在设备模式下部署 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：

- 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。
- 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。

本章介绍如何在 ASA 设备模式下在网络中部署 Firepower 2100。默认情况下，Firepower 2100 会在设备模式下运行以使用平台模式，请参阅在平台模式下部署 ASA。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

ASA 在一台设备中提供高级状态防火墙和 VPN 集中器功能。您可以使用以下任一管理器管理 ASA：

- 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。

也可以访问 FXOS CLI 以进行故障排除。

不支持的功能

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

迁移 ASA 5500-X 配置

您可以将 ASA 5500-X 配置复制并粘贴到 Firepower 2100（设备模式）中。但是，您需要修改配置。另请注意平台之间的一些行为差异。

1. 要复制配置，请在 ASA 5500-X 上输入 **more system:running-config** 命令。
2. 根据需要编辑配置（请参阅下文）。
3. 连接至 Firepower 2100（设备模式）的控制台端口，然后进入全局配置模式：

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa# configure terminal
ciscoasa(config)#
```

4. 使用 **clear configure all** 命令清除当前配置。
5. 在 ASA CLI 上粘贴已修改的配置。

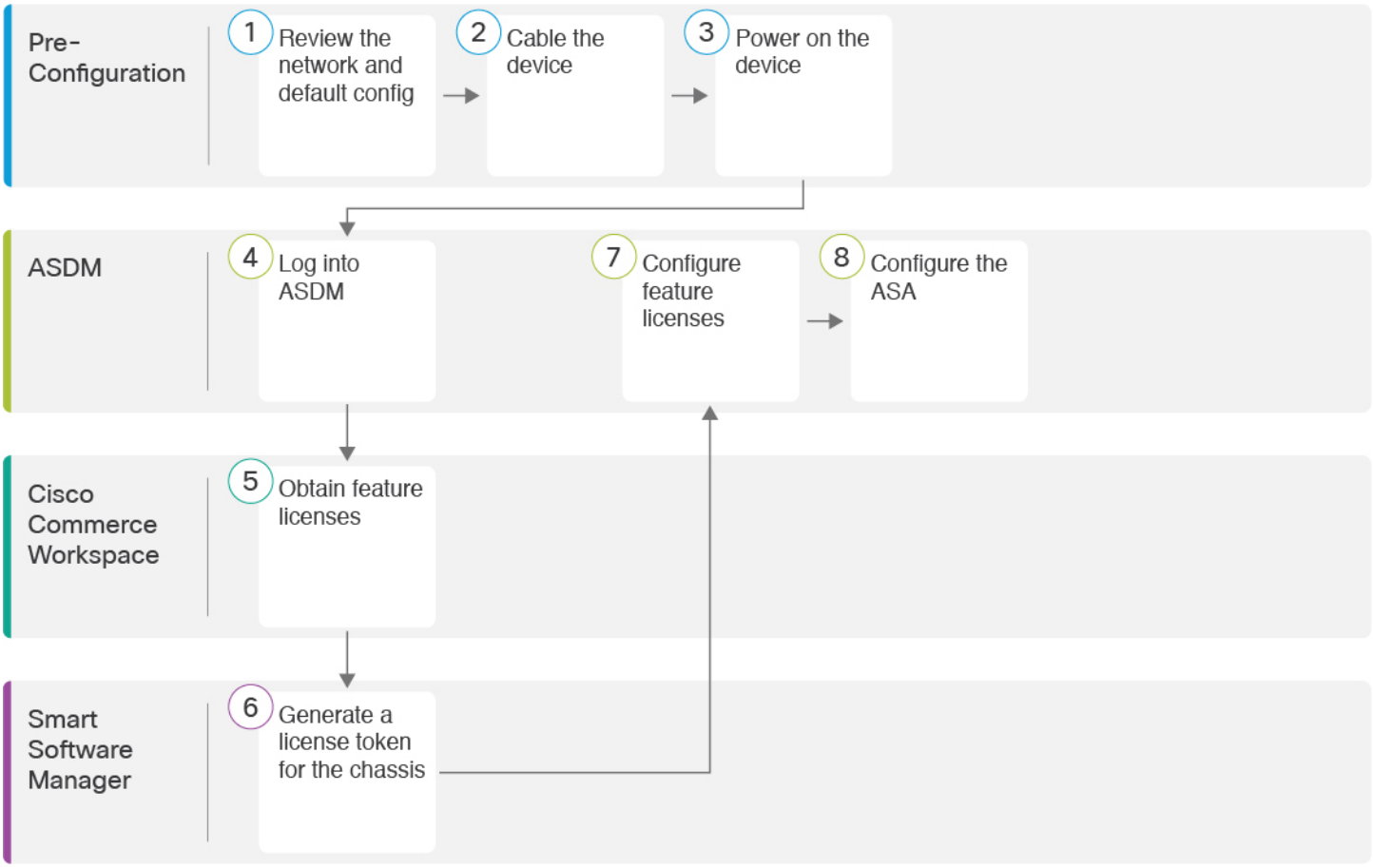
本指南假设采用出厂默认配置，因此，如果在现有配置下粘贴，则本指南中的某些程序将不适用于您的 ASA。

ASA 5500-X 配置	Firepower 2100（设备模式）配置
PAK 许可证	智能许可证 复制和粘贴配置时，不会应用 PAK 许可。默认情况下没有已安装的许可证。智能许可要求连接到智能许可服务器以获取许可证。智能许可还会影响 ASDM 或 SSH 访问（请参阅下文）。
初始 ASDM 访问	如果无法连接 ASDM 或向智能许可服务器注册，请删除任何 VPN 或其他强加密功能配置（即使仅配置了弱加密）。 您可以在获取强加密 (3DES) 许可证后重新启用这些功能。 此问题的原因是，ASA 默认情况下仅包含用于管理访问的 3DES 功能。如果启用强加密功能，则系统会阻止 ASDM 和 HTTPS 流量（例如，与智能许可服务器之间的流量）。此规则的例外是您连接到仅限管理的接口，例如管理 1/1。SSH 不受影响。
接口 ID	确保更改接口 ID 以便与新硬件 ID 匹配。例如，ASA 5525-X 包括管理 0/0 和千兆以太网 0/0 至 0/5。Firepower 1120 包括管理 1/1 和以太网 1/1 至 1/8。

ASA 5500-X 配置	Firepower 2100（设备模式）配置
boot system commands ASA 5500-X 最多允许四个 **boot system** 命令指定要使用的启动映像。	Firepower 2100（设备模式）仅允许一个 **boot system** 命令，因此在粘贴之前应删除多余的命令，只剩下一个命令。实际上在配置中不需要存在任何 **boot system** 命令，因为启动时不会读取它来确定启动映像。最后加载的启动图像将始终在重新加载时运行。 此 **boot system** 命令会在您输入时执行操作：系统验证并解压缩映像，并将其复制到引导位置（FXOS 管理的 disk0 上的内部位置）。重新加载 ASA 时，系统将加载新图像。

端到端程序

