



Firepower Threat Defense 업그레이드: 기타 FTD 디바이스

- 업그레이드 체크리스트: 기타 FTD 디바이스, 1 페이지
- 업그레이드 경로: 기타 FTD 디바이스, 4 페이지
- FTD 소프트웨어 업그레이드: 기타 FTD 디바이스, 5 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.	업그레이드 경로: 기타 FTD 디바이스, 4 페이지
	버전 확인 디바이스의 현재 버전과 대상 버전을 확인합니다. <ul style="list-style-type: none"> • Firepower Threat Defense 소프트웨어 • 가상 호스팅 환경(FTDv) 	Firepower 디바이스

□	작업/확인	세부 사항
	FMC 호환성 확인 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?
	릴리스 노트 읽기 다음을 포함하여 업그레이드에 영향을 줄 수 있는 사항에 특히 주의하면서 릴리스 노트를 확인하십시오. <ul style="list-style-type: none"> • 버전별 업그레이드 지침 및 경고 • 업그레이드에 영향을 미치는 알려진 문제 • 최신/지원 중단 기능 	Firepower 릴리스 노트

업그레이드 전 작업 및 확인

유지 보수 기간이 아닐 때 사전 확인을 수행하여 중단을 최소화합니다.

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

□	작업/확인	세부 사항
	Firepower 소프트웨어 업그레이드 패키지 푸시 업그레이드 패키지를 디바이스에 푸시합니다. 버전 6.2.3 이상이 필요합니다.	FMC 관리 디바이스로 업그레이드 패키지 푸시
	Firepower 소프트웨어 준비도 확인 실행 준비 확인을 실행합니다. 버전 6.1 이상이 필요합니다.	Firepower 소프트웨어 준비도 확인 실행
	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.	Firepower Management Center 구성 가이드
	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
	Maintenance Window 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 및 시간 테스트 및 디스크 공간 요구 사항

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.
	Firepower 소프트웨어 업그레이드 Firepower 소프트웨어를 업그레이드합니다.	FTD 소프트웨어 업그레이드: 기타 FTD 디바이스, 5 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 가능한가?](#)를 참조하십시오.

표 1: 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](#)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](#)을 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](#)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.

