



# 在平台模式下部署 ASA

本章对您适用吗？

Firepower 2100 运行名为 Firepower 可扩展操作系统 (FXOS) 的底层操作系统。可以在以下模式下针对 ASA 运行 Firepower 2100：

- 平台模式 - 处于平台模式时，您必须在 FXOS 中配置基本的操作参数和硬件接口设置。这些设置包括启用接口、建立 EtherChannel、NTP、映像管理等。您可以使用 Firepower 机箱管理器 web 界面或 FXOS CLI。然后，您可以使用 ASDM 或 ASA CLI 在 ASA 操作系统中配置安全策略。
- 设备模式（默认）-设备模式允许您配置 ASA 中的所有设置。FXOS CLI 中仅提供高级故障排除命令。

本章介绍如何在 ASA 平台模式下在网络中部署 Firepower 2100。默认情况下，Firepower 2100 在设备模式下运行，因此本章介绍如何将模式设置为平台模式。本章不涉及以下部署，请参考《[ASA 配置指南](#)》了解相关内容：

- 故障切换
- CLI 配置

本章还演示如何配置基本安全策略；如果您有更高级的要求，请参阅配置指南。



## 注释

Firepower 2100 硬件可以运行 ASA 软件或 FTD 软件。在 ASA 和 FTD 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

隐私收集声明 - Firepower 2100 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。

- [关于 ASA , 第 2 页](#)
- [端到端程序 , 第 4 页](#)
- [查看网络部署和默认配置 , 第 6 页](#)

- 连接设备电缆，第 9 页
- 接通设备电源，第 10 页
- 启用平台模式，第 10 页
- （可选）登录 Firepower 机箱管理器，第 13 页
- （可选）在 Firepower 机箱管理器中启用其他接口，第 13 页
- 登录 ASDM，第 15 页
- 配置许可，第 16 页
- 配置 ASA，第 20 页
- （可选）在数据接口上配置对 FXOS 的管理访问，第 22 页
- 访问 ASA 和 FXOS CLI，第 23 页
- （可选）更改 FXOS 管理 IP 地址或网关，第 25 页
- 后续操作，第 31 页
- 平台模式下 Firepower 2100 的历史记录，第 31 页

## 关于 ASA

ASA 在一台设备中提供高级状态防火墙和 VPN 集中器功能。

Firepower 2100 是适用于 ASA 的单一应用设备。可以在平台模式或设备模式（默认）下运行 ASA。Firepower 2100 运行名为 Firepower 可扩展操作系统 (FXOS) 的底层操作系统。处于平台模式时，必须在 FXOS 中配置基本的操作参数和硬件接口设置。这些设置包括启用接口、建立 EtherChannel、NTP、映像管理等。您可以使用 Firepower 机箱管理器 web 界面或 FXOS CLI。然后，可以使用以下其中一个管理器在 ASA 操作系统中配置安全策略。

- ASDM - 设备上的单设备管理器。本指南介绍使用 ASDM 管理 ASA 的方法。
- CLI
- 思科安全管理器 - 位于单独的服务器上的多设备管理器。

设备模式允许您配置 ASA 中的所有设置。FXOS CLI 中仅提供高级故障排除命令。

## ASA 和 FXOS 管理

ASA 和 FXOS 操作系统共享管理 1/1 接口。此接口拥有单独的 IP 地址，用于连接到 ASA 和 FXOS。




---

**注释** 此接口在 ASA 中被称为管理 1/1；在 FXOS 中，您可能会看到它显示为 MGMT、management0 或其他类似名称。本指南将此接口称为管理 1/1，以保持一致性和简洁性。

---

某些功能必须在 FXOS 上进行监控，而其他功能则必须在 ASA 上进行监控，因此您需要利用这两个操作系统进行持续维护。对于 FXOS 上的初始配置，您可以使用 SSH 或您的浏览器 (<https://192.168.45.45>) 连接到默认的 192.168.45.45 IP 地址。

对于 ASA 的初始配置，您可以使用 ASDM 连接到 <https://192.168.45.1/admin>。在 ASDM 中，您以后可以任何从任何接口配置 SSH 访问。

这两个操作系统都可从控制台端口获得。初始连接将访问 FXOS CLI。您可以使用 **connect asa** 命令来访问 ASA CLI。

您还可以允许从 ASA 数据接口进行 FXOS 管理；配置 SSH、HTTPS 和 SNMP 访问。此功能对远程管理非常有用。

## 不支持的功能

### 不支持的 ASA 功能

Firepower 2100 不支持以下 ASA 功能：

- 集成路由和桥接
- 冗余接口
- 群集
- 无客户端 SSL VPN 与 KCD
- ASA REST API
- ASA FirePOWER 模块
- 僵尸网络流量过滤器
- 以下检查：
  - SCTP 检查图（支持使用 ACL 的 SCTP 状态检查）
  - Diameter
  - GTP/GPRS

