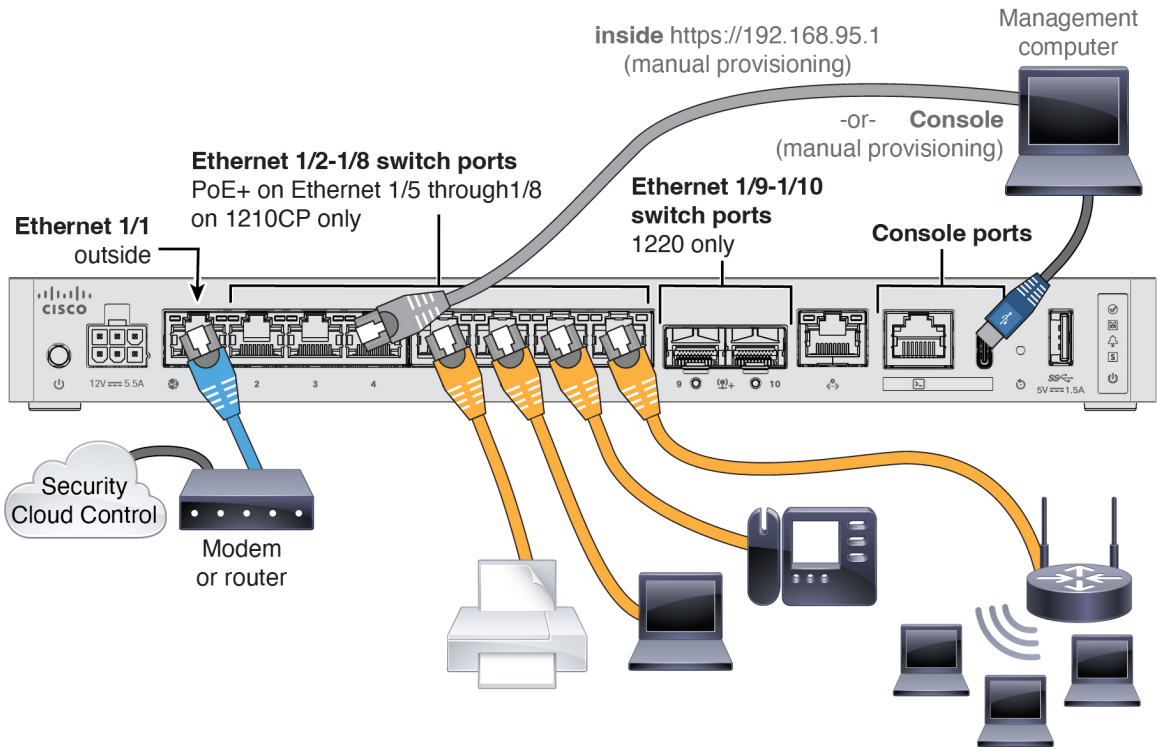
连接并载入防火墙

连接防火墙并载入到安全云控制。

连接防火墙的电缆

- 对于 Cisco Secure Firewall 1220，请将 SFP 安装到以太网 1/9 和 1/10 端口中。端口是需要使用 SFP/SFP+ 模块的 1/10-Gb SFP+ 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，否则不要将电缆连接到管理接口。在此情况下，请参阅使用 思科安全云控制 中的云交付的防火墙管理中心来管理 Cisco Secure Firewall Threat Defense 。本指南仅涵盖 零接触调配 的外部接口。



将防火墙载入 安全云控制

使用 零接触调配 或手动调配载入防火墙。

通过零接触调配载入防火墙

使用 零接触调配 和设备序列号载入 威胁防御。

过程

步骤 1 在 安全云控制 导航窗格中，点击 **安全设备 (Security Devices)**，然后点击蓝色加号按钮（ ）以便**载入**设备。

步骤 2 选择 **FTD** 磁贴。

步骤 3 在 **管理模式**下，确保选择 **FTD** 。

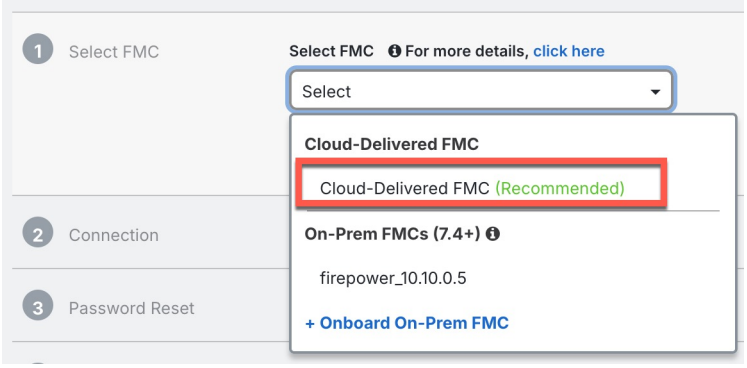
选择**FTD** 作为管理模式后，您可以随时点击 **管理智能许可证**注册或修改设备可用的现有智能许可证。请参阅获取许可证以查看可用的许可证。

