



## Cisco Firepower Management Center 업그레이드 설명서

초판: 2018년 3월 29일

최종 변경: 2020년 11월 10일

### 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

---

장 1	시작하기 1
	가이드 사용 1
	업그레이드 체크리스트 2
	Firepower 소프트웨어 새로 설치 2

---

부 1:	업그레이드 준비 5
------	------------

---

장 2	구축 평가 7
	구축 평가 질문 7
	현재 버전 정보 찾기 7

---

장 3	업그레이드 경로 계획 9
	업그레이드 경로 정보: 업그레이드가 가능합니까? 9
	직접 업그레이드가 가능합니까? 10
	FMC 디바이스 버전 호환성을 유지할 수 있습니까? 12
	시작해야 하는 위치 13
	Firepower 소프트웨어 릴리스 유형 14
	사전 설치 패키지 식별(버전 6.0, 6.0.1, 6.1) 18
	새 디바이스를 추가할 시기 파악 19
	트래픽 흐름 및 검사에서 중단 식별 19
	기타 주요 작업 확인 20

---

장 4	Firepower 소프트웨어 업그레이드 패키지 다운로드 21
	Firepower 소프트웨어 업그레이드 패키지 정보 21

업그레이드 패키지 관리를 위한 지침 및 제한 사항 23

Firepower 소프트웨어 업그레이드 패키지 다운로드 24

    Cisco에서 직접 업그레이드 패키지 다운로드 26

FMC에 Firepower 소프트웨어 업그레이드 패키지 업로드 26

내부 서버에서 FTD 업그레이드 패키지 가져오기 27

FMC 관리 디바이스로 업그레이드 패키지 푸시 28

---

장 5           **Firepower** 소프트웨어 준비도 확인 실행 31

    준비도 확인 지침 및 제한 사항 31

    준비도 확인 실행(버전 6.7 이상) 32

    준비도 확인 실행(버전 6.1~6.6.x) 33

---

장 6           업그레이드 전 기타 작업 및 확인 35

    유지 보수 기간 예약 35

    어플라이언스 액세스, 커뮤니케이션 및 상태 확인 35

    관리 네트워크 대역폭 36

    구성 변경 계획 36

    백업 수행 36

    NTP 동기화 확인 37

---

부 11:           **Firepower** 어플라이언스 업그레이드 39

---

장 7           **Firepower Management Center** 업그레이드 41

    업그레이드 체크리스트: Firepower Management Center 41

    업그레이드 경로: Firepower Management Center 43

    독립형 FMC 업그레이드 45

    고가용성 FMC 업그레이드 46

---

장 8           **Firepower Threat Defense** 업그레이드: **Firepower 4100/9300** 49

    업그레이드 체크리스트: Firepower 4100/9300 새시의 FTD 49

    업그레이드 경로: Firepower 4100/9300 새시의 FTD 52

FXOS 업그레이드: Firepower 4100/9300 새시 55

    Firepower 4100/9300 새시용 FXOS 업그레이드 패키지 55

    독립형 FTD 논리 디바이스 또는 FTD 새시 내 클러스터용 FXOS 업그레이드 56

        사용해 독립형 FTD 논리 디바이스 또는 FTD 새시 내 클러스터용 FXOS 업그레이드 Firepower Chassis Manager 56

        FXOS CLI를 사용해 독립형 FTD 논리 디바이스 또는 FTD 새시 내 클러스터용 FXOS 업그레이드 58

    Firepower Threat Defense 고가용성 쌍에서 FXOS 업그레이드 61

        Firepower Chassis Manager를 사용하여 FTD 고가용성 쌍에서 FXOS 업그레이드 61

        FXOS CLI를 사용하여 FTD 고가용성 쌍에서 FXOS 업그레이드 64

    Firepower Threat Defense 새시 간 클러스터에서 FXOS 업그레이드 69

        Firepower Chassis Manager를 사용하여 FTD 새시 간 클러스터에서 FXOS 업그레이드 69

        FXOS CLI를 사용하여 FTD 새시 간 클러스터에서 FXOS 업그레이드 72

FTD 소프트웨어 업그레이드: Firepower 4100/9300 새시 75

---

장 9                   **Firepower Threat Defense 업그레이드: 기타 FTD 디바이스 79**

    업그레이드 체크리스트: 기타 FTD 디바이스 79

    업그레이드 경로: 기타 FTD 디바이스 82

    FTD 소프트웨어 업그레이드: 기타 FTD 디바이스 83

---

장 10                   **Firepower 7000/8000 Series 및 NGIPSv 업그레이드 87**

    업그레이드 체크리스트: Firepower 7000/8000 Series 및 NGIPSv 87

    업그레이드 경로: Firepower 7000/8000 Series 90

    업그레이드 경로: NGIPSv 91

    Firepower 7000/8000 Series 및 NGIPSv 업그레이드 92

---

장 11                   **ASA with FirePOWER Services 업그레이드 95**

    업그레이드 체크리스트: ASA with FirePOWER Services 95

    업그레이드 경로: ASA FirePOWER 98

    ASA 업그레이드 101

        독립형 유닛 업그레이드 101

CLI를 사용하여 독립형 유닛 업그레이드 101

ASDM을 사용하여 로컬 컴퓨터에서 독립형 유닛 업그레이드 103

ASDM Cisco.com 마법사를 사용하여 독립형 유닛 업그레이드 105

액티브/스탠바이 페일오버 쌍 업그레이드 106

CLI를 사용하여 액티브/스탠바이 페일오버 쌍 업그레이드 107

ASDM을 사용하여 액티브/스탠바이 페일오버 쌍 업그레이드 109

액티브/액티브 페일오버 쌍 업그레이드 111

CLI를 사용하여 액티브/액티브 페일오버 쌍 업그레이드 111

ASDM을 사용하여 액티브/액티브 페일오버 쌍 업그레이드 114

ASA 클러스터 업그레이드 116

CLI를 사용하여 ASA 클러스터 업그레이드 116

ASDM을 사용하여 ASA 클러스터 업그레이드 121

ASA FirePOWER 모듈 업그레이드 124

---

부 III:                   참조 127

---

장 12                   호환성 129

    Firepower Management Center 129

        Firepower Management Center: 물리적 129

        Firepower Management Center: 가상 130

        FMC용 BIOS 및 펌웨어 132

    Firepower 디바이스 133

        Firepower 1000/2100 Series FTD 133

        FMC를 사용하는 Firepower 4100/9300 133

        FTD를 사용하는 ASA 5500-X Series 및 ISA 3000 136

        Firepower Threat Defense Virtual 136

        Firepower 7000/8000 Series 및 레거시 디바이스 138

        ASA 5500-X Series 및 ISA 3000 with FirePOWER Services 138

        NGIPSv 150

---

장 13                   버전별 **Firepower** 소프트웨어 업그레이드 지침 153

        버전 6.7.0 지침 154

Firepower 1010 스위치 포트에서 유효하지 않은 VLAN ID로 업그레이드 실패 154

버전 6.6.0 가이드라인 155

    FMCv 업그레이드에 28GB RAM 필요 156

    FMC 업그레이드 후 일시적으로 사용할 수 없는 이벤트 157

버전 6.5.0 지침 158

    Firepower 1000 Series 디바이스에서 업그레이드 후 전원 켜다 다시 켜기 필요 159

    버전 6.5.0에 대한 이그레스 최적화 비활성화 159

    새 URL 카테고리 및 평판 160

        URL 카테고리 및 평판을 위한 사전 업그레이드 작업 161

        URL 카테고리 및 평판에 대한 업그레이드 후 작업 163

        병합된 URL 카테고리가 있는 규칙 지침 164

버전 6.4.0 가이드라인 166

    Firepower 1010 디바이스의 EtherChannel은 이그레스 트래픽 블랙홀이 가능합니다. 168

    업데이트 실패: 컨테이너 인스턴스의 디스크 공간 부족 168

    업그레이드 실패: 이전 버전이 6.2.3.12인 NGIPS 디바이스 168

    TLS 암호화 가속 활성화/비활성화 불가 169

버전 6.3.0 지침 169

    업그레이드 및 설치 패키지 이름 변경됨 171

    버전 6.3 이상으로 이미지를 재설치하면 대부분의 어플라이언스에서 LOM 비활성화 172

    FMC, 7000/8000 Series, NGIPSv에서 준비도 확인이 실패할 수 있음 173

    RA VPN 기본 설정 변경이 VPN 트래픽을 차단할 수 있음 173

    업그레이드 시 TLS/SSL 하드웨어 가속 활성화 174

    업그레이드 실패: 버전 6.3.0-83에서 FMC 및 ASA FirePOWER으로 업그레이드 174

    보안 인텔리전스가 애플리케이션 식별 활성화 174

    업그레이드 후 CIP 탐지를 활성화하기 위해 VDB 업데이트 175

    유효하지 않은 침입 변수 집합으로 구축 오류가 발생할 수 있음 175

    Firepower 4100/9300에서 FXOS 업그레이드 전 FTD 푸시 필요 176

버전 6.2.3 지침 177

    Cisco와 데이터 공유 177

    업그레이드 후 액세스 컨트롤 정책 수정/다시 저장 178

    보고서의 결과 제한 변경 178

업그레이드 전 FTD 클러스터에서 버전 6.1.x에서 사이트 ID 제거 179

버전 6.2.2 지침 179

    보안 강화: 서명된 업그레이드 패키지 180

    8000 Series 보안 인증서 및 컴플라이언스는 버전 6.2.2.1 이상이 필요합니다. 180

버전 6.2.0 지침 181

    액세스 제어는 SRU에서 지연 기반 성능 설정을 가져올 수 있습니다. 181

    'Snort Fail Open'이 FTD의 'Failsafe'를 대체합니다. 182

    업그레이드 시 IAB '모든 애플리케이션' 옵션 삭제 182

    업그레이드 시 비활성화된 메모리 부족 장치에 대한 URL 필터링 하위 사이트 조회 183

버전 6.1.0 지침 184

버전 6.0.0 지침 185

버전별 패치 지침 187

    버전 6.6.x.x 지침 187

        FDM을 사용하는 버전 6.6.0.1 FTD 업그레이드에서 HA 일시 중단 187

    버전 6.4.0.x 지침 188

        버전 6.4.0.9~6.4.0.11로 업그레이드하기 전에 이전 Firepower 7000/8000 디바이스를 버전 6.4.0으로 이미지 재설치 188

    버전 6.3.0.x 지침 189

    버전 6.2.3.x 지침 189

        CC 모드를 사용하는 버전 6.2.3.10 FTD 업그레이드의 FSIC 오류 189

        버전 6.2.3.3 FTD 디바이스는 로컬 관리로 전환할 수 없습니다. 190

        버전 6.2.3-88 FMC 업그레이드 전 핫픽스 190

    버전 6.2.2.x 지침 190

        Firepower 2100 Series HA 쌍 버전 6.2.2가 6.2.2.4로 업그레이드 불가 191

    버전 6.2.0.x 지침 191

        버전 6.2.0.3 FMC에 핫픽스 BH 적용 191

날짜 기반 지침 192

    동적 분석용 만료 CA 인증서 192

---

장 14                   시간 테스트 및 디스크 공간 요구 사항 195

                          시간 테스트 정보 197



디스크 공간 요구 사항 정보 198

버전 6.7.0 시간 및 디스크 공간 198

버전 6.6.1 시간 및 디스크 공간 199

버전 6.6.0.1 시간 및 디스크 공간 200

버전 6.6.0 시간 및 디스크 공간 200

버전 6.5.0.5 시간 및 디스크 공간 201

버전 6.5.0.4 시간 및 디스크 공간 202

버전 6.5.0.3 시간 및 디스크 공간 202

버전 6.5.0.2 시간 및 디스크 공간 202

버전 6.5.0.1 시간 및 디스크 공간 203

버전 6.5.0 시간 및 디스크 공간 203

버전 6.4.0.11 시간 및 디스크 공간 204

버전 6.4.0.10 시간 및 디스크 공간 204

버전 6.4.0.9 시간 및 디스크 공간 205

버전 6.4.0.8 시간 및 디스크 공간 206

버전 6.4.0.7 시간 및 디스크 공간 206

버전 6.4.0.6 시간 및 디스크 공간 207

버전 6.4.0.5 시간 및 디스크 공간 207

버전 6.4.0.4 시간 및 디스크 공간 208

버전 6.4.0.3 시간 및 디스크 공간 208

버전 6.4.0.2 시간 및 디스크 공간 209

버전 6.4.0.1 시간 및 디스크 공간 210

버전 6.4.0 시간 및 디스크 공간 210

버전 6.3.0.5 시간 및 디스크 공간 211

버전 6.3.0.4 시간 및 디스크 공간 211

버전 6.3.0.3 시간 및 디스크 공간 212

버전 6.3.0.2 시간 및 디스크 공간 213

버전 6.3.0.1 시간 및 디스크 공간 213

버전 6.3.0 시간 및 디스크 공간 214

버전 6.2.3.16 시간 및 디스크 공간 214

버전 6.2.3.15 시간 및 디스크 공간 215

버전 6.2.3.14 시간 및 디스크 공간	216
버전 6.2.3.13 시간 및 디스크 공간	216
버전 6.2.3.12 시간 및 디스크 공간	217
버전 6.2.3.11 시간 및 디스크 공간	217
버전 6.2.3.10 시간 및 디스크 공간	218
버전 6.2.3.9 시간 및 디스크 공간	218
버전 6.2.3.8 시간 및 디스크 공간	219
버전 6.2.3.7 시간 및 디스크 공간	219
버전 6.2.3.6 시간 및 디스크 공간	220
버전 6.2.3.5 시간 및 디스크 공간	220
버전 6.2.3.4 시간 및 디스크 공간	221
버전 6.2.3.3 시간 및 디스크 공간	221
버전 6.2.3.2 시간 및 디스크 공간	222
버전 6.2.3.1 시간 및 디스크 공간	223
버전 6.2.3 시간 및 디스크 공간	223
버전 6.2.2.5 시간 및 디스크 공간	224
버전 6.2.2.4 시간 및 디스크 공간	225
버전 6.2.2.3 시간 및 디스크 공간	226
버전 6.2.2.2 시간 및 디스크 공간	227
버전 6.2.2.1 시간 및 디스크 공간	227
버전 6.2.2 시간 및 디스크 공간	228
버전 6.2.0.6 시간 및 디스크 공간	228
버전 6.2.0.5 시간 및 디스크 공간	229
버전 6.2.0.4 시간 및 디스크 공간	230
버전 6.2.0.3 시간 및 디스크 공간	230
버전 6.2.0.2 시간 및 디스크 공간	231
버전 6.2.0.1 시간 및 디스크 공간	231
버전 6.2.0 시간 및 디스크 공간	232
버전 6.1.0.7 시간 및 디스크 공간	232
버전 6.1.0.6 시간 및 디스크 공간	233
버전 6.1.0.5 시간 및 디스크 공간	234

버전 6.1.0.4 시간 및 디스크 공간 234

버전 6.1.0.3 시간 및 디스크 공간 235

버전 6.1.0.2 시간 및 디스크 공간 236

버전 6.1.0.1 시간 및 디스크 공간 236

버전 6.1.0 시간 및 디스크 공간 237

버전 6.0.1.4 시간 및 디스크 공간 237

버전 6.0.1.3 시간 및 디스크 공간 238

버전 6.0.1.2 시간 및 디스크 공간 238

버전 6.0.1.1 시간 및 디스크 공간 239

버전 6.0.1 시간 및 디스크 공간 239

버전 6.0.0.1 시간 및 디스크 공간 240

버전 6.0 시간 및 디스크 공간 240

장 15

트래픽 흐름, 검사 및 디바이스 동작 241

    FTD 업그레이드 동작: Firepower 4100/9300 채시 241

    FTD 업그레이드 동작: 기타 장치 245

    Firepower 7000/8000 Series 업그레이드 동작 247

    ASA FirePOWER 업그레이드 동작 249

    NGIPSv 업그레이드 동작 250





# 1 장

## 시작하기

Firepower Management Center 업그레이드 설명서입니다. 이 가이드에서는 모든 어플라이언스가 적어도 Firepower 버전 5.4.0.2/5.4.11을 실행 중인 FMC 구축의 성공적인 업그레이드를 준비하고 완료하는 방법을 설명합니다.



**참고** 이 가이드에는 로컬로 관리되는(FDM/ASDM) 디바이스에 대한 업그레이드 정보가 포함되어 있지 않습니다. 대신 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#) 또는 [Cisco ASA 업그레이드 설명서](#)를 참조하십시오.

Firepower 구축 업그레이드는 복잡한 프로세스일 수 있습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다. 업그레이드 프로세스의 대부분은 업그레이드 스크립트를 호출하는 기계적 단계를 실제로 수행하는 것입니다.

- [가이드 사용, 1 페이지](#)
- [업그레이드 체크리스트, 2 페이지](#)
- [Firepower 소프트웨어 새로 설치, 2 페이지](#)

## 가이드 사용

이 가이드는 다음 3개의 주요 부분으로 구성되어 있습니다.

- [업그레이드 준비, 5 페이지](#): 구축 평가, 업그레이드 경로 계획, 업그레이드 패키지 등.
- [Firepower 어플라이언스 업그레이드, 39 페이지](#): 필요한 경우 운영 체제 업그레이드를 포함해 실제 Firepower 어플라이언스 업그레이드 프로세스를 설명합니다. 체크리스트(다음 항목 참조) 및 업그레이드 경로가 포함됩니다.
- [참조, 127 페이지](#): Firepower 업그레이드를 계획 및 실행하는 데 도움이 되는 참고용 정보. 가이드 절차를 이미 숙지하고 있다면 이 가이드를 통해 FAQ(자주 묻는 질문)에 대한 대답을 빠르게 찾을 수 있습니다.

## 업그레이드 체크리스트

이 가이드에서는 Firepower 플랫폼용 업그레이드 체크리스트를 제공합니다. 이러한 체크리스트는 계획과 준비를 포함한 업그레이드 프로세스를 차례로 보여줍니다. 업그레이드할 때마다 체크리스트를 작성하십시오. 단계를 건너뛰면 업그레이드에 실패할 수 있습니다.

플랫폼	체크리스트
Firepower Management Center FMCv 및 FMCv 300을 포함합니다.	<a href="#">업그레이드 체크리스트: Firepower Management Center, 41 페이지</a>
Firepower Threat Defense: <ul style="list-style-type: none"> <li>• Firepower 4100 Series</li> <li>• Firepower 9300</li> </ul>	<a href="#">업그레이드 체크리스트: Firepower 4100/9300 새시의 FTD, 49 페이지</a>
Firepower Threat Defense: <ul style="list-style-type: none"> <li>• Firepower 1000 Series</li> <li>• Firepower 2100 Series</li> <li>• ASA 5500-X Series</li> <li>• ISA 3000</li> <li>• Firepower Threat Defense Virtual</li> </ul>	<a href="#">업그레이드 체크리스트: 기타 FTD 디바이스, 79 페이지</a>
NGIPS 소프트웨어: <ul style="list-style-type: none"> <li>• Firepower 7000/8000 시리즈</li> <li>• NGIPSv</li> </ul>	<a href="#">업그레이드 체크리스트: Firepower 7000/8000 Series 및 NGIPSv, 87 페이지</a>
ASA with FirePOWER Services: <ul style="list-style-type: none"> <li>• ASA 5500-X Series</li> <li>• ISA 3000</li> </ul>	<a href="#">업그레이드 체크리스트: ASA with FirePOWER Services, 95 페이지</a>

## Firepower 소프트웨어 새로 설치

Firepower 어플라이언스를 업그레이드할 수 없거나 필요한 업그레이드 경로를 따르지 않을 경우, 주요 Firepower 릴리스를 새로 설치할 수 있습니다. 이를 이미지 재설치라고도 합니다. 특정 패치를 실행하려면 주요 버전을 설치하고 업그레이드하십시오.

이미지 재설치가 필요하다고 생각되는 경우 사용자의 버전에 대한 [Cisco Firepower 릴리스 노트](#)에서 새로 설치 장을 확인하십시오. 다음을 확인해야 합니다.

- 이미지 재설치가 필요한 시나리오입니다.
- 백업 생성, 어플라이언스 액세스 확인, 라이선스 문제 해결 등 중요한 지침 및 제한 사항.
- 설치 지침 위치.







## 부

# 업그레이드 준비

- 구축 평가, 7 페이지
- 업그레이드 경로 계획, 9 페이지
- Firepower 소프트웨어 업그레이드 패키지 다운로드, 21 페이지
- Firepower 소프트웨어 준비도 확인 실행, 31 페이지
- 업그레이드 전 기타 작업 및 확인, 35 페이지





## 2 장

# 구축 평가

Firepower 어플라이언스를 업그레이드하기 전에 현재 구축 상태를 확인합니다. 이처럼 현재 상태를 파악하면 업그레이드 목표에 따라 업그레이드 방법을 결정할 수 있습니다.

- [구축 평가 질문, 7 페이지](#)
- [현재 버전 정보 찾기, 7 페이지](#)

## 구축 평가 질문

- 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?

## 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.

표 1: 현재 **Firepower** 버전 검색

Component(구성 요소)	플랫폼	버전 정보
Firepower 소프트웨어	Firepower Management Center	FMC에서 <b>Help</b> (도움말) > <b>About</b> (정보)를 선택합니다.
	로 관리되는 디바이스 FMC	FMC에서 <b>Devices</b> (디바이스) > <b>Device Management</b> (디바이스 관리)를 선택합니다.
FXOS	Firepower 4100/9300 새시	FXOS CLI에서 <b>show version</b> 명령을 사용합니다.
ASA OS	ASA with FirePOWER Services	ASA CLI에서 <b>show version</b> 명령을 사용합니다.
가상 호스팅 환경	Firepower 가상 어플라이언스	가상 호스팅 환경 설명서를 참조하십시오.



# 3 장

## 업그레이드 경로 계획

이 지침을 참조하면 업그레이드 경로를 작성하는 데 도움이 됩니다.

- 업그레이드 경로 정보: 업그레이드가 가능합니까?, 9 페이지
- Firepower 소프트웨어 릴리스 유형, 14 페이지
- 사전 설치 패키지 식별(버전 6.0, 6.0.1, 6.1), 18 페이지
- 새 디바이스를 추가할 시기 파악, 19 페이지
- 트래픽 흐름 및 검사에서 중단 식별, 19 페이지
- 기타 주요 작업 확인, 20 페이지

## 업그레이드 경로 정보: 업그레이드가 가능합니까?

업그레이드 경로는 업그레이드 내용 및 시기에 대한 자세한 계획입니다. 일반적으로는 Firepower Management Center을 업그레이드한 뒤 관리되는 디바이스를 업그레이드합니다. 그러나 디바이스를 먼저 업그레이드해야 할 수도 있습니다. 사용 중인 구축을 평가했다면 현재 구축과 원하는 구축에 대해 파악할 수 있으며 업그레이드 경로를 작성할 준비를 할 수 있습니다.



**팁** 중간 버전을 거쳐야 하는 업그레이드 경로가 필요한 경우 시간이 오래 걸릴 수 있습니다. 특히 대체 FMC 및 디바이스 업그레이드를 수행해야 하는 대규모 구축에서는 업그레이드하는 대신 이전 디바이스 이미지를 재설치하는 것이 좋습니다. 먼저 FMC에서 디바이스를 제거합니다. 그런 다음 FMC를 업그레이드하고, 디바이스에 이미지를 재설치하고, FMC에 다시 추가합니다.

두 가지 중요 질문에 '예' 선택

FMC 또는 디바이스를 업그레이드할 때마다 다음 두 가지 질문에 '예'라고 대답해야 합니다.

- 직접 업그레이드가 가능합니까?, 10 페이지
- FMC 디바이스 버전 호환성을 유지할 수 있습니까?, 12 페이지

질문에 대한 답이 '아니오'인 경우 업그레이드 경로가 무효화됩니다.

## 직접 업그레이드가 가능합니까?

여러 버전에서 업그레이드하는 경우가 많습니다. 단, 사용 중인 버전이 '한참 이전 버전'인 경우 중간 업그레이드 또는 전략적 이미지 재설치가 필요할 수 있습니다. 이 테이블에는 Firepower Management Center 및 관리되는 디바이스의 업그레이드 가능 여부가 간략히 나와 있습니다. 각 어플라이언스 유형에 대한 자세한 업그레이드 경로는 업그레이드 장([Firepower 어플라이언스 업그레이드, 39 페이지](#))을 참조하십시오.



**참고** 패치는 네 번째 숫자만 변경할 수 있습니다. 예를 들어, 버전 6.4.0.1로 패치하려면 버전 6.4.0을 실행 중이어야 합니다. 이전 주 버전 또는 유지 보수 릴리스의 패치 레벨로 곧장 건너뛸 수는 없습니다.

### 버전 6.2.3에서 6.6.0으로 직접 업그레이드

이 테이블에는 현재 버전 6.2.3 이상을 실행 중인 경우에 유효한 업그레이드 대상이 간략히 나와 있습니다.

표 2: 버전 6.2.3에서 6.6.0으로 직접 업그레이드

현재 버전	대상 버전: 직접 업그레이드 지원				
	6.7.0/6.7.x로 업그레이드	6.6.0/6.6.x	6.5.0	6.4.0	6.3.0
6.6.0/6.6.x에서 업그레이드	예	—	—	—	—
6.5.0	예	예	—	—	—
6.4.0	예	예	예	—	—
6.3.0	예	예	예	예	—
6.2.3	—	예	예	예	예

### 버전 5.4에서 6.2.2로 직접 업그레이드

이 테이블에는 현재 버전 5.4~6.2.2를 실행 중인 경우에 유효한 업그레이드 대상이 간략히 나와 있습니다.

표 3: 버전 5.4에서 6.2.2로 직접 업그레이드

현재 버전	대상 버전: 직접 업그레이드 지원								
	6.4.0으로 업그레이드	6.3.0	6.2.3	6.2.2	6.2.1	6.2.0	6.1.0	6.0.1	6.0.0
6.2.2에서 업그레이드	예	예	예	—	—	—	—	—	—
6.2.1	예	예	예	예	—	—	—	—	—
6.2.0	예	예	예	예	—	—	—	—	—
6.1.0	예 †	예 †	예	—	—	예	—	—	—
6.0.1	—	—	—	—	—	—	예	—	—
6.0.0	—	—	—	—	—	—	—	예	—
5.4.x	—	—	—	—	—	—	—	—	예*

## 업그레이드할 최소 버전별 직접 업그레이드

즉, 최소한 오른쪽 열의 버전을 실행하고 있어야 왼쪽 열의 대상 버전으로 직접 업그레이드할 수 있습니다.

표 4: 업그레이드할 최소 버전별 직접 업그레이드

대상 버전	직접 업그레이드에 필요한 최소 현재 버전
6.7.0 또는 모든 6.7.x 유지 보수 릴리스	6.3.0
6.6.0 또는 모든 6.6.x 유지 보수 릴리스	6.2.3
6.5.0	6.2.3
6.4.0	6.1.0 †
6.3.0	6.1.0 †
6.2.3	6.1.0
6.2.2	6.2.0
6.2.1	버전 6.2.1로의 업그레이드는 지원되지 않습니다.
6.2.0	6.1.0
6.1.0	6.0.1

## FMC 디바이스 버전 호환성을 유지할 수 있습니까?

대상 버전	직접 업그레이드에 필요한 최소 현재 버전
6.0.1	6.0.0
6.0.0	5.4.0.2 또는 5.4.1.1

\* 버전 6.0으로 업그레이드하려면 적어도 버전 5.4.0.2/5.4.1.1을 실행 중이어야 합니다.

† 운영체제가 호환되지 않으므로 Firepower 4100/9300 Series 디바이스에서는 버전 6.1에서 6.4로 직접 업그레이드할 수 없습니다. 비슷한 이유로 버전 6.1에서 6.3으로 업그레이드하지 않는 것이 좋습니다. 버전 6.1을 실행 중인 경우, FXOS 2.3.1에서 버전 6.2.3으로 업그레이드한 다음에 그 이후 버전으로 업그레이드하는 것이 좋습니다.

## FMC 디바이스 버전 호환성을 유지할 수 있습니까?

Firepower Management Center는 관리되는 디바이스와 동일하거나 최신 버전을 실행해야 합니다. 이것은 다음을 의미합니다:

- 일반적으로 몇 가지 주요 버전인 최신 FMC로 이전 디바이스를 관리할 수 있습니다.

예를 들어, 버전 6.7.0 FMC는 버전 6.3.0 디바이스를 관리할 수 있습니다.

- FMC 이상으로 디바이스를 업그레이드할 수 없습니다.

FMC 업그레이드 전, 업그레이드된 FMC가 현재 디바이스를 관리할 수 있는지 확인합니다. 예를 들어, 버전 6.7.1 FMC는 버전 6.7.0 디바이스를 관리할 수 있어도 버전 6.7.2 디바이스는 관리할 수 없습니다.

아래에는 관리할 수 있는 FMC 버전 및 디바이스가 나와 있습니다. 첫 번째 열에서 현재 버전을 찾은 다음, 가로로 읽으며 관리할 수 있는 디바이스를 확인합니다. 주 버전 내에서 FMC는 관리되는 디바이스와 동일하거나 새로운 유지 보수(3자리) 릴리스를 실행해야 합니다.

표 5: FMC 관리 기능: 버전 6.2.3 이상

FMC 버전	관리 가능: 디바이스 버전									
	6.7.x	6.6.x	6.5.0	6.4.0	6.3.0	6.2.3	6.2.2	6.2.1	6.2.0	6.1.0
6.7.x	예	예	예	예	예	—	—	—	—	—
6.6.x	—	예	예	예	예	예	—	—	—	—
6.5.0	—	—	예	예	예	예	—	—	—	—
6.4.0	—	—	—	예	예	예	예	예	예	예
6.3.0	—	—	—	—	예	예	예	예	예	예
6.2.3	—	—	—	—	—	예	예	예	예	예



표 6: FMC 관리 기능: 버전 5.4.0-6.2.2

FMC 버전	관리 가능: 디바이스 버전							
	6.2.2	6.2.1	6.2.0	6.1.0	6.0.1	6.0.0	5.4.1	5.4.0
6.2.2	예	예	예	예	—	—	—	—
6.2.1	—	예	예	예	—	—	—	—
6.2.0	—	—	예	예	—	—	—	—
6.1.0	—	—	—	예	예	예	예*	예*
6.0.1	—	—	—	—	예	예	예*	예*
6.0.0	—	—	—	—	—	예	예*	예*
5.4.1	—	—	—	—	—	—	예	예
5.4.0	—	—	—	—	—	—	—	예

\* 디바이스가 FMC 버전 6.0, 6.0.1 또는 6.1로 관리되려면 적어도 버전 5.4.0.2/5.4.1.1을 실행해야 합니다.

기술적으로 패치가 적용되지 않은 FMC를 사용하는 패치된 디바이스(4자리 릴리스)를 관리할 수는 있습니다. 그러나 이는 별로 권장되지 않습니다. 항상 전체 구축을 업데이트해야 합니다. 새로운 기능을 사용하고 해결된 문제를 적용하려면 FMC와 관리되는 디바이스 모두에서 최신 릴리스를 사용해야 하는 경우가 많습니다.

## 시작해야 하는 위치

대부분의 경우 FMC를 먼저 업그레이드합니다. FMC-디바이스 호환성을 계속 유지하면서 최대 수준까지 업그레이드해야 합니다. 그러나 디바이스가 너무 오래된 경우, 디바이스를 FMC와 동일한 주 버전으로 업그레이드하는 것부터 시작해야 합니다.

그래도 어디서부터 시작해야 할지 확실치 않은 경우에는 구축 평가를 참조하고 아래에서 현재 FMC-디바이스 버전 조합을 찾아보십시오. 이러한 권장 사항에서는 직접 업그레이드 기능 및 FMC-디바이스 호환성을 고려합니다.

이 테이블에서는 최신 주 버전/유지 보수 릴리스(현재 버전 **6.7.0/6.7.x**)로 업그레이드한다고 가정합니다.

표 7: 버전 6.7.x로 Firepower 업그레이드 시작

현재 구축		권장 첫 단계	
FMC	디바이스	업그레이드	수신
6.7.x	6.3.0~6.7.x	FMC	모든 6.7.x 이후 유지 보수 릴리스
6.6.x	6.3.0~6.6.x	FMC	6.7.x
	6.2.3	디바이스	6.6.x
6.5.0	6.3.0~6.5.0	FMC	6.7.x
	6.2.3	디바이스	6.5.0
6.4.0	6.3.0~6.4.0	FMC	6.7.x
	6.1.0~6.2.3	디바이스	6.4.0
6.3.0	6.3.0	FMC	6.7.x
	6.1.0~6.2.3	디바이스	6.3.0
6.2.3	6.2.3	FMC	6.6.x
	6.1.0~6.2.2	디바이스	6.2.3
6.2.2	6.1.0~6.2.2	FMC	6.4.0
6.2.1	6.1.0~6.2.1	FMC	6.4.0
6.2.0	6.1.0~6.2.0	FMC	6.4.0
6.1.0	6.1.0	FMC	6.4.0
	5.4.0~6.0.1	디바이스	6.1.0
6.0.1	5.4.0~6.0.1	FMC	6.1.0
6.0.0	5.4.0~6.0.0	FMC	6.0.1
5.4.x	5.4.x	FMC	6.0.0

## Firepower 소프트웨어 릴리스 유형

Cisco에서는 3가지 레벨의 Firepower 소프트웨어 릴리스(주 버전, 유지 보수 및 패치)를 제공합니다.



**참고** 유지 보수 릴리스에는 버전 6.6.x가 도입되었습니다. 버전 6.0.1, 6.2.1, 6.2.2 및 6.2.3은 세 번째 숫자가 변경된 것이지만, 주요 릴리스로 간주됩니다.

자세한 내용은 [Cisco NGFW 제품 라인 소프트웨어 출시 및 유지보수 게시판](#)을 참조하십시오.

#### 주요 릴리스

주요 릴리스에는 새로운 기능과 향상된 기능이 포함되어 있습니다. 여기에는 인프라 또는 아키텍처 변경 사항이 포함될 수 있습니다.

표 8: 주요 릴리스

특성	세부정보
번호 지정 체계	다음과 같이 첫 번째 또는 두 번째 숫자를 변경합니다. <ul style="list-style-type: none"> <li>• 5.0, 6.0, 7.0 ...</li> <li>• 5.3, 5.4 ...</li> <li>• 6.1, 6.2 ...</li> </ul>
업그레이드 경로	여러 버전에서 대부분의 주요 릴리스로 업그레이드할 수 있습니다. 사용 중인 버전이 '한참 이전 버전'인 경우 중간 업그레이드가 필요할 수 있습니다. 대표적인 예는 다음과 같습니다. <ul style="list-style-type: none"> <li>• 6.1에서 6.7은 지원되지 않습니다.</li> <li>• 6.3에서 6.7은 지원됩니다.</li> </ul> 자세한 내용은 플랫폼에 지원되는 업그레이드 경로를 참조하십시오.
운영체제 업그레이드	Firepower 4100/9300 새시의 경우, FXOS를 업그레이드해야 합니다. ASA FirePOWER의 경우, 문제를 해결하려면 ASA 업그레이드가 필요할 수 있습니다.
직접 다운로드	아니요. 주요 업그레이드에서는 직접 다운로드가 지원되지 않습니다. Cisco 지원 및 다운로드 사이트에서 다운로드해야 합니다.
새로 설치(이미지 재설치)	예. 주요 릴리스로 이미지를 재설치할 수 있습니다.

특성	세부정보
제거 중	아니요. FMC 구축에서는 주요 릴리스를 제거하거나 되돌릴 수 없습니다. 이전 버전으로 돌아가려면 이미지를 재설치해야 합니다. 그렇기 때문에 업그레이드 전에 백업하는 것이 좋습니다.

### 유지 보수 릴리스

유지 보수 릴리스에는 일반적인 버그 및 보안 관련 수정 사항이 포함되어 있습니다. 동작 변경은 거의 포함되지 않으며, 동작 변경이 포함되는 경우 이러한 수정과 관련이 있습니다.

표 9: 유지 보수 릴리스

특성	세부정보
번호 지정 체계	다음과 같이 세 번째 숫자를 변경합니다. <ul style="list-style-type: none"> <li>• 6.6.1, 6.6.2 ...</li> <li>• 6.7.1, 6.7.2 ...</li> </ul>
업그레이드 경로	여러 버전에서 유지 보수 릴리스로 업그레이드할 수 있습니다. 사용 중인 버전이 '한참 이전 버전'인 경우 중간 업그레이드가 필요할 수 있습니다. 대표적인 예는 다음과 같습니다. <ul style="list-style-type: none"> <li>• 6.1에서 6.6.1은 지원되지 않습니다.</li> <li>• 6.2.3에서 6.6.1은 지원됩니다.</li> </ul> 자세한 내용은 플랫폼에 지원되는 업그레이드 경로를 참조하십시오.
운영체제 업그레이드	문제를 해결하려면 운영체제를 패치해야 할 수 있습니다.
직접 다운로드	FMC는 수동 다운로드가 제공된 후 일정 시간이 지나고 나서 유지 보수 릴리스를 직접 다운로드할 수 있습니다. 지연되는 기간은 릴리스 채택 및 기타 요인에 따라 달라집니다.
새로 설치(이미지 재설치)	예. 유지 보수 릴리스로 이미지를 재설치 할 수 있습니다.
제거 중	아니요. FMC 구축에서는 유지 보수 릴리스를 제거하거나 되돌릴 수 없습니다. 이전 버전으로 돌아가려면 이미지를 재설치해야 합니다. 그렇기 때문에 업그레이드 전에 백업하는 것이 좋습니다.

## 패치

패치는 온디맨드 업데이트로, 시급한 중요 수정 사항만을 제공합니다.



참고 버전 6.6 이전에는 대부분의 패치에 구체적인 대상이 지정되지 않았습니다.

표 10: 패치

특성	세부정보
번호 지정 체계	다음과 같이 네 번째 숫자를 변경합니다. <ul style="list-style-type: none"> <li>• 6.6.0.1, 6.6.0.2 ...</li> <li>• 6.6.1.1, 6.6.1.2 ...</li> </ul>
업그레이드 경로	패치는 네 번째 숫자만 변경할 수 있습니다. 대표적인 예는 다음과 같습니다. <ul style="list-style-type: none"> <li>• 6.4.0에서 6.4.0.10은 지원됩니다. 패치는 누적 방식으로 적용됩니다. 언제든지 주요 릴리스 또는 유지 보수 릴리스에 최신 패치를 설치할 수 있습니다.</li> <li>• 6.4.0에서 6.5.0.4는 지원되지 않습니다. 이 경우 패치를 적용하기 전에 6.5.0으로 업그레이드해야 합니다.</li> </ul>
운영체제 업그레이드	문제를 해결하려면 운영체제를 패치해야 할 수 있습니다.
직접 다운로드	FMC 구축: <ul style="list-style-type: none"> <li>• 6.6.0 이상 버전 불가능 특수 예외 사항이 적용될 수 있습니다.</li> <li>• 6.5.0 이하 버전 가능 단, 2020년 중반 이후에는 유지 보수 릴리스와 동일한 지연을 구현했습니다.</li> </ul>
새로 설치(이미지 재설치)	아니요. 패치 레벨로 곧바로 이미지를 재설치할 수 없습니다.

특성	세부정보
제거 중	<p>FMC 구축에서는 대부분의 패치를 제거할 수 있습니다. 개별 예외 사항은 릴리스 노트를 참조하십시오.</p> <p>다음에서 패치를 제거할 수 있습니다.</p> <ul style="list-style-type: none"> <li>6.2.3 이상에서 패치를 제거하면 업그레이드한 패치 레벨로 돌아갑니다.</li> <li>6.2.2 이하에서 패치를 제거하면 시작 위치에 관계없이 이전에 릴리스된 패치로 돌아갑니다.</li> </ul>

## 사전 설치 패키지 식별(버전 6.0, 6.0.1, 6.1)

일부 플랫폼에서 업그레이드하는 경우 업그레이드를 최적화하고, 특정 업그레이드 기능을 활성화하거나 업그레이드 문제를 수정하는 사전 설치 패키지 또는 핫픽스를 제공합니다.

사전 설치 패키지 및 핫픽스는 업그레이드 및 설치 패키지와 동일한 위치인 Cisco 지원 및 다운로드 사이트에서 받을 수 있습니다. 일반 업그레이드 패키지와 동일하게 FMC 관련 **System(시스템) > Update(업데이트)** 페이지를 사용해 사전 설치 또는 핫픽스를 실행합니다. 이 작업은 업그레이드 전에 수행하는 것이 좋습니다.

표 11: Firepower 사전 설치 패키지

대상 버전	플랫폼	심각도	세부정보
6.1.0	FMC & FMCv 모든 장치	선택 사항	<p>버전 6.1.0 업그레이드에 대한 준비도 상태를 검사할 수 있습니다.</p> <p>버전 6.1.0 이후에는 준비도 확인이 업그레이드 패키지에 포함되어 있습니다.</p> <p>참조: <a href="#">Firepower System 릴리스 노트 버전 6.1.0 사전 설치 패키지</a></p>
6.1.0	HA 쌍의 FTD 디바이스	선택 사항	<p>FTD HA 쌍의 무중단 업그레이드를 허용합니다.</p> <p>사전 설치를 하지 않고 버전 6.1.0로 업그레이드하기 전 고가용성을 해제해야 합니다.</p> <p>참조: <a href="#">Firepower System 릴리스 노트 버전 6.1.0 사전 설치 패키지</a></p>

대상 버전	플랫폼	심각도	세부정보
6.0.1	FMC & FMCv	필수	업그레이드를 최적화합니다. 참조: <a href="#">Firepower System 릴리스 노트 버전 6.0.1 사전 설치</a>
6.0.0	FMC & FMCv 모든 장치	필수 버전: • 5.4.0.2 ~ 5.4.0.6 • 5.4.1.1 ~ 5.4.1.5  권장 버전: • 5.4.0.7 이상 • 5.4.1.6 이상	업그레이드를 최적화합니다. STIG 모드에서 어플라이언스를 업그레이드할 수 있습니다. 참조: <a href="#">FireSIGHT 시스템 릴리스 노트 버전 6.0.0 사전 설치</a>

## 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 FMC를 업그레이드하지 마십시오.
- 가상 디바이스: FMC를 대상 버전으로 업그레이드한 후에 생성합니다. 새 가상 디바이스를 추가할 때는 주 버전 업그레이드를 수행해서는 안 되며 패치만 수행해야 합니다.

## 트래픽 흐름 및 검사에서 중단 식별

업그레이드 중 트래픽 흐름 및 검사에서 잠재적인 중단을 식별해야 합니다. 다음과 같은 경우 발생할 수 있습니다.

- 디바이스를 재부팅할 때.
- 디바이스에서 운영 체제 또는 가상 호스팅 환경을 업그레이드할 때
- 디바이스에서 Firepower 소프트웨어를 업그레이드하거나 패치를 제거할 때
- 업그레이드 또는 삭제 프로세스의 일부로 구성 변경 사항을 배포할 때(Snort 프로세스가 다시 시작).

디바이스 유형, 구축 유형(독립형, 고가용성, 클러스터) 및 인터페이스 구성(패시브, IPS, 방화벽 등)은 중단 특성을 결정합니다. Cisco는 유지 보수 기간 또는 중단으로 구축에 가장 적은 영향이 발생할 때 업그레이드 또는 삭제를 수행할 것을 강력하게 권장합니다.

자세한 내용은 [트래픽 흐름, 검사 및 디바이스 동작, 241 페이지](#)를 참고하십시오.

## 기타 주요 작업 확인

업그레이드 프로세스의 대다수 단계는 시간이 매우 많이 걸릴 수 있습니다. 계획에 이러한 단계를 명시적으로 포함해야 합니다. 여기에는 다음이 해당되지만 이에 국한되지는 않습니다.

- 백업 -백업 수행, [36 페이지](#)
- 다운로드 및 푸시 -[Firepower 소프트웨어 업그레이드 패키지 다운로드, 21 페이지](#)
- 준비도 확인 -[Firepower 소프트웨어 준비도 확인 실행, 31 페이지](#)
- 업그레이드 전/후 컨피그레이션 변경 -[구성 변경 계획, 36 페이지](#)





## 4 장

# Firepower 소프트웨어 업그레이드 패키지 다운로드

Firepower 소프트웨어를 업그레이드하려면 소프트웨어 업그레이드 패키지가 어플라이언스에 있어야 합니다.

- [Firepower 소프트웨어 업그레이드 패키지 정보, 21 페이지](#)
- [업그레이드 패키지 관리를 위한 지침 및 제한 사항, 23 페이지](#)
- [Firepower 소프트웨어 업그레이드 패키지 다운로드, 24 페이지](#)
- [FMC에 Firepower 소프트웨어 업그레이드 패키지 업로드, 26 페이지](#)
- [내부 서버에서 FTD 업그레이드 패키지 가져오기, 27 페이지](#)
- [FMC 관리 디바이스로 업그레이드 패키지 푸시, 28 페이지](#)

## Firepower 소프트웨어 업그레이드 패키지 정보

Firepower 소프트웨어를 업그레이드하거나 준비도 확인을 실행하려면 소프트웨어 업그레이드 패키지가 어플라이언스에 있어야 합니다.

버전 6.5.0 이하에서는 FMC 관리 디바이스가 FMC에서 업그레이드 패키지를 가져와야 합니다. 즉, FMC 및 디바이스 업그레이드 패키지를 모두 FMC에 업로드해야 합니다. 버전 6.6.0에서는 FTD 업그레이드 패키지의 소스로 FMC 대신 자체 내부 웹 서버를 사용할 수 있는 기능이 추가되었습니다. 이는 FTD 업그레이드 패키지가 더 이상 FMC를 '통과'해야 할 필요가 없음을 의미합니다.

이 테이블에서는 FMC에 업그레이드 패키지를 가져오는 방법을 설명합니다.