### 不支持的 FXOS 功能

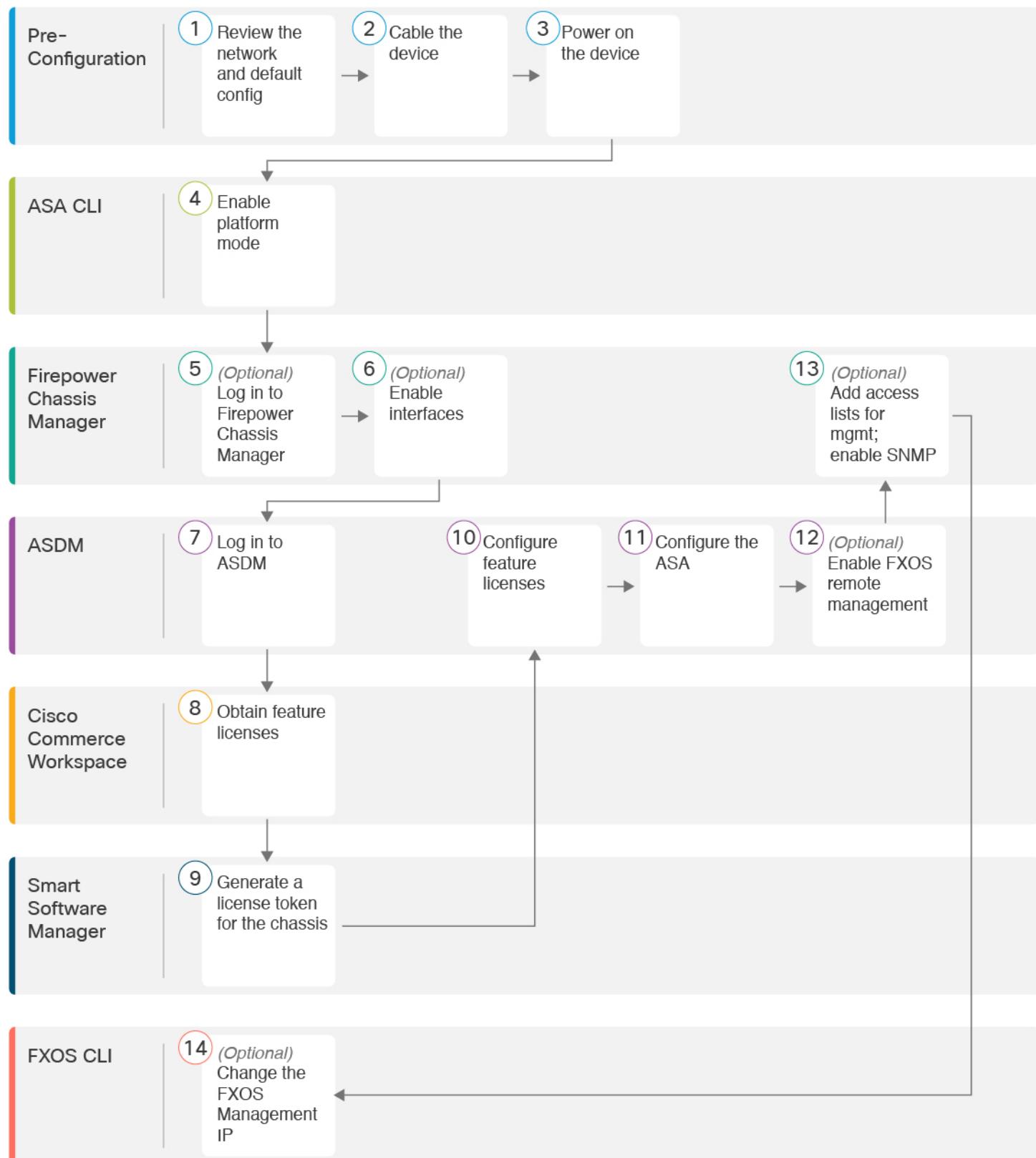
Firepower 2100 不支持以下 FXOS 功能：

- 备份与还原 FXOS 配置
- FXOS 的外部 AAA 身份验证

请注意，当您从 FXOS (**connect asa**) 连接到 ASA 控制台时，会应用适用于控制台访问的 ASA AAA 配置 (**aaa authentication serial console**)。

# 端到端程序

请参阅以下任务以在机箱上部署和配置 ASA。



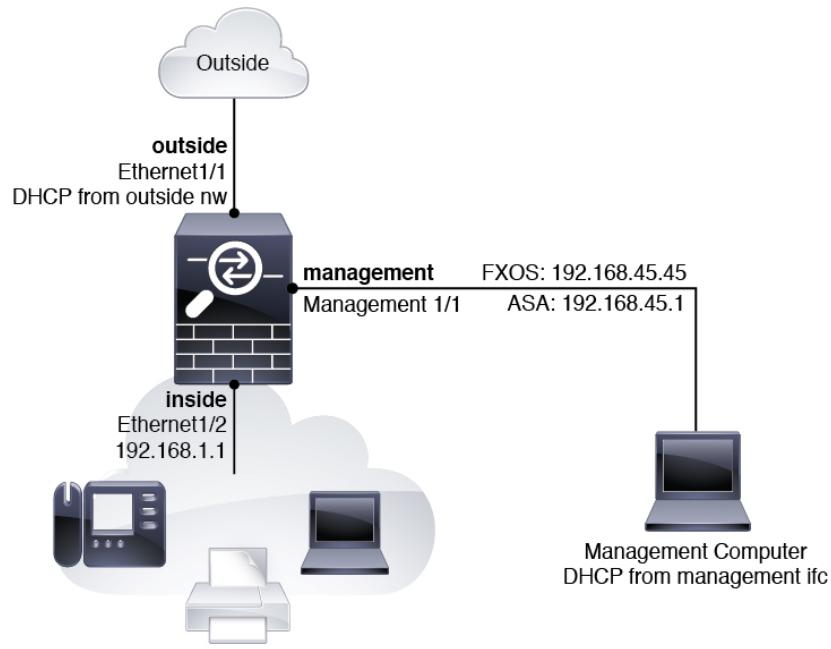
## 查看网络部署和默认配置

1	配置前准备工作	<a href="#">查看网络部署和默认配置 , 第 6 页。</a>
2	配置前准备工作	<a href="#">连接设备电缆 , 第 9 页。</a>
3	配置前准备工作	<a href="#">接通设备电源 , 第 10 页。</a>
4	ASA CLI	<a href="#">启用平台模式 , 第 10 页。</a>
5	Firepower 机箱管理器	<a href="#">(可选) 登录 Firepower 机箱管理器 , 第 13 页。</a>
6	Firepower 机箱管理器	<a href="#">(可选) 在 Firepower 机箱管理器中启用其他接口 , 第 13 页。</a>
7	ASDM	<a href="#">登录 ASDM , 第 15 页。</a>
8	思科商务工作空间	<a href="#">配置许可 , 第 16 页: 获取功能许可证。</a>
9	智能软件管理器	<a href="#">配置许可 , 第 16 页: 为机箱生成许可证令牌。</a>
10	ASDM	<a href="#">配置许可 , 第 16 页: 配置功能许可证。</a>
11	ASDM	<a href="#">配置 ASA , 第 20 页。</a>
12	ASDM	<a href="#">(可选) 在数据接口上配置对 FXOS 的管理访问 , 第 22 页: 启用 FXOS 远程管理; 允许 FXOS 从 ASA 接口启动管理连接。</a>
13	Firepower 机箱管理器	<a href="#">(可选) 在数据接口上配置对 FXOS 的管理访问 , 第 22 页: 配置访问列表以允许您的管理地址;启用 SNMP (默认情况下启用 HTTPS 和 SSH) ;</a>
14	FXOS CLI	<a href="#">(可选) 更改 FXOS 管理 IP 地址或网关 , 第 25 页。</a>

## 查看网络部署和默认配置

下图显示使用默认配置的 Firepower 2100 在 ASA 平台模式下的默认网络部署。

图 1: 您的网络中的 Firepower 2100



## Firepower 2100平台模式默认配置

您可以将 Firepower 2100 设置为在平台模式下运行;设备模式为默认模式。



**注释** 对于 9.13(1) 之前的版本，平台模式是默认选项和唯一选项。如果从平台模式升级，则会保留此模式。

### ASA 配置

Firepower 2100 上的 ASA 的出厂默认配置包含以下配置：

- 内部→外部流量 - 以太网 1/1（外部），以太网 1/2（内部）
- 从 DHCP 的外部 IP 地址，内部 IP 地址 - 192.168.1.1
- **DHCP** 服务器在内部接口上
- 来自外部 DHCP 的默认路由
- 管理 - 管理端口 1/1（管理），IP 地址 192.168.45.1
- **ASDM** 访问 - 允许管理主机。
- **NAT** - 从内部到外部所有流量的接口 PAT。
- **FXOS** 管理流量启动 - FXOS 机箱可以在接口外部的 ASA 上启动管理流量。

## Firepower 2100平台模式默认配置

- **DNS 服务器 - OpenDNS 服务器已预配置。**

配置由以下命令组成：

```

interface Management1/1
management-only
nameif management
security-level 100
ip address 192.168.45.1 255.255.255.0
no shutdown
!
interface Ethernet1/1
nameif outside
security-level 0
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
object network obj_any
subnet 0.0.0.0 0.0.0.0
nat (any,outside) dynamic interface
!
http server enable
http 192.168.45.0 255.255.255.0 management
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
ip-client outside
!
dns domain-lookup outside
dns server-group DefaultDNS
  name-server 208.67.222.222 outside
  name-server 208.67.220.220 outside