请参阅以下任务以在机箱上部署和配置 ASA。

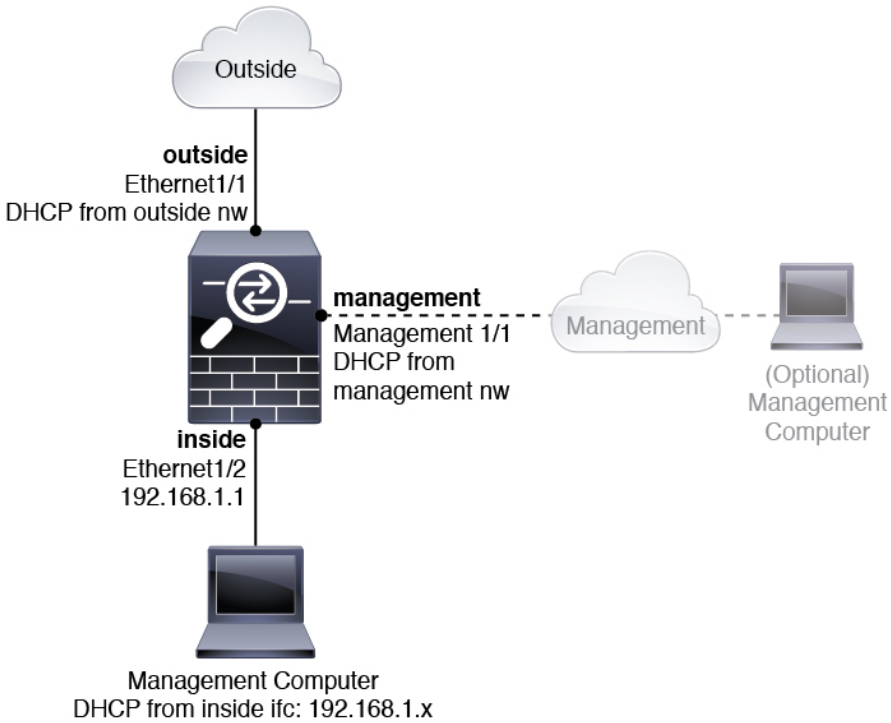


1	配置前准备工作	查看网络部署和默认配置， 第 5 页。

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	ASDM	登录 ASDM，第 8 页。
5	思科商务工作空间	配置许可，第 9 页：获取功能许可证。
6	智能软件管理器	配置许可，第 9 页：为机箱生成许可证令牌。
7	ASDM	配置许可，第 9 页：配置功能许可证。
8	ASDM	配置 ASA，第 14 页。

查看网络部署和默认配置

下图显示在 ASA 设备模式下使用默认配置的 Firepower 2100 的默认网络部署。



Firepower 2100 设备模式默认配置

默认情况下，Firepower 2100 在设备模式下运行。

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，则会保留平台模式。

设备模式下 Firepower 2100 的出厂默认配置包含以下配置：

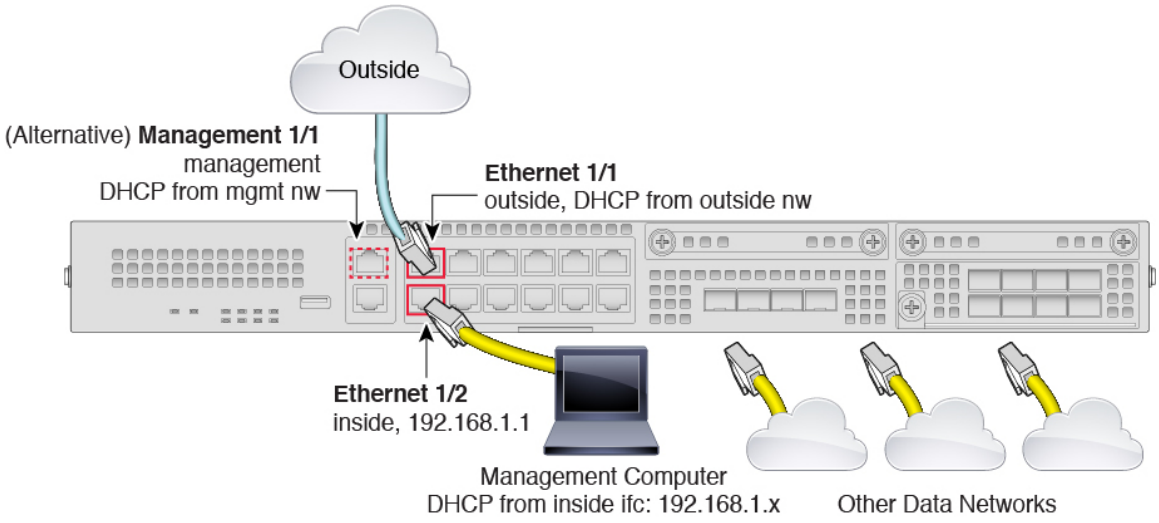
- **内部→外部流量** - 以太网 1/1（外部），以太网 1/2（内部）
- **外部 IP 地址**来自 DHCP，**内部 IP 地址**—192.168.1.1
- DHCP 中的**管理 IP 地址** - 管理 1/1（管理）
- **DHCP 服务器**在内部接口上
- **默认路由** 来自外部 DHCP，管理 DHCP
- **ASDM** 访问 - 允许管理和内部主机。内部主机限制为 192.168.1.0/24 网络。
- **NAT** - 从内部到外部所有流量的接口 PAT。
- **DNS** 服务器 - OpenDNS 服务器已预配置。

配置由以下命令组成：