步骤 4 选择**使用序列号 (Use Serial Number)** 作为激活方法。

图 *1:* 使用序列号

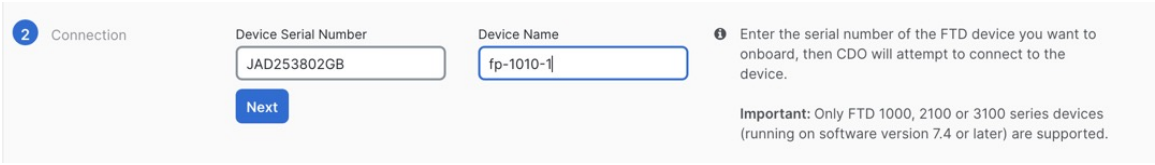
步骤 5 在**选择 FMC (Select FMC)** 中，从列表中选择**云交付 FMC (Cloud-Delivered FMC)** > **云交付 FMC (Cloud-Delivered FMC)**，然后点击**下一步 (Next)**。

图 *2:* 选择 ***FMC***



步骤 6 在**连接 (Connection)** 区域中，输入**设备序列号 (Device Serial Number)** 和**设备名称 (Device Name)**，然后点击**下一步 (Next)**。

图 *3:* 连接

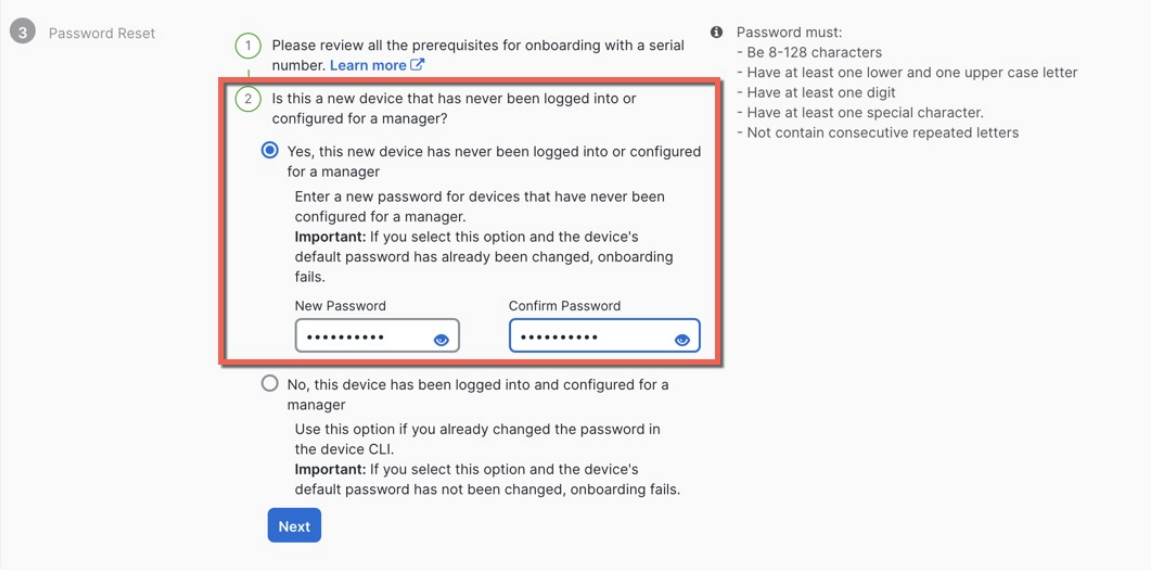


步骤 7 在**密码重置 (Password Reset)** 中，点击**是... (Yes...)**。输入设备的新密码并确认新密码，然后点击**下一步 (Next)**。

对于零接触调配，设备必须是全新的或已重新映像。

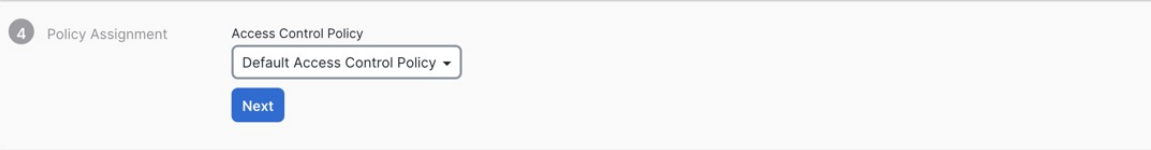
注释
如果您已经登录了设备并重置了密码，并且没有以禁用零接触调配的方式更改配置，则应选择**否... (No...)** 选项。有许多配置会禁用零接触调配调配，因此我们不建议登录设备，除非您需要这样做，例如执行重新映像。

