Cisco FXOS Firepower 机箱管理器配置指南，1.1(1)

首次发布日期: 2015 年 07 月 16 日

上次修改日期: 2015 年 10 月 12 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

文本部件号： 仅提供在线版本

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系以获取副本。

思科所采用的 TCP 报头压缩是加州大学伯克利分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。版权所有 © 1981，加州大学董事会。

无论本手册中是否有任何其他保证，这些供应商的所有文档文件和软件均按“原样”提供，并可能包含缺陷。思科和上面所提及的提供商拒绝所有明示或暗示担保，包括（但不限于）适销性、特定用途适用性和无侵权担保，或者因买卖或使用以及商业惯例所引发的担保。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请访问此网址：http://www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

目 录

第 1 章

Firepower 安全设备简介

关于 Firepower 安全设备

Cisco FXOS 机箱是下一代网络和内容安全解决方案平台。FXOS 机箱是思科以应用为中心的基础设施 (ACI) 安全解决方案的一部分，提供灵活、开放的安全平台，专为可扩展性、一致控制和简化管理而构建。

FXOS 机箱具有以下特性：

- 基于机箱的模块化安全系统 - 提供高性能、灵活的输入/输出配置和可扩展性。
- Firepower 机箱管理器 - 图形用户界面，简单、直观地显示当前机箱状态并提供简化的机箱功能配置。
- FXOS CLI - 提供基于命令的接口，用于配置功能、监控机箱状态和访问高级故障排除功能。
- FXOS REST API - 允许用户以编程方式配置和管理其机箱。

Firepower 机箱管理器概述

Firepower 可扩展操作系统提供 Web 界面，让您轻松配置平台设置和接口，调配设备，以及监控系统状态。用户界面顶部的导航栏提供到下列页面的访问：

- 概述 (Overview) - 从“概述 (Overview)”页面，您可以轻松监控 Firepower 机箱的状态。有关详细信息，请参阅监控机箱状态，第 2 页。
- 接口 (Interfaces) - 从“接口 (Interfaces)”页面，您可以查看机箱上安装的接口的状态，编辑接口属性，启用或禁用接口，以及创建端口通道。有关详细信息，请参阅接口管理，第 55 页。

- 逻辑设备 (Logical Devices) - 从“逻辑设备 (Logical Devices)”页面，您可以创建、编辑和删除逻辑设备。有关详细信息，请参阅逻辑设备，第 59 页。
- 平台设置 (Platform Settings) - 从“平台设置 (Platform Settings)”页面，您可以配置机箱的下列设置：日期和时间、SSH、SNMP、HTTPS、AAA、系统日志和 DNS。有关详细信息，请参阅平台设置，第 31 页。
- 系统设置 (System Settings) - 从“系统 (System)”菜单，您可以管理下列设置：

  许可 (Licensing) - 从“许可 (Licensing)”页面，您可以配置 Smart Call Home 设置，向许可证颁发机构注册 Firepower 机箱。有关详细信息，请参阅许可证管理，第 11 页。

  更新 (Updates) - 从“更新 (Updates)”页面，您可以将平台捆绑包和应用映像上传到 Firepower 机箱。有关详细信息，请参阅映像管理，第 27 页。

  用户管理 (User Management) - 从“用户管理 (User Management)”页面，您可以为 FXOS 机箱配置用户设置和定义用户帐户。有关详细信息，请参阅用户管理，第 17 页。

监控机箱状态

从“概述 (Overview)”页面，您可以轻松监控 Firepower 机箱的状态。“概述 (Overview)”页面提供下列元素：

- 设备信息 (Device Information) -“概述 (Overview)”页面顶部包含下列有关 Firepower 机箱的信息：

  机箱名称 (Chassis name) - 显示初始配置期间分配给机箱的名称。

  IP 地址 (IP address) - 显示初始配置期间分配给机箱的管理 IP 地址。

  型号 (Model) - 显示 Firepower 机箱型号。

  版本 (Version) - 显示机箱上运行的 FXOS 的版本号。

  模式 (Mode) - 显示机箱的运行模式；独立或集群。

  总体状态 (Overall status) - 显示机箱的最高故障级别。

  机箱运行时间 (Chassis uptime) - 显示自上次系统重新启动以来所经过的时间。

  提示 您可以将光标悬停在“机箱运行时间 (Chassis uptime) 字段”右侧的图标上，查看安全模块/引擎的运行时间。

- 直观状态显示 (Visual Status Display) -“设备信息 (Device Information)”部分下面是机箱的直观展示图，显示机箱中安装的组件，并提供这些组件的常规状态。您可以将光标悬停在“直观状态显示 (Visual Status Display)”中显示的端口上，以获取更多信息，例如接口名称、速度、类型、管理状态和运行状态。对于带有多个安全模块的型号，您可以将光标悬停在“直观状态显

示 (Visual Status Display)”中显示的安全模块上，以获取更多信息，例如设备名称、模板类型、管理状态和运行状态。

- 详细状态信息 (Detailed Status Information) -“直观状态显示 (Visual Status Display)”下面有一个表，其中包含机箱的详细状态信息。状态信息分为五个部分：“故障 (Faults)”、“接口 (Interfaces)”、“设备 (Devices)”、“许可证 (License)”和“资产 (Inventory)”。您可以看到表上面各个部分的摘要，点击您想要查看信息的摘要区域，可以看到每个部分的更多详细信息。

  系统提供机箱的下列详细状态信息：

  故障 (Faults) - 列出系统中发生的故障。故障按严重性排序：“严重 (Critical)”、“主要 (Major)”、“次要 (Minor)”、“警告 (Warning)”和“信息 (Info)”。对于列出的每个故障，您可以查看严重性、故障描述、故障原因、发生次数以及最近发生时间。您还可以查看是否已确认故障。

  点击任何故障，可查看故障的更多详细信息或确认故障。

  注释 在消除了故障根源后，系统会在下个轮询间隔内自动将故障从列表中清除。如果用户正在想办法解决特定故障，他们可以确认故障，以便让其他用户了解当前正在处理故障。

  接口 (Interfaces) - 列出系统中安装的接口，提供每个接口的下列详细信息：接口名称、运行状态、管理状态、接收字节数以及传输字节数。

  您可以点击任何接口，查看以图形显示的最近 15 分钟内该接口的输入和输出字节数。

  设备 (Devices) - 列出在系统中配置的逻辑设备，提供每个逻辑设备的下列详细信息：设备名称、设备状态、应用模板类型、运行状态、管理状态、映像版本、管理IP地址和ASDM URL。

  许可证 (License) - 显示智能许可是否已启用，提供 Firepower 许可证的当前注册状态，并且显示机箱的许可证授权信息。

  资产 (Inventory) - 列出机箱中安装的组件，提供这些组件的相关详细信息，例如：组件名称、核心数量、安装位置、运行状态、互通性、容量、功率、温度、序列号、型号、部件号和供应商。

第 2 章

入门

任务流

以下程序显示配置 FXOS 机箱时应当完成的基本任务。

过程

步骤 1 配置 FXOS 机箱硬件（请参阅Cisco 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 6 页）。
步骤 3 登录 Firepower 机箱管理器（请参阅登录或注销 Firepower 机箱管理器， 第 8 页）。
步骤 4 设置日期和时间（请参阅设置日期和时间， 第 33 页）。
步骤 5 配置 DNS 服务器（请参阅配置 DNS 服务器， 第 54 页）。
步骤 6 注册产品许可证（请参阅许可证管理， 第 11 页）。
步骤 7 配置用户（请参阅用户管理， 第 17 页）。
步骤 8 按需执行软件更新（请参阅映像管理， 第 27 页）。
步骤 9 配置其他平台设置（请参阅平台设置， 第 31 页）。
步骤 10 配置接口（请参阅接口管理， 第 55 页）。
步骤 11 创建逻辑设备（请参阅逻辑设备， 第 59 页）。

初始配置

在您可以使用 Firepower 机箱管理器或 FXOS CLI 配置和管理您系统之前，必须使用通过控制台端口访问的 FXOS CLI 执行一些初始配置任务。当第一次使用 FXOS CLI 访问 FXOS 机箱时，您将会看到安装向导，您可以用它来配置系统。

您可以选择从现有的备份文件恢复系统配置，或者遍历安装向导手动设置系统。如果选择恢复系统，备份文件必须可从管理网络访问。

您必须为 FXOS 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 FXOS 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。

有关详细信息，请参阅 Cisco Firepower 安全设备硬件安装指南。

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如下所示：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

过程

步骤 1 连接到控制台端口。

步骤 2 打开 FXOS 机箱的电源。
在 FXOS 机箱启动时，您将看到开机自测消息。

步骤 3 当未配置的系统启动时，安装向导将提示您输入配置系统所需的下列信息：

- 设置模式（从完整系统备份或初始设置中恢复）
- 强密码执行策略（对于强密码准则，请参阅用户帐户，第 17 页）
- 管理员密码
- 系统名称
- 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

- DNS 服务器 IPv4 或 IPv6 地址
- 默认域名

步骤 4 检查安装摘要，输入 **yes**，保存并应用设置，或者输入 **no**，再次遍历安装向导更改某些设置。如果选择再次遍历安装向导，您之前输入的值将显示在括号中。要接受之前输入的值，请按 **Enter** 键。

以下示例使用 IPv4 管理地址设置配置：

```
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (y/n) [y]: n
Enter the password for "admin": adminpassword%958
Confirm the password for "admin": adminpassword%958
Enter the system name: foo
Physical Switch Mgmt0 IP address : 192.168.10.10
Physical Switch Mgmt0 IPv4 netmask: 255.255.255.0
IPv4 address of the default gateway: 192.168.10.1
Configure the DNS Server IP address? (yes/no) [n]: yes
  DNS IP address: 20.10.20.10
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Enforce Strong Password=no
  Physical Switch Mgmt0 IP Address=192.168.10.10
  Physical Switch Mgmt0 IP Netmask=255.255.255.0
  Default Gateway=192.168.10.1
  IPv6 value=0
  DNS Server=20.10.20.10
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

以下示例使用 IPv6 管理地址设置配置：

```
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (y/n) [y]: n
Enter the password for "admin": adminpassword%652
Confirm the password for "admin": adminpassword%652
Enter the system name: foo
Physical Switch Mgmt0 IP address :  2001::107
Physical Switch Mgmt0 IPv6 prefix: 64
IPv6 address of the default gateway: 2001::1
Configure the DNS Server IPv6 address? (yes/no) [n]: yes
  DNS IP address: 2001::101
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Enforced Strong Password=no
  Physical Switch Mgmt0 IPv6 Address=2001::107
  Physical Switch Mgmt0 IPv6 Prefix=64
  Default Gateway=2001::1
  Ipv6 value=1
  DNS Server=2001::101
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

登录或注销 Firepower 机箱管理器

过程

步骤 1 要登录 Firepower 机箱管理器，请执行以下操作：

a) 使用支持的浏览器，在地址栏中输入以下 URL：
https://<*chassis_mgmt_ip_address*>

其中 <*chassis_mgmt_ip_address*> 是您在初始配置期间输入的 FXOS 机箱的 IP 地址或主机名。

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

b) 输入您的用户名和密码。

c) 点击**登录 (Login)**。

您已登录，Firepower 机箱管理器打开以显示“概述 (Overview)”页面。

步骤 2 要注销Firepower 机箱管理器，请指向导航栏中的用户名，然后选择**注销 (Logout)**。
您已注销 Firepower 机箱管理器，并返回登录屏幕。

访问 FXOS CLI

您可以使用插入控制台端口的终端连接到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。Firepower 可扩展操作系统最多支持 8 个 SSH 并发连接。要使用 SSH 连接，您需要知道 FXOS 机箱的主机名或 IP 地址。

使用下列语法示例之一，通过 SSH、Telnet 或 Putty 登录：

注释 SSH 登录区分大小写。

使用 SSH 从 Linux 终端登录：

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

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

- **ssh -lucs-***auth-domain\\username {UCSM-ip-address| UCSM-ipv6-address| UCSM-host-name}*

```
ssh -l ucs-example\\jsmith 192.0.20.11
ssh -l ucs-example\\jsmith 2001::1
```

