



使用 ASDM 部署 ASA

本章对您适用吗？

本章介绍如何部署独立式 ASA 逻辑设备，包括如何配置智能许可。本章不涉及以下部署，请参考《ASA 配置指南》了解相关内容：

- 集群
- 故障切换
- CLI 配置

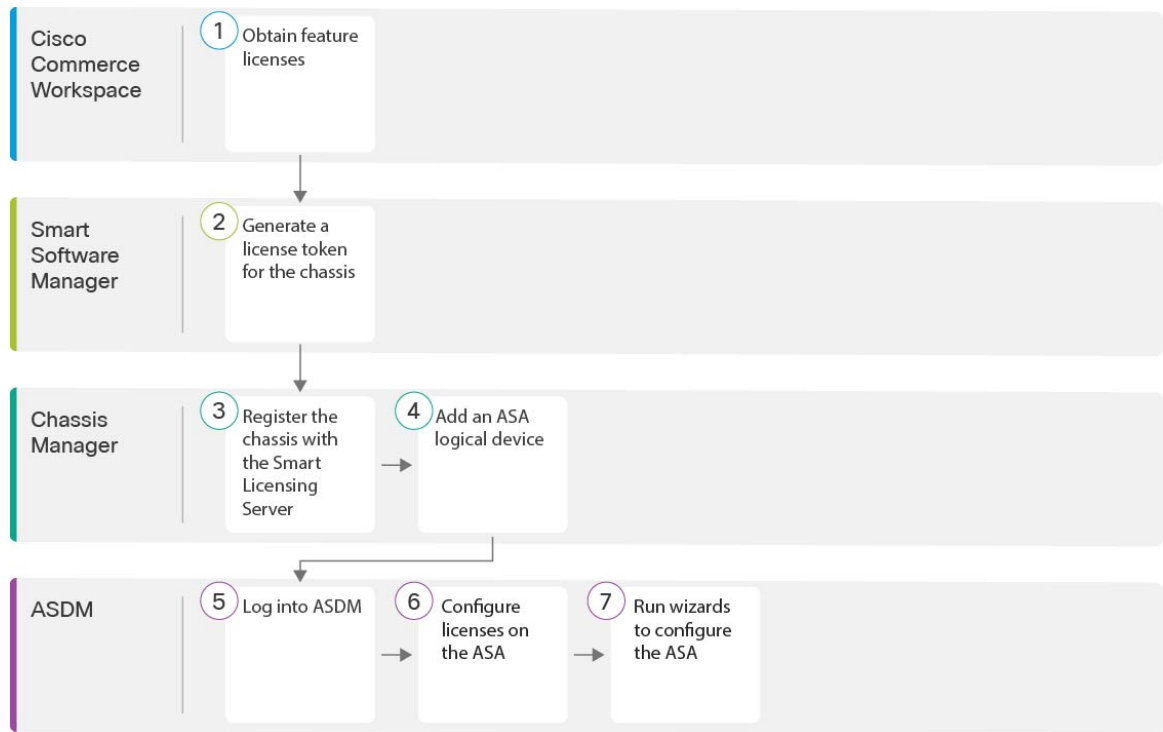
本章还演示如何配置基本安全策略；如果您有更高级的要求，请参阅配置指南。

隐私收集声明 - Firepower 4100 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，第 1 页](#)
- [机箱管理器：向许可证服务器注册机箱，第 2 页](#)
- [机箱管理器：添加 ASA 逻辑设备，第 7 页](#)
- [登录 ASDM，第 10 页](#)
- [在 ASA 上配置许可证授权，第 11 页](#)
- [配置 ASA，第 12 页](#)
- [访问 ASA CLI，第 13 页](#)
- [后续步骤，第 14 页](#)
- [ASA 的历史记录，第 15 页](#)

