

重新映像FireSIGHT管理中心和FirePOWER裝置

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[重新映像流程](#)

[開始之前](#)

[重新映像流程概覽](#)

[Cisco Firepower Management Center 1000、2500和4500](#)

[疑難排解](#)

[未列出System Restore LILO選單選項](#)

[7010、7020和7030裝置](#)

[7110和7120裝置](#)

[8000系列裝置或管理中心型號FS750、FS1500或FS3500](#)

[型號FMC1000、FMC2500、FMC4500 \(基於M4的FMC\) 的系統還原](#)

[未列出啟動選項](#)

簡介

本檔案將以Cisco FireSIGHT管理中心(FMC)和FirePOWER裝置的重新映像程式的範例說明這些流程。

必要條件

需求

本文件沒有特定需求。

採用元件


本文中的資訊係根據以下軟體和硬體版本：

| 受管裝置 | FireSIGHT管理中心 可重新映像的軟體版本 | |
|-------------------------|--------------------------|----------|
| 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 Cisco AMP 7150 Cisco AMP 8150 | | 5.3或更高版本 |
|--|--|----------|


本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

重新映像流程


 注意：升級或重新映像FireSIGHT管理中心或FirePOWER裝置時，請勿插入USB儲存裝置或插入鍵盤、影片和滑鼠(KVM)交換機。

開始之前

1. 如果您計畫重新映像管理中心或獨立的Firepower裝置，建議在繼續之前備份您的裝置。
2. 識別感測器的型號，並使用「Components Used（已使用的元件）」部分中的型號清單驗證本指南是否正確。
3. 從思科支援網站下載您所需的軟體版本的適當安裝指南和磁碟映像。

 註：請勿重新命名.iso檔案


為映像服務：必須將.iso檔案複製到從裝置的管理網路可訪問的、運行SSH伺服器的主機。

 註：如果沒有其他SSH伺服器可用，則可以使用FMC進行此過程。

驗證iso的完整性：檔案的md5sum位於頁面的右側，用於使用md5sum實用程式進行驗證。

4. 安裝指南包含重新映像的逐步說明，還概述了重新映像處理的幾種方法。本文中提供的圖片可供參考。

重新映像流程概覽

 註：5.3版用於捕獲本文中顯示的影象。對於其他5.x版本，除了在圖中所示的版本號之外，重新映像過程完全相同。

```
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: _
```

圖1

```


          LILO 22.8  Boot Menu
-----
 3D-5.3.0
System_Restore

Hit any key to cancel timeout      --:--
Use +↑↓+ arrow keys to make selection
Enter choice & options, hit CR to boot

boot: 3D-5.3.0_
```

圖2 — 系統重新啟動時，按鍵盤上的箭頭鍵以停止倒計時，為下一幅螢幕選擇System_Restore選項

○

 註：如果System_Restore提示符未顯示，則必須更改引導順序以直接引導到恢復分割槽 (DOM)。有關詳細資訊，請參閱[缺少System_Restore LILO選單選項](#)。

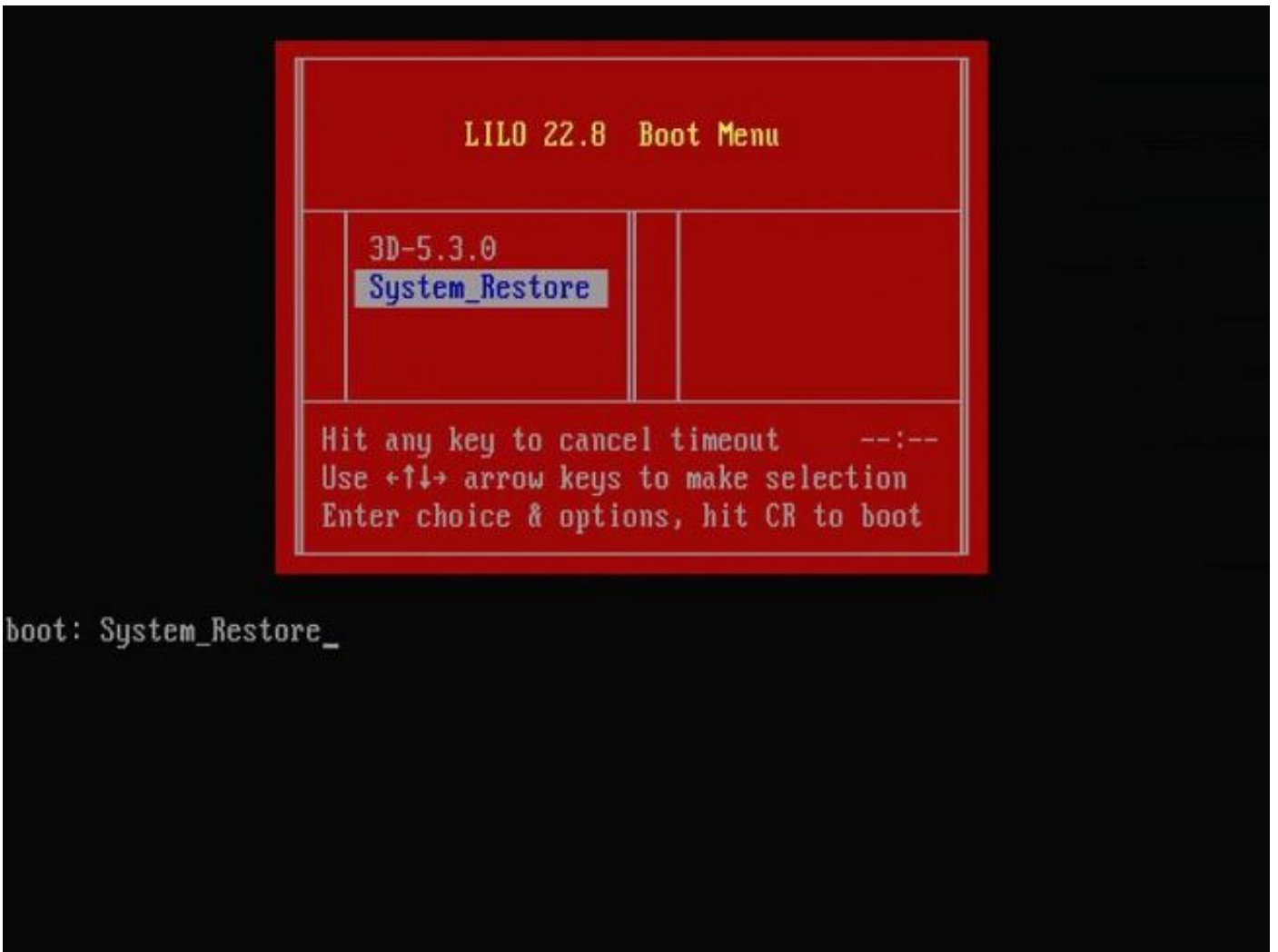


圖3


```
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.....
.....
```

圖4 — 如果您使用鍵盤和顯示器，請選擇選項0。

 註：有時會看到「Restore (還原)」選項的選單僅在僅連線控制檯時顯示 (鍵盤已拔出)。一旦選擇「恢復」選項，鍵盤就可以重新連線回來

Sourcefire Copyright

The software contained on this media
is the proprietary and confidential
property of Sourcefire.
Copyright 2009 Sourcefire, Inc.
All Rights Reserved

