覆盖, on page 346

SSL 解密问题故障排除

处理解密重签名适用于浏览器而非应用的 Web 站点（SSL 或证书颁发机构锁定）

智能手机和其他设备的某些应用使用 SSL（或证书颁发机构）锁定技术。SSL 锁定技术将原始服务器证书的散列值嵌入到应用本身内部。因此，当应用收到来自 FDM 管理设备的重签名证书时，散列验证会失败并中止连接。

主要表现是，用户使用站点应用无法连接到网站，但可以使用网络浏览器连接，即使在应用无法正常工作的同一台设备上使用浏览器也可以连接。例如，用户不能使用 Facebook iOS 或 Android 应用，但可以通过 https://www.facebook.com/ 转至 Safari 或 Chrome，进行成功连接。

由于 SSL 锁定专用于避免中间人攻击，因此此问题无法解决。必须从以下选项中选择一项：

- 支持应用用户，在这种情况下无法解密流向网站的任何流量。为站点应用创建“不解密”规则（在 SSL 解密规则的“应用”选项卡上），并确保该规则排在应用于连接的任何解密重签名规则前面
- 强制用户只使用浏览器。如果必须解密流向网站的流量，需要向用户说明，通过您的网络连接时，他们无法使用站点应用，只能使用浏览器。

更多详细信息

如果站点在浏览器中可用，但不能在同一设备的应用中使用，几乎可以肯定这是一个 SSL 锁定实例。但是，如果您想要更深入地挖掘，除了浏览器测试之外，还可以使用连接事件确定 SSL 锁定。

应用可能会通过两种方式处理散列验证失败：

- 第 1 组应用，例如 Facebook，从服务器收到 SH、CERT、SHD 消息后立即发送 SSL 警告消息。警告通常是一个表示 SSL 锁定的“Unknown CA (48)” 警告。紧接着警告消息发送 TCP 重置。在事件详细信息中，您应看到以下现象：
  - SSL 流标志包括 ALERT_SEEN。
  - SSL 流标志不包括 APP_DATA_C2S 或 APP_DATA_S2C。
  - SSL 流消息通常是：CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE。
- 第 2 组应用，例如 Dropbox，不会发送任何警告。而是，等到完成握手后发送 TCP 重置。在事件中，您应看到以下现象：
  - SSL 流标志不包括 ALERT_SEEN、APP_DATA_C2S 或 APP_DATA_S2C。
  - SSL 流消息通常是：CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED、SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED。

CA 证书的下载按钮已禁用

对于在CDO上暂存但尚未部署回设备的证书（自签名和上传），下载按钮处于禁用状态。只有在将证书部署到设备后，才能下载证书。

对使用序列号载入 FDM 管理 设备进行故障排除

- 调配错误
  - 设备密码尚未更改
  - 设备密码已更改
- 申领错误
  - 无效的序列号无效
  - 设备序列号已被申领
  - 设备离线
  - 未能申领设备

申领错误

无效的序列号无效

在 思科防御协调器 中申领设备时输入了错误的序列号。

解决方法

1. 删除 CDO 中的 FDM 管理 设备实例。
2. 通过输入正确的序列号创建新的 FDM 管理 设备实例并申领设备。

设备序列号已被申领

在使用设备的序列号载入 FDM 管理 设备时发生以下错误。

原因

发生此错误的原因之一可能如下：

- 设备可能是从外部供应商处购买的，并且设备在供应商的租户中。
- 该设备之前可能已由其他区域中的另一个 CDO 实例管理，并已注册到其云租户。

解决方法

您需要从其他云租户中注销设备的序列号，然后在您租户中将其收回。

前提条件

设备必须连接到可以访问云租户的互联网。

从外部供应商处购买的设备

从外部供应商处购买的设备可能已注册到供应商的云租户。

1. 从 CDO 中删除设备实例。
2. 在设备上安装 FXOS 映像。有关详细信息，请参阅《适用于具备 FTD 的 Firepower 1000/21000 的思科 FXOS 故障排除指南》的“重新映像程序”一章。
3. 从控制台端口连接到 FXOS CLI。
4. 使用您当前的管理员密码登录 FXOS。
5. 在 FXOS CLI 中，连接到 local-mgmt: firepower # **connect local-mgmt**。
6. 执行命令以从云租户中取消注册设备：firepower(local-mgmt) # **cloud deregister**。

7. 成功取消注册后，CLI 界面会返回成功消息。

   示例：firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9

   如果设备已从云租户中注销，则CLI界面会指明设备序列号未向云租户注册。 **RESULT=success MESSAGE=DEVICE_NOT_FOUND: Device with serial number JAD213082x9 is not registered with** 安全服务交换 **, X-Flow-Id: 63e48b4c-8426-48fb-9bd0-25fcd7777b99**

8. 通过提供设备序列号在 CDO 中重新申领设备。有关详细信息，请参阅 使用设备的序列号载入 FDM 管理 设备 。

9. 在设备上安装 FDM 管理 设备应用（版本 6.7 或更高版本）。低接触调配会在设备上启动，并在思科云中注册。CDO 会载入设备。

载入其他区域中已由其他云租户管理的 FDM 管理 设备

该设备之前可能已由其他区域中的另一个 CDO 实例管理，并已注册到其云租户。

情况 1：您可以访问拥有设备的租户。

1. 从区域 1 中的 CDO 删除设备实例。
2. 在 防火墙设备管理器 中，转到**系统设置 (System Settings)** > **云服务 (Cloud Services)** 页面。系统将显示一条警告消息，指明设备已从 CDO 中删除。
3. 点击 链接并从下拉列表中选择**注销云服务 (Unregister Cloud Services)**。
4. 阅读警告并点击**注销**。
5. 从区域 2 中的 CDO 申领设备。
6. 在 防火墙设备管理器 中，转至**系统设置 (System Settings)** > **云服务 (Cloud Services)** ，然后选择**通过思科防御协调器自动注册租用 (Auto-enroll with Tenancy from Cisco Defense Orchestrator)** 选项并点击**注册 (Register)**。设备会映射到属于新区域的新租户，而 CDO 会载入设备。

情况 2：您无法访问拥有设备的租户。

1. 从控制台端口连接到 FXOS CLI。
2. 使用您当前的管理员密码登录 FXOS。
3. 在 FXOS CLI 中，连接到 local-mgmt: firepower # **connect local-mgmt**。
4. 执行命令以从云租户中取消注册设备：firepower(local-mgmt) # **cloud deregister**。
5. 成功取消注册后，CLI 界面会返回成功消息。

   示例：firepower(local-mgmt) # cloud deregister Release Image Detected RESULT=success MESSAGE=SUCCESS 10, X-Flow-Id: 2b3c9e8b-76c3-4764-91e4-cfd9828e73f9

   设备会从云注销。

6. 从区域 2 中的 CDO 申领设备。

7. 在 防火墙设备管理器 中，转至**系统设置 (System Settings)** > **云服务 (Cloud Services)**，然后选择**通过思科防御协调器自动注册租用 (Auto-enroll with Tenancy from Cisco Defense Orchestrator)** 选项并点击**注册 (Register)**。设备会映射到属于新区域的新租户，而 CDO 会载入设备。

设备离线

原因

设备由于以下原因之一而无法访问思科云：

- 设备布线不正确。
- 您的网络可能要求提供设备的静态 IP 地址。
- 您的网络使用自定义 DNS，或者客户网络上存在外部 DNS 屏蔽。
- 需要进行 PPPoE 身份验证。（常见于欧洲地区。）
- FDM 管理 设备位于代理后面。

解决方法

1. 登录到设备并完成引导程序 CLI 过程或 CDO 轻松设置过程，以便首先配置设备，这样它才能访问互联网。
2. 检查布线和网络连接。
3. 确保您的防火墙未阻止任何流量。
4. 确保 安全服务交换 域可访问。有关详细信息，请参阅通过低接触调配载入FDM 管理设备。

未能申领设备

原因

可能会由于以下原因之一而发生此错误：

- 安全服务交换 可能存在临时问题。
- 服务器可能已关闭。

解决方法

1. 删除 CDO 中的 FDM 管理 设备实例。
2. 创建新的 FDM 管理 设备实例，并在一段时间后再次申领设备。

注释 如果您无法申领设备，请转至工作流程查看错误消息，并将详细信息发送给 CDO 支持团队。

调配错误

设备密码尚未更改

从 思科防御协调器 申领设备时，设备的初始调配可能会失败，并在 **清单 (Inventory)** 页面中显示“未调配”(Unprovisioned) 消息。

原因

您可能在 CDO FDM 管理 设备序列号载入向导中为默认密码未更改的新 FDM 管理 设备选择了“默认密码已更改”(Default Password Changed) 选项。

解决方法

您需要点击**清单 (Inventory)** 页面中的**输入密码 (Enter Password)**才能更改设备的密码。CDO 会继续输入新密码并启动设备。

设备密码已被更改

从 CDO 申领设备时，设备的初始调配可能会失败，并在 **清单 (Inventory)** 页面中显示“未调配”(Unprovisioned) 消息。

原因

您可能在 CDO FDM 管理 设备序列号载入向导中为默认密码已被更改的 FDM 管理 设备选择了“默认密码未更改”(Default Password Not Changed) 选项。

解决方法

您需要在**清单 (Inventory)** 页面中点击**确认并继续 (Confirm and Proceed)**，以忽略串行载入向导中提供的新密码。CDO 会继续输入新密码并启动设备。

对于其他错误

对于所有其他调配错误，您可以点击**重试 (Retry)** 以重新启动调配。如果多次重试后仍失败，请执行以下步骤：

1. 从 CDO 中删除 FDM 管理 设备实例并创建新实例。有关载入步骤，请参阅使用设备的序列号载入 FDM 管理 设备。
2. 在 防火墙设备管理器 中，转至**系统设置 (System Settings)** > **云服务 (Cloud Services)**，然后选择**通过思科防御协调器自动注册租用 (Auto-enroll with Tenancy from Cisco Defense Orchestrator)** 选项并点击**注册 (Register)**。

对 HA 创建进行故障排除FDM 管理

事件 说明 错误

如果您尝试在 思科防御协调器 中载入或创建 FDM 管理 HA 对，可能无法形成 HA 对，并且您可能会看到一条错误消息，并显示以下消息：

事件描述：CD 应用同步错误是在主用设备上启用了思科威胁响应，但在备用设备上未启用

如果您看到此错误，则表明 HA 对中的一个或两个设备未配置为允许设备将事件发送到思科云服务器（例如 CDO、Firepower Threat Response 或思科成功网络）。

您**必须**从 防火墙设备管理器 UI 启用**将事件发送到思科云 (Send Events to the Cisco Cloud)** 功能。有关详细信息，请参阅所运行版本的《Firepower 设备管理器配置指南》的**配置云服务**一章。

创建高可用性后，我的一台设备处于不良状态

如果其中一个设备在 HA 创建期间处于运行状况不佳或发生故障的状态，请中断 HA 对并解析设备的状态，然后重新创建 HA。故障切换历史记录可能有助于诊断问题。FDM 管理 高可用性故障转移历史记录, on page 519

对安全设备连接器进行故障排除

使用这些主题对现场安全设备连接器 (SDC) 进行故障排除。

如果这些场景都不符合您的情况，CDO 客户如何通过 TAC 提交支持请求。

SDC 无法接通

如果 SDC 未能连续响应来自 CDO 的两个心跳请求，则该 SDC 处于“无法访问”状态。如果您的 SDC 无法访问，您的租户将无法与您已自行激活的任何设备通信。

CDO 表示无法通过以下方式访问 SDC：

- 您会看到消息“某些安全设备连接器 (SDC) 无法访问。您将无法与与这些 SDC 关联的设备进行通信。”在 CDO 主页上。
- “安全连接器”(Secure Connectors) 页面中的 SDC 状态为“无法访问”(Unreachable)。

首先，尝试将 SDC 重新连接到租户以解决此问题：

1. 检查 SDC 虚拟机是否正在运行，并且可以访问您所在地区的 CDO IP 地址。请参阅将 思科防御协调器 连接到托管设备，第 11 页。
2. 尝试通过手动请求心跳来重新连接 CDO 和 SDC。如果 SDC 响应心跳请求，它将返回“活动”状态。要手动请求心跳，请执行以下操作：
   1. 从 CDO 菜单中选择 **管理** > **安全连接器**。
   2. 点击无法访问的 SDC。
   3. 在“操作”(Actions) 窗格中，点击**请求检测信号 (Request Heartbeat)**。
   4. 点击**重新连接 (Reconnect)**。
3. 如果在手动尝试将 SDC 重新连接到租户后，SDC 未返回到主用状态，请按照中的说明进行操作。部署后，SDC 状态在 CDO 上未变为活动状态，第 700 页

。

部署后，SDC 状态在 CDO 上未变为活动状态

如果 CDO 在部署后约 10 分钟内未指示您的 SDC 处于活动状态，请使用您在部署 SDC 时创建的 cdo 用户和密码，通过 SSH 连接到 SDC VM。

Procedure

步骤 1 查看 /opt/cdo/configure.log。它会显示您为 SDC 输入的配置设置，以及这些设置是否已成功应用。如果设置过程中出现任何故障，或者值输入不正确，请再次运行 sdc-onboard 设置：

a) 在 [cdo@localhost cdo]$ 提示符后，输入 sudo sdc-onboard setup。
b) 输入 `cdo` 用户的密码。
c) 按照提示操作。设置脚本将指导您完成在设置向导中执行的所有配置步骤，并为您提供更改输入的值的机会。

步骤 2 如果在查看日志并运行 sudo sdc-onboard setup 后，CDO 仍不指示 SDC 处于活动状态，请联系 CDO 支持。联系思科威胁防御支持, on page 752

更改后的 SDC IP 地址未反映在 CDO 中

如果您更改了 SDC 的 IP 地址，则在格林威治标准时间上午 3:00 之前，它不会反映在 CDO 中。

排除设备与 SDC 的连接故障

使用此工具可测试从CDO通过安全设备连接器(SDC)到您的设备的连接。如果您的设备未能载入，或者您想在载入之前确定 CDO 是否可以访问您的设备，则可能需要测试此连接。

Procedure

步骤 1 从 CDO 菜单中选择**管理 (Admin)** > **安全连接器 (Secure Connectors)**。

步骤 2 选择 SDC。

步骤 3 在右侧的**故障排除 (Troubleshooting)** 窗格中，点击**设备连接 (Device Connectivity)**。

步骤 4 输入您尝试进行故障排除或尝试连接的设备的有效IP地址或FQDN和端口号，然后点击**开始 (Go)**。CDO 执行以下验证：

a) **DNS 解析 (DNS Resolution)** - 如果您提供 FQDN 而不是 IP 地址，这将验证 SDC 可以解析域名并获取 IP 地址。
b) **连接测试 (Connection Test)** - 验证设备是否可访问。
c) **TLS 支持 (TLS Support)** - 检测设备和 SDC 支持的 TLS 版本和密码。

- **不支持的密码 (Unsupported Cipher)** - 如果没有设备和 SDC 都支持的 TLS 版本，则 CDO 还会测试设备（而不是 SDC）支持的 TLS 版本和密码。

d) “SSL 证书”(SSL Certificate) - 故障排除提供证书信息。

步骤 5 如果在载入或连接设备方面仍有问题，请联系思科威胁防御支持。

与 SDC 间歇性连接或无连接

本节中讨论的解决方案仅适用于本地安全设备连接器 (SDC)。

症状：与 SDC 的连接断断续续或无连接。

诊断：如果磁盘空间几乎已满（80% 以上），可能会出现此问题。

执行以下步骤以检查磁盘空间使用情况。

1. 打开 Secure Device Connector (SDC) VM 的控制台。
2. 使用用户名 **cdo** 登录。
3. 输入初始登录时创建的密码。
4. 首先，通过键入 df -h 确认没有可用磁盘空间，以检查可用磁盘空间量。

   您可以确认磁盘空间已被 Docker 占用。正常磁盘使用量应低于 2 GB。
5. 要查看 Docker 文件夹的磁盘使用情况，

   执行 sudo du -h /var/lib/docker | sort -h.

