Cisco Defense Orchestrator 基础知识

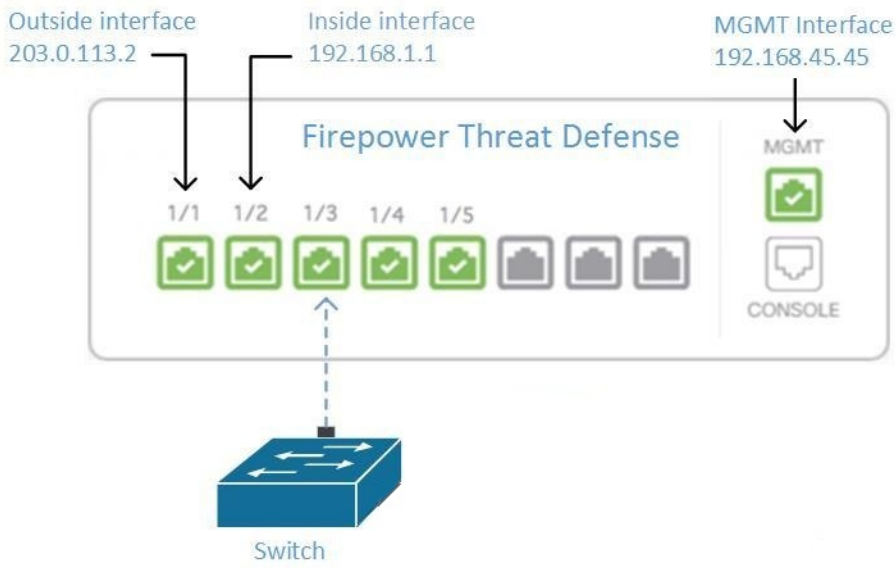
( ) 通过清晰简洁的界面提供策略管理的独特视图。思科防御协调器CDO以下主题介绍了首次使用的基础知识。CDO

联网要求

从内部接口管理设备FDM 管理

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

Figure 1: 接口地址



远程接入 VPN 要求

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

后续操作：

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

从内部接口管理设备FDM 管理

此配置方法：

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

Before you begin

在以下主题中查看此配置的前提条件：

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

Procedure

步骤 1 登录Firepower 设备管理器。

步骤 2 在系统设置菜单中，点击管理访问。

步骤 3 点击数据接口选项卡，然后点击创建数据接口。

a. 在接口字段中，从接口列表中选择预先命名为“内部”的接口。

b. 在协议字段中，选择 HTTPS（如果尚未选择）。

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

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

步骤 4 部署更改。您现在可以使用内部接口管理设备。

What to do next

如果您使用的是云连接器，该怎么办？

使用上述程序并添加以下步骤：

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

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

- 35.157.12.126
- 35.157.12.15

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

- 52.34.234.2
- 52.36.70.147

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

- 54.199.195.111
- 52.199.243.0

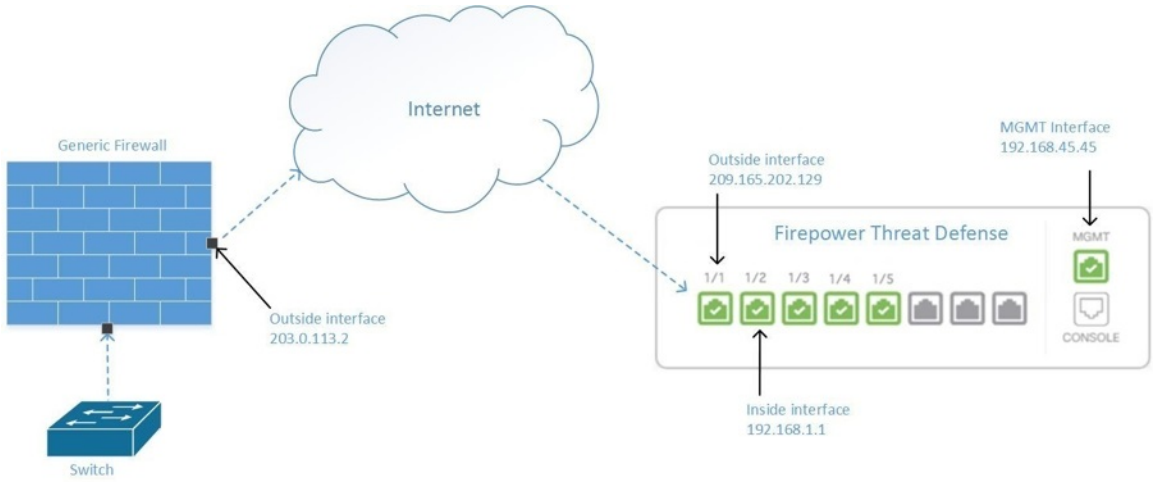
载入 FDM 管理 设备

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

从外部接口管理设备FDM 管理

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

Figure 2: 外部接口上的设备管理



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

远程接入 VPN 要求

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

后续操作：

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

管理设备的外部接口FDM 管理

此配置方法：

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

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

Before you begin

在以下主题中查看此配置的前提条件：

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

Procedure

步骤 1 登录Firepower 设备管理器。

步骤 2 在系统设置菜单中，点击管理访问。

步骤 3 点击数据接口选项卡，然后点击创建数据接口。

a. 在接口字段中，从接口列表中选择预先命名为“外部”的接口。

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

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

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

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

步骤 5 部署更改。您现在可以使用外部接口管理设备。

What to do next

如果您使用的是云连接器，该怎么办？

该过程非常相似，但有两点不同：

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

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

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

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

请求 CDO 租户

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

准备工作

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

操作步骤

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

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

   有关首次登录 CDO 租户的信息，请参阅新 CDO 租户的初始登录。

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

请求额外的 CDO 租户

如果要为现有租户创建其他租户，请联系您的客户经理。

许可证

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

关于许可证

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

订用

思科防御协调器 订用是基于期限的：

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

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

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

注释 您无法通过思科智能许可门户管理许可。CDO

软件订用支持

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

评估许可证

思科防御协调器 试用期许可证

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

云交付的防火墙管理中心 评估许可证

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

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

云交付防火墙管理中心和威胁防御许可证

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

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

云交付防火墙管理中心的威胁防御许可证

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

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

更多支持的设备和许可证

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

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

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

您将需要CDO基本授权许可证和特定于要管理的设备的许可证。

安全设备连接器 (SDC)

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

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

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

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

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

为租户部署多个 SDC 还具有以下优势：

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

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

相关信息：

- 将 思科防御协调器 连接到托管设备
- 对安全设备连接器进行故障排除

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

将 思科防御协调器 连接到托管设备

CDO 通过云连接器或安全设备连接器 (SDC) 连接到其管理的设备。

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

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

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

您的网络中需要有本地 SDC 才能载入：

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

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

通过云连接器将设备连接到 CDO

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

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

- 35.157.12.126
- 35.157.12.15

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

- 52.34.234.2
- 52.36.70.147

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

- 54.199.195.111
- 52.199.243.0

使用 SDC 将设备连接到 CDO

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

您还必须确保部署了 SDC 的虚拟机与受管设备的管理接口建立了网络连接。

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

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

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

ASA 或 Cisco Secure Firewall Cloud Native 命令示例

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

要启用外部接口，请输入以下命令：

欧洲、中东和非洲地区：

http 35.157.12.126 255.255.255.255 outside

http 35.157.12.15 255.255.255.255 outside

美国：

http 52.34.234.2 255.255.255.255 outside

http 52.36.70.147 255.255.255.255 outside

亚太地区-日本-中国地区：

http 54.199.195.111 255.255.255.255 outside

http 52.199.243.0 255.255.255.255 outside

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

http server enable 8443

使用 CDO 的 VM 映像部署安全设备连接器

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

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

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

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

开始之前

在部署 SDC 之前，请查看以下前提条件：

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

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

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

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

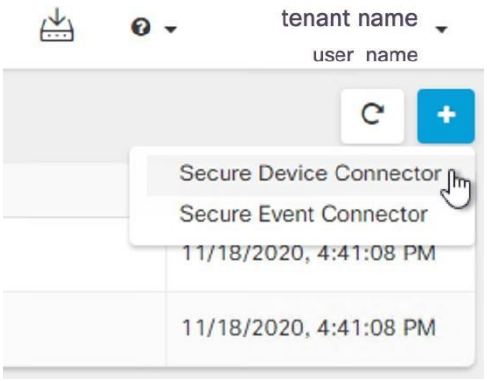
- Docker 的 IP 必须与 SDC 的 IP 范围和设备 IP 范围位于不同的子网中。
- 在开始安装之前收集以下信息：
  - 要用于 SDC 的静态 IP 地址。
  - 您在安装过程中创建的 `root` 和 `cdo` 用户的密码。
  - 您的组织使用的 DNS 服务器的 IP 地址。
  - SDC 地址所在网络的网关 IP 地址。
  - 时间服务器的 FQDN 或 IP 地址。
- SDC 虚拟机配置为定期安装安全补丁，为此，需要打开端口 80 出站。

过程

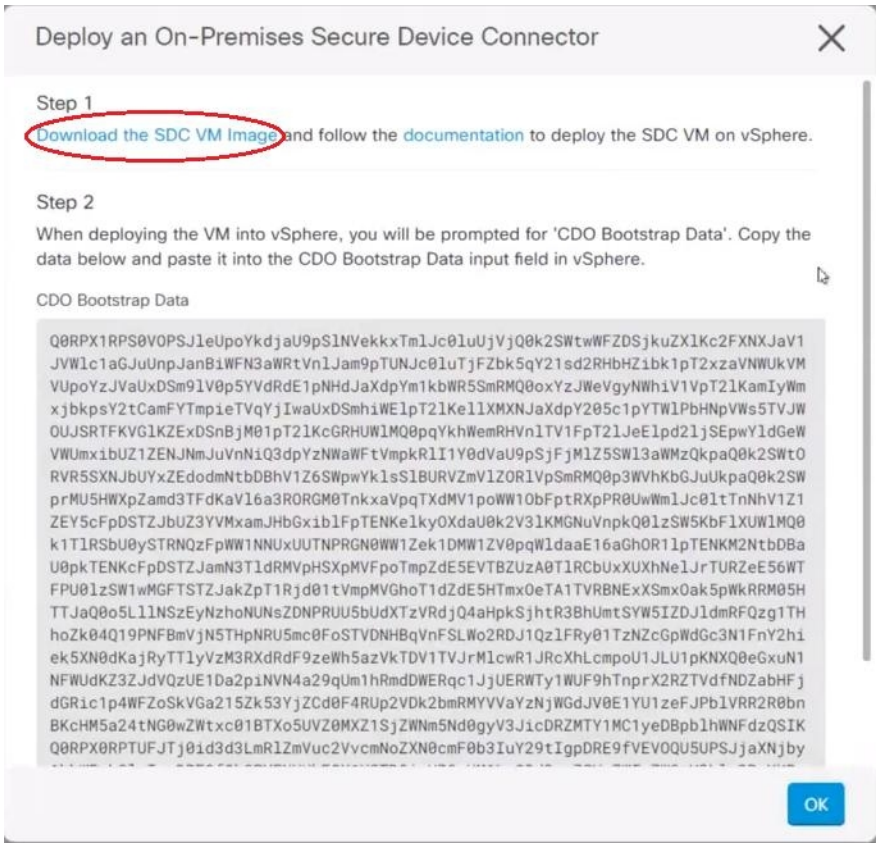
步骤 1 登录到要为其创建 SDC 的 CDO 租户。

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

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



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



步骤 5 从 zip 文件中提取所有文件。它们看起来和下面有些相似：

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

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

注释 请勿使用 ESXi Web 客户端。

步骤 7 按照提示从 OVF 模板部署安全设备连接器虚拟机。

步骤 8 设置完成后，打开 SDC VM。

步骤 9 打开新 SDC VM 的控制台。

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

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

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

步骤 12 出现密码提示时，输入 `adm123`。

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

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

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

步骤 16 系统提示时，输入以下的 SDC 的域信息：

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

如果 Docker 网桥不适用，请按 Enter 键。

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

步骤 18 确认您的输入内容。

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

步骤 20 VM 控制台会自动将您注销。

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

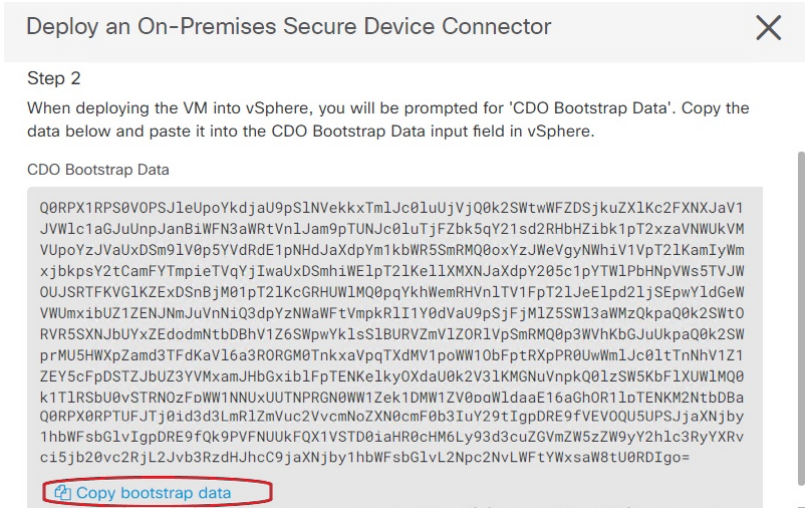
步骤 22 在提示符后，键入 `sudo sdc-onboard bootstrap`。

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

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

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

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



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

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

相关信息：

- 对安全设备连接器进行故障排除
- 排除设备与 SDC 的连接故障

在您自己的虚拟机上部署安全设备连接器

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

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

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

此程序介绍如何使用您自己的虚拟机映像在网络中安装 SDC。

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

开始之前

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

注释 我们不支持使用 vSphere 桌面客户端进行安装。

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

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

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

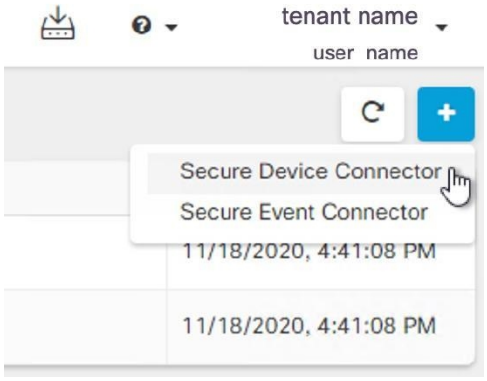
注释 **开始之前**：不要将程序中的命令复制并粘贴到终端窗口中，而应键入这些命令。某些命令包括“n-dash”，在剪切和粘贴过程中，这些命令可以作为 “m-dash” 应用，这可能会导致命令失败。

过程

步骤 1 登录到要为其创建 SDC 的 CDO 租户。

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

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



步骤 4 将窗口中步骤 2 中的引导程序数据复制到记事本。

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

- 8 GB RAM
- 10GB 磁盘空间

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

步骤 7 配置 DNS（域名服务器）服务器。

步骤 8 配置 NTP（网络时间协议）服务器。

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

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

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

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

注释 请勿使用 **--user** 标志。

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

注释 使用“使用存储库安装”方法。

步骤 13 启动 Docker 服务并使其在启动时启动：

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

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

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

步骤 15 为 cdo 用户设置密码。

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

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

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

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

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

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

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

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

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

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

步骤 20 将目录更改为 **/usr/local/cdo**。

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

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

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

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

运行 cat 命令以查看解码后的数据。命令和解码后的数据应如下所示：

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

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

步骤 23 运行以下命令，将解码的引导程序数据部分导出到环境变量。

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

步骤 24 从 CDO 下载引导程序捆绑包。

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

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

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

SDC 现在应在 CDO 中显示“活动”。

下一步做什么

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

- 如果要在租户上安装**第二个或多个**安全事件连接器，请返回为租户安装多个 SEC。

使用 Terraform 模块在 AWS VPC 上部署安全设备连接器

开始之前

在尝试在 AWS VPC 上部署 SDC 之前，请查看以下前提条件：

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

过程

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

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

有关输入变量和说明的列表，请参阅安全设备连接器 Terraform 模块。

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

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

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

下一步做什么

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

更改安全设备连接器的 IP 地址

开始之前

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

注释 更改 SDC 的 IP 地址后，您无需将任何设备重新载入 CDO。

过程

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

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

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

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

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

步骤 4 出现提示时，请输入密码。

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

步骤 5 在提示符后键入 n 以重置 root 和 CDO 密码。

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

步骤 6 在提示符后键入 y 以重新配置网络。

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

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

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

如果 NTP 服务器或 FQDN 不适用，请按 Enter 键。

e) Docker 网桥

如果 Docker 网桥不适用，请按 Enter 键。

步骤 8 当系统提示输入值是否正确时，请使用 y 确认输入。

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

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

步骤 9 使用分配给 SDC 的新 IP 地址创建 SSH 连接并登录。

步骤 10 您可以运行连接状态测试命令，以确保 SDC 正常运行。

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

所有检查都必须以绿色显示 [OK]。

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

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

步骤 12 刷新页面并选择已更改 IP 地址的安全连接器。

步骤 13 在操作窗格中，点击请求检测信号。

您应该会看到已成功请求心跳消息，并且上次心跳应显示当前日期和时间。

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

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

删除安全设备连接器

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

要从租户中删除 SDC，请遵循以下程序：

Procedure

步骤 1 删除连接到您要删除的 SDC 的任何设备。

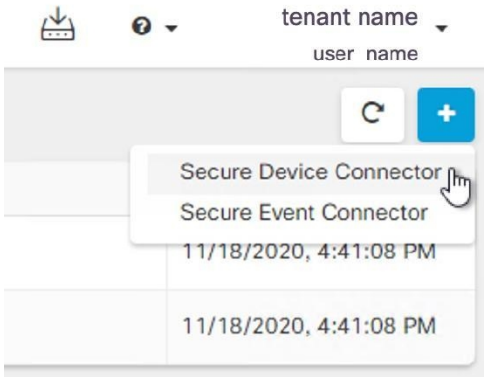
- **a.** 请参阅查找所有使用相同 SDC 连接到 CDO 的设备，以便确定 SDC 使用的所有设备。

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

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

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

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



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

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

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

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

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

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

步骤 7 点击**确定 (OK)** 以确认删除 SDC。

将 ASA 从一个 SDC 移至另一个 SDC

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

过程

步骤 1 在导航栏中，点击 **设备和服务**。

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

步骤 3 选择要移动到其他 SDC 的 ASA。

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

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

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

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

更新 Meraki MX 连接凭证

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

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

使用以下程序更新 Meraki MX 设备的凭证：

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。

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

步骤 3 选择要更新其连接凭证的 Meraki MX。

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

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

重命名安全设备连接器

过程

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

步骤 2 选择要重命名的 SDC。

步骤 3 在详细信息窗格中，点击 SDC 名称旁边的编辑图标。

步骤 4 重命名 SDC。

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

更新您的安全设备连接器

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

Procedure

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

步骤 2 以 **cdo** 用户身份登录 SDC。

步骤 3 切换到 SDC 用户以更新 SDC Docker 容器：

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

步骤 4 升级 SDC 工具包：

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

步骤 5 升级 SDC：

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

在单个 CDO 租户上使用多个 SDC

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

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

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

查找所有使用相同 SDC 连接到 CDO 的设备

请按照以下程序识别所有使用相同 SDC 连接到 CDO 的设备：

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击设备类型选项卡。

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

步骤 5 点击过滤器按钮  以展开过滤器菜单。

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

步骤 7 （可选）检查过滤器菜单中的其他过滤器，以便进一步细化搜索。

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

安全设备连接器开源和第三方许可证归属

==========

*** amqplib ***

amqplib 版权所有 (c) 2013, 2014

米歇尔·布里根<mikeb@squaremobius.net>

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

http://opensource.org/licenses/MIT

==========

*** async ***

版权所有 (c) 2010-2016 Caolan McMaho

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

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

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

==========

*** bluebird ***

MIT 许可证 (MIT)

版权所有 **(c) 2013-2015 Petka Antonov**

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

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

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

==========

***cheerio ***

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

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

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

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

==========

*** command-line-args ***

MIT 许可证 (MIT)