```

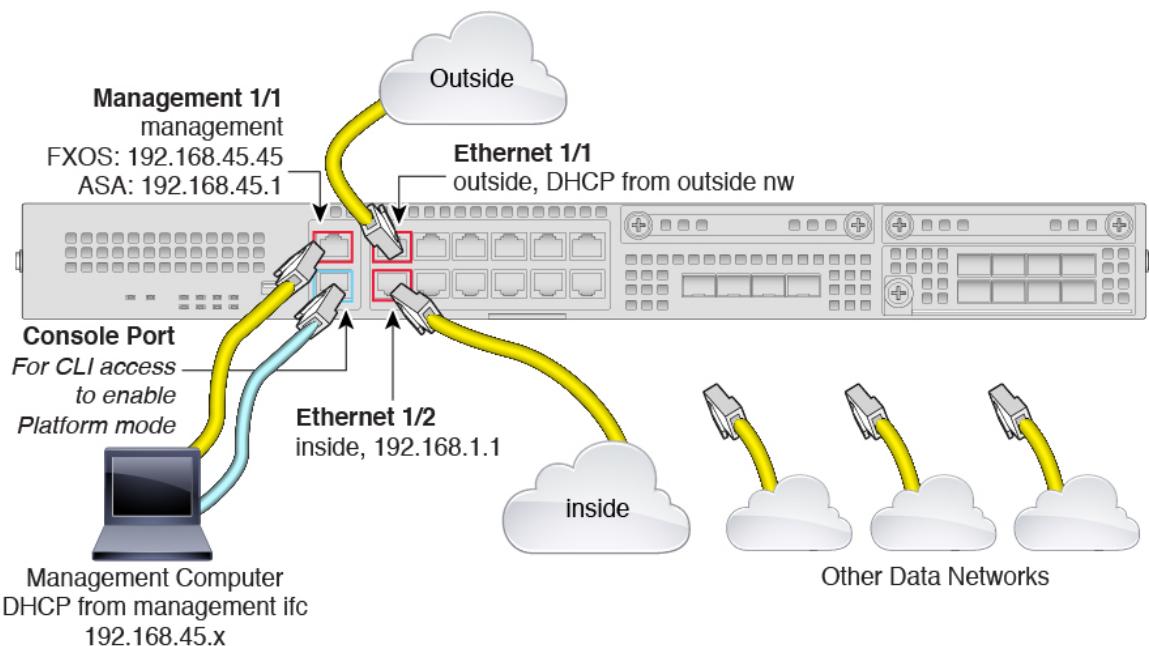
## FXOS 配置

Firepower 2100 上的 FXOS 的出厂默认配置包含以下配置：

- **管理 1/1 - IP 地址 192.168.45.45**
- **默认网关 - ASA 数据接口**
- **Firepower 机箱管理器和 SSH 访问 - 仅从管理网络。**
- **默认用户名 - admin, 默认密码 Admin123**
- **DHCP 服务器 - 客户端 IP 地址范围 192.168.45.10-192.168.45.12**
- **NTP 服务器 - 思科 NTP 服务器: 0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org**
- **DNS 服务器 - OpenDNS: 208.67.222.222、208.67.220.220**

- 以太网 1/1 和以太网 1/2 - 已启用

## 连接设备电缆



在管理 1/1 接口上管理 Firepower 2100。您可以对 FXOS 和 ASA 使用同一管理计算机。默认配置还会将以太网 1/1 配置为外部接口。

### 过程

#### 步骤 1 将您的管理计算机直接连接至管理 1/1 以进行初始配置，或将管理 1/1 连接至您的管理网络。

请确保您的管理计算机在管理网络上，因为只有该网络上的客户端可以访问 ASA 或 FXOS。管理 1/1 具有默认的 FXOS IP 地址 (192.168.45.45) 和 ASA 默认 IP 地址 (192.168.45.1)。FXOS 还运行 DHCP 服务器向客户端（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管理网络设置冲突（请参阅 [Firepower 2100 平台模式默认配置，第 7 页](#)）。

稍后，可以从数据接口配置 FXOS 和 ASA 管理访问。有关 FXOS 访问的信息，请参阅 [\(可选\) 在数据接口上配置对 FXOS 的管理访问，第 22 页](#)。有关 ASA 访问的信息，请参阅 [ASA 一般操作配置指南](#)。

#### 步骤 2 将管理计算机连接到控制台端口。

您需要访问 ASA CLI，以从设备模式更改为平台模式。Firepower 2100 配有一条 DB-9 转 RJ-45 串行线缆，所以您需要第三方串行转 USB 线缆进行连接。确保为操作系统安装任何必要的 USB 串行驱动程序。

## 接通设备电源

**步骤3** 将外部网络连接至以太网 1/1 接口（标记为 WAN）。

对于智能软件许可，ASA 需要互联网接入，以便它可以访问许可证颁发机构。

**步骤4** 将内部网络连接至以太网 1/2。

**步骤5** 将其他网络连接到其余接口。

---

## 接通设备电源

系统电源由位于设备后部的摇杆电源开关控制。电源开关以软通知开关形式实施，支持平稳地关闭系统以降低系统软件及数据损坏的风险。

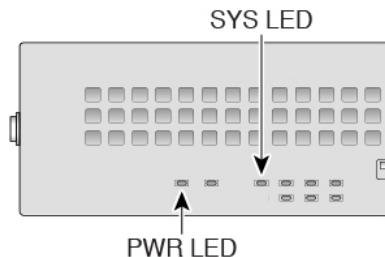
### 过程

---

**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** 将开关从开切换到关时，系统可能需要几秒钟才会最终关闭。在此期间，设备前面的 PWR LED 将闪烁绿色。在 PWD LED 完全关闭之前，请勿拔出电源。

---

## 启用平台模式

默认情况下，Firepower 2100 在设备模式下运行。此程序将告知如何将模式更改为平台模式，以及如何将其更改回设备模式（可选）。

更改模式时，会清除配置，因此需要重新加载系统。重新加载时会应用默认配置。

## 过程

**步骤 1** 将管理计算机连接到控制台端口。Firepower 2100 配有一条 DB-9 转 RJ-45 串行线缆，所以您需要第三方串行转 USB 线缆进行连接。确保为操作系统安装任何必要的 USB 串行驱动程序。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

连接到 ASA CLI。默认情况下，访问控制台时不需要提供用户凭证。

**注释** 更改为平台模式后，控制台连接将访问 FXOS CLI，而不是 ASA CLI。但是，可以在平台模式下从控制台访问 ASA CLI；请参阅[连接到控制台端口以访问 FXOS 和 ASA CLI，第 23 页](#)。

**步骤 2** 访问特权 EXEC 模式。

### **enable**

第一次输入 **enable** 命令时，系统会提示您更改密码。

**示例：**

```
ciscoasa> enable  
Password:  
The enable password is not set. Please set it now.  
Enter Password: *****  
Repeat Password: *****  
ciscoasa#
```

在特权 EXEC 模式中，所有非配置命令均可用。还可从特权 EXEC 模式进入配置模式。

要退出特权模式，请输入 **disable**、**exit** 或 **quit** 命令。

**步骤 3** 访问全局配置模式。

### **configure terminal**

**示例：**

```
ciscoasa# configure terminal  
ciscoasa(config)#
```

**步骤 4** 将模式设置为平台模式。

**no fxos mode appliance**

**write memory**

**reload**

## 启用平台模式

设置模式后，需要保存配置并重新加载设备。在重新加载之前，可以在不造成任何中断的情况下将模式设置回原始值。

**示例：**

```
ciscoasa(config)# no fxos mode appliance
Mode set to platform mode
WARNING: This command will take effect after the running-config is saved and the system has
been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684

23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

**步骤 5** 重新启动后，查看当前模式以确认更改。

**show fxos mode**

**示例：**

```
ciscoasa(config)# show fxos mode
Mode is currently set to platform
```

**步骤 6**（可选）将模式设置回设备模式。

**fxos mode appliance**

**write memory**

**reload**

设置模式后，需要保存配置并重新加载设备。在重新加载之前，可以在不造成任何中断的情况下将模式设置回原始值。

**示例：**

```
ciscoasa(config)# fxos mode appliance
Mode set to appliance mode
WARNING: This command will take effect after the running-config is saved and the system has
been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684

23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

## (可选) 登录 Firepower 机箱管理器

使用 Firepower 机箱管理器配置机箱设置，包括启用接口和创建 EtherChannel。

### 开始之前

- 有关受支持的浏览器的信息，请参阅您使用的版本的发行说明（请参阅 <http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html>）。
- 如果需要更改 FXOS 和 ASA 管理 IP 地址，请参阅 (可选) 更改 FXOS 管理 IP 地址或网关，第 25 页。

