보안 방화벽을 위한 ASA 액티브/스탠바이 장애 조치 쌍 업그레이드

목차

소개

이 문서에서는 어플라이언스 모드의 Secure Firewall 1000, 2100 및 Secure Firewall 3100/4200에 대한 장애 조치 구축을 위해 ASA를 업그레이드하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Firewall 위협 방어.
- Cisco ASA 컨피그레이션.

사용되는 구성 요소

이 문서의 정보는 소프트웨어 버전을 기반으로 합니다.

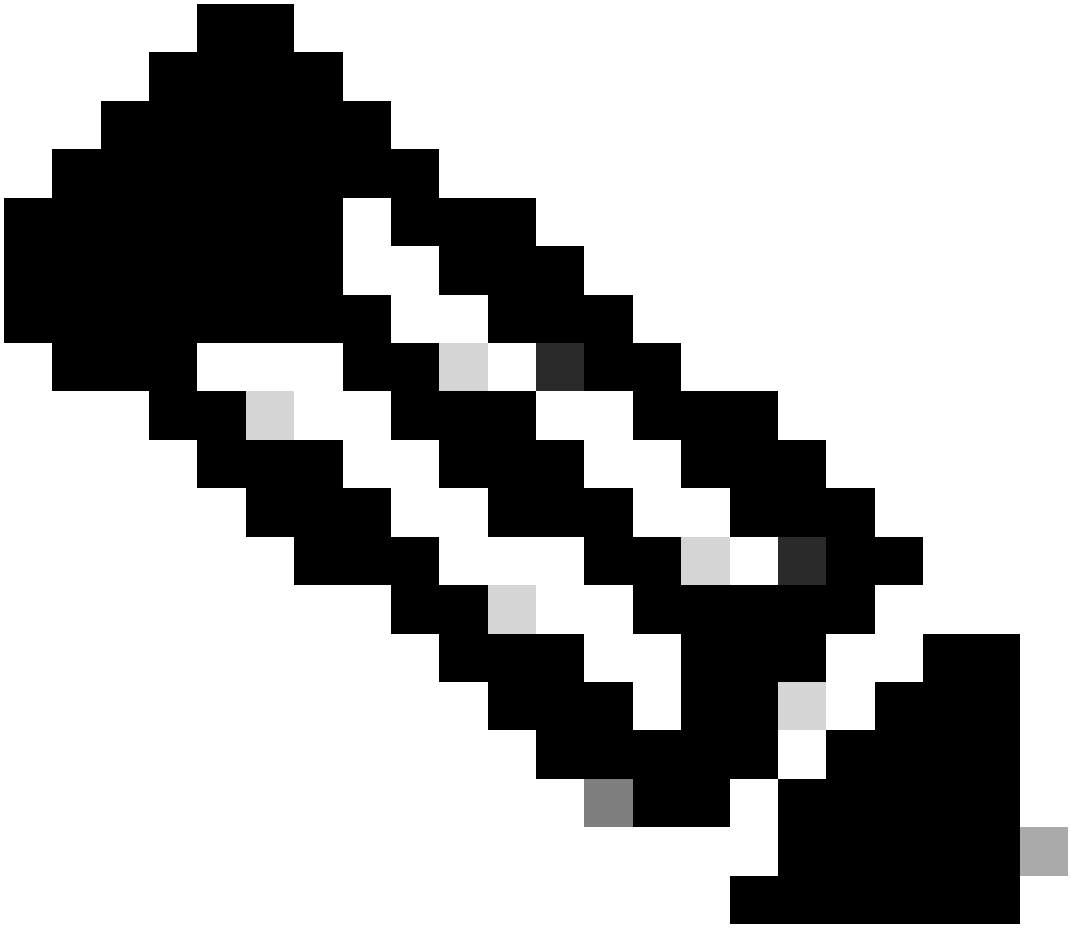
- Cisco Adaptive Security Appliance Software 버전 9.14(4)
- Cisco Adaptive Security Appliance Software 버전 9.16(4)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

사전 요구 사항 확인

1단계. show fxos 모드를 실행하여 디바이스가 어플라이언스 모드에 있는지 확인합니다



참고: 9.13 이전 버전의 Secure Firewall 21XX에서는 플랫폼 모드만 지원합니다. 버전 9.14 이상에서는 어플라이언스 모드가 기본값입니다.

<#root>

ciscoasa#

show fxos mode

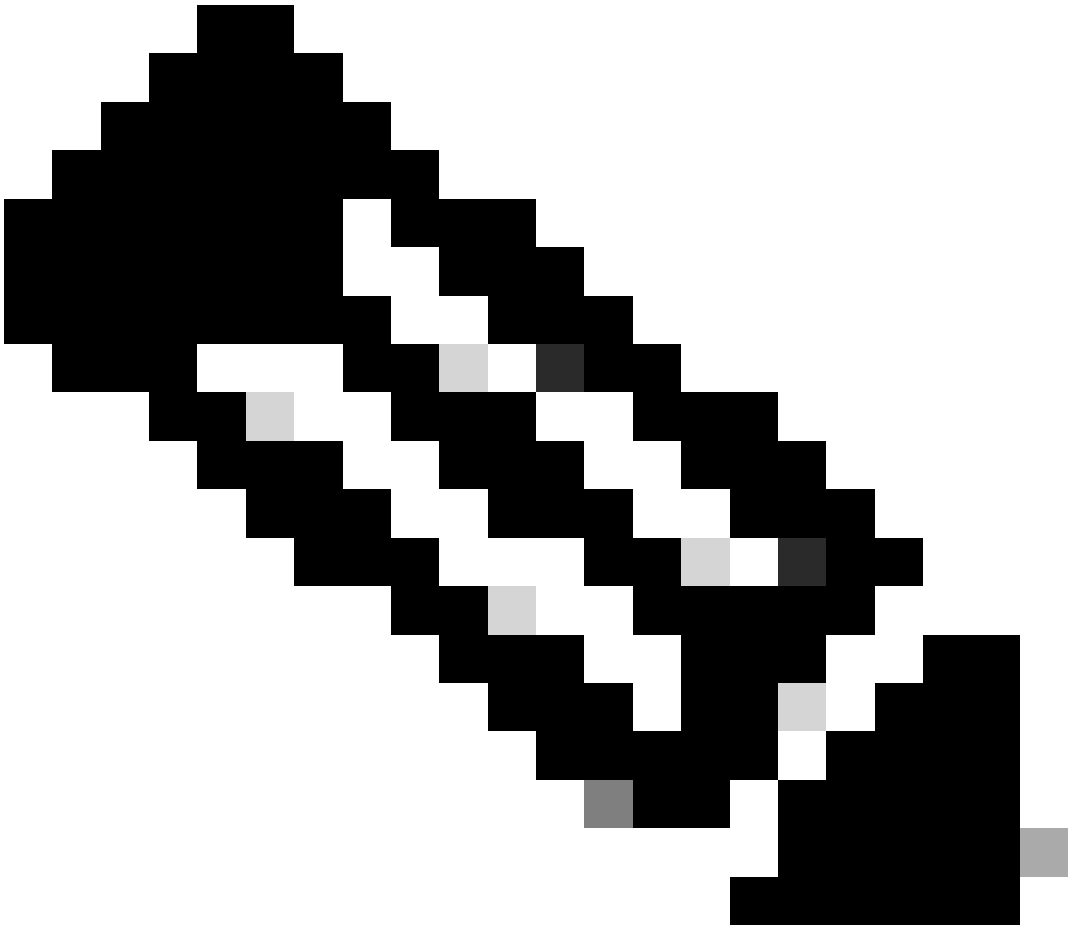
Mode is currently set to appliance

2단계. 호환성을 확인합니다.

FTD 하드웨어 플랫폼과 Secure Firewall ASA 소프트웨어 간의 호환성을 확인하려면 Cisco Secure Firewall ASA 호환성 문서를 참조하십시오. 을 참조하십시오.

Cisco Secure Firewall ASA 호환성

3단계. Cisco Software Central에서 업그레이드 패키지를 다운로드합니다.



참고: Secure Firewall 1000/2100 및 Secure Firewall 3100/4200의 경우 ASA 또는 FXOS를 별도로 설치할 수 없습니다. 두 이미지 모두 번들에 속합니다.

번들에 포함된 ASA 및 FXOS의 버전을 알아보려면 연결된 제목을 참조하십시오. 보안 방화벽 1000/2100 및 3100/4200 ASA 및 FXOS 번들 버전을 참조하십시오.

CLI를 사용하여 업그레이드

1단계. ASDM 이미지를 재설정합니다.

전역 컨피그레이션 모드에서 기본 유닛에 연결하고 다음 명령을 실행합니다.

