使用 CDO 部署 Firepower Threat Defense

本章对您适用吗？

本章介绍如何使用 CDO 的载入向导将 Firepower 威胁防御 (FTD) 设备载入 思科防御协调器 (首席数据官)。在载入 FTD 设备之前，需要使用设备上直接托管的本地 Firepower 设备管理器 (FDM) 完成初始系统配置。

首席数据官是一个基于云的多设备管理器，有助于管理高度分散的环境中的安全策略，从而实现策略的一致实施。首席数据官 帮助您优化安全策略，找出策略中的不一致之处并提供解决这些不一致的工具。首席数据官 让您能够共享对象和策略并制作配置模板，以提升跨设备的策略一致性。

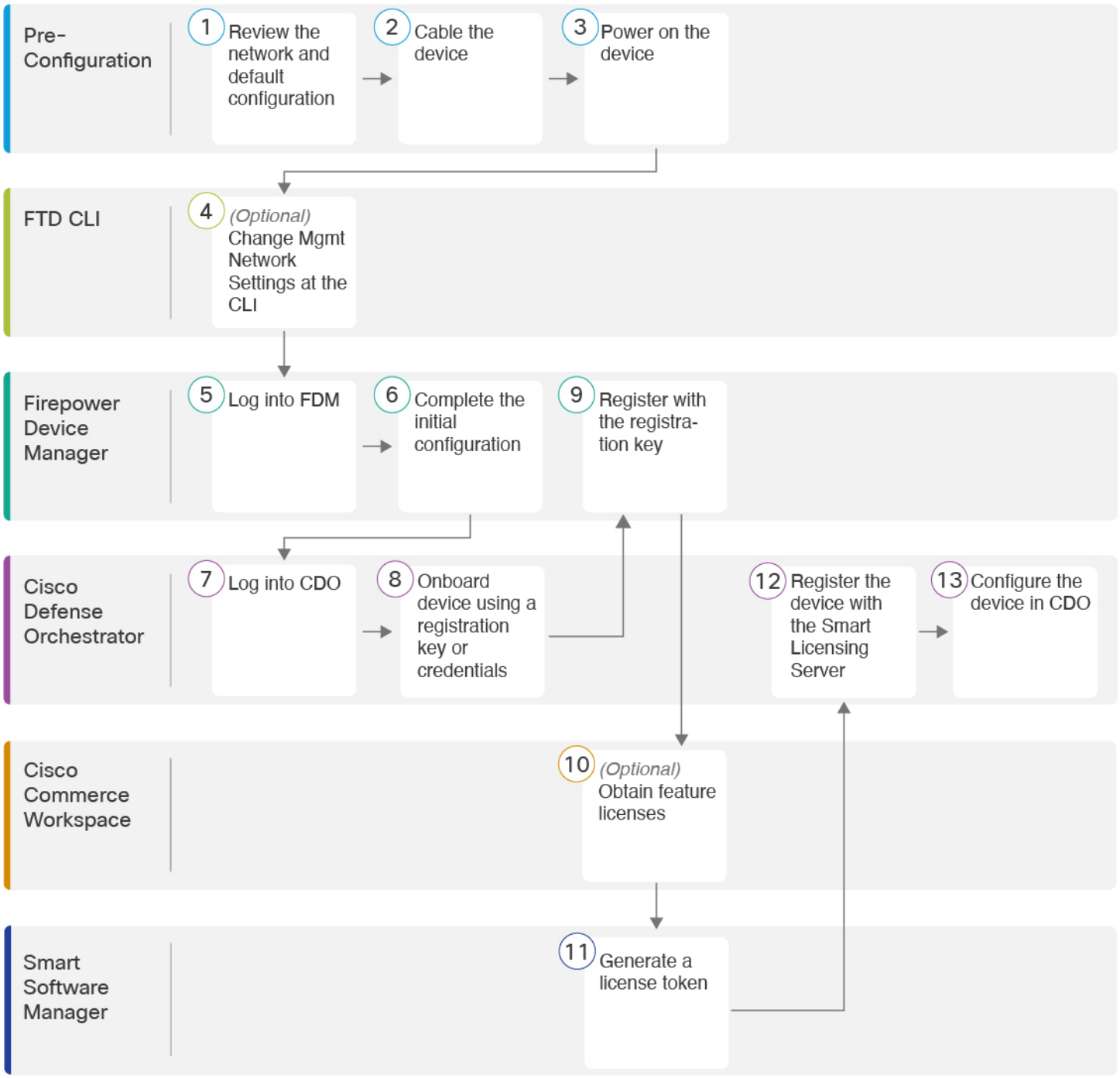
注释 本文档假设 Firepower 2100 硬件上有预装的 FTD 映像。Firepower 2100 硬件可以运行 FTD 软件或 ASA 软件。在 FTD 和 ASA 之间切换需要您对设备进行重新映像。请参阅重新映像思科 ASA 或 Firepower 威胁防御设备。

注释 Firepower 2100 运行名为 Firepower 可扩展操作系统 (FXOS) 的底层操作系统。Firepower 2100 不支持 FXOS Firepower Chassis Manager；出于故障排除目的，仅支持受限的 CLI。有关详细信息，请参阅 FXOS 故障排除指南。

注释 **隐私收集声明** - Firepower 1100 系列不要求或主动收集个人身份信息。不过，您可以在配置中使用个人身份信息，例如用于用户名。在这种情况下，管理员在执行配置或使用 SNMP 时可能会看到此信息。

端到端程序

请参阅以下任务以在机箱上部署 FTD和 首席数据官。



1	配置前准备工作	查看网络部署和默认配置， 第 4 页。
2	配置前准备工作	连接设备电缆， 第 7 页。

3	配置前准备工作	接通设备电源，第 8 页。
4	FTD CLI	（可选）在 CLI 中更改管理网络设置，第 9 页。
5	Firepower 设备管理器	登录 FDM，第 10 页。
6	Firepower 设备管理器	完成初始配置，第 11 页。
7	思科 Defense Orchestrator	使用 Cisco Secure Sign-On 登录 CDO ，第 15 页。
8	思科 Defense Orchestrator	将设备载入 CDO，第 17 页。
9	思科 Defense Orchestrator	在 CDO 中配置设备，第 20 页。
10	思科商务工作空间	（可选）配置许可，第 24 页：获取功能许可证。
11	智能软件管理器	配置许可，第 24 页：生成许可证令牌
12	思科 Defense Orchestrator	配置许可，第 24 页：向智能许可服务器注册设备。
13	思科 Defense Orchestrator	使用 CDO 管理设备，第 30 页。

查看网络部署和默认配置

您可以从管理 1/1 接口或内部接口使用 FDM 管理 FTD。专用管理接口是一种具有自己的网络设置的特殊接口。

下图显示了推荐用于 Firepower 2100 的网络部署。如果您将外部接口直接连接到电缆调制解调器或 DSL 调制解调器，我们建议您将调制解调器置于网桥模式，以便 FTD 为您的内部网络执行所有路由和 NAT。如果您需要为外部接口配置 PPPoE 以连接到您的 ISP，可以在 FDM 中完成初始设置后执行此操作。

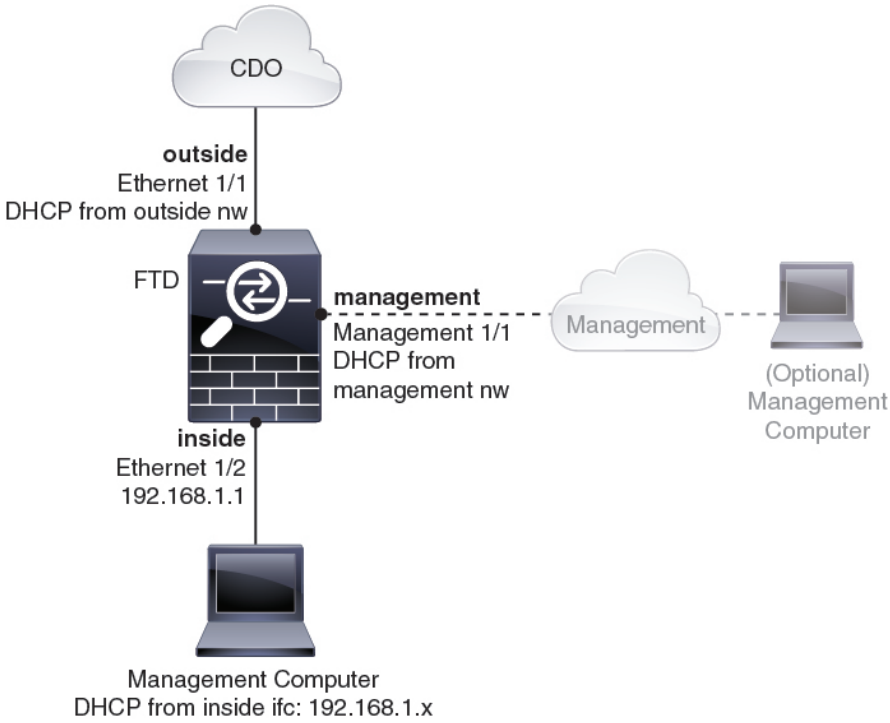
注释 如果您无法使用默认管理 IP 地址（例如，您的管理网络不包括 DHCP 服务器），可以连接到控制台端口并在 CLI 中执行初始设置，包括设置管理 IP 地址、网关和其他基本网络设置。请参阅（可选）在 CLI 中更改管理网络设置，第 9 页。