< OK >

圖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>

圖6

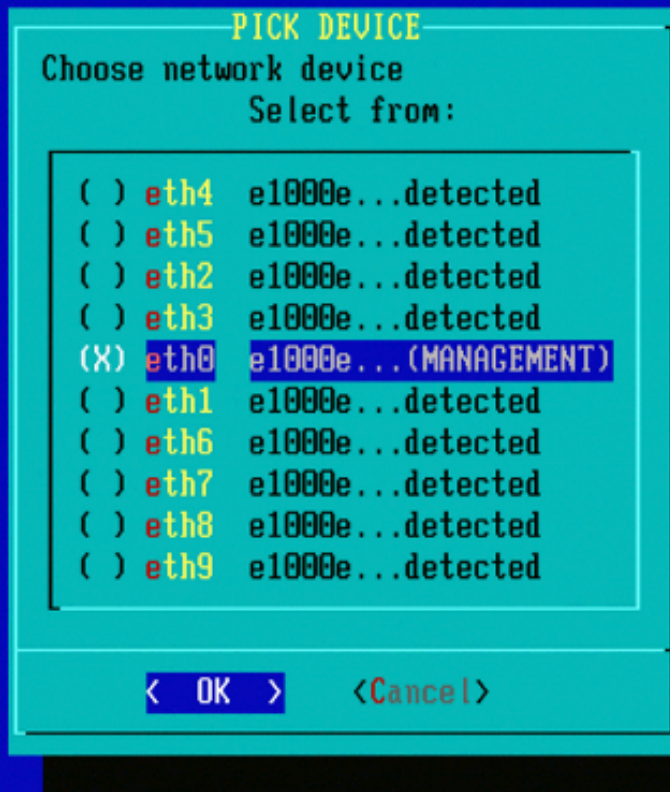


圖7 — 要選擇網路裝置，按空格鍵。

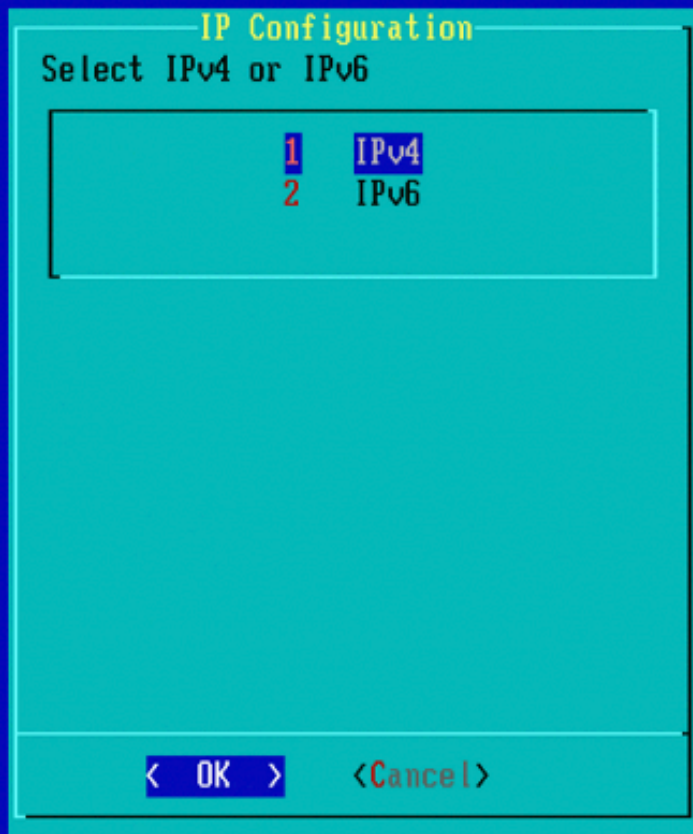


圖8



圖9

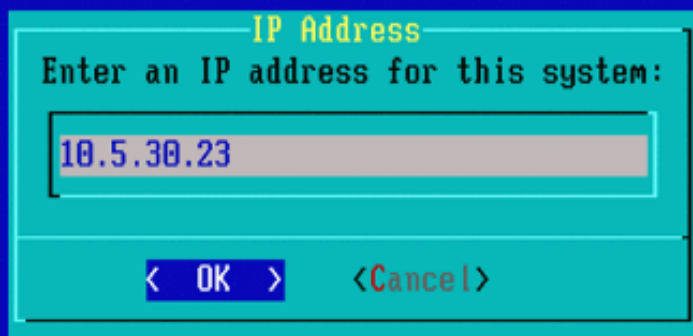


圖10

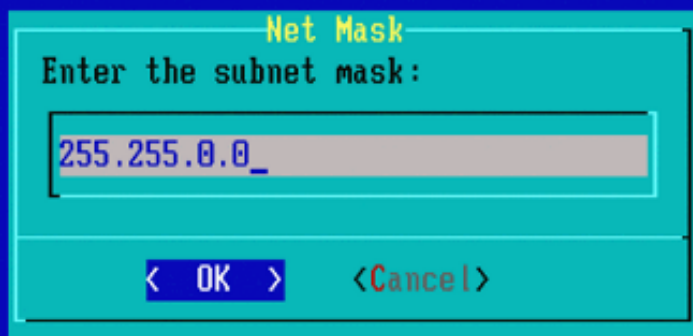


圖11

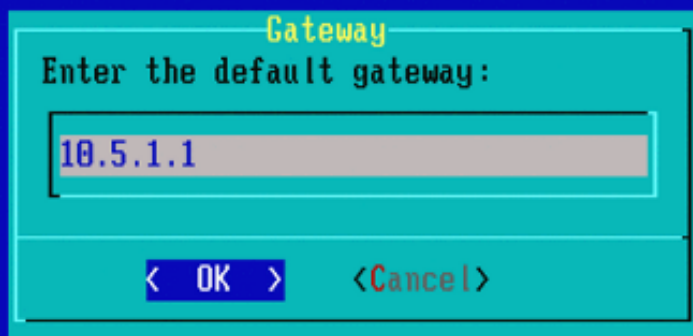


圖12

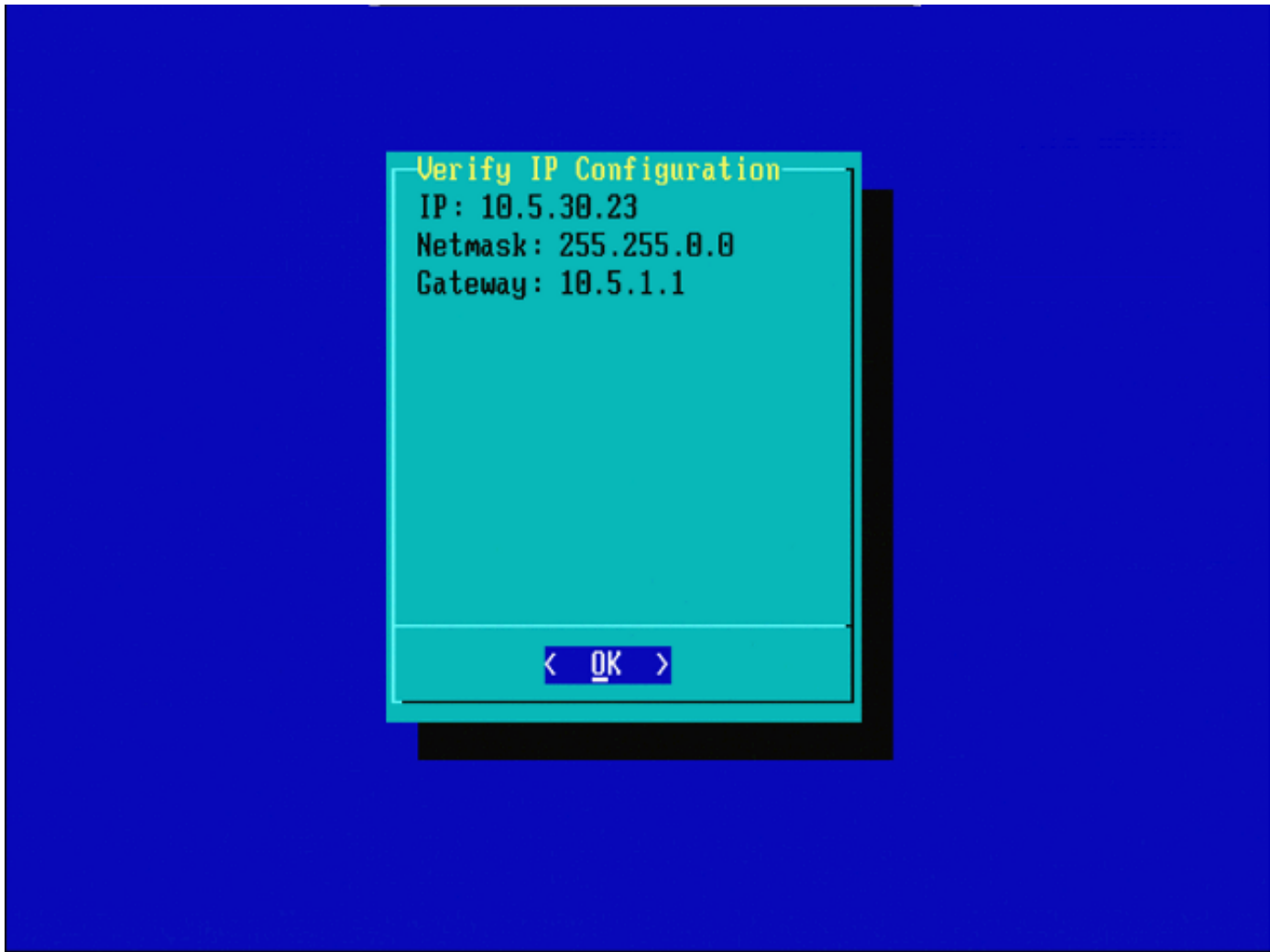


圖13

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>

圖 14



圖15 — 思科支援人員建議您使用安全複製(SCP)協定。

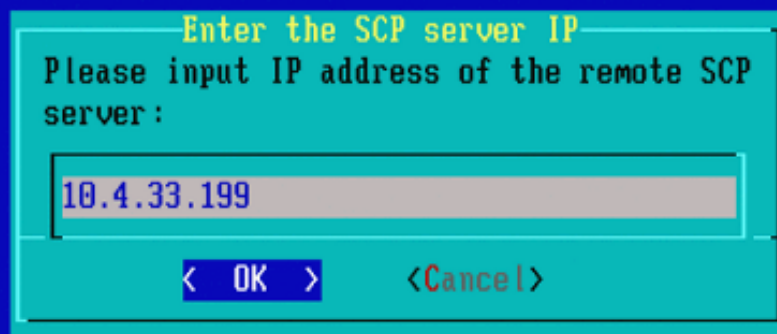



圖 16 — 可以使用FireSIGHT管理中心作為此步驟的SCP伺服器。繼續此過程，並使用管理中心的IP地址和憑據填充System Restore選單中的字段。更多詳細資訊，請參閱

安全複製(SCP)伺服器用於安全地傳輸檔案。如果 如果需要，可以將Sourcefire防禦中心(DC)用作SCP伺服器，將檔案傳輸到其他Sourcefire裝置。當需要將iso映像傳輸到Sourcefire裝置以進行重新映像時，當常規SCP伺服器無法訪問或不可用時，此命令非常有用。

