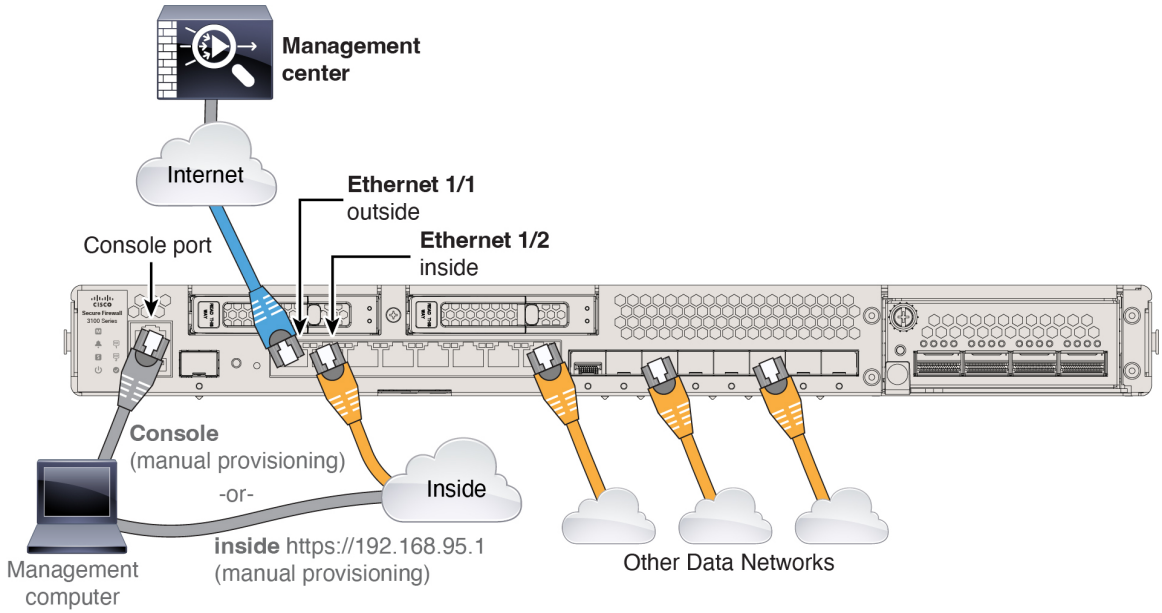
连接并注册防火墙

连接防火墙，然后将防火墙注册到 管理中心。

连接防火墙的电缆

- （可选）获取控制台适配器 - 防火墙配有一条 DB-9 转 RJ-45 串行电缆，所以您需要购买第三方 DB-9-to-USB 串行电缆进行连接。
- 将 SFP/SFP+ 模块安装到以太网 1/9 及以上端口。
- 有关详细信息，请参阅硬件安装指南。
- 除非您在使用具有 零接触调配 的高可用性或打算通过手动调配来使用集群，否则不要将电缆连接到管理接口。在此情况下，请参阅《Cisco Secure Firewall Management Center 设备配置指南》。本指南仅涵盖外部接口。



执行初始配置（手动调配）

对于手动调配，请使用 Cisco Secure Firewall 设备管理器 或 CLI 来执行行初始配置。

初始配置：设备管理器

使用这种方法，在注册防火墙后，除管理接口外还将预先配置以下接口：

- 以太网 1/1 - **outside**，IP 地址来自 DHCP、IPv6 自动配置
- 以太网 1/2 - **inside**，192.168.95.1/24
- 默认路由 - 通过外部接口上的 DHCP 获取
- 其他接口 - 保留 设备管理器 中的任何接口配置。

