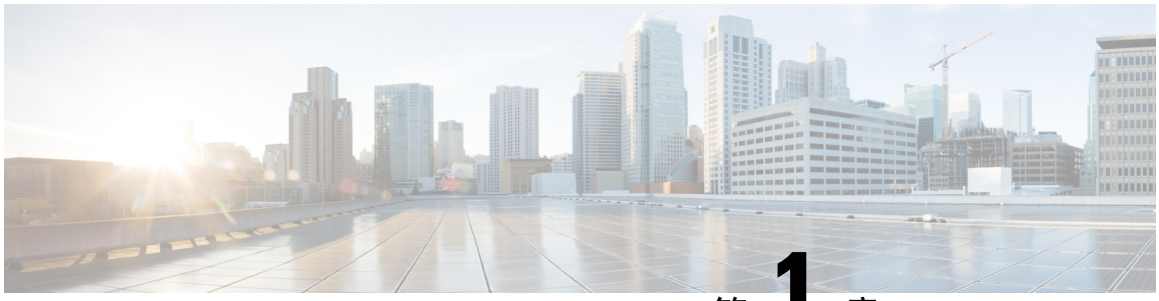
Cisco Firepower 2100 ASA 平台模式 FXOS 配置指南

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

目录



第 1 章

Firepower 2100 ASA 平台模式下的 FXOS 简介

Firepower 2100 是适用于 ASA 的单一应用程序设备。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。

本指南介绍仅适用于平台模式的 FXOS 设置。

- ASA 和 FXOS 管理，第 1 页
- 不支持的功能，第 2 页

ASA 和 FXOS 管理

ASA 和 FXOS 操作系统共享管理 1/1 接口。此接口拥有单独的 IP 地址，用于连接到 ASA 和 FXOS。

注释 此接口在 ASA 中被称为管理 1/1；在 FXOS 中，您可能会看到它显示为 MGMT、management0 或其他类似名称。本指南将此接口称为管理 1/1，以保持一致性和简洁性。

某些功能必须在 FXOS 上进行监控，而其他功能则必须在 ASA 上进行监控，因此您需要利用这两个操作系统进行持续维护。对于 FXOS 上的初始配置，您可以使用 SSH 或您的浏览器 (https://192.168.45.45) 连接到默认的 192.168.45.45 IP 地址。

对于 ASA 的初始配置，您可以使用 ASDM 连接到 https://192.168.45.1/admin。在 ASDM 中，您可以以后从任何接口配置 SSH 访问。

这两个操作系统都可从控制台端口获得。初始连接将访问 FXOS CLI。您可以使用 **connect asa** 命令来访问 ASA CLI。

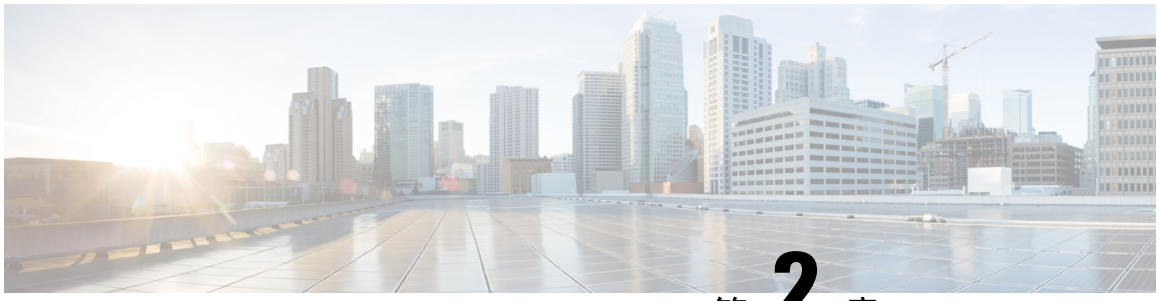
您还可以允许从 ASA 数据接口进行 FXOS 管理；配置 SSH、HTTPS 和 SNMP 访问。此功能对远程管理非常有用。

不支持的功能

Firepower 2100 不支持以下 FXOS 功能：

- 备份与还原 FXOS 配置
- FXOS 的外部 AAA 身份验证

  请注意，当您从 FXOS (**connect asa**) 连接到 ASA 控制台时，会应用适用于控制台访问的 ASA AAA 配置 (**aaa authentication serial console**)。



第 2 章

Firepower 机箱管理器设置

Firepower 2100 运行 FXOS 来控制设备的基本操作。您可以使用 GUI Firepower 机箱管理器或 FXOS CLI 来配置这些功能；本文档涵盖了 Firepower 机箱管理器的内容。请注意，所有安全策略和其他操作都是在 ASA OS 中配置的（使用 CLI 或 ASDM）。

概述

在**概述 (Overview)** 选项卡上，您可以轻松监控 Firepower 2100 的状态。**概述 (Overview)** 选项卡提供下列元素：

- 设备信息 (Device Information) - **概述 (Overview)** 选项卡顶部包含下列有关 Firepower 2100 的信息：
  - 机箱名称 (Chassis name) - 显示分配给机箱的名称。默认情况下，该名称为 **firepower-**型号，例如 firepower-2140。此名称显示在 CLI 提示符中。要更改机箱名称，请使用 FXOS CLI **scope system / set name** 命令。
  - IP 地址 (IP address) - 显示分配给机箱的管理 IP 地址。
  - 型号 (Model) - 显示 Firepower 2100 的型号。
  - 版本 (Version) - 显示在机箱上运行的 ASA 的版本号。
  - 运行状态 (Operational State) - 显示机箱的运行状态。
  - 机箱正常运行时间 (Chassis uptime) - 显示自从系统上次重新启动后经过的时间。

- 正常运行时间信息 (Uptime Information) 图标 - 将光标悬停在该图标上可以查看机箱和 ASA 安全引擎的正常运行时间。

- 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。
- 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。状态信息分为以下部分：“故障 (Faults)”、“接口 (Interfaces)”、“设备 (Devices)”和“资产 (Inventory)”。您可以看到表上面各个部分的摘要，单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。

  系统为机箱提供以下详细状态信息：

  - **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)”。对于所列的每个故障，可以查看严重性、故障说明、原因、出现次数以及最新出现时间。您还可以查看是否已确认故障。

    单击任何故障，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，并显示接口名称、运行状态、管理状态、收到的字节数和传输的字节数。

    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)** - 显示 ASA，并提供以下详细信息：设备名称、设备状态、应用、运行状态、管理状态、映像版本和管理 IP 地址。
  - **资产 (Inventory)** - 列出机箱中安装的组件，并提供这些组件的相关详细信息，如：**组件**名称、核心数量、安装位置、运行状态、可操作性、容量、功率、温度、序列号、型号、部件号和供应商。

接口

您可以在 FXOS 中管理物理接口。要使用某一接口，必须在 FXOS 中以物理方式启用它，并在 ASA 中以逻辑方式启用它。

Firepower 2100 默认启用巨帧支持。最大 MTU 为 9184。

注释 如果在启用故障转移（通过增加或删除网络模块，或通过更改 EtherChannel 配置）后更改接口，请在备用设备上的 FXOS 中更改接口，然后在主用设备上进行相同更改。

如果在 FXOS 中删除一个接口（例如，如果您移除网络模块，移除 EtherChannel，或将某个接口重新分配到 EtherChannel），则 ASA 配置会保留原始命令，以便您可以进行任何必要的调整；从配置中删除接口会产生广泛的影响。您可以在 ASA OS 中手动移除旧的接口配置。

配置接口

您可以通过物理方式启用和禁用接口，并设置接口速度和双工。要使用某一接口，必须在 FXOS 中以物理方式启用它，并在 ASA 中以逻辑方式启用它。

过程

步骤 1 点击**接口 (Interface)** 选项卡。

步骤 2 要启用或禁用接口，请点击**管理状态 (Admin State)** 滑块。复选标记表示已启用，而 X 则表示已禁用。

注释 管理 1/1 接口在该表中显示为 **MGMT**。

步骤 3 点击要编辑其速度或双工的接口对应的**编辑 (Edit)** 铅笔图标。

注释 您只能启用或禁用管理 1/1 接口；但不能编辑其属性。

步骤 4 选中**启用 (Enable)** 复选框以启用该接口。

步骤 5 从**管理速度 (Admin Speed)** 下拉列表中，选择接口的速度。

步骤 6 点击**自动协商 (Auto Negotiation) 是 (Yes)** 或**否 (No)** 单选按钮。

步骤 7 从**管理双工 (Admin Duplex)** 下拉列表中，选择该接口的双工。

步骤 8 点击**确定**。

添加 EtherChannel

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

注释 EtherChannel 成员端口在 ASA 上可见，但您只能在 FXOS 中配置 EtherChannels 和端口成员身份。

如果在启用故障转移后更改 EtherChannel 配置，请在备用设备上的 FXOS 中更改接口，然后在主用设备上进行相同更改。

开始之前

Firepower 2100 在链路汇聚控制协议 (LACP) 活动或开启模式下支持 EtherChannel。默认情况下，LACP 模式设置为“活动 (Active)”；您可以在 CLI 中将该模式更改为“开启 (On)”。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 点击**接口 (Interface)** 选项卡。

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

步骤 3 在**端口通道 ID (Port Channel ID)** 字段中，输入端口通道的 ID。有效值介于 1 与 47 之间。

步骤 4 选中**启用 (Enable)** 复选框以启用端口通道。

忽略**类型 (Type)** 下拉列表；唯一可用的类型是**数据 (Data)**。

步骤 5 从**管理速度 (Admin Speed)** 下拉列表中，选择所有成员接口的速度。

如果您选择的接口无法达到所选速度（以及您选择的其他设置），则会自动应用尽可能最快的速度。

步骤 6 为所有成员接口点击**自动协商 (Auto Negotiation) 是 (Yes)** 或**否 (No)** 单选按钮。

步骤 7 在**管理双工 (Admin Duplex)** 下拉列表中，为所有成员接口选择双工。

步骤 8 在**可用接口 (Available Interface)** 列表中，选择您要添加的接口，然后点击**添加接口 (Add Interface)**。

您最多可以添加16个同一类型和速度的接口。添加到通道组的第一个接口确定正确的类型和速度。

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。

注释 您要删除 EtherChannel 中的接口时，ASA 配置将保留相关命令，以便您可以进行任何必要的调整；从配置中删除接口可能具有广泛影响。您可以在 ASA OS 中手动移除旧的接口配置。

例如，将 Ethernet1/4 分配给 FXOS 中的 Port-channel7 后，Ethernet1/4 仍显示为 ASA OS 中的可用接口，并且 Ethernet1/4 的任何配置都将保留。如果您输入**show interface ethernet1/4**，ASA 会显示接口 "未与管理引擎关联"。使用 **no interface ethernet1/4** 命令可删除无关配置。

步骤 9 点击**确定**。

监控接口

在**接口 (Interfaces)** 选项卡上，可以查看机箱上已安装的接口的状态。下半部分包含安装在 Firepower 机箱中的接口的表。上面部分显示 Firepower 机箱中安装的接口的直观表示。您可以将鼠标悬停在上半部分中任何接口上方，以获取有关该接口的其他信息。

接口带有色标，表示其当前状态：

- 绿色 - 运行状态为“开启 (Up)”。
- 暗灰色 - 管理状态为“已禁用 (Disabled)”。
- 红色 - 运行状态为“关闭 (Down)”。
- 浅灰色 - 未安装 SFP。

逻辑设备

逻辑设备 (Logical Devices) 页显示有关 ASA 的信息和状态。您还可以使用滑块禁用或重新启用 ASA 以进行故障排除（选中标记表示它已被启用，而 X 则表示它已被禁用）。

ASA 的标题提供了**状态 (Status)**：

- **正常 (ok)** - 逻辑设备配置已完成。
- **未完成配置 (incomplete-configuration)** - 逻辑设备配置未完成。

逻辑设备区域还为 ASA 提供了更详细的**状态 (Status)**：

- **在线 (Online)** - ASA 正在运行和操作。
- **离线 (Offline)** - ASA 已停止且无法操作。
- **正在安装 (Installing)** - 正在进行 ASA 安装。
- **未安装 (Not Installed)** - 未安装 ASA。
- **安装失败 (Install Failed)** - ASA 安装失败。
- **正在启动 (Starting)** - ASA 正在启动。
- **启动失败 (Start Failed)** - ASA 未能启动。
- **已启动 (Started)** - ASA 已成功启动，并且正在等待应用代理心跳。
- **正在停止 (Stopping)** - ASA 正在停止。
- **停止失败 (Stop Failed)** - ASA 无法进入离线状态。
- **没有响应 (Not Responding)** - ASA 没有响应。
- **正在更新 (Updating)** - 正在进行 ASA 软件升级。
- **更新失败 (Update Failed)** - ASA 软件升级失败。
- **更新成功 (Update Succeeded)** - ASA 软件升级成功。

平台设置

平台设置 (Platform Settings) 选项卡允许您为 FXOS 设置基本操作，包括时间和管理访问。

NTP：设置时间

您可以手动设置时钟，或使用 NTP 服务器（推荐）。您最多可以配置 4 个 NTP 服务器。

开始之前

- 默认情况下，NTP 配置为以下思科 NTP 服务器：0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org。
- 如果您要将主机名用于 NTP 服务器，则必须配置 DNS 服务器。请参阅 DNS：配置 DNS 服务器，第 17 页。

过程

步骤 1 点击**平台设置 (Platform Settings)** 选项卡，然后点击左侧导航窗格中的 **NTP**。

默认情况下，将选择**时间同步 (Time Synchronization)** 选项卡。

步骤 2 要使用 NTP 服务器：

a) 点击**使用 NTP 服务器 (Use NTP Server)** 单选按钮。

b) （可选）（ASA 9.10(1) 及更高版本）如果您需要使用 NTP 服务器进行身份验证，选中 **NTP 服务器身份验证: 启用**复选框。

单击**是**以要求身份验证密钥 ID 和值。

仅支持使用 SHA1 进行 NTP 服务器身份验证。

c) 单击**添加**以通过 IP 地址或主机名标识最多 4 个 NTP 服务器。

如果您要将主机名用于 NTP 服务器，请在完成此程序后配置 DNS 服务器。

d) （ASA 9.10(1) 及更高版本）输入 NTP 服务器的**身份验证密钥** ID 和**身份验证值**。

从 NTP 服务器获取密钥 ID 和值。例如，要在安装了 OpenSSL 的 NTP 服务器 4.2.8p8 版或更高版本上生成 SHA1 密钥，请输入 **ntp-keygen -M** 命令，然后在 ntp.keys 文件中查看密钥 ID 和值。密钥用于告知客户端和服务器在计算消息摘要时要使用哪个值。

e) 单击**保存**以保存服务器。

步骤 3 要手动设置时间：

a) 点击**手动设置时间 (Set Time Manually)** 单选按钮。

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

c) 使用对应的下拉列表将时间指定为小时、分钟和 **AM/PM**。

步骤 4 点击**当前时间 (Current Time)** 选项卡，然后从**时区 (Time Zone)** 下拉列表中，为机箱选择适当的时区。

步骤 5 单击**保存 (Save)**。

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。

SSH：配置 SSH

以下程序说明如何启用或禁用对 Firepower 机箱的 SSH 访问，以及如何将机箱作为 SSH 客户端启用。默认情况下，SSH 服务器和客户端处于启用状态。

过程

步骤 1 依次选择**平台设置 (Platform Settings)** > **SSH** > **SSH 服务器 (SSH Server)**。

步骤 2 要启用 SSH 服务器，以提供对 Firepower 机箱的 SSH 访问，请勾选**启用 SSH (Enable SSH)** 复选框。

步骤 3 对于服务器**加密算法 (Encryption Algorithm)**，请选中每种允许的加密算法对应的复选框。

步骤 4 对于服务器**密钥交换算法**，请勾选每个允许的 Diffie-Hellman (DH) 密钥交换的复选框。

DH 密钥交换提供无法由任何一方单独确定的共享密钥。密钥交换与签名和主机密钥配合使用，以提供主机身份验证。此密钥交换方法提供显式服务器身份验证。有关使用 DH 密钥交换方法的详细信息，请参阅 RFC 4253。

步骤 5 对于服务器 **Mac 算法 (Mac Algorithm)**，请勾选允许的每种完整性算法所对应的复选框。

步骤 6 对于服务器**主机密钥**，请输入 RSA 密钥对的模块大小。

模数值（以位为单位）应为 8 的倍数，且介于 1024 到 2048 之间。指定的密钥模块大小越大，生成 RSA 密钥对所需的时间就越长。建议值为 2048。

步骤 7 对于服务器**密钥更新数量限制 (Volume Rekey Limit)**，请设置在 FXOS 断开会话连接之前允许通过该连接的流量（以 KB 为单位）。

步骤 8 对于服务器**密钥更新时间限制**，请设置 FXOS 断开会话连接之前允许的 SSH 会话空闲时间（以分钟为单位）。

步骤 9 单击**保存 (Save)**。

步骤 10 单击 **SSH 客户端 (SSH Client)** 选项卡，以自定义 FXOS 机箱 SSH 客户端。

步骤 11 对于**严格主机密钥检查**，可选择**启用**、**禁用**或**提示**来控制 SSH 主机密钥检查。

- **启用 (enable)** - 如果 FXOS 已知的主机文件中不包括主机密钥，连接将被拒绝。您必须在 FXOS CLI 中使用系统/服务范围的 **enter ssh-host** 命令手动添加主机。
- **提示 (prompt)** - 对于机箱中未存储的主机密钥，系统会提示您接受或拒绝该主机密钥。
- **禁用 (disable)** - （默认）机箱将自动接受以前未存储的主机密钥。

步骤 12 对于客户端**加密算法 (Encryption Algorithm)**，请选中每种允许的加密算法对应的复选框。

步骤 13 对于客户端**密钥交换算法**，请勾选每个允许的 Diffie-Hellman (DH) 密钥交换的复选框。

DH 密钥交换提供无法由任何一方单独确定的共享密钥。密钥交换与签名和主机密钥配合使用，以提供主机身份验证。此密钥交换方法提供显式服务器身份验证。有关使用 DH 密钥交换方法的详细信息，请参阅 RFC 4253。

