Cisco Secure Firewall Management Center 1700、2700 和 4700 入门指南

上次修改日期: 2026 年 2 月 24 日

关于 Cisco Secure Firewall Management Center 1700、2700 和 4700

该Firewall Management Center提供威胁防御设备的集中化、集成化和简化管理。它还提供应用控制、入侵防御系统 (IPS)、URL 过滤和恶意软件防护功能。在大型网络的典型部署中，需在网段上安装多台受管威胁防御设备。每台设备都会控制、检查、监控和分析流量，然后向Firewall Management Center报告。

Cisco Secure Firewall Management Center 1700、2700 和 4700 设备可提供卓越的性能和效率。

本文档介绍如何完成Firewall Management Center的布线和初始配置。

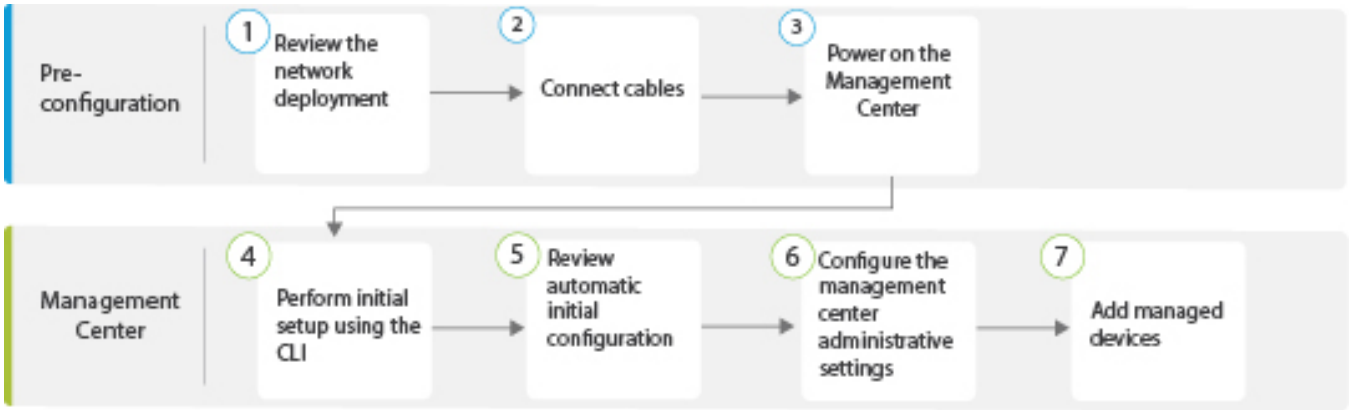
准备工作

安装管理中心。有关详细信息，请参阅《*Cisco Secure Firewall Management Center 1700、2700 和 4700 硬件安装指南*》。