- **ssh** *{UCSM-ip-address | UCSM-ipv6-address | UCSM-host-name}* **-lucs-***auth-domain\\username*

```
ssh 192.0.20.11 -l ucs-example\\jsmith
ssh 2001::1 -l ucs-example\\jsmith
```

- **sshucs-***auth-domain\\username@{UCSM-ip-address|UCSM-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，第 34 页。

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

```
telnet ucs-qa-10
login: ucs-ldap23\blradmin
```

- **telnetucs-***{UCSM-ip-address|UCSM-ipv6-address}ucs-auth-domain\username*

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

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。

第 3 章

许可证管理

通过思科智能软件许可，您可以集中购买和管理许可证池。您可以轻松部署或停用设备，而不必管理每台设备的许可密钥。通过智能软件许可，您还可以直观地了解许可证使用情况和需求。

关于智能软件许可

本部分介绍智能软件许可的工作原理。

FXOS 机箱上的应用的智能软件许可

对于 FXOS 机箱上的 应用，智能软件许可配置分为两部分，分别在 FXOS 机箱管理引擎和应用中进行。

- FXOS 机箱 - 在管理引擎中配置所有智能软件许可基础设施，包括用于与许可证颁发机构进行通信的参数。FXOS 机箱本身不需要任何许可证即可运行。
- 应用 - 在应用中配置所有许可证授权。

智能软件管理器和帐户

为设备购买一个或多个许可证时，可在思科智能软件管理器中对这些许可证进行管理：

https://software.cisco.com/#module/SmartLicensing

通过智能软件管理器，您可以为组织创建一个主帐户。

注释 如果您还没有帐户，请点击链接设置新帐户。通过智能软件管理器，您可以为组织创建一个主帐户。

默认情况下，许可证分配给主帐户下的默认虚拟帐户。作为帐户管理员，您可以选择创建其他虚拟帐户；例如，您可以为区域、部门或子公司创建帐户。通过多个虚拟帐户，您可以更轻松地管理大量许可证和设备。

按虚拟帐户管理的许可证和设备

仅当虚拟帐户的设备可以使用分配给该帐户的许可证时，才能按虚拟帐户对许可证和设备进行管理。如果您需要其他许可证，则可以从另一个虚拟帐户传输未使用的许可证。您还可以在虚拟帐户之间迁移设备。

仅 FXOS 机箱注册为设备，而机箱中的 应用会请求自己的许可证。例如，对于有 3 个安全模块的 Firepower 9300 机箱，机箱算作一台设备，但这些模块使用 3 个独立许可证。

设备注册和令牌

对于每个虚拟帐户，可以创建注册令牌。默认情况下，此令牌有效期为30天。当部署每台设备时，或者注册现有设备时，请输入此令牌 ID 以及授权级别。如果现有令牌已过期，则可以创建新的令牌。

注释 设备注册在 FXOS 机箱管理引擎中配置，而不是在 安全模块上配置。

在完成部署后或在现有设备上手动配置这些参数后启动时，设备会向思科许可证颁发机构进行注册。当设备向令牌注册时，许可证颁发机构会为设备与许可证颁发机构之间的通信颁发ID证书。此证书有效期为 1 年，但需要每 6 个月续签一次。

与许可证颁发机构的定期通信

设备每30天与许可证颁发机构进行通信。如果您在智能软件管理器中进行更改，则可以刷新设备上的授权，以使更改立即生效。或者，也可以等待设备按计划通信。

您可以选择配置 HTTP 代理。设备必须可以直接访问互联网，或者至少每 90 天通过 HTTP 代理访问互联网。常规许可证通信每30天进行一次，但是，如果您的设备具有宽限期，则会最多运行90天，而不会进行自动通报。您必须在 90 天截止前与许可证颁发机构联系。

注释 不支持离线许可。

不合规状态

设备在以下情况下可能会处于不合规状态：

- 过度使用 - 当设备使用不可用许可证时。
- 许可证到期 - 当基于时间的许可证到期时。
- 通信不畅 - 当设备无法访问许可证颁发机构以重新获得授权时。

在 90 天重新授权尝试过后，设备将以某种方式受限，具体情况取决于应用。

Smart Call Home 基础设施

默认情况下，Smart Call Home 配置文件存在于配置中，指定许可授权机构的 URL。您无法删除此配置文件。请注意，许可证配置文件的唯一可配置选项是许可证颁发机构的目标地址 URL。除非获得 Cisco TAC 的指示，否则不应更改许可证颁发机构 URL。

无法针对智能软件许可禁用 Smart Call Home。

智能软件许可必备条件

- 在思科智能软件管理器上创建主帐户：

  https://software.cisco.com/#module/SmartLicensing

  如果您还没有帐户，请点击链接设置新帐户。通过智能软件管理器，您可以为组织创建一个主帐户。

- 从思科软件中心购买一个或多个许可证。
- 确保可从设备访问互联网或访问 HTTP 代理，以使设备能够联系许可颁发机构。不支持离线许可。
- 配置 DNS 服务器，以使设备能够解析许可颁发机构服务器的名称。请参阅配置 DNS 服务器，第 54 页。
- 设置设备时钟。请参阅设置日期和时间，第 33 页。

智能软件许可的默认设置

FXOS 机箱默认配置包括名为“SLProf”的 Smart Call Home 配置文件，该文件用于指定许可颁发机构的 URL。

配置智能软件许可

要与思科许可证颁发机构通信，您可以选择配置 HTTP 代理。要向许可证颁发机构注册，必须在 FXOS 机箱上输入您从智能软件许可证帐户获得的注册令牌 ID。

过程

步骤 1 （可选）配置 HTTP 代理，第 14 页。

步骤 2 向许可证颁发机构注册 Firepower 安全设备，第 14 页。

（可选）配置 HTTP 代理

如果您的网络使用 HTTP 代理进行互联网访问，则必须为智能软件许可配置代理地址。此代理一般也用于 Smart Call Home。

过程

步骤 1 选择**系统 (System)** > **许可 (Licensing)** > **Call Home**。
Call Home 页面提供用于配置许可证颁发机构的目标地址 URL 以及配置 HTTP 代理的字段。

注释 除非获得 Cisco TAC 的指示，否则不应更改许可证颁发机构 URL。

步骤 2 在“服务器启用 (Server Enable)”下拉列表中，选择**开 (on)**。

步骤 3 在**服务器 URL (Server URL)** 和 **服务器端口 (Server Port)** 字段中输入代理 IP 地址和端口。例如，为 HTTPS 服务器输入端口 443。

步骤 4 点击**保存 (Save)**。

向许可证颁发机构注册 Firepower 安全设备

当您注册 FXOS 机箱时，许可证颁发机构将签发一张 ID 证书用于 FXOS 机箱与许可证颁发机构之间的通信。它还会将 FXOS 机箱分配到相应的虚拟帐户。通常情况下，此程序是一次性实例。但是，如果 ID 证书由于通信问题等原因而过期，则稍后您可能需要重新注册 FXOS 机箱。

过程

步骤 1 在智能软件管理器中，为您希望将此 FXOS 机箱添加到的虚拟帐户请求并复制注册令牌。

步骤 2 在 Firepower 机箱管理器中，选择**系统 (System)** > **许可 (Licensing)** > **智能许可证 (Smart License)**。

步骤 3 在**输入产品实例注册令牌 (Enter Product Instance Registration Token)** 字段中输入注册令牌。

步骤 4 点击**注册 (Register)**。
FXOS 机箱尝试向许可证颁发机构注册。

要取消注册设备，请点击**取消注册 (Unregister)**。

对 FXOS 机箱注销会从帐户中删除设备。系统会删除设备上的所有许可证授权和证书。您可能要注销以释放许可证用于新的 FXOS 机箱。或者，也可以从智能软件管理器删除设备。

智能软件许可历史记录

功能名称	平台版本	说明
面向 FXOS 机箱的思科智能软件许可	1.1(1)	通过智能软件许可，您可以购买和管理许可证池。智能许可证不与特定序列号关联。您可以轻松部署或停用设备，而不必管理每台设备的许可密钥。通过智能软件许可，您还可以直观地了解许可证使用情况和需求。智能软件许可配置在 FXOS 机箱管理引擎和安全模块之间拆分。 我们引入了以下屏幕： **系统 (System)** > **许可 (Licensing)** > **Call Home** **系统 (System)** > **许可 (Licensing)** > **智能许可证 (Smart License)**

第 4 章

用户管理

用户帐户

用户帐户用于访问系统。最多可以配置48个本地用户帐户。每个用户帐户必须有唯一的用户名和密码。

管理员帐户

管理员帐户是默认用户帐户，不能修改或删除。此帐户是系统管理员或超级用户帐户，拥有完整权限。管理员帐户没有已分配的默认密码；您必须在初始系统设置中选择密码。

管理员帐户始终为活动状态，不会过期。不能将管理员帐户配置为非活动状态。

本地身份验证用户帐户

本地身份验证用户帐户直接通过机箱进行身份验证，并且可以由具有管理员或AAA权限的任何用户来启用或禁用。一旦本地用户帐户被禁用，该用户将无法登录。已禁用本地用户帐户的详细配置信息不会被数据库删除。如果您重新启用已禁用的本地用户帐户，此帐户将再次处于活动状态，且采用现有配置（包括用户名和密码）。

远程身份验证用户帐户

远程身份验证用户帐户是通过 LDAP、RADIUS 或 TACACS+ 进行身份验证的任意用户帐户。

如果用户同时持有本地用户帐户和远程用户帐户，则在本地用户帐户中定义的角色将覆盖在远程用户帐户中持有的角色。

用户帐户过期

用户帐户可以配置为在预定义时间过期。到了过期时间，用户帐户将被禁用。

默认情况下，用户帐户不会过期。

在为用户帐户配置过期日期后，无法将帐户重新配置为不过期。然而，您可以为帐户配置可用的最新过期日期。

用户名准则

用户名也可用作 Firepower 机箱管理器和 FXOS CLI 的登录 ID。当您为用户帐户分配登录 ID 时，请考虑以下准则和限制：

- 登录 ID 可以包含 1 到 32 个字符，包括以下字符：

  任意字母字符

  任意数字

  _（下划线）

  -（短划线）

  .（圆点）

- 登录 ID 必须唯一。
- 登录 ID 必须以字母字符开头。它不能以数字或特殊字符开头，例如下划线。
- 登录 ID 区分大小写。
- 不能创建全数字登录 ID。
- 创建用户帐户后，不能更改登录 ID。必须删除该用户帐户，创建新的用户帐户。

密码准则

密码对于每个本地认证的用户帐户都是必需的。拥有管理员或AAA权限的用户可以将系统配置为对用户密码执行密码强度检查。如果密码强度检查已启用，则每个用户必须使用强密码。

我们建议每个用户都使用强密码。如果对本地身份验证用户启用密码强度检查，Firepower可扩展操作系统将拒绝任何不符合以下要求的密码：

- 必须包含最少 8 个字符，最多 80 个字符。
- 必须包含至少以下三项：

  小写字母

  大写字母

  数字

特殊字符

- 不得包含连续重复 3 次以上的字符，例如 aaabbb。
- 不得包含三个连续数字，例如 password123。
- 不得与用户名相同，或与用户名正好相反。
- 必须通过密码词典检查。例如，密码不可以是标准词典单词。
- 不得包含以下符号：$（美元符号）、?（问号）和 =（等号）。
- 本地用户和管理员帐户的密码不得为空。

默认用户角色

系统包含下列默认用户角色：

管理员

对整个系统的完整读写访问权限。默认情况下，为默认管理员帐户分配此角色，不能更改。

只读

对系统配置的只读权限，无权修改系统状态。

本地身份验证用户的密码配置文件

密码配置文件包含所有本地身份验证用户的密码历史记录和密码更改时间间隔属性。您不能为每个本地身份验证用户指定不同的密码配置文件。

密码历史记录计数

借助密码历史记录计数，您可以阻止本地身份验证的用户反复使用同一密码。当配置此属性时，Firepower 机箱存储本地身份验证用户曾经使用的密码，最多存储 15 个密码。密码存储的顺序与时间顺序正好相反，最近的密码在前，这样可确保当达到历史记录计数阈值后仅重复使用最旧的密码。

