

Réinstaller une appliance FireSIGHT Management Center et FirePOWER

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Processus de réimage](#)

[Avant de commencer](#)

[Présentation du processus de réinstallation](#)

[Cisco Firepower Management Center 1000, 2500 et 4500](#)

[Dépannage](#)

[Option de menu LILO System Restore non répertoriée](#)

[Périphériques 7010, 7020 et 7030](#)

[Périphériques 7110 et 7120](#)

[Périphériques de la gamme 8000 ou modèles Management Center FS750, FS1500 ou FS3500](#)

[Restauration du système pour les modèles FMC1000, FMC2500 et FMC4500 \(FMC M4\)](#)

[Option de démarrage non répertoriée](#)

Introduction

Ce document décrit les processus avec des exemples pour la procédure de réinstallation d'une appliance Cisco FireSIGHT Management Center (FMC) et FirePOWER.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

Périphérique géré	Centre de gestion FireSIGHT	Versions logicielles disponibles pour la réinstallation
-------------------	-----------------------------	---

Cisco Firepower, série 7000 Cisco Firepower, série 7100 Cisco Firepower, série 8100 Cisco Firepower, série 8200	FS 750 FS 1500 FS 3500	5.2 ou ultérieure
Gamme Firepower 8300 Cisco AMP 7150 Cisco AMP 8150		5.3 ou ultérieure

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Processus de réimage

Attention : n'insérez pas de périphérique de stockage USB et ne branchez pas de commutateur KVM (clavier, vidéo et souris) lorsque vous mettez à niveau ou réinstallez une appliance FireSIGHT Management Center ou FirePOWER.

Avant de commencer

1. Si vous prévoyez de réinstaller un périphérique Management Center ou Firepower autonome, il est recommandé de sauvegarder votre appliance avant de continuer.
2. Identifiez le modèle de votre capteur et utilisez la liste des modèles dans la section Composants utilisés afin de vérifier que ce guide est approprié.
3. Téléchargez le guide d'installation approprié et l'image du disque correspondant à la version de logiciel souhaitée sur le site d'assistance Cisco.

Remarque : ne renommez pas un fichier .iso

Servir l'image : le fichier .iso doit être copié sur un hôte qui exécute un serveur SSH accessible depuis le réseau de gestion de l'appliance à réimager.

Remarque : si aucun autre serveur SSH n'est disponible, un FMC peut être utilisé pour ce processus.

Vérification de l'intégrité de l'iso : la somme md5sum des fichiers est fournie sur le côté droit de la page pour vérification avec un utilitaire md5sum.

4. Les guides d'installation contiennent des instructions de réinstallation pas à pas et décrivent également plusieurs méthodes de réinstallation. Les images fournies dans ce document peuvent être utilisées à titre de référence.

Présentation du processus de réinstallation

Remarque : la version 5.3 a été utilisée pour capturer les images présentées dans cet article. Le processus de réinstallation est identique pour les autres versions 5.x, à l'exception des numéros de version qui apparaissent dans les images affichées.

```
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: _
```

Figure 1



Figure 2 : lorsque le système redémarre, appuyez sur une touche fléchée du clavier pour interrompre le compte à rebours et choisir l'option System_Restore pour l'écran suivant.

Remarque : si l'invite System_Restore ne s'affiche pas, vous devez modifier l'ordre de démarrage pour démarrer directement sur la partition de restauration (DOM). Pour plus d'informations, consultez [L'option de menu System_Restore LILO est manquante](#).



Figure 3

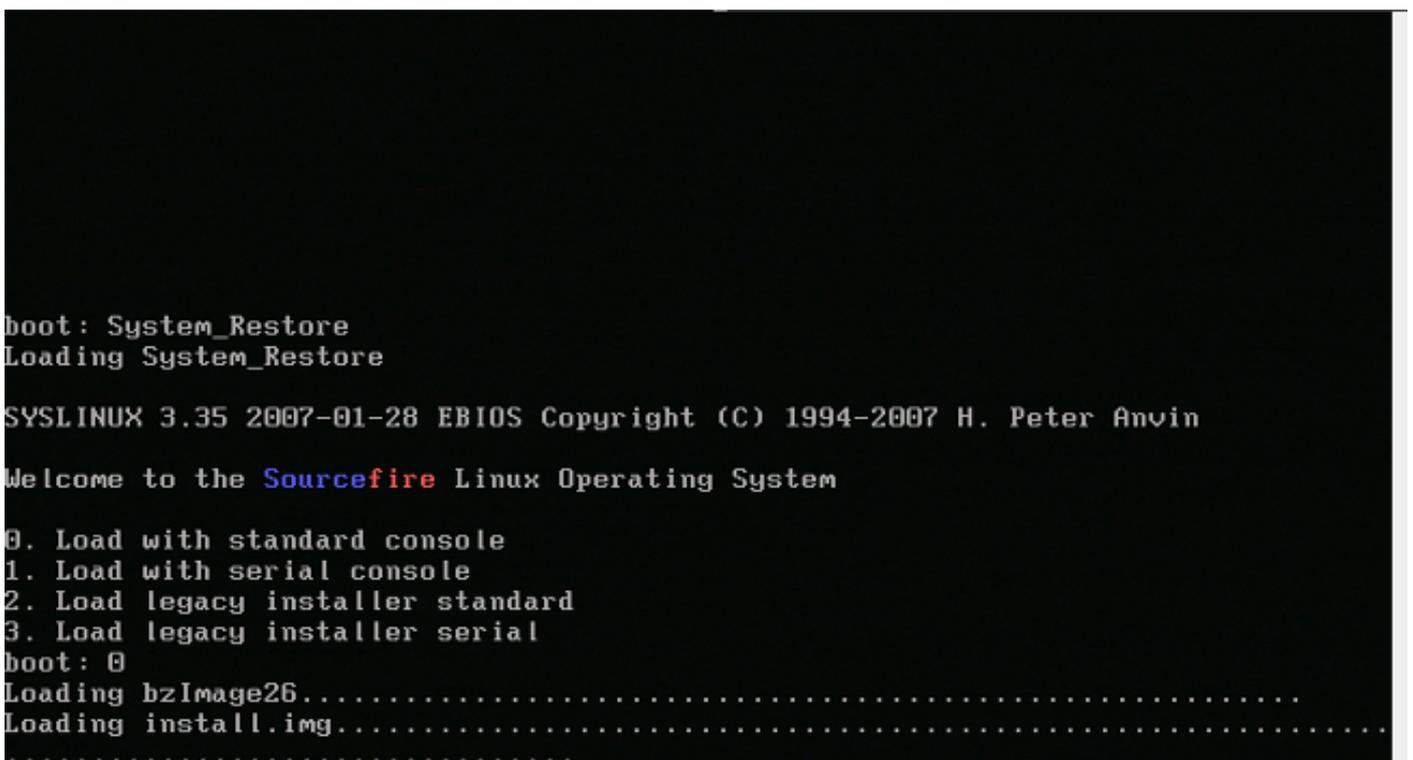


Figure 4 : sélectionnez l'option 0 si vous utilisez un clavier et un moniteur.

