



## 使用入门

---

本章介绍如何快速使用思科 ASA。

- [访问命令行界面的控制台，第 1 页](#)
- [配置 ASDM 访问，第 8 页](#)
- [启动 ASDM，第 11 页](#)
- [出厂默认配置，第 13 页](#)
- [将 Firepower 2100 设置为设备或平台模式，第 29 页](#)
- [处理配置，第 31 页](#)
- [将配置更改应用于连接，第 36 页](#)
- [重新加载 ASA，第 36 页](#)

## 访问命令行界面的控制台

对于初始配置，请从控制台端口直接访问 CLI。之后，您可以根据[#unique\\_33](#)使用 Telnet 或 SSH 配置远程访问。如果系统已处于多情景模式，则访问控制台端口会将您引导至系统执行空间。



---

**注释** 有关 ASA 控制台访问，请参阅《ASA 快速入门指南》。

---

## 访问 ASA 硬件或 ISA 3000 控制台

按照以下步骤访问设备控制台。

### 过程

---

**步骤 1** 使用所提供的控制台电缆将计算机连接到控制台端口，并使用已设置为 9600 波特、8 个数据位、无奇偶校验、1 个停止位、无流量控制功能的终端仿真器连接到控制台。

请参阅 ASA 硬件指南，了解有关控制台电缆的详细信息。

**步骤 2** 按 **Enter** 键将看到以下提示符：

```
ciscoasa>
```

此提示符表明您正处于用户 EXEC 模式。用户 EXEC 模式仅能获取基本命令。

**步骤 3** 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 4** 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。

---

## 访问 Firepower 2100 平台模式控制台

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。如果您通过 SSH 连接到 FXOS，您也可以连接到 ASA CLI；来自 SSH 的连接不是控制台连接，因此您可以有多个来自 FXOS SSH 连接的 ASA 连接。同样，如果您通过 SSH 连接到 ASA，您可以连接到 FXOS CLI。

#### 开始之前

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。

**步骤 2** 连接到 ASA：

**connect asa**

示例：

```
firepower-2100# 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** 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 4** 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 5** 要返回到 FXOS 控制台，请输入 **Ctrl+a, d**。

**步骤 6** 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

kp2110 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

[...]
```

```
kp2110#
kp2110# 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#
```

## 访问 Firepower1000 和 2100 设备模式控制台

Firepower1000 和 2100 设备模式控制台端口可将您连接到 ASA CLI（与 Firepower 2100 平台模式控制台不同，后者用于将您连接到 FXOS CLI）。然后，您可以在 ASA CLI 中使用 Telnet 连接到 FXOS CLI 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 1000 随附了一根 USB A 转 B 串行电缆。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。确保为您的操作系统安装必要的 USB 串行驱动程序（请参阅 Firepower 1010 [硬件指南](#) 或 Firepower 1100 [硬件指南](#)）。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#

```

## 访问 Firepower 4100/9300 机箱上的 ASA 控制台

对于初始配置，请通过依次连接到 Firepower 4100/9300 机箱管理引擎（连接控制台端口或使用 Telnet 或 SSH 进行远程连接）和 ASA 安全模块来访问命令行界面。

### 过程

**步骤 1** 连接到 Firepower 4100/9300 机箱管理引擎 CLI（控制台或 SSH），然后将会话连接到 ASA：

```
connect module slot {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。

首次访问模块时，您将访问 FXOS 模块 CLI。然后必须连接到 ASA 应用。

```
connect asa
```

示例：

```

Firepower# connect module 1 console
Firepower-module1> connect asa

asa>

```

**步骤 2** 访问授权的 EXEC 模式，该模式具有最高权限级别。

```
enable
```

第一次输入 **enable** 命令时，系统会提示您更改密码。

示例：

```

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

```

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** 进入全局配置模式。

### configure terminal

示例:

```
asa# configure terminal
asa(config)#
```

要退出全局配置模式，请输入 **disable**、**exit** 或 **quit** 命令。

**步骤 4** 输入 **Ctrl-a, d** 使应用程序控制台返回到 FXOS 模块 CLI

出于故障排除目的，您可能想使用 FXOS 模块 CLI。

**步骤 5** 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-], .**

---

## 访问软件模块控制台

如果已安装软件模块，例如，在 ASA 5506-X 上已安装 ASA FirePOWER 模块，则可以发起到模块控制台的会话。



**注释** 无法使用 **session** 命令访问 ASA 背板上的硬件模块 CLI。

---

### 过程

从 ASA CLI 中，发起到模块的会话:

```
session {sfr | cxsc | ips} console
```

示例:

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
```

```
asasfr login: admin
Password: Admin123
```

---

## 访问 ASA 5506W-X 无线接入点控制台

要访问无线接入点控制台，请执行以下步骤。

### 过程

---

**步骤 1** 从 ASA CLI 发起到接入点的会话：

**session wlan console**

示例：

