Actualización del par de failover activo/en espera de ASA para el firewall seguro

Contenido

Introducción

Este documento describe cómo actualizar ASA para implementaciones de failover para Secure Firewall 1000, 2100 en modo Appliance, y Secure Firewall 3100/4200.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Secure Firewall Threat Defence.
- Configuración del dispositivo de seguridad adaptable (ASA) de Cisco.

Componentes Utilizados

La información de este documento se basa en las versiones de software:

- Software Cisco Adaptive Security Appliance Versión 9.14(4)
- Software Cisco Adaptive Security Appliance Versión 9.16(4)

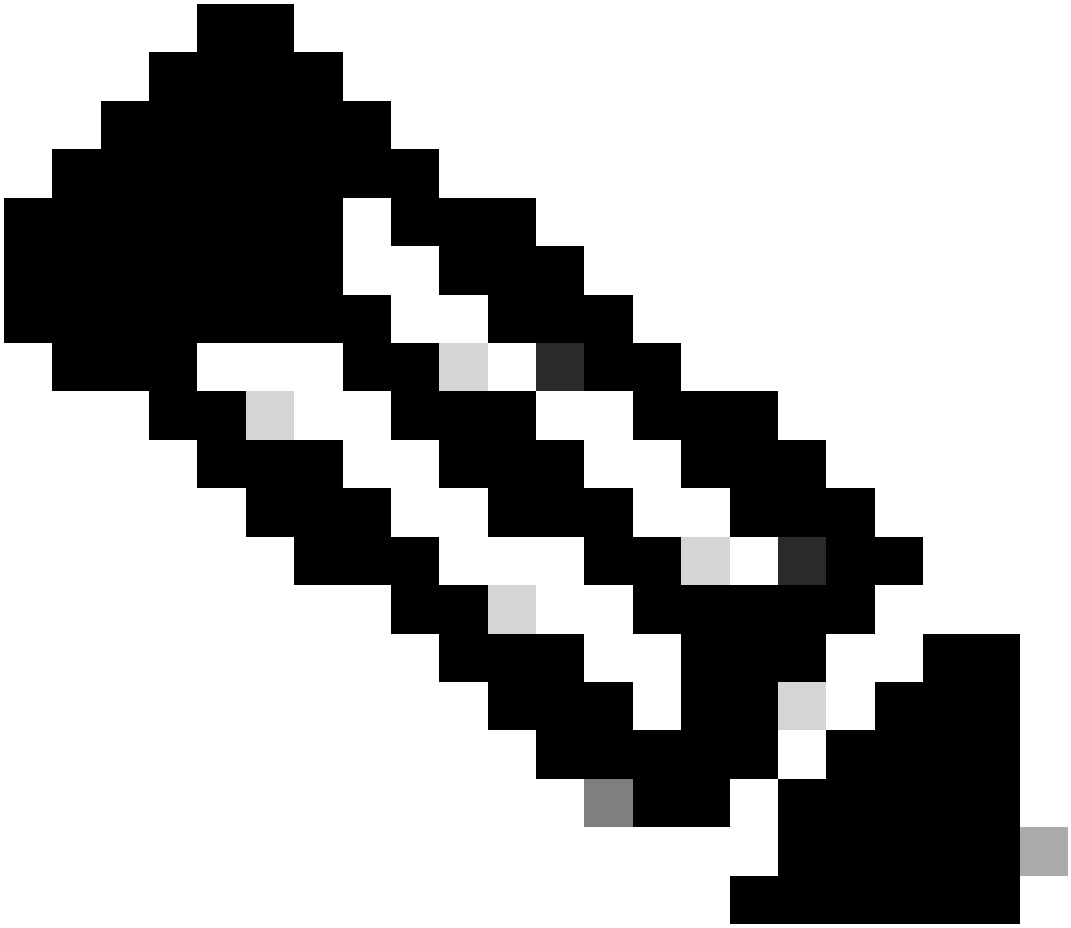
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Verifique los requisitos previos

Paso 1. Ejecute el comando show fxos mode para verificar que su dispositivo está en modo de dispositivo

---



> Nota: para Secure Firewall 21XX en la versión 9.13 y anteriores, solo es compatible con el modo de plataforma. En la versión 9.14 y posteriores, el modo de dispositivo es el predeterminado.

<#root>

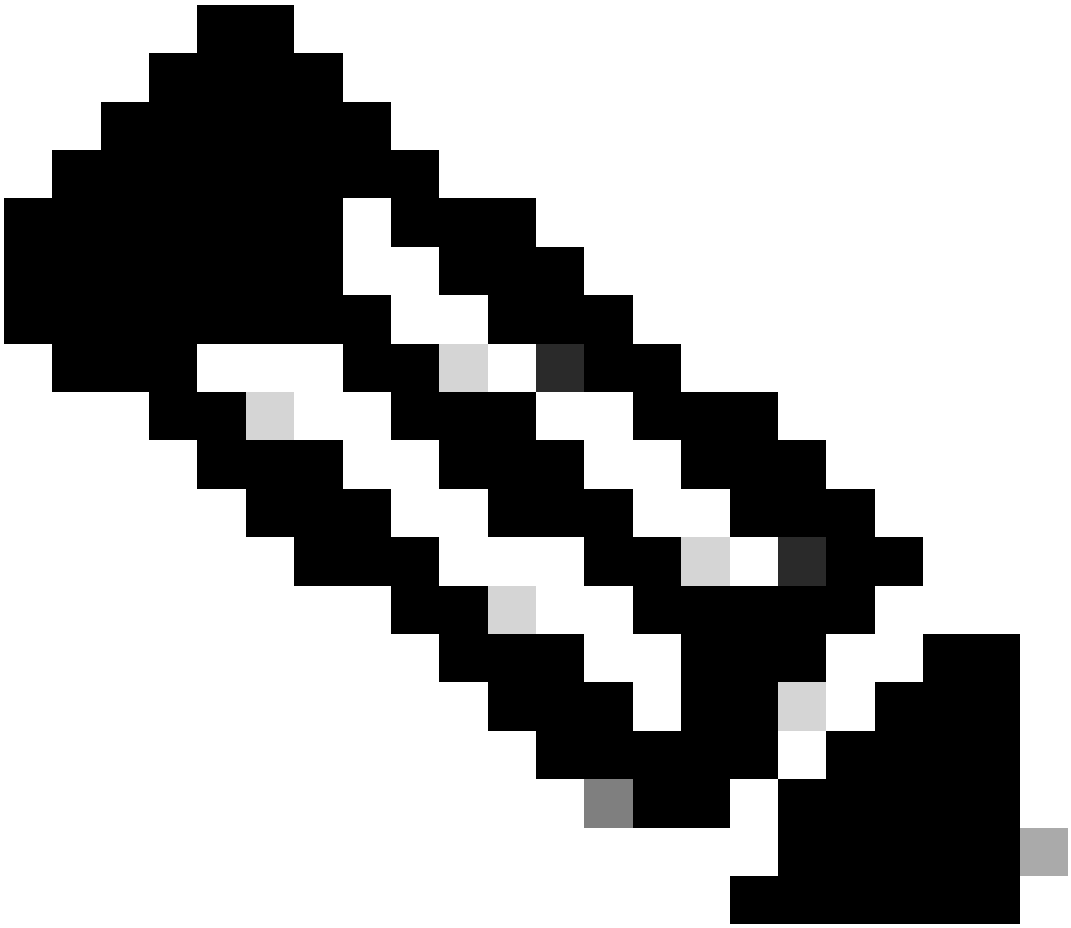
```
ciscoasa#

show fxos mode


Mode is currently set to appliance
```

Paso 2. Verifique la compatibilidad.

Consulte el documento de compatibilidad de Cisco Secure Firewall ASA para verificar la compatibilidad entre la plataforma de hardware FTD y el software Secure Firewall ASA. Consulte

Compatibilidad con Cisco Secure Firewall ASA

Paso 3. Descargue el paquete de actualización de Cisco Software Central.



> Nota: para Secure Firewall 1000/2100 y Secure Firewall 3100/4200, no puede instalar ASA ni FXOS por separado; ambas imágenes forman parte de un paquete.

Consulte el título vinculado para conocer la versión de ASA y FXOS que forman parte del paquete. Consulte Secure Firewall 1000/2100 y 3100/4200 ASA y FXOS Bundle Versions .

Actualización mediante la CLI

Paso 1. Restablezca la imagen de ASDM.

