

# 重新映像FireSIGHT管理中心和FirePOWER设备

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[重新映像流程](#)

[开始使用前](#)

[重新映像流程概述](#)

[Cisco Firepower管理中心1000、2500和4500](#)

[故障排除](#)

[未列出System Restore LILO菜单选项](#)

[7010、7020和7030设备](#)

[7110和7120设备](#)

[8000系列设备或管理中心型号FS750、FS1500或FS3500](#)

[型号FMC1000、FMC2500、FMC4500 \( 基于M4的FMC \) 的系统恢复](#)

[未列出启动选项](#)

---

## 简介

本文档通过示例介绍Cisco FireSIGHT管理中心(FMC)和FirePOWER设备的重新映像过程。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件


本文档中的信息基于以下软件和硬件版本：

受管设备	FireSIGHT 管理中心 可用于重新映像的软件版本	
Cisco Firepower 7000 系列		
Cisco Firepower 7100 系列	FS 750	5.2 或更高版本
Cisco Firepower 8100 系列	FS 1500	
Cisco Firepower 8200 系列	FS 3500	

Firepower 8300系列 思科AMP 7150 思科AMP 8150		5.3 或更高版本
--	--	-----------


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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 重新映像流程

 **注意：**在升级或重新映像FireSIGHT管理中心或FirePOWER设备时，请勿插入USB存储设备或插入键盘、视频和鼠标(KVM)交换机。

### 开始使用前

1. 如果计划重新映像管理中心或独立Firepower设备，建议在继续之前备份设备。
2. 识别传感器的型号，并使用“使用的组件”一节中的型号列表确认本指南是否正确。
3. 从思科支持站点下载适合所需软件版本的安装指南和磁盘映像。

 **注：**请勿重命名.iso文件


提供映像：必须将.iso文件复制到运行SSH服务器的主机，该主机可从设备的管理网络重新映像。

 **注意：**如果没有其他SSH服务器可用，则可以使用FMC进行此过程。

验证iso的完整性：文件的md5sum位于页面右侧，用于使用md5sum实用程序进行验证。

4. 安装指南包含逐步重新映像说明，还概述了重新映像处理的几种方法。本文档中提供的图像可供参考。

### 重新映像流程概述

 **注：**5.3版本用于捕获本文中显示的图像。对于其他5.x版本，除了在图中所示的版本号外，重新映像过程是相同的。

```
admin@9900:~$ sudo shutdown -r now

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

Password: _
```

图 1

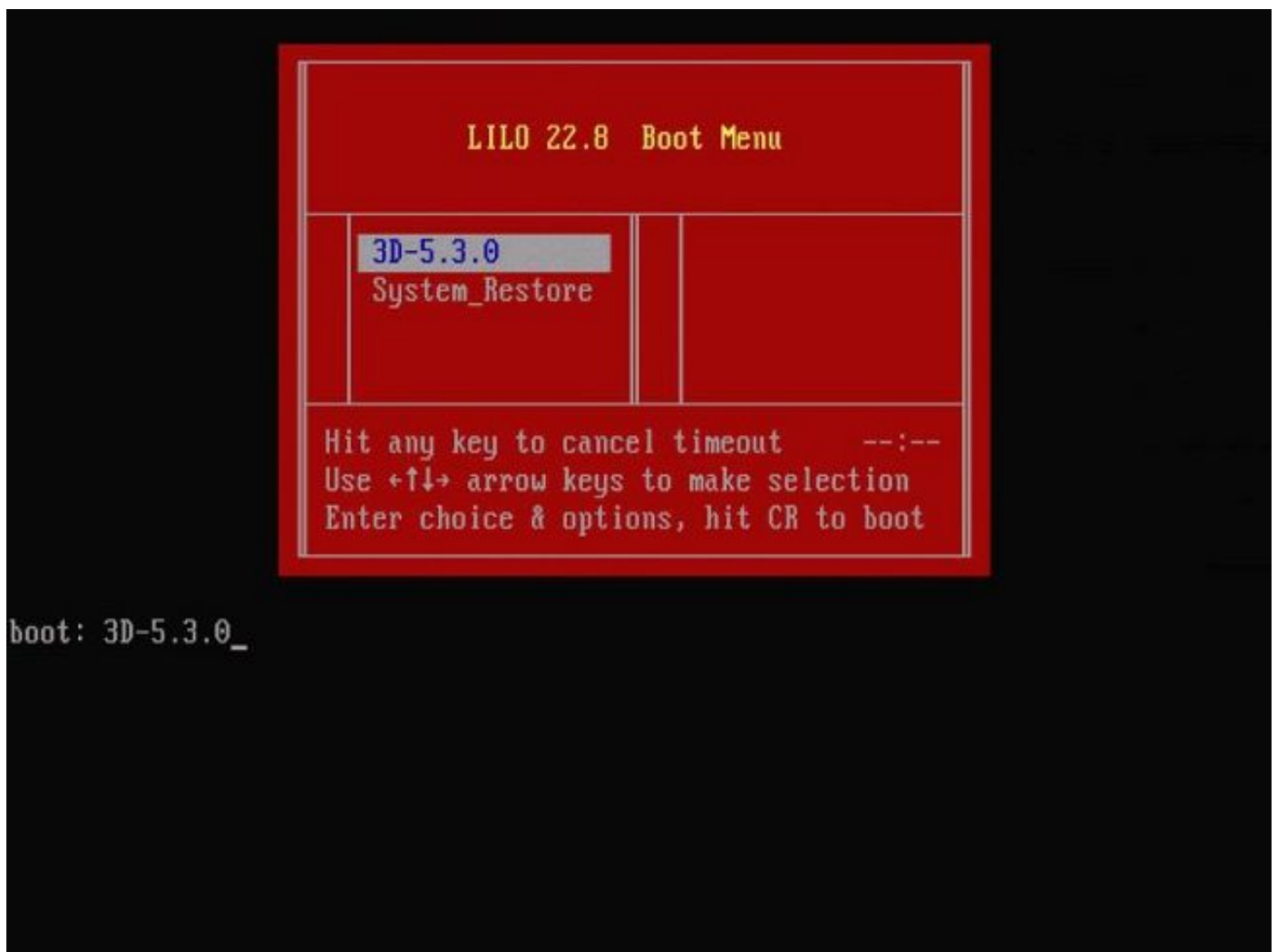


图2 — 系统重新启动时，按键盘上的箭头键以停止倒计时，为下面显示的屏幕选择

System\_Restore选项。

 注意：如果System\_Restore提示符未显示，则必须更改引导顺序以直接引导到恢复分区 (DOM)。有关详细信息，请参阅[System\\_Restore LILO菜单选项缺失](#)。



图 3

```
boot: System_Restore
Loading System_Restore


SYS LINUX 3.35 2007-01-28 EB IOS Copyright (C) 1994-2007 H. Peter Anvin

Welcome to the Sourcefire Linux Operating System

0. Load with standard console
1. Load with serial console
2. Load legacy installer standard
3. Load legacy installer serial
boot: 0
Loading bzImage26.....
Loading install.img.....
.....
```

图4 — 如果使用键盘和显示器，请选择选项0。

---

 注：有时会看到“Restore（恢复）”选项的菜单仅在仅连接控制台时显示（键盘已拔下）。一旦选中“恢复”选项，键盘就可以重新连接回来

---



图 5

Sourcefire 3D Appliance 5.3.0-52 Configuration Menu  
Choose one of the following or press <Cancel> to exit

- 1 IP Configuration
- 2 Choose the transport protocol
- 3 Select Patches/Rule Updates
- 4 Download and Mount ISO
- 5 Run the Install
- 6 Save Configuration
- 7 Load Configuration
- 8 Wipe Contents of Disk