有关 Cisco Secure Firewall 系列文档的完整列表及获取位置，请参阅文档路线图。

端到端程序

以下流程图说明了部署和配置管理中心的任务。



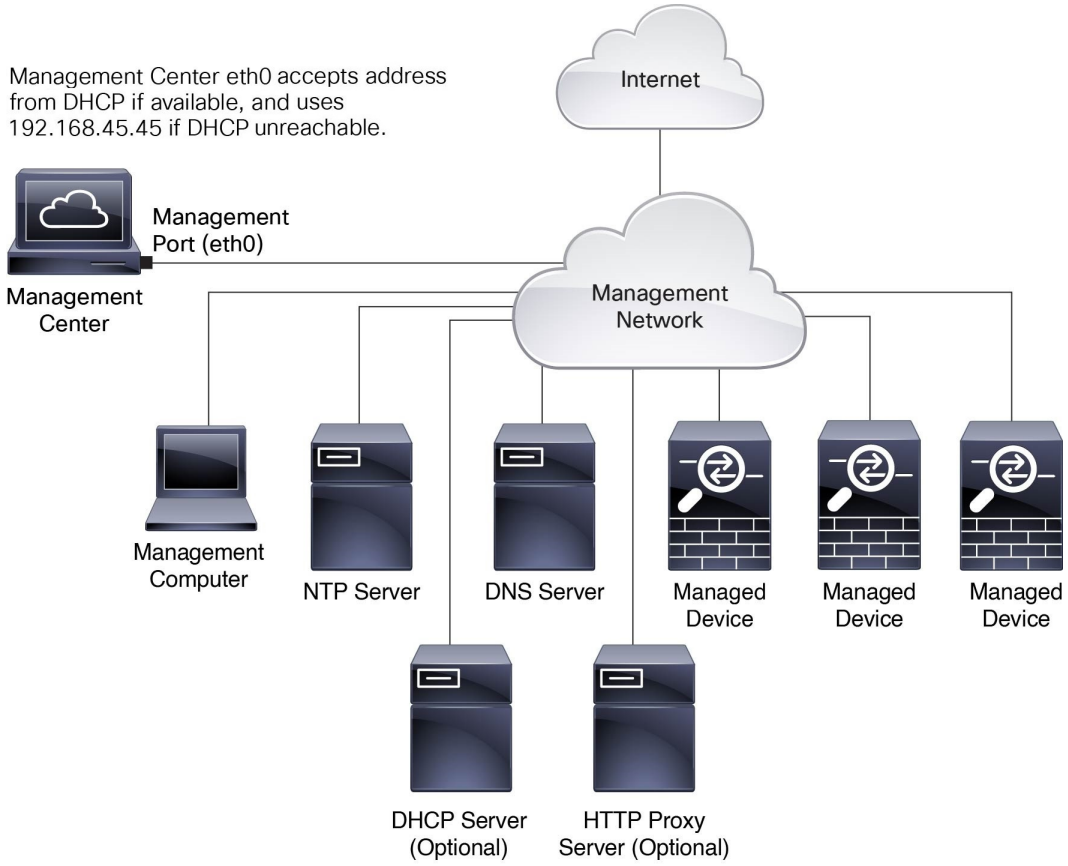
1	配置前准备工作	查看网络部署，第 2 页

2	配置前准备工作	连接到管理中心，第 4 页
3	配置前准备工作	开启管理中心电源，第 5 页
4	Firewall Management Center	使用 CLI 执行Firewall Management Center的初始设置，第 7 页
5	Firewall Management Center	查看自动初始配置，第 13 页
6	Firewall Management Center	配置 Firewall Management Center 管理设置，第 14 页
7	Firewall Management Center	将受管设备添加到 Firewall Management Center，第 15 页

查看网络部署

在部署Firewall Management Center之前，您需要了解其运行环境的相关信息。

下图显示了管理中心的典型网络部署。



默认情况下，Firewall Management Center通过其管理接口 (eth0) 连接到本地管理网络。通过此连接，Firewall Management Center会与管理计算机、受管设备、DHCP、DNS、NTP 等服务以及互联网进行通信。

Firewall Management Center需要访问互联网以支持智能许可、Cisco Secure Firewall 威胁智能导向器和恶意软件防御服务。根据您本地管理网络提供的服务，Firewall Management Center可能还需要访问互联网才能连接到 NTP 或 DNS 服务器。您可以将网络配置为直接或通过防火墙设备为Firewall Management Center提供互联网访问权限。

您可以从具备互联网连接的设备，或从已从互联网获取这些更新的本地计算机，直接将系统软件、漏洞数据库 (VDB)、地理位置数据库 (GeoDB) 和入侵规则的更新上传到Firewall Management Center。

要在Firewall Management Center与其某台受管设备之间建立连接，您至少需要其中一台设备的 IP 地址：Firewall Management Center或受管设备。如果可用，我们建议同时使用两个 IP 地址。但是，您可能只知道其中一个 IP 地址。例如，受管设备可能在 NAT 之后使用私有地址，因此您只知道Firewall Management Center的地址。在这种情况下，您可以指定受管设备上的Firewall Management Center地址，以及您选择的称为 NAT ID 的一次性唯一密码。在Firewall Management Center上，指定相同的 NAT ID 以标识受管设备。

本文档所述的初始设置和配置适用于具备互联网访问权限的Firewall Management Center。如果您在气隙环境中部署Firewall Management Center，请参阅对应您所用版本的*Cisco Secure Firewall Management Center 管理指南*，了解可用于支持某些功能的替代方法，例如为 HTTP 通信配置代理，或使用智能软件卫星服务器进行智能许可。

Firewall Management Center的初始网络配置

- 管理接口

  默认情况下，Firewall Management Center会查找本地 DHCP 服务器，以获取用于管理接口 (eth0) 的 IP 地址、网络掩码和默认网关。如果Firewall Management Center无法访问 DHCP 服务器，它将使用默认 IPv4 地址 192.168.45.45、网络掩码 255.255.255.0 和网关 192.168.45.1。在初始设置期间，您可以接受这些默认值或指定不同的值。

  注释 如果使用 DHCP，则必须使用 DHCP 预留，因此分配的地址不会更改。如果 DHCP 地址更改，设备注册将失败，因为 Firewall Management Center 网络配置不同步。要从 DHCP 地址更改中恢复，请连接到 Firewall Management Center（使用主机名或新 IP 地址）并导航到 **系统** (⚙) > **配置**，然后点击**管理接口**重置网络。

  如果您对管理接口使用 IPv6 寻址，则完成初始设置后，必须使用 Web 界面配置地址。

- DNS 服务器

  为最多两个 DNS 服务器指定 IP 地址。如果使用评估许可证，您可以选择不使用 DNS。

  注释 在初始配置期间，您还可以提供主机名和域，以促进Firewall Management Center与其他主机通过 DNS 通信；完成初始设置后，您可以配置更多域。

- NTP 服务器

  在初始配置期间，同步Firewall Management Center及其受管设备的系统时间。您可以接受默认值（0.sourcefire.pool.ntp.org 和 1.sourcefire.pool.ntp.org 分别作为主用和备用 NTP 服务器），也可以提供可从您的网络访问的一个或两个受信任 NTP 服务器的 FQDN 或 IP 地址。如果不使用 DNS，则无法使用 FQDN 指定 NTP 服务器。