步骤 14 对于客户端 **Mac 算法**，请勾选每个允许的完整性算法的复选框。

步骤 15 对于客户端**密钥更新数量限制 (Volume Rekey Limit)**，请设置在 FXOS 断开会话连接之前允许通过该连接的流量（以 KB 为单位）。

步骤 16 对于客户端**密钥更新时间限制**，请设置 FXOS 断开会话连接之前允许的 SSH 会话空闲时间（以分钟为单位）。

步骤 17 点击**保存**。

SNMP：配置 SNMP

使用 **SNMP** 页面，在 Firepower 机箱上配置简单网络管理协议 (SNMP)。

关于 SNMP

SNMP 是一种应用层协议，提供 SNMP 管理器和代理之间的通信消息格式。SNMP 提供用于监控和管理网络中的设备的标准化框架和通用语言。

SNMP 框架由三个部分组成：

- SNMP 管理器 - 用于通过 SNMP 来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 机箱的数据并根据需要向 SNMP 管理器报告数据。Firepower 机箱包含代理和 MIB 集合。
- 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。

SNMP 通知

SNMP 的一个关键功能是能够生成来自 SNMP 代理的通知。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 机箱将 SNMP 通知生成为陷阱或通知。陷阱不如通知可靠，因为 SNMP 管理器在收到陷阱时不发送任何确认，并且 Firepower 机箱无法确定是否已收到陷阱。收到通告请求的 SNMP 管理器使用一个 SNMP 响应协议数据单元 (PDU) 来确认消息。如果 Firepower 机箱不接收 PDU，则其可以再次发送通知请求。

SNMP 安全级别和权限

SNMPv1、SNMPv2c 和 SNMPv3 分别表示不同的安全模型。安全模型与所选安全级别结合来确定处理 SNMP 消息时应用的安全机制。

安全级别确定查看与 SNMP 陷阱关联的消息时所需的权限。权限级别确定是否需要防范消息泄露或免受身份验证。受支持的安全级别取决于实施的安全模式。SNMP 安全级别支持以下一个或多个权限：

- 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级别。安全模型是为用户和用户所处的角色设置的身份验证策略。安全级别是安全模型中允许的安全级别。安全模型和安全级别相结合来确定在处理 SNMP 数据包时采用的安全机制。

支持的 SNMP 安全模型和级别组合

下表确定安全模型和级别的组合含义。

表 *1: SNMP* 安全模型和级别

型号	级别	身份验证	加密	状况
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。除基于密码块链 (CBC) DES (DES-56) 标准的身份验证外，还提供数据加密标准 (DES) 56 位加密。

SNMPv3 安全功能

SNMPv3 通过将在网络上对帧进行身份验证和加密相结合来提供对设备的安全接入。SNMPv3 仅按已配置的用户来授权管理操作，并会加密 SNMP 消息。SNMPv3 基于用户的安全模型 (USM) 是指 SNMP 消息级别安全，并提供以下服务：

- 消息完整性 - 确保消息未在未经授权的情况下进行修改或销毁，并且数据序列未修改至超出可以非恶意形式出现的程度。
- 消息来源身份验证 - 确保对用户（系统代表该用户发出此已接收数据）的声明身份进行确认。
- 消息机密性和加密 - 确保不向未经授权的个人、实体或流程提供或披露信息。

SNMP 支持

Firepower 机箱为 SNMP 提供下列支持：

针对 MIB 的支持

Firepower 机箱支持对 MIB 的只读访问。

适用于 SNMPv3 用户的身份验证协议

Firepower 机箱针对 SNMPv3 用户支持 HMAC-SHA-96 (SHA) 身份验证协议。

适用于 SNMPv3 用户的 AES 隐私协议

除了基于SHA的身份验证，Firepower机箱还提供了使用AES-128位高级加密标准的隐私。Firepower机箱使用隐私密码生成 128 位 AES 密钥。AES 隐私密码至少可具有八个字符。如果口令用明文指定，您可以指定最多 80 个字符。

配置 SNMP

启用 SNMP，添加陷阱和 SNMPv3 用户。

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 个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**。 请注意，如果**社区/用户名 (Community/Username)** 字段已设置，空字段右侧会显示文本**已设置：是 (Set: Yes)**。如果**社区/用户名 (Community/Username)**字段尚未填充值，空字段右侧会显示文本**已设置：否 (Set: No)**。
系统管理员名称 (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，例如邮件地址或姓名和电话号码。

名称	说明
位置字段	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 在 **SNMP 陷阱 (SNMP Traps)** 区域中，单击**添加 (Add)**。

步骤 4 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 个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。
版本 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 5 单击**确定 (OK)**，可关闭**添加 SNMP 陷阱 (Add SNMP Trap)** 对话框。

步骤 6 在 **SNMP 用户 (SNMP Users)** 区域中，单击**添加 (Add)**。

步骤 7 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。 最多输入 32 个字母或数字。名称必须以字母开始，也可以指定 _（下划线）、.（句点）、@（邮箱符号）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	如果选中此复选框，则此用户使用 AES-128 加密。
密码 (Password) 字段	此用户的密码。
确认密码 (Confirm Password) 字段	用于再次确认的密码。
隐私密码 (Privacy Password) 字段	此用户的隐私密码。
确认隐私密码 (Confirm Privacy Password) 字段	用于再次确认的隐私密码。

步骤 8 单击**确定 (OK)**，可关闭**添加 SNMP 用户 (Add SNMP User)** 对话框。

步骤 9 点击**保存 (Save)**。

HTTPS：更改端口

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。

开始之前

如果在 ASA 数据接口上启用 HTTPS 访问，则不要从 443 更改 HTTPS 端口；仅支持默认端口。

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 单击**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。

DHCP：为管理客户端配置 DHCP 服务器

您可以为连接到管理 1/1 接口的客户端启用 DHCP 服务器。默认情况下，使用以下地址范围启用服务器：192.168.45.10-192.168.45.12。如果要更改管理 IP 地址，则必须禁用 DHCP 。然后，您可以为新网络重新启用 DHCP。

过程

步骤 1 依次选择**平台设置 (Platform Settings)** > **DHCP**。

步骤 2 选中**启用 DNS 服务 (Enable DHCP service)** 复选框。

步骤 3 输入**起始 IP (Start IP)** 和**结束 IP (End IP)** 地址。

步骤 4 点击**保存**。

系统日志：配置系统日志消息传送

日志对常规故障排除及事件处理均有帮助。您可以将系统日志消息发送到 Firepower 2100 控制台、SSH 会话或本地文件。

这些系统日志消息仅适用于 FXOS 机箱。对于 ASA 系统日志消息，必须在 ASA 配置中配置日志记录。

注释 不支持远程目标。

过程

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

步骤 2 配置本地目的：

a) 单击**本地目的 (Local Destinations)** 选项卡。

b) 填写以下字段：

名称	说明
控制台 (Console)	

名称	说明
管理状态 (Admin State)	勾选启用 (Enable) 复选框可在控制台上显示系统日志消息。
级别 (Level)	点击要在控制台上显示的最低消息级别。Firepower 机箱将显示该级别及以上级别的消息。 • 紧急 • 提醒 • 严重
平台	
管理状态 (Admin State)	平台系统日志始终处于启用状态。
级别 (Level)	选择要显示的最低消息级别。Firepower 机箱将显示该级别及以上级别的消息。默认值为信息 (Informational)。 • 紧急 • 提醒 • 严重 • 错误 • 警告 • 通知 • 信息 • 调试
文件	
管理状态 (Admin State)	勾选启用 (Enable) 复选框可将系统日志消息保存到文件中。

名称	说明
级别 (Level)	选择要保存的最低消息级别。系统将保存该级别及以上级别的消息。 • 紧急 • 提醒 • 严重 • 错误 • 警告 • 通知 • 信息 • 调试
名称 (Name)	设置文件的名称，最多 16 个字符。
大小 (Size)	在系统开始用最新消息覆写最旧消息之前，请指定最大文件大小（以字节为单位）。范围为 4096 到 4194304 字节。

c) 单击保存 (Save)。

步骤 3 配置本地来源：

a) 单击本地来源 (Local Sources) 选项卡。

b) 填写以下字段：

名称	说明
故障管理状态 (Faults Admin State)	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)	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)	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。

DNS：配置 DNS 服务器

如果系统要求将主机名解析为 IP 地址，则您需要指定 DNS 服务器。您最多可以配置 4 个 DNS 服务器。配置多个 DNS 服务器时，系统仅以任意随机顺序搜索服务器。

开始之前

- 默认情况下，DNS 配置为以下 OpenDNS 服务器：208.67.222.222、208.67.220.220。

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，单击**添加 (Add)**。

步骤 4 单击**保存 (Save)**。

步骤 5 点击**域名配置 (Domain Name Configuration)** 选项卡，输入要将 Firepower 机箱作为后缀附加到非限定名称的**域名 (Domain name)**，然后点击**添加 (Add)**。

例如，如果您将域名设置为“example.com”并通过不受限定的名称“jupiter”来指定系统日志服务器，则 Firepower 机箱会将名称限定为“jupiter.example.com”。

FIPS 和通用标准：启用 FIPS 和通用标准模式

执行以下步骤可在 Firepower 2100 上启用 FIPS 或“通用标准 (CC) ”模式。

您还必须使用 **fips enable** 命令在 ASA 上单独启用 FIPS 模式。在 ASA 上没有用于通用标准模式的单独设置；对 CC 或 UCAPL 法规合规性的任何其他限制都必须按照思科安全策略文档进行配置。

我们建议您首先在 ASA 上设置 FIPS 模式，等待设备重新加载，然后在 FXOS 中设置 FIPS 模式。

过程

步骤 1 依次选择**平台设置 (Platform Settings)** > **FIPS 和通用标准 (FIPS and Common Criteria)**。

步骤 2 通过选中**启用 (Enable)** 复选框启用 **FIPS**。

步骤 3 通过选中**启用 (Enable)** 复选框启用**通用标准 (Common Criteria)**。

在启用“通用标准 (Common Criteria)”后，默认情况下将启用 **FIPS 启用 (FIPS Enable)** 复选框。

步骤 4 点击**保存 (Save)**。

步骤 5 按照提示重新启动系统。

访问列表：配置管理访问

默认情况下，Firepower 2100 允许对 Firepower 机箱管理器进行 HTTPS 访问，和在管理 1/1 192.168.45.0/24 网络上进行 SSH 访问。如果您要允许从其他网络进行访问，或者允许 SNMP，则必须添加或更改访问列表。

对于每个 IP 地址块（v4 或 v6），最多可为每项服务配置 25 个不同子网。

过程

步骤 1 依次选择**平台设置 (Platform Settings)** > **访问列表 (Access List)**。

步骤 2 在 **IPv4 访问列表 (IPv4 Access List)** 区域中：

a) 点击**添加 (Add)**。

b) 输入以下字段的值：

- **IP 地址 (IP Address)** - 设置 IP 地址。输入 **0.0.0.0** 以允许所有网络。
- **前缀长度 (Prefix Length)** - 设置子网掩码。输入 **0** 以允许所有网络。
- **协议 (Protocol)** - 选择 **HTTPS**、**SNMP** 或 **SSH**。

c) 点击**确定 (OK)**。

d) 重复这些步骤为每项服务添加其他网络。

步骤 3 在 **IPv6 访问列表 (IPv6 Access List)** 区域中：

a) 点击**添加 (Add)**。

b) 输入以下字段的值：

- **IP 地址 (IP Address)** - 设置 IP 地址。输入 :: 以允许所有网络。
- **前缀长度 (Prefix Length)** - 设置前缀长度。输入 **0** 以允许所有网络。
- **协议 (Protocol)** - 选择 **HTTPS**、**SNMP** 或 **SSH**。

c) 点击**确定 (OK)**。

d) 重复这些步骤为每项服务添加其他网络。

步骤 4 点击**保存**。

系统更新

此任务适用于独立 ASA。如果要升级故障切换对，请参阅思科 ASA 升级指南。升级过程通常需要 20 到 30 分钟。

ASA、ASDM 和 FXOS 映像被捆绑成一个单一的包。包更新由 FXOS 管理；不能在 ASA 操作系统中升级 ASA。不能单独升级 ASA 和 FXOS；它们始终捆绑在一起。

不过 ASDM 是个例外，此时您可以从 ASA 操作系统中升级，因此无需只使用捆绑的 ASDM 映像。手动上传的 ASDM 映像不会出现在 FXOS 映像列表中；您必须从 ASA 管理 ASDM 映像。

注释 在升级捆绑包时，捆绑包中的 ASDM 映像将替换以前的 ASDM 捆绑包映像，因为它们具有相同的名称 (**asdm.bin**)。但是，如果您手动选择了您上传的其他 ASDM 映像（例如，**asdm-782.bin**），那么即使捆绑包升级之后，您仍可继续使用该映像。为了确保您运行的是兼容版本的 ASDM，您应该在升级捆绑包之前先升级 ASDM，或者应该在升级 ASA 捆绑包之前，或将 ASA 重新配置为使用捆绑的 ASDM 映像 (**asdm.bin**)。

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 依次选择**系统 (System)** > **更新 (Updates)**。

可用更新 (Available Updates) 页面将显示机箱上可用的包的列表。

步骤 2 点击**上传映像 (Upload Image)**。

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

步骤 4 单击**上传 (Upload)**。

所选映像将上传到机箱。新映像添加至机箱后，系统将自动验证映像的完整性。如果要手动验证其完整性，请点击**验证 (Verify)**（勾选标记图标）。

步骤 5 选择要升级到的 ASA 包，然后点击**升级 (Upgrade)**。

步骤 6 点击**是 (Yes)**，确认您想要继续安装，或者点击**否 (No)** 取消安装。

升级过程中，系统会将您从 Firepower 机箱管理器注销。

用户管理

用户帐户用于访问 Firepower 2100 机箱。这些帐户用于 Firepower 机箱管理器和 SSH 访问。ASA 拥有单独的用户帐户和身份验证。

关于用户帐户

管理员帐户

管理员帐户是默认用户帐户，并且无法修改或删除。此帐户是系统管理员或超级用户帐户并具有完整权限。默认密码为 **Admin123**。

管理员帐户始终处于活动状态，并且不会到期。无法将管理员帐户配置为非活动状态。

本地身份验证的用户帐户

您最多可配置 48 个本地用户帐户。每个用户帐户必须具有唯一的用户名和密码。

本地身份验证用户帐户可以由具有管理员权限的任何用户来启用或禁用。

用户帐户的准则

用户名

用户名用作 Firepower 机箱管理器和 FXOS CLI 的登录 ID。分配登录 ID 时，请考虑以下指导原则和限制：

- 登录 ID 可以包含 1 到 32 个字符，包括以下字符：
  - 任何字母字符
  - 任何数字
  - _（下划线）
  - -（连字符）
  - .（圆点）
- 登录 ID 必须唯一。
- 登录 ID 必须以字母字符开头，而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。
- 无法创建全数字登录 ID。
- 创建用户帐户后，无法更改登录 ID。必须删除该用户帐户，创建新的用户帐户。

密码

密码对于每个本地认证的用户帐户都是必需的。具有管理员权限的用户可以配置系统，以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。

建议每个用户都使用强密码。如果对本地身份验证的用户启用密码强度检查，则 FXOS 将拒绝不符合以下要求的任何密码：

- 必须包含最少 8 个字符，最多 127 个字符。

  注释 您可以选择在系统上配置 15 个字符（最小密码长度）的密码，以符合通用标准需求。

- 必须包含至少一个大写字母字符。

- 必须包含至少一个小写字母字符。
- 必须包含至少一个非字母数字（特殊）字符。
- 不能包含连续重复 3 次的字符，例如 aaabbb。
- 不得包含三个以任何顺序排列的连续数字或字母，例如 passwordABC 或 password321。
- 不能与用户名相同，或与用户名正好相反。
- 必须通过密码字典检查。例如，密码不可以是标准的词典单词。
- 不得包含以下符号：$（美元符号）、?（问号）和 =（等号）。
- 不得为空。

添加用户

为 Firepower 机箱管理器和 FXOS CLI 访问添加本地用户。

过程

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

步骤 2 单击**本地用户 (Local Users)** 选项卡。

步骤 3 单击**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：

- **用户名** - 设置用户名。此名称必须唯一，并满足用户帐户名称的准则和限制（请参阅用户帐户的准则，第 21 页）。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** - 设置用户的名字。该字段最多包含 32 个字符。
- **姓氏** - 用户的姓氏该字段最多包含 32 个字符。
- **电子邮箱** - 设置用户的电子邮件地址。
- **电话号码** - 设置用户的电话号码。
- **密码**和**确认密码** - 设置与此帐户关联的密码。如果启用了密码强度检查，则密码必须为强密码，FXOS 会拒绝任何不满足强度检查要求的密码（请参阅配置用户设置，第 23 页 和 用户帐户的准则，第 21 页）。
- **帐户状态** - 将状态设置为**活动**或**非活动**。
- **用户角色** - 设置表示要分配给用户帐户的权限的角色。系统会默认为所有用户分配**只读**角色，并且此角色无法取消选择。要分配管理员角色，请在窗口中单击**管理**以使其突出显示。管理员角色允许对配置进行读写访问。用户角色和权限的更改在用户下一次登录之后才会生效。如果在向用户帐户分配新角色或从中删除现有角色时用户已登录，则活动会话将继续使用上一个角色和权限。

- **帐户到期** - 设置帐户到期。在**到期日期**字段中指定的日期过后，无法使用帐户。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。默认情况下，用户帐户不会到期。
- **到期日期** - 帐户到期的日期。日期格式应为 yyyy-mm-dd。单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 单击**添加 (Add)**。