< OK >

<Cancel>

图 6

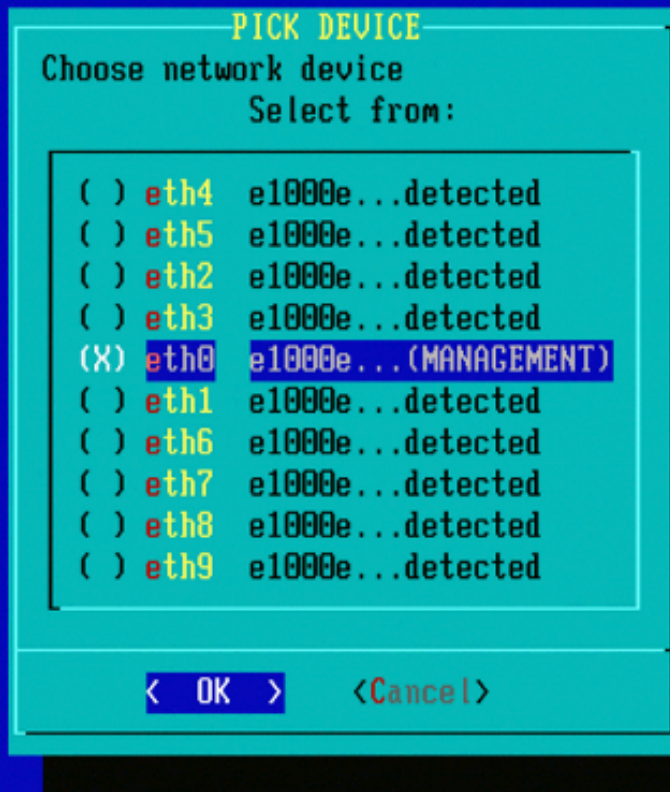


图7 — 要选择网络设备，请按空格键。



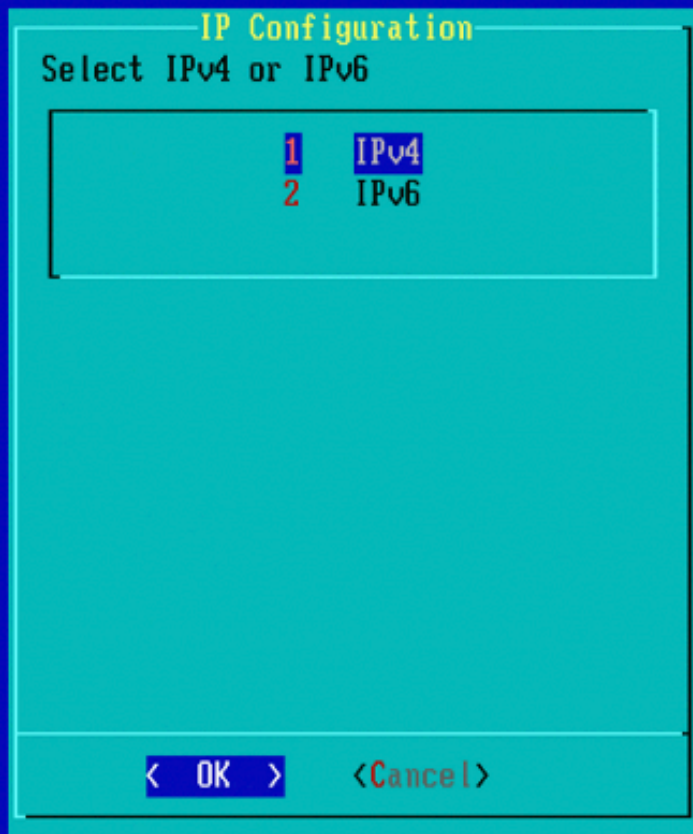


图 8



图 9

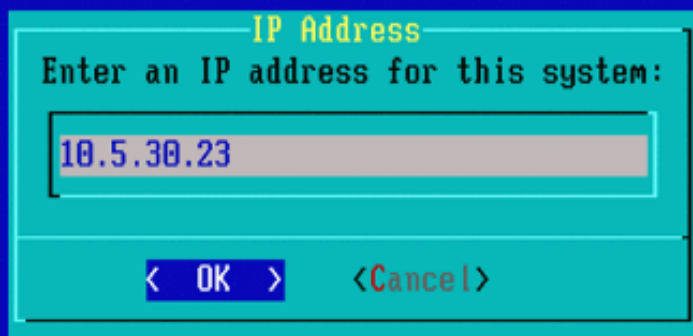


图 10

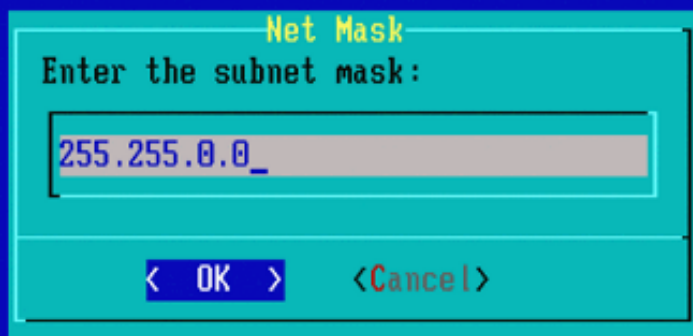


图 11

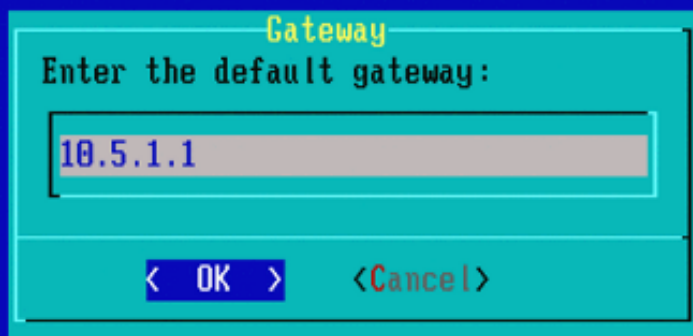


图 12



图 13

Sourcefire 3D Appliance 5.3.0-52 Configuration Menu  
Choose one of the following or press <Cancel> to exit

- 1 IP Configuration
- 2 Choose the transport protocol
- 3 Select Patches/Rule Updates
- 4 Download and Mount ISO
- 5 Run the Install
- 6 Save Configuration
- 7 Load Configuration
- 8 Wipe Contents of Disk

< OK >

<Cancel>

图 14



图15 — 思科支持建议您使用安全复制(SCP)协议。



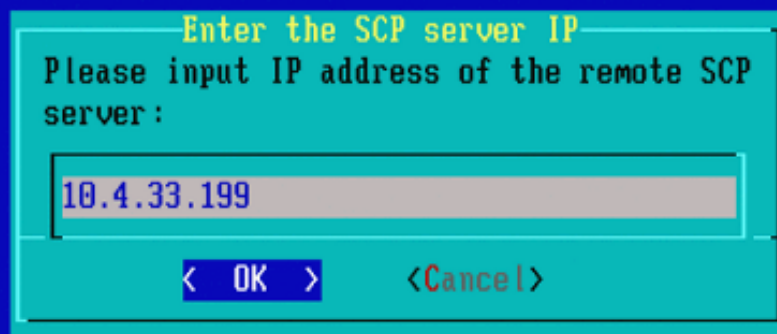



图 16 — 可以使用FireSIGHT管理中心作为此步骤的SCP服务器。继续此过程，并使用管理中心的IP地址和凭证填充System Restore菜单中的字段。更多详细信息，请参阅

安全复制(SCP)服务器用于安全地传输文件。如果必要时，可以使用Sourcefire防御中心(DC)作为SCP服务器将文件传输到另一个Sourcefire设备。当需要将iso映像传输到Sourcefire设备以重新映像时，当常规SCP服务器无法访问或不可用时，此命令非常有用。

步骤1:从[Sourcefire支持门户](#)将相应的.iso文件下载到您的桌面。

第二步：使用SCP客户端，将文件从桌面复制到防御中心。

 提示:SCP客户端通常在Linux或Mac操作系统中可用。但是，在Windows操作系统中，您可能必须安装第三方SCP客户端软件。Sourcefire不提供安装任何特定SCP客户端软件的建议或支持。

下一个示例演示如何将Sourcefire .iso映像文件从Linux系统的Downloads目录复制到Sourcefire防御中心的/var/tmpdirectory:

```
<#root>
```

```
LinuxSystem:~$ cd Downloads
```

```
LinuxSystem:~/Downloads$ scp Sourcefire_3D_Sensor_S3-4.10.2-Restore.iso
```


user\_name

@

IP\_Address\_of\_Defense\_Center

:/var/tmp


---

 注意:请勿更改.iso文件的名称。它可能会在重新映像期间产生检测文件的问题。

---

现在文件被复制到防御中心。您可以继续对Sourcefire设备进行重新映像处理。在重新映像时，如有必要，您可以提供DC的IP地址和用户名，以及您使用之前的说明复制映像文件的路径。