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

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

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

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

==========

*** ip ***

此软件根据 **MIT** 许可证获得许可。

Fedor Indutny, 2012 版权所有。

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

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

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

==========

*** json-buffer ***

版权所有 **(c) 2013 Dominic Tarr**

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

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

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

==========

*** json-stable-stringify ***

此软件在 **MIT** 许可证下发布：

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

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

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

==========

*** json-stringify-safe ***

ISC 许可证

版权所有 **(c) Isaac Z. Schlueter** 和贡献者

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

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

==========

*** lodash ***

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

基于 **Underscore.js**，版权所有，

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

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

以下许可证适用于本软件的所有部分，但作为

记录如下：

====

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

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

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

====

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

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

====

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

==========

*** log4js ***

版权所有 **2015 Gareth Jones**（许多其他人的贡献）

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

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

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

==========

*** mkdirp ***

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

此项目是在 **MIT/X11** 许可证下发布的免费软件：

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

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

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

==========

*** node-forge ***

新 **BSD** 许可证（**3** 个子句）

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

版权所有。

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

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

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

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

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

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

==========

*** request ***

Apache 许可证

版本 **2.0**，**2004** 年 **1** 月

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

使用、复制和分发条款和条件

1. 定义。

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

“许可方”是指版权所有者或由版权所有者授权进行许可授予的实体。

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

“您”（或“您的”）是指行使此许可证所授权限的个人或法律实体。

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

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

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

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

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

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

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

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

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

您必须向作品或衍生作品的任何其他接收者提供本许可证的副本；和

您必须在任何已修改的文件上放置醒目的通知，说明您更改了文件；和

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

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

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

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

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

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

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

条款和条件结束

==========

*** rimraf ***

ISC 许可证

版权所有 **(c) Isaac Z. Schlueter** 和贡献者

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

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

==========

*** uuid ***

版权所有 **(c) 2010-2012 Robert Kieffer**

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

==========

***** 验证器 *****

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

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

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

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

==========

***** 何时 *****

开源计划 **OSI - MIT** 许可证

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

版权所有 **(c) 2011** 布赖恩·卡瓦利埃

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

上述版权声明和本许可声明应包含在软件的所有副本或重要部分中。

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

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

登录到 CDO

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

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

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

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

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

注释

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

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

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

新 CDO 租户的初始登录

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

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

重要事项

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

准备工作

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

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

后续操作？

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

登录失败故障排除

登录失败，因为您无意中登录到错误的 CDO 区域

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

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

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

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

注释

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

准备工作

我们强烈建议在迁移之前执行以下步骤：

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

迁移后的登录失败故障排除

由于用户名或密码不正确，CDO 登录失败

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

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

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

使用保存的书签登录失败

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

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

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

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

Procedure

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

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

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

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

租户视图显示您拥有用户记录的多个租户。

管理租户的超级管理员

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

CDO 支持的软件和硬件

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

相关信息：

Secure Firewall Threat Defense 设备支持详情

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

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

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

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

CDO 支持的硬件和软件映像

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

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

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

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

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

CDO 支持的虚拟机平台和软件映像

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

Table 2: 按管理器和版本***FTDv***

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

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

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

有关使用 CDO 管理 Firepower 设备接口的详细信息，请参阅 Firepower 接口配置准则和限制。

ASA FirePOWER 服务模块

CDO 不支持 ASA FirePOWER 服务模块。

浏览器支持

CDO 支持以下浏览器的最新版本：

- Google Chrome
- Mozilla Firefox

思科防御协调器平台维护计划

Cisco Defense Orchestrator 维护计划

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

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

表 *3: CDO* 维护时间表

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

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

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

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

云交付的防火墙管理中心维护时间表

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

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

表 *4:* 云交付的防火墙管理中心维护时间表

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

租户管理

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

相关信息：

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

常规设置

在右上角的“管理”下拉列表中，点击 **设置**。

请参阅以下有关常规 CDO 设置的主题：

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

用户设置

选择所需的 CDO UI 显示语言。此选择仅影响进行此更改的用户。

我的令牌

有关详细信息，请参阅 API 令牌。API 令牌, on page 53

租户设置

启用更改请求跟踪

启用更改请求跟踪会影响租户的所有用户。要启用更改请求跟踪，请执行以下程序：

Procedure

步骤 1 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 2 点击**常规**选项卡。

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

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

阻止思科支持人员查看您的租户

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

要防止思科支持人员查看您的租户，请执行以下程序：

Procedure

步骤 1 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 2 点击**常规**选项卡。

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

启用自动接受设备更改的选项

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

要启用设备更改自动接受，请执行以下程序：

Procedure

步骤 1 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 2 点击**常规**选项卡。

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

默认冲突检测间隔

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

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

要配置此选项并选择新的冲突检测间隔，请执行以下程序：

Procedure

步骤 1 在右上角的“管理”下拉列表中，点击 **设置**。

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

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

启用计划自动部署的选项

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

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

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

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

要启用该选项以计划自动部署，请执行以下程序：

Procedure

步骤 1 在右上角的“管理”下拉列表中，点击 **设置**。

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

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

Web 分析

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

默认启用网络分析。要禁用 Web 分析或在将来启用，请执行以下程序：

Procedure

步骤 1 在右上角的“管理”下拉列表中，点击 **设置**。

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

步骤 3 点击**网络分析 (Web Analytics)** 下的滑块。

配置默认定期备份计划

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

Procedure

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

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

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

步骤 3 点击**保存 (Save)**。

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

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更改日志。

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

发送设备工作流程警报

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

请务必检查您想要通知的所有设备工作流程场景。手动检查以下任何操作：

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

  从 FMC 到 CDO 的设备管理器。

发送设备事件警报

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

请务必检查您想要通知的所有设备工作流程场景。手动检查以下任何操作：

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

发送后台日志搜索警报

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

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

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

用户

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

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

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

查看 CDO 通知

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

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

服务集成

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

为 CDO 通知启用服务集成

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

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

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

Webex Teams 的传入 Webhook

开始之前

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

使用以下程序为 Webex Teams 允许传入 Webhook：

过程

步骤 1 打开 Webex Teams 应用。

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

步骤 3 使用搜索栏查找传入 Webhook。

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

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

步骤 6 进行以下配置：

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

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

步骤 8 复制 Webhook URL。

步骤 9 登录至 CDO。

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

步骤 11 滚动到服务集成。

步骤 12 点击蓝色加号按钮。

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

步骤 14 展开下拉菜单并选择 Webex 作为服务类型。

步骤 15 粘贴从服务生成的 Webhook URL。

步骤 16 点击“确定”。

Slack 的传入 Webhook

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

使用以下程序允许 Slack 的传入 Webhook：

过程

步骤 1 登录您的 Slack 帐户。

步骤 2 在左侧的面板中，滚动到底部并选择添加应用。

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

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

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

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

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

步骤 8 登录至 CDO。

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

步骤 10 滚动到服务集成。

步骤 11 点击蓝色加号按钮。

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

步骤 13 展开下拉菜单并选择 Slack 作为服务类型。

步骤 14 粘贴从服务生成的 Webhook URL。

步骤 15 点击“确定”。

自定义集成的传入 Webhook

开始之前

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

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

过程

步骤 1 从您选择的自定义服务或应用生成并复制 Webhook URL。

步骤 2 登录至 CDO。

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

步骤 4 滚动到服务集成。

步骤 5 点击蓝色加号按钮。

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

步骤 7 展开下拉菜单并选择自定义作为服务类型。

步骤 8 粘贴从服务生成的 Webhook URL。

步骤 9 点击“确定”。

日志记录设置

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

点击“查看历史使用情况”可查看租户在过去 12 个月内收到的所有日志记录。

您还可以使用链接请求额外的存储空间。

将 SAML 单点登录与 Cisco Defense Orchestrator 集成

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

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

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

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

更新 SSO 证书

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

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

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

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

API 令牌

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

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

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

API 令牌格式和声明

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

CDO API 令牌提供以下一组声明：

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

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

令牌管理

生成 API 令牌

Procedure

步骤 1 在左侧的导航栏中，点击**设置 (Settings)** > **常规设置 (General Settings)**。
步骤 2 在我的令牌中，点击生成 API 令牌。
步骤 3 根据企业维护敏感数据的最佳实践，将令牌保存在安全位置。

续订 API 令牌

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

Procedure

步骤 1 在左侧导航栏中，点击 **设置 (Settings)** > **常规设置 (General Settings)**。
步骤 2 在“我的令牌”(My Tokens) 中，点击**续约 (Renew)**。CDO 会生成新的令牌。
步骤 3 根据企业维护敏感数据的最佳实践，将新令牌保存在安全位置。

撤销 API 令牌

Procedure

步骤 1 在左侧导航栏中，点击 **设置 (Settings)** > **常规设置 (General Settings)**。
步骤 2 在“我的令牌”(My Tokens) 中，点击**撤销 (Revoke)**。CDO 将撤销令牌。

身份提供程序账户与思科防御协调器用户记录之间的关系

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

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

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

登录工作流程

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

Procedure

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

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

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

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

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

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

此架构的含义

使用 Cisco Security Cloud Sign On 的客户

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

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

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

拥有自己的身份提供程序的客户

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

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

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

思科托管服务提供商

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

相关主题

- 常规设置
- 用户管理
- 思科防御协调器中的用户角色

管理多租户门户

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

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

准备工作

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

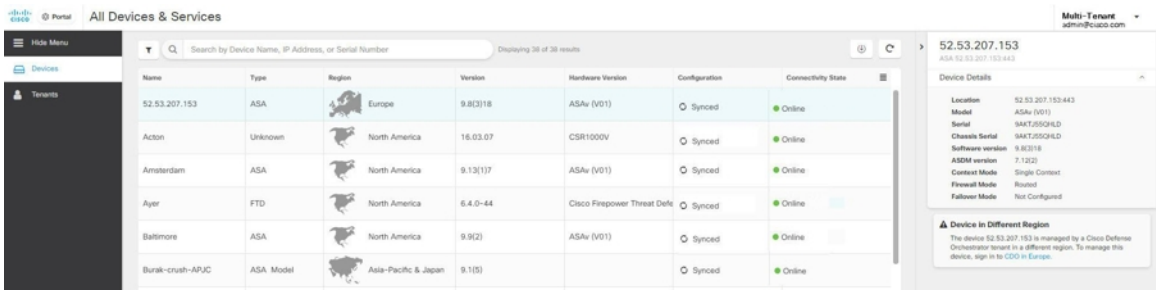
我们建议您从 Web 浏览器清除缓存和 Cookie，以避免可能发生的某些浏览器相关问题。

多租户门户

门户提供以下菜单：

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

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



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

将租户添加到多租户门户

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

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

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

Procedure

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

步骤 2 点击生成 API 令牌，然后复制它。

步骤 3 转到门户，然后点击租户选项卡。

步骤 4 点击右侧的添加租户按钮。

步骤 5 粘贴令牌，然后点击保存。

从多租户门户删除租户

Procedure

步骤 1 转到门户，然后点击租户选项卡。

步骤 2 点击右侧显示的相应删除图标，删除所需的租户。

步骤 3 点击**删除 (Remove)**。关联的设备也会从门户中删除。

管理租户门户设置

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

设置

常规设置

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

默认启用网络分析。要禁用 Web 分析或在将来启用，请执行以下程序：

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

用户管理

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

切换租户

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

Procedure

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

思科成功网络

思科成功网络是一项用户启用的云服务。启用思科成功网络时，设备与思科云之间会建立安全连接以传输使用情况信息和统计信息。数据流遥测提供一种机制，可从设备选择相关数据，并以结构化的格式将其传输至远程管理站，从而获得以下优势：

- 通知您在网络中可用来改进产品效果的未使用功能。
- 通知您适用于您产品的其他技术支持服务和监控。
- 帮助思科改善我们的产品。

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

注释

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

启用或禁用思科成功网络

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

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

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

用户管理

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

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

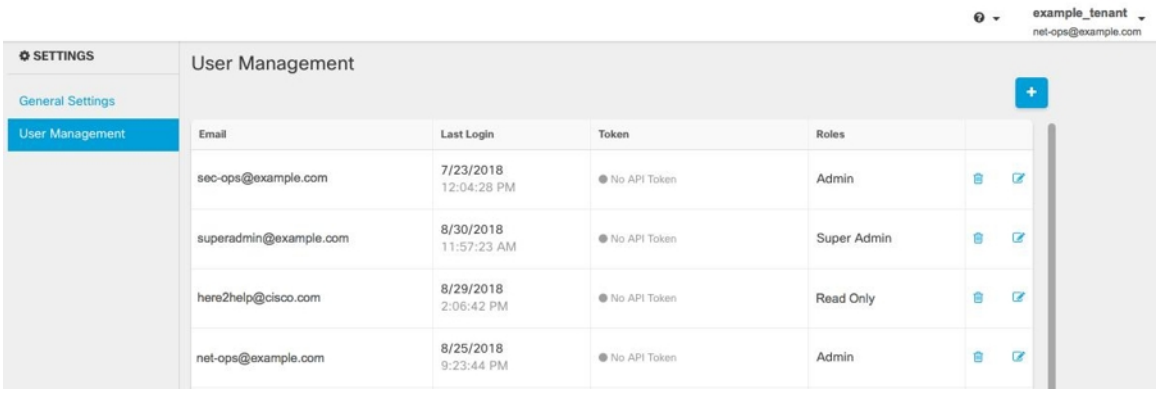
您可以在**用户管理 (User Management)** 屏幕上查看与您的租户关联的所有用户记录。这包括临时与您的账户关联以解决支持请求的任何思科支持工程师。

查看与您的租户关联的用户记录

过程

步骤 1 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 2 点击**用户管理**。



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

用户管理中的 Active Directory 组

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

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

“Active Directory 组”选项卡

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

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

“审核日志”选项卡

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

多角色用户

作为 CDO 中 IAM 功能的扩展，用户现在可以拥有多个角色。

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

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

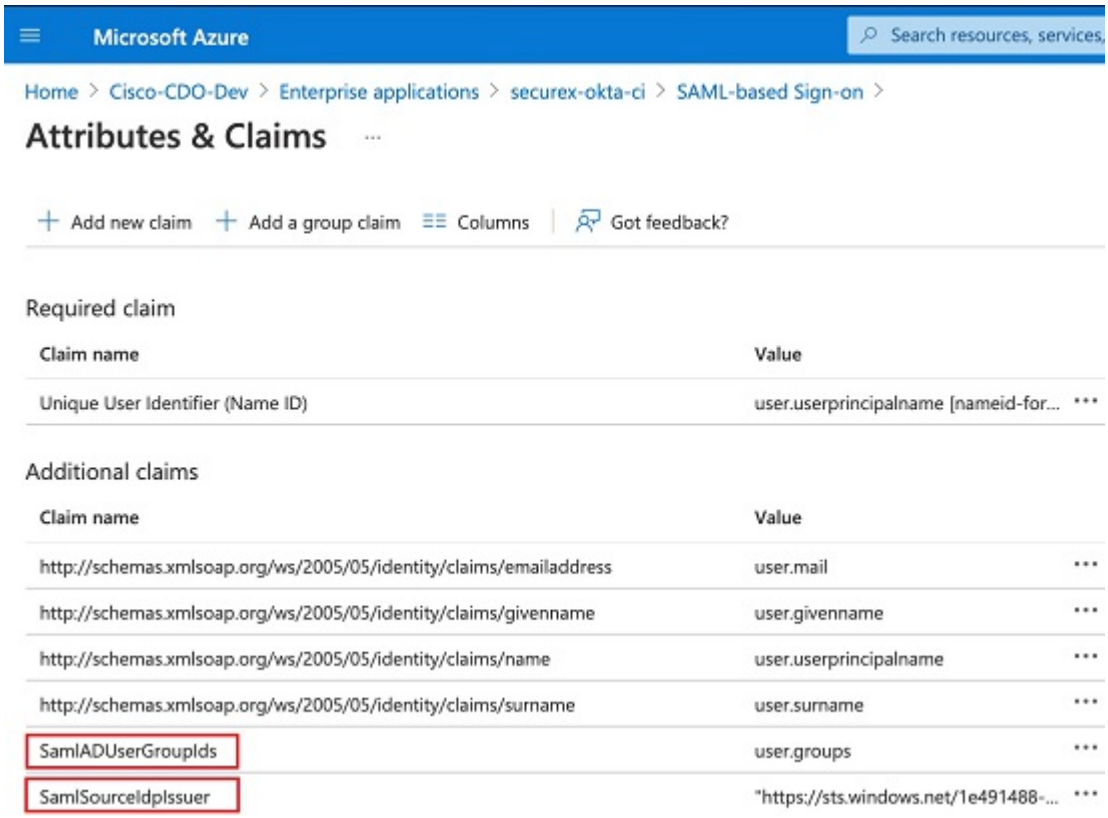
注释 如果用户既是单个用户又是同一租户上的 AD 组的一部分，则单个用户的用户角色将覆盖 AD 组的用户角色。

准备工作

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

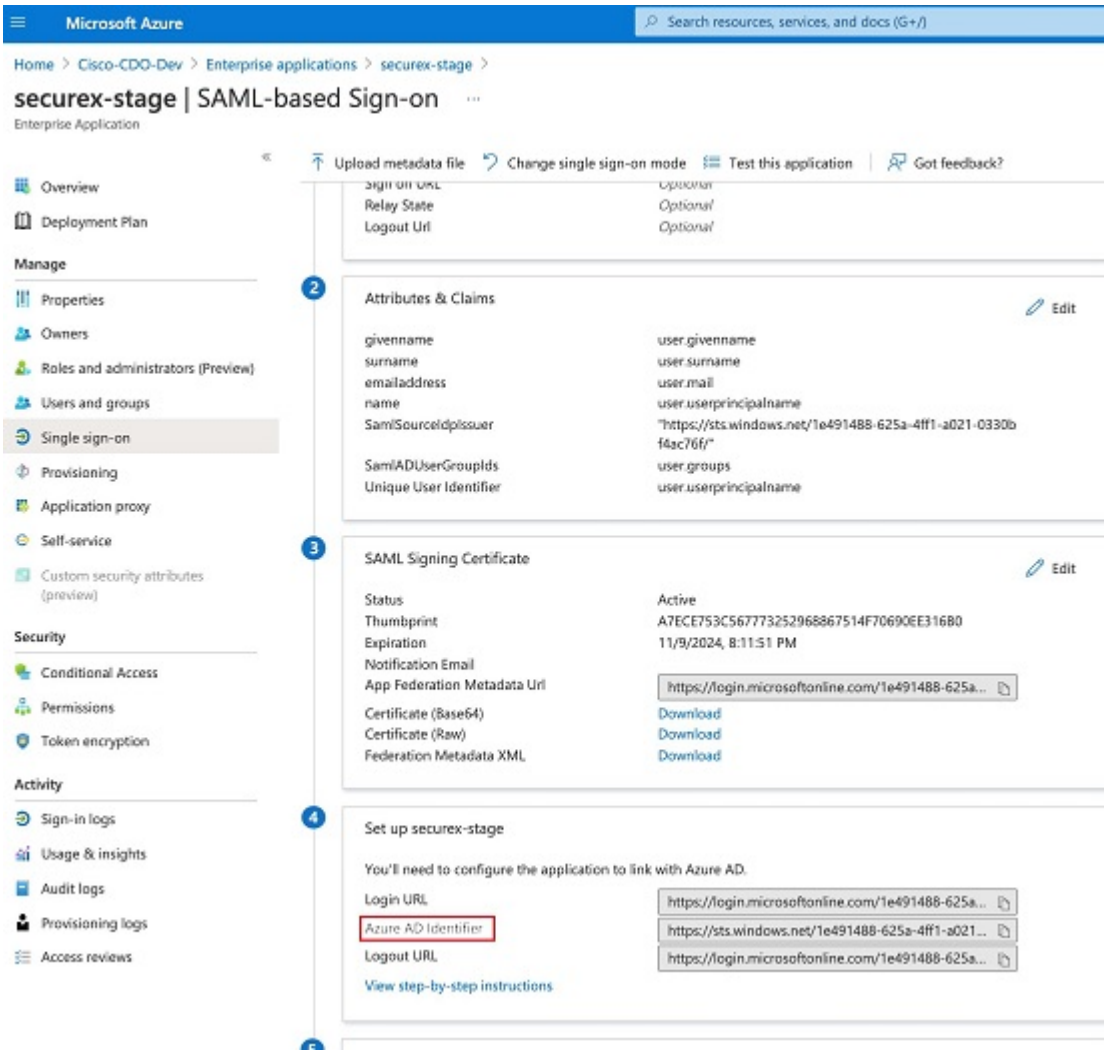
1. 向思科 TAC 提交支持案例，并请求使用以下信息进行自定义 AD IdP 集成：https://mycase.cloudapps.cisco.com/case
   - 您的 CDO 租户名称和区域。
   - 定义自定义路由的域（例如：@cisco.com、@myenterprise.com）。
   - XML 格式的证书和联合元数据。
2. 在 AD 中添加以下自定义 SAML 声明。请注意，这些值区分大小写。
   - SamlADUserGroupIds - 此属性描述用户在 AD 上的所有组关联。例如，在 Azure 中选择 + 添加组申领，如下面的屏幕截图所示：

