



Cisco Secure Firewall 3100 ASA 入门

上次修改日期: 2025 年 3 月 19 日

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



第 1 章

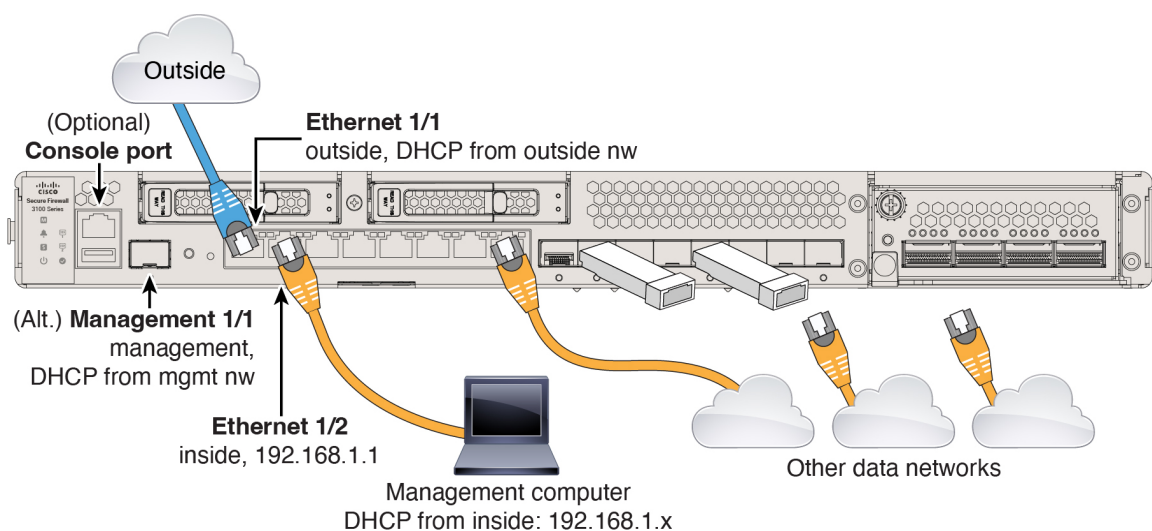
准备工作

使用 ASDM 来配置 ASA。

- 连接防火墙的电缆，第 1 页
- 打开防火墙电源，第 2 页
- 安装的哪个应用程序：威胁防御还是 ASA？，第 2 页
- 访问 ASA CLI，第 3 页
- 获取许可证，第 5 页

连接防火墙的电缆

- （可选）获取控制台适配器 - 防火墙配有一条 DB-9 转 RJ-45 串行电缆，所以您需要购买第三方 DB-9-to-USB 串行电缆进行连接。
- 将 SFP/SFP+ 模块安装到以太网 1/9 及以上端口。
- 有关详细信息，请参阅[硬件安装指南](#)。



打开防火墙电源

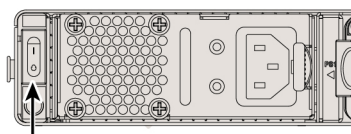
系统电源由位于防火墙后部的摇杆电源开关控制。摇杆电源开关提供软通知，支持平稳地关闭系统以降低系统软件及数据损坏的风险。

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摇杆电源开关打开电源。

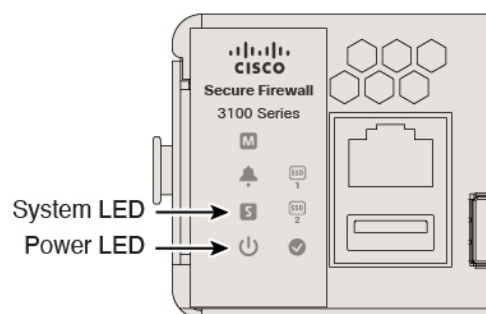
图 1: 电源按钮



Power button

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 2: 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。

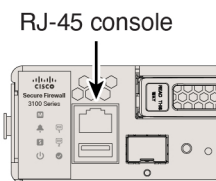
安装的哪个应用程序：威胁防御还是 ASA？

硬件上支持威胁防御或 ASA 两种应用。连接到控制台端口，并确定出厂时安装的应用。

过程

步骤 1 连接到控制台端口。

图 3: 控制台端口



步骤 2 请参阅 CLI 提示，确定防火墙运行的是威胁防御还是 ASA。

威胁防御

您会看到 Firepower 登录 (FXOS) 提示。您无需登录和设置新密码即可断开连接。

```
firepower login:
```

ASA

您将看到 ASA 提示。

```
ciscoasa>
```

步骤 3 如果您运行的是错误的应用，请参阅[Cisco Secure Firewall ASA](#) 和 [Secure Firewall Threat Defense 重新映像指南](#)。

