# 在VMware ESXi上部署FireSIGHT管理中心

## 目录



## 简介

本文档介绍在VMware ESXi上运行的FireSIGHT管理中心（也称为防御中心）的初始设置。FireSIGHT管理中心允许您管理一个或多个FirePOWER设备、下一代入侵防御系统(NGIPS)虚拟设备和具备FirePOWER服务的自适应安全设备(ASA)。

> **注意**：本文档是《FireSIGHT系统安装指南》和《用户指南》的补充。有关ESXi特定配置和故障排除问题，请参阅VMware知识库和文档。

## 先决条件

### 使用的组件

本文档中的信息基于以下平台：

- 思科FireSIGHT管理中心
- 思科FireSIGHT管理中心虚拟设备
- VMware ESXI 5.0

在本文档中，“设备”是指以下平台：

- Sourcefire FirePOWER 7000系列设备和8000系列设备
- 适用于VMware ESXi的Sourcefire NGIPS虚拟设备
- 具备FirePOWER服务的Cisco ASA 5500-X系列

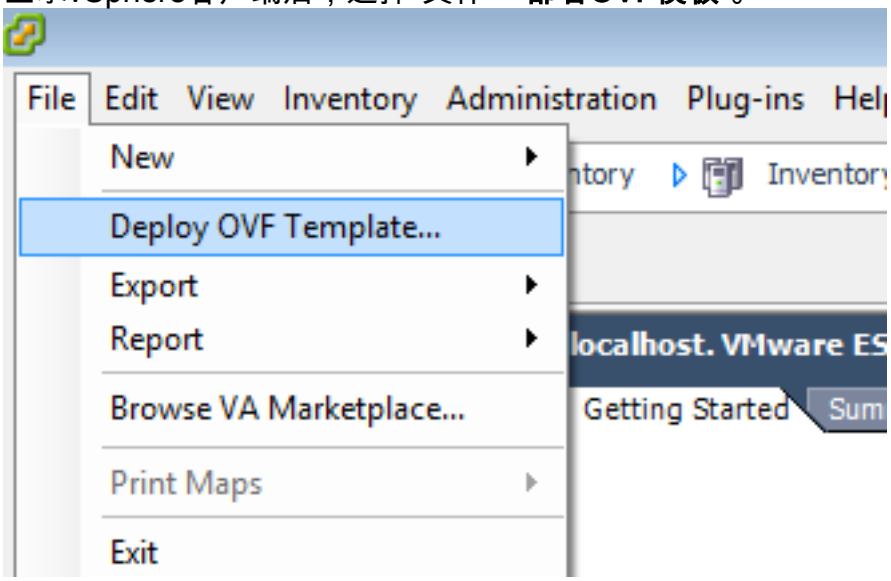
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 配置

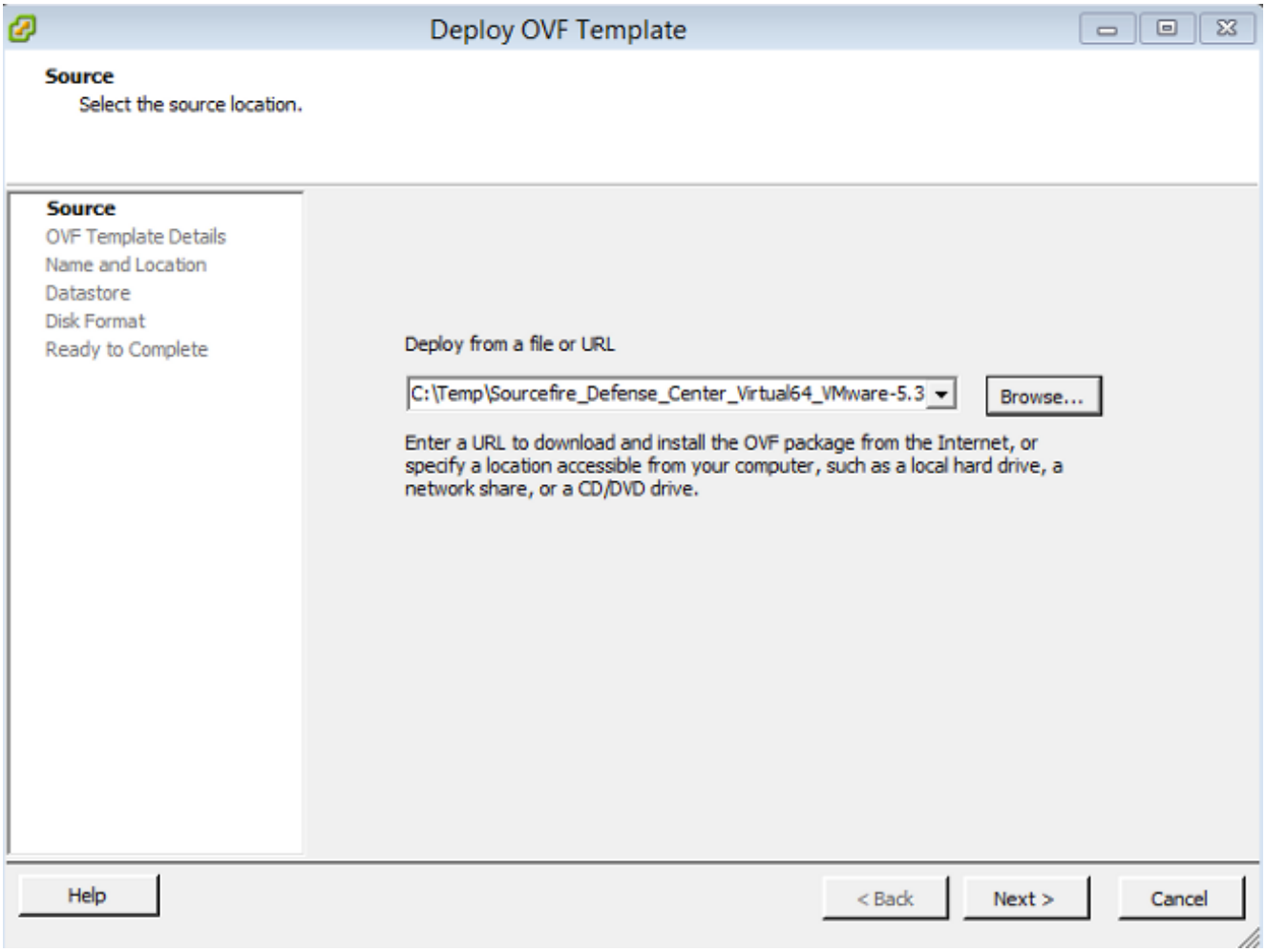
### 部署OVF模板

1. 从思科支**持和下载站点下**载Cisco FireSIGHT管理中心虚拟设备。
2. 将tar.gz文件的内容解压到本地目录。
3. 使用VMware vSphere客户端连**接到ESXi服务器**。