표 12: FMC에 Firepower 소프트웨어 업그레이드 패키지 가져오기

방법	세부정보
수동	Cisco 지원 및 다운로드 사이트에서 다운로드한 다음 FMC에 업로드합니다. <a href="#">Firepower 소프트웨어 업그레이드 패키지 다운로드, 24 페이지</a> 및 <a href="#">FMC에 Firepower 소프트웨어 업그레이드 패키지 업로드, 26 페이지</a> 를 참조하십시오.

방법	세부정보
Cisco에서 직접	<p>버전 6.2.3~6.5.0 Firepower 패치 및 모든 유지 보수 릴리스(3자리 업그레이드)가 수동 다운로드용으로 제공되고 약 2주 후에 Cisco에서 인터넷에 액세스할 수 있는 FMC가 이를 직접 다운로드할 수 있습니다. 다음은 Cisco에서 직접 다운로드할 수 없습니다.</p> <ul style="list-style-type: none"> <li>• 주요 릴리스</li> <li>• 버전 6.6 이상에 대한 대부분의 패치</li> </ul> <p><a href="#">Cisco에서 직접 업그레이드 패키지 다운로드, 26 페이지</a>의 내용을 참조하십시오.</p>

이 테이블에서는 FMC 관리 디바이스에 업그레이드 패키지를 가져오는 방법을 설명합니다.

표 13: FMC 관리 디바이스에 Firepower 소프트웨어 업그레이드 패키지 가져오기

방법	소스	세부정보	장점	지원되는 버전/플랫폼
업그레이드 전에 패키지를 복사(푸시)합니다. 권장.	FMC	<p>디바이스업그레이드 패키지를 FMC에 업로드하되, 디바이스에 언제 복사할지 선택합니다.</p> <p><a href="#">FMC 관리 디바이스로 업그레이드 패키지 푸시, 28 페이지</a>의 내용을 참조하십시오.</p>	업그레이드 유지 보수 기간을 줄일 수 있습니다.	버전 6.2.3 FMC
	내부 웹 서버	<p>FTD 업그레이드 패키지의 소스로 FMC 대신 내부 웹 서버를 설정하고, 다음으로 패키지를 디바이스에 언제 복사할지 선택합니다.</p> <p><a href="#">내부 서버에서 FTD 업그레이드 패키지 가져오기, 27 페이지</a> 및 <a href="#">FMC 관리 디바이스로 업그레이드 패키지 푸시, 28 페이지</a>를 참조하십시오.</p>	<p>업그레이드 유지 보수 기간을 줄일 수 있습니다.</p> <p>FMC와 해당 디바이스 간의 대역폭이 제한되어 있는 경우 유용합니다.</p> <p>FMC 공간을 절약합니다.</p>	버전 6.6.0 이상 FTD 디바이스

방법	소스	세부정보	장점	지원되는 버전/플랫폼
업그레이드의 일부로 패키지를 복사합니다.  디바이스 업그레이드를 시작하면 시스템에서 첫 번째 작업으로 업그레이드 패키지를 디바이스에 복사합니다.	FMC	디바이스를 업그레이드하기 전에 FMC에 디바이스 업그레이드 패키지를 업로드합니다.  이전 테이블을 참조하십시오.	—	모두  FMC가 버전 6.2.2 이하이면 이 옵션만 선택할 수 있습니다.
	내부 웹 서버	디바이스 업그레이드 패키지를 내부 웹 서버에 업로드합니다. 그런 다음 FMC 대신 서버에서 업그레이드 패키지를 가져오도록 FTD 디바이스를 설정합니다.  <a href="#">내부 서버에서 FTD 업그레이드 패키지 가져오기, 27 페이지</a> 의 내용을 참조하십시오.	FMC와 해당 디바이스 간의 대역폭이 제한되어 있는 경우 유용합니다.  FMC 공간을 절약합니다.	버전 6.6.0 이상 FTD 디바이스

## 업그레이드 패키지 관리를 위한 지침 및 제한 사항

다음 지침 및 제한 사항은 업그레이드 패키지를 가져오고 관리하는 데 적용됩니다.

### 고가용성 FMC

FMC 고가용성 구축에서는 업그레이드 패키지를 활성/기본 FMC와 스탠바이/보조 FMC로 모두 전송해야 합니다. 또한 스탠바이 FMC로 패키지를 전송하기 전 동기화를 일시 중단해야 합니다.

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

- 활성 FMC: 업그레이드 준비 단계에서 패키지를 전송합니다.
- 스탠바이 FMC: 동기화를 일시 중단한 후 실제 업그레이드 프로세스의 일부로 패키지를 전송합니다.

자세한 내용은 [고가용성 FMC 업그레이드, 46 페이지](#)를 참조하십시오.

**FXOS** 업그레이드 전에 **Firepower** 업그레이드 패키지 푸시

FTD를 사용하는 Firepower 4100/9300의 경우, 필수 컴패니언 FXOS 업그레이드를 시작하기 전에 Firepower 업그레이드 패키지를 푸시하는 것이 좋습니다.



참고 버전 6.1.0에서 버전 6.3.0 또는 6.4.0으로 직접 업그레이드하려면 FMC에서 푸시해야 합니다. FXOS를 업그레이드하기 전에 반드시 푸시해야 합니다.

## 대역폭 확인

Firepower 업그레이드 패키지 크기는 다양합니다. 관리 네트워크에 대용량 데이터 전송을 수행할 대역폭이 있는지 확인합니다. 자세한 내용은 [Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침](#)(문제해결 TechNote)을 참조하십시오.

## Firepower 소프트웨어 업그레이드 패키지 다운로드

Firepower 소프트웨어 업그레이드 패키지는 Cisco 지원 및 다운로드 사이트에서 제공됩니다.

- Firepower Management Center(FMCv 포함): <https://www.cisco.com/go/firepower-software>
- Firepower Threat Defense(ISA 3000): <https://www.cisco.com/go/isa3000-software>
- Firepower Threat Defense(FTDv를 포함한 기타 모든 모델): <https://www.cisco.com/go/ftd-software>
- Firepower 7000 시리즈: <https://www.cisco.com/go/7000series-software>
- Firepower 8000 시리즈: <https://www.cisco.com/go/8000series-software>
- ASA with FirePOWER Services(ASA 5500-X Series): <https://www.cisco.com/go/asa-firepower-sw>
- ASA with FirePOWER Services(ISA 3000): <https://www.cisco.com/go/isa3000-software>
- NGIPSv: <https://www.cisco.com/go/ngipsv-software>

업그레이드 패키지를 찾으려면 Firepower 어플라이언스 모델을 선택하거나 검색한 다음, 현재 버전의 Firepower 소프트웨어 다운로드 페이지로 이동하십시오. 사용 가능한 업그레이드 패키지는 설치 패키지, 핫픽스 및 기타 해당 다운로드와 함께 나열됩니다.

제품군 또는 시리즈의 모든 Firepower 모델에 동일한 업그레이드 패키지를 사용하십시오. 업그레이드 패키지 파일 이름은 플랫폼, 패키지 유형(업그레이드, 패치, 핫픽스) 및 Firepower 버전을 반영합니다. 유지 보수 릴리스에서는 업그레이드 패키지 유형을 사용합니다.

대표적인 예는 다음과 같습니다.

- 패키지: Cisco\_Firepower\_Mgmt\_Center\_Upgrade-6.6.0-90.sh.REL.tar
- 플랫폼: Firepower Management Center
- 패키지 유형: 업그레이드

- 버전 및 빌드: 6.6.0-90
- 파일 확장명: sh.REL.tar

버전 6.2.1 이상의 업그레이드 패키지는 서명된 tar 아카이브(.tar)입니다. 압축을 풀지 마십시오. 업그레이드 패키지를 이메일로 전송하지 마십시오.

표 14: Firepower 소프트웨어 업그레이드 패키지 명명 체계

Platform(플랫폼)	버전	패키지
FMC/FMCv	6.3.0 이상	Cisco_Firepower_Mgmt_Center
	5.4.0~6.2.3	Sourcefire_3D_Defense_Center_S3
Firepower 1000 Series	Any(모든 상태)	Cisco_FTD_SSP-FP1K
Firepower 2100 Series	Any(모든 상태)	Cisco_FTD_SSP-FP2K
Firepower 4100/9300 채시	Any(모든 상태)	Cisco_FTD_SSP
ASA 5500-X series with FTD ISA 3000 with FTD FTDv	Any(모든 상태)	Cisco_FTD
Firepower 7000/8000 시리즈 AMP 모델	6.3.0~6.4.0	Cisco_Firepower_NGIPS_Appliance
	5.4.0~6.2.3	Sourcefire_3D_Device_S3
ASA FirePOWER	Any(모든 상태)	Cisco_Network_Sensor
NGIPSv	6.3.0 이상	Cisco_Firepower_NGIPS_Virtual
	6.2.2~6.2.3	Sourcefire_3D_Device_VMware
	5.4.0~6.2.0	Sourcefire_3D_Device_Virtual64_VMware

#### 운영체제 업그레이드 패키지

운영체제 업그레이드 패키지에 대한 자세한 내용은 다음 설명서의 업그레이드 계획 장을 참조하십시오.

- [Cisco ASA 업그레이드 설명서](#), ASA OS용
- [Cisco Firepower 4100/9300 업그레이드 설명서](#), FXOS용

## Cisco에서 직접 업그레이드 패키지 다운로드

인터넷에 액세스할 수 있는 FMC는 Cisco에서 직접 선택한 업그레이드 패키지를 가져올 수 있습니다. [Firepower 소프트웨어 업그레이드 패키지 정보, 21 페이지](#)를 참조하십시오.

시작하기 전에

고가용성 쌍의 스탠바이 FMC를 사용 중인 경우 동기화를 일시 정지합니다. [업그레이드 패키지 관리를 위한 지침 및 제한 사항, 23 페이지](#)의 내용을 참조하십시오.

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

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

FMC에서는 구축에 적합한 모든 패키지와 필요한 경우 최신 VDB를 다운로드합니다.

검색된 업그레이드 패키지의 수와 패키지를 검색하는 시간은 현재 구축이 최신 상태인지, 얼마나 많은 디바이스 유형을 보유하고 있는지에 따라 달라집니다.

다음에 수행할 작업

사용 중인 플랜을 참조하십시오. 선택 사항이지만, 업그레이드 패키지를 관리되는 디바이스에 복사하는 것이 좋습니다. [FMC 관리 디바이스로 업그레이드 패키지 푸시, 28 페이지](#)의 내용을 참조하십시오.

## FMC에 Firepower 소프트웨어 업그레이드 패키지 업로드

다음 절차를 사용하여 업그레이드 패키지를 디바이스 자체와 관리하는 디바이스용 FMC에 수동으로 업로드합니다.

시작하기 전에

- Cisco 지원 및 다운로드 사이트에서 적절한 업그레이드 패키지를 다운로드합니다. [Firepower 소프트웨어 업그레이드 패키지 다운로드, 24 페이지](#)의 내용을 참조하십시오.
- 고가용성 쌍의 스탠바이 FMC를 사용 중인 경우 동기화를 일시 정지합니다. [업그레이드 패키지 관리를 위한 지침 및 제한 사항, 23 페이지](#)의 내용을 참조하십시오.

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

단계 2 **Upload Update(업데이트 업로드)**를 클릭합니다.

단계 3 (버전 6.6.0 이상) **Action(작업)**에서 **Upload local software update package(로컬 소프트웨어 업데이트 패키지 업로드)** 라디오 버튼을 클릭합니다.

단계 4 **Choose File(파일 선택)**을 클릭합니다.

단계 5 패키지를 찾은 다음 업로드를 클릭합니다.

다음에 수행할 작업

사용 중인 플랜을 참조하십시오. 선택 사항이지만, 디바이스 업그레이드 패키지를 관리되는 디바이스에 복사하는 것이 좋습니다. [FMC 관리 디바이스로 업그레이드 패키지 푸시](#), 28 페이지의 내용을 참조하십시오.

## 내부 서버에서 FTD 업그레이드 패키지 가져오기

버전 6.6.0부터 Firepower Threat Defense 디바이스는 FMC가 아닌 내부 웹 서버에서 업그레이드 패키지를 가져올 수 있습니다. 이는 FMC와 해당 디바이스 간의 대역폭이 제한된 경우 특히 유용합니다. 또한 FMC의 공간을 절약합니다.



**참고** 이 기능은 버전 6.6.0 이상을 실행하는 FTD 디바이스에서만 지원됩니다. 버전 6.6.0으로의 업그레이드에는 지원되지 않으며, FMC 또는 클래식 디바이스에서는 지원되지 않습니다.

이 기능을 설정하려면 웹 서버의 업그레이드 패키지 위치에 포인터(URL)를 저장하십시오. 그러면 업그레이드 프로세스가 FMC 대신 웹 서버에서 업그레이드 패키지를 가져옵니다. 업그레이드 전에 FMC에서 푸시 기능을 사용하여 패키지를 복사할 수도 있습니다.

각 FTD 업그레이드 패키지에 대해 이 절차를 반복합니다. 업그레이드 패키지당 하나의 위치만 설정할 수 있습니다.

시작하기 전에

- Cisco 지원 및 다운로드 사이트에서 적절한 업그레이드 패키지를 다운로드합니다. [Firepower 소프트웨어 업그레이드 패키지 다운로드](#), 24 페이지의 내용을 참조하십시오.
- FTD 디바이스가 액세스할 수 있는 내부 웹 서버에 업그레이드 패키지를 복사합니다.
- 보안 웹 서버(HTTPS)의 경우, 서버의 디지털 인증서(PEM 형식)를 가져옵니다. 서버 관리자로부터 인증서를 얻을 수 있어야 합니다. 브라우저 또는 OpenSSL과 같은 툴을 사용하여 서버의 인증서 세부 정보를 보고 인증서를 내보내거나 복사할 수도 있습니다.

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

단계 2 **Upload Update(업데이트 업로드)**를 클릭합니다.

아무것도 업로드하지 않더라도 이 옵션을 선택합니다. 다음 페이지에서 URL을 입력하라는 프롬프트가 표시됩니다.

단계 3 **Action(작업)**에서 **Specify software update source(소프트웨어 업데이트 소스 지정)** 라디오 버튼을 클릭합니다

단계 4 업그레이드 패키지의 소스 URL을 입력합니다.

프로토콜(HTTP/HTTPS) 및 전체 경로를 제공합니다. 예를 들면, 다음과 같습니다.

```
https://internal_web_server/upgrade_package.sh.REL.tar
```

업그레이드 패키지 파일 이름은 플랫폼, 패키지 유형(업그레이드, 패치, 핫픽스) 및 업그레이드하려는 Firepower 버전을 반영하도록 합니다. 올바른 파일 이름을 입력했는지 확인하십시오.

단계 5 HTTPS 서버의 경우, CA 인증서를 제공합니다.

이 인증서는 이전에 얻은 서버의 디지털 인증서입니다. BEGIN CERTIFICATE(인증서 시작) 및 END CERTIFICATE(인증서 끝)를 포함하는 전체 텍스트 블록을 복사하여 붙여넣습니다.

단계 6 Save(저장)를 클릭합니다.

Product Updates(제품 업데이트) 페이지로 다시 연결됩니다. 업로드된 업그레이드 패키지 및 업그레이드 패키지 URL이 함께 나열되지만, 구별을 위해 레이블이 서로 다르게 지정됩니다.

다음에 수행할 작업

사용 중인 플랜을 참조하십시오. 선택 사항이지만, 디바이스 업그레이드 패키지를 디바이스에 복사하는 것이 좋습니다. [FMC 관리 디바이스로 업그레이드 패키지 푸시, 28 페이지](#)를 참조하십시오.

## FMC 관리 디바이스로 업그레이드 패키지 푸시

버전 6.2.3부터는 업그레이드 전에 FMC에서 업그레이드 패키지를 복사하거나 푸시할 수 있습니다. 따라서 업그레이드 유지 보수 기간을 줄일 수 있습니다. 버전 6.6.0에서는 FTD 업그레이드 패키지의 소스로 FMC 대신 내부 웹 서버를 사용할 수 있는 기능이 추가되었습니다.

푸시하면 각 디바이스가 소스에서 개별적으로 업그레이드 패키지를 가져옵니다. 시스템은 클러스터, 스택 또는 HA 멤버 유닛 간에 업그레이드 패키지를 복사하지 않습니다.

업그레이드 전에 푸시하지 않으면 디바이스는 업그레이드 프로세스의 첫 번째 단계로 업그레이드 패키지를 가져옵니다.

시작하기 전에

Firepower 업그레이드 패키지 크기는 다양합니다. 관리 네트워크에 대용량 데이터 전송을 수행할 대역폭이 있는지 확인합니다. 자세한 내용은 [Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침](#)(문제해결 TechNote)을 참조하십시오.

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

단계 2 업그레이드 패키지를 디바이스가 가져올 수 있는 곳에 저장합니다. 선택:

- FMC

패키지를 FMC에 수동으로 업로드하거나 직접 검색합니다. [FMC에 Firepower 소프트웨어 업그레이드 패키지 업로드, 26 페이지](#) 또는 [Cisco에서 직접 업그레이드 패키지 다운로드, 26 페이지](#)를 참조하십시오.

- 내부 웹 서버(FTD 버전 6.6.0 이상)



내부 웹 서버에 업로드하고 해당 서버에서 패키지를 가져오도록 FTD 디바이스를 설정합니다. [내부 서버에서 FTD 업그레이드 패키지 가져오기, 27 페이지](#)의 내용을 참조하십시오.

**단계 3** 푸시하려는 업그레이드 패키지 옆의 푸시(버전 6.5.0 이전) 또는 푸시 또는 단계 업데이트(버전 6.6.0 이상) 아이콘을 클릭하고 대상 디바이스를 선택합니다.

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

**단계 4** 패키지를 푸시합니다. 대상:

- FMC에서 **Push**(푸시)를 클릭합니다.
- 내부 웹 서버에서 **Download Update to Device from Source**(소스에서 디바이스로 업데이트 다운로드)를 클릭합니다.

---

다음에 수행할 작업

디바이스로의 파일 전송이 완료되면 준비도 확인 및/또는 실제 업그레이드를 진행할 수 있습니다. [사용 중인 플랜을 참조하십시오](#).





# 5 장

## Firepower 소프트웨어 준비도 확인 실행

준비도 확인은 소프트웨어 업그레이드를 위해 Firepower 어플라이언스가 준비되어 있는지 평가합니다. 데이터베이스 무결성, 버전 불일치, 디바이스 등록 등의 문제를 식별합니다. 준비도 확인은 버전 6.1.0 이상의 Firepower 소프트웨어 업그레이드 패키지에 포함되어 있습니다.

- 준비도 확인 지침 및 제한 사항, 31 페이지
- 준비도 확인 실행(버전 6.7 이상), 32 페이지
- 준비도 확인 실행(버전 6.1~6.6.x), 33 페이지

### 준비도 확인 지침 및 제한 사항

이러한 지침 및 제한 사항은 Firepower 준비도 확인에 적용됩니다.

#### Firepower 소프트웨어 준비도만 평가

준비도 확인은 Firepower 소프트웨어 준비도만 확인합니다. 침입 규칙, VDB, GeoDB 업데이트에 대한 준비도를 평가하지 않습니다. 핫픽스 또는 패치 제거 프로그램에 대해서는 준비도 확인이 지원되지 않습니다.

#### 버전 및 플랫폼 요구 사항

표 15: 버전 및 플랫폼별 준비도 확인 지원

현재 FMC 버전	준비도 확인 지원
5.4~6.0	지원되지 않음
6.0.1	<p>사전 설치 패키지와 함께 지원됩니다.</p> <p>버전 6.0.1에서 6.1로의 업그레이드에서 준비도 확인을 실행하려면 먼저 버전 6.1 사전 설치 패키지를 설치하십시오. FMC 및 관리되는 디바이스에 대해 이 작업을 수행해야 합니다. <a href="#">Firepower System 릴리스 노트 버전 6.1.0 사전 설치 패키지</a>를 참조하십시오.</p>

현재 <b>FMC</b> 버전	준비도 확인 지원
6.1~6.6.x	<p>버전 6.1~6.6.x Firepower Management Center를 사용하여 자체 및 독립형 관리 디바이스의 준비도 검사를 수행할 수 있습니다.</p> <p>클러스터형 디바이스, 스택형 디바이스 및 고가용성 쌍 디바이스는 Linux 셸(전문가 모드라고도 함)에서 준비도 확인을 실행할 수 있습니다. 검사를 실행하려면 먼저 업그레이드 패키지를 각 디바이스의 올바른 위치에 푸시하거나 복사하고 다음 명령어를 사용합니다: <code>sudo install_update.pl --detach --readiness-check /var/sf/updates/upgrade_package_name</code>. 자세한 안내는 Cisco TAC에 문의하십시오.</p>
6.7.0 이상	<p>버전 6.7.0 이상 Firepower Management Center를 사용하면 고가용성 및 확장성을 위해 설정된 FTD 디바이스를 비롯하여 디바이스 자체와 관리하는 디바이스에 대해 준비도 확인을 수행할 수 있습니다.</p>

#### 시간 요구 사항

준비도 확인을 실행하는 데 필요한 시간은 어플라이언스 모델 및 데이터베이스 크기에 따라 다릅니다. 구축이 대규모인 경우 편의상 준비도 확인을 건너뛸 수 있습니다.



**팁** 모든 디바이스를 6.2.3~6.6.x로 업데이트하는 경우, 시작하기 전 업그레이드 패키지를 디바이스에 복사(푸시)하여 준비도 확인을 실행하는 데 걸리는 시간을 줄일 수 있습니다.

버전 6.7.0 이상으로 FTD 디바이스를 업그레이드할 준비가 되었는지를 확인하기 위해 디바이스에 업그레이드 패키지를 설치할 필요는 없습니다. 업그레이드를 시작하기 전에 업그레이드 패키지를 디바이스에 복사하는 것이 좋지만, 준비도 확인을 실행하기 전에 업그레이드 패키지를 디바이스에 복사할 필요는 없습니다.

#### 확인 중/확인 실패

준비도 확인을 실행 중에는 어플라이언스를 수동으로 재부팅하거나 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.

## 준비도 확인 실행(버전 6.7 이상)

이 절차를 통해 이전 버전(6.3.0~6.6.x)을 실행하는 디바이스와 고가용성 및 확장성 구축의 FTD 디바이스를 포함하여 버전 6.7.0 이상 FMC 및 관리되는 디바이스에서 준비도 확인을 수행합니다.

#### 시작하기 전에

- FMC를 버전 6.7.0 이상으로 업그레이드합니다. FMC에서 현재 이전 버전을 실행 중인 경우, [준비도 확인 실행\(버전 6.1~6.6.x\)](#), 33 페이지를 참조하십시오.

- 확인할 어플라이언스에 대한 업그레이드 패키지를 FMC에 업로드합니다. 버전 6.6.0 이상 FTD 디바이스를 확인하려는 경우, 내부 웹 서버에서 업그레이드 패키지 위치를 지정할 수도 있습니다. 준비도 검사가 업그레이드 패키지에 포함되므로, 이 작업이 필요합니다.
- (선택 사항)ASA FirePOWER/NGIPSv 디바이스를 임의의 버전으로 업그레이드하거나 FTD 디바이스를 버전 6.3.0.1~6.6.x로 업그레이드하는 경우, 업그레이드 패키지를 디바이스에 푸시하십시오. 이렇게 하면 준비도 확인을 실행하는 데 필요한 시간이 줄어들 수 있습니다. FTD 디바이스를 버전 6.7.0 이상으로 업그레이드하는 경우, 이 단계를 건너뛸 수 있습니다. 업그레이드를 시작하기 전에 업그레이드 패키지를 디바이스에 푸시하는 것이 좋지만, 준비도 확인을 실행하기 전에 업그레이드 패키지를 디바이스에 푸시할 필요는 없습니다.

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

단계 2 Available Updates(사용 가능한 업데이트) 아래에서 적절한 업그레이드 패키지 옆에 있는 설치 아이콘을 클릭합니다.

시스템에는 사전 업그레이드 호환성 확인 결과와 함께 적합한 어플라이언스 목록이 표시됩니다. 버전 6.7.0부터 FTD 디바이스에서는 특정 기본 확인을 통과해야 더 복잡한 준비도 확인을 실행할 수 있습니다. 사전 확인에서는 업그레이드 실패의 원인이 되는 문제를 잡아내지만, 이제 이를 더 일찍 발견하여 진행하지 않을 수 있습니다.

단계 3 확인할 어플라이언스를 선택하고 **Check Readiness(준비도 확인)**를 클릭합니다.

적합한 어플라이언스를 선택할 수 없는 경우, 호환성 검사를 통과했는지 확인하십시오. 운영체제를 업그레이드하거나 구성 변경 사항을 구축해야 할 수 있습니다.

단계 4 Message Center에서 준비 확인 진행 상황을 모니터링합니다.

확인에 실패하면 Message Center에서 실패 로그가 제공됩니다.

다음에 수행할 작업

**System(시스템) > Updates(업데이트)** 페이지에서 **Readiness Checks(준비도 확인)**를 클릭하여 진행 중인 확인 및 실패한 확인 등 FTD 구축에 대한 준비도 확인 상태를 확인합니다. 이 페이지에서 장애 발생 후 확인을 쉽게 다시 실행할 수도 있습니다.

## 준비도 확인 실행(버전 6.1~6.6.x)

이 절차는 현재 버전 6.1~6.6.x를 실행 중인 FMC 및 독립형 관리 디바이스에 적용됩니다.



참고 이 절차를 사용하여 버전 6.0.1에서 6.1로의 업그레이드에서 준비도 확인을 실행할 수 있지만, 먼저 버전 6.1 사전 설치 패키지를 설치해야 합니다. FMC 및 관리되는 디바이스에 대해 이 작업을 수행해야 합니다. **Firepower System 릴리스 노트 버전 6.1.0 사전 설치 패키지**를 참조하십시오.

### 시작하기 전에

- 확인할 어플라이언스에 대한 업그레이드 패키지를 FMC에 업로드합니다. 버전 6.6 이상 FTD 디바이스를 확인하려는 경우, 내부 웹 서버에서 업그레이드 패키지 위치를 지정할 수도 있습니다. 준비도 검사가 업그레이드 패키지에 포함되므로, 이 작업이 필요합니다.
- (선택 사항, 버전 6.2.3 이상) 업그레이드 패키지를 관리되는 디바이스에 푸시합니다. 이렇게 하면 검사를 실행하는 데 필요한 시간이 줄어들 수 있습니다.
- 구성이 오래된 관리되는 디바이스에 구성을 구축합니다. 그러지 않으면 준비 확인에 실패할 수 있습니다.

---

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

단계 2 적절한 업그레이드 패키지 옆에 있는 설치 아이콘을 클릭합니다.

단계 3 확인할 어플라이언스를 선택하고 **Launch Readiness Check(준비도 확인 시작)**를 클릭합니다.

단계 4 Message Center에서 준비 확인 진행 상황을 모니터링합니다.

---



## 6 장

# 업그레이드 전 기타 작업 및 확인

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

- 유지 보수 기간 예약, 35 페이지
- 어플라이언스 액세스, 커뮤니케이션 및 상태 확인, 35 페이지
- 관리 네트워크 대역폭, 36 페이지
- 구성 변경 계획, 36 페이지
- 백업 수행, 36 페이지
- NTP 동기화 확인, 37 페이지

## 유지 보수 기간 예약

중단이 구축에 미치는 영향이 가장 적은 시간에 업그레이드를 예약하는 것이 좋습니다.

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, 준비도 확인 실행, 백업 생성 등은 유지 보수 기간까지 기다리지 말고 수행하십시오.

## 어플라이언스 액세스, 커뮤니케이션 및 상태 확인

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

Firepower 디바이스는 인터페이스 컨피그레이션에 따라 업그레이드 중에 또는 업그레이드에 실패한 경우 트래픽 전달을 중지할 수 있습니다. Firepower 디바이스를 업그레이드하기 전 사용자의 위치에서 트래픽이 디바이스 자체를 통과해 디바이스의 관리 인터페이스에 액세스해야 하는지 확인합니다. 또한 FMC 구축에서 디바이스를 통과하지 않아도 FMC 관리 인터페이스에 액세스할 수 있어야 합니다.

업그레이드 중인 어플라이언스를 종료하거나, 수동으로 리부팅하거나, 해당 어플라이언스로/어플라이언스에서 변경 사항을 구축하지 마십시오. 진행 중인 업그레이드를 재시작하지 마십시오. 사전 확

인 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.

## 관리 네트워크 대역폭

Firepower 어플라이언스를 업그레이드하거나 준비도 확인을 실행하려면 업그레이드 패키지가 어플라이언스에 있어야 합니다. Firepower 업그레이드 패키지 크기는 다양합니다. 관리 네트워크에 대용량 데이터 전송을 수행할 대역폭이 있는지 확인합니다.

업그레이드 시 업그레이드 패키지를 관리되는 디바이스로 전송하는 경우, 대역폭이 부족하면 업그레이드 시간이 늘어나거나 업그레이드가 시간 초과될 수 있습니다. 가능하면 FMC 또는 FTD 디바이스의 경우 자체 내부 웹 서버에서 업그레이드하기 전에 관리되는 디바이스에 수동으로 Firepower 업그레이드 패키지를 푸시(복사)하는 것이 좋습니다.

자세한 내용은 다음을 참고하십시오.

- [Firepower 소프트웨어 업그레이드 패키지 다운로드, 21 페이지](#)
- [Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침\(트리블슈팅 TechNote\)](#)

## 구성 변경 계획

특히 주요 업그레이드의 경우, 업그레이드 전이나 후에 구성이 크게 변경되거나 구성을 대폭 변경해야 할 수 있습니다. 예를 들어, 지원이 중단된 FlexConfig 명령은 업그레이드 후 구축 문제를 일으킬 수 있습니다.

## 백업 수행

업그레이드 전후에 모두 Firepower 어플라이언스를 백업합니다.

- 업그레이드 전: 업그레이드가 심각하게 실패할 경우, 이미지를 재설치하고 복구해야 할 수 있습니다. 이미지 재설치는 시스템 비밀번호를 포함하여 대부분의 설정을 공장 기본값으로 되돌립니다. 최근 백업이 있는 경우, 보다 신속하게 정상 작업으로 돌아갈 수 있습니다.
- 업그레이드 후: 새로 업그레이드한 구축의 스냅샷을 생성합니다. 매니지드 디바이스를 업그레이드한 후 FMC를 백업하는 것이 좋습니다. 그러면 새 FMC 백업 파일이 해당 디바이스가 업그레이드되었음을 '인식'합니다.





주의 Firepower 어플라이언스를 안전한 원격 위치에 백업하고 전송 성공을 확인하는 것이 좋습니다. 어플라이언스에 남아 있는 백업은 수동으로 또는 업그레이드 프로세스에 의해 삭제되어 로컬에 저장된 백업을 제거할 수 있습니다.

특히 백업 파일은 암호화되지 않으므로, 무단 액세스를 허용해서는 안 됩니다. 백업 파일이 수정되면 복원 프로세스가 실패하게 됩니다. Admin/Maint(관리/유지 관리) 역할의 사용자는 원격 스토리지에서 파일을 이동하고 삭제할 수 있는 백업 관리 페이지에 액세스할 수 있습니다.

Firepower 백업 기능은 플랫폼 및 버전에 따라 다릅니다. 요구 사항, 지침, 제한 사항, 모범 사례 및 절차는 [Firepower Management Center 구성 가이드](#)를 참조하십시오.

## NTP 동기화 확인

업그레이드하기 전에 Firepower 어플라이언스가 시간을 제공하는 데 사용할 NTP 서버와 동기화되었는지 확인해야 합니다. 동기화되지 않으면 업그레이드 실패가 발생할 수 있습니다. FMC 구축에서 시간 오차가 10초 이상인 경우 시간 동기화 상태 상태 모듈이 경고를 표시하지만 수동으로 확인할 수 있습니다.

시간을 확인하려면 다음을 수행하십시오.

- FMC: **System**(시스템) > **Configuration**(구성) > **Time**(시간)
- 디바이스 **show time** CLI 명령을 사용합니다.





## II 부

# Firepower 어플라이언스 업그레이드

- Firepower Management Center 업그레이드, 41 페이지
- Firepower Threat Defense 업그레이드: Firepower 4100/9300, 49 페이지
- Firepower Threat Defense 업그레이드: 기타 FTD 디바이스, 79 페이지
- Firepower 7000/8000 Series 및 NGIPSv 업그레이드, 87 페이지
- ASA with FirePOWER Services 업그레이드, 95 페이지





# 7 장

## Firepower Management Center 업그레이드

- 업그레이드 체크리스트: Firepower Management Center, 41 페이지
- 업그레이드 경로: Firepower Management Center, 43 페이지
- 독립형 FMC 업그레이드, 45 페이지
- 고가용성 FMC 업그레이드, 46 페이지

### 업그레이드 체크리스트: Firepower Management Center

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

업그레이드할 때마다 체크리스트를 작성하십시오. 단계를 건너뛰면 업그레이드에 실패할 수 있습니다. 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 경로 확인 업그레이드 경로에서 현재 위치를 확인합니다. 방금 수행한 업그레이드와 다음에 수행할 업그레이드를 파악합니다.	<a href="#">업그레이드 경로: Firepower Management Center, 43 페이지</a>
	버전 확인 FMC의 현재 버전과 대상 버전을 확인합니다. <ul style="list-style-type: none"> <li>• Firepower 소프트웨어</li> <li>• 가상 호스팅 환경(FMCv)</li> </ul>	<a href="#">Firepower Management Center, 129 페이지</a>

□	작업/확인	세부 사항
	<b>FMC 호환성 확인</b> FMC가 업그레이드 후에 디바이스를 관리할 수 있는지 확인합니다. 디바이스를 관리할 수 없는 경우 디바이스를 먼저 업그레이드할 수 있도록 업그레이드 경로를 수정합니다.	FMC 디바이스 버전 호환성을 유지할 수 있습니까?, 12 페이지
	릴리스 노트 읽기 다음을 포함하여 업그레이드에 영향을 줄 수 있는 사항에 특히 주의하면서 릴리스 노트를 확인하십시오. <ul style="list-style-type: none"> <li>• 버전별 업그레이드 지침 및 경고</li> <li>• 업그레이드에 영향을 미치는 알려진 문제</li> <li>• 최신/지원 중단 기능</li> </ul>	Firepower 릴리스 노트

## 업그레이드 전 작업 및 확인

유지 보수 기간이 아닐 때 사전 확인을 수행하여 중단을 최소화합니다.

□	작업/확인	세부 사항
	<b>필수 구성 변경 수행</b> 업그레이드 전 필수 구성 변경을 완료하고 업그레이드 후에 필요한 구성 변경을 준비하십시오.	Firepower 릴리스 노트
	<b>디스크 공간 확인</b> Firepower 소프트웨어 업그레이드를 위한 예비 디스크 공간 확인을 실행합니다.	시간 테스트 및 디스크 공간 요구 사항, 195 페이지
	<b>업그레이드 패키지 받기</b> 올바른 업그레이드 패키지를 입수하여 FMC에 업로드합니다. 서명된(.tar) 패키지의 압축을 풀지 마십시오.	Firepower 소프트웨어 업그레이드 패키지 다운로드, 21 페이지
	<b>Firepower 소프트웨어 준비도 확인 실행</b> 준비 확인을 실행합니다. 버전 6.1 이상이 필요합니다.	Firepower 소프트웨어 준비도 확인 실행, 31 페이지
	<b>이벤트 및 구성 백업</b> 이벤트 및 구성 데이터를 백업합니다. 외부 위치에 백업한 후 전송 성공을 확인합니다. 디바이스 백업을 FMC에 저장하는 경우 외부에서도 백업되었는지 확인합니다. FMC를 업그레이드할 때 로컬에 저장된 백업을 제거합니다.	Firepower Management Center 구성 가이드

□	작업/확인	세부 사항
	<b>Maintenance Window</b> 예약 반드시 수행해야 하는 작업, 업그레이드 예상 소요 시간을 고려해 영향이 가장 적을 것으로 예상되는 유지 보수 기간을 예약합니다.	<a href="#">시간 테스트 및 디스크 공간 요구 사항, 195 페이지</a>

**Firepower Management Center** 업그레이드

유지 보수 기간에 업그레이드를 수행합니다.

□	작업/확인	세부 사항
	호스팅 업그레이드 필요한 경우 호스팅 환경(FMCv)을 업그레이드합니다.	<a href="#">호스팅 환경 설명서를 참조하십시오.</a>
	<b>Firepower</b> 소프트웨어 업그레이드 Firepower 소프트웨어를 업그레이드합니다.	<a href="#">독립형 FMC 업그레이드, 45 페이지</a> 또는 <a href="#">고가용성 FMC 업그레이드, 46 페이지</a>

## 업그레이드 경로: Firepower Management Center

이 테이블은 FMCv를 포함해 Firepower Management Center의 업그레이드 경로를 제공합니다.



**참고** FMC를 버전 6.0.0 및 버전 6.0.1로 업그레이드하려면 사전 설치 패키지가 필요합니다. 자세한 내용은 [사전 설치 패키지 식별\(버전 6.0, 6.0.1, 6.1\), 18 페이지](#)를 참조하십시오.

왼쪽 열에서 현재 Firepower 버전을 찾습니다. 오른쪽 열에 나열된 버전으로 직접 업그레이드할 수 있습니다. 현재 버전에서 대상 버전으로 직접 업그레이드를 수행할 수 없는 경우, 안내와 같이 업그레이드 경로에 중간 버전이 포함되어야 합니다. 이 정보를 보는 다른 방법은 [직접 업그레이드가 가능한지?, 10 페이지](#)를 참조하십시오.

표 16: FMC 직접 업그레이드

현재 버전	대상 버전
6.7.0	다음 중 하나로:
6.7.x(유지 보수 릴리스)	→ 모든 6.7.x 이후 유지 보수 릴리스

현재 버전	대상 버전
6.6.0 6.6.x(유지 보수 릴리스) FMC 2000 및 4000에 대한 마지막 지원 입니다.	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 6.7.x 유지 보수 릴리스 → 모든 6.6.x 이후 유지 보수 릴리스
6.5.0	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 6.7.x 유지 보수 릴리스 → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스
6.4.0 FMC 750, 1500 및 3500에 대한 마지막 지원입니다.	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 모든 6.7.x 유지 보수 릴리스 → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스 → 6.5.0
6.3.0	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 모든 6.7.x 유지 보수 릴리스 → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스 → 6.5.0 → 6.4.0
6.2.3	다음 중 하나로 직접 업그레이드: → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스 → 6.5.0 → 6.4.0 → 6.3.0
6.2.2	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0 → 6.2.3
6.2.1	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.2.0	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	직접 업그레이드: → 6.1.0
6.0.0	직접 업그레이드: → 6.0.1



현재 버전	대상 버전
5.4.1.1	직접 업그레이드: → 6.0.0

## 독립형 FMC 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.

FMC 메뉴 바에서 **Deploy**(구축)를 클릭합니다. 디바이스를 선택하고 **Deploy**(구축)를 다시 클릭합니다. 업그레이드하기 전에 배포하면 실패 가능성이 줄어듭니다.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 구성을 구축하면 Snort를 재시작하여 트래픽 검사가 중단되고, 디바이스가 트래픽을 처리하는 방법에 따라 재시작이 완료될 때까지 트래픽이 종료될 수 있습니다. 자세한 내용은 [트래픽 흐름, 검사 및 디바이스 동작, 241 페이지](#)를 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. 디스크 공간 요구 사항은 [시간 테스트 및 디스크 공간 요구 사항, 195 페이지](#)를 참조하십시오.

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

**단계 4** 사용하려는 업그레이드 패키지 옆의 **Install**(설치) 아이콘을 클릭하고 FMC를 선택합니다.

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

업그레이드할 것임을 확인하고 FMC를 리부팅합니다.

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

FMC가 업그레이드되는 중에는 컨피그레이션을 변경하거나 컨피그레이션 변경 사항을 디바이스에 구축하지 마십시오. **Message Center**에서 몇 분간 진행 상황이 표시되지 않거나 업그레이드에서 장애가 발생했다고 나타나더라도 업그레이드를 재시작하거나 FMC를 리부팅하지 마십시오. 그 대신 Cisco TAC에 문의하십시오.

**단계 7** 가능할 때 FMC에 다시 로그인합니다.

- 부 버전 업그레이드(패치 및 핫픽스): 업그레이드가 완료되고 FMC가 리부팅된 후에 로그인할 수 있습니다.
- 주 버전 업그레이드: 업그레이드가 완료되기 전에 로그인할 수 있습니다. FMC에는 업그레이드의 진행 상황을 모니터링하고 업그레이드 로그 및 오류 메시지를 확인할 수 있는 페이지가 표시됩니다. 업그레이드가 완료되고 FMC가 리부팅되면 다시 로그아웃됩니다. 재부팅 후 다시 로그인합니다.

**단계 8** 프롬프트가 표시되면 EULA(최종 사용자 라이선스 계약)를 검토하고 동의합니다.

**단계 9** 업그레이드 성공을 확인합니다.

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

**단계 10** **Message Center**를 사용하여 구축 상태를 다시 확인합니다.

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

Cisco 지원 및 다운로드 사이트에서 제공되는 SRU 또는 VDB가 현재 실행 중인 버전보다 최신 상태이면 최신 버전을 설치합니다. 자세한 내용은 [Firepower Management Center 구성 가이드](#)를 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 FMC 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 FMC가 사전 확인을 시작하면 해당 상태가 스탠바이에서 액티브로 전환되므로 두 피어가 모두 액티브 상태가 됩니다. 스플릿 브레인이라는 일시적인 상태는 업그레이드 중을 제외하고는 지원되지 않습니다. 고가용성 쌍이 스플릿 브레인 상태

인 동안에는 컨피그레이션을 변경하거나 변경 사항을 구축하지 마십시오. 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 FMC에서 컨피그레이션이 오래된 매니지드 디바이스로 변경 사항을 구축합니다.

FMC 메뉴 바에서 **Deploy**(구축)를 클릭합니다. 디바이스를 선택하고 **Deploy**(구축)를 다시 클릭합니다. 업그레이드 하기 전에 배포하면 실패 가능성이 줄어듭니다.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 구성을 구축하면 Snort를 재시작하여 트래픽 검사가 중단되고, 디바이스가 트래픽을 처리하는 방법에 따라 재시작이 완료될 때까지 트래픽이 종료될 수 있습니다. 자세한 내용은 [트래픽 흐름, 검사 및 디바이스 동작, 241 페이지](#)를 참조하십시오.

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

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

**단계 4** FMC를 한 번에 하나씩 업그레이드합니다. 먼저 스탠바이를 업그레이드하고 액티브를 업그레이드합니다.

독립형 FMC 업그레이드, 45 페이지의 지침을 따르되 초기 구축은 생략하고 각 FMC에서 업데이트 성공을 확인한 후에 작업을 중지합니다. 요약하면 각 FMC마다:

- a) 최종 사전 업그레이드 검사(상태, 실행 중인 작업, 디스크 공간)를 수행합니다.
- b) **System**(시스템) > **Updates**(업데이트) 페이지에서 업그레이드를 설치합니다.
- c) 로그아웃될 때까지 진행을 모니터링하고 로그인 가능해지면 다시 로그인합니다(주요 업그레이드의 경우 두 번 발생합니다).
- d) 업그레이드 성공을 확인합니다.

고가용성 쌍이 스플릿 브레인 상태인 동안에는 컨피그레이션을 변경하거나 변경 사항을 구축하지 마십시오.

**단계 5** 액티브 피어로 설정할 FMC에서 동기화를 재시작합니다.

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

- b) **High Availability**(고가용성) 탭에서 **Make-Me-Active**(액티브 상태로 전환)를 클릭합니다.
- c) 동기화가 재시작되고 다른 FMC가 스탠바이 모드로 전환될 때까지 기다립니다.

단계 6 Message Center를 사용하여 구축 상태를 다시 확인합니다.

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

Cisco 지원 및 다운로드 사이트에서 제공되는 SRU 또는 VDB가 현재 실행 중인 버전보다 최신 상태이면 최신 버전을 설치합니다. 자세한 내용은 [Firepower Management Center 구성 가이드](#)를 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.



# 8 장

## Firepower Threat Defense 업그레이드: Firepower 4100/9300

- 업그레이드 체크리스트: Firepower 4100/9300 새시의 FTD, 49 페이지
- 업그레이드 경로: Firepower 4100/9300 새시의 FTD, 52 페이지
- FXOS 업그레이드: Firepower 4100/9300 새시, 55 페이지
- FTD 소프트웨어 업그레이드: Firepower 4100/9300 새시, 75 페이지

### 업그레이드 체크리스트: Firepower 4100/9300 새시의 FTD

이 체크리스트로 에서 FTD을(를) 사용하는 Firepower 4100/9300 새시을(를) 업그레이드합니다.

업그레이드할 때마다 체크리스트를 작성하십시오. 단계를 건너뛰면 업그레이드에 실패할 수 있습니다. 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 경로 확인 업그레이드 경로에서 현재 위치를 확인합니다. 방금 수행한 업그레이드와 다음에 수행할 업그레이드를 파악합니다.	업그레이드 경로: Firepower 4100/9300 새시의 FTD, 52 페이지
	버전 확인 디바이스의 현재 버전과 대상 버전을 확인합니다. • Firepower 소프트웨어 • FXOS	FMC를 사용하는 Firepower 4100/9300, 133 페이지

□	작업/확인	세부 사항
	<b>FMC 호환성 확인</b> 디바이스를 업그레이드한 후 FMC에서 해당 디바이스를 관리할 수 있는지 확인합니다. 디바이스를 관리할 수 없는 경우 FMC를 먼저 업그레이드할 수 있도록 업그레이드 경로를 수정합니다.	<a href="#">FMC 디바이스 버전 호환성을 유지할 수 있습니까?, 12 페이지</a>
	<b>릴리스 노트 읽기</b> 다음을 포함하여 업그레이드에 영향을 줄 수 있는 사항에 특히 주의하면서 릴리스 노트를 확인하십시오. <ul style="list-style-type: none"> <li>• 버전별 업그레이드 지침 및 경고</li> <li>• 업그레이드에 영향을 미치는 알려진 문제</li> <li>• 최신/지원 중단 기능</li> </ul>	<a href="#">Firepower 릴리스 노트</a> 및 <a href="#">FXOS 릴리스 노트</a>

## 업그레이드 전 작업 및 확인

유지 보수 기간이 아닐 때 사전 확인을 수행하여 중단을 최소화합니다.