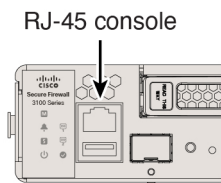
访问ASA CLI

您可能需要访问 CLI 进行配置或故障排除。

过程

步骤 1 连接到控制台端口。

图 4: 控制台端口



步骤 2 在用户 EXEC 模式下连接到 ASA CLI。此模式允许您使用许多 **show** 命令。

```
ciscoasa>
```

步骤 3 访问特权 EXEC 模式。在此受密码保护的模式下，您可以执行许多操作，包括访问配置模式。

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#
```

步骤 4 访问全局配置模式。

configure terminal

示例：

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

步骤 5 访问 FXOS CLI。使用此 CLI 在硬件级别进行故障排除。

connect fxos [admin]

- **admin**- 提供管理员级的访问权限。如果不选择此选项，您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**。

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#
```

获取许可证

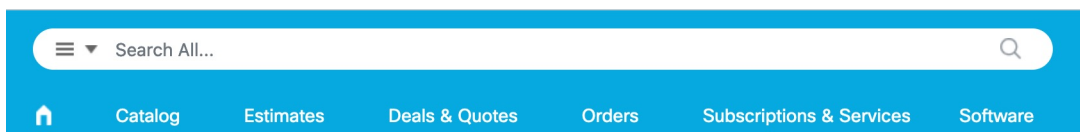
当您从思科或经销商那里购买设备时，您的许可证应该已链接到您的智能软件许可证帐户。如果您没有[智能软件管理器](#)帐户，请点击链接[建立新账户](#)。

ASA 具有以下许可证：

- 基础版 — 必需
- 安全情景
- 运营商 - Diameter、GTP/GPRS、M3UA、SCTP
- Cisco Secure Client

1. 如果您需要自己添加许可证，请前往[思科商务工作空间](#)并使用[搜索全部 \(Search All\)](#) 字段。

图 5: 许可证搜索



2. 搜索以下许可证 PID。

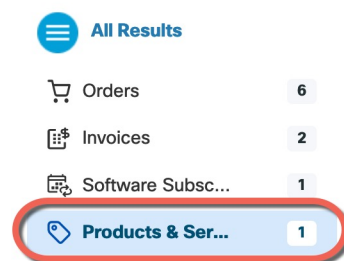


注释 如果未找到 PID，您可以手动将 PID 添加到订单中。

- 基础—自动包含。
- 5 情景—L-FPR3K-ASASC-5=。情景许可证是累加的，可购买多个许可证。
- 10 情景—L-FPR3K-ASASC-10=。情景许可证是累加的，可购买多个许可证。
- 运营商 (Diameter, GTP/GPRS, M3UA, SCTP) — L-FPR3K-ASA-CAR=
- Cisco Secure 客户端 — 请参阅 [Cisco Secure 客户端订购指南](#)。您不能直接在 ASA 中启用此许可证。

3. 从结果中选择产品和服务 (Products & Services)。

图 6: 结果



All Results	
Orders	6
Invoices	2
Software Subsc...	1
Products & Ser...	1



第 2 章

配置基本策略

使用 ASDM 向导来配置许可并添加到默认配置中。

- (可选) 更改 IP 地址，第 7 页
- 登录 ASDM，第 8 页
- 配置许可，第 9 页
- 使用启动向导配置 ASA，第 12 页

(可选) 更改 IP 地址

默认情况下，您可以从以下界面启动 ASDM:

- 以太网 1/2 - 192.168.1.1
- 管理 1/1 - DHCP 的 IP 地址

如果不能使用默认 IP 地址，则可以在 ASA CLI 上设置以太网 1/2 接口的 IP 地址。

过程

步骤 1 连接到控制台端口并访问全局配置模式。请参阅[访问ASA CLI](#)，第 3 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。

过程

步骤 1 在浏览器中输入以下 URL 之一。

- **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 1/1 接口 IP 地址。

注释

请务必指定 **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

将防火墙注册到智能软件管理器。

开始之前

根据[获取许可证](#)，第 5 页为防火墙获取许可证。

过程

步骤 1 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**)。

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

Alerts **Inventory** Convert to Smart Licensing |

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

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances t

New Token...

