配置 AWS 设备

本章涵盖以下部分：

更新 AWS VPC 连接凭证

如果创建新的访问密钥和秘密访问密钥以连接到 AWS VPC，则必须在 CDO 中更新连接凭证。在 AWS 控制台中更新凭证，然后使用以下程序从 CDO 控制台更新凭证。请参阅 管理 *IAM* 用户的访问密钥 (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html) 或 创建、禁用和删除 *AWS* 账户根用户的访问密钥 (https://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html）了解更多信息。

您**无法**从 CDO 更改访问密钥或秘密访问密钥；您必须从 AWS 控制台或 AWS CLI 控制台来手动管理连接凭证。

Note 如果您的 CDO 租户中有多个 AWS VPC，则必须一次更新一台设备的凭证。

步骤 1 在导航栏中，点击**清单 (Inventory)**。

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

步骤 3 选择要更新其连接凭证的 AWS VPC。

您可以使用过滤器和搜索功能来查找所需的设备。

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

步骤 5 输入要用于连接到 AWS VPC 的新**访问密钥**和**秘密访问密钥**。

步骤 6 点击**更新**。

Note 如果 CDO 无法同步设备，CDO 中的连接状态可能会显示“无效凭证”(Invalid Credentials)。如果是这种情况，您可能尝试使用无效的用户名和密码组合。请参阅 对无效凭证进行故障排除

相关信息

- 载入 AWS VPC

使用 AWS 传输网关监控 AWS VPC 隧道

Amazon Web Service (AWS) 传输网关充当云路由器，通过中央集线器将企业虚拟私有云 (VPC) 连接到 AWS VPC，从而简化对等关系。

Cisco Defense Orchestrator (CDO) 允许您使用 AWS 传输网关监控已注册的 AWS VPC 的连接状态。

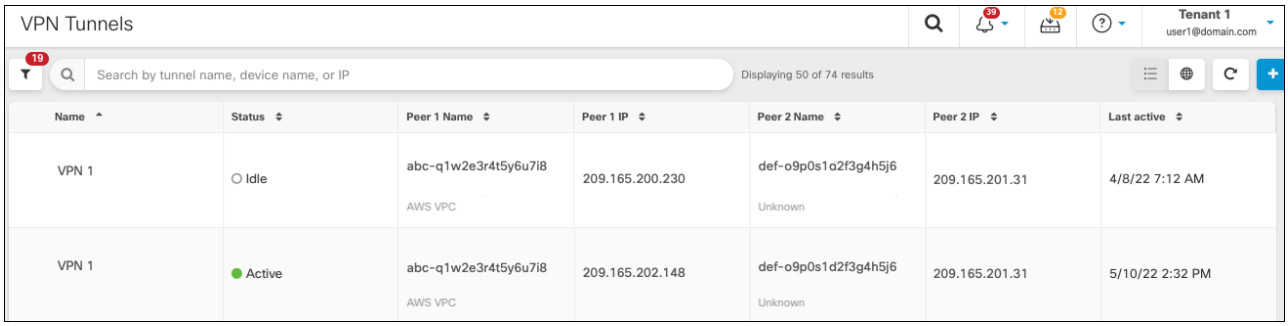
Note 您无需在 CDO 中载入安全防火墙云原生 (SFCN) VPC，即可使用 AWS 传输网关进行监控。

步骤 1 在 CDO 菜单栏中，选择 VPN > Site-to-Site VPN。

步骤 2 “VPN 隧道”(VPN Tunnels) 页面显示您的 CDO 租户管理的所有网络隧道的连接状态。VPN 隧道的连接状态可以是活动或空闲。搜索和过滤器站点间 VPN 隧道, on page 3

步骤 3 选择一个 VPC，然后在操作下点击检查连接以触发对隧道的实时连接检查，并确定隧道当前处于活动状态还是空闲状态。搜索和过滤器站点间 VPN 隧道, on page 3除非您点击按需连接检查链接，否则每十分钟检查一次所有已自行激活设备上可用的隧道。

Note 如果 VPN 隧道的连接断开，CDO 会提示通知。但是，如果链路已备份，则没有通知提示。



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。

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。

查看对 AWS VPC 隧道所做更改的历史记录

要查看对 AWS VPC 隧道所做更改的历史记录，请执行以下操作：

步骤 1 在 CDO 菜单栏中，选择“更改日志”。

步骤 2 在“更改日志”页面上，点击过滤器图标并选择按设备过滤选项卡，然后点击 AWS VPC。

步骤 3 选择要查看其历史记录的 AWS VPC，然后点击确定。

相关信息

- 变更日志

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。

- AWS VPC 策略，第 4 页

AWS VPC 策略

Cisco Defense Orchestrator (CDO) 使用户能够在与您的 AWS 账户关联的 Amazon Web 服务 (AWS) 虚拟私有云 (VPC) 中保持安全策略的一致性。您还可以使用 CDO 在多种设备类型之间共享对象。有关详细信息，请参阅以下主题：