步骤 6 要停用某一用户，请执行以下操作：

a) 对于要禁用的用户，请点击 编辑图标（）。

管理员用户帐户始终设置为活动，且不能停用。

b) 在**帐户状态 (Account Status)** 字段中，单击**非活动状态 (Inactive)** 单选按钮。

c) 点击**保存**。

配置用户设置

您可以为所有用户配置全局设置。

过程

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

步骤 2 单击**设置** (Settings) 选项卡。

步骤 3 填写以下字段。

- **默认身份验证**—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。
  - **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。
- **密码强度检验**—如果选中，所有本地用户密码都必须符合强密码准则（请参阅用户帐户的准则，第 21 页）。默认情况下，系统会启用强密码。
- **历史记录计数**—用户在重新使用先前使用的密码之前必须创建的唯一密码的数量。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**字段设置为 0，这表示禁用历史记录计数，使用户能够重复使用之前已使用的密码。
- **更改间隔** — 在其期间执行在**更改计数**字段中指定的密码更改次数的小时数。该值可以是 1 至 745（小时）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。选中此复选框以启用此功能。

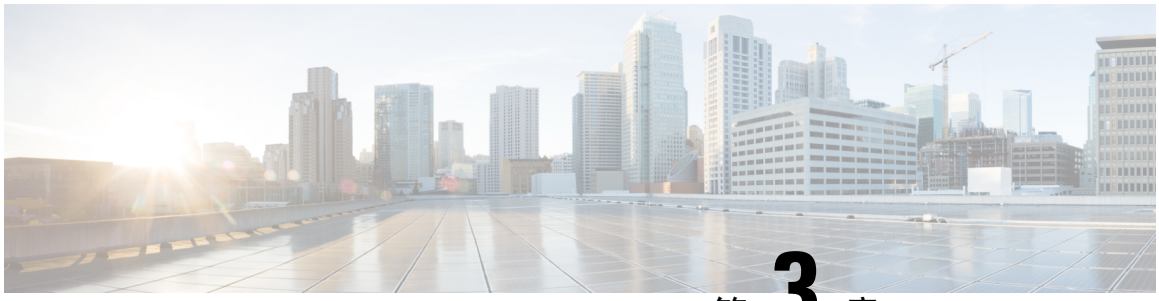
- **更改计数**—本地身份验证用户能够在“更改间隔”内更改其密码的最大次数。该值可以是介于 0 和 10 之间的任意值。
- **不更改间隔**—指定经过本地身份验证的用户在更改新建密码之前必须等待的最少小时数。该值可以是 1 至 745（小时）的任意值。选中此复选框以启用此功能。
- **口令到期天数** — 将到期时间设置为 1 到 9999 天。默认情况下，禁用过期。
- **口令到期警告期限** — 设置到期前的天数，以警告用户每次登录时的密码到期，范围介于 0 到 9999 之间。默认时间为 14 天。
- **到期宽限期** — 设置用户在到期后必须更改其密码的天数，范围介于 0 到 9999 之间。默认值为 3 天。
- **密码重复使用间隔** — 设置可重复使用密码的天数，范围介于 1 到365 之间。默认值为 15 天。如果同时启用**历史记录计数**和**密码重复使用间隔**，则必须满足两个要求。例如，如果您将历史计数设置为 3，并将重复使用间隔设置为 10 天，则您只能在更改 3 次密码的 10 天后更改密码。

步骤 4 点击**保存**。

Firepower 机箱管理器设置历史

功能	版本	详细信息
用户密码改进	9.13(1)	添加了密码安全改进，包括以下内容： • 用户密码最多可达 127 个字符。旧限制为 80 个字符。 • 默认情况下，系统会启用强密码。 • 提示设置管理员密码。 • 密码到期。 • 限制密码重复使用。 新增/修改的屏幕： • **系统** > **用户管理** > **本地用户** • **系统** > **用户管理** > **设置**

功能	版本	详细信息
在 Firepower 2100 上支持 NTP 身份验证	9.10(1)	现在，您可以在 FXOS 中配置 SHA1 NTP 服务器身份验证。 新增/修改的 Firepower 机箱管理器菜单项： **平台设置** > **NTP** > **NTP 服务器身份验证**：**启用**复选框、**身份验证密钥**、**字段身份验证值**字段



第 3 章

FXOS CLI 设置

Firepower 2100 运行 FXOS 来控制设备的基本操作。您可以使用 FXOS CLI 或 GUI Firepower 机箱管理器来配置这些功能；本文档涵盖FXOS CLI的内容。请注意，所有安全策略和其他操作都是在ASA OS 中配置的（使用 CLI 或 ASDM）。

CLI 和配置管理

Firepower 可扩展操作系统 (FXOS) 与 ASA CLI 的操作方式不同。本节介绍 CLI 以及如何管理您的 FXOS 配置。

关于 CLI

(FXOS) 使用受管对象模型（受管对象为可管理的物理或逻辑实体的抽象表示形式）。例如，机箱、网络模块、端口和处理器是表示为受管对象的物理实体，许可证、用户角色和平台策略是表示为受管对象的逻辑实体。

四个通用命令可用于对象管理：

- **create** *object*
- **delete** *object*
- **enter** *object*
- **scope** *object*

可以将 **scope** 命令用于任何受管对象（无论是永久对象，还是用户实例化对象）。其他命令用于创建和管理用户实例化对象。对于每个 **create** *object* 命令，都存在一个对应的 **delete** *object* and **enter**

object 命令。您可以使用 **enter** *object* 命令创建新对象和编辑现有对象，因此您可以使用它代替 **create** *object* 命令，如果对象已存在，则会出现错误。

您可以随时键入 **?** 字符来显示在命令语法的当前状态下可用的选项。

连接到 ASA 或 FXOS 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。

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-2110# 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 要返回到 FXOS 控制台，请输入 **Ctrl+a**, **d**。

使用 SSH 连接到 FXOS

您可以使用默认 IP 地址 192.168.45.45 连接到管理 1/1 上的 FXOS。如果配置远程管理（ASA **fxos permit** 命令），则还可以连接到非标准端口（默认情况下为 3022）上的数据接口 IP 地址。

要使用 SSH 连接到 ASA，必须首先根据 ASA 通用操作配置指南配置 SSH 访问。

您可以从 FXOS 连接到 ASA CLI，反之亦然。

FXOS 最多允许 8 条 SSH 连接。

开始之前

要更改管理 IP 地址，请参阅更改 FXOS 管理 IP 地址或网关，第 93 页。

过程

步骤 1 在连接到管理 1/1 的管理计算机上，将 SSH 连接到管理 IP 地址（默认情况下为 https://192.168.45.45，使用用户名：**admin** 和密码：**Admin123**）。

可以使用任何用户名登录（请参阅添加用户，第 22 页）。如果配置远程管理，则将 SSH 连接到端口 3022 上的 ASA 数据接口 IP 地址（默认端口）。

步骤 2 连接到 ASA CLI。

connect asa

要返回到 FXOS CLI，请输入 **Ctrl+a**, **d**。

示例：

```
firepower-2110# 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 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

firepower-2110 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

[…]

firepower-2110#
firepower-2110# 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#
```

提交、丢弃和查看待处理命令

当在 CLI 中输入配置命令时，将不会应用该命令，直至保存配置为止。直到提交后，配置命令才处于待处理状态，并可进行放弃。当所有命令处于待处理状态时，在命令提示符之前会出现星号 (*)。当您保存或丢弃配置更改时，星号会消失。可以累积多命令模式下的待处理更改，并将其一起应用。可以在任意命令模式下查看待处理命令。

过程

步骤 1 查看待处理的配置更改。

show configuration pending

示例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter ntp-server 10.1.1.1
firepower-2110 /system/services/ntp-server* # show configuration pending
+enter ntp-server 10.1.1.1
+    set ntp-sha1-key-id 0
+!   set ntp-sha1-key-string
+exit
firepower-2110 /system/services/ntp-server* #
```

步骤 2 保存配置。

commit-buffer

注释 将多条命令一起提交不是单一操作。如果任何命令失败，则即便失败也会应用成功的命令。在错误消息中会报告失败的命令。

示例：

```
firepower-2110 /system/services/ntp-server* # commit-buffer
firepower-2110 /system/services/ntp-server #
```

步骤 3 丢弃配置更改。

discard-buffer

示例：

```
firepower-2110 /system/services/ntp-server* # discard-buffer
firepower-2110 /system/services/ntp-server #
```

示例

以下示例显示提示符在命令输入过程中如何更改：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter ntp-server 10.1.1.1
firepower-2110 /system/services/ntp-server* # show configuration pending
+enter ntp-server 10.1.1.1
+    set ntp-sha1-key-id 0
+!   set ntp-sha1-key-string
+exit
firepower-2110 /system/services/ntp-server* #
firepower-2110 /system/services/ntp-server* # commit-buffer
firepower-2110 /system/services/ntp-server #
```

接口

您可以在 FXOS 中管理物理接口。要使用某一接口，必须在 FXOS 中以物理方式启用它，并在 ASA 中以逻辑方式启用它。

Firepower 2100 默认启用巨帧支持。最大 MTU 为 9184。

有关管理接口的信息，请参阅 ASA 和 FXOS 管理，第 1 页。

配置接口

您可以通过物理方式启用和禁用接口，并设置接口速度和双工。要使用某一接口，必须在 FXOS 中以物理方式启用它，并在 ASA 中以逻辑方式启用它。默认情况下，仅在 FXOS 和 ASA 中启用以太网 1/1 和以太网 1/2。

开始之前

不能单独修改已经是 EtherChannel 成员的接口。务必在将接口添加到 EtherChannel 之前为其配置设置。

过程

步骤 1 进入以太网上行链路，然后进入交换矩阵模式。

scope eth-uplink

scope fabric a

示例：

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink # scope fabric a
firepower-2110 /eth-uplink/fabric #
```

步骤 2 启用接口。

enter interface *interface_id*

enable

示例：

```
firepower-2110 /eth-uplink/fabric # enter interface Ethernet1/8
firepower-2110 /eth-uplink/fabric/interface # enable
firepower-2110 /eth-uplink/fabric/interface* #
```

步骤 3 启用或禁用自动协商。

set auto-negotiation {**on** | **off**}

对于 RJ-45 接口，默认设置为 **on**。

对于 SFP 接口，默认设置为关闭，并且您无法启用自动协商。

示例：

```
firepower-2110 /eth-uplink/fabric/interface* # set auto-negotiation off
```

步骤 4 如果禁用自动协商，则设置接口速度。

set admin-speed {**10mbps** | **100mbps** | **1gbps** | **10gbps**}

对于铜缆接口，仅当禁用自动协商时，才会使用此速度。

示例：

```
firepower-2110 /eth-uplink/fabric/interface* # set admin-speed 1gbps
```

步骤 5 设置接口双工模式。

set admin-duplex {**fullduplex** |**halfduplex**}

对于铜缆接口，仅当禁用自动协商时，才会使用此双工。

示例：

```
firepower-2110 /eth-uplink/fabric/interface* # set admin-duplex halfduplex
```

步骤 6 保存配置。

commit-buffer

示例：

```
firepower-2110 /eth-uplink/fabric/interface* # commit-buffer
firepower-2110 /eth-uplink/fabric/interface #
```

示例

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink* # scope fabric a
firepower-2110 /eth-uplink/fabric* # enter interface ethernet1/6
firepower-2110 /eth-uplink/fabric/interface* # enable
firepower-2110 /eth-uplink/fabric/interface* # set flow-control-policy FlowControlPolicy23
firepower-2110 /eth-uplink/fabric/interface* # commit-buffer
firepower-2110 /eth-uplink/fabric/interface #
```

添加 EtherChannel

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

注释 EtherChannel 成员端口在 ASA 上可见，但您只能在 FXOS 中配置 EtherChannels 和端口成员身份。

开始之前

Firepower 2100 在活动或开启链路汇聚控制协议 (LACP) 模式下支持 EtherChannel。默认情况下，LACP 模式设置为“活动 (Active)”；您可以在 CLI 中将该模式更改为“开启 (On)”。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 进入以太网上行链路，然后进入交换矩阵模式。

scope eth-uplink

scope fabric a

示例：

```
firepower-2110# scope eth-uplink
```

```
firepower-2110 /eth-uplink # scope fabric a
firepower-2110 /eth-uplink/fabric #
```

步骤 2 启用端口通道。

enter port-channel *id*

enable

将 *id* 设置为介于 1 和 47 之间的整数。

示例：

```
firepower-2110 /eth-uplink/fabric # enter port-channel 1
firepower-2110 /eth-uplink/fabric/port-channel* # enable
```

步骤 3 分配成员接口。

enter member-port *interface_id*

示例：

```
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet1/1
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet1/2
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet1/3
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet1/4
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* #
```

步骤 4 （可选） 设置 LACP 模式。

set port-channel-mode {**active** |**on**}

默认为活动模式。

示例：

```
firepower-2110 /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

步骤 5 （可选） 将端口通道的所有成员的接口速度设置为覆盖各个接口上设置的属性。

set speed {**10mbps** | **100mbps** | **1gbps** | **10gbps**}

此方法提供了设置这些参数的快捷方式，因为端口通道中所有接口的这些参数都必须匹配。

示例：

```
firepower-2110 /eth-uplink/fabric/port-channel* # set speed 1gbps
```

步骤 6 （可选） 对于铜缆端口，将端口通道的所有成员的接口双工模式设置为覆盖各个接口上设置的属性。

set duplex {**fullduplex** |**halfduplex**}

此方法提供了设置这些参数的快捷方式，因为端口通道中所有接口的这些参数都必须匹配。

示例：

```
firepower-2110 /eth-uplink/fabric/port-channel* # set duplex fullduplex
```

步骤 7 （可选） 配置最多 256 个字符的说明。

set descr "文本**"**

示例：

```
firepower-2110 /eth-uplink/fabric/port-channel* # set descr "Inside Interface"
```

步骤 8 保存配置。

commit-buffer

示例：

```
firepower-2110 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-2110 /eth-uplink/fabric/port-channel #
```

示例

以下示例将 3 个接口添加到一个 EtherChannel，将 LACP 模式设置为开启，并设置速度和流量控制策略：

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink # scope fabric a
firepower-2110 /eth-uplink/fabric #
firepower-2110 /eth-uplink/fabric # enter port-channel 1
firepower-2110 /eth-uplink/fabric/port-channel* # enable
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet2/1
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet2/2
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # enter member-port ethernet2/3
firepower-2110 /eth-uplink/fabric/port-channel/member-port* # exit
firepower-2110 /eth-uplink/fabric/port-channel* # set port-channel-mode on
firepower-2110 /eth-uplink/fabric/port-channel* # set speed 10gbps

firepower-2110 /eth-uplink/fabric/port-channel* # commit-buffer
firepower-2110 /eth-uplink/fabric/port-channel #
```

监控接口

查看机箱上已安装的接口的状态。

过程

步骤 1 进入以太网上行链路，然后进入交换矩阵模式。

scope eth-uplink

scope fabric a

示例：

```
firepower-2110# scope eth-uplink
firepower-2110 /eth-uplink # scope fabric a
firepower-2110 /eth-uplink/fabric #
```

步骤 2 显示机箱上的已安装接口。

show interface

Etherchannel 中的成员接口不会显示在此列表中。

示例：

```
firepower-2110 /eth-uplink/fabric # show interface

Interface:
    Port Name       Port Type          Admin State Oper State       State Reason
    --------------- ------------------ ----------- ---------------- ------------
    Ethernet1/1     Mgmt               Enabled     Up
    Ethernet1/2     Data               Enabled     Link Down        Link failure
 or not-connected
    Ethernet1/3     Data               Enabled     Up
    Ethernet1/4     Data               Enabled     Sfp Not Present  Unknown
    Ethernet1/6     Data               Enabled     Sfp Not Present  Unknown
    Ethernet1/7     Data               Enabled     Sfp Not Present  Unknown
    Ethernet1/8     Data               Disabled    Sfp Not Present  Unknown
    Ethernet2/1     Data               Enabled     Up
    Ethernet2/2     Data               Enabled     Up
    Ethernet2/4     Data               Enabled     Up
    Ethernet2/5     Data               Enabled     Up
    Ethernet2/6     Data               Enabled     Up
    Ethernet3/2     Data               Enabled     Up
    Ethernet3/4     Data               Enabled     Up
```

平台设置

您可以为 FXOS 设置基本操作，包括时间和管理访问。

设置日期和时间

您可以配置网络时间协议（NTP），手动设置日期和时间，或者查看当前的系统时间。在 Firepower 2100 机箱和 ASA 操作系统之间时钟设置自动同步。

使用 NTP 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，例如验证 CRL，其包括精确时间戳。默认情况下会配置 NTP，以便 ASA 可以访问许可证服务器。您最多可以配置 4 个 NTP 服务器。Firepower 2100 使用 NTP 版本 3。

过程

步骤 1 进入系统，然后进入服务模式。

scope system

scope services

示例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

步骤 2 添加 NTP 服务器。

enter ntp-server {*hostname* |*ip_addr* |*ip6_addr*}

示例：

```
firepower-2110 /system/services # enter ntp-server 192.168.6.5
firepower-2110 /system/services/ntp-server* #
```

步骤 3 （可选）（ASA 9.10(1) 及更高版本）配置 NTP 身份验证。

仅支持使用 SHA1 进行 NTP 服务器身份验证。从 NTP 服务器获取密钥 ID 和值。例如，要在安装了 OpenSSL 的 NTP 服务器 4.2.8p8 版或更高版本上生成 SHA1 密钥，请输入 **ntp-keygen -M** 命令，然后在 ntp.keys 文件中查看密钥 ID 和值。密钥用于告知客户端和服务器在计算消息摘要时要使用哪个值。

a) 设置 SHA1 密钥 ID。

set ntp-sha1-key-id *key_id*

b) 设置 SHA1 密钥字符串。

set ntp-sha1-key-string

系统会提示您输入密钥字符串。

c) 退出 ntp-server 模式。

exit

d) 启用 NTP 认证。

enable ntp-authentication

示例：

```
firepower-2110 /system/services/ntp-server* # set ntp-sha1-key-string 11
firepower-2110 /system/services/ntp-server* # set ntp-sha1-key-string
NTP SHA-1 key string: 7092334a7809ab9873124c08123df9097097fe72
firepower-2110 /system/services/ntp-server* # exit
firepower-2110 /system/services* # enable authentication
```