连接到管理中心

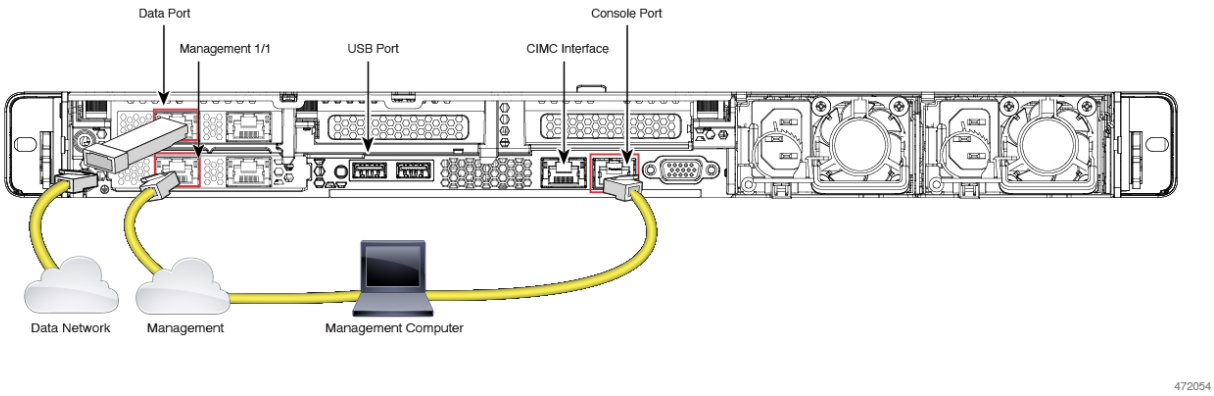
您可以使用下面列出的三种连接方式中的一种或多种连接管理中心：

- 将键盘连接到管理中心的 USB 端口，将显示器连接到其 VGA 端口。默认情况下，管理中心会将控制台消息发送到 VGA 端口。
- 将管理中心的 **CIMC** 端口连接到可从本地计算机访问的本地网络，您可在该计算机上运行用于无人值守管理的 IPMI 实用程序。要使用此连接，请参阅设置无人值守管理，第 16 页。
- 按照以下步骤所述，将本地计算机连接到管理中心的串行端口。

交流电源具有内部接地，因此使用支持的交流电源线时不需要额外的机箱接地。有关受支持电源线的详细信息，请参阅《*Cisco Secure Firewall Management Center 1700、2700 和 4700 硬件安装指南*》

完成机箱的机架安装后，请按照下列步骤连接电缆。

图 *1:* 使用电缆将设备连接到管理网络



开始之前

重要事项 在安装管理中心机箱之前，请仔细阅读法规与合规安全信息文档。

按照《*Cisco Secure Firewall Management Center 1700、2700 和 4700 硬件安装指南*》中所述，以机架方式安装该设备。

如果您计划使用控制台端口和本地计算机为设备布线，请将控制台输出重定向到控制台端口。有关详细信息，请参阅使用 Web 界面重定向控制台输出，第 10 页和使用 CLI 重定向控制台输出，第 11 页。

过程

步骤 1 使用电缆将以下内容连接到您的管理网络：

- 管理 1/1 接口
- 管理计算机

步骤 2 使用 RJ-45 转 DB-9 控制台电缆将管理计算机连接到控制台端口。您需要使用控制台端口访问 CLI 以进行初始设置。

步骤 3 在本地计算机上使用终端仿真软件（例如 HyperTerminal 或 XModem）与管理中心进行交互。终端仿真程序设置如下：9600 波特、8 个数据位、无奇偶校验、1 个停止位和无流量控制。

步骤 4 （可选） 在 1700、2700 和 4700 管理中心的 10 千兆以太网 SFP+ 接口（数据端口）或 4700 管理中心的 25 千兆以太网 SFP+ 接口中，安装任何支持的 SFP+ 收发器和电缆。可根据您的网络需求，将此接口与其他管理接口连接到同一网络或不同网络。

注释
我们建议您仅使用受支持的 SFP+ 收发器。有关 1700、2700 和 4700 管理中心支持的 SFP 相关详细信息，请参阅《*Cisco Secure Firewall Management Center 1700、2700 和 4700 硬件安装指南*》。

下一步做什么

1. 开启管理中心电源，第 5 页
2. 使用 CLI 执行Firewall Management Center的初始设置，第 7 页

开启管理中心电源

管理中心 1700、2700 和 4700 设备使用 1050-W 交流电源。有关电源供应器和受支持电源线的详细信息，请参阅《*Cisco Secure Firewall Management Center 1700、2700 和 4700 硬件安装指南*》。

开始之前

为设备提供可靠的电源（例如，使用不间断电源 (UPS)）非常重要。未事先关闭机箱就断电，可能会导致严重的文件系统损坏。

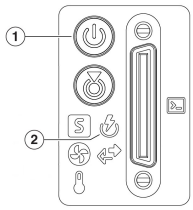
过程

步骤 1 使用受支持的电源线之一，将机箱的电源连接到您的电源插座。

注释
我们建议连接管理中心的两个电源供应器。如果仅连接一个电源，设备会生成运行状况警报。

步骤 2 按下机箱正面的电源按钮（标注为“**1**”），并确认电源状态 LED（标注为“**2**”）已亮起。

图 *2:* 电源按钮和电源状态 *LED*



在 FMC 上访问 CLI 或 Linux Shell Firewall Management Center

注意 强烈建议您不要使用 Linux Shell，除非 Cisco TAC 或用户文档明确说明需要这样做。

开始之前

使用串行端口、键盘和监视器与 Firewall Management Center 直接建立物理连接，并通过 Firewall Management Center 界面监控或建立 SSH 会话。

过程

步骤 1 使用 CLI **admin** 用户的凭证登录Firewall Management Center。

此操作允许您访问Firewall Management Center CLI。

步骤 2 请使用 **show version** 命令验证Firewall Management Center的软件版本。

示例：

```
> show version
-----------[ firepower ]------------
Model                  : Cisco Firewall Management Center 4700 (66) Version 7.4.0 (Build
```

```
1482)
UUID                    : a10ed34e-d127-11e8-b440-728439d95305
Rules update version    : 2023-11-15-001-vrt
LSP version             : lsp-rel-20231115-1600
VDB version             : 375
----------------------------------------------------
```