```
ciscoasa# session wlan console
opening console session with module wlan
connected to module wlan. Escape character sequence is 'CTRL-^X'

ap>
```

**步骤 2** 有关接入点 CLI 的信息，请参阅《[自主 Aironet 接入点思科 IOS 配置指南](#)》。

---

## 配置 ASDM 访问

本节介绍如何通过默认配置访问 ASDM，以及在没有默认配置的情况下如何配置访问。

### 使用出厂默认配置进行 ASDM 访问

通过出厂默认配置，已采用默认网络设置对 ASDM 连接进行了预配置。

### 过程

---

使用以下接口和网络设置连接到 ASDM：

- 管理接口取决于设备型号：
  - Firepower 1010 - Management 1/1 (192.168.45.1) 或内部以太网 1/2 至 1/8 (192.168.1.1)。管理主机限制为 192.168.45.0/24 网络，内部主机限制为 192.168.1.0/24 网络。
  - 设备模式下的 Firepower 1100、2100 - 内部以太网 1/2 (192.168.1.1) 或 Management 1/1（来自 DHCP）。内部主机限制为 192.168.1.0/24 网络。管理主机允许来自任何网络。

- 平台模式下的 Firepower 2100 - Management 1/1 (192.168.45.1)。管理主机受限于192.168.45.0/24 网络。
- Firepower 4100/9300 - 部署时定义的管理类型接口和您选择的 IP 地址。管理主机允许来自任何网络。
- ASA 5506-X、ASA 5506W-X - 内部 GigabitEthernet 1/2 至 1/8 和 wifi GigabitEthernet 1/9 (192.168.10.1)。管理主机限制为 192.168.1.0/24 网络，内部主机限制为 192.168.10.0/24。
- ASA 5508-X 和 ASA 5516-X - 内部千兆以太网 1/2 (192.168.1.1)，。管理主机限制为 192.168.1.0/24 网络。
- ASAv - Managemetn 0/0（在部署期间设置）。管理主机仅限于管理网络。
- ISA 3000 - Management 1/1 (192.168.1.1)。管理主机受限于192.168.1.0/24 网络。

注释 如果更改为多情景模式，则可使用上述网络设置从管理情景访问 ASDM。

---

#### 相关主题

[出厂默认配置](#)，第 13 页

[启用或禁用多情景模式](#)

[启动 ASDM](#)，第 11 页

## 自定义 ASDM 访问

如果满足一个或多个以下条件，可使用该程序：

- 没有出厂默认配置
- 想要更改管理 IP 地址
- 想要更改为透明防火墙模式
- 想要更改为多情景模式

对于单一路由模式，为了实现快速轻松的 ASDM 访问，我们建议应用出厂默认配置，但可选择设置您自己的管理 IP 地址。只有您有特殊需求（如设置透明或多情景模式）或有需要保留的其他配置时，才应使用本节所述程序。



注释

对于 ASAv，可以在部署过程中配置透明模式，所以此程序主要用在类似于部署之后需要清除配置等情况。

## 过程

---

**步骤 1** 在控制台端口访问 CLI。

**步骤 2** （可选）启用透明防火墙模式：

该命令清除您的配置。

**firewall transparent**

**步骤 3** 配置管理接口：

```
interface interface_id
  nameif name
  security-level level
  no shutdown
  ip address ip_address mask
```

示例：

```
ciscoasa(config)# interface management 0/0
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```

**security-level** 是介于 1 到 100 之间的数字，其中 100 为最安全级别。

**步骤 4** （对于直连管理主机）为管理网络设置 DHCP 池：

```
dhcpd address ip_address-ip_address interface_name
dhcpd enable interface_name
```

示例：

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# dhcpd enable management
```

确保此范围内不包括接口地址。

**步骤 5** （对于远程管理主机）配置管理主机路由：

**route management\_ifc management\_host\_ip mask gateway\_ip 1**

示例：

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

**步骤 6** 为 ASDM 启用 HTTP 服务器：

**http server enable**

**步骤 7** 允许管理主机访问 ASDM：

**http** *ip\_address mask interface\_name*

示例:

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

**步骤 8** 保存配置:

**write memory**

**步骤 9** (可选) 将模式设置为多模式:

**mode multiple**

出现提示时, 请确认要将现有配置转换为管理情景。然后系统将提示重新加载 ASA。

---

示例

以下配置将防火墙模式转换为透明模式, 配置 Management 0/0 接口, 并为管理主机启用 ASDM:

```
firewall transparent
interface management 0/0

ip address 192.168.1.1 255.255.255.0
nameif management
security-level 100
no shutdown

dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

相关主题

[恢复出厂默认配置, 第 14 页](#)

[设置防火墙模式](#)

[访问 ASA 硬件或 ISA 3000 控制台, 第 1 页](#)

[启动 ASDM, 第 11 页](#)

## 启动 ASDM

可使用以下两种方法启动 ASDM:

- ASDM-IDM 启动器 - 该启动器是使用您可以连接用其连接到任意 ASA IP 地址的 Web 浏览器从 ASA 下载的一款应用。如果要连接至其他 ASA, 无需重新下载该启动器。

- Java Web Start - 对于您管理的每个 ASA，需要与网络浏览器进行连接，然后保存或启动 Java Web Start 应用。后者，可以将快捷方式保存至您的计算机；但每个 ASA IP 地址需要单独的快捷方式。



