paloalto TECHDOCS

PAN-OS 업그레이드 가이드

11.0

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

March 29, 2023

Table of Contents

소프트웨어 및 콘텐츠 업데이트

PAN-OS는 Palo Alto Networks의 모든 차세대 방화벽을 실행하는 소프트웨어입니다. Palo Alto Networks는 또한 방화벽에 최신 보안 기능을 제공하기 위한 업데이트를 자주 게시합니다. 방화벽은 방화벽 구성을 업데이트할 필요 없이 콘텐츠 업데이트가 제공하는 애플리케이션 및 위협 서명(및 그 이상)을 기반으로 정책을 시행할 수 있습니다.

물리적 방화벽에 PAN-OS 소프트웨어 업데이트를 성공적으로 다운로드하고 설치한 후 PAN-OS 소프트웨어 무결성을 보장하기 위해 소프트웨어 설치 프로세스의 일부로 물리적 방화벽이 재부팅된 후 소프트웨어 업데이트가 검증됩니다. 이렇게 하면 새로 실행 중인 소프트웨어 업데이트가 양호한 것으로 알려지고 방화벽이 원격 또는 물리적 악용으로 인해 손상되지 않도록 합니다.

PAN-OS 소프트웨어 업데이트

PAN-OS는 Palo Alto Networks의 모든 차세대 방화벽을 실행하는 소프트웨어입니다. 방화벽이 실행 중인 PAN-OS 소프트웨어 버전은 방화벽 대시보드에 표시됩니다.

새로운 PAN-OS 릴리스는 방화벽이나 Palo Alto Networks 지원 포털에서 직접 확인할 수 있습니다. 방화벽을 최신 버전의 PAN-OS로 업그레이드하려면:

STEP 1 | 최신 PAN-OS 릴리스 노트를 검토하여 새로운 기능을 확인합니다. 또한, 다운그레이드 고려 사항을(를) 살펴보고 PAN-OS 릴리스가 도입할 수 있는 모든 잠재적 변경 사항을 이해했는지 확인합니다.

STEP 2 | 새로운 PAN-OS 릴리스 확인:

- 지원 포털—support.paloaltonetworks.com으로 이동하고 왼쪽 메뉴 모음에서 업데이트 > 소프트웨어 업데이트를 선택합니다. 방화벽을 업그레이드하는 데 사용할 릴리스를 다운로드하고 저장합니다.
- 방화벽에서—새로운 PAN-OS 릴리스 버전에 대해 Palo Alto Networks 업데이트 서버에서 방화벽을 확인하려면 기기 > 소프트웨어 및 지금 확인을 선택합니다.

소프트웨어 업데이트를 확인하는 데 어려움이 있습니까? 일반적인 연결 문제에 대한 해결 방법은 이 문서를 참조하십시오.

STEP 3 | 원하는 릴리스 버전을 결정한 후 전체 워크플로를 따라 방화벽을 PAN-OS 11.0으로 업그레이드을(를) 수행합니다. 수행할 단계는 현재 실행 중인 릴리스 버전, HA를 사용하는 경우, Panorama를 사용하여 방화벽을 관리하는지 여부에 따라 달라질 수 있습니다.

동적 콘텐츠 업데이트

Palo Alto Networks는 PAN-OS 소프트웨어를 업그레이드하거나 방화벽 구성을 변경할 필요 없이 방화벽이 보안 정책을 시행하는 데 사용할 수 있는 업데이트를 자주 게시합니다. 이러한 업데이트는 방화벽에 최신 보안 기능과 위협 인텔리전스를 제공합니다.

모든 방화벽에서 수신할 수 있는 애플리케이션 업데이트 및 일부 바이러스 백신 업데이트를 제외하고 사용 가능한 동적 콘텐츠 업데이트는 구독에 따라 달라질 수 있습니다. 각 동적 콘텐츠 업데이트에 대한 일정을 설정하여 방화벽이 새 업데이트(디바이스 > 동적 업데이트)를 확인하고 다운로드하거나 설치하는 빈도를 정의할 수 있습니다.

동적 콘텐츠 업데이트	이 패키지에는 무엇이 포함되어 있나요?
바이러스 백신	바이러스 백신 업데이트는 24시간마다 릴리스되며 • 새로 발견된 맬웨어에 대한 WildFire 서명을 포함합니다. 이러한 업데이트를 매일 한 번이 아니라 5분마다 받으려면 WildFire 구독이 필요합니다. • (위협 예방 필요) C2 트래픽에서 특정 패턴을 감지하는 자동 생성 명령 및 제어(C2) 서명. 이러한 서명을 통해 방화벽은 C2 호스트를 알 수 없거나 빠르게 변경되는 경우에도 C2 활동을 감지할 수 있습니다. • (위협 예방 필요) 포함된 외부 동적 목록에 대한 신규 및 업데이트된 목록 항목입니다. 이러한 목록에는 악성, 고위험 및 방탄 호스트 제공 IP 주소가 포함되며 악성 호스트로부터 사용자를 보호하는 데 도움이 될 수 있습니다. • (위협 예방 필요) 방화벽이 알려진 악성 도메인을 식별하는 데 사용하는 DNS 서명의 로컬 집합에 대한 업데이트입니다. DNS 싱크홀링을 설정한 경우 방화벽은 네트워크에서 이러한 도메인에 연결을 시도하는 호스트를 식별할 수 있습니다. 방화벽이 DNS 서명의 전체 데이터베이스에 대해 도메인을 확인하도록 허용하려면 DNS 보안을 설정합니다.
애플리케이션	애플리케이션 업데이트는 신규 및 수정된 애플리케이션 서명 또는 앱 ID를 제공합니다. 이 업데이트에는 추가 구독이 필요하지 않지만 유효한 유지 관리/지원 계약이 필요합니다. 새로운 애플리케이션 업데이트는 매월 세 번째 화요일에만 게시되어 필요한 정책 업데이트를 미리 준비할 수 있는 시간을 제공합니다. 드문 경우지만 새 *App-ID*가 포함된 업데이트의 게시가 하루 또는 이틀 지연될 수 있습니다. App-ID에 대한 수정 사항이 더 자주 릴리스됩니다. 신규 및 수정된 App-ID를 사용하면 방화벽이 보안 정책을 더욱 정확하게 시행할 수 있으므로 보안 정책 시행이 변경되어 애플리케이션 가용성에 영향을 미칠 수 있습니다. 애플리케이션 업데이트를 최대한 활용하려면 신규 및 수정된 앱 ID 관리에 대한 도움말을 따르십시오.

동적 콘텐츠 업데이트	이 패키지에는 무엇이 포함되어 있나요?
애플리케이션 및 위협	신규 및 업데이트된 애플리케이션과 위협 서명이 포함됩니다. 이 업데이트는 Threat Prevention 구독이 있는 경우 사용할 수 있습니다(이 경우 애플리케이션 업데이트 대신 이 업데이트를 받게 됩니다). 새로운 위협 업데이트는 업데이트된 App-ID와 함께 잦은 빈도로(때로는 일주일에 여러 번) 게시됩니다. 새 App-ID는 매월 세 번째 화요일에만 게시됩니다. 드문 경우지만 새 *App-ID*가 포함된 업데이트의 게시가 하루 또는 이틀 지연될 수 있습니다. 방화벽은 가용성이 확보된 후 30분 이내에 최신 위협 및 애플리케이션 업데이트를 검색할 수 있습니다. 애플리케이션 가용성과 최신 위협으로부터의 보호를 모두 보장하기 위해 애플리케이션 및 위협 업데이트를 가장 잘 활성화하는 방법에 대한 지침은 애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례을(를) 검토합니다.
디바이스 사전	디바이스 사전은 Device-ID를 기반으로 하는 보안 정책 규칙에서 사용할 방화벽용 XML 파일입니다. 여기에는 다양한 디바이스 속성에 대한 항목이 포함되어 있으며 정기적으로 완전히 새로 고쳐지고 업데이트 서버에 새 파일로 게시됩니다. 사전 항목에 변경 사항이 있는 경우 수정된 파일이 업데이트 서버에 게시되어 Panorama와 방화벽이 다음에 업데이트 서버를 확인할 때 자동으로 다운로드하여 설치하며, 이는 2시간마다 자동으로 수행됩니다.
GlobalProtect 데이터 파일	GlobalProtect 앱에서 반환된 HIP(호스트 정보 프로파일) 데이터를 정의하고 평가하기 위한 공급자별 정보가 포함되어 있습니다. 이러한 업데이트를 받으려면 GlobalProtect 게이트웨이 구독이 있어야 합니다. 또한 GlobalProtect가 작동하기 전에 이러한 업데이트에 대한 일정을 생성해야 합니다.
GlobalProtect Clientless VPN	GlobalProtect 포털에서 일반 웹 애플리케이션에 대한 클라이언트리스 VPN 액세스를 가능하게 하는 신규 및 업데이트된 애플리케이션 서명이 포함되어 있습니다. 이러한 업데이트를 받으려면 GlobalProtect 구독이 있어야 합니다. 또한 GlobalProtect Clientless VPN이 작동하기 전에 이러한 업데이트에 대한 일정을 생성해야 합니다. 모범 사례로 항상 GlobalProtect Clientless VPN에 대한 최신 콘텐츠 업데이트를 설치하는 것이 좋습니다.
WildFire	WildFire 퍼블릭 클라우드에서 생성된 멀웨어 및 바이러스 백신 서명에 대한 액세스를 실시간으로 제공합니다. 선택적으로 WildFire 서명 업데이트 패키지를 대신 검색하도록 PAN-OS를 구성할 수 있습니다. 방화벽이 1분 이내에 최신 WildFire 서명을 검색할 수 있도록 1분마다 새 업데이트를 확인하도록 방화벽을 설정할 수 있습니다. WildFire 구독이 없으면 바이러스 백신 업데이트에서 서명이 제공될 때까지 최소 24시간을 기다려야 합니다.

동적 콘텐츠 업데이트	이 패키지에는 무엇이 포함되어 있나요?
WF-Private	WildFire 어플라이언스에서 수행한 분석 결과로 생성된 실시간 멀웨어 및 바이러스 백신 서명을 제공합니다. WildFire 어플라이언스에서 콘텐츠 업데이트를 수신하려면 방화벽과 어플라이언스가 모두 PAN-OS 6.1 이상의 버전을 실행하고 있어야 하며 파일과 이메일 링크를 WildFire 사설 클라우드로 포워딩하도록 방화벽을 구성해야 합니다.

콘텐츠 업데이트 설치

최신 위협(아직 발견되지 않은 위협 포함)으로부터 항상 보호받으려면 Palo Alto Networks에서 게시한 최신 콘텐츠 및 소프트웨어 업데이트로 방화벽을 최신 상태로 유지해야 합니다. 사용 가능한 동적 콘텐츠 업데이트은(는) 보유하고 있는 구독에 따라 다릅니다.

콘텐츠 업데이트를 설치하려면 다음 단계를 따르세요. 방화벽이 업데이트를 검색하고 설치하는 빈도를 정의하기 위해 콘텐츠 업데이트 일정을 설정할 수도 있습니다.