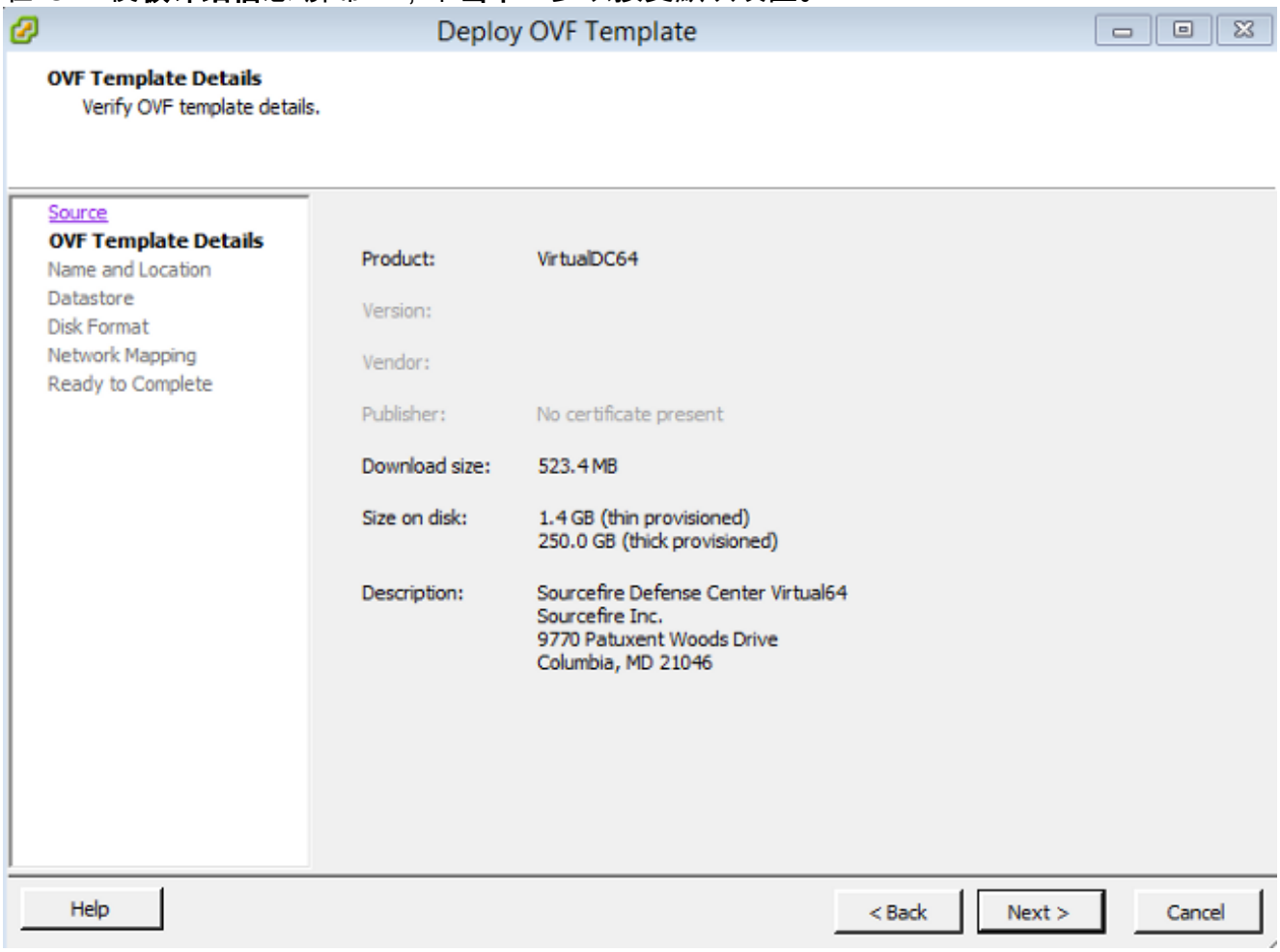

4. 登录vSphere客户端后，选择“文件”**>“部署OVF模板”**。



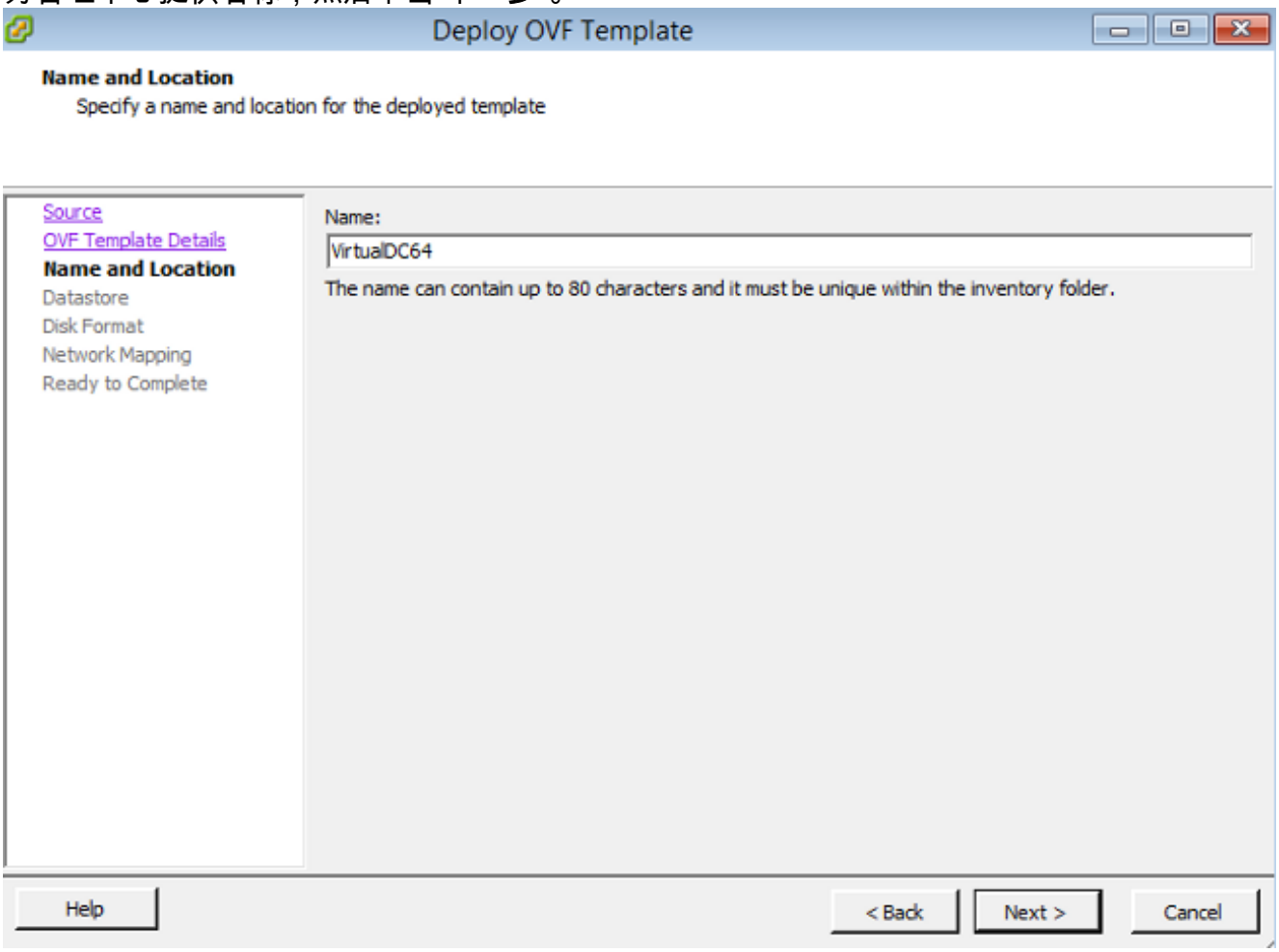

5. 单击**Browse**并找到您在步骤2中提取的文件。选择OVF文件Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf，然后单击**Next。**



