Cisco ASA 및 Firepower Threat Defense 이미지 재설치 가이드

초판: 2016년 5월 10일

최종 변경: 2018년 4월 17일

Cisco ASA 및 Firepower Threat Defense 이미지 재설치 가이드

콘솔 포트 액세스 필요

이미지 재설치를 수행하려면 컴퓨터를 콘솔 포트에 연결해야 합니다.

Firepower 2100, ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X의 경우 연결을 설정하려면 서드파티 직렬 대 USB 케이블을 사용해야 할 수도 있습니다. 기타 모델은 소형 USB 유형 B 콘솔 포트를 포함하므로 모든 소형 USB 케이블을 사용할 수 있습니다. Windows의 경우, software.cisco.com에서 USB 직렬 드라이버를 설치해야 할 수도 있습니다. 콘솔 포트 옵션과 드라이버 요건에 대한 자세한 내용은 하드웨어 가이드(http://www.cisco.com/go/asa5500x-install)를 참조하십시오.

9600 보드, 8 데이터 비트, 패리티 없음, 1 정지 비트, 흐름 제어 없음에 터미널 에뮬레이터 설정을 사용합니다.

지원되는 모델

다음 모델은 ASA 소프트웨어 또는 Firepower Threat Defense 소프트웨어를 지원합니다. ASA 및 Firepower Threat Defense 버전 지원에 대한 자세한 내용은 ASA 호환성 가이드 또는 Firepower 호환성 가이드를 참조하십시오.

- ASA 5506-X
- ASA 5506W-X
- ASA 5506H-X
- ASA 5508-X
- ASA 5512-X
- ASA 5515-X
- ASA 5516-X
- ASA 5525-X
- ASA 5545-X

- ASA 5555-X
- ISA 3000
- Firepower 2100

참고 Firepower 4100 및 9300도 ASA 또는 Firepower Threat Defense를 지원하지만, 논리적 디바이스로 설치됩니다. 자세한 내용은 FXOS 컨피그레이션 가이드를 참조하십시오.

참고 ASA 5512-X~ASA 5555-X에 설치된 Firepower Threat Defense의 경우 Cisco SSD(Solid State Drive)를 설치해야 합니다. 자세한 내용은 ASA 5500-X 하드웨어 가이드를 참조하십시오. ASA에서는 ASA FirePOWER 모듈을 사용하려는 경우에도 SSD가 필요합니다. (ASA 5506-X, 5508-X, 5516-X에서는 SSD가 표준입니다.)

ASA 5500-X 또는 ISA 3000 이미지 재설치

대다수의 ASA 5500-X 또는 ISA 3000 Series 모델은 Firepower Threat Defense 또는 ASA 소프트웨어를 지원합니다.

소프트웨어 다운로드

Firepower Threat Defense 소프트웨어 또는 ASA, ASDM 및 ASA FirePOWER 모듈 소프트웨어를 가져옵니다. 이 문서의 절차상 초기 다운로드를 위해 TFTP 서버에 소프트웨어를 둬야 합니다. 다른 이미지는 기타 서버 유형(예: HTTP 또는 FTP)에서 다운로드할 수 있습니다. 정확한 소프트웨어 패키지 및 서버 유형의 경우, 절차를 참조하십시오.

참고 Cisco.com 로그인 및 Cisco 서비스 계약이 필요합니다.

표 *1: Firepower Threat Defense* 소프트웨어

Firepower Threat Defense 모델	다운로드 위치	패키지
ASA 5506-X, ASA 5508-X 및 ASA 5516-X	참조 페이지: http://www.cisco.com/go/asa-firepower-sw	참고 또한 **.sh**로 끝나는 패치 파일을 확인할 수 있습니다. 패치 업그레이드 프로세스에 대해서는 이 문서에서 다루지 않습니다.
	부트 이미지 사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	부트 이미지의 파일 이름은 ftd-boot-9.6.2.0**.lfbff**와 같은 형식입니다.
	시스템 소프트웨어 설치 패키지 사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	시스템 소프트웨어 설치 패키지의 파일 이름은 ftd-6.1.0-330**.pkg**와 같은 형식입니다.
ASA 5512-X ~ ASA 5555-X	참조 페이지: http://www.cisco.com/go/asa-firepower-sw	참고 또한 **.sh**로 끝나는 패치 파일을 확인할 수 있습니다. 패치 업그레이드 프로세스에 대해서는 이 문서에서 다루지 않습니다.
	부트 이미지 사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	부트 이미지의 파일 이름은 ftd-boot-9.6.2.0**.cdisk**와 같은 형식입니다.
	시스템 소프트웨어 설치 패키지 사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	시스템 소프트웨어 설치 패키지의 파일 이름은 ftd-6.1.0-330**.pkg**와 같은 형식입니다.

Firepower Threat Defense 모델	다운로드 위치	패키지
ISA 3000	참조: http://www.cisco.com/go/isa3000-software	참고 또한 **.sh**로 끝나는 패치 파일을 확인할 수 있습니다. 패치 업그레이드 프로세스에 대해서는 이 문서에서 다루지 않습니다.
	사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	부트 이미지의 파일 이름은 ftd-boot-9.9.2.0**.lfbff**와 같은 형식입니다.
	사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	시스템 소프트웨어 설치 패키지의 파일 이름은 ftd-6.2.3-330**.pkg**와 같은 형식입니다.

표 *2: ASA* 소프트웨어

ASA 모델	다운로드 위치	패키지
ASA 5506-X, ASA 5508-X 및 ASA 5516-X	http://www.cisco.com/go/asa-firepower-sw	
	ASA 소프트웨어 사용 중인 *model(*모델*)* > **Adaptive Security Appliance (ASA) Software(ASA(Adaptive Security Appliance)** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	ASA 소프트웨어 파일 이름은 asa962-**lfbff-k8.SPA**와 같은 형식입니다.
	ASDM 소프트웨어 사용 중인 *model(*모델*)* > **Adaptive Security Appliance (ASA) Device Manager(ASA(Adaptive Security Appliance) Device Manager)** > *version(*버전*)*을 선택합니다.	ASDM 소프트웨어 파일 이름은 asdm-762**.bin**과 같은 형식입니다.
	REST API 소프트웨어 사용 중인 *model(*모델*)* > **Adaptive Security Appliance REST API Plugin(Adaptive Security Appliance REST API** 플러그인**)** > *version(*버전*)*을 선택합니다.	API 소프트웨어 파일 이름은 asa-restapi-132-**lfbff-k8.SPA**와 같은 형식입니다. REST API를 설치하려면 API 빠른 시작 가이드를 참조하십시오.
	ROMMON 소프트웨어 사용 중인 *model(*모델*)* > **ASA Rommon Software(ASA Rommon** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	ROMMON 소프트웨어 파일 이름은 asa5500-firmware-1108**.SPA**와 같은 형식입니다.

ASA 모델	다운로드 위치	패키지
ASA 5512-X ~ ASA 5555-X	http://www.cisco.com/go/asa-software	
	ASA 소프트웨어 사용 중인 *model(*모델*)* > **Software on Chassis(**섀시의 소프트웨어**)** > **Adaptive Security Appliance(ASA) Software(ASA(Adaptive Security Appliance)** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	ASA 소프트웨어 파일 이름은 asa962-**smp-k8.bin**과 같은 형식입니다.
	ASDM 소프트웨어 사용 중인 *model(*모델*)* > **Software on Chassis(**섀시의 소프트웨어**)** > **Adaptive Security Appliance(ASA) Device Manager(ASA(Adaptive Security Appliance) Device Manager)** > *version(*버전*)*을 선택합니다.	ASDM 소프트웨어 파일 이름은 asdm-762**.bin**과 같은 형식입니다.
	REST API 소프트웨어 사용 중인 *model(*모델*)* > **Software on Chassis(**섀시의 소프트웨어**)** > **Adaptive Security Appliance REST API Plugin(Adaptive Security Appliance REST API** 플러그인**)** > *version(*버전*)*을 선택합니다.	API 소프트웨어 파일 이름은 asa-restapi-132-**lfbff-k8.SPA**와 같은 형식입니다. REST API를 설치하려면 API 빠른 시작 가이드를 참조하십시오.
	Cisco APIC(Application Policy Infrastructure Controller)용 **ASA** 디바이스 패키지 사용 중인 *model(*모델*)* > **Software on Chassis(**섀시의 소프트웨어**)** > **ASA for Application Centric Infrastructure (ACI) Device Packages(ACI(Application Centric Infrastructure)**용 **ASA** 디바이스 패키지**)** > *version(*버전*)*을 선택합니다.	APIC 1.2(7) 이상의 경우 Policy Orchestration with Fabric Insertion 또는 Fabric Insertion 전용 패키지를 선택합니다. 디바이스 패키지 소프트웨어 파일 이름은 asa-device-pkg-1.2.7.10**.zip**과 같은 형식입니다. ASA 디바이스 패키지를 설치하려면 Cisco APIC 레이어 4~레이어 7 서비스 구축 가이드의 "디바이스 패키지 가져오기" 장을 참조하십시오.

