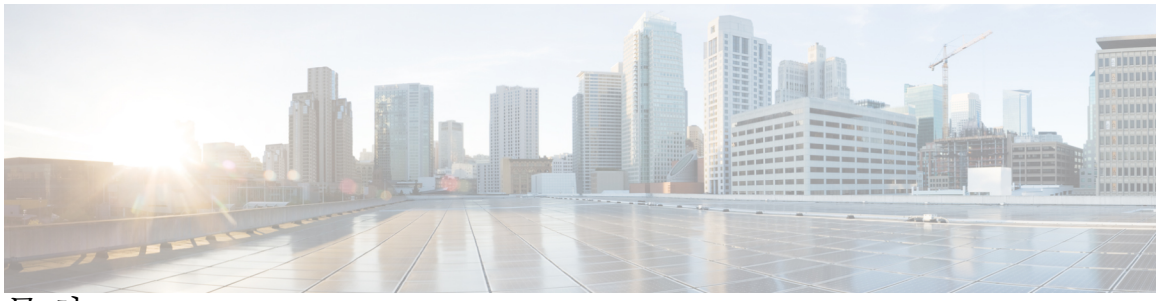
Firepower Management Center 업그레이드 가이드

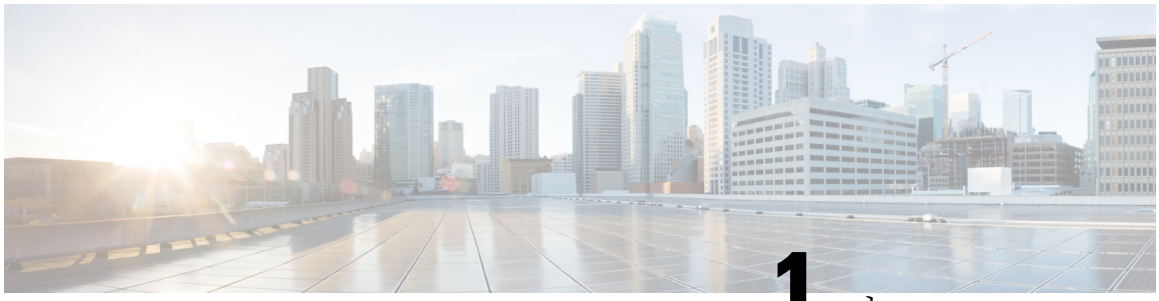
초판: 2018년 3월 29일

최종 변경: 2018년 4월 2일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차



1 장

시작하기

다음 주제에서는 Firepower Management Center 구축 업그레이드를 시작하는 방법을 설명합니다.

가이드의 적합성 확인

이 가이드에서는 모든 어플라이언스가 Firepower 버전 5.4 이상을 실행 중인 Firepower Management Center 구축의 성공적인 업그레이드를 준비하고 완료하는 방법을 설명합니다. 사용 중인 구축에서 Firepower Management Center를 사용하지 않거나 Firepower 소프트웨어를 새로 설치해야 하는 경우에는 다음 리소스를 사용하십시오.

단일 디바이스 구축 업그레이드

다음 가이드에서는 단일 디바이스 구축 업그레이드에 관해 설명합니다.

- Cisco ASA 업그레이드 가이드 - ASDM이 설치된 ASA FirePOWER 모듈을 업그레이드합니다.
- Firepower Device Manager용 Cisco Firepower Threat Defense 컨피그레이션 가이드 - Firepower Threat Defense 디바이스를 업그레이드합니다.

Firepower 소프트웨어 새로 설치

다음 표에는 새 설치를 위한 지침을 찾을 수 있는 위치가 나와 있습니다. 설치 패키지는 Cisco.com에서 제공됩니다. 업그레이드 패키지 다운로드, 9 페이지를 참조하십시오. Cisco에서는 패치용 설치 패키지를 제공하지 않습니다. 최신 주 버전을 설치한 후에 업그레이드하십시오.

표 *1: Firepower Management Center* 설치 지침

어플라이언스	가이드
MC750, 1500, 2000, 3500, 4000	모델 750, 1500, 2000, 3500 및 4000용 Cisco Firepower Management Center 시작 가이드 - Firepower Management Center를 공장 기본값으로 복원

어플라이언스	가이드
MC1000, 2500, 4500	모델 1000, 2500 및 4500용 Cisco Firepower Management Center 시작 가이드 - Firepower Management Center를 공장 기본값으로 복원
가상: VMware	VMware용 Cisco Firepower Management Center Virtual 구축 빠른 시작 가이드
가상: KVM	KVM용 Cisco Firepower Management Center Virtual 구축 빠른 시작 가이드
가상: AWS	AWS 클라우드용 Cisco Firepower Management Center Virtual 빠른 시작 가이드

표 ***2: Firepower Threat Defense*** 설치 지침

어플라이언스		가이드
Firepower 2100 Series		Cisco ASA 또는 Firepower Threat Defense 디바이스 이미지 재설치 및 Firepower Threat Defense를 실행하는 Firepower 2100 Series용 Cisco FXOS 트러블슈팅 가이드
Firepower 4100 Series Firepower 9300		Cisco FXOS CLI 컨피그레이션 가이드 - Firepower 4100/9300 Series 소프트웨어 이미지 재설치 및 재해 복구 절차
ASA 5500-X Series ISA 3000		Cisco ASA 또는 Firepower Threat Defense 디바이스 이미지 재설치
가상: VMware	Firepower Management Center 포함	Cisco Firepower Threat Defense Virtual for VMware 구축 빠른 시작 가이드
	Firepower Device Manager 포함	Firepower Device Manager for VMware를 사용한 Cisco Firepower Threat Defense Virtual 구축 빠른 시작 가이드
가상: KVM	Firepower Management Center 포함	Cisco Firepower Threat Defense Virtual for KVM 구축 빠른 시작 가이드
	Firepower Device Manager 포함	Firepower Device Manager for KVM을 사용한 Cisco Firepower Threat Defense Virtual 구축 빠른 시작 가이드
가상: AWS		Cisco Firepower Threat Defense Virtual for the AWS Cloud 빠른 시작 가이드
가상: Azure		Cisco Firepower Threat Defense Virtual for the Microsoft Azure Cloud 빠른 시작 가이드

표 *3: Firepower 7000/8000 Series, NGIPSv, ASA FirePOWER* 설치 지침

어플라이언스	가이드
Firepower 7000 Series	Cisco Firepower 7000 Series 시작 가이드 - 디바이스를 공장 기본값으로 복원
Firepower 8000 Series	Cisco Firepower 8000 Series 시작 가이드 - 디바이스를 공장 기본값으로 복원
NGIPSv	VMware용 Cisco Firepower NGIPSv 빠른 시작 가이드
ASA with FirePOWER Services: • ASA 5500-X Series • ISA 3000	Cisco ASA 또는 Firepower Threat Defense 디바이스 이미지 재설치 및 ASDM 설명서 2: Cisco ASA Series 방화벽 ASDM 컨피그레이션 가이드 - ASA FirePOWER 모듈 관리

가이드 사용

Firepower Management Center 구축 업그레이드는 복잡한 프로세스일 수 있습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다. 업그레이드 프로세스에서 업그레이드 스크립트를 호출하는 기계적 단계를 실제로 수행하는 것만큼 계획과 준비도 철저하게 고려해야 합니다.

이를 위해 이 가이드는 다음의 3개 주요 부분으로 구성되어 있습니다.

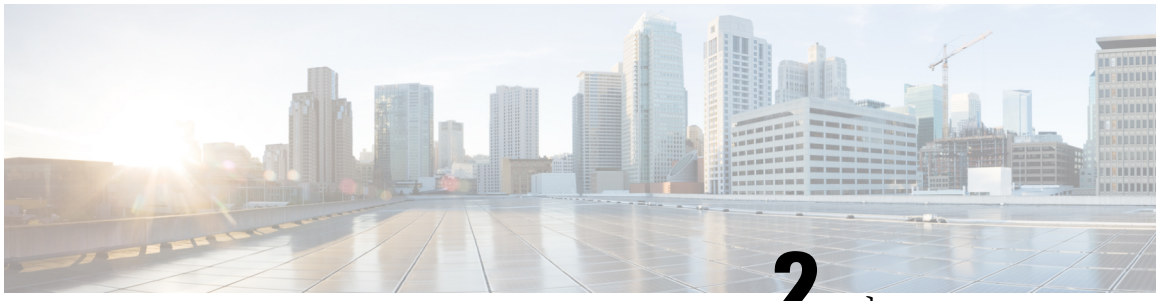
- 업그레이드 준비, 5 페이지- 구축 평가, 업그레이드 경로 계획, 업그레이드 패키지 다운로드 등의 내용이 포함되어 있습니다.
- Firepower 어플라이언스 업그레이드, 23 페이지- Firepower 어플라이언스를 업그레이드하는 실제 프로세스가 설명되어 있습니다(필요한 경우 운영 체제 업그레이드 포함).
- 참조 정보, 97 페이지- Firepower 업그레이드를 계획하고 실행하는 데 도움이 되는 참조 정보가 포함되어 있습니다. 업그레이드 절차를 이미 숙지하고 있다면 이 가이드를 통해 FAQ(자주 묻는 질문)에 대한 대답을 빠르게 찾을 수 있습니다.

업그레이드 체크리스트

이 가이드에서는 다양한 Firepower 어플라이언스 모델용 업그레이드 체크리스트를 제공합니다. 이러한 체크리스트는 계획과 준비를 포함한 전체 업그레이드 프로세스를 차례로 보여줍니다.

주의 업그레이드할 때마다 체크리스트를 작성하십시오. 단계를 건너뛰면 업그레이드에 실패할 수 있습니다.

어플라이언스	체크리스트
다음을 포함한 Firepower Management Center: • Firepower Management Center Virtual • 고가용성 쌍	Firepower Management Center 업그레이드 체크리스트, 25 페이지
Firepower Threat Defense: • Firepower 2100 Series • ASA 5500-X Series • ISA 3000 • Firepower Threat Defense Virtual	Firepower Threat Defense 업그레이드 체크리스트, 31 페이지
Firepower Threat Defense: • Firepower 4100 Series • Firepower 9300	Firepower Threat Defense 업그레이드 체크리스트 — Firepower 4100/9300 섀시, 37 페이지
NGIPS 소프트웨어: • Firepower 7000 및 8000 Series • NGIPSv	Firepower 7000/8000 Series 및 NGIPSv 업그레이드 체크리스트, 63 페이지
ASA with FirePOWER Services: • ASA 5500-X Series • ISA 3000	ASA with FirePOWER Services 업그레이드 체크리스트, 69 페이지



2 장

업그레이드 준비

Firepower Management Center 구축 업그레이드는 복잡한 프로세스일 수 있습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다. 업그레이드 프로세스에서 업그레이드 스크립트를 호출하는 기계적 단계를 실제로 수행하는 것만큼 계획과 준비도 철저하게 고려해야 합니다.

자세한 내용은 다음 링크를 참조하십시오.

구축 평가

Firepower 어플라이언스를 업그레이드하기 전에 현재 구축 상태를 확인합니다.

이때 다음과 같은 질문을 고려해야 합니다.

- 어떤 어플라이언스를 보유하고 있으며, 이러한 어플라이언스에서 어떤 Firepower 버전을 실행하고 있습니까? 어떤 버전을 실행하려고 합니까? 해당 버전을 실행할 수 있습니까?
- 어플라이언스에서 운영 체제를 별도로 업그레이드해야 합니까, 아니면 운영 체제만 업그레이드하려고 합니까?
- 호스팅 환경을 업그레이드해야 하는 가상 어플라이언스가 있습니까, 아니면 호스팅 환경만 업그레이드하려고 합니까?
- 독립형 Firepower Management Center를 사용 중입니까, 아니면 고가용성 Firepower Management Center 쌍이 있습니까?
- 디바이스가 독립형입니까, 아니면 클러스터, 스택 및 디바이스 고가용성 쌍이 있습니까?
- 디바이스는 어떤 방식으로 구축되어 있습니까(수동으로, IPS로, 방화벽으로)?
- 어플라이언스를 교체합니까, 아니면 구축에 새 어플라이언스를 추가합니까?

이처럼 현재 상태를 파악하면 업그레이드 목표에 따라 업그레이드 방법을 결정할 수 있습니다.

현재 버전 정보 찾기

이 표에는 사용 중인 Firepower 구축의 업그레이드 가능한 구성 요소의 현재 실행 중인 버전에 대한 정보를 찾을 수 있는 위치가 나와 있습니다.

Component(구성 요소**)**	어플라이언스	버전 정보
Firepower 소프트웨어	Firepower Management Center	Firepower Management Center에서 **Help(**도움말**)** > **About(**정보**)**를 선택합니다.
Firepower 소프트웨어	Firepower Management Center에서 관리하는 모든 Firepower 디바이스	Firepower Management Center에서 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.
FXOS	Firepower 4100/9300 섀시	FXOS CLI에서 **show version** 명령을 사용합니다.
ASA	ASA with FirePOWER Services	ASA CLI에서 **show version** 명령을 사용합니다.
가상 호스팅 환경	모든 Firepower 가상 어플라이언스	가상 호스팅 환경 설명서를 참조하십시오.

업그레이드 경로 계획

업그레이드 경로는 어떤 어플라이언스 및 구성 요소를 업그레이드할 것이며, 어떤 순서로 업그레이드할 것인지 상세하게 나와 있는 계획입니다.

사용 중인 구축을 평가했다면 현재 구축과 원하는 구축에 대해 파악할 수 있으며 업그레이드 경로를 작성할 준비를 할 수 있습니다. 각 어플라이언스 유형에 지원되는 업그레이드 경로에 대한 빠른 참조와 다양한 구축 유형에 대한 상세한 예시 업그레이드 경로는 업그레이드 경로, 109 페이지를 참조하십시오.

업그레이드 경로를 작성하는 데 도움이 되는 다음 지침을 참조하십시오.

Firepower 주 버전 이해**/**업그레이드와 패치 비교

Firepower 주 버전 업그레이드의 경우 버전의 첫 번째, 두 번째 또는 세 번째 숫자가 변경됩니다. 주 버전 업그레이드에는 새로운 기능이 포함되며 대규모의 제품 변경이 수반될 수 있습니다. 운영 체제를 별도로 업그레이드하는 디바이스의 경우 Firepower 주 버전 업그레이드로 인해 컴패니언 운영 체제도 함께 업그레이드해야 할 가능성이 높습니다.

참고 대부분의 경우에는 Firepower 소프트웨어를 업그레이드하지 않고 어플라이언스 운영 체제(또는 가상 호스팅 환경)를 업그레이드할 수 있으며, 그 반대의 경우도 가능합니다. 예를 들어 운영 체제 패치를 적용하면 Firepower 소프트웨어와 관련이 없는 문제를 해결할 수 있습니다. 또는 하이퍼바이저를 업그레이드 하지 않고 새 Firepower 기능을 활용할 수도 있습니다. 업그레이드하려는 구성 요소의 대상 버전이 업그레이드하지 않을 구성 요소와 호환되는지만 확인하면 됩니다.

Firepower 패치를 적용하면 버전의 네 번째 숫자가 변경됩니다. 패치는 일반적으로 제한된 범위의 수정 사항을 포함합니다.

업그레이드 경로에 여러 Firepower 주 버전(예: 버전 6.0.1~버전 6.2.3)이 포함되는 경우에는 중간 버전(버전 6.1)의 패치를 건너뛸 수 있습니다. 즉, 주 버전 간에 직접 업그레이드할 수 있습니다. 대상 주 버전으로 업그레이드한 후에 최신 패치를 적용하면 됩니다.

관리자-디바이스 호환성 유지

Firepower Management Center와 해당 디바이스는 별도로 업그레이드합니다. 고가용성 Firepower Management Center는 한 번에 하나씩 수동으로 업그레이드합니다.

관리자-디바이스 호환성을 유지하기 위해서는 구축을 업그레이드해야 하는 정도에 따라 다음을 수행해야 합니다.

- 중간 버전 업그레이드를 수행합니다.
- Firepower Management Center 및 해당 디바이스를 교대로 업그레이드합니다.

자세한 내용은 Firepower Management Center 및 매니지드 디바이스 버전 호환성, 99 페이지를 참조하십시오.

FXOS 업그레이드 포함(Firepower 4100/9300 섀시)

Firepower 4100 Series 및 Firepower 9300 디바이스는 FXOS 운영 체제를 사용합니다.

Firepower 주 버전에는 컴패니언 FXOS 버전이 있습니다. Firepower 4100/9300 섀시에서 Firepower 소프트웨어를 업그레이드하기 전에 FXOS의 해당 컴패니언 버전을 실행해야 합니다.

Firepower Threat Defense 고가용성 또는 클러스터링이 구성되어 있더라도 각 섀시에서 FXOS를 독립적으로 업그레이드합니다. 업그레이드 중단을 최소화하려면 항상 고가용성 쌍의 스탠바이 유닛이나 섀시 간 클러스터의 전체 슬레이브 섀시를 업그레이드하십시오.

자세한 내용은 Firepower Threat Defense 업그레이드 경로 - Firepower Management Center 포함, 112 페이지를 참조하십시오.

ASA 업그레이드 포함(ASA with FirePOWER Services)

ASA with FirePOWER Services 디바이스는 ASA 운영 체제를 사용합니다.

ASA 및 ASA FirePOWER 버전은 광범위하게 호환됩니다. 하지만 ASA 업그레이드가 필요하지 않더라도 문제를 해결하려면 지원되는 최신 버전으로 업그레이드해야 할 수 있습니다.

ASA 클러스터링 또는 페일오버 쌍이 구성되어 있더라도 각 섀시에서 ASA를 독립적으로 업그레이드합니다. 업그레이드 중단을 최소화하려면 업그레이드 전에 각 유닛의 클러스터링을 비활성화하거나 페일오버하고 ASA를 업그레이드하면서 ASA FirePOWER 모듈을 한 번에 하나씩 업그레이드합니다.

자세한 내용은 ASA FirePOWER 모듈 업그레이드 경로 - Firepower Management Center 포함, 118 페이지를 참조하십시오.

가상 호스팅 환경 업그레이드 포함

가상 Firepower 어플라이언스는 다양한 호스팅 환경에서 실행됩니다. Firepower 소프트웨어는 호스팅 환경과 계속 호환되어야 합니다. 업그레이드 경로는 호환성에 따라 달라집니다.

- 호스팅 환경 먼저 업그레이드 - 예를 들어 VMware ESXi 5.0에서 NGIPSv 버전 5.4.x를 실행 중인 경우 NGIPSv를 Firepower 6.0으로 업그레이드하기 전에 VMware ESXi를 버전 5.1 또는 버전 5.5로 업그레이드해야 합니다.
- Firepower 소프트웨어 먼저 업그레이드 - 예를 들어 VMware ESXi 6.0에서 Firepower Threat Defense Virtual 버전 6.1.x를 실행 중인 경우 VMware ESXi를 버전 6.5로 업그레이드하기 전에 Firepower 소프트웨어를 버전 6.2.3으로 업그레이드합니다.

새 디바이스를 추가할 시기 파악

업그레이드 경로에 새 디바이스 추가 작업이 포함되는 경우 디바이스 추가 시기는 디바이스 유형에 따라 달라집니다.

- 물리적 디바이스 - 디바이스에서 현재 실행 중인 Firepower 버전을 확인합니다. 디바이스를 최대한 빨리 추가한 다음 Firepower Management Center를 사용하여 나머지 구축과 함께 새 디바이스를 업그레이드합니다. 아웃오브더박스(out-of-the-box) 디바이스를 더 이상 관리할 수 없는 기간을 지나서 Firepower Management Center를 업그레이드하지 마십시오.
- 가상 디바이스 - Firepower Management Center를 대상 버전으로 업그레이드한 후에 생성합니다. 새 가상 디바이스를 추가할 때는 주 버전 업그레이드를 수행해서는 안 되며 패치만 수행해야 합니다.

기타 주요 작업 확인

업그레이드 프로세스의 대다수 단계는 시간이 매우 많이 걸릴 수 있습니다. 계획에 이러한 단계를 명시적으로 포함해야 합니다. 예를 들면 다음과 같습니다.

- 백업
- 다운로드 및 푸시
- 준비 확인
- 업그레이드 전/후 컨피그레이션 변경

트래픽 흐름 및 검사에서 중단 식별

자세한 내용은 업그레이드 중의 트래픽 흐름, 검사 및 디바이스 동작, 125 페이지를 참조하십시오.

어디서부터 시작해야 합니까**?**

구축 평가를 참조하십시오. 일반적으로 첫 번째 업그레이드는 매니지드 디바이스에서 실행 중인 Firepower 버전에 따라 달라집니다.

디바이스 버전	먼저 업그레이드해야 할 디바이스	업그레이드 대상 버전
모든 디바이스가 버전 6.1 이상	Firepower Management Center	모든 주 버전, 6.2 이상
일부 또는 모든 디바이스가 6.1 이전 버전이지만 Firepower Management Center와 같은 주 버전 실행 중	Firepower Management Center	다음 주 버전
일부 또는 모든 디바이스가 6.1 이전 버전이며 Firepower Management Center보다 이전의 주 버전 실행 중	디바이스	Firepower Management Center와 같은 주 버전

업그레이드 패키지 다운로드

Firepower Management Center 또는 Firepower Management Center가 관리하는 디바이스에서 Firepower 소프트웨어를 업그레이드하려면 적절한 업그레이드 패키지를 Firepower Management Center에 업로드해야 합니다. 고가용성 쌍의 두 피어에 모두 Firepower Management Center 업그레이드 패키지(매니지드 디바이스 패키지 제외)를 업로드합니다.

참고 버전 6.2.1 이상의 업그레이드 패키지는 서명이 되어 있으며 이름이 .sh가 아닌 .sh.REL.tar로 끝납니다. 서명된 업그레이드 패키지는 압축을 풀지 마십시오.

Firepower Management Center 웹 인터페이스를 사용하면 Cisco.com에서 패치와 핫픽스를 바로 다운로드할 수 있습니다. 하지만 주 버전 업그레이드 패키지는 Cisco.com에서 직접 다운로드한 다음 Firepower Management Center에 업로드해야 합니다.

자세한 내용은 다음 링크를 참조하십시오.

Firepower Management Center를 사용하여 업그레이드 패키지 다운로드

Firepower Management Center를 사용하면 패치와 핫픽스 자체 및 Firepower Management Center가 관리하는 디바이스를 검색할 수 있습니다.

검색되는 업그레이드 패키지의 수와 검색 시간은 다음 요소에 따라 달라집니다.

- 현재 구축의 최신 상태 - 시스템은 어플라이언스가 현재 실행 중인 버전과 연결된 각 패치 및 핫픽스용 패키지를 다운로드합니다.
- 각 디바이스 유형의 수 - 시스템은 각 디바이스 유형에 대해 서로 다른 패키지를 다운로드합니다. 구축에 같은 유형의 디바이스 여러 개가 포함된 경우(예: Firepower Threat Defense 디바이스 10개) 시스템은 단일 패키지를 다운로드하여 모든 디바이스를 업그레이드합니다.

시작하기 전에

- Firepower Management Center에서 인터넷에 액세스할 수 있는지 확인합니다.
- 고가용성 쌍의 스탠바이 Firepower Management Center를 사용 중인 경우 동기화를 일시 정지합니다. 자세한 내용은 고가용성 Firepower Management Center 다운로드 지침, 17 페이지를 참조하십시오.

단계 **1** Firepower Management Center 웹 인터페이스에서 **System**(시스템) > **Updates**(업데이트)를 선택합니다.

단계 **2** **Download Updates**(업데이트 다운로드)를 클릭합니다.

Cisco.com에서 소프트웨어 다운로드

모든 업그레이드 패키지는 Cisco.com에서 다운로드할 수 있지만, 주 버전 업그레이드의 경우에는 반드시 Cisco.com에서 다운로드해야 합니다. 업그레이드 경로를 참조하여 다운로드해야 하는 업그레이드 패키지를 확인하십시오.

대다수 업그레이드 패키지는 이름이 비슷하므로 정확한 패키지를 다운로드해야 합니다. 지원 사이트에서 패키지를 직접 다운로드하십시오. 이메일로 전송하는 업그레이드 패키지는 손상될 수 있습니다. 버전 6.2.1 이상의 업그레이드 패키지는 서명이 되어 있으며 이름이 .sh가 아닌 .sh.REL.tar로 끝납니다. 서명된 업그레이드 패키지는 압축을 풀지 마십시오.

단계 **1** Cisco.com에서 업그레이드 패키지를 찾은 다음 컴퓨터에 다운로드합니다.

다음 표에서는 탐색 경로와 업그레이드 패키지 이름이 제공됩니다.

- Firepower Management Center 소프트웨어 다운로드, 11 페이지
- Firepower Threat Defense 소프트웨어 다운로드, 12 페이지
- Firepower 7000/8000 Series 및 NGIPSv 소프트웨어 다운로드, 13 페이지

단계 **2** Firepower Management Center에서 **System**(시스템) > **Updates**(업데이트)를 선택합니다.

단계 **3** **Upload Update**(업데이트 업로드)와 **Choose File**(파일 선택)을 차례로 클릭합니다. 업그레이드를 찾은 다음 **Upload**(업로드)를 클릭합니다.

Firepower Management Center 소프트웨어 다운로드

이 섹션에서는 Firepower Management Center의 다운로드 위치와 패키지 이름을 설명합니다.

고가용성 Firepower Management Center의 경우에는 두 피어에 모두 패키지를 업로드합니다. 보조 피어의 경우 동기화를 일시 정지합니다. 자세한 내용은 고가용성 Firepower Management Center 다운로드 지침, 17 페이지를 참조하십시오.

다운로드 위치

https://www.cisco.com/web/go/firepower-software로 이동합니다.

사용 중인 *model(*모델*)* > **FireSIGHT System Software(FireSIGHT System** 소프트웨어**)** > *version(*버전*)*을 선택합니다.

패키지 이름

버전 6.2.1 이상의 업그레이드 패키지는 서명이 되어 있으며 이름이 .sh가 아닌 .sh.REL.tar로 끝납니다. 서명된 업그레이드 패키지는 압축을 풀지 마십시오. 설치 패키지는 새 설치(이미지 재설치)에만 사용됩니다.

모델	패키지 유형	패키지 이름
All(모두)	업그레이드	Sourcefire_3D_Defense_Center_S3_**Upgrade-***version***.sh** Sourcefire_3D_Defense_Center_S3_**Upgrade-***version***.sh.REL.tar**
	패치	Sourcefire_3D_Defense_Center_S3_**Patch-***version***.sh** Sourcefire_3D_Defense_Center_S3_**Patch-***version***.sh.REL.tar**
	Hotfix	Sourcefire_3D_Defense_Center_S3_**Hotfix_***letter***-***version***.sh** Sourcefire_3D_Defense_Center_S3_**Hotfix_***letter***-***version***.sh.REL.tar**
MC750, MC1500, MC3500, MC2000, MC4000	사전 설치 패키지(일부 릴리스에만 해당)	Sourcefire_3D_Defense_Center_S3_*targetversion*_**Pre-install-***currentversion***.sh**
	시스템 소프트웨어 설치	Sourcefire_Defense_Center_S3-*version*-Restore**.iso**
MC1000, MC2500, MC4500	시스템 소프트웨어 설치	Sourcefire_Defense_Center_M4-*version*-Restore**.iso**
Firepower Management Center Virtual	Firepower 소프트웨어 설치: VMware	Cisco_Firepower_Management_Center_Virtual_VMware-*version***.tar.gz**
	Firepower 소프트웨어 설치: KVM	Cisco_Firepower_Management_Center_Virtual-*version***.qcow2**
	Firepower 소프트웨어 설치: AWS	클라우드 서비스에 로그인하여 Marketplace에서 구축합니다.

Firepower Threat Defense 소프트웨어 다운로드

이 섹션에서는 Firepower Threat Defense 디바이스의 다운로드 위치와 패키지 이름을 설명합니다.

다운로드 위치

다음 위치로 이동합니다.

- ISA 3000—http://www.cisco.com/go/isa3000-software
- 다른 모든 항목 —https://www.cisco.com/go/ftd-software

사용 중인 *model(*모델*)* > **Firepower Threat Defense Software(Firepower Threat Defense** 소프트웨어**)** > *version(*버전*)*을 선택합니다.

패키지 이름

버전 6.2.1 이상의 업그레이드 패키지는 서명이 되어 있으며 이름이 .sh가 아닌 .sh.REL.tar로 끝납니다. 서명된 업그레이드 패키지는 압축을 풀지 마십시오. 부트 이미지와 설치 패키지는 새 설치(이미지 재설치)에만 사용됩니다.

모델	패키지 유형	패키지 이름
Firepower 2100 Series	업그레이드	Cisco_FTD_SSP_FP2K_**Upgrade-***version***.sh.REL.tar**
	패치	Cisco_FTD_SSP-FP2K_**Patch-***version***.sh.REL.tar**
	Hotfix	Cisco_FTD_SSP-FP2K_**Hotfix_***letter-version***.sh.REL.tar**
	시스템 소프트웨어 설치	cisco-ftd-fp2k.*version***.SPA**
Firepower 4100 Series Firepower 9300	업그레이드	Cisco_FTD_SSP_**Upgrade-***version***.sh** Cisco_FTD_SSP_**Upgrade-***version***.sh.REL.tar**
	패치	Cisco_FTD_SSP_**Patch-***version***.sh** Cisco_FTD_SSP_**Patch-***version***.sh.REL.tar**
	Hotfix	Cisco_FTD_SSP_**Hotfix_***letter-version***.sh** Cisco_FTD_SSP_**Hotfix_***letter-version***.sh.REL.tar**
	Firepower 소프트웨어 설치	cisco-ftd.*version***.SPA.csp**
	FXOS	Firepower 4100/9300 새 시용 FXOS 다운로드, 16 페이지을 참조하십시오.

모델	패키지 유형	패키지 이름
ASA 5500-X Series ISA 3000	업그레이드	Cisco_FTD_**Upgrade**-*version*.**sh** Cisco_FTD_**Upgrade**-*version*.**sh.REL.tar**
	패치	Cisco_FTD_**Patch**-*version*.**sh** Cisco_FTD_**Patch**-*version*.**sh.REL.tar**
	Hotfix	Cisco_FTD_**Hotfix**_*letter*-*version*.**sh** Cisco_FTD_**Hotfix**_*letter*-*version*.**sh.REL.tar**
	부트 이미지: 5506-X, 08-X, 16-X ISA 3000	ftd-**boot**-*version*.**lfbff**
	부트 이미지: 5512-X, 15-X, 25-X, 45-X, 55-X	ftd-**boot**-*version*.**cdisk**
	Firepower 소프트웨어 설치	ftd-*version*.**pkg**
Firepower Threat Defense Virtual(NGFW Virtual): • VMWare • KVM • AWS • Microsoft Azure	업그레이드	Cisco_FTD_**Upgrade**-*version*.**sh** Cisco_FTD_**Upgrade**-*version*.**sh.REL.tar**
	패치	Cisco_FTD_**Patch**-*version*.**sh** Cisco_FTD_**Patch**-*version*.**sh.REL.tar**
	Hotfix	Cisco_FTD_**Hotfix**_*letter*-*version*.**sh** Cisco_FTD_**Hotfix**_*letter*-*version*.**sh.REL.tar**
	Firepower 소프트웨어 설치: VMware	Cisco_Firepower_Threat_Defense_Virtual-*version*.**tar.gz**
	Firepower 소프트웨어 설치: KVM	Cisco_Firepower_Threat_Defense_Virtual-*version*.**qcow2**
	Firepower 소프트웨어 설치: AWS, Azure	클라우드 서비스에 로그인하여 Marketplace에서 구축합니다.

Firepower 7000/8000 Series 및 NGIPSv 소프트웨어 다운로드

이 섹션에서는 Firepower 7000/8000 Series 및 NGIPSv 디바이스의 다운로드 위치와 패키지 이름을 설명합니다.

다운로드 위치

다음 위치로 이동합니다.

- 7000 Series —https://www.cisco.com/go/7000series-software
- 8000 Series —https://www.cisco.com/go/8000series-software
- NGIPSv —http://www.cisco.com/go/ngipsv-software

사용 중인 *model(*모델*)* > **FireSIGHT System Software(FireSIGHT System** 소프트웨어**)** > *version(*버전*)*을 선택합니다.

패키지 이름

버전 6.2.1 이상의 업그레이드 패키지는 서명이 되어 있으며 이름이 .sh가 아닌 .sh.REL.tar로 끝납니다. 서명된 업그레이드 패키지는 압축을 풀지 마십시오. 설치 패키지는 새 설치(이미지 재설치)에만 사용됩니다.

표 ***4: Firepower 7000/8000 Series*** 및 ***AMP*** 패키지 이름

패키지 유형	패키지 이름
업그레이드	Sourcefire_3D_Device_S3_**Upgrade**-*version***.sh** Sourcefire_3D_Device_S3_**Upgrade**-*version***.sh.REL.tar**
패치	Sourcefire_3D_Device_S3_**Patch**-*version***.sh** Sourcefire_3D_Device_S3_**Patch**-*version***.sh.REL.tar**
Hotfix	Sourcefire_3D_Device_S3_**Hotfix**_*letter*-*version***.sh** Sourcefire_3D_Device_S3_**Hotfix**_*letter*-*version***.sh.REL.tar**
사전 설치 패키지(일부 릴리스에만 해당)	Sourcefire_3D_Device_S3_*targetversion*_**Pre-install**-*currentversion***.sh**
시스템 소프트웨어 설치	Sourcefire_3D_Device_S3-*version*-Restore**.iso**

표 ***5: NGIPSv*** 패키지 이름

패키지 유형	패키지 이름
업그레이드	Sourcefire_3D_Device_Virtual64_VMware_**Upgrade**-*version***.sh** Sourcefire_3D_Device_VMware_**Upgrade**-*version***.sh.REL.tar**
패치	Sourcefire_3D_Device_Virtual64_VMware_**Patch**-*version***.sh** Sourcefire_3D_Device_VMware_**Patch**-*version***.sh.REL.tar**
Hotfix	Sourcefire_3D_Device_Virtual64_VMware_**Hotfix**_*letter*-*version***.sh** Sourcefire_3D_Device_VMware_**Hotfix**_*letter*-*version***.sh.REL.tar**

패키지 유형	패키지 이름
사전 설치 패키지(일부 릴리스에만 해당)	Sourcefire_3D_Device_Virtual64_VMware_*targetversion*_**Pre-install**-*currentversion*.**sh**
Firepower 소프트웨어 설치	Cisco_Firepower_NGIPSv_VMware-*version*.**tar.gz**

ASA FirePOWER 소프트웨어 다운로드

이 섹션에서는 ASA FirePOWER 모듈의 다운로드 위치와 패키지 이름을 설명합니다.

다운로드 위치

다음 위치로 이동합니다.

- ASA 5500-X Series—http://www.cisco.com/go/asa-firepower-sw
- ISA 3000—http://www.cisco.com/go/isa3000-software

*model(*모델*)* > **FirePOWER Services Software for ASA(ASA**용 **FirePOWER Services** 소프트웨어**)** > *version(*버전*)*을 선택합니다.

패키지 이름

버전 6.2.1 이상의 업그레이드 패키지는 서명이 되어 있으며 이름이 .sh가 아닌 .sh.REL.tar로 끝납니다. 서명된 업그레이드 패키지는 압축을 풀지 마십시오. 부트 이미지와 설치 패키지는 새 설치(이미지 재설치)에만 사용됩니다.

모델	패키지 유형	패키지 이름
ASA 5500-X Series	업그레이드	Cisco_Network_Sensor_**Upgrade**-*version*.**sh** Cisco_Network_Sensor_**Upgrade**-*version*.**sh.REL.tar**
	패치	Cisco_Network_Sensor_**Patch**-*version*.**sh** Cisco_Network_Sensor_**Patch**-*version*.**sh.REL.tar**
	Hotfix	Cisco_Network_Sensor_**Hotfix**_*letter*-*version*.**sh** Cisco_Network_Sensor_**Hotfix**_*letter*-*version*.**sh.REL.tar**
	사전 설치 패키지 (일부 릴리스에만 해당)	Cisco_Network_Sensor_*targetversion*_**Pre-install**-*currentversion*.**sh**
	부트 이미지: ASA 5506-X, 08-X, 16-X ASA 5512-X, 15-X, 25-X, 45-X, 55-X	asasfr-**boot**-*version*.**img**
	부트 이미지: ASA 5585-X	asasfr-**boot**-*version*.**img**
	시스템 소프트웨어 설치	asasfr-**sys**-*version*.**pkg**
	ASA OS	Cisco ASA 업그레이드 가이드의 *ASA* 소프트웨어 다운로드 참조
ISA 3000	패치	Cisco_Network_Sensor_**Patch**-*version*.**sh**
	Hotfix	Cisco_Network_Sensor_**Hotfix**_*letter*-*version*.**sh**
	부트 이미지	asasfr-ISA-3000-**boot**-*version*.**img**
	시스템 소프트웨어 설치	asasfr-**sys**-*version*.**pkg**
	ASA OS	Cisco ASA 업그레이드 가이드의 *ASA* 소프트웨어 다운로드 참조

Firepower 4100/9300 섀시용 FXOS 다운로드

이 섹션에서는 Firepower 4100/9300 섀시용 FXOS 운영 체제의 다운로드 위치와 패키지 이름을 설명합니다.

다운로드 위치

다음 위치로 이동합니다.

- Firepower 4100 Series—http://www.cisco.com/go/firepower4100-software
- Firepower 9300—http://www.cisco.com/go/firepower9300-software

사용 중인 *model(*모델*)* > **Firepower Extensible Operating System(Firepower Extensible** 운영 체제**)** > *version(*버전*)*을 선택합니다.

패키지 이름

패키지 유형	패키지 이름
FXOS 이미지	fxos-k9.*version*.**SPA**
복구(Kickstart)	fxos-k9-**kickstart**.*version*.**SPA**
복구(관리자)	fxos-k9-**manager**.*version*.**SPA**
복구(시스템)	fxos-k9-**system**.*version*.**SPA**
MIB	fxos-**mibs**-fp9k-fp4k.*version*.**zip**
펌웨어: Firepower 4100 Series	fxos-k9-fpr4k-**firmware**.*version*.**SPA**
펌웨어: Firepower 9300	fxos-k9-fpr9k-**firmware**.*version*.**SPA**

고가용성 **Firepower Management Center** 다운로드 지침

고가용성 컨피그레이션의 Firepower Management Center를 업그레이드할 때는 액티브/기본 Firepower Management Center 및 스탠바이/보조 Firepower Management Center에 모두 패키지를 다운로드해야 합니다.

액티브/기본 Firepower Management Center에는 동기화를 일시 정지하지 않고도 패키지를 다운로드할 수 있지만, 스탠바이/보조 Firepower Management Center에 패키지를 다운로드하기 전에는 동기화를 일시 정지해야 합니다.

업그레이드 프로세스 중에 고가용성 동기화 중단을 제한하려면 다음을 수행하는 것이 좋습니다.

- 업그레이드 준비 단계 중에 액티브/기본 Firepower Management Center용 소프트웨어를 다운로드합니다.
- 동기화를 일시 정지한 후 업그레이드 단계 중에 스탠바이/보조 Firepower Management Center용 소프트웨어를 다운로드합니다.

자세한 내용은 고가용성 Firepower Management Center 업그레이드, 29 페이지를 참조하십시오.

매니지드 디바이스로 업그레이드 패키지 푸시

6.2.3 이상 버전에서는 실제 업그레이드를 실행하기 전에 매니지드 디바이스로 업그레이드 패키지를 복사(푸시)할 수 있습니다. 따라서 업그레이드 유지 보수 기간을 줄일 수 있습니다. 6.2.3 이전 버전에서는 Firepower Management Center가 설치 중에 매니지드 디바이스에 패키지를 복사하며, 해당 작업을 별도로 수행할 수는 없습니다.

업그레이드 패키지를 디바이스 클러스터나 스택으로 푸시하면 Firepower Management Center에서는 패키지를 먼저 한 유닛으로 푸시한 후에 다른 유닛으로 푸시합니다. 고가용성 쌍으로 푸시할 때는 Firepower Management Center가 기본 유닛으로 패키지를 푸시하며, 그리고 나면 기본 유닛이 보조 유닛과 동기화됩니다.

시작하기 전에

- 적절한 업그레이드 패키지를 다운로드하여 Firepower Management Center에 업로드합니다. 업그레이드 패키지 다운로드, 9 페이지을 참조하십시오.
- 업그레이드 패키지를 푸시하는 시기는 관리 네트워크의 대역폭에 따라 달라집니다. Firepower Management Center에서 디바이스로의 대량 데이터 전송을 수행할 수 있는 대역폭이 있는지 확인합니다. 자세한 내용은 Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침(트러블슈팅 TechNote)을 참조하십시오.

단계 **1** **System**(시스템) > **Updates**(업데이트)를 선택합니다.

단계 **2** 푸시하려는 업그레이드 패키지 옆의 **Push**(푸시) 아이콘을 클릭하고 대상 디바이스를 선택합니다.

업그레이드 패키지를 푸시하려는 디바이스가 나열되어 있지 않은 경우 업그레이드 패키지를 잘못 선택한 것입니다.