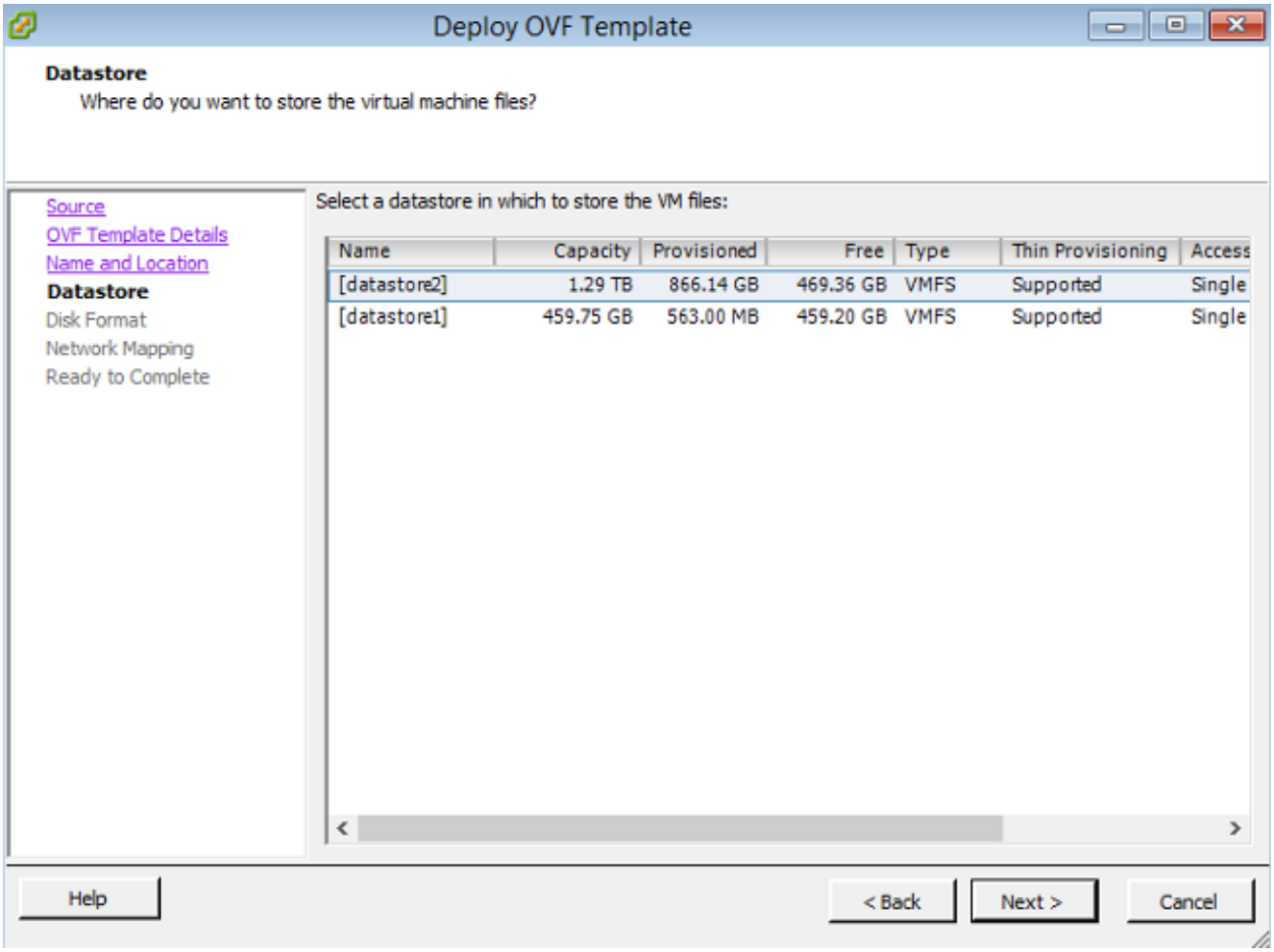

6. 在“OVF模**板详细信息**”屏幕上，单**击下**一步以接受默认设置。



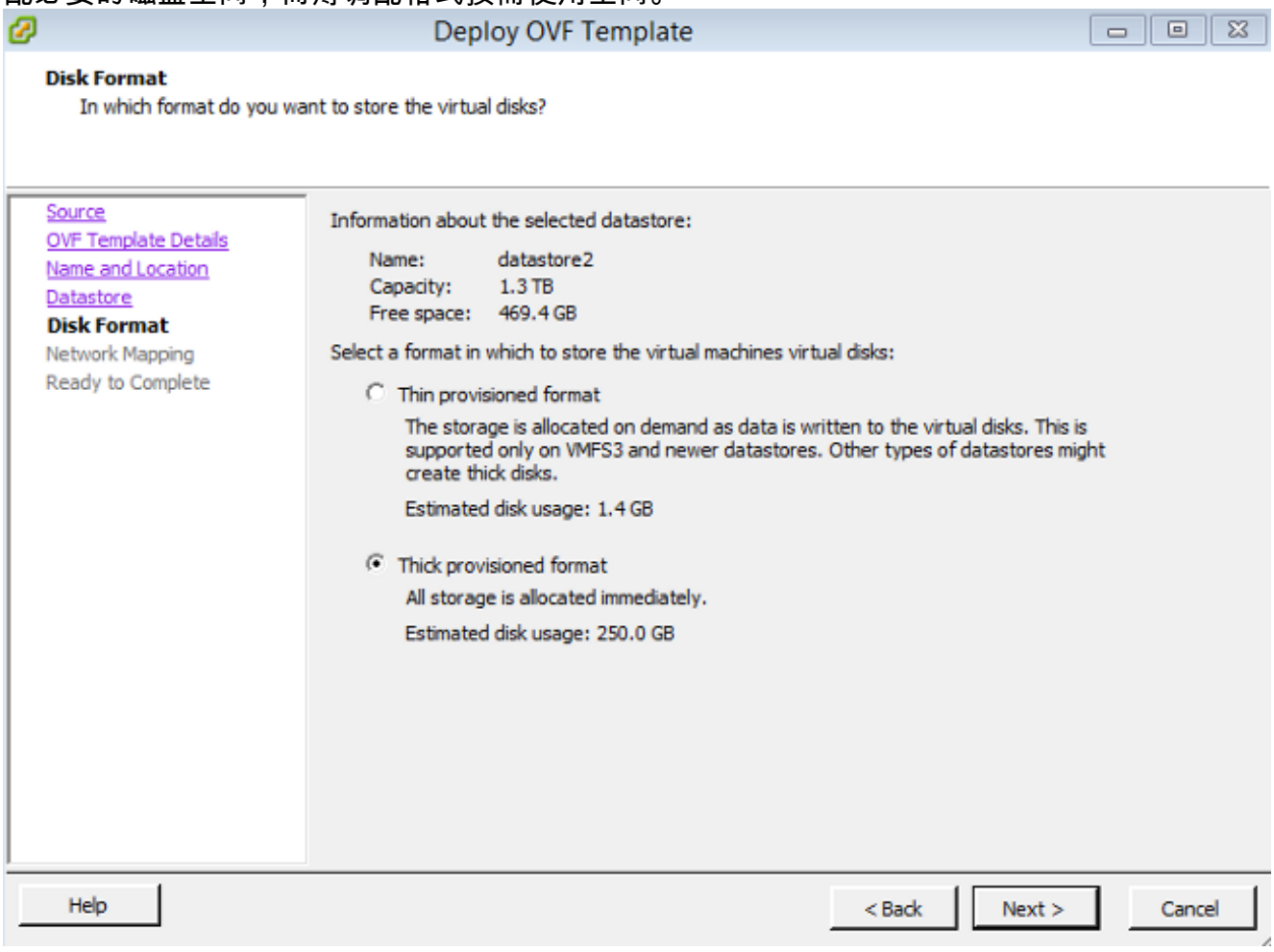
