使用 Cisco Defense Orchestrator 管理 AWS

首次发布日期: 2020 年 12 月 22 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

使用 Cisco Defense Orchestrator 管理 AWS

使用 Cisco Defense Orchestrator 管理 AWS

使用 Cisco Defense Orchestrator 管理 AWS VPC

CDO 为您的 Amazon Web 服务 (AWS) 虚拟私有云 (VPC) 提供简化的管理界面。您可以在管理其他设备的同一界面中管理 AWS VPC 及其组件。

使用 CDO 执行这些任务：

- 载入 AWS VPC, on page 97
- 查看 VPC 详细信息
- 使用安全组
- 与其他受管设备共享 AWS 对象
- 监控站点间 VPN 连接
- 监控 AWS 设备的更改
- 查看 AWS 站点间 VPN 隧道

这些是 CDO 期望在未来支持的常见 AWS 功能：

- 显示负载均衡器（弹性负载均衡器、网络负载均衡器和应用负载均衡器）与安全组的关系。
- 显示自动扩展组与安全组的关系。

您无法使用 CDO 管理安全组的以下方面：

- 创建安全组。
- 将安全组链接到实例。
- 将安全组分配给负载均衡器。

使用 Cisco Defense Orchestrator 管理 AWS

- VPC 对等互连

载入 AWS VPC

首先使用 CDO 的载入向导来载入 AWS VPC。有关更多信息，请参阅载入 AWS VPC。

请注意，如果 AWS VPC 包含标签，则在载入设备时，这些标签会被导入到 CDO 中。CDO 将标记表示为**标签**。与安全云对象或规则不同，标签不会自动同步到 AWS VPC。有关详细信息，请参阅标签和过滤 。

通过 CDO 控制台处理 AWS VPC 登录凭证和权限。如果没有正确的凭证或权限，CDO 将无法与 AWS VPC 通信。有关更多信息，请参阅 更新 AWS VPC 连接凭证, on page 101 和更改 IAM 用户的权限。

查看 AWS VPC 详细信息

在载入 AWS VPC 后，您可以查看 AWS VPC 的 ID、区域、安全组以及分配给这些安全组的规则和对象。

使用安全组

安全组是管理与安全组关联的所有 AWS 实例和其他实体的入站和出站网络流量的规则集合。在将 AWS VPC 载入 CDO 时，安全组将作为安全组对象存储在 CDO 中。

使用 CDO，您可以执行以下任务：

- 创建安全组规则。
- 检查配置更改、编辑安全组规则和删除安全组规则安全组中的规则。

目前，您无法在 VPC 中创建新的安全组。

有关详细信息，请参阅这些主题：

- CDO 中的 AWS VPC 和安全组
- 管理 AWS VPC 安全组规则
- 在 AWS 和其他受管设备之间共享对象

在 AWS 和其他受管设备之间共享对象

CDO 支持在规则中使用对象。对象是值的容器。例如，您可以拥有一个包含资源 IP 地址的网络对象，并为其指定一个有意义的名称。然后，您可以在访问规则中使用该对象作为规则的源或目标的一部分，而不是使用资源的文字 IP 地址。您可以将此对象重用不同的规则。如果更改对象的值一次，则使用该对象的任何规则都将开始使用新值。

在载入 AWS VPC 后，CDO 会将 AWS 概念转换为安全组对象以及现有安全组规则中的网络对象和服务对象。

网络对象和服务对象（有时称为端口对象）可以在 AWS VPC 和您使用 CDO 管理的其他设备之间共享。安全组对象对于 AWS 是唯一的。

使用 Cisco Defense Orchestrator 管理 AWS

有关详细信息，请参阅在 AWS 和其他受管设备之间共享对象。

监控站点间 VPN 连接

AWS 站点间 VPN 通过安全隧道将您的 AWS VPC 连接到您的企业网络。有关详细信息，请参阅查看 AWS 站点间 VPN 隧道。

监控对 AWS VPC 和 AWS 安全组的更改

更改日志

变更日志会持续捕获在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。

更改请求管理

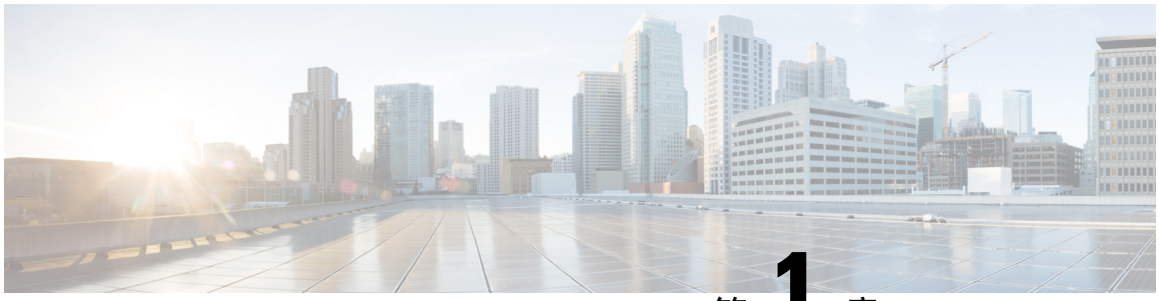
更改请求管理允许您将在第三方故障单系统中打开的变更请求及其业务理由与变更日志中的事件相关联。使用更改请求管理在CDO中创建更改请求，使用唯一名称进行标识，输入更改说明，并将更改请求与更改日志事件相关联。您可以稍后在更改日志中搜索更改请求名称。

支持常见管理任务

CDO 支持 AWS 安全组的以下常见管理任务：

- 批量部署设备配置, on page 119
- 读取所有设备配置, on page 116
- 设备上的带外更改
- 冲突检测
- 解决配置冲突

使用 Cisco Defense Orchestrator 管理 AWS



第 1 章

Cisco Defense Orchestrator 基础知识

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

- AWS 安全组和云安全组对象, on page 94
- 服务对象, on page 95

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

- 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

您将需要基本授权许可证和特定于要管理的设备的许可证。CDO

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 5 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 7 页和在您自己的虚拟机上部署安全设备连接器，第 11 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 145 页
- 更新您的安全设备连接器，第 20 页
- 删除安全设备连接器，第 18 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。

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 21 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 11 页。

开始之前

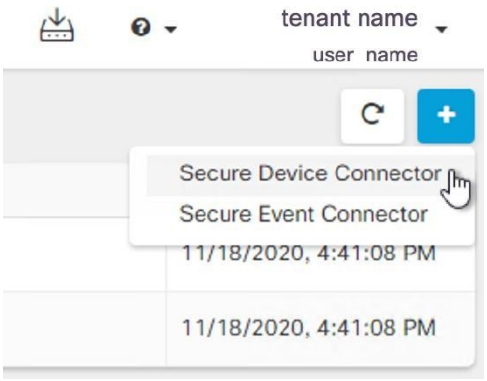
在部署 SDC 之前，请查看以下前提条件：

- 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。
- 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。