Remarque : il est parfois apparu que le menu de l'option Restaurer n'est affiché que lorsque seule la console est connectée (le clavier étant débranché). Dès que l'option Récupération est sélectionnée, le clavier peut être reconnecté

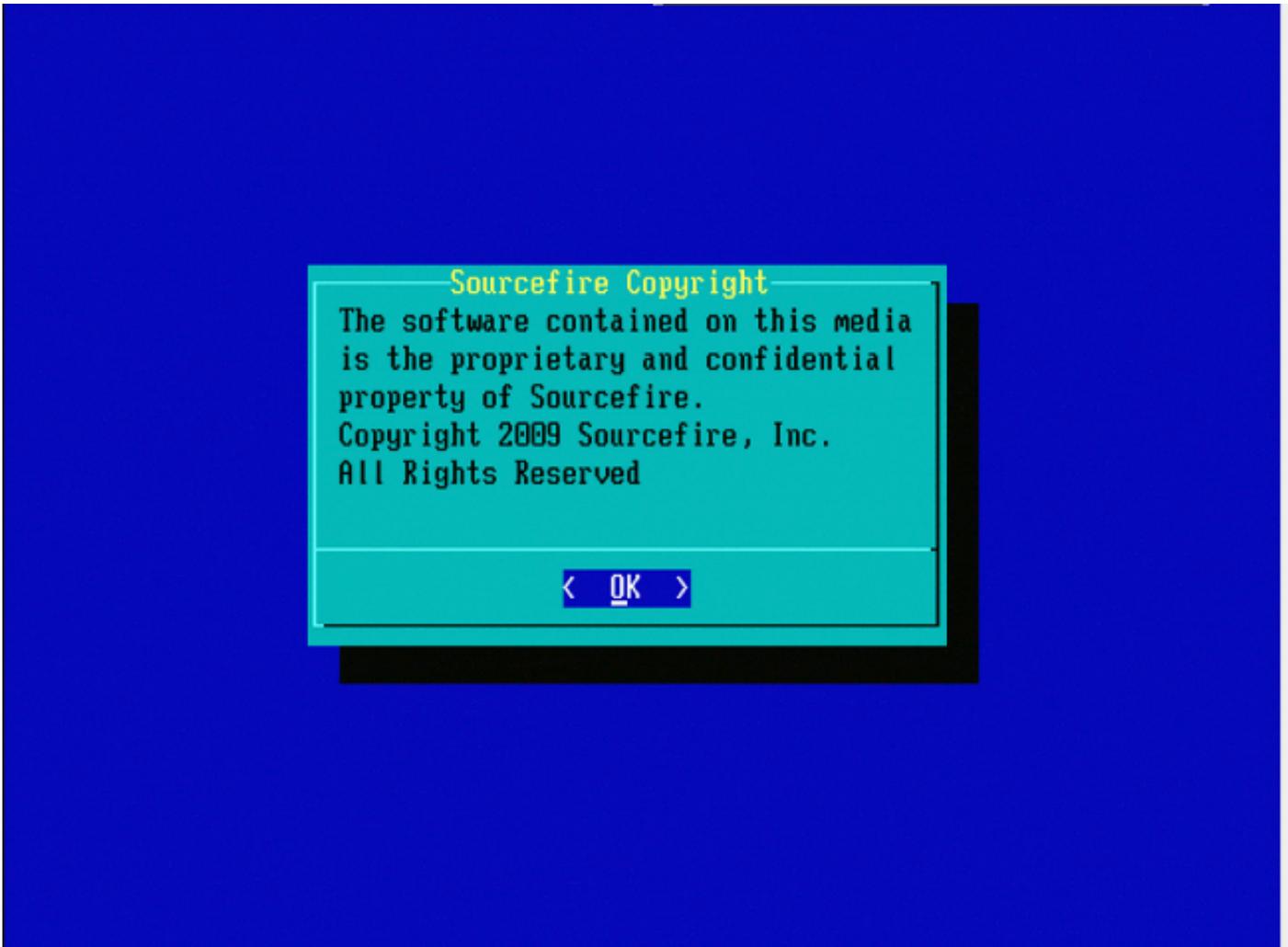


Figure 5

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>

Figure 6

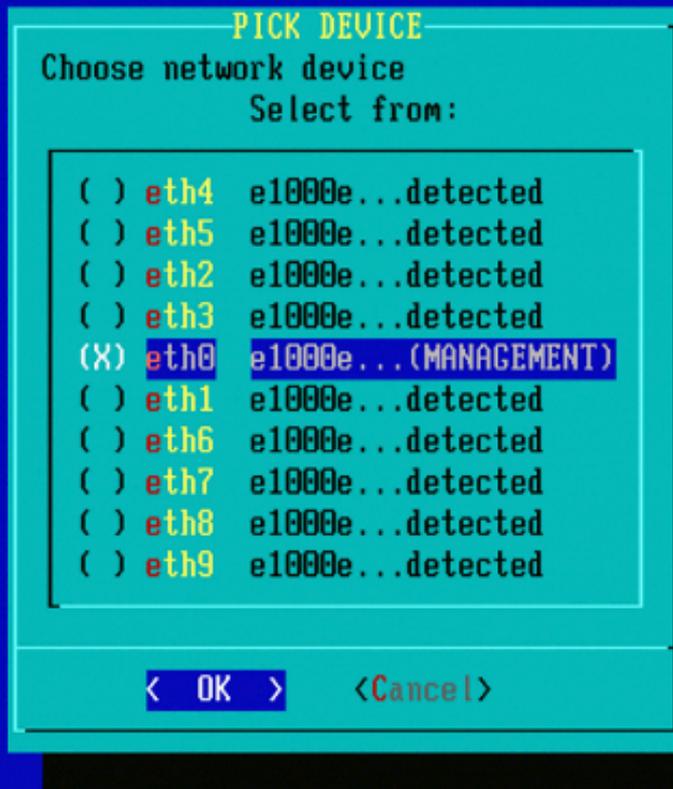


Figure 7 : pour sélectionner le périphérique réseau, appuyez sur la barre d'espace.

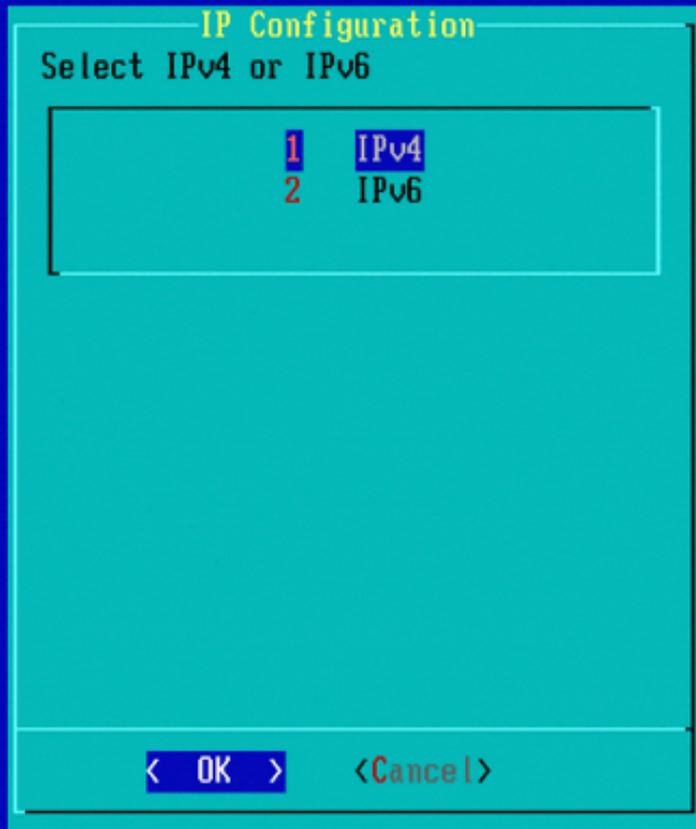


Figure 8



Figure 9

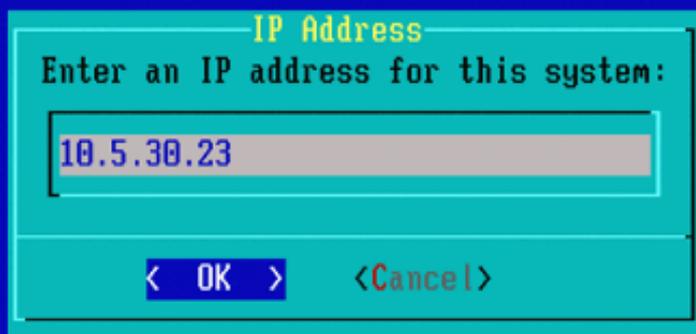


Figure 10

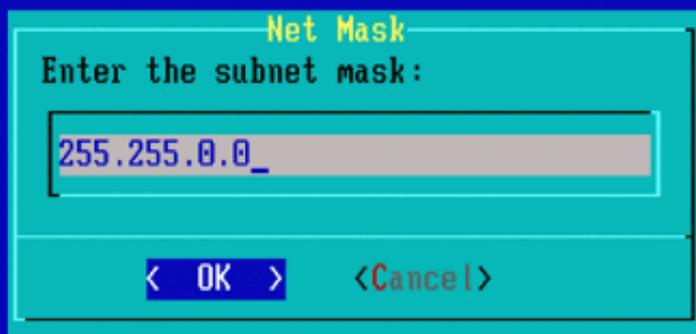


Figure 11

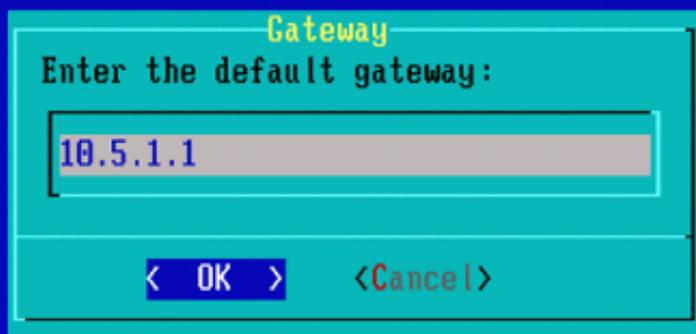


Figure 12



Figure 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>

Figure 14



Figure 15 - L'assistance Cisco vous recommande d'utiliser le protocole Secure Copy (SCP).