애플리케이션 및 위협 콘텐츠 업데이트는 다른 업데이트 유형과 약간 다르게 작동합니다. 최신 애플리케이션 지식과 위협 방지를 최대한 활용하려면 여기에 있는 단계 대신 애플리케이션 및 위협 콘텐츠 업데이트 배포에 대한 지침을 따르십시오.

STEP 1 | 방화벽이 업데이트 서버에 액세스할 수 있는지 확인하십시오.

1. 기본적으로 방화벽은 **`updates.paloaltonetworks.com`**에서 업데이트 서버에 액세스하여 가장 가까운 서버에서 콘텐츠 업데이트를 수신합니다. 방화벽이 인터넷에 대한 액세스를 제한하는 경우 업데이트 다운로드와 관련된 서버에 액세스할 수 있도록 허용 목록을 구성해야 할 수 있습니다. 콘텐츠 업데이트 서버에 대한 자세한 내용은 동적 업데이트를 위한 콘텐츠 전송 네트워크 인프라를 참조합니다. 추가 참조 정보가 필요하거나 연결 및 업데이트 다운로드 문제가 발생하는 경우 https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000001UtRCAU를 참조하십시오.

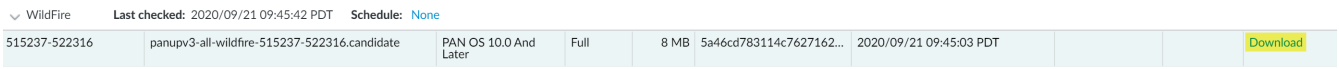
   디바이스가 중국 본토에 있는 경우 *Palo Alto Networks*는 업데이트 다운로드를 위해 ***`updates.paloaltonetworks.cn`*** 서버를 사용할 것을 권장합니다.

2. (선택사항) 업데이트 서버 **ID** 확인을 클릭하여 방화벽이 서버의 SSL 인증서가 신뢰할 수 있는 기관에 의해 서명되었는지 확인할 수 있도록 추가 수준의 유효성 검사를 수행합니다. 이 기능은 기본적으로 활성화되어 있습니다.
3. (선택) 방화벽이 프록시 서버를 사용하여 Palo Alto Networks 업데이트 서비스에 도달해야 하는 경우 프록시 서버 창에서 다음을 입력합니다.
   - 서버 - 프록시 서버의 IP 주소 또는 호스트 이름입니다.
   - 포트 - 프록시 서버용 포트입니다. 범위: 1-65535.
   - 사용자 - 서버에 액세스하기 위한 사용자명입니다.
   - 비밀번호—사용자가 프록시 서버에 액세스하기 위한 비밀번호입니다. 비밀번호 확인에서 비밀번호를 다시 입력하십시오.
4. (선택) 연결 실패가 발생할 경우 최대 3번의 재연결 시도를 구성합니다 ### ## ### #### ## #를 사용하여 연결 시도 횟수를 설정합니다. 기본값은 0입니다.

STEP 2 | 최신 콘텐츠 업데이트를 확인합니다.

디바이스 > 동적 업데이트를 선택하고 지금 확인(창의 왼쪽 하단에 있음)을 클릭하여 최신 업데이트를 확인합니다. 작업 열의 링크는 업데이트가 있는지의 여부를 나타냅니다.

- 다운로드 - 새 업데이트 파일을 사용할 수 있음을 나타냅니다. 링크를 클릭하여 방화벽에 직접 파일 다운로드를 시작합니다. 다운로드에 성공하면 **Action** 열의 링크가 **Download**에서 **Install**로 변경됩니다.



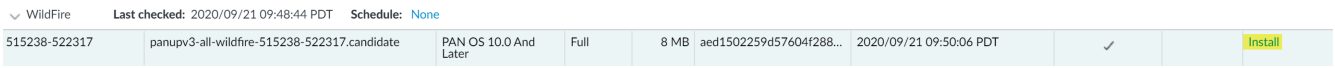
애플리케이션 및 위협 업데이트를 설치할 때까지 바이러스 백신 업데이트를 다운로드할 수 없습니다.

- 되돌리기 - 이전에 설치된 버전의 콘텐츠 또는 소프트웨어 버전을 사용할 수 있음을 나타냅니다. 이전에 설치된 버전으로 되돌리도록 선택할 수 있습니다.

STEP 3 | 콘텐츠 업데이트를 설치합니다.

설치는 *PA-220* 방화벽에서 최대 *10*분, *PA-5200* 시리즈, *PA-7000* 시리즈 또는 *VM* 시리즈 방화벽에서 최대 *2*분이 소요될 수 있습니다.

작업 열에서 설치 링크를 클릭합니다. 설치가 완료되면 현재 설치됨 열에 확인 표시가 나타납니다.



STEP 4 | 각 콘텐츠 업데이트를 예약합니다.

예약하려는 각 업데이트에 대해 이 단계를 반복합니다.

방화벽은 한 번에 하나의 업데이트만 다운로드할 수 있으므로 업데이트 일정에 시차를 두십시오. 동일한 시간의 인터벌 동안 다운로드하도록 업데이트를 예약하면 첫 번째 다운로드만 성공합니다.

1. 없음 링크를 클릭하여 각 업데이트 유형의 일정을 설정합니다.

2. 반복 드롭다운에서 값을 선택하여 업데이트를 수행할 빈도를 지정합니다. 사용 가능한 값은 콘텐츠 유형에 따라 다릅니다(WildFire 업데이트는 실시간, **1**분마다, **15**분마다, **30**분마다 또는 매시

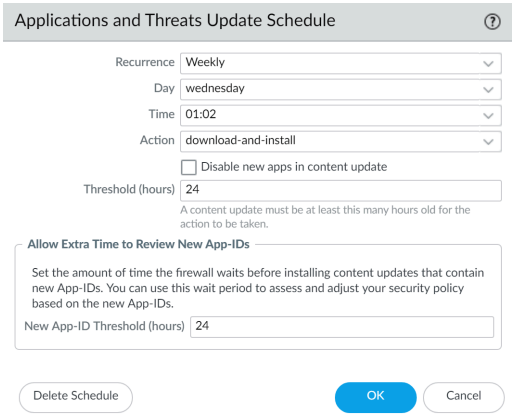
간이며, 여기에서 애플리케이션 및 위협 업데이트는 매주, 매일, 매시간 또는 **30**분마다로 예약하거나 바이러스 백신 업데이트는 매시간, 매일 또는 매주로 예약할 수 있습니다).

애플리케이션 및 위협 또는 안티바이러스 업데이트에 대해 없음**(**수동**)**을 선택할 수도 있습니다. 즉, 이 항목에 대한 반복 일정이 없으며 수동으로 업데이트를 설치해야 합니다. 일정 노드를 완전히 제거하려면 일정 삭제를 선택합니다.

3. 시간 및(또는 WildFire의 경우 시간이 지난 분)을 지정하고 선택한 반복 값에 따라 적용 가능한 경우 업데이트를 원하는 주의 요일을 지정합니다.
4. 시스템이 업데이트를 다운로드만하도록 할지 아니면 모범 사례로 다운로드 및 설치할지 지정합니다.
5. 임계값**(**시간**)** 필드에 콘텐츠 업데이트를 수행하기 전에 릴리스 후 대기할 시간을 입력합니다. 드문 경우지만 콘텐츠 업데이트에서 오류가 발견될 수 있습니다. 이러한 이유로 특정 시간 동안 릴리스될 때까지 새 업데이트 설치를 연기할 수 있습니다.

   100% 사용 가능해야 하는 미션 크리티컬 애플리케이션이 있는 경우 애플리케이션 임계값 또는 애플리케이션 및 위협 업데이트를 최소 *24*시간 이상으로 설정하고 애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례을*(*를*)* 따릅니다. 또한 콘텐츠 업데이트 예약은 일회성 또는 간헐적인 작업이지만 이러한 *App-ID*는 보안 정책이 시행되는 방식을 변경할 수 있기 때문에 일정을 설정한 후에는 콘텐츠 릴리스에 포함된 새 앱 ID 및 수정된 앱 ID 관리를 계속해야 합니다.

6. (선택사항) 새 App-ID가 포함된 콘텐츠 업데이트를 설치하기 전에 방화벽이 대기하는 시간을 설정하려면 새 **App-ID** 임계값을 시간 단위로 입력합니다.



7. 일정 설정을 저장하려면 확인을 클릭합니다.
8. 실행 중인 구성에 설정을 저장하려면 커밋을 클릭합니다.

STEP 5 | PAN-OS를 업데이트하십시오.

*PAN-OS*를 업데이트하기 전에 항상 콘텐츠를 업데이트하십시오. 모든 *PAN-OS* 버전에는 최소 지원되는 콘텐츠 릴리스 버전이 있습니다.

1. 릴리스 노트를 검토합니다.
2. PAN-OS 소프트웨어를 업데이트합니다.

애플리케이션 및 위협 콘텐츠 업데이트

애플리케이션 및 위협 콘텐츠 업데이트는 최신 애플리케이션 및 위협 서명을 방화벽에 제공합니다. 패키지의 애플리케이션 부분에는 신규 및 수정된 App-ID가 포함되며 라이선스가 필요하지 않습니다. 신규 및 수정된 위협 서명도 포함하는 전체 애플리케이션 및 위협 콘텐츠 패키지에는 위협 예방 라이선스가 필요합니다. 방화벽이 자동으로 최신 애플리케이션 및 위협 서명(사용자 지정 설정 기반)을 검색 및 설치하면 추가 구성 없이 최신 App-ID 및 위협 보호를 기반으로 보안 정책을 시행하기 시작합니다.

신규 및 수정된 위협 서명과 수정된 App-ID는 최소한 주 단위 미만으로 자주 릴리스됩니다. 매월 세 번째 화요일에 새로운 App-ID가 출시됩니다.

드문 경우지만 새 *App-ID*가 포함된 업데이트의 게시가 하루 또는 이틀 지연될 수 있습니다.

새로운 App-ID는 보안 정책이 트래픽을 적용하는 방식을 변경할 수 있으므로 보다 제한적인 이 새로운 App-ID 릴리스는 보안 정책을 준비하고 업데이트할 수 있는 예측 가능한 기간을 제공하기 위한 것입니다. 또한 콘텐츠 업데이트는 누적됩니다. 즉, 최신 콘텐츠 업데이트에는 항상 이전 버전에서 릴리스된 애플리케이션 및 위협 서명이 포함됩니다.

애플리케이션 및 위협 서명은 단일 패키지로 제공되기 때문에 서명을 함께 배포할지 아니면 별도로 배포할지 고려해야 합니다(애플리케이션 서명이 애플리케이션을 식별할 수 있도록 하는 동일한 디코더를 통해 위협 서명이 트래픽을 검사할 수 있음). 콘텐츠 업데이트 배포 방법은 조직의 네트워크 보안 및 애플리케이션 가용성 요구 사항에 따라 다릅니다. 출발점으로 조직이 다음 중 하나(또는 방화벽 위치에 따라 둘 다)를 갖고 있는지 확인합니다.