用户必须创建和使用在密码历史记录计数中配置的密码数量，然后才能重新使用密码。例如，如果您将密码历史记录计数设置为 8，本地身份验证用户无法重新使用第一个密码，直至第九个密码过期为止。

默认情况下，密码历史记录设置为0。该值禁用历史记录计数，允许用户随时重新使用以前的密码。

如果需要，您可以清除本地身份验证用户的密码历史记录计数，启用重新使用以前的密码。

密码更改间隔

通过密码更改间隔，您可以限制本地身份验证用户在给定小时数内更改密码的次数。下表列出了密码更改间隔的两个配置选项。

间隔配置	说明	示例
不允许密码更改 (No password change allowed)	此选项不允许在密码更改之后的指定小时数内更改本地身份验证用户的密码。 您可以将无更改间隔指定为介于 1 和 745 小时之间。默认情况下，无更改间隔指定为 24 小时。	例如，要在本地身份验证用户更改其密码后 48 小时内阻止更改密码，请进行以下设置： • 间隔内更改设置为禁用 • 无更改间隔设置为 48
更改间隔内允许密码更改 (Password changes allowed within change interval)	此选项指定本地身份验证用户可以在预定义间隔内更改密码的最大次数。 您可以将更改间隔指定为介于 1 和 745 小时之间，密码更改最大次数介于 0 和 10 之间。默认情况下，允许本地身份验证用户在 48 小时间隔内最多执行 2 次密码更改。	例如，要在本地身份验证用户更改其密码后 24 小时内最多允许一次密码更改，请进行以下设置： • 间隔内更改设置为启用 • 更改计数设置为 1 • 更改间隔设置为 24

配置用户设置

过程

步骤 1 选择**系统 (System)** > **用户管理 (User Management)**。

步骤 2 点击**设置 (Settings)** 选项卡。

步骤 3 使用必填信息填写下列字段：

名称	说明
默认身份验证 (Default Authentication) 字段	在远程登录期间，对用户进行身份验证的默认方式。这可以是以下其中一项： • **本地 (Local)** - 必须在 Firepower 机箱本地定义用户帐户。 • **Radius** - 必须在为 Firepower 机箱指定的 RADIUS 服务器上定义用户帐户。 • **TACACS** - 必须在为 Firepower 机箱指定的 TACACS+ 服务器上定义用户帐户。 • **LDAP** - 必须在为 Firepower 机箱指定的 LDAP/MS-AD 服务器上定义用户帐户。 • **无 (None)** - 如果用户帐户是 Firepower 机箱的本地帐户，当用户在远程登录时，不需要密码。

名称	说明
远程用户设置	
远程用户角色策略	控制当用户尝试登录并且远程身份验证提供程序不向用户角色提供身份验证信息时发生的事情： • **分配默认角色 (Assign Default Role)** - 允许用户使用只读用户角色登录。 • **无登录 (No-Login)** - 不允许用户登录系统，即使用户名和密码正确也是如此。
本地用户设置	
密码强度检查 (Password Strength Check) 复选框	如果选中，所有本地用户密码都必须符合以下密码安全要求： • 必须包含最少 8 个字符，最多 80 个字符。 • 必须包含至少以下三项： 小写字母 大写字母 数字 特殊字符 • 不得包含连续重复 3 次以上的字符，例如 aaabbb。 • 不得包含三个连续数字，例如 password123。 • 不得与用户名相同，或与用户名正好相反。 • 必须通过密码词典检查。例如，密码不可以是标准词典单词。 • 不得包含以下符号：$（美元符号）、?（问号）和 =（等号）。 • 对于本地用户和管理员帐户不应为空。
历史记录计数 (History Count) 字段	用户可创建的密码数量。超过此数量后，使用只能使用先前已使用过的旧密码。历史记录计数的顺序与时间顺序正好相反，最近的密码在前，这样可确保当达到历史记录计数阈值后仅重复使用最旧的密码。 该值可以是介于 0 和 15 之间的任意值。 您可以将**历史记录计数 (History Count)** 字段设置为 0，这表示禁用历史记录计数，使用户随时都能够重复使用之前已使用的密码。

名称	说明
间隔内更改 (Change During Interval) 字段	控制本地验证用户何时能够更改其密码。该字段可以是： • **启用 (Enable)** - 本地身份验证用户可以根据“更改间隔 (Change Interval)”和“更改计数 (Change Count)”设置更改其密码。 • **禁用 (Disable)** - 本地身份验证用户不能在为“无更改间隔 (No Change Interval)”指定的期限内更改其密码。
更改间隔 (Change Interval) 字段	在其期间执行在**更改计数 (Change Count)** 字段中指定的密码更改次数的小时数。 该值可以是介于 1 和 745 小时之间的任意值。 例如，如果该字段设置为 48，**更改计数 (Change Count)** 字段设置为 2，那么本地身份验证用户在 48 小时内执行的密码更改不能超过 2 次。
更改计数 (Change Count) 字段	本地身份验证用户能够在“更改间隔 (Change Interval)”内更改其密码的最大次数。 该值可以是介于 0 和 10 之间的任意值。
无更改间隔 (No Change Interval) 字段	本地身份验证用户在更改新建密码之前必须等待的最少小时数。 该值可以是介于 1 和 745 小时之间的任意值。 如果未将**间隔期间更改 (Change During Interval)** 属性设置为**禁用 (Disable)**，该时间间隔将被忽略。

步骤 4 点击**保存 (Save)**。

创建本地用户帐户

过程

步骤 1 选择**系统 (System)** > **用户管理 (User Management)**。
步骤 2 点击**本地用户 (Local Users)** 选项卡。
步骤 3 点击**添加用户 (Add User)**，可打开**添加用户 (Add User)** 对话框。
步骤 4 使用关于用户的必填信息，填写下列字段：

名称	说明
用户名 (User Name) 字段	登录此帐户时使用的帐户名称。此帐户必须为唯一，且符合下列用户帐户准则和限制： • 登录 ID 可以包含 1 到 32 个字符，包括以下字符： 任意字母字符 任意数字 _（下划线） -（短划线） .（圆点） • 登录 ID 必须唯一。 • 登录 ID 必须以字母字符开头。它不能以数字或特殊字符开头，例如下划线。 • 登录 ID 区分大小写。 • 不能创建全数字登录 ID。 • 创建用户帐户后，不能更改登录ID。必须删除该用户帐户，创建新的用户帐户。 保存用户后，不能更改登录ID。必须删除该用户帐户，创建新的用户帐户。
名字 (Name) 字段	用户的名字。该字段最多包含 32 个字符。
姓氏 (Last Name) 字段	用户的姓氏。该字段最多包含 32 个字符。
电邮 (Email) 字段	用户的电邮地址。
电话号码 (Phone Number) 字段	用户的电话号码。

名称	说明
密码 (Password) 字段	与此帐户关联的密码。如果启用密码强度检查，用户的密码必须为强密码，Firepower可扩展操作系统会拒绝任何不满足下列要求的密码： • 必须包含最少 8 个字符，最多 80 个字符。 • 必须包含至少以下三项： 小写字母 大写字母 数字 特殊字符 • 不得包含连续重复 3 次以上的字符，例如 aaabbb。 • 不得包含三个连续数字，例如 password123。 • 不得与用户名相同，或与用户名正好相反。 • 必须通过密码词典检查。例如，密码不可以是标准词典单词。 • 不得包含以下符号：$（美元符号）、?（问号）和 =（等号）。 • 对于本地用户和管理员帐户不应为空。
确认密码 (Confirm Password) 字段	第二次用于确认目的的密码。
帐户状态 (Account Status) 字段	如果状态设置为**活动 (Active)**，用户可以登录使用此登录 ID 和密码登录 Firepower 机箱管理器和 FXOS CLI。
用户角色 (User Role) 下拉列表	表示您想分配给用户帐户的权限的角色： **管理员** 对整个系统的完整读写访问权限。默认情况下，为默认管理员帐户分配此角色，不能更改。 **只读** 对系统配置的只读权限，无权修改系统状态。

名称	说明
帐户到期 (Account Expires) 复选框	如果选中，在**到期日期 (Expiration Date)** 字段中指定的日期过后，此帐户将到期且无法使用。 **注释** 在为用户帐户配置过期日期后，无法将帐户重新配置为不过期。然而，您可以为帐户配置可用的最新过期日期。
到期日期 (Expiry Date) 字段	帐户到期日期。日期格式应为 yyyy-mm-dd。 点击此字段末尾的日历图标，查看您可以用来选择到期日期的日历。

步骤 5 点击**添加 (Add)**。

删除本地用户帐户

过程

步骤 1 选择**系统 (System)** > **用户管理 (User Management)**。
步骤 2 点击**本地用户 (Local Users)** 选项卡。
步骤 3 在与您想要删除的用户帐户对应的行中，点击**删除 (Delete)**。
步骤 4 在**确认 (Confirm)** 对话框中，点击**是 (Yes)**。

激活或停用本地用户帐户

您必须是拥有管理员或 AAA 权限的用户，才能激活或停用本地用户帐户。

过程

步骤 1 选择**系统 (System)** > **用户管理 (User Management)**。
步骤 2 点击**本地用户 (Local Users)** 选项卡。
步骤 3 在您要激活或停用的用户帐户所在的行中，点击**编辑 (Edit)**（铅笔图标）。
步骤 4 在**编辑用户 (Edit User)** 对话框中，执行以下操作之一：

- 要激活用户帐户，请点击**帐户状态 (Account Status)** 字段中的**活动 (Active)** 单选按钮。

- 要停用用户帐户，请点击**帐户状态 (Account Status)** 字段中的**非活动 (Inactive)** 单选按钮。

管理员用户帐户始终设置为活动。不能修改。

步骤 5 点击**保存 (Save)**。

第 5 章

映像管理

关于映像管理

FXOS 机箱使用的映像分为两个基本类型：

注释 所有映像都可通过安全启动进行数字签名和验证。请勿以任何方式修改映像，否则系统会报告验证错误。

- 平台捆绑包 (Platform Bundle) - Firepower 平台捆绑包是一系列运行在 Firepower 管理引擎和 Firepower 安全模块/引擎上的多个独立映像。平台捆绑包是 Firepower 可扩展操作系统软件包。
- 应用 (Application) - 应用是您想在 安全模块/引擎的FXOS 机箱上部署的软件映像。应用映像作为思科安全数据包文件 (CSP) 进行交付，在部署到安全模块/引擎之前，存储在管理引擎上，参与逻辑设备创建，或者为稍后的逻辑设备创建做准备。版本 1.1.1 是适用于 ASA 的唯一可用应用映像。您可以将同一应用映像类型的多个不同版本存储在 Firepower 管理引擎上。

注释 如果您正在升级平台捆绑包映像和一个或多个应用映像，必须首先升级平台捆绑包。

从 Cisco.com 下载映像

开始之前

您必须有 Cisco.com 帐户。

过程

步骤 1 选择**系统 (System)** > **更新 (Updates)**。
“可用更新 (Available Updates)”页面显示机箱上可用的 FXOS 平台捆绑包映像和应用映像列表。

步骤 2 点击页面底部的**从 CCO 下载最新更新 (Download latest updates from CCO)** 链接。
FXOS 机箱的软件下载页面可在浏览器中的新标签中打开。

步骤 3 查找适当的软件映像，然后将其下载到本地计算机。

将映像上传到 Firepower 安全设备

开始之前

确保您要上传的映像在本地计算机上可用。

过程

步骤 1 选择**系统 (System)** > **更新 (Updates)**。
“可用更新 (Available Updates)”页面显示机箱上可用的 Firepower 可扩展操作系统 平台捆绑包映像和应用映像列表。

步骤 2 点击**上传映像 (Upload Image)**，可打开“上传映像 (Upload Image)”对话框。

步骤 3 点击**浏览 (Browse)**，可导航到并选择想要上传的映像。

步骤 4 点击**上传 (Upload)**。
已选中的映像被上传到 FXOS 机箱。

升级 Firepower 可扩展操作系统平台捆绑包

开始之前

从 Cisco.com 下载平台捆绑包软件映像（请参阅从 Cisco.com 下载映像， 第 28 页），然后将此映像上传到 FXOS 机箱（请参阅将映像上传到 Firepower 安全设备， 第 28 页）。