   您可以看到 Docker 文件夹的磁盘空间使用情况。

操作步骤

如果 Docker 文件夹的磁盘空间使用量快要满了，请在 Docker 配置文件中定义以下内容：

- 最大大小：在当前文件达到最大大小后强制执行日志轮换。
- 最大文件：在达到最大限制时删除多余的轮换日志文件。

请执行以下操作：

1. 执行 sudo vi /etc/docker/daemon.json。
2. 将以下行插入文件。

```
{
"log-driver": "json-file",
"log-opts": {"max-size": "100m", "max-file": "5" }
}
```

3. 按 ESC，然后键入 :wq!写入更改并关闭文件。

注释 您可以执行 sudo cat /etc/docker/daemon.json 来验证对文件所做的更改。

4. 执行 sudo systemctl restart docker 以重新启动 docker 文件。

   更改需要几分钟才能生效。您可以执行 sudo du -h /var/lib/docker | sort -h 以查看 docker 文件夹的更新磁盘使用情况。

5. 执行 df -h 以验证可用磁盘大小是否已增加。

6. 在 SDC 状态从“无法连通”(Unreachable) 变成“活动”(Active) 之前，您必须从 CDO 转到“安全连接器”(Secure Connectors) 页面，然后从“操作”(Actions) 菜单中点击**请求重新连接 (Request Reconnect)**。

影响安全设备连接器的容器权限升级漏洞：cisco-sa-20190215-runc

思科产品安全事件响应团队 (PSIRT) 发布了安全公告 **cisco-sa-20190215-runc**，其中描述了 Docker 中的一个高严重性漏洞。阅读整个 PSIRT 团队公告，了解漏洞的完整说明。

此漏洞会影响所有 CDO 客户：

- 使用 CDO 云部署的安全设备连接器 (SDC) 的客户无需执行任何操作，因为 CDO 运营团队已执行补救步骤。
- 使用本地部署的 SDC 的客户需要升级其 SDC 主机才能使用最新的 Docker 版本。他们可以按照以下说明执行此操作：
  - 更新 CDO 标准 SDC 主机，第 702 页
  - 更新自定义 SDC 主机，第 703 页
  - 缺陷跟踪，第 703 页

更新 CDO 标准 SDC 主机

如果您使用 CDO 映像部署了 SDC，请使用以下说明。使用 CDO 的 VM 映像部署安全设备连接器，第 13 页

过程

步骤 1 使用 SSH 或虚拟机监控程序控制台连接到 SDC 主机。

步骤 2 运行以下命令检查 Docker 服务的版本：

```
docker version
```

步骤 3 如果您运行的是最新的虚拟机 (VM)，您应该会看到如下输出：

```
 > docker version
Client:
     Version: 18.06.1-ce
     API version: 1.38
     Go version: go1.10.3
     Git commit: e68fc7a
     Built: Tue Aug 21 17:23:03 2018
     OS/Arch: linux/amd64
     Experimental: false
```

您可能会在这里看到旧版本。

步骤 4 运行以下命令以更新 Docker 并重新启动服务：

```
> sudo yum update docker-ce
> sudo service docker restart
```

注释 当 Docker 服务重新启动时，CDO 和您的设备之间会出现短暂的连接中断。

步骤 5 再次运行 docker version 命令。您应该会看到以下输出：

```
> docker version
Client:
    Version: 18.09.2
    API version: 1.39
    Go version: go1.10.6
    Git commit: 6247962
    Built: Sun Feb XX 04:13:27 2019
    OS/Arch: linux/amd64
    Experimental: false
```

步骤 6 大功告成。您现在已升级到 Docker 的最新版本并安装了补丁。

更新自定义 SDC 主机

如果您已创建自己的 SDC 主机，则需要按照说明根据 Docker 的安装方式进行更新。如果您使用的是 CentOS、yum 和 Docker-ce（社区版），则前面的程序将起作用。

如果您已安装 Docker-ee（企业版）或使用其他方法安装 Docker，则 Docker 的固定版本可能不同。您可以查看 Docker 页面以确定要安装的正确版本：Docker 安全更新和容器安全最佳实践。
https://blog.docker.com/2019/02/docker-security-update-cve-2018-5736-and-container-security-best-practices/

缺陷跟踪

思科将继续评估此漏洞，并将在获得更多信息时更新公告。公告被标记为最终版本后，您可以参考相关的思科漏洞了解更多详细信息：

CSCvo33929-CVE-2019-5736: runc container breakout

安全事件连接器故障排除

如果这些场景都不符合您的情况，CDO 客户如何通过 TAC 提交支持请求。

安全事件连接器载入故障排除

这些故障排除主题介绍了与安全事件连接器 (SEC) 载入失败相关的许多不同症状。

SEC 自行激活失败

症状：SEC 自行激活失败。

修复：删除 SEC 并重新载入。

如果收到此错误：

1. 从虚拟机容器中删除安全事件连接器及其文件。
2. 更新您的安全设备连接器，第 27 页。通常，SDC 会自动更新，您不必使用此程序，但此程序在故障排除的情况下非常有用。
3. 在 SDC 虚拟机上安装安全事件连接器，第 600 页。

提示 激活 SEC 时，请始终使用复制链接复制引导程序数据。

注释 如果此程序无法解决问题，请事件日志记录故障排除日志文件并联系您的托管服务提供商或思科技术支持中心。

未提供 SEC Bootstrap 数据

消息：错误，无法引导程序安全事件连接器，不提供引导程序数据，正在退出。(ERROR cannot bootstrap Secure Event Connector, bootstrap data not provided, exiting.)

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector, bootstrap data not
provided, exiting.
```

诊断：系统提示时，Boostrap 数据未输入到设置脚本中。

修复：在载入时，如果提示输入引导程序数据，提供在 CDO UI 中生成的 SEC 引导程序数据。

引导程序配置文件不存在

消息：错误，无法为租户引导安全事件连接器：<tenant_name>，引导程序配置文件（“/usr/local/cdo/es_bootstrapdata”）不存在，正在退出。(ERROR Cannot bootstrap Secure Event Connector for tenant: <tenant_name>, bootstrap config file ("/usr/local/cdo/es_bootstrapdata") does not exist, exiting.)

诊断：SEC 引导程序数据文件（“/usr/local/cdo/es_bootstrapdata”）不存在。

修复：将 CDO UI 中生成的 SEC 引导程序数据放到文件 **/usr/local/cdo/es_bootstrapdata** 中，然后再次尝试载入。

1. 重复载入程序。
2. 复制引导程序日期。
3. 以“sdc”用户身份登录 SEC VM。
4. 将 CDO UI 中生成的 SEC 引导程序数据放到文件 **/usr/local/cdo/es_bootstrapdata** 中，然后再次尝试载入。

解码引导程序数据失败

消息：错误无法为租户引导安全事件连接器：<tenant_name>，未能解码 SEC Boostrap 数据，正在退出。(ERROR cannot bootstrap Secure Event Connector for tenant: <tenant_name>, faile to decode SEC boostrap data, exiting.)

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
base64: invalid input
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: tenant_XYZ,
 failed to decode SEC bootstrap data, exiting.
```

诊断：解码引导程序数据失败

修复：重新生成 SEC 引导程序数据，然后再次尝试载入。

引导程序数据没有载入 SEC 所需的信息

消息：

- 错误，无法为租户引导安全事件连接器容器，安全服务交换 FQDN 未设置，正在退出。
- 错误，无法为租户引导安全事件连接器容器，安全服务交换 OTP 未设置，正在退出。

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: 安全服务交换
 FQDN not set, exiting.
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: 安全服务交换
 FQDN not set, exiting.
```

诊断：引导程序数据没有载入 SEC 所需的信息

修复：重新生成 bootstrapdata，然后再次尝试载入。

当前正在运行的工具包 Cron

消息：错误，SEC 工具包已在运行，正在退出。(ERROR SEC toolkit already running, exiting.)

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
 [2020-06-10 04:37:26] ERROR SEC toolkit already running.
```

诊断： 工具包 cron 当前正在运行。

修复：再次重试载入命令。

没有足够的 CPU 和内存

消息：错误，无法设置安全事件连接器，需要至少 4 个 CPU 和 8 GB 内存，正在退出。(ERROR unable to setup Secure Event Connector, minimum 4 cpus and 8 GB ram required, exiting.)

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, minimum 4 cpus and 8
GB ram required, exiting.
```

诊断：没有足够的 CPU 和内存。

修复：确保至少为虚拟机上的 SEC 调配了 4 个 CPU 和 8 GB RAM，然后再次尝试载入。

SEC 已在运行

消息：错误安全事件连接器已在运行，在载入新的安全事件连接器并退出之前执行“cleanup”。

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR Secure Event Connector already running, execute 'cleanup' before
 onboarding a new Secure Event Connector, exiting.
```

诊断：SEC 已在运行。

修复：在载入新的 SEC 之前运行 SEC 清理命令。

SEC 域无法访问

消息：

- 未能连接到 api-sse.cisco.com:443；连接被拒绝 (Failed connect to api-sse.cisco.com:443; Connection refused)
- 错误，无法设置安全事件连接器，无法访问域 api-sse.cisco.com，正在退出。(ERROR unable to setup Secure Event Connector, domain api-sse.cisco.com unreachable, exiting.)

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
curl: (7) Failed connect to api-sse.cisco.com:443; Connection refused
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, domain api-sse.cisco.com
 unreachable, exiting.
```

诊断：SEC 域不可达

修复：确保本地 SDC 具有互联网连接，然后再次尝试载入。

载入 SEC 命令成功且未出错，但 SEC docker 容器未启动

症状：载入 SEC 命令成功且未出错，但 SEC docker 容器未启动

诊断：载入 SEC 命令成功且未出错，但 SEC docker 容器未启动

修复：

1. 以“sdc”用户身份登录 SEC。
2. 检查 SEC docker 容器启动日志中是否存在任何错误 (/usr/local/cdo/data/<tenantDir>/event_streamer/logs/startup.log)。
3. 如果是，请运行 SEC 清理命令，然后再次尝试载入。

联系 CDO 支持人员

如果这些场景都不符合您的情况，CDO 客户如何通过 TAC 提交支持请求。

安全事件连接器注册失败故障排除

症状：向云事件服务注册思科安全事件连接器失败。

诊断：这些是 SEC 无法注册到事件云服务的最常见原因。

- **SEC 无法从 SEC 访问 Eventing 云服务**

  修复：确保可在端口 443 上访问互联网，并且 DNS 配置正确。

- **由于 SEC bootstrapdata 中的一次性密码无效或过期，注册失败**

  修复：

Procedure

步骤 1 以“sdc”用户身份登录 SDC。

步骤 2 查看连接器日志：(/usr/local/cdo/data/<tenantDir>/event_streamer/logs/connector.log) 以检查注册状态。

如果注册因令牌无效而失败，您将在日志文件中看到类似于以下内容的错误消息。

context:(*contextImpl).handleFailed] registration - CE2001：注册失败 - 因无效令牌，注册设备失败。请使用新的有效令牌重试。- 失败"

步骤 3 在 SDC VM 上运行 SEC 清理命令步骤，从“安全连接器”(Secure Connectors) 页面删除 SEC。

步骤 4 生成新的 SEC 引导程序数据，然后重试 SEC 激活步骤。

使用安全和分析日志记录事件排除网络问题

以下是使用事件查看器排除网络问题的基本框架。

此场景假设您的网络运营团队收到报告，指出用户无法访问网络上的资源。根据报告问题的用户及其位置，网络运营团队可以合理地了解哪个防火墙控制其对资源的访问。

Note 此场景还假设 FDM 管理 设备是管理网络流量的防火墙。安全分析和日志记录不会从其他设备类型收集日志记录信息。

Procedure

步骤 1 在导航窗格中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

步骤 2 点击**历史 (Historical)** 选项卡。

步骤 3 按**时间范围 (Time Range)** 开始过滤事件。默认情况下，“历史”(Historical) 选项卡显示最近一小时的事件。如果这是正确的时间范围，请输入当前日期和时间作为**结束**时间。如果该时间范围不正确，请输入包含所报告问题时间的开始和结束时间。

步骤 4 在**传感器 ID (Sensor ID)** 字段中输入您怀疑控制用户访问的防火墙的 IP 地址。如果可能是多个防火墙，请使用搜索栏中的 **attribute:value** 对过滤事件。输入两个条目并将其与 OR 语句组合在一起。例如：`SensorID:192.168.10.2 OR SensorID:192.168.20.2`。

步骤 5 在事件过滤器栏中的**源 IP (Source IP)** 字段中输入用户的 IP 地址。

步骤 6 如果用户无法访问资源，请尝试在**目标 IP (Destination IP)** 字段中输入该资源的 IP 地址。

步骤 7 展开结果中的事件并查看其详细信息。以下是一些需要查看的详细信息：

- **AC_RuleAction** - 触发规则时采取的操作（允许、信任、阻止）。
- **FirewallPolicy** - 触发事件的规则所在的策略。
- **FirewallRule** - 触发事件的关联规则的名称。如果值为“默认操作”(Default Action)，则触发事件的是策略的默认操作，而不是策略中的某个规则。
- **UserName** - 与发起方 IP 地址关联的用户。发起方 IP 地址与源 IP 地址相同。

步骤 8 如果规则操作阻止访问，请查看 FirewallRule 和 FirewallPolicy 字段，以确定策略中阻止访问的规则。

NSEL 数据流故障排除

后，请使用以下程序验证 NSEL 事件是否从ASA发送到思科云以及思科云是否正在接收这些事件。

请注意，一旦ASA配置为将 NSEL 事件发送到安全事件连接器 (SEC)，然后再发送到思科云，数据不会立即流动。假设ASA上生成了与 NSEL 相关的流量，第一个 NSEL 数据包可能需要几分钟才能到达。

Note 此工作流程向您展示如何直接使用“flow-export counters”命令和“capture”命令对 NSEL 数据流进行故障排除。有关这些命令用法的更详细讨论，请参阅《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》中的“数据包捕获”和《思科 ASA NetFlow 实施指南》中的“监控 NSEL”。

执行这些任务：

- 验证 NetFlow 数据包是否正在发送到 SEC
- 验证思科云是否正在接收 NetFlow 数据包

事件日志记录故障排除日志文件

安全事件连接器 (SEC) troubleshoot.sh 收集所有事件流传输器日志，并将其压缩到单个 .tar.gz 文件中。

使用以下程序创建 comparessed.tar.gz 文件并解压缩该文件：

1. 运行故障排除脚本，第 709 页。
2. 解压缩 sec_troubleshoot.tar.gz 文件，第 710 页。

运行故障排除脚本

安全事件连接器 (SEC) troubleshoot.sh 收集所有事件流传输器日志，并将其压缩到单个 .tar.gz 文件中。请按照以下程序运行 Troubleshooting.sh 脚本：

Procedure

步骤 1 打开 VM 虚拟机监控程序并启动安全设备连接器 (SDC) 的控制台会话。

步骤 2 登录并切换到 **root** 用户：

