# Mise à niveau de la paire de basculement actif/veille ASA pour le pare-feu sécurisé

## Table des matières



## Introduction

Ce document décrit comment mettre à niveau ASA pour les déploiements de basculement pour Secure Firewall 1000, 2100 en mode Appliance, et Secure Firewall 3100/4200.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Secure Firewall Threat Defense.
- Configuration de l'appareil de sécurité adaptatif Cisco (ASA).

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions logicielles :

- Logiciel Cisco Adaptive Security Appliance Version 9.14(4)
- Logiciel Cisco Adaptive Security Appliance Version 9.16(4)

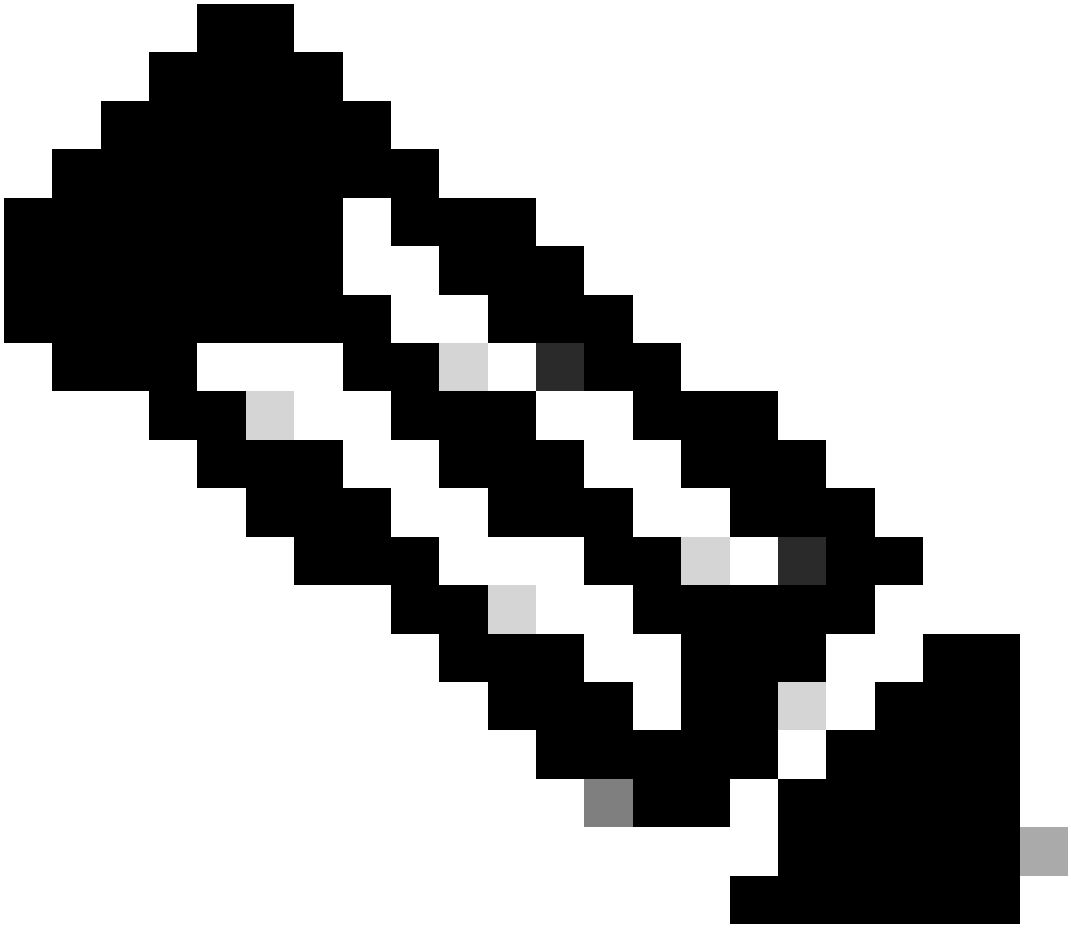
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

# Configurer

## Vérification des conditions préalables

Étape 1. Exécutez la commande show fxos mode pour vérifier que votre périphérique est en mode appliance

---



> Remarque : pour Secure Firewall 21XX dans les versions 9.13 et antérieures, ne prenez en charge que le mode Plate-forme. Dans les versions 9.14 et ultérieures, le mode Appliance est le mode par défaut.

---

<#root>

**ciscoasa#**

**show fxos mode**

**Mode is currently set to appliance**

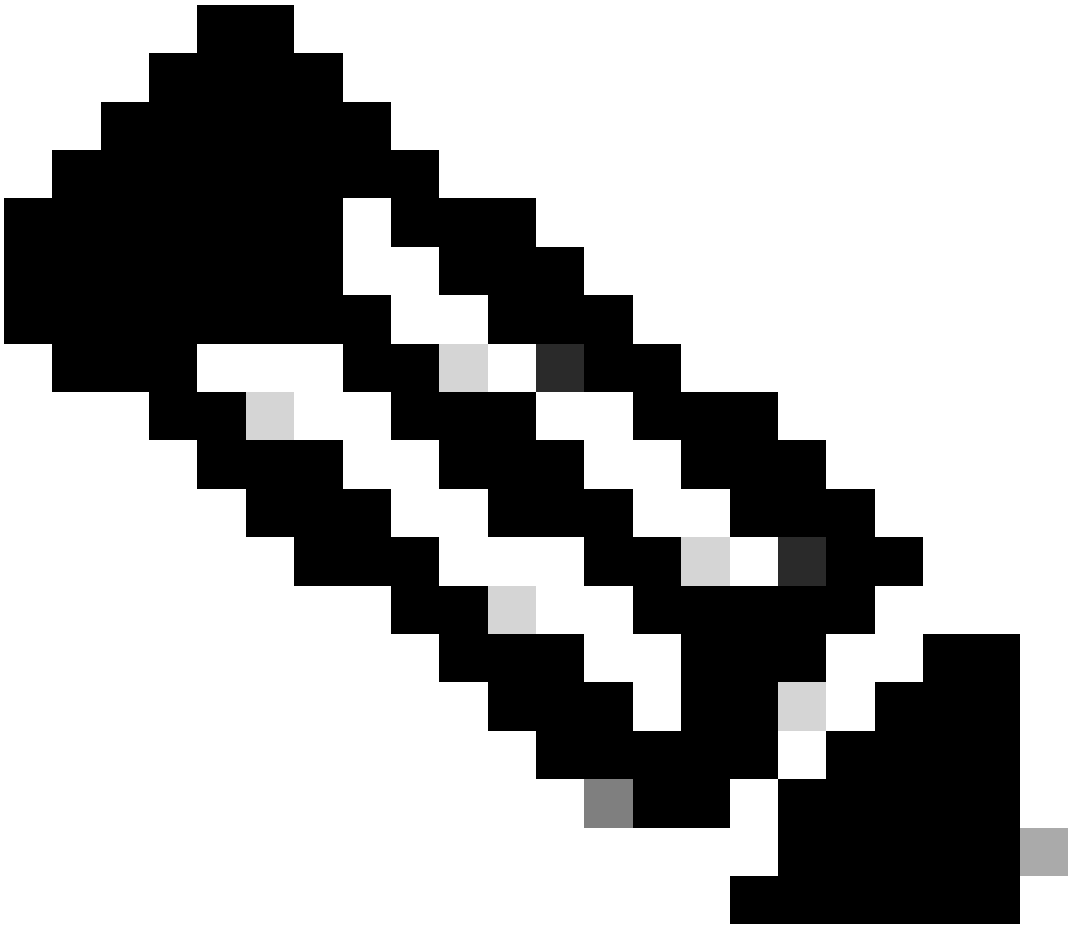
Étape 2. Vérifiez la compatibilité.

Consultez le document de compatibilité Cisco Secure Firewall ASA pour vérifier la compatibilité entre la plate-forme matérielle FTD et le logiciel Secure Firewall ASA. Reportez-vous à:

Compatibilité Cisco Secure Firewall ASA

Étape 3. Téléchargez le package de mise à niveau depuis Cisco Software Central.

---



> Remarque : pour les pare-feu 1000/2100 et 3100/4200, vous ne pouvez pas installer ASA ou FXOS séparément ; les deux images font partie d'un bundle.

---

Consultez le titre lié pour connaître la version d'ASA et de FXOS qui font partie de l'offre. Reportez-vous à la section Versions groupées ASA et FXOS du pare-feu sécurisé 1000/2100 et 3100/4200 .

## Mise à niveau via la CLI

Étape 1. Réinitialisez l'image ASDM.