**注释** 如果您使用网络启动，则清除 Java 缓存，否则可能会丢失对某些预登录策略（例如 Hostscan）的更改。如果您使用启动器，就不会出现此问题。

在 ASDM 内，可以选择其他 ASA IP 地址进行管理；启动器和 Java Web Start 功能之间的差异主要在于初始连接至 ASA 并启动 ASDM 的方式。

本节介绍最初如何连接 ASDM，以及如何使用启动程序或 java Web Start 启动 ASDM。

ASDM 将文件存储在本地 \Users\\.asdm 目录（包括缓存、日志和首选项）和临时目录中（包括 AnyConnect 配置文件）中。

## 过程

**步骤 1** 在指定为 ASDM 客户端的计算机上，输入以下 URL：

**https://asa\_ip\_address/admin**

**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。

系统将显示 ASDM 启动页面和以下按钮：

- **Install ASDM Launcher and Run ASDM**
- **运行 ASDM (Run ASDM)**
- **Run Startup Wizard**

**步骤 2** 要下载启动程序，请执行以下操作：

- a) 单击 **Install ASDM Launcher and Run ASDM**。
- b) 将用户名和密码字段留空（适用于新安装），然后单击 **OK**。如果未配置 HTTPS 身份验证，可以在没有用户名和 **enable** 密码（默认为空）的情况下获得对 ASDM 的访问权限。首次在 CLI 中输入 **enable** 命令时，系统会提示您更改密码；登录 ASDM 时不会强制执行此行为。建议您尽快更改启用密码，不要再保持空白状态；请参阅 [设置主机名、域名及启用密码和 Telnet 密码](#)。注意：如果您启用了 HTTPS 身份验证，则输入您的用户名及关联的密码。即使不使用身份验证，如果您在登录屏幕输入用户名和密码（而不是将用户名留空），ASDM 也会从本地数据库中检查是否有匹配项。
- c) 将安装程序保存到计算机，然后启动安装程序。安装完成后，将自动打开 ASDM-IDM 启动程序。
- d) 输入管理 IP 地址、同一个用户名和密码（新安装则留空），然后单击 **OK**。

**步骤 3** 要使用 Java Web Start，请执行以下操作：

- a) 点击**运行 ASDM (Run ASDM)** 或**运行启动向导 (Run Startup Wizard)**。
- b) 出现提示时，将快捷方式保存到计算机上。或者，也可以选择打开快捷方式，而不是保存快捷方式。
- c) 从该快捷方式启动 Java Web Start。
- d) 根据显示的对话框接受所有证书。系统将显示思科 ASDM-IDM 启动程序。
- e) 将用户名和密码字段留空（适用于新安装），然后单击**OK**。如果未配置 HTTPS 身份验证，可以在没有用户名和 **enable** 密码（默认为空）的情况下获得对 ASDM 的访问权限。首次在 CLI 中输入 **enable** 命令时，系统会提示您更改密码；登录 ASDM 时不会强制执行此行为。建议您尽快更改启用密码，不要再保持空白状态；请参阅 [设置主机名、域名及启用密码和 Telnet 密码](#)。**注意：**如果您启用了 HTTPS 身份验证，则输入您的用户名及关联的密码。即使不使用身份验证，如果您在登录屏幕输入用户名和密码（而不是将用户名留空），ASDM 也会从本地数据库中检查是否有匹配项。

## 出厂默认配置

出厂默认配置是思科对新的 ASA 应用的配置。

- ASA 5506-X - 出厂默认配置启用功能性内部/外部配置。您可以从内部接口使用 ASDM 管理 ASA，内部接口使用集成路由和桥接放置在桥接组中。
- ASA 5508-X 和 5516-X - 出厂默认配置启用功能性内部/外部配置。您可以从内部接口使用 ASDM 管理 ASA。
- Firepower 1010 - 出厂默认配置启用功能性内部/外部配置。您可以从管理接口或内部交换机端口使用 ASDM 管理 ASA。
- Firepower 1100 - 出厂默认配置启用功能性内部/外部配置。您可以从管理接口或内部接口使用 ASDM 管理 ASA。
- Firepower 2100 - 平台模式（默认）：出厂默认配置启用功能性内部/外部配置。您可以从管理界面使用 Firepower 机箱管理器和 ASDM 管理 ASA。  
设备模式 - 如果更改为设备模式，则出厂默认配置会启用功能性内部/外部配置。您可以从管理接口或内部接口使用 ASDM 管理 ASA。
- Firepower 4100/9300 机箱 - 在部署独立 ASA 或 ASA 集群时，出厂默认配置可配置管理接口，以便可以使用 ASDM 与其连接，然后通过它完成配置。
- ASAv - 根据虚拟机监控程序，在部署过程中，部署配置（初始虚拟部署设置）可配置管理接口，以便可以使用 ASDM 与其连接，然后通过它完成配置。还可以配置故障切换 IP 地址。还可应用“出厂默认”配置（如果需要）。
- ISA 3000 - 出厂默认配置是几乎完全透明的防火墙模式配置，所有内部和外部接口都位于同一网络中；您可以使用 ASDM 连接到管理接口来设置网络的 IP 地址。已为两个接口对 启用硬件旁路，并且所有流量在内联分路仅监控模式下发送到 ASA FirePOWER 模块。此模式仅会向 ASA Firepower 模块发送流量流副本，以用于监控。

