Ricreare l'immagine di un centro di gestione FireSIGHT e di un'appliance FirePOWER

Sommario

Introduzione

Questo documento descrive i processi con esempi per la procedura di ricreazione dell'immagine di un Cisco FireSIGHT Management Center (FMC) e di appliance FirePOWER.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

Dispositivo gestito	Centro di gestione FireSIGHT	Versioni software disponibili per la ricreazione dell'immagine
Cisco Firepower serie 7000	FS 750	5.2 o successiva

Cisco Firepower serie 7100 Cisco Firepower serie 8100 Cisco Firepower serie 8200	FS 1500 FS 3500	
Firepower serie 8300 Cisco AMP 7150 Cisco AMP 8150		5.3 o successiva

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Ricrea immagine del processo

⚠ Attenzione: non inserire un dispositivo di storage USB né collegare uno switch KVM (Keyboard, Video, and Mouse) quando si aggiorna o si ricrea l'immagine di un centro di gestione FireSIGHT o di un accessorio FirePOWER.

Operazioni preliminari

1. Se si prevede di ricreare l'immagine di un centro di gestione o di un dispositivo Firepower autonomo, è consigliabile eseguire il backup dell'accessorio prima di procedere.
2. Identificare il modello del sensore e utilizzare l'elenco dei modelli nella sezione Componenti usati per verificare che questa guida sia appropriata.
3. Scaricare la guida all'installazione e l'immagine del disco appropriate per la versione software desiderata dal sito del supporto Cisco.

   Nota: non rinominare un file ISO

   Utilizzare l'immagine: il file con estensione iso deve essere copiato su un host che esegue un server SSH raggiungibile dalla rete di gestione dell'accessorio di cui si desidera ricreare l'immagine.

> Nota: se non è disponibile alcun altro server SSH, è possibile usare un FMC per questo processo.

Verificare l'integrità dell'ISO: la somma md5 dei file viene fornita sul lato destro della pagina per la verifica con un'utility md5sum.

4. Le guide all'installazione contengono istruzioni dettagliate per la ricreazione dell'immagine e delineano inoltre diversi metodi per il processo di ricreazione dell'immagine. Le immagini fornite in questo documento possono essere utilizzate come riferimento.

Panoramica del processo di ricreazione immagine

> Nota: la versione 5.3 è stata utilizzata per acquisire le immagini mostrate in questo articolo. Il processo di ricreazione immagine è identico per le altre versioni 5.x, ad eccezione dei numeri di versione che appaiono nelle immagini mostrate.

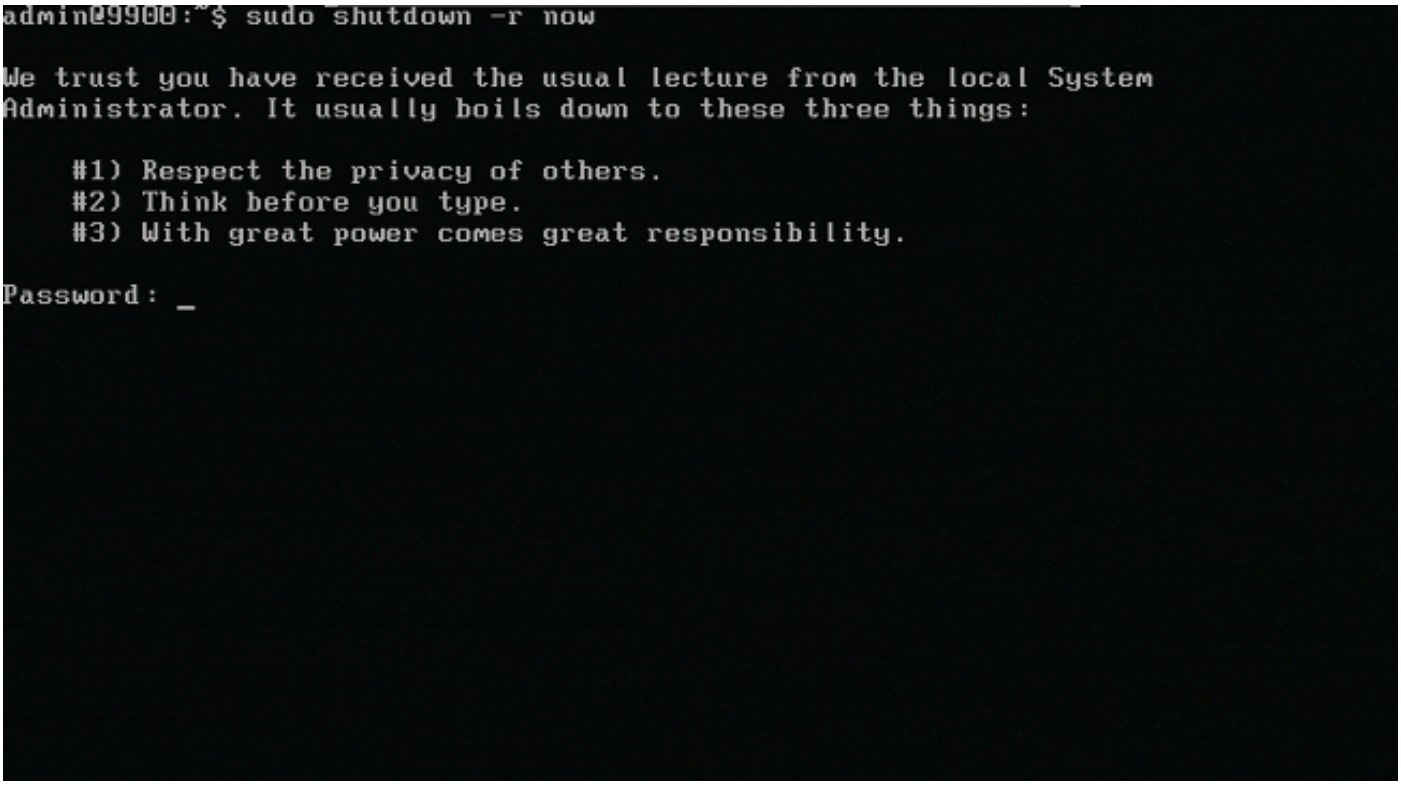


Figura 1

Figura 2 - Quando il sistema viene riavviato, premere un tasto freccia sulla tastiera per interrompere il conto alla rovescia e scegliere l'opzione System_Restore per la schermata mostrata di seguito.

Nota: se il prompt System_Restore non viene visualizzato, è necessario modificare l'ordine di avvio per avviare direttamente la partizione di ripristino (DOM). Per ulteriori informazioni, vedere Opzione di menu LILO di System_Restore mancante.

Figura 3

Figura 4 - Scegliere l'opzione 0 se si utilizzano una tastiera e un monitor.

Nota: a volte si è visto che il menu per l'opzione Ripristina è visualizzato solo quando è collegata solo la console (con la tastiera scollegata). Quando l'opzione Recovery (Ripristino) è selezionata, la tastiera può essere nuovamente connessa

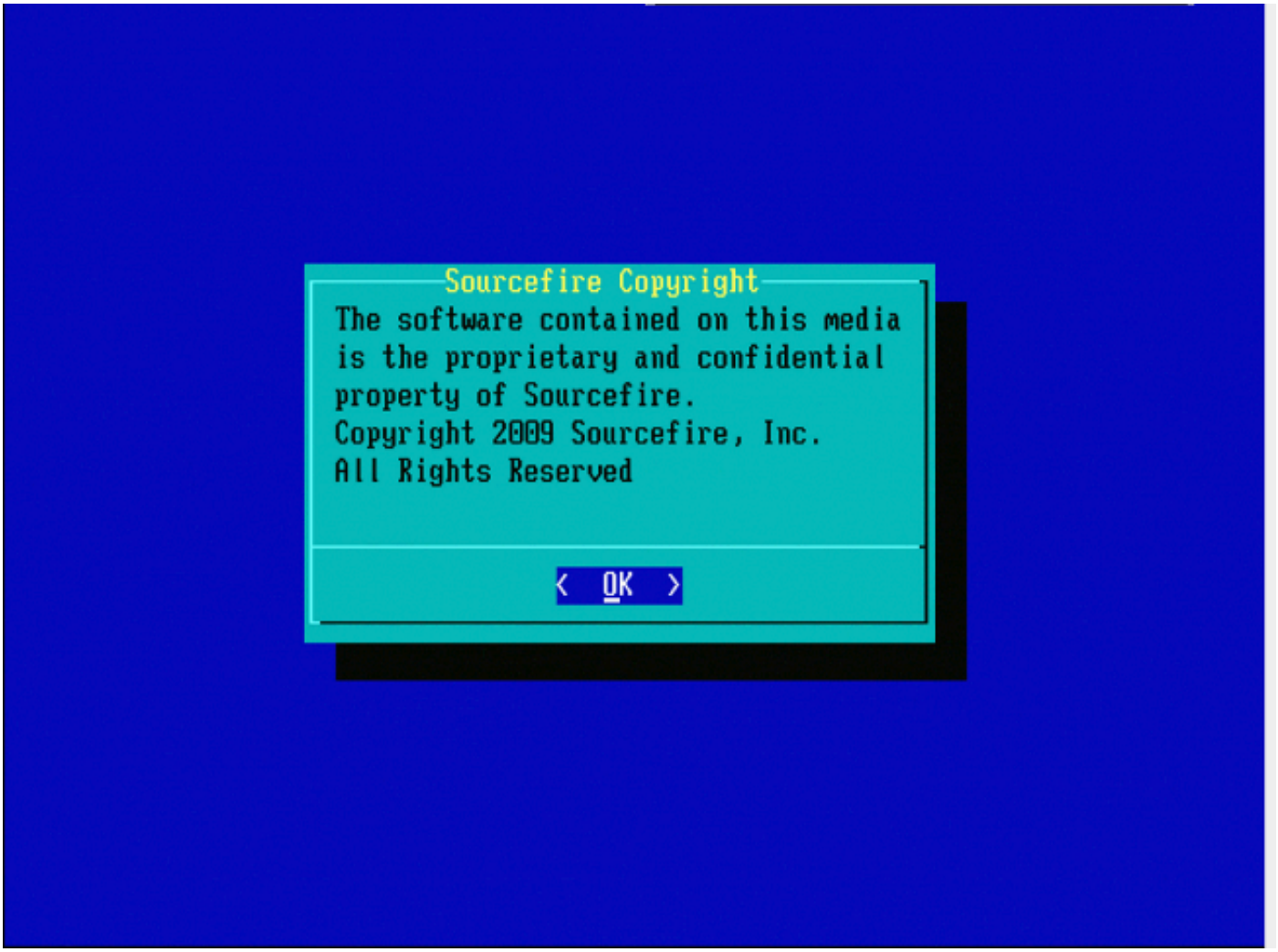


Figura 5


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>

Figura 6

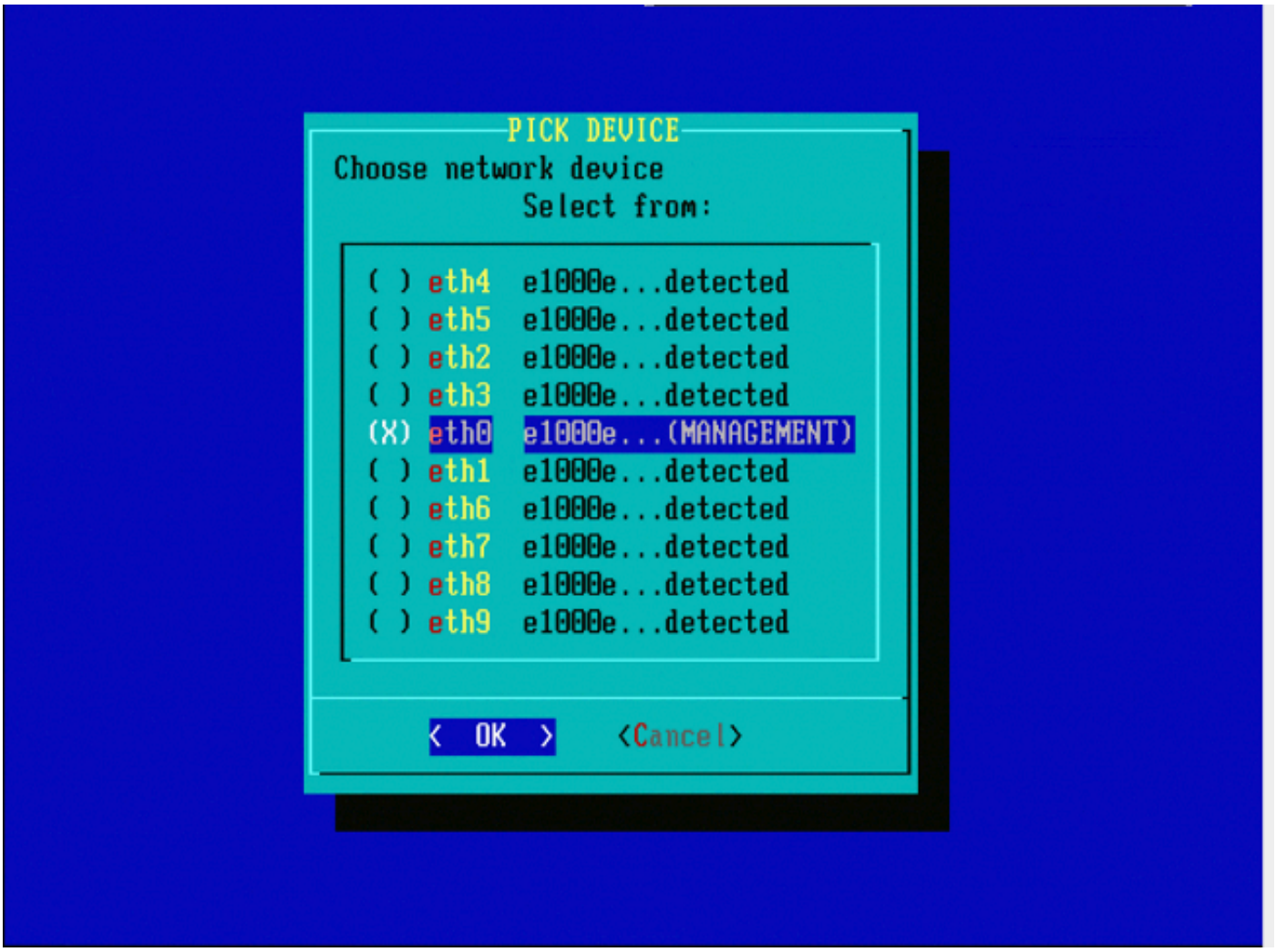


Figura 7 - Per selezionare il dispositivo di rete, premere la barra spaziatrice.