단계 **3** **Push**(푸시)를 클릭합니다.

단계 **4** Message Center에서 푸시 진행 상황을 모니터링합니다.

준비 확인 실행

준비 확인(선택 사항)은 어플라이언스가 Firepower 업그레이드를 위해 준비되어 있는지를 평가합니다. 업그레이드 패키지에 포함되어 있는 준비 확인은 데이터베이스 무결성, 버전 불일치, 디바이스 등록 등의 문제를 식별합니다.

주의 준비 확인 과정에서 어플라이언스를 리부팅하거나 종료하지 마십시오. 어플라이언스가 준비 확인을 통과하지 못하면 문제점을 바로잡고 다시 준비 확인을 실행합니다. 준비 확인을 통해 직접 해결할 수 없는 문제가 확인되면 업그레이드를 시작하지 마십시오. 그 대신 Cisco TAC에 문의하십시오.

준비 확인에 대한 지침 및 제한 사항

- Firepower 소프트웨어 준비만 확인함 - 준비 확인은 침입 규칙, VDB 또는 GeoDB 업데이트에 대한 준비는 평가하지 않습니다.
- 버전 6.1 이상 필요 - 준비 확인은 버전 6.1에 도입되었습니다. 버전 6.1로의 업그레이드에 대한 준비 확인은 정확한 결과를 반환하지 않을 수도 있습니다.
- 웹 인터페이스와 셸 비교 - Firepower Management Center 웹 인터페이스를 사용하면 자체 준비 확인 및 해당 독립형 매니지드 디바이스에 대해서만 준비 확인을 실행할 수 있습니다. 클러스터형 디바이스, 스택형 디바이스 및 고가용성 쌍의 디바이스에 대해서는 각 디바이스의 셸에서 준비 확인을 실행합니다.
- 시간 요구 사항 - 준비 확인을 실행하는 데 필요한 시간은 어플라이언스 모델 및 데이터베이스 크기에 따라 달라집니다. 구축이 대규모인 경우에는 편의상 준비 확인을 무시할 수 있습니다(예: Firepower Management Center에서 100개가 넘는 디바이스를 관리하는 경우).

Management Center에서 준비 확인 실행

Firepower Management Center 웹 인터페이스를 사용하면 Firepower Management Center 및 해당 독립형 매니지드 디바이스에 대해 준비 확인을 수행할 수 있습니다.

시작하기 전에

- 준비를 확인할 버전 6.1 이상 어플라이언스용 업그레이드 패키지를 Firepower Management Center에 업로드합니다. 준비 확인은 업그레이드 패키지에 포함되어 있습니다. 버전 6.2.1 이상의 업그레이드 패키지는 서명이 되어 있으며 이름이 .sh가 아닌 .sh.REL.tar로 끝납니다. 준비 확인 또는 업그레이드 자체를 수행하기 전에 서명된 업그레이드 패키지의 압축을 풀지 마십시오.
- 모든 매니지드 디바이스에 컨피그레이션 변경사항을 재구축합니다. 그러지 않으면 준비 확인에 실패할 수 있습니다.

단계 **1** Firepower Management Center 웹 인터페이스에서 **System(**시스템**)** > **Updates(**업데이트**)**를 선택합니다.

단계 **2** 준비 확인을 평가할 업그레이드 옆의 Install(설치) 아이콘을 클릭합니다.

단계 **3** **Launch Readiness Check(**준비 확인 실행**)**를 클릭합니다.

단계 **4** Message Center에서 준비 확인 진행 상황을 모니터링합니다.
준비 확인이 완료되면 시스템이 Readiness Check Status(준비 확인 상태) 페이지에 성공이나 실패를 보고합니다.

단계 **5** 종합 준비 확인 보고서(`/var/log/sf/`*`$rpm_name`*`/upgrade_readiness`)에 액세스합니다.

셸에서 준비 확인 실행

셸에서 모든 버전 6.1 이상 Firepower 어플라이언스에 대해 준비 확인을 실행할 수 있습니다. 클러스터형 디바이스, 스택형 디바이스 및 고가용성 쌍의 디바이스에 대해서는 셸을 반드시 사용해야 합니다.

⚠

주의 콘솔 세션에서 준비 확인을 실행하는 것이 좋습니다. SSH를 사용하여 어플라이언스에 액세스하는 경우에는 연결 시간이 초과되지 않는지 확인하십시오. 준비 확인은 사용자 셸의 하위 프로세스로 실행됩니다. SSH 연결이 종료되면 이러한 프로세스는 중단되고 확인도 중단되며 어플라이언스가 불안정한 상태로 유지될 수 있습니다.

시작하기 전에

- 준비를 확인할 업그레이드 패키지 어플라이언스를 다운로드합니다(업그레이드 패키지 다운로드, 9 페이지 참조). 준비 확인은 업그레이드 패키지에 포함되어 있습니다. 버전 6.2.1 이상의 업그레이드 패키지는 서명이 되어 있으며 이름이 .sh가 아닌 .sh.REL.tar로 끝납니다. 서명된 업그레이드 패키지는 압축을 풀지 마십시오.
- 모든 매니지드 디바이스에 컨피그레이션을 구축합니다. 그러지 않으면 준비 확인에 실패할 수 있습니다.

단계 **1** 관리자 권한이 있는 사용자로 셸에 로그인합니다.

단계 **2** 어플라이언스에 업그레이드 패키지가 있는지 확인합니다.

버전 6.2.3 이전 매니지드 디바이스의 경우 디바이스의 셸에서 SCP를 사용하여 업그레이드 패키지를 `/var/sf/updates`에 복사합니다. 버전 6.2.3 이상에서는 SCP를 사용할 수도 있고 Firepower Management Center를 사용하여 업그레이드 패키지를 푸시할 수도 있습니다.

Firepower Management Center의 경우에는 SCP 또는 웹 인터페이스를 사용합니다.

단계 **3** 루트 사용자로 다음 명령을 실행합니다.

```
sudo install_update.pl --readiness-check /var/sf/updates/update_package_name
```

단계 **4** 준비 확인이 완료되면 `/var/log/sf/$rpm_name/upgrade_readiness`에서 전체 준비 확인 보고서에 액세스합니다.

업그레이드 전 기타 작업 및 확인

업그레이드를 성공적으로 수행하려면 다음의 업그레이드 전 작업과 확인도 반드시 수행해야 합니다.

어플라이언스 통신 및 상태 확인

업그레이드 프로세스 중에 항상 구축의 어플라이언스가 성공적으로 통신하는지, 상태 모니터에서 보고하는 문제가 없는지 확인합니다. 사소한 문제가 중요한 문제로 커지기 전에 해결합니다.

릴리스 노트 검토

항상 릴리스 노트에서 중요한 정보와 릴리스 관련 정보를 읽어 봅니다.

- Firepower 릴리스 노트
- ASA 릴리스 노트
- FXOS 릴리스 노트

업그레이드 전/후 컨피그레이션 변경 계획

특히 주 버전을 업그레이드할 때는 업그레이드로 인해 컨피그레이션이 크게 변경되거나 컨피그레이션을 대폭 변경해야 할 수 있습니다.

예를 들어 버전 6.0에서는 Firepower Management Center 고가용성 지원이 제거되었습니다. 그러므로 업그레이드를 시작하기 전에 고가용성 쌍을 해제해야 합니다. 다른 예로, 버전 6.2.3에서는 보고서 섹션에서 사용하거나 포함할 수 있는 결과 수가 제한됩니다. 업그레이드 전 컨피그레이션에 따라 업그레이드 프로세스에서 결과 제한 수를 낮추고 PDF 보고서를 비활성화할 수 있습니다. 업그레이드 후에 새 제한에 맞게 보고서 템플릿을 조정하고 PDF 보고서를 다시 활성화할 수 있습니다.

업그레이드 전 및 후 컨피그레이션 변경 사항에 대한 자세한 내용은 릴리스 노트와 Firepower 소프트웨어 업그레이드 버전별 지침, 133 페이지를 참조하십시오.

시간 및 디스크 공간 확인

Firepower 어플라이언스를 업그레이드하려면 사용 가능한 디스크 공간이 충분해야 합니다. 그렇지 않으면 업그레이드에 실패합니다. 또한 업그레이드를 수행할 시간도 충분해야 합니다. 사용 중인 구축에 따라 제공된 예상 시간보다 업그레이드가 더 오래 걸릴 수도 있습니다. 예를 들어 메모리가 적은 어플라이언스와 로드가 많은 어플라이언스의 경우 업그레이드 시간이 더 오래 걸릴 수 있습니다. 준비 확인을 완료하는 데 필요한 시간도 제공된 예상 시간에 포함되지 않습니다.

릴리스별 시간 및 디스크 공간 목록은 Firepower 소프트웨어 업그레이드 시간 및 디스크 공간, 141 페이지를 참조하십시오.

대역폭 확인

6.2.3 이전 버전에서는 Firepower Management Center가 설치 중에 매니지드 디바이스에 업그레이드 패키지를 복사하며, 해당 작업을 별도로 수행할 수는 없습니다. 6.2.3 이상 버전에서는 실제 업그레이드를 실행하기 전에 매니지드 디바이스로 업그레이드 패키지를 복사(푸시)할 수 있습니다. 따라서 업그레이드 유지 보수 기간을 줄일 수 있습니다.

어떤 경우든 Firepower Management Center에서 디바이스로의 대량 데이터 전송을 수행할 수 있는 대역폭이 있는지 확인해야 합니다. 자세한 내용은 Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침(트러블슈팅 TechNote)을 참조하십시오.

컨피그레이션 및 이벤트 데이터 백업

업그레이드를 시작하기 전에 이벤트 및 컨피그레이션 데이터를 외부 위치에 백업합니다.

- Firepower Management Center - Firepower Management Center를 사용하여 컨피그레이션 및 이벤트 데이터 자체적으로 백업합니다.
- 대부분의 매니지드 디바이스 - Firepower Management Center를 사용하여 매니지드 디바이스에서 이벤트를 백업합니다. 대부분의 매니지드 디바이스의 경우, 개별 컨피그레이션 및 이벤트 백업 파일을 생성하는 방법은 없습니다.
- 7000 및 8000 Series 디바이스만 해당 - Firepower Management Center 또는 로컬 디바이스 GUI를 사용하여 컨피그레이션 및 이벤트 데이터를 백업합니다.

자세한 내용은 Firepower Management Center 컨피그레이션 가이드를 참조하십시오.

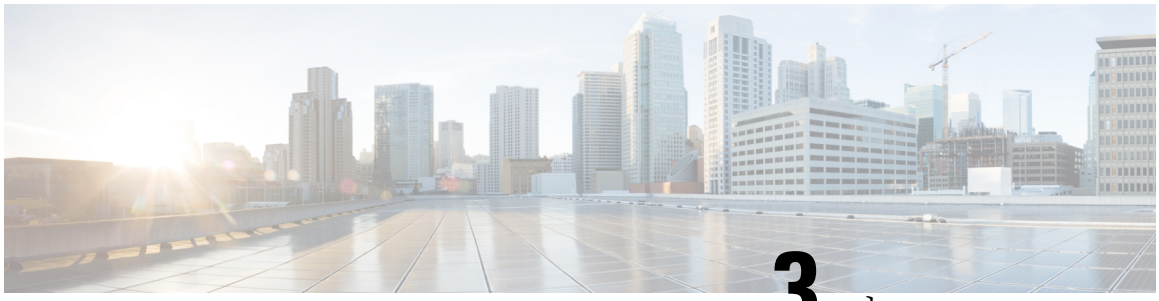
참고 외부 위치에 백업한 후 전송 성공을 확인하는 것이 좋습니다. Firepower Management Center는 업그레이드 시 로컬에 저장된 백업을 제거합니다.

유지 보수 기간 예약

유지 보수 기간을 예약할 때는 업그레이드가 트래픽 흐름 및 검사에 미치는 영향과 업그레이드에 걸릴 것으로 예상되는 시간을 고려합니다. 그리고 해당 기간에 반드시 수행해야 하는 작업과 미리 수행할 수 있는 작업도 고려합니다. 면밀한 계획과 준비를 통해 중단을 최소화해야 합니다. 업그레이드 패키지 다운로드/푸시, 준비 확인 실행, 백업 생성 등은 유지 보수 기간까지 기다리지 말고 수행하십시오.

I 부

Firepower 어플라이언스 업그레이드



3 장

Firepower Management Center 업그레이드

Firepower Management Center 업그레이드 체크리스트

이 체크리스트를 참조하여 Firepower Management Center(Firepower Management Center Virtual 포함)를 업그레이드합니다. 고가용성 쌍의 Firepower Management Center를 업그레이드하는 경우에는 각 피어에 대해 체크리스트를 작성합니다.

업그레이드할 때마다 체크리스트를 작성하십시오. 단계를 건너뛰면 업그레이드에 실패할 수 있습니다. 업그레이드 프로세스 중에 항상 구축의 어플라이언스가 성공적으로 통신하는지, 상태 모니터에서 보고하는 문제가 없는지 확인합니다.

업그레이드 계획

업그레이드 경로를 정확하게 계획하고 준수하여 항상 구축 호환성을 유지해야 합니다.

☐	작업/확인	세부 사항
	업그레이드 경로에서 현재 위치를 확인합니다. 방금 수행한 업그레이드와 다음에 수행할 업그레이드를 파악합니다.	업그레이드 경로 계획, 6 페이지
	Firepower Management Center의 현재 버전과 대상 버전을 확인합니다. • Firepower 소프트웨어 • 가상 호스팅 환경(Firepower Management Center Virtual)	Firepower Management Center: 물리적, 101 페이지 Firepower Management Center: 가상, 102 페이지

☐	작업/확인	세부 사항
	Firepower Management Center가 업그레이드 후에 디바이스를 관리할 수 있는지 확인합니다. 디바이스를 관리할 수 없는 경우 디바이스를 먼저 업그레이드할 수 있도록 업그레이드 경로를 수정합니다.	Firepower Management Center 및 매니지드 디바이스 버전 호환성, 99 페이지
	릴리스 노트에서 다음 업그레이드/업그레이드 집합을 확인하고 릴리스별 지침을 특히 주의하여 확인합니다.	Firepower 릴리스 노트

업그레이드 전 작업 및 확인

유지 보수 기간이 아닐 때 사전 확인을 수행하여 중단을 최소화합니다.

☐	작업/확인	세부 사항
	필요한 업그레이드 전 컨피그레이션을 변경합니다. 필요한 업그레이드 후 컨피그레이션을 변경할 수 있도록 준비합니다.	Firepower 소프트웨어 업그레이드 버전별 지침, 133 페이지 Firepower 릴리스 노트
	Firepower 소프트웨어 업그레이드를 위한 예비 디스크 공간 확인을 실행합니다.	Firepower 소프트웨어 업그레이드 시간 및 디스크 공간, 141 페이지
	올바른 Firepower 소프트웨어 업그레이드 패키지를 다운로드하여 Firepower Management Center에 업로드합니다. 버전 6.2.1 이상의 업그레이드 패키지는 서명이 되어 있으며 이름이 .sh가 아닌 .sh.REL.tar로 끝납니다. 서명된 업그레이드 패키지는 압축을 풀지 마십시오.	업그레이드 패키지 다운로드, 9 페이지
	준비 확인을 실행합니다. (선택 사항, 6.1 이상)	준비 확인 실행, 18 페이지
	이벤트 및 컨피그레이션 데이터 백업 외부 위치에 백업한 후 전송 성공을 확인합니다. Firepower Management Center는 업그레이드 시 로컬에 저장된 백업을 제거합니다.	Firepower Management Center 컨피그레이션 가이드
	다음 사항을 고려하여 업그레이드의 영향이 가장 적은 유지 보수 기간을 예약합니다. • 유지 보수 기간에 수행해야 하는 작업. • 업그레이드에 걸릴 것으로 예상되는 최소 시간.	Firepower 소프트웨어 업그레이드 시간 및 디스크 공간, 141 페이지

Firepower Management Center 업그레이드

유지 보수 기간에 업그레이드를 수행합니다.

☐	작업/확인	세부 사항
	필요한 경우 호스팅 환경을 업그레이드합니다 (Firepower Management Center Virtual에만 해당).	호스팅 환경 설명서를 참조하십시오.
	Firepower 소프트웨어를 업그레이드합니다.	독립형 Firepower Management Center 업그레이드, 27 페이지 고가용성 Firepower Management Center 업그레이드, 29 페이지

독립형 Firepower Management Center 업그레이드

독립형 Firepower Management Center(Firepower Management Center Virtual 포함)를 업그레이드하려면 이 절차를 사용합니다.

⚠

주의 업그레이드 중인 어플라이언스를 종료하거나, 수동으로 리부팅하거나, 해당 어플라이언스로/어플라이언스에서 변경 사항을 구축하지 마십시오. 진행 중인 업그레이드를 재시작하지 마십시오. 사전 확인 중에는 업그레이드 프로세스가 비활성 상태로 표시될 수 있으며 이는 정상적인 현상입니다. 업그레이드에 문제(업그레이드 실패 또는 응답하지 않는 어플라이언스 포함)가 있을 경우 Cisco TAC에 문의하십시오.

시작하기 전에

업그레이드 경로(호스팅 환경 및 매니지드 디바이스 업그레이드 포함)에서 현재 위치를 확인합니다. 이 단계를 완벽하게 계획하고 준비했는지 확인합니다.

단계 **1** 컨피그레이션이 오래된 매니지드 디바이스에 구축합니다.

Firepower Management Center 메뉴 바에서 **Deploy(구축)**를 클릭합니다. 디바이스를 선택하고 **Deploy(구축)**를 다시 클릭합니다. 지금 오래된 디바이스에 구축하지 않으면 최종 업그레이드에 실패할 수 있으며, 그러면 해당 디바이스에 이미지를 재설치해야 할 수 있습니다.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하면 Snort 프로세스가 재시작되어 트래픽 검사가 중단되며 디바이스가 트래픽을 처리하는 방법에 따라서 재시작이 완료될 때까지 트래픽도 중단될 수 있습니다. .

단계 **2** 업그레이드 전 최종 확인을 수행합니다.

- 상태 확인 - Message Center를 사용합니다(메뉴 바에서 System Status(시스템 상태) 아이콘 클릭). 구축의 어플라이언스가 성공적으로 통신하는지, 상태 모니터에서 보고하는 문제가 없는지 확인합니다.

- 작업 실행 - 역시 Message Center에서 필수 작업이 완료되었는지 확인합니다. 업그레이드를 시작할 때 실행 중인 작업은 중지되어 실패한 작업이 되며 다시 시작할 수 없습니다. 장애 발생 상태 메시지는 나중에 수동으로 삭제할 수 있습니다.
- 디스크 공간 확인 - 최종 디스크 공간 확인을 수행합니다. 사용 가능한 디스크 공간이 부족하면 업그레이드에 실패합니다.

단계 **3** **System**(시스템) > **Updates**(업데이트)를 선택합니다.

단계 **4** 사용하려는 업그레이드 패키지 옆의 Install(설치) 아이콘을 클릭하고 Firepower Management Center를 선택합니다.

단계 **5** **Install**(설치)을 클릭하여 업그레이드를 시작합니다.

업그레이드할 것임을 확인하고 Firepower Management Center를 리부팅합니다.

단계 **6** 로그아웃될 때까지 Message Center에서 사전 확인 진행 상황을 모니터링합니다.

Firepower Management Center가 업그레이드되는 중에는 컨피그레이션을 변경하거나 컨피그레이션 변경 사항을 디바이스에 구축하지 마십시오. Message Center에서 몇 분간 진행 상황이 표시되지 않거나 업그레이드에서 장애가 발생했다고 나타나더라도 업그레이드를 재시작하거나 Firepower Management Center를 리부팅하지 마십시오. 그 대신 Cisco TAC에 문의하십시오.

단계 **7** 가능할 때 Firepower Management Center에 다시 로그인합니다.

- 부 버전 업그레이드(패치 및 핫픽스) - 업그레이드가 완료되고 Firepower Management Center가 리부팅된 후에 로그인할 수 있습니다.
- 주 버전 업그레이드 - 업그레이드가 완료되기 전에 로그인할 수 있습니다. Firepower Management Center에는 업그레이드의 진행 상황을 모니터링하고 업그레이드 로그 및 오류 메시지를 확인할 수 있는 페이지가 표시됩니다. 업그레이드가 완료되고 Firepower Management Center가 리부팅되면 다시 로그아웃됩니다.

단계 **8** (주 버전 업그레이드에만 해당) Firepower Management Center에 다시 로그인합니다.

프롬프트가 표시되면 EULA(최종 사용자 라이선스 계약)를 검토하고 동의합니다. 이렇게 하지 않으면 로그아웃됩니다.

단계 **9** 업그레이드 성공을 확인합니다.

로그인할 때 Firepower Management Center에서 업그레이드 성공 알림이 표시되지 않으면 **Help**(도움말) > **About**(정보)을 선택하여 현재 소프트웨어 버전 정보를 표시합니다.

단계 **10** Message Center를 사용하여 구축 상태를 다시 확인합니다.

단계 **11** 침입 규칙 및 취약점 데이터베이스(VDB)를 업데이트합니다.

지원 사이트에서 제공되는 침입 규칙 업데이트 또는 VDB가 현재 실행 중인 버전보다 최신 상태이면 최신 버전을 설치합니다. 자세한 내용은 Firepower Management Center 컨피그레이션 가이드을 참조하십시오. 침입 규칙을 업데이트할 때는 정책을 자동으로 다시 적용할 필요가 없습니다. 정책은 나중에 다시 적용합니다.

단계 **12** 릴리스 노트에 설명되어 있는 업그레이드 후 컨피그레이션 변경을 완료합니다.

단계 **13** 컨피그레이션을 재구축합니다.

모든 매니지드 디바이스에 컨피그레이션을 재구축합니다. 특정 디바이스에 컨피그레이션을 구축하지 않으면 최종 업그레이드에 실패할 수 있으며, 그러면 해당 디바이스에 이미지를 재설치해야 합니다.

고가용성 Firepower Management Center 업그레이드

고가용성 쌍의 Firepower Management Center에서 Firepower 소프트웨어를 업그레이드하려면 이 절차를 참조합니다.

피어는 한 번에 하나씩 업그레이드합니다. 동기화가 일시 정지되면 스탠바이 피어를 먼저 업그레이드한 다음 액티브 피어를 업그레이드합니다. 스탠바이 Firepower Management Center가 사전 확인을 시작하면 해당 상태가 스탠바이에서 액티브로 전환되므로 두 피어가 모두 액티브 상태가 됩니다. 스플릿 브레인이라는 이 일시적인 상태는 업그레이드 중을 제외하고는 지원되지 않습니다. 고가용성 쌍이 스플릿 브레인 상태인 동안에는 컨피그레이션을 변경하거나 변경 사항을 구축하지 마십시오. Firepower Management Center를 업그레이드하고 동기화를 재시작한 후에는 변경 사항이 손실됩니다.

주의 업그레이드 중인 어플라이언스를 종료하거나, 수동으로 리부팅하거나, 해당 어플라이언스로/어플라이언스에서 변경 사항을 구축하지 마십시오. 진행 중인 업그레이드를 재시작하지 마십시오. 사전 확인 중에는 업그레이드 프로세스가 비활성 상태로 표시될 수 있으며 이는 정상적인 현상입니다. 업그레이드에 문제(업그레이드 실패 또는 응답하지 않는 어플라이언스 포함)가 있을 경우 Cisco TAC에 문의하십시오.

시작하기 전에

업그레이드 경로(매니지드 디바이스 업그레이드 포함)에서 현재 위치를 확인합니다. 이 단계를 완벽하게 계획하고 준비했는지 확인합니다.

단계 **1** 액티브 Firepower Management Center에서 컨피그레이션이 오래된 매니지드 디바이스로 변경 사항을 구축합니다.

Firepower Management Center 메뉴 바에서 **Deploy(**구축**)**를 클릭합니다. 디바이스를 선택하고 **Deploy(**구축**)**를 다시 클릭합니다. 지금 오래된 디바이스에 구축하지 않으면 최종 업그레이드에 실패할 수 있으며, 그러면 해당 디바이스에 이미지를 재설치해야 할 수 있습니다.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하면 Snort 프로세스가 재시작되어 트래픽 검사가 중단되며 디바이스가 트래픽을 처리하는 방법에 따라서 재시작이 완료될 때까지 트래픽도 중단될 수 있습니다. .

단계 **2** 동기화를 일시 정지하기 전에 Message Center를 사용하여 구축 상태를 확인합니다.

Firepower Management Center 메뉴 바에서 System Status(시스템 상태) 아이콘을 클릭하여 Message Center를 표시합니다. 구축의 어플라이언스가 성공적으로 통신하는지, 상태 모니터에서 보고하는 문제가 없는지 확인합니다.

단계 **3** 동기화를 일시 정지합니다.

a) **System(**시스템**)** > **Integration**(통합)을 선택합니다.

b) **High Availability(**고가용성**)** 탭에서 **Pause Synchronization(**동기화 일시 정지**)**을 클릭합니다.

단계 **4** Firepower Management Center를 한 번에 하나씩 업그레이드합니다.

a) 스탠바이 유닛을 업그레이드합니다.

b) 액티브 유닛을 업그레이드합니다.

업그레이드를 수행하려면 독립형 Firepower Management Center 업그레이드, 27 페이지의 지침을 따르되 초기 구축은 생략하고 각 Firepower Management Center에서 업데이트 성공을 확인한 후에 작업을 중지합니다. 고가용성 쌍이 스플릿 브레인 상태인 동안에는 컨피그레이션을 변경하거나 변경 사항을 구축하지 마십시오.

단계 **5** 액티브 피어로 설정할 Firepower Management Center에서 동기화를 재시작합니다.

a) **System(**시스템**)** > **Integration(**통합**)**을 선택합니다.

b) **High Availability(**고가용성**)** 탭에서 **Make-Me-Active(**액티브 상태로 전환**)**를 클릭합니다.

c) 고가용성 동기화가 재시작되고 다른 Firepower Management Center가 스탠바이 모드로 전환될 때까지 기다립니다.

단계 **6** Message Center를 사용하여 구축 상태를 다시 확인합니다.

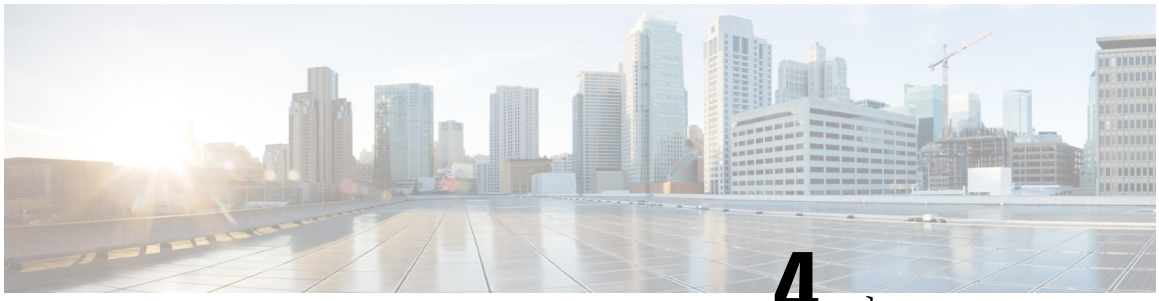
단계 **7** 침입 규칙 및 취약점 데이터베이스(VDB)를 업데이트합니다.

지원 사이트에서 제공되는 침입 규칙 업데이트 또는 VDB가 현재 실행 중인 버전보다 최신 상태이면 최신 버전을 설치합니다. 자세한 내용은 Firepower Management Center 컨피그레이션 가이드을 참조하십시오. 침입 규칙을 업데이트할 때는 정책을 자동으로 다시 적용할 필요가 없습니다. 정책은 나중에 다시 적용합니다.

단계 **8** 릴리스 노트에 설명되어 있는 업그레이드 후 컨피그레이션 변경을 완료합니다.

단계 **9** 컨피그레이션을 재구축합니다.

모든 매니지드 디바이스에 컨피그레이션을 재구축합니다. 특정 디바이스에 컨피그레이션을 구축하지 않으면 최종 업그레이드에 실패할 수 있으며, 그러면 해당 디바이스에 이미지를 재설치해야 합니다.



4 장

Firepower Threat Defense 디바이스 업그레이드

Firepower Threat Defense 업그레이드 체크리스트

이 체크리스트를 참조하여 Firepower 2100 Series, ASA 5500-X Series, ISA 3000 및 Firepower Threat Defense Virtual 디바이스를 업그레이드합니다.

업그레이드할 때마다 체크리스트를 작성하십시오. 단계를 건너뛰면 업그레이드에 실패할 수 있습니다. 업그레이드 프로세스 중에 항상 구축의 어플라이언스가 성공적으로 통신하는지, 상태 모니터에서 보고하는 문제가 없는지 확인합니다.

업그레이드 계획

업그레이드 경로를 정확하게 계획하고 준수하여 항상 구축 호환성을 유지해야 합니다.

☐	작업/확인	세부 사항
	업그레이드 경로에서 현재 위치를 확인합니다. 방금 수행한 업그레이드와 다음에 수행할 업그레이드를 파악합니다.	업그레이드 경로 계획, 6 페이지 Firepower Threat Defense 업그레이드 경로 - Firepower Management Center 포함, 112 페이지
	디바이스의 현재 버전과 대상 버전을 확인합니다. • Firepower Threat Defense 소프트웨어 • 가상 호스팅 환경(Firepower Threat Defense Virtual)	Firepower Threat Defense 디바이스, 102 페이지

☐	작업/확인	세부 사항
	디바이스를 업그레이드한 후 Firepower Management Center에서 해당 디바이스를 관리할 수 있는지 확인합니다. 디바이스를 관리할 수 없는 경우 Firepower Management Center를 먼저 업그레이드할 수 있도록 업그레이드 경로를 수정합니다.	Firepower Management Center 및 매니지드 디바이스 버전 호환성, 99 페이지
	릴리스 노트에서 다음 업그레이드/업그레이드 집합을 확인하고 릴리스별 지침을 특히 주의하여 확인합니다.	Firepower 릴리스 노트

업그레이드 전 작업 및 확인

유지 보수 기간이 아닐 때 사전 확인을 수행하여 중단을 최소화합니다.

☐	작업/확인	세부 사항
	필요한 업그레이드 전 컨피그레이션을 변경합니다. 필요한 업그레이드 후 컨피그레이션을 변경할 수 있도록 준비합니다.	Firepower 소프트웨어 업그레이드 버전별 지침, 133 페이지 Firepower 릴리스 노트
	Firepower 소프트웨어 업그레이드를 위한 예비 디스크 공간 확인을 실행합니다.	Firepower 소프트웨어 업그레이드 시간 및 디스크 공간, 141 페이지
	올바른 Firepower 소프트웨어 업그레이드 패키지를 다운로드하여 Firepower Management Center에 업로드합니다. 버전 6.2.1 이상의 업그레이드 패키지는 서명이 되어 있으며 이름이 .sh가 아닌 .sh.REL.tar로 끝납니다. 서명된 업그레이드 패키지는 압축을 풀지 마십시오.	업그레이드 패키지 다운로드, 9 페이지
	Firepower Management Center에서 디바이스로의 대량 데이터 전송을 수행할 수 있는 대역폭이 있는지 확인합니다.	Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침(트러블슈팅 TechNote)
	Firepower 소프트웨어 업그레이드 패키지를 디바이스로 푸시합니다. (선택 사항, 6.2.3 이상)	매니지드 디바이스로 업그레이드 패키지 푸시, 18 페이지
	준비 확인을 실행합니다. (선택 사항, 6.1 이상)	준비 확인 실행, 18 페이지
	Firepower Management Center를 사용하여 디바이스의 이벤트 데이터를 백업합니다. 외부 위치에 백업한 후 전송 성공을 확인합니다. Firepower Management Center는 업그레이드 시 로컬에 저장된 백업을 제거합니다.	Firepower Management Center 컨피그레이션 가이드

☐	작업/확인	세부 사항
		업그레이드 전 기타 작업 및 확인, 20 페이지
	다음 사항을 고려하여 업그레이드의 영향이 가장 적은 유지 보수 기간을 예약합니다. • 유지 보수 기간에 수행해야 하는 작업. • 업그레이드가 트래픽 흐름 및 검사에 미치는 영향. • 업그레이드에 걸릴 것으로 예상되는 최소 시간.	Firepower Threat Defense 업그레이드 동작, 128 페이지 Firepower 소프트웨어 업그레이드 시간 및 디스크 공간, 141 페이지

디바이스 업그레이드

업그레이드로 인해 트래픽 흐름이나 검사가 중단될 수 있으므로 유지 보수 기간에 업그레이드를 수행하십시오.

☐	작업/확인	세부 사항
	필요한 경우 호스팅 환경을 업그레이드합니다(Firepower Threat Defense Virtual에만 해당).	호스팅 환경 설명서를 참조하십시오.
	Firepower 소프트웨어를 업그레이드합니다.	Firepower Threat Defense 소프트웨어 업그레이드, 33 페이지

Firepower Threat Defense 소프트웨어 업그레이드

Firepower 2100 Series, ASA 5500-X Series, ISA 3000 및 Firepower Threat Defense Virtual 디바이스를 업그레이드하려면 이 절차를 사용합니다. 여러 디바이스가 동일한 업그레이드 패키지를 사용하는 경우 해당 디바이스를 한 번에 업데이트할 수 있습니다. 고가용성 쌍의 멤버는 동시에 업그레이드해야 합니다.

⚠

주의 업그레이드 중인 어플라이언스를 종료하거나, 수동으로 리부팅하거나, 해당 어플라이언스로/어플라이언스에서 변경 사항을 구축하지 마십시오. 진행 중인 업그레이드를 재시작하지 마십시오. 사전 확인 중에는 업그레이드 프로세스가 비활성 상태로 표시될 수 있으며 이는 정상적인 현상입니다. 업그레이드에 문제(업그레이드 실패 또는 응답하지 않는 어플라이언스 포함)가 있을 경우 Cisco TAC에 문의하십시오.

시작하기 전에

업그레이드 경로(가상 호스팅 환경 및 Firepower Management Center 업그레이드 포함)에서 현재 위치를 확인합니다. 이 단계를 완벽하게 계획하고 준비했는지 확인합니다.

단계 **1** 업그레이드하려는 디바이스에 컨피그레이션을 구축합니다.

Firepower Management Center 메뉴 바에서 **Deploy(**구축**)**를 클릭합니다. 디바이스를 선택하고 **Deploy(**구축**)**를 다시 클릭합니다. 지금 오래된 디바이스에 구축하지 않으면 최종 업그레이드에 실패할 수 있으며, 그러면 해당 디바이스에 이미지를 재설치해야 할 수 있습니다.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하면 Snort 프로세스가 재시작되어 트래픽 검사가 중단되며 디바이스가 트래픽을 처리하는 방법에 따라서 재시작이 완료될 때까지 트래픽도 중단될 수 있습니다. 자세한 내용은 Firepower Threat Defense 업그레이드 동작, 128 페이지를 참조하십시오.

단계 **2** 업그레이드 전 최종 확인을 수행합니다.

- 상태 확인 - Message Center를 사용합니다(메뉴 바에서 System Status(시스템 상태) 아이콘 클릭). 구축의 어플라이언스가 성공적으로 통신하는지, 상태 모니터에서 보고하는 문제가 없는지 확인합니다.
- 작업 실행 - 역시 Message Center에서 필수 작업이 완료되었는지 확인합니다. 업그레이드를 시작할 때 실행 중인 작업은 중지되어 실패한 작업이 되며 다시 시작할 수 없습니다. 장애 발생 상태 메시지는 나중에 수동으로 삭제할 수 있습니다.
- 디스크 공간 확인 - 최종 디스크 공간 확인을 수행합니다. 사용 가능한 디스크 공간이 부족하면 업그레이드에 실패합니다.

단계 **3** (선택 사항, 고가용성에만 해당) 고가용성 디바이스 쌍의 활성/스탠바이 역할을 전환합니다.

고가용성 쌍의 스탠바이 디바이스가 먼저 업그레이드됩니다. 디바이스에서 역할을 전환한 후 새 스탠바이 피어가 업그레이드됩니다. 업그레이드가 완료되어도 디바이스 역할은 전환된 상태로 유지됩니다. 액티브/스탠바이 역할을 유지하려면 업그레이드 전에 역할을 수동으로 전환하십시오. 이렇게 하면 업그레이드 프로세스에서 역할을 다시 전환합니다.

Devices(디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 쌍 옆의 **Switch Active Peer(**액티브 피어 전환**)** 아이콘을 클릭한 다음 선택을 확인합니다.

단계 **4** **System(**시스템**)** > **Updates(**업데이트**)**를 선택합니다.

단계 **5** 사용하려는 업그레이드 패키지 옆의 설치 아이콘을 클릭하고 업그레이드할 디바이스를 선택합니다.

업그레이드하려는 디바이스가 나열되어 있지 않은 경우 업그레이드 패키지를 잘못 선택한 것입니다.

참고 6개 이상의 디바이스를 동시에 업그레이드하지 않는 것이 좋습니다. 선택한 모든 디바이스에서 프로세스를 완료할 때까지 Firepower Management Center에서는 디바이스 업그레이드 중지를 허용하지 않습니다. 디바이스 하나의 업그레이드에서 문제가 발생하는 경우 모든 디바이스가 업그레이드를 완료해야 문제를 해결할 수 있습니다.

단계 **6** **Install(**설치**)**을 클릭하고 디바이스를 업그레이드 및 리부팅할 것임을 확인합니다.

일부 디바이스는 업데이트 중 두 번 리부팅될 수 있습니다. 이는 정상 동작입니다.

디바이스가 구성 및 구축된 방식에 따라 트래픽은 업그레이드 전 과정에서 삭제되거나 검사 없이 네트워크를 통과합니다. 자세한 내용은 Firepower Threat Defense 업그레이드 동작, 128 페이지를 참조하십시오.

단계 **7** Message Center에서 업그레이드 진행 상황을 모니터링합니다.

업그레이드되고 있는 디바이스에는 컨피그레이션을 구축하지 마십시오. Message Center에서 몇 분간 진행 상황이 표시되지 않거나 업그레이드에서 장애가 발생했다고 나타나더라도 업그레이드를 재시작하거나 디바이스를 리부팅하지 마십시오. 그 대신 Cisco TAC에 문의하십시오.

단계 **8** 업데이트 성공을 확인합니다.

업그레이드가 완료되면 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 업그레이드된 디바이스의 소프트웨어 버전이 정확한지 확인합니다.

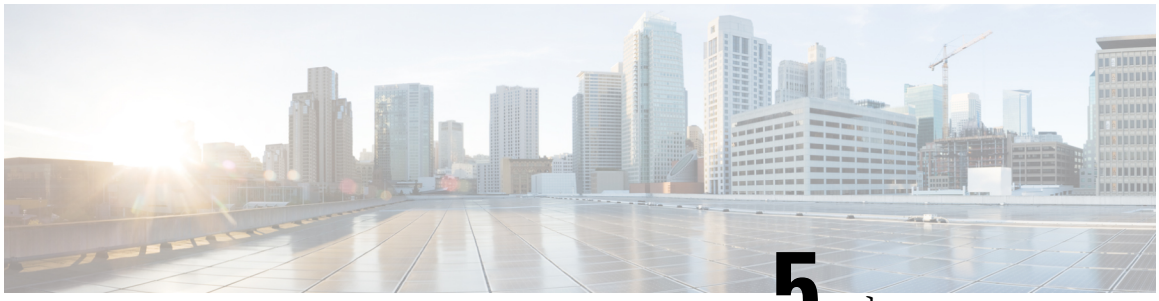
단계 **9** Message Center를 사용하여 구축 상태를 다시 확인합니다.

단계 **10** 침입 규칙 및 취약점 데이터베이스(VDB)를 업데이트합니다.

지원 사이트에서 제공되는 침입 규칙 업데이트 또는 VDB가 현재 실행 중인 버전보다 최신 상태이면 최신 버전을 설치합니다. 자세한 내용은 Firepower Management Center 컨피그레이션 가이드을 참조하십시오. 침입 규칙을 업데이트할 때는 정책을 자동으로 다시 적용할 필요가 없습니다. 정책은 나중에 다시 적용합니다.

단계 **11** 릴리스 노트에 설명되어 있는 업그레이드 후 컨피그레이션 변경을 완료합니다.

단계 **12** 방금 업그레이드한 디바이스에 컨피그레이션을 재구축합니다.



5 장

Firepower Threat Defense 디바이스 업그레이드 - Firepower 4100/9300 Series

Firepower Threat Defense 업그레이드 체크리스트 — Firepower 4100/9300 새시

이 체크리스트를 참조하여 Firepower 4100/9300 새시를 업그레이드합니다.

업그레이드할 때마다 체크리스트를 작성하십시오. 단계를 건너뛰면 업그레이드에 실패할 수 있습니다.업그레이드 프로세스 중에 항상 구축의 어플라이언스가 성공적으로 통신하는지, 상태 모니터에서 보고하는 문제가 없는지 확인합니다.

업그레이드 계획

업그레이드 경로를 정확하게 계획하고 준수하여 항상 구축 호환성을 유지해야 합니다.