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



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

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



添加用于用户管理的 Active Directory 组

过程

步骤 1 登录 CDO。

步骤 2 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 3 点击 **用户管理** 选项卡。

步骤 4 选择表顶部的 Active Directory 组选项卡。

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

步骤 6 输入以下信息：

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

步骤 7 点击**确定**。

编辑用于用户管理的 Active Directory 组

开始之前

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

过程

步骤 1 登录 CDO。

步骤 2 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 3 点击 **用户管理** 选项卡。

步骤 4 选择表顶部的 Active Directory 组选项卡。

步骤 5 确定要编辑的 AD 组，然后选择编辑图标。

步骤 6 修改以下值：

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

删除用于用户管理的 Active Directory 组

过程

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

创建新的 CDO 用户

要创建新的 CDO 用户，需要执行这两项任务。它们不需要按顺序执行：

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

完成这些任务后，用户可以新用户从思科安全登录控制面板打开 CDO。

为新用户创建 Cisco Security Cloud Sign On 账户

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

关于登录 CDO

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

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

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

登录前

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

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

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

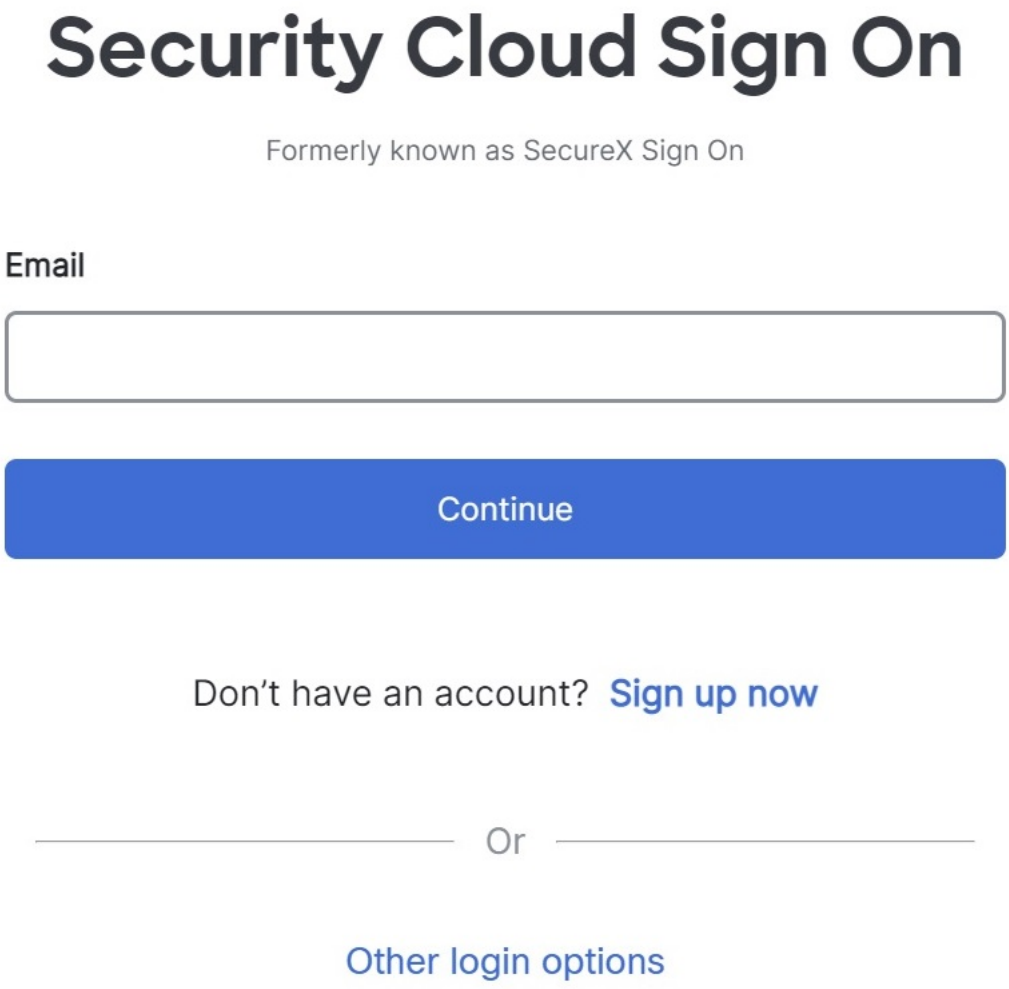
初始登录工作流程分为四步。您需要完成所有四个步骤。

Procedure

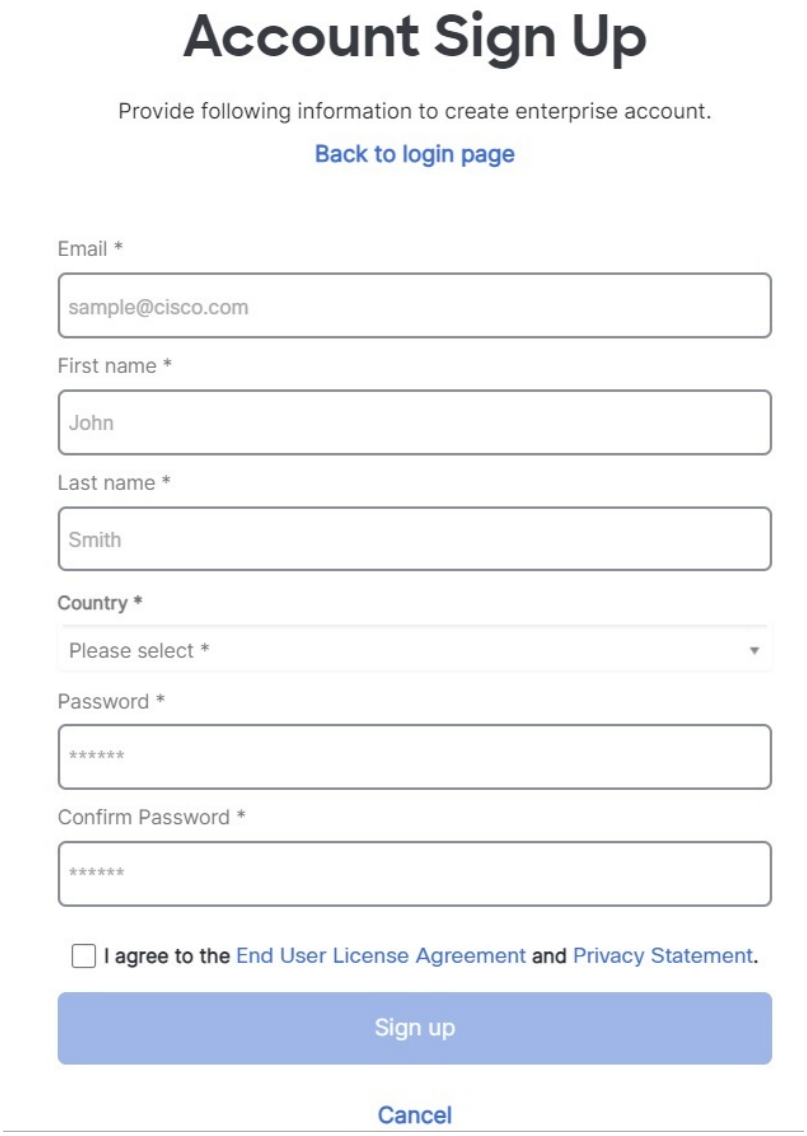
步骤 1 注册新的 **Cisco Security Cloud Sign On** 账户

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

b. 在“登录”屏幕的底部，点击**注册**。



c. 填写“创建帐户”(Create Account) 对话框中的字段。



我们为您提供了以下提示：

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

d. 在您点击**创建帐户 (Create Account)** 之后。

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

步骤 2 使用 Duo 设置多因素身份验证

我们建议在设置多因素身份验证时使用移动设备。

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

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

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

c. 在向导结束时，点击**继续登录**。

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

步骤 3 （可选）将 **Google 身份验证器设置为附加身份验证器**

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

b. 按照安装向导中的提示设置 Google Authenticator。

步骤 4 **配置思科安全登录账户的账户恢复选项**

a. 选择恢复电话号码以使用 SMS 重置帐户。

b. 选择安全图像。

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

Tip

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

使用您的 CDO 用户名创建 CDO 用户记录

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

使用以下程序创建具有适当用户角色的用户记录：

Procedure

步骤 1 登录 CDO。

步骤 2 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 3 点击 **用户管理** 选项卡。

步骤 4 点击蓝色加号按钮  ，将新用户添加到租户。

步骤 5 提供用户的邮件地址。

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

步骤 6 从下拉菜单中选择用户的 思科防御协调器中的用户角色 。

步骤 7 点击**确定 (OK)**。

新用户从思科安全登录控制面板打开 CDO

Procedure

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

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

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

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

租户视图显示您拥有用户记录的多个租户。

思科防御协调器中的用户角色

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

只读角色

分配了只读角色的用户会在每个页面上看到此蓝色横幅：

Read Only User. You cannot make configuration changes.

。

具有只读角色的用户可以执行以下操作：

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

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

只读用户不能执行以下操作：

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

仅编辑角色

具有“仅编辑”角色的用户可以执行以下操作：

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

仅编辑用户不能执行以下操作：

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

- 创建 CDO 用户记录。
- 更改用户角色。

仅部署角色

具有“仅部署”角色的用户可以执行以下操作：

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

仅部署用户不能执行以下操作：

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

VPN 会话管理器角色

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

具有 VPN 会话管理器角色的用户可以执行以下操作：

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

VPN 会话管理器用户不能执行以下操作：

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

管理角色

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

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

管理员用户不能执行以下操作：

- 创建 CDO 用户记录。
- 更改用户角色。

超级管理员角色

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

- 更改用户角色。
- 创建用户记录。

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

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

更改用户角色的记录

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

您必须是超级管理员才能更改用户记录。如果您的租户没有超级管理员，请联系 Defense Orchestrator 支持。

为用户角色创建用户记录

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

Note 您需要在 CDO 上具有超级管理员角色角色才能执行此任务。

创建用户记录

使用以下程序创建具有适当用户角色的用户记录：

Procedure

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

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

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

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

创建仅 API 用户

过程

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

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

步骤 7 从下拉菜单中选择用户的 思科防御协调器中的用户角色 。

步骤 8 点击**确定**。

步骤 9 点击 **用户管理** 选项卡。

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

编辑用户角色的用户记录

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

Note 您需要在 CDO 上具有超级管理员角色角色才能执行此任务。

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

编辑用户角色

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

要编辑用户记录中定义的角色，请执行以下程序：

Procedure

步骤 1 登录 CDO。

步骤 2 在右上角的“管理”下拉列表中，点击 **设置**。

步骤 3 点击 **用户管理** 选项卡。

步骤 4 点击用户行中的编辑图标。

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

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

步骤 7 点击 v。

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

删除用户角色的用户记录

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

Note 您需要在 CDO 上具有超级管理员角色角色才能执行此任务。

删除用户记录

要删除用户记录中定义的角色，请参阅以下程序：

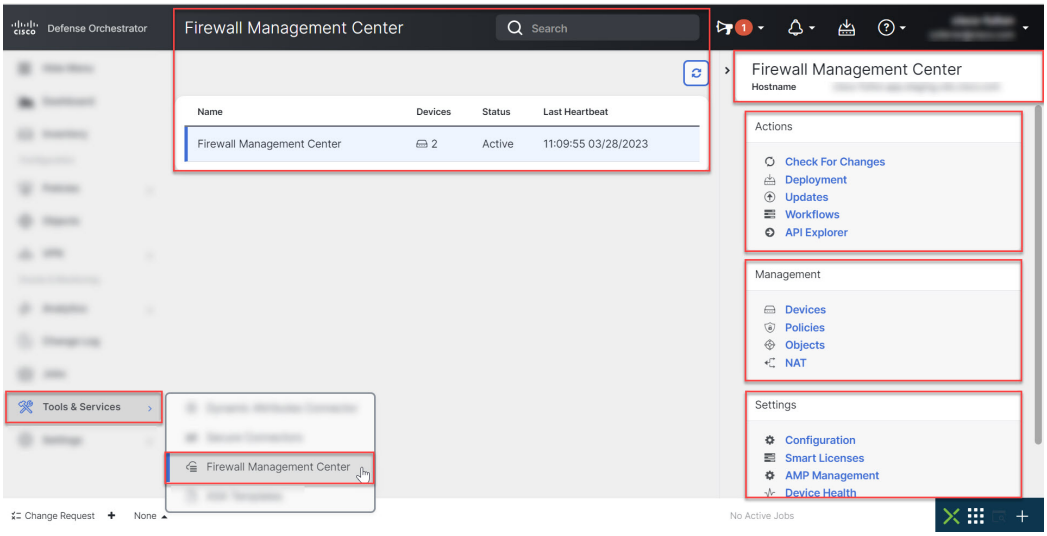
Procedure

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

云交付的防火墙管理中心 应用页面

从 CDO 的主菜单打开 云交付的防火墙管理中心 应用页面。

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



“防火墙管理中心”页面显示以下信息：

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

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

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

更新 云交付的防火墙管理中心 设备计数和状态

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

支持在不同的选项卡上打开 CDO 和 云交付的防火墙管理中心 应用

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

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

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

注释 点击一下即可在同一选项卡中打开 云交付的防火墙管理中心 页面。

以下是在新选项卡中打开 云交付的防火墙管理中心 门户页面的一些示例：

- 选择 **工具和服务** > **防火墙管理中心**。

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

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

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

- 选择 **控制面板** > **快速操作**。

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

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

设备和服务管理

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

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

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

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

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

在 CDO 中更改设备的 IP 地址

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

要更改 CDO 用于与设备通信的 IP 地址，请执行以下程序：

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击设备类型选项卡。

您可以使用 过滤器 和 搜索 功能查找所需的设备。

步骤 4 选择要更改其 IP 地址的设备。

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

步骤 6 在字段中输入新的 IP 地址，然后点击蓝色的复选按钮。

设备本身不会发生更改，因此设备的配置状态将继续显示已同步。

相关信息：

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

在 CDO 中更改设备的名称

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

Procedure

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

步骤 2 点击**设备 (Device)** 选项卡以找到设备。

步骤 3 选择要更改其名称的设备。

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

步骤 5 在字段中输入新的名称，然后点击蓝色的复选按钮。

设备本身不会发生更改，因此设备的配置状态将继续显示已同步。

导出设备和服务列表

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

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

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

Procedure

步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

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

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

您可以使用 过滤器 和 搜索 功能查找所需的设备。

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

步骤 5 如果出现提示，请保存 .csv 文件。

步骤 6 在电子表格应用中打开 .csv 文件，对结果进行排序和过滤。

导出设备配置

一次只能导出一个设备配置。使用以下程序将设备的配置导出到 JSON 文件：

过程

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

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

步骤 3 点击设备类型选项卡。

您可以使用 过滤器 和 搜索 功能查找所需的设备。

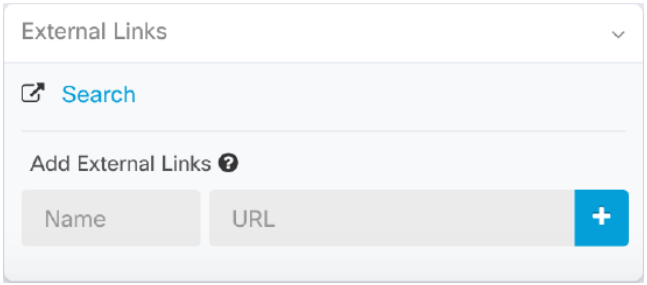
步骤 4 选择所需的设备以便将其突出显示。

步骤 5 在操作窗格中，选择导出配置。

步骤 6 选择确认以将配置另存为 JSON 文件。

设备的外部链接

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



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

位置变量

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

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

或 FTD 托管设备的 FDM。

相关信息：

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

从您的设备创建外部链路

Procedure

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

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

步骤 3 点击设备类型选项卡。

步骤 4 选择设备或型号。

您可以使用 过滤器 和 搜索 功能查找所需的设备。

步骤 5 在右侧的详细信息窗格中，转到**外部链接**部分。

步骤 6 输入链接的名称。

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

步骤 8 点击 + 将链接与设备关联。

创建到 ASDM FDM 的外部链路

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

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

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

步骤 3 点击设备类型选项卡。

您可以使用 过滤器 和 搜索 功能查找所需的设备。

步骤 4 选择设备或型号。

步骤 5 在右侧的详细信息窗格中，转到“外部链接”部分。

步骤 6 输入链路的名称，例如 ASDM FDM。

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

步骤 8 点击 + 框。

为多个设备创建外部链路

Procedure

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

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

步骤 3 点击设备类型选项卡。

您可以使用过滤器和搜索功能来查找所需的设备。

步骤 4 请选择多个设备或型号。

步骤 5 在右侧的详细信息窗格中，转到“外部链接”部分。

步骤 6 输入链接的名称。

步骤 7 使用以下方法之一输入要访问的 URL：

- 输入

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

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

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

步骤 8 点击 + 将链接与设备关联。

编辑或删除外部链接

Procedure

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

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

步骤 3 点击设备类型选项卡。

您可以使用 过滤器 和 搜索 功能查找所需的设备。

步骤 4 选择设备或型号。

步骤 5 在右侧的详细信息窗格中，转到“外部链接”部分。

步骤 6 将鼠标悬停在链接名称上可显示编辑和删除图标。

步骤 7 点击相应的图标可编辑或删除外部链接，并确认您的操作。

编辑或删除多台设备的外部链接

Procedure

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

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

步骤 3 点击设备类型选项卡。

您可以使用过滤器和搜索功能来查找所需的设备。

步骤 4 请选择多个设备或型号。

步骤 5 在右侧的详细信息窗格中，转到**外部链接**部分。

步骤 6 将鼠标悬停在链接名称上可显示编辑和删除图标。

步骤 7 点击相应的图标可编辑或删除外部链接，并确认您的操作。

将设备批量重新连接到 CDO

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

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

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击设备类型选项卡。

使用过滤器查找连接状态为“无法访问”的设备。

步骤 4 从过滤结果中，选择要尝试重新连接的设备。

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

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

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

在租户之间移动设备

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

编写设备说明

使用此程序为设备创建单个纯文本注释文件。

Procedure

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

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

步骤 3 点击设备类型选项卡。

步骤 4 选择要为其创建备注的设备或型号。

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

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

步骤 7 编辑“备注”(Notes) 页面。

步骤 8 点击**保存 (Save)**。
注释会被保存在选项卡中。

查看资产页面信息

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

您可以在此页面上查看以下详细信息：

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

标签和过滤

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

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

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

将标签应用于设备和对象

要将标签应用于设备，请执行以下步骤：

过程

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

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

步骤 3 点击设备类型选项卡。

步骤 4 在生成的表中选择一个或多个设备或型号。

步骤 5 在右侧的添加组和标签字段中，指定设备的标签。

步骤 6 点击蓝色 + 图标。

过滤器

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

要过滤，请点击设备和服务、策略和对象选项卡的左侧窗格中的 ：

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

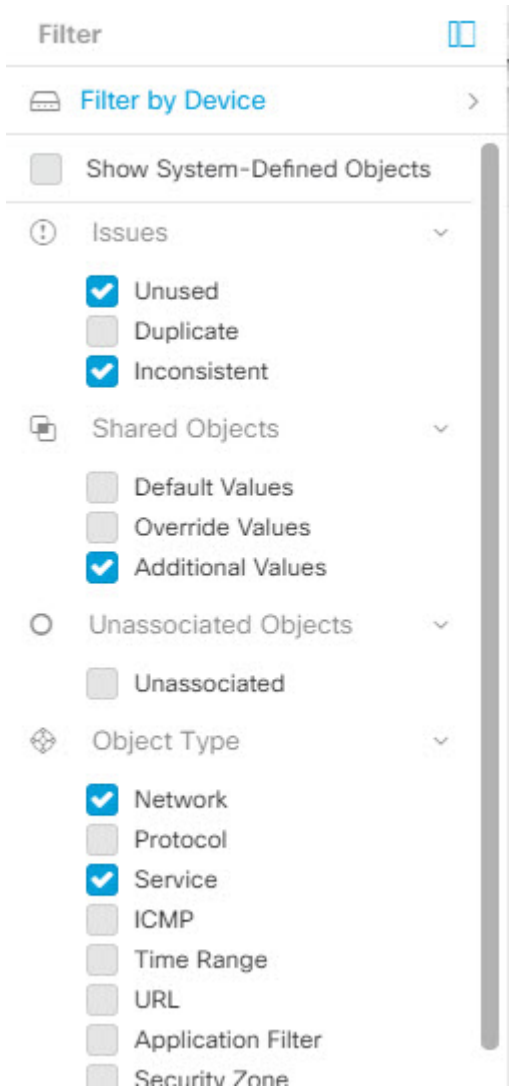
注释 打开 **FTD** 选项卡时，过滤器窗格将提供过滤器，以根据从 CDO 访问设备的管理应用来显示 FDM 管理 设备。

