Aggiornamento della coppia di failover attivo/standby ASA per il firewall protetto

Sommario

Introduzione

In questo documento viene descritto come aggiornare ASA per le distribuzioni di failover per Secure Firewall 1000, 2100 in modalità Appliance e Secure Firewall 3100/4200.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Firewall Threat Defense.
- Configurazione di Cisco Adaptive Security Appliance (ASA).

Componenti usati

Le informazioni fornite in questo documento si basano sulle versioni software:

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

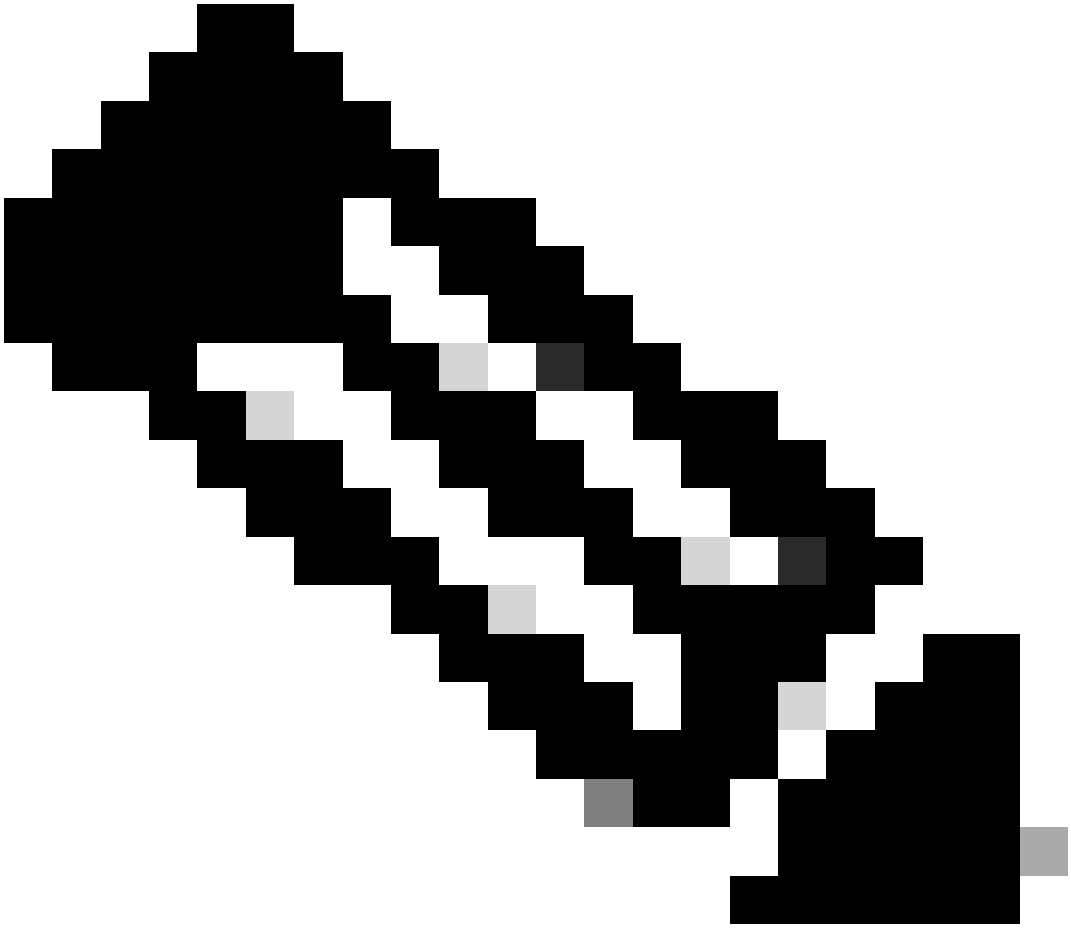
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Verifica dei prerequisiti

Passaggio 1. Eseguire il comando show fax mode per verificare che il dispositivo sia in modalità accessorio

---



> Nota: per Secure Firewall 21XX versione 9.13 e precedenti, supporta solo la modalità Piattaforma. Nella versione 9.14 e successive, la modalità accessorio è quella predefinita.

<#root>

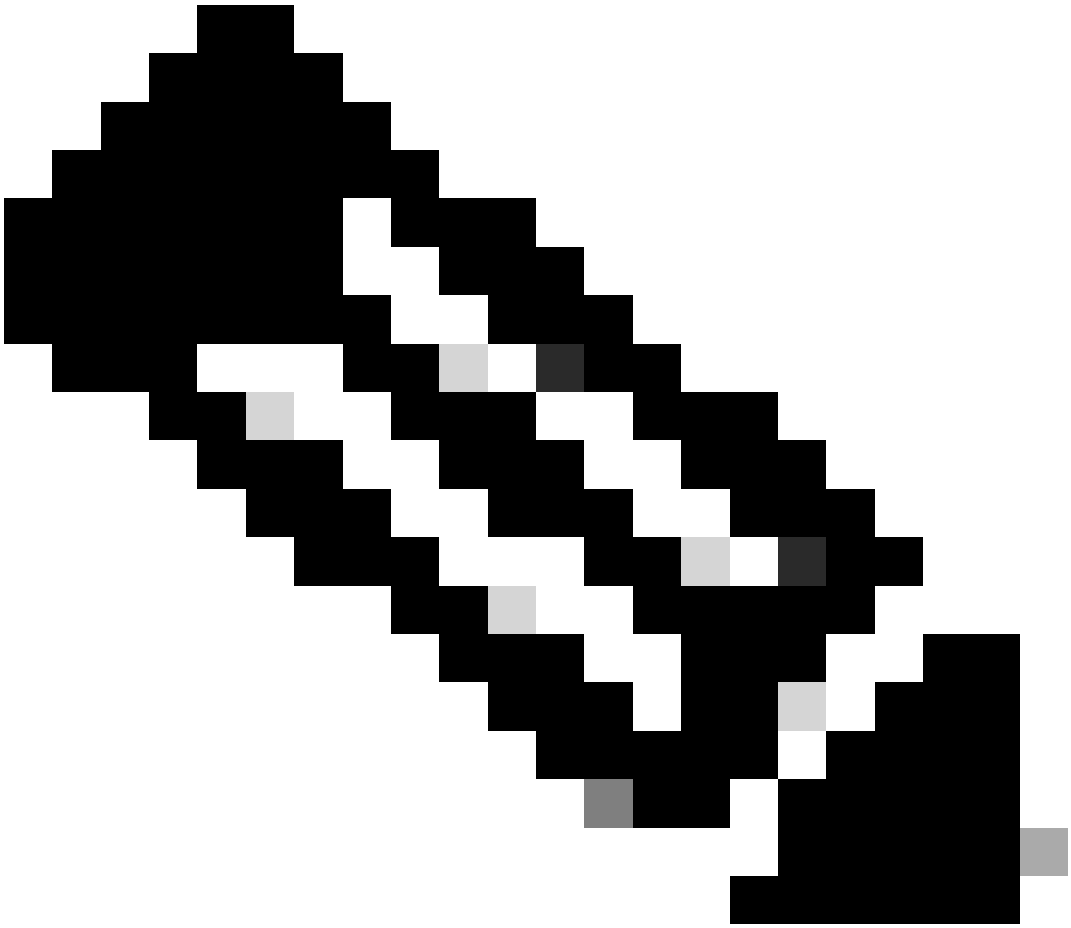
```
ciscoasa#

show fxos mode


Mode is currently set to appliance
```

Passaggio 2. Verificare la compatibilità.

Consultare il documento sulla compatibilità di Cisco Secure Firewall ASA per verificare la compatibilità tra la piattaforma hardware FTD e il software Secure Firewall ASA. Fare riferimento a

Compatibilità ASA Cisco Secure Firewall

Passaggio 3. Scaricare il pacchetto di aggiornamento da Cisco Software Central.



Nota: per Secure Firewall 1000/2100 e Secure Firewall 3100/4200, non è possibile installare ASA o FXOS separatamente; entrambe le immagini fanno parte di un pacchetto.

Consultare il titolo collegato per conoscere la versione di ASA e FXOS che fanno parte del pacchetto. Vedere versioni Secure Firewall 1000/2100 e 3100/4200 ASA e FXOS Bundle .

Aggiornamento tramite CLI

Passaggio 1. Reimpostare l'immagine ASDM.