7. 为管理中心提供名称，然后单击“下一步”。



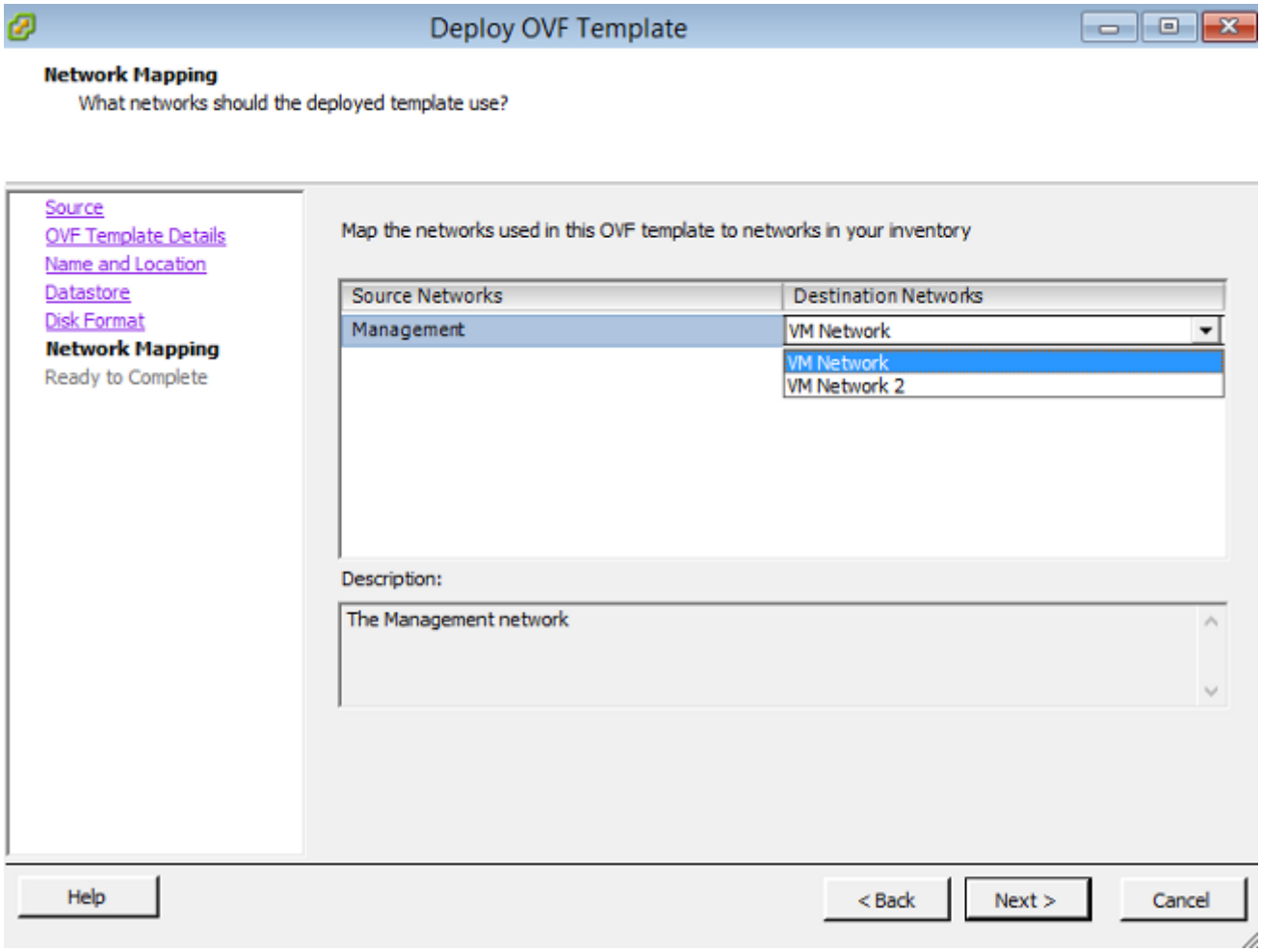

8. 选择要在其上创建虚拟机的Datastore，然后单击“下一步”。