对于设备和，出厂默认配置仅可用于路由防火墙模式和单一情景模式，除了 ISA 3000，后者的出厂默认配置仅在透明模式中可用。对于 ASA 和 Firepower 4100/9300 机箱，可以在部署时选择透明模式或路由模式。



**注释** 除映像文件和（隐藏的）默认配置外，以下文件夹和文件是闪存中的标准配置：log/、crypto\_archive/ 和 coredumpinfo/coredump.cfg。这些文件上的日期可能与闪存中映像文件的日期不匹配。这些文件有助于潜在的故障排除；它们不表示已发生故障。

## 恢复出厂默认配置

本节介绍如何恢复出厂默认配置。对于 ASA，该程序可擦除部署配置并对各 ASA 5525-X 应用以下配置：

```
interface management 0/0
  ip address 192.168.1.1 255.255.255.0
  nameif management
  security-level 100
  no shutdown
!
asdm logging informational
asdm history enable
!
http server enable
http 192.168.1.0 255.255.255.0 management
!
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
```



**注释** 在 Firepower 4100/9300 上，恢复出厂默认配置会擦除配置；要恢复默认配置，必须从管理引擎重新部署 ASA。

### 开始之前

此功能仅在路由防火墙模式下可用，但 ISA 3000 除外，ISA 3000 仅在透明模式下支持此命令。此外，该功能仅可用于单一情景模式；已清除配置的 ASA 没有任何定义的情景可使用该功能自动进行配置。

### 过程

**步骤 1** 恢复出厂默认配置：

**configure factory-default** [*ip\_address* [*mask*]]

示例：

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
```

**注释** 此命令不会清除 Firepower 2100 的当前设置模式（设备或平台）。

如果指定 *ip\_address*，则根据设备型号设置内部或管理接口 IP 地址，而不是使用默认 IP 地址。有关由 *ip\_address* 选项设置的接口，请参阅以下型号指南：

- Firepower 1010 - 设置管理界面 IP 地址。
- Firepower 1100-设置内部接口IP地址。
- Firepower 2100在设备模式下-设置内部接口IP地址。
- Firepower 2100在平台模式下-设置管理接口IP地址。
- Firepower 4100/9300-无影响。
- ASAv - 设置管理接口 IP 地址。
- ASA 5506-X - 设置内部接口 IP 地址。
- ASA 5508-X和5516-X-设置内部接口IP地址。
- ISA 3000 - 设置管理接口 IP 地址。

**http** 命令使用您指定的子网。同样，**dhcpd address** 命令范围包含比你指定的 IP 地址更高的所有可用地址。例如，如果指定 10.5.6.78，子网掩码为 255.255.255.0，则 DHCP 地址范围为 10.5.6.79-10.5.6.254。

对于 Firepower 1000，处于设备模式的 Firepower 2100 和 安全防火墙 3100：此命令会清除命令（如果有）以及配置的其余部分。**boot system** 此配置更改不会影响启动时的映像：继续使用当前加载的映像。

对于平台模式下的 Firepower 2100：此型号不使用 **boot system** 命令；软件包由 FXOS 管理。

对于所有其他型号：此命令可清除 **boot system** 命令（如果存在）和其他配置。该命令允许您从特定映像启动。**boot system** 下次在恢复出厂配置后重新加载 ASA 时，它将从内部闪存的第一个映像启动；如果内部闪存中无映像，ASA 将不启动。

**示例：**

```
docs-bxb-asa3(config)# configure factory-default 10.86.203.151 255.255.254.0
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
```

```
WARNING: The new maximum-session limit will take effect after the running-config is saved
and the system boots next time. Command accepted
WARNING: Local user database is empty and there are still 'aaa' commands for 'LOCAL'.
```

```

Executing command: interface management0/0
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.86.203.151 255.255.254.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.86.202.0 255.255.254.0 management
Executing command: dhcpd address 10.86.203.152-10.86.203.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#

```

**步骤 2** 将默认配置保存到闪存:

#### **write memory**

该命令将运行配置保存到启动配置的默认位置，即使以前已将 **boot config** 命令配置为设置另一个位置也是如此；配置清除后，该路径也将清除。

## 恢复 ASA 部署配置

此部分介绍如何恢复 ASA 部署（第 0 天）配置。

### 过程

**步骤 1** 为了执行故障切换，请关闭备用设备。

为防止备用设备变成主用设备，必须将其关闭。如果让其处于打开状态，则当清除主用设备配置后，备用设备将变为主用设备。当原来的主用设备重新加载并且通过故障切换链路重新连接后，旧配置将从新主用设备同步，并且擦除所需要的部署配置。

**步骤 2** 重新加载后，恢复部署配置。为了执行故障切换，请在主用设备上输入以下命令：

#### **write erase**

**注释** ASA 会启动当前运行的映像，因此，不会恢复到原始启动映像。要使用原始启动映像，请参阅 **boot image** 命令。

请勿保存该配置。

**步骤 3** 重新加载 ASA，并加载部署配置：

#### **reload**

**步骤 4** 为了执行故障切换，请开启备用设备。

主用设备重新加载后，开启备用设备。部署配置将同步备用设备。

## ASA 5506-X 系列默认配置

ASA 5506-X 系列的默认出厂配置如下：

- 集成路由和桥接功能 - GigabitEthernet 1/2 至 1/8 属于网桥组 1；网桥虚拟接口 (BVI) 1
- 内部 --> 外部流量 - GigabitEthernet 1/1（外部），BVI 1（内部）
- 从 DHCP 的外部 IP 地址，内部 IP 地址 - 192.168.1.1
- (ASA 5506W-X) WiFi <--> 内部，WiFi --> 外部流量 - GigabitEthernet 1/9 (WiFi)
- (ASA 5506W-X) wifi IP 地址—192.168.10.1
- 内部和 wifi 上的客户端的 DHCP 接入点本身及其所有客户端均使用 ASA 作为 DHCP 服务器。
- ASDM 接入 - 允许内部和 wifi 主机。
- NAT- 从内部、wifi 和管理到外部的所有流量的接口 PAT。

配置由以下命令组成：

