



使用入门

- [任务流](#)，第 1 页
- [初始配置](#)，第 1 页
- [访问 FXOS CLI](#)，第 8 页

任务流

以下程序显示配置 Firepower 4100/9300 机箱时应当完成的基本任务。

过程

- 步骤 1** 配置 Firepower 4100/9300 机箱硬件（请参阅[思科 Firepower 安全设备硬件安装指南](#)）。
 - 步骤 2** 完成初始配置（请参阅[初始配置](#)，第 1 页）。
 - 步骤 3** 设置日期和时间（请参阅[设置日期和时间](#)）。
 - 步骤 4** 配置 DNS 服务器（请参阅[配置 DNS 服务器](#)）。
 - 步骤 5** 注册产品许可证（请参阅[ASA 的许可证管理](#)）。
 - 步骤 6** 配置用户（请参阅[用户管理](#)）。
 - 步骤 7** 按需执行软件更新（请参阅[映像管理](#)）。
 - 步骤 8** 配置其他平台设置（请参阅[平台设置](#)）。
 - 步骤 9** 配置接口（请参阅[接口管理](#)）。
 - 步骤 10** 创建逻辑设备（请参阅[逻辑设备](#)）。
-

初始配置

在可以使用 Firepower 机箱管理器或 FXOS CLI 配置和管理系统之前，必须执行一些初始配置任务。您可以使用通过控制台端口访问的 FXOS CLI 或使用通过管理端口访问的 SSH、HTTPS 或 REST API 来执行初始配置（此程序也称为低接触调配）。

使用控制台端口的初始配置

当第一次使用 FXOS CLI 访问 Firepower 4100/9300 机箱时，您将会看到安装向导，可以用它来配置系统。



注释 要重复初始设置，您需要使用以下命令清除任何现有配置：

```
Firepower-chassis# connect local-mgmt  
firepower-chassis(local-mgmt)# erase configuration
```

您必须为 Firepower 4100/9300 机箱上的单一管理端口指定一个 IPv4 地址、网关和子网掩码，或者一个 IPv6 地址、网关和网络前缀。您可以为管理端口 IP 地址配置 IPv4 或 IPv6 地址。

开始之前

1. 在 Firepower 4100/9300 机箱上验证下列物理连接：

- 控制台端口以物理方式连接到计算机终端或控制台服务器。
- 1 Gbps 以太网管理端口连接到外部集线器、交换机或路由器。

有关更多信息，请参阅硬件安装指南。

2. 验证连接到控制台端口的计算机终端（或控制台服务器）上的控制台端口参数是否为如下所示：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

3. 收集以下信息以与设置脚本一起使用：

- 新管理员密码
- 管理 IP 地址和子网掩码
- 网关 IP 地址
- 要从中允许 HTTPS 和 SSH 访问的子网
- 主机名和域名
- DNS 服务器 IP 地址

过程

步骤 1 接通机箱电源。

步骤 2 使用终端仿真器连接到串行控制台端口。

Firepower 4100/9300 随附 RS-232 转 RJ-45 串行控制台电缆。可能需要使用第三方串口转 USB 电缆建立连接。使用以下串行参数：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

步骤 3 根据提示完成系统配置。

注释 您可以在初始配置期间随时进入调试菜单，以调试任何设置问题或中止配置并重新引导系统。要进入调试菜单，请按 Ctrl-C。要退出调试菜单，请按两次 Ctrl-D。请注意，您在第一次按下 Ctrl-D 与第二次按下 Ctrl-D 之间输入任何内容，都将在第二次按下后运行。