<#root>

ciscoasa(config)#

asdm image disk0:/asdm.bin

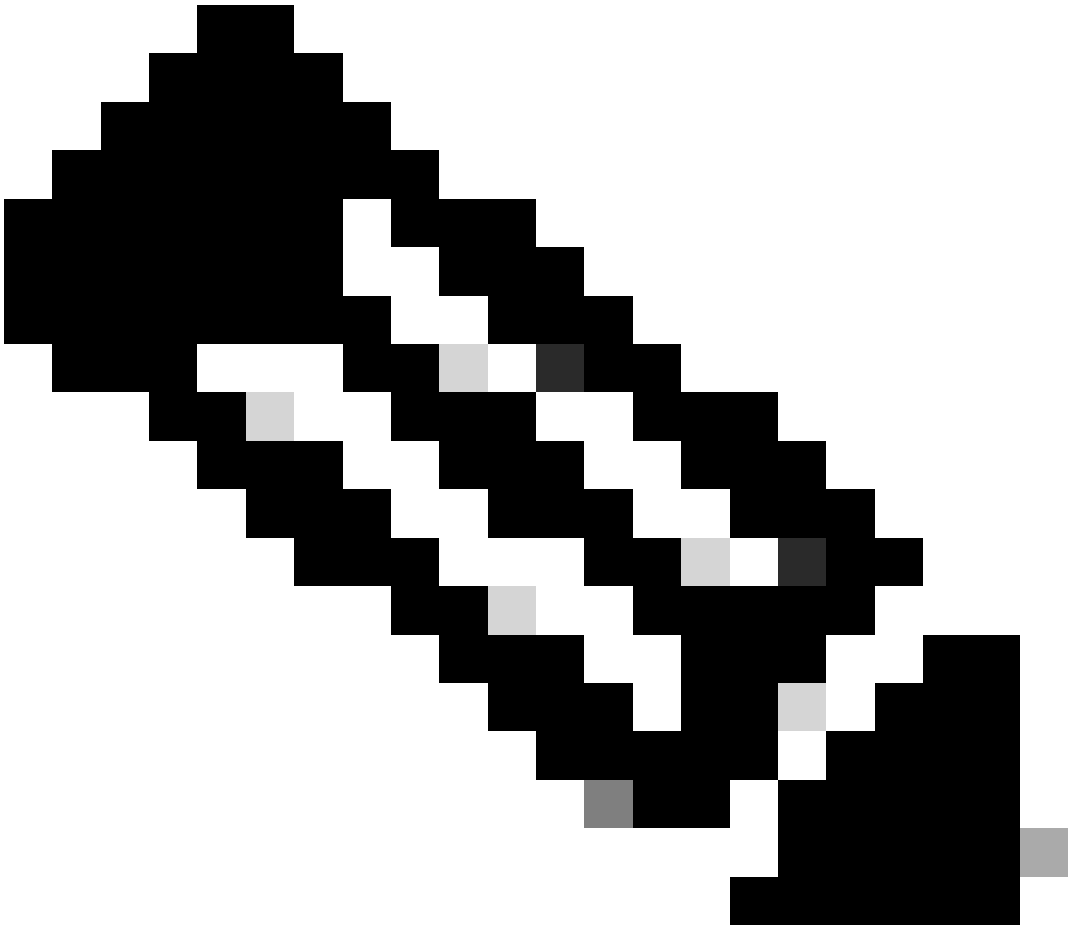
ciscoasa(config)# exit
ciscoasa#

copy running-config startup-config

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

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

2단계. 기본 유닛에 소프트웨어 이미지를 업로드합니다.



참고: 이 문서에서는 FTP 서버를 사용하지만 TFTP, HTTP 또는 기타 서버 유형을 사용할 수 있습니다.

<#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)
```

3단계. 소프트웨어 이미지를 보조 유닛에 업로드합니다.

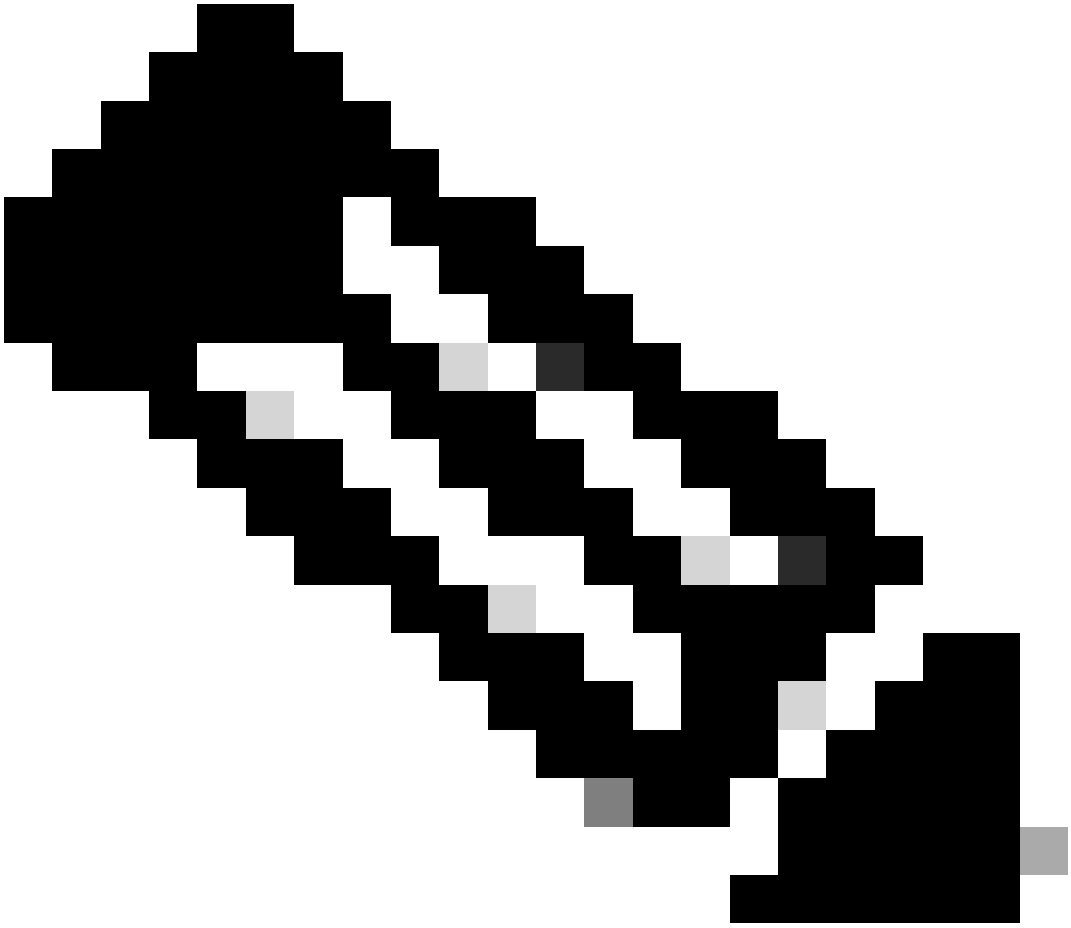
기본 유닛에서 명령을 실행합니다.

<#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)
```

4단계. 현재 부트 이미지가 이 명령으로 구성되어 있는지 **show running-config boot system** 확인합니다.



참고: 부트 시스템을 구성하지 않았을 수 있습니다.

<#root>

ciscoasa(config)#

show running-config boot system

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

5단계(선택 사항) 부팅 이미지가 구성되어 있으면 제거해야 합니다.

부팅 시스템 디스크 없음:/asa_image_name

예:

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

6단계. 부팅할 이미지를 선택합니다.

```
   <#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
```

7단계. copy running-config startup-**config 명령을 사용하여 컨피그레이션을** 저장합니다.

단계. 보조 유닛을 다시 로드하여 새 버전을 설치합니다.

```
<#root>

ciscoasa(config)#

failover reload-standby
```

보조 유닛이 로드될 때까지 기다립니다.

9단계. 스탠바이 유닛이 다시 로드되면 기본 유닛을 액티브 상태에서 스탠바이 상태로 변경합니다.

```
<#root>

ciscoasa#

no failover active
```

10단계. 새 대기 유닛을 다시 로드하여 새 버전을 설치합니다. 새 액티브 유닛에 연결해야 합니다.

```
<#root>
```

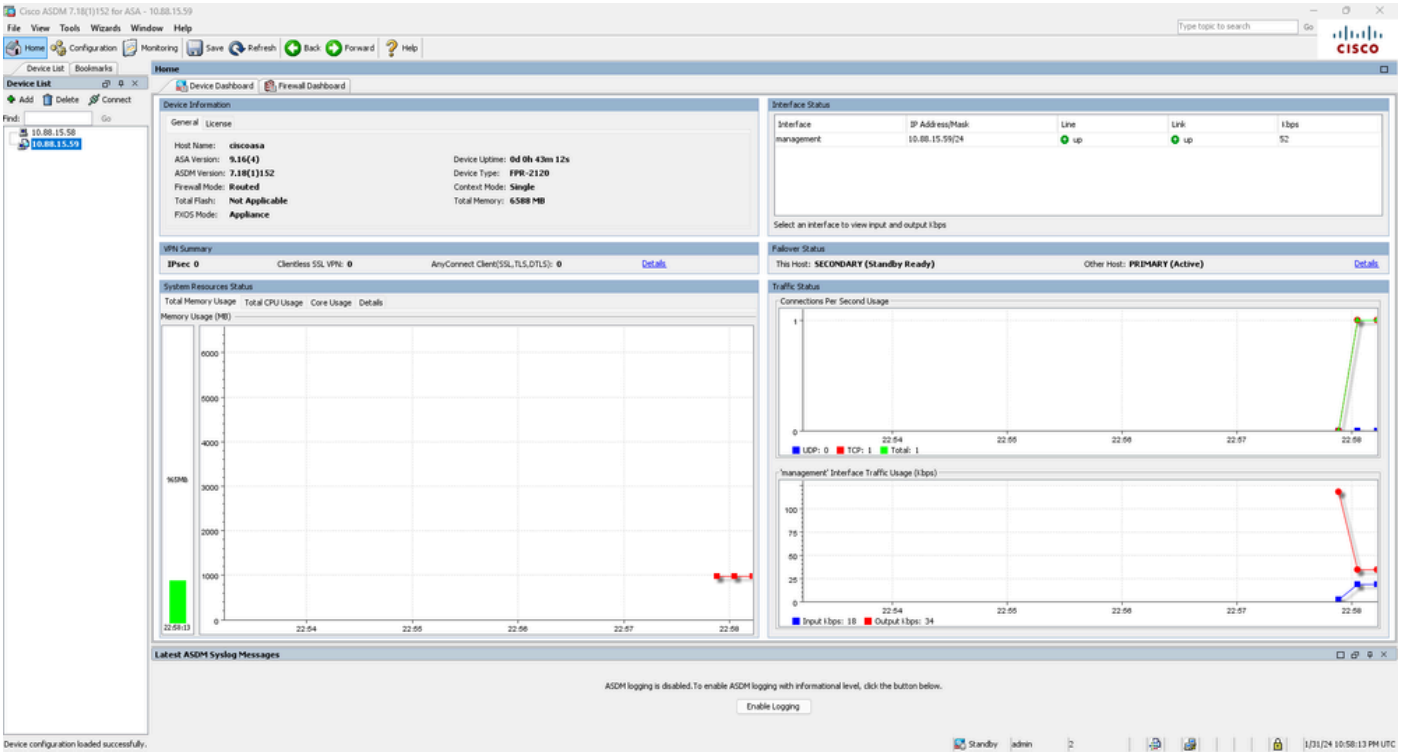
ciscoasa(config)#

```
failover reload-standby
```