---

 警告：完成重新映像后，您必须从防御中心的/var/tmp目录中移除.iso文件，以减少磁盘空间的利用率。

---

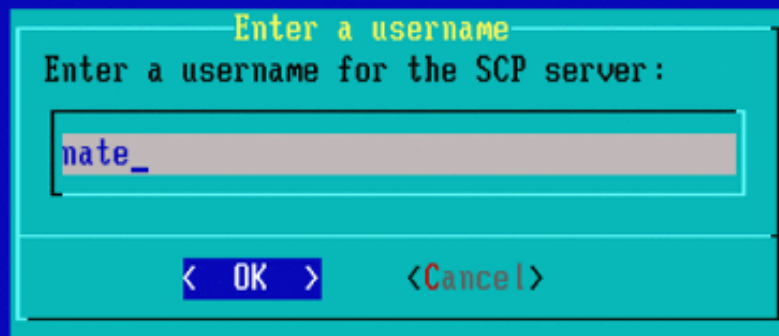


图 17

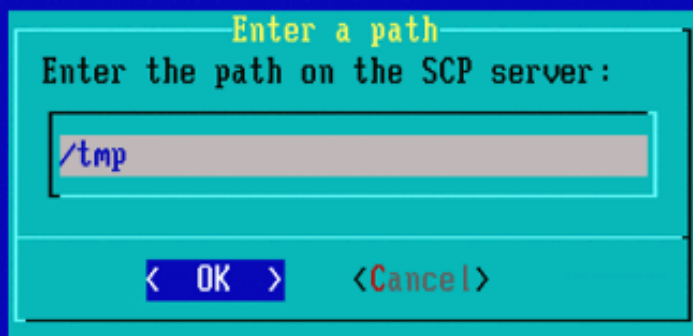


图 18

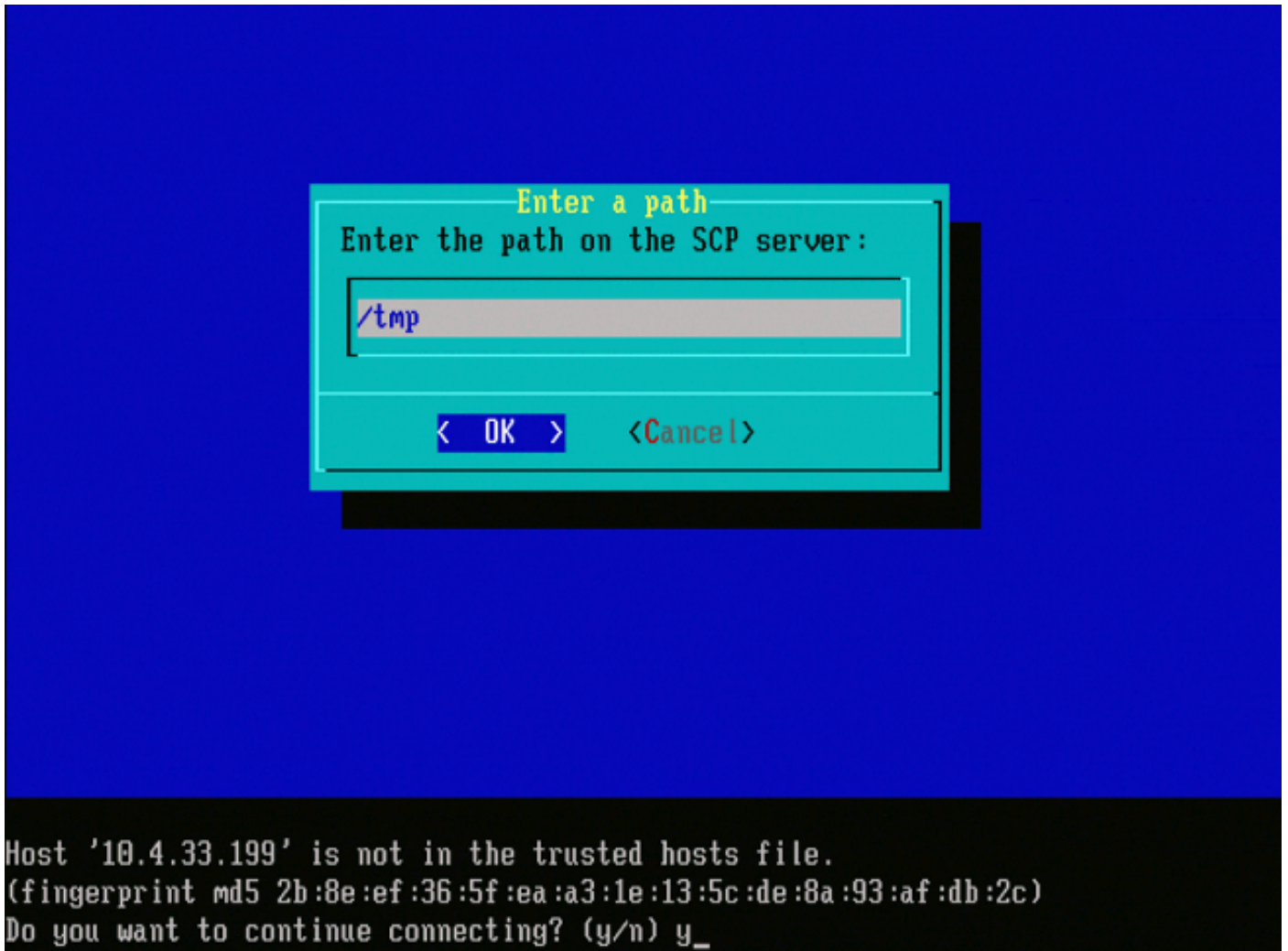



图 19

---

 注意：如果此时收到连接错误而不是预期消息，请验证与SSH服务器的连接。

---

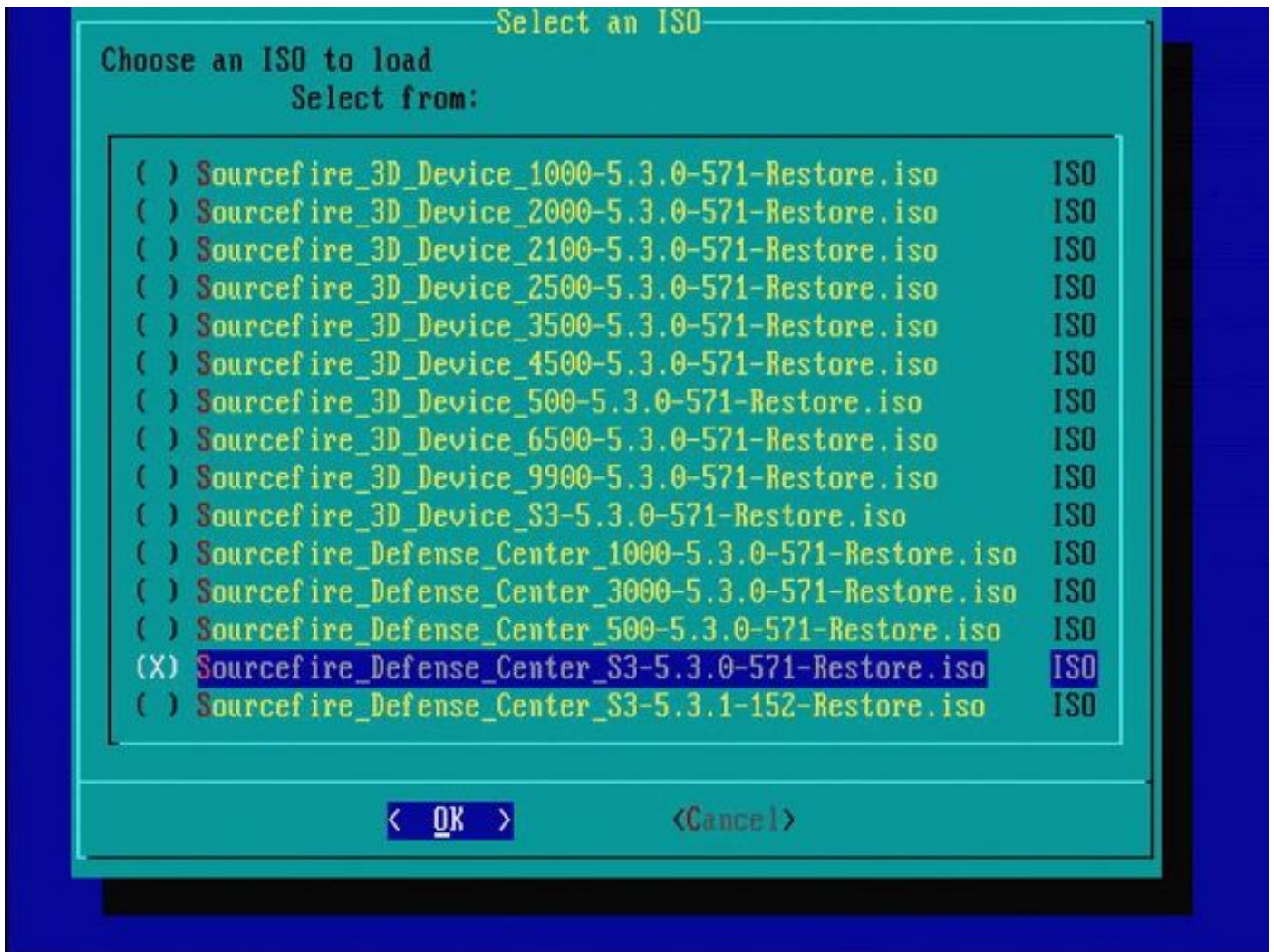



图20 — 要选择.iso映像，请按空格键。

 注：需要为.iso文件使用默认文件名，否则在此步骤中可能检测不到这些文件。  
错误：未找到ISO映像  
在版本6.3中，ISO名称约定已从Sourcefire\_3D\_Device\_S3-<ver>-<build>-Restore.iso更改为Cisco\_Firepower\_NGIPS\_Appliance-<ver>-<build>-Restore.iso。如果遇到“未找到ISO映像”，请将ISO文件重命名为旧文件名。当将6.2.x或更旧版本重新映像到6.3.0或更高版本时，通常会发生这种情况。