端到端程序

请参阅以下任务以在机箱上部署和配置 ASA。



①	Cisco Commerce Workspace	机箱管理器：向许可证服务器注册机箱，第 2 页；获取功能许可证。
②	智能软件管理器	机箱管理器：向许可证服务器注册机箱，第 2 页；为机箱生成许可证令牌。
③	机箱管理器	机箱管理器：向许可证服务器注册机箱，第 2 页；向智能许可服务器注册机箱。
④	机箱管理器	机箱管理器：添加 ASA 逻辑设备，第 7 页。
⑤	ASDM	登录 ASDM，第 10 页。
⑥	ASDM	在 ASA 上配置许可证授权，第 11 页。
⑦	ASDM	配置 ASA，第 12 页。

机箱管理器：向许可证服务器注册机箱

ASA 使用智能许可。您可以使用常规智能许可，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预留或智能软件管理器本地版（之前称为卫星服务器）。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许可。

有关思科许可的更详细概述，请访问 cisco.com/go/licensingguide

对于 Firepower 4100 上的 ASA，智能软件许可配置分为两部分，分别在机箱上的 FXOS 和 ASA 中进行。

- Firepower 4100- 所有智能软件许可基础设施均在 FXOS 中配置，包括用于与许可证颁发机构进行通信的参数。Firepower 4100 本身无需任何许可证即可运行。
- ASA - 在 ASA 中配置所有许可证授权。

注册机箱时，智能软件管理器会为防火墙和智能软件管理器之间的通信颁发 ID 证书。它还会将防火墙分配到相应的虚拟帐户。除非您向智能软件管理器注册，否则您将无法进行配置更改，因为有些功能需要特殊许可，但其他方面的操作不受影响。许可的功能包括：

- 基础
- 安全情景
- 运营商 - Diameter、GTP/GPRS、M3UA、SCTP
- 强加密 (3DES/AES)- 如果您的智能帐户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的帐户。
- Cisco Secure 客户端 - Secure Client Advantage、Secure Client Premier 或 Secure Client VPN Only

当您向智能软件管理器请求 ASA 的注册令牌时，请选中在使用此令牌注册的产品上允许导出控制的功能 (**Allow export-controlled functionality on the products registered with this token**) 复选框，以便应用完整的强加密许可证（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。如果您的智能帐户未获得强加密授权，但 Cisco 已确定允许您使用强加密，您可以手动将强加密许可证添加到您的帐户。

进行 ASDM 访问需要强加密。

开始之前

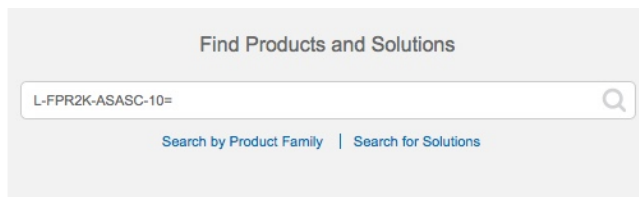
- 拥有 [智能软件管理器](#) 主帐户。
如果您还没有帐户，请点击此链接以 [设置新帐户](#)。通过智能软件管理器，您可以为组织创建一个主帐户。
- 您的智能软件管理器帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。
- 如果尚未执行此操作，请 [配置 NTP](#)。
- 如果在初始设置期间没有配置 DNS，请在 [平台设置 > DNS](#) 页面添加 DNS 服务器。

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，包括最低限度的基础许可证。

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管理器帐户。但是，如果您需要自己添加许可证，则请使用 [Cisco Commerce Workspace](#) 上的 **Find Products and Solutions** 搜索字段。搜索以下许可证 PID：

图 1: 许可证搜索



- 基础许可证 — L-FPR4100-ASA=。基础许可证是免费的，但您仍然需要将其添加到您的智能软件许可帐户中。
- 10 情景许可证 - L-FPR4K-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。
- 230 情景许可证 - L-FPR4K-ASASC-230=。情景许可证是附加的；请购买多份许可证以满足您的需要。
- 250 情景许可证 - L-FPR4K-ASASC-250=。情景许可证是附加的；请购买多份许可证以满足您的需要。
- 运营商 (Diameter, GTP/GPRS, M3UA, SCTP) — L-FPR4K-ASA-CAR=
- 强加密 (3DES/AES) 许可证 - FPR4K-ENC-K9 =。仅当帐户未获授权使用强加密时需要。
- Cisco Secure 客户端 - 请参阅 [思科安全客户端订购指南](#)。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) 点击 **Inventory**。