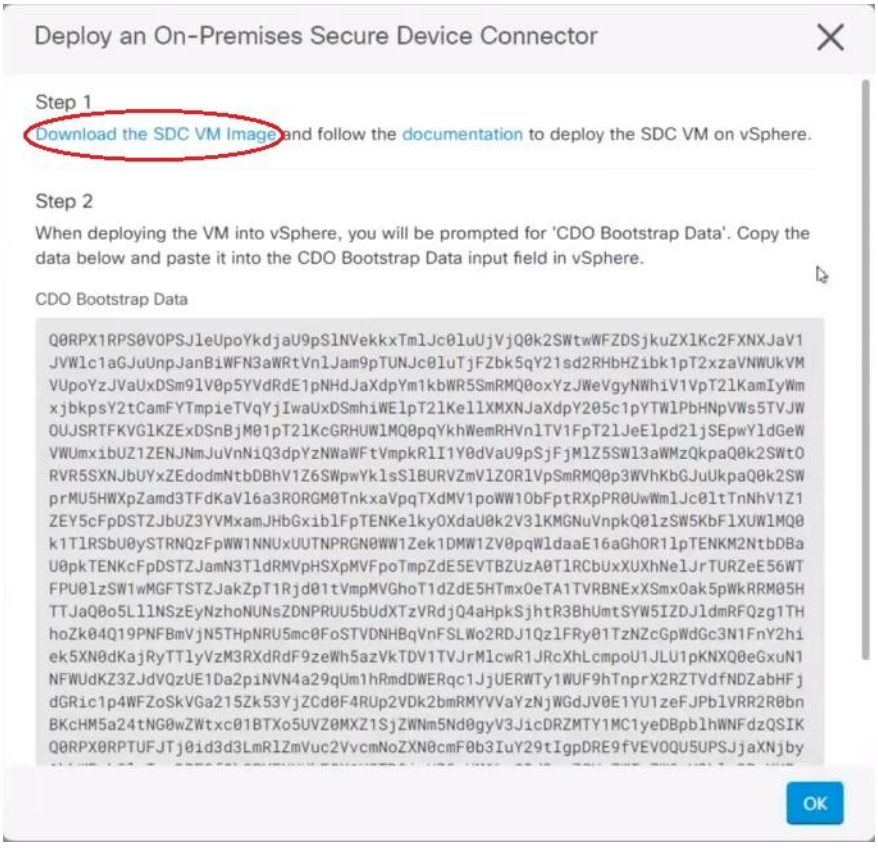
步骤 1 登录到要为其创建 SDC 的 CDO 租户。

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。

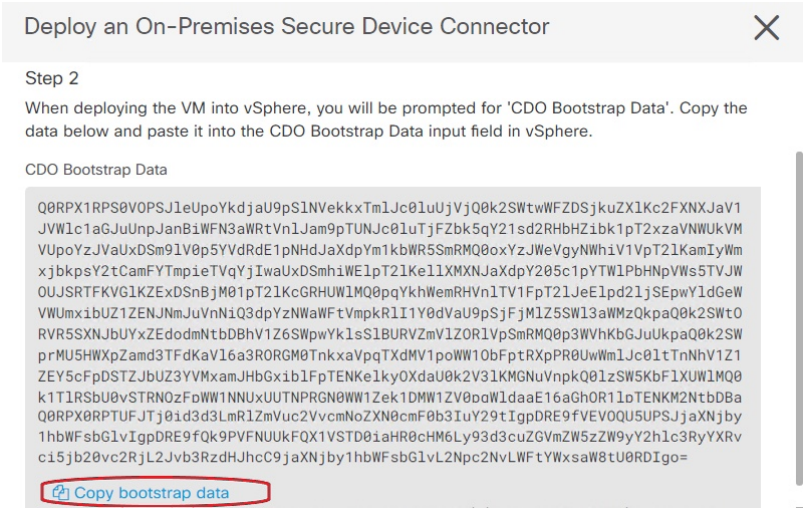
步骤 22　在提示符后，键入 `sudo sdc-onboard bootstrap`。

```
[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 145 页
- 排除设备与 SDC 的连接故障，第 146 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 21 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 7 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。

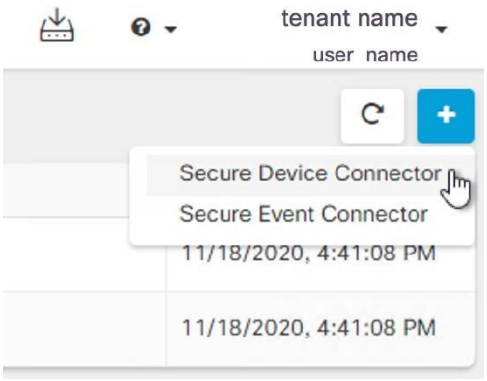
- ESXi 5.1 虚拟机监控程序。
- Cent OS 7 访客操作系统。
- 仅具有 SDC 的 VM 的系统要求：
  - VMware ESXi 主机需要 2 个 CPU。
  - VMware ESXi 主机至少需要 2 GB 内存。
  - VMware ESXi 需要 64 GB 磁盘空间来支持虚拟机，具体取决于您的调配选择。此值假定您对分区使用逻辑卷管理 (LVM)，因此您可以根据需要扩展所需的磁盘空间。
- 更新 VM 上的 CPU 和内存后，打开 VM 并确保“安全连接器”页面指示 SDC 处于“活动”状态。
- 执行此过程的用户应该能够轻松地在 Linux 环境中使用 vi 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。

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。

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 的专用子网连接了 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。

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。

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 11 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。

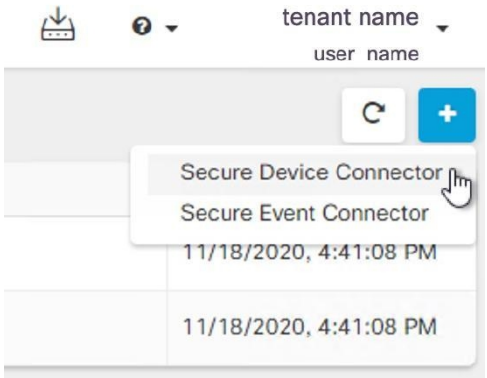
要从租户中删除 SDC，请遵循以下程序：

步骤 1 删除连接到您要删除的 SDC 的任何设备。您可以采用以下两种方式之一：

- 将某些设备移至不同的 SDC 或完全移出 SDC。有关详细信息，请参阅下文：
  - 更新 AWS VPC 连接凭证, on page 101
- 从 CDO 中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 21 页您可以使用以下程序将受管 ASA 从一个 SDC 移至另一个 SDC：

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：

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

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。

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：

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

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 30 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 30 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 30 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 56 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 30 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 56 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 56 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

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 46。

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 49

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：

- 云设备支持详情，第 33 页
- 浏览器支持，第 33 页

云设备支持详情

下表介绍了基于云的设备的软件和设备类型支持。阅读附属链接，了解有关下表中设备类型的载入和功能的详细信息：

设备类型	注意
Amazon Web 服务 VPC	AWS VPC 通过 AWS 控制台接收更新。有关平台和可用服务的详细信息，请参阅 AWS 文档。 您必须先在 AWS 控制台中启动 AWS VPC，然后再将其载入 CDO。
Google 云平台	Google 云平台 (GCP) 会通过 GCP 控制台接收任何更新。有关平台和可用服务的详细信息，请参阅 Google Cloud 文档。请参阅
Microsoft Azure	Azure 通过 Azure 控制台接收任何更新。有关平台和可用服务的详细信息，请参阅 Azure 文档。

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 *1: 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 *2:* 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 35 页
- 用户管理
- 日志记录设置
- 通知设置，第 38 页

常规设置

在右上角的管理下拉列表中，点击**设置 (Settings)**。

请参阅以下有关常规 CDO 设置的主题：

- 用户设置, on page 35
- 对于我的令牌，请参阅 API 令牌, on page 43
- 有关租户设置，请参阅：
  - 启用更改请求跟踪, on page 35
  - 阻止思科支持人员查看您的租户, on page 36
  - 默认冲突检测间隔, on page 36
  - Web 分析, on page 37
  - 租户 ID, on page 37
  - 租户名称, on page 38

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 43

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：

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：

步骤 1 在右上角的管理下拉列表中，点击**设置 (Settings)**。

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：

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：

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：

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：

步骤 1 在右上角的管理下拉列表中，点击**设置 (Settings)**。

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。

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。

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：

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：

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：

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。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CDO 客户如何通过 TAC 提交支持请求，并提供 metadata.xml 文件。

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。

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** - 安全服务交换 订用（可选）
- **client_id** - "**api-client**"
- **jti** - 令牌 ID

令牌管理

生成 API 令牌

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。