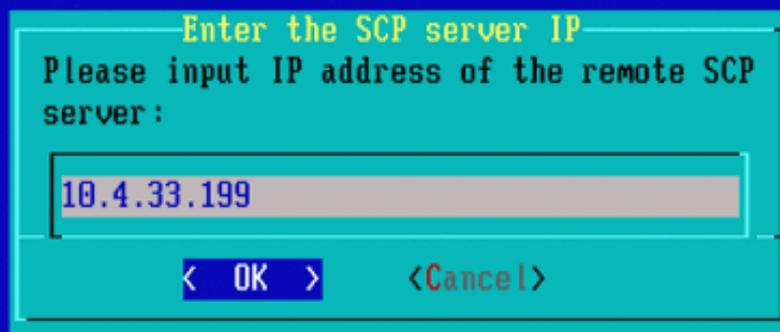


Figure 16 : il est possible d'utiliser FireSIGHT Management Center comme serveur SCP pour cette étape. Poursuivez cette procédure et utilisez l'adresse IP et les informations d'identification pour Management Center afin de remplir les champs du menu Restauration du système. Plus de détails dans

Un serveur de copie sécurisée (SCP) est utilisé pour transférer des fichiers en toute sécurité. Si nécessaire, un centre de défense Sourcefire (DC) peut être utilisé comme serveur SCP pour transférer des fichiers vers un autre périphérique Sourcefire. Cela peut être utile lorsqu'une image ISO doit être transférée vers un périphérique Sourcefire à des fins de réinstallation, mais que le serveur SCP normal est inaccessible ou indisponible.

Étape 1. Téléchargez un fichier .iso approprié sur votre bureau à partir du [portail d'assistance Sourcefire](#).

Étape 2. Utilisez un client SCP, copiez le fichier du bureau vers le Centre de défense.

Conseil : un client SCP est généralement disponible dans un système d'exploitation Linux ou Mac. Cependant, dans le système d'exploitation Windows, vous pouvez avoir à installer un logiciel client SCP tiers. Sourcefire ne fournit aucune recommandation ni assistance pour l'installation d'un logiciel client SCP spécifique.

L'exemple suivant montre comment copier un fichier image Sourcefire .iso du répertoire

Downloads d'un système Linux vers le répertoire /var/tmp du Centre de défense Sourcefire :

```
<#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
```

Attention : ne modifiez pas le nom du fichier .iso. Il peut créer un problème avec la détection du fichier lors d'une réinstallation.

À présent, le fichier est copié vers le Centre de défense. Vous pouvez poursuivre le processus de réinstallation des périphériques Sourcefire. Lors de la réinstallation, si nécessaire, vous pouvez fournir l'adresse IP et le nom d'utilisateur du contrôleur de domaine, ainsi que le chemin d'accès où vous avez copié le fichier image avec les instructions précédentes.

Avertissement : une fois la réinstallation terminée, vous devez supprimer le fichier .iso du répertoire /var/tmp du Centre de défense pour réduire l'utilisation de l'espace disque.

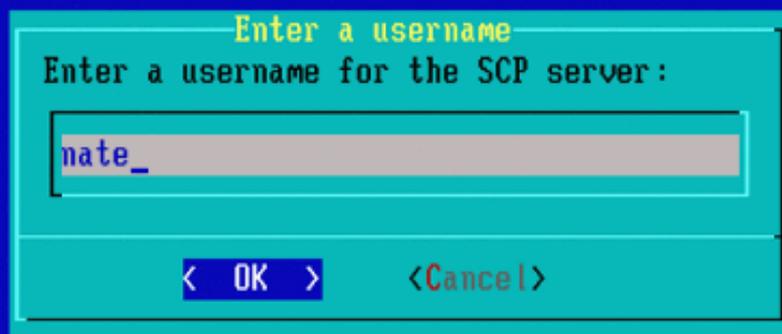


Figure 17

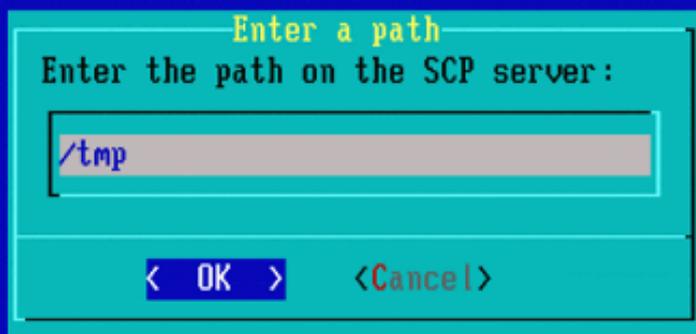
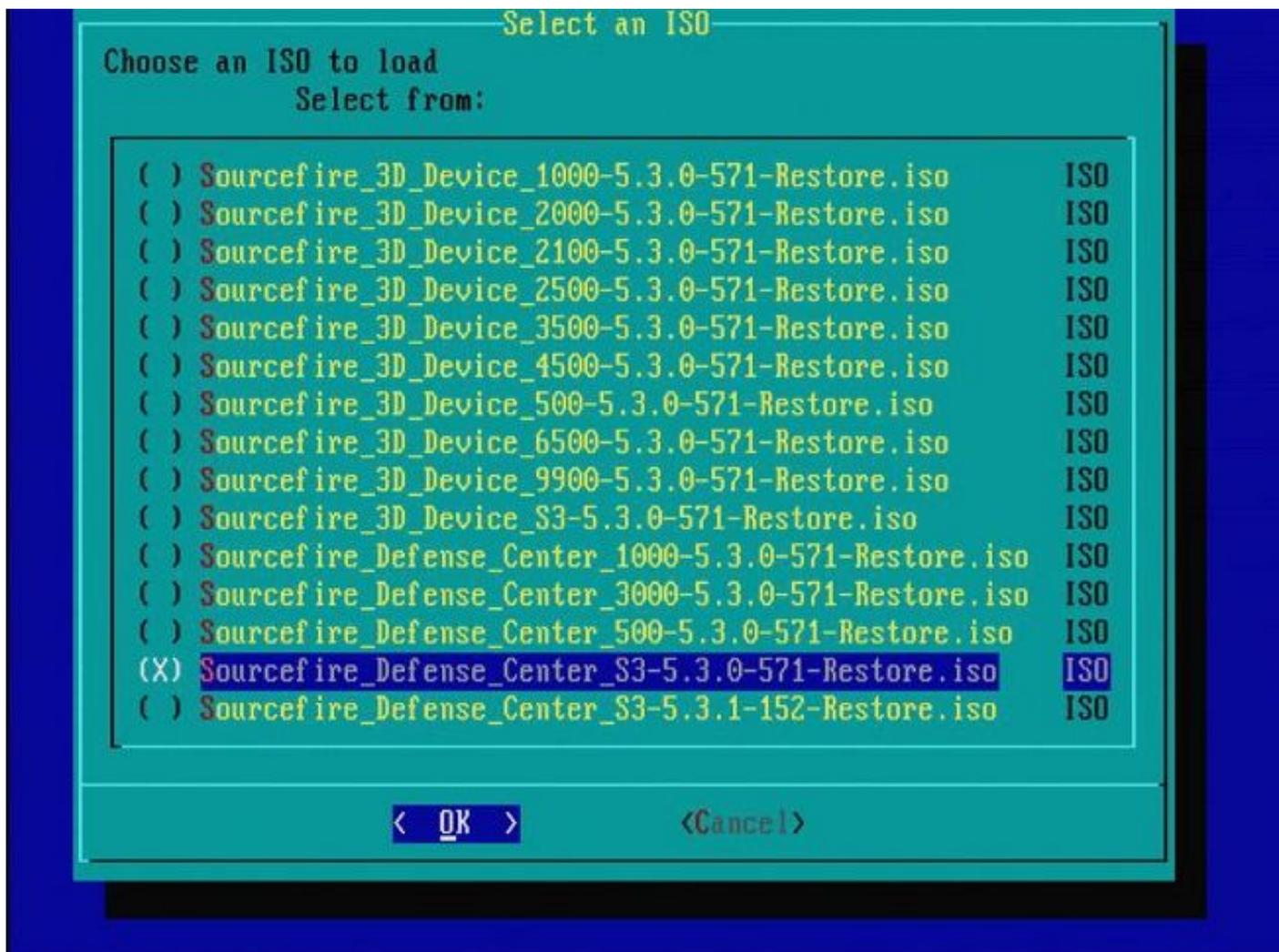