步骤 4 设置时区。

set timezone

系统将提示您输入与您所在的洲、国家/地区和时区区域对应的编号。在每个系统提示符处输入适当的信息。

示例：

```
firepower-2110 /system/services* # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? 2
Please select a country.
 1) Anguilla                28) Haiti
 2) Antigua & Barbuda       29) Honduras
 3) Argentina               30) Jamaica
 4) Aruba                   31) Martinique
 5) Bahamas                 32) Mexico
 6) Barbados                33) Montserrat
 7) Belize                  34) Nicaragua
 8) Bolivia                 35) Panama
 9) Brazil                  36) Paraguay
10) Canada                  37) Peru
11) Caribbean Netherlands   38) Puerto Rico
12) Cayman Islands          39) St Barthelemy
13) Chile                   40) St Kitts & Nevis
14) Colombia                41) St Lucia
15) Costa Rica              42) St Maarten (Dutch part)
16) Cuba                    43) St Martin (French part)
17) Curacao                 44) St Pierre & Miquelon
18) Dominica                45) St Vincent
19) Dominican Republic      46) Suriname
20) Ecuador                 47) Trinidad & Tobago
21) El Salvador             48) Turks & Caicos Is
22) French Guiana           49) United States
23) Greenland               50) Uruguay
24) Grenada                 51) Venezuela
25) Guadeloupe              52) Virgin Islands (UK)
26) Guatemala               53) Virgin Islands (US)
27) Guyana
#? 49
Please select one of the following time zone regions.
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
 5) Eastern Time - Indiana - most locations
 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
 7) Eastern Time - Indiana - Pulaski County
```

```
 8) Eastern Time - Indiana - Crawford County
 9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Standard Time - Arizona (except Navajo)
21) Pacific Time
22) Pacific Standard Time - Annette Island, Alaska
23) Alaska Time
24) Alaska Time - Alaska panhandle
25) Alaska Time - southeast Alaska panhandle
26) Alaska Time - Alaska panhandle neck
27) Alaska Time - west Alaska
28) Aleutian Islands
29) Hawaii
#? 21

The following information has been given:

        United States
        Pacific Time

Therefore timezone 'America/Los_Angeles' will be set.
Local time is now:      Wed Jun 24 07:39:25 PDT 2018.
Universal Time is now:  Wed Jun 24 14:39:25 UTC 2018.
Is the above information OK?
1) Yes
2) No
#? 1
firepower-2110 /system/services* #
```

步骤 5 保存配置。

commit-buffer

示例：

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

步骤 6 查看时钟详细信息。

- 查看所有已配置的 NTP 服务器的同步状态。

  show ntp-server[*hostname* |*ip_addr* |*ip6_addr*]

```
firepower-2110 /system/services # show ntp-server

NTP server hostname:
    Name                 Time Sync Status
    -------------------- ----------------
    0.sourcefire.pool.nt Unreachable Or Invalid Ntp Server
    1.sourcefire.pool.nt Unreachable Or Invalid Ntp Server
```

```
    2.sourcefire.pool.nt Unreachable Or Invalid Ntp Server
```

- 查看特定 NTP 服务器的同步状态。

  enter ntp-server {*hostname* |*ip_addr* |*ip6_addr*}

  show detail

  exit

```
firepower-2110 /system/services # enter ntp-server 0.sourcefire.pool.ntp.org
firepower-2110 /system/services/ntp-server # show detail

NTP server hostname:
    Name: 0.sourcefire.pool.ntp.org
    Time Sync Status: Unreachable Or Invalid Ntp Server
    Error Msg: Failed to translate domain name to IP, please verify the domain name or
 check if DNS server is configured.

firepower-2110 /system/services/ntp-server # exit
firepower-2110 /system/services #
```

- 查看已配置的时区。

  show timezone

```
firepower-2110 /system/services # show timezone
Timezone: America/Los_Angeles
```

- 查看配置的日期和时间。

  show clock

```
firepower-2110 /system/services # show clock
Wed Apr 18 08:49:35 PDT 2018
```

示例

以下示例配置具有 IPv4 地址 192.168.200.101 的 NTP 服务器。

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter ntp-server 192.168.200.101
firepower-2110 /system/services/ntp-server* # commit-buffer
firepower-2110 /system/services/ntp-server #
```

手动设置日期和时间

本部分介绍如何在 Firepower 2100 机箱上手动设置日期和时间。系统时钟修改立即生效。如果系统时钟当前正在与 NTP 服务器同步，您将无法手动设置日期和时间。

过程

步骤 1 进入系统，然后进入服务模式。

scope system

scope services

示例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

步骤 2 设置时间和日期。

set clock *month day year hour min sec*

- 月份 — 将月份设置为月份名称的前三个字母，例如 Jan 表示一月份。
- 日期 — 设置日期，范围介于 1 到 31 之间。
- 年份 — 将年份设置为 4 位数字，例如 2018。
- 小时 — 以 24 小时格式设置小时，其中“晚上 7 点”输入为 19。
- 分钟 — 设置介于 0 和 59 之间的分钟数。
- 秒 — 设置介于 0 和 59 之间的秒数。

系统时钟修改立即生效。无需确认缓冲区。

示例：

```
firepower-2110 /system/services # set clock apr 18 2018 9 39 30
Wed Apr 18 09:39:30 PDT 2018
firepower-2110 /system/services #
```

步骤 3 设置时区。

set timezone

系统将提示您输入与您所在的洲、国家/地区和时区区域对应的编号。在每个系统提示符处输入适当的信息。

示例：

```
firepower-2110 /system/services* # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? 2
Please select a country.
 1) Anguilla                28) Haiti
```

```
 2) Antigua & Barbuda        29) Honduras
 3) Argentina                30) Jamaica
 4) Aruba                    31) Martinique
 5) Bahamas                  32) Mexico
 6) Barbados                 33) Montserrat
 7) Belize                   34) Nicaragua
 8) Bolivia                  35) Panama
 9) Brazil                   36) Paraguay
10) Canada                   37) Peru
11) Caribbean Netherlands    38) Puerto Rico
12) Cayman Islands           39) St Barthelemy
13) Chile                    40) St Kitts & Nevis
14) Colombia                 41) St Lucia
15) Costa Rica               42) St Maarten (Dutch part)
16) Cuba                     43) St Martin (French part)
17) Curacao                  44) St Pierre & Miquelon
18) Dominica                 45) St Vincent
19) Dominican Republic       46) Suriname
20) Ecuador                  47) Trinidad & Tobago
21) El Salvador              48) Turks & Caicos Is
22) French Guiana            49) United States
23) Greenland                50) Uruguay
24) Grenada                  51) Venezuela
25) Guadeloupe               52) Virgin Islands (UK)
26) Guatemala                53) Virgin Islands (US)
27) Guyana
#? 49
Please select one of the following time zone regions.
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
 5) Eastern Time - Indiana - most locations
 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
 7) Eastern Time - Indiana - Pulaski County
 8) Eastern Time - Indiana - Crawford County
 9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Standard Time - Arizona (except Navajo)
21) Pacific Time
22) Pacific Standard Time - Annette Island, Alaska
23) Alaska Time
24) Alaska Time - Alaska panhandle
25) Alaska Time - southeast Alaska panhandle
26) Alaska Time - Alaska panhandle neck
27) Alaska Time - west Alaska
28) Aleutian Islands
29) Hawaii
#? 21

The following information has been given:

        United States
        Pacific Time
```

```
Therefore timezone 'America/Los_Angeles' will be set.
Local time is now:      Wed Jun 24 07:39:25 PDT 2018.
Universal Time is now:  Wed Jun 24 14:39:25 UTC 2018.
Is the above information OK?
1) Yes
2) No
#? 1
firepower-2110 /system/services* #
```

步骤 4 保存配置。

commit-buffer

示例：

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

步骤 5 查看时钟详细信息。

- 查看已配置的时区。

  show timezone

  ```
  firepower-2110 /system/services # show timezone
  Timezone: America/Los_Angeles
  ```

- 查看配置的日期和时间。

  show clock

  ```
  firepower-2110 /system/services # show clock
  Wed Apr 18 08:49:35 PDT 2018
  ```

示例

以下示例配置了系统时钟。

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # set clock jun 24 2015 15 27 00
firepower-2110 /system/services #
```

设置机箱名称

开始之前

您可以从 FXOS CLI 中设置用于 Firepower 2100 的名称。

过程

步骤 1 进入系统模式：

scope system

示例：

```
firepower-2110# scope system
firepower-2110 /system #
```

步骤 2 查看当前名称。

show

示例：

```
firepower-2110 /system # show
Systems:
    Name       Mode        System IP Address System IPv6 Address
    ---------- ----------- ----------------- -------------------
    firepower-2110
               Stand Alone 10.122.203.17     ::
```

步骤 3 配置新名称。

set name *device_name*

示例：

```
firepower-2110 /system # set name fp2110-2
Warning: System name modification changes FC zone name and redeploys them non-disruptively
firepower-2110 /system* #
```

步骤 4 保存配置。

commit-buffer

示例：

```
firepower-2110 /system* # commit-buffer
firepower-2110 /system #
fp2110-2 /system #
```

示例

以下示例将更改设备名称：

```
firepower-2110# scope system
firepower-2110 /system # set name New-name
Warning: System name modification changes FC zone name and redeploys them non-disruptively
```

```
firepower-2110 /system* # commit-buffer
firepower-2110 /system # show

Systems:
    Name       Mode        System IP Address System IPv6 Address
    ---------- ----------- ----------------- ------------------
    New-name   Stand Alone 192.168.100.10    ::
New-name-A /system #
```

配置域名

Firepower 2100 将域名作为后缀附加到非限定名称。例如，如果您将域名设置为“example.com”并通过不受限定的名称“jupiter”来指定系统日志服务器，则 Firepower 2100 会将名称限定为“jupiter.example.com”。

过程

步骤 1 进入系统，然后进入服务模式。

scope system

scope services

示例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

步骤 2 设置域名。

set domain-name *name*

示例：

```
firepower-2110 /system/services # set domain-name example.com
firepower-2110 /system/services* #
```

步骤 3 保存配置。

commit-buffer

示例：

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

示例

以下示例将域设置为 example.com：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # set domain-name example.com
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

配置 DNS 服务器

如果系统要求将主机名解析为 IP 地址，则您需要指定 DNS 服务器。配置多个 DNS 服务器时，系统仅以任意随机顺序搜索服务器。需要使用 DNS 来与 NTP 服务器进行通信。

开始之前

默认情况下，DNS 配置为以下 OpenDNS 服务器：208.67.222.222、208.67.220.220。

过程

步骤 1 进入系统，然后进入服务模式。

scope system

scope services

示例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

步骤 2 添加至 4 个 DNS 服务器。

enter dns*{ipv4_addr |ipv6_addr}*

示例：

```
firepower-2110 /system/services* # enter dns 10.10.5.6
firepower-2110 /system/services* # enter dns 192.168.7.2
```

步骤 3 保存配置。

commit-buffer

示例：

```
firepower-2110 /system/services* # commit-buffer
```

```
firepower-2110 /system/services #
```

示例

以下示例配置具有 IPv4 地址 192.168.200.105 的 DNS 服务器：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter dns 192.168.200.105
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

以下示例配置具有 IPv6 地址 2001:db8::22:F376:FF3B:AB3F 的 DNS 服务器。

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter dns 2001:db8::22:F376:FF3B:AB3F
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

以下示例删除具有 IP 地址 192.168.200.105 的 DNS 服务器：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # delete dns 192.168.200.105
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

添加登录前横幅

如果配置了登录前横幅，当用户登录到 Firepower 机箱管理器 时，浏览器将显示横幅文本，用户必须在消息屏幕上单击**确定**，然后系统才会提示输入用户名和密码。如果未配置登录前横幅，系统会直接进入用户名和密码输入提示屏幕。

当用户登录到 FXOS CLI 时，终端显示横幅文本，然后提示输入密码。

过程

步骤 1 进入安全模式，然后进入横幅模式：

scope security

scope banner

示例：

```
firepower-2110# scope security
```

```
firepower-2110 /security # scope banner
firepower-2110 /security/banner #
```

步骤 2 创建登录前横幅。

enter pre-login-banner

示例：

```
firepower-2110 /security/banner # enter pre-login-banner
firepower-2110 /security/banner/pre-login-banner* #
```

步骤 3 指定在用户登录 Firepower 机箱管理器或 FXOS CLI 前 FXOS 向用户显示的消息。

set message

在提示符处，键入登录前横幅消息。您可以在此字段中输入任何标准 ASCII 字符。您可以输入多行文本，每行最多 192 个字符。按 **Enter** 键换行。

在您输入信息的下一行，键入 **ENDOFBUF** 并按 **Enter** 键以完成操作。

按 **Ctrl+c** 取消设置消息对话框。

示例：

```
firepower-2110 /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower 2100
>**Unauthorized use is prohibited**
>ENDOFBUF
firepower-2110 /security/banner/pre-login-banner* #
```

步骤 4 保存配置。

commit-buffer

示例：

```
firepower-2110 /security/banner/pre-login-banner* # commit-buffer
firepower-2110 /security/banner/pre-login-banner #
```

示例

以下示例创建登录前横幅：

```
firepower-2110# scope security
firepower-2110 /security # scope banner
firepower-2110 /security/banner # create pre-login-banner
firepower-2110 /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower 2110
>**Unauthorized use is prohibited**
```

```
>Contact admin@example.com for information.
>ENDOFBUF
firepower-2110 /security/banner/pre-login-banner* # commit-buffer
firepower-2110 /security/banner/pre-login-banner #
```

配置 SSH

以下程序说明如何启用或禁用对 FXOS 机箱的 SSH 访问。默认情况下，SSH 处于启用状态。

开始之前

我们建议您在控制台执行以下步骤；否则，您可能断开与 SSH 会话的连接。

过程

步骤 1 进入系统，然后进入服务模式。

scope system

scope services

示例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

步骤 2 要配置对 Firepower 机箱的 SSH 访问，请执行以下操作之一：

- 允许对 Firepower 机箱进行 SSH 访问。

  enable ssh-server

- 禁止对 Firepower 机箱进行 SSH 访问。

  disable ssh-server

示例：

```
firepower-2110 /system/services # disable ssh-server
firepower-2110 /system/services* #
```

步骤 3 设置加密算法。

set ssh-server encrypt-algorithm 协议

设置以下一个或多个协议，用空格或逗号分隔：

- 3des-cbc
- aes128-cbc
- aes128-ctr

- aes128-gcm_openssh_com
- aes192-cbc
- aes192-ctr
- aes256-cbc
- aes256-ctr
- aes256-gcm_openssh_com
- chacha20-poly1305_openssh_com

默认情况下，允许所有协议。

示例：

```
firepower-2110 /system/services* # set ssh-server encrypt-algorithm aes256-ctr,aes256-cbc
```

步骤 4 设置密钥交换算法。

set ssh-server kex-algorithm 算法

设置以下一个或多个算法，用空格或逗号分隔：

- curve25519-sha256
- curve25519-sha256_libssh_org
- diffie-hellman-group14-sha1
- diffie-hellman-group14-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

默认情况下，允许所有协议。

示例：

```
firepower-2110 /system/services* # set ssh-server kex-algorithm
diffie-hellman-group14-sha256,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

步骤 5 设置完整性算法。

set ssh-server mac-algorithm 协议

设置以下一个或多个协议，用空格或逗号分隔：

- hmac-sha1
- hmac-sha2-256

- hmac-sha2-512

默认情况下，允许所有协议。

示例：

```
firepower-2110 /system/services* # set ssh-server mac-algorithm hmac-sha2-512
```

步骤 6 设置服务器主机密钥。

set ssh-server host-key rsa *modulus*

模数值（以位为单位）应为 8 的倍数，且介于 1024 到 2048 之间。指定的密钥模块大小越大，生成 RSA 密钥对所需的时间就越长。建议值为 2048。

示例：

```
firepower-2110 /system/services* # set ssh-server host-key rsa 2048
```

步骤 7 设置服务器密钥更新限制，以设置 FXOS 断开会话连接之前的数量（连接上允许的流量（以 KB 为单位））和次数（连接上允许的 SSH 会话空闲时间（以分钟为单位））。

set ssh-server rekey-limit volume{*kb* |**none**} **time** {分钟|**none**}

- **volume** *kb* - 设置介于 100 和 4194303 KB 之间的最大流量。默认值为无限制（无）。
- **time** 分钟 - 设置介于 10 和 1440 分钟之间的最长时间。默认值为无限制（无）。
- **none**— 禁用限制。该设置为默认设置。

示例：

```
firepower-2110 /system/services* # set ssh-server rekey-limit volume none time 1440
```

步骤 8 保存配置。

commit-buffer

示例：

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

示例

以下示例启用对 Firepower 机箱的 SSH 访问：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enable ssh-server
firepower-2110 /system/services* # commit-buffer
```

```
firepower-2110 /system/services #
```

为 HTTP 或 IPSec 配置证书、密钥环和受信任点

HTTPS 和 IPSec 使用公钥基础设施 (PKI) 的组件在两个设备（例如客户端浏览器和 Firepower 2100）之间建立安全通信。

关于证书、密钥环和受信任点

HTTPS 使用公钥基础设施 (PKI) 的组件在两个设备（例如客户端浏览器和 Firepower 2100）之间建立安全通信。

加密密钥和密钥环

每个 PKI 设备具有一对非对称 Rivest-Shamir-Adleman (RSA) 加密密钥或椭圆曲线数字签名算法 (ECDSA) 加密密钥（其中一个保持为私有，另一个公开），存储在内部密钥环中。用任一密钥加密的消息均可用另一密钥解密。要发送加密消息，发送方使用接收方的公钥加密消息，接收方使用自己的私钥解密消息。发送方也可以通过使用其自有私钥加密（也称为“签名”）已知消息来证明其对公钥的所有权。如果接收方可使用上述公钥成功解密消息，则发送方对相应私钥的所有权得以证明。加密密钥长度可以不同，典型的长度为 512 位至 2048 位。一般来说，秘钥长度越长，安全性就越高。FXOS 提供一个默认 RSA 密钥环，带有 2048 位的初始密钥对，并允许创建更多密钥环。