ASA 모델	다운로드 위치	패키지
ISA 3000	http://www.cisco.com/go/isa3000-software	
	ASA 소프트웨어 사용 중인 *model(*모델*)* > **Adaptive Security Appliance (ASA) Software(ASA(Adaptive Security Appliance)** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	ASA 소프트웨어 파일 이름은 asa962-**lfbff-k8.SPA**와 같은 형식입니다.
	ASDM 소프트웨어 사용 중인 *model(*모델*)* > **Adaptive Security Appliance (ASA) Device Manager(ASA(Adaptive Security Appliance) Device Manager)** > *version(*버전*)*을 선택합니다.	ASDM 소프트웨어 파일 이름은 asdm-762**.bin**과 같은 형식입니다.
	REST API 소프트웨어 사용 중인 *model(*모델*)* > **Adaptive Security Appliance REST API Plugin(Adaptive Security Appliance REST API** 플러그인**)** > *version(*버전*)*을 선택합니다.	API 소프트웨어 파일 이름은 asa-restapi-132-**lfbff-k8.SPA**와 같은 형식입니다. REST API를 설치하려면 API 빠른 시작 가이드를 참조하십시오.

ROMMON 이미지 업그레이드(ASA 5506-X, 5508-X 및 5516-X)

ASA 5506-X Series, ASA 5508-X 및 ASA 5516 X용 ROMMON 이미지를 업그레이드하려면 아래 단계를 수행합니다.

참고 Firepower Threat Defense로 이미지를 재설치한 후에는 ROMMON 이미지를 업그레이드할 수 없습니다.

시작하기 전에

새 버전으로 업그레이드만 가능하며 다운그레이드할 수 없습니다. 현재 버전을 보려면 **show module** 명령을 입력하고 MAC 주소 범위 테이블의 Mod 1에 대한 출력에서 Fw 버전을 확인하십시오.

```
ciscoasa# show module
[...]
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   1 7426.aceb.ccea to 7426.aceb.ccf2  0.3          1.1.5        9.4(1)
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

프로시저

단계 **1** Cisco.com에서 새 ROMMON 이미지를 가져와 ASA에 복사할 서버에 둡니다. 이 절차에서는 TFTP 복사에 대해 설명합니다.

다음 위치에서 이미지를 다운로드합니다.

https://software.cisco.com/download/type.html?mdfid=286283326&flowid=77251

단계 **2** ASA 플래시 메모리에 ROMMON 이미지를 복사합니다.

copy tftp://*server_ip***/asa5500-firmware-***xxxx***.SPA disk0:asa5500-firmware-***xxxx***.SPA**

단계 **3** ROMMON 이미지를 업그레이드합니다.

upgrade rommon disk0:asa5500-firmware-*xxxx***.SPA**

예제:

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af


Digital signature successfully validated
File Name                     : disk0:/asa5500-firmware-1108.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 553156F4
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

단계 **4** 프롬프트가 표시되면 ASA 다시 로드를 확인합니다.

ASA가 ROMMON 이미지를 업그레이드한 다음 ASA OS를 다시 로드합니다.

ASA를 Firepower Threat Defense 이미지로 재설치

ASA를 Firepower Threat Defense 소프트웨어 이미지로 재설치하려면 ROMMON 프롬프트에 액세스해야 합니다. ROMMON에서 Firepower Threat Defense 부트 이미지를 다운로드하려면 관리 인터페이

스에서 TFTP를 사용해야 하며 TFTP만 지원됩니다. 그런 다음 부트 이미지에서 HTTP 또는 FTP를 사용하여 Firepower Threat Defense 시스템 소프트웨어 설치 패키지를 다운로드할 수 있습니다. TFTP 다운로드에 시간이 오래 걸릴 수 있습니다. 패킷 손실을 방지하기 위해 ASA와 TFTP 서버 간에 연결이 안정적인지 확인합니다.

시작하기 전에

ASA를 이미지로 재설치하는 프로세스를 쉽게 수행하려면 다음과 같이 하십시오.

1. **backup** 명령을 사용하여 전체 시스템 백업을 수행합니다.

   자세한 내용과 기타 백업 기술은 컨피그레이션 가이드를 참조하십시오.

2. **show activation-key** 명령을 사용하여 라이선스를 재설치할 수 있도록 현재 액티베이션 키를 복사하고 저장합니다.

프로시저

단계 **1** 관리 인터페이스에 있는 ASA에서 액세스 가능한 TFTP 서버에 Firepower Threat Defense 부트 이미지(소프트웨어 다운로드, 2 페이지 참조)를 다운로드합니다.

ASA 5506-X, 5508-X, 5516-X, ISA 3000의 경우 관리 1/1 포트를 사용하여 이미지를 다운로드해야 합니다. 다른 모델의 경우, 모든 인터페이스를 사용할 수 있습니다.

단계 **2** 관리 인터페이스에 있는 ASA에서 액세스 가능한 HTTP 또는 FTP 서버에 Firepower Threat Defense 시스템 소프트웨어 설치 패키지(소프트웨어 다운로드, 2 페이지 참조)를 다운로드합니다.

단계 **3** 콘솔 포트에서 ASA를 다시 로드합니다.

reload

예제:

```
ciscoasa# reload
```

단계 **4** 부팅 중에 ROMMON 프롬프트와 연결하라는 메시지가 나타나면 **Esc** 키를 누릅니다.

모니터를 자세히 살펴봅니다.

예제:

```
[...]
Booting from ROMMON

Cisco Systems ROMMON Version (2.1(9)8) #1: Wed Oct 26 17:14:40 PDT 2011

Platform ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in   7 seconds.
```

이 시점에서 **Esc** 키를 누릅니다.

다음 메시지가 나타나고 너무 오래 기다린 경우 부팅을 완료한 후 ASA를 다시 로드해야 합니다.

```
Launching BootLoader...
Boot configuration file contains 2 entries.
[...]
```

단계 **5** 네트워크 설정을 설정하고 다음 ROMMON 명령을 사용하여 부트 이미지를 로드합니다.

a) **interface**- (ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X 전용) 관리 인터페이스 ID. 기타 모델은 항상 관리 1/1 인터페이스를 사용합니다.

b) **address**- 관리 인터페이스 IP 주소

c) **server**- TFTP 서버 IP 주소

d) **gateway**- 서버가 같은 네트워크에 있으면 이 IP 주소를 TFTP 서버 IP 주소와 동일하게 설정합니다.

e) **file**- TFTP 파일 경로 및 이름

f) **set**- (선택 사항) 네트워크 설정을 확인합니다. 또한 서버에 대한 연결성을 확인하기 위해 ping 명령을 사용할 수 있습니다.

g) **sync**- (선택 사항) 네트워크 설정을 저장합니다.

h) **tftpdnld**- 부트 이미지를 로드합니다.

예제**:**

ASA 5555-X의 예**:**

```
rommon #0> interface gigabitethernet0/0
rommon #1> address 10.86.118.4
rommon #2> server 10.86.118.21
rommon #3> gateway 10.86.118.21
rommon #4> file ftd-boot-latest.cdisk
rommon #5> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=ftd-boot-latest.cdisk
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon #6> sync

Updating NVRAM Parameters...

rommon #7> tftpdnld
```

ASA 5506-X의 예**:**

```
rommon #0> address 10.86.118.4
rommon #1> server 10.86.118.21
rommon #2> gateway 10.86.118.21
rommon #3> file ftd-boot-latest.lfbff
```

```
rommon #4> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  VLAN=untagged
  IMAGE=ftd-boot-latest.lfbff
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon #5> sync

Updating NVRAM Parameters...

rommon #6> tftpdnld
```

Firepower Threat Defense 부트 이미지가 다운로드되고 부트 CLI로 부팅됩니다.

단계 **6** **setup**을 입력하고 관리 인터페이스에서 시스템 소프트웨어 패키지를 다운로드 및 설치하기 위한 HTTP 또는 FTP 서버와의 임시 연결을 설정하도록 네트워크 설정을 구성합니다. 예를 들면 다음과 같습니다.

- 호스트 이름: **ftd1**
- IPv4 주소: **10.86.118.4**
- 넷마스크: **255.255.252.0**
- 게이트웨이: **10.86.116.1**
- DNS 서버: **10.86.116.5**
- Ntp 서버: **ntp.example.com**

단계 **7** Firepower Threat Defense 시스템 소프트웨어 설치 패키지를 다운로드합니다. 다음 단계는 HTTP 설치를 보여줍니다.

system install [**noconfirm**] *url*

예제**:**