如果您需要更改内部 IP 地址，可以在 FDM 中完成初始设置后执行此操作。例如，在以下情况下，您可能需要更改内部 IP 地址：

- 如果外部接口尝试获取 192.168.1.0 网络（这是一个通用默认网络）上的 IP 地址，DHCP 租用将失败，外部接口不会获得 IP 地址。出现此问题的原因在于 FTD 在同一网络上不能有两个接口。在这种情况下，您必须将内部 IP 地址更改到新网络上。
- 如果将 FTD 添加到现有内部网络中，需要将内部 IP 地址更改到现有网络上。

下图显示在使用默认配置的 Firepower 2100 系列设备上，使用 Firepower 设备管理器 的 Firepower 威胁防御 默认网络部署。

图 *1:* 建议的网络部署



注释 对于 6.5 及更早版本，管理 1/1 默认 IP 地址为 192.168.45.45。

默认配置

在初始设置后，Firepower 设备的配置包括以下内容：

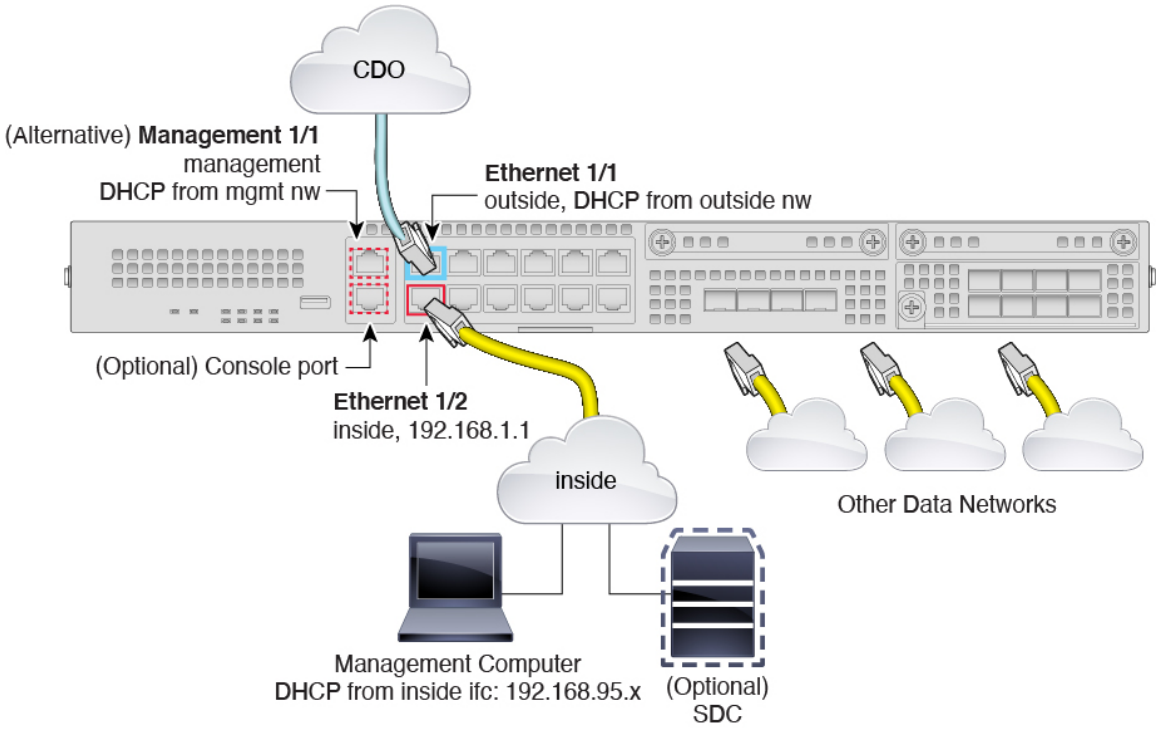
- **内部** - 以太网 1/2、IP 地址 192.168.1.1
- **外部** - 以太网 1/1、来自 DHCP 的 IP 地址或在设置过程中指定的地址
- **内部→外部**流量
- **管理** - 管理 1/1（管理）
  - （6.6 及更高版本）IP 地址来自 DHCP
  - （6.5 及更早版本）IP 地址 192.168.45.45

注释 管理 1/1 接口是不同于数据接口的特殊接口，用于管理、智能许可和数据库更新。物理接口与第二个逻辑接口（诊断接口）共享。诊断是一种数据接口，但仅限于其他类型的管理流量（发往设备和发自设备），例如 syslog 或 SNMP。通常不使用诊断接口。有关详细信息，请参阅 FDM 配置指南。

- **管理型 DNS 服务器** - OpenDNS：208.67.222.222、208.67.220.220 或在设置过程中指定的服务器。系统从不使用从 DHCP 获取的 DNS 服务器。
- **NTP** - 思科 NTP 服务器：0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org 或您在设置过程中指定的服务器
- **默认路由**
  - **数据接口** - 从外部 DHCP 获取，或在设置过程中指定的网关 IP 地址
  - **管理接口** -（6.6 和更高版本）从管理 DHCP 获取。如果没有收到网关，则默认路由在背板上并通过数据接口。（6.5 及更早版本）在背板上并通过数据接口

    请注意，FTD 需要接入互联网才能许可和更新。
- **DHCP 服务器** - 在内部接口和 （仅限 6.5 和更低版本）上启用
- **FDM 访问** - 允许管理和内部主机
- **NAT**- 接口 PAT 用于所有从内部到外部的流量

连接设备电缆



注释 对于 6.5 及更早版本，管理 1/1 默认 IP 地址为 192.168.45.45。

在管理 1/1 或以太网 1/2 上管理 Firepower 2100。默认配置还会将以太网 1/1 配置为外部接口。

过程

步骤 1 将您的管理计算机连接至以下任一接口：

- 以太网 1/2 - 将您的管理计算机直接连接至以太网 1/2 以进行初始配置，或将以太网 1/2 连接至内部网络。以太网 1/2 具有默认 IP 地址 (192.168.1.1)，并且还会运行 DHCP 服务器以向客户端（包括管理计算机）提供 IP 地址，因此，请确保这些设置不会与任何现有内部网络设置冲突（请参阅 默认配置，第 6 页）。
- 管理 1/1（标记为 MGMT）- 将管理 1/1 接口连接到管理网络，并确保管理计算机位于管理网络上，或者可以访问管理网络。管理 1/1 接口从管理网络上的 DHCP 服务器获取 IP 地址；如果使用此接口，则必须确定分配给 FTD 的 IP 地址，以便可以从管理计算机连接到 IP 地址。

  如果需要将管理 1/1 IP 地址从默认值更改为配置静态 IP 地址，还必须将管理计算机连接到控制台端口。请参阅 （可选）在 CLI 中更改管理网络设置，第 9 页。

可以稍后从其他接口配置 FDM 管理访问；请参阅 FDM 配置指南。

步骤 2 将外部网络连接至以太网 1/1 接口（标记为 WAN）。

步骤 3 将其他网络连接到其余接口。

接通设备电源

电源开关位于机箱背面电源模块 1 的左侧，是一个拨动式开关，用于控制系统供电。如果电源开关处于“备用”(Standby) 位置，电源模块将仅启用 3.3V 备用电源，12V 主电源则处于关闭状态。当开关处于“打开”(ON) 位置时，12V 主电源将开启，且系统将启动。

开始之前

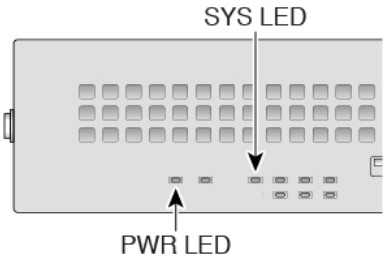
为设备提供可靠的电源（例如，使用不间断电源 (UPS)）非常重要。未事先关闭就断电可能会导致严重的文件系统损坏。后台始终有许多进程在运行，因此断电会使得系统无法正常关闭。

