



使用 ASDM 部署 ASA

本章对您适用吗？

要查看所有可用的操作系统和管理器，请参阅[哪种应用和管理器适合您？](#)。本章适用于使用 ASDM 的 ASA。

关于防火墙

硬件可以运行威胁防御软件或 ASA 软件。在威胁防御和 ASA 之间切换需要您对设备进行重新映像。如果您需要不同于当前安装的软件版本，则还应重新映像。请参阅[Cisco Secure Firewall ASA 和 Secure Firewall Threat Defense 重新映像指南](#)。

防火墙会运行被称为 Secure Firewall eXtensible 操作系统 (FXOS) 的底层操作系统。防火墙不支持 FXOS Cisco Secure Firewall 机箱管理器；出于故障排除目的，仅支持受限的 CLI。有关详细信息，请参阅[适用于具备 Firepower 威胁防御的 Firepower 1000/2100 和 Cisco Secure Firewall 3100/4200 的思科 FXOS 故障排除指南](#)。

隐私收集声明 - 防火墙不要求或主动收集个人身份信息。但是，您可以在配置中使用个人身份信息，例如用户名。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 1 页](#)
- [端到端任务，第 3 页](#)
- [查看网络部署和默认配置，第 5 页](#)
- [连接防火墙的电缆，第 7 页](#)
- [打开防火墙电源，第 8 页](#)
- [（可选）更改 IP 地址，第 9 页](#)
- [登录 ASDM，第 10 页](#)
- [配置许可，第 11 页](#)
- [配置 ASA，第 16 页](#)
- [访问 ASA 和 FXOS CLI，第 18 页](#)
- [后续步骤，第 19 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。

迁移 ASA 5500-X 配置

您可以将 ASA 5500-X 配置复制并粘贴到 Cisco Secure Firewall 4200 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 Cisco Secure Firewall 4200 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。