```
> system install noconfirm http://10.86.118.21/ftd-6.0.1-949.pkg
```

확인 메시지에 응답하지 않으려면 **noconfirm** 옵션을 포함합니다.

단계 **8** 설치가 완료되고 디바이스 재부팅 옵션이 표시되면 **Yes(**예**)**를 선택합니다.

재부팅에는 30분 이상 소요되며 훨씬 더 오래 걸릴 수도 있습니다. 재부팅 시 사용자는 Firepower Threat Defense CLI에 있게 됩니다.

단계 **9** Firepower Device Manager 또는 Firepower Management Center를 사용하여 디바이스를 관리할 수 있습니다. 사용 중인 모델과 Manager용 빠른 시작 가이드(http://www.cisco.com/go/ftd-asa-quick)를 참조하여 설치를 계속합니다.

Firepower Threat Defense를 ASA 이미지로 재설치

Firepower Threat Defense를 ASA 소프트웨어 이미지로 재설치하려면 ROMMON 프롬프트에 액세스해야 합니다. ROMMON에서 디스크를 지운 다음 ASA 이미지를 다운로드하기 위해 관리 인터페이스에서 TFTP를 사용합니다. 이때 TFTP만 지원됩니다. ASA를 다시 로드한 후, 기본 설정을 구성한 다음 FirePOWER 모듈 소프트웨어를 로드할 수 있습니다.

시작하기 전에

- 패킷 손실을 방지하기 위해 ASA와 TFTP 서버 간에 연결이 안정적인지 확인합니다.

프로시저

단계 **1** Firepower Management Center에서 Firepower Threat Defense 디바이스를 관리하는 경우에는 Management Center에서 디바이스를 삭제합니다.

단계 **2** Firepower Device Manager를 사용하여 Firepower Threat Defense를 관리하는 경우, Smart Software Licensing 서버(Firepower Device Manager 또는 Smart Software Licensing 서버)에서 디바이스 등록을 취소해야 합니다.

단계 **3** 관리 인터페이스에 있는 Firepower Threat Defense 디바이스에서 액세스 가능한 TFTP 서버에 ASA 이미지(소프트웨어 다운로드, 2 페이지 참조)를 다운로드합니다.

ASA 5506-X, 5508-X, 5516-X, ISA 3000의 경우 관리 1/1 포트를 사용하여 이미지를 다운로드해야 합니다. 다른 모델의 경우, 모든 인터페이스를 사용할 수 있습니다.

단계 **4** 콘솔 포트에서 Firepower Threat Defense 디바이스를 재부팅합니다.

예제:

```
> reboot
This command will reboot the system.  Continue?
Please enter 'YES' or 'NO': yes
```

재부팅하려면 **yes**를 입력합니다.

단계 **5** 부팅 중에 ROMMON 프롬프트와 연결하라는 메시지가 나타나면 **Esc** 키를 누릅니다.

모니터를 자세히 살펴봅니다.

예제:

```
[...]
Booting from ROMMON

Cisco Systems ROMMON Version (2.1(9)8) #1: Wed Oct 26 17:14:40 PDT 2011
```

```
Platform ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in   7 seconds.
```

이 시점에서 **Esc** 키를 누릅니다.

다음 메시지가 나타나는 경우 너무 오래 기다렸다는 뜻이며, 부팅을 완료한 다음에 Firepower Threat Defense 디바이스를 다시 재부팅해야 합니다.

```
Launching BootLoader...
Boot configuration file contains 2 entries.
[...]
```

단계 **6** Firepower Threat Defense 디바이스에서 모든 디스크를 지웁니다. 내부 플래시를 disk0이라고 합니다. 외부 USB 드라이브가 있는 경우, disk1입니다.

예제**:**

```
Example:
rommon #0> erase disk0:

About to erase the selected device, this will erase
all files including configuration, and images.
Continue with erase? y/n [n]: y

Erasing Disk0:
.......................
[...]
```

이 단계에서는 ASA가 여러 가지 오류를 유발하는 잘못된 컨피그레이션 파일을 로드하려고 시도하지 않도록 Firepower Threat Defense 파일을 지웁니다.

단계 **7** 네트워크 설정을 지정하고 다음 ROMMON 명령을 사용하여 ASA 이미지를 로드합니다.

interface *interface_id*

address *management_ip_address*

server *tftp_ip_address*

gateway *gateway_ip_address*

file*path/filename*

set

sync

tftpdnld

ASA 이미지가 다운로드되고 CLI에 부팅됩니다.

다음 정보를 참조하십시오.

- **interface**- (ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X 전용) 관리 인터페이스 ID를 지정합니다. 기타 모델은 항상 관리 1/1 인터페이스를 사용합니다.
- **gateway**- 게이트웨이 주소가 서버 IP 주소와 같은 네트워크에 있으면 두 주소를 동일하게 설정합니다.
- **set**- 네트워크 설정을 표시합니다. 또한 서버에 대한 연결성을 확인하기 위해 **ping** 명령을 사용할 수 있습니다.
- **sync**- 네트워크 설정을 저장합니다.
- **tftpdnld**- 부트 이미지를 로드합니다.

예제:

ASA 5555-X의 예:

```
rommon #2> interface gigabitethernet0/0
rommon #3> address 10.86.118.4
rommon #4> server 10.86.118.21
rommon #5> gateway 10.86.118.21
rommon #6> file asalatest-smp-k8.bin
rommon #7> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asalatest-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

rommon #8> sync

Updating NVRAM Parameters...

rommon #9> tftpdnld
```

ASA 5506-X의 예:

```
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asalatest-lfbff-k8.SPA
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  VLAN=untagged
  IMAGE=asalatest-lfbff-k8.SPA
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

```
rommon #7> sync

Updating NVRAM Parameters...

rommon #8> tftpdnld
```

단계 **8** 네트워크 설정을 구성하고 디스크를 준비합니다.

ASA가 처음으로 부팅될 때는 컨피그레이션이 없습니다. ASDM 액세스를 위해 관리 인터페이스를 구성하려면 인터랙티브 프롬프트를 따르거나 저장된 컨피그레이션을 붙여 넣을 수 있습니다. 또는 저장된 컨피그레이션이 없는 경우, 권장되는 컨피그레이션(아래)을 붙여 넣을 수 있습니다.

저장된 컨피그레이션이 없는 경우, ASA FirePOWER 모듈을 사용할 계획이라면 권장되는 컨피그레이션을 붙여넣는 것이 좋습니다. ASA FirePOWER 모듈은 관리 인터페이스에서 관리되며 업데이트를 위해 인터넷에 연결해야 합니다. 간단한 권장되는 네트워크 구축은 관리에 연결해주는 내부 스위치(FirePOWER 관리 전용), 내부 인터페이스(ASA 관리 및 내부 트래픽용) 및 동일한 내부 네트워크에 대한 관리 PC를 포함합니다. 네트워크 구축에 대한 자세한 내용은 빠른 시작 가이드를 참조하십시오.

- http://www.cisco.com/go/asa5506x-quick
- http://www.cisco.com/go/asa5508x-quick
- http://www.cisco.com/go/asa5500x-quick

a) ASA 콘솔 프롬프트에서 관리 인터페이스에 대한 몇 가지 컨피그레이션을 입력할지 묻는 프롬프트가 표시됩니다.

```
Pre-configure Firewall now through interactive prompts [yes]?
```

컨피그레이션을 붙여 넣거나 동일한 네트워크 구축을 위해 권장되는 컨피그레이션을 생성하려면 **no**를 입력하고 절차를 계속 진행합니다.

관리 인터페이스를 구성하려는 경우, ASDM에 연결할 수 있으며 **yes**를 입력하고 프롬프트에 따라 작업을 수행합니다.

b) 콘솔 프롬프트에서 권한 있는 EXEC 모드에 액세스합니다.

enable

다음 프롬프트가 나타납니다.

```
Password:
```

c) **Enter**를 누릅니다. 기본적으로 비밀번호는 비어 있습니다.

d) 전역 컨피그레이션 모드에 액세스합니다.

configure terminal

e) 인터랙티브 프롬프트를 사용하지 않은 경우, 프롬프트에서 컨피그레이션을 복사하여 붙여 넣습니다.

저장된 컨피그레이션이 없으나 빠른 시작 가이드에 설명된 대로 간단한 컨피그레이션을 사용하려는 경우, 프롬프트에서 다음 컨피그레이션을 복사하여 IP 주소 및 인터페이스 ID를 알맞게 변경하십시오. 프롬프트를 사용했지만 이 컨피그레이션을 대신 사용하려는 경우, **clear configure all** 명령을 사용하여 컨피그레이션을 먼저 지웁니다.

```
interface gigabitethernetn/n
   nameif outside
   ip address dhcp setroute
   no shutdown
interface gigabitethernetn/n
   nameif inside
   ip address ip_address netmask
   security-level 100
   no shutdown
interface managementn/n
   no shutdown
object network obj_any
   subnet 0 0
   nat (any,outside) dynamic interface
http server enable
http inside_network netmask inside
dhcpd address inside_ip_address_start-inside_ip_address_end inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

ASA 5506W-X의 경우, wifi 인터페이스에 대해 다음을 추가합니다.

