Een FireSIGHT Management Center en FirePOWER-applicatie installeren

Inhoud

Inleiding

Dit document beschrijft de processen met voorbeelden voor de procedure voor het opnieuw installeren van een image van Cisco FireSIGHT Management Center (FMC) en FirePOWER-apparaten.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

Beheerd apparaat	FireSIGHT Management Center	Beschikbare softwareversies voor Installatiekopie
Cisco FirePOWER-applicatie 7000 Series Cisco FirePOWER 7100 Series Cisco FirePOWER-applicatie 8100 Series Cisco FirePOWER-applicatie 8200 Series	FS 750 FS 1500 FS 3500	5.2 of hoger

Firepower 8300 Series Cisco Advanced Malware Protection 7150 Cisco Advanced Malware Protection 8150		5.3 of hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Installatiekopieproces

Let op: plaats geen USB-opslagapparaat of steek geen KVM-switch (Keyboard, Video and Mouse) in wanneer u een upgrade uitvoert of een nieuw image maakt van een FireSIGHT Management Center of een FirePOWER-applicatie.

Voordat u begint

1. Als u een nieuw image wilt maken van een beheercentrum of een zelfstandige firewall, wordt u aangeraden een reservekopie van uw apparaat te maken voordat u verdergaat.

2. Identificeer het model van uw sensor en gebruik de lijst met modellen in de sectie Gebruikte componenten om te verifiëren dat deze handleiding geschikt is.

3. Download de juiste installatiehandleiding en het juiste schijfbestand voor uw gewenste softwareversie van de Cisco-ondersteuningswebsite.

   Opmerking: hernoem een .iso-bestand niet

   Serveer het beeld: het .iso-bestand moet worden gekopieerd naar een host die een SSH-server uitvoert die bereikbaar is via het beheernetwerk van het apparaat dat moet worden gekopieerd.

   Opmerking: Als er geen andere SSH-server beschikbaar is, kan voor dit proces een VCC worden gebruikt.

   Controleer de integriteit van de iso: De md5sum van de bestanden wordt aan de rechterkant van de pagina ter verificatie geleverd met een md5sum hulpprogramma.

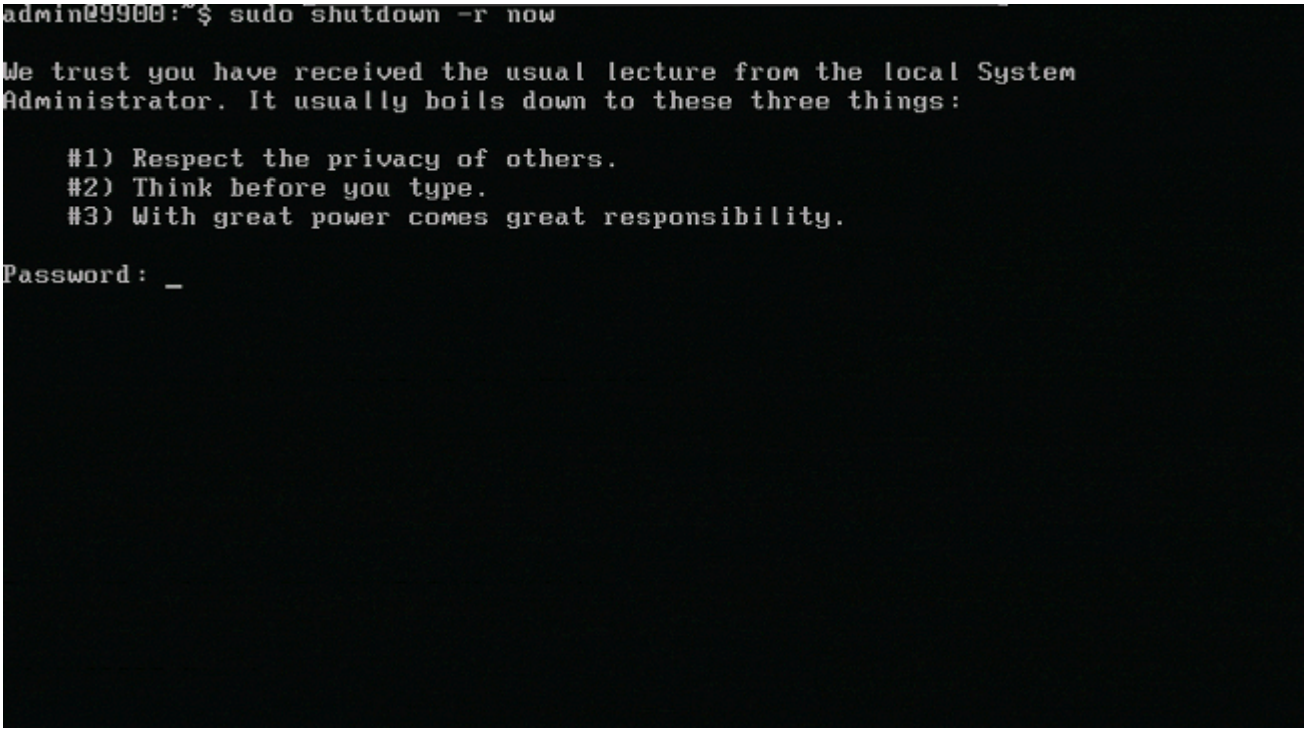
4. De installatiegidsen bevatten stapsgewijze instructies voor het opnieuw installeren van een afbeelding en bevatten ook verschillende methoden voor het opnieuw installeren van een afbeelding. De afbeeldingen in dit document kunnen ter referentie worden gebruikt.

Overzicht van het herstelproces

Opmerking: De versie 5.3 werd gebruikt om de afbeeldingen in dit artikel op te nemen. Het reimage-proces is identiek voor andere 5.x-versies, met uitzondering van de versienummers die in de getoonde

---

afbeeldingen worden weergegeven.



Afbeelding 1

Afbeelding 2 - Wanneer het systeem opnieuw opgestart wordt, drukt u op een pijltjestoets op het toetsenbord om het aftellen te stoppen en de optie **System_Restore** te kiezen voor het volgende scherm dat wordt

weergegeven.

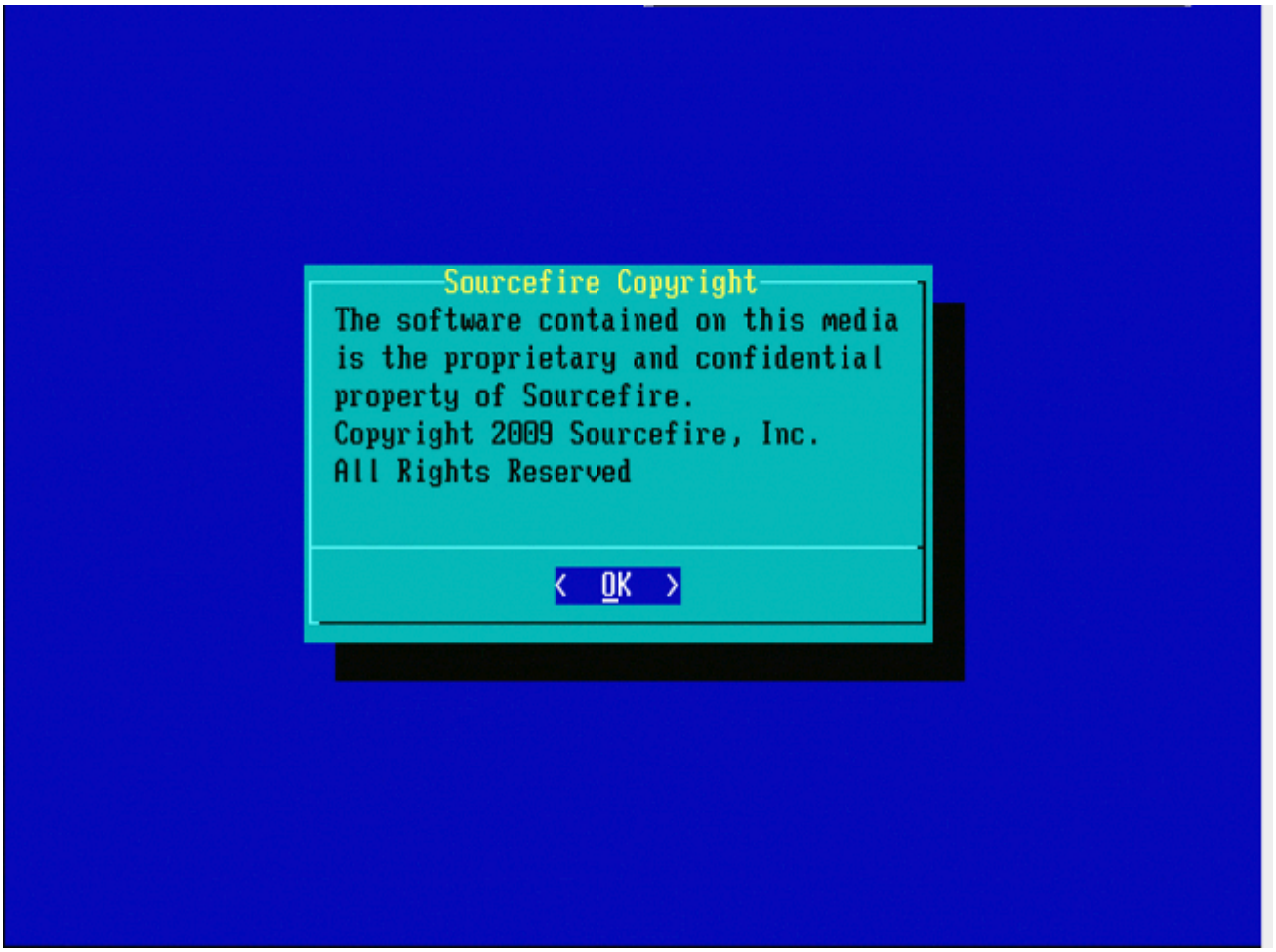
Opmerking: Als de prompt **System_Restore** niet wordt weergegeven, moet u de opstartvolgorde wijzigen om direct op te starten in de herstelpartitie (DOM). Zie Systeemherstel LILO menuoptie ontbreekt voor meer informatie.

Afbeelding 3

Afbeelding 4 - Kies optie **0** als u een toetsenbord en monitor gebruikt.

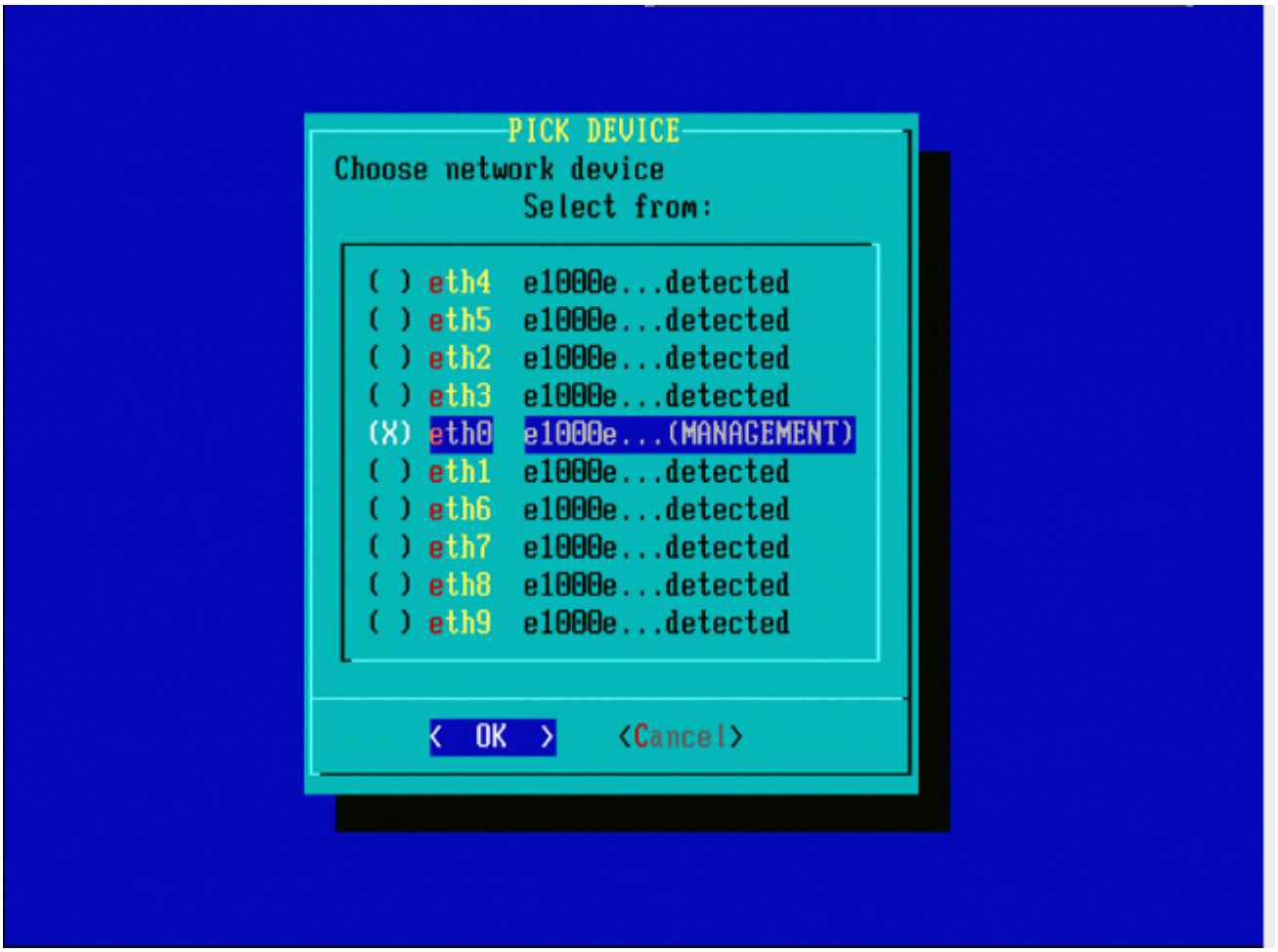
> **Opmerking**: soms is gezien dat het menu voor de optie Terugzetten alleen wordt weergegeven wanneer alleen de console is aangesloten (met het toetsenbord losgekoppeld). Zodra de hersteloptie is geselecteerd, kan het toetsenbord weer worden aangesloten