过程

更新逻辑设备的映像版本

开始之前

从 Cisco.com 下载要用于逻辑设备的应用映像（请参阅从 Cisco.com 下载映像，第 28 页），然后将映像上传到 FXOS 机箱（请参阅将映像上传到 Firepower 安全设备，第 28 页）。

如果您正在升级平台捆绑包映像和一个或多个应用映像，必须首先升级平台捆绑包。

过程

步骤 1 选择**逻辑设备 (Logical Devices)**，可打开“逻辑设备 (Logical Devices)”页面。
“逻辑设备 (Logical Devices)”页面显示在机箱上配置的逻辑设备列表。如果尚未配置逻辑设备，系统将显示一条消息，要求您进行相关配置。

步骤 2 点击想要更新的逻辑设备对应的**更新版本 (Update Version)**，可打开**更新映像版本 (Update Image Version)** 对话框。

步骤 3 对于**新版本 (New Version)**，选择想要更新的软件版本。

步骤 4 点击**确定 (OK)**。

第 6 章

平台设置

更改管理 IP 地址

开始之前

您可以从 FXOS CLI 更改 FXOS 机箱上的管理 IP 地址。

注释 更改管理 IP 地址后，您需要使用新地址重新建立到 Firepower 机箱管理器或 FXOS CLI的任何连接。

过程

步骤 1 连接到 FXOS CLI（请参阅访问 FXOS CLI，第 8 页）。

步骤 2 要配置 IPv4 管理 IP 地址，请执行以下操作：

a) 设置交换矩阵互联 a 的范围：

Firepower-chassis# **scopefabric-interconnecta**

b) 要查看当前管理 IP 地址，请输入以下命令：
Firepower-chassis /fabric-interconnect # **show**

c) 输入以下命令，配置新的管理 IP 地址和网关：
Firepower-chassis /fabric-interconnect #
setout-of-bandip*ip_address***netmask***network_mask***gw***gateway_ip_address*

d) 确认系统配置任务：
Firepower-chassis /fabric-interconnect* # **commit-buffer**

步骤 3 要配置 IPv6 管理 IP 地址，请执行以下操作：

a) 设置交换矩阵互联 a 的范围：
Firepower-chassis# **scopefabric-interconnecta**

b) 设置管理 IPv6 配置的范围：
Firepower-chassis /fabric-interconnect # **scopeipv6-config**

c) 要查看当前管理 IPv6 地址，请输入以下命令：
Firepower-chassis /fabric-interconnect/ipv6-config # **show ipv6-if**

d) 输入以下命令，配置新的管理 IP 地址和网关：
Firepower-chassis /fabric-interconnect/ipv6-config #
setout-of-bandipv6*ipv6_address***ipv6-prefix***prefix_length***ipv6-gw***gateway_address*

e) 确认系统配置任务：
Firepower-chassis /fabric-interconnect/ipv6-config* # **commit-buffer**

以下示例配置 IPv4 管理接口和网关：

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    192.0.2.112     192.0.2.1       255.255.255.0   ::               ::
 64     Operable
Firepower-chassis /fabric-interconnect # set out-of-band ip 192.0.2.111 netmask 255.255.255.0
 gw 192.0.2.1
Warning: When committed, this change may disconnect the current CLI session
Firepower-chassis /fabric-interconnect* #commit-buffer
Firepower-chassis /fabric-interconnect #
```

以下示例配置 IPv6 管理接口和网关：

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                      Prefix     IPv6 Gateway
    --------------------------------- ---------- ------------
    2001::8998                        64         2001::1
```

```
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999
ipv6-prefix 64 ipv6-gw 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #
```

设置日期和时间

使用 NTP 页面手动设置日期和时间，或者配置 NTP 服务器。

注释 NTP 设置无法在 Firepower 机箱和任何安装在机箱上的应用之间同步。为确保正常运行，您必须在 Firepower 机箱中以及在机箱中运行的应用上配置相同的 NTP 设置。

使用 NTP 服务器设置日期和时间

NTP 用于实施分层服务器系统，可在网络系统中提供精确的同步时间。时间敏感性操作需要这种精确度，如验证 CRL，包括精确时间戳。

过程

步骤 1 选择**平台设置 (Platform Settings)** > **NTP**。

步骤 2 从**时区 (Time Zone)** 下拉列表中为 Firepower 机箱选择适当的时区。

步骤 3 在**设置时间来源 (Set Time Source)** 下面，点击**使用 NTP 服务器 (Use NTP Server)**，然后在 **NTP 服务器 (NTP Server)** 字段中输入想要使用的 NTP 服务器的 IP 地址或主机名。

步骤 4 点击**保存 (Save)**。
使用指定的 NTP 服务器配置 Firepower 机箱。

注释 如果系统时间修改超过 10 分钟，系统会将您注销，稍后，您需要再次登录 Firepower 机箱管理器。

手动设置日期和时间

本部分介绍如何在 Firepower 机箱上手动设置日期和时间。

过程

步骤 1 选择**平台设置 (Platform Settings)** > **NTP**。

步骤 2 从**时区 (Time Zone)** 下拉列表中为 Firepower 机箱选择适当的时区。

步骤 3 在**设置时间来源 (Set Time Source)** 下面，点击**手动设置时间 (Set Time Manually)**。

步骤 4 点击**日期 (Date)** 下拉列表，显示日历，然后使用日历中的可用控件设置日期。

步骤 5 使用对应的下拉列表将时间指定为小时、分钟和 AM/PM。

提示 您可以点击**获取系统时间 (Get System Time)**，设置日期和时间，以匹配您正在用来连接到 Firepower 机箱管理器的系统上所配置的日期和时间。

步骤 6 点击**保存 (Save)**。
使用指定的日期和时间配置 Firepower 机箱。

注释 如果系统时间修改超过 10 分钟，系统会将您注销，稍后，您需要再次登录 Firepower 机箱管理器。

配置 SSH

以下程序介绍如何启用或禁用对 Firepower 机箱的 SSH 访问。默认情况下，SSH 处于启用状态。

过程

步骤 1 选择**平台设置 (Platform Settings)** > **SSH**。

步骤 2 要启用到 Firepower 机箱的 SSH 访问，请选中**启用 SSH (Enable SSH)** 复选框。要禁用 SSH 访问，请取消选中**启用 SSH (Enable SSH)** 复选框。