Figure 18



Figure 19

Remarque : si vous recevez une erreur de connectivité à ce stade au lieu du message attendu, vérifiez votre connexion au serveur SSH.



Remarque : il est nécessaire d'utiliser les noms de fichiers par défaut pour les fichiers .iso ou les fichiers sont peut-être non détectés à cette étape.

Erreur : Aucune image ISO n'a été trouvée

Dans la version 6.3, la convention de nom ISO est passée de Sourcefire_3D_Device_S3-
<ver>-<build>-Restore.iso à Cisco_Firepower_NGIPS_Appliance-<ver>-<build>-Restore.iso.

Si vous rencontrez "Aucune image ISO n'a été trouvée", renommez le fichier ISO avec le nom de fichier hérité. Cela se produit normalement lorsqu'une nouvelle image de la version 6.2.x ou antérieure à la version 6.3.0 ou ultérieure.

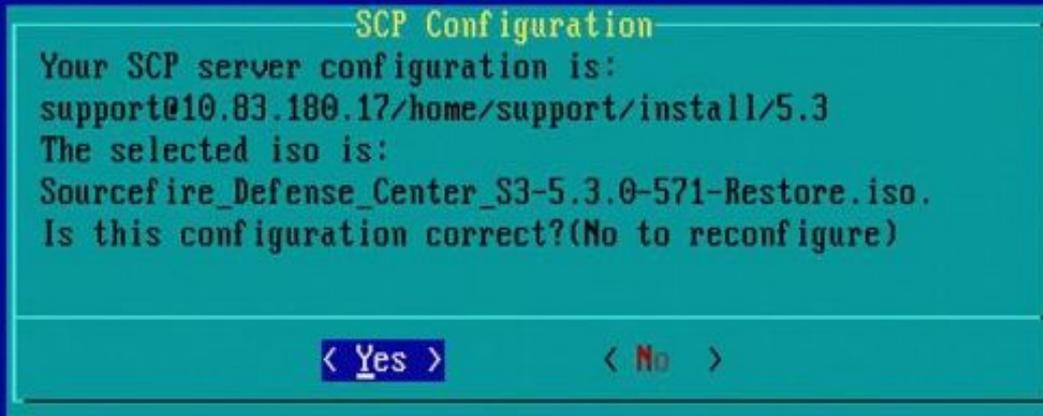


Figure 21



Figure 22 - L'assistance Cisco recommande d'ignorer l'étape 3 de ce processus. Les correctifs et les mises à jour des règles de renversement (SRU) peuvent être installés une fois la réinstallation terminée.