步骤 3 要从 Firewall Management Center CLI 访问 Linux Shell，请输入 **expert** 命令。

关闭或重新启动防火墙管理中心

使用 Web 界面启动有序关闭或重启。

您也可以从 防火墙管理中心 CLI 使用 **system shutdown** 命令关闭防火墙管理中心。

提示 对于虚拟设备，请参阅您所用虚拟平台的文档。特别是对于 VMware，自定义电源选项是 VMware 工具的一部分。

注意 请勿使用电源按钮关闭防火墙管理中心；此操作可能导致数据丢失。通过 Web 界面或 **shutdown** 命令让系统做好准备，在不丢失配置数据的情况下安全断电和重新启动。

过程

步骤 1 登录到管理中心，选择**系统** (⚙) > **配置** > **流程**。

步骤 2 选择以下其中一个选项：

- **关闭管理中心**以启动防火墙管理中心服务器的正常关闭。
- **重启管理中心**以正常关闭并重新启动防火墙管理中心。
- **重启管理中心控制台**以重启通信、数据库和 HTTP 服务器进程。此操作通常在故障排除期间使用，可能会导致已删除的主机重新显示在网络映射中。

使用 CLI 执行Firewall Management Center的初始设置

您也可以使用 CLI 执行初始设置。您必须完成初始配置向导来配置新设备，以便在受信任的管理网络上进行通信。

开始之前

- 按照相关文档中的说明为Firewall Management Center布线连接到管理中心，第 4 页。
- 请确保您拥有Firewall Management Center在管理网络上通信所需的以下信息：
  - IPv4 管理 IP 地址。
  - 网络掩码和默认网关（如果不使用 DHCP）
- 使用以下三种方法之一连接到 Firewall Management Center：
  - 将 USB 键盘和 VGA 显示器连接到 Firewall Management Center 进行控制台访问。
  - 使用 RJ-45 转 DP-9 控制台电缆将本地计算机连接到 Firewall Management Center 串行端口。
  - 使用上述任一方法配置 IP 后，通过 SSH 访问设备，使用 IPv4 管理 IP 地址连接到Firewall Management Center。

过程

步骤 1 在设备控制台使用**管理员**帐户（用户名：**admin**，密码：**Admin123**）登录到Firewall Management Center。密码区分大小写。

步骤 2 在出现提示时，按 **Enter** 以显示最终用户许可协议 (EULA)。

步骤 3 审查 the EULA。在出现提示时，输入 **`yes`**、**`YES`**，或按 **Enter** 接受 EULA。

重要事项
不接受 EULA 您无法继续。如果您回复 **`yes`**、 **`YES`** 或 **Enter** 以外的内容，系统会将您注销。

步骤 4 为了确保系统安全和隐私，您第一次登录 Firewall Management Center 时，必须更改 **admin** 密码。当系统提示设置新密码时，输入符合限制要求的新密码，并在系统提示确认时再次输入该密码。

注释
Firewall Management Center 会将您的密码与密码破解词典进行比较，该词典不仅会检查许多英语词典单词，还会检查其他容易被常用密码破解技术破解的字符串。例如，初始配置脚本可能会拒绝“abcdefg”或“passw0rd”等密码。

注释
完成初始配置后，系统会将两个 **admin** 帐户（一个用于 Web 访问，另一个用于 CLI 访问）的密码设置为相同值，且符合*Cisco Secure Firewall Management Center 管理指南*中所述的强密码要求。如果此后更改任一 **admin** 帐户的密码，两者将不再相同。您可以从 Web 界面 **admin** 帐户中取消强密码要求。

步骤 5 配置网络设置。

当您按照提示操作时，选项会显示在括号中，例如 **`(y/n)`**。默认值会列在方括号内，例如 **`[y]`**。回复提示时注意以下要点：

- 如果您在将设备恢复为出厂默认设置后（请参阅相关章节）进行设置，且未删除设备的许可证和网络设置，则提示会预填充保留的值。
- 按 **Enter** 接受默认值。
- 对于主机名，请输入完全限定域名 (`<hostname>.<domain>`) 或主机名。此栏必填。
- 如果使用 DHCP，则必须使用 DHCP 预留，因此分配的地址不会更改。如果 DHCP 地址更改，设备注册将失败，因为 Firewall Management Center 网络配置不同步。要从 DHCP 地址更改中恢复，请连接到 Firewall Management Center（使用主机名或新 IP 地址）并导航到 **系统** (⚙) > **配置**，然后点击**管理接口**重置网络。
- 如果您选择手动配置 IPv4，系统会提示您输入 IPv4 地址、网络掩码和默认网关。
- 可以配置 DNS 服务器；要指定无 DNS 服务器，输入 **none**。否则，指定一个或两个DNS 服务器的 IPv4 地址。如果指定两个地址，请用逗号将它们分隔开来。如果指定超过两台 DNS 服务器，系统将忽略多余的条目。如果Firewall Management Center无法访问互联网，您将无法使用本地网络之外的 DNS。

  注释
  如果您使用评估许可证，DNS 配置为可选，但部署永久许可证时必须配置 DNS。

- 您必须输入至少一个通过您网络可到达的完全限定域名 or IP 地址。如果未使用 DHCP，则不能指定 NTP 服务器的 FQDN。您可以指定两个服务器（一个主服务器，一个辅助服务器）；用逗号将它们的信息分隔开。如果指定超过两台 DNS 服务器，系统将忽略多余的条目。如果Firewall Management Center不能访问互联网，您将无法使用本地网络之外的 NTP 服务器。

示例：

```
Enter a hostname or fully qualified domain name for this system [firepower]: fmc
Configure IPv4 via DHCP or manually? (dhcp/manual) [DHCP]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.0.66
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.224
Enter the IPv4 default gateway for the management interface [ ]: 10.10.0.65
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
208.67.222.222,208.67.220.220
Enter a comma-separated list of NTP servers [0.sourcefire.pool.ntp.org,
1.sourcefire.pool.ntp.org]:
```