---

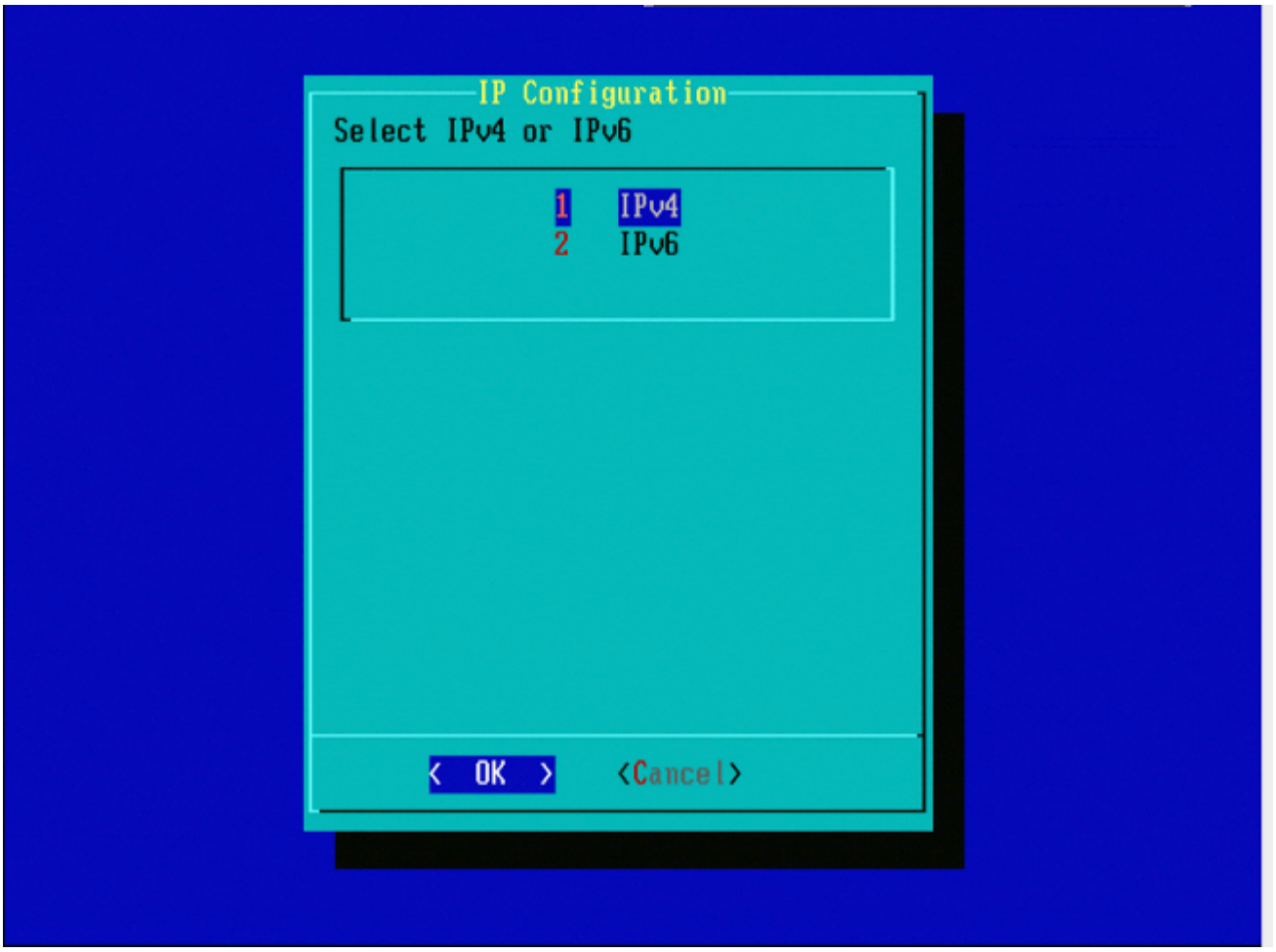


Afbeelding 5

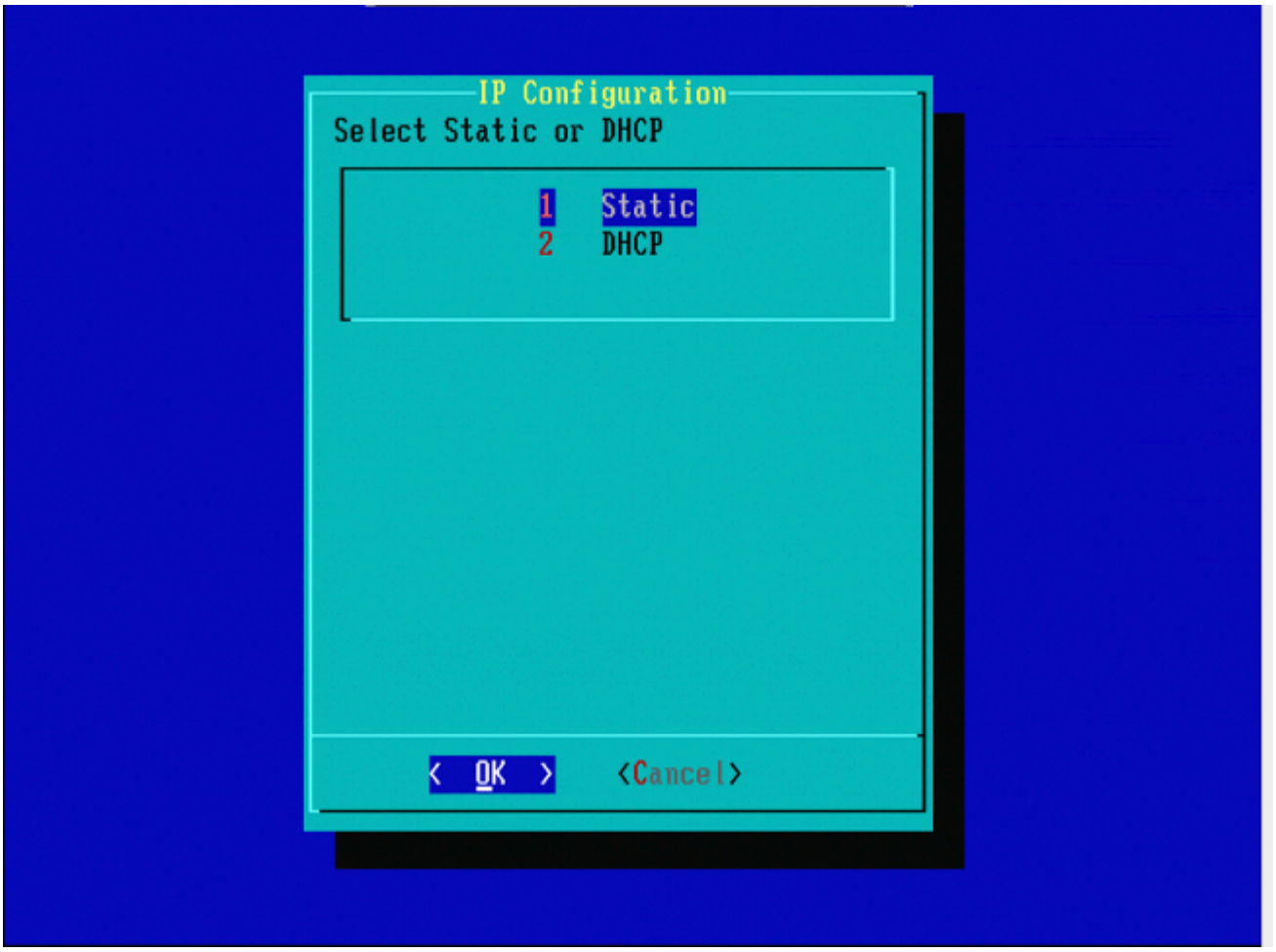
Afbeelding 6



Afbeelding 7 - Druk op de spatiebalk om het netwerkapparaat te selecteren.



Afbeelding 8



Afbeelding 9

Afbeelding 10

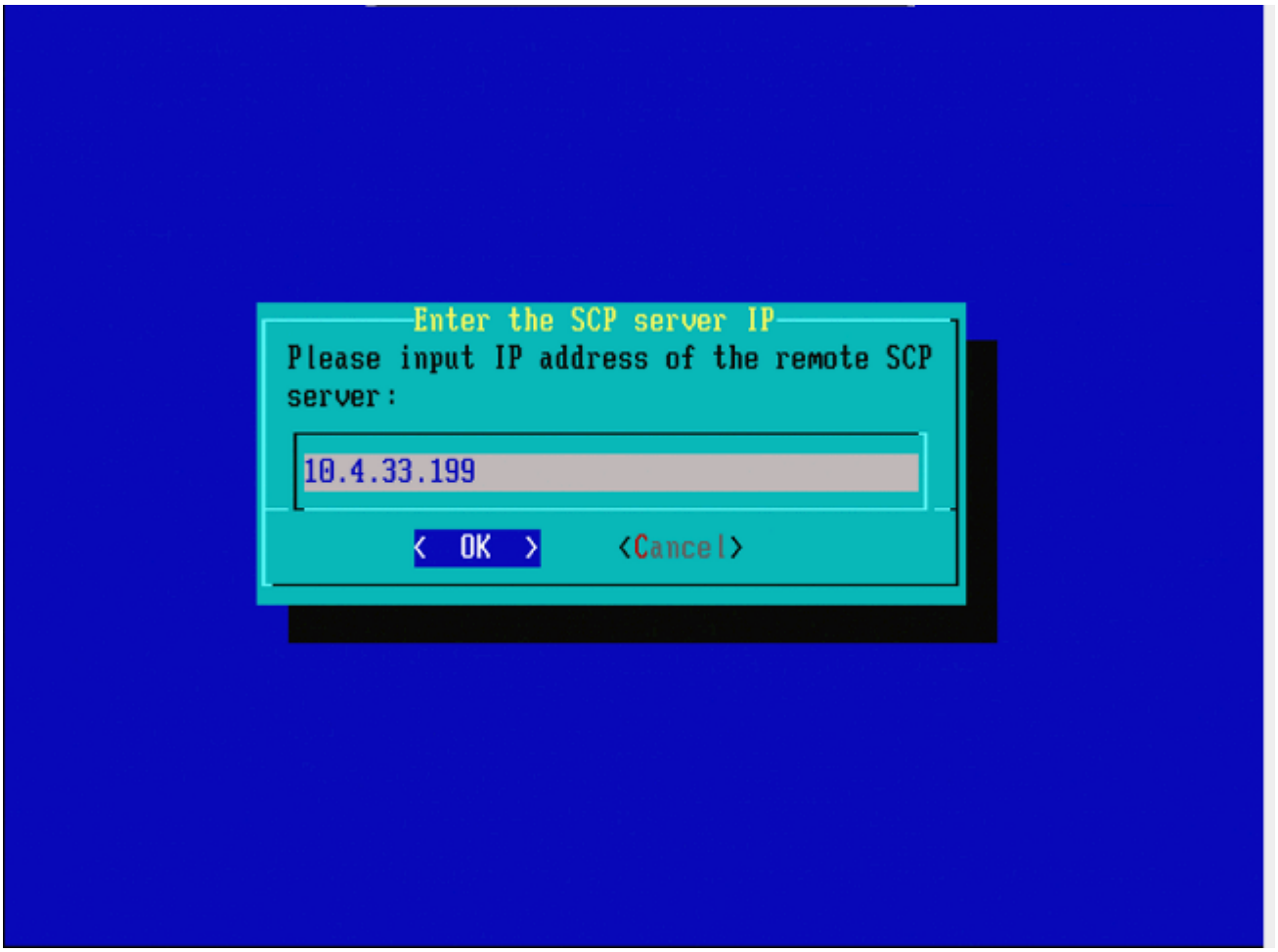
Afbeelding 11

Afbeelding 12

Afbeelding 13

Afbeelding 14

Afbeelding 15 - Cisco-ondersteuning raadt u aan het protocol Secure Copy (SCP) te gebruiken.



Afbeelding 16 - Het is mogelijk om een FireSIGHT Management Center als SCP-server te gebruiken voor deze stap. Ga door met deze procedure en gebruik het IP-adres en de referenties voor het Management Center om de velden in het menu **Systeemherstel te** vullen. Meer informatie in

Een Secure Copy (SCP)-server wordt gebruikt om bestanden veilig over te dragen. Indien Indien nodig kan een Sourcefire Defense Center (DC) worden gebruikt als een SCP-server om bestanden naar een ander Sourcefire-apparaat over te brengen. Dit kan handig zijn wanneer een iso-afbeelding moet worden overgebracht naar een Sourcefire-apparaat voor afbeeldingsdoeleinden, maar de reguliere SCP-server is onbereikbaar of niet beschikbaar.

Stap 1. Download een geschikt .iso-bestand naar uw bureaublad vanuit het Sourcefire Support Portal.
Stap 2. Gebruik een SCP client, kopieer het bestand van het bureaublad naar het Defence Center.

> **Tip**: Een SCP client is meestal beschikbaar in een Linux of Mac Operating System. In Windows-besturingssysteem kunt u echter een SCP-clientsoftware van derden installeren. Sourcefire geeft geen aanbevelingen of ondersteuning om specifieke SCP-clientsoftware te installeren.

Het volgende voorbeeld laat zien hoe je een Sourcefire .iso beeldbestand kopieert van de Downloads directory van een Linux systeem naar de **/var/tmpdirectory** van het Sourcefire Defence Center:

<#root>

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

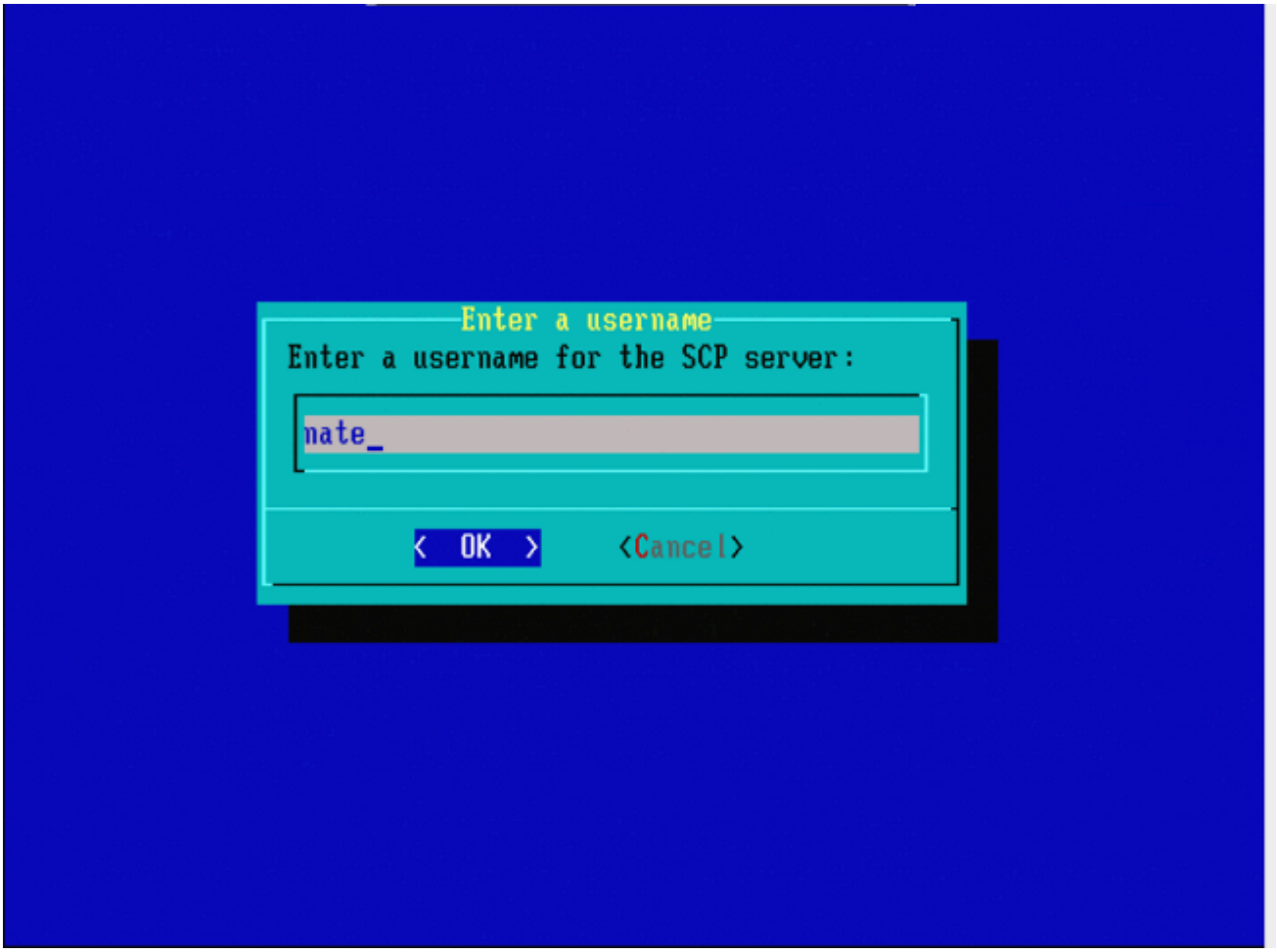
user_name

```
@
IP_Address_of_Defense_Center
:/var/tmp
```

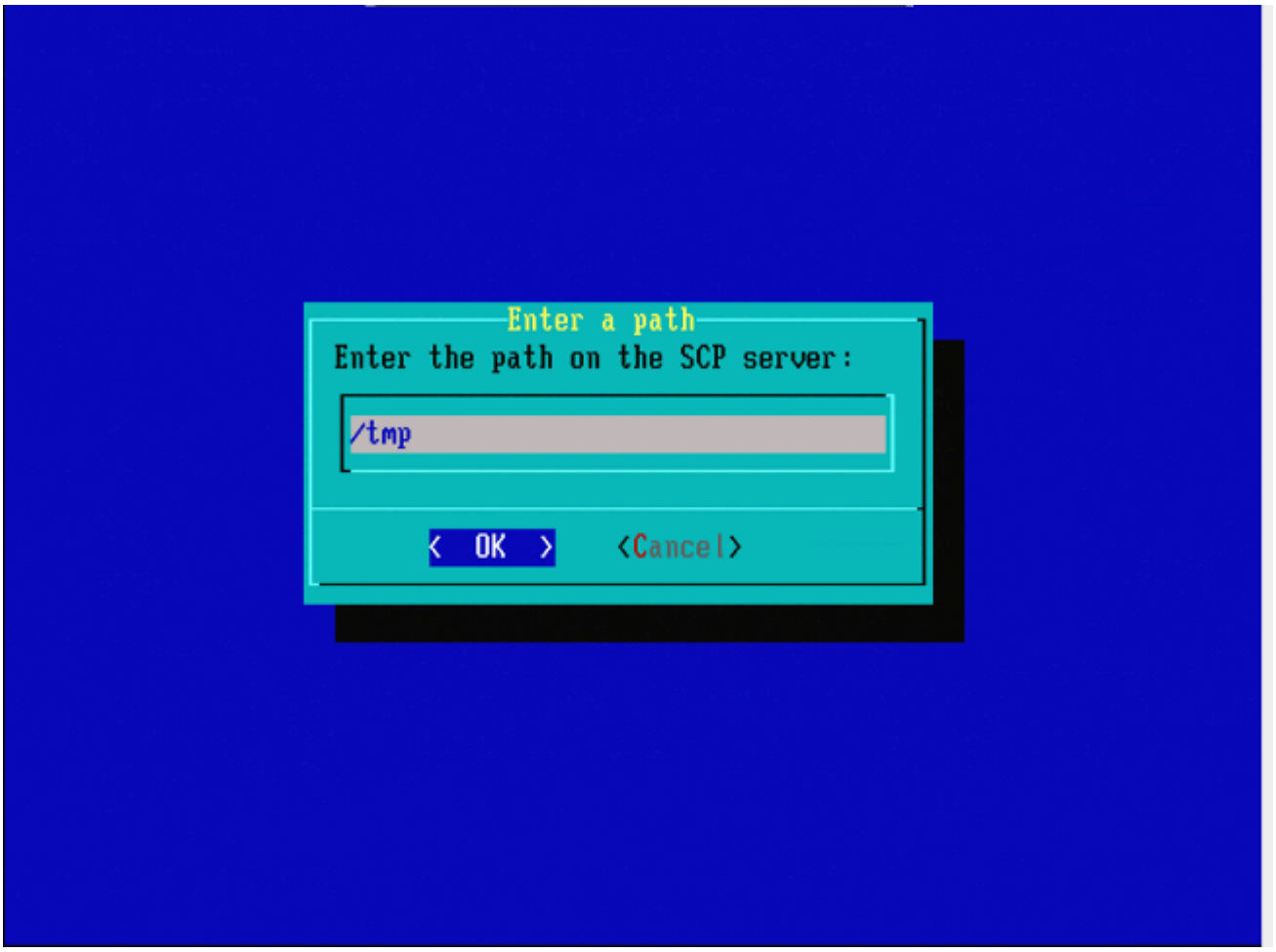
Waarschuwing: Wijzig de naam van het .iso-bestand niet. Het kan een probleem met de detectie van het bestand tijdens een reimage maken.

