# 버전별 Firepower 소프트웨어 업그레이드 지침

편의상 업그레이드 설명서에는 Cisco Firepower 릴리스 노트와 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

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

표 *1:* 버전 *6.7.0* 최신 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | Firepower 1010 스위치 포트에서 유효하지 않은 VLAN ID로 업그레이드 실패, 2 페이지 | Firepower 1010 | 6.4.0~6.6.x | 6.7.0 이상 |

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

표 *2:* 버전 *6.7.0* 이전에 게시된 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | FMCv 업그레이드에 28GB RAM 필요, 4 페이지 | FMCv | 6.2.3~6.5.0.x | 6.6.0 이상 |
| | FMC 업그레이드 후 일시적으로 사용할 수 없는 이벤트, 5 페이지 | FMC | 6.2.3~6.5.0.x | 6.6.0 이상 |
| | Firepower 1000 Series 디바이스에서 업그레이드 후 전원 껐다 다시 켜기 필요, 7 페이지 | Firepower 1000 Series | 6.4.0.x | 6.5.0 이상 |
| | 새 URL 카테고리 및 평판, 8 페이지 | Any(모든) | 6.2.3~6.4.0.x | 6.5.0 이상 |
| | TLS 암호화 가속 활성화/비활성화 불가, 17 페이지 | Firepower 2100 Series<br>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 **6.2.3~6.5.0**을 실행 중인 경우, 다음 지침을 검토하십시오.

표 *3:* 버전 *6.6.0* 새 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | FMCv 업그레이드에 28GB RAM 필요, 4 페이지 | FMCv | 6.2.3~6.5.0.x | 6.6.0 이상 |
| | FMC 업그레이드 후 일시적으로 사용할 수 없는 이벤트, 5 페이지 | FMC | 6.2.3~6.5.0.x | 6.6.0 이상 |

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

표 *4:* 버전 *6.6.0* 이전에 게시된 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | Firepower 1000 Series 디바이스에서 업그레이드 후 전원 껐다 다시 켜기 필요, 7 페이지 | Firepower 1000 Series | 6.4.0.x | 6.5.0 이상 |
| | 새 URL 카테고리 및 평판, 8 페이지 | Any(모든) | 6.2.3~6.4.0.x | 6.5.0 이상 |
| | TLS 암호화 가속 활성화/비활성화 불가, 17 페이지 | Firepower 2100 Series<br>Firepower 4100/9300 | 6.2.3~6.3.0.x | 6.4.0 이상 |
| | FMC, 7000/8000 Series, NGIPSv에서 준비도 확인이 실패할 수 있음, 21 페이지 | FMC<br>NGIPSv | 6.1.0~6.1.0.6<br>6.2.0~6.2.0.6<br>6.2.1<br>6.2.2~6.2.2.4<br>6.2.3~6.2.3.4 | 6.3.0 이상 |
| | RA VPN 기본 설정 변경이 VPN 트래픽을 차단할 수 있음, 21 페이지 | FMC를 사용하는 FTD | 6.2.0~6.2.3.x | 6.3.0 이상 |
| | 보안 인텔리전스가 애플리케이션 식별 활성화, 22 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, 23 페이지 | Any(모든) | 6.1.0~6.2.3.x | 6.3.0 이상 |
| | 유효하지 않은 침입 변수 집합으로 구축 오류가 발생할 수 있음, 23 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 가이드를 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 *5:* 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.<br>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 | 인스턴스 크기 조정:<br>• c3.xlarge에서 c3.4xlarge로<br>• c3.2.xlarge에서 c3.4xlarge로<br>• c4.xlarge에서 c4.4xlarge로<br>• c4.2xlarge에서 c4.4xlarge로<br>또한 신규 구축을 위한 c5.4xlarge 인스턴스도 제공합니다. | 크기를 조정하기 전에 인스턴스를 중지합니다. 이 작업을 수행하면 인스턴스 저장 볼륨의 데이터가 손실되므로 인스턴스 저장 기반 인스턴스를 먼저 마이그레이션하십시오. 또한 관리 인터페이스에 탄력적 IP 주소가 없는 경우, 해당 공용 IP 주소가 사용됩니다.<br>자세한 내용은 Linux 인스턴스용 AWS 사용 설명서의 인스턴스 유형 변경에 대한 문서를 참조하십시오. |
| Azure | 인스턴스 크기 조정:<br>• Standard_D3_v2 에서 Standard_D4_v2로 | 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.<br>Windows VM 크기 조정에 대한 Azure 설명서에서 지침을 참조하십시오. |

