载入设备和服务

您可以将实时设备和模型设备载入 CDO。模型设备是您可以使用 CDO 查看和编辑的已上传配置文件。

大多数实时设备和服务都需要开放的 HTTPS 连接，以便安全设备连接器可以将 CDO 连接到设备或服务。

有关 SDC 及其状态的详细信息，请参阅安全设备连接器 (SDC)。

本章涵盖以下部分：

载入 本地管理中心

有关详细信息，请查看将 思科防御协调器 连接到托管设备。

注释 CDO 不支持创建或修改与 本地管理中心 或向 本地管理中心 注册的设备关联的对象或策略。您必须在 本地管理中心 UI 中进行这些更改。

限制和准则

以下是适用于载入 本地管理中心 的限制：

- 载入 本地管理中心 还会载入注册到 本地管理中心 的所有设备。请注意，如果托管设备已被禁用或无法访问，CDO 可能会在**清单 (Inventory)** 页面中显示该设备，但无法成功发送请求或查看设备信息。
- 我们建议在 本地管理中心 上创建一个新用户，专门用于具有管理员级别权限的 CDO 通信。如果您载入 本地管理中心，然后使用相同的登录凭证同时登录 本地管理中心，则载入会失败。
- 如果在 本地管理中心 上为 CDO 通信创建了新用户，则用户配置的**最大登录失败次数 (Maximum Number of Failed Logins)** 必须设置为“0”。

网络要求

在载入设备之前，请确保以下端口具有外部访问权限。如果通信端口被防火墙阻止，则激活设备可能会失败。

端口	协议/功能	平台	方向	详细信息
7 / UDP	UDP/审核日志记录	FMC	发送	在配置审核日志记录时，验证与系统日志服务器的连接。
25/tcp	SMTP	FMC	发送	发送邮件通知和警报。
53/tcp 53/udp	DNS	FMC	发送	DNS
67/udp 68/udp	DHCP	FMC	发送	DHCP
80/tcp	HTTP	FMC	发送	在控制面板中显示 RSS 源。
80/tcp	HTTP	FMC	发送	下载或查询 URL 类别和信誉数据（还需要端口 443）。
80/tcp	HTTP	FMC	发送	通过 HTTP 下载自定义安全情报源。
123/udp	NTP	FMC	发送	同步时间。
162/udp	SNMP	FMC	发送	发送 SNMP 警报至远程陷阱服务器。
389/tcp 636/tcp	LDAP	FMC	发送	与 LDAP 服务器通信以进行外部身份验证。 获取检测到的 LDAP 用户元数据（仅限 FMC）。 可配置。
443/tcp	HTTPS	FMC	接收	如果您使用本地安全设备连接器激活 FMC，则允许与端口 443 的入站连接。
443/tcp	HTPS	FMC	出站	如果使用云连接器将 FMC 载入 CDO，则允许来自端口 443 的出站流量。
443/tcp	HTPS	FMC	出站	如果使用 SecureX 激活 FMC，则允许端口 443 的出站连接。
443/tcp	HTTPS	FMC	发送	发送和接收来自互联网的数据。

端口	协议/功能	平台	方向	详细信息
443	HTTPS	FMC	发送	与 AMP 云（公共或私有）通信
514/udp	系统日志（警报）	FMC	发送	向远程系统日志服务器发送警报。
1812/udp 1813/udp	RADIUS	FMC	发送	与 RADIUS 服务器通信以进行外部身份验证和记账。 可配置。
5222/tcp	ISE	FMC	发送	与 ISE 身份源通信。
6514/tcp	系统日志（审核事件）	FMC	发送	配置 TLS 后，将审核日志发送到远程系统日志服务器。
8305/tcp	设备通信	FMC	双向	在同一部署中的设备之间安全地进行通信。 可配置。如果更改此端口，必须为部署中的所有设备更改此端口。建议保留默认值。
8989/tcp	思科成功网络	FMC	发送	传输使用信息和统计信息。