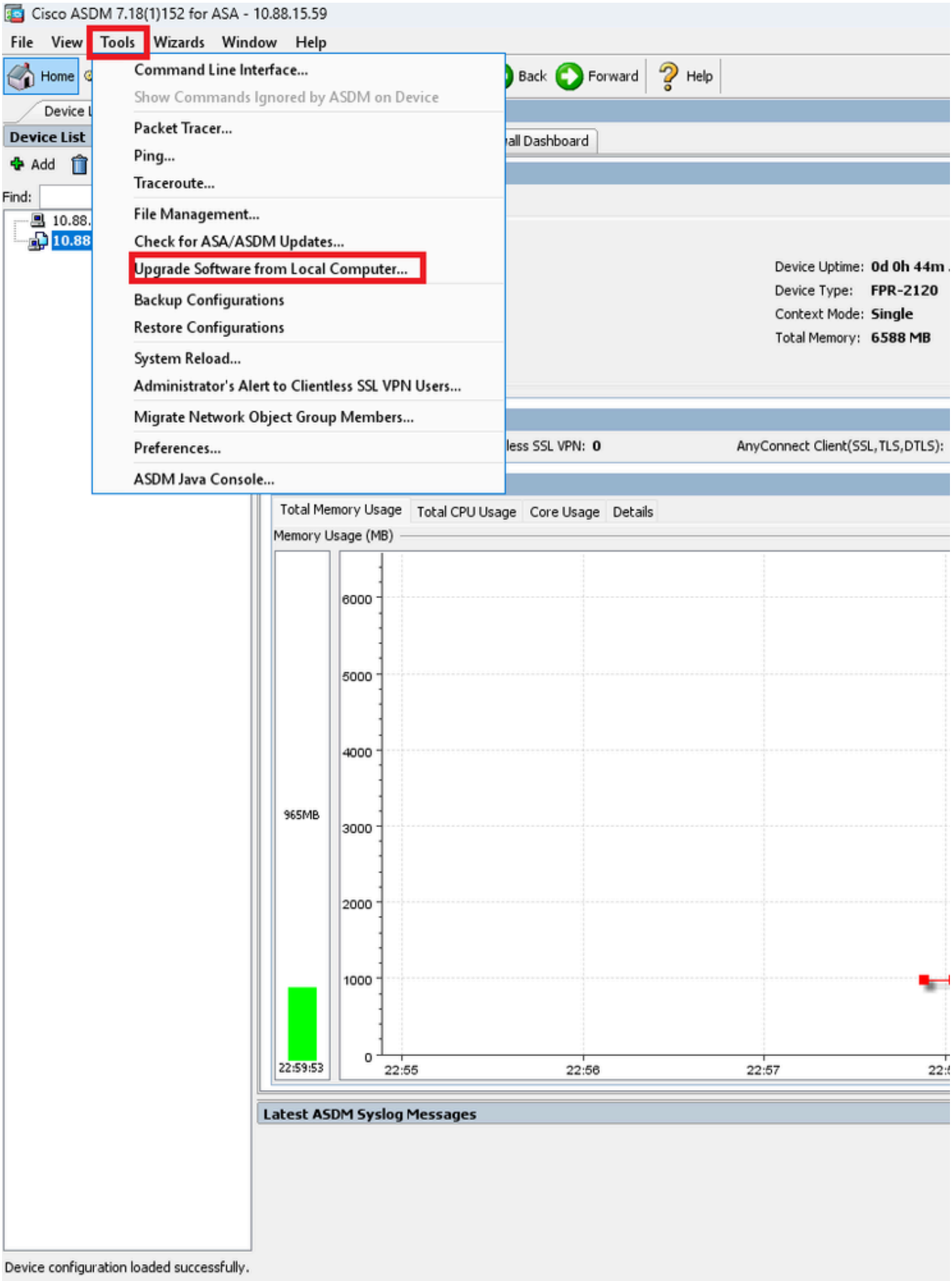
새 스탠바이 유닛이 로드되면 업그레이드가 완료됩니다.

ASDM을 사용하여 업그레이드

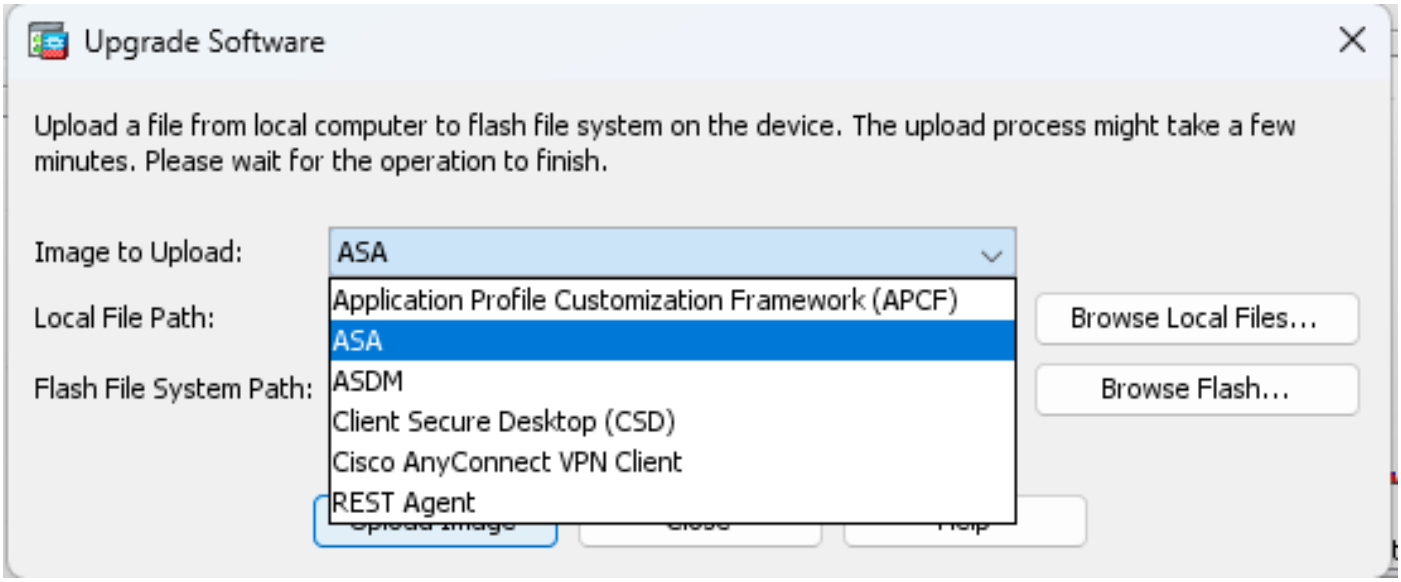
1단계. ASDM을 사용하여 보조 유닛에 연결합니다.