Connettersi all'unità primaria in modalità di configurazione globale ed eseguire i comandi seguenti:

<#root>

ciscoasa(config)#

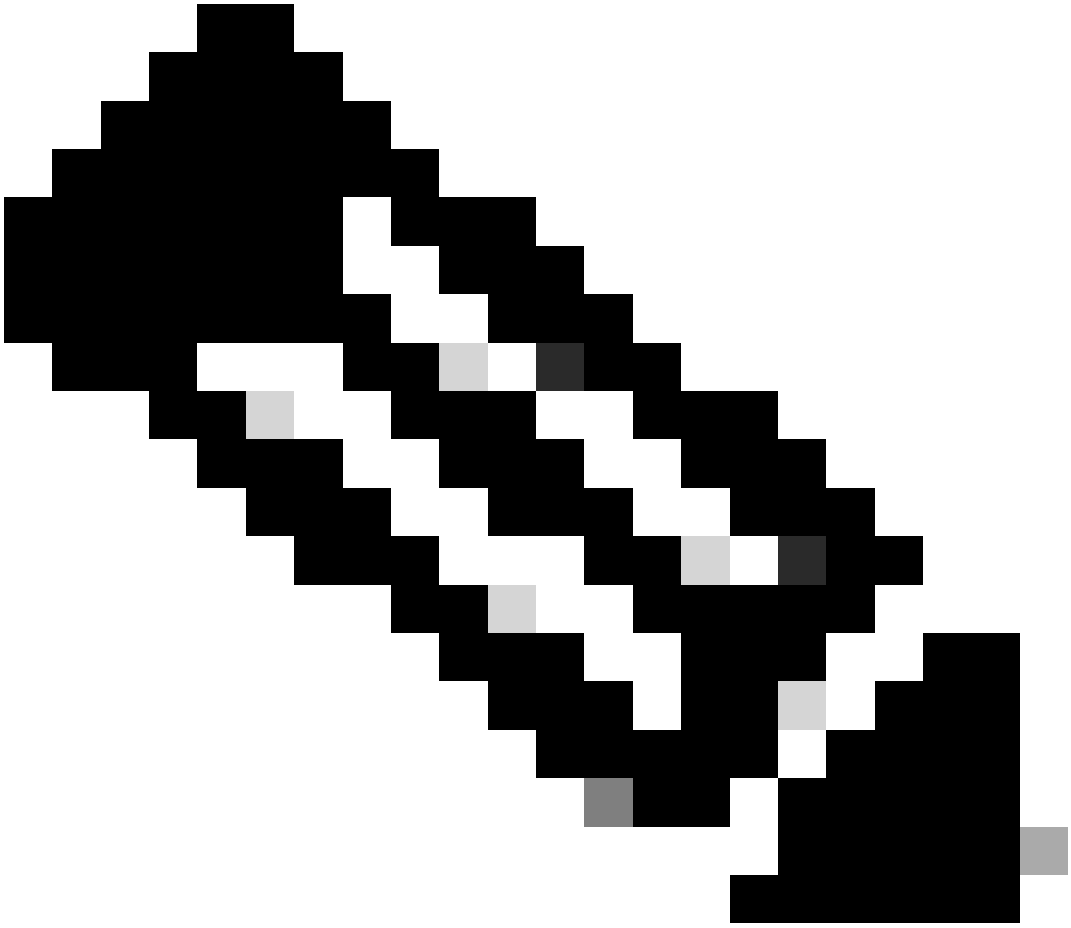
asdm image disk0:/asdm.bin

```
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)
```

Passaggio 2. Caricare l'immagine software sull'unità principale.



Nota: in questo documento si utilizza un server FTP, ma è possibile utilizzare TFTP, HTTP o altri tipi di server.

<#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)

Passaggio 3. Caricare l'immagine software sull'unità secondaria.

Eseguire il comando sull'unità primaria.

<#root>

ciscoasa#

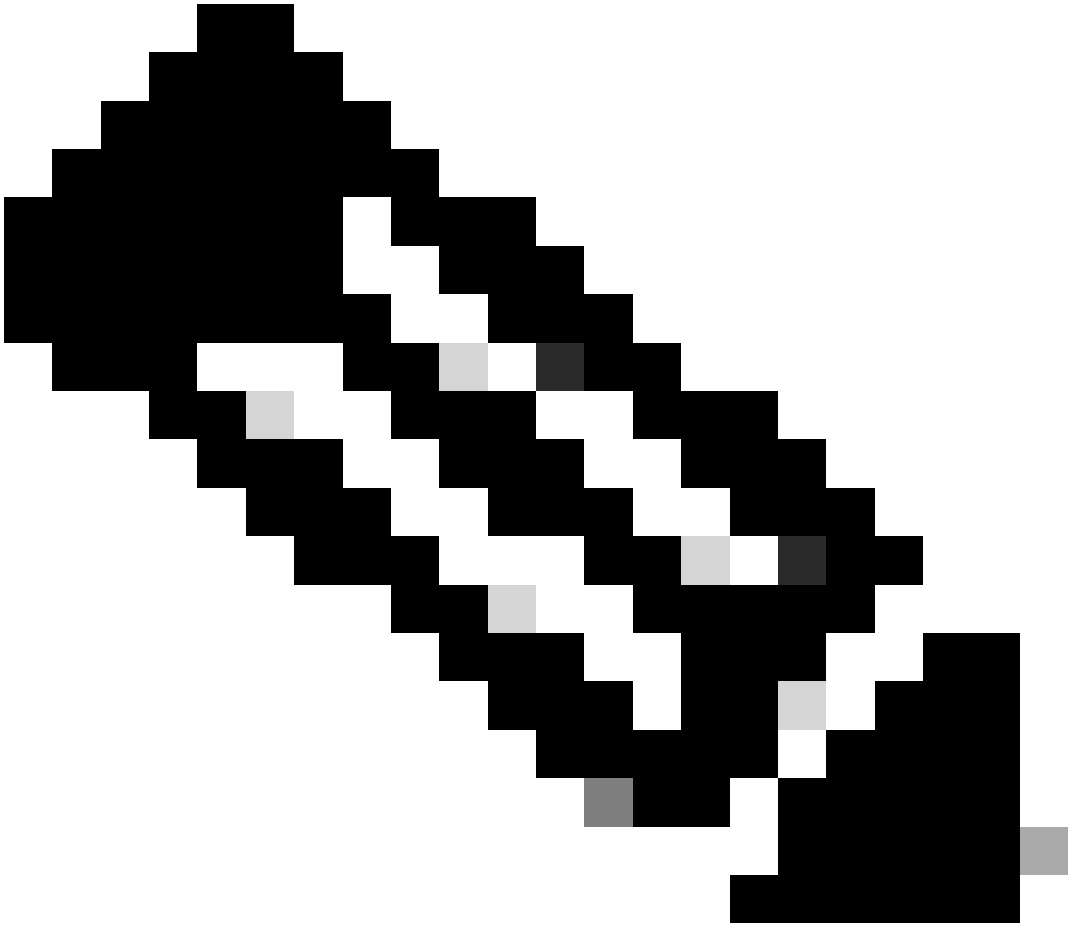
failover exec mate copy /noconfirm ftp://calo:calo@10.88.7.12/cisco-asa-fp2k.9.16.4.SPA disk0:/cisco-asa

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)

Passaggio 4. Verificare se l'immagine di avvio corrente è stata configurata con il **show running-config boot system** comando.



Nota: è possibile che non sia stato configurato un sistema di avvio.

<#root>

ciscoasa(config)#

show running-config boot system

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

Passaggio 5 (facoltativo). Se è stata configurata un'immagine d'avvio, è necessario rimuoverla.

nessun disco del sistema di avvio:/asa_image_name

Esempio:

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

Passaggio 6. Selezionare l'immagine da avviare.

```
   <#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
```

Passaggio 7. Salvare la configurazione con il comando copy running-config startup-config.

Passaggio 8. Ricaricare l'unità secondaria per installare la nuova versione.

<#root>

ciscoasa(config)#

failover reload-standby

Attendere il caricamento dell'unità secondaria.

Passaggio 9. Una volta ricaricata l'unità in standby, modificare lo stato dell'unità principale da attivo a standby.

<#root>

ciscoasa#

no failover active

Passaggio 10. Ricaricare la nuova unità di standby per installare la nuova versione. È necessario collegarsi alla nuova unità attiva.

<#root>

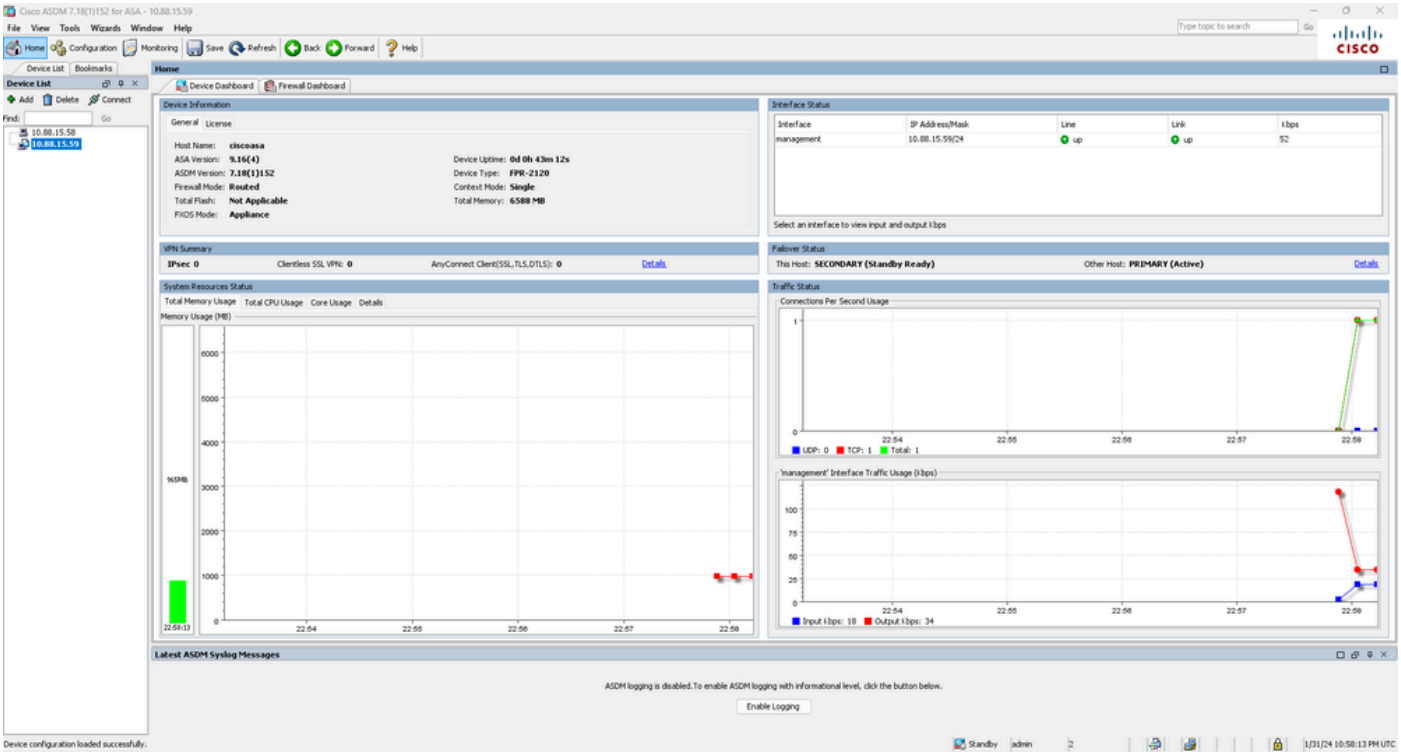
ciscoasa(config)#

```
failover reload-standby
```