- 보안 최우선 자세를 취하는 조직은 애플리케이션 가용성보다 최신 위협 서명을 사용하여 보호를 우선시합니다. 위협 방지 기능을 위해 주로 방화벽을 사용하고 있습니다. 보안 정책이 애플리케이션 트래픽을 적용하는 방식에 영향을 미치는 App-ID에 대한 모든 변경 사항은 부차적입니다.
- 미션 크리티컬 네트워크는 최신 위협 서명을 사용하여 보호보다 애플리케이션 가용성을 우선시합니다. 네트워크는 가동 중지 시간을 허용하지 않습니다. 방화벽은 보안 정책을 시행하기 위해 인라인으로 배포되며 보안 정책에서 App-ID를 사용하는 경우 App-ID에 영향을 주는 콘텐츠 릴리스가 도입하는 변경 사항으로 인해 가동 중지 시간이 발생할 수 있습니다.

콘텐츠 업데이트 배포에 중요 업무 또는 보안 우선 접근 방식을 취하거나 두 접근 방식을 혼합하여 적용하여 비즈니스 요구 사항을 충족할 수 있습니다. 애플리케이션 및 위협 업데이트의 구현 방법을 결정하려면 애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례을(를) 검토하고 고려합니다. 다음 절차:

- 애플리케이션 및 위협 콘텐츠 업데이트 배포.
- 콘텐츠 업데이트를 위한 팁을(를) 따릅니다.

콘텐츠 업데이트 일정을 잡는 것은 일회성이거나 자주 수행되지 않는 작업이지만 일정을 설정한 후에는 콘텐츠 릴리스에 포함된 새 앱 및 수정된 App-ID 관리를 계속해야 합니다. *App-ID*는 보안 정책이 시행되는 방식을 변경할 수 있습니다.

애플리케이션 및 위협 콘텐츠 업데이트 배포

애플리케이션 및 위협 콘텐츠 업데이트를 구성하는 단계를 수행하기 전에 애플리케이션 및 위협 콘텐츠 업데이트 작동 방식에 대해 알아보고 애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례 구현 방법을 결정합니다.

또한 Panorama를 사용하면 콘텐츠 업데이트를 방화벽에 쉽고 빠르게 배포할 수 있습니다. Panorama를 사용하여 방화벽을 관리하는 경우 아래 단계 대신 이 단계에 따라 콘텐츠 업데이트를 배포합니다.

STEP 1 | 전체 애플리케이션 및 위협 콘텐츠 패키지의 잠금을 해제하려면 위협 예방 라이선스를 받고 방화벽에서 라이선스를 활성화합니다.

1. 디바이스 > 라이선스를 선택합니다.
2. 라이선스 키를 수동으로 업로드하거나 Palo Alto Networks 라이선스 서버에서 검색합니다.
3. Threat Prevention 라이선스가 활성 상태인지 확인합니다.

STEP 2 | 방화벽이 콘텐츠 업데이트를 검색하고 설치하도록 일정을 설정합니다.

다음 단계를 완료할 때 조직이 미션 크리티컬한지 또는 보안 우선인지(또는 둘의 혼합) 여부를 고려하고 애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례을(를) 검토하는 것이 특히 중요합니다.

1. 디바이스 > 동적 업데이트를 선택합니다.
2. 애플리케이션 및 위협 콘텐츠 업데이트에 대한 일정을 선택합니다.
3. 방화벽이 Palo Alto Networks 업데이트 서버에서 새 애플리케이션 및 위협 콘텐츠 릴리스를 확인하는 빈도(반복)와 요일 및 시간을 설정합니다.
4. 방화벽이 새 콘텐츠 릴리스를 찾아 검색할 때 수행할 작업을 설정합니다.
5. 콘텐츠 릴리스에 대한 설치 임계값을 설정합니다. 콘텐츠 릴리스는 방화벽이 릴리스를 검색하고 마지막 단계에서 구성한 작업을 수행하기 전에 최소한 이 시간 동안 Palo Alto Networks 업데이트 서버에서 사용할 수 있어야 합니다.
6. 애플리케이션 다운타임이 허용되지 않는 미션 크리티컬 네트워크인 경우(애플리케이션 가용성은 최신 위협 방지 수준에 해당함) 새 **App-ID** 임계값을 설정할 수 있습니다. 방화벽은 이 시간 동안 사용 가능한 새 App-ID가 포함된 콘텐츠 업데이트만 검색합니다.
7. 확인을 클릭하여 애플리케이션 및 위협 콘텐츠 업데이트 일정을 저장하고 커밋합니다.

STEP 3 | 로그 포워딩을 설정하여 네트워크 및 방화벽 활동을 모니터링하는 데 사용하는 외부 서비스에 Palo Alto Networks 중요 콘텐츠 경고를 보냅니다. 이를 통해 적절한 직원이 중요한 콘텐츠 문제에 대해 알림을 받도록 하여 필요에 따라 조치를 취할 수 있습니다. 중요 콘텐츠 경고는 (subtype eq 콘텐츠) 및 (eventid eq palo-alto-networks-message) 유형 및 이벤트와 함께 시스템 로그 항목으로 기록됩니다.

STEP 4 | 콘텐츠 업데이트 일정을 잡는 것은 일회성이거나 자주 수행되지 않는 작업이지만 일정을 설정한 후에는 콘텐츠 릴리스에 포함된 새 앱 및 수정된 App-ID 관리를 계속해야 합니다. App-ID는 보안 정책이 시행되는 방식을 변경할 수 있습니다.

콘텐츠 업데이트를 위한 팁

Palo Alto Networks 애플리케이션 및 위협 콘텐츠 릴리스는 엄격한 성능 및 품질 보증을 거칩니다. 그러나 고객 환경에는 가능한 변수가 너무 많기 때문에 콘텐츠 릴리스가 예기치 않은 방식으로 네트워크에 영향을 줄 수 있는 경우가 거의 없습니다. 다음 팁에 따라 콘텐츠 릴리스 문제를 완화하거나 해결하여 네트워크에 최대한 영향을 미치지 않도록 하십시오.

- 애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례를 따르십시오.

  애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례을(를) 검토하고 구현합니다. 콘텐츠 업데이트 배포 방법은 네트워크 보안 및 애플리케이션 가용성 요구 사항에 따라 다를 수 있습니다.

- 최신 콘텐츠를 실행하고 있는지 확인합니다.

  자동으로 다운로드하여 설치하도록 방화벽을 구성하지 않은 경우 최신 콘텐츠로 업데이트를 하십시오.

  방화벽은 다운로드한 콘텐츠 업데이트가 여전히 Palo Alto Networks(설치 시 권장됨)인지 확인합니다. 방화벽이 기본적으로 수행하는 이 검사는 콘텐츠 업데이트가 설치 전에 Palo Alto Networks 업데이트 서버(수동으로 또는 일정에 따라)에서 다운로드되는 경우에 유용합니다. Palo Alto Networks가 가용성에 있어서 콘텐츠 업데이트를 제거하는 경우가 드물기 때문에 이 옵션은 방화벽이 이미 다운로드한 경우에도 Palo Alto Networks가 제거한 콘텐츠 업데이트를 방화벽이 설치하지 못하도록 합니다. 설치하려는 콘텐츠 업데이트가 더 이상 유효하지 않다는 오류 메시지가 표시되면 지금 확인하여 최신 콘텐츠 업데이트를 다운로드하고 대신 해당 버전을 설치합니다(기기 > 동적 업데이트).

- 위협 인텔리전스 원격 분석을 켭니다.

  방화벽이 Palo Alto Networks로 보내는 위협 인텔리전스 원격 분석을 켭니다. 당사는 원격 측정 데이터를 사용하여 콘텐츠 업데이트 문제를 식별하고 해결합니다.

  원격 측정 데이터는 Palo Alto Networks 고객 기반 전체에서 예기치 않은 방식으로 방화벽 성능 또는 보안 정책 시행에 영향을 미치는 콘텐츠 업데이트를 빠르게 인식하는 데 도움이 됩니다. 문제를 더 빨리 식별할수록 문제를 완전히 방지하거나 네트워크에 미치는 영향을 완화하는 데 더 빨리 도움을 드릴 수 있습니다.

  방화벽이 Palo Alto Networks와 원격 측정 데이터를 수집하고 공유할 수 있도록 하려면 다음을 따릅니다.

  1. 디바이스 > 설정 > 원격 측정을 선택합니다.
  2. 원격 측정 설정을 수정하고 모두 선택합니다.
  3. 확인 및 커밋을 클릭하여 변경 사항을 저장합니다.

- **Palo Alto Networks** 콘텐츠 업데이트 알림을 적합한 인원에게 포워딩합니다.

  콘텐츠 릴리스 문제에 대한 중요한 메시지가 해당 담당자에게 직접 포워딩되도록 Palo Alto Networks의 중요한 콘텐츠 경고에 대한 로그 포워딩을 활성화합니다.

  Palo Alto Networks는 이제 방화벽 웹 인터페이스 또는 모니터링에 사용하는 외부 서비스(로그 포워딩이 활성화된 경우)에 콘텐츠 업데이트 문제에 대한 경고를 보낼 수 있습니다. 중요한 콘텐츠 경고는 문

제가 사용자에게 미치는 영향을 이해할 수 있도록 문제를 설명하고 필요한 경우 조치를 취하는 단계를 포함합니다.

방화벽 웹 인터페이스에서 콘텐츠 문제에 대한 중요한 경고는 오늘의 메시지와 유사하게 표시됩니다. Palo Alto Networks가 콘텐츠 업데이트에 대한 중요 경고를 알리면 방화벽 웹 인터페이스에 로그인할 때 경고가 기본적으로 표시됩니다. 방화벽 웹 인터페이스에 이미 로그인한 경우 웹 인터페이스 하단에 있는 메뉴 표시줄의 메시지 아이콘 위에 느낌표가 표시되는 것을 확인할 수 있습니다. 경고를 보려면 메시지 아이콘을 클릭하십시오.

중요한 콘텐츠 업데이트 알림은 유형이 **dynamic-updates**이고 이벤트가 **palo-alto-networks-message**인 시스템 로그 항목으로도 기록됩니다. 이 로그 항목을 보려면 (subtype eq dynamic-updates) 및 (eventid eq palo-alto-networks-message) 필터를 사용하십시오.

- 필요한 경우 **Panorama**를 사용하여 이전 콘텐츠 릴리스로 롤백합니다**.**

  콘텐츠 업데이트 문제에 대한 알림을 받은 후 개별 방화벽(Panorama에서 콘텐츠 업데이트 되돌리기)의 콘텐츠 버전을 수동으로 되돌리는 대신 Panorama를 사용하여 관리형 방화벽을 마지막 콘텐츠 업데이트 버전으로 빠르게 되돌릴 수 있습니다.

애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례

콘텐츠 업데이트를 배포하는 모범 사례는 방화벽이 지속적으로 새롭고 수정된 애플리케이션 및 위협 서명을 갖추고 있으므로 원활한 정책 시행을 보장하는 데 도움이 됩니다. 애플리케이션 및 위협 서명이 단일 콘텐츠 업데이트 패키지로 함께 제공되더라도(애플리케이션 및 위협 콘텐츠 업데이트에 대한 자세한 내용 참조) 네트워크 보안 및 가용성 요구 사항에 따라 다르게 배포할 수 있는 유연성이 있습니다.