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

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：

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。

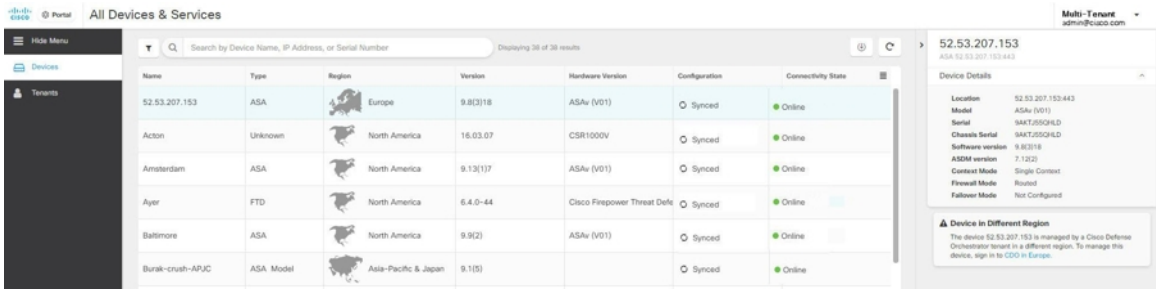
我们建议您从 Web 浏览器清除缓存和 Cookie，以避免可能发生的某些浏览器相关问题。

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。

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

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。

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。

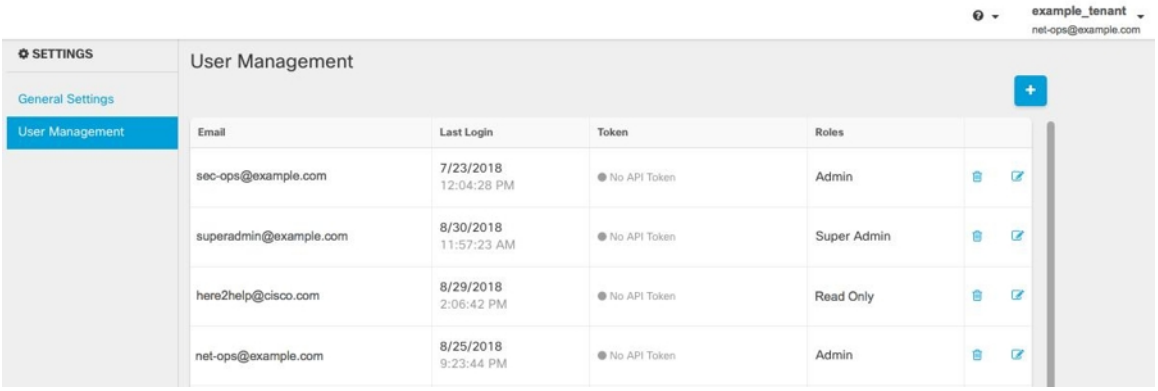
除非您的企业有自己的 IdP，否则思科安全登录是所有 CDO 租户的身份提供程序。本文的其余部分假设您使用思科安全登录作为身份提供程序。

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

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 35 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。

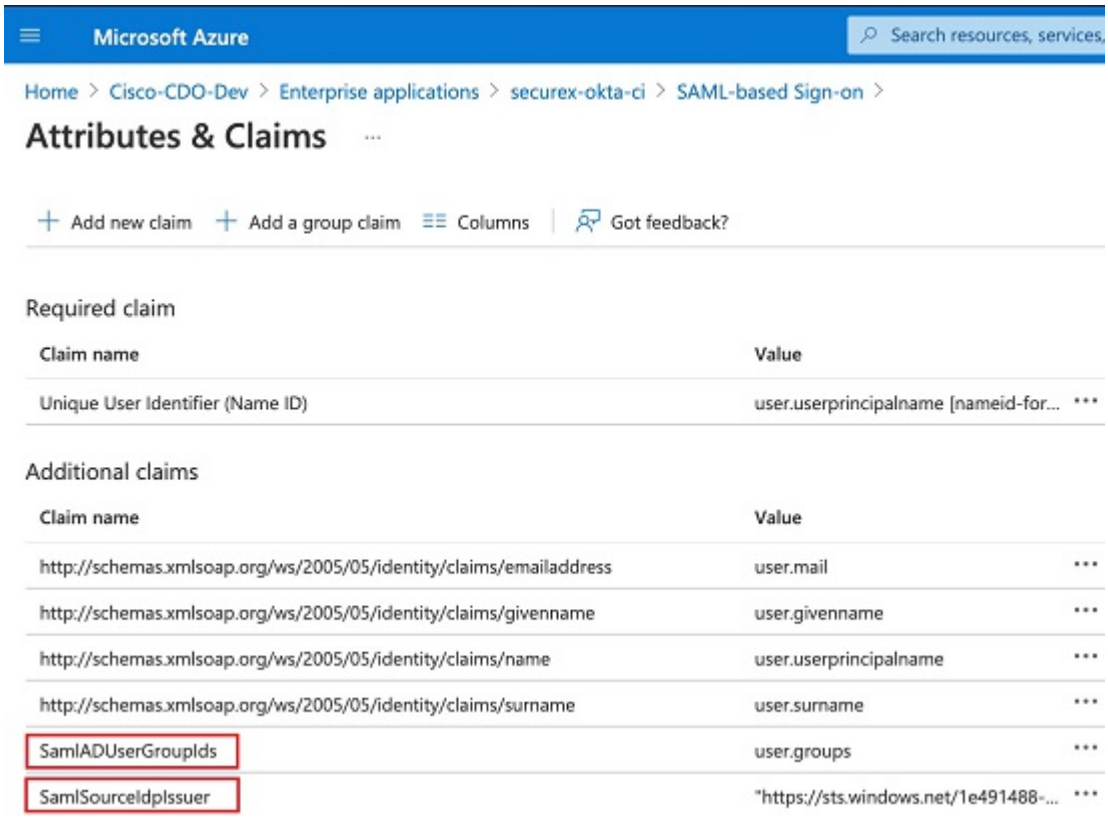
注释 如果用户既是单个用户又是同一租户上的 AD 组的一部分，则单个用户的用户角色将覆盖 AD 组的用户角色。

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：

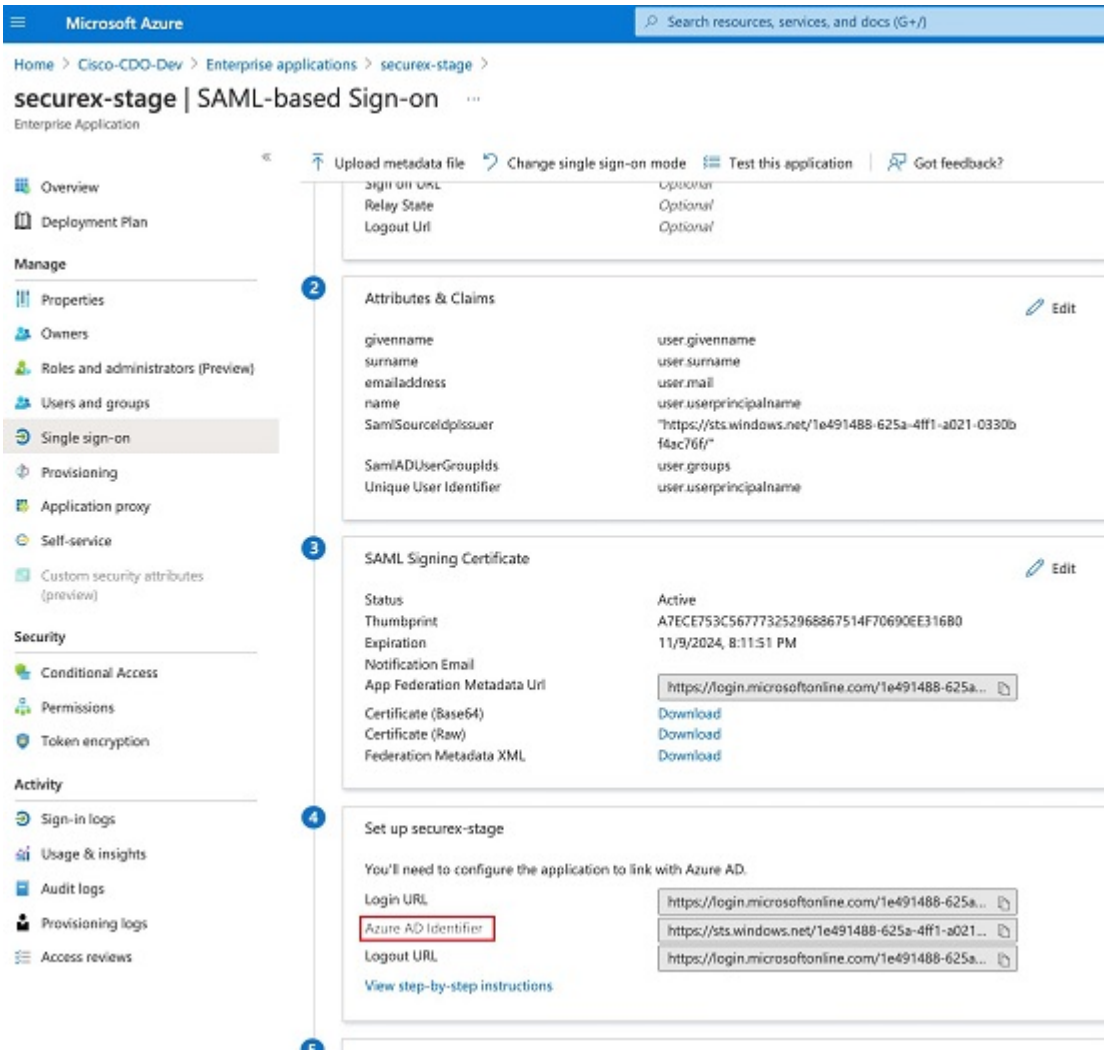
1. 向思科 TAC 提交支持案例，并请求使用以下信息进行自定义 AD IdP 集成：
   https://mycase.cloudapps.cisco.com/case
   - 您的 CDO 租户名称和区域。
   - 定义自定义路由的域（例如：@cisco.com、@myenterprise.com）。
   - XML 格式的证书和联合元数据。
2. 在 AD 中添加以下自定义 SAML 声明。请注意，这些值区分大小写。
   - SamlADUserGroupIds - 此属性描述用户在 AD 上的所有组关联。例如，在 Azure 中选择 + 添加组申领，如下面的屏幕截图所示：

图 *1: 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 2: 找到 *Azure Active Directory* 标识符



添加用于用户管理的 Active Directory 组

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。

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

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，用户可以从 Cisco Secure Sign-On 控制面板打开 CDO。新用户从思科安全登录控制面板打开 CDO, on page 61

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 30 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。

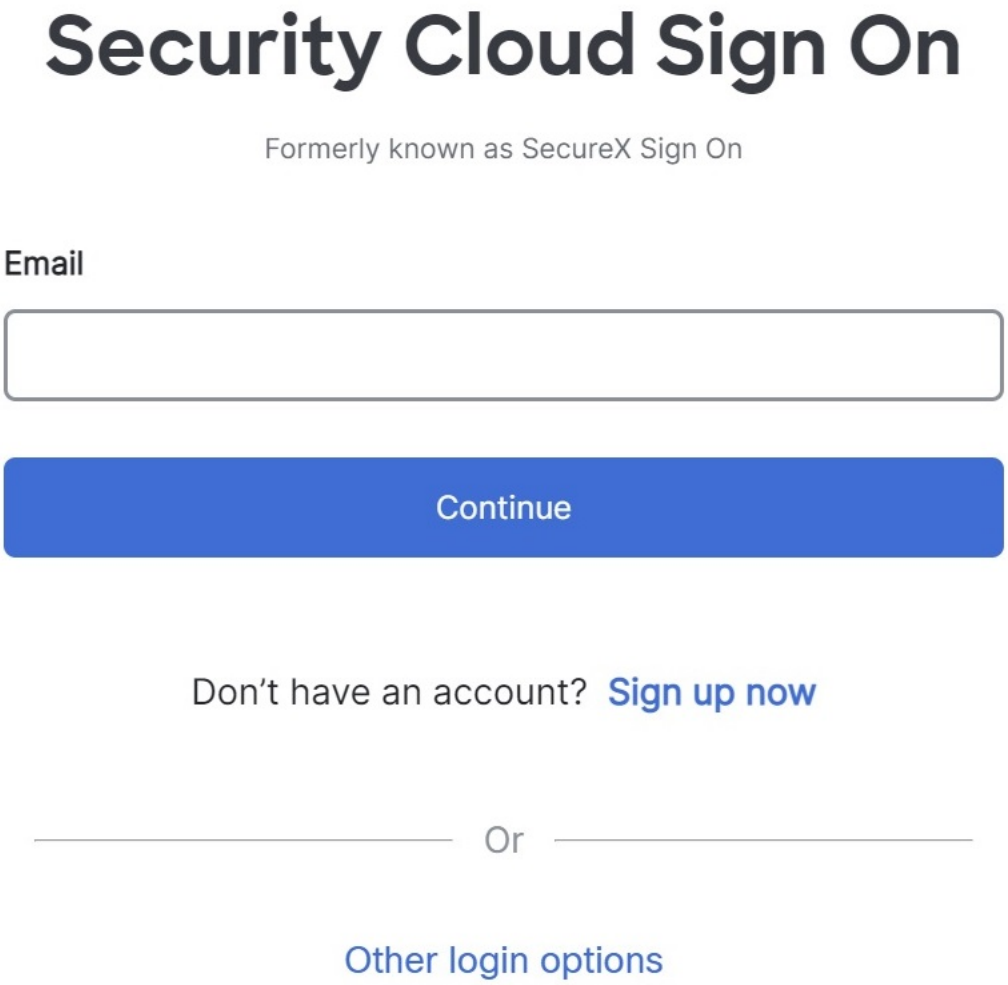
创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证

初始登录工作流程分为四步。您需要完成所有四个步骤。

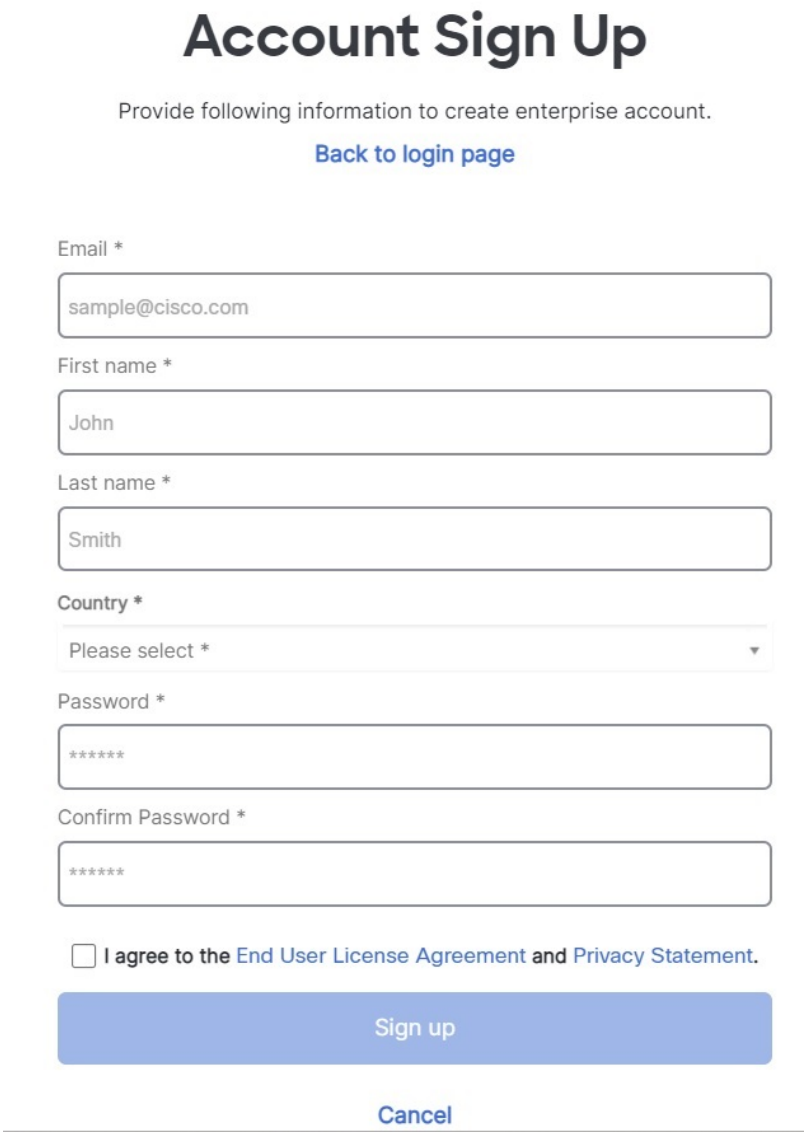
步骤 1 注册新的 **Cisco Security Cloud Sign On** 账户

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项卡。

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：

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 (Settings)**。

步骤 3 点击**用户管理 (User Management)** 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

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 46

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 30。

- 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。用户管理, on page 49

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 Defense Orchestrator 支持。CDO 客户如何通过 TAC 提交支持请求, on page 179

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：

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 30。

创建仅 API 用户

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 43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：

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

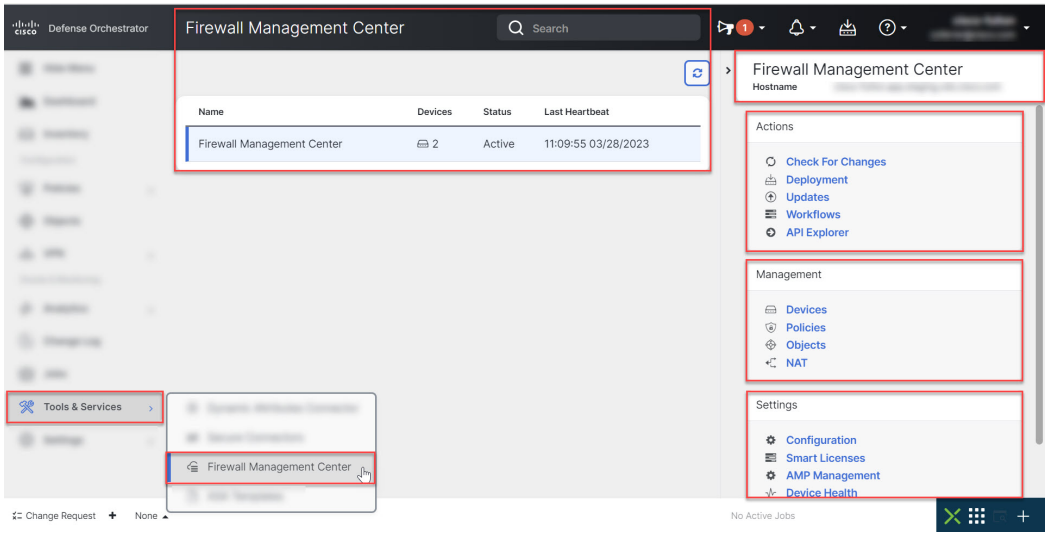
要删除用户记录中定义的角色，请参阅以下程序：

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 (Settings)**。
步骤 3 点击**用户管理 (User Management)** 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**。
- 云交付的防火墙管理中心上部署的Secure Firewall Threat Defense设备数量。

- CDO与云交付的防火墙管理中心页面之间的连接状态。
- 云交付的防火墙管理中心的最后一次心跳。这表示上次将云交付的防火墙管理中心本身的状态及其管理的设备数量与此页面上的表同步。
- 所选云交付的防火墙管理中心的主机名。

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

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云交付的防火墙管理中心同步时可用的信息进行更新。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 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。

  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 (Objects)** > **其他 FTD 对象 (Other FTD Objects)**。
- 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 (Dashboard)** > **快速操作 (Quick Actions)**。

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

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 77 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 80 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 78 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：

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 77
- 将设备批量重新连接到 CDO, on page 76

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。

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。

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：

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。

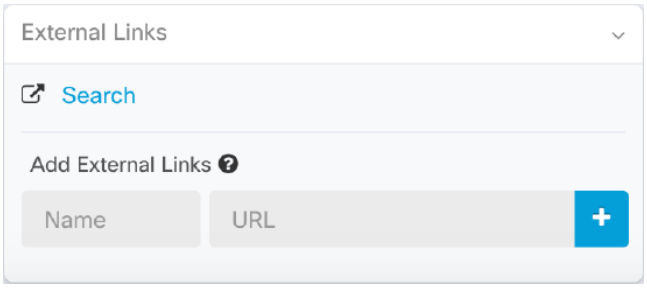
步骤 4 选择所需的设备以便将其突出显示。

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（）。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}
```