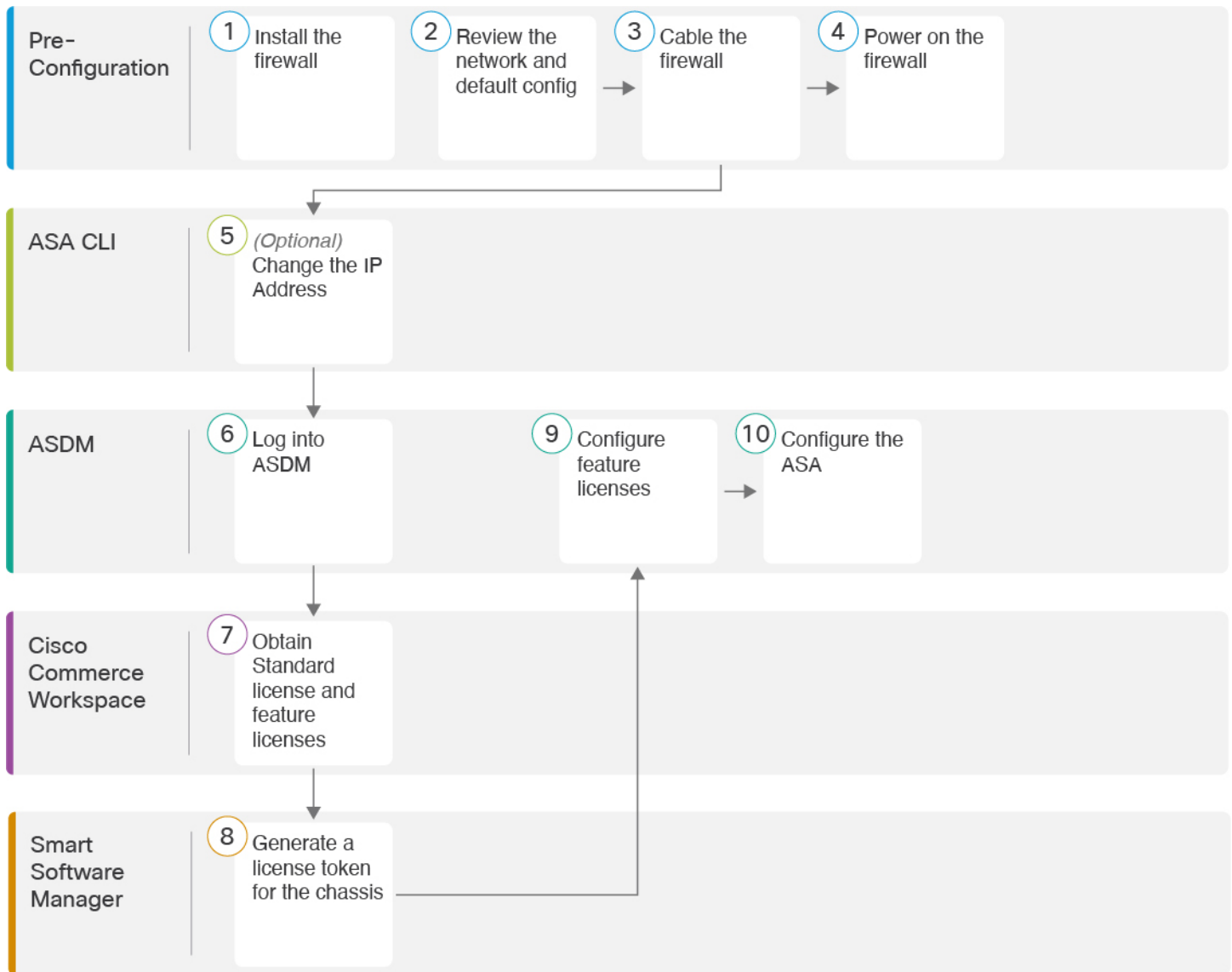
| ASA 5500-X 配置 | Cisco Secure Firewall 4200 配置 |
|---------------|--|
| PAK 许可证 | 智能许可证 复制和粘贴配置时，不会应用 PAK 许可。默认情况下没有已安装的许可证。智能许可要求连接到智能许可服务器以获取许可证。智能许可还会影响 ASDM 或 SSH 访问（请参阅下文）。 |
| 初始 ASDM 访问 | 如果无法连接 ASDM 或向智能许可服务器注册，请删除任何 VPN 或其他强加密功能配置（即使仅配置了弱加密）。 您可以在获取强加密 (3DES) 许可证后重新启用这些功能。 此问题的原因是，ASA 默认情况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 | Cisco Secure Firewall 4200 配置 |
|--|--|
| <p>boot system commands</p> <p>ASA 5500-X 最多允许四个 boot system 命令指定要使用的启动映像。</p> | <p>Cisco Secure Firewall 4200 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。</p> <p>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。</p> |

端到端任务

请参阅以下任务以在机箱上部署和配置 ASA。

图 1: 端到端任务



| | | |
|---|---------|---------------------------------------|
| ① | 配置前准备工作 | 安装防火墙。请参阅 硬件安装指南 。 |
| ② | 配置前准备工作 | 查看网络部署和默认配置 ，第 5 页。 |
| ③ | 配置前准备工作 | 连接防火墙的电缆 ，第 7 页。 |
| ④ | 配置前准备工作 | 打开防火墙电源 ，第 8 页。 |
| ⑤ | ASA CLI | (可选) 更改 IP 地址 ，第 9 页。 |

| | | |
|----|--------------------------|--------------------------------|
| 6 | ASDM | 登录 ASDM，第 10 页。 |
| 7 | Cisco Commerce Workspace | 获取标准许可证和可选功能许可证 (配置许可，第 11 页)。 |
| 8 | 智能软件管理器 | 为机箱生成许可证令牌 (配置许可，第 11 页)。 |
| 9 | ASDM | 配置功能许可证 (配置许可，第 11 页)。 |
| 10 | ASDM | 配置 ASA，第 16 页。 |