Conéctese a la unidad primaria en el modo de configuración global y ejecute los comandos:

<#root>

ciscoasa(config)#

asdm image disk0:/asdm.bin

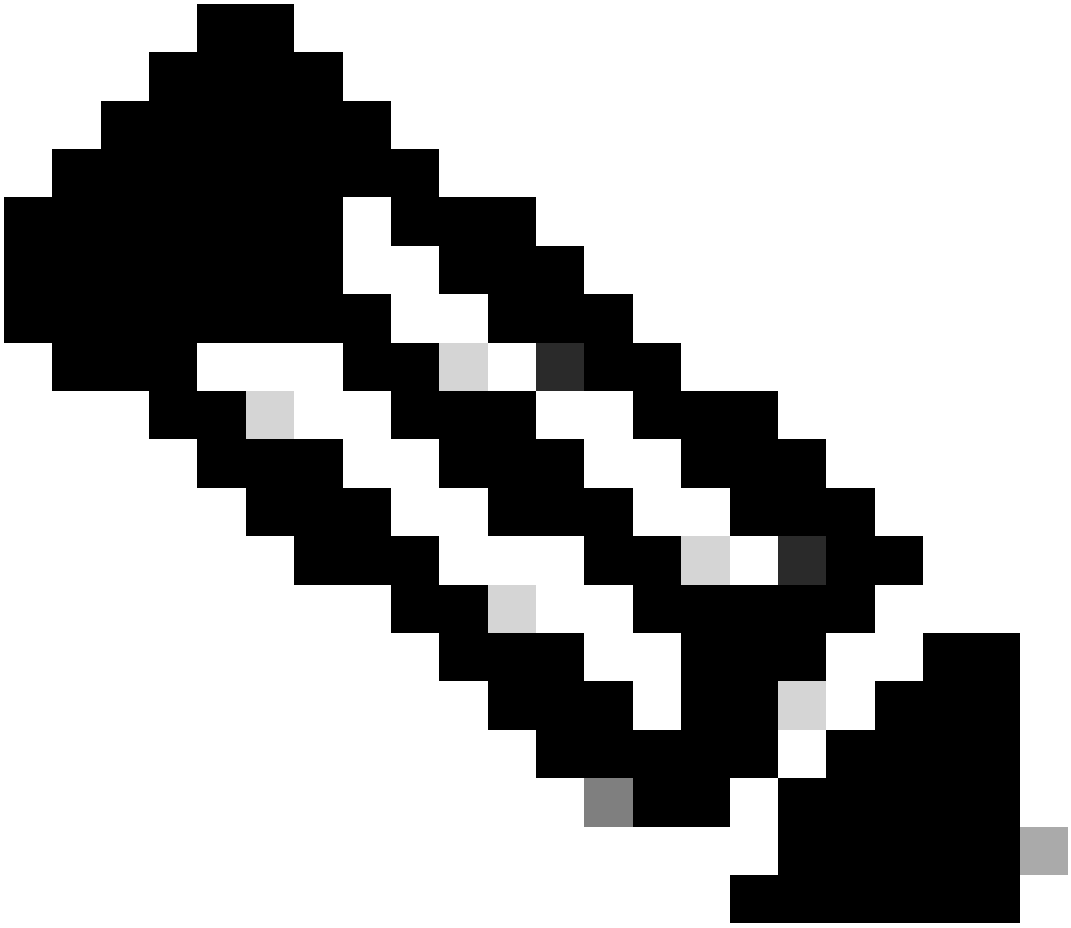
ciscoasa(config)# exit
ciscoasa#

copy running-config startup-config

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

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

Paso 2. Cargue la imagen de software en la unidad principal.



Nota: En este documento, está utilizando un servidor FTP, pero puede utilizar TFTP, HTTP u otros tipos de servidor.

<#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)
```

Paso 3. Cargue la imagen del software en la unidad secundaria.

Ejecute el comando en la unidad primaria.

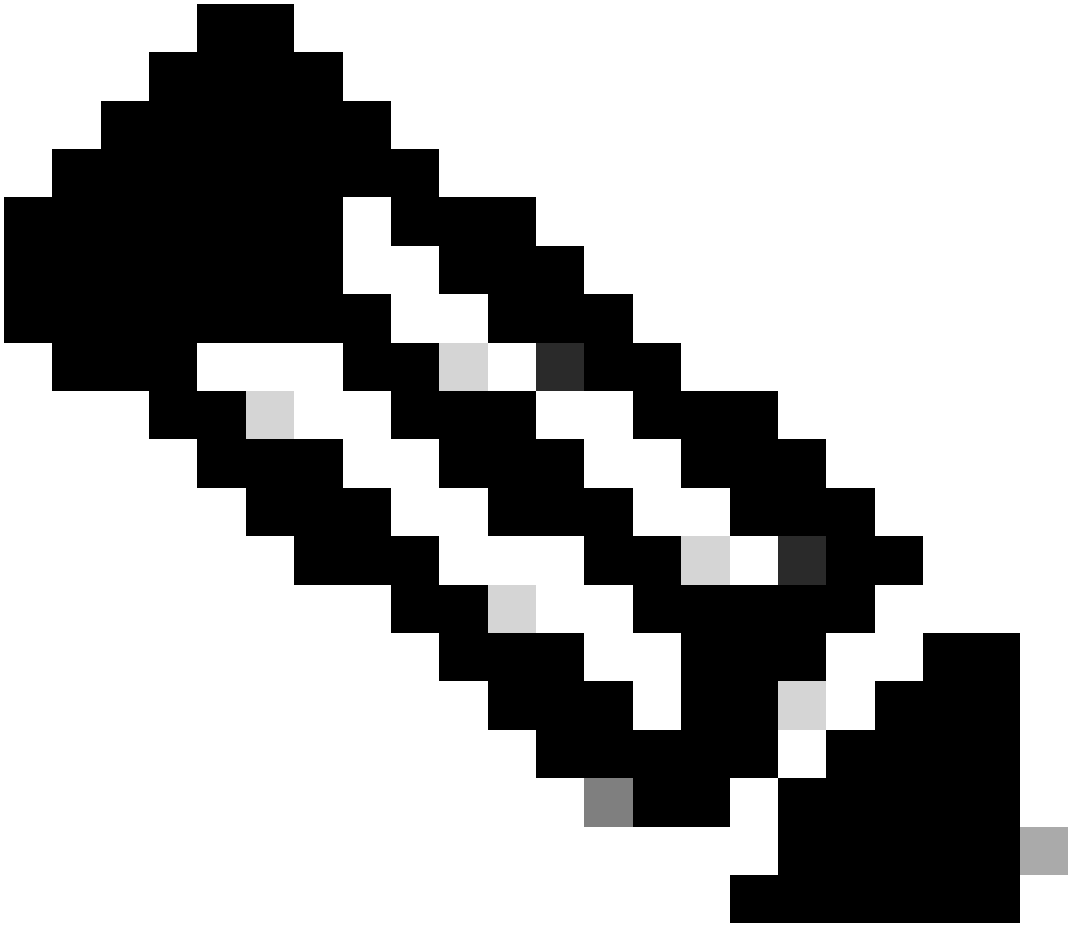
<#root>

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)
```

Paso 4. Verifique si tiene una imagen de inicio actual configurada con el **show running-config boot system** comando.



Nota: Es posible que no haya configurado un sistema de arranque.

<#root>

ciscoasa(config)#

show running-config boot system

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

Paso 5 (opcional). En caso de que tenga configurada la imagen de arranque, debe eliminarla.

no boot system disk:/asa_image_name

Ejemplo:

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

Paso 6. Seleccione la imagen que desea arrancar.

<#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
```

Paso 7. Guarde la configuración con el comando copy running-config startup-config.

Paso 8. Vuelva a cargar la unidad secundaria para instalar la nueva versión.

<#root>

ciscoasa(config)#

failover reload-standby

Espere hasta que se cargue la unidad secundaria.

Paso 9. Una vez recargada la unidad en espera, cambie la unidad primaria del estado activo al estado en espera.

<#root>

ciscoasa#

no failover active

Paso 10. Vuelva a cargar la nueva unidad en espera para instalar la nueva versión. Debe conectarse a la nueva unidad activa.

<#root>

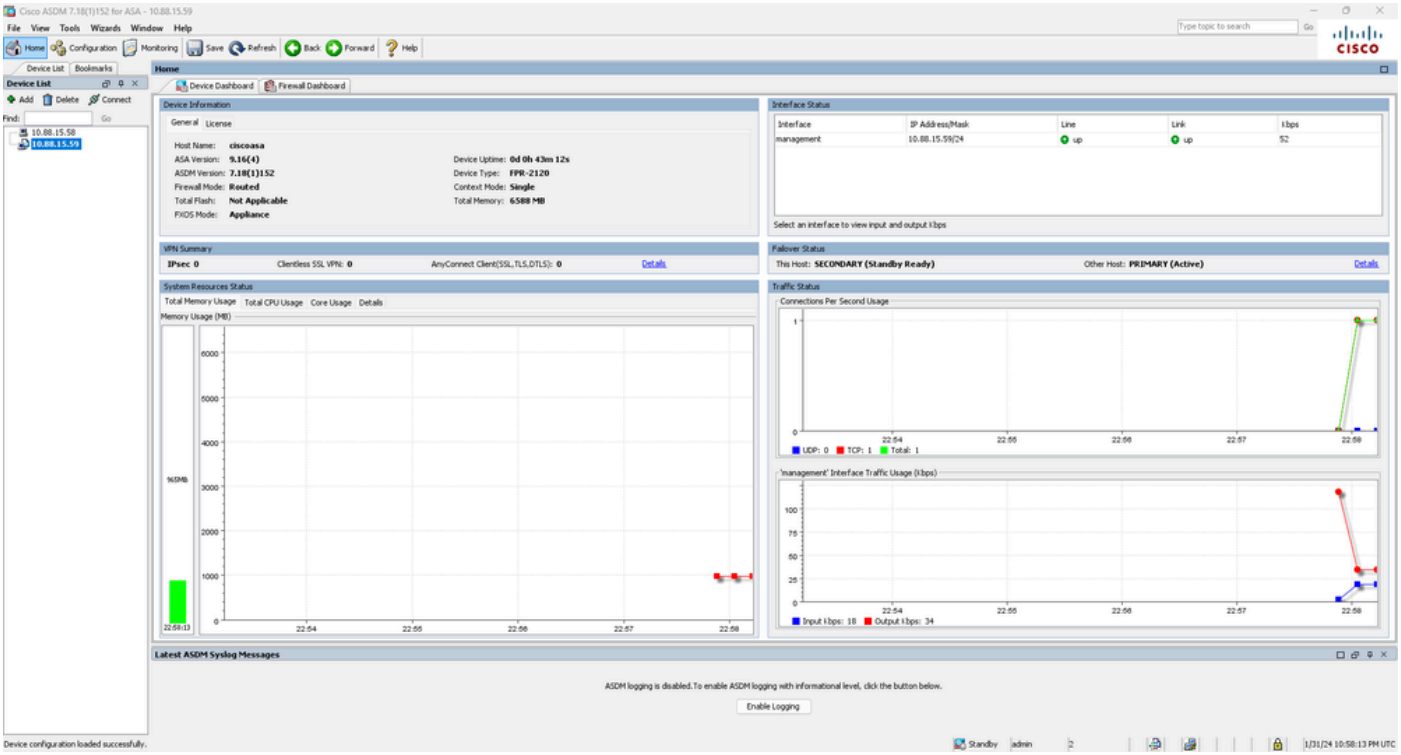
ciscoasa(config)#