步驟 1.從[Sourcefire支援門戶](#)將適當的.iso檔案下載到您的案頭。

步驟 2.使用SCP客戶端，將檔案從案頭複製到防禦中心。

 提示:SCP客戶端通常在Linux或Mac作業系統中可用。但是，在Windows作業系統中，您可能必須安裝第三方SCP客戶端軟體。Sourcefire不提供安裝任何特定SCP客戶端軟體的建議或支援。

下一個示例演示如何將Sourcefire .iso映像檔案從Linux系統的「下載」目錄複製到Sourcefire防禦中心的/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:請勿更改.iso檔案的名稱。重新映像期間可能會產生偵測檔案的問題。

現在，檔案被複製到防禦中心。您可以繼續對Sourcefire裝置進行重新映像處理。在重新映像時，如有必要，您可以提供DC的IP地址和使用者名稱，以及用以前的說明複製映像檔案的路徑。

 警告：完成重新映像後，您必須從防禦中心的/var/tmp目錄中移除.iso檔案，以減少磁碟空間的利用率。

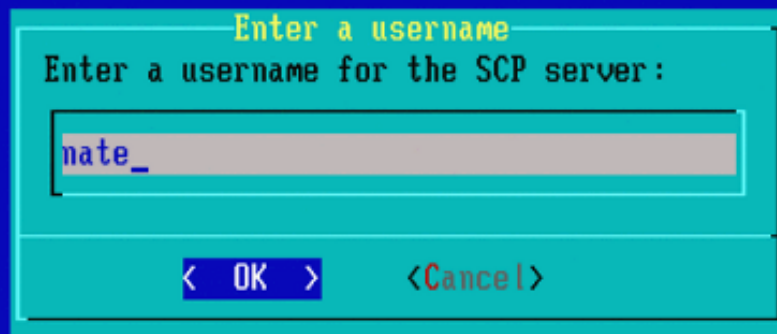


圖17

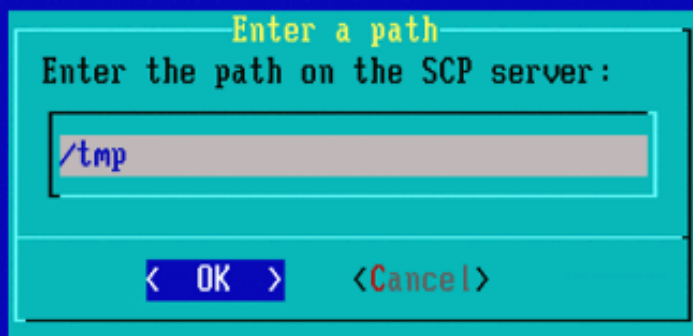


圖18

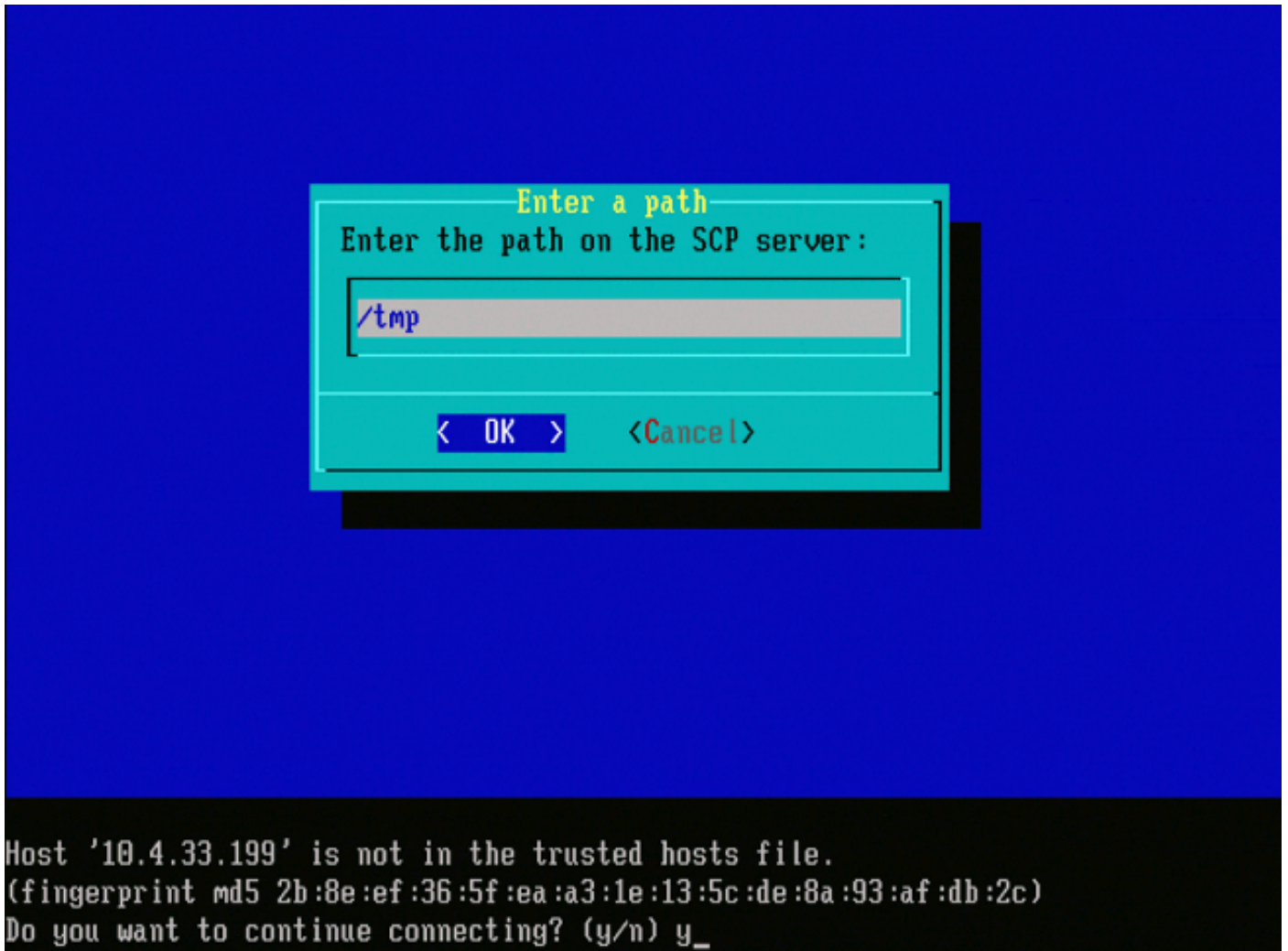



圖19

 注意：如果您此時收到連線錯誤而不是預期消息，請驗證與SSH伺服器的連線。

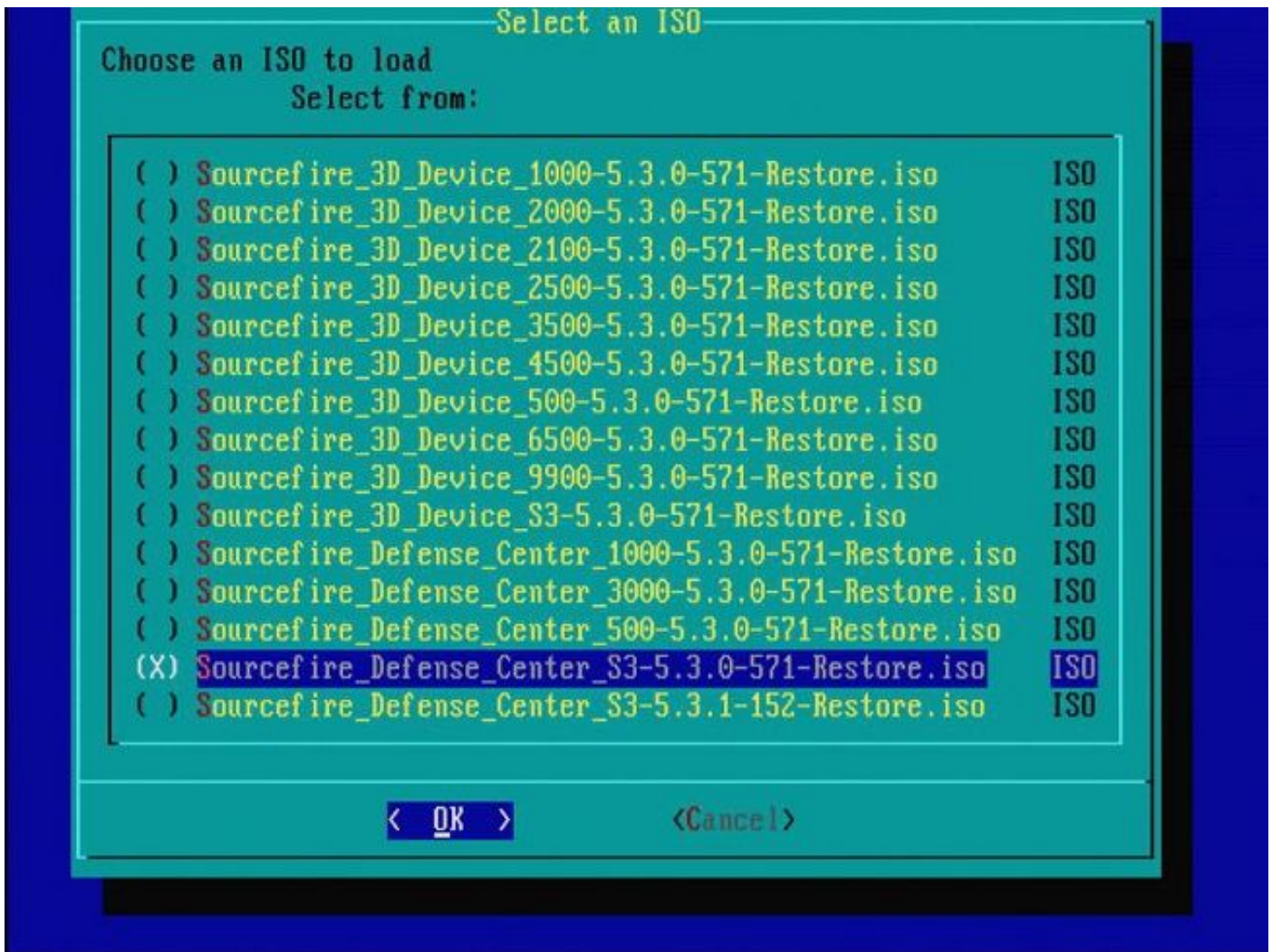



圖20 — 要選擇.iso影象，請按空格鍵。

 註：必須使用.iso檔案的預設檔名，否則在此步驟中可能檢測不到這些檔案。
錯誤：未找到ISO映像
在版本6.3中，ISO名稱約定已從Sourcefire_3D_Device_S3-<ver>-<build>-Restore.iso更改為Cisco_Firepower_NGIPS_Appliance-<ver>-<build>-Restore.iso。如果您遇到「未找到ISO映像」，請將ISO檔案重新命名為舊版檔名。將6.2.x或更舊版本重新映像到6.3.0或更高版本時，通常會發生這種情況。