# **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 **6.2.3~6.4.0**을 실행 중인 경우, 다음 지침을 검토하십시오.

표 *6:* 버전 *6.5.0* 새 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | Firepower 1000 Series 디바이스에서 업그레이드 후 전원 껐다 다시 켜기 필요, 7 페이지 | Firepower 1000 Series | 6.4.0.x | 6.5.0 이상 |
| | 버전 6.5.0에 대한 이그레스 최적화 비활성화, 7 페이지 | FTD | 6.2.3~6.4.0.x | 6.5.0 한정 |
| | 새 URL 카테고리 및 평판, 8 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 **6.3.0**을 실행 중인 경우, 다음 지침을 검토하십시오.

표 *7:* 버전 *6.5.0* 이전에 게시된 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | 업데이트 실패: 컨테이너 인스턴스의 디스크 공간 부족, 16 페이지 | Firepower 4100/9300 | 6.3.0~6.4.0.x | 6.3.0.1~6.5.0 |
| | TLS 암호화 가속 활성화/비활성화 불가, 17 페이지 | Firepower 2100 Series<br>Firepower 4100/9300 | 6.2.3~6.3.0.x | 6.4.0 이상 |
| | FMC, 7000/8000 Series, NGIPSv에서 준비도 확인이 실패할 수 있음, 21 페이지 | FMC<br>Firepower 7000/8000 시리즈<br>NGIPSv | 6.1.0~6.1.0.6<br>6.2.0~6.2.0.6<br>6.2.1<br>6.2.2~6.2.2.4<br>6.2.3~6.2.3.4 | 6.3.0 이상 |
| | RA VPN 기본 설정 변경이 VPN 트래픽을 차단할 수 있음, 21 페이지 | FMC를 사용하는 FTD | 6.2.0~6.2.3.x | 6.3.0 이상 |
| | 보안 인텔리전스가 애플리케이션 식별 활성화, 22 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, 23 페이지 | Any(모든) | 6.1.0~6.2.3.x | 6.3.0 이상 |
| | 유효하지 않은 침입 변수 집합으로 구축 오류가 발생할 수 있음, 23 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

CSCvq34340을 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 중단을 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 카테고리와 이름이 변경된 평판을 도입했습니다.카테고리 변경에 대한 자세한 목록은 Cisco Firepower 릴리스 노트, 버전 6.5.0을 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 *URL*의 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 *URL*은 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 ***8:*** 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.<br>• 액세스 제어<br>• SSL<br>• QoS(FMC만)<br>• 상관 관계(FMC만)<br>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. |
| URL 규칙 평판 이름이 변경됩니다. | 업그레이드로 URL 규칙이 수정되어 새 평판 이름을 사용합니다.<br>**1.** 신뢰할 수 없음(이전 높은 위험)<br>**2.** 의심스러운(이전 의심스러운 사이트)<br>**3.** 보통(이전 보안 위험이 있는 일반 사이트)<br>**4.** 양호(이전 일반 사이트)<br>**5.** 신뢰(이전 알려진) |
| 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 ***9:*** 사전 업그레이드 작업