```
failover reload-standby
```

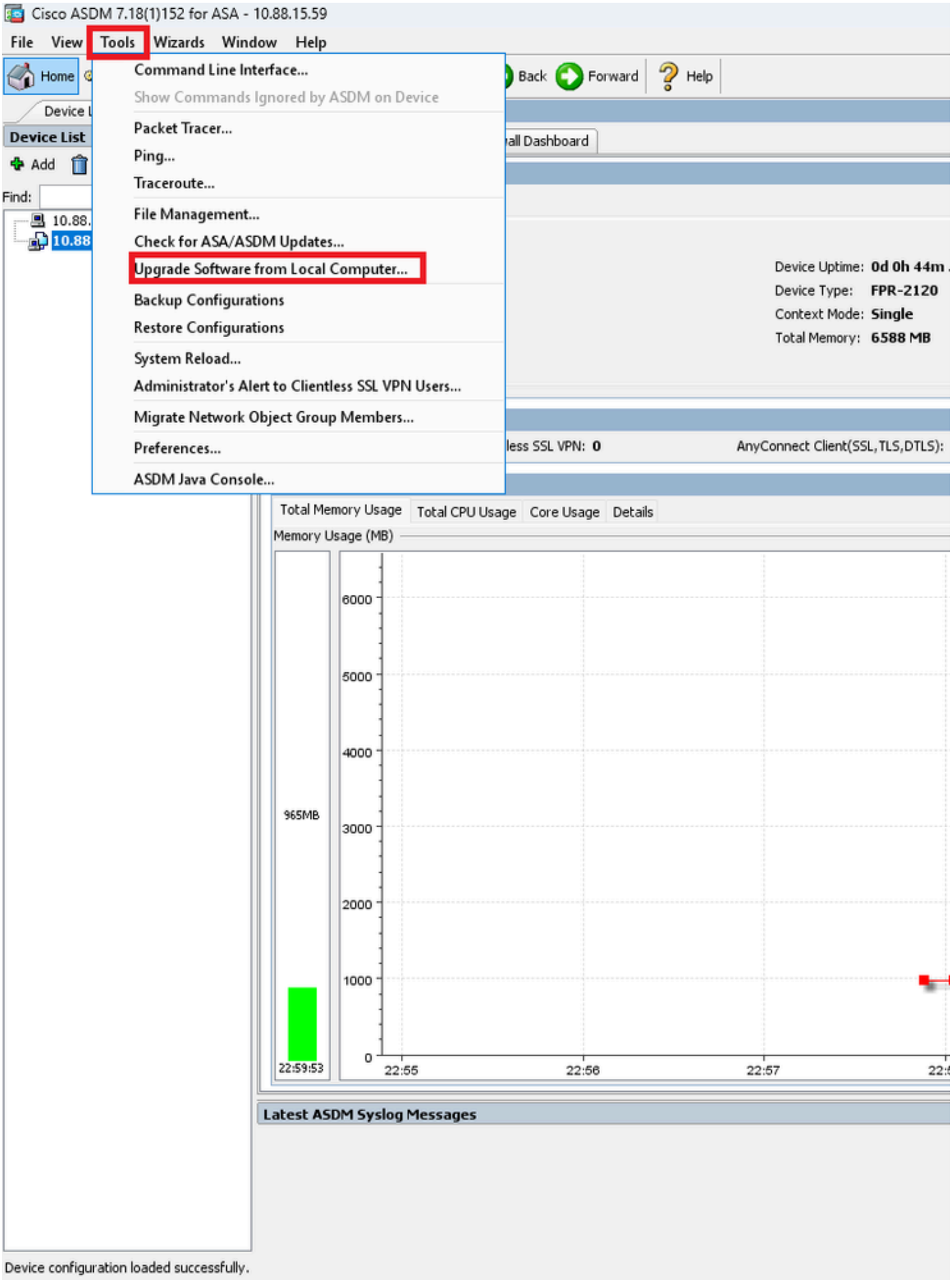
Una vez que se carga la nueva unidad en espera, la actualización se completa.

Actualización mediante ASDM

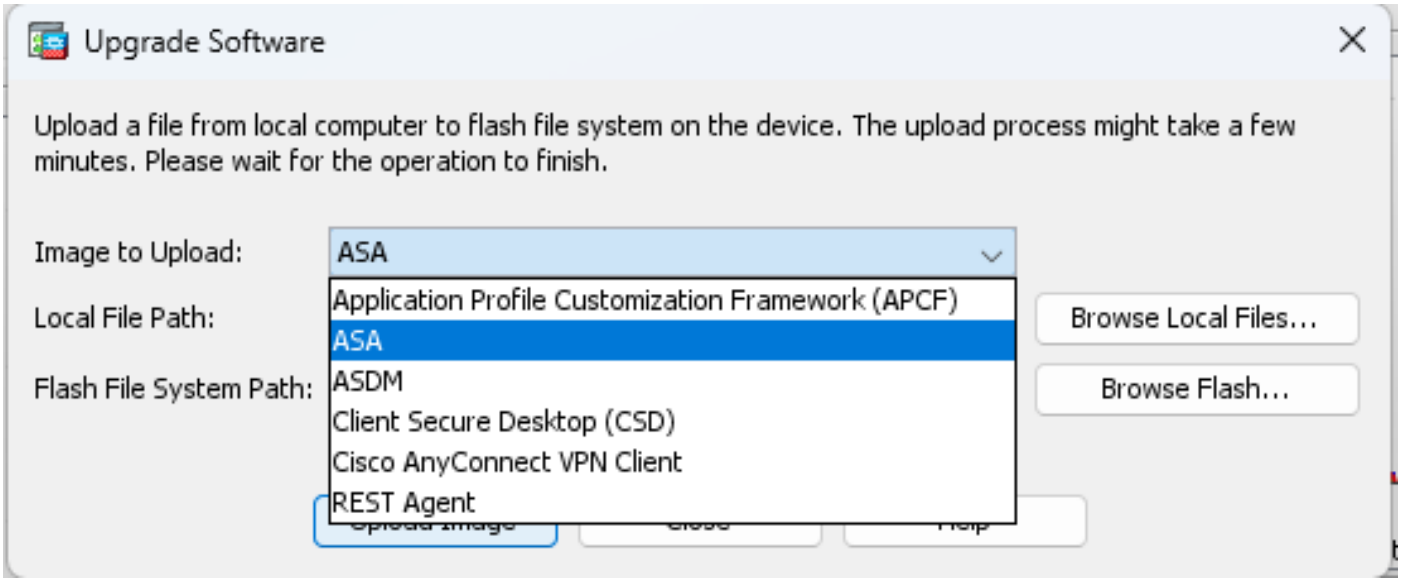
Paso 1. Conecte a la unidad secundaria con ASDM.



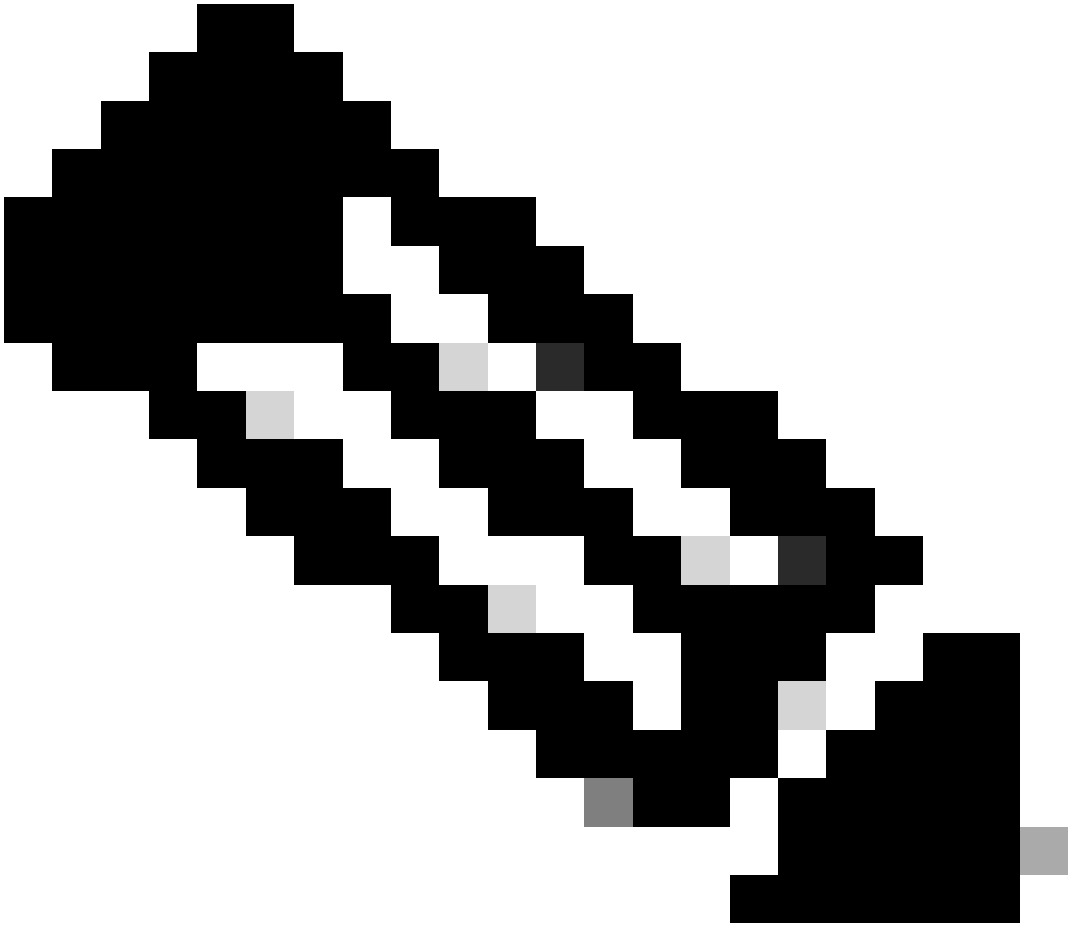
Paso 2. Vaya a Tools > Upgrade Software from Local Computer.



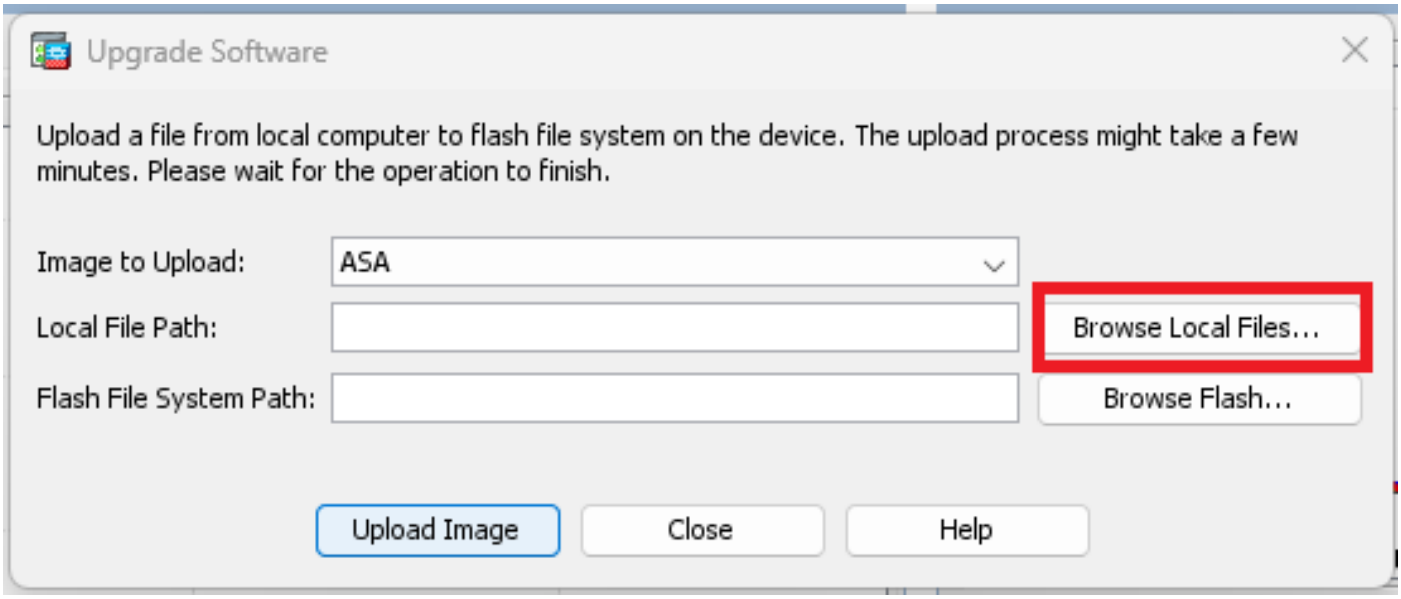
Paso 3. Seleccione ASA en la lista desplegable.



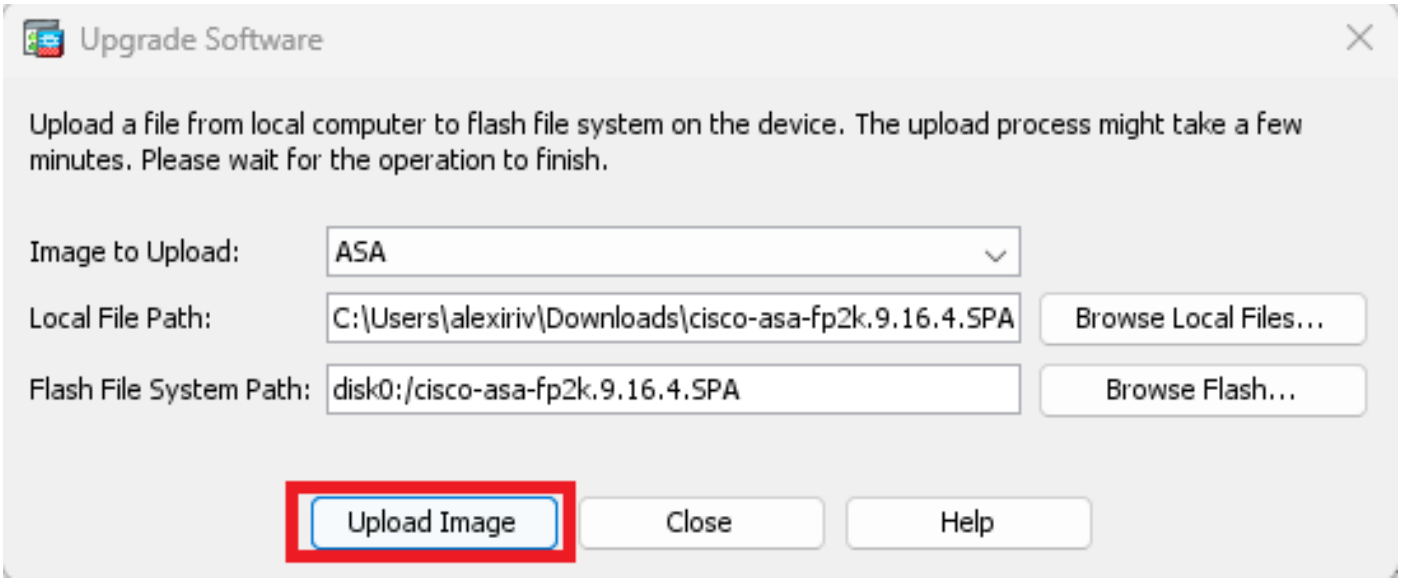
Paso 4. En la ventana Upgrade Software, haga clic en **Browse Local Files** para cargar la imagen del software en la unidad secundaria.