查看网络部署和默认配置

下图显示在 ASA 设备模式。

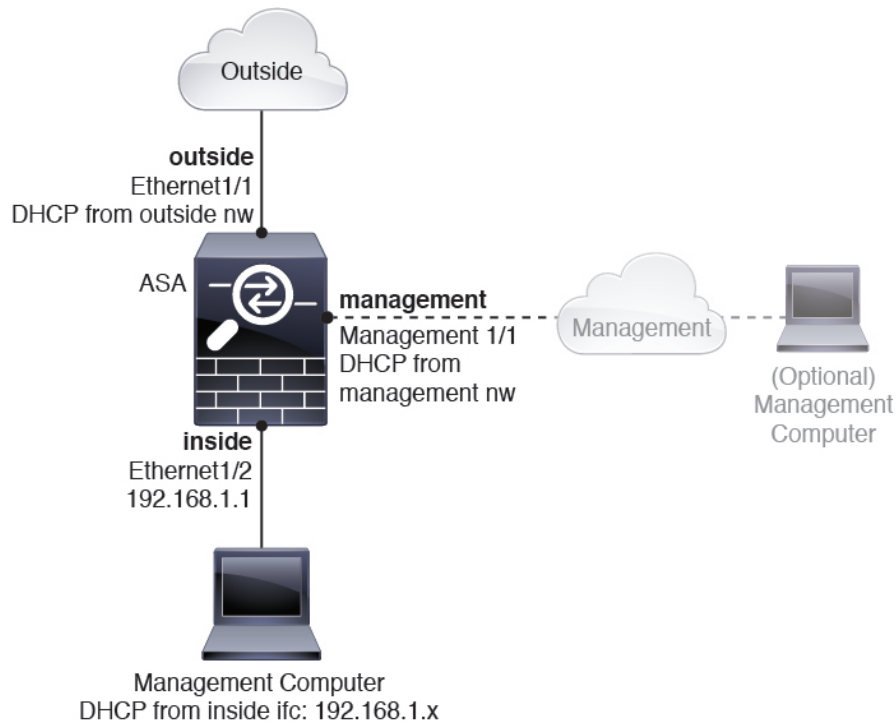
如果您将外部接口直接连接到电缆调制解调器或 DSL 调制解调器，我们建议您将调制解调器置于桥接模式，以便 ASA 为您的内部网络执行所有路由和 NAT。如果您需要为外部接口配置 PPPoE 以连接到您的 ISP，可以在 ASDM 启动向导中执行此操作。



注释 如果不能使用默认管理 IP 地址进行 ASDM 访问，可以在 ASA CLI 上设置管理 IP 地址。请参阅 [\(可选\) 更改 IP 地址，第 9 页](#)。

如果您需要更改内部 IP 地址，可以使用 ASDM 启动向导执行此操作。例如，在以下情况下，您可能需要更改内部 IP 地址：

- 如果外部接口尝试获取 192.168.1.0 网络（这是一个通用默认网络）上的 IP 地址，DHCP 租用将失败，外部接口不会获得 IP 地址。出现此问题的原因在于 ASA 在同一网络上不能有两个接口。在这种情况下，您必须将内部 IP 地址更改到新网络上。
- 如果将 ASA 添加到现有内部网络中，需要将内部 IP 地址更改到现有网络上。



安全防火墙4200默认配置

Cisco Secure Firewall 4200 的默认出厂配置用于配置以下内容：

- 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
- 管理—管理 1/1（管理），IP 地址来自 DHCP
- **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
!
```

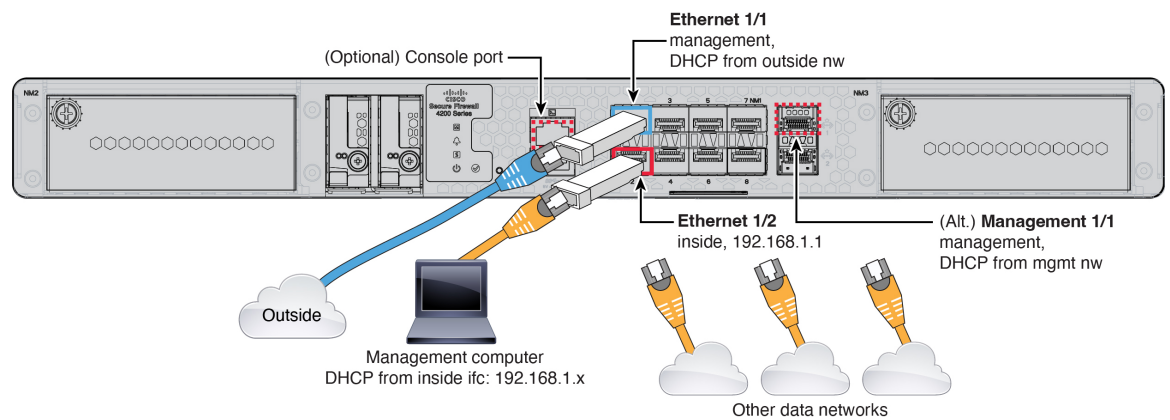
```