图 *4:* 密码重设



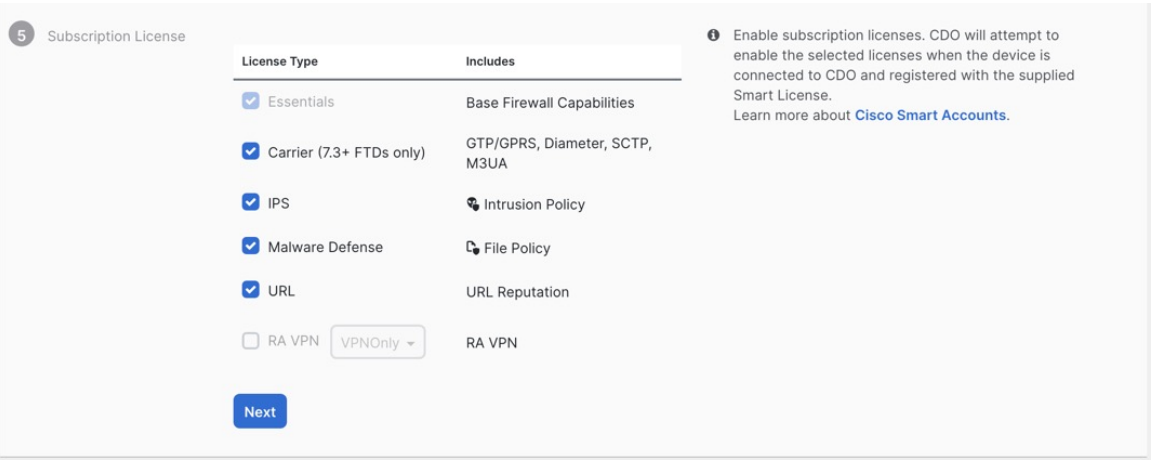
步骤 8 对于**策略分配 (Policy Assignment)**，请使用下拉菜单为设备选择访问控制策略。如果未配置策略，请选择**默认访问控制策略 (Default Access Control Policy)**。

图 *5:* 策略分配



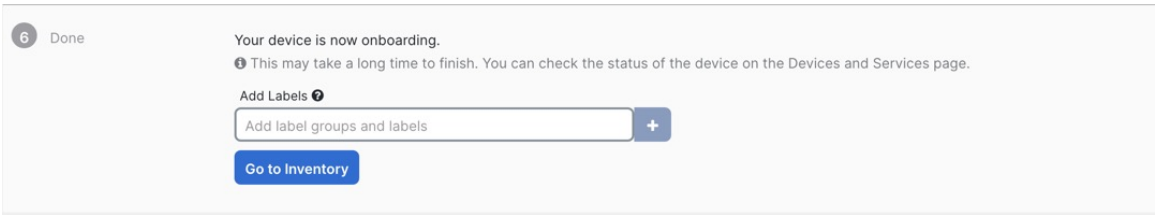
步骤 9 对于**订用许可证 (Subscription License)**，请选中要启用的每个功能许可证。点击**下一步**。

图 *6:* 订用许可证



步骤 10 （可选）向设备添加标签，以帮助对**安全设备 (Security Devices)** 页面进行排序和过滤。输入标签，然后选择蓝色加号按钮（+）。标签会在设备载入 安全云控制后应用到设备。

图 7: 完成



下一步做什么

在**安全设备 (Security Devices)** 页面中，选择您刚刚激活的设备，然后选择位于右侧的**管理 (Management)** 窗格下列出的任何选项。

通过手动调配载入防火墙

使用 CLI 注册密钥载入防火墙。

过程

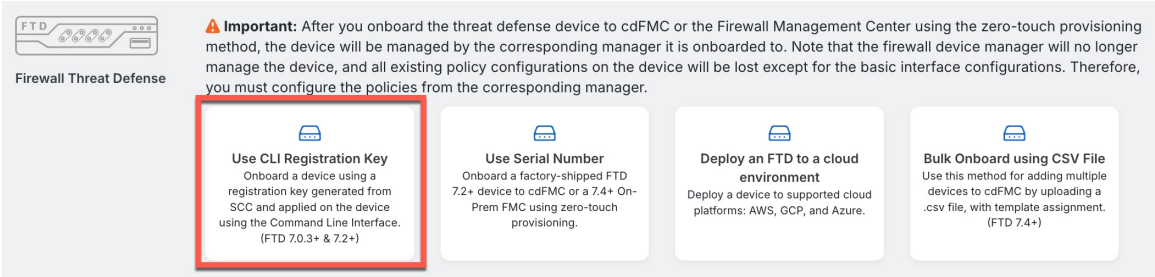
步骤 1 在 安全云控制 导航窗格中，点击 **安全设备 (Security Devices)**，然后点击蓝色加号按钮（+）以便**载入**设备。