过程

步骤 1 将电源线一端连接到设备，另一端连接到电源插座。

步骤 2 按下设备后部的电源开关。

步骤 3 检查设备前面的 PWD LED；如果该 LED 呈绿色稳定亮起，表示设备已接通电源。



步骤 4 检查设备正面的 SYS LED；在其绿灯常亮后，表示系统已通过启动诊断。

注释 在将电源开关切换到“关闭”(OFF) 位置之前，请使用 shutdown 命令，以便系统能够正常关闭。此过程需要几分钟时间才能完成。正常关闭之后，控制台会显示现在可以安全关闭电源。前面板蓝色定位器信标 LED 亮起，指示系统已准备好关闭电源。可以将开关切换到“关闭”(OFF) 位置。前面板 PWR LED 会瞬间闪烁并熄灭。在 PWD LED 完全关闭之前，请勿拔出电源。

请参阅 FXOS 配置指南，了解有关使用 shutdown 命令的详细信息。

（可选）在 CLI 中更改管理网络设置

如果您无法使用默认管理 IP 地址，可以连接到控制台端口并在 CLI 中执行初始设置，包括设置管理 IP 地址、网关和其他基本网络设置。只能配置管理接口设置；您无法配置内部或外部接口，稍后可在 CDO 或 FDM 中配置它们。

注释 除非清除配置，否则无法重复 CLI 设置脚本（例如，通过重新建立映像）。但是，可以稍后在 CLI 中使用 **configure network** 命令更改所有这些设置。请参阅 FTD 命令参考。

过程

步骤 1 连接到 FTD 控制台端口。有关详细信息，请参阅访问 FTD 和 FXOS CLI，第 30 页。

使用用户名 **admin** 和默认密码 **Admin123** 登录。

您将连接到 FXOS CLI。第一次输入登录时，系统会提示您更改密码。此密码也用于 SSH 的 FTD 登录。

示例：

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

步骤 2 连接到 FTD CLI。

connect ftd

示例：

```
firepower# connect ftd
>
```

步骤 3 首次登录 FTD 时，系统会提示您接受“最终用户许可协议”(EULA) 并。然后，系统将显示 CLI 设置脚本。

默认值或以前输入的值会显示在括号中。要接受之前输入的值，请按 **Enter** 键。

请参阅以下准则：

- **输入管理接口的 IPv4 默认网关** - 如果您设置手动 IP 地址，则可以输入网关路由器的**数据接口**或 IP 地址。**data-interfaces** 设置将通过背板发送传出管理流量，以退出数据接口。如果您没有可以访问互联网的单独管理网络，则此设置非常有用。源自管理接口的流量包括需要访问互联网的许可证注册和数据库更新。如果使用 **data-interfaces**，仍可以在管理接口上使用 FDM（如果直接连接到管理网络），但是，要在“管理”网络上进行远程管理，则需要在“管理”网络上输入网关路由器的 IP 地址。请注意，数据接口上的 FDM 管理不受此设置的影响。如果使用 DHCP，则系统使用 DHCP 提供的网关，如果 DHCP 不提供网关，则使用**数据接口**作为回退方法。
- **如果网络信息已更改则需要重新连接** - 如果您已通过 SSH 连接到默认 IP 地址，但在初始设置时更改了 IP 地址，则会断开连接。使用新 IP 地址和密码重新进行连接。控制台连接不会受影响。
- **在本地管理设备**？ - 输入 **yes** 以使用 CDO 或 FDM。回答 **no** 表示您打算使用 FMC 来管理设备。