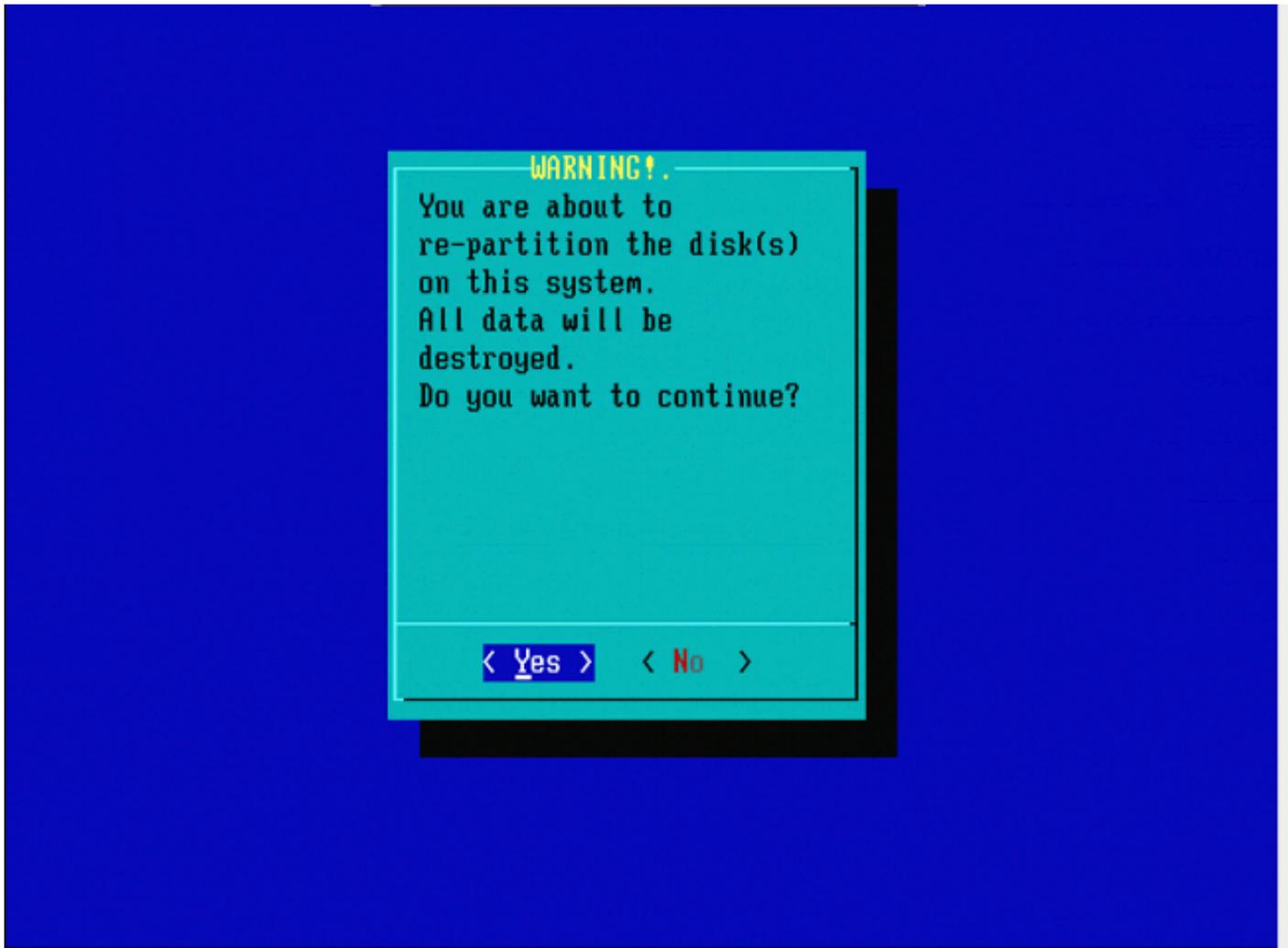


Figure 23

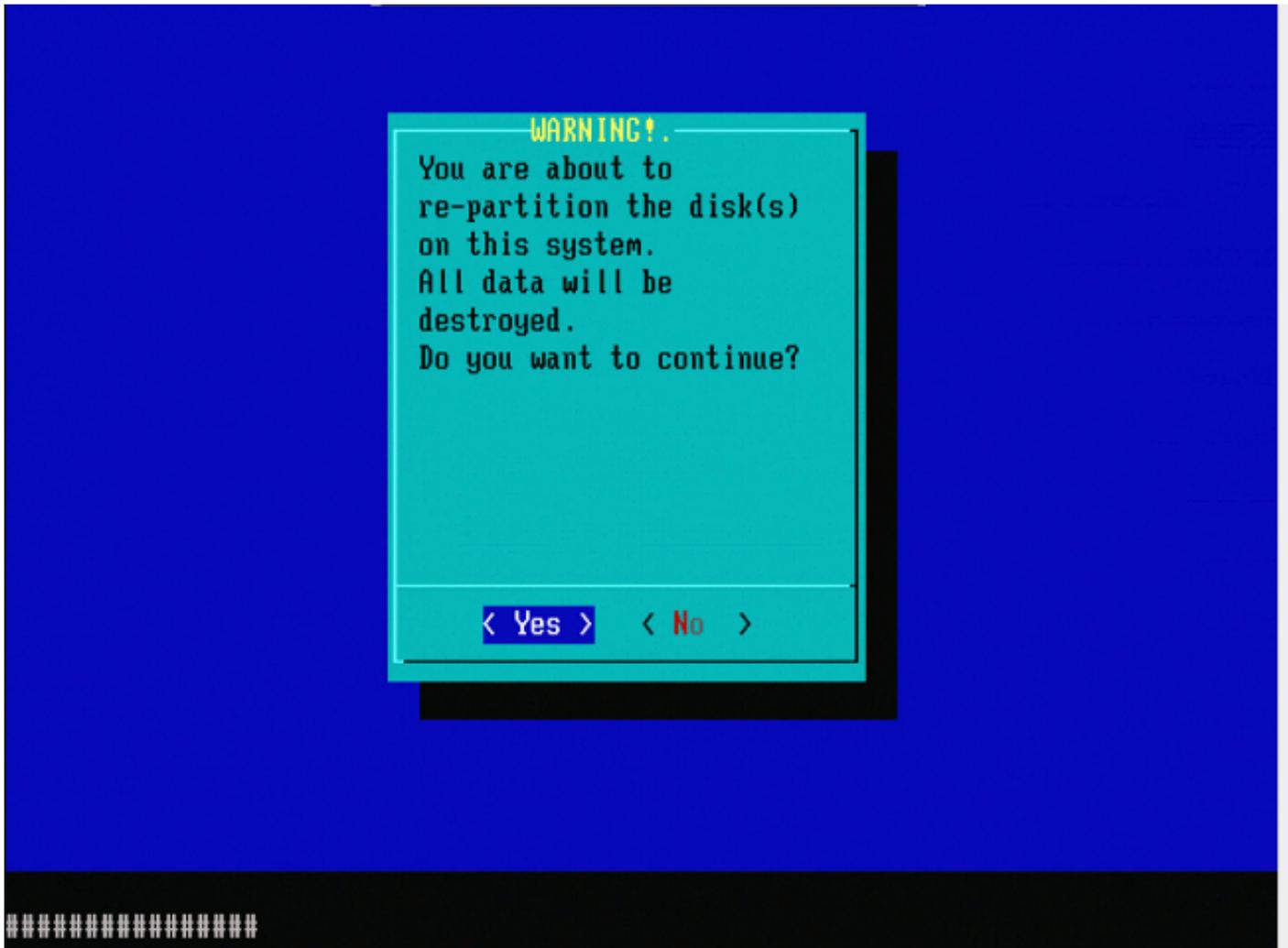


Figure 24

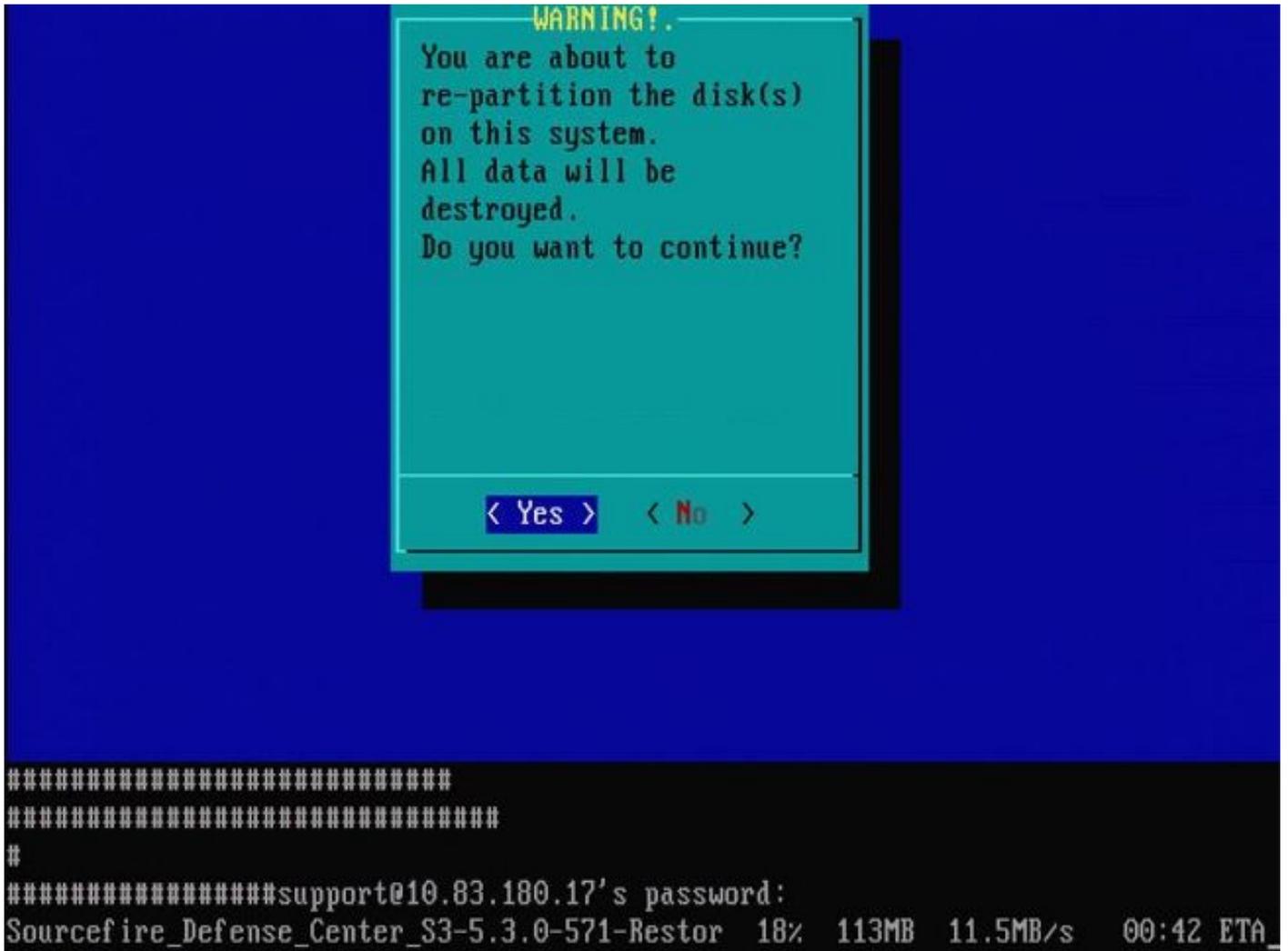


Figure 25



Figure 26

Remarque importante concernant une réinstallation à partir d'une autre version principale du logiciel : si vous tentez de réinstaller un périphérique qui exécutait précédemment une autre version principale du logiciel, par exemple si vous réinstallez 5.1 > 5.2, 5.2 > 5.3, 5.3 > 5.2, etc., vous devez effectuer les étapes décrites dans les Figures 1 à 26 deux fois.

1. Une fois que vous avez sélectionné OK à l'invite, comme illustré dans l'image 26, la partition Restauration du système est mise en mémoire flash avec la nouvelle version et l'appliance redémarre.
2. Après le redémarrage, vous devez recommencer le processus de réinstallation depuis le début et continuer le processus décrit dans les Figures 27b à 31.

S'il s'agit de la première réinstallation à partir d'une autre version principale du logiciel, l'écran s'affiche comme illustré dans l'image 27a, puis dans les figures 31 et 32.