步骤 2 点击 **FTD** 磁贴。

步骤 3 在 **管理模式**下，确保选择 **FTD** 。

步骤 4 选择**使用 CLI 注册密钥 (Use CLI Registration Key)** 作为激活方法。

图 8: 使用 ***CLI*** 注册密钥

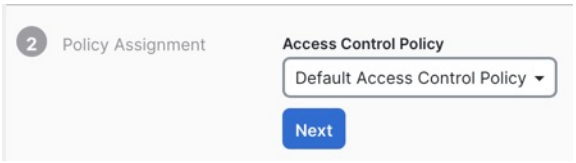


步骤 5 输入**设备名称 (Device Name)**，然后点击**下一步 (Next)**。

图 *9:* 设备名称

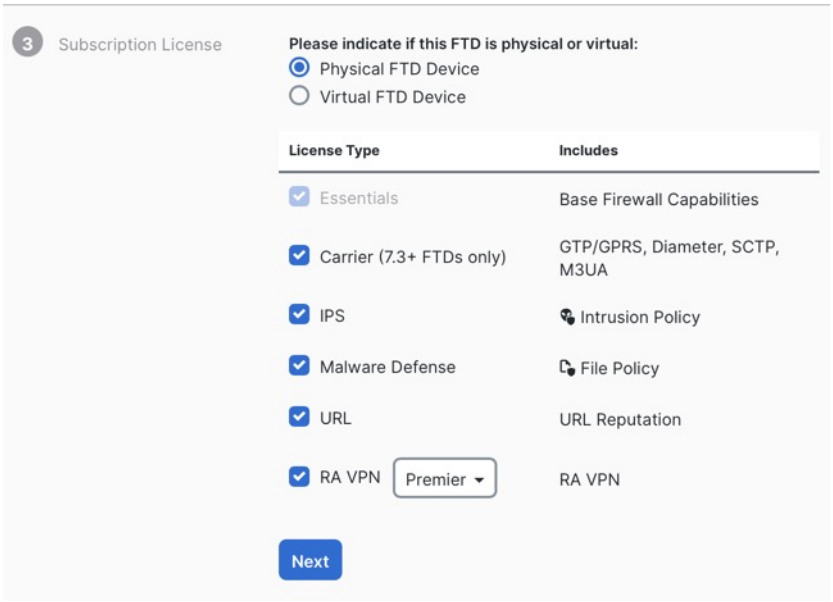
步骤 6 对于**策略分配 (Policy Assignment)**，请使用下拉菜单为设备选择访问控制策略。如果未配置策略，请选择**默认访问控制策略 (Default Access Control Policy)**。

图 *10:* 访问控制策略



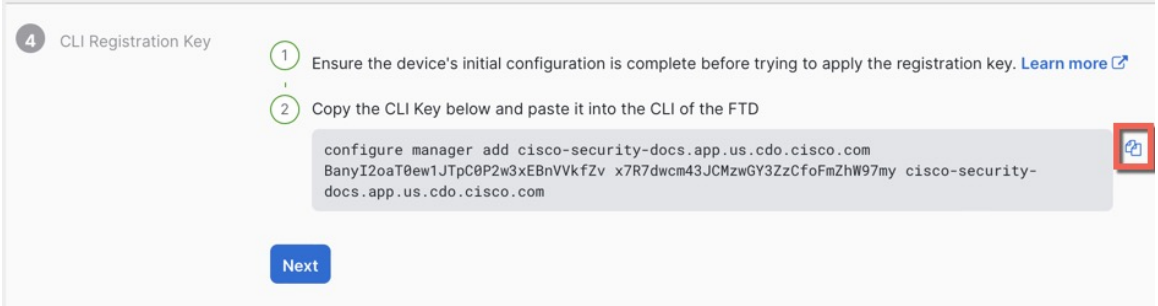
步骤 7 对于**订用许可证 (Subscription License)**，请点击**物理 FTD 设备 (Physical FTD Device)** 单选按钮，然后选中要启用的每个功能许可证。点击**下一步**。

图 *11:* 订用许可证



步骤 8 对于 **CLI 注册密钥**，安全云控制 会使用注册密钥和其他参数来生成命令。您必须复制此命令并在威胁防御的初始配置中使用它。

图 *12: CLI* 注册密钥



configure manager add 安全云控制_*hostname registration_key nat_id display_name*

在 CLI 或使用 设备管理器 完成初始配置：

- 初始配置：CLI，第 14 页-完成启动脚本后，在 威胁防御 CLI 中复制此命令。
- 初始配置：设备管理器，第 8 页 - 将命令的 *scc_hostname*、*registration_key* 和 *nat_id* 部分复制到**管理中心/安全云控制 主机名/IP 地址**、**管理中心/安全云控制 注册密钥**以及 **NAT ID** 字段中。