步骤 6 检查配置设置。系统会显示配置选项的摘要。

示例：

```
Hostname:                           fmc
IPv4 configured via:                manual configuration
Management interface IPv4 address:  10.10.0.66
Management interface IPv4 netmask:  255.255.255.224
Management interface IPv4 gateway:  10.10.0.65
DNS servers:                        208.67.222.222,208.67.220.220
NTP servers:                        0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org
```

步骤 7 确认设置。

- 如果设置正确，输入 **y**，然后按 **Enter**键接受设置并继续。

- 如果设置不正确，输入 **n**，然后按 **Enter**键。系统会再次提示输入设置信息，从主机名开始。

示例：

```
Are these settings correct? (y/n) y
If your networking information has changed, you will need to reconnect.

Updated network configuration.
```

步骤 8 接受设置后，您可以输入 **exit** 退出Firewall Management Center CLI。

下一步做什么

- 您可以使用刚才配置的网络信息连接到Firewall Management Center Web 界面。
- 查看初始配置过程中Firewall Management Center自动配置的每周维护活动。这些活动旨在使系统保持最新状态并备份您的数据。有关详细信息，请参阅查看自动初始配置，第 13 页。
- 如需配置Firewall Management Center IPv6 地址，可在完成初始设置后，通过 Web 界面进行配置（具体操作请参阅您所用版本的相关文档）。有关详细信息，请参阅*Cisco Secure Firewall Management Center 设备配置指南*。
- （可选）请按照设置无人值守管理，第 16 页中的说明，配置Firewall Management Center以支持 SOL 或 LOM 访问。

使用 Web 界面重定向控制台输出

您必须是管理员用户才能执行此程序。

开始之前

- 完成设备的初始设置流程。
- 禁用与设备管理接口连接的所有第三方交换设备上的生成树协议 (STP)。

过程

步骤 1 选择 **系统** (⚙) > **配置**。

步骤 2 选择**控制台配置**。

步骤 3 选择远程控制台访问选项：

- （默认）选择 **VGA** 以使用设备的 VGA 端口。
- 选择**物理串行端口**以使用设备的串行端口。

步骤 4 点击**保存 (Save)**。

步骤 5 要使更改生效，请输入 sudo reboot 命令重新启动设备。

使用 CLI 重定向控制台输出

开始之前

完成Firewall Management Center的初始设置流程。

过程

步骤 1 使用Firewall Management Center CLI **admin** 凭证访问 Firewall Management Center上的 Linux 外壳。有关详细信息，请参阅在 FMC 上访问 CLI 或 Linux Shell Firewall Management Center，第 6 页。

步骤 2 在提示符后输入以下命令之一以设置控制台输出：

- 要将控制台消息定向到 VGA 端口，请入以下命令：**`sudo /usr/local/sf/bin/configure_console.sh vga`**
- 要将控制台消息定向到物理串行端口，请输入以下命令：**`sudo /usr/local/sf/bin/configure_console.sh serial`**