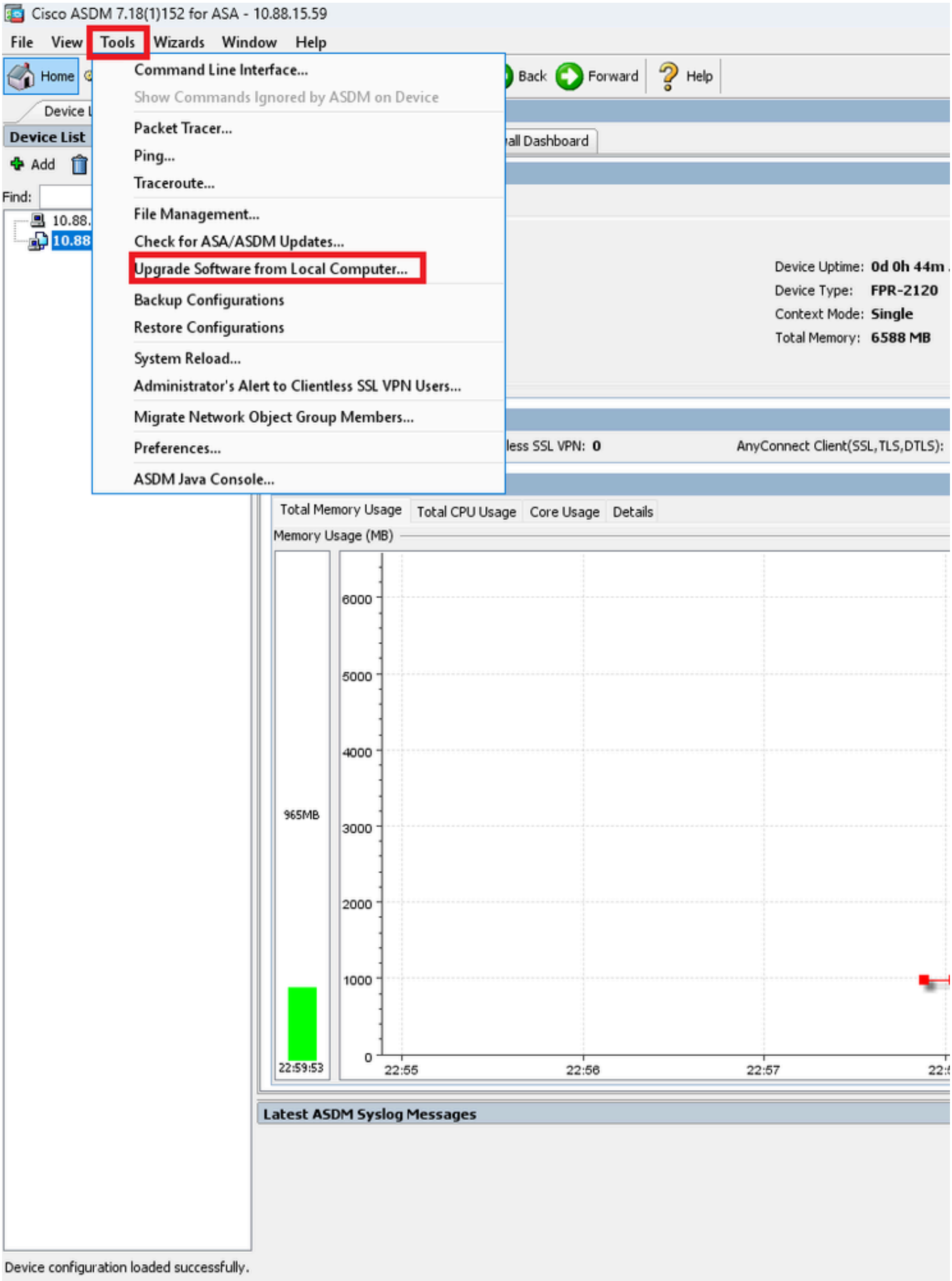
Una volta caricata la nuova unità di standby, l'aggiornamento è completo.

Aggiornamento tramite ASDM

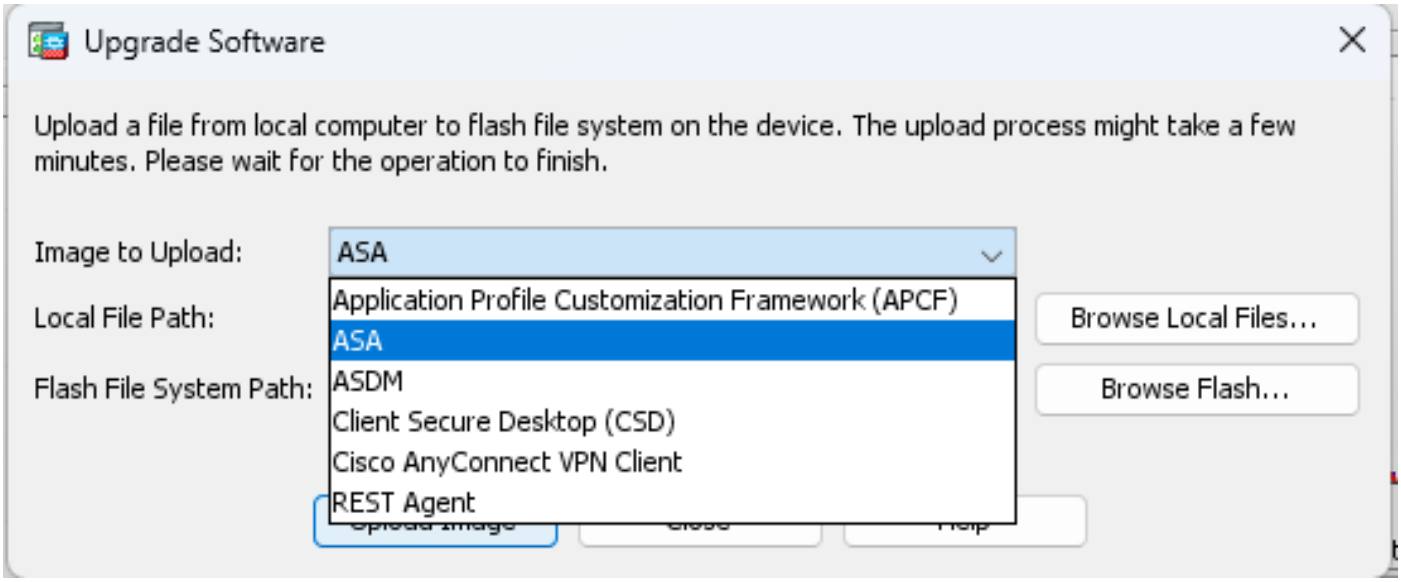
Passaggio 1. Collegare l'unità secondaria con ASDM.