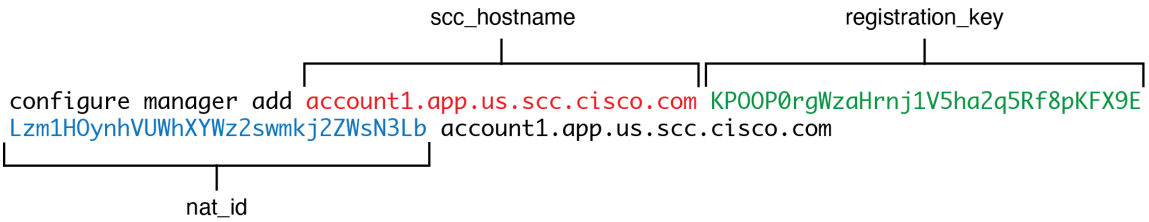
示例：

CLI 设置的命令示例：

```
configure manager add account1.app.us.scc.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.scc.cisco.com
```

GUI 设置的命令组件示例：

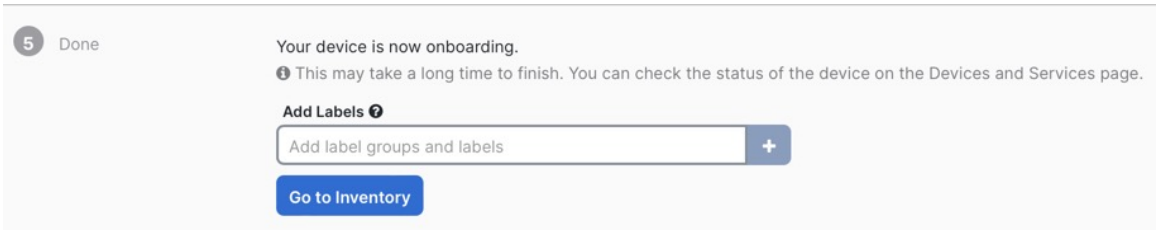
图 *13:* 配置管理器添加命令组件



步骤 9 在激活向导中点击**下一步 (Next)**，以便开始注册设备。

步骤 10 （可选） 向设备添加标签，以帮助对**安全设备 (Security Devices)** 页面进行排序和过滤。输入标签，然后选择蓝色加号按钮（+）。标签会在设备载入 安全云控制后应用到设备。

图 *14:* 完成



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
- VLAN1 - **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 至 1/8，或者对于 Cisco Secure Firewall 1220，为 1/2 至 1/10）。