示例：

```
---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the FXOS Supervisor is performed through these steps.

Type Ctrl-C at any time for more options or to abort configuration
and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.

You have chosen to setup a new Security Appliance.
Continue? (yes/no): y

Enforce strong password? (yes/no) [y]: n

Enter the password for "admin": Farscape&32
Confirm the password for "admin": Farscape&32
Enter the system name: firepower-9300

Supervisor Mgmt IP address : 10.80.6.12

Supervisor Mgmt IPv4 netmask : 255.255.255.0

IPv4 address of the default gateway : 10.80.6.1

The system cannot be accessed via SSH if SSH Mgmt Access is not configured.

Do you want to configure SSH Mgmt Access? (yes/no) [y]: y

SSH Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0
```

```

SSH Mgmt Access IPv4 netmask: 255.0.0.0

Firepower Chassis Manager cannot be accessed if HTTPS Mgmt Access is not configured.

Do you want to configure HTTPS Mgmt Access? (yes/no) [y]: y

HTTPS Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

HTTPS Mgmt Access IPv4 netmask: 255.0.0.0

Configure the DNS Server IP address? (yes/no) [n]: y

    DNS IP address : 10.164.47.13

Configure the default domain name? (yes/no) [n]: y

    Default domain name : cisco.com

Following configurations will be applied:

Switch Fabric=A
System Name=firepower-9300
Enforced Strong Password=no
Supervisor Mgmt IP Address=10.89.5.14
Supervisor Mgmt IP Netmask=255.255.255.192
Default Gateway=10.89.5.1
SSH Access Configured=yes
    SSH IP Address=10.0.0.0
    SSH IP Netmask=255.0.0.0
HTTPS Access Configured=yes
    HTTPS IP Address=10.0.0.0
    HTTPS IP Netmask=255.0.0.0
DNS Server=72.163.47.11
Domain Name=cisco.com

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y
Applying configuration. Please wait... Configuration file - Ok
.....

Cisco FPR Series Security Appliance
firepower-9300 login: admin
Password: Farscape&32
Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.

[...]

firepower-chassis#

```

使用管理端口的低接触调配

当您的 Firepower 4100/9300 机箱启动时，如果其找不到启动配置，设备将进入低接触调配模式，在该模式中，设备会寻找动态主机控制协议 (DHCP) 服务器，然后使用其管理接口 IP 地址自行启动。然后，您可以通过管理接口进行连接，以使用 SSH、HTTPS 或 FXOS REST API 配置系统。



注释 要重复初始设置，您需要使用以下命令清除任何现有配置：

```
Firepower-chassis# connect local-mgmt  
firepower-chassis(local-mgmt)# erase configuration
```

您必须为 Firepower 4100/9300 机箱上的单一管理端口指定一个 IPv4 地址、网关和子网掩码，或者一个 IPv6 地址、网关和网络前缀。您可以为管理端口 IP 地址配置 IPv4 或 IPv6 地址。

开始之前

收集以下信息以与设置脚本一起使用：

- 新管理员密码
- 管理 IP 地址和子网掩码
- 网关 IP 地址
- 要从中允许 HTTPS 和 SSH 访问的子网
- 主机名和域名
- DNS 服务器 IP 地址

过程

步骤 1 配置您的 DHCP 服务器以将 IP 地址分配到 Firepower 4100/9300 机箱的管理端口。

来自 Firepower 4100/9300 机箱的 DHCP 客户端请求将包含以下内容：

- 管理接口的 MAC 地址。
- DHCP 选项 60 (vendor-class-identifier) - 设置为“FPR9300”或“FPR4100”。
- DHCP 选项 61(dhcp-client-identifier) - 设置为 Firepower 4100/9300 机箱序列号。此序列号可在机箱的拉出卡舌上找到。

步骤 2 打开 Firepower 4100/9300 机箱的电源。

如果在机箱启动时找不到启动配置，设备将进入低接触调配模式。

步骤 3 要使用 HTTPS 配置系统：

a) 使用支持的浏览器，在地址栏中输入以下 URL：

```
https://<ip_address>/api
```

其中 <ip_address> 是您的 DHCP 服务器分配的 Firepower 4100/9300 机箱上的管理端口 IP 地址。

注释 有关受支持的浏览器的信息，请参阅您使用的版本的发行说明（请参阅 <http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html>）