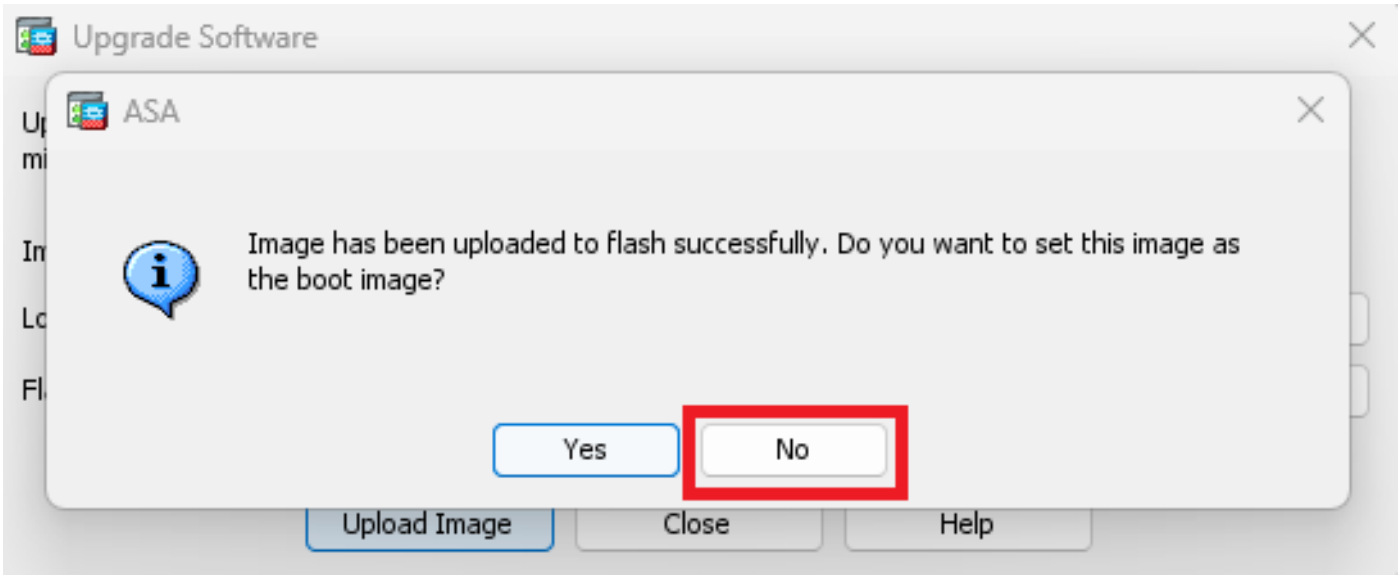
Nota: De forma predeterminada, la **ruta del sistema de archivos Flash** es disk0; para cambiarla, haga clic en **Browse Flash y seleccione la nueva ruta.**



Haga clic en **Cargar imagen.**



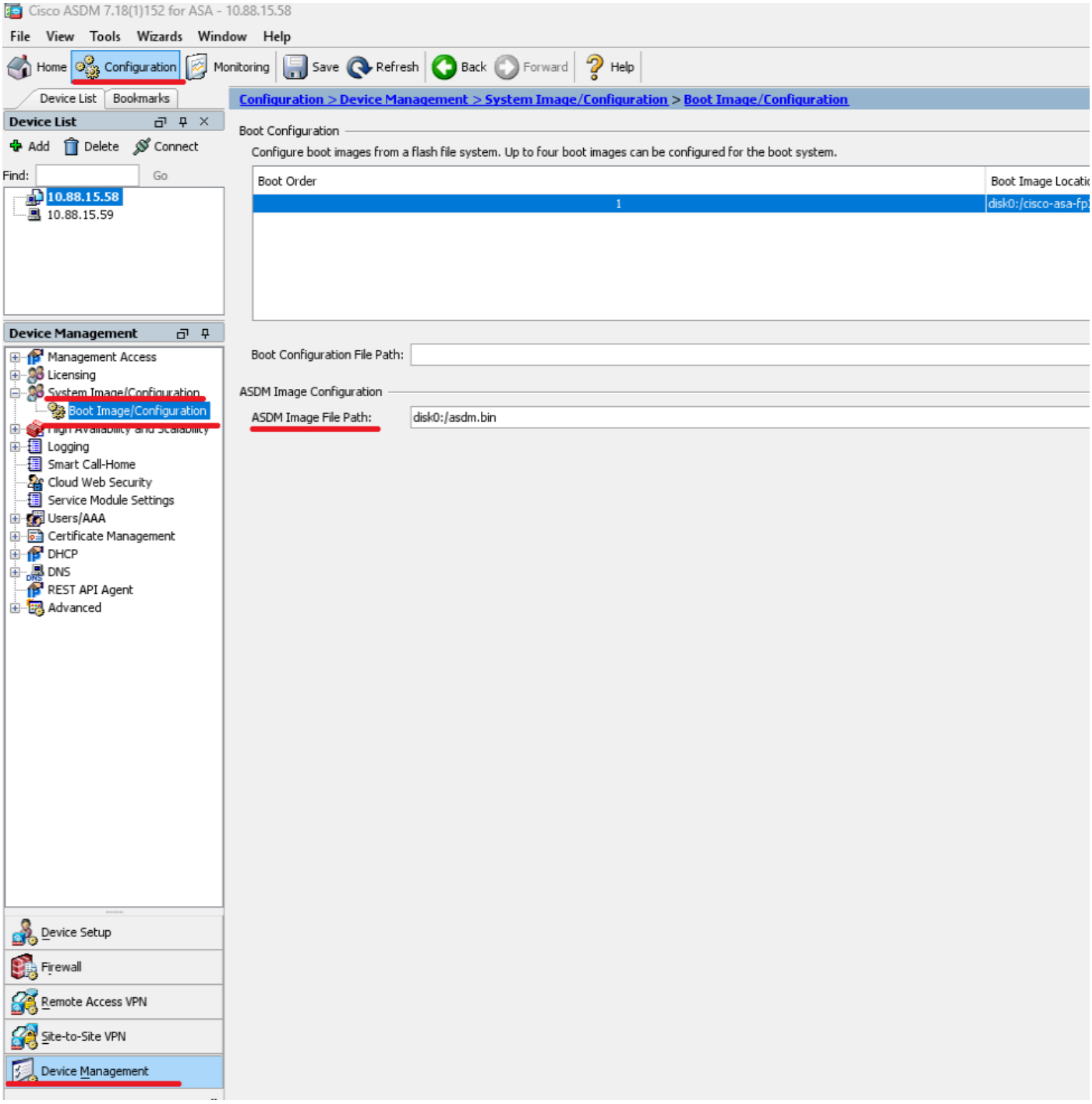
Una vez que haya terminado la carga de la imagen, haga clic en **No**.



Paso 5. Restablezca la imagen de ASDM**.**

Conéctese a la unidad primaria con ASDM y vaya a **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration**.

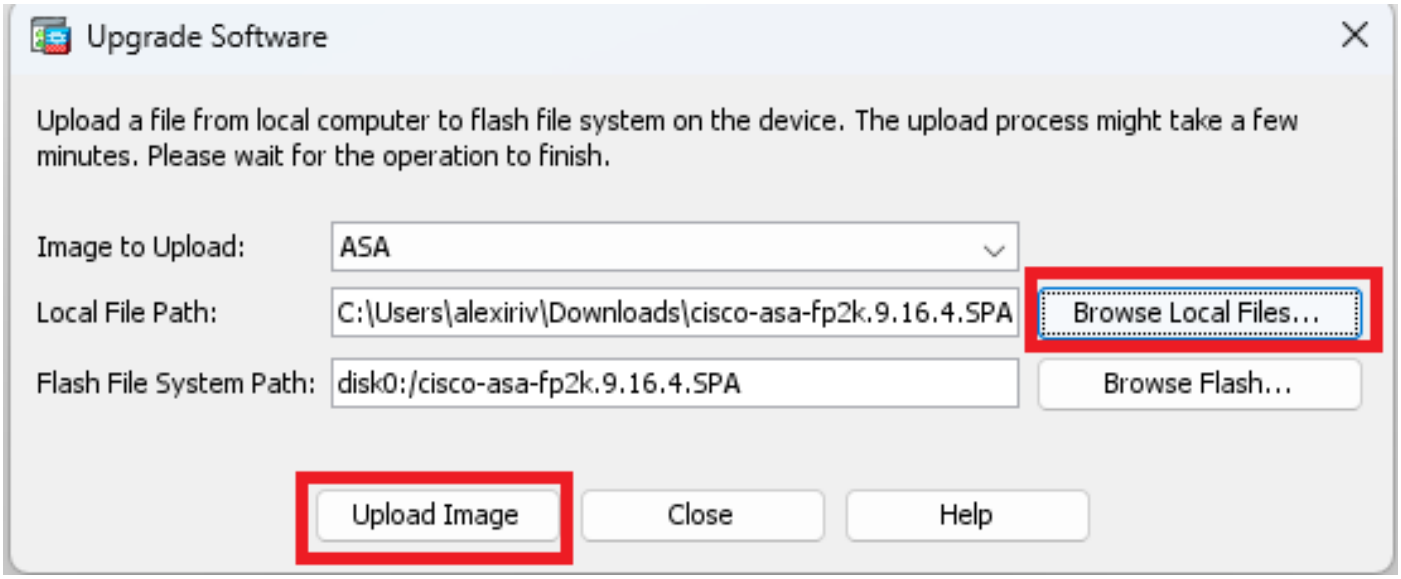