步骤 3 点击**保存 (Save)**。

配置 Telnet

以下程序介绍如何启用或禁用对 Firepower 机箱的 Telnet 访问。默认情况下，Telnet 处于禁用状态。

注释 目前，Telnet 配置只有在使用 CLI 时才可使用。

过程

步骤 1 进入系统模式：
Firepower-chassis #**scope system**

步骤 2 进入系统服务模式：
Firepower-chassis /system #**scope services**

步骤 3 要配置对 Firepower 机箱的 Telnet 访问，请执行以下操作之一：

- 要允许对 Firepower 机箱进行 Telnet 访问，请输入以下命令：

  Firepower-chassis /system/services # **enable telnet-server**

- 要禁止对 Firepower 机箱进行 Telnet 访问，请输入以下命令：

  Firepower-chassis /system/services # **disable telnet-server**

步骤 4 确认系统配置任务：
Firepower /system/services # **commit-buffer**

以下示例启用 Telnet 并且确认任务：

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /services # enable telnet-server
Firepower-chassis /services* # commit-buffer
Firepower-chassis /services #
```

配置 SNMP

使用 SNMP 页面，在 Firepower 机箱上配置简单网络管理协议 (SNMP)。有关详细信息，请参阅以下主题：

关于 SNMP

简单网络管理协议 (SNMP) 是一个应用层协议，用于为 SNMP 管理器和代理之间的通信提供消息格式。SNMP 提供了标准化的框架和通用语言，可用于监控和管理网络中的设备。

SNMP 框架由三个部分组成：

- SNMP 管理器 - 用于使用 SNMP 控制和监控网络设备的活动的系统。
- SNMP 代理 - Firepower 机箱内的软件组件，用于维护 Firepower 机箱的数据，并按需向 SNMP 管理器报告数据。Firepower 机箱包括代理和一系列的 MIB。要启用 SNMP 代理并在管理器和代理之间创建关系，请在 Firepower 机箱管理器或 FXOS CLI 中启用和配置 SNMP。
- 管理信息库 (MIB) - SNMP 代理上的受管对象集合。

Firepower 机箱支持 SNMPv1、SNMPv2c 和 SNMPv3。SNMPv1 和 SNMPv2c 都使用基于社区形式的安全性。有关 SNMP 的定义，请参阅以下标准：

- RFC 3410 (http://tools.ietf.org/html/rfc3410)
- RFC 3411 (http://tools.ietf.org/html/rfc3411)
- RFC 3412 (http://tools.ietf.org/html/rfc3412)
- RFC 3413 (http://tools.ietf.org/html/rfc3413)
- RFC 3414 (http://tools.ietf.org/html/rfc3414)
- RFC 3415 (http://tools.ietf.org/html/rfc3415)
- RFC 3416 (http://tools.ietf.org/html/rfc3416)
- RFC 3417 (http://tools.ietf.org/html/rfc3417)
- RFC 3418 (http://tools.ietf.org/html/rfc3418)
- RFC 3584 (http://tools.ietf.org/html/rfc3584)

SNMP 通知

SNMP 的主要特性是能够从 SNMP 代理生成通知。这些通知不要求从 SNMP 管理器发送请求。通知可以指示不恰当的用户验证、重新启动、连接断开、到相邻路由器的连接丢失或其他重要事件。

Firepower 机箱生成 SNMP 通知，作为陷阱或通告。陷阱不如通告可靠，因为 SNMP 管理器在接收陷阱时不会发送任何确认信息，而且 Firepower 机箱无法确定陷阱是否已收到。接收通告请求的 SNMP 管理器通过 SNMP 响应协议数据单元 (PDU) 确认消息。如果 Firepower 机箱没有收到 PDU，它可以再次发送通告请求。

SNMP 安全等级和权限

SNMPv1、SNMPv2c 和 SNMPv3 分别代表不同的安全模型。安全模型与选中的安全等级相结合，确定处理 SNMP 消息时应用的安全机制。

安全等级确定查看与 SNMP 陷阱关联的消息所需的权限。权限等级确定消息是否需要保护以防止泄露或进行身份验证。支持的安全等级取决于实施哪种安全模型。SNMP 安全等级支持下列一个或多个权限：

- noAuthNoPriv - 无身份验证或加密
- authNoPriv - 身份验证，但无加密
- authPriv - 身份验证和加密

SNMPv3 同时提供了安全模型和安全等级。安全模型是为用户和用户所承担的角色而设置的身份验证策略。安全等级是安全模型中允许的安全级别。安全模型和安全级别两者共同决定了处理 SNMP 数据包时使用的安全机制。

支持的 SNMP 安全模型和级别组合

下表列出了安全模型和级别组合的含义。

表 *1*： *SNMP* 安全模型和级别

模型	级别	身份验证	加密	发生的事件
v1	noAuthNoPriv	社区字符串	否	使用社区字符串匹配进行身份验证。
v2c	noAuthNoPriv	社区字符串	否	使用社区字符串匹配进行身份验证。
V3	noAuthNoPriv	用户名	否	使用用户名匹配进行身份验证。
V3	authNoPriv	HMAC-SHA	否	提供基于 HMAC 安全散列算法 (SHA) 的身份验证。
V3	authPriv	HMAC-SHA	DES	提供基于 HMAC-SHA 算法的身份验证。除了基于密码块链 (CBC) DES (DES-56) 标准的身份验证，还提供数据加密标准 (DES) 56 位加密。

SNMPv3 安全功能

SNMPv3 通过将网络帧身份验证和加密结合在一起，提供对设备的安全访问。SNMPv3 仅授权已配置的用户执行管理操作，并加密 SNMP 消息。SNMPv3 基于用户的安全模型 (USM) 指的是 SNMP 消息级安全性，提供下列服务：

- 消息完整性 - 确保消息没有以未经授权的方式被更改或损坏，确保数据顺序的更改程度未超出非恶意性更改。
- 消息起源身份验证 - 确保已接收数据的起源用户的声明身份已得到确认。
- 消息保密性和加密 - 确保消息未被公布或披露给未经授权的个人、实体或进程。

SNMP 支持

Firepower 机箱为 SNMP 提供下列支持：

MIB 支持

Firepower 机箱支持对 MIB 的只读访问。

面向 SNMPv3 用户的身份验证协议

Firepower 机箱支持面向 SNMPv3 用户的 HMAC-SHA-96 (SHA) 身份验证协议。

面向 SNMPv3 用户的 AES 隐私协议

Firepower机箱使用高级加密标准 (AES) 作为用于SNMPv3 消息加密的一个隐私协议，并且符合 RFC 3826。

隐私密码或 priv 选项为 SNMP 安全加密提供 DES 或 128 位 AES 加密选项。如果您启用 AES-128 配置，并且包含 SNMPv3 用户的隐私密码，Firepower 机箱将使用此隐私密码生成 128 位 AES 密钥。AES 隐私密码至少有 8 个字符。如果口令用明文指定，您可以指定最多 64 个字符。

启用 SNMP 并配置 SNMP 属性

过程

步骤 1 选择**平台设置 (Platform Settings)** > **SNMP**。

步骤 2 在 **SNMP** 区域中，填写以下字段：

名称	说明
管理状态 (Admin State) 复选框	SNMP 已启用还是已禁用。仅当系统包含与 SNMP 服务器的集成时才启用此服务。
端口 (Port) 字段	Firepower 机箱与 SNMP 主机通信时使用的端口。无法更改默认端口。
社区/用户名 (Community/Username) 字段	Firepower 机箱在它发送给 SNMP 主机的任何陷阱消息中包含的默认 SNMP v1 或 v2 社区名或 SNMP v3 用户名。 输入介于 1 和 32 字符之间的字母数字字符串。请勿使用 @（at 号）、\（反斜线）、"（双引号）、?（问号）或空格。默认值为 public。

名称	说明
系统管理员姓名 (System Administrator Name) 字段	负责 SNMP 实施的联系人。 输入一个字符串，最多 255 个字符，例如电邮地址或姓名和电话号码。
位置 (Location)字段	SNMP 代理（服务器）运行所在的主机的位置。 输入一个字母数字字符串，最多 510 个字符。

步骤 3 点击**保存 (Save)**。

接下来的操作

创建 SNMP 陷阱和用户。

创建 SNMP 陷阱

过程

步骤 1 选择**平台设置 (Platform Settings)** > **SNMP**。

步骤 2 在 **SNMP 陷阱 (SNMP Traps)** 区域中，点击**添加 (Add)**。

步骤 3 在**添加 SNMP 陷阱 (Add SNMP Trap)** 对话框中，填写以下字段：

名称	说明
主机名 (Host Name) 字段	Firepower 机箱应向其发送陷阱的 SNMP 主机的主机名或 IP 地址。
社区/用户名 (Community/Username) 字段	向 SNMP 主机发送陷阱时，Firepower 机箱包含的 SNMP v1 或 v2 社区名或 SNMP v3 用户名。这必须与为 SNMP 服务配置的社区或用户名相同。 输入介于 1 和 32 字符之间的字母数字字符串。请勿使用 @（at 号）、\（反斜线）、"（双引号）、?（问号）或空格。
端口 (Port) 字段	Firepower 机箱与 SNMP 主机通信以布设陷阱时使用的端口。 输入一个介于 1 和 65535 之间的整数。

名称	说明
版本 (Version) 字段	用于陷阱的 SNMP 版本和型号。这可以是以下其中一项： • **V1** • **V2** • **V3**
类型 (Type) 字段	如果为版本选择 **V2** 或 **V3**，则是要发送的陷阱类型。这可以是以下其中一项： • **陷阱 (Traps)** • **告知 (Informs)**
v3 权限 (v3 Privilege) 字段	如果为版本选择 **V3**，与陷阱相关联的权限。这可以是以下其中一项： • **身份验证 (Auth)** - 有身份验证，但没有加密 • **无身份验证 (Noauth)** - 没有身份验证和加密 • **权限 (Priv)** - 有身份验证和加密

步骤 4 点击**确定 (OK)**，可关闭**添加 SNMP 陷阱 (Add SNMP Trap)** 对话框。

步骤 5 点击**保存 (Save)**。

删除 SNMP 陷阱

过程

步骤 1 选择**平台设置 (Platform Settings)** > **SNMP**。

步骤 2 在 **SNMP 陷阱 (SNMP Traps)** 区域中，在与您想要删除的陷阱对应的表的行中点击**删除 (Delete)** 图标。

创建 SNMPv3 用户

过程

步骤 1 选择**平台设置 (Platform Settings)** > **SNMP**。

步骤 2 在 **SNMP 用户 (SNMP Users)** 区域中，点击**添加 (Add)**。

步骤 3 在**添加 SNMP 用户 (Add SNMP User)** 对话框中，填写以下字段：

名称	说明
名称 (Name) 字段	分配给 SNMP 用户的用户名。 输入最多 32 个字母或数字。名称必须以字母开头，您还可以指定 _（下划线）、.（句号）、@（at 号）和 -（连字符）。
授权类型 (Auth Type) 字段	授权类型：**SHA**。
使用 AES-128 (Use AES-128) 复选框	如果选中，该用户将使用 AES-128 加密。
密码 (Password) 字段	该用户的密码：
确认密码 (Confirm Password) 字段	用于确认目的的再次输入的密码。
隐私密码 (Privacy Password) 字段	该用户的隐私密码。
确认隐私密码 (Confirm Privacy Password) 字段	用于确认目的的再次输入的隐私密码。

步骤 4 点击**确定 (OK)**，可关闭**添加 SNMP 用户 (Add SNMP User)** 对话框。

步骤 5 点击**保存 (Save)**。

删除 SNMPv3 用户

过程

步骤 1 选择**平台设置 (Platform Settings)** > **SNMP**。

步骤 2 在 **SNMP 用户 (SNMP Users)** 区域中，在与您想要删除的用户对应的表的行中点击**删除 (Delete)** 图标。

更改 HTTPS 端口

默认情况下，在端口 443 上启用 HTTPS 服务。您无法禁用 HTTPS，但可以更改端口，将其用于 HTTPS 连接。

过程

步骤 1 选择**平台设置 (Platform Settings)** > **HTTPS**。

步骤 2 在**端口 (Port)** 字段中输入要用于 HTTPS 连接的端口。指定一个介于 1 和 65535 之间的整数。默认情况下，在端口 443 上启用此服务。

步骤 3 点击**保存 (Save)**。
使用指定的 HTTPS 端口配置 Firepower 机箱。

更改 HTTPS 端口后，所有当前 HTTPS 会话都将关闭。用户需要使用新端口重新登录 Firepower 机箱管理器，如下所示：

https://<*chassis_mgmt_ip_address*>:<*chassis_mgmt_port*>

其中 <*chassis_mgmt_ip_address*> 是您在初始配置期间输入的 Firepower 机箱的 IP 地址或主机名，<*chassis_mgmt_port*> 是您刚刚配置的 HTTPS 端口。

配置 AAA

本部分介绍身份验证、授权和记帐。有关详细信息，请参阅以下主题：

关于 AAA

AAA 是一组服务，用于控制对计算机资源的访问、执行策略、评估使用情况并提供对服务进行计费所需的信息。这些过程对于高效进行网络管理和安全性而言至关重要。

身份验证