不会保留其他设置，如内部的 DHCP 服务器、访问控制策略或安全区域。

过程

步骤 1 将计算机连接到内部接口（以太网 1/2 ）。

步骤 2 登录设备管理器。

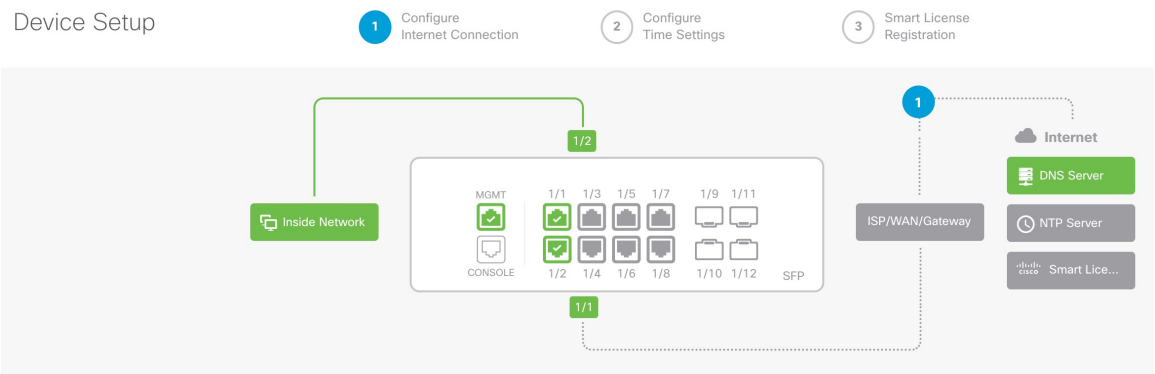
a) 转至https://192.168.95.1。

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

c) 系统会提示您阅读并接受“一般条款”并更改管理员密码。

步骤 3 使用设置向导。

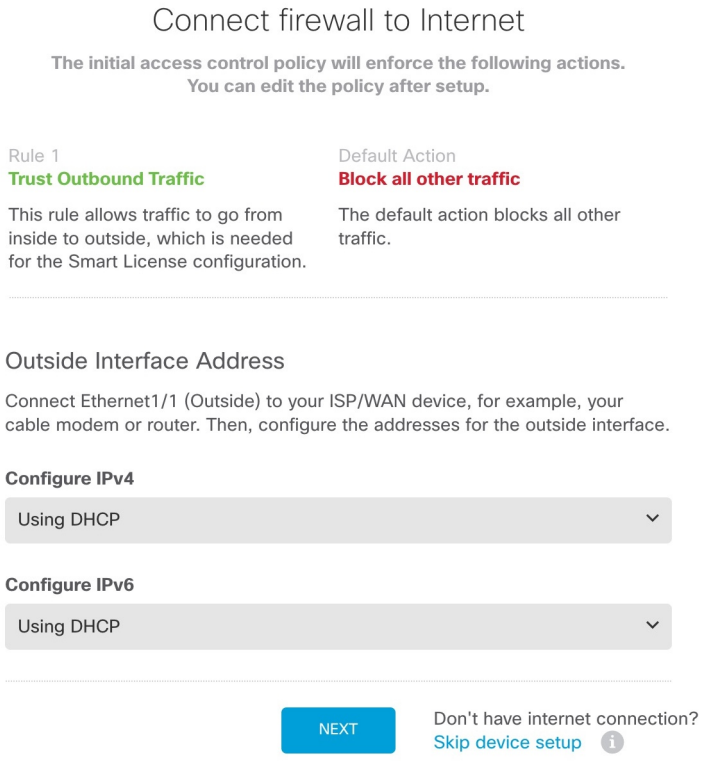
图 *1:* 设备设置



注释
具体的端口配置取决于您的型号。

a) 配置外部接口和管理接口。

图 *2:* 将防火墙连接到互联网



1. **外部接口地址** - 如果您计划实现高可用性，请使用静态 IP 地址。您不能使用设置向导配置 PPPoE；您可以在完成向导后配置 PPPoE。

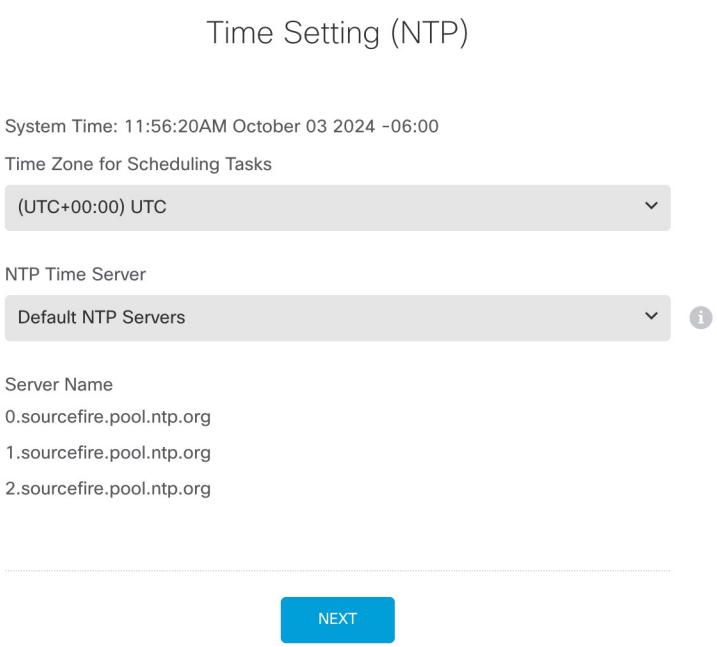
2. **管理接口** - 即使在外部接口上使用管理器访问，也会使用管理接口设置。例如，通过外部接口在背板上路由的管理流量将使用这些管理接口 DNS 服务器，而不是外部接口 DNS 服务器解析 FQDN。

   DNS 服务器 - 系统管理地址的 DNS 服务器。默认值为 OpenDNS 公共 DNS 服务器。这些服务器很可能与您稍后设置的外部接口 DNS 服务器一致，因为它们都是从外部接口访问的。