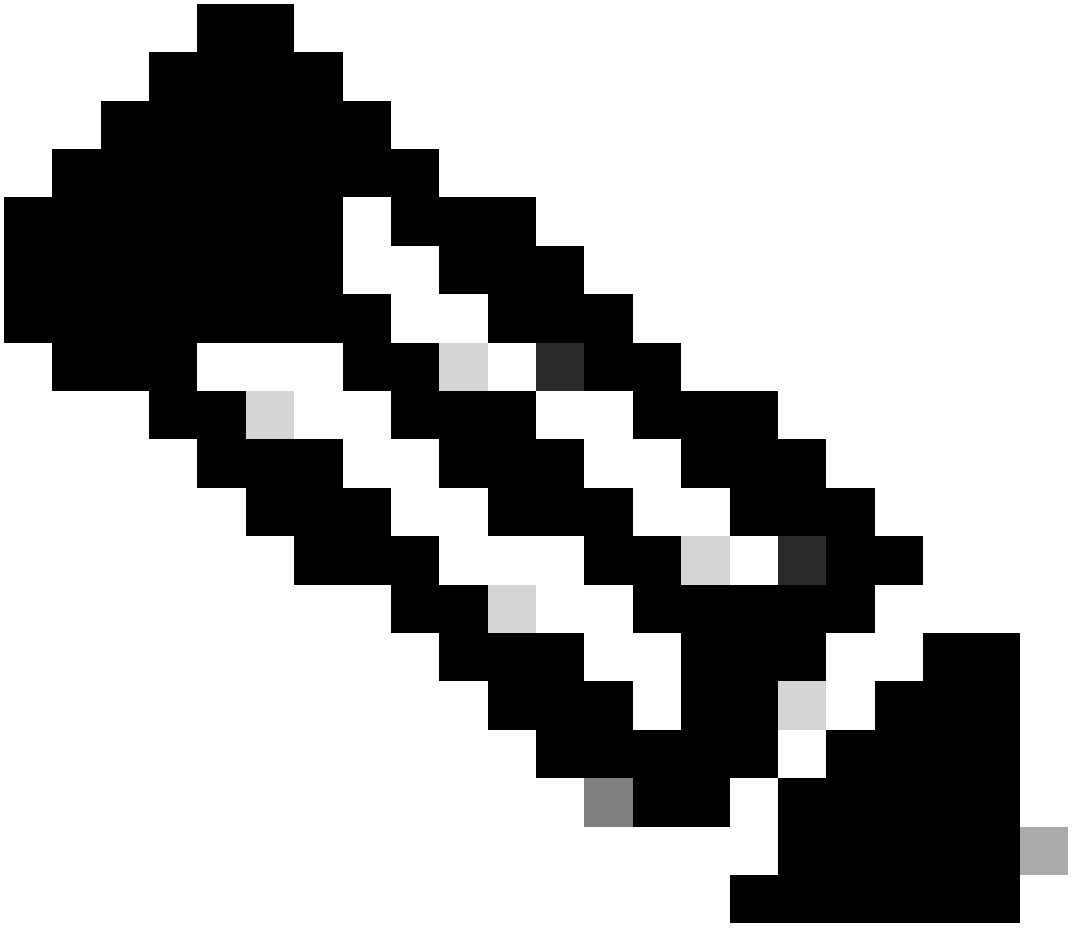
Passaggio 2. Selezionare **Strumenti > Aggiorna software dal computer locale**.



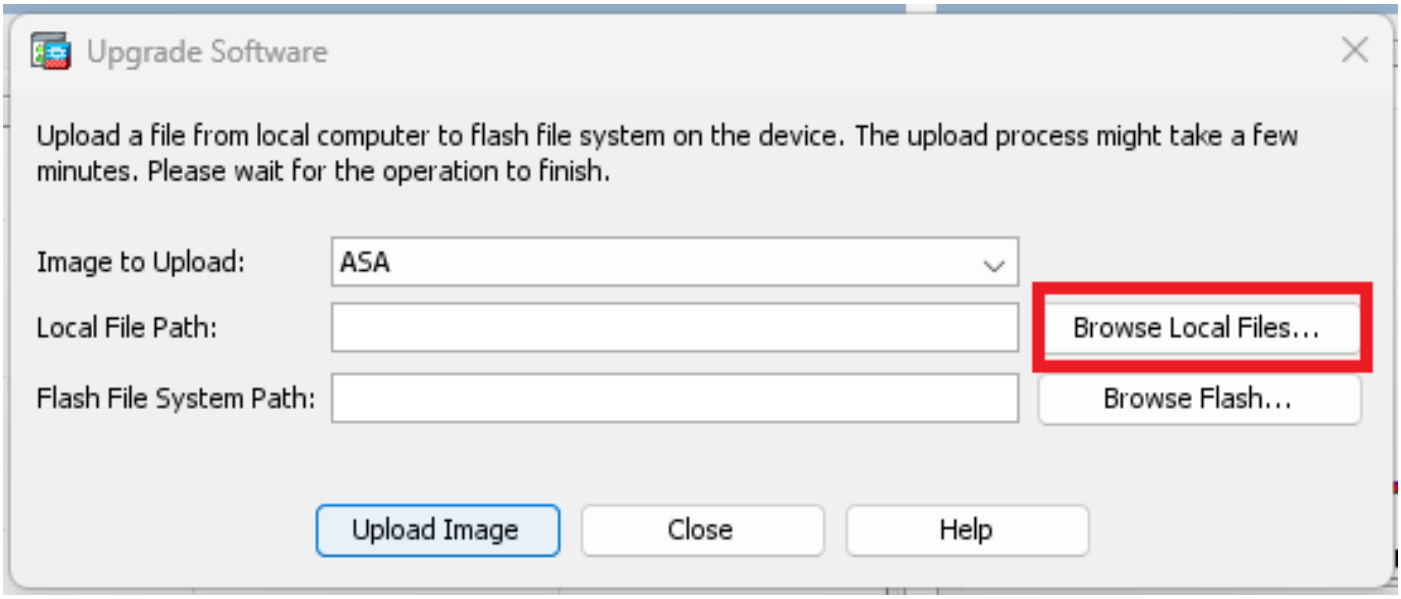
Passaggio 3. Selezionare ASA dall'elenco a discesa.



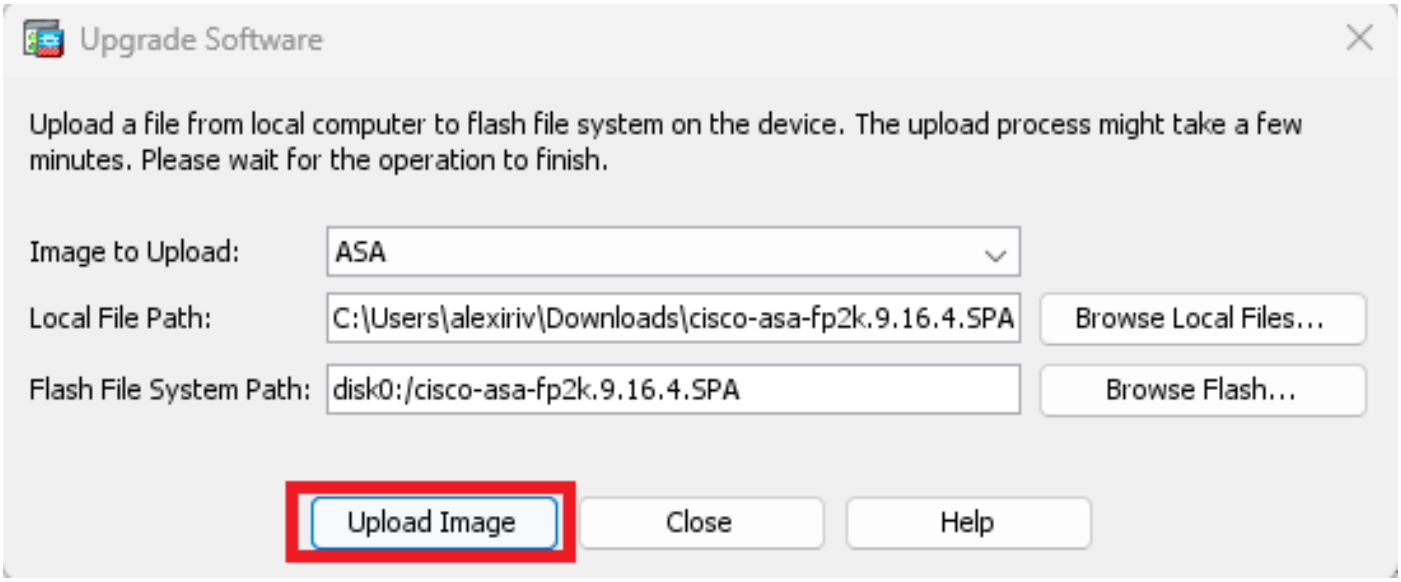
Passaggio 4. Nella finestra **Upgrade Software,** fare clic su **Browse Local Files** per caricare l'immagine software sull'unità secondaria.