步骤 3 要使更改生效，请输入 **sudo** `reboot` 命令重新启动设备。

重置 CLI 管理员密码

您可以更改用于访问 Firewall Management Center CLI 的管理员账户密码。

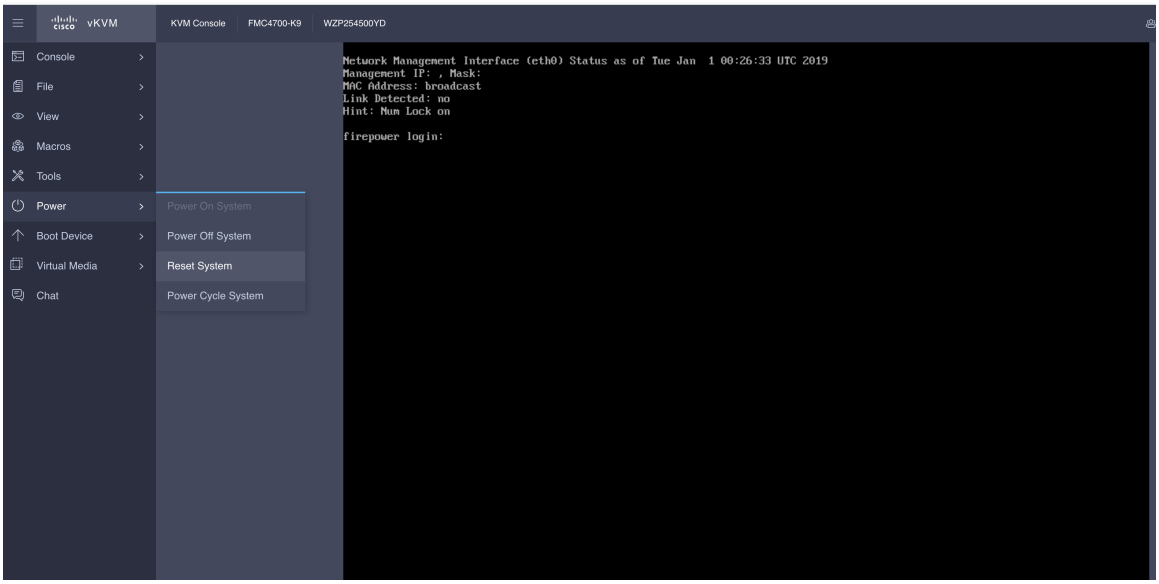
开始之前

要重置管理员密码，必须与设备建立控制台连接。

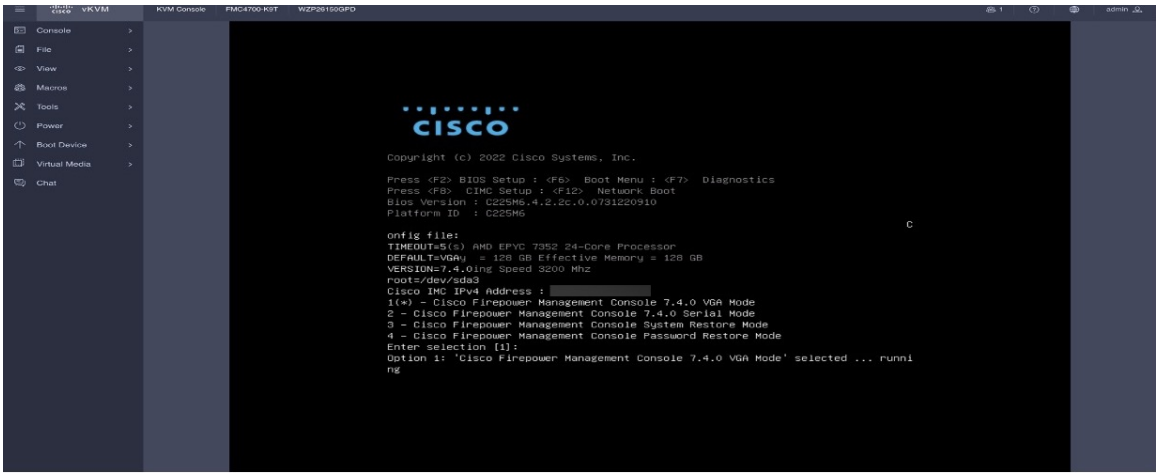
过程

步骤 1 以管理员用户身份登录 Firewall Management Center CLI。

步骤 2 在控制台中，依次选择**电源** > **重置系统**。



控制台中会显示以下消息：



步骤 3 输入选项 4 以重置密码。

步骤 4 在 # 提示符下，输入 **passwd admin** 命令。

步骤 5 输入新的管理员密码。

注释
我们建议您使用复杂密码。

步骤 6 输入 **reboot** 命令。等待重启过程完成。

重置 Web 界面管理员密码

您可以更改管理员账户的密码以访问Firewall Management Center Web 界面。

过程

步骤 1 以管理员用户身份登录Firewall Management Center的 Web 界面。要重置管理员密码，您需要与设备建立控制台连接。

步骤 2 要从 CLI 访问 Linux Shell，请输入 **expert** 命令。

步骤 3 在外壳提示符下，输入 **sudo usertool.pl -p "admin password"** 命令。其中 *password* 是 Web 界面管理员用户的新密码。

以下示例中，密码为 **SourcefireM1!**。

```
>
>
>
>
>
>
> show version
-------------------[ firepower ]--------------------
Model                     : Secure Firewall Management Center 4700 (66) Version 7.4.0 (Build 1482)
UUID                      : d65dab0a-1989-11e0-bee7-1b7119c5584b
Rules update version      : 2022-01-06-001-vrt
LSP version               : lsp-rel-20221122-1610
VDB version               : 361
----------------------------------------------------

> expert
admin@firepower:~$ sudo usertool.pl -p "admin SourcefireM1!"
Changing BMC password for user admin at /usr/local/sf/lib/perl/5.32.1/SF/Auth.pm line 3696.
admin@firepower:~$
```

步骤 4 在密码提示下，输入新密码。

查看自动初始配置

在初始配置过程中（无论是通过初始配置向导还是 CLI 执行），Firewall Management Center都会自动配置维护任务，以保持系统为最新状态并持续备份您的数据。

这些任务计划为 UTC，这意味着在本地发生时，取决于日期和您的特定位置。此外，由于这些任务是以UTC时间计划的，因此它们不会根据您所在地区可能实行的夏令时、夏令时或任何此类季节性调整进行调整。如果您受此影响，则根据当地时间，计划任务在夏季会比冬季晚一小时执行。

注释 我们强烈建议您查看这些自动计划的配置，确认Firewall Management Center已成功创建这些配置，并在必要时进行调整。

表 *1: Firewall Management Center*的维护任务

任务	说明	GUI 路径	更多信息
每周 GeoDB 更新	GeoDB 是一款可根据地理位置查看和过滤流量的数据库。	系统 > 更新 > 地理位置更新 > 定期地理位置更新	*Cisco Secure Firewall Management Center 管理指南*
每周Firewall Management Center软件更新	Firewall Management Center 会自动安排每周任务，以下载 Firewall Management Center 及其托管设备的最新软件。	系统 > 工具 > 计划	
每周Firewall Management Center配置备份	Firewall Management Center会自动安排每周任务，执行本地存储的仅配置备份。	系统 > 工具 > 计划	*Cisco Secure Firewall Management Center 管理指南*
漏洞数据库更新	Firewall Management Center会从思科支持站点下载并安装最新的漏洞数据库 (VDB) 更新。这是一次性操作。	系统 > 工具 > 计划	*Cisco Secure Firewall Management Center 管理指南*
每日入侵规则更新	Firewall Management Center会从思科支持站点配置每日自动入侵规则更新。Firewall Management Center会在下次部署受影响的策略时，向受影响的受管设备部署自动入侵规则更新。	系统 > 更新 > 规则更新	

配置 Firewall Management Center 管理设置

完成Firewall Management Center的初始设置并验证成功后，我们建议您完成部署相关的一些管理任务，以便更易于管理。此外，您还应完成在初始设置过程中跳过的所有任务，例如许可证配置。使用默认 **admin** 帐户或具有管理员访问权限的其他帐户建立这些配置。