| 작업 | 세부 사항 |
|---|---|
| 어플라이언스가 Talos 리소스에 연결할 수 있는지 확인합니다. | 시스템 업그레이드 후 다음 Cisco 리소스와 통신할 수 있어야 합니다.<br>• https://regsvc.sco.cisco.com/ — 등록<br>• https://est.sco.cisco.com/ — 보안 통신 인증서 획득<br>• https://updates-talos.sco.cisco.com/ — 클라이언트/서버 매니페스트 획득<br>• http://updates.ironport.com/ — 데이터베이스 다운로드(참고: 포트 80 사용)<br>• https://v3.sds.cisco.com/ — 클라우드 쿼리<br>클라우드 쿼리 서비스는 다음 IP 주소 블록을 사용합니다.<br>• IPv4 클라우드 쿼리:<br>• 146.112.62.0/24<br>• 146.112.63.0/24<br>• 146.112.255.0/24<br>• 146.112.59.0/24<br>• IPv6 클라우드 쿼리:<br>• 2a04: e4c7: ffff::/48<br>• 2a04: e4c7: fffe::/48 |
| 잠재적인 규칙 문제를 식별합니다. | 예정된 변경 사항을 이해합니다. 현재 URL 필터링 구성을 검사하고 업그레이드 후 작업을 수행해야 하는지 결정합니다(다음 섹션 참조).<br>참고 이제 사용되지 않는 카테고리를 사용하는 URL 규칙을 수정할 수 있습니다. 그렇지 않으면 이를 사용하는 규칙은 업그레이드 후 배포를 방지합니다.<br>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 **Policies(**정책**)** > **Access Control(**액세스 제어**)** 을 선택하고 적절한 정책 옆의 보고서 아이콘 ( )을 클릭합니다. |

# 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 ***10:*** 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.<br>FMC에서는 이러한 규칙이 표시됩니다. |
| 새 카테고리를 포함하도록 규칙을 만들거나 수정합니다. | 대부분의 새 카테고리는 위협을 식별합니다. 사용을 강력하게 권장합니다.<br>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 병합된 URL 카테고리가 있는 규칙 지침, 12 페이지를 참조하십시오.<br>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 영향 받는 규칙을 수정할 수 있습니다.<br>이러한 변경 내용은 표시되지 않습니다. |
| 이름이 변경되었거나 변경되지 않은 카테고리를 파악합니다. | 아무 작업도 필요하지 않지만 변경 사항에 대해 알고 있어야 합니다.<br>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.<br>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 ***11:*** 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 | 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.<br>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 해결하하는 방법은 규칙 순서, 규칙과 관련된 작업 및 평판 수준, 규칙을 포함한 다른 URL 카테고리, 규칙에 포함된 비 URL 조건에 따라 달라집니다. |
| 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 | 병합 후 다른 규칙은 다른 작업 및 평판 수준에 연관된 동일한 카테고리를 포함할 수 있습니다.<br>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.<br>FMC에서는 동일한 카테고리 및 평판이 있는 규칙에 경고가 표시됩니다. 그러나 이러한 경고는 평판이 다른 동일한 카테고리를 포함한 규칙을 표시하지는 않습니다.<br>주의: 중복 또는 중복 카테고리 해결 방법을 결정할 때는 규칙의 모든 조건을 고려합니다. |
| 규칙의 기타 URL 카테고리 | 병합된 URL이 있는 규칙은 다른 URL 카테고리도 포함할 수 있습니다. 따라서 병합 후 특정 카테고리가 중복되는 경우 해당 규칙을 삭제하는 대신 수정할 수 있습니다. |
| 규칙의 비 URL 조건 | 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. |