- 보안 최우선 자세를 취하는 조직은 애플리케이션 가용성보다 최신 위협 서명을 사용하여 보호를 우선시합니다. 위협 방지 기능을 위해 주로 방화벽을 사용하고 있습니다.
- 미션 크리티컬 네트워크는 최신 위협 서명을 사용하여 보호보다 애플리케이션 가용성을 우선시합니다. 네트워크는 가동 중지 시간을 허용하지 않습니다. 방화벽은 보안 정책을 시행하기 위해 인라인으로 배포되며 보안 정책에서 App-ID를 사용하는 경우 App-ID에 영향을 미치는 콘텐츠 변경으로 인해 다운타임이 발생할 수 있습니다.

콘텐츠 업데이트 배포에 중요 업무 또는 보안 우선 접근 방식을 취하거나 두 접근 방식을 혼합하여 적용하여 비즈니스 요구 사항을 충족할 수 있습니다. 신규 및 수정된 위협 및 애플리케이션 서명을 가장 효과적으로 활용하기 위해 다음 모범 사례를 적용할 때 접근 방식을 고려하십시오.

- 콘텐츠 업데이트 모범 사례 - 미션 크리티컬
- 콘텐츠 업데이트 모범 사례 - 보안 우선

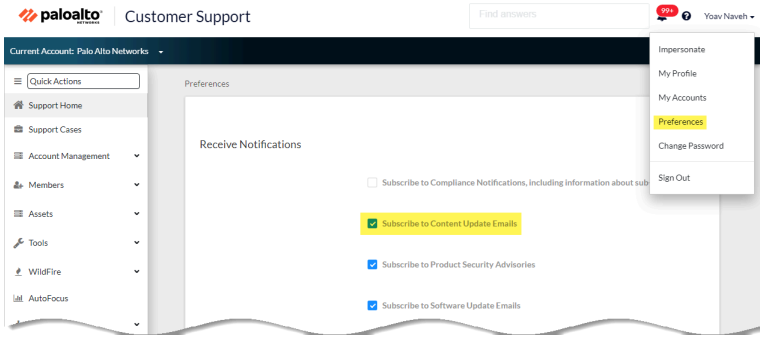
콘텐츠 업데이트 모범 사례 - 미션 크리티컬

애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례은(는) 새 애플리케이션 및 위협 서명이 릴리스될 때 원활한 정책 시행을 보장하는 데 도움이 됩니다. 애플리케이션 다운타임이 허용되지 않는 미션 크리티컬 네트워크에 콘텐츠 업데이트를 배포하려면 다음 모범 사례를 따르십시오.

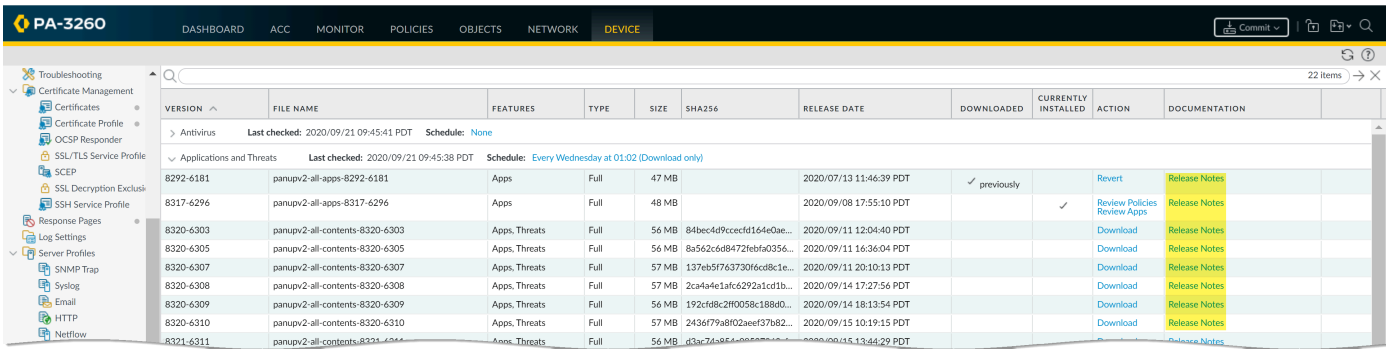
- ❑ 콘텐츠 릴리스가 도입하는 새로 식별 및 수정된 애플리케이션 및 위협 서명 목록에 대해서는 항상 콘텐츠 릴리스 정보를 검토하십시오. 콘텐츠 릴리스 정보는 또한 업데이트가 기존 보안 정책 시행에 어떤 영

향을 미칠 수 있는지 설명하고 새로운 기능을 최대한 활용하기 위해 보안 정책을 수정할 수 있는 방법에 대한 권장 사항을 제공합니다.

새로운 콘텐츠 업데이트에 대한 알림을 받도록 구독하려면 고객 지원 포털을 방문하여 기본 설정을 수정하고 콘텐츠 업데이트 이메일 구독을 선택하십시오.



Palo Alto Networks 지원 포털이나 방화벽 웹 인터페이스에서 직접 앱 및 위협에 대한 콘텐츠 출시 정보를 검토할 수도 있습니다. 디바이스 > 동적 업데이트를 선택하고 특정 콘텐츠 릴리스 버전에 대한 릴리스 노트를 엽니다.

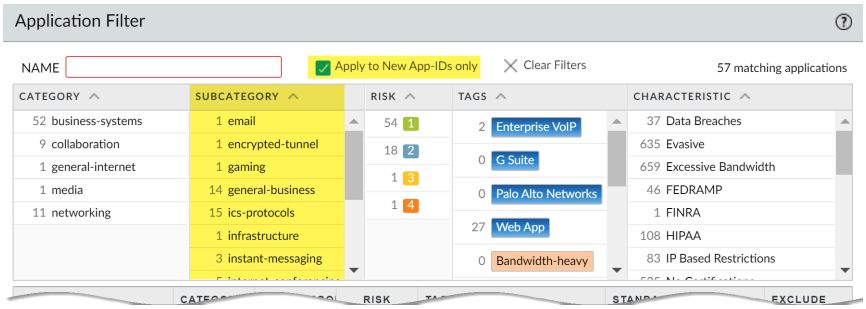


콘텐츠 릴리스 노트의 메모 섹션에서는 *Palo Alto Networks*가 범위에 상당한 영향을 미칠 수 있는 것으로 식별한 향후 업데이트*(*예*:* 새로운 *App-ID* 또는 디코더*)*를 강조합니다. 이러한 향후 업데이트를 확인하여 릴리스 전에 정책 영향을 설명할 수 있습니다.

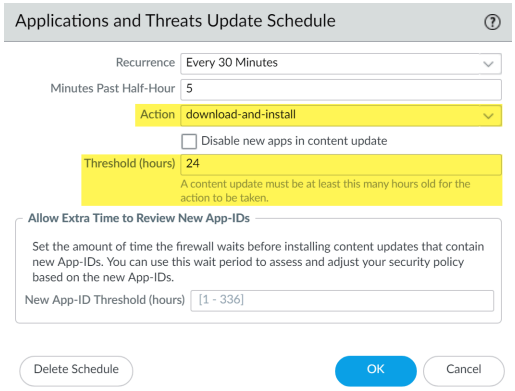
- 중요한 비즈니스 기능이 의존하는 인증 또는 소프트웨어 개발 애플리케이션과 같이 항상 특정 카테고리의 새로운 App-ID를 허용하는 보안 정책 규칙을 만듭니다. 이는 콘텐츠 릴리스가 중요한 비즈니스 애플리케이션에 대한 적용 범위를 도입하거나 변경할 때 보안 정책을 업데이트할 필요 없이 방화벽이 애플리케이션을 계속 원활하게 허용한다는 것을 의미합니다. 이렇게 하면 중요한 카테고리의 App-ID에 대

한 잠재적인 가용성 영향을 제거하고 업무에 중요한 App-ID를 허용하도록 보안 정책을 조정할 수 있는 30일(새 App-ID가 매월 릴리스됨)을 제공합니다.

이렇게 하려면 중요 카테고리의 새 App-ID에 대한 애플리케이션 필터(개체 > 애플리케이션 필터)를 만들고 애플리케이션 필터를 보안 정책 규칙에 추가합니다.



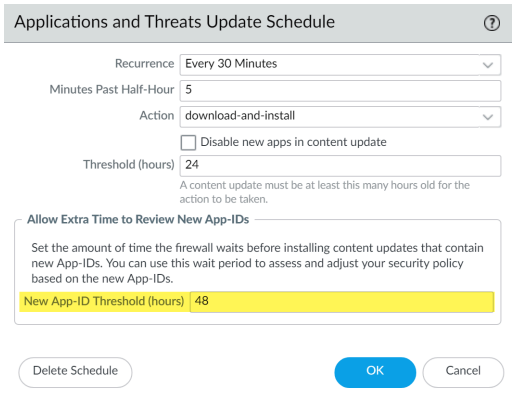
- 새 애플리케이션 및 위협 서명 사용과 관련된 보안 정책 시행에 대한 영향을 완화하려면 새 콘텐츠의 롤아웃에 시차를 두십시오. 비즈니스 위험이 더 낮은 곳(예: 중요한 애플리케이션이 있는 위치)에 배포하기 전에 비즈니스 위험이 적은 곳(새틀라이트 오피스의 사용자 수가 적음)에 새 콘텐츠를 제공합니다. 최신 콘텐츠 업데이트를 네트워크에 배포하기 전에 특정 방화벽으로 제한하면 발생하는 문제를 더 쉽게 해결할 수 있습니다. Panorama를 사용하여 조직 또는 위치에 따라 시차를 둔 일정 및 설치 임계값을 방화벽 및 디바이스 그룹에 푸시할 수 있습니다(Panorama를 사용하여 방화벽 업데이트 배포).
- 콘텐츠 업데이트를 예약하여 자동으로 다운로드 및 설치하도록 합니다. 그런 다음 방화벽이 최신 콘텐츠를 설치하기 전에 대기하는 시간을 결정하는 임계값을 설정합니다. 미션 크리티컬 네트워크에서는 최대 48시간 임계값을 예약합니다.