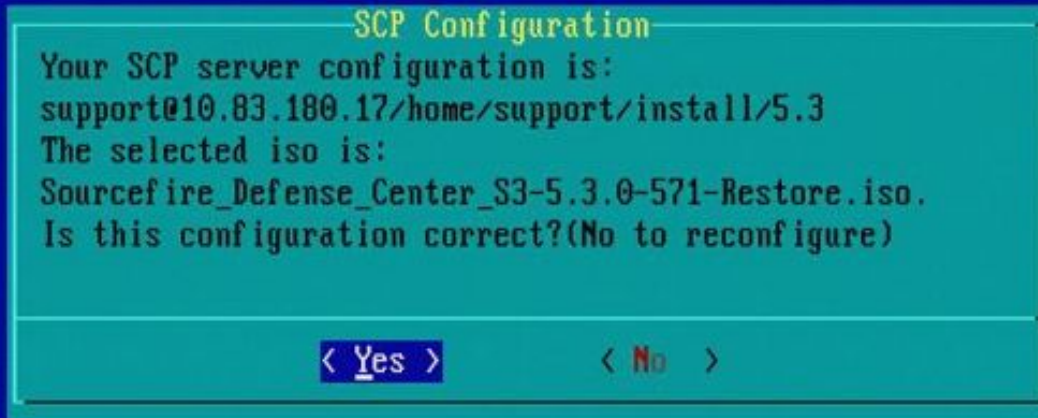


圖21

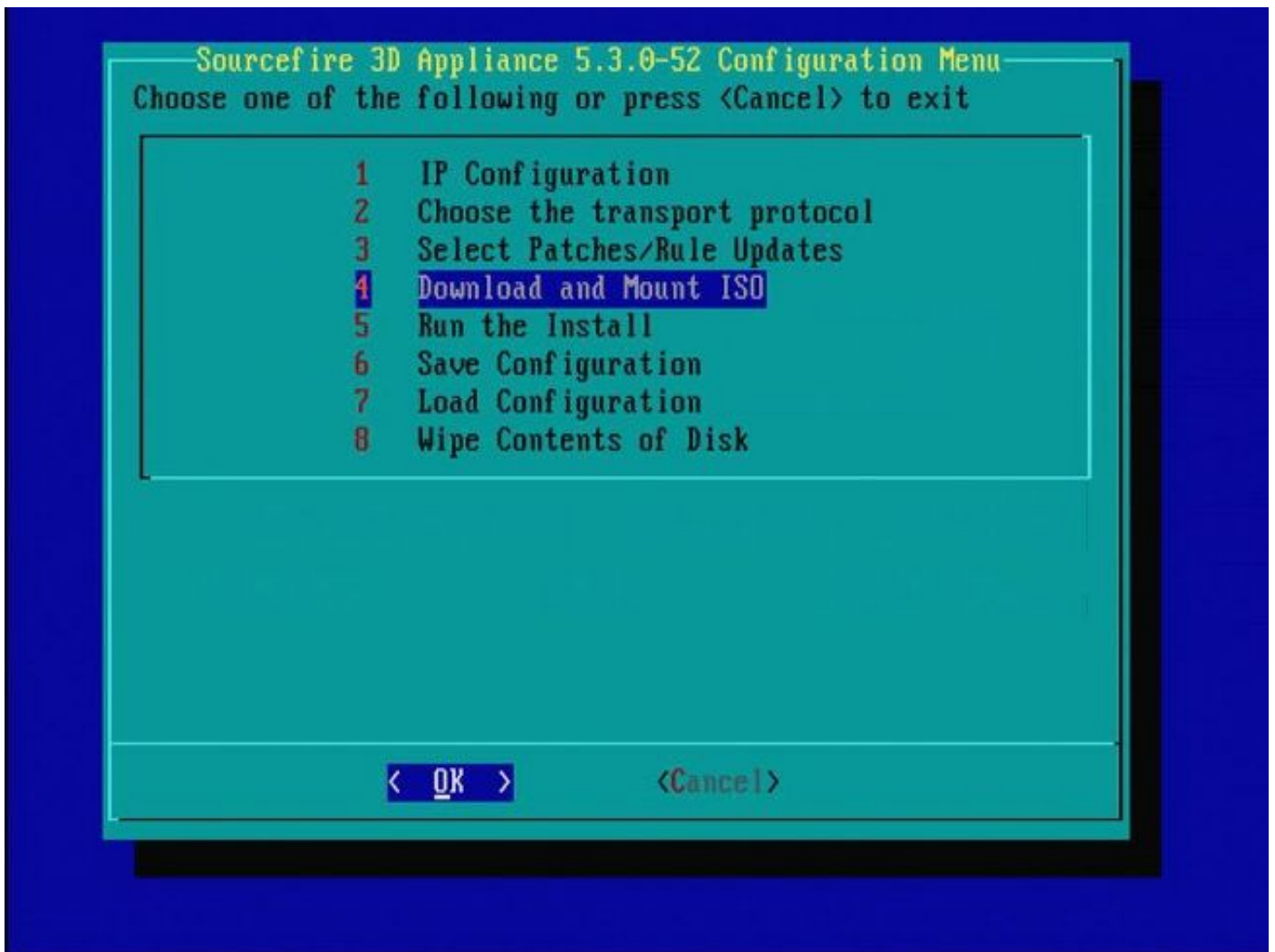


圖22 — 思科支援人員建議跳過此過程中的步驟3。重新映像完成後，即可安裝修補程式和Snort規則更新(SRU)。

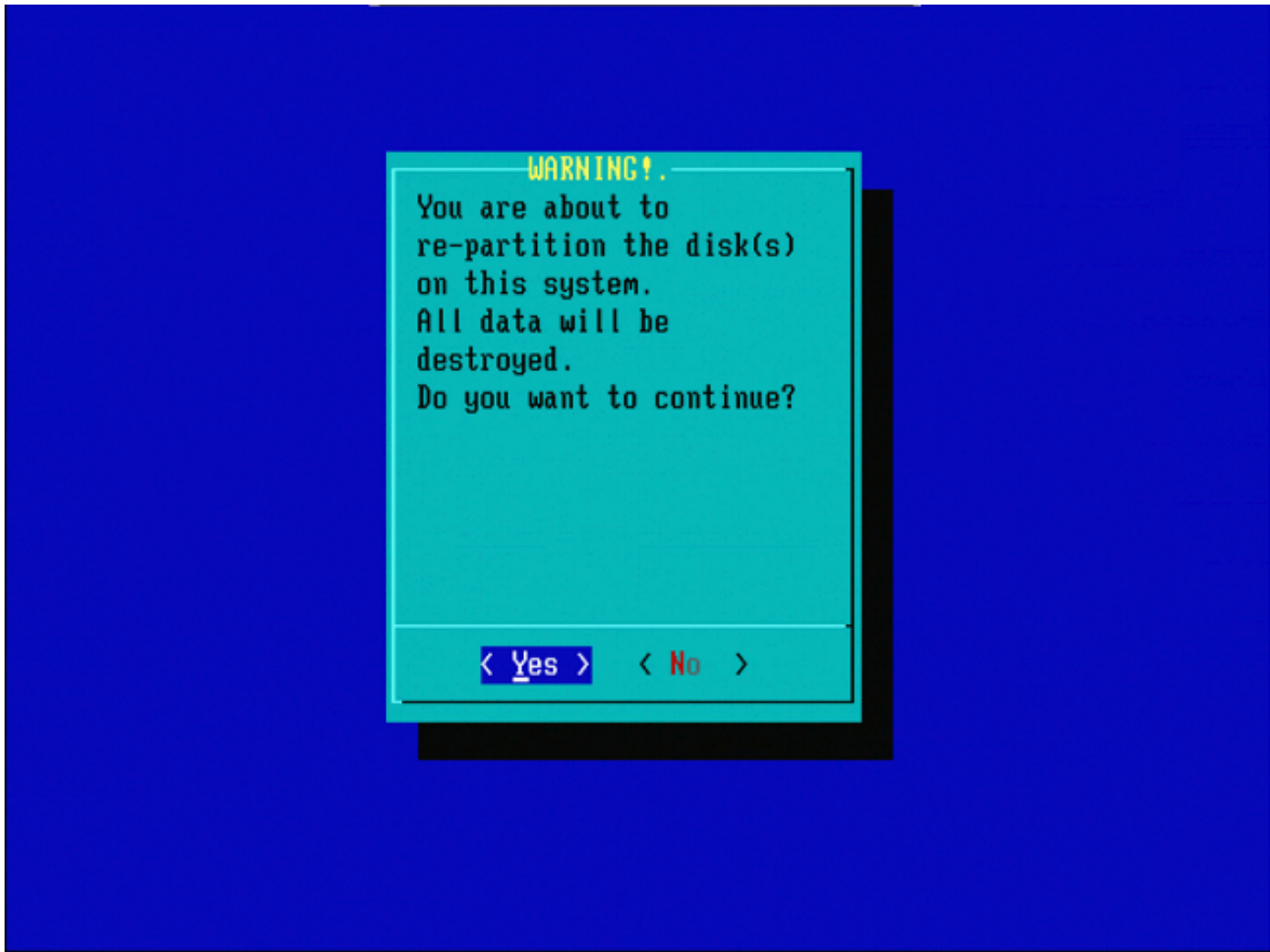


圖23