证书

作为安全通信前的准备，两台设备首先会交换数字证书。证书是包含设备的公钥以及有关设备身份的签名信息的文件。要仅支持加密通信，设备可生成自己的密钥对和自签名证书。远程用户连接至显示自签名证书的设备时，用户无法轻易验证设备身份，且用户浏览器最初会显示身份验证警告。默认情况下，FXOS 包含内置的自签名证书，其中包含来自默认密钥环的公钥。

如果证书过期，则必须手动重新生成默认密钥环证书。

受信任点

要为 FXOS 提供更强的身份验证，您可从受信任来源或信任点获取并安装确认设备身份的第三方证书。第三方证书由颁发证书的受信任点签署，该受信任点可以是根证书颁发机构 (CA)，也可以是中间 CA 或信任锚（通向根 CA 的信任链一部分）。要获取新证书，您必须通过 FXOS 生成证书请求，并将请求提交至受信任点。

注释 证书必须采用 Base64 编码 X.509 (CER) 格式。

安装受信任身份证书

默认情况下，生成登录 SSL 证书以与 Firepower 机箱管理器一起使用。由于该证书是自签名证书，客户端浏览器不会自动信任它。新的客户端浏览器首次访问 Firepower 机箱管理器时，浏览器会显示 SSL 警告，要求用户在访问 Firepower 机箱之前接受证书。使用以下程序，使用 FXOS CLI 生成证书

签名请求 (CSR)，并安装得到的身份证书以供 Firepower 机箱管理器使用。此身份证书允许客户端浏览器信任连接，并直接启动 Web 界面而无警告。FXOS 支持最大值为 8 的密钥环，包括**默认**密钥环。

开始之前

配置 DNS 服务器，第 46 页。

过程

步骤 1 进入安全模式。

scope security

示例：

```
firepower-2110# scope security
firepower-2110 /security #
```

步骤 2 为要添加到密钥环的证书定义受信任点。

create trustpoint *name*

示例：

```
firepower-2110 /security # create trustpoint trust1
firepower-2110 /security/trustpoint* #
```

步骤 3 粘贴到证书链中。从信任锚或证书颁发机构获取证书信任链。

set certchain [*certchain*]

如果不在命令中指定证书信息，系统将提示您输入证书或信任点列表，定义到根证书授权 (CA) 的证书路径。在您输入信息的下一行，键入 **ENDOFBUF** 以完成操作。证书必须采用 Base64 编码 X.509 (CER) 格式。

对于使用中间证书的证书颁发机构，必须对根证书和中间证书进行组合。在文本文件中，将根证书粘贴在顶部，然后是链中的每一个中间证书，包括所有 BEGIN CERTIFICATE 和 END CERTIFICATE 标记。在 FXOS CLI 中复制并粘贴整个文本块。

示例：

```
firepower-2110 /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
```

```
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
firepower-2110 /security/trustpoint* #
```

步骤 4 退出信任点模式。

exit

示例：

```
firepower-2110 /security/trustpoint* # exit
firepower-2110 /security* #
```

步骤 5 创建密钥环。

create keyring *keyring_name*

示例：

```
firepower-2110 /security # create keyring keyring1
firepower-2110 /security/keyring* #
```

步骤 6 将密钥类型设置为 RSA（默认）或 ECDSA。

set keypair-type {**rsa** | **edcsa**}

示例：

```
firepower-2110 /security/keyring* # set keypair-type edcsa
```

步骤 7 （对于 RSA）设置 SSL 密钥长度（以位为单位）。

set modulus {**mod1536** |**mod2048** | **mod2560** | **mod3072** | **mod3584** | **mod4096**}

示例：

```
firepower-2110 /security/keyring* # set modulus mod2048
```

步骤 8 （对于 EDCSA）设置椭圆曲线。

set elliptic-curve {**secp256r1** | **secp384r1** | **secp384r1**}

示例：

```
firepower-2110 /security/keyring* # set elliptic-curve secp384r1
```

步骤 9 创建证书请求。

create certreq

示例：

```
firepower-2110 /security/keyring* # create certreq
firepower-2110 /security/keyring/certreq* #
```

步骤 10 创建证书密码。

set password

示例：

```
firepower-2110 /security/keyring/certreq* # set password
Certificate request password: diagonalapple
Confirm certificate request password: diagonalapple
```

步骤 11 指定 Firepower 2100 的 IP 地址 或 FQDN 。

set{**ip** |**ipv6**} {*ipv_address* |*fqdn*}

您可以配置多个 IP 地址。

示例：

```
firepower-2110 /security/keyring/certreq* # set ip 10.10.9.2
```

步骤 12 指定用于机箱的 DNS 查找的机箱的完全限定域名。

set subject-name *fqdn*

SubjectName 和至少一个 DNS SubjectAlternateName 名称为必填项。SubjectName 会自动添加为 DNS SubjectAlternateName。

示例：

```
firepower-2110 /security/keyring/certreq* # set subject-name firepower1.example.com
```

步骤 13 （可选） 配置高级选项。

a) 指定公司所在国家/地区的国家/地区两字代码：

set country *country_name*

示例：

```
firepower-2110 /security/keyring/certreq* # set country us
```

b) 指定使用者备用名称以将此证书应用于另一个主机名。

set dns *subject_alt_name*

您可以配置多个 DNS 名称。

示例：

```
firepower-2110 /security/keyring/certreq* # set dns firepower2.example.com
```

c) 指定与证书请求相关联的邮件地址。

set e-mail *E-mail_name*

您可以配置多个电子邮件地址。

示例：

```
firepower-2110 /security/keyring/certreq* # set e-mail admin@example.com
```

d) 指定请求此证书的公司总部所在的城市或城镇。

set locality *locality_name*

示例：

```
firepower-2110 /security/keyring/certreq* # set locality boulder
```

e) 指定请求证书的组织。

set org-name *organization_name*

示例：

```
firepower-2110 /security/keyring/certreq* # set org-name Example.com
```

f) 指定组织单位。

set org-unit-name *organizational_unit_name*

示例：

```
firepower-2110 /security/keyring/certreq* # set org-unit-name engineering
```

g) 指定请求此证书的公司总部所在的省、市或自治区。

set state *state_province_or_county*

示例：

```
firepower-2110 /security/keyring/certreq* # set state co
```

步骤 14 保存配置。

commit-buffer

在生成证书签名请求之前，将使用DNS解析所有主机名。如果任何主机名无法解析，则命令错误。

示例：

```
firepower-2110 /security/keyring/certreq* # commit-buffer
firepower-2110 /security/keyring/certreq #
```

步骤 15 显示证书请求，复制并发送至信任锚或证书颁发机构。

show certreq

复制证书请求文本（包括开始 [BEGIN] 和结束 [END] 行），并将其保存到文件中。

示例：

```
firepower-2110 /security/keyring/certreq # show certreq
Certificate request subject name: firepower1.example.com
Certificate request ip address: 10.10.10.9
Certificate request e-mail name:
Certificate request ipv6 address: ::
Certificate request country name:
State, province or county (full name):
Locality name (eg, city):
Organisation name (eg, company):
Organisational Unit Name (eg, section):
DNS name (subject alternative name):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIICoDCCAYgCAQAwITEfMB0GA1UEAwwWZmlyZXBvd2VyMS5leGFtcGxlLmNvbTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALJM7bmSCJte3gAU9DgDVN3E
tEfrbf0hMeLYgs5qkkvW7T8x3gHKn2Lwk4wFFAdHPxceVZwaBnXW8F5MFzdtyBY+
Du+RkpraLtle4HEMdNw1rnoDcv4ZHmbK47XYR1SFXSzer5lOXptGbOCloUn34L6/
pKlDlfV+1L+LlDYD++RG2DhbekWcFk13loZvCVhw99Wmc4X7CsypKY4uGH3lAwnl
/TF32ORXi0t2GXju6kbqUahhxN2kGxL7+4eLBeA/ninajCkJDIGJlnXuFa2ArfbF
39p+3UuVzcc9V/OH6d+buLjmQvtn+DwoPQhCVDYlNt+p3ZgnqnJWULNLBPMlof0C
AwEAAaA6MDgGCSqGSIb3DQEJDjErMCkwJwYDVR0RBCAwHoIWZmlyZXBvd2VyMS5l
eGFtcGxlLmNvbYcECgoKCTANBgkqhkiG9w0BAQsFAAOCAQEAjBw8lEb6cRapyMh/
Dfiyuet4wT0QmXQKy3xLXQjv6RGb5SOf3NkcaNvcx3KuKJwoJQGhdRV4Jhk4rgmT
QmlWX4rY7B2MFUwf6qSaj/E5W0N0RQg+5aZ/hZjPGV3zcuzY6yfixxXBpoPAirZQ
2luPaa21+HR4LTDInRj0127xMIkeKmv7AHSjyMoJdgs8DGJilTwPy93kZV//Iq9P
LrnKR7gpsXzXOoK6PTxP3pwhC21qjdmevn3ICPjDI68AtqjAuB15p/T2l+GFi/gB
XJMx2Mm9qiope3FEXIGH2ZhbJ+P7oBfGzgx2EHSI8H98O8a9uO8WV2yd/dKtv2IG
ICxHEw==
-----END CERTIFICATE REQUEST-----
```

步骤 16 根据证书颁发机构的注册流程，向证书颁发机构提供CSR输出。如果请求成功，证书颁发机构将发回一份已使用 CA 的私钥进行数字签名的身份证书。

步骤 17 退出证书请求模式。

exit

示例：

```
firepower-2110 /security/keyring/certreq # exit
firepower-2110 /security/keyring #
```

步骤 18 指定您之前创建的受信任点。

set trustpoint *name*

示例：

```
firepower-2110 /security/keyring # set trustpoint trust1
firepower-2110 /security/keyring* #
```

步骤 19 从信任锚或证书颁发机构上传证书。

set cert

在提示符后，粘贴从信任锚或证书颁发机构接收到的证书文本。在证书后的下一行，键入**ENDOFBUF**完成证书输入。

注释　证书必须采用 Base64 编码 X.509 (CER) 格式。

示例：

```
firepower-2110 /security/keyring* #
```

步骤 20 保存配置。

commit-buffer

示例：

```
firepower-2110 /security/keyring* # commit-buffer
firepower-2110 /security/keyring #
```

步骤 21 显示导入的证书的内容，确认 **Certificate Status** 值显示为 **Valid**。

show keyring *keyring_name* **detail**

示例：

```
firepower-2110 /security #  scope security
firepower-2110 /security #  show keyring kr1 detail
Keyring firepower_cert:
    RSA key modulus: Mod2048
    Trustpoint CA: firepower_chain
    Certificate status: Valid
    Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            45:00:00:00:0a:de:86:55:16:82:24:f3:be:00:00:00:00:00:0a
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: DC=local, DC=naaustin, CN=naaustin-NAAUSTIN-PC-CA
        Validity
            Not Before: Apr 28 13:09:54 2016 GMT
            Not After : Apr 28 13:09:54 2018 GMT
        Subject: C=US, ST=California, L=San Jose, O=Cisco Systems, OU=TAC,
CN=fp4120.test.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b3:43:8d:e6:06:a0:91:f6:76:7e:2e:09:54:40:
                    0d:1b:ee:d8:1a:07:07:6e:75:2d:ec:ba:55:c8:c0:
                    a1:9c:a3:8f:26:30:70:91:43:0d:40:0d:66:42:c4:
                    50:0d:c6:c9:db:7d:bf:b0:ad:1f:31:29:f2:a8:e2:
                    fc:27:30:bb:8a:dc:5e:54:46:51:cb:3e:ff:6b:1e:
```

```
                    d6:18:db:de:83:f5:cf:fb:37:74:de:7b:78:19:73:
                    3a:dc:5b:2b:3d:c3:e6:03:b1:30:82:a0:d2:2e:84:
                    a1:b4:11:15:d7:48:61:7f:8f:8d:c3:8a:4a:09:9f:
                    9e:49:29:12:26:44:c1:d5:91:da:29:5f:5b:b6:d6:
                    20:de:47:ff:50:45:14:82:4f:c4:ca:b5:6a:dc:1f:
                    ae:d8:3b:28:a0:f5:6a:ef:a9:93:9b:c0:70:60:ca:
                    87:6c:91:2f:e0:f9:ae:46:35:84:f3:cc:84:bd:5c:
                    07:ec:94:c4:8a:3f:4e:bf:16:da:b6:30:e3:55:22:
                    47:64:15:11:b4:26:a7:bf:20:6f:1a:e2:cf:fd:0f:
                    cd:9a:fd:cb:a3:71:bd:21:36:cb:2f:98:08:61:95:
                    5a:b5:3c:69:e8:74:d4:7b:31:f6:30:82:33:39:ab:
                    d4:e9:dd:6d:07:da:e7:cb:18:06:b6:1e:5d:3d:5d:
                    1d:85
                Exponent: 65537 (0x10001)
            X509v3 extensions:
                X509v3 Subject Alternative Name:
                    DNS:fp4120.test.local
                X509v3 Subject Key Identifier:
                    FF:55:A9:B2:D8:84:60:4C:6C:F0:39:59:59:CB:87:67:03:ED:BB:94
                X509v3 Authority Key Identifier:
                    keyid:C8:89:DB:0C:73:EB:17:01:04:05:C6:F1:19:28:10:5B:BA:4E:54:89
                X509v3 CRL Distribution Points:
                    Full Name:
                      URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=naaustin-pc,CN=CDP,
                        CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
                      DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint

                Authority Information Access:
                    CA Issuers - URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=AIA,
                      CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
                      DC=local?cACertificate?base?objectClass=certificationAuthority
                1.3.6.1.4.1.311.20.2:
                    ...W.e.b.S.e.r.v.e.r
                X509v3 Key Usage: critical
                    Digital Signature, Key Encipherment
                X509v3 Extended Key Usage:
                    TLS Web Server Authentication
    Signature Algorithm: ecdsa-with-SHA256
         30:45:02:20:57:b0:ec:d7:09:8a:b1:2d:15:1b:f2:c6:39:10:
         e3:f7:55:a3:6a:08:e8:24:41:df:4f:16:41:b6:07:35:4b:bf:
         02:21:00:ed:47:4e:6e:24:89:04:6f:cf:05:98:e6:b2:0a:08:
         2b:ad:1a:91:b8:e8:b4:e4:ef:51:d5:1d:f5:be:8a:d5:4c
-----BEGIN CERTIFICATE-----
MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkjOPQQDAjBT
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs
aWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFjAUBgNVBAoTDUNpc2NvIFN5c3Rl
bXMxDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
BwdudS3sulXIwKGco48mMHCRQw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
yodskS/g+a5GNYTzzIS9XAfslMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
/cujcb0hNssvmAhhlVq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2Hl09XR2FAgMB
AAGjggJYMIICVDAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
FgQU/1WpstiEYExs8DlZWcuHZwPtu5QwHwYDVR0jBBgwFoAUyInbDHPrFwEEBcbx
GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp
b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlz
dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHMBggrBgEF
BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
QVVTVElOLVBDLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
```

```
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
P2NBQ2VydGlmaWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0
aG9yaXR5MCEGCSsGAQQBgjcUAgQUHhIAVwBlAGIAUwBlAHIAdgBlAHIwDgYDVR0P
AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
sgoIK60akbjotOTvUdUd9b6K1Uw=
-----END CERTIFICATE-----

    Zeroized: No
```

示例

以下示例将证书添加到新的密钥环。

```
firepower-2110# scope security
firepower-2110 /security # enter trustpoint tPoint10
firepower-2110 /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
firepower-2110 /security/trustpoint* # exit
firepower-2110 /security* # enter keyring kr220
firepower-2110 /security/keyring* # set modulus mod1024
firepower-2110 /security/keyring* # enter certreq
Certificate request password: peonygarage
Confirm certificate request password: peonygarage
firepower-2110 /security/keyring/certreq* # set ip 192.168.200.123
firepower-2110 /security/keyring/certreq* # set subject-name sjc04.example.com
firepower-2110 /security/keyring/certreq* # commit-buffer
firepower-2110 /security/keyring/certreq # show certreq
Certificate request subject name: sjc04.example.com
Certificate request ip address: 192.168.200.123
Certificate request e-mail name:
Certificate request country name:
State, province or county (full name):
Locality (eg, city):
Organization name (eg, company):
Organization Unit name (eg, section):
```

```
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

firepower-2110 /security/keyring/certreq # exit
firepower-2110 /security/keyring #
firepower-2110 /security/keyring # set trustpoint tPoint10
firepower-2110 /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
firepower-2110 /security/keyring* # commit-buffer
firepower-2110 /security/keyring #
```

重新生成默认密钥环证书

如果证书过期，则必须手动重新生成默认密钥环证书。

过程

步骤 1 进入安全模式。

scope security

示例：

```
firepower-2110# scope security
firepower-2110 /security #
```

步骤 2 输入默认密钥环。

enter keyring default

示例：

```
firepower-2110 /security # enter keyring default
firepower-2110 /security/keyring #
```

步骤 3 重新生成默认密钥环：

set regenerate yes

示例：

```
firepower-2110 /security/keyring # set regenerate yes
```

步骤 4 保存配置。

commit-buffer

示例：

```
firepower-2110 /security/keyring* # commit-buffer
firepower-2110 /security/keyring #
```

示例

以下示例重新生成默认密钥环：

```
firepower-2110# scope security
firepower-2110 /security # enter keyring default
firepower-2110 /security/keyring # set regenerate yes
firepower-2110 /security/keyring* # commit-buffer
firepower-2110 /security/keyring #
```

配置 HTTPS

默认情况下，在端口 443 上启用 HTTPS 服务。如果要禁止 Firepower 机箱管理器访问，则可以禁用 HTTPS，或自定义 HTTPS 配置，包括指定用于 HTTPS 会话的密钥环。默认情况下，Firepower 2100 使用具有自签名证书的默认密钥环。