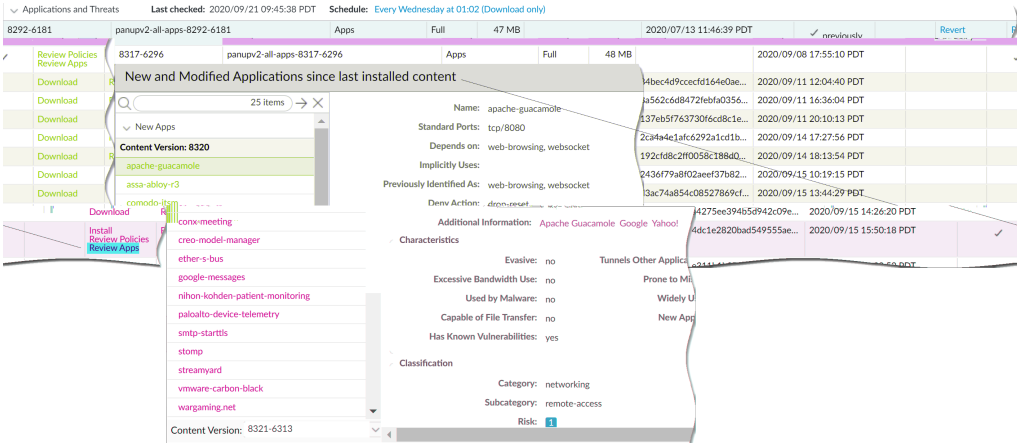
설치 지연은 방화벽이 지정된 시간 동안 고객 환경에서 사용 가능하고 작동하는 콘텐츠만 설치하도록 합니다. 콘텐츠 업데이트를 예약하려면 디바이스 > 동적 업데이트 > 예약을 선택합니다.

- 새로운 App-ID를 설치하기 전에 이를 기반으로 보안 정책을 조정할 수 있는 추가 시간을 확보하십시오. 이렇게 하려면 새 App-ID가 포함된 콘텐츠 업데이트에만 적용되는 설치 임계값을 설정하십시오. 새로

운 App-ID를 사용한 콘텐츠 업데이트는 한 달에 한 번만 릴리스되며 설치 임계값은 해당 시간에만 트리거됩니다. 콘텐츠 업데이트 예약을 하여 새 앱 **ID** 임계값 구성(디바이스 > 동적 업데이트 > 예약).

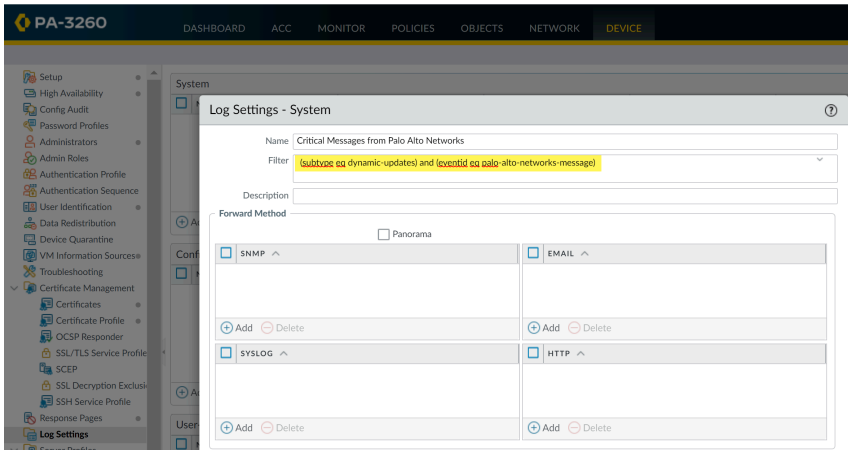


- 변경 사항이 보안 정책에 어떤 영향을 미칠 수 있는지 평가하기 위해 콘텐츠 릴리스가 도입하는 신규 및 수정된 App-ID를 항상 검토하십시오. 다음 주제에서는 새 App-ID를 설치하기 전과 후에 보안 정책을 업데이트하는 데 사용할 수 있는 옵션에 대해 설명합니다. 신규 및 수정된 App-ID를 관리합니다.



- 로그 포워딩을 설정하여 네트워크 및 방화벽 활동을 모니터링하는 데 사용하는 외부 서비스에 Palo Alto Networks 중요 콘텐츠 경고를 보냅니다. 이를 통해 적절한 직원이 중요한 콘텐츠 문제에 대해 알림을 받도록 하여 필요에 따라 조치를 취할 수 있습니다. 중요한 콘텐츠 경고는 유형 및 이벤트가 **(subtype**

eq dynamic-updates) # (eventid eq palo-alto-networks-message)인 시스템 로그 항목으로 기록됩니다.



*PAN-OS 8.1.2*는 중요한 콘텐츠 경고의 로그 유형을 ##에서 ## ####로 변경했습니다. *PAN-OS 8.1.0* 또는 *PAN-OS 8.1.1*을 사용하는 경우 중요한 콘텐츠는 다음 유형 및 이벤트와 함께 시스템 로그 항목으로 기록되며 다음 필터를 사용하여 이러한 경고에 대한 포워딩을 설정해야 합니다: ***(subtype eq general) # (eventid eq palo-alto-networks-message)***.

- 프로덕션 환경에서 활성화하기 전에 전용 스테이징 환경에서 새로운 애플리케이션 및 위협 콘텐츠 업데이트를 테스트하십시오. 새로운 애플리케이션과 위협을 테스트하는 가장 쉬운 방법은 테스트 방화벽을 사용하여 프로덕션 트래픽을 활용하는 것입니다. 테스트 방화벽에 최신 콘텐츠를 설치하고 프로덕션 환경에서 복사된 트래픽을 처리하는 방화벽을 모니터링합니다. 테스트 클라이언트와 테스트 방화벽 또는 PCAP(패킷 캡처)를 사용하여 프로덕션 트래픽을 시뮬레이션할 수도 있습니다. PCAP를 사용하면 방화벽 보안 정책이 위치에 따라 달라지는 다양한 배포에 대한 트래픽을 시뮬레이션하는 데 적합합니다.

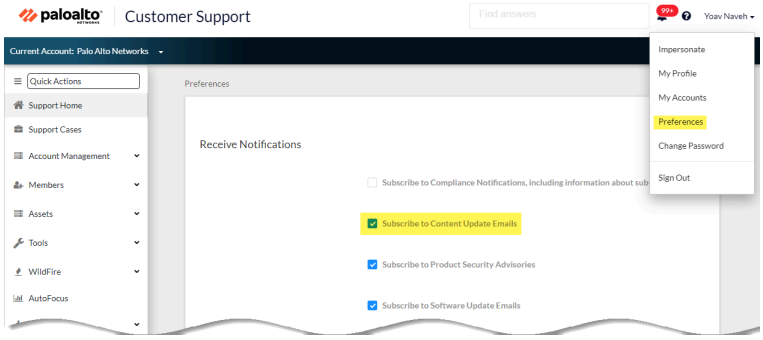
콘텐츠 업데이트 모범 사례 - 보안 우선

애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례은(는) 새 애플리케이션 및 위협 서명이 릴리스될 때 원활한 정책 시행을 보장하는 데 도움이 됩니다. 다음 모범 사례에 따라 보안 우선 네트워크에 콘텐츠 업데이트를 배포합니다. 여기서 위협 방지 기능을 위해 주로 방화벽을 사용하고 공격 방어를 최우선으로 합니다.

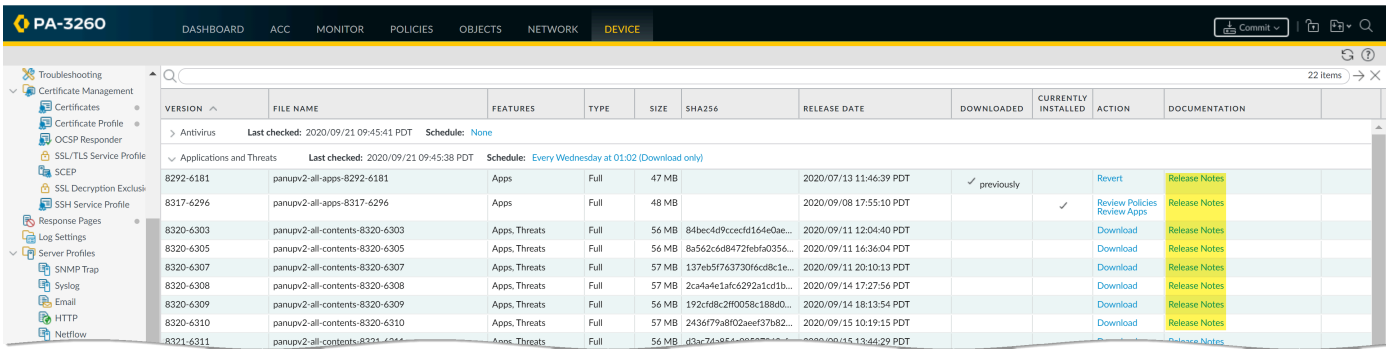
- 콘텐츠 릴리스가 도입하는 새로 식별 및 수정된 애플리케이션 및 위협 서명 목록에 대해서는 항상 콘텐츠 릴리스 정보를 검토하십시오. 콘텐츠 릴리스 정보는 또한 업데이트가 기존 보안 정책 시행에 어떤 영

향을 미칠 수 있는지 설명하고 새로운 기능을 최대한 활용하기 위해 보안 정책을 수정할 수 있는 방법에 대한 권장 사항을 제공합니다.

새로운 콘텐츠 업데이트에 대한 알림을 받도록 구독하려면 고객 지원 포털을 방문하여 기본 설정을 수정하고 콘텐츠 업데이트 이메일 구독을 선택하십시오.



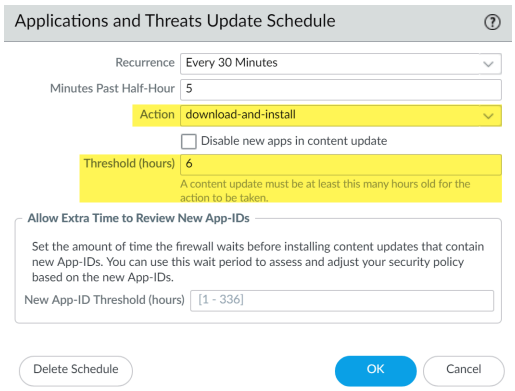
Palo Alto Networks 지원 포털이나 방화벽 웹 인터페이스에서 직접 앱 및 위협에 대한 콘텐츠 출시 정보를 검토할 수도 있습니다. 디바이스 > 동적 업데이트를 선택하고 특정 콘텐츠 릴리스 버전에 대한 릴리스 노트를 엽니다.



콘텐츠 릴리스 노트의 메모 섹션에서는 *Palo Alto Networks*가 범위에 상당한 영향을 미칠 수 있는 것으로 식별한 향후 업데이트*(*예*:* 새로운 *App-ID* 또는 디코더*)*를 강조합니다. 이러한 향후 업데이트를 확인하여 릴리스 전에 정책 영향을 설명할 수 있습니다.

- 새 애플리케이션 및 위협 서명 사용과 관련된 보안 정책 시행에 대한 영향을 완화하려면 새 콘텐츠의 롤아웃에 시차를 두십시오. 비즈니스 위험이 더 낮은 곳(예: 중요한 애플리케이션이 있는 위치)에 배포하기 전에 비즈니스 위험이 적은 곳(새틀라이트 오피스의 사용자 수가 적음)에 새 콘텐츠를 제공합니다. 최신 콘텐츠 업데이트를 네트워크에 배포하기 전에 특정 방화벽으로 제한하면 발생하는 문제를 더 쉽게 해결할 수 있습니다. Panorama를 사용하여 조직 또는 위치에 따라 시차를 둔 일정 및 설치 임계값을 방화벽 및 디바이스 그룹에 푸시할 수 있습니다(Panorama를 사용하여 방화벽 업데이트 배포).