身份验证提供了一种标识用户的方法，这种方法通常先请用户输入有效用户名和有效密码，然后再授予访问权限。AAA服务器将用户的身份验证凭证与数据库中存储的其他用户凭证进行比较。如果凭证匹配，则允许用户访问网络。如果凭证不匹配，则身份验证失败，并拒绝网络访问。

您可以将 FXOS 机箱配置对机箱的管理连接进行身份验证，包括以下会话：

- HTTPS
- SSH
- 串行控制台

授权

授权是强制实施策略的过程：确定允许用户访问哪些类型的活动、资源或服务。对用户进行身份验证后，可能会授权该用户执行各种类型的访问或活动。

记帐

记帐用于测量用户在访问期间使用的资源量，这可以包括系统时间长度或者用户在会话期间发送或接收的数据量。记帐是通过记录会话统计信息和使用量信息来执行的，这些信息用于进行授权控制、计费、趋势分析、资源利用和容量规划活动。

身份验证、授权和记帐之间的交互

您可以单独使用身份验证功能，也可以将其与授权和记帐功能配合使用。授权始终要求先对用户进行身份验证。您可以单独使用记帐功能，也可以将其与身份验证和授权功能配合使用。

AAA 服务器

AAA服务器是用于进行访问控制的网络服务器。身份验证用于标识用户。授权实现策略，这些策略确定经过身份验证的用户能够访问哪些资源和服务。记帐对时间和数据资源进行追踪，这些资源用于计费和分析。

本地数据库支持

Firepower机箱维护本地数据库，您可以在其中填入用户配置文件。您可以使用本地数据库代替AAA服务器来提供用户验证、授权和记帐。

配置 LDAP 提供程序

配置 LDAP 提供程序的属性

在此任务中配置的属性对于此类型的所有提供程序连接而言是默认设置。如果单个提供程序包括任何这些属性的设置，Firepower 可扩展操作系统将使用该设置并忽略默认设置。

如果使用 Active Directory 作为 LDAP 服务器，请在 Active Directory 服务器中创建用户帐户以绑定 Firepower 可扩展操作系统。此帐户应具有永不过期的密码。

过程

步骤 1 选择**平台设置 (Platform Settings)** > **AAA**.

步骤 2 点击 **LDAP** 选项卡。

步骤 3 在**属性 (Properties)** 区域中，填写以下字段：

名称	说明
超时 (Timeout) 字段	在系统超时之前，系统尝试连接 LDAP 数据库时应花费的时间（以秒为单位）。 请输入一个介于 1 到 60 秒的整数。默认值为 30 秒。该属性为必填项。
属性 (Attribute) 字段	LDAP 属性，存储用户角色值和区域设置值。此属性始终是一个名称值对。系统在用户记录中查询匹配此属性名称的值。
基础 DN (Base DN) 字段	LDAP 层级结构中的特定区别名，在此层次结构中，当远程用户登录并且系统尝试根据其用户名获取用户的 DN 时，服务器应当开始搜索。基础 DN 的长度可以设置为最大 255 个字符减去 CN=$userid 的长度，其中，$userid 标识尝试使用 LDAP 身份验证访问 Firepower 机箱的远程用户。 该属性为必填项。如果您没有在此选项卡上指定基础 DN，则必须为自己定义的每个 LDAP 提供程序指定一个基础 DN。
过滤器 (Filter) 字段	LDAP 搜索仅限于那些匹配已定义过滤器的用户名。 该属性为必填项。如果您没有在此选项卡上指定过滤器，则必须为自己定义的每个 LDAP 提供程序指定一个过滤器。

步骤 4 点击**保存 (Save)**。

接下来的操作

创建 LDAP 提供程序。

创建 LDAP 提供程序

Firepower 可扩展操作系统最多支持 16 个 LDAP 提供程序。

开始之前

如果使用 Active Directory 作为 LDAP 服务器，请在 Active Directory 服务器中创建用户帐户以绑定 Firepower 可扩展操作系统。此帐户应具有永不过期的密码。

过程

步骤 1 选择**平台设置 (Platform Settings)** > **AAA**.

步骤 2 点击 **LDAP** 选项卡。

步骤 3 对于要添加的每个 LDAP 提供程序：

a) 在 **LDAP 提供程序 (LDAP Providers)** 区域中，点击**添加 (Add)**。

b) 在**添加 LDAP 提供程序 (Add LDAP Provider)** 对话框中，填写以下字段：

名称	说明
主机名/FDQN（或 IP 地址） (Hostname/FDQN (or IP Address))字段	LDAP 提供程序所驻留的主机名或 IP 地址。如果启用了 SSL，此字段必须精确匹配LDAP数据库安全认证中的通用名称(CN)。
顺序 (Order) 字段	Firepower可扩展操作系统使用此提供程序对用户进行身份验证的顺序。 输入一个介于 1 和 16 之间的整数，或者输入最低可用值或 0（零），前提是您想让 Firepower 可扩展操作系统根据在 Firepower 机箱管理器或 FXOS CLI 定义的其他提供程序分配下一个可用顺序。
绑定 DN (Bind DN) 字段	LDAP 数据库帐户的区别名 (DN)，对基础 DN 下的所有对象拥有读取和搜索权限。 支持的最大字符串长度为 255 个 ASCII 字符。
基础 DN (Base DN) 字段	LDAP 层级结构中的特定区别名，在此层次结构中，当远程用户登录并且系统尝试根据其用户名获取用户的 DN 时，服务器应当开始搜索。基础 DN 的长度可以设置为最大长度 255 个字符减去 CN=$userid 的长度，其中 $userid 标识尝试使用 LDAP 身份验证访问 Firepower 机箱管理器或 FXOS CLI 的远程用户。 该值为必填项，除非已在**LDAP**选项卡上设置了默认基础DN。
端口 (Port) 字段	Firepower 机箱管理器或 FXOS CLI 与 LDAP 数据库进行通信所使用的端口。标准端口号为 389。
启用 SSL (Enable SSL) 复选框	如果选中，需要对与 LDAP 数据库之间的通信进行加密。如果取消选中，身份验证信息将以明文发送。 LDAP 使用 STARTTLS。这允许使用端口 389 进行加密通信。

名称	说明
过滤器 (Filter) 字段	LDAP 搜索仅限于那些匹配已定义过滤器的用户名。 该值为必填项，除非已在 **LDAP** 选项卡上设置了默认过滤器。
属性 (Attribute) 字段	LDAP 属性，存储用户角色值和区域设置值。此属性始终是一个名称值对。系统在用户记录中查询匹配此属性名称的值。 该值为必填项，除非已在 **LDAP** 选项卡上设置了默认属性。
密钥 (Key) 字段	在**绑定 DN (Bind DN)** 字段中指定的 LDAP 数据库帐户的密码。您可以输入任意标准 ASCII 字符，但空格、§（分节号）、?（问号）或 =（等号）除外。
确认密钥 (Confirm Key)字段	重复用于确认目的的 LDAP 数据库密码。
超时 (Timeout) 字段	在系统超时之前，系统尝试连接 LDAP 数据库时应花费的时间（以秒为单位）。 输入一个介于 1 和 60 秒之间的整数，或者输入 0（零），以使用在 **LDAP** 选项卡上指定的全局超时值。默认值为 30 秒。
供应商 (Vendor) 字段	此选择标识提供 LDAP 提供程序或服务器详细信息的供应商： • 如果 LDAP 提供程序是 Microsoft Active Directory，请选择 **MS AD**。 • 如果 LDAP 提供程序不是 Microsoft Active Directory，请选择**打开 LDAP (Open LDAP)**。 默认值为**打开 LDAP (Open LDAP)**。

c）点击**确定 (OK)**，可关闭**添加 LDAP 提供程序 (Add LDAP Provider)** 对话框。

步骤 4 点击**保存 (Save)**。

删除 LDAP 提供程序

过程

步骤 1 选择平台设置 **(Platform Settings)** > **AAA**.

步骤 2 点击 **LDAP** 选项卡。

步骤 3 在 **LDAP 提供程序 (LDAP Providers)** 区域中，在与您想要删除的 LDAP 提供程序对应的表的行中点击删除 **(Delete)** 图标。

配置 RADIUS 提供程序

配置 RADIUS 提供程序的属性

在此任务中配置的属性对于此类型的所有提供程序连接而言是默认设置。如果单个提供程序包括任何这些属性的设置，Firepower 可扩展操作系统将使用该设置并忽略默认设置。

过程

步骤 1 选择平台设置 **(Platform Settings)** > **AAA**.

步骤 2 点击 **RADIUS** 选项卡。

步骤 3 在属性 **(Properties)** 区域中，填写以下字段：

名称	说明
超时 (Timeout) 字段	在系统超时之前，系统尝试连接 RADIUS 数据库时应花费的时间（以秒为单位）。 请输入一个介于 1 到 60 秒的整数。默认值为 5 秒。 该属性为必填项。
重试 (Retries) 字段	请求被视为失败之前的连接重试次数。

步骤 4 点击保存 **(Save)**。

接下来的操作

创建 RADIUS 提供程序。

创建 RADIUS 提供程序

Firepower 可扩展操作系统最多支持 16 个 RADIUS 提供程序。

过程

步骤 1 选择**平台设置 (Platform Settings)** > **AAA**.

步骤 2 点击 **RADIUS** 选项卡。

步骤 3 对于要添加的每个 RADIUS 提供程序：

a) 在 **RADIUS 提供程序 (RADIUS Providers)** 区域中，点击**添加 (Add)**。

b) 在**添加 RADIUS 提供程序 (Add RADIUS Provider)** 对话框中，填写以下字段：

名称	说明
主机名/FDQN（或 IP 地址）(Hostname/FDQN (or IP Address))字段	RADIUS 提供程序所驻留的主机名或 IP 地址。
顺序 (Order) 字段	Firepower 可扩展操作系统使用此提供程序对用户进行身份验证的顺序。 输入一个介于 1 和 16 之间的整数，或者输入最低可用值或 0（零），前提是您想让 Firepower 可扩展操作系统根据在 Firepower 机箱管理器或 FXOS CLI 定义的其他提供程序分配下一个可用顺序。
密钥 (Key) 字段	数据库 SSL 加密密钥。
确认密钥 (Confirm Key)字段	反复用于确认目的的 SSL 加密密钥。
授权端口 (Authorization Port) 字段	Firepower 机箱管理器或 FXOS CLI 与 RADIUS 数据库进行通信时使用的端口。有效范围为 1 至 65535。标准端口号为 1700。
超时 (Timeout) 字段	在系统超时之前，系统尝试连接 RADIUS 数据库时应花费的时间（以秒为单位）。 输入一个介于 1 和 60 秒之间的整数，或者输入 0（零），使用在 **RADIUS** 选项卡上指定的全局超时值。默认值为 5 秒。
重试 (Retries) 字段	请求被视为失败之前的连接重试次数。 如果需要，请输入一个介于 0 和 5 之间的整数。如果不指定该值，Firepower 机箱管理器将使用在 **RADIUS** 选项卡上指定的值。

c) 点击**确定 (OK)**，可关闭**添加 RADIUS 提供程序 (Add RADIUS Provider)** 对话框。

步骤 4 点击**保存 (Save)**。

删除 RADIUS 提供程序

过程

步骤 1 选择**平台设置 (Platform Settings)** > **AAA**.

步骤 2 点击 **RADIUS** 选项卡。

步骤 3 在 **RADIUS 提供程序 (RADIUS Providers)** 区域中，在与您想要删除的 RADIUS 提供程序对应的表的行中点击**删除 (Delete)** 图标。

配置 TACACS+ 提供程序

配置 TACACS+ 提供程序的属性

在此任务中配置的属性对于此类型的所有提供程序连接而言是默认设置。如果单个提供程序包括任何这些属性的设置，Firepower 可扩展操作系统将使用该设置并忽略默认设置。

过程

步骤 1 选择**平台设置 (Platform Settings)** > **AAA**.

步骤 2 点击 **TACACS** 选项卡。

步骤 3 在**属性 (Properties)** 区域中，填写以下字段：

名称	说明
超时 (Timeout) 字段	在系统超时之前，系统尝试连接 TACACS+ 数据库时应花费的时间（以秒为单位）。 请输入一个介于 1 到 60 秒的整数。默认值为 5 秒。 该属性为必填项。

步骤 4 点击**保存 (Save)**。

接下来的操作

创建 TACACS+ 提供程序。

创建 TACACS+ 提供程序

Firepower 可扩展操作系统最多支持 16 个 TACACS+ 提供程序。

过程

步骤 1 选择**平台设置 (Platform Settings)** > **AAA**.

步骤 2 点击 **TACACS** 选项卡。

步骤 3 对于您要添加的每个 TACACS+ 提供程序：

a) 在 **TACACS 提供程序 (TACACS Providers)** 区域中，点击**添加 (Add)**。

b) 在**添加 TACACS 提供程序 (Add TACACS Provider)** 对话框中，填写以下字段：

名称	说明
主机名/FDQN（或 IP 地址）(Hostname/FDQN (or IP Address))字段	TACACS+ 提供程序所驻留的主机名或 IP 地址。
顺序 (Order) 字段	Firepower可扩展操作系统使用此提供程序对用户进行身份验证的顺序。 输入一个介于 1 和 16 之间的整数，或者输入最低可用值或 0（零），前提是您想让 Firepower 可扩展操作系统根据在 Firepower 机箱管理器或 FXOS CLI 定义的其他提供程序分配下一个可用顺序。
密钥 (Key) 字段	数据库 SSL 加密密钥。
确认密钥 (Confirm Key)字段	反复用于确认目的的 SSL 加密密钥。
端口 (Port) 字段	Firepower 机箱管理器或 FXOS CLI与 TACACS+ 数据库进行通信时使用的端口。 输入一个介于 1 和 65535 之间的整数。默认端口为 49。
超时 (Timeout) 字段	在系统超时之前，系统尝试连接 TACACS+ 数据库时应花费的时间（以秒为单位）。 输入一个介于 1 和 60 秒之间的整数，或者输入 0（零），以使用在 **TACACS+** 选项卡上指定的全局超时值。默认值为 5 秒。