□	작업/확인	세부 사항
	<b>필수 구성 변경 수행</b> 업그레이드 전 필수 구성 변경을 완료하고 업그레이드 후에 필요한 구성 변경을 준비하십시오.	<a href="#">Firepower 릴리스 노트</a> 및 <a href="#">FXOS 릴리스 노트</a>
	<b>디스크 공간 확인</b> Firepower 소프트웨어 업그레이드를 위한 예비 디스크 공간 확인을 실행합니다.	<a href="#">시간 테스트 및 디스크 공간 요구 사항, 195 페이지</a>
	<b>FXOS 업그레이드 패키지 가져오기</b> 올바른 FXOS 업그레이드 패키지를 다운로드합니다.	<a href="#">Firepower 4100/9300 새시용 FXOS 업그레이드 패키지, 55 페이지</a>
	<b>Firepower 소프트웨어 업그레이드 패키지 가져오기</b> 올바른 Firepower 소프트웨어 업그레이드 패키지를 다운로드합니다. 서명된(.tar) 패키지의 압축을 풀지 마십시오. 다음 중 하나를 수행할 수 있습니다. <ul style="list-style-type: none"> <li>• FMC에 패키지를 업로드합니다.</li> <li>• 내부 웹 서버를 FTD 업그레이드 패키지의 소스로 설정합니다. 버전 6.6.0이 필요합니다.</li> </ul>	<a href="#">Firepower 소프트웨어 업그레이드 패키지 다운로드, 21 페이지</a>

□	작업/확인	세부 사항
	<p><b>대역폭 확인</b></p> <p>관리되는 디바이스로 대량 데이터 전송을 수행할 수 있는 대역폭을 사용하고 있는지 확인합니다.</p>	<p><a href="#">Firepower Management Center</a> 에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침(트러블슈팅 TechNote)</p>
	<p><b>Firepower</b> 소프트웨어 업그레이드 패키지 푸시</p> <p>업그레이드 패키지를 디바이스에 푸시합니다. 필요한 컴패니언 FXOS 업그레이드를 시작하기 전 푸시를 강력하게 권장합니다(필수인 경우도 있습니다). 버전 6.2.3 이상이 필요합니다.</p>	<p><a href="#">FMC 관리 디바이스로 업그레이드 패키지 푸시, 28 페이지</a></p>
	<p><b>Firepower</b> 소프트웨어 준비도 확인 실행</p> <p>준비 확인을 실행합니다. 버전 6.1 이상이 필요합니다.</p>	<p><a href="#">Firepower 소프트웨어 준비도 확인 실행, 31 페이지</a></p>
	<p><b>디바이스 백업</b></p> <p>FMC를 사용하여 지원되는 FTD 플랫폼에 대한 구성 데이터를 백업합니다(일부 FTD 플랫폼에서만 백업 지원) 외부 위치에 백업한 후 전송 성공을 확인합니다. 버전 6.3 이상이 필요합니다.</p>	<p><a href="#">Firepower Management Center 구성 가이드</a></p>
	<p><b>어플라이언스 액세스 확인</b></p> <p>사용 중인 컴퓨터가 디바이스 자체를 통과하지 않고 FMC의 관리 인터페이스와 디바이스의 관리 인터페이스에 모두 연결할 수 있는지 확인합니다.</p>	<p><a href="#">어플라이언스 액세스, 커뮤니케이션 및 상태 확인, 35 페이지</a></p>
	<p><b>Maintenance Window</b> 예약</p> <p>반드시 수행해야 하는 작업, 업그레이드가 트래픽 흐름 및 검사에 미치는 영향, 업그레이드 예상 소요 시간을 고려해 영향이 가장 적을 것으로 예상되는 유지 보수 기간을 예약합니다.</p>	<p><a href="#">FTD 업그레이드 동작: Firepower 4100/9300 새시, 241 페이지</a></p> <p>및</p> <p><a href="#">시간 테스트 및 디스크 공간 요구 사항, 195 페이지</a></p>

디바이스 업그레이드

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

□	작업/확인	세부 사항
	<p><b>FXOS</b> 업그레이드</p> <p>필요한 경우, FXOS을 업그레이드합니다. 트래픽 흐름 및 검사 중단을 방지하려면 고가용성 쌍의 새시와 새시 간 클러스터를 한 번에 하나씩 업그레이드하십시오.</p>	<p><a href="#">FXOS 업그레이드: Firepower 4100/9300 새시, 55 페이지</a></p>

<input type="checkbox"/>	작업/확인	세부 사항
	<b>Firepower</b> 소프트웨어 업그레이드 Firepower 소프트웨어를 업그레이드합니다.	<a href="#">FTD 소프트웨어 업그레이드: Firepower 4100/9300 새시, 75 페이지</a>

## 업그레이드 경로: Firepower 4100/9300 새시의 FTD

이 테이블에서는 FTD를 사용하는 Firepower 4100/9300 새시의 업그레이드 경로를 제공합니다.

왼쪽 열에서 현재 Firepower 버전을 찾습니다. 오른쪽 열에 나열된 버전으로 직접 업그레이드할 수 있습니다. 현재 버전에서 대상 버전으로 직접 업그레이드를 수행할 수 없는 경우, 안내와 같이 업그레이드 경로에 중간 버전이 포함되어야 합니다. 이 정보를 보는 다른 방법은 [직접 업그레이드가 가능한지? 10 페이지](#)를 참조하십시오.

표 17: 직접 업그레이드: Firepower 4100/9300 새시

현재 버전	대상 버전
6.7.0 6.7.x(유지 보수 릴리스)	다음 중 하나로: → 모든 6.7.x 이후 유지 보수 릴리스
6.6.0 6.6.x(유지 보수 릴리스)	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 6.7.x 유지 보수 릴리스 → 모든 6.6.x 이후 유지 보수 릴리스
6.5.0	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 6.7.x 유지 보수 릴리스 → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스
6.4.0	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 모든 6.7.x 유지 보수 릴리스 → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스 → 6.5.0
6.3.0	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 모든 6.7.x 유지 보수 릴리스 → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스 → 6.5.0 → 6.4.0
6.2.3	다음 중 하나로 직접 업그레이드: → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스 → 6.5.0 → 6.4.0 → 6.3.0



현재 버전	대상 버전
6.2.2	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0 → 6.2.3
6.2.0	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0*	다음 중 하나로 직접 업그레이드: → 6.2.3 → 6.2.0
6.0.1	직접 업그레이드: → 6.1.0

\* 운영체제가 호환되지 않으므로 Firepower 4100/9300 Series 디바이스에서는 버전 6.1에서 6.4로 직접 업그레이드할 수 없습니다. 비슷한 이유로 버전 6.1에서 6.3으로 업그레이드하지 않는 것이 좋습니다. 버전 6.1을 실행 중인 경우, FXOS 2.3.1에서 버전 6.2.3으로 업그레이드한 다음에 그 이후 버전으로 업그레이드하는 것이 좋습니다.

### FXOS 업그레이드

Firepower 주 버전에는 특별히 검증된 컴패니언 FXOS 버전이 있습니다. Firepower 소프트웨어를 업그레이드하기 전에 FXOS를 업그레이드합니다. 일반적으로 버전 시퀀스에서 가장 최신 FXOS 빌드를 권장하지만 최소 요구 빌드는 [FMC를 사용하는 Firepower 4100/9300, 133 페이지](#)를 참조하십시오.

표 18: FXOS 컴패니언 버전

Firepower 버전	FXOS 컴패니언 버전
6.7.0 및 6.7.x	2.9.1
6.6.0 및 6.6.x	2.8.1
6.5.0	2.7.1
6.4.0	2.6.1
6.3.0	2.4.1
6.2.3	2.3.1
6.2.2	2.2.2
6.2.0	2.1.1, 2.2.1 및 2.2.2
6.1.0	2.0.1
6.0.1	1.1.4

디바이스 클러스터 또는 고가용성 쌍에서는 유닛 단위로 Firepower 소프트웨어를 업그레이드하지만, FXOS에서는 새시마다 독립적으로 업그레이드합니다. 이 테이블에서는 독립형 및 HA/확장성 구축에 대한 FXOS 업그레이드 순서를 간략하게 설명합니다. 자세한 내용은 [FXOS 업그레이드: Firepower 4100/9300 새시, 55 페이지](#)를 참고하십시오.

표 19: FXOS + FTD 업그레이드 순서

FTD 구축	업그레이드 순서
독립형 디바이스	<ol style="list-style-type: none"> <li>1. FXOS 업그레이드</li> <li>2. Firepower 소프트웨어를 업그레이드합니다.</li> </ol>
고가용성	<p>중단을 최소화하려면 항상 스탠바이를 업그레이드하십시오.</p> <ol style="list-style-type: none"> <li>1. 스탠바이 유닛의 FXOS를 업그레이드합니다.</li> <li>2. 역할을 전환합니다.</li> <li>3. 새 스탠바이 유닛의 FXOS를 업그레이드합니다.</li> <li>4. Firepower 소프트웨어를 업그레이드합니다.</li> </ol>
새시 내 클러스터링 (Firepower 9300 전용)	<ol style="list-style-type: none"> <li>1. FXOS 업그레이드</li> <li>2. Firepower 소프트웨어를 업그레이드합니다.</li> </ol>
새시 간 클러스터(6.2 이상)	<p>중단을 최소화하기 위해 항상 전체 데이터 유닛 새시를 업그레이드합니다. 예를 들어 새시가 2개인 클러스터는 다음과 같이 업그레이드합니다.</p> <ol style="list-style-type: none"> <li>1. 전체 데이터 유닛 새시에서 FXOS를 업그레이드합니다.</li> <li>2. 제어 모듈을 방금 업그레이드한 새시로 전환합니다.</li> <li>3. 새로운 데이터 유닛 새시 전체에서 FXOS를 업그레이드합니다.</li> <li>4. Firepower 소프트웨어를 업그레이드합니다.</li> </ol>

고가용성 및 클러스터링 무중단 업그레이드 요구 사항

무중단 업그레이드를 수행하려면 다음 추가 요구 사항이 필요합니다.

**플로우 오프로드:** 플로우 오프로드 기능의 버그 수정으로 일부 FXOS 및 FTD 조합은 플로우 오프로드를 지원하지 않습니다. [Cisco FirePOWER 호환성 가이드](#)를 참조하십시오. 고가용성 또는 클러스터링 구축의 무중단 업그레이드를 수행하려면 항상 호환되는 조합이 실행 중인지 확인해야 합니다.

업그레이드 경로에 FXOS를 2.2.2.91, 2.3.1.130 또는 그 이후 버전(FXOS 2.4.1.x, 2.6.1.x 등 포함)으로 업그레이드하는 내용이 포함된 경우 다음 경로를 사용합니다.

1. FTD를 6.2.2.2 이상으로 업그레이드합니다.
2. FXOS를 2.2.2.91, 2.3.1.130 또는 그 이후 버전으로 업그레이드합니다.

3. FTD를 최종 버전으로 업그레이드합니다.

예를 들어 FXOS 2.2.2.17/FTD 6.2.2.0를 사용 중일 때 FXOS 2.6.1/FTD 6.4.0으로 업그레이드하려는 경우 다음을 수행할 수 있습니다.

1. FTD를 6.2.2.5로 업그레이드합니다.
2. FXOS를 2.6.1로 업그레이드합니다.
3. FTD를 6.4.0으로 업그레이드합니다.

버전 **6.1.0** 업그레이드: FTD 고가용성 쌍을 버전 6.1.0으로 무중단 업그레이드하려면 사전 설치 패키지가 필요합니다. 자세한 내용은 [Firepower System 릴리스 노트 버전 6.1.0 사전 설치 패키지](#)를 참조하십시오.

## FXOS 업그레이드: Firepower 4100/9300 새시

Firepower 4100/9300 새시에서는 FXOS 운영 체제를 Firepower 소프트웨어와 별도로 업그레이드합니다. Firepower 새시 간 클러스터링 또는 고가용성 쌍이 구성되어 있더라도 각 새시에서 FXOS를 독립적으로 업그레이드합니다.

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

FXOS를 업그레이드하면 새시가 리부팅됩니다. 사용 중인 구축에 따라 트래픽이 삭제되거나 검사 없이 네트워크를 통과할 수 있습니다. [FTD 업그레이드 동작: Firepower 4100/9300 새시, 241 페이지](#)를 참조하십시오.

## Firepower 4100/9300 새시용 FXOS 업그레이드 패키지

Firepower 4100/9300 새시용 FXOS 업그레이드 패키지는 다음으로 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.

표 20: FXOS 업그레이드 패키지

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

패키지 유형	패키지 이름
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

## 독립형 FTD 논리 디바이스 또는 FTD 새시 내 클러스터용 FXOS 업그레이드

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

### 사용해 독립형 FTD 논리 디바이스 또는 FTD 새시 내 클러스터용 FXOS 업그레이드 Firepower Chassis Manager

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

여기서는 다음 디바이스 유형에 대한 업그레이드 프로세스를 설명합니다.

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

시작하기 전에

업그레이드를 시작하기 전에 다음 작업을 이미 완료했는지 확인하십시오.

- 업그레이드 대상 FXOS 플랫폼 번들 소프트웨어 패키지를 다운로드합니다. [Firepower 4100/9300 새시용 FXOS 업그레이드 패키지, 55 페이지](#)를 참조하십시오.
- FXOS 및 FTD 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 새시에서 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 이미지가 Firepower 4100/9300 새시에 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**을 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
```

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

- a) **top**을 입력합니다.
- b) **scope ssa**을 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**을 입력합니다.
- f) 새시에 설치된 모든 논리적 디바이스의 Oper State(작동 상태)가 Online(온라인) 인지 확인합니다.

## FXOS CLI를 사용해 독립형 FTD 논리 디바이스 또는 FTD 새시 내 클러스터용 FXOS 업그레이드

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

여기서는 다음 디바이스 유형에 대한 FXOS 업그레이드 프로세스를 설명합니다.

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

시작하기 전에

업그레이드를 시작하기 전에 다음 작업을 이미 완료했는지 확인하십시오.

- 업그레이드 대상 FXOS 플랫폼 번들 소프트웨어 패키지를 다운로드합니다. [Firepower 4100/9300 새시용 FXOS 업그레이드 패키지, 55 페이지](#)를 참조하십시오.
- FXOS 및 FTD 컨피그레이션을 백업합니다.
- Firepower 4100/9300 새시에 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 새시에 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 # scope auto-install
```

단계 5 FXOS 플랫폼 번들을 설치합니다.

```
Firepower-chassis-a /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 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.

**yes**를 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.

- scope system**을 입력합니다.
- show firmware monitor**을 입력합니다.
- 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.

- top**을 입력합니다.
- scope ssa**을 입력합니다.
- show slot**을 입력합니다.
- 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.
- show app-instance**을 입력합니다.



- f) 새시에 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 FTD 고가용성 쌍에서 FXOS 업그레이드

FTD 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 새시용 FXOS 업그레이드 패키지, 55 페이지](#)를 참조하십시오.
- FXOS 및 FTD 컨피그레이션을 백업합니다.



참고 업그레이드 프로세스에는 일반적으로 새시당 20~30분이 소요됩니다.

- 단계 1** 스텝바이 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 새시에서 사용 가능한 Firepower eXtensible 운영 체제 플랫폼 번들 이미지와 애플리케이션 이미지 목록을 보여줍니다.
- 단계 3** 새 플랫폼 번들 이미지를 업로드합니다.
  - Upload Image(이미지 업로드)**를 클릭하여 Upload Image(이미지 업로드) 대화 상자를 엽니다.
  - Choose File(파일 선택)**을 클릭하여 업로드할 이미지로 이동한 다음 해당 이미지를 선택합니다.
  - Upload(업로드)**를 클릭합니다.  
선택한 이미지가 Firepower 4100/9300 새시에 업로드됩니다.
  - 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(아니오)**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**을 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
```

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

- a) **top**을 입력합니다.
- b) **scope ssa**을 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**을 입력합니다.
- f) 새시에 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 새시에서 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 이미지가 Firepower 4100/9300 새시에 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**을 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

```

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

- a) **top**을 입력합니다.
- b) **scope ssa**을 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**을 입력합니다.
- f) 새시에 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 FTD 고가용성 쌍에서 FXOS 업그레이드

FTD 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 새시용 FXOS 업그레이드 패키지, 55 페이지](#)를 참조하십시오.
- FXOS 및 FTD 컨피그레이션을 백업합니다.
- Firepower 4100/9300 새시에 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 새시당 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 새시에 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 # **scope auto-install**

단계 5 FXOS 플랫폼 번들을 설치합니다.

Firepower-chassis-a /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 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.

**yes**를 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**을 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 계속 됩니다.

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**을 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**을 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 새시에 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 # scope auto-install
```

단계 15 FXOS 플랫폼 번들을 설치합니다.

```
Firepower-chassis-a /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 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.

**yes**를 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**을 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 계속 됩니다.

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 19 모든 구성 요소가 업그레이드되면 다음 명령을 입력하여 보안 모듈/보안 엔진과 설치된 애플리케이션의 상태를 확인합니다.
- top**을 입력합니다.
  - scope ssa**을 입력합니다.
  - show slot**을 입력합니다.
  - 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.
  - show app-instance**을 입력합니다.
  - 새시에 설치된 모든 논리적 디바이스의 Oper State(작동 상태)가 Online (온라인) 인지 확인합니다.
- 단계 20 방금 업그레이드한 유닛을 업그레이드 이전처럼 액티브 유닛으로 만듭니다.
- Firepower Management Center에 연결합니다.
  - Devices(디바이스) > Device Management(디바이스 관리)**를 선택합니다.
  - 액티브 피어를 변경할 고가용성 쌍 옆에 있는 Switch Active Peer(액티브 피어 전환) 아이콘()을 클릭합니다.
  - Yes(예)**를 클릭하여 스탠바이 디바이스를 고가용성 쌍의 액티브 디바이스로 즉시 설정합니다.

## Firepower Threat Defense 새시 간 클러스터에서 FXOS 업그레이드

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

### Firepower Chassis Manager를 사용하여 FTD 새시 간 클러스터에서 FXOS 업그레이드

FTD 논리적 디바이스가 새시 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 새시용 FXOS 업그레이드 패키지, 55 페이지](#)를 참조하십시오.
- FXOS 및 FTD 컨피그레이션을 백업합니다.



참고 업그레이드 프로세스에는 일반적으로 새시당 20~30분이 소요됩니다.

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

- 새시 #2(제어 유닛이 없는 새시)의 FXOS CLI에 연결합니다.

- b) **top**을 입력합니다.
- c) **scope ssa**을 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**을 입력합니다.
- g) 새시에 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 FTD 소프트웨어 버전이 Running Version(실행 중인 버전)으로 표시되는지 확인합니다.

참고 제어 유닛이 이 새시에 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 새시 #2(제어 유닛이 없는 새시)의 Firepower Chassis Manager에 연결합니다.

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

Available Updates(사용 가능한 업데이트) 페이지는 새시에서 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 이미지가 Firepower 4100/9300 새시에 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**을 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 계속 됩니다.

- d) **top**을 입력합니다.  
 e) **scope ssa**을 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**을 입력합니다.  
 i) 새시에 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
Cluster   Slave
ftd        2         Enabled    Online       6.2.2.81     6.2.2.81
Cluster   Slave
ftd        3         Disabled   Not Available 6.2.2.81
Applicable None
```

FP9300-A /ssa #

단계 8 새시 #2의 보안 모듈 중 하나를 제어 모듈로 설정합니다.

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

단계 9 클러스터의 다른 모든 새시에 대해 1~7단계를 반복합니다.

단계 10 제어 역할을 새시 #1로 돌려놓으려면 새시 #1의 보안 모듈 중 하나를 제어 모듈로 설정합니다.

## FXOS CLI를 사용하여 FTD 새시 간 클러스터에서 FXOS 업그레이드

FTD 논리적 디바이스가 새시 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 새시용 FXOS 업그레이드 패키지, 55 페이지](#)를 참조하십시오.
- FXOS 및 FTD 컨피그레이션을 백업합니다.
- Firepower 4100/9300 새시에 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 새시당 20~30분이 소요됩니다.

단계 1 새시 #2(제어 유닛이 없는 새시)의 FXOS CLI에 연결합니다.

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

- a) **top**을 입력합니다.
- b) **scope ssa**을 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**을 입력합니다.

- f) 새시에 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 FTD 소프트웨어 버전이 Running Version(실행 중인 버전)으로 표시되는지 확인합니다.

참고 제어 유닛이 이 새시에 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 새시에 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.

**yes**를 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**을 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 계속 됩니다.

d) **top**을 입력합니다.

e) **scope ssa**을 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**을 입력합니다.

i) 새시에 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
Cluster   Slave
ftd        2         Enabled   Online      6.2.2.81    6.2.2.81
Cluster   Slave
ftd        3         Disabled  Not Available 6.2.2.81
Applicable None
FP9300-A /ssa #

```

**단계 10** 새시 #2의 보안 모듈 중 하나를 제어 모듈로 설정합니다.

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

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

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

## FTD 소프트웨어 업그레이드: Firepower 4100/9300 새시

Firepower 4100/9300 새시의 FTD 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 FMC 업그레이드 포함)에서 현재 위치를 확인합니다. 이 단계를 완벽하게 계획하고 준비했는지 확인합니다.

**단계 1** 업그레이드하려는 디바이스에 컨피그레이션을 구축합니다.

FMC 메뉴 바에서 **Deploy**(구축)를 클릭합니다. 디바이스를 선택하고 **Deploy**(구축)를 다시 클릭합니다. 업그레이드하기 전에 배포하면 실패 가능성이 줄어듭니다.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 구성을 구축하면 Snort를 재시작하여 트래픽 검사가 중단되고, 디바이스가 트래픽을 처리하는 방법에 따라 재시작이 완료될 때까지 트래픽이 종료될 수 있습니다. 자세한 내용은 [FTD 업그레이드 동작: Firepower 4100/9300 새시, 241 페이지](#)를 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. 디스크 공간 요구 사항은 [시간 테스트 및 디스크 공간 요구 사항, 195 페이지](#)를 참조하십시오.

**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 FMC에서는 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 [FTD 업그레이드 동작: Firepower 4100/9300 새시, 241 페이지](#)를 참조하십시오.

**단계 7 Message Center**에서 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(SRU) 및 취약점 데이터베이스(VDB)를 업데이트합니다.

Cisco 지원 및 다운로드 사이트에서 제공되는 SRU 또는 VDB가 현재 실행 중인 버전보다 최신 상태이면 최신 버전을 설치합니다. 자세한 내용은 [Firepower Management Center 구성 가이드](#)를 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.





# 9 장

## Firepower Threat Defense 업그레이드: 기타 FTD 디바이스

- 업그레이드 체크리스트: 기타 FTD 디바이스, 79 페이지
- 업그레이드 경로: 기타 FTD 디바이스, 82 페이지
- FTD 소프트웨어 업그레이드: 기타 FTD 디바이스, 83 페이지

### 업그레이드 체크리스트: 기타 FTD 디바이스

이 체크리스트를 참조하여 Firepower 1000/2100 series, ASA 5500-X series, ISA 3000 및 FTDv 디바이스를 업그레이드합니다.

업그레이드할 때마다 체크리스트를 작성하십시오. 단계를 건너뛰면 업그레이드에 실패할 수 있습니다. 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 경로 확인 업그레이드 경로에서 현재 위치를 확인합니다. 방금 수행한 업그레이드와 다음에 수행할 업그레이드를 파악합니다.	<a href="#">업그레이드 경로: 기타 FTD 디바이스, 82 페이지</a>
	버전 확인 디바이스의 현재 버전과 대상 버전을 확인합니다. <ul style="list-style-type: none"> <li>• Firepower Threat Defense 소프트웨어</li> <li>• 가상 호스팅 환경(FTDv)</li> </ul>	<a href="#">Firepower 디바이스, 133 페이지</a>

□	작업/확인	세부 사항
	<b>FMC 호환성 확인</b> 디바이스를 업그레이드한 후 FMC에서 해당 디바이스를 관리할 수 있는지 확인합니다. 디바이스를 관리할 수 없는 경우 FMC를 먼저 업그레이드할 수 있도록 업그레이드 경로를 수정합니다.	<a href="#">FMC 디바이스 버전 호환성을 유지할 수 있습니까?, 12 페이지</a>
	<b>릴리스 노트 읽기</b> 다음을 포함하여 업그레이드에 영향을 줄 수 있는 사항에 특히 주의하면서 릴리스 노트를 확인하십시오. <ul style="list-style-type: none"> <li>• 버전별 업그레이드 지침 및 경고</li> <li>• 업그레이드에 영향을 미치는 알려진 문제</li> <li>• 최신/지원 중단 기능</li> </ul>	<a href="#">Firepower 릴리스 노트</a>

## 업그레이드 전 작업 및 확인

유지 보수 기간이 아닐 때 사전 확인을 수행하여 중단을 최소화합니다.

□	작업/확인	세부 사항
	<b>필수 구성 변경 수행</b> 업그레이드 전 필수 구성 변경을 완료하고 업그레이드 후에 필요한 구성 변경을 준비하십시오.	<a href="#">Firepower 릴리스 노트</a>
	<b>디스크 공간 확인</b> Firepower 소프트웨어 업그레이드를 위한 예비 디스크 공간 확인을 실행합니다.	<a href="#">시간 테스트 및 디스크 공간 요구 사항, 195 페이지</a>
	<b>Firepower 소프트웨어 업그레이드 패키지 가져오기</b> 올바른 Firepower 소프트웨어 업그레이드 패키지를 다운로드합니다. 서명된(.tar) 패키지의 압축을 풀지 마십시오. 다음 중 하나를 수행할 수 있습니다. <ul style="list-style-type: none"> <li>• FMC에 패키지를 업로드합니다.</li> <li>• 내부 웹 서버를 FTD 업그레이드 패키지의 소스로 설정합니다. 버전 6.6.0이 필요합니다.</li> </ul>	<a href="#">Firepower 소프트웨어 업그레이드 패키지 다운로드, 21 페이지</a>
	<b>대역폭 확인</b> 관리되는 디바이스로 대량 데이터 전송을 수행할 수 있는 대역폭을 사용하고 있는지 확인합니다.	<a href="#">Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침(트러블슈팅 TechNote)</a>

□	작업/확인	세부 사항
	<b>Firepower</b> 소프트웨어 업그레이드 패키지 푸시 업그레이드 패키지를 디바이스에 푸시합니다. 버전 6.2.3 이상이 필요합니다.	FMC 관리 디바이스로 업그레이드 패키지 푸시, 28 페이지
	<b>Firepower</b> 소프트웨어 준비도 확인 실행 준비 확인을 실행합니다. 버전 6.1 이상이 필요합니다.	Firepower 소프트웨어 준비도 확인 실행, 31 페이지
	디바이스 백업 FMC를 사용하여 지원되는 FTD 플랫폼에 대한 구성 데이터를 백업합니다(일부 FTD 플랫폼에서만 백업 지원) 외부 위치에 백업한 후 전송 성공을 확인합니다. 버전 6.3 이상이 필요합니다.	<a href="#">Firepower Management Center 구성 가이드</a>
	어플라이언스 액세스 확인 사용 중인 컴퓨터가 디바이스 자체를 통과하지 않고 FMC의 관리 인터페이스와 디바이스의 관리 인터페이스에 모두 연결할 수 있는지 확인합니다.	어플라이언스 액세스, 커뮤니케이션 및 상태 확인, 35 페이지
	<b>Maintenance Window</b> 예약 반드시 수행해야 하는 작업, 업그레이드가 트래픽 흐름 및 검사에 미치는 영향, 업그레이드 예상 소요 시간을 고려해 영향이 가장 적을 것으로 예상되는 유지 보수 기간을 예약합니다.	FTD업그레이드 동작: 기타 장치, 245 페이지 및 시간 테스트 및 디스크 공간 요구 사항, 195 페이지

디바이스 업그레이드

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

□	작업/확인	세부 사항
	호스팅 업그레이드 필요한 경우 호스팅 환경(FTDv)을 업그레이드합니다.	호스팅 환경 설명서를 참조하십시오.
	<b>Firepower</b> 소프트웨어 업그레이드 Firepower 소프트웨어를 업그레이드합니다.	FTD 소프트웨어 업그레이드: 기타 FTD 디바이스, 83 페이지

## 업그레이드 경로: 기타 FTD 디바이스

이 테이블에는 운영체제를 업데이트할 필요가 없는 Firepower Management Center에서 관리하는 FTD 디바이스의 업그레이드 경로가 나와 있습니다(Firepower 1000/2100 Series, ASA 5500-X Series, ISA 3000, FTDv).



**참고** FTD 고가용성 쌍을 버전 6.1.0으로 무중단 업그레이드하려면 사전 설치 패키지가 필요합니다. 자세한 내용은 [Firepower System 릴리스 노트 버전 6.1.0 사전 설치 패키지](#)를 참조하십시오.

왼쪽 열에서 현재 Firepower 버전을 찾습니다. 오른쪽 열에 나열된 버전으로 직접 업그레이드할 수 있습니다. 현재 버전에서 대상 버전으로 직접 업그레이드를 수행할 수 없는 경우, 안내와 같이 업그레이드 경로에 중간 버전이 포함되어야 합니다. 이 정보를 보는 다른 방법은 [직접 업그레이드가 가능한지?, 10 페이지](#)를 참조하십시오.

표 21: 직접 업그레이드: FMC를 사용하는 FTDv, Firepower 1000/2100 Series, ASA 5500-X Series, ISA 3000

현재 버전	대상 버전
6.7.0 6.7.x(유지 보수 릴리스)	다음 중 하나로: → 모든 6.7.x 이후 유지 보수 릴리스
6.6.0 6.6.x(유지 보수 릴리스) ASA 5525-X, 5545-X 및 5555-X에 대한 마지막 Firepower 지원입니다.	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 6.7.x 유지 보수 릴리스 → 모든 6.6.x 이후 유지 보수 릴리스
6.5.0	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 6.7.x 유지 보수 릴리스 → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스
6.4.0 ASA 5515-X에 대한 마지막 Firepower 지원입니다.	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 모든 6.7.x 유지 보수 릴리스 → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스 → 6.5.0
6.3.0	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 모든 6.7.x 유지 보수 릴리스 → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스 → 6.5.0 → 6.4.0

현재 버전	대상 버전
6.2.3 ASA 5506-X Series에 대한 마지막 Firepower 지원입니다.	다음 중 하나로 직접 업그레이드: → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스 → 6.5.0 → 6.4.0 → 6.3.0
6.2.2	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0 → 6.2.3
6.2.1	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.2.0	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	직접 업그레이드: → 6.1.0

## FTD 소프트웨어 업그레이드: 기타 FTD 디바이스

이 절차를 사용해 Firepower 1000/2100 series, ASA 5500-X series, ISA 3000 및 FTDv 디바이스를 업그레이드합니다. 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 FMC 업그레이드 포함)에서 현재 위치를 확인합니다. 이 단계를 완벽하게 계획하고 준비했는지 확인합니다.

**단계 1** 업그레이드하려는 디바이스에 컨피그레이션을 구축합니다.

FMC 메뉴 바에서 **Deploy**(구축)를 클릭합니다. 디바이스를 선택하고 **Deploy**(구축)를 다시 클릭합니다. 업그레이드하기 전에 배포하면 실패 가능성이 줄어듭니다.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 구성을 구축하면 Snort를 재시작하여 트래픽 검사가 중단되고, 디바이스가 트래픽을 처리하는 방법에 따라 재시작이 완료될 때까지 트래픽이 종료될 수 있습니다. 자세한 내용은 [FTD업그레이드 동작: 기타 장치, 245 페이지](#)를 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. 디스크 공간 요구 사항은 [시간 테스트 및 디스크 공간 요구 사항, 195 페이지](#)를 참조하십시오.

**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 FMC에서는 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 [FTD업그레이드 동작: 기타 장치, 245 페이지](#)를 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(SRU) 및 취약점 데이터베이스(VDB)를 업데이트합니다.

Cisco 지원 및 다운로드 사이트에서 제공되는 SRU 또는 VDB가 현재 실행 중인 버전보다 최신 상태이면 최신 버전을 설치합니다. 자세한 내용은 [Firepower Management Center 구성 가이드](#)를 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.





# 10 장

## Firepower 7000/8000 Series 및 NGIPSv 업그레이드

- 업그레이드 체크리스트: Firepower 7000/8000 Series 및 NGIPSv, 87 페이지
- 업그레이드 경로: Firepower 7000/8000 Series, 90 페이지
- 업그레이드 경로: NGIPSv, 91 페이지
- Firepower 7000/8000 Series 및 NGIPSv 업그레이드, 92 페이지

### 업그레이드 체크리스트: Firepower 7000/8000 Series 및 NGIPSv

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

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

<input type="checkbox"/>	작업/확인	세부 사항
	업그레이드 경로 확인 업그레이드 경로에서 현재 위치를 확인합니다. 방금 수행한 업그레이드와 다음에 수행할 업그레이드를 파악합니다.	업그레이드 경로: <a href="#">Firepower 7000/8000 Series, 90 페이지</a> 또는 업그레이드 경로: <a href="#">NGIPSv, 91 페이지</a>

□	작업/확인	세부 사항
	<b>버전 확인</b> 디바이스의 현재 버전과 대상 버전을 확인합니다. <ul style="list-style-type: none"> <li>• Firepower 소프트웨어</li> <li>• 가상 호스팅 환경(NGIPSv)</li> </ul>	<a href="#">Firepower 7000/8000 Series 및 레거시 디바이스, 138 페이지</a> 또는 <a href="#">NGIPSv, 150 페이지</a>
	<b>FMC 호환성 확인</b> 디바이스를 업그레이드한 후 FMC에서 해당 디바이스를 관리할 수 있는지 확인합니다. 디바이스를 관리할 수 없는 경우 FMC를 먼저 업그레이드할 수 있도록 업그레이드 경로를 수정합니다.	<a href="#">FMC 디바이스 버전 호환성을 유지할 수 있습니까?, 12 페이지</a>
	<b>릴리스 노트 읽기</b> 다음을 포함하여 업그레이드에 영향을 줄 수 있는 사항에 특히 주의하면서 릴리스 노트를 확인하십시오. <ul style="list-style-type: none"> <li>• 버전별 업그레이드 지침 및 경고</li> <li>• 업그레이드에 영향을 미치는 알려진 문제</li> <li>• 최신/지원 중단 기능</li> </ul>	<a href="#">Firepower 릴리스 노트</a>

## 업그레이드 전 작업 및 확인

유지 보수 기간이 아닐 때 사전 확인을 수행하여 중단을 최소화합니다.

□	작업/확인	세부 사항
	<b>필수 구성 변경 수행</b> 업그레이드 전 필수 구성 변경을 완료하고 업그레이드 후에 필요한 구성 변경을 준비하십시오.	<a href="#">Firepower 릴리스 노트</a>
	<b>디스크 공간 확인</b> Firepower 소프트웨어 업그레이드를 위한 예비 디스크 공간 확인을 실행합니다.	<a href="#">시간 테스트 및 디스크 공간 요구 사항, 195 페이지</a>
	<b>업그레이드 패키지 받기</b> 올바른 업그레이드 패키지를 입수하여 FMC에 업로드합니다. 서명된(.tar) 패키지의 압축을 풀지 마십시오.	<a href="#">Firepower 소프트웨어 업그레이드 패키지 다운로드, 21 페이지</a>
	<b>대역폭 확인</b> 관리되는 디바이스로 대량 데이터 전송을 수행할 수 있는 대역폭을 사용하고 있는지 확인합니다.	<a href="#">Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침(트러블슈팅 TechNote)</a>

□	작업/확인	세부 사항
	<b>Firepower</b> 소프트웨어 업그레이드 패키지 푸시 업그레이드 패키지를 디바이스에 푸시합니다. 버전 6.2.3 이상이 필요합니다.	<a href="#">FMC 관리 디바이스로 업그레이드 패키지 푸시, 28 페이지</a>
	<b>Firepower</b> 소프트웨어 준비도 확인 실행 준비 확인을 실행합니다. 버전 6.1 이상이 필요합니다.	<a href="#">Firepower 소프트웨어 준비도 확인 실행, 31 페이지</a>
	디바이스 백업 FMC를 사용해 7000/8000 Series 디바이스에 대한 구성 데이터를 백업합니다. 외부 위치에 백업한 후 전송 성공을 확인합니다. NGIPSv는 지원하지 않습니다.	<a href="#">Firepower Management Center 구성 가이드</a>
	어플라이언스 액세스 확인 사용 중인 컴퓨터가 디바이스 자체를 통과하지 않고 FMC의 관리 인터페이스와 디바이스의 관리 인터페이스에 모두 연결할 수 있는지 확인합니다.	<a href="#">어플라이언스 액세스, 커뮤니케이션 및 상태 확인, 35 페이지</a>
	<b>Maintenance Window</b> 예약 반드시 수행해야 하는 작업, 업그레이드가 트래픽 흐름 및 검사에 미치는 영향, 업그레이드 예상 소요 시간을 고려해 영향이 가장 적을 것으로 예상되는 유지 보수 기간을 예약합니다.	다음 중 하나에 해당합니다. <a href="#">Firepower 7000/8000 Series 업그레이드 동작, 247 페이지</a> <a href="#">NGIPSv 업그레이드 동작, 250 페이지</a> 및 <a href="#">시간 테스트 및 디스크 공간 요구 사항, 195 페이지</a>

디바이스 업그레이드

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

□	작업/확인	세부 사항
	호스팅 업그레이드 필요한 경우 호스팅 환경(NGIPSv)을 업그레이드합니다.	호스팅 환경 설명서를 참조하십시오.
	<b>Firepower</b> 소프트웨어 업그레이드 Firepower 소프트웨어를 업그레이드합니다.	<a href="#">Firepower 7000/8000 Series 및 NGIPSv 업그레이드, 92 페이지</a>

## 업그레이드 경로: Firepower 7000/8000 Series

이 테이블에는 Firepower Management Center에서 관리하는 Firepower 7000/8000 Series 디바이스의 업그레이드 경로가 나와 있습니다.



**참고** Firepower 7000/8000 Series 디바이스를 버전 6.0.0으로 업그레이드하려면 사전 설치 패키지가 필요합니다. 자세한 내용은 [FireSIGHT System 릴리스 노트 버전 6.0.0 사전 설치](#)를 참조하십시오.

왼쪽 열에서 현재 Firepower 버전을 찾습니다. 오른쪽 열에 나열된 버전으로 직접 업그레이드할 수 있습니다. 현재 버전에서 대상 버전으로 직접 업그레이드를 수행할 수 없는 경우, 안내와 같이 업그레이드 경로에 중간 버전이 포함되어야 합니다. 이 정보를 보는 다른 방법은 [직접 업그레이드가 가능한지?, 10 페이지](#)를 참조하십시오.

표 22: 직접 업그레이드: FMC를 사용하는 Firepower 7000/8000 Series

현재 버전	대상 버전
6.4.0	없음 버전 6.4.0은 Firepower 7000/8000 Series 디바이스의 마지막 주 릴리스입니다.
6.3.0	직접 업그레이드: → 6.4.0
6.2.3	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0
6.2.2	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0 → 6.2.3
6.2.0	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	직접 업그레이드: → 6.1.0

현재 버전	대상 버전
6.0.0	직접 업그레이드: → 6.0.1
5.4.0.2	직접 업그레이드: → 6.0.0

## 업그레이드 경로: NGIPSv

이 테이블에는 Firepower Management Center에서 관리하는 NGIPSv의 업그레이드 경로가 나와 있습니다.



**참고** NGIPSv를 버전 6.0.0으로 업그레이드하려면 사전 설치 패키지가 필요합니다. 자세한 내용은 [FireSIGHT System 릴리스 노트 버전 6.0.0 사전 설치](#)를 참조하십시오.

왼쪽 열에서 현재 Firepower 버전을 찾습니다. 오른쪽 열에 나열된 버전으로 직접 업그레이드할 수 있습니다. 현재 버전에서 대상 버전으로 직접 업그레이드를 수행할 수 없는 경우, 안내와 같이 업그레이드 경로에 중간 버전이 포함되어야 합니다. 이 정보를 보는 다른 방법은 [직접 업그레이드가 가능합니까?, 10 페이지](#)를 참조하십시오.

표 23: 직접 업그레이드: FMC를 사용하는 NGIPSv

현재 버전	대상 버전
6.7.0 6.7.x(유지 보수 릴리스)	다음 중 하나로: → 모든 6.7.x 이후 유지 보수 릴리스
6.6.0 6.6.x(유지 보수 릴리스)	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 모든 6.7.x 유지 보수 릴리스 → 모든 6.6.x 이후 유지 보수 릴리스
6.5.0	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 모든 6.7.x 유지 보수 릴리스 → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스
6.4.0	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 모든 6.7.x 유지 보수 릴리스 → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스 → 6.5.0

현재 버전	대상 버전
6.3.0	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 모든 6.7.x 유지 보수 릴리스 → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스 → 6.5.0 → 6.4.0
6.2.3	다음 중 하나로 직접 업그레이드: → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스 → 6.5.0 → 6.4.0 → 6.3.0
6.2.2	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0
6.2.0	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	직접 업그레이드: → 6.1.0
6.0.0	직접 업그레이드: → 6.0.1
5.4.1.1	직접 업그레이드: → 6.0.0

## 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 FMC 업그레이드 포함)에서 현재 위치를 확인합니다. 이 단계를 완벽하게 계획하고 준비했는지 확인합니다.

**단계 1** 업그레이드하려는 디바이스에 컨피그레이션을 구축합니다.

FMC 메뉴 바에서 **Deploy(구축)**를 클릭합니다. 디바이스를 선택하고 **Deploy(구축)**를 다시 클릭합니다. 업그레이드하기 전에 배포하면 실패 가능성이 줄어듭니다.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 구성을 구축하면 Snort를 재시작하여 트래픽 검사가 중단되고, 디바이스가 트래픽을 처리하는 방법에 따라 재시작이 완료될 때까지 트래픽이 종료될 수 있습니다. 자세한 내용은 [Firepower 7000/8000 Series 업그레이드 동작, 247 페이지](#) 또는 [NGIPSv 업그레이드 동작, 250 페이지](#)를 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. 디스크 공간 요구 사항은 [시간 테스트 및 디스크 공간 요구 사항, 195 페이지](#)를 참조하십시오.

**단계 3** (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 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 FMC에서는 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 [Firepower 7000/8000 Series 업그레이드 동작, 247 페이지](#) 또는 [NGIPSv 업그레이드 동작, 250 페이지](#)를 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(SRU) 및 취약점 데이터베이스(VDB)를 업데이트합니다.

Cisco 지원 및 다운로드 사이트에서 제공되는 SRU 또는 VDB가 현재 실행 중인 버전보다 최신 상태이면 최신 버전을 설치합니다. 자세한 내용은 [Firepower Management Center 구성 가이드](#)를 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.



# 11 장

## ASA with FirePOWER Services 업그레이드

- 업그레이드 체크리스트: ASA with FirePOWER Services, 95 페이지
- 업그레이드 경로: ASA FirePOWER, 98 페이지
- ASA 업그레이드, 101 페이지
- ASA FirePOWER 모듈 업그레이드, 124 페이지

### 업그레이드 체크리스트: ASA with FirePOWER Services

이 체크리스트를 참조하여 ASA with FirePOWER Services를 업그레이드합니다.

업그레이드할 때마다 체크리스트를 작성하십시오. 단계를 건너뛰면 업그레이드에 실패할 수 있습니다. 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
	<b>업그레이드 경로 확인</b> 업그레이드 경로에서 현재 위치를 확인합니다. 방금 수행한 업그레이드와 다음에 수행할 업그레이드를 파악합니다.	<a href="#">업그레이드 경로: ASA FirePOWER, 98 페이지</a>
	<b>버전 확인</b> 디바이스의 현재 버전과 대상 버전을 확인합니다. <ul style="list-style-type: none"> <li>• ASA FirePOWER 모듈</li> <li>• ASA OS</li> </ul>	<a href="#">ASA 5500-X Series 및 ISA 3000 with FirePOWER Services, 138 페이지</a>

□	작업/확인	세부 사항
	<b>FMC 호환성 확인</b> 디바이스를 업그레이드한 후 FMC에서 해당 디바이스를 관리할 수 있는지 확인합니다. 디바이스를 관리할 수 없는 경우 FMC를 먼저 업그레이드할 수 있도록 업그레이드 경로를 수정합니다.	FMC 디바이스 버전 호환성을 유지할 수 있습니까?, 12 페이지
	릴리스 노트 읽기 다음을 포함하여 업그레이드에 영향을 줄 수 있는 사항에 특히 주의하면서 릴리스 노트를 확인하십시오. <ul style="list-style-type: none"> <li>• 버전별 업그레이드 지침 및 경고</li> <li>• 업그레이드에 영향을 미치는 알려진 문제</li> <li>• 최신/지원 중단 기능</li> </ul>	Firepower 릴리스 노트 및 ASA 릴리스 노트

## 업그레이드 전 작업 및 확인

유지 보수 기간이 아닐 때 사전 확인을 수행하여 중단을 최소화합니다.

□	작업/확인	세부 사항
	<b>필수 구성 변경 수행</b> 업그레이드 전 필수 구성 변경을 완료하고 업그레이드 후에 필요한 구성 변경을 준비하십시오.	Firepower 릴리스 노트 및 Cisco ASA 업그레이드 가이드의 업그레이드 계획
	<b>디스크 공간 확인</b> Firepower 소프트웨어 업그레이드를 위한 예비 디스크 공간 확인을 실행합니다.	시간 테스트 및 디스크 공간 요구 사항, 195 페이지
	<b>업그레이드 패키지 받기</b> 올바른 업그레이드 패키지를 입수하여 FMC에 업로드합니다. 서명된(.tar) 패키지의 압축을 풀지 마십시오.	Firepower 소프트웨어 업그레이드 패키지 다운로드, 21 페이지
	<b>대역폭 확인</b> 관리되는 디바이스로 대량 데이터 전송을 수행할 수 있는 대역폭을 사용하고 있는지 확인합니다.	Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침(트러블슈팅 TechNote)
	<b>Firepower 소프트웨어 업그레이드 패키지 푸시</b> 업그레이드 패키지를 디바이스에 푸시합니다. 버전 6.2.3 이상이 필요합니다.	FMC 관리 디바이스로 업그레이드 패키지 푸시, 28 페이지

□	작업/확인	세부 사항
	<b>Firepower</b> 소프트웨어 준비도 확인 실행 준비 확인을 실행합니다. 버전 6.1 이상이 필요합니다.	<a href="#">Firepower 소프트웨어 준비도 확인 실행, 31 페이지</a>
	어플라이언스 액세스 확인 사용 중인 컴퓨터가 디바이스 자체를 통과하지 않고 FMC의 관리 인터페이스와 디바이스의 관리 인터페이스에 모두 연결할 수 있는지 확인합니다.	<a href="#">어플라이언스 액세스, 커뮤니티 케이션 및 상태 확인, 35 페이지</a>
	<b>Maintenance Window</b> 예약 반드시 수행해야 하는 작업, 업그레이드가 트래픽 흐름 및 검사에 미치는 영향, 업그레이드 예상 소요 시간을 고려해 영향이 가장 적을 것으로 예상되는 유지 보수 기간을 예약합니다.	<a href="#">ASA FirePOWER 업그레이드 동작, 249 페이지</a> 및 <a href="#">시간 테스트 및 디스크 공간 요구 사항, 195 페이지</a>

**ASA 및 ASA with FirePOWER Services** 업그레이드

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

□	작업/확인	세부 사항
	독립 실행형 <b>ASA</b> 디바이스 업그레이드 독립형 ASA 디바이스에서 ASA FirePOWER 모듈을 업그레이드합니다. ASA도 업그레이드하는 중인 경우 FMC를 사용해 ASA를 업그레이드하고 다시 로드한 후 ASA FirePOWER 모듈을 업그레이드합니다.	<a href="#">독립형 유닛 업그레이드, 101 페이지</a> 및 <a href="#">ASA FirePOWER 모듈 업그레이드, 124 페이지</a>
	<b>ASA</b> 클러스터 및 페일오버 쌍 업그레이드 러스터 및 페일오버 쌍의 ASA 디바이스에서 ASA 및 ASA FirePOWER 모듈을 업그레이드합니다. 트래픽 흐름 및 검사 중단을 방지하려면 이러한 디바이스를 한 번에 하나씩 완전히 업그레이드하십시오. ASA도 업그레이드하는 중인 경우 FMC를 사용해 ASA를 업그레이드하기 위해 각 유닛을 다시 로드하기 직전에 ASA FirePOWER 모듈을 업그레이드합니다.	다음 중 하나에 해당합니다. <a href="#">액티브/스탠바이 페일오버 쌍 업그레이드, 106 페이지</a> <a href="#">액티브/액티브 페일오버 쌍 업그레이드, 111 페이지</a> <a href="#">ASA 클러스터 업그레이드, 116 페이지</a> 및 <a href="#">ASA FirePOWER 모듈 업그레이드, 124 페이지</a>

## 업그레이드 경로: ASA FirePOWER

이 테이블은 Firepower Management Center에서 관리되는 ASA FirePOWER 모듈의 업그레이드 경로를 제공합니다.



**참고** ASA FirePOWER를 버전 6.0.0으로 업그레이드하려면 사전 설치 패키지가 필요합니다. 자세한 내용은 [FireSIGHT System 릴리스 노트 버전 6.0.0 사전 설치](#)를 참조하십시오.

왼쪽 열에서 현재 Firepower 버전을 찾습니다. 오른쪽 열에 나열된 버전으로 직접 업그레이드할 수 있습니다. 현재 버전에서 대상 버전으로 직접 업그레이드를 수행할 수 없는 경우, 안내와 같이 업그레이드 경로에 중간 버전이 포함되어야 합니다. 이 정보를 보는 다른 방법은 [직접 업그레이드가 가능합니까?, 10 페이지](#)를 참조하십시오.

표 24: 직접 업그레이드: FMC를 사용하는 ASA FirePOWER

현재 버전	대상 버전
6.7.0 6.7.x(유지 보수 릴리스)	다음 중 하나로: → 모든 6.7.x 이후 유지 보수 릴리스
6.6.0 6.6.x(유지 보수 릴리스) ASA 5525-X, 5545-X 및 5555-X에 대한 마지막 Firepower 지원입니다.	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 모든 6.7.x 유지 보수 릴리스 → 모든 6.6.x 이후 유지 보수 릴리스
6.5.0	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 모든 6.7.x 유지 보수 릴리스 → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스
6.4.0 ASA 5585-X Series 및 ASA 5510-X에 대한 마지막 Firepower 지원입니다.	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 모든 6.7.x 유지 보수 릴리스 → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스 → 6.5.0
6.3.0	다음 중 하나로 직접 업그레이드: → 6.7.0 또는 모든 6.7.x 유지 보수 릴리스 → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스 → 6.5.0 → 6.4.0
6.2.3 ASA 5506-X Series 및 ASA 5512-X에 대한 마지막 Firepower 지원입니다.	다음 중 하나로 직접 업그레이드: → 6.6.0 또는 모든 6.6.x 유지 보수 릴리스 → 6.5.0 → 6.4.0 → 6.3.0

현재 버전	대상 버전
6.2.2	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0 → 6.2.3
6.2.0	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	다음 중 하나로 직접 업그레이드: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	직접 업그레이드: → 6.1.0
6.0.0	직접 업그레이드: → 6.0.1
5.4.0.2 또는 5.4.1.1	직접 업그레이드: → 6.0.0

### ASA 업그레이드

ASA 및 ASA FirePOWER 버전은 광범위하게 호환됩니다. 하지만 ASA 업그레이드가 필요하지 않더라도 문제를 해결하려면 지원되는 최신 버전으로 업그레이드해야 할 수 있습니다. 자세한 호환성 정보는 [ASA 5500-X Series 및 ISA 3000 with FirePOWER Services, 138 페이지](#)를 참조하십시오.

ASA 클러스터링 또는 페일오버 쌍이 구성되어 있더라도 각 디바이스에서 ASA를 독립적으로 업그레이드합니다. ASA FirePOWER 모듈(ASA 리로드 전후)을 업그레이드하는 시기는 구축에 따라 달라집니다. 이 테이블에서는 독립형 및 HA/확장성 구축에 대한 ASA 업그레이드 순서를 간략하게 설명합니다. 자세한 내용은 [ASA 업그레이드, 101 페이지](#)를 참고하십시오.

표 25: ASA + ASA FirePOWER 업그레이드 순서

ASA 구축	업그레이드 순서
독립형 디바이스	<ol style="list-style-type: none"> <li>1. 다시 로드를 포함해 ASA를 업그레이드합니다.</li> <li>2. ASA FirePOWER을 업그레이드합니다.</li> </ol>

ASA 구축	업그레이드 순서
ASA 페일오버: 액티브/ 스탠바이	<p>항상 스탠바이 유닛을 업그레이드합니다.</p> <ol style="list-style-type: none"> <li>1. 스탠바이에서 ASA를 업그레이드하지만 다시 로드하지 않습니다.</li> <li>2. 스탠바이에서 ASA FirePOWER을 업그레이드합니다.</li> <li>3. 스탠바이에서 ASA를 다시 로드합니다.</li> <li>4. 페일오버를 수행합니다.</li> <li>5. 새 스탠바이 유닛의 ASA를 업그레이드합니다.</li> <li>6. 새 스탠바이에서 ASA FirePOWER을 업그레이드합니다.</li> <li>7. 새 스탠바이에서 ASA를 다시 로드합니다.</li> </ol>
ASA 페일오버: 액티브/ 액티브	<p>업그레이드하지 않은 유닛에서 두 페일오버 그룹을 액티브로 설정합니다.</p> <ol style="list-style-type: none"> <li>1. 기본 유닛에서 두 페일오버 그룹을 모두 액티브로 설정합니다.</li> <li>2. 보조에서 ASA를 업그레이드하지만 다시 로드하지 않습니다.</li> <li>3. 보조에서 ASA FirePOWER를 업그레이드합니다.</li> <li>4. 보조에 ASA를 다시 로드합니다.</li> <li>5. 보조 유닛에서 두 페일오버 그룹을 액티브로 설정합니다.</li> <li>6. 기본에서 ASA를 업그레이드하지만 다시 로드하지 않습니다.</li> <li>7. 기본에서 ASA FirePOWER를 업그레이드합니다.</li> <li>8. 기본에서 ASA를 다시 로드합니다.</li> </ol>



ASA 구축	업그레이드 순서
ASA 클러스터	<p>업그레이드하기 전에 각 유닛에 클러스터링을 사용하지 않도록 설정합니다. 한 번에 하나의 유닛을 업그레이드하고 제어 유닛을 마지막으로 남겨둡니다.</p> <ol style="list-style-type: none"> <li>1. 데이터 유닛의 클러스터링을 비활성화합니다.</li> <li>2. 해당 데이터 유닛에서 ASA를 업그레이드하지만, 다시 로드하지 않습니다.</li> <li>3. 유닛에서 ASA FirePOWER를 업그레이드합니다.</li> <li>4. ASA를 다시 로드합니다.</li> <li>5. 클러스터링을 다시 활성화합니다. 유닛이 클러스터에 다시 참여할 때까지 대기합니다.</li> <li>6. 각 데이터 유닛에 대해 위의 단계를 반복합니다.</li> <li>7. 제어 유닛에서 클러스터링을 비활성화합니다. 새 제어 권한을 확보할 때까지 기다립니다.</li> <li>8. 이전 제어 유닛에서 ASA를 업그레이드하지만, 다시 로드하지 않습니다.</li> <li>9. 이전 제어 유닛에서 ASA FirePOWER를 업그레이드합니다.</li> <li>10. 클러스터링을 다시 활성화합니다.</li> </ol>

## 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 참조](#)에서 copy 명령을 참조하십시오.

단계 1 특권 실행 모드에서 ASA 소프트웨어를 플래시 메모리에 복사합니다.

**copy ftp://[[user[:password]]@]server[/path]/asa\_image\_name disk://[path]/asa\_image\_name**

예제:

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asa-9-12-1-smp-k8.bin disk0:/asa-9-12-1-smp-k8.bin
```