Attention : si vous voyez cet écran, il y a un délai possible sans sortie visible après "Vérification du matériel" et avant "Le périphérique USB...". N'appuyez pas sur une touche pour le moment, sinon le périphérique redémarre et devient inutilisable et doit être réimagé une fois de plus.

Si ce n'est pas le cas, vous pouvez voir les écrans de la Figure 27b à la Figure 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.
-
```

Figure 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

Figure 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

Figure 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

Figure 29

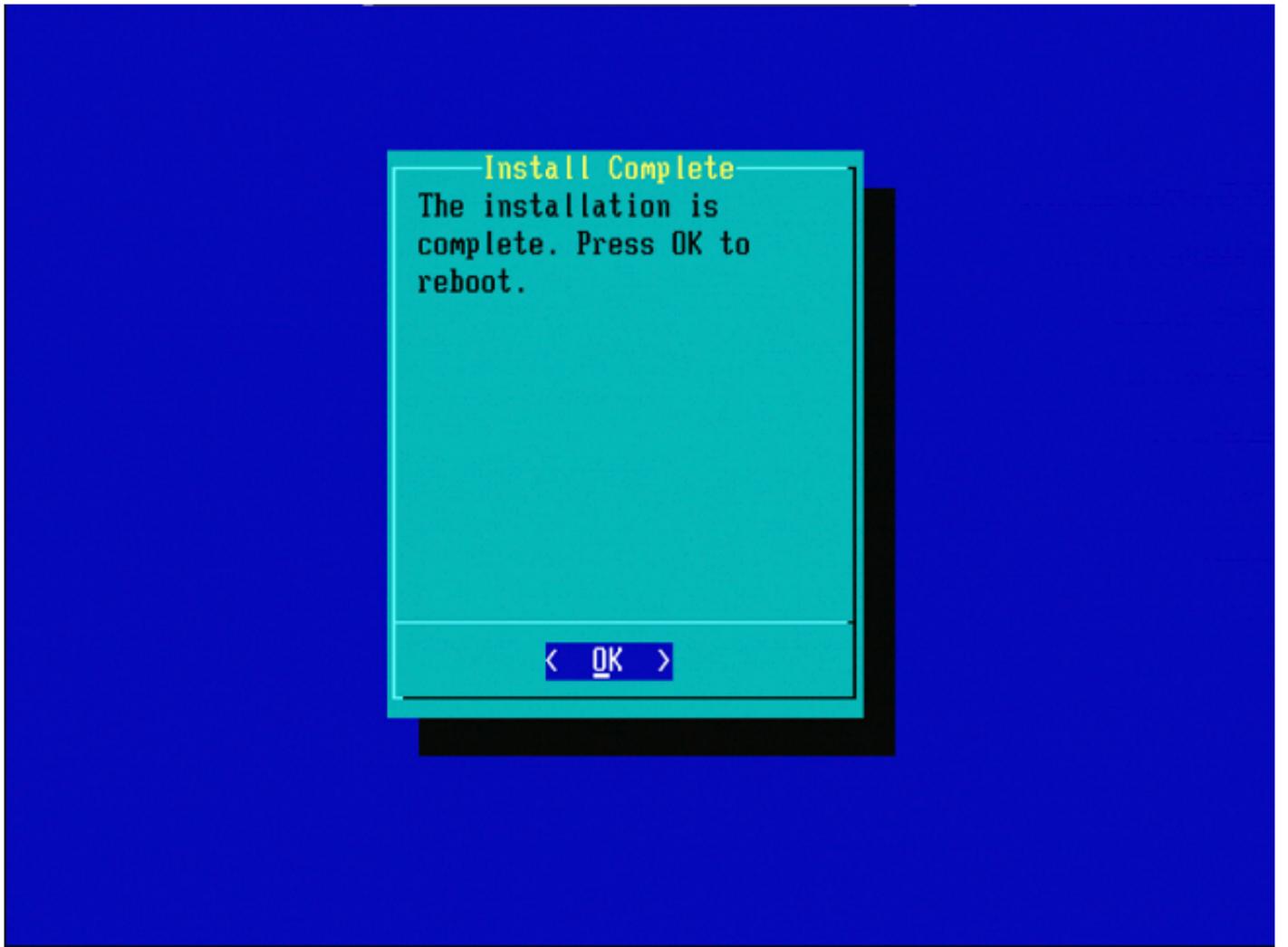


Figure 31



Figure 32

Cisco Firepower Management Center 1000, 2500 et 4500

Les options sont différentes sur les modèles FMC 1000, 2500 et 4500. Utilisez un commutateur KVM ou la console CIMC et, au démarrage du périphérique, les options suivantes s'affichent :

- 1 - Mode VGA de la console de gestion Cisco Firepower
- 2 - Console de gestion Cisco Firepower série
- 3 - Mode de restauration du système de Cisco Firepower Management Console
- 4 - Mode de restauration du mot de passe de Cisco Firepower Management Console

Si vous souhaitez passer en mode de restauration avec interface utilisateur, sélectionnez l'option « Mode de restauration du système de la console de gestion Cisco Firepower » (option 3), puis « Mode VGA de restauration du système de la console de gestion Cisco Firepower » (option 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.
```

Figure 33

Le reste du processus est identique à celui des autres appliances FMC.

Dépannage

Option de menu LILO System_Restore non répertoriée

Les appliances FireSIGHT Management Center et FirePOWER 7000 et 8000 sont dotées d'un lecteur flash intégré qui contient le système de réinstallation. Si l'option "System_Restore" n'est pas répertoriée dans le menu de démarrage de LILO (Linux Loader), il est toujours possible d'accéder à ce lecteur afin de terminer la réinstallation.

Périphériques 7010, 7020 et 7030

Si vous utilisez un périphérique de la gamme 70XX, procédez comme suit afin de sélectionner le périphérique de démarrage :

1. Mettez le périphérique hors tension.
2. Mettez l'apppliance sous tension et appuyez plusieurs fois sur la touche Delete pendant le démarrage de l'apppliance afin d'accéder à l'écran de sélection du périphérique de démarrage. Voir l'image ici :