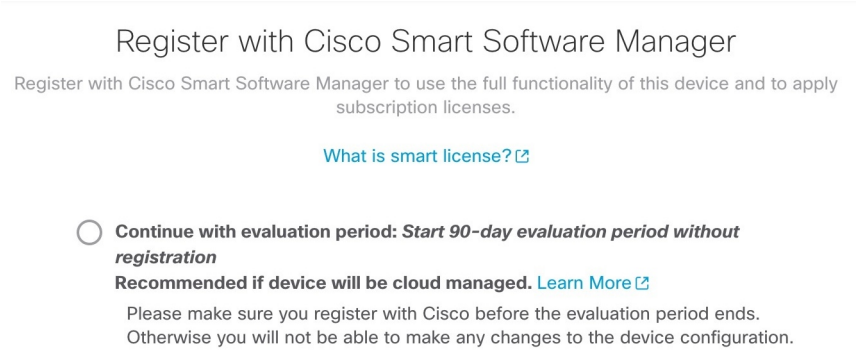
   防火墙主机名

b) 配置**时间设置 (NTP) (Time Setting [NTP])** 并点击**下一步 (Next)**。

图 *3:* 时间设置 *(NTP)*



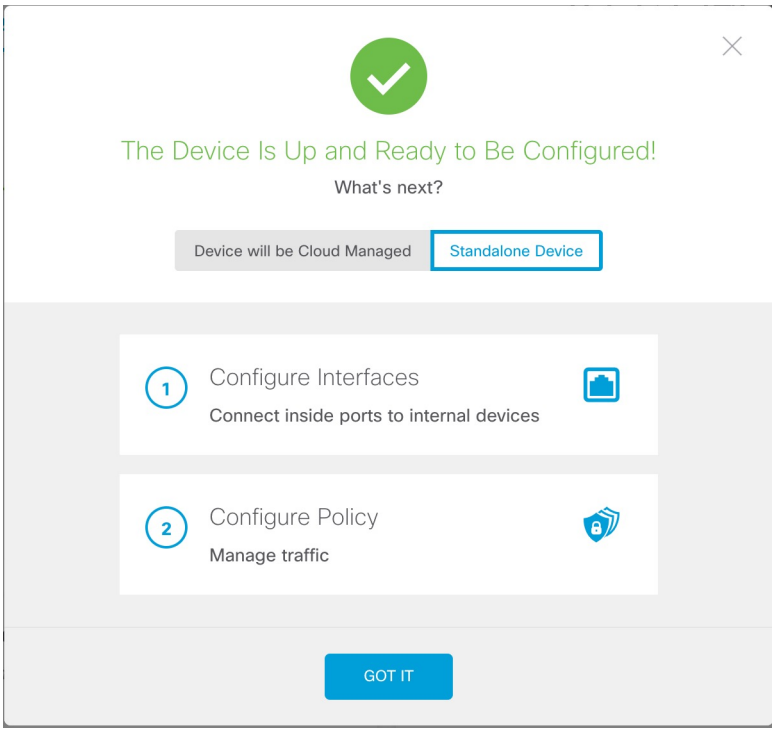
c) 选择**启动 90 日评估期而不注册**。



不要向智能软件管理器注册 威胁防御；所有许可均在 管理中心 上执行。

d) 点击**完成**。

图 *4:* 后续操作



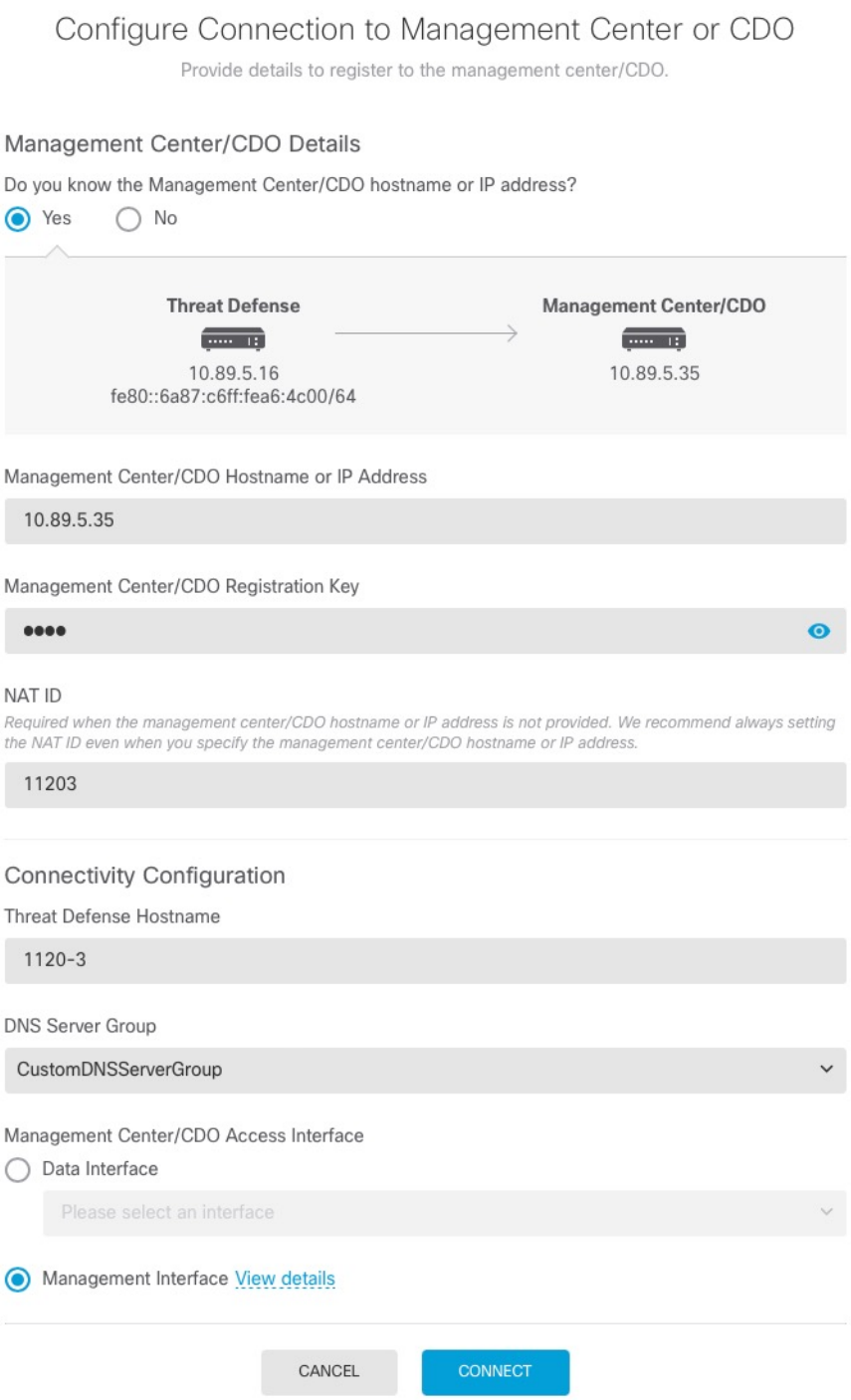
e) 依次选择**独立设备 (Standalone Device)** 和 **明白 (Got It)**。