Connectez-vous à l'unité principale en mode de configuration globale et exécutez les commandes suivantes :

<#root>

ciscoasa(config)#

**asdm image disk0:/asdm.bin**

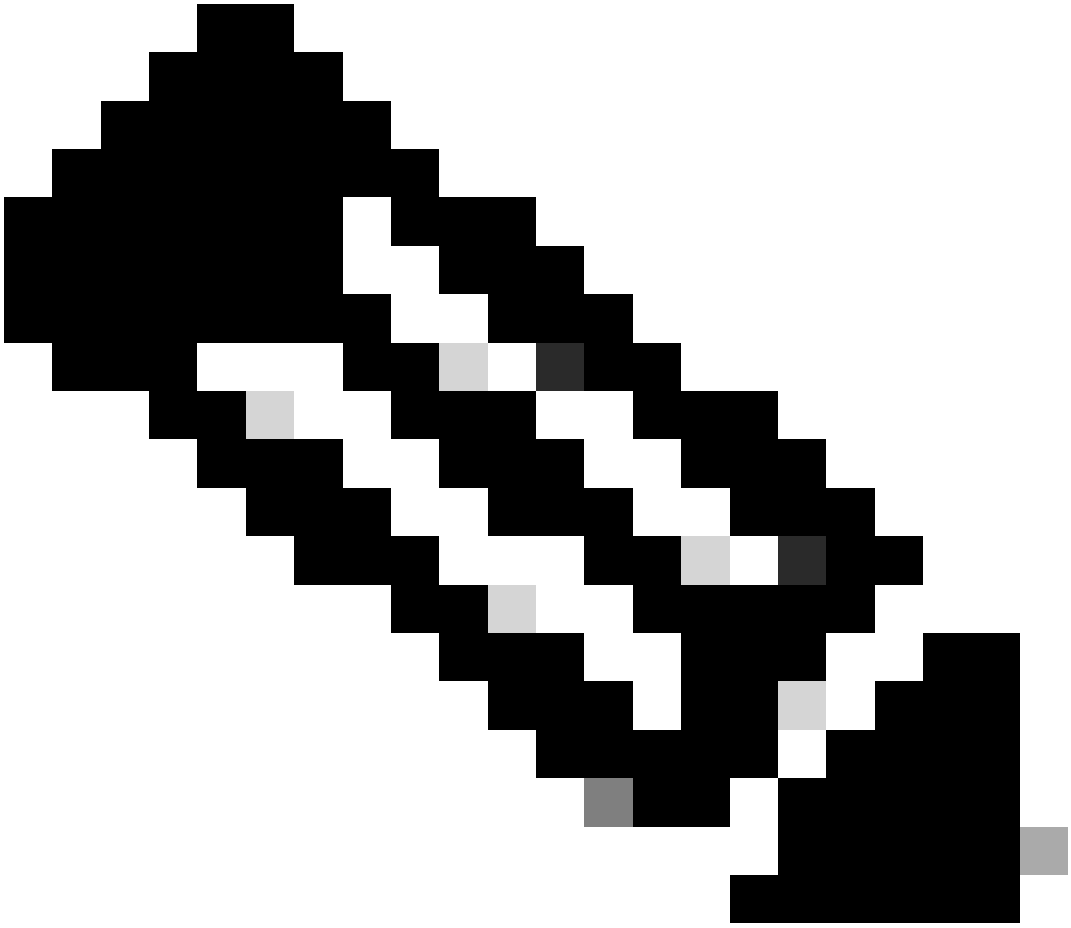
ciscoasa(config)# exit
ciscoasa#

**copy running-config startup-config**

Source filename [running-config]?
Cryptochecksum: 6beb01d1 b7a3c30f 5e8eb557 a8ebb8ca

12067 bytes copied in 3.780 secs (4022 bytes/sec)

Étape 2. Téléchargez l'image logicielle sur l'unité principale.



Remarque : dans ce document, vous utilisez un serveur FTP, mais vous pouvez utiliser TFTP, HTTP ou d'autres types de serveurs.

<#root>

ciscoasa#

```
copy  ftp://calo:calo@10.88.7.12/cisco-asa-fp2k.9.16.4.SPA disk0:/cisco-asa-fp2k.9.16.4.SPA

Address or name of remote host [10.88.7.12]?

Source username [calo]?

Source password []? ****

Source filename [cisco-asa-fp2k.9.16.4.SPA]?

Destination filename [cisco-asa-fp2k.9.16.4.SPA]?

Accessing  ftp:/calo:<password>@10.88.7.12/cisco-asa-fp2k.9.16.4.SPA...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Verifying file disk0:/cisco-asa-fp2k.9.16.4.SPA...
```

```
Writing file disk0:/cisco-asa-fp2k.9.16.4.SPA...

474475840 bytes copied in 843.230 secs (562842 bytes/sec)
```

Étape 3. Téléchargez l'image logicielle sur l'unité secondaire.

Exécutez la commande sur l'unité principale.

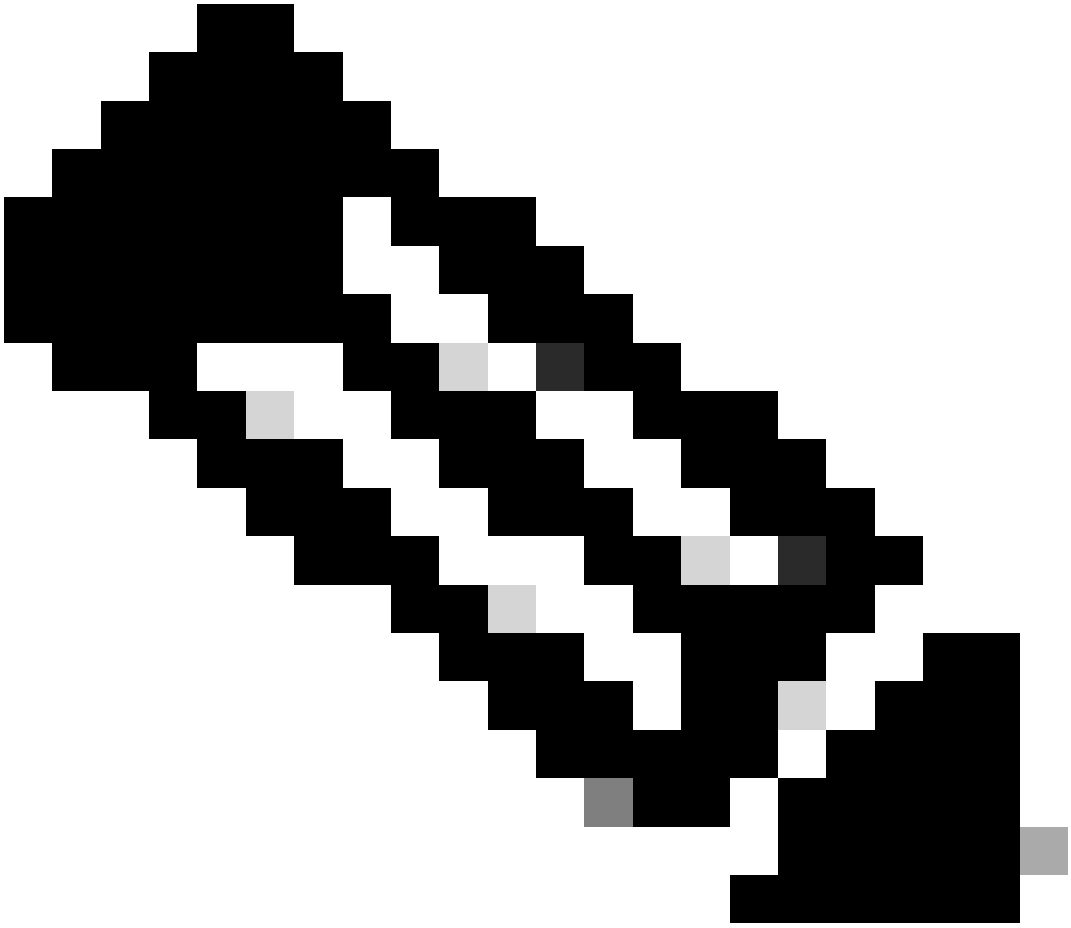
<#root>

ciscoasa#

```
failover exec mate copy /noconfirm ftp://calo:calo@10.88.7.12/cisco-asa-fp2k.9.16.4.SPA disk0:/cisco-asa
```

```
Accessing ftp://calo :<password>@10.88.7.12/cisco-asa-fp2k.9.16.4.SPA...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Verifying file disk0:/cisco-asa-fp2k.9.16.4.SPA...

Writing file disk0:/cisco-asa-fp2k.9.16.4.SPA...

474475840 bytes copied in 843.230 secs (562842 bytes/sec)
```

Étape 4. Vérifiez si une image de démarrage est actuellement configurée avec la **show running-config boot system** commande.



**Remarque** : vous n'avez peut-être pas configuré de système d'amorçage.

**<#root>**

**ciscoasa(config)#**

**show running-config boot system**

```
boot system disk0:/cisco-asa-fp2k.9.14.4.SPA
```

**Étape 5 (facultative).** Si vous avez configuré l'image de démarrage, vous devez la supprimer.

**no boot system diskn:/asa_image_name**

**Exemple :**

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp2k.9.14.4.SPA
```

**Étape 6.** Sélectionnez l'image à démarrer.

```
   <#root>

ciscoasa(config)#

boot system disk0:/cisco-asa-fp2k.9.16.4.SPA
```

```
The system is currently installed with security software package 9.14.4, which has:
   - The platform version:  2.8.1.172
   - The CSP (asa) version: 9.14.4
Preparing new image for install...
!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.16.4 will do the following:
   - upgrade to the new platform version 2.10.1.217
   - upgrade to the CSP ASA version 9.16.4
After installation is complete, ensure to do write memory and reload to save this config and apply the
Finalizing image install process...