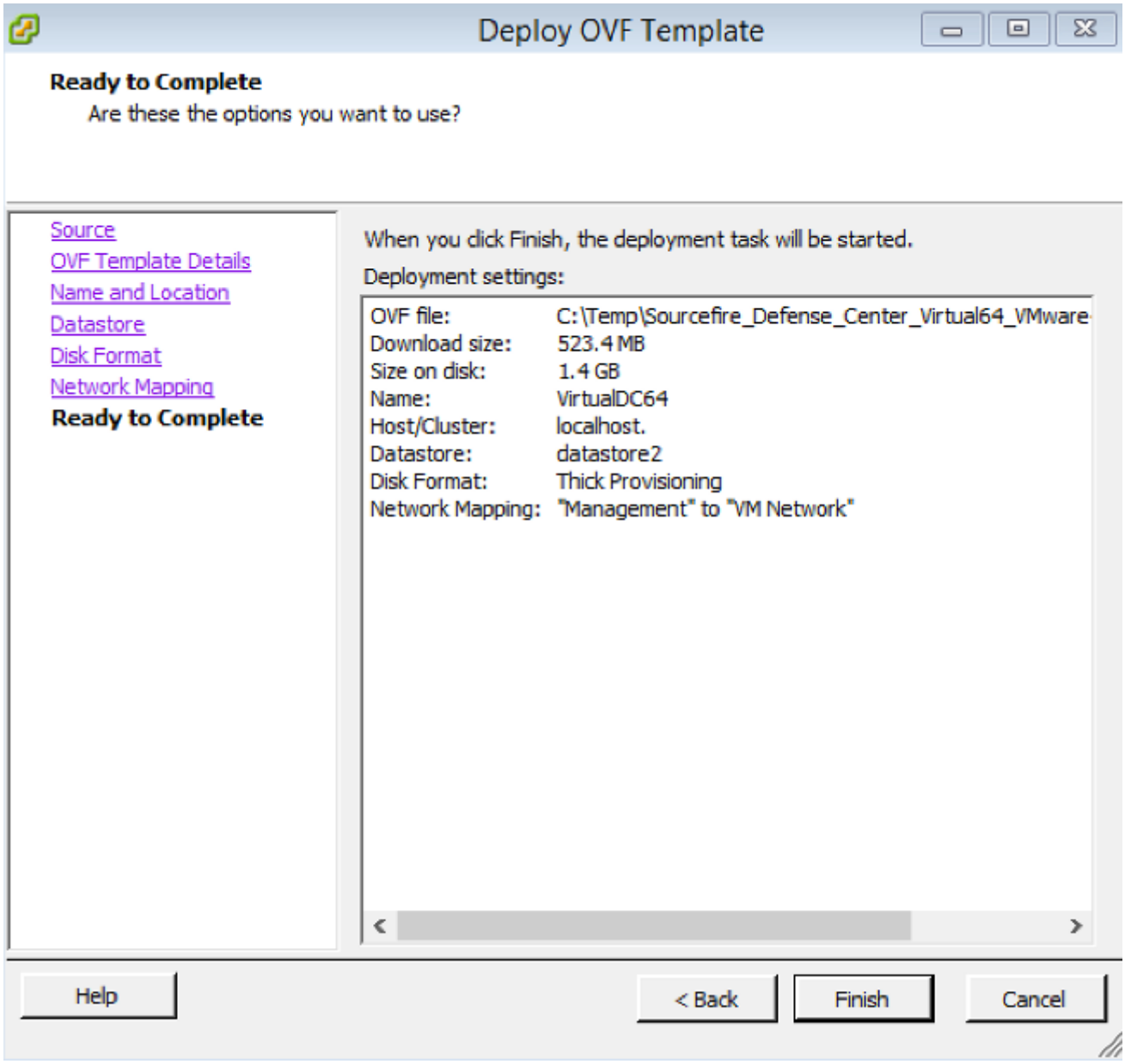

9. 单击“磁盘**格式”的“**厚调配格式”单选**按钮，然**后单击**“下一步”**。厚调配格式在创建虚拟磁盘时分配必要的磁盘空间，而薄调配格式按需使用空间。



