Erstellen Sie ein neues Image des FireSIGHT Management Center und der FirePOWER-Appliance

Inhalt

Einleitung

In diesem Dokument werden die Prozesse mit Beispielen für das Verfahren zum erneuten Abbilden von Cisco FireSIGHT Management Center (FMC) und FirePOWER-Appliances beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

Verwaltetes Gerät	FireSIGHT Management Center	Für neues Image verfügbare Softwareversionen
Cisco Firepower 7000-Serie Cisco Firepower 7100-Serie Cisco Firepower 8100-	FS 750 FS 1500 FS 3500	5.2 oder spätere Version

Serie Cisco Firepower 8200-Serie		
Firepower Serie 8300 Cisco AMP 7150 Cisco AMP 8150		5.3 oder spätere Version

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Prozess neu aufzeichnen

Vorsicht: Schließen Sie bei der Aktualisierung oder Neuerstellung eines Images eines FireSIGHT Management Center oder einer FirePOWER-Appliance kein USB-Speichergerät oder keinen KVM-Switch (Keyboard, Video, and Mouse) an.

Vorbereitungen

1. Wenn Sie ein neues Image eines Management Center- oder eigenständigen FirePOWER-Geräts erstellen möchten, wird empfohlen, die Appliance zu sichern, bevor Sie fortfahren.

2. Identifizieren Sie das Modell Ihres Sensors, und verwenden Sie die Liste der Modelle im Abschnitt Verwendete Komponenten, um sicherzustellen, dass dieser Leitfaden angemessen ist.

3. Laden Sie die entsprechende Installationsanleitung und das Festplatten-Image für die gewünschte Softwareversion von der Cisco Support-Website herunter.

   Hinweis: ISO-Datei nicht umbenennen

   Bereitstellen des Images: Die ISO-Datei muss auf einen Host kopiert werden, auf dem ein SSH-Server ausgeführt wird, der vom Verwaltungsnetzwerk der Appliance aus erreichbar ist, damit ein Image erstellt werden kann.

   Hinweis: Wenn kein anderer SSH-Server verfügbar ist, kann für diesen Prozess ein FMC verwendet werden.

   Überprüfen Sie die Integrität des ISO: Die MD5sum-Dateien werden auf der rechten Seite der Seite bereitgestellt, um mithilfe des MD5sum-Dienstprogramms überprüft zu werden.

4. Die Installationshandbücher enthalten schrittweise Anweisungen zum erneuten Abspielen von Images und erläutern verschiedene Methoden für den erneuten Abbildungsprozess. Die in diesem Dokument bereitgestellten Bilder können als Referenz verwendet werden.

Überblick über den Neubildprozess

> **Hinweis**: Die Version 5.3 wurde verwendet, um die in diesem Artikel gezeigten Bilder zu erfassen. Der Reimage-Prozess ist für andere 5.x-Versionen identisch, mit Ausnahme der Versionsnummern, die in den abgebildeten Bildern angezeigt werden.

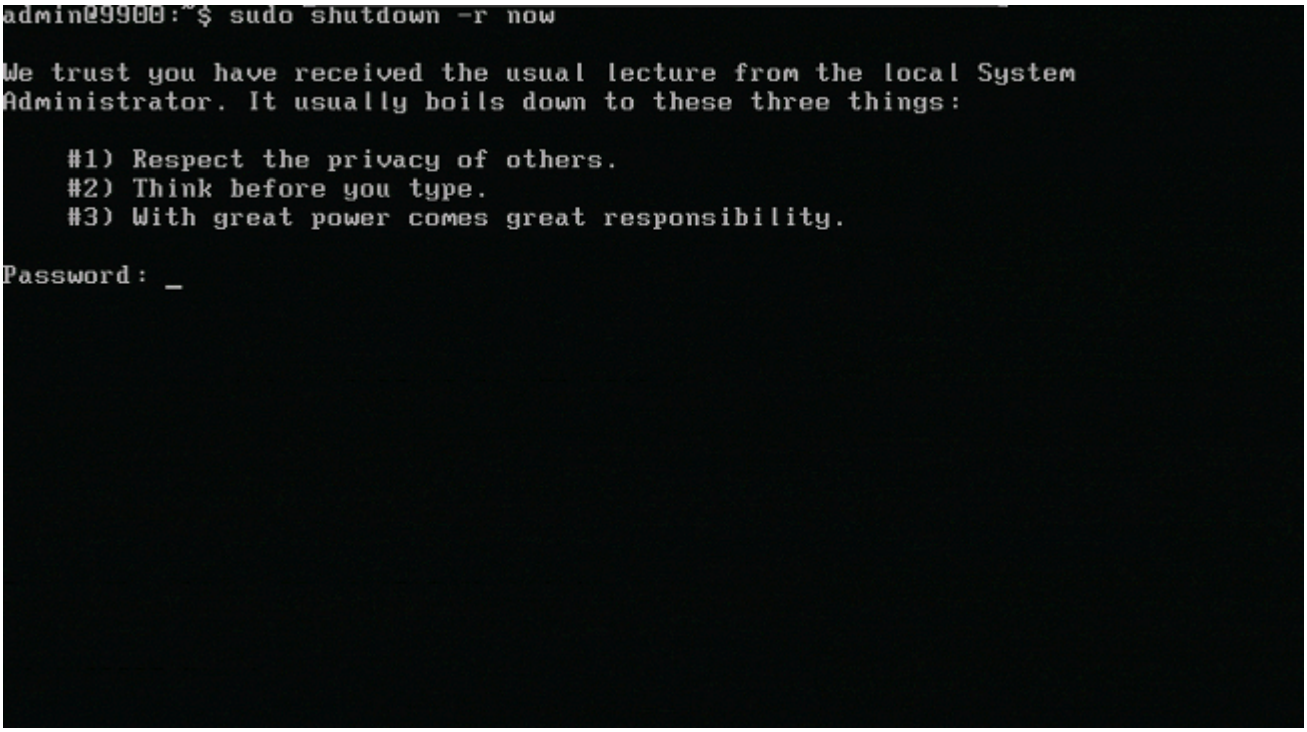


Abbildung 1

Abbildung 2: Wenn das System neu gestartet wird, drücken Sie eine Pfeiltaste auf der Tastatur, um den Countdown anzuhalten und die Option **System_Restore** für den als Nächstes dargestellten Bildschirm auszuwählen.

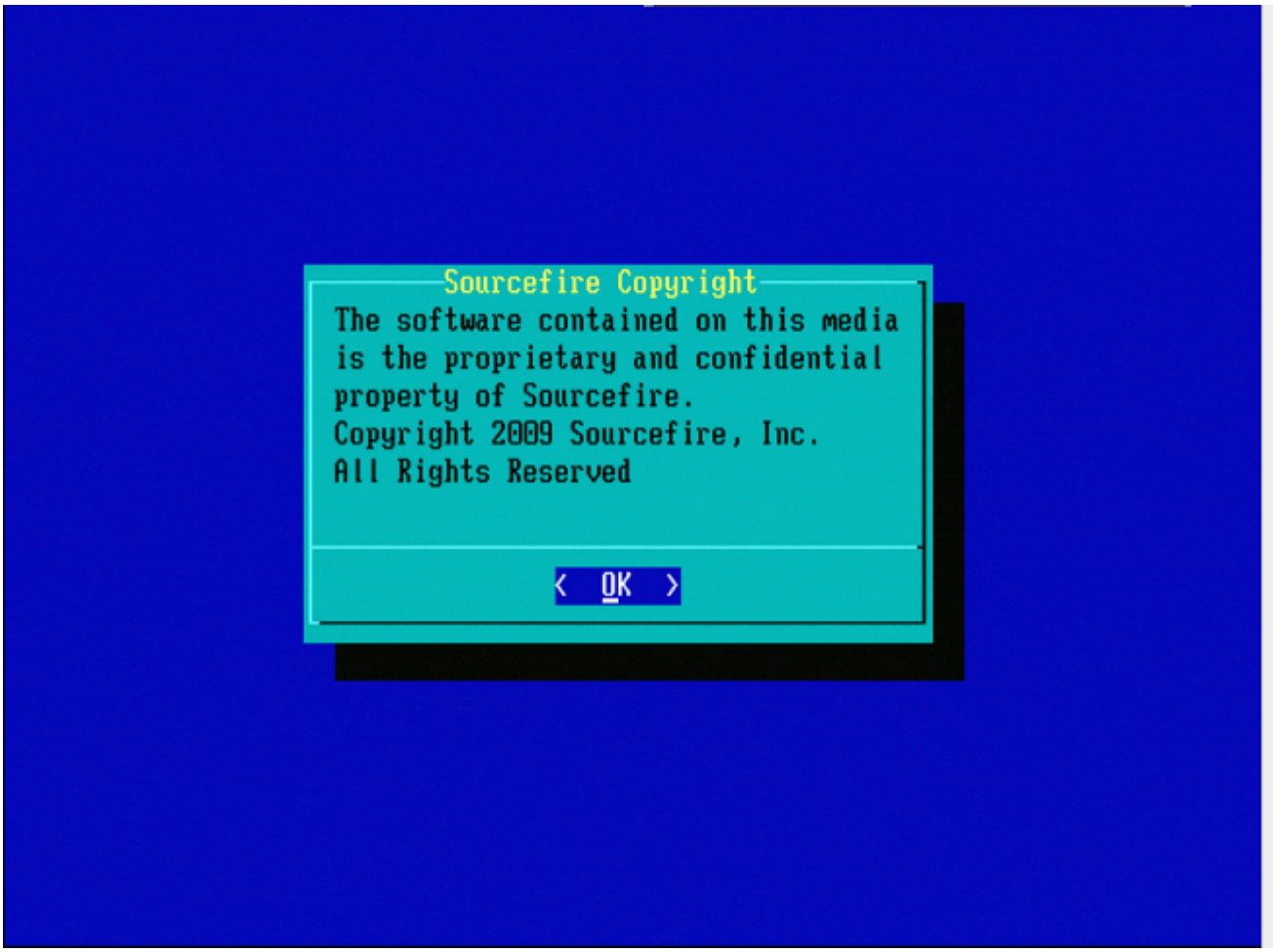
Hinweis: Wenn die Eingabeaufforderung **System_Restore** nicht angezeigt wird, müssen Sie die Bootreihenfolge ändern, um direkt von der Wiederherstellungspartition (DOM) zu starten. Weitere Informationen finden Sie unter LILO-Menüoption "System_Restore" fehlt.

Abbildung 3

Abbildung 4: Wählen Sie Option **0,** wenn Sie eine Tastatur und einen Monitor verwenden.

Hinweis: Manchmal wurde festgestellt, dass das Menü für die Wiederherstellungsoption nur angezeigt wird, wenn nur die Konsole angeschlossen ist (ohne Tastatur). Sobald die Wiederherstellungsoption ausgewählt ist, kann die Tastatur wieder angeschlossen werden

---


Sourcefire Copyright
The software contained on this media
is the proprietary and confidential
property of Sourcefire.
Copyright 2009 Sourcefire, Inc.
All Rights Reserved
< OK >
Abbildung 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>
Abbildung 6

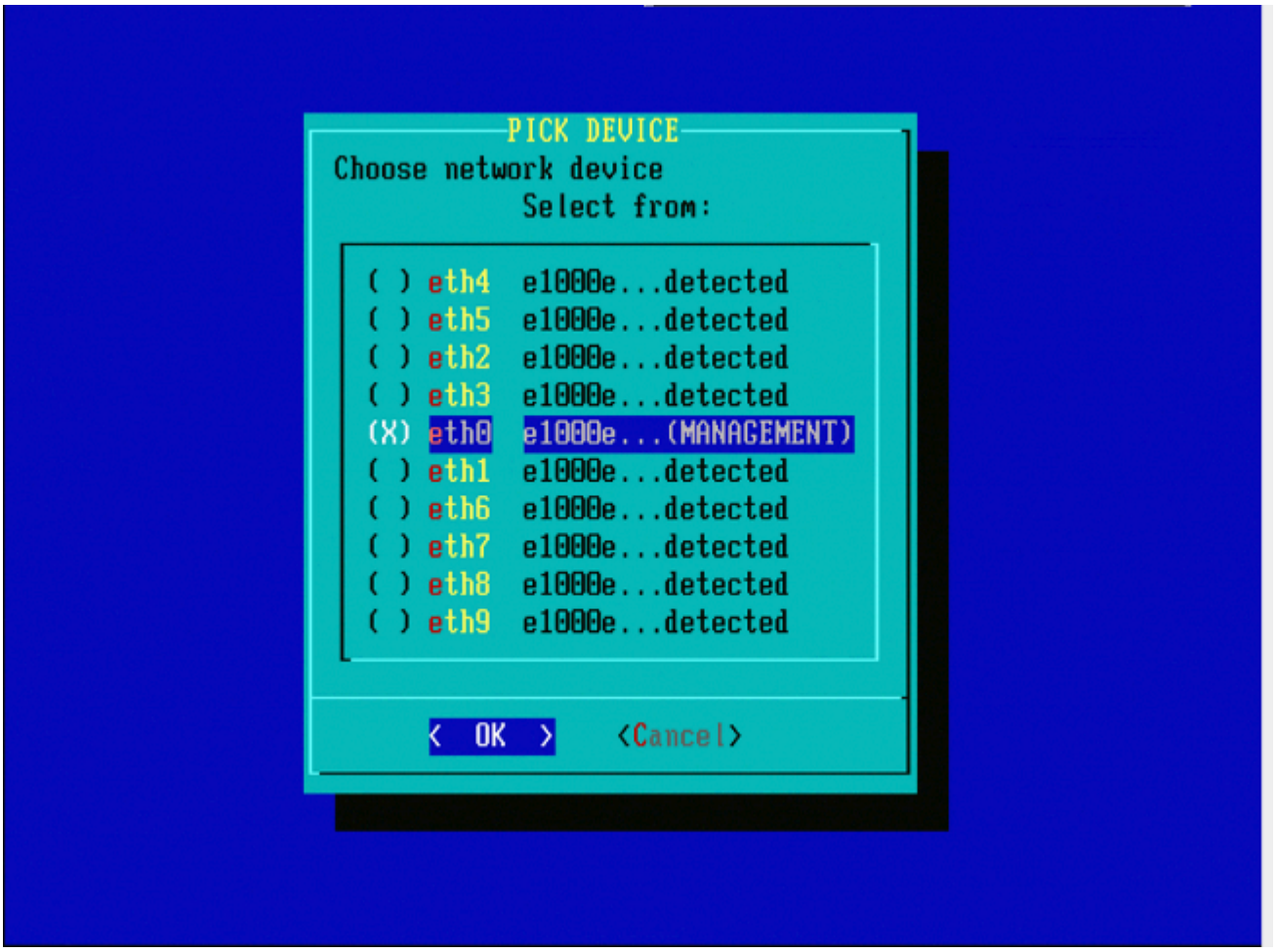


Abbildung 7: Drücken Sie die Leertaste, um das Netzwerkgerät auszuwählen.