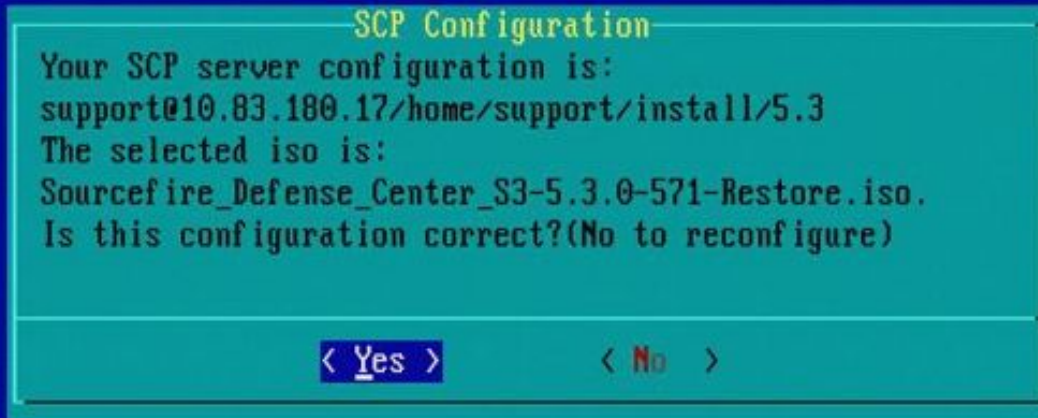


图 21

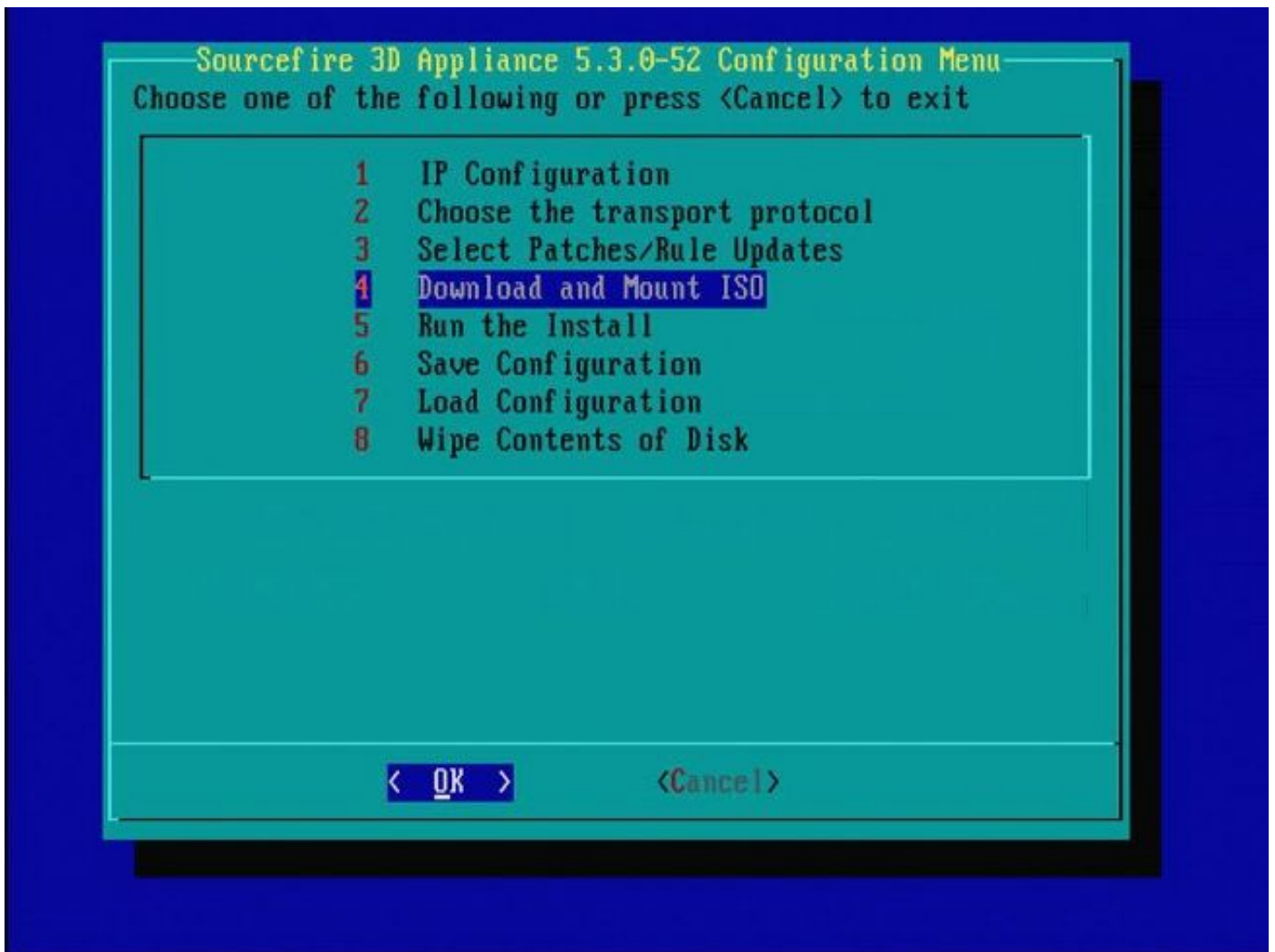


图22 — 思科支持人员建议跳过此过程中的步骤3。可在重新映像完成后安装补丁和Snort规则更新 (SRU)。

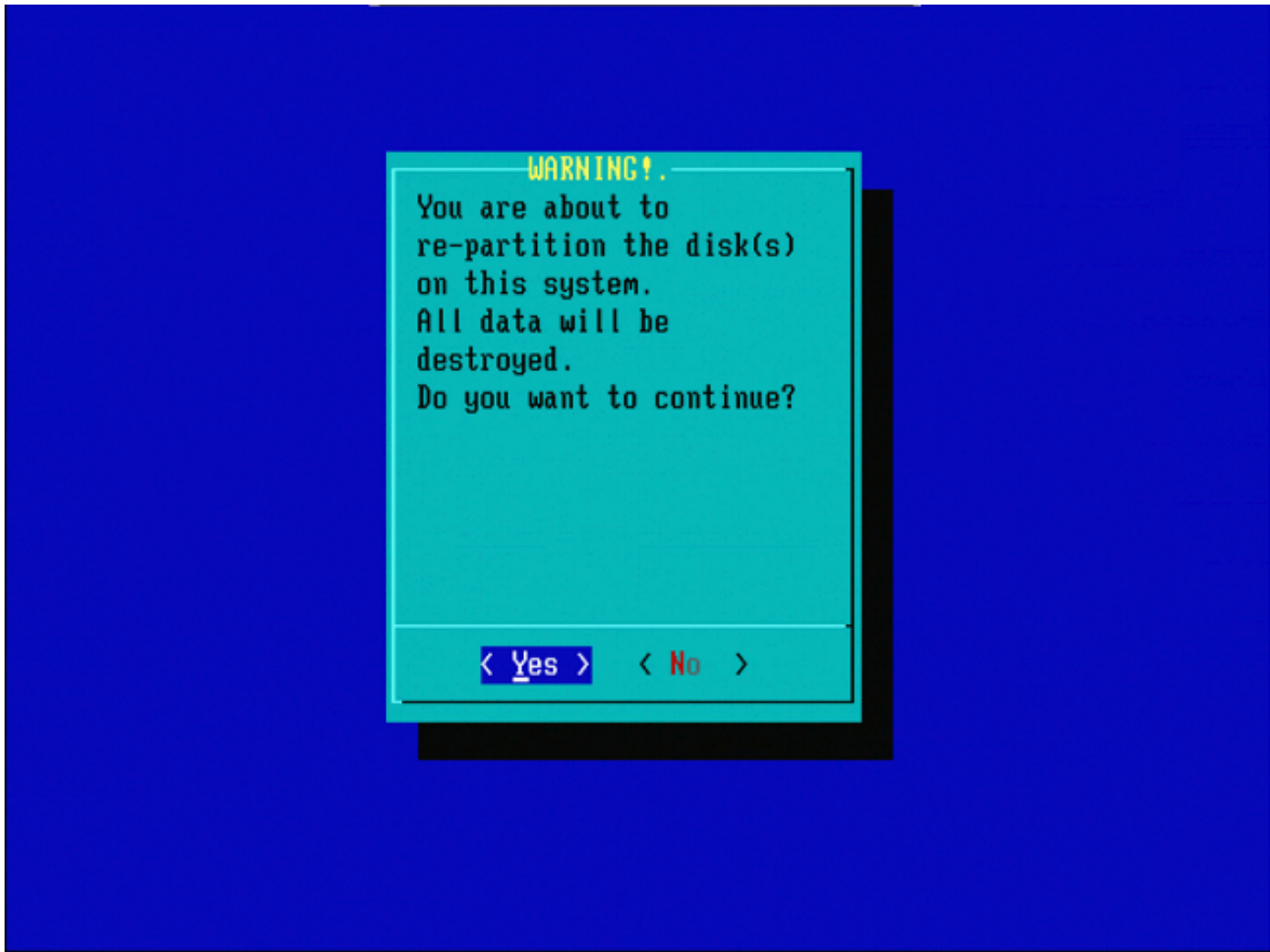


图 23





图 24

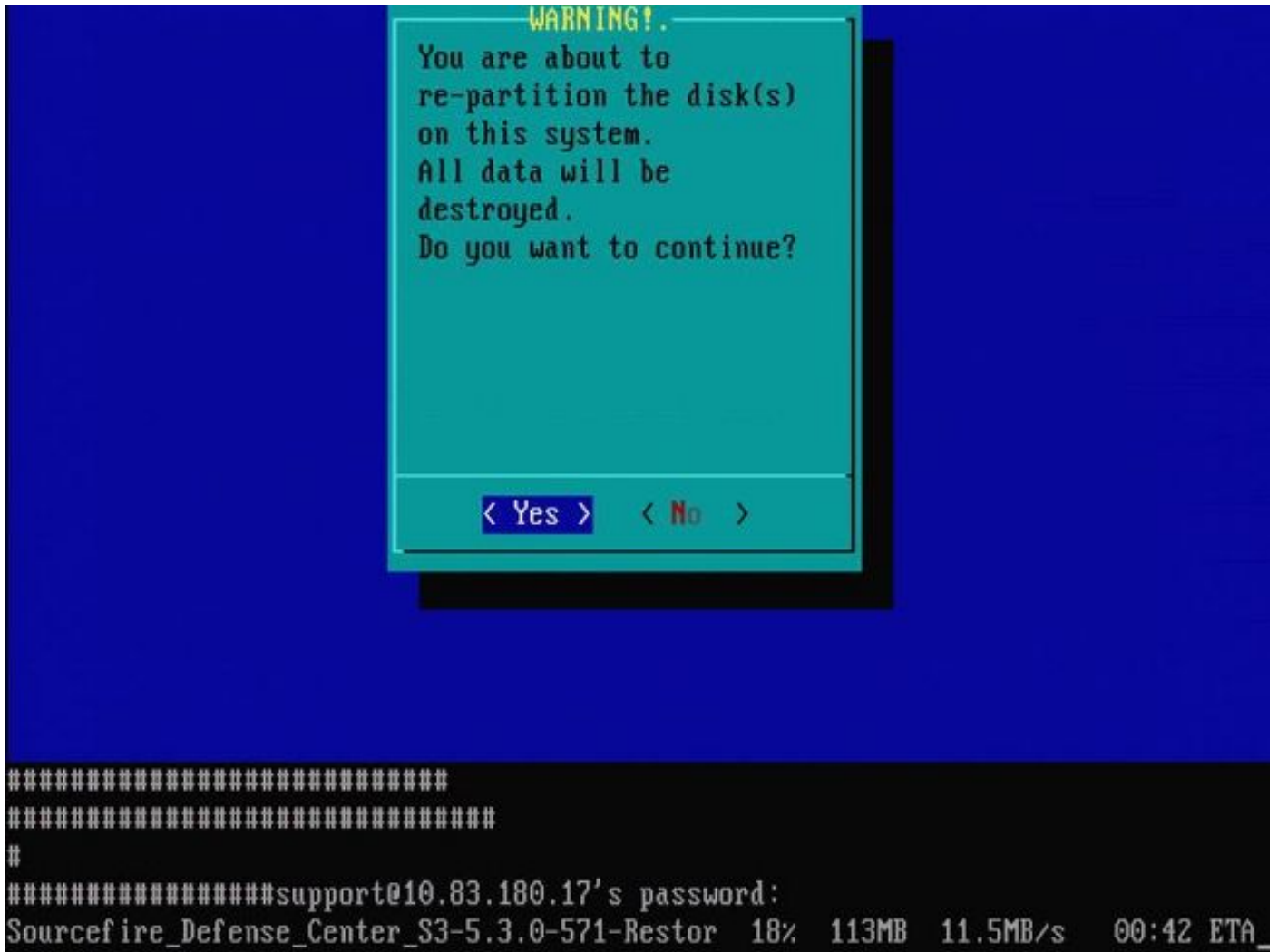


图 25




图 26

有关从不同主要软件版本重新映像的重要注意：如果您尝试重新映像之前运行不同主要软件版本的设备，例如您重新映像5.1 > 5.2、5.2 > 5.3、5.3 > 5.2等，则必须完成图1 - 26中描述的步骤两次。

1. 在如映像26所示的提示符上选择OK后，系统还原分区将刷新到新版本，设备将重新启动。
2. 重新启动后，您必须从头开始重新映像过程，并继续执行图27b至图31中所示的过程。

如果这是来自不同主要软件版本的第一次重新映像，则您会看到如映像27a所示的屏幕，然后是图31和图32。

---

 注意：如果您看到此屏幕，在“检查硬件”之后和“USB设备.....”之前，可能存在没有可见输出的延迟。此时不要按任何键，否则设备将重新引导至不可用状态，需要重新映像一次。

---

如果不是这种情况，您可以看到图27b至图32中的屏幕。

```
*****
Restore CD      Sourcefire Linux OS 5.1.0-57 x86_64
                Sourcefire 3D Sensor S3 5.1.0-365

        Checking Hardware

The USB device was successfully imaged. Reboot from the USB device to continue i
nallation...
#####

#####
The system will restart after you press enter.
-
```

图27a

\*\*\*\*\*

Restore CD    Sourcefire Linux OS 5.3.0-52 x86\_64  
              Sourcefire Defense Center S3 5.3.0-571

Checking Hardware

####

This CD will restore your Defense Center S3  
to its original factory state. All data will be destroyed  
on the appliance.

Restore the system? (yes/no): yes

图27b

\*\*\*\*\*

Restore CD    Sourcefire Linux OS 5.3.0-52 x86\_64  
              Sourcefire Defense Center S3 5.3.0-571

### Checking Hardware

####

This CD will restore your Defense Center S3  
to its original factory state. All data will be destroyed  
on the appliance.

Restore the system? (yes/no): yes  
During the restore process, the license file and basic  
network settings are preserved. These files can also be  
reset to factory settings

Delete license and network settings? (yes/no): no

图 28

\*\*\*\*\*

Restore CD    Sourcefire Linux OS 5.3.0-52 x86\_64  
              Sourcefire Defense Center S3 5.3.0-571