```
interface Management1/1
  management-only
  no nameif
  no security-level
  no ip address
  no shutdown
interface GigabitEthernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface GigabitEthernet1/2
  nameif inside_1
  security-level 100
  bridge-group 1
  no shutdown
interface GigabitEthernet1/3
  nameif inside_2
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet1/4
  nameif inside_3
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet1/5
  nameif inside_4
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet1/6
  nameif inside_5
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet1/7
```

```

    nameif inside_6
    security-level 100
    no shutdown
    bridge-group 1
interface GigabitEthernet1/8
    nameif inside_7
    security-level 100
    no shutdown
    bridge-group 1
!
interface bvi 1
    nameif inside
    security-level 100
    ip address 192.168.1.1 255.255.255.0
!
object network obj_any1
    subnet 0.0.0.0 0.0.0.0
    nat (inside_1,outside) dynamic interface
object network obj_any2
    subnet 0.0.0.0 0.0.0.0
    nat (inside_2,outside) dynamic interface
object network obj_any3
    subnet 0.0.0.0 0.0.0.0
    nat (inside_3,outside) dynamic interface
object network obj_any4
    subnet 0.0.0.0 0.0.0.0
    nat (inside_4,outside) dynamic interface
object network obj_any5
    subnet 0.0.0.0 0.0.0.0
    nat (inside_5,outside) dynamic interface
object network obj_any6
    subnet 0.0.0.0 0.0.0.0
    nat (inside_6,outside) dynamic interface
object network obj_any7
    subnet 0.0.0.0 0.0.0.0
    nat (inside_7,outside) dynamic interface
!
same-security-traffic permit inter-interface
!
http server enable
http 192.168.1.0 255.255.255.0 inside_1
http 192.168.1.0 255.255.255.0 inside_2
http 192.168.1.0 255.255.255.0 inside_3
http 192.168.1.0 255.255.255.0 inside_4
http 192.168.1.0 255.255.255.0 inside_5
http 192.168.1.0 255.255.255.0 inside_6
http 192.168.1.0 255.255.255.0 inside_7
!
dhcpd auto_config outside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
!
logging asdm informational

```

对于 ASA 5506W-X，还包括以下命令：

```

interface GigabitEthernet 1/9
    security-level 100
    nameif wifi
    ip address 192.168.10.1 255.255.255.0
    no shutdown
!
object network obj_any_wifi

```

```

subnet 0.0.0.0 0.0.0.0
nat (wifi,outside) dynamic interface
!
http 192.168.10.0 255.255.255.0 wifi
!
dhcpd address 192.168.10.2-192.168.10.254 wifi
dhcpd enable wifi

```

## ASA5508-X 和 5516-X 默认配置

ASA5508-X 和 5516-X 的默认出厂配置如下：

- 内部 --> 外部流量 - GigabitEthernet 1/1（外部）、GigabitEthernet 1/2（内部）
- 外部 IP 地址从 DHCP 获取
- 内部 IP 地址—192.168.1.1
- 内部 DHCP 服务器。
- 来自外部 DHCP 的默认路由
- **Management 1/1** 接口已启用，但未进行其他配置。ASA FirePOWER 模块随后可以使用此接口接入 ASA 内部网络，并将内部接口用作通向互联网的网关。
- **ASDM 接入** - 允许内部主机。
- **NAT**- 从内部 和管理到外部的所有流量的接口 PAT。

配置由以下命令组成：

```

interface Management1/1
management-only
no nameif
no security-level
no ip address
no shutdown
interface GigabitEthernet1/1
nameif outside
security-level 0
ip address dhcp setroute
no shutdown
interface GigabitEthernet1/2
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 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside

```

```
!
logging asdm informational
```

## Firepower 1010 默认配置

Firepower 1010 的出厂默认配置包含以下配置：

- 硬件交换机 - 以太网 1/2 至 1/8 属于 VLAN 1
- 内部→外部流量 - 以太网 1/1（外部），VLAN1（内部）
- 管理 - 管理端口 1/1（管理），IP 地址 192.168.45.1
- 从 DHCP 的外部 IP 地址，内部 IP 地址 - 192.168.1.1
- 内部接口、管理接口上的 DHCP 服务器
- 来自外部 DHCP 的默认路由
- ASDM 访问 - 允许管理和内部主机。管理主机限制为 192.168.45.0/24 网络，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 Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
management-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
```

```
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
  name-server 208.67.222.222 outside
  name-server 208.67.220.220 outside
!
```