Token	Expiration Date	Uses
OWFINTZiYtGtY2Ew...	2024-May-18 17:41:53 (in 30 days)	0 of 10

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:

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 ⓘ

Create Token Cancel

• 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 7: 查看令牌

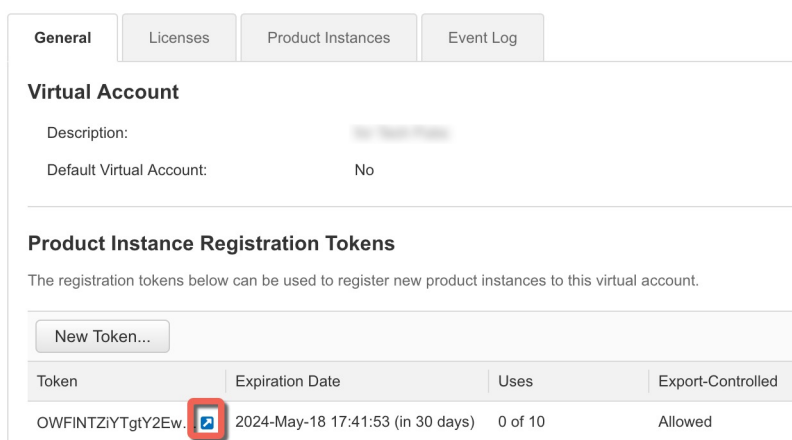
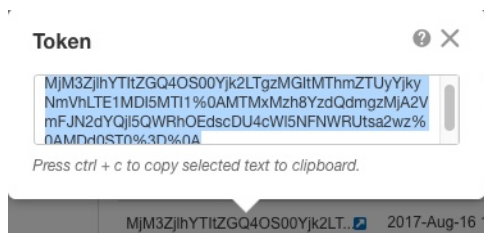


图 8: 复制令牌



步骤 2 在 ASDM 中，依次选择配置 (Configuration) > 设备管理器 (Device Management) > 许可 (Licensing) > 智能许可 (Smart Licensing)。

步骤 3 设置许可授权。

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

仅基础层可用。

- (可选) 如果使用的是情景许可证，则输入情景的数量。

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：

- Cisco Secure Firewall 3100 — 100 个情景

例如，对于 Cisco Secure Firewall 3110 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。

- d) （可选）选中启用运营商 (**Enable Carrier**) 以进行 Diameter、GTP/GPRS、SCTP 检查。
- e) 点击应用。
- f) 点击工具栏中的 **Save** 图标。

步骤 4 点击 **Register**。

Configuration > Device Management > Licensing > Smart Licensing

To configure an HTTP proxy for Smart Licensing using Call Home, go to [Smart Call-Home](#). If you are using Smart Transport, configure

☒ Enable Smart license configuration

Feature Tier: Essentials

Context: 3

☐ Enable strong-encryption protocol

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide

Transport ☐ Call Home ☒ Smart Transport

Configure Transport URL

☒ Default ☐ Custom URL

Registration

Proxy URL

Proxy Port

Registration Status:

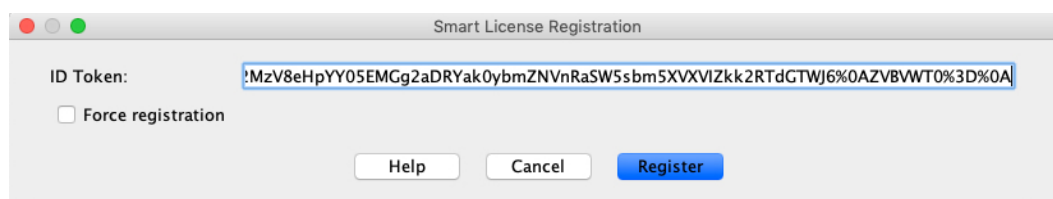
Register Renew ID Certificate Renew Authorization

Effective Running Licenses

License Feature	License Value	License Duration
Maximum Physical Interfaces	Unlimited	
Maximum VLANs	512	
Inside Hosts	Unlimited	
Failover	Active/Active	
Encryption-DES	Enabled	
Encryption-3DES-AES	Disabled	
Security Contexts	5	
Carrier	Disabled	
Secure Client Premium Peers	150	
Secure Client Essentials	Disabled	
Other VPN Peers	150	
Total VPN Peers	150	
Secure Client for Mobile	Enabled	
Secure Client for Cisco VPN Phone	Enabled	
Advanced Endpoint Assessment	Enabled	
Shared License	Disabled	
Total TLS Proxy Sessions	220	