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

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

过滤设备和对象时，您可以组合搜索词来创建多个潜在的搜索策略来查找相关结果。

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



查找所有使用相同 SDC 连接到 CDO 的设备

请按照以下程序识别所有使用相同 SDC 连接到 CDO 的设备：

Procedure

步骤 1 在导航栏中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击设备类型选项卡。

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

步骤 5 点击过滤器按钮  以展开过滤器菜单。

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

步骤 7 （可选）检查过滤器菜单中的其他过滤器，以便进一步细化搜索。

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

搜索

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

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

Procedure

步骤 1 导航到界面顶部附近的搜索栏。

步骤 2 在搜索栏中键入搜索条件，系统将显示相应的结果。

Global Search

通过全局搜索功能，您可以快速查找并导航至 管理的设备。CDO

所有搜索结果都基于您选择的索引选项。索引选项如下：

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

  有关详细信息，请参阅启动完全索引，第 94 页。

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

您在搜索字段中输入的信息不区分大小写。您可以使用以下实体执行全局搜索：

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

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

- 访问控制策略
- 预过滤器策略
- 威胁防御 NAT 策略

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

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

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

注释

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

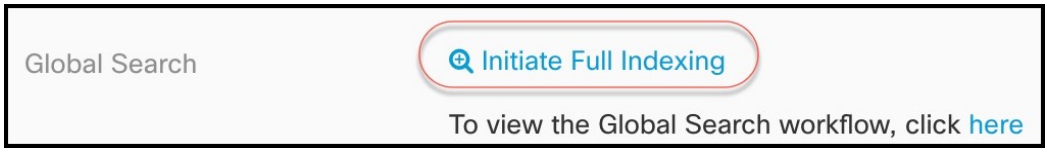
启动完全索引

过程

步骤 1 使用具有管理员或超级管理员权限的帐户登录 CDO。

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

步骤 3 在全局搜索中，点击启动完整索引以触发索引。



注释 启动完整索引会清除 CDO 租户的现有索引。

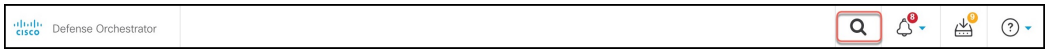
步骤 4 点击此处查看全局搜索工作流程。

执行全局搜索

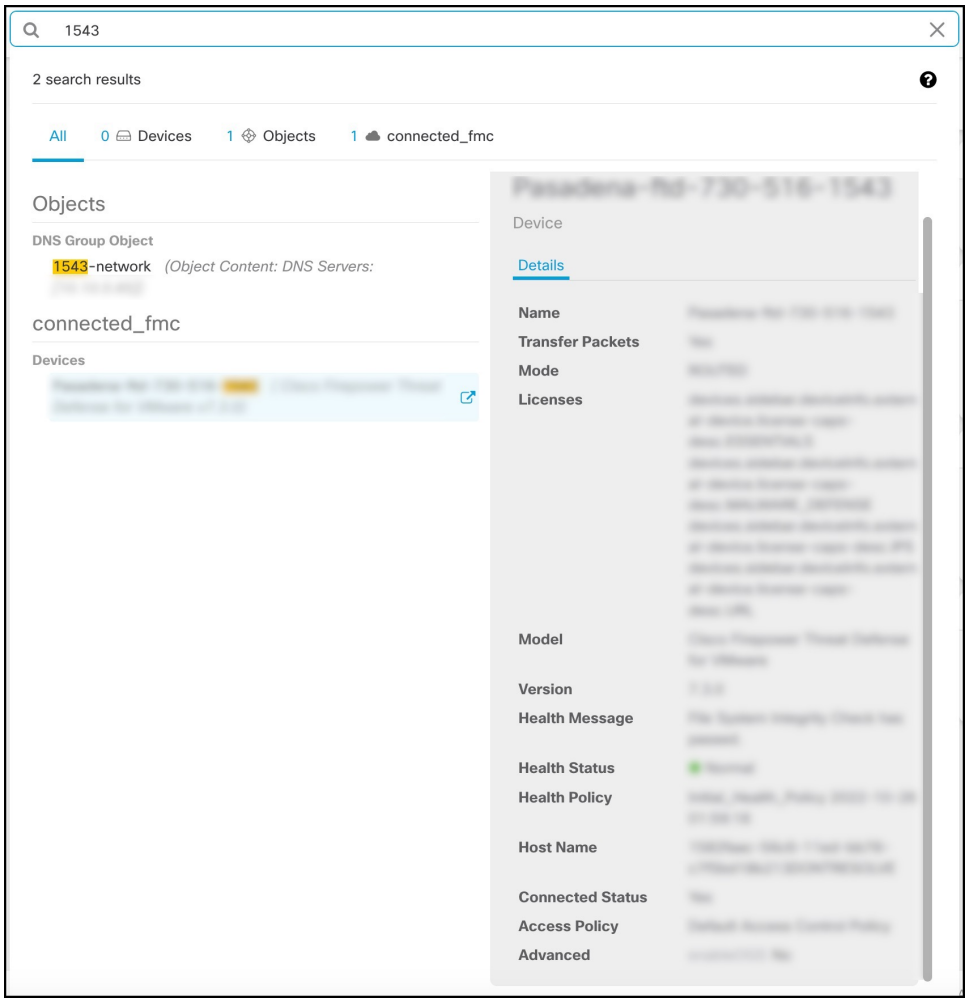
过程

步骤 1 登录至 CDO。

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



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



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

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

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

步骤 4 点击 **X** 关闭搜索栏。

CDO 命令行接口

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

相关信息：

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

使用命令行接口

Procedure

步骤 1 打开**资产 (Inventory)** 页面。

步骤 2 点击资产表上方的设备按钮。

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

步骤 4 选择设备。

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

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

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

Note 如果可以运行的命令有限制，则会在命令窗格上方列出这些限制。

Related Topics

在命令行接口中输入命令 ， 第 97 页

在命令行接口中输入命令

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

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

使用命令历史记录

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

Procedure

步骤 1 在资产页面上，选择要配置的设备。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

步骤 3 点击设备类型选项卡。

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

步骤 5 点击时钟图标可展开历史记录窗格（如果尚未展开）。

步骤 6 在历史记录窗格中选择要修改或重新发送的命令。

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

Note CDO 显示 Done!两种情况下响应窗格中的消息：

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

批量命令行接口

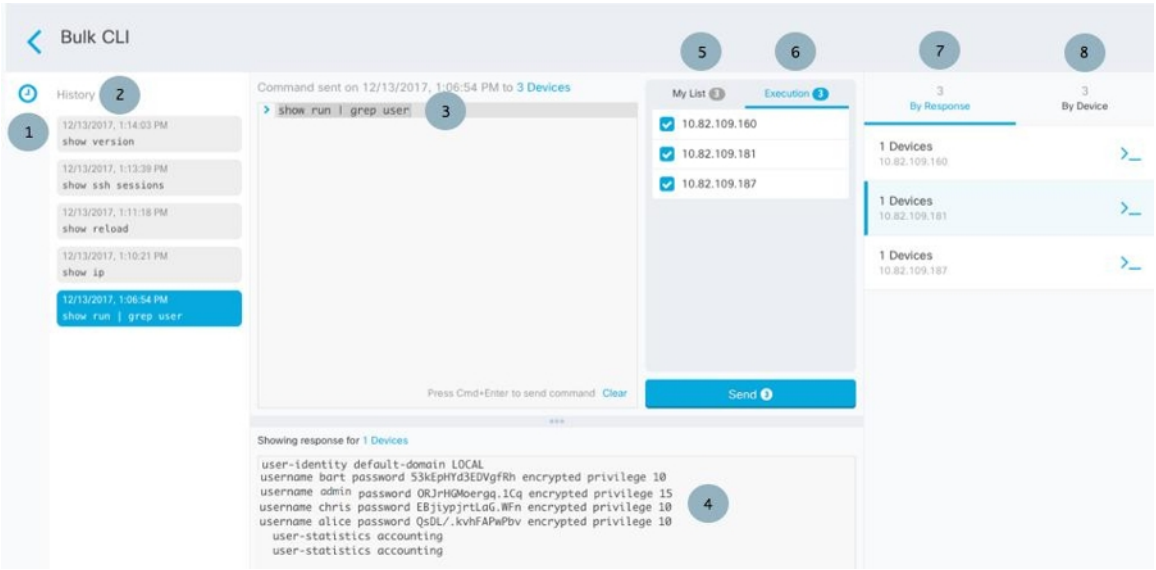
CDO 为用户提供使用命令行接口 (CLI) 管理 Secure Firewall ASA、FDM 管理 威胁防御、SSH、Cisco IOS 和 Cisco Secure Firewall Cloud Native设备。用户可以将命令发送到单个设备或同时发送到多个同类设备。本节介绍一次向多台设备发送 CLI 命令。

相关信息：

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

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

批量 CLI 接口



Note CDO 显示 Done!两种情况下的消息：

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

编号	说明
1	点击时钟可展开或折叠命令历史记录窗格。

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

批量发送命令

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡以找到设备。

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

步骤 4 选择设备。

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

步骤 6 您可以在“我的列表”字段中选中或取消选中要向其发送命令的设备。

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

使用批量命令历史记录

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

Procedure

步骤 1 在导航栏中，点击**资产 (Inventory)**。

步骤 2 点击 **设备** 选项卡以找到设备。

步骤 3 点击相应的设备类型选项卡，然后点击过滤器图标以查找要配置的设备。

步骤 4 选择设备。

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

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

步骤 7 查看我的列表选项卡，确保您要发送的命令将发送到您期望的设备。

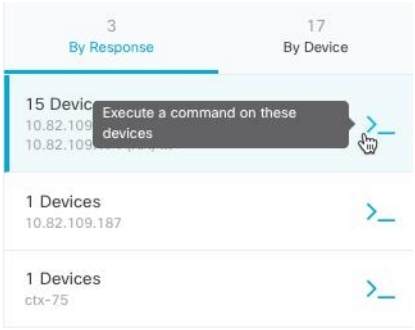
步骤 8 在命令窗格中编辑命令，然后点击发送。CDO 在响应窗格中显示命令的结果。

使用批量命令过滤器

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

按响应过滤器

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



要将命令发送到与命令响应关联的设备列表，请执行以下程序：

Procedure

步骤 1 点击 By Response 选项卡中一行中的命令符号。

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

步骤 3 查看从命令收到的响应。

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

按设备过滤器

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

要在同一设备列表上运行命令，请执行以下程序：

Procedure

步骤 1 点击**按设备 (By Device)** 选项卡。

步骤 2 点击 >_ 在这些设备上执行命令。

步骤 3 点击清除以清除命令窗格并输入新命令。

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

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

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

用于管理设备的 CLI 宏

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

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

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

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

Note 只有在设备载入 CDO 后，才能为设备创建宏。

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

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

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

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

您可以随意命名参数。您还可以使用此参数名称创建相同的宏：

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

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

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

命令的一部分，必须对要向其发送命令的设备使用正确的 CLI 语法。

从新命令创建 CLI 宏

Procedure

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

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

步骤 2 在导航栏中，点击**清单 (Inventory)**。

步骤 3 点击 **设备 (Devices)**选项卡以找到设备。

步骤 4 点击相应的设备类型选项卡，然后选择在线和同步的设备。

步骤 5 点击 **>_Command Line Interface**。

步骤 6 点击 CLI 宏收藏夹星标 ，以查看已经存在的宏。

步骤 7 点击加号按钮 。

步骤 8 请为宏指定唯一的名称。如果需要，请为 CLI 宏提供说明和注释。

步骤 9 在**命令 (Command)** 字段中输入完整命令。

步骤 10 运行命令时，将要修改的命令部分替换为用大括号括起来的参数名称。

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

要运行命令，请参阅运行 CLI 宏。

从 CLI 历史记录或现有 CLI 宏创建 CLI 宏

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

过程

步骤 1 在导航栏中，点击 **设备和服务**。

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

步骤 2 点击**设备**选项卡。

步骤 3 点击相应的设备类型选项卡，然后选择在线和同步的设备。

步骤 4 点击 **>_命令行接口**。

步骤 5 查找要生成 CLI 宏的命令，然后选择该命令。使用以下方法之一：

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

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

步骤 7 请为宏指定唯一的名称。如果需要，请为 CLI 宏提供说明和注释。

步骤 8 查看命令字段中的命令，并进行所需的更改。

步骤 9 运行命令时，将要修改的命令部分替换为用大括号括起来的参数名称。

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

要运行命令，请参阅运行 CLI 宏。

运行 CLI 宏

Procedure

步骤 1 在导航栏中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击相应的设备类型选项卡，然后选择一个或多个设备。

步骤 4 点击 **>_命令行接口**。

步骤 5 在命令面板中，点击星号 ★。

步骤 6 从命令面板中选择 CLI 宏。

步骤 7 使用以下两种方式之一运行宏：

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

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

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

- 对于 FTD，会更新设备的活动配置。

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

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

编辑 CLI 宏

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

Procedure

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

有关如何运行 CLI 宏的说明，请参阅运行 CLI 宏。

删除 CLI 宏

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

Procedure

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

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

步骤 6 选择要删除的用户定义的 CLI 宏。

步骤 7 点击 CLI 宏标签中的垃圾桶图标 。

步骤 8 确认要删除 CLI 宏。

命令行接口文档

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

导出 CLI 命令结果

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

- 设备
- 日期
- 用户
- 命令
- 输出

导出 CLI 命令结果

您可以将刚刚在命令窗口中执行的命令的结果导出到 .csv 文件：

Procedure

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

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备，使其突出显示。

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

步骤 6 在命令行界面窗格中，输入命令并点击发送以向设备发出命令。

步骤 7 在已输入命令的窗口右侧，点击导出图标。

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

导出 CLI 宏的结果

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

Procedure

步骤 1 打开 **设备和服务** 页面。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备，使其突出显示。

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

步骤 6 在 CLI 窗口的左侧窗格中，选择 CLI 宏收藏夹星型。

步骤 7 点击要导出的宏命令。填写任何适当的参数，然后点击发送。

步骤 8 在已输入命令的窗口右侧，点击导出图标。

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

导出 CLI 命令历史记录

使用以下程序将一个或多个设备的 CLI 历史记录导出到 .csv 文件：

Procedure

步骤 1 在导航窗格中，点击 **设备和服务**。

步骤 2 点击**设备**选项卡。

步骤 3 点击适当的设备类型选项卡。

步骤 4 选择一个或多个设备，使其突出显示。

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

步骤 6 如果历史记录窗格尚未展开，请点击时钟图标将其展开。

步骤 7 在已输入命令的窗口右侧，点击导出图标。

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

相关信息：

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

导出 CLI 宏列表

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

过程

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

对象

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

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

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

有时，共享对象会产生一些“问题”，并且不再在多个策略或设备之间完美共享：

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

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

您可以通过导航至对象菜单或在网络策略的详细信息中查看对象来查看对象。CDO

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

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

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

对象类型

下表介绍您可以为设备创建和使用 CDO 管理的对象。

Table 5: FDM 托管设备对象类型

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

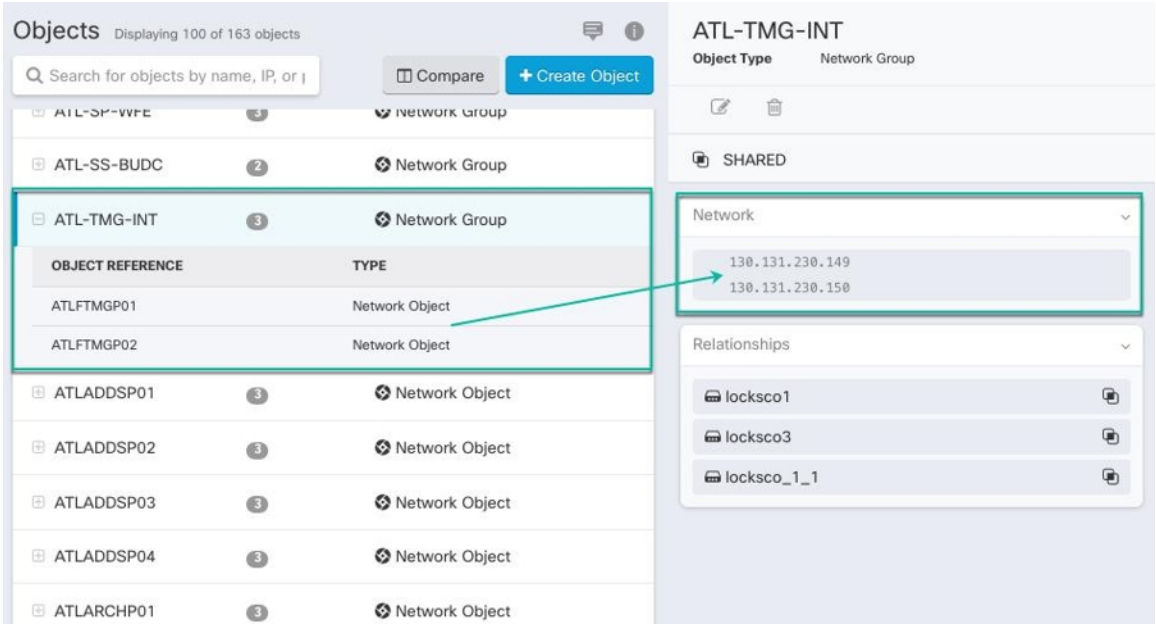
对象	说明
创建 SGT 组	SGT 动态对象根据 ISE 分配的 SGT 识别源或目标地址，然后可以与传入流量进行匹配。
系统日志服务器对象	系统日志服务器对象标识可接收面向连接的消息或诊断系统日志（系统日志）消息的服务器。
URL 对象	使用 URL 对象和组（统称为“URL 对象”）可定义 Web 请求的 URL 或 IP 地址。可以使用这些对象在访问控制策略中执行手动URL过滤，或在安全情报策略中进行阻止。