示例：

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes

>
```

步骤 4 在新的管理 IP 地址上登录 FDM。

登录 FDM

登录 FDM 以配置 FTD。在将设备载入 CDO 之前，使用 FDM 安装向导完成初始配置。

开始之前

- 使用当前版本的 Firefox 或 Chrome。

过程

步骤 1 在浏览器中输入以下 URL。

- 内部（以太网 1/2）- **https://192.168.1.1**。
- （6.6 和更高版本）管理 - **https://***management_ip*。管理接口是 DHCP 客户端，因此 IP 地址取决于您的 DHCP 服务器。如果在 CLI 设置中更改了管理 IP 地址，则输入该地址。
- （6.5 和更低版本）管理 - **https://192.168.45.45**。如果在 CLI 设置中更改了管理 IP 地址，则输入该地址。

步骤 2 使用用户名 **admin** 和默认密码 **Admin123** 登录。

下一步做什么

- 通过 FDM 安装向导运行；请参阅完成初始配置，第 11 页。

完成初始配置

首次登录FDM以完成初始配置时，请使用设置向导。完成设置向导后，您的设备应该会正常工作并应部署了下列基本策略：

- 外部（Ethernet1/1）和内部接口（Ethernet1/2）。
- 内部和外部接口的安全区域。
- 信任所有内部到外部流量的访问规则。
- 接口 NAT 规则，用于将所有内部到外部流量转换到外部接口 IP 地址上的唯一端口。
- 在内部接口上运行的 DHCP 服务器。

过程

步骤 1 系统会提示您阅读和接受“最终用户许可协议”并更改管理员密码。

只有完成这些步骤，才能继续。

步骤 2 为外部接口和管理接口配置以下选项，然后单击**下一步**。

注释　单击**下一步**后，您的设置将部署到设备中。该接口将命名为“outside”，并添加到“outside_zone”安全区。确保您的设置正确。

a) **外部接口** - 即连接到网关路由器的数据端口。在初始设备设置期间，您不能选择其他外部接口。第一个数据接口是默认的外部接口。

配置 IPv4 (Configure IPv4) - 外部接口的 IPv4 地址。可以使用 DHCP，也可以手动输入静态 IP 地址、子网掩码和网关。另外，也可以选择**关**，不配置 IPv4 地址。 您无法使用设置向导配置 PPPoE。如果接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，并且 ISP 使用 PPPoE 来提供 IP 地址，则可能需要使用 PPPoE。您可以在完成向导后配置 PPPoE。

配置 Ipv6 - 外部接口的 Ipv6 地址可以使用 DHCP，也可以手动输入静态 IP 地址、前缀和网关。另外，也可以选择**关**，不配置 IPv6 地址。

b) **管理接口**

DNS 服务器 - 系统管理地址的 DNS 服务器。输入 DNS 服务器的一个或多个地址以解析名称。默认值为 OpenDNS 公共 DNS 服务器。如果您编辑字段并想要恢复默认值，请单击**使用 OpenDNS** 以重新将合适的 IP 地址载入字段。

防火墙主机名 - 系统管理地址的主机名。

步骤 3 配置系统时间设置，然后单击**下一步**。

a) **时区** - 选择系统时区。

b) **NTP 时间服务器** - 选择使用默认 NTP 服务器，还是手动输入 NTP 服务器的地址。可以添加多个服务器来提供备份。

步骤 4 选择**启动 90 日评估期而不注册**。

您购买的 Firepower 威胁防御设备自动包含一个基础许可证。其他所有许可证均是可选的。

注意　即使您有 Smart Software Manager 帐户和可用许可证，也可以选择使用 90 日评估许可证。您可以在 FTD 载入 CDO 后再授予智能许可。这种选择可避免取消注册后再重新注册许可证。

步骤 5 单击**完成**。

下一步做什么

- 继续登录 CDO，第 12 页，开始载入过程。
- 您应在载入 CDO 后注册并许可您的设备；请参阅将设备载入 CDO，第 17 页。

登录 CDO

CDO 使用 Cisco Secure Sign-On 作为身份提供商，并使用 Duo Security 进行多因素身份验证 (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 Duo Security 按需生成的一次性密码 (OTP)。

建立 Cisco Secure Sign-On 凭证后，您可以从 Cisco Secure Sign-On 控制板登录 CDO。在 Cisco Secure Sign-On 控制板上，还可以登录任何其他支持的 Cisco 产品。

- 如果您有 Cisco Secure Sign-On 帐户，请提前跳转至 使用 Cisco Secure Sign-On 登录 CDO ，第 15 页。
- 如果您没有 Cisco Secure Sign-On 帐户，请参阅创建新的 Cisco Secure Sign-On 帐户，第 13 页。

创建新的 Cisco Secure Sign-On 帐户

初始登录工作流程分为四步。您需要完成所有四个步骤。

开始之前

- **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设置为正确的时间。
- 使用当前版本的 Firefox 或 Chrome。

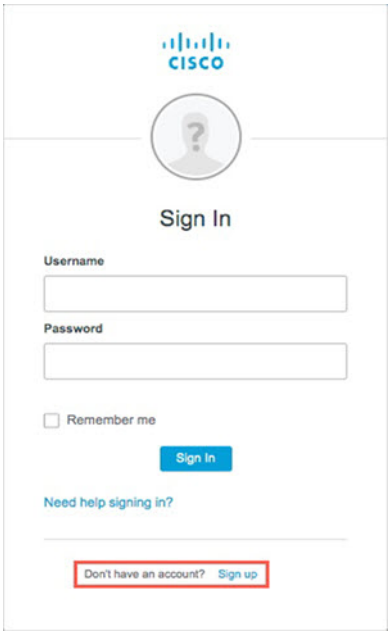
过程

步骤 1 注册新的 **Cisco Secure Sign-On** 帐户。

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

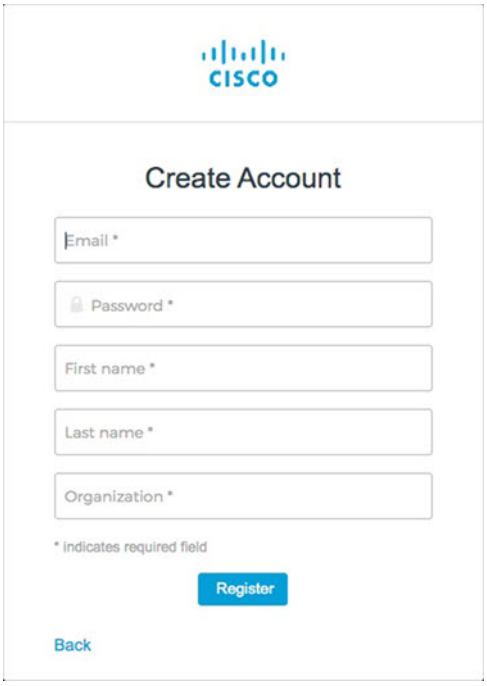
b) 在“登录”屏幕的底部，单击**注册**。

图 *2: Cisco SSO* 注册



c) 填写**创建帐户**对话框中的字段，然后单击**注册**。

图 *3:* 创建账户



提示 输入您计划用于登录 CDO 的电子邮件地址，并添加组织名称以代表您的公司。

d) 单击**注册**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，然后单击**激活帐户**。

步骤 2 使用 **Duo** 设置多因素身份验证。

a) 在**设置多因素身份验证**屏幕中，单击**配置**。

b) 单击**开始设置**，按照提示选择设备，然后验证该设备与您的帐户是否配对。

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，单击**继续登录**。

d) 通过双因素身份验证登录 Cisco Secure Sign-On。

步骤 3 （可选） **将 Google Authenticator 设置为附加身份验证器**。

a) 选择要与 Google Authenticator 配对的移动设备，然后单击**下一步**。

b) 按照设置向导中的提示设置 Google Authenticator。

步骤 4 配置 **Cisco Secure Sign-On** 帐户的帐户恢复选项。

a) 选择一个“忘记密码”问答。

b) 选择恢复电话号码以使用 SMS 重置帐户。

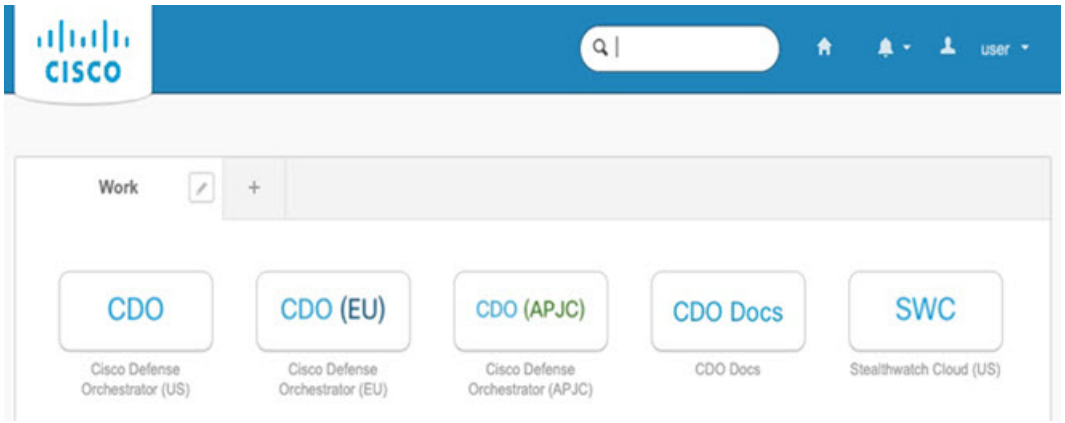
c) 选择安全图像。

d) 单击**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。

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

图 *4: Cisco SSO* 控制板



使用 Cisco Secure Sign-On 登录 CDO

登录 CDO 以载入和管理您的 FTD。

开始之前

Cisco Defense Orchestrator (CDO) 使用 Cisco Secure Sign-On 作为身份提供商，并使用 Duo Security 进行多因素身份验证 (MFA)。

- 要登录 CDO，必须先在 Cisco Secure Sign-On 中创建帐户，然后再使用 Duo 配置 MFA；请参阅创建新的 Cisco Secure Sign-On 帐户，第 13 页。