```
same-security-traffic permit inter-interface
interface GigabitEthernet 1/9
security-level 100
nameif wifi
ip address ip_address netmask
no shutdown
http wifi_network netmask wifi
dhcpd address wifi_ip_address_start-wifi_ip_address_end wifi
dhcpd enable wifi
```

f) 디스크를 다시 포맷합니다.

format disk0:

format disk1:

내부 플래시를 disk0이라고 합니다. 외부 USB 드라이브가 있는 경우, disk1입니다. 디스크를 다시 포맷하지 않는 경우, ASA 이미지를 복사하려고 시도할 때 다음 오류가 표시됩니다.

```
%Error copying ftp://10.86.89.125/asa971-smp-k8.bin (Not enough space on device)
```

g) 새 컨피그레이션을 저장합니다.

write memory

단계 **9** ASA 및 ASDM 이미지를 설치합니다.

ROMMON 모드에서 ASA를 부팅해도 다시 로드를 통해 시스템 이미지가 보존되지 않습니다. 플래시 메모리에 이미지를 계속해서 다운로드해야 합니다. 또한 플래시 메모리에 ASDM을 다운로드해야 합니다.

a) ASA 및 ASDM 이미지(소프트웨어 다운로드, 2 페이지 참조)를 ASA에서 액세스 가능한 서버에 다운로드합니다. ASA는 여러 서버 유형을 지원합니다. 자세한 내용은 **copy** 명령(http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/A-H/cmdref1/c4.html#pgfId-2171368)을 참조하십시오.

b) ASA 플래시 메모리에 ASA 이미지를 복사합니다. 다음 단계는 FTP 복사를 보여줍니다.

copy ftp://*user***:***password***@***server_ip***/***asa_file***disk0:***asa_file*

예제:

```
ciscoasa# copy ftp://admin:test@10.86.118.21/asa961-smp-k8.bin disk0:asa961-smp-k8.bin
```

c) ASA 플래시 메모리에 ASDM 이미지를 복사합니다. 다음 단계는 FTP 복사를 보여줍니다.

copy ftp://*user***:***password***@***server_ip***/***asdm_file***disk0:***asdm_file*

예제:

```
ciscoasa# copy ftp://admin:test@10.86.118.21/asdm-761.bin disk0:asdm-761.bin
```

d) ASA를 다시 로드합니다.

reload

disk0의 이미지를 사용하여 ASA를 다시 로드합니다.

단계 **10** (선택 사항) ASA FirePOWER 모듈 소프트웨어를 설치합니다.

이 절차에 따라 ASA FirePOWER 부트 이미지를 설치하고 SSD를 분할하며 시스템 소프트웨어를 설치해야 합니다.

a) 부트 이미지를 ASA에 복사합니다. 시스템 소프트웨어를 전송하지 마십시오. 나중에 SSD로 다운로드됩니다. 다음 단계는 FTP 복사를 보여줍니다.

copy ftp://*user***:***password***@***server_ip***/***firepower_boot_file***disk0:***firepower_boot_file*

예제:

```
ciscoasa# copy ftp://admin:test@10.86.118.21/asasfr-5500x-boot-6.0.1.img
disk0:/asasfr-5500x-boot-6.0.1.img
```

b) Cisco.com의 ASA FirePOWER Services 시스템 소프트웨어 설치 패키지를 관리 인터페이스에서 액세스할 수 있는 HTTP, HTTPS 또는 FTP 서버에 다운로드합니다. ASA의 disk0에 다운로드하지 마십시오.

c) ASA disk0에서 ASA FirePOWER 모듈 부트 이미지 위치를 설정합니다.

sw-module module sfr recover configure image disk0:*file_path*

예제:

```
ciscoasa# sw-module module sfr recover configure image disk0:asasfr-5500x-boot-6.0.1.img
```

d) ASA FirePOWER 부트 이미지를 로드합니다.

sw-module module sfr recover boot

예제:

```
ciscoasa# sw-module module sfr recover boot

Module sfr will be recovered. This may erase all configuration and all data
on that device and attempt to download/install a new image for it. This may take
several minutes.

Recover module sfr? [confirm] y
Recover issued for module sfr.
```

e) ASA FirePOWER 모듈이 부팅할 때까지 몇 분 정도 기다린 후 현재 실행 중인 ASA FirePOWER 부트 이미지에 대한 콘솔 세션을 엽니다. 로그인 프롬프트로 이동하려면 세션을 연 후 **Enter** 키를 눌러야 할 수 있습니다. 기본 사용자 이름은 **admin**이고 기본 비밀번호는 **Admin123**입니다.

예제:

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

asasfr login: admin
Password: Admin123
```

모듈 부트가 완료되지 않을 경우 session 명령이 실패하고 ttyS1을 통해 연결할 수 없다는 메시지가 표시됩니다. 기다렸다가 다시 시도하십시오.

a) 시스템 소프트웨어 설치 패키지를 설치할 수 있도록 시스템을 구성합니다.

setup

다음에 대한 프롬프트가 표시됩니다. 관리 주소, 게이트웨이 및 DNS 정보는 컨피그레이션을 위한 핵심 설정입니다.

- 호스트 이름 - 공백 없이 영숫자 최대 65자를 사용합니다. 하이픈은 허용됩니다.
- 네트워크 주소 - 고정 IPv4 또는 IPv6 주소를 사용하거나, DHCP(IPv4용) 또는 IPv6 상태 비저장 자동 컨피그레이션을 설정할 수 있습니다.
- DNS 정보 - 하나 이상의 DNS 서버를 지정해야 합니다. 도메인 이름 및 검색 도메인도 설정할 수 있습니다.
- NTP 정보 - NTP를 활성화하고, 시스템 시간 설정을 위해 NTP 서버를 구성할 수 있습니다.

예제:

```
asasfr-boot> setup
```

```
Welcome to Cisco FirePOWER Services Setup
[hit Ctrl-C to abort]
Default values are inside []
```

a) 다음을 입력하여 시스템 소프트웨어 설치 패키지를 설치합니다.

system install [**noconfirm**] *url*

확인 메시지에 응답하지 않으려면 **noconfirm** 옵션을 포함합니다. HTTP, HTTPS 또는 FTP URL을 사용합니다. 사용자 이름과 비밀번호가 필요한 경우 입력하라는 메시지가 표시됩니다. 파일이 큰 경우 네트워크 상태에 따라 다운로드하는 데 시간이 오래 걸릴 수 있습니다.

설치가 완료되면 시스템이 다시 부팅됩니다. 애플리케이션 구성 요소 설치 및 ASA FirePOWER Services 시작에 필요한 시간은 매우 다릅니다. 최첨단 플랫폼은 10분 이상의 시간이 걸리지만 사양이 낮은 플랫폼은 60~80분 이상이 소요될 수 있습니다. **show module sfr** 출력에 모든 프로세스가 Up으로 표시되어야 합니다.

예제:

```
asasfr-boot> system install
http://admin:pa$$wd@upgrades.example.com/packages/asasfr-sys-6.0.1-58.pkg
Verifying
Downloading
Extracting
Package Detail
        Description:                    Cisco ASA-FirePOWER 6.0.1-58 System Install
        Requires reboot:                Yes

Do you want to continue with upgrade? [y]: y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Upgrading
Starting upgrade process ...
Populating new system image

Reboot is required to complete the upgrade. Press 'Enter' to reboot the system. [type
Enter]
Broadcast message from root (ttyS1) (Mon Feb 17 19:28:38 2016):

The system is going down for reboot NOW!
Console session with module sfr terminated.
```

a) 패치 릴리스를 설치해야 하는 경우, 관리자(ASDM 또는 Firepower Management Center)에서 나중에 수행할 수 있습니다.

단계 **11** 액티베이션 키를 저장하지 않은 기존 ASA로 Strong Encryption 라이선스 및 기타 라이선스를 받습니다. 자세한 내용은 http://www.cisco.com/go/license를 참조하십시오. **Manage(관리)** > **Licenses(라이선스)** 섹션에서 라이선스를 다시 다운로드할 수 있습니다.

ASDM(및 기타 다른 기능)을 사용하려면 강력한 암호화(3DES/AES) 라이선스를 설치해야 합니다. 이전에 Firepower Threat Defense 디바이스를 이미지로 재설치하기 전에 이 ASA의 라이선스 액티베이션 키를 저장한 경우, 액티베이션 키를 재설치할 수 있습니다. 액티베이션 키를 저장하지 않았지만 이 ASA에 대해 라이선스를 소유한 경우, 이 라이선스를 다시 다운로드할 수 있습니다. 새로운 ASA의 경우, 새로운 ASA 라이선스를 요청해야 합니다.

단계 **12** 새 ASA용 라이선스를 받습니다.