☐	작업/확인	세부 사항
	업그레이드 경로에서 현재 위치를 확인합니다. 방금 수행한 업그레이드와 다음에 수행할 업그레이드를 파악합니다.	업그레이드 경로 계획, 6 페이지 Firepower Threat Defense 업그레이드 경로 - Firepower Management Center 포함, 112 페이지
	디바이스의 현재 버전과 대상 버전을 확인합니다. • Firepower 소프트웨어 • FXOS	Firepower 4100/9300 새시 with Firepower Threat Defense, 103 페이지

☐	작업/확인	세부 사항
	디바이스를 업그레이드한 후 Firepower Management Center에서 해당 디바이스를 관리할 수 있는지 확인합니다. 디바이스를 관리할 수 없는 경우 Firepower Management Center를 먼저 업그레이드할 수 있도록 업그레이드 경로를 수정합니다.	Firepower Management Center 및 매니지드 디바이스 버전 호환성, 99 페이지
	릴리스 노트에서 다음 업그레이드/업그레이드 집합을 확인하고 릴리스별 지침을 특히 주의하여 확인합니다.	Firepower 릴리스 노트 FXOS 릴리스 노트

업그레이드 전 작업 및 확인

유지 보수 기간이 아닐 때 사전 확인을 수행하여 중단을 최소화합니다.

☐	작업/확인	세부 사항
	필요한 업그레이드 전 컨피그레이션을 변경합니다. 필요한 업그레이드 후 컨피그레이션을 변경할 수 있도록 준비합니다.	Firepower 소프트웨어 업그레이드 버전별 지침, 133 페이지 Firepower 릴리스 노트 FXOS 릴리스 노트
	Firepower 소프트웨어 업그레이드를 위한 예비 디스크 공간 확인을 실행합니다.	Firepower 소프트웨어 업그레이드 시간 및 디스크 공간, 141 페이지
	올바른 Firepower 소프트웨어 업그레이드 패키지를 다운로드하여 Firepower Management Center에 업로드합니다. 버전 6.2.1 이상의 업그레이드 패키지는 서명이 되어 있으며 이름이 .sh가 아닌 .sh.REL.tar로 끝납니다. 서명된 업그레이드 패키지는 압축을 풀지 마십시오.	업그레이드 패키지 다운로드, 9 페이지
	Firepower Management Center에서 디바이스로의 대량 데이터 전송을 수행할 수 있는 대역폭이 있는지 확인합니다.	Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침(트러블슈팅 TechNote)
	Firepower 소프트웨어 업그레이드 패키지를 디바이스로 푸시합니다. (선택 사항, 6.2.3 이상)	매니지드 디바이스로 업그레이드 패키지 푸시, 18 페이지
	준비 확인을 실행합니다. (선택 사항, 6.1 이상)	준비 확인 실행, 18 페이지
	Firepower Management Center를 사용하여 디바이스의 이벤트 데이터를 백업합니다. 외부 위치에 백업한 후 전송 성공을 확인합니다. Firepower Management Center는 업그레이드 시 로컬에 저장된 백업을 제거합니다.	Firepower Management Center 컨피그레이션 가이드

☐	작업/확인	세부 사항
		업그레이드 전 기타 작업 및 확인, 20 페이지
	다음 사항을 고려하여 업그레이드의 영향이 가장 적은 유지 보수 기간을 예약합니다. • 유지 보수 기간에 수행해야 하는 작업. • 업그레이드가 트래픽 흐름 및 검사에 미치는 영향. • 업그레이드에 걸릴 것으로 예상되는 최소 시간.	Firepower Threat Defense 업그레이드 동작 — Firepower 4100/9300 섀시, 125 페이지 Firepower 소프트웨어 업그레이드 시간 및 디스크 공간, 141 페이지

디바이스 업그레이드

업그레이드로 인해 트래픽 흐름이나 검사가 중단될 수 있으므로 유지 보수 기간에 업그레이드를 수행하십시오.

☐	작업/확인	세부 사항
	필요한 경우, FXOS을 업그레이드합니다. 트래픽 흐름 및 검사 중단을 방지하려면 고가용성 쌍의 섀시와 섀시 간 클러스터를 한 번에 하나씩 업그레이드하십시오.	FXOS 업그레이드 - Firepower 4100/9300 섀시, 39 페이지
	Firepower 소프트웨어를 업그레이드합니다.	Firepower Threat Defense 소프트웨어 업그레이드 - Firepower 4100/9300 섀시, 59 페이지

FXOS 업그레이드 - Firepower 4100/9300 섀시

Firepower 4100/9300 섀시에서는 FXOS 운영 체제를 Firepower 소프트웨어와 별도로 업그레이드합니다. Firepower 섀시 간 클러스터링 또는 고가용성 쌍이 구성되어 있더라도 각 섀시에서 FXOS를 독립적으로 업그레이드합니다.

Firepower 주 버전에는 컴패니언 FXOS 버전이 있습니다. Firepower 4100/9300 섀시에서 Firepower 소프트웨어를 업그레이드하기 전에 FXOS의 해당 컴패니언 버전을 실행해야 합니다.

FXOS를 업그레이드하면 섀시가 리부팅됩니다. 사용 중인 구축에 따라 트래픽이 삭제되거나 검사 없이 네트워크를 통과할 수 있습니다.Firepower Threat Defense 업그레이드 동작 — Firepower 4100/9300 섀시, 125 페이지를 참조하십시오.

독립형 Firepower 4100/9300 섀시에서 FXOS 업그레이드

FXOS CLI 또는 Firepower Chassis Manager를 사용하여 독립형 또는 섀시 내 클러스터형 Firepower Threat Defense 논리적 디바이스가 설치되어 있는 Firepower 4100/9300 Series 보안 어플라이언스에서 FXOS 플랫폼 번들을 업그레이드합니다.

Firepower Chassis Manager를 사용하여 독립형 Firepower 4100/9300 섀시에서 FXOS 업그레이드

이 섹션에서는 독립형 Firepower 4100/9300 섀시에 대해 FXOS 플랫폼 번들을 업그레이드하는 방법을 설명합니다.

여기서는 다음 디바이스 유형에 대한 업그레이드 프로세스를 설명합니다.

- Firepower Threat Defense 논리적 디바이스로 구성되어 있으며 페일오버 쌍이나 섀시 간 클러스터의 일부분이 아닌 Firepower 4100 Series 섀시
- 페일오버 쌍이나 섀시 간 클러스터의 일부분이 아닌 독립형 Firepower Threat Defense 논리적 디바이스 하나 이상으로 구성된 Firepower 9300 섀시
- 섀시 내 클러스터에서 Firepower Threat Defense 논리적 디바이스로 구성된 Firepower 9300 섀시

시작하기 전에

업그레이드를 시작하기 전에 다음 작업을 이미 완료했는지 확인하십시오.

- 업그레이드 대상 FXOS 플랫폼 번들 소프트웨어 패키지를 다운로드합니다. Firepower 4100/9300 섀시용 FXOS 다운로드, 16 페이지를 참조하십시오.
- FXOS 및 Firepower Threat Defense 컨피그레이션을 백업합니다.

참고 업그레이드 프로세스에는 일반적으로 20~30분이 소요됩니다. 트래픽은 업그레이드되고 있는 디바이스를 통과하지 않습니다.

단계 **1** Firepower Chassis Manager에서 **System(**시스템**)** > **Updates(**업데이트**)**를 선택합니다.
Available Updates(사용 가능한 업데이트) 페이지는 섀시에서 사용 가능한 Firepower eXtensible 운영 체제 플랫폼 번들 이미지와 애플리케이션 이미지 목록을 보여줍니다.

단계 **2** 새 플랫폼 번들 이미지를 업로드합니다.

a) **Upload Image(**이미지 업로드**)**를 클릭하여 Upload Image(이미지 업로드) 대화 상자를 엽니다.
b) **Choose File(**파일 선택**)**을 클릭하여 업로드할 이미지로 이동한 다음 해당 이미지를 선택합니다.
c) **Upload(**업로드**)**를 클릭합니다.
선택한 이미지는 Firepower 4100/9300 섀시에 업로드됩니다.
d) 이미지를 업로드한 후에 특정 소프트웨어 이미지에 대한 최종 사용자 라이선스 계약이 표시됩니다. 시스템 프롬프트에 따라 최종 사용자 라이선스 계약에 동의합니다.

단계 **3** 새 플랫폼 번들 이미지가 업로드되면 업그레이드할 FXOS 플랫폼 번들의 **Upgrade(**업그레이드**)**를 클릭합니다.

시스템은 설치할 소프트웨어 패키지를 먼저 확인합니다. 시스템은 현재 설치된 애플리케이션과 지정된 FXOS 플랫폼 소프트웨어 패키지 간에 비호환성이 있는지 알려줍니다. 또한 기존 세션이 종료되고 시스템이 업그레이드의 일부로 재부팅되어야 한다고 경고합니다.

단계 **4** **Yes(**예**)**를 클릭하여 설치를 계속할지 확인하거나 **No(**아니요**)**를 클릭하여 설치를 취소합니다.

Firepower eXtensible 운영 체제에서는 번들의 압축을 풀고 구성 요소를 업그레이드하거나 다시 로드합니다. 업그레이드 프로세스를 완료하려면 최대 30분이 소요될 수 있습니다.

단계 **5** 업그레이드 중에는 Firepower Chassis Manager를 사용할 수 없습니다. FXOS CLI를 사용하여 업그레이드 프로세스를 모니터링할 수 있습니다.

a) **scope system**을 입력합니다.
b) **show firmware monitor**를 입력합니다.
c) 모든 구성 요소(FPRM, Fabric Interconnect 및 섀시)가 `Upgrade-Status: Ready`(업그레이드 상태: 준비)로 표시될 때까지 기다립니다.

참고 FPRM 구성 요소가 업그레이드되고 나면 시스템이 리부팅된 후 다른 구성 요소 업그레이드가 계속됩니다.

예제:

```
FP9300-A# scope systems
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

단계 **6** 모든 구성 요소가 업그레이드되면 다음 명령을 입력하여 보안 모듈/보안 엔진과 설치된 애플리케이션의 상태를 확인합니다.

a) **top**을 입력합니다.
b) **scope ssa**를 입력합니다.
c) **show slot**을 입력합니다.
d) Firepower 4100 Series 어플라이언스의 보안 엔진 또는 Firepower 9300 Appliance에 설치된 모든 보안 모듈의 Admin State(관리 상태)가 `Ok`(정상)이고 Oper State(작동 상태)가 `Online`(온라인) 인지 확인합니다.
e) **show app-instance**를 입력합니다.
f) 섀시에 설치된 모든 논리적 디바이스의 Oper State(작동 상태)가 `Online`(온라인) 인지 확인합니다.

FXOS CLI를 사용하여 독립형 Firepower 4100/9300 섀시에서 FXOS 업그레이드

이 섹션에서는 독립형 Firepower 4100/9300 섀시에 대해 FXOS 플랫폼 번들을 업그레이드하는 방법을 설명합니다.

여기서는 다음 디바이스 유형에 대한 FXOS 업그레이드 프로세스를 설명합니다.

- Firepower Threat Defense 논리적 디바이스로 구성되어 있으며 페일오버 쌍이나 섀시 간 클러스터의 일부분이 아닌 Firepower 4100 Series 섀시
- 페일오버 쌍이나 섀시 간 클러스터의 일부분이 아닌 독립형 Firepower Threat Defense 디바이스 하나 이상으로 구성된 Firepower 9300 섀시
- 섀시 내 클러스터에서 Firepower Threat Defense 논리적 디바이스로 구성된 Firepower 9300 섀시

시작하기 전에

업그레이드를 시작하기 전에 다음 작업을 이미 완료했는지 확인하십시오.

- 업그레이드 대상 FXOS 플랫폼 번들 소프트웨어 패키지를 다운로드합니다. Firepower 4100/9300 섀시용 FXOS 다운로드, 16 페이지를 참조하십시오.
- FXOS 및 Firepower Threat Defense 컨피그레이션을 백업합니다.
- Firepower 4100/9300 섀시에 소프트웨어 이미지를 다운로드하는 데 필요한 다음 정보를 수집합니다.
  - 이미지를 복사하고 있는 원본 서버의 IP 주소 및 인증 크리덴셜.
  - 이미지 파일의 정규화된 이름.

참고 업그레이드 프로세스에는 일반적으로 20~30분이 소요됩니다. 트래픽은 업그레이드되고 있는 디바이스를 통과하지 않습니다.

단계 **1** FXOS CLI에 연결합니다.

단계 **2** 새 플랫폼 번들 이미지를 Firepower 4100/9300 섀시에 다운로드합니다.

a) 펌웨어 모드를 입력합니다.

```
Firepower-chassis-a # scope firmware
```

b) FXOS 플랫폼 번들 소프트웨어 이미지를 다운로드합니다.

```
Firepower-chassis-a /firmware # download image URL
```

다음 구문 중 하나를 사용하여 가져올 파일의 URL을 지정합니다.

- **ftp**://*username@hostname/path/image_name*
- **scp**://*username@hostname/path/image_name*

- **sftp**://*username@hostname* / *path* / *image_name*
- **tftp**://*hostname* **:** *port-num* / *path* / *image_name*

c) 다음 명령을 사용하여 다운로드 프로세스를 모니터링합니다.

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

예제**:**

다음 예에서는 SCP 프로토콜을 사용하여 이미지를 복사합니다.

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

단계 **3** 필요한 경우 펌웨어 모드를 다시 설정합니다.

Firepower-chassis-a /firmware/download-task # **up**

단계 **4** 자동 설치 모드를 입력합니다.

Firepower-chassis-a /firmware # **scopeauto-install**

단계 **5** FXOS 플랫폼 번들을 설치합니다.

Firepower-chassis-a /firmware/auto-install # **installplatformplatform-vers** *version_number*

*version_number*는 설치 중인 FXOS 플랫폼 번들의 버전 번호입니다(예: 2.3(1.58)).

단계 **6** 시스템은 설치할 소프트웨어 패키지를 먼저 확인합니다. 시스템은 현재 설치된 애플리케이션과 지정된 FXOS 플랫폼 소프트웨어 패키지 간에 비호환성이 있는지 알려줍니다. 또한 기존 세션이 종료되고 시스템이 업그레이드의 일부로 재부팅되어야 한다고 경고합니다.

yes를 입력하여 검증을 계속할 것인지 확인합니다.

단계 **7** **yes**를 입력하여 설치를 계속할 것인지 확인하거나 **no**를 입력하여 설치를 취소합니다.

Firepower eXtensible 운영 체제에서는 번들의 압축을 풀고 구성 요소를 업그레이드하거나 다시 로드합니다.

단계 **8** 업그레이드 프로세스를 모니터링하려면 다음과 같이 합니다.

a) **scope system**을 입력합니다.

b) **show firmware monitor**를 입력합니다.

c) 모든 구성 요소(FPRM, Fabric Interconnect 및 섀시)가 `Upgrade-Status: Ready`(업그레이드 상태: 준비)로 표시될 때까지 기다립니다.

참고 FPRM 구성 요소가 업그레이드되고 나면 시스템이 리부팅된 후 다른 구성 요소 업그레이드가 계속됩니다.

예제:

```
FP9300-A# scope systems
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

단계 **9** 모든 구성 요소가 업그레이드되면 다음 명령을 입력하여 보안 모듈/보안 엔진과 설치된 애플리케이션의 상태를 확인합니다.

a) **top**을 입력합니다.
b) **scope ssa**를 입력합니다.
c) **show slot**을 입력합니다.
d) Firepower 4100 Series 어플라이언스의 보안 엔진 또는 Firepower 9300 Appliance에 설치된 모든 보안 모듈의 Admin State(관리 상태)가 `Ok`(정상)이고 Oper State(작동 상태)가 `Online`(온라인)인지 확인합니다.
e) **show app-instance**를 입력합니다.
f) 섀시에 설치된 모든 논리적 디바이스의 Oper State(작동 상태)가 `Online`(온라인)인지 확인합니다.

Firepower Threat Defense 고가용성 쌍에서 FXOS 업그레이드

FXOS CLI 또는 Firepower Chassis Manager를 사용하여 고가용성 쌍으로 구성된 Firepower Threat Defense 논리적 디바이스를 포함하는 Firepower 4100/9300 Series 보안 어플라이언스에서 FXOS 플랫폼 번들을 업그레이드합니다.

Firepower Chassis Manager를 사용하여 Firepower Threat Defense 고가용성 쌍에서 FXOS 업그레이드

Firepower Threat Defense 논리적 디바이스가 고가용성 쌍으로 구성된 Firepower 9300 또는 Firepower 4100 Series 보안 어플라이언스가 있는 경우 다음 절차에 따라 Firepower 9300 또는 Firepower 4100 Series 보안 어플라이언스에서 FXOS 플랫폼 번들을 업데이트하십시오.

시작하기 전에

업그레이드를 시작하기 전에 다음 작업을 이미 완료했는지 확인하십시오.

- 업그레이드 대상 FXOS 플랫폼 번들 소프트웨어 패키지를 다운로드합니다. Firepower 4100/9300 섀시용 FXOS 다운로드, 16 페이지를 참조하십시오.
- FXOS 및 Firepower Threat Defense 컨피그레이션을 백업합니다.

참고 업그레이드 프로세스에는 일반적으로 섀시당 20~30분이 소요됩니다.

단계 **1** 스탠바이 Firepower Threat Defense 논리적 디바이스가 포함된 Firepower 보안 어플라이언스에서 Firepower Chassis Manager에 연결합니다.

단계 **2** Firepower Chassis Manager에서 **System(**시스템**)** > **Updates(**업데이트**)**를 선택합니다.
Available Updates(사용 가능한 업데이트) 페이지는 섀시에서 사용 가능한 Firepower eXtensible 운영 체제 플랫폼 번들 이미지와 애플리케이션 이미지 목록을 보여줍니다.

단계 **3** 새 플랫폼 번들 이미지를 업로드합니다.

a) **Upload Image(**이미지 업로드**)**를 클릭하여 Upload Image(이미지 업로드) 대화 상자를 엽니다.
b) **Choose File(**파일 선택**)**을 클릭하여 업로드할 이미지로 이동한 다음 해당 이미지를 선택합니다.
c) **Upload(**업로드**)**를 클릭합니다.
선택한 이미지는 Firepower 4100/9300 섀시에 업로드됩니다.
d) 이미지를 업로드한 후에 특정 소프트웨어 이미지에 대한 최종 사용자 라이선스 계약이 표시됩니다. 시스템 프롬프트에 따라 최종 사용자 라이선스 계약에 동의합니다.

단계 **4** 새 플랫폼 번들 이미지가 업로드되면 업그레이드할 FXOS 플랫폼 번들의 **Upgrade(**업그레이드**)**를 클릭합니다.

시스템은 설치할 소프트웨어 패키지를 먼저 확인합니다. 시스템은 현재 설치된 애플리케이션과 지정된 FXOS 플랫폼 소프트웨어 패키지 간에 비호환성이 있는지 알려줍니다. 또한 기존 세션이 종료되고 시스템이 업그레이드의 일부로 재부팅되어야 한다고 경고합니다.

단계 **5** **Yes(**예**)**를 클릭하여 설치를 계속할지 확인하거나 **No(**아니요**)**를 클릭하여 설치를 취소합니다.

Firepower eXtensible 운영 체제에서는 번들의 압축을 풀고 구성 요소를 업그레이드하거나 다시 로드합니다. 업그레이드 프로세스를 완료하려면 최대 30분이 소요될 수 있습니다.

단계 **6** 업그레이드 중에는 Firepower Chassis Manager를 사용할 수 없습니다. FXOS CLI를 사용하여 업그레이드 프로세스를 모니터링할 수 있습니다.

a) **scope system**을 입력합니다.
b) **show firmware monitor**를 입력합니다.
c) 모든 구성 요소(FPRM, Fabric Interconnect 및 섀시)가 `Upgrade-Status: Ready`(업그레이드 상태: 준비)로 표시될 때까지 기다립니다.

참고 FPRM 구성 요소가 업그레이드되고 나면 시스템이 리부팅된 후 다른 구성 요소 업그레이드가 계속됩니다.

예제:

```
FP9300-A# scope systems
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

단계 **7** 모든 구성 요소가 업그레이드되면 다음 명령을 입력하여 보안 모듈/보안 엔진과 설치된 애플리케이션의 상태를 확인합니다.

a) **top**을 입력합니다.
b) **scope ssa**를 입력합니다.
c) **show slot**을 입력합니다.
d) Firepower 4100 Series 어플라이언스의 보안 엔진 또는 Firepower 9300 Appliance에 설치된 모든 보안 모듈의 Admin State(관리 상태)가 `Ok`(정상)이고 Oper State(작동 상태)가 `Online`(온라인)인지 확인합니다.
e) **show app-instance**를 입력합니다.
f) 섀시에 설치된 모든 논리적 디바이스의 Oper State(작동 상태)가 `Online`(온라인)인지 확인합니다.

단계 **8** 방금 업그레이드한 유닛을 액티브 유닛으로 만들어 트래픽이 업그레이드된 유닛으로 이동하게 합니다.

a) Firepower Management Center에 연결합니다.
b) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.
c) 액티브 피어를 변경할 고가용성 쌍 옆에 있는 Switch Active Peer(액티브 피어 전환) 아이콘()을 클릭합니다.
d) **Yes(**예**)**를 클릭하여 스탠바이 디바이스를 고가용성 쌍의 액티브 디바이스로 즉시 설정합니다.

단계 **9** 새 스탠바이 Firepower Threat Defense 논리적 디바이스가 포함된 Firepower 보안 어플라이언스에서 Firepower Chassis Manager에 연결합니다.

단계 **10** Firepower Chassis Manager에서 **System(**시스템**)** > **Updates(**업데이트**)**를 선택합니다.
Available Updates(사용 가능한 업데이트) 페이지는 섀시에서 사용 가능한 Firepower eXtensible 운영 체제 플랫폼 번들 이미지와 애플리케이션 이미지 목록을 보여줍니다.

단계 **11** 새 플랫폼 번들 이미지를 업로드합니다.

a) **Upload Image(**이미지 업로드**)**를 클릭하여 Upload Image(이미지 업로드) 대화 상자를 엽니다.
b) **Choose File(**파일 선택**)**을 클릭하여 업로드할 이미지로 이동한 다음 해당 이미지를 선택합니다.
c) **Upload(**업로드**)**를 클릭합니다.
선택한 이미지는 Firepower 4100/9300 섀시에 업로드됩니다.
d) 이미지를 업로드한 후에 특정 소프트웨어 이미지에 대한 최종 사용자 라이선스 계약이 표시됩니다. 시스템 프롬프트에 따라 최종 사용자 라이선스 계약에 동의합니다.

단계 **12** 새 플랫폼 번들 이미지가 업로드되면 업그레이드할 FXOS 플랫폼 번들의 **Upgrade(**업그레이드**)**를 클릭합니다.

시스템은 설치할 소프트웨어 패키지를 먼저 확인합니다. 시스템은 현재 설치된 애플리케이션과 지정된 FXOS 플랫폼 소프트웨어 패키지 간에 비호환성이 있는지 알려줍니다. 또한 기존 세션이 종료되고 시스템이 업그레이드의 일부로 재부팅되어야 한다고 경고합니다.

단계 **13** **Yes(**예**)**를 클릭하여 설치를 계속할지 확인하거나 **No(**아니요**)**를 클릭하여 설치를 취소합니다.

Firepower eXtensible 운영 체제에서는 번들의 압축을 풀고 구성 요소를 업그레이드하거나 다시 로드합니다. 업그레이드 프로세스를 완료하려면 최대 30분이 소요될 수 있습니다.

단계 **14** 업그레이드 중에는 Firepower Chassis Manager를 사용할 수 없습니다. FXOS CLI를 사용하여 업그레이드 프로세스를 모니터링할 수 있습니다.

a) **scope system**을 입력합니다.
b) **show firmware monitor**를 입력합니다.
c) 모든 구성 요소(FPRM, Fabric Interconnect 및 섀시)가 `Upgrade-Status: Ready`(업그레이드 상태: 준비)로 표시될 때까지 기다립니다.

참고 FPRM 구성 요소가 업그레이드되고 나면 시스템이 리부팅된 후 다른 구성 요소 업그레이드가 계속됩니다.

예제:

```
FP9300-A# scope systems
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

단계 **15** 모든 구성 요소가 업그레이드되면 다음 명령을 입력하여 보안 모듈/보안 엔진과 설치된 애플리케이션의 상태를 확인합니다.

a) **top**을 입력합니다.

b) **scope ssa**를 입력합니다.
c) **show slot**을 입력합니다.
d) Firepower 4100 Series 어플라이언스의 보안 엔진 또는 Firepower 9300 Appliance에 설치된 모든 보안 모듈의 Admin State(관리 상태)가 `Ok`(정상)이고 Oper State(작동 상태)가 `Online`(온라인)인지 확인합니다.
e) **show app-instance**를 입력합니다.
f) 섀시에 설치된 모든 논리적 디바이스의 Oper State(작동 상태)가 `Online`(온라인)인지 확인합니다.

단계 **16** 방금 업그레이드한 유닛을 업그레이드 이전처럼 액티브 유닛으로 만듭니다.

a) Firepower Management Center에 연결합니다.
b) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.
c) 액티브 피어를 변경할 고가용성 쌍 옆에 있는 Switch Active Peer(액티브 피어 전환) 아이콘()을 클릭합니다.
d) **Yes(**예**)**를 클릭하여 스탠바이 디바이스를 고가용성 쌍의 액티브 디바이스로 즉시 설정합니다.

FXOS CLI를 사용하여 Firepower Threat Defense 고가용성 쌍에서 FXOS 업그레이드

Firepower Threat Defense 논리적 디바이스가 고가용성 쌍으로 구성된 Firepower 9300 또는 Firepower 4100 Series 보안 어플라이언스가 있는 경우 다음 절차에 따라 Firepower 9300 또는 Firepower 4100 Series 보안 어플라이언스에서 FXOS 플랫폼 번들을 업데이트하십시오.

시작하기 전에

업그레이드를 시작하기 전에 다음 작업을 이미 완료했는지 확인하십시오.

- 업그레이드 대상 FXOS 플랫폼 번들 소프트웨어 패키지를 다운로드합니다. Firepower 4100/9300 섀시용 FXOS 다운로드, 16 페이지를 참조하십시오.
- FXOS 및 Firepower Threat Defense 컨피그레이션을 백업합니다.
- Firepower 4100/9300 섀시에 소프트웨어 이미지를 다운로드하는 데 필요한 다음 정보를 수집합니다.
  - 이미지를 복사하고 있는 원본 서버의 IP 주소 및 인증 크리덴셜.
  - 이미지 파일의 정규화된 이름.

참고 업그레이드 프로세스에는 일반적으로 섀시당 20~30분이 소요됩니다.

단계 **1** 스탠바이 Firepower Threat Defense 논리적 디바이스가 포함된 Firepower 보안 어플라이언스에서 FXOS CLI에 연결합니다.

단계 **2** 새 플랫폼 번들 이미지를 Firepower 4100/9300 섀시에 다운로드합니다.

a) 펌웨어 모드를 입력합니다.

Firepower-chassis-a # **scope firmware**

b) FXOS 플랫폼 번들 소프트웨어 이미지를 다운로드합니다.

Firepower-chassis-a /firmware # **download image** *URL*

다음 구문 중 하나를 사용하여 가져올 파일의 URL을 지정합니다.

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

c) 다음 명령을 사용하여 다운로드 프로세스를 모니터링합니다.

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

예제**:**

다음 예에서는 SCP 프로토콜을 사용하여 이미지를 복사합니다.

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

단계 **3** 필요한 경우 펌웨어 모드를 다시 설정합니다.

Firepower-chassis-a /firmware/download-task # **up**

단계 **4** 자동 설치 모드를 입력합니다.

Firepower-chassis-a /firmware # **scopeauto-install**

단계 **5** FXOS 플랫폼 번들을 설치합니다.

Firepower-chassis-a /firmware/auto-install # **installplatformplatform-vers** *version_number*

*version_number*는 설치 중인 FXOS 플랫폼 번들의 버전 번호입니다(예: 2.3(1.58)).

단계 **6** 시스템은 설치할 소프트웨어 패키지를 먼저 확인합니다. 시스템은 현재 설치된 애플리케이션과 지정된 FXOS 플랫폼 소프트웨어 패키지 간에 비호환성이 있는지 알려줍니다. 또한 기존 세션이 종료되고 시스템이 업그레이드의 일부로 재부팅되어야 한다고 경고합니다.

yes를 입력하여 검증을 계속할 것인지 확인합니다.

단계 **7** **yes**를 입력하여 설치를 계속할 것인지 확인하거나 **no**를 입력하여 설치를 취소합니다.

Firepower eXtensible 운영 체제에서는 번들의 압축을 풀고 구성 요소를 업그레이드하거나 다시 로드합니다.

단계 **8** 업그레이드 프로세스를 모니터링하려면 다음과 같이 합니다.

a) **scope system**을 입력합니다.

b) **show firmware monitor**를 입력합니다.

c) 모든 구성 요소(FPRM, Fabric Interconnect 및 새시)가 `Upgrade-Status: Ready`(업그레이드 상태: 준비)로 표시될 때까지 기다립니다.

참고 FPRM 구성 요소가 업그레이드되고 나면 시스템이 리부팅된 후 다른 구성 요소 업그레이드가 계속됩니다.

예제:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

단계 **9** 모든 구성 요소가 업그레이드되면 다음 명령을 입력하여 보안 모듈/보안 엔진과 설치된 애플리케이션의 상태를 확인합니다.

a) **top**을 입력합니다.

b) **scope ssa**를 입력합니다.

c) **show slot**을 입력합니다.

d) Firepower 4100 Series 어플라이언스의 보안 엔진 또는 Firepower 9300 Appliance에 설치된 모든 보안 모듈의 Admin State(관리 상태)가 `Ok`(정상)이고 Oper State(작동 상태)가 `Online`(온라인)인지 확인합니다.

e) **show app-instance**를 입력합니다.

f) 새시에 설치된 모든 논리적 디바이스의 Oper State(작동 상태)가 `Online`(온라인)인지 확인합니다.

단계 **10** 방금 업그레이드한 유닛을 액티브 유닛으로 만들어 트래픽이 업그레이드된 유닛으로 이동하게 합니다.

a) Firepower Management Center에 연결합니다.

b) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

c) 액티브 피어를 변경할 고가용성 쌍 옆에 있는 Switch Active Peer(액티브 피어 전환) 아이콘()을 클릭합니다.

d) **Yes(**예**)**를 클릭하여 스탠바이 디바이스를 고가용성 쌍의 액티브 디바이스로 즉시 설정합니다.

단계 **11** 새 스탠바이 Firepower Threat Defense 논리적 디바이스가 포함된 Firepower 보안 어플라이언스에서 FXOS CLI에 연결합니다.

단계 **12** 새 플랫폼 번들 이미지를 Firepower 4100/9300 섀시에 다운로드합니다.

a) 펌웨어 모드를 입력합니다.

Firepower-chassis-a # **scope firmware**

b) FXOS 플랫폼 번들 소프트웨어 이미지를 다운로드합니다.

Firepower-chassis-a /firmware # **download image** *URL*

다음 구문 중 하나를 사용하여 가져올 파일의 URL을 지정합니다.

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

c) 다음 명령을 사용하여 다운로드 프로세스를 모니터링합니다.

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

예제:

다음 예에서는 SCP 프로토콜을 사용하여 이미지를 복사합니다.

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

단계 **13** 필요한 경우 펌웨어 모드를 다시 설정합니다.

Firepower-chassis-a /firmware/download-task # **up**

단계 **14** 자동 설치 모드를 입력합니다.

Firepower-chassis-a /firmware # **scopeauto-install**

단계 **15** FXOS 플랫폼 번들을 설치합니다.

Firepower-chassis-a /firmware/auto-install # **installplatformplatform-vers** *version_number*

*version_number*는 설치 중인 FXOS 플랫폼 번들의 버전 번호입니다(예: 2.3(1.58)).

단계 **16** 시스템은 설치할 소프트웨어 패키지를 먼저 확인합니다. 시스템은 현재 설치된 애플리케이션과 지정된 FXOS 플랫폼 소프트웨어 패키지 간에 비호환성이 있는지 알려줍니다. 또한 기존 세션이 종료되고 시스템이 업그레이드의 일부로 재부팅되어야 한다고 경고합니다.

yes를 입력하여 검증을 계속할 것인지 확인합니다.

단계 **17** **yes**를 입력하여 설치를 계속할 것인지 확인하거나 **no**를 입력하여 설치를 취소합니다.

Firepower eXtensible 운영 체제에서는 번들의 압축을 풀고 구성 요소를 업그레이드하거나 다시 로드합니다.

단계 **18** 업그레이드 프로세스를 모니터링하려면 다음과 같이 합니다.

a) **scope system**을 입력합니다.
b) **show firmware monitor**를 입력합니다.
c) 모든 구성 요소(FPRM, Fabric Interconnect 및 섀시)가 `Upgrade-Status: Ready`(업그레이드 상태: 준비)로 표시될 때까지 기다립니다.

참고 FPRM 구성 요소가 업그레이드되고 나면 시스템이 리부팅된 후 다른 구성 요소 업그레이드가 계속됩니다.

예제:

```
FP9300-A# scope systems
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

단계 **19** 모든 구성 요소가 업그레이드되면 다음 명령을 입력하여 보안 모듈/보안 엔진과 설치된 애플리케이션의 상태를 확인합니다.

a) **top**을 입력합니다.
b) **scope ssa**를 입력합니다.
c) **show slot**을 입력합니다.
d) Firepower 4100 Series 어플라이언스의 보안 엔진 또는 Firepower 9300 Appliance에 설치된 모든 보안 모듈의 Admin State(관리 상태)가 `Ok`(정상)이고 Oper State(작동 상태)가 `Online`(온라인)인지 확인합니다.
e) **show app-instance**를 입력합니다.
f) 섀시에 설치된 모든 논리적 디바이스의 Oper State(작동 상태)가 `Online`(온라인)인지 확인합니다.

단계 **20** 방금 업그레이드한 유닛을 업그레이드 이전처럼 액티브 유닛으로 만듭니다.

a) Firepower Management Center에 연결합니다.
b) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.
c) 액티브 피어를 변경할 고가용성 쌍 옆에 있는 Switch Active Peer(액티브 피어 전환) 아이콘()을 클릭합니다.
d) **Yes(**예**)**를 클릭하여 스탠바이 디바이스를 고가용성 쌍의 액티브 디바이스로 즉시 설정합니다.

Firepower Threat Defense 섀시 간 클러스터에서 FXOS 업그레이드

FXOS CLI 또는 Firepower Chassis Manager를 사용하여 섀시 간 클러스터로 구성된 Firepower Threat Defense 논리적 디바이스를 포함하는 Firepower 4100/9300 Series 보안 어플라이언스에서 FXOS 플랫폼 번들을 업그레이드합니다.

Firepower Chassis Manager를 사용하여 Firepower Threat Defense 섀시 간 클러스터에서 FXOS 업그레이드

Firepower Threat Defense 논리적 디바이스가 섀시 간 클러스터로 구성된 Firepower 9300 또는 Firepower 4100 Series 보안 어플라이언스가 있는 경우 다음 절차에 따라 Firepower 9300 또는 Firepower 4100 Series 보안 어플라이언스에서 FXOS 플랫폼 번들을 업데이트하십시오.

시작하기 전에

업그레이드를 시작하기 전에 다음 작업을 이미 완료했는지 확인하십시오.

- 업그레이드 대상 FXOS 플랫폼 번들 소프트웨어 패키지를 다운로드합니다. Firepower 4100/9300 섀시용 FXOS 다운로드, 16 페이지를 참조하십시오.
- FXOS 및 Firepower Threat Defense 컨피그레이션을 백업합니다.

참고 업그레이드 프로세스에는 일반적으로 섀시당 20~30분이 소요됩니다.

단계 **1** 다음 명령을 입력하여 보안 모듈/보안 엔진과 설치된 애플리케이션의 상태를 확인합니다.

a) 섀시 #2(기본 유닛이 없는 섀시)의 FXOS CLI에 연결합니다.
b) **top**을 입력합니다.
c) **scope ssa**를 입력합니다.
d) **show slot**을 입력합니다.
e) Firepower 4100 Series 어플라이언스의 보안 엔진 또는 Firepower 9300 Appliance에 설치된 모든 보안 모듈의 Admin State(관리 상태)가 `Ok`(정상)이고 Oper State(작동 상태)가 `Online`(온라인)인지 확인합니다.
f) **show app-instance**를 입력합니다.
g) 섀시에 설치된 모든 논리적 디바이스의 Oper State(작동 상태)가 `Online`(온라인)이고 Cluster State(클러스터 상태)가 `In Cluster`(클러스터 내)인지 확인합니다. 그리고 정확한 Firepower Threat Defense 소프트웨어 버전이 Running Version(실행 중인 버전)으로 표시되는지 확인합니다.

참고 기본 유닛이 이 섀시에 없음을 확인합니다. Cluster Role(클러스터 역할)이 `Master(마스터)`로 설정된 Firepower Threat Defense 인스턴스가 없어야 합니다.

h) 다음 명령을 사용하여 Firepower 9300 Appliance에 설치된 모든 보안 모듈 또는 Firepower 4100 Series 어플라이언스의 보안 엔진에 대해 FXOS 버전이 정확한지 확인합니다.

scope server 1/*slot_id*. 여기서 *slot_id*는 Firepower 4100 Series 보안 엔진의 경우 1입니다.

show version.

단계 **2** 섀시 #2(기본 유닛이 없는 섀시)의 Firepower Chassis Manager에 연결합니다.

단계 **3** Firepower Chassis Manager에서 **System(**시스템**)** > **Updates(**업데이트**)**를 선택합니다.
Available Updates(사용 가능한 업데이트) 페이지는 섀시에서 사용 가능한 Firepower eXtensible 운영 체제 플랫폼 번들 이미지와 애플리케이션 이미지 목록을 보여줍니다.

단계 **4** 새 플랫폼 번들 이미지를 업로드합니다.

a) **Upload Image(**이미지 업로드**)**를 클릭하여 Upload Image(이미지 업로드) 대화 상자를 엽니다.
b) **Choose File(**파일 선택**)**을 클릭하여 업로드할 이미지로 이동한 다음 해당 이미지를 선택합니다.
c) **Upload(**업로드**)**를 클릭합니다.
선택한 이미지는 Firepower 4100/9300 섀시에 업로드됩니다.
d) 이미지를 업로드한 후에 특정 소프트웨어 이미지에 대한 최종 사용자 라이선스 계약이 표시됩니다. 시스템 프롬프트에 따라 최종 사용자 라이선스 계약에 동의합니다.

단계 **5** 새 플랫폼 번들 이미지가 업로드되면 업그레이드할 FXOS 플랫폼 번들의 **Upgrade(**업그레이드**)**를 클릭합니다.

시스템은 설치할 소프트웨어 패키지를 먼저 확인합니다. 시스템은 현재 설치된 애플리케이션과 지정된 FXOS 플랫폼 소프트웨어 패키지 간에 비호환성이 있는지 알려줍니다. 또한 기존 세션이 종료되고 시스템이 업그레이드의 일부로 재부팅되어야 한다고 경고합니다.

단계 **6** **Yes(**예**)**를 클릭하여 설치를 계속할지 확인하거나 **No(**아니요**)**를 클릭하여 설치를 취소합니다.

Firepower eXtensible 운영 체제에서는 번들의 압축을 풀고 구성 요소를 업그레이드하거나 다시 로드합니다. 업그레이드 프로세스를 완료하려면 최대 30분이 소요될 수 있습니다.

단계 **7** 업그레이드 중에는 Firepower Chassis Manager를 사용할 수 없습니다. FXOS CLI를 사용하여 업그레이드 프로세스를 모니터링할 수 있습니다.

a) **scope system**을 입력합니다.
b) **show firmware monitor**를 입력합니다.
c) 모든 구성 요소(FPRM, Fabric Interconnect 및 섀시)가 `Upgrade-Status: Ready(업그레이드 상태: 준비)`로 표시될 때까지 기다립니다.

참고 FPRM 구성 요소가 업그레이드되고 나면 시스템이 리부팅된 후 다른 구성 요소 업그레이드가 계속됩니다.

d) **top**을 입력합니다.
e) **scope ssa**를 입력합니다.
f) **show slot**을 입력합니다.

g) Firepower 4100 Series 어플라이언스의 보안 엔진 또는 Firepower 9300 Appliance에 설치된 모든 보안 모듈의 Admin State(관리 상태)가 `Ok`(정상)이고 Oper State(작동 상태)가 `Online`(온라인) 인지 확인합니다.

h) **show app-instance**를 입력합니다.

i) 섀시에 설치된 모든 논리적 디바이스의 Oper State(작동 상태)가 `Online`(온라인)이고 Cluster State(클러스터 상태)가 `In Cluster`(클러스터 내)이며 Cluster Role(클러스터 역할)이 `Slave`(슬레이브) 인지 확인합니다.

예제:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
FP9300-A /ssa #

FP9300-A /ssa # show app-instance
App Name   Slot ID    Admin State Oper State      Running Version Startup Version Profile Name Cluster
 State   Cluster Role
---------- ---------- ----------- ---------------- --------------- --------------- ------------
--------------- ------------
ftd        1          Enabled     Online           6.2.2.81        6.2.2.81                    In
Cluster      Slave
ftd        2          Enabled     Online           6.2.2.81        6.2.2.81                    In
Cluster      Slave
ftd        3          Disabled    Not Available                    6.2.2.81                    Not
Applicable  None
FP9300-A /ssa #
```

단계 **8** 섀시 #2의 보안 모듈 중 하나를 기본 모듈로 설정합니다.