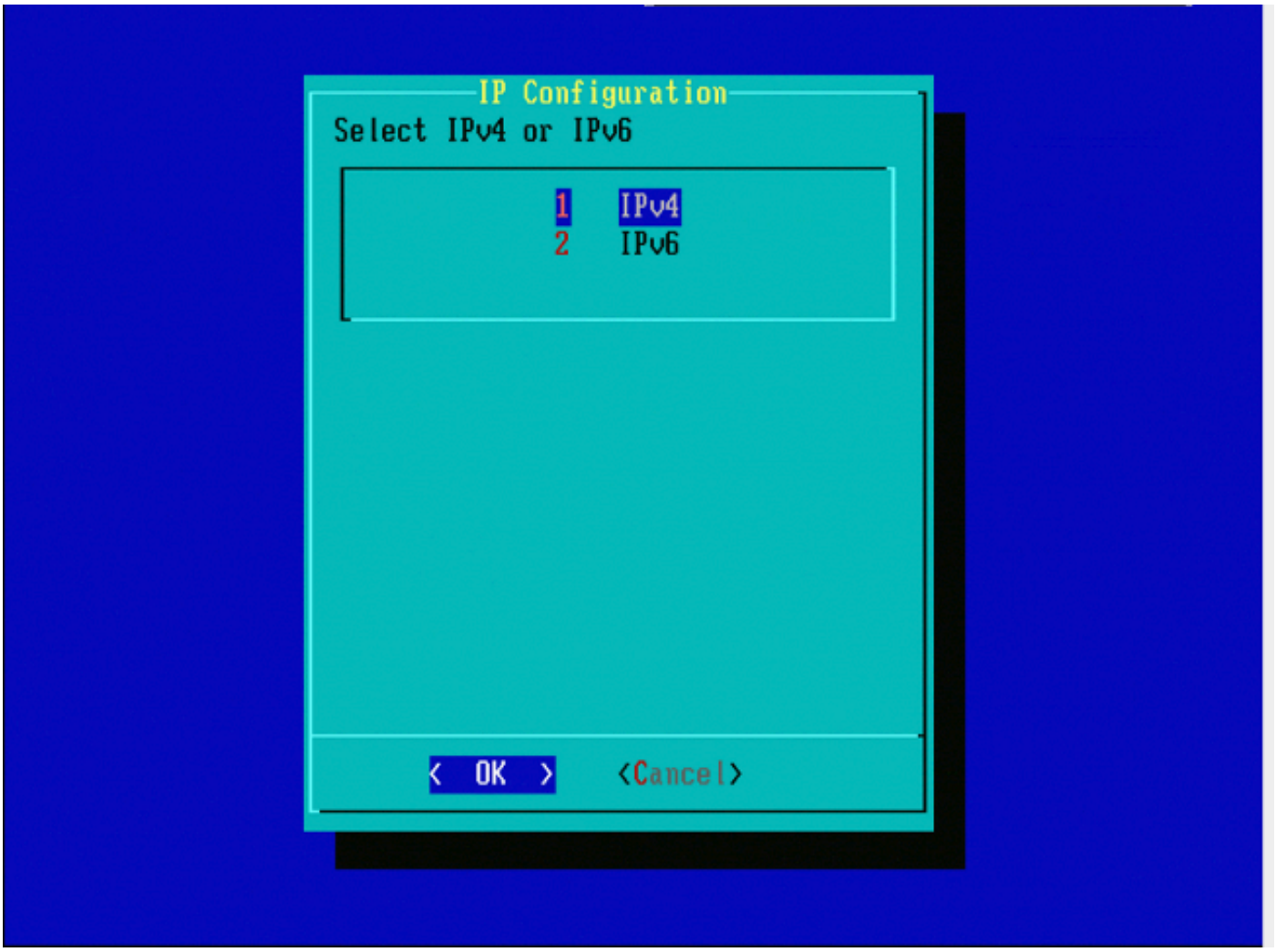


Figura 8

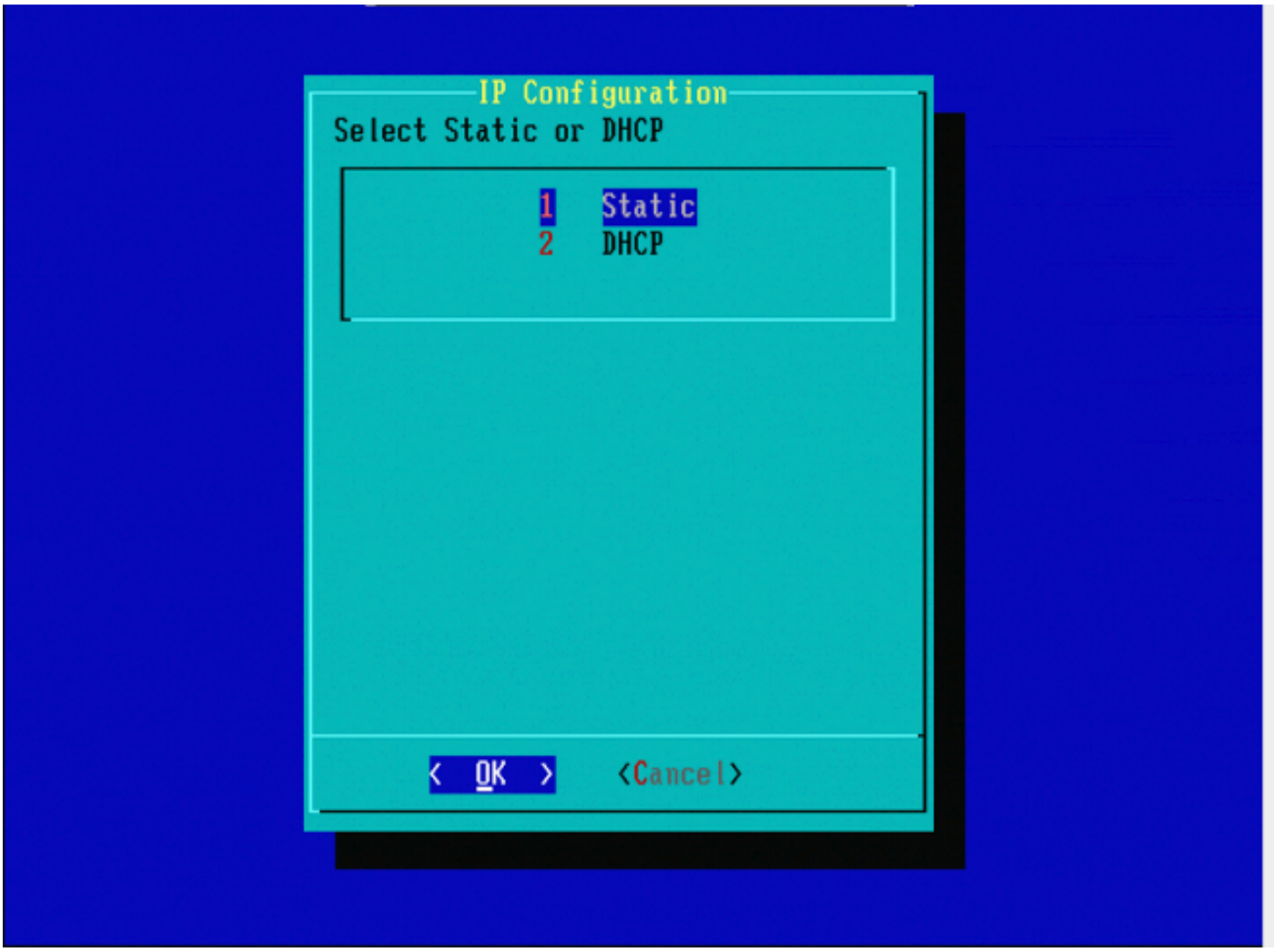

IP Configuration
Select Static or DHCP
1 Static
2 DHCP
< OK >
<Cancel>

Figura 9


IP Address
Enter an IP address for this system:
10.5.30.23
< OK >
<Cancel>

Figura 10

Figura 11

Figura 12


Verify IP Configuration
IP: 10.5.30.23
Netmask: 255.255.0.0
Gateway: 10.5.1.1
< OK >

Figura 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>

Figura 14

Figura 15 - Il supporto Cisco consiglia di utilizzare il protocollo Secure Copy (SCP).

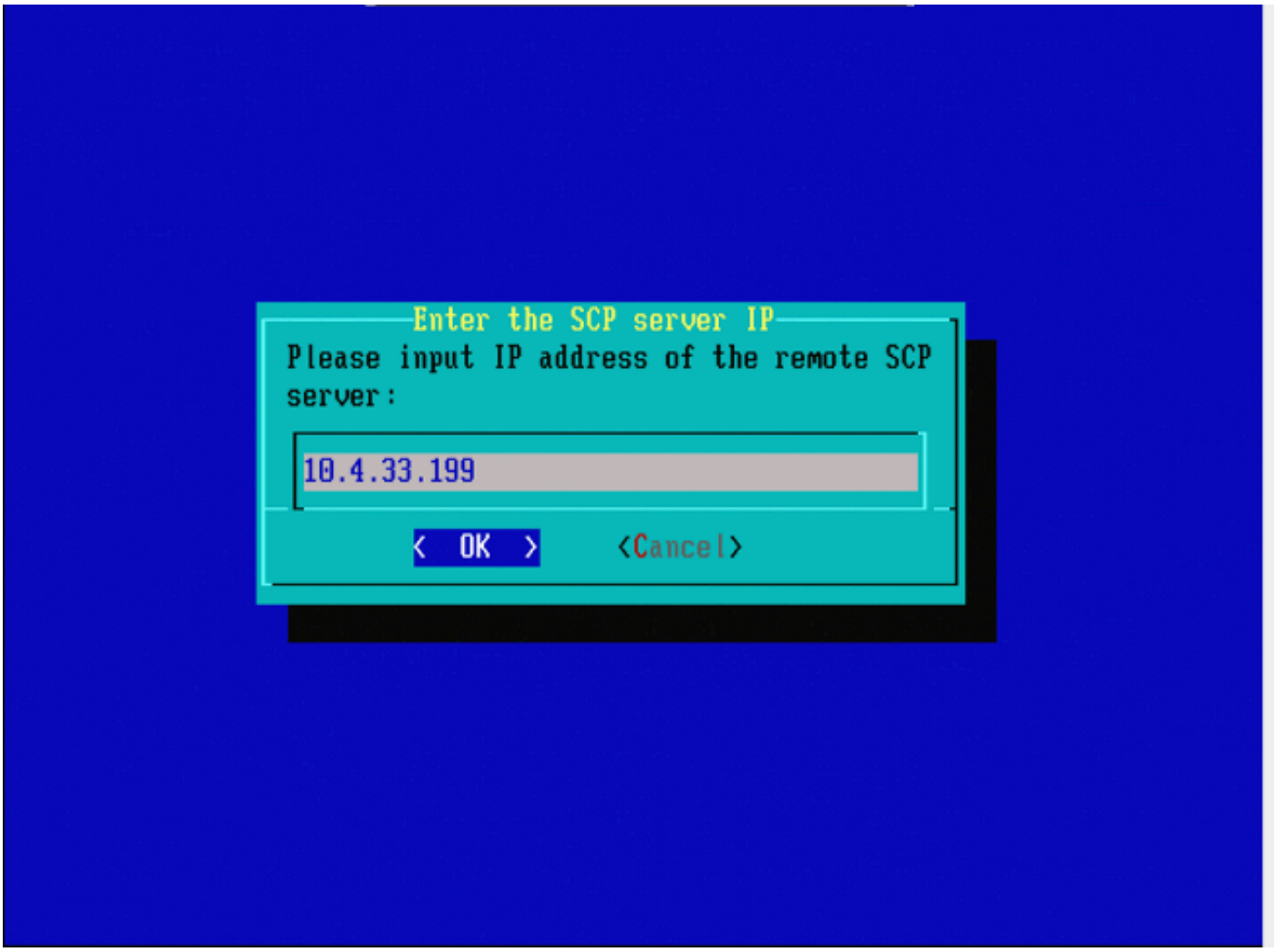


Figura 16 - È possibile utilizzare un centro di gestione FireSIGHT come server SCP per questa fase. Continuare con questa procedura e utilizzare l'indirizzo IP e le credenziali per il centro di gestione per compilare i campi del menu Ripristino configurazione di sistema. Ulteriori informazioni in

Per trasferire i file in modo sicuro viene utilizzato un server Secure Copy (SCP). Se Se necessario, è possibile utilizzare un centro di difesa Sourcefire (DC) come server SCP per trasferire file a un altro dispositivo Sourcefire. Ciò può essere utile quando un'immagine ISO deve essere trasferita a un dispositivo Sourcefire per la ricreazione dell'immagine, ma il normale server SCP non è raggiungibile o non è disponibile.

Passaggio 1. Scaricare un file .iso appropriato sul desktop dal portale di supporto Sourcefire.
Passaggio 2. Utilizzare un client SCP, copiare il file dal desktop al centro difesa.

Suggerimento: un client SCP è generalmente disponibile in un sistema operativo Linux o Mac. Tuttavia, nel sistema operativo Windows, è possibile che sia necessario installare un software client SCP di terze parti. Sourcefire non fornisce consigli o supporto per l'installazione di software client SCP specifici.

Nell'esempio seguente viene illustrato come copiare un file di immagine .iso Sourcefire dalla directory Downloads di un sistema Linux alla directory /var/tmpdirectory di Sourcefire Defense

Center:

<#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

⚠ Attenzione: non modificare il nome del file ISO. Può creare un problema con il rilevamento del file durante una nuova immagine.

A questo punto il file viene copiato nel centro difesa. È possibile procedere con il processo di ricreazione immagine dei dispositivi Sourcefire. Nella nuova immagine, se necessario, è possibile fornire l'indirizzo IP e il nome utente del controller di dominio e il percorso in cui è stato copiato il file immagine con le istruzioni precedenti.

⚠ Avviso: dopo aver completato la ricreazione dell'immagine, è necessario rimuovere il file .iso dalla directory /var/tmp del centro difesa per ridurre l'utilizzo dello spazio su disco.