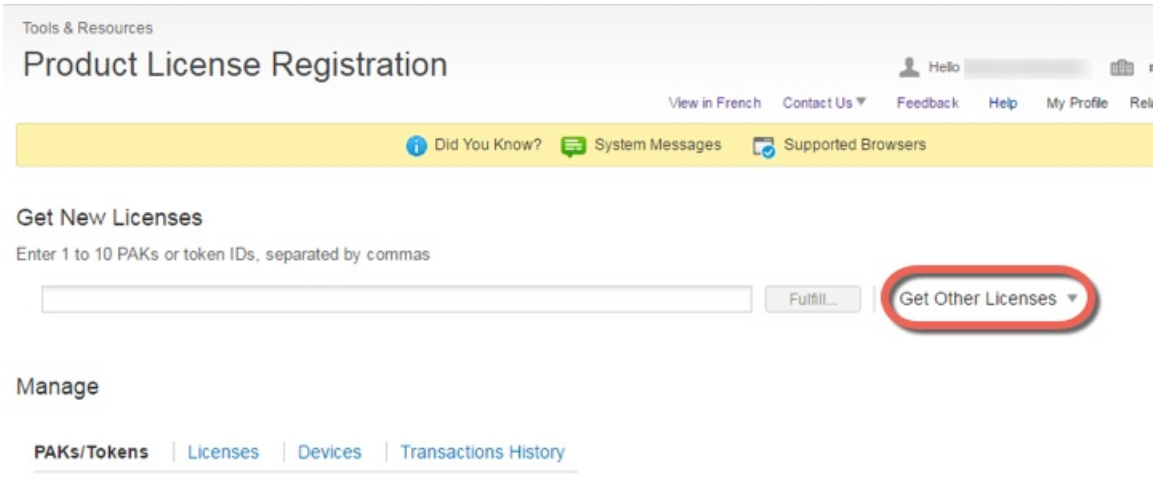
a) 다음 명령을 입력하여 ASA의 시리얼 번호를 가져옵니다.

show version | grep Serial

이 시리얼 번호는 하드웨어 외부에 인쇄된 섀시 시리얼 번호와는 다릅니다. 섀시 시리얼 번호는 기술 지원에 사용되지만 라이선싱에 대해서는 사용되지 않습니다.

b) http://www.cisco.com/go/license를 확인한 후 **Get Other Licenses(**다른 라이선스 가져오기**)**를 클릭합니다.

그림 ***1:*** 다른 라이선스 가져오기

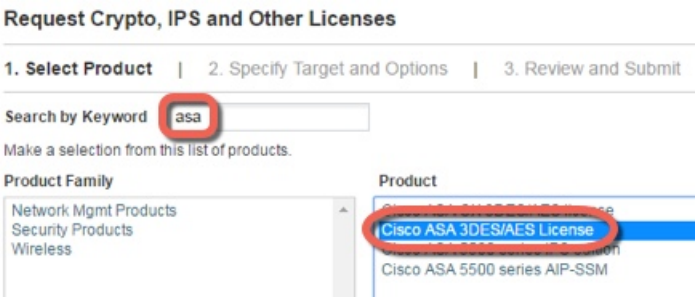


c) **IPS, Crypto, Other(IPS,** 암호화**,** 기타**)**를 선택합니다.

그림 ***2: IPS,*** 암호화, 기타

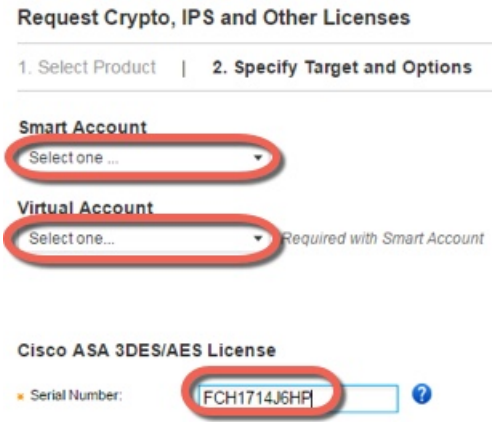
d) **Search by Keyword(**키워드별 검색**)** 필드에서 **asa**를 입력하고 **Cisco ASA 3DES/AES License(Cisco ASA 3DES/AES** 라이선스**)**를 선택합니다.

그림 *3: Cisco ASA 3DES/AES* 라이선스



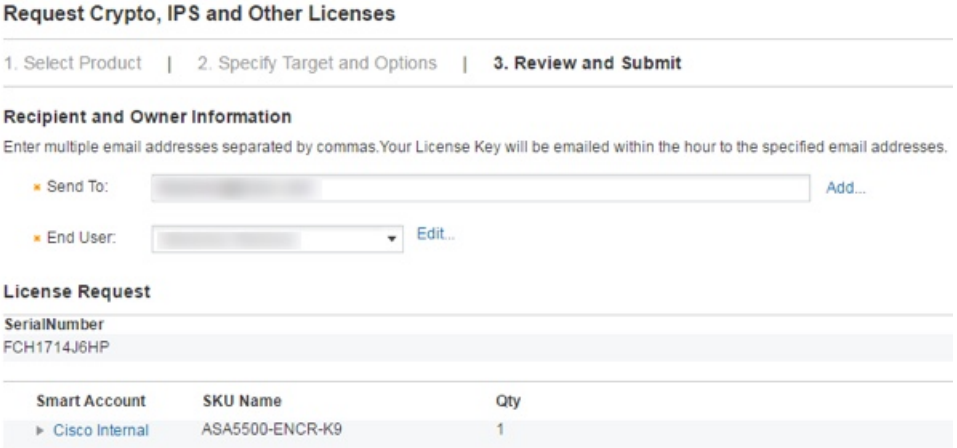
e) **Smart Account**(스마트 어카운트), **Virtual Account**(가상 어카운트)를 선택하고 ASA **Serial Number**(시리얼 번호)를 입력한 후에 **Next**(다음)를 클릭합니다.

그림 *4:* 스마트 어카운트, 가상 어카운트, 및 시리얼 번호



f) 이메일 전송 주소 및 최종 사용자 이름이 자동으로 채워집니다. 필요 시 추가 이메일 주소를 입력합니다. **I Agree**(동의합니다.) 확인란을 선택하고 **Submit**(제출)을 클릭합니다.

그림 *5:* 제출



g) 그러면 액티베이션 키가 포함된 이메일이 수신됩니다. 하지만 **Manage(관리)** > **Licenses(라이선스)** 영역에서 키를 즉시 다운로드할 수도 있습니다.

h) 기본 라이선스에서 Security Plus 라이선스로 업그레이드하거나 AnyConnect 라이선스를 구매하려는 경우 http://www.cisco.com/go/ccw를 참조하십시오. 라이선스를 구매하면 http://www.cisco.com/go/license에서 입력할 수 있는 PAK(제품 인증 키)가 포함된 이메일을 받게 됩니다. AnyConnect 라이선스의 경우, 사용자 세션의 동일한 풀을 사용하는 여러 ASA에 적용할 수 있는 다용도의 PAK를 받습니다. 결과 액티베이션 키는 영구 라이선스(3DES/AES 포함)에 현재까지 등록한 모든 기능을 포함합니다. 기간별 라이센스의 경우, 각 라이센스에는 별도의 액티베이션 키가 있습니다.

단계 **13** 액티베이션 키를 적용합니다.

activation-key *key*

예제**:**

```
ciscoasa(config)# activation-key 7c1aff4f e4d7db95 d5e191a4 d5b43c08 0d29c996
Validating activation key. This may take a few minutes...
Failed to retrieve permanent activation key.
Both Running and Flash permanent activation key was updated with the requested key.
```

이 ASA에서 아직 액티베이션 키를 설치하지 않았으므로 "Failed to retrieve permanent activation key.(영구 액티베이션 키를 검색하는 데 실패했습니다.)" 메시지가 표시됩니다. 이 메시지는 무시하셔도 됩니다.

하나의 영구 키만 설치하고, 여러 개의 기간별 키를 설치할 수 있습니다. 새 영구 키를 입력하면 이전에 설치한 키를 덮어씁니다. 3DES/AES 라이선스를 설치한 후에 추가 라이선스를 주문한 경우, 통합된 액티베이션 키는 3DES/AES 라이선스 외에 모든 라이선스를 포함하므로 3DES/AES 전용 키를 덮어쓸 수 있습니다.

단계 **14** ASA FirePOWER 모듈은 ASA에서 제공되는 별도의 라이선싱 메커니즘을 사용합니다. 라이선스를 미리 설치하지 않았지만 주문에 따라 이 상자는 다음 라이선스에 대한 라이선스 액티베이션 키를 다운로드할 수 있도록 인쇄물에 PAK를 포함할 수 있습니다.

- **Control and Protection(**제어 및 보호**)**. 제어는 "AVC(Application Visibility and Control)" 또는 "앱"이라고도 합니다. 보호는 "IPS"라고도 합니다. 이 라이선스에 대한 액티베이션 키 외에 이러한 기능에 대한 자동화된 업데이트를 위해 "사용 권한" 서브스크립션이 필요합니다.

  Control(제어**)**(AVC) 업데이트는 Cisco 지원 계약에 포함됩니다.