步骤 4 如果要配置其他接口，请选择**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的链接。

步骤 5 通过选择**设备 (Device)** 、 > **系统设置 (System Settings)** 、 > **集中管理 (Central Management)** 并点击**继续 (Proceed)**，向 管理中心 注册

配置**管理中心/CDO** 详细信息。

图 *5:* 管理中心*/CDO* 详细信息



a) 对于**是否知道管理中心/CDO 主机名或 IP 地址**，如果您可以使用 IP 地址或主机名访问 管理中心，请点击**是 (Yes)**，如果 管理中心 位于 NAT 之后或没有公共 IP 地址或主机名，请点击**否 (No)**。
b) 如果选择**是 (Yes)**，请输入**管理中心**/CDO **主机名/IP 地址**。
c) 指定**管理中心/CDO 注册密钥**。

此密钥是您选择的一次性注册密钥，注册 防火墙时也要在 管理中心 上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 可用于将多个防火墙注册到 管理中心。

d) 指定 **NAT ID**。

此 ID 是您选择的唯一一次性字符串，您还需要在 管理中心上指定它。即使您知道两台设备的 IP 地址，我们仍建议您指定 NAT ID。NAT ID 不得超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 不能用于将任何其他防火墙注册到 管理中心。NAT ID 与 IP 地址结合使用，用于验证连接是否来自正确的设备；只有在对 IP 地址/NAT ID 进行身份验证后，才会检查注册密钥。

步骤 6 配置**连接配置**。

a) 指定**威胁防御主机名**。

此 FQDN 将用于外部接口。

b) 指定 **DNS 服务器组**。

选择一个现有组，或创建一个新组。默认 DNS 组名为 **CiscoUmbrellaDNSServerGroup**，其中包括 OpenDNS 服务器。

要在注册后保留外部 DNS 服务器设置，您需要在 管理中心 中重新配置 DNS 平台设置。

c) 对于**管理中心/CDO 访问接口**，点击**数据接口 (Data Interface)**，然后选择 **outside**。

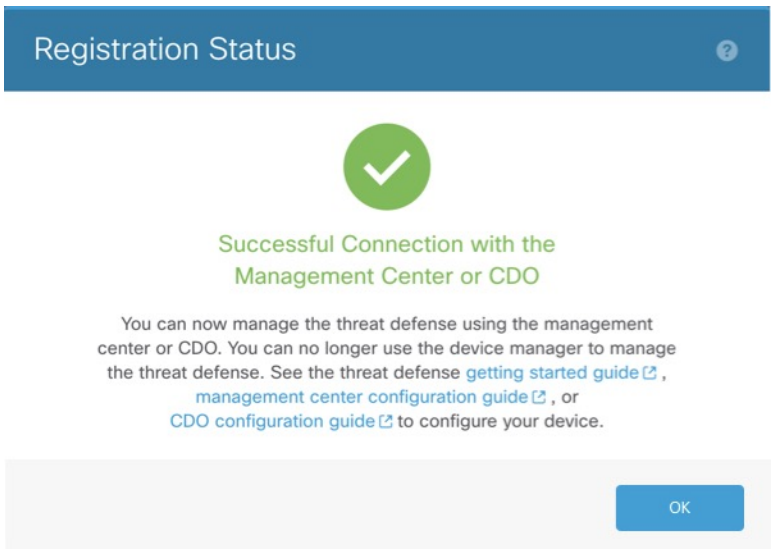
步骤 7 （可选） 点击**添加动态 DNS (DDNS) 方法 (Add a Dynamic DNS [DDNS] method)**。

如果 威胁防御 的 IP 地址发生变化，DDNS 将确保 管理中心 可访问其 FQDN 内的 威胁防御。

步骤 8 点击**连接 (Connect)**。

注册状态 (Registration Status) 对话框将显示 管理中心 注册的当前状态。

图 *6:* 成功连接



步骤 9 在**保存管理中心/CDO 注册设置**步骤之后，转到 管理中心，然后添加防火墙。请参阅通过手动调配向管理中心添加防火墙，第 14 页。

初始配置：CLI

使用 CLI 设置脚本设置专用管理 IP 地址、网关和其他基本网络设置。

过程

步骤 1 连接控制台端口并访问 威胁防御 CLI。请参阅访问威胁防御 CLI。

步骤 2 完成管理界面设置的 CLI 设置脚本。

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 Cisco Secure Firewall Threat Defense 命令参考。

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
Cisco General Terms
[...]