### 过程

**步骤 1** 在连接到管理 1/1 接口的管理计算机上，通过访问以下 URL 启动 Firepower 机箱管理器。

**https://192.168.45.45**

**步骤 2** 输入默认用户名：admin。系统会提示您设置密码。

## (可选) 在 Firepower 机箱管理器中启用其他接口

默认情况下，管理 1/1、以太网 1/1 和以太网 1/2 接口将以物理方式为机箱启用，并以逻辑方式在 ASA 配置中启用。要使用任何其他接口，必须使用此程序为机箱启用它，然后在 ASA 配置中启用它。您还可以添加 EtherChannel（称为端口通道）。



### 注释

如果在启用故障转移（通过增加或删除网络模块，或通过更改 EtherChannel 配置）后更改接口，请在备用设备上的 FXOS 中更改接口，然后在主用设备上进行相同更改。

如果在 FXOS 中删除一个接口（例如，如果您移除网络模块，移除 EtherChannel，或将某个接口重新分配到 EtherChannel），则 ASA 配置会保留原始命令，以便您可以进行任何必要的调整；从配置中删除接口会产生广泛的影响。您可以在 ASA OS 中手动移除旧的接口配置。

### 开始之前

- 登录 Firepower 机箱管理器。请参阅 (可选) 登录 Firepower 机箱管理器，第 13 页。
- Firepower 2100 在链路汇聚控制协议 (LACP) 活动或开启模式下支持 EtherChannel。默认情况下，LACP 模式设置为“活动 (Active)”；您可以在 CLI 中将该模式更改为“开启 (On)”。我们建议将连接交换机端口设置为“活动 (Active)”模式，以实现最佳兼容性。
- 要从默认值更改管理 IP 地址，请参阅 (可选) 更改 FXOS 管理 IP 地址或网关，第 25 页。

(可选) 在 Firepower 机箱管理器中启用其他接口

## 过程

**步骤 1** 在 Firepower 机箱管理器中，单击 **接口**。

所有接口页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

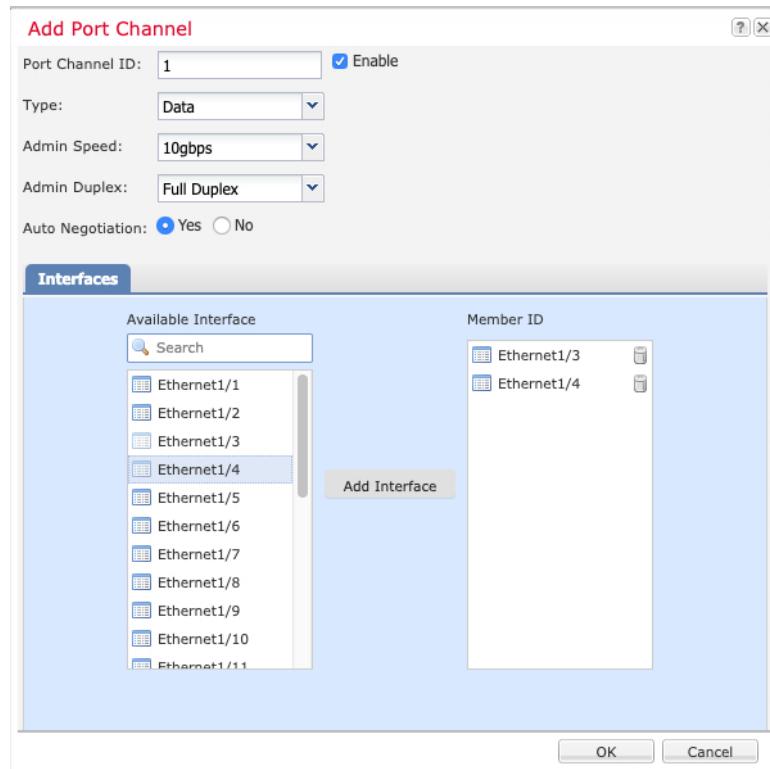
**步骤 2** 要启用或禁用接口，请单击启用滑块 () 或禁用滑块 ()。

**注释** 管理 1/1 接口在该表中显示为 **MGMT**。

**步骤 3** (可选) 添加 EtherChannel.

**注释** EtherChannel 成员端口在 ASA 上可见，但您只能在 FXOS 中配置 EtherChannels 和端口成员身份。

a) 点击接口表上方的添加端口通道 (Add Port Channel)。



- b) 在端口通道 ID (Port Channel ID) 字段中，输入端口通道的 ID。有效值介于 1 与 47 之间。
- c) 选中启用 (Enable) 复选框以启用端口通道。

忽略类型 (Type) 下拉列表；唯一可用的类型是数据 (Data)。

- d) 从管理速度 (Admin Speed) 下拉列表中，选择所有成员接口的速度。

如果您选择的接口无法达到所选速度（以及您选择的其他设置），则会自动应用尽可能最快的速度。

- e) 为所有成员接口点击自动协商 (Auto Negotiation) 是 (Yes) 或否 (No) 单选按钮。
- f) 在管理双工 (Admin Duplex) 下拉列表中, 为所有成员接口选择双工。
- g) 在可用接口 (Available Interface) 列表中, 选择您要添加的接口, 然后点击添加接口 (Add Interface)。

您最多可以添加 16 个同一类型和速度的接口。添加到通道组的第一个接口确定正确的类型和速度。

**提示** 一次可添加多个接口。要选择多个独立接口, 请点击所需的接口, 同时按住 **Ctrl** 键。要选择一个接口范围, 请选择范围中的第一个接口, 然后, 在按住 **Shift** 键的同时, 点击选择范围中的最后一个接口。

- h) 点击确定。
- 

## 登录 ASDM

启动 ASDM 以便配置 ASA。

强加密 (3DES/AES) 可在您连接到许可证颁发机构或卫星服务器之前用于管理连接, 以便您能够启动 ASDM。请注意, ASDM 访问仅在具有默认加密的管理专用接口上可用。在您连接并获取强加密许可证之前, 不允许通过设备的流量。

### 开始之前

请参阅 Cisco.com 上的 [ASDM 发行说明](#) 了解运行 ASDM 的要求。

### 过程

---

**步骤 1** 使用支持的浏览器输入以下 URL。

**https://management\_ip/admin**

- *management\_ip* - 标识 ASA 管理接口 (192.168.45.1) 的 IP 地址或主机名。

此时将显示 **Cisco ASDM** 网页。您可能会看到浏览器安全警告, 因为 ASA 没有安装证书; 您可以安全地忽略这些警告并访问网页。

**步骤 2** 单击以下可用选项之一: **Install ASDM Launcher** 或 **Run ASDM**。

**步骤 3** 根据您选择的选项, 按照屏幕上的说明启动 ASDM。

系统将显示 **Cisco ASDM-IDM Launcher**。

**步骤 4** 将用户名留空, 输入您在部署 ASA 时设置的启用密码, 然后单击 **OK**。

系统将显示 ASDM 主窗口。

---

# 配置许可

ASA 使用思科智能软件许可。您可以使用常规智能软件许可，这需要互联网接入；或者对于离线管理，您可以配置永久许可证保留或卫星服务器。有关这些离线许可方法的更多信息，请参阅[思科 ASA 系列功能许可证](#)；本指南适用于常规智能软件许可。

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。在向许可证颁发机构注册之前，您将无法对需要特殊许可证的功能进行配置更改，但操作则不受影响。许可的功能包括：

- 标准
- 安全情景
- 强加密 (3DES/AES)
- AnyConnect-AnyConnect Plus、AnyConnect Apex 或仅 AnyConnect VPN。

强加密 (3DES/AES) 可在您连接到许可证颁发机构或卫星服务器之前用于管理连接，以便您能够启动 ASDM。请注意，ASDM 访问仅在具有默认加密的管理专用接口上可用。在您连接并获取强加密许可证之前，不允许通过设备的流量。