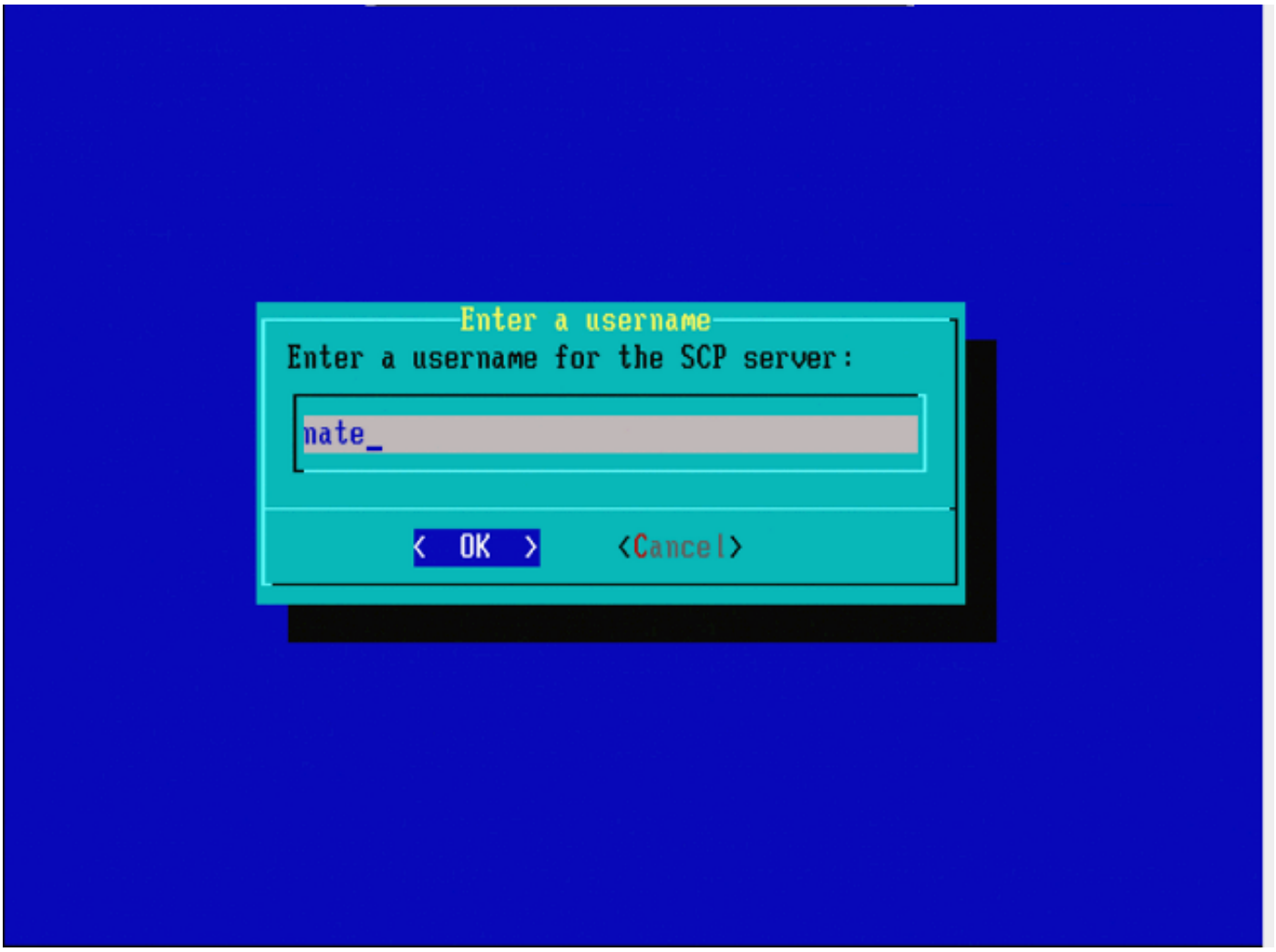

Enter a username
Enter a username for the SCP server:
nate_
< OK >
<Cancel>

Figura 17

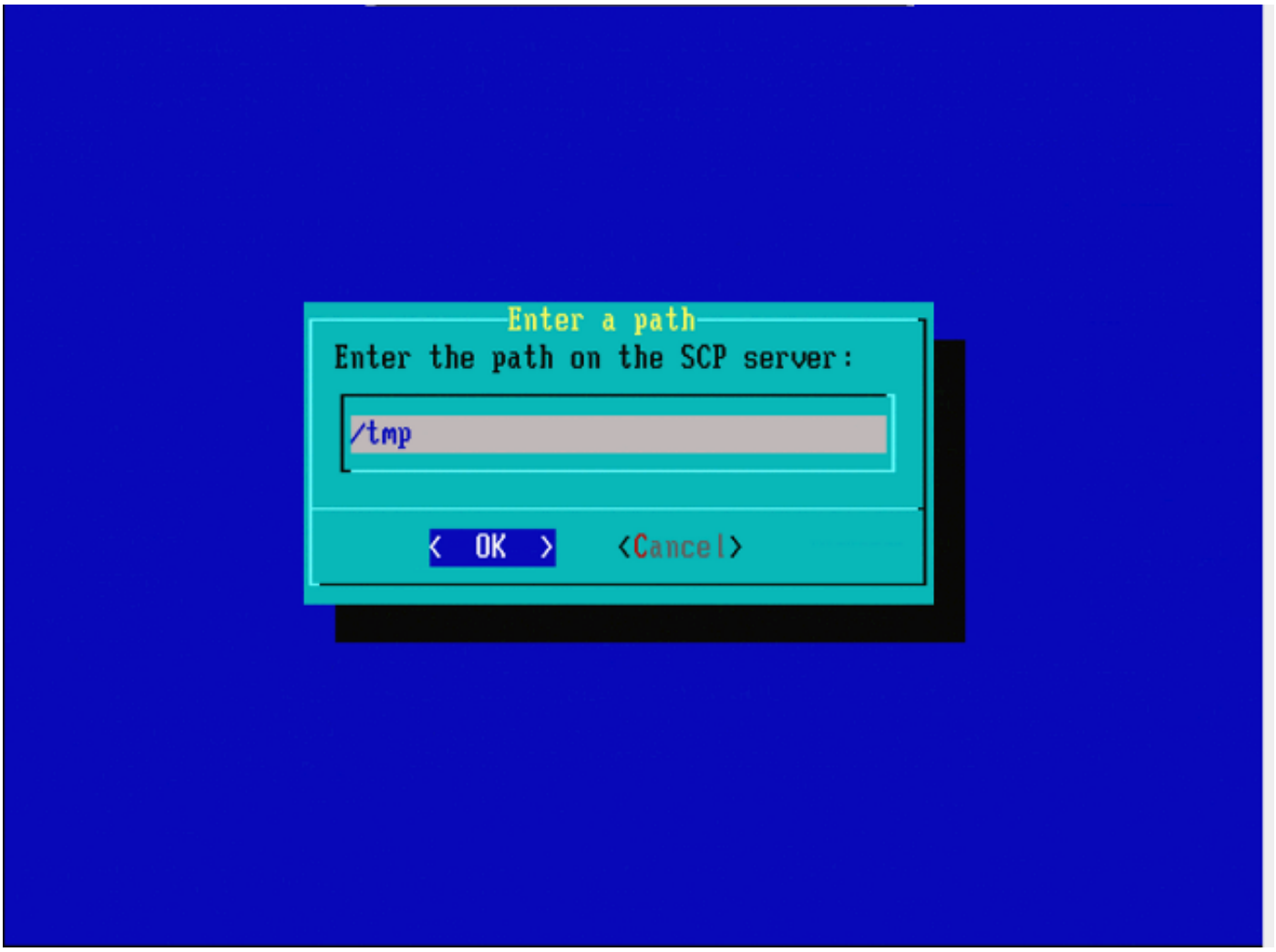


Figura 18

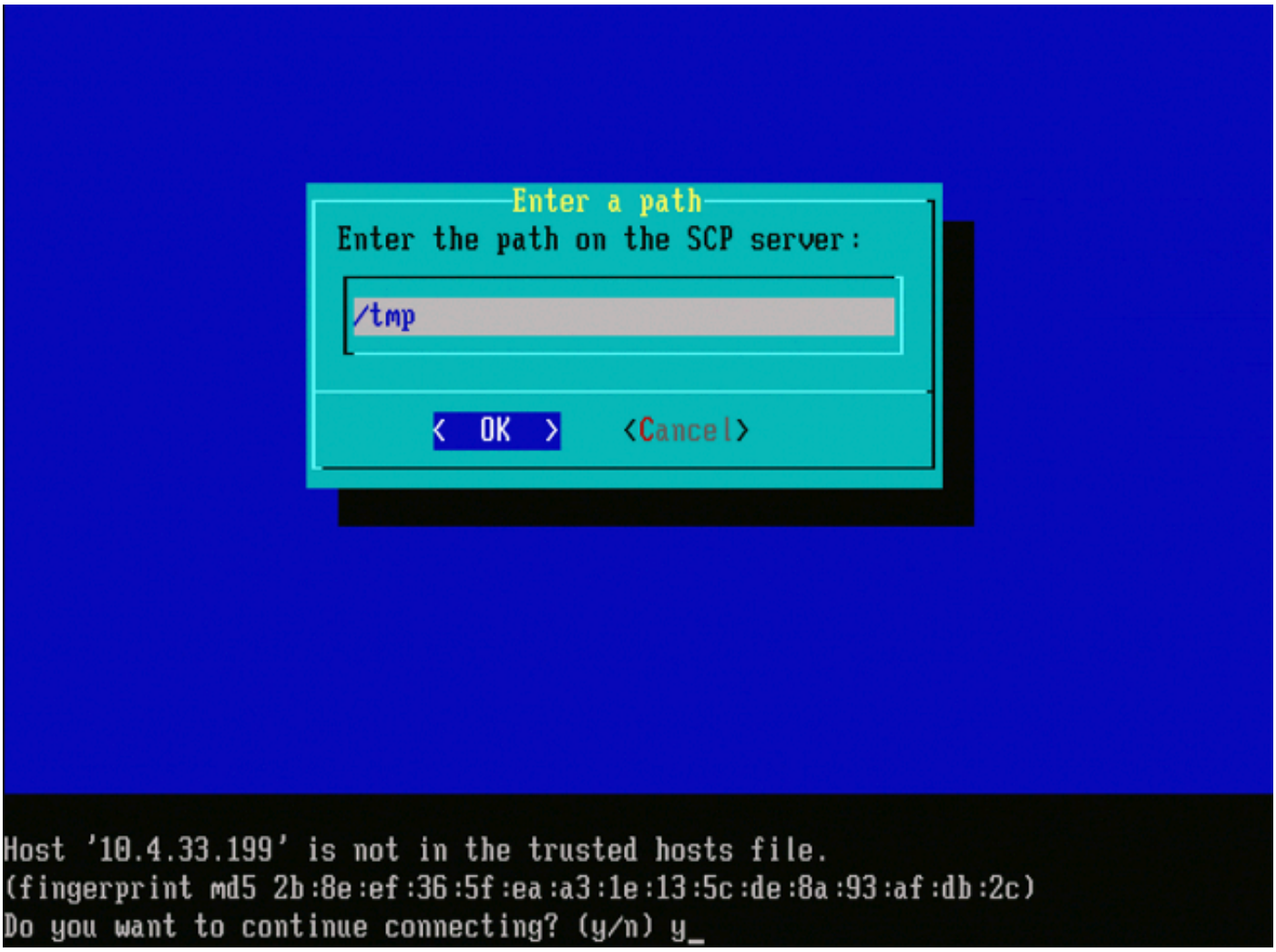


Figura 19

Nota: se si riceve un errore di connettività in questo punto anziché il messaggio previsto, verificare la connessione al server SSH.

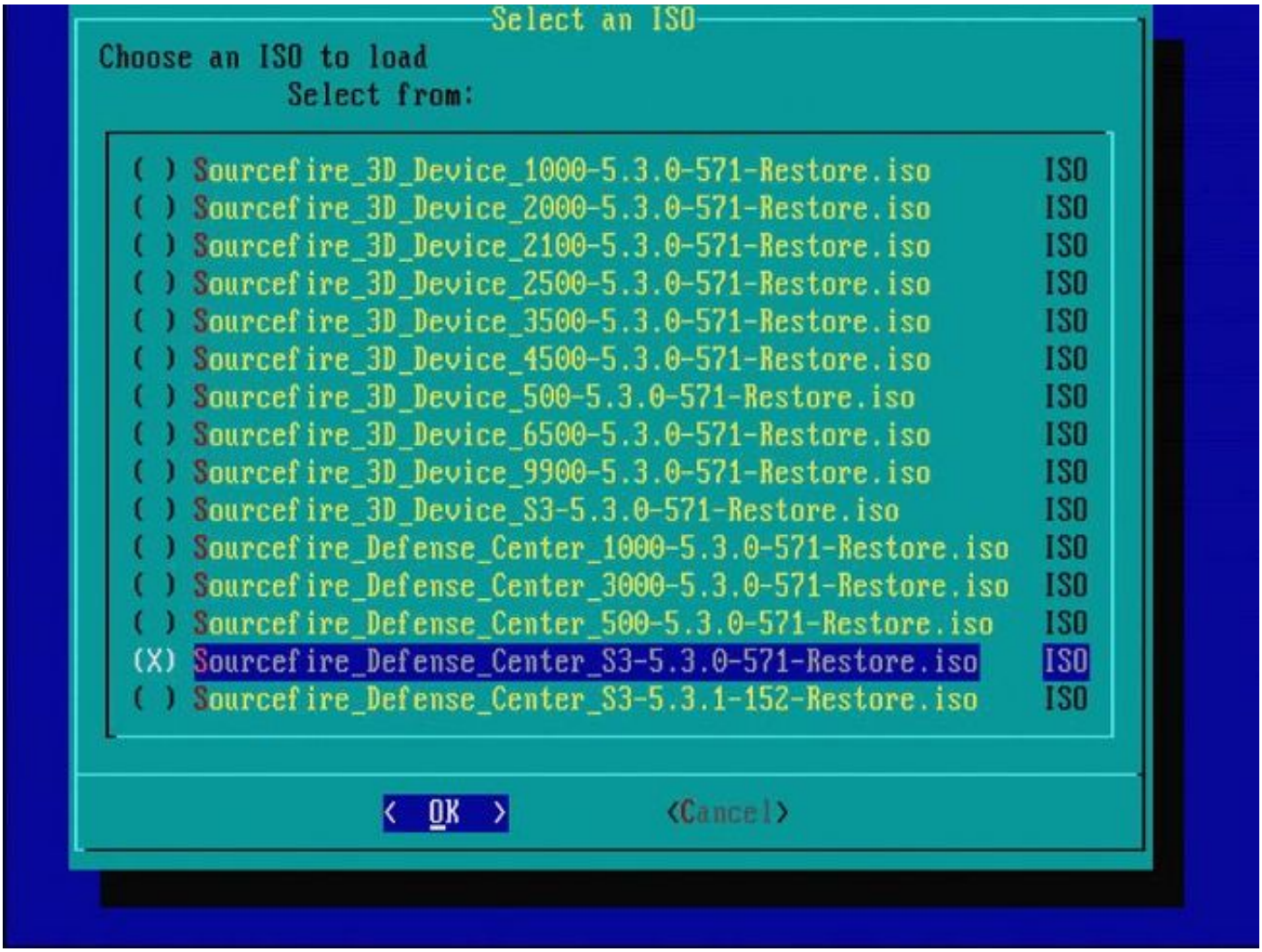


Figura 20 - Per selezionare l'immagine ISO, premere la barra spaziatrice.

Nota: è necessario utilizzare i nomi file predefiniti per i file con estensione iso, altrimenti i file potrebbero non essere rilevati in questa fase.
Errore: nessuna immagine ISO trovata
Nella versione 6.3, la convenzione dei nomi ISO è cambiata da Sourcefire_3D_Device_S3-<ver>-<build>-Restore.iso a Cisco_Firepower_NGIPS_Appliance-<ver>-<build>-Restore.iso. Se viene visualizzato "No ISO Image Were Found" (Nessuna immagine ISO trovata), rinominare il file ISO con il nome file precedente. Ciò si verifica in genere quando si ricrea l'immagine della versione 6.2.x o precedente nella versione 6.3.0 o successiva.

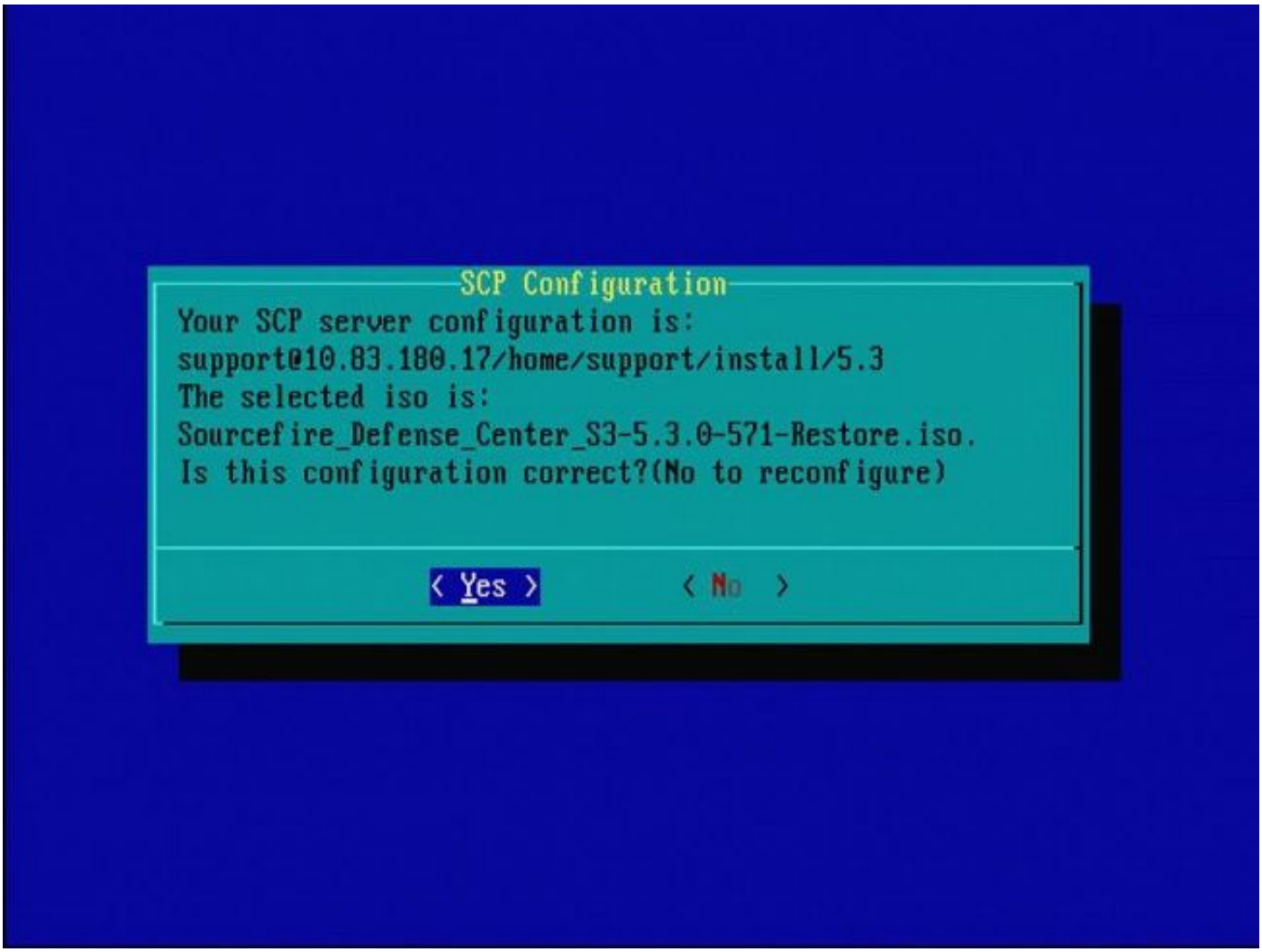

SCP Configuration
Your SCP server configuration is:
support@10.83.180.17/home/support/install/5.3
The selected iso is:
Sourcefire_Defense_Center_S3-5.3.0-571-Restore.iso.
Is this configuration correct?(No to reconfigure)
< Yes >
< No >

Figura 21

Figura 22 - Il supporto Cisco consiglia di saltare il passaggio 3 in questo processo. Le patch e gli SRU (Snort Rule Updates) possono essere installati al termine della ricreazione dell'immagine.