- 使用当前版本的 Firefox 或 Chrome。

过程

步骤 1 在网络浏览器中，导航到https://sign-on.security.cisco.com/。

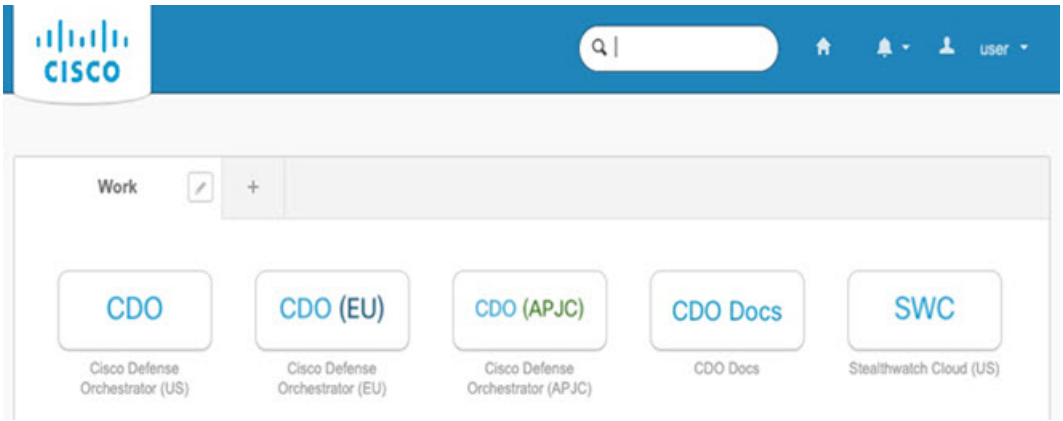
步骤 2 输入您的**用户名**和**密码**。

步骤 3 单击 **Log in**（登录）。

步骤 4 使用 Duo Security 接收另一个身份验证因素，然后确认登录。系统将确认您登录并显示 Cisco Secure Sign-On 控制板。

步骤 5 在 Cisco Secure Sign-On 控制板上单击适当的 CDO 图块。**CDO** 图块将您导向 https://defenseorchestrator.com，**CDO (EU)** 图块将您导向 https://defenseorchestrator.eu。

图 *5: Cisco SSO* 控制板



步骤 6 请单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帐户。

将设备载入 CDO

载入设备之前，请确保完成 FDM 安装向导。然后使用 CDO 的载入向导来载入您的设备并许可该设备。

您可以通过以下两种方式之一载入设备：

- 使用注册密钥（推荐）。
- 使用设备凭证（用户名和密码）和 IP 地址。

注意 我们建议在载入设备之前使用评估许可证。必须在载入 CDO 之前先取消注册向 Smart Software Manager 注册的任何其他许可证，然后重新注册；请参阅配置许可。

使用注册密钥载入（推荐）

您可以使用注册密钥载入设备。我们建议使用此方法，尤其是您的设备使用 DHCP 获取 IP 地址时。如果该 IP 地址更改，您的设备仍会连接到 CDO。

使用凭证和 IP 地址载入

您可以使用设备的管理员用户名和密码，以及设备的外部、内部或管理接口的 IP 地址（具体取决于您的网络中配置设备的方式）载入 FTD；请参阅您的设备的网络配置和部署详细信息。

CDO 需要通过 HTTPS 访问设备才能管理它。如何允许通过 HTTPS 访问设备取决于您的 FTD 在网络中的配置方式，以及您的 Secure Device Connector (SDC) 安装在本地还是云中。

重要事项 如果您连接到 https://www.defenseorchestrator.eu，则必须使用用户名、密码和 IP 地址载入您的设备。您不能使用注册密钥载入 FTD 设备。

使用云 SDC 可对设备的外部接口进行管理访问。使用本地 SDC 可使用内部或管理接口对设备进行管理访问。请注意，当使用 FTD 作为 VPN 连接的前端时，将无法使用外部接口来管理设备。

有关如何将 CDO 连接到您的 SDC 以及需要允许何种网络访问的详细信息，请参阅将 Cisco Defense Orchestrator 连接到 Secure Device Connector。

使用注册密钥载入 FTD（版本 6.4 或 6.5）

按照以下程序使用注册密钥载入 FTD 设备。

开始之前

- （版本 6.4）此方法仅支持美国地区 (defenseorchestrator.com)。

注释 对于欧盟地区 (defenseorchestrator.eu)，此方法自版本 6.5 起提供。对于运行版本 6.4 的设备，您只能使用用户名、密码和 IP 地址载入 FTD 设备。您不能使用注册密钥。

- （版本 6.5）美国、欧盟和亚太及日本 (apj.cdo.cisco.com) 地区支持此方法。
- 您的设备必须通过 Firepower Device Manager (FDM) 进行管理。
- 确保设备上安装的许可证未注册到 Cisco Smart Software Manager。如果 FTD 已经过智能许可，您将需要取消注册；请参阅取消注册智能许可的 FTD，第 32 页。
- 您的设备应配置为使用 90 天评估许可证。
- 登录 FDM 并确保设备上没有等待处理的更改。
- 确保在您的 FTD 设备上正确配置 DNS。
- 请确保在 FTD 设备上正确配置时间服务。请确保 FTD 设备显示正确的日期和时间，否则载入将失败。
- 请查看将 Cisco Defense Orchestrator 连接到 Secure Device Connector。

过程

步骤 1 在导航窗格中，单击**设备和服务**，然后单击蓝色的加号按钮**载入**设备。

步骤 2 单击 **FTD** 卡。

步骤 3 在“载入 FTD 设备”屏幕上，单击**使用注册密钥**。

步骤 4 在“设备名称”区域的**设备名称**字段中输入设备名称。它可以是设备的主机名或您选择的任何其他名称，然后单击**下一步**。

步骤 5 在**数据库更新**区域中，**立即执行安全更新并启用定期更新**默认启用。

此选项立即触发安全更新并自动安排设备在每周一凌晨 2 点检查是否有额外更新。有关详细信息，请参阅更新 FTD 安全数据库和计划安全数据库更新。

注释 禁用此选项不会影响您通过 FDM 配置的以前计划的任何更新。

步骤 6 单击**下一步**。

步骤 7 在**创建注册密钥**区域中，CDO 将生成注册密钥。

注意 如果您在密钥生成后和设备完全载入之前离开载入屏幕，将无法再返回到载入屏幕。但是，CDO 会在**设备和服务**页面上为该设备创建占位符。选择设备占位符以查看该设备的密钥。

步骤 8 单击**复制**图标可复制注册密钥。

注释 您可以跳过复制注册密钥的步骤，然后单击**下一步**完成设备的占位符输入，稍后注册设备。如果您尝试先创建设备后注册，或者您是在客户网络中安装价值证明 (POV) 设备的 Cisco 合作伙伴，则此选项很有用。

设备现在处于连接状态“未提供”。将**未提供**下显示的注册密钥复制到 Firepower Defense Manager，以完成载入过程。

步骤 9 在要载入 CDO 的设备上登录 FDM。

步骤 10 在 Cisco Defense Orchestrator 图块中，单击**开始**。

步骤 11 在**注册密钥**字段中，粘贴您在 CDO 中生成的注册密钥。

步骤 12 在**区域**字段中，选择您的租户要分配到的 Cisco 云区域：

- 如果您登录到 *defenseorchestrator.com*，请选择**美国**。
- 如果您登录到 *defenseorchestrator.eu*（版本 6.5），请选择**欧盟**。
- 如果您登录到 *apj.cdo.cisco.com*（版本 6.5），请选择**亚太及日本地区**。

步骤 13 单击**注册**，然后**接受** Cisco 披露声明。FDM 将注册请求发送到 CDO。

步骤 14 返回 CDO。在**智能许可证**区域中，将智能许可证应用到 FTD 设备，然后单击**下一步**。

有关详细信息，请参阅 配置许可，第 24 页。单击**跳过**以使用 90 天评估许可证继续载入。

步骤 15 从**设备和服务**中，观察设备状态从“未提供”到“正在定位”到“正在同步”再到“已同步”的发展过程。

步骤 16 在**完成**区域中，单击**转到设备**页面以查看载入的设备。

使用凭证和 IP 地址载入 FTD

按照此程序仅使用管理员的用户名和密码以及设备的管理 IP 地址载入 FTD 设备。

开始之前

载入 FTD 设备的最简单方法是使用登录凭证（用户名和密码）和 IP 地址。不过，我们建议您使用注册密钥载入设备；请参阅使用注册密钥载入（推荐），第 17 页。

重要事项 将设备载入 CDO 之前，请阅读载入 FTD。它列出了载入 FTD 设备的一般设备要求和前提条件。

使用此方法载入设备需要以下信息：

- 管理员的用户名和密码。
- 用来管理设备的接口的 IP 地址。它可以是管理接口、内部接口或外部接口，具体取决于您的网络配置。

- 设备必须由 Firepower Device Manager (FDM) 管理，并针对本地管理而配置，以便将其载入 CDO。它不能由 Firepower Management Center (FMC) 管理。

过程

步骤 1 导航到**设备和服务**页面。

步骤 2 单击**载入**。

步骤 3 单击 **FTD** 卡。

注释 CDO 可能会提示您阅读并接受 Firepower Threat Defense 最终用户许可协议 (EULA)，这是租户中的一次性活动。接受本协议后，CDO 不会在后续的 FTD 载入中再次提示您接受协议。如果 EULA 协议未来发生变化，则您必须在收到提示时再次接受它。