En **Ruta del Archivo de Imagen ASDM,** ingrese el valor **disk0:/asdm.bin** y **Aplicar**.



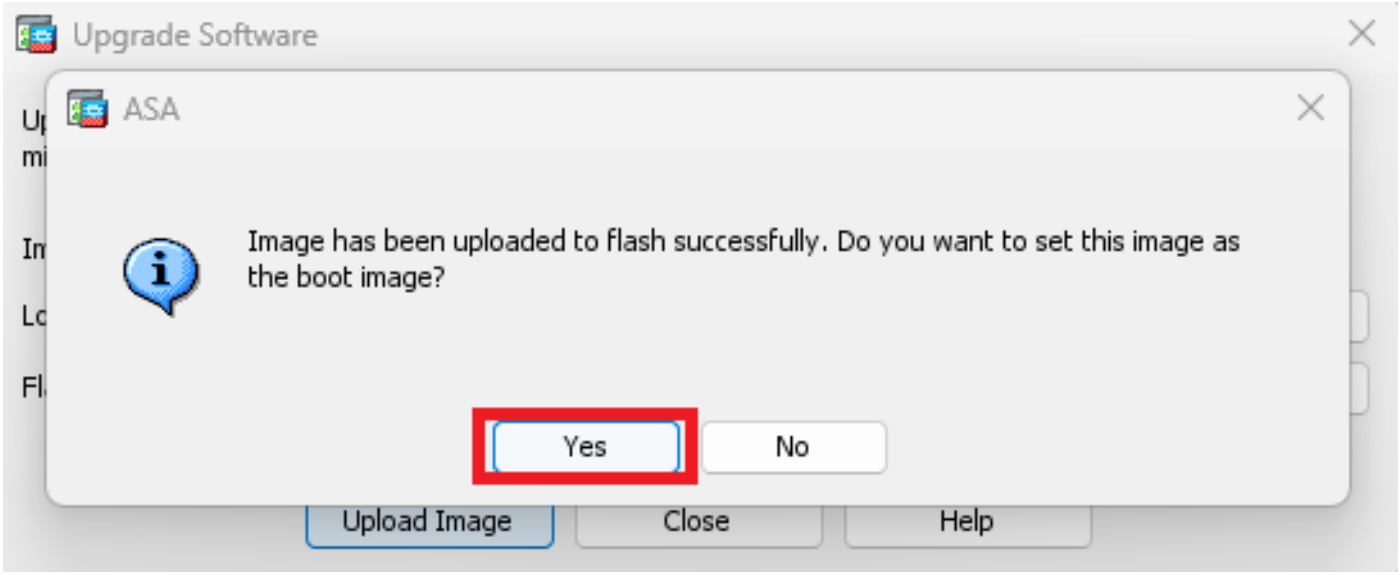
Paso 6. Cargue la imagen de software en la unidad principal.

Haga clic en **Browse Local Files** y seleccione el paquete de actualización en su dispositivo.

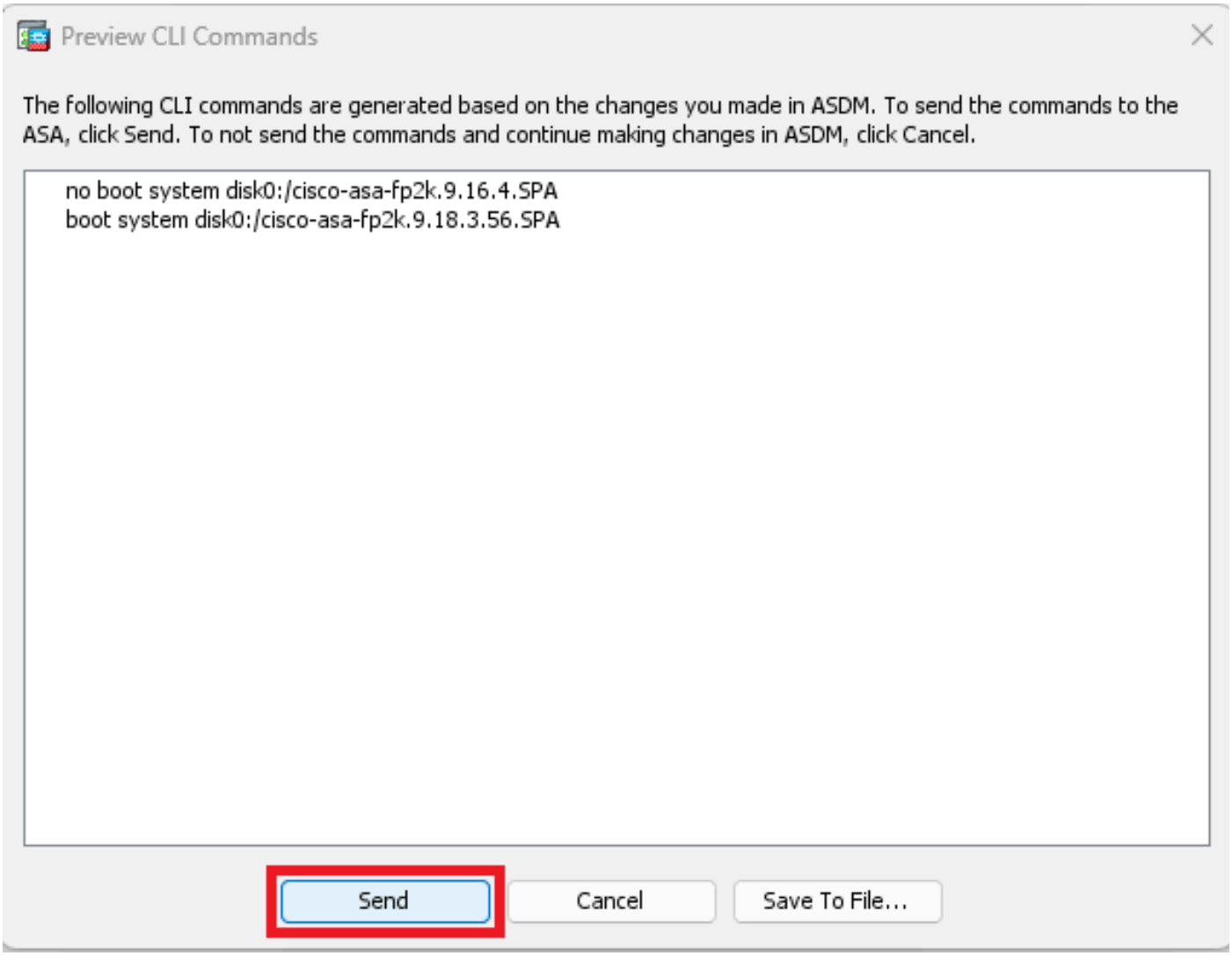
Haga clic en **Cargar imagen.**



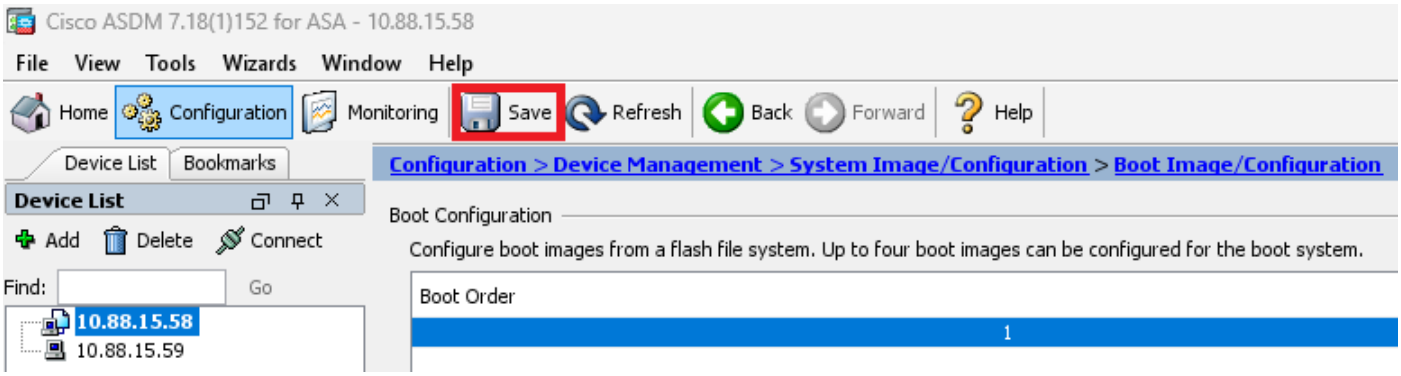
Una vez que haya terminado la carga de la imagen, haga clic en **Yes**.



En las ventanas de vista previa, haga clic en el botón **Send** para guardar la configuración.