。

相关信息：

- 编写设备说明, on page 77
- 导出设备和服务列表, on page 72

从您的设备创建外部链路

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。
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。

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

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

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

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。

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 136。

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。

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：

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。

AWS VPC 中的标签和标签

当您将 AWS VPC 载入 CDO 时，CDO 会在配置过程中读取所有 AWS VPC 标签。也就是说，它们从 AWS 复制并存储在 CDO 的数据库中。这些标签表示为 CDO 标签，可以在**设备和服务 (Devices & Services)** 页面上查看，就像任何其他设备类型上的标签一样。如果您从 CDO 删除现有标签或创建新标签，这些更改不会同步到 AWS VPC。您必须使用 AWS 控制台手动进行相同的更改。在载入 AWS VPC 后，在 AWS 控制台中创建或修改的 VPC 标签不会存储在 CDO 的配置副本中，也不会作为带外更改被检测出来。

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。

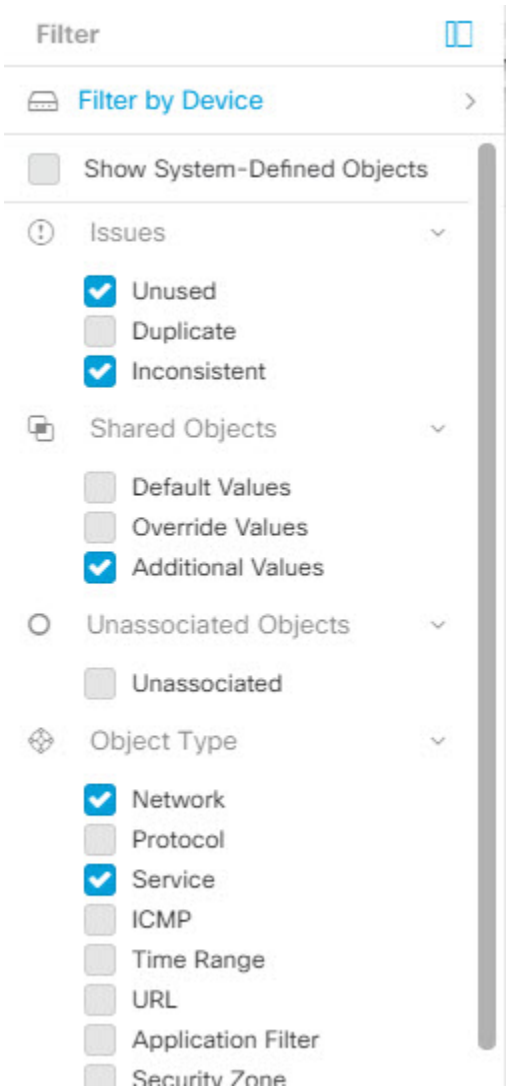
要过滤，请点击设备和服务、策略和对象选项卡的左侧窗格中的 ：

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。

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：

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。

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。

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 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 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

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

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。

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

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**。

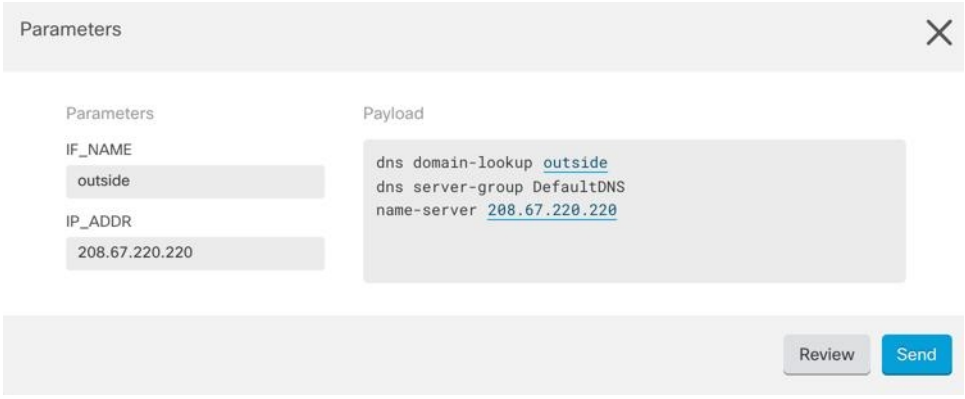
步骤 5 在命令面板中，点击星号。

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！

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 设备。宏并非特定于特定设备。

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。

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。

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 90
- 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 149