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 inside
!
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
!

```

连接防火墙的电

图 2: 布线 Cisco Secure Firewall 4200



在管理 1/1 或以太网 1/2 上管理 Cisco Secure Firewall 4200。默认配置还会将以太网 1/1 配置为外部接口。

开始之前

- 将 SFP 安装到数据接口和可选管理端口 - 内置端口是需要 SFP 模块的 1/10/25-Gb SFP 端口。

- (可选) 获取控制台电缆-默认情况下, 防火墙不随附控制台电缆, 因此您需要购买第三方 USB 转 RJ-45 串行电缆。

过程

步骤 1 安装机箱。请参阅[硬件安装指南](#)。

步骤 2 将您的管理计算机连接至以下任一接口:

- **Ethernet 1/2**—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 [安全防火墙4200默认配置, 第 6 页](#))。只有 192.168.1.0/24 上的客户端可以访问 ASA。

如果需要将以太网 1/2 IP 地址从默认值更改为其他值, 还必须将管理计算机连接至控制台端口。请参阅 [\(可选\) 更改 IP 地址, 第 9 页](#)。

- **Management 1/1**—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。

如果需要其他管理接口, 可以稍后设置管理 1/2。

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 3 将外部网络连接至以太网 1/1 接口。

对于智能软件许可, ASA 需要访问互联网。

步骤 4 将其他网络连接到其余接口。

打开防火墙电源

系统电源由位于防火墙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。

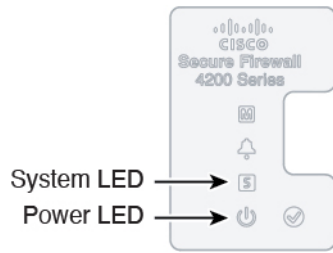
过程

步骤 1 将电源线一端连接到防火墙, 另一端连接到电源插座。

步骤 2 使用位于机箱背面电源线旁边的标准摇杆型电源开关打开电源。

步骤 3 检查防火墙背面的电源 LED; 如果该 LED 呈绿色稳定亮起, 表示防火墙已接通电源。

图 3: 系统和电源 LED



步骤 4 检查防火墙背面的系统 LED；其呈绿色稳定亮起之后，系统已通过通电诊断。

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，机箱前面的电源 LED 将闪烁绿色。在电源 LED 完全关闭之前，请勿拔出电源。

(可选) 更改 IP 地址

如果不能使用默认 IP 地址进行 ASDM 访问，可以在 ASA CLI 上设置 inside 接口的 IP 地址。



注释 此程序恢复默认配置并设置您选择的 IP 地址，所以如果有任何要保留的 ASA 配置更改，请不要使用此程序。

过程

步骤 1 连接到 ASA 控制台端口，然后进入全局配置模式。有关详细信息，请参阅[访问ASA和FXOS CLI](#)，第 18 页。

步骤 2 恢复默认配置和您选择的 IP 地址。

configure factory-default [*ip_address* [*mask*]]

示例:

```
ciscoasa(config)# configure factory-default 10.1.1.151 255.255.255.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256
```

```
WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.
```

```
Begin to apply factory-default configuration:
Clear all configuration
Executing command: interface ethernet1/2
```