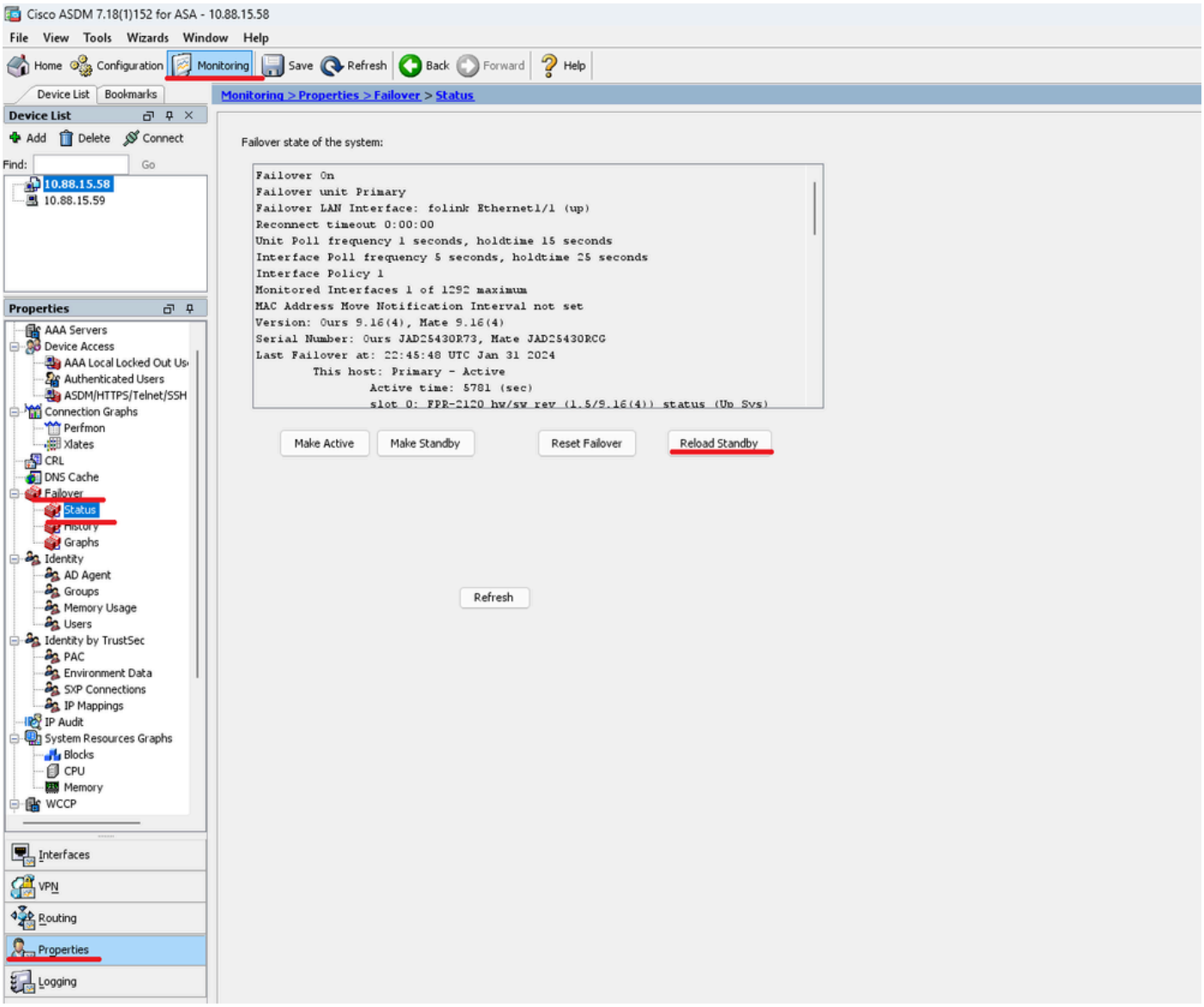


Paso 7. Haga clic en Save para guardar la configuración.



Paso 8. Vuelva a cargar la unidad secundaria para instalar la nueva versión.

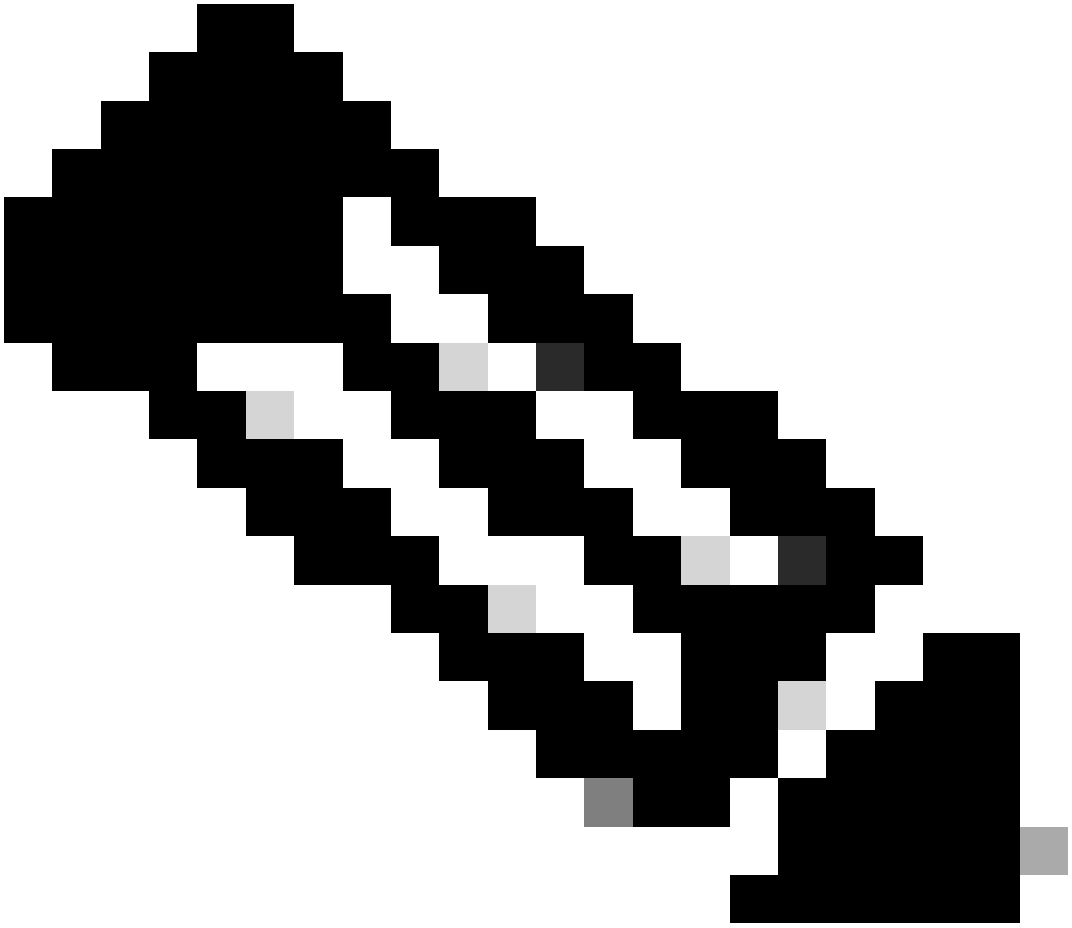
Vaya a Monitoring > **Properties** > Failover > Status **y haga clic en** Reload Standby**.**



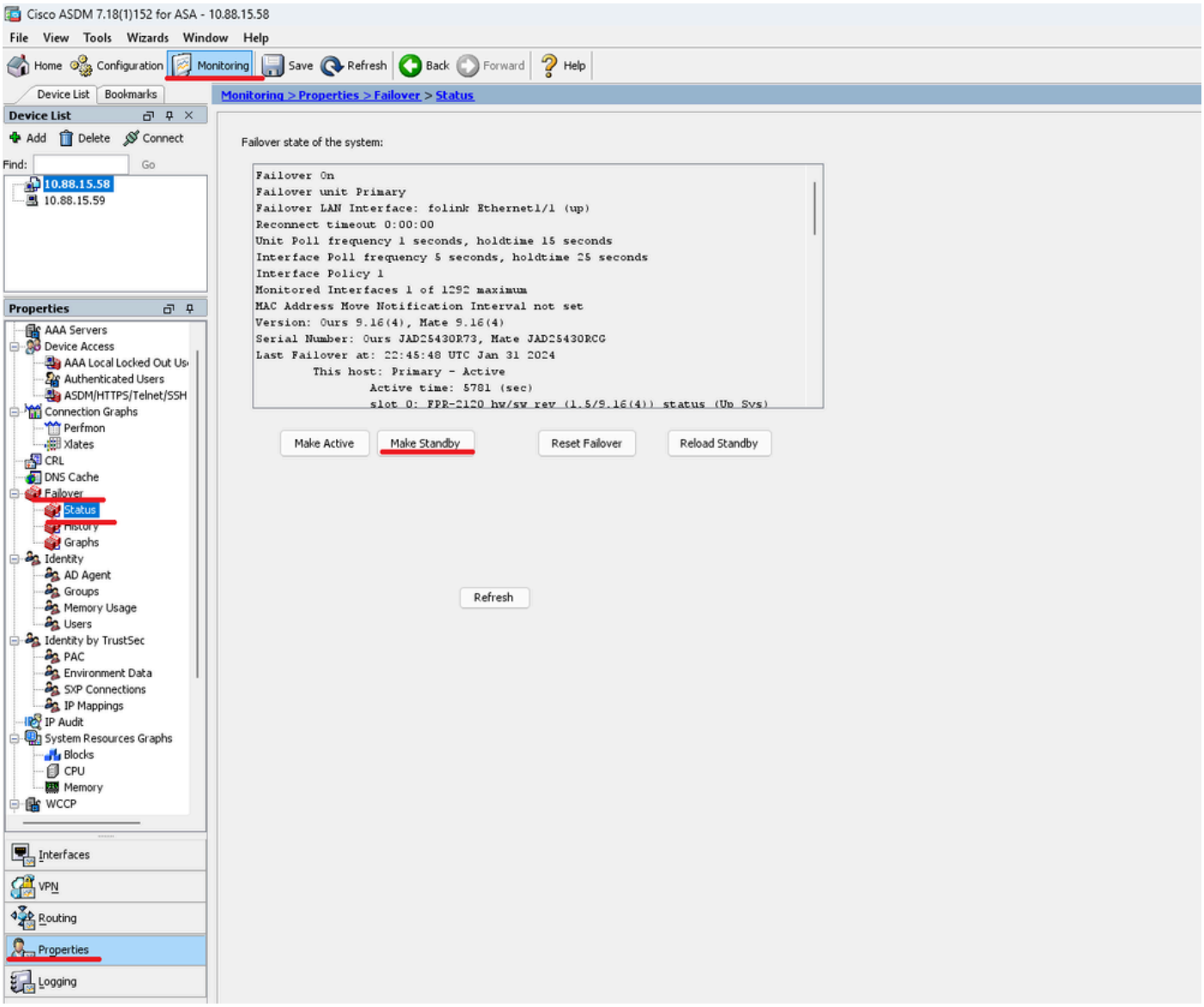
Espere hasta que se cargue la unidad en espera.

Paso 9. Una vez recargada la unidad en espera, cambie la unidad primaria del estado activo al estado en espera.

Vaya a Monitoring > **Properties** > Failover > Status **y haga clic en** Make Standby**.**