```
[cdo@localhost ~]$sudo su root
```

Note 您也可以切换到 sdc 用户，但作为根用户，您还将收到 IP 表信息。IP 表信息显示防火墙正在设备上运行，并且所有防火墙路由。如果防火墙阻止安全事件连接器 TCP 或 UDP 端口，事件将不会显示在事件日志记录表中。IP 表将帮助您确定是否属于这种情况。

步骤 3 在提示符后，运行故障排除脚本并指定租户名称。以下是命令语法：

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_[tenant_name]
```

以下为输出示例：

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_example_tenant
```

在命令输出中，您会看到 sec_troubleshoot 文件存储在 SDC 上的 **/tmp/troubleshoot** 目录中。文件名遵循约定 **sec_troubleshoot-*timestamp*.tar.gz.**

步骤 4 要检索文件，请以 CDO 用户身份登录并使用 SCP 或 SFTP 下载文件。

以下为输出示例：

```
[root@localhost troubleshoot]# scp sec_troubleshoot-timestamp.tar.gz
root@server-ip:/scp/sec_troubleshoot-timestamp.tar.gz
```

What to do next

请继续解压缩 sec_troubleshoot.tar.gz 文件, on page 710。

解压缩 sec_troubleshoot.tar.gz 文件

安全事件连接器 (SEC) 运行故障排除脚本 脚本收集所有事件流传输器日志，并将其压缩到一个 sec_troubleshoot.tar.gz 文件中。按照此程序解压缩 sec_troubleshoot.tar.gz 文件。

1. 打开 VM 虚拟机监控程序并启动安全设备连接器 (SDC) 的控制台会话。
2. 登录并切换到 **root** 用户：

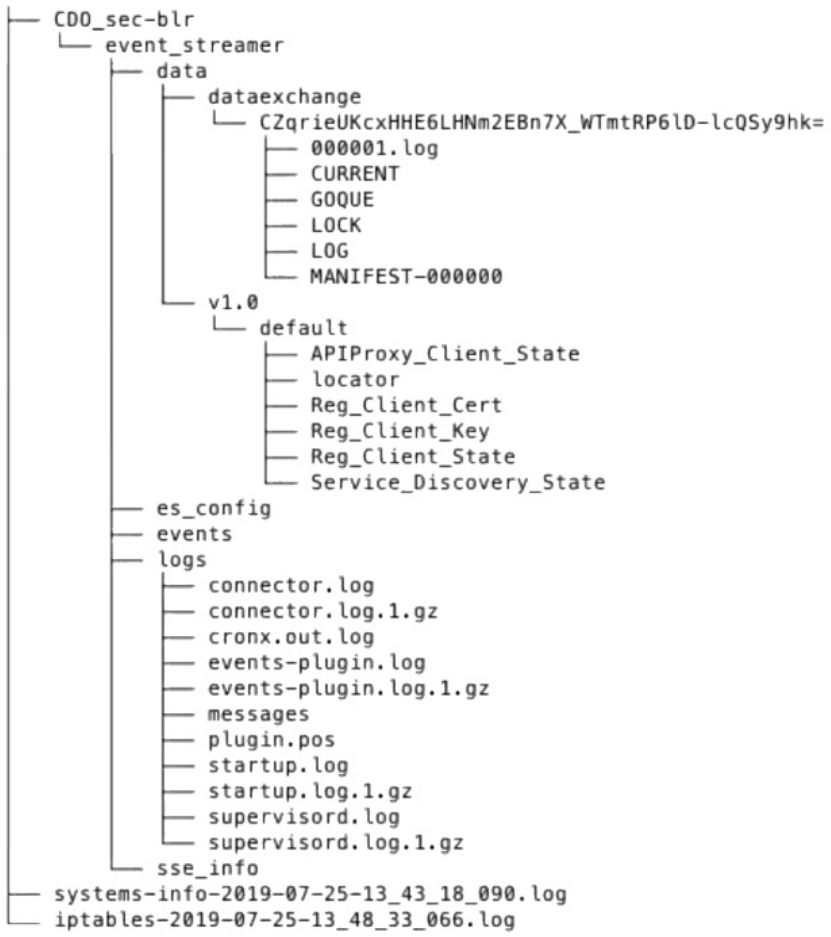
```
[cdo@localhost ~]$sudo su root
```

Note 您也可以切换到 **sdc** 用户，但作为根用户，您还将收到 IP 表信息。IP 表信息显示防火墙正在设备上运行，并且所有防火墙路由。如果防火墙阻止安全事件连接器 TCP 或 UDP 端口，事件将不会显示在事件日志记录表中。IP 表将帮助您确定是否属于这种情况。

3. 在提示符后，键入以下命令：

```
[root@localhost ~]$ tar xvf sec_troubleshoot-timestamp.tar.gz
```

日志文件存储在以租户命名的目录中。这些是存储在 sec_troubelshoot-timestamp.tar.gz 文件中的日志类型。如果您以 root 用户身份收集所有日志文件，则包括 iptables 文件。



生成 SEC 引导程序数据失败。

症状：在 CDO 中生成 SEC 引导程序数据时，“引导程序生成”步骤失败并显示错误：“获取引导程序数据时出错。请重试。"

修复：再次重试引导程序数据生成。如果仍然失败，请联系 CDO 支持。CDO 客户如何通过 TAC 提交支持请求, on page 753

自行激活后，CDO 安全连接器页面中的 SEC 状态为“非活动”

症状：由于以下原因之一，CDO 安全连接器页面中的安全事件连接器状态显示为“非活动”：

- 心跳失败
- 连接器注册失败

修复：

- 心跳失败：请求 SEC 心跳并刷新“安全连接器”页面，以查看状态是否更改为“活动”，如果未更改，请检查安全设备连接器注册是否失败。

- 连接器注册失败：请参阅问题“SEC注册失败故障排除”。安全事件连接器注册失败故障排除, on page 707

SEC 处于“在线”状态，但 CDO 事件日志记录页面中没有事件

症状：安全事件连接器在 CDO 安全连接器页面中显示“活动”，但在 CDO 事件查看器中看不到事件。

解决方案或解决方法：

Procedure

步骤 1 以“sdc”用户身份登录到本地 SDC 的虚拟机。在提示符后，键入 **sudo su - sdc**。

步骤 2 执行以下检查：

- 查看 SEC 连接器日志 (/usr/local/cdo/data/<tenantDir>/event_streamer/logs/connector.log) 并确保 SEC 注册已成功。如未成功，请参阅问题“安全事件连接器注册失败故障排除”。
- 检查 SEC 事件日志 (/usr/local/cdo/data/<tenantDir> /event_streamer/logs/events-plugin.log）并确保事件正在处理。否则，请CDO 客户如何通过 TAC 提交支持请求。
- 登录到 SEC docker 容器并执行命令“supervisorctl -c /opt/cssp/data/conf/supervisord.conf”，并确保输出如下所示，并且所有进程都处于 RUNNING 状态。否则，请CDO 客户如何通过 TAC 提交支持请求。

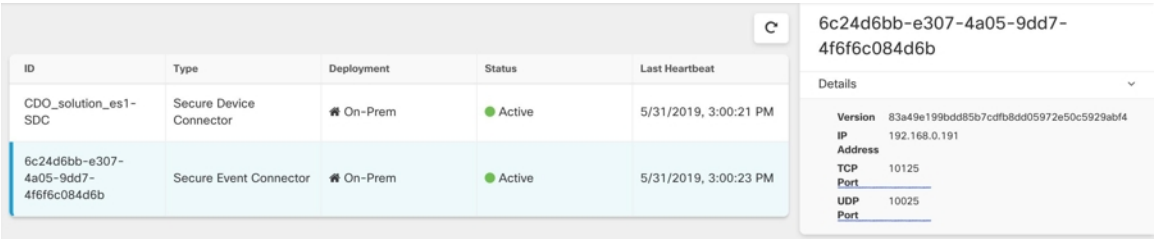
estreamer-connector RUNNING pid 36, uptime 5:25:17

estreamer-cron RUNNING pid 39, uptime 5:25:17

estreamer-plugin RUNNING pid 37, uptime 5:25:17

estreamer-rsyslog RUNNING pid 38, uptime 5:25:17

- 确保本地 SDC 上的防火墙规则未阻止“安全连接器”(Secure Connectors) 页面上为 SEC 显示的 UDP 和 TCP 端口。要确定需要打开的端口，请参阅查找用于安全日志记录分析 (SaaS) 的设备 TCP、UDP 和 NSEL 端口。



- 如果您使用自己的CentOS 7 虚拟机手动设置了 SDC，并将防火墙配置为阻止传入请求，则可以执行以下命令来取消阻止 UDP 和 TCP 端口：

firewall-cmd --zone=public --add-port=<udp_port> /udp --permanent

firewall-cmd --zone=public --add-port=<tcp_port> /tcp --permanent

firewall-cmd --reload

- 使用您选择的 Linux 网络工具，检查是否在这些端口上接收数据包。如果未收到，请重新检查 FTD 日志记录配置。

如果上述修复方法均无效，请向 CDO 支持人员提交支持请求。 CDO 客户如何通过 TAC 提交支持请求, on page 753。

SEC 清理命令

安全事件连接器 (SEC) 清理命令可从安全设备连接器 (SDC) 虚拟机中删除 SEC 容器及其关联的文件。您可以在 安全事件连接器注册失败故障排除, on page 707 或载入失败的情况下运行此命令。

运行命令：

Before you begin

要执行此任务，您需要知道租户的名称。要查找租户名称，请在CDO中打开用户菜单，然后点击**设置 (Settings)**。向下滚动页面以找到您的**租户名称 (Tenant Name)**。

Procedure

步骤 1 以 `sdc` 用户身份登录 SDC。在提示符后，键入 `sudo su - sdc`。

步骤 2 连接到 `/usr/local/cdo/toolkit` 目录。

步骤 3 运行 `sec.sh remove`*`tenant_name`* 并确认您打算删除 SEC。

示例：

```
 [sdc@localhost~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ
Are you sure you want to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y
```

What to do next

如果此命令无法删除 SEC，请继续执行 SEC 清理命令失败, on page 713：

SEC 清理命令失败

如果 SEC 清理命令, on page 713 失败，请使用此程序。

消息：找不到 SEC，正在退出。

症状：清理 SEC 命令无法清理现有 SEC。

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ Are you sure you want
to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y [2020-06-10 04:50:42] SEC
 not found, exiting.
```

修复： 当清理命令失败时，手动清理安全事件连接器。

删除已在运行的 SEC docker 容器：

Procedure

步骤 1 以“sdc”用户身份登录 SDC。在提示符后，键入 `sudo su - sdc`。

步骤 2 运行 **docker ps** 命令以查找 SEC 容器的名称。SEC 名称的格式为“es_ *name*”。

步骤 3 运行 **docker stop** 命令以停止 SEC 容器。

步骤 4 运行 **rm** 命令以删除 SEC 容器。

例如：

```
$ docker stop <SEC_docker_container_name>
$ docker rm <SEC_docker_container_name>
```

使用运行状况检查了解安全事件连接器的状态

安全事件连接器 (SEC) 运行状况检查脚本提供有关 SEC 状态的信息。

请按照以下程序运行运行状况检查：

Procedure

步骤 1 打开 VM 监控程序并启动安全设备连接器 (SDC) 的控制台会话。

步骤 2 以“cdo”用户身份登录 SDC。

步骤 3 切换到“sdc”用户：

```
[cdo@tenant]$sudo su sdc
```

步骤 4 在提示符后，运行 healthcheck.sh 脚本并指定租户名称：

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_[tenant_name]
```

例如：

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_example_tenant
```

脚本的输出提供以下信息：

```
================================================
Running SEC health check for tenant [redacted]
------------------------------------------------
SEC cloud URL [redacted] is: Reachable
------------------------------------------------
SEC Connector status: Active
------------------------------------------------
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
------------------------------------------------
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the event in CDO events viewer page.
================================================
```

运行状况检查输出的值：

- **SEC 云 URL**：显示 CDO 云 URL 以及 SEC 是否可以访问 CDO。
- **SEC 连接器**：如果 SEC 连接器已正确载入并启动，则会显示“正在运行”(Running)。
- **SEC UDP 系统日志服务器**：如果 UDP 系统日志服务器已准备好发送 UDP 事件，则显示“正在运行”。
- **SEC TCP 系统日志服务器**：如果 TCP 系统日志服务器已准备好发送 TCP 事件，将显示“正在运行”。
- **SEC 连接器状态**：如果 SEC 正在运行并已载入到 CDO，则会显示为“活动”(Active)。
- **SEC 发送示例事件**：如果在运行状况检查结束时，所有状态检查均为“绿色”，则该工具会发送示例事件。（如果有任何进程“关闭”，则工具会跳过发送测试事件。）示例事件在事件日志中显示为名为 “sec-health-check” 的策略。

对思科防御协调器进行故障排除

登录失败故障排除

登录失败，因为您无意中登录到错误的 CDO 区域

请确保您登录的是适当的 CDO 区域。登录 https://sign-on.security.cisco.com 后，您可以选择要访问的区域。点击 **CDO** 磁贴访问 Defenseorchestrator.com 或点击 **CDO (EU)** 访问 Defenseorchestrator.eu。

迁移后的登录失败故障排除

由于用户名或密码不正确，CDO 登录失败

解决方法 如果您尝试登录 CDO，并且知道您使用的是正确的用户名和密码，但登录失败，或者您尝试“忘记密码”无法恢复有效的密码，则您可能已尝试在未创建新 Cisco Security Cloud Sign On 帐户的情况下进行登录，则您需要按照创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证，第 66 页中的说明注册新的 Cisco Security Cloud Sign On 帐户。

登录到 Cisco Security Cloud Sign On 控制面板成功，但您无法启动 CDO

解决方法 您可能使用与 CDO 租户不同的用户名创建了 Cisco Security Cloud Sign On 账户。请联系思科技术支持中心 (TAC)，以规范 CDO 和 Cisco Secure Sign-On 之间的用户信息。

使用保存的书签登录失败

解决方法 您可能正在尝试使用浏览器中保存的旧书签登录。书签可能指向 https://cdo.onelogin.com。https://cdo.onelogin.com/

解决方法 登录 https://sign-on.security.cisco.com。

- **解决方法** 如果您尚未创建 Cisco Secure Sign-On 账户，请创建一个账户。创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证，第 66 页
- **解决方法** 如果您已创建新账户，请点击控制面板上与 思科防御协调器（美国）、思科防御协调器（欧盟）或 思科防御协调器（亚太地区）对应的 CDO 磁贴
- **解决方法** 将书签更新为指向 https://sign-on.security.cisco.com。https://sign-on.security.cisco.com/