步骤 2 登录设备管理器。

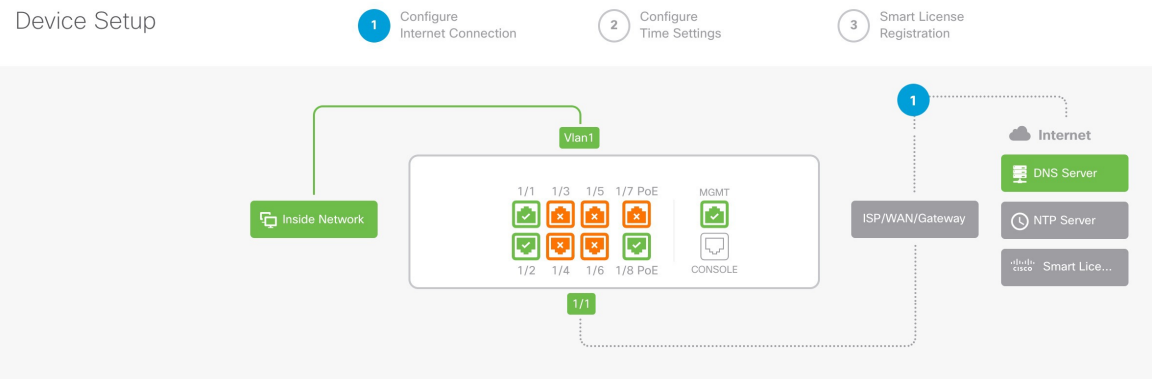
a) 转至https://192.168.95.1。

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。

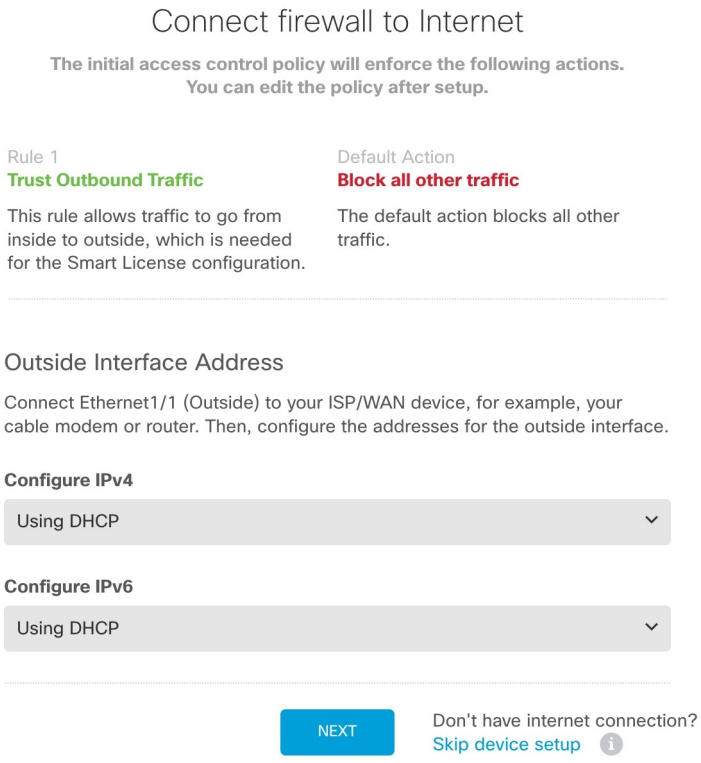
图 *15:* 设备设置



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 *16:* 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。

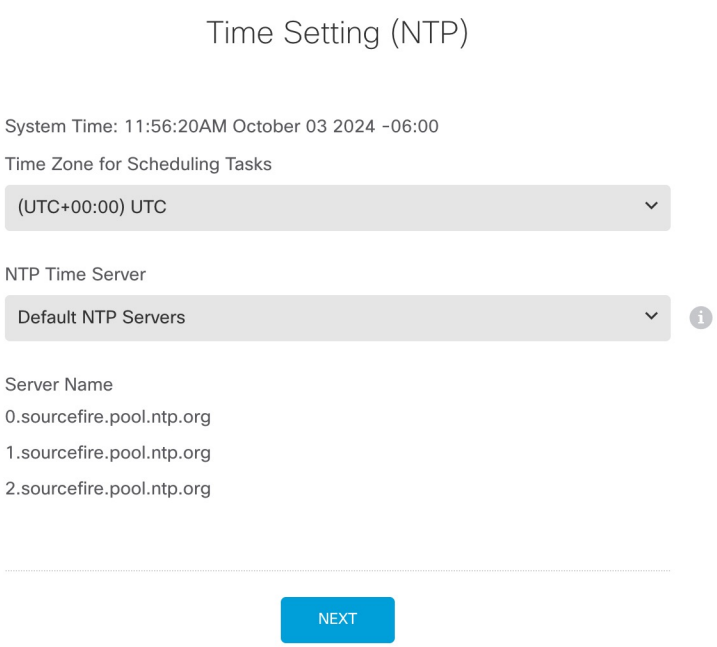
2. **管理接口** - 即使在外部接口上使用管理器访问，也会使用管理接口设置。例如，通过外部接口在背板上路由的管理流量将使用这些管理接口 DNS 服务器，而不是外部接口 DNS 服务器解析 FQDN。