## Firepower 1100 默认配置

Firepower 1100 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
- 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
!
```

## 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。
- 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

## 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
!
```

## Firepower 4100/9300 机箱 默认配置

在 Firepower 4100/9300 机箱上部署 ASA 时，可预设置许多可供您使用 ASDM 连接到 Management 0/0 接口的参数。典型配置包括以下设置：

- 管理接口：
  - 您选择的管理类型接口已在 Firepower 4100/9300 机箱管理引擎上定义
  - 命名为 “management”
  - 您选择的 IP 地址
  - 安全级别为 0
  - 管理专用
- 通过管理接口的默认路由
- ASDM 访问 - 允许所有主机。

独立设备的配置包括以下命令。有关集群设备的其他配置，请参阅[创建 ASA 集群](#)。

```
interface <management_ifc>
```

```

management-only
ip address <ip_address> <mask>
ipv6 address <ipv6_address>
ipv6 enable
nameif management
security-level 0
no shutdown
!
http server enable
http 0.0.0.0 0.0.0.0 management
http ::/0 management
!
route management 0.0.0.0 0.0.0.0 <gateway_ip> 1
ipv6 route management ::/0 <gateway_ipv6>

```

## ISA 3000 的默认配置

ISA 3000 的默认出厂配置如下：

- **透明防火墙模式** - 透明防火墙是第 2 层防火墙，充当“嵌入式防火墙”或“隐藏防火墙”，并且不会被视为所连接设备的路由器跃点。
- **1 个网桥虚拟接口** - 所有成员接口都位于同一网络中（**IP 地址未预先配置；必须进行设置以与您的网络相匹配**）：GigabitEthernet 1/1 (outside1)、GigabitEthernet 1/2 (inside1)、GigabitEthernet 1/3 (outside2)、GigabitEthernet 1/4 (inside2)
- 所有内部和外部接口均可互相通信。
- **管理 1/1 接口** - 192.168.1.1/24 用于 ASDM 访问。
- 用于管理上的客户端的 **DHCP**。
- **ASDM 访问** - 允许管理主机。
- 为以下接口对启用了**硬件旁路**：GigabitEthernet 1/1 和 1/2；GigabitEthernet 1/3 和 1/4



**注 释** 当 ISA 3000 断电并进入硬件旁路模式时，只有上述接口对能够通信；inside1 和 inside2 以及 outside1 和 outside2 将不再能通信。这些接口之间的任何现有连接都将断开。在恢复供电后，将随着 ASA 接管流而发生短暂连接中断。

- **ASA FirePOWER 模块** - 在内联 Tap 监控器专用模式下，所有流量都将发送到该模块。此模式将重复的流量流发送到 ASA Firepower 模块，仅用于监控目的。
- **精确时间协议** - 不会将 PTP 流量发送到 FirePOWER 模块。

配置由以下命令组成：

```

firewall transparent

interface GigabitEthernet1/1

```

```
bridge-group 1
nameif outside1
security-level 0
no shutdown
interface GigabitEthernet1/2
bridge-group 1
nameif inside1
security-level 100
no shutdown
interface GigabitEthernet1/3
bridge-group 1
nameif outside2
security-level 0
no shutdown
interface GigabitEthernet1/4
bridge-group 1
nameif inside2
security-level 100
no shutdown
interface Management1/1
management-only
no shutdown
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0
interface BVI1
  no ip address

access-list allowAll extended permit ip any any
access-group allowAll in interface outside1
access-group allowAll in interface outside2

same-security-traffic permit inter-interface

hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4

http server enable
http 192.168.1.0 255.255.255.0 management

dhcpd address 192.168.1.5-192.168.1.254 management
dhcpd enable management

object-group service bypass_sfr_inspect
  service-object udp destination range 319 320
access-list sfrAccessList extended deny object-group bypass_sfr_inspect any any
access-list sfrAccessList extended permit ip any any
class-map sfrclass
  match access-list sfrAccessList
policy-map global_policy
  class sfrclass
    sfr fail-open monitor-only
service-policy global_policy global
```

## ASAv 部署配置

部署 ASAv 时，可预设置许多可供您使用 ASDM 连接到 Management 0/0 接口的参数。典型配置包括以下设置：

- 路由或透明防火墙模式

- Management 0/0 接口：
  - 命名为 “management”
  - IP 地址或 DHCP
  - 安全级别为 0
- 管理主机 IP 地址的静态路由（如果其没有位于管理子网中）
- 启用或禁用 HTTP 服务器
- 管理主机 IP 地址的 HTTP 访问
- （可选）GigabitEthernet 0/8 的故障切换链路 IP 地址和 Management0/0 备用 IP 地址
- DNS 服务器
- 智能许可 ID 令牌
- 智能许可吞吐量水平和标准功能层
- （可选）Smart Call Home HTTP 代理 URL 和端口
- （可选）SSH 管理设置：
  - 客户端 IP 地址
  - 本地用户名和密码
  - 使用本地数据库进行 SSH 所需的身份验证
- （可选）启用或禁用 REST API