访问和证书故障排除

解析检测到的新指纹状态

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择处于检测到**新指纹状态**的设备。

步骤 5 点击检测到的新指纹窗格中的**查看指纹**。

步骤 6 当系统提示您查看并接受指纹时：

a. 点击**下载指纹**并进行查看。

b. 如果您对指纹满意，请点击**接受**。如果不是，请点击**取消**。

步骤 7 解决新的指纹问题后，设备的连接状态可能会显示为**在线**，而配置状态可能会显示“未同步”或“检测到冲突”。回顾解决配置冲突 以查看和解决 CDO 与设备之间的配置差异。

使用安全和分析日志记录事件排除网络问题

以下是使用事件查看器排除网络问题的基本框架。

此场景假设您的网络运营团队收到报告，指出用户无法访问网络上的资源。根据报告问题的用户及其位置，网络运营团队可以合理地了解哪个防火墙控制其对资源的访问。

Note 此场景还假设 FDM 管理 设备是管理网络流量的防火墙。安全分析和日志记录不会从其他设备类型收集日志记录信息。

Procedure

步骤 1 在导航窗格中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

步骤 2 点击**历史 (Historical)** 选项卡。

步骤 3 按**时间范围 (Time Range)** 开始过滤事件。默认情况下，“历史”(Historical) 选项卡显示最近一小时的事件。如果这是正确的时间范围，请输入当前日期和时间作为**结束**时间。如果该时间范围不正确，请输入包含所报告问题时间的开始和结束时间。

步骤 4 在**传感器 ID (Sensor ID)** 字段中输入您怀疑控制用户访问的防火墙的 IP 地址。如果可能是多个防火墙，请使用搜索栏中的 **attribute:value** 对过滤事件。输入两个条目并将其与 OR 语句组合在一起。例如：`SensorID:192.168.10.2 OR SensorID:192.168.20.2`。

步骤 5 在事件过滤器栏中的**源 IP (Source IP)** 字段中输入用户的 IP 地址。

步骤 6 如果用户无法访问资源，请尝试在**目标 IP (Destination IP)** 字段中输入该资源的 IP 地址。

步骤 7 展开结果中的事件并查看其详细信息。以下是一些需要查看的详细信息：

- **AC_RuleAction** - 触发规则时采取的操作（允许、信任、阻止）。
- **FirewallPolicy** - 触发事件的规则所在的策略。
- **FirewallRule** - 触发事件的关联规则的名称。如果值为“默认操作”(Default Action)，则触发事件的是策略的默认操作，而不是策略中的某个规则。
- **UserName** - 与发起方 IP 地址关联的用户。发起方 IP 地址与源 IP 地址相同。

步骤 8 如果规则操作阻止访问，请查看 FirewallRule 和 FirewallPolicy 字段，以确定策略中阻止访问的规则。

SSL 解密问题故障排除

处理解密重签名适用于浏览器而非应用的 Web 站点（SSL 或证书颁发机构锁定）

智能手机和其他设备的某些应用使用 SSL（或证书颁发机构）锁定技术。SSL 锁定技术将原始服务器证书的散列值嵌入到应用本身内部。因此，当应用收到来自 Firepower Threat Defense设备的重签证书时，散列验证会失败并中止连接。

主要表现是，用户使用站点应用无法连接到网站，但可以使用网络浏览器连接，即使在应用无法正常工作的同一台设备上使用浏览器也可以连接。例如，用户不能使用 Facebook iOS 或 Android 应用，但可以通过 https://www.facebook.com 转至 Safari 或 Chrome，进行成功连接。

由于 SSL 锁定专用于避免中间人攻击，因此此问题无法解决。必须从以下选项中选择一项：

更多详细信息

如果站点在浏览器中可用，但不能在同一设备的应用中使用，几乎可以肯定这是一个 SSL 锁定实例。但是，如果您想要更深入地挖掘，除了浏览器测试之外，还可以使用连接事件确定 SSL 锁定。

应用可能会通过两种方式处理散列验证失败：

- 第 1 组应用，例如 Facebook，从服务器收到 SH、CERT、SHD 消息后立即发送 SSL 警告消息。警告通常是一个表示 SSL 锁定的“Unknown CA (48)” 警告。紧接着警告消息发送 TCP 重置。在事件详细信息中，您应看到以下现象：
  - SSL 流标志包括 ALERT_SEEN。
  - SSL 流标志不包括 APP_DATA_C2S 或 APP_DATA_S2C。
  - SSL 流消息通常是：CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE。
- 第 2 组应用，例如 Dropbox，不会发送任何警告。而是，等到完成握手后发送 TCP 重置。在事件中，您应看到以下现象：
  - SSL 流标志不包括 ALERT_SEEN、APP_DATA_C2S 或 APP_DATA_S2C。
  - SSL 流消息通常是：CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED、SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED。

入侵防御系统故障排除

IPS 策略选项有哪些？

每个已自行激活的设备都会自动关联 CDO 提供的名为“默认覆盖”的 IPS 策略。CDO 为每个 FTD 设备生成一个新的 IPS 策略，因此可能有多个具有此名称的策略。如果要使用默认 IP 策略，但要修改签名覆盖选项，请参阅 Firepower 入侵策略签名覆盖了解详细信息。请注意，为每台设备配置不同的签名覆盖可能会导致默认覆盖策略变得不一致。

如何为每台设备设置不同的 IPS 策略？

CDO 为每个 FTD 设备生成一个新的 IPS 策略，因此可能有多个具有此名称的策略。在自行激活每个设备后，您不必重命名 CDO 提供的 IPS 策略。展开策略会显示与其关联的设备，您还可以按设备或策略过滤威胁事件页面和签名覆盖页面。要自定义默认覆盖策略，请按设备配置签名覆盖。这将导致默认覆盖入侵策略变得不一致，但这不会抑制任何功能。

我已自行激活已从 FDM 配置覆盖的设备。

在 CDO 外部配置的覆盖不会对设备配置或功能造成问题。

如果您载入已配置覆盖的设备，并且此新设备与**没有**覆盖的设备共享 IP 策略，则 IPS 策略将显示为**不一致**。请参阅 Firepower 入侵策略签名覆盖中的步骤 3，以解决不一致问题。

迁移后的登录失败故障排除

由于用户名或密码不正确，CDO 登录失败

解决方法 如果您尝试登录 CDO，并且知道您使用的是正确的用户名和密码，但登录失败，或者您尝试“忘记密码”无法恢复有效的密码，则您可能已尝试在未创建新 Cisco Security Cloud Sign On 帐户的情况下进行登录，则您需要按照创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证，第 66 页中的说明注册新的 Cisco Security Cloud Sign On 帐户。

登录到 Cisco Security Cloud Sign On 控制面板成功，但您无法启动 CDO

解决方法 您可能使用与 CDO 租户不同的用户名创建了 Cisco Security Cloud Sign On 账户。请联系思科技术支持中心 (TAC)，以规范 CDO 和 Cisco Secure Sign-On 之间的用户信息。

使用保存的书签登录失败

解决方法 您可能正在尝试使用浏览器中保存的旧书签登录。书签可能指向 https://cdo.onelogin.com。https://cdo.onelogin.com/

解决方法 登录 https://sign-on.security.cisco.com。

- **解决方法** 如果您尚未创建 Cisco Secure Sign-On 账户，请创建一个账户。创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证，第 66 页
- **解决方法** 如果您已创建新账户，请点击控制面板上与 思科防御协调器（美国）、思科防御协调器（欧盟）或 思科防御协调器（亚太地区）对应的 CDO 磁贴
- **解决方法** 将书签更新为指向 https://sign-on.security.cisco.com。https://sign-on.security.cisco.com/

对象故障排除

解决重复对象问题

重复对象 是指同一设备上具有不同名称但值相同的两个或多个对象。这些对象通常是意外创建的，可用于类似的目的，并供不同的策略使用。解决重复对象问题后，CDO 会使用保留的对象名称来更新所有受影响的对象引用。

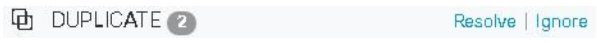
要解决重复对象问题，请执行以下操作：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

步骤 2 然后对象过滤器对象以查找重复的对象问题。

步骤 3 选择其中一个结果。在对象详细信息面板中，您将看到“重复”(DUPLICATE) 字段以及受影响的重复项数：



步骤 4 点击**解决**。CDO 会显示要比较的重复对象。

步骤 5 选择两个要比较的对象。

步骤 6 您现在有以下选项：

- 如果要将其中一个对象替换为另一个对象，请点击要保留的对象的**选择 (Pick)**，点击**解决 (Resolve)**以查看将受到影响的设备和网络策略，如果对更改满意，请点击**确认 (Confirm)**。CDO 会保留您选择替换的对象，同时删除重复项。
- 如果列表中有要忽略的对象，请点击**忽略 (Ignore)**。如果您忽略某个对象，它就会从 CDO 显示的重复对象列表中删除。
- 如果要保留对象，但又不希望 CDO 在搜索重复对象时找到该对象，请点击**全部忽略 (Ignore All)**。

步骤 7 一旦解决重复对象问题，请预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。

解决不一致或未使用的安全区域对象

安全区域对象可以像其他对象一样标记为不一致或未使用。有关如何解决这些问题的说明，请参阅解决未使用的对象问题和解决不一致的对象问题。解决未使用的对象问题, on page 720解决不一致的对象问题, on page 721

相关信息：

- 安全区域对象
- 将 Firepower 接口分配给安全区域
- 删除对象

解决未使用的对象问题

未使用的对象 ⬚ 是设备配置中存在但未被其他对象、访问列表或 NAT 规则引用的对象。

相关信息：

- 导出设备和服务列表，第 84 页
- 将设备批量重新连接到 CDO，第 88 页

解决未使用的对象问题

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

步骤 2 然后对象过滤器对象以查找未使用的对象问题。

步骤 3 选择一个或多个未使用的对象。

步骤 4 您现在有以下选项：

- 在操作窗格中，点击**删除 (Remove)** 以从 CDO 中删除未使用的对象。

- 在问题窗格中，点击**忽略 (Ignore)**。如果您忽略某个对象，CDO 将停止在未使用的对象的结果中显示该对象。

步骤 5 如果您删除了未使用的对象、预览和部署所有设备的配置更改, on page 556 您现在所做的更改，或者等待并一次部署多个更改。

Note 要批量解决未使用的对象问题，请参阅批量解决对象问题。

批量删除未使用的对象

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

步骤 2 然后对象过滤器对象以查找未使用的对象问题。

步骤 3 选择要删除的未使用对象：

- 点击对象表头行中的复选框，以便选择页面上的所有对象。
- 在对象表中选择单个未使用的对象。

步骤 4 在“操作”(Actions) 窗格中，点击**删除 (Remove)** 以删除在 CDO 中选定的所有未使用的对象。一次可以删除 99 个对象。

步骤 5 点击**确定 (OK)** 以确认您要删除未使用的对象。

步骤 6 您有两种选择来部署这些更改：

- 预览和部署所有设备的配置更改您现在所做的更改，或者等待并一次部署多个更改。
- 打开**资产**页面并查找受更改影响的设备。选择受更改影响的所有设备，然后在管理窗格中点击**全部部署**。阅读警告并采取适当的措施。

解决不一致的对象问题

不一致对象 INCONSISTENT 2 Resolve | Ignore 是指两台或多台设备上具有相同名称但值不同的对象。有时，用户会在不同的配置中创建具有相同名称和内容的对象，但随着时间的推移，这些对象的值会出现分歧，从而造成不一致。

注意：要批量解决不一致的对象问题，请参阅批量解决对象问题。

您可以对不一致的对象执行以下操作：

- **忽略**：CDO 忽略对象之间的不一致并保留其值。对象将不再列在不一致类别下。
- **合并**：CDO 将所有选定对象及其值合并到一个对象组中。

- **重命名**：CDO 允许您重命名其中一个不一致的对象并为其指定新名称。
- **将共享网络对象转换为覆盖**：CDO 允许您将不一致的共享对象（有或没有覆盖）合并为一个具有覆盖的共享对象。不一致对象中最常见的默认值设置为新形成的对象中的默认值。

Note 如果有多个通用默认值，则选择其中一个作为默认值。其余默认值和覆盖值设置为该对象的覆盖。

- **将共享网络组转换为其他值**： - CDO 允许您将不一致的共享网络组合并为具有其他值的单个共享网络组。此功能的条件是，要转换的不一致网络组必须至少有一个具有相同值的通用对象。与此条件匹配的所有默认值都将成为默认值，其余对象将作为新形成的网络组的其他值进行分配。

  例如，请考虑两个不一致的共享网络组。第一个网络组“shared_network_group”由“object_1”（192.0.2.x）和“object_2”（192.0.2.y）组成。它还包含附加值“object_3”(192.0.2.a)。第二个网络组“shared_network_group”由“object_1”(192.0.2.x) 和附加值“object_4”(192.0.2.b) 组成。将共享网络组转换为其他值时，新形成的组“shared_network_group”包含默认值“object_1”(192.0.2.x) 和“object_3”(192.0.2.y)”。 2.a) 和 'object_4' (192.0.2.b) 作为附加值。

Note 当您创建新的网络对象时，CDO 会自动将其值作为覆盖分配给具有相同名称的现有共享网络对象。这也适用于将新设备载入 CDO 的情况。

仅当满足以下条件时才会进行自动分配：

1. 必须将新网络对象分配给设备。
2. 租户中只能存在一个具有相同名称和类型的共享对象。
3. 共享对象必须已包含覆盖。

要解决不一致的对象问题，请执行以下操作：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

步骤 2 然后对象过滤器对象以查找不一致的对象问题。

步骤 3 选择不一致的对象。在对象详细信息面板中，您将看到包含受影响对象数量的不一致字段：

步骤 4 点击**解决**。CDO 显示不一致的对象以供比较。

步骤 5 您现在有以下选项：

- **全部忽略**：

a. 比较显示的对象，然后在其中一个对象上点击**忽略 (Ignore)**。或者，要忽略所有对象，请点击**全部忽略 (Ignore All)**。

b. 点击**确定 (OK)**以进行确认。

- **通过合并对象来解决：**

a. 点击**通过合并 X 对象来解决 (Resolve by Merging X Objects)**。

b. 点击 **Confirm**。

- **重命名：**

a. 点击**重命名**。

b. 保存对受影响的网络策略和设备所做的更改，然后点击**确认 (Confirm)**。

- **转换为覆盖（对于不一致的共享对象）**：将共享对象与覆盖进行比较时，比较面板仅显示**不一致的值 (Inconsistent Values)** 字段中的默认值。

a. 点击**转换为覆盖 (Convert to Overrides)**。所有不一致的对象都将转换为具有覆盖的单个共享对象。

b. 点击 **Confirm**。您可以点击**编辑共享对象 (Edit Shared Object)** 以查看新创建的对象的详细信息。您可以使用向上和向下箭头在默认值和覆盖之间移动值。

- **转换为其他值（对于不一致的网络组）：**

a. 点击**转换为其他值 (Convert to Additional Values)**。所有不一致的对象都将转换为具有其他值的单个共享对象。

b. 保存对受影响的网络策略和设备所做的更改，然后点击**确认 (Confirm)**。

步骤 6 解决不一致问题后，请立即预览和部署所有设备的配置更改所做的更改，或者等待并立即部署多个更改。

批量解决对象问题

解决具有解决未使用的对象问题、解决重复对象问题或解决不一致的对象问题, on page 721 问题的对象的方法之一是忽略它们。您可以选择并忽略多个对象，即使对象表现出多个问题也是如此。例如，如果对象既不一致又未使用，则一次只能忽略一种问题类型。