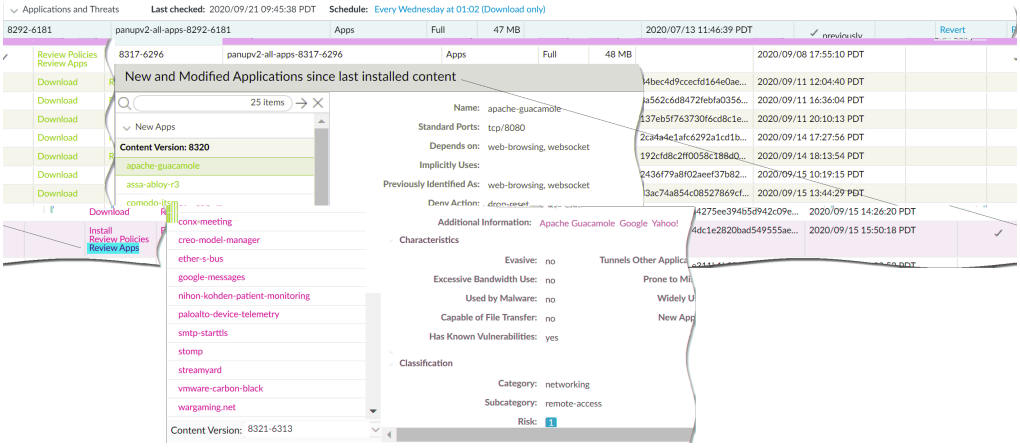
- 콘텐츠 업데이트를 예약하여 자동으로 다운로드 및 설치하도록 합니다. 그런 다음 방화벽이 최신 콘텐츠를 설치하기 전에 대기하는 시간을 결정하는 임계값을 설정합니다. 보안 우선 네트워크에서는 6~12시간 임계값을 예약합니다.



  설치 지연은 방화벽이 지정된 시간 동안 고객 환경에서 사용 가능하고 작동하는 콘텐츠만 설치하도록 합니다. 콘텐츠 업데이트를 예약하려면 디바이스 > 동적 업데이트 > 예약을 선택합니다.

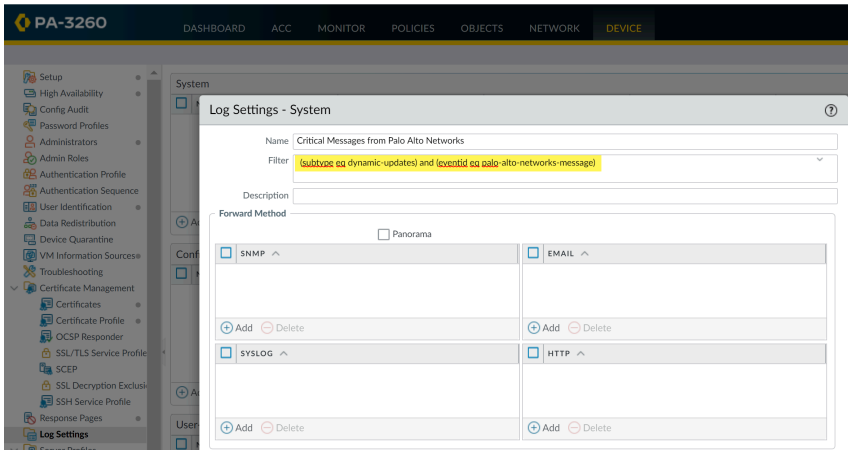
  새 앱 ***ID*** 임계값을 예약하지 마십시오. 이 임계값은 미션 크리티컬 조직이 새로운 *App-ID*를 기반으로 보안 정책 시행을 조정할 수 있는 추가 시간을 허용합니다. 그러나 이 임계값은 또한 최신 위협 방지 업데이트의 전달을 지연시키므로 보안을 최우선으로 하는 조직에는 권장되지 않습니다.

- 변경 사항이 보안 정책에 어떤 영향을 미칠 수 있는지 평가하기 위해 콘텐츠 릴리스에서 도입한 신규 및 수정된 App-ID를 검토하십시오. 다음 주제에서는 새 App-ID를 설치하기 전과 후에 보안 정책을 업데이트하는 데 사용할 수 있는 옵션에 대해 설명합니다. 신규 및 수정된 App-ID를 관리합니다.



- 로그 포워딩을 설정하여 네트워크 및 방화벽 활동을 모니터링하는 데 사용하는 외부 서비스에 Palo Alto Networks 중요 콘텐츠 경고를 보냅니다. 이를 통해 적절한 직원이 중요한 콘텐츠 문제에 대해 알림을 받도록 하여 필요에 따라 조치를 취할 수 있습니다. 중요 콘텐츠 경고는 (`subtype eq dynamic-`

`updates`) 및 (`eventid eq palo-alto-networks-message`)와 같은 유형 및 이벤트와 함께 시스템 로그 항목으로 기록됩니다.



*PAN-OS 8.1.2*는 중요한 콘텐츠 경고의 로그 유형을 *##*에서 *## ####*로 변경했습니다. *PAN-OS 8.1.0* 또는 *PAN-OS 8.1.1*을 사용하는 경우 중요한 콘텐츠는 다음 유형 및 이벤트와 함께 시스템 로그 항목으로 기록되며 다음 필터를 사용하여 이러한 경고에 대한 포워딩을 설정해야 합니다: ***(subtype eq general) # (eventid eq palo-alto-networks-message)***.

콘텐츠 전송 네트워크 인프라

Palo Alto Networks는 콘텐츠 업데이트를 Palo Alto Networks 방화벽에 전달하기 위한 CDN(콘텐츠 전송 네트워크) 인프라를 유지 관리합니다. 방화벽은 CDN의 웹 리소스에 액세스하여 다양한 콘텐츠 및 애플리케이션 식별 기능을 수행합니다.

다음 표에는 기능 또는 애플리케이션에 대해 방화벽이 액세스하는 웹 리소스가 나열되어 있습니다.

리소스	URL	고정 주소(고정 서버가 필요한 경우)
애플리케이션 데이터베이스 위협/안티바이러스 데이터베이스	• updates.paloaltonetworks.com(글로벌, 중국 본토 제외) • updates.paloaltonetworks.cn(중국 본토만 해당) 방화벽의 인터넷 액세스가 제한된 경우 방화벽 허용 목록에 다음 URL 추가: • downloads.paloaltonetworks.com:443 • proditpdownloads.paloaltonetworks.com:443 가장 좋은 방법은 업데이트 서버를 updates.paloaltonetworks.com으로 설정하는 것입니다. 이를 통해 Palo Alto Networks 방화벽은 CDN 인프라에서 가장 가까운 서버로부터 콘텐츠를 업데이트할 수 있습니다. 추가 참조 정보가 필요하거나 연결 및 업데이트 다운로드 문제가 발생하는 경우, https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000001UtRCAU 를 참조하십시오. Palo Alto Networks ThreatVault 데이터베이스에는 취약성, 악용, 바이러스 및 스파이웨어 위협에 대한 정보가 포함되어 있습니다. DNS 보안 및 바이러스 백신 프로필을 포함한 방화벽 기능은 • data.threatvault.paloaltonetworks.com 의 리소스를 사용하여 위협 ID 정보를 검색하여 예외를 생성합니다.	us-static.updates.paloaltonetworks.com 방화벽 허용 목록에 다음 IPv4 또는 IPv6 고정 서버 주소 세트를 추가합니다. • **IPv4**—35.186.202.45:443 및 34.120.74.244:443 • **IPv6**—[2600:1901:0:669::]:443 및 [2600:1901:0:5162::]:443 적절한 기능을 위해 지정된 프로토콜 유형에 대해 제공된 두 *IP* 주소를 모두 허용 목록에 추가해야 합니다.

리소스	URL	고정 주소(고정 서버가 필요한 경우)
PAN-DB URL 필터링 | 고급 URL 필터링	*.urlcloud.paloaltonetworks.com 기본 URL은 s0000.urlcloud.paloaltonetworks.com이며 다음 중 가장 가까운 리전 서버로 리디렉션됩니다. • s0100.urlcloud.paloaltonetworks.com • s0200.urlcloud.paloaltonetworks.com • s0300.urlcloud.paloaltonetworks.com • s0500.urlcloud.paloaltonetworks.com	고정 IP 주소는 사용할 수 없습니다. 그러나 URL을 IP 주소로 수동으로 확인하고 지역 서버 IP 주소에 대한 액세스를 허용할 수 있습니다.
클라우드 서비스	hawkeye.services-edge.paloaltonetworks.com으로 확인되고 다음 중 가장 가까운 리전 서버로 리디렉션됩니다. • US - **us.hawkeye.services-edge.paloaltonetworks.com** • EU - **eu.hawkeye.services-edge.paloaltonetworks.com** • 영국 - **uk.hawkeye.services-edge.paloaltonetworks.com** • APAC - **apac.hawkeye.services-edge.paloaltonetworks.com**	고정 IP 주소는 사용할 수 없습니다.
DNS 보안	• 클라우드 - dns.service.paloaltonetworks.com:443 • 텔레메트리 - io.dns.service.paloaltonetworks.com:443 허용 목록을 다운로드할 때 dns.service.paloaltonetworks.com은 다음 서버로 확인됩니다. • static.dns.service.paloaltonetworks.com:443 • data.threatvault.paloaltonetworks.com(DNS 예외 생성에 사용됨)	고정 IP 주소는 사용할 수 없습니다.
방화벽 기반 인라인 ML: • URL 필터링 인라인 ML	• ml.service.paloaltonetworks.com:443	고정 IP 주소는 사용할 수 없습니다.

리소스	URL	고정 주소(고정 서버가 필요한 경우)
• WildFire Inline ML		
WildFire	• 클라우드(보고서 검색) - wildfire.paloaltonetworks.com:443 WildFire 클라우드 리전: • 글로벌 - wildfire.paloaltonetworks.com • 유럽 연합 - eu.wildfire.paloaltonetworks.com • 일본 - jp.wildfire.paloaltonetworks.com • 싱가포르 - sg.wildfire.paloaltonetworks.com • 영국 - uk.wildfire.paloaltonetworks.com • 캐나다 - ca.wildfire.paloaltonetworks.com • 호주 - au.wildfire.paloaltonetworks.com • 독일 - de.wildfire.paloaltonetworks.com • 인도 - in.wildfire.paloaltonetworks.com	고정 IP 주소는 사용할 수 없습니다.

Panorama 업그레이드

Panorama용 콘텐츠 업데이트 및 소프트웨어 업그레이드 설치

유효한 지원 구독을 통해 Panorama 소프트웨어 이미지 및 릴리스 정보에 접속할 수 있습니다. 최신 수정 사항 및 향상된 보안 기능을 활용하려면, 리셀러 또는 Palo Alto Networks 시스템 엔지니어가 배포에 권장하는 최신 소프트웨어 및 콘텐츠 업데이트로 업그레이드하십시오. 소프트웨어 및 콘텐츠 업데이트를 설치하는 절차는 Panorama가 인터넷에 직접 연결되어 있는지의 여부와 고가용성(HA) 구성이 있는지의 여부에 따라 다릅니다.