  Protection(보호**)**(IPS) 업데이트의 경우 http://www.cisco.com/go/ccw에서 IPS 서브스크립션을 구매해야 합니다. 이 서브스크립션은 규칙, 엔진, 취약점, 지리적 위치 업데이트에 대한 자격을 포함합니다. 참고**:** 사용 권한 서브스크립션은 ASA FirePOWER 모듈용 PAK/라이선스 액티베이션 키를 생성하거나 요구하지 않으며 업데이트 사용 권한만 제공합니다.

ASA FirePOWER Services를 포함하는 ASA 5500-X를 구매하지 않은 경우, 필요한 라이선스를 다운로드하기 위해 업그레이드 번들을 구매할 수 있습니다. 자세한 내용은 Cisco ASA with FirePOWER Services 주문 가이드를 참조하십시오.

구매할 수 있는 기타 라이선스는 다음과 같습니다.

- **AMP(Advanced Malware Protection)**

- **URL** 필터링

이 라이선스는 ASA FirePOWER 모듈용 PAK/라이선스 액티베이션 키를 생성합니다. 주문 정보는 Cisco ASA with FirePOWER Services 주문 가이드를 참조하십시오. Cisco Firepower System 기능 라이선스도 참조하십시오.

제어 및 보호 라이선스 및 기타 선택적인 라이선스를 설치하려면, 사용 중인 모델별 ASA 빠른 시작 가이드를 참조하십시오.

Firepower 2100 Series 이미지 재설치

Firepower 2100 Series는 Firepower Threat Defense 또는 ASA 소프트웨어를 지원합니다.

- 소프트웨어 다운로드, 23 페이지
- ASA를 Firepower Threat Defense 이미지로 재설치, 24 페이지
- Firepower Threat Defense를 ASA 이미지로 재설치, 29 페이지

소프트웨어 다운로드

Firepower Threat Defense 소프트웨어 또는 ASA 소프트웨어를 다운로드합니다. 이 문서의 절차상 초기 다운로드를 위해 TFTP 서버에 소프트웨어를 둬야 합니다. 다른 이미지는 기타 서버 유형(예: HTTP 또는 FTP)에서 다운로드할 수 있습니다. 정확한 소프트웨어 패키지 및 서버 유형의 경우, 절차를 참조하십시오.

참고 Cisco.com 로그인 및 Cisco 서비스 계약이 필요합니다.

표 *3: Firepower Threat Defense* 소프트웨어

Firepower Threat Defense 모델	다운로드 위치	패키지
Firepower 2100 Series	참조 페이지: https://www.cisco.com/go/ftd-software	
	Firepower Threat Defense 패키지 사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	패키지의 파일 이름은 cisco-ftd-fp2k.6.2.2.**SPA**와 같은 형식입니다.

표 *4: ASA* 소프트웨어

ASA 모델	다운로드 위치	패키지
Firepower 2100 Series	참조 페이지: https://www.cisco.com/go/asa-firepower-sw	
	ASA 패키지 사용 중인 *model(*모델*)* > **Adaptive Security Appliance (ASA) Software(ASA(Adaptive Security Appliance)** 소프트웨어**)** > *version(*버전*)*을 선택합니다.	패키지의 파일 이름은 cisco-asa-fp2k.9.8.2.**SPA**와 같은 형식입니다. 이 패키지에는 ASA, ASDM, FXOS 및 Firepower Chassis Manager가 포함되어 있습니다.
	ASDM 소프트웨어**(**업그레이드**)** 현재 ASDM 또는 ASA CLI를 사용하여 최신 버전의 ASDM으로 업그레이드하려면 사용 중인 *model(*모델*)* > **Adaptive Security Appliance(ASA) Device Manager(ASA(Adaptive Security Appliance) Device Manager)** > *version(*버전*)*을 선택합니다.	ASDM 소프트웨어 파일 이름은 asdm-782**.bin**과 같은 형식입니다.

ASA를 Firepower Threat Defense 이미지로 재설치

Firepower 2100의 ASA를 Firepower Threat Defense 소프트웨어 이미지로 재설치하려면 ROMMON 프롬프트에 액세스해야 합니다. ROMMON에서 디스크를 지운 다음 관리 1/1 인터페이스에서 TFTP를 사용하여 Firepower Threat Defense 패키지에서 FXOS를 로드합니다. 이때 TFTP만 지원됩니다. FXOS를 처음 부팅한 후에 네트워크 설정을 구성하고, 선택한 서버에서 Firepower Threat Defense 패키지를 다운로드한 후에 FXOS를 재부팅합니다.

프로시저

단계 **1** Smart Software Licensing 서버(ASA CLI/ASDM 또는 Smart Software Licensing 서버)에서 ASA 등록을 취소합니다.

단계 **2** 관리 1/1 인터페이스에 있는 ASA에서 액세스 가능한 TFTP 서버에 Firepower Threat Defense 이미지(소프트웨어 다운로드, 23 페이지 참조)를 다운로드합니다.

단계 **3** 콘솔 포트에서 FXOS에 **admin**으로 로그인하여 시스템을 다시 포맷합니다.

connect local-mgmt

format everything

```
firepower-2110# connect local-mgmt
firepower-2110(local-mgmt)# format everything
All configuration and bootable images will be lost.
Do you still want to format? (yes/no):yes
```

yes를 입력하면 Firepower 2100이 재부팅됩니다.

단계 **4** 부팅 중에 ROMMON 프롬프트와 연결하라는 메시지가 나타나면 **Esc** 키를 누릅니다. 모니터를 자세히 살펴봅니다.

예제**:**

```
********************************************************************************
Cisco System ROMMON, Version 1.0.03, RELEASE SOFTWARE
Copyright (c) 1994-2017  by Cisco Systems, Inc.
Compiled Thu 04/06/2017 12:16:16.21 by builder
********************************************************************************

Current image running: Boot ROM0
Last reset cause: ResetRequest
DIMM_1/1 : Present
DIMM_2/1 : Present

Platform FPR-2130 with 32768 MBytes of main memory
BIOS has been successfully locked !!
MAC Address: 0c:75:bd:08:c9:80

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

이 시점에서 **Esc** 키를 누릅니다. 중단 프롬프트에서 Esc 키를 누르지 않으면 Firepower 2100에는 이미지가 없으며 ROMMON만 사용 가능하므로 재부팅을 3회 시도합니다.

단계 **5** 관리 1/1용 네트워크 설정을 지정하고 다음 ROMMON 명령을 사용하여 Firepower Threat Defense 패키지의 일부분인 FXOS를 로드합니다.

address *management_ip_address*

netmask *subnet_mask*

server *tftp_ip_address*

gateway *gateway_ip_address*

file*path/filename*

set

sync

tftp -b

FXOS 이미지가 다운로드되고 CLI에 부팅됩니다.

다음 정보를 참조하십시오.

- **gateway**- 게이트웨이 주소가 서버 IP 주소와 같은 네트워크에 있으면 두 주소를 동일하게 설정합니다.
- **set**- 네트워크 설정을 표시합니다. 또한 서버에 대한 연결성을 확인하기 위해 **ping** 명령을 사용할 수 있습니다.
- **sync**- 네트워크 설정을 저장합니다.
- **tftp -b**- FXOS를 로드합니다.

예제:

```
rommon 1> address 10.86.118.4
rommon 2> netmask 255.255.252.0
rommon 3> server 10.86.118.21
rommon 4> gateway 10.86.118.21
rommon 5> file cisco-ftd-fp2k.6.2.2.SPA
rommon 6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.4
  NETMASK=255.255.252.0
  GATEWAY=10.86.118.21
  SERVER=10.86.118.21
  IMAGE=cisco-ftd-fp2k.6.2.2.SPA
  CONFIG=
  PS1="rommon ! > "

rommon 7> sync
rommon 8> tftp -b
Enable boot bundle: tftp_reqsize = 268435456

             ADDRESS: 10.86.118.4
             NETMASK: 255.255.252.0
             GATEWAY: 10.86.118.21
              SERVER: 10.86.118.21
               IMAGE: cisco-asa-fp2k.9.8.2.SPA
             MACADDR: d4:2c:44:0c:26:00
           VERBOSITY: Progress
               RETRY: 40
          PKTTIMEOUT: 7200
             BLKSIZE: 1460
            CHECKSUM: Yes
                PORT: GbE/1
             PHYMODE: Auto Detect

link up
Receiving cisco-ftd-fp2k.6.2.2.SPA from 10.86.118.21!!!!!!!!
[…]
```

단계 **6** 기본 사용자 이름인 **admin**과 비밀번호인 **Admin123**을 사용하여 FXOS에 로그인합니다.

디바이스가 FXOS에 부팅되면 ROMMON에서 설정한 관리 IP 주소가 지워지고 기본값인 192.168.45.45로 설정됩니다. FXOS에서 네트워크의 정확한 IP 주소 및 기타 관련 설정을 지정해야 서버에서 Firepower Threat Defense 패키지를 다운로드할 수 있습니다.

단계 **7** DHCP 서버를 비활성화합니다.

scope system

scope services

disable dhcp-server

commit-buffer

관리 IP 주소를 변경하려면 DHCP 서버를 비활성화해야 합니다.

예제:

```
firepower-2110# scope system
firepower-2110 /system # scope services
```

```
firepower-2110 /system/services # disable dhcp-server
firepower-2110 /system/services* # commit-buffer
```

단계 **8** IPv4 관리 IP 주소를 구성하고 필요한 경우 게이트웨이를 구성합니다.

scopefabric-interconnecta

setout-of-band staticip *ip_address***netmask** *network_mask***gw** *gateway_ip_address*

commit-buffer

현재 설정되어 있는 게이트웨이(기본적으로 0.0.0.0, Firepower Threat Defense 데이터 인터페이스를 나타냄)를 유지하려면 **gw** 키워드를 생략합니다. 다운로드 서버가 로컬 관리 1/1 네트워크에 있지 않으면 게이트웨이 IP 주소를 변경합니다. Firepower Threat Defense 데이터 인터페이스는 아직 없으므로 기본 설정으로는 원격 서버에 연결할 수 없습니다.

예제**:**

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect #
firepower-2100 /fabric-interconnect # set out-of-band ip 10.86.118.4 netmask 255.255.255.0

Warning: When committed, this change may disconnect the current CLI session
firepower-2100 /fabric-interconnect* # commit-buffer
firepower-2100 /fabric-interconnect #
```

단계 **9** Firepower Threat Defense 패키지를 다운로드하여 부팅합니다.

a) 패키지를 다운로드합니다.

scope firmware

download image *url*

show download-task

이전에 사용했던 것과 같은 TFTP 서버나 관리 1/1에서 연결할 수 있는 다른 서버에서 패키지를 다운로드할 수 있습니다.

예제**:**

```
firepower-2110# scope firmware
firepower-2110 /firmware # download image tftp://10.86.118.21/cisco-ftd-fp2k.6.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
firepower-2110 /firmware # show download-task
Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-ftd-fp2k.6.2.2.SPA
              Tftp     10.88.29.21             0                 Downloaded
```

b) 패키지 다운로드가 완료되면(**Downloaded(**다운로드됨**)** 상태) 패키지를 부팅합니다.

show package

scope auto-install

install security-pack version *version*

show package 출력에서 **security-pack version** 번호용으로 **Package-Vers** 값을 복사합니다. 섀시에 Firepower Threat Defense 이미지가 설치되고 섀시가 재부팅됩니다.

예제:

```
firepower 2110 /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-ftd-fp2k.6.2.2.SPA                   6.2.2
firepower 2110 /firmware # scope auto-install
firepower 2110 /firmware/auto-install # install security-pack version 6.2.2
The system is currently installed with security software package not set, which has:
   - The platform version: not set
If you proceed with the upgrade 6.2.2, it will do the following:
   - upgrade to the new platform version 2.2.2.52
   - install with CSP ftd version 6.2.2
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
   If you proceed the system will be re-imaged. All existing configuration will be lost,

   and the default configuration applied.
Do you want to proceed? (yes/no):yes

Triggered the install of software package version 6.2.2
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
```

단계 **10** 섀시 재부팅이 완료될 때까지 5~10분 정도 기다렸다가 기본 사용자 이름인 **admin**과 비밀번호인 **Admin123**을 사용하여 FXOS에 로그인합니다.

FXOS이 작동하더라도 Firepower Threat Defense가 작동할 때까지 30분 동안 기다려야 합니다. 다음 메시지가 나타날 때까지 기다립니다.

```
[…]
User enable_1 logged in to firepower
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
firepower> Aug 26 01:31:48 firepower port-manager: Alert: Ethernet1/2 link changed to DOWN
Aug 26 01:31:48 firepower port-manager: Alert: Ethernet1/1 link changed to DOWN

firepower#
```

나머지 Firepower Threat Defense 시작 메시지가 표시되고 나면 FXOS 프롬프트로 돌아올 수 있습니다.

단계 **11** Firepower Threat Defense CLI에 연결합니다.

connect ftd

단계 **12** EULA에 동의하라는 프롬프트가 표시됩니다. **Enter** 키를 누른 후 다음 프롬프트가 표시될 때까지 **More(자세히)** 프롬프트에서 스페이스바를 누릅니다.

```
Please enter 'YES' or press <ENTER> to AGREE to the EULA:
```

yes를 입력합니다.

단계 **13** 비밀번호를 변경하고 초기 설정을 수행하라는 프롬프트가 표시됩니다. Firepower Device Manager 또는 Firepower Management Center 빠른 시작 가이드를 참조하여 시스템을 구성합니다.

Firepower Threat Defense를 ASA 이미지로 재설치

Firepower 2100의 Firepower Threat Defense를 ASA 소프트웨어 이미지로 재설치하려면 ROMMON 프롬프트에 액세스해야 합니다. ROMMON에서 디스크를 지운 다음 관리 1/1 인터페이스에서 TFTP를 사용하여 ASA 패키지에서 FXOS를 로드합니다. 이때 TFTP만 지원됩니다. FXOS를 처음 부팅한 후에 네트워크 설정을 구성하고, 선택한 서버에서 ASA 패키지를 다운로드한 후에 FXOS를 재부팅합니다.

프로시저

단계 **1** Firepower Management Center에서 Firepower Threat Defense 디바이스를 관리하는 경우에는 Management Center에서 디바이스를 삭제합니다.

단계 **2** Firepower Device Manager를 사용하여 Firepower Threat Defense를 관리하는 경우, Smart Software Licensing 서버(Firepower Device Manager 또는 Smart Software Licensing 서버)에서 디바이스 등록을 취소해야 합니다.

단계 **3** 관리 1/1 인터페이스에 있는 Firepower Threat Defense 디바이스에서 액세스 가능한 TFTP 서버에 ASA 이미지(소프트웨어 다운로드, 23 페이지 참조)를 다운로드합니다.

단계 **4** 콘솔 포트에서 FXOS에 **admin**으로 로그인하여 시스템을 다시 포맷합니다.

connect local-mgmt

format everything

```
firepower-2110# connect local-mgmt
firepower-2110(local-mgmt)# format everything
All configuration and bootable images will be lost.
Do you still want to format? (yes/no):yes
```

yes를 입력하면 Firepower 2100이 재부팅됩니다.

단계 **5** 부팅 중에 ROMMON 프롬프트와 연결하라는 메시지가 나타나면 **Esc** 키를 누릅니다. 모니터를 자세히 살펴봅니다.

예제:

```
********************************************************************************
Cisco System ROMMON, Version 1.0.03, RELEASE SOFTWARE
Copyright (c) 1994-2017  by Cisco Systems, Inc.
Compiled Thu 04/06/2017 12:16:16.21 by builder
```

```
********************************************************************************

Current image running: Boot ROM0
Last reset cause: ResetRequest
DIMM_1/1 : Present
DIMM_2/1 : Present

Platform FPR-2130 with 32768 MBytes of main memory
BIOS has been successfully locked !!
MAC Address: 0c:75:bd:08:c9:80

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

이 시점에서 **Esc** 키를 누릅니다. 중단 프롬프트에서 Esc 키를 누르지 않으면 Firepower 2100에는 이미지가 없으며 ROMMON만 사용 가능하므로 재부팅을 3회 시도합니다.

단계 **6** 관리 1/1용 네트워크 설정을 지정하고 다음 ROMMON 명령을 사용하여 ASA 패키지의 일부분인 FXOS를 로드합니다.

address *management_ip_address*

netmask *subnet_mask*

server *tftp_ip_address*

gateway *gateway_ip_address*

file*path/filename*

set

sync

tftp -b

FXOS 이미지가 다운로드되고 CLI에 부팅됩니다.

다음 정보를 참조하십시오.

- **gateway**- 게이트웨이 주소가 서버 IP 주소와 같은 네트워크에 있으면 두 주소를 동일하게 설정합니다.
- **set**- 네트워크 설정을 표시합니다. 또한 서버에 대한 연결성을 확인하기 위해 **ping** 명령을 사용할 수 있습니다.
- **sync**- 네트워크 설정을 저장합니다.
- **tftp -b**- FXOS를 로드합니다.

예제**:**

```
rommon 1> address 10.86.118.4
rommon 2> netmask 255.255.252.0
rommon 3> server 10.86.118.21
rommon 4> gateway 10.86.118.21
rommon 5> file cisco-asa-fp2k.9.8.2.SPA
rommon 6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.4
```