Important 如果该对象稍后与其他问题类型关联，则您提交的忽略操作仅影响您当时选择的问题。例如，如果您忽略某个对象，因为它是重复的，并且该对象后来被标记为不一致，则将其忽略为重复对象并不意味着它将作为不一致的对象被忽略。

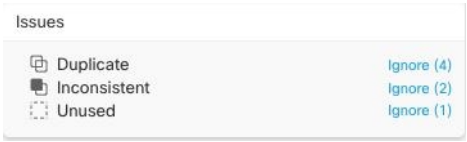
要批量忽略问题，请执行以下程序：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

步骤 2 要缩小搜索范围，您可以对象过滤器对象问题。

步骤 3 在对象表中，选择要忽略的所有适用对象。“问题”窗格按问题类型对对象进行分组。



步骤 4 点击**忽略 (Ignore)** 可按类型忽略问题。您必须单独**忽略**每种问题。

步骤 5 点击**确定 (OK)** 以确认要忽略这些对象。

设备连接状态

您可以查看 CDO 租户中载入的设备的连接状态。本主题可帮助您了解各种连接状态。在资产页面上，连接列显示设备连接状态。

当设备连接状态为“在线”时，表示设备已通电并连接到CDO。当设备由于各种原因遇到问题时，通常会出现下表中所述的其他状态。下表提供了从此类问题中恢复的方法。可能有多个问题导致连接失败。当您尝试重新连接时，CDO 会提示您先解决所有这些问题，然后再执行重新连接。

设备连接状态	可能的原因	解决方法
在线	设备已通电并连接到 CDO。	不适用
离线	设备已关闭或丢失网络连接。	检查设备是否处于离线状态。
许可证不足	设备没有足够的许可证。	许可证不足故障排除, on page 726
凭证无效	CDO 用于连接到设备的用户名和密码组合不正确。	对无效凭证进行故障排除, on page 726
检测到新证书	设备上的证书已更改。如果设备使用自签名证书，则可能是由于设备重新启动而导致的。	新证书问题故障排除, on page 727
设备已注销	FTD 设备已通过 FDM 从云中注销。	排除设备未注册故障, on page 691
申领错误	CDO 无法申领 FTD 设备。一些可能的原因可能是输入了无效的序列号或设备序列号已被申领。	申领错误

设备连接状态	可能的原因	解决方法
载入错误	在自行激活设备时，CDO 可能已失去与设备的连接。	对自行激活错误进行故障排除, on page 735
调配错误	FTD 设备初始调配失败。	调配错误
无法访问	• 设备已断电。 • 设备上的 IP 地址已更改。 • 设备已从思科云中删除。	对无法访问的连接状态进行故障排除, on page 736

排除设备未注册故障

FDM 管理 设备可能已通过 防火墙设备管理器 从云注销。

执行以下操作，在云上重新注册设备：

过程

步骤 1 在**清单 (Inventory)** 页面中，点击**设备 (Devices)** 选项卡。

步骤 2 点击 FTD 选项卡并选择处于“设备未注册”状态的设备，然后查看右侧的错误消息。

步骤 3 如果未注册的设备是使用注册密钥自行激活的，则思科防御协调器会提示您生成新的注册密钥，因为之前应用的密钥已过期。

a) 点击刷新按钮以生成新的注册密钥，然后点击复制图标。

b) 登录到要向其重新注册 CDO 的设备的 防火墙设备管理器。

c) 在 **系统设置**下，点击 **云服务**。

d) 在 思科防御协调器 区域中，展开**入门 (Get Started)**。

e) 在**注册密钥 (Registration Key)**字段中，粘贴您在 CDO 中生成的注册密钥。

f) 点击**注册 (Register)**，然后点击**接受 (Accept)** 以接受思科披露声明。防火墙设备管理器 会将注册请求发送至 CDO。

g) 在 CDO 中刷新**清单 (Inventory)** 页面，直到您看到设备的连接状态更改为“读取错误”(Read Error)。

h) 点击 CDO 的**读取配置 (Read Configuration)** 以从设备读取配置。

步骤 4 如果未注册的设备是使用序列号自行激活的，CDO 会提示您从 防火墙设备管理器 自动注册设备。

a) 登录到要向其重新注册 CDO 的设备的 防火墙设备管理器。

b) 在 **系统设置**下，点击 **云服务**。

c) 选择**通过思科防御协调器自动注册租用 (Auto-enroll with Tenancy from Cisco Defense Orchestrator)** 选项并点击**注册 (Register)**。

d) 在 CDO 中刷新**清单 (Inventory)** 页面，直到您看到设备的连接状态更改为“读取错误”(Read Error)。

e) 点击 CDO 的**读取配置 (Read Configuration)** 以从设备读取配置。

许可证不足故障排除

如果设备连接状态显示“许可证不足”(Insufficient License)，请执行以下操作：

- 等待一段时间，直到设备获得许可证。通常，思科智能软件管理器需要一些时间才能将新许可证应用于设备。
- 如果设备状态未更改，请从 CDO 注销并重新签名，以刷新 CDO 门户，以解决许可证服务器和设备之间的任何网络通信故障。
- 如果门户刷新未更改设备状态，请执行以下操作：

Procedure

步骤 1 从思科智能软件管理器生成新的令牌并进行复制。您可以观看生成智能许可视频了解详细信息。

步骤 2 在 CDO 导航栏中，点击**设备和服务 (Devices & Services)** 页面。

步骤 3 点击**设备**选项卡。

步骤 4 点击相应的设备类型选项卡，然后选择状态为**许可证不足**的设备。

步骤 5 在**设备详细信息 (Device Details)** 窗格中，点击**许可证不足 (Insufficient Licenses)**中出现的**管理许可证 (Manage Licenses)**。此时将出现**管理许可证 (Manage Licenses)** 窗口。

步骤 6 在**激活 (Activate)** 字段中，粘贴新的令牌，然后点击**注册设备 (Register Device)**。

将令牌成功应用于设备后，其连接状态将变为**在线 (Online)**。

对无效凭证进行故障排除

执行以下操作以解决由于凭证无效而导致设备断开连接的问题：

Procedure

步骤 1 通过在**清单 (Inventory)** 页面中导航来打开。

步骤 2 点击**设备 (Devices)** 选项卡。

步骤 3 点击相应的设备类型选项卡，然后选择具有**无效凭证 (Invalid Credentials)** 状态的设备。

步骤 4 在**设备详细信息 (Device Details)** 窗格中，点击**无效凭证 (Invalid Credentials)** 中显示的 **重新连接 (Reconnect)**。CDO 尝试与您的设备重新连接。

步骤 5 出现提示时，输入设备的用户名和密码。

步骤 6 点击**继续**。

步骤 7 设备在线并准备好使用后，点击**关闭 (Close)**。

步骤 8 可能是因为 CDO 尝试使用错误的凭证连接到设备，因此直接在设备上更改了 CDO 用于连接到设备的用户名和密码组合。您现在可能会看到设备处于“在线”(Online) 状态，但配置状态为“检测到冲突”(Conflict Detected)。使用解决配置冲突 以查看和解决 CDO 与设备之间的配置差异。

新证书问题故障排除

CDO 对证书的使用

CDO 在连接到设备时检查证书的有效性。具体而言，CDO 要求：

1. 设备使用 TLS 版本 1.0 或更高版本。
2. 设备提供的证书未过期，并且其颁发日期是过去的日期（即，它已经有效，未计划在以后生效）。
3. 证书必须是 SHA-256 证书。不接受 SHA-1 证书。
4. 以下条件之一成立：
   - 设备使用自签名证书，并且与授权用户信任的最新证书相同。
   - 设备使用受信任证书颁发机构 (CA) 签名的证书，并提供将所提供的枝叶证书链接到相关 CA 的证书链。

以下是 CDO 使用与浏览器不同的证书的方式：

- 如果是自签名证书，则 CDO 会覆盖域名检查，而不会在设备载入或重新连接期间检查证书是否与授权用户信任的证书完全匹配。
- CDO 尚不支持内部 CA。目前无法检查由内部 CA 签名的证书。

  可以按设备禁用 ASA 设备的证书检查。当 CDO 无法信任 ASA 的证书时，您可以选择禁用该设备的证书检查。如果您已尝试禁用设备的证书检查，但仍无法将其载入，则可能是您为设备指定的 IP 地址和端口不正确或无法访问。无法全局禁用证书检查，也无法对具有受支持证书的设备禁用证书检查。无法禁用非 ASA 设备的证书检查。

  当您禁用设备的证书检查时，CDO 仍将使用 TLS 连接到设备，但不会验证用于建立连接的证书。这意味着被动的中间人攻击者将无法窃听连接，但主动的中间人可以通过提供具有无效证书的 CDO 来拦截连接。

确定证书问题

CDO 可能无法载入设备的原因有很多种。当 UI 显示消息“CDO 无法使用提供的证书连接到设备”时，表示证书存在问题。当 UI 不显示此消息时，问题更有可能与连接问题（设备无法访问）或其他网络错误有关。

要确定 CDO 拒绝给定证书的原因，您可以在 SDC 主机或可访问相关设备的其他主机上使用 openssl 命令行工具。使用以下命令创建显示设备提供的证书的文件：

```
openssl s_client -showcerts -connect <host>:<port> &> <filename>.txt
```

此命令将启动交互式会话，因此您需要在几秒钟后使用 Ctrl-c 退出。

您现在应该有一个包含如下输出的文件：

```
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = Google Inc, CN = Google Internet Authority G2
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN = *.google.com
verify return:1 CONNECTED(00000003)
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
  i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
  i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
  i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits

---
SSL handshake has read 4575 bytes and written 434 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 48F046F3360225D51BE3362B50CE4FE8DB6D6B80B871C2A6DD5461850C4CF5AB
    Session-ID-ctx:
    Master-Key:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FBFEBAB1B6

    Key-Arg : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 100800 (seconds)
```

```
    TLS session ticket:
    0000 - 7a eb 54 dd ac 48 7e 76-30 73 b2 97 95 40 5b de z.T..H~v0s...@[.
    0010 - f3 53 bf c8 41 36 66 3e-5b 35 a3 03 85 6f 7d 0c .S..A6f>[5...o}.
    0020 - 4b a6 90 6f 95 e2 ec 03-31 5b 08 ca 65 6f 8f a6 K..o....1[..eo..
    0030 - 71 3d c1 53 b1 29 41 fc-d3 cb 03 bc a4 a9 33 28 q=.S.)A.......3(
    0040 - f8 c8 6e 0a dc b3 e1 63-0e 8f f2 63 e6 64 0a 36 ..n....c...c.d.6
    0050 - 22 cb 00 3a 59 1d 8d b2-5c 21 be 02 52 28 45 9d "..:Y...\!..R(E.
    0060 - 72 e3 84 23 b6 f0 e2 7c-8a a3 e8 00 2b fd 42 1d r..#...|....+.B.
    0070 - 23 35 6d f7 7d 85 39 1c-ad cd 49 f1 fd dd 15 de #5m.}.9...I.....
    0080 - f6 9c ff 5e 45 9c 7c eb-6b 85 78 b5 49 ea c4 45 ...^E.|.k.x.I..E
    0090 - 6e 02 24 1b 45 fc 41 a2-87 dd 17 4a 04 36 e6 63 n.$.E.A....J.6.c
    00a0 - 72 a4 ad
    00a4 - <SPACES/NULS> Start Time: 1476476711 Timeout : 300 (sec)
Verify return code: 0 (ok)
---
```

在此输出中要注意的第一件事是最后一行，您可以在其中看到**验证返回代码 (Verify return code)**。如果存在证书问题，返回代码将为非零值，并且会有错误说明。

展开此证书错误代码列表，查看常见错误及其补救方法

0 X509_V_OK 操作成功。

2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT 无法找到不受信任证书的颁发者证书。

3 X509_V_ERR_UNABLE_TO_GET_CRL 无法找到证书的 CRL。

4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE 无法解密证书签名。这意味着无法确定实际签名值，而不是与预期值不匹配。这仅对 RSA 密钥有意义。

5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE 无法解密 CRL 签名。这意味着无法确定实际签名值，而不是与预期值不匹配。未使用。

6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY 无法读取证书 SubjectPublicKeyInfo 中的公钥。

7 X509_V_ERR_CERT_SIGNATURE_FAILURE 证书签名无效。

8 X509_V_ERR_CRL_SIGNATURE_FAILURE 证书签名无效。

9 X509_V_ERR_CERT_NOT_YET_VALID 证书无效：notBefore 日期晚于当前时间。有关详细信息，请参阅下面的验证返回代码：9（证书尚未生效）。

10 X509_V_ERR_CERT_HAS_EXPIRED The certificate has expired;也就是说，notAfter 日期早于当前时间。有关详细信息，请参阅下面的验证返回代码：10（证书已过期）。

11 X509_V_ERR_CRL_NOT_YET_VALID CRL 尚未生效。

12 X509_V_ERR_CRL_HAS_EXPIRED CRL 已过期。

13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD 证书 notBefore 字段包含无效时间。

14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD 证书 notAfter 字段包含无效时间。

15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD CRL lastUpdate 字段包含无效时间。

16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD CRL nextUpdate 字段包含无效时间。

17 X509_V_ERR_OUT_OF_MEM 尝试分配内存时发生错误。这绝不应该发生。

18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT 通过的证书是自签名证书，在受信任证书列表中找不到相同的证书。

19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN 可以使用不受信任的证书建立证书链，但无法在本地找到根证书。

20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY 无法找到本地查找的证书的颁发者证书。这通常意味着受信任证书列表不完整。

21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE 无法验证签名，因为该链仅包含一个证书，并且它不是自签名证书。有关详细信息，请参阅下面的“验证返回代码：21（无法验证第一个证书）”。验证返回代码：21（无法验证下面的第一个证书）以了解详细信息。

22 X509_V_ERR_CERT_CHAIN_TOO_LONG 证书链长度大于提供的最大深度。未使用。

23 X509_V_ERR_CERT_REVOKED 证书已被撤销。

24 X509_V_ERR_INVALID_CA CA 证书无效。它不是 CA 或其扩展名与提供的用途不一致。

25 X509_V_ERR_PATH_LENGTH_EXCEEDED BasicConstraints 路径长度参数已被超过。

26 X509_V_ERR_INVALID_PURPOSE 提供的证书不能用于指定的目的。

27 X509_V_ERR_CERT_UNTRUSTED 根 CA 未标记为用于指定用途的受信任。

28 X509_V_ERR_CERT_REJECTED 根 CA 被标记为拒绝指定用途。

29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH 当前候选颁发者证书被拒绝，因为其使用者名称与当前证书的颁发者名称不匹配。仅在设置了 -issuer_checks 选项时显示。

30 X509_V_ERR_AKID_SKID_MISMATCH 当前候选颁发者证书被拒绝，因为其使用者密钥标识符存在且与当前证书的颁发机构密钥标识符不匹配。仅在设置了 -issuer_checks 选项时显示。

31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH 当前候选颁发者证书被拒绝，因为其颁发者名称和序列号存在，并且与当前证书的颁发机构密钥标识符不匹配。仅在设置了 -issuer_checks 选项时显示。