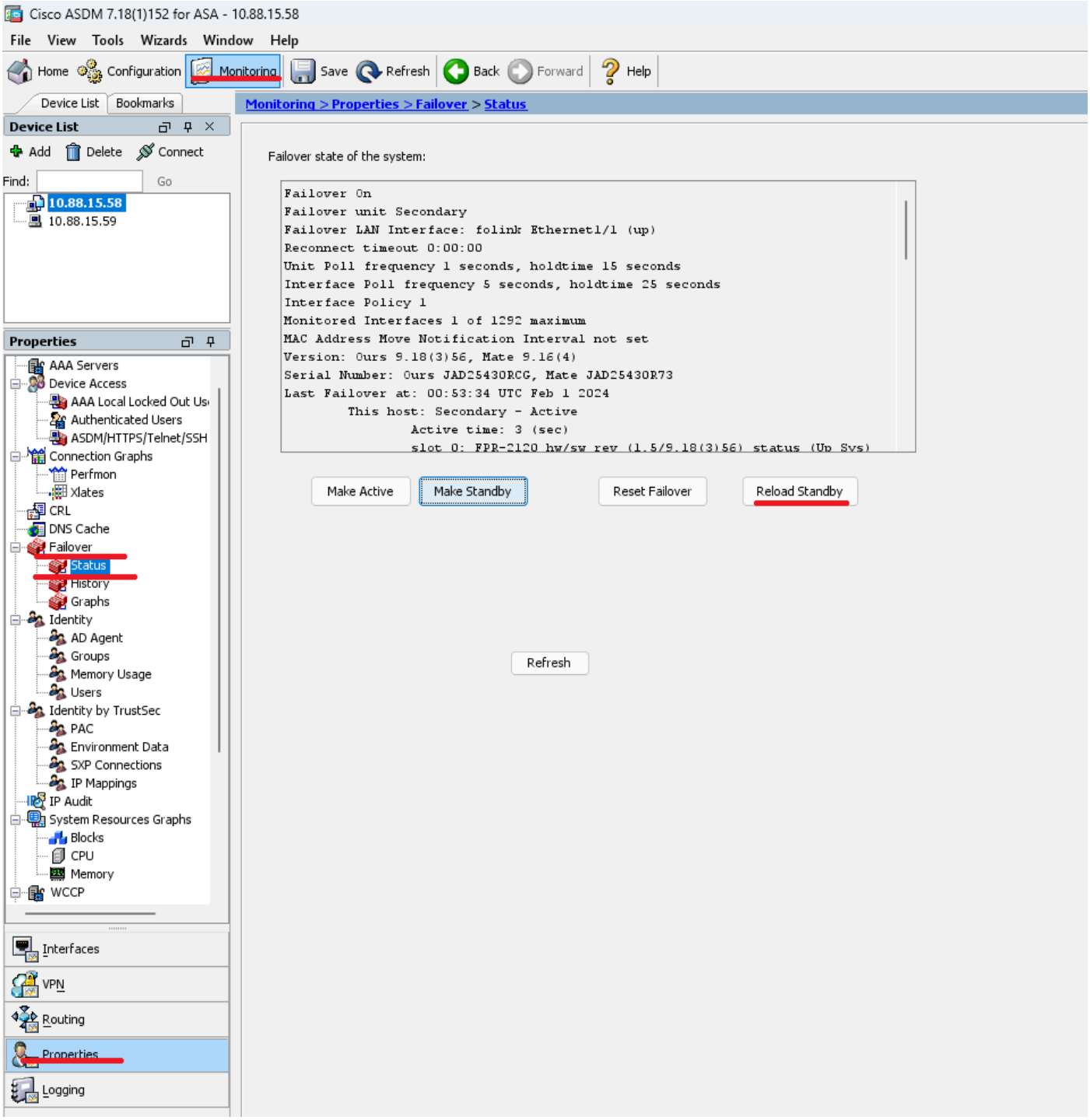


Nota: ASMD se conecta automáticamente a la nueva unidad activa.



Paso 10. Vuelva a cargar la nueva unidad en espera para instalar la nueva versión.

Vaya a Monitoring > **Properties** > Failover > Status **y haga clic en** Reload Standby**.**



Una vez que se carga la nueva unidad en espera, la actualización se completa.

Verificación

Para validar que la actualización se ha completado en ambas unidades, verifique la actualización a través de CLI y ASDM.

Mediante 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
```