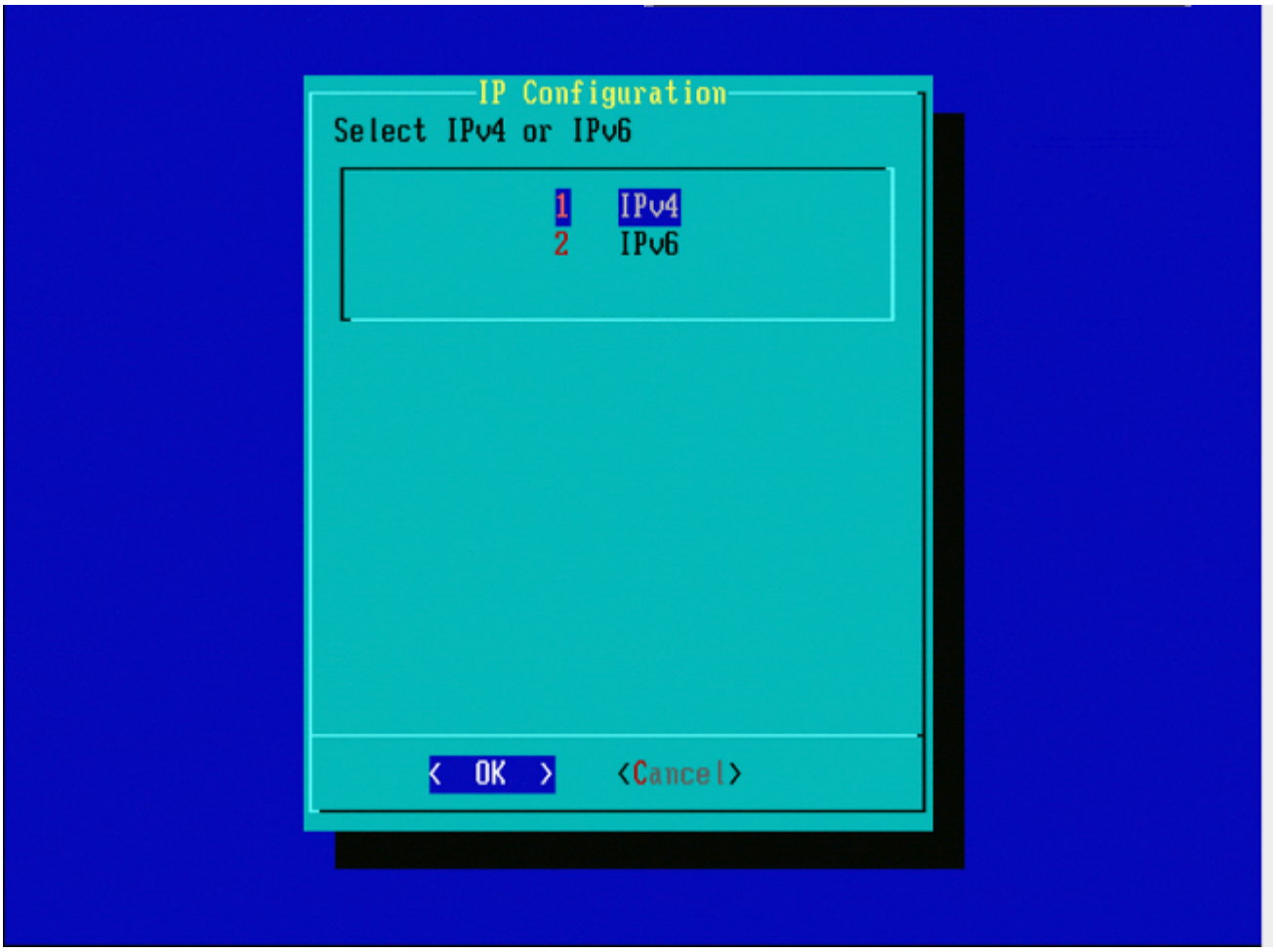


Abbildung 8

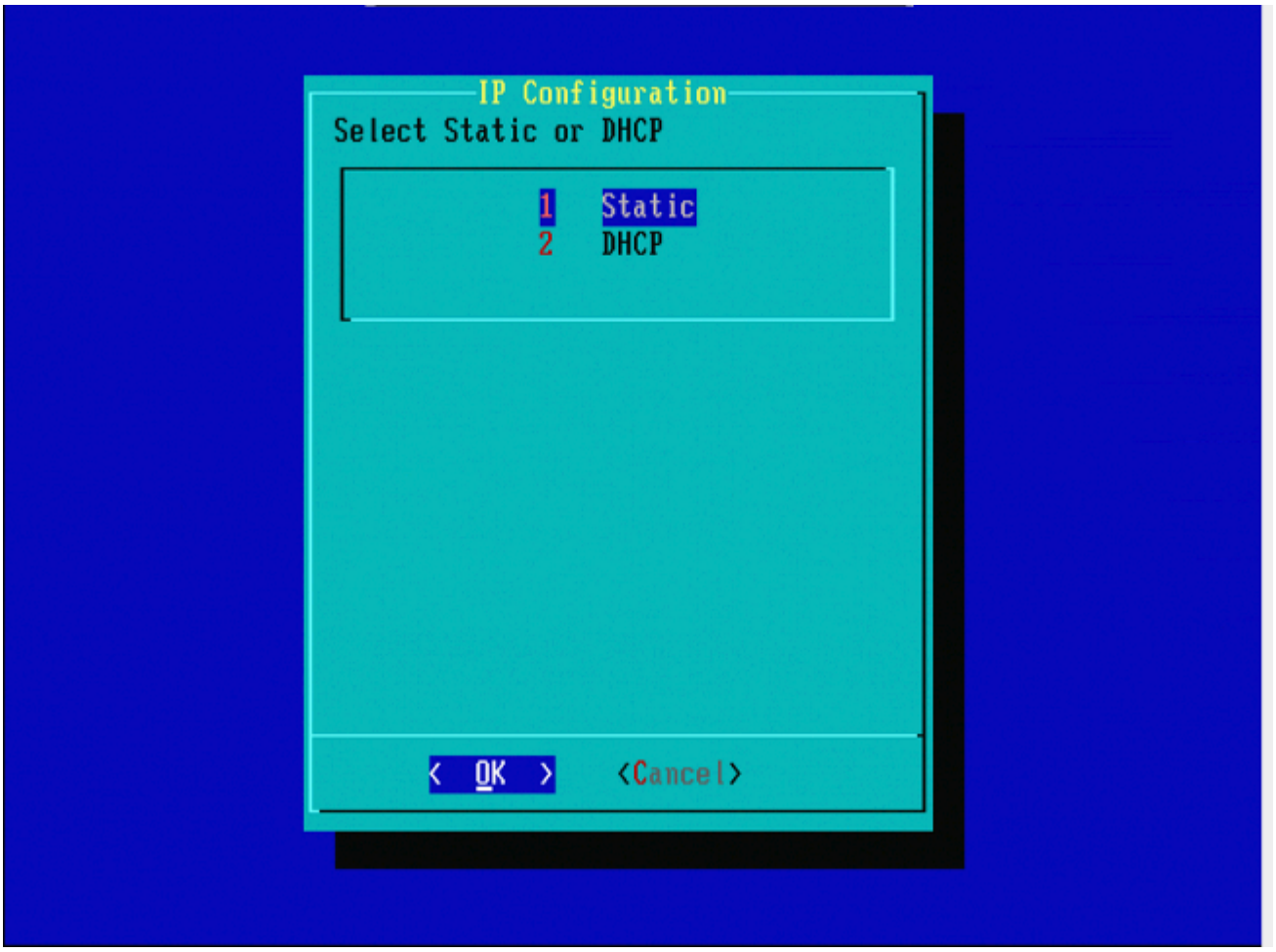

IP Configuration
Select Static or DHCP
1 Static
2 DHCP
< OK >
<Cancel>
Abbildung 9

Abbildung 10

Abbildung 11

Abbildung 12

Abbildung 13

Abbildung 14

Abbildung 15: Der Cisco Support empfiehlt die Verwendung des Secure Copy (SCP)-Protokolls.

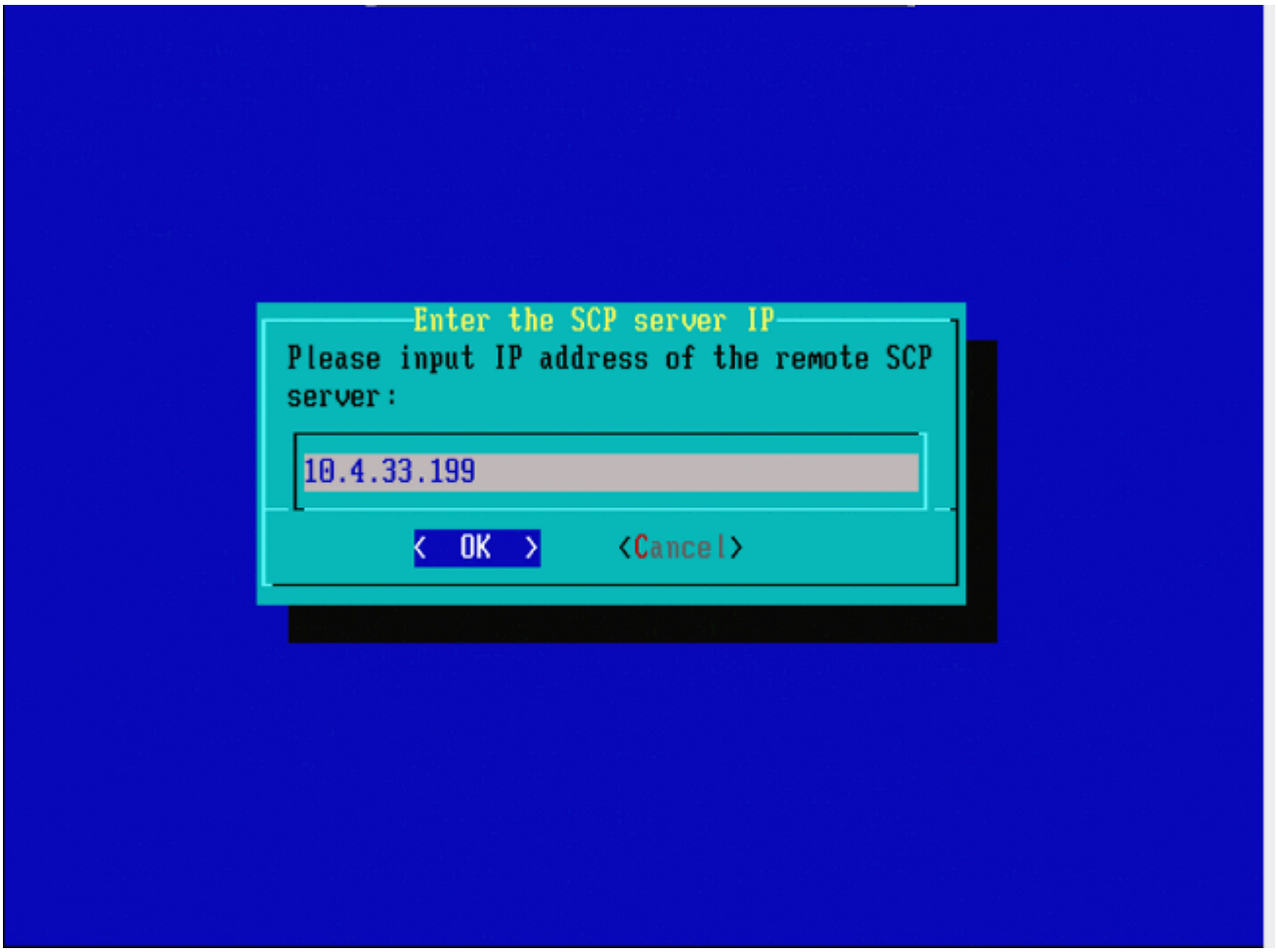


Abbildung 16: Für diesen Schritt kann ein FireSIGHT Management Center als SCP-Server verwendet werden. Fahren Sie mit diesem Verfahren fort, und verwenden Sie die IP-Adresse und die Anmeldeinformationen für das Management Center, um die Felder im Menü **Systemwiederherstellung** auszufüllen. Weitere Einzelheiten in

Ein Secure Copy (SCP)-Server wird verwendet, um Dateien sicher zu übertragen. Wenn Bei Bedarf kann ein Sourcefire Defense Center (DC) als SCP-Server verwendet werden, um Dateien auf ein anderes Sourcefire-Gerät zu übertragen. Dies kann nützlich sein, wenn ein ISO-Image zu Image-Zwecken auf ein Sourcefire-Gerät übertragen werden muss, der reguläre SCP-Server jedoch nicht erreichbar oder nicht verfügbar ist.

Schritt 1: Laden Sie eine entsprechende ISO-Datei vom Sourcefire Support-Portal auf Ihren Desktop herunter.
Schritt 2: Verwenden Sie einen SCP-Client, kopieren Sie die Datei vom Desktop in das Defense Center.

> **Tipp**: Ein SCP-Client ist normalerweise unter Linux oder Mac verfügbar. Unter Windows kann es jedoch erforderlich sein, eine SCP-Client-Software eines Drittanbieters zu installieren. Sourcefire bietet keine Empfehlungen oder Supportleistungen zur Installation bestimmter SCP-Client-Software.

Im folgenden Beispiel wird veranschaulicht, wie eine ISO-Image-Datei von Sourcefire aus dem Download-Verzeichnis eines Linux-Systems in das **/var/tmpdirectory** des Sourcefire Defense Center kopiert wird:

<#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

> **Achtung**: Ändern Sie nicht den Namen der ISO-Datei. Es kann zu Problemen bei der Erkennung der Datei während eines neuen Images führen.

Jetzt wird die Datei in das Verteidigungszentrum kopiert. Sie können mit dem Neuabbildungsprozess für Sourcefire-Geräte fortfahren. Bei Bedarf können Sie beim erneuten Abbild die IP-Adresse und den Benutzernamen des Rechenzentrums sowie den Pfad angeben, in den Sie die Abbilddatei mit den vorherigen Anweisungen kopiert haben.

> **Warnung:** Nach Abschluss des neuen Images müssen Sie die .iso-Datei aus dem **/var/tmp-**Verzeichnis des Defense Center entfernen, um die Auslastung des Festplattenspeichers zu reduzieren.