### Checking Hardware

####

This CD will restore your Defense Center S3 to its original factory state. All data will be destroyed on the appliance.

Restore the system? (yes/no): yes  
During the restore process, the license file and basic network settings are preserved. These files can also be reset to factory settings

Delete license and network settings? (yes/no): no

\*\*\*\*\*

THIS IS YOUR FINAL WARNING. ANSWERING YES WILL REMOVE ALL FILES FROM THIS DEFENSE CENTER S3.

\*\*\*\*\*

Are you sure? (yes/no): yes

图 29







图 31



图 32

## Cisco Firepower管理中心1000、2500和4500

在FMC 1000、2500和4500上，选项有所不同。使用KVM交换机或CIMC，在设备启动时，系统会显示以下选项：

- 1 - Cisco Firepower管理控制台VGA模式
- 2 - Cisco Firepower管理控制台串行
- 3 - Cisco Firepower管理控制台系统还原模式
- 4 - Cisco Firepower管理控制台密码恢复模式

如果要使用UI进入恢复模式，请选择选项“Cisco Firepower管理控制台系统恢复模式”(选项3)，然后选择“Cisco Firepower管理控制台系统恢复VGA模式”(选项1)

```
Please wait, preparing to boot.. .....
.....Config file:
TIMEOUT=5
DEFAULT=VGA
VERSION=6.3.0
root=/dev/sda3

1(*) - Cisco Firepower Management Console 6.3.0 VGA Mode
2 - Cisco Firepower Management Console 6.3.0 Serial Mode
3 - Cisco Firepower Management Console System Restore Mode
4 - Cisco Firepower Management Console Password Restore Mode
Enter selection [1]: 3
Option 3: 'Cisco Firepower Management Console System Restore Mode' selected ... running
Config file:
TIMEOUT=5
DEFAULT=VGA
VERSION=System Restore
initrd=install.img
NO_RESTORE

1(*) - Cisco Firepower Management Console System Restore VGA Mode
2 - Cisco Firepower Management Console System Restore Serial Mode
Enter selection [1]: 1
Option 1: 'Cisco Firepower Management Console System Restore VGA Mode' selected ... running
EFI stub: UEFI Secure Boot is enabled.
```

图 33

该过程的其余部分与其他FMC设备上的相同。

## 故障排除

### 未列出System\_Restore LILO菜单选项

FireSIGHT管理中心和FirePOWER 7000和8000系列设备具有包含重新映像系统的集成闪存驱动器。如果“System\_Restore”选项未列在LILO(Linux Loader)启动菜单中，仍可以访问此驱动器以完成重新映像。