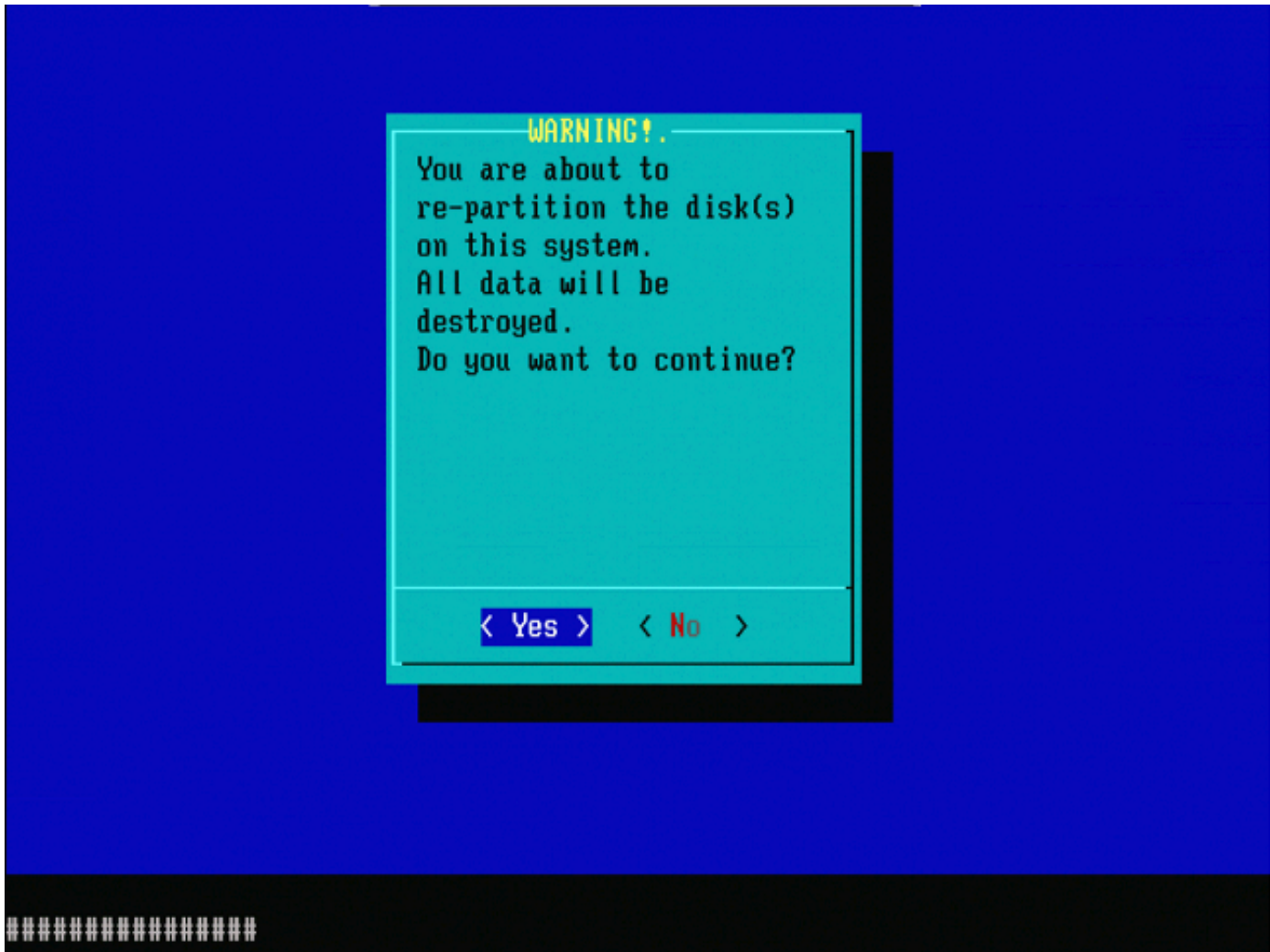


圖24

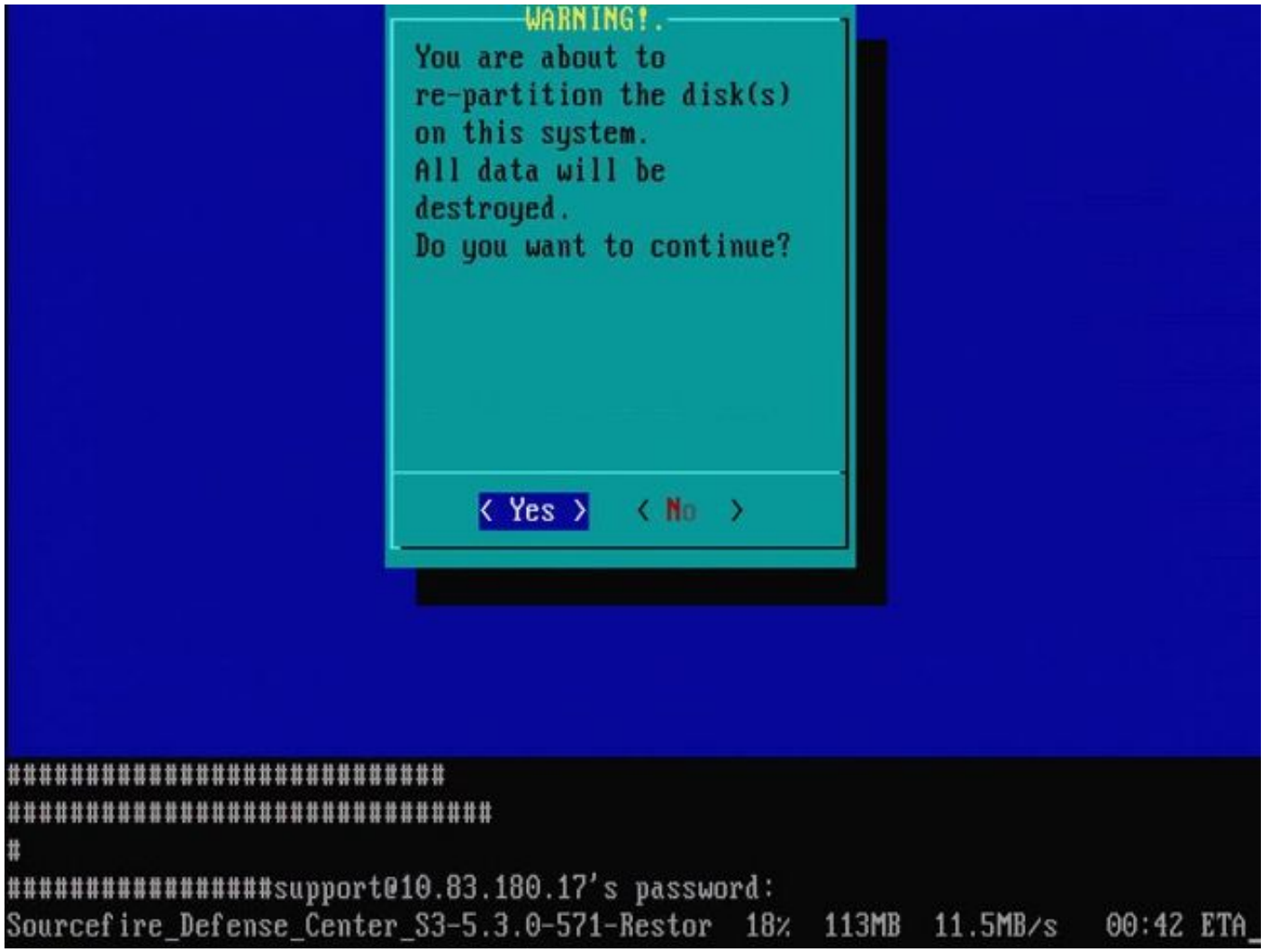


圖25



圖26

有關從不同主要軟體版本重新映像的重要註意：如果您嘗試重新映像以前運行不同主要軟體版本的裝置，例如重新映像5.1 > 5.2、5.2 > 5.3、5.3 > 5.2等，則必須完成圖1 - 26中描述的步驟兩次。