32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN 当前候选颁发者证书被拒绝，因为其 keyUsage 扩展不允许证书签名。

50 X509_V_ERR_APPLICATION_VERIFICATION 应用特定错误。未使用。

检测到新证书

如果升级具有自签名证书的设备，并且在升级过程后生成了新证书，则CDO可能会生成“检测到新证书”(New Certificate Detected) 消息作为**配置状态 (Configuration Status)** 和**连接 (Connectivity)** 状态。您必须手动确认并解决此问题，然后才能继续从CDO对其进行管理。证书同步且设备处于正常状态后，即可管理设备。

Note 当您同时将多个托管设备将设备批量重新连接到 CDO连接到 CDO 时，CDO 会自动审核并接受设备上的新证书，并继续与其重新连接。

使用以下程序解析新证书：

1. 导航到**设备和服务 (Device & Services)** 页面。
2. 使用过滤器显示**检测到新证书 (New Certificate Detected)** 连接或配置状态的设备，然后选择所需的设备。
3. 在右侧窗格中，点击**查看证书 (Review Certificate)**。CDO 允许您下载证书以供审核并接受新证书。
4. 在设备同步窗口中，点击**接受 (Accept)**，或在重新连接到设备窗口中，点击**继续 (Continue)**。

   CDO 会自动将设备与新的自签名证书同步。您可能需要手动刷新**设备和服务 (Devices & Services)** 页面，才能在设备同步后查看设备。

证书错误代码

验证返回代码：0（正常），但 CDO 返回证书错误

CDO 获得证书后，它会尝试通过对“https://”进行 GET 调用来连接到设备的 URL。<device_ip>：<port> "。如果这不起作用，CDO 将显示证书错误。如果您发现证书有效（openssl 返回 0 ok），则问题可能是其他服务正在侦听您尝试连接的端口。只能使用命令：

```
curl -k -u <username>:<password> https://<device_id>:<device_port>/admin/exec/show%20version
```

确定您是否确实在与 ASA 通信，并检查 HTTPS 服务器是否在 ASA 上的正确端口上运行：

```
 # show asp table socket
Protocol         Socket         State         Local Address             Foreign Address
SSL             00019b98         LISTEN        192.168.1.5:443             0.0.0.0:*
SSL             00029e18         LISTEN        192.168.2.5:443             0.0.0.0:*
TCP             00032208         LISTEN        192.168.1.5:22              0.0.0.0:*
```

验证返回代码：9（证书尚未生效）

此错误意味着所提供证书的颁发日期是未来，因此客户端不会将其视为有效。这可能是由于证书构建不良导致的，或者在自签名证书的情况下，可能是由于设备生成证书时时间错误。

您应该会在错误中看到一行，包括证书的 notBefore 日期：

```
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=9:certificate is not yet valid
notBefore=Oct 21 19:43:15 2016 GMT
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
notBefore=Oct 21 19:43:15 2016 GMT
```

通过此错误，您可以确定证书何时生效。

补救

证书的 notBefore 日期需要是过去的日期。您可以使用更早的 notBefore 日期重新颁发证书。当客户端或颁发设备上的时间设置不正确时，也会出现此问题。

验证返回代码：10（证书已过期）

此错误意味着所提供的至少一个证书已过期。您应该会在错误中看到一行，包括证书的 notBefore 日期：

```
 error 10 at 0 depth lookup:certificate has expired
```

到期日期位于证书正文中。

补救

如果证书确实已过期，则唯一的补救方法是获取另一个证书。如果证书仍将到期，但openssl声称它已过期，请检查计算机上的时间和日期。例如，如果某个证书设置为在2020年到期，但您的计算机上的日期是 2021 年，则您的计算机会将该证书视为已过期。

验证返回代码：21（无法验证第一个证书）

此错误表示证书链存在问题，并且openssl无法验证设备提供的证书是否应受信任。我们来看看上面示例中的证书链，了解证书链的工作原理：

```
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2

-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority

-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE----- ---
```

证书链是服务器提供的证书列表，从服务器自己的证书开始，然后包括将服务器的证书与证书颁发机构的顶级证书链接的更高级别的中间证书。每个证书都会列出其使用者（以“s:”开头的行及其颁发者）（以“i”开头的行）。

使用者是证书所标识的实体。它包括组织名称，有时还包括为其颁发证书的实体的通用名称。

颁发者是颁发证书的实体。它还包括一个组织字段，有时还包括一个通用名称。

如果服务器具有由受信任证书颁发机构直接颁发的证书，则无需在其证书链中包含任何其他证书。它将显示一个如下所示的证书：

```
--- Certificate chain 0 s:/C=US/ST=California/L=Anytown/O=ExampleCo/CN=*.example.com
i:/C=US/O=Trusted Authority/CN=Trusted Authority
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE----- ---
```

鉴于此证书，openssl 将验证 ***.example.com** 的 ExampleCo 证书是否由受信任的颁发机构证书正确签名，该证书存在于 openssl 的内置信任存储区中。验证后，openssl 将成功连接到设备。

但是，大多数服务器没有直接由受信任 CA 签名的证书。相反，与第一个示例一样，服务器的证书由一个或多个中间设备签名，而最高级别的中间设备具有由受信任 CA 签名的证书。默认情况下，OpenSSL 不信任这些中间 CA，并且只有在获得以受信任 CA 结尾的完整证书链时才能对其进行验证。

由中间机构签署证书的服务器必须提供将其链接到受信任 CA 的所有证书，包括所有中间证书。如果它们不提供整个链，则 openssl 的输出将如下所示：

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=20:unable to get local issuer certificate
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=27:certificate not trusted
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=21:unable to verify the first certificate
verify return:1

CONNECTED(00000003)

---
Certificate chain
0 s:/OU=Example Unit/CN=example.com
i:/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
-----BEGIN CERTIFICATE-----
...lots of b64...
-----END CERTIFICATE-----
---
Server certificate
subject=/OU=Example Unit/CN=example.com
issuer=/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
---
No client certificate CA names sent
---
SSL handshake has read 1509 bytes and written 573 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 24B45B2D5492A6C5D2D5AC470E42896F9D2DDDD54EF6E3363B7FDA28AB32414B
Session-ID-ctx:
Master-Key:
21BAF9D2E1525A5B935BF107DA3CAF691C1E499286CBEA987F64AE5F603AAF8E65999BD21B06B116FE9968FB7C62EF7C

Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
```

```
Start Time: 1476711760
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

此输出显示服务器仅提供一个证书，并且提供的证书是由中间机构而不是受信任的根签名的。输出还显示特征验证错误。

补救

此问题是由设备提供的证书配置错误引起的。解决此问题的唯一方法是将正确的证书链加载到设备上，以便 CDO 或任何其他程序可以安全地连接到设备，以便为连接的客户端提供完整的证书链。

要将中间 CA 添加到信任点，请访问以下链接之一（具体取决于您的情况 - 是否在 ASA 上生成了 CSR）：

- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc13
- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc15

检测到新证书

如果升级具有自签名证书的设备，并且在升级过程后生成了新证书，则CDO可能会生成“检测到新证书”(New Certificate Detected) 消息作为**配置状态 (Configuration Status)** 和**连接 (Connectivity)** 状态。您必须手动确认并解决此问题，然后才能继续从CDO对其进行管理。证书同步且设备处于正常状态后，即可管理设备。

注释 当您选择将设备批量重新连接到 CDO 同时将多个托管设备连接到CDO时，CDO会自动审核并接受设备上的新证书，并继续与其重新连接。

使用以下程序解析新证书：

过程

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 使用过滤器显示**检测到新证书 (New Certificate Detected)** 连接或配置状态的设备，然后选择所需的设备。

步骤 5 在右侧窗格中，点击**查看证书 (Review Certificate)**。CDO 允许您下载证书以供审核并接受新证书。

步骤 6 在设备同步窗口中，点击**接受 (Accept)**，或在重新连接到设备窗口中，点击**继续 (Continue)**。

CDO 会自动将设备与新的自签名证书同步。您可能需要手动刷新**设备和服务 (Devices & Services)** 页面，才能在设备同步后查看设备。

对自行激活错误进行故障排除

出现设备自行激活错误的原因有很多。

可以采取以下操作：

Procedure

步骤 1 在**清单 (Inventory)** 页面中，点击**设备 (Devices)** 选项卡。

步骤 2 点击相应的设备类型选项卡，然后选择遇到此错误的设备。在某些情况下，您会在右侧看到错误说明。执行说明中提到的必要操作。

或

步骤 3 从 CDO 中删除设备实例，然后尝试重新载入设备。

解决“检测到冲突”状态

CDO 允许您在每个实时设备上启用或禁用冲突检测。如果 冲突检测, on page 563 已启用，并且在未使用 CDO 的情况下对设备的配置进行了更改，则设备的配置状态将显示为**检测到冲突 (Conflict Detected)**。

要解决“检测到冲突”(Conflict Detected) 状态，请执行以下程序：

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择报告冲突的设备，然后点击右侧详细信息窗格中的**查看冲突 (Review Conflict)**。

步骤 5 在**设备同步 (Device Sync)** 页面中，通过查看突出显示的差异来比较两种配置。

- 标记为“最后一次设备配置”(Last Known Device Configuration) 的面板是存储在 CDO 上的设备配置。
- 标记为“在设备上找到”(Found on Device) 的面板是存储在运行 ASA 配置中的配置。

步骤 6 通过选择以下选项之一来解决冲突：

- **接受设备更改 (Accept Device changes)**：这将使用设备的运行配置覆盖 CDO **上存储的配置** 和任何待处理的更改。

Note 由于 CDO 不支持在命令行界面之外部署对Cisco IOS 设备的更改，因此在解决冲突时，您对Cisco IOS 设备的唯一选择是选择**接受而不查看 (Accept Without Review)**。

- **拒绝设备更改 (Reject Device Changes)**：这将使用存储在 CDO 上的配置覆盖设备上存储的配置。

Note 所有配置更改（拒绝或接受）都记录在更改日志中。

解决“未同步”状态

使用以下程序解决配置状态为“未同步”的设备：

Procedure

步骤 1 在导航栏中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

步骤 3 点击设备类型选项卡。

步骤 4 选择报告为“未同步”的设备。

步骤 5 在右侧的未同步面板中，选择以下任一选项：

- **预览并部署...** - 如果要将配置更改从 CDO 推送到设备，请预览并部署您现在所做的更改，或者等待并一次部署多个更改。预览和部署所有设备的配置更改, on page 556
- 放弃更改 - 如果您不想将配置更改从 CDO 推送到设备，或者您想要“撤消”您开始在 CDO 上进行的配置更改。此选项使用设备上存储的运行配置覆盖 CDO 中存储的配置。

对无法访问的连接状态进行故障排除

由于各种原因，设备可能处于“无法访问”状态：

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击相应的设备类型选项卡，然后选择具有**无法接通 (Unreachable)** 状态的设备。

步骤 4 点击 **重新连接 (Reconnect)** 。

步骤 5 根据右侧显示的消息执行以下操作之一：

a. 如果您已使用 IP 地址和设备凭证自行激活设备，系统将显示以下消息：FDM 管理

“此设备无法访问，请查看 IP 地址和端口”，在消息框中输入设备的新 IP 地址和/或新端口信息。可能是因为 CDO 尝试连接到无效的 IP 地址，因此直接在设备上更改了设备的 IP 地址。

Note 如果设备已重新启动，并且没有其他待处理的更改，则设备应返回到在线连接状态，并且无需进一步操作。

您现在可能会看到设备处于“在线”(Online) 状态，但配置状态为“检测到冲突”(Conflict Detected)。使用解决配置冲突 以查看 CDO 与设备之间的配置差异。

b. 如果您使用注册令牌或序列号自行激活设备，系统将显示以下消息：FDM 管理

" 此设备已从思科云中删除。删除可能是退货授权 *(RMA)* 流程的一部分。这意味着您退回 RMA 团队的故障设备已作为 RMA 流程的一部分从思科云中删除。

因此，您将看到 CDO 中的设备连接状态为“无法访问”。

- 对于 RMA 案例，您需要在 CDO 中执行以下步骤：

  1. 如果设备已成功自行激活，则需要将设备配置另存为模板。请参阅配置 FDM 模板。

     从 CDO 中删除设备实例。

  2. 打开您从 RMA 团队收到的新更换设备的电源，并将其载入 CDO。请参阅使用设备的序列号载入 FDM 管理 设备。

     Important 替换设备可能具有不同的序列号，需要作为新设备自行激活。

     您现在将看到设备处于“在线”(Online) 状态，但配置状态为“检测到冲突”(Conflict Detected)。

  3. 使用解决配置冲突 以查看 CDO 与设备之间的配置差异。

     将之前保存的模板应用于新设备。请参阅应用 FDM 模板。

- 如果您已将设备出售或将其所有权转让给租户之外的其他用户，则不会清除设备的配置，您将不再拥有该设备。当买方重新映像设备时，会发生此错误。如果设备之前已正确配置并同步，则可以将设备配置另存为模板，然后从 CDO 中删除设备实例。

SecureX 故障排除

尝试将 CDO 与 SecureX 结合使用时，可能会遇到错误、警告和问题。对于 SecureX UI 中发现的问题，您必须使用 SecureX 文档。有关详细信息，请参阅 SecureX 的支持。https://visibility.amp.cisco.com/iroh/iroh-auth/login?redirect_after_login=https://securex.us.security.cisco.com/help/terms-privacy-support

要创建有关 CDO 中 SecureX 功能区功能的案例，或有关 SecureX 功能区的租户可访问性，请参阅 CDO 思科 TAC 以了解详细信息。联系思科威胁防御支持, on page 752系统可能会要求您提供租户 ID。

SecureX UI 故障排除

我在 SecureX 控制面板中看到重复的 CDO 模块

您可以在 SecureX 中手动配置单个产品的多个模块。例如，如果您有多个 CDO 租户，则可以为每个租户创建一个 CDO 模块。重复的模块意味着来自同一 CDO 租户的两个单独的 API 令牌。这种冗余可能会导致控制面板混乱和混乱。

如果您碰巧在 SecureX 中手动配置了一个 CDO 模块，然后在 CDO 的常规设置页面中选择了连接 SecureX，这可能会导致一个租户在 SecureX 中具有多个模块。

作为一种解决方法，我们建议从 SecureX 中删除原始 CDO 模块，并继续使用重复模块监控 CDO 性能。此模块使用更强大的 API 令牌生成，该令牌更安全，并与 SecureX 功能区兼容。

CDO UI 故障排除

要在 SecureX 中提交有关 CDO 模块的支持案例，请参阅 SecureX 条款、隐私、支持的“支持”部分了解详细信息。https://visibility.amp.cisco.com/iroh/iroh-auth/login?redirect_after_login=https://securex.us.security.cisco.com/help/terms-privacy-support

OAuth 错误

您可能会遇到 oAuth 错误，并显示以下消息：“用户似乎不具有所有必需的范围或足够的权限”。如果您遇到此问题，请考虑以下可能性：

- 您的帐户可能未激活。请参阅 https://visibility.test.iroh.site/ 并使用您的注册邮箱地址查看您的账户是否已激活。https://visibility.test.iroh.site/iroh/iroh-auth/login?redirect_after_login=https://visibility.test.iroh.site/investigate&title=Threat%20Response如果账户未激活，您的 CDO 租户可能不会与 SecureX 合并；您必须联系思科 TAC 来解决此问题。有关详细信息，请参阅联系思科威胁防御支持。