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

The screenshot shows the ASA configuration interface with tabs for General, Licenses, Product Instances, and Event Log. Under the 'Product Instances' tab, there is a 'Virtual Account' section and a 'Product Instance Registration Tokens' section. The 'New Token...' button is highlighted with a red circle.

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，然后点击 **Create Token**：

The 'Create Registration Token' dialog box contains the following fields and options:

- Virtual Account: [Redacted]
- Description: [Empty text box]
- Expire After: 30 Days
- Allow export-controlled functionality on the products registered with this token:

Buttons: Create Token, Cancel

- **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) 点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 2: 查看令牌

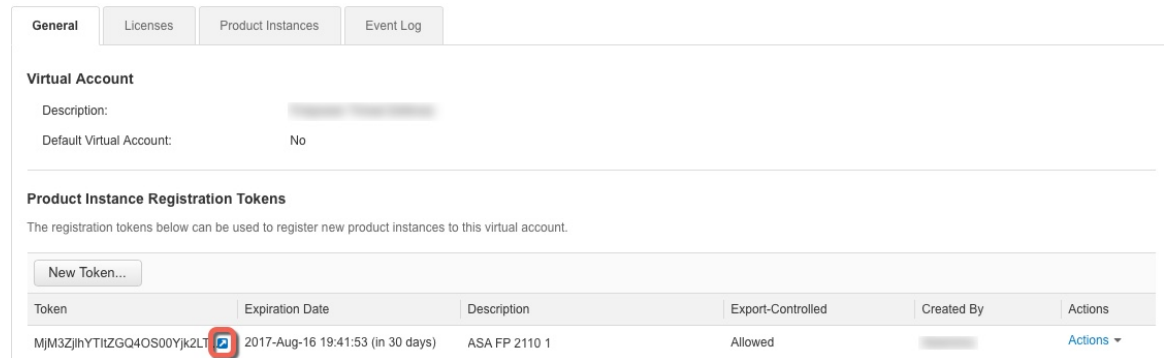
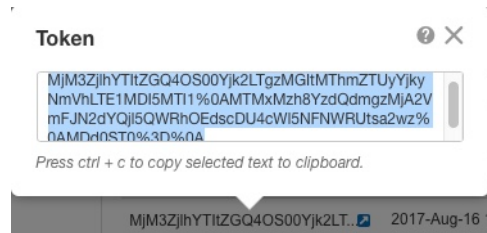
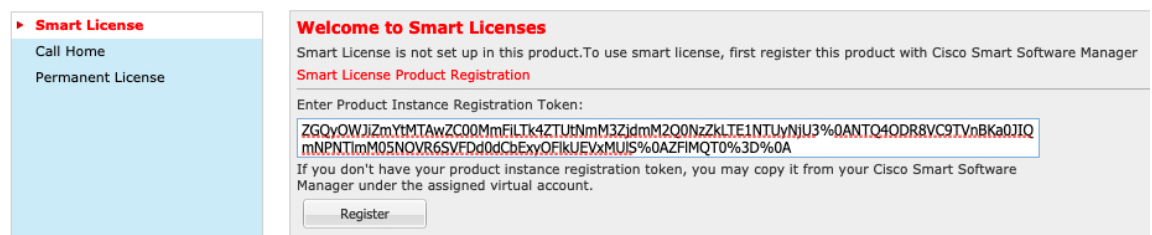