섀시 #2의 보안 모듈 중 하나를 기본 모듈로 설정하면 섀시 #1은 더 이상 기본 유닛을 포함하지 않으므로 업그레이드할 수 있습니다.

단계 **9** 클러스터의 다른 모든 섀시에 대해 1~7단계를 반복합니다.

단계 **10** 기본 역할을 섀시 #1로 돌려놓으려면 섀시 #1의 보안 모듈 중 하나를 기본 모듈로 설정합니다.

FXOS CLI를 사용하여 Firepower Threat Defense 섀시 간 클러스터에서 FXOS 업그레이드

Firepower Threat Defense 논리적 디바이스가 섀시 간 클러스터로 구성된 Firepower 9300 또는 Firepower 4100 Series 보안 어플라이언스가 있는 경우 다음 절차에 따라 Firepower 9300 또는 Firepower 4100 Series 보안 어플라이언스에서 FXOS 플랫폼 번들을 업데이트하십시오.

시작하기 전에

업그레이드를 시작하기 전에 다음 작업을 이미 완료했는지 확인하십시오.

- 업그레이드 대상 FXOS 플랫폼 번들 소프트웨어 패키지를 다운로드합니다. Firepower 4100/9300 섀시용 FXOS 다운로드, 16 페이지를 참조하십시오.
- FXOS 및 Firepower Threat Defense 컨피그레이션을 백업합니다.
- Firepower 4100/9300 섀시에 소프트웨어 이미지를 다운로드하는 데 필요한 다음 정보를 수집합니다.
  - 이미지를 복사하고 있는 원본 서버의 IP 주소 및 인증 크리덴셜.
  - 이미지 파일의 정규화된 이름.

참고 업그레이드 프로세스에는 일반적으로 섀시당 20~30분이 소요됩니다.

단계 **1** 섀시 #2(기본 유닛이 없는 섀시)의 FXOS CLI에 연결합니다.

단계 **2** 다음 명령을 입력하여 보안 모듈/보안 엔진과 설치된 애플리케이션의 상태를 확인합니다.

a) **top**을 입력합니다.
b) **scope ssa**를 입력합니다.
c) **show slot**을 입력합니다.
d) Firepower 4100 Series 어플라이언스의 보안 엔진 또는 Firepower 9300 Appliance에 설치된 모든 보안 모듈의 Admin State(관리 상태)가 `Ok`(정상)이고 Oper State(작동 상태)가 `Online`(온라인)인지 확인합니다.
e) **show app-instance**를 입력합니다.
f) 섀시에 설치된 모든 논리적 디바이스의 Oper State(작동 상태)가 `Online`(온라인)이고 Cluster State(클러스터 상태)가 `In Cluster`(클러스터 내)인지 확인합니다. 그리고 정확한 Firepower Threat Defense 소프트웨어 버전이 Running Version(실행 중인 버전)으로 표시되는지 확인합니다.

   참고 기본 유닛이 이 섀시에 없음을 확인합니다. Cluster Role(클러스터 역할)이 `Master`(마스터)로 설정된 Firepower Threat Defense 인스턴스가 없어야 합니다.

g) 다음 명령을 사용하여 Firepower 9300 Appliance에 설치된 모든 보안 모듈 또는 Firepower 4100 Series 어플라이언스의 보안 엔진에 대해 FXOS 버전이 정확한지 확인합니다.

scope server 1/*slot_id*. 여기서 *slot_id*는 Firepower 4100 Series 보안 엔진의 경우 1입니다.

show version.

단계 **3** 새 플랫폼 번들 이미지를 Firepower 4100/9300 섀시에 다운로드합니다.

a) **top**을 입력합니다.

b) 펌웨어 모드를 입력합니다.

Firepower-chassis-a # **scope firmware**

c) FXOS 플랫폼 번들 소프트웨어 이미지를 다운로드합니다.

Firepower-chassis-a /firmware # **download image** *URL*

다음 구문 중 하나를 사용하여 가져올 파일의 URL을 지정합니다.

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

d) 다음 명령을 사용하여 다운로드 프로세스를 모니터링합니다.

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

예제**:**

다음 예에서는 SCP 프로토콜을 사용하여 이미지를 복사합니다.

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

단계 **4** 필요한 경우 펌웨어 모드를 다시 설정합니다.

Firepower-chassis-a /firmware/download-task # **up**

단계 **5** 자동 설치 모드를 입력합니다.

Firepower-chassis /firmware # **scope auto-install**

단계 **6** FXOS 플랫폼 번들을 설치합니다.

Firepower-chassis /firmware/auto-install # **install platform platform-vers** *version_number*

*version_number*는 설치 중인 FXOS 플랫폼 번들의 버전 번호입니다(예: 2.3(1.58)).

단계 **7** 시스템은 설치할 소프트웨어 패키지를 먼저 확인합니다. 시스템은 현재 설치된 애플리케이션과 지정된 FXOS 플랫폼 소프트웨어 패키지 간에 비호환성이 있는지 알려줍니다. 또한 기존 세션이 종료되고 시스템이 업그레이드의 일부로 재부팅되어야 한다고 경고합니다.

yes를 입력하여 검증을 계속할 것인지 확인합니다.

단계 **8** **yes**를 입력하여 설치를 계속할 것인지 확인하거나 **no**를 입력하여 설치를 취소합니다.

Firepower eXtensible 운영 체제에서는 번들의 압축을 풀고 구성 요소를 업그레이드하거나 다시 로드합니다.

단계 **9** 업그레이드 프로세스를 모니터링하려면 다음과 같이 합니다.

a) **scope system**을 입력합니다.
b) **show firmware monitor**를 입력합니다.
c) 모든 구성 요소(FPRM, Fabric Interconnect 및 섀시)가 `Upgrade-Status: Ready`(업그레이드 상태: 준비)로 표시될 때까지 기다립니다.

참고 FPRM 구성 요소가 업그레이드되고 나면 시스템이 리부팅된 후 다른 구성 요소 업그레이드가 계속됩니다.

d) **top**을 입력합니다.
e) **scope ssa**를 입력합니다.
f) **show slot**을 입력합니다.
g) Firepower 4100 Series 어플라이언스의 보안 엔진 또는 Firepower 9300 Appliance에 설치된 모든 보안 모듈의 Admin State(관리 상태)가 `Ok`(정상)이고 Oper State(작동 상태)가 `Online`(온라인)인지 확인합니다.
h) **show app-instance**를 입력합니다.
i) 섀시에 설치된 모든 논리적 디바이스의 Oper State(작동 상태)가 `Online`(온라인)이고 Cluster State(클러스터 상태)가 `In Cluster`(클러스터 내)이며 Cluster Role(클러스터 역할)이 `Slave`(슬레이브)인지 확인합니다.

예제:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
```

```
FP9300-A /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
FP9300-A /ssa #

FP9300-A /ssa # show app-instance
App Name   Slot ID    Admin State Oper State      Running Version Startup Version Profile Name Cluster
 State   Cluster Role
---------- ---------- ----------- ---------------- --------------- --------------- ------------
--------------- ------------
ftd        1          Enabled     Online           6.2.2.81        6.2.2.81                     In
Cluster      Slave
ftd        2          Enabled     Online           6.2.2.81        6.2.2.81                     In
Cluster      Slave
ftd        3          Disabled    Not Available                    6.2.2.81                     Not
Applicable  None
FP9300-A /ssa #
```

단계 **10** 섀시 #2의 보안 모듈 중 하나를 기본 모듈로 설정합니다.

섀시 #2의 보안 모듈 중 하나를 기본 모듈로 설정하면 섀시 #1은 더 이상 기본 유닛을 포함하지 않으므로 업그레이드할 수 있습니다.

단계 **11** 클러스터의 다른 모든 섀시에 대해 1~9단계를 반복합니다.

단계 **12** 기본 역할을 섀시 #1로 돌려놓으려면 섀시 #1의 보안 모듈 중 하나를 기본 모듈로 설정합니다.

Firepower Threat Defense 소프트웨어 업그레이드 - Firepower 4100/9300 섀시

Firepower 4100/9300 섀시의 Firepower Threat Defense 소프트웨어를 업그레이드하려면 이 절차를 사용합니다. 여러 디바이스를 한 번에 업그레이드할 수 있습니다. 디바이스 클러스터 및 고가용성(HA) 쌍의 멤버는 동시에 업그레이드해야 합니다.

⚠

주의 업그레이드 중인 어플라이언스를 종료하거나, 수동으로 리부팅하거나, 해당 어플라이언스로/어플라이언스에서 변경 사항을 구축하지 마십시오. 진행 중인 업그레이드를 재시작하지 마십시오. 사전 확인 중에는 업그레이드 프로세스가 비활성 상태로 표시될 수 있으며 이는 정상적인 현상입니다. 업그레이드에 문제(업그레이드 실패 또는 응답하지 않는 어플라이언스 포함)가 있을 경우 Cisco TAC에 문의하십시오.

시작하기 전에

업그레이드 경로(FXOS 및 Firepower Management Center 업그레이드 포함)에서 현재 위치를 확인합니다. 이 단계를 완벽하게 계획하고 준비했는지 확인합니다.

단계 **1** 업그레이드하려는 디바이스에 컨피그레이션을 구축합니다.

Firepower Management Center 메뉴 바에서 **Deploy(**구축**)**를 클릭합니다. 디바이스를 선택하고 **Deploy(**구축**)**를 다시 클릭합니다. 지금 오래된 디바이스에 구축하지 않으면 최종 업그레이드에 실패할 수 있으며, 그러면 해당 디바이스에 이미지를 재설치해야 할 수 있습니다.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하면 Snort 프로세스가 재시작되어 트래픽 검사가 중단되며 디바이스가 트래픽을 처리하는 방법에 따라서 재시작이 완료될 때까지 트래픽도 중단될 수 있습니다. 자세한 내용은 Firepower Threat Defense 업그레이드 동작 — Firepower 4100/9300 섀시, 125 페이지를 참조하십시오.

단계 **2** 업그레이드 전 최종 확인을 수행합니다.

- 상태 확인 - Message Center를 사용합니다(메뉴 바에서 System Status(시스템 상태) 아이콘 클릭). 구축의 어플라이언스가 성공적으로 통신하는지, 상태 모니터에서 보고하는 문제가 없는지 확인합니다.
- 작업 실행 - 역시 Message Center에서 필수 작업이 완료되었는지 확인합니다. 업그레이드를 시작할 때 실행 중인 작업은 중지되어 실패한 작업이 되며 다시 시작할 수 없습니다. 장애 발생 상태 메시지는 나중에 수동으로 삭제할 수 있습니다.
- 디스크 공간 확인 - 최종 디스크 공간 확인을 수행합니다. 사용 가능한 디스크 공간이 부족하면 업그레이드에 실패합니다.

단계 **3** (선택 사항, 고가용성에만 해당) 고가용성 디바이스 쌍의 활성/스탠바이 역할을 전환합니다.

고가용성 쌍의 스탠바이 디바이스가 먼저 업그레이드됩니다. 디바이스에서 역할을 전환한 후 새 스탠바이 피어가 업그레이드됩니다. 업그레이드가 완료되어도 디바이스 역할은 전환된 상태로 유지됩니다. 액티브/스탠바이 역할을 유지하려면 업그레이드 전에 역할을 수동으로 전환하십시오. 이렇게 하면 업그레이드 프로세스에서 역할을 다시 전환합니다.

Devices(디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 쌍 옆의 **Switch Active Peer(**액티브 피어 전환**)** 아이콘을 클릭한 다음 선택을 확인합니다.

단계 **4** **System(**시스템**)** > **Updates(**업데이트**)**를 선택합니다.

단계 **5** 사용하려는 업그레이드 패키지 옆의 설치 아이콘을 클릭하고 업그레이드할 디바이스를 선택합니다.

업그레이드하려는 디바이스가 나열되어 있지 않은 경우 업그레이드 패키지를 잘못 선택한 것입니다.

참고 6개 이상의 디바이스를 동시에 업그레이드하지 않는 것이 좋습니다. 선택한 모든 디바이스에서 프로세스를 완료할 때까지 Firepower Management Center에서는 디바이스 업그레이드 중지를 허용하지 않습니다. 디바이스 하나의 업그레이드에서 문제가 발생하는 경우 모든 디바이스가 업그레이드를 완료해야 문제를 해결할 수 있습니다.

단계 **6** **Install(**설치**)**을 클릭하고 디바이스를 업그레이드 및 리부팅할 것임을 확인합니다.

일부 디바이스는 업데이트 중 두 번 리부팅될 수 있습니다. 이는 정상 동작입니다.

디바이스가 구성 및 구축된 방식에 따라 트래픽은 업그레이드 전 과정에서 삭제되거나 검사 없이 네트워크를 통과합니다. 자세한 내용은 Firepower Threat Defense 업그레이드 동작 — Firepower 4100/9300 섀시, 125 페이지를 참조하십시오.

단계 **7** Message Center에서 업그레이드 진행 상황을 모니터링합니다.

업그레이드되고 있는 디바이스에는 컨피그레이션을 구축하지 마십시오. Message Center에서 몇 분간 진행 상황이 표시되지 않거나 업그레이드에서 장애가 발생했다고 나타나더라도 업그레이드를 재시작하거나 디바이스를 리부팅하지 마십시오. 그 대신 Cisco TAC에 문의하십시오.

단계 **8** 업데이트 성공을 확인합니다.

업그레이드가 완료되면 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 업그레이드된 디바이스의 소프트웨어 버전이 정확한지 확인합니다.

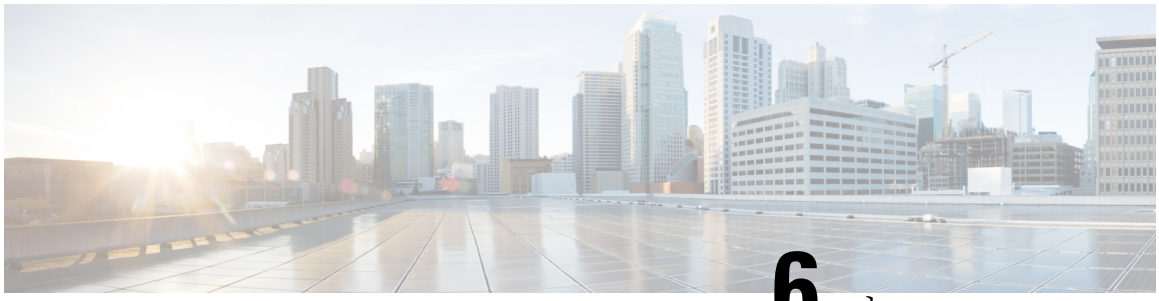
단계 **9** Message Center를 사용하여 구축 상태를 다시 확인합니다.

단계 **10** 침입 규칙 및 취약점 데이터베이스(VDB)를 업데이트합니다.

지원 사이트에서 제공되는 침입 규칙 업데이트 또는 VDB가 현재 실행 중인 버전보다 최신 상태이면 최신 버전을 설치합니다. 자세한 내용은 Firepower Management Center 컨피그레이션 가이드을 참조하십시오. 침입 규칙을 업데이트할 때는 정책을 자동으로 다시 적용할 필요가 없습니다. 정책은 나중에 다시 적용합니다.

단계 **11** 릴리스 노트에 설명되어 있는 업그레이드 후 컨피그레이션 변경을 완료합니다.

단계 **12** 방금 업그레이드한 디바이스에 컨피그레이션을 재구축합니다.



6 장

Firepower 7000/8000 Series 및 NGIPSv 디바이스 업그레이드

Firepower 7000/8000 Series 및 NGIPSv 업그레이드 체크리스트

이 체크리스트를 참조하여 Firepower 7000/8000 Series 및 NGIPSv 디바이스를 업그레이드합니다.

업그레이드할 때마다 체크리스트를 작성하십시오. 단계를 건너뛰면 업그레이드에 실패할 수 있습니다.업그레이드 프로세스 중에 항상 구축의 어플라이언스가 성공적으로 통신하는지, 상태 모니터에서 보고하는 문제가 없는지 확인합니다.

업그레이드 계획

업그레이드 경로를 정확하게 계획하고 준수하여 항상 구축 호환성을 유지해야 합니다.

☐	작업/확인	세부 사항
	업그레이드 경로에서 현재 위치를 확인합니다. 방금 수행한 업그레이드와 다음에 수행할 업그레이드를 파악합니다.	업그레이드 경로 계획, 6 페이지 Firepower 7000/8000 Series 및 NGIPSv 업그레이드 경로 - Firepower Management Center 포함, 117 페이지
	디바이스의 현재 버전과 대상 버전을 확인합니다. • Firepower 소프트웨어 • 가상 호스팅 환경(NGIPSv)	7000/8000 Series 및 레거시 디바이스, 107 페이지 NGIPSv(Virtual Managed Devices), 108 페이지

☐	작업/확인	세부 사항
	디바이스를 업그레이드한 후 Firepower Management Center에서 해당 디바이스를 관리할 수 있는지 확인합니다. 디바이스를 관리할 수 없는 경우 Firepower Management Center를 먼저 업그레이드할 수 있도록 업그레이드 경로를 수정합니다.	Firepower Management Center 및 매니지드 디바이스 버전 호환성, 99 페이지
	릴리스 노트에서 다음 업그레이드/업그레이드 집합을 확인하고 릴리스별 지침을 특히 주의하여 확인합니다.	Firepower 릴리스 노트

업그레이드 전 작업 및 확인

유지 보수 기간이 아닐 때 사전 확인을 수행하여 중단을 최소화합니다.

☐	작업/확인	세부 사항
	필요한 업그레이드 전 컨피그레이션을 변경합니다. 필요한 업그레이드 후 컨피그레이션을 변경할 수 있도록 준비합니다.	Firepower 소프트웨어 업그레이드 버전별 지침, 133 페이지 Firepower 릴리스 노트
	Firepower 소프트웨어 업그레이드를 위한 예비 디스크 공간 확인을 실행합니다.	Firepower 소프트웨어 업그레이드 시간 및 디스크 공간, 141 페이지
	올바른 Firepower 소프트웨어 업그레이드 패키지를 다운로드하여 Firepower Management Center에 업로드합니다. 버전 6.2.1 이상의 업그레이드 패키지는 서명이 되어 있으며 이름이 .sh가 아닌 .sh.REL.tar로 끝납니다. 서명된 업그레이드 패키지는 압축을 풀지 마십시오.	업그레이드 패키지 다운로드, 9 페이지
	Firepower Management Center에서 디바이스로의 대량 데이터 전송을 수행할 수 있는 대역폭이 있는지 확인합니다.	Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침(트러블슈팅 TechNote)
	Firepower 소프트웨어 업그레이드 패키지를 디바이스로 푸시합니다. (선택 사항, 6.2.3 이상)	매니지드 디바이스로 업그레이드 패키지 푸시, 18 페이지
	준비 확인을 실행합니다. (선택 사항, 6.1 이상)	준비 확인 실행, 18 페이지
	Firepower Management Center를 사용하여 디바이스의 이벤트 데이터를 백업합니다. 외부 위치에 백업한 후 전송 성공을 확인합니다. Firepower Management Center는 업그레이드 시 로컬에 저장된 백업을 제거합니다.	Firepower Management Center 컨피그레이션 가이드

☐	작업/확인	세부 사항
		업그레이드 전 기타 작업 및 확인, 20 페이지
	다음 사항을 고려하여 업그레이드의 영향이 가장 적은 유지 보수 기간을 예약합니다. • 유지 보수 기간에 수행해야 하는 작업. • 업그레이드가 트래픽 흐름 및 검사에 미치는 영향. • 업그레이드에 걸릴 것으로 예상되는 최소 시간.	업그레이드 중의 트래픽 흐름, 검사 및 디바이스 동작, 125 페이지 Firepower 소프트웨어 업그레이드 시간 및 디스크 공간, 141 페이지

디바이스 업그레이드

업그레이드로 인해 트래픽 흐름이나 검사가 중단될 수 있으므로 유지 보수 기간에 업그레이드를 수행하십시오.

☐	작업/확인	세부 사항
	필요한 경우 호스팅 환경을 업그레이드합니다(NGIPSv에만 해당).	호스팅 환경 설명서를 참조하십시오.
	Firepower 소프트웨어를 업그레이드합니다.	Firepower 7000/8000 Series 및 NGIPSv 업그레이드, 65 페이지

Firepower 7000/8000 Series 및 NGIPSv 업그레이드

Firepower 7000/8000 Series 및 NGIPSv 디바이스를 업그레이드하려면 이 절차를 사용합니다. 여러 디바이스가 동일한 업그레이드 패키지를 사용하는 경우 해당 디바이스를 한 번에 업데이트할 수 있습니다. 디바이스 스택 및 고가용성 쌍의 멤버는 동시에 업그레이드해야 합니다.

⚠

주의 업그레이드 중인 어플라이언스를 종료하거나, 수동으로 리부팅하거나, 해당 어플라이언스로/어플라이언스에서 변경 사항을 구축하지 마십시오. 진행 중인 업그레이드를 재시작하지 마십시오. 사전 확인 중에는 업그레이드 프로세스가 비활성 상태로 표시될 수 있으며 이는 정상적인 현상입니다. 업그레이드에 문제(업그레이드 실패 또는 응답하지 않는 어플라이언스 포함)가 있을 경우 Cisco TAC에 문의하십시오.

시작하기 전에

업그레이드 경로(가상 호스팅 환경 및 Firepower Management Center 업그레이드 포함)에서 현재 위치를 확인합니다. 이 단계를 완벽하게 계획하고 준비했는지 확인합니다.

단계 **1** 업그레이드하려는 디바이스에 컨피그레이션을 구축합니다.

Firepower Management Center 메뉴 바에서 **Deploy(**구축**)**를 클릭합니다. 디바이스를 선택하고 **Deploy(**구축**)**를 다시 클릭합니다. 지금 오래된 디바이스에 구축하지 않으면 최종 업그레이드에 실패할 수 있으며, 그러면 해당 디바이스에 이미지를 재설치해야 할 수 있습니다.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하면 Snort 프로세스가 재시작되어 트래픽 검사가 중단되며 디바이스가 트래픽을 처리하는 방법에 따라서 재시작이 완료될 때까지 트래픽도 중단될 수 있습니다. 자세한 내용은 Firepower 7000/8000 Series 업그레이드 동작, 130 페이지 또는 NGIPSv 업그레이드 동작, 132 페이지를 참조하십시오.

단계 **2** 업그레이드하려는 디바이스에 컨피그레이션을 구축합니다.

Firepower Management Center 메뉴 바에서 **Deploy(**구축**)**를 클릭합니다. 디바이스를 선택하고 **Deploy(**구축**)**를 다시 클릭합니다. 지금 오래된 디바이스에 구축하지 않으면 최종 업그레이드에 실패할 수 있으며, 그러면 해당 디바이스에 이미지를 재설치해야 할 수 있습니다.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하면 Snort 프로세스가 재시작되어 트래픽 검사가 중단되며 디바이스가 트래픽을 처리하는 방법에 따라서 재시작이 완료될 때까지 트래픽도 중단될 수 있습니다.

단계 **3** 업그레이드 전 최종 확인을 수행합니다.

- 상태 확인 - Message Center를 사용합니다(메뉴 바에서 System Status(시스템 상태) 아이콘 클릭). 구축의 어플라이언스가 성공적으로 통신하는지, 상태 모니터에서 보고하는 문제가 없는지 확인합니다.
- 작업 실행 - 역시 Message Center에서 필수 작업이 완료되었는지 확인합니다. 업그레이드를 시작할 때 실행 중인 작업은 중지되어 실패한 작업이 되며 다시 시작할 수 없습니다. 장애 발생 상태 메시지는 나중에 수동으로 삭제할 수 있습니다.
- 디스크 공간 확인 - 최종 디스크 공간 확인을 수행합니다. 사용 가능한 디스크 공간이 부족하면 업그레이드에 실패합니다.

단계 **4** (선택 사항, 고가용성에만 해당) 스위칭/라우팅을 수행하는 고가용성 디바이스 쌍의 활성/스탠바이 역할을 전환합니다.

고가용성 쌍이 액세스 컨트롤만 수행하도록 구축된 경우에는 액티브 피어가 먼저 업그레이드됩니다. 업그레이드가 완료되면 액티브 및 스탠바이 피어의 이전 역할이 유지됩니다.

그러나 라우팅 또는 스위칭 구축에서는 스탠바이 피어가 먼저 업그레이드됩니다. 디바이스에서 역할을 전환한 후 새 스탠바이 피어가 업그레이드됩니다. 업그레이드가 완료되어도 디바이스 역할은 전환된 상태로 유지됩니다. 액티브/스탠바이 역할을 유지하려면 업그레이드 전에 역할을 수동으로 전환하십시오. 이렇게 하면 업그레이드 프로세스에서 역할을 다시 전환합니다.

Devices(디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 쌍 옆의 **Switch Active Peer(**액티브 피어 전환**)** 아이콘을 클릭한 다음 선택을 확인합니다.

단계 **5** **System(**시스템**)** > **Updates(**업데이트**)**를 선택합니다.

단계 **6** 사용하려는 업그레이드 패키지 옆의 설치 아이콘을 클릭하고 업그레이드할 디바이스를 선택합니다.

업그레이드하려는 디바이스가 나열되어 있지 않은 경우 업그레이드 패키지를 잘못 선택한 것입니다.

참고 6개 이상의 디바이스를 동시에 업그레이드하지 않는 것이 좋습니다. 선택한 모든 디바이스에서 프로세스를 완료할 때까지 Firepower Management Center에서는 디바이스 업그레이드 중지를 허용하지 않습니다. 디바이스 하나의 업그레이드에서 문제가 발생하는 경우 모든 디바이스가 업그레이드를 완료해야 문제를 해결할 수 있습니다.

단계 **7** **Install**(설치)을 클릭하고 디바이스를 업그레이드 및 리부팅할 것임을 확인합니다.

디바이스가 구성 및 구축된 방식에 따라 트래픽은 업그레이드 전 과정에서 삭제되거나 검사 없이 네트워크를 통과합니다. 자세한 내용은 Firepower 7000/8000 Series 업그레이드 동작, 130 페이지 또는 NGIPSv 업그레이드 동작, 132 페이지를 참조하십시오.

단계 **8** Message Center에서 업그레이드 진행 상황을 모니터링합니다.

업그레이드되고 있는 디바이스에는 컨피그레이션을 구축하지 마십시오. Message Center에서 몇 분간 진행 상황이 표시되지 않거나 업그레이드에서 장애가 발생했다고 나타나더라도 업그레이드를 재시작하거나 디바이스를 리부팅하지 마십시오. 그 대신 Cisco TAC에 문의하십시오.

단계 **9** 업데이트 성공을 확인합니다.

업그레이드가 완료되면 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 업그레이드된 디바이스의 소프트웨어 버전이 정확한지 확인합니다.

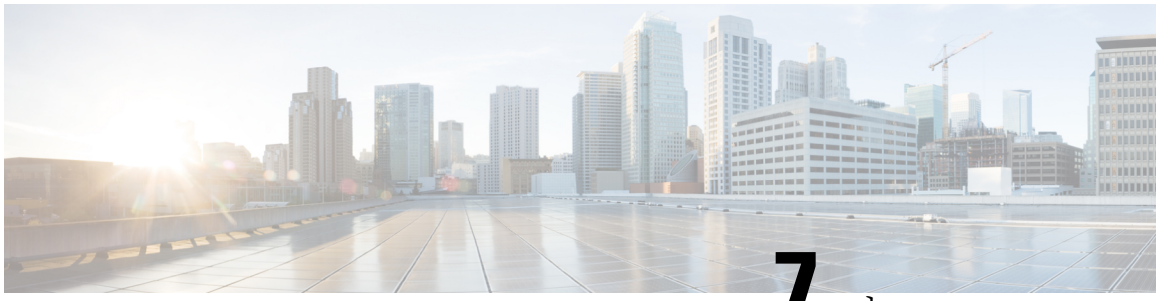
단계 **10** Message Center를 사용하여 구축 상태를 다시 확인합니다.

단계 **11** 침입 규칙 및 취약점 데이터베이스(VDB)를 업데이트합니다.

지원 사이트에서 제공되는 침입 규칙 업데이트 또는 VDB가 현재 실행 중인 버전보다 최신 상태이면 최신 버전을 설치합니다. 자세한 내용은 Firepower Management Center 컨피그레이션 가이드을 참조하십시오. 침입 규칙을 업데이트할 때는 정책을 자동으로 다시 적용할 필요가 없습니다. 정책은 나중에 다시 적용합니다.

단계 **12** 릴리스 노트에 설명되어 있는 업그레이드 후 컨피그레이션 변경을 완료합니다.

단계 **13** 방금 업그레이드한 디바이스에 컨피그레이션을 재구축합니다.



7 장

ASA with FirePOWER Services 업그레이드

ASA with FirePOWER Services 업그레이드 체크리스트

이 체크리스트를 참조하여 ASA with FirePOWER Services를 업그레이드합니다.

업그레이드할 때마다 체크리스트를 작성하십시오. 단계를 건너뛰면 업그레이드에 실패할 수 있습니다.업그레이드 프로세스 중에 항상 구축의 어플라이언스가 성공적으로 통신하는지, 상태 모니터에서 보고하는 문제가 없는지 확인합니다.

업그레이드 계획

업그레이드 경로를 정확하게 계획하고 준수하여 항상 구축 호환성을 유지해야 합니다.

☐	작업/확인	세부 사항
	업그레이드 경로에서 현재 위치를 확인합니다. 방금 수행한 업그레이드와 다음에 수행할 업그레이드를 파악합니다.	업그레이드 경로 계획, 6 페이지 ASA FirePOWER 모듈 업그레이드 경로 - Firepower Management Center 포함, 118 페이지
	디바이스의 현재 버전과 대상 버전을 확인합니다. • ASA FirePOWER 모듈 • ASA OS	ASA with FirePOWER Services 디바이스, 105 페이지
	디바이스를 업그레이드한 후 Firepower Management Center에서 해당 디바이스를 관리할 수 있는지 확인합니다. 디바이스를 관리할 수 없는 경우 Firepower Management Center를 먼저 업그레이드할 수 있도록 업그레이드 경로를 수정합니다.	Firepower Management Center 및 매니지드 디바이스 버전 호환성, 99 페이지

☐	작업/확인	세부 사항
	릴리스 노트에서 다음 업그레이드/업그레이드 집합을 확인하고 릴리스별 지침을 특히 주의하여 확인합니다.	Firepower 릴리스 노트 ASA 릴리스 노트

업그레이드 전 작업 및 확인

유지 보수 기간이 아닐 때 사전 확인을 수행하여 중단을 최소화합니다.

☐	작업/확인	세부 사항
	필요한 업그레이드 전 컨피그레이션을 변경합니다. 필요한 업그레이드 후 컨피그레이션을 변경할 수 있도록 준비합니다.	Firepower 소프트웨어 업그레이드 버전별 지침, 133 페이지 *Cisco ASA* 업그레이드 가이드의 업그레이드 계획
	Firepower 소프트웨어 업그레이드를 위한 예비 디스크 공간 확인을 실행합니다.	Firepower 소프트웨어 업그레이드 시간 및 디스크 공간, 141 페이지
	올바른 Firepower 소프트웨어 업그레이드 패키지를 다운로드하여 Firepower Management Center에 업로드합니다. 버전 6.2.1 이상의 업그레이드 패키지는 서명이 되어 있으며 이름이 .sh가 아닌 .sh.REL.tar로 끝납니다. 서명된 업그레이드 패키지는 압축을 풀지 마십시오.	업그레이드 패키지 다운로드, 9 페이지
	Firepower Management Center에서 디바이스로의 대량 데이터 전송을 수행할 수 있는 대역폭이 있는지 확인합니다.	Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침(트러블슈팅 TechNote)
	Firepower 소프트웨어 업그레이드 패키지를 디바이스로 푸시합니다. (선택 사항, 6.2.3 이상)	매니지드 디바이스로 업그레이드 패키지 푸시, 18 페이지
	준비 확인을 실행합니다. (선택 사항, 6.1 이상)	준비 확인 실행, 18 페이지
	Firepower Management Center를 사용하여 디바이스의 이벤트 데이터를 백업합니다. 외부 위치에 백업한 후 전송 성공을 확인합니다. Firepower Management Center는 업그레이드 시 로컬에 저장된 백업을 제거합니다.	Firepower Management Center 컨피그레이션 가이드
		업그레이드 전 기타 작업 및 확인, 20 페이지

☐	작업/확인	세부 사항
	다음 사항을 고려하여 업그레이드의 영향이 가장 적은 유지 보수 기간을 예약합니다. • 유지 보수 기간에 수행해야 하는 작업. • 업그레이드가 트래픽 흐름 및 검사에 미치는 영향. • 업그레이드에 걸릴 것으로 예상되는 최소 시간.	ASA FirePOWER 업그레이드 동작, 131 페이지 Firepower 소프트웨어 업그레이드 시간 및 디스크 공간, 141 페이지

ASA with FirePOWER Services 업그레이드

업그레이드로 인해 트래픽 흐름이나 검사가 중단될 수 있으므로 유지 보수 기간에 업그레이드를 수행하십시오.

☐	작업/확인	세부 사항
	ASA 업그레이드가 필요 없는 디바이스에서 ASA FirePOWER 모듈을 업그레이드합니다.	ASA FirePOWER 모듈 업그레이드 - Firepower Management Center 포함, 94 페이지
	독립형 ASA 디바이스에서 ASA 및 ASA FirePOWER 모듈을 업그레이드합니다. ASA를 업그레이드하고 다시 로드한 직후에 Firepower Management Center를 사용하여 ASA FirePOWER 모듈을 업그레이드합니다.	독립형 유닛 업그레이드, 72 페이지 결과 ASA FirePOWER 모듈 업그레이드 - Firepower Management Center 포함, 94 페이지
	클러스터 및 페일오버 쌍의 ASA 디바이스에서 ASA 및 ASA FirePOWER 모듈을 업그레이드합니다. 트래픽 흐름 및 검사 중단을 방지하려면 이러한 디바이스를 한 번에 하나씩 완전히 업그레이드하십시오. 각 유닛을 다시 로드하여 ASA를 업그레이드하기 직전에 Firepower Management Center를 사용하여 ASA FirePOWER 모듈을 업그레이드합니다.	다음 중 하나에 해당합니다. 액티브/스탠바이 페일오버 쌍 업그레이드, 77 페이지 액티브/액티브 페일오버 쌍 업그레이드, 81 페이지 ASA 클러스터 업그레이드, 86 페이지 결과 ASA FirePOWER 모듈 업그레이드 - Firepower Management Center 포함, 94 페이지

ASA 업그레이드

독립형, 페일오버 또는 클러스터링 구축에 대해 ASA 및 ASDM을 업그레이드하려면 이 섹션의 절차를 참조합니다.

독립형 유닛 업그레이드

CLI 또는 ASDM을 사용하여 독립형 유닛을 업그레이드합니다.

CLI를 사용하여 독립형 유닛 업그레이드

이 섹션에서는 ASDM 및 ASA 이미지를 설치하는 방법과 ASA FirePOWER 모듈을 업그레이드하는 시기에 대해 설명합니다.

시작하기 전에

이 절차에서는 FTP를 사용합니다. TFTP, HTTP 또는 기타 서버 유형의 경우 ASA 명령 참조에서 **copy** 명령을 참조하십시오.

단계 **1** 특권 실행 모드에서 ASA 소프트웨어를 플래시 메모리에 복사합니다.

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name***disk***n***:/**[*path/*]*asa_image_name*

예제**:**

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asa991-smp-k8.bin disk0:/asa991-smp-k8.bin
```

단계 **2** ASDM 이미지를 플래시 메모리에 복사합니다.

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name***disk***n***:/**[*path/*]*asdm_image_name*

예제**:**

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-771791.bin disk0:/asdm-771791.bin
```

단계 **3** 전역 컨피그레이션 모드에 액세스합니다.

configure terminal

예제**:**

```
ciscoasa# configure terminal
ciscoasa(config)#
```

단계 **4** 현재 구성된 부트 이미지를 표시합니다(최대 4개).

show running-config boot system

ASA에서는 나열된 순서대로 이미지를 사용합니다. 첫 번째 이미지를 사용할 수 없으면 그 다음 이미지를 사용하는 식입니다. 새 이미지 URL을 목록의 맨 위에 삽입할 수 없습니다. 새 이미지가 맨 앞에 오게 하려면 기존 항목을 모두 삭제한 다음 원하는 순서대로 이미지 URL을 입력해야 합니다(다음 단계 참조).

예제:

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

단계 **5** 새 부트 이미지를 첫 번째 선택 사항으로 입력할 수 있도록 기존 부트 이미지 컨피그레이션을 제거합니다.

no boot system disk*n***:/**[*path*/]*asa_image_name*

예제:

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa931-smp-k8.bin
```

단계 **6** 부팅할 ASA 이미지(방금 업로드한 이미지)를 설정합니다.

boot system disk*n***:/**[*path*/]*asa_image_name*

이 이미지를 사용할 수 없을 경우에 사용하려는 모든 백업 이미지에 대해 이 명령을 반복합니다. 예를 들어 이전에 제거한 이미지를 다시 입력할 수 있습니다.

예제:

```
ciscoasa(config)# boot system disk0:/asa991-smp-k8.bin
```

단계 **7** 사용할 ASDM 이미지(방금 업로드한 이미지)를 설정합니다.

asdm image disk*n***:/**[*path*/]*asdm_image_name*

사용할 ASDM 이미지는 하나만 구성할 수 있습니다. 따라서 먼저 기존 컨피그레이션을 삭제할 필요 없습니다.

예제:

```
ciscoasa(config)# asdm image disk0:/asdm-771791.bin
```

단계 **8** 새 설정을 시작 컨피그레이션에 저장합니다.

write memory

단계 **9** ASA를 다시 로드합니다.

reload

단계 **10** ASA FirePOWER 모듈을 업그레이드하는 경우 ASA REST API를 비활성화합니다. 이렇게 하지 않으면 업그레이드에서 장애가 발생합니다.

no rest-api agent

업그레이드 후에 REST API를 다시 활성화할 수 있습니다.

rest-api agent

참고 FirePOWER 모듈 버전 6.0 이상을 실행 중인 경우 ASA 5506-X Series는 ASA REST API를 지원하지 않습니다.

단계 **11** ASA FirePOWER 모듈을 업그레이드합니다.

ASDM을 사용하여 로컬 컴퓨터에서 독립형 유닛 업그레이드

Upgrade Software from Local Computer(로컬 컴퓨터에서 소프트웨어 업그레이드**)** 툴을 사용하면 컴퓨터의 이미지 파일을 플래시 파일 시스템에 업로드하여 ASA를 업그레이드할 수 있습니다.

단계 **1** 기본 ASDM 애플리케이션 창에서 **Tools(**툴**)** > **Upgrade Software from Local Computer(**로컬 컴퓨터에서 소프트웨어 업그레이드**)**를 선택합니다.

Upgrade Software(소프트웨어 업그레이드**)** 대화 상자가 나타납니다.

단계 **2** **Image to Upload(**업로드할 이미지**)** 드롭다운 목록에서 **ASDM**을 선택합니다.

단계 **3** **Local File Path(**로컬 파일 경로**)** 필드에서 **Browse Local Files(**로컬 파일 찾아보기**)**를 클릭하여 PC의 파일을 찾습니다.

단계 **4** **Flash File System Path(**플래시 파일 시스템 경로**)** 필드에서 **Browse Flash(**플래시 찾아보기**)**를 클릭하여 플래시 파일 시스템의 디렉토리 또는 파일을 찾습니다.

단계 **5** **Upload Image(**이미지 업로드**)**를 클릭합니다.

업로드 프로세스에 몇 분이 걸릴 수 있습니다.

단계 **6** 이 이미지를 ASDM 이미지로 설정할지 묻습니다. **Yes(**예**)**를 클릭합니다.

단계 **7** ASDM을 종료하고 컨피그레이션을 저장하라는 메시지가 다시 표시됩니다. **OK(**확인**)**를 클릭합니다.

Upgrade(업그레이드**)** 툴을 종료합니다. 참고**:** ASA 소프트웨어를 업그레이드한 다음 컨피그레이션을 저장하고 ASDM을 종료한 후 ASDM에 다시 연결합니다.

단계 **8** **Image to Upload(**업로드할 이미지**)** 드롭다운 목록에서 **ASA**를 선택하여 이러한 단계를 반복합니다. 다른 파일 유형을 업로드하는 데에도 이 절차를 사용할 수 있습니다.

단계 **9** **Tools(**툴**)** > **System Reload(**시스템 다시 로드**)**를 선택하여 ASA를 다시 로드합니다.