10. 在“网**络映射**”部分，将FireSIGHT管理中心的管理接口关联到VMware网络，然后单击“下**一步**”。

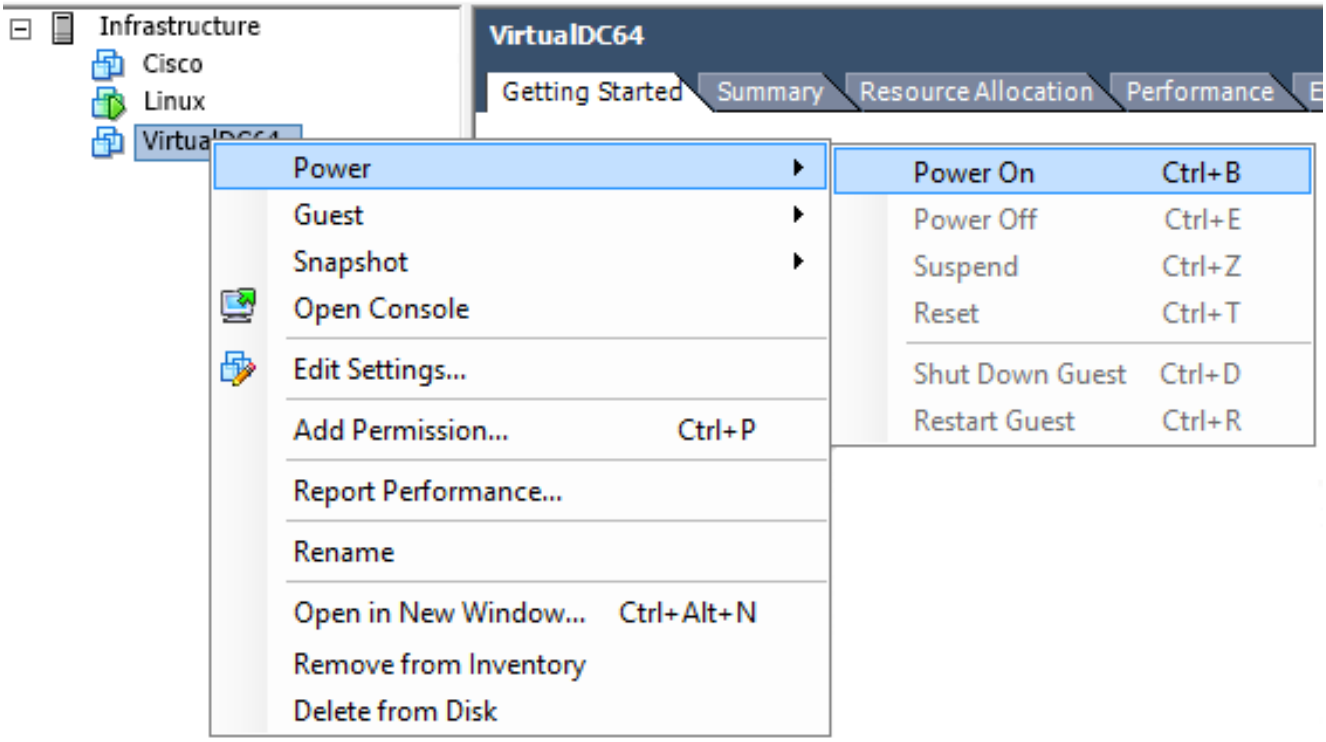



11. 单击**Finish**以完成OVF模板部署。

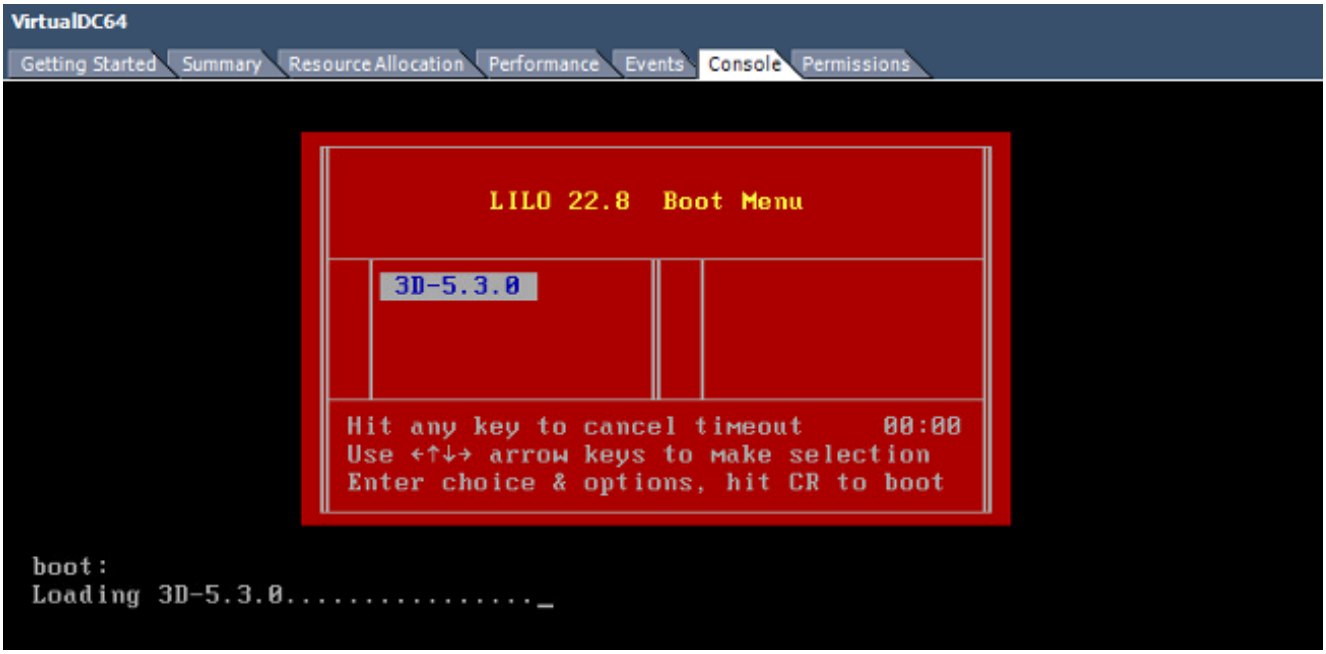



## 开机并完成初始化

1. 导航至新创建的虚拟机。 右键单击服务器名称，然后选择**Power > Power On**，以便首次启动服务器。




2. 导航至**Console**选项卡以监控服务器控制台。系统将显示LILO Boot Menu。




一旦BIOS数据检查成功，初始化过程就会启动。第一次启动可能需要额外时间才能完成，因为配置数据库首次初始化。

```
Firstboot detected, executing scripts
Executing S03install-math-pari.sh                                  [  OK  ]
Executing S04async_syslog_dc.sh                                    [  OK  ]
Executing S04fix-httpd.sh                                          [  OK  ]
Executing S05set-mgmnt-port                                        [  OK  ]
Executing S06addusers                                              [  OK  ]
Executing S07uuid-init                                             [  OK  ]
Executing S09configure_mysql                                       [  OK  ]

************ Attention **********

   Initializing the configuration database.  Depending on available