단계 2 ASDM 이미지를 플래시 메모리에 복사합니다.

**copy ftp://[[user[:password]]@]server[/path]/asdm\_image\_name disk://[path]/asdm\_image\_name**

예제:

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-7121.bin disk0:/asdm-7121.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://[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://[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:/asa-9-12-1-smp-k8.bin
```

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

**asdm image diskn:[/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-7121.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.

ASDM을 사용하여 로컬 컴퓨터에서 독립형 유닛 업그레이드

- 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.
- Save the running configuration at the time of reload**(다시 로드 시 실행 중인 구성 저장) 라디오 버튼을(기본값)을 클릭합니다.
  - 다시 로드할 시간(예: 기본값인 **Now**(지금))을 선택합니다.
  - 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 9.9(1)을 다운로드했지만 다운로드 버전이 9.9(1.2)일 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 다시 로드하여 구성을 저장하고 업그레이드를 완료합니다.

시작하기 전에

내부 변경으로 마법사는 ASDM 7.10(1) 및 이후 버전만 지원합니다. 또한 이미지 이름 변경으로 ASDM 7.12(1) 또는 이후 버전을 사용해 ASA 9.10(1) 이후 버전을 업그레이드해야 합니다. ASDM은 이전 ASA 릴리스와 역으로 호환되므로 실행 중인 ASA 버전에 관계없이 ASDM을 업그레이드할 수 있습니다.

**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.

**Cisco.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.**

- ASA 영역에서 Upgrade to(다음으로 업그레이드)** 확인란을 선택한 다음 드롭다운 목록에서 어떤 ASA 버전으로 업그레이드할지 선택합니다.

- b) **ASDM** 영역에서 **Upgrade to**(다음으로 업그레이드) 확인란을 선택한 다음 드롭다운 목록에서 어떤 ASDM 버전으로 업그레이드할지 선택합니다.

단계 5 **Next**(다음)를 클릭하면 **Review Changes**(변경사항 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 참조**에서 **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 diskn:[/path]/asa\_image\_name**

예제:

```
asa/act# copy ftp://jcrichon:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin disk0:/asa9829-15-1-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 diskn:[/path]/asa\_image\_name**

예제:

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichon:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin disk0:/asa9829-15-1-smp-k8.bin
```

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

**copy ftp://[[user[:password]]@]server[/path]/asdm\_image\_name diskn:[/path]/asdm\_image\_name**

예제:

```
asa/act# copy ftp://jcrichon:aeryn@10.1.1.1/asdm-77178271417151.bin disk0:/asdm-77178271417151.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 diskn:[/path]/asdm\_image\_name**

예제:

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichon:aeryn@10.1.1.1/asdm-77178271417151.bin
```

CLI를 사용하여 액티브/스탠바이 페일오버 쌍 업그레이드

```
disk0:/asdm-77178271417151.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 diskn:[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 diskn:[path]asa\_image\_name**

예제:

```
asa/act(config)# boot system disk0://asa9829-15-1-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 diskn:[path]asdm\_image\_name**

예제:

```
asa/act(config)# asdm image disk0:/asdm-77178271417151.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 상태를 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 디렉토리 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**를 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 페일오버 합니다.

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 참조](#)에서 **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:/[path]/asa_image_name
```

예제:

```
asa/act/pri# copy ftp://jcrichon:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin disk0:/asa9829-15-1-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:/[path]/asa_image_name
```

예제:

```
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichon:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin
```

CLI를 사용하여 액티브/액티브 페일오버 쌍 업그레이드

```
disk0:/asa9829-15-1-smp-k8.bin
```

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

**copy ftp://[[user[:password]]@]server[/path]/asdm\_image\_name diskn:[/path]/asdm\_image\_name**

예제:

```
asa/act/pri# ciscoasa# copy ftp://jcrichon:aeryn@10.1.1.1/asdm-77178271417151.bin
disk0:/asdm-77178271417151.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  
diskn:[/path]/asdm\_image\_name**

예제:

```
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichon:aeryn@10.1.1.1/asdm-77178271417151.bin
disk0:/asdm-77178271417151.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 diskn:[/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 diskn:[/path]/asa\_image\_name**

예제:

```
asa/act/pri(config)# boot system disk0://asa9829-15-1-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 diskn:[path/]asdm_image_name
```

예제:

```
asa/act/pri(config)# asdm image disk0://asdm-77178271417151.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 상태를 확인합니다.

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

```
no failover active group 1
```

```
no failover active group 2
```

예제:

## ASDM을 사용하여 액티브/액티브 페일오버 쌍 업그레이드

```
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 디렉토리 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**(아니오)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**(아니오)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**를 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 참조](#)에서 **copy** 명령을 참조하십시오.

시작하기 전에

- 제어 유닛에서 다음 단계를 수행합니다. ASA FirePOWER 모듈도 업그레이드하는 경우에는 각 데이터 유닛에서 콘솔 또는 ASDM에 액세스해야 합니다. 클러스터 유닛과 상태(제어 또는 데이터)를 표시하도록 ASA 프롬프트를 설정할 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 제어 유닛에서 ASA 소프트웨어를 클러스터의 모든 유닛에 복사합니다.

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

예제:

```
asa/unit1/master# cluster exec copy /noconfirm
ftp://jcrichon:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin disk0:/asa9829-15-1-smp-k8.bin
```

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

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



예제:

```
asa/unit1/master# cluster exec copy /noconfirm ftp://jcrichon:aeryn@10.1.1.1/asdm-77178271417151.bin
disk0:/asdm-77178271417151.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 diskn:[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 diskn:[path]asa\_image\_name**

예제:

```
asa/unit1/master(config)# boot system disk0://asa9829-15-1-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 diskn:[path]asdm\_image\_name**

예제:

```
asa/unit1/master(config)# asdm image disk0:/asdm-77178271417151.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 구성 변경 사항은 데이터 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 poolname**을 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** 데이터 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 데이터 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 데이터 유닛을 제어로 강제 지정하지 마십시오. 이렇게 하면 네트워크 연결 및 클러스터 안정성 관련 문제가 발생할 수 있습니다. 전체 데이터 유닛을 먼저 업그레이드하고 다시 로드한 다음, 이 절차를 계속 진행하여 현재 제어 유닛에서 새 제어 유닛으로 원활하게 전환해야 합니다.

**ASA FirePOWER** 모듈을 업그레이드하지 않는 경우:

- a) 제어 유닛에서 멤버 이름을 보려면 **cluster exec unit ?**를 입력하거나 **show cluster info** 명령을 입력합니다.
- b) 데이터 유닛을 다시로드합니다.

**cluster exec unit data-unit reload noconfirm**

예제:

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

- c) 각 데이터 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 클러스터에 언제 다시 합류하는지 확인하려면 **show cluster info**를 입력합니다.

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

- a) 데이터 유닛의 콘솔 포트에 연결한 다음 전역 구성 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 데이터 유닛에서 ASA FirePOWER 모듈을 업그레이드합니다.

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

- d) 데이터 유닛을 다시 로드합니다.

**reload noconfirm**

- e) 각 데이터 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 클러스터에 언제 다시 합류하는지 확인하려면 **show cluster info**를 입력합니다.

ASDM을 사용하여 ASA FirePOWER 모듈도 업그레이드하는 경우:

- 앞에서 확인한 이 데이터 유닛의 개별 관리 IP 주소에 ASDM을 연결합니다.
- Configuration(구성) > Device Management High Availability and Scalability(디바이스 관리 고가용성 및 확장성) > ASA Cluster(ASA 클러스터) > Cluster Configuration(클러스터 구성)**을 선택합니다.
- 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** 이름 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.

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

업그레이드가 완료될 때까지 기다립니다.

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

- Schedule Reload(다시 로드 예약)**를 클릭합니다.
- Yes(예)**를 클릭하여 다시 로드를 계속합니다.
- 각 데이터 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 제어 유닛에서 **Monitoring(모니터링) > ASA Cluster(ASA 클러스터) > Cluster Summary(클러스터 요약)** 패널을 확인합니다.

단계 12 제어 유닛을 업그레이드합니다.

- a) 클러스터링을 비활성화합니다.

**cluster group name**

**no enable**

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

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

새 제어 유닛이 최대한 확실하고 빠르게 선택될 수 있도록 가능하면 제어 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 제어 유닛에 속합니다. 개별 관리 IP 주소에서는 이 이전 제어 유닛에 계속 액세스할 수 있습니다.

업그레이드가 완료될 때까지 기다립니다.

- c) 이 유닛을 다시 로드합니다.

**reload noconfirm**

이전의 제어 유닛은 다시 클러스터에 합류하면 데이터 유닛이 됩니다.

## ASDM을 사용하여 ASA 클러스터 업그레이드

ASA 클러스터의 모든 유닛을 업그레이드하려면 다음 단계를 수행합니다.

시작하기 전에

- 제어 유닛에서 다음 단계를 수행합니다. ASA FirePOWER 모듈도 업그레이드하는 경우에는 각 데이터 유닛에 대한 ASDM 액세스 권한이 필요합니다.
- 여러 컨텍스트 모드인 경우 시스템 실행 영역에서 다음 단계를 수행합니다.

- 로컬 관리 컴퓨터에 ASA 및 ASDM 이미지를 저장합니다.

- 
- 단계 1** 주 클러스터 IP 주소에 연결하여 제어 유닛에서 ASDM을 실행합니다.  
이 IP 주소는 항상 제어 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 데이터 유닛에 자동으로 저장됩니다.
- 단계 12** 나중에 ASDM을 데이터 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 멤버)**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**를 입력하여 ASA REST API를 비활성화합니다.  
REST API를 비활성화하지 않으면 ASA FirePOWER 모듈 업그레이드에 실패하게 됩니다.
- 단계 14** 데이터 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) 페이지에서 데이터 유닛이 제어 유닛이 되도록 제어 유닛을 변경하지 마십시오. 이렇게 하면 네트워크 연결 및 클러스터 안정성 관련 문제가 발생할 수 있습니다. 전체 데이터 유닛을 먼저 다시 로드한 다음, 이 절차를 계속 진행하여 현재 제어 유닛에서 새 제어 유닛으로 원활하게 전환해야 합니다.

**ASA FirePOWER** 모듈을 업그레이드하지 않는 경우:

- 제어 유닛에서 **Tools**(툴) > **System Reload**(시스템 다시 로드)를 선택합니다.
- Device**(디바이스) 드롭다운 목록에서 데이터 유닛 이름을 선택합니다.
- Schedule Reload**(다시 로드 예약)를 클릭합니다.
- Yes**(예)를 클릭하여 다시 로드를 계속합니다.
- 각 데이터 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) 패널을 확인합니다.

**ASA FirePOWER** 모듈도 업그레이드하는 경우:

- 제어 유닛에서 **Configuration**(컨피그레이션) > **Device Management**(디바이스 관리) > **High Availability and Scalability**(고가용성 및 확장성) > **ASA Cluster**(ASA 클러스터) > **Cluster Members**(클러스터 멤버)를 선택합니다.
- 업그레이드할 데이터 유닛을 선택하고 **Delete**(삭제)를 클릭합니다.
- Apply**(적용)를 클릭합니다.
- ASDM을 종료하고 앞에서 확인한 개별 관리 IP 주소에 연결하여 데이터 유닛에 ASDM을 연결합니다.
- ASA FirePOWER 모듈을 업그레이드합니다.

업그레이드가 완료될 때까지 기다립니다.

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

- Schedule Reload**(다시 로드 예약)를 클릭합니다.
- Yes**(예)를 클릭하여 다시 로드를 계속합니다.
- 각 데이터 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) 패널을 확인합니다.

**단계 15** 제어 유닛을 업그레이드합니다.

- a) 제어 유닛의 ASDM에서 **Configuration**(컨피그레이션) > **Device Management**(디바이스 관리) > **High Availability and Scalability**(고가용성 및 확장성) > **ASA Cluster**(ASA 클러스터) > **Cluster Configuration**(클러스터 컨피그레이션) 패널을 선택합니다.
- b) **Participate in ASA cluster**(ASA 클러스터에 참여) 체크 박스를 선택 취소하고 **Apply**(적용)를 클릭합니다.  
ASDM을 종료하라는 메시지가 표시됩니다.
- c) 새 제어 유닛이 선택되고 트래픽이 안정화될 때까지 최대 5분간 기다립니다.  
이전의 제어 유닛은 다시 클러스터에 합류하면 데이터 유닛이 됩니다.
- d) 앞에서 확인한 개별 관리 IP 주소에 연결하여 ASDM을 이전 제어 유닛에 다시 연결합니다.  
주 클러스터 IP 주소는 이제 새 제어 유닛에 속합니다. 개별 관리 IP 주소에서는 이 이전 제어 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 제어 유닛에 다시 연결됩니다.

## ASA FirePOWER 모듈 업그레이드

FMC로 관리되는 ASA FirePOWER 모듈을 업그레이드하려면 이 절차를 사용합니다. 모듈을 업그레이드하는 시기는 ASA 업그레이드 여부 및 ASA 구축에 따라 달라집니다.

- 독립형 ASA 디바이스 업그레이드: ASA도 업그레이드하는 중인 경우 FMC를 사용해 ASA를 업그레이드하고 다시 로드한 후 ASA FirePOWER 모듈을 업그레이드합니다.
- ASA 클러스터 및 페일오버 쌍 업그레이드: "트래픽 흐름 및 검사 중단을 방지하려면 이러한 디바이스를 한 번에 하나씩 완전히 업그레이드하십시오. ASA도 업그레이드하는 중인 경우 FMC를 사용해 ASA를 업그레이드하기 위해 각 유닛을 다시 로드하기 직전에 ASA FirePOWER 모듈을 업그레이드합니다.

자세한 내용은 [업그레이드 경로: ASA FirePOWER, 98 페이지](#) 및 ASA 업그레이드 절차를 참조하십시오.





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 FMC 업그레이드 포함)에서 현재 위치를 확인합니다. 이 단계를 완벽하게 계획하고 준비했는지 확인합니다.

**단계 1** 업그레이드하려는 디바이스에 컨피그레이션을 구축합니다.

FMC 메뉴 바에서 **Deploy**(구축)를 클릭합니다. 디바이스를 선택하고 **Deploy**(구축)를 다시 클릭합니다. 업그레이드하기 전에 배포하면 실패 가능성이 줄어듭니다.

구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 구성을 구축하면 Snort를 재시작하여 트래픽 검사가 중단되고, 디바이스가 트래픽을 처리하는 방법에 따라 재시작이 완료될 때까지 트래픽이 종료될 수 있습니다. 자세한 내용은 [ASA FirePOWER 업그레이드 동작, 249 페이지](#)를 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. 디스크 공간 요구 사항은 [시간 테스트 및 디스크 공간 요구 사항, 195 페이지](#)를 참조하십시오.

**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 FMC에서는 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, 249 페이지](#)를 참조하십시오.

**단계 7 Message Center**에서 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 Center**를 사용하여 구축 상태를 다시 확인합니다.

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

Cisco 지원 및 다운로드 사이트에서 제공되는 SRU 또는 VDB가 현재 실행 중인 버전보다 최신 상태이면 최신 버전을 설치합니다. 자세한 내용은 [Firepower Management Center 구성 가이드](#)을 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.



## III 부

### 참조

- 호환성, 129 페이지
- 버전별 Firepower 소프트웨어 업그레이드 지침, 153 페이지
- 시간 테스트 및 디스크 공간 요구 사항, 195 페이지
- 트래픽 흐름, 검사 및 디바이스 동작, 241 페이지





# 12 장

## 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. 추가 정보는 [Cisco FirePOWER 호환성 가이드](#)를 참조하십시오.

- [Firepower Management Center, 129 페이지](#)
- [Firepower 디바이스, 133 페이지](#)

## Firepower Management Center

### Firepower Management Center: 물리적

표 26: Firepower Management Center 호환성

Firepower 버전	FMC 1600 FMC 2600 FMC 4600	FMC 1000 FMC 2500 FMC 4500	FMC 2000 FMC 4000	FMC 750 FMC 1500 FMC 3500	DC 500 DC 1000 DC 3000
6.7.x	예	예	—	—	—
6.6.x	예	예	예	—	—
6.5.0	예	예	예	—	—
6.4.0	예	예	예	예	—
6.3.0	예	예	예	예	—
6.2.3	—	예	예	예	—

Firepower 버전	FMC 1600	FMC 1000	FMC 2000	FMC 750	DC 500
	FMC 2600	FMC 2500	FMC 4000	FMC 1500	DC 1000
	FMC 4600	FMC 4500		FMC 3500	DC 3000
6.2.2	—	예	예	예	—
6.2.1	—	예	예	예	—
6.2.0	—	예	예	예	—
6.1.0	—	—	예	예	—
6.0.1	—	—	예	예	—
6.0.0	—	—	예	예	—
5.4.1	—	—	예	예	예
5.4.0*	—	—	예	예	예

\* 5.4.0만 해당됩니다. 5.4.x 디바이스를 관리하려면 5.4.1.x Defense Center 사용하십시오.

## Firepower Management Center: 가상

이 테이블에는 FMCv에 대한 Firepower 호환성 및 가상 호스팅 환경 요구 사항이 나와 있습니다. VMware에 대한 FMCv 300 지원은 버전 6.5.0부터 지원됩니다.

표 27: FMCv 호환성: VMware용 Firepower 버전 6.2.3 이상

Firepower 버전	VMware vSphere/VMware ESXi				
	6.7	6.5	6.0	5.5	5.1
6.7.x	예	예	예	—	—
6.6.x	예	예	예	—	—
6.5.0	예	예	예	—	—
6.4.0	—	예	예	—	—
6.3.0	—	예	예	—	—
6.2.3	—	예	예	예	—

표 28: FMCv 호환성: VMware용 Firepower 버전 5.4-6.2.2 이상

Firepower 버전	VMware vSphere/VMware ESXi				VMware vCloud Director
	6.0	5.5	5.1	5.0	
6.2.2	예	예	—	—	—
6.2.1	예	예	—	—	—
6.2.0	예	예	—	—	—
6.1.0	예	예	—	—	—
6.0.1	—	예	예	—	—
6.0.0	—	예	예	—	—
5.4.1	—	예	예	예	예
5.4.0*	—	예	예	예	예

\*5.4.0만 해당, 5.4.x 디바이스를 관리하려면 5.4.1.x Defense Center 사용

표 29: FMCv 호환성: 기타 하이퍼 바이저

Firepower 버전	AWS(Amazon Web Services)	Microsoft Azure	OCI(Oracle Cloud Infrastructure)	GCP(Google Cloud Platform)	KVM(Kernel-Based Virtual Machine)
6.7.x	예	예	예	예	예
6.6.x	예	예	—	—	예
6.5.0	예	예	—	—	예
6.4.0	예	예	—	—	예
6.3.0	예	—	—	—	예
6.2.3	예	—	—	—	예
6.2.2	예	—	—	—	예
6.2.1	예	—	—	—	예
6.2.0	예	—	—	—	예
6.1.0	예	—	—	—	예
6.0.1	예	—	—	—	—

## FMC용 BIOS 및 펌웨어

BIOS 및 RAID 컨트롤러 펌웨어에 대한 업데이트를 제공합니다. FMC가 다음 테이블에 나열된 요구 사항을 충족하지 않으면 적절한 핫픽스를 적용합니다. FMC가 목록에 없으면 공장 기본값이 최소 요구 사항을 충족하는 것입니다.

표 30: BIOS 및 펌웨어 최소 요구 사항

Platform(플랫폼)	Firepower 버전	BIOS	RAID 컨트롤러 펌웨어	Hotfix
FMC 1600, 2600, 4600	6.3.0 이상	C220M5.4.1.1c.0	51.10.0-2978	BIOS 업데이트 핫픽스 EC
FMC 1000, 2500, 4500	6.2.3 이상	C220M4.4.0.2d.0	24.12.1-0433	BIOS 업데이트 핫픽스 CJ
FMC 2000, 4000	6.2.3~6.6.x	C220M3.2.0.8.0	23.33.0-0049	BIOS 업데이트 핫픽스 CJ

핫픽스는 BIOS 및 RAID 컨트롤러 펌웨어를 업데이트할 수 있는 유일한 방법입니다. Firepower 소프트웨어를 업그레이드해도 이 작업을 수행할 수 없으며, 이후 버전으로 이미지를 재설치할 수도 없습니다. 핫픽스를 적용하면 CIMC 펌웨어도 업데이트됩니다. FMC에서는 CIMC를 사용한 구성 변경을 지원하지는 않지만, 문제가 있는 경우 핫픽스를 적용하십시오. FMC가 이미 최신 상태라면 핫픽스가 적용되지 않습니다.

핫픽스를 적용하려면 일반 업그레이드 프로세스를 사용하십시오. Cisco 지원 및 다운로드 사이트에 대한 빠른 링크가 포함된 핫픽스 릴리스 노트는 [Cisco Firepower 핫픽스 릴리스 노트](#)를 참조하십시오.



참고 FMC 웹 인터페이스에 FMC의 현재 버전과 다른 버전의 BIOS 업데이트 핫픽스가 표시될 수 있습니다(예: 핫픽스 EC 버전 6.8.0). 이는 정상적인 동작이므로, 핫픽스를 적용해도 문제가 없습니다.

### BIOS 및 펌웨어 버전 확인

FMC에서 현재 버전을 확인하려면 Linux 셸/전문가 모드에서 다음 명령을 실행합니다.

- BIOS: `sudo dmidecode -t bios -q`
- RAID 컨트롤러 펌웨어(FMC 4500): `sudo MegaCLI -AdpAllInfo -aALL | grep "FW Package"`
- RAID 컨트롤러 펌웨어(기타 모든 모델): `sudo storcli /c0 show | grep "FW Package"`



# Firepower 디바이스

## Firepower 1000/2100 Series FTD

Firepower 1000 및 Firepower 2100 Series 디바이스는 FXOS 운영 체제를 사용합니다. Firepower Threat Defense을 업그레이드하면 FXOS도 자동으로 업그레이드됩니다.

이러한 디바이스는 FTD 대신 ASA를 실행할 수도 있습니다. 자세한 내용은 [Cisco ASA 호환성](#)를 참고하십시오.

표 31: Firepower 1000/2100 Series 호환성

Firepower 버전	Firepower 2110 Firepower 2120 Firepower 2130 Firepower 2140	Firepower 1010 Firepower 1120 Firepower 1140	Firepower 1150
6.7.x	예	예	예
6.6.x	예	예	예
6.5.0	예	예	예
6.4.0	예	예	—
6.3.0	예	—	—
6.2.3	예	—	—
6.2.2	예	—	—
6.2.1	예	—	—

## FMC를 사용하는 Firepower 4100/9300

Firepower 4100/9300 새시에서는 아래에 굵게 표시된 주요 Firepower 버전에 대해 특별히 검증되고 권장된 컴패니언 FXOS 버전이 있습니다. 이런 조합에 대해서는 향상된 테스트를 수행하므로 가능한 경우라면 언제든지 사용하십시오.

이러한 디바이스는 FTD 대신 ASA를 실행할 수도 있습니다. ASA 9.12 이상 및 FTD 6.4.0 이상을 사용하면 동일한 Firepower 9300 새시의 별도 모듈에서 ASA와 FTD를 모두 실행할 수 있습니다. 자세한 내용은 [Cisco Firepower 4100/9300 FXOS 호환성](#)을 참조하십시오.

문제를 해결하려면 FXOS를 최신 빌드로 업그레이드해야 할 수 있습니다. 결정에 도움이 필요하다면 [Cisco Firepower 4100/9300 FXOS 릴리스 노트](#)를 참조하십시오.



참고 다음 주요 버전 시퀀스에서 흐름 오프로드를 수행하려면 Firepower 및 FXOS의 특정 조합을 실행해야 합니다.

- 버전 6.2.2.x: FXOS 2.3.1.130 이상에서 버전 6.2.2.2 이상
- 버전 6.2.0.x: FXOS 2.2.1.x 또는 FXOS 2.2.2 빌드 17-86에서 버전 6.2.0.3 이상

표 32: Firepower 4100/9300 호환성

Firepower 버전	FXOS 버전	Firepower 9300		Firepower 4100 Series			
		SM-26 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
6.7.x	2.9.1.131 이상	예	예	예	예	예	예
6.6.x	2.8.1.105 이상 2.9.1.131 이상	예	예	예	예	예	예
6.5.0	2.7.1.92 이상 2.8.1.105 이상 2.9.1.131 이상	예	예	예	예	—	예
6.4.0	2.6.1.157 이상 2.7.1.92 이상 2.8.1.105 이상 2.9.1.131 이상	예	예	예	예	—	예
6.3.0	2.4.1.214 이상 2.6.1.157 이상 2.7.1.92 이상 2.8.1.105 이상 2.9.1.131 이상	예	—	예	예	—	—

Firepower 버전	FXOS 버전	Firepower 9300		Firepower 4100 Series			
		SM-26 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
6.2.3	<b>2.3.1.73</b> 이상 2.4.1.214 이상 2.6.1.157 이상 2.7.1.92 이상 2.8.1.105 이상 참고 Firepower 6.2.3.16 이상에 는 FXOS 2.3.1.157 이상이 필요합 니다.	예	—	예	예	—	—
6.2.2	<b>2.2.2.x</b> 2.3.1.73 이상 2.4.1.214 이상 2.6.1.157 이상 2.7.1.92 이상	예	—	예	예	—	—
6.2.1	—	—	—	—	—	—	—
6.2.0	<b>2.1.1.x, 2.2.1.x, 2.2.2.x</b> 2.3.1.73 이상 2.4.1.214 이상 2.6.1.157 이상	예	—	예	예	—	—
6.1.0	<b>2.0.1.x</b> 2.1.1.x 2.3.1.73 이상	예	—	예	예	—	—
6.0.1	<b>1.1.4.x</b> 2.0.1.x	예	—	예	—	—	—

## FTD을 사용하는 ASA 5500-X Series 및 ISA 3000

ASA 5500-X Series 및 ISA 3000 디바이스는 ASA 운영 체제를 사용합니다. Firepower Threat Defense을 업그레이드하면 ASA도 자동으로 업그레이드됩니다.

표 33: ASA 5500-X Series 및 ISA 3000 호환성

Firepower 버전	ASA 5508-X ASA 5516-X	ISA 3000	ASA 5525-X ASA 5545-X ASA 5555-X	ASA 5515-X	ASA 5506-X ASA 5506H-X ASA 5506W-X ASA 5512-X
6.7.x	예	예	—	—	—
6.6.x	예	예	예	—	—
6.5.0	예	예	예	—	—
6.4.0	예	예	예	예	—
6.3.0	예	예	예	예	—
6.2.3	예	예	예	예	예
6.2.2	예	—	예	예	예
6.2.1	—	—	—	—	—
6.2.0	예	—	예	예	예
6.1.0	예	—	예	예	예
6.0.1	예	—	예	예	예

## Firepower Threat Defense Virtual

이 테이블에는 FTDv에 대한 Firepower 호환성 및 가상 호스팅 환경 요구 사항이 나와 있습니다.

표 34: FTDv 호환성: VMware

Firepower 버전	VMware vSphere/VMware ESXi				
	6.7	6.5	6.0	5.5	5.1
6.7.x	예	예	예	—	—
6.6.x	예	예	예	—	—
6.5.0	예	예	예	—	—

Firepower 버전	VMware vSphere/VMware ESXi				
	6.7	6.5	6.0	5.5	5.1
6.4.0	—	예	예	—	—
6.3.0	—	예	예	—	—
6.2.3	—	예	예	예	—
6.2.2	—	—	예	예	—
6.2.1	—	—	—	—	—
6.2.0	—	—	예	예	—
6.1.0	—	—	예	예	—
6.0.1	—	—	—	예	예

표 35: FTDv 호환성: 기타 하이퍼바이저

Firepower 버전	AWS(Amazon Web Services)	Microsoft Azure	OCI(Oracle Cloud Infrastructure)	GCP(Google Cloud Platform)	KVM(Kernel-Based Virtual Machine)
6.7.x	예	예	예	예	예
6.6.x	예	예	—	—	예
6.5.0	예	예	—	—	예
6.4.0	예	예	—	—	예
6.3.0	예	예	—	—	예
6.2.3	예	예	—	—	예
6.2.2	예	예	—	—	예
6.2.1	—	—	—	—	—
6.2.0	예	예	—	—	예
6.1.0	예	—	—	—	예
6.0.1	예	—	—	—	—

## Firepower 7000/8000 Series 및 레거시 디바이스

이 테이블에는 7000/8000 Series 디바이스, AMP 모델 및 레거시 디바이스 플랫폼과 Firepower의 호환성이 나열되어 있습니다.

표 36: Firepower 7000/8000 Series 호환성

Firepower 버전	7000/8000 Series (AMP 포함)	시리즈 2 (레거시)	Cisco NGIPS for Blue Coat X-Series(레거시)
6.4.0	예	—	—
6.3.0	예	—	—
6.2.3	예	—	—
6.2.2	예	—	—
6.2.1	—	—	—
6.2.0	예	—	—
6.1.0	예	—	—
6.0.0	예	—	—
5.4.0	예	예	5.4.0 및 5.4.0.2~5.4.0.5 한정 XOS 9.7.2.x 또는 10.x 가 필요합니다.

## ASA 5500-X Series 및 ISA 3000 with FirePOWER Services

ASA FirePOWER 모듈은 별도로 업그레이드된 ASA 운영 체제에서 실행됩니다. ASA 및 ASA FirePOWER 버전은 광범위하게 호환됩니다. 하지만 ASA 업그레이드가 필요하지 않더라도 문제를 해결하려면 지원되는 최신 버전으로 업그레이드해야 할 수 있습니다.



참고 ASA 9.14(x)/ASDM 7.14(x)/FirePOWER 6.6은 ASA 5525-X, 5545-X 및 5555-X의 최종 버전입니다.

ASA 9.12(x)/ASDM 7.12(x)/FirePOWER 6.4는 ASA 5515-X 및 5585-X의 최종 버전입니다.

달리 명시되지 않는 한 ASDM 버전은 이전의 모든 ASA 버전과 호환됩니다. 예를 들어, ASDM 7.13(1)은 ASA 9.10(1)에서 ASA 5516-X를 관리할 수 있습니다. ASDM 7.13(1) 및 ASDM 7.14(1)은 ASA 5512-X, 5515-X, 5585-X 및 ASASM을 지원하지 않았습니다. ASDM 지원을 복구하려면 ASDM 7.13(1.101) 또는 7.14(1.48)로 업그레이드해야 합니다.

이 테이블에는 ASA 디바이스 모델, ASA OS 버전 및 ASDM과의 ASA FirePOWER 호환성이 나와 있습니다. FMC를 사용하여 ASA FirePOWER를 관리하는 경우, ASDM 요구 사항을 무시해도 됩니다. Firepower 종속 포털 기능을 사용하려면 ASA 9.5(2)의 ASA FirePOWER 버전 6.0.0 이상이 필요합니다.

표 37: ASA 및 ASA FirePOWER 호환성

ASA FirePOWER 버전	ASDM 버전(로컬 관리용)	ASA 버전	ASA 모델						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X(SSP 참고는 아래 참조)	ISA 3000
6.7.x	ASDM 7.15(1)	ASA 9.15(x) ASA 9.14(x) ASA 9.13(x) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3)	—	예	—	—	—	—	예
6.6.x	ASDM 7.14(1)	ASA 9.15(x)(5525-X, 5545-X, 5555-X 제외) ASA 9.14(x) ASA 9.13(x) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3)	—	예	—	—	예	—	예

ASA FirePOWER 버전	ASDM 버전(로컬 관리용)	ASA 버전	ASA 모델						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X(SSP 참고는 아래 참조)	ISA 3000
6.5.0	ASDM 7.13(1)	ASA 9.15(x)(5525-X, 5545-X, 5555-X 제외) ASA 9.14(x) ASA 9.13(x) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3)	—	예	—	—	예	—	예
6.4.0	ASDM 7.12(1)	ASA 9.15(x)(5515-X, 5525-X, 5545-X, 5555-X, 5585-X 제외) ASA 9.14(x)(5515-X, 5585-X 제외) ASA 9.13(x)(5515-X, 5585-X 제외) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3)	—	예	—	예	예	예	예



ASA FirePOWER 버전	ASDM 버전(로컬 관리용)	ASA 버전	ASA 모델						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X(SSP 참고는 아래 참조)	ISA 3000
6.3.0	ASDM 7.10(1)	ASA 9.15(x)(5515-X, 5525-X, 5545-X, 5555-X, 5585-X 제외) ASA 9.14(x)(5515-X, 5585-X 제외) ASA 9.13(x)(5515-X, 5585-X 제외) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3)	—	예	—	예	예	예	예

ASA FirePOWER 버전	ASDM 버전(로컬 관리용)	ASA 버전	ASA 모델						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X(SSP 참고는 아래 참조)	ISA 3000
6.2.3	ASDM 7.9(2)	ASA 9.15(x)(5506-X, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X 제외) ASA 9.14(x)(5506-X, 5512-X, 5515-X, 5585-X 제외) ASA 9.13(x)(5506-X, 5512-X, 5515-X, 5585-X 제외) ASA 9.12(x)(5506-X, 5512-X 제외) ASA 9.10(x)(5506-X, 5512-X 제외) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3)(5506-X 제외)	예	예	예	예	예	예	—

ASA FirePOWER 버전	ASDM 버전(로컬 관리용)	ASA 버전	ASA 모델						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X(SSP 참고는 아래 참조)	ISA 3000
6.2.2	ASDM 7.8(2)	ASA 9.15(x)(5506-X, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X 제외) ASA 9.14(x)(5506-X, 5512-X, 5515-X, 5585-X 제외) ASA 9.13(x)(5506-X, 5512-X, 5515-X, 5585-X 제외) ASA 9.12(x)(5506-X, 5512-X 제외) ASA 9.10(x)(5506-X, 5512-X 제외) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3)(5506-X 제외)	예	예	예	예	예	예	—

ASA FirePOWER 버전	ASDM 버전(로컬 관리용)	ASA 버전	ASA 모델						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X(SSP 참고는 아래 참조)	ISA 3000
6.2.0	ASDM 7.7(1)	ASA 9.15(x)(5506-X, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X 제외) ASA 9.14(x)(5506-X, 5512-X, 5515-X, 5585-X 제외) ASA 9.13(x)(5506-X, 5512-X, 5515-X, 5585-X 제외) ASA 9.12(x)(5506-X, 5512-X 제외) ASA 9.10(x)(5506-X, 5512-X 제외) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3)(5506-X 제외)	예	예	예	예	예	예	—

ASA FirePOWER 버전	ASDM 버전(로컬 관리용)	ASA 버전	ASA 모델						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X(SSP 참고는 아래 참조)	ISA 3000
6.1.0	ASDM 7.6(2)	ASA 9.15(x)(5506-X, 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, 5585-X 제외) ASA 9.14(x)(5506-X, 5512-X, 5515-X, 5585-X 제외) ASA 9.13(x)(5506-X, 5512-X, 5515-X, 5585-X 제외) ASA 9.12(x)(5506-X, 5512-X 제외) ASA 9.10(x)(5506-X, 5512-X 제외) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3)(5506-X 제외)	예	예	예	예	예	예	—
6.0.1	ASDM 7.6(1)(ASDM에서 ASA 9.4(x) 지원 없음, FMC만 해당)	ASA 9.6(x) ASA 9.5(1.5), 9.5(2), 9.5(3) ASA 9.4(x) CSCuv91730으로 인해 9.4(2) 이상으로 업그레이드하는 것이 좋습니다.	예	예	예	예	예	예	—

ASA FirePOWER 버전	ASDM 버전(로컬 관리용)	ASA 버전	ASA 모델						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X(SSP 참고는 아래 참조)	ISA 3000
6.0.0	ASDM 7.5(1.112)(ASDM에서 ASA 9.4(x) 지원 없음, FMC만 해당)	ASA 9.6(x) ASA 9.5(1.5), 9.5(2), 9.5(3) ASA 9.4(x) <a href="#">CSCuv91730</a> 으로 인해 9.4(2) 이상으로 업그레이드하는 것이 좋습니다.	예	예	예	예	예	예	—

ASA FirePOWER 버전	ASDM 버전(로컬 관리용)	ASA 버전	ASA 모델						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X(SSP 참고는 아래 참조)	ISA 3000
5.4.1.7 이상	ASDM 7.5(1.112)(ASDM에서 ASA 9.4(x) 지원 없음, FMC만 해당)	ASA 9.15(x)(5525-X, 5545-X, 5555-X 제외) ASA 9.14(x)(5506-X 제외) ASA 9.13(x)(5506-X 제외) ASA 9.12(x)(5506-X 제외) ASA 9.10(x)(5506-X 제외) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3) ASA 9.4(x) ASA 9.4(1.225)(ISA 3000만 해당) ASA 9.3(2), 9.3(3)(5508-X 또는 5516-X 제외) CSCuv91730으로 인해 9.3(3.8) 또는 9.4(2) 이상으로 업그레이드하는 것이 좋습니다.	예	예	—	—	—	—	예

ASA FirePOWER 버전	ASDM 버전(로컬 관리용)	ASA 버전	ASA 모델						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X(SSP 참고는 아래 참조)	ISA 3000
5.4.1	ASDM 7.3(3)	ASA 9.15(x)(5506-X 제외) ASA 9.14(x)(5506-X 제외) ASA 9.13(x)(5506-X 제외) ASA 9.12(x)(5506-X 제외) ASA 9.10(x)(5506-X 제외) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(1.5), 9.5(2), 9.5(3) ASA 9.4(x) ASA 9.3(2), 9.3(3)(5506-X만 해당) CSCuv91730으로 인해 9.3(3.8) 또는 9.4(2) 이상으로 업그레이드하는 것이 좋습니다.	예	예	—	—	—	—	—



ASA FirePOWER 버전	ASDM 버전(로컬 관리용)	ASA 버전	ASA 모델						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X(SSP 참고는 아래 참조)	ISA 3000
5.4.0.2 이상	—	ASA 9.14(x)(5512-X, 5515-X, 5585-X 제외) ASA 9.13(x)(5512-X, 5515-X, 5585-X 제외) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(1.5), 9.5(2), 9.5(3) ASA 9.4(x) ASA 9.3(2), 9.3(3) CSCuv91730으로 인해 9.3(3.8) 또는 9.4(2) 이상으로 업그레이드하는 것이 좋습니다.	—	—	예	예	예	예	—
5.4.0.1	—	ASA 9.2(2.4), 9.2(3), 9.2(4) CSCuv91730으로 인해 9.2(4.5) 이상으로 업그레이드하는 것이 좋습니다.	—	—	예	예	예	예	—
5.3.1	—	ASA 9.2(2.4), 9.2(3), 9.2(4) CSCuv91730으로 인해 9.2(4.5) 이상으로 업그레이드하는 것이 좋습니다.	—	—	예	예	예	예	—

**ASA 5585-X SSP 호환성**

동일한 레벨 SSP

ASA FirePOWER SSP -10, -20, -40 및 -60

요구 사항 : 슬롯 1에 설치, 슬롯 0에 일치 레벨 ASA SSP 포함

혼합 레벨 SSP

다음 조합에 대한 지원은 버전 5.4.0.1부터 시작됩니다.