Install_status: ready.........................
Install_status: validating-images....
Install_status: upgrading-npu
Install_status: upgrading-system.
Install_status: update-software-pack-completed
```

**Étape 7. Enregistrez la configuration avec la commande copy running-config startup-config**.

**Étape 8.** Rechargez l'unité secondaire pour installer la nouvelle version.

<#root>

ciscoasa(config)#

**failover reload-standby**

Attendez que l'unité secondaire se charge.

**Étape 9.** Une fois l'unité en veille rechargée, passez de l'état actif à l'état en veille.

<#root>

ciscoasa#

**no failover active**

**Étape 10.** Rechargez la nouvelle unité en veille pour installer la nouvelle version. Vous devez vous connecter à la nouvelle unité active.

<#root>

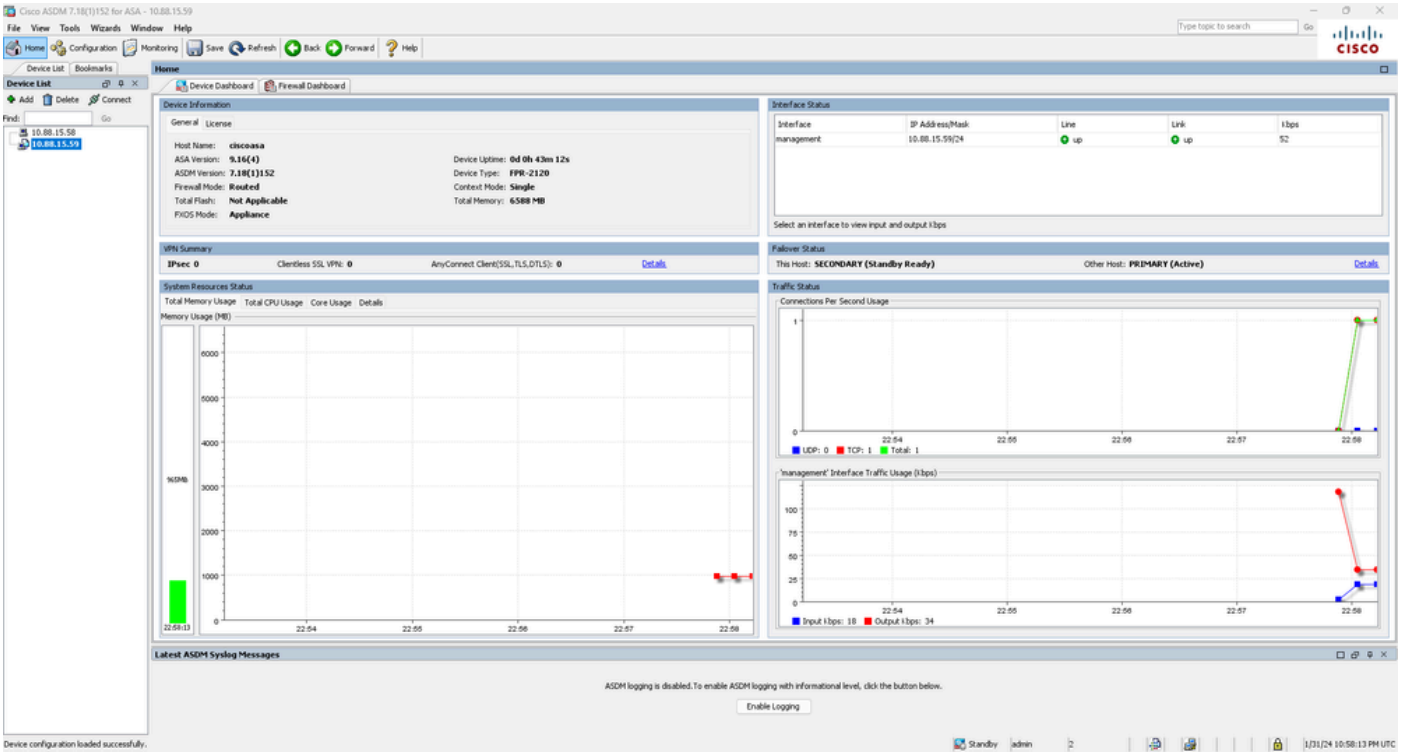
ciscoasa(config)#