새 창이 나타나 다시 로드하기 위한 세부 사항을 확인합니다.

a) **Save the running configuration at the time of reload(**다시 로드할 때 실행 중인 컨피그레이션 저장**)** 라디오 버튼(기본값)을 클릭합니다.
b) 다시 로드할 시간(예: 기본값인 **Now(**지금**)**)을 선택합니다.
c) **Schedule Reload(**다시 로드 예약**)**를 클릭합니다.

다시 로드하는 과정이 진행되면 **Reload Status(**다시 로드 상태**)** 창이 나타나 다시 로드하는 작업이 수행되고 있음을 알립니다. ASDM 종료 옵션도 제공됩니다.

단계 **10** ASA가 다시 로드된 다음 ASDM을 재시작합니다.

콘솔 포트에서 다시 로드 상태를 확인하거나 몇 분 동안 기다렸다가 ASDM을 사용하여 성공할 때까지 연결을 시도할 수 있습니다.

단계 **11** ASA FirePOWER 모듈을 업그레이드하는 경우 **Tools(툴)** > **Command Line Interface(CLI(Command Line Interface))**를 선택하고 **no rest-api agent**를 입력하여 ASA REST API를 비활성화합니다.

REST API를 비활성화하지 않으면 ASA FirePOWER 모듈 업그레이드에 실패하게 됩니다. 업그레이드 후에 REST API를 다시 활성화할 수 있습니다.

rest-api agent

참고 FirePOWER 모듈 버전 6.0 이상을 실행 중인 경우 ASA 5506-X Series는 ASA REST API를 지원하지 않습니다.

단계 **12** ASA FirePOWER 모듈을 업그레이드합니다.

ASDM Cisco.com 마법사를 사용하여 독립형 유닛 업그레이드

Upgrade Software from Cisco.com Wizard(Cisco.com에서 소프트웨어 업그레이드 마법사**)**에서는 ASDM과 ASA를 최신 버전으로 자동 업그레이드할 수 있습니다.

이 마법사에서는 다음을 수행할 수 있습니다.

- 업그레이드할 ASA 이미지 파일 및/또는 ASDM 이미지 파일을 선택합니다.

참고 ASDM은 빌드 번호가 포함된 최신 이미지 버전을 다운로드합니다. 예를 들어, 9.4(1)을 다운로드하는 경우 9.4(1.2)가 다운로드될 수 있습니다. 이는 정상적인 동작이므로 예정된 업그레이드를 계속 진행하면 됩니다.

- 선택한 업그레이드 변경 사항을 검토합니다.
- 이미지를 다운로드하고 설치합니다.
- 설치 상황을 검토합니다.
- 설치가 성공적으로 완료되면 ASA를 재시작하여 컨피그레이션을 저장하고 업그레이드를 완료합니다.

단계 **1** **Tools(툴)** > **Check for ASA/ASDM Updates(ASA/ASDM** 업데이트 확인**)**를 선택합니다.

다중 컨텍스트 모드에서는 System(시스템)에서 이 메뉴에 액세스합니다.

Cisco.com Authentication(Cisco.com 인증**)** 대화 상자가 나타납니다.

단계 **2** Cisco.com 사용자 이름과 비밀번호를 입력하고 **Login(**로그인**)**을 클릭합니다.

isco.com Upgrade Wizard(Cisco.com 업그레이드 마법사**)**가 나타납니다.

참고 사용 가능한 업그레이드가 없으면 대화 상자가 나타납니다. **OK(**확인**)**를 클릭하면 마법사를 종료합니다.

단계 **3** **Next(**다음**)**를 클릭하면 **Select Software(**소프트웨어 선택**)** 화면이 표시됩니다.

현재 ASA 버전 및 ASDM 버전이 나타납니다.

단계 **4** ASA 버전과 ASDM 버전을 업그레이드하려면 다음 단계를 수행합니다.

a) **ASA** 영역에서 **Upgrade to(**업그레이드할 버전**)** 확인란을 선택한 다음 드롭다운 목록에서 어떤 ASA 버전으로 업그레이드할지 선택합니다.

b) **ASDM** 영역에서 **Upgrade to(**업그레이드할 버전**)** 확인란을 선택한 다음 드롭다운 목록에서 어떤 ASDM 버전으로 업그레이드할지 선택합니다.

단계 **5** **Next(**다음**)**를 클릭하면 **Review Changes(**변경 사항 검토**)** 화면이 표시됩니다.

단계 **6** 다음 항목을 확인합니다.

- 다운로드한 ASA 이미지 파일 및/또는 ASDM 이미지 파일이 정확합니다.
- 업로드하려는 ASA 이미지 파일 및/또는 ASDM 이미지 파일이 정확합니다.
- 정확한 ASA 부트 이미지가 선택되었습니다.

단계 **7** **Next(**다음**)**를 클릭하여 업그레이드 설치를 시작합니다.

그런 다음 업그레이드 설치의 진행 상황을 확인합니다.

Results(결과**)** 화면이 나타납니다. 여기서는 업그레이드 설치 상태(성공 또는 실패)와 같은 추가 세부 사항을 제공합니다.

단계 **8** 업그레이드 설치가 성공한 경우 업그레이드 버전을 적용하려면 **Save configuration and reload device now(**구성 저장 및 지금 디바이스 다시 로드**)** 확인란을 선택하여 ASA를 재시작하고 ASDM도 재시작합니다.

단계 **9** 마법사를 종료하고 컨피그레이션 변경 사항을 저장하려면 **Finish(**마침**)**를 클릭합니다.

참고 그 다음으로 높은 버전이 있어 그 버전으로 업그레이드하려면 마법사를 재시작해야 합니다.

단계 **10** ASA가 다시 로드된 다음 ASDM을 재시작합니다.

콘솔 포트에서 다시 로드 상태를 확인하거나 몇 분 동안 기다렸다가 ASDM을 사용하여 성공할 때까지 연결을 시도할 수 있습니다.

단계 **11** ASA FirePOWER 모듈을 업그레이드하는 경우 **Tools(**툴**)** > **Command Line Interface(CLI(Command Line Interface))**를 선택하고 **no rest-api agent**를 입력하여 ASA REST API를 비활성화합니다.

REST API를 비활성화하지 않으면 ASA FirePOWER 모듈 업그레이드에 실패하게 됩니다. 업그레이드 후에 REST API를 다시 활성화할 수 있습니다.

rest-api agent

참고 FirePOWER 모듈 버전 6.0 이상을 실행 중인 경우 ASA 5506-X Series는 ASA REST API를 지원하지 않습니다.

단계 **12** ASA FirePOWER 모듈을 업그레이드합니다.

액티브/스탠바이 페일오버 쌍 업그레이드

제로 다운타임 업그레이드를 수행하려면 CLI 또는 ASDM을 사용하여 액티브/스탠바이 페일오버 쌍을 업그레이드합니다.

CLI를 사용하여 액티브/스탠바이 페일오버 쌍 업그레이드

액티브/스탠바이 페일오버 쌍을 업그레이드하려면 다음 단계를 수행합니다.

시작하기 전에

- 액티브 유닛에서 다음 단계를 수행합니다. SSH 액세스의 경우 활성 IP 주소에 연결합니다. 액티브 유닛은 항상 이 IP 주소를 소유합니다. CLI에 연결할 때는 ASA 프롬프트를 통해 페일오버 상태를 확인합니다. 페일오버 상태와 우선 순위(기본 또는 보조)를 표시하도록 ASA 프롬프트를 구성할 수 있습니다. 이렇게 하면 연결된 유닛을 확인하는 데 유용합니다. prompt 명령을 참조하십시오. 또는 **show failover** 명령을 입력하여 이 유닛의 상태와 우선 순위(기본 또는 보조)를 확인합니다.
- 이 절차에서는 FTP를 사용합니다. TFTP, HTTP 또는 기타 서버 유형의 경우 ASA 명령 참조에서 **copy** 명령을 참조하십시오.

단계 **1** 특권 실행 모드의 액티브 유닛에서 ASA 소프트웨어를 액티브 유닛 플래시 메모리에 복사합니다.

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name***disk***n***:/**[*path/*]*asa_image_name*

예제**:**

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asa991-smp-k8.bin disk0:/asa991-smp-k8.bin
```

단계 **2** 소프트웨어를 스탠바이 유닛에 복사합니다. 액티브 유닛과 동일한 경로를 지정해야 합니다.

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name***disk***n***:/**[*path/*]*asa_image_name*

예제**:**

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asa991-smp-k8.bin
disk0:/asa991-smp-k8.bin
```

단계 **3** 액티브 유닛 플래시 메모리에 ASDM 이미지를 복사합니다.

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name***disk***n***:/**[*path/*]*asdm_image_name*

예제**:**

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-771791.bin disk0:/asdm-771791.bin
```

단계 **4** ASDM 이미지를 스탠바이 유닛에 복사합니다. 액티브 유닛과 동일한 경로를 지정해야 합니다.

failover exec mate copy /noconfirm
ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name***disk***n***:/**[*path*/]*asdm_image_name*

예제**:**

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-771791.bin
disk0:/asdm-771791.bin
```

단계 **5** 아직 전역 컨피그레이션 모드가 아닐 경우 전역 컨피그레이션 모드에 액세스합니다.

configure terminal

단계 **6** 현재 구성된 부트 이미지를 표시합니다(최대 4개).

show running-config boot system

예제**:**

```
asa/act(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ASA에서는 나열된 순서대로 이미지를 사용합니다. 첫 번째 이미지를 사용할 수 없으면 그 다음 이미지를 사용하는 식입니다. 새 이미지 URL을 목록의 맨 위에 삽입할 수 없습니다. 새 이미지가 맨 앞에 오게 하려면 기존 항목을 모두 삭제한 다음 원하는 순서대로 이미지 URL을 입력해야 합니다(다음 단계 참조).

단계 **7** 새 부트 이미지를 첫 번째 선택 사항으로 입력할 수 있도록 기존 부트 이미지 컨피그레이션을 제거합니다.

no boot system disk*n***:/**[*path*/]*asa_image_name*

예제**:**

```
asa/act(config)# no boot system disk0:/cdisk.bin
asa/act(config)# no boot system disk0:/asa931-smp-k8.bin
```

단계 **8** 부팅할 ASA 이미지(방금 업로드한 이미지)를 설정합니다.

boot system disk*n***:/**[*path*/]*asa_image_name*

예제**:**

```
asa/act(config)# boot system disk0://asa991-smp-k8.bin
```

이 이미지를 사용할 수 없을 경우에 사용하려는 모든 백업 이미지에 대해 이 명령을 반복합니다. 예를 들어 이전에 제거한 이미지를 다시 입력할 수 있습니다.

단계 **9** 사용할 ASDM 이미지(방금 업로드한 이미지)를 설정합니다.

asdm image disk*n***:/**[*path*/]*asdm_image_name*

예제**:**

```
asa/act(config)# asdm image disk0:/asdm-771791.bin
```

사용할 ASDM 이미지는 하나만 구성할 수 있습니다. 따라서 먼저 기존 컨피그레이션을 삭제할 필요 없습니다.

단계 **10** 새 설정을 시작 컨피그레이션에 저장합니다.

write memory

이러한 컨피그레이션 변경 사항은 스탠바이 유닛에 자동으로 저장됩니다.

단계 **11** ASA FirePOWER 모듈을 업그레이드하는 경우 ASA REST API를 비활성화합니다. 이렇게 하지 않으면 업그레이드에 실패합니다.

no rest-api agent

단계 **12** 스탠바이 유닛에서 ASA FirePOWER 모듈을 업그레이드합니다.

ASDM으로 관리되는 ASA FirePOWER 모듈의 경우에는 스탠바이 관리 IP 주소에 ASDM을 연결합니다. 업그레이드가 완료될 때까지 기다립니다.

단계 **13** 새 이미지를 부팅하기 위해 스탠바이 유닛을 다시 로드합니다.

failover reload-standby

스탠바이 유닛에서 로딩을 마칠 때까지 기다립니다. **show failover** 명령을 사용하여 스탠바이 유닛이 Standby Ready 상태임을 확인합니다.

단계 **14** 액티브 유닛을 스탠바이 유닛으로 강제 페일오버합니다.

no failover active

SSH 세션에서 연결이 끊긴 경우 이제 새 활성/이전 스탠바이 유닛에서 주 IP 주소에 다시 연결합니다.

단계 **15** 이전 액티브 유닛에서 ASA FirePOWER 모듈을 업그레이드합니다.

ASDM으로 관리되는 ASA FirePOWER 모듈의 경우에는 스탠바이 관리 IP 주소에 ASDM을 연결합니다. 업그레이드가 완료될 때까지 기다립니다.

단계 **16** 새 액티브 유닛에서 이전 액티브 유닛(현재는 새 스탠바이 유닛)을 다시 로드합니다.

failover reload-standby

예제**:**

```
asa/act# failover reload-standby
```

참고 이전 액티브 유닛 콘솔 포트에 연결되어 있는 경우에는 대신 **reload** 명령을 입력하여 이전 액티브 유닛을 다시 로드해야 합니다.

ASDM을 사용하여 액티브/스탠바이 페일오버 쌍 업그레이드

액티브/스탠바이 페일오버 쌍을 업그레이드하려면 다음 단계를 수행합니다.

시작하기 전에

로컬 관리 컴퓨터에 ASA 및 ASDM 이미지를 저장합니다.

단계 **1** 스탠바이 IP 주소에 연결하여 스탠바이 유닛에서 ASDM을 실행합니다.

단계 **2** 기본 ASDM 애플리케이션 창에서 **Tools(**툴**)** > **Upgrade Software from Local Computer(**로컬 컴퓨터에서 소프트웨어 업그레이드**)**를 선택합니다.

Upgrade Software(소프트웨어 업그레이드**)** 대화 상자가 나타납니다.

단계 **3** **Image to Upload(**업로드할 이미지**)** 드롭다운 목록에서 **ASDM**을 선택합니다.

단계 **4** **Local File Path(**로컬 파일 경로**)** 필드에 컴퓨터에 있는 파일의 로컬 경로를 입력하거나 **Browse Local Files(**로컬 파일 찾아보기**)**를 클릭하여 PC의 파일을 찾습니다.

단계 **5** **Flash File System Path(**플래시 파일 시스템 경로**)** 필드에 플래시 파일 시스템의 경로를 입력하거나 **Browse Flash(**플래시 찾아보기**)**를 클릭하여 플래시 파일 시스템의 디렉터리 또는 파일을 찾습니다.

단계 **6** **Upload Image(**이미지 업로드**)**를 클릭합니다. 업로드 프로세스에 몇 분이 걸릴 수 있습니다.

이 이미지를 ASDM 이미지로 설정할지 묻는 프롬프트가 표시되면 **No(**아니요**)**를 클릭합니다. Upgrade(업그레이드) 툴을 종료합니다.

단계 **7** **Image to Upload(**업로드할 이미지**)** 드롭다운 목록에서 **ASA**를 선택하여 이러한 단계를 반복합니다.

이 이미지를 ASA 이미지로 설정할지 묻는 프롬프트가 표시되면 **No(**아니요**)**를 클릭합니다. Upgrade(업그레이드) 툴을 종료합니다.

단계 **8** 주 IP 주소에 연결하여 ASDM을 액티브 유닛에 연결하고 스탠바이 유닛에서 사용했던 것과 같은 파일 위치를 사용하여 ASDM 소프트웨어를 업로드합니다.

단계 **9** 이미지를 ASDM 이미지로 설정할지 묻는 프롬프트가 표시되면 **Yes(**예**)**를 클릭합니다.

ASDM을 종료하고 컨피그레이션을 저장하라는 메시지가 다시 표시됩니다. **OK(**확인**)**를 클릭합니다. Upgrade(업그레이드) 툴을 종료합니다. 참고**:** ASA 소프트웨어를 업그레이드한 다음 컨피그레이션을 저장하고 ASDM을 다시 로드합니다.

단계 **10** 스탠바이 유닛에서 사용했던 것과 같은 파일 위치를 사용하여 ASA 소프트웨어를 업로드합니다.

단계 **11** 이미지를 ASA 이미지로 설정할지 묻는 프롬프트가 표시되면 **Yes(**예**)**를 클릭합니다.

새 이미지를 사용할 ASA를 다시 로드하라는 메시지가 다시 표시됩니다. **OK(**확인**)**를 클릭합니다. Upgrade(업그레이드) 툴을 종료합니다.

단계 **12** 도구 모음에서 **Save(**저장**)** 아이콘을 클릭하여 컨피그레이션 변경 사항을 저장합니다.

이러한 컨피그레이션 변경 사항은 스탠바이 유닛에 자동으로 저장됩니다.

단계 **13** ASA FirePOWER 모듈을 업그레이드하는 경우 **Tools(**툴**)** > **Command Line Interface(CLI(Command Line Interface))**를 선택하고 **no rest-api enable**을 입력하여 ASA REST API를 비활성화합니다.

REST API를 비활성화하지 않으면 ASA FirePOWER 모듈 업그레이드에 실패하게 됩니다.

단계 **14** 스탠바이 유닛에서 ASA FirePOWER 모듈을 업그레이드합니다.

ASDM으로 관리되는 ASA FirePOWER 모듈의 경우에는 스탠바이 관리 IP 주소에 ASDM을 연결합니다. 업그레이드가 완료될 때까지 기다렸다가 ASDM을 액티브 유닛에 다시 연결합니다.

단계 **15** **Monitoring(**모니터링**)** > **Properties(**속성**)** > **Failover(**페일오버**)** > **Status(**상태**)**를 선택하고 **Reload Standby(**스탠바이 다시 로드**)**를 선택하여 스탠바이 유닛을 다시 로드합니다.

System(시스템**)** 창을 계속 표시한 상태로 스탠바이 유닛이 다시 로드되는 시기를 모니터링합니다.

단계 **16** 스탠바이 유닛이 다시 로드되고 나면 **Monitoring(**모니터링**)** > **Properties(**속성**)** > **Failover(**페일오버**)** > **Status(**상태**)**를 선택하고 **Make Standby(**스탠바이로 만들기**)**를 클릭하여 액티브 유닛을 스탠바이 유닛으로 강제 페일오버합니다.

ASDM이 자동으로 새 액티브 유닛에 다시 연결됩니다.

단계 **17** 이전 액티브 유닛에서 ASA FirePOWER 모듈을 업그레이드합니다.

ASDM으로 관리되는 ASA FirePOWER 모듈의 경우에는 스탠바이 관리 IP 주소에 ASDM을 연결합니다. 업그레이드가 완료될 때까지 기다렸다가 ASDM을 액티브 유닛에 다시 연결합니다.

단계 **18** **Monitoring(**모니터링**)** > **Properties(**속성**)** > **Failover(**페일오버**)** > **Status(**상태**)**를 선택하고 **Reload Standby(**스탠바이 다시 로드**)**를 선택하여 새 스탠바이 유닛을 다시 로드합니다.

액티브/액티브 페일오버 쌍 업그레이드

제로 다운타임 업그레이드를 수행하려면 CLI 또는 ASDM을 사용하여 액티브/액티브 페일오버 쌍을 업그레이드합니다.

CLI를 사용하여 액티브/액티브 페일오버 쌍 업그레이드

액티브/액티브 페일오버 컨피그레이션의 두 유닛을 업그레이드하려면 다음 단계를 수행합니다.

시작하기 전에

- 기본 유닛에서 다음 단계를 수행합니다.
- 시스템 실행 영역에서 다음 단계를 수행합니다.
- 이 절차에서는 FTP를 사용합니다. TFTP, HTTP 또는 기타 서버 유형의 경우 ASA 명령 참조에서 **copy** 명령을 참조하십시오.

단계 **1** 특권 실행 모드의 기본 유닛에서 ASA 소프트웨어를 플래시 메모리에 복사합니다.

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name***disk***n***:/**[*path/*]*asa_image_name*

예제**:**

```
asa/act/pri# copy ftp://jcrichton:aeryn@10.1.1.1/asa991-smp-k8.bin disk0:/asa991-smp-k8.bin
```

단계 **2** 소프트웨어를 보조 유닛에 복사합니다. 기본 유닛과 동일한 경로를 지정해야 합니다.

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name***disk***n***:/**[*path/*]*asa_image_name*

예제**:**

```
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asa991-smp-k8.bin
disk0:/asa991-smp-k8.bin
```

단계 **3** 기본 유닛 플래시 메모리에 ASDM 이미지를 복사합니다.

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name***disk***n***:/**[*path/*]*asdm_image_name*

예제**:**

```
asa/act/pri# ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-771791.bin disk0:/asdm-771791.bin
```

단계 **4** ASDM 이미지를 보조 유닛에 복사합니다. 기본 유닛과 동일한 경로를 지정해야 합니다.

failover exec mate copy /noconfirm
ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name***disk***n***:/**[*path/*]*asdm_image_name*

예제**:**

```
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-771791.bin
disk0:/asdm-771791.bin
```

단계 **5** 아직 전역 컨피그레이션 모드가 아닐 경우 전역 컨피그레이션 모드에 액세스합니다.

configure terminal

단계 **6** 현재 구성된 부트 이미지를 표시합니다(최대 4개).

show running-config boot system

예제**:**

```
asa/act/pri(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ASA에서는 나열된 순서대로 이미지를 사용합니다. 첫 번째 이미지를 사용할 수 없으면 그 다음 이미지를 사용하는 식입니다. 새 이미지 URL을 목록의 맨 위에 삽입할 수 없습니다. 새 이미지가 맨 앞에 오게 하려면 기존 항목을 모두 삭제한 다음 원하는 순서대로 이미지 URL을 입력해야 합니다(다음 단계 참조).

단계 **7** 새 부트 이미지를 첫 번째 선택 사항으로 입력할 수 있도록 기존 부트 이미지 컨피그레이션을 제거합니다.

no boot system disk*n***:/**[*path/*]*asa_image_name*

예제**:**

```
asa/act/pri(config)# no boot system disk0:/cdisk.bin
asa/act/pri(config)# no boot system disk0:/asa931-smp-k8.bin
```

단계 **8** 부팅할 ASA 이미지(방금 업로드한 이미지)를 설정합니다.

boot system disk*n***:/**[*path*/]*asa_image_name*

예제**:**

```
asa/act/pri(config)# boot system disk0://asa991-smp-k8.bin
```

이 이미지를 사용할 수 없을 경우에 사용하려는 모든 백업 이미지에 대해 이 명령을 반복합니다. 예를 들어 이전에 제거한 이미지를 다시 입력할 수 있습니다.

단계 **9** 사용할 ASDM 이미지(방금 업로드한 이미지)를 설정합니다.

asdm image disk*n***:/**[*path*/]*asdm_image_name*

예제**:**

```
asa/act/pri(config)# asdm image disk0:/asdm-771791.bin
```

사용할 ASDM 이미지는 하나만 구성할 수 있습니다. 따라서 먼저 기존 컨피그레이션을 삭제할 필요 없습니다.

단계 **10** 새 설정을 시작 컨피그레이션에 저장합니다.

write memory

이러한 컨피그레이션 변경 사항은 보조 유닛에 자동으로 저장됩니다.

단계 **11** ASA FirePOWER 모듈을 업그레이드하는 경우 ASA REST API를 비활성화합니다. 이렇게 하지 않으면 업그레이드에 실패합니다.

no rest-api agent

단계 **12** 기본 유닛에서 두 페일오버 그룹을 액티브 상태로 만듭니다.

failover active group 1

failover active group 2

예제**:**

```
asa/act/pri(config)# failover active group 1
asa/act/pri(config)# failover active group 2
```

단계 **13** 보조 유닛에서 ASA FirePOWER 모듈을 업그레이드합니다.

ASDM으로 관리되는 ASA FirePOWER 모듈의 경우에는 페일오버 그룹 1 또는 2 스탠바이 관리 IP 주소에 ASDM을 연결합니다. 업그레이드가 완료될 때까지 기다립니다.

단계 **14** 새 이미지를 부팅하기 위해 보조 유닛을 다시 로드합니다.

failover reload-standby

보조 유닛에서 로딩을 마칠 때까지 기다립니다. **show failover** 명령을 사용하여 두 페일오버 그룹 모두 Standby Ready 상태임을 확인합니다.

단계 **15** 강제적으로 보조 유닛에서 두 페일오버 그룹이 액티브 상태가 되게 합니다.

no failover active group 1

no failover active group 2

예제**:**

```
asa/act/pri(config)# no failover active group 1
asa/act/pri(config)# no failover active group 2
asa/stby/pri(config)#
```

SSH 세션에서 연결이 끊긴 경우 이제 보조 유닛에서 페일오버 그룹 1 IP 주소에 다시 연결합니다.

단계 **16** 기본 유닛에서 ASA FirePOWER 모듈을 업그레이드합니다.

ASDM으로 관리되는 ASA FirePOWER 모듈의 경우에는 페일오버 그룹 1 또는 2 스탠바이 관리 IP 주소에 ASDM을 연결합니다. 업그레이드가 완료될 때까지 기다립니다.

단계 **17** Reload the primary unit:

failover reload-standby

예제**:**

```
asa/act/sec# failover reload-standby
```

참고 기본 유닛 콘솔 포트에 연결되어 있는 경우에는 대신 **reload** 명령을 입력하여 기본 유닛을 다시 로드해야 합니다.

SSH 세션에서 연결이 끊어질 수 있습니다.

단계 **18** 페일오버 그룹이 **preempt** 명령으로 구성된 경우, 우선적 지연 시간이 지나면 지정된 유닛에서 자동으로 액티브 상태가 됩니다.

ASDM을 사용하여 액티브/액티브 페일오버 쌍 업그레이드

액티브/액티브 페일오버 컨피그레이션의 두 유닛을 업그레이드하려면 다음 단계를 수행합니다.

시작하기 전에

- 시스템 실행 영역에서 다음 단계를 수행합니다.
- 로컬 관리 컴퓨터에 ASA 및 ASDM 이미지를 저장합니다.

단계 **1** 페일오버 그룹 2의 관리 주소에 연결하여 보조 유닛에서 ASDM을 실행합니다.

단계 **2** 기본 ASDM 애플리케이션 창에서 **Tools(**툴**)** > **Upgrade Software from Local Computer(**로컬 컴퓨터에서 소프트웨어 업그레이드**)**를 선택합니다.

Upgrade Software(소프트웨어 업그레이드**)** 대화 상자가 나타납니다.

단계 **3** **Image to Upload(**업로드할 이미지**)** 드롭다운 목록에서 **ASDM**을 선택합니다.

단계 **4** **Local File Path(**로컬 파일 경로**)** 필드에 컴퓨터에 있는 파일의 로컬 경로를 입력하거나 **Browse Local Files(**로컬 파일 찾아보기**)**를 클릭하여 PC의 파일을 찾습니다.

단계 **5** **Flash File System Path(**플래시 파일 시스템 경로**)** 필드에 플래시 파일 시스템의 경로를 입력하거나 **Browse Flash(**플래시 찾아보기**)**를 클릭하여 플래시 파일 시스템의 디렉터리 또는 파일을 찾습니다.

단계 **6** **Upload Image(**이미지 업로드**)**를 클릭합니다. 업로드 프로세스에 몇 분이 걸릴 수 있습니다.

이 이미지를 ASDM 이미지로 설정할지 묻는 프롬프트가 표시되면 **No(**아니요**)**를 클릭합니다. Upgrade(업그레이드) 툴을 종료합니다.

단계 **7** **Image to Upload(**업로드할 이미지**)** 드롭다운 목록에서 **ASA**를 선택하여 이러한 단계를 반복합니다.

이 이미지를 ASA 이미지로 설정할지 묻는 프롬프트가 표시되면 **No(**아니요**)**를 클릭합니다. Upgrade(업그레이드) 툴을 종료합니다.

단계 **8** 페일오버 그룹 1의 관리 IP 주소에 연결하여 ASDM을 기본 유닛에 연결하고 보조 유닛에서 사용했던 것과 같은 파일 위치를 사용하여 ASDM 소프트웨어를 업로드합니다.

단계 **9** 이미지를 ASDM 이미지로 설정할지 묻는 프롬프트가 표시되면 **Yes(**예**)**를 클릭합니다.

ASDM을 종료하고 컨피그레이션을 저장하라는 메시지가 다시 표시됩니다. **OK(**확인**)**를 클릭합니다. Upgrade(업그레이드) 툴을 종료합니다. 참고**:** ASA 소프트웨어를 업그레이드한 다음 컨피그레이션을 저장하고 ASDM을 다시 로드합니다.

단계 **10** 보조 유닛에서 사용했던 것과 같은 파일 위치를 사용하여 ASA 소프트웨어를 업로드합니다.

단계 **11** 이미지를 ASA 이미지로 설정할지 묻는 프롬프트가 표시되면 **Yes(**예**)**를 클릭합니다.

새 이미지를 사용할 ASA를 다시 로드하라는 메시지가 다시 표시됩니다. **OK(**확인**)**를 클릭합니다. Upgrade(업그레이드) 툴을 종료합니다.

단계 **12** 도구 모음에서 **Save(**저장**)** 아이콘을 클릭하여 컨피그레이션 변경 사항을 저장합니다.

이러한 컨피그레이션 변경 사항은 보조 유닛에 자동으로 저장됩니다.

단계 **13** ASA FirePOWER 모듈을 업그레이드하는 경우 **Tools(**툴**)** > **Command Line Interface(CLI(Command Line Interface))**를 선택하고 **no rest-api enable**을 입력하여 ASA REST API를 비활성화합니다.

REST API를 비활성화하지 않으면 ASA FirePOWER 모듈 업그레이드에 실패하게 됩니다.

단계 **14** **Monitoring(**모니터링**)** > **Failover(**페일오버**)** > **Failover Group #(**페일오버 그룹 **#)**을 선택(#은 기본 유닛으로 이동할 페일오버 그룹의 번호)한 다음 **Make Active(**활성으로 설정**)**를 클릭하여 기본 유닛에서 두 페일오버 그룹을 모두 활성으로 설정합니다.

단계 **15** 보조 유닛에서 ASA FirePOWER 모듈을 업그레이드합니다.

ASDM으로 관리되는 ASA FirePOWER 모듈의 경우에는 페일오버 그룹 1 또는 2 스탠바이 관리 IP 주소에 ASDM을 연결합니다. 업그레이드가 완료될 때까지 기다렸다가 ASDM을 기본 유닛에 다시 연결합니다.

단계 **16** **Monitoring(**모니터링**)** > **Failover(**페일오버**)** > **System(**시스템**)**을 선택하고 **Reload Standby(**스탠바이 다시 로드**)**를 선택하여 보조 유닛을 다시 로드합니다.

System(시스템**)** 창을 계속 표시한 상태로 보조 유닛이 다시 로드되는 시기를 모니터링합니다.

단계 **17** 보조 유닛이 작동하고 나면 **Monitoring(**모니터링**)** > **Failover(**페일오버**)** > **Failover Group #(**페일오버 그룹 **#)**을 선택(#은 보조 유닛으로 이동할 페일오버 그룹의 번호)한 다음 **Make Standby(**스탠바이로 만들기**)**를 클릭하여 보조 유닛에서 두 페일오버 그룹을 모두 활성으로 설정합니다.

ASDM이 자동으로 보조 유닛의 페일오버 그룹 1 IP 주소에 다시 연결됩니다.

단계 **18** 기본 유닛에서 ASA FirePOWER 모듈을 업그레이드합니다.

ASDM으로 관리되는 ASA FirePOWER 모듈의 경우에는 페일오버 그룹 1 또는 2 스탠바이 관리 IP 주소에 ASDM을 연결합니다. 업그레이드가 완료될 때까지 기다렸다가 ASDM을 보조 유닛에 다시 연결합니다.

단계 **19** **Monitoring(**모니터링**)** > **Failover(**페일오버 > **System(**시스템**)**을 선택하고 **Reload Standby(**스탠바이 다시 로드**)**를 선택하여 기본 유닛을 다시 로드합니다.

단계 **20** 페일오버 그룹이 Preempt Enabled로 구성된 경우, 우선적 지연 시간이 지나면 지정된 유닛에서 자동으로 액티브 상태가 됩니다. ASDM이 자동으로 기본 유닛의 페일오버 그룹 1 IP 주소에 다시 연결됩니다.

ASA 클러스터 업그레이드

제로 다운타임 업그레이드를 수행하려면 CLI 또는 ASDM을 사용하여 ASA 클러스터를 업그레이드합니다.

CLI를 사용하여 ASA 클러스터 업그레이드

ASA 클러스터의 모든 유닛을 업그레이드하려면 다음 단계를 수행합니다. 이 절차에서는 FTP를 사용합니다. TFTP, HTTP 또는 기타 서버 유형의 경우 ASA 명령 참조에서 **copy** 명령을 참조하십시오.

시작하기 전에

- 마스터 유닛에서 다음 단계를 수행합니다. ASA FirePOWER 모듈도 업그레이드하는 경우에는 각 슬레이브 유닛에서 콘솔 또는 ASDM에 액세스해야 합니다. 클러스터 유닛과 상태(마스터 또는 슬레이브)를 표시하도록 ASA 프롬프트를 구성할 수 있습니다. 이렇게 하면 연결된 유닛을 확인하는 데 유용합니다. prompt 명령을 참조하십시오. 또는 **show cluster info** 명령을 입력하여 각 유닛의 역할을 확인합니다.
- 콘솔 포트를 사용해야 합니다. 원격 CLI 연결에서는 클러스터링을 활성화하거나 비활성화할 수 없습니다.
- 여러 컨텍스트 모드의 경우 시스템 실행 영역에서 다음 단계를 수행합니다.

단계 **1** 특권 실행 모드의 마스터 유닛에서 ASA 이미지를 클러스터의 모든 유닛에 복사합니다.

cluster exec copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name***disk***n***:/**[*path/*]*asa_image_name*

예제**:**

```
asa/unit1/master# cluster exec copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asa991-smp-k8.bin disk0:/asa991-smp-k8.bin
```

단계 **2** ASDM 이미지를 클러스터의 모든 유닛에 복사합니다.

cluster exec copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]/*asdm_image_name***disk***n***:/**[*path/*]*asdm_image_name*

예제**:**

```
asa/unit1/master# cluster exec copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-771791.bin
disk0:/asdm-771791.bin
```

단계 **3** 아직 전역 컨피그레이션 모드가 아닐 경우 지금 해당 모드에 액세스합니다.

configure terminal

예제**:**

```
asa/unit1/master# configure terminal
asa/unit1/master(config)#
```

단계 **4** 현재 구성된 부트 이미지를 표시합니다(최대 4개).

show running-config boot system

예제**:**

```
asa/unit1/master(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ASA에서는 나열된 순서대로 이미지를 사용합니다. 첫 번째 이미지를 사용할 수 없으면 그 다음 이미지를 사용하는 식입니다. 새 이미지 URL을 목록의 맨 위에 삽입할 수 없습니다. 새 이미지가 맨 앞에 오게 하려면 기존 항목을 모두 삭제한 다음 원하는 순서대로 이미지 URL을 입력해야 합니다(다음 단계 참조).

단계 **5** 새 부트 이미지를 첫 번째 선택 사항으로 입력할 수 있도록 기존 부트 이미지 컨피그레이션을 제거합니다.

no boot system disk*n***:/**[*path/*]*asa_image_name*

예제**:**

```
asa/unit1/master(config)# no boot system disk0:/cdisk.bin
asa/unit1/master(config)# no boot system disk0:/asa931-smp-k8.bin
```

단계 **6** 부팅할 ASA 이미지(방금 업로드한 이미지)를 설정합니다.

boot system disk*n***:/**[*path/*]*asa_image_name*

예제**:**

```
asa/unit1/master(config)# boot system disk0://asa991-smp-k8.bin
```

이 이미지를 사용할 수 없을 경우에 사용하려는 모든 백업 이미지에 대해 이 명령을 반복합니다. 예를 들어 이전에 제거한 이미지를 다시 입력할 수 있습니다.

단계 **7** 사용할 ASDM 이미지(방금 업로드한 이미지)를 설정합니다.

asdm image disk*n*:/[*path*/]*asdm_image_name*

예제:

```
asa/unit1/master(config)# asdm image disk0:/asdm-771791.bin
```

사용할 ASDM 이미지는 하나만 구성할 수 있습니다. 따라서 먼저 기존 컨피그레이션을 삭제할 필요 없습니다.

단계 **8** 새 설정을 시작 컨피그레이션에 저장합니다.

write memory

이러한 컨피그레이션 변경 사항은 슬레이브 유닛에 자동으로 저장됩니다.

단계 **9** ASA FirePOWER 모듈을 업그레이드하는 경우 ASA REST API를 비활성화합니다. 이렇게 하지 않으면 ASA FirePOWER 모듈 업그레이드에서 장애가 발생합니다.

no rest-api agent

단계 **10** ASDM으로 관리되는 ASA FirePOWER 모듈을 업그레이드하는 경우에는 ASDM을 개별 관리 IP 주소에 연결해야 하므로 각 유닛의 IP 주소를 확인해야 합니다.

show running-config interface *management_interface_id*

사용하는 **cluster-pool** poolname을 확인합니다.

show ip[**v6**] **local pool** *poolname*

클러스터 유닛 IP 주소를 확인합니다.

예제:

```
asa/unit2/slave# show running-config interface gigabitethernet0/0
!
interface GigabitEthernet0/0
 management-only
 nameif inside
 security-level 100
 ip address 10.86.118.1 255.255.252.0 cluster-pool inside-pool
asa/unit2/slave# show ip local pool inside-pool
Begin           End             Mask            Free     Held     In use
10.86.118.16    10.86.118.17    255.255.252.0       0        0        2

Cluster Unit                    IP Address Allocated
unit2                           10.86.118.16
unit1                           10.86.118.17
asa1/unit2/slave#
```

단계 **11** 슬레이브 유닛을 업그레이드합니다.

ASA FirePOWER 모듈도 업그레이드하는지 여부에 따라 아래에서 절차를 선택합니다. ASA FirePOWER 절차를 수행하면 ASA FirePOWER 모듈도 업그레이드하는 경우 ASA 다시 로드 횟수를 최소화할 수 있습니다. 이러한 절차에는 슬레이브 콘솔 또는 ASDM을 사용하도록 선택할 수 있습니다. 모든 콘솔 포트에 즉시 액세스할 수는 없지만 네트워크를 통해 ASDM에 연결할 수는 있는 경우 콘솔 대신 ASDM을 사용할 수 있습니다.

참고 업그레이드 프로세스 중에는 **cluster master unit** 명령을 사용하여 슬레이브 유닛을 마스터로 강제 지정하지 마십시오. 이렇게 하면 네트워크 연결 및 클러스터 안정성 관련 문제가 발생할 수 있습니다. 전체 슬레이브 유닛을 먼저 업그레이드하고 다시 로드한 다음, 이 절차를 계속 진행하여 현재 마스터 유닛에서 새 마스터 유닛으로 원활하게 전환해야 합니다.

ASA FirePOWER 모듈을 업그레이드하지 않는 경우**:**

a) 마스터 유닛에서 멤버 이름을 보려면 **cluster exec unit ?**를 입력하거나 **show cluster info** 명령을 입력합니다.
b) 슬레이브 유닛을 다시 로드합니다.

cluster exec unit *slave-unit***reload noconfirm**

예제**:**

```
asa/unit1/master# cluster exec unit unit2 reload noconfirm
```

c) 각 슬레이브 유닛에 대해 위의 단계를 반복합니다.

연결 손실을 방지하고 트래픽이 안정화될 수 있도록 각 유닛이 다시 작동되고 클러스터에 다시 합류할 때까지 5분 정도 기다렸다가 다음 유닛에 대해 이러한 단계를 반복합니다. 유닛이 언제 클러스터에 다시 합류하는지 보려면 **show cluster info**를 입력합니다.

슬레이브 콘솔을 사용하여 **ASA FirePOWER** 모듈도 업그레이드하는 경우**:**

a) 슬레이브 유닛의 콘솔 포트에 연결한 다음 전역 설정 모드를 설정합니다.

enable

configure terminal

예제**:**

```
asa/unit2/slave> enable
Password:
asa/unit2/slave# configure terminal
asa/unit2/slave(config)#
```

b) 클러스터링을 비활성화합니다.

cluster group *name*

no enable

이 컨피그레이션을 저장하지 마십시오. 다시 로드 시에 클러스터링이 활성화되어야 합니다. 업그레이드 프로세스 중에 여러 번의 장애와 다시 합류를 방지하려면 클러스터링을 비활성화해야 합니다. 이 유닛은 모든 업그레이드 및 다시 로드가 완료된 후에만 다시 합류해야 합니다.

예제**:**

```
asa/unit2/slave(config)# cluster group cluster1
asa/unit2/slave(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable
clustering or remove cluster group configuration.