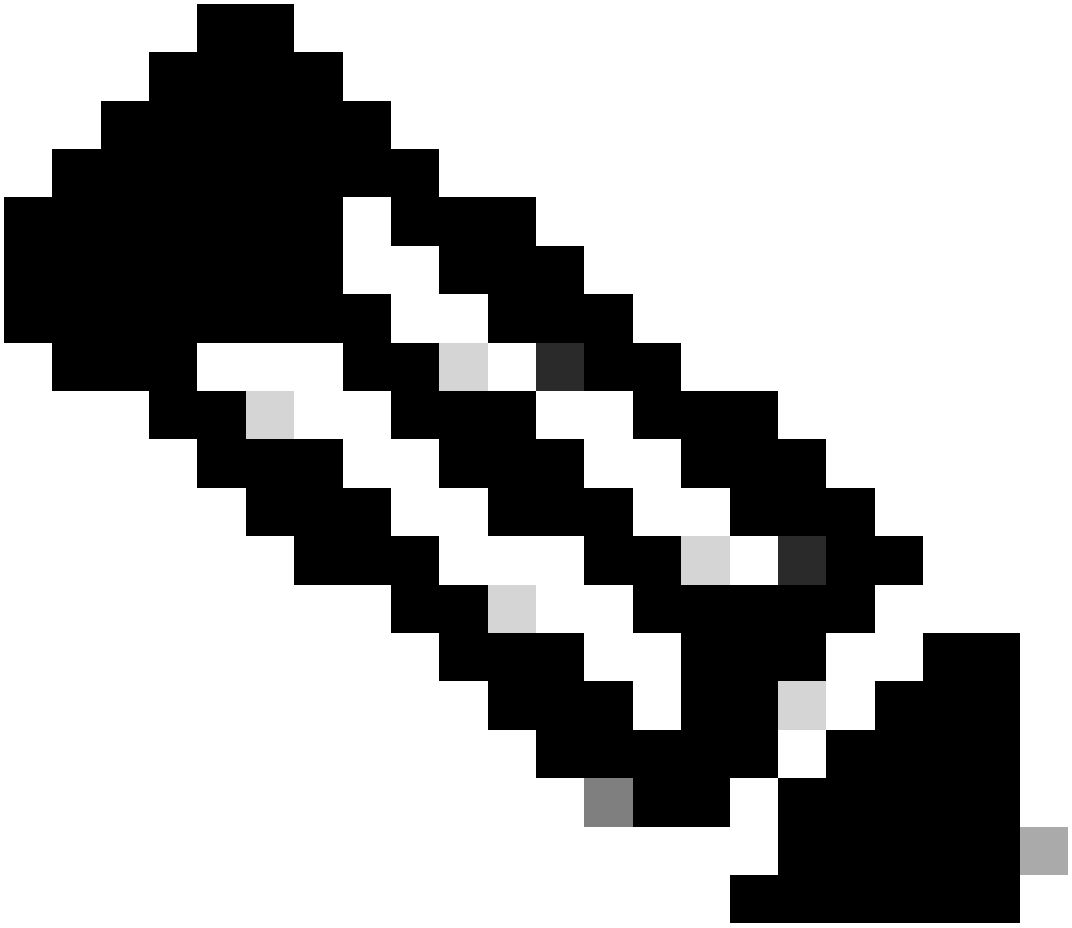
2단계. Tools(**툴**) > **Upgrade Software from Local Computer(로컬 컴퓨터에서 소프트웨어 업그레이드)로 이동합니다**.



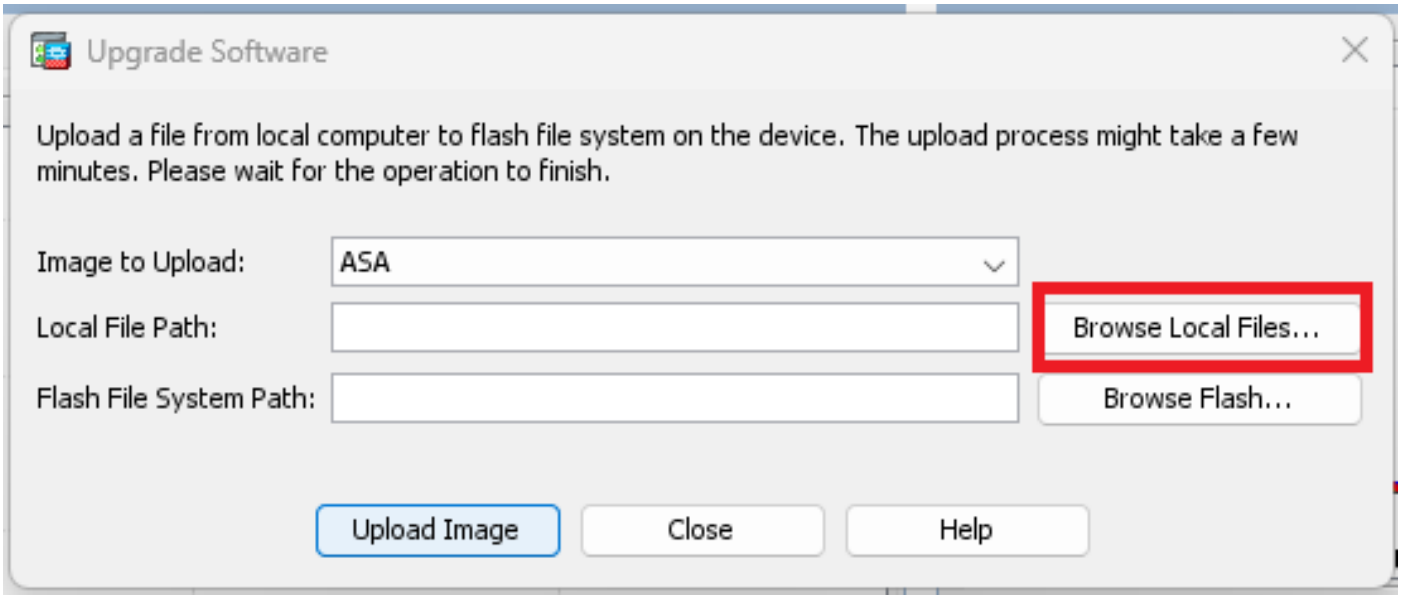
3단계. 드롭다운 목록에서 **ASA**를 선택합니다.



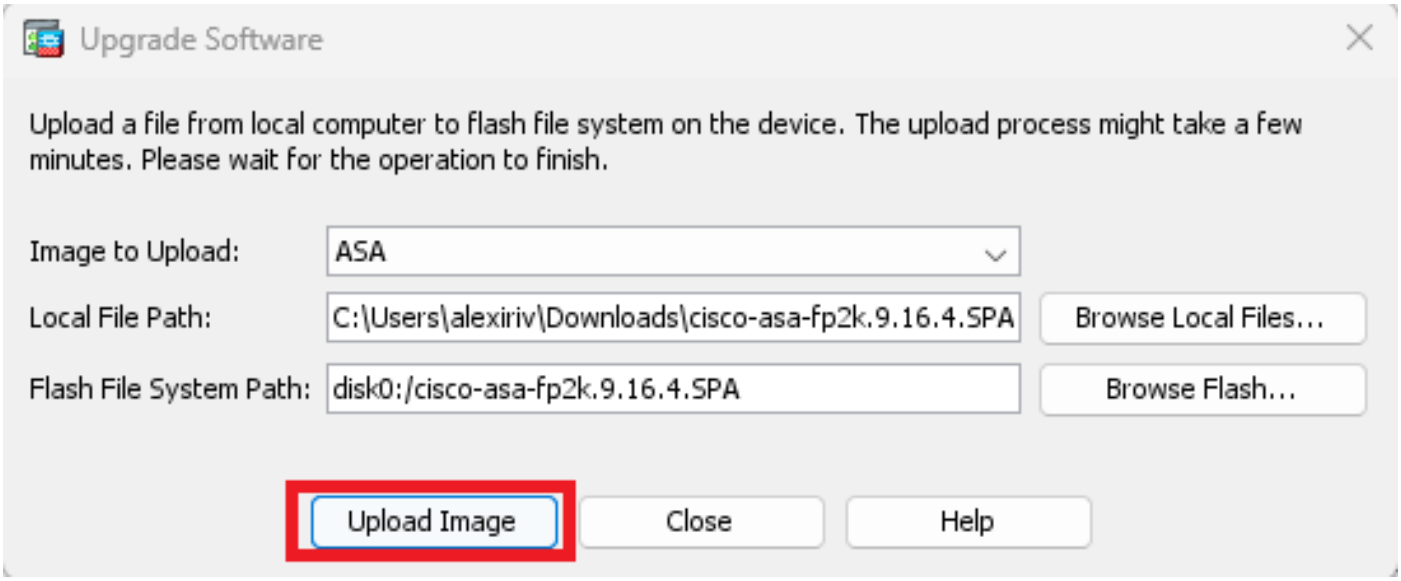
4단계. Upgrade **Software(소프트웨어 업그레이드) 창**에서 **Browse Local Files(로컬 파일 찾아보기)**를 클릭하여 소프트웨어 이미지를 보조 유닛에 업로드합니다.



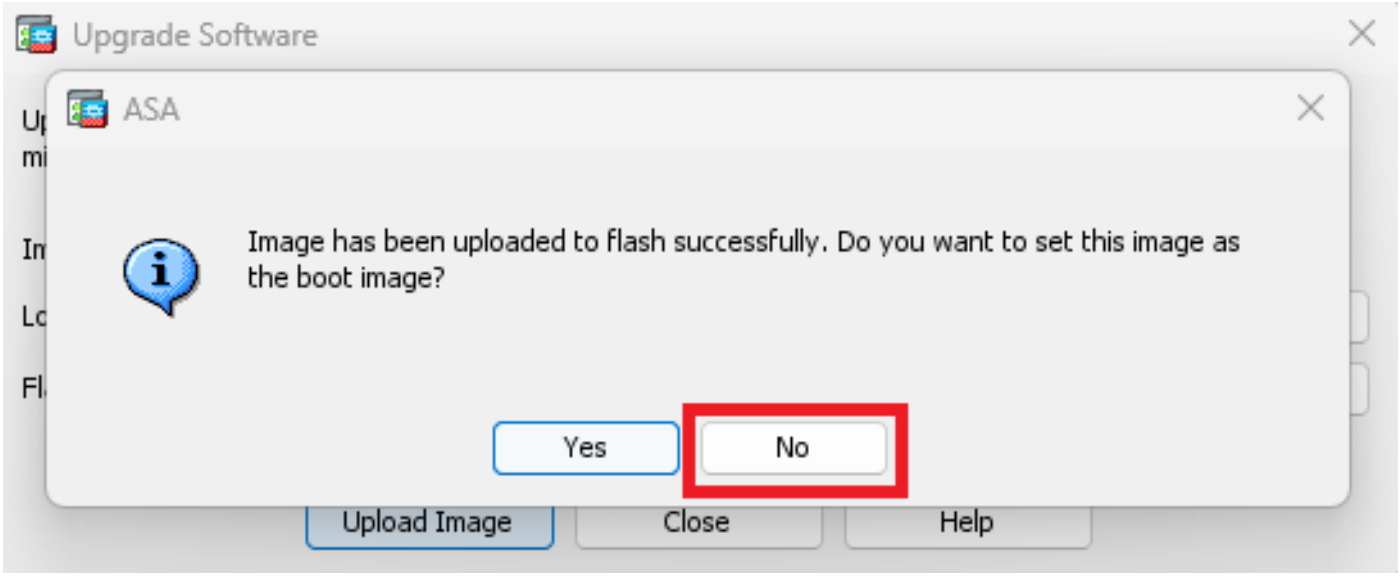
참고: 기본적으로 **플래시 파일 시스템 경로**는 disk0입니다. 변경하려면 Browse Flash(**플래시 찾아보기)를** 클릭하고 새 경로를 선택합니다.