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

표 ***12:*** 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 | 규칙 1에는 카테고리 A가 있습니다.<br>규칙 2에는 카테고리 B가 있습니다. | 규칙 1에는 카테고리 AB가 있습니다.<br>규칙 2에는 카테고리 AB가 있습니다.<br>구체적인 결과는 목록의 규칙 순서, 평판 수준 및 관련 작업에 따라 다릅니다. 중복을 해결하는 방법을 결정할 때 규칙의 다른 모든 조건을 고려해야 합니다. |

| 시나리오 | 업그레이드 전 | 업그레이드 후 |
|---|---|---|
| 다른 동작이 있는 다른 규칙의 병합된 카테고리<br>(평판은 동일합니다) | 규칙 1에는 허용으로 설정된 카테고리 A가 있습니다.<br>규칙 2에는 차단으로 설정된 카테고리 B가 있습니다.<br>(평판은 동일합니다) | 규칙 1에는 허용으로 설정된 카테고리 AB가 있습니다.<br>규칙 2에는 차단으로 설정된 카테고리 AB가 있습니다.<br>규칙 1은 이 카테고리의 모든 트래픽과 일치합니다.<br>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.<br>모든 평판과 관련된 카테고리 A<br>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.<br>규칙 2에는 평판 1~3과 관련된 카테고리 B가 포함됩니다. | 규칙 1에는 평판이 있는 카테고리 AB가 포함됩니다.<br>규칙 2에는 평판 1~3과 관련된 카테고리 AB가 포함됩니다.<br>규칙 1은 이 카테고리의 모든 트래픽과 일치합니다.<br>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 **6.1.0~6.3.0**을 실행 중인 경우, 다음 지침을 검토하십시오.

표 ***13:*** 버전 ***6.4.0*** 새 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | Firepower 1010 디바이스의 EtherChannel은 이그레스 트래픽 블랙홀이 가능합니다., 16 페이지 | Firepower 1010 | 6.4.0 | 6.4.0.3~6.4.0.5 |
| | 업데이트 실패: 컨테이너 인스턴스의 디스크 공간 부족, 16 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 6.2.3.12인 NGIPS 디바이스, 16 페이지 | Firepower 7000/8000 시리즈<br>ASA FirePOWER<br>NGIPSv | 6.2.3~6.3.0.x | 6.4.0 한정 |
| | TLS 암호화 가속 활성화/비활성화 불가, 17 페이지 | Firepower 2100 Series<br>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 **6.1.0~6.2.3**을 실행 중인 경우, 다음 지침을 검토하십시오.

표 ***14:*** 버전 ***6.4.0*** 이전에 게시된 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | FMC, 7000/8000 Series, NGIPSv에서 준비도 확인이 실패할 수 있음, 21 페이지 | FMC<br>Firepower 7000/8000 시리즈<br>NGIPSv | 6.1.0~6.1.0.6<br>6.2.0~6.2.0.6<br>6.2.1<br>6.2.2~6.2.2.4<br>6.2.3~6.2.3.4 | 6.3.0 이상 |
| | RA VPN 기본 설정 변경이 VPN 트래픽을 차단할 수 있음, 21 페이지 | FMC를 사용하는 FTD | 6.2.0~6.2.3.x | 6.3.0 이상 |
| | 보안 인텔리전스가 애플리케이션 식별 활성화, 22 페이지 | FMC 구축 | 6.1.0~6.2.3.x | 6.3.0 이상 |
| | 업그레이드 후 CIP 탐지를 활성화하기 위해 VDB 업데이트, 23 페이지 | Any(모든) | 6.1.0~6.2.3.x | 6.3.0 이상 |
| | 유효하지 않은 침입 변수 집합으로 구축 오류가 발생할 수 있음, 23 페이지 | Any(모든) | 6.1.0~6.2.3.x | 6.3.0 이상 |
| | 보고서의 결과 제한 변경, 26 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, 27 페이지 | FTD 클러스터 | 6.1.0.x | 6.2.3~6.4.0 |
| | 액세스 제어는 SRU에서 지연 기반 성능 설정을 가져올 수 있습니다., 29 페이지 | FMC | 6.1.0.x | 6.2.0~6.4.0 |

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | 'Snort Fail Open'이 FTD의 'Failsafe'를 대체합니다. , 30 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 섀시

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 *6.4.0*으로 업그레이드*:* Firepower 4100/9300 섀시의 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 섀시의 다중 인스턴스 기능을 사용하는 경우 FXOS CLI를 사용하여 Firepower 4100/9300 섀시의 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 **6.1.0~6.2.3**을 실행 중인 경우, 다음 지침을 검토하십시오.