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  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 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 management
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
```

```
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

连接设备电缆



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：

- 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 ASA 的 IP 地址，以便可以从管理计算机连接到 IP 地址。
- 以太网 1/2 - 将管理计算机直接连接至以太网 1/2 以进行初始配置。或者将以太网 1/2 连接到内部网络；请确保管理计算机位于内部网络上，因为只有该网络上的客户端才能访问 ASA。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Firepower 2100 设备模式默认配置，第 6 页）。

可以稍后从其他接口配置 ASA 管理访问；请参阅 ASA 常规操作配置指南。

步骤 2 将外部网络连接至以太网 1/1 接口（标记为 WAN）。

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 3 将其他网络连接到其余接口。

接通设备电源

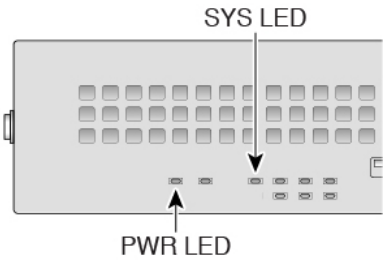
系统电源由位于设备后部的摇杆电源开关控制。电源开关以软通知开关形式实施，支持平稳地关闭系统以降低系统软件及数据损坏的风险。

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。

登录 ASDM

启动 ASDM 以便配置 ASA。