步骤 4 在“载入 FTD 设备”屏幕上，单击**使用凭证**并为设备指定名称。

步骤 5 在**设备位置**字段中，输入设备的管理接口 IP 地址、主机名或完全限定设备名称。默认端口为 443。您可以更改端口号以反映设备的配置。

步骤 6 单击 **Go**（**前往**）。

验证设备的位置后，系统将提示您输入设备管理员的用户名和密码。

步骤 7 在**数据库更新**区域中，**立即执行安全更新并启用定期更新**默认启用。

此选项立即触发安全更新并自动安排设备在每周一凌晨 2 点检查是否有额外更新。有关详细信息，请参阅更新 FTD 安全数据库和计划安全数据库更新。

注释 禁用此选项不会影响您通过 FDM 配置的以前计划的任何更新。

步骤 8 单击**连接**。

步骤 9 （可选）为您的设备添加标签。

验证凭证后，系统会提示您为设备或服务添加标签。有关详细信息，请参阅标签和标签组。

步骤 10 载入完成后，CDO 会在**设备和服务**页面上显示状态为“已同步”的设备。

步骤 11 在**智能许可证**区域中，可将智能许可证应用到 FTD 设备，然后单击**下一步**。

有关详细信息，请参阅 配置许可，第 24 页。单击**跳过**以使用 90 天评估许可证继续载入。

在 CDO 中配置设备

以下步骤概述了可能需要配置的其他功能。请单击页面上的帮助按钮 (**?**)，获取有关每个步骤的详细信息。

过程

步骤 1 登录 CDO 门户网站，从 CDO 菜单中选择**设备和服务**，然后选择您刚载入的设备。

步骤 2 选择**管理** > **接口**，然后选择要配置的物理接口。

步骤 3 单击要配置的每个接口对应的编辑图标 ( )，然后为接口提供**逻辑名称**和**说明**（可选）。

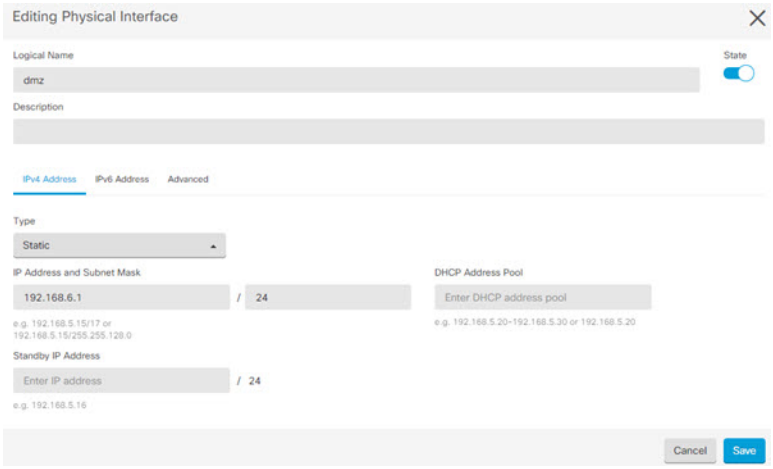
除非配置子接口，否则接口应有名称。

注释 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

步骤 4 设置**类型**并定义 IP 地址和其他设置。

以下示例将一个接口配置为用作“隔离区”(DMZ)，可以将可公开访问的资产（例如 Web 服务器）放在该区域中。完成后单击 **Save**。

图 *6:* 编辑接口

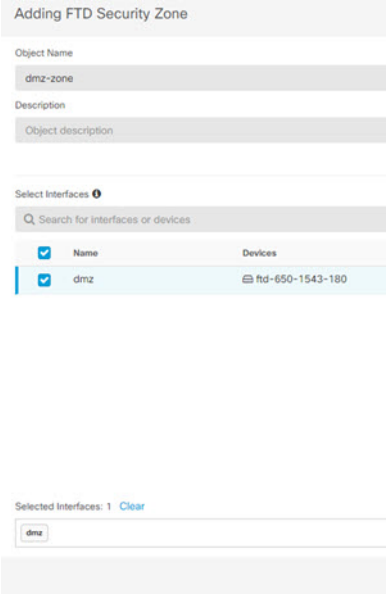


步骤 5 如果您配置了新接口，请选择**管理** > **对象**。

根据需要编辑或创建新的**安全区域**。每个接口都必须属于一个区域，因为需要根据安全区域而不是接口来配置策略。配置接口时不能将其放在区域中，因此每当创建新接口或更改现有接口的用途之后，都必须编辑区域对象。

以下示例显示如何为 DMZ 接口创建一个新的 DMZ 区域。

图 *7:* 安全区域对象



步骤 6 如果希望内部客户端使用 DHCP 从设备获取 IP 地址，请选择**管理** > **设置** > **DHCP 服务器**，然后查看 **DHCP 服务器**部分。

内部接口已配置了 DHCP 服务器，但可以编辑地址池或甚至将其删除。如果配置了其他内部接口，则在这些接口上设置 DHCP 服务器是非常典型的做法。单击 +，为每个内部接口配置服务器和地址池。

您还可以在 **DNS 服务器**选项卡上查看提供给客户端的 DNS 设置。以下示例显示如何在 inside2 接口（地址池为 192.168.45.46-192.168.45.254）上设置 DHCP 服务器。

图 *8: DHCP* 服务器

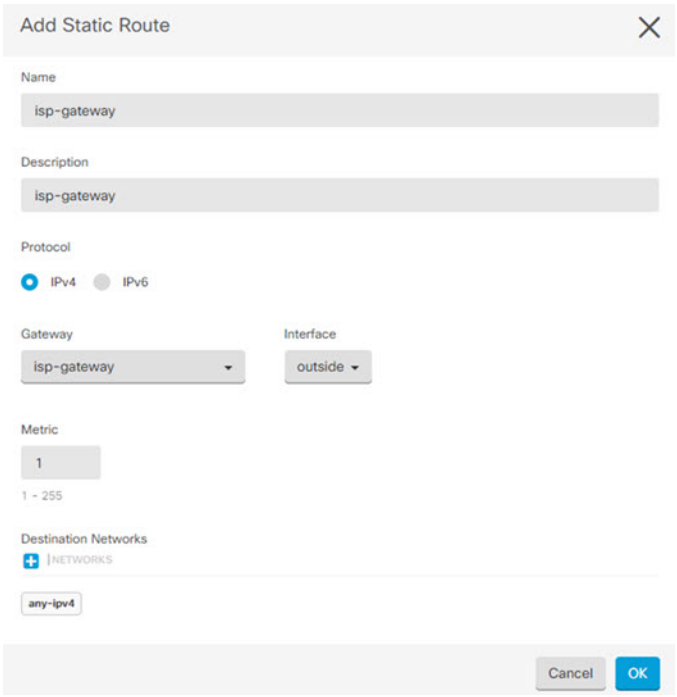
步骤 7 选择**管理** > **路由**，然后单击“添加”图标以配置默认路由。

默认路由通常指向位于外部接口之外的上游或 ISP 路由器。默认的 IPv4 路由适用于 any-ipv4 (0.0.0.0/0)，而默认的 IPv6 路由适用于 any-ipv6 (::0/0)。为所使用的每个 IP 版本创建路由。如果使用 DHCP 获取外部接口的地址，则可能已经拥有所需的默认路由。

注释　此页面上定义的路由仅适用于数据接口，而不会影响管理接口。在**管理** > **设置** > **管理访问**中设置管理网关。

以下示例显示 IPv4 的默认路由。在此示例中，isp-gateway 是用于标识 ISP 网关 IP 地址的网络对象（必须从 ISP 中获取地址）。可以通过单击**网关**下拉列表底部的**创建新对象**，以创建该对象。

图 *9:* 默认路由



步骤 8　选择**管理** > **策略**并配置网络的安全策略。

初始设置允许内部区域与外部区域之间的流量流动，并对流量通往外部接口的所有接口启用网络地址转换 (NAT)。即使配置了新接口，如果将其添加到内部区域对象中，访问控制规则也将自动应用于这些接口。

但是，如果有多个内部接口，则需要一条访问控制规则来允许内部区域之间的流量。如要添加其他安全区域，则需要规则来允许这些区域之间的流量。这是您需要进行的最低限度的更改。

此外，您还可配置其他策略以提供附加服务，并对 NAT 和访问规则进行精细调整，以实现组织需要的结果。您可以配置以下策略：

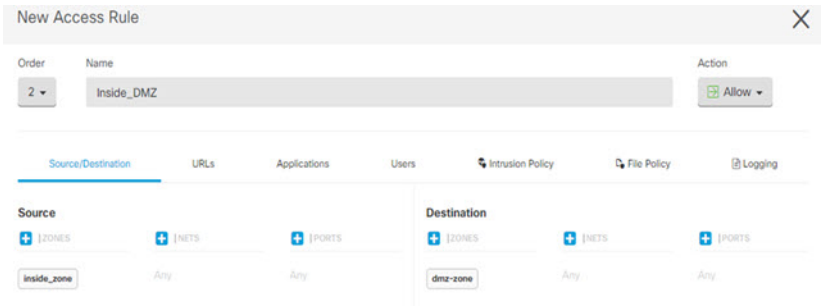
- **SSL 解密** - 如果要检查加密连接（例如 HTTPS）是否存在入侵、恶意软件等，则必须解密连接。使用 SSL 解密策略确定需要解密的连接。系统检查连接后，会将其重新加密。
- **身份** - 如果要将网络活动与各个用户相关联，或根据用户或用户组成员身份控制网络访问，请使用身份策略确定与给定源 IP 地址关联的用户。
- **Security Intelligence** - 使用安全情报策略快速丢弃进出列入黑名单的 IP 地址或 URL 的连接。将已知恶意站点列入黑名单后，在访问控制策略中即可无需考虑这些站点。思科提供定期更新的

已知恶意地址和URL源，可使安全情报黑名单实现动态更新。使用情报源，无需通过编辑策略来添加或删除黑名单中的项目。

- **访问控制** - 使用访问控制策略确定网络上允许的连接。您可以按安全区域、IP 地址、协议、端口、应用、URL、用户或用户组进行过滤。您还可以使用访问控制规则来应用入侵策略和文件（恶意软件）策略。使用此策略实施 URL 过滤。

以下示例显示如何在访问控制策略中允许内部区域与 DMZ 区域之间的流量。在此示例中，任何其他选项卡上均未设置任何选项，**日志记录**除外，其中**在连接结束时**选项已被选中。

图 *10*: 访问控制策略



步骤 9 找到**安全数据库更新**部分，创建一个计划的任务，以检查和更新 FTD 设备的安全数据库。

当您将 FTD 设备载入 CDO 时，在载入过程中可以**启用计划的数据库定期更新**。默认情况下，会选中此选项。启用后，CDO 会立即检查并应用任何安全更新，并自动安排设备检查是否有额外更新。在设备载入后，您可以修改计划任务的日期和时间。

如果使用入侵策略，请为“规则”和“VDB”数据库设置定期更新。如果使用安全情报源，请为“规则”和“VDB”数据库设置更新计划。如果在任何安全策略中使用地理位置作为匹配条件，请为“规则”和“VDB”数据库设置更新计划。

步骤 10 单击菜单中的**预览和部署**按钮，然后单击**立即部署**按钮，以部署对设备的更改。

只有将更改部署至设备，更改才会生效。

下一步做什么

- 您应在载入后注册并许可您的设备；请参阅配置许可 ， 第 24 页。

配置许可

FTD 使用思科智能软件许可，这使得您可以集中购买和管理许可证池。

当您注册机箱时，许可证颁发机构会颁发一张ID证书，用于机箱与许可证颁发机构之间的通信。它还会将机箱分配到相应的虚拟帐户。

基本许可证会自动包含在内。智能许可不会阻止您使用尚未购买的产品功能。只要您向思科智能软件管理器进行了注册，即可立即开始使用许可证，并在以后购买该许可证。这使您能够部署和使用功能，并避免由于采购订单审批造成延迟。请参阅以下许可证：

- **威胁** - 安全情报和 Cisco Firepower 下一代 IPS
- **恶意软件** - 适用于网络的高级恶意软件防护 (AMP)
- **URL** - URL 过滤
- **RA VPN** - AnyConnect Plus、AnyConnect Apex 或仅 AnyConnect VPN。

有关为系统授权许可的完整信息，请参阅《FDM 配置指南》。