使用凭证将 本地防火墙管理中心 载入 CDO

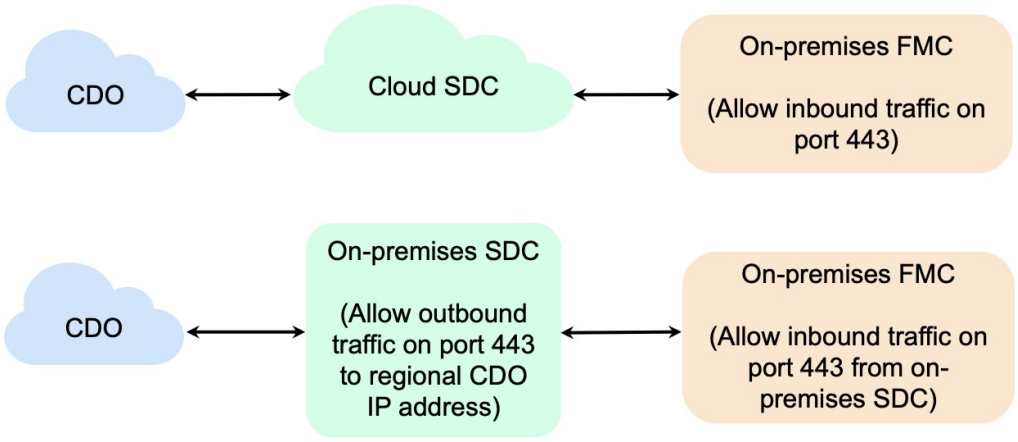
要使用凭证将 本地防火墙管理中心 载入 CDO，请执行以下程序：

Before you begin

查看 载入 本地管理中心, on page 1。

确保在本地防火墙管理中心上允许正确的端口访问：

- 如果您使用本地安全设备连接器载入本地FMC，则允许端口 443 上的入站连接。
- 如果您使用云连接器载入FMC，则允许端口 443 上的出站连接。



步骤 1 在 CDO 导航栏中，点击**清单 (Inventory)**。

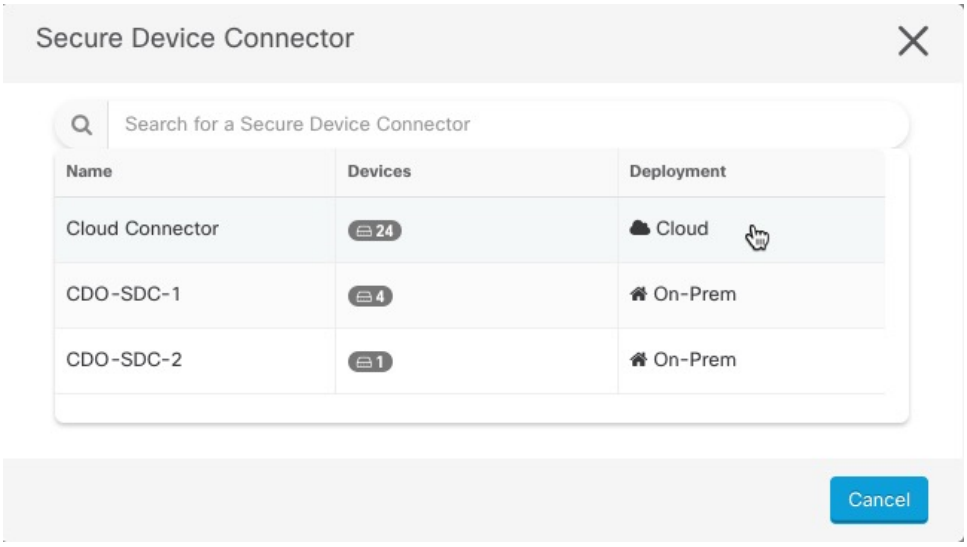
步骤 2 点击 + 以载入设备。

步骤 3 点击**本地 FMC (On-Prem FMC)**。

步骤 4 选择**使用凭证 (Use Credentials)** 卡。

步骤 5 点击**安全设备连接器 (Secure Device Connector)** 按钮，然后选择网络中安装的 SDC。如果您不想使用 SDC，CDO 可以使用云连接器连接到 本地管理中心。您的选择取决于您如何 将 CDO 连接到托管设备。

Figure 1: 选择安全设备连接器



步骤 6 输入设备名称和位置。点击**下一步**。

步骤 7 输入要用于访问 本地管理中心的账户凭证的 **用户名 (Username)** 和**密码 (Password)**。点击**下一步**。

步骤 8 设备已载入。在这里，您可以选择为您的 本地管理中心 设备添加标签，或者点击**转至清单 (Go to Inventory)** 以查看已载入的设备的页面。如果运行状况正常，FMC 将显示**已同步 (Synced)** 状态。