- ASA SSP-10/ASA FirePOWER SSP-40
- ASA SSP-20/ASA FirePOWER SSP-60
- ASA SSP-40/ASA FirePOWER SSP-60

요구 사항: 슬롯 0에 ASA SSP, 슬롯 1에 ASA FirePOWER SSP



참고 SSP40/60 조합의 경우, 이 조합이 지원되지 않는다는 오류 메시지가 표시될 수 있습니다. 이 메시지는 무시해도 됩니다.

**NGIPSv**

이 표에는 NGIPSv(VMware에서 실행되는 가상 NGIPS 장치)에 대한 Firepower 호환성 및 가상 호스팅 환경 요구 사항이 나열되어 있습니다.

표 38: NGIPSv 호환성

Firepower 버전	VMware vSphere/VMware ESXi						VMware vCloud Director
	6.7	6.5	6.0	5.5	5.1	5.0	5.1
6.7.x	예	예	예	—	—	—	—
6.6.x	예	예	예	—	—	—	—
6.5.0	예	예	예	—	—	—	—
6.4.0	—	예	예	—	—	—	—
6.3.0	—	예	예	—	—	—	—
6.2.3	—	예	예	예	—	—	—
6.2.2	—	—	예	예	—	—	—
6.2.1	—	—	—	—	—	—	—

Firepower 버전	VMware vSphere/VMware ESXi						VMware vCloud Director
	6.7	6.5	6.0	5.5	5.1	5.0	5.1
6.2.0	—	—	예	예	—	—	—
6.1.0	—	—	예	예	—	—	—
6.0.1	—	—	—	예	예	—	—
6.0.0	—	—	—	예	예	—	—
5.4.0	—	—	—	예	예	예	예





# 13 장

## 버전별 **Firepower** 소프트웨어 업그레이드 지침

편의상 업그레이드 설명서에는 [Cisco Firepower 릴리스 노트](#)와 동일한 버전별 업그레이드 지침이 나와 있습니다.

버전을 건너뛰어 업그레이드하는 경우, 중간 릴리스 지침을 적용할 수 있습니다. 이 장의 체크리스트는 적용 가능한 모든 지침을 파악하는 데 도움이 됩니다. 상호 참조/링크를 따라가면 해당 지침을 확인할 수 있습니다. 이 장에서 업그레이드 지침은 처음 적용되는 버전 아래에 표시됩니다.



**중요** 이 지침 목록은 릴리스 노트를 대체하지 않습니다. 추가 중요 및 버전별 정보는 릴리스 노트에서 확인해야 합니다. 예를 들어, 최신 기능 및 지원이 중단된 기능은 업그레이드 전이나 후에 구성을 변경하거나 업그레이드까지 차단할 수 있습니다. 혹은 알려진 문제(버그)가 업그레이드에 영향을 미칠 수 있습니다.

- 버전 6.7.0 지침, 154 페이지
- 버전 6.6.0 가이드라인, 155 페이지
- 버전 6.5.0 지침, 158 페이지
- 버전 6.4.0 가이드라인, 166 페이지
- 버전 6.3.0 지침, 169 페이지
- 버전 6.2.3 지침, 177 페이지
- 버전 6.2.2 지침, 179 페이지
- 버전 6.2.0 지침, 181 페이지
- 버전 6.1.0 지침, 184 페이지
- 버전 6.0.0 지침, 185 페이지
- 버전별 패치 지침, 187 페이지
- 날짜 기반 지침, 192 페이지

## 버전 6.7.0 지침

이 체크리스트에는 버전 6.7.0에만 적용되거나 새롭게 추가된 업그레이드 지침이 포함되어 있습니다. 현재 버전 6.3.0~6.6.x를 실행 중인 경우, 다음 지침을 검토하십시오.

표 39: 버전 6.7.0 최신 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	Firepower 1010 스위치 포트에서 유효하지 않은 VLAN ID로 업그레이드 실패, 154 페이지	Firepower 1010	6.4.0~6.6.x	6.7.0 이상

이 체크리스트에는 중간 릴리스에 적용되는 업그레이드 지침이 포함되어 있습니다. 현재 버전 6.3.0~6.5.0을 실행 중인 경우, 다음 지침을 검토하십시오.

표 40: 버전 6.7.0 이전에 게시된 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	FMCv 업그레이드에 28GB RAM 필요, 156 페이지	FMCv	6.2.3~6.5.0.x	6.6.0 이상
	FMC 업그레이드 후 일시적으로 사용할 수 없는 이벤트, 157 페이지	FMC	6.2.3~6.5.0.x	6.6.0 이상
	Firepower 1000 Series 디바이스에서 업그레이드 후 전원 껐다 다시 켜기 필요, 159 페이지	Firepower 1000 Series	6.4.0.x	6.5.0 이상
	새 URL 카테고리 및 평판, 160 페이지	Any(모든)	6.2.3~6.4.0.x	6.5.0 이상
	TLS 암호화 가속 활성화/비활성화 불가, 169 페이지	Firepower 2100 Series Firepower 4100/9300	6.2.3~6.3.0.x	6.4.0 이상

## Firepower 1010 스위치 포트에서 유효하지 않은 VLAN ID로 업그레이드 실패

구축: Firepower 1010

업그레이드 시작 버전: 버전 6.4.0~6.6.x

직접 업그레이드: 버전 6.7.0 이상

Firepower 1010의 경우, 3968~4047 범위의 VLAN ID로 스위치 포트를 설정했다면 버전 6.7.0 이상으로의 FTD 업그레이드가 실패합니다. 이러한 ID는 내부 전용으로 사용됩니다.

## 버전 6.6.0 가이드라인

이 체크리스트에는 버전 6.6.0에만 적용되거나 새롭게 추가된 업그레이드 지침이 포함되어 있습니다. 현재 버전 6.2.3~6.5.0을 실행 중인 경우, 다음 지침을 검토하십시오.

표 41: 버전 6.6.0 새 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	<a href="#">FMCv 업그레이드에 28GB RAM 필요, 156 페이지</a>	FMCv	6.2.3~6.5.0.x	6.6.0 이상
	<a href="#">FMC 업그레이드 후 일시적으로 사용할 수 없는 이벤트, 157 페이지</a>	FMC	6.2.3~6.5.0.x	6.6.0 이상

이 체크리스트에는 중간 릴리스에 적용되는 업그레이드 지침이 포함되어 있습니다. 현재 버전 6.2.3~6.4.0을 실행 중인 경우, 다음 지침을 검토하십시오.

표 42: 버전 6.6.0 이전에 게시된 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	<a href="#">Firepower 1000 Series 디바이스에서 업그레이드 후 전원 껐다 다시 켜기 필요, 159 페이지</a>	Firepower 1000 Series	6.4.0.x	6.5.0 이상
	<a href="#">새 URL 카테고리 및 평판, 160 페이지</a>	Any(모든)	6.2.3~6.4.0.x	6.5.0 이상
	<a href="#">TLS 암호화 가속 활성화/비활성화 불가, 169 페이지</a>	Firepower 2100 Series Firepower 4100/9300	6.2.3~6.3.0.x	6.4.0 이상
	<a href="#">FMC, 7000/8000 Series, NGIPSv에서 준비도 확인이 실패할 수 있음, 173 페이지</a>	FMC NGIPSv	6.1.0~6.1.0.6 6.2.0~6.2.0.6 6.2.1 6.2.2~6.2.2.4 6.2.3~6.2.3.4	6.3.0 이상
	<a href="#">RA VPN 기본 설정 변경이 VPN 트래픽을 차단할 수 있음, 173 페이지</a>	FMC를 사용하는 FTD	6.2.0~6.2.3.x	6.3.0 이상
	<a href="#">보안 인텔리전스가 애플리케이션 식별 활성화, 174 페이지</a>	FMC 구축	6.1.0~6.2.3.x	6.3.0 이상

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	업그레이드 후 CIP 탐지를 활성화하기 위해 VDB 업데이트, 175 페이지	Any(모든)	6.1.0~6.2.3.x	6.3.0 이상
	유효하지 않은 침입 변수 집합으로 구축 오류가 발생할 수 있음, 175 페이지	Any(모든)	6.1.0~6.2.3.x	6.3.0 이상

## FMCv 업그레이드에 28GB RAM 필요

구축: FMCv

업그레이드 대상: 버전 6.2.3~6.5.0.x

직접 업그레이드: 버전 6.6.0 이상

이제 모든 FMCv 구현에 동일한 RAM 요구 사항이 적용됩니다. 32GB 권장, 28GB 필수 (FMCv 300의 경우 64GB) 가상 어플라이언스에 28GB 미만을 할당하면 버전 6.6.0 이상으로의 업그레이드가 실패합니다. 업그레이드 후에는 메모리 할당량을 줄이면 상태 모니터에 경고가 표시됩니다.

이러한 새로운 메모리 요구 사항은 모든 가상 환경에서 균일한 요구 사항을 적용하고 성능을 개선하며 새로운 기능을 활용할 수 있도록 합니다. 기본 설정을 사용하는 것이 좋습니다. 그러나 성능을 개선하려는 경우 가용 리소스에 따라 가상 어플라이언스의 메모리와 CPU 수를 늘릴 수 있습니다. FMCv 메모리 요구 사항에 대한 자세한 내용은 [Cisco Firepower Management Center Virtual 시작 가이드](#)를 참조하십시오.



**참고** 버전 6.6.0 릴리스부터는 클라우드 기반 FMCv 구축(AWS, Azure)의 메모리 부족 인스턴스 유형이 완전히 사용되지 않습니다. 이전 Firepower 버전에서도 해당 인스턴스를 사용하여 새 FMCv 인스턴스를 생성할 수 없습니다. 기존 인스턴스는 계속 실행할 수 있습니다.

이 테이블에는 메모리 부족 FMCv 구축의 업그레이드 전 요구 사항이 간략히 나와 있습니다.

표 43: 버전 6.6.0 이상 업그레이드를 위한 FMCv 메모리 요구 사항

Platform(플랫폼)	사전 업그레이드 작업	세부정보
VMWare	최소 28GB/32GB를 할당하는 것이 좋습니다.	먼저 가상 머신의 전원을 끕니다. 자세한 내용은 VMware 문서를 참조하십시오.
KVM	최소 28GB / 32GB를 할당하는 것이 좋습니다.	자세한 내용은 KVM 환경 설명서를 참조하십시오.



Platform(플랫폼)	사전 업그레이드 작업	세부정보
AWS	<p>인스턴스 크기 조정:</p> <ul style="list-style-type: none"> <li>• c3.xlarge에서 c3.4xlarge로</li> <li>• c3.2.xlarge에서 c3.4xlarge로</li> <li>• c4.xlarge에서 c4.4xlarge로</li> <li>• c4.2xlarge에서 c4.4xlarge로</li> </ul> <p>또한 신규 구축을 위한 c5.4xlarge 인스턴스도 제공합니다.</p>	<p>크기를 조정하기 전에 인스턴스를 중지합니다. 이 작업을 수행하면 인스턴스 저장 볼륨의 데이터가 손실되므로 인스턴스 저장기반 인스턴스를 먼저 마이그레이션하십시오. 또한 관리 인터페이스에 탄력적 IP 주소가 없는 경우, 해당 공용 IP 주소가 사용됩니다.</p> <p>자세한 내용은 Linux 인스턴스용 AWS 사용 설명서의 인스턴스 유형 변경에 대한 문서를 참조하십시오.</p>
Azure	<p>인스턴스 크기 조정:</p> <ul style="list-style-type: none"> <li>• Standard_D3_v2 에서 Standard_D4_v2 로</li> </ul>	<p>Azure 포털 또는 PowerShell을 사용합니다. 크기를 조정하기 전에 인스턴스를 중지할 필요는 없지만, 중지하면 추가적인 크기가 표시될 수 있습니다. 크기를 조정하면 실행 중인 가상 머신이 재시작됩니다.</p> <p>Windows VM 크기 조정에 대한 Azure 설명서에서 지침을 참조하십시오.</p>

## FMC 업그레이드 후 일시적으로 사용할 수 없는 이벤트

구축: FMC

업그레이드 대상: 버전 6.2.3~6.5.0.x

직접 업그레이드: 버전 6.6.0 이상

버전 6.6.0에서는 연결 및 보안 인텔리전스 이벤트에 새 데이터 저장소를 사용합니다.

업그레이드가 완료되고 FMC가 재부팅되면 기록 연결 및 보안 인텔리전스 이벤트가 백그라운드에서 마이그레이션되고 리소스가 제한됩니다. FMC 모델, 시스템 로드 및 저장한 이벤트 수에 따라 몇 시간에서 최대 하루가 걸릴 수 있습니다.

기록 이벤트는 최신 이벤트부터 기간별로 마이그레이션됩니다. 마이그레이션되지 않은 이벤트는 쿼리 결과 또는 대시보드에 나타나지 않습니다. 예를 들어, 업그레이드 이후 이벤트로 인해 마이그레이션이 완료되기 전에 연결 이벤트 데이터베이스 제한에 도달하면 가장 오래된 기록 이벤트는 마이그레이션되지 않습니다.



**팁** 메뉴 모음에서 시스템 상태 아이콘을 클릭하여 Message Center에서 이벤트 마이그레이션 진행 상황을 모니터링하십시오.

## 버전 6.5.0 지침

이 체크리스트에는 버전 6.5.0에만 적용되거나 새롭게 추가된 업그레이드 지침이 포함되어 있습니다. 현재 버전 6.2.3~6.4.0을 실행 중인 경우, 다음 지침을 검토하십시오.

표 44: 버전 6.5.0 새 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	Firepower 1000 Series 디바이스에서 업그레이드 후 전원 켜다 다시 켜기 필요, 159 페이지	Firepower 1000 Series	6.4.0.x	6.5.0 이상
	버전 6.5.0에 대한 이그레스 최적화 비활성화, 159 페이지	FTD	6.2.3~6.4.0.x	6.5.0 한정
	새 URL 카테고리 및 평판, 160 페이지	Any(모든)	6.2.3~6.4.0.x	6.5.0 이상

이 체크리스트에는 중간 릴리스에 적용되는 업그레이드 지침이 포함되어 있습니다. 현재 버전 6.2.3 또는 6.3.0을 실행 중인 경우, 다음 지침을 검토하십시오.

표 45: 버전 6.5.0 이전에 게시된 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	업데이트 실패: 컨테이너 인스턴스의 디스크 공간 부족, 168 페이지	Firepower 4100/9300	6.3.0~6.4.0.x	6.3.0.1~6.5.0
	TLS 암호화 가속 활성화/비활성화 불가, 169 페이지	Firepower 2100 Series Firepower 4100/9300	6.2.3~6.3.0.x	6.4.0 이상
	FMC, 7000/8000 Series, NGIPSv에서 준비도 확인이 실패할 수 있음, 173 페이지	FMC Firepower 7000/8000 시리즈 NGIPSv	6.1.0~6.1.0.6 6.2.0~6.2.0.6 6.2.1 6.2.2~6.2.2.4 6.2.3~6.2.3.4	6.3.0 이상
	RA VPN 기본 설정 변경이 VPN 트래픽을 차단할 수 있음, 173 페이지	FMC를 사용하는 FTD	6.2.0~6.2.3.x	6.3.0 이상
	보안 인텔리전스가 애플리케이션 식별 활성화, 174 페이지	FMC 구축	6.1.0~6.2.3.x	6.3.0 이상

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	업그레이드 후 CIP 탐지를 활성화하기 위해 VDB 업데이트, 175 페이지	Any(모든)	6.1.0~6.2.3.x	6.3.0 이상
	유효하지 않은 침입 변수 집합으로 구축 오류가 발생할 수 있음, 175 페이지	Any(모든)	6.1.0~6.2.3.x	6.3.0 이상

## Firepower 1000 Series 디바이스에서 업그레이드 후 전원 껐다 다시 켜기 필요

구축: Firepower 1000 series

업그레이드 대상: 버전 6.4.0.x

직접 업그레이드: 버전 6.5.0 이상

버전 6.5.0에서 Firepower 1000/2100 및 Firepower 4100/9300 Series 디바이스에 FXOS CLI '보안 기반 초기화' 사용이 가능합니다.

Firepower 1000 Series 디바이스에서 이 기능이 제대로 작동하려면 버전 6.5.0 이상으로 업그레이드한 후 디바이스의 전원을 껐다가 다시 켜야 합니다. 자동 재부팅으로는 충분하지 않습니다. 다른 지원되는 디바이스에서는 전원 껐다 다시 켜기가 필요하지 않습니다.

## 버전 6.5.0에 대한 이그레스 최적화 비활성화

구축: FTD

업그레이드 대상: 버전 6.2.3~6.4.0.x

직접 업그레이드: 버전 6.5.0 한정

[CSCVq34340](#)을 완화하기 위해 FTD 디바이스를 버전 6.4.0.7 이상 또는 버전 6.5.0.2 이상으로 패치하면 이그레스 최적화 처리가 해제됩니다. 이는 이그레스 최적화 기능의 활성화 여부에 관계없이 이루어집니다.

버전 6.5.0으로 업그레이드:

- 버전 6.2.3.x부터: 이그레스 최적화를 활성화하고 켭니다.
- 버전 6.3.0.x부터: 이그레스 최적화를 활성화하고 켭니다.
- 버전 6.4.0.x부터: 현재 설정을 따릅니다. 그러나 버전 6.4.0.x 패치에서 이그레스 최적화를 해제했는데도 기능이 계속 활성화되어 있는 경우, 버전 6.5.0으로 업그레이드하면 다시 설정됩니다.



참고 버전 6.5.0.2 이상으로 패치하거나 버전 6.6.0으로 업그레이드하는 것이 좋습니다. 버전 6.5.0 또는 6.5.0.1을 계속 사용하는 경우, FTD CLI: **no asp inspect-dp egress-optimization**에서 이그레스 최적화를 수동으로 비활성화해야 합니다.

이 문제는 이그레스 최적화가 정상적으로 작동하는 버전 6.6.0에서 해결되었습니다. 자세한 내용은 소프트웨어 권고: [이그레스 최적화 기능으로 발생하는 9344 블록 크기 고갈로 인한 FTD 트래픽 중단](#)을 참조하십시오.

## 새 URL 카테고리 및 평판

구축: 모두

업그레이드 대상: 버전 6.2.3~6.4.0.x

직접 업그레이드: 버전 6.5.0 이상

Cisco Talos Intelligence Group(Talos)에서는 URL을 분류하고 필터링하기 위해 새로운 카테고리 와 이름이 변경된 평판을 도입했습니다. 카테고리 변경에 대한 자세한 목록은 [Cisco Firepower 릴리스 노트, 버전 6.5.0](#)을 참조하십시오. 새 URL 카테고리에 대한 설명은 [Talos Intelligence 카테고리](#) 사이트를 참조하십시오.

분류되지 않고 평판 없는 URL 개념은 새로운 것이지만, 규칙 구성 옵션은 동일합니다.

- 분류되지 않은 URL의 평판은 의심스러움, 보통, 양호, 신뢰가 있습니다.

분류되지 않은 URL을 필터링할 수 있지만 평판에 따라 추가 제한할 수 없습니다. 이러한 규칙은 평판에 관계없이 분류되지 않은 모든 URL을 매칭합니다.

카테고리가 없는 신뢰할 수 없는 규칙 등은 존재하지 않습니다. 그렇지 않으면 신뢰할 수 없는 평판의 분류되지 않은 URL은 자동으로 새 악성 사이트 위협 카테고리로 할당됩니다.

- 평판이 없는 URL은 모든 카테고리에 속할 수 있습니다.

평판이 없는 URL은 필터링할 수 없습니다. 규칙 편집기에서는 '평판 없음'에 대한 옵션이 없습니다. 그러나 평판이 없는 URL을 포함하는 모든 평판을 가진 URL을 필터링할 수 있습니다. 이러한 URL은 카테고리별로 제한할 수도 있습니다. 모든/모든 규칙에 해당하는 유틸리티는 없습니다.

다음 표는 업그레이드 변경 사항을 요약해 나타냅니다. 영향을 최소화할 수 있도록 설계되었으며 대부분의 고객은 업그레이드 후 구축을 차단하지 않지만, 이 릴리스 노트 및 현재 URL 필터링 구성을 검토할 것을 강력하게 권장합니다. 신중한 계획 및 준비는 실수를 방지하며 업그레이드 사후 문제 해결에 소요되는 시간을 줄이는 데 도움이 될 수 있습니다.


표 46: 업그레이드 시 구축 변경 사항

변경	세부 사항
URL 규칙 카테고리를 수정합니다.	업그레이드로 URL 규칙이 수정되어 다음 정책에서 새 카테고리 설정과 가장 가까운 설정을 사용합니다. <ul style="list-style-type: none"> <li>• 액세스 제어</li> <li>• SSL</li> <li>• QoS(FMC만)</li> <li>• 상관 관계(FMC만)</li> </ul> <p>이러한 변경으로 중복 또는 선점 규칙이 생성되어 성능이 저하될 수 있습니다. 구성에 병합된 카테고리가 포함된 경우 허용 또는 차단된 URL에 약간의 변경이 발생할 수 있습니다.</p>
URL 규칙 평판 이름이 변경됩니다.	업그레이드로 URL 규칙이 수정되어 새 평판 이름을 사용합니다. <ol style="list-style-type: none"> <li>1. 신뢰할 수 없음(이전 높은 위험)</li> <li>2. 의심스러운(이전 의심스러운 사이트)</li> <li>3. 보통(이전 보안 위험이 있는 일반 사이트)</li> <li>4. 양호(이전 일반 사이트)</li> <li>5. 신뢰(이전 알려진)</li> </ol>
URL 캐시가 삭제됩니다.	업그레이드로 과거에 시스템이 클라우드에서 검색한 결과를 포함한 URL 캐시가 삭제됩니다. 사용자가 로컬 데이터 집합에 없는 URL에 액세스하는 시간이 일시적으로 더 오래 걸릴 수 있습니다.
'레거시' 이벤트에 레이블을 지정합니다.	이미 기록된 이벤트의 경우 업그레이드 후 관련 URL 카테고리 및 평판 정보에 레거시라는 레이블을 지정합니다. 이 레거시 이벤트는 시간이 지나면 데이터베이스에서 삭제됩니다.

## URL 카테고리 및 평판을 위한 사전 업그레이드 작업

업그레이드하기 전에 다음 작업을 수행합니다.

표 47: 사전 업그레이드 작업

작업	세부 사항
<p>어플라이언스가 Talos 리소스에 연결할 수 있는지 확인합니다.</p>	<p>시스템 업그레이드 후 다음 Cisco 리소스와 통신할 수 있어야 합니다.</p> <ul style="list-style-type: none"> <li>• <a href="https://regsvc.sco.cisco.com/">https://regsvc.sco.cisco.com/</a> — 등록</li> <li>• <a href="https://est.sco.cisco.com/">https://est.sco.cisco.com/</a> — 보안 통신 인증서 획득</li> <li>• <a href="https://updates-talos.sco.cisco.com/">https://updates-talos.sco.cisco.com/</a> — 클라이언트/서버 매니페스트 획득</li> <li>• <a href="http://updates.ironport.com/">http://updates.ironport.com/</a> — 데이터베이스 다운로드(참고: 포트 80 사용)</li> <li>• <a href="https://v3.sds.cisco.com/">https://v3.sds.cisco.com/</a> — 클라우드 쿼리</li> </ul> <p>클라우드 쿼리 서비스는 다음 IP 주소 블록을 사용합니다.</p> <ul style="list-style-type: none"> <li>• IPv4 클라우드 쿼리: <ul style="list-style-type: none"> <li>• 146.112.62.0/24</li> <li>• 146.112.63.0/24</li> <li>• 146.112.255.0/24</li> <li>• 146.112.59.0/24</li> </ul> </li> <li>• IPv6 클라우드 쿼리: <ul style="list-style-type: none"> <li>• 2a04: e4c7: ffff::/48</li> <li>• 2a04: e4c7: fffe::/48</li> </ul> </li> </ul>
<p>잠재적인 규칙 문제를 식별합니다.</p>	<p>예정된 변경 사항을 이해합니다. 현재 URL 필터링 구성을 검사하고 업그레이드 후 작업을 수행해야 하는지 결정합니다(다음 섹션 참조).</p> <p>참고 이제 사용되지 않는 카테고리를 사용하는 URL 규칙을 수정할 수 있습니다. 그렇지 않으면 이를 사용하는 규칙은 업그레이드 후 배포를 방지합니다.</p> <p>FMC 배포에서는 액세스 제어 규칙 및 SSL과 같은 하위 정책의 규칙을 포함하여 정책의 현재 저장된 구성에 대한 세부 정보를 제공하는 액세스 제어 정책 보고서를 생성하는 것이 좋습니다. 각 URL 규칙에 대해 현재 카테고리, 평판 및 관련 규칙 작업을 볼 수 있습니다. FMC에서 <b>Policies(정책) &gt; Access Control(액세스 제어)</b> 을 선택하고 적절한 정책 옆의 보고서 아이콘()을 클릭합니다.</p>

## URL 카테고리 및 평판에 대한 업그레이드 후 작업

업그레이드 후 URL 필터링 구성을 다시 검토하고 가능한 한 빨리 다음 작업을 수행해야 합니다. 구축 유형 및 업그레이드로 인한 변경 사항에 따라 전부는 아니지만 일부 문제가 GUI에 표시될 수 있습니다. 예를 들어 FMC/FDM의 액세스 제어 정책에서는 **Show Warning**(경고 표시)(FMC) 또는 **Show Problem Rules**(문제 규칙 표시)(FDM)을 클릭합니다.

표 48: 업그레이드 후 작업

작업	세부 사항
규칙에서 지원되지 않는 카테고리를 제거합니다. 필수.	업그레이드는 지원이 중단된 카테고리를 사용하는 URL 규칙을 수정하지 않습니다. 이를 사용하는 규칙은 배포되지 않습니다. FMC에서는 이러한 규칙이 표시됩니다.
새 카테고리를 포함하도록 규칙을 만들거나 수정합니다.	대부분의 새 카테고리는 위협을 식별합니다. 사용을 강력하게 권장합니다. FMC에서 이러한 새 카테고리는 이 업그레이드 이후에는 표시되지 않지만, Talos에서 이후에 추가 카테고리를 추가할 수 있습니다. 이 경우 새 카테고리가 표시됩니다.
병합된 카테고리의 결과로 변경된 규칙을 평가합니다.	영향을 받는 카테고리가 하나라도 포함된 각 규칙은 이제 영향을 받는 모든 카테고리를 포함합니다. 원래 카테고리가 서로 다른 평판에 연결되었다면 새 규칙은 더 광범위하고 포괄적인 평판에 연결됩니다. 이전과 같이 URL을 필터링하려면 일부 구성을 수정하거나 삭제해야 합니다. 자세한 내용은 <a href="#">병합된 URL 카테고리가 있는 규칙 지침, 164 페이지</a> 를 참조하십시오. 변경된 내용 및 플랫폼이 규칙 경고를 처리하는 방법에 따라 변경 내용이 표시될 수 있습니다. 예를 들어 FMC는 완전히 중복되고 선점된 규칙을 표시하지만, 부분 중복된 규칙은 표시하지 않습니다.
분할된 카테고리의 결과로 변경된 규칙을 평가합니다.	업그레이드는 URL 규칙의 이전 및 단일 카테고리 각각을 이전 카테고리로 매핑하는 모든 새 카테고리로 교체합니다. 이렇게 하면 URL을 필터링하는 방식은 변경되지 않지만, 새 세분화를 사용할 수 있도록 영향을 받는 규칙을 수정할 수 있습니다. 이러한 변경 내용은 표시되지 않습니다.
이름이 변경되었거나 변경되지 않은 카테고리를 파악합니다.	아무 작업도 필요하지 않지만 변경 사항에 대해 알고 있어야 합니다. 이러한 변경 내용은 표시되지 않습니다.

작업	세부 사항
분류되지 않고 평판이 없는 URL을 처리하는 방법을 평가합니다.	이제 분류되지 않고 평판이 없는 URL을 사용할 수 있지만 평판별로 분류되지 않은 URL을 필터링하거나 평판이 없는 URL을 필터링할 수 없습니다.  분류되지 않은 카테고리 또는 모든 평판에 따라 필터링되는 규칙이 예상대로 작동하는지 확인합니다.

## 병합된 URL 카테고리가 있는 규칙 지침

업그레이드 전 URL 필터링 구성을 검사할 때 다음 중 사용자에게 적용되는 시나리오 및 지침을 확인하십시오. 이렇게 하면 업그레이드 후 구성을 예상대로 할 수 있으며, 문제를 해결하기 위해 빠른 조치를 취할 수 있습니다.

표 49: 병합된 URL 카테고리가 있는 규칙 지침

지침	세부 사항
규칙 순서는 트래픽과 일치하는 규칙을 결정합니다.	동일한 카테고리를 포함하는 규칙을 고려할 때 트래픽은 조건을 포함하는 목록의 첫 번째 규칙을 매칭합니다.
동일한 규칙의 카테고리 vs 다른 규칙의 카테고리	<p>단일 규칙에서 카테고리 병합은 규칙 내 단일 카테고리로 병합됩니다. 예를 들어 카테고리 A와 카테고리 B가 카테고리 AB로 병합되면, 카테고리 A와 B에 하나의 규칙이 존재하며, 규칙을 병합하면 단일 카테고리 AB가 됩니다.</p> <p>서로 다른 규칙의 카테고리를 병합하면 병합 후 각 규칙에 동일한 카테고리가 있는 별도의 규칙이 생성됩니다. 예를 들어 카테고리 A와 카테고리 B가 카테고리 AB로 병합되고, 카테고리 A에 규칙 1이, 카테고리 B에 규칙 2가 있는 경우, 규칙 1, 2를 병합한 후에는 각각이 카테고리 AB에 포함됩니다. 이 상황을 해결하는 방법은 규칙 순서, 규칙과 관련된 작업 및 평판 수준, 규칙을 포함한 다른 URL 카테고리, 규칙에 포함된 비 URL 조건에 따라 달라집니다.</p>
관련 작업	서로 다른 규칙의 병합된 카테고리가 다른 작업과 연관된 경우 병합 후 동일한 카테고리의 다른 작업에 대해 두 개 이상의 규칙이 있을 수 있습니다.
관련 평판 수준	단일 규칙이 병합 전 다른 평판 수준과 관련된 카테고리를 포함한다면, 병합된 카테고리는 더 포괄적인 평판 수준과 관련됩니다. 예를 들어 카테고리 A가 모든 평판이 있는 특정 규칙과 관련되고, 카테고리 B가 평판 레벨 3- 보안 위험이 있는 일반 사이트이 있는 동일한 조건과 관련되었다면, 규칙의 카테고리 AB를 병합한 후에는 모든 평판과 관련됩니다.



지침	세부 사항
중복 및 중복 카테고리 및 규칙	<p>병합 후 다른 규칙은 다른 작업 및 평판 수준에 연관된 동일한 카테고리를 포함할 수 있습니다.</p> <p>중복 규칙은 정확히 일치하지는 않지만, 규칙 순서가 더 빠른 규칙이 대신 매칭되지 않는 경우 트래픽을 매칭할 수 없을 수 있습니다. 예를 들어 병합 전 모든 평판에 적용되는 카테고리 A가 있는 규칙 1과 평판 1-3에만 적용되는 카테고리 B가 있는 규칙 2를 병합하면, 병합 후 규칙 1, 2에 카테고리 AB가 포함되지만, 규칙 1의 규칙 순서가 높지 않으면 규칙 2는 절대 매칭되지 않습니다.</p> <p>FMC에서는 동일한 카테고리 및 평판이 있는 규칙에 경고가 표시됩니다. 그러나 이러한 경고는 평판이 다른 동일한 카테고리를 포함한 규칙을 표시하지는 않습니다.</p> <p>주의: 중복 또는 중복 카테고리 해결 방법을 결정할 때는 규칙의 모든 조건을 고려합니다.</p>
규칙의 기타 URL 카테고리	<p>병합된 URL이 있는 규칙은 다른 URL 카테고리도 포함할 수 있습니다. 따라서 병합 후 특정 카테고리가 중복되는 경우 해당 규칙을 삭제하는 대신 수정할 수 있습니다.</p>
규칙의 비 URL 조건	<p>병합된 URL 카테고리가 있는 규칙은 애플리케이션 조건 같은 다른 규칙 조건을 포함할 수 있습니다. 따라서 병합 후 특정 카테고리가 중복되는 경우 해당 규칙을 삭제하는 대신 수정할 수 있습니다.</p>

다음 테이블의 예에서는 카테고리 A와 카테고리 B가 카테고리 AB로 병합된 경우를 사용합니다. 두 개의 규칙 예제에서 규칙 1이 규칙 2에 선행합니다.

표 50: 병합된 URL 카테고리가 있는 규칙 예

시나리오	업그레이드 전	업그레이드 후
동일한 규칙의 병합된 카테고리	규칙 1에는 카테고리 A와 B가 있습니다.	규칙 1에는 카테고리 AB가 있습니다.
서로 다른 규칙의 병합된 카테고리	<p>규칙 1에는 카테고리 A가 있습니다.</p> <p>규칙 2에는 카테고리 B가 있습니다.</p>	<p>규칙 1에는 카테고리 AB가 있습니다.</p> <p>규칙 2에는 카테고리 AB가 있습니다.</p> <p>구체적인 결과는 목록의 규칙 순서, 평판 수준 및 관련 작업에 따라 다릅니다. 중복을 해결하는 방법을 결정할 때 규칙의 다른 모든 조건을 고려해야 합니다.</p>

시나리오	업그레이드 전	업그레이드 후
다른 동작이 있는 다른 규칙의 병합된 카테고리 (평판은 동일합니다)	규칙 1에는 허용으로 설정된 카테고리 A가 있습니다. 규칙 2에는 차단으로 설정된 카테고리 B가 있습니다. (평판은 동일합니다)	규칙 1에는 허용으로 설정된 카테고리 AB가 있습니다. 규칙 2에는 차단으로 설정된 카테고리 AB가 있습니다. 규칙 1은 이 카테고리의 모든 트래픽과 일치합니다. 규칙 2는 트래픽과 일치하지 않으며 병합 후 카테고리 및 평판이 동일하기 때문에 병합 후 경고가 표시되면 경고 표시등이 표시됩니다.
다른 평판 수준이 있는 동일한 규칙의 병합된 카테고리	규칙 1에는 다음이 포함됩니다. 모든 평판과 관련된 카테고리 A 평판 1~3과 관련된 카테고리 B	규칙 1에는 평판이 있는 카테고리 AB가 포함됩니다.
다른 평판 수준이 있는 다른 규칙의 병합된 카테고리	규칙 1에는 모든 평판과 관련된 카테고리 A가 포함됩니다. 규칙 2에는 평판 1~3과 관련된 카테고리 B가 포함됩니다.	규칙 1에는 평판이 있는 카테고리 AB가 포함됩니다. 규칙 2에는 평판 1~3과 관련된 카테고리 AB가 포함됩니다. 규칙 1은 이 카테고리의 모든 트래픽과 일치합니다. 규칙 2는 트래픽을 절대 매칭하지 않지만, 평판이 동일하지 않기 때문에 경고 표시등이 표시되지 않습니다.

## 버전 6.4.0 가이드라인

이 체크리스트에는 버전 6.4.0에만 적용되거나 새롭게 추가된 업그레이드 지침이 포함되어 있습니다. 현재 버전 6.1.0~6.3.0을 실행 중인 경우, 다음 지침을 검토하십시오.

표 51: 버전 6.4.0 새 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	<a href="#">Firepower 1010 디바이스의 EtherChannel은 이그레스 트래픽 블랙홀이 가능합니다.</a> , 168 페이지	Firepower 1010	6.4.0	6.4.0.3~6.4.0.5
	<a href="#">업데이트 실패: 컨테이너 인스턴스의 디스크 공간 부족</a> , 168 페이지	Firepower 4100/9300	6.3.0~6.4.0.x	6.3.0.1~6.5.0

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	업그레이드 실패: 이전 버전이 6.2.3.12 인 NGIPS 디바이스, 168 페이지	Firepower 7000/8000 시리즈 ASA FirePOWER NGIPSv	6.2.3~6.3.0.x	6.4.0 한정
	TLS 암호화 가속 활성화/비활성화 불가, 169 페이지	Firepower 2100 Series  Firepower 4100/9300	6.1.0~6.3.0.x	6.4.0 이상

이 체크리스트에는 중간 릴리스에 적용되는 업그레이드 지침이 포함되어 있습니다. 현재 버전 6.1.0~6.2.3을 실행 중인 경우, 다음 지침을 검토하십시오.

표 52: 버전 6.4.0 이전에 게시된 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	FMC, 7000/8000 Series, NGIPSv에서 준비도 확인이 실패할 수 있음, 173 페이지	FMC Firepower 7000/8000 시리즈 NGIPSv	6.1.0~6.1.0.6 6.2.0~6.2.0.6 6.2.1 6.2.2~6.2.2.4 6.2.3~6.2.3.4	6.3.0 이상
	RA VPN 기본 설정 변경이 VPN 트래픽을 차단할 수 있음, 173 페이지	FMC를 사용하는 FTD	6.2.0~6.2.3.x	6.3.0 이상
	보안 인텔리전스가 애플리케이션 식별 활성화, 174 페이지	FMC 구축	6.1.0~6.2.3.x	6.3.0 이상
	업그레이드 후 CIP 탐지를 활성화하기 위해 VDB 업데이트, 175 페이지	Any(모든)	6.1.0~6.2.3.x	6.3.0 이상
	유효하지 않은 침입 변수 집합으로 구축 오류가 발생할 수 있음, 175 페이지	Any(모든)	6.1.0~6.2.3.x	6.3.0 이상
	보고서의 결과 제한 변경, 178 페이지	FMC	6.1.0~6.2.2.x	6.2.3~6.4.0
	업그레이드 전 FTD 클러스터에서 버전 6.1.x에서 사이트 ID 제거, 179 페이지	FTD 클러스터	6.1.0.x	6.2.3~6.4.0
	액세스 제어는 SRU에서 지연 기반 성능 설정을 가져올 수 있습니다., 181 페이지	FMC	6.1.0.x	6.2.0~6.4.0

Firepower 1010 디바이스의 EtherChannel은 이그레스 트래픽 블랙홀이 가능합니다.

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	'Snort Fail Open'이 FTD의 'Failsafe'를 대체합니다. , 182 페이지	FMC를 사용하는 FTD	6.1.0.x	6.2.0~6.4.0

## Firepower 1010 디바이스의 EtherChannel은 이그레스 트래픽 블랙홀이 가능합니다.

구축: FTD를 사용하는 Firepower 1010

영향을 받는 버전: 버전 6.4.0~6.4.0.5

관련 버그: [CSCvq81354](#)

FTD 버전 6.4.0~6.4.0.5를 실행하는 Firepower 1010 디바이스에서 EtherChannel을 구성하지 않는 것을 강력하게 권장합니다. (이 모델에서는 버전 6.4.0.1 및 6.4.0.2를 지원하지 않습니다.)

내부 트래픽 해시 문제로 Firepower 1010 디바이스의 일부 EtherChannel은 이그레스 트래픽을 블랙홀할 수 있습니다. 해시는 소스/대상 IP 주소를 기반으로 하므로 지정된 소스/대상 IP 쌍과 동작이 동일합니다. 즉 일부 트래픽은 둘 다에서 작동하며, 일부 트래픽은 둘 다에서 실패합니다.

이 문제는 버전 6.4.0.6 및 버전 6.5.0에서 해결되었습니다.

## 업데이트 실패: 컨테이너 인스턴스의 디스크 공간 부족

구축: FTD를 사용하는 Firepower 4100/9300

업그레이드 대상: 버전 6.3.0~6.4.0.x

직접 업그레이드: 버전 6.3.0.1~버전 6.5.0

컨테이너 인스턴스로 구성된 FTD 디바이스가 사전 확인 단계에서 디스크 공간 부족 경고를 표시하며 실패할 수 있습니다. 주요 업그레이드 중 가장 자주 발생하며 패치 중에도 발생할 수 있습니다.

이 오류가 발생하면 더 많은 디스크 공간을 확보하십시오. 그래도 해결되지 않는 경우 Cisco TAC에 문의하십시오.

## 업그레이드 실패: 이전 버전이 6.2.3.12인 NGIPS 디바이스

구축: 7000/8000 series, ASA FirePOWER, NGIPSv

관련 버그: [CSCvp42398](#)

업그레이드 대상: 버전 6.2.3~6.3.0.x

직접 업그레이드: 버전 6.4.0만

다음과 같은 경우 NGIPS 장치를 버전 6.4.0으로 업그레이드할 수 없습니다.

- 이전에 이 장치에서 실행되던 버전이 6.2.3.12입니다.

- 버전 6.2.3.12 패치를 제거하거나 버전 6.3.0.x로 업그레이드했습니다.

여기에는 버전 6.2.3.12 패치를 제거한 다음 버전 6.3.0.x로 업그레이드된 시나리오도 포함됩니다.

현재 상황이 이러한 경우 Cisco TAC에 문의하십시오.

## TLS 암호화 가속 활성화/비활성화 불가

구축: Firepower 2100 Series, Firepower 4100/9300 새시

업그레이드 대상: 버전 6.1.0~6.3.x

직접 업그레이드: 버전 6.4.0 이상

SSL 하드웨어 가속은 TLS 암호화 가속으로 이름이 변경되었습니다.

디바이스에 따라 TLS 암호화 가속은 소프트웨어나 하드웨어에서 실행됩니다. 업그레이드하면 이전에 이 기능을 수동으로 비활성화한 경우에도 모든 대상 디바이스에서 자동으로 가속화가 활성화됩니다. 대부분의 경우 이 기능을 구성할 수 없습니다. 이 기능은 자동으로 활성화되면 사용자가 비활성화할 수 없습니다.

버전 6.4.0으로 업그레이드: Firepower 4100/9300 새시의 다중 인스턴스 기능을 사용한다면 FXOS CLI를 사용해 모듈/보안 엔진당 하나의 컨테이너 인스턴스에 대해 TLS 암호화 가속화를 활성화할 수 있습니다. 다른 컨테이너 인스턴스에서는 가속화가 비활성화되지만 기본 인스턴스에서는 활성화됩니다.