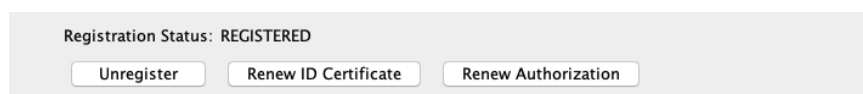
Reset Apply

步骤 5 将思科智能软件管理器中的注册令牌输入 **ID 令牌 (ID Token)** 字段中。



步骤 6 点击 **Register**。

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 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。

使用启动向导配置 ASA

利用 ASDM，您可以使用向导来配置基本功能和高级功能。“启动向导”以默认配置为基础：

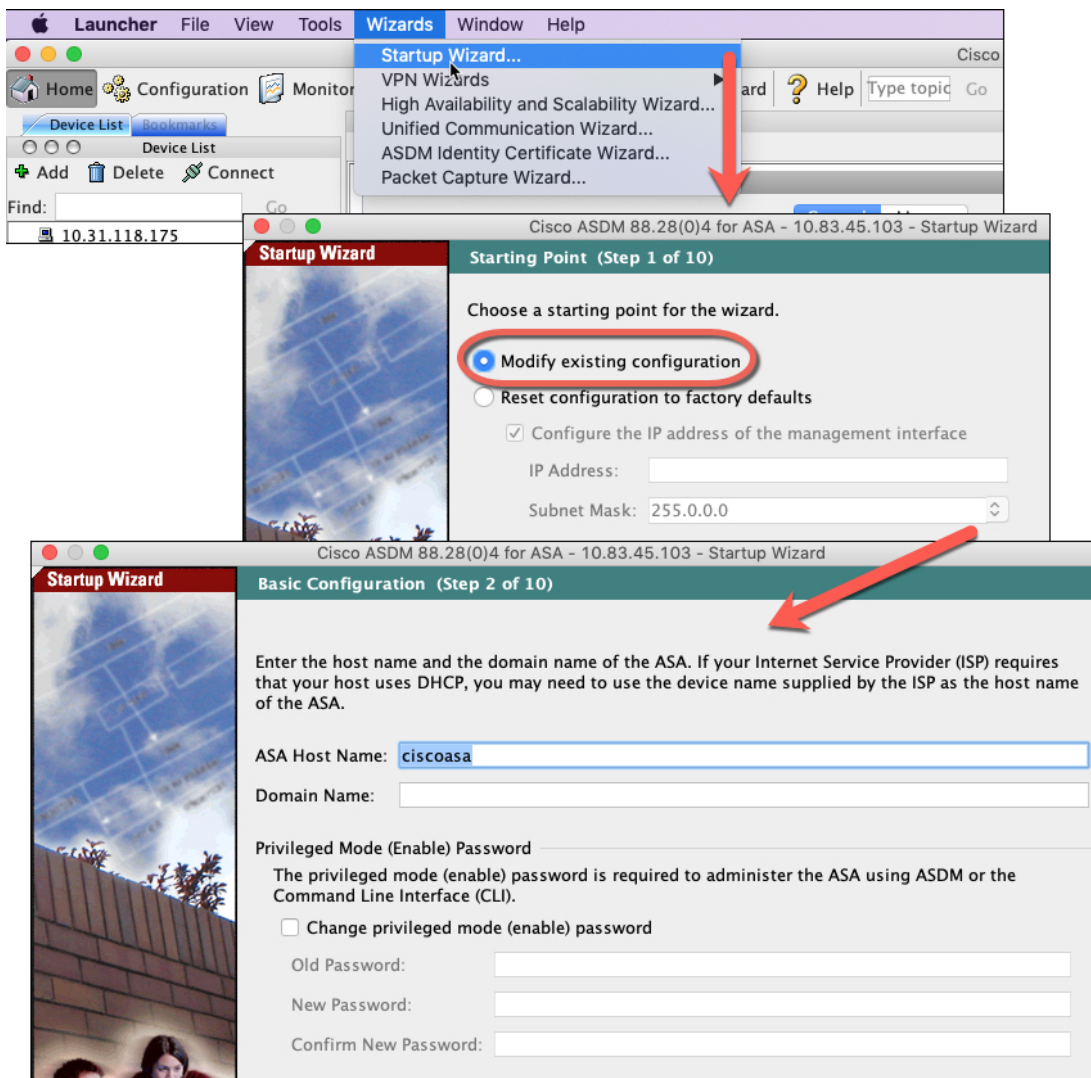
- 内部→外部流量
- 从内部到外部所有流量的接口 PAT。

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...

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 在每个页面上点击下一步 (Next) 以配置您需要的功能。

步骤 3 有关其他向导，请参阅《ASDM 一般操作配置指南》。

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。