```

Executing command: nameif inside
INFO: Security level for "inside" set to 100 by default.
Executing command: ip address 10.1.1.151 255.255.255.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.1.1.0 255.255.255.0 management
Executing command: dhcpd address 10.1.1.152-10.1.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#

```

步骤 3 将默认配置保存到闪存。

write memory

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，因此您可以连接到智能软件管理器，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，这要求您先向智能软件管理器注册。



注释 如果您在注册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。如果您丢失了 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。

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 **安装 ASDM 启动程序**。

步骤 3 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，然后点击**确定 (OK)**。

系统将显示 ASDM 主窗口。

配置许可

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

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

ASA 默认情况下包含 3DES 功能，仅用于管理访问，因此您可以连接到智能软件管理器，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，这要求您先向智能软件管理器注册。



注释 如果您在注册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。如果您丢失了 HTTPS 连接，可以连接到控制台端口以重新配置 ASA、连接到仅限管理接口，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。

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。

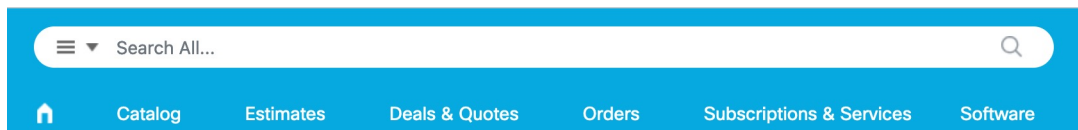
- 您的智能软件管理器帐户必须符合强加密 (3DES/AES) 许可证的要求，才能使用某些功能（已使用导出合规性标志启用）。

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。

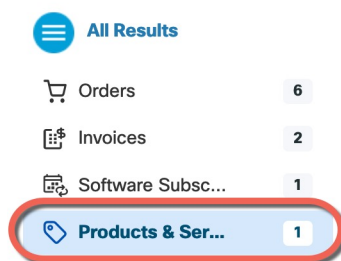
当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。但是，如果您需要自己添加许可证，则请使用 [思科商务工作空间](#) 上的 **搜索全部 (Search All)** 字段。

图 4: 许可证搜索



从结果中选择 **产品和服务 (Products & Services)**。

图 5: 成果



搜索以下许可证 PID:

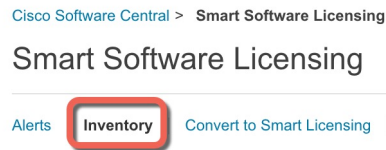
注释 如果未找到 PID，您可以手动将 PID 添加到订单中。