当您向智能软件许可帐户请求 ASA 的注册令牌时，请选中 **Allow export-controlled functionality on the products registered with this token** 复选框，以便应用完整的 Strong Encryption 许可证（您的帐户必须符合其使用条件）。当您在机箱上应用注册令牌时，对于符合条件的用户，系统会自动启用强加密许可证，因此您无需进行其他操作。




---

**注释** 与 Firepower 4100/9300 机箱不同，您在 ASA 上执行所有许可配置，而不是在 FXOS 配置中执行。

---

## 开始之前

- 拥有[思科智能软件管理器](#)主帐户。

如果您还没有帐户，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帐户。

- 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）。

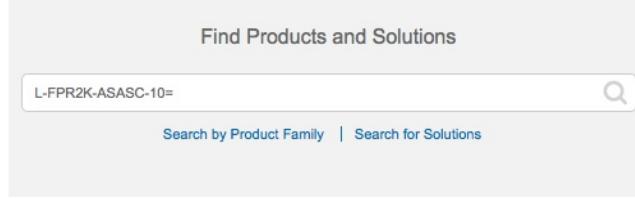
## 过程

---

### 步骤 1 请确保您的智能许可帐户包含您所需的可用许可证，包括最低限度的标准许可证。

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 2: 许可证搜索



- 标准许可证 - L-FPR2100-ASA=。标准许可证是免费的，但您仍然需要将其添加到您的智能软件许可帐户中。
- 5 情景许可证 - L-FPR2K-ASASC-5=。情景许可证是附加的；请购买多份许可证以满足您的需要。
- 10 情景许可证 - L-FPR2K-ASASC-10=。情景许可证是附加的；请购买多份许可证以满足您的需要。
- 强加密 (3DES/AES) 许可证 - L-FPR2K-ENC-K9=。此许可证是免费的。虽然通常不需要此许可证（例如，使用 2.3.0 以前版本的较旧卫星服务器的 ASA 需要此许可证），但您仍应将其添加到您的帐户中以进行跟踪。
- AnyConnect - 请参阅思科 AnyConnect 订购指南。您不能直接在 ASA 中启用此许可证。

**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。

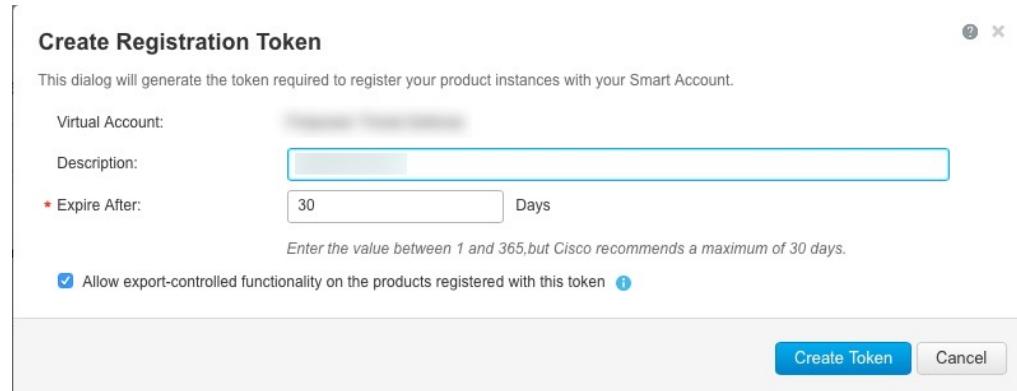
- a) 单击 **Inventory**。

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

Token	Expiration Date	Description
NWU1MzY1MzEtZJNmOS00MjF...	2018-Jul-06 14:20:13 (in 354 days)	FTD-5506

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

## 配置许可



- **Description**

- **Expire After** - 思科建议该时间为 30 天。

- **Allow export-controlled functionality on the products registered with this token** - 启用导出合规性标志。

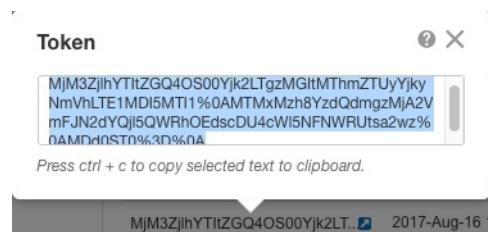
系统将令牌添加到您的资产中。

- 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 ASA 时，请准备好此令牌，以在该程序后面的部分使用。

图 3: 查看令牌

General	Licenses	Product Instances	Event Log		
<b>Virtual Account</b>					
Description:					
Default Virtual Account:	No				
<b>Product Instance Registration Tokens</b>					
The registration tokens below can be used to register new product instances to this virtual account.					
<b>New Token...</b>					
Token	Expiration Date	Description	Export-Controlled	Created By	Actions
MjM3ZjhYTlTZGQ4OS00Yjk2LT...	2017-Aug-16 19:41:53 (in 30 days)	ASA FP 2110 1	Allowed		

图 4: 复制令牌



**步骤 3** 在 ASDM 中，依次选择 **Configuration > Device Management > Licensing > Smart Licensing**。

**步骤 4** 单击 **Register**。

To configure an HTTP proxy for smart licensing, see the [Smart Call-Home](#) page. Note that Smart Call Home is automatically enabled and is required for smart licensing.

Enable Smart license configuration

Feature Tier: -- None --  
Context: (1-38)  
 Enable strong-encryption protocol

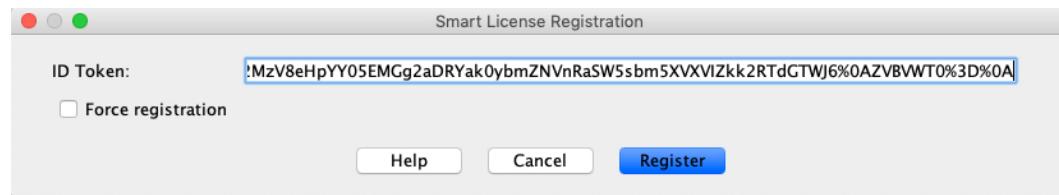
Registration Status: UNREGISTERED

**Register** (highlighted with a red oval) | Renew ID Certificate | Renew Authorization

**Effective Running Licenses**

License Feature	License Value	License Duration
Maximum Physical Interfaces	Unlimited	
Maximum VLANs	1024	
Inside Hosts	Unlimited	
Failover	Active/Active	
Encryption-DES	Enabled	
Encryption-3DES-AES	Enabled	
Security Contexts	2	
Carrier	Disabled	
AnyConnect Premium Peers	10000	
AnyConnect Essentials	Disabled	
Other VPN Peers	10000	
Total VPN Peers	10000	

### 步骤 5 在 ID Token 字段中输入注册令牌。



您可以勾选 **Force registration** 复选框，注册已注册但可能与许可证颁发机构不同步的 ASA。例如，如果从智能软件管理器中意外删除了 ASA，请使用 **Force registration**。

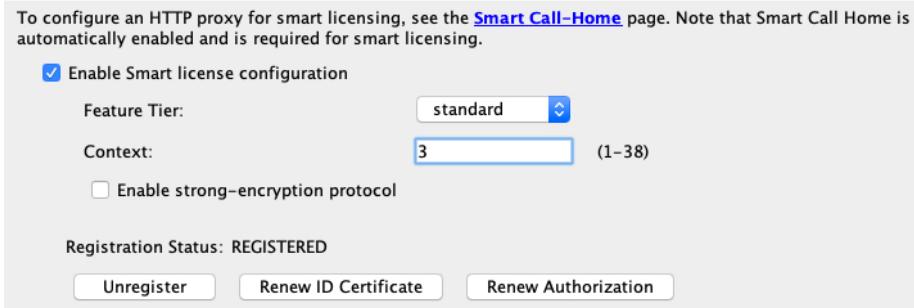
### 步骤 6 单击 Register。

ASA 使用预先配置的外部接口向许可证颁发机构注册，并请求对已配置的许可证授权进行授权。如果您的帐户允许，则许可证颁发机构还会应用强加密(3DES/AES)许可证。当许可状态更新时，ASDM 会刷新页面。您还可以选择 **Monitoring > Properties > Smart License** 以检查许可证状态，尤其是注册失败时。