共享对象

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

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

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

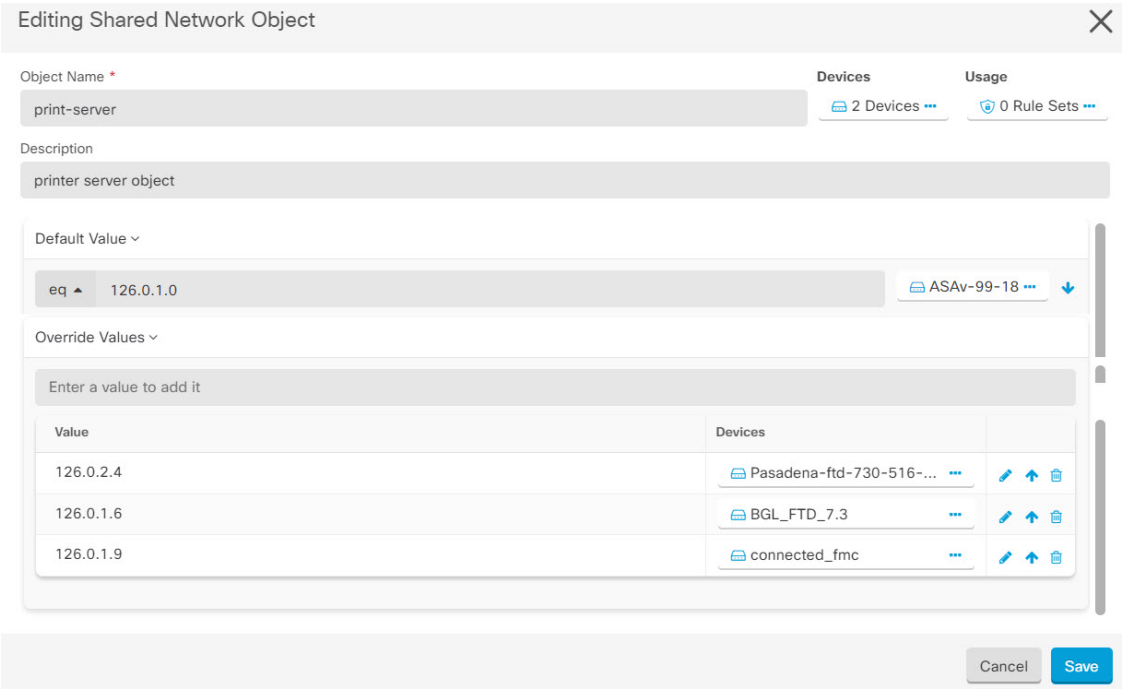


对象覆盖

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

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

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



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

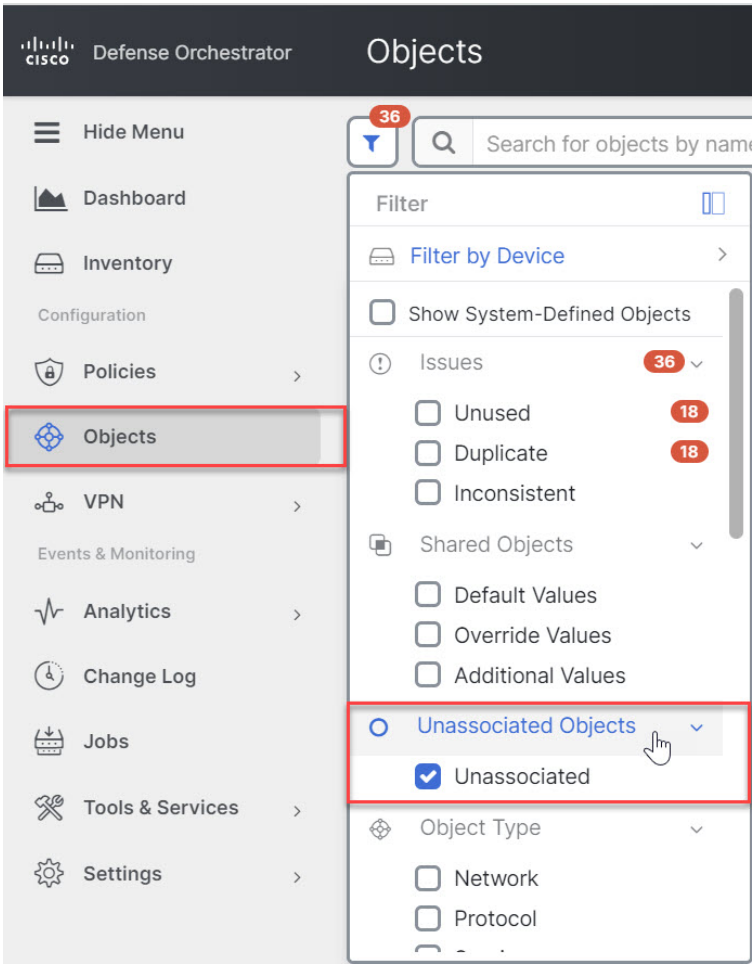
Note 如果存在不一致的对象，您可以将它们合并为一个具有覆盖的共享对象。有关详细信息，请参阅解决不一致的对象问题。

未关联的对象

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

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

要查看未关联的对象，请点击对象选项卡的左侧窗格，然后选中未关联的复选框。



比较对象

Procedure

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

步骤 2 过滤页面上的对象以查找要比较的对象。

步骤 3 点击**比较**按钮 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。

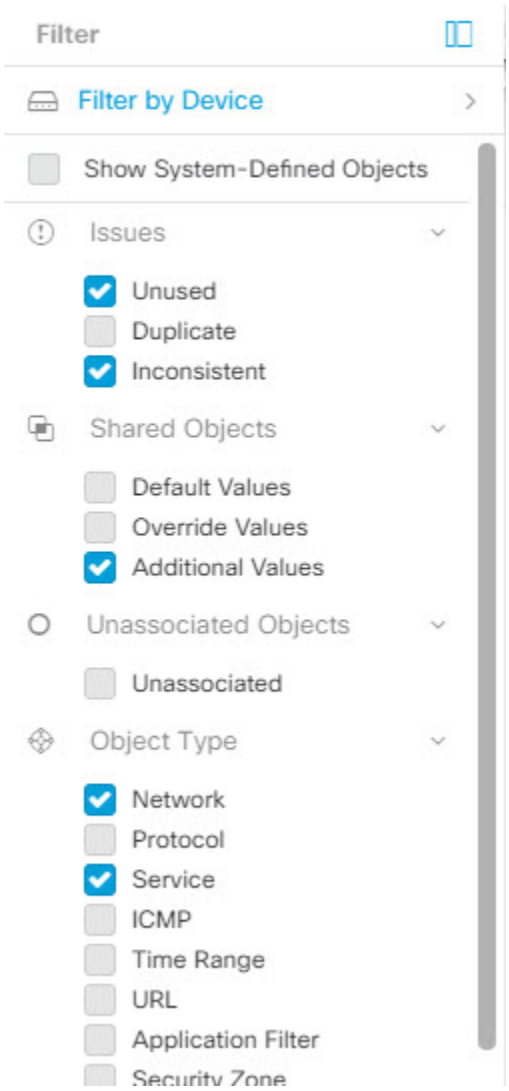
注释 打开 **FTD** 选项卡时，过滤器窗格将提供过滤器，以根据从 CDO 访问设备的管理应用来显示 FDM 管理 设备。

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

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

过滤设备和对象时，您可以组合搜索词来创建多个潜在的搜索策略来查找相关结果。

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



对象过滤器

要过滤，请点击“对象”(Objects) 选项卡的左侧窗格的 ：

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

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

此过滤器栏中的选定过滤器将返回与以下条件匹配的对象：

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

*** 不一致** 对象 AND 是

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

***** 包含**"组"** 在对象命名约定中

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

显示系统对象过滤器

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

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

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

配置对象过滤器

您可以根据需要过滤任意数量的条件。过滤所依据的类别越多，预期的结果就越少。

Procedure

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

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

步骤 3 如果要将结果限制为在特定设备上找到的结果，请执行以下操作：

a. 点击**按设备过滤 (Filter By Device)**。

b. 搜索所有设备或点击设备选项卡以仅搜索特定类型的设备。

c. 选中要包含在过滤条件中的设备。

d. 点击**确定 (OK)**。

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

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

步骤 6 如果要查看存在问题但被管理员忽略的对象，请选中**已忽略 (Ignored)** 的问题。

步骤 7 如果要过滤两台或多台设备之间共享的对象，请在**共享对象 (Shared Objects)** 中选中所需的过滤器。

- **默认值 (Default Values)**：过滤仅具有默认值的对象。
- **覆盖值 (Override Values)**：过滤具有覆盖值的对象。

- **其他值 (Additional Values)**：过滤具有其他值的对象。

步骤 8 如果要过滤不属于任何规则或策略的对象，请选中**未关联 (Unassociated)** 。

步骤 9 选中要作为过滤依据的**对象类型 (Object Types)**。

步骤 10 您还可以将对象名称、IP 地址或端口号添加到对象搜索字段，以在过滤结果中查找符合搜索条件的对象。

何时从过滤条件中排除设备

将设备添加到过滤条件时，结果会显示设备上的对象，但不会显示这些对象与其他设备的关系。例如，假设 ObjectA 在 ASA1 和 ASA2 之间共享。如果要过滤对象以查找 ASA1 上的共享对象，则会找到 ObjectA，但“关系”窗格只会显示该对象位于 ASA1 上。

要查看与对象相关的所有设备，请不要在搜索条件中指定设备。按其他条件过滤并添加搜索条件（如果您愿意）。选择CDO识别的对象，然后在“关系”窗格中进行查看。您将看到与对象相关的所有设备和策略。

忽略对象

解决具有未使用、重复或不一致问题对象的方法之一是忽略它们。您可以决定，尽管对象未使用、重复或不一致，但该状态存在正当理由，并且您选择不解决对象问题。解决未使用的对象问题解决重复对象问题解决不一致的对象问题在未来的某个时候，您可能希望解析这些被忽略的对象。由于CDO在搜索对象问题时不显示已忽略的对象，因此您需要过滤已忽略对象的对象列表，然后对结果执行操作。

Procedure

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

步骤 2 过滤和搜索被忽略的对象。对象过滤器, on page 115

步骤 3 在**对象 (Object)** 表中，选择要取消忽略的对象。一次可以取消忽略一个对象。

步骤 4 点击详细信息窗格中的取消忽略。

步骤 5 确认您的请求。现在，当您按问题过滤对象时，您应该会找到以前忽略的对象。

删除对象

可以删除单个对象或多个对象。

删除单个对象

Caution 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure

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

步骤 2 使用对象过滤器和搜索字段找到要删除的对象，然后将其选中。

步骤 3 查看关系窗格。如果在策略或对象组中使用了对象，则在将其从该策略或组中删除之前，无法删除该对象。

步骤 4 点击“操作”(Actions) 窗格中，点击**编辑**图标 。

步骤 5 点击确定，确认要删除对象。

步骤 6 查看并部署您所做的更改，或等待并一次部署多个更改。

删除一组未使用的对象

当您载入设备并开始解决对象问题时，您会发现许多未使用的对象。一次最多可以删除50个未使用的对象。

过程

步骤 1 使用问题过滤器查找未使用的对象。您还可以使用设备过滤器通过选择无设备来查找未与设备关联的对象。过滤对象列表后，系统将显示对象复选框。

步骤 2 选中对象表标题中的全选复选框，以选择过滤器找到的显示在对象表中的所有对象；或者，选中要删除的各个对象的各个复选框。

步骤 3 点击“操作”(Actions) 窗格中，点击**编辑**图标 。

步骤 4 立即查看并部署您所做的更改，或等待并一次部署多个更改。

网络对象

网络对象 可以包含主机、网络 IP 地址、IP 地址范围、完全限定域名 (FQDN)或用 CIDR 符号表示的子网 。**网络组**是添加到组中的网络对象和其他单个地址或子网络的集合。网络对象和网络组用于访问规则、网络策略和 NAT 规则。您可以使用 CDO 创建、更新和删除网络对象和网络组。

Table 6: 网络对象的允许值

设备类型	**IPv4 / IPv6**	单个地址	地址范围	域名名称	使用 **CIDR** 表示法的子网。
FTD	IPv4 和 IPv6	是	是	是	是

Table 7: 网络组允许的内容

设备类型	**IP** 值	网络对象	网络组
FTD	不支持	是	是

跨产品重用网络对象

如果您的 思科防御协调器 租户具有云交付的防火墙管理中心：

在创建 Secure Firewall Threat Defense、FDM 管理 威胁防御、ASA 或 Meraki 网络对象或组时，对象的副本也会被添加到在配置 云交付的防火墙管理中心 时使用的**对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的对象列表中。

对任一页面上的网络对象或组所做的更改适用于两个页面上的对象或组实例。从一个页面删除对象也会从另一个页面删除该对象的相应副本。

例外情况：

- 如果 云交付的防火墙管理中心 已存在同名的网络对象，则不会在 思科防御协调器 的**对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上复制新的 Secure Firewall Threat Defense、FDM 管理 威胁防御、ASA 或 Meraki 网络对象
- 由本地 Cisco Secure Firewall Management Center 管理的载入 威胁防御 设备中的网络对象和组不会复制到**对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面，因此无法在 云交付的防火墙管理中心 中使用。

  请注意，对于已迁移到 云交付的防火墙管理中心 的本地 Cisco Secure Firewall Management Center 实例，如果在部署到 FTD 设备的策略中使用网络对象和组，它们将被复制到 CDO 对象页面。
- 新租户上会自动启用在 CDO 和 云交付的防火墙管理中心 之间共享网络对象，但现有租户必须另行请求。如果您的网络对象未与 云交付的防火墙管理中心 共享，请联系 TAC 以在您的租户上启用这些功能。

查看网络对象

使用 CDO 创建的网络对象以及已载入的设备配置中的 CDO 识别的网络对象会显示在对象页面上。它们标有对象类型。这使您可以按对象类型进行过滤，以快速找到要查找的对象。

在“对象”(Objects) 页面上选择网络对象时，您可在“详细信息”(Details) 窗格中看到该对象的值。“关系”(Relationships) 窗格显示对象是否用于策略中，以及对象存储在什么设备上。

在点击网络组时，您会看到该组的内容。网络组是网络对象为其提供的所有值的综合体。

相关信息：

- 创建或编辑 Firepower 网络对象或网络组

创建或编辑 Firepower 网络对象或网络组

Firepower 网络对象可以包含以 CIDR 表示法表示的主机名、IP 地址或子网地址。**网络组**是在访问规则、网络策略和NAT规则中使用的网络对象和网络组的集合。您可以使用 思科防御协调器(CDO)来创建、读取、更新和删除网络对象和网络组。

Firepower 网络对象和组可供 ASA、威胁防御、FDM 管理 和 Meraki 设备使用。请参阅跨产品重用网络对象, on page 119。

Note 如果 云交付的防火墙管理中心 被部署在您的租户上：

在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上创建网络对象或组时，对象的副本会自动添加到 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面，反之亦然。

Caution 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Table 8: 可以添加到网络对象的 ***IP*** 地址

设备类型	IPv4 / IPv6	单个地址	地址范围	部分限定域名 (PQDN)	使用 CIDR 表示法的子网。
FirePower	IPv4 / IPv6	是	是	是	是

相关信息：

- 编辑 Firepower 网络对象, on page 121
- 编辑 Firepower 网络对象, on page 123

- 向共享网络组添加其他值, on page 125
- 编辑共享网络组中的其他值, on page 127

编辑 Firepower 网络对象

Note 如果 云交付的防火墙管理中心 被部署在您的租户上：

在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上创建网络对象或组时，对象的副本会自动添加到 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面，反之亦然。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮  以创建新的对象。

步骤 3 点击**FTD** > **网络 (Network)**。

步骤 4 输入 **对象名称**。

步骤 5 选择 **创建网络对象**。

步骤 6 在**值 (Value)** 部分中：

- 选择 **eq** 并输入以 CIDR 表示法表示的单个 IP 地址、子网地址或部分限定域名 (PQDN)。
- 选择**范围**并输入 IP 地址范围。

Note 请勿设置主机位值。如果输入的主机位值不是 0，CDO 会在创建对象时取消设置，因为云交付的防火墙管理中心 仅接受未设置主机位的 IPv6 对象。

步骤 7 点击**添加 (Add)**。

注意：新创建的网络对象不与任何 FDM 管理 设备关联，因为它们不属于任何规则或策略。要查看这些对象，请在对象过滤器中选择**未关联**的对象类别。有关详细信息，请参阅配置对象过滤器。在设备的规则或策略中使用未关联的对象后，此类对象将与该设备关联。

创建 Firepower 网络组

网络组可以包含网络对象和网络组。创建新的网络组时，可以按名称、IP 地址、IP 地址范围或 FQDN 搜索现有对象，并将其添加到网络组。如果对象不存在，您可以立即在同一接口中创建该对象并将其添加到网络组。

Note 如果 云交付的防火墙管理中心 被部署在您的租户上：

在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上创建网络对象或组时，对象的副本会自动添加到 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面，反之亦然。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮 以创建新的对象。

步骤 3 点击**FTD** > **网络 (Network)**。

步骤 4 输入 **对象名称**。

步骤 5 选择创建网络组。

步骤 6 在**值 (Values)** 字段中输入值或名称。当您开始输入时，CDO 会提供与您的条目匹配的对象名称或值。

步骤 7 您可以选择一个显示的现有对象，也可以根据输入的名称或值创建一个新对象。

步骤 8 如果 CDO 找到了匹配项，要选择现有对象，请点击**添加 (Add)** 将网络对象或网络组添加到新网络组。

步骤 9 如果输入的值或对象不存在，则可以执行以下操作之一：

- 点击**添加为此名称的新对象 (Add as New Object With This Name)**，以创建具有该名称的新对象。输入一个值，然后点击复选标记将其保存。
- 点击**添加为新对象 (Add as New Object)** 以创建一个新对象。对象名称和值相同。输入名称，然后点击复选标记将其保存。

即使该值已存在，也可以创建一个新对象。您可以对这些对象进行更改并将它们保存。

注意：您可以点击编辑图标修改详细信息。点击“删除”按钮不会删除对象本身；相反，它会将其从网络组中删除。

步骤 10 添加所需的对象后，点击保存以创建新的网络组。

步骤 11 预览并部署所有设备的配置更改。

编辑 Firepower 网络对象

Caution 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的对象。

步骤 3 选择网络对象，然后点击**操作 (Actions)** 窗格中的编辑图标 。

步骤 4 以在“创建 Firepower 网络组”(Create a Firepower Network Group) 中创建值的相同方式编辑对话框中的值。

Note 点击旁边的删除图标，从网络组中删除对象。

步骤 5 点击**保存 (Save)**。CDO 会显示将受更改影响的设备。

步骤 6 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

编辑 Firepower 网络组

Caution 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到您要编辑的网络组。

步骤 3 选择网络组，然后点击**操作 (Actions)** 窗格中的编辑图标 。

步骤 4 如有必要，更改对象名称和说明。

步骤 5 如果要更改已添加到网络组的对象或网络组，请执行以下步骤：

a. 点击对象名称或网络组旁边的编辑图标可对其进行修改。

b. 点击复选标记以保存更改。**注意**：您可以点击删除图标从网络组中删除该值。

步骤 6 如果要向此网络组添加新的网络对象或网络组，必须执行以下步骤：

a. 在值字段中，输入新值或现有网络对象的名称。当您开始输入时，CDO 会提供与您的条目匹配的对象名称或值。您可以选择一个显示的现有对象，也可以根据输入的名称或值创建一个新对象。

b. 如果 CDO 找到了匹配项，要选择现有对象，请点击**添加 (Add)** 将网络对象或网络组添加到新网络组。

c. 如果输入的值或对象不存在，则可以执行以下操作之一：

- 点击**添加为此名称的新对象 (Add as New Object With This Name)**，以创建具有该名称的新对象。输入一个值，然后点击复选标记将其保存。
- 点击**添加为新对象 (Add as New Object)** 以创建一个新对象。对象名称和值相同。输入名称，然后点击复选标记将其保存。

即使该值已存在，也可以创建一个新对象。您可以对这些对象进行更改并将它们保存。

步骤 7 点击**保存 (Save)**。CDO 显示将受更改影响的策略。

步骤 8 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

步骤 9 预览并部署所有设备的配置更改。

添加对象覆盖

注意 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

过程

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到具有要编辑的覆盖的对象。

步骤 3 选择网络对象，然后点击**操作 (Actions)** 窗格中的编辑图标 。

步骤 4 在**覆盖值 (Override Values)** 对话框中输入值，然后点击 **+ 添加值 (+ Add Value)**。

重要事项 要添加的覆盖必须具有与对象所包含的值类型相同。例如，对于网络对象，只能使用网络值而不是主机值来配置覆盖。

步骤 5 看到添加的值后，点击**覆盖值 (Override Values)** 的**设备 (Devices)** 列中的单元格。

步骤 6 点击**添加设备 (Add Devices)**，然后选择要向其添加覆盖的设备。您选择的设备必须包含要向其添加覆盖的对象。

步骤 7 点击**保存 (Save)**。CDO 会显示将受更改影响的设备。

步骤 8 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的覆盖添加。

注释 您可以向一个对象添加多个覆盖。但每次添加覆盖时，都必须选择包含对象的不同设备。

步骤 9 请参阅对象覆盖，第 112 页，了解有关对象覆盖和编辑对象覆盖，第 125 页的详细信息以编辑现有覆盖。

编辑对象覆盖

只要设备上存在对象，您就可以修改现有覆盖的值。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到具有要编辑的覆盖的对象。