Cluster unit unit2 transitioned from SLAVE to DISABLED
```

```
asa/unit2/ClusterDisabled(cfg-cluster)#
```

c) 이 슬레이브 유닛에서 ASA FirePOWER 모듈을 업그레이드합니다.

ASDM으로 관리되는 ASA FirePOWER 모듈의 경우에는 앞에서 확인한 개별 관리 IP 주소에 ASDM을 연결합니다. 업그레이드가 완료될 때까지 기다립니다.

d) 슬레이브 유닛을 다시 로드합니다.

reload noconfirm

e) 각 슬레이브 유닛에 대해 위의 단계를 반복합니다.

연결 손실을 방지하고 트래픽이 안정화될 수 있도록 각 유닛이 다시 작동되고 클러스터에 다시 합류할 때까지 5분 정도 기다렸다가 다음 유닛에 대해 이러한 단계를 반복합니다. 유닛이 언제 클러스터에 다시 합류하는지 보려면 **show cluster info**를 입력합니다.

ASDM을 사용하여 **ASA FirePOWER** 모듈도 업그레이드하는 경우**:**

a) 앞에서 확인한 이 슬레이브 유닛의 개별 관리 IP 주소에 ASDM을 연결합니다.
b) **Configuration(**컨피그레이션**)** > **Device ManagementHigh Availability and Scalability(**디바이스 관리 고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Configuration(**클러스터 컨피그레이션**)** > 을 선택합니다.
c) **Participate in ASA cluster(ASA** 클러스터에 참가**)** 확인란의 선택을 취소합니다.

업그레이드 프로세스 중에 여러 번의 장애와 다시 합류를 방지하려면 클러스터링을 비활성화해야 합니다. 이 유닛은 모든 업그레이드 및 다시 로드가 완료된 후에만 다시 합류해야 합니다.

Configure ASA cluster settings(ASA 클러스터 설정 구성**)** 확인란의 선택을 취소하지 마십시오. 취소할 경우 모든 클러스터 컨피그레이션이 지워지며 ASDM이 연결된 모든 관리 인터페이스를 비롯한 모든 인터페이스도 종료됩니다. 이 경우 연결을 복원하려면 콘솔 포트의 CLI에 액세스해야 합니다.

참고 일부 이전 버전 ASDM의 경우 이 화면에서 클러스터를 비활성화할 수 없습니다. 이 경우에는 **Tools(**툴**)** > **Command Line Interface(CLI(Command Line Interface))** 툴을 사용하여 **Multiple Line(**여러 행**)** 라디오 버튼을 클릭하고 **cluster group** *name* 및 **no enable**을 입력합니다. **Home(**홈**)** > **Device Dashboard(**디바이스 대시보드**)** > **Device Information(**디바이스 정보**)** > **ASA Cluster(ASA** 클러스터**)** 영역에서 클러스터 그룹 이름을 확인할 수 있습니다.

d) **Apply(**적용**)**를 클릭합니다.
e) ASDM을 종료하라는 메시지가 표시됩니다. 같은 IP 주소에 ASDM을 다시 연결합니다.
f) ASA FirePOWER 모듈을 업그레이드합니다.

업그레이드가 완료될 때까지 기다립니다.

g) ASDM에서 **Tools(**툴**)** > **System Reload(**시스템 다시 로드**)**를 선택합니다.
h) **Reload without saving the running configuration(**실행 중인 컨피그레이션을 저장하지 않고 다시 로드**)** 라디오 버튼을 클릭합니다.

컨피그레이션은 저장하지 않아야 합니다. 이 유닛이 다시 로드될 때 유닛에서 클러스터링이 활성화되어야 합니다.

i) **Schedule Reload(**다시 로드 예약**)**를 클릭합니다.

j) **Yes(**예**)**를 클릭하여 다시 로드를 계속합니다.
k) 각 슬레이브 유닛에 대해 위의 단계를 반복합니다.

연결 손실을 방지하고 트래픽이 안정화될 수 있도록 각 유닛이 다시 작동되고 클러스터에 다시 합류할 때까지 5분 정도 기다렸다가 다음 유닛에 대해 이러한 단계를 반복합니다. 유닛이 언제 클러스터에 다시 합류하는지 보려면 마스터 유닛에서 **Monitoring(**모니터링**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Summary(**클러스터 요약**)**를 확인합니다.

단계 **12** 마스터 유닛을 업그레이드합니다.

a) 클러스터링을 비활성화합니다.

cluster group *name*

no enable

새 마스터 유닛이 선택되고 트래픽이 안정화될 때까지 5분 동안 기다립니다.

이 컨피그레이션을 저장하지 마십시오. 다시 로드 시에 클러스터링이 활성화되어야 합니다.

새 마스터 유닛이 최대한 확실하고 빠르게 선택될 수 있도록 가능하면 마스터 유닛에서 클러스터를 수동으로 비활성화하는 것이 좋습니다.

예제**:**

```
asa/unit1/master(config)# cluster group cluster1
asa/unit1/master(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable
clustering or remove cluster group configuration.