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.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
```

指南：为至少其中一种地址类型输入 **y**。虽然您不打算使用管理接口，但必须设置 IP 地址，例如专用地址。

```
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
```

指南：选择**手动**。使用外部接口访问管理器时，不支持DHCP。确保此接口与管理器访问接口位于不同的子网上，以防止出现路由问题。

```
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
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]:
```

指南：将网关设置为 **data-interfaces**。此设置可将管理流量转发到背板上，以便通过外部接口进行路由。

```
Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
```

指南：设置管理接口 DNS 服务器。这些服务器很可能与您稍后设置的外部接口 DNS 服务器一致，因为它们都是从外部接口访问的。

```
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

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

指南：输入 **no** 以使用 管理中心。

```
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'
```

指南：输入 **routed**。只有路由防火墙模式支持外部管理器访问。

```
Configuring firewall mode ...


Device is in OffBox mode - disabling/removing port 443 from iptables.
Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

步骤 3 配置用于管理器访问的外部接口。

configure network management-data-interface

然后，系统会提示您为外部接口配置基本网络设置。

手动 IP 地址

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
```

```
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
```

指南：要在注册后保留外部 DNS 服务器，您需要在 管理中心 中重新配置 DNS 平台设置。

```
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to change the manager
 access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

DHCP 的 IP 地址

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://dwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to change the manager
 access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

步骤 4 识别 管理中心。

configure manager add {主机名 | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key nat_id*

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} - 指定 管理中心 的 FQDN 或 IP 地址。如果 管理中心 无法直接寻址，请使用 **DONTRESOLVE**，在这种情况下，防火墙必须具有可访问的 IP 地址或主机名。
- *reg_key* - 指定您选择的一次性注册密钥，注册威胁防御时也要在管理中心上指定它。注册密钥不得超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。
- *nat_id* - 指定了您选择的唯一一次性字符串，您还需要在 管理中心 上指定它。NAT ID 不得超过 37 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。此 ID 不能用于将任何其他设备注册到管理中心。

示例：