在多个防火墙管理中心共享同一 IP 地址且通过端口号区分的 NAT 环境中：继续之前请注意以下条件：

- 每个防火墙管理中心只能支持一个登录会话。
- 要访问不同的防火墙管理中心，请为每次登录使用不同的浏览器（例如 Firefox 和 Chrome），或将浏览器设置为隐身或隐私模式。

过程

步骤 1 登录Firewall Management Center。

步骤 2 在**用户名**和**密码**字段中，输入用户名和密码。

步骤 3 点击**登录 (Login)**。

步骤 4 配置以下管理任务：

任务	GUI 路径	更多信息
创建用户账户	系统 > 用户	*Cisco Secure Firewall Management Center* 管理指南
配置时间设置	系统 > 配置 > 时间同步	
配置智能许可	系统 > 许可证 > 智能许可证	

将受管设备添加到 Firewall Management Center

对于每台受管设备，请按照以下说明建立不包含多租户、集群或高可用性的简单部署。要使用任何这些功能配置部署，请参阅适用于您的版本的*Cisco Secure Firewall Management Center 设备配置指南*。

开始之前

- 执行设备特定的设置操作，并将设备配置为支持远程管理（具体操作请参阅该设备的《入门指南》）。

重要事项 请务必记下用于该设备的注册密钥。

- 如果您的环境使用 NAT，请记录设备设置期间使用的 NAT ID。
- 如果您的环境使用 DNS，请记下解析为设备的有效 IP 地址的主机名。如果网络使用 DHCP 来分配 IP 地址，请使用主机名而不是 IP 地址。
- 如果您的环境不使用 DNS，则需要设备的 IP 地址。

- 确定受管设备所需的许可证并将其添加到Firewall Management Center；您可以在将受管设备添加到Firewall Management Center的过程中，为其分配许可证。
- 将受管设备添加到Firewall Management Center后，为其分配访问控制策略。以下说明包括为此目的建立基本访问控制策略的程序。

过程

步骤 1 依次选择 **设备** > **设备管理** > **添加 (Add)** > **添加设备 (Add Device)**。

步骤 2 在**主机**字段中，输入要添加的设备的 IP 地址或主机名。

设备的主机名是完全限定名称或通过本地 DNS 解析为有效 IP 地址的名称。如果网络使用 DHCP 来分配 IP 地址，请使用主机名而不是 IP 地址。

在 NAT 环境中，如果在将设备配置为由Firewall Management Center管理时已指定Firewall Management Center的 IP 地址或主机名，则可能无需指定设备的 IP 地址或主机名。

步骤 3 在**显示名称 (Display Name)** 字段中，输入要在 Firewall Management Center Web 接口中显示的设备名称。

步骤 4 在**注册密钥**字段中，输入将设备配置为由 Firewall Management Center管理时所使用的同一注册密钥。该注册密钥是您在设备上最初关联此Firewall Management Center时配置的一次性共享密钥。

步骤 5 选择初始**访问控制策略 (Access Control Policy)**。除非您已有明确需要使用的自定义策略，否则选择**创建新策略**，然后选择**阻止所有流量**。之后您可以更改此设置以允许流量通过。

如果设备与所选策略不兼容，部署将会失败。这种不兼容可能由多种原因导致，包括许可不匹配、型号限制、被动模式与串联模式相关问题以及其他配置错误。有关详细信息，请参阅《*Cisco Secure Firewall Management Center 设备配置指南*》。解决导致失败的问题后，请手动将配置部署到该设备。

步骤 6 选择要应用到设备的许可证。

步骤 7 如果在设备安装过程中使用了 NAT ID，请展开**高级**部分，并在**唯一 NAT ID** 字段中输入相同的 NAT ID。

步骤 8 点击**注册 (Register)**。

Firewall Management Center可能需要长达两分钟来验证设备的心跳并建立通信。

设置无人值守管理

通过局域网串行 (SOL) 连接，LOM 功能允许您在Firewall Management Center设备上执行有限的操作。借助于LOM，可使用带外管理连接上的CLI执行诸如查看机箱序列号或监控运行状况（如风扇速度和温度）之类的任务。

注释 您只能在 CIMC 接口上使用 LOM。

如果需要将Firewall Management Center恢复为出厂默认设置，但您无法物理访问该设备，可以使用 LOM 执行恢复流程。

注意 恢复过程会重置设备上的 LOM 设置；您无法使用 LOM 访问新恢复的设备。当使用 LOM 将管理中心恢复出厂设置时，如果您无法物理访问该设备，且删除了许可证和网络设置，则恢复后将无法访问该设备。

注释 防火墙设备也支持 LOM。您可以通过每个设备的本地 Web 界面，为其配置 LOM 及 LOM 用户。您无法使用Firewall Management Center配置防火墙设备上的 LOM。同样，因为每个设备的用户都是独立管理的，因此，在 Firewall Management Center 上启用或创建 LOM 用户不会将此功能转移到防火墙设备上的用户。

前提条件

- 在您的本地计算机上安装智能平台管理接口 (IMPI) 实用程序。有关详细信息，请参阅IPMI 实用程序安装，第 17 页。
- 确定使用 IPMI 工具访问设备所需的命令。有关详细信息，请参阅*Cisco Secure Firewall Management Center 管理指南*。

要设置 LOM，请执行以下操作：

步骤	任务	GUI 路径	更多信息
1	启用 LOM	系统 > 用户 > 用户	*Cisco Secure Firewall Management Center 管理指南*
2	启用 LOM 用户访问	系统 > 配置 > 控制台配置 > 无人值守管理	*Cisco Secure Firewall Management Center 管理指南*
3	使用第三方 IPMI 实用程序，创建与设备的 SOL 连接。	-	IPMI 实用程序安装，第 17 页