Cluster unit unit1 transitioned from MASTER to DISABLED
asa/unit1/ClusterDisabled(cfg-cluster)#
```

b) 이 유닛에서 ASA FirePOWER 모듈을 업그레이드합니다.

ASDM으로 관리되는 ASA FirePOWER 모듈의 경우에는 앞에서 확인한 개별 관리 IP 주소에 ASDM을 연결합니다. 주 클러스터 IP 주소는 이제 새 마스터 유닛에 속합니다. 개별 관리 IP 주소에서는 이 이전 마스터 유닛에 계속 액세스할 수 있습니다.

업그레이드가 완료될 때까지 기다립니다.

c) 이 유닛을 다시 로드합니다.

reload noconfirm

이전의 마스터 유닛은 다시 클러스터에 합류하면 슬레이브 유닛이 됩니다.

ASDM을 사용하여 ASA 클러스터 업그레이드

ASA 클러스터의 모든 유닛을 업그레이드하려면 다음 단계를 수행합니다.

시작하기 전에

- 마스터 유닛에서 다음 단계를 수행합니다. ASA FirePOWER 모듈도 업그레이드하는 경우에는 각 슬레이브 유닛에서 ASDM에 액세스해야 합니다.
- 여러 컨텍스트 모드의 경우 시스템 실행 영역에서 다음 단계를 수행합니다.
- 로컬 관리 컴퓨터에 ASA 및 ASDM 이미지를 저장합니다.

단계 **1** 주 클러스터 IP 주소에 연결하여 마스터 유닛에서 ASDM을 실행합니다.

이 IP 주소는 항상 마스터 유닛에 할당된 상태로 유지됩니다.

단계 **2** 기본 ASDM 애플리케이션 창에서 **Tools(**툴**)** > **Upgrade Software from Local Computer(**로컬 컴퓨터에서 소프트웨어 업그레이드**)**를 선택합니다.

Upgrade Software from Local Computer(로컬 컴퓨터에서 소프트웨어 업그레이드**)** 대화 상자가 나타납니다.

단계 **3** **All devices in the cluster(**클러스터에 있는 모든 디바이스**)** 라디오 버튼을 클릭합니다.

Upgrade Software(소프트웨어 업그레이드**)** 대화 상자가 나타납니다.

단계 **4** **Image to Upload(**업로드할 이미지**)** 드롭다운 목록에서 **ASDM**을 선택합니다.

단계 **5** **Local File Path(**로컬 파일 경로**)** 필드에서 **Browse Local Files(**로컬 파일 찾아보기**)**를 클릭하여 컴퓨터의 파일을 찾습니다.

단계 **6** (선택 사항) **Flash File System Path(**플래시 파일 시스템 경로**)** 필드에 플래시 파일 시스템의 경로를 입력하거나 **Browse Flash(**플래시 찾아보기**)**를 클릭하여 플래시 파일 시스템의 디렉터리 또는 파일을 찾습니다.

기본적으로 이 필드에는 **disk0:**/*filename* 경로가 미리 입력되어 있습니다.

단계 **7** **Upload Image(**이미지 업로드**)**를 클릭합니다. 업로드 프로세스에 몇 분이 걸릴 수 있습니다.

단계 **8** 이 이미지를 ASDM 이미지로 설정할지 묻습니다. **Yes(**예**)**를 클릭합니다.

단계 **9** ASDM을 종료하고 컨피그레이션을 저장하라는 메시지가 다시 표시됩니다. **OK(**확인**)**를 클릭합니다.

Upgrade(업그레이드) 툴을 종료합니다. 참고**:** ASA 소프트웨어를 업그레이드한 다음 컨피그레이션을 저장하고 ASDM을 다시 로드합니다.

단계 **10** **Image to Upload(**업로드할 이미지**)** 드롭다운 목록에서 **ASA**를 선택하여 이러한 단계를 반복합니다.

단계 **11** 도구 모음에서 **Save(**저장**)** 아이콘을 클릭하여 컨피그레이션 변경 사항을 저장합니다.

이러한 컨피그레이션 변경 사항은 슬레이브 유닛에 자동으로 저장됩니다.

단계 **12** 나중에 ASDM을 슬레이브 유닛에 직접 연결할 수 있도록 **Configuration(**컨피그레이션**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Members(**클러스터 요소**)**에서 각 유닛의 개별 관리 IP 주소를 확인합니다.

단계 **13** ASA FirePOWER 모듈을 업그레이드하는 경우 **Tools(**툴**)** > **Command Line Interface(CLI(Command Line Interface))**를 선택하고 **no rest-api enable**을 입력하여 ASA REST API를 비활성화합니다.

REST API를 비활성화하지 않으면 ASA FirePOWER 모듈 업그레이드에 실패하게 됩니다.

단계 **14** 슬레이브 유닛을 업그레이드합니다.

ASA FirePOWER 모듈도 업그레이드하는지 여부에 따라 아래에서 절차를 선택합니다. ASA FirePOWER 절차를 수행하면 ASA FirePOWER 모듈도 업그레이드하는 경우 ASA 다시 로드 횟수를 최소화할 수 있습니다.

참고 업그레이드 프로세스 중에는 **Monitoring(**모니터링**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Summary(**클러스터 요약**)** > **Change Master To(**마스터 변경 대상**)** 드롭다운 목록을 사용하여 슬레이브 유닛을 마스터로 강제 지정하지 마십시오. 이렇게 하면 네트워크 연결 및 클러스터 안정성 관련 문제가 발생할 수 있습니다. 전체 슬레이브 유닛을 먼저 다시 로드한 다음, 이 절차를 계속 진행하여 현재 마스터 유닛에서 새 마스터 유닛으로 원활하게 전환해야 합니다.

ASA FirePOWER 모듈을 업그레이드하지 않는 경우**:**

a) 마스터 유닛에서 **Tools(**툴**)** > **System Reload(**시스템 다시 로드**)**를 선택합니다.
b) **Device(**디바이스**)** 드롭다운 목록에서 슬레이브 유닛 이름을 선택합니다.
c) **Schedule Reload(**다시 로드 예약**)**를 클릭합니다.
d) **Yes(**예**)**를 클릭하여 다시 로드를 계속합니다.
e) 각 슬레이브 유닛에 대해 위의 단계를 반복합니다.

연결 손실을 방지하고 트래픽이 안정화될 수 있도록 각 유닛이 다시 작동되고 클러스터에 다시 합류할 때까지 5분 정도 기다렸다가 다음 유닛에 대해 이러한 단계를 반복합니다. 유닛이 언제 클러스터에 다시 합류하는지 보려면 **Monitoring(**모니터링**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Summary(**클러스터 요약**)** 창을 확인합니다.

ASA FirePOWER 모듈도 업그레이드하는 경우**:**

a) 마스터 유닛에서 **Configuration(**컨피그레이션**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Members(**클러스터 요소**)**를 선택합니다.
b) 업그레이드할 슬레이브 유닛을 선택하고 **Delete(**삭제**)**를 클릭합니다.
c) **Apply(**적용**)**를 클릭합니다.
d) ASDM을 종료한 다음 앞에서 확인한 개별 관리 IP 주소에 연결하여 슬레이브 유닛에 ASDM을 연결합니다.
e) ASA FirePOWER 모듈을 업그레이드합니다.

업그레이드가 완료될 때까지 기다립니다.

f) ASDM에서 **Tools(**툴**)** > **System Reload(**시스템 다시 로드**)**를 선택합니다.
g) **Reload without saving the running configuration(**실행 중인 컨피그레이션을 저장하지 않고 다시 로드**)** 라디오 버튼을 클릭합니다.

컨피그레이션은 저장하지 않아야 합니다. 이 유닛이 다시 로드될 때 유닛에서 클러스터링이 활성화되어야 합니다.

h) **Schedule Reload(**다시 로드 예약**)**를 클릭합니다.
i) **Yes(**예**)**를 클릭하여 다시 로드를 계속합니다.
j) 각 슬레이브 유닛에 대해 위의 단계를 반복합니다.

연결 손실을 방지하고 트래픽이 안정화될 수 있도록 각 유닛이 다시 작동되고 클러스터에 다시 합류할 때까지 5분 정도 기다렸다가 다음 유닛에 대해 이러한 단계를 반복합니다. 유닛이 언제 클러스터에 다시 합류하

는지 보려면 **Monitoring(**모니터링**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Summary(**클러스터 요약**)** 창을 확인합니다.

단계 **15** 마스터 유닛을 업그레이드합니다.

a) 마스터 유닛의 ASDM에서 **Configuration(**컨피그레이션**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Configuration(**클러스터 컨피그레이션**)** 창을 선택합니다.

b) **Participate in ASA cluster(ASA** 클러스터에 참여**)** 체크 박스를 선택 취소하고 **Apply(**적용**)**를 클릭합니다.

ASDM을 종료하라는 메시지가 표시됩니다.

c) 새 마스터 유닛이 선택되고 트래픽이 안정화될 때까지 최대 5분 동안 기다립니다.

이전의 마스터 유닛은 다시 클러스터에 합류하면 슬레이브 유닛이 됩니다.

d) ASDM을 앞에서 확인한 개별 관리 IP 주소에 연결하여 이전 마스터 유닛에 다시 연결합니다.

주 클러스터 IP 주소는 이제 새 마스터 유닛에 속합니다. 개별 관리 IP 주소에서는 이 이전 마스터 유닛에 계속 액세스할 수 있습니다.

e) ASA FirePOWER 모듈을 업그레이드합니다.

업그레이드가 완료될 때까지 기다립니다.

f) **Tools(**툴**)** > **System Reload(**시스템 다시 로드**)**를 선택합니다.

g) **Reload without saving the running configuration(**실행 중인 컨피그레이션을 저장하지 않고 다시 로드**)** 라디오 버튼을 클릭합니다.

컨피그레이션은 저장하지 않아야 합니다. 이 유닛이 다시 로드될 때 유닛에서 클러스터링이 활성화되어야 합니다.

h) **Schedule Reload(**다시 로드 예약**)**를 클릭합니다.

i) **Yes(**예**)**를 클릭하여 다시 로드를 계속합니다.

ASDM을 종료하라는 메시지가 표시됩니다. 주 클러스터 IP 주소에서 ASDM을 재시작합니다. 그러면 새 마스터 유닛에 다시 연결됩니다.

ASA FirePOWER 모듈 업그레이드 - Firepower Management Center 포함

Firepower Management Center로 관리되는 ASA FirePOWER 모듈을 업그레이드하려면 이 절차를 사용합니다.

독립형 ASA 디바이스의 ASA FirePOWER 모듈과 함께 ASA를 업그레이드하는 경우에는 ASA를 업그레이드하고 다시 로드한 후에 모듈을 업그레이드하십시오. 클러스터형 또는 페일오버 ASA 디바이스에서 ASA와 ASA FirePOWER 모듈을 업그레이드하는 경우에는 각 유닛을 다시 로드하기 전에

각 모듈을 업그레이드하십시오. 자세한 내용은 ASA FirePOWER 모듈 업그레이드 경로 - Firepower Management Center 포함, 118 페이지 및 ASA 업그레이드 절차를 참조하십시오.

ASA를 업그레이드하지 않는 경우 ASA 페일오버 또는 클러스터링 컨피그레이션과 관계없이 모든 ASA FirePOWER 모듈을 함께 업그레이드할 수 있습니다. 하지만 이 경우에도 트래픽 손실을 방지하기 위해 모듈 업그레이드 전에 유닛에서 클러스터링을 비활성화하거나 페일오버를 수행할 수 있도록 ASA 페일오버 및 클러스터링 업그레이드 절차를 참조해야 합니다.

⚠

주의 업그레이드 중인 어플라이언스를 종료하거나, 수동으로 리부팅하거나, 해당 어플라이언스로/어플라이언스에서 변경 사항을 구축하지 마십시오. 진행 중인 업그레이드를 재시작하지 마십시오. 사전 확인 중에는 업그레이드 프로세스가 비활성 상태로 표시될 수 있으며 이는 정상적인 현상입니다. 업그레이드에 문제(업그레이드 실패 또는 응답하지 않는 어플라이언스 포함)가 있을 경우 Cisco TAC에 문의하십시오.

시작하기 전에

업그레이드 경로(ASA 및 Firepower Management Center 업그레이드 포함)에서 현재 위치를 확인합니다. 이 단계를 완벽하게 계획하고 준비했는지 확인합니다.

ASA 및 ASA FirePOWER 버전은 광범위하게 호환됩니다. 하지만 ASA 업그레이드가 필요하지 않더라도 문제를 해결하려면 지원되는 최신 버전으로 업그레이드해야 할 수 있습니다.

단계 **1** 업그레이드하려는 디바이스에 컨피그레이션을 구축합니다.

Firepower Management Center 메뉴 바에서 **Deploy(**구축**)**를 클릭합니다. 디바이스를 선택하고 **Deploy(**구축**)**를 다시 클릭합니다. 지금 오래된 디바이스에 구축하지 않으면 최종 업그레이드에 실패할 수 있으며, 그러면 해당 디바이스에 이미지를 재설치해야 할 수 있습니다.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하면 Snort 프로세스가 재시작되어 트래픽 검사가 중단되며 디바이스가 트래픽을 처리하는 방법에 따라서 재시작이 완료될 때까지 트래픽도 중단될 수 있습니다. 자세한 내용은 ASA FirePOWER 업그레이드 동작, 131 페이지를 참조하십시오.

단계 **2** (버전 6.1 이상으로 업그레이드) ASA REST API를 비활성화합니다.

REST API를 비활성화하지 않으면 업그레이드에 실패하게 됩니다. ASA FirePOWER 모듈의 버전 6.0 이상을 실행 중인 경우에도 ASA 5506-X Series 디바이스는 ASA REST API를 지원하지 않습니다.

ASA에서 CLI를 사용하여 REST API를 비활성화합니다.

no rest-api agent

업그레이드 후에 REST API를 다시 활성화할 수 있습니다.

rest-api agent

단계 **3** 업그레이드 전 최종 확인을 수행합니다.

- 상태 확인 - Message Center를 사용합니다(메뉴 바에서 System Status(시스템 상태) 아이콘 클릭). 구축의 어플라이언스가 성공적으로 통신하는지, 상태 모니터에서 보고하는 문제가 없는지 확인합니다.

- 작업 실행 - 역시 Message Center에서 필수 작업이 완료되었는지 확인합니다. 업그레이드를 시작할 때 실행 중인 작업은 중지되어 실패한 작업이 되며 다시 시작할 수 없습니다. 장애 발생 상태 메시지는 나중에 수동으로 삭제할 수 있습니다.
- 디스크 공간 확인 - 최종 디스크 공간 확인을 수행합니다. 사용 가능한 디스크 공간이 부족하면 업그레이드에 실패합니다.

단계 **4** **System**(시스템) > **Updates**(업데이트)를 선택합니다.

단계 **5** 사용하려는 업그레이드 패키지 옆의 설치 아이콘을 클릭하고 업그레이드할 디바이스를 선택합니다.

업그레이드하려는 디바이스가 나열되어 있지 않은 경우 업그레이드 패키지를 잘못 선택한 것입니다.

참고 6개 이상의 디바이스를 동시에 업그레이드하지 않는 것이 좋습니다. 선택한 모든 디바이스에서 프로세스를 완료할 때까지 Firepower Management Center에서는 디바이스 업그레이드 중지를 허용하지 않습니다. 디바이스 하나의 업그레이드에서 문제가 발생하는 경우 모든 디바이스가 업그레이드를 완료해야 문제를 해결할 수 있습니다.

단계 **6** **Install**(설치)을 클릭하고 디바이스를 업그레이드 및 리부팅할 것임을 확인합니다.

디바이스가 구성 및 구축된 방식에 따라 트래픽은 업그레이드 전 과정에서 삭제되거나 검사 없이 네트워크를 통과합니다. 자세한 내용은 ASA FirePOWER 업그레이드 동작, 131 페이지를 참조하십시오.

단계 **7** Message Center에서 업그레이드 진행 상황을 모니터링합니다.

업그레이드되고 있는 디바이스에는 컨피그레이션을 구축하지 마십시오. Message Center에서 몇 분간 진행 상황이 표시되지 않거나 업그레이드에서 장애가 발생했다고 나타나더라도 업그레이드를 재시작하거나 디바이스를 리부팅하지 마십시오. 그 대신 Cisco TAC에 문의하십시오.

단계 **8** 업데이트 성공을 확인합니다.

업그레이드가 완료되면 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 업그레이드된 디바이스의 소프트웨어 버전이 정확한지 확인합니다.

단계 **9** Message Center를 사용하여 구축 상태를 다시 확인합니다.

단계 **10** 침입 규칙 및 취약점 데이터베이스(VDB)를 업데이트합니다.

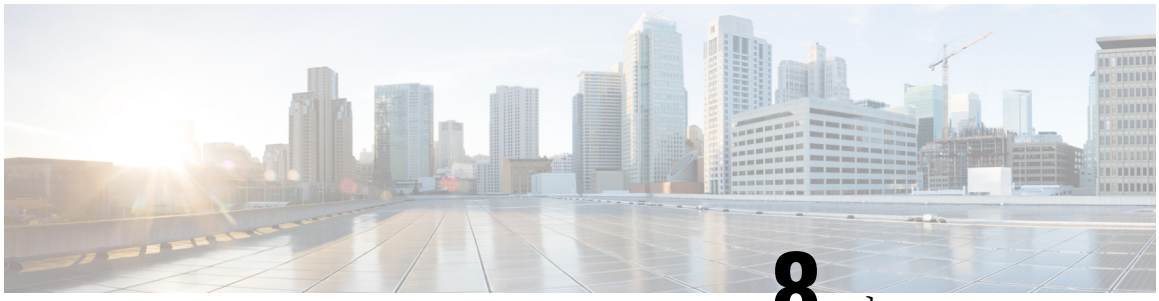
지원 사이트에서 제공되는 침입 규칙 업데이트 또는 VDB가 현재 실행 중인 버전보다 최신 상태이면 최신 버전을 설치합니다. 자세한 내용은 Firepower Management Center 컨피그레이션 가이드을 참조하십시오. 침입 규칙을 업데이트할 때는 정책을 자동으로 다시 적용할 필요가 없습니다. 정책은 나중에 다시 적용합니다.

단계 **11** 릴리스 노트에 설명되어 있는 업그레이드 후 컨피그레이션 변경을 완료합니다.

단계 **12** 방금 업그레이드한 디바이스에 컨피그레이션을 재구축합니다.

II 부

참조 정보



8 장

Firepower 어플라이언스의 호환성

다음 주제에서는 지원되는 각 Firepower 버전의 Cisco Firepower 소프트웨어 및 하드웨어 호환성(운영 체제 및 호스팅 환경 요구 사항 포함)을 설명합니다.

참고 이 가이드는 업그레이드 프로세스와 관련된 호환성 정보를 제공합니다. 자세한 내용은 *Firepower* 호환성 가이드를 참조하십시오.

Firepower Management Center 및 매니지드 디바이스 버전 호환성

아래 표에는 매니지드 디바이스 버전과의 Firepower Management Center 호환성이 나와 있습니다.

참고 대다수 기능의 사용 가능성은 디바이스에서 실행 중인 Firepower 버전에 따라 달라집니다. Firepower Management Center에서 특정 릴리스를 실행 중이더라도 매니지드 디바이스 역시 해당 릴리스로 업그레이드할 때까지는 구축에서 일부 기능이 지원되지 않을 수 있습니다.

표 ***6: Firepower Management Center*** 및 매니지드 디바이스 버전 호환성

Firepower Management Center 버전	매니지드 디바이스 버전
6.2.3	6.2.3 6.2.2 6.2.1(Firepower 2100만 해당) 6.2.0 6.1.0

Firepower Management Center 버전	매니지드 디바이스 버전
6.2.2	6.2.2 6.2.1(Firepower 2100만 해당) 6.2.0 6.1.0
6.2.1	6.2.1(Firepower 2100만 해당) 6.2.0 6.1.0
6.2.0	6.2.0 6.1.0
6.1.0	6.1.0 6.0.1 6.0.0 5.4.1 5.4.0
6.0.1	6.0.1(첫 번째 Firepower Threat Defense 릴리스) 6.0.0 5.4.1 5.4.0
6.0.0	6.0.0 5.4.1 5.4.0
5.4.1	5.4.1(ASA 5506-X, 5508-X 및 5516-X의 첫 번째 ASA FirePOWER 모듈 릴리스) 5.4.0 5.3.1 5.3.0
5.4.0	5.4.0 5.3.1 5.3.0
5.3.1	5.3.1(첫 번째 ASA FirePOWER 모듈 릴리스) 5.3.0

Firepower Management Center 버전	매니지드 디바이스 버전
5.3.0	5.3.0

모델별 Firepower 호환성

이 섹션의 표에는 모델별로 구성된 Firepower 소프트웨어, 플랫폼 및 운영 체제 간 호환성이 나와 있습니다.

Firepower Management Center: 물리적

Firepower 버전	DC500(EOL) DC1000(EOL) DC3000(EOL)	MC750 MC1500 MC3500	MC2000 MC4000	MC1000 MC2500 MC4500
6.2.3	—	예	예	예
6.2.2.x	—	예	예	예
6.2.1	—	예	예	예
6.2.0.x	—	예	예	예
6.1.x.x	—	예	예	—
6.0.1.x	—	예	예	—
6.0.0.x	—	예	예	—
5.4.1.x	예	예	예	—
5.4 5.4.0만 해당, 5.4.x 디바이스를 관리하려면 5.4.1.x Defense Center 사용	예	예	예	—
5.3.1.x	Yes(예) 5.3.1.4~5.3.1.7 제외	예	—	—
5.3.0.x 5.3.0.4~5.3.0.8 제외	예	예	—	—

Firepower Management Center: 가상

Firepower 버전	VMware vCloud Director	VMware vSphere/VMware ESXi					AWS(Amazon Web Services)	KVM(Kernel-Based Virtual Machine)
	5.1	5.0	5.1	5.5	6.0	6.5	EC2/VPC	KVM
6.2.3	—	—	—	예	예	예	예	예
6.2.2.x	—	—	—	예	예	—	예	예
6.2.1	—	—	—	예	예	—	예	예
6.2.0.x	—	—	—	예	예	—	예	예
6.1.x.x	—	—	—	예	예	—	예	예
6.0.1.x	—	—	예	예	—	—	예	—
6.0.0.x	—	—	예	예	—	—	—	—
5.4.1.x	예	예	예	예	—	—	—	—
5.4 5.4.0만 해당, 5.4.x 디바이스를 관리하려면 5.4.1.x Defense Center 사용	예	예	예	예	—	—	—	—
5.3.1.x	Yes(예) 5.3.1 제외	예	예	—	—	—	—	—
5.3.0.x 5.3.0.4~5.3.0.8 제외	예	예	예	—	—	—	—	—

Firepower Threat Defense 디바이스

다음 표에는 다양한 디바이스 플랫폼과의 Firepower Threat Defense 호환성이 나와 있습니다. 또한 일부 플랫폼의 FXOS 요구 사항과 가상 구현과 호환 가능한 호스팅 환경도 포함되어 있습니다.

Firepower 2100 Series with Firepower Threat Defense

Firepower 2100 Series 디바이스는 FXOS 운영 체제를 사용합니다. Firepower 소프트웨어를 업그레이드하면 FXOS가 자동으로 업그레이드됩니다.

Firepower 버전	**Firepower 2110** **Firepower 2120** **Firepower 2130** **Firepower 2140**
6.2.3	Yes(예)
6.2.2.x	Yes(예)
6.2.1	Yes(예)

Firepower 4100/9300 섀시 with Firepower Threat Defense

Firepower 소프트웨어를 실행하는 Firepower 4100/9300 섀시는 FXOS 운영 체제를 사용합니다. FXOS는 Firepower 소프트웨어와 별도로 업그레이드해야 합니다.

굵게 표시된 FXOS 버전은 Firepower 버전의 컴패니언 릴리스입니다. 지정된 Firepower 버전을 실행하려면 굵게 표시된 FXOS 버전을 사용하십시오. 업그레이드 상황에서만 최신 버전 FXOS와 이전 버전 Firepower를 함께 사용해야 합니다.

Firepower 버전	**Firepower 9300**	**Firepower 4110** **Firepower 4120** **Firepower 4140**	**Firepower 4150**
6.2.3	**2.3.1.73** 이상	**2.3.1.73** 이상	**2.3.1.73** 이상
6.2.2.x	**2.2.2.x** 2.3.1.73 이상	**2.2.2.x** 2.3.1.73 이상	**2.2.2.x** 2.3.1.73 이상
6.2.1	—	—	—
6.2.0.x	**2.1.1.x** **2.2.1.x** **2.2.2.x** 2.3.1.73 이상	**2.1.1.x** **2.2.1.x** **2.2.2.x** 2.3.1.73 이상	**2.1.1.x** **2.2.1.x** **2.2.2.x** 2.3.1.73 이상
6.1.x.x	**2.0.1.x** 2.1.1.x 2.3.1.73 이상	**2.0.1.x** 2.1.1.x 2.3.1.73 이상	**2.0.1.x** 2.1.1.x 2.3.1.73 이상
6.0.1.x	**1.1.4.x** 2.0.1.x(6.0.1.1 제외)	**1.1.4.x** 2.0.1.x(6.0.1.1 제외)	—

ASA 5500-X Series with Firepower Threat Defense

Firepower 버전	ASA 5506-X ASA 5506H-X ASA 5506W-X ASA 5508-X ASA 5516-X	ASA 5512-X ASA 5515-X ASA 5525-X ASA 5545-X ASA 5555-X
6.2.3	예	예
6.2.2.x	예	예
6.2.1	—	—
6.2.0.x	예	예
6.1.x.x	예	예
6.0.1.x	예	예

ISA 3000 with Firepower Threat Defense

Firepower 버전	ISA 3000
6.2.3	Yes(예)

Firepower Threat Defense Virtual

Firepower 버전	VMware vSphere/VMware ESXi				AWS(Amazon Web Services)	KVM(Kernel-Based Virtual Machine)	Microsoft Azure
	5.1	5.5	6.0	6.5	EC2/VPC	KVM	Std. D3, D3_v2
6.2.3	—	예	예	예	예	예	예
6.2.2.x	—	예	예	—	예	예	예
6.2.1	—	—	—	—	—	—	—
6.2.0.x	—	예	예	—	예	예	예
6.1.x.x	—	예	예	—	예	예	—
6.0.1.x	예	예	—	—	예	—	—

ASA with FirePOWER Services 디바이스

ASA FirePOWER 모듈은 ASA 운영 체제에서 실행됩니다.

ASA with FirePOWER Services 디바이스의 경우에는 ASA를 ASA FirePOWER 모듈과 별도로 업그레이드해야 하며, 모듈을 업그레이드하기 전에 업그레이드하는 것이 좋습니다.

ASA 5500-X Series with ASA FirePOWER

참고 CSCuc91730으로 인해 ASA 9.2(4.5) 이상, 9.3(3.8) 이상 또는 9.4(2) 이상으로 업그레이드하는 것이 좋습니다.

표 *7: ASA 5500-X Series with ASA FirePOWER Versions 6.x*

Firepower 버전	**ASA 5506-X** **ASA 5506H-X** **ASA 5506W-X** **ASA 5508-X** **ASA 5516-X**	**ASA 5512-X** **ASA 5515-X** **ASA 5525-X** **ASA 5545-X** **ASA 5555-X**	**ASA 5585-X**	**ASDM Management**
6.2.3	9.5(2), 9.5(3) - 5506 모델 제외 9.6(x) 9.7(x) 9.8(x) 9.9(x)			7.9(2)
6.2.2.x	9.5(2), 9.5(3) - 5506 모델 제외 9.6(x) 9.7(x) 9.8(x) 9.9(x)			7.8(2) 이상
6.2.1	—			—
6.2.0.x	9.5(2), 9.5(3) - 5506 모델 제외 9.6(x) 9.7(x) 9.8(x) 9.9(x)			7.7(1) 이상

Firepower 버전	ASA 5506-X ASA 5506H-X ASA 5506W-X ASA 5508-X ASA 5516-X	ASA 5512-X ASA 5515-X ASA 5525-X ASA 5545-X ASA 5555-X	ASA 5585-X	ASDM Management
6.1.x.x	9.5(2), 9.5(3) - 5506 모델 제외 9.6(x) 9.7(x) 9.8(x) 9.9(x)			7.6(2) 이상
6.0.1.x	9.4(x) - ASDM 또는 종속 포털 없음 9.5(1.5) - 종속 포털 없음 9.5(2), 9.5(3) 9.6(x)			7.6(1) 이상
6.0.0.x	9.4(x) - ASDM 또는 종속 포털 없음 9.5(1.5) - 종속 포털 없음 9.5(2), 9.5(3) 9.6(x)			7.5(1.112) 이상

표 *8: ASA 5500-X Series with ASA FirePOWER Versions 5.x*

Firepower 버전	ASA 5506-X ASA 5506H-X ASA 5506W-X ASA 5508-X ASA 5516-X	ASA 5512-X ASA 5515-X ASA 5525-X ASA 5545-X ASA 5555-X	ASA 5585-X	ASDM Management
5.4.1.x	9.3(2), 9.3(3) - 5506 모델만 해당 9.4(x) 9.5(1.5), 9.5(2), 9.5(3) 9.6(x) 9.7(x) 9.8(x) 9.9(x)	—		7.3(3) 이상 - 5506 모델만 해당 7.4(1) 이상

Firepower 버전	**ASA 5506-X** **ASA 5506H-X** **ASA 5506W-X** **ASA 5508-X** **ASA 5516-X**	**ASA 5512-X** **ASA 5515-X** **ASA 5525-X** **ASA 5545-X** **ASA 5555-X**	**ASA 5585-X**	**ASDM Management**
5.4.0.x	—	9.2(2.4), 9.2(3), 9.2(4) - 버전 5.4.0만 해당 9.3(2), 9.3(3) 9.4(x) 9.5(1.5), 9.5(2), 9.5(3) 9.6(x) 9.7(x) 9.8(x) 9.9(x)		—
5.3.1.x	—	9.2(2.4), 9.2(3), 9.2(4)		—

ISA 3000 with ASA FirePOWER

Firepower 버전	**ASA OS**	**ASDM Management**
5.4.1.7 이상 5.4.1.x 시퀀스만 해당	9.4(1.225) 9.5(2), 9.5(3) 9.6(x)	7.5(1.112) 이상

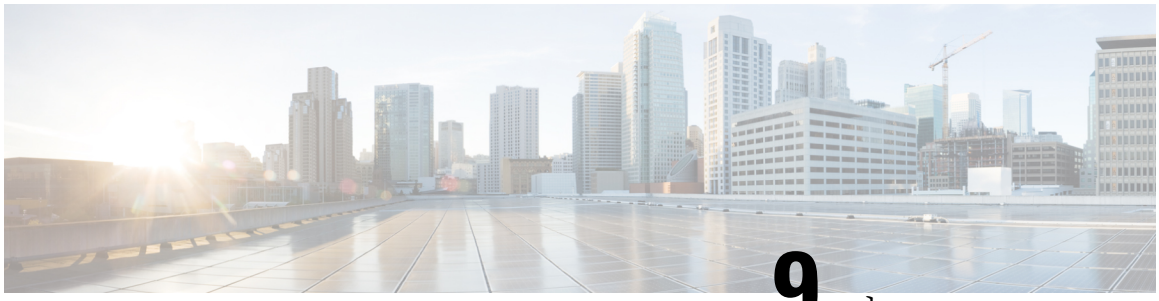
7000/8000 Series 및 레거시 디바이스

Firepower 버전	**7000** 및 **8000 Series(AMP** 포함**)**	**Series 2**
6.2.3	예	—
6.2.2.x	예	—
6.2.1	—	—
6.2.0.x	예	—
6.1.x.x	예	—
6.0.x.x	예	—

Firepower 버전	7000 및 8000 Series(AMP 포함)	Series 2
5.4.0.x	예	예
5.3.0.x	Yes(예) 3D7050, AMP 8150, AMP 8350 제외	Yes(예)

NGIPSv(Virtual Managed Devices)

Firepower 버전	VMware vCloud Director	VMware vSphere/VMware ESXi				
	5.1	5.0	5.1	5.5	6.0	6.5
6.2.3	—	—	—	예	예	예
6.2.2.x	—	—	—	예	예	—
6.2.1	—	—	—	—	—	—
6.2.0.x	—	—	—	예	예	—
6.1.x.x	—	—	—	예	예	—
6.0.1.x	—	—	예	예	—	—
6.0.0.x	—	—	예	예	—	—
5.4.1.x	예	예	예	예	—	—
5.4.0.x	예	예	예	예	—	—
5.3.0.x	예	예	예	—	—	—



9 장

업그레이드 경로

다음 주제에서는 Firepower 어플라이언스에 지원되는 업그레이드 경로와 상세한 예시 업그레이드 경로를 설명합니다. 일반 업그레이드 경로 지침은 업그레이드 경로 계획, 6 페이지를 참조하십시오.

Firepower Management Center 업그레이드 경로

이 표에는 Firepower Management Center의 업그레이드 경로(Firepower Management Center Virtual 포함)가 나와 있습니다. 현재 버전과 대상 버전 사이의 모든 중간 버전으로 업그레이드해야 합니다.

Current Version	업그레이드 경로		
6.2.2	→ 6.2.3		
6.2.1	→ 6.2.2 또는 6.2.3		
6.2.0	→ 6.2.1 또는 6.2.2 또는 6.2.3		
6.1.0	→ 6.2.0 또는 6.2.3		
6.0.1	→ 6.1.0	→ 6.2.0 또는 6.2.3	
6.0.0	→ 6.0.1	→ 6.1.0	→ 6.2.0 또는 6.2.3
5.4.1.1	→ 6.0.0	→ 6.0.1	→ 6.1.0

예: 고가용성 **Firepower Management Center** 업그레이드

고가용성 Firepower Management Center는 한 번에 하나씩 수동으로 업그레이드합니다. (업그레이드 프로세스에서는 고가용성 디바이스에 대해 이 작업을 자동으로 수행합니다.) 동기화가 일시 정지되면 스탠바이 Firepower Management Center를 먼저 업그레이드한 다음 액티브 Management Center를 업그레이드합니다.

Firepower 5.4.x는 Firepower Management Center 고가용성을 지원하지만 버전 6.0에서는 지원이 중단되었습니다. 사용 중인 구축을 버전 5.4.x에서 버전 6.0으로 업그레이드하려면 고가용성 상태를 단순히 일시 정지하는 대신 해제해야 합니다. 버전 6.1에서는 Firepower Management Center 고가용성이 다시 지원됩니다. 고가용성 상태를 재구성한 후에는 후속 업그레이드를 위해 고가용성 상태를 해제할 필요가 없습니다.

이 예시에는 NGIPS 소프트웨어를 실행하는 레거시 디바이스인 Firepower 7000 및 8000 Series 디바이스가 포함되어 있습니다. 이러한 디바이스는 독립형 디바이스, 고가용성 쌍 및 스택으로 구성할 수 있습니다.

구축

어플라이언스	현재	대상
Firepower 7000 및 8000 Series 디바이스: • 독립형 디바이스 • 고가용성 쌍 • 스택	Firepower 5.4.0.x(여러 버전)	Firepower 6.2.3
Firepower Management Center 고가용성 쌍: • A(액티브) • B(스탠바이)	Firepower 5.4.1.x	Firepower 6.2.3

업그레이드 경로

단계	작업	어플라이언스	세부 사항
1	버전 6.0 사전 설치 패키지 설치	Firepower 디바이스	5.4.0.2~5.4.0.6의 경우 필수, 이후 버전의 경우 권장.
2	A(액티브)에 등록된 디바이스는 모두 유지하면서 고가용성 상태 해제	Firepower Management Center 쌍	6.0에서는 고가용성 지원이 중단됨.
3	버전 6.0 사전 설치 패키지 설치	Firepower Management Center B	5.4.1.1~5.4.1.5의 경우 필수, 이후 버전의 경우 권장.

단계	작업	어플라이언스	세부 사항
4	버전 6.0 사전 설치 패키지 설치	Firepower Management Center A	5.4.1.1~5.4.1.5의 경우 필수, 이후 버전의 경우 권장.
5	업그레이드	Firepower Management Center B	Firepower 5.4.1.x → 6.0
6	업그레이드	Firepower Management Center A	Firepower 5.4.1.x → 6.0
7	업그레이드	Firepower 디바이스 같은 패키지를 사용하여 함께 업그레이드합니다.	Firepower 5.4.0.x → 6.0
8	업그레이드	Firepower Management Center B	Firepower 6.0 → 6.1
9	업그레이드	Firepower Management Center A	Firepower 6.0 → 6.1
10	A를 다시 액티브로, B를 스탠바이로 구성하여 고가용성 재구성	Firepower Management Center 쌍	6.1에서는 고가용성이 다시 지원됨.
11	업그레이드	Firepower 디바이스 같은 패키지를 사용하여 함께 업그레이드합니다.	Firepower 6.0 → 6.1
12	동기화 일시 정지	Firepower Management Center A	스플릿 브레인을 입력함.
13	업그레이드	Firepower Management Center B	Firepower 6.1 → 6.2.3
14	업그레이드	Firepower Management Center A	Firepower 6.1 → 6.2.3
15	동기화 재시작	Firepower Management Center A	스플릿 브레인을 종료함.
16	업그레이드	Firepower 디바이스	Firepower 6.1 → 6.2.3

Firepower Threat Defense 업그레이드 경로 - Firepower Management Center 포함

이 표에는 Firepower Management Center를 통해 관리되는 Firepower Threat Defense 디바이스의 업그레이드 경로가 나와 있습니다. 현재 버전과 대상 버전 사이의 모든 중간 버전으로 업그레이드해야 합니다.

Current Version	업그레이드 경로	
6.2.2	→ 6.2.3	
6.2.1(Firepower 2100 Series만 해당)	→ 6.2.2 또는 6.2.3	
6.2.0	→ 6.2.2 또는 6.2.3	
6.1.0	→ 6.2.0 또는 6.2.3	
6.0.1	→ 6.1.0	→ 6.2.0 또는 6.2.3

FXOS 포함 업그레이드 순서(Firepower 4100/9300 섀시)

Firepower 4100/9300 섀시가 사용하는 FXOS 운영 체제는 Firepower 소프트웨어와는 별도로 업그레이드합니다. 각 섀시의 FXOS를 독립적으로 업그레이드합니다.

Firepower Threat Defense 구축	업그레이드 순서
독립형 섀시 내 클러스터(Firepower 9300에만 해당)	**1.** FXOS 업그레이드 **2.** Firepower 소프트웨어를 업그레이드합니다.
고가용성 쌍	항상 스탠바이 유닛을 업그레이드합니다. **1.** 스탠바이 유닛의 FXOS를 업그레이드합니다. **2.** 역할을 전환합니다. **3.** 새 스탠바이 유닛의 FXOS를 업그레이드합니다. **4.** 고가용성 쌍의 Firepower 소프트웨어를 업그레이드합니다.

Firepower Threat Defense 구축	업그레이드 순서
섀시 간 클러스터(6.2 이상)	항상 전체 슬레이브 섀시를 업그레이드합니다. 예를 들어 섀시가 2개인 클러스터는 다음과 같이 업그레이드합니다. **1.** 전체 슬레이브 섀시에서 FXOS를 업그레이드합니다. **2.** 마스터 모듈을 방금 업그레이드한 섀시로 전환합니다. **3.** 새 전체 슬레이브 섀시에서 FXOS를 업그레이드합니다. **4.** 클러스터의 Firepower 소프트웨어를 업그레이드합니다.

예: 번들 운영 체제와 함께 **Firepower Threat Defense** 업그레이드

Firepower 6.0.1에는 Firepower Threat Defense가 도입되었습니다. 일부 플랫폼에서는 Firepower 소프트웨어를 업그레이드하면 운영 체제가 자동으로 업그레이드됩니다. 따라서 이러한 작업을 별도로 수행할 필요가 없습니다.

구축

어플라이언스	현재	대상
ASA 5500-X Series with Firepower Threat Defense	Firepower 6.0.1	Firepower 6.2.3
Firepower 2100 Series	Firepower 6.2.1(관리되지 않는 미개봉 상태)	Firepower 6.2.3
ISA 3000 with Firepower Threat Defense	Firepower 6.2.3(관리되지 않는 미개봉 상태)	Firepower 6.2.3
Firepower Management Center	Firepower 6.0.1	Firepower 6.2.3

업그레이드 경로

단계	작업	어플라이언스	세부 사항
1	업그레이드	Firepower Management Center	Firepower 6.0.1 → 6.1
2	업그레이드	ASA 5500-X Series	Firepower 6.0.1 → 6.1
3	업그레이드	Firepower Management Center	Firepower 6.1 → 6.2.3

단계	작업	어플라이언스	세부 사항
4	업그레이드	ASA 5500-X Series	Firepower 6.1 → 6.2.3
5	구축에 추가	Firepower 2100 Series	디바이스를 추가할 수 있는 첫 번째 기회.
6	업그레이드	Firepower 2100 Series	Firepower 6.2.1 → 6.2.3
7	구축에 추가	ISA 3000	디바이스를 추가할 수 있는 첫 번째 기회.

예: Firepower 4100/9300 섀시 업그레이드(섀시 내 클러스터 포함)

Firepower 6.0.1에서는 Firepower 4100/9300 섀시에 Firepower Threat Defense가 도입되었습니다. 각 섀시의 FXOS를 독립적으로 업그레이드합니다.

구축

어플라이언스	현재	대상
보안 모듈 3개가 포함된 Firepower 9300 섀시 내 클러스터	Firepower 6.0.1 FXOS 1.1.4	Firepower 6.2.3 FXOS 2.3.1
Firepower 4100 Series	Firepower 6.0.1 FXOS 1.1.4	Firepower 6.2.3 FXOS 2.3.1
Firepower Management Center	Firepower 6.0.1	Firepower 6.2.3

업그레이드 경로

단계	작업	어플라이언스	세부 사항
1	업그레이드	Firepower Management Center	Firepower 6.0.1 → 6.1
2	FXOS 업그레이드	Firepower 9300	FXOS 1.1.4 → 2.0.1
3	FXOS 업그레이드	Firepower 4100 Series	FXOS 1.1.4 → 2.0.1
4	Firepower 소프트웨어 업그레이드	Firepower 9300 및 4100 Series 같은 패키지를 사용하여 함께 업그레이드합니다.	Firepower 6.0.1 → 6.1
5	업그레이드	Firepower Management Center	Firepower 6.1 → 6.2.3
6	FXOS 업그레이드	Firepower 9300	FXOS 2.0.1 → 2.3.1
7	FXOS 업그레이드	Firepower 4100 Series	FXOS 2.0.1 → 2.3.1

단계	작업	어플라이언스	세부 사항
8	Firepower 소프트웨어 업그레이드	Firepower 9300 및 4100 Series 같은 패키지를 사용하여 함께 업그레이드합니다.	Firepower 6.1 → 6.2.3

예: Firepower 4100/9300 섀시 고가용성 쌍 업그레이드

Firepower 6.0.1에서는 Firepower 4100/9300 섀시에 Firepower Threat Defense가 도입되었습니다. 각 섀시에서 FXOS를 독립적으로 업그레이드하고 항상 스탠바이 유닛을 업그레이드합니다.

구축

어플라이언스	현재	대상
Firepower 4100 Series 고가용성 쌍: • A(액티브) • B(스탠바이)	Firepower 6.0.1 FXOS 1.1.4	Firepower 6.2.3 FXOS 2.3.1
Firepower Management Center	Firepower 6.0.1	Firepower 6.2.3

업그레이드 경로

단계	작업	어플라이언스	세부 사항
1	업그레이드	Firepower Management Center	Firepower 6.0.1 → 6.1
2	FXOS 업그레이드	디바이스 B(스탠바이)	FXOS 1.1.4 → 2.0.1
3	역할 전환	Firepower 4100 Series 고가용성 쌍	항상 스탠바이 유닛을 업그레이드합니다.
4	FXOS 업그레이드	디바이스 A(새 스탠바이)	FXOS 1.1.4 → 2.0.1
5	Firepower 소프트웨어 업그레이드	Firepower 4100 Series 고가용성 쌍	Firepower 6.0.1 → 6.1
6	업그레이드	Firepower Management Center	Firepower 6.1 → 6.2.3
7	FXOS 업그레이드	디바이스 A(스탠바이)	FXOS 2.0.1 → 2.3.1
8	역할 전환	Firepower 4100 Series 가용성 쌍	항상 스탠바이 유닛을 업그레이드합니다.
9	FXOS 업그레이드	디바이스 B(새 스탠바이)	FXOS 2.0.1 → 2.3.1

단계	작업	어플라이언스	세부 사항
10	Firepower 소프트웨어 업그레이드	Firepower 4100 Series 고가용성 쌍	Firepower 6.1 → 6.2.3

예: Firepower Threat Defense 4100/9300 섀시 간 클러스터 업그레이드

Firepower 6.2에는 Firepower 4100/9300 섀시에 Firepower Threat Defense 섀시 간 클러스터링이 도입되었습니다. 각 섀시에서 FXOS를 독립적으로 업그레이드하고 항상 전체 슬레이브 섀시를 업그레이드합니다.

구축

어플라이언스	현재	대상
섀시 2개가 포함된 Firepower 9300 섀시 간 클러스터: • A(모듈 3개, 마스터 포함) • B(모듈 3개, 모두 슬레이브)	Firepower 6.2 FXOS 2.1.1	Firepower 6.2.3 FXOS 2.3.1
Firepower Management Center	Firepower 6.2	Firepower 6.2.3

업그레이드 경로

단계	작업	어플라이언스	세부 사항
1	업그레이드	Firepower Management Center	Firepower 6.2 → 6.2.3
2	FXOS 업그레이드	섀시 B(모두 슬레이브)	FXOS 2.1.1 → 2.3.1
3	마스터 모듈을 섀시 B로 전환	Firepower 9300 섀시 간 클러스터	항상 전체 슬레이브 섀시를 업그레이드합니다.
4	FXOS 업그레이드	섀시 A(마스터 모듈을 섀시 B로 이동했으므로 모두 슬레이브)	FXOS 2.1.1 → 2.3.1
5	Firepower 소프트웨어 업그레이드	Firepower 9300 섀시 간 클러스터	Firepower 6.2 → 6.2.3

Firepower 7000/8000 Series 및 NGIPSv 업그레이드 경로 - Firepower Management Center 포함

이 표에는 Firepower Management Center를 통해 관리되는 7000 Series, 8000 Series 및 NGIPSv 디바이스의 업그레이드 경로가 나와 있습니다. 현재 버전과 대상 버전 사이의 모든 중간 버전으로 업그레이드해야 합니다.

현재 버전	업그레이드 경로		
6.2.2	→ 6.2.3		
6.2.1	이러한 플랫폼에서는 지원되지 않음		
6.2.0	→ 6.2.2 또는 6.2.3		
6.1.0	→ 6.2.0 또는 6.2.3		
6.0.1	→ 6.1.0	→ 6.2.0 또는 6.2.3	
6.0.0	→ 6.0.1	→ 6.1.0	→ 6.2.0 또는 6.2.3
5.4.1.1	→ 6.0.0	→ 6.0.1	→ 6.1.0
5.4.0.2	→ 6.0.0	→ 6.0.1	→ 6.1.0

예: 가상 구축 업그레이드

가상 구축에서는 호스팅 환경이 가상 어플라이언스의 대상 버전과 호환되는지 확인합니다.

구축

어플라이언스	현재	대상
NGIPSv	5.4.x(여러 버전) VMware ESXi 5.0	Firepower 6.2.3 VMware ESXi 6.5
Firepower Management Center Virtual	Firepower 6.0 VMware ESXi 5.5	Firepower 6.2.3 VMware ESXi 6.5

업그레이드 경로

단계	작업	어플라이언스	세부 사항
1	버전 6.0 사전 설치 패키지 설치	NGIPSv(5.4.0.x)	5.4.0.2~5.4.0.6의 경우 필수, 이후 버전의 경우 권장.

단계	작업	어플라이언스	세부 사항
2	버전 6.0 사전 설치 패키지 설치	NGIPSv(5.4.1.x)	5.4.1.1~5.4.1.5의 경우 필수, 이후 버전의 경우 권장.
3	VMware ESXi 업그레이드	NGIPSv	ESXi 5.0 → 5.5
4	Firepower 소프트웨어 업그레이드	NGIPSv	Firepower 5.4.x → 6.0
5	Firepower 소프트웨어 업그레이드	Firepower Management Center Virtual	Firepower 6.0 → 6.1
6	Firepower 소프트웨어 업그레이드	NGIPSv	Firepower 6.0 → 6.1
7	Firepower 소프트웨어 업그레이드	Firepower Management Center Virtual	Firepower 6.1 → 6.2.3
8	VMware ESXi 업그레이드	Firepower Management Center Virtual	ESXi 5.5 → 6.5
9	Firepower 소프트웨어 업그레이드	NGIPSv	Firepower 6.1 → 6.2.3
10	VMware ESXi 업그레이드	NGIPSv	ESXi 5.5 → 6.5

ASA FirePOWER 모듈 업그레이드 경로 - Firepower Management Center 포함

이 표에는 Firepower Management Center를 통해 관리되는 ASA FirePOWER 모듈의 업그레이드 경로가 나와 있습니다. 현재 버전과 대상 버전 사이의 모든 중간 버전으로 업그레이드해야 합니다.

Current Version	업그레이드 경로		
6.2.2	→ 6.2.3		
6.2.1	이 플랫폼에서는 지원되지 않음		
6.2.0	→ 6.2.2 또는 6.2.3		
6.1.0	→ 6.2.0 또는 6.2.3		
6.0.1	→ 6.1.0	→ 6.2.0 또는 6.2.3	
6.0.0	→ 6.0.1	→ 6.1.0	→ 6.2.0 또는 6.2.3

Current Version	업그레이드 경로			
5.4.1	→ 6.0.0	→ 6.0.1	→ 6.1.0	→ 6.2.0 또는 6.2.3
5.4.0.2	→ 6.0.0	→ 6.0.1	→ 6.1.0	→ 6.2.0 또는 6.2.3

ASA 포함 업그레이드 순서

ASA with FirePOWER Services 디바이스가 사용하는 ASA 운영 체제는 Firepower 소프트웨어와는 별도로 업그레이드합니다. ASA 및 ASA FirePOWER 버전은 광범위하게 호환됩니다. 하지만 ASA 업그레이드가 필요하지 않더라도 문제를 해결하려면 지원되는 최신 버전으로 업그레이드해야 할 수 있습니다.

각 섀시의 ASA를 독립적으로 업그레이드합니다. 클러스터형 ASA 디바이스 또는 페일오버 ASA 디바이스의 ASA 및 ASA FirePOWER 모듈을 모두 업그레이드하려는 경우 다음 표에 나와 있는 것처럼 ASA를 업그레이드하면서 ASA FirePOWER 모듈을 한 번에 하나씩 업그레이드합니다.

ASA 구축	업그레이드 순서
독립형	**1.** ASA를 업그레이드합니다. **2.** ASA FirePOWER 모듈을 업그레이드합니다.
페일오버: 액티브/스탠바이	**1.** 스탠바이 유닛의 ASA를 업그레이드합니다. **2.** 스탠바이 유닛의 ASA FirePOWER 모듈을 업그레이드합니다. **3.** 페일오버를 수행합니다. **4.** 새 스탠바이 유닛의 ASA를 업그레이드합니다. **5.** 새 스탠바이 유닛의 ASA FirePOWER 모듈을 업그레이드합니다.
페일오버: 액티브/액티브	**1.** 기본 유닛에서 두 페일오버 그룹을 모두 액티브로 설정합니다. **2.** 보조 유닛의 ASA를 업그레이드합니다. **3.** 보조 유닛의 ASA FirePOWER 모듈을 업그레이드합니다. **4.** 보조 유닛에서 두 페일오버 그룹을 모두 액티브로 설정 **5.** 기본 유닛의 ASA를 업그레이드합니다. **6.** 기본 유닛의 ASA FirePOWER 모듈을 업그레이드합니다.

ASA 구축	업그레이드 순서
클러스터	모든 유닛에서 다음을 수행합니다. **1.** 클러스터에서 유닛을 제거합니다. 슬레이브 유닛을 먼저 업그레이드합니다. 마스터 유닛을 마지막으로 제거할 때 다른 유닛이 마스터로 대신 설정될 때까지 기다렸다가 ASA를 업그레이드합니다. **2.** 제거한 유닛에서 ASA를 업그레이드합니다. **3.** 제거한 유닛에서 ASA FirePOWER 모듈을 업그레이드합니다. **4.** 클러스터에 유닛을 슬레이브 유닛으로 다시 추가합니다.

예: ASA with FirePOWER Services 업그레이드

각 섀시의 ASA를 독립적으로 업그레이드합니다. 클러스터형 ASA 디바이스 또는 페일오버 ASA 디바이스의 ASA 및 ASA FirePOWER 모듈을 모두 업그레이드하려는 경우, ASA를 업그레이드하면서 ASA FirePOWER 모듈을 한 번에 하나씩 업그레이드합니다.

구축

어플라이언스	현재	대상
여러 ASA 5500-X Series 모델에서 실행되는 ASA with FirePOWER Services: • A 및 B(독립형) • C 및 D(액티브/스탠바이 페일오버 쌍) • E 및 F(액티브/액티브 페일오버 쌍) • G, H, I(마스터/슬레이브/슬레이브 클러스터)	Firepower 5.4.x(여러 버전) ASA 9.3(2)	Firepower 6.2.3 ASA 9.9(2)
Firepower Management Center	Firepower 6.0	Firepower 6.2.3

업그레이드 경로

단계	작업	어플라이언스	세부 사항
1	버전 6.0 사전 설치 패키지 설치	ASA FirePOWER 모듈(5.4.0.x)	Firepower 5.4.0.2~5.4.0.6의 경우 필수, 이후 버전의 경우 권장.

단계	작업	어플라이언스	세부 사항
2	버전 6.0 사전 설치 패키지 설치	ASA FirePOWER 모듈(5.4.1.x)	Firepower 5.4.1.1~5.4.1.5의 경우 필수, 이후 버전의 경우 권장.
독립형 디바이스 A 및 B의 ASA 및 ASA FirePOWER 모듈 업그레이드			
3a	ASA 업그레이드	디바이스 A(독립형)	ASA 9.3(2) → 9.9(2)
3b	ASA 업그레이드	디바이스 B(독립형)	ASA 9.3(2) → 9.9(2)
3c	ASA FirePOWER 모듈 업그레이드	디바이스 A 및 디바이스 B 같은 패키지를 사용하여 함께 업그레이드합니다.	Firepower 5.4.x → 6.0
액티브/스탠바이 페일오버 쌍 C 및 D의 ASA 및 ASA FirePOWER 모듈 업그레이드			
4a	ASA 업그레이드	디바이스 D(액티브/스탠바이 쌍의 스탠바이)	ASA 9.3(2) → 9.9(2)
4b	ASA FirePOWER 모듈 업그레이드	디바이스 D	Firepower 5.4.x → 6.0
4c	페일오버	디바이스 C 및 디바이스 D 쌍	항상 스탠바이 유닛을 업그레이드합니다.
4d	ASA 업그레이드	디바이스 C(새 스탠바이)	ASA 9.3(2) → 9.9(2)
4e	ASA FirePOWER 모듈 업그레이드	디바이스 C	Firepower 5.4.x → 6.0
액티브/액티브 페일오버 쌍 E 및 F의 ASA 및 ASA FirePOWER 모듈 업그레이드			
5a	기본 유닛에서 두 페일오버 그룹을 모두 액티브로 설정	디바이스 E(액티브/액티브 쌍의 기본)	
5b	ASA 업그레이드	디바이스 F(액티브/액티브 쌍의 보조)	ASA 9.3(2) → 9.9(2)
5c	ASA FirePOWER 모듈 업그레이드	디바이스 F	ASA 9.3(2) → 9.9(2)
5d	보조 유닛에서 두 페일오버 그룹을 모두 액티브로 설정	디바이스 F	
5e	ASA 업그레이드	디바이스 E	ASA 9.3(2) → 9.9(2)
5f	ASA FirePOWER 모듈 업그레이드	디바이스 E	Firepower 5.4.x → 6.0

단계	작업	어플라이언스	세부 사항
ASA 클러스터 H, G 및 I의 ASA 및 ASA FirePOWER 모듈 업그레이드			
6a	클러스터에서 제거	디바이스 H(슬레이브)	트래픽 중단을 방지합니다.
6b	ASA 업그레이드	디바이스 H	ASA 9.3(2) → 9.9(2)
6c	ASA FirePOWER 모듈 업그레이드	디바이스 H	Firepower 5.4.x → 6.0
6d	클러스터로 돌아가기	디바이스 H	트래픽 처리를 다시 시작합니다.
6e	클러스터에서 제거	디바이스 G(슬레이브)	트래픽 중단을 방지합니다.
6f	ASA 업그레이드	디바이스 G	ASA 9.3(2) → 9.9(2)
6g	ASA FirePOWER 모듈 업그레이드	디바이스 G	Firepower 5.4.x → 6.0
6h	클러스터로 돌아가기	디바이스 G	트래픽 처리를 다시 시작합니다.
6i	클러스터에서 제거	디바이스 G(마스터)	트래픽 중단을 방지합니다.
6j	ASA 업그레이드	디바이스 G	ASA 9.3(2) → 9.9(2)
6k	ASA FirePOWER 모듈 업그레이드	디바이스 G	Firepower 5.4.x → 6.0
6l	클러스터로 돌아가기	디바이스 G	트래픽 처리를 다시 시작합니다. 디바이스 G가 슬레이브 유닛으로 돌아옵니다.
ASA를 업그레이드하지 않고 ASA FirePOWER 모듈 업그레이드.			
7	업그레이드	Firepower Management Center	Firepower 6.0 → 6.0.1
8	ASA FirePOWER 모듈 업그레이드	ASA FirePOWER 모듈 같은 패키지를 사용하여 함께 업그레이드합니다.	Firepower 6.0 → 6.0.1
9	업그레이드	Firepower Management Center	Firepower 6.0.1 → 6.1
10	ASA FirePOWER 모듈 업그레이드	ASA FirePOWER 모듈 같은 패키지를 사용하여 함께 업그레이드합니다.	Firepower 6.0.1 → 6.1
11	업그레이드	Firepower Management Center	Firepower 6.1 → 6.2.3

단계	작업	어플라이언스	세부 사항
12	ASA FirePOWER 모듈 업그레이드	ASA FirePOWER 모듈 같은 패키지를 사용하여 함께 업그레이드합니다.	Firepower 6.1 → 6.2.3

Firepower 버전 6.0 사전 설치 패키지

Cisco에서는 버전 5.4.x에서 버전 6.x로의 업그레이드에 대해 업그레이드를 최적화하는 사전 설치 패키지를 제공합니다.

경우에 따라 다음 표에 나와 있는 사전 설치 패키지를 반드시 사용해야 합니다. 그리고 사전 설치 패키지를 사용할 필요가 없더라도 업그레이드 경로에 버전 6.0 사전 설치 패키지를 포함하고 사용하는 것이 좋습니다.

어플라이언스	업그레이드할최소버전	필요한사전설치패키지	권장 사전 설치 패키지
FireSIGHT Defense Center(Firepower Management Center)	5.4.1.1	5.4.1.1 ~ 5.4.1.5	5.4.1.6 이상
7000/8000 Series 디바이스	5.4.0.2	5.4.0.2 ~ 5.4.0.6	
NGIPSv	5.4.0.2 5.4.1.1	5.4.0.2 ~ 5.4.0.6 5.4.1.1 ~ 5.4.1.5	5.4.1.6 이상 5.4.0.7 이상
ASA FirePOWER 모듈 (5.4.1.x 시퀀스의 모델)	5.4.1	5.4.1 5.4.1.1 ~ 5.4.1.5	5.4.1.6 이상
ASA FirePOWER 모듈 (5.4.0.x 시퀀스의 모델)	5.4.0.2	5.4.0.2 ~ 5.4.0.6	5.4.0.7 이상

10 장

업그레이드 중의 트래픽 흐름, 검사 및 디바이스 동작

Firepower Threat Defense 업그레이드 동작 — Firepower 4100/9300 섀시

이 섹션에서는 Firepower 4100/9300 섀시를 업그레이드할 때의 디바이스 및 트래픽 동작을 설명합니다.

섀시: FXOS 업그레이드

섀시 간 클러스터링 또는 고가용성 쌍이 구성되어 있더라도 각 섀시에서 FXOS를 독립적으로 업그레이드합니다. 업그레이드를 수행하는 방법에 따라 FXOS 업그레이드 중에 디바이스가 트래픽을 처리하는 방법이 결정됩니다.

구축	메서드	트래픽 동작
독립형	—	삭제됨
고가용성	모범 사례: 스탠바이 섀시에서 FXOS를 업데이트하고 액티브 피어를 전환한 다음 새 스탠바이 섀시를 업그레이드합니다.	영향 없음
	스탠바이 섀시 업그레이드가 완료되기 전에 액티브 피어에서 FXOS를 업그레이드합니다.	하나의 피어가 온라인 상태가 될 때까지 삭제됨

구축	메서드	트래픽 동작
섀시 간 클러스터(6.2 이상)	모범 사례: 하나 이상의 모듈이 항상 온라인 상태가 되도록 섀시를 한 번에 하나씩 업그레이드합니다.	영향 없음
	특정 시점에 모든 섀시가 가동 중지되도록 섀시를 동시에 업그레이드합니다.	하나 이상의 모듈이 온라인 상태가 될 때까지 삭제됨
섀시 내 클러스터(Firepower 9300에만 해당)	Fail-to-Wire 활성화됨: 바이패스: 스탠바이 또는 바이패스-강제. (6.1 이상)	검사 없이 통과됨
	Fail-to-Wire 비활성화됨: 바이패스: 비활성화. (6.1 이상)	하나 이상의 모듈이 온라인 상태가 될 때까지 삭제됨
	Fail-to-Wire 모듈 없음.	하나 이상의 모듈이 온라인 상태가 될 때까지 삭제됨

독립형 섀시: **Firepower** 소프트웨어 업그레이드

인터페이스 컨피그레이션에 따라 독립형 디바이스가 업그레이드 중에 트래픽을 처리하는 방법이 결정됩니다.

인터페이스 컨피그레이션		트래픽 동작
방화벽 인터페이스	라우팅 또는 스위칭(EtherChannel, 이중화, 하위 인터페이스 포함) (스위칭 인터페이스는 브리지 그룹 또는 Transparent 인터페이스라고도 함)	삭제됨
IPS 전용 인터페이스	인라인 집합, Fail-to-Wire 활성화됨: 바이패스: 스탠바이 또는 바이패스-강제. (6.1 이상)	다음 중 하나에 해당합니다. • 검사 없이 통과됨(6.2.3 이상) • 삭제됨(6.1~6.2.2.x)
	인라인 집합, Fail-to-Wire 비활성화됨: 바이패스: 비활성화. (6.1 이상)	삭제됨
	인라인 집합, Fail-to-Wire 모듈 없음	삭제됨
	인라인 집합, 탭 모드	즉시 패킷 이그레스, 복사 검사되지 않음
	패시브, ERSPAN 패시브	중단되지 않음, 검사되지 않음

고가용성 쌍: Firepower 소프트웨어 업그레이드

고가용성 쌍의 디바이스에서 Firepower 소프트웨어를 업그레이드하는 동안 트래픽 흐름 또는 검사가 중단되어서는 안 됩니다. 운영의 연속성을 보장하기 위해 이러한 디바이스는 한 번에 하나씩 업그레이드됩니다. 디바이스는 업그레이드 중에 유지 보수 모드로 작동합니다.

스탠바이 디바이스가 먼저 업그레이드됩니다. 디바이스에서 역할을 전환한 후 새 스탠바이 피어가 업그레이드됩니다. 업그레이드가 완료되어도 디바이스 역할은 전환된 상태로 유지됩니다. 액티브/스탠바이 역할을 유지하려면 업그레이드 전에 역할을 수동으로 전환하십시오. 이렇게 하면 업그레이드 프로세스에서 역할을 다시 전환합니다.

클러스터: Firepower 소프트웨어 업그레이드

Firepower Threat Defense 클러스터의 디바이스에서 Firepower 소프트웨어를 업그레이드하는 동안 트래픽 흐름 또는 검사가 중단되어서는 안 됩니다. 운영의 연속성을 보장하기 위해 이러한 디바이스는 한 번에 하나씩 업그레이드됩니다. 디바이스는 업그레이드 중에 유지 보수 모드로 작동합니다.