Note 请注意，由 本地管理中心 管理的设备会自动命名为 “<*fmcname*> _<*manageddevicename*>”。

使用 SecureX 自动载入本地防火墙管理中心

作为 CDO 上的超级管理员或管理员用户，您可以使用平台的自动载入 本地管理中心 功能。此功能会自动启动链接到您的 SecureX 租户的所有本地 FMC 的载入过程。此外，它还会载入连接到这些本地 FMC 的 威胁防御 设备。

默认情况下，此功能在 CDO 中启用，因此您可以自动载入所有本地 FMC 和 威胁防御 设备，这样可以显着提高效率。

CDO 会每小时轮询 SecureX 的新 本地管理中心。它会载入主用 本地管理中心 高可用性 (HA) 对。

开始之前

确保满足以下要求：

- 本地管理中心 必须至少运行 7.2 版本。
- 您必须有一个有效的账户。SecureX
- 必须在 上启用。SecureX本地管理中心有关步骤和详细信息，请参阅《Cisco Secure Firewall Management Center（7.0.2 和 7.2）和 SecureX 集成指南》。
- 您必须在 中添加 Firepower 集成模块。SecureX有关步骤和详细信息，请参阅将 Firepower 管理中心与 SecureX 集成。https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/SecureX/cisco-fmc-and-securex-integration-guide.html#Cisco_Concept.dita_70428fed-4183-49ce-9563-1ad75f1db8fc
- 必须允许来自 上的端口 443 的出站流量。本地管理中心
- 本地管理中心 必须具有已配置的模块。
- 在载入设备之前，请合并您的 CDO 租户和 SecureX/CTR 账户。有关说明，请参阅合并账户。
- 在合并您的 CDO 租户和 SecureX/CTR 后，请确保注销 CDO 租户并重新登录。

步骤 1 点击**清单 (Inventory)** >  > **本地 FMC (On-Prem FMC)**。

步骤 2 点击**从 SecureX 帐户发现**作为方法。

使用 SecureX 功能自动载入本地 FMC 会默认启用。您可以转到**清单 (Inventory)**，然后转到**本地 FMC (On-Prem FMC)**，以查看与链接到 CDO 租户的 SecureX 租户关联的新载入的 本地管理中心。

步骤 3 您可以点击可用链接来禁用该功能。

步骤 4 在**常规设置 (General Settings)** 屏幕中，导航至**租户设置 (Tenant Settings)** 部分，然后禁用**使用 SecureX 租户自动载入本地 FMC (Auto onboard On-Prem FMCs using SecureX tenant)**。

注释 当您禁用此功能时，CDO 会停止载入与 SecureX 租户关联的 本地管理中心。它不会删除已自行激活的本地 FMC。您必须在禁用该功能后手动将其删除。

重定向到 CDO本地防火墙管理中心

载入 后，必须在 UI 中更新管理接口的主机名，以包含 FQDN。本地管理中心CDO本地管理中心否则，您将无法从 交叉启动。CDO

使用以下程序更新管理接口主机名，并从 重定向到 ：CDO本地管理中心

步骤 1 登录本地管理中心 UI。

步骤 2 导航至**系统 (System)** > **配置 (Configuration)**。

步骤 3 选择**管理接口 (Management Interfaces)** 选项卡。

步骤 4 展开共享设置标题，然后点击编辑图标。

步骤 5 找到主机名字段并输入 的 FQDN。FMC

步骤 6 保存更改。

注意：您可能需要先注销，然后才能点击 Firepower 管理中心中的管理设备并交叉启动 UI。CDO本地管理中心

从 CDO 中删除 本地防火墙管理中心

如果您选择从 CDO 中删除 本地管理中心，您也将选择从 CDO 中删除所有管理的设备。请注意，这不会从 SecureX 中删除 本地管理中心。

使用以下程序从 CDO 中删除 及其注册的设备：本地管理中心

步骤 1 从导航窗格中，点击**清单 (Inventory)**。

步骤 2 点击**设备 (Devices)** 选项卡。

步骤 3 点击**本地 FMC (On-Prem FMC)** 选项卡，然后选择要删除的 本地管理中心。

步骤 4 在右侧的**设备操作 (Device Actions)** 窗格中，点击**删除本地 FMC 及其托管设备 (Remove On-Prem FMC and its managed devices)**。

步骤 5 点击**确定 (OK)** 以确认要从租户中删除 本地管理中心 及其托管的设备。

步骤 6 刷新浏览器以查看可用设备的更新列表。

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。