步骤 3 选择带有覆盖的对象，然后点击“操作”(Actions) 窗格中的编辑图标  。

步骤 4 修改覆盖值：

- 点击编辑图标以修改值。
- 在**覆盖值 (Override Values)** 中点击**设备 (Devices)** 列，以便分配新设备。您可以选择已分配的设备，然后点击**删除覆盖 (Remove Overrides)** 以删除该设备上的覆盖。
- 点击**覆盖值 (Override Values)** 中的 箭头，将其推送并设置为共享对象的默认值。
- 点击要删除的覆盖旁边的删除图标。

步骤 5 点击**保存 (Save)**。CDO 会显示将受更改影响的设备。

步骤 6 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

步骤 7 预览并部署所有设备的配置更改。

向共享网络组添加其他值

共享网络组中与其关联的所有设备上都存在的值被称为“默认值”。CDO 允许您向共享网络组添加“其他值”，并将这些值分配给与该共享网络组关联的某些设备。当CDO将更改部署到设备时，它

会确定内容并将“默认值”推送到与共享网络组关联的所有设备，而“其他值”只会被推送到指定的设备。

例如，假设您的总部有四台 AD 主服务器，那么这些服务器应可从您的所有站点进行访问。因此，您创建了一个名为“Active-Directory”的对象组，以便用于所有站点。现在，您要为其中一个分支机构再添加两台 AD 服务器。为此，您可以通过将其详细信息添加为对象组“Active-Directory”上该分支机构的特定附加值来执行此操作。这两台服务器不参与确定对象“Active-Directory”是一致的还是共享的。因此，您可从所有站点访问四台 AD 主服务器，但分支机构（具有两台附加服务器）可以访问两台 AD 服务器和四台 AD 主服务器。

Note 如果存在不一致的共享网络组，则您可以将它们合并为具有其他值的单个共享网络组。有关详细信息，请参阅解决不一致的对象问题。

Caution 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到您要编辑的共享网络组。

步骤 3 点击**操作 (Actions)** 窗格中的编辑图标 。

- **设备 (Devices)** 字段会显示共享网络组所在的设备。
- **使用情况 (Usage)** 字段会显示与共享网络组关联的规则集。
- **默认值 (Default Values)** 字段将指定默认网络对象及其与创建期间提供的共享网络组关联的值。在此字段旁边，您可以看到包含此默认值的设备数量，您可以点击查看其名称和设备类型。您还可以查看与此值关联的规则集。

步骤 4 在**其他值 (Additional Values)** 字段中输入值或名称。当您开始输入时，CDO 会提供与您的条目匹配的对象名称或值。

步骤 5 您可以选择一个显示的现有对象，也可以根据输入的名称或值创建一个新对象。

步骤 6 如果 CDO 找到了匹配项，要选择现有对象，请点击**添加 (Add)** 将网络对象或网络组添加到新网络组。

步骤 7 如果输入的值或对象不存在，则可以执行以下操作之一：

- 点击**添加为此名称的新对象 (Add as New Object With This Name)**，以创建具有该名称的新对象。输入一个值，然后点击复选标记将其保存。
- 点击**添加为新对象 (Add as New Object)** 以创建一个新对象。对象名称和值相同。输入名称，然后点击复选标记将其保存。

即使该值已存在，也可以创建一个新对象。您可以对这些对象进行更改并将它们保存。

步骤 8 在**设备 (Devices)** 列中，点击与新添加的对象关联的单元格，然后点击**添加设备 (Add Devices)**。

步骤 9 选择所需的设备，然后点击**确定 (OK)**。

步骤 10 点击**保存 (Save)**。CDO 会显示将受更改影响的设备。

步骤 11 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

步骤 12 预览并部署所有设备的配置更改。

编辑共享网络组中的其他值

⚠

Caution 如果 云交付的防火墙管理中心 被部署在您的租户上：

您在 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面上对网络对象和组所做的更改会反映在 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面上的相应的 云交付的防火墙管理中心 网络对象或组中。

从任一页面删除网络对象或组都会从两个页面中删除该对象或组。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到具有要编辑的覆盖的对象。

步骤 3 点击 **操作** 窗格中的编辑图标 。

步骤 4 修改覆盖值：

- 点击编辑图标以修改值。
- 点击**设备 (Devices)** 列中的单元格以分配新设备。您可以选择已分配的设备，然后点击**删除覆盖 (Remove Overrides)** 以删除该设备上的覆盖。
- 点击**默认值 (Default Values)** 中的 箭头，将其设置为共享网络组的其他值。与共享网络组关联的所有设备都会自动分配到该共享网络组。
- 点击**覆盖值 (Override Values)** 中的 箭头，将其推送并设置为共享网络组的默认对象。
- 点击旁边的删除图标，从网络组中删除对象。

步骤 5 点击**保存 (Save)**。CDO 会显示将受更改影响的设备。

步骤 6 点击**确认 (Confirm)** 以完成对对象以及受其影响的任何设备的更改。

步骤 7 预览并部署所有设备的配置更改。

删除网络对象和组

如果 云交付的防火墙管理中心 被部署在您的租户上：

从 或 **对象 (Objects) > FDM 对象 (FDM Objects)** 页面删除网络对象或组都会从 **对象 (Objects) > 其他 FTD 对象 (Other FTD Objects)** 页面中删除复制的对象或组，反之亦然。

应用过滤器对象

应用过滤器对象由 Firepower 设备使用。应用过滤器对象定义 IP 连接中使用的应用，或按类型、类别、标记、风险或业务相关性定义应用的过滤器。您可以在策略中使用这些对象而不是使用端口规格来控制流量。

虽然您可以指定个别应用，但应用过滤器可简化策略创建和管理。例如，您可以创建一条访问控制规则，用于识别并阻止所有业务相关性较低的高风险应用。如果用户尝试使用这些应用中的任何一个，系统会阻止会话。

您可以直接在策略中选择应用和应用过滤器，而不使用应用过滤器对象。但是，如果要为同一组应用或过滤器创建多个策略，使用对象则非常方便。该系统包括多个预定义的应用过滤器，您不能编辑或删除它们。

Note 思科会通过系统和漏洞数据库 (VDB) 更新频繁更改并添加其他应用检测器。因此，阻止高风险应用的规则可自动应用到新应用中，而无需您手动更新规则。

Note 当 FDM 托管的 FTD 设备被载入 CDO 时，它会将应用过滤器转换为应用过滤器对象，而不会更改访问规则或 SSL 解密中定义的规则。由于配置更改，设备的配置状态更改为“未同步”，需要从 CDO 进行配置部署。通常，在您手动保存过滤器之前，FDM 不会将应用过滤器转换为应用过滤器对象。

相关信息：

- 创建和编辑 Firepower 应用过滤器对象
- 删除对象

创建和编辑 Firepower 应用过滤器对象

应用过滤器对象允许您以精选应用或由过滤器识别的一组应用为目标。此应用过滤器对象可用于策略中。

创建 Firepower 应用过滤器对象

要创建应用过滤器对象，请执行以下程序：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

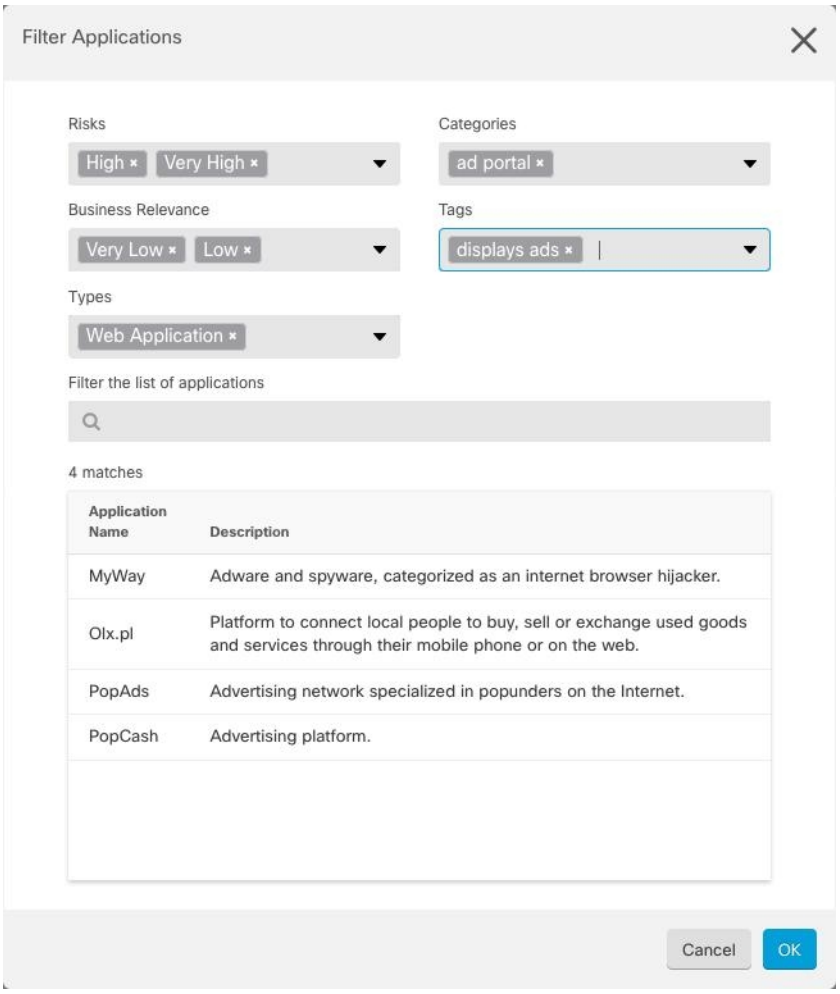
步骤 2 点击创建对象 > FTD > 应用服务。

步骤 3 输入对象的 **对象名称** 和 **说明**（后者为可选项）。

步骤 4 点击**添加过滤器 (Add Filter)**，然后选择要添加到对象的应用程序和过滤器。

初始列表将在连续滚动的列表中显示应用。点击**高级过滤器 (Advanced Filter)** 可查看过滤器选项，可更加方便地查看和选择应用。完成选择后，点击**添加 (Add)**。您可以重复该过程，以添加更多应用或过滤器。

Note 单个过滤器条件中的多个选项具有 OR 关系。例如，风险高 OR 非常高。过滤器之间的关系是 AND，因此是风险高 OR 非常高，AND 业务相关性低 OR 非常低。在选择过滤器时，显示屏中的应用列表更新，只显示符合条件的应用。您可以使用这些过滤器来帮助查找要单独添加的应用，或确认是否要选择所需的过滤器以添加到规则中。



风险 (Risks)：应用所用的用途可能违反组织安全策略的可能性，从非常低到非常高。

业务相关性 (Business Relevance)：在组织的业务运营环境（非娱乐性）下使用应用的可能性，从非常低到非常高。

类型 (Types)：应用类型。

- **应用协议 (Application Protocol)**：应用协议（例如 HTTP 和 SSH），代表主机之间的通信。
- **客户端协议 (Client Protocol)**：客户端（例如 Web 浏览器和邮件客户端），代表主机上运行的软件。
- **Web 应用 (Web Application)**：Web 应用（例如 MPEG 视频和 Facebook），代表 HTTP 流量的内容或请求的 URL。

类别 (Categories)：对应用的一般分类，说明其最基本的功能。

标记 (Tags)：关于应用的其他信息，与类别类似。

对于加密流量，系统可以仅使用标记有 SSL 协议的应用识别和过滤流量。只有在未加密或已解密的流量中才能检测到没有此标记的应用。此外，系统仅将已解密的流量标记分配给可在已解密的流量中检测到的应用，而不会将它们分配给加密或未加密的流量中检测到的应用。

应用列表 (Applications List)（显示底部）：在从列表上方的选项中选择过滤器时，此列表将进行更新，所以您可查看当前符合过滤器的应用。在计划将过滤器条件添加到规则中时，使用此列表可确认您的过滤器是否针对所需的应用。要将特定应用添加到对象，请从过滤列表中选择它们。选择应用后，过滤器将不再适用。如果您希望过滤器本身作为对象，请勿从列表中选择应用。然后，该对象将代表过滤器识别的应用。

步骤 5 点击**确定 (OK)**，保存更改。

编辑 Firepower 应用过滤器对象

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的对象。

步骤 3 选择要编辑的对象。

步骤 4 点击“操作”(Actions) 窗格中的编辑图标  。

步骤 5 以在上述过程中创建值的相同方式编辑对话框中的值。

步骤 6 点击**保存 (Save)**。

步骤 7 CDO 显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

相关信息：

- 对象
- 对象过滤器
- 删除对象

地理位置对象

地理位置对象定义托管设备（流量的源或目的）的国家/地区和大洲。您可以在策略中使用这些对象而不是使用 IP 地址来控制流量。例如，使用地理位置可以很容易地将访问权限限制为特定国家/地区，而无需知道此处使用的所有潜在 IP 地址。

通常，可以直接在策略中选择地理位置，而无需使用地理位置对象。但是，如果要为同一组国家/地区或大洲创建多个策略，使用对象则非常方便。

更新地理定位数据库

为了确保使用最新的地理位置数据来过滤流量，思科强烈建议您定期更新地理位置数据库(GeoDB)。目前，这不是您可以使用 Cisco Defense Orchestrator 执行的任务。请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》的以下部分，了解您的设备正在运行的版本，以了解有关 GeoDB 及其更新方式的详细信息。

- 更新系统数据库和源
- 更新系统数据库

创建和编辑 Firepower 地理位置过滤器对象

您可以在对象页面上或在创建安全策略时单独创建地理位置对象。此程序从对象页面创建地理位置对象。

要创建地理位置对象，请执行以下步骤：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
步骤 2 点击**创建对象 (Create Object)** > **FTD** > **地理位置 (Geolocation)**。
步骤 3 输入对象的 **对象名称** 和 **说明**（后者为可选项）。
步骤 4 在过滤器栏中，开始键入国家/地区或地区的名称，系统会显示可能的匹配项列表。
步骤 5 选中要添加到对象的国家/地区或地区。
步骤 6 点击**添加**。

编辑地理位置对象

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
步骤 2 使用过滤器窗格和搜索字段查找对象。
步骤 3 在“操作”(Actions) 窗格中，点击**编辑 (Edit)**。
步骤 4 您可以更改对象的名称，并向对象添加或删除国家/地区和地区。
步骤 5 点击**保存 (Save)**。
步骤 6 如果有任何设备受到影响，您会收到通知。点击 **Confirm**。
步骤 7 如果设备或策略受到影响，请打开资产页面并预览并将更改部署到设备。

DNS 服务器组对象

域名系统 (DNS) 组定义 DNS 服务器列表和某些相关联的属性。需要使用 DNS 服务器将完全限定域名 (FQDN) 解析为 IP 地址，例如 www.example.com。您可以为管理和数据接口配置不同的 DNS 组对象。

FDM 管理 设备必须先配置 DNS 服务器，然后才能创建新的 DNS 组对象。您可以将 DNS 服务器添加到 思科防御协调器 (CDO) 中的 Firepower 威胁防御设备设置，也可以在 防火墙设备管理器 中创建 DNS 服务器，然后将 FDM 管理 配置同步到 CDO。要在 防火墙设备管理器 中创建或修改 DNS 服务器设置，请参阅《思科 Firepower 设备管理器配置指南》，版本 6.4 或更高版本中的**为数据和管理接口配置 DNS**。

创建 DNS 组对象

使用以下程序在 CDO 中创建新的 DNS 组对象：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮  以创建新的对象。

步骤 3 点击 FTD DNS 组。 >

步骤 4 输入 **对象名称 (Object Name)**。

步骤 5 （可选）添加说明。

步骤 6 输入 **DNS 服务器**的 IP 地址。您最多可以添加六个 DNS 服务器；点击添加 DNS 服务器。如果您想要删除服务器地址，请点击删除图标。

Note 列表采用优先顺序：始终使用列表中的第一个服务器，只有当从前面的服务器收不到响应时，才使用后面的服务器。虽然最多可以添加六台服务器，但只有列出的前 3 台服务器将用于管理接口。

步骤 7 输入**域搜索名称 (Domain Search Name)**。此域将被添加到非完全限定的主机名，例如 serverA 而不是 serverA.example.com。

步骤 8 输入重试次数。系统接收不到响应时，重试 DNS 服务器列表的次数，介于 0 和 10 次之间。默认值为 2。此设置仅适用于数据接口上使用的 DNS 组。

步骤 9 输入**超时**值。尝试下一个 DNS 服务器之前要等待的秒数，介于 1 和 30 秒之间。默认值为 2 秒。每次系统重试服务器列表，此超时将加倍。此设置仅适用于数据接口上使用的 DNS 组。

步骤 10 点击**添加**。

编辑 DNS 组对象

您可以编辑在 思科防御协调器 或 防火墙设备管理器 中创建的 DNS 组对象。使用以下程序编辑现有的 DNS 组对象：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的 **DNS 组对象**。

步骤 3 选择对象，然后点击**操作 (Actions)** 窗格中的编辑图标 。

步骤 4 编辑以下任何条目：

- 对象名称。
- 说明。
- DNS 服务器。您可以在此列表中编辑、添加或删除 DNS 服务器。
- 域搜索名称。
- 重试。
- 超时。

步骤 5 点击**保存 (Save)**。

步骤 6 预览并部署所有设备的配置更改。

删除 DNS 组对象

使用以下程序从 CDO 中删除 DNS 组对象：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到要编辑的 **DNS 组对象**。

步骤 3 选择对象，然后点击删除图标。

步骤 4 确认要删除 DNS 组对象，然后点击确定。

步骤 5 预览并部署所有设备的配置更改。

将 DNS 组对象添加为 DNS 服务器FDM 管理

您可以将 DNS 组对象添加为数据接口或管理接口的首选 DNS 组。有关详细信息，请参阅 FDM 托管设备设置。FDM 管理 设备设置

证书对象

数字证书是一种用于身份验证的数字识别方式。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。

请参阅适用于您的设备的版本的《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》中可恢复对象一章的**关于证书**和**配置证书**部分。

关于证书

数字证书是一种用于身份验证的数字识别方式。数字证书包括用于识别设备或用户的信息，例如名称、序列号、公司、部门或 IP 地址。数字证书还包括用户或设备的公钥副本。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。

您可以创建以下类型的证书：

- **内部证书 (Internal certificates)** - 内部身份证书是用于特定系统或主机的证书。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名证书。

  系统提供以下预定义内部证书（您可以按原样使用或替换它们）：**DefaultInternalCertificate** 和 **DefaultWebServerCertificate**

- **内部证书颁发机构 (CA)** 证书 - 内部 CA 证书是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名的内部 CA 证书。如果配置自签名的内部 CA 证书，该 CA 将在设备自身上运行。

  系统提供以下预定义内部CA证书（您可以按原样使用或替换它们）：**NGFW-Default-InternalCA**

- **可信证书颁发机构 (CA)** 证书 - 可信的 CA 证书可用于签署其他证书。它是自签名证书，也称为根证书。由另一个 CA 证书颁发的证书称为从属证书。

  证书颁发机构 (CA) 是指“签署”证书以确认其真实性，从而确保设备或用户的身份的可信颁发机构。CA 在 PKI（使用公钥或私钥加密以确保安全性）的情景下颁发数字证书。CA 可以是可信的第三方（例如 VeriSign），也可以是组织内建立的私有（内部）CA。CA 负责管理证书请求和颁发数字证书。

  系统包括许多从第三方证书颁发机构获取的受信任的 CA 证书。SSL 解密策略可使用这些证书执行解密重新签署操作。

有关详细信息，请参阅《适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南》中“可重用对象”一章的**功能使用的证书类型**部分。

功能使用的证书类型

您需要为每个功能创建正确类型的证书。以下功能需要证书。

身份策略（强制网络门户）- 内部证书

（可选。）强制网络门户用于身份策略中。在向设备进行身份验证时，为了标识自己的身份并接收与其用户名关联的 IP 地址，用户必须接受此证书。如果不提供证书，设备将使用自动生成的证书。

SSL 解密策略 - 内部、内部 CA 和受信任 CA 证书。

（必需。）SSL 解密策略将证书用于以下目的：

- 内部证书用于已知的密钥解密规则。
- 在客户端和 FTD 设备之间创建会话时，内部 CA 证书用于解密重签名规则。
- 受信任 CA 证书
  - 在 FTD 设备和服务器之间创建会话时，它们可直接用于解密重签名规则。与其他证书不同，这些证书不能直接在 SSL 解密策略中配置，而是需要上传到系统。系统包括大量受信任 CA 证书，因此，您无需上传任何其他证书。
  - 创建 Active Directory 领域对象并将目录服务器配置为使用加密时。