CDO 中的 AWS VPC 和安全组

AWS VPC 安全组规则

AWS安全组是一个规则集合，用于管理所有 AWS EC2 实例以及与安全组相关的其他实体的入站和出站网络流量。

与 Amazon Web 服务 (AWS) 控制台类似，CDO 会单独显示每个规则。只要您的 SDC 可以访问互联网，您就可以为以下环境创建和管理 AWS 虚拟私有云 (VPC) 规则：

- 允许信息传入或传出同一 AWS VPC 中的另一个安全组的安全组。
- 允许传入或传出 IPv4 或 IPv6 地址的安全组。

在包含 AWS 安全组的 CDO 中创建规则时，请记住以下限制：

- 对于允许入站流量的规则，来源可以是同一 AWS VPC、IPv4 或 IPv6 CIDR 块或者单个 IPv4 或 IPv6 地址中的一个或多个安全组对象。入站规则只能将一个安全组对象作为目标。

- 对于允许出站流量的规则，目标可以是同一 AWS VPC 中的一个或多个安全组对象、前缀列表 ID、IPv4 或 IPv6 CIDR 块、单个 IPv4 或 IPv6 地址。出站规则只能将**一个**安全组对象作为来源。
- CDO 会将包含多个实体（例如多个端口或子网）的规则转换为单独的规则，然后再将其部署到 AWS VPC。
- 添加或删除规则时，更改会被自动应用于与安全组关联的所有 AWS 实体。
- 一个 AWS 安全组最多只能拥有 60 条入站规则和 60 条出站规则。此限制会对 IPv4 规则和 IPv6 规则分别实施；在 CDO 中创建的任何其他规则均包含在规则总数中。简而言之，载入 CDO 的数量不能超过 60 条规则限制。

Warning 对现有规则所做的任何编辑都将导致已编辑的规则被删除，并使用新的详细信息创建新的规则。这会导致依赖该规则的流量在很短的时间内就被丢弃，直到可以创建新的规则。如果创建全新的规则，则不会发生这种情况。

如果您需要有关可从 AWS 控制台创建的规则类型的更多信息，请参阅 AWS 安全组对象。有关可与 AWS VPC 关联的对象的更多信息，请参阅AWS 安全组和云安全组对象。

相关信息

- 创建安全组规则, on page 5
- 编辑安全组规则, on page 6
- 删除安全组规则, on page 7

创建安全组规则

默认情况下，Amazon Web Services (AWS) 虚拟私有云 (VPC) 会阻止所有网络流量。这意味着所有规则都会自动配置为**允许**流量。您无法编辑此操作。

Note 创建新的安全组规则时，必须将其与安全组关联。

AWS 控制台不支持包含多个源或目标的规则。这意味着，如果部署包含多个实体的单个安全组规则，则 CDO 会将该规则转换为单独的规则，然后再将其部署到 AWS VPC。例如，如果您创建的入站规则允许来自两个端口范围的流量进入一个云安全组对象，则 CDO 会将其转换为两个单独的规则：(1) 允许流量从第一个端口范围进入安全组；(2)以允许从第二个端口范围到安全组的流量。

使用此程序创建安全组规则：

步骤 1 在导航窗格中，点击**设备和服务 (Devices & Services)**。

步骤 2 点击**模板 (Template)** 选项卡。

步骤 3 点击 **AWS** 选项卡，然后选择要编辑其访问控制策略的 AWS VPC 设备模板。

步骤 4 在右侧的管理窗格中，选择**策略 (Policy)**。

步骤 5 点击要向其添加规则的安全组旁边的蓝色加号按钮。

步骤 6 点击**入站 (Inbound)** 或**出站 (Outbound)**。

- **入站**规则 - 源网络可以包含一个或多个 IPv4 地址、IPv6 地址或云安全组对象。目标网络**必须**定义为单个云安全组对象。
- **出站**规则 - 源网络**必须**定义为单个云安全组对象。目的网络可以包含一个或多个 IPv4 地址、IPv6 地址或安全组对象