注释 完成 HTTPS 配置（包括更改将由 HTTPS 使用的端口和密钥环）后，一旦保存或提交任务，所有当前 HTTP 和 HTTPS 会话都将关闭，而不显示警告。

过程

步骤 1 （可选） 安装受信任身份证书，第 52 页。

步骤 2 进入系统，然后进入服务模式。

scope system

scope services

示例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
Firepower-chassis /system/services #
```

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

- 允许对 Firepower 机箱进行 HTTPS 访问。

  enable https

- 禁止对 Firepower 机箱进行 HTTPS 访问。

  disable https

示例：

```
firepower-2110 /system/services # disable https
firepower-2110 /system/services* #
```

步骤 4 （可选） 指定 HTTPS 端口。默认端口为端口 443。

set https port *port_num*

示例：

```
Firepower-chassis /system/services* # set https port 4443
```

步骤 5 （可选） 指定您添加的密钥环的名称。请参阅 安装受信任身份证书，第 52 页。

set https keyring *keyring_name*

示例：

```
Firepower-chassis /system/services* # set https keyring kr1
```

步骤 6 （可选） 指定域使用的 Cipher Suite 安全级别。

set https cipher-suite-mode*cipher_suite_mode*

cipher_suite_mode 可以是以下关键字之一：

- **high-strength**
- （默认） **medium-strength**
- **low-strength**
- **custom** - 允许您使用 **set https cipher-suite** 命令指定用户定义的 Cipher Suite 规格规范字符串。

示例：

```
Firepower-chassis /system/services* # set https cipher-suite-mode high-strength
```

步骤 7 （可选） 如果将密码套件模式设置为 **custom**，请指定自定义密码套件。

set https cipher-suite*cipher_suite_string*

cipher_suite_string 可以包含最多 256 个字符，并且必须符合 OpenSSL Cipher Suite 规范。不得使用任何空格或特殊字符，！（感叹号）、+（加号）、-（连字符）和 :（冒号）除外。有关详细信息，请参阅 http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite。

例如，默认情况下，FXOS 使用的中强度规范字符串为：
ALL:!ADH:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL

示例：

```
Firepower-chassis /system/services* # set https cipher-suite
DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
```

步骤 8 设置 SSL 版本

set https access-protocols *comma_separated_values*

comma_separated_values 包括：

- **tlsv1**
- **tlsv1.1**
- **tlsv1.2**
- **sslv3**

注释 较新的浏览器不支持 SSLv3，因此您还应指定其他协议。如果您仅指定 SSLv3，您可能会在浏览器中看到指示安全协议版本不受支持的错误。

步骤 9 （可选） 启用或禁用证书吊销列表检查。

set revoke-policy {**relaxed** |**strict**}

示例：

```
Firepower-chassis /system/services* # set revoke-policy strict
```

步骤 10 保存配置。

commit-buffer

示例：

```
Firepower-chassis /system/services* # commit-buffer
```

```
firepower-2110 /system/services #
```

示例

以下示例启用 HTTPS，将端口号设置为 4443，将密钥环名称设为 kring7984，将 Cipher Suite 安全级别设置为高：

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # enable https
Firepower-chassis /system/services* # set https port 4443
Warning: When committed, this closes all the web sessions.
Firepower-chassis /system/services* # set https keyring kring7984
Firepower-chassis /system/services* # set https cipher-suite-mode high
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

配置 IPSec 安全通道

您可以配置 IPSec 隧道来加密管理流量。Firepower 2100 支持以下密码和算法：

表 *2: IKE* 和 *ESP* 密码和算法

类型	值
密码	aes128、aes192、aes256、aes128gcm16
伪随机函数 (PRF)（仅 IKE）	prfsha1、prfsha384、prfsha512、prfsha256
完整性算法	sha1、sha256、sha384、sha512、sha1_160
Diffie-Hellman 组	modp2048、curve25519、ecp256、ecp384、ecp521、modp3072、modp4096

注释 在 FIPS 或 Common Criteria 模式下不支持 curve25519。

开始之前

对于 FIPS 模式，IPSec 对等体必须支持 RFC 7427。

过程

步骤 1 安装受信任身份证书，第 52 页。

步骤 2 进入安全模式，随后进入 IPSec 模式：

scope security

scope ipsec

示例：

```
Firepower-2110# scope security
Firepower-2110 /security # scope ipsec
Firepower-2110 /security/ipsec #
```

步骤 3 （可选） 设置日志冗长级别：

set log-level *0-4*

示例：

```
Firepower-2110 /security/ipsec # set log-level 3
Firepower-2110 /security/ipsec* #
```

步骤 4 （可选） 配置执行 IKE 和 SA 连接间加密密钥强度的匹配：

set sa-strength-enforcement {**yes** |**no**}

- **yes**- 如果 IKE 协商的密钥大小小于 ESP 协商的密钥大小时，连接失败。
- **no**- SA 执行检查通过且连接成功。

示例：

```
Firepower-2110 /security/ipsec # set sa-strength-enforcement yes
Firepower-2110 /security/ipsec* #
```

步骤 5 创建并输入一个 IPSec 连接：

create connection *connection_name*

步骤 6 将 IPSec 模式设置为隧道或传输：

set mode *tunnel_or_transport*

步骤 7 设置本地 IP 地址：

set local-address *ip_address*

步骤 8 设置远程 IP 地址：

set remote-address *ip_address*

如果已配置 DNS 服务器，则可以将远程地址指定为 FQDN（请参阅配置 DNS 服务器，第 46 页）。

示例：

```
Firepower-2110 /security/ipsec/connection* # set remote-address
```

步骤 9 如果使用隧道模式，则设置远程子网：

set remote-subnet *ip/mask*

步骤 10 设置远程身份：

set remote-ike-id *remote_identity_name*

如果您使用 **set fqdn-enforce** 命令执行 FQDN 使用，则需要使用 FQDN 来执行此命令。

示例：

```
Firepower-2110 /security/ipsec/connection* # set remote-ike-id charlesdarwin.cisco.com
```

步骤 11 执行 FQDN 使用。

set fqdn-enforce {**none** | **remote-ike-id**}

如果启用此功能，则必须配置 DNS（请参阅 配置 DNS 服务器，第 46 页）。默认情况下会启用实施，但在 9.13(1) 之前创建的连接除外；您必须手动启用这些旧连接的实施。

您必须以 FQDN 格式配置有效的远程 IKE ID (**set remote-ike-id**)。如果禁用 FQDN 实施，则远程 IKE ID 是可选的，并且可以设置为任何格式（FQDN、IP 地址、使用者名称等）。

示例：

```
Firepower-2110 /security/ipsec/connection* # set fqdn-enforce remote-ike-id
```

步骤 12 设置密钥环名称：

set keyring-name *name*

步骤 13 （可选）设置密钥环密码：

set keyring-passwd *passphrase*

步骤 14 （可选）设置 IKE-SA 生命周期（分钟）：

set ike-rekey-time *minutes*

minutes 值可以是 60-1440（包含在内）之间的任何整数。

步骤 15 （可选）设置子 SA 生命周期（分钟）(30-480)：

set esp-rekey-time 分钟

minutes 值可以是 30-480（包含在内）之间的任何整数。

步骤 16 （可选）设置初次连接期间重新传输序列的执行次数：

set keyringtries *retry_number*

retry_number 值可以是 1-5（包含在内）之间的任何整数。

步骤 17 （可选）启用或禁用证书吊销列表检查：

set revoke-policy *{ relaxed | strict }*

步骤 18 启用连接：

set admin-state enable

步骤 19 重新加载连接：

reload-conns

将重试以前未建立的连接。已建立的连接保持不变。

步骤 20 （可选）将现有信任点名称添加至 IPsec：

create authority *trustpoint_name*

配置管理访问

默认情况下，Firepower 2100 允许对 Firepower 机箱管理器进行 HTTPS 访问，和在管理 1/1 192.168.45.0/24 网络上进行 SSH 访问。如果您要允许从其他网络进行访问，或者允许 SNMP，则必须添加或更改访问列表。

过程

步骤 1 进入系统，然后进入服务模式。

scope system

scope services

示例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

步骤 2 为要启用访问权限的服务创建访问列表。

IPv4：

enter ip-block *ip prefix_length* {**https** | **snmp** | **ssh**}

IPv6：

enter ipv6-block *ip prefix_length* **https** | **snmp** | **ssh**}

对于各 IP 地址块（v4 或 v6），可为各服务配置最多 25 个不同子网。

- *ip* — 子网 0.0.0.0 和前缀 0 允许无限制无限访问服务。
- *prefix_length* — 对于 IPv4，前缀长度为 0 到 32。对于 IPv6，前缀长度为 0 到 128。

示例：

```
firepower-2110 /system/services # enter ip-block 0.0.0.0 0 https
```

```
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 10.0.0.0 8 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.0.0 16 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 10.10.3.0 24 snmp
firepower-2110 /system/services/ip-block* #
```

步骤 3 保存配置。

commit-buffer

示例：

```
firepower-2110 /system/services/ip-block* # commit-buffer
firepower-2110 /system/services/ip-block #
```

示例

IPv4：

```
firepower-2110 # scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enter ip-block 10.1.1.0 24 https
firepower-2110 /system/services/ip-block* # commit-buffer
firepower-2110 /system/services/ip-block # exit
firepower-2110 /system/services # enter ip-block 10.2.1.0 24 ssh
firepower-2110 /system/services/ip-block* # commit-buffer
firepower-2110 /system/services/ip-block # exit
firepower-2110 /system/services # enter ip-block 10.3.1.0 24 snmp
firepower-2110 /system/services/ip-block* # commit-buffer
firepower-2110 /system/services/ip-block # exit
firepower-2110 /system/services # show ip-block
Permitted IP Block:
    IP Address      Prefix Length Protocol
    --------------- ------------- --------
    10.1.1.0        24            Https
    10.2.1.0        24            Ssh
    10.3.1.0        24            Snmp
```

IPv6：

```
firepower-2110 /system/services # enter ipv6-block 2001:0DB8:BA98:: 64 ssh
firepower-2110 /system/services/ipv6-block* # commit-buffer
firepower-2110 /system/services/ipv6-block # exit
firepower-2110 /system/services # enter ipv6-block 2001:0DB8:BA98:: 64 snmp
firepower-2110 /system/services/ipv6-block* # commit-buffer
firepower-2110 /system/services/ipv6-block # exit
firepower-2110 /system/services # enter ipv6-block 2001:0DB8:BA98:: 64 https
firepower-2110 /system/services/ipv6-block* # commit-buffer
firepower-2110 /system/services/ipv6-block # exit
firepower-2110 /system/services # show ipv6-block
Permitted IPv6 Block:
    IPv6 Address Prefix Length Protocol
    ------------ ------------- --------
```

```
2001:0DB8:BA98::    64      Https
2001:0DB8:BA98::    64      Snmp
2001:0DB8:BA98::    64      Ssh
```

为管理客户端配置 DHCP 服务器

您可以为连接到管理 1/1 接口的客户端启用 DHCP 服务器。默认情况下，使用以下地址范围启用服务器：192.168.45.10-192.168.45.12。如果要更改管理 IP 地址，则必须禁用 DHCP（请参阅更改 FXOS 管理 IP 地址或网关，第 93 页）。然后，您可以为新网络重新启用 DHCP。

过程

步骤 1 进入系统，然后进入服务模式。

scope system

scope services

示例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services #
```

步骤 2 要配置 DHCP 服务器，请执行以下操作之一：

- 启用 DHCP 服务器。

  enable dhcp-server *start_ip end_ip*

- 禁用 DHCP 服务器。

  disable dhcp-server

示例：

```
firepower-2110 /system/services # enable dhcp-server 10.10.10.5 10.10.10.50
firepower-2110 /system/services* #
```

步骤 3 保存配置。

commit-buffer

示例：

```
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

示例

以下示例启用 DHCP 服务器：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enable dhcp-server 192.168.1.8 192.168.1.40
firepower-2110 /system/services* # commit-buffer
firepower-2110 /system/services #
```

配置系统日志消息传递

日志对常规故障排除及事件处理均有帮助。您可以将系统日志消息发送到 Firepower 2100 控制台、SSH 会话或本地文件。

这些系统日志消息仅适用于 FXOS 机箱。对于 ASA 系统日志消息，必须在 ASA 配置中配置日志记录。

过程

步骤 1 进入监控模式。

scope monitoring

示例：

```
firepower-2110# scope monitoring
firepower-2110 /monitoring #
```

步骤 2 配置生成系统日志消息的本地源。

- **enable syslog source** {**audits** | **events** | **faults**}
- **disable syslog source** {**audits** | **events** | **faults**}

示例：

```
firepower-2110 /monitoring # disable syslog source audits
firepower-2110 /monitoring* # enable syslog source events
firepower-2110 /monitoring* # enable syslog source faults
```

步骤 3 将系统日志消息发送到控制台。

a) 启用或禁用向控制台发送系统日志。

- **enable syslog console**
- **disable syslog console**

示例：

```
firepower-2110 /monitoring* # enable syslog console
```

b) 选择要在控制台上显示的最低消息级别。

set syslog console level {**emergencies** | **alerts** | **critical**}

系统在控制台上显示此级别及更高级别。级别选项按紧急程度从高到低的顺序列出。默认级别为“严重 (Critical)”。

示例：

```
firepower-2110 /monitoring* # set syslog console level alerts
```

步骤 4 将系统日志消息发送到 SSH 会话。

a) 启用或禁用将系统日志消息发送到 SSH 会话。

- **enable syslog monitor**
- **disable syslog monitor**

示例：

```
firepower-2110 /monitoring* # enable syslog monitor
```

b) 选择要在 SSH 上显示的最低消息级别。

set syslog monitor level {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}

系统显示此级别及更高级别。级别选项按紧急程度从高到低的顺序列出。默认级别为“严重 (Critical)”。

注释 只有当您输入了 **terminal monitor** 命令之后，才在终端监视器上显示低于“严重”级别的消息。

示例：

```
firepower-2110 /monitoring* # set syslog monitor level alerts
```

步骤 5 将系统日志消息发送至文件。

a) 启用或禁用向系统日志文件写入系统日志消息。

- **enable syslog file**
- **disable syslog file**

示例：

```
firepower-2110 /monitoring* # enable syslog file
```

b) 指定记录消息的文件的名称。

set syslog file name *filename*

文件名中最多包含 16 个字符。

示例：

```
firepower-2110 /monitoring* # set syslog file name syslog1
```

c) 选择要存储到文件中的最低消息级别。

set syslog file level {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}

系统在系统日志中存储此级别及以上消息。级别选项按紧急程度从高到低的顺序列出。默认级别为“严重 (Critical)”。

示例：

```
firepower-2110 /monitoring* # set syslog file level debugging
```

d) 在系统开始用最新消息覆写最旧消息之前，请指定最大文件大小（以字节为单位）。

set syslog file size 文件大小

范围为 4096 到 4194304 字节。

示例：

```
firepower-2110 /monitoring* # set syslog file size 60000
```

步骤 6 保存配置。

commit-buffer

示例：

```
firepower-2110 /monitoring* # commit-buffer
firepower-2110 /monitoring #
```

示例

以下示例介绍如何启用在本地文件中存储系统日志消息：

```
firepower-2110# scope monitoring
firepower-2110 /monitoring # disable syslog console
firepower-2110 /monitoring* # disable syslog monitor
```

```
firepower-2110 /monitoring* # enable syslog file
firepower-2110 /monitoring* # set syslog file name SysMsgsFirepower
firepower-2110 /monitoring* # set syslog file level notifications
firepower-2110 /monitoring* # set syslog file size 4194304
firepower-2110 /monitoring* # commit-buffer
firepower-2110 /monitoring #
```

启用 SNMP

本节介绍如何在 Firepower 机箱上配置简单网络管理协议 (SNMP)。

关于 SNMP

SNMP 是一种应用层协议，提供 SNMP 管理器和代理之间的通信消息格式。SNMP 提供用于监控和管理网络中的设备的标准化框架和通用语言。

SNMP 框架由三个部分组成：

- SNMP 管理器 - 用于通过 SNMP 来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 机箱的数据并根据需要向 SNMP 管理器报告数据。Firepower 机箱包含代理和 MIB 集合。
- 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。

SNMP 通知

SNMP 的一个关键功能是能够生成来自 SNMP 代理的通知。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 机箱将 SNMP 通知生成为陷阱或通知。陷阱不如通知可靠，因为 SNMP 管理器在收到陷阱时不发送任何确认，并且 Firepower 机箱无法确定是否已收到陷阱。收到通告请求的 SNMP 管理器使用一个 SNMP 响应协议数据单元 (PDU) 来确认消息。如果 Firepower 机箱不接收 PDU，则其可以再次发送通知请求。

SNMP 安全级别和权限

SNMPv1、SNMPv2c 和 SNMPv3 分别表示不同的安全模型。安全模型与所选安全级别结合来确定处理 SNMP 消息时应用的安全机制。

安全级别确定查看与 SNMP 陷阱关联的消息时所需的权限。权限级别确定是否需要防范消息泄露或免受身份验证。受支持的安全级别取决于实施的安全模式。SNMP 安全级别支持以下一个或多个权限：

- 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级别。安全模型是为用户和用户所处的角色设置的身份验证策略。安全级别是安全模型中允许的安全级别。安全模型和安全级别相结合来确定在处理 SNMP 数据包时采用的安全机制。

支持的 SNMP 安全模型和级别组合

下表确定安全模型和级别的组合含义。

表 *3: SNMP* 安全模型和级别

型号	级别	身份验证	加密	状况
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。除基于密码块链 (CBC) DES (DES-56) 标准的身份验证外，还提供数据加密标准 (DES) 56 位加密。

SNMPv3 安全功能

SNMPv3 通过将在网络上对帧进行身份验证和加密相结合来提供对设备的安全接入。SNMPv3 仅按已配置的用户来授权管理操作，并会加密 SNMP 消息。SNMPv3 基于用户的安全模型 (USM) 是指 SNMP 消息级别安全，并提供以下服务：