   system resources (CPU, memory, and disk), this may take 30 minutes
   or more to complete.

************ Attention **********

Executing S10database
_
```

完成后，您可能会看到“No thic device”(无此类设备)的消息。

```
  Copyright (c) 1999-2010 Intel Corporation.
  Silicom Bypass-SD Control driver v5.0.39.5
  No such device
  _
```

3. 按**Enter**以获取登录提示。

```
 Copyright (c) 1999-2010 Intel Corporation.
 Silicom Bypass-SD Control driver v5.0.39.5
 No such device

 Sourcefire Virtual Defense Center 64bit v5.3.0 (build 571)
 Sourcefire3D login: _
```

**注意：**消息“WRITE SAME（写入相同）”失败。手动归零。” 可能在系统首次启动后出现。这不表示有缺陷，它正确表示VMware存储驱动程序不支持WRITE SAME命令。 系统显示此消息，然后使用fallback命令执行相同的操作。

## 配置网络设置

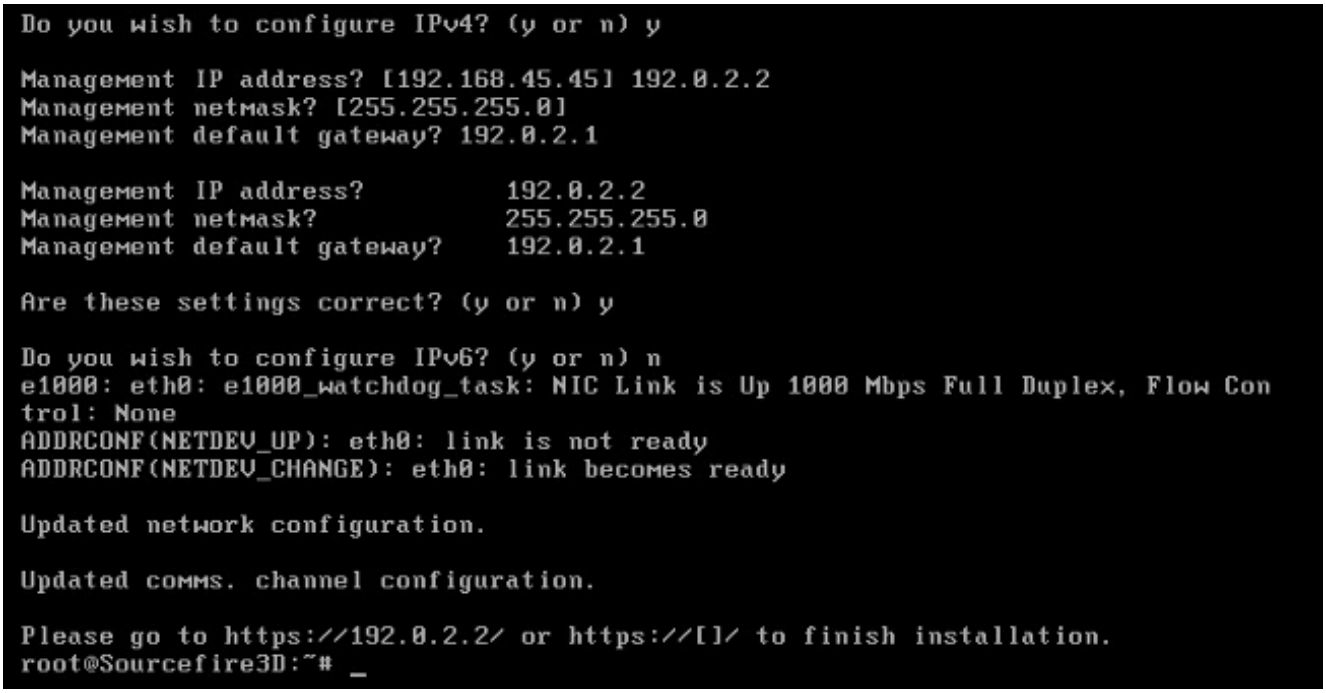
1. 在Sourcefire3D登录提示符上，使用以下凭证登录： 对于版本5.xusername：**admin**密码：**Sourcefire**适用于6.x及更高版本username：**admin**密码：**管理123提示：**在GUI的初始设置过程中，您可以更改默认密码。
2. 网络的初始配置使用脚本完成。您需要以根用户身份运行该脚本。要切换到根用户，请输入**sudo su -命令和密码Sourcefire或Admin123**（用于6.x）。 以根用户身份登录管理中心命令行时，请谨慎。

```
admin@Sourcefire3D:~$ sudo su -
Password:
```