ASA 默认情况下包含 3DES 功能，仅用于管理访问，因此您可以连接到许可证颁发机构，还可以立即使用 ASDM。如果之后在 ASA 上配置了 SSH 访问，也可以使用 SSH 和 SCP。其他需要强加密（例如 VPN）的功能必须启用强加密许可证，这要求您先向许可证颁发机构注册。

注释 如果您在拥有许可证之前尝试配置任何可使用强加密的功能（即使您仅配置了弱加密），您的HTTPS 连接会在该接口上断开，并且您无法重新连接。此规则的例外是您连接到仅限管理的接口，例如管理 1/1。SSH 不受影响。如果您丢失 HTTPS 连接，可以连接到控制台端口以重新配置 ASA、连接到仅管理接口，或者连接到没有为强加密功能配置的接口。

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 在浏览器中输入以下 URL：

- **https://192.168.1.1** - 内部（以太网 1/2）接口 IP 地址。
- **https://***management_ip* - 从 DHCP 分配的管理接口 IP 地址。

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 将用户名和密码字段留空 时设置的启用密码，然后单击**确定**。

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。

ASA 默认情况下包含 3DES 功能，仅用于管理访问，因此您可以连接到许可证颁发机构，还可以立即使用 ASDM。如果之后在 ASA 上配置了 SSH 访问，也可以使用 SSH 和 SCP。其他需要强加密（例如 VPN）的功能必须启用强加密许可证，这要求您先向许可证颁发机构注册。

注释 如果您在拥有许可证之前尝试配置任何可使用强加密的功能（即使您仅配置了弱加密），您的HTTPS连接会在该接口上断开，并且您无法重新连接。此规则的例外是您连接到仅限管理的接口，例如管理 1/1。SSH 不受影响。如果您丢失 HTTPS 连接，可以连接到控制台端口以重新配置 ASA、连接到仅管理接口，或者连接到没有为强加密功能配置的接口。