#### 7010、7020和7030设备

如果使用70XX系列设备，请完成以下步骤以选择启动设备：

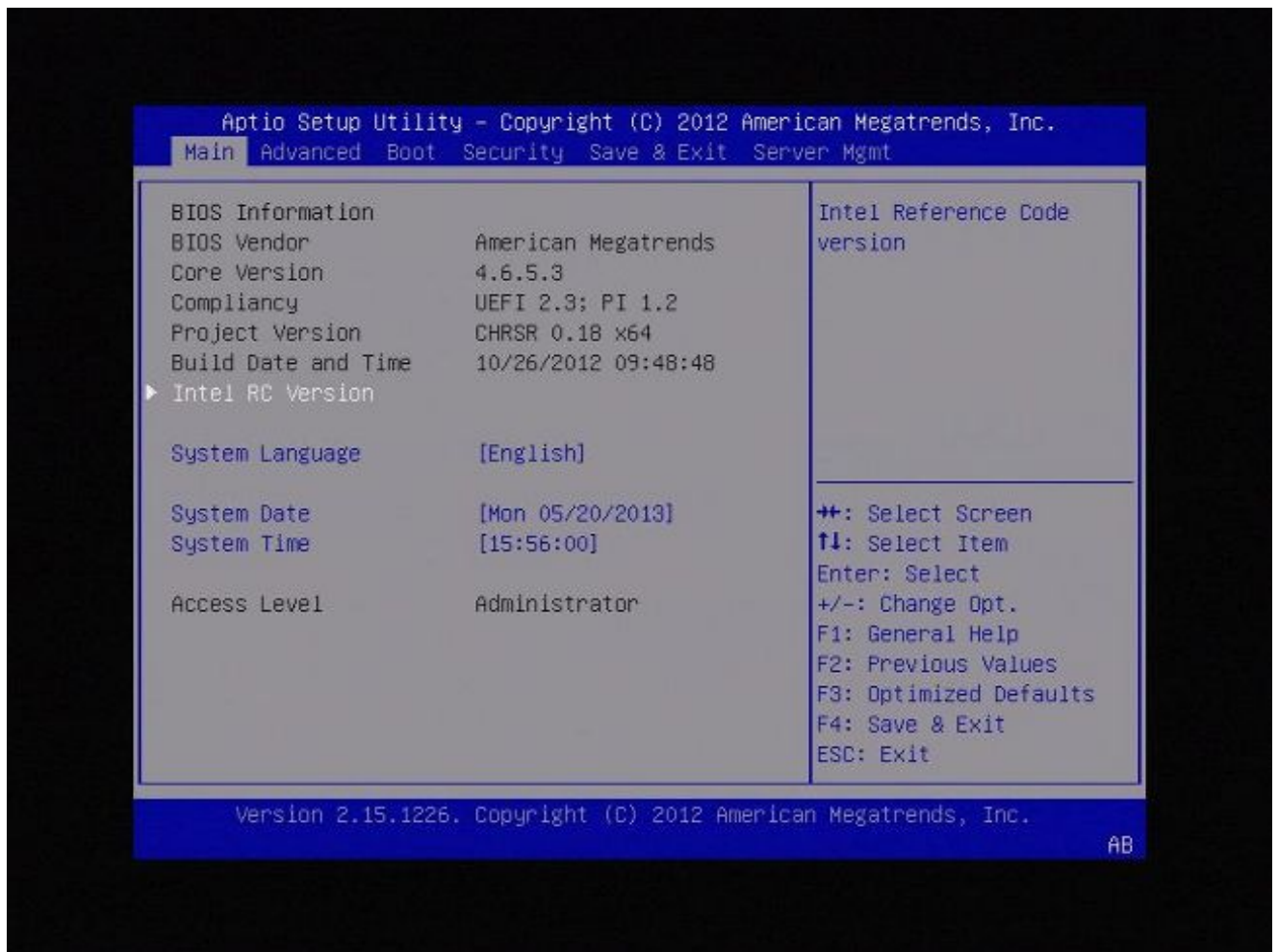
1. 正常关闭设备电源。
2. 在设备启动时打开设备电源，并重复按Delete键，以访问启动设备选择屏幕。请在此处查看图像：



Version 2.15.1226. Copyright (C) 2012 American Megatrends, Inc.  
BIOS Date: 10/26/2012 09:48:48 Ver: CHRSR018  
Press <DEL> or <ESC> to enter setup.

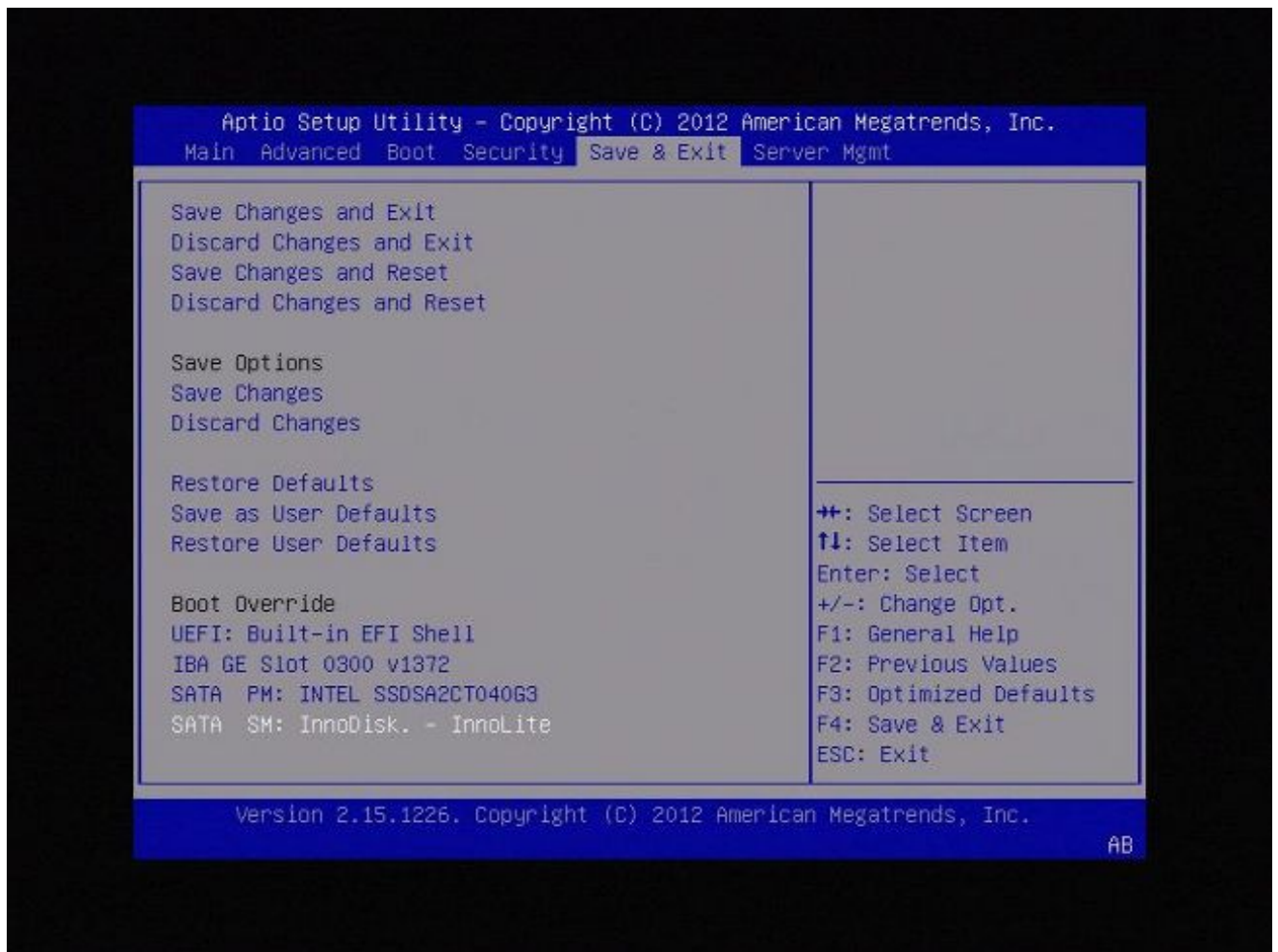
B2

图A1



图A2

3. 使用向右箭头键选择Save & Exit选项卡。在此选项卡上，使用向下箭头键选择SATA SM: InnoDisk。 - InnoLite并按Enter键。



图A3

4. 如果使用键盘和显示器，请选择选项0。

SYS LINUX 3.35 2007-01-28 EBIOS Copyright (C) 1994-2007 H. Peter Anvin

Welcome to the **Sourcefire** Linux Operating System

- 0. Load with standard console
- 1. Load with serial console
- 2. Load legacy installer standard
- 3. Load legacy installer serial