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 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)** 选项卡并添加或删除网络（包括网络和大洲）。不能将端口或端口范围定义为源。
- **目标 (Destination)** - 点击**目标 (Destination)** 选项卡，然后添加或删除网络（包括网络和大洲）或流量到达的端口。默认值为“任意”。
  - **注：**

    如果未定义网络对象，它将在 AWS 控制台中转换为两个规则：一个用于 IPv4 (0.0.0.0/0)，另一个用于 IPv6 (::0/0)

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。

Caution 如果部署失败，CDO 会尝试将 AWS VPC 的状态恢复到您尝试部署之前的状态。这是在“尽力而为”的基础上完成的。由于 AWS 不维护状态，因此此回滚尝试可能会失败。在这种情况下，您必须登录 AWS 管理控制台并手动将 AWS VPC 恢复为之前的配置，然后 读取、丢弃、检查和部署更改 CDO。

编辑安全组规则

按照以下程序使用 CDO 编辑 AWS VPC 的访问控制规则：

步骤 1 打开 **设备和服务** 页面。

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 **AWS** 选项卡，然后选择要编辑其访问控制策略的 AWS VPC。

步骤 4 在右侧的**管理 (Management)** 窗格中，选择 **策略 (Policy)**。

步骤 5 要编辑现有安全组规则，请选择规则，然后点击操作窗格中的编辑图标 。（也可以在不进入编辑模式的情况下内联执行简单编辑。）有关规则限制和例外情况，请参阅 AWS VPC 安全组规则。

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。

Caution 如果部署失败，CDO 会尝试将 AWS VPC 的状态恢复到您尝试部署之前的状态。这是在“尽力而为”的基础上完成的。由于 AWS 不维护状态，因此此回滚尝试可能会失败。在这种情况下，您必须登录 AWS 管理控制台并手动将 AWS VPC 恢复为之前的配置，然后轮询 AWS VPC 设备配置与 CDO 中的配置之间的更改。

删除安全组规则

步骤 1 打开 **设备和服务** 页面。

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 **AWS** 选项卡，然后选择要编辑其访问控制策略的 AWS VPC。

步骤 4 在右侧的**管理 (Management)** 窗格中，选择 **策略 (Policy)**。

步骤 5 要删除不再需要的安全组规则，请选择该规则，然后点击**操作 (Actions)** 窗格中的删除图标 。

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。

Caution 如果部署失败，CDO 会尝试将 AWS VPC 的状态恢复到您尝试部署之前的状态。这是在“尽力而为”的基础上完成的。由于AWS不会维护“状态”，因此此回滚尝试可能会失败。在这种情况下，您必须登录 AWS 管理控制台并手动将 AWS VPC 恢复为之前的配置，然后轮询 AWS VPC 设备配置与 CDO 中的配置之间的更改。

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。

本节适用于自适应安全设备 (ASA) FDM 管理的设备上的远程访问和站点间 VPN。 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 7 页

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 。

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。

相关信息：

- 监控 AWS 站点间虚拟专用网络

监控 AWS 站点间虚拟专用网络

通过 CDO，您可以监控已载入的 ASA 设备上的现有站点间 VPN 配置。它不允许您修改或删除站点间配置。

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 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：

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 10

查找缺少对等体的 *VPN* 隧道

“缺少 IP 对等体”情况在 ASA 设备上比设备上更可能发生。FDM 管理

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

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。

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。

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, on page 10

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。

步骤 1 在 CDO 导航栏中，点击**库存 (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 解决“检测到冲突”状态。

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 17 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。

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：

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
- 载入 AWS VPC

查看 AWS 站点间 VPN 隧道

AWS 站点间 VPN 通过安全隧道将您的虚拟私有云 (VPC) 连接到您的企业网络。

所有站点间 VPN 配置都在 AWS 管理控制台中进行。载入 VPC 后，CDO 能够显示由 AWS VPC 维护的站点间 VPN 连接，并将其显示在 VPN 隧道页面上，以便您可以将其与所有其他站点间连接一起进行管理。从您的网络到 VPC 的每个 VPN 连接都由两个独立的 VPN 隧道组成。

在 CDO 的“VPN 隧道”(VPN Tunnels) 页面中，您可以查看站点间 VPN 隧道信息，搜索和过滤器站点间 VPN 隧道，以及载入非托管设备。

CDO 每 10 分钟轮询一次 AWS 管理控制台，以查找站点间 VPN 配置的更改。如果 CDO 发现有更改，它会轮询该配置中的更改并将更改存储在其数据库中。然后，CDO 管理员将能够在 CDO 中查看新配置。