- 消息完整性 - 确保消息未在未经授权的情况下进行修改或销毁，并且数据序列未修改至超出可以非恶意形式出现的程度。
- 消息来源身份验证 - 确保对用户（系统代表该用户发出此已接收数据）的声明身份进行确认。
- 消息机密性和加密 - 确保不向未经授权的个人、实体或流程提供或披露信息。

SNMP 支持

Firepower 机箱为 SNMP 提供下列支持：

针对 MIB 的支持

Firepower 机箱支持对 MIB 的只读访问。

适用于 SNMPv3 用户的身份验证协议

Firepower 机箱针对 SNMPv3 用户支持 HMAC-SHA-96 (SHA) 身份验证协议。

适用于 SNMPv3 用户的 AES 隐私协议

除了基于SHA的身份验证，Firepower机箱还提供了使用AES-128位高级加密标准的隐私。Firepower机箱使用隐私密码生成128位AES密钥。AES隐私密码至少可具有八个字符。如果口令用明文指定，您可以指定最多80个字符。

配置 SNMP

启用 SNMP，添加陷阱和 SNMPv3 用户。

过程

步骤 1 进入监控模式。

scope monitoring

示例：

```
firepower-2110# scope monitoring
firepower-2110 /monitoring #
```

步骤 2 启用 SNMP。

enable snmp

示例：

```
firepower-2110 /monitoring # enable snmp
firepower-2110 /monitoring* #
```

步骤 3 设置 SNMP 社区名称。

set snmp community

系统会提示您输入 SNMP 社区名称。社区名可以是任意字母数字字符串，最多 32 个字符。

示例：

```
firepower-2110 /monitoring* # set snmp community
Enter a snmp community: community1
firepower-2110 /monitoring* #
```

步骤 4 指定负责 SNMP 的系统联系人。

set snmp syscontact *system-contact-name*

系统联系人姓名可以是任意字母数字字符串，最多 255 个字符，例如电邮地址或姓名和电话号码。

示例：

```
firepower-2110 /monitoring* # set snmp syscontact jcrichton@example.com
firepower-2110 /monitoring* #
```

步骤 5 指定 SNMP 代理（服务器）运行所在的主机的位置。

set snmp syslocation *system-location-name*

系统位置名称可以是任意字母数字字符串，最多 512 个字符。

示例：

```
firepower-2110 /monitoring* # set snmp syslocation boulder, co
firepower-2110 /monitoring* #
```

步骤 6 创建 SNMPv3 用户。

a) 指定用户名和密码

enter snmp-user *user-name*

系统会提示您输入密码。

示例：

```
firepower-2110 /monitoring* # enter snmp-user jcrichton
Password: aerynsun
firepower-2110 /monitoring/snmp-user* #
```

b) 启用 AES-128 加密。

set aes-128 {**no** |**yes**}

默认情况下会禁用 AES-128 加密。

示例：

```
firepower-2110 /monitoring/snmp-user* # set aes-128 yes
firepower-2110 /monitoring/snmp-user* #
```

c) 指定用户隐私密码。

set priv-password

系统会提示您输入并确认隐私密码。

示例：

```
firepower-2110 /monitoring/snmp-user* # set priv-password
Enter a password: moyahome
Confirm the password: moyahome
firepower-2110 /monitoring/snmp-user* #
```

d) 退出 SNMP 用户模式。

exit

示例：

```
firepower-2110 /monitoring/snmp-user* # exit
firepower-2110 /monitoring* #
```

步骤 7 添加 SNMP 陷阱。

a) 创建 SNMP 陷阱。

enter snmp-trap {*hostname* | *ip-addr* | *ip6-addr*}

示例：

```
firepower-2110 /monitoring* # enter snmp-trap 10.10.10.67
firepower-2110 /monitoring/snmp-trap* #
```

b) 指定用于 SNMP 陷阱的 SNMP 社区名。

set community *community-name*

示例：

```
firepower-2110 /monitoring/snmp-trap* # set community community1
firepower-2110 /monitoring/snmp-trap* #
```

c) 指定用于 SNMP 陷阱的端口。

set port *port-num*

示例：

```
firepower-2110 /monitoring/snmp-trap* # set port 3434
firepower-2110 /monitoring/snmp-trap* #
```

d) 指定用于陷阱的 SNMP 版本和型号。

set version {**v1** | **v2c** | **v3**}

示例：

```
firepower-2110 /monitoring/snmp-trap* # set version v2c
firepower-2110 /monitoring/snmp-trap* #
```

e) （可选） 指定要发送的陷阱类型。

set notificationtype {**traps** |**informs**}

- **traps**- 如果为版本选择 v2c 或 v3，将类型设置为“陷阱”。
- **informs**— 如果为版本选择 v2c，将类型设置为“通告”。

示例：

```
firepower-2110 /monitoring/snmp-trap* # set notificationtype informs
firepower-2110 /monitoring/snmp-trap* #
```

f) （可选） 如果为版本选择 v3，请指定与陷阱相关的权限。

set v3privilege {**auth** | **noauth** | **priv**}

- **auth**— 启用身份验证，但不启用加密

- **noauth**— 不启用身份验证或加密
- **priv**— 启用身份验证和加密

示例：

```
firepower-2110 /monitoring/snmp-trap* # set v3privilege priv
firepower-2110 /monitoring/snmp-trap* #
```

g) 退出 SNMP 陷阱模式。

exit

示例：

```
firepower-2110 /monitoring/snmp-trap* # exit
firepower-2110 /monitoring* #
```

步骤 8 保存配置。

commit-buffer

示例：

```
firepower-2110 /monitoring* # commit-buffer
firepower-2110 /monitoring #
```

示例

以下示例启用 SNMP。

```
firepower-2110# scope monitoring
firepower-2110 /monitoring # enable snmp
firepower-2110 /monitoring* # set snmp community
Enter a snmp community: SnmpCommSystem2
firepower-2110 /monitoring* # set snmp syscontact contactperson1
firepower-2110 /monitoring* # set snmp syslocation systemlocation
firepower-2110 /monitoring* # enter snmp-user snmp-user14
Password: happy
firepower-2110 /monitoring/snmp-user* # set aes-128 yes
firepower-2110 /monitoring/snmp-user* # set priv-password
Enter a password: ecstatic
Confirm the password: ecstatic
firepower-2110 /monitoring/snmp-user* # exit
firepower-2110 /monitoring* #
firepower-2110 /monitoring* # enter snmp-trap 192.168.100.112
firepower-2110 /monitoring/snmp-trap* # set community SnmpCommSystem2
firepower-2110 /monitoring/snmp-trap* # set port 12009
firepower-2110 /monitoring/snmp-trap* # set version v3
firepower-2110 /monitoring/snmp-trap* # set notificationtype traps
firepower-2110 /monitoring/snmp-trap* # set v3privilege priv
firepower-2110 /monitoring/snmp-trap* # exit
firepower-2110 /monitoring* #
```

```
firepower-2110 /monitoring* # enter snmp-trap 2001::1
firepower-2110 /monitoring/snmp-trap* # set community SnmpCommSystem3
firepower-2110 /monitoring/snmp-trap* # set port 12009
firepower-2110 /monitoring/snmp-trap* # set version v3
firepower-2110 /monitoring/snmp-trap* # set notificationtype traps
firepower-2110 /monitoring/snmp-trap* # set v3privilege priv
firepower-2110 /monitoring/snmp-trap* # commit-buffer
firepower-2110 /monitoring/snmp-trap #
```

启用 FIPS 和通用标准模式

执行以下步骤可在 Firepower 2100 上启用 FIPS 或“通用标准 (CC) ”模式。

您还必须使用 **fips enable** 命令在 ASA 上单独启用 FIPS 模式。在 ASA 上没有用于通用标准模式的单独设置；对 CC 或 UCAPL 法规合规性的任何其他限制都必须按照思科安全策略文档进行配置。

我们建议您首先在 ASA 上设置 FIPS 模式，等待设备重新加载，然后在 FXOS 中设置 FIPS 模式。

过程

步骤 1 进入安全模式。

scope security

示例：

```
firepower-2110# scope security
firepower-2110 /security #
```

步骤 2 启用 FIPS 模式。

enable fips-mode

示例：

```
firepower-2110 /security # enable fips-mode
Warning: Connectivity to one or more services may be denied when committed. Please consult
 the product's FIPS Security Policy documentation.
WARNING: A reboot of the system is required in order for the system to be operating in a
FIPS approved mode.
firepower-2110 /security* #
```

步骤 3 启用通用标准模式。

enable cc-mode

示例：

```
firepower-2110 /security* # enable cc-mode
Warning: Connectivity to one or more services may be denied when committed. Please consult
 the product's CC Security Policy documentation.
WARNING: A reboot of the system is required in order for the system to be operating in a
```

```
CC approved mode.
```

步骤 4 保存配置。

commit-buffer

示例：

```
firepower-2110 /security* # commit-buffer
firepower-2110 /security #
```

步骤 5 重启系统。

scope chassis 1

reboot

示例：

```
firepower-2110 /security # scope chassis 1
firepower-2110 /chassis # reboot
```

用户管理

用户帐户用于访问 Firepower 2100 机箱。这些帐户用于 Firepower 机箱管理器和 SSH 访问。ASA 拥有单独的用户帐户和身份验证。

关于用户帐户

管理员帐户

管理员帐户是默认用户帐户，并且无法修改或删除。此帐户是系统管理员或超级用户帐户并具有完整权限。默认密码为 **Admin123**。

管理员帐户始终处于活动状态，并且不会到期。无法将管理员帐户配置为非活动状态。

本地身份验证的用户帐户

您最多可配置 48 个本地用户帐户。每个用户帐户必须具有唯一的用户名和密码。

本地身份验证用户帐户可以由具有管理员权限的任何用户来启用或禁用。

用户帐户的准则

用户名

用户名用作 Firepower 机箱管理器和 FXOS CLI 的登录 ID。分配登录 ID 时，请考虑以下指导原则和限制：

- 登录 ID 可以包含 1 到 32 个字符，包括以下字符：
  - 任何字母字符
  - 任何数字
  - _（下划线）
  - -（连字符）
  - .（圆点）
- 登录 ID 必须唯一。
- 登录 ID 必须以字母字符开头，而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。
- 无法创建全数字登录 ID。
- 创建用户帐户后，无法更改登录 ID。必须删除该用户帐户，创建新的用户帐户。

密码

密码对于每个本地认证的用户帐户都是必需的。具有管理员权限的用户可以配置系统，以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。

建议每个用户都使用强密码。如果对本地身份验证的用户启用密码强度检查，则 FXOS 将拒绝不符合以下要求的任何密码：

- 必须包含最少 8 个字符，最多 127 个字符。

注释 您可以选择在系统上配置 15 个字符（最小密码长度）的密码，以符合通用标准需求。

- 必须包含至少一个大写字母字符。
- 必须包含至少一个小写字母字符。
- 必须包含至少一个非字母数字（特殊）字符。
- 不能包含连续重复 3 次的字符，例如 aaabbb。
- 不得包含三个以任何顺序排列的连续数字或字母，例如 passwordABC 或 password321。
- 不能与用户名相同，或与用户名正好相反。
- 必须通过密码字典检查。例如，密码不可以是标准的词典单词。
- 不得包含以下符号：$（美元符号）、?（问号）和 =（等号）。
- 不得为空。

添加用户

为 Firepower 机箱管理器和 FXOS CLI 访问添加本地用户。

开始之前

您必须是拥有管理员权限的用户，才能添加本地用户帐户。

过程

步骤 1 进入安全模式：

scope security

示例：

```
firepower-2110# scope security
firepower-2110 /security #
```

步骤 2 创建用户帐户：

enter local-user *local-user-name*

- *local-user-name* - 设置登录此帐户时要使用的帐户名称。此名称必须唯一，并满足用户帐户名称的准则和限制（请参阅用户帐户的准则，第 81 页）。

创建用户后，不能更改登录 ID。必须删除该用户帐户，创建新的用户帐户。

示例：

```
firepower-2110 /security # enter local-user johncrichton
firepower-2110 /security/local-user* #
```

步骤 3 指定本地用户帐户是活动还是非活动状态：

set account-status {**active**| **inactive**}

默认情况下，用户处于活动状态。

示例：

```
firepower-2110 /security/local-user* # set account-status inactive
```

步骤 4 设置用户帐户的密码：

set password

输入密码：*password*

确认密码：*password*

如果启用了密码强度检查，则密码必须为强密码，FXOS会拒绝任何不满足强度检查要求的密码（请参阅 配置用户设置，第 85 页 和 用户帐户的准则，第 81 页）。

示例：

```
firepower-2110 /security/local-user* # set password
Enter a password: aeryn
Confirm the password: aeryn
firepower-2110 /security/local-user* #
```

步骤 5 （可选）指定用户的名字：

set firstname *first-name*

示例：

```
firepower-2110 /security/local-user* # set firstname John
```

步骤 6 （可选）指定用户的姓氏：

set lastname *last-name*

示例：

```
firepower-2110 /security/local-user* # set lastname Crichton
```

步骤 7 （可选）指定用户帐户到期日期：

set expiration *month* *day-of-month* *year*

- *month* — 将月份设置为月份名称的前三个字母。

在指定的日期过后，无法使用帐户。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。

默认情况下，用户帐户不会到期。

示例：

```
firepower-2110 /security/local-user* # set expiration oct 10 2019
```

步骤 8 （可选）指定用户邮件地址。

set email *email-addr*

示例：

```
firepower-2110 /security/local-user* # set email jcrichton@example.com
```

步骤 9 （可选）指定用户电话号码。

set phone *phone-num*

示例：

```
firepower-2110 /security/local-user* # set phone 303-555-7891
```

步骤 10 （可选）将管理员角色分配给用户。

enter role admin

所有用户均默认分配了 **read-only** 角色，并且此角色无法删除。**admin** 角色允许对配置进行读写访问。

用户角色和权限的更改在用户下一次登录之后才会生效。如果在向用户帐户分配新角色或从中删除现有角色时用户已登录，则活动会话将继续使用上一个角色和权限。

示例：

```
firepower-2110 /security/local-user* # enter role admin
```

步骤 11 保存配置。

commit-buffer

示例：

```
firepower-2110 security/local-user* # commit-buffer
firepower-2110 security/local-user #
```

示例

以下示例创建名为 aerynsun 的用户帐户，启用用户帐户，将密码设置为 rygel，分配管理员用户角色，并且提交任务：

```
firepower-2110# scope security
firepower-2110 /security # create local-user aerynsun
firepower-2110 /security/local-user* # set password
Enter a password: rygel
Confirm the password: rygel
firepower-2110 /security/local-user* # enter role admin
firepower-2110 /security/local-user* # commit-buffer
firepower-2110 /security/local-user #
```

配置用户设置

您可以为所有用户配置全局设置。

过程

步骤 1 进入安全模式：

scope security

示例：

```
firepower-2110# scope security
firepower-2110 /security #
```

步骤 2 启用或禁用密码强度检查。

set enforce-strong-password {yes |no}

如果启用密码强度检查，则 Firepower 2100 不允许用户选择不符合强密码准则的密码（请参阅 用户帐户的准则，第 81 页）。默认情况下，系统会启用强密码。

示例：

```
firepower-2110 /security # set enforce-strong-password yes
firepower-2110 /security* #
```

步骤 3 输入密码配置文件模式。

scope password-profile

示例：

```
firepower-2110 /security* # scope password-profile
firepower-2110 /security/password-profile* #
```

步骤 4 配置最小密码长度。

set min-password-length *min_length*

如果启用最小密码长度检查，则必须使用指定的最小数目的字符创建密码。

示例：

```
firepower-2110 /security/password-profile* # set min-password-length 8
```

步骤 5 启用或禁用本地身份验证用户在给定小时数内是否更改密码。

允许更改：

set change-interval *num-of-hours*

set change-count *pass-change-num*

- *num_of_hours* — 设置执行密码更改次数的小时数，该值介于 1 到 745 小时之间。
- *pass_change_num* — 设置本地身份验证用户能够在“更改间隔”内更改其密码的最大次数。

要禁止更改，请将 **set change-interval** 设置为 **disabled**。

示例：

```
firepower-2110 /security/password-profile* # set change-count 2
```

```
firepower-2110 /security/password-profile* # set change-interval 24
```

禁止更改：

set no-change-interval*min_num_hours*}

- *min_num_hours* — 设置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，该值介于 1 到 745 小时之间。

要允许更改，请将 **set no-change-interval** 设置为 **disabled**。

示例：

```
firepower-2110 /security/password-profile* # set no-change-interval 1
```

步骤 6 设置密码重复使用要求。

set history-count{ num_of_passwords | **disabled**}

set password-reuse-interval { 天数 | **disabled**}

- *num_of_passwords* — 指定本地身份验证用户必须创建的唯一密码数量，在此之前，用户可以重新使用以前用过的密码，该值介于 0 到 15 小时之间：默认情况下，最小值为 0，这表示禁用历史计数，使用户随时都能够重复使用之前已使用的密码。
- *days* — 设置可重复使用密码的天数，范围介于 1 到 365 之间。默认值为 15 天。

如果启用这两个命令，则必须满足两个要求。例如，如果您将历史计数设置为 3，并将重复使用间隔设置为 10 天，则您只能在更改 3 次密码的十天后更改密码。

示例：

```
firepower-2110 /security/password-profile* # set history-count 5
firepower-2110 /security/password-profile* # set password-reuse-interval 120
```

步骤 7 设置密码到期设置。

set password-expiration { 天数 | **never**}

set expiration-warning-period 天

set expiration-grace-period 天

- {days |**set password-expiration**} **never** — 将到期时间设置为 1 到9999 天。默认情况下，禁用过期 (**never**)。
- **set expiration-warning-period** *days* — 设置到期前的天数，以警告用户每次登录时的密码到期，范围介于 0 到 9999 之间。默认时间为 14 天。
- **set expiration-grace-period** *days* — 设置用户在到期后必须更改其密码的天数，范围介于 0 到 9999 之间。默认值为 3 天。