Nu wordt het bestand gekopieerd naar het Defence Center. U kunt doorgaan met het opnieuw image maken van Sourcefire-apparaten. Bij het opnieuw image, indien nodig, kunt u het IP-adres en de gebruikersnaam van de DC en het pad waar u het afbeeldingsbestand met de vorige instructies hebt gekopieerd, opgeven.

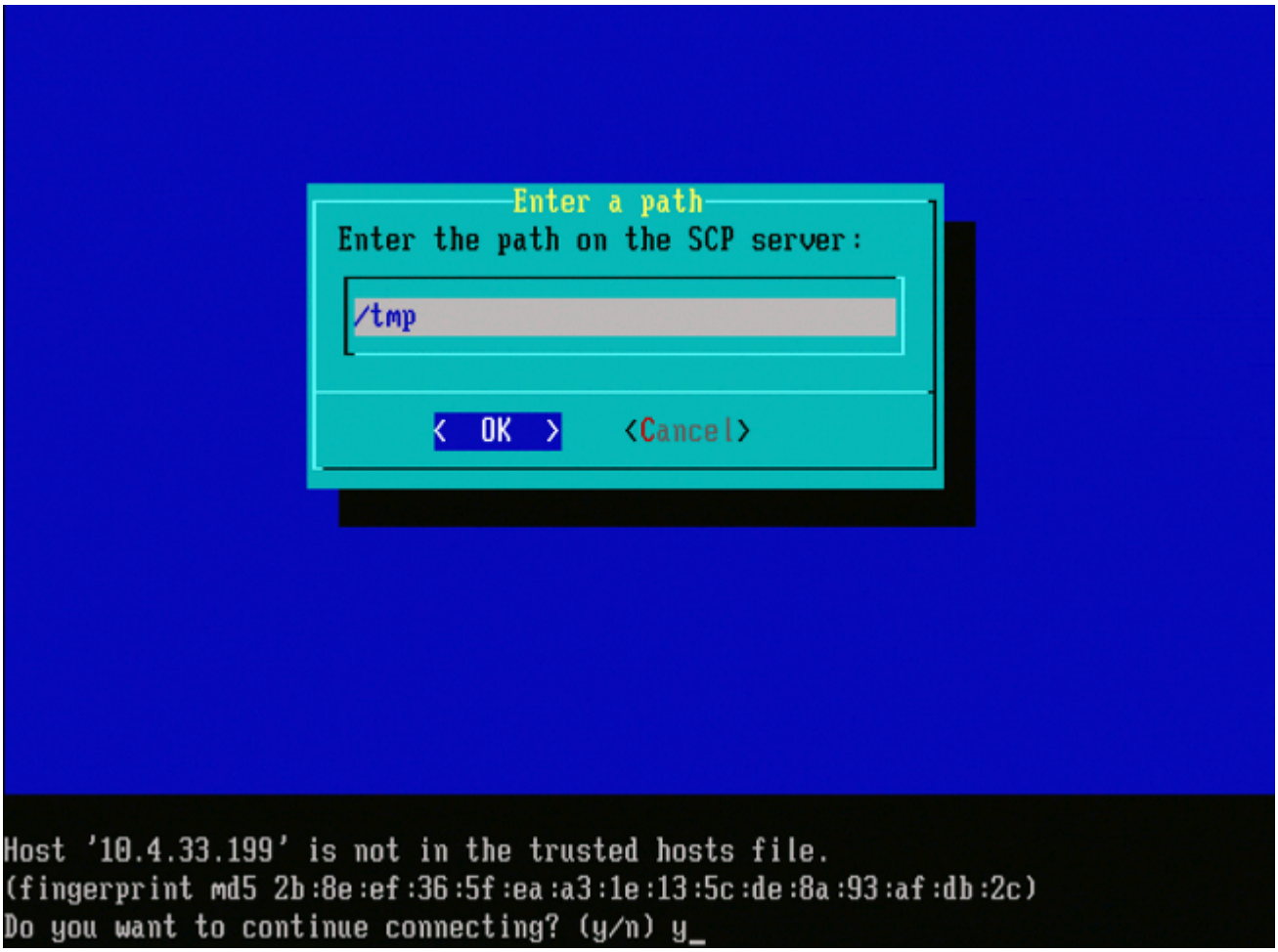
Waarschuwing: nadat de installatiekopie is voltooid, moet u het .iso-bestand uit de **/var/tmp**-map van het Defense Center verwijderen om het gebruik van de schijfruimte te beperken.



Afbeelding 17

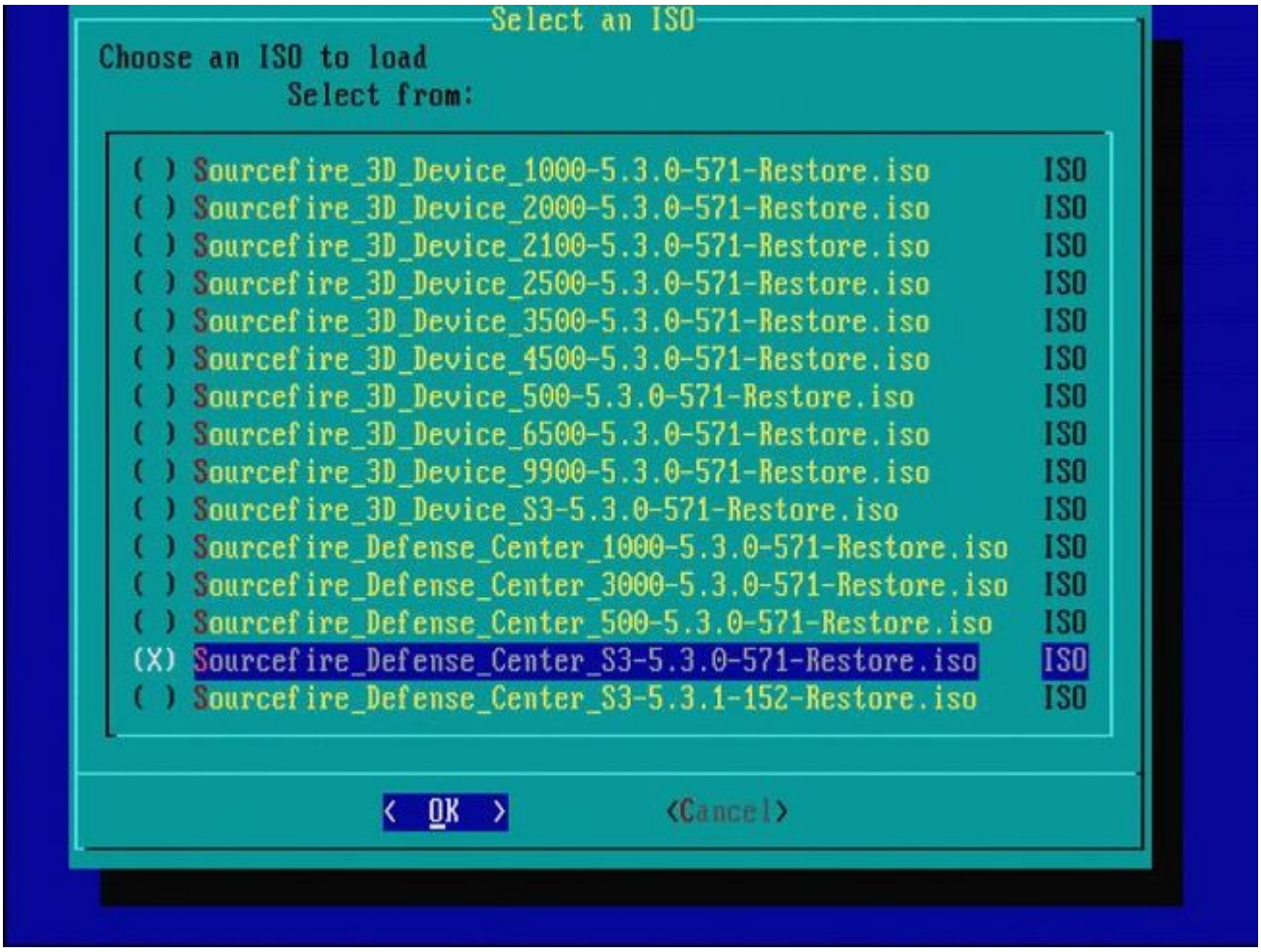


Afbeelding 18



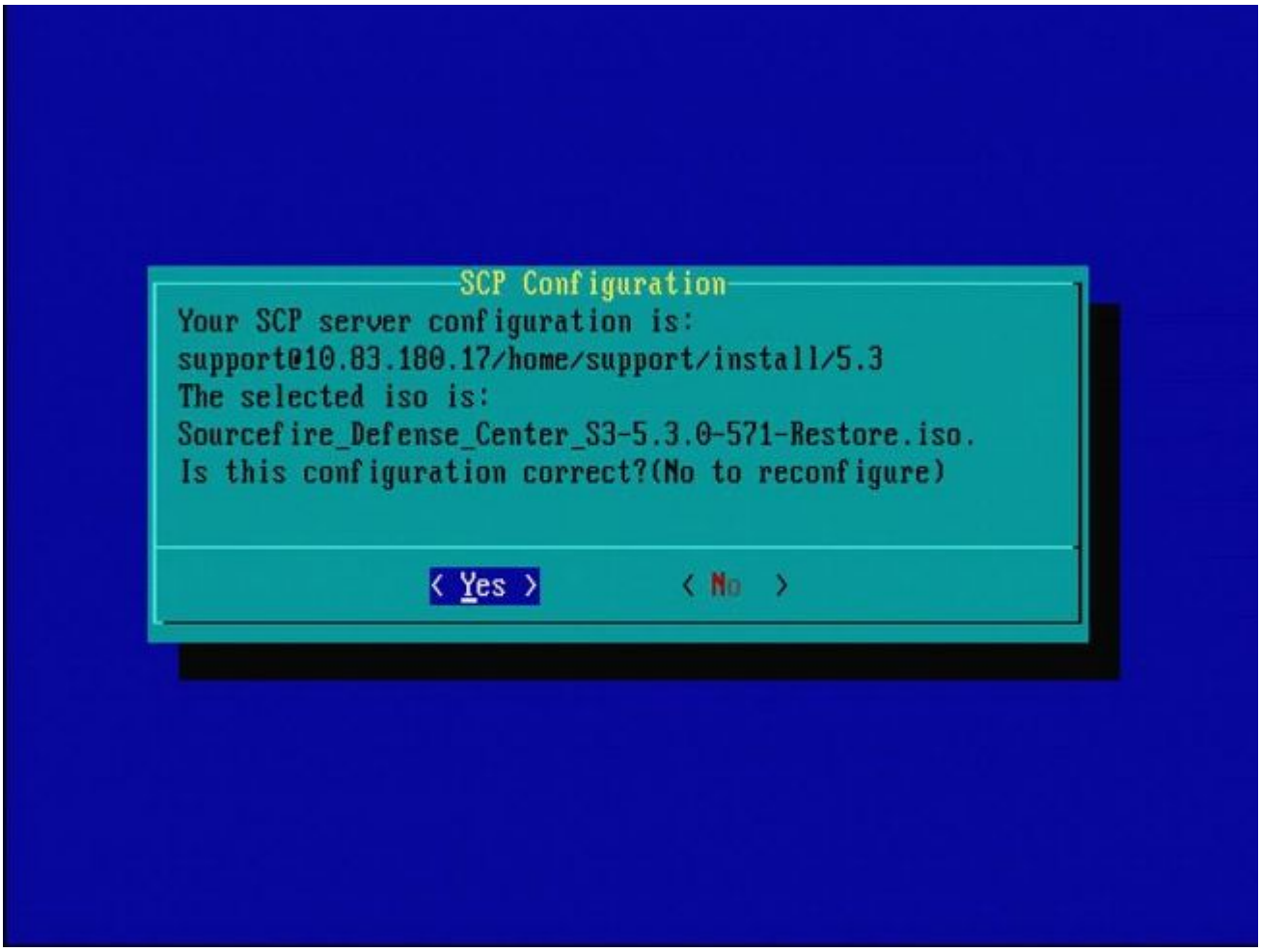
Afbeelding 19

Opmerking: Als u op dit punt een connectiviteitsfout ontvangt in plaats van het verwachte bericht, verifieert u de verbinding met de SSH-server.



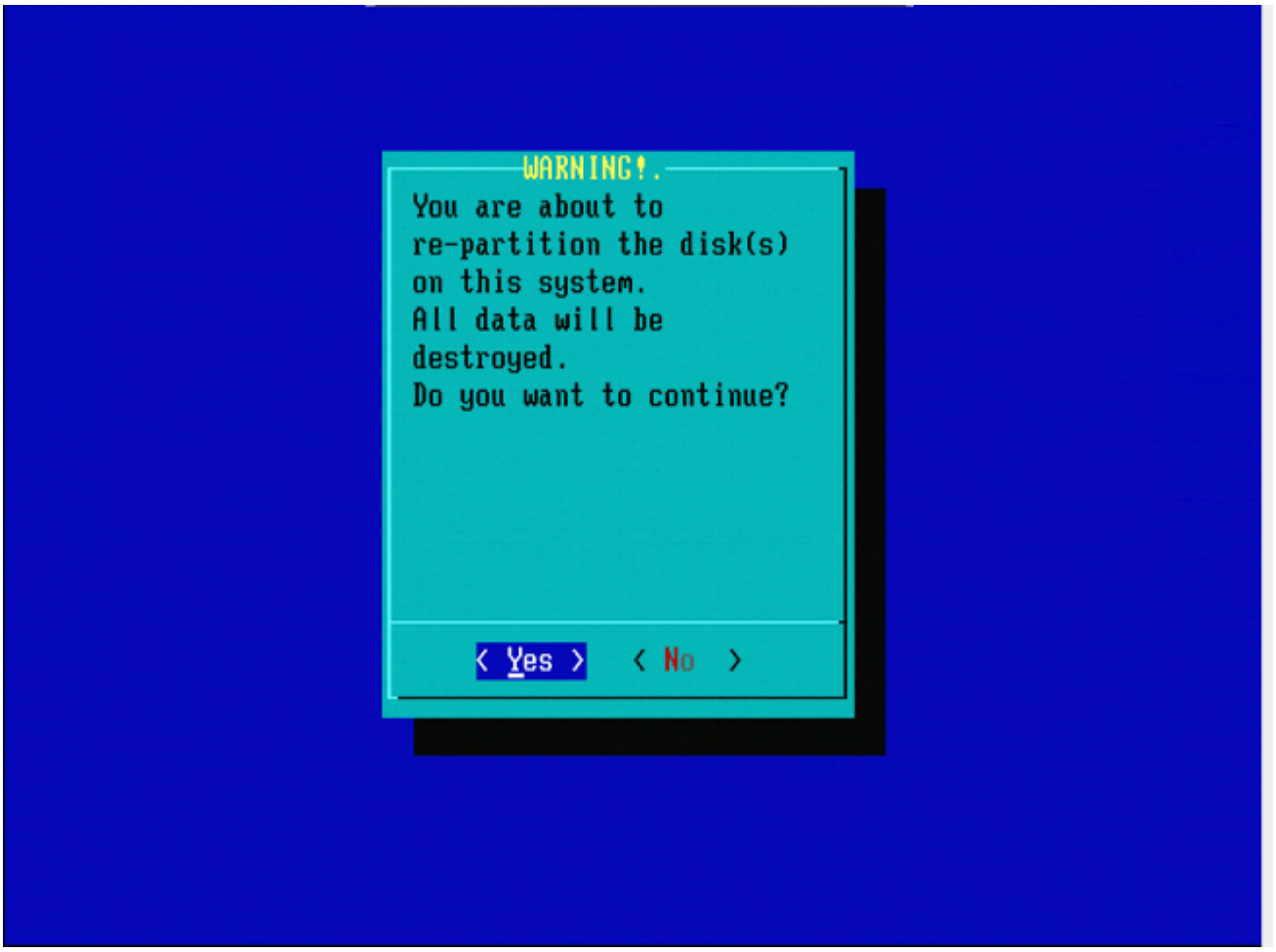
Afbeelding 20 - Druk op de spatiebalk om het .iso-beeld te selecteren.