图 3: 复制令牌



步骤 3 在机箱管理器中，选择系统 (System) > 许可 (Licensing) > 智能许可证 (Smart License)。

步骤 4 在输入产品实例注册令牌 (Enter Product Instance Registration Token) 字段中输入注册令牌。



步骤 5 点击 Register。

Firepower 4100 向许可证颁发机构注册。成功注册可能需要几分钟时间。刷新此页面可查看状态。

图 4: 正在注册

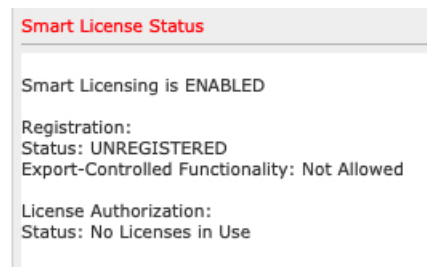
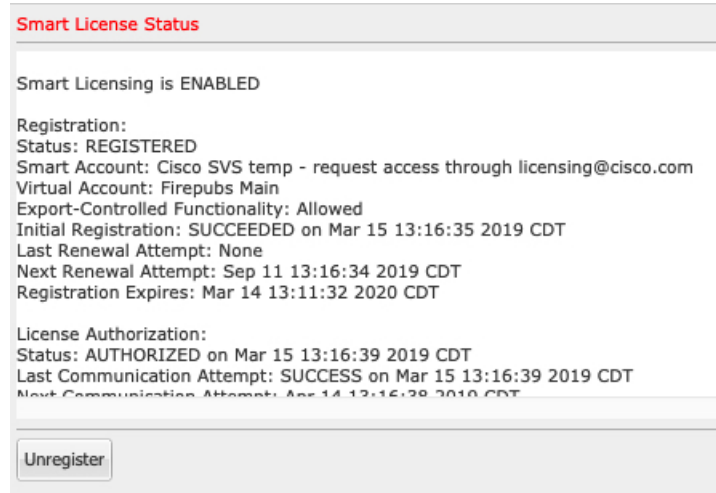


图 5: 注册成功



机箱管理器：添加 ASA 逻辑设备

您可以从 Firepower 4100 将 ASA 部署为本地实例。

要添加故障转移对或集群，请参阅 ASA 通用操作配置指南。

您可以通过此程序配置逻辑设备特性，包括应用程序使用的引导程序配置。

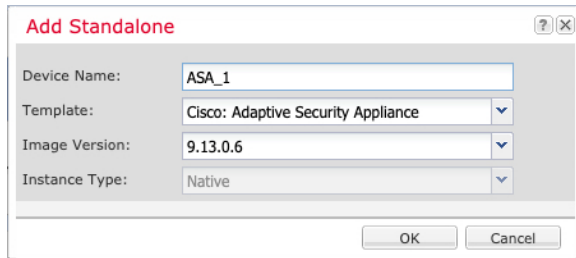
开始之前

- 配置与 ASA 一起使用的管理接口；请参阅[配置接口](#)。管理接口是必需的。请注意，此管理接口与仅用于机箱管理的机箱管理端口（并且该端口在[接口选项卡](#)的顶部显示为 **MGMT**）不同。
- 收集以下信息：
 - 此设备的接口 ID
 - 管理接口 IP 地址和网络掩码
 - 网关 IP 地址
 - 新管理员密码/启用密码