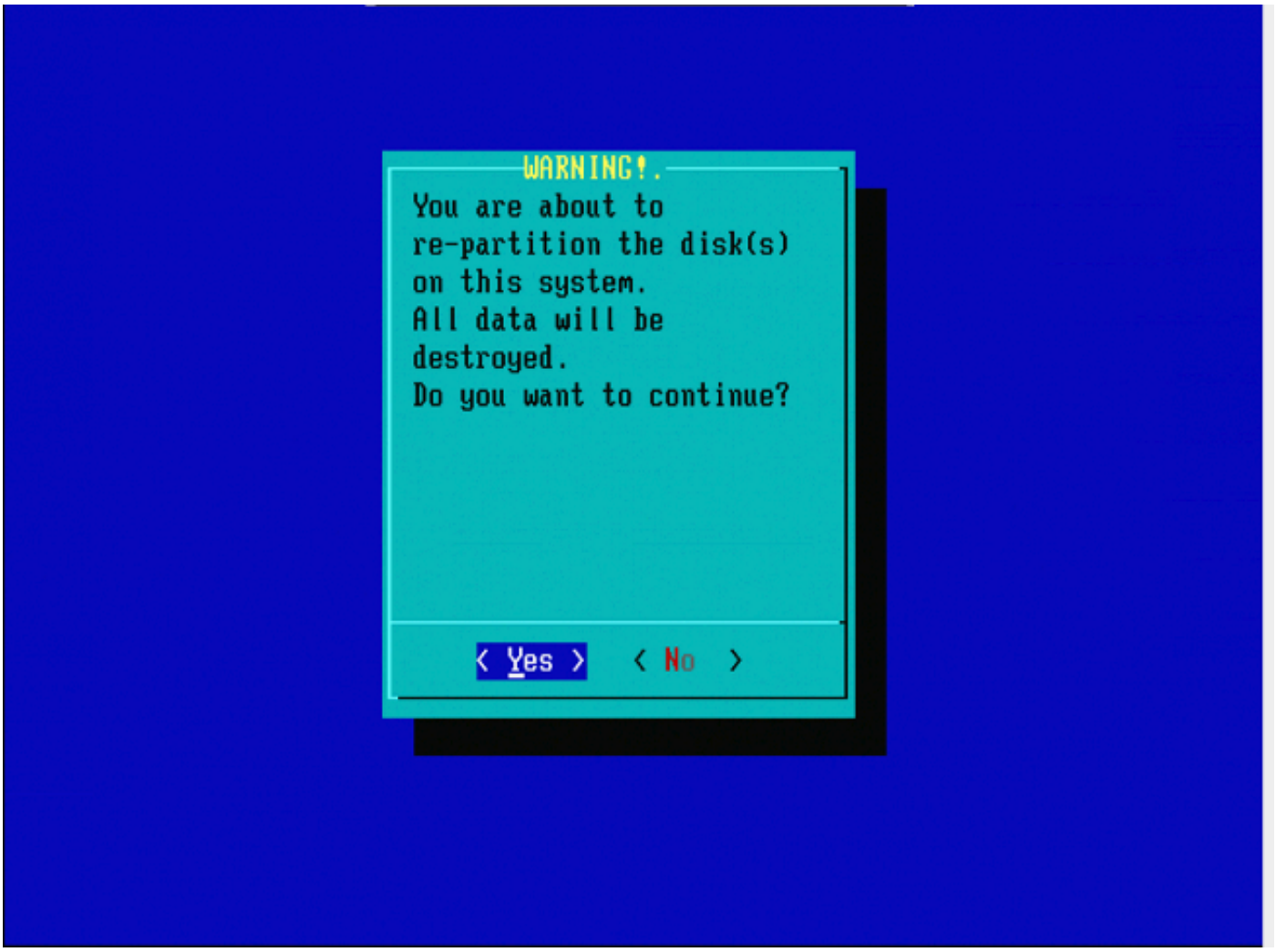
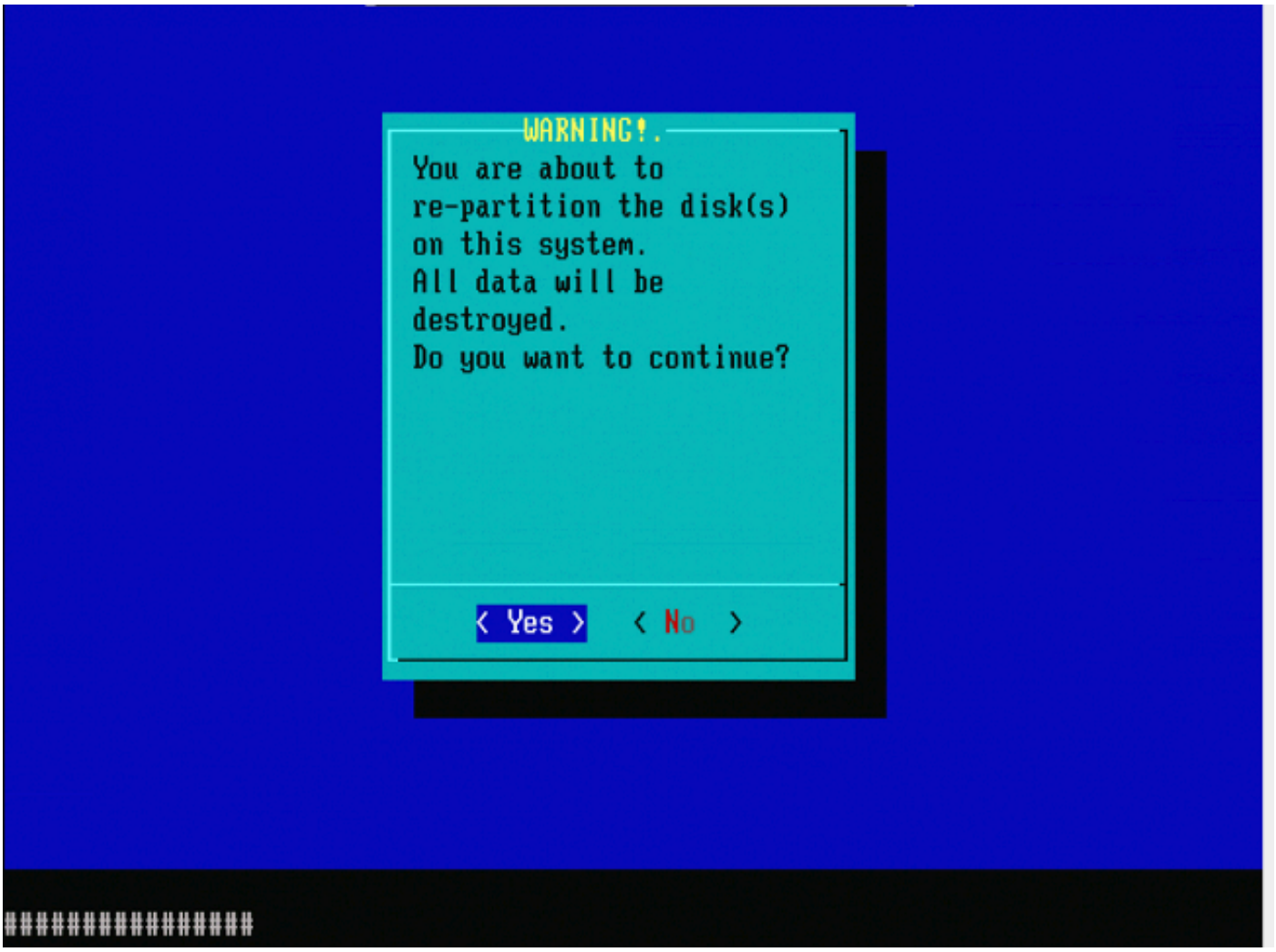

WARNING!.
You are about to
re-partition the disk(s)
on this system.
All data will be
destroyed.
Do you want to continue?
< Yes >
< No >

Figura 23


WARNING!.
You are about to
re-partition the disk(s)
on this system.
All data will be
destroyed.
Do you want to continue?
< Yes >
< No >
##################
Figura 24

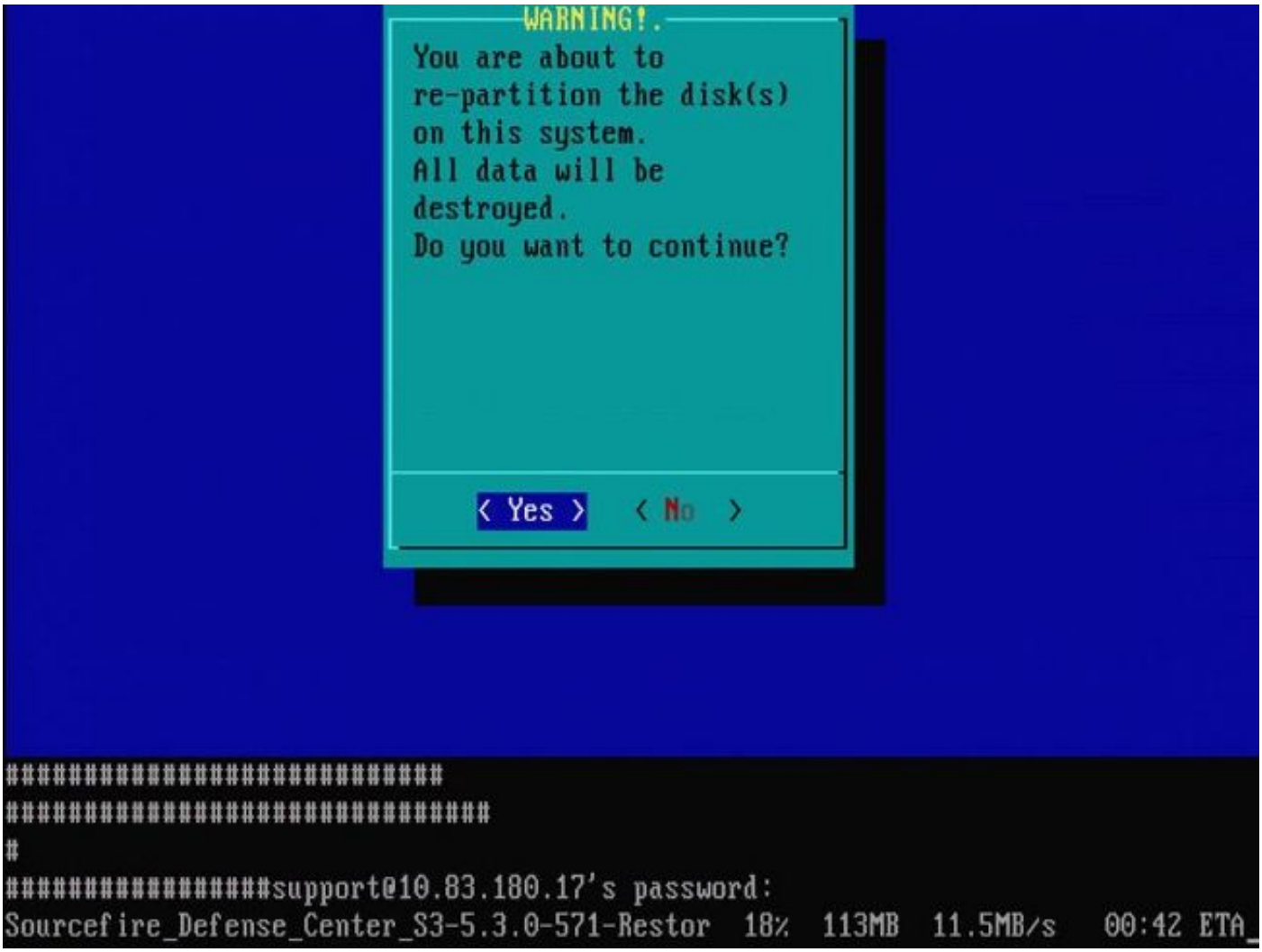

WARNING!.
You are about to
re-partition the disk(s)
on this system.
All data will be
destroyed.
Do you want to continue?
< Yes >
< No >
##############################
##################################
#
##################support@10.83.180.17's password:
Sourcefire_Defense_Center_S3-5.3.0-571-Restor 18% 113MB 11.5MB/s 00:42 ETA

Figura 25

Figura 26

Nota importante per quanto riguarda la ricreazione di un'immagine da una versione principale del software diversa: se si tenta di ricreare un'immagine di un dispositivo che in precedenza aveva una versione principale diversa del software, ad esempio se si ricrea l'immagine 5.1 > 5.2, 5.2 > 5.3, 5.3 > 5.2 e così via, è necessario completare due volte i passaggi descritti nelle figure da 1 a 26.

1. Dopo aver scelto OK nel prompt, come mostrato nell'immagine 26, la partizione di Ripristino configurazione di sistema viene visualizzata nella nuova versione e l'accessorio viene riavviato.
2. Dopo il riavvio, è necessario iniziare di nuovo il processo di ricreazione dell'immagine dall'inizio e continuare con il processo illustrato nelle figure da 27b a 31.

Se questa è la prima immagine da una versione principale diversa del software, viene visualizzata la schermata come mostrato nell'immagine 27a, quindi nelle figure 31 e 32.

⚠ Attenzione: se viene visualizzata questa schermata, è possibile che si verifichi un ritardo senza output visibile dopo "Check Hardware" e prima di "The USB device..." (Il dispositivo USB...). Non premere alcun tasto in questo momento, o il dispositivo si riavvia in uno stato inutilizzabile e deve essere nuovamente sottoposto a imaging.

In caso contrario, è possibile vedere le schermate dalla Figura 27b alla Figura 32.

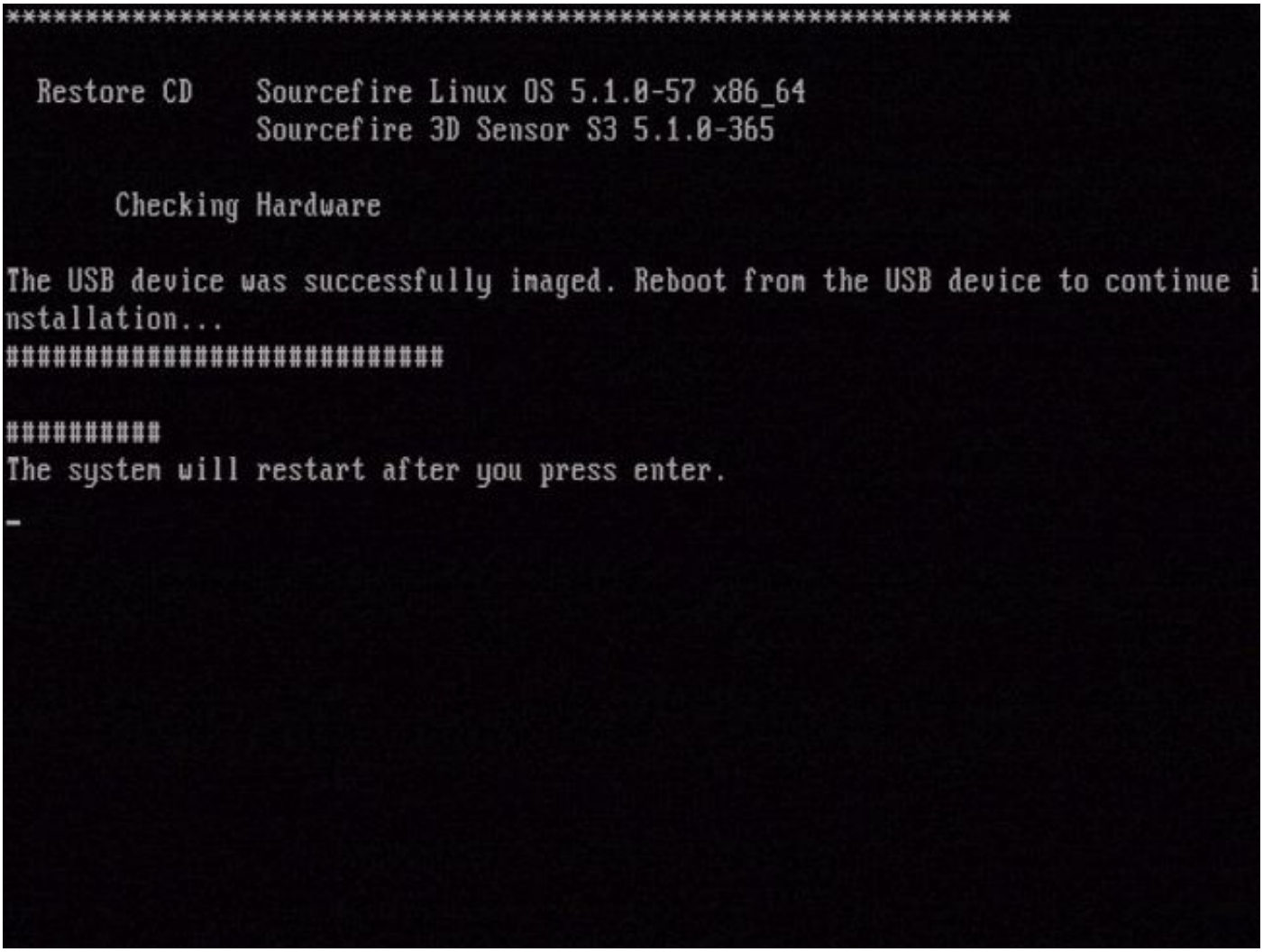


Figura 27a

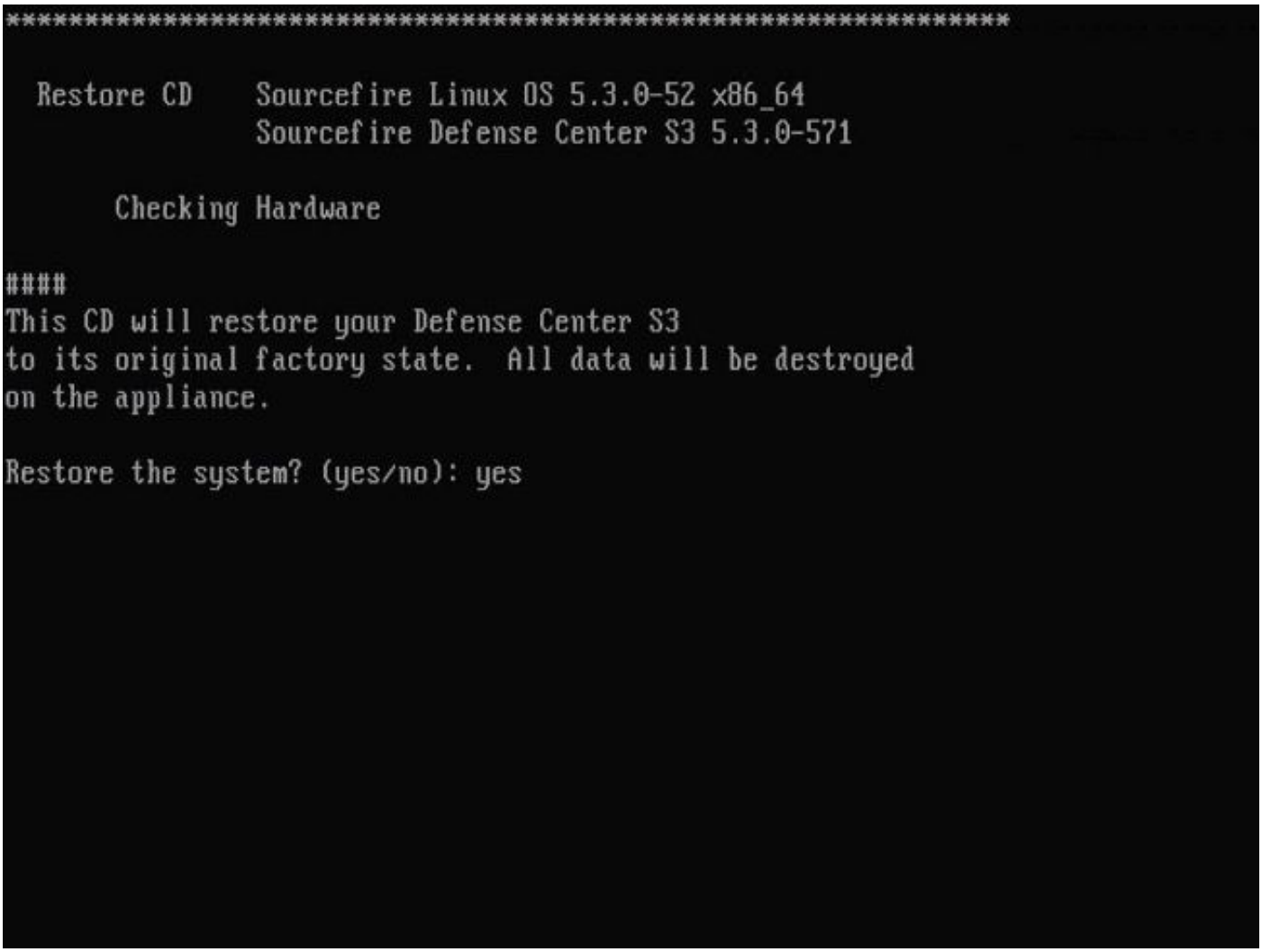

****
Restore CD Sourcefire Linux OS 5.3.0-52 x86_64
Sourcefire Defense Center S3 5.3.0-571
Checking Hardware
####
This CD will restore your Defense Center S3
to its original factory state. All data will be destroyed
on the appliance.
Restore the system? (yes/no): yes