Opmerking: Het is vereist om de standaardbestandsnamen voor de .iso-bestanden te gebruiken of de bestanden zijn mogelijk nog niet gedetecteerd.
Fout: geen ISO-afbeelding gevonden
In versie 6.3 is de ISO-naamconventie gewijzigd van Sourcefire_3D_Device_S3-<ver>-<build>-Restore.iso in Cisco_Firepower_NGIPS_applicatie-<ver>-<build>-Restore.iso. Als u **"No ISO Image Were Found" (Geen ISO-afbeelding gevonden) tegenkomt,** moet u de naam van het ISO-bestand wijzigen in de oude bestandsnaam. Dit gebeurt normaal wanneer een nieuwe afbeelding van 6.2.x of ouder naar 6.3.0 of hoger wordt weergegeven.

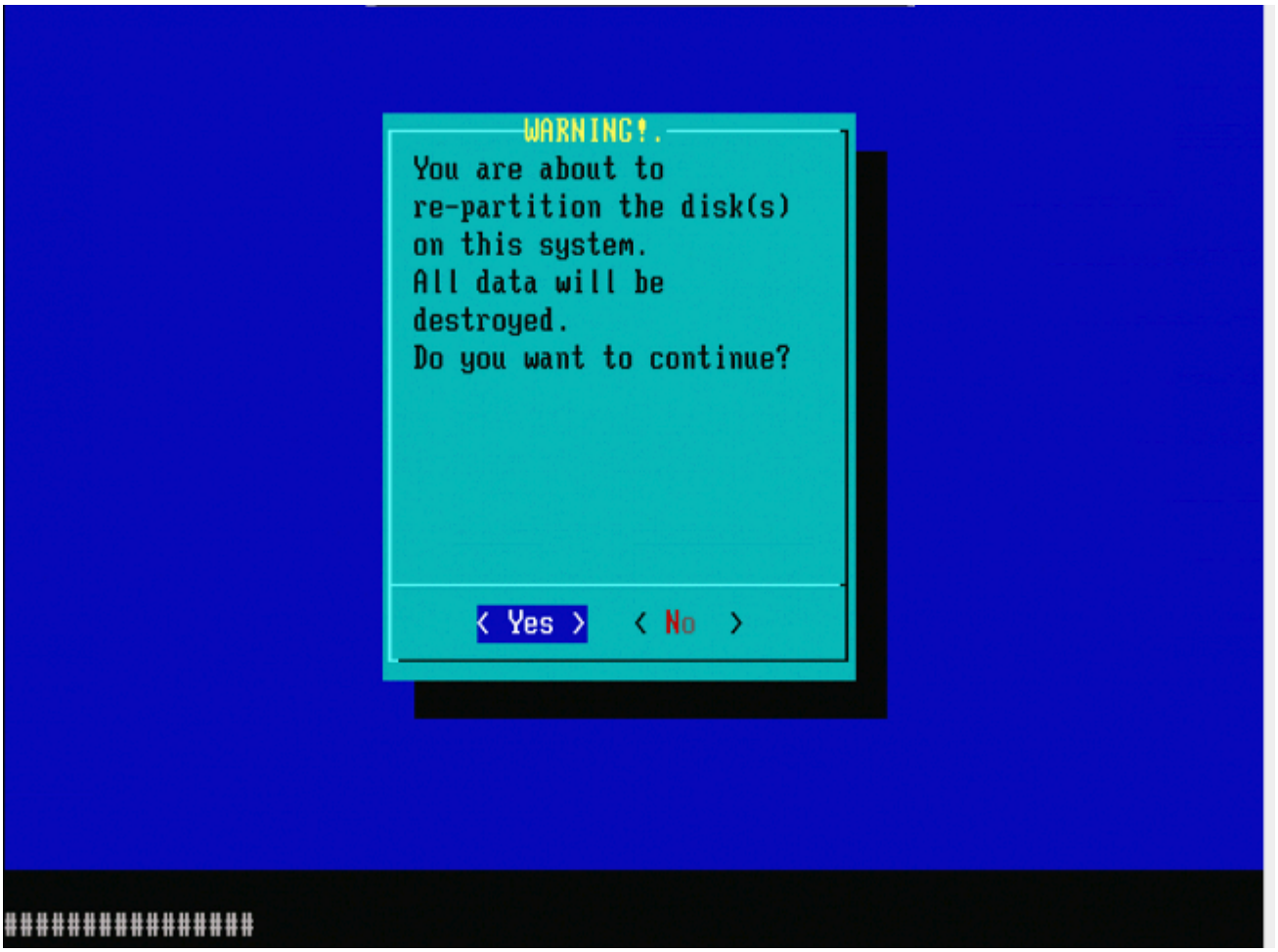


Afbeelding 21

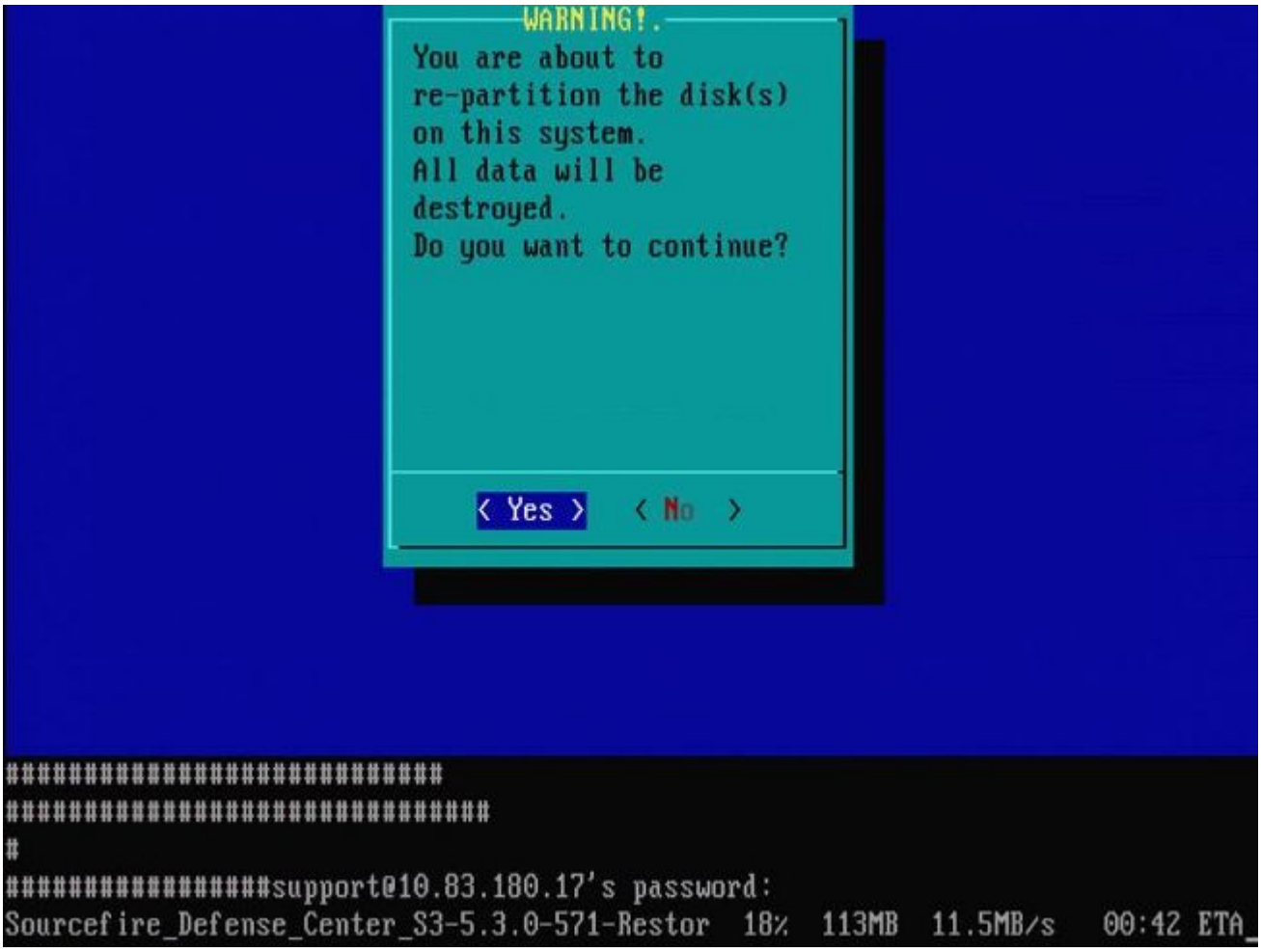
Afbeelding 2 - Cisco Support raadt aan stap 3 in dit proces over te slaan. Patches en snort Rule Updates (SRU's) kunnen worden geïnstalleerd nadat de reimage is voltooid.



Afbeelding 23



Afbeelding 24



Afbeelding 25

Afbeelding 26

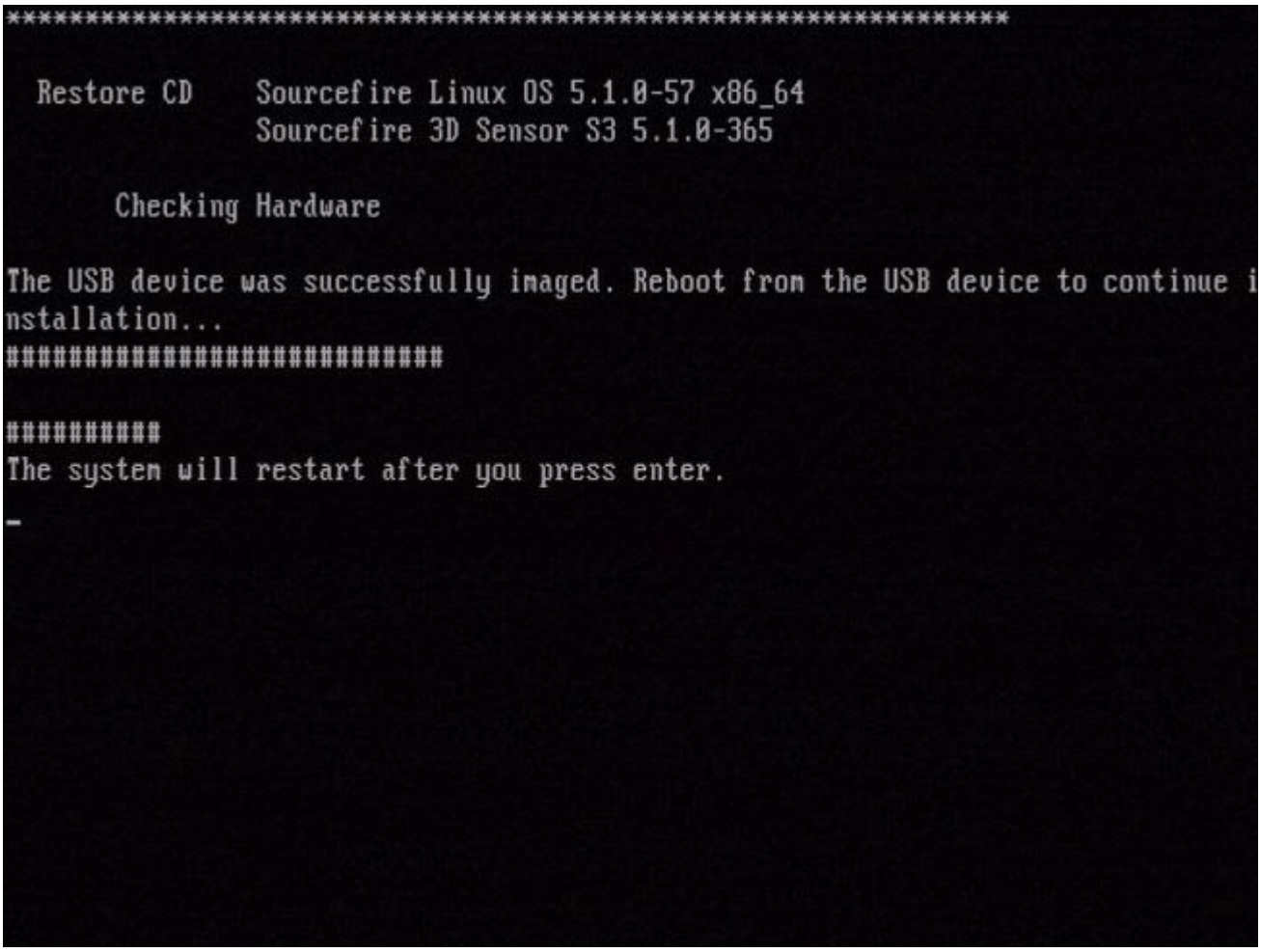
Belangrijke opmerking met betrekking tot een reimage van een andere grote softwareversie: Als u probeert een apparaat te reimagebr dat eerder een andere grote softwareversie draaide, zoals als u 5.1 > 5.2, 5.2 > 5.3, 5.3 > 5.2, enzovoort, opnieuw image, moet u de stappen die in de figuren 1 - 26 **tweemaal** worden weergegeven, voltooien.

1. Nadat u **OK** hebt gekozen op de prompt zoals in afbeelding 26, wordt de systeemherstelpartitie geflitst op de nieuwe versie en wordt het apparaat opnieuw opgestart.
2. Na de reboot, moet u het reimage proces opnieuw beginnen vanaf het begin en doorgaan door het proces dat in de figuren 27b tot en met 31 wordt weergegeven.

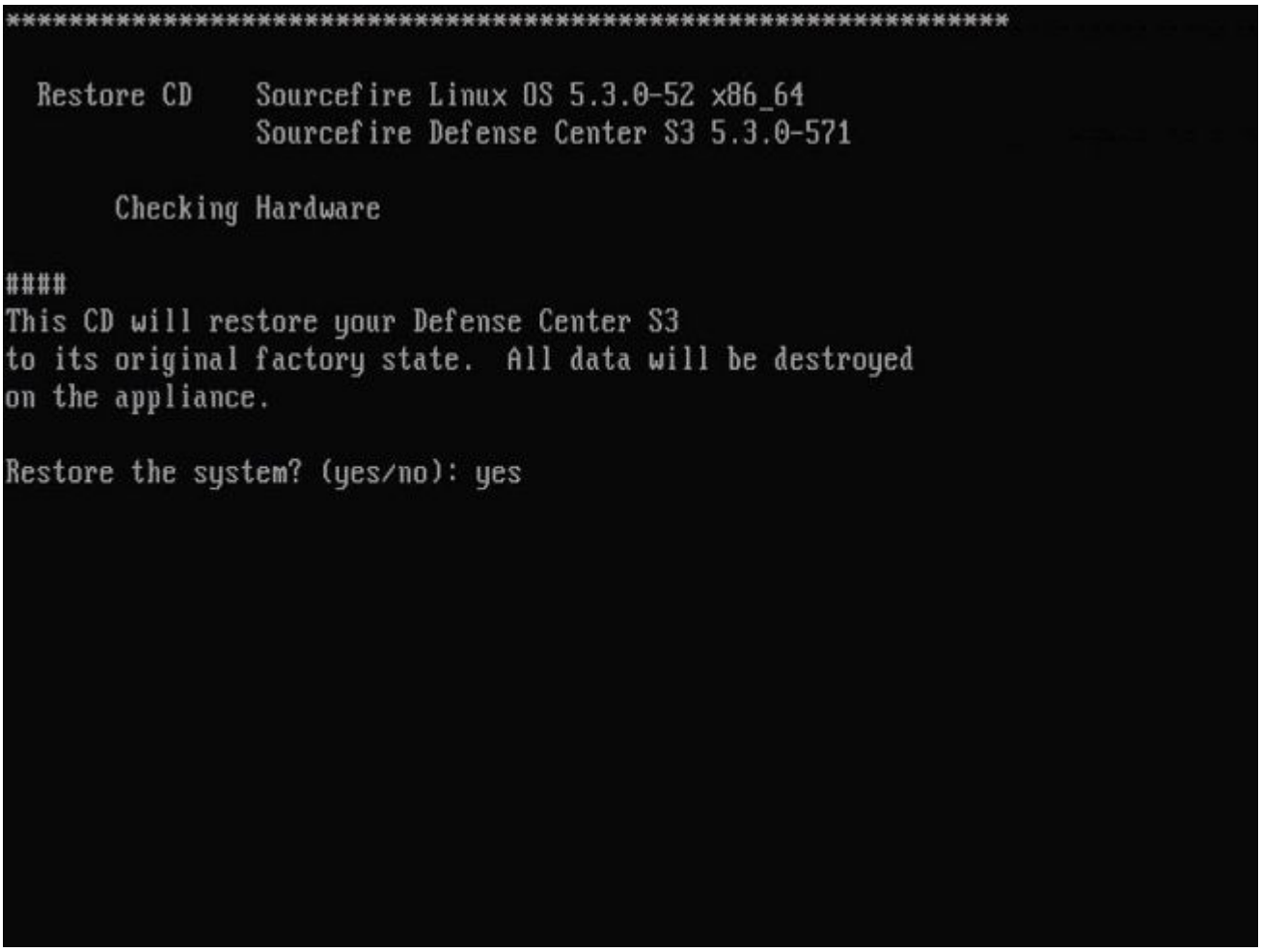
Als dit de eerste reimage is van een andere belangrijke softwareversie, ziet u het scherm zoals getoond in afbeelding 27a, en vervolgens de figuren 31 en 32.