**注释** 为成功向思科许可授权机构注册 ASA，ASA 需要互联网访问。部署之后，可能需要执行其他配置，以实现互联网访问和成功注册许可证。

有关独立设备，请参阅以下配置示例：

```
interface Management0/0
  nameif management
  security-level 0
  ip address ip_address

  no shutdown
  http server enable
  http management_host_IP mask management
  route management management_host_IP mask gateway_ip 1
  dns server-group DefaultDNS
  name-server ip_address
  call-home
  http-proxy ip_address port port
  license smart
  feature tier standard
```

```

throughput level {100M | 1G | 2G}
license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent

```

有关故障切换对中的主要设备，请参阅以下配置示例：

```

nameif management
  security-level 0
  ip address ip_address standby standby_ip

  no shutdown
route management management_host_IP mask gateway_ip 1
http server enable
http management_host_IP mask management
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
failover
failover lan unit primary
failover lan interface fover gigabitethernet0/8
failover link fover gigabitethernet0/8
failover interface ip fover primary_ip mask standby standby_ip

```

## 将 Firepower 2100 设置为设备或平台模式

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

此程序介绍如何更改模式。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。请注意，**clear configure all** 和 **configure factory-default** 命令不会清除当前模式。

## 开始之前

您只能在 CLI 中更改模式。

## 过程

---

**步骤 1** (可选) 备份当前配置。请参阅 [备份和恢复配置或其他文件](#)。

虽然设备模式配置和平台模式配置之间存在细微差异，但旧配置的副本可能是一个很好的起点。例如，对于平台模式，NTP、DNS 和 EtherChannel 配置不是 ASA 配置的一部分，因此不会包含在备份中，但大多数其他 ASA 设置对两种模式均有效。

**步骤 2** 查看当前模式。

**show fxos mode**

示例:

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

**步骤 3** 将模式设置为平台模式。

**no 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)# 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 4** 将模式设置为设备模式。

**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]
```

## 处理配置

本节介绍如何处理配置。ASA 从文本文件（称为启动配置）加载配置。默认情况下，该文件作为隐藏文件驻留在内部闪存中。但是，也可为启动配置指定不同路径。

输入命令时，仅对内存中的运行配置进行更改。必须将运行配置手动保存到启动配置，以便重新启动后更改仍旧有效。

除非另有说明，否则本节中的信息适用于单一安全情景和多安全情景。

## 保存配置更改

本节介绍如何保存配置。

### 在单情景模式下保存配置更改

要将运行配置保存到启动配置，请执行以下程序。

过程

将运行配置保存到启动配置中。

**write memory**

注释 **copy running-config startup-config** 命令等同于 **write memory** 命令。

## 在多情景模式下保存配置更改

可分别保存每个情景（和系统）配置，或者，也可同时保存所有情景配置。

### 分别保存每个情景和系统

使用以下程序保存系统或情景配置。

#### 过程

---

从情景或系统中，将运行配置保存到启动配置：

#### **write memory**

对于多情景模式，情景启动配置可以驻留在外部服务器。在这种情况下，ASA 会将配置重新保存至您在情景 URL 中标识的服务器，但 HTTP 或 HTTPS URL 除外，它们不允许您将配置保存至服务器。

**注释** `copy running-config startup-config` 命令等同于 `write memory` 命令。

---

### 同时保存所有情景配置

请按照以下操作步骤同时保存所有情景配置以及系统配置。

#### 过程

---

从系统执行空间，将运行配置保存到所有情景的启动配置和系统配置：

#### **write memory all [/noconfirm]**

如果不输入 `/noconfirm` 关键字，则将看到以下提示：

```
Are you sure [Y/N]:
```

在输入 **Y** 后，ASA 会保存系统配置和每个情景。情景启动配置可驻留在外部服务器上。在这种情况下，ASA 会将配置保存回您在情景 URL 中标识的服务器，但 HTTP 或 HTTPS URL 除外，它们不允许您将配置保存到服务器。

在 ASA 保存每个情景后，系统将显示以下消息：

```
'Saving context 'b' ... ( 1/3 contexts saved )'
```

有时，情景会由于出错而不能保存。请参阅以下错误的相关信息：

- 对于因内存不足而未保存的情景，系统将显示以下消息：

```
The context 'context a' could not be saved due to Unavailability of resources
```

- 对于因无法到达远程目标而未保存的情景，系统将显示以下消息：

```
The context 'context a' could not be saved due to non-reachability of destination
```

- 对于因情景被锁定而无法保存的情景，系统将显示以下消息：

```
Unable to save the configuration for the following contexts as these contexts are locked.
context 'a' , context 'x' , context 'z' .
```

仅在其他用户已在保存配置或正在删除情景时，才会锁定情景。

- 对于因启动配置为只读配置而不能保存的情景（例如，在 HTTP 服务器上），在所有其他消息的末尾将显示以下消息报告：

```
Unable to save the configuration for the following contexts as these contexts have
read-only config-urls:
context 'a' , context 'b' , context 'c' .
```

- 对于因闪存扇区错误而未保存的情景，系统将显示以下消息：