boot: 0\_

图A4



图A5

## 7110和7120设备

如果使用71XX系列设备，请完成以下步骤以选择启动设备：

1. 正常关闭设备电源。
2. 打开设备电源，并在设备启动时重复按F11键，以访问启动设备选择屏幕。请参阅此处显示的图像：





American  
Megatrends

www.ami.com

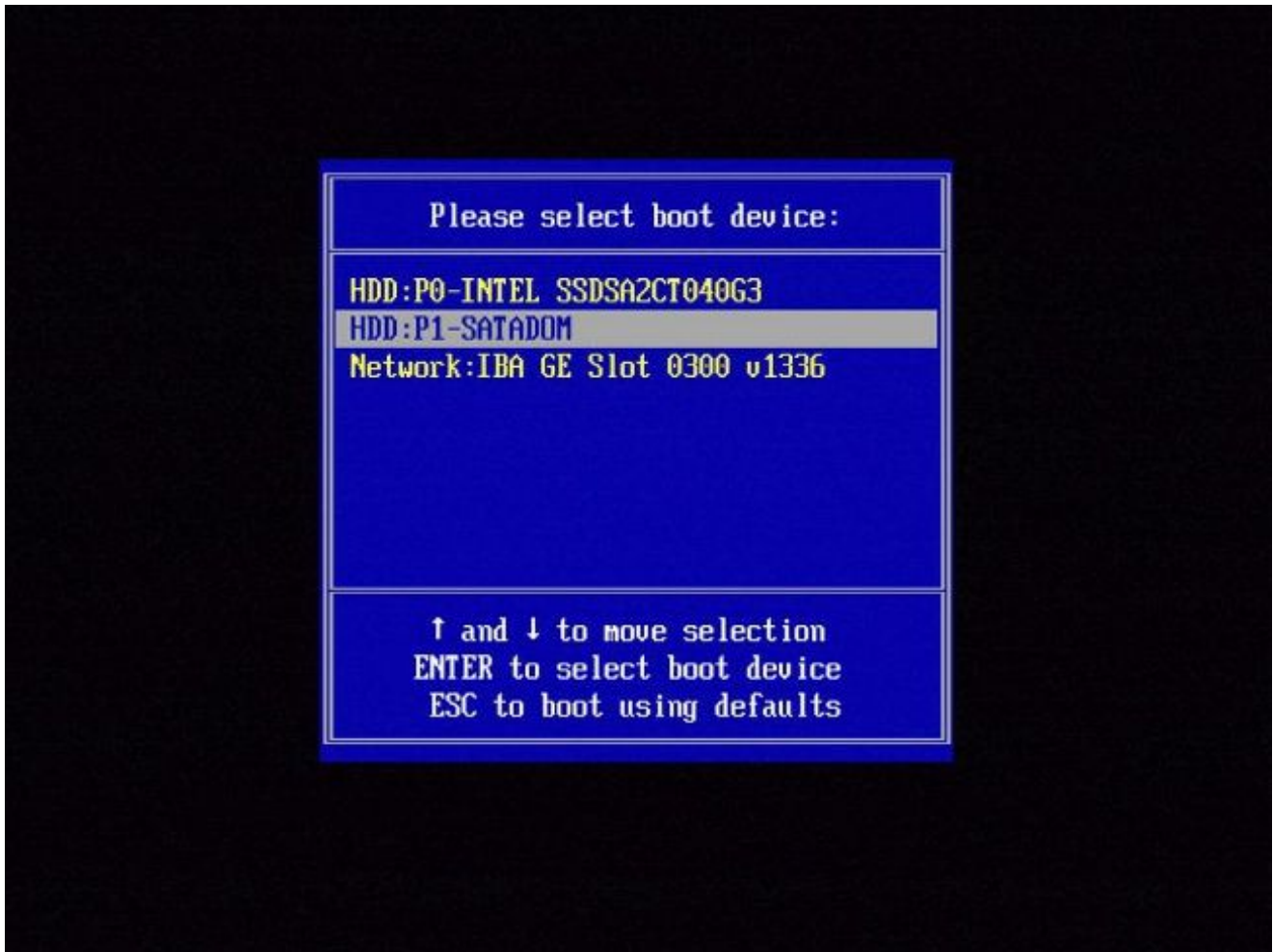
AMIBIOS (C) 2006 American Megatrends, Inc.  
Aquila BIOS Version:AQNIS093 Date:11/21/2011  
CPU : Intel(R) Xeon(R) CPU X3430 @ 2.40GHz  
Speed : 2.40 GHz

Press DEL to run Setup (F4 on Remote Keyboard)  
Press F12 if you want to boot from the network  
Press F11 for BBS POPUP (F3 on Remote Keyboard)  
The IMC is operating with DDR3 1333MHz, 9 CAS Latency  
DRAM Timings: Tras:24/Trp:9/Trcd:9/Twr:10/Trfc:107/Twtr:5/Trrd:4/Trtp  
BMC Initializing Virtual USB Device .. Done  
Initializing USB Controllers ..

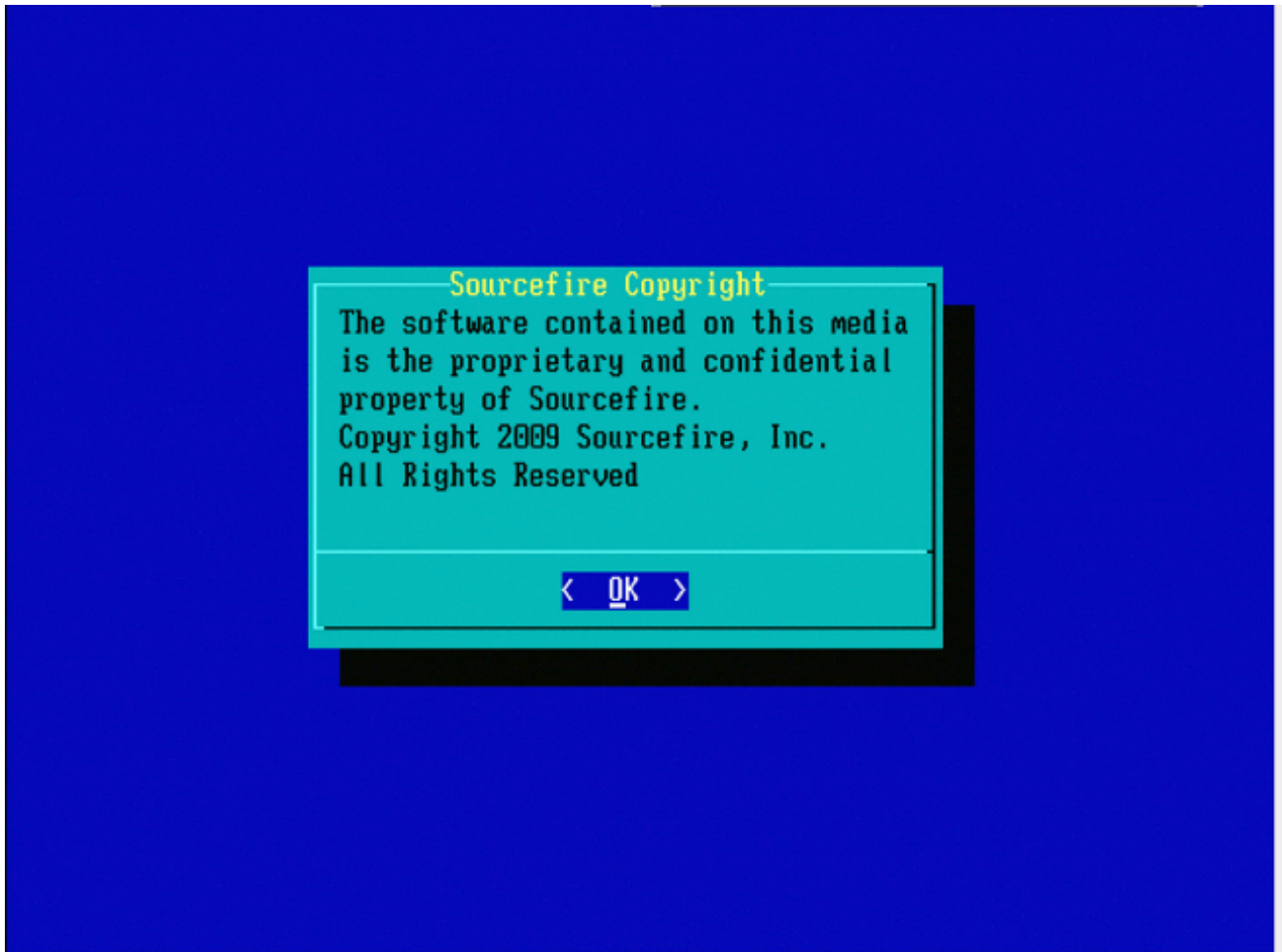
(C) American Megatrends, Inc.  
66-0100-000001-00101111-112111-LfdHvdImc-AQNIS093-Y2KC