IPMI 实用程序安装

在计算机上使用第三方 IPMI 实用程序创建与设备的 SOL 连接。IPMItool 是许多 Linux 发行版的标准配置，但在 Mac 和 Windows 系统上必须安装实用程序。

如果计算机运行的是 Mac OS，请安装 IPMItool。首先，请确认您的 Mac 已安装 Apple 的 Xcode 开发者工具包。请确保已安装命令行开发的可选组件（较高版本中的“UNIX 开发”和“系统工具”，或较低版本中的“命令行支持”）。最后，安装 MacPorts 和 IPMItool。有关详细信息，请参阅 https://developer.apple.com/technologies/tools/和http://www.macports.org/。

对于 Windows 环境，请使用 ipmiutil，这需要自己编译。如果无法访问编译器，可以使用 ipmiutil 自身来编译。有关详细信息，请参阅http://ipmiutil.sourceforge.net/。

预配置Firewall Management Center

您可以在暂存位置（用于预配置或暂存多台设备的中心位置）预配置Firewall Management Center，然后在目标位置（暂存位置以外的任何位置）部署它。

要预配置并部署设备至目标位置，请执行以下步骤：

1. 在暂存位置的设备上安装系统。
2. 关闭设备并装运至目标位置。
3. 在目标位置部署设备。

注释 保存所有包装材料，并在重新包装设备时将所有参考材料和电源线一起包装。

预配置的前提条件

在预配置设备之前，收集暂存位置和目标位置的网络设置、许可证和其他相关信息。

在初始设置期间，使用足够信息配置设备以将设备连接到网络并安装系统。

预配置设备至少需要以下信息：

- 新密码（初始设置要求更改密码）
- 设备的主机名
- 设备的域名
- 设备的 IP 管理地址
- 设备在目标位置的网络掩码
- 设备在目标位置的默认网关
- DNS 服务器在暂存位置或目标位置（如可访问）的 IP 地址
- NTP 服务器在暂存位置或目标位置（如可访问）的 IP 地址

预配置可选信息

可更改某些默认配置，包括以下内容：

- 时区（如果选择手动设置设备的时间）
- 自动备份的远程存储位置
- 用于启用 LOM 的 LOM IP 地址

预配置时间管理

过程

步骤 1 将时间与物理 NTP 服务器同步。

步骤 2 使用以下方法之一设置 DNS 和 NTP 服务器的 IP 地址：

- 如果暂存位置的网络可访问目标位置的 DNS 和 NTP 服务器，则使用目标位置 DNS 和 NTP 服务器的 IP 地址。
- 如果暂存位置的网络无法访问目标位置的 DNS 和 NTP 服务器，请使用暂存位置的相关信息，并在目标位置重置设备。

步骤 3 如手动设置设备上的时间（而不是使用 NTP），请使用目标部署的时区。有关详细信息，请参阅您版本的《*Cisco Secure Firewall Management Center* 管理指南》。

为Firewall Management Center装运做准备

过程

步骤 1 按照《*Cisco Secure Firewall Management Center 1700*、*2700* 和 *4700* 硬件安装指南》中的说明安装机箱。

步骤 2 为设备连接电缆并打开设备电源。

步骤 3 使用 CLI 执行设备的初始设置。

步骤 4 安全地关闭 Firewall Management Center 电源。

步骤 5 确保安全地准备装运设备。有关详细信息，请参阅装运注意事项，第 19 页。

装运注意事项

要准备将设备运往目标位置，必须安全地关闭并重新包装设备。请注意以下事项：

- 用原装包装重新包装设备。

- 将所有参考资料和电源线随设备一起包装。
- 为目标位置提供所有设置和配置信息，包括新密码和检测模式。

设备预配置故障排除

如果已针对目标部署正确地预配置了设备，则无需进一步配置就可安装并部署 Firewall Management Center。

如果无法正常登录设备，可能是预配置存在错误。尝试完成以下故障诊断程序：

- 确认所有电源线和通信线已正确地连接到设备。
- 确认拥有设备的当前密码。暂存位置的初始设置提示更改密码。有关新密码，请参阅暂存位置提供的配置信息。
- 确认网络设置正确。有关详细信息，请参阅使用 CLI 执行Firewall Management Center的初始设置，第 7 页。
- 确认通信端口正确并正常运行。有关防火墙端口管理及所需开放端口的信息，请参阅*Cisco Secure Firewall Management Center* 管理指南。

如果登录设备时仍然遇到问题，请联系 Cisco TAC。

关闭Firewall Management Center电源

正确关闭系统非常重要。仅拔掉电源或按下电源开关可能会导致文件系统严重损坏。设备后台始终运行着许多进程，直接拔掉电源或关闭电源无法让设备正常关机。

您可以使用以下方法之一关闭设备：

- Firewall Management Center设备管理页面的 Web 界面：选择**系统** > **配置** > **进程** > **关闭管理中心**。
- Firewall Management Center CLI 中的 **shutdown** 命令。

对于虚拟设备，您可以关闭主机电源。有关详细信息，请参阅您所用虚拟平台的文档。特别是对于 VMware，自定义电源选项是 VMware 工具的一部分。

后续步骤

要继续配置Firewall Management Center，请参阅《*Cisco Secure Firewall Management Center* 管理指南》和《*Cisco Secure Firewall Management Center* 设备配置指南》。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. 保留所有权利。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。