过程

步骤 1 在机箱管理器中，选择逻辑设备。

步骤 2 点击添加 > 独立设备，并设置以下参数：



a) 提供设备名称。

此名称由机箱管理引擎用于配置管理设置和分配接口；它不是在应用配置中使用的设备名称。

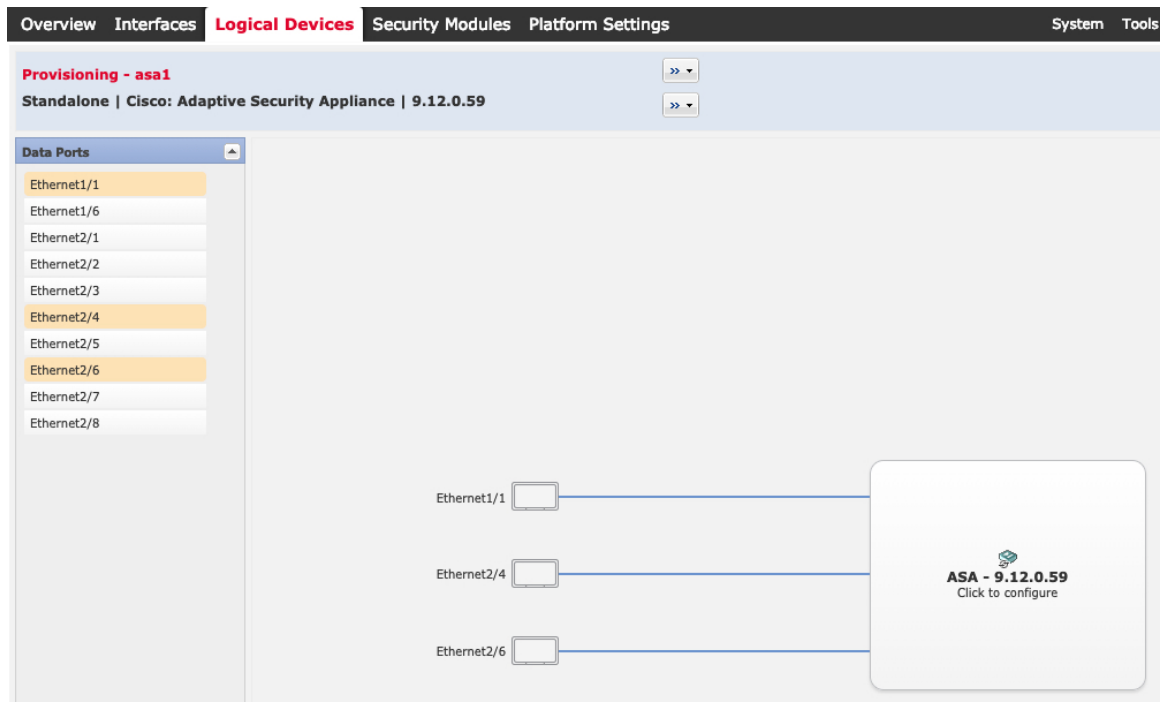
b) 对于模板，请选择思科：自适应安全设备。

c) 选择映像版本。

d) 点击确定 (OK)。

屏幕会显示调配 - 设备名称窗口。

步骤 3 展开数据端口区域，然后点击要分配给设备的每个接口。



仅可分配先前在接口页面上启用的数据接口。稍后需要在 ASDM 中启用和配置这些接口，包括设置 IP 地址。

步骤 4 点击屏幕中心的设备图标。

系统将显示对话框，可以在该对话框中配置初始引导程序设置。这些设置仅用于仅初始部署或灾难恢复。为了实现正常运行，稍后可以更改应用 CLI 配置中的大多数值。

步骤 5 在一般信息 (General Information) 页面上，完成下列操作：

Cisco: Adaptive Security Appliance - Bootstrap Configuration

General Information Settings

Interface Information

Management Interface:

DEFAULT

Address Type:

IPv4

Management IP:

Network Mask:

Network Gateway:

- 选择管理接口。
此接口用于管理逻辑设备。此接口独立于机箱管理端口。
- 选择管理接口地址类型：仅 IPv4、仅 IPv6 或 IPv4 和 IPv6。
- 配置管理 IP 地址。
设置用于此接口的唯一 IP 地址。
- 输入网络掩码或前缀长度。
- 输入网络网关地址。

步骤 6 点击设置。

Cisco: Adaptive Security Appliance - Bootstrap Configuration

General Information **Settings**

Firewall Mode:

Password:

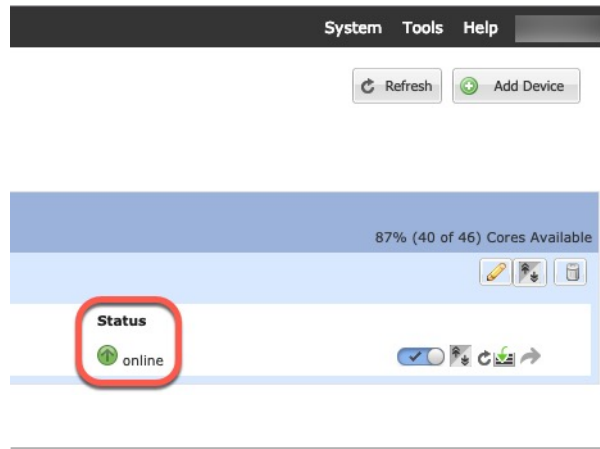
Confirm Password:

- 选择防火墙模式：路由式或透明。
在路由模式下，ASA 被视为网络中的一个路由器跃点。要在其间路由的每个接口都位于不同的子网上。另一方面，透明防火墙是一个第2层防火墙，充当“电缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。
系统仅在初始部署时设置防火墙模式。如果您重新应用引导程序设置，则不会使用此设置。
- 输入并确认管理员用户和启用密码的密码。
预配置的 ASA 管理员用户/密码和启用密码在进行密码恢复时非常有用；如果有 FXOS 访问权限，在忘记管理员用户密码/启用密码时，可以将其重置。

步骤 7 点击确定 (OK) 关闭配置对话框。

步骤 8 点击保存 (Save)。

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。在逻辑设备 (Logical Devices) 页面中，查看新逻辑设备的状态。当逻辑设备将其状态显示为在线时，可以开始在应用中配置安全策略。



登录 ASDM

启动 ASDM 以便配置 ASA。

开始之前

- 请参阅 Cisco.com 上的 [ASDM 发行说明](#) 了解运行 ASDM 的要求。
- 确保机箱管理器逻辑设备 (Logical Devices) 页面上 ASA 逻辑设备的状态 (Status) 为在线 (online)。

过程

步骤 1 在浏览器中输入以下 URL。

- **https://management_ip** - 在引导程序配置中输入的管理接口 IP 地址。

注释 确保指定 **https://**，而非指定 **http://** 或只指定 IP 地址（默认为 HTTP）；ASA 不会自动将 HTTP 请求转发到 HTTPS。

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 点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，输入在部署 ASA 时设置的启用密码，然后点击**确定**。

系统将显示 ASDM 主窗口。

在 ASA 上配置许可证授权

向 ASA 分配许可证。必须至少分配标准许可证。

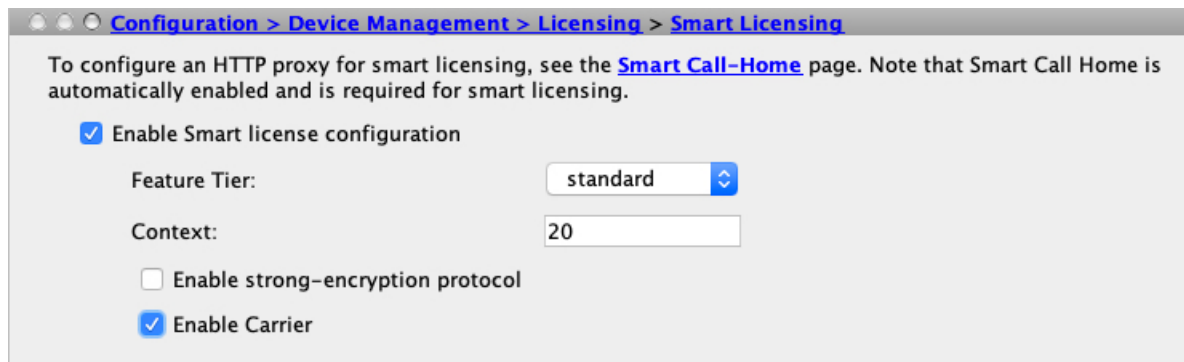
开始之前

- **机箱管理器**：向许可证服务器注册机箱，第 2 页。

过程

步骤 1 在 ASDM 中，依次选择 **Configuration > Device Management > Licensing > Smart Licensing**。