Upload Image(이미지 업로드)를 클릭합니다.



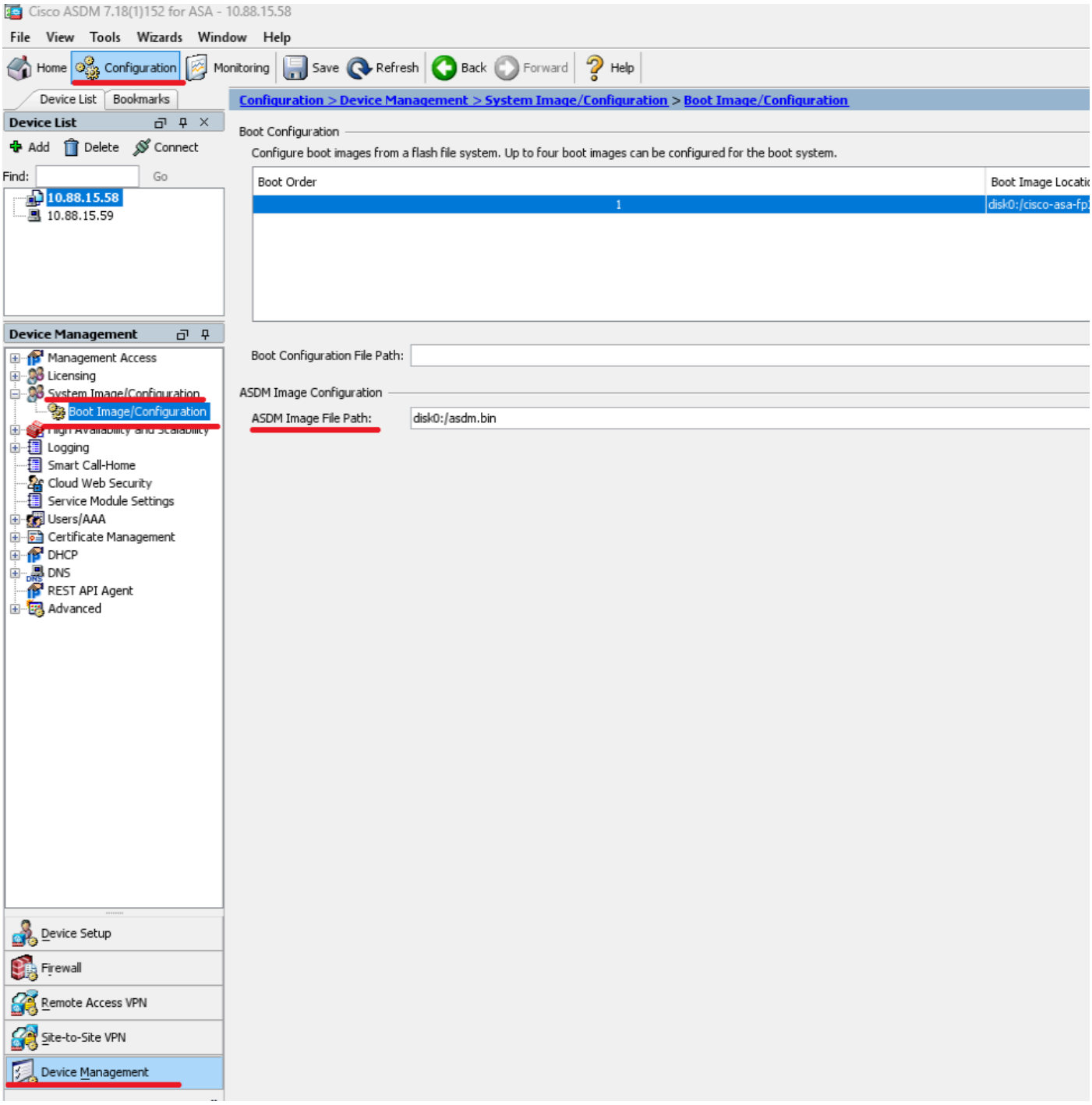
이미지 업로드가 완료되면 No(**아니요**)를 클릭합니다.



5단계. ASDM 이미지를 재설정합니다.

ASDM을 사용하여 기본 유닛에 연결하고 Configuration(컨피그레이션) > **Device Management(디바이스 관리)** > **System Image/Configuration(시스템 이미지/컨피그레이션)** > **Boot Image/Configuration(부팅 이미지/컨피그레이션)으로** 이동합니다.

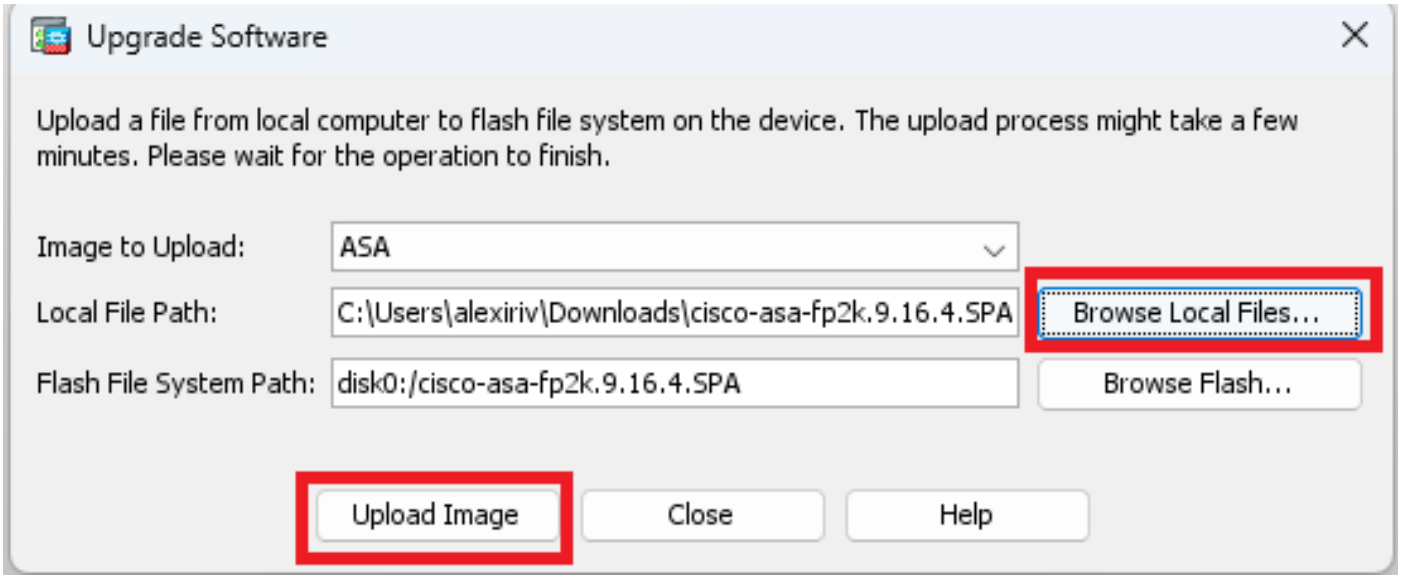
ASDM **Image File Path(ASDM 이미지 파일 경로)**에 **disk0:/asdm.bin 값**을 입력하고 **Apply(적용)를 클릭합니다**.