```
> configure manager add fmc-1.example.com regk3y78 natid56
Manager successfully configured.
```

步骤 5 关闭 威胁防御，以便将设备发送到远程分支机构。

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系统。

a) 输入 **shutdown** 命令。
b) 观察电源 LED 和状态 LED 以验证机箱是否已断电（不亮）。
c) 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。

向管理中心注册防火墙

根据您使用的部署方法向 管理中心 注册防火墙。

使用零接触调配将防火墙添加到管理中心

通过零接触调配，您可以按序列号将设备注册到 管理中心，而无需在设备上执行任何初始设置。管理中心 与思科安全云和 CDO 集成以实现此功能。

使用 零接触调配时，系统会预配置以下接口：请注意，不会保留其他配置设置，例如访问控制策略或安全区。请注意，诸如内部的 DHCP 服务器、访问控制策略或安全区域等其他设置均未配置。

- 以太网 1/1—“外部”，IP 地址来自 DHCP、IPv6 自动配置
- 以太网 1/2（或对于 ，为 VLAN1 接口）-“内部”，192.168.95.1/24
- 默认路由 - 通过外部接口上的 DHCP 获取

零接触调配 不支持集群或多实例模式。

仅当使用管理接口时才支持高可用性，因为 零接触调配 使用 DHCP，数据接口和高可用性不支持 DHCP。

注释 对于 管理中心 版本 7.4，您需要使用 CDO 来添加设备；有关详细信息，请参阅 7.4 指南。7.6 中添加了本地 管理中心 工作流程。此外，对于 7.4 中的云集成，请参阅管理中心中的 **SecureX 集成**页面。

开始之前

- 如果设备没有公共 IP 地址或 FQDN，请为 管理中心 设置公共 IP 地址/FQDN（例如，如果它在 NAT 之后），以便设备可以发起管理连接。请参阅 。

过程

步骤 1 首次使用序列号添加设备时，请将 管理中心 与思科安全云集成。

注释
对于 管理中心 高可用性对，您还需要将辅助 管理中心 与思科安全云集成。

a) 选择**集成 (Integration)** > **思科安全云 (Cisco Security Cloud)**。
b) 点击 **启用思科安全云 (Enable Cisco Security Cloud)** 打开单独的浏览器选项卡，让您登录思科安全云账户并确认显示的代码。

   确保此页面未被弹出窗口阻止程序阻止。如果您还没有思科安全云和CDO账户，您可以在程序期间添加一个。

   有关此集成的详细信息，请参阅 。

   CDO 会在您将 管理中心 与思科安全云集成后载入本地 管理中心 。CDO 需要在其清单中添加 管理中心 ，以便进行零接触调配。但是，您不需要直接使用CDO。如果您使用CDO，其 管理中心 支持仅限于设备载入、查看其托管设备、查看与 管理中心 关联的对象，以及交叉启动 管理中心。