표 *15:* 버전 *6.3.0* 새 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | 업그레이드 및 설치 패키지 이름 변경됨, 19 페이지 | FMC<br>Firepower 7000/8000 시리즈<br>NGIPSv | Any(모든) | 6.3.0 이상 |

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | 버전 6.3 이상으로 이미지를 재설치하면 대부분의 어플라이언스에서 LOM 비활성화, 20 페이지 | FMC(물리적)<br>Firepower 7000/8000 시리즈 | Any(모든) | 6.3.0 이상 |
| | FMC, 7000/8000 Series, NGIPSv에서 준비도 확인이 실패할 수 있음, 21 페이지 | FMC<br>Firepower 7000/8000 시리즈<br>NGIPSv | 6.2.3~6.2.3.4<br>6.2.2~6.2.2.4<br>6.2.1<br>6.2.0~6.2.0.6<br>6.1.0~6.1.0.6 | 6.3.0 이상 |
| | RA VPN 기본 설정 변경이 VPN 트래픽을 차단할 수 있음, 21 페이지 | FMC를 사용하는 FTD | 6.2.0~6.2.3.x | 6.3.0 이상 |
| | 업그레이드 시 TLS/SSL 하드웨어 가속 활성화, 22 페이지 | Firepower 2100 Series<br>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, 22 페이지 | FMC<br>ASDM을 사용하는 ASA FirePOWER | 6.1.0~6.2.3.x | 6.3.0 한정 |
| | 보안 인텔리전스가 애플리케이션 식별 활성화, 22 페이지 | FMC 구축 | 6.1.0~6.2.3.x | 6.3.0 이상 |
| | 업그레이드 후 CIP 탐지를 활성화하기 위해 VDB 업데이트, 23 페이지 | Any(모든) | 6.1.0~6.2.3.x | 6.3.0 이상 |
| | 유효하지 않은 침입 변수 집합으로 구축 오류가 발생할 수 있음, 23 페이지 | Any(모든) | 6.1.0~6.2.3.x | 6.3.0 이상 |
| | Firepower 4100/9300에서 FXOS 업그레이드 전 FTD 푸시 필요, 24 페이지 | Firepower 4100/9300 | 6.1.0.x | 6.3.0 한정 |

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

표 ***16:*** 버전 ***6.3.0*** 이전에 게시된 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | 보고서의 결과 제한 변경, 26 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, 27 페이지 | FTD 클러스터 | 6.1.0.x | 6.2.3~6.4.0 |
| | 액세스 제어는 SRU에서 지연 기반 성능 설정을 가져올 수 있습니다., 29 페이지 | FMC | 6.1.0.x | 6.2.0~6.4.0 |
| | 'Snort Fail Open'이 FTD의 'Failsafe'를 대체합니다. , 30 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 ***17:*** 명명 체계*:* 업그레이드*,* 패치 및 핫픽스 패키지

| 플랫폼 | 명명 체계 |
|---|---|
| FMC | 신규**:** Cisco_Firepower_Mgmt_Center<br>기존**:** Sourcefire_3D_Defense_Center_S3 |
| Firepower 7000/8000 시리즈 | 신규**:** Cisco_Firepower_NGIPS_Appliance<br>기존**:** Sourcefire_3D_Device_S3 |
| NGIPSv | 신규**:** Cisco_Firepower_NGIPS_Virtual<br>기존**:** Sourcefire_3D_Device_VMware<br>기존**:** Sourcefire_3D_Device_Virtual64_VMware |