버전 6.5.0 이상으로 업그레이드: Firepower 4100/9300 새시의 다중 인스턴스 기능을 사용하는 경우 FXOS CLI를 사용하여 Firepower 4100/9300 새시의 여러 컨테이너 인스턴스(최대 16개)에 TLS 암호화 가속을 활성화할 수 있습니다. 새 인스턴스에는 기본적으로 이 기능이 활성화되어 있습니다. 그러나 업그레이드는 기존 인스턴스에서 가속화를 활성화하지 않습니다. 대신 `config hwCrypto enable` CLI 명령을 사용합니다.

## 버전 6.3.0 지침

이 체크리스트에는 버전 6.3.0에만 적용되거나 새롭게 추가된 업그레이드 지침이 포함되어 있습니다. 현재 버전 6.1.0~6.2.3을 실행 중인 경우, 다음 지침을 검토하십시오.

표 53: 버전 6.3.0 새 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	업그레이드 및 설치 패키지 이름 변경됨, 171 페이지	FMC Firepower 7000/8000 시리즈 NGIPSv	Any(모든)	6.3.0 이상

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	버전 6.3 이상으로 이미지를 재설치하면 대부분의 어플라이언스에서 LOM 비활성화, 172 페이지	FMC(물리적) Firepower 7000/8000 시리즈	Any(모든)	6.3.0 이상
	FMC, 7000/8000 Series, NGIPsv에서 준비도 확인이 실패할 수 있음, 173 페이지	FMC Firepower 7000/8000 시리즈 NGIPsv	6.2.3~6.2.3.4 6.2.2~6.2.2.4 6.2.1 6.2.0~6.2.0.6 6.1.0~6.1.0.6	6.3.0 이상
	RA VPN 기본 설정 변경이 VPN 트래픽을 차단할 수 있음, 173 페이지	FMC를 사용하는 FTD	6.2.0~6.2.3.x	6.3.0 이상
	업그레이드 시 TLS/SSL 하드웨어 가속 활성화, 174 페이지	Firepower 2100 Series Firepower 4100/9300	6.1.0~6.2.3.x	6.3.0 한정
	업그레이드 실패: 버전 6.3.0-83에서 FMC 및 ASA FirePOWER으로 업그레이드, 174 페이지	FMC ASDM을 사용하는 ASA FirePOWER	6.1.0~6.2.3.x	6.3.0 한정
	보안 인텔리전스가 애플리케이션 식별 활성화, 174 페이지	FMC 구축	6.1.0~6.2.3.x	6.3.0 이상
	업그레이드 후 CIP 탐지를 활성화하기 위해 VDB 업데이트, 175 페이지	Any(모든)	6.1.0~6.2.3.x	6.3.0 이상
	유효하지 않은 침입 변수 집합으로 구축 오류가 발생할 수 있음, 175 페이지	Any(모든)	6.1.0~6.2.3.x	6.3.0 이상
	Firepower 4100/9300에서 FXOS 업그레이드 전 FTD 푸시 필요, 176 페이지	Firepower 4100/9300	6.1.0.x	6.3.0 한정

이 체크리스트에는 중간 릴리스에 적용되는 업그레이드 지침이 포함되어 있습니다. 현재 버전 6.1.0~6.2.2를 실행 중인 경우, 다음 지침을 검토하십시오.

표 54: 버전 6.3.0 이전에 게시된 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	보고서의 결과 제한 변경, 178 페이지	FMC	6.1.0~6.2.2.x	6.2.3~6.4.0

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	업그레이드 전 FTD 클러스터에서 버전 6.1.x에서 사이트 ID 제거, 179 페이지	FTD 클러스터	6.1.0.x	6.2.3~6.4.0
	액세스 제어는 SRU에서 지연 기반 성능 설정을 가져올 수 있습니다., 181 페이지	FMC	6.1.0.x	6.2.0~6.4.0
	'Snort Fail Open'이 FTD의 'Failsafe'를 대체합니다., 182 페이지	FMC를 사용하는 FTD	6.1.0.x	6.2.0~6.4.0

## 업그레이드 및 설치 패키지 이름 변경됨

구축: FMC, 7000/8000 series, NGIPSv

업그레이드 대상: 버전 6.1.0~6.2.3.x

직접 업그레이드: 버전 6.3 이상

일부 플랫폼에서는 버전 6.3.0부터 업그레이드, 패치, 핫픽스 및 설치 패키지용 명명 체계(즉 이름의 앞부분)이 변경되었습니다.



참고

이 변경으로 기존 물리적 어플라이언스인 DC750, 1500, 2000, 3500 및 4000과 7000/8000 Series 디바이스 및 AMP 모델의 이미지 재설치에 오류가 발생합니다. 현재 버전 5.x를 실행하고 있고 해당 어플라이언스 중 하나에 버전 6.3.0 또는 6.4.0을 새롭게 설치해야 하는 경우 설치 패키지를 Cisco 지원 및 다운로드 사이트에서 다운로드한 후 "기존" 이름으로 변경합니다. 이러한 어플라이언스는 버전 6.5 이상으로 이미지 재설치할 수 없습니다.

표 55: 명명 체계: 업그레이드, 패치 및 핫픽스 패키지

플랫폼	명명 체계
FMC	신규: Cisco_Firepower_Mgmt_Center 기존: Sourcefire_3D_Defense_Center_S3
Firepower 7000/8000 시리즈	신규: Cisco_Firepower_NGIPS_Appliance 기존: Sourcefire_3D_Device_S3
NGIPSv	신규: Cisco_Firepower_NGIPS_Virtual 기존: Sourcefire_3D_Device_VMware 기존: Sourcefire_3D_Device_Virtual64_VMware

표 56: 명명 체계; 설치 패키지

플랫폼	명명 체계
FMC (물리적)	신규: Cisco_Firepower_Mgmt_Center 기존: Sourcefire_Defense_Center_M4 기존: Sourcefire_Defense_Center_S3
FMCv: VMware	신규: Cisco_Firepower_Mgmt_Center_Virtual_VMware 기존: Cisco_Firepower_Management_Center_Virtual_VMware
FMCv: KVM	신규: Cisco_Firepower_Mgmt_Center_Virtual_KVM 기존: Cisco_Firepower_Management_Center_Virtual
Firepower 7000/8000 시리즈	신규: Cisco_Firepower_NGIPS_Appliance 기존: Sourcefire_3D_Device_S3
NGIPsv	신규: Cisco_Firepower_NGIPsv_VMware 기존: Cisco_Firepower_NGIPS_VMware

## 버전 6.3 이상으로 이미지를 재설치하면 대부분의 어플라이언스에서 LOM 비활성화

구축: 물리적 FMC, 7000/8000 Series 디바이스

재이미지 대상: 버전 6.0 이상

직접 업그레이드: 버전 6.3 이상

최근 설치된 버전 6.3 이상에서는 보안상의 이유로 이제 자동으로 대부분의 어플라이언스에서 LOM(Lights-Out Management) 설정을 삭제합니다. 일부 구형 FMC 모델에서는 관리 네트워크 설정과 함께 LOM 설정을 유지하는 옵션이 있습니다.

버전 6.3 이상으로 이미지 재설치 중 네트워크 설정을 삭제하는 경우 초기 구성을 수행하기 위해 반드시 어플라이언스에 물리적으로 액세스할 수 있는지 확인해야 합니다. LOM을 사용할 수 없습니다. 초기 구성을 수행한 후 LOM 및 LOM 사용자를 다시 활성화할 수 있습니다.

표 57: LOM 설정에 영향을 주는 이미지 재설치

플랫폼	버전 6.2.3 또는 이전으로 이미지 재설치	버전 6.3 이상으로 이미지 재설치
MC1600, 2600, 4600 MC1000, 2500, 4500 MC2000, 4000	항상 유지	항상 삭제



플랫폼	버전 <b>6.2.3</b> 또는 이전으로 이미지 재설치	버전 <b>6.3</b> 이상으로 이미지 재설치
MC750, 1500, 3500	네트워크 설정을 삭제하면 삭제	네트워크 설정을 삭제하면 삭제
7000/8000 시리즈	항상 삭제	항상 삭제

## FMC, 7000/8000 Series, NGIPSv에서 준비도 확인이 실패할 수 있음

구축: FMC, 7000/8000 Series 디바이스, NGIPSv

업그레이드 대상: 버전 6.1.0~6.1.0.6, 버전 6.2.0~6.2.0.6, 버전 6.2.1, 버전 6.2.2~6.2.2.4, 버전 6.2.3~6.2.3.4

직접 업그레이드: 버전 6.3.0 이상

목록의 Firepower 버전 중 하나에서 업그레이드할 때 목록의 모델에 대한 준비도 확인을 실행할 수 없습니다. 이는 준비도 확인 프로세스가 새 업그레이드 패키지와 호환되지 않아 발생하는 문제입니다.

표 58: 버전 **6.3.0** 이상의 준비도 확인이 포함된 패치

준비도 확인 지원되지 않음	수정이 포함된 첫 번째 패치
6.1.0~6.1.0.6	6.1.0.7
6.2.0~6.2.0.6	6.2.0.7
6.2.1	없음 버전 6.2.3.5 이상으로 업그레이드
6.2.2~6.2.2.4	6.2.2.5
6.2.3~6.2.3.4	6.2.3.5

## RA VPN 기본 설정 변경이 VPN 트래픽을 차단할 수 있음

구축: Firepower Threat Defense Remote Access VPN용으로 구성

업그레이드 대상: 버전 6.2.x

직접 업그레이드: 버전 6.3 이상

버전 6.3은 숨겨진 옵션 **sysopt connection permit-vpn**의 기본 설정을 변경합니다. 업그레이드하면 Remote Access VPN이 트래픽 전달을 중지할 수 있습니다. 이 경우 다음 기법 중 하나를 사용합니다.

- **sysopt connection permit-vpn** 명령을 구성하는 FlexConfig 개체를 생성합니다. 이 명령의 새 기본 값은 **no sysopt connection permit-vpn**입니다.

이 방법은 외부 사용자가 원격 액세스 VPN 주소 풀에서 IP 주소를 스누핑할 수 없기 때문에 VPN에서 트래픽을 더 안전하게 허용할 수 있습니다. 하지만 VPN 트래픽이 검사되지 않는다는 단점이 있습니다. 즉, 침입 및 파일 보호, URL 필터링 또는 기타 고급 기능이 트래픽에 적용되지 않습니다.

- 원격 액세스 VPN 주소 풀에서 연결을 허용하는 액세스 제어 규칙을 생성합니다.

이 방법을 사용하는 경우 VPN 트래픽이 검사되며, 연결에 고급 서비스를 적용할 수 있습니다. 하지만 외부 사용자가 IP 주소를 스푸핑하여 내부 네트워크에 액세스할 가능성이 있다는 단점이 있습니다.

## 업그레이드 시 TLS/SSL 하드웨어 가속 활성화

구축: Firepower 2100 Series, Firepower 4100/9300 새시

업그레이드 대상: 버전 6.1.0~6.2.3.x

직접 업그레이드: 버전 6.3.0 한정

업그레이드 프로세스가 사용 가능한 디바이스에서 자동으로 TLS/SSL 하드웨어 가속(TLS 암호화 가속이라고도 함)을 활성화합니다. 버전 6.2.3에서 도입되었을 때 이 기능은 Firepower 4100/9300 새시에서 기본적으로 비활성화되었고, Firepower 2100 Series 디바이스에서 사용할 수 없었습니다.

트래픽을 암호 해독하지 않는 매니지드 디바이스에서 TLS/SSL 하드웨어 가속을 사용하면 성능에 영향을 줄 수 있습니다. 버전 6.3.0.x의 경우 트래픽의 암호 해독을 하지 않는 디바이스에서는 이 기능을 비활성화하는 것이 좋습니다.

비활성화하려면 다음 CLI 명령을 사용합니다.

시스템 지원 `SSL-HW-Offload` 비활성화

## 업그레이드 실패: 버전 6.3.0-83에서 FMC 및 ASA FirePOWER으로 업그레이드

구축: Firepower Management Center, ASA FirePOWER(로컬로 관리)

업그레이드 대상: 버전 6.1.0~6.2.3.x

직접 업그레이드: 버전 6.3.0-83

일부 Firepower Management Center 및 로컬(ASDM) 관리되는 ASA FirePOWER 모듈의 버전 6.3.0 빌드 83에서 업그레이드 오류가 발생했습니다. 이 문제는 버전 5.4.x에서 업그레이드한 고객의 하위 집합에 한정되었습니다. 자세한 내용은 Cisco Bug Search Tool에서 [CSCvn62123](#)를 참조하십시오.

이제 새 업그레이드 패키지를 사용할 수 있습니다. 버전 6.3.0-83 업그레이드 패키지를 다운로드한 경우 사용하지 마십시오. 이 문제로 인해 이미 업그레이드 오류가 발생한 경우 Cisco TAC에 문의하십시오.

## 보안 인텔리전스가 애플리케이션 식별 활성화

구축: Firepower Management Center

업그레이드 대상: 버전 6.1~6.2.3.x

직접 업그레이드: 버전 6.3 이상

버전 6.3에서 보안 인텔리전스 구성이 애플리케이션 탐지 및 식별을 활성화합니다. 현재 배포에서 검색을 비활성화하면 업그레이드 프로세스에서 이 기능을 다시 활성화할 수 있습니다. 필요하지 않을 경우 (IPS 전용 구축 등) 검색을 비활성화하면 성능을 향상시킬 수 있습니다.

검색을 사용하지 않도록 설정하려면 다음을 수행해야 합니다.

- 네트워크 검색 정책의 모든 규칙을 삭제합니다.
- 영역, IP 주소, VLAN 태그, 포트의 액세스 제어를 수행하는 단순한 네트워크 기반 조건만 사용합니다. 모든 유형의 애플리케이션, 사용자, URL 또는 지오로케이션 제어를 수행하지 마십시오.
- (신규) 기본 전역 목록을 포함해 액세스 제어 정책의 보안 인텔리전스 설정에서 모든 화이트리스트와 블랙리스트를 삭제하면 네트워크 및 URL 기반 보안 인텔리전스를 비활성화합니다.
- (신규) DNS 규칙에 대해 DNS 및 전역 블랙리스트에 대한 기본 전역 화이트리스트를 포함해 DNS 정책과 관련된 모든 규칙을 삭제 또는 비활성화하여 DNS 기반 보안 인텔리전스를 비활성화합니다.

## 업그레이드 후 CIP 탐지를 활성화하기 위해 VDB 업데이트

구축: 모두

업그레이드 대상: VDP 299 이상을 사용하는 버전 6.1.0~6.2.3.x

직접 업그레이드: 버전 6.3.0 이상

취약성 데이터베이스(VDB) 299 이상을 사용하는 동안 업그레이드하는 경우 업그레이드 프로세스 중 발생하는 오류로 인해 CIP 탐지 사후 업그레이드를 사용할 수 없습니다. 여기에는 2018년 6월부터 가장 최신 릴리스를 비롯해 현재까지 릴리스된 모든 VDB가 포함됩니다.

업그레이드 후 취약성 데이터베이스(VDB) 업데이트가 항상 권장되지만, 이 경우에는 특히 중요합니다.

이 문제에 영향을 받는지 확인하려면 CIP 기반 애플리케이션 조건을 사용하는 액세스 제어 규칙으로 구성을 시도합니다. 규칙 편집기에서 CIP 애플리케이션을 찾을 수 없는 경우 VDB를 수동으로 업데이트합니다.

## 유효하지 않은 침입 변수 집합으로 구축 오류가 발생할 수 있음

구축: 모두

업그레이드 대상: 버전 6.1~6.2.3.x

직접 업그레이드: 버전 6.3.0 이상

침입 변수 집합의 네트워크 변수의 경우 사용자가 제외하는 모든 IP 주소는 사용자가 포함한 IP 주소의 하위 집합이어야 합니다. 이 표는 유효한 구성 및 유효하지 않은 구성을 나타냅니다.

유효함	유효하지 않음
포함: 10.0.0.0/8 제외: 10.1.0.0/16	포함: 10.1.0.0/16 제외: 172.16.0.0/12 제외: 10.0.0.0/8

버전 6.3.0 이전에는 이런 유형의 유효하지 않은 구성이 있는 네트워크 변수도 문제 없이 저장할 수 있었습니다. 이제 이러한 구성을 구축하려고 하면 변수 집합에 유효하지 않은 제외된 값이 있습니다. 오류가 발생하며 차단됩니다.

이 경우 잘못 구성된 변수 집합을 식별해 편집하고 다시 구축합니다. 변수 집합에서 참조하는 네트워크 개체나 그룹을 편집해야 할 수 있습니다.

## Firepower 4100/9300에서 FXOS 업그레이드 전 FTD 푸시 필요

구축: FTD를 사용하는 Firepower 4100/9300

업그레이드 대상: FXOS 2.0.1, 2.1.1 또는 2.3.1의 버전 6.1.x

직접 업그레이드: FXOS 2.4.1의 버전 6.3.0

Firepower Management Center가 버전 6.2.3 이상을 실행 중인 경우 업그레이드하기 전 관리되는 디바이스에 Firepower 업그레이드 패키지를 푸시(복사)하도록 강력하게 권장합니다. 따라서 업그레이드 유지 보수 기간을 줄일 수 있습니다.

FTD를 사용하는 Firepower 4100/9300의 경우 모범 사례는 필수 컴패니언 FXOS 업그레이드를 시작하기 전 푸시하는 것입니다. 버전 6.1에서 버전 6.3으로 직접 업그레이드하는 경우 이 푸시가 필요합니다. FXOS를 업그레이드하기 전에 반드시 푸시해야 합니다.

이는 Firepower 6.1이 실행 중인 상태에서 FXOS를 버전 2.4.1로 업그레이드하면 디바이스 관리 포트가 플랩되어 디바이스와 FMC 간 간헐적인 통신 오류가 발생하기 때문입니다. 'sftunnel daemon exited' 경고가 표시될 수 있으며 대규모 업그레이드 패키지 푸시 등 지속적인 통신 관련 작업에 오류가 발생할 수 있습니다.

FTD를 사용하는 Firepower 4100/9300을 업그레이드하려면 항상 다음 순서를 따르십시오.

1. FMC를 대상 버전으로 업그레이드합니다.
2. Cisco 지원 및 다운로드 사이트에서 디바이스 업그레이드 패키지를 확보하여 FMC에 업로드합니다.
3. FMC를 사용하여 업그레이드 패키지를 디바이스로 푸시합니다.
4. 푸시가 완료되면 FXOS를 대상 버전으로 업그레이드합니다.
5. 이어서 FMC를 사용하여 디바이스의 Firepower 소프트웨어를 업그레이드합니다.

Firepower 소프트웨어 업그레이드가 완료될 때까지 관리 포트 플랩이 발생할 수 있습니다.

## 버전 6.2.3 지침

이 체크리스트에는 버전 6.2.3에만 적용되거나 새롭게 추가된 업그레이드 지침이 포함되어 있습니다. 현재 버전 6.1.0~6.2.2를 실행 중인 경우, 다음 지침을 검토하십시오.

표 59: 버전 6.2.3 새 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	<a href="#">Cisco와 데이터 공유, 177 페이지</a>	Any(모든)	Any(모든)	6.2.3 이상
	<a href="#">업그레이드 후 액세스 컨트롤 정책 수정/다시 저장, 178 페이지</a>	Any(모든)	6.1.0~6.2.2.x	6.2.3 한정
	<a href="#">보고서의 결과 제한 변경, 178 페이지</a>	FMC	6.1.0~6.2.2.x	6.2.3~6.4.0
	<a href="#">업그레이드 전 FTD 클러스터에서 버전 6.1.x에서 사이트 ID 제거, 179 페이지</a>	FTD 클러스터	6.1.0.x	6.2.3~6.4.0

이 체크리스트에는 중간 릴리스에 적용되는 업그레이드 지침이 포함되어 있습니다. 현재 버전 6.1~6.2.1을 실행 중인 경우, 다음 지침을 검토하십시오.

표 60: 버전 6.2.3 이전에 게시된 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	<a href="#">액세스 제어는 SRU에서 지연 기반 성능 설정을 가져올 수 있습니다., 181 페이지</a>	FMC	6.1.0.x	6.2.0~6.4.0
	<a href="#">'Snort Fail Open'이 FTD의 'Failsafe'를 대체합니다., 182 페이지</a>	FMC를 사용하는 FTD	6.1.0.x	6.2.0~6.4.0

## Cisco와 데이터 공유

구축: 모두

업그레이드 대상: 버전 6.1.0 이상

직접 업그레이드: 버전 6.2.3 이상

일부 기능은 Cisco와의 데이터 공유에 관련됩니다.

### Cisco Success Network

버전 6.2.3+에서 *Cisco Success Network*는 사용자에게 기술 지원을 제공하는 데 필요한 사용 정보와 통계를 Cisco로 전송합니다.

초기 설정 및 업그레이드 중에 참여를 수락할지 아니면 거절할지 묻는 메시지가 표시될 수 있습니다. 또한 언제든지 이러한 참여를 옵트인하거나 옵트아웃할 수도 있습니다.

#### 웹 분석 추적

버전 6.2.3 이상에서 웹 분석 추적은 비 개인 식별 가능 사용 데이터를 Cisco로 전송합니다. 이러한 데이터에는 페이지 상호 작용, 브라우저 버전, 제품 버전, 사용자 위치, FMC의 관리 IP 주소 또는 호스트네임 등이 포함되나 이에 국한되지 않습니다.

웹 분석 추적은 기본적으로 켜져 있으며(버전 6.5.0 이상 EULA에 동의하면 웹 분석 추적에 동의하게 됨) 초기 설정을 완료한 후 언제든지 옵트아웃할 수 있습니다.



**참고** 버전 6.2.3~6.6.x로 업그레이드하면 웹 분석 추적이 활성화되거나 재활성화될 수 있습니다. 이는 현재 설정이 옵트아웃인 경우에도 일어날 수 있습니다. Cisco에서 이 데이터를 수집하는 것을 원하지 않는 경우, 업그레이드 후 옵트아웃하십시오. 6.7.0 이상으로 업그레이드하면 현재 설정이 적용됩니다.

#### Cisco Support Diagnostics

버전 6.5.0 이상에서 Cisco 지원 진단(Cisco 사전 지원이라고도 함)은 구성 및 운영 상태 데이터를 Cisco에 전달하여 해당 데이터를 자동 문제 탐지 시스템에서 처리하여 문제가 발생하기 전에 사전에 안내할 수 있도록 합니다. 또한 이 기능은 Cisco TAC에서 TAC 케이스를 해결하는 동안 디바이스에서 필요한 정보를 수집하도록 합니다.

초기 설정 및 업그레이드 중에 참여를 수락할지 아니면 거절할지 묻는 메시지가 표시될 수 있습니다. 또한 언제든지 이러한 참여를 옵트인하거나 옵트아웃할 수도 있습니다.

## 업그레이드 후 액세스 컨트롤 정책 수정/다시 저장

구축: 모두

업그레이드 대상: 버전 6.1~6.2.2.x

직접 업그레이드: 버전 6.2.3 한정

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

구축: Firepower Management Center

업그레이드 대상: 버전 6.1.0~6.2.2.x

직접 업그레이드: 버전 6.2.3~6.4.0

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.

표 61: 보고서에 새 결과 제한

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 섹션이 HTML/CSV 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.

## 업그레이드 전 FTD 클러스터에서 버전 6.1.x에서 사이트 ID 제거

구축: Firepower Threat Defense 클러스터

업그레이드 대상: 버전 6.1.x

직접 업그레이드: 버전 6.2.3~6.4.0

Firepower Threat Defense 버전 6.1.x 클러스터는 사이트 간 클러스터링을 지원하지 않습니다(버전 6.2.0에서 시작하는 FlexConfig를 사용하여 사이트 간 기능을 구성할 수 있습니다).

FXOS 2.1.1에 버전 6.1.x 클러스터를 구축하거나 다시 구축하고 (지원되지 않는) 사이트 ID 값을 입력한 경우 업그레이드 전 FXOS의 각 유닛에 있는 사이트 ID를 삭제(0으로 설정)합니다. 그렇지 않으면 업그레이드 후 유닛이 클러스터에 다시 참여할 수 없습니다.

이미 업그레이드한 경우 각 유닛에서 사이트 ID를 제거한 다음 클러스터를 다시 설정합니다. 사이트 ID를 보거나 변경하려면 [Cisco FXOS CLI 설정 가이드](#)를 참조합니다.

## 버전 6.2.2 지침

이 체크리스트에는 버전 6.2.2에만 적용되거나 새롭게 추가된 업그레이드 지침이 포함되어 있습니다. 현재 버전 6.2.0~6.2.1을 실행 중인 경우, 다음 지침을 검토하십시오.

표 62: 버전 6.2.2 새 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	<a href="#">보안 강화: 서명된 업그레이드 패키지</a> , 180 페이지	Any(모든)	Any(모든)	6.2.2 이상
	<a href="#">8000 Series 보안 인증서 및 컴플라이언스는 버전 6.2.2.1 이상이 필요합니다.</a> , 180 페이지	Firepower 8000 Series	6.2.0.x	6.2.2 한정

## 보안 강화: 서명된 업그레이드 패키지

구축: 모두

업그레이드 대상: 버전 6.2.1 이상

직접 업그레이드: 버전 6.2.2 이상

Firepower가 올바른 파일을 사용하고 있는지 확인할 수 있도록 버전 6.2.1 이상이 대상인 업그레이드 패키지 (및 핫픽스)는 서명된 tar 아카이브 파일(.tar)을 사용합니다. 이전 버전 대상 업그레이드는 서명되지 않은 패키지를 계속 사용합니다.

주요 업그레이드 또는 에어 갭 구축과 같이 Cisco 지원 및 다운로드 사이트에서 수동으로 업그레이드 패키지를 다운로드할 때 올바른 패키지를 다운로드했는지 확인하십시오. 서명된(.tar) 패키지의 압축을 풀지 마십시오.



**참고** 서명된 업그레이드 패키지를 업로드하면 시스템이 패키지 파일을 확인하므로 GUI가 로드되는 데 몇 분 정도 걸릴 수 있습니다. 표시 속도를 높이기 위해 이후 필요하지 않은 패키지는 서명된 패키지를 제거합니다.

## 8000 Series 보안 인증서 및 컴플라이언스는 버전 6.2.2.1 이상이 필요합니다.

구축: Firepower 8000 Series 디바이스

업그레이드 대상: 버전 6.2.0.x

직접 업그레이드: 버전 6.2.2 한정

버전 6.2.2를 실행하는 8000 Series 디바이스에서 보안 인증 컴플라이언스(CC/UCAPL 모드)를 활성화 하면 FSIC(파일 시스템 무결성 검사) 오류가 발생할 수 있습니다. 디바이스를 버전 6.2.2.1 이상으로 업그레이드할 때까지 기다립니다.





주의 FSIC 오류가 발생하면 Firepower 소프트웨어가 시작하지 않고, 원격 SSH 액세스가 비활성화되며, 로컬 콘솔을 통해서만 어플라이언스에 액세스할 수 있습니다. 이러한 현상이 발생한다면 Cisco TAC에 문의하십시오.

## 버전 6.2.0 지침

이 체크리스트에는 버전 6.2.0에만 적용되거나 새롭게 추가된 업그레이드 지침이 포함되어 있습니다. 현재 버전 6.1.0을 실행 중인 경우, 다음 지침을 검토하십시오.

표 63: 버전 6.2.0 새 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	액세스 제어는 SRU에서 지연 기반 성능 설정을 가져올 수 있습니다., 181 페이지	FMC	6.1.0.x	6.2.0~6.4.0
	'Snort Fail Open'이 FTD의 'Failsafe'를 대체합니다., 182 페이지	FMC를 사용하는 FTD	6.1.0.x	6.2.0~6.4.0
	업그레이드 시 IAB '모든 애플리케이션' 옵션 삭제, 182 페이지	FMC ASDM을 사용하는 ASA FirePOWER	6.1.0.3 또는 이후 패치	6.2.0 한정
	업그레이드 시 비활성화된 메모리 부족 장치에 대한 URL 필터링 하위 사이트 조회, 183 페이지	Any(모든)	6.1.0.1 또는 이후 패치	6.2.0 한정

### 액세스 제어는 **SRU**에서 지연 기반 성능 설정을 가져올 수 있습니다.

구축: FMC

업그레이드 대상: 6.1.x

직접 업그레이드: 6.2.0 이상

버전 6.2.0 이상의 새 액세스 제어 정책은 기본적으로 최신 침입 규칙 업데이트(SRU)에서 지연 기반 성능 설정을 가져옵니다. 이 동작은 새 이전 설정 적용(**Apply Settings From**) 옵션에 의해 제어됩니다. 이 옵션을 구성하려면 액세스 제어 정책을 편집 또는 생성하고 고급을 클릭하여 지연 기반 성능 설정을 편집합니다.

버전 6.2.0 이상으로 업그레이드하면 현재 버전(6.1.x) 구성에 따라 새로운 옵션이 설정됩니다. 현재 설정이 다음과 같은 경우

'Snort Fail Open'이 FTD의 'Failsafe'를 대체합니다.

- 기본값: 새 옵션이 설치된 규칙 업데이트로 설정됩니다. 업그레이드 후 배포할 때 시스템은 가장 최근 SRU의 지연 기반 성능 설정을 사용합니다. 가장 최근 SRU가 지정한 내용에 따라 트래픽 처리가 변경될 수 있습니다.
- 사용자 지정: 새 옵션이 사용자 지정으로 설정됩니다. 시스템이 현재 성능 설정을 유지합니다 이 옵션은 동작을 변경하지 않습니다.

업그레이드 전 구성을 검토하는 것이 좋습니다. 버전 6.1.x FMC 웹 인터페이스에서 앞서 설명한 대로 정책의 지연 기반 성능 설정을 확인하고 기본값으로 되돌리기 버튼이 흐리게 표시되는지 확인합니다. 버튼이 흐리게 표시되는 경우 기본 설정을 사용합니다. 활성 상태인 경우 사용자 정의 설정을 구성했습니다.

## 'Snort Fail Open'이 FTD의 'Failsafe'를 대체합니다.

구축: FMC를 사용하는 FTD

업그레이드 대상: 버전 6.1.x

직접 업그레이드: 버전 6.2 이상

버전 6.2에서는 Snort Fail Open 구성이 FMC가 관리하는 Firepower Threat Defense 디바이스의 Failsafe 옵션을 대체합니다. Snort가 사용 중일 때 Failsafe는 트래픽 삭제를 허용하지만, Snort가 종료된 경우 트래픽은 자동으로 검사 없이 통과됩니다. Snort Fail Open은 트래픽 삭제를 허용합니다.

FTD 디바이스를 업그레이드할 때 새 Snort Fail Open 설정은 다음과 같이 기존 Failsafe 설정에 따라 달라집니다. 새 구성은 트래픽 처리 방법을 변경하지 않지만, 업그레이드 전 Failsafe의 활성화 여부를 고려하는 것이 좋습니다.

표 64: Failsafe를 Snort Fail Open으로 마이그레이션

버전 6.1 Failsafe	버전 6.2 Snort Fail Open	행동
비활성화됨(기본 동작)	사용 중: 비활성 종료: 활성	Snort 프로세스가 사용 중이면 새 연결과 기존 연결이 삭제되고, Snort 프로세스가 중단되면 새 연결과 기존 연결이 검사 없이 통과됩니다.
Enabled(활성화)	사용 중: 활성 종료: 활성	Snort 프로세스가 사용 중이거나 중단되면 새 연결과 기존 연결이 검사 없이 통과됩니다.

Snort Fail Open은 디바이스에 버전 6.2가 필요합니다. 버전 6.1.x 디바이스를 관리 중인 경우 FMC 웹 인터페이스는 Failsafe 옵션을 표시합니다.

## 업그레이드 시 IAB '모든 애플리케이션' 옵션 삭제

구축: FMC, ASA FirePOWER with ASDM

업그레이드 대상: 6.1.0.3 또는 이후 패치

직접 업그레이드: 6.2.0 한정

IAB(Intelligent Application Bypass) 옵션 '식별되지 않은 애플리케이션을 포함한 모든 애플리케이션'은 IAP 검사 성능 한계 중 하나를 만족할 경우 애플리케이션 유형과 상관없이 플로우 바이패스 임계값을 초과하는 애플리케이션을 신뢰합니다. 이 옵션은 다음 버전에서 사용할 수 있습니다.

- 버전 6.0.1.4 및 이후 패치
- 버전 6.1.0.3 및 이후 패치
- 버전 6.2.0.1 및 이후 패치
- 버전 6.2.2 및 모든 이후 패치와 주요 버전

옵션이 지원되는 버전에서 옵션이 지원되지 않는 버전으로 업그레이드하면 해당 옵션이 삭제됩니다. 또한 실제로 이 옵션을 활성화하고 사용자의 액세스 제어 정책에 IAB 우회 가능 애플리케이션 및 필터 구성이 포함되지 않는 경우 업그레이드된 사용자 인터페이스는 다음과 같이 예기치 않은 동작을 수행합니다.

- IAB가 활성화되지만 식별되지 않은 애플리케이션을 포함한 모든 애플리케이션 옵션이 더 이상 표시되지 않습니다.
- IAB 컨피그레이션 페이지의 1 Applications/Filters (애플리케이션/필터) 에서 하나의 애플리케이션 또는 필터를 구성했다고 잘못 표시됩니다.
- 애플리케이션 및 필터 편집기의 선택된 애플리케이션 및 필터 창이 삭제됨(FMC) 또는 모든 애플리케이션(ASDM) 중 하나를 표시합니다. 이 선택 항목을 삭제하는 것이 좋습니다.

옵션을 복원하려면 6.2.0.x 버전의 패치를 적용하거나 버전 6.2.2 이상으로 업그레이드(권장)합니다.

## 업그레이드 시 비활성화된 메모리 부족 장치에 대한 URL 필터링 하위 사이트 조회

구축: URL 필터링을 수행하는 메모리 부족 장치

업그레이드 대상: 버전 6.1.0.3 또는 이후 패치

직접 업그레이드: 버전 6.2.0 한정

메모리 제한으로 인해 일부 디바이스 모델은 크기가 더 작은 카테고리 및 평판 데이터베이스를 사용해 URL 필터링을 수행합니다. URL의 하위 사이트에 상위 사이트와 다른 URL 카테고리 및 평판이 존재하지만 디바이스에 상위 사이트의 데이터만 있는 경우 문제가 발생할 수 있습니다.

버전 6.1.0.3에서는 상위 사이트의 URL 카테고리 및 평판에 의존하는 대신 디바이스가 이런 하위 사이트를 '알 수 없는' 카테고리 및 평판으로 간주하도록 시스템의 동작을 변경했습니다. 이렇게 하면 디바이스가 하위 사이트의 데이터에 대해 클라우드 조회를 수행(및 다음을 위해 결과 캐싱)합니다.

버전 6.2.0에서는 이러한 하위 사이트 클라우드 조회에 대한 지원을 중단합니다. 영향을 받는 디바이스:

- Firepower 7010, 7020, 및 7030
- ASA 5506-X series, 5508-X, 5516-X

- ASA 5512-X, 5515-X, 5525-X

버전 6.2.0.1에서 지원이 다시 도입됩니다.

## 버전 6.1.0 지침

다음의 중요 지침은 버전 6.1.0에 적용됩니다.

### ASA FirePOWER 모듈을 업그레이드하기 전 ASA REST API 비활성화

구축: ASA FirePOWER



참고 이 경고는 모든 향후 릴리스에 적용됩니다. 이제 업그레이드 절차에 이 단계가 명시적으로 포함됩니다.

ASA FirePOWER 모듈을 업그레이드하기 전 ASA CLI를 사용해 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

디바이스는 버전 6.0 이상의 ASA FirePOWER 모듈도 실행 중인 경우 ASA REST API를 지원하지 않습니다.

### STIG 모드가 UCAPL 모드로 변경됨

구축: Firepower Management Center

버전 6.1에서는 STIG(Security Technical Implementation Guide) 모드로 알려진 보안 인증서 컴플라이언스 모드의 이름이 UCAPL(Unified Capabilities Approved Products List) 모드로 바뀌었습니다. 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

구축: Firepower Management Center

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

다음의 중요 지침은 버전 6.0.0에 적용됩니다.

### 용어 및 브랜딩

버전 6.0에서는 다음을 포함한 주요 용어 및 브랜딩이 변경되었습니다.

- FireSIGHT System → Firepower
- FireSIGHT Defense Center → Firepower Management Center(FMC)
- Series 3 디바이스 → 7000 Series 디바이스 또는 8000 Series 디바이스
- 가상 매니지드 디바이스 → NGIPSv

자세한 내용은 [Cisco Firepower 용어 가이드](#)를 참조하십시오.

### 버전 6.0 사전 설치 패키지

Cisco에서는 버전 5.4.x에서 버전 6.0으로의 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. 자세한 내용은 [FireSIGHT System 릴리스 노트 버전 6.0.0 사전 설치](#)를 참조하십시오.

플랫폼	업그레이드할 최소 버전	패키지 필수	패키지 권장
FireSIGHT Defense Center(FMC)	5.4.1.1	5.4.1.1~5.4.1.5	5.4.1.6 이상
7000/8000 시리즈	5.4.0.2	5.4.0.2~5.4.0.6	5.4.0.7 이상
NGIPSv	5.4.0.2	5.4.0.2~5.4.0.6	5.4.0.7 이상
ASA FirePOWER: 5.4.1.x	5.4.1.1	5.4.1.1~5.4.1.5	5.4.1.6 이상
ASA FirePOWER: 5.4.0.x	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 적절한 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 업그레이드](#)를 참조하십시오.
- 메모리 업그레이드 - *Firepower Management Center* 설치 설명서의 [Firepower Management Center 용 메모리 업그레이드 지침](#)을 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 사용](#)을 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.

## 버전별 패치 지침

이 체크리스트에는 Firepower 패치에 대한 중요한 업그레이드 지침과 경고가 포함됩니다.

### 버전 6.6.x.x 지침

이 체크리스트에는 버전 6.6.x 패치에 대한 업그레이드 지침이 포함되어 있습니다.

표 65: 버전 6.6.x.x 가이드라인

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	<a href="#">FDM을 사용하는 버전 6.6.0.1 FTD 업그레이드에서 HA 일시 중단, 187 페이지</a>	FDM을 사용하는 FTD	6.6.0	6.6.0.1

### FDM을 사용하는 버전 6.6.0.1 FTD 업그레이드에서 HA 일시 중단

구축: FDM을 사용하는 FTD, 고가용성 쌍으로 설정됨

업그레이드 시작 버전: 버전 6.6.0

직접 업그레이드: 버전 6.6.0.1

관련 버그: [CSCvv45500](#)

HA(고가용성)의 FDM 관리 FTD 디바이스를 버전 6.6.0.1로 업그레이드하고 나서 업그레이드 후 재부팅을 하면 디바이스가 일시 중단 모드로 전환됩니다. HA를 수동으로 다시 시작해야 합니다.

FMC 구축은 영향을 받지 않습니다.

FDM 관리 FTD HA 쌍을 버전 6.6.0.1로 업그레이드하려면 다음을 수행합니다.

1. 스탠바이 디바이스를 업그레이드합니다.
2. 업그레이드가 완료되고 디바이스가 재부팅되면 HA를 수동으로 다시 시작합니다. FDM 또는 CLI를 사용할 수 있습니다.

- FDM: **Device**(디바이스) > **High Availability**(고가용성)를 클릭한 다음 기어 메뉴(⚙)에서 **Resume HA**(HA 다시 시작)를 클릭합니다.

- CLI: **configure high-availability resume**

유닛이 피어와 상태를 협상하고 나면 새로 업그레이드된 디바이스의 HA 상태가 정상(스탠바이 유닛) 상태로 돌아갑니다.

3. 새로 업그레이드된 디바이스가 활성 피어가 되도록 활성 및 대기 피어를 전환합니다(강제 페일오버).
4. 새 스탠바이 피어에 대해 이 절차를 반복합니다.

FDM을 사용한 고가용성 구성 및 관리에 대한 자세한 내용은 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)를 참조하십시오.

## 버전 6.4.0.x 지침

이 체크리스트에는 버전 6.4.0 패치에 대한 업그레이드 지침이 포함되어 있습니다.

표 66: 버전 6.4.0.x 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	<a href="#">업데이트 실패: 컨테이너 인스턴스의 디스크 공간 부족, 168 페이지</a>	Firepower 4100/9300	6.4.0.x	이후 패치 6.5.0
	<a href="#">Firepower 1010 디바이스의 EtherChannel은 이그레스 트래픽 블랙홀이 가능합니다., 168 페이지</a>	Firepower 1010	6.4.0 한정	6.4.0.3~6.4.0.5
	<a href="#">버전 6.4.0.9~6.4.0.11로 업그레이드하기 전에 이전 Firepower 7000/8000 디바이스를 버전 6.4.0으로 이미지 재설치, 188 페이지</a>	Firepower 7000/8000 시리즈	6.4.0~6.4.0.10	6.4.0.9~6.4.0.11

## 버전 6.4.0.9~6.4.0.11로 업그레이드하기 전에 이전 Firepower 7000/8000 디바이스를 버전 6.4.0으로 이미지 재설치

구축: Firepower 7000/8000 Series

업그레이드 시작 버전: 버전 6.4.0~6.4.0.10

직접 업그레이드: 버전 6.4.0.9~6.4.0.11

관련 버그: [CSCvw01028](#)



Firepower 7000/8000 Series 디바이스에서 버전 6.4.0 이전 버전을 실행한 경우, 버전 6.4.0.9, 6.4.0.10 또는 6.4.0.11로 업그레이드하기 전에 버전 6.4.0으로 이미지를 다시 설치해야 합니다. 그렇지 않으면 디바이스가 응답하지 않을 수 있으며, 이미지를 다시 생성해야 합니다.

버전 6.4.0.9 또는 6.4.0.10을 이미 실행 중인 경우

- 이 문제에 취약하므로 지금 이미지 재설치/다시 업그레이드해야 합니다. 또는 Cisco TAC에 핫픽스를 문의하십시오.
- 이미 핫픽스를 적용했으므로, 버전 6.4.0.11로 당장 업그레이드하지 마십시오. 수정 사항이 적용되지 않습니다. 대신 버전 6.4.0으로 이미지를 재설치한 다음 6.4.0.11로 업그레이드하십시오.

이 문제는 향후 패치에서 해결됩니다.

## 버전 6.3.0.x 지침

이 체크리스트에는 버전 6.3.0 패치에 대한 업그레이드 지침이 포함되어 있습니다.

표 67: 버전 6.3.0.x 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	<a href="#">업데이트 실패: 컨테이너 인스턴스의 디스크 공간 부족, 168 페이지</a>	Firepower 4100/9300	6.3.0.x	이후 패치 6.4.0 및 6.5.0

## 버전 6.2.3.x 지침

이 체크리스트에는 버전 6.2.3 패치에 대한 업그레이드 지침이 포함되어 있습니다.

표 68: 버전 6.2.3.x 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	<a href="#">CC 모드를 사용하는 버전 6.2.3.10 FTD 업그레이드의 FSIC 오류, 189 페이지</a>	FTD	6.2.3~6.2.3.9	6.2.3.10 한정
	<a href="#">버전 6.2.3.3 FTD 디바이스는 로컬 관리로 전환할 수 없습니다., 190 페이지</a>	FMC를 사용하는 FTD	6.2.3~6.2.3.2	6.2.3.3
	<a href="#">버전 6.2.3-88 FMC 업그레이드 전 핫픽스, 190 페이지</a>	FMC	6.2.3-88	6.2.3.1~6.2.3.3

### CC 모드를 사용하는 버전 6.2.3.10 FTD 업그레이드의 FSIC 오류

구축: Firepower Threat Defense

업그레이드 대상: 버전 6.2.3~6.2.3.9

버전 6.2.3.3 FTD 디바이스는 로컬 관리로 전환할 수 없습니다.

직접 업그레이드: 버전 6.2.3.10

알려진 문제: [CSCvo39052](#)

FTD 디바이스를 CC 모드를 활성화한 상태로 버전 6.2.3.10으로 업그레이드하면 디바이스가 재부팅할 때 FSIC(파일 시스템 무결성 검사) 오류가 발생합니다.



주의 보안 인증 컴플라이언스를 활성화하고 FSIC가 실패하면 Firepower 소프트웨어가 시작되지 않고 원격 SSH 액세스가 비활성화되며 로컬 콘솔을 통해서만 어플라이언스에 액세스할 수 있습니다. 이러한 현상이 발생한다면 Cisco TAC에 문의하십시오.

FTD 구축에 보안 인증서 컴플라이언스(CC 모드)가 필요한 경우 버전 6.2.3.13 이상으로 직접 업그레이드하는 것이 좋습니다. 또한 Firepower 4100/9300 디바이스의 경우 FXOS 2.3.1.130 이상으로 업그레이드하는 것이 좋습니다.

## 버전 6.2.3.3 FTD 디바이스는 로컬 관리로 전환할 수 없습니다.

구축: FMC를 사용하는 FTD

업그레이드 대상: 버전 6.2.3~버전 6.2.3.2

직접 업그레이드: 버전 6.2.3.3 한정

버전 6.2.3.3에서는 Firepower Threat Defense 디바이스 관리를 FMC에서 FDM으로 전환할 수 없습니다. 이 문제는 버전 6.2.3.3 패치를 제거해도 발생합니다. 해당 시점에서 로컬 관리로 전환하려면 버전 6.2.3을 새롭게 설치하거나 Cisco TAC에 문의하십시오.

해결 방법으로는 버전 6.2.3.3으로 업그레이드하기 전 관리를 전환하거나 최신 패치로 업그레이드합니다. 관리를 전환하면 디바이스 구성이 제거됩니다.

버전 6.2.3.3에서는 FDM에서 FMC로 관리를 전환할 수 있습니다.