注意 将设备载入 CDO 之前使用评估许可证。必须在载入 CDO 之前先取消注册向 Smart Software Manager 注册的任何其他许可证，然后重新注册；请参阅取消注册智能许可的 FTD，第 32 页。

开始之前

- 拥有思科智能软件管理器主帐户。

  如果您还没有账户，请单击此链接以设置新账户。通过智能软件管理器，您可以为组织创建一个主账户。

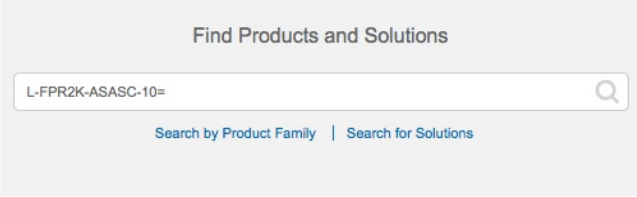
- 您的思科智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

过程

步骤 1 请确保智能许可帐户包含所需的可用许可证。

当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。但是，如果您需要自己添加许可证，则请使用思科商务工作空间上的 **Find Products and Solutions** 搜索字段。搜索以下许可证 PID：

图 *11:* 许可证搜索



注释 如果未找到 PID，您可以手动将 PID 添加到订单中。

- 威胁、恶意软件和 URL 许可证组合：
  - L-FPR2110T-TMC=

- L-FPR2120T-TMC=
- L-FPR2130T-TMC=
- L-FPR2140T-TMC=

当您将上述 PID 之一添加到您的订单时，可以选择与以下 PID 之一对应的定期订用：

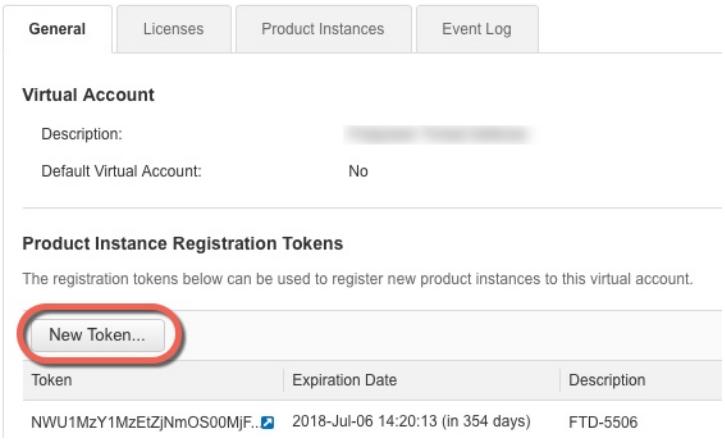
- L-FPR2110T-TMC-1Y
- L-FPR2110T-TMC-3Y
- L-FPR2110T-TMC-5Y
- L-FPR2120T-TMC-1Y
- L-FPR2120T-TMC-3Y
- L-FPR2120T-TMC-5Y
- L-FPR2130T-TMC-1Y
- L-FPR2130T-TMC-3Y
- L-FPR2130T-TMC-5Y
- L-FPR2140T-TMC-1Y
- L-FPR2140T-TMC-3Y
- L-FPR2140T-TMC-5Y

- RA VPN - 请参阅思科 AnyConnect 订购指南。

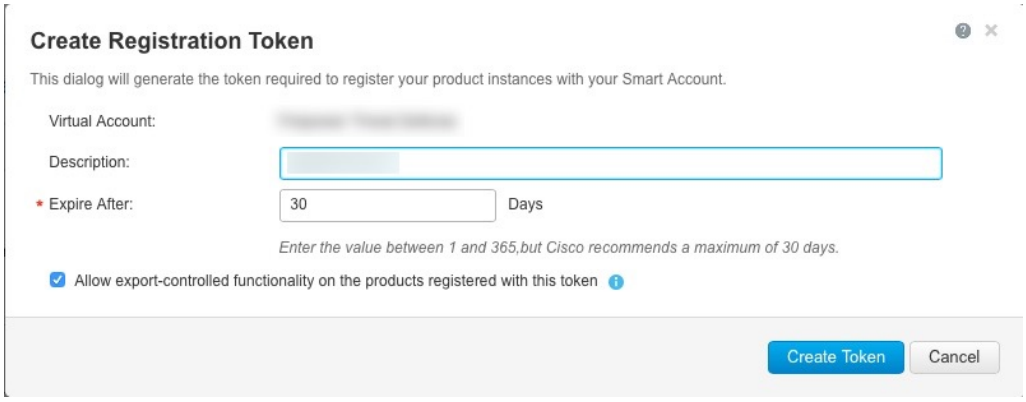
步骤 2 在 Cisco Smart Software Manager 中，为要将此设备添加到的虚拟帐户请求并复制注册令牌。

a) 单击 **Inventory**。

b) 在 **General** 选项卡上，单击 **New Token**。



c) 在 **Create Registration Token** 对话框中，输入以下设置，然后单击 **Create Token**：



- **Description**
- **Expire After** - 思科建议该时间为 30 天。
- **Allow export-controlled functionaility on the products registered with this token**（在使用此令牌注册的产品上允许导出控制的功能）- 在您所在的国家/地区允许进行强加密的情况下启用导出合规性标志。

系统将令牌添加到您的资产中。

d) 单击令牌右侧的箭头图标可以打开 **Token** 对话框，可以从中将令牌 ID 复制到剪贴板。当需要注册 FTD 时，请准备好此令牌，以在该程序后面的部分使用。

图 *12:* 查看令牌

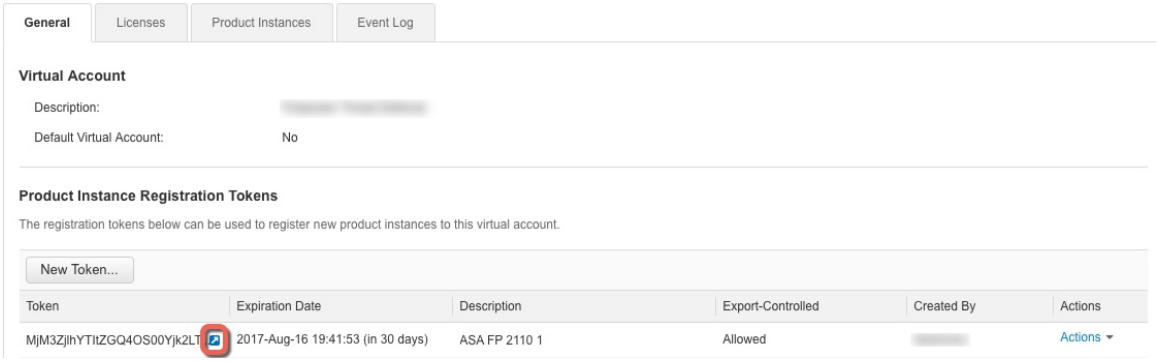
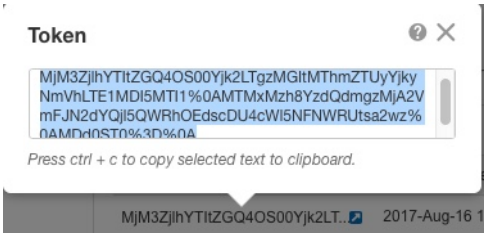


图 *13:* 复制令牌



步骤 3 在 CDO 中，单击**设备和服务**，然后选择要许可的 FTD 设备。

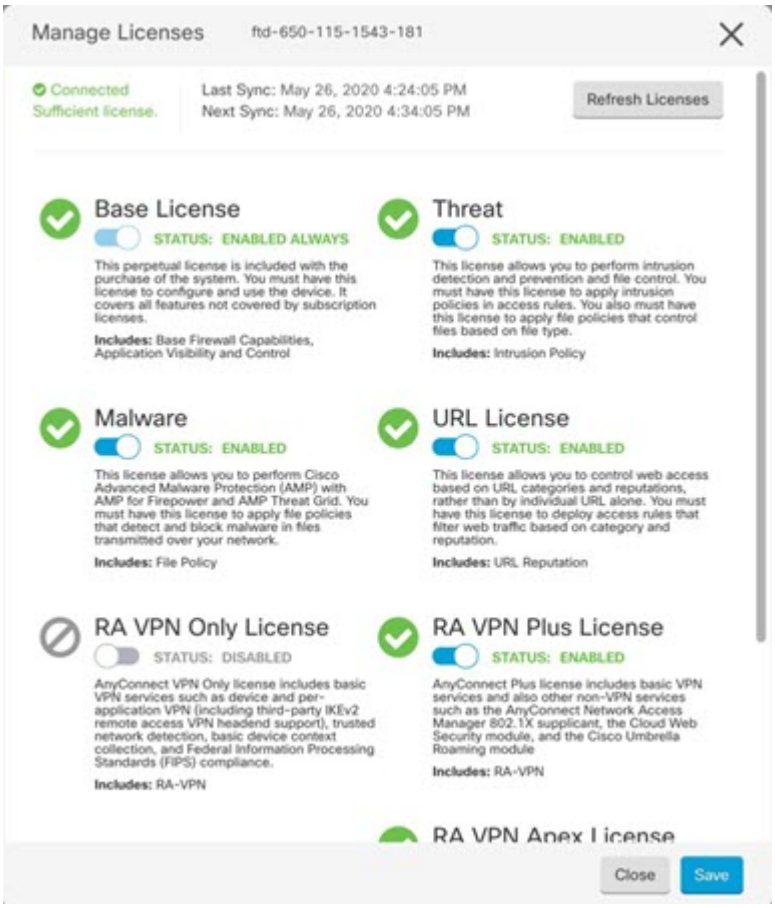
步骤 4 在**设备操作**窗格中，单击**管理许可证**，然后按照屏幕上的说明输入 Smart Software Manager 生成的智能许可证。

步骤 5 单击 **Register Device**。与设备同步后，连接状态变为“在线”。

您将返回到**管理许可证**页面。在设备注册时，您会看到以下消息：

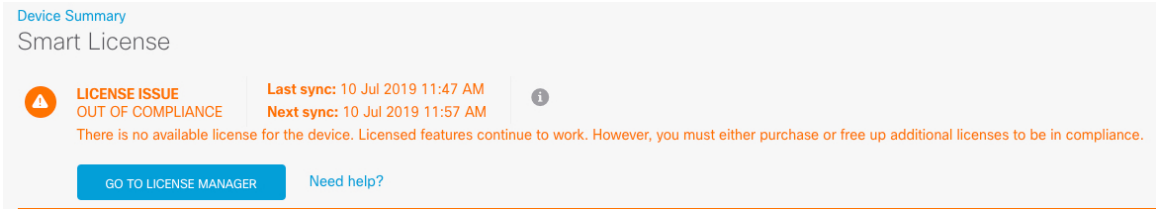
Registration request sent on 10 Jul 2019. Please wait. Normally, it takes about one minute to complete the registration. You can check the task status in Task List. Refresh this page to see the updated status.

步骤 6 成功将智能许可证应用到 FTD 设备后，设备状态将显示**已连接**，**许可证足够**。根据需要，单击每个可选许可证的**启用/禁用**滑块控件。



- **启用** - 将许可证注册到您的思科智能软件管理器账户，并启用控制的功能。现在，您可以配置和部署该许可证控制的策略了。
- **禁用** - 取消许可证向思科智能软件管理器账户的注册，并禁用控制的功能。新策略中无法配置这些功能，也不能再部署使用该功能的策略。
- 如果启用了 **RA VPN** 许可证，请选择要使用的许可证类型：**Plus**、**Apex**、**仅 VPN**或 **Plus 和 Apex**。

启用功能后，如果您的帐户中没有许可证，在刷新页面后，您将看到以下非合规消息：**许可证问题**，**不合规**



步骤 7 选择**刷新许可证**，与 Cisco Smart Software Manager 同步许可证信息。

使用 CDO 管理设备

将设备载入 CDO 后，您可以使用 CDO 管理设备。使用 CDO 管理 FTD：

1. 浏览到 https://sign-on.security.cisco.com。
2. 以您在 创建新的 Cisco Secure Sign-On 帐户，第 13 页 中创建的用户身份登录。
3. 查看使用 Cisco Defense Orchestrator 管理 FTD 中常见管理任务的链接。

后续操作

现在，您已配置了 FTD 设备并将其载入 CDO，后者为 FTD 设备提供简化的管理接口和云访问。使用 CDO 为 FTD 设备升级软件、配置高可用性并配置设备设置和网络资源。

其他 FTD 管理程序

以下主题提供了有关管理 FTD 设备的一些其他信息：

- - 使用命令行界面 (CLI) 执行基本的系统故障排除。仅将 FXOS CLI 用于机箱级故障排除。使用 FTD CLI 进行基本配置、监控和正常的系统故障排除。
- 取消注册智能许可的 FTD，第 32 页- 我们强烈建议您使用评估许可证，直到设备载入 CDO。必须在载入 CDO 之前先取消注册向 Smart Software Manager 注册的任何其他许可证，然后重新注册。
- 断开设备电源，第 32 页- 如果出于任何原因（如重定位设备）需要关闭系统，必须遵循推荐的程序正常关闭设备电源。
- 后续操作，第 33 页- 提供指向 CDO 资源的有用链接。

访问 FTD 和 FXOS CLI

使用命令行界面 (CLI) 可设置系统以及对系统进行基本的故障排除。无法通过 CLI 会话配置策略。可以连接到控制台端口以访问 CLI。

也可以访问 FXOS CLI 以进行故障排除。

注释 您也可以通过 SSH 连接到 FTD 设备的管理接口。与控制台会话不同，SSH 会话默认使用 FTD CLI，由此可使用 **connect fxos** 命令连接到 FXOS CLI。如果您为 SSH 连接打开某个数据接口，稍后可以连接到该接口上的地址。默认情况下，禁用 SSH 数据接口访问。此程序介绍控制台端口的访问（默认使用 FXOS CLI）。

过程

步骤 1 要登录CLI，请将管理计算机连接到控制台端口。控制台端口默认为FXOS CLI。有关控制台电缆的详细信息，请参阅设备的硬件指南。使用以下串行设置：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

您将连接到 FXOS CLI。使用 **admin** 用户名和初始设置时设置的密码（默认值为 **Admin123**）登录 CLI。

示例：

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

步骤 2 访问 FTD CLI。

connect ftd

示例：