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

Figure A1

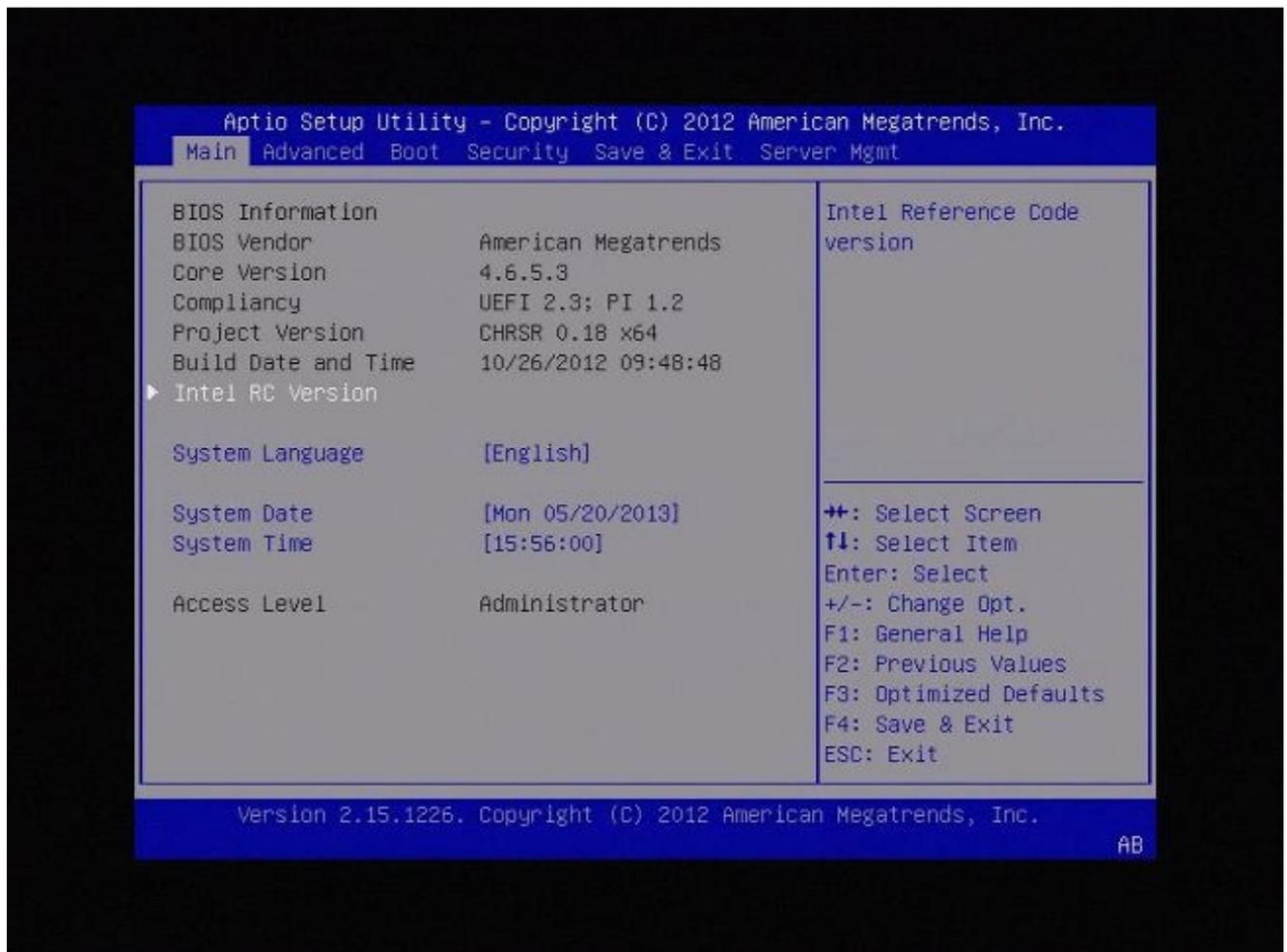


Figure A2

3. Utilisez la flèche droite pour sélectionner l'onglet Enregistrer et quitter. Dans cet onglet, utilisez la flèche vers le bas afin de sélectionner SATA SM : InnoDisk. - InnoLite et appuyez sur la touche Entrée.



Figure A3

4. Choisissez l'option 0 si vous utilisez un clavier et un moniteur.

```
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_
```

Figure A4

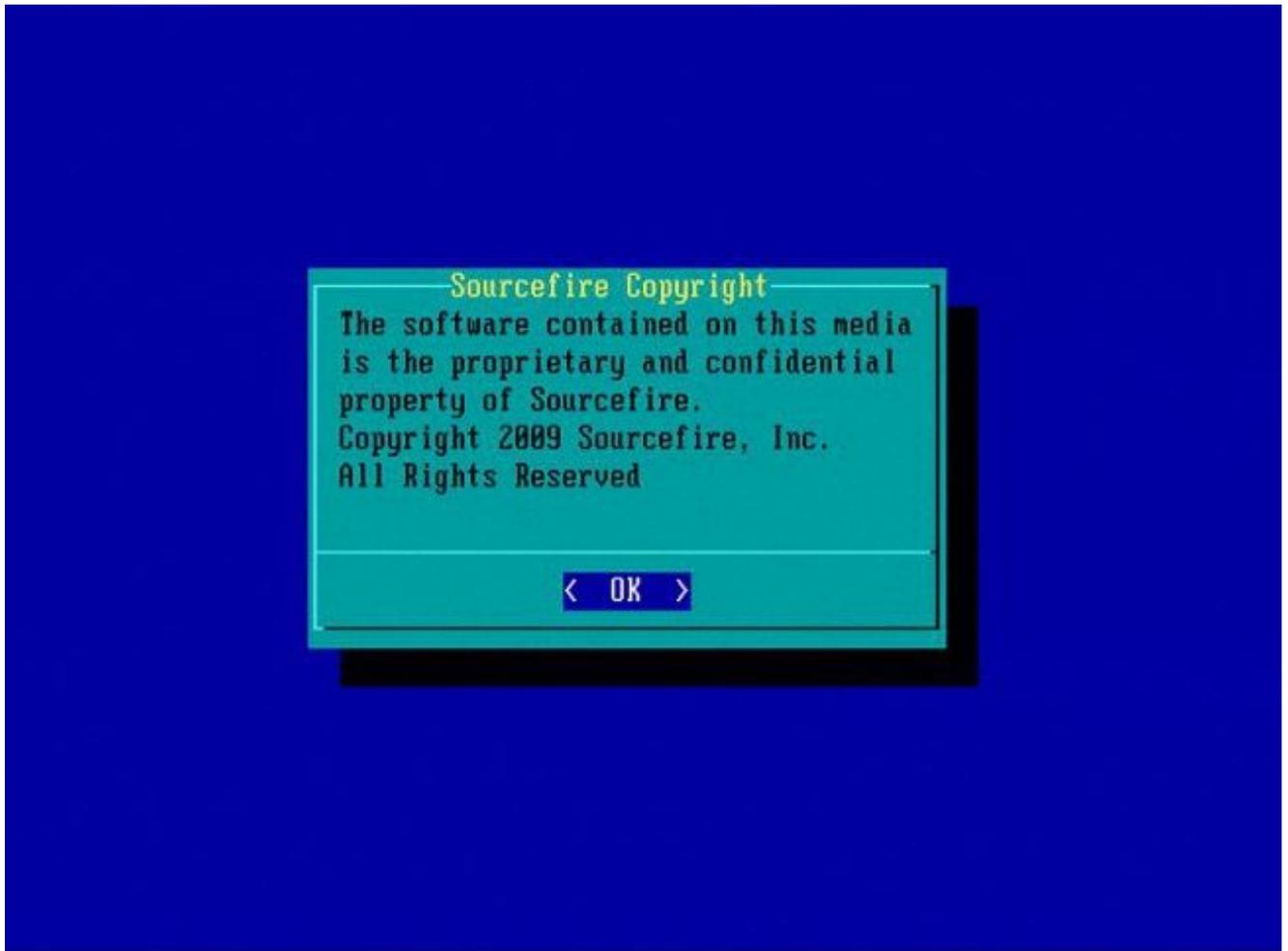


Figure A5

Périphériques 7110 et 7120

Si vous utilisez un périphérique de la gamme 71XX, procédez comme suit afin de sélectionner le périphérique de démarrage :

1. Mettez le périphérique hors tension.
2. Mettez le périphérique sous tension et appuyez plusieurs fois sur la touche F11 pendant le démarrage du périphérique afin d'accéder à l'écran de sélection du périphérique de démarrage. Reportez-vous à l'image suivante :



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

Figure B1

3. Sélectionnez l'option HDD:P1-SATADOM et appuyez sur Entrée afin de démarrer à la partition System_Restore.



Figure B2



Figure B3

Périphériques de la gamme 8000 ou modèles Management Center FS750, FS1500 ou FS3500

Si vous utilisez un périphérique de la gamme 8000 ou un modèle Management Center FS750, FS1500 ou FS3500, procédez comme suit afin de sélectionner le périphérique d'amorçage :

1. Mettez le périphérique hors tension.
2. Mettez le périphérique sous tension et appuyez plusieurs fois sur la touche F6 pendant le démarrage du périphérique afin d'accéder à l'écran de sélection du périphérique de démarrage. Reportez-vous à l'image suivante :