步骤 2 设置以下参数：



- a) 选中 **Enable Smart license configuration**。
- b) 从功能层 (**Feature Tier**) 下拉列表中，选择**基础 (Essentials)**。

仅基础层可用。

- c) （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 10 种情景。最大情景数为 250。例如，要使用最大值，请为情景数输入 240；此值将与默认值 10 相加。

- d) （可选）检查**运营商**。

步骤 3 点击 **Apply**。

如果您的帐户中没有相应的许可证，则无法应用许可证更改。

步骤 4 点击工具栏中的 **Save** 图标。

步骤 5 退出并重新启动 ASDM。

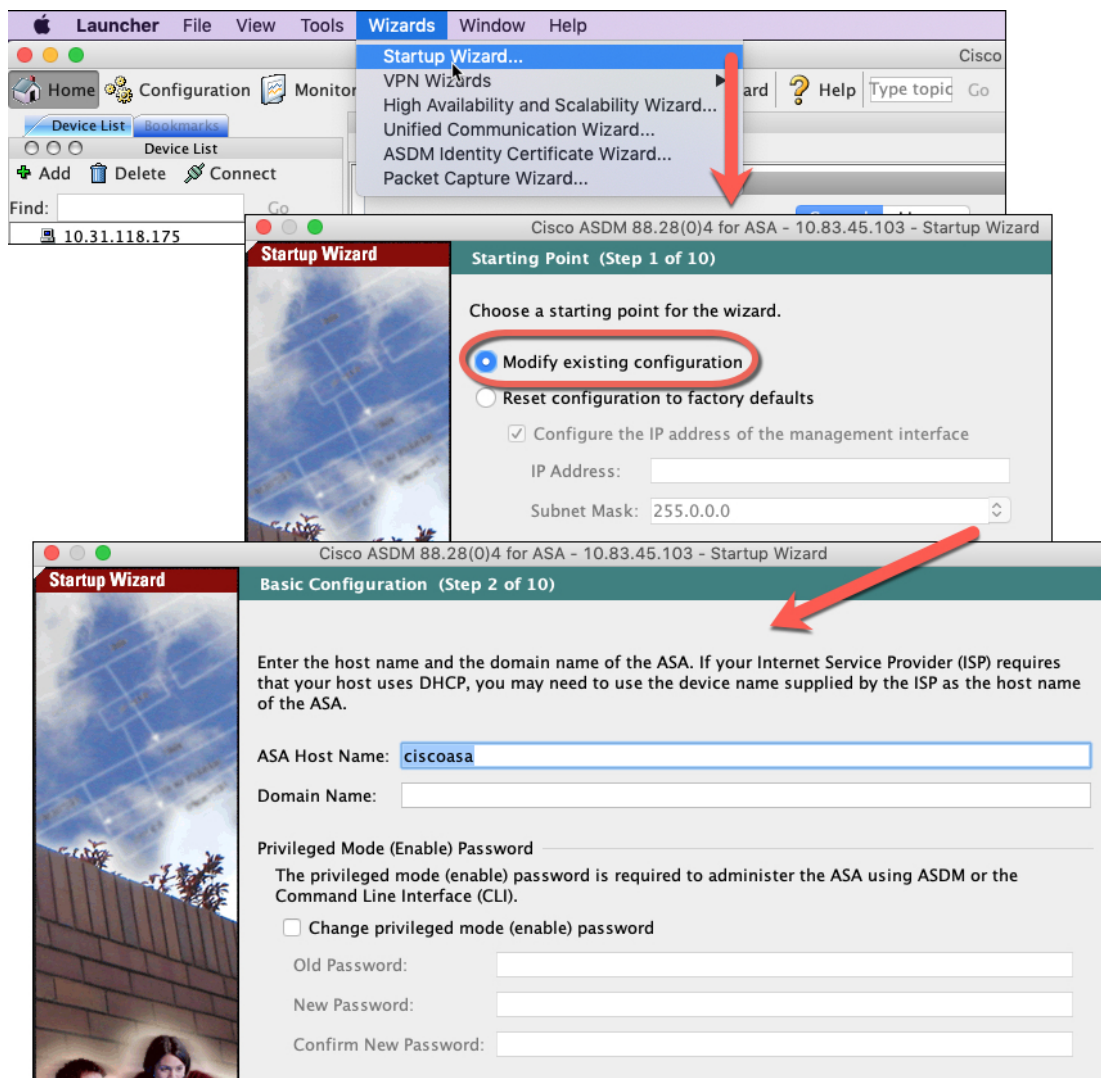
当您更改许可证时，您需要重新启动 ASDM 才能显示更新屏幕。

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。

访问 ASA CLI

您可以使用 ASA CLI (而非 ASDM) 对 ASA 进行故障排除或配置。您可以通过 FXOS CLI 连接以访问 CLI。之后, 您就可以在任何接口上配置对 ASA 的 SSH 访问。有关更多信息, 请参阅 ASA 一般操作配置指南。

过程

步骤 1 从 FXOS CLI, 使用控制台连接或 Telnet 连接以连接到模块 CLI。

connect module 1 { console | telnet }

使用 Telnet 连接的优点在于, 您可以同时对模块开展多个会话, 并且连接速度更快。

示例:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

步骤 2 连接到 ASA 控制台。

connect asa

示例:

```
Firepower-module1> connect asa
Connecting to asa(asal) console... hit Ctrl + A + D to return to bootCLI
```

```
[...]
asa>
```

步骤 3 输入 **Ctrl-a, d** 使应用程序控制台返回到 FXOS 模块 CLI。