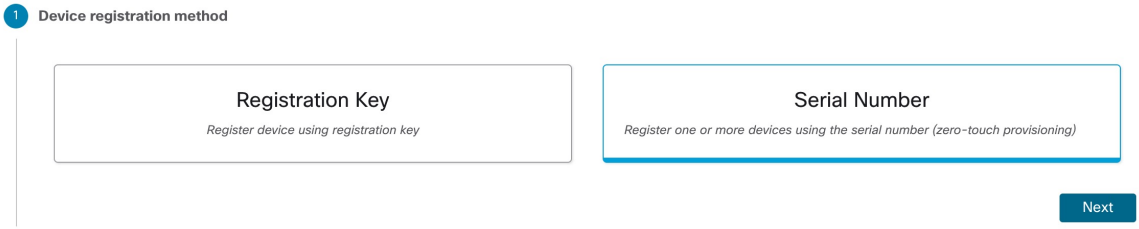
c) 确保选中**启用零接触调配 (Enable Zero-Touch Provisioning)** 。
d) 点击**保存 (Save)**。

步骤 2 选择**设备** > **设备管理**。

步骤 3 从**添加 (Add)** 下拉菜单中，选择**设备（向导）(Device [Wizard])**。

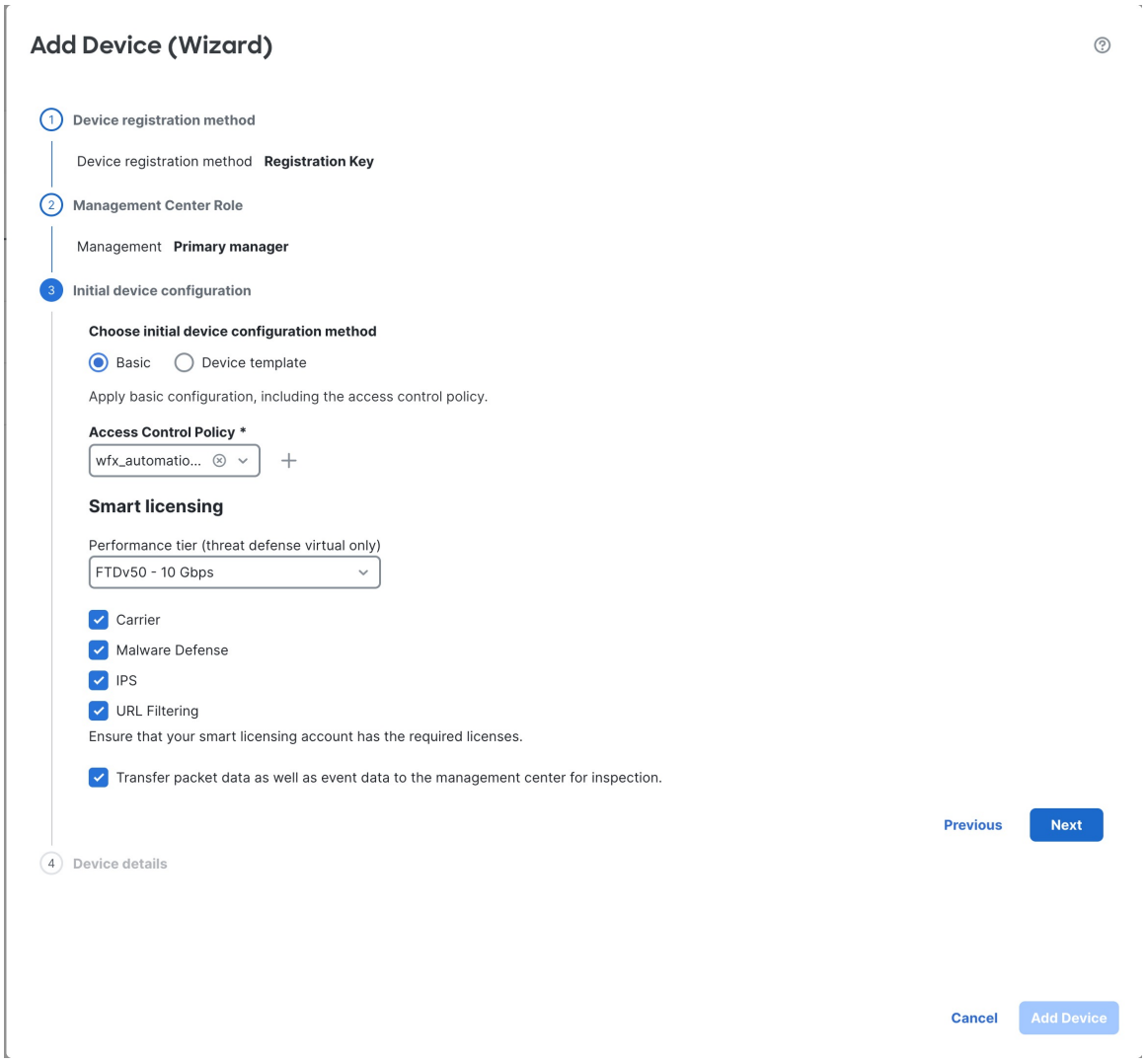
步骤 4 点击**使用序列号 (Use Serial Number)**，然后点击**下一步 (Next)**。

图 *7:* 设备注册方法



步骤 5 对于**初始设备配置 (Initial device configuration)**，点击**基本 (Basic)** 单选按钮。

图 *8:* 初始设备配置方法



a) 选择初始**访问控制策略**以在注册时部署到设备，或创建一个新策略。

如果设备与所选策略不兼容，部署会失败。这种不兼容有多种可能的原因，包括许可不匹配、型号限制、被动与内联问题和其他配置错误。请在解决导致失败的问题后，手动将配置部署到设备。

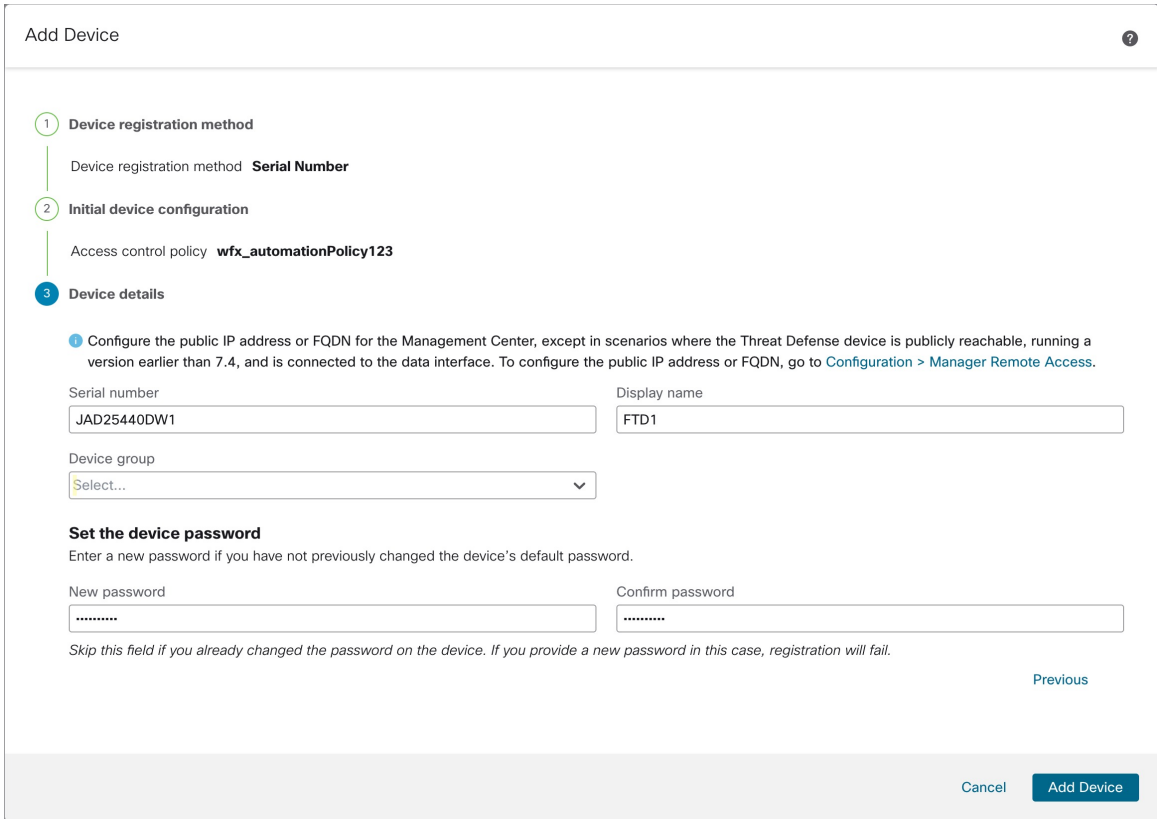
b) 选择要应用到设备的**智能许可**许可证。

在添加设备后，您可以从**系统 (System)** > **许可证 (Licenses)** > **智能许可证 (Smart Licenses)** 页面应用许可证。

c) 点击**下一步**。

步骤 6 配置**设备详细信息 (Device details)**。

图 *9:* 设备详细信息



a) 输入**序列号**。
b) 输入要在 管理中心 中显示的**显示名称**
c) （可选） 选择**设备组 (Device Group)**。
d) **设置设备密码**。

   如果此设备未配置或全新安装，则需要设置新密码。如果您已登录并更改了密码，请将此字段留空。否则，注册将失败。

步骤 7 点击**添加设备**。

管理中心可能需要长达两分钟来验证设备的心跳并建立通信。如果注册成功，设备将添加到列表中。

通过手动调配向管理中心添加防火墙

使用设备 IP 地址或主机名以及注册密钥将防火墙手动注册到 管理中心。

过程

步骤 1 登录管理中心。

a) 输入以下 URL。

https://*fmc_ip_address*

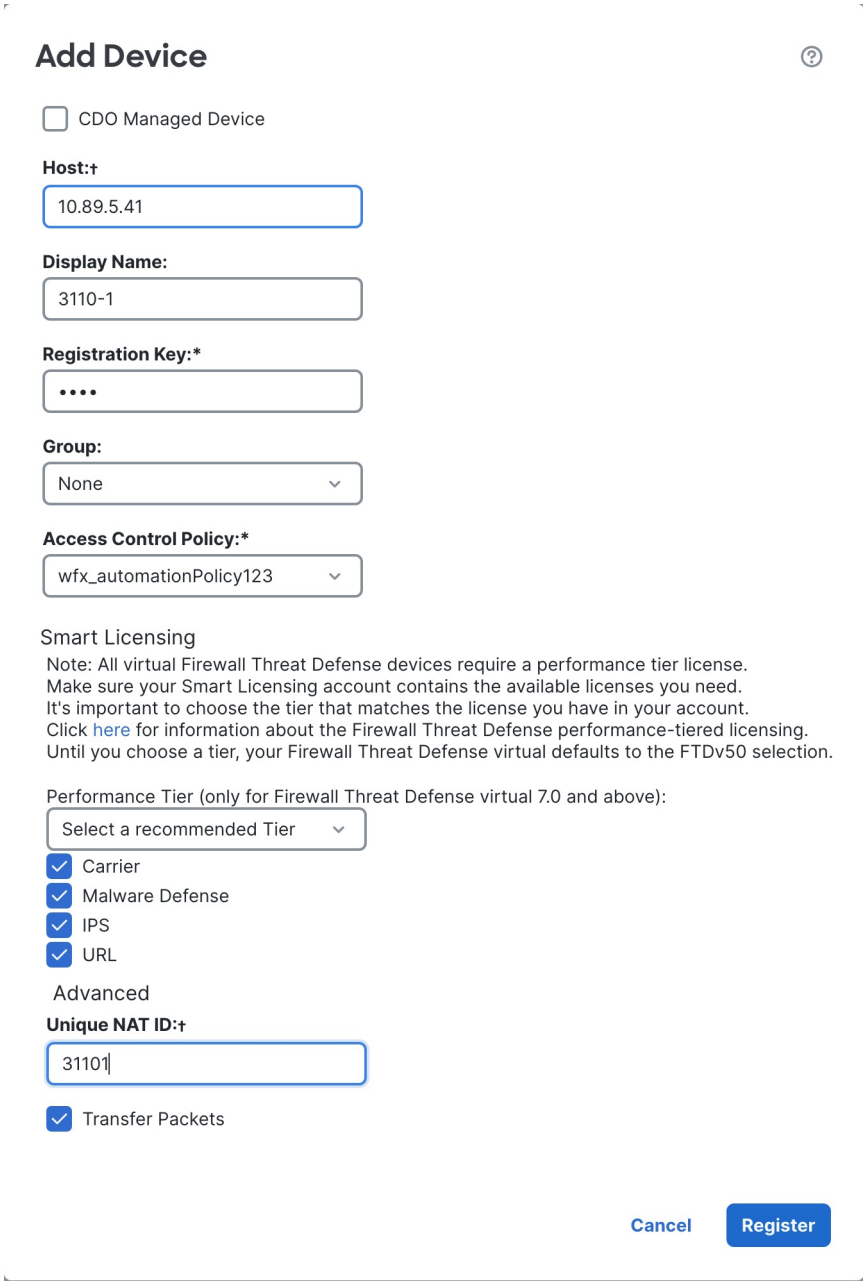
b) 输入您的用户名和密码。

c) 点击**登录**。

步骤 2 选择**设备** > **设备管理**。

步骤 3 从**添加**下拉列表中，选择**添加设备**。

图 *10:* 使用注册密钥添加设备