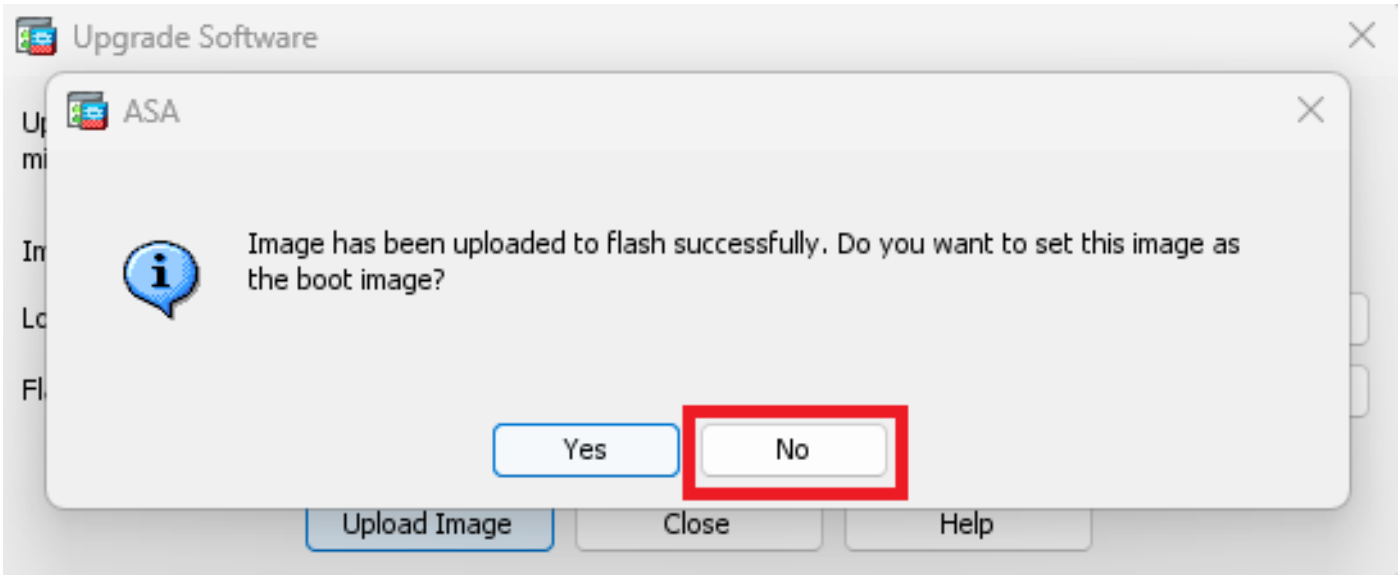
Nota: per impostazione predefinita, il **percorso del file system Flash** è disk0; per modificarlo, fare clic su **Sfoglia Flash** e selezionare il nuovo percorso.



Fare clic su **Upload Image (Carica immagine).**



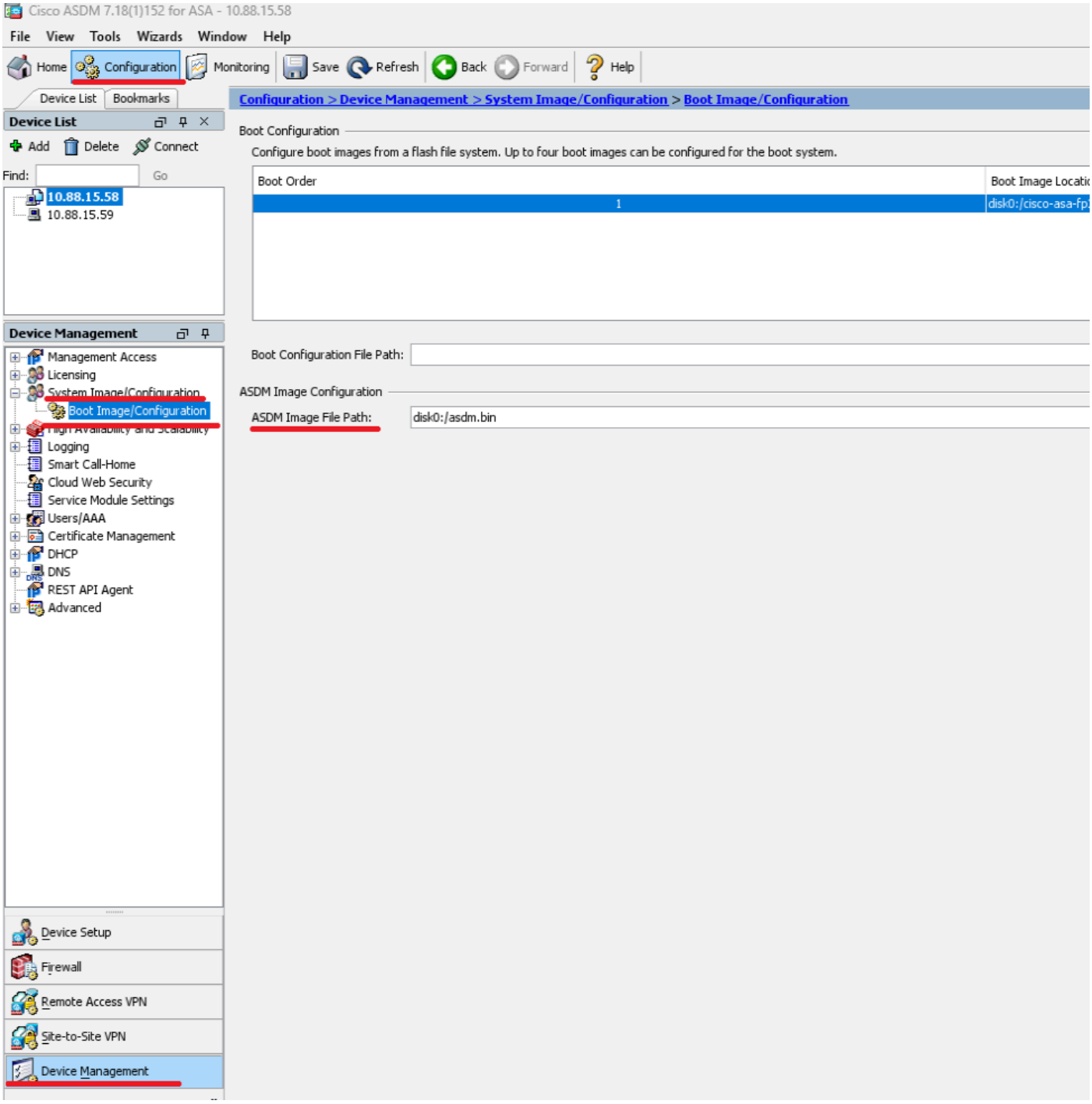
Al termine del caricamento dell'immagine, fare clic su **No**.



Passaggio 5. Reimpostare l'immagine ASDM**.**

Collegarsi all'unità principale con ASDM e selezionare **Configurazione > Gestione dispositivi > Immagine/configurazione del sistema > Immagine/configurazione di avvio**.

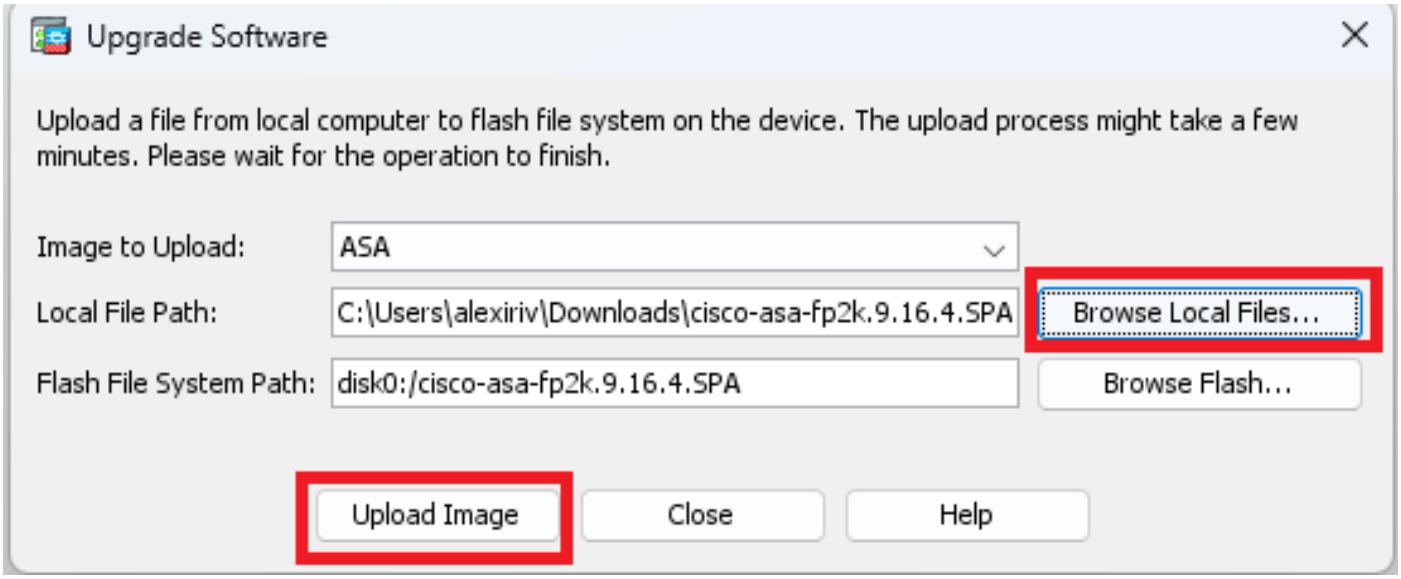
In **Percorso file immagine ASDM,** immettere il valore **disk0:/asdm.bin** e **Apply**.