   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。

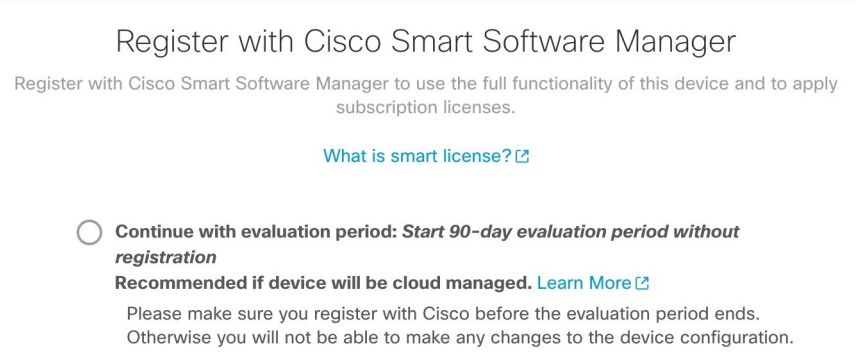
   防火墙主机名

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

图 *17:* 时间设置 *(NTP)*



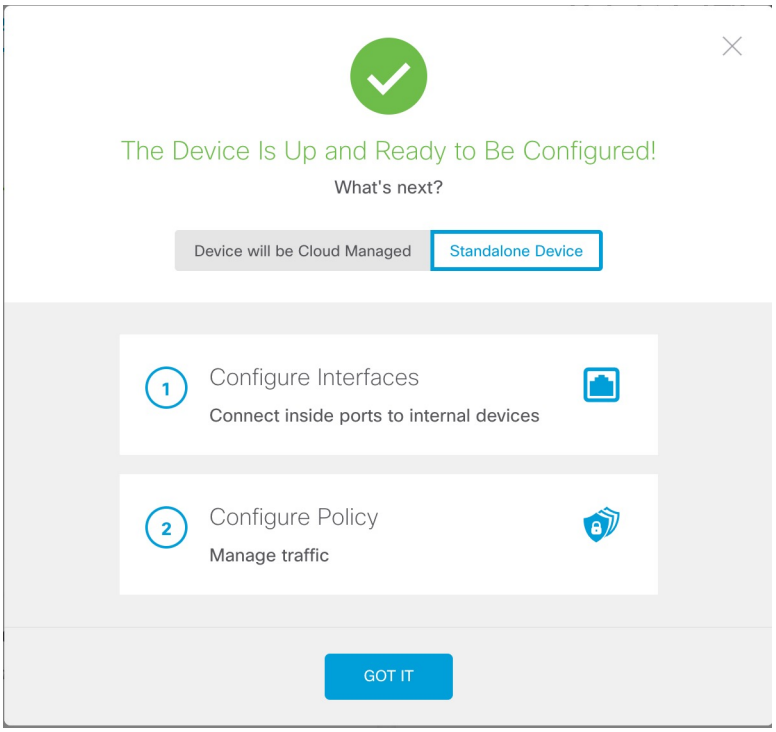
c) 选择**启动 90 日评估期而不注册**。



不要向智能软件管理器注册 威胁防御；所有许可均在 安全云控制 上执行。

d) 点击**完成**。

图 *18:* 后续操作



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

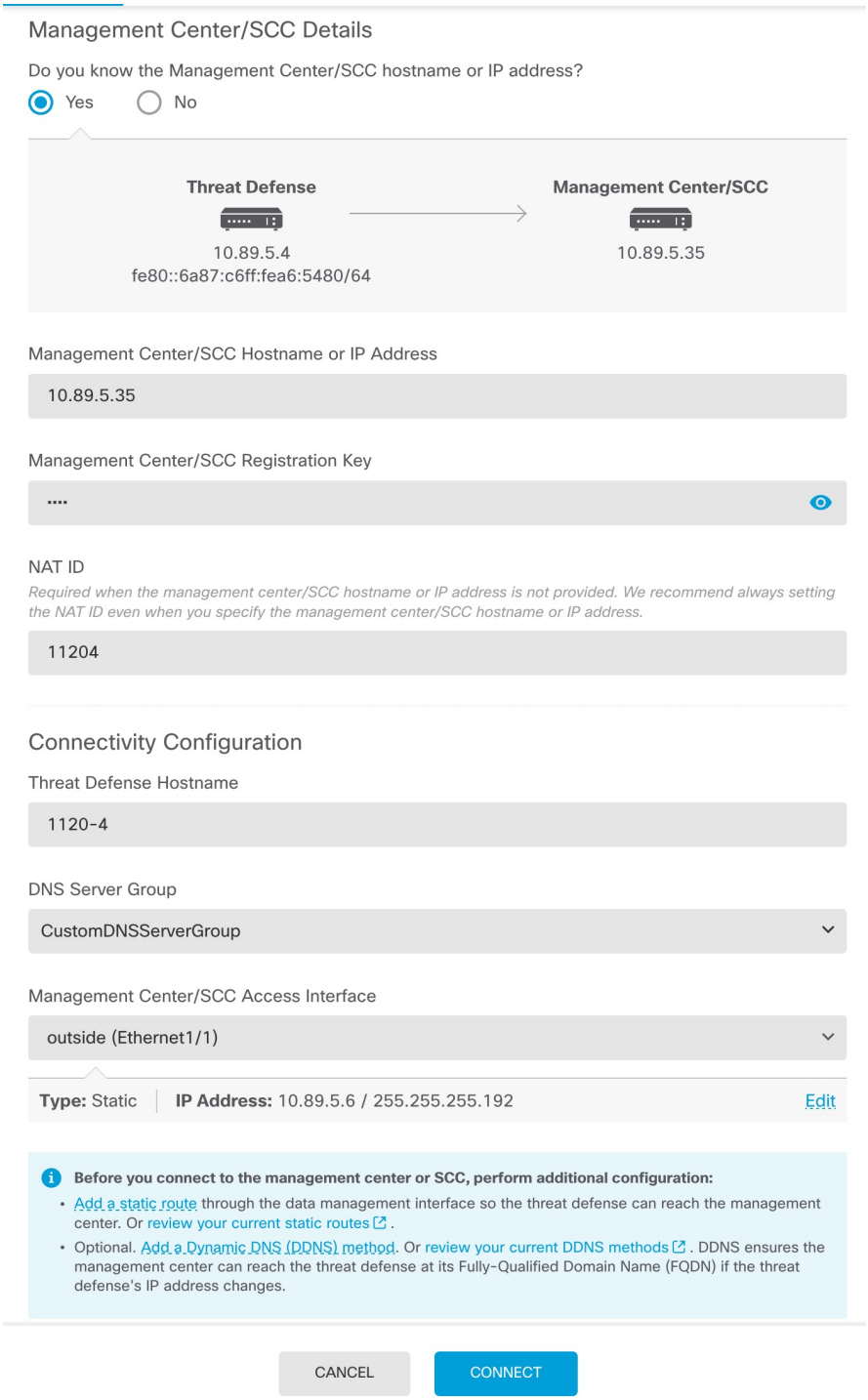
步骤 4 如果要配置其他接口，请选择**设备 (Device)**，然后点击**接口 (Interfaces)** 摘要中的链接。