步骤 4 返回 FXOS CLI 的管理引擎层。

退出控制台：

a) 输入 ~

您将退出至 Telnet 应用。

b) 要退出 Telnet 应用，请输入：

```
telnet>quit
```

退出 Telnet 会话：

a) 输入 **Ctrl-]**。

示例

以下示例说明了如何连接至上的 ASA，然后退回到 FXOS CLI 的管理引擎层。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa
asa> ~
telnet> quit
Connection closed.
Firepower#
```

后续步骤

- 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。

ASA 的历史记录

特性	版本	详细信息
适用于 Firepower 4115、4125 和 4145 的 ASA	9.12(1)	我们推出了 Firepower 4115、4125 和 4145。 注释 需要 FXOS 2.6.1。
支持在同一个 Firepower 9300 上使用独立的 ASA 和 威胁防御 模块	9.12(1)	您现在可以在同一个 Firepower 9300 上同时部署 ASA 和 威胁防御 逻辑设备。 注释 需要 FXOS 2.6.1。
支持 ASA 逻辑设备的透明模式部署	9.10(1)	您现在可以在部署 ASA 时指定透明模式或路由模式。 注释 需要 FXOS 2.4.1。 新增/修改的 机箱管理器 菜单项： 逻辑设备 > 添加设备 > 设置 > 防火墙模式下拉列表
智能代理升级至 v1.6	9.6(2)	智能代理从 1.1 版本升级到 1.6 版本。此升级支持永久许可证预留，同时也支持依据许可证账号中的权限集设置强加密 (3DES/AES) 许可证授权。
新运营商许可证	9.5(2)	用于替换现有的 GTP/GPRS 许可证的新运营商许可证提供的支持包括 SCTP 和 Diameter 检测。对于 Firepower 9300 上的 ASA， feature mobile-sp 命令将自动迁移到 feature carrier 命令。 修改了以下菜单项：配置 > 设备管理 > 许可 > 智能许可

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。