- 基础许可证 — L-FPR4215-BSE=。基础许可证是必需的许可证。
- 基础许可证 — L-FPR4225-BSE=。基础许可证是必需的许可证。
- 基础许可证 — L-FPR4245-BSE=。基础许可证是必需的许可证。

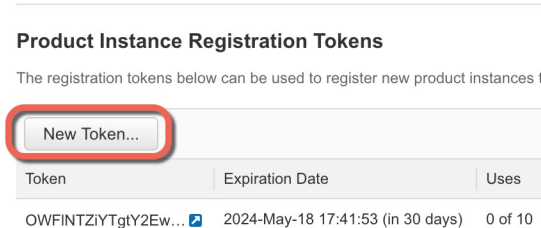
- 5 情景许可证 - L-FPR4200-ASASC-5=。情景许可证是附加的；请购买多份许可证以满足您的需要。
- 10 情景许可证 - L-FPR4200-ASASC-10=。情景许可证是附加的；请购买多份许可证以满足您的需要。
- 运营商 (Diameter, GTP/GPRS, M3UA, SCTP)—L-FPR4200-ASA-CAR=
- 强加密 (3DES/AES) 许可证 - L-FPR4200-ENC-K9=。仅当帐户未获授权使用强加密时需要。
- Cisco Secure 客户端 - 请参阅[思科安全客户端订购指南](#)。您不能直接在 ASA 中启用此许可证。

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**清单 (Inventory)**。



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



c) 在 **Create Registration Token** 对话框中，输入以下设置，然后点击 **Create Token**：

Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account: XXXXXXXXXX

Description:

* Expire After: Days
Between 1 - 365, 30 days recommended

Max. Number of Uses:

The token will be expired when either the expiration or the maximum uses is reached

Allow export-controlled functionality on the products registered with this token ⓘ

- **Description**
- **Expire After** - 思科建议该时间为 30 天。

- 最大使用次数
- **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清单中。

- 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 6: 查看令牌

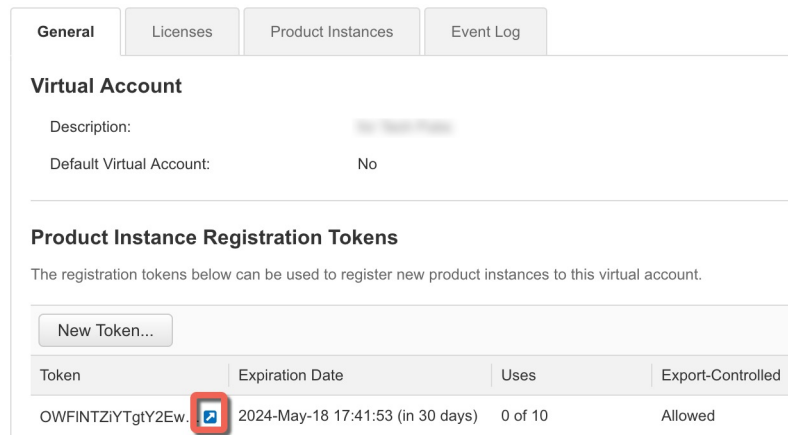
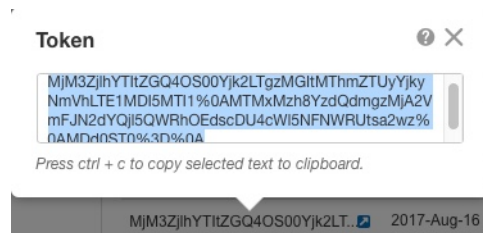


图 7: 复制令牌



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

步骤 4 点击 **Register**。

Configuration > Device Management > Licensing > Smart Licensing

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:

Throughput Level:

Privacy Host Name Version

Transport Call Home Smart Transport

Configure Transport URL

Default URL

Registration

Utility

Proxy URL

Proxy Port

Configure Utility Mode

Enable Standard Utility Mode

Custom ID

Customer Company Identifier