```
The context 'context a' could not be saved due to Unknown errors
```

## 将启动配置复制到运行配置

使用以下命令之一，将新启动配置复制到运行配置：

- **copy startup-config running-config**

将启动配置与运行配置合并。合并会将新配置中的所有新命令添加到运行配置中。如果配置相同，则不会发生任何更改。如果命令冲突或命令影响情景的运行，则合并的影响取决于命令。可能会发生错误，也可能出现意外结果。

- **reload**

重新加载 ASA，即加载启动配置并丢弃运行配置。

- **clear configure all**，然后 **copy startup-config running-config**

加载启动配置并丢弃运行配置，无需重新加载。

## 查看配置

以下命令可供您查看运行配置和启动配置：

- **show running-config**  
查看运行配置。
- **show running-config *command***  
查看特定命令的运行配置。
- **show startup-config**  
查看启动配置。

## 清除和删除配置设置

要擦除设置，请输入以下命令之一：

- **clear configure *configurationcommand* [*level2configurationcommand*]**  
清除指定命令的所有配置。如果只想清除特定版本命令的配置，则可输入 *level2configurationcommand* 的值。  
例如，要清除所有 **aaa** 命令的配置，请输入以下命令：

```
ciscoasa(config)# clear configure aaa
```

要仅清除 **aaa authentication** 命令的配置，请输入以下命令：

```
ciscoasa(config)# clear configure aaa authentication
```

- **no *configurationcommand* [*level2configurationcommand*] *qualifier***  
禁用命令的特定参数或选项。在这种情况下，可使用 **no** 命令删除 *qualifier* 识别的特定配置。  
例如，要删除特定 **access - list** 命令，请输入足够命令对其进行唯一标识；可能必须输入整个命令：

```
ciscoasa(config)# no access-list abc extended permit icmp any any object-group obj_icmp_1
```

- **write erase**  
擦除启动配置。



注释

对于 ASAv，此命令将在重新加载后恢复部署配置。要完全擦除配置，请使用 **clear configure all** 命令。

- **clear configure all**  
擦除运行配置。



**注释** 在多情景模式下，如果从系统配置输入 **clear configure all**，还将删除所有情景并使它们停止运行。情景配置文件将不删除，仍保留在原始位置。



**注释** 对于设备模式下的 Firepower 1000 和 Firepower 2100：此命令会清除 **boot system** 命令（如果有）以及配置的其余部分。此配置更改不会影响启动时的映像：继续使用当前加载的映像。

对于平台模式下的 Firepower 2100：此型号不使用 **boot system** 命令；软件包由 FXOS 管理。

对于所有其他型号：此命令可清除 **boot system** 命令（如果存在）和其他配置。**boot system** 命令使您可以从特定映像上启动，包括外部闪存卡上的映像。下次重新加载 ASA 时，它将从内部闪存的第一个映像启动；如果内部闪存中无映像，则 ASA 将不启动。



**注释** 此命令不会清除 Firepower 2100 的当前设置模式（设备或平台）。

## 离线创建文本配置文件

本指南介绍如何使用 CLI 配置 ASA；保存命令时，更改将写入文本文件。但是，如果不使用 CLI，则可以直接在计算机上编辑文本文件，并将配置完整地或逐行粘贴在配置模式命令行提示符处。或者，也可将文本文件下载至 ASA 内部闪存。有关如何将配置文件下载至 ASA 的信息，请参阅[软件和配置](#)。

在大多数情况下，本指南所述的命令之前都有 CLI 提示符。以下示例中的提示为“ciscoasa(config)#”：

```
ciscoasa(config)# context a
```

在文本配置文件中，系统不提示您输入命令，因此提示符省略如下：

```
context a
```

有关格式化文件的其他信息，请参阅[使用命令行界面](#)。

## 将配置更改应用于连接

更改配置的安全策略后，所有新连接将使用新安全策略。现有连接继续使用在建立连接时配置的策略。旧连接的 **show** 命令输出反映旧配置，在某些情况下不会包含旧连接的数据。

例如，如果要从接口删除 QoS **service-policy**，然后重新添加修改版本，则 **show service-policy** 命令仅显示与匹配新服务策略的新连接相关联的 QoS 计数器；旧策略的现有连接不再显示在命令输出中。

要确保所有连接使用新策略，需要断开当前连接，以便其使用新策略重新连接。

要断开连接，请输入以下命令：

```
• clear conn [all] [protocol {tcp | udp}] [address src_ip [-src_ip] [netmask mask]] [port src_port [-src_port]] [address dest_ip [-dest_ip] [netmask mask]] [port dest_port [-dest_port]]
```

该命令可在任何状态中终止连接。要查看所有当前连接，请参阅 **show conn** 命令。

如果不带参数，该命令将清除所有受影响的出站连接。要清除进站连接（包括当前的管理会话），请使用 **all** 关键字。要根据源 IP 地址、目标 IP 地址、端口和/或协议清除特定连接，可以指定所需选项。

## 重新加载 ASA

要重新加载 ASA，请完成以下操作步骤。

### 过程

---

重新加载 ASA：

```
reload
```

注释 在多情景模式下，仅可从系统执行空间重新加载。

---