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 安全云控制 注册

配置 **管理中心/SCC/详细信息 (Management Center/SCC/Details)**。

注释
较早的版本可能会显示“CDO”而不是“SCC”。

图 *19:* 管理中心/*SCC* 详细信息



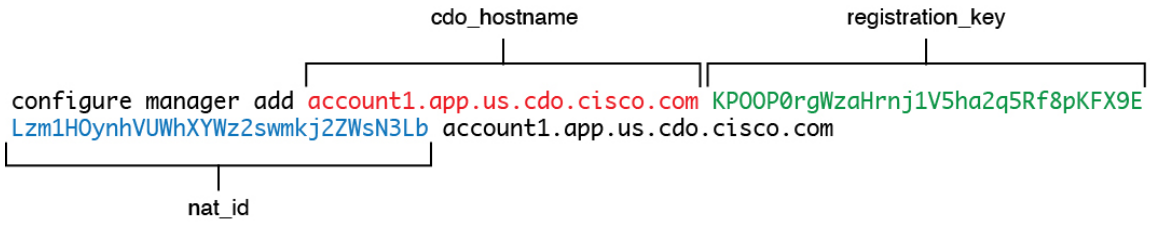
a) 对于 **是否知道管理中心/SCC 主机名或 IP 地址**，如果您可以使用 IP 地址或主机名访问 管理中心 ，请点击**是 (Yes)**。

安全云控制 会生成 **configure manager add** 命令。请参阅通过手动调配载入防火墙 ， 第 5 页以生成命令。

configure manager add *_hostname registration_key nat_id display_name*

示例：

图 *20:* 配置管理器添加命令组件



b) 将命令的 *cdo_hostname*、 *registration_key*和 *nat_id* 部分复制到以下字段中：

- **管理中心/SCC 主机名/IP 地址**
- **管理中心/SCC 注册密钥**
- **NAT ID**

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/SCC 访问接口**，点击 **数据接口**，然后选择 **外部**。

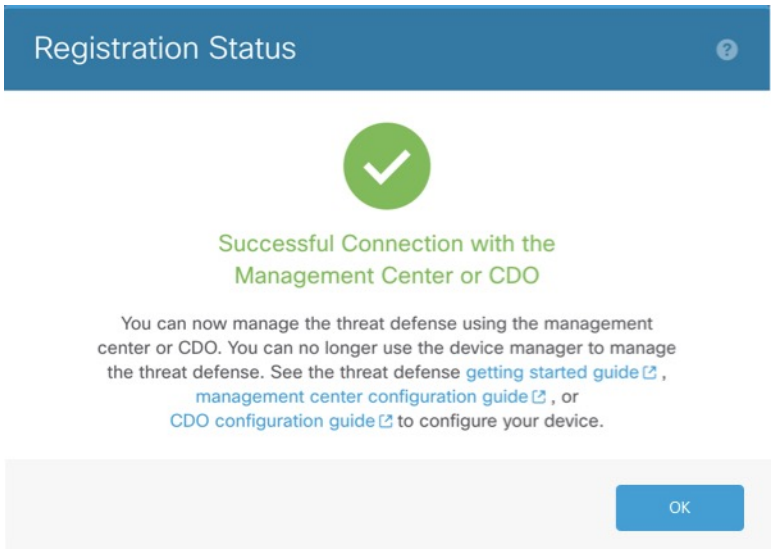
步骤 7 （可选） 点击**添加动态 DNS (DDNS) 方法 (Add a Dynamic DNS [DDNS] method)**。

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 安全云控制 注册的当前状态。

图 *21:* 成功连接



步骤 9 在状态屏幕上完成 **保存管理中心/SCC 注册设置** 步骤之后，转到 安全云控制，然后添加防火墙。请参阅通过手动调配载入防火墙，第 5 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 使用 安全云控制 生成的 **configure manager add** 命令确定将管理此 威胁防御 的 安全云控制。请参阅通过手动调配载入防火墙，第 5 页以生成命令。

示例：

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
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。

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。