图B1

3. 选择选项HDD:P1-SATADOM并按Enter以引导至System\_Restore分区。



图B2



图B3

8000系列设备或管理中心型号FS750、FS1500或FS3500

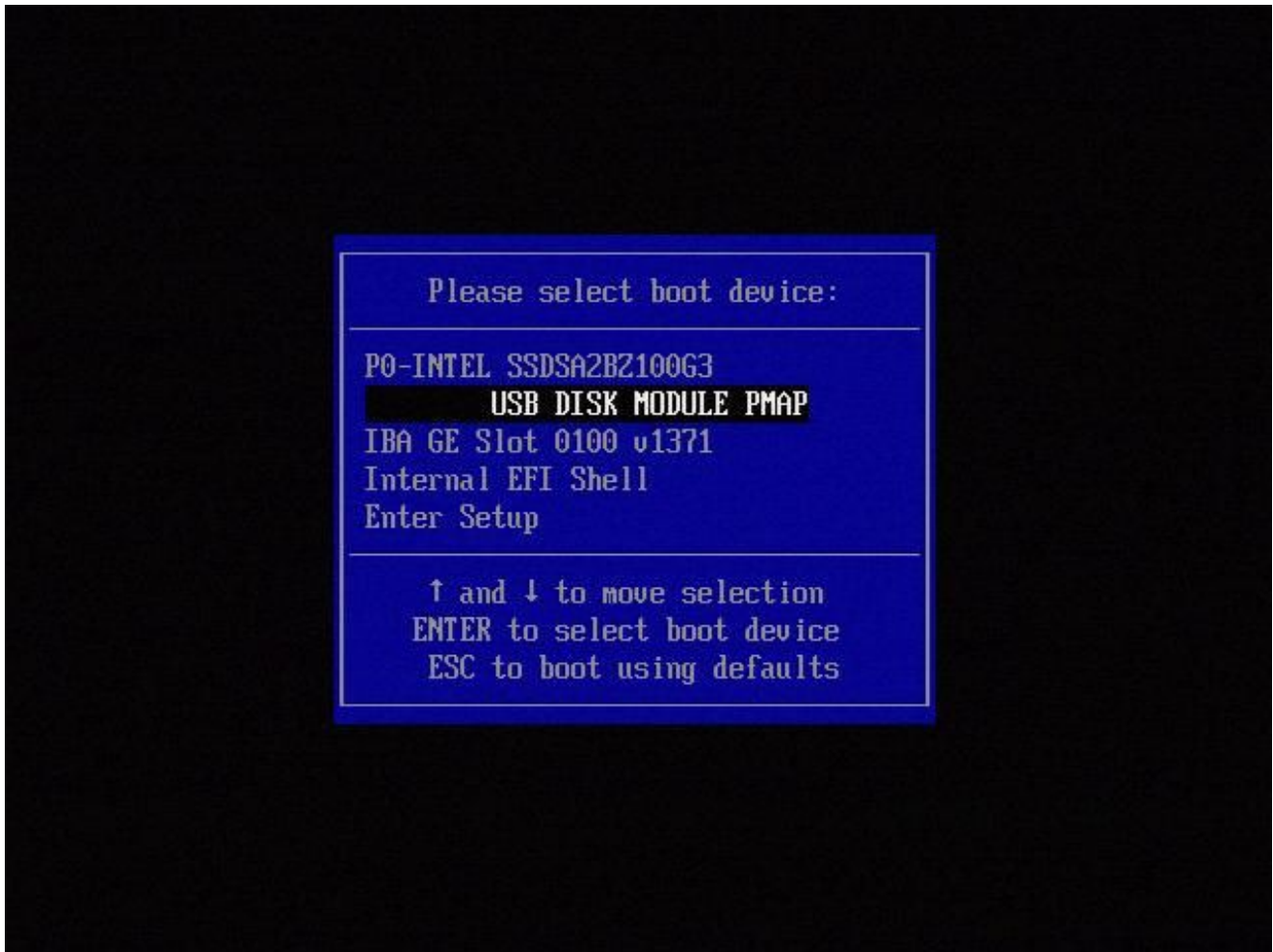
如果使用8000系列设备或管理中心型号FS750、FS1500或FS3500，请完成以下步骤以选择引导设备：

1. 正常关闭设备电源。
2. 在设备启动时打开设备电源，并重复按F6键，以便访问启动设备选择屏幕。请参阅此处显示的图像：

Version 1.23.1114. Copyright (C) 2010 American Megatrends, Inc.  
Press <F2> to enter setup, <F6> Boot Menu, <F12> Network Boot

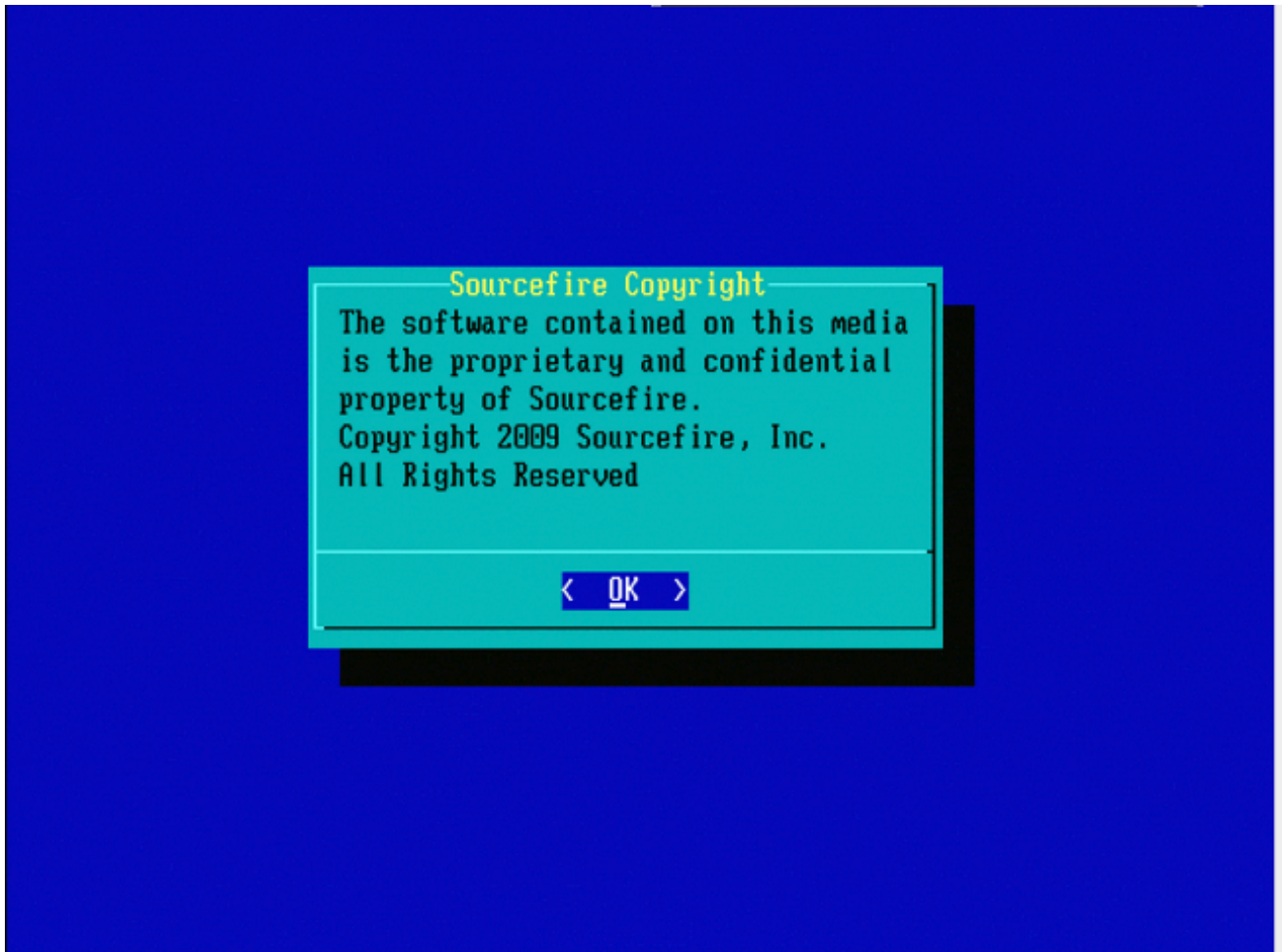
图C1

3. 选择USB选项。



图C2

4. 设备从System\_Restore分区启动并显示System\_Restore菜单。



图C3

## 型号FMC1000、FMC2500、FMC4500 ( 基于M4的FMC ) 的系统恢复

 注意：对于FMC4500，此型号具有不同的启动菜单，更多详细信息在下一[链接](#)中

对于以下型号，选择系统还原的提示显示不同：FMC1000、FMC2500、FMC4500

1. 在启动过程中，您可以看到此屏幕5秒：

```
Please wait, preparing to boot.. .....
.....Config file:
TIMEOUT=5
DEFAULT=VGA
VERSION=6.2.2
root=/dev/sda3

1(*) - Cisco Firepower Management Console 6.2.2 VGA Mode
2 - Cisco Firepower Management Console 6.2.2 Serial Mode
3 - Cisco Firepower Management Console System Restore Mode
4 - Cisco Firepower Management Console Password Restore Mode
Enter selection [1]:
```

图D1

2. 选择System Restore ( 系统还原 ) 选项#3在本例中是如此)。

```
1(*) - Cisco Firepower Management Console 6.2.2 VGA Mode
2 - Cisco Firepower Management Console 6.2.2 Serial Mode
3 - Cisco Firepower Management Console System Restore Mode
4 - Cisco Firepower Management Console Password Restore Mode
Enter selection [1]: 3
Option 3: 'Cisco Firepower Management Console System Restore Mode' selected ...
running
Config file:
TIMEOUT=5
DEFAULT=VGA
VERSION=System Restore
initrd=install.img
NO_RESTORE

1(*) - Cisco Firepower Management Console System Restore VGA Mode
2 - Cisco Firepower Management Console System Restore Serial Mode
Enter selection [1]:
```

图D2

3. 选择系统还原的显示方法(#1情况下为VGA)

```
1(*) - Cisco Firepower Management Console System Restore VGA Mode
2 - Cisco Firepower Management Console System Restore Serial Mode
Enter selection [1]: 1
Option 1: 'Cisco Firepower Management Console System Restore VGA Mode' selected
... running
```

图D3

4. 然后，您到达图5所示的提示符，此过程继续正常进行。

### 未列出启动选项

引导至重新映像分区的选项可能未列在BIOS或引导菜单中。如果出现这种情况，包含重新映像系统的驱动器可能丢失或损坏。可能需要RMA。

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。