하나 이상의 슬레이브 보안 모듈이 먼저 업그레이드된 후에 마스터가 업그레이드됩니다. 보안 모듈은 업그레이드 중에 유지 보수 모드로 작동합니다.

마스터 보안 모듈이 업그레이드되는 동안에는 트래픽 검사 및 처리가 정상적으로 계속되지만, 시스템에서는 이벤트 로깅이 중지됩니다. 로깅 다운타임 중에 처리되는 트래픽에 대한 이벤트는 업그레이드가 완료된 후 동기화되지 않은 타임스탬프와 함께 표시됩니다. 그러나 로깅 다운타임이 길면 시스템은 가장 오래된 이벤트를 로깅하기 전에 정리할 수 있습니다.

구축 중의 트래픽 동작

업그레이드 프로세스 중에는 컨피그레이션을 여러 번 구축합니다. Snort 프로세스는 일반적으로 업그레이드 직후 첫 번째 구축 중에 재시작됩니다. 구축하기 전에 특정 정책 또는 디바이스 컨피그레이션을 수정하는 경우가 아니면 다른 구축 중에는 프로세스가 재시작되지 않습니다. 자세한 내용은 Firepower Management Center 컨피그레이션 가이드의 구축 또는 활성화 시 *Snort* 프로세스를 재시작하는 컨피그레이션을 참조하십시오.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 Snort 프로세스를 재시작하면 Firepower Threat Defense 독립형 디바이스, 고가용성 쌍 및 클러스터에서 트래픽 검사가 중단됩니다. 인터페이스 컨피그레이션에 따라 중단되는 동안 트래픽이 삭제되는지 아니면 검사 없이 통과되는지가 결정됩니다.

인터페이스 컨피그레이션		트래픽 동작
방화벽 인터페이스	라우팅 또는 스위칭(EtherChannel, 이중화, 하위 인터페이스 포함) (스위칭 인터페이스는 브리지 그룹 또는 Transparent 인터페이스라고도 함)	삭제됨

인터페이스 컨피그레이션		트래픽 동작
IPS 전용 인터페이스	인라인 집합, **Failsafe** 활성화 또는 비활성화됨(6.0.1~6.1.0.x)	검사 없이 통과됨 **Failsafe**가 비활성화되어 있고 Snort가 중단되지는 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음
	인라인 집합, **Snort Fail Open:** 중단: 비활성화됨(6.2 이상)	삭제됨
	인라인 집합, **Snort Fail Open:** 중단: 활성화됨(6.2 이상)	검사 없이 통과됨
	인라인 집합, 탭 모드	즉시 패킷 이그레스, 복사 검사되지 않음
	패시브, ERSPAN 패시브	중단되지 않음, 검사되지 않음

Firepower Threat Defense 업그레이드 동작

이 섹션에서는 Firepower 2100 Series, ASA 5500-X Series, ISA 3000 및 Firepower Threat Defense Virtual 디바이스를 업그레이드할 때의 디바이스 및 트래픽 동작을 설명합니다.

독립형 디바이스**: Firepower** 소프트웨어 업그레이드

인터페이스 컨피그레이션에 따라 독립형 디바이스가 업그레이드 중에 트래픽을 처리하는 방법이 결정됩니다.

인터페이스 컨피그레이션		트래픽 동작
방화벽 인터페이스	라우팅 또는 스위칭 (EtherChannel, 이중화, 하위 인터페이스 포함) (스위칭 인터페이스는 브리지 그룹 또는 Transparent 인터페이스라고도 함)	삭제됨
IPS 전용 인터페이스	인라인 집합	삭제됨
	인라인 집합, 탭 모드	즉시 패킷 이그레스, 복사 검사되지 않음
	패시브, ERSPAN 패시브	중단되지 않음, 검사되지 않음

고가용성 쌍: Firepower 소프트웨어 업그레이드

고가용성 쌍의 디바이스에서 Firepower 소프트웨어를 업그레이드하는 동안 트래픽 흐름 또는 검사가 중단되어서는 안 됩니다. 운영의 연속성을 보장하기 위해 이러한 디바이스는 한 번에 하나씩 업그레이드됩니다. 디바이스는 업그레이드 중에 유지 보수 모드로 작동합니다.

스탠바이 디바이스가 먼저 업그레이드됩니다. 디바이스에서 역할을 전환한 후 새 스탠바이 피어가 업그레이드됩니다. 업그레이드가 완료되어도 디바이스 역할은 전환된 상태로 유지됩니다. 액티브/스탠바이 역할을 유지하려면 업그레이드 전에 역할을 수동으로 전환하십시오. 이렇게 하면 업그레이드 프로세스에서 역할을 다시 전환합니다.

구축 중의 트래픽 동작

업그레이드 프로세스 중에는 컨피그레이션을 여러 번 구축합니다. Snort 프로세스는 일반적으로 업그레이드 직후 첫 번째 구축 중에 재시작됩니다. 구축하기 전에 특정 정책 또는 디바이스 컨피그레이션을 수정하는 경우가 아니면 다른 구축 중에는 프로세스가 재시작되지 않습니다. 자세한 내용은 Firepower Management Center 컨피그레이션 가이드의 구축 또는 활성화 시 *Snort* 프로세스를 재시작하는 컨피그레이션을 참조하십시오.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 Snort 프로세스를 재시작하면 Firepower Threat Defense 독립형 디바이스 및 고가용성 쌍에서 트래픽 검사가 중단됩니다. 인터페이스 컨피그레이션에 따라 중단되는 동안 트래픽이 삭제되는지 아니면 검사 없이 통과되는지가 결정됩니다.

인터페이스 컨피그레이션		트래픽 동작
방화벽 인터페이스	라우팅 또는 스위칭 (EtherChannel, 이중화, 하위 인터페이스 포함) (스위칭 인터페이스는 브리지 그룹 또는 Transparent 인터페이스라고도 함)	삭제됨
IPS 전용 인터페이스	인라인 집합, **Failsafe** 활성화 또는 비활성화됨(6.0.1~6.1.0.x)	검사 없이 통과됨 **Failsafe**가 비활성화되어 있고 Snort가 중단되지는 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음
	인라인 집합, **Snort Fail Open:** 중단: 비활성화됨(6.2 이상)	삭제됨
	인라인 집합, **Snort Fail Open:** 중단: 활성화됨(6.2 이상)	검사 없이 통과됨
	인라인 집합, 탭 모드	즉시 패킷 이그레스, 복사 검사되지 않음
	패시브, ERSPAN 패시브	중단되지 않음, 검사되지 않음

Firepower 7000/8000 Series 업그레이드 동작

다음 섹션에서는 Firepower 7000 및 8000 Series 디바이스를 업그레이드할 때의 디바이스 및 트래픽 동작을 설명합니다.

독립형 디바이스: Firepower 소프트웨어 업그레이드

인터페이스 컨피그레이션에 따라 업그레이드 중에 독립형 디바이스가 트래픽을 처리하는 방법이 결정됩니다.

인터페이스 컨피그레이션	트래픽 동작
인라인, 하드웨어 바이패스 활성화됨(바이패스 모드: 바이패스))	검사 없이 통과됨. 단, 다음의 두 시점에서 트래픽이 잠시 중단됨. • 업그레이드 프로세스 시작 시 링크가 끊겼다 연결되었다 하고 네트워크 카드가 하드웨어 바이패스로 전환될 때. • 업그레이드 완료 후 링크가 끊겼다 연결되었다 하고 네트워크 카드가 바이패스에서 전환될 때. 엔드포인트가 다시 연결되고 디바이스 인터페이스와의 링크가 다시 설정되면 검사가 다시 시작됨.
인라인, 하드웨어 바이패스 모듈 없음 또는 하드웨어 바이패스 비활성화됨(바이패스모드: 바이패스 없음))	삭제됨
인라인, 탭 모드	즉시 패킷 이그레스, 복사 검사되지 않음
수동	중단되지 않음, 검사되지 않음
라우팅, 스위칭	삭제됨

고가용성 쌍: Firepower 소프트웨어 업그레이드

고가용성 쌍의 디바이스 또는 디바이스 스택을 업그레이드하는 동안 트래픽 흐름 또는 검사가 중단되어서는 안 됩니다. 운영의 연속성을 보장하기 위해 이러한 디바이스는 한 번에 하나씩 업그레이드됩니다. 디바이스는 업그레이드 중에 유지 보수 모드로 작동합니다.

먼저 업그레이드되는 피어는 구축에 따라 달라집니다.

- 라우팅 또는 스위칭 - 스탠바이 피어가 먼저 업그레이드됩니다. 디바이스에서 역할을 전환한 후 새 스탠바이 피어가 업그레이드됩니다. 업그레이드가 완료되어도 디바이스 역할은 전환된 상태로 유지됩니다. 액티브/스탠바이 역할을 유지하려면 업그레이드 전에 역할을 수동으로 전환하십시오. 이렇게 하면 업그레이드 프로세스에서 역할을 다시 전환합니다.
- 액세스 컨트롤만 해당 - 액티브 피어가 먼저 업그레이드됩니다. 업그레이드가 완료되면 액티브 및 스탠바이 피어의 이전 역할이 유지됩니다.

8000 Series 스택: Firepower 소프트웨어 업그레이드

8000 Series 스택에서는 디바이스가 동시에 업그레이드됩니다. 기본 디바이스에서 업그레이드를 완료하고 스택의 작동이 다시 시작될 때까지는 스택이 독립형 디바이스인 것처럼 트래픽이 동작합니다. 모든 디바이스가 업그레이드를 완료할 때까지 스택은 제한된 혼합 버전 상태로 작동합니다.

구축 중의 트래픽 동작

업그레이드 프로세스 중에는 컨피그레이션을 여러 번 구축합니다. Snort 프로세스는 일반적으로 업그레이드 직후 첫 번째 구축 중에 재시작됩니다. 구축하기 전에 특정 정책 또는 디바이스 컨피그레이션을 수정하는 경우가 아니면 다른 구축 중에는 프로세스가 재시작되지 않습니다. 자세한 내용은 Firepower Management Center 컨피그레이션 가이드의 구축 또는 활성화 시 *Snort* 프로세스를 재시작하는 컨피그레이션을 참조하십시오.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 Snort 프로세스를 재시작하면 Firepower 독립형 디바이스, 고가용성 쌍 및 8000 Series 스택에서 트래픽 검사가 중단됩니다. 인터페이스 컨피그레이션에 따라 중단되는 동안 트래픽이 삭제되는지 아니면 검사 없이 통과되는지가 결정됩니다.

인터페이스 컨피그레이션	재시작 트래픽 동작
인라인, **Failsafe** 활성화 또는 비활성화	검사 없이 통과됨 **Failsafe**가 비활성화되어 있고 Snort가 중단되지는 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음
인라인, 탭 모드	즉시 패킷 이그레스, 복사 시 Snort 우회
수동	중단되지 않음, 검사되지 않음
라우팅, 스위칭	삭제됨

ASA FirePOWER 업그레이드 동작

ASA FirePOWER 모듈로 트래픽을 리디렉션하는 것에 대한 ASA 서비스 정책에 따라 Snort 프로세스를 재시작하는 특정 컨피그레이션을 구축할 때를 포함하여 Firepower 소프트웨어 업그레이드 중에 모듈이 트래픽을 처리하는 방법이 결정됩니다.

트래픽 리디렉션 정책	트래픽 동작
Fail open(**sfr fail-open**)	검사 없이 통과됨
Fail closed(**sfr fail-close**)	삭제됨
모니터링 전용(**sfr {fail-close}|{fail-open} monitor-only**)	즉시 패킷 이그레스, 복사 검사되지 않음

구축 중의 트래픽 동작

Snort 프로세스가 재시작되는 동안의 트래픽 동작은 ASA FirePOWER 모듈을 업그레이드할 때와 동일합니다. 업그레이드 프로세스 중에는 컨피그레이션을 여러 번 구축합니다. Snort 프로세스는 일반적으로 업그레이드 직후 첫 번째 구축 중에 재시작됩니다. 구축하기 전에 특정 정책 또는 디바이스 컨피그레이션을 수정하는 경우가 아니면 다른 구축 중에는 프로세스가 재시작되지 않습니다.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 Snort 프로세스를 재시작하면 트래픽 검사가 중단됩니다. 서비스 정책에 따라 중단되는 동안 트래픽이 삭제되는지 아니면 검사 없이 통과되는지가 결정됩니다.

NGIPSv 업그레이드 동작

인터페이스 컨피그레이션에 따라 Firepower 소프트웨어 업그레이드 중에 NGIPSv가 트래픽을 처리하는 방법이 결정됩니다.

인터페이스 컨피그레이션	트래픽 동작
인라인	삭제됨
인라인, 탭 모드	즉시 패킷 이그레스, 복사 검사되지 않음
수동	중단되지 않음, 검사되지 않음

구축 중의 트래픽 동작

업그레이드 프로세스 중에는 컨피그레이션을 여러 번 구축합니다. Snort 프로세스는 일반적으로 업그레이드 직후 첫 번째 구축 중에 재시작됩니다. 구축하기 전에 특정 정책 또는 디바이스 컨피그레이션을 수정하는 경우가 아니면 다른 구축 중에는 프로세스가 재시작되지 않습니다. 자세한 내용은 Firepower Management Center 컨피그레이션 가이드의 구축 또는 활성화 시 *Snort* 프로세스를 재시작하는 컨피그레이션을 참조하십시오.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 Snort 프로세스를 재시작하면 트래픽 검사가 중단됩니다. 인터페이스 컨피그레이션에 따라 중단되는 동안 트래픽이 삭제되는지 아니면 검사 없이 통과되는지가 결정됩니다.

인터페이스 컨피그레이션	재시작 트래픽 동작
인라인, **Failsafe** 활성화 또는 비활성화	검사 없이 통과됨 **Failsafe**가 비활성화되어 있고 Snort가 중단되지는 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음
인라인, 탭 모드	즉시 패킷 이그레스, 복사 시 Snort 우회
수동	중단되지 않음, 검사되지 않음

11 장

Firepower 소프트웨어 업그레이드 버전별 지침

다음 주제에서는 Firepower 소프트웨어 업그레이드를 위한 중요 정보 및 릴리스별 정보를 설명합니다. 예를 들어 업그레이드 전이나 후에 컨피그레이션을 변경하거나 일부 디바이스에 라이선싱을 다시 적용해야 할 수 있습니다.

여러 버전에 영향을 미치는 지침

Firepower Threat Defense 클러스터**(6.1.x):** 업그레이드 전에 사이트 **ID** 제거

유효한 경우**:** Firepower 6.1.x에서 Firepower 6.2.3 이상으로 업그레이드

버전 **6.2.3** 지침

업그레이드 중 및 후에 **Cisco**와 데이터 공유

버전 6.2.3의 새로운 기능에는 Cisco와의 데이터 공유가 포함됩니다.

Cisco Network Participation 및 *Cisco Success Network*는 사용자에게 기술 지원을 제공하는 데 필요한 사용 정보와 통계를 Cisco로 전송합니다. 업그레이드 중에 이러한 프로그램 참여를 수락하거나 거부할 수 있습니다. 또한 언제든지 이러한 참여를 옵트인하거나 옵트아웃할 수도 있습니다.

웹 분석 추적은 개인 식별 사용 데이터 외의 데이터를 Cisco로 전송합니다. 이러한 데이터에는 확인한 페이지, 특정 페이지를 사용한 시간, 브라우저 버전, 제품 버전, 사용자 위치, Firepower Management Center의 관리 IP 주소 또는 호스트 이름 등이 포함되나 이에 국한되지 않습니다.

참고 업그레이드 프로세스 중에는 웹 분석 참여를 옵트아웃할 수 없습니다. 업그레이드 후에 웹 분석을 비활성화하거나 업그레이드를 설치하지 않을 수 있습니다.

업그레이드 후 액세스 컨트롤 정책 수정/다시 저장

침입 정책 변수 집합에서만 사용되는 네트워크 또는 포트 개체를 구성한 경우, 업그레이드 후 관련 액세스 컨트롤 정책 구축에 실패합니다. 이러한 현상이 발생하면 액세스 컨트롤 정책을 수정하고 변경을 적용한 후(예: 설명 수정), 정책을 저장하고 재구축합니다.

보고서의 결과 제한 변경

버전 6.2.3에서는 보고서 섹션에서 사용하거나 포함할 수 있는 결과 수가 다음과 같이 제한됩니다. 테이블 보기와 세부 정보 보기의 경우에는 HTML/CSV 보고서보다 PDF 보고서에 포함할 수 있는 레코드 수가 더 적습니다.

보고서 섹션 유형	최대 레코드 수: **HTML/CSV** 보고서 섹션	최대 레코드 수: **PDF** 보고서 섹션
막대 그래프 원형 차트	100개(상단 또는 하단)	100개(상단 또는 하단)
테이블 보기	400,000	100,000
세부 정보 보기	1,000	500

Firepower Management Center를 업그레이드하기 전에 보고서 템플릿의 한 섹션에 HTML/CSV의 최대값보다 더 많은 결과 수를 지정하는 경우, 업그레이드 프로세스에서 해당 설정을 새로운 최대값으로 낮춥니다.

PDF 보고서를 생성하는 보고서 템플릿의 경우, 임의의 템플릿 섹션에서 PDF 제한이 초과되면 업그레이드 프로세스에서 출력 형식을 HTML로 변경합니다. PDF를 계속 생성하려면 결과 제한을 PDF 최대값으로 낮춥니다. 업그레이드 후에 이 작업을 수행하는 경우에는 출력 형식을 PDF로 다시 설정합니다.

버전 **6.2.2** 지침

8000 Series 디바이스에서 **CC(Common Criteria)** 또는 **UCAPL** 모드 비활성화

버전 6.2.2를 실행 중인 8000 Series 디바이스에서는 CC(Common Criteria) 또는 UCAPL 모드를 활성화하지 않는 것이 좋습니다. 센서에서 CC 모드 또는 UCAPL 모드를 활성화하면 8000 Series 디바이스에서 FSIC(File System Integrity Check)에 실패할 수 있으며 디바이스가 응답하지 않을 수 있습니다. CC 또는 UCAPL 모드를 활성화한 후 디바이스가 응답하지 않으면 디바이스를 베이스라이닝하여 작동

하도록 만들어야 합니다. CC 모드 또는 UCAPL을 활성화해야 하는 경우 8000 Series 디바이스를 버전 6.2.2.1로 업데이트한 후에 CC 모드 또는 UCAPL 모드를 활성화합니다.

버전 6.2.0 지침

상관관계 정책의 업데이트 전 수정

상관관계 정책을 구성했던 Firepower Management Center를 업데이트하는 경우에는 아래에 나열된 규칙 수정을 진행합니다. Firepower Management Center를 업데이트하지 않고 이미지를 재설치하는 경우 또는 상관관계 정책을 구성하지 않은 경우에는 아래에 나열된 규칙 수정을 진행하지 않아도 됩니다.

버전 6.2.0은 더 이상 중첩 상관관계 규칙을 지원하지 않습니다. 이전 릴리스에서는 여러 규칙이 기본 이벤트 유형을 공유하는 경우 특정 상관관계 규칙을 다른 상관관계 규칙의 트리거로 사용할 수 있습니다. 예를 들어 침입 이벤트에 대해 각각 트리거되는 규칙 A와 규칙 B를 생성하는 경우, "규칙 A가 True인 경우" 기준을 규칙 B의 제약 조건으로 사용할 수 있습니다. 이 컨피그레이션에서 규칙 A는 규칙 B 내에 "중첩"된 것으로 간주됩니다.

업데이트 프로세스는 중첩된 상관관계 규칙(규칙 A)의 설정을 중첩할 상관관계 규칙(규칙 B)에 복사한 다음 중첩된 규칙을 삭제하는 방식으로 특정 중첩 상관관계 규칙을 평면화합니다. 업데이트 시 호스트 프로파일/사용자 자격 및 스누즈/비활성 기간을 중첩된 규칙에서 중첩할 규칙으로 복사합니다.

시스템은 비활성 기간 제외한 이러한 모든 설정이 중첩할 규칙에 없는 경우에만 해당 설정을 중첩된 규칙에서 중첩할 규칙으로 복사할 수 있습니다. 시스템은 비활성 기간을 중첩된 규칙에서 중첩할 규칙으로 복사할 때 중첩할 규칙의 비활성 기간을 유지합니다. 따라서 결과 규칙은 중첩할 컨피그레이션에 원래 포함되어 있던 두 규칙의 설정을 모두 사용합니다.

중첩된 규칙과 중첩할 규칙에서 특정 유형의 충돌이 발생하는 경우, 업데이트 시 중첩된 규칙을 평면화할 수 없습니다. 이러한 경우, 업데이트에 실패합니다.

이러한 업데이트 실패를 방지하려면 업데이트를 실행하기 전에 상관관계 규칙을 다음과 같이 수정합니다.

- 중첩된 컨피그레이션에서 하나의 규칙만 호스트 프로파일 자격, 사용자 자격 및 스누즈 기간 설정을 지정하도록 중첩된 규칙이나 중첩할 규칙에서 이러한 설정을 제거합니다.
- 모든 중첩된 규칙에서 연결 추적기를 제거합니다.
- 중첩된 규칙에서 True일 필요가 없는 호스트 프로파일 자격, 사용자 자격, 스누즈 기간 및 비활성 기간을 제거합니다. 즉, 중첩할 규칙 내에서 OR 연산자를 사용하여 다른 규칙 조건에 연결되어 있는 중첩된 규칙에서 이러한 설정을 제거합니다.

상관관계 규칙에 대한 정보는 Firepower Management Center 컨피그레이션 가이드, 버전 6.2.0을 참조하십시오.

업데이트 중 **Failsafe** 컨피그레이션 자동 수정

버전 6.2.0에서는 Snort Fail Open 컨피그레이션이 Firepower Management Center에 의해 관리되는 Firepower Threat Defense 물리적 및 가상 디바이스의 Failsafe 옵션을 대체합니다. 이 새로운 기능은

Failsafe 옵션과 같은 기능을 제공하지만, Snort 프로세스가 중단되었을 때 트래픽을 삭제할지 여부도 선택할 수 있습니다.

Firepower Management Center를 버전 6.2.0으로 업데이트하더라도 다음 매니지드 디바이스에 대해서는 Failsafe가 계속 지원됩니다.

- 버전 6.1.x를 실행 중인 Firepower Threat Defense 디바이스
- 버전 6.2.0을 실행 중인 7000 Series, 8000 Series 및 NGIPSv 디바이스

Firepower Threat Defense 디바이스를 버전 6.2.0으로 업데이트할 때는 Failsafe가 활성화되어 있는지를 확인하며, Failsafe가 활성화되어 있는 경우 Failsafe 옵션을 일치하는 Snort Fail Open 컨피그레이션으로 마이그레이션합니다. Firepower Threat Defense 디바이스를 업데이트하기 전에 Failsafe를 활성화할지 여부를 고려하는 것이 좋습니다.

표 ***9: Failsafe*를 *Snort Fail Open*으로 마이그레이션**

버전 **6.1 Failsafe**의 상태	**Snort Fail Open** 설정	
	사용 중	중단
비활성화됨(기본 동작) Snort 프로세스가 사용 중이면 새 연결과 기존 연결이 삭제되고, Snort 프로세스가 중단되면 새 연결과 기존 연결이 검사 없이 통과됩니다.	비활성화됨 Snort 프로세스가 사용 중이면 새 연결과 기존 연결이 삭제됩니다.	활성화됨 Snort 프로세스가 중단되면 새 연결과 기존 연결이 검사 없이 통과됩니다.
Enabled(활성화) Snort 프로세스가 사용 중이거나 중단되면 새 연결과 기존 연결이 검사 없이 통과됩니다.	Enabled(활성화) Snort 프로세스가 사용 중이면 새 연결과 기존 연결이 검사 없이 통과됩니다.	Enabled(활성화) Snort 프로세스가 중단되면 새 연결과 기존 연결이 검사 없이 통과됩니다.

자세한 내용은 Firepower Management Center 컨피그레이션 가이드, 버전 6.2.0의 Firepower System의 인라인 집합 장에서 Failsafe 섹션을 참조하십시오.

버전 6.1.0 지침

ASA FirePOWER 모듈을 버전 **6.1** 이상으로 업그레이드하기 전에 **ASA REST API** 비활성화

ASA FirePOWER 모듈을 버전 6.1 이상으로 업그레이드하기 전에 ASA CLI를 사용하여 ASA REST API를 비활성화합니다.

no rest-api agent

REST API를 비활성화하지 않으면 업그레이드에 실패하게 됩니다. 업그레이드 후에 REST API를 다시 활성화할 수 있습니다.

rest-api agent

ASA FirePOWER 모듈의 버전 6.0 이상을 실행 중인 경우에도 ASA 5506-X Series 디바이스는 ASA REST API를 지원하지 않습니다.

STIG 모드가 UCAPL 모드로 변경됨

버전 6.1에서는 STIG(Security Technical Implementation Guide) 모드로 알려진 보안 인증서 컴플라이언스 모드의 이름이 UCAPL(Unified Capabilities Approved Products List) 모드로 바뀌었습니다.

버전 6.1 업그레이드 후에는 STIG 모드의 Firepower 어플라이언스가 UCAPL 모드로 바뀝니다. 그리고 UCAPL 모드와 연관된 시스템 기능의 모든 제한과 변경 사항이 적용됩니다.

UCAPL 컴플라이언스를 위해 시스템을 강화하는 정보를 비롯한 자세한 내용은 *Firepower Management Center* 컨피그레이션 가이드의 보안 인증서 컴플라이언스 장과 인증 기관이 제공하는 이 제품 관련 지침을 참조하십시오.

업그레이드 후 기본 라이선스 복원

Firepower Management Center를 버전 6.1로 업그레이드하면 매니지드 NGIPSv, ASA FirePOWER, 7000 Series 및 8000 Series 디바이스의 기본 라이선스가 삭제되거나 비활성화될 수 있습니다.

업데이트를 시작하기 전에 Cisco TAC에 문의하여 이 문제를 방지하기 위해 실행할 수 있는 스크립트를 확인하십시오. 업그레이드 전 스크립트를 실행하지 않는 경우 업데이트 후에 다음을 수행합니다.

- 삭제된 라이선스 확인 및 다시 설치 - **System**(시스템) > **Licenses**(라이선스) > **Classic Licenses**(기본 라이선스)를 선택합니다.
- 영향을 받는 디바이스 수정 및 라이선스 다시 활성화 - **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택합니다.

버전 6.0.0 지침

용어 및 브랜딩

버전 6.0에서는 다음을 포함한 주요 용어 및 브랜딩이 변경되었습니다.

- FireSIGHT System → Firepower
- FireSIGHT Defense Center → Firepower Management Center
- Series 3 디바이스 → 7000 Series 디바이스 또는 8000 Series 디바이스
- 가상 매니지드 디바이스 → NGIPSv

자세한 내용은 Cisco Firepower 용어 가이드를 참조하십시오.

버전 6.0 사전 설치 패키지

Cisco에서는 버전 5.4.x에서 버전 6.x로의 업그레이드에 대해 업그레이드를 최적화하는 사전 설치 패키지를 제공합니다.

경우에 따라 다음 표에 나와 있는 사전 설치 패키지를 반드시 사용해야 합니다. 그리고 사전 설치 패키지를 사용할 필요가 없더라도 업그레이드 경로에 버전 6.0 사전 설치 패키지를 포함하고 사용하는 것이 좋습니다.

어플라이언스	업그레이드할최소버전	필요한사전설치패키지	권장 사전 설치 패키지
FireSIGHT Defense Center(Firepower Management Center)	5.4.1.1	5.4.1.1 ~ 5.4.1.5	5.4.1.6 이상
7000/8000 Series 디바이스	5.4.0.2	5.4.0.2 ~ 5.4.0.6	
NGIPSv	5.4.0.2 5.4.1.1	5.4.0.2 ~ 5.4.0.6 5.4.1.1 ~ 5.4.1.5	5.4.1.6 이상 5.4.0.7 이상
ASA FirePOWER 모듈 (5.4.1.x 시퀀스의 모델)	5.4.1	5.4.1 5.4.1.1 ~ 5.4.1.5	5.4.1.6 이상
ASA FirePOWER 모듈 (5.4.0.x 시퀀스의 모델)	5.4.0.2	5.4.0.2 ~ 5.4.0.6	5.4.0.7 이상

DC750, DC1500, DC3500 및 Virtual Defense Center의 메모리 업그레이드

다음 FireSIGHT Defense Center 모델의 경우 버전 6.0을 실행하기 위해 추가 메모리가 필요할 수 있습니다.

- DC750
- DC1500
- DC3500
- 가상 방어 센터

메모리 증량은 Cisco 제품 요구 사항에 따라 이루어지므로 Cisco에서는 적격한 DC750 또는 DC1500에서 버전 6.0을 실행할 수 있는 고객에게 무료로 메모리 업그레이드 키트를 제공합니다.

- 키트 주문 방법은 필드 알림: FN - 64077 - Cisco FireSIGHT 및 Sourcefire Defense Center Management Appliance - FirePOWER 소프트웨어 V6.0 이상에 필요한 메모리 업그레이드를 참조하십시오.
- 메모리 업그레이드 - Firepower Management Center 설치 가이드의 Firepower Management Center 메모리 업그레이드 지침을 참조하십시오.

Defense Center 고가용성 쌍 해제

버전 6.0.x에서는 Firepower Management Center의 고가용성을 지원하지 않습니다.

Defense Center의 버전 5.4.x 고가용성 쌍을 Firepower Management Center의 버전 6.0 고가용성 쌍으로 업그레이드할 수는 없습니다. 그러므로 고가용성 쌍을 해제한 후 각 Defense Center를 개별적으로 업그레이드해야 합니다. 버전 6.1에서 고가용성을 다시 설정할 수 있습니다.

"Retry URL Cache Miss Lookup(URL 캐시 누락 조회 재시도)" 옵션 비활성화

버전 5.4.0.6, 버전 5.4.1.5 이하를 실행 중인 디바이스를 관리하는 경우 Firepower Management Center를 버전 6.0으로 업그레이드하면 트래픽 중단 및 시스템 문제가 발생할 수 있습니다.

Defense Center를 업그레이드하기 전에 **Retry URL cache miss lookup(URL** 캐시 누락 조회 재시도**)** 옵션을 비활성화해야 합니다. 이 옵션은 디바이스에 구축된 액세스 컨트롤 정책의 Advanced(고급) 탭에서 설정할 수 있습니다. 그런 다음, 디바이스를 재구축합니다. 매니지드 디바이스를 버전 5.4.0.7 이상이나 버전 5.4.1.6 이상 또는 버전 6.0으로 업그레이드한 후 옵션을 다시 활성화할 수 있습니다.

Defense Center HTTPS 인증서 업데이트

다음의 HTTPS 인증서 중 하나를 사용 중인 버전 5.4.x Defense Center를 버전 6.0 Firepower Management Center로 업그레이드하는 경우 로그인할 수 없으며 Cisco TAC에 문의해야 합니다.

- RSASSA-PSS 서명 알고리즘으로 생성된 인증서.

  업그레이드 전에 sha1WithRSAEncryption 알고리즘 또는 sha256WithRSAEncryption 알고리즘으로 생성된 인증서나 Defense Center 기본 인증서로 교체합니다. 재부팅합니다.

- 2048비트가 넘는 공용 서버 키를 사용하여 생성된 인증서.

  업그레이드 전에 CSR(서버 인증서 요청)로 생성된 인증서로 교체합니다. 재부팅합니다.

또한 업그레이드 후에는 이러한 유형의 인증서를 업로드하지 마십시오. 버전 5.4.x 어플라이언스에서 인증서를 생성하려면 *FireSIGHT System* 사용 설명서, 버전 5.4.1의 맞춤형 HTTPS 인증서 사용을 참조하십시오.

프라이빗 AMP 클라우드 미지원

버전 6.0에서는 프라이빗 AMP 클라우드의 Firepower용 AMP 서명 조회 기능이 지원되지 않습니다. 버전 6.0에서는 시스템이 퍼블릭 AMP 클라우드로 SHA-256 서명을 자동으로 제출합니다. 프라이빗 AMP 클라우드를 사용 중이며 엔드포인트로부터 이벤트를 수신하는 경우 컨피그레이션을 추가로 변경하지 않아도 버전 6.0 Defense Center가 해당 이벤트를 계속 수신할 수 있습니다.

12 장

Firepower 소프트웨어 업그레이드 시간 및 디스크 공간

Firepower 어플라이언스를 업그레이드하려면 사용 가능한 디스크 공간이 충분해야 합니다. 그렇지 않으면 업그레이드에 실패합니다. Firepower Management Center를 사용하여 매니지드 디바이스를 업그레이드할 때 Firepower Management Center의 /Volume 파티션에는 추가 디스크 공간이 필요합니다.

또한 업그레이드를 수행할 시간도 충분해야 합니다. 사용 중인 구축에 따라 제공된 예상 시간보다 업그레이드가 더 오래 걸릴 수도 있습니다. 예를 들어 메모리가 적은 어플라이언스와 로드가 많은 어플라이언스의 경우 업그레이드 시간이 더 오래 걸릴 수 있습니다. 준비 확인을 완료하는 데 필요한 시간도 이러한 예상 시간에 포함되지 않습니다.

버전 6.2.3 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower Management Center	6.1.0 이상: 17MB 6.2.0 이상: 24MB 6.2.1 이상: 23MB 6.2.2 이상: 24MB	6.1.0 이상: 7415MB 6.2.0 이상: 8863MB 6.2.1 이상: 8263MB 6.2.2 이상: 11860MB	—	6.1.0 이상: 38분 6.2.0 이상: 43분 6.2.1 이상: 37분 6.2.2 이상: 37분

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower Management Center Virtual	6.1.0 이상: 23MB 6.2.0 이상: 28MB 6.2.1 이상: 24MB 6.2.2 이상: 24MB	6.1.0 이상: 7993MB 6.2.0 이상: 9320MB 6.2.1 이상: 11571MB 6.2.2 이상: 11487MB	—	하드웨어에 따라 다름
Firepower 2100 Series	6.2.1 이상: 7356MB 6.2.2 이상: 11356MB	6.2.1 이상: 7356MB 6.2.2 이상: 11356MB	1000MB	6.2.1 이상: 15분 6.2.2 이상: 15분
Firepower 4100 Series Firepower 9300	6.1.0 이상: 5593MB 6.2.0 이상: 5122MB 6.2.2 이상: 7498MB	6.1.0 이상: 5593MB 6.2.0 이상: 5122MB 6.2.2 이상: 7498MB	795MB	6.1.0 이상: 10분 6.2.0 이상: 12분 6.2.2 이상: 15분
ASA 5500-X series with Firepower Threat Defense	6.1.0 이상: 0.088MB 6.2.0 이상: 0.092MB 6.2.2 이상: 0.088MB	6.1.0 이상: 4322MB 6.2.0 이상: 6421MB 6.2.2 이상: 6450MB	1000MB	6.1.0 이상: 54분 6.2.0 이상: 53분 6.2.2 이상: 28분
Firepower Threat Defense Virtual	6.1.0 이상: 0.076MB 6.2.0 이상: 0.092MB 6.2.2 이상: 0.092MB	6.1.0 이상: 4225MB 6.2.0 이상: 5179MB 6.2.2 이상: 6450MB	1000MB	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	6.1.0 이상: 18MB 6.2.0 이상: 18MB 6.2.2 이상: 18MB	6.1.0 이상: 5145MB 6.2.0 이상: 5732MB 6.2.2 이상: 6752MB	840MB	6.1.0 이상: 29분 6.2.0 이상: 31분 6.2.2 이상: 31분
ASA FirePOWER 모듈	6.1.0 이상: 16MB 6.2.0 이상: 16MB 6.2.2 이상: 16MB	6.1.0 이상: 7286MB 6.2.0 이상: 7286MB 6.2.2 이상: 10748MB	6.1.0 이상: 1200MB 6.2.0 이상: 1200MB	6.1.0 이상: 94분 6.2.0 이상: 104분 6.2.2 이상: 96분
NGIPSv	6.1.0 이상: 18MB 6.2.0 이상: 19MB 6.2.2 이상: 19MB	6.1.0 이상: 4115MB 6.2.0 이상: 5505MB 6.2.2 이상: 5871MB	741MB	하드웨어에 따라 다름

버전 6.2.2 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower Management Center	6.2.0 이상: 22MB 6.2.1 이상: 21MB	6.2.0 이상: 6467MB 6.2.1 이상: 6916MB	—	6.2.0 이상: 52분 6.2.1 이상: 61분
Firepower Management Center Virtual	6.2.0 이상: 24MB 6.2.1 이상: 24MB	6.2.0 이상: 6987MB 6.2.1 이상: 5975MB	—	하드웨어에 따라 다름
Firepower 2100 Series	5613MB	5613MB	925MB	57분
Firepower 4100 Series Firepower 9300	4635MB	4635MB	743MB	14분
Firepower Threat Defense Virtual	0.92MB	3586MB	987MB	하드웨어에 따라 다름
ASA 5500-X series with Firepower Threat Defense	.16MB	3683MB	987MB	80분
Firepower 7000 Series Firepower 8000 Series	18MB	6745MB	1300MB	27분
ASA FirePOWER 모듈	16MB	7021MB	1200MB	131분
NGIPSv	18MB	7261MB	1300MB	하드웨어에 따라 다름

버전 6.2.2.2 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower Management Center	18MB	1656MB	—	6.2.2 이상: 34분 6.2.2.1 이상: 27분
Firepower Management Center Virtual	19MB	2356MB	—	하드웨어에 따라 다름
Firepower 2100 Series	2377MB	2377MB	497MB	6.2.2 이상: 41분 6.2.2.1 이상: 20분
Firepower 4100 Series Firepower 9300	561MB	561MB	41MB	6.2.2 이상: 21분 6.2.2.1 이상: 13분

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
ASA 5500-X series with Firepower Threat Defense	122MB	984MB	136MB	6.2.2 이상: 110분 6.2.2.1 이상: 70분
Firepower Threat Defense Virtual	122MB	984MB	136MB	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	16MB	1706MB	310MB	6.2.2 이상: 56분 6.2.2.1 이상: 40분
ASA FirePOWER 모듈	15MB	1602MB	190MB	6.2.2 이상: 113분 6.2.2.1 이상: 80분
NGIPSv	17MB	170MB	16MB	하드웨어에 따라 다름

버전 6.2.2.1 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	6.2.2에서 업데이트하는 시간
Firepower Management Center	18MB	480MB	—	52분
Firepower Management Center Virtual	30MB	775MB	—	하드웨어에 따라 다름
Firepower 2100 Series	1003MB	1003MB	47MB	28분
Firepower 4100 Series Firepower 9300	299MB	299MB	47MB	35분
ASA 5500-X series with Firepower Threat Defense	121MB	674MB	69MB	72분
Firepower Threat Defense Virtual	121MB	674MB	69MB	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	14MB	664MB	61MB	33분
ASA FirePOWER 모듈	15MB	758MB	83MB	90분
NGIPSv	17MB	106MB	10MB	하드웨어에 따라 다름

버전 **6.2.0** 시간 및 디스크 공간

어플라이언스	**/**에 필요한 공간	**/Volume**에 필요한 공간	**Manager**에 필요한 공간	**Time**(시간)
Firepower Management Center	17MB	10207MB	—	57분
Firepower Management Center Virtual	17MB	10207MB	—	하드웨어에 따라 다름
Firepower 4100 Series Firepower 9300	5234MB	5234MB	734MB	21분
ASA 5500-X series with Firepower Threat Defense	0.096MB	5213MB	938MB	83분
Firepower Threat Defense Virtual	1MB	5663MB	936MB	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	17MB	6129MB	1200MB	27분
ASA FirePOWER 모듈	16MB	6619MB	1100MB	165분
NGIPSv	18MB	7028MB	1300MB	하드웨어에 따라 다름

버전 **6.2.0.5** 시간 및 디스크 공간

어플라이언스	**/**에 필요한 공간	**/Volume**에 필요한 공간	**Manager**에 필요한 공간	**Time**(시간)
Firepower Management Center	180MB	6009MB	—	6.2.0 이상: 72분 6.2.0.4 이상: 34분
Firepower Management Center Virtual	20MB	6943MB	—	하드웨어에 따라 다름
Firepower 4100 Series Firepower 9300	3009MB	3009MB	441MB	6.2.0 이상: 28분 6.2.0.4 이상: 16분
Firepower Threat Defense Virtual	135MB	2805MB	548MB	하드웨어에 따라 다름
ASA 5500-X series with Firepower Threat Defense	135MB	4316MB	548MB	6.2.0 이상: 46분 6.2.0.4 이상: 22분

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower 7000 Series Firepower 8000 Series	18MB	5806MB	693MB	6.2.0 이상: 51분 6.2.0.4 이상: 18분
ASA FirePOWER 모듈	16MB	5945MB	703MB	6.2.0 이상: 66분 6.2.0.4 이상: 27분
NGIPSv	18MB	1301MB	211MB	하드웨어에 따라 다름

버전 6.2.0.4 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower Management Center	167MB	5271MB	—	6.2.0 이상: 84분 6.2.0.3 이상: 50분
Firepower Management Center Virtual	20MB	5346MB	—	하드웨어에 따라 다름
Firepower 4100 Series Firepower 9300	1828MB	1828MB	325MB	6.2.0 이상: 23분 6.2.0.3 이상: 12분
ASA 5500-X series with Firepower Threat Defense	134MB	3593MB	448MB	6.2.0 이상: 2시간 28분 6.2.0.3 이상: 69분
Firepower Threat Defense Virtual	136MB	275MB	448MB	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	18MB	4614MB	608MB	6.2.0 이상: 45분 6.2.0.3 이상: 17분
ASA FirePOWER 모듈	16 B	4585MB	597MB	6.2.0 이상: 3시간 34분 6.2.0.3 이상: 83분
NGIPSv	18MB	1067MB	208MB	하드웨어에 따라 다름

버전 6.2.0.3 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower Management Center	18MB	3352MB	—	6.2.0 이상: 75분 6.2.0.2 이상: 37분

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower Management Center Virtual	19MB	3342MB	—	하드웨어에 따라 다름
Firepower 4100 Series Firepower 9300	1355MB	—	319MB	6.2.0 이상: 18분 6.2.0.2 이상: 12분
ASA 5500-X series with Firepower Threat Defense	2302MB	131MB	384MB	6.2.0 이상: 118분 6.2.0.2 이상: 76분
Firepower Threat Defense Virtual	17MB	842MB	384MB	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	17MB	3526MB	554MB	6.2.0 이상: 38분 6.2.0.2 이상: 19분
ASA FirePOWER 모듈	3361MB	15MB	521MB	6.2.0 이상: 3시간 6.2.0.2 이상: 97분
NGIPSv	17MB	842MB	202MB	하드웨어에 따라 다름

버전 6.2.0.2 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower Management Center	35MB	1665MB	—	6.2.0 이상: 36분 6.2.0.1 이상: 30분
Firepower Management Center Virtual	21MB	2834MB	—	하드웨어에 따라 다름
Firepower 4100 Series Firepower 9300	1060MB	1060MB	274MB	6.2.0 이상: 12분 6.2.0.1 이상: 9분
ASA 5500-X series with Firepower Threat Defense	144MB	1808MB	295MB	6.2.0 이상: 95분 6.2.0.1 이상: 59분
Firepower Threat Defense Virtual	143MB	998MB	295MB	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	17MB	2110MB	458MB	6.2.0 이상: 54분 6.2.0.1 이상: 35분

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
ASA FirePOWER 모듈	17MB	2014MB	383MB	6.2.0 이상: 40분 6.2.0.1 이상: 80분
NGIPSv	19MB	612MB	195MB	하드웨어에 따라 다름

버전 6.2.0.1 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	6.2.0에서 업데이트하는 시간
Firepower Management Center	50MB	1237MB	—	28분
Firepower Management Center Virtual	23MB	1488MB	—	하드웨어에 따라 다름
Firepower 4100 Series Firepower 9300	524MB	524MB	137MB	12분
ASA 5500-X series with Firepower Threat Defense	144MB	945MB	159MB	62분
Firepower Threat Defense Virtual	10MB	144MB	159MB	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	18MB	1134MB	186MB	22분
ASA FirePOWER 모듈	17MB	97MB	206MB	69분
NGIPSv	19MB	721MB	98MB	하드웨어에 따라 다름

버전 6.1.0 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower Management Center	18MB	10722MB	—	47분
Firepower Management Center Virtual	17MB	10128MB	—	하드웨어에 따라 다름

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
ASA 5500-X series with Firepower Threat Defense	0.096MB	5213MB	914MB	21분
Firepower Threat Defense Virtual	0.096MB	5403MB	914MB	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	61MB	7108MB	1740MB	39분
ASA FirePOWER 모듈	47MB	8392MB	1300MB	59분
NGIPSv	54MB	6368MB	1229MB	하드웨어에 따라 다름

버전 6.1.0.6 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	6.1.0.5에서 업데이트하는 시간
Firepower Management Center	215MB	10503MB	—	6.1.0 이상: 66분 6.1.0.5 이상: 27분
Firepower Management Center Virtual	196MB	1367MB	—	하드웨어에 따라 다름
Firepower 4100 Series Firepower 9300	8140MB	8140MB	1126MB	6.1.0 이상: 270분 6.1.0.5 이상: 75분
ASA 5500-X series with Firepower Threat Defense	1034MB	8540MB	1229MB	6.1.0 이상: 40분 6.1.0.5 이상: 15분
Firepower Threat Defense Virtual	1033MB	7414MB	1229MB	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	237MB	12725MB	1434MB	6.1.0 이상: 136분 6.1.0.5 이상: 34분
ASA FirePOWER 모듈	31MB	11189MB	1131MB	6.1.0 이상: 257분 6.1.0.5 이상: 60분
NGIPSv	196MB	4606MB	644MB	하드웨어에 따라 다름

버전 **6.1.0.5** 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	6.1.0.4에서 업데이트하는 시간
Firepower Management Center	46MB	7673MB	—	6.1.0 이상: 56분 6.1.0.4 이상: 28분
Firepower Management Center Virtual	216MB	10790MB	—	하드웨어에 따라 다름
Firepower 4100 Series Firepower 9300	7680MB	7680MB	1060MB	6.1.0 이상: 30분 6.1.0.4 이상: 10분
ASA 5500-X series with Firepower Threat Defense	137MB	7952MB	1141MB	6.1.0 이상: 186분 6.1.0.4 이상: 70분
Firepower Threat Defense Virtual	1140MB	7453MB	1141MB	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	259MB	11877MB	1403MB	6.1.0 이상: 115분 6.1.0.4 이상: 25분
ASA FirePOWER 모듈	34MB	8955MB	1217MB	6.1.0 이상: 208분 6.1.0.4 이상: 105분
NGIPSv	215MB	4298MB	640MB	하드웨어에 따라 다름

버전 **6.1.0.4** 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower Management Center	218808MB	6739516MB	—	6.1.0 이상: 65분 6.1.0.3 이상: 30분
Firepower Management Center Virtual	200748MB	675984MB	—	하드웨어에 따라 다름
Firepower 4100 Series Firepower 9300	6010092MB	6010092MB	1020MB	6.1.0 이상: 26분 6.1.0.3 이상: 10분
ASA 5500-X series with Firepower Threat Defense	1058968MB	6155828MB	1100MB	6.1.0 이상: 49분 6.1.0.3 이상: 20분

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower Threat Defense Virtual	1059632MB	1059632MB	1100MB	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	240940MB	8713068MB	1200MB	6.1.0 이상: 48분 6.1.0.3 이상: 17분
ASA FirePOWER 모듈	31740MB	7442808MB	1100MB	6.1.0 이상: 63분 6.1.0.3 이상: 45분
NGIPSv	20120MB	3367536MB	636MB	하드웨어에 따라 다름

버전 6.1.0.3 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower Management Center	218676MB	5537816MB	—	6.1.0 이상: 46분 6.1.0.2 이상: 35분
Firepower Management Center Virtual	200904MB	6611148MB	—	하드웨어에 따라 다름
Firepower 4100 Series Firepower 9300	5014020MB	5014020MB	929MB	6.1.0 이상: 22분 6.1.0.2 이상: 13분
ASA 5500-X series with Firepower Threat Defense	1057776MB	1057776MB	1000MB	6.1.0 이상: 40분 6.1.0.2 이상: 23분
Firepower Threat Defense Virtual	1059932MB	1059932MB	1000MB	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	228728MB	7357340MB	1100MB	6.1.0 이상: 43분 6.1.0.2 이상: 25분
ASA FirePOWER 모듈	31792MB	4782384MB	1000MB	6.1.0 이상: 160분 6.1.0.2 이상: 80분
NGIPSv	200896MB	2710540MB	635MB	하드웨어에 따라 다름

버전 **6.1.0.2** 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower Management Center	235MB	3872MB	—	6.1.0 이상: 44분 6.1.0.1 이상: 22분
Firepower Management Center Virtual	219MB	3871MB	—	하드웨어에 따라 다름
Firepower 4100 Series Firepower 9300	4046MB	4046MB	886MB	6.1.0 이상: 20분 6.1.0.1 이상: 14분
ASA 5500-X series with Firepower Threat Defense	96MB	2291MB	918MB	6.1.0 이상: 74분 6.1.0.1 이상: 106
Firepower Threat Defense Virtual	1137MB	2797MB	918MB	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	260MB	4130MB	965MB	6.1.0 이상: 62분 6.1.0.1 이상: 24분
ASA FirePOWER 모듈	40MB	4549MB	816MB	6.1.0 이상: 139분 6.1.0.1 이상: 34분
NGIPSv	200896MB	2710540MB	635MB	하드웨어에 따라 다름

버전 **6.1.0.1** 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	6.1.0에서 업데이트하는 시간
Firepower Management Center	140MB	1893MB	—	23분
Firepower Management Center Virtual	207MB	2144MB	—	하드웨어에 따라 다름
Firepower 4100 Series	580MB	2580MB	600MB	15분
Firepower 9300	1877MB	1877MB	600MB	20분
ASA 5500-X series with Firepower Threat Defense	846MB	1377MB	600MB	10분

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	6.1.0에서 업데이트하는 시간
Firepower Threat Defense Virtual	846MB	1377MB	600MB	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	156MB	2094MB	513MB	47분
ASA FirePOWER 모듈	34MB	1728MB	433MB	76분
NGIPSv	130MB	793MB	295MB	하드웨어에 따라 다름

버전 6.0.1 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower Management Center	18MB	8959MB	—	66분
Firepower Management Center Virtual	—	—	—	—
Firepower 7000 Series Firepower 8000 Series	227MB	3683MB	614MB	30분
ASA FirePOWER 모듈	54MB	2966MB	429MB	91분
NGIPSv	196MB	2090MB	3050MB	하드웨어에 따라 다름

버전 6.0.1.4 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower Management Center	201MB	3428MB	—	6.0.0 이상: 92분 6.0.1.3 이상: 39분
Firepower Management Center Virtual	95MB	3108MB	—	하드웨어에 따라 다름
Firepower 4100 Series	5237MB	5237MB	1000MB	6.0.0 이상: 30분 6.0.1.3 이상: 18분
Firepower 9300	5434MB	1360MB	1000MB	6.0.0 이상: 26분 6.0.1.3 이상: 14분

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
ASA 5500-X series with Firepower Threat Defense	1017MB	3416MB	1000MB	6.0.0 이상: 26분 6.0.1.3 이상: 14분
Firepower Threat Defense Virtual	1020MB	3619MB	1000MB	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	222MB	7891MB	1270MB	6.0.0 이상: 47분 6.0.1.3 이상: 23분
ASA FirePOWER 모듈	45MB	6049MB	990MB	6.0.0 이상: 95분 6.0.1.3 이상: 43분
NGIPSv	192MB	2916MB	990MB	하드웨어에 따라 다름

버전 **6.0.1.3** 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower Management Center	110MB	2419MB	—	58분
Firepower Management Center Virtual	101MB	2419MB	—	하드웨어에 따라 다름
Firepower 4100 Series Firepower 9300	2781MB	2781MB	473MB	22분
ASA 5500-X series with Firepower Threat Defense	813MB	2641MB	473MB	24분
Firepower Threat Defense Virtual	813MB	2651MB	473MB	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	125MB	4757MB	926MB	55분
ASA FirePOWER 모듈	58MB	3883MB	685MB	184분
NGIPSv	107MB	1695MB	430MB	하드웨어에 따라 다름

버전 **6.0.1.2** 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower Management Center	54MB	272MB	—	7분
Firepower Management Center Virtual	54MB	368MB	—	하드웨어에 따라 다름
Firepower 4100 Series Firepower 9300	56MB	2101MB	302MB	16분
ASA 5500-X series with Firepower Threat Defense	807MB	740MB	302MB	13분
Firepower Threat Defense Virtual	56MB	2101MB	302MB	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	63MB	3190MB	412MB	17분
ASA FirePOWER 모듈	54MB	2027MB	577MB	99분
NGIPSv	56MB	602MB	243MB	하드웨어에 따라 다름

버전 **6.0.1.1** 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	6.0.1에서 업데이트하는 시간
Firepower Management Center	54MB	14MB	—	23분
Firepower Management Center Virtual	54MB	14MB	—	하드웨어에 따라 다름
Firepower 4100 Series Firepower 9300	54MB	54MB	2MB	6분
ASA 5500-X series with Firepower Threat Defense	54MB	54MB	2MB	7분
Firepower Threat Defense Virtual	54MB	14MB	2MB	하드웨어에 따라 다름

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	6.0.1에서 업데이트하는 시간
Firepower 7000 Series Firepower 8000 Series	61MB	944MB	166MB	39분
ASA FirePOWER 모듈	54MB	824MB	84MB	46분
NGIPSv	56MB	54MB	1MB	하드웨어에 따라 다름

버전 6.0 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	Time(시간)
Firepower Management Center	16MB	8022MB	—	58분
Firepower Management Center Virtual	16MB	8022MB	—	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	16MB	6496MB	1200MB	94분
ASA FirePOWER 모듈	32MB	7644MB	1200MB	41분
NGIPSv	17MB	6046MB	102000MB	하드웨어에 따라 다름

버전 6.0.0.1 시간 및 디스크 공간

어플라이언스	/에 필요한 공간	/Volume에 필요한 공간	Manager에 필요한 공간	6.0에서 업데이트하는 시간
Firepower Management Center	120MB	976MB	—	25분
Firepower Management Center Virtual	119MB	969MB	—	하드웨어에 따라 다름
Firepower 7000 Series Firepower 8000 Series	134MB	1568MB	273MB	25분
ASA FirePOWER 모듈	56MB	1101MB	181MB	56분
NGIPSv	26MB	929MB	174MB	하드웨어에 따라 다름