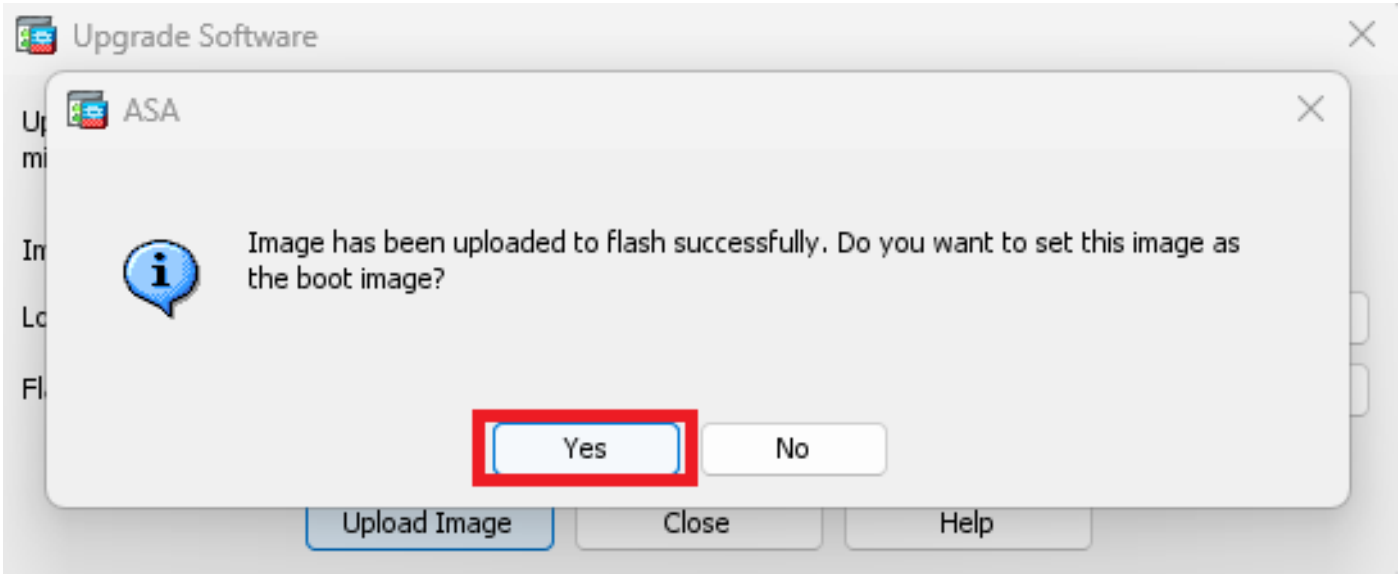
6단계. 기본 유닛에 소프트웨어 이미지를 업로드합니다.

Browse **Local Files(로컬 파일 찾아보기)**를 클릭하고 디바이스에서 업그레이드 패키지를 선택합니다.

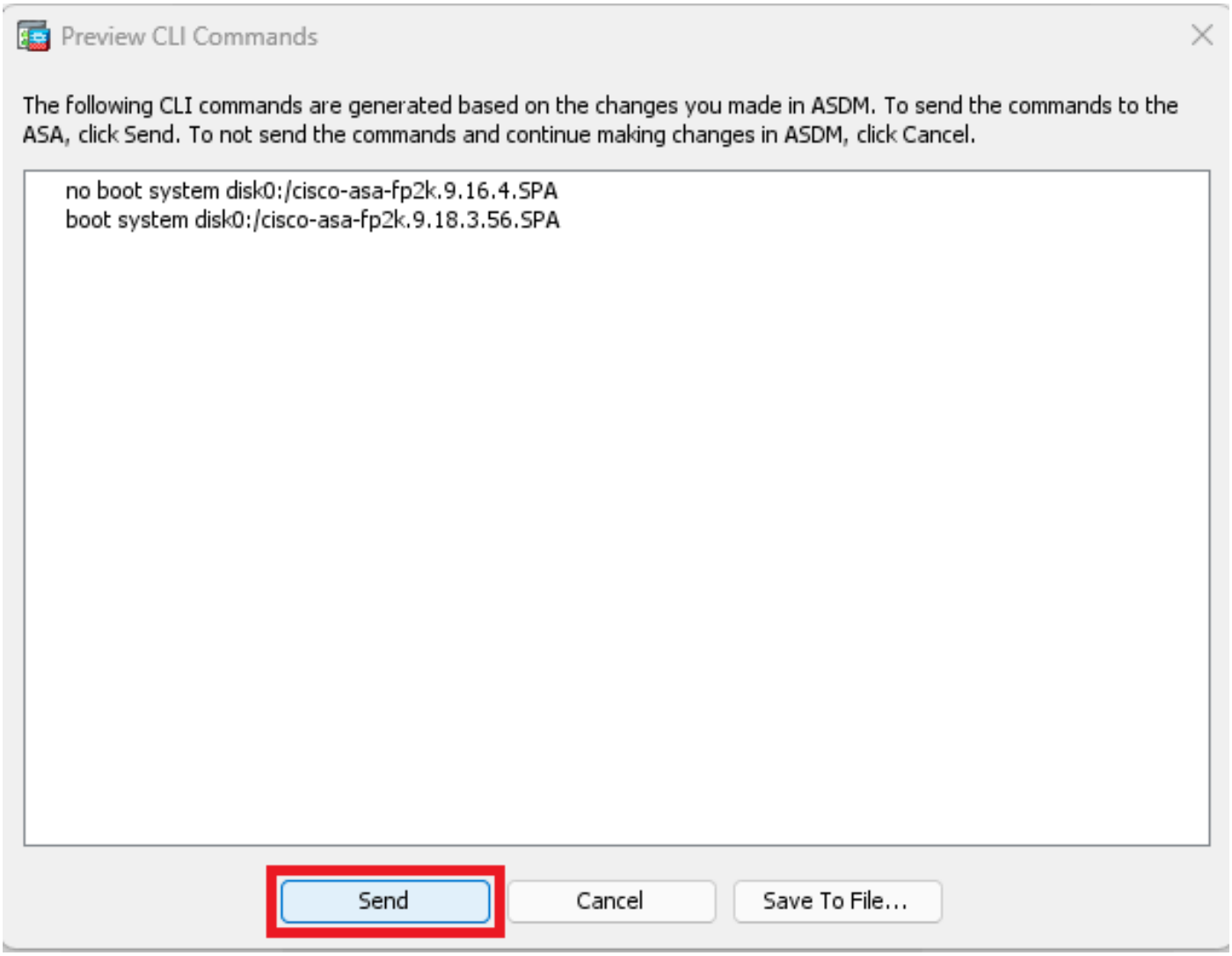
Upload Image(이미지 업로드)를 클릭합니다.



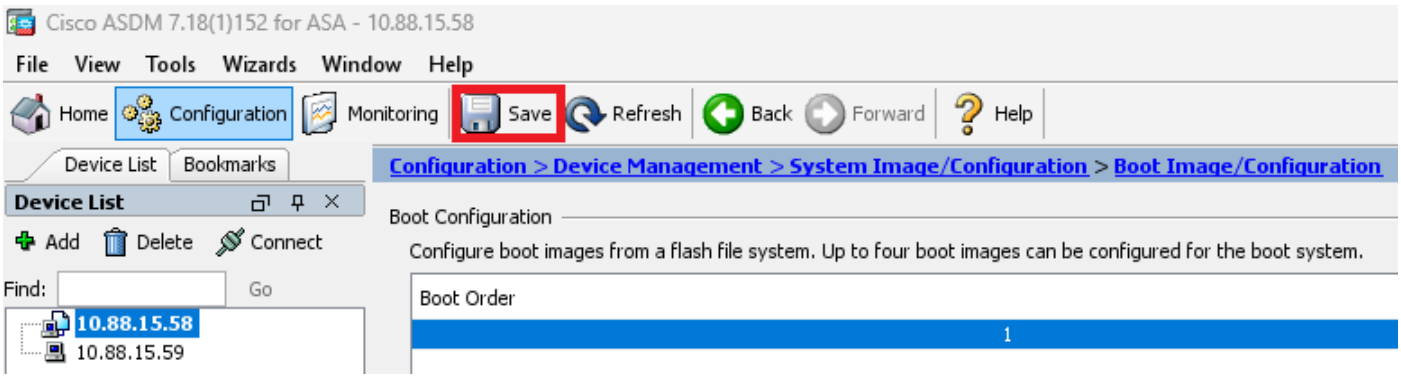
이미지 업로드가 완료되면 Yes(**예**)를 클릭합니다.



미리 보기 창에서 **보내기** 단추를 클릭하여 구성을 저장합니다.