- b) 系统提示时，使用用户名 **install** 和密码 `<chassis_serial_number>` 登录。
检查机箱上的标签可获取 `<chassis_serial_number>`。
- c) 根据提示完成系统配置。
 - 强密码执行策略（对于强密码准则，请参阅[用户帐户](#)）
 - 管理员帐户的密码。
 - 系统名称
 - 监控程序管理端口 IPv4 地址和子网掩码，或者 IPv6 地址和前缀。
 - 默认网关 IPv4 或 IPv6 地址。
 - 允许使用 SSH 访问的主机/网络地址和网络掩码/前缀。
 - 允许使用 HTTPS 访问的主机/网络地址和网络掩码/前缀。
 - DNS 服务器 IPv4 或 IPv6 地址。
 - 默认域名。
- d) 单击**提交**。

步骤 4 要使用 SSH 配置系统：

- a) 使用以下命令连接到管理端口：

```
ssh install@<ip_address>
```

其中 `<ip_address>` 是您的 DHCP 服务器分配的 Firepower 4100/9300 机箱上的管理端口 IP 地址。

- b) 出现提示时，使用密码 **Admin123** 登录。
- c) 根据提示完成系统配置。

注释 您可以在初始配置期间随时进入调试菜单，以调试任何设置问题或中止配置并重新引导系统。要进入调试菜单，请按 **Ctrl-C**。要退出调试菜单，请按两次 **Ctrl-D**。请注意，您在第一次按下 **Ctrl-D** 与第二次按下 **Ctrl-D** 之间输入任何内容，都将在第二次按下后运行。

示例：

```
---- Basic System Configuration Dialog ----
```

```
This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the FXOS Supervisor is performed through these steps.
```

```
Type Ctrl-C at any time for more options or to abort configuration
and reboot system.
```

```
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.
```

```
You have chosen to setup a new Security Appliance.
```

```
Continue? (yes/no): y

Enforce strong password? (yes/no) [y]: n

Enter the password for "admin": Farscape&32
Confirm the password for "admin": Farscape&32
Enter the system name: firepower-9300

Supervisor Mgmt IP address : 10.80.6.12

Supervisor Mgmt IPv4 netmask : 255.255.255.0

IPv4 address of the default gateway : 10.80.6.1

The system cannot be accessed via SSH if SSH Mgmt Access is not configured.

Do you want to configure SSH Mgmt Access? (yes/no) [y]: y

SSH Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

SSH Mgmt Access IPv4 netmask: 255.0.0.0

Firepower Chassis Manager cannot be accessed if HTTPS Mgmt Access is not configured.

Do you want to configure HTTPS Mgmt Access? (yes/no) [y]: y

HTTPS Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

HTTPS Mgmt Access IPv4 netmask: 255.0.0.0

Configure the DNS Server IP address? (yes/no) [n]: y

DNS IP address : 10.164.47.13

Configure the default domain name? (yes/no) [n]: y

Default domain name : cisco.com

Following configurations will be applied:

Switch Fabric=A
System Name=firepower-9300
Enforced Strong Password=no
Supervisor Mgmt IP Address=10.89.5.14
Supervisor Mgmt IP Netmask=255.255.255.192
Default Gateway=10.89.5.1
SSH Access Configured=yes
  SSH IP Address=10.0.0.0
  SSH IP Netmask=255.0.0.0
HTTPS Access Configured=yes
  HTTPS IP Address=10.0.0.0
  HTTPS IP Netmask=255.0.0.0
DNS Server=72.163.47.11
Domain Name=cisco.com

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y
Applying configuration. Please wait... Configuration file - Ok
.....

Initial Setup complete, Terminating sessions
.Connection to <ip_address> closed.
```

步骤 5 要使用 FXOS REST API 配置您的系统:

使用以下示例通过 REST API 配置系统。有关详细信息，请参阅<https://developer.cisco.com/site/ssp/firepower/>。