```
  NETMASK=255.255.252.0
  GATEWAY=10.86.118.21
  SERVER=10.86.118.21
  IMAGE=cisco-asa-fp2k.9.8.2.SPA
  CONFIG=
  PS1="rommon ! > "

rommon 7> sync
rommon 8> tftp -b
Enable boot bundle: tftp_reqsize = 268435456

             ADDRESS: 10.86.118.4
             NETMASK: 255.255.252.0
             GATEWAY: 10.86.118.21
              SERVER: 10.86.118.21
               IMAGE: cisco-asa-fp2k.9.8.2.SPA
             MACADDR: d4:2c:44:0c:26:00
           VERBOSITY: Progress
               RETRY: 40
          PKTTIMEOUT: 7200
             BLKSIZE: 1460
            CHECKSUM: Yes
                PORT: GbE/1
             PHYMODE: Auto Detect

link up
Receiving cisco-asa-fp2k.9.8.2.SPA from 10.86.118.21!!!!!!!!
[…]
```

단계 **7** 기본 사용자 이름인 **admin**과 비밀번호인 **Admin123**을 사용하여 FXOS에 로그인합니다.

디바이스가 FXOS에 부팅되면 ROMMON에서 설정한 관리 IP 주소가 지워지고 기본값인 192.168.45.45로 설정됩니다. FXOS에서 네트워크의 정확한 IP 주소 및 기타 관련 설정을 지정해야 서버에서 ASA 패키지를 다운로드할 수 있습니다.

단계 **8** DHCP 서버를 비활성화합니다.

scope system

scope services

disable dhcp-server

commit-buffer

관리 IP 주소를 변경하려면 DHCP 서버를 비활성화해야 합니다. 관리 IP 주소를 변경한 후 새 클라이언트 IP 주소를 사용하여 DHCP를 다시 활성화할 수 있습니다.

예제**:**

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # disable dhcp-server
firepower-2110 /system/services* # commit-buffer
```

단계 **9** IPv4 관리 IP 주소를 구성하고 필요한 경우 게이트웨이를 구성합니다.

scopefabric-interconnecta

setout-of-band staticip *ip_address***netmask** *network_mask***gw** *gateway_ip_address*

현재 설정되어 있는 게이트웨이(기본값: ASA 데이터 인터페이스를 나타내는 0.0.0.0)를 유지하려면 **gw** 키워드를 생략합니다. 다운로드 서버가 로컬 관리 1/1 네트워크에 있지 않으면 게이트웨이 IP 주소를 변경합니다. ASA 데이터 인터페이스는 아직 없으므로 기본 설정으로는 원격 서버에 연결할 수 없습니다.

예제:

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect #
firepower-2110 /fabric-interconnect # set out-of-band static ip 10.86.118.4 netmask
255.255.255.0
Warning: When committed, this change may disconnect the current CLI session
firepower-2110 /fabric-interconnect* #
```

단계 **10** 새로운 네트워크에서 관리 연결을 허용하도록 HTTPS, SSH 및 SNMP용 액세스 목록을 삭제한 후에 새로 추가합니다.

a) 시스템/서비스의 범위를 설정합니다.

scope system

scope services

예제:

```
firepower-2110# scope system
firepower-2110 /system # scope services
```

b) 현재 액세스 목록을 확인합니다.

show ip-block

예제:

```
firepower-2110 /system/services # show ip-block

Permitted IP Block:
    IP Address      Prefix Length Protocol
    --------------- ------------- --------
    192.168.45.0               24 https
    192.168.45.0               24 ssh
firepower-2140 /system/services #
```

c) 새 액세스 목록을 추가 합니다.

IPv4의 경우:

enterip-block *ip_address prefix* [**http** | **snmp** | **ssh**]

IPv6의 경우:

enteripv6-block *ipv6_address prefix* [**https** | **snmp** | **ssh**]

IPv4의 경우 모든 네트워크를 허용하려면 **0.0.0.0** 및 접두사 **0**을 입력합니다. IPv6의 경우 모든 네트워크를 허용하려면 **::** 및 접두사 **0**을 입력합니다. Firepower Chassis Manager의 **Platform Settings(**플랫폼 설정**)** > **Access List(**액세스 목록**)**에서 액세스 목록을 추가할 수도 있습니다.

예제:

```
firepower-2110 /system/services # enter ip-block 192.168.4.0 24 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.4.0 24 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* #
```

a) 이전 액세스 목록을 삭제합니다.

IPv4의 경우:

delete ip-block *ip_address prefix* [**http** | **snmp** | **ssh**]

IPv6의 경우:

delete ipv6-block *ipv6_address prefix* [**https** | **snmp** | **ssh**]

예제:

```
firepower-2110 /system/services # delete ip-block 192.168.45.0 24 https
firepower-2110 /system/services* # delete ip-block 192.168.45.0 24 ssh
firepower-2110 /system/services* #
```

단계 **11** (선택 사항) IPv4 DHCP 서버를 다시 활성화합니다.

scope system

scope services

enable dhcp-server *start_ip_address end_ip_address*

예제:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enable dhcp-server 10.86.118.10 10.86.118.20
```

단계 **12** 컨피그레이션을 저장합니다.

commit-buffer

예제:

```
firepower-2110 /system/services* # commit-buffer
```

단계 **13** ASA 패키지를 다운로드하여 부팅합니다.

a) 패키지를 다운로드합니다.

scope firmware

download image *url*

show download-task

이전에 사용했던 것과 같은 TFTP 서버나 관리 1/1에서 연결할 수 있는 다른 서버에서 패키지를 다운로드할 수 있습니다.

예제:

```
firepower-2110# scope firmware
firepower-2110 /firmware # download image tftp://10.86.118.21/cisco-asa-fp2k.9.8.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
firepower-2110 /firmware # show download-task
Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.21             0                 Downloaded
```

b) 패키지 다운로드가 완료되면(**Downloaded(**다운로드됨**)** 상태) 패키지를 부팅합니다.

show package

scope auto-install

install security-pack version *version*

show package 출력에서 **security-pack version** 번호용으로 **Package-Vers** 값을 복사합니다. 섀시에 ASA 이미지가 설치되고 섀시가 재부팅됩니다.

예제:

```
firepower 2110 /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
firepower 2110 /firmware # scope auto-install
firepower 2110 /firmware/auto-install # install security-pack version 9.8.2
The system is currently installed with security software package not set, which has:
   - The platform version: not set
If you proceed with the upgrade 9.8.2, it will do the following:
   - upgrade to the new platform version 2.2.2.52
   - install with CSP asa version 9.8.2
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
   If you proceed the system will be re-imaged. All existing configuration will be lost,

   and the default configuration applied.
Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.2
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
```

단계 **14** 새시 재부팅이 완료될 때까지 5~10분 정도 기다렸다가 기본 사용자 이름인 **admin**과 비밀번호인 **Admin123**을 사용하여 FXOS에 로그인합니다.

FXOS이 작동하더라도 ASA가 작동할 때까지 5분 동안 기다려야 합니다. 다음 메시지가 나타날 때까지 기다립니다.

```
firepower-2110#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2 ...
Verifying signature for cisco-asa.9.8.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

나머지 ASA 시작 메시지가 표시되고 나면 FXOS 프롬프트로 돌아올 수 있습니다.

단계 **15** 이 절차에서 FXOS 관리 1/1 주소를 변경한 경우에는 ASA 주소를 올바른 네트워크의 주소로 변경해야 합니다. 기본 ASA 관리 1/1 인터페이스 IP 주소는 192.168.45.1입니다.

a) 콘솔에서 ASA CLI에 연결하여 전역 컨피그레이션 모드에 액세스합니다.

connect asa

enable

configure terminal

활성화 비밀번호는 기본적으로 비어 있습니다.

예제**:**

```
firepower-2110# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa> enable
Password: <blank>
ciscoasa# configure terminal
ciscoasa(config)#
```

b) 관리 1/1 IP 주소를 변경합니다.

interface management1/1

ip address *ip_address mask*

예제**:**

```
ciscoasa(config)# interface management1/1
ciscoasa(config-ifc)# ip address 10.86.118.4 255.255.255.0
```

c) ASDM에 액세스할 수 있는 네트워크를 변경합니다.

no http 192.168.45.0 255.255.255.0 management

http *ip_address mask***management**

예제:

```
ciscoasa(config)# no http 192.168.45.0 255.255.255.0 management
ciscoasa(config)# http 10.86.118.0 255.255.255.0 management
```

d) 컨피그레이션을 저장합니다.

write memory

e) FXOS 콘솔로 돌아가려면 **Ctrl+a**, **d**를 입력합니다.

단계 **16** Firepower 2100 Series용 ASA 시작 가이드를 참조하여 시스템을 구성합니다.

다음 단계는 무엇인가요?

Firepower Threat Defense

사용 중인 모델 및 관리 애플리케이션별 빠른 시작 가이드를 참조하십시오.

- ASA 5506-X용 Firepower Device Manager
- ASA 5506-X용 Firepower Management Center
- ASA 5508-X 및 5516-X용 Firepower Device Manager
- ASA 5506-X 및 5516-X용 Firepower Management Center
- ASA 5512-X~ASA 5555-X용 Firepower Device Manager
- ASA 5512-X~5555-X용 Firepower Management Center
- Firepower 2100용 Firepower Device Manager
- Firepower 2100용 Firepower Management Center

ASA

사용 중인 모델별 빠른 시작 가이드를 참조하십시오.

- ASA 5506-X용 ASA
- ASA 5508-X 및 5516-X용 ASA
- ASA 5512-X~5555-X용 ASA
- Firepower 2100용 ASA