### 步骤 7 设置以下参数：

## 配置 ASA



- 选中 **Enable Smart license configuration**。
- 从 **Feature Tier** 下拉列表中，选择 **Standard**。

仅标准层可用。

- (可选) 对于情景 (**Context**) 许可证，输入情景的数目。

您可以在没有许可证的情况下使用 2 种情景。情景的最大数目取决于您的型号：

- Firepower 2110 - 25 种情景
- Firepower 2120 - 25 种情景
- Firepower 2130 - 30 种情景
- Firepower 2140 - 40 种情景

例如，对于 Firepower 2110 而言，要使用最大值 - 25 种情景，请为情景数输入 23；此值将与默认值 2 相加。

**步骤 8** (可选) 启用强加密协议通常不是必需的；例如，使用 2.3.0 以前版本的较旧卫星服务器的 ASA 需要此许可证，但如果您知道自己需要，或者想要在帐户中跟踪此许可证的使用情况，可以选中此框。

**步骤 9** 单击 **Apply**。

**步骤 10** 单击工具栏中的 **Save** 图标。

**步骤 11** 退出并重新启动 ASDM。

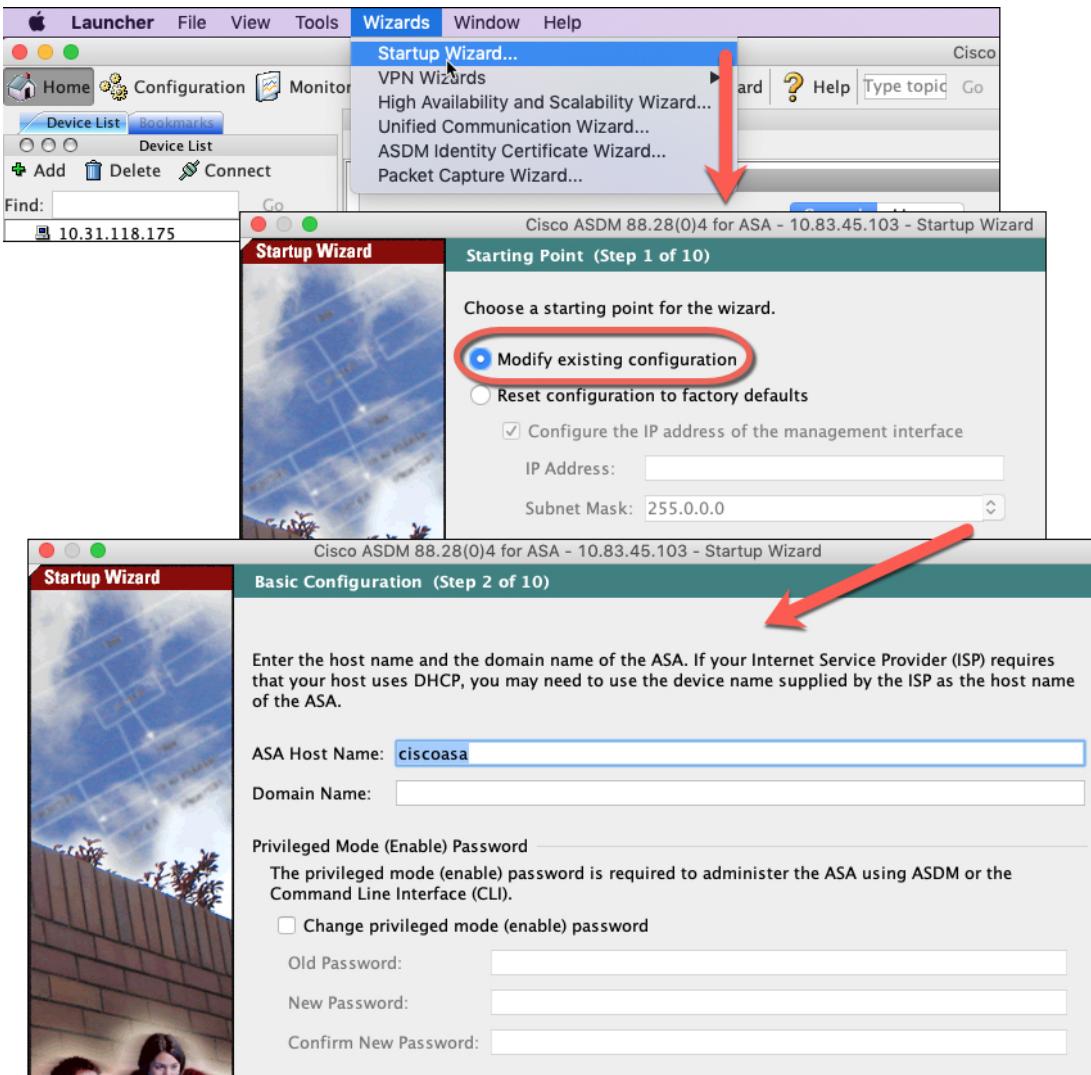
当您更改许可证时，您需要重新启动 ASDM 才能显示更新屏幕。

## 配置 ASA

利用 ASDM，您可以使用向导来配置基本功能和高级功能。您还可以手动配置向导中未包括的功能。

### 过程

**步骤 1** 依次选择 **Wizards > Startup Wizard**，然后单击 **Modify existing configuration** 单选按钮。



**步骤 2** Startup Wizard 将引导您完成配置：

- 启用密码
- 接口，包括更改内部和外部接口 IP 地址以及启用接口。
- 静态路由
- DHCP 服务器
- 其他...

**步骤 3** (可选) 在 Wizards 菜单中，运行其他向导。

**步骤 4** 要继续配置 ASA，请参阅**浏览思科 ASA 系列文档**中适合您的软件版本的文档。

(可选) 在数据接口上配置对 FXOS 的管理访问

## (可选) 在数据接口上配置对 FXOS 的管理访问

如果要从数据接口管理 Firepower 2100 上的 FXOS，则可以配置 SSH、HTTPS 和 SNMP 访问。如果要远程管理设备，并且保持管理 1/1（这是访问 FXOS 的本机方式）位于独立网络中，则此功能非常有用。如果启用此功能，则可以继续使用管理 1/1 进行本地访问。请注意，您不能在使用此功能时允许从管理 1/1 对 FXOS 进行远程访问。此功能需要通过背板将流量转发到 ASA 数据接口（默认），并且您只能指定一个 FXOS 管理网关。

ASA 使用非标准端口进行 FXOS 访问；标准端口将被保留以供同一接口上的 ASA 使用。当 ASA 将流量转发到 FXOS 时，它会针对每个协议将非标准目标端口转换为 FXOS 端口（不会更改 FXOS 中的 HTTPS 端口）。数据包目标 IP 地址（即 ASA 接口 IP 地址）也会被转换为内部地址，供 FXOS 使用。源地址保持不变。为了返回流量，ASA 使用其数据路由表来确定正确的出口接口。当您访问管理应用的 ASA 数据 IP 地址时，必须使用 FXOS 用户名登录；ASA 用户名只适用于 ASA 管理访问。

您还可以在 ASA 数据接口上启用 FXOS 管理流量启动，这是 SNMP 陷阱或进行 NTP 和 DNS 服务器等所需的。默认情况下，将为 ASA 外部接口启用 FXOS 管理流量启动，以进行 DNS 和 NTP 服务器通信（这是进行智能软件许可通信所必需的）。