我使用错误的组织凭证登录 SecureX

如果您选择使用“常规设置”(General Settings) 页面的“租户设置”(Tenant Settings) 部分中的“连接 SecureX”(Connect SecureX) 选项将 CDO 事件发送到 SecureX，但使用错误的凭证登录 SecureX，您可能会在 SecureX 控制面板中看到来自错误租户的事件。

解决方法是，在 CDO 的“常规设置”(General Settings) 页面中点击断开 SecureX。这将终止用于向 SecureX 组织发送和接收信息的只读 API 用户，从而终止 SecureX 控制面板。

然后，您必须重新启用 Connect Tenant to SecureX，并在系统提示登录 SecureX 时使用正确的组织登录凭证。

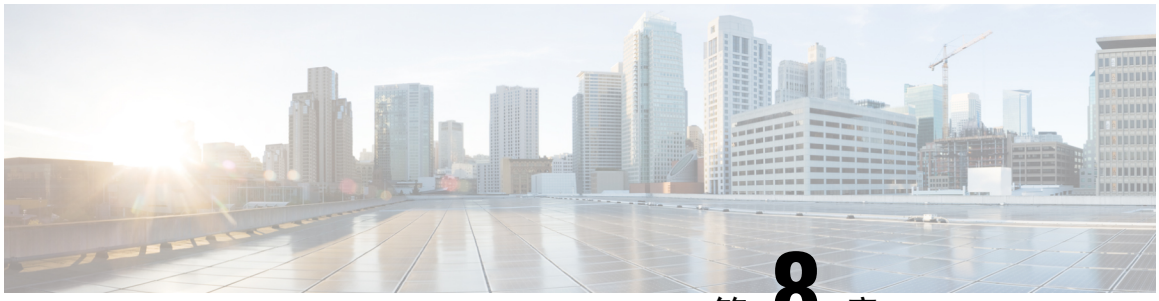
我使用错误的帐户登录功能区

此时，如果使用错误的帐户信息登录功能区，则无法注销功能区。您必须在支持案例管理器中创建案例，才能手动重置功能区登录。https://mycase.cloudapps.cisco.com/case

无法启动 SecureX 功能区

您可能无权访问适当的范围；您必须联系思科 TAC 来解决此问题。有关详细信息，请参阅联系思科威胁防御支持。

有关 SecureX 功能区如何运行的其他信息，请参阅 SecureX 功能区文档。https://visibility.amp.cisco.com/iroh/iroh-auth/login?redirect_after_login=https://securex.us.security.cisco.com/help/ribbon



第 8 章

常见问题和支持

本章包含以下各节：

思科 Defense Orchestrator

什么是 Cisco Defense Orchestrator？

Cisco Defense Orchestrator (CDO) 是一种基于云的多设备管理器，允许网络管理员跨各种安全设备创建和维护一致的安全策略。

您可以使用 CDO 管理以下设备：

- Cisco Secure Firewall ASA
- Cisco 安全防火墙威胁防御
- Cisco Secure Firewall Cloud Native
- 思科资安防护伞
- Meraki
- 思科 IOS 设备

- Amazon Web 服务 (AWS) 实例
- 使用 SSH 连接管理的设备

CDO 管理员可以通过一个界面监控和维护所有这些设备类型。

有关将设备自行激活到思科 Defense Orchestrator 的常见问题解答

关于 CDO 自行激活的常见问题Secure Firewall ASA

如何使用凭证自行激活？ASA

您可以一次载入一个或批量载入 ASA 设备。载入属于高可用性对的 ASA 时，请使用载入 ASA 设备 (Onboard an ASA Device) 仅载入该对的主设备。载入安全情景或管理情景的方法与载入任何其他 ASA 的方法相同。

如何一次自行激活多个设备？ASA

您可以使用 CSV 文件创建一个 ASA 列表，CDO 将载入列表中的所有 ASA。有关如何批量载入 ASA 的说明，请参阅批量载入 ASA。

自行激活 后应该怎么做？ASA

有关入门，请参阅使用思科防御协调器管理 ASA。

关于将 FDM 管理的设备自行激活的常见问题 CDO

如何载入 FDM 管理的设备？

有多种方法可以载入 FDM 管理的设备。我们建议使用注册密钥方法。请参阅载入 FDM 管理的设备以开始使用。https://docs.defenseorchestrator.com/#!c_onboard-an-ftd.html

关于将安全防火墙威胁防御自行激活的常见问题云交付的防火墙管理中心

如何载入 Cisco Secure Firewall Threat Defense？

您可以使用 CLI 注册密钥、通过低接触调配或使用序列号载入 FTD 设备。

在注册 Cisco Secure Firewall Threat Defense 后应该怎么做？

在设备同步后，导航至“工具和服务”(Tools & Services)>“防火墙管理中心”(Firewall Management Center)，然后从“操作”(Actions)、“管理”(Management) 或“设置”(Settings) 窗格中选择一个操作，以开始在云交付的防火墙管理中心中配置威胁防御设备。请参阅云交付的防火墙管理中心应用页面以开始。

如何对 Cisco Secure Firewall Threat Defense 进行故障排除？

请参阅对载入 Cisco Secure Firewall Threat Defense 进行故障排除。

关于本地 Cisco Secure Firewall Management Center 的常见问题

如何载入本地管理中心？

您可以将本地管理中心载入 CDO。自行激活本地管理中心也会将注册到本地管理中心的所有设备自行激活。CDO 不支持创建或修改与本地管理中心或注册到本地管理中心的设备关联的对象或策略。您必须在本地管理中心 UI 中进行这些更改。请参阅载入本地管理中心以开始使用。
https://docs.defenseorchestrator.com/#!c-onboard-an-fmc-.html

有关将 Meraki 设备自行激活的常见问题解答 CDO

如何载入 Meraki 设备？

MX 设备既可由 CDO 管理，也可由 Meraki 控制面板管理。CDO 将配置更改部署到 Meraki 控制面板，后者又将配置安全地部署到设备。请参阅载入 Meraki MX 设备以开始使用。
https://docs.defenseorchestrator.com/#!g-chapterwrapper-for-olh-onboard-meraki-mx-devices.html

有关自行激活 SSH 设备的常见问题解答 CDO

如何载入 SSH 设备？

您可以使用 SSH 设备上存储的高权限用户的用户名和密码，通过安全设备连接器 (SDC) 载入设备。请参阅载入 SSH 设备以开始使用。https://docs.defenseorchestrator.com/#!t-onboard-an-ssh-device.html

如何删除设备？

您可以从资产页面中删除设备。

关于自行激活 IOS 设备的常见问题解答 CDO

如何载入思科 IOS 设备？

您可以使用安全设备连接器 (SDC) 载入运行思科 IOS（互联网操作系统）的实时思科设备。请参阅载入思科 IOS 设备以开始使用。https://docs.defenseorchestrator.com/#!c-onboard-a-cisco-ios-device.html

如何删除设备？

您可以从“资产”页面删除设备。

设备类型

什么是自适应安全设备 (ASA)？

思科 ASA 在一台设备以及带附加模块的集成服务中提供高级状态防火墙和 VPN 集中器功能。ASA 包括许多高级功能，例如多安全情景（类似于虚拟化防火墙）、集群（将多个防火墙组合成一个防火墙）、透明（第 2 层）防火墙或路由（第 3 层）防火墙操作、高级检测引擎、IPsec VPN、SSL VPN 和无客户端 SSL VPN 支持以及许多其他功能。ASA 可以安装在虚拟机或受支持的硬件上。

什么是 ASA 型号？

ASA 型号是已载入 CDO 的 ASA 设备的运行配置文件的副本。您可以使用 ASA 模型分析 ASA 设备的配置，而无需自行激活设备。

什么是 Firepower 威胁防御 (FTD)？

思科的下一代防火墙软件映像。它力求将 Sourcefire 下一代防火墙服务与 ASA 平台的精华相结合。它可以安装在许多不同的 Firepower 硬件设备或虚拟机上。这与 ASA FirePOWER 模块不同。有关详细信息，请参阅 CDO 支持的软件和硬件。

什么是 Firepower 设备管理器 (FDM)？

Firepower 设备管理器是随 FTD 映像提供的 Firepower 威胁防御管理软件。FDM 旨在管理随附的一个 FTD。您可能还会听到 FDM 被称为“本地设备管理器”。

Firepower 是什么？

Firepower 是一个通用术语，指的是一组下一代防火墙硬件和软件。

设备何时同步？

当 CDO 上的配置和设备本地存储的配置相同时。

何时设备未同步？

如果 CDO 中存储的配置已更改，现在存储在设备上的配置有所不同。

设备何时处于“检测到冲突”状态？

设备上的配置在 CDO 外部（带外）更改，现在与 CDO 上存储的配置不同。

什么是带外更改？

在对 CDO 外部设备进行了更改时。使用 CLI 命令或使用设备上的管理器（例如 ASDM 或 FDM）直接在设备上进行更改。带外更改会导致 CDO 报告设备的“检测到冲突”状态。

将更改部署到设备意味着什么？

将设备载入 CDO 后，CDO 会维护其配置的副本。当您对 CDO 进行更改时，CDO 会对其设备配置的副本进行更改。当您将该更改“部署”回设备时，CDO 会将您所做的更改复制到设备的配置副本。请参阅以下主题：

- 预览和部署所有设备的配置更改, on page 556
- 将配置更改从 CDO 部署到 FDM 管理 设备

当前支持哪些 ASA 命令？

所有命令。点击设备操作下的命令行界面链接以使用 ASA CLI。

设备管理是否有任何规模限制？

CDO 的云架构使其能够扩展到数千台设备。

CDO 会管理思科集成多业务和汇聚多业务路由器吗？

CDO 允许您为 ISR 和 ASR 创建模型设备并导入其配置。然后，您可以根据导入的配置创建模板，并将配置导出为可部署到新的或现有的 ISR 和 ASR 设备的标准化配置，以实现一致的安全性。

CDO 能否管理 SMA？

否，CDO 当前不管理 SMA。

安全

CDO 安全吗？

CDO 通过以下功能为客户数据提供端到端安全：

- 新 CDO 租户的初始登录, on page 36
- API 和数据库操作的身份验证调用
- 传输中和静态数据隔离
- 角色分离

CDO 需要对用户进行多因素身份验证才能连接到其云门户。多因素身份验证是保护客户身份所需的重要功能。

传输中和静态的所有数据均已加密。来自客户端和 CDO 设备的通信使用 SSL 进行加密，并且所有客户-租户数据量都已加密。

CDO 的多租户架构可隔离租户数据并加密数据库与应用服务器之间的流量。当用户进行身份验证以获得对 CDO 的访问权限时，他们会收到一个令牌。此令牌用于从密钥管理服务获取密钥，该密钥用于加密到数据库的流量。

CDO 快速为客户创造价值，同时确保客户凭证的安全。这是通过在云或客户自己的网络（路线图）中部署“安全数据连接器”来实现的，该网络控制所有入站和出站流量，以确保凭证数据不会离开客户场所。

第一次登录 CDO 时收到错误“无法验证您的 OTP”

检查您的桌面或移动设备时钟是否与世界时间服务器同步。时钟不同步的时间少于或超过一分钟可能会导致生成不正确的 OTP。

我的设备是否直接连接到思科 Defense Orchestrator 云平台？

是。使用 CDO SDC 执行安全连接，该 CDO SDC 用作设备和 CDO 平台之间的代理。CDO 架构在设计时考虑到了安全性，可以完全分离到设备的数据来回传输。

如何连接没有公共 IP 地址的设备？

您可以利用 CDO 安全设备连接器 (SDC)，该连接器可部署在您的网络内，无需打开任何外部端口。安全设备连接器 (SDC), on page 10部署 SDC 后，您可以使用内部（非互联网路由）IP 地址载入设备。

SDC 是否需要任何额外费用或许可证？

否。

CDO 当前支持哪些类型的虚拟专用网络？

对于客户，CDO 仅支持 IPsec 站点到站点 VPN 隧道管理。ASA请继续关注我们的“新功能”页面的更新。

如何检查隧道状态？状态选项

CDO 每小时自动执行一次隧道连接检查，但可以通过选择隧道并请求检查连接来执行临时 VPN 隧道连接检查。处理结果可能需要几秒钟。

是否可以根据设备名称及其对等体之一的 IP 地址搜索隧道？

是。使用名称和对等体 IP 地址上的可用过滤器和搜索功能，搜索并转至特定 VPN 隧道的详细信息。

故障排除

在从 CDO 到受管设备执行设备配置的完整部署时，我收到一条警告“无法将更改部署到设备”。我该怎么做才能解决这个问题？

如果在将完整配置（在CDO支持的命令之外执行的更改）部署到设备时发生错误，请点击“检查更改”以从设备提取最新的可用配置。这可能会解决问题，您将能够继续对 CDO 进行更改并进行部署。如果问题仍然存在，请从“联系支持”页面联系思科 TAC。

在解决带外问题（在 CDO 外部执行的更改；直接对设备进行更改）时，将 CDO 中的配置与设备的配置进行比较，CDO 会显示我未添加或修改的其他元数据。为什么会出现这种情况？

随着CDO扩展其功能，将从设备的配置中收集其他信息，以丰富和维护所有所需的数据，以便更好地进行策略和设备管理分析。这些不是在受管设备上发生的更改，而是已经存在的信息。通过检查设备中的更改并查看发生的更改，可以轻松解决检测到的冲突状态。

为什么 CDO 会拒绝我的证书？

请参阅解析新证书 新证书问题故障排除, on page 727

低接触调配中使用的术语和定义

- **已申领 (Claimed)** - 用于在 CDO 中载入序列号的情景。如果设备的序列号已载入 CDO 租户，则该设备为“已申领”。
- **暂留 (Parked)** - 用于在 CDO 中载入序列号的情景。如果设备已连接到思科云，并且 CDO 租户未申领其序列号，则该设备为“暂留”。
- **初始调配 (Initial provisioning)** - 用于初始FTD 设置的情景。在此阶段期间，设备会接受 EULA，创建新密码，配置管理 IP 地址，设置 FQDN，设置 DNS 服务器，并选择使用 FDM 在本地管理设备。
- **低接触调配 (Low-touch provisioning)** - 将 FTD 从工厂运送到客户现场（通常是分支机构），现场的员工将 FTD 连接到其网络，然后设备与思科云联系。此时，如果设备的序列号已被“申领”，则设备会被载入 CDO 租户，否则 FTD 会在思科云中“暂留”，直到 CDO 租户申领。
- **序列号载入 (Serial number onboarding)** - 这是使用已配置（安装和设置）的序列号载入 FTD 的过程。

策略优化

当两个或多个访问列表（在同一访问组内）相互重叠时，如何识别情况？

Cisco Defense Orchestrator 网络策略管理 (NPM) 能够识别并提醒用户，如果在规则集中，某个顺序更高的规则正在重影其他规则。用户可以在所有网络策略之间导航，也可以过滤以识别所有影子问题。