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 functionaility 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。

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。

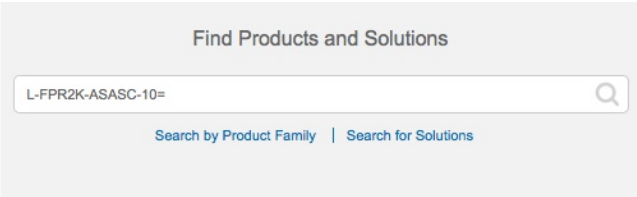
- 您的思科智能软件许可帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

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 *1:* 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。

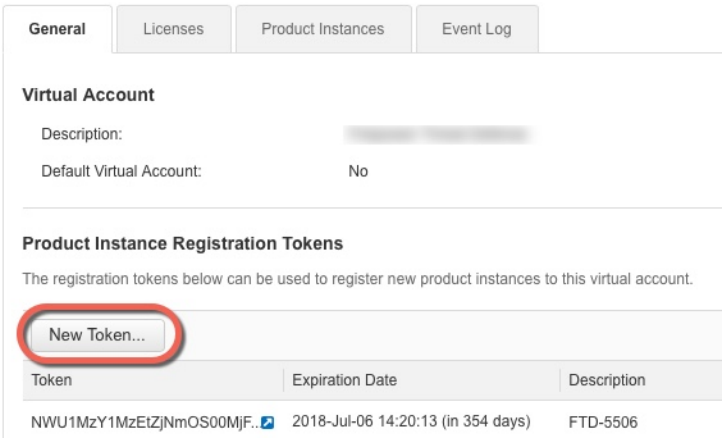
- 强加密 (3DES/AES) 许可证 - L-FPR2K-ENC-K9=。此许可证是免费的。虽然通常不需要此许可证（例如，使用 2.3.0 以前版本的较旧卫星服务器的 ASA 需要此许可证），但您仍应将其添加到您的帐户中以进行跟踪。

- 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。

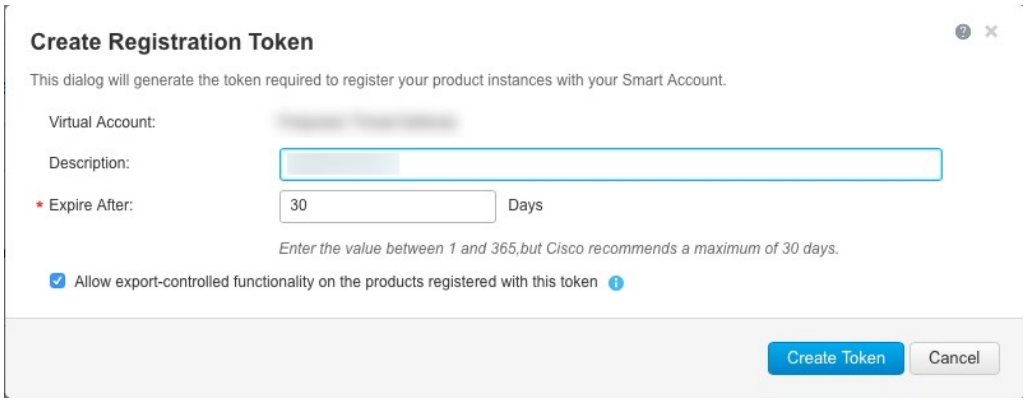
步骤 2 在 Cisco Smart Software Manager 中，为要将此设备添加到的虚拟帐户请求并复制注册令牌。

a) 单击 **Inventory**。

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



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** - 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 *2:* 查看令牌