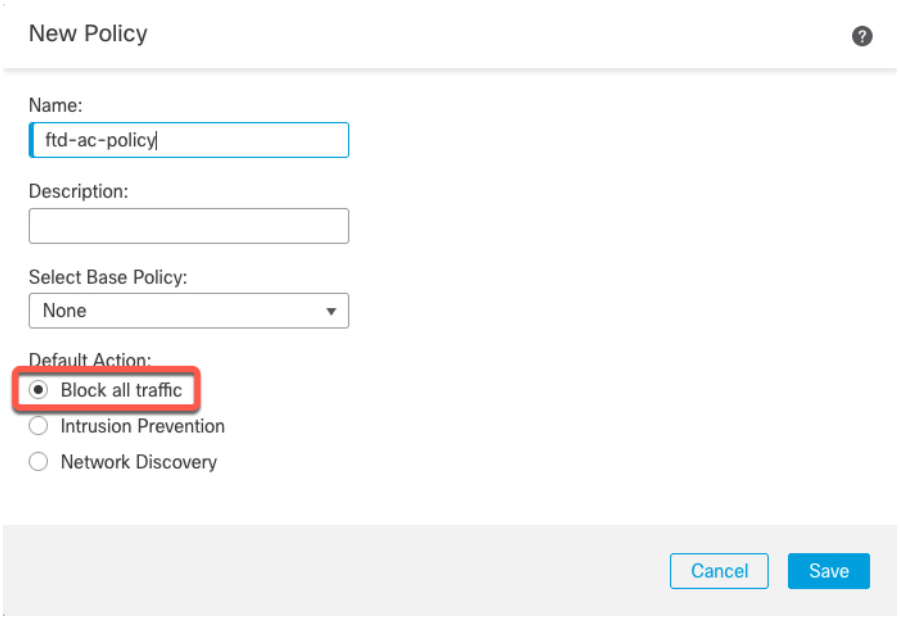


设置以下参数：

- **主机 (Host)** - 输入要添加的防火墙的 IP 地址或主机名（如果可用）。如果不可用，请将此字段留空。
- **显示名称 (Display Name)** - 输入要在 管理中心 中显示的防火墙名称。之后将无法更改该名称。
- **注册密钥 (Registration Key)** - 输入您在防火墙初始配置中指定的注册密钥。
- **域 (Domain)** - 如果有多域环境，请将设备分配给分叶域。

- **组 (Group)** - 如果在使用组，则将其分配给设备组。
- **访问控制策略 (Access Control Policy)** - 选择初始策略。除非已经拥有您知道自己需要使用的自定义策略，否则选择**新建策略 (Create new policy)**，然后选择**阻止所有流量 (Block all traffic)**。之后您可以更改此设置以允许流量通过；请参阅配置访问控制规则。

图 *11:* 新建策略



- **智能许可**—为要部署的功能分配所需的智能许可证。**注意：** 在添加设备后，您可以从 **系统** > **许可证** > **智能许可证** 页面应用 Secure Client 远程访问 VPN 许可证。
- **唯一 NAT ID (Unique NAT ID)** - 指定您在防火墙初始配置中指定的 NAT ID。
- **传输数据包 (Transfer Packets)** - 选中**传输数据包 (Transfer Packets)** 复选框，以便对于每个入侵事件，设备将数据包传输到 管理中心 进行检查。

  默认情况下，此选项已启用。对于每个入侵事件，设备会将事件信息和触发事件的数据包发送到 管理中心 进行检查。如果禁用此选项，则只会向 管理中心 发送事件信息，而不会发送数据包。

步骤 4 点击 **Register**。

如果 威胁防御注册失败，请检查以下项：

- Ping - 访问 威胁防御 CLI（请参阅访问威胁防御 CLI），然后使用以下命令 ping 管理中心 IP 地址：

  ping system *fmc_ip_address*

  如果 ping 不成功，使用 **show network** 命令检查网络设置。如果需要更改防火墙管理 IP 地址，请使用 **configure network management-data-interface** 命令。

- 注册密钥、NAT ID 和 管理中心 IP 地址 - 确保在两个设备上使用相同的注册密钥和 NAT ID。可以在防火墙上使用 **configure manager add** 命令设定注册密钥和 NAT ID。

有关更多故障排除信息，请参阅 https://cisco.com/go/fmc-reg-error。

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。