对象类型

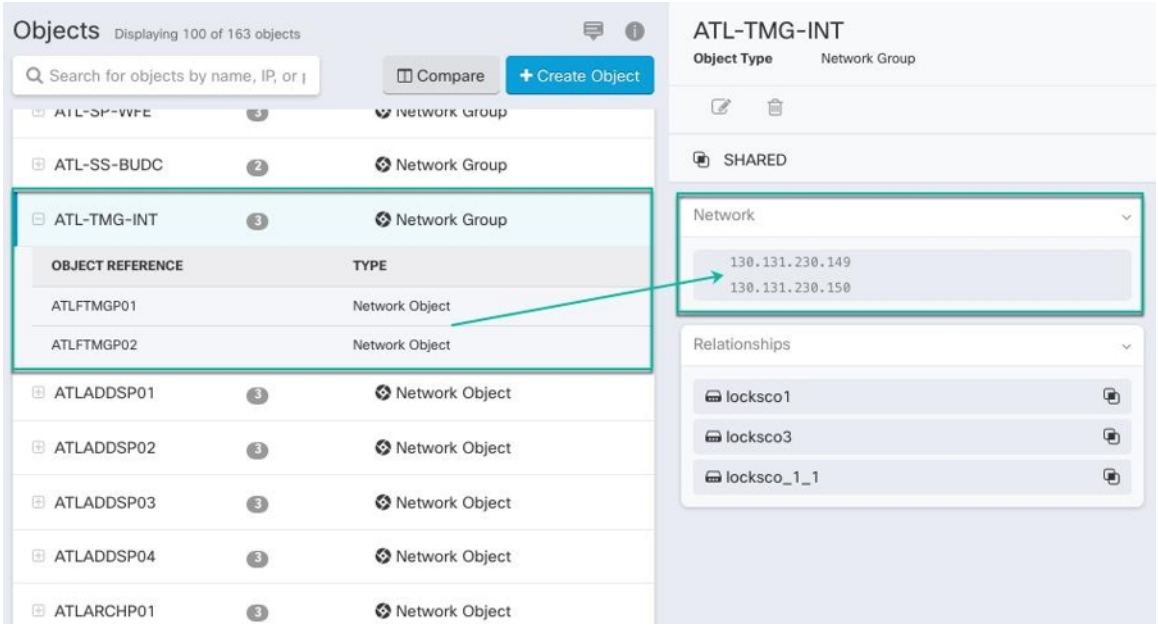
下表介绍您可以为设备创建和使用 CDO 管理的对象。

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。

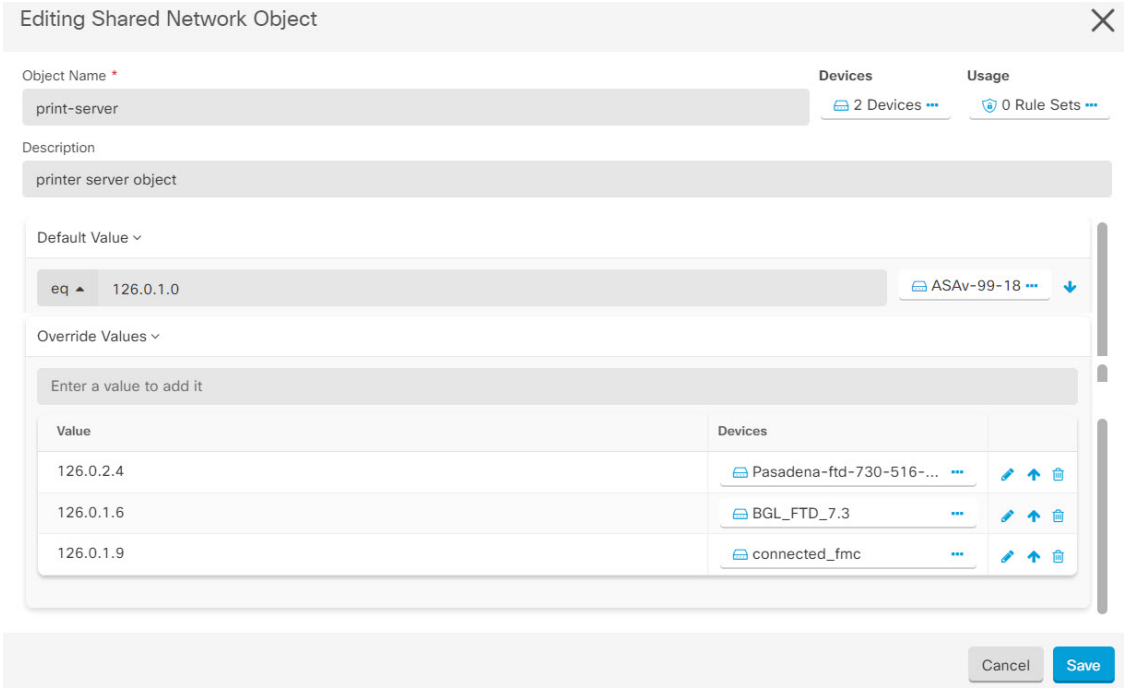


对象覆盖

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。



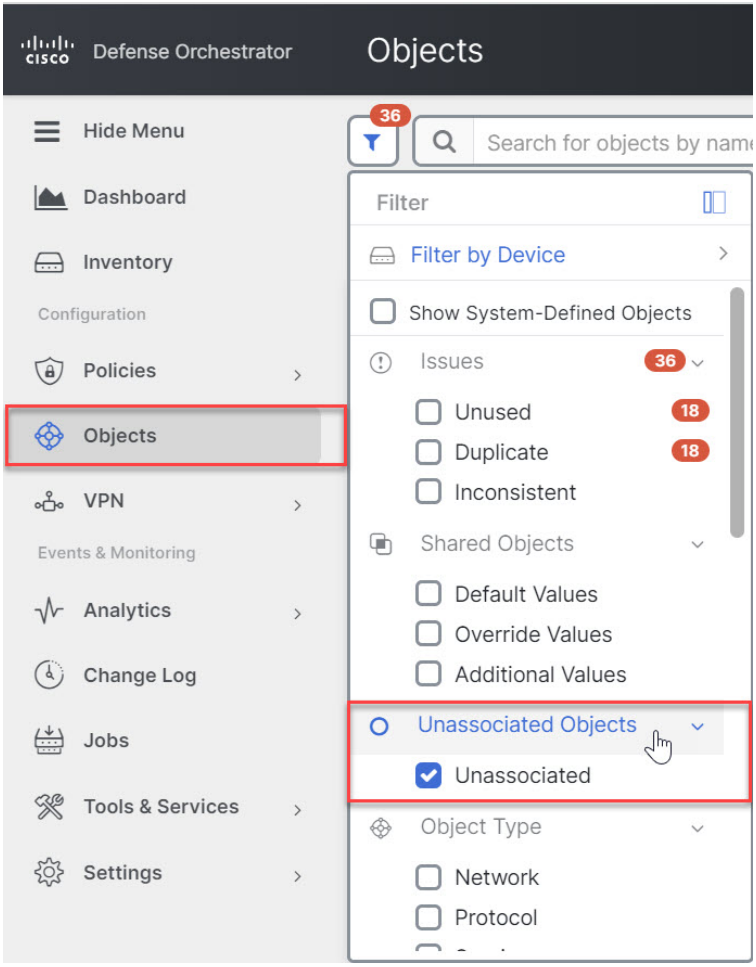
Note 如果存在不一致的对象，您可以将它们合并为一个具有覆盖的共享对象。有关详细信息，请参阅解决不一致的对象问题, on page 155。

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

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 Compare。

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。

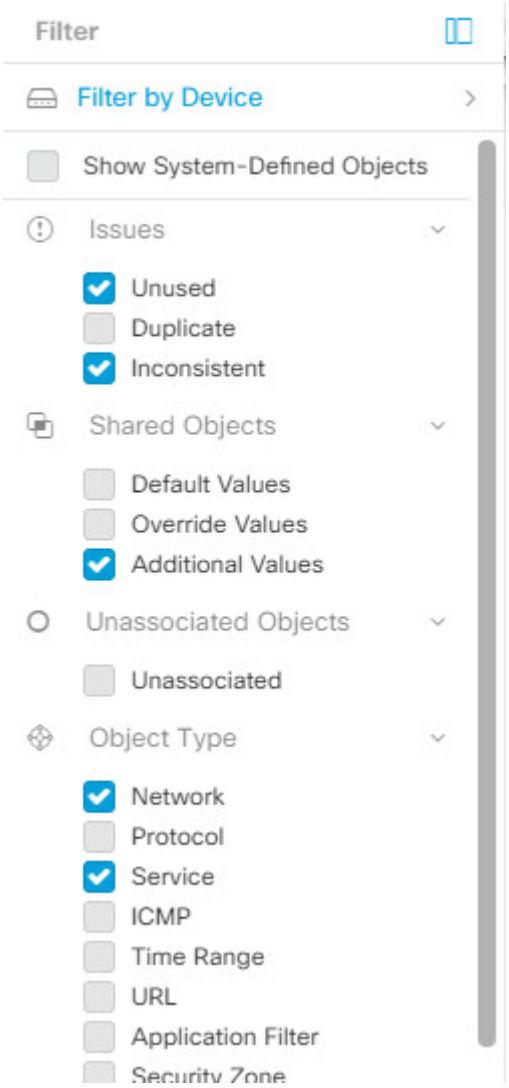
要过滤，请点击设备和服务、策略和对象选项卡的左侧窗格中的 ：

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。

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。

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 154解决重复对象问题, on page 153解决不一致的对象问题, on page 155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。

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 90

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 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。

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。

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。

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。

AWS 安全组和云安全组对象

AWS 安全组和云安全组对象之间的关系

Amazon Web 服务 (AWS) 控制台中的安全组是充当安全组中包含的实例和其他实体的虚拟防火墙的规则集合。安全组可以与其他安全组、端口、端口范围、IPV4 或 IPV6 地址、子网和负载均衡器关联。

在将 AWS VPC 载入 CDO 时，AWS 安全组将转换为 CDO **云安全组对象**。AWS 控制台不支持包含多个源、目标或端口/端口范围的规则。如果您在 CDO 和部署中的单个规则中定义了多个源、目标或端口/端口范围，则 CDO 会在将它们部署到 AWS VPC 之前将其转换为单独的规则。例如，如果您在 CDO 中创建允许从一个安全组“A”到另一个安全组“B”的流量的出站规则，则 CDO 会将此作为两个单独的规则部署到 AWS：(1) 以允许出站从安全组对象 A 到安全组对象 B 的流量，以及 (2) 允许从安全组对象 A 到 IPv6 地址的出站流量。