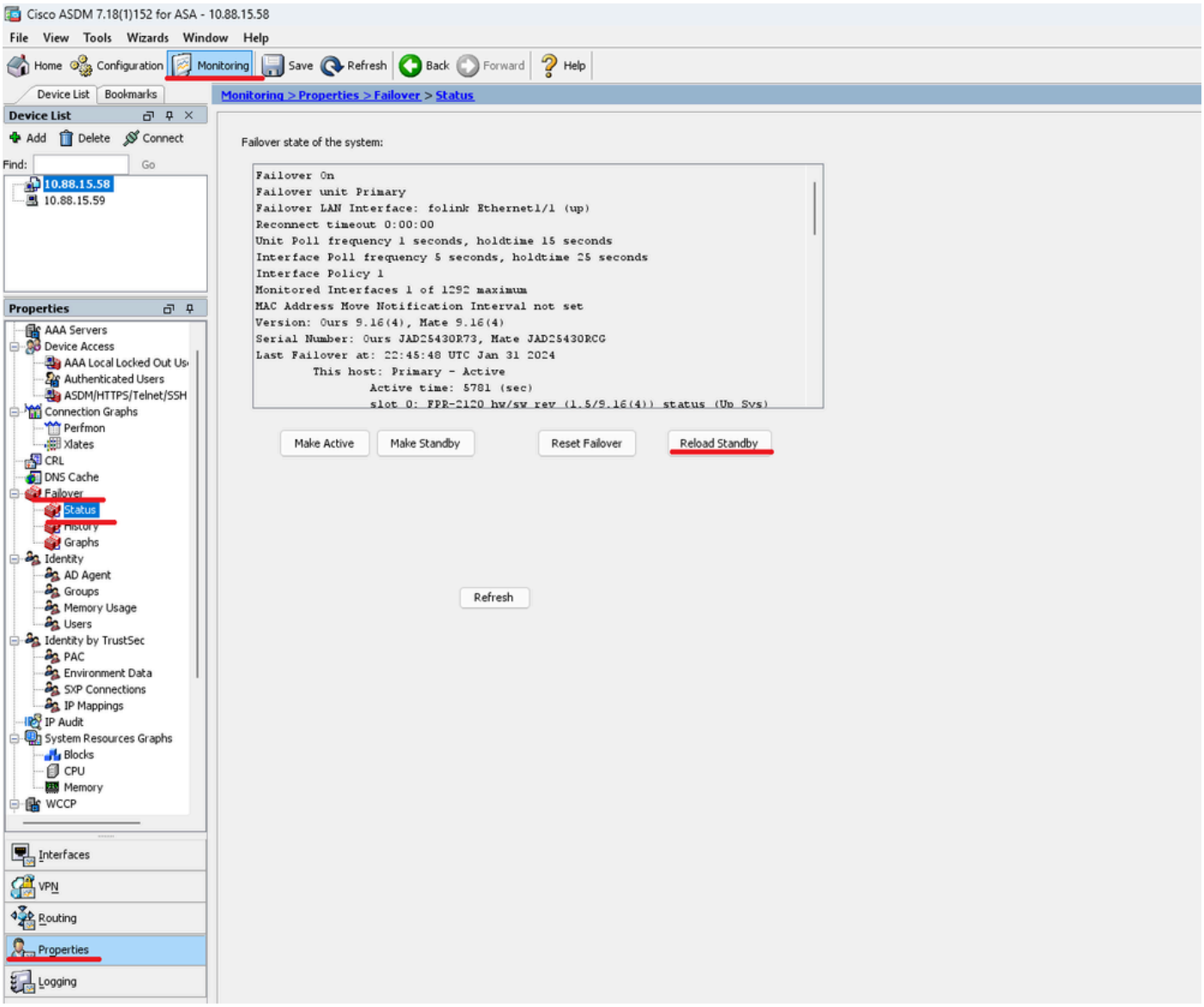


7단계. 컨피그레이션을 **저장하려면** Save를 클릭합니다.



8단계. 보조 유닛을 다시 로드하여 새 버전을 설치합니다.

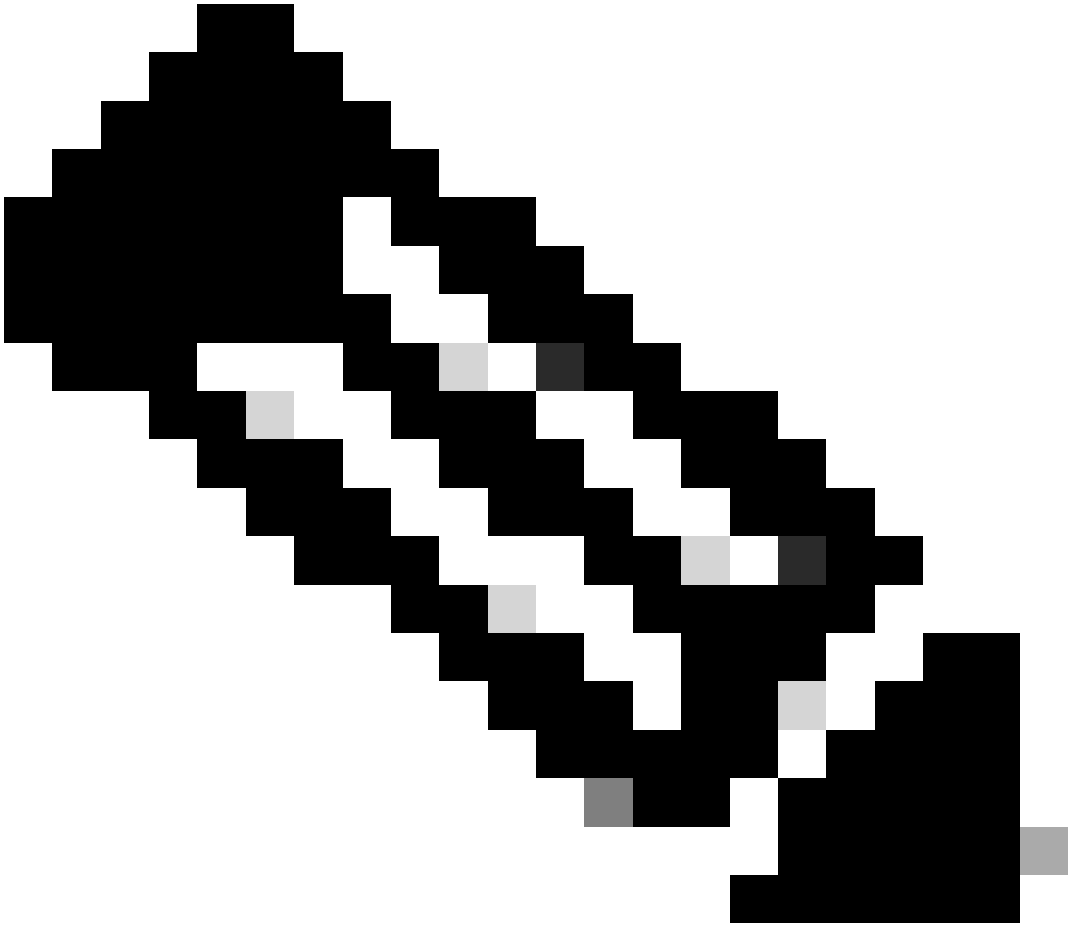
Monitoring(모니터링) > **Properties(속성)** > **Failover(장애 조치)** > **Status(상태)로** 이동하고 Reload Standby(스탠바이 **다시 로드)를 클릭합니다.**



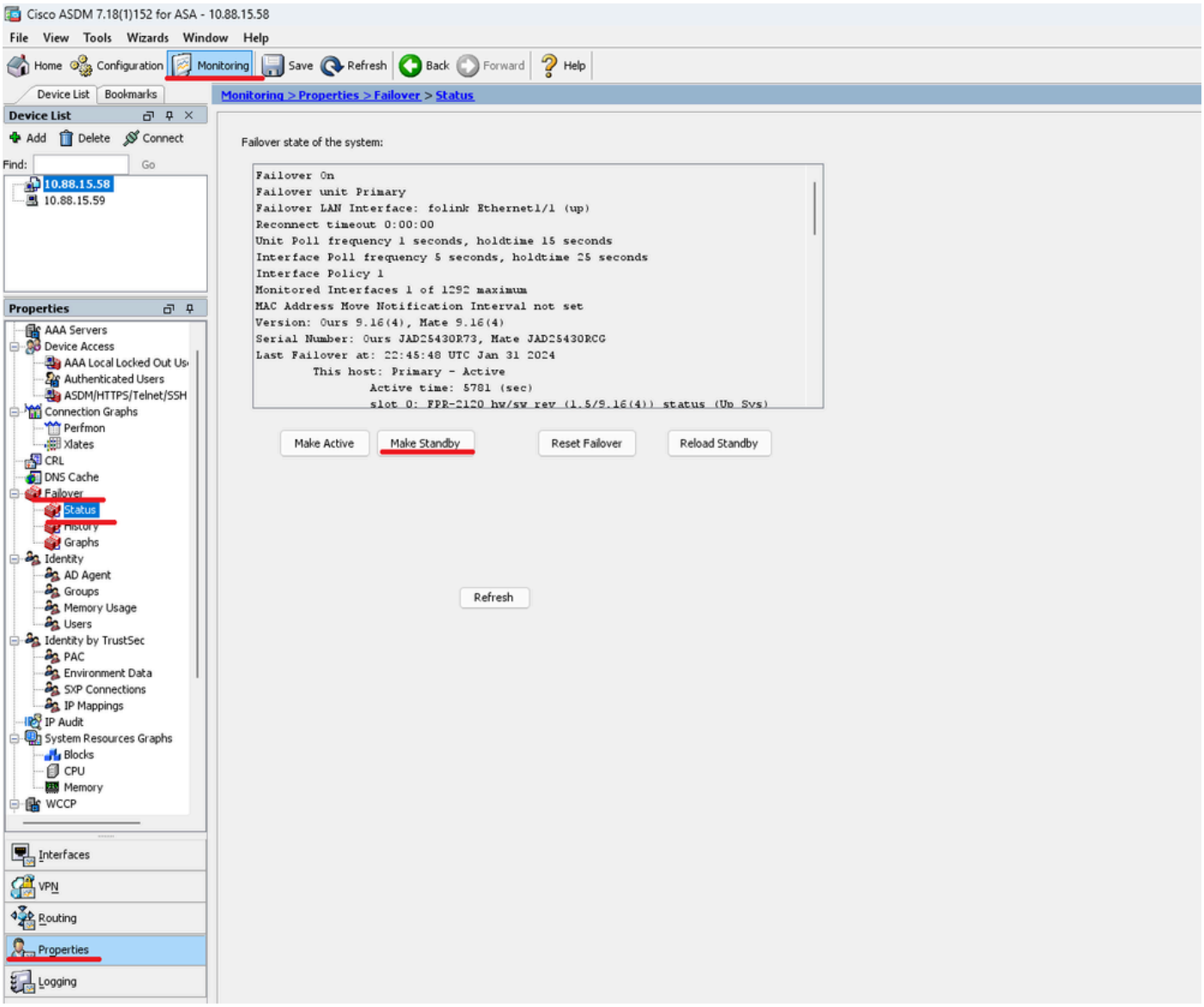
대기 유닛이 로드될 때까지 기다립니다.