1. 在提示符下選擇OK (如圖26所示) 後，系統還原分割槽將刷新到新版本，裝置將重新啟動。
2. 重新引導後，您必須從頭開始重新映像過程，並繼續執行圖27b至31中所示的過程。

如果這是從其他主要軟體版本進行的第一次重新映像，則您將看到如下所示的螢幕：映像27a，然後圖31和圖32。

⚠ 注意：如果您看到此螢幕，在「檢查硬體」之後和「USB裝置.....」之前可能會出現延遲，並且輸出不可見。此時不要按任何鍵，否則裝置將重新啟動至不可用狀態，需要重新映像一次。

如果不是，您可以看到圖27b至圖32中的螢幕。

```
*****
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.
-
```

圖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

圖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

圖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

圖29

Restore CD Sourcefire Linux OS 5.3.0-52 x86_64
 Sourcefire Defense Center S3 5.3.0-571

(1) Preparing Disk

#####

(2) Installing System

#####

圖30



圖31



圖32

Cisco Firepower Management Center 1000、2500和4500

FMC 1000、2500和4500上的選項不同。使用KVM交換機或CIMC，在裝置啟動時，將顯示以下選項：

- 1 - Cisco Firepower管理控制檯VGA模式
- 2 - Cisco Firepower管理控制檯串列
- 3 - Cisco Firepower管理控制檯系統還原模式
- 4 - Cisco Firepower管理控制檯密碼恢復模式