Amazon Web 服务 (AWS) 参考资料

AWS 虚拟专用网络文档

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。

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

步骤 1 查看 IPsec 站点间虚拟专用网络隧道信息。查看站点间 VPN 隧道信息, on page 13

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：

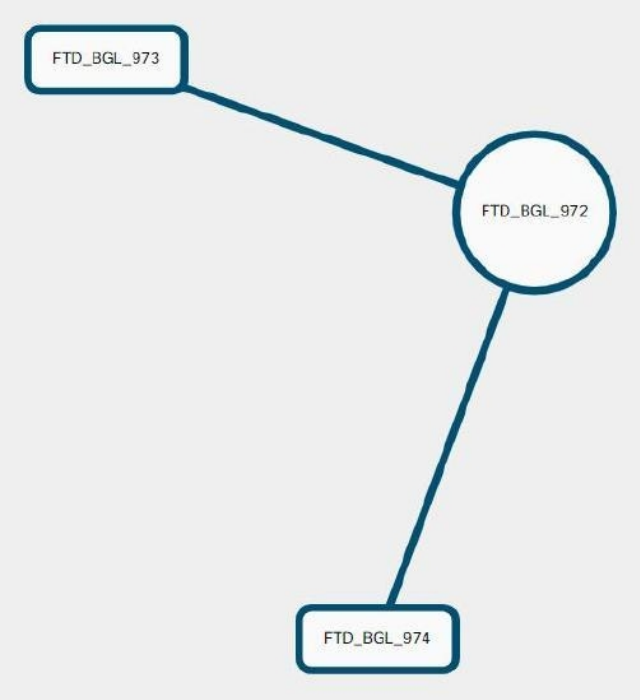
步骤 1 在主导航栏中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

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。



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。

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。

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。

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）创建更改请求标签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 查看通知选项卡以了解“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”(Jobs) 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

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。

SUMMARY STEPS

1. 在屏幕的右上角，点击**部署 (Deploy)** 图标  。
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。
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。
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。
5. （可选）创建更改请求以跟踪更改，而无需离开**具有待处理更改的设备 (Devices with Pending Changes)** 页面。
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。
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。
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。

DETAILED STEPS

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）创建更改请求以跟踪更改，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

将更改部署到设备

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

- 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 17。

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：

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。

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 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。

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：

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。

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 16
- 预览和部署所有设备的配置更改, on page 17

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：

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 AWS 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：

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接口通过 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 27。

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。

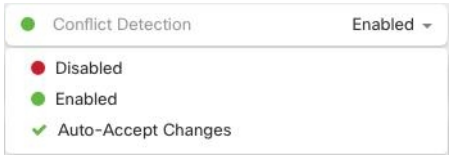
步骤 1 从导航栏中，点击**清单 (Inventory)**。

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 24。

配置自动接受更改

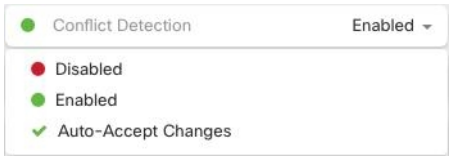
步骤 1 使用具有管理员或超级管理员权限的帐户登录 CDO。

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

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：

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 17
- 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 24 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：

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 24 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 (Default Conflict Detection Interval) 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：

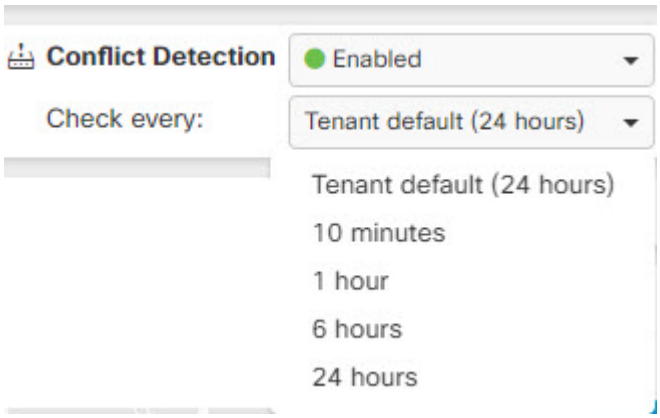
步骤 1 在导航栏中，点击 **设备和服务**。

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：


Conflict Detection
Enabled
Check every:
Tenant default (24 hours)
Tenant default (24 hours)
10 minutes
1 hour
6 hours
24 hours

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。