Figura 27b

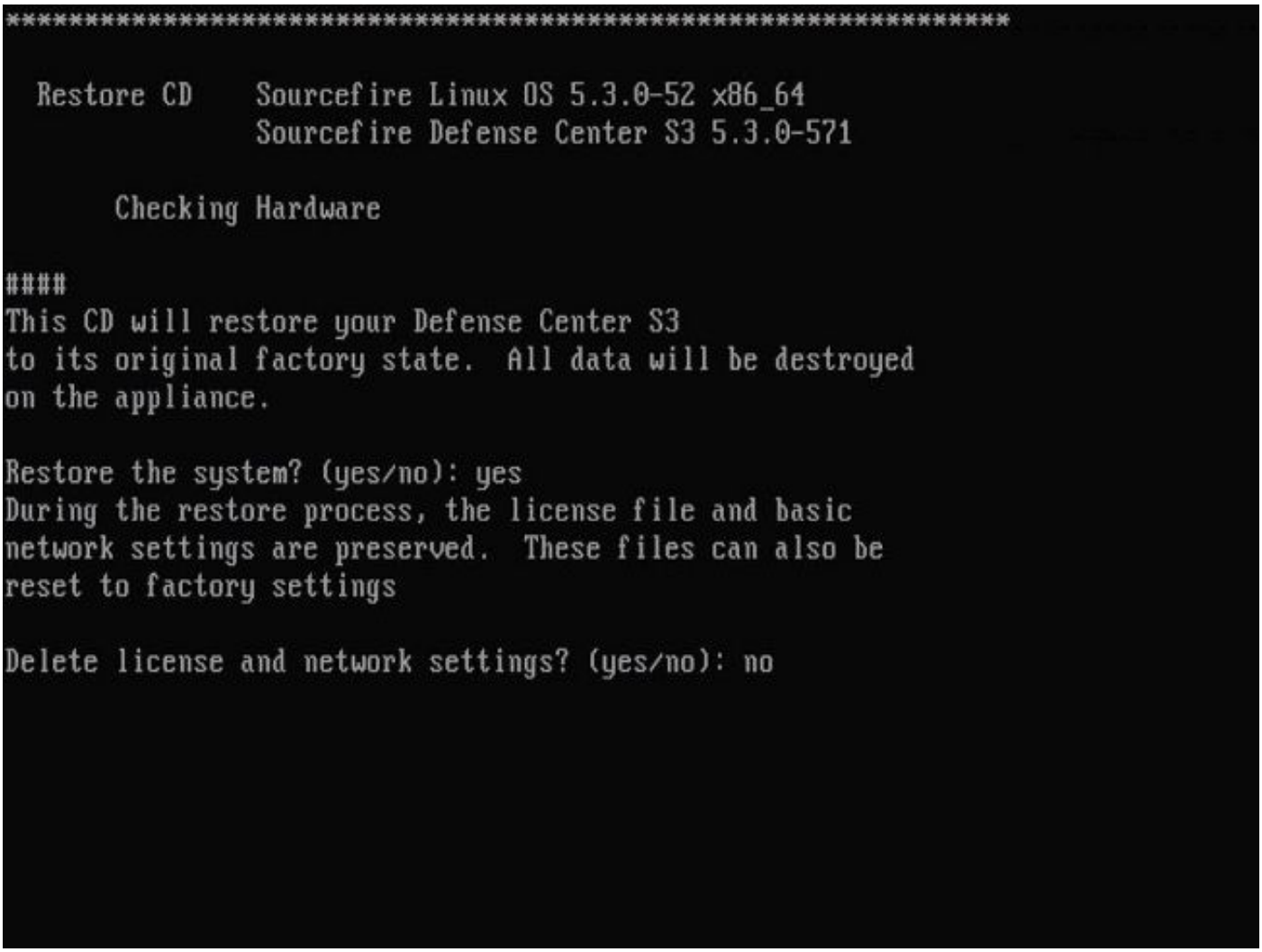
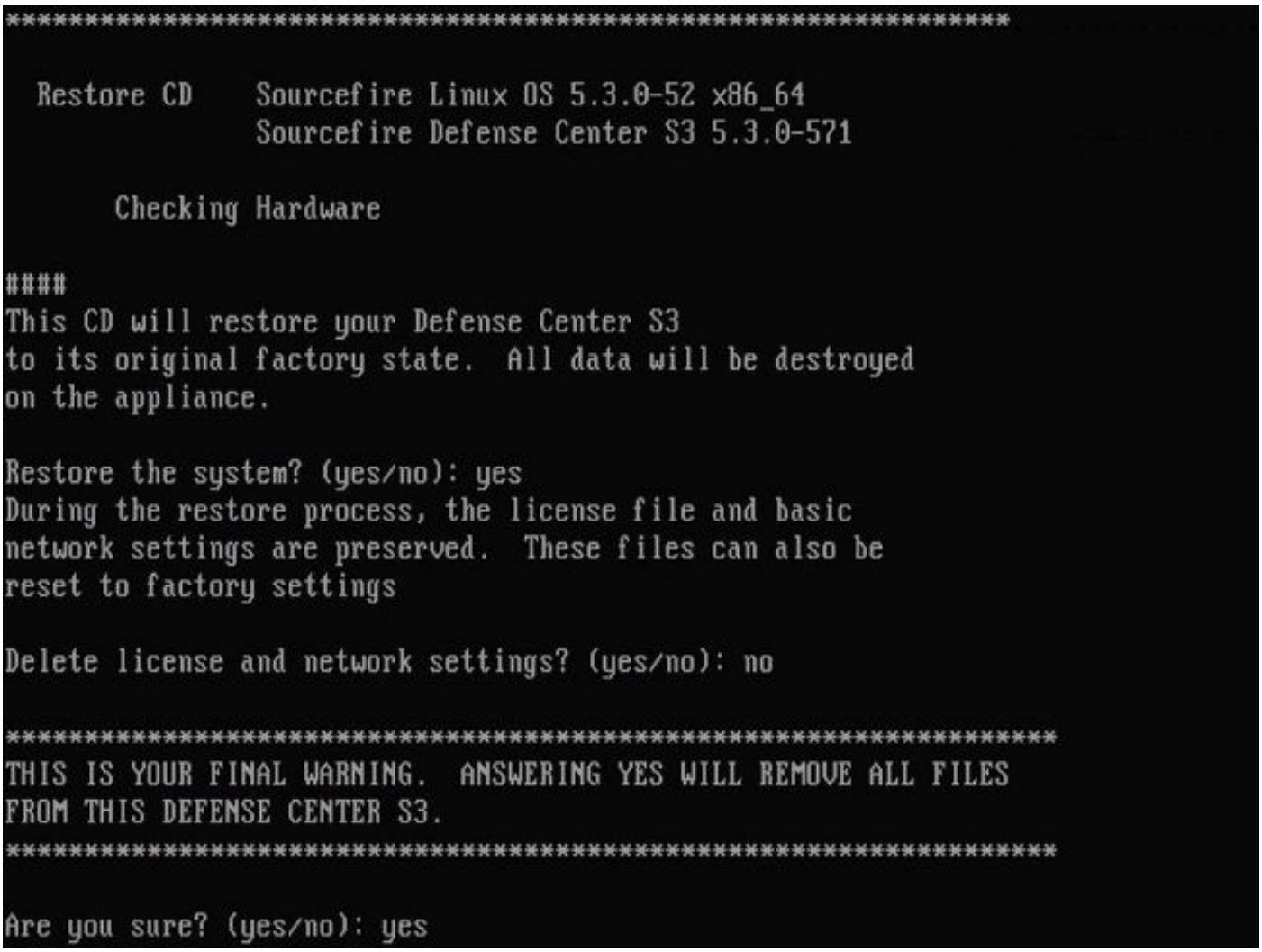

****
Restore CD Sourcefire Linux OS 5.3.0-52 x86_64
Sourcefire Defense Center S3 5.3.0-571
Checking Hardware
####
This CD will restore your Defense Center S3
to its original factory state. All data will be destroyed
on the appliance.
Restore the system? (yes/no): yes
During the restore process, the license file and basic
network settings are preserved. These files can also be
reset to factory settings
Delete license and network settings? (yes/no): no

Figura 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
Figura 29

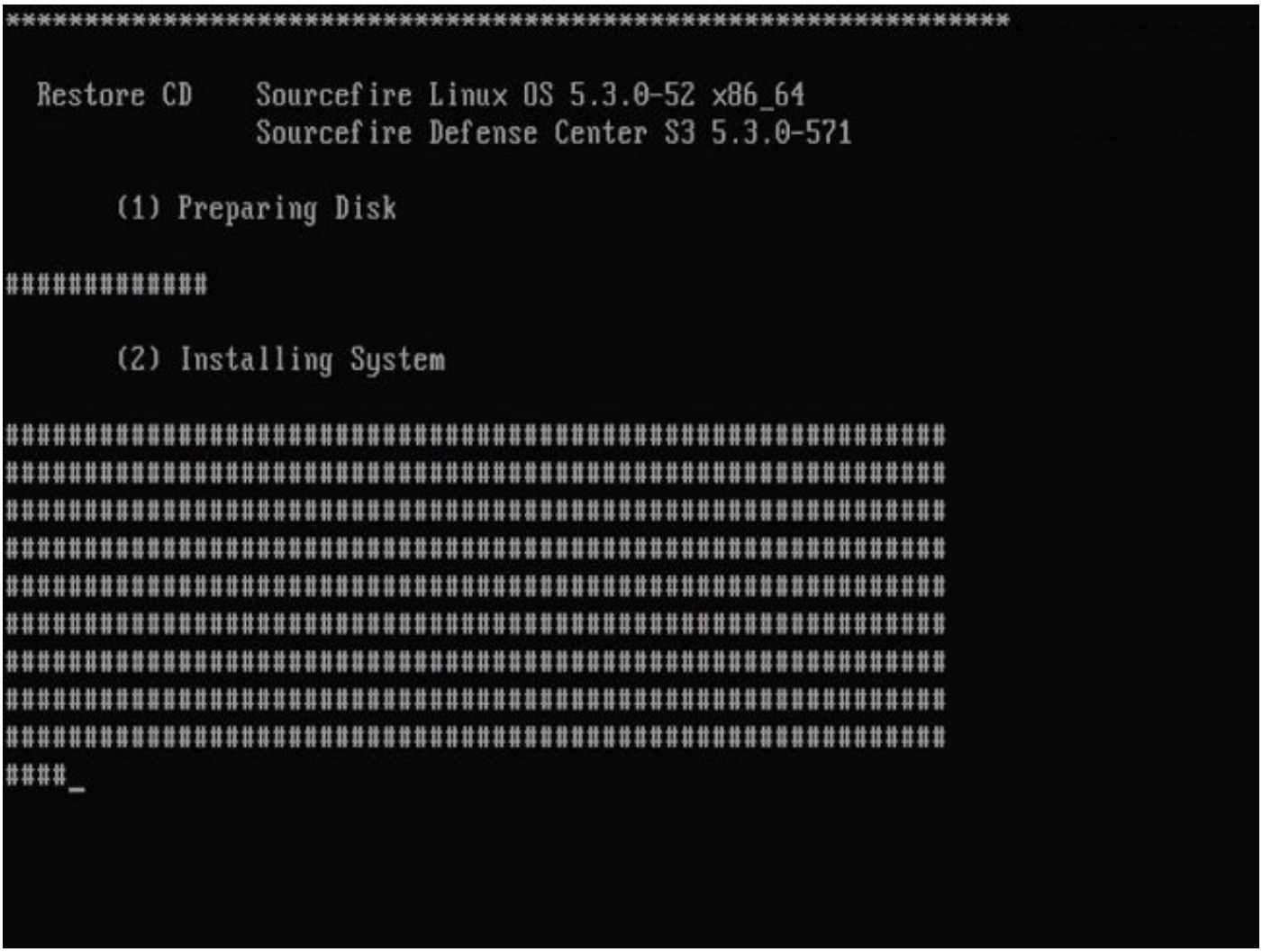

Restore CD Sourcefire Linux OS 5.3.0-52 x86_64
Sourcefire Defense Center S3 5.3.0-571
(1) Preparing Disk
(2) Installing System