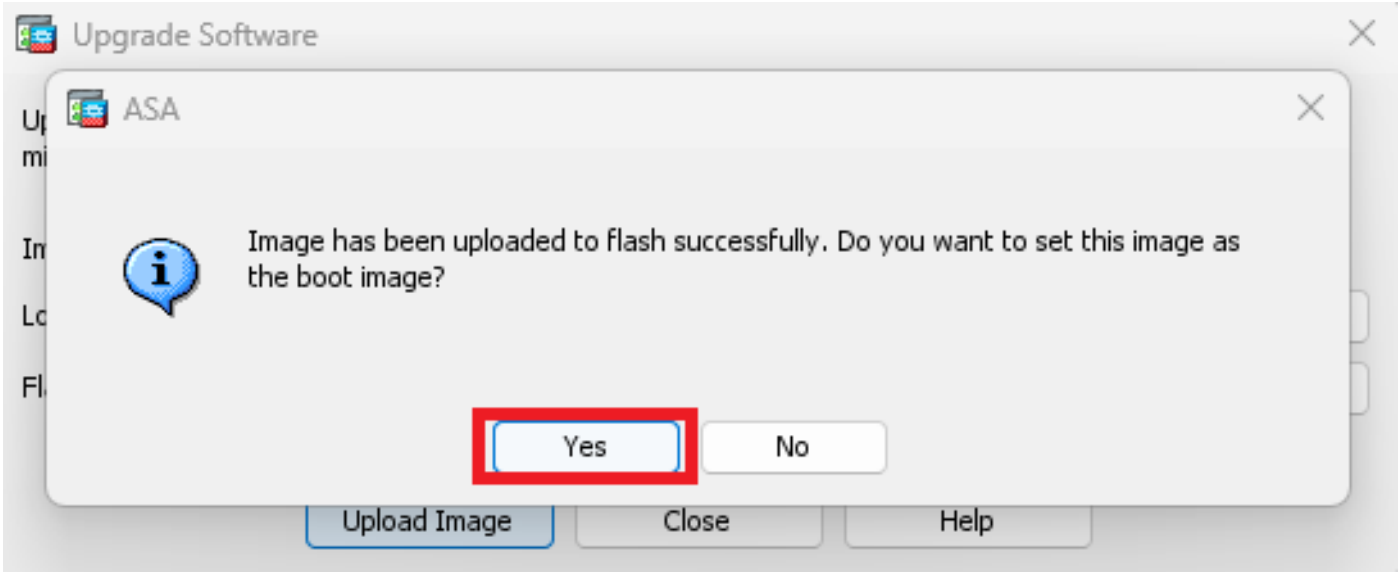
Passaggio 6. Caricare l'immagine software sull'unità principale.

Fare clic su **Sfoglia file locali** e selezionare il pacchetto di aggiornamento sul dispositivo.

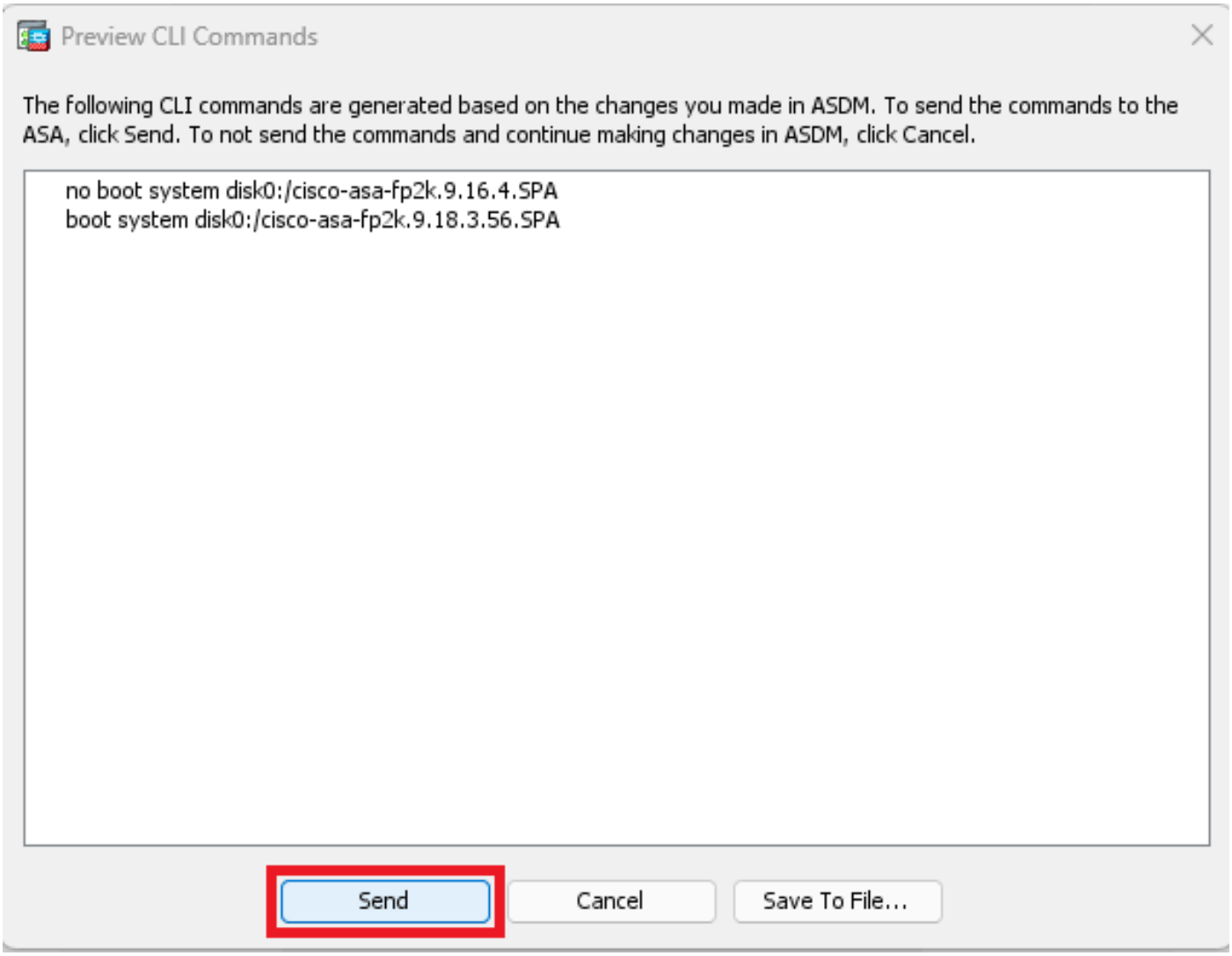
Fare clic su **Upload Image (Carica immagine).**



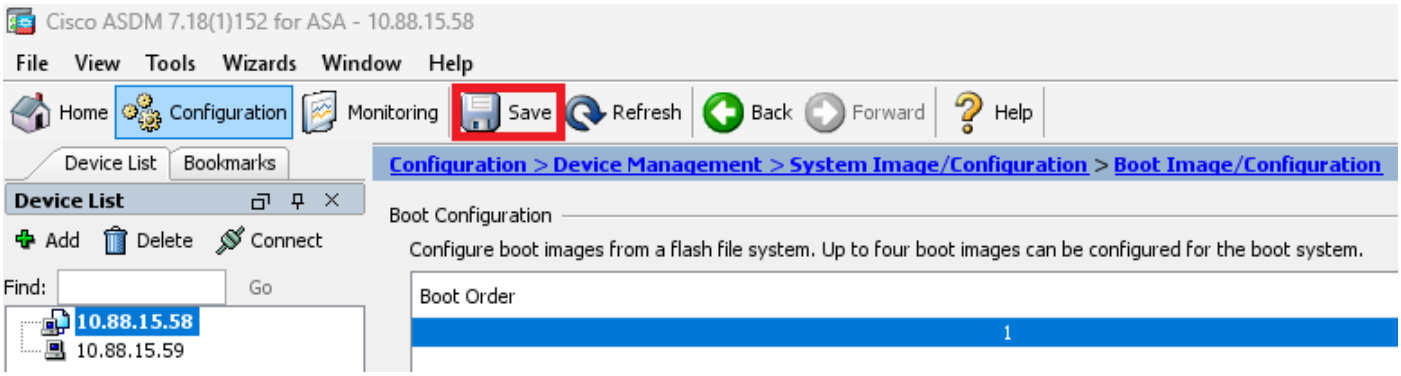
Al termine del caricamento dell'immagine, fare clic su **Yes** (Sì).



Nelle finestre di anteprima, fare clic sul pulsante **Send** per salvare la configurazione.