c) 点击**确定 (OK)**，可关闭**添加 TACACS 提供程序 (Add TACACS Provider)** 对话框。

步骤 4 点击**保存 (Save)**。

删除 TACACS+ 提供程序

过程

步骤 1 选择**平台设置 (Platform Settings)** > **AAA**.

步骤 2 点击 **TACACS** 选项卡。

步骤 3 在 **TACACS 提供程序 (TACACS Providers)** 区域中，在与您想要删除的 TACACS+ 提供程序对应的表的行中点击**删除 (Delete)** 图标。

配置系统日志

系统日志记录是将来自设备的消息收集到运行系统日志后台守护程序的服务器的方法。记录到中央系统日志服务器有助于汇聚日志和警报。系统日志服务接受消息并将其存储在文件中，或者根据简单配置文件将其打印。此形式的日志记录为日志提供受保护的长期存储。日志在例程故障排除和事件处理方面均有帮助。

过程

步骤 1 选择**平台设置 (Platform Settings)** > **系统日志 (Syslog)**。

步骤 2 配置本地目标：

a) 点击**本地目标 (Local Destinations)** 选项卡。

b) 在**本地目标 (Local Destinations)** 选项卡上，填写以下字段：

名称	说明
控制台 (Console) 部分	
管理状态 (Admin State) 字段	Firepower 机箱是否在控制台上显示系统日志消息。 如果您想在控制台上显示系统日志消息并将这些日志消息添加到日志中，请选中**启用 (Enable)** 复选框。如果取消选中**启用 (Enable)** 复选框，系统日志消息将会添加到日志中，但不会显示在控制台上。

名称	说明
级别 (Level) 字段	如果选中了**控制台 - 管理状态 (Console - Admin State)** 的**启用 (Enable)** 复选框，请选择您想在控制台上显示的最低消息级别。Firepower 机箱在控制台上显示此级别及以上消息。这可以是以下其中一项： • **紧急 (Emergencies)** • **警报 (Alerts)** • **严重 (Critical)**
监视器 (Monitor) 部分	
管理状态 (Admin State) 字段	Firepower 机箱是否在监视器上显示系统日志消息。 如果您想在监视器上显示系统日志消息并将这些日志消息添加到日志中，请选中**启用 (Enable)** 复选框。如果取消选中**启用 (Enable)** 复选框，系统日志消息将会添加到日志中，但不会显示在监视器上。
级别 (Level) 下拉列表	如果选中了**监视器 - 管理状态 (Monitor - Admin State)** 的**启用 (Enable)** 复选框，请选择您想在监视器上显示的最低消息级别。系统在监视器上显示此级别及以上消息。这可以是以下其中一项： • **紧急 (Emergencies)** • **警报 (Alerts)** • **严重 (Critical)** • **错误 (Errors)** • **警告 (Warnings)** • **通知 (Notifications)** • **信息 (Information)** • **调试 (Debugging)**

c) 点击**保存 (Save)**。

步骤 3 配置远程目标：

a) 点击**远程目标 (Remote Destinations)** 选项卡。

b) 在**远程目标 (Remote Destinations)** 选项卡上，为最多三个外部日志填写下列字段，这些日志可以存储 Firepower 机箱生成的消息：

通过将系统日志消息发送到远程目标，您可以根据外部系统日志服务器上的可用磁盘空间存档消息，并在保存日志记录数据后对其进行处理。例如，可以指定在记录某些类型的系统日志消息后要执行的操作，从日志提取数据并将记录保存到其他文件以进行报告，或者使用特定于站点的脚本跟踪统计信息。

名称	说明
管理状态 (Admin State) 字段	如果您想在远程日志文件中存储系统日志消息，请选中**启用 (Enable)** 复选框。
级别 (Level) 下拉列表	选择您想让系统存储的最低消息级别。系统在远程文件中存储此级别及以上消息。这可以是以下其中一项： • **紧急 (Emergencies)** • **警报 (Alerts)** • **严重 (Critical)** • **错误 (Errors)** • **警告 (Warnings)** • **通知 (Notifications)** • **信息 (Information)** • **调试 (Debugging)**
主机名/IP 地址 (Hostname/IP Address) 字段	远程日志文件所驻留的主机名或 IP 地址。 **注释** 如果使用主机名而不使用 IP 地址，必须配置 DNS 服务器。
设备 (Facility) 下拉列表	为系统日志服务器选择要用作文件消息基础的系统日志设备。这可以是以下其中一项： • **Local0** • **Local1** • **Local2** • **Local3** • **Local4** • **Local5** • **Local6** • **Local7**

c) 点击**保存 (Save)**。

步骤 4 配置本地来源：

a) 点击**本地来源 (Local Sources)** 选项卡。

b) 在**本地来源 (Local Sources)** 选项卡上，填写以下字段：

名称	说明
故障管理状态 (Faults Admin State) 字段	是否启用系统故障日志记录。如果选中**启用 (Enable)** 复选框，Firepower 机箱将记录所有系统故障。
审核管理状态 (Audits Admin State) 字段	是否启用审核日志记录。如果选中**启用 (Enable)** 复选框，Firepower 机箱将记录所有审核日志事件。
事件管理状态 (Events Admin State) 字段	是否启用系统事件日志记录。如果选中**启用 (Enable)** 复选框，Firepower 机箱将记录所有系统事件。

c) 点击**保存 (Save)**。

配置 DNS 服务器

如果系统要求将主机名解析为 IP 地址，您需要指定 DNS 服务器。例如，如果不配置 DNS 服务器，当您在 Firepower 机箱上配置设置时，不能使用 www.cisco.com 等名称。您可能需要使用服务器的 IP 地址，其可以是 IPv4 或 IPv6 地址。您最多可以配置 4 个 DNS 服务器。

注释 配置多个 DNS 服务器时，系统仅以任意随机顺序搜索服务器。如果本地管理命令要求 DNS 服务器查询，它只能以随机顺序搜索 3 个 DNS 服务器。

过程

步骤 1 选择**平台设置 (Platform Settings)** > **DNS**。

步骤 2 选中**启用 DNS 服务器 (Enable DNS Server)** 复选框。

步骤 3 对于您要添加的每个 DNS 服务器（最多 4 个），请在 **DNS 服务器 (DNS Server)** 字段中输入 DNS 服务器的 IP 地址，点击**添加 (Add)**。

步骤 4 点击**保存 (Save)**。

第 7 章

接口管理

关于 Firepower 安全设备接口

从 Firepower 机箱管理器的“接口 (Interfaces)”页面，您可以查看机箱上已安装接口的状态，编辑接口属性，启用或禁用接口，以及创建端口通道。

“接口 (Interfaces)”页面由两部分组成：

- 上半部分以直观的方式显示安装在 Firepower 机箱中的接口。您可以将鼠标悬停在任何接口的上方，获得关于此接口的更多信息。

  接口带有色标，表示其当前状态：

  绿色 - 接口已安装且已启用。

  深灰色 - 接口已安装，但被禁用。

  黄色 - 接口的运行状态存在问题。

  浅灰色 - 接口未安装。

- 下半部分包含安装在 Firepower 机箱中的接口的表。对于每个接口，您可以启用或禁用接口。您也可以点击**编辑 (Edit)** 编辑接口属性，例如速度和接口类型。

FXOS 机箱支持单个接口以及 EtherChannel（端口通道）接口。EtherChannel 接口最多可包含 16 个相同类型的成员接口。

每个接口可以是以下类型之一：

- 数据 (Data)（默认设置）- 不能在逻辑设备之间共享数据接口。
- 管理 (Management) - 可以在逻辑设备之间共享管理接口。您只能为每个逻辑设备分配一个管理接口。
- 集群 (Cluster) - 用于集群逻辑设备的特殊接口类型。此类型自动分配给集群控制链路，用于实现设备间集群通信。默认情况下，系统会在端口通道 48 上自动创建集群控制链路。

编辑接口属性

过程

步骤 1 选择**接口 (Interfaces)**，可打开“接口 (Interfaces)”页面。
“接口 (Interfaces)”页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 在您要编辑的接口所对应的行中点击**编辑 (Edit)**，可打开**编辑接口 (Edit Interface)** 对话框。

步骤 3 要启用接口，请选中**启用 (Enable)** 复选框。要禁用接口，请取消选中**启用 (Enable)** 复选框。

步骤 4 （可选）从**类型 (Type)** 下拉列表中选择**数据 (data)**，将此接口配置为数据接口，或者选择**管理 (mgmt)**，以将接口配置为管理接口。

注释 请勿选择**集群 (Cluster)** 类型。

步骤 5 （可选）从**速度 (Speed)** 下拉列表中选择接口速度。

步骤 6 点击**确定 (OK)**。

更改接口的管理状态

过程

步骤 1 选择**接口 (Interfaces)**，可打开“接口 (Interfaces)”页面。
“接口 (Interfaces)”页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 对于您想更改其管理状态的每个接口，请执行以下操作之一：

- 要将接口的管理状态设置为启用，请点击您想启用的接口的“状态 (State)”栏中的**已禁用 (Disabled)** 开关，将设置更改为**已启用 (Enabled)**。点击**是 (Yes)**，确认更改。

  接口的管理状态更改为已启用。以直观展示图表现的对应接口从灰色变为绿色。

- 要将接口的管理状态更改为已禁用，请点击您想禁用的接口的“状态 (State)”栏中的**已启用 (Enabled)** 开关，将设置更改为**已禁用 (Disabled)**。点击**是 (Yes)**，确认更改。

  接口的管理状态更改为已禁用。以直观展示图表现的对应接口从绿色变为灰色。

创建端口通道

EtherChannel（也称为端口通道）最多可以包含 16 个同一类型的成员接口。

开始之前

FXOS 机箱仅在有效链路汇聚控制协议 (LACP) 模式下支持 EtherChannel。我们建议将连接交换机端口设置为“活动 (Active)”模式，以实现最佳兼容性。

过程

步骤 1 选择**接口 (Interfaces)**，可打开“接口 (Interfaces)”页面。
“接口 (Interfaces)”页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 点击接口表上方的**添加端口通道 (Add Port Channel)**，可打开**添加端口通道 (Add Port Channel)** 对话框。

步骤 3 在**端口通道 ID (Port Channel ID)** 字段中输入端口通道 ID。有效值介于 1 和 47 之间。
部署集群逻辑设备时，端口通道 48 为集群控制链路预留。如果不想将端口通道 48 用于集群控制链路，您可以为 EtherChannel 配置不同的 ID，为接口选择“集群 (Cluster)”类型。不要将任何接口分配给集群 EtherChannel。

步骤 4 要启用端口通道，请选中**启用 (Enable)** 复选框。要禁用端口通道，请取消选中**启用 (Enable)** 复选框。

步骤 5 从**类型 (Type)** 下拉列表中选择端口通道类型：**数据 (Data)**、**管理 (Mgmt)** 或**集群 (Cluster)**。

步骤 6 如果未选中，请点击**接口 (Interfaces)** 选项卡。

步骤 7 要将接口添加到端口通道，请在**可用接口 (Available Interface)** 列表中选择该接口，点击**添加接口 (Add Interface)**，将接口移动至“成员 ID (Member ID)”列表。您最多可以添加 16 个同一类型和速度的接口。

提示 一次可添加多个接口。要选择多个独立接口，请点击所需的接口，同时按住 **Ctrl** 键。要选择一个接口范围，请选择范围中的第一个接口，然后，在按住 **Shift** 键的同时，点击选择范围中的最后一个接口。

步骤 8 要从端口通道删除接口，请点击“成员 ID (Member ID)”列表中接口右侧的**删除 (Delete)** 按钮。

步骤 9 点击**设置 (Settings)** 选项卡。

步骤 10 从**速度 (Speed)** 下拉列表中选择端口通道的速度。

步骤 11 点击**确定 (OK)**。

配置分支线缆

以下程序介绍如何配置分支线缆以供FXOS机箱使用。您可以使用分支线缆提供4个10 Gbps端口，代替单个 40 Gbps 端口。

过程

步骤 1 选择**接口 (Interfaces)**，可打开“接口 (Interfaces)”页面。
“接口(Interfaces)”页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

接口对应的行中的“分支端口(Breakout Port)”图标表示能够支持分支线缆但当前未配置为支持的接口。对于已配置为使用分支线缆的接口，分别列出各个分支接口（例如，以太网2/1/1、2/1/2、2/1/3和2/1/4）。

步骤 2 要将 40 Gbps 接口转换为 4 个 10 Gbps 接口，请执行以下操作：

a) 点击您想转换的接口所对应的**分支端口 (Breakout Port)** 图标。
“创建分支端口(Breakout Port Creation)”对话框打开，要求您确认是否想要继续，并警告您机箱将被重启。

b) 点击**是 (Yes)** 进行确认。
Firepower 机箱重启，指定接口转换为 4 个 10 Gbps 接口。