```
failover reload-standby
```

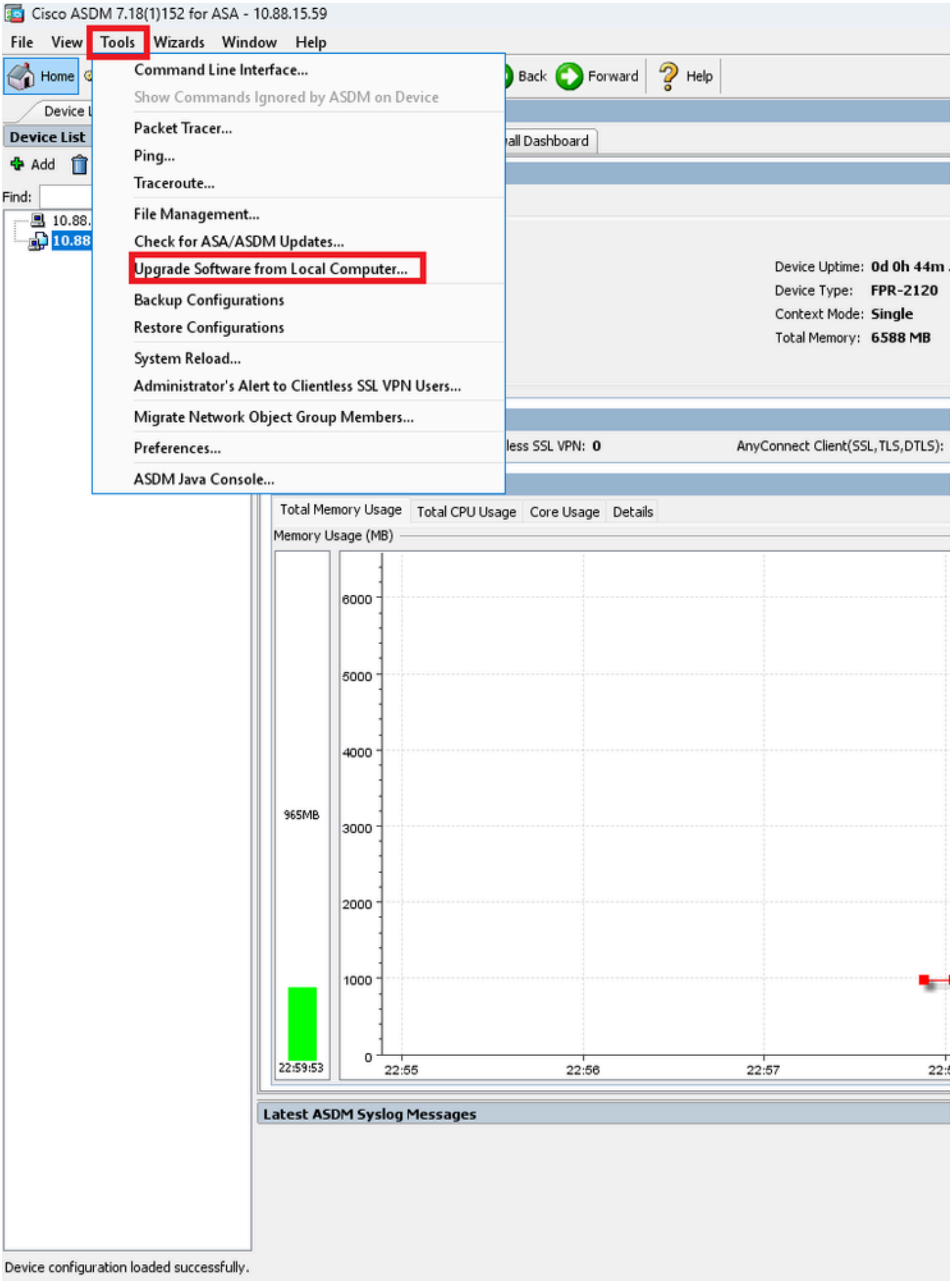
Une fois la nouvelle unité en veille chargée, la mise à niveau est terminée.

## Mise à niveau avec ASDM

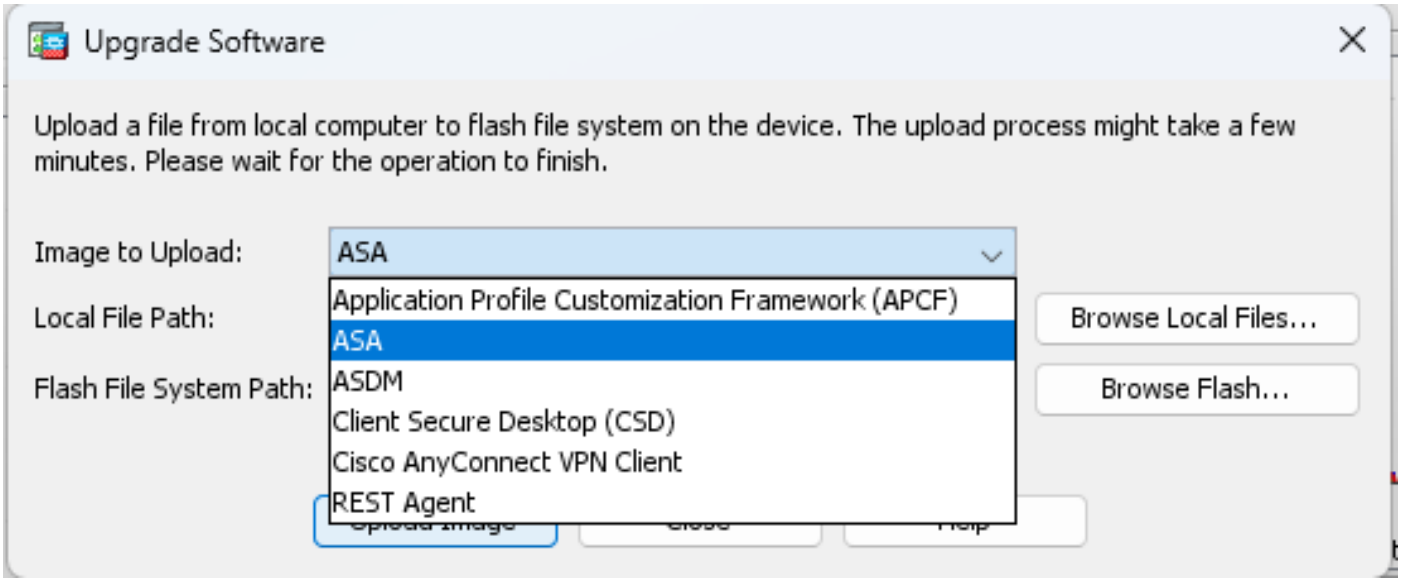
**Étape 1.** Connectez-vous à l'unité secondaire avec ASDM.



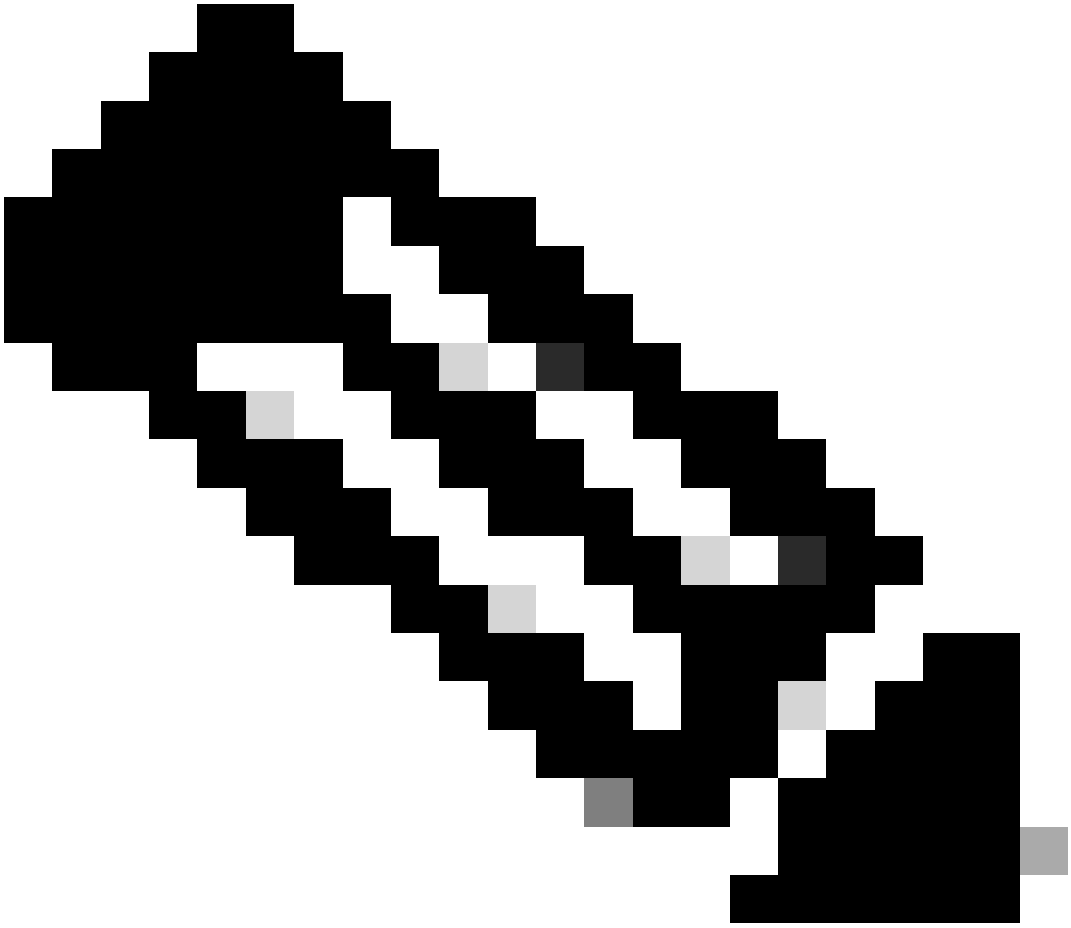

**Étape 2. Accédez à Outils > Mettre à niveau le logiciel à partir de l'ordinateur local**.



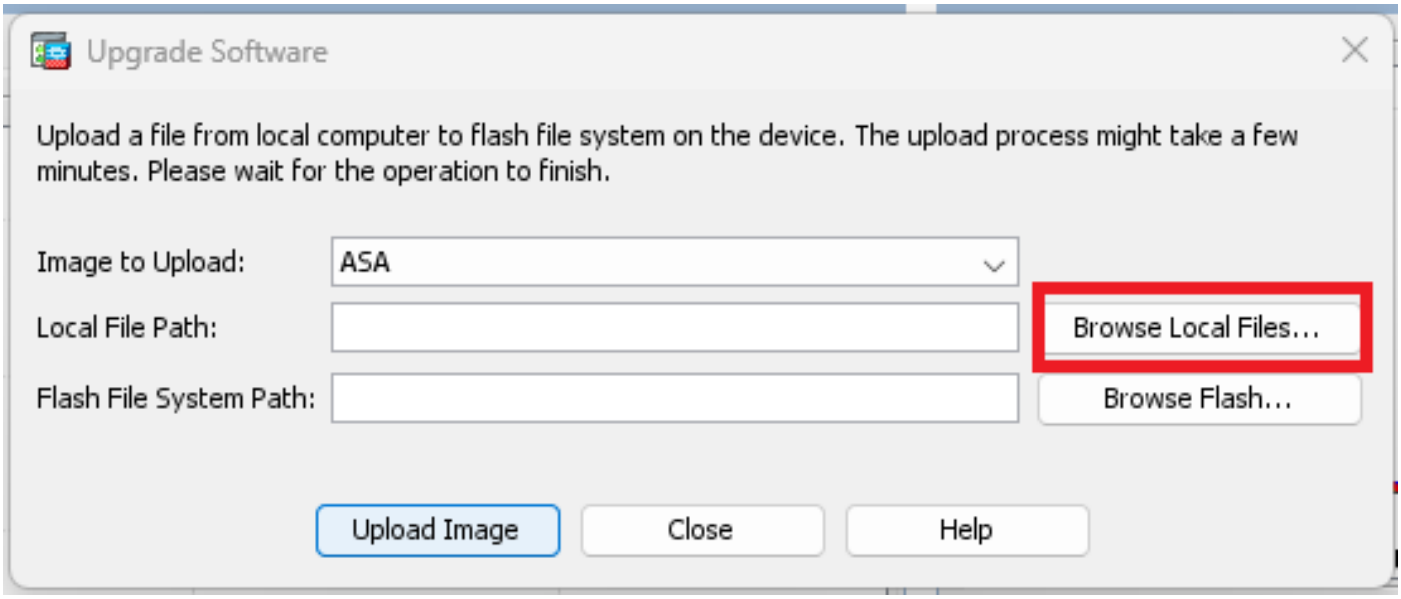

**Étape 3. Sélectionnez ASA** dans la liste déroulante.



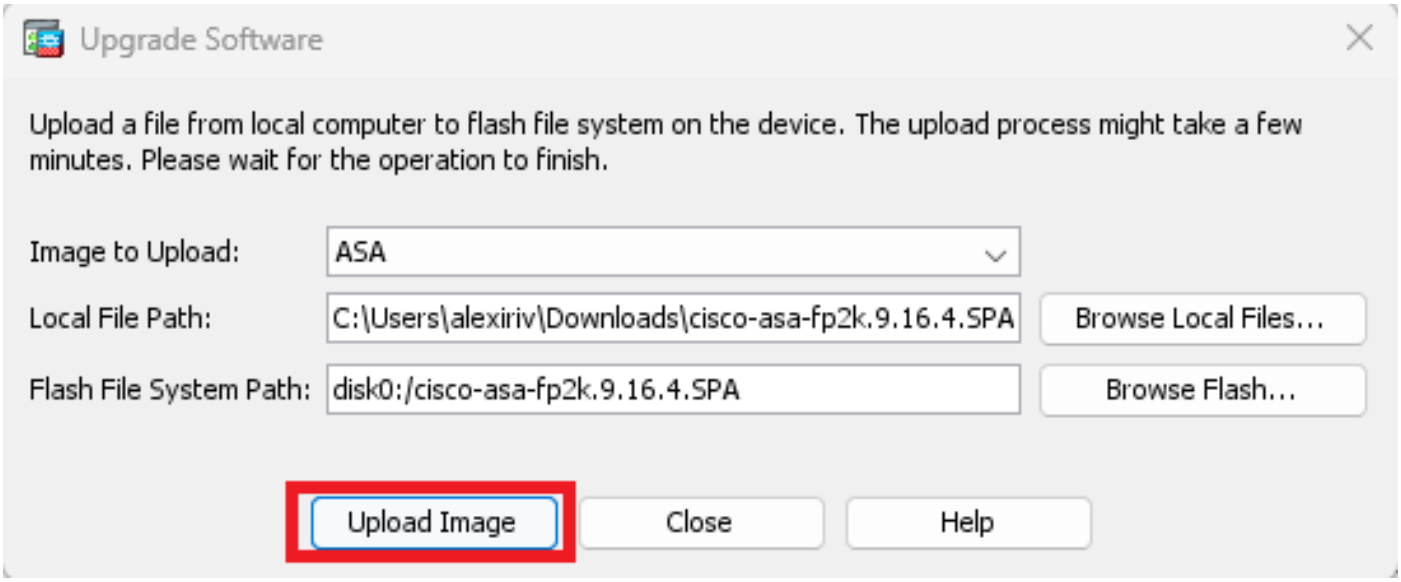

**Étape 4. Dans la fenêtre Upgrade Software, cliquez sur Browse Local Files** pour télécharger l'image logicielle sur l'unité secondaire.



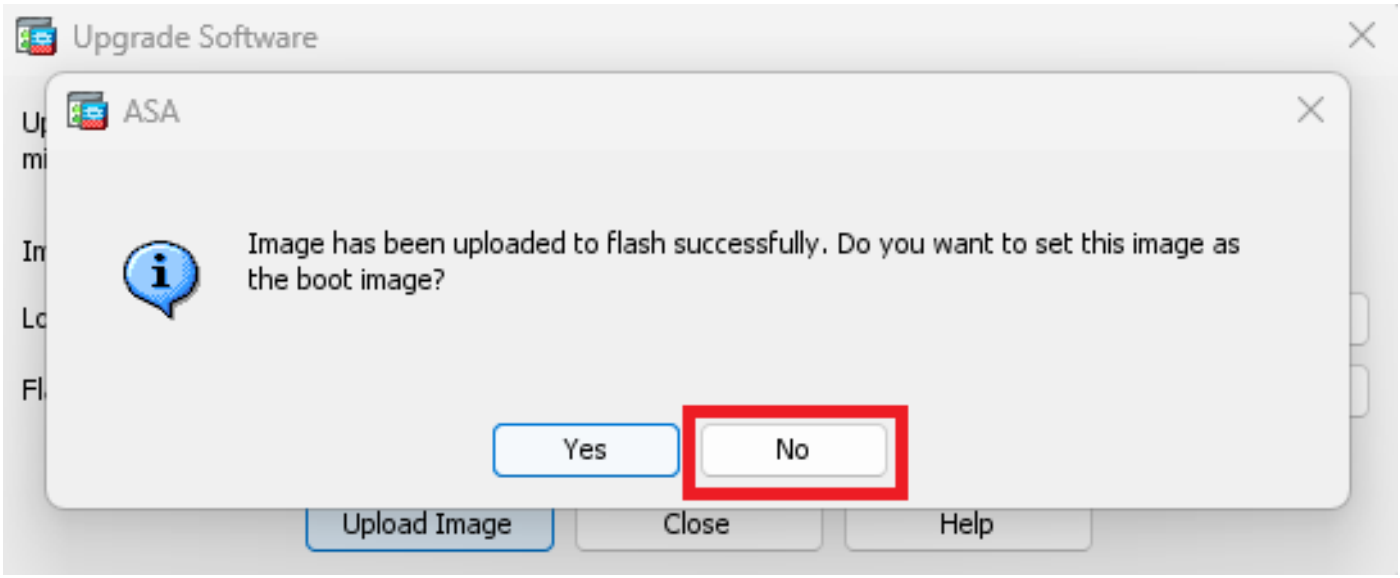
**Remarque** : par défaut, le **chemin d'accès du système de fichiers Flash** est disk0 ; pour le modifier, cliquez sur **Browse Flash** et sélectionnez le nouveau chemin d'accès.




Cliquez sur **Upload Image.**



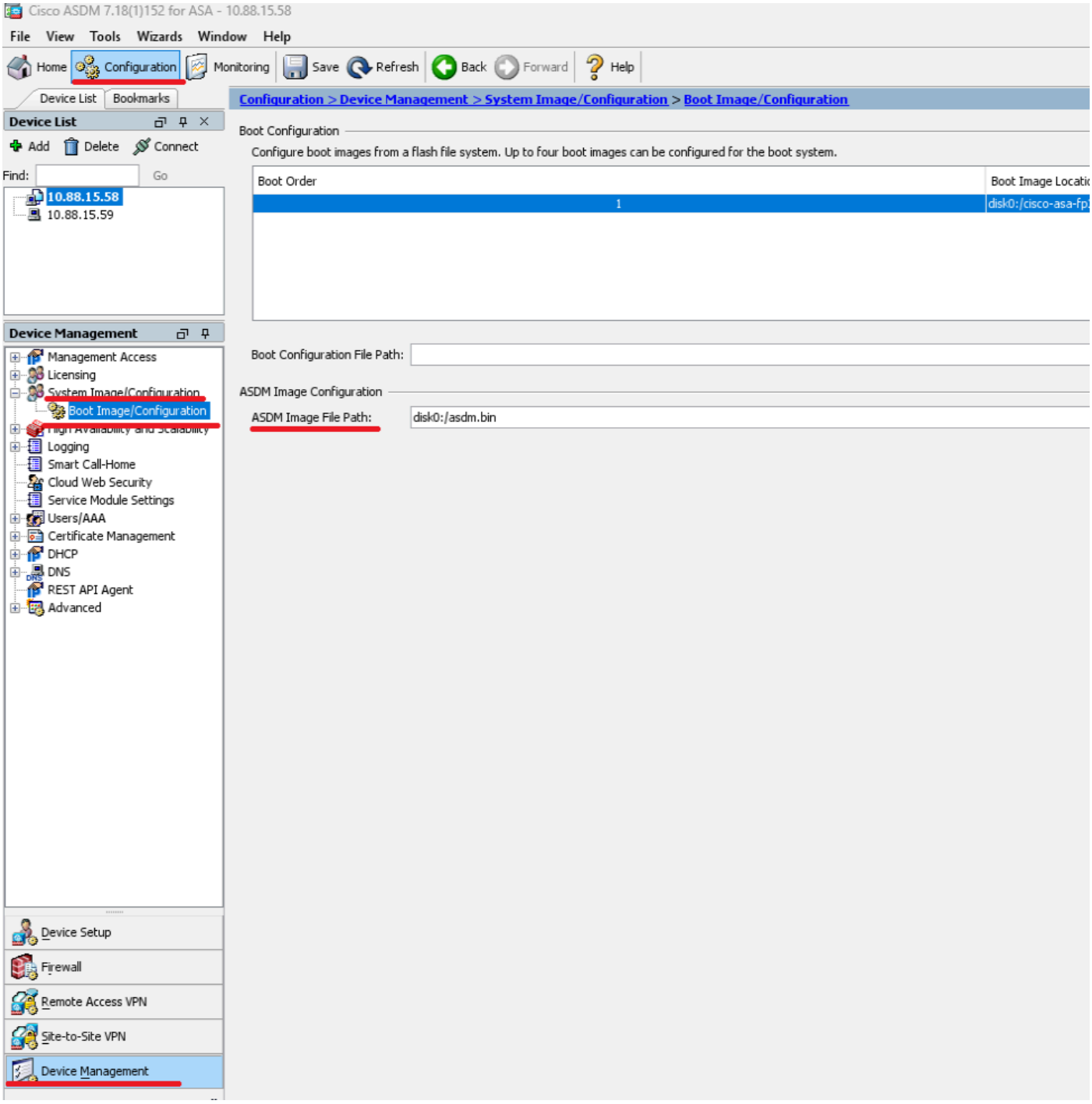