请注意，安全组与各个 AWS VPC 关联，并且不能跨设备类型共享。这意味着您无法与 ASA、FTD、IOS、SSH 或 Meraki 设备共享云安全组对象。

在 AWS 和其他受管设备之间共享对象

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。

ICMP 对象

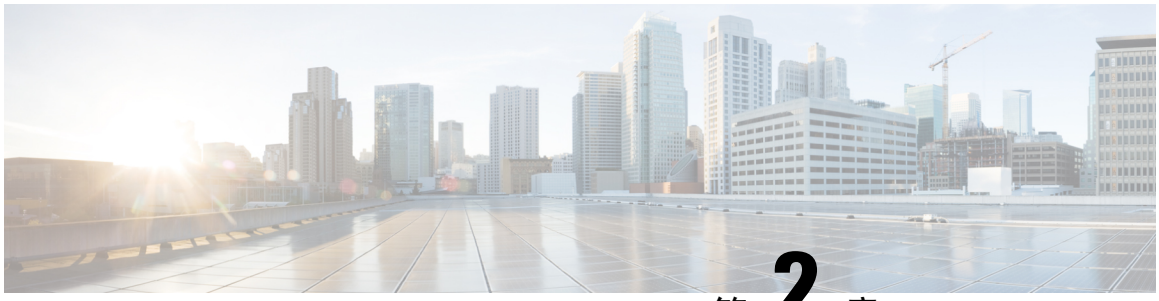
互联网控制消息协议 (ICMP) 对象是专门用于 ICMP 和 IPv6-ICMP 消息的服务对象。当 ASA 和 Firepower配置中的这些设备已载入时，CDO 会识别这些对象，并且CDO 会为其提供自己的“ICMP”过滤器，以便您轻松找到这些对象。

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。

相关信息：

- 删除对象, on page 92



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 5 页。

本章涵盖以下部分：

载入 AWS VPC

要将 AWS VPC 载入 CDO，请执行以下程序：

Before you begin

Note CDO 不支持对等的 AWS VPC。如果您尝试载入引用了对等 VPC 上定义的安全组的对等 VPC，则载入过程会失败。

在将 Amazon Web 服务 (AWS) 虚拟私有云 (VPC) 载入 CDO 之前，请查看以下前提条件：

- 查看 将 思科防御协调器 连接到托管设备, on page 5 将 CDO 连接到 AWS VPC 所需的网络要求。
- 要载入 AWS VPC，您需要使用身份和访问管理 (IAM) 控制台来生成 AWS VPC 的访问密钥和秘密访问密钥。有关详细信息，请参阅了解和获取安全凭证。
- 配置权限以允许 CDO 与您的 AWS VPC 通信。有关更多信息，请参阅更改 IAM 用户的权限。有关所需权限，请参阅以下示例：

```
"cloudformation:CreateStack",
"cloudformation:CreateStackInstances",
```

```
"cloudformation:DescribeStackInstance",
"cloudformation:DescribeStackResource",
"cloudformation:DescribeStackResources",
"cloudformation:DescribeStacks",
"ec2:AllocateAddress",
"ec2:AllocateHosts",
"ec2:AssignPrivateIpAddresses",
"ec2:AssociateAddress",
"ec2:AssociateDhcpOptions",
"ec2:AssociateRouteTable",
"ec2:AssociateSubnetCidrBlock",
"ec2:AttachInternetGateway",
"ec2:AttachNetworkInterface",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateDhcpOptions",
"ec2:CreateEgressOnlyInternetGateway",
"ec2:CreateInternetGateway",
"ec2:CreateNetworkAcl",
"ec2:CreateNetworkInterface",
"ec2:CreateNetworkInterfacePermission",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:CreateSecurityGroup",
"ec2:CreateSubnet",
"ec2:CreateTags",
"ec2:DescribeAddresses",
"ec2:DescribeAddressesAttribute",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeDhcpOptions",
"ec2:DescribeEgressOnlyInternetGateways",
"ec2:DescribeInstanceStatus",
"ec2:DescribeInstances",
"ec2:DescribeInternetGateways",
"ec2:DescribeNetworkAcls",
"ec2:DescribeNetworkInterfaceAttribute",
"ec2:DescribeNetworkInterfacePermissions",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRegions",
"ec2:DescribeRouteTables",
"ec2:DescribeSecurityGroupReferences",
"ec2:DescribeSecurityGroupRules",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeTransitGatewayVpcAttachments",
"ec2:DescribeTransitGateways",
"ec2:DescribeVpcs",
"ec2:DescribeVpnGateways",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ModifySecurityGroupRules",
"ec2:ModifySubnetAttribute",
"ec2:RunInstances",
"sts:GetCallerIdentity"
```

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

步骤 2 点击  以开始载入设备。

步骤 3 点击 **AWS VPC**。

步骤 4 输入访问密钥 ID 和秘密访问密钥凭证以连接到 AWS 账户。从您提供登录凭证的 AWS VPC 检索生成的名称列表。

步骤 5 点击**连接 (Connect)**。

步骤 6 从下拉菜单中选择区域。所选区域应为 VPC 的本地区域。

步骤 7 点击 **Select**。

步骤 8 使用下拉菜单选择正确的 AWS 名称。从您提供登录凭证的 AWS VPC 检索生成的名称列表。从下拉菜单中选择所需的 AWS VPC。请注意，AWS VPC ID 名称是唯一的，并且不能有两个或多个具有相同 ID 的实例。

步骤 9 点击 **Select**。

步骤 10 输入要在 CDO UI 中显示的名称。

步骤 11 点击**继续**。

步骤 12 （可选）输入设备的标签。请注意，如果您为 AWS VPC 创建标签，则表不会自动同步到您的设备。您必须在 AWS 控制台中手动重新创建标签作为标签。有关详细信息，请参阅AWS VPC 中的标签和标签 , on page 78。

步骤 13 点击**继续**。

步骤 14 返回**清单 (Inventory)** 页面。设备成功载入后，您将看到配置状态为“已同步”(Synced)，连接状态为“在线”(Online)。

相关信息：

- 更新 AWS VPC 连接凭证, on page 101
- AWS VPC 策略, on page 104
- CDO 中的 AWS VPC 和安全组
- 在 AWS 和其他受管设备之间共享对象

从CDO删除设备

使用以下程序可从 中删除设备：CDO

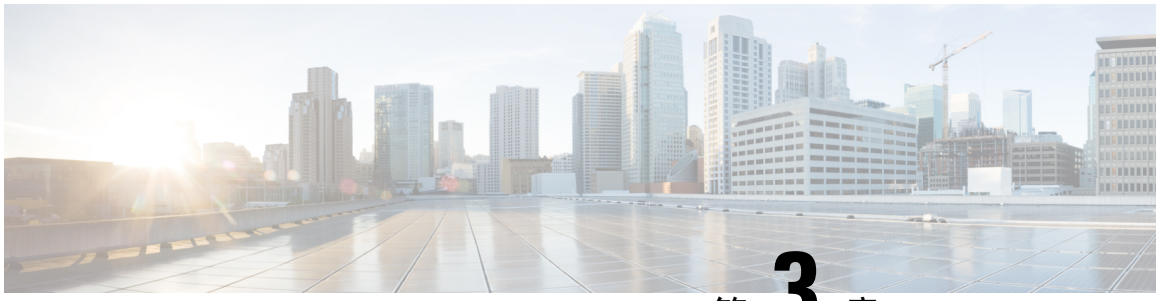
步骤 1 登录至 CDO。

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。



第 3 章

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, on page 158

相关信息

- 载入 AWS VPC, on page 97

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。

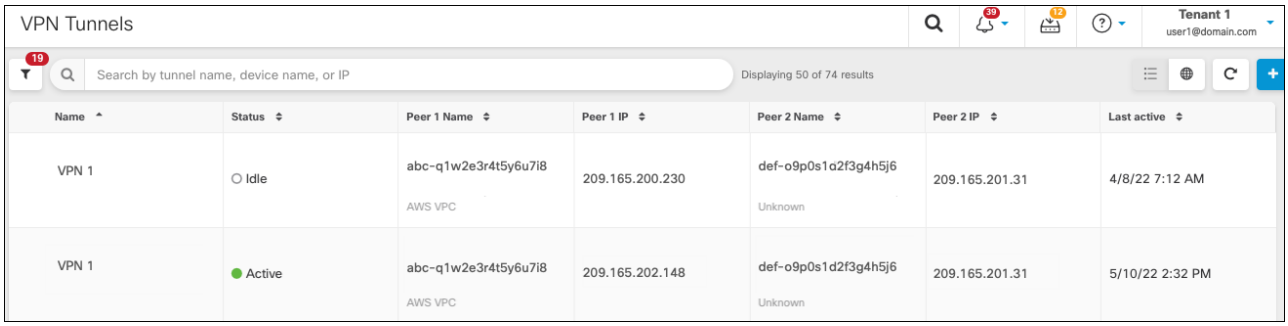
Note 您无需在 CDO 中载入安全防火墙云原生 (SFCN) VPC，即可使用 AWS 传输网关进行监控。

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 103

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 103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，第 129 页

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 104 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, on page 94。

相关信息

- 创建安全组规则, on page 105
- 编辑安全组规则, on page 106
- 删除安全组规则, on page 107

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 107 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 110

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 110

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 117 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, on page 97
- 载入 AWS VPC, on page 97

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 113

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：

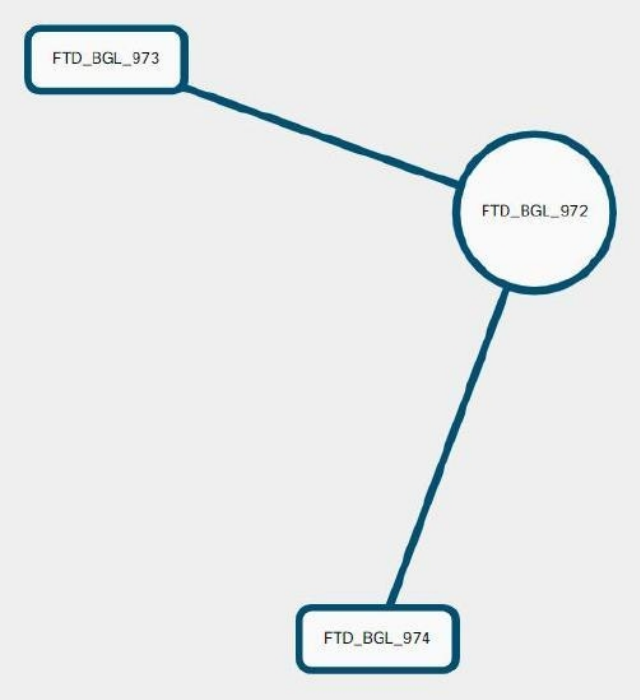
步骤 1 在主导航栏中，点击 **VPN > ASA/FDM 站点间 VPN (ASA/FDM Site-to-Site VPN)**。