注释 属性 `dn`、`domain_name`、`https_net`、`https_mask`、`ssh_net` 和 `ssh_mask` 都为选填。REST API 配置的所有其他属性都为必填。

IPv4 REST API example:

```
{
  "fxosBootstrap": {
    "dns": "1.1.1.1",
    "domain_name": "cisco.com",
    "mgmt_gw": "192.168.0.1",
    "mgmt_ip": "192.168.93.3",
    "mgmt_mask": "255.255.0.0",
    "password1": "admin123",
    "password2": "admin123",
    "strong_password": "yes",
    "system_name": "firepower-9300",
    "https_mask": "2",
    "https_net": "::",
    "ssh_mask": "0",
    "ssh_net": "::"
  }
}
```

IPv6 REST API example

```
{
  "fxosBootstrap": {
    "dns": "2001::3434:4343",
    "domain_name": "cisco.com",
    "https_mask": "2",
    "https_net": "::",
    "mgmt_gw": "2001::1",
    "mgmt_ip": "2001::2001",
    "mgmt_mask": "64",
    "password1": "admin123",
    "password2": "admin123",
    "ssh_mask": "0",
    "ssh_net": "::",
    "strong_password": "yes",
    "system_name": "firepower-9300"
  }
}
```

访问 FXOS CLI

您可以使用插入到控制台端口中的终端来连接到 FXOS CLI。验证连接到控制台端口的计算机终端（或控制台服务器）上的控制台端口参数是否为如下所示：

- 9600 波特率
- 8 个数据位

- 无奇偶校验
- 1 个停止位

您也可以使用 SSH 和 Telnet 连接到 FXOS CLI。FXOS 最多支持八个 SSH 并发连接。要使用 SSH 进行连接，您需要知道 Firepower 4100/9300 机箱的主机名或 IP 地址。

使用以下语法示例之一来通过 SSH、Telnet 或 Putty 进行登录：



注释 SSH 登录区分大小写。

使用 SSH 从 Linux 终端登录：

- **ssh ucs-auth-domain \username@{UCSM-ip-address | UCMS-ipv6-address}**

```
ssh ucs-example\jsmith@192.0.20.11
ssh ucs-example\jsmith@2001::1
```
- **ssh -l ucs-auth-domain \username {UCSM-ip-address| UCMS-ipv6-address| UCMS-host-name}**

```
ssh -l ucs-example\jsmith 192.0.20.11
ssh -l ucs-example\jsmith 2001::1
```
- **ssh {UCSM-ip-address | UCMS-ipv6-address | UCMS-host-name} -l ucs-auth-domain \username**

```
ssh 192.0.20.11 -l ucs-example\jsmith
ssh 2001::1 -l ucs-example\jsmith
```
- **ssh ucs-auth-domain \username@{UCSM-ip-address | UCMS-ipv6-address}**

```
ssh ucs-ldap23\jsmith@192.0.20.11
ssh ucs-ldap23\jsmith@2001::1
```

使用 Telnet 从 Linux 终端登录：



注释 默认情况下，Telnet 处于禁用状态。有关启用 Telnet 的说明，请参阅[配置 Telnet](#)。

- **telnet ucs-UCSM-host-name ucs-auth-domain \username**

```
telnet ucs-qa-10
login: ucs-ldap23\bladmin
```
- **telnet ucs-{UCSM-ip-address | UCMS-ipv6-address} ucs-auth-domain \username**

```
telnet 10.106.19.12 2052
ucs-qa-10-A login: ucs-ldap23\bladmin
```

从 Putty 客户端登录：

- 登录方式：**ucs-auth-domain \username**

```
Login as: ucs-example\jsmith
```



注释 如果默认身份验证设置为本地，并且控制台身份验证设置为 LDAP，您可以使用 `ucs-local\admin` 从 Putty 客户端登录交换矩阵互联，其中 `admin` 是本地帐户名称。