Une fois le téléchargement de l'image terminé, cliquez sur **No**.




**Étape 5.** Réinitialisez l'image ASDM**.**

Connectez-vous à l'unité principale avec ASDM et accédez à **Configuration > Device Management** > **System Image/Configuration** > **Boot Image/Configuration**.

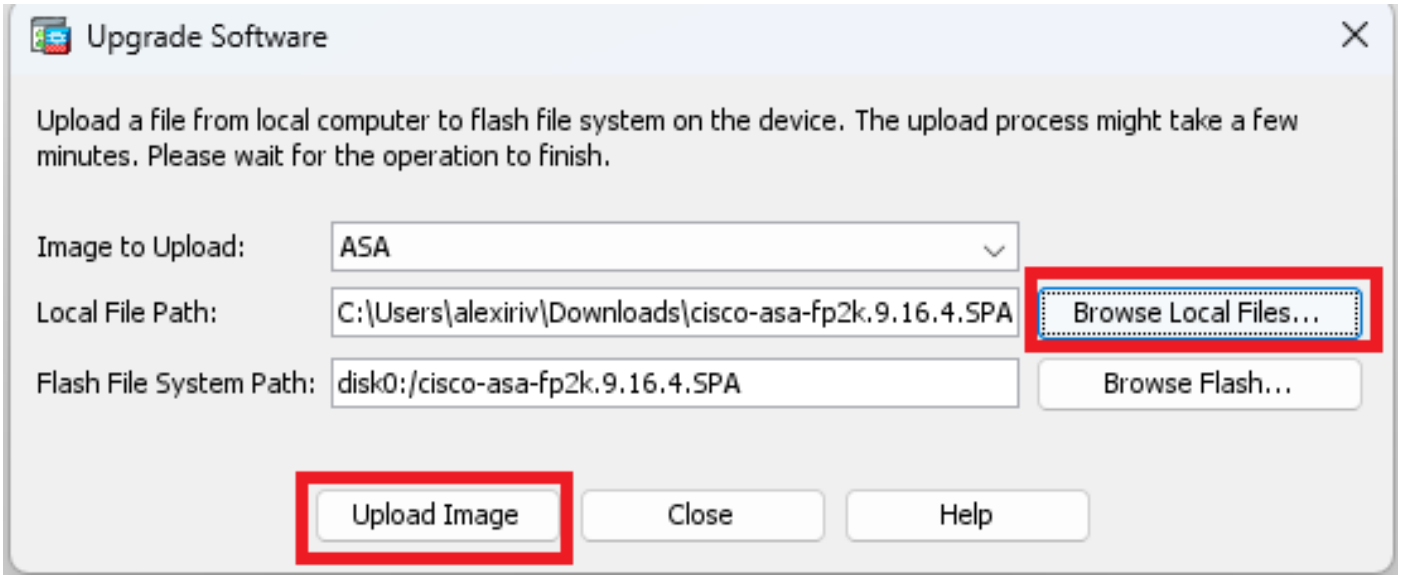
Dans **ASDM Image File Path,** entrez la valeur **disk0:/asdm.bin** et **Apply**.



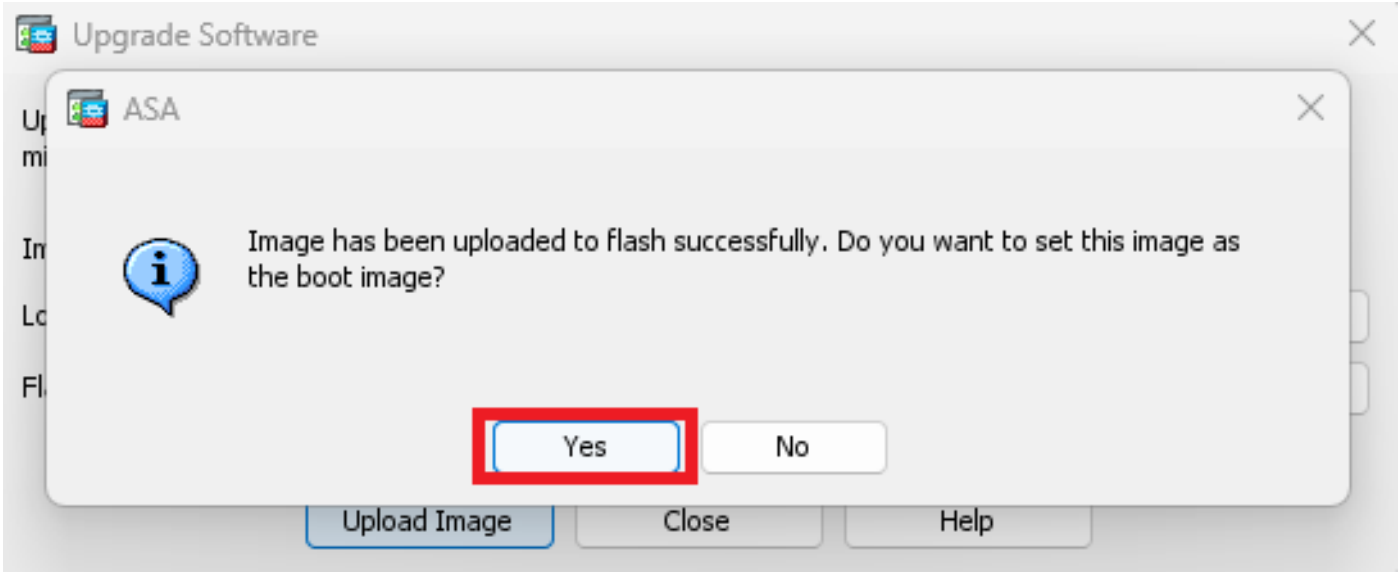

**Étape 6.** Téléchargez l'image logicielle sur l'unité principale.

Cliquez sur **Browse Local Files** et sélectionnez le package de mise à niveau sur votre périphérique.

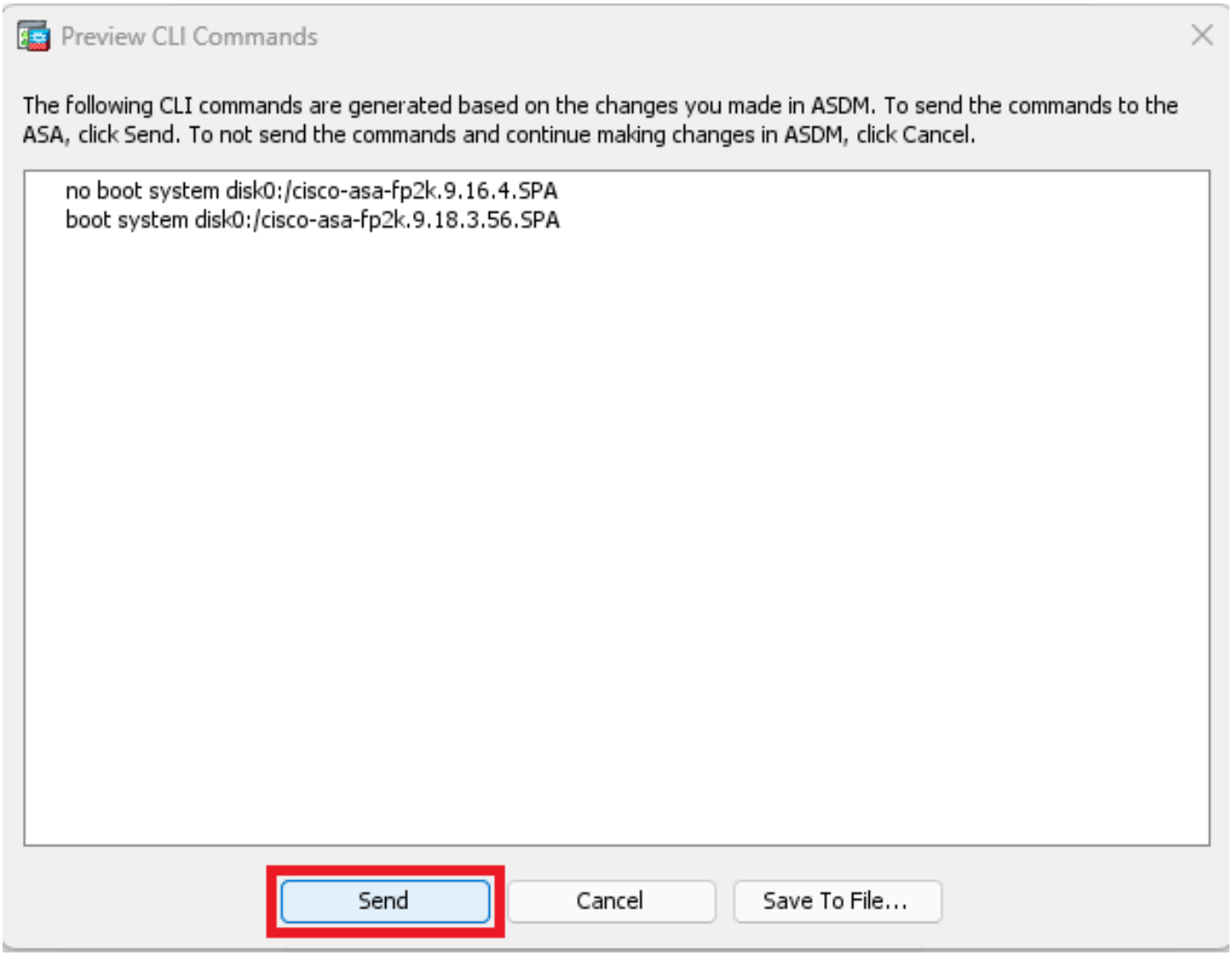
Cliquez sur **Upload Image.**



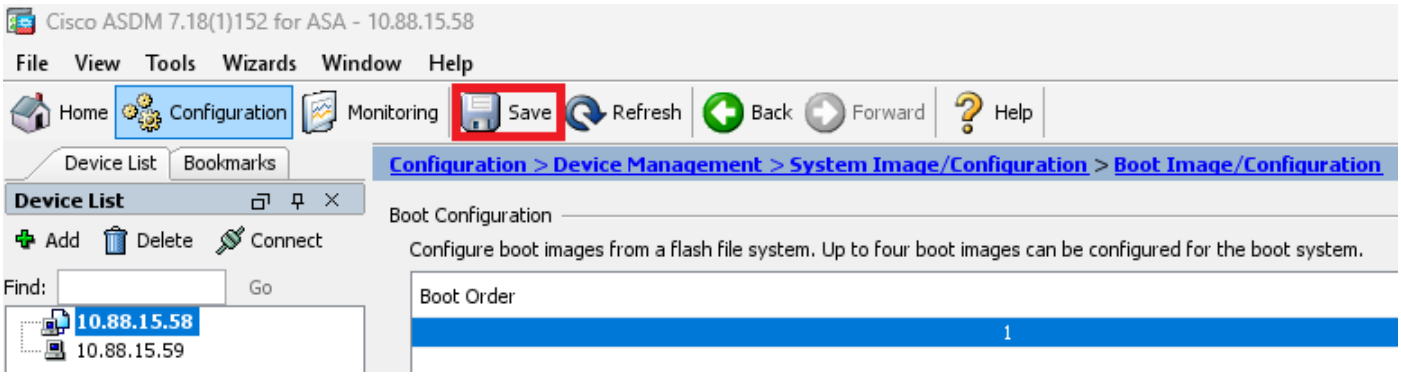

Une fois le téléchargement de l'image terminé, cliquez sur **Yes**.




Dans les fenêtres d'aperçu, cliquez sur le bouton **Send** pour enregistrer la configuration.

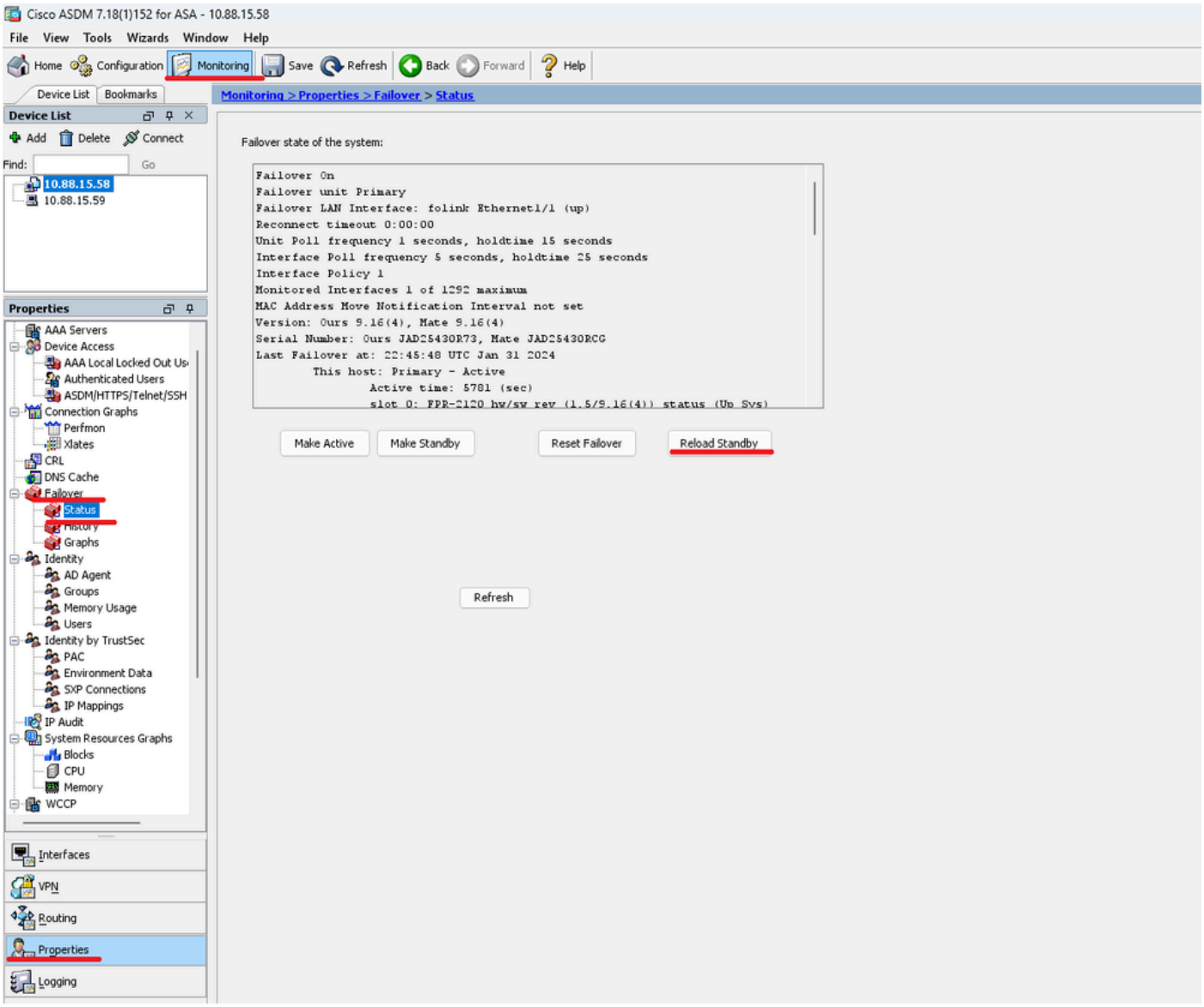



**Étape 7. Cliquez sur Save** pour enregistrer la configuration.




**Étape 8.** Rechargez l'unité secondaire pour installer la nouvelle version.

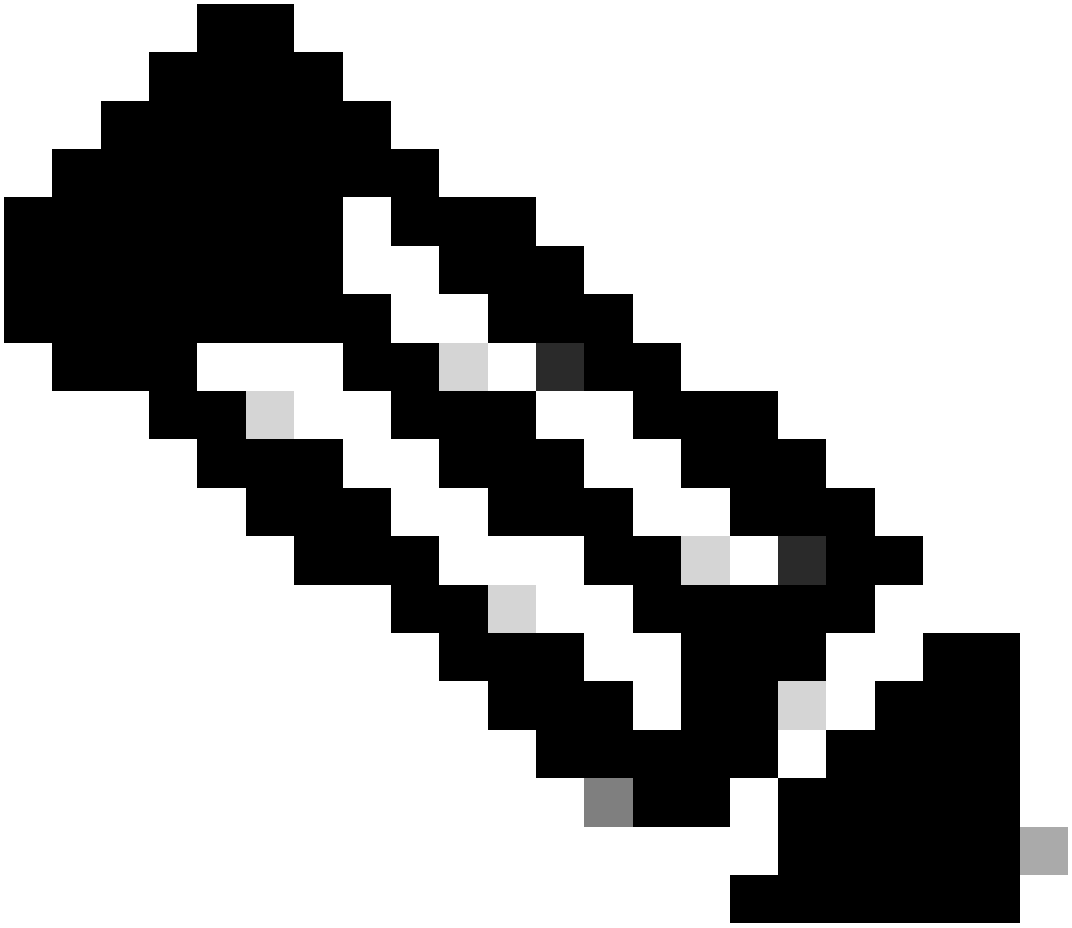