配置证书

身份策略或 SSL 解密策略中使用的证书必须是 PEM 或 DER 格式的 X509 证书。如果需要，您可以使用 OpenSSL 生成证书、从受信任的证书颁发机构获取证书或创建自签名证书。

使用以下程序配置证书对象：

- 上传内部证书和内部 CA 证书
- 上传受信任的 CA 证书
- 生成自签名的内部证书和内部 CA 证书
- 要查看或编辑证书，请点击证书的编辑图标或视图图标。
- 要删除未引用的证书，请点击证书的垃圾桶图标（删除图标）。请参阅删除对象。

上传内部证书和内部 CA 证书

内部身份证书是特定系统或主机的证书。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名证书。

内部证书颁发机构 (CA) 证书（内部 CA 证书）是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些

证书。此外，您还可以生成自签名的内部CA证书。如果配置自签名的内部CA证书，该CA将在设备自身上运行。

有关使用这些证书的功能的信息，请参阅功能使用的证书类型。

操作步骤

此程序通过上传证书文件或将现有证书文本粘贴到文本框中来创建内部证书身份或内部 CA 证书。如果要生成自签名证书，请参阅生成自签名内部证书和内部 CA 证书。生成自签名的内部证书和内部 CA 证书, on page 139

要创建内部或内部 CA 证书对象，或者在向策略添加新证书对象时，请执行以下程序：

Procedure

步骤 1 执行以下操作之一：

- 在对象页面中创建证书对象：
  a. 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
  b. 点击加号按钮，然后选择 FTD 证书 >
- 将新证书对象添加到策略时，点击创建新对象。

步骤 2 键入证书的**名称**。该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 3 在步骤 1 中，选择内部证书或内部 CA。

步骤 4 在步骤 2 中，选择**上传 (Upload)** 以上传证书文件。

步骤 5 在步骤 3 的**服务器证书 (Server Certificate)** 区域中，将证书内容粘贴到文本框中，或按照向导中的说明上传证书文件。如果将证书粘贴到文本框中，则证书必须包括 BEGIN CERTIFICATE 和 END CERTIFICATE 两行。例如：

```
-----BEGIN CERTIFICATE-----
 MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0
(...5 lines removed...)
shGJDReRYJQqilhHZrYTWZAYTrD7NQPHutK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZlzJM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQCB02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfxwCUn
RV7LRfQGFYd76V/5uor4Wx2ZCjqy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
vlk3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

步骤 6 在步骤 3 的**证书密钥 (Certificate Key)** 区域中，将密钥内容粘贴到证书密钥文本框中，或者按照向导中的说明上传密钥文件。如果将密钥粘贴到文本框中，则密钥必须包含 BEGIN PRIVATE KEY 或 BEGIN RSA PRIVATE KEY 和 END PRIVATE KEY 或 END PRIVATE KEY 行。

Note 密钥不能加密。

步骤 7 点击**添加**。

上传受信任的 CA 证书

受信任证书颁发机构 (CA) 证书用于签署其他证书。它是自签名证书，也称为根证书。由另一个 CA 证书颁发的证书称为从属证书。

有关使用这些证书的功能的信息，请参阅功能使用的证书类型。

受信任 CA 证书可从外部证书颁发机构获取，也可以使用自己的内部 CA 创建（例如通过 OpenSSL 工具生成证书）。然后，使用以下步骤程序上传证书。

操作步骤

Procedure

步骤 1 执行以下操作之一：

- 在对象页面中创建证书对象：
  a. 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
  b. 点击加号按钮，然后选择 FTD 证书。 >
- 将新证书对象添加到策略时，点击创建新对象。

步骤 2 键入证书的**名称**。该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 3 在步骤 1 中，选择外部 CA 证书，然后点击继续。向导前进到步骤 3。

步骤 4 在步骤 3 的**证书内容 (Certificate Contents)** 区域中，将证书内容粘贴到文本框中，或按照向导中的说明上传证书文件。

证书必须遵循以下准则：

- 证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 10.10.10.250 作为 IP 地址，但证书中的地址为 ad.example.com，则连接失败。
- 该证书必须为 PEM 或 DER 格式的 X509 证书。
- 您粘贴的证书必须包括 BEGIN CERTIFICATE 和 END CERTIFICATE 行。例如：

```
-----BEGIN CERTIFICATE-----
MIIFgTCCA2mgAwIBAgIJANvdcLnabFGYMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJUWDEPMA0GA1UEBwwGYXVzdGluMRQwEgYDVQQKDAsx
OTIuMTY4LjEuMTEUMBIGA1UEAwwLMTkyLjE2OC4xLjEwHhcNMTYxMDI3MjIzNDE3
WhcNMTcxMDI3MjIzNDE3WjBXMQswCQYDVQQGEwJVUzELMAkGA1UECAwCVFgxDzAN
BgNVBAcMBmF1c3RpbjEUMBIGA1UECgwLMTkyLjE2OC4xLjExFDASBgNVBAMMCzE5
Mi4xNjguMS4xMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA5NceYwtP
ES6Ve+S9z7WLKGX5JlF58AvH82GPkOQdrixn3FZeWLQapTpJZt/vgtAI2FZIK31h
(...20 lines removed...)
```