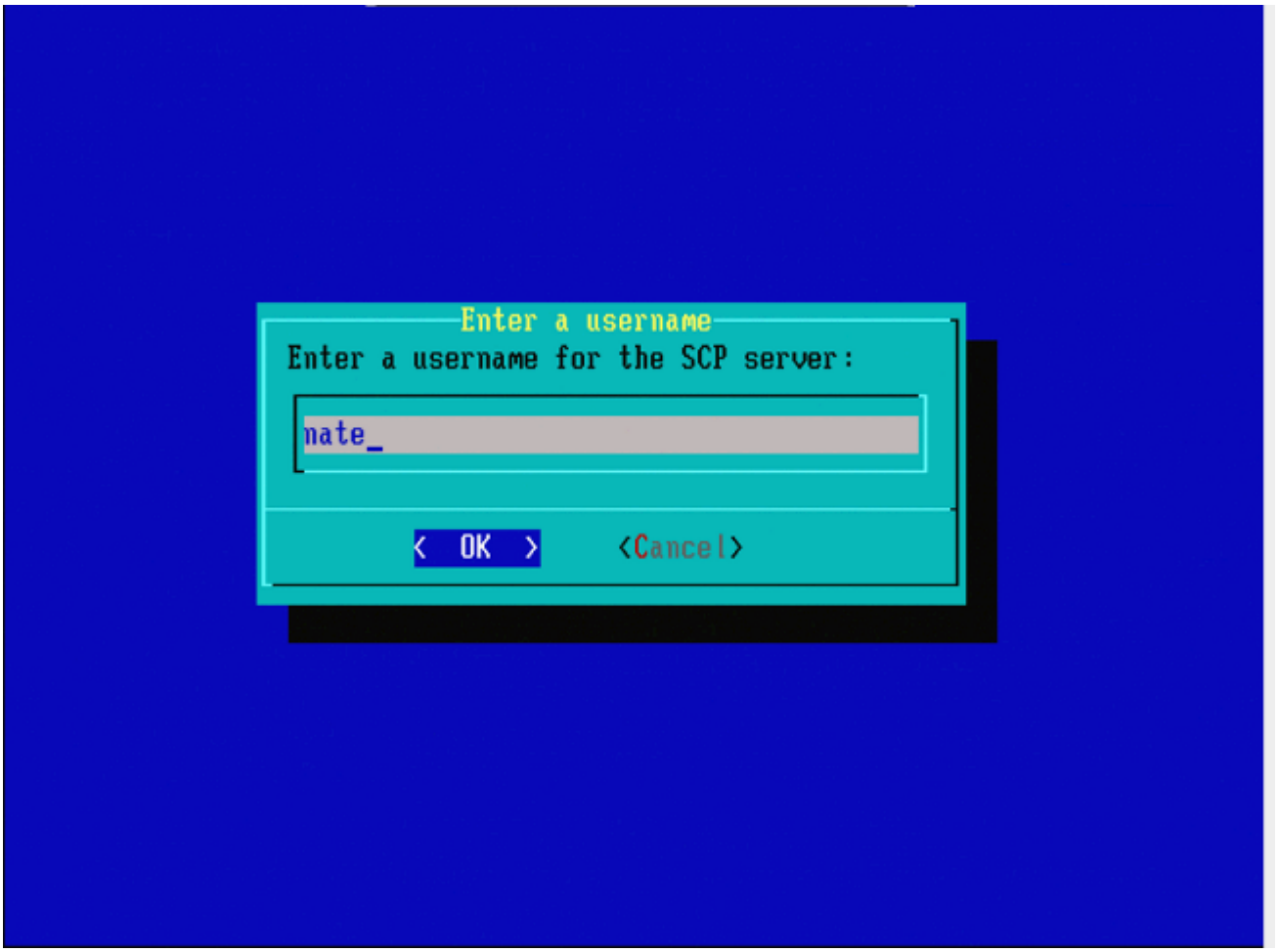


Abbildung 17

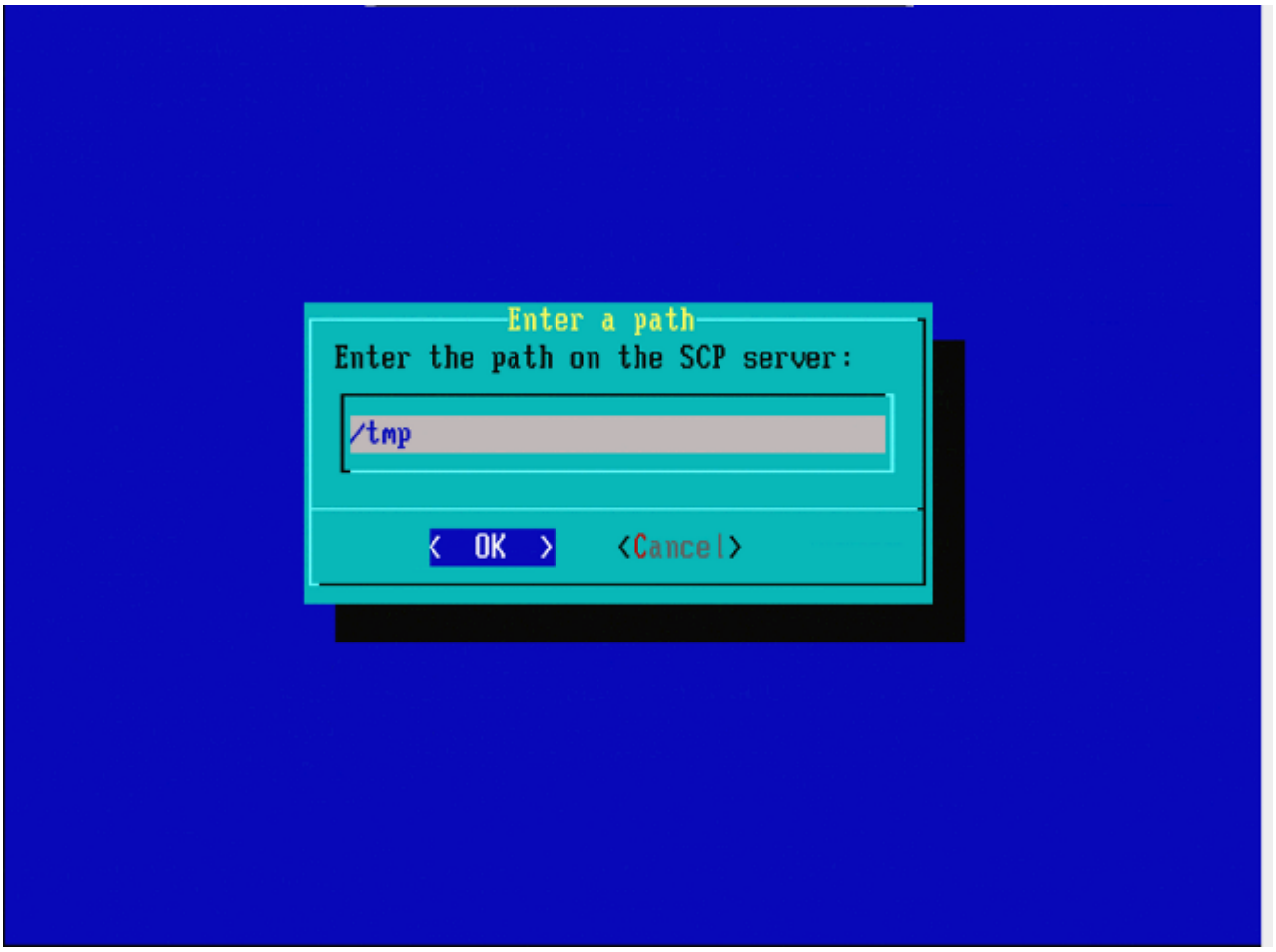


Abbildung 18

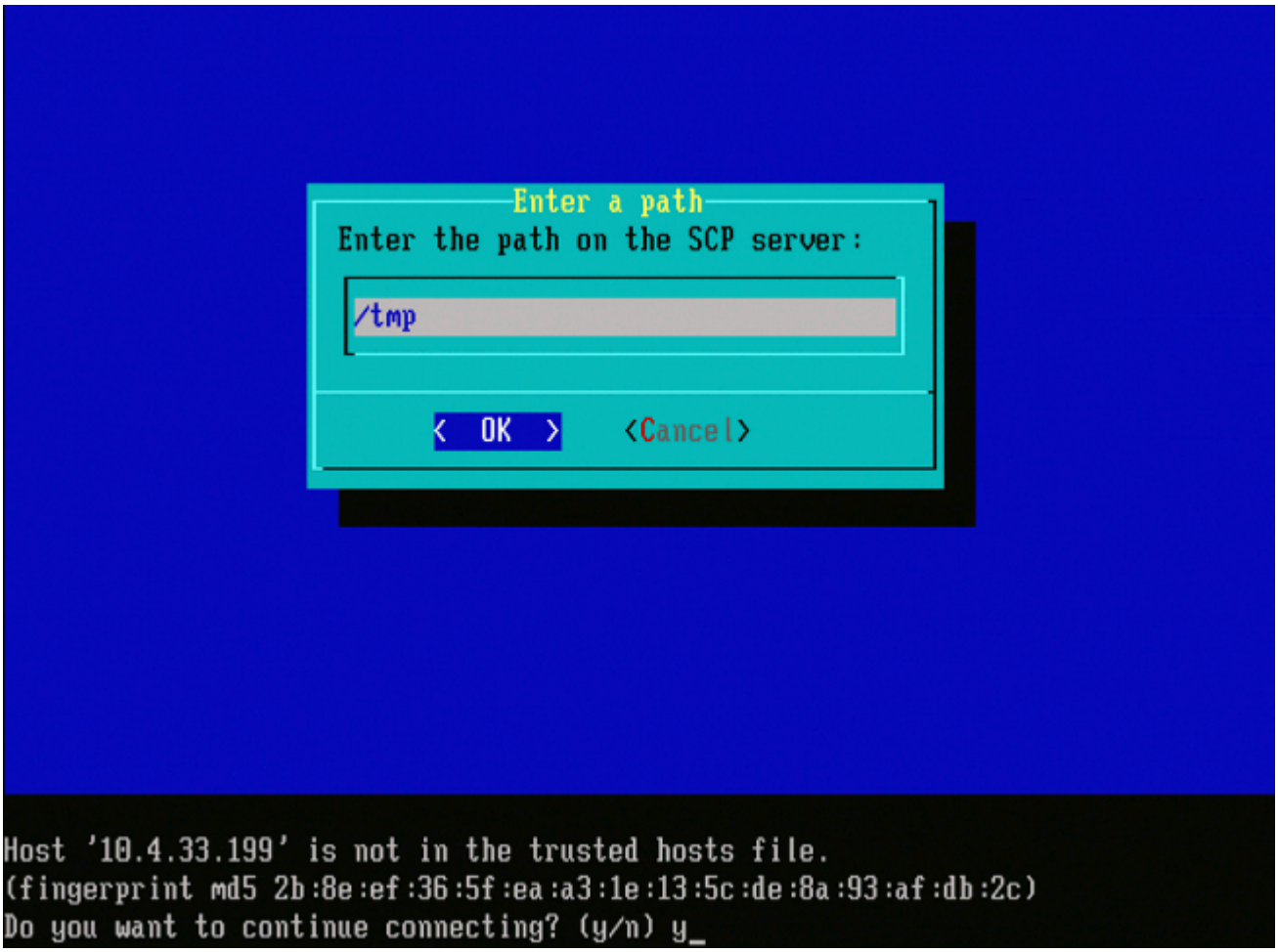


Abbildung 19

Hinweis: Wenn Sie an dieser Stelle anstelle der erwarteten Meldung einen Verbindungsfehler erhalten, überprüfen Sie Ihre Verbindung zum SSH-Server.

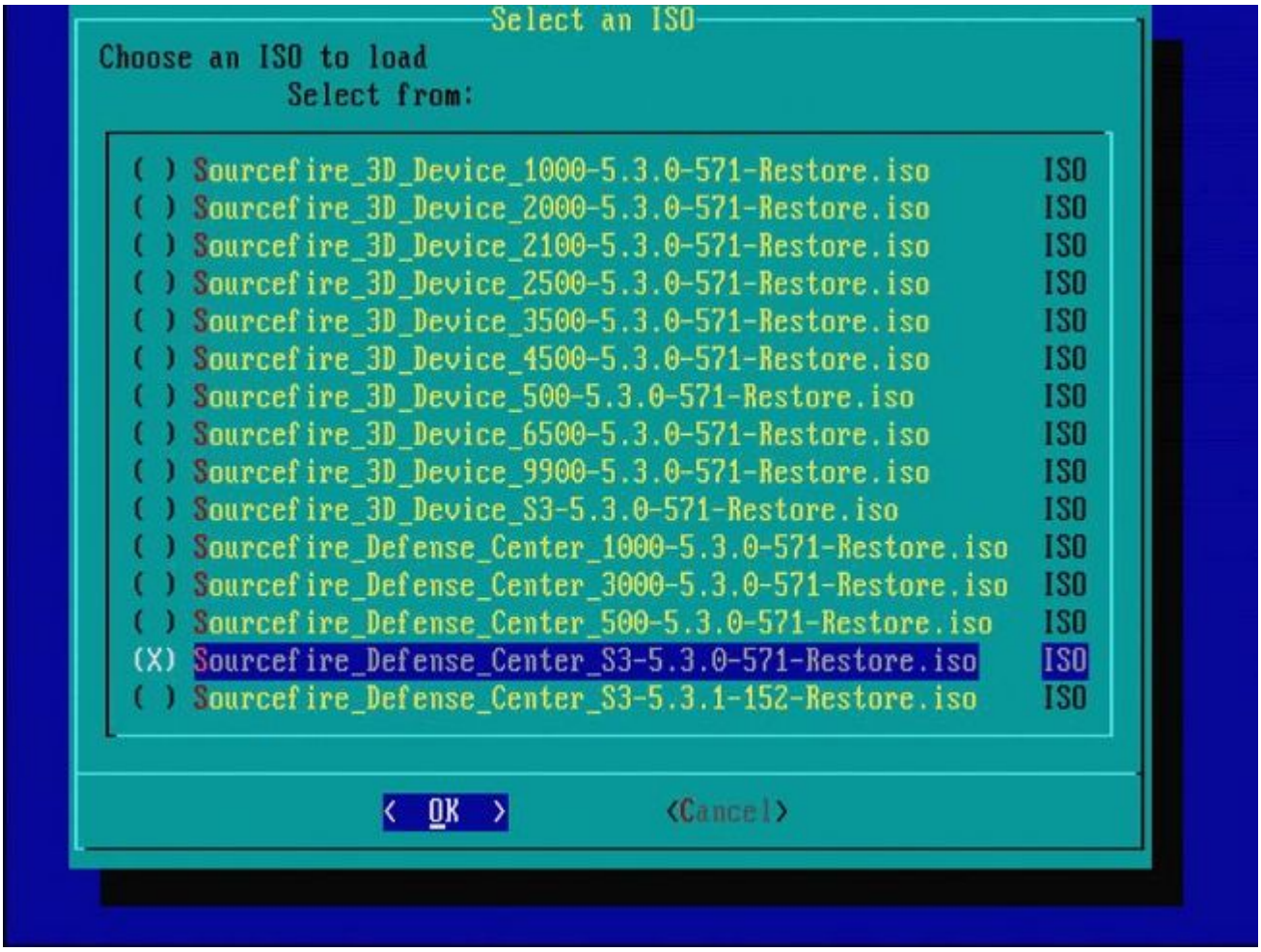


Abbildung 20: Drücken Sie die Leertaste, um das ISO-Bild auszuwählen.

Hinweis: Es ist erforderlich, die Standarddateinamen für die ISO-Dateien zu verwenden. Andernfalls werden die Dateien in diesem Schritt möglicherweise nicht erkannt.
Fehler: Kein ISO-Image gefunden
In Version 6.3 wurde die ISO-Namenskonvention von Sourcefire_3D_Device_S3-<ver>-<build>-Restore.iso in Cisco_Firepower_NGIPS_Appliance-<ver>-<build>-Restore.iso geändert. Wenn Sie auf **"No ISO Image Were Found" (Kein ISO-Image gefunden) stoßen,** benennen Sie die ISO-Datei in den alten Dateinamen um. Dies geschieht in der Regel, wenn ein Re-Image von 6.2.x oder älteren Version auf 6.3.0 oder höher.

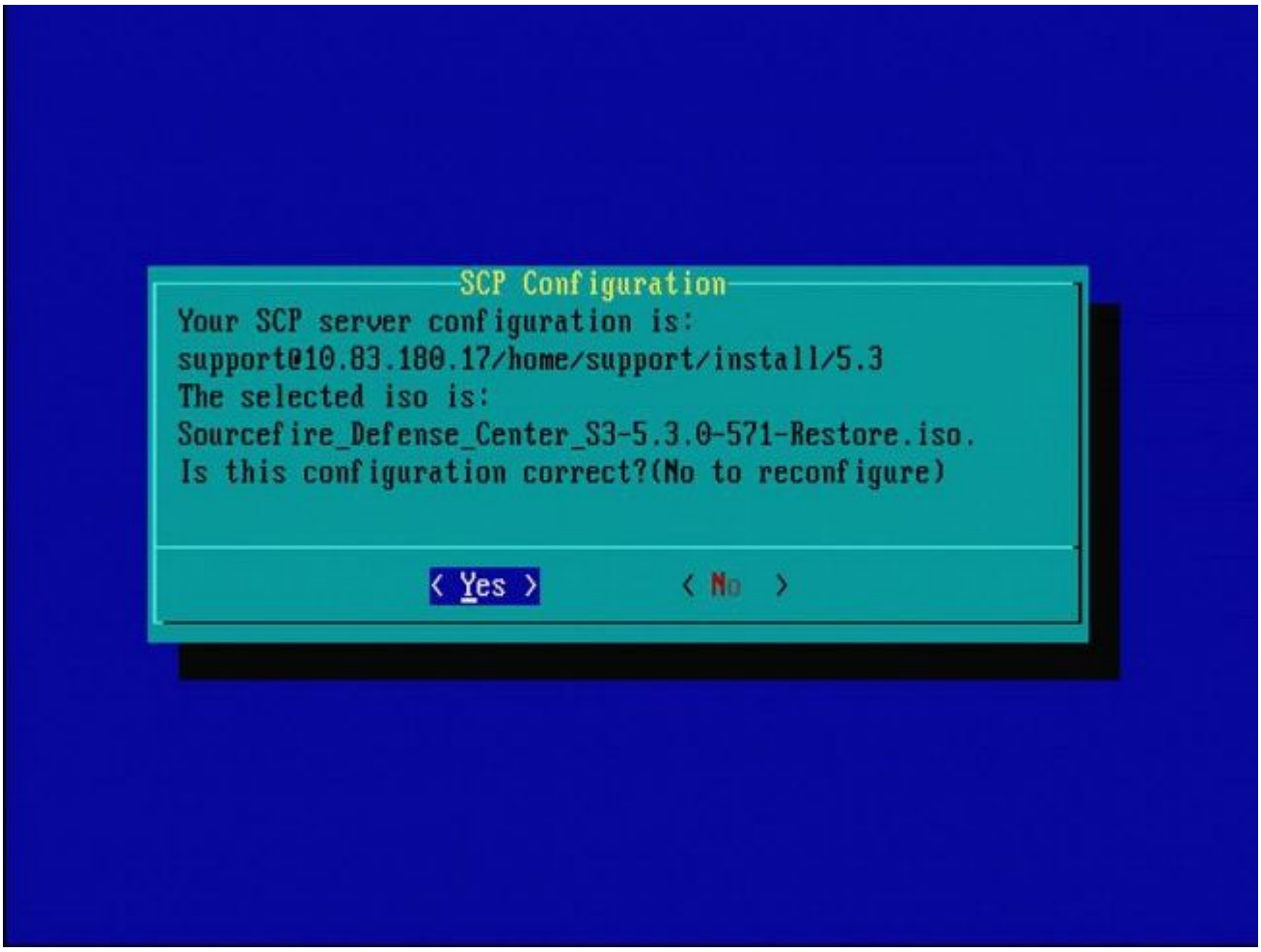


Abbildung 21

Abbildung 22: Der Cisco Support empfiehlt, Schritt 3 in diesem Prozess zu überspringen. Patches und Snort Rule Updates (SRUs) können nach Abschluss des neuen Images installiert werden.

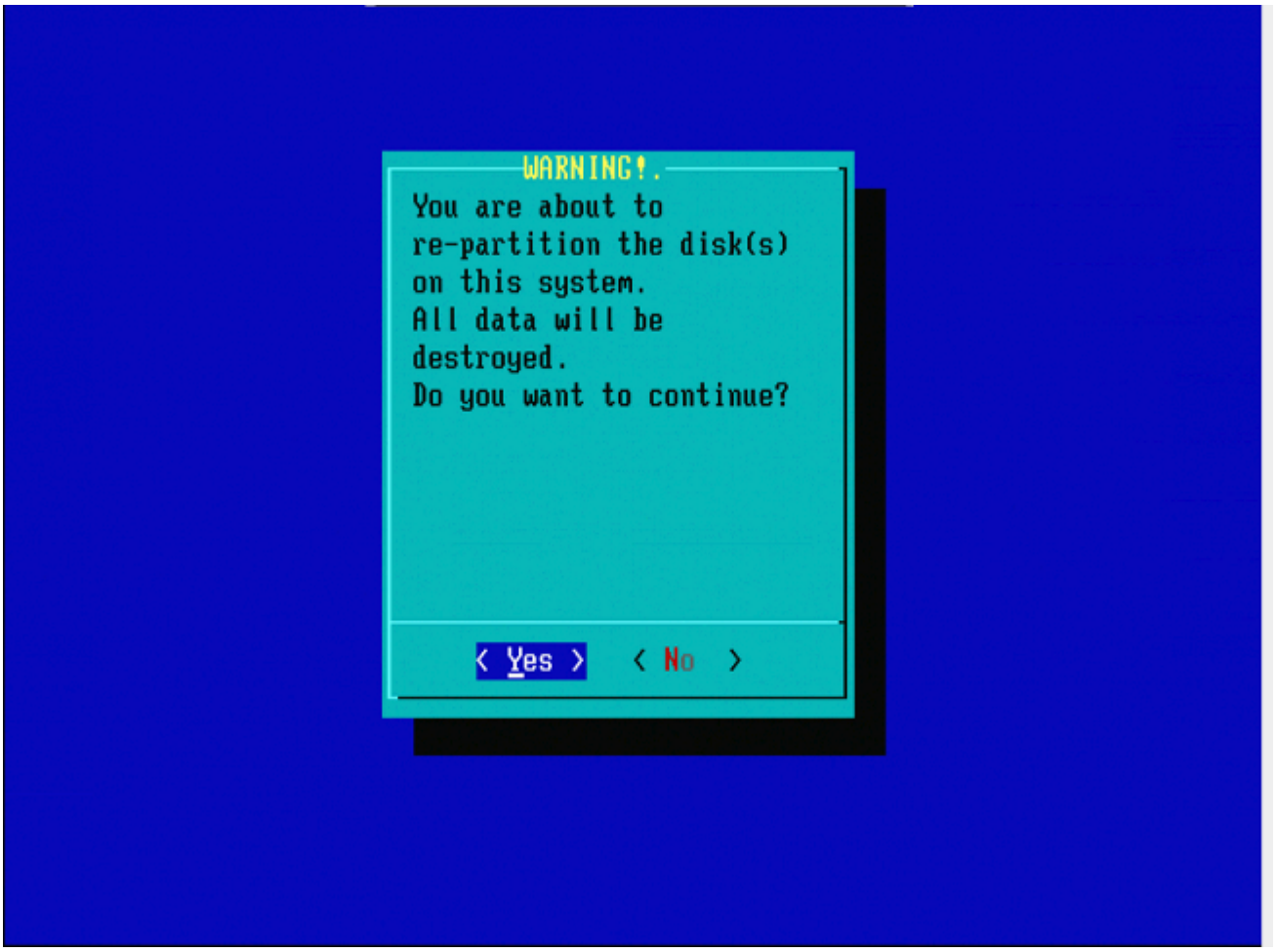


Abbildung 23

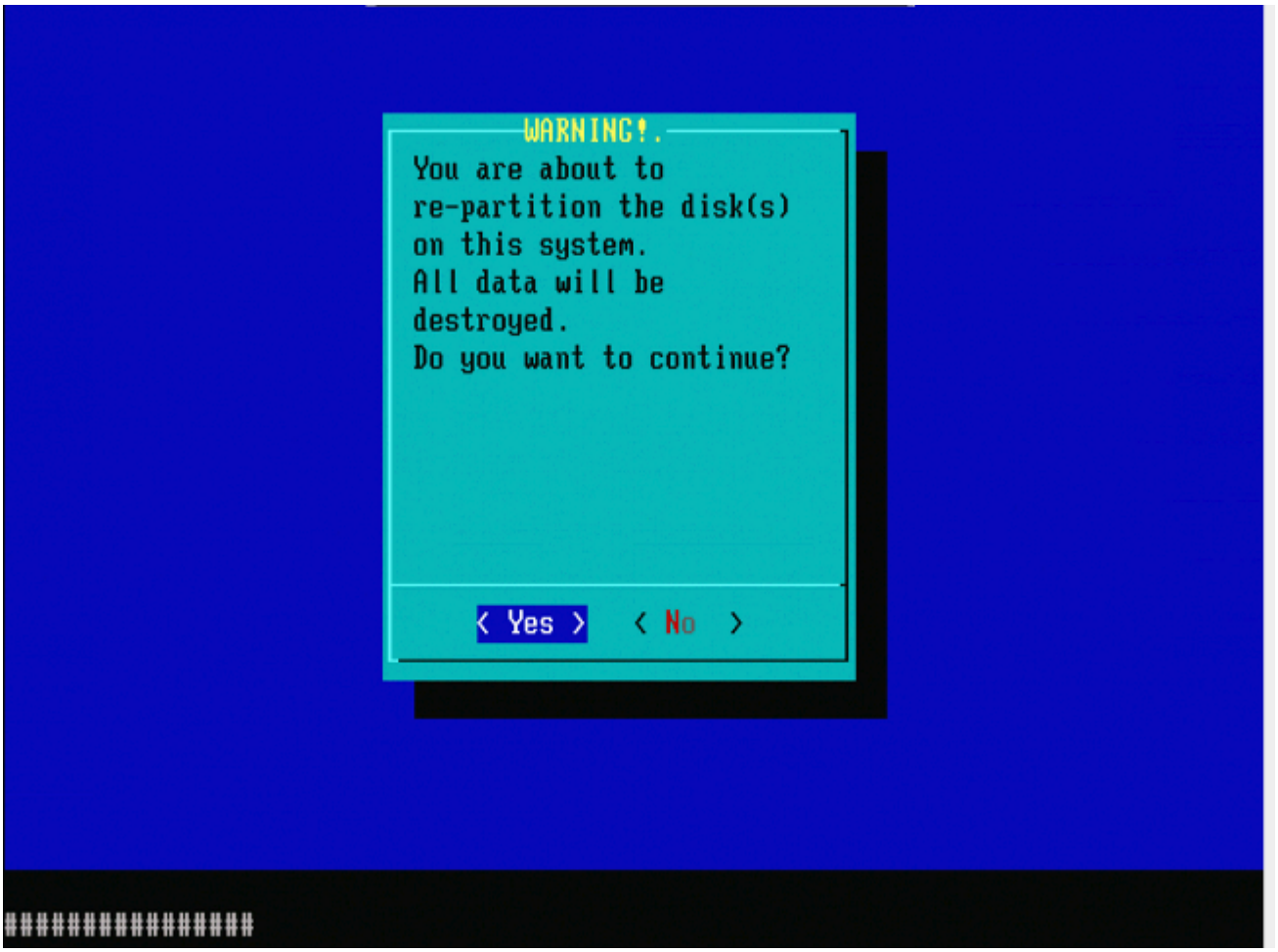


Abbildung 24

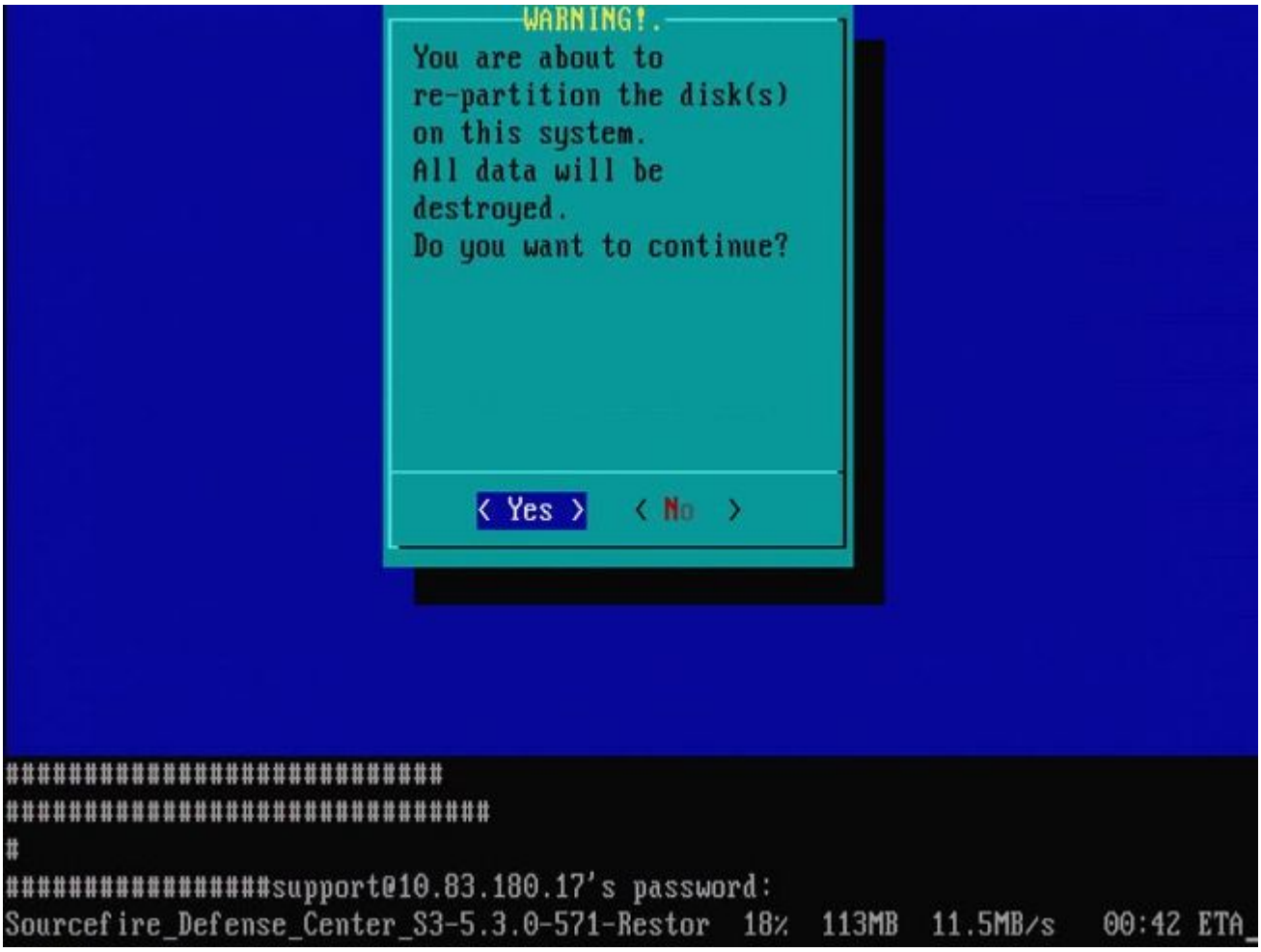


Abbildung 25

Abbildung 26

Wichtiger Hinweis in Bezug auf ein Reimage von einer anderen Haupt-Softwareversion: Wenn Sie versuchen, ein Image eines Geräts wiederherzustellen, auf dem zuvor eine andere Haupt-Softwareversion ausgeführt wurde, z. B. ein Reimage von 5.1 > 5.2, 5.2 > 5.3, 5.3 > 5.2 usw., müssen Sie die Schritte in den Abbildungen 1 - 26 **zweimal** ausführen.

1. Nachdem Sie an der Eingabeaufforderung **OK** ausgewählt haben, wie in Abbildung 26 dargestellt, wird die Partition zur Systemwiederherstellung auf die neue Version geflashed und die Appliance wird neu gestartet.
2. Nach dem Neustart müssen Sie den Neuabbildungsprozess von vorn beginnen und den in den Abbildungen 27b bis 31 dargestellten Prozess fortsetzen.

Wenn es sich um das erste Reimage aus einer anderen Haupt-Softwareversion handelt, sehen Sie den Bildschirm wie in Abbildung 27a und dann Abbildungen 31 und 32 dargestellt.

> **Achtung**: Wenn Sie diesen Bildschirm sehen, gibt es eine mögliche Verzögerung ohne sichtbare Ausgabe nach "Hardware prüfen" und vor "Das USB-Gerät...". Drücken **Sie** zu diesem Zeitpunkt **keine** Tasten, oder das Gerät wird in einen unbrauchbaren Zustand versetzt und muss erneut mit einem Image versehen werden.

Wenn dies nicht der Fall ist, sehen Sie die Bildschirme in Abbildung 27b bis Abbildung 32.

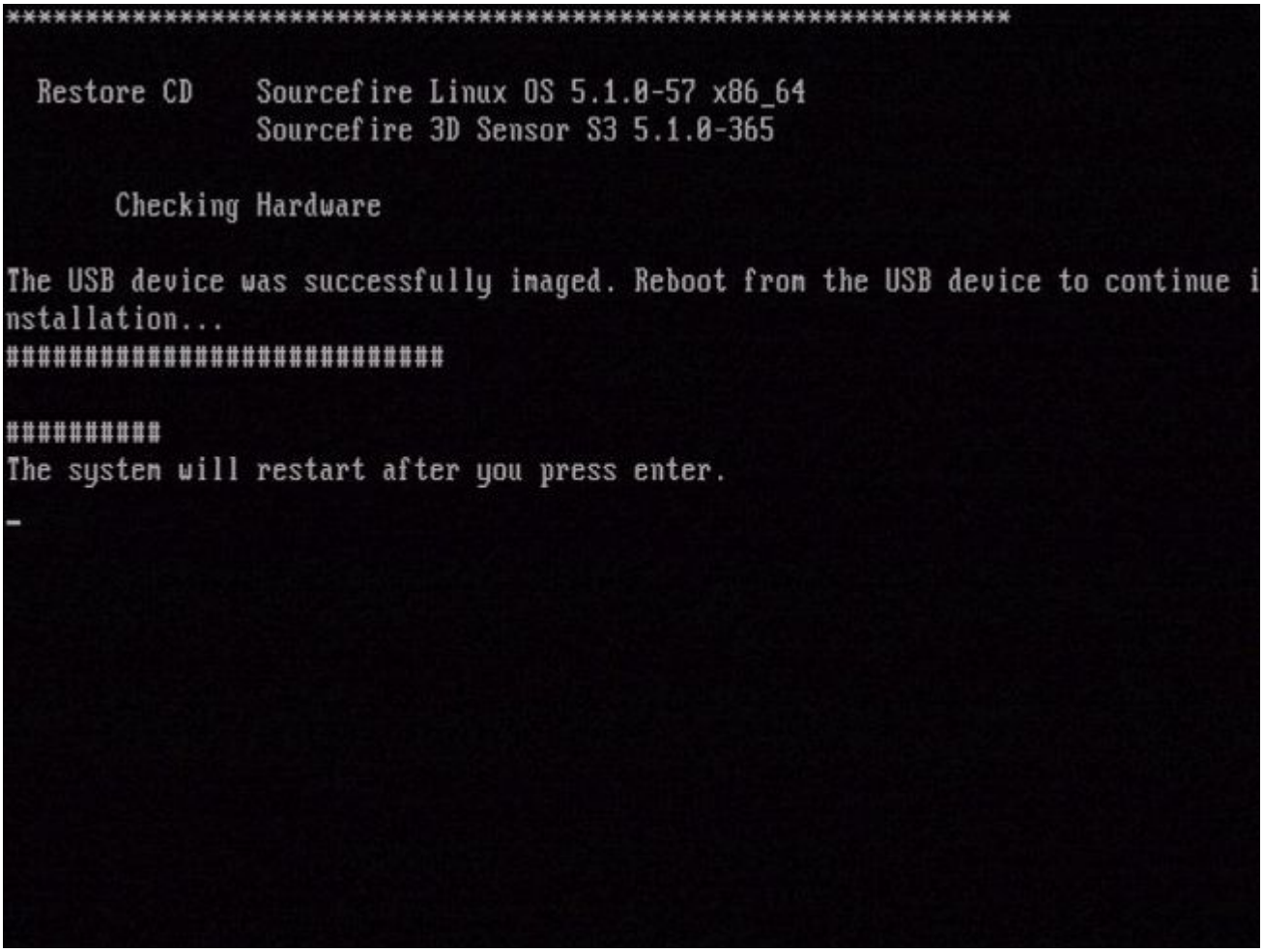


Abbildung 27a

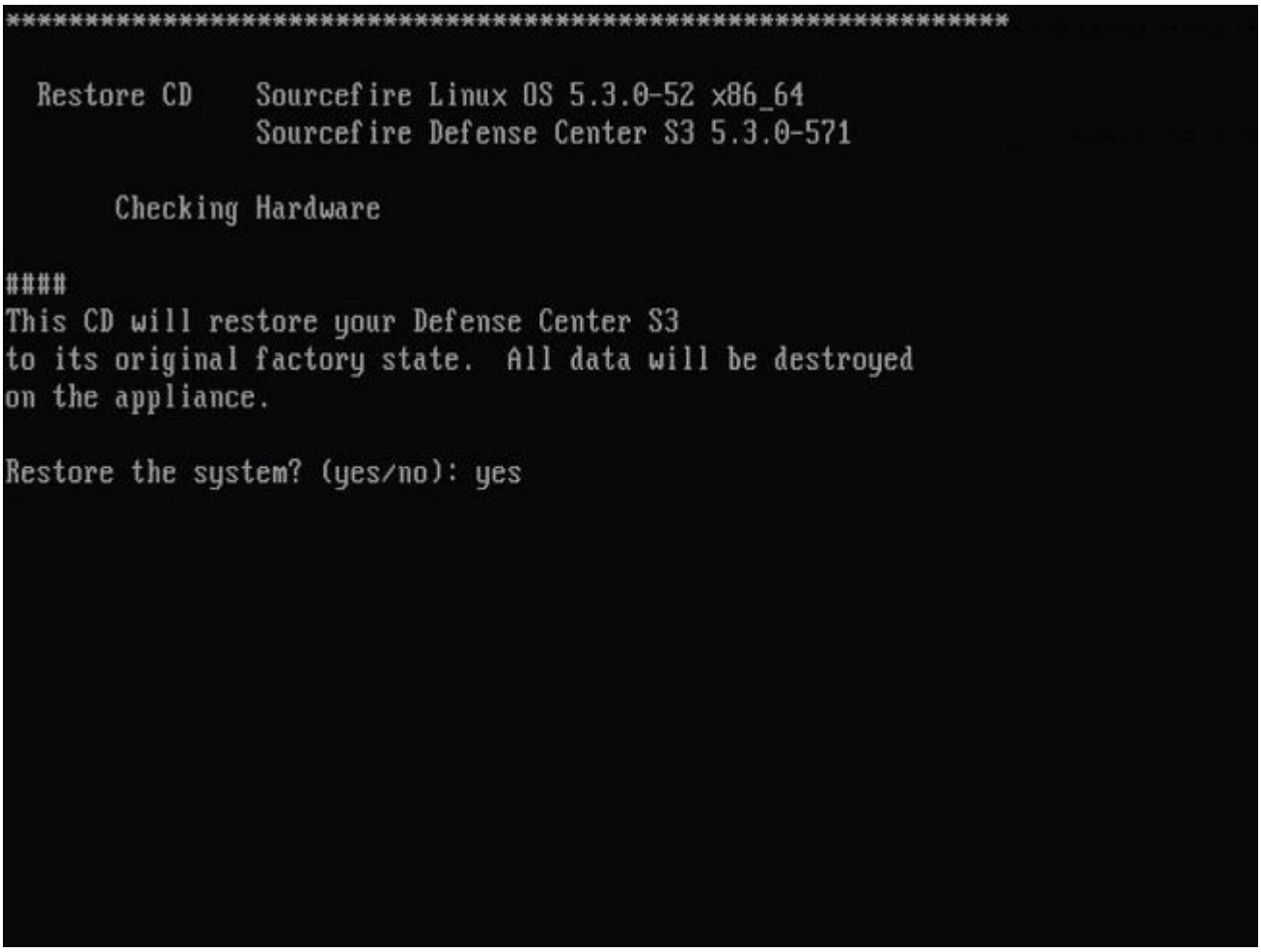


Abbildung 27b

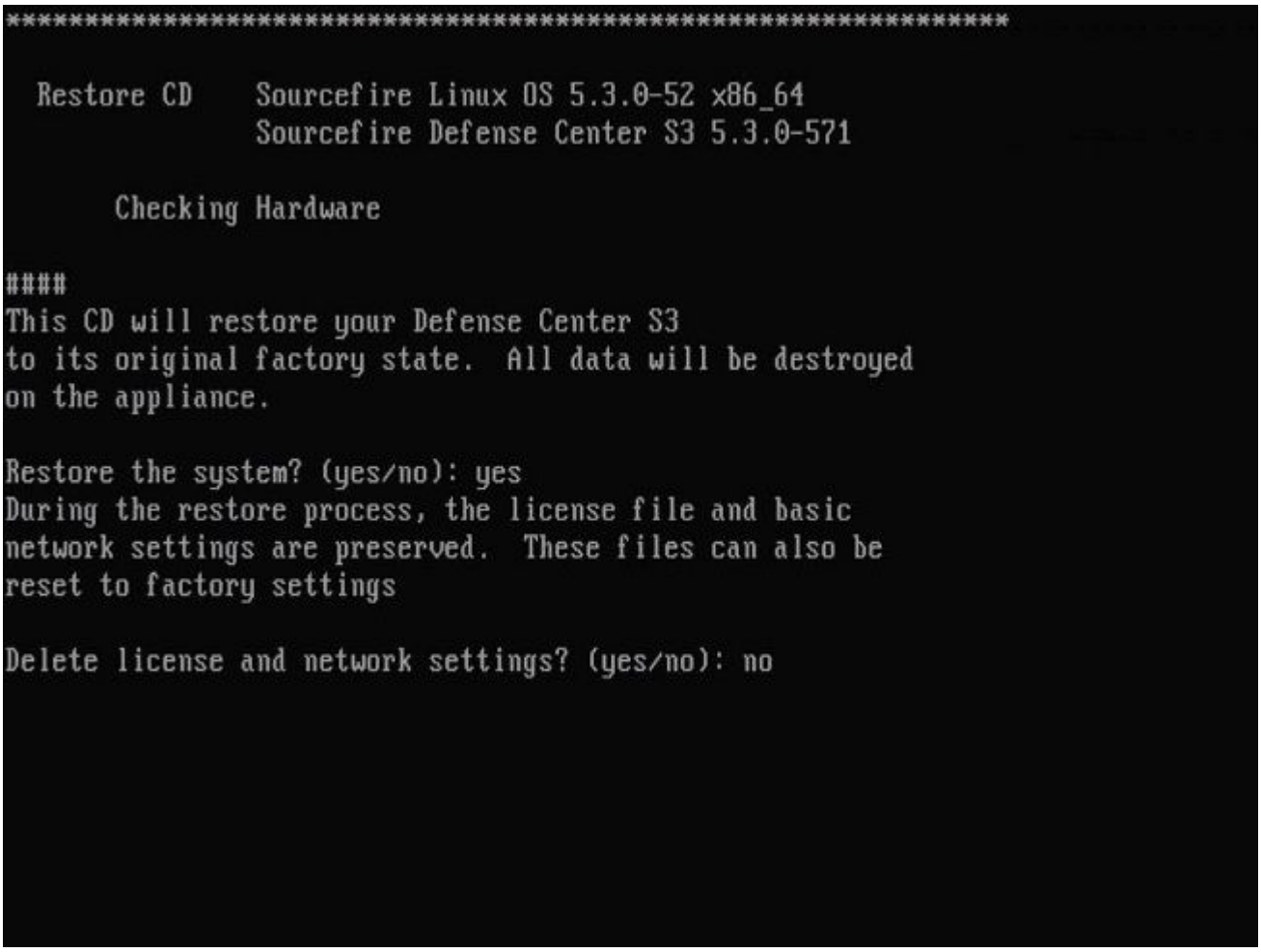


Abbildung 28

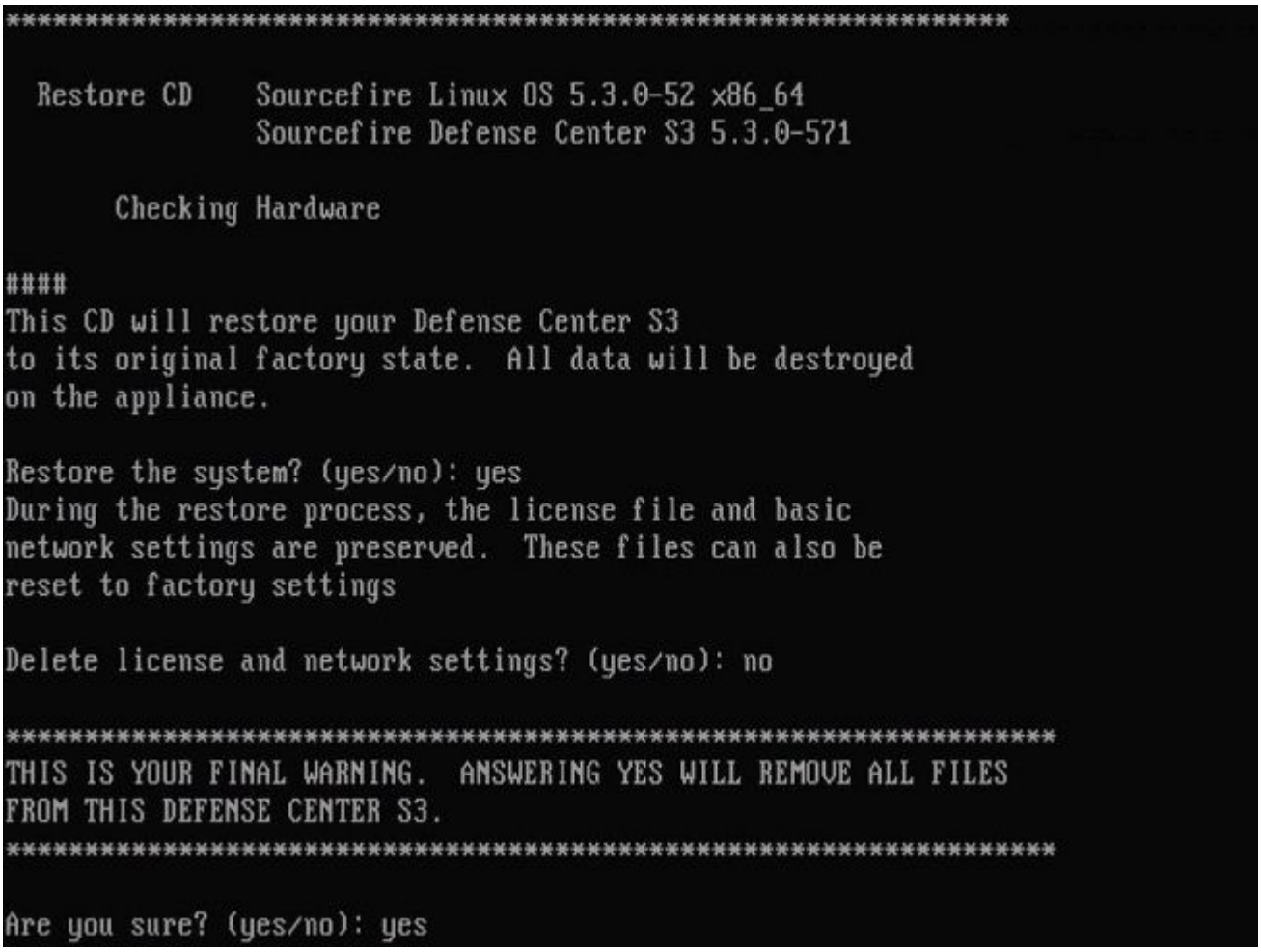


Abbildung 29

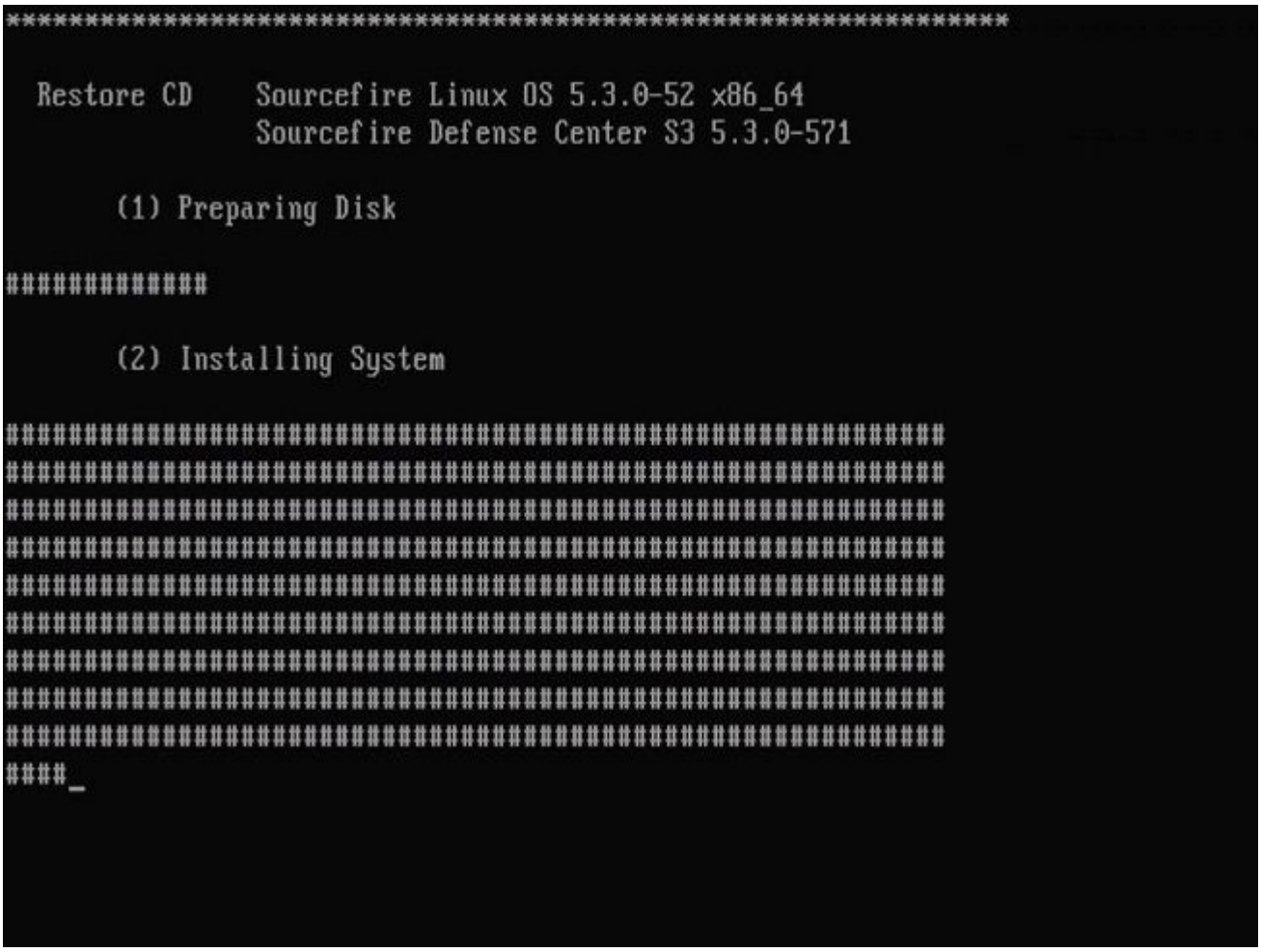


Abbildung 30

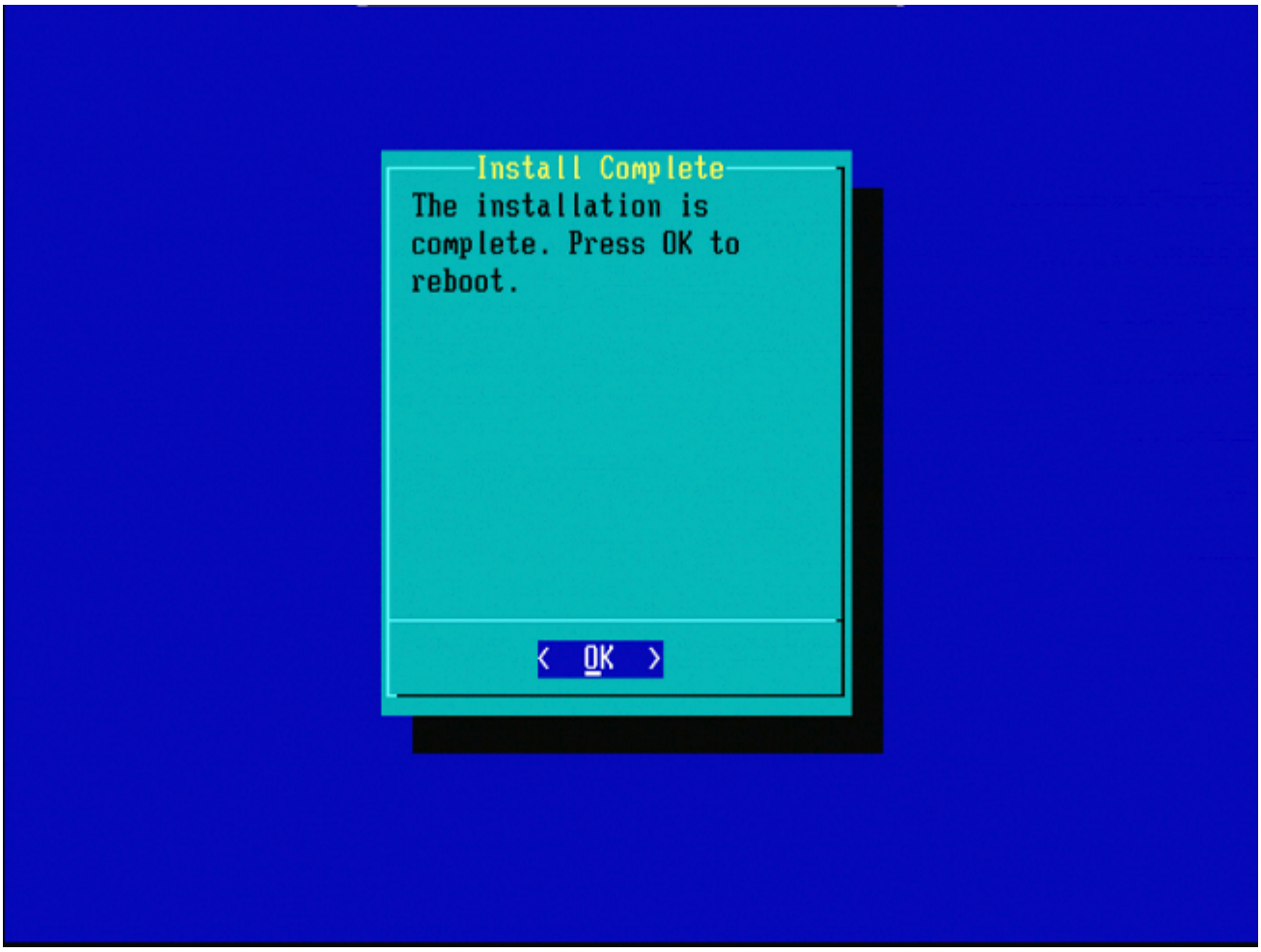


Abbildung 31

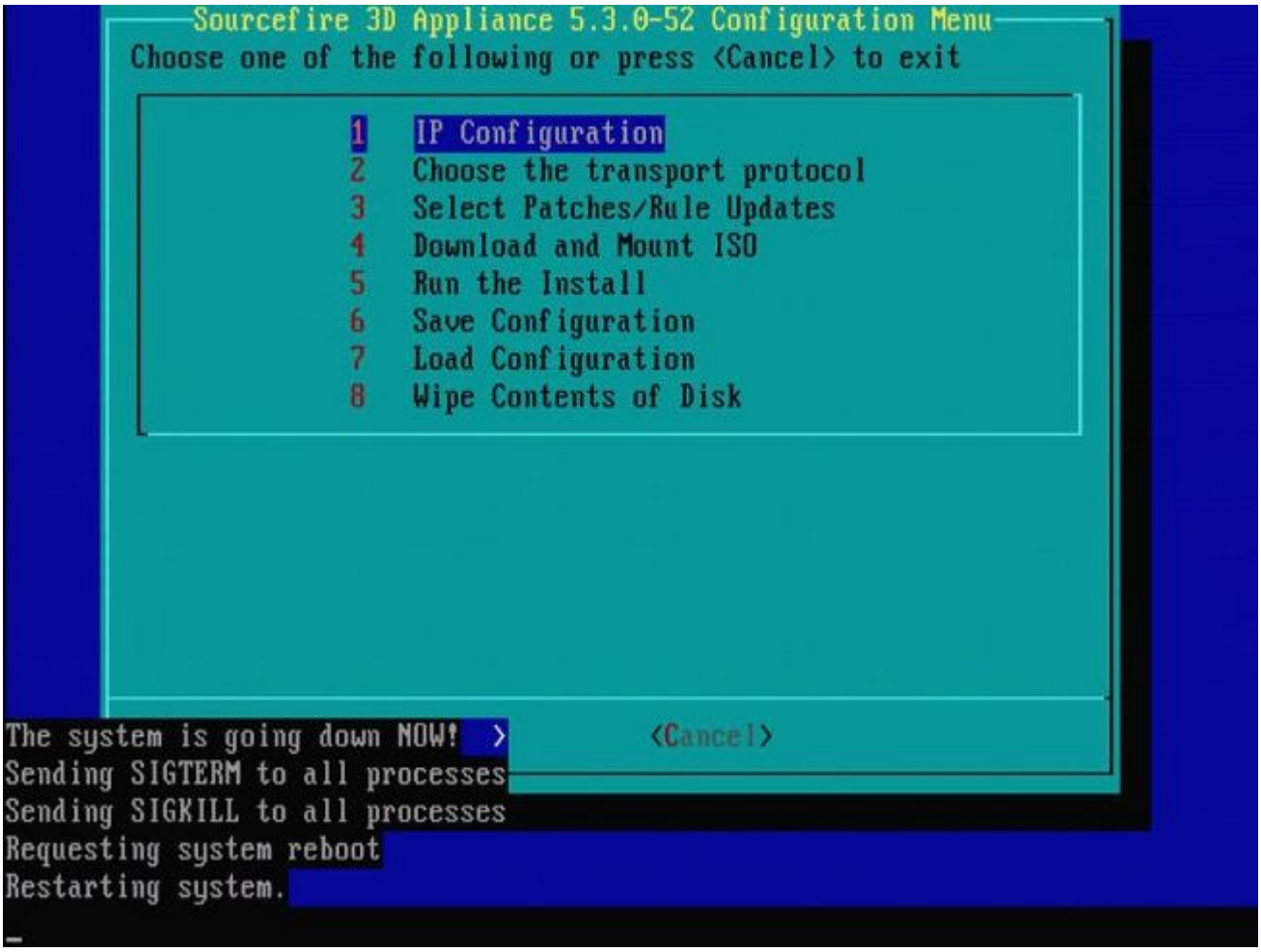


Abbildung 32

Cisco Firepower Management Center 1000, 2500 und 4500

Bei FMC 1000, 2500 und 4500 sind die Optionen unterschiedlich. Verwenden Sie einen KVM-Switch oder den CIMC, und während das Gerät startet, stehen Ihnen folgende Optionen zur Verfügung:

1 - Cisco FirePOWER Management Console VGA-Modus

2 - Cisco FirePOWER Management Console (seriell)

3 - Systemwiederherstellungsmodus der Cisco FirePOWER Management Console

4 - Kennwortwiederherstellungsmodus der Cisco FirePOWER Management-Konsole

Wenn Sie in den Wiederherstellungsmodus mit Benutzeroberfläche wechseln möchten, wählen Sie die Option "Cisco FirePOWER Management Console System Restor Mode" (Option **3)** und dann "Cisco FirePOWER Management Console System Restore VGA Mode" (Option **1) aus.**

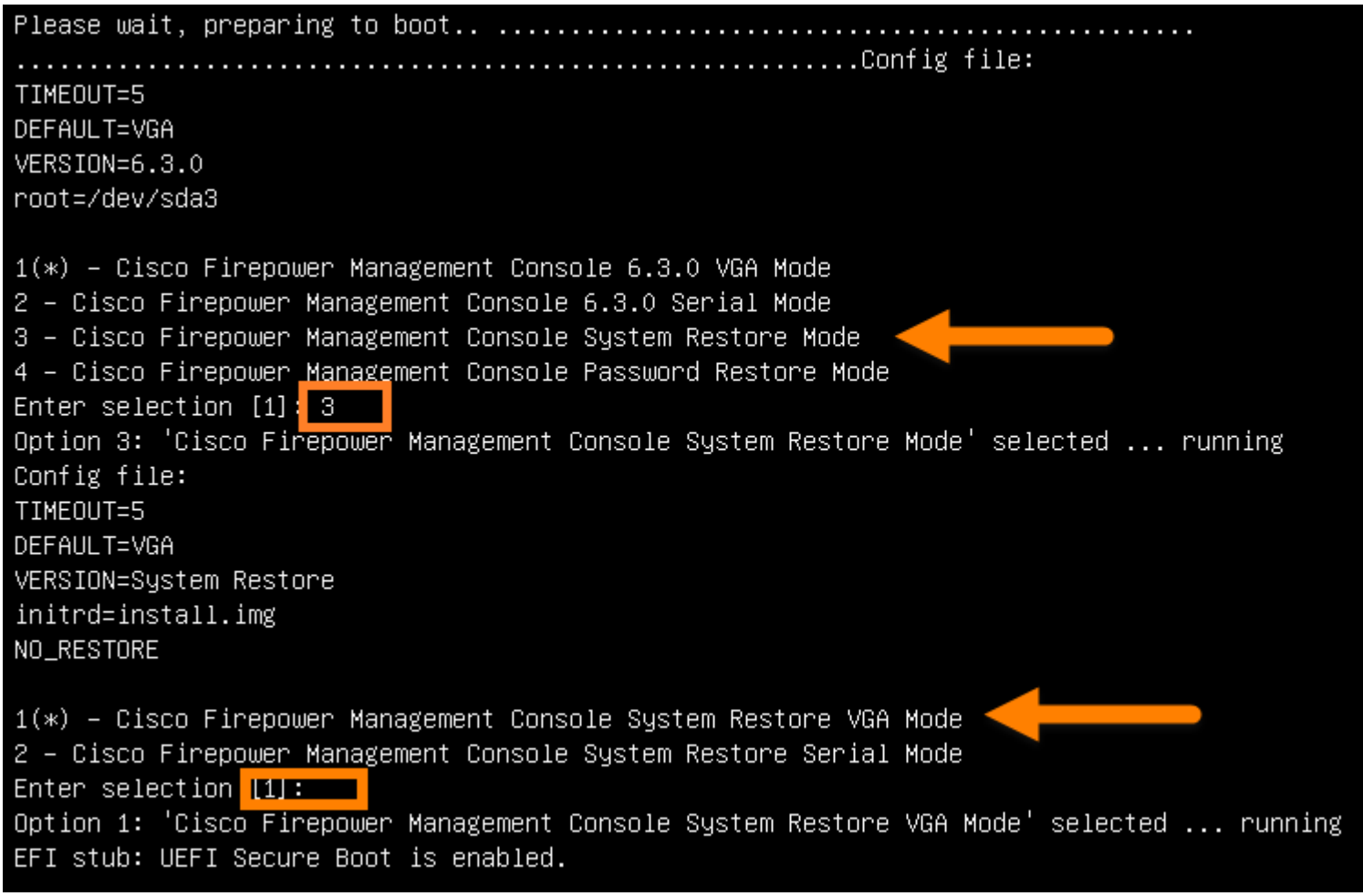


Abbildung 33

Der restliche Prozess ist der gleiche wie bei anderen FMC Appliances.

Fehlerbehebung

Die Menüoption System_Restore LILO ist nicht aufgeführt.

Das FireSIGHT Management Center und die Appliances der Serien FirePOWER 7000 und 8000 verfügen über ein integriertes Flash-Laufwerk, auf dem sich das Image-System befindet. Wenn die Option "**System_Restore**" nicht im Startmenü von LILO (Linux Loader) aufgeführt ist, ist es weiterhin möglich, auf dieses Laufwerk zuzugreifen, um das neue Image abzuschließen.

7010-, 7020- und 7030-Geräte

Wenn Sie ein Gerät der 70XX-Serie verwenden, führen Sie die folgenden Schritte aus, um das Startgerät auszuwählen:

1. Schalten Sie die Einheit ordnungsgemäß aus.

2. Schalten Sie die Appliance ein, und drücken Sie wiederholt die **Entf**-Taste, während die Appliance hochgefahren wird, um auf den Bildschirm zur Auswahl des Startgeräts zuzugreifen. Das Bild finden Sie hier:

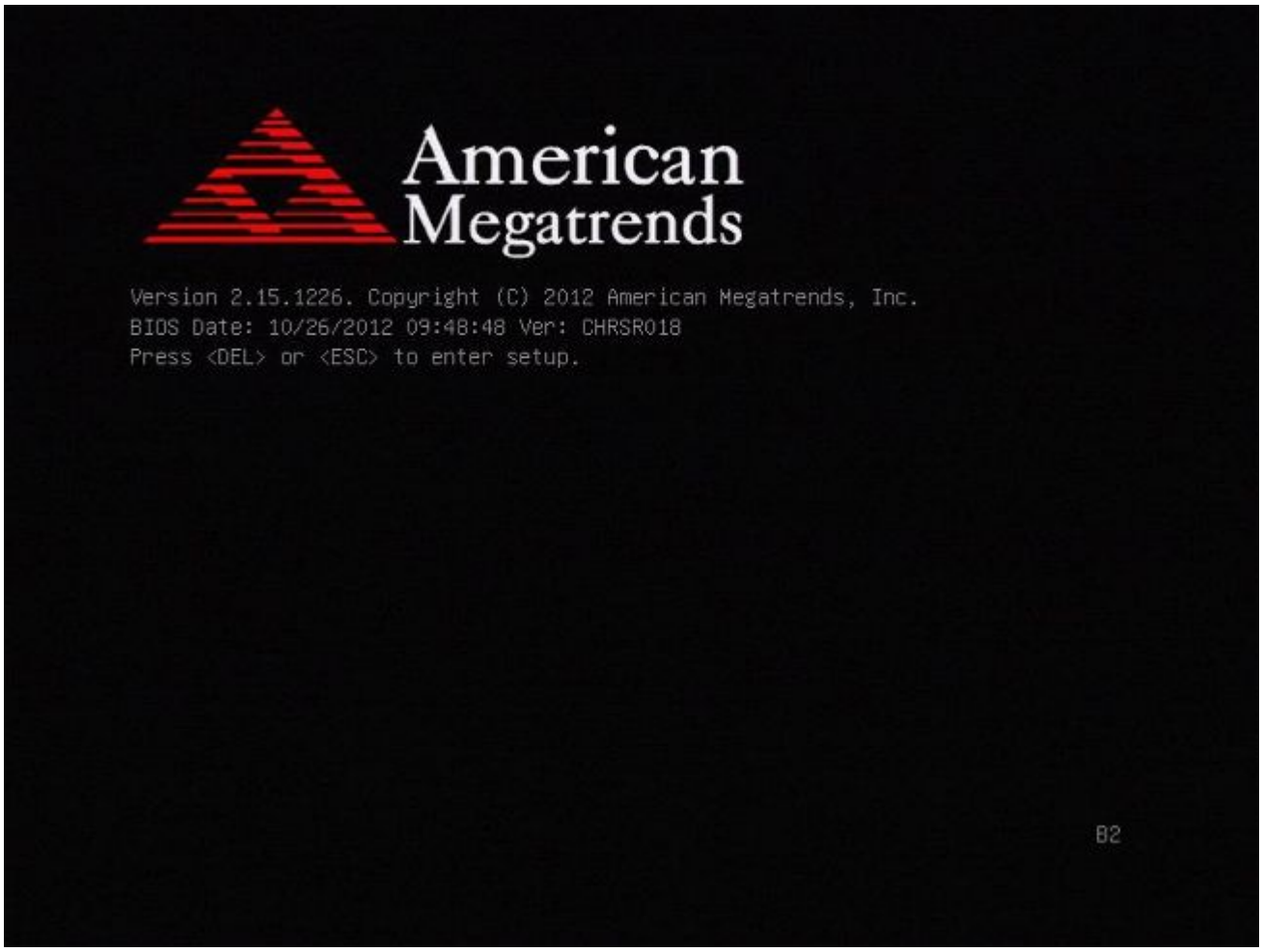


Abbildung A1

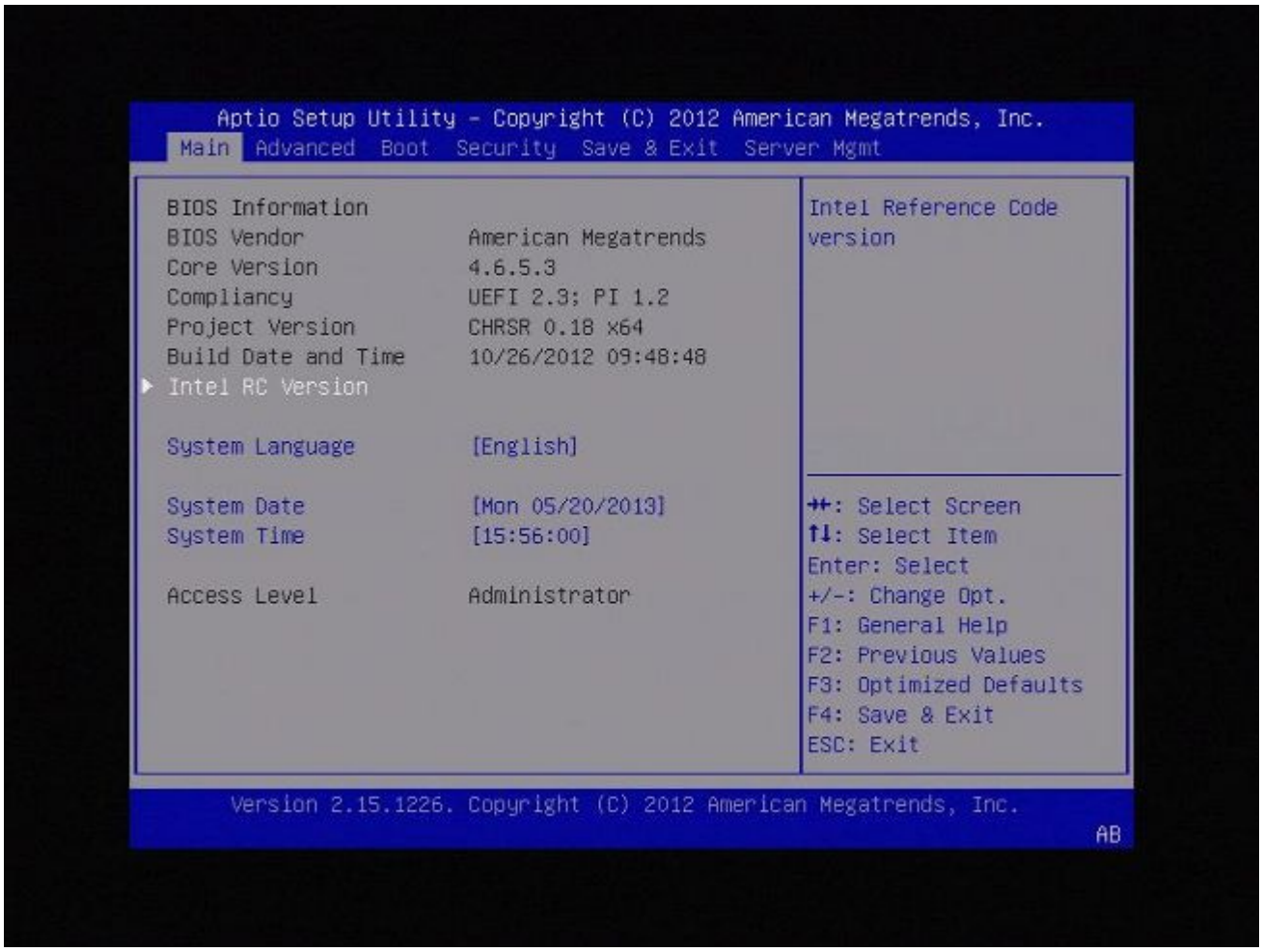


Abbildung A2

3. Verwenden Sie den Pfeil nach rechts, um die Registerkarte **Speichern und Beenden** auszuwählen. Verwenden Sie auf dieser Registerkarte die Nach-unten-Taste, um **SATA SM: InnoDisk** auszuwählen**. - InnoLite** und drücken Sie die **Eingabetaste**.

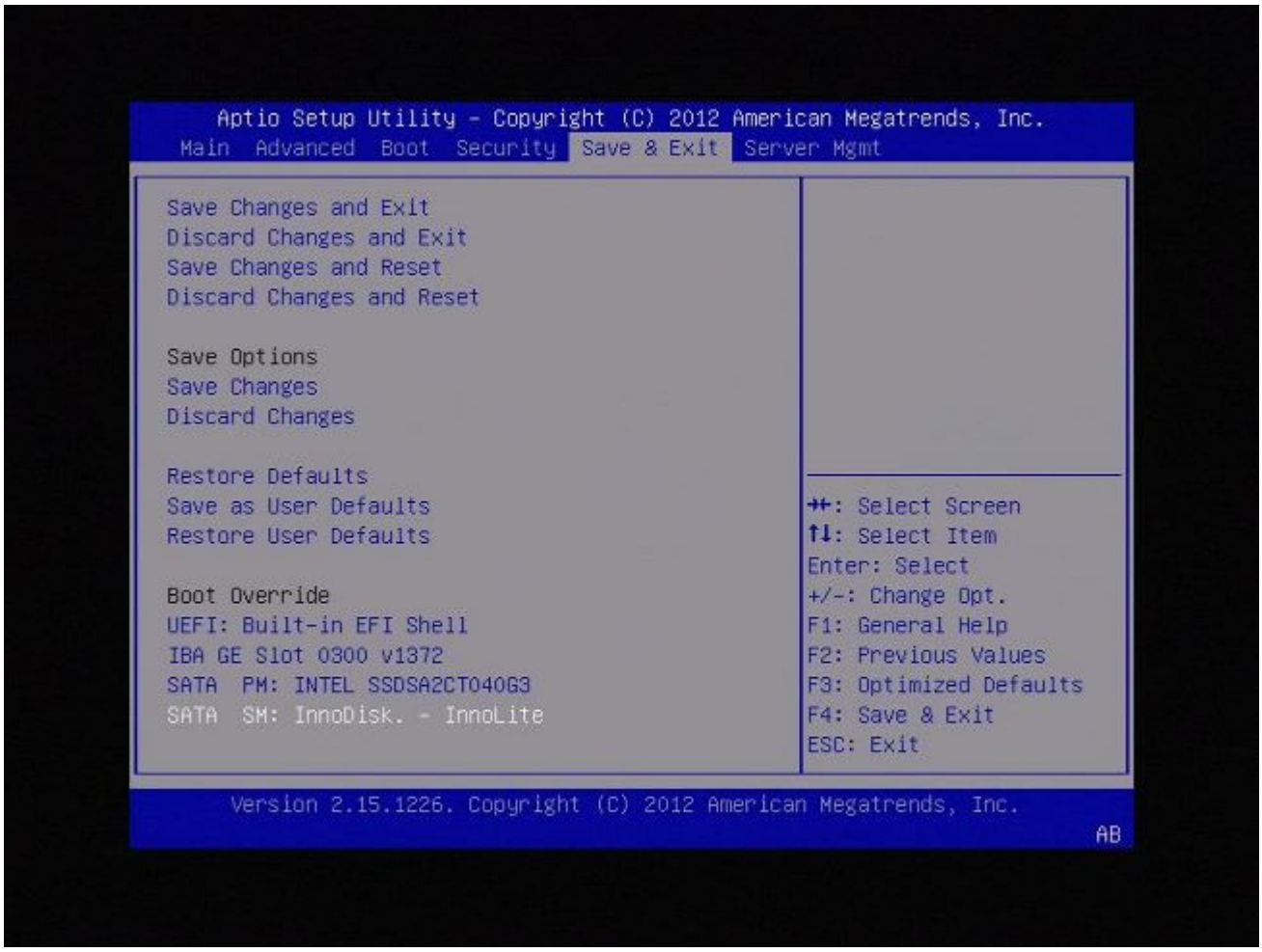


Abbildung A3

4. Wählen Sie Option **0**, wenn Sie eine Tastatur und einen Monitor verwenden.

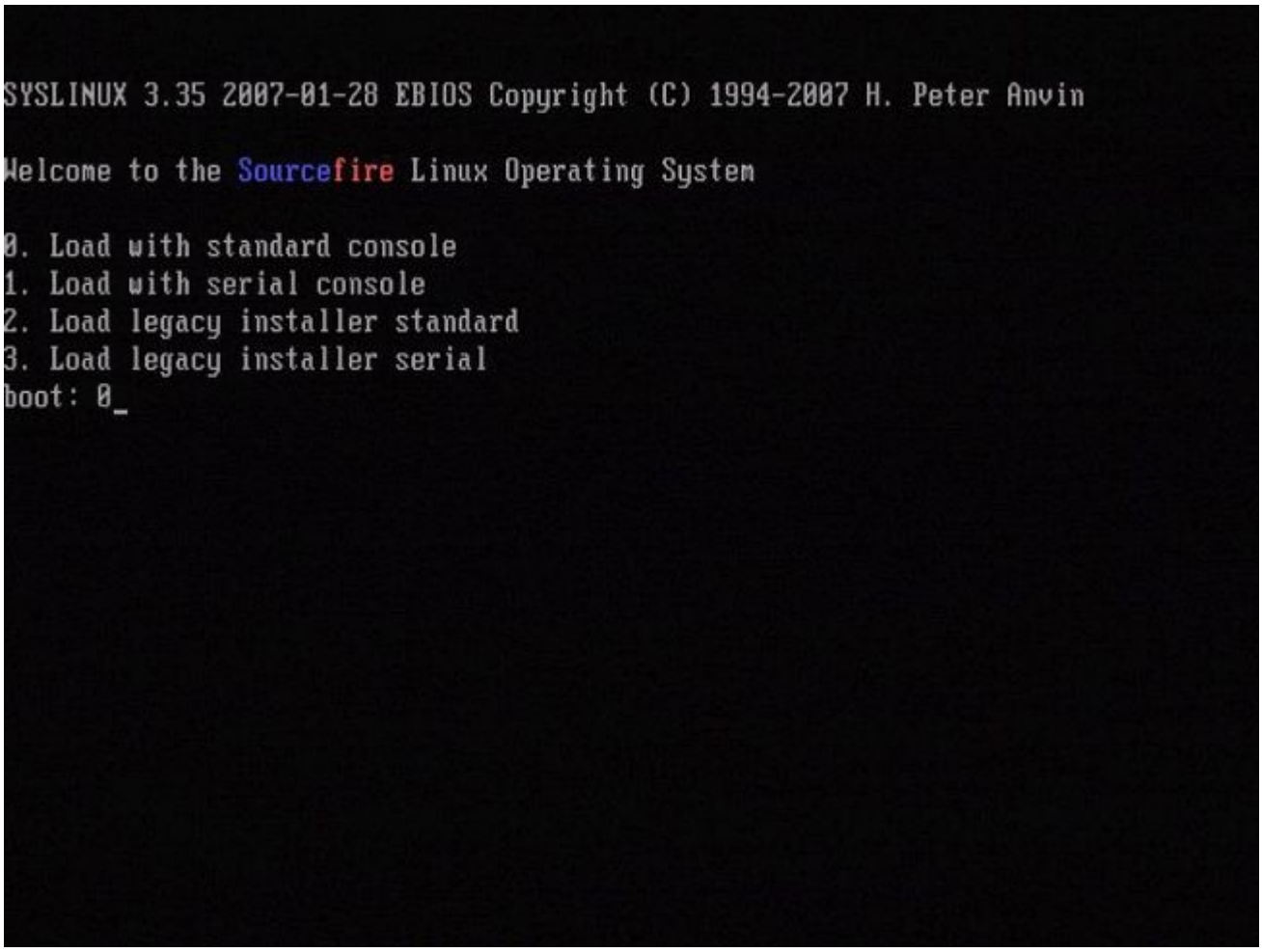


Abbildung A4

Abbildung A5

7110- und 7120-Geräte

Wenn Sie ein Gerät der 71XX-Serie verwenden, führen Sie die folgenden Schritte aus, um das Startgerät auszuwählen:

1. Schalten Sie die Einheit ordnungsgemäß aus.

2. Schalten Sie die Einheit ein, und drücken Sie wiederholt die **F11**-Taste, während die Einheit gestartet wird, um auf den Bildschirm zur Auswahl des Startgeräts zuzugreifen. Das Bild ist hier zu sehen:

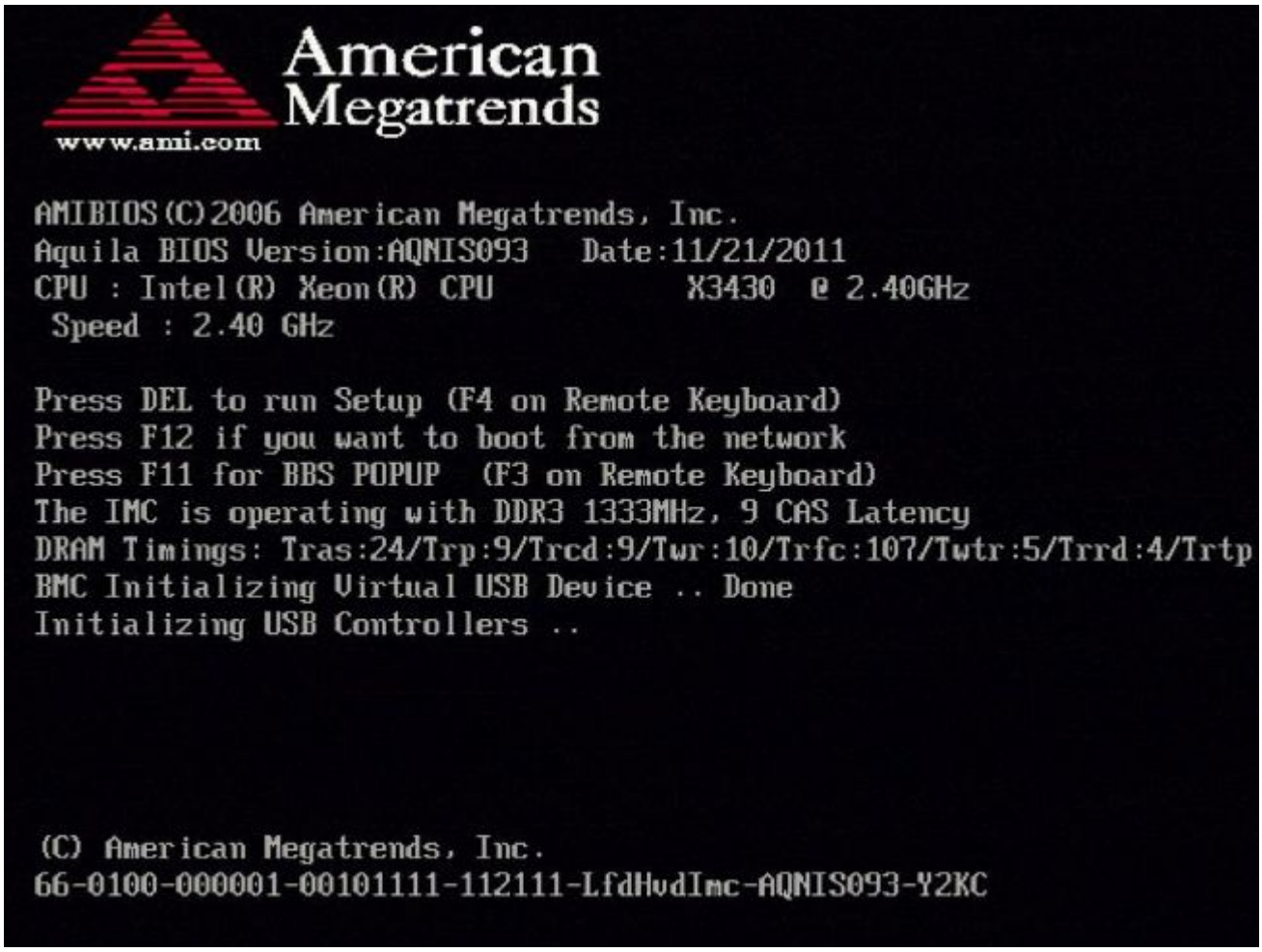


Abbildung B1

3. Wählen Sie die Option **HDD:P1-SATADOM aus**, und drücken **Sie die Eingabetaste**, um die **System_Restore**-Partition zu starten.

Abbildung B2

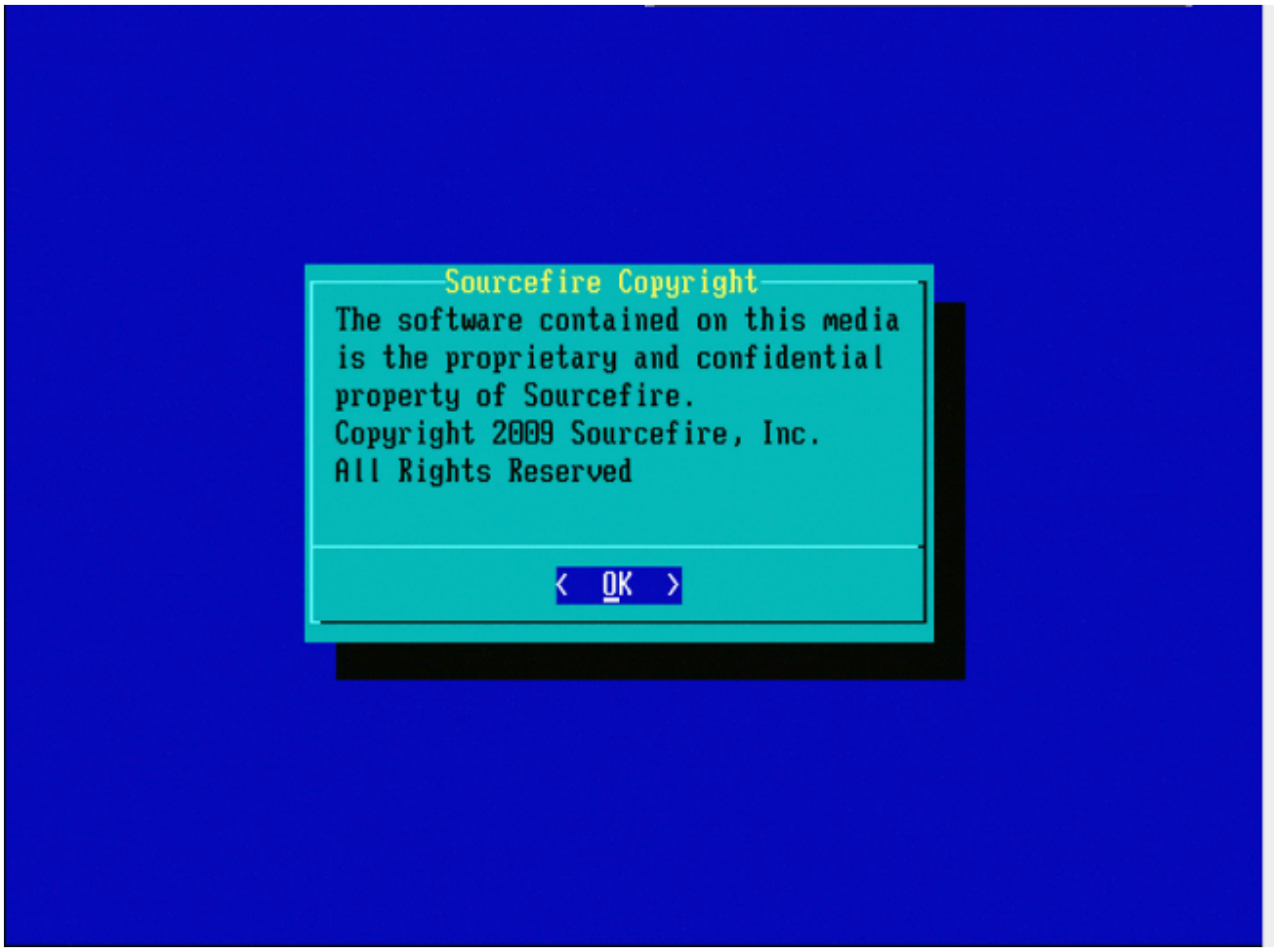


Abbildung B3

Geräte der Serie 8000 oder Management Center-Modelle FS750, FS1500 oder FS3500

Wenn Sie ein Gerät der Serie 8000 oder das Management Center-Modell FS750, FS1500 oder FS3500 verwenden, führen Sie die folgenden Schritte aus, um das Boot-Gerät auszuwählen:

1. Schalten Sie die Einheit ordnungsgemäß aus.

2. Schalten Sie die Appliance ein, und drücken Sie wiederholt die **F6**-Taste, während die Appliance hochgefahren wird, um auf den Bildschirm zur Auswahl des Startgeräts zuzugreifen. Das Bild ist hier zu sehen:

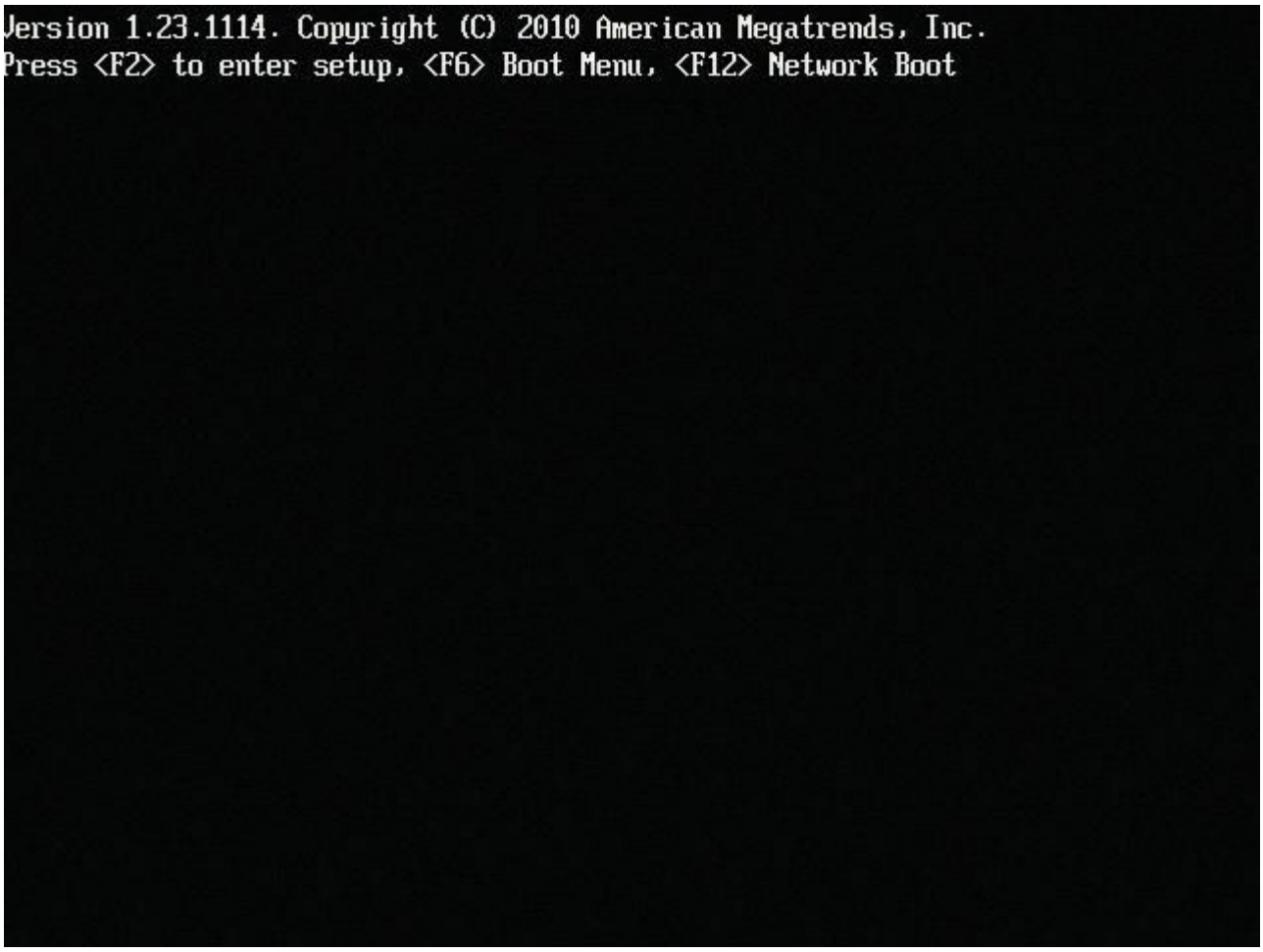


Abbildung C1

3. Wählen Sie die USB-Option aus.

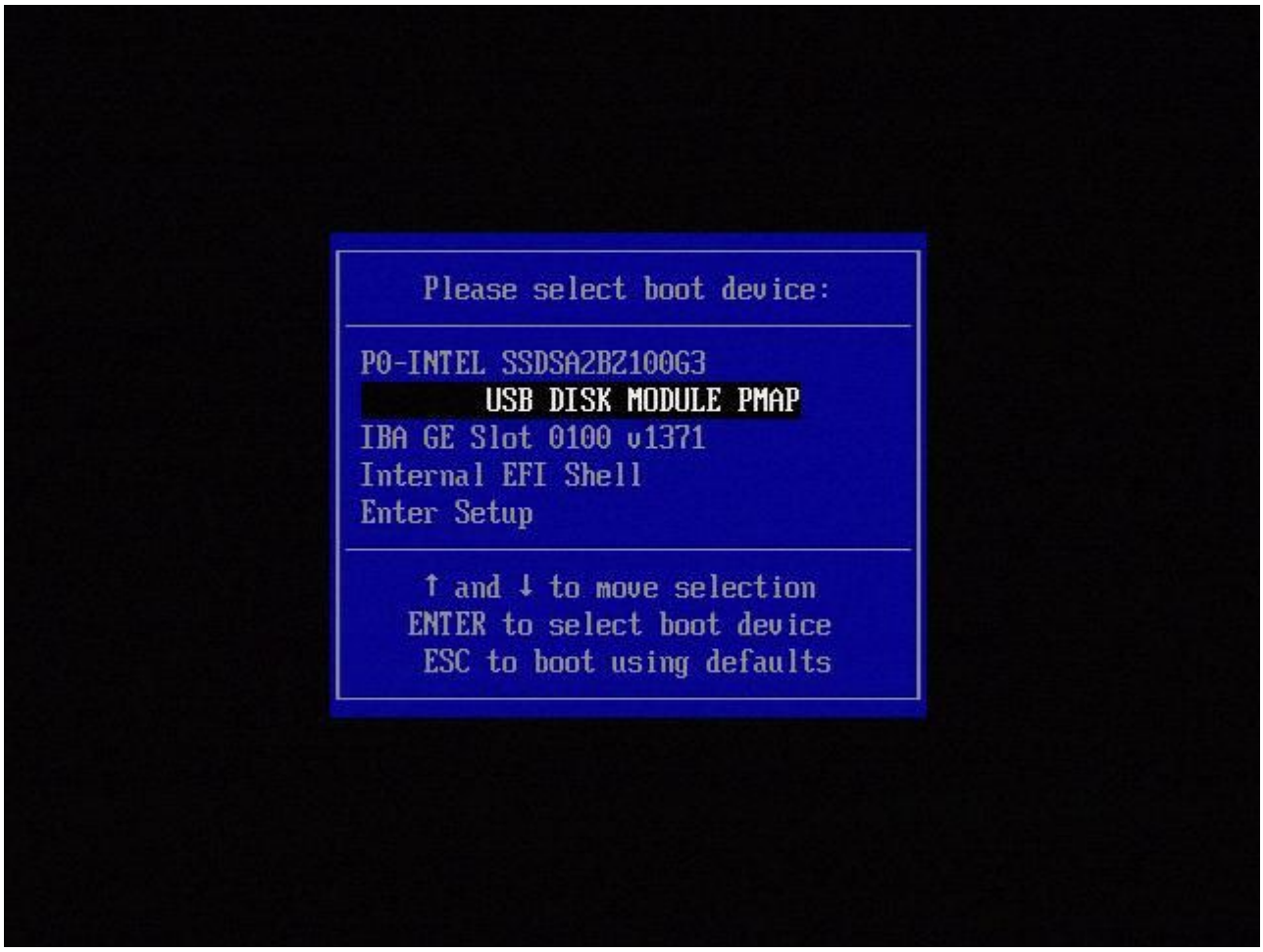


Abbildung C2

4. Die Appliance startet von der System_Restore-Partition und zeigt das Menü **System_Restore** an.

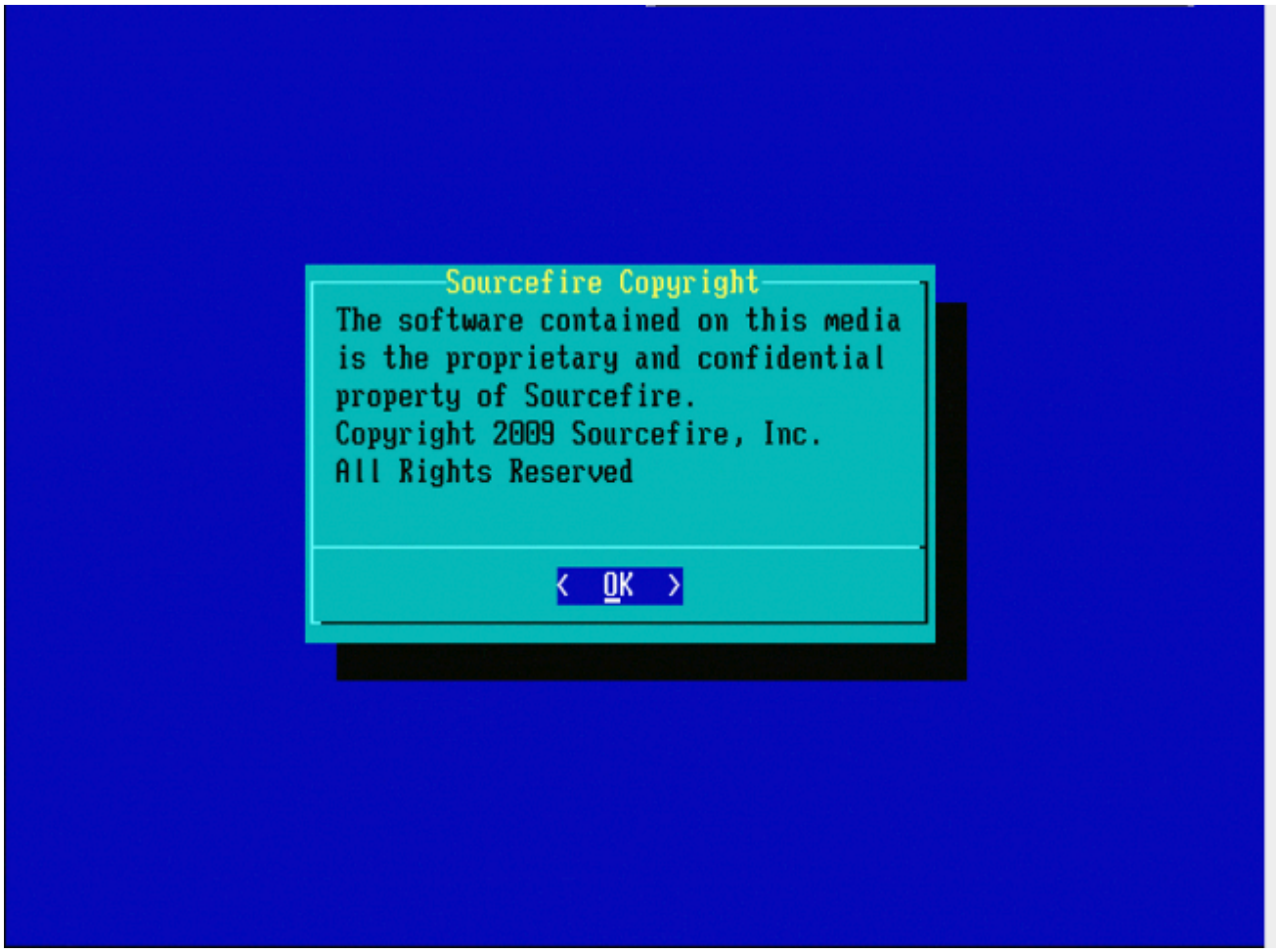


Abbildung C3

Systemwiederherstellung für die Modelle FMC1000, FMC2500, FMC4500 (M4-basierte FMCs)

> **Hinweis**: Für FMC4500 hat dieses Modell ein anderes Boot-Menü, weitere Details finden Sie im nächsten Link

---

Die Aufforderung zur Auswahl der Systemwiederherstellung sieht bei diesen Modellen anders aus: FMC1000, FMC2500, FMC4500

1. Während des Bootvorgangs wird dieser Bildschirm 5 Sekunden lang angezeigt:

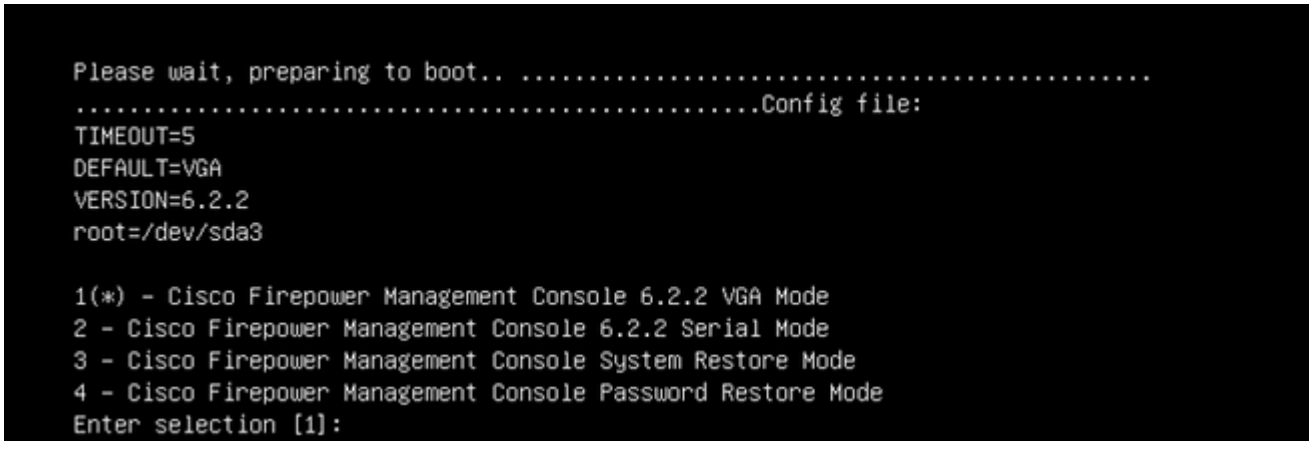


Abbildung D1

2. Wählen Sie die Option Systemwiederherstellung (in diesem Fall #3) aus.

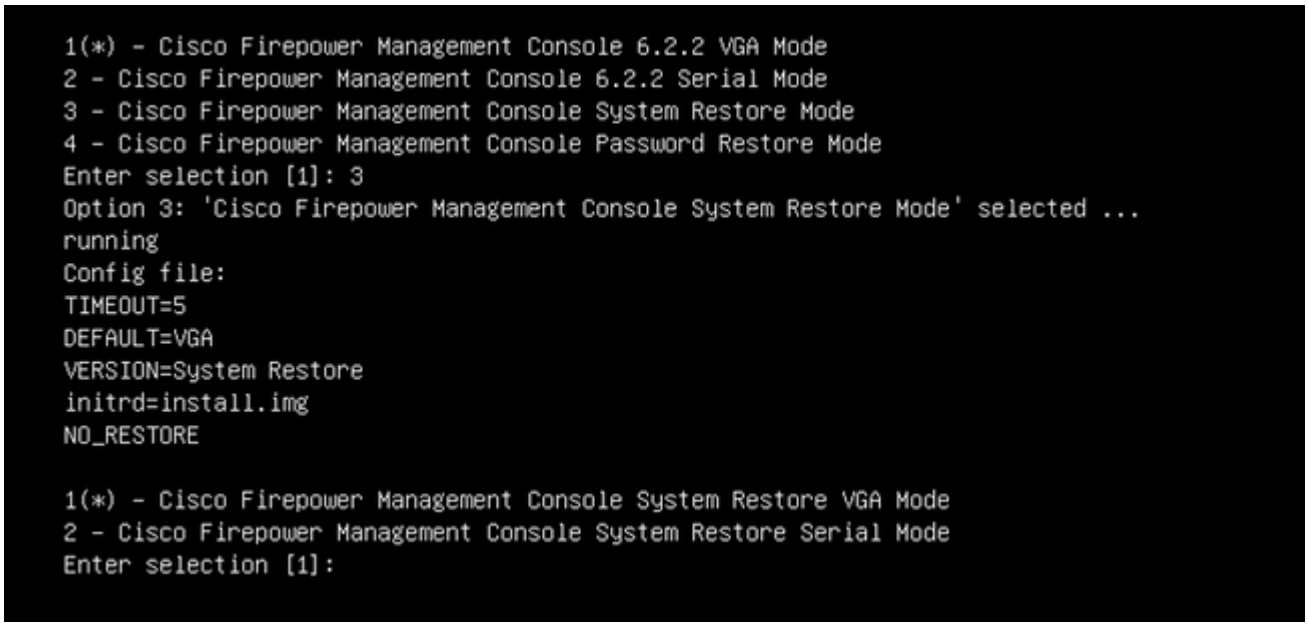


Abbildung D2

3. Wählen Sie die Anzeigemethode für die Systemwiederherstellung aus (in diesem Fall #1 für VGA).

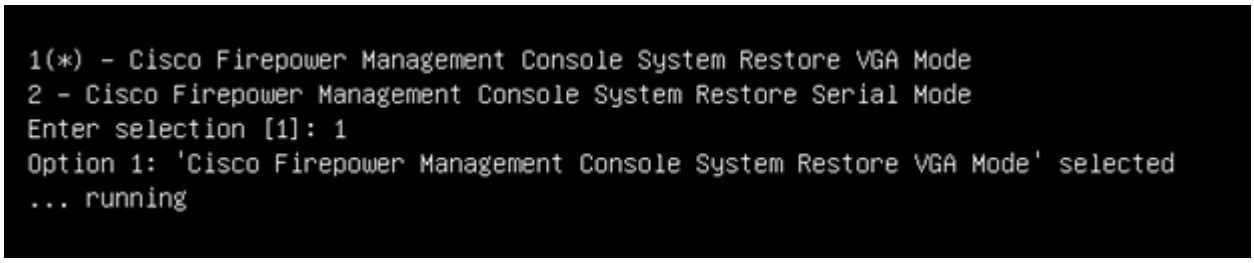


Abbildung D3

4. Anschließend gelangen Sie zur Eingabeaufforderung in Abbildung 5, und der Vorgang wird wie gewohnt fortgesetzt.

Boot-Option nicht aufgeführt

Es ist möglich, dass die Option zum Booten auf die Reimage-Partition nicht im BIOS oder im Boot-Menü aufgeführt ist. Wenn dies der Fall ist, fehlt möglicherweise das Laufwerk, das das Reimage-System enthält, oder es ist beschädigt. Wahrscheinlich ist eine RMA erforderlich.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.