Accédez à Monitoring > **Properties** > **Failover** > Status et cliquez sur **Reload Standby**.



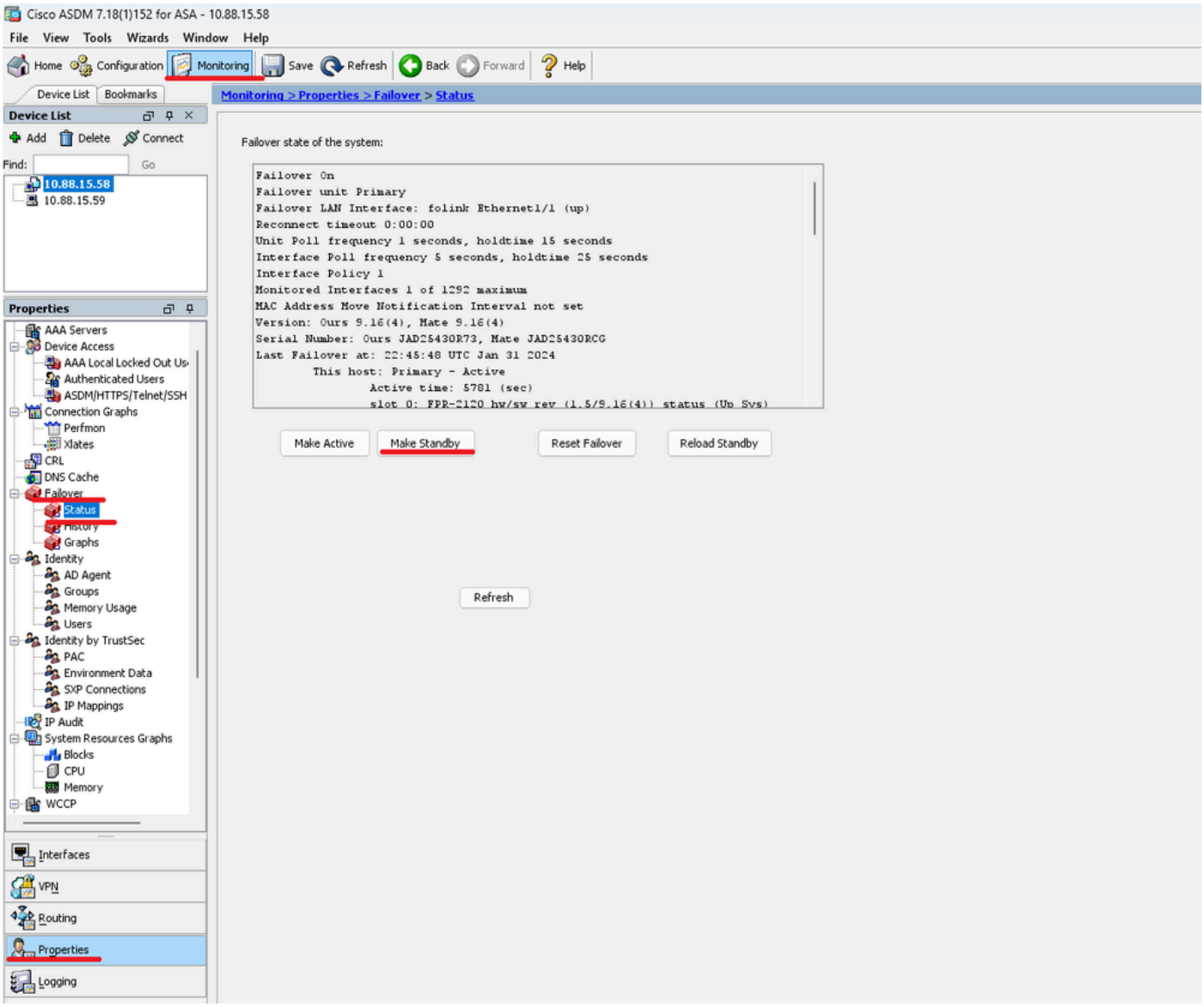

Attendez que l'unité en veille se charge.

**Étape 9.** Une fois l'unité en veille rechargée, passez de l'état actif à l'état en veille.

Accédez à Monitoring > **Properties** > **Failover** > Status et cliquez sur **Make Standby**.

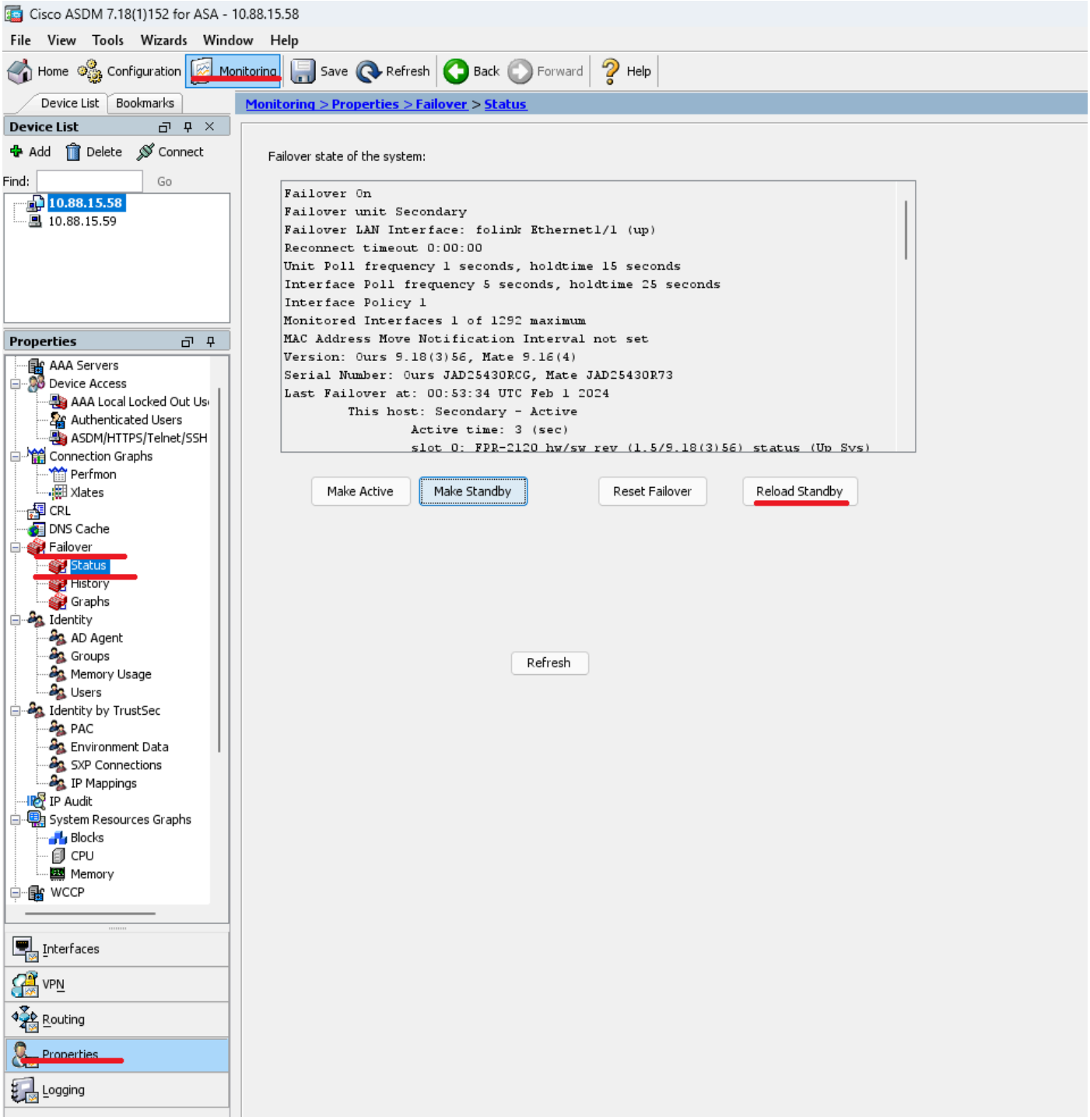


**Remarque** : ASMD se connecte automatiquement à la nouvelle unité active.




**Étape 10.** Rechargez la nouvelle unité en veille pour installer la nouvelle version.

Accédez à Monitoring **> Properties > Failover >** Status et cliquez sur **Reload Standby**.




Une fois la nouvelle unité en veille chargée, la mise à niveau est terminée.

# Vérifier

Pour vérifier que la mise à niveau a été effectuée sur les deux unités, vérifiez la mise à niveau via CLI et ASDM.

**Via CLI**

<#root>

ciscoasa#

**show failover**