9단계. 스탠바이 유닛이 다시 로드되면 기본 유닛을 액티브 상태에서 스탠바이 상태로 변경합니다.

Monitoring(모니터링) > **Properties(속성)** > **Failover(장애 조치) > Status(상태)로** 이동하여 Make Standby(스탠바이 **상태로 만들기)를 클릭합니다.**

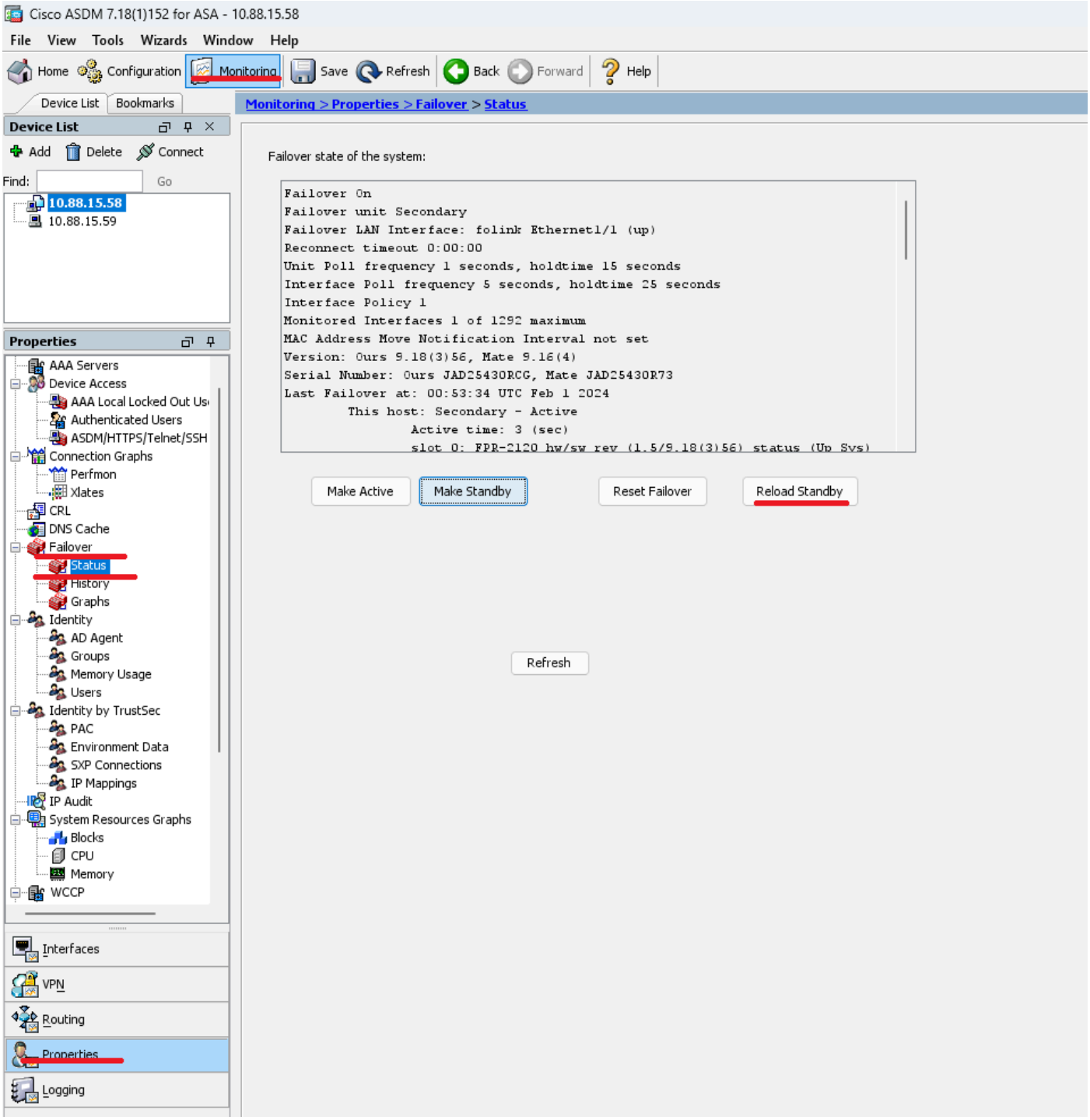


참고: ASMD는 자동으로 새 액티브 유닛에 연결됩니다.



10단계. 새 대기 유닛을 다시 로드하여 새 버전을 설치합니다.

Monitoring(모니터링) > **Properties(속성)** > **Failover(장애 조치) > Status(상태)로** 이동하고 Reload Standby(스탠바이 **다시 로드)를 클릭합니다.**



새 스탠바이 유닛이 로드되면 업그레이드가 완료됩니다.

다음을 확인합니다.

두 유닛 모두에서 업그레이드가 완료되었는지 확인하려면 CLI 및 ASDM을 통해 업그레이드를 확인합니다.

CLI를 통해

```
<#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
```

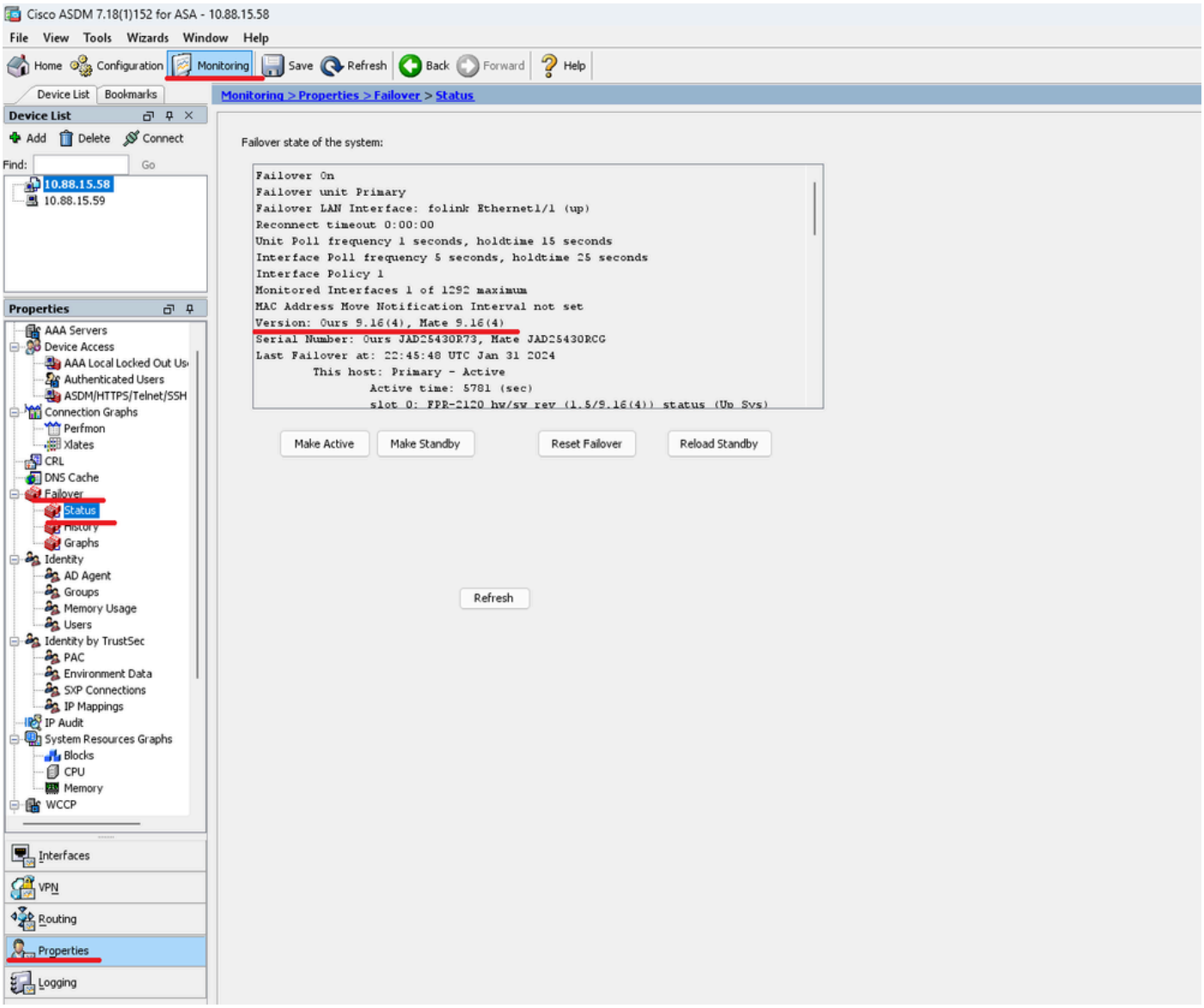
Version: Ours 9.16(4), Mate 9.16(4)

```
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
```

ASDM을 통해

Monitoring(**모니터링**) > **Properties(속성)** > **Failover(장애 조치)** > **Status(상태)로** 이동합니다. 두 디바이스 모두에 대한 ASA 버전을 볼 수 있습니다.



관련 정보

- Cisco Secure Firewall ASA 호환성
- Cisco Secure Firewall ASA 업그레이드 가이드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.