- 인터넷 연결을 통해 Panorama 업그레이드
- 인터넷 연결 없이 Panorama 업그레이드
- 인터넷 연결 없이 Panorama 콘텐츠 업데이트 자동 설치
- HA 구성에서 Panorama 업그레이드
- Panorama 로그를 새 로그 형식으로 마이그레이션
- 향상된 디바이스 관리 용량을 위한 Panorama 업그레이드
- FIPS-CC 모드에서 Panorama 및 관리형 디바이스 업그레이드
- Panorama 11.0에서 다운그레이드

인터넷 연결을 통해 Panorama 업그레이드

Panorama™가 인터넷에 직접 연결되어 있는 경우 다음 단계를 수행하여 필요에 따라 Panorama 소프트웨어 및 콘텐츠 업데이트를 설치합니다. Panorama가 고가용성(HA) 구성에서 실행 중인 경우 각 피어에서 Panorama 소프트웨어를 업그레이드합니다(HA 구성에서 Panorama 업그레이드 참조). Panorama 및 FIPS-CC 모드의 관리형 디바이스를 PAN-OS 10.2 또는 이전 릴리스에서 PAN-OS® 11.0으로 업그레이드하는 경우 PAN-OS 10.2 릴리스를 실행하는 동안 Panorama 관리에 추가된 경우 FIPS-CC 모드에서 디바이스의 보안 연결 상태를 재설정하는 추가 단계를 수행해야 합니다. FIPS-CC 모드에서 Panorama 및 FIPS-CC 디바이스를 업그레이드하는 방법에 대한 자세한 내용은 FIPS-CC 모드에서 Panorama 및 관리형 디바이스 업그레이드을(를) 참조하십시오.

Panorama 가상 어플라이언스에서 소프트웨어를 업그레이드해도 시스템 모드는 변경되지 않습니다. Panorama 모드 또는 관리 전용 모드로 전환하는 것은 로컬 로그 수집기로 Panorama 가상 어플라이언스 설정에 설명된 대로 추가 설정이 필요한 수동 작업입니다.

*Palo Alto Networks*는 업그레이드할 *PAN-OS* 버전에 따라 업그레이드 경로의 여러 지점에 새로운 로그 데이터 형식을 도입했습니다.

- ***PAN-OS 8.1***에서 ***PAN-OS 9.0***으로 업그레이드 - *PAN-OS 9.0*은 로컬 및 전용 *Log Collector*에 대한 새로운 로그 데이터 형식을 도입했습니다. *PAN-OS 11.0*으로의 업그레이드 경로에서 *PAN-OS 8.1*에서 *PAN-OS 9.0*으로 업그레이드하면 기존 로그 데이터가 새 형식으로 자동 마이그레이션됩니다.
- ***PAN-OS 10.0***에서 ***PAN-OS 10.1***로 업그레이드 - *PAN-OS 10.1*은 로컬 및 전용 *Log Collector*에 대한 새로운 로그 형식을 도입했습니다. *PAN-OS 11.0*으로의 업그레이드 경로에서는 *PAN-OS 8.1* 이전 버전에서 생성된 로그를 더 이상 사용할 수 없습니다. 여기에는 *PAN-OS 9.0*으로의 업그레이드의 일부로 마이그레이션된 로그가 포함됩니다. *PAN-OS 10.1*로 업그레이드한 후에는 이러한 로그를 복구하여 *PAN-OS 10.1* 로그 형식으로 마이그레이션할 수 있습니다.

로그 데이터 손실을 방지하려면 수집기 그룹의 모든 로그 수집기를 동시에 업그레이드해야 합니다. 수집기 그룹의 로그 수집기가 모두 동일한 PAN-OS 버전을 실행하지 않는 경우 로그 포워딩 또는 로그 수집이 발생하지 않습니다. 또한 수집기 그룹의 로그 수집기에 대한 로그 데이터는 모든 로그 수집기가 동일한 PAN-OS 버전을 실행할 때까지 **ACC** 또는 모니터 탭에 표시되지 않습니다. 예를 들어 수집기 그룹에 세 개의 로그 수집기가 있고 두 개의 로그 수집기를 업그레이드하는 경우 수집기 그룹의 로그 수집기로 로그가 포워딩되지 않습니다.

Panorama를 업그레이드하기 전에 PAN-OS® 11.0에 필요한 최소 콘텐츠 릴리스 버전에 대한 릴리스 노트를 참조하십시오.

STEP 1 | 설치하려는 업데이트가 Panorama 배포에 적합한지 확인하십시오.

*Palo Alto Networks*는 *Panorama*, *Log Collectors* 및 모든 관리 방화벽이 동일한 콘텐츠 릴리스 버전을 실행할 것을 적극 권장합니다.

- ❑ Panorama 소프트웨어 릴리스에 필요한 최소 콘텐츠 릴리스 버전은 릴리스 노트를 참조하십시오. 특정 릴리스로 로그 수집기 및 방화벽을 업그레이드하려는 경우 먼저 Panorama를 해당 릴리스(또는 이후 버전)로 업그레이드해야 합니다.
- ❑ 하이퍼바이저에서 실행되는 Panorama 가상 어플라이언스의 경우 인스턴스가 Panorama 가상 어플라이언스 설정 전제 조건을 충족하는지 확인하십시오.

STEP 2 | PAN-OS 11.0으로의 업그레이드 경로 결정.

현재 실행 중인 PAN-OS 버전에서 PAN-OS 11.0으로 이동하는 경로에 있는 기능 릴리스 버전의 설치를 건너뛸 수 없습니다.

업그레이드 경로의 일부로 통과하는 각 릴리스에 대한 릴리스 노트 및 다운그레이드 고려 사항의 알려진 문제 및 기본 동작에 대한 변경 사항은 PAN-OS 업그레이드 점검표에서 확인할 수 있습니다.

STEP 3 | 업그레이드에 문제가 있는 경우 구성을 복원하는 데 사용할 수 있는 현재 Panorama 구성 파일의 백업을 저장하십시오.

*Panorama*는 구성의 백업을 자동으로 생성하지만 가장 좋은 방법은 업그레이드하기 전에 백업을 생성하고 외부에 저장하는 것입니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. 이름이 지정된 **Panorama** 구성 스냅샷 저장(**Panorama** > 설정 > 작업)을 수행하고, 이름 입력 구성을 선택한 후 확인을 클릭합니다.
3. 이름이 지정된 **Panorama** 구성 스냅샷 내보내기를 수행하고, 방금 저장한 구성의 이름을 선택한 다음 확인하고 내보낸 파일을 Panorama 외부 위치에 저장합니다.

STEP 4 | (모범 사례) CDL(Cortex Data Lake)을 활용하는 경우 Panorama 디바이스 인증서를 설치합니다.

Panorama는 PAN-OS 11.0으로 업그레이드할 때 CDL 수집 및 쿼리 엔드포인트 인증에 디바이스 인증서를 사용하도록 자동 전환됩니다.

*PAN-OS 11.0*으로 업그레이드하기 전에 디바이스 인증서를 설치하지 않으면 *Panorama*는 인증을 위해 기존 로깅 서비스 인증서를 계속 사용합니다.

STEP 5 | 최신 콘텐츠 업데이트를 설치합니다.

*Panorama*가 업그레이드하려는 *Panorama* 릴리스에 필요한 최소 콘텐츠 버전을 실행하지 않는 경우 소프트웨어 업데이트를 설치하기 전에 콘텐츠 버전을 최소*(*또는 그 이상*)* 버전으로 업데이트해야 합니다. *Panorama* 릴리스의 최소 콘텐츠 릴리스 버전은 릴리스 노트를 참조합니다.

Palo Alto Networks®는 *Panorama, Log Collectors* 및 모든 관리 방화벽이 동일한 콘텐츠 릴리스 버전을 실행할 것을 적극 권장합니다. 또한 항상 최신 콘텐츠 버전을 실행하도록 자동 반복 업데이트를 예약하는 것이 좋습니다*(*14 참조*)*.

1. 최신 업데이트를 보려면 **Panorama** > 동적 업데이트 및 지금 확인을 선택합니다. 작업 열의 값이 다운로드인 경우 업데이트를 사용할 수 있습니다.

   *Panorama*가 관리 방화벽 및 로그 수집기에서 실행되는 것과 동일하지만 이후 콘텐츠 릴리스 버전이 아니라 실행 중인지 확인합니다.

2. (Panorama에서 콘텐츠 릴리스 버전을 업데이트하기 전에 방화벽을 Panorama에서 PAN-OS 11.0으로 업그레이드 및 Log Collector(Panorama가 인터넷에 연결된 경우 Log Collector 업그레이드 참조)를 동일한(또는 이후) 콘텐츠 릴리스 버전으로 업데이트해야 합니다.

   지금 콘텐츠 업데이트를 설치할 필요가 없으면 다음 단계로 건너뜁니다.

3. 필요에 따라 나머지 콘텐츠 업데이트를 설치합니다. 설치되면 현재 설치됨 열에 확인 표시가 표시됩니다.

   1. 애플리케이션 또는 애플리케이션 및 위협 업데이트를 다운로드하고 설치합니다. 구독에 관계없이 Panorama는 위협 콘텐츠가 아닌 애플리케이션 콘텐츠 업데이트만 설치하고 이를 필요로 합니다. 자세한 내용은 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조합니다.
   2. 필요에 따라 순서에 관계없이 한 번에 하나씩 다운로드하고 다른 업데이트(안티바이러스, WildFire® 또는 URL 필터링)를 설치합니다.

STEP 6 | **Panorama** > **Plugins**를 선택하고 현재 Panorama에 설치된 모든 플러그인에 대해 PAN-OS 11.0에서 지원되는 플러그인 버전을 다운로드합니다.

대상 PAN-OS 11.0 릴리스에 대해 지원되는 Panorama 플러그인 버전은 호환성 매트릭스를 참조하십시오.

이는 Panorama를 PAN-OS 10.2에서 PAN-OS 11.0으로 성공적으로 업그레이드하는 데 필요합니다. 지원되는 플러그인 버전을 다운로드하지 않으면 PAN-OS 11.0으로의 업그레이드가 차단됩니다.

*PAN-OS 11.0*으로 업그레이드하는 데 필요한 다운로드한 플러그인은 *PAN-OS 11.0*으로 성공적으로 업그레이드한 후 자동으로 설치됩니다. 다운로드한 플러그인이 자동으로 설치되지 않는 경우 *PAN-OS 11.0*으로 업그레이드한 후 영향을 받는 플러그인을 수동으로 설치해야 합니다.

STEP 7 | PAN-OS 11.0으로의 업그레이드 경로에 따라 Panorama를 PAN-OS 릴리스로 업그레이드합니다.

1. 인터넷을 연결하여 Panorama를 PAN-OS 8.1로 업그레이드합니다.
2. 인터넷을 연결하여 Panorama를 PAN-OS 9.0으로 업그레이드합니다.