Figura 30

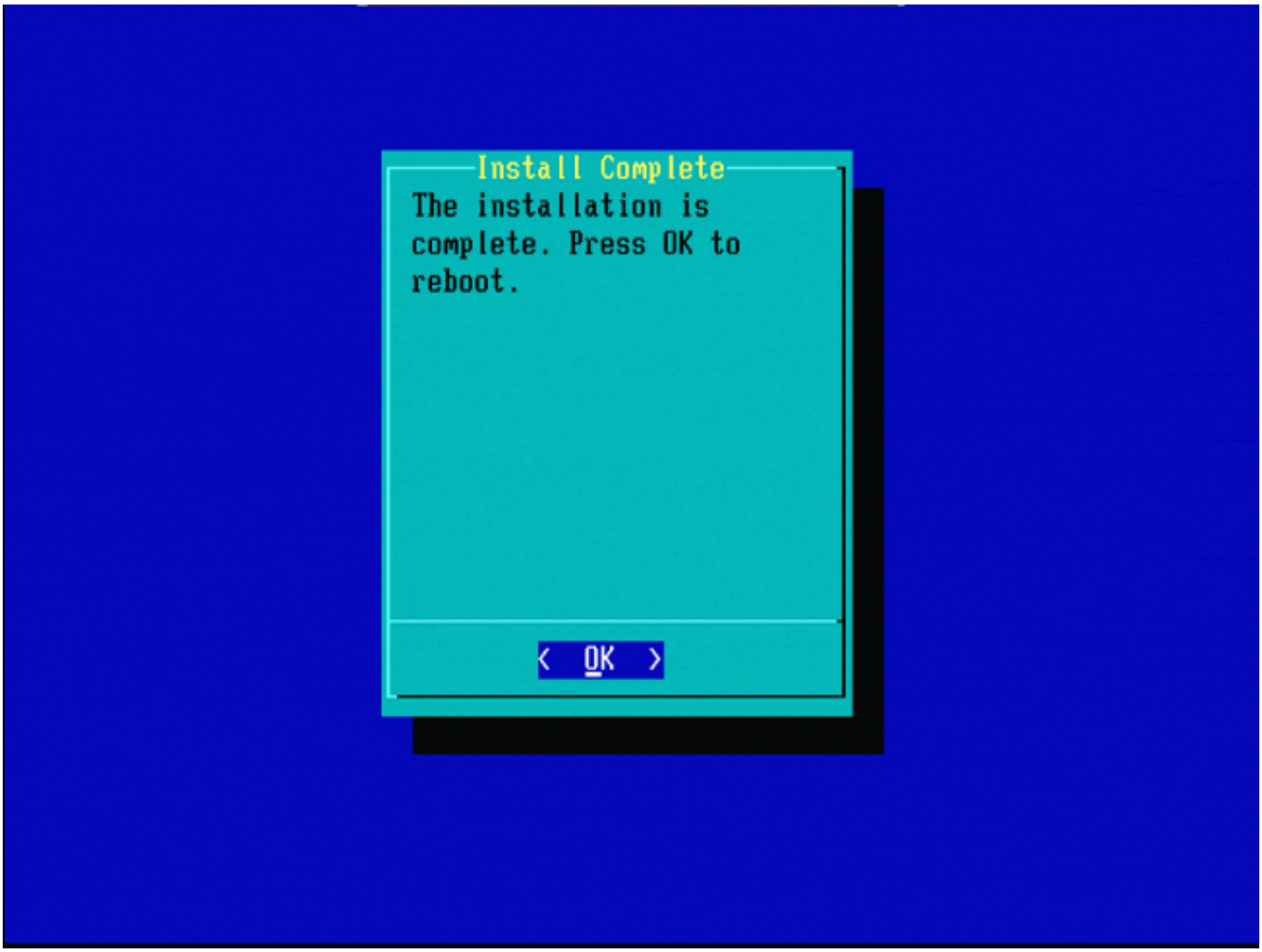

Install Complete
The installation is complete. Press OK to reboot.
< OK >

Figura 31

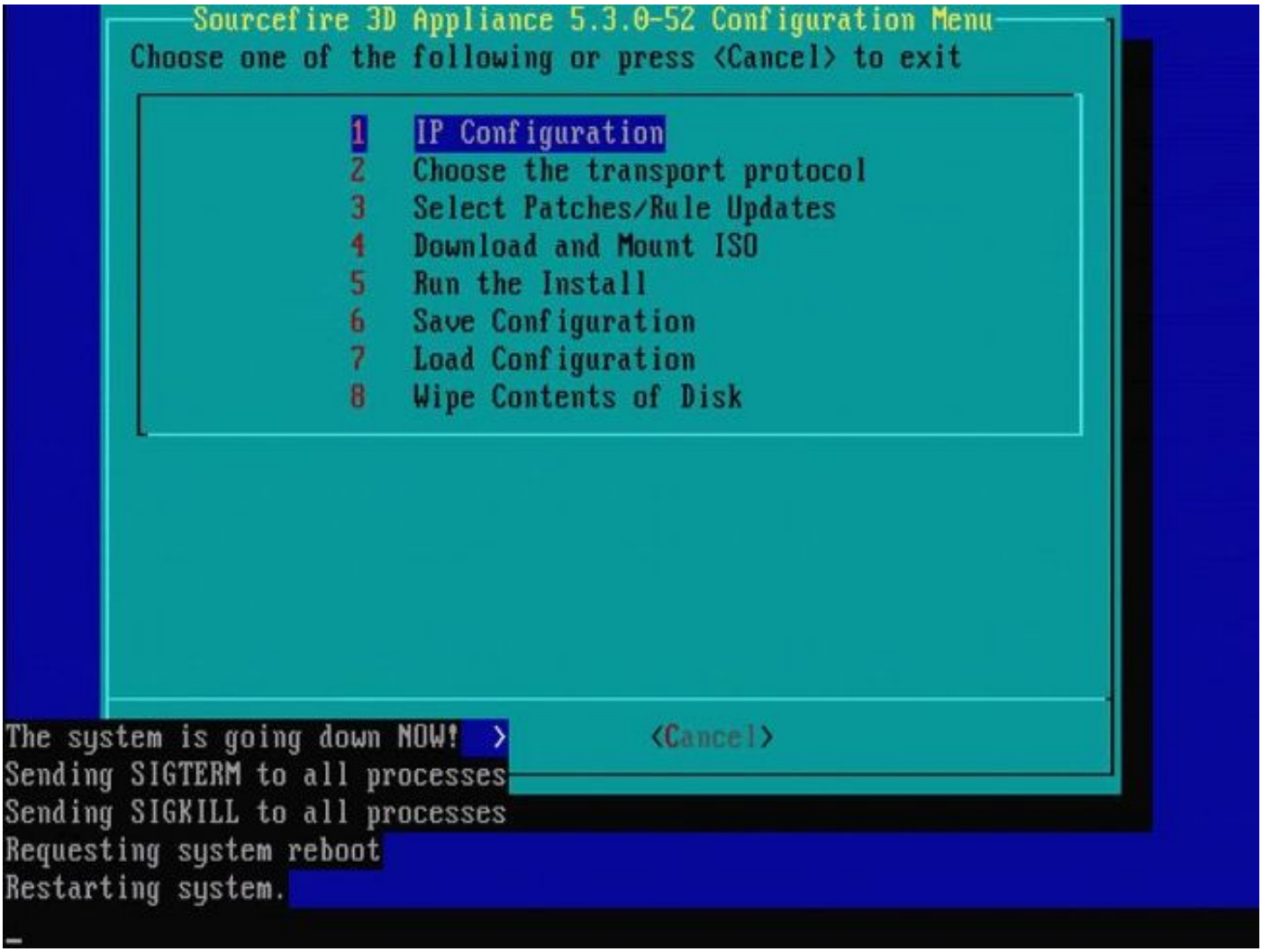


Figura 32

Cisco Firepower Management Center 1000, 2500 e 4500

Le opzioni di FMC 1000, 2500 e 4500 sono diverse. Utilizzare uno switch KVM o il CIMC e durante l'avvio del dispositivo sono disponibili le seguenti opzioni:

1 - Modalità VGA della console Cisco Firepower Management

2 - Cisco Firepower Management Console seriale

3 - Modalità Ripristino Configurazione Di Sistema Della Console Cisco Firepower Management

4 - Modalità di ripristino password della console Cisco Firepower Management

Per accedere alla modalità di ripristino con interfaccia utente, selezionare l'opzione 'Cisco Firepower Management Console System Restore Mode' (opzione 3) e quindi 'Cisco Firepower Management Console System Restore VGA Mode' (opzione 1)

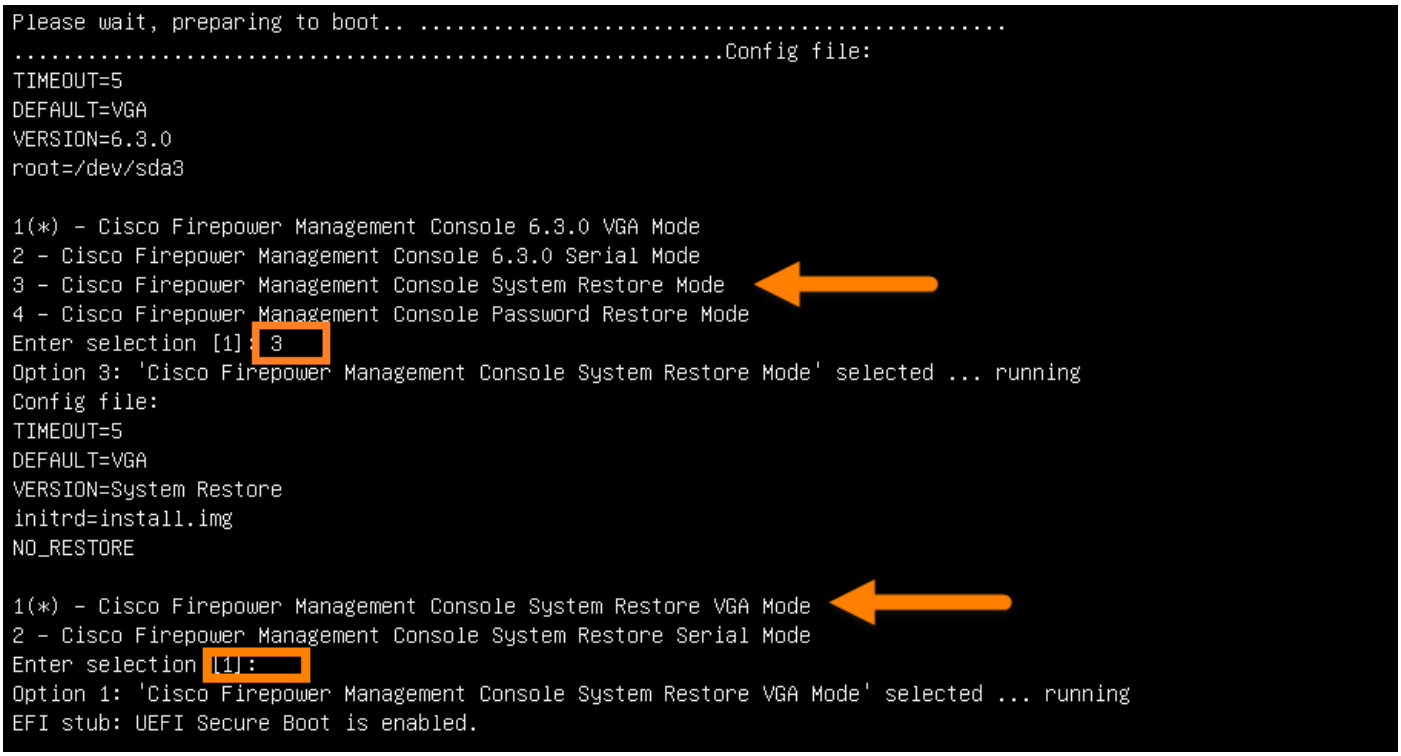


Figura 33

Il resto del processo è identico a quello di altri accessori FMC.

Risoluzione dei problemi

L'opzione di menu LILO di System_Restore non è elencata

Il centro di gestione FireSIGHT e gli accessori FirePOWER serie 7000 e 8000 dispongono di un'unità flash integrata che contiene il sistema di reimage. Se l'opzione "System_Restore" non è elencata nel menu di avvio di LILO (Linux Loader), è comunque possibile accedere a questa unità per completare la ricreazione dell'immagine.

Dispositivi 7010, 7020 e 7030

Se si usa un dispositivo della serie 70XX, attenersi alla seguente procedura per selezionare il dispositivo di avvio:

1. Spegnere l'accessorio normalmente.

2. Accendere l'accessorio e premere ripetutamente Canc durante l'avvio per accedere alla schermata di selezione del dispositivo di avvio. Vedere l'immagine qui:

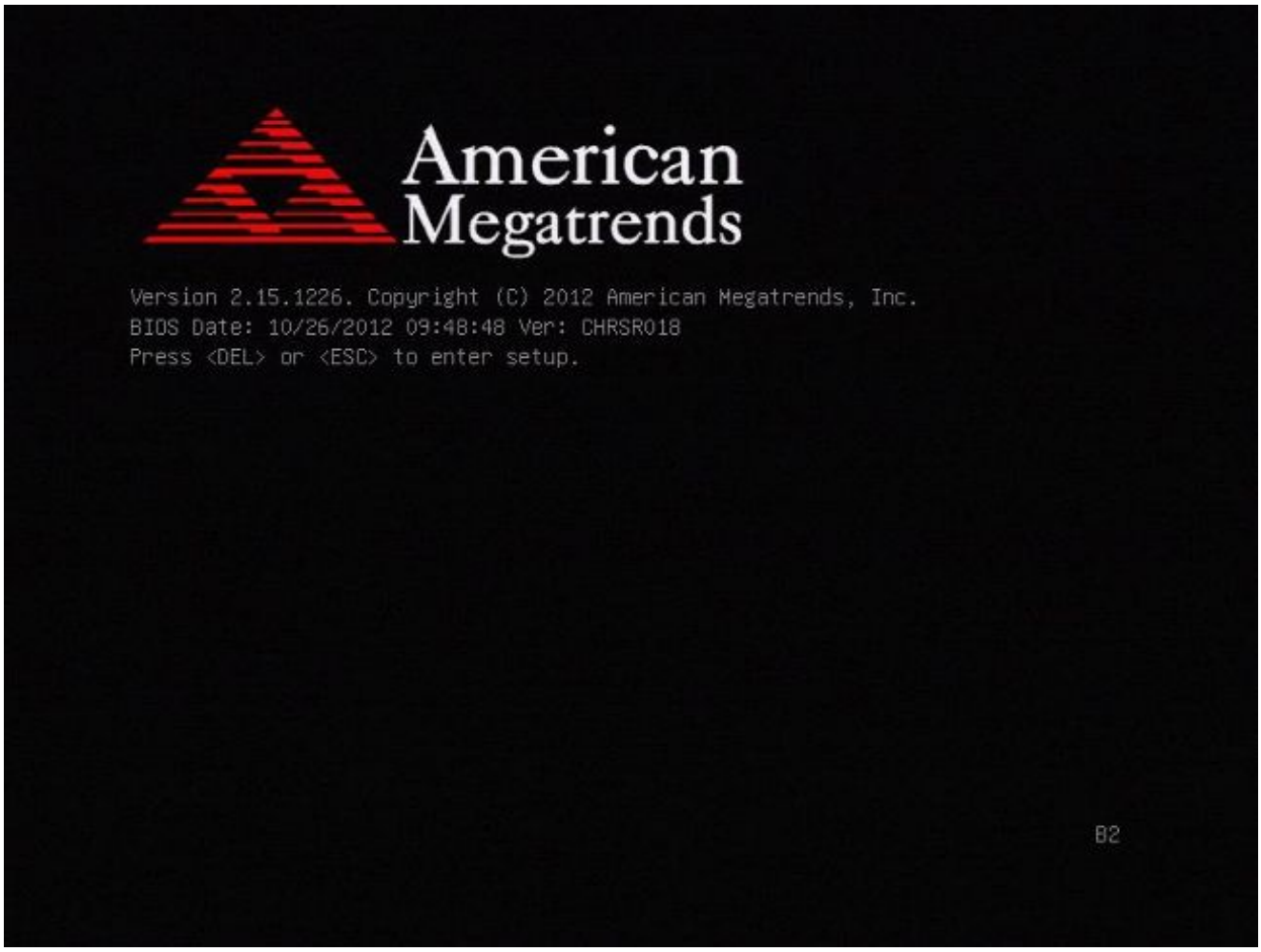

American
Megatrends
Version 2.15.1226. Copyright (C) 2012 American Megatrends, Inc.
BIOS Date: 10/26/2012 09:48:48 Ver: CHRSR018
Press <DEL> or <ESC> to enter setup.
B2

Figura A1

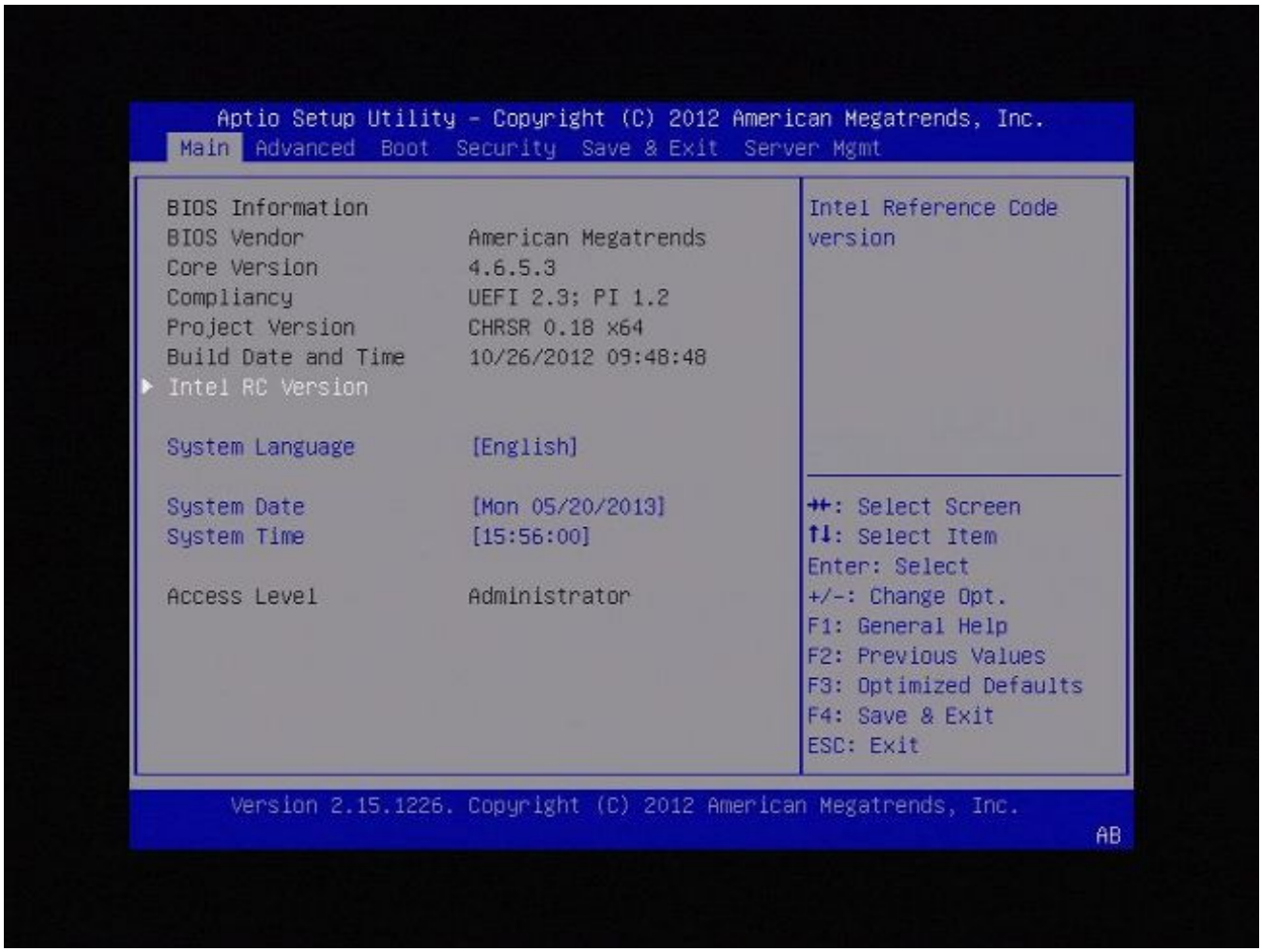


Figura A2

3. Utilizzare il tasto freccia destra per selezionare la scheda Salva ed esci. In questa scheda, usare il tasto freccia giù per selezionare SATA SM: InnoDisk. - InnoLite e premere il tasto Invio.