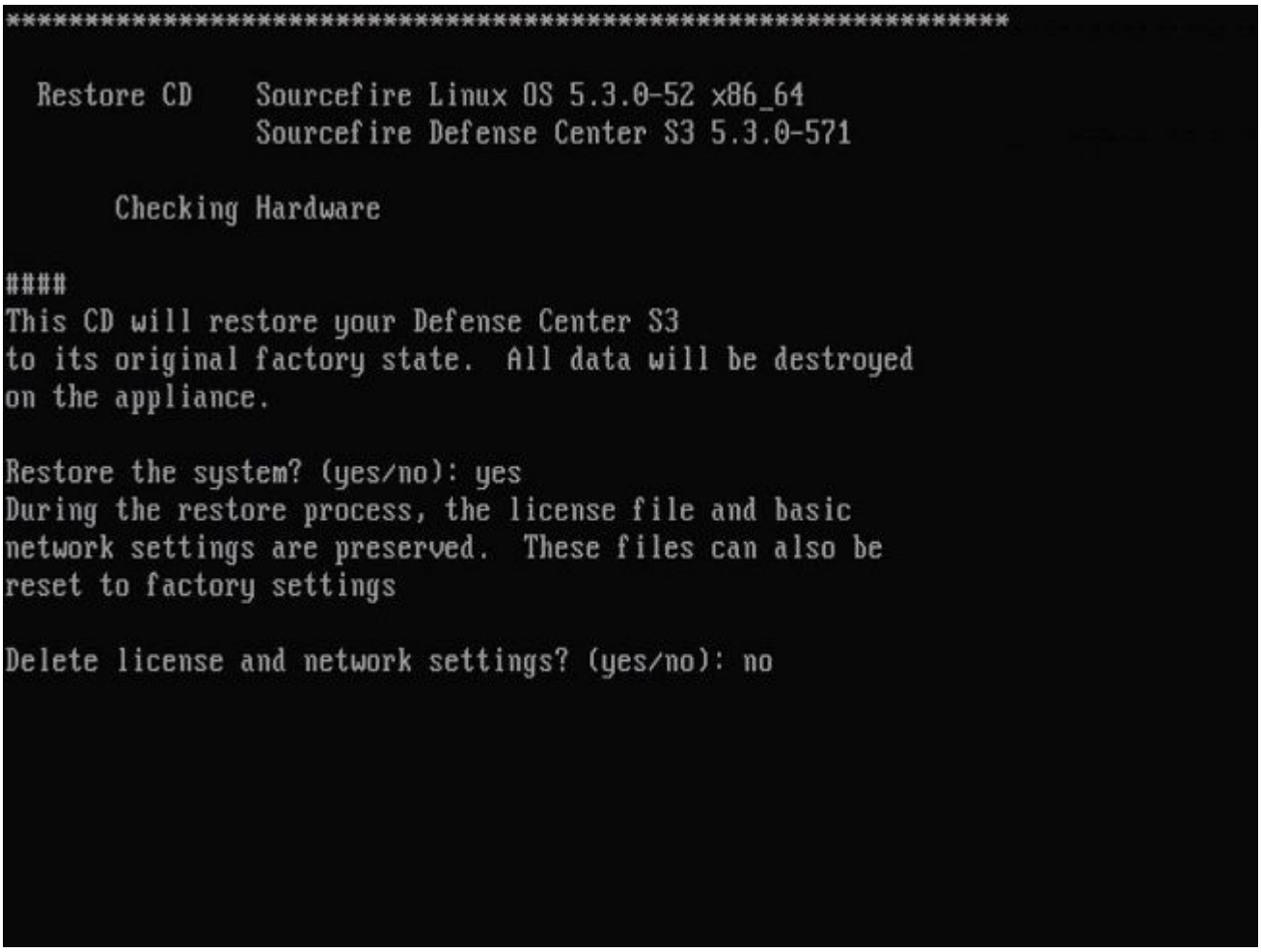
> **Waarschuwing**: als u dit scherm ziet, is er een mogelijke vertraging zonder zichtbare uitvoer na "Hardware controleren" en voor "Het USB-apparaat...". Druk momenteel **niet** op een toets of het apparaat start opnieuw op in een onbruikbare toestand en moet opnieuw worden gebeeldhouwd.

Als dit niet het geval is, kunt u de schermen in figuur 27b zien door figuur 32.

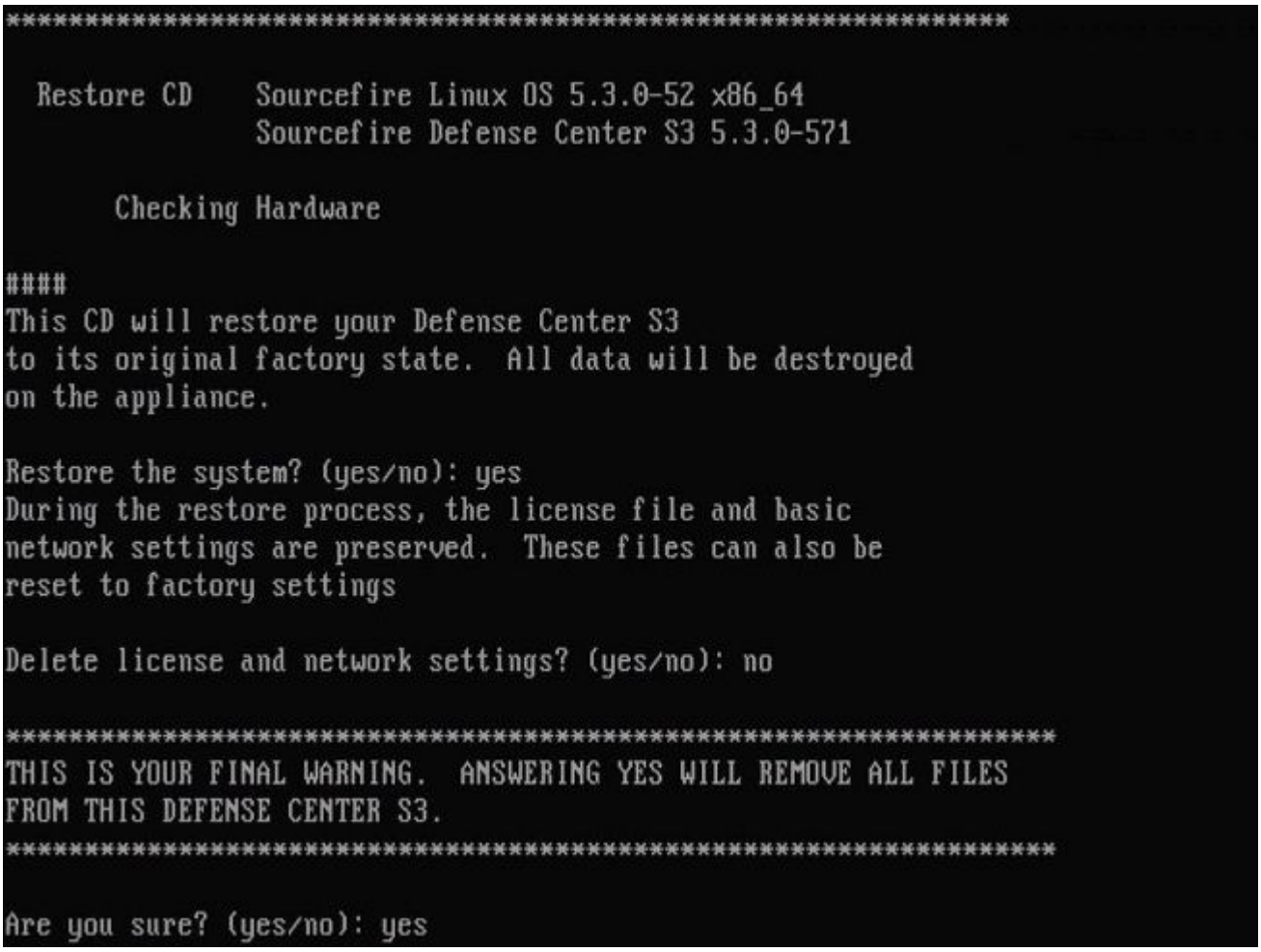

****
Restore CD Sourcefire Linux OS 5.1.0-57 x86_64
Sourcefire 3D Sensor S3 5.1.0-365
Checking Hardware
The USB device was successfully imaged. Reboot from the USB device to continue i
nstallation...
##########
##########
The system will restart after you press enter.

Figuur 27a

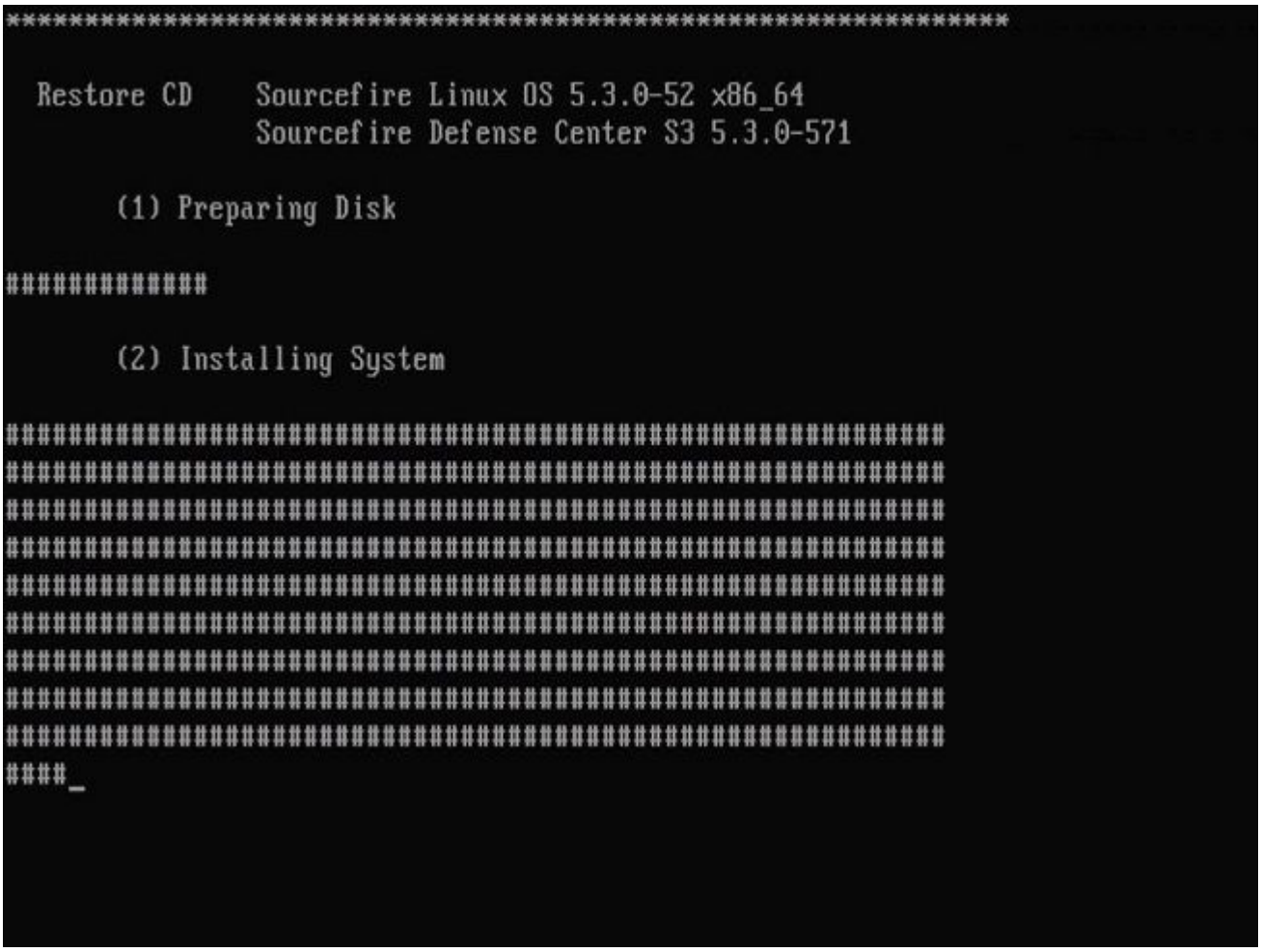

****
Restore CD Sourcefire Linux OS 5.3.0-52 x86_64
Sourcefire Defense Center S3 5.3.0-571
Checking Hardware
####
This CD will restore your Defense Center S3
to its original factory state. All data will be destroyed
on the appliance.
Restore the system? (yes/no): yes
Figuur 27b