Customer Company Name

Customer Street

Customer City

Customer State

Customer Country

Customer Postal Code

Registration Status: UNREGISTERED

Effective Running Licenses

| License Feature | License Value |
|---------------------|---------------|
| Maximum VLANs | 200 |
| Inside Hosts | Unlimited |
| Failover | Active/Active |
| Encryption-DES | Enabled |
| Encryption-3DES-AES | Enabled |
| Security Contexts | 2 |
| Carrier | Disabled |

步骤 5 在 **ID Token** 字段中输入注册令牌。

Smart License Registration

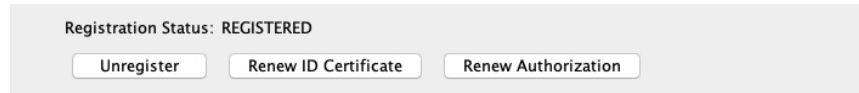
ID Token:

Force registration

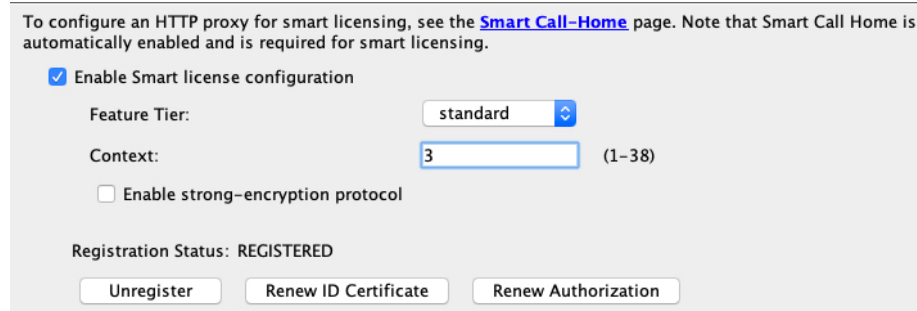
您可以勾选强制注册 (**Force registration**) 复选框，注册已注册但可能与智能软件管理器不同步的 ASA。例如，如果从智能软件管理器中意外删除了 ASA，请使用强制注册 (**Force registration**)。

步骤 6 点击 **Register**。

ASA 使用预先配置的外部接口向智能软件管理器注册，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，则智能软件管理器还会应用强加密(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**监控 (Monitoring) > 属性 (Properties) > 智能许可证 (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。
 - Cisco Secure Firewall 4200 - 100 个情景

例如，对于 Cisco Secure Firewall 4215 而言，要使用最大值 - 100 种情景，请为情景数输入 98；此值将与默认值 2 相加。

步骤 8 点击 **Apply**。

步骤 9 点击工具栏中的 **Save** 图标。

步骤 10 退出并重新启动 ASDM。

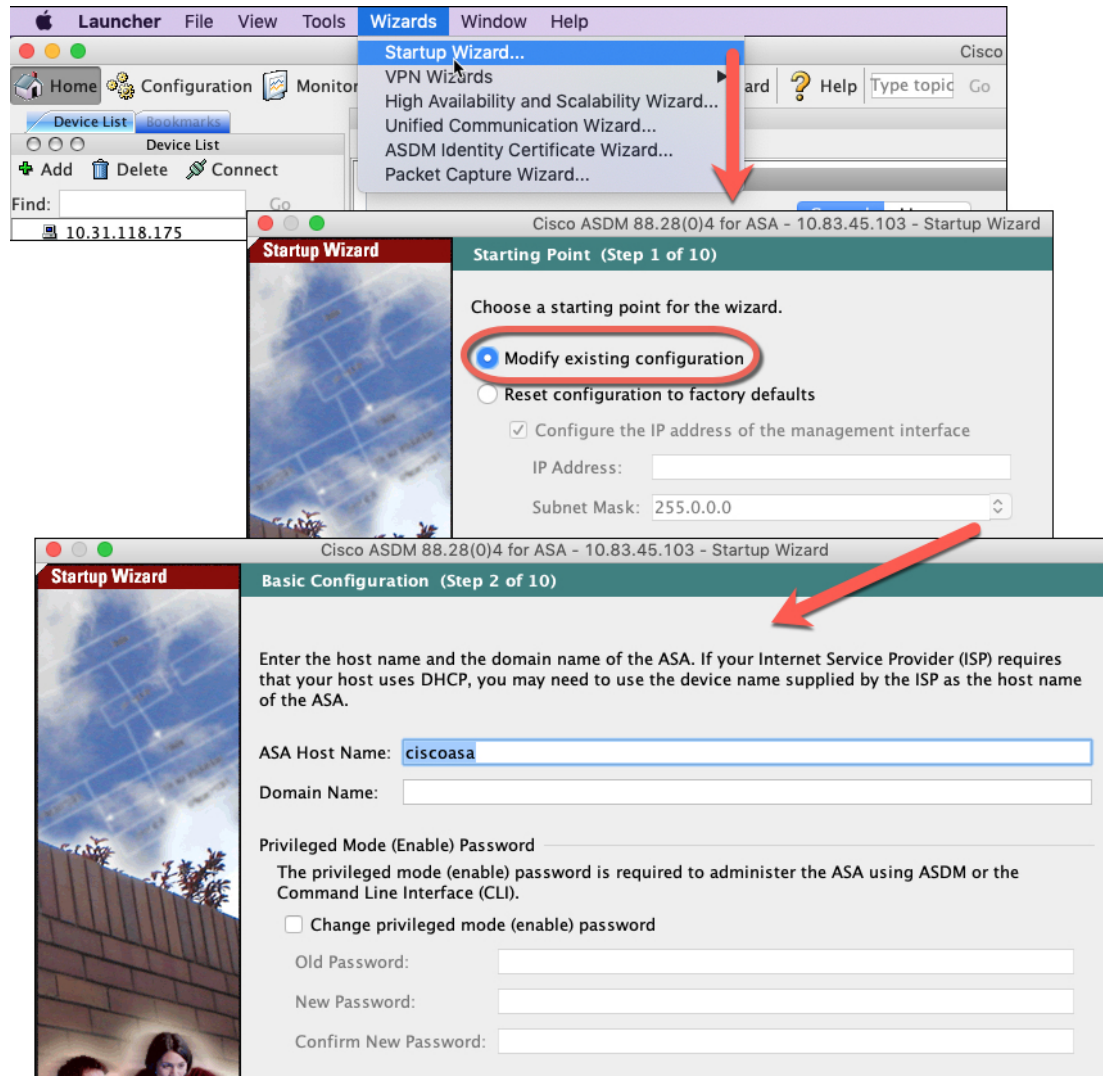
当您更改许可证时，您需要重新启动 ASDM 才能显示更新屏幕。

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 依次选择向导 (Wizards) > 启动向导 (Startup Wizard)，然后点击修改现有配置 (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。您可以稍后在任何接口上配置对 ASA 的 SSH 访问；在默认情况下，SSH 访问是禁用的。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。确保为操作系统安装任何必要的串行驱动程序。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 EXEC 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](#)》。

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。