### 开始之前

- 仅限单一情景模式。
- 不包括 ASA 仅管理接口。
- 不能直接通过 VPN 隧道连接至 ASA 数据接口，也不能直接访问 FXOS。作为 SSH 的一种变通方法，可以通过 VPN 连接到 ASA，访问 ASA CLI，然后使用 **connect fxos** 命令访问 FXOS CLI。请注意，SSH、HTTPS 和 SNMPv3 已经加密/可以加密，因此直接连接到数据接口是安全的。
- 确保 FXOS 网关已设置为将流量转发到 ASA 数据接口（默认值）。如果更改了网关，请参阅 [\(可选\) 更改 FXOS 管理 IP 地址或网关，第 25 页](#)。

### 过程

---

**步骤 1** 在 ASDM 中，选择配置 > 设备管理 > 管理访问 > FXOS 远程管理。

**步骤 2** 启用 FXOS 远程管理。

- a) 从导航窗格中选择 **HTTPS、SNMP 或 SSH**。
- b) 点击添加 (**Add**)，并设置要允许管理的接口 (**Interface**)，设置允许连接的 IP 地址 (**IP Address**)，然后点击确定 (**OK**)。

您可以为每个协议类型创建多个条目。如果不使用以下默认值，请设置端口 (**Port**):

- HTTPS 默认端口 - 3443
- SNMP 默认端口 - 3061
- SSH 默认端口 - 3022

**步骤 3** 允许 FXOS 从 ASA 接口启动管理连接。

- 从导航窗格中选择 **FXOS 流量启动 (FXOS Traffic Initiation)**。
- 点击 **添加 (Add)**，并启用发送 FXOS 管理流量所需的 ASA 接口。默认情况下，外部接口处于启用状态。

**步骤 4** 点击 **Apply**。

**步骤 5** 连接到 Firepower 机箱管理器（默认情况下网址为 <https://192.168.45.45>，用户名为 **admin**，密码为初次登录时设置的密码）。

**步骤 6** 点击 **平台设置 (Platform Settings)** 选项卡，然后启用 **SSH、HTTPS 或 SNMP**。

默认情况下，SSH 和 HTTPS 处于启用状态。

**步骤 7** 将 **平台设置 (Platform Settings)** 选项卡上的 **访问列表 (Access List)** 配置为允许您的管理地址。默认情况下，SSH 和 HTTPS 只允许管理 1/1 192.168.45.0 网络。您需要允许在 ASA 上的 **FXOS 远程管理 (FXOS Remote Management)** 配置中指定的任何地址。

## 访问 ASA 和 FXOS CLI

本节介绍如何连接到 FXOS 和 ASA 控制台，以及如何使用 SSH 连接到 FXOS。

### 连接到控制台端口以访问 FXOS 和 ASA CLI

Firepower 2100 控制台端口会将您连接到 FXOS CLI。您可以从 FXOS CLI 中连接到 ASA 控制台，然后再次返回。

每次只能使用一个控制台连接。当您从 FXOS 控制台连接到 ASA 控制台时，此连接是一个持久控制台连接，而不像 Telnet 或 SSH 连接那样。

#### 过程

**步骤 1** 将管理计算机连接到控制台端口。Firepower 2100 配有一条 DB-9 转 RJ-45 串行线缆，所以您需要第三方串行转 USB 线缆进行连接。确保为操作系统安装任何必要的 USB 串行驱动程序。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。输入用户凭证；默认情况下，您可以使用用户 **admin** 和默认密码 **Admin123** 登录。首次登录时，系统会提示您更改 **admin** 密码。

## 使用 SSH 连接到 FXOS

### 步骤 2 连接到 ASA:

**connect asa**

示例:

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

### 步骤 3 要返回到 FXOS 控制台, 请输入 **Ctrl+a, d**。

---

## 使用 SSH 连接到 FXOS

您可以使用默认 IP 地址 192.168.45.45 连接到管理 1/1 上的 FXOS。如果配置远程管理（[（可选）在数据接口上配置对 FXOS 的管理访问, 第 22 页](#)），则还可以连接到非标准端口（默认情况下为 3022）上的数据接口 IP 地址。

要使用 SSH 连接到 ASA，必须首先根据 [ASA 通用操作配置指南](#) 配置 SSH 访问。

您可以从 FXOS 连接到 ASA CLI，反之亦然。

FXOS 最多允许 8 条 SSH 连接。

### 开始之前

要更改管理 IP 地址，请参阅 [（可选）更改 FXOS 管理 IP 地址或网关, 第 25 页](#)。

### 过程

---

#### 步骤 1 在连接到管理 1/1 的管理计算机上，将 SSH 连接到管理 IP 地址（默认情况下为 https://192.168.45.45，使用用户名: **admin** 和密码: **Admin123**）。

如果在 FXOS 中添加了用户，则可以使用任何用户名登录。如果配置远程管理，则将 SSH 连接到端口 3022 上的 ASA 数据接口 IP 地址（默认端口）。

#### 步骤 2 连接到 ASA CLI。

**connect asa**

要返回到 FXOS CLI，请输入 **Ctrl+a, d**。

示例:

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

**步骤 3** 如果您将 SSH 连接到 ASA（在 ASA 中配置 SSH 访问后），请连接到 FXOS CLI。

#### connect fxos

系统会提示您对 FXOS 进行身份验证；使用默认用户名：**admin** 和密码：**Admin123**。要返回到 ASA CLI，请输入 **exit** 或键入 **Ctrl-Shift-6, x**。

**示例：**

```
ciscoasa# connect fxos
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
FXOS 2.2(2.32) kp2110

firepower-2110 login: admin
Password: Admin123
Last login: Sat Jan 23 16:20:16 UTC 2017 on pts/1
Successful login attempts for user 'admin' : 4
Cisco Firepower Extensible Operating System (FX-OS) Software

[...]

firepower-2110#
firepower-2110# exit
Remote card closed command session. Press any key to continue.
Connection with fxos terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

## (可选) 更改 FXOS 管理 IP 地址或网关

您可以从 FXOS CLI 更改 Firepower 2100 机箱上的 FXOS 管理 IP 地址。默认地址为 192.168.45.45。您还可以更改默认网关。默认网关设置为 0.0.0.0，它将流量发送到背板上的 ASA。如果要改为在管理 1/1 网络中使用路由器，则可以更改网关 IP 地址。此外，您还必须更改管理连接的访问列表以匹配新网络。

通常，FXOS 管理 1/1 IP 地址将与 ASA 管理 1/1 IP 地址在同一网络上；因此该过程也显示如何更改 ASA 上的 ASA IP 地址。

### 开始之前

- 更改管理 IP 地址后，需要使用新地址重新建立所有 Firepower 机箱管理器和 SSH 连接。
- 由于默认情况下在管理 1/1 上启用了 DHCP 服务器，因此在更改管理 IP 地址之前必须禁用 DHCP。

(可选) 更改 FXOS 管理 IP 地址或网关

## 过程

**步骤 1** 连接到控制台端口（请参阅 [连接到控制台端口以访问 FXOS 和 ASA CLI，第 23 页](#)）。我们建议您连接到控制台端口，以避免连接断开。

**步骤 2** 禁用 DHCP 服务器。

```
scope system
scope services
disable dhcp-server
commit-buffer
```

更改管理 IP 地址后，可以使用新客户端 IP 地址重新启用 DHCP。您还可以通过平台设置 (Platform Settings) > **DHCP** 在 Firepower 机箱管理器中启用或禁用 DHCP 服务器。

示例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # disable dhcp-server
firepower-2110 /system/services* # commit-buffer
```

**步骤 3** 配置 IPv4 管理 IP 地址，还可以配置网关（可选）。

a) 设置交换矩阵互联 a 的范围。

```
scope fabric-interconnect a
```

示例：

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect #
```

b) 查看当前的管理 IP 地址。