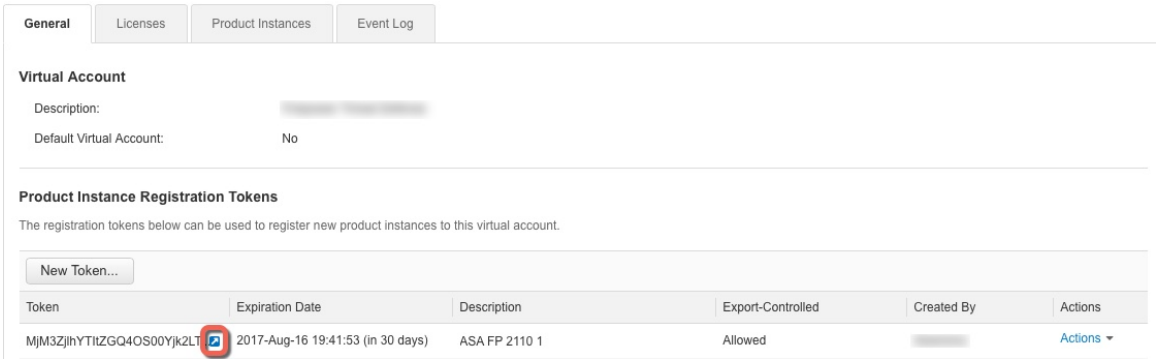
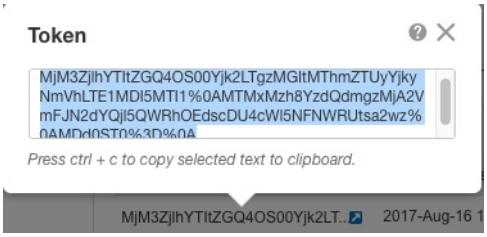
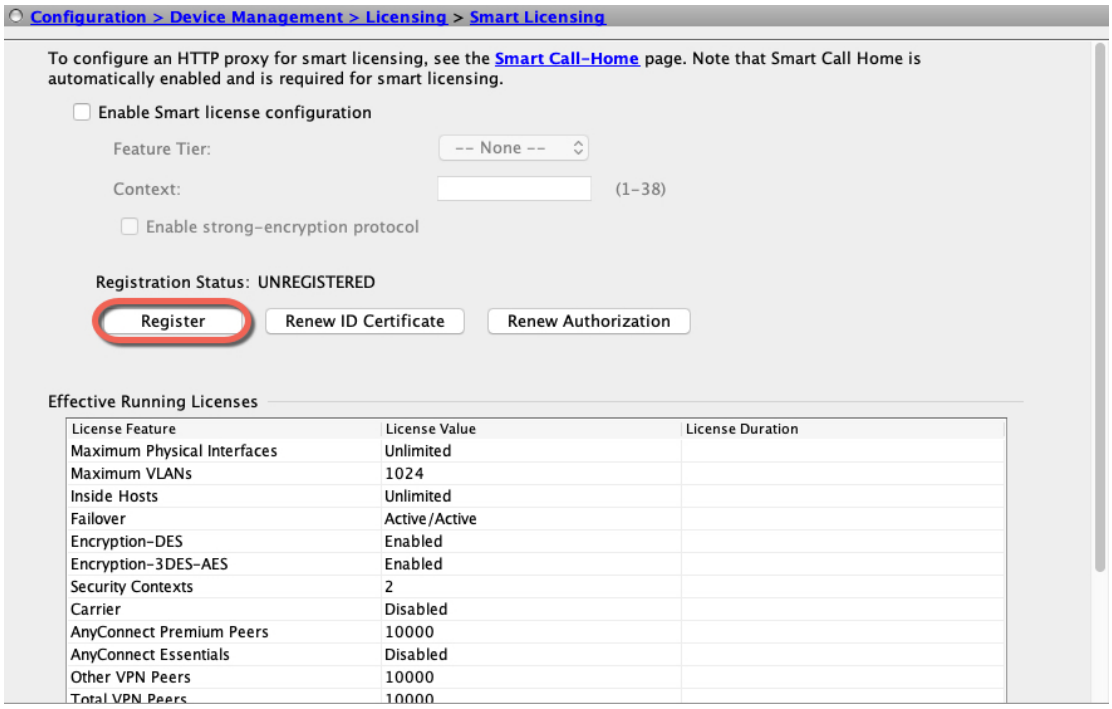


图 *3:* 复制令牌

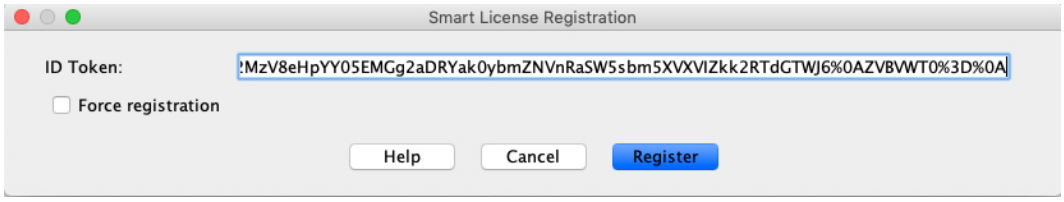


步骤 3 在 ASDM 中，依次选择 **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**。

步骤 4 单击 **Register**。



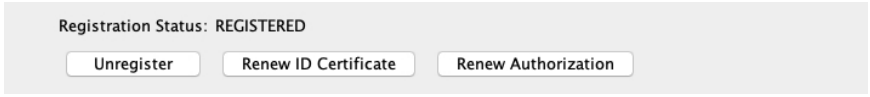
步骤 5 在 **ID Token** 字段中输入注册令牌。



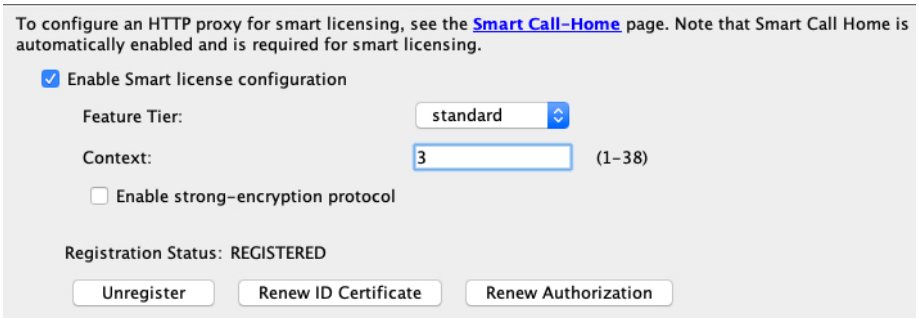
您可以勾选 **Force registration** 复选框，注册已注册但可能与许可证颁发机构不同步的 ASA。例如，如果从智能软件管理器中意外删除了 ASA，请使用 **Force registration**。

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：



a) 选中 **Enable Smart license configuration**。

b) 从 **Feature Tier** 下拉列表中，选择 **Standard**。

仅标准层可用。

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 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。

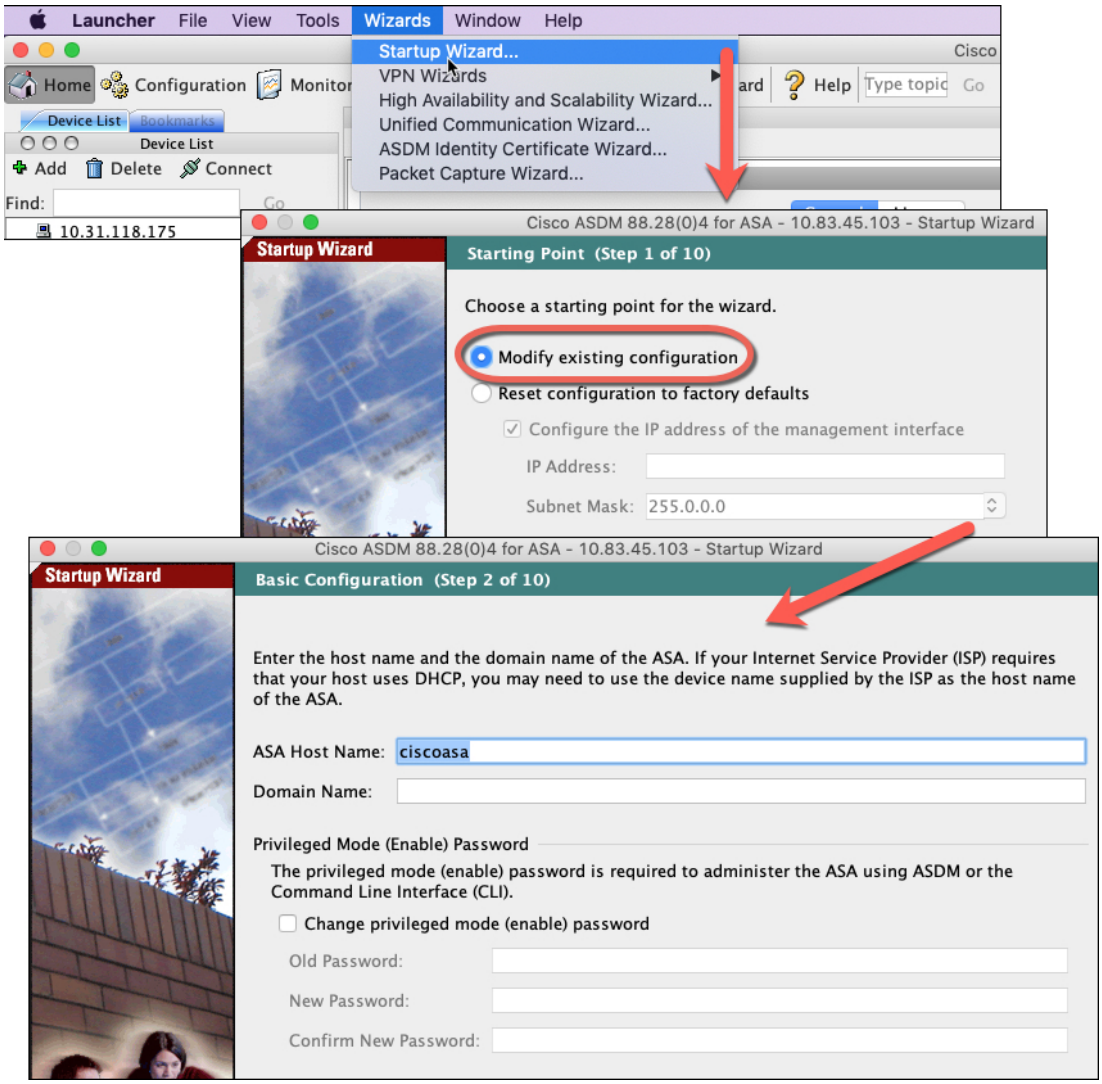
当您更改许可证时，您需要重新启动 ASDM 才能显示更新屏幕。

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。

访问 ASA 和 FXOS CLI

您可以使用 ASA CLI（而非 ASDM）对 ASA 进行故障排除或配置。可以连接到控制台端口以访问 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。

也可以从 ASA CLI 访问 FXOS CLI，以便进行故障排除。

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。

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#
```

如果 ASA 无法启动，并且您进入 FXOS 故障保护模式，则您在 ASA 上设置的启用密码也是 FXOS **管理员**用户密码。

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)#
```

可从全局配置模式开始配置 ASA。要退出全局配置模式，请输入 **exit**、**quit** 或 **end** 命令。

步骤 4 （可选） 连接到 FXOS CLI。

connect fxos [**admin**]

- **admin**- 提供管理员级的访问权限。如果不选择此选项，用户将拥有只读访问权限。请注意，即使在管理员模式下，也没有任何配置命令可用。

系统不会提示您提供用户凭证。当前的 ASA 用户名将传递给 FXOS，无需其他登录。要返回到 ASA CLI，请输入 **exit** 或键入 **Ctrl-Shift-6**、**x**。

在 FXOS 中，您可以使用 **scope security/show audit-logs** 命令查看用户活动。

示例：

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

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。
- 有关故障排除，请参阅《 FXOS 故障排除指南》 。