步骤 3 要将 4 个 10 Gbps 分支接口转换回单个 40 Gbps 接口，请执行以下操作：

a) 点击任意分支接口所对应的 **删除 (Delete)**。
确认对话框打开，要求您确认是否想要继续，并警告您全部4个分支接口都将被删除，机箱将重启。

b) 点击**是 (Yes)** 进行确认。
Firepower 机箱重启，指定的接口转换为单个 40 Gbps 接口。

第 8 章

逻辑设备

关于逻辑设备

使用 Firepower 机箱管理器的“逻辑设备 (Logical Devices)”页面创建、编辑和删除逻辑设备。

当您创建逻辑设备时，FXOS 机箱管理引擎会部署逻辑设备，方法是下载指定软件版本，将引导程序配置和管理接口设置推送到指定的安全模块/引擎，或者，如果是机箱内集群，则推送到安装在 Firepower 机箱内的所有安全模块。

您可以创建以下两类逻辑设备之一：

注释 在支持多个安全模块的FXOS机箱上，只能以独立或集群方式创建一类逻辑设备。换句话说，如果您已安装三个安全模块，则不能在一个安全模块上创建独立逻辑设备，使用剩余的两个逻辑设备创建集群。

- 独立 (Standalone) - 您可以为安装在 Firepower 机箱中的每个安全模块/引擎创建独立逻辑设备。
- 集群 (Cluster) - 通过集群，您可以将多个安全模块组合成一个逻辑设备。集群具有单台设备的全部便捷性（管理、集成到一个网络中），同时还能提高吞吐量并实现多台设备的冗余性。Firepower 9300 等多模块设备支持机箱内集群。

创建独立的 ASA 逻辑设备

您可以为 FXOS 机箱中安装的每个 安全模块/引擎 创建独立逻辑设备。在 Firepower 9300 等多模块设备上，如果您已配置了集群，则无法创建独立逻辑设备。您需要删除集群，然后才能配置独立设备。

开始之前

- 如果您想用于逻辑设备的安全模块/引擎上已配置了逻辑设备，必须首先删除现有的逻辑设备（请参阅删除逻辑设备）。
- 从 Cisco.com 下载要用于逻辑设备的应用映像（请参阅从 Cisco.com 下载映像，第 28 页），然后将映像上传到 FXOS 机箱（请参阅将映像上传到 Firepower 安全设备，第 28 页）。
- 配置逻辑设备要使用的管理接口。

过程

步骤 1 选择**逻辑设备 (Logical Devices)**，可打开“逻辑设备 (Logical Devices)”页面。
“逻辑设备 (Logical Devices)”页面显示在机箱上配置的逻辑设备列表。如果尚未配置逻辑设备，系统将显示一条消息，要求您进行相关配置。

步骤 2 点击**添加设备 (Add Device)**，可打开**添加设备 (Add Device)** 对话框。

步骤 3 对于**设备名称 (Device Name)**，请为逻辑设备提供一个名称。

步骤 4 对于**模板 (Template)**，请选择**思科自适应安全设备 (Cisco Adaptive Security Appliance)**。

步骤 5 对于**映像版本 (Image Version)**，请选择 ASA 软件版本。

步骤 6 对于**设备模式 (Device Mode)**，请点击**独立 (Standalone)** 单选按钮。

步骤 7 点击**确定 (OK)**。
屏幕将显示调配 - 设备名称 *(Provisioning - device name)* 窗口。

步骤 8 展开**数据端口 (Data Ports)** 区域，然后点击要分配给设备的每个端口。

步骤 9 点击屏幕中心的设备图标。
系统将显示“ASA 配置 (ASA Configuration)”对话框。

步骤 10 在**一般信息 (General Information)** 选项卡上，完成下列操作：

a) 在 Firepower 9300 等多模块设备上，在“安全模块选择 (Security Module Selection)”下面，点击您想用于此逻辑设备的安全模块，将其选中。

b) 从**管理接口 (Management Interface)** 下拉列表中选择逻辑设备要使用的管理接口。

c) 在默认情况下，配置管理接口：
此信息用于配置安全模块/引擎配置中的管理接口。此管理 IP 地址也是将用于连接 ASDM 的 IP 地址。

1. 从**地址类型 (Address Type)** 下拉列表中选择地址类型。
2. 在**管理 IP (Management IP)** 字段中，配置本地 IP 地址。

3 输入**网络掩码 (Network Mask)** 或**前缀长度 (Prefix Length)**。

4 输入**网络网关 (Network Gateway)** 地址。

步骤 11 在**设置 (Settings)** 选项卡中，在**密码 (Password)** 字段中输入“管理员 (admin)”用户的密码。

步骤 12 点击**确定 (OK)**，可关闭“ASA 配置 (ASA Configuration)”对话框。

步骤 13 点击**保存 (Save)**。

Firepower可扩展操作系统通过下载指定的软件版本，并将引导程序配置和管理接口设置推送到指定的安全模块/引擎来部署逻辑设备。

部署集群

通过集群，您可以将多个安全模块组合成一个逻辑设备。集群具有单台设备的全部便捷性（管理、集成到一个网络中），同时还能提高吞吐量并实现多台设备的冗余性。Firepower 9300 等多模块设备支持机箱内集群。

注释 Firepower 9300 不支持跨多个机箱（机箱间）的集群；仅支持机箱内集群。

关于 FXOS 机箱上的集群

集群由多台设备组成，这些设备作为一个整体运行。当您在FXOS 机箱 上部署集群时，它执行以下操作：

- 为设备到设备通信创建集群控制链路（端口通道48）。对于机箱内集群，此链路利用Firepower 9300背板进行集群通信。
- 在应用内创建集群引导程序配置。

  部署集群时，FXOS 机箱 管理引擎向包含此集群名称、集群控制链路接口和其他集群设置的每台设备推送最低引导程序配置。如果您需要自定义集群环境，可以在应用内对引导程序配置的某些用户可配置部分进行配置。
- 将数据接口作为跨网络接口分配给集群。

  对于机箱内集群，跨网络接口不仅限于 EtherChannel，与机箱间集群类似。Firepower 9300管理引擎在内部利用 EtherChannel 技术，将流量负载均衡到共享接口上的多个模块，使任何数据接口类型都可用于跨网络模式。

注释 不支持单个接口，但管理接口除外。

- 向集群中的所有设备分配管理接口。

以下部分将更加详细地介绍集群概念和实施。

主设备和从设备角色

集群的一个成员是主设备。自动确定主设备。所有其他成员均为从设备。

您必须仅在主设备上执行所有配置；随后，配置将被复制到从设备。

集群控制链路

使用端口通道48接口自动创建集群控制链路。对于机箱内集群，此接口没有成员接口。此集群类型EtherChannel 利用 Firepower 9300 背板进行集群通信，实现机箱内集群。

集群控制链路流量包括控制流量和数据流量。

管理界面

您可以将管理类型接口分配给集群。与跨网络接口相比，此接口是一个特殊的独立接口。通过管理接口，可以直接连接每台设备。

对于ASA，主集群IP地址是集群的固定地址，始终属于当前的主设备。还要配置一个地址范围，以便包括当前主设备在内的每台设备都可以使用该范围内的本地地址。主集群 IP 地址提供对地址的统一管理访问权限；当主设备更改时，主集群 IP 地址将转移给新的主设备，使集群管理可以无缝衔接。本地 IP 地址用于路由，在故障排除时也非常有用。例如，您可以通过连接到主集群 IP 地址来管理集群，该地址始终属于当前的主设备。要管理单个成员，您可以连接到本地IP地址。对于TFTP或系统日志等出站管理流量，包括主设备在内的每台设备都使用本地 IP 地址连接到服务器。

集群准则

- 我们建议将 EtherChannel 连接到 VSS 或 vPC，以实现冗余。
- 在机箱内，您不能对某些安全模块进行集群，也不能在单机模式下运行其他安全模块；必须在集群内包含所有安全模块。

集群默认设置

集群控制链路使用端口通道 48。

配置 ASA 集群

您可以从 FXOS 机箱管理引擎轻松部署集群。自动为每台设备生成所有初始配置。

过程

步骤 1 部署集群之前，至少添加一个“数据 (Data)”类型接口或 EtherChannel（也称为端口通道）。请参阅创建端口通道，第 57 页或编辑接口属性，第 56 页。
部署之后，您也可以将数据接口添加到集群。

步骤 2 添加“管理 (Management)”类型接口或 EtherChannel。请参阅创建端口通道，第 57 页或编辑接口属性，第 56 页。

步骤 3 选择**逻辑设备 (Logical Devices)**，可打开“逻辑设备 (Logical Devices)”页面。
“逻辑设备 (Logical Devices)”页面显示在机箱上配置的逻辑设备列表。如果尚未配置逻辑设备，系统将显示一条消息，要求您进行相关配置。

步骤 4 点击**添加设备 (Add Device)**，可打开**添加设备 (Add Device)** 对话框。
如果您目前有一个集群，系统将提示您删除该集群并添加新集群。安全模块上的所有集群相关配置将被新信息代替。

步骤 5 对于**设备名称 (Device Name)**，请为逻辑设备提供一个名称。FXOS 机箱管理引擎使用该名称配置集群设置以及分配接口；该名称不是在安全模块配置中使用的集群名称。

步骤 6 对于**模板 (Template)**，请选择**思科自适应安全设备 (Cisco Adaptive Security Appliance)**。

步骤 7 对于**映像版本 (Image Version)**，请选择 ASA 软件版本。

步骤 8 对于**设备模式 (Device Mode)**，请点击**集群 (Cluster)** 单选按钮。

步骤 9 点击**确定 (OK)**。
如果您配置了任何独立设备，系统将提示您用新集群替代它们。屏幕将显示调配 - 设备名称 *(Provisioning - device name)* 窗口。

默认情况下，所有接口都会分配给集群。

步骤 10 点击屏幕中心的设备图标。
系统将显示“ASA 配置 (ASA Configuration)”对话框，其中**集群信息 (Cluster Information)** 选项卡已选定。

步骤 11 在**集群密钥 (Cluster Key)** 字段中，为集群控制链路上的控制流量配置身份验证密钥。
共享密钥是长度介于 1 和 63 个字符之间的 ASCII 字符串。共享密钥用于生成密钥。此选项不影响数据路径流量，包括连接状态更新和转发的数据包，它们始终以明文发送。

步骤 12 设置**服务类型名称 (Service Type Name)**，这是安全模块配置中的集群组名称。
名称必须是长度介于 1 和 38 个字符之间的 ASCII 字符串。

步骤 13 点击**管理接口 (Management Interface)**，选择您之前创建的管理接口。

步骤 14 选择管理接口的**地址类型 (Address Type)**。
此信息用于配置安全模块配置中的管理接口。

a) 在**管理 IP 池 (Management IP Pool)** 字段中，配置本地 IP 地址池，其中一个地址将分配给接口的每个集群设备，方法是输入以连字符分隔的起始地址和结束地址。
至少包含与集群中的设备数量相同的地址。如果计划扩展集群，则应包含更多地址。属于当前主设备的虚拟 IP 地址（称作“主集群 IP 地址”）不在此地址池中；请务必在同一个网络中为主集群 IP 地址保留一个 IP 地址。您可以使用 IPv4 和/或 IPv6 地址。

b) 输入**网络掩码 (Network Mask)** 或**前缀长度 (Prefix Length)**。
c) 输入**网络网关 (Network Gateway)**。
d) 输入**虚拟 IP 地址 (Virtual IP address)**。
此 IP 地址必须与集群池地址属于同一个网络，但不在地址池中。

步骤 15 在**设置 (Settings)** 选项卡中，对于**密码 (Password)**，输入“管理员 (admin)”用户的密码。

步骤 16 点击**确定 (OK)**，可关闭“ASA 配置 (ASA Configuration)”对话框。

步骤 17 点击**保存 (Save)**。
FXOS 机箱管理引擎通过下载指定的软件版本并向每个安全模块推送集群引导程序配置和管理接口设置来部署集群。

步骤 18 连接到主设备安全模块以自定义集群配置。

集群历史记录

功能名称	平台版本	功能信息
对 Cisco ASA 进行机箱内集群	1.1.1	您可以对 Firepower 9300 机箱内的所有 ASA 安全模块创建集群。 我们引入了以下屏幕：**逻辑设备 (Logical Devices)** > **配置 (Configuration)**

连接到应用或修饰程序的控制台

使用以下程序连接至应用或修饰程序的控制台。

注释 如果您在访问控制台时遇到任何问题，我们建议您尝试不同的 SSH 客户端，或者将 SSH 客户端升级到较新的版本。

过程

步骤 1 要连接至应用或修饰程序的控制台，请执行以下操作：

a) 从 FXOS CLI，连接至安全模块/引擎：
Firepower-chassis # **connectmodule***slot_number***console**

注释 要连接至不支持多个安全模块的设备的安全引擎，请使用 1 作为 *slot_number*。

首次连接到安全模块时，您会进入 FXOS 模块 CLI。

b) 要连接到应用或修饰程序，请输入：
Firepower-module1>**connect asa**

从 FXOS CLI 的管理引擎层到安全模块/引擎的后续连接直接访问安全模块/引擎操作系统。

步骤 2 （可选） 键入 **Ctrl-A-D**，使应用控制台返回到 FXOS 模块 CLI。
出于故障排除目的，您可能想访问 FXOS 模块 CLI。

步骤 3 返回 FXOS CLI 的管理引擎层。

a) 要退出安全模块/引擎控制台，请键入 ~。
您将退出至 Telnet 应用。

b) 要退出 Telnet 应用，请输入：
telnet>**quit**

示例

以下示例连接至安全模块 1 上的 ASA，然后返回到 FXOS CLI 的管理引擎层。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa
asa> ~
telnet> quit
Connection closed.
Firepower#
```

索 引

字母

B

C

D

F

G

J

L

M

P

Q

R

S

T

X

Y

Z