```
show
```

示例：

```
firepower-2110 /fabric-interconnect # show

Fabric Interconnect:
  ID   OOB IP Addr      OOB Gateway      OOB Netmask      OOB IPv6 Address OOB IPv6 Gateway
  Prefix Operability
  -----
  A     192.168.45.45    0.0.0.0          0.0.0.0          ::                      ::
  64    Operable
```

c) 配置新管理 IP 地址，还可以配置新的默认网关（可选）。

```
set out-of-band static ip ip_address netmask network_mask gw gateway_ip_address
```

要保留当前设置的网关，请省略关键字 **gw**。同样，要在更改网关时保留现有的管理 IP 地址，请省略关键字 **ip** and **netmask**。

要将网关设置为 ASA 数据接口，请将 **gw** 设置为 0.0.0.0。这是默认设置。

**示例:**

```
firepower-2110 /fabric-interconnect # set out-of-band static ip 192.168.4.1 netmask
255.255.255.0
Warning: When committed, this change may disconnect the current CLI session
firepower-2110 /fabric-interconnect* #
```

#### 步骤 4 配置 IPv6 管理 IP 地址和网关。

- 设置交换矩阵互联 a 的范围，然后设置 IPv6 配置的范围。

**scope fabric-interconnect a**

**scope ipv6-config**

**示例:**

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # scope ipv6-config
firepower-2110 /fabric-interconnect/ipv6-config #
```

- 查看当前的管理 IPv6 地址。

**show ipv6-if**

**示例:**

```
firepower-2110 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
IPv6 Address          Prefix      IPv6 Gateway
-----:-----:-----:-----:
::                  ::          ::
```

- 配置新的管理 IPv6 地址和网关：

```
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band static ipv6 ipv6_address ipv6-prefix
prefix_length ipv6-gw gateway_address
```

要保留当前设置的网关，请省略关键字 **ipv6-gw**。同样，要在更改网关时保留现有的管理 IP 地址，请省略关键字 **ipv6** and **ipv6-prefix**。

要将网关设置为 ASA 数据接口，请将 **gw** 设置为 ::。这是默认设置。

**示例:**

```
firepower-2110 /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001:DB8::34
ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config* #
```

#### 步骤 5 删 除 HTTPS、SSH 和 SNMP 的访问列表并添加新列表，以允许来自新网络的管理连接。

## (可选) 更改 FXOS 管理 IP 地址或网关

- a) 为系统/服务设置范围。

**scope system**

**scope services**

示例:

```
firepower-2110# scope system
firepower-2110 /system # scope services
```

- b) 查看当前访问列表。

**show ip-block**

示例:

```
firepower-2110 /system/services # show ip-block

Permitted IP Block:
  IP Address      Prefix Length Protocol
  -----          -----        -----
  192.168.45.0    24 https
  192.168.45.0    24 ssh
firepower-2140 /system/services #
```

- c) 添加新的访问列表。

IPv4:

**enter ip-block ip\_address prefix[http | snmp | ssh]**

IPv6:

**enter ipv6-block ipv6\_address prefix[https | snmp | ssh]**

对于 IPv4，请输入 **0.0.0.0** 和前缀 **0** 以允许所有网络。对于 IPv6，请输入 **::** 和前缀 **0** 以允许所有网络。还可以通过平台设置 (Platform Settings) > 访问列表 (Access List) 在 Firepower 机箱管理器中添加访问列表。

示例:

```
firepower-2110 /system/services # enter ip-block 192.168.4.0 24 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.4.0 24 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.4.0 24 snmp
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 snmp
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* #
```

- a) 删除旧的访问列表。

IPv4:

**delete ip-block ip\_address prefix[http | snmp | ssh]**

IPv6:

**delete ipv6-block ipv6\_address prefix[https | snmp | ssh]**

示例:

```
firepower-2110 /system/services # delete ip-block 192.168.45.0 24 https
firepower-2110 /system/services* # delete ip-block 192.168.45.0 24 ssh
firepower-2110 /system/services* #
```

#### 步骤 6 (可选) 重新启用 IPv4 DHCP 服务器。

**scope system**

**scope services**

**enable dhcp-server start\_ip\_address end\_ip\_address**

您还可以通过平台设置 (Platform Settings) > DHCP 在 Firepower 机箱管理器中启用或禁用 DHCP 服务器。

示例:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enable dhcp-server 192.168.4.10 192.168.4.20
```

#### 步骤 7 保存配置。

**commit-buffer**

示例:

```
firepower-2110 /system/services* # commit-buffer
```

#### 步骤 8 将 ASA 地址更改为在正确的网络上。默认 ASA 管理接口 1/1 IP 地址为 192.168.45.1。

- 从控制台连接到 ASA CLI 并访问全局配置模式。

**connect asa**

**enable**

**configure terminal**

示例:

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: *****
Repeat Password: *****
```

## (可选) 更改 FXOS 管理 IP 地址或网关

```
ciscoasa# configure terminal
ciscoasa(config)#
```

- b) 更改管理 1/1 IP 地址。

**interface management1/1**

**ip address ip\_address mask**

示例:

```
ciscoasa(config)# interface management1/1
ciscoasa(config-ifc)# ip address 10.86.118.4 255.255.255.0
```

- c) 更改可访问 ASDM 的网络。

**no http 192.168.45.0 255.255.255.0 management**

**http ip\_address mask management**

示例:

```
ciscoasa(config)# no http 192.168.45.0 255.255.255.0 management
ciscoasa(config)# http 10.86.118.0 255.255.255.0 management
```

- d) 保存配置。

**write memory**

- e) 要返回到 FXOS 控制台, 请输入 **Ctrl+a, d**。

### 示例

以下示例配置 IPv4 管理接口和网关:

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # show

Fabric Interconnect:
  ID   OOB IP Addr      OOB Gateway      OOB Netmask      OOB IPv6 Address OOB IPv6 Gateway
  Prefix Operability
  ---- -----
  A     192.168.2.112    192.168.2.1      255.255.255.0   2001:DB8::2      2001:DB8::1
  64    Operable

firepower-2110 /fabric-interconnect # set out-of-band static ip 192.168.2.111 netmask
255.255.255.0 gw 192.168.2.1
Warning: When committed, this change may disconnect the current CLI session
firepower-2110 /fabric-interconnect* # commit-buffer
firepower-2110 /fabric-interconnect #
```

以下示例配置 IPv6 管理接口和网关:

```
firepower-2110# scope fabric-interconnect a
```

```

firepower-2110 /fabric-interconnect # scope ipv6-config
firepower-2110 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
  IPv6 Address           Prefix      IPv6 Gateway
  -----
  2001:DB8::2             64          2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001:DB8::2
ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config* # commit-buffer
firepower-2110 /fabric-interconnect/ipv6-config #

```

## 后续操作

- 要继续配置 ASA，请参阅[浏览思科 ASA 系列文档中适合您的软件版本的文档](#)。
- 要配置 FXOS 机箱设置，请参阅《[FXOS 配置指南](#)》。
- 有关故障排除，请参阅《[FXOS 故障排除指南](#)》。

## 平台模式下 Firepower 2100 的历史记录

功能名称	版本	功能信息
默认模式已更改为设备模式	9.13(1)	<p>引入设备模式后，默认模式已更改为设备模式。在早期版本中，只能使用平台模式。如果您要升级到 9.13(1)，该模式将保留在平台模式下。</p> <p>新增/修改的命令：<b>fxos mode appliance</b>、<b>show fxos mode</b>。</p>
提示设置管理员密码	9.13(1)	首次登录 Firepower 机箱管理器时，系统不会提示您设置管理员密码。以前，默认密码为 <b>Admin123</b> 。

■ 平台模式下 Firepower 2100 的历史记录