3. 要开始网络配置，请输入configure-network**脚本**作为根。

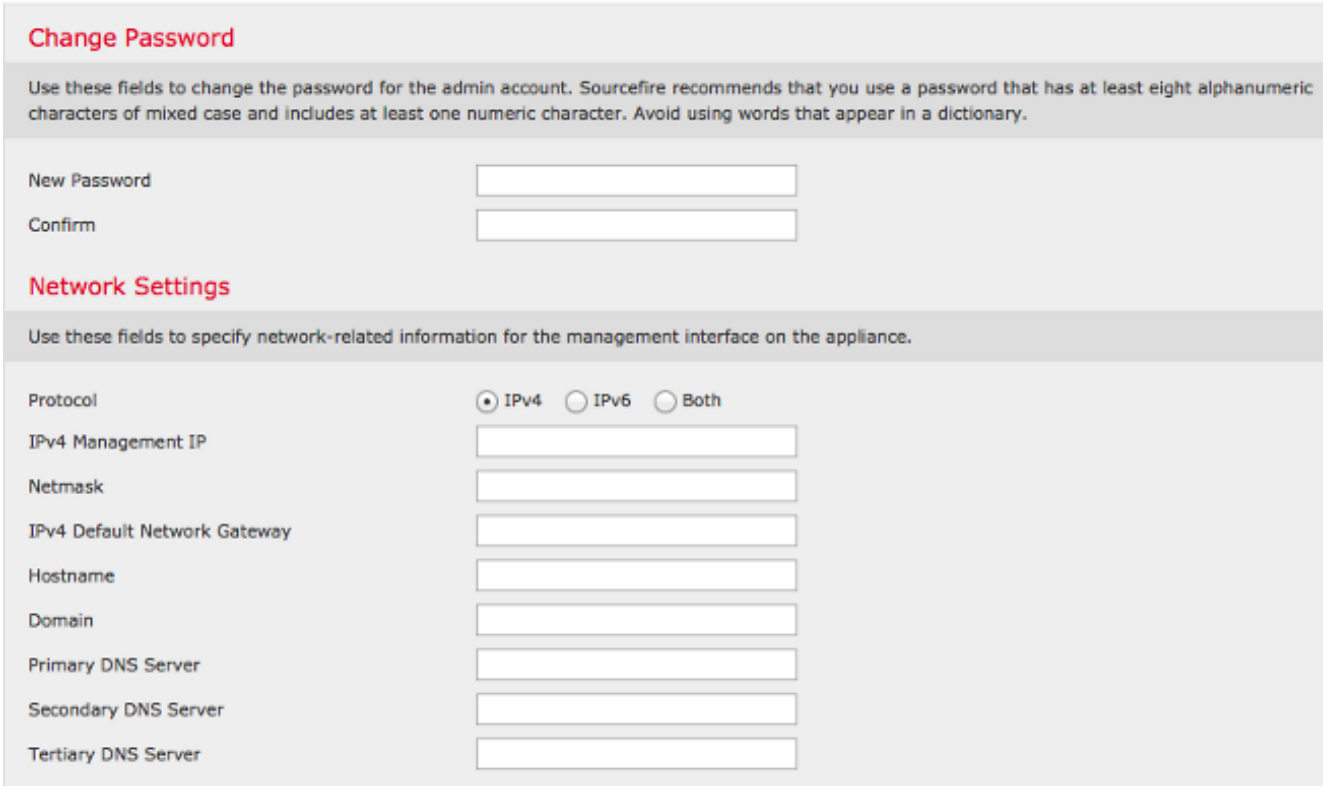
```
root@Sourcefire3D:~# configure-network

Do you wish to configure IPv4? (y or n) y
```

系统将要求您提供管理IP地址、网络掩码和默认网关。确认设置后，网络服务将重新启动。因此，管理接口关闭，然后恢复。




## 执行初始设置

1. 配置网络设置后，打开Web浏览器，通过HTTPS浏览到已配置的IP(本例中为 https://192.0.2.2)。 根据提示对默认SSL证书进行身份验证。使用以下凭证登录：对于版本5.x username：**admin**密码：**Sourcefire**适用于6.x及更高版本username：**admin**密码：**管理123**
2. 在下面的屏幕上，除密码更改和接受服务条款外，所有GUI配置部分都是可选的。 如果知道信息，建议使用设置向导来简化管理中心的初始配置。配置后，单击**Apply**以将配置应用到管理中心和注册设备。 配置选项的简要概述如下：**更改密码:** 允许您更改默认管理员帐户的密码。 需要更改密码。 **网络设置:** 允许您修改之前为设备或虚拟机的管理接口配置的IPv4和IPv6网络设置。**时间设置：** 建议您将管理中心与可靠的NTP源同步。IPS传感器可以通过系统策略进行配置，以便与管理中心同步其时间。 或者，可以手动设置时区和显示时区。**定期规则更新导入：** 在初始设置期间，启用定期Snort规则更新，或立即安装。**定期地理定位更新：** 在初始设置期间，启用周期性地理定位规则更新，或立即安装。**自动备份：** 安排自动配置备份。**许可证设置：** 添加功能许可证。**设备注册：** 允许您添加、许可初始访问控制策略并将其应用于预注册设备。 主机名/IP地址和注册密钥应与FirePOWER IPS模块上配置的IP地址和注册密钥匹配。**最终用户许可协议:** 必须接受EULA。




# 相关信息

- 适用于VMware的Firepower管理中心虚拟快速入门指南，版本6.0
- 技术支持和文档 - Cisco Systems