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

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）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。
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）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, on page 129

- 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 117。

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, on page 37 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 116
- 预览和部署所有设备的配置更改, on page 117

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 127。

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。

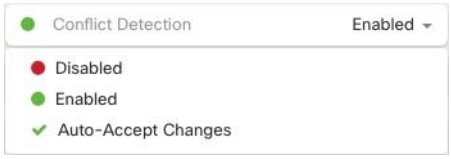
步骤 1 从导航栏中，点击**清单 (Inventory)**。

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 124。

配置自动接受更改

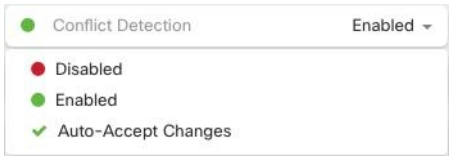
步骤 1 使用具有管理员或超级管理员权限的帐户登录 CDO。

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 117
- 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 124 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 124 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：

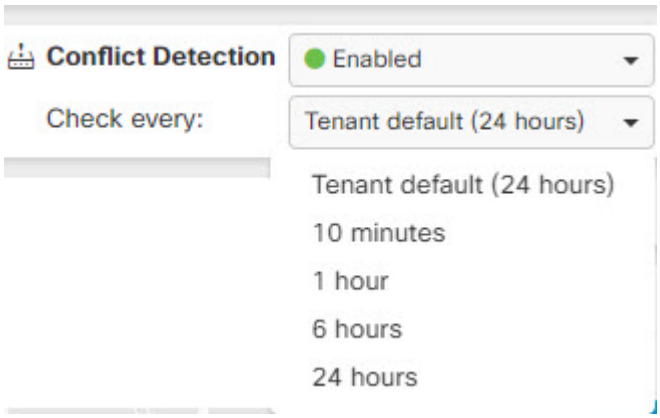
步骤 1 在导航栏中，点击 **设备和服务**。

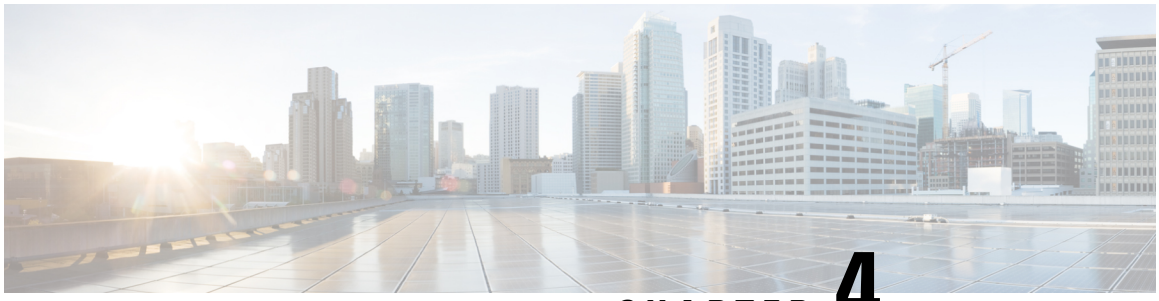
步骤 2 点击 **设备** 选项卡，找到您的设备。

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



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 131。

“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。

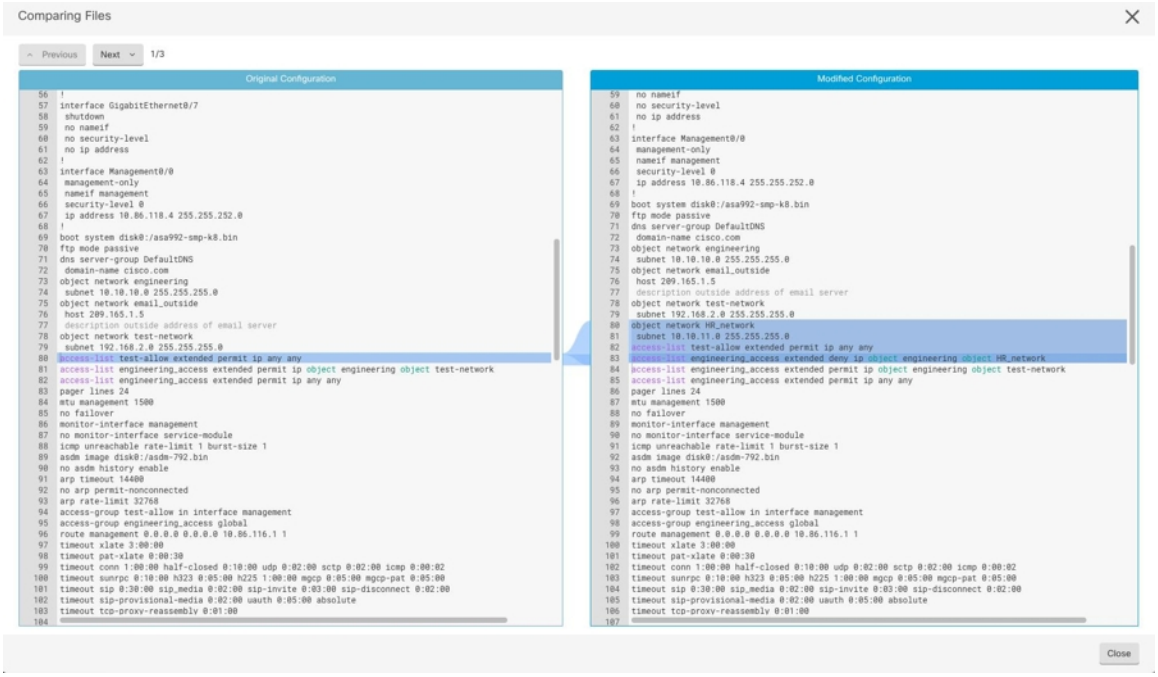
在更改日志中查找条目

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。

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 129

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：

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：

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

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

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

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

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。

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。

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

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。

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：

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 132。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. 完成后清除更改请求工具栏, on page 134。

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 132。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 133。
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

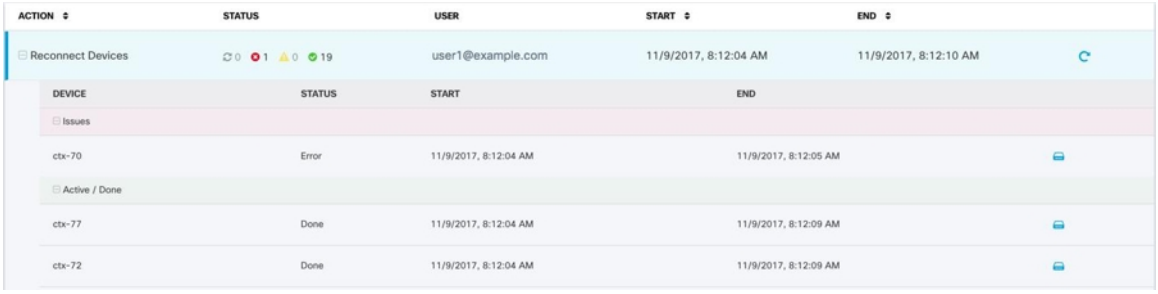
在此使用案例中，用户希望了解由于解决外部系统中维护的故障单而导致的更改日志中记录了哪些更改日志事件。请按照以下程序搜索与更改请求关联的更改日志事件：

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 133 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。

作业页面

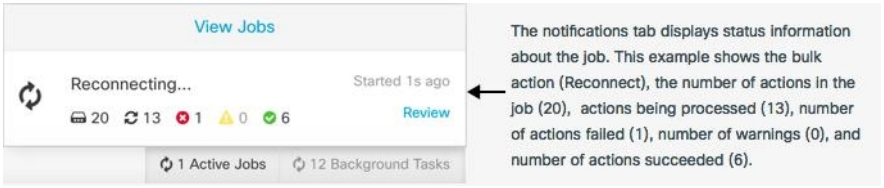
“作业”(Jobs)会页面显示有关批量操作状态的信息。批量操作可能是重新连接多个设备、从多个设备读取配置或同时升级多个设备。作业表中用颜色标记的行表示成功或失败的各个操作。