## 버전 6.2.3-88 FMC 업그레이드 전 핫픽스

구축: FMC

업그레이드 대상: 버전 6.2.3-88

직접 업그레이드: 버전 6.2.3.1, 버전 6.2.3.2 또는 버전 6.2.3.3

Cisco가 Firepower 업그레이드 패키지의 업데이트된 빌드를 릴리스하는 경우가 있습니다. 버전 6.2.3-88은 이후 빌드로 대체되었습니다. 버전 6.2.3-88을 실행하는 FMC를 버전 6.2.3.1, 버전 6.2.3.2 또는 버전 6.2.3.3으로 업그레이드하면 SSE 클라우드 연결이 지속적으로 삭제되어 오류가 발생합니다. 패치를 제거해도 문제가 해결되지 않습니다.

버전 6.2.3-88을 실행 중인 경우 업그레이드 전 [핫픽스 T](#)를 설치합니다.

## 버전 6.2.2.x 지침

이 체크리스트에는 버전 6.2.2 패치에 대한 업그레이드 지침이 포함되어 있습니다.

표 69: 버전 6.2.2.x 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	<a href="#">Firepower 2100 Series HA 쌍 버전 6.2.2가 6.2.2.4로 업그레이드 불가, 191 페이지</a>	Firepower 2100 series HA 쌍	6.2.2 한정	6.2.2.4 한정

## Firepower 2100 Series HA 쌍 버전 6.2.2가 6.2.2.4로 업그레이드 불가

구축: FTD 고가용성 쌍으로 구성된 Firepower 2100 Series 디바이스

업그레이드 대상: 버전 6.2.2 한정

직접 업그레이드: 버전 6.2.2.4 한정

버전 6.2.2에서 버전 6.2.2.4로 업그레이드하면 Firepower 2100 고가용성 디바이스에 오류가 발생합니다. 버전 6.2.2가 실행 중이며 버전 6.2.2.4 버전으로 업그레이드가 필요한 경우 먼저 버전 6.2.2.1로 업그레이드하십시오. 그렇지 않으면 이 버전은 건너뛰는 것이 좋습니다.

이미 업그레이드를 시작해 업그레이드가 실패한 경우에도 이미지를 재설치하는 것이 좋습니다.

## 버전 6.2.0.x 지침

이 체크리스트에는 버전 6.2.0 패치에 대한 업그레이드 지침이 포함되어 있습니다.

표 70: 버전 6.2.0.x 지침

□	지침	플랫폼	업그레이드 대상	직접 업그레이드
	<a href="#">버전 6.2.0.3 FMC에 핫픽스 BH 적용, 191 페이지</a>	FMC	6.2.0~6.2.0.2	6.2.0.3 한정

## 버전 6.2.0.3 FMC에 핫픽스 BH 적용

구축: FMC

업그레이드 대상: 버전 6.2~6.2.0.2

직접 업그레이드: 버전 6.2.0.3만

해결 방법: [CSCvg32885](#)

버전 6.2.0.3으로 업그레이드한 후에는 핫픽스 BH를 적용해야 합니다. 핫픽스 BH를 적용하지 않으면 액세스 제어 규칙을 편집하거나 구성 변경을 배포할 수 없습니다.

자세한 내용은 [Firepower 핫픽스 릴리스 노트](#)를 참조하십시오.

# 날짜 기반 지침

경우에 따라 Cisco에서는 날짜 기반 업그레이드 지침 및 경고를 제공합니다.

## 동적 분석용 만료 CA 인증서

배포: 동적 분석용 파일을 제출하는 네트워크용 AMP(악성코드 탐지) 구축

영향을 받는 버전: 버전 6.0 이상

해결 방법: [CSCvj07038](#)

2018년 6월 15일부터 일부 Firepower 구축에서 동적 분석용 파일 제출이 중단되었습니다. 이는 AMP Threat Grid 클라우드와의 통신에 필요한 CA 인증서 만료로 발생되었습니다. 버전 6.3.0은 새 인증서를 처음으로 사용하는 주요 버전입니다.



**참고** 6.3.0 이상 버전으로 업그레이드하지 않으려면 새 인증서를 가져와 동적 분석을 재활성화할 수 있도록 패치 또는 핫픽스를 설치해야 합니다. 그러나 나중에 패치 또는 핫픽스를 설치한 구축을 버전 6.2.0 또는 6.2.3으로 업그레이드하면 이전 인증서로 되돌아가므로 패치나 핫픽스를 다시 설치해야 합니다.

패치 또는 핫픽스를 처음으로 설치하는 경우 방화벽이 FMC와 관리되는 디바이스에서 `fmc.api.threatgrid.com`(`panacea.threatgrid.com` 대체)으로 아웃바운드 연결을 허용하는지 확인하십시오. 관리되는 장치는 동적 분석을 위해 파일을 클라우드에 제출합니다. 결과는 FMC 쿼리입니다.

이 테이블에는 각 주요 버전 시퀀스 및 플랫폼에 대해 이전 인증서가 포함된 버전 및 새 인증서를 포함한 패치와 핫픽스 목록이 나열되어 있습니다. 패치 및 핫픽스는 Cisco 지원 및 다운로드 사이트에서 사용할 수 있습니다.

표 71: 새 CA 인증서가 포함된 패치 및 핫픽스

이전 인증서가 포함된 버전	새 인증서가 포함된 첫 번째 패치	새 인증서가 포함된 핫픽스	
6.2.3~6.2.3.3	6.2.3.4	핫픽스 G	FTD 디바이스
		핫픽스 H	FMC, NGIPS 디바이스
6.2.2~6.2.2.3	6.2.2.4	핫픽스 BN	모든 플랫폼
6.2.1	없음 업그레이드가 필요합니다.	없음 업그레이드가 필요합니다.	
6.2.0~6.2.0.5	6.2.0.6	핫픽스 BX	FTD 디바이스
		핫픽스 BW	FMC, NGIPS 디바이스
6.1.0~6.1.0.6	6.1.0.7	핫픽스 EM	모든 플랫폼

이전 인증서가 포함된 버전	새 인증서가 포함된 첫 번째 패치	새 인증서가 포함된 핫픽스
6.0.x	없음 업그레이드가 필요합니다.	없음 업그레이드가 필요합니다.





# 14 장

## 시간 테스트 및 디스크 공간 요구 사항

Firepower 어플라이언스를 업그레이드하려면 사용 가능한 디스크 공간이 충분해야 합니다. 그렇지 않으면 업그레이드에 실패합니다. Firepower Management Center을 사용하여 관리되는 디바이스를 업그레이드하는 경우 FMC에서 디바이스 업그레이드 패키지를 위해 /Volume 파티션에 추가 디스크 공간을 요구합니다. 또한 업그레이드를 수행할 시간도 충분해야 합니다.

Cisco에서는 참조 목적으로 사내 시간 및 디스크 공간 테스트 결과를 제공합니다.

- [시간 테스트 정보, 197 페이지](#)
- [디스크 공간 요구 사항 정보, 198 페이지](#)
- [버전 6.7.0 시간 및 디스크 공간, 198 페이지](#)
- [버전 6.6.1 시간 및 디스크 공간, 199 페이지](#)
- [버전 6.6.0.1 시간 및 디스크 공간, 200 페이지](#)
- [버전 6.6.0 시간 및 디스크 공간, 200 페이지](#)
- [버전 6.5.0.5 시간 및 디스크 공간, 201 페이지](#)
- [버전 6.5.0.4 시간 및 디스크 공간, 202 페이지](#)
- [버전 6.5.0.3 시간 및 디스크 공간, 202 페이지](#)
- [버전 6.5.0.2 시간 및 디스크 공간, 202 페이지](#)
- [버전 6.5.0.1 시간 및 디스크 공간, 203 페이지](#)
- [버전 6.5.0 시간 및 디스크 공간, 203 페이지](#)
- [버전 6.4.0.11 시간 및 디스크 공간, 204 페이지](#)
- [버전 6.4.0.10 시간 및 디스크 공간, 204 페이지](#)
- [버전 6.4.0.9 시간 및 디스크 공간, 205 페이지](#)
- [버전 6.4.0.8 시간 및 디스크 공간, 206 페이지](#)
- [버전 6.4.0.7 시간 및 디스크 공간, 206 페이지](#)
- [버전 6.4.0.6 시간 및 디스크 공간, 207 페이지](#)
- [버전 6.4.0.5 시간 및 디스크 공간, 207 페이지](#)
- [버전 6.4.0.4 시간 및 디스크 공간, 208 페이지](#)
- [버전 6.4.0.3 시간 및 디스크 공간, 208 페이지](#)
- [버전 6.4.0.2 시간 및 디스크 공간, 209 페이지](#)
- [버전 6.4.0.1 시간 및 디스크 공간, 210 페이지](#)
- [버전 6.4.0 시간 및 디스크 공간, 210 페이지](#)

- 버전 6.3.0.5 시간 및 디스크 공간, 211 페이지
- 버전 6.3.0.4 시간 및 디스크 공간, 211 페이지
- 버전 6.3.0.3 시간 및 디스크 공간, 212 페이지
- 버전 6.3.0.2 시간 및 디스크 공간, 213 페이지
- 버전 6.3.0.1 시간 및 디스크 공간, 213 페이지
- 버전 6.3.0 시간 및 디스크 공간, 214 페이지
- 버전 6.2.3.16 시간 및 디스크 공간, 214 페이지
- 버전 6.2.3.15 시간 및 디스크 공간, 215 페이지
- 버전 6.2.3.14 시간 및 디스크 공간, 216 페이지
- 버전 6.2.3.13 시간 및 디스크 공간, 216 페이지
- 버전 6.2.3.12 시간 및 디스크 공간, 217 페이지
- 버전 6.2.3.11 시간 및 디스크 공간, 217 페이지
- 버전 6.2.3.10 시간 및 디스크 공간, 218 페이지
- 버전 6.2.3.9 시간 및 디스크 공간, 218 페이지
- 버전 6.2.3.8 시간 및 디스크 공간, 219 페이지
- 버전 6.2.3.7 시간 및 디스크 공간, 219 페이지
- 버전 6.2.3.6 시간 및 디스크 공간, 220 페이지
- 버전 6.2.3.5 시간 및 디스크 공간, 220 페이지
- 버전 6.2.3.4 시간 및 디스크 공간, 221 페이지
- 버전 6.2.3.3 시간 및 디스크 공간, 221 페이지
- 버전 6.2.3.2 시간 및 디스크 공간, 222 페이지
- 버전 6.2.3.1 시간 및 디스크 공간, 223 페이지
- 버전 6.2.3 시간 및 디스크 공간, 223 페이지
- 버전 6.2.2.5 시간 및 디스크 공간, 224 페이지
- 버전 6.2.2.4 시간 및 디스크 공간, 225 페이지
- 버전 6.2.2.3 시간 및 디스크 공간, 226 페이지
- 버전 6.2.2.2 시간 및 디스크 공간, 227 페이지
- 버전 6.2.2.1 시간 및 디스크 공간, 227 페이지
- 버전 6.2.2 시간 및 디스크 공간, 228 페이지
- 버전 6.2.0.6 시간 및 디스크 공간, 228 페이지
- 버전 6.2.0.5 시간 및 디스크 공간, 229 페이지
- 버전 6.2.0.4 시간 및 디스크 공간, 230 페이지
- 버전 6.2.0.3 시간 및 디스크 공간, 230 페이지
- 버전 6.2.0.2 시간 및 디스크 공간, 231 페이지
- 버전 6.2.0.1 시간 및 디스크 공간, 231 페이지
- 버전 6.2.0 시간 및 디스크 공간, 232 페이지
- 버전 6.1.0.7 시간 및 디스크 공간, 232 페이지
- 버전 6.1.0.6 시간 및 디스크 공간, 233 페이지
- 버전 6.1.0.5 시간 및 디스크 공간, 234 페이지
- 버전 6.1.0.4 시간 및 디스크 공간, 234 페이지
- 버전 6.1.0.3 시간 및 디스크 공간, 235 페이지



- 버전 6.1.0.2 시간 및 디스크 공간, 236 페이지
- 버전 6.1.0.1 시간 및 디스크 공간, 236 페이지
- 버전 6.1.0 시간 및 디스크 공간, 237 페이지
- 버전 6.0.1.4 시간 및 디스크 공간, 237 페이지
- 버전 6.0.1.3 시간 및 디스크 공간, 238 페이지
- 버전 6.0.1.2 시간 및 디스크 공간, 238 페이지
- 버전 6.0.1.1 시간 및 디스크 공간, 239 페이지
- 버전 6.0.1 시간 및 디스크 공간, 239 페이지
- 버전 6.0.0.1 시간 및 디스크 공간, 240 페이지
- 버전 6.0 시간 및 디스크 공간, 240 페이지

## 시간 테스트 정보

여기에 표시된 시간 값은 내부 테스트 기반입니다.



**참고** 모든 업그레이드 테스트 중 특정 플랫폼/시리즈에서 가장 오래 걸리는 시간이 표시되지만, 여러 이유로 제공된 시간보다 업그레이드에 더 오랜 시간이 소요될 수 있습니다(아래 제공).

### 테스트 조건

- 구축: Firepower Management Center 구축에서 테스트한 값입니다. 이는 유사한 조건일 때 원격 및 로컬 관리 디바이스의 원시 업그레이드 시간이 유사하기 때문입니다.
- 버전: 주요 업그레이드의 경우 모든 대상 이전 주요 버전에서의 업그레이드를 테스트했습니다. 패치의 경우 기본 버전에서 업그레이드를 테스트합니다.
- 모델: 대부분의 경우 각 시리즈의 최저 사양 모델에서 테스트하였지만, 일부는 시리즈 내 여러 모델에서 테스트했습니다.
- 가상 설정: 메모리 및 리소스는 기본 설정으로 테스트했습니다.
- 고가용성 및 확장성: 독립형 디바이스에서 테스트합니다.

고가용성 또는 클러스터된 구성에서는 업그레이드 시 각 디바이스가 유지 관리 모드로 가동되며 가동 연속성을 유지하기 위해 디바이스 업그레이드는 한 번에 하나씩 업그레이드합니다. 따라서 디바이스 쌍 또는 전체 클러스터 업그레이드는 독립형 디바이스 업그레이드보다 더 오랜 시간이 소요됩니다. 스택된 8000 Series 디바이스는 동시에 업그레이드하며, 모든 디바이스의 업그레이드가 완료될 때까지 스택 가동이 제한된 혼합 버전 상태로 가동됩니다. 이때는 독립형 디바이스의 업그레이드 소요 시간과 큰 차이가 나지 않습니다.

- 구성: 최소한의 구성 및 트래픽 부하로 어플라이언스를 테스트합니다.

구성의 복잡성, 이벤트 데이터베이스 크기, 업그레이드의 영향 여부 및 정도에 따라 업그레이드 소요 시간이 증가할 수 있습니다. 예를 들어 액세스 제어 규칙을 많이 사용하여 백엔드에서 규칙 저장 방식을 변경해야 하는 경우, 업그레이드에 오랜 시간이 소요될 수 있습니다.

업그레이드에 걸리는 시간

값은 각 플랫폼에서 Firepower 업그레이드 스크립트가 실행되는 데 걸린 시간만을 나타냅니다. 다음에 대한 시간은 포함되지 않습니다.

- 업그레이드하기 전에 또는 업그레이드하는 동안 관리되는 디바이스로 업그레이드 패키지 전송
- 준비도 확인
- VDB 및 침입 규칙(SRU/LSP) 업데이트
- 구성 구축
- 재부팅(값은 별도로 제공될 수 있음)

## 디스크 공간 요구 사항 정보

공간 예상은 모든 업그레이드에서 보고된 가장 큰 용량입니다. 2020년 초 이후 릴리스의 경우 다음과 같습니다.

- 반올림되지 않습니다(1MB 미만).
- 다음 1MB로 반올림됩니다(1MB~100MB).
- 다음 10MB(100MB~1GB)로 반올림됩니다.
- 다음 100MB(1GB 이상)로 반올림됩니다.

## 버전 6.7.0 시간 및 디스크 공간

표 72: 버전 6.7.0 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	업그레이드 시간	재부팅 시간
FMC	13.6GB	70MB	—	46분	9분
FMCv: VMware 6.0	15.5GB	64MB	—	35분	8분
Firepower 1000 Series	430MB	11GB	2GB	17분	16분
Firepower 2100 Series	500MB	11GB	1.1 GB	15분	16분
Firepower 4100 Series	10MB	10GB	1.1 GB	10분	12분

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	업그레이드 시간	재부팅 시간
Firepower 4100 Series 컨테이너 인스턴스	8MB	9.5GB	1.1 GB	10분	9분
Firepower 9300	64MB	11.1GB	1.1 GB	13분	12분
ASA 5500-X Series with FTD	8.7GB	96KB	1.1 GB	26분	13분
FTDv: VMware 6.0	8.1GB	26KB	1.1 GB	14분	18분
ASA FirePOWER	10.3GB	64MB	1.3 GB	62분	11분
NGIPSv: VMware 6.0	5.5GB	54MB	840MB	10분	6분

## 버전 6.6.1 시간 및 디스크 공간

표 73: 버전 6.6.1 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	업그레이드 시간	재부팅 시간
FMC	18.6GB	23MB	—	54분	14분
FMCv: VMware 6.0	15.8GB	58MB	—	56분	13분
Firepower 1000 Series	10.8GB	400MB	1.1 GB	20분	17분
Firepower 2100 Series	10.9GB	450MB	1.1 GB	16분	21분
Firepower 4100 Series	9.7GB	10MB	1GB	15분	14분
Firepower 4100 Series 컨테이너 인스턴스	11.2 GB	9MB	1GB	10분	13분
Firepower 9300	9.8GB	11MB	1GB	15분	15분
ASA 5500-X Series with FTD	9.3GB	1MB	1.2 GB	21분	24분
FTDv: VMware 6.0	9.3GB	1MB	1.2 GB	18분	19분
ASA FirePOWER	12.3GB	26MB	1.4GB	72분	23분
NGIPSv: VMware 6.0	7.1GB	54MB	860MB	14분	20분

## 버전 6.6.0.1 시간 및 디스크 공간

이 테이블에서 업그레이드 시간에는 재부팅이 포함됩니다.

표 74: 버전 6.6.0.1 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.6.0에서 업그레이드 시간
FMCv: VMware 6.0	1.1 GB	23MB	—	17분
Firepower 1000 Series	450MB	450MB	240MB	21분
Firepower 2100 Series	260MB	260MB	270MB	17분
Firepower 4100 Series	470MB	470MB	46MB	11분
Firepower 9300	460MB	460MB	46MB	33분
ASA 5500-X Series with FTD	440MB	120MB	46MB	17분
ISA 3000 with FTD	440MB	120MB	46MB	21분
FTDv: VMware 6.0	430MB	120MB	46MB	11분
ASA FirePOWER	80MB	20MB	15MB	18분
NGIPSv: VMware 6.0	64MB	28MB	15MB	9분

## 버전 6.6.0 시간 및 디스크 공간



참고 ASA 5545-X with FirePOWER Services의 경우, 디바이스의 SRU가 버전 6.6.0 업그레이드 패키지 (2020-01-16-001-vrt)의 SRU와 같거나 최신 버전이면 업그레이드 시간이 예상보다 1시간 이상 더 걸릴 수 있습니다. 이러한 현상이 사용자에게 영향을 미치는지 확인하려면 디바이스에서 Firepower CLI에 로그인하고 **show version** 명령을 사용하여 **Rules update version**(규칙 업데이트 버전)을 표시합니다.

표 75: 버전 6.6.0 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	업그레이드 시간	재부팅 시간
FMC	16.5GB	71MB	—	46분	15분

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	업그레이드 시간	재부팅 시간
FMCv: VMware 6.0	16.7GB	57MB	—	36분	7분
Firepower 1000 Series	410MB	11.5GB	1.1 GB	20분	17분
Firepower 2100 Series	470MB	10.3GB	1GB	14분	14분
Firepower 4100 Series	61MB	9.3GB	980MB	11분	9분
Firepower 4100 Series 컨테이너 인스턴스	46MB	11.3GB	980MB	11분	6분
Firepower 9300	64MB	10.5GB	980MB	15분	12분
ASA 5500-X Series with FTD	8.7GB	70KB	1.2GB	23분	26분
FTDv: VMware 6.0	8.7GB	70KB	1.2 GB	14분	17분
ASA FirePOWER	11.4GB	63MB	1.4GB	93분	10분
NGIPSv: VMware 6.0	6.1GB	53MB	860MB	10분	5분

## 버전 6.5.0.5 시간 및 디스크 공간

표 76: 버전 6.5.0.5 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	업그레이드 시간	재부팅 시간
FMC	4.4GB	28MB	—	47분	8분
FMCv: VMware 6.0	4.2GB	25MB	—	36분	4분
Firepower 1000 Series	2.6GB	2.6GB	510MB	9분	11분
Firepower 2100 Series	2.5GB	2.5GB	530MB	7분	10분
Firepower 4100 Series	2.6GB	2.6GB	360MB	5분	8분
Firepower 9300	2.6GB	2.6GB	360MB	5분	8분
ASA 5500-X Series with FTD	1.9GB	120MB	310MB	9분	8분
FTDv: VMware 6.0	2.2GB	120MB	310MB	7분	6분

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	업그레이드 시간	재부팅 시간
ASA FirePOWER	4.3GB	32MB	610MB	52분	6분
NGIPSv: VMware 6.0	2.2GB	420MB	470MB	6분	4분

## 버전 6.5.0.4 시간 및 디스크 공간

표 77: 버전 6.5.0.4 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
Firepower 1000 Series	2.6GB	2.6GB	500MB	20분
Firepower 2100 Series	2.5GB	2.5GB	530MB	18분
Firepower 4100 Series	2.5GB	2.5GB	360MB	13분
Firepower 9300	2.5GB	2.5GB	360MB	17분
ASA 5500-X Series with FTD	1.9GB	110MB	310MB	16분
FTDv: VMware 6.0	1.9GB	110MB	310MB	9분
ASA FirePOWER	2.6GB	20MB	340MB	72분
NGIPSv: VMware 6.0	740MB	20MB	230MB	8분

## 버전 6.5.0.3 시간 및 디스크 공간

버전 6.5.0.3은 2019년 02월 04일(FMC용) 및 2020년 03월 02일(디바이스용)에 Cisco 지원 및 다운로드 사이트에서 제거되었습니다. 이 버전을 실행 중인 경우, 계속 사용해도 문제가 없습니다.

## 버전 6.5.0.2 시간 및 디스크 공간

표 78: 버전 6.5.0.2 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	2.6GB	20MB	—	42분
FMCv: VMware 6.0	2.7GB	23MB	—	34분

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
Firepower 1000 Series	2.5GB	2.5GB	480MB	12분
Firepower 2100 Series	2.3GB	2.3GB	500MB	17분
Firepower 4100 Series	2.3GB	2.3GB	340MB	13분
Firepower 9300	2.3GB	2.3GB	340MB	17분
ASA 5500-X Series with FTD	1.9GB	110MB	280MB	22분
FTDv: VMware 6.0	1.7GB	110MB	280MB	10분
ASA FirePOWER	2.5GB	20MB	320MB	56분
NGIPSv: VMware 6.0	680MB	18MB	210MB	9분

## 버전 6.5.0.1 시간 및 디스크 공간

버전 6.5.0.1은 Cisco 지원 및 다운로드 사이트에서 2019년 12월 19일에 제거되었습니다. 버전 6.2.1을 사용 중인 경우 업그레이드를 강력하게 권장합니다.

## 버전 6.5.0 시간 및 디스크 공간

표 79: 버전 6.5.0 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	18.6GB	24MB	—	47분
FMCv: VMware 6.0	18.7GB	30MB	—	35분
Firepower 1000 Series	1GB	11.3GB	1.1 GB	10분
Firepower 2100 Series	1.1 GB	12.3GB	1GB	12분
Firepower 4100 Series	20MB	10.8GB	990MB	8분
Firepower 9300	23MB	10.9GB	990MB	8분
ASA 5500-X Series with FTD	10.4GB	120KB	1.1 GB	17분
FTDv: VMware 6.0	10GB	120KB	1.1 GB	10분
ASA FirePOWER	12.2GB	26MB	1.3 GB	81분

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
NGIPsv: VMware 6.0	6.6GB	22 MB	870MB	9분

## 버전 6.4.0.11 시간 및 디스크 공간

표 80: 버전 6.4.0.11 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.4.0에서 업그레이드 시간	재부팅 시간
FMC	3.8GB	170MB	—	30분	8분
FMCv: VMware 6.0	4.1GB	170MB	—	27분	7분
Firepower 1000 Series	3GB	3GB	530MB	14분	9분
Firepower 2100 Series	2.5GB	2.5GB	510MB	9분	6분
Firepower 4100 Series	1.8GB	1.8GB	310MB	8분	7분
Firepower 9300	1.8GB	1.8GB	310MB	9분	9분
ASA 5500-X Series with FTD	1.6GB	110MB	290MB	12분	12분
FTDv: VMware 6.0	4.4GB	170MB	290MB	28분	4분
Firepower 7000/8000 시리즈	3.6GB	170MB	680MB	11분	97분
ASA FirePOWER	4.2GB	36MB	630MB	54분	51분
NGIPsv: VMware 6.0	2.4GB	150MB	470MB	11분	15분

## 버전 6.4.0.10 시간 및 디스크 공간

표 81: 버전 6.4.0.10 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.4.0에서 업그레이드 시간	재부팅 시간
FMC	3.8GB	170MB	—	30분	8분
FMCv: VMware 6.0	4.1GB	170MB	—	27분	7분



Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.4.0에서 업그레이드 시간	재부팅 시간
Firepower 1000 Series	2.9GB	2.9GB	560MB	11분	14분
Firepower 2100 Series	2.5GB	2.5GB	530MB	8분	13분
Firepower 4100 Series	1.8GB	1.8GB	330MB	5분	11분
Firepower 9300	1.8GB	1.8GB	330MB	5분	17분
ASA 5500-X Series with FTD	1.9GB	110MB	310MB	12분	31분
FTDv: VMware 6.0	2GB	110MB	310MB	8분	8분
Firepower 7000/8000 시리즈	3.6GB	170MB	680MB	11분	97분
ASA FirePOWER	4.2GB	36MB	630MB	54분	51분
NGIPSv: VMware 6.0	2.4GB	150MB	470MB	11분	15분

## 버전 6.4.0.9 시간 및 디스크 공간

표 82: 버전 6.4.0.9 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.4.0에서 업그레이드 시간	재부팅 시간
FMC	3.7GB	170MB	—	41분	10분
FMCv: VMware 6.0	3.7GB	170MB	—	28분	6분
Firepower 1000 Series	2.9GB	2.9GB	530MB	11분	14분
Firepower 2100 Series	2.6GB	2.6GB	510MB	10분	13분
Firepower 4100 Series	1.8GB	1.8GB	310MB	4분	10분
Firepower 9300	1.8GB	1.8GB	310MB	4분	10분
ASA 5500-X Series with FTD	1.9GB	290MB	290MB	12분	42분
FTDv: VMware 6.0	1.9GB	290MB	290MB	7분	9분
Firepower 7000/8000 시리즈	3.7GB	170MB	650MB	20분	6분

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.4.0에서 업그레이드 시간	재부팅 시간
ASA FirePOWER	4.2GB	36MB	600MB	48분	48분
NGIPSv: VMware 6.0	2.1GB	150MB	450MB	6분	4분

## 버전 6.4.0.8 시간 및 디스크 공간

표 83: 버전 6.4.0.8 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.4.0 이상 시간
FMC	5GB	170MB	—	44분
FMCv: VMware 6.0	5.1GB	170MB	—	32분
Firepower 1000 Series	3GB	3GB	530MB	18분
Firepower 2100 Series	2.5GB	2.5GB	510MB	18분
Firepower 4100 Series	1.8GB	1.8GB	310MB	14분
Firepower 9300	2GB	2GB	310MB	11분
ASA 5500-X Series with FTD	1.8GB	110MB	290MB	17분
FTDv: VMware 6.0	1.9GB	110MB	290MB	12분
Firepower 7000/8000 시리즈	3.7GB	190MB	650MB	25분
ASA FirePOWER	2.2GB	110MB	590MB	16분
NGIPSv: VMware 6.0	2.1GB	150MB	450MB	9분

## 버전 6.4.0.7 시간 및 디스크 공간

표 84: 버전 6.4.0.7 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.4.0 이상 시간
FMC	4.9GB	170MB	—	41분
FMCv: VMware 6.0	5.1GB	170MB	—	32분
Firepower 1000 Series	2.9GB	2.9GB	530MB	17분

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.4.0 이상 시간
Firepower 2100 Series	2.4GB	2.4GB	500MB	17분
Firepower 4100 Series	1.7GB	1.7GB	310MB	15분
Firepower 9300	2.4GB	2.4GB	310MB	12분
ASA 5500-X Series with FTD	1.9GB	110MB	290MB	18분
FTDv: VMware 6.0	1.8GB	110MB	290MB	9분
Firepower 7000/8000 시리즈	3.7GB	190MB	650MB	28분
ASA FirePOWER	4.2GB	36MB	590MB	54분
NGIPSv: VMware 6.0	2.3GB	150MB	450MB	9분

## 버전 6.4.0.6 시간 및 디스크 공간

버전 6.4.0.6은 Cisco 지원 및 다운로드 사이트에서 2019년 12월 19일에 제거되었습니다. 이 버전을 사용 중인 경우, 업그레이드하는 것이 좋습니다.

## 버전 6.4.0.5 시간 및 디스크 공간

표 85: 버전 6.4.0.5 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.4.0 이상 시간
FMC	5GB	170MB	—	39분
FMCv: VMware 6.0	3.7GB	170MB	—	27분
Firepower 1000 Series	2.9GB	2.9GB	530MB	26분
Firepower 2100 Series	2.5GB	2.5GB	500MB	16분
Firepower 4100 Series	1.8GB	1.8GB	310MB	12분
Firepower 9300	1.8GB	1.8GB	310MB	11분
ASA 5500-X Series with FTD	1.8GB	110MB	290MB	20분
FTDv: VMware 6.0	1.8GB	110MB	290MB	10분
Firepower 7000/8000 시리즈	3.6GB	170MB	650MB	26분

Platform(플랫폼)	/Volume에 필요한공간	/에 필요한 공간	Space on FMC	6.4.0 이상 시간
ASA FirePOWER	4.1GB	36MB	590MB	45분
NGIPSv: VMware 6.0	2.1GB	150MB	450MB	10분

## 버전 6.4.0.4 시간 및 디스크 공간

표 86: 버전 6.4.0.4 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한공간	/에 필요한 공간	Space on FMC	6.4.0 이상 시간
FMC	4.4GB	170MB	—	35분
FMCv: VMware 6.0	4.8GB	170MB	—	31분
Firepower 1000 Series	2.9GB	2.9GB	520MB	28분
Firepower 2100 Series	2.4GB	2.4GB	500MB	10분
Firepower 4100 Series	2GB	2GB	310MB	12분
Firepower 9300	1.7GB	1.7GB	310MB	10분
ASA 5500-X Series with FTD	1.8GB	110MB	290MB	29분
FTDv: VMware 6.0	1.8GB	110MB	290MB	8분
Firepower 7000/8000 시리즈	3.6GB	170MB	650MB	24분
ASA FirePOWER	4.2GB	36MB	600MB	55분
NGIPSv: VMware 6.0	2.1GB	150MB	550MB	10분

## 버전 6.4.0.3 시간 및 디스크 공간

표 87: 버전 6.4.0.3 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한공간	/에 필요한 공간	Space on FMC	6.4.0 이상 시간
FMC	3.2GB	24MB	—	34분
FMCv: VMware 6.0	2.5GB	23MB	—	25분
Firepower 1000 Series	2.9GB	2.9GB	520MB	22분

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.4.0 이상 시간
Firepower 2100 Series	2.4GB	2.4GB	500MB	19분
Firepower 4100 Series	1.7GB	1.7GB	310MB	12분
Firepower 9300	1.7GB	1.7GB	310MB	14분
ASA 5500-X Series with FTD	1.8GB	110MB	290MB	18분
FTDv: VMware 6.0	1.8GB	110MB	290MB	12분
Firepower 7000/8000 시리즈	1.9GB	21MB	370MB	20분
ASA FirePOWER	2.5GB	2.5GB	320MB	28분
NGIPSv: VMware 6.0	690MB	21MB	210MB	8분

## 버전 6.4.0.2 시간 및 디스크 공간

표 88: 버전 6.4.0.2 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.4.0 이상 시간
FMC	3.1GB	24MB	—	39분
FMCv: VMware 6.0	2.5GB	23MB	—	24분
Firepower 2100 Series	1.9GB	1.9GB	480MB	19분
Firepower 4100 Series	2.3GB	2.3GB	290MB	11분
Firepower 9300	1.7GB	1.7GB	290MB	11분
ASA 5500-X Series with FTD	1.8GB	110MB	270MB	21분
FTDv: VMware 6.0	1.2 GB	110MB	270MB	10분
Firepower 7000/8000 시리즈	1.9GB	36MB	350MB	20분
ASA FirePOWER	2GB	21MB	300MB	34분
NGIPSv: VMware 6.0	630MB	21MB	190MB	10분

## 버전 6.4.0.1 시간 및 디스크 공간

표 89: 버전 6.4.0.1 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.4.0 이상 시간
FMC	1.8GB	24MB	—	50분
FMCv: VMware 6.0	1.8GB	23MB	—	20분
Firepower 2100 Series	1.4GB	1.4GB	300MB	17분
Firepower 4100 Series	1.1 GB	1.1 GB	95MB	9분
Firepower 9300	1.1 GB	1.1 GB	95MB	10분
ASA 5500-X Series with FTD	550MB	110MB	76MB	16분
FTDv: VMware 6.0	550MB	110MB	76MB	15분
Firepower 7000/8000 시리즈	59MB	21MB	2MB	14분
ASA FirePOWER	85MB	20MB	2MB	30분
NGIPSv: VMware 6.0	45MB	21MB	2MB	10분

## 버전 6.4.0 시간 및 디스크 공간

표 90: 버전 6.4.0 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	13.3GB	26MB	—	41분
FMCv: VMware 6.0	13.6GB	29MB	—	30분
Firepower 2100 Series	12MB	8.9GB	950MB	20분
Firepower 4100 Series	10MB	7.5GB	920MB	6분
Firepower 9300	10MB	7.7GB	920MB	7분
ASA 5500-X Series with FTD	9GB	110KB	1.1 GB	24분
FTDv: VMware 6.0	7.5GB	100KB	1.1 GB	12분
Firepower 7000/8000 시리즈	7.7GB	19MB	980MB	34분

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
ASA FirePOWER	11.5GB	22 MB	1.3 GB	66분
NGIPSv: VMware 6.0	6.5GB	19MB	840MB	16분

## 버전 6.3.0.5 시간 및 디스크 공간

표 91: 버전 6.3.0.5 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.3.0 이상 시간
FMC	4.9GB	200MB	—	46분
FMCv: VMware 6.0	4.5GB	180MB	—	41분
Firepower 2100 Series	2.3GB	2.3GB	480MB	21분
Firepower 4100 Series	1.6GB	1.6GB	280MB	13분
Firepower 9300	1.6GB	1.6GB	280MB	17분
ASA 5500-X Series with FTD	1.7GB	110MB	270MB	26분
FTDv: VMware 6.0	1.7GB	110MB	270MB	17분
Firepower 7000/8000 시리즈	2.6GB	210MB	600MB	23분
ASA FirePOWER	3.6GB	47MB	540MB	74분
NGIPSv: VMware 6.0	2.1GB	160MB	440MB	17분

## 버전 6.3.0.4 시간 및 디스크 공간

표 92: 버전 6.3.0.4 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.3.0 이상 시간
FMC	3.4 GB	180MB	—	34분
FMCv: VMware 6.0	4.4GB	180MB	—	38분
Firepower 2100 Series	2.3GB	2.3GB	480MB	17분
Firepower 4100 Series	1.6GB	1.6GB	280MB	12분

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.3.0 이상 시간
Firepower 9300	1.8GB	1.8GB	280MB	12분
ASA 5500-X Series with FTD	1.7GB	110MB	270MB	23분
FTDv: VMware 6.0	1.7GB	110MB	270MB	18분
Firepower 7000/8000 시리즈	3.3GB	170MB	600MB	21분
ASA FirePOWER	3.5GB	31MB	530MB	48분
NGIPSv: VMware 6.0	2.1GB	160MB	430MB	16분

## 버전 6.3.0.3 시간 및 디스크 공간

표 93: 버전 6.3.0.3 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.3.0 이상 시간
FMC	3.7GB	180MB	—	33분
FMCv: VMware 6.0	3.2GB	180MB	—	24분
Firepower 2100 Series	1.2 GB	1.2 GB	290MB	18분
Firepower 4100 Series	990MB	990MB	99MB	11분
Firepower 9300	990MB	990MB	99MB	12분
ASA 5500-X Series with FTD	620MB	110MB	79MB	18분
FTDv: VMware 6.0	240MB	110MB	79MB	7분
Firepower 7000/8000 시리즈	2.6GB	170MB	400MB	20분
ASA FirePOWER	2.9GB	30MB	340MB	45분
NGIPSv: VMware 6.0	1.5 GB	160MB	250MB	4분



## 버전 6.3.0.2 시간 및 디스크 공간

표 94: 버전 6.3.0.2 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.3.0 이상 시간
FMC	3.5GB	180MB	—	53분
FMCv: VMware 6.0	3.2GB	180MB	—	28분
Firepower 2100 Series	1.2 GB	1.2 GB	100 MB	17분
Firepower 4100 Series	970MB	970MB	100 MB	12분
Firepower 9300	970MB	970MB	100 MB	11분
ASA 5500-X Series with FTD	570MB	110MB	80MB	12분
FTDv: VMware 6.0	600MB	110MB	80 MB	10분
Firepower 7000/8000 시리즈	2.5GB	170MB	400MB	20분
ASA FirePOWER	3GB	30MB	340MB	45분
NGIPSv: VMware 6.0	1.5 GB	160MB	250MB	10분

## 버전 6.3.0.1 시간 및 디스크 공간

표 95: 버전 6.3.0.1 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.3.0 이상 시간
FMC	3GB	170MB	—	31분
FMCv: VMware 6.0	2.4GB	170MB	—	25분
Firepower 2100 Series	1.2 GB	1.2 GB	290MB	18분
Firepower 4100 Series	740MB	740MB	100 MB	12분
Firepower 9300	740MB	740MB	100 MB	12분
ASA 5500-X Series with FTD	400MB	150MB	72MB	17분
FTDv: VMware 6.0	400MB	150MB	72MB	10분
Firepower 7000/8000 시리즈	2.1GB	170MB	350MB	20분

Platform(플랫폼)	/Volume에 필요한공간	/에 필요한 공간	Space on FMC	6.3.0 이상 시간
ASA FirePOWER	2.4GB	28MB	270MB	44분
NGIPsv: VMware 6.0	1.5 GB	150MB	350MB	10분

## 버전 6.3.0 시간 및 디스크 공간

표 96: 버전 6.3.0 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한공간	/에 필요한 공간	Space on FMC	시간
FMC	12.7GB	29MB	—	47분
FMCv 위치: VMware 6.0	12.7GB	29MB	—	29분
Firepower 2100 Series	13MB	8.8GB	930MB	20분
Firepower 4100/9300 새시	10MB	7.6GB	930MB	6분
ASA 5500-X Series with FTD	7.9GB	100KB	1.1 GB	25분
FTDv: VMware 6.0	7.3GB	100KB	1.1 GB	12분
Firepower 7000/8000 시리즈	7.0GB	19MB	920MB	32분
ASA FirePOWER	11.3GB	22 MB	1.2 GB	63분
NGIPsv	5.7GB	19MB	810MB	16분

## 버전 6.2.3.16 시간 및 디스크 공간

표 97: 버전 6.2.3.16 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3에서 업그레이드 시간	재부팅 시간
FMC	3.6GB	250MB	—	40분	9분
FMCv: VMware 6.0	3.3GB	220MB	—	25분	4분
Firepower 2100 Series	2.6GB	2.6GB	620MB	11분	12분
Firepower 4100 Series	1.7GB	1.7GB	410MB	5분	5분

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3에서 업그레이드 시간	재부팅 시간
Firepower 9300	1.8GB	1.8GB	410MB	5분	9분
ASA 5500-X Series with FTD	2GB	200MB	430MB	18분	33분
FTDv: VMware 6.0	2GB	190MB	430MB	8분	5분
Firepower 7000/8000 시리즈	3.5GB	200MB	670MB	31분	14분
ASA FirePOWER	3.8GB	58MB	600MB	74분	77분
NGIPSv: VMware 6.0	2.3GB	180MB	500MB	6분	4분

## 버전 6.2.3.15 시간 및 디스크 공간

표 98: 버전 6.2.3.15 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
FMC	4.7GB	260MB	—	50분
FMCv: VMware 6.0	4.7GB	210MB	—	하드웨어에 따라 다름
Firepower 2100 Series	2.3GB	2.3GB	590MB	27분
Firepower 4100 Series	1.7GB	1.7GB	390MB	10분
Firepower 9300	2.4GB	2.4GB	390MB	11분
ASA 5500-X Series with FTD	2GB	190MB	410MB	38분
FTDv: VMware 6.0	2.4GB	190MB	410MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	3.5GB	210MB	640MB	19분
ASA FirePOWER	3.9GB	56MB	580MB	100분
NGIPSv: VMware 6.0	2.7GB	180MB	470MB	하드웨어에 따라 다름

## 버전 6.2.3.14 시간 및 디스크 공간

표 99: 버전 6.2.3.14 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
FMC	4.5GB	260MB	—	58분
FMCv: VMware 6.0	4.7GB	190MB	—	하드웨어에 따라 다름
Firepower 2100 Series	1.9GB	1.9GB	590MB	23분
Firepower 4100 Series	1.7GB	1.7GB	390MB	11분
Firepower 9300	1.7GB	1.7GB	390MB	10분
ASA 5500-X Series with FTD	2GB	200MB	410MB	32분
FTDv: VMware 6.0	2.4GB	190MB	410MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	3.4 GB	200MB	630MB	19분
ASA FirePOWER	3.7GB	53MB	560MB	106분
NGIPSv: VMware 6.0	2.6GB	190MB	470MB	하드웨어에 따라 다름

## 버전 6.2.3.13 시간 및 디스크 공간

표 100: 버전 6.2.3.13 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
FMC	4.7GB	290MB	—	50분
FMCv: VMware 6.0	4.6GB	190MB	—	하드웨어에 따라 다름
Firepower 2100 Series	2.6GB	2.6GB	590MB	25분
Firepower 4100 Series	1.7GB	1.7GB	390MB	11분
Firepower 9300	1.8GB	1.8GB	390MB	11분
ASA 5500-X Series with FTD	2.4GB	190MB	410MB	32분
FTDv: VMware 6.0	2.3GB	190MB	410MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	3.8GB	190MB	620MB	18분

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
ASA FirePOWER	3.7GB	51MB	560MB	105분
NGIPSv: VMware 6.0	2.6GB	180MB	470MB	하드웨어에 따라 다름

## 버전 6.2.3.12 시간 및 디스크 공간

표 101: 버전 6.2.3.12 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
FMC	3.9GB	220MB	—	49분
FMCv: VMware 6.0	4.6GB	160MB	—	하드웨어에 따라 다름
Firepower 2100 Series	1.9GB	1.9GB	390MB	21분
Firepower 4100 Series	970MB	970MB	190MB	14분
Firepower 9300	1.7GB	1.7GB	190MB	11분
ASA 5500-X Series with FTD	1.4GB	96MB	210MB	30분
FTDv: VMware 6.0	2.4GB	200MB	210MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	3.6GB	160MB	540MB	19분
ASA FirePOWER	3.5GB	31MB	480MB	104분
NGIPSv: VMware 6.0	2.6GB	130MB	400MB	하드웨어에 따라 다름

## 버전 6.2.3.11 시간 및 디스크 공간

표 102: 버전 6.2.3.11 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
FMC	4.5GB	250MB	—	39분
FMCv: VMware 6.0	4.6GB	35MB	—	하드웨어에 따라 다름
Firepower 2100 Series	2.8GB	2.8GB	590MB	40분
Firepower 4100 Series	2GB	2GB	380MB	10분

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
Firepower 9300	1.6GB	1.6GB	380MB	11분
ASA 5500-X Series with FTD	1.8GB	230MB	410MB	33분
FTDv: VMware 6.0	2.2GB	230MB	410MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	3.3GB	170MB	600MB	23분
ASA FirePOWER	3.6GB	50MB	530MB	110분
NGIPSv: VMware 6.0	2.6GB	130MB	450MB	하드웨어에 따라 다름

## 버전 6.2.3.10 시간 및 디스크 공간

표 103: 버전 6.2.3.10 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
FMC	4.2GB	200MB	—	40분
FMCv	4.5GB	230MB	—	하드웨어에 따라 다름
Firepower 2100 Series	1.8GB	1.8GB	390MB	21분
Firepower 4100/9300 새시	1.3 GB	1.3 GB	190MB	11분
ASA 5500-X Series with FTD	1.3 GB	140MB	210MB	25분
FTDv	1.6GB	140MB	210MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	3.2GB	190MB	560MB	25분
ASA FirePOWER	3.4 GB	31MB	480MB	100분
NGIPSv	2.1GB	160MB	400MB	하드웨어에 따라 다름

## 버전 6.2.3.9 시간 및 디스크 공간

표 104: 버전 6.2.3.9 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
FMC	3630MB	190MB	—	35분

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
FMCv	3596MB	172MB	—	하드웨어에 따라 다름
Firepower 2100 Series	1677MB	1677MB	385MB	21분
Firepower 4100/9300 새시	779MB	779MB	184MB	9분
ASA 5500-X Series with FTD	1105MB	130MB	206MB	12분
ISA 3000 with FTD	1071MB	130MB	206MB	25분
FTDv	1094MB	130MB	206MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	2975MB	161MB	538MB	30분
ASA FirePOWER	3211MB	27MB	462MB	38분
NGIPsv	1883MB	146MB	378MB	하드웨어에 따라 다름

## 버전 6.2.3.8 시간 및 디스크 공간

버전 6.2.3.8은 2019년 1월 7일에 Cisco 지원 및 다운로드 사이트에서 제거되었습니다. 이 버전을 사용 중인 경우, 업그레이드하는 것이 좋습니다.