如果要使用UI進入還原模式，請選擇選項「Cisco Firepower Management Console System Restore Mode」(選項3)，然後選擇「Cisco Firepower Management Console System Restore VGA Mode」(選項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.

```

圖33

該過程的其餘部分與其他FMC裝置上的相同。

疑難排解

未列出System_Restore LILO選單選項

FireSIGHT管理中心和FirePOWER 7000和8000系列裝置具有包含重新映像系統的整合快閃記憶體驅動器。如果LILO(Linux Loader)啟動選單中沒有「System_Restore」選項，仍可以訪問此驅動器以完成重新映像。

7010、7020和7030裝置

如果使用70XX系列裝置，請完成以下步驟以選擇啟動裝置：

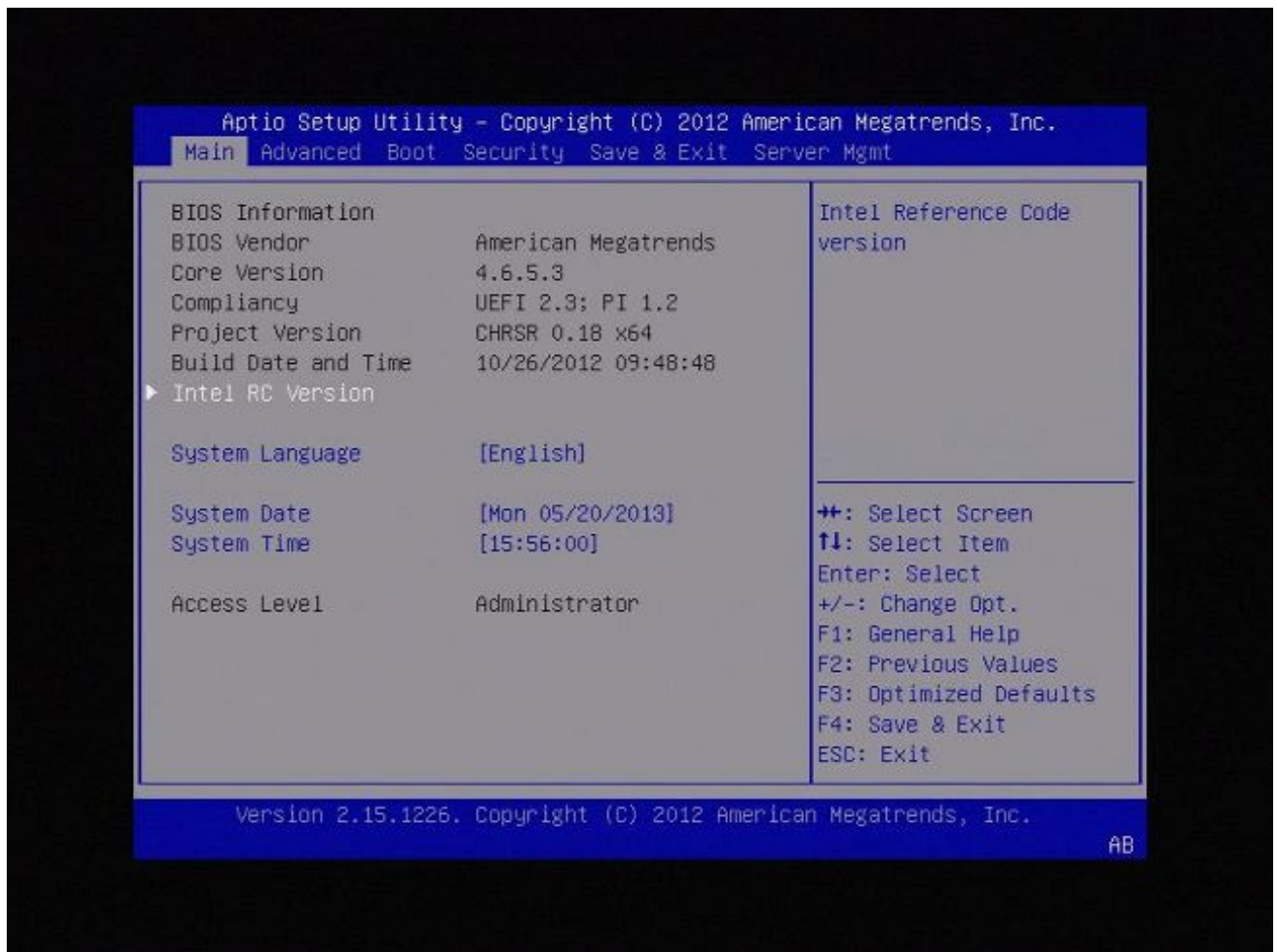
1. 正常關閉裝置電源。
2. 在裝置啟動時開啟裝置電源，並重複按Delete鍵，以訪問啟動裝置選擇螢幕。請參閱以下圖示：



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

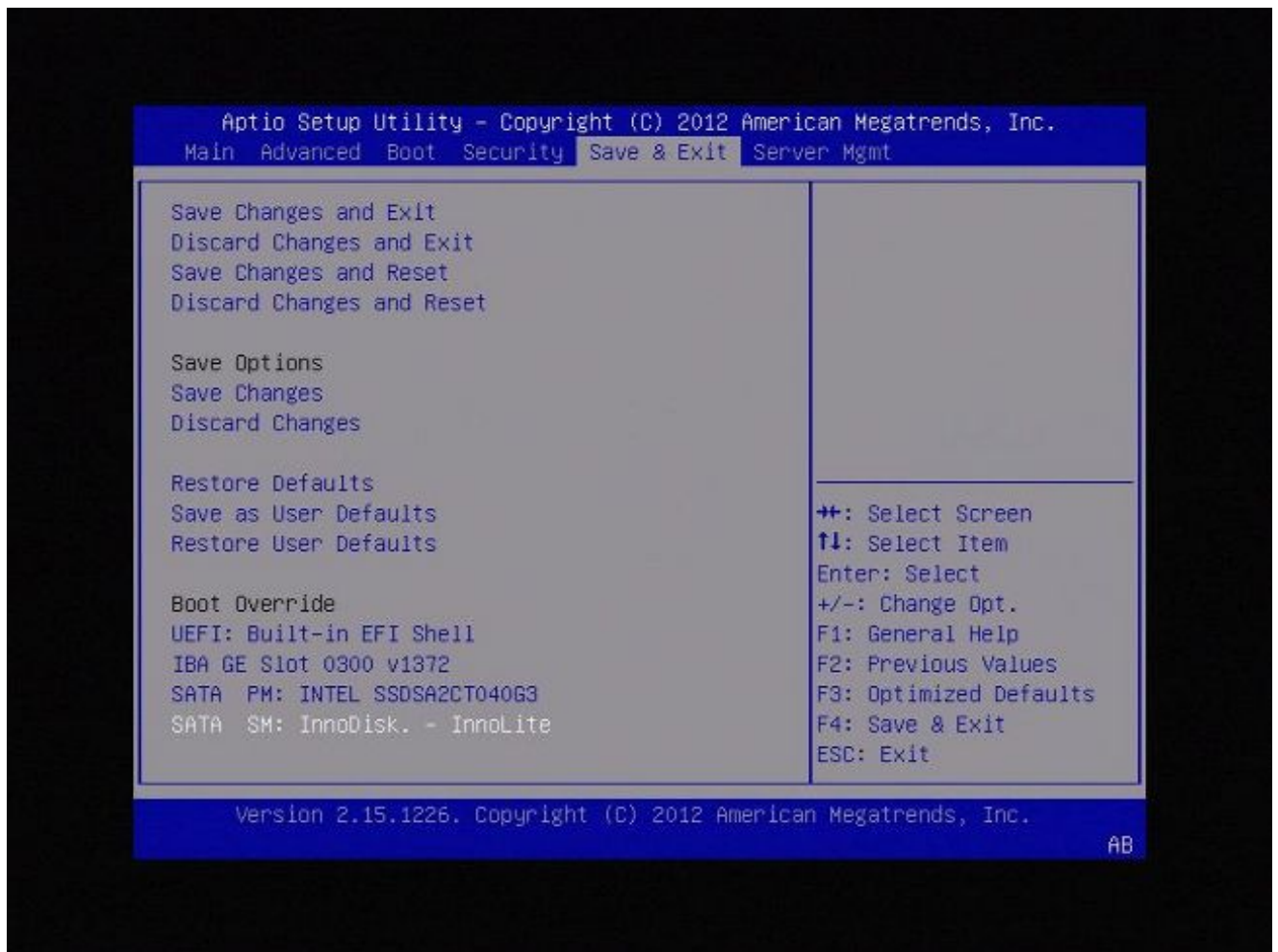
B2

圖A1



圖A2

3. 使用右箭頭鍵選擇「Save & Exit」頁籤。在此頁籤上，使用向下箭頭鍵選擇SATA SM: InnoDisk。 - InnoLite並按Enter鍵。



圖A3

4. 如果使用鍵盤和顯示器，請選擇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_

圖A4



圖A5

7110和7120裝置

如果使用71XX系列裝置，請完成以下步驟以選擇啟動裝置：

1. 正常關閉裝置電源。
2. 在裝置啟動時開啟裝置電源，並重複按F11鍵，以訪問啟動裝置選擇螢幕。請參閱此處顯示的圖片：



American Megatrends

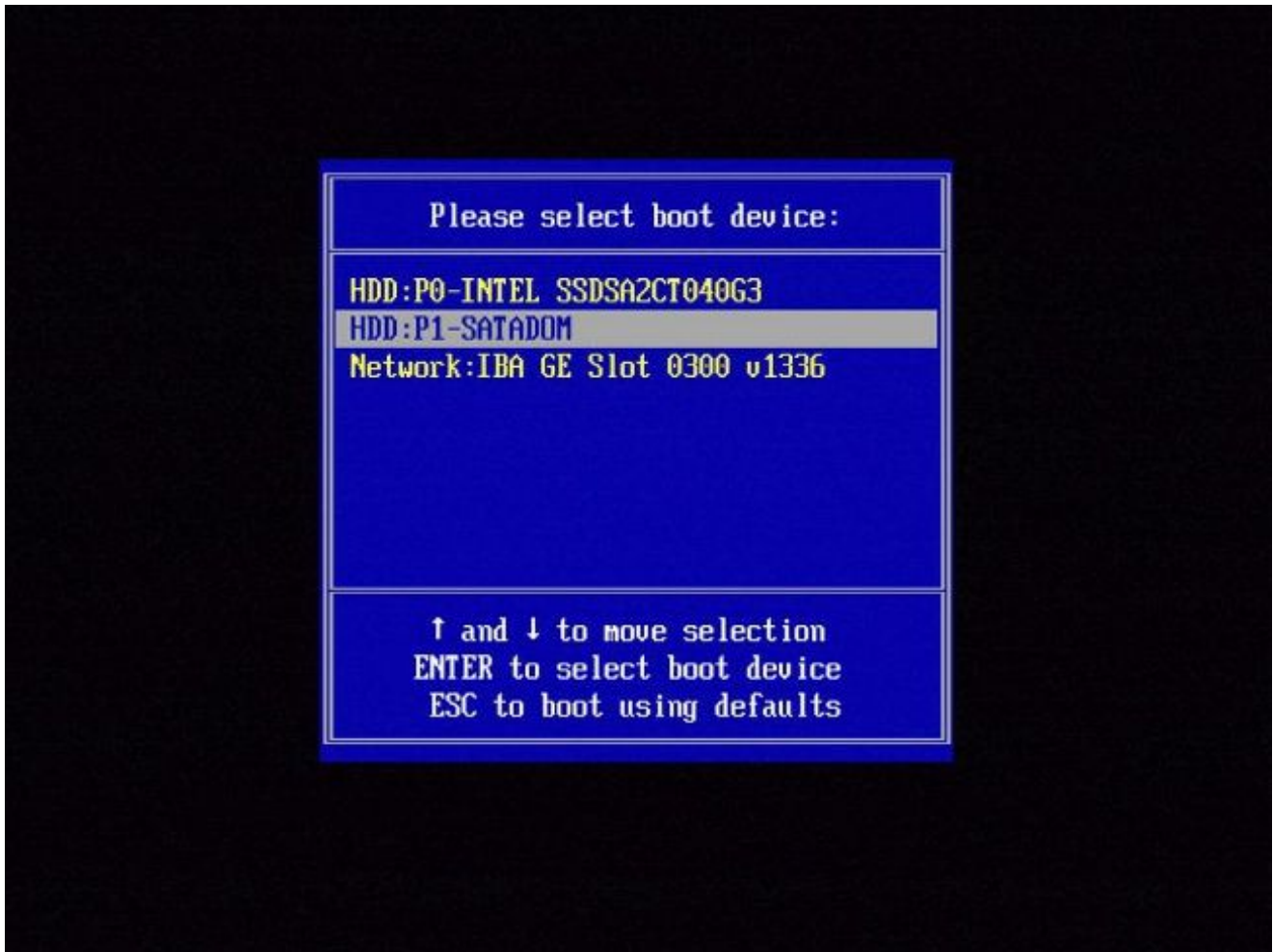
AMIBIOS (C) 2006 American Megatrends, Inc.
Aquila BIOS Version:AQNIS093 Date:11/21/2011
CPU : Intel(R) Xeon(R) CPU X3430 @ 2.40GHz
Speed : 2.40 GHz