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：

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：

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。

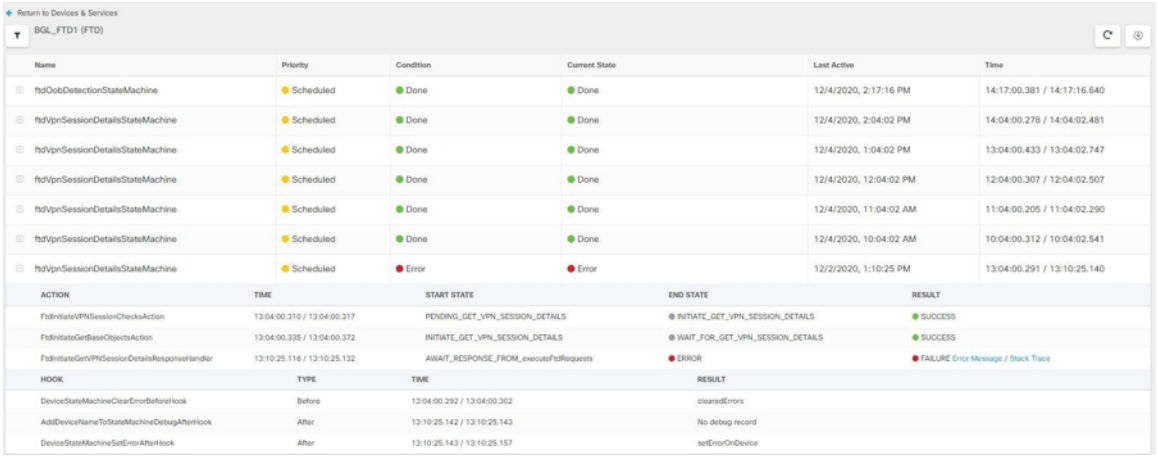
工作流程页面

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。

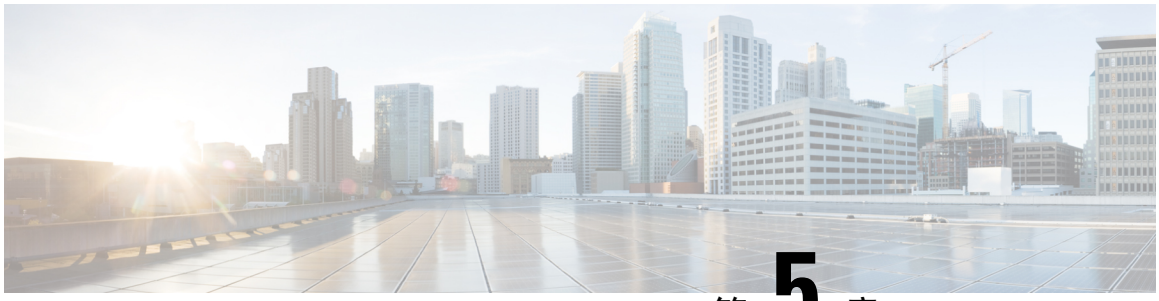


下载工作流程信息

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

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 168

相关信息：

- 关于 SecureX
- 合并您的 CDO 和 SecureX 帐户
- 在 CDO 中连接 SecureX, on page 141
- 在 CDO 中断开 SecureX 的连接, on page 142
- 将 CDO 添加到 SecureX
- SecureX 故障排除 , on page 168

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 168

使用以下程序从 CDO 获取 API 令牌并将 CDO 模块添加到 SecureX：

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。

步骤 1 登录至 CDO。

步骤 2 从右上角的用户菜单中，选择设置。

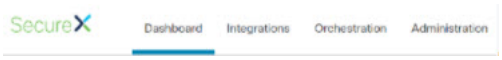
步骤 3 选择窗口左侧的常规设置选项卡。

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：

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。

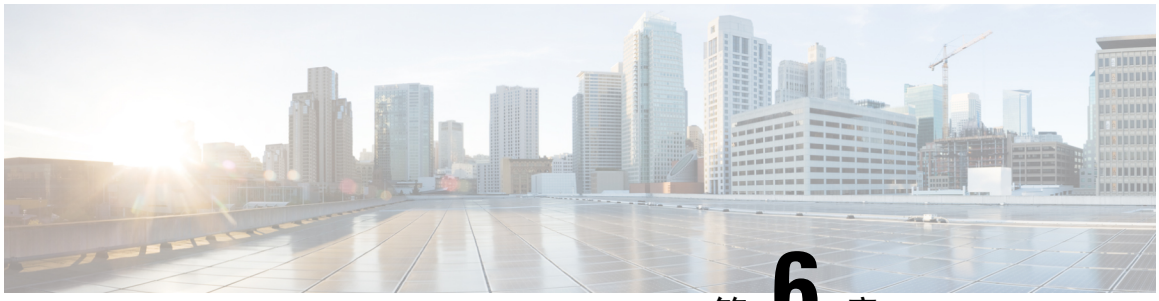
- **CDO 设备摘要 (CDO Device Summary)** - 此磁贴列出当前加入 CDO 租户的所有设备及其状态。
- **CDO 对象和策略 (CDO Objects and Policies)** - 此磁贴列出当前应用于设备的所有策略以及与这些策略关联的对象。

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 6 章

故障排除

本章涵盖以下部分：

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 5 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 146 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。

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安装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**，联系思科威胁防御支持。

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。

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 148 页
  - 更新自定义 SDC 主机，第 149 页
  - 缺陷跟踪，第 149 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 7 页

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

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 56 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 56 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

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。

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。

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 56 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 56 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

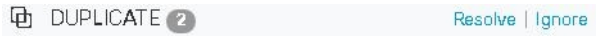
重复对象 是指同一设备上具有不同名称但值相同的两个或多个对象。这些对象通常是意外创建的，可用于类似的目的，并供不同的策略使用。解决重复对象问题后，CDO 会使用保留的对象名称来更新所有受影响的对象引用。

要解决重复对象问题，请执行以下操作：

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 72 页
- 将设备批量重新连接到 CDO， 第 76 页

解决未使用的对象问题

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 117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

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。

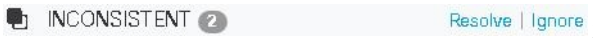
步骤 5 点击**确定 (OK)** 以确认您要删除未使用的对象。

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  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：

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 155 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。

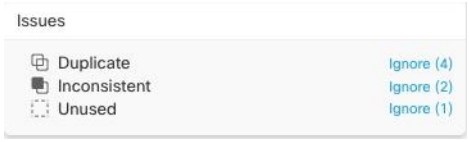
Important 如果该对象稍后与其他问题类型关联，则您提交的忽略操作仅影响您当时选择的问题。例如，如果您忽略某个对象，因为它是重复的，并且该对象后来被标记为不一致，则将其忽略为重复对象并不意味着它将作为不一致的对象被忽略。

要批量忽略问题，请执行以下程序：

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 158
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 158

设备连接状态	可能的原因	解决方法
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 159
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 167

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：

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：

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：

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：

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 124 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。

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 117
- 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。

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。

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，请参阅联系思科威胁防御支持 以了解详细信息。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。

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。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。

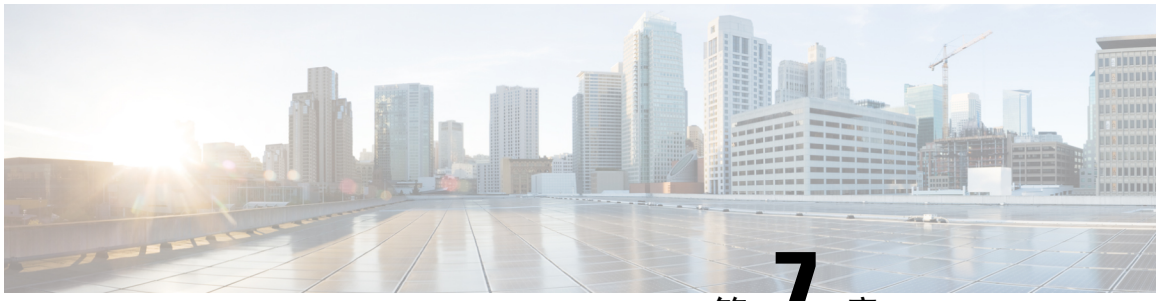
我使用错误的帐户登录功能区

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。

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。



第 7 章

常见问题和支持

本章包含以下各节：

思科 Defense Orchestrator

什么是思科防御协调器？

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。

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。

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 117

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 30
- 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。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 ASA 客户，CDO 仅支持 IPsec 站点到站点 VPN 隧道管理。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 159

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 71将设备批量重新连接到 CDO, on page 76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。

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：

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。

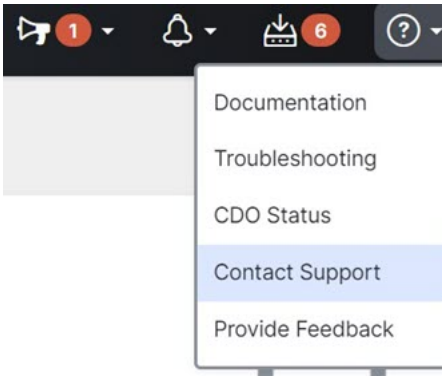
- CDO 客户如何通过 TAC 提交支持请求。
- CDO 试用客户如何向 TAC 提交支持请求。CDO 试用客户如何向 TAC 提交支持请求，第 181 页

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。

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：

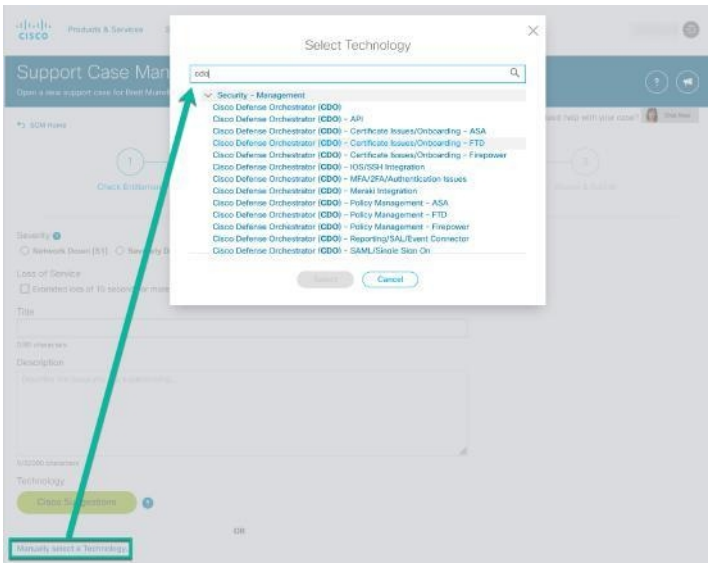
- **产品名称 (PID) (Product Name [PID])** - 如果您没有此编号，请参阅思科防御协调器产品手册。
- **产品说明 (Product Description)** - 这是 PID 的说明。
- **站点名称 (Site Name)** - 输入站点名称。如果您是为某个客户创建案例的思科合作伙伴，请输入该客户的姓名。
- **服务合同 (Service Contract)** - 输入服务合同号。
  - **重要提示：**为了使您的案例与您的 Cisco.com 账户相关联，您需要将您的合同编号与您的 Cisco.com 配置文件相关联。使用此程序将您的合同编号关联到您的 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)**。



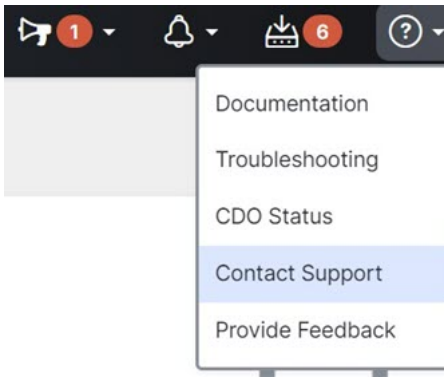
步骤 13 完成服务请求的其余部分，然后点击**提交 (Submit)**。

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。

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。