```
firepower# connect ftd
>
```

登录后，如需了解 CLI 中可用命令的相关信息，请输入 **help** 或 **?**。有关使用信息，请参阅 *Firepower 威胁防御命令参考*。

步骤 3 要退出 FTD CLI, 请输入 **exit** 或 **logout** 命令。

此命令会将您重新导向至 FXOS CLI 提示。有关 CLI 中可用命令的相关信息，请输入 **?**。

示例：

```
> exit
firepower#
```

取消注册智能许可的 FTD

如果 FTD 已经过智能许可，设备可能会注册到 Smart Software Manager。您必须先从 Smart Software Manager 取消注册该设备，然后再使用注册密钥将其载入 CDO。取消注销时，与设备关联的基本许可证和所有可选许可证将在您的虚拟帐户中释放。

注释 在取消注册设备后，设备上的当前配置和策略仍会继续原样运行，但您无法进行或部署任何更改。

过程

步骤 1 使用 FDM 登录 FTD。

步骤 2 在 FDM 菜单中单击设备的名称，然后单击智能许可证摘要区域中的**查看配置**。

步骤 3 从齿轮下拉菜单中选择**取消注册设备**。

步骤 4 阅读警告并单击**取消注册**，以取消注册该设备。

下一步做什么

- 在 Smart Software Manager 中取消注册设备后，您可以使用注册令牌将设备载入 CDO；请参阅使用注册密钥载入 FTD（版本 6.4 或 6.5），第 17 页。

断开设备电源

使用FDM正确关闭系统非常重要。仅拔掉电源或按下电源开关可能会导致文件系统严重损坏。请记住，有许多进程一直在后台运行，拔掉或关闭电源不能正常关闭 Firepower 系统。

过程

步骤 1 （6.5 及更高版本）使用 FDM 关闭设备。

注释 对于 6.4 及更早版本，请在 FDM CLI 中输入**shutdown**命令。

a) 单击**设备**，然后单击**系统设置** > **重新引导/关闭**链接。

b) 单击**关闭**。

步骤 2 观察电源 LED 和状态 LED 以验证机箱是否已断电（不亮）。

步骤 3 在机箱成功关闭电源后，您可以在必要时拔下电源插头以物理方式断开机箱的电源。

后续操作

要使用 CDO 继续配置 FTD 设备，请参阅 CDO 配置指南。

有关使用 CDO 的其他信息，请参阅 Cisco Defense Orchestrator 主页。