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 ..

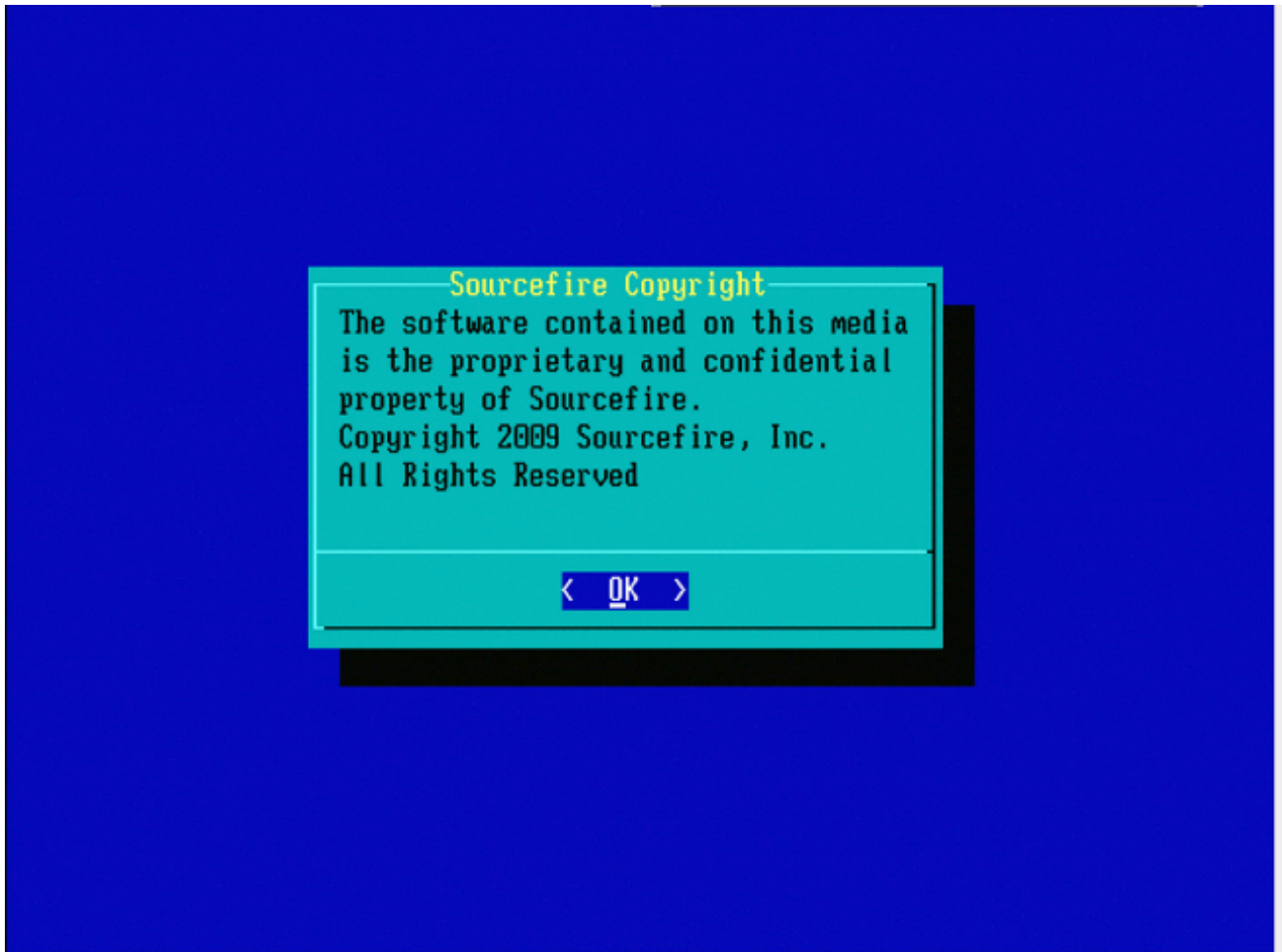
(C) American Megatrends, Inc.
66-0100-000001-00101111-112111-LfdHvdImc-AQNIS093-Y2KC

圖B1

3. 選擇選項HDD:P1-SATADOM，然後按Enter以引導至System_Restore分割槽。



圖B2



圖B3

8000系列裝置或管理中心型號FS750、FS1500或FS3500

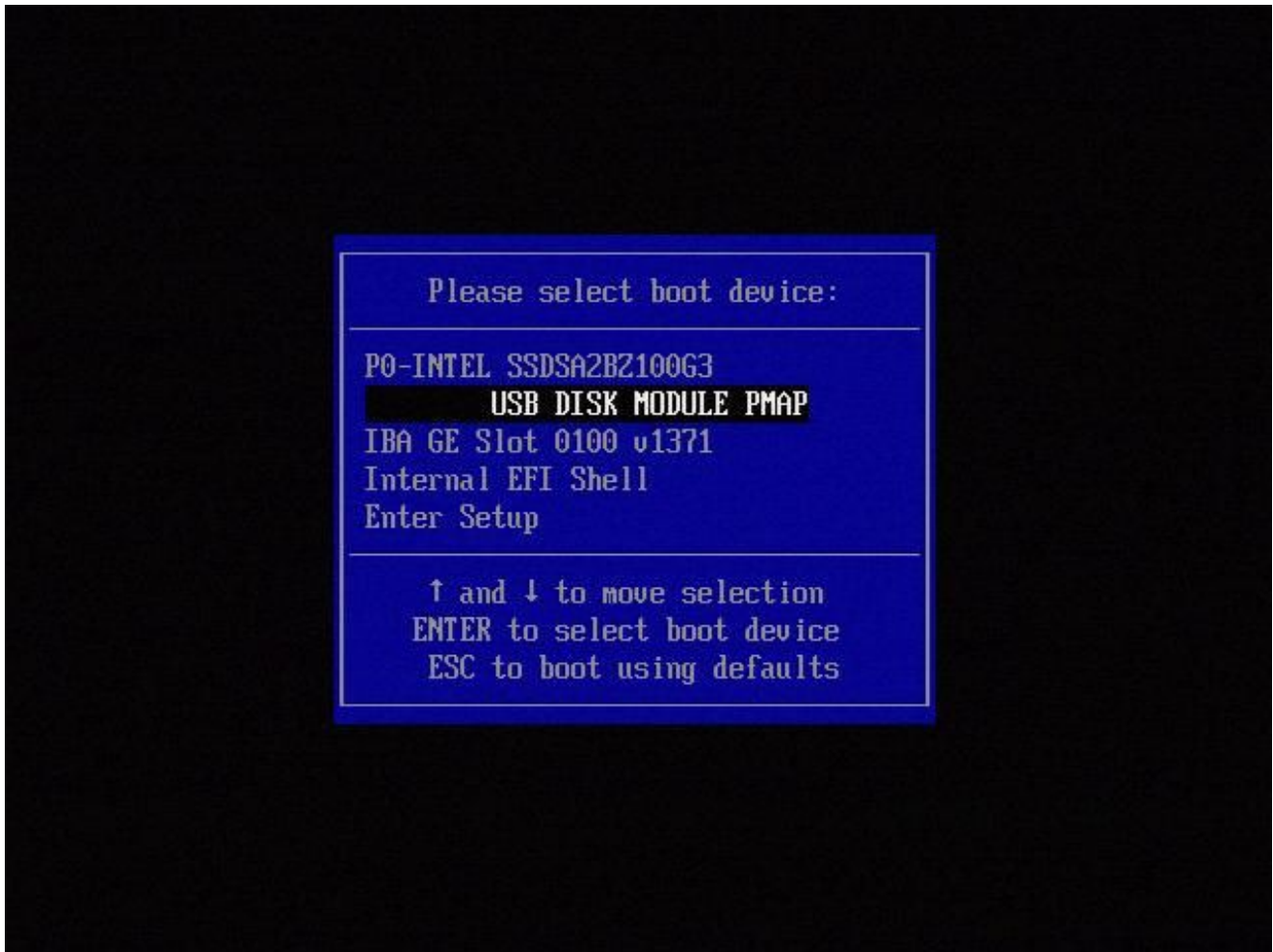
如果使用8000系列裝置或管理中心型號FS750、FS1500或FS3500，請完成以下步驟以選擇引導裝置：

1. 正常關閉裝置電源。
2. 在裝置啟動時開啟裝置電源，並重複按F6鍵，以訪問啟動裝置選擇螢幕。請參閱此處顯示的圖片：

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

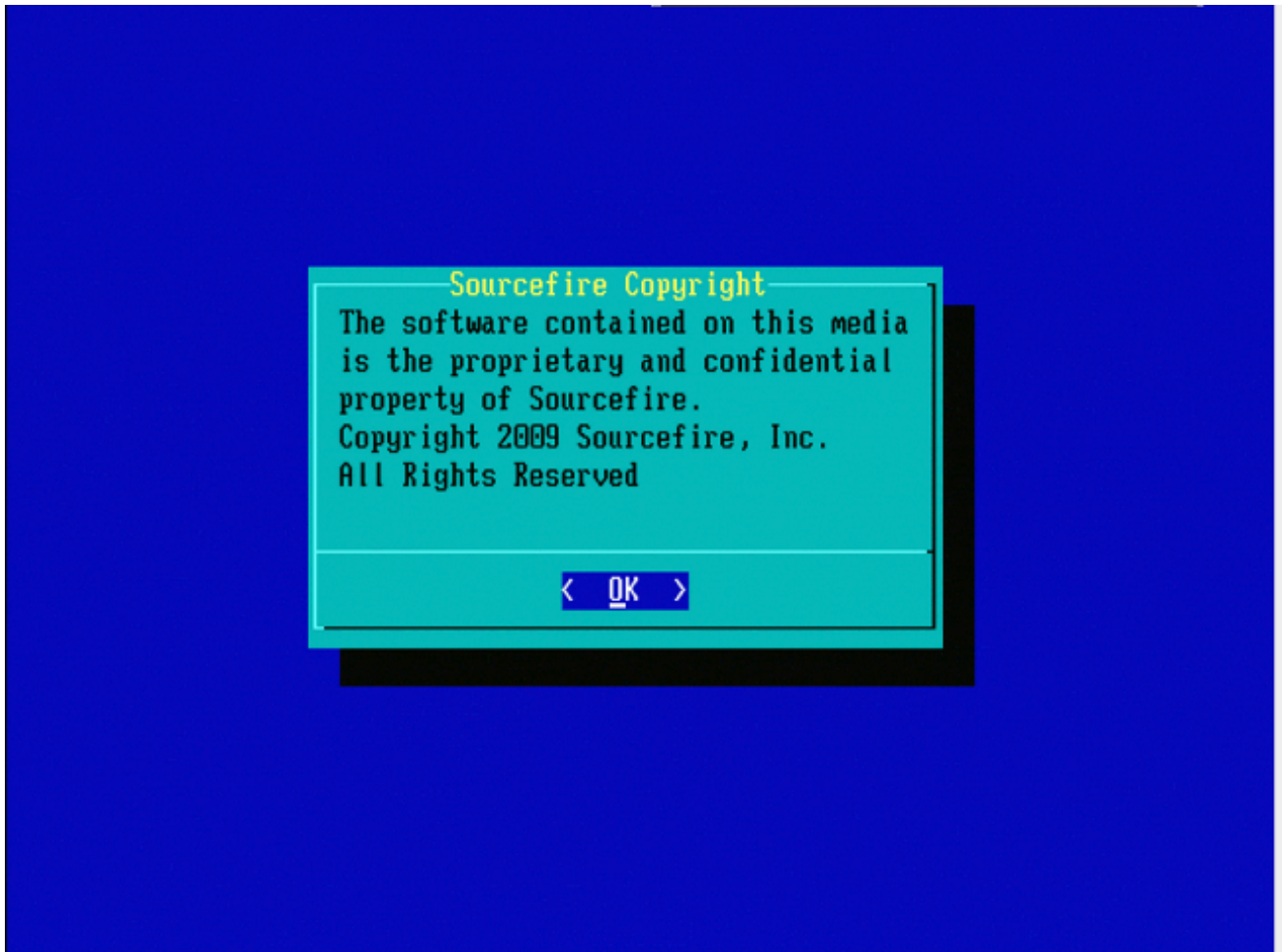
圖C1

3. 選擇USB選項。




圖C2

4. 裝置從System_Restore分割槽啟動並顯示System_Restore選單。



圖C3

型號FMC1000、FMC2500、FMC4500 (基於M4的FMC) 的系統還原

 註：對於FMC4500，此型號有不同的啟動選單，更多詳細資訊在下一連結[中](#)

對於以下型號，選擇系統還原的提示顯示不同：FMC1000、FMC2500、FMC4500

1. 啟動期間，您可以看到此螢幕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]:
```

圖D1

2. 選擇System Restore(系統還原#3項，本例中為)。

```
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]:
```

圖D2

3. 選擇系統還原的顯示方法(#1情況下為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
```

圖D3

4. 然後您到達圖5中所示的提示符，此過程繼續正常進行。

未列出啟動選項

引導至重新映像分割槽的選項可能未列在BIOS或引導選單中。如果是這種情況，包含重新映像系統的驅動器可能丟失或損壞。可能需要RMA。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。