표 ***18:*** 명명 체계*;* 설치 패키지

| 플랫폼 | 명명 체계 |
|---|---|
| FMC (물리적) | 신규**:** Cisco_Firepower_Mgmt_Center<br>기존**:** Sourcefire_Defense_Center_M4<br>기존**:** Sourcefire_Defense_Center_S3 |
| FMCv: VMware | 신규**:** Cisco_Firepower_Mgmt_Center_Virtual_VMware<br>기존**:** Cisco_Firepower_Management_Center_Virtual_VMware |
| FMCv: KVM | 신규**:** Cisco_Firepower_Mgmt_Center_Virtual_KVM<br>기존**:** Cisco_Firepower_Management_Center_Virtual |
| Firepower 7000/8000 시리즈 | 신규**:** Cisco_Firepower_NGIPS_Appliance<br>기존**:** Sourcefire_3D_Device_S3 |
| NGIPSv | 신규**:** Cisco_Firepower_NGIPSv_VMware<br>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 ***19: LOM*** 설정에 영향을 주는 이미지 재설치

| 플랫폼 | 버전 **6.2.3** 또는 이전으로 이미지 재설치 | 버전 **6.3** 이상으로 이미지 재설치 |
|---|---|---|
| MC1600, 2600, 4600<br>MC1000, 2500, 4500<br>MC2000, 4000 | 항상 유지 | 항상 삭제 |

| 플랫폼 | 버전 **6.2.3** 또는 이전으로 이미지 재설치 | 버전 **6.3** 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 ***20:*** 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 기본값은 **no sysopt connection permit-vpn**입니다.

  이 방법은 외부 사용자가 원격 액세스 VPN 주소 풀에서 IP 주소를 스푸핑할 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 섀시

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 섀시에서 기본적으로 비활성화되었고, Firepower 2100 Series 디바이스에서 사용할 수 없었습니다.

트래픽을 암호 해독하지 않는 매니지드 디바이스에서 TLS/SSL 하드웨어 가속를 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 CSCvn62123를 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<br>제외: 10.1.0.0/16 | 포함: 10.1.0.0/16<br>제외: 172.16.0.0/12<br>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 **6.1.0~6.2.2**를 실행 중인 경우, 다음 지침을 검토하십시오.

표 *21:* 버전 *6.2.3* 새 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | Cisco와 데이터 공유, 25 페이지 | Any(모든) | Any(모든) | 6.2.3 이상 |
| | 업그레이드 후 액세스 컨트롤 정책 수정/다시 저장, 26 페이지 | Any(모든) | 6.1.0~6.2.2.x | 6.2.3 한정 |
| | 보고서의 결과 제한 변경, 26 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, 27 페이지 | FTD 클러스터 | 6.1.0.x | 6.2.3~6.4.0 |

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

표 *22:* 버전 *6.2.3* 이전에 게시된 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | 액세스 제어는 SRU에서 지연 기반 성능 설정을 가져올 수 있습니다., 29 페이지 | FMC | 6.1.0.x | 6.2.0~6.4.0 |
| | 'Snort Fail Open'이 FTD의 'Failsafe'를 대체합니다. , 30 페이지 | 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 ***23:*** 보고서에 새 결과 제한

| 보고서 섹션 유형 | 최대 레코드 수: **HTML/CSV** 보고서 섹션 | 최대 레코드 수: **PDF** 보고서 섹션 |
|---|---|---|
| 막대 그래프<br>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 2.1.1.에 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 가이드를 참조합니다.

# 버전 6.2.2 지침

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

표 *24:* 버전 *6.2.2* 새 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | 보안 강화: 서명된 업그레이드 패키지, 28 페이지 | Any(모든) | Any(모든) | 6.2.2 이상 |
| | 8000 Series 보안 인증서 및 컴플라이언스는 버전 6.2.2.1 이상이 필요합니다., 28 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 활성화하면 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 **6.1.0**을 실행 중인 경우, 다음 지침을 검토하십시오.