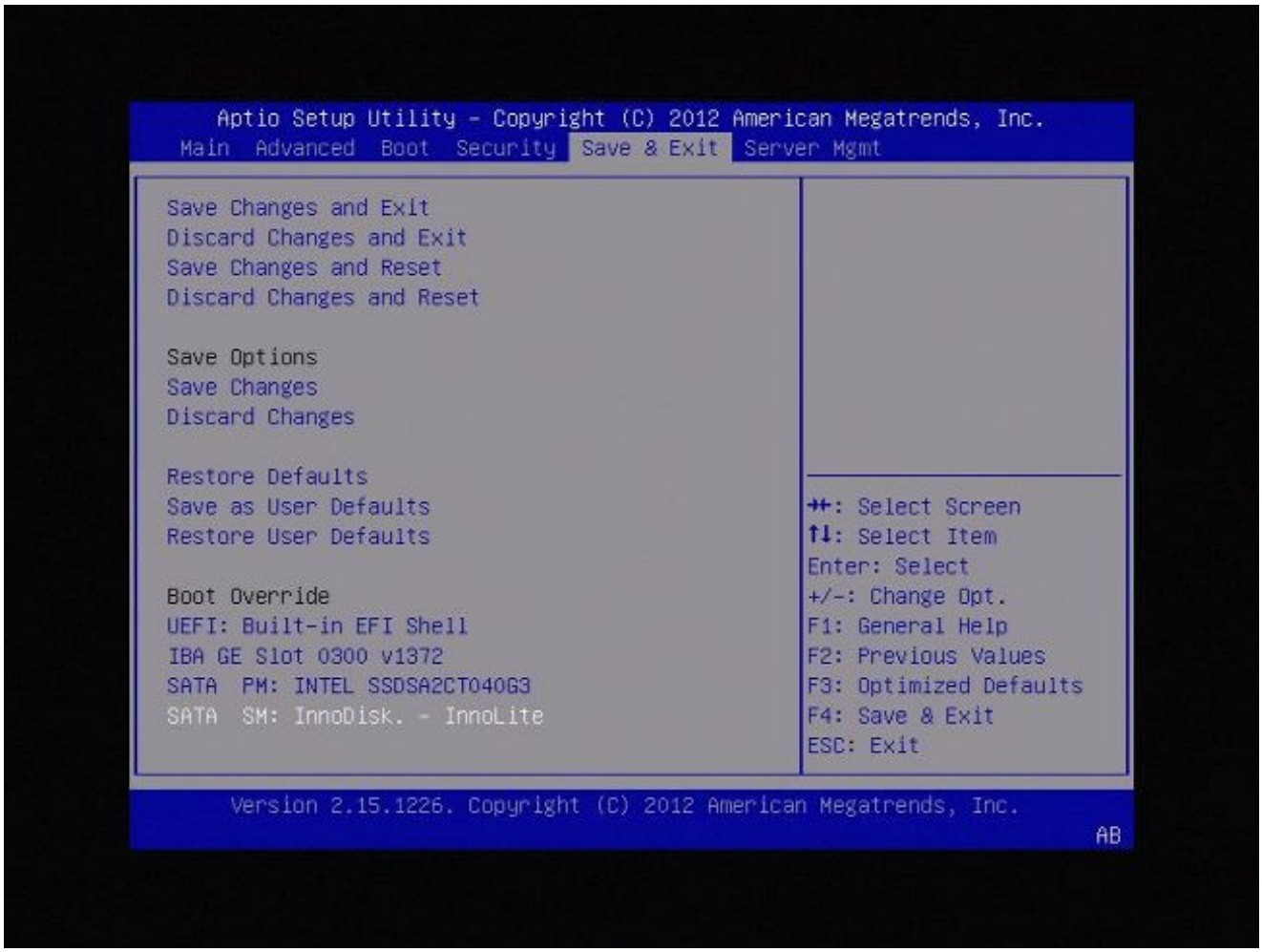


Figura A3

4. Scegliere l'opzione 0 se si utilizza una tastiera e un monitor.

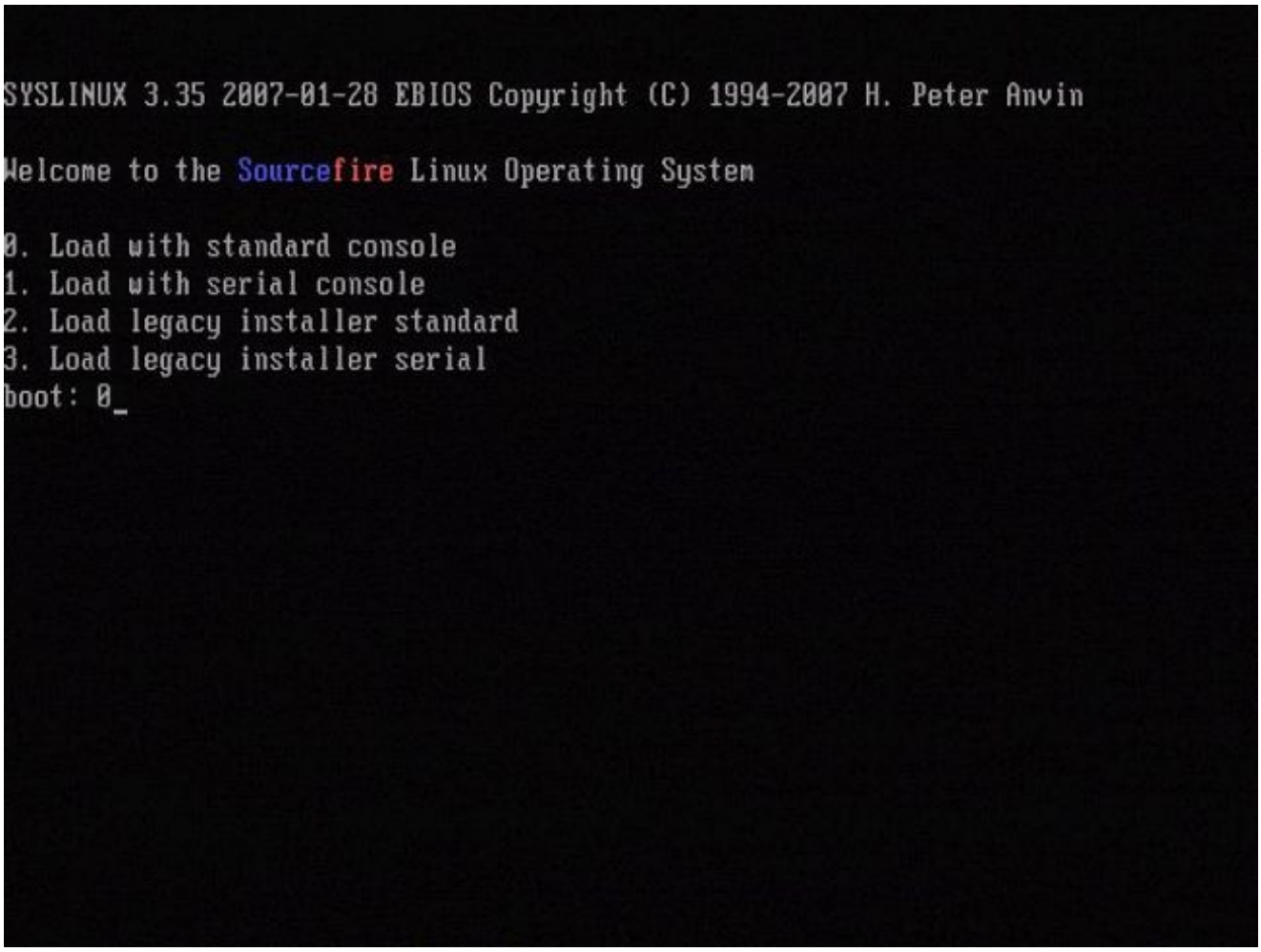

SYSLINUX 3.35 2007-01-28 EBIOS Copyright (C) 1994-2007 H. Peter Anvin
Welcome to the Sourcefire Linux Operating System
0. Load with standard console
1. Load with serial console
2. Load legacy installer standard
3. Load legacy installer serial
boot: 0_
Figura A4

Figura A5

Dispositivi 7110 e 7120

Se si usa un dispositivo della serie 71XX, attenersi alla seguente procedura per selezionare il dispositivo di avvio:

1. Spegnere l'accessorio normalmente.

2. Accendere l'accessorio e premere ripetutamente il tasto F11 durante l'avvio per accedere alla schermata di selezione del dispositivo di avvio. Vedere l'immagine mostrata di seguito:

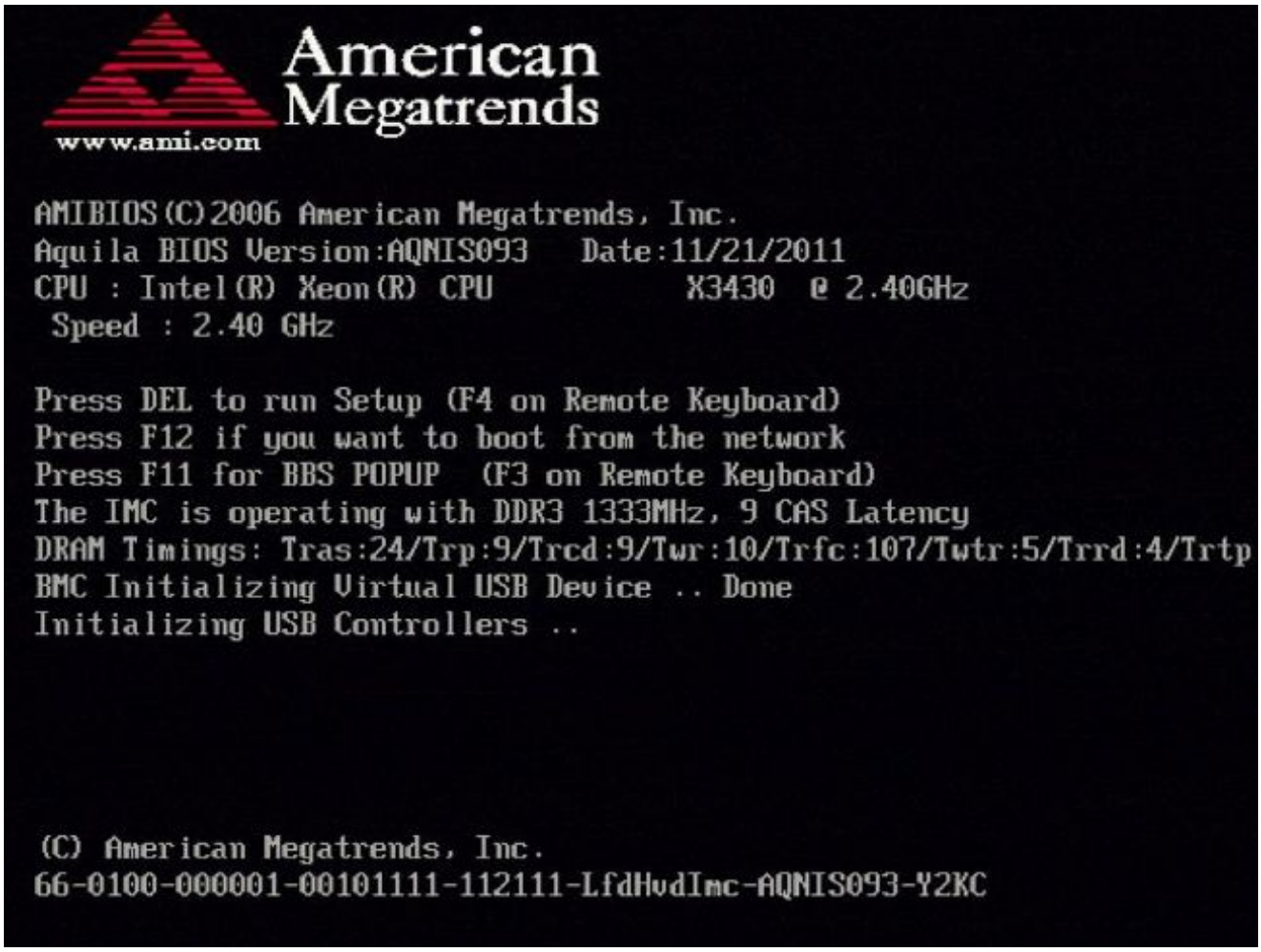


Figura B1

3. Selezionare l'opzione HDD:P1-SATADOM e premere Invio per avviare la partizione System_Restore.


Please select boot device:
HDD:P0-INTEL SSDSA2CT040G3
HDD:P1-SATADOM
Network:IBA GE Slot 0300 v1336
↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults

Figura B2

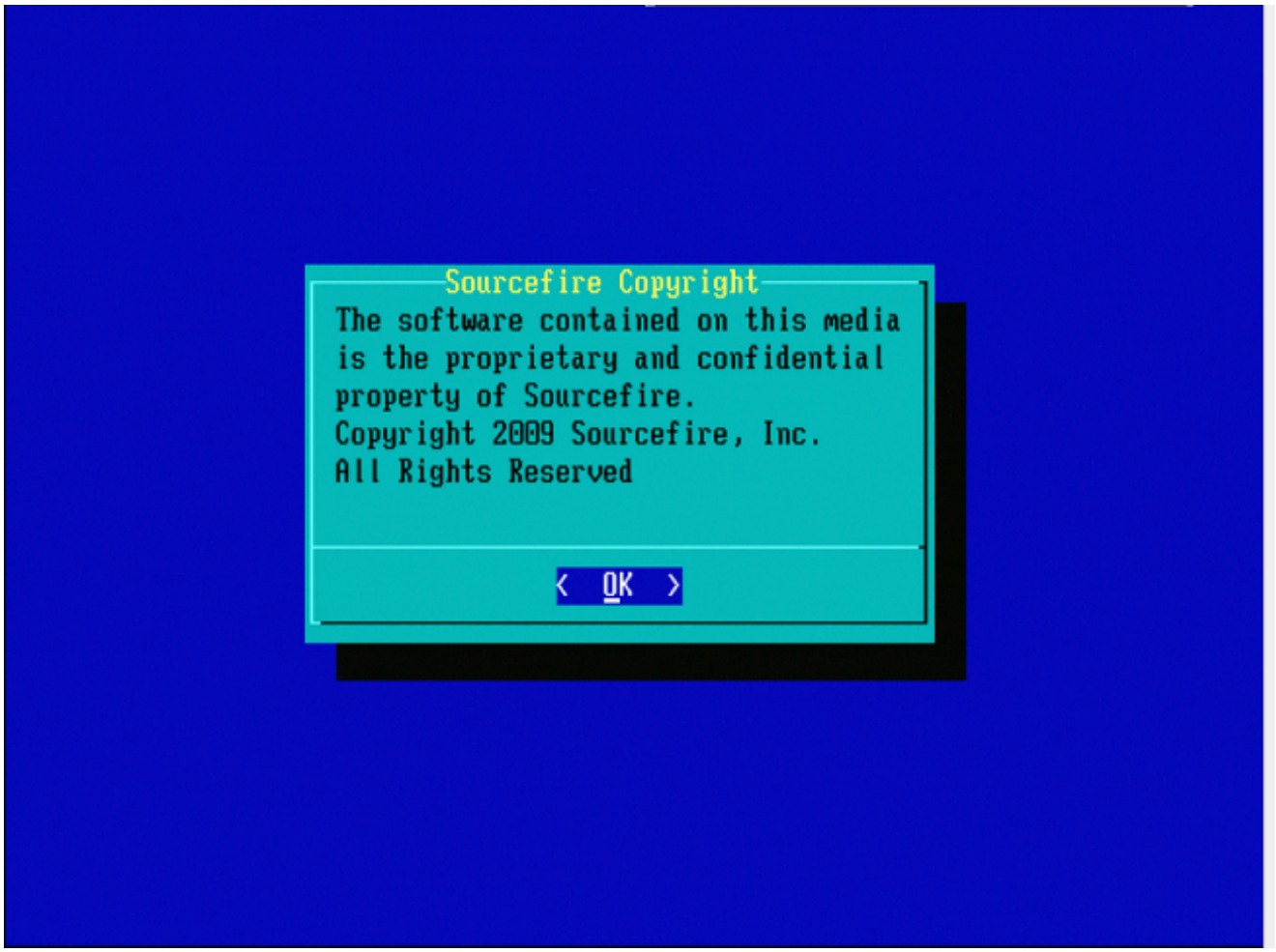


Figura B3

Dispositivi serie 8000 per Management Center modelli FS750, FS1500 o FS3500

Se si utilizza un dispositivo della serie 8000 o un modello FS750, FS1500 o FS3500 di Management Center, attenersi alla seguente procedura per selezionare il dispositivo di avvio:

1. Spegnere l'accessorio normalmente.

2. Accendere l'accessorio e premere ripetutamente il tasto F6 durante l'avvio per accedere alla schermata di selezione del dispositivo di avvio. Vedere l'immagine mostrata di seguito:

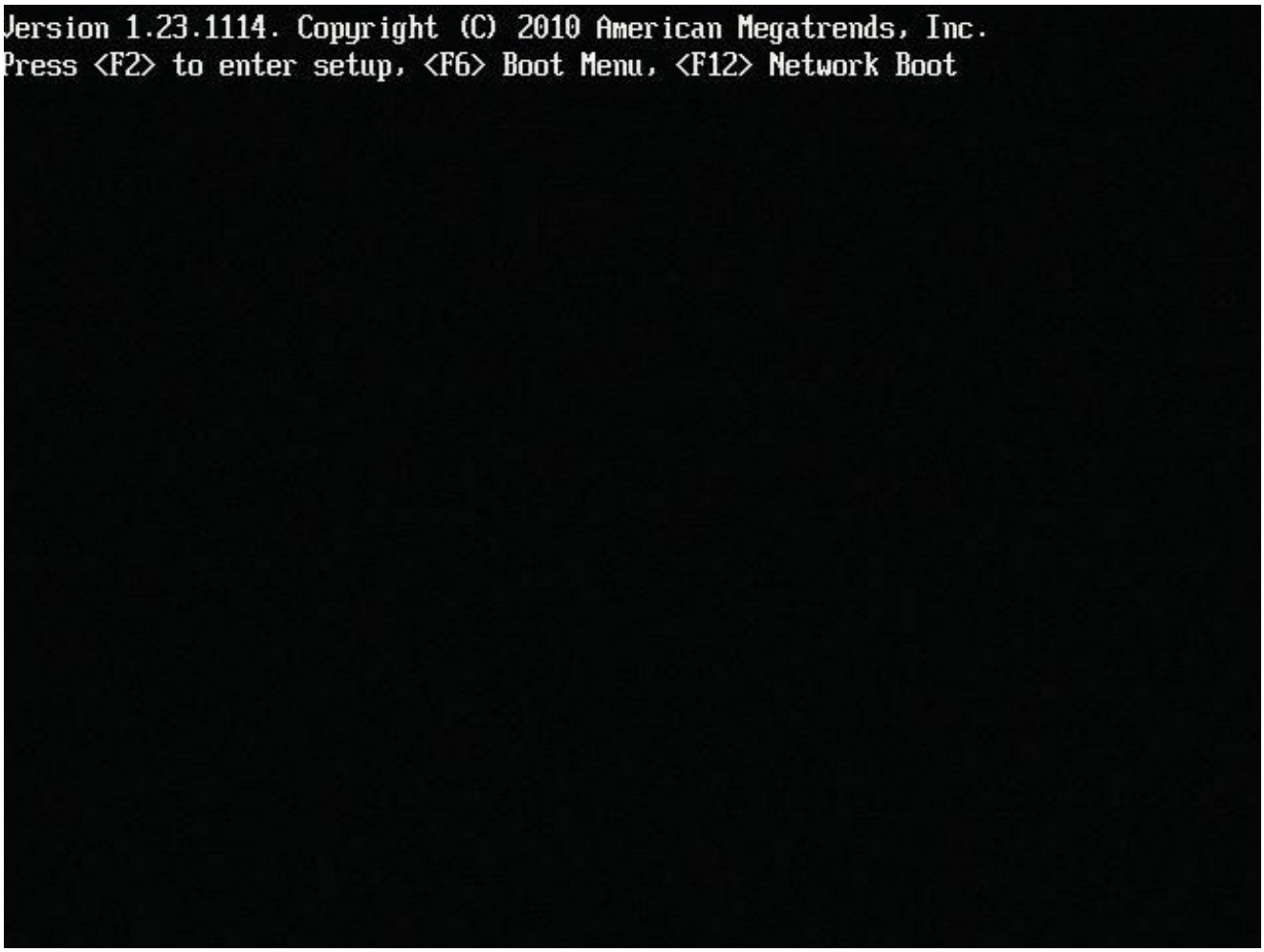


Figura C1

3. Selezionare l'opzione USB.

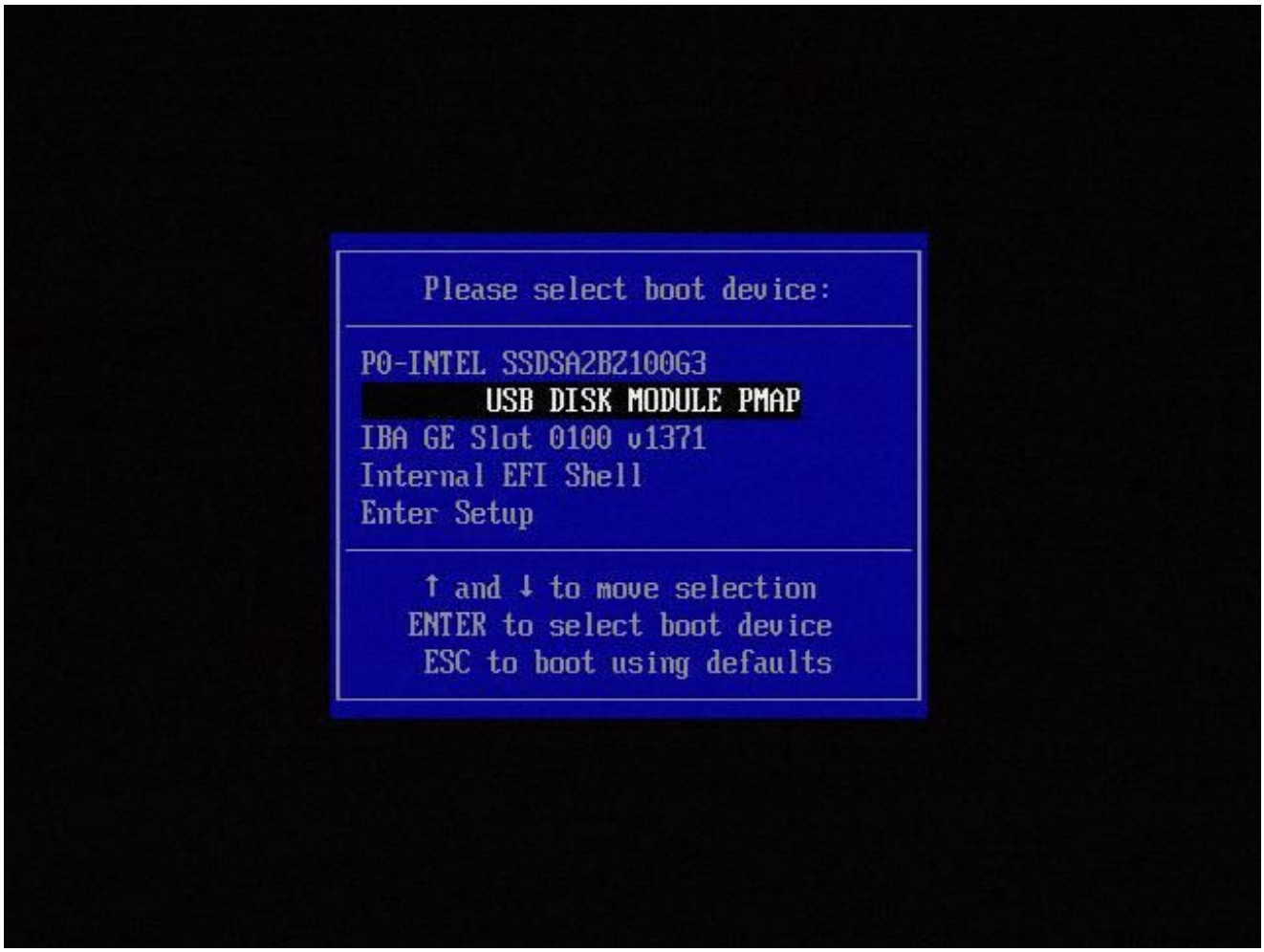


Figura C2

4. L'accessorio viene avviato dalla partizione System_Restore e viene visualizzato il menu System_Restore.

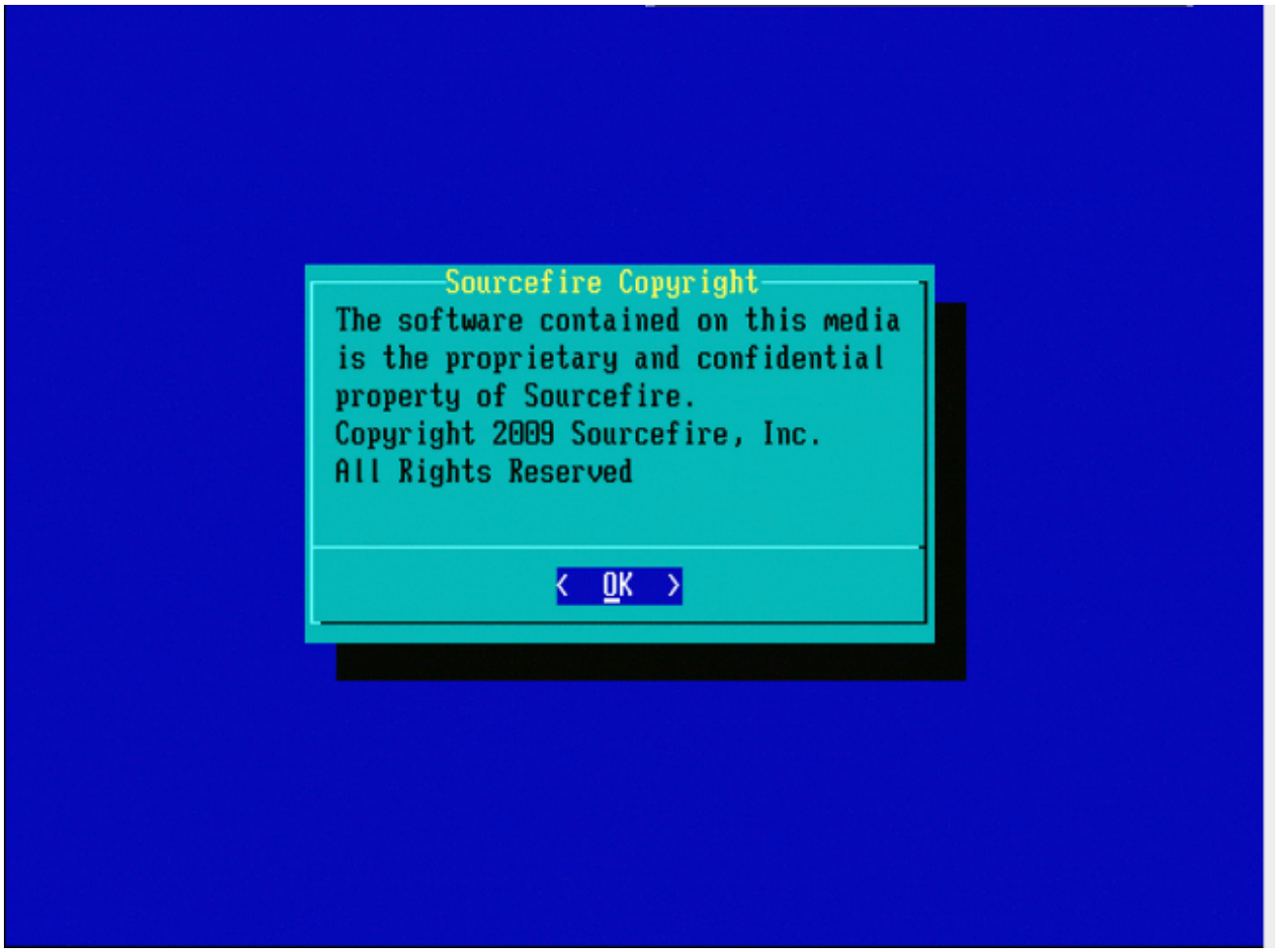


Figura C3

Ripristino del sistema per i modelli FMC1000, FMC2500, FMC4500 (FMC basati su M4)

Nota: per FMC4500 questo modello ha un menu di avvio diverso, ulteriori dettagli sono disponibili nel collegamento successivo

La richiesta di selezione di Ripristino configurazione di sistema viene visualizzata in modo diverso per i seguenti modelli: FMC1000, FMC2500, FMC4500

1. Durante l'avvio, è possibile visualizzare questa schermata per 5 secondi:

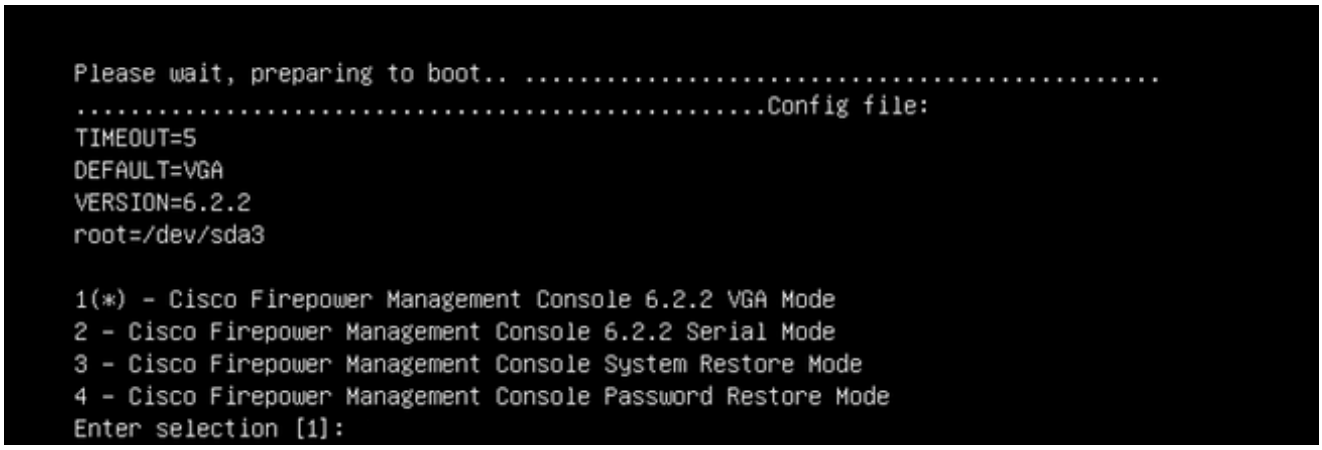


Figura D1

2. Selezionare l'opzione Ripristino configurazione di sistema (#3 in questo caso).

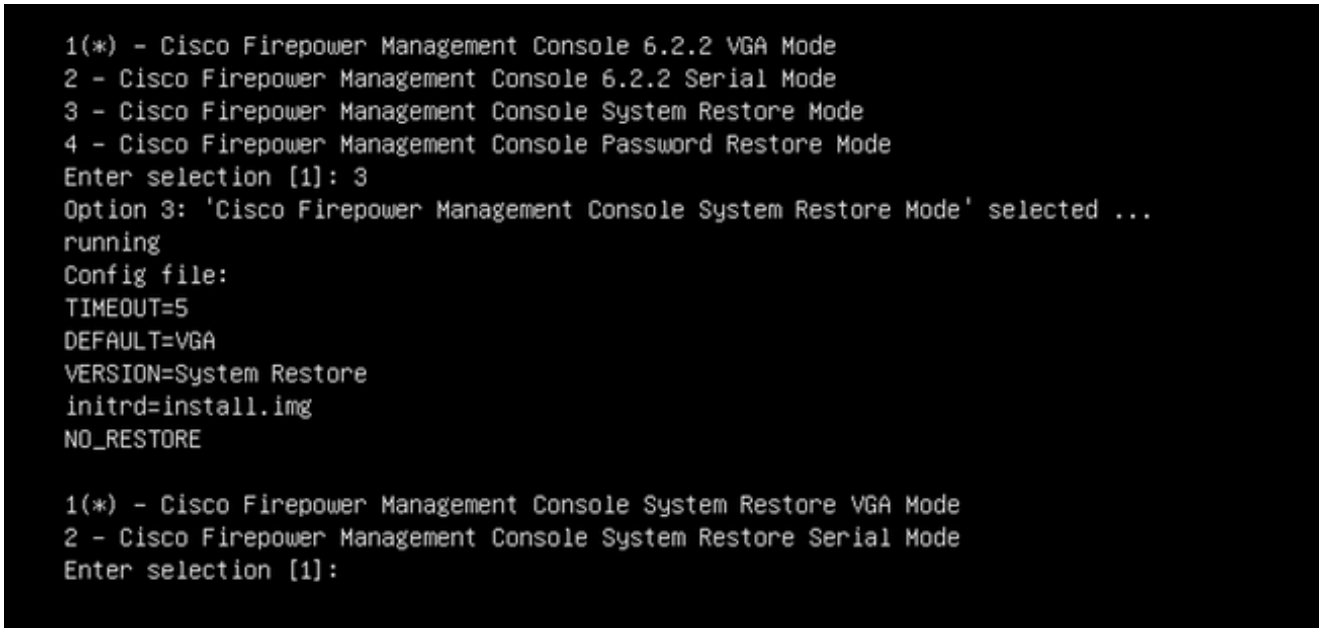


Figura D2

3. Selezionare il metodo di visualizzazione per il ripristino del sistema (in questo caso, 1 per VGA)

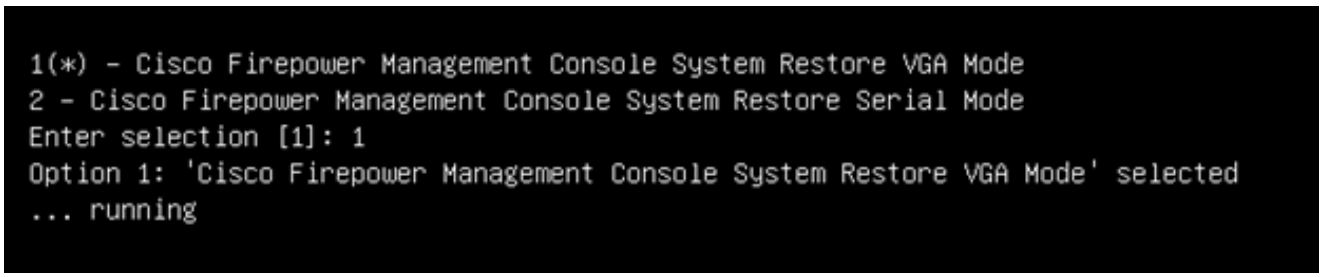


Figura D3

4. Si arriva quindi al prompt illustrato nella figura 5 e il processo continua normalmente.

Opzione di avvio non elencata

È possibile che l'opzione per l'avvio dalla partizione di ricreazione immagine non sia elencata nel BIOS o nel menu di avvio. In questo caso, l'unità che contiene il sistema di ricreazione immagine potrebbe essere mancante o danneggiata. Probabilmente è necessaria una RMA.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).