```
Failover On
Failover unit Primary
Failover LAN Interface: folink Ethernet1/1 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1292 maximum
MAC Address Move Notification Interval not set
```

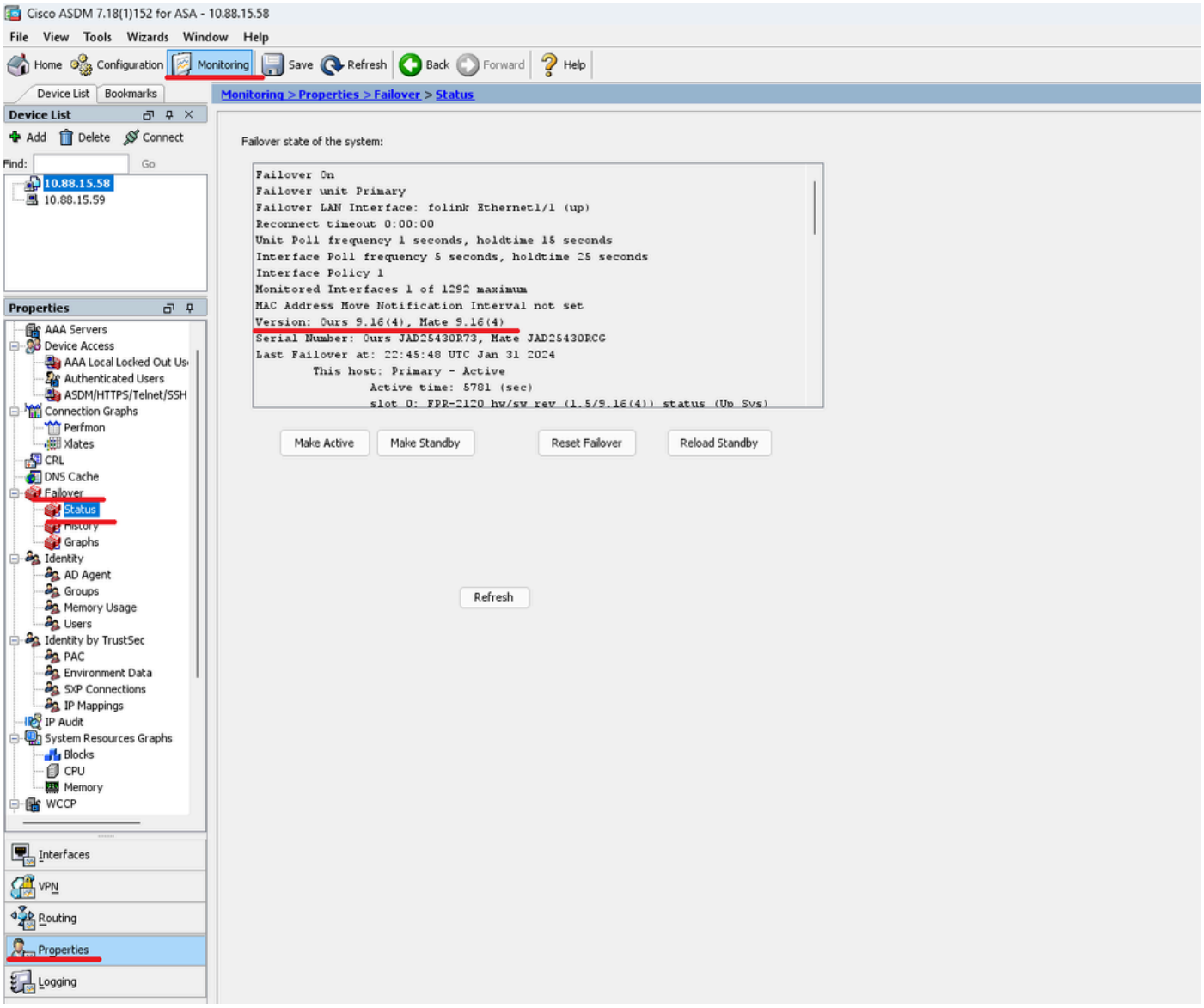
**Version: Ours 9.16(4), Mate 9.16(4)**