표 ***25:*** 버전 ***6.2.0*** 새 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | 액세스 제어는 SRU에서 지연 기반 성능 설정을 가져올 수 있습니다., 29 페이지 | FMC | 6.1.0.x | 6.2.0~6.4.0 |
| | 'Snort Fail Open'이 FTD의 'Failsafe'를 대체합니다. , 30 페이지 | FMC를 사용하는 FTD | 6.1.0.x | 6.2.0~6.4.0 |
| | 업그레이드 시 IAB '모든 애플리케이션' 옵션 삭제, 30 페이지 | FMC<br>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 , 31 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

- 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 **FTD**의 **'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 ***26: Failsafe***를 ***Snort Fail Open***으로 마이그레이션

| 버전 **6.1 Failsafe** | 버전 **6.2 Snort Fail Open** | 행동 |
|---|---|---|
| 비활성화됨(기본 동작) | 사용 중: 비활성<br>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<br>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 카테고리와 평판이 존재하지만 디바이스에 상위 사이트의 데이터만 있는 경우 문제가 발생할 수 있습니다.

버전 6.1.0.3에서는 상위 사이트의 URL 카테고리와 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 가이드를 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 설치를 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 적격한 DC750 또는 DC1500에서 버전 6.0을 실행할 수 있는 고객에게 무료로 메모리 업그레이드 키트를 제공합니다.

- 키트 주문 방법은 필드 알림: FN - 64077 - Cisco FireSIGHT 및 Sourcefire Defense Center Management Appliance - FirePOWER 소프트웨어 V6.0 이상에 필요한 메모리 업그레이드를 참조하십시오.
- 메모리 업그레이드 - *Firepower Management Center* 설치 설명서의 Firepower Management Center용 메모리 업그레이드 지침을 참조하십시오.

### Defense Center 고가용성 쌍 해제

버전 6.0.x에서는 Firepower Management Center의 고가용성을 지원하지 않습니다.

Defense Center의 버전 5.4.x 고가용성 쌍을 Firepower Management Center의 버전 6.0 고가용성 쌍으로 업그레이드할 수는 없습니다. 그러므로 고가용성 쌍을 해제한 후 각 Defense Center를 개별적으로 업그레이드해야 합니다. 버전 6.1에서 고가용성을 다시 설정할 수 있습니다.

### "Retry URL Cache Miss Lookup(URL 캐시 누락 조회 재시도)" 옵션 비활성화

버전 5.4.0.6, 버전 5.4.1.5 이하를 실행 중인 디바이스를 관리하는 경우 Firepower Management Center를 버전 6.0으로 업그레이드하면 트래픽 중단 및 시스템 문제가 발생할 수 있습니다.

Defense Center를 업그레이드하기 전에 **Retry URL cache miss lookup(URL 캐시 누락 조회 재시도)** 옵션을 비활성화해야 합니다. 이 옵션은 디바이스에 구축된 액세스 컨트롤 정책의 Advanced(고급) 탭에서 설정할 수 있습니다. 그런 다음, 디바이스를 재구축합니다. 매니지드 디바이스를 버전 5.4.0.7 이상이나 버전 5.4.1.6 이상 또는 버전 6.0으로 업그레이드한 후 옵션을 다시 활성화할 수 있습니다.

### Defense Center HTTPS 인증서 업데이트

다음의 HTTPS 인증서 중 하나를 사용 중인 버전 5.4.x Defense Center를 버전 6.0 Firepower Management Center로 업그레이드하는 경우 로그인할 수 없으며 Cisco TAC에 문의해야 합니다.

- RSASSA-PSS 서명 알고리즘으로 생성된 인증서.

  업그레이드 전에 sha1WithRSAEncryption 알고리즘 또는 sha256WithRSAEncryption 알고리즘으로 생성된 인증서나 Defense Center 기본 인증서로 교체합니다. 재부팅합니다.