## 버전 6.2.3.7 시간 및 디스크 공간

표 105: 버전 6.2.3.7 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
FMC	2909MB	137MB	—	25분
FMCv	3972MB	211MB	—	하드웨어에 따라 다름
Firepower 2100 Series	1668MB	1668MB	384MB	19분
Firepower 4100/9300 새시	795MB	795MB	183MB	8분
ASA 5500-X Series with FTD	1067MB	130MB	205MB	9분
ISA 3000 with FTD	1080MB	130MB	205MB	20분
FTDv	1146MB	130MB	205MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	3300MB	136MB	477MB	20분

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
ASA FirePOWER	2291MB	26MB	411MB	80분
NGIPSv	1588MB	121MB	327MB	하드웨어에 따라 다름

## 버전 6.2.3.6 시간 및 디스크 공간

표 106: 버전 6.2.3.6 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
FMC	2524MB	47MB	—	30분
FMCv	2315MB	101MB	—	하드웨어에 따라 다름
Firepower 2100 Series	1673MB	1673MB	383MB	10분
Firepower 4100/9300 샐시	790MB	790MB	182MB	17분
ASA 5500-X Series with FTD	1220MB	130MB	205MB	21분
ISA 3000 with FTD	1087MB	130MB	205MB	21분
FTDv	1133MB	130MB	205MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	1196MB	17MB	204MB	30분
ASA FirePOWER	1844MB	16MB	226MB	106분
NGIPSv	364MB	17MB	142MB	하드웨어에 따라 다름

## 버전 6.2.3.5 시간 및 디스크 공간

표 107: 버전 6.2.3.5 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
FMC	1566MB	24MB	—	28분
FMCv	2266MB	80MB	—	하드웨어에 따라 다름
Firepower 2100 Series	1001MB	1001MB	257MB	20분
Firepower 4100/9300 샐시	370MB	370MB	56MB	7분



Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
ASA 5500-X Series with FTD	587MB	130MB	78MB	20분
ISA 3000 with FTD	379MB	130MB	78MB	20분
Firepower 7000/8000 시리즈	806MB	17MB	78MB	22분
ASA FirePOWER	1465MB	15MB	100 MB	70분
NGIPSv	120MB	17MB	16MB	하드웨어에 따라 다름

## 버전 6.2.3.4 시간 및 디스크 공간

표 108: 버전 6.2.3.4 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
FMC	2191MB	107MB	—	80분
FMCv	1760MB	35MB	—	하드웨어에 따라 다름
Firepower 2100 Series	1014MB	1014MB	261MB	17분
Firepower 4100/9300 새시	334MB	334MB	59MB	7분
ASA 5500-X Series with FTD	411MB	128 MB	82MB	20분
ISA 3000 with FTD	393MB	128 MB	82MB	20분
FTDv	411MB	128 MB	82MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	800MB	17MB	82MB	23분
ASA FirePOWER	1385MB	15MB	103MB	25분
NGIPSv	191MB	17MB	20MB	하드웨어에 따라 다름

## 버전 6.2.3.3 시간 및 디스크 공간

표 109: 버전 6.2.3.3 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
FMC	1879MB	88MB	—	26분

Platform(플랫폼)	/Volume에 필요한공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
FMCv	2093MB	90MB	—	하드웨어에 따라 다름
Firepower 2100 Series	987MB	987MB	255MB	15분
Firepower 4100/9300 샐시	313MB	313MB	54MB	5분
ASA 5500-X Series with FTD	553MB	128 MB	77MB	16분
ISA 3000 with FTD	307MB	90MB	77MB	15분
FTDv	307MB	90MB	77MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	825MB	17MB	77MB	15분
ASA FirePOWER	634MB	16MB	98MB	40분
NGIPSv	102MB	17MB	77MB	하드웨어에 따라 다름

## 버전 6.2.3.2 시간 및 디스크 공간

표 110: 버전 6.2.3.2 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
FMC	1743MB	27MB	—	24분
FMCv	1976MB	70MB	—	하드웨어에 따라 다름
Firepower 2100 Series	977MB	977MB	252MB	17분
Firepower 4100/9300 샐시	374MB	374MB	51MB	4분
ASA 5500-X Series with FTD	585MB	126MB	73MB	16분
ISA 3000 with FTD	676MB	126MB	73MB	17분
FTDv	585MB	126MB	73MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	688MB	11MB	76MB	13분
ASA FirePOWER	1440MB	15MB	98MB	40분
NGIPSv	96MB	17MB	14MB	하드웨어에 따라 다름

## 버전 6.2.3.1 시간 및 디스크 공간

표 111: 버전 6.2.3.1 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.3 이상 시간
FMC	1361.8MB	59.67MB	—	25분
FMCv	1240.8MB	40.8MB	—	하드웨어에 따라 다름
Firepower 2100 Series	948.3MB	948.3MB	246MB	81분
Firepower 4100/9300 새시	278MB	278MB	45MB	8분
ASA 5500-X Series with FTD	275.5MB	89.9MB	68MB	16분
ISA 3000 with FTD	343.4MB	127.5MB	68MB	15분
FTDv	275.5MB	89.9MB	67MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	99.8MB	36MB	10MB	19분
ASA FirePOWER	867.9MB	15.45MB	32MB	60분
NGIPSv	101.9MB	17.18MB	9MB	하드웨어에 따라 다름

## 버전 6.2.3 시간 및 디스크 공간

표 112: 버전 6.2.3 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	6.1.0 이상: 7415MB	6.1.0 이상: 17MB	—	6.1.0 이상: 38분
	6.2.0 이상: 8863MB	6.2.0 이상: 24MB		6.2.0 이상: 43분
	6.2.1 이상: 8263MB	6.2.1 이상: 23MB		6.2.1 이상: 37분
	6.2.2 이상: 11860MB	6.2.2 이상: 24MB		6.2.2 이상: 37분
FMCv	6.1.0 이상: 7993MB	6.1.0 이상: 23MB	—	하드웨어에 따라 다름
	6.2.0 이상: 9320MB	6.2.0 이상: 28MB		
	6.2.1 이상: 11571MB	6.2.1 이상: 24MB		
	6.2.2 이상: 11487MB	6.2.2 이상: 24MB		

Platform(플랫폼)	/Volume에 필요한공간	/에 필요한 공간	Space on FMC	시간
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 4100/9300 새시	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 FTD	6.1.0 이상: 4322MB 6.2.0 이상: 6421MB 6.2.2 이상: 6450MB	6.1.0 이상: 0.088MB 6.2.0 이상: 0.092MB 6.2.2 이상: 0.088MB	1000MB	6.1.0 이상: 54분 6.2.0 이상: 53분 6.2.2 이상: 50분
FTDv	6.1.0 이상: 4225MB 6.2.0 이상: 5179MB 6.2.2 이상: 6450MB	6.1.0 이상: 0.076MB 6.2.0 이상: 0.092MB 6.2.2 이상: 0.092MB	1000MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	6.1.0 이상: 5145MB 6.2.0 이상: 5732MB 6.2.2 이상: 6752MB	6.1.0 이상: 18MB 6.2.0 이상: 18MB 6.2.2 이상: 18MB	840MB	6.1.0 이상: 29분 6.2.0 이상: 31분 6.2.2 이상: 31분
ASA FirePOWER	6.1.0 이상: 7286MB 6.2.0 이상: 7286MB 6.2.2 이상: 10748MB	6.1.0 이상: 16MB 6.2.0 이상: 16MB 6.2.2 이상: 16MB	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: 4115MB 6.2.0 이상: 5505MB 6.2.2 이상: 5871MB	6.1.0 이상: 18MB 6.2.0 이상: 19MB 6.2.2 이상: 19MB	741MB	하드웨어에 따라 다름

## 버전 6.2.2.5 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한공간	/에 필요한 공간	Space on FMC	시간
FMC	5271MB	25MB	—	6.2.2 이상: 60분 6.2.2.4 이상: 42분
FMCv	5292MB	33MB	—	하드웨어에 따라 다름

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
Firepower 2100 Series	9113MB	9113MB	2GB	6.2.2 이상: 87분 6.2.2.4 이상: 32분
Firepower 4100/9300 새시	3325MB	3325MB	612MB	6.2.2 이상: 28분 6.2.2.4 이상: 12분
ASA 5500-X series with FTD	3809MB	226MB	724MB	6.2.2 이상: 49분 6.2.2.4 이상: 25분
FTDv	3809MB	226MB	724MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	566MB	28MB	419MB	6.2.2 이상: 54분 6.2.2.4 이상: 12분
ASA FirePOWER	3714MB	28MB	432MB	6.2.2 이상: 215분 6.2.2.4 이상: 105분
NGIPSv	3799MB	24MB	98MB	하드웨어에 따라 다름

## 버전 6.2.2.4 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	4435MB	217MB	—	6.2.2 이상: 85분 6.2.2.3 이상: 42분
FMCv	3691MB	48MB	—	하드웨어에 따라 다름
Firepower 2100 Series	6965MB	6965MB	1GB	6.2.2 이상: 58분 6.2.2.3 이상: 34분
Firepower 4100/9300 새시	1676MB	1676MB	339MB	6.2.2 이상: 24분 6.2.2.3 이상: 13분
ASA 5500-X series with FTD	1695MB	225MB	427MB	6.2.2 이상: 142분 6.2.2.3 이상: 68분
FTDv	1695MB	225MB	427MB	하드웨어에 따라 다름

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
Firepower 7000/8000 시리즈	3343MB	36MB	414MB	6.2.2 이상: 45분 6.2.2.3 이상: 19분
ASA FirePOWER	3192MB	27MB	405MB	6.2.2 이상: 182분 6.2.2.3 이상: 80분
NGIPSv	444MB	28MB	94MB	하드웨어에 따라 다름

## 버전 6.2.2.3 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	3766.6MB	205MB	—	6.2.2 이상: 66분 6.2.2.2 이상: 41분
FMCv	3485MB	17.5MB	—	하드웨어에 따라 다름
Firepower 2100 Series	4486.64MB	4486.64MB	132MB	6.2.2 이상: 61분 6.2.2.2 이상: 36분
Firepower 4100/9300 샤페	811.7MB	811.7MB	132MB	6.2.2 이상: 20분 6.2.2.2 이상: 12분
ASA 5500-X series with FTD	1636.6MB	125.1MB	199MB	6.2.2 이상: 35분 6.2.2.2 이상: 20분
FTDv	1810.7MB	125MB	199MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	2775MB	17MB	339MB	6.2.2 이상: 80분 6.2.2.2 이상: 42분
ASA FirePOWER	2301.5MB	15.69MB	308MB	6.2.2 이상: 184분 6.2.2.2 이상: 100분
NGIPSv	576.3MB	17.5MB	20MB	하드웨어에 따라 다름

## 버전 6.2.2.2 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	1656MB	18MB	—	6.2.2 이상: 34분 6.2.2.1 이상: 27분
FMCv	2356MB	19MB	—	하드웨어에 따라 다름
Firepower 2100 Series	2377MB	2377MB	497MB	6.2.2 이상: 41분 6.2.2.1 이상: 20분
Firepower 4100/9300 새시	561MB	561MB	41MB	6.2.2 이상: 21분 6.2.2.1 이상: 13분
ASA 5500-X series with FTD	984MB	122MB	136MB	6.2.2 이상: 110분 6.2.2.1 이상: 70분
FTDv	984MB	122MB	136MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	1706MB	16MB	310MB	6.2.2 이상: 56분 6.2.2.1 이상: 40분
ASA FirePOWER	1602MB	15MB	190MB	6.2.2 이상: 113분 6.2.2.1 이상: 80분
NGIPSv	170MB	17MB	16MB	하드웨어에 따라 다름

## 버전 6.2.2.1 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.2에서 업데이트하는 시간
FMC	480MB	18MB	—	52분
FMCv	775MB	30MB	—	하드웨어에 따라 다름
Firepower 2100 Series	1003MB	1003MB	47MB	28분
Firepower 4100/9300 새시	299MB	299MB	47MB	35분
ASA 5500-X series with FTD	674MB	121MB	69MB	72분

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.2에서 업데이트하는 시간
FTDv	674MB	121MB	69MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	664MB	14MB	61MB	33분
ASA FirePOWER	758MB	15MB	83MB	90분
NGIPSv	106MB	17MB	10MB	하드웨어에 따라 다름

## 버전 6.2.2 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	6.2.0 이상: 6467MB 6.2.1 이상: 6916MB	6.2.0 이상: 22MB 6.2.1 이상: 21MB	—	6.2.0 이상: 52분 6.2.1 이상: 61분
FMCv	6.2.0 이상: 6987MB 6.2.1 이상: 5975MB	6.2.0 이상: 24MB 6.2.1 이상: 24MB	—	하드웨어에 따라 다름
Firepower 2100 Series	5613MB	5613MB	925MB	57분
Firepower 4100/9300 새시	4635MB	4635MB	743MB	14분
FTDv	3586MB	0.92MB	987MB	하드웨어에 따라 다름
ASA 5500-X series with FTD	3683MB	.16MB	987MB	80분
Firepower 7000/8000 시리즈	6745MB	18MB	1300MB	27분
ASA FirePOWER	7021MB	16MB	1200MB	131분
NGIPSv	7261MB	18MB	1300MB	하드웨어에 따라 다름

## 버전 6.2.0.6 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	8547MB	104MB	—	6.2.0 이상: 97분 6.2.0.5 이상: 36분
FMCv	8543MB	30MB	—	하드웨어에 따라 다름



Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
Firepower 4100/9300 새시	4085MB	4085MB	789MB	6.2.0 이상: 23분 6.2.0.5 이상: 13분
FTDv	4526MB	226MB	918MB	하드웨어에 따라 다름
ASA 5500-X series with FTD	4960MB	227MB	918MB	6.2.0 이상: 56분 6.2.0.5 이상: 27분
Firepower 7000/8000 시리즈	7464MB	29MB	944MB	6.2.0 이상: 60분 6.2.0.5 이상: 24분
ASA FirePOWER	7191MB	28MB	878MB	6.2.0 이상: 75분 6.2.0.5 이상: 49분
NGIPSv	1658MB	29MB	284MB	하드웨어에 따라 다름

## 버전 6.2.0.5 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	6009MB	180MB	—	6.2.0 이상: 72분 6.2.0.4 이상: 34분
FMCv	6943MB	20MB	—	하드웨어에 따라 다름
Firepower 4100/9300 새시	3009MB	3009MB	441MB	6.2.0 이상: 28분 6.2.0.4 이상: 16분
FTDv	2805MB	135MB	548MB	하드웨어에 따라 다름
ASA 5500-X series with FTD	4316MB	135MB	548MB	6.2.0 이상: 46분 6.2.0.4 이상: 22분
Firepower 7000/8000 시리즈	5806MB	18MB	693MB	6.2.0 이상: 51분 6.2.0.4 이상: 18분
ASA FirePOWER	5945MB	16MB	703MB	6.2.0 이상: 66분 6.2.0.4 이상: 27분
NGIPSv	1301MB	18MB	211MB	하드웨어에 따라 다름

## 버전 6.2.0.4 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	5271MB	167MB	—	6.2.0 이상: 84분 6.2.0.3 이상: 50분
FMCv	5346MB	20MB	—	하드웨어에 따라 다름
Firepower 4100/9300 샐시	1828MB	1828MB	325MB	6.2.0 이상: 23분 6.2.0.3 이상: 12분
ASA 5500-X series with FTD	3593MB	134MB	448MB	6.2.0 이상: 2시간 28분 6.2.0.3 이상: 69분
FTDv	275MB	136MB	448MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	4614MB	18MB	608MB	6.2.0 이상: 45분 6.2.0.3 이상: 17분
ASA FirePOWER	4585MB	16MB	597MB	6.2.0 이상: 3시간 34분 6.2.0.3 이상: 83분
NGIPSv	1067MB	18MB	208MB	하드웨어에 따라 다름

## 버전 6.2.0.3 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	3352MB	18MB	—	6.2.0 이상: 75분 6.2.0.2 이상: 37분
FMCv	3342MB	19MB	—	하드웨어에 따라 다름
Firepower 4100/9300 샐시	—	1355MB	319MB	6.2.0 이상: 18분 6.2.0.2 이상: 12분
ASA 5500-X series with FTD	131MB	2302MB	384MB	6.2.0 이상: 118분 6.2.0.2 이상: 76분
FTDv	842MB	17MB	384MB	하드웨어에 따라 다름

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
Firepower 7000/8000 시리즈	3526MB	17MB	554MB	6.2.0 이상: 38분 6.2.0.2 이상: 19분
ASA FirePOWER	15MB	3361MB	521MB	6.2.0 이상: 3시간 6.2.0.2 이상: 97분
NGIPSv	842MB	17MB	202MB	하드웨어에 따라 다름

## 버전 6.2.0.2 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	1665MB	35MB	—	6.2.0 이상: 36분 6.2.0.1 이상: 30분
FMCv	2834MB	21MB	—	하드웨어에 따라 다름
Firepower 4100/9300 새시	1060MB	1060MB	274MB	6.2.0 이상: 12분 6.2.0.1 이상: 9분
ASA 5500-X series with FTD	1808MB	144MB	295MB	6.2.0 이상: 95분 6.2.0.1 이상: 59분
FTDv	998MB	143MB	295MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	2110MB	17MB	458MB	6.2.0 이상: 54분 6.2.0.1 이상: 35분
ASA FirePOWER	2014MB	17MB	383MB	6.2.0 이상: 40분 6.2.0.1 이상: 80분
NGIPSv	612MB	19MB	195MB	하드웨어에 따라 다름

## 버전 6.2.0.1 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.0에서 업데이트하는 시간
FMC	1237MB	50MB	—	28분

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.2.0에서 업데이트하는 시간
FMCv	1488MB	23MB	—	하드웨어에 따라 다름
Firepower 4100/9300 새시	524MB	524MB	137MB	12분
ASA 5500-X series with FTD	945MB	144MB	159MB	62분
FTDv	144MB	10MB	159MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	1134MB	18MB	186MB	22분
ASA FirePOWER	97MB	17MB	206MB	69분
NGIPSv	721MB	19MB	98MB	하드웨어에 따라 다름

## 버전 6.2.0 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	10207MB	17MB	—	57분
FMCv	10207MB	17MB	—	하드웨어에 따라 다름
Firepower 4100/9300 새시	5234MB	5234MB	734MB	21분
ASA 5500-X series with FTD	5213MB	0.096MB	938MB	83분
FTDv	5663MB	1MB	936MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	6129MB	17MB	1200MB	27분
ASA FirePOWER	6619MB	16MB	1100MB	165분
NGIPSv	7028MB	18MB	1300MB	하드웨어에 따라 다름

## 버전 6.1.0.7 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	1941MB	187MB	—	6.1.0 이상: 111분 6.1.0.5 이상: 41분
FMCv	12435MB	218MB	—	하드웨어에 따라 다름

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
Firepower 4100/9300 새시	9881MB	9881MB	1400MB	6.1.0 이상: 43분 6.1.0.5 이상: 13분
ASA 5500-X series with FTD	8846MB	1033MB	1480MB	6.1.0 이상: 251분 6.1.0.5 이상: 75분
FTDv	1339MB	185MB	1480MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	5896MB	33MB	159MB	6.1.0 이상: 39분 6.1.0.5 이상: 25분
ASA FirePOWER	13061MB	45MB	1390MB	6.1.0 이상: 156분 6.1.0.5 이상: 28분
NGIPSv	5477MB	185MB	717MB	하드웨어에 따라 다름

## 버전 6.1.0.6 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	10503MB	215MB	—	6.1.0 이상: 66분 6.1.0.5 이상: 27분
FMCv	1367MB	196MB	—	하드웨어에 따라 다름
Firepower 4100/9300 새시	8140MB	8140MB	1126MB	6.1.0 이상: 270분 6.1.0.5 이상: 75분
ASA 5500-X series with FTD	8540MB	1034MB	1229MB	6.1.0 이상: 40분 6.1.0.5 이상: 15분
FTDv	7414MB	1033MB	1229MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	12725MB	237MB	1434MB	6.1.0 이상: 136분 6.1.0.5 이상: 34분
ASA FirePOWER	11189MB	31MB	1131MB	6.1.0 이상: 257분 6.1.0.5 이상: 60분
NGIPSv	4606MB	196MB	644MB	하드웨어에 따라 다름

## 버전 6.1.0.5 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	7673MB	46MB	—	6.1.0 이상: 56분 6.1.0.4 이상: 28분
FMCv	10790MB	216MB	—	하드웨어에 따라 다름
Firepower 4100/9300 샐시	7680MB	7680MB	1060MB	6.1.0 이상: 30분 6.1.0.4 이상: 10분
ASA 5500-X series with FTD	7952MB	137MB	1141MB	6.1.0 이상: 186분 6.1.0.4 이상: 70분
FTDv	7453MB	1140MB	1141MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	11877MB	259MB	1403MB	6.1.0 이상: 115분 6.1.0.4 이상: 25분
ASA FirePOWER	8955MB	34MB	1217MB	6.1.0 이상: 208분 6.1.0.4 이상: 105분
NGIPSv	4298MB	215MB	640MB	하드웨어에 따라 다름

## 버전 6.1.0.4 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	6739516MB	218808MB	—	6.1.0 이상: 65분 6.1.0.3 이상: 30분
FMCv	675984MB	200748MB	—	하드웨어에 따라 다름
Firepower 4100/9300 샐시	6010092MB	6010092MB	1020MB	6.1.0 이상: 26분 6.1.0.3 이상: 10분
ASA 5500-X series with FTD	6155828MB	1058968MB	1100MB	6.1.0 이상: 49분 6.1.0.3 이상: 20분
FTDv	1059632MB	1059632MB	1100MB	하드웨어에 따라 다름

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
Firepower 7000/8000 시리즈	8713068MB	240940MB	1200MB	6.1.0 이상: 48분 6.1.0.3 이상: 17분
ASA FirePOWER	7442808MB	31740MB	1100MB	6.1.0 이상: 63분 6.1.0.3 이상: 45분
NGIPSv	3367536MB	20120MB	636MB	하드웨어에 따라 다름

## 버전 6.1.0.3 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	5537816MB	218676MB	—	6.1.0 이상: 46분 6.1.0.2 이상: 35분
FMCv	6611148MB	200904MB	—	하드웨어에 따라 다름
Firepower 4100/9300 새시	5014020MB	5014020MB	929MB	6.1.0 이상: 22분 6.1.0.2 이상: 13분
ASA 5500-X series with FTD	1057776MB	1057776MB	1000MB	6.1.0 이상: 40분 6.1.0.2 이상: 23분
FTDv	1059932MB	1059932MB	1000MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	7357340MB	228728MB	1100MB	6.1.0 이상: 43분 6.1.0.2 이상: 25분
ASA FirePOWER	4782384MB	31792MB	1000MB	6.1.0 이상: 160분 6.1.0.2 이상: 80분
NGIPSv	2710540MB	200896MB	635MB	하드웨어에 따라 다름

## 버전 6.1.0.2 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	3872MB	235MB	—	6.1.0 이상: 44분 6.1.0.1 이상: 22분
FMCv	3871MB	219MB	—	하드웨어에 따라 다름
Firepower 4100/9300 샐시	4046MB	4046MB	886MB	6.1.0 이상: 20분 6.1.0.1 이상: 14분
ASA 5500-X series with FTD	2291MB	96MB	918MB	6.1.0 이상: 74분 6.1.0.1 이상: 106
FTDv	2797MB	1137MB	918MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	4130MB	260MB	965MB	6.1.0 이상: 62분 6.1.0.1 이상: 24분
ASA FirePOWER	4549MB	40MB	816MB	6.1.0 이상: 139분 6.1.0.1 이상: 34분
NGIPSv	2710540MB	200896MB	635MB	하드웨어에 따라 다름

## 버전 6.1.0.1 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.1.0에서 업데이트하는 시간
FMC	1893MB	140MB	—	23분
FMCv	2144MB	207MB	—	하드웨어에 따라 다름
Firepower 4100 Series	2580MB	580MB	600MB	15분
Firepower 9300	1877MB	1877MB	600MB	20분
ASA 5500-X series with FTD	1377MB	846MB	600MB	10분
FTDv	1377MB	846MB	600MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	2094MB	156MB	513MB	47분



Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.1.0에서 업데이트하는 시간
ASA FirePOWER	1728MB	34MB	433MB	76분
NGIPSv	793MB	130MB	295MB	하드웨어에 따라 다름

## 버전 6.1.0 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	10722MB	18MB	—	47분
FMCv	10128MB	17MB	—	하드웨어에 따라 다름
ASA 5500-X series with FTD	5213MB	0.096MB	914MB	21분
FTDv	5403MB	0.096MB	914MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	7108MB	61MB	1740MB	39분
ASA FirePOWER	8392MB	47MB	1300MB	59분
NGIPSv	6368MB	54MB	1229MB	하드웨어에 따라 다름

## 버전 6.0.1.4 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	3428MB	201MB	—	6.0.0 이상: 92분 6.0.1.3 이상: 39분
FMCv	3108MB	95MB	—	하드웨어에 따라 다름
Firepower 4100 Series	5237MB	5237MB	1000MB	6.0.0 이상: 30분 6.0.1.3 이상: 18분
Firepower 9300	1360MB	5434MB	1000MB	6.0.0 이상: 26분 6.0.1.3 이상: 14분
ASA 5500-X series with FTD	3416MB	1017MB	1000MB	6.0.0 이상: 26분 6.0.1.3 이상: 14분

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FTDv	3619MB	1020MB	1000MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	7891MB	222MB	1270MB	6.0.0 이상: 47분 6.0.1.3 이상: 23분
ASA FirePOWER	6049MB	45MB	990MB	6.0.0 이상: 95분 6.0.1.3 이상: 43분
NGIPSv	2916MB	192MB	990MB	하드웨어에 따라 다름

## 버전 6.0.1.3 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	2419MB	110MB	—	58분
FMCv	2419MB	101MB	—	하드웨어에 따라 다름
Firepower 4100/9300 새시	2781MB	2781MB	473MB	22분
ASA 5500-X series with FTD	2641MB	813MB	473MB	24분
FTDv	2651MB	813MB	473MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	4757MB	125MB	926MB	55분
ASA FirePOWER	3883MB	58MB	685MB	184분
NGIPSv	1695MB	107MB	430MB	하드웨어에 따라 다름

## 버전 6.0.1.2 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	272MB	54MB	—	7분
FMCv	368MB	54MB	—	하드웨어에 따라 다름
Firepower 4100/9300 새시	2101MB	56MB	302MB	16분
ASA 5500-X series with FTD	740MB	807MB	302MB	13분
FTDv	2101MB	56MB	302MB	하드웨어에 따라 다름

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
Firepower 7000/8000 시리즈	3190MB	63MB	412MB	17분
ASA FirePOWER	2027MB	54MB	577MB	99분
NGIPSv	602MB	56MB	243MB	하드웨어에 따라 다름

## 버전 6.0.1.1 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.0.1에서 업데이트하는 시간
FMC	14MB	54MB	—	23분
FMCv	14MB	54MB	—	하드웨어에 따라 다름
Firepower 4100/9300 새시	54MB	54MB	2MB	6분
ASA 5500-X series with FTD	54MB	54MB	2MB	7분
FTDv	14MB	54MB	2MB	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	944MB	61MB	166MB	39분
ASA FirePOWER	824MB	54MB	84MB	46분
NGIPSv	54MB	56MB	1MB	하드웨어에 따라 다름

## 버전 6.0.1 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	8959MB	18MB	—	66분
FMCv	—	—	—	—
Firepower 7000/8000 시리즈	3683MB	227MB	614MB	30분
ASA FirePOWER	2966MB	54MB	429MB	91분
NGIPSv	2090MB	196MB	3050MB	하드웨어에 따라 다름

## 버전 6.0.0.1 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	6.0에서 업데이트하는 시간
FMC	976MB	120MB	—	25분
FMCv	969MB	119MB	—	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	1568MB	134MB	273MB	25분
ASA FirePOWER	1101MB	56MB	181MB	56분
NGIPSv	929MB	26MB	174MB	하드웨어에 따라 다름

## 버전 6.0 시간 및 디스크 공간

Platform(플랫폼)	/Volume에 필요한 공간	/에 필요한 공간	Space on FMC	시간
FMC	8022MB	16MB	—	58분
FMCv	8022MB	16MB	—	하드웨어에 따라 다름
Firepower 7000/8000 시리즈	6496MB	16MB	1200MB	94분
ASA FirePOWER	7644MB	32MB	1200MB	41분
NGIPSv	6046MB	17MB	102000MB	하드웨어에 따라 다름



# 15 장

## 트래픽 흐름, 검사 및 디바이스 동작

업그레이드 중 트래픽 흐름 및 검사에서 잠재적인 중단을 식별해야 합니다. 다음과 같은 경우 발생할 수 있습니다.

- 디바이스를 재부팅할 때.
- 디바이스에서 운영 체제 또는 가상 호스팅 환경을 업그레이드할 때
- 디바이스에서 Firepower 소프트웨어를 업그레이드하거나 패치를 제거할 때
- 업그레이드 또는 삭제 프로세스의 일부로 구성 변경 사항을 배포할 때(Snort 프로세스가 다시 시작).

디바이스 유형, 구축 유형(독립형, 고가용성, 클러스터) 및 인터페이스 구성(패시브, IPS, 방화벽 등)은 중단의 특성을 결정합니다. Cisco는 유지 보수 기간 또는 중단으로 구축에 가장 적은 영향이 발생할 때 업그레이드 또는 삭제를 수행할 것을 강력하게 권장합니다.

- FTD 업그레이드 동작: Firepower 4100/9300 새시, 241 페이지
- FTD 업그레이드 동작: 기타 장치, 245 페이지
- Firepower 7000/8000 Series 업그레이드 동작, 247 페이지
- ASA FirePOWER 업그레이드 동작, 249 페이지
- NGIPSv 업그레이드 동작, 250 페이지

### FTD 업그레이드 동작: Firepower 4100/9300 새시

이 섹션은 FTD를 사용하는 Firepower 4100/9300 새시를 업그레이드할 때 디바이스 및 트래픽 동작을 설명합니다.

#### Firepower 4100/9300 새시: FXOS 업그레이드

새시 간 클러스터링 또는 고가용성 쌍이 구성되어 있더라도 각 새시에서 FXOS를 독립적으로 업그레이드합니다. 업그레이드를 수행하는 방법에 따라 FXOS 업그레이드 중에 디바이스가 트래픽을 처리하는 방법이 결정됩니다.

표 113: FXOS 업그레이드 중 트래픽 동작

구축	메서드	트래픽 동작
독립형	—	삭제됨
고가용성	모범 사례: 스탠바이 새시에서 FXOS를 업데이트하고 액티브 피어를 전환한 다음 새 스탠바이 새시를 업그레이드합니다.	영향 없음
	스탠바이 새시 업그레이드가 완료되기 전에 액티브 피어에서 FXOS를 업그레이드합니다.	하나의 피어가 온라인 상태가 될 때까지 삭제됨
새시 간 클러스터 (6.2 이상)	모범 사례: 하나 이상의 모듈이 항상 온라인 상태가 되도록 새시를 한 번에 하나씩 업그레이드합니다.	영향 없음
	특정 시점에 모든 새시가 가동 중지되도록 새시를 동시에 업그레이드합니다.	하나 이상의 모듈이 온라인 상태가 될 때까지 삭제됨
새시 내 클러스터 (Firepower 9300에만 해당)	하드웨어 우회 활성화됨: 우회: 스탠바이 또는 우회-강제 (6.1 이상)	검사 없이 통과됨
	하드웨어 우회 비활성화됨: 우회: 비활성화됨 (6.1 이상)	하나 이상의 모듈이 온라인 상태가 될 때까지 삭제됨
	하드웨어 우회 모듈이 없습니다.	하나 이상의 모듈이 온라인 상태가 될 때까지 삭제됨

독립형 FTD 디바이스: Firepower 소프트웨어 업그레이드

Firepower 디바이스/보안 모듈은 업그레이드 중에 유지 보수 모드로 작동합니다. 업그레이드를 시작할 때 유지 보수 모드에 진입하면 트래픽 검사가 2~3초 중단됩니다. 인터페이스 컨피그레이션에 따라 독립형 디바이스가 업그레이드 도중에 트래픽을 처리하는 방법이 결정됩니다.

표 114: Firepower 소프트웨어 업그레이드 중 트래픽 동작: 독립형 FTD 디바이스

인터페이스 컨피그레이션	트래픽 동작
방화벽 인터페이스 라우팅 또는 스위칭 (EtherChannel, 이중화, 하위 인터페이스 포함)  스위칭 인터페이스는 브리지 그룹 또는 투명 모드 인터페이스라고도 합니다.	삭제됨

인터페이스 컨피그레이션		트래픽 동작
IPS 전용 인터페이스	인라인 집합, 하드웨어 우회 강제 활성화됨: 우회: 강제(6.1 이상)	하드웨어 우회를 비활성화하거나 다시 스탠바이 모드로 설정할 때까지 검사 없이 통과됨
	인라인 집합, 하드웨어 우회 스탠바이 모드: 우회: 스탠바이(6.1 이상)	디바이스가 유지 보수 모드에 있는 동안 업그레이드 중 삭제된 다음 디바이스 업그레이드 후 재부팅을 완료하는 동안 검사 없이 통과됨
	인라인 집합, 하드웨어 우회 비활성화됨: 우회: 비활성화됨(6.1 이상)	삭제됨
	인라인 집합, 하드웨어 우회 모듈 없음	삭제됨
	인라인 집합, 탭 모드	즉시 패킷 이그레스, 복사 검사되지 않음
	패시브, ERSPAN 패시브	중단됨, 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. 하나 이상의 데이터 보안 모듈이 먼저 업그레이드된 후에 제어 모듈이 업그레이드됩니다. 보안 모듈은 업그레이드 중에 유지 보수 모드로 작동합니다.

제어 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.



**참고** 버전 6.2.0, 6.2.0.1 또는 6.2.0.2에서 새시 간 클러스터를 업그레이드하면 트래픽 검사 시 각 모듈이 클러스터에서 제거될 때 약 2~3초의 트래픽 중단이 발생합니다.

고가용성 및 클러스터링 무중단 업그레이드 요구 사항

무중단 업그레이드를 수행하려면 다음 추가 요구 사항이 필요합니다.

**플로우 오프로드:** 플로우 오프로드 기능의 버그 수정으로 일부 FXOS 및 FTD 조합은 플로우 오프로드를 지원하지 않습니다. [Cisco FirePOWER 호환성 가이드](#)를 참조하십시오. 고가용성 또는 클러스터링 구축의 무중단 업그레이드를 수행하려면 항상 호환되는 조합이 실행 중인지 확인해야 합니다.

업그레이드 경로에 FXOS를 2.2.2.91, 2.3.1.130 또는 그 이후 버전(FXOS 2.4.1.x, 2.6.1.x 등 포함)으로 업그레이드하는 내용이 포함된 경우 다음 경로를 사용합니다.

1. FTD를 6.2.2.2 이상으로 업그레이드합니다.
2. FXOS를 2.2.2.91, 2.3.1.130 또는 그 이후 버전으로 업그레이드합니다.
3. FTD를 최종 버전으로 업그레이드합니다.

예를 들어 FXOS 2.2.2.17/FTD 6.2.2.0를 사용 중일 때 FXOS 2.6.1/FTD 6.4.0으로 업그레이드하려는 경우 다음을 수행할 수 있습니다.

1. FTD를 6.2.2.5로 업그레이드합니다.
2. FXOS를 2.6.1로 업그레이드합니다.
3. FTD를 6.4.0으로 업그레이드합니다.

**버전 6.1.0 업그레이드:** FTD 고가용성 쌍을 버전 6.1.0으로 무중단 업그레이드하려면 사전 설치 패키지가 필요합니다. 자세한 내용은 [Firepower System 릴리스 노트 버전 6.1.0 사전 설치 패키지](#)를 참조하십시오.

구축 중의 트래픽 동작

업그레이드 프로세스 중에는 컨피그레이션을 여러 번 구축합니다. Snort는 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 구성 가이드](#)의 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 HA/확작성 구성을 비롯해 모든 Firepower 디바이스에서 트래픽 검사가 중단됩니다. 인터페이스 구성에 따라 중단되는 동안 트래픽이 삭제되는지 아니면 검사 없이 통과되는지가 결정됩니다.

표 115: FTD 구축 중 트래픽 동작

인터페이스 컨피그레이션		트래픽 동작
방화벽 인터페이스	라우팅 또는 스위칭(EtherChannel, 이중화, 하위 인터페이스 포함)  스위칭 인터페이스는 브리지 그룹 또는 투명 모드 인터페이스라고도 합니다.	삭제됨



인터페이스 컨피그레이션		트래픽 동작
IPS 전용 인터페이스	인라인 집합, <b>Failsafe</b> 활성화 또는 비활성화됨(6.0.1~6.1)	검사 없이 통과됨 <b>Failsafe</b> 가 비활성화되어 있고 Snort가 중단되지는 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음
	인라인 집합, <b>Snort Fail Open: 중단: 비</b> 활성화됨(6.2 이상)	삭제됨
	인라인 집합, <b>Snort Fail Open: 중단: 활</b> 성화됨(6.2 이상)	검사 없이 통과됨
	인라인 집합, 탭 모드	즉시 패킷 이그레스, 복사 검사되지 않음
	패시브, ERSPAN 패시브	중단됨, 검사되지 않음

## FTD업그레이드 동작: 기타 장치

이 섹션에서는 Firepower 1000/2100 series, ASA 5500-X series, ISA 3000 및 FTDv의 Firepower Threat Defense를 업그레이드할 때의 디바이스 및 트래픽 동작을 설명합니다.

독립형 **FTD** 디바이스: **Firepower** 소프트웨어 업그레이드

Firepower 디바이스는 업그레이드 중에 유지 보수 모드로 작동합니다. 업그레이드를 시작할 때 유지 보수 모드에 진입하면 트래픽 검사가 2~3초 중단됩니다. 인터페이스 구성에 따라 독립형 디바이스가 업그레이드 도중에 트래픽을 처리하는 방법이 결정됩니다.

표 116: **Firepower** 소프트웨어 업그레이드 중 트래픽 동작: 독립형 **FTD** 디바이스

인터페이스 컨피그레이션		트래픽 동작
방화벽 인터페이스	라우팅 또는 스위칭(EtherChannel, 이중화, 하위 인터페이스 포함)  스위칭 인터페이스는 브리지 그룹 또는 투명 모드 인터페이스라고도 합니다.	삭제됨

인터페이스 컨피그레이션		트래픽 동작
IPS 전용 인터페이스	인라인 집합, 하드웨어 우회 강제 활성화됨: 우회: 강제(Firepower 2100 Series, 6.3 이상)	하드웨어 우회를 비활성화하거나 다시 스탠바이 모드로 설정할 때까지 검사 없이 통과됨
	인라인 집합, 하드웨어 우회 스탠바이 모드: 우회: 스탠바이(Firepower 2100 Series, 6.3 이상)	디바이스가 유지 보수 모드에 있는 동안 업그레이드 중에 삭제됨 디바이스 업그레이드 후 재부팅을 완료하는 동안 검사 없이 통과됨
	인라인 집합, 하드웨어 우회 비활성화됨: 우회: 비활성화됨(Firepower 2100 Series, 6.3 이상)	삭제됨
	인라인 집합, 하드웨어 우회 모듈 없음	삭제됨
	인라인 집합, 탭 모드	즉시 패킷 이그레스, 복사 검사되지 않음
	패시브, ERSpan 패시브	중단됨, 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 중인 트래픽 동작**

업그레이드 프로세스 중에는 컨피그레이션을 여러 번 구축합니다. Snort는 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 구성 가이드](#)의 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 HA/확작성 구성을 비롯해 모든 Firepower 디바이스에서 트래픽 검사가 중단됩니다. 인터페이스 구성에 따라 중단되는 동안 트래픽이 삭제되는지 아니면 검사 없이 통과되는지가 결정됩니다.

표 117: FTD 구축 중 트래픽 동작

인터페이스 컨피그레이션	트래픽 동작	
방화벽 인터페이스 라우팅 또는 스위칭(EtherChannel, 이중화, 하위 인터페이스 포함) 스위칭 인터페이스는 브리지 그룹 또는 투명 모드 인터페이스라고도 합니다.	삭제됨	
IPS 전용 인터페이스	인라인 집합, <b>Failsafe</b> 활성화 또는 비활성화됨(6.0.1~6.1)	검사 없이 통과됨 <b>Failsafe</b> 가 비활성화되어 있고 Snort가 중단되지는 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음
	인라인 집합, <b>Snort Fail Open: 중단: 비</b> 활성화됨(6.2 이상)	삭제됨
	인라인 집합, <b>Snort Fail Open: 중단: 활</b> 성화됨(6.2 이상)	검사 없이 통과됨
	인라인 집합, 탭 모드	즉시 패킷 이그레스, 복사 검사되지 않음
	패시브, ERSPAN 패시브	중단됨, 검사되지 않음

## Firepower 7000/8000 Series 업그레이드 동작

다음 섹션에서는 Firepower 7000 및 8000 Series 디바이스를 업그레이드할 때의 디바이스 및 트래픽 동작을 설명합니다.

독립형 **7000/8000 Series: Firepower** 소프트웨어 업그레이드

인터페이스 컨피그레이션에 따라 독립형 디바이스가 업그레이드 중에 트래픽을 처리하는 방법이 결정됩니다.

표 118: 업그레이드 중 트래픽 동작: 독립형 7000/8000 Series

인터페이스 컨피그레이션	트래픽 동작
인라인, 하드웨어 바이패스 활성화됨(바이패스 모드: 바이패스))	검사 없이 통과됨. 단, 다음의 두 시점에서 트래픽이 잠시 중단됨. <ul style="list-style-type: none"> <li>업그레이드 프로세스 시작 시 링크가 끊겼다 연결되었다 하고 네트워크 카드가 하드웨어 바이패스로 전환될 때.</li> <li>업그레이드 완료 후 링크가 끊겼다 연결되었다 하고 네트워크 카드가 바이패스에서 전환될 때. 엔드포인트가 다시 연결되고 디바이스 인터페이스와의 링크가 다시 설정되면 검사가 다시 시작됨.</li> </ul>
인라인, 하드웨어 바이패스 모듈 없음 또는 하드웨어 바이패스 비활성화됨(바이패스 모드: 바이패스 없음))	삭제됨
인라인, 탭 모드	즉시 패킷 이그레스, 복사 검사되지 않음
수동	중단되지 않음, 검사되지 않음
라우팅, 스위칭	삭제됨

**7000/8000 Series** 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 전환: 대기 업그레이드가 먼저 진행됩니다. 디바이스에서 역할을 전환한 후 새 스텐바이 피어가 업그레이드됩니다. 업그레이드가 완료되어도 디바이스 역할은 전환된 상태로 유지됩니다. 액티브/스텐바이 역할을 유지하려면 업그레이드 전에 역할을 수동으로 전환하십시오. 이렇게 하면 업그레이드 프로세스에서 역할을 다시 전환합니다.
- 액세스 제어만: 액티브 업그레이드가 먼저 진행됩니다. 업그레이드가 완료되면 액티브 및 스텐바이 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. Snort는 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 구성 가이드](#)의 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 HA/확작성 구성을 비롯해 모든 Firepower 디바이스에서 트래픽 검사가 중단됩니다. 인터페이스 구성에 따라 중단되는 동안 트래픽이 삭제되는지 아니면 검사 없이 통과되는지가 결정됩니다.

표 119: 구축 중 트래픽 동작: 7000/8000 Sereis

인터페이스 컨피그레이션	트래픽 동작
인라인, <b>Failsafe</b> 활성화 또는 비활성화	검사 없이 통과됨 <b>Failsafe</b> 가 비활성화되어 있고 Snort가 중단되지 않는 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.

표 120: ASA FirePOWER 업그레이드 중 트래픽 동작

트래픽 리디렉션 정책	트래픽 동작
Fail open ( <b>sfr fail-open</b> )	검사 없이 통과됨
Fail closed ( <b>sfr fail-close</b> )	삭제됨
모니터링 전용( <b>sfr {fail-close} {fail-open} monitor-only</b> )	즉시 패킷 이그레스, 복사 검사되지 않음

### ASA FirePOWER 구축 중 트래픽 동작

Snort 프로세스가 재시작되는 동안의 트래픽 동작은 ASA FirePOWER 모듈을 업그레이드할 때와 동일합니다.

업그레이드 프로세스 중에는 컨피그레이션을 여러 번 구축합니다. Snort는 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 구성 가이드](#)의 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. 서비스 정책에 따라 중단되는 동안 트래픽이 삭제되는지 아니면 검사 없이 통과되는지가 결정됩니다.

## NGIPSv 업그레이드 동작

이 섹션에서는 NGIPSv를 업그레이드할 때의 디바이스 및 트래픽 동작을 설명합니다.

### Firepower 소프트웨어 업그레이드

인터페이스 구성은 업그레이드 중 NGIPSv이 트래픽을 처리하는 방법을 결정합니다.

표 121: NGIPSv 업그레이드 중 트래픽 동작

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. Snort는 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 구성 가이드](#)의 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 구성에 따라 중단되는 동안 트래픽이 삭제되는지 아니면 검사 없이 통과되는지가 결정됩니다.

표 122: NGIPSv 구축 중 트래픽 동작

인터페이스 컨피그레이션	트래픽 동작
인라인, <b>Failsafe</b> 활성화 또는 비활성화	검사 없이 통과됨  <b>Failsafe</b> 가 비활성화되어 있고 Snort가 중단되지 않았으나 사용 중인 경우 일부 패킷이 삭제될 수 있음

인터페이스 컨피그레이션	트래픽 동작
인라인, 탭 모드	즉시 패킷 이그레스, 복사 시 Snort 우회
수동	중단되지 않음, 검사되지 않음