Note CDO 仅支持完全镜像的规则。

连接

安全设备连接器已更改 IP 地址，但这未反映在 CDO 中。如何反映更改？

要在 CDO 中获取和更新新的安全设备连接器 (SDC)，您需要使用以下命令重新启动容器：

```
 Stop Docker deamon>#service docker stop
Change IP address
Start Docker deamon >#service docker start
Restart container on the SDC virtual appliance >bash-4.2$ ./cdo/toolkit/toolkit.sh restartSDC
 <tenant-name>
```

如果 CDO 用于管理我的设备（ FTD 或 ）的 IP 地址发生更改，会发生什么情况？ ASA

如果设备的 IP 地址因任何原因发生更改，无论是静态 IP 地址更改还是 DHCP 导致的 IP 地址更改，您都可以更改 CDO 用于连接到设备的 IP 地址（请参阅）然后重新连接设备（请参阅）。在 CDO 中更改设备的 IP 地址, on page 83将设备批量重新连接到 CDO, on page 88重新连接设备时，系统会要求您输入设备的新 IP 地址，并重新输入身份验证凭证。

将 ASA 连接到 CDO 需要什么网络？

- 已为 ASA 启用并启用 ASDM 映像。
- 对 52.25.109.29、52.34.234.2、52.36.70.147 的公共接口访问
- ASA 的 HTTPS 端口必须设置为 443 或 1024 或更高的值。例如，不能将其设置为端口 636。
- 如果管理的 ASA 也配置为接受 AnyConnect VPN 客户端连接，则必须将 ASA HTTPS 服务器端口更改为 1024 或更高的值。

使用 CLI 完成 Secure Firewall Threat Defense 设备初始配置

连接到设备的 CLI 以执行初始设置，包括使用安装向导设置管理 IP 地址、网关和其他基本网络设置。确保所有 DNS 和防火墙端口均可访问以进行通信。

专用管理接口是一种具有自己的网络设置的特殊接口。如果您不想使用管理接口，可以使用 CLI 配置数据接口。

Before you begin

此程序适用于以下场景：

- Firepower 1000、 Firepower 2100、 Secure Firewall 3100和 ISA 3000 型号。
- 此配置非常适合使用 CLI 注册密钥自行激活的设备。

Note 请 **勿** 对使用低接触调配进行自行激活的设备使用此配置程序。

Procedure

步骤 1 连接到设备的 CLI，无论从控制台端口还是使用 SSH 至管理接口。如果您打算更改网络设置，我们建议使用控制台端口，以免断开连接。

步骤 2 使用用户名 **admin** 和密码 **Admin123** 登录。

Note 如果密码已更改，但您不知道，则必须重新映像设备以将密码重置为默认值。

步骤 3 第一次登录设备时，系统会提示您接受《最终用户许可协议》(EULA)和 则会提示您更改管理员密码。然后，系统将显示 CLI 设置脚本。

Note 除非清除配置，否则无法重复 CLI 安装向导（例如，通过重新建立映像）。但是，可以稍后在 CLI 中使用 **configure network** 命令更改所有这些设置。请参阅 威胁防御命令参考。

默认值或以前输入的值会显示在括号中。要接受之前输入的值，请按 **Enter** 键。

Note 即使您在数据接口上启用FTD 访问，也使用管理接口设置。例如，通过数据接口在背板上路由的管理流量将使用管理接口 DNS 服务器解析 FQDN，而非使用数据接口 DNS 服务器。

请参阅以下准则：

- **通过 DHCP 或手动配置 IPv4**？-如果想要使用数据接口而非管理接口进行 FTD 访问，请选择 **手动**。虽然您不打算使用管理接口，但必须设置 IP 地址，例如专用地址。如果管理接口设置为 DHCP，则无法配置数据接口用于管理，因为默认路由（必须是 **data-interfaces**，请参阅下一个要点）可能会被接收自 DHCP 服务器的路由覆盖。
- **输入管理接口的 IPv4 默认网关**-如果想要使用数据接口而非管理接口进行 FTD 访问，请将网关设置为 **data-interfaces**。此设置将在背板上转发管理流量，因此可路由通过 FMC 访问数据接口。
- **如果您的网络信息已更改，需要重新连接** - 如果您已建立 SSH 连接，但在初始设置时更改了 IP 地址，连接将断开。使用新 IP 地址和密码重新进行连接。控制台连接不会受影响。

- **在本地管理设备？**-输入 **是** 以配置由 云交付的防火墙管理中心 或 Firepower 设备管理器管理的设备。

  在本地管理设备？-输入 **否** 以配置设备进行 本地管理中心管理。

- **配置防火墙模式？**-建议您在初始配置时设置防火墙模式。在初始设置后更改防火墙模式将会清除正在运行的配置。请注意，只有路由防火墙模式支持数据接口 FTD 访问。

步骤 4 (Optional) 配置用于 FMC 访问的数据接口。

configure network management-data-interface

然后，系统会提示您为数据接口配置基本网络设置。

Note 使用此命令时，应使用控制台端口。如果使用 SSH 访问管理接口，连接可能会断开，您必须重新连接到控制台端口。有关 SSH 用法的详细信息，请参阅下文。

请参阅以下有关使用此命令的详细信息。有关详细信息，请参阅 关于数据接口, on page 751 。

- 如果您要使用数据接口进行管理，则原始管理接口无法使用 DHCP。如果在初始设置期间没有手动设置 IP 地址，则可以使用 **configure network {ipv4 | ipv6} manual** 命令立即设置它。如果您尚未将管理接口网关设置为 **data-interfaces**，此命令将立即设置它。
- 当您通过 思科防御协调器 为 威胁防御 管理载入设备时，思科防御协调器 会发现并维护接口配置，包括以下设置：接口名称和 IP 地址、网关静态路由、DNS 服务器和 DDNS 服务器。有关 DNS 服务器配置的详细信息，请参阅下文。您可以稍后对访问接口配置进行更改，但要确保更改不会阻止设备或 思科防御协调器 重新建立管理连接。如果管理连接中断，设备将包含 **configure policy rollback** 命令以恢复以前的部署。
- 此命令设置数据接口 DNS 服务器。使用设置脚本（或使用 **configure network dns servers** 命令）设置的管理 DNS 服务器用于管理流量。数据 DNS 服务器用于 DDNS（如果已配置）或适用于此接口的安全策略。

  此外，仅当在初始注册时发现 DNS 服务器， 才会保留本地 DNS 服务器。例如，如果您使用管理接口注册了设备，但随后使用 **configure network management-data-interface** 命令配置数据接口，则必须在 CDO中手动配置所有这些设置（包括 DNS 服务器），以便与设备配置匹配。
- 在通过为 威胁防御 管理载入 FTD 后，您可以将该管理接口更改为管理接口或另一数据接口。
- 您在安装向导中设置的 FQDN 将用于此接口。
- 您可以通过命令清除整个设备配置；在恢复场景中可使用此选项，但我们不建议您在初始设置或正常操作中使用它。
- 要禁用数据管理，请输入 **configure network management-data-interface disable** 命令。

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
```

```
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

步骤 5 (Optional) 限制在特定网络上通过数据接口访问 思科防御协调器 。

configure network management-data-interface client *ip_address netmask*

默认情况下，允许所有网络。

关于数据接口

您可以使用专用的管理接口或常规数据接口与设备通信。如果想要从外部接口远程管理 FTD，或者您没有单独的管理网络，则在数据接口上进行 访问非常有用。

从数据接口进行 FTD 管理访问具有以下限制：

- 只能在一个物理数据接口上启用管理器访问。不能使用子接口或 EtherChannel。
- 仅路由防火墙模式，使用路由接口。
- 不支持 PPPoE。如果您的 ISP 需要 PPPoE，则必须在 FTD 与 WAN 调制解调器之间放入支持 PPPoE 的路由器。
- 接口只能位于全局 VRF 中。

- 默认不对数据接口启用 SSH，因此必须稍后使用 启用 SSH。由于管理接口网关将更改为数据接口，因此您也无法启动从远程网络到管理接口的 SSH 会话，除非您使用 **configure network static-routes** 命令为管理接口添加静态路由。

CDO 如何处理个人信息

要了解 Cisco Defense Orchestrator 如何处理您的个人身份信息，请参阅《思科防御协调器隐私数据表》。

联系思科威胁防御支持

本章涵盖以下部分：

导出工作流程

我们强烈建议在提交支持请求之前导出遇到问题的设备的工作流程。此附加信息可帮助支持团队快速识别并纠正任何故障排除工作。

使用以下程序导出工作流程：

过程

步骤 1 在导航栏中，点击**设备和服务 (Devices & Service)**。

步骤 2 点击 **设备** 选项卡，找到您的设备。

步骤 3 点击相应的设备类型选项卡，然后选择需要进行故障排除的设备。

使用过滤器或搜索栏查找需要进行故障排除的设备。选择设备以便将其突出显示。

步骤 4 在设备操作窗格中，选择工作流程。

步骤 5 点击页面右上角、事件表上方的导出按钮。该文件在本地自动保存为 .json 文件。将此附加到您使用 TAC 打开的任何邮件或故障单。

通过 TAC 打开提交支持请求

使用 30 天试用版或许可 CDO 账户的客户可以向思科技术支持中心 (TAC) 提交支持请求。

- CDO 客户如何通过 TAC 提交支持请求。
- CDO 试用客户如何向 TAC 提交支持请求。CDO 试用客户如何向 TAC 提交支持请求，第 754 页

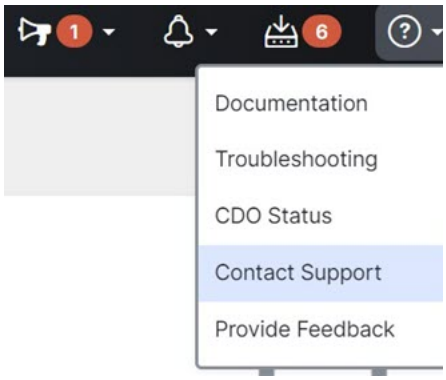
CDO 客户如何通过 TAC 提交支持请求

本节介绍使用许可 CDO 租户的客户如何向思科技术支持中心 (TAC) 提交支持请求。

Procedure

步骤 1 登录 CDO。

步骤 2 点击租户名称旁边的帮助按钮，然后选择**联系支持 (Contact Support)**。



步骤 3 点击**支持请求管理器 (Support Case Manager)**。

步骤 4 点击**打开新案例 (Open New Case)** 按钮。

步骤 5 点击**创建支持案例 (Open Case)**。

步骤 6 选择**产品和服务 (Products and Services)**，然后点击**提交支持案例 (Open Case)**。

步骤 7 选择**请求类型 (Request Type)**。

步骤 8 展开**按服务协议查找产品 (Find Product by Service Agreement)** 行。

步骤 9 填写所有字段。许多字段是显而易见的。这是一些额外信息：

- **产品名称 (PID) (Product Name [PID])** - 如果您没有此编号，请参阅思科防御协调器产品手册。
- **产品说明 (Product Description)** - 这是 PID 的说明。
- **站点名称 (Site Name)** - 输入站点名称。如果您是为某个客户创建案例的思科合作伙伴，请输入该客户的姓名。
- **服务合同 (Service Contract)** - 输入服务合同号。
  - **重要提示：**为了使您的案例与您的 Cisco.com 账户相关联，您需要将您的合同编号与您的 Cisco.com 配置文件相关联。使用此程序将您的合同编号关联到您的 Cisco.com 配置文件。
    a. 打开至思科配置文件管理器 (Cisco Profile Manager)。
    b. 点击**访问管理 (Access Management)** 选项卡。
    c. 点击**添加访问 (Add Access)**。
    d. 选择 **TAC 和 RMA 支持请求提交、软件下载、支持工具和 Cisco.com** 上的授权内容，点击**跳转 (Go)**。

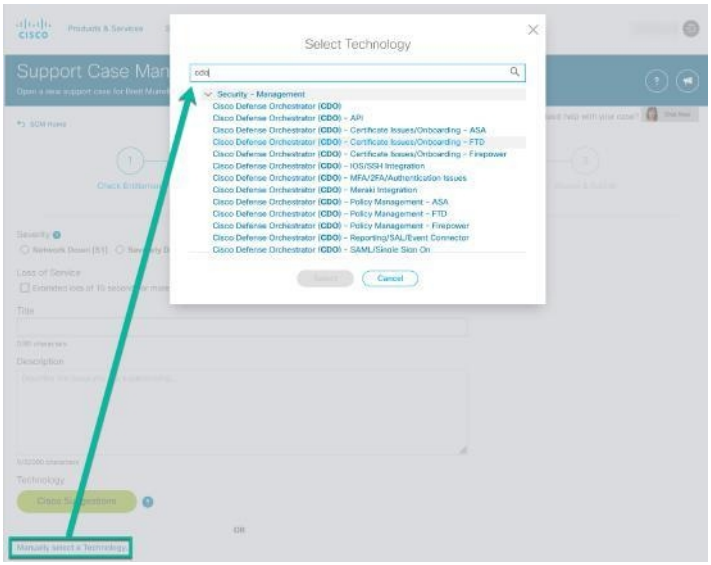
e. 在提供的空白处输入服务合同编号，然后点击**提交 (Submit)**。您将通过邮件收到服务合同关联已完成的通知。完成服务合同关联最多可能需要 6 小时。

Important 重要提示：如果您无法访问以下任何链接，请联系您的思科授权合作伙伴或经销商、您的思科客户代表或您公司中负责管理思科服务协议信息的人员。

步骤 10 点击**下一步**。

步骤 11 在**描述问题 (Describe Problem)** 屏幕中，向下滚动到**手动选择技术 (Manually select a Technology)**，点击该技术，然后在搜索字段中键入 **CDO**。

步骤 12 选择最符合您的请求的类别，然后点击**选择 (Select)**。



步骤 13 完成服务请求的其余部分，然后点击**提交 (Submit)**。

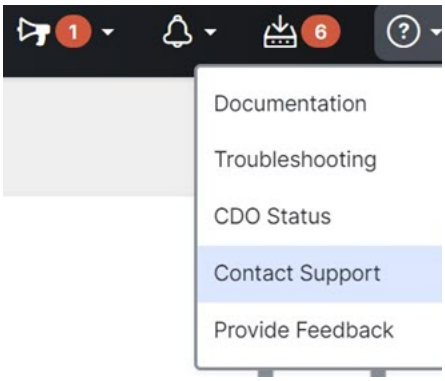
CDO 试用客户如何向 TAC 提交支持请求

本节介绍使用 CDO 租户免费试用的客户如何向思科技术支持中心 (TAC) 提交支持请求。

过程

步骤 1 登录 CDO。

步骤 2 点击租户和账户名称旁边的帮助按钮，然后选择**联系支持 (Contact Support)**。



步骤 3 在下方输入问题或请求字段中，指定您面临的问题或请求，然后点击提交。

您的请求以及技术信息将发送给支持团队，技术支持工程师将回复您的查询。

CDO 服务状态页面

CDO 维护着一个面向客户的服务状态页面，该页面显示 CDO 服务是否已启动以及它可能遇到的任何服务中断。您可以使用每日、每周或每月图表查看正常运行时间信息。

您可以通过点击 CDO 中任何页面上的帮助菜单中的 CDO 状态来访问 CDO 状态页面。

在状态页面上，您可以点击订用更新，以便在 CDO 服务关闭时收到通知。

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。