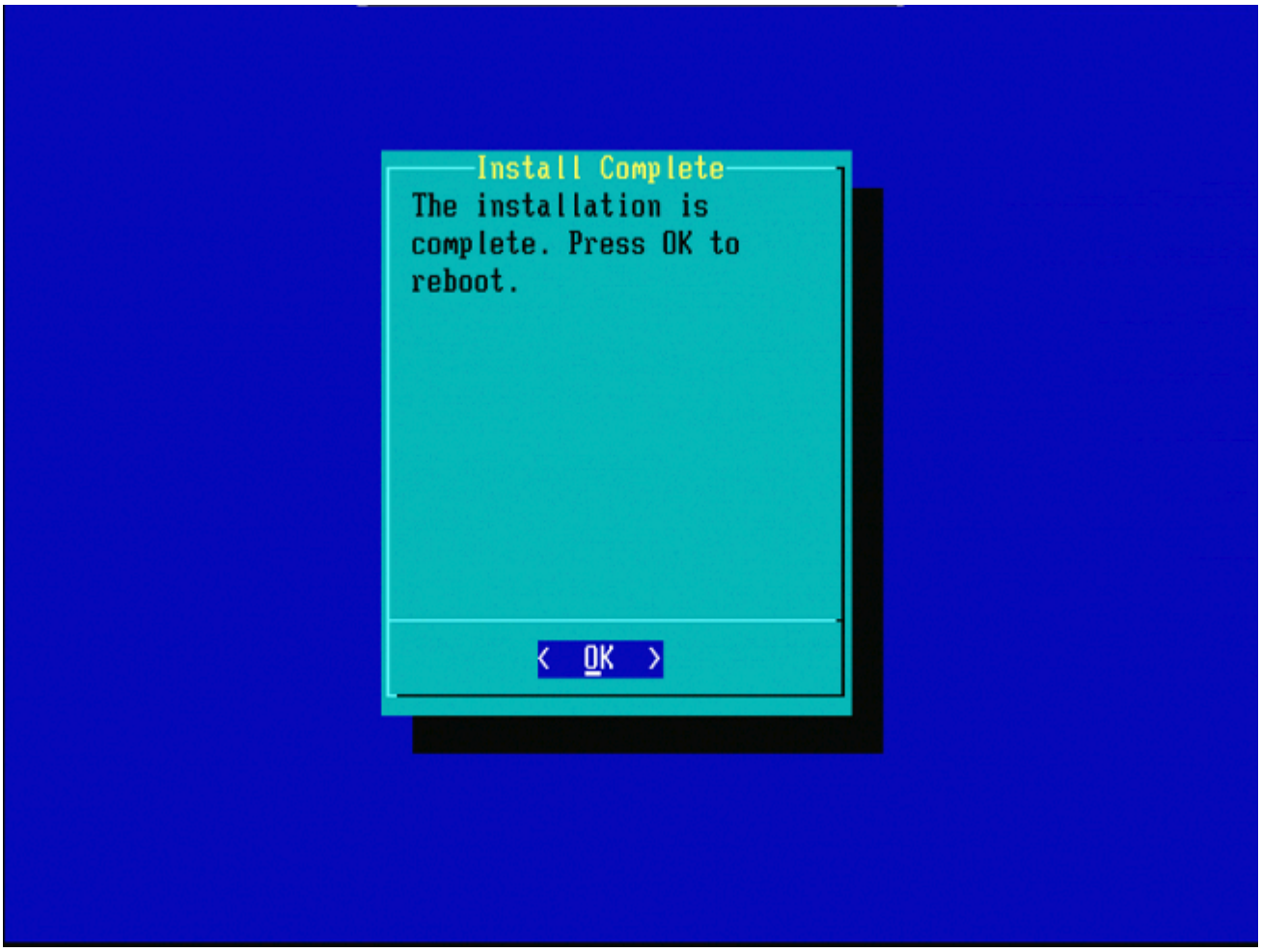
Afbeelding 28



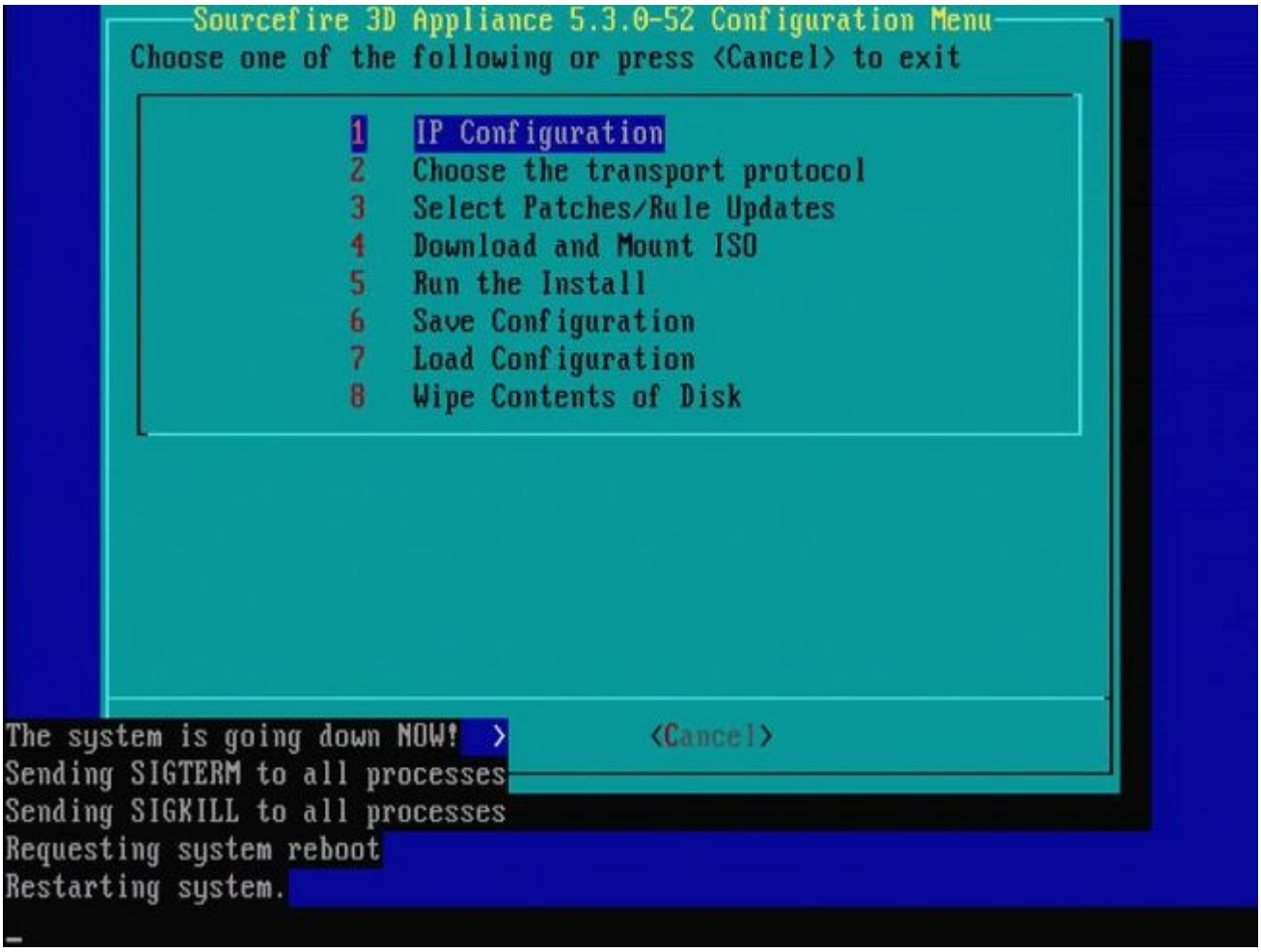
Afbeelding 29



Afbeelding 30



Afbeelding 31



Afbeelding 32

Cisco Firepower Management Center 1000, 2500 en 4500

Op VCC 1000, 2500 en 4500 zijn de opties verschillend. Gebruik een KVM-switch of de CIMC en wanneer het apparaat start, krijgt u deze opties:

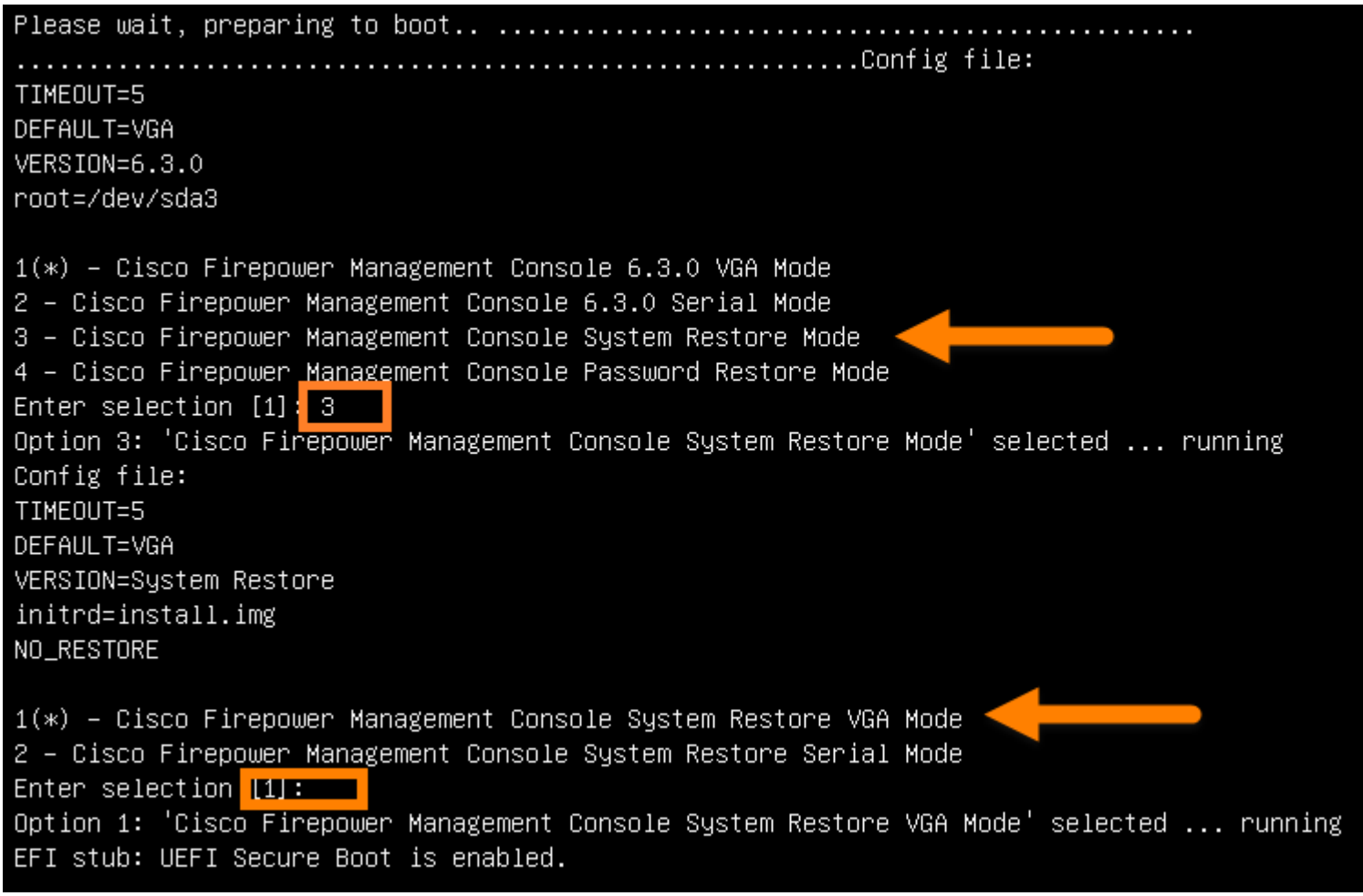
1 - Cisco Firepower Management Console VGA-modus

2 - Cisco Firepower Management Console - seriële netwerkmodule

3 - Cisco Firepower Management Console systeemterugzetmodus

4 - Cisco Firepower Management Console wachtwoordterugzetmodus

Als u de terugzetmodus met de UI wilt invoeren, selecteert u de optie 'Cisco Firepower Management Console System Restor Mode' (optie **3**) en vervolgens 'Cisco Firepower Management Console System Restore VGA Mode' (optie **1)**



Afbeelding 33

De rest van het proces is hetzelfde als bij andere toestellen van het VCC.

Problemen oplossen

De optie Menu System_Restore LILO is niet vermeld

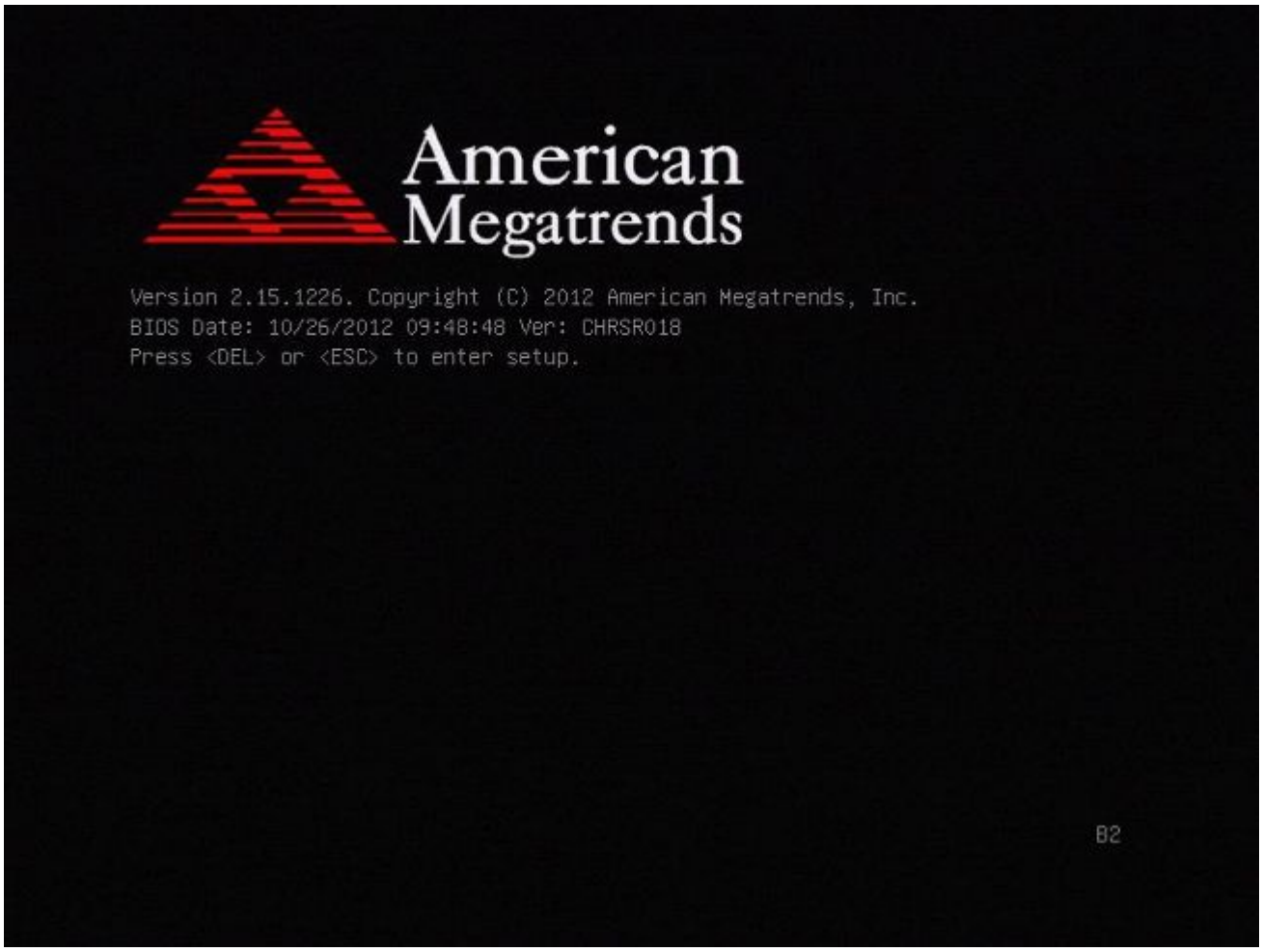
Het FireSIGHT Management Center en de FirePOWER 7000 en 8000 Series apparaten hebben een geïntegreerde flash drive die het reimage systeem bevat. Als de optie "**System_Restore**" niet wordt vermeld in het opstartmenu van LILO (Linux Loader), is het nog steeds mogelijk om toegang te krijgen tot dit station om het image te voltooien.

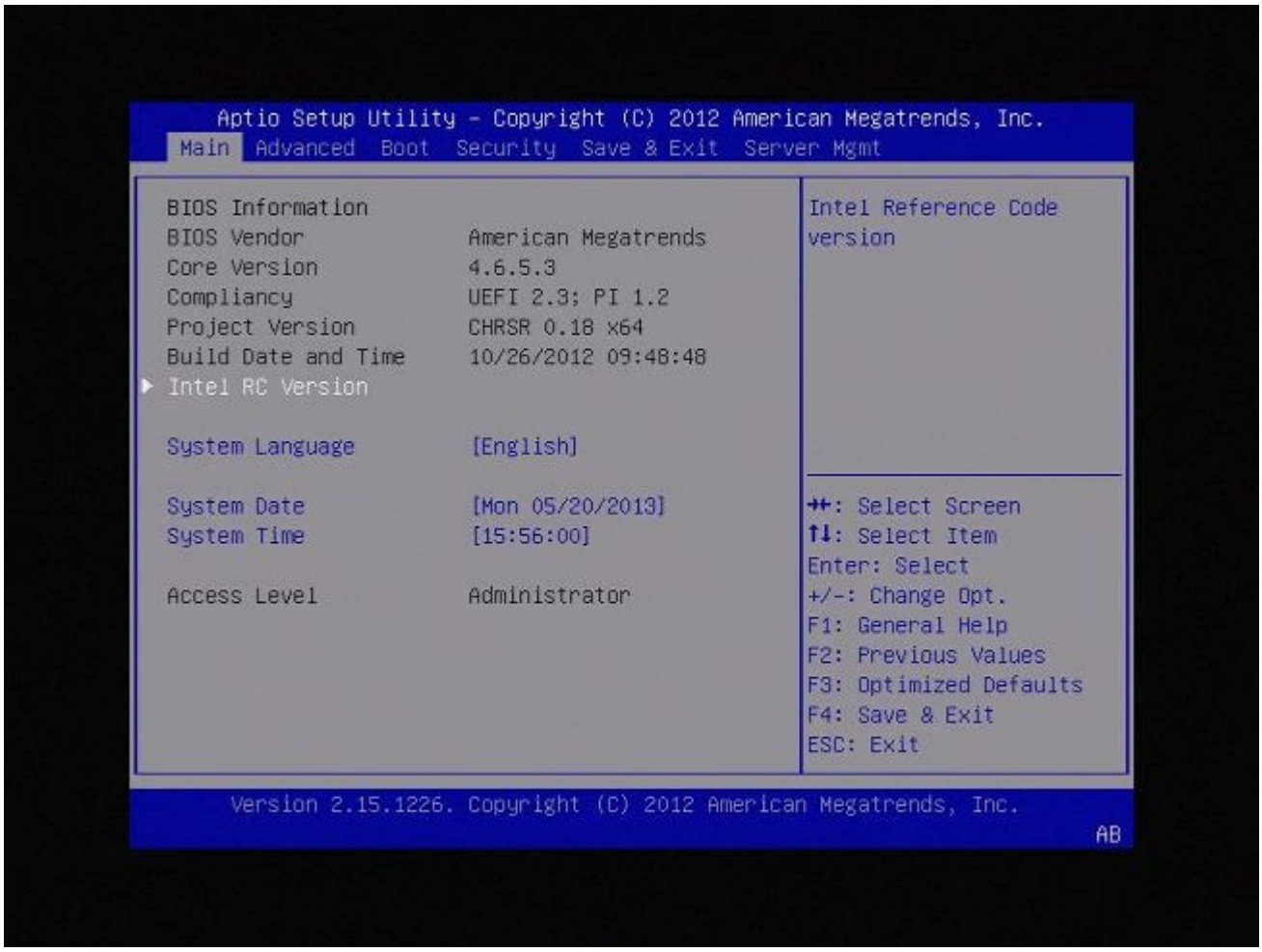
7010, 7020 en 7030 apparaten

Als u een 70XX Series apparaat gebruikt, moet u deze stappen uitvoeren om het opstartapparaat te selecteren:

1. Schakel het apparaat zorgvuldig uit.

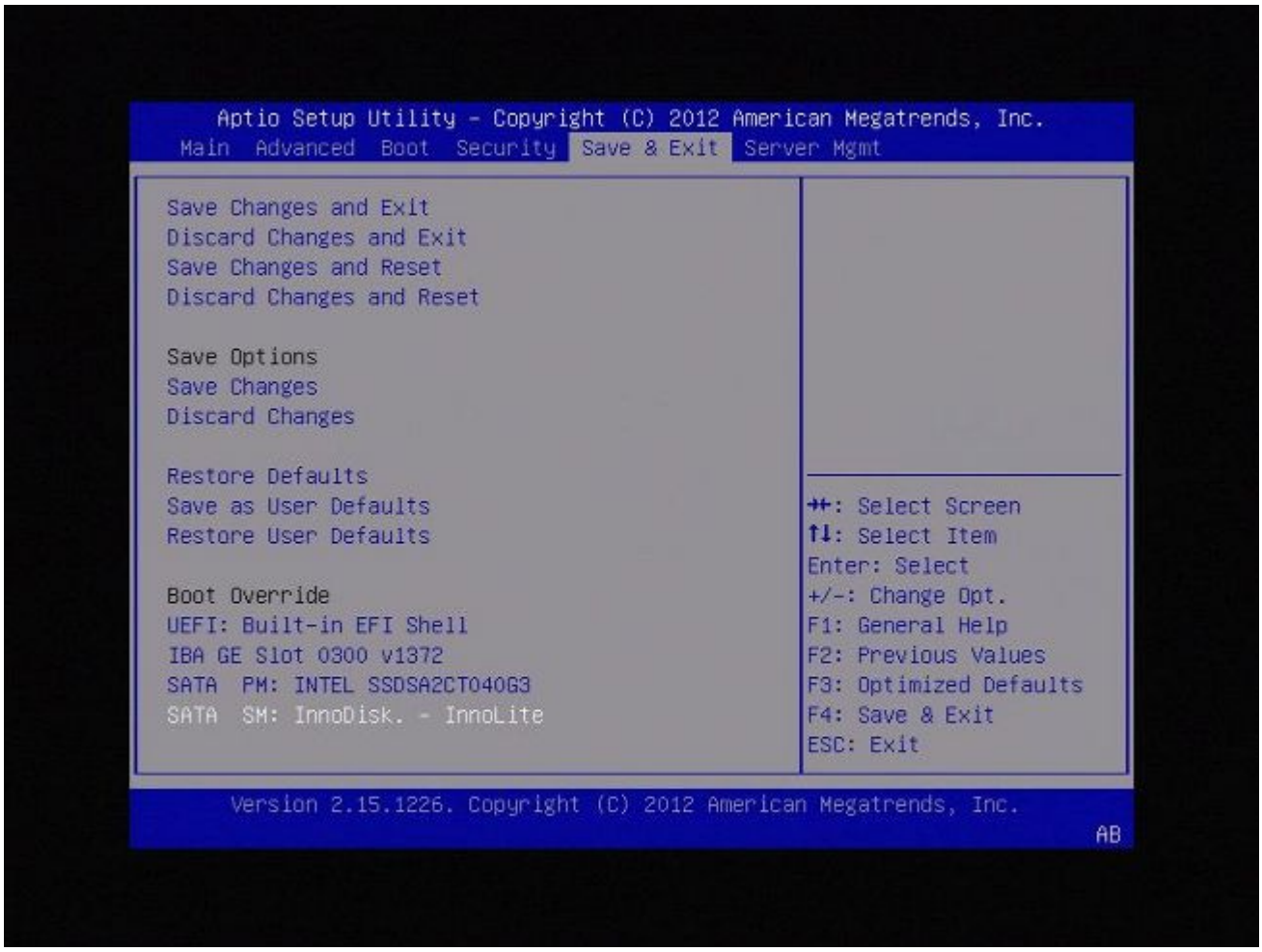
2. Schakel het apparaat in en druk herhaaldelijk op de toets **Delete** terwijl het apparaat opgestart wordt om toegang te krijgen tot het selectiescherm met opstartapparaten. Zie de afbeelding hier:


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
Figuur A1



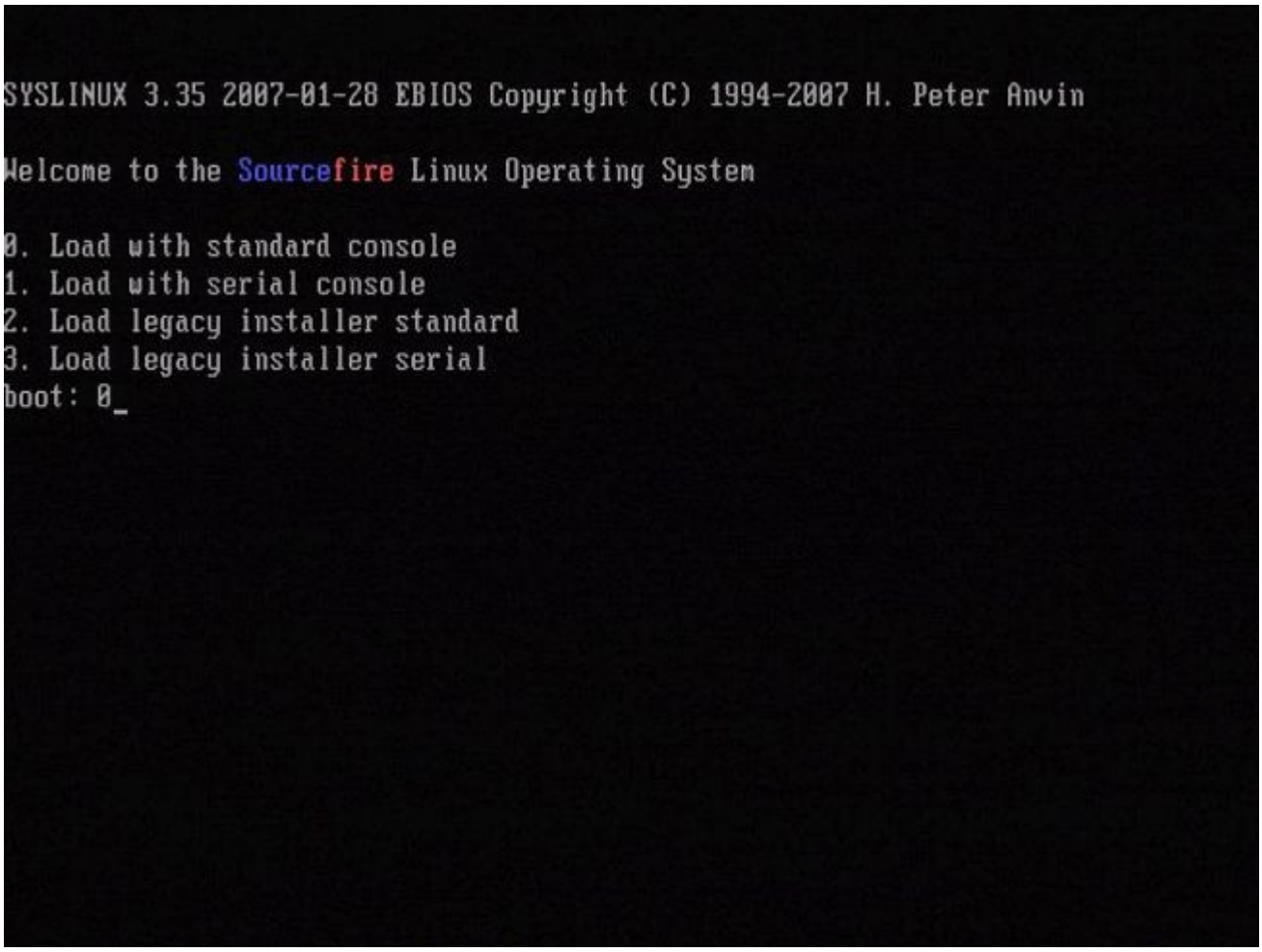
Figuur A2

3. Gebruik de pijltoets rechts om het tabblad **Opslaan en afsluiten** te selecteren. Gebruik op dit tabblad de pijltoets omlaag om **SATA SM: InnoDisk** te selecteren**. - InnoLite** en druk op de toets **Enter**.



Figuur A3

4. Kies optie **0** als u een toetsenbord en monitor gebruikt.


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_
Figuur A4

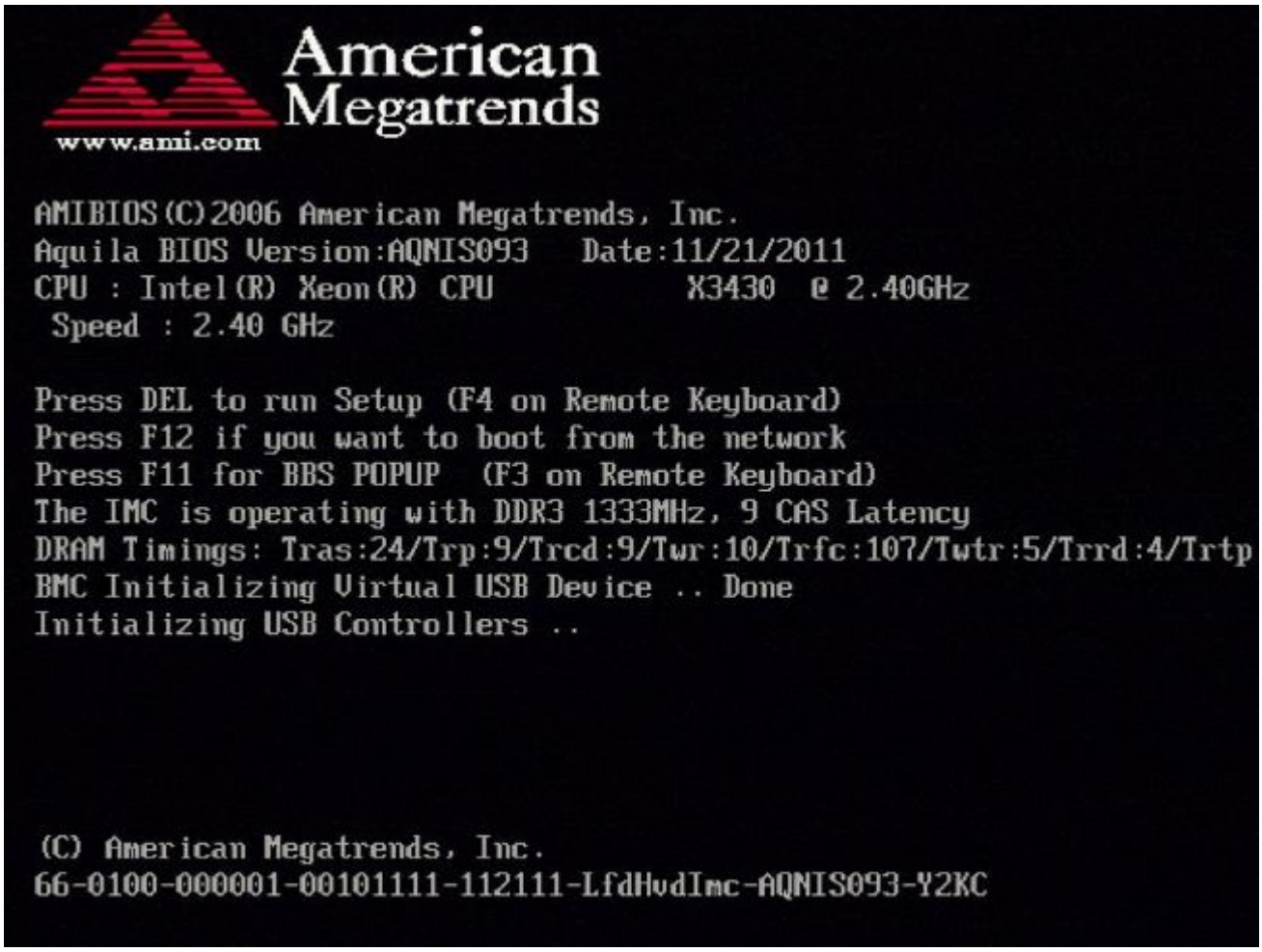
Figuur A5

7110 en 7120 apparaten

Als u een 71XX Series apparaat gebruikt, moet u deze stappen uitvoeren om het opstartapparaat te selecteren:

1. Schakel het apparaat zorgvuldig uit.

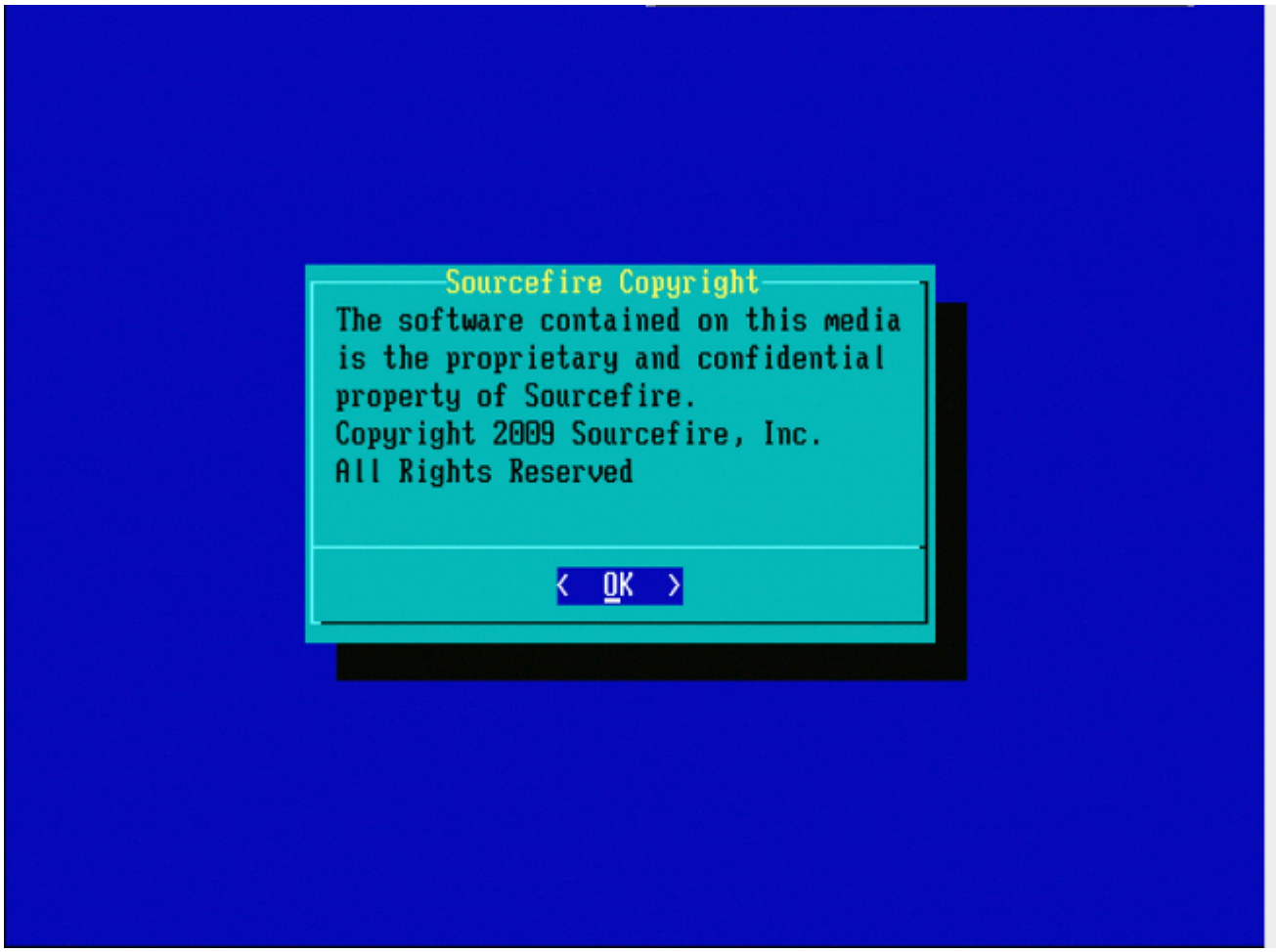
2. Schakel het apparaat in en druk herhaaldelijk op de **F11**-toets terwijl het apparaat opgestart wordt om toegang te krijgen tot het selectiescherm voor het opstartapparaat. Zie het hier getoonde beeld:



Figuur B1

3. Selecteer optie **HDD:P1-SATADOM** en druk op **ENTER** om te beginnen met de partitie **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
Figuur B2



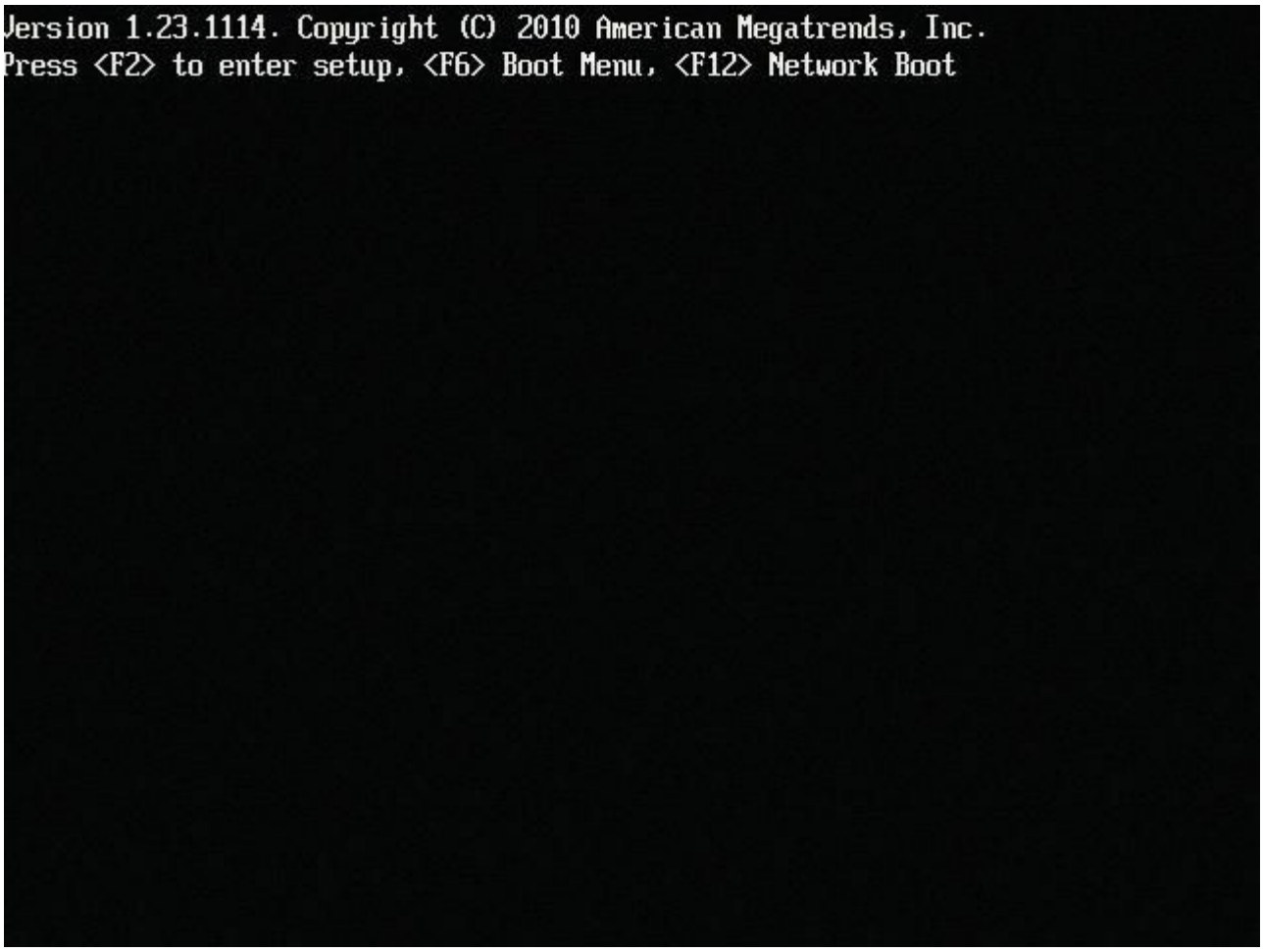
Figuur B3

800 Series apparaten voor Management Center-modellen FS750, FS1500 of FS3500

Als u een 8000 Series apparaat of Management Center model FS750, FS1500, of FS3500 gebruikt, voltooi deze stappen om het opstartapparaat te selecteren:

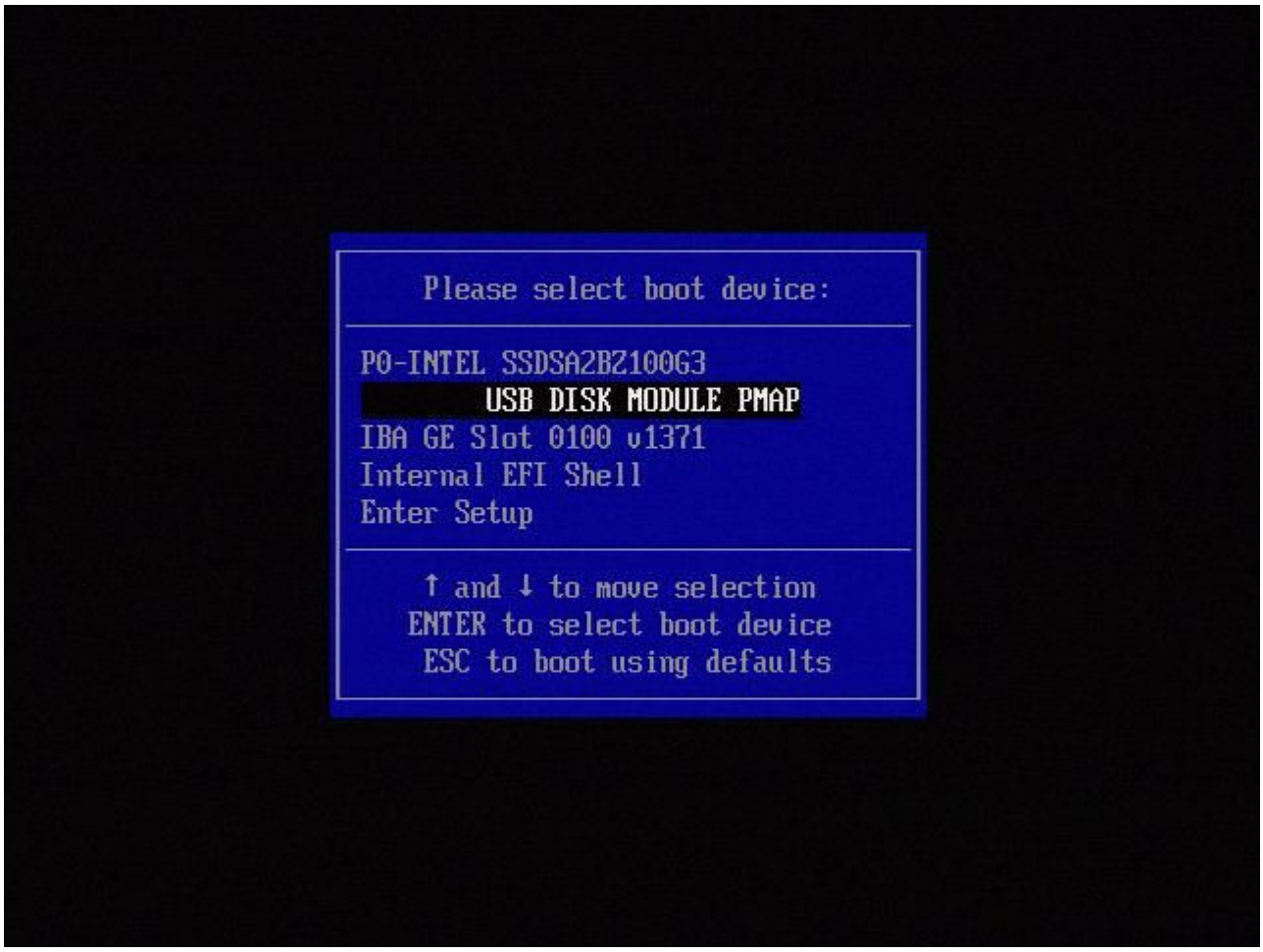
1. Schakel het apparaat zorgvuldig uit.

2. Schakel het apparaat in en druk herhaaldelijk op de **F6**-toets terwijl het apparaat wordt opgestart om toegang te krijgen tot het selectiescherm voor het opstartapparaat. Zie het hier getoonde beeld:



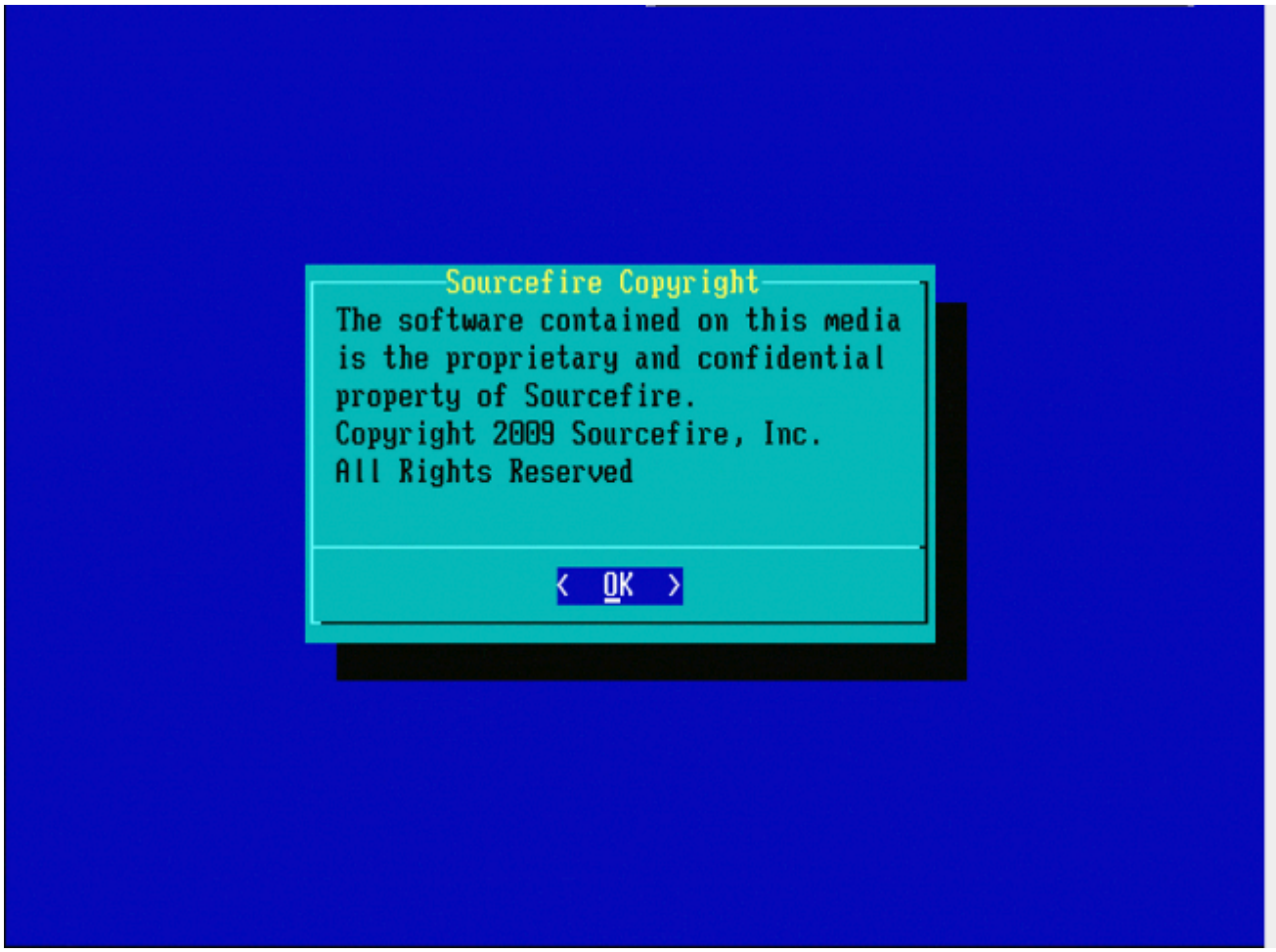
Figuur C1

3. Selecteer de USB-optie.



Figuur C2

4. Het apparaat start op vanaf de System_Restore-partitie en geeft het menu **System_Restore weer**.



Figuur C3

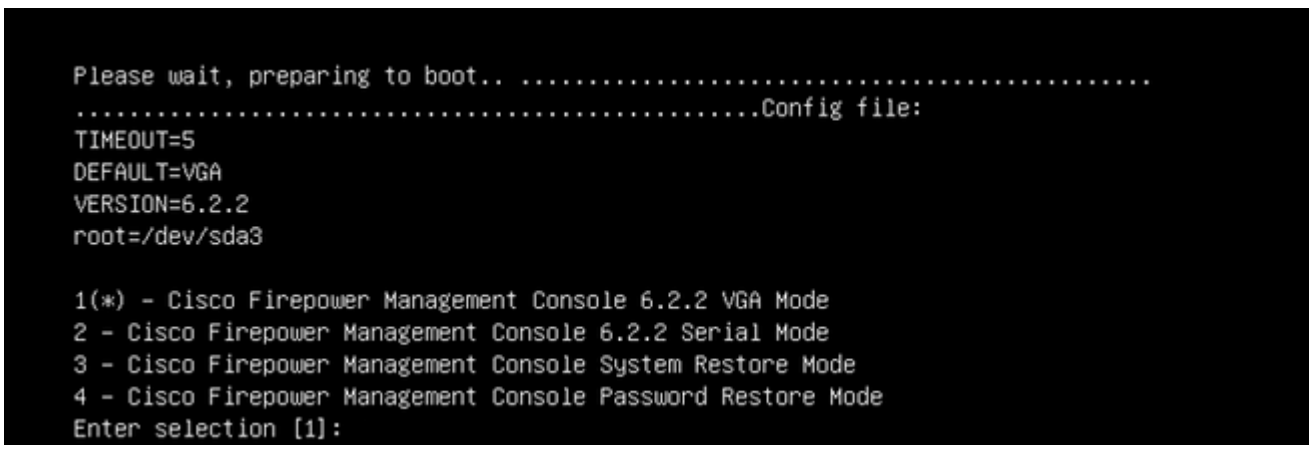
Systeemherstel voor de modellen FMC1000, FMC2500, FMC4500 (op M4 gebaseerde FMCâ€™s)

> **Opmerking**: Voor FMC4500 heeft dit model een ander opstartmenu, meer details zijn te vinden in de volgende link

---

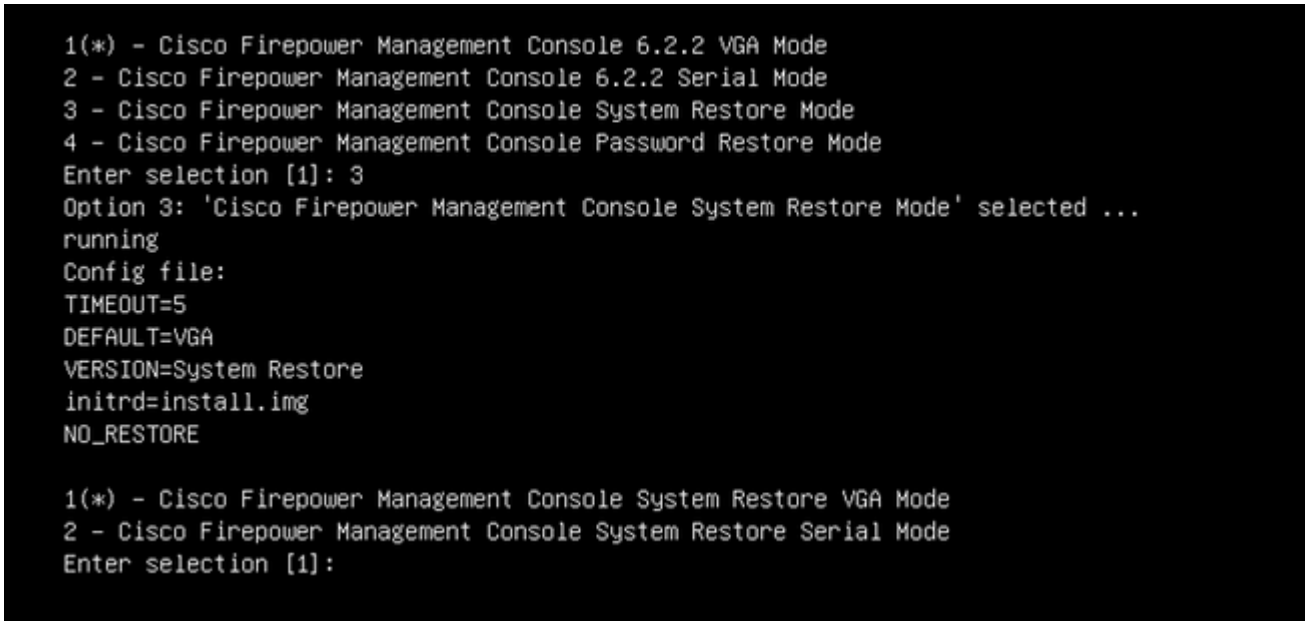
De vraag om systeem te herstellen verschijnt voor deze modellen anders: FMC1000, FMC2500, FMC4500

1. Tijdens het opstarten ziet u dit scherm 5 seconden:



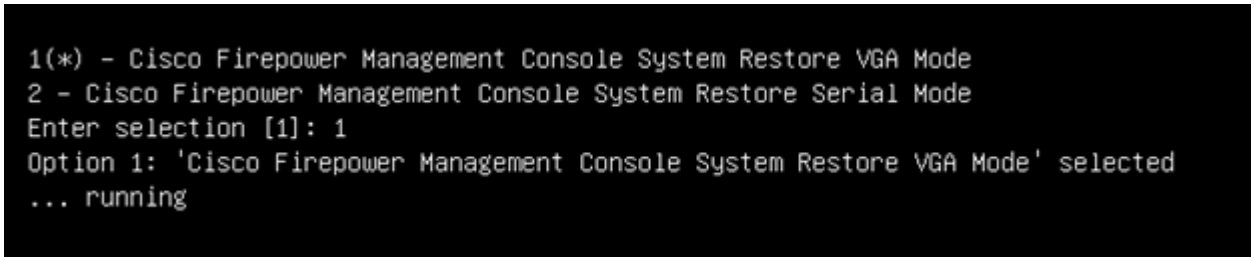
Figuur D1

2. Selecteer de optie Systeemherstel (in dit geval #3).



Figuur D2

3. Selecteer de weergavemethode voor het systeemherstel (in dit geval #1 voor VGA)



Figuur D3

4. Dan komt u bij de herinnering die in figuur 5 wordt gezien, en het proces gaat normaal verder.

Opstartoptie niet vermeld

Het is mogelijk dat de optie om op te starten naar de reimage-partitie niet wordt vermeld in het BIOS of het opstartmenu. Als dit het geval is, is het station dat het beeldsysteem bevat mogelijk ontbreekt of beschadigd. Een RMA is waarschijnlijk nodig.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.