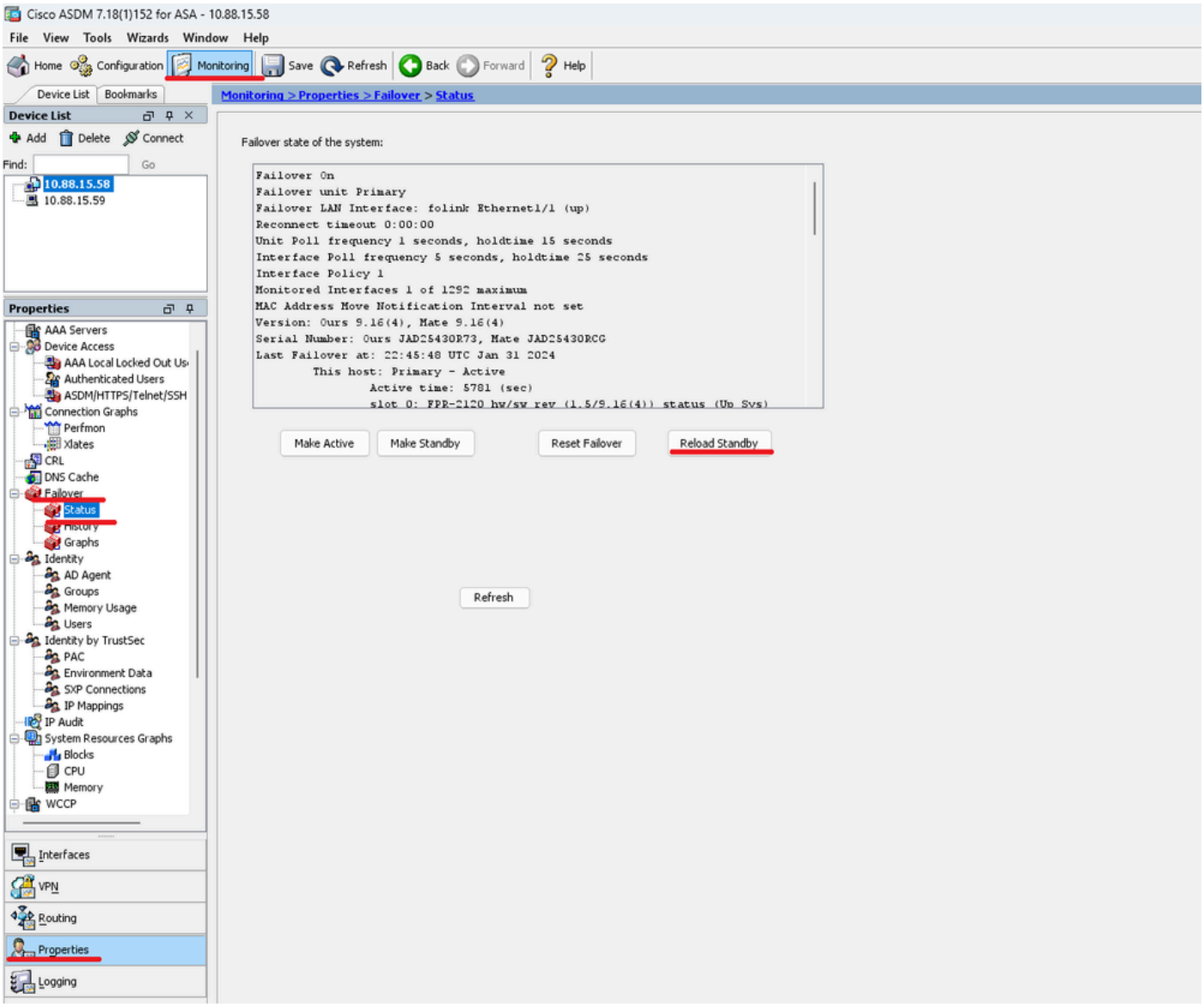


Passaggio 7. Fare clic su Save (Salva) per salvare la configurazione.



Passaggio 8. Ricaricare l'unità secondaria per installare la nuova versione.

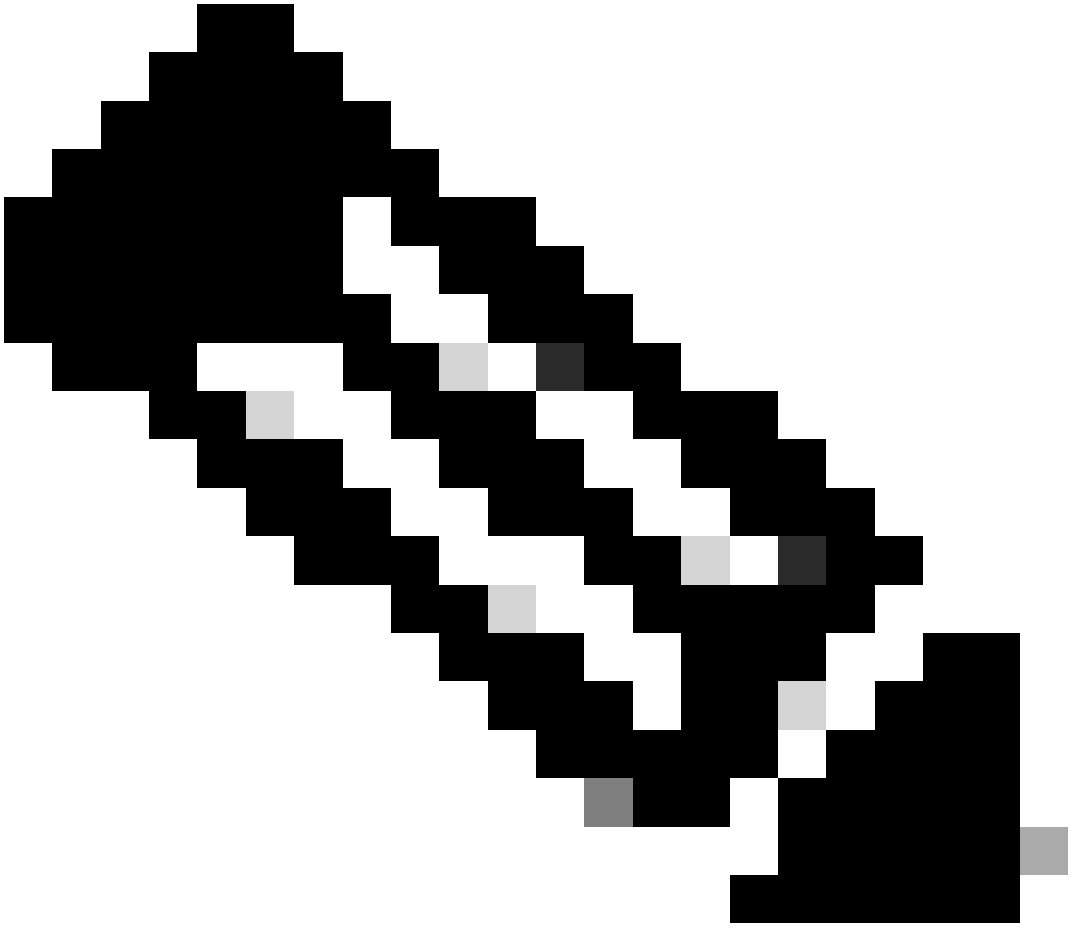
Selezionare Monitoraggio **> Proprietà > Failover > Stato** e fare clic su **Ricarica standby**.



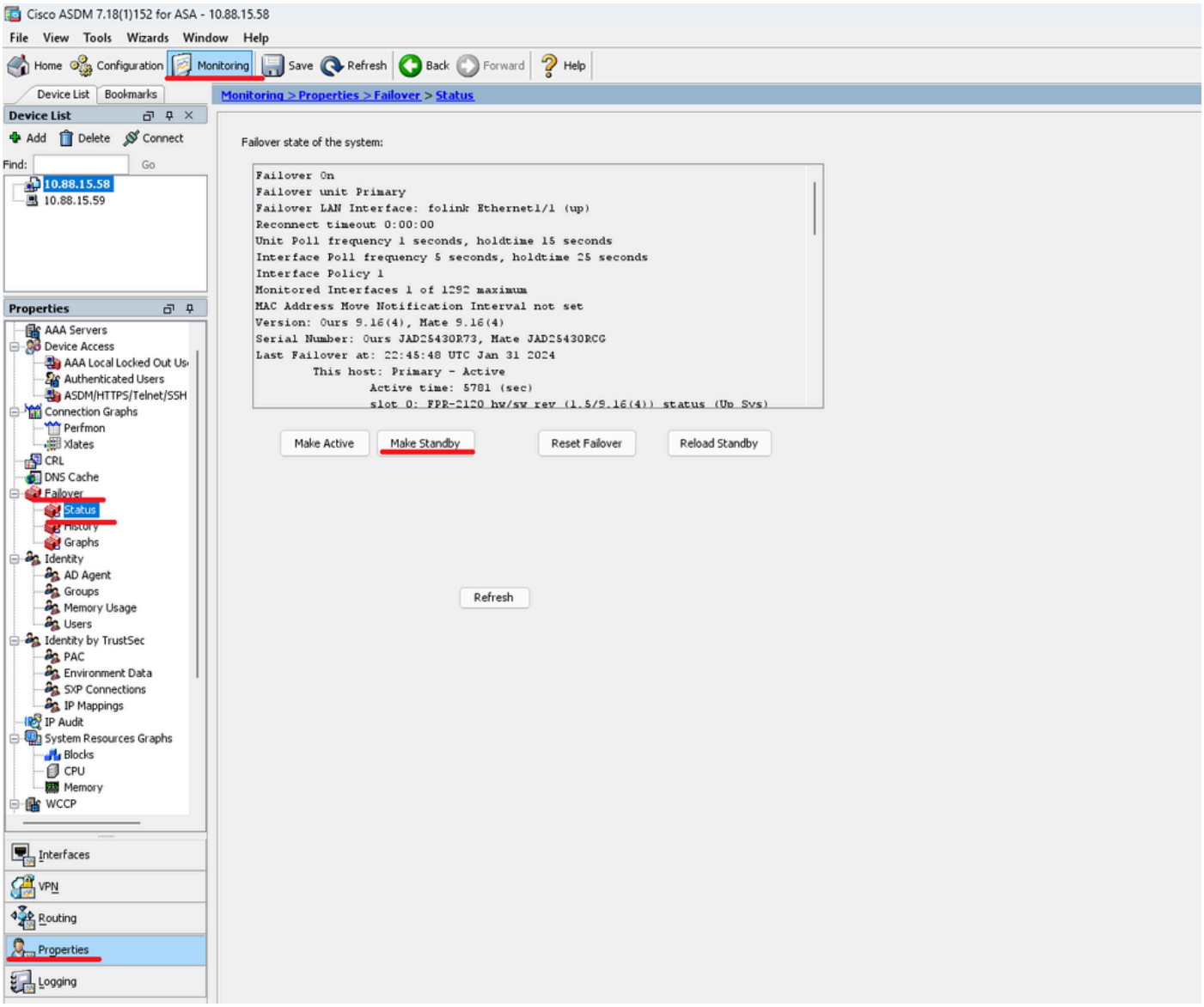
Attendere il caricamento dell'unità di standby.