- 2048비트가 넘는 공용 서버 키를 사용하여 생성된 인증서.

  업그레이드 전에 CSR(서버 인증서 요청)로 생성된 인증서로 교체합니다. 재부팅합니다.

또한 업그레이드 후에는 이러한 유형의 인증서를 업로드하지 마십시오. 버전 5.4.x 어플라이언스에서 인증서를 생성하려면 *FireSIGHT System* 사용 설명서, 버전 5.4.1의 맞춤형 HTTPS 인증서 사용을 참조하십시오.

프라이빗 **AMP** 클라우드 미지원

버전 6.0에서는 프라이빗 AMP 클라우드의 Firepower용 AMP 서명 조회 기능이 지원되지 않습니다. 버전 6.0에서는 시스템이 퍼블릭 AMP 클라우드로 SHA-256 서명을 자동으로 제출합니다. 프라이빗 AMP 클라우드를 사용 중이며 엔드포인트로부터 이벤트를 수신하는 경우 컨피그레이션을 추가로 변경하지 않아도 버전 6.0 Defense Center가 해당 이벤트를 계속 수신할 수 있습니다.

# 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 ***27:*** 버전 ***6.6.x.x*** 가이드라인

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | FDM을 사용하는 버전 6.6.0.1 FTD 업그레이드에서 HA 일시 중단, 35 페이지 | FDM을 사용하는 FTD | 6.6.0 | 6.6.0.1 |

### **FDM**을 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 가이드를 참조하십시오.

# 버전 6.4.0.x 지침

이 체크리스트에는 버전 6.4.0 패치에 대한 업그레이드 지침이 포함되어 있습니다.

표 *28:* 버전 *6.4.0.x* 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | 업데이트 실패: 컨테이너 인스턴스의 디스크 공간 부족, 16 페이지 | Firepower 4100/9300 | 6.4.0.x | 이후 패치<br>6.5.0 |
| | Firepower 1010 디바이스의 EtherChannel은 이그레스 트래픽 블랙홀이 가능합니다., 16 페이지 | Firepower 1010 | 6.4.0 한정 | 6.4.0.3~6.4.0.5 |
| | 버전 6.4.0.9~6.4.0.11로 업그레이드하기 전에 이전 Firepower 7000/8000 디바이스를 버전 6.4.0으로 이미지 재설치, 36 페이지 | 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 *29:* 버전 *6.3.0.x* 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | 업데이트 실패: 컨테이너 인스턴스의 디스크 공간 부족, 16 페이지 | Firepower 4100/9300 | 6.3.0.x | 이후 패치<br>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 *30:* 버전 *6.2.3.x* 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | CC 모드를 사용하는 버전 6.2.3.10 FTD 업그레이드의 FSIC 오류, 37 페이지 | FTD | 6.2.3~6.2.3.9 | 6.2.3.10 한정 |
| | 버전 6.2.3.3 FTD 디바이스는 로컬 관리로 전환할 수 없습니다., 38 페이지 | FMC를 사용하는 FTD | 6.2.3~6.2.3.2 | 6.2.3.3 |
| | 버전 6.2.3-88 FMC 업그레이드 전 핫픽스, 38 페이지 | 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

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 T를 설치합니다.

# 버전 6.2.2.x 지침

이 체크리스트에는 버전 6.2.2 패치에 대한 업그레이드 지침이 포함되어 있습니다.

표 31: 버전 6.2.2.x 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | Firepower 2100 Series HA 쌍 버전 6.2.2가 6.2.2.4로 업그레이드 불가, 39 페이지 | 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 32: 버전 6.2.0.x 지침

| ☐ | 지침 | 플랫폼 | 업그레이드 대상 | 직접 업그레이드 |
|---|---|---|---|---|
| | 버전 6.2.0.3 FMC에 핫픽스 BH 적용, 39 페이지 | 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 노트를 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 ***33:*** 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. |