   PAN-OS 9.0은 새로운 로그 형식을 도입했습니다. 로컬 로그 수집기가 구성된 경우 Panorama를 PAN-OS 9.0으로 성공적으로 업그레이드한 후 로그가 자동으로 새 형식으로 마이그레이션됩니다.

   자동 로그 마이그레이션이 성공적으로 완료되었는지 확인할 때까지 업그레이드 경로를 계속 진행하지 마십시오.
3. 인터넷을 연결하여 Panorama를 PAN-OS 9.1로 업그레이드합니다.
4. 인터넷을 연결하여 Panorama를 PAN-OS 10.0으로 업그레이드합니다.

   *(레거시 모드의 Panorama만 해당) PAN-OS 10.0.0*을 다운로드한 다음 다운로드하고 업그레이드 경로를 계속하기 전에 *PAN-OS 10.0.8* 이상 릴리스를 설치합니다.

   이는 *NFS* 스토리지 파티션에 저장된 모든 로그를 보존하는 데 필요합니다. *PAN-OS 10.0.7* 또는 이전 *PAN-OS 10.0* 릴리스를 설치하면 레거시 모드에서 *Panorama*의 *NFS* 스토리지 파티션에 저장된 일부 로그가 삭제됩니다.
5. 인터넷에 연결하여 Panorama를 PAN-OS 10.1로 업그레이드합니다.

   PAN-OS 10.1에는 새로운 로그 형식이 도입되었습니다. PAN-OS 10.0에서 PAN-OS 10.1로 업그레이드할 때 PAN-OS 8.1 또는 이전 릴리스에서 생성된 로그를 마이그레이션하도록 선택할 수 있습니다. 그렇지 않으면 이러한 로그는 PAN-OS 10.1로 성공적으로 업그레이드될 때 자동으로 삭제됩니다. 마이그레이션 중에는 ACC 또는 모니터 탭에 로그 데이터가 표시되지 않습니다. 마이그레이션이 진행되는 동안 로그 데이터는 적절한 Log Collector로 계속 포워딩되지만 성능에 약간의 영향을 미칠 수 있습니다.

   *(레거시 모드의 Panorama만 해당) PAN-OS 10.1.0*을 다운로드한 다음 *PAN-OS 10.1.3* 이상 릴리스를 다운로드하고 설치합니다.

   이는 *NFS* 스토리지 파티션에 저장된 모든 로그를 보존하는 데 필요합니다. *PAN-OS 10.1.2* 또는 이전 *PAN-OS 10.1* 릴리스를 설치하면 레거시 모드에서 *Panorama*의 *NFS* 스토리지 파티션에 저장된 일부 로그가 삭제됩니다.
6. 인터넷을 연결하여 Panorama를 PAN-OS 10.2로 업그레이드합니다.

STEP 8 | Panorama를 PAN-OS 11.0으로 업그레이드합니다.

1. 최신 릴리스가 있는지 지금 확인(**Panorama** > 소프트웨어)합니다. 소프트웨어 릴리스를 사용할 수 있는 경우 작업 열에 다운로드가 표시됩니다.
2. PAN-OS 11.0.0 이미지를 찾아 다운로드합니다. 다운로드에 성공하면 다운로드한 이미지의 작업 열이 다운로드에서 설치로 변경됩니다.
3. 다운로드한 이미지를 설치한 후 재부팅합니다.
   1. 이미지를 설치합니다.
   2. 설치가 성공적으로 완료되면 다음 방법 중 하나를 사용하여 재부팅합니다.
      - 재부팅하라는 메시지가 표시되면 예를 클릭합니다. CMS 로그인 프롬프트가 표시되면 사용자명이나 암호를 입력하지 않고 Enter 키를 누릅니다. Panorama 로그인 프롬프트가 나타나면 초기 구성 중에 지정한 사용자명과 암호를 입력합니다.
      - 재부팅하라는 메시지가 표시되지 않으면 디바이스 작동 섹션에서 **Panorama**를 재부팅합니다(**Panorama** > **Setup** > **Operations**).

STEP 9 | Panorama 재부팅 후 Panorama 플러그인 버전이 PAN-OS 11.0을 지원하는지 확인합니다.

Panorama를 성공적으로 업그레이드한 후 PAN-OS 11.0에서 지원되는 Panorama 플러그인 버전을 확인하고 설치해야 합니다. PAN-OS 11.0에서 지원되는 Panorama 플러그인에 대한 자세한 내용은 호환성 매트릭스를 참조하십시오.

1. Panorama 웹 인터페이스에 로그인하고 대시보드의 일반 정보 위젯을 검토하여 PAN-OS 11.0 호환 플러그인 버전이 성공적으로 설치되었는지 확인합니다.

   Panorama CLI에 로그인하고 `show plugins installed` 명령을 입력하여 현재 설치된 플러그인 목록을 볼 수도 있습니다.
2. **Panorama** > 플러그인을 선택하고 설치되지 않은 플러그인을 검색합니다.
3. PAN-OS 11.0에서 지원되는 플러그인 버전을 설치합니다.
4. Panorama에 설치된 모든 플러그인이 PAN-OS 11.0에서 지원되는 버전을 실행할 때까지 위 단계를 반복합니다.

STEP 10 | (로컬 Log Collector가 수집기 그룹에 있는 경우) 수집기 그룹의 나머지 Log Collector를 업그레이드합니다.

- Panorama가 인터넷에 연결되어 있을 때 로그 수집기 업그레이드
- Panorama가 인터넷에 연결되어 있지 않을 때 로그 수집기 업그레이드

STEP 11 | (FIPS-CC 모드의 Panorama 및 관리형 디바이스)FIPS-CC 모드에서 Panorama 및 관리형 디바이스 업그레이드.

FIPS-CC 모드에서 Panorama 및 관리형 디바이스를 업그레이드하려면 PAN-OS 11.0 릴리스를 실행하는 동안 Panorama 관리에 추가된 경우 FIPS-CC 모드에서 디바이스의 보안 연결 상태를 재설정해야 합니다. 다음 관리형 디바이스를 Panorama 관리에 다시 온보딩해야 합니다.

FIPS-CC 모드의

관리형 디바이스는 디바이스 등록 인증 키를 사용하여 Panorama에 추가됩니다.

디바이스 등록 인증 키를 사용하여 Panorama에 추가된 일반 작동 모드의 관리형 디바이스

관리형 디바이스가 PAN-OS 10.0 이하 릴리스를 실행하는 동안 Panorama 관리에 추가된 관리형 디바이스를 다시 온보딩할 필요가 없습니다.

STEP 12 | (PAN-OS 10.2 이상 릴리스) OpenSSL 보안 수준 2를 준수하려면 모든 인증서를 재생성하거나 다시 가져옵니다.

PAN-OS 10.1 또는 이전 릴리스에서 PAN-OS 11.0으로 업그레이드하는 경우 이 단계가 필요합니다. PAN-OS 10.2에서 업그레이드하고 이미 인증서를 재생성했거나 다시 가져온 경우 이 단계를 건너뜁니다.

모든 인증서는 다음 최소 요구 사항을 충족해야 합니다.

- RSA 2048비트 이상 또는 ECDSA 256비트 이상
- SHA256 이상의 다이제스트

인증서 재생성 또는 다시 가져오기에 대한 자세한 내용은 PAN-OS 관리자 가이드 또는 Panorama 관리자 가이드를 참조하십시오.

STEP 13 | (Panorama 모드에 권장) Panorama 가상 어플라이언스의 메모리를 64GB로 늘립니다.

Panorama 모드의 Panorama 가상 어플라이언스를 PAN-OS 11.0으로 성공적으로 업그레이드한 후, Palo Alto Networks는 부족 프로비저닝된 Panorama 가상 어플라이언스와 관련된 로깅, 관리 및 운영 성능 문제를 방지하기 위해 증가된 시스템 요구 사항을 충족하도록 Panorama 가상 어플라이언스의 메모리를 64GB로 늘릴 것을 권장합니다.

STEP 14 | (모범 사례) 반복되는 자동 콘텐츠 업데이트를 예약합니다.

> *Panorama*는 *HA* 피어 간에 콘텐츠 업데이트 일정을 동기화하지 않습니다. 능동형 및 수동형 *Panorama* 모두에서 이 작업을 수행해야 합니다.

각 업데이트 유형(**Panorama** > 동적 업데이트)의 헤더 행에서 일정은 처음에 없음으로 설정됩니다. 각 업데이트 유형에 대해 다음 단계를 수행하십시오.

1. 없음을 클릭하고 업데이트 빈도(반복)를 선택합니다. 빈도 옵션은 업데이트 유형에 따라 다릅니다.
2. 일정 작업을 선택합니다.
   - 다운로드 및 설치(모범 사례) - Panorama는 업데이트를 다운로드한 후 자동으로 설치합니다.

     다운로드 전용 - Panorama에서 업데이트를 다운로드한 후 수동으로 업데이트를 설치해야 합니다.
3. 조직의 보안 상태에 대한 모범 사례에 따라 Panorama가 업데이트를 다운로드하기 전에 업데이트를 사용할 수 있게 된 후 지연(임계값)을 구성합니다.
4. 확인을 클릭하여 변경 사항을 저장합니다.
5. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

STEP 15 | (Enterprise DLP만 해당) Enterprise DLP 데이터 필터링 설정을 편집하여 최대 파일 크기를 20MB 이하로 줄입니다.

이 플러그인 버전은 대용량 파일 크기 검사를 지원하지 않으므로 Enterprise DLP 3.0.3 이상 릴리스용 Panorama 플러그인을 Enterprise DLP 4.0.0으로 업그레이드할 때 필요합니다.

인터넷 연결 없이 Panorama 업그레이드

Panorama™가 인터넷에 직접 연결되어 있지 않으면 다음 단계를 수행하여 필요에 따라 Panorama 소프트웨어 및 콘텐츠 업데이트를 설치하십시오. Panorama가 고가용성(HA) 구성으로 배포된 경우 각 피어를 업그레이드해야 합니다(HA 구성에서 Panorama 업그레이드 참조). Panorama 및 FIPS-CC 모드의 관리형 디바이스를 PAN-OS 10.2 또는 이전 릴리스에서 PAN-OS 11.0으로 업그레이드하는 경우, PAN-OS 10.2 릴리스를 실행하는 동안 Panorama 관리에 추가되었다면 FIPS-CC 모드에서 디바이스의 보안 연결 상태를 재설정하는 추가 단계를 수행해야 합니다. FIPS-CC 모드에서 Panorama 및 FIPS-CC 디바이스를 업그레이드하는 방법에 대한 자세한 내용은 FIPS-CC 모드에서 Panorama 및 관리형 디바이스 업그레이드을(를) 참조하십시오.

Panorama 가상 어플라이언스에서 소프트웨어를 업그레이드해도 시스템 모드는 변경되지 않습니다. Panorama 모드 또는 관리 전용 모드로 전환하는 것은 로컬 로그 수집기로 Panorama 가상 어플라이언스 설정에 설명된 대로 추가 설정이 필요한 수동 작업입니다.

*Palo Alto Networks*는 업그레이드할 *PAN-OS* 버전에 따라 업그레이드 경로의 여러 지점에 새