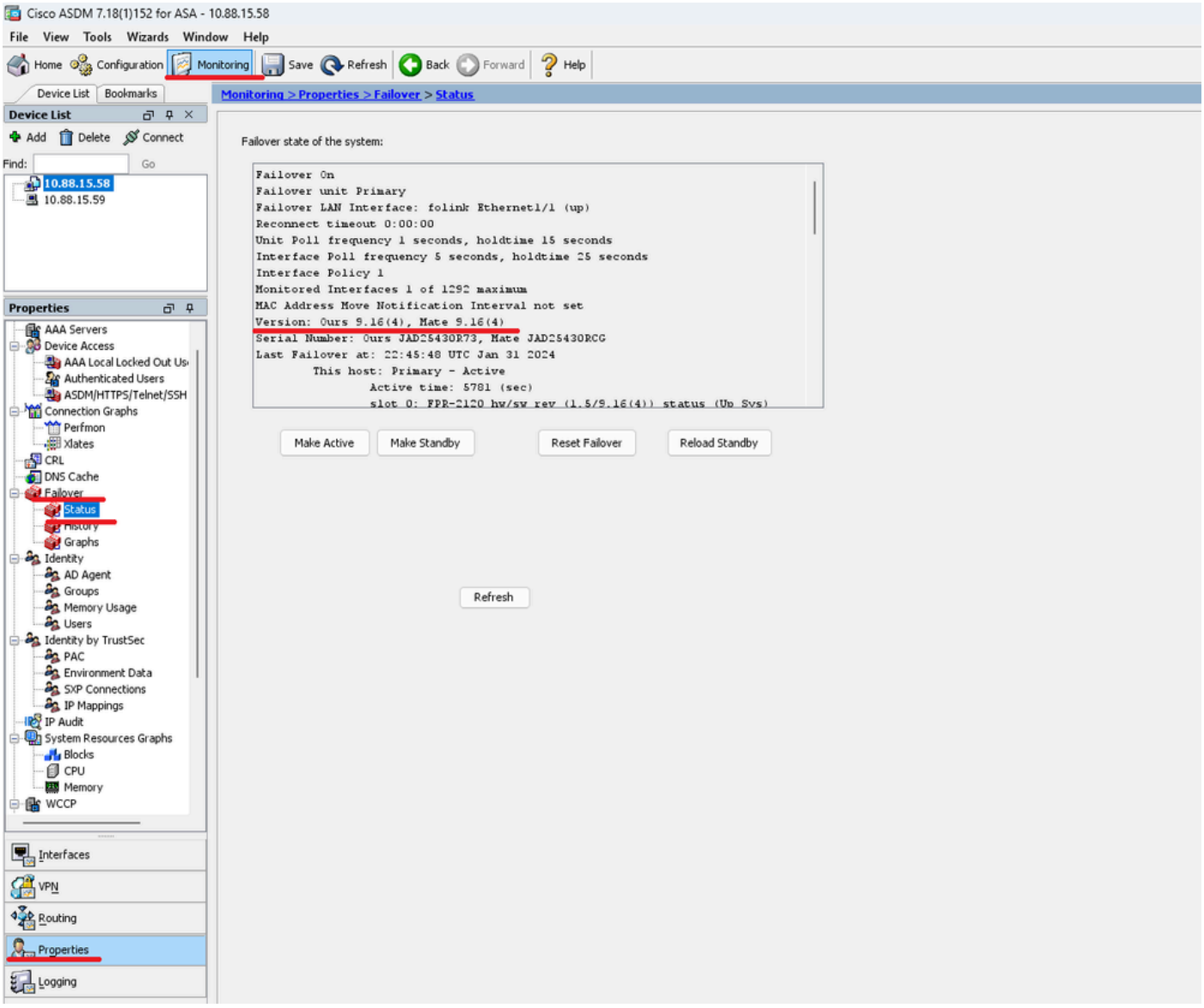
Version: Ours 9.16(4), Mate 9.16(4)

```
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
```

Vía ASDM

Vaya a **Monitoring** > **Properties** > **Failover** > **Status**, Puede ver la versión de ASA para ambos dispositivos.



Información Relacionada

- Compatibilidad con Cisco Secure Firewall ASA
- Guía de actualización de Cisco Secure Firewall ASA

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).