```
hbr6HOgKlOwXbRvOdksTzTEzVUqbgxt5Lwupg3b2ebQhWJz4BZvMsZX9etveEXDh
PY184V3yeSeYjbSCF5rP71fObG9Iu6+u4EfHp/NQv9s9dN5PMffXKieqpuN20Ojv
2b1sfOydf4GMUKLBUMkhQnip6+3W
-----END CERTIFICATE-----
```

步骤 5 点击**添加**。

生成自签名的内部证书和内部 CA 证书

内部身份证书是特定系统或主机的证书。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名证书。

内部证书颁发机构 (CA) 证书（内部 CA 证书）是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。您可以使用 OpenSSL 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名的内部 CA 证书。如果配置自签名的内部 CA 证书，该 CA 将在设备自身上运行。

此外，还可以使用 OpenSSL 创建证书或从受信任的 CA 获取证书，再上传它们。有关详细信息，请参阅上传内部证书和内部 CA 证书。

有关使用这些证书的功能的信息，请参阅功能使用的证书类型。

Note 新的自签名证书生成的有效期为 5 年。请务必在证书过期前进行更换。

Warning 升级具有自签名证书的设备可能会遇到问题；有关详细信息，请参阅检测到新证书。

操作步骤

此程序可通过在向导中输入相应的证书字段值来生成自签名证书。如果要通过上传证书文件来创建内部或内部 CA 证书，请参阅上传内部和内部 CA 证书。上传内部证书和内部 CA 证书, on page 136

要生成自签名证书，请执行以下程序：

Procedure

步骤 1 执行以下操作之一：

- 在对象页面中创建证书对象：
  a. 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。
  b. 点击加号按钮，然后选择 FTD 证书。 >

- 将新证书对象添加到策略时，点击创建新对象。

步骤 2 键入证书的**名称**。该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 3 在步骤 1 中，选择内部证书或内部 CA。

步骤 4 在步骤 2 中，选择自签名以在此步骤中创建自签名证书。

步骤 5 为证书主题和颁发者信息至少配置以下一项。

- 国家/地区 (Country [C]) - 从下拉列表中选择国家/地区代码。
- 州或省 (ST) (State or Province [ST]) - 证书中包括的州或省。
- 地区或城市 (Locality or City) (L) - 证书中包括的地区，例如城市名称。
- 组织 (O) (Organization [O]) - 要包含在证书中的组织或公司名称。
- 组织单位（部门）(Organizational Unit [Department]) (OU) - 证书中包含的组织单位名称（例如部门名称）。
- 公用名 (CN)(Common Name [CN]) - 要包含在证书中的 X.500 公用名。它们可能是设备、网站或其他文本字符串的名称。通常需要有此元素，才能成功进行连接。例如，用于远程访问 VPN 的内部证书中必须包括 CN。

步骤 6 点击**添加**。

配置 IPsec 提议

IPsec 是设置 VPN 的最安全方法之一。IPsec 在 IP 数据包级别提供数据加密，提供一种基于标准的强大的安全解决方案。使用 IPsec，数据通过隧道在公共网络上传输。隧道是两个对等体之间安全的逻辑通信路径。进入 IPsec 隧道的流量由称为转换集的安全协议和算法组合保护。在 IPsec 安全关联 (SA) 协商期间，对等体搜索在两个对等体处相同的转换集。

根据 IKE 版本（IKEv1 或 IKEv2），存在不同的 IPsec 提议对象：

- 当创建 IKEv1 IPsec 提议时，可以选择 IPsec 运行的模式，并定义所需的加密和身份验证类型。您可以为算法选择单一选项。如果要在 VPN 中支持多个组合，请创建和选择多个 IKEv1 IPsec 提议对象。
- 当创建 IKEv2 IPsec 提议时，可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序，并与对等体进行协商，直到找到匹配。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

Note 我们建议对 IPsec 隧道使用加密和身份验证。

以下主题介绍如何为每个 IKE 版本配置 IPsec 提议：

- 管理 IKEv1 IPsec 提议对象
- 管理 IKEv2 IPsec 提议对象

管理 IKEv1 IPsec 提议对象

IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。IKEv1 和 IKEv2 有单独的对象。目前， Cisco Defense Orchestrator (CDO) 支持 IKEv1 IPsec 提议对象。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

Note 我们建议对 IPsec 隧道使用加密和身份验证。

Related Topics

创建或编辑 IKEv1 IPsec 提议对象

创建或编辑 IKEv1 IPsec 提议对象

有几个预定义的IKEv1 IPsec提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑站点间 VPN 连接中的 IKEv1 IPsec 设置时，点击对象列表中所示的**创建新 IKEv1 提议 (Create New IKEv1 Proposal)** 链接来创建 IKEv1 IPsec 提议对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FTD > IKEv1 IPsec 提议 (IKEv1 IPsec Proposal)** 以创建新对象。
- 在对象页面中，选择要编辑的IPsec方案，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

步骤 3 为新对象输入**对象名称**。

步骤 4 选择 IKEv1 IPsec 提议对象的运行模式。

- **隧道**模式会封装整个 IP 数据包。IPSec 报头被添加到原始 IP 报头和新的 IP 报头之间。这是默认值。当防火墙对出入位于防火墙后的主机的流量进行保护时，请使用隧道模式。在通过不可

信网络（例如互联网）连接的两个防火墙（或其他安全网关）之间，通常采用隧道模式实施常规 IPSec。

- **传输**模式只封装 IP 数据包的上层协议。IPSec 报头被插入到 IP 报头和上层协议报头（例如 TCP）之间。传输模式要求源和目的主机都支持 IPSec，并且只有在隧道的目的对等体是 IP 数据包的最终目的时才可使用。通常只有在保护第 2 层或第 3 层隧道协议（例如 GRE、L2TP 和 DLSW）时，才会使用传输模式。

步骤 5 选择**加密 (Encryption)**提议的（封装安全协议加密）算法。有关选项的说明，请参阅决定使用哪个加密算法。

步骤 6 选择要用于身份验证的 **ESP 散列 (ESP Hash)** 或完整性算法。有关选项的说明，请参阅决定使用哪些散列算法。

步骤 7 点击**添加**。

管理 IKEv2 IPsec 提议对象

IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。

当创建 IKEv2 IPsec 提议时，可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序，并与对等体进行协商，直到找到匹配。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

Related Topics

创建或编辑 IKEv2 IPsec 提议对象

创建或编辑 IKEv2 IPsec 提议对象

有几个预定义的IKEv2 IPsec提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑 VPN 连接中的 IKEv2 IPsec 设置时，点击对象列表中所示的创建新 IPsec 提议链接来创建 IKEv2 IPsec 提议对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FTD > IKEv2 IPsec 提议 (IKEv2 IPsec Proposal)** 以创建新对象。
- 在对象页面中，选择要编辑的IPsec方案，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

步骤 3 为新对象输入**对象名称**。

步骤 4 配置 IKEv2 IPsec 方案对象：

- **加密** - 此提议的封装安全协议 (ESP) 加密算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪个加密算法。
- **完整性散列** - 要用于身份验证的散列或完整性算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪些散列算法。

步骤 5 点击**添加**。

配置全局 IKE 策略

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。

IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用提议。IKE 提议是一组两个对等体用于保护其之间的协商的算法。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数用于保护后续 IKE 协商。

IKE 策略对象为这些协商定义 IKE 提议。您启用的对象是对等体协商 VPN 连接时使用的对象：不能为每个连接指定不同的 IKE 策略。每个对象的相对优先级确定首先尝试这些策略中的哪一个，数字越小优先级越高。如果协商无法找到两个对等体全都支持的策略，则不建立连接。

要定义全局 IKE 策略，需要为每个 IKE 版本选择启用哪些对象。如果预定义的对象不能满足您的要求，请创建新的策略来执行您的安全策略。

以下步骤说明如何通过“对象”(Objects) 页面配置全局策略。在编辑 VPN 连接时，您还可以点击 IKE 策略设置的编辑，来启用、禁用和创建策略。

以下主题介绍如何为每个 IKE 策略版本配置 IPsec 提议：

- 管理 IKEv1 策略
- 管理 IKEv2 策略

管理 IKEv1 策略

介绍如何创建和编辑 IKEv1 策略。

关于 IKEv1 策略

互联网密钥交换 (IKE) 版本 1 策略对象包含定义 VPN 连接时 IKEv1 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义 IKEv1 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

Related Topics

创建或编辑 IKEv1 策略

创建或编辑 IKEv1 策略

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。您还可以点击对象列表中所示的**创建新 IKE 策略 (Create New IKEv1 Policy)** 链接，以便在站点间 VPN 连接中编辑 IKEv1 设置时创建 IKEv1 策略对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FTD > IKEv1 Policy** 策略以创建新的 IKEv1 策略。
- 在对象页面中，选择要编辑的IKEv1策略，然后点击右侧“操作”(Actions)窗格中的**编辑 (Edit)**。

步骤 3 输入**对象名称**，最多 128 个字符。

步骤 4 配置 IKEv1 属性。

- **优先级 (Priority)** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **加密** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。有关选项的说明，请参阅“决定使用哪种加密算法”。
- **Diffie-Hellman 组** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。有关选项的解释，请看“决定要使用的 Diffie-Hellman 模数组”。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。
- **身份验证** - 在两个对等体之间使用的身份验证方法。有关详细信息，请参阅确定使用哪种身份验证方法。
  - **预共享密钥** - 使用在每个设备上定义的预共享密钥。在身份验证阶段，此类密钥允许密钥在两个对等体之间共享并由 IKE 使用。如果未使用同一预共享密钥配置对等体，则无法建立 IKE SA。

- **证书** - 使用对等体的设备身份证书来识别彼此。必须通过在证书颁发机构中注册每个对等体来获取这些证书。还须上传用于签署每个对等体的身份证书的受信任 CA 根证书和中间 CA 证书。对等体可以注册到相同或不同的 CA 中。对于任一对等体，都不能使用自签证书。

- **散列** - 用于创建消息摘要的散列算法，以确保消息的完整性。有关选项的说明，请参阅VPN 中使用的加密和散列算法。

步骤 5 点击**添加**。

管理 IKEv2 策略

介绍如何创建和编辑 IKEv2 策略。

关于 IKEv2 策略

互联网密钥交换 (IKE) 版本 2 策略对象包含定义 VPN 连接时 IKEv2 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv2 策略有多个。如果哪个符合您的需求，只需点击状态开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

Related Topics

创建或编辑 IKEv2 策略

创建或编辑 IKEv2 策略

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。您还可以点击对象列表中所示的 **创建新的 IKE 策略** 链接，以便在站点间 VPN 连接中编辑 IKEv1 设置时创建 IKEv1 策略对象。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 执行以下操作之一：

- 点击蓝色加号按钮  ，然后选择 **FTD > IKEv2 策略 (IKEv2 Policy)** 以创建新的 IKEv2 策略。
- 在对象页面中，选择要编辑的 IKEv2 策略，然后点击右侧“操作”(Actions) 窗格中的**编辑 (Edit)**。

步骤 3 输入**对象名称 (object name)**，最多 128 个字符。

步骤 4 配置 IKEv2 属性。

- **优先级 (Priority)** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **状态 (State)** - IKE 策略是启用还是禁用状态。点击开关以更改状态。在 IKE 协商期间仅使用启用的策略。
- **加密** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。选择要允许的所有算法，但不能在同一策略中同时包括混合模式 (AES-GCM) 和正常模式选项。（正常模式要求选择完整性散列，而混合模式禁止选择单独的完整性散列。) 系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪个加密算法。
- **Diffie-Hellman 组** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。选择要允许的所有算法。系统与对等体协商，从最强到最弱组，直到达成匹配。有关选项的说明，请参阅决定要使用的 Diffie-Hellman 模数组。
- **完整性散列** - 用于创建消息摘要的散列算法的完整性部分，用于确保消息完整性。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。完整性散列不与 AES-GCM 加密选项一起使用。有关选项的说明，请参阅VPN 中使用的加密和散列算法。
- **伪随机函数 (PRF) 散列 (Pseudo-Random Function [PRF] Hash)** - 散列算法中用作派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法的伪随机函数 (PRF) 部分。在 IKEv1 中，完整性和 PRF 算法不分开，但在 IKEv2 中，可以为这些元素指定不同的算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅VPN 中使用的加密和散列算法。
- **生命周期 (Lifetime)** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。

步骤 5 点击**添加**。

RA VPN 对象

安全区域对象

安全区是一组接口。区域将网络划分成网段，帮助您管理流量以及对流量进行分类。您可以定义多个区域，但一个给定接口只能位于一个区域中。

Firepower 系统会在初始配置期间创建以下区域，这些区域显示在 Defense Orchestrator 的对象页面中。您可以编辑区域以添加或移除接口；如果不再使用这些区域，也可以删除它们。

- **inside_zone** - 包括内部接口。此区域用于表示内部网络。
- **outside_zone** - 包括外部接口。此区域用于表示在您控制之外的网络，例如互联网。

通常，按接口在网络中扮演的角色对它们分组。例如，可将连接至互联网的接口放在 **outside_zone** 安全区，并将内部网络的所有接口放在 **inside_zone** 安全区。然后，可以对来自外部区域和传至内部区域的流量应用访问控制规则。

在创建区域之前，请考虑要应用至网络的访问规则和其他策略。例如，无需将所有内部接口都放到同一个区域。如果您有 4 个内部网络，并希望将其中一个与另外三个区别对待，则可以创建两个区域（而不是一个区域）。如果有一个接口需允许外部访问公共 Web 服务器，您可能希望对该接口使用单独的区域。

相关信息：

- 创建或编辑 Firepower 安全区域对象
- 将 Firepower 接口分配给安全区域
- 删除对象

创建或编辑 Firepower 安全区域对象

安全区是一组接口。区域将网络划分成网段，帮助您管理流量以及对流量进行分类。您可以定义多个区域，但一个给定接口只能位于一个区域中。有关详细信息，请参阅安全区域对象。

安全区域对象不与设备关联，除非在该设备的规则中使用该对象。

创建安全区域对象

要创建安全区域对象，请按照以下说明操作：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮  ，然后选择 **FTD** > **安全区域 (Security Zone)** 以创建对象。

步骤 3 为对象命名，也可输入说明（可选）。

步骤 4 选择要加入安全区域的的接口。

步骤 5 点击**添加**。

编辑安全区域对象

自行激活设备后，您会发现至少有两个安全区域，一个是 inside_zone，另一个是 outside_zone。FDM 管理可以编辑或删除这些区域。要编辑任何安全区域对象，请按照以下说明操作：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 查找要编辑的对象：

- 如果您知道对象的名称，则可以在“对象”页面中进行搜索：
  - 按安全区域过滤列表。
  - 在搜索字段中输入对象名称。
  - 选择对象。
- 如果您知道对象与设备关联，则可以从“资产”页面开始搜索。
  - 在导航窗格中，点击**清单 (Inventory)**。
  - 点击**设备**选项卡。
  - 点击相应的选项卡。
  - 使用设备过滤器和搜索栏查找您的设备。过滤器, on page 90搜索, on page 93
  - 选择设备。
  - 在右侧的“管理”(Management) 窗格中，点击  **对象 (Objects)**。
  - 使用对象过滤器和搜索栏查找要查找的对象。

Note 如果您创建的安全区域对象未与设备策略中的规则关联，则该对象将被视为“未关联”，您将不会在设备的搜索结果中看到该对象。

步骤 3 选择对象。

步骤 4 点击右侧“操作”(Actions) 窗格中的**编辑**图标 。

步骤 5 编辑对象的任何属性后。点击**保存 (Save)**。

步骤 6 点击保存后，您会收到一条消息，说明这些更改将如何影响其他设备。点击**确认 (Confirm)** 以保存更改或点击取消。

服务对象

FirePOWER 服务对象

FTD 服务对象、服务组和端口组是包含被视为 IP 协议簇一部分的协议或端口的可重用组件。

FTD 服务组是服务对象的集合。服务组可能包含一个或多个协议的对象。您可以在安全策略中使用这些对象和组来定义网络流量匹配条件，例如使用访问规则来允许流量传送至特定 TCP 端口。该系统中包括多个针对通用服务的预定义对象。您可以使用策略中的这些对象；但无法编辑或删除系统定义的对象。

Firepower 设备管理器和 Firepower 管理中心将服务对象称为端口对象以及服务组和端口组。

有关详细信息，请参阅创建和编辑 Firepower 服务对象。

协议对象

协议对象是一种包含不太常用或传统协议的服务对象。协议对象由名称和协议编号来标识。CDO 可识别 ASA 和 Firepower（FDM 管理 设备）配置中的这些对象，并为其提供自己的“协议”过滤器，以便您可以轻松找到它们。

有关详细信息，请参阅创建和编辑 Firepower 服务对象。

ICMP 对象

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

使用 CDO，您可以从 ASA 配置中重命名或删除 ICMP 对象。您可以使用 CDO 在 Firepower 配置中创建、更新和删除 ICMP 和 ICMPv6 对象。

Note 对于 ICMPv6 协议，AWS 不支持选择特定参数。仅支持允许所有 ICMPv6 消息的规则。

有关详细信息，请参阅创建和编辑 Firepower 服务对象。

相关信息：

- 删除对象, on page 117

创建和编辑 Firepower 服务对象

要创建 Firepower 服务对象，请执行以下步骤：

防火墙设备管理器 (FDM 管理) 服务对象是可重用组件，可指定 TCP/IP 协议和端口。防火墙设备管理器、本地防火墙管理中心 和 云交付的防火墙管理中心 将这些对象称为“端口对象”。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击右侧的蓝色按钮  以创建对象，然后选择 **FTD** > **服务 (Service)**。

步骤 3 输入对象名称和说明。

步骤 4 选择**创建服务对象 (Create a service object)**。

步骤 5 点击**服务类型 (Service Type)** 按钮，然后选择要为其创建对象的协议。

步骤 6 按如下方式配置协议：

- **TCP**、 **UDP**
  - 选择 **eq**，然后输入端口号或协议名称。例如，您可以输入 80 作为端口号或 HTTP 作为协议名称。
  - 您还可以选择**范围**，然后输入端口号范围，例如 **1 65535**（以涵盖所有端口）。
- **ICMP**、 **IPv6-ICMP**-选择 ICMP **类型**。选择 **Any** 类型可应用于所有 ICMP 消息。有关类型和代码的信息，请参阅以下页面：
  - ICMP-http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - ICMPv6-http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- **其他 (Other)** - 选择所需协议。

步骤 7 点击**添加 (Add)**。

步骤 8 查看并部署您现在所做的更改，或者等待并一次部署多个更改。

创建 Firepower 服务组

服务组可以由代表一个或多个协议的一个或多个服务对象组成。需要先创建服务对象，然后才能将其添加到组。Firepower 设备管理器和 Firepower 管理中心将这些对象称为“端口对象”。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击右侧的蓝色按钮  以创建对象，然后选择 **FTD > 服务 (Service)**。

步骤 3 输入对象名称和说明。

步骤 4 选择**创建服务组 (Create a service group)**。

步骤 5 通过点击添加对象 (Add Object) 将对象添加到组。

- 点击创建以创建新对象，就像上面创建 Firepower 服务对象中的操作一样。创建和编辑 Firepower 服务对象, on page 149
- 点击选择 (Choose) 以将现有服务对象添加到组。重复此步骤以添加更多对象。

步骤 6 将服务对象添加到服务组后，点击添加。

步骤 7 查看并部署您现在所做的更改，或者等待并一次部署多个更改。

编辑 Firepower 服务对象或服务组

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 过滤对象以查找要编辑的对象，然后在对象表中选择该对象。

步骤 3 在“操作”(Actions) 窗格中，点击**编辑 (Edit)**  。

步骤 4 以在上述过程中创建值的相同方式编辑对话框中的值。

步骤 5 点击**保存 (Save)**。

步骤 6 CDO 显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

步骤 7 查看并部署您现在所做的更改，或者等待并一次部署多个更改。

安全组标记组

安全组标记

关于安全组标记

如果使用思科身份服务引擎 (ISE) 定义并使用**安全组标记** (SGT) 来对 Cisco TrustSec 网络中的流量进行分类，则可以编写使用 SGT 作为匹配条件的访问控制规则。因此，可以基于安全组成员身份阻止或允许访问，而不是使用 IP 地址。

在 ISE 中，您可以创建 SGT，并将主机或网络 IP 地址分配至各标记。如果您将 SGT 分配给用户帐户，SGT 就会被分配给用户流量。将 FDM 管理 设备配置为连接到 ISE 服务器并创建 SGT 后，您可以在 思科防御协调器 中创建 SGT 组并围绕它们构建访问控制规则。请注意，您必须先配置 ISE 的 SGT 交换协议 (SXP) 映射，然后才能将 SGT 关联到 FDM 管理 设备。有关详细信息，请参阅您当前运行的版本的《思科身份服务引擎管理员指南》中的**安全组标记交换协议**。

FDM 管理 设备评估 SGT 作为访问控制规则的流量匹配条件时，会使用以下优先级：

1. 数据包中定义的源 SGT（如有）。使用此技术无法进行目的地匹配。对于数据包中的 SGT，必须配置网络中的交换机和路由器以添加它们。有关如何实施此方法的信息，请参阅 ISE 文档。
2. 分配给用户会话的 SGT，从 ISE 会话目录下载。您需要启用此选项才能侦听此类 SGT 匹配的会话目录信息，但是，当您首次创建 ISE 身份源时，此选项会默认打开。SGT 可以与源或目标相匹配。尽管非必需，但您通常还会使用 ISE 身份源和 AD 域来设置被动身份验证身份规则，以收集用户身份信息。
3. 使用 SXP 下载的 SGT-IP 地址映射。如果 IP 地址在 SGT 范围内，则流量与使用 SGT 的访问控制规则相匹配。SGT 可以与源或目标相匹配。

Note 您无法直接在访问控制规则中使用从 ISE 检索到的信息。相反，您需要创建引用已下载 SGT 信息的 SGT 组。您的 SGT 组可以引用多个 SGT，因此您可以在适当的情况下根据相关的标记集合应用策略。

版本支持

CDO 当前在运行 6.5 和更高版本的 FDM 管理 设备上支持 SGT 和 SGT 组。FDM 管理 设备允许您在版本 6.5 及更高版本中配置并连接到 ISE 服务器，但在 6.7 之前版本中不支持在 UI 中配置 SGT。

从 FDM 管理 UI 中，这意味着运行版本 6.5 或更高版本的 FDM 管理 设备可以下载 SGT 的 SXP 映射，但不能手动添加到对象或访问控制规则。要更改运行版本 6.5 或版本 6.6 的设备的 SGT，您必须使用 ISE UI。但是，如果运行版本 6.5 的设备已被载入 思科防御协调器，则可以查看与设备关联的当前 SGT 并创建 SGT 组。

CDO 中的 SGT

安全组标记

SGT 在 CDO 中为只读。您无法在 CDO 中创建或编辑 SGT。要创建 SGT，请参阅当前运行版本的《思科身份服务引擎管理员指南》。

SGT 组

Note FDM 管理 设备将 SGT 组称作 SGT 动态对象。在 CDO 中，这些标签列表当前被称作 SGT 组。您可以在 CDO 中创建 SGT 组，而无需参考 FDM 管理 设备或 ISE UI。

使用 SGT 组可以根据 ISE 分配的 SGT 来识别源或目标地址。然后，可以将访问控制规则中的对象用于定义流量匹配条件。您无法直接在访问控制规则中使用从 ISE 检索到的信息。相反，您需要创建引用已下载 SGT 信息的 SGT 组。

您的 SGT 组可以引用多个 SGT，因此您可以在适当的情况下根据相关的标记集合应用策略。

要在 CDO 中创建 SGT 组，必须至少已经配置一个 SGT，并为要使用的设备的 FDM 管理 控制台配置来自 ISE 服务器的 SGT 映射。请注意，如果多个 FDM 管理 设备与同一 ISE 服务器关联，则可以将 SGT 或 SGT 组应用于多个设备。如果设备未与 ISE 服务器关联，则不能在访问控制规则中包含 SGT 对象，也不能将 SGT 组应用于该设备配置。

规则中的 SGT 组

SGT 组可被添加到访问控制规则；它们会显示为源或目标网络对象。有关网络如何在规则中工作的详细信息，请参阅 FDM 访问控制规则中的源和目标条件。

您可以从“对象”(Objects) 页面创建 SGT 组。有关详细信息，请参阅创建 SGT 组, on page 153。

创建 SGT 组

要创建可用于访问控制规则的 SGT 组，请使用以下程序：

Before you begin

在创建安全组标记 (SGT) 组之前，必须配置以下配置或环境：

- FDM 管理 设备必须至少运行版本 6.5。
- 必须配置 ISE 身份源以订用 SXP 映射并启用部署更改。要管理 SXP 映射，请参阅所用版本（版本 6.7 及更高版本）的 Firepower 设备管理器配置指南中的**在 ISE 中配置安全组和 SXP 发布**。
- 所有 SGT 都必须在 ISE 中创建。要创建 SGT，请参阅当前运行版本的《思科身份服务引擎配置指南》。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击蓝色加号按钮  以创建新的对象。

步骤 3 点击 **FTD > 网络 (Network)**。

步骤 4 输入 **对象名称 (Object Name)**。

步骤 5 （可选）添加说明。

步骤 6 点击 **SGT** 并使用下拉菜单选中要包含在组中的所有适用 SGT。您可以按 SGT 名称对列表进行排序。

步骤 7 点击**保存 (Save)**。

Note 您无法在 CDO 中创建或编辑 SGT，只能在 SGT 组中添加或删除它们。要创建或编辑 SGT，请参阅当前运行版本的《思科身份服务引擎配置指南》。

编辑 SGT 组

要编辑 SGT 组，请使用以下程序：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 使用对象过滤器和搜索字段找到您要编辑的 SGT 组。

步骤 3 选择 SGT 组，然后点击**操作 (Actions)** 窗格中的编辑图标  。

步骤 4 修改 SGT 组。编辑与该组关联的名称、说明或 SGT。

步骤 5 点击**保存 (Save)**。

Note 您无法在 CDO 中创建或编辑 SGT，只能在 SGT 组中添加或删除它们。要创建或编辑 SGT，请参阅当前运行版本的《思科身份服务引擎配置指南》。

将 SGT 组添加到访问控制规则

要将 SGT 组添加到访问控制规则，请使用以下程序：

Procedure

步骤 1 在导航窗格中，点击**清单 (Inventory)**。

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

步骤 3 点击 FTD 选项卡，然后选择要向其添加 SGT 组的设备。

步骤 4 在**管理 (Management)** 窗格中，选择**策略 (Policy)**。

步骤 5 点击源或目标对象的蓝色加号按钮，然后选择 SGT 组。 

步骤 6 使用对象过滤器和搜索字段找到您要编辑的 SGT 组。

步骤 7 点击**保存 (Save)**。

步骤 8 预览并部署所有设备的配置更改。

Note 如果需要创建其他 SGT 组，请点击创建新对象。填写创建 FTD SGT 组并将 SGT 组添加到规则中提到的必填信息。创建 SGT 组, on page 153

系统日志服务器对象

FDM管理 设备用来存储事件的容量有限。要尽可能提高事件存储量，您可以配置外部服务器。系统日志 (syslog) 服务器对象标识可接收面向连接的消息或诊断 syslog 消息的服务器。如果已为日志收集和分析设置一台系统日志服务器，您可以使用 思科防御协调器 来创建对象以进行定义并在相关策略中使用这些对象。

创建和编辑系统日志服务器对象

要创建新的系统日志服务器对象，请执行以下步骤：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击**创建对象 (Create Object)** 按钮  。

步骤 3 选择 FDM 管理 设备对象类型下方的**系统日志服务器 (Syslog Server)**

步骤 4 配置系统日志服务器对象属性：

- **IP 地址** - 输入系统日志服务器的 IP 地址。
- **协议类型 (Protocol Type)** - 选择系统日志服务器用于接收消息的协议。如果您选择 TCP，系统可以识别何时系统日志服务器不可用，并停止发送事件，直至服务器再次可用。
- **端口号 (Port Number)** - 输入要用于系统日志的有效端口号。如果系统日志服务器使用默认端口，请输入 514 作为默认 UDP 端口或 1470 作为默认 TCP 端口。如果服务器不使用默认端口，请输入正确的端口号。端口范围必须介于 1025 至 65535 之间。
- **选择接口**-选择应使用哪个接口发送诊断系统日志消息。连接和入侵事件始终使用管理接口。接口选择决定与系统日志消息关联的 IP 地址。请注意，您只能选择下面列出的选项**之一**。不能同时选择两者。选择以下选项之一：
  - **数据接口** - 选择用于诊断系统日志消息的数据接口。从生成列表中选择一个接口。如果可以通过网桥组成员接口访问该服务器，请选择该网桥组接口 (BVI)。如果通过诊断接口（物理管理接口）访问，我们建议您选择管理接口，而不是此选项。您不能选择被动接口。对于连接和入侵系统日志消息，源 IP 地址是管理接口的地址；如果您通过数据接口进行路由，则是网关接口的地址。
  - **管理接口** - 对所有类型的系统日志消息使用虚拟管理接口。源 IP 地址是管理接口的地址；如果您通过数据接口进行路由，则是网关接口的地址。

步骤 5 点击**添加 (Add)**。

步骤 6 立即查看并部署您所做的更改，或等待并一次部署多个更改。

编辑系统日志服务器对象

要编辑现有的系统日志服务器对象，请执行以下步骤：

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 找到所需的系统日志服务器对象并选择它。您可以按系统日志服务器对象类型过滤对象列表。

步骤 3 在“操作”(Actions) 窗格中，点击**编辑 (Edit)**。

步骤 4 进行所需的编辑，然后点击**保存 (Save)**。

步骤 5 确认您所做的更改。

步骤 6 立即 查看并部署 您所做的更改，或等待并一次部署多个更改。

相关信息：

- 删除对象

为安全日志记录分析 (SaaS) 创建系统日志服务器对象

使用要向其发送事件的安全事件连接器 (SEC) 的 IP 地址、TCP 端口或 UDP 端口创建系统日志服务器对象。您将为已载入租户的每个 SEC 创建一个系统日志对象，但您只能将来自一个规则的事件发送到一个代表一个 SEC 的系统日志对象。

前提条件

此任务是更大工作流程的一部分。开始前，请参阅 为 FDM 管理 设备实施安全日志记录分析 (SaaS)。

操作步骤

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击**创建对象 (Create Object)** 按钮  。

步骤 3 选择 FDM 管理 设备对象类型下方的**系统日志服务器 (Syslog Server)**。

步骤 4 配置系统日志服务器对象属性。要查找 SEC 的这些属性，请从 CDO 菜单中选择**管理 (Admin) > 安全连接器 (Secure Connectors)**。然后，选择要为其配置系统日志对象的安全事件连接器，并查看右侧的“详细信息”窗格。

- **IP 地址 (IP Address)** - 输入 SEC 的 IP 地址。
- 协议类型 - 选择 TCP 或 UDP。
- 端口号 - 如果您选择了 TCP，请输入端口 10125；如果您选择了 UDP，请输入 10025。
- 选择接口 - 选择配置用于访问 SEC 的接口。

Note FDM 管理 设备支持每个 IP 地址一个系统日志对象，因此您必须在使用 TCP 和 UDP 之间进行选择。

步骤 5 点击**添加 (Add)**。

What to do next

继续步骤 3 实施安全日志记录分析 (SaaS) 并通过安全事件连接器将事件发送到思科云的现有 CDO 客户工作流程。

URL 对象

URL 对象和 URL 组由 Firepower 设备使用。使用 URL 对象和组（统称为“URL 对象”）可定义 Web 请求的 URL 或 IP 地址。可以使用这些对象在访问控制策略中执行手动 URL 过滤，或在安全情报策略中进行阻止。URL 对象定义单个 URL 或 IP 地址，而 URL 组可以定义多个 URL 或地址。

准备工作

在创建 URL 对象时，请记住以下要点：

- 如果不包含路径（即 URL 中无 / 字符），则匹配仅基于服务器主机名。如果主机名位于 :// 分隔符之后，或在主机名中的任何点之后，则认为该主机名匹配。例如，ign.com 匹配 ign.com 和 www.ign.com，但不匹配 verisign.com。
- 如果包含一个或多个 / 字符，则整个 URL 字符串将用于子字符串匹配，其中包括服务器名称、路径和任何查询参数。但是，我们建议您不要使用手动URL过滤阻止或允许个别网页或部分网站，因为这样可能会重组服务器并将页面移至新路径。子字符串匹配还可能导致意外匹配，其中 URL 对象中包含的字符串也与非预期服务器上的路径或查询参数中的字符串匹配。
- 系统忽略加密协议（HTTP 与 HTTPS）。换句话说，如果阻止网站，系统将阻止发往该网站的 HTTP 和 HTTPS 流量，除非您使用一个应用条件指定特定协议。在创建 URL 对象时，您不需要指定创建对象时的协议。例如，使用 example.com 而不是 http://example.com。
- 如果您计划使用 URL 对象匹配访问控制规则中的 HTTPS 流量，请使用加密流量时所使用的公钥中的使用者公用名创建该对象。此外，系统会忽略使用者公用名中的子域，因此，不包括子域信息。例如，使用 example.com 而不是 www.example.com。

  但请注意，证书中的使用者公用名可能与网站的域名完全无关。例如，youtube.com 证书中的使用者公用名是 *.google.com（当然，这可能会随时更改）。如果使用 SSL 解密策略解密 HTTPS 流量以便 URL 过滤规则可用于解密策略，则可能获得更一致的结果。

注释 如果由于证书信息不再可用，浏览器恢复 TLS 会话，则 URL 对象将不匹配 HTTPS 流量。因此，即使精心配置 URL 对象，也可能会得到不一致的 HTTPS 连接结果。

创建或编辑 FDM 管理 URL 对象

URL 对象是指定 URL 或 IP 地址的可重用组件。

要创建 URL 对象，请执行以下步骤：

Procedure

步骤 1 在左侧的 思科防御协调器 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击创建对象**创建对象 (Create Object)** > **FTD** > **URL**。

步骤 3 输入对象名称和说明。

步骤 4 选择**创建 URL 对象 (Create a URL object)**。

步骤 5 为对象输入特定 URL 或 IP 地址。

步骤 6 点击**添加**。

创建 Firepower URL 组

URL 组可以由表示一个或多个 URL 或 IP 地址的一个或多个 URL 对象组成。Firepower 设备管理器和 Firepower 管理中心也将这些对象称为“URL 对象”。

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 点击创建对象**创建对象 (Create Object)** > **FTD** > **URL**。

步骤 3 输入对象名称和说明。

步骤 4 选择**创建 URL 组 (Create a URL group)**。

步骤 5 通过点击**添加对象 (Add Object)**，选择一个对象，然后点击**选择 (Select)**，添加现有对象。重复此步骤以添加更多对象。

步骤 6 将 URL 对象添加到 URL 组后，点击**添加**。

编辑 Firepower URL 对象或 URL 组

Procedure

步骤 1 在左侧的 CDO 导航栏中，点击 **对象 (Objects) > FDM 对象 (FDM Objects)**。

步骤 2 过滤对象以查找要编辑的对象，然后在对象表中选择该对象。

步骤 3 在详细信息窗格中，点击以进行编辑。

步骤 4 以在上述过程中创建值的相同方式编辑对话框中的值。

步骤 5 点击**保存 (Save)**。

步骤 6 CDO 显示将受更改影响的策略。点击**确认 (Confirm)** 以完成对对象和受其影响的任何策略的更改。

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。