示例：

```
firepower-2110 /security/password-profile* # set password-expiration 120
firepower-2110 /security/password-profile* # set expiration-warning-period 5
firepower-2110 /security/password-profile* # set expiration-grace-period 5
```

步骤 8 设置绝对会话超时，适用于所有形式的访问（包括串行控制台、SSH 和 HTTPS）。

scope default-auth

set absolute-session-timeout 秒

- *seconds* — 设置介于 0 和 7200 之间的绝对超时值（以秒为单位）。默认值为 3600 秒（60 分钟）。要禁用此设置，请将会话超时值设置为 0。

示例：

```
firepower-2110 /security* scope default-auth#
firepower-2110 /security/default-auth* # set absolute-session-timeout 7200
```

步骤 9 保存配置。

commit-buffer

示例：

```
firepower-2110 /security/default-auth* # commit-buffer
firepower-2110 /security/default-auth #
```

示例

以下示例设置了许多用户要求：

```
firepower-2110 # scope security
firepower-2110 /security # set enforce-strong-password yes
firepower-2110 /security* # scope password-profile
firepower-2110 /security/password-profile* # set change-during-interval enable
firepower-2110 /security/password-profile* # set change-count 5
firepower-2110 /security/password-profile* # set change-interval 72
firepower-2110 /security/password-profile* # set history-count 5
firepower-2110 /security/password-profile* # commit-buffer
firepower-2110 /security/password-profile #
```

系统管理

您可以升级 ASA 软件包、重新加载或关闭机箱电源。

升级映像

此任务适用于独立 ASA。如果要升级故障切换对，请参阅思科 ASA 升级指南。升级过程通常需要 20 到 30 分钟。

ASA、ASDM 和 FXOS 映像被捆绑成一个单一的包。包更新由 FXOS 管理；不能在 ASA 操作系统中升级 ASA。不能单独升级 ASA 和 FXOS；它们始终捆绑在一起。

不过 ASDM 是个例外，此时您可以从 ASA 操作系统中升级，因此无需只使用捆绑的 ASDM 映像。手动上传的 ASDM 映像不会出现在 FXOS 映像列表中；您必须从 ASA 管理 ASDM 映像。

注释 在升级捆绑包时，捆绑包中的 ASDM 映像将替换以前的 ASDM 捆绑包映像，因为它们具有相同的名称 (**asdm.bin**)。但是，如果您手动选择了您上传的其他 ASDM 映像（例如，**asdm-782.bin**），那么即使捆绑包升级之后，您仍可继续使用该映像。为了确保您运行的是兼容版本的 ASDM，您应该在升级捆绑包之前先升级 ASDM，或者应该在升级 ASA 捆绑包之前，或将 ASA 重新配置为使用捆绑的 ASDM 映像 (**asdm.bin**)。

开始之前

请确保您要上传的映像在 FTP、SCP、SFTP、TFTP 服务器或 USB 驱动器上可用。

过程

步骤 1 通过控制台端口（首选）或使用 SSH 连接到 FXOS CLI。如果在控制台端口连接，则立即访问 FXOS CLI。输入 FXOS 登录凭证。默认用户名是 **admin**，默认密码是 **Admin123**。

如果使用 SSH 连接到 ASA 管理 IP 地址，请输入 **connect fxos** 以访问 FXOS。

步骤 2 将软件包下载到机箱。

a) 进入固件模式。

scope firmware

示例：

```
firepower-2110# scope firmware
firepower-2110 /firmware#
```

b) 下载软件包。

download image *url*

使用以下各项之一，为正在导入的文件指定 URL：

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*

- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*
- **usbA:**/*path*/*filename*

示例：

```
firepower-2110 /firmware # download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

c) 监控下载过程。

show download-task

示例：

```
firepower-2110 /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
firepower-2110 /firmware #
```

步骤 3 当新软件包完成下载（**已下载**状态）时，启动软件包。

a) 查看新软件包的版本号。

show package

示例：

```
firepower-2110 /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
firepower-2110 /firmware #
```

b) 安装软件包。

scope auto-install

install security-pack version *version*

在 **show package** 输出中，复制与 **security-pack version** 号对应的 **Package-Vers** 值。机箱会安装 ASA 安装包并重新启动。

示例：

```
firepower 2110 /firmware # scope auto-install
firepower-2110 /firmware/auto-install # install security-pack version 9.8.2.2

The system is currently installed with security software package 9.8.2, which has:
```

```
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.2.2, it will do the following:
   - upgrade to the CSP asa version 9.8.2.2

Do you want to proceed ? (yes/no): yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
   If you proceed the system will be re-imaged. All existing configuration will be lost,

   and the default configuration applied.
Do you want to proceed? (yes/no): yes

Triggered the install of software package version 9.8.2.2
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
firepower-2110 /firmware/auto-install #
```

注释 忽略此消息“所有现有配置均会丢失，且系统将应用默认配置”。系统不会清除配置，并且不会应用默认配置。默认配置仅在重新映像期间应用，而不是在升级过程中应用。

步骤 4 等待机箱完成重新启动（5-10 分钟）。FXOS 会首先启动，但您仍需等待 ASA 启动。

在 ASA 启动并连接到应用后，您可以在 CLI 中访问用户 EXEC 模式。

示例：

```
 [...]
Cisco FPR Series Security Appliance
firepower-2140 login: admin
Password:

Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2018, Cisco Systems, Inc. All rights reserved.
[...]

User enable_1 logged in to ciscoasa
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
[press Enter to see the prompt below:]

firepower-2140# connect asa
Attaching to ASA CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ciscoasa>
```

重新启动机箱

过程

步骤 1 进入机箱模式。

scope chassis 1

示例：

```
firepower-2110 # scope chassis 1
firepower-2110 /chassis #
```

步骤 2 重新启动机箱。

reboot["原因"] [**no-prompt**]

如果您使用 **no-prompt** 关键字，则输入命令后机箱将立即重新启动。否则，在您输入 **commit-buffer** 命令之前，机箱不会重新启动。

示例：

```
firepower-2110 /chassis # reboot "This system is rebooting" no-prompt
```

步骤 3 监控重新启动过程。

show fsm status

关闭机箱电源

在关闭 Firepower 2100 机箱电源之前，机箱会正常关闭 ASA 操作系统。此过程大约需要 15-20 分钟。在机箱成功关闭电源后，您可以拔掉机箱的电源插头。

过程

步骤 1 进入机箱模式。

scope chassis 1

示例：

```
firepower-2110 # scope chassis 1
firepower-2110 /chassis #
```

步骤 2 关闭机箱电源。

shutdown["原因"] [**no-prompt**]

如果您使用 **no-prompt** 关键字，则输入命令后机箱将立即关闭。否则，在您输入 **commit-buffer** 命令之前，机箱不会关闭。

示例：

```
firepower-2110 /chassis # shutdown "This system is powering off" no-prompt
```

步骤 3 监控关闭过程。

show fsm status

更改 FXOS 管理 IP 地址或网关

您可以从 FXOS CLI 更改 Firepower 2100 机箱上的 FXOS 管理 IP 地址。默认地址为 192.168.45.45。您还可以更改默认网关。默认网关设置为 0.0.0.0，它将流量发送到背板上的 ASA。如果要改为在管理 1/1 网络中使用路由器，则可以更改网关 IP 地址。此外，您还必须更改管理连接的访问列表以匹配新网络。

通常，FXOS 管理 1/1 IP 地址将与 ASA 管理 1/1 IP 地址在同一网络上；因此该过程也显示如何更改 ASA 上的 ASA IP 地址。

开始之前

- 更改管理 IP 地址后，需要使用新地址重新建立所有 Firepower 机箱管理器和 SSH 连接。
- 由于默认情况下在管理 1/1 上启用了 DHCP 服务器，因此在更改管理 IP 地址之前必须禁用 DHCP。

过程

步骤 1 连接到控制台端口（请参阅 连接到 ASA 或 FXOS 控制台，第 28 页）。我们建议您连接到控制台端口，以避免连接断开。

步骤 2 禁用 DHCP 服务器。

scope system

scope services

disable dhcp-server

commit-buffer

更改管理 IP 地址后，可以使用新客户端 IP 地址重新启用 DHCP。您还可以通过**平台设置 (Platform Settings)** > **DHCP** 在 Firepower 机箱管理器中启用或禁用 DHCP 服务器。

示例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
```

```
firepower-2110 /system/services # disable dhcp-server
firepower-2110 /system/services* # commit-buffer
```

步骤 3 配置 IPv4 管理 IP 地址，还可以配置网关（可选）。

a) 设置交换矩阵互联 a 的范围。

scope fabric-interconnect a

示例：

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect #
```

b) 查看当前的管理 IP 地址。

show

示例：

```
firepower-2110 /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    192.168.45.45    0.0.0.0         0.0.0.0          ::               ::
     64     Operable
```

c) 配置新管理 IP 地址，还可以配置新的默认网关（可选）。

set out-of-band static ip *ip_address* **netmask** *network_mask* **gw** *gateway_ip_address*

要保留当前设置的网关，请省略关键字 **gw**。同样，要在更改网关时保留现有的管理 IP 地址，请省略关键字 **ip** and **netmask**。

要将网关设置为 ASA 数据接口，请将 **gw** 设置为0.0.0.0。这是默认设置。

示例：

```
firepower-2110 /fabric-interconnect # set out-of-band static ip 192.168.4.1 netmask
255.255.255.0
Warning: When committed, this change may disconnect the current CLI session
firepower-2110 /fabric-interconnect* #
```

步骤 4 配置 IPv6 管理 IP 地址和网关。

a) 设置交换矩阵互联 a 的范围，然后设置 IPv6 配置的范围。

scope fabric-interconnect a

scope ipv6-config

示例：

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # scope ipv6-config
```

```
firepower-2110 /fabric-interconnect/ipv6-config #
```

b) 查看当前的管理 IPv6 地址。

show ipv6-if

示例：

```
firepower-2110 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                       Prefix     IPv6 Gateway
    ---------------------------------- ---------- ------------
    ::                                 ::         ::
```

c) 配置新的管理 IPv6 地址和网关：

Firepower-chassis /fabric-interconnect/ipv6-config # **set out-of-band static ipv6** *ipv6_address* **ipv6-prefix** *prefix_length* **ipv6-gw** *gateway_address*

要保留当前设置的网关，请省略关键字 **ipv6-gw**。同样，要在更改网关时保留现有的管理 IP 地址，请省略关键字 **ipv6** and **ipv6-prefix**。

要将网关设置为 ASA 数据接口，请将 **gw** 设置为：：。这是默认设置。

示例：

```
firepower-2110 /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001:DB8::34
 ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config* #
```

步骤 5 删除 HTTPS、SSH 和 SNMP 的访问列表并添加新列表，以允许来自新网络的管理连接。

a) 为系统/服务设置范围。

scope system

scope services

示例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
```

b) 查看当前访问列表。

show ip-block

示例：

```
firepower-2110 /system/services # show ip-block

Permitted IP Block:
    IP Address      Prefix Length Protocol
    --------------- ------------- --------
    192.168.45.0               24 https
    192.168.45.0               24 ssh
```

```
firepower-2140 /system/services #
```

c) 添加新的访问列表。

IPv4：

enter ip-block *ip_address prefix*[**http** | **snmp** | **ssh**]

IPv6：

enter ipv6-block *ipv6_address prefix*[**https** | **snmp** | **ssh**]

对于 IPv4，请输入 **0.0.0.0** 和前缀 **0** 以允许所有网络。对于 IPv6，请输入 **::** 和前缀 **0** 以允许所有网络。还可以通过**平台设置 (Platform Settings)** > **访问列表 (Access List)** 在 Firepower 机箱管理器中添加访问列表。

示例：

```
firepower-2110 /system/services # enter ip-block 192.168.4.0 24 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.4.0 24 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.4.0 24 snmp
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 snmp
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* #
```

a) 删除旧的访问列表。

IPv4：

delete ip-block *ip_address prefix*[**http** | **snmp** | **ssh**]

IPv6：

delete ipv6-block *ipv6_address prefix*[**https** | **snmp** | **ssh**]

示例：

```
firepower-2110 /system/services # delete ip-block 192.168.45.0 24 https
firepower-2110 /system/services* # delete ip-block 192.168.45.0 24 ssh
firepower-2110 /system/services* #
```

步骤 6 （可选） 重新启用 IPv4 DHCP 服务器。

scope system

scope services

enable dhcp-server *start_ip_address end_ip_address*

您还可以通过**平台设置 (Platform Settings)** > **DHCP** 在 Firepower 机箱管理器中启用或禁用 DHCP 服务器。

示例：

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enable dhcp-server 192.168.4.10 192.168.4.20
```

步骤 7 保存配置。

commit-buffer

示例：

```
firepower-2110 /system/services* # commit-buffer
```

步骤 8 将 ASA 地址更改为在正确的网络上。默认 ASA 管理接口 1/1 IP 地址为 192.168.45.1。

a) 从控制台连接到 ASA CLI 并访问全局配置模式。

connect asa

enable

configure terminal

示例：

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa# configure terminal
ciscoasa(config)#
```

b) 更改管理 1/1 IP 地址。

interface management1/1

ip address *ip_address mask*

示例：

```
ciscoasa(config)# interface management1/1
ciscoasa(config-ifc)# ip address 10.86.118.4 255.255.255.0
```

c) 更改可访问 ASDM 的网络。

no http 192.168.45.0 255.255.255.0 management

http *ip_address mask* **management**

示例：

```
ciscoasa(config)# no http 192.168.45.0 255.255.255.0 management
```

```
ciscoasa(config)# http 10.86.118.0 255.255.255.0 management
```

d) 保存配置。

write memory

e) 要返回到 FXOS 控制台，请输入 **Ctrl+a**，**d**。

示例

以下示例配置 IPv4 管理接口和网关：

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ ------------
    A    192.168.2.112    192.168.2.1     255.255.255.0   2001:DB8::2     2001:DB8::1
  64     Operable
firepower-2110 /fabric-interconnect # set out-of-band static ip 192.168.2.111 netmask
255.255.255.0 gw 192.168.2.1
Warning: When committed, this change may disconnect the current CLI session
firepower-2110 /fabric-interconnect* # commit-buffer
firepower-2110 /fabric-interconnect #
```

以下示例配置 IPv6 管理接口和网关：

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # scope ipv6-config
firepower-2110 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                       Prefix     IPv6 Gateway
    ---------------------------------- ---------- ------------
    2001:DB8::2                         64         2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001:DB8::2
ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config* # commit-buffer
firepower-2110 /fabric-interconnect/ipv6-config #
```

FXOS CLI 设置的历史记录

功能	版本	详细信息
可配置的 HTTPS 协议	9.13(1)	您可以为 HTTPS 访问设置 SSL/TLS 版本。 新增/修改的命令：**set https access-protocols**
针对 IPSec 和 Keyrings 的 FQDN 实施	9.13(1)	您可以配置 FQDN 实施，使对等体的 FDQN 需要与对等体所提供的 X.509 证书中的 DNS 名称匹配。对于 IPSec，默认情况下会启用实施，但在 9.13(1) 之前创建的连接除外；您必须手动启用这些旧连接的实施。对于 keyrings，所有主机名都必须是 Fqdn，并且不能使用通配符。 新增/修改的命令：**set dns**、**set e-mail**、**set fqdn-enforce**、**set ip**、**set ipv6**、**set remote-address**、**set remote-ike-id** 删除的命令：**fi-a-ip**、**fi-a-ipv6**、**fi-b-ip**、**fi-b-ipv6**
新 IPSec 密码和算法	9.13(1)	添加了以下 IKE 和 ESP 密码和算法（不可配置）： • 密码 - aes192。现有密码包括：aes128、aes256、aes128gcm16。 • 伪随机函数 (PRF)（仅限 IKE）— prfsha384、prfsha512、prfsha256。现有 PRF 包括：prfsha1。 • 完整性算法-sha256、sha384、sha512、sha1_160。现有算法包括：sha1。 • Diffie-hellman 组-curve25519、ecp256、ecp384、ecp521、modp3072、modp4096。现有组包括：modp2048。

功能	版本	详细信息
SSH 身份验证增强功能	9.13(1)	添加了以下 SSH 服务器加密 algoritghms： • aes128-gcm@openssh.com • aes256-gcm@openssh.com • chacha20-poly@openssh.com 添加了以下SSH服务器密钥交换方法： • diffie-hellman-group14-sha256 • curve25519-sha256 • curve25519-sha256@libssh.org • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 新增/修改的命令：**set ssh-server encrypt-algorithm**、**set ssh-server kex-algorithm**。
用于 X.509 证书的 EDCS 密钥	9.13(1)	现在，您可以将 EDCS 密钥用于证书。以前，仅支持 RSA 密钥。 新增/修改的命令：**set elliptic-curve**、**set keypair-type**。

功能	版本	详细信息
用户密码改进	9.13(1)	添加了密码安全改进，包括以下内容： • 用户密码最多可达 127 个字符。旧限制为 80 个字符。 • 默认情况下，系统会启用强密码。 • 提示设置管理员密码。 • 密码到期。 • 限制密码重复使用。 • 删除了 **set change-during-interval** 命令，并为 **set change-interval**、**set no-change-interval** 和 **set history-count** 命令添加了 **disabled** 选项。 新增/修改的命令：**set change-during-interval**、**set expiration-grace-period**、 **set expiration-warning-period**、**set history-count**、**set no-change-interval**、**set password**、**set password-expiration**、**set password-reuse-interval**
set lacp-mode 命令已更改为 **set port-channel-mode**	9.10(1)	为了与 Firepower 4100/9300 中的命令用法保持一致，**set lacp-mode** 命令已更改为 **set port-channel-mode**。 新增/修改的命令：**set port-channel-mode**
在 Firepower 2100 上支持 NTP 身份验证	9.10(1)	现在，您可以在 FXOS 中配置 SHA1 NTP 服务器身份验证。 新增/修改的 FXOS 命令：**enable ntp-authentication**、**set ntp-sha1-key-id**、**set ntp-sha1-key-string**