```
Serial Number: Ours JAD25430R73, Mate JAD25430RCG
Last Failover at: 22:45:48 UTC Jan 31 2024
This host: Primary - Active
Active time: 45 (sec)
slot 0: FPR-2120 hw/sw rev (1.5/9.16(4)) status (Up Sys)
Interface management (10.88.15.58): Normal (Monitored)
Other host: Secondary - Standby Ready
Active time: 909 (sec)
slot 0: FPR-2120 hw/sw rev (1.5/9.16(4)) status (Up Sys)
Interface management (10.88.15.59): Normal (Monitored)

Stateful Failover Logical Update Statistics
Link : folink Ethernet1/1 (up)
Stateful Obj xmit xerr rcv rerr
General 27 0 29 0
sys cmd 27 0 27 0
up time 0 0 0 0
RPC services 0 0 0 0
TCP conn 0 0 0 0
UDP conn 0 0 0 0
ARP tbl 0 0 1 0
Xlate_Timeout 0 0 0 0
IPv6 ND tbl 0 0 0 0
VPN IKEv1 SA 0 0 0 0
VPN IKEv1 P2 0 0 0 0
VPN IKEv2 SA 0 0 0 0
VPN IKEv2 P2 0 0 0 0
VPN CTCP upd 0 0 0 0
VPN SDI upd 0 0 0 0
VPN DHCP upd 0 0 0 0
SIP Session 0 0 0 0
SIP Tx 0 0 0 0
SIP Pinhole 0 0 0 0
Route Session 0 0 0 0
Router ID 0 0 0 0
```

```
User-Identity 0 0 1 0
CTS SGTNAME 0 0 0 0
CTS PAC 0 0 0 0
TrustSec-SXP 0 0 0 0
IPv6 Route 0 0 0 0
STS Table 0 0 0 0
Umbrella Device-ID 0 0 0 0

Logical Update Queue Information
Cur Max Total
Recv Q: 0 10 160
Xmit Q: 0 1 53
```

**Via ASDM**

Accédez à **Surveillance** > **Propriétés** > **Basculement** > **État**, Vous pouvez voir la version ASA pour les deux périphériques.




## Informations connexes

- Compatibilité Cisco Secure Firewall ASA
- Guide de mise à niveau Cisco Secure Firewall ASA

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.