Passaggio 9. Una volta ricaricata l'unità in standby, modificare lo stato dell'unità principale da attivo a standby.

Selezionare Monitoraggio **> Proprietà > Failover > Stato** e fare clic su **Rendi standby**.

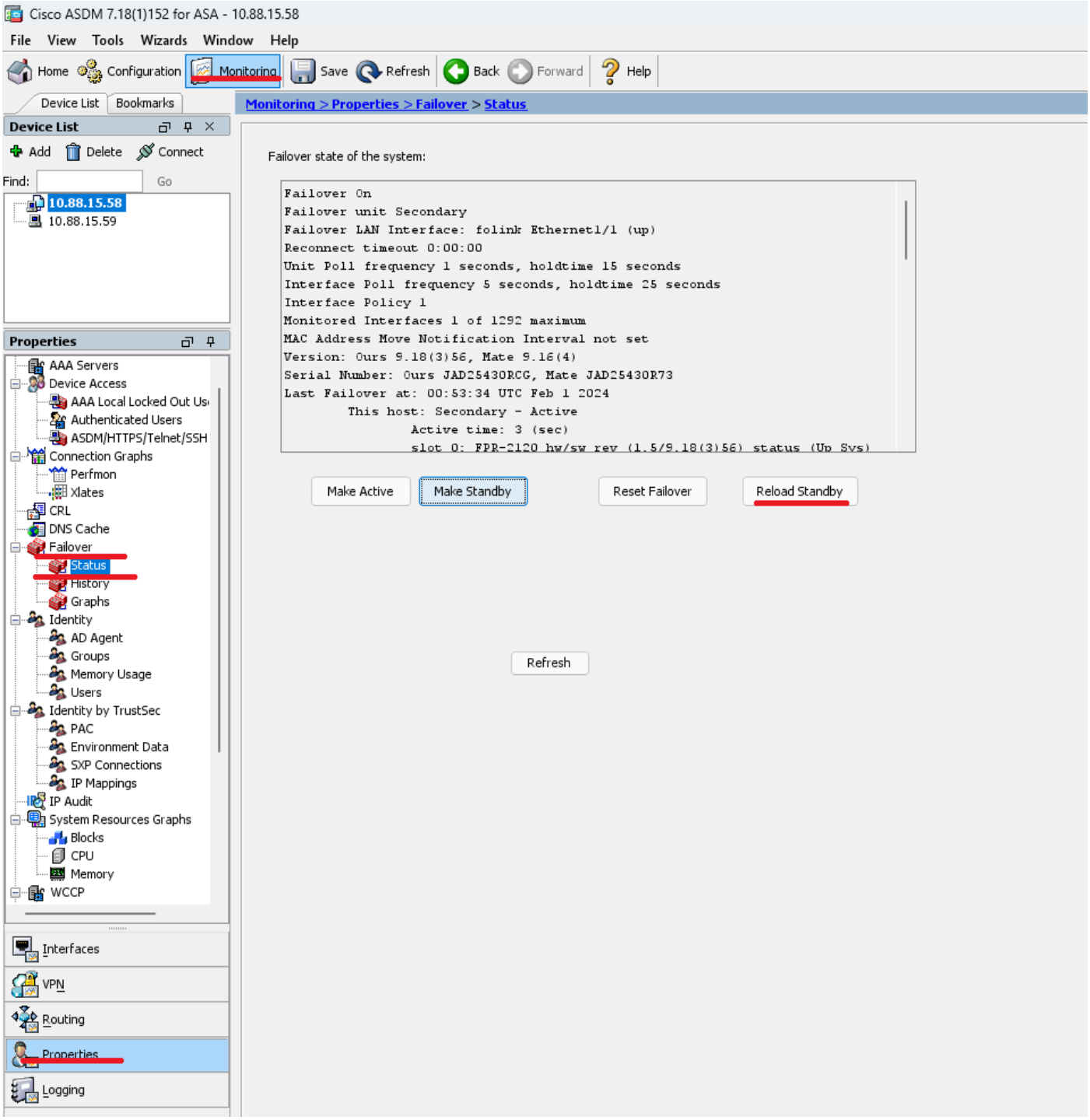


Nota: ASMD si connette automaticamente alla nuova unità attiva.



Passaggio 10. Ricaricare la nuova unità di standby per installare la nuova versione.

Selezionare Monitoraggio **> Proprietà > Failover > Stato** e fare clic su **Ricarica standby**.



Una volta caricata la nuova unità di standby, l'aggiornamento è completo.

Verifica

Per verificare che l'aggiornamento sia stato completato su entrambe le unità, controllare l'aggiornamento tramite CLI e ASDM.

Tramite 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
```

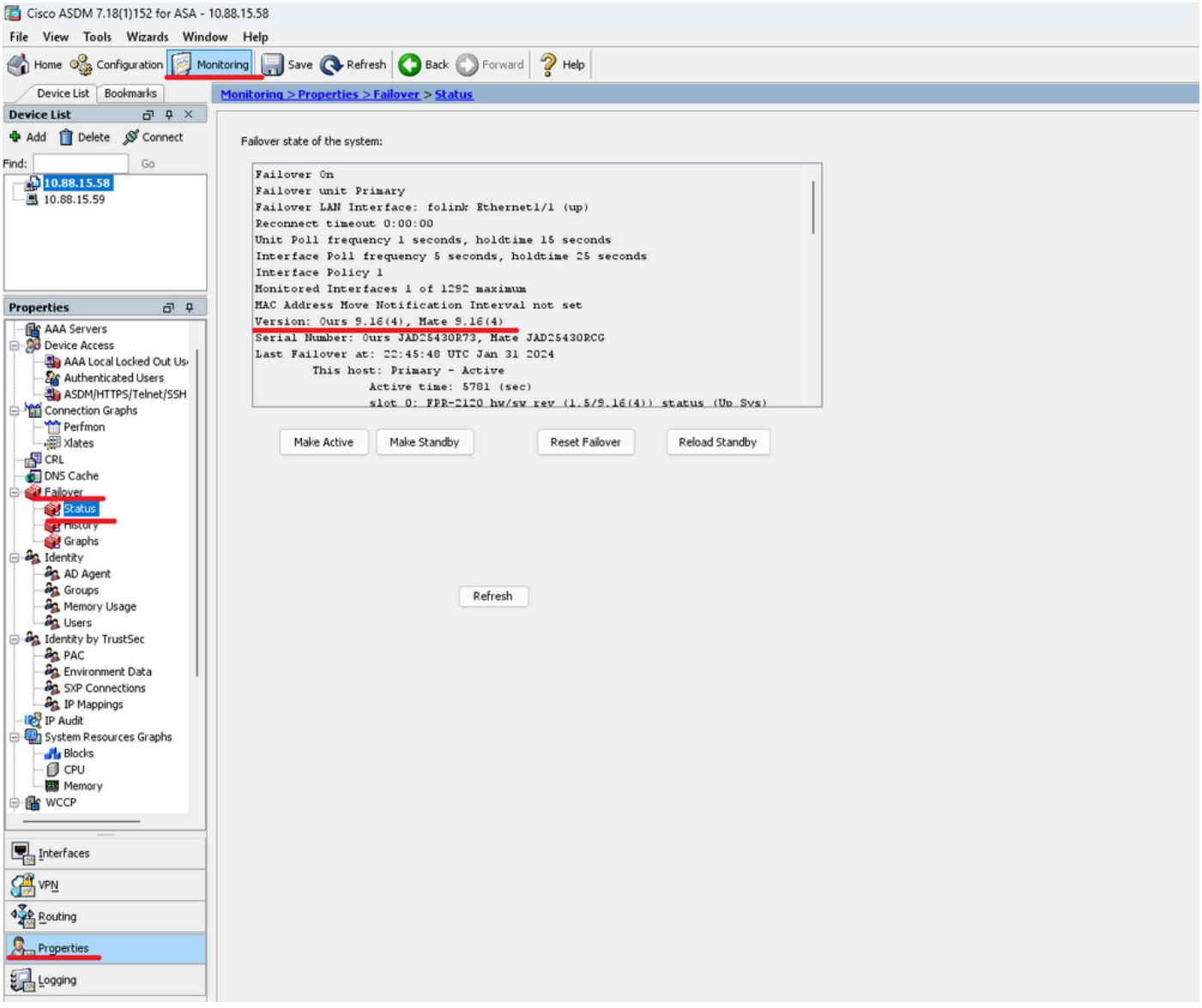
Version: Ours 9.16(4), Mate 9.16(4)

```
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
```

Tramite ASDM

Selezionare **Monitoring** > **Properties** > **Failover** > **Status** (Monitoraggio > **Proprietà > Failover > Stato**) per verificare la versione ASA per entrambi i dispositivi.



Informazioni correlate

- Compatibilità ASA Cisco Secure Firewall
- Guida all'aggiornamento di Cisco Secure Firewall ASA

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).