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

Figure C1

3. Sélectionnez l'option USB.

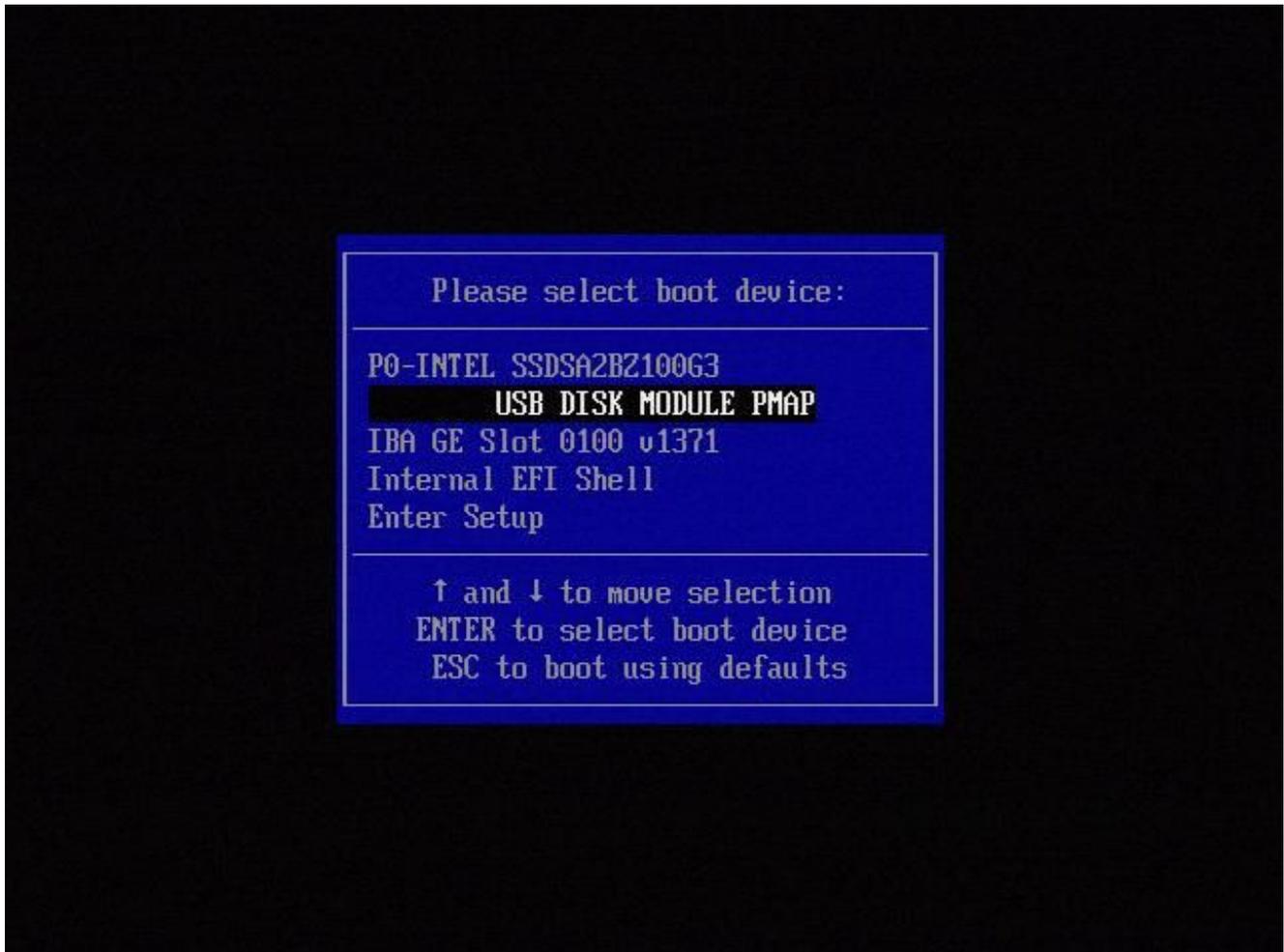


Figure C2

4. L'appliance démarre à partir de la partition System_Restore et affiche le menu System_Restore.

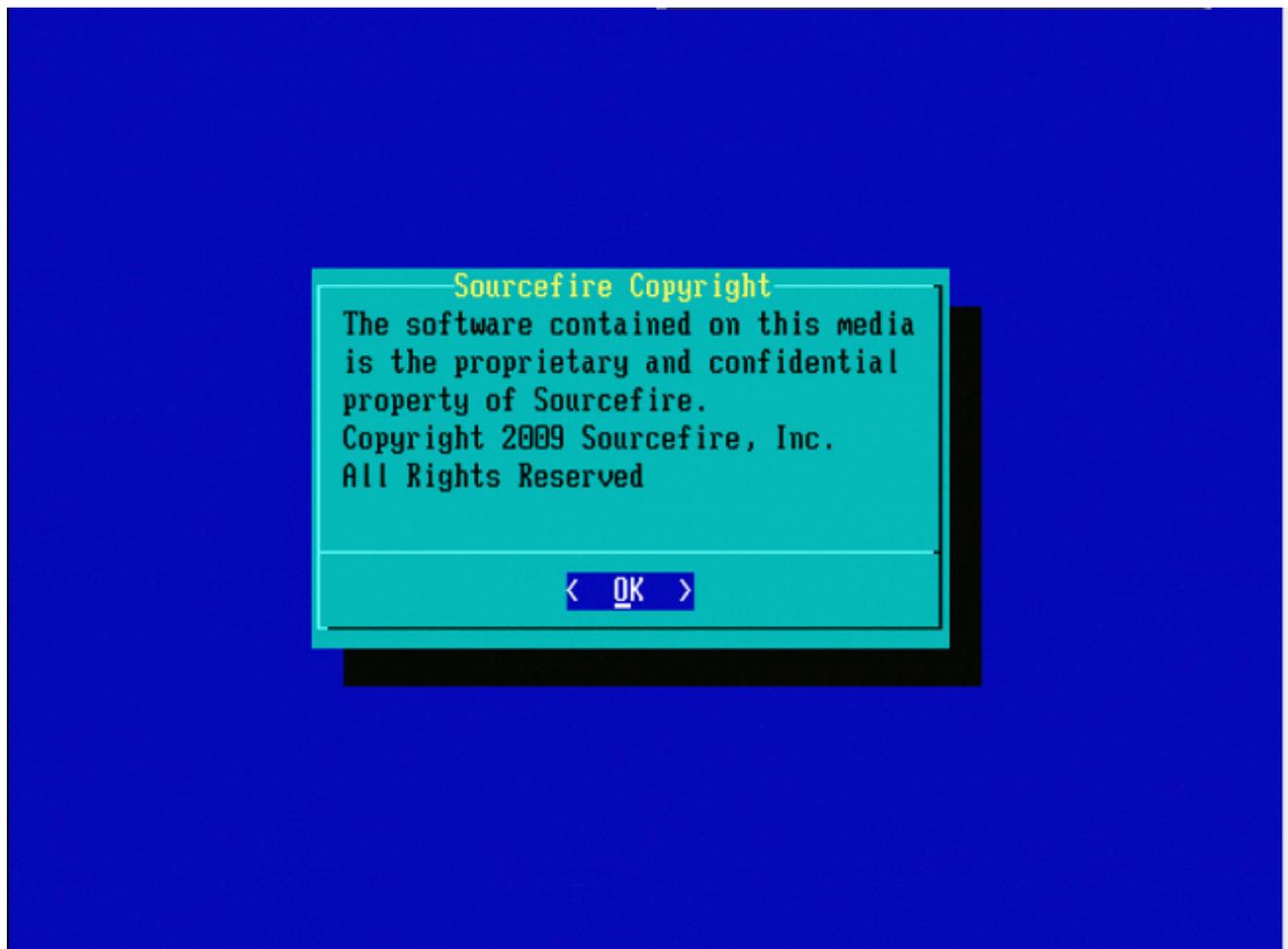


Figure C3

Restauration du système pour les modèles FMC1000, FMC2500 et FMC4500 (FMC M4)

Remarque : pour le FMC4500, ce modèle dispose d'un menu de démarrage différent. Pour plus d'informations, cliquez sur le [lien](#) suivant

L'invite de sélection de la restauration du système apparaît différemment pour les modèles suivants : FMC1000, FMC2500, FMC4500

1. Pendant le démarrage, cet écran s'affiche pendant 5 secondes :

```

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]:

```

Figure D1

2. Sélectionnez l'option Restauration du système (#3 dans ce cas).

```

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]:

```

Figure D2

3. Sélectionnez la méthode d'affichage pour la restauration du système (#1 pour VGA dans ce cas)

```

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

```

Figure D3

4. Vous arrivez ensuite à l'invite de la figure 5 et le processus se poursuit normalement.

Option de démarrage non répertoriée

Il est possible que l'option permettant de démarrer à partir de la partition de réinstallation ne figure pas dans le BIOS ou dans le menu de démarrage. Si c'est le cas, le lecteur contenant le système de réinstallation est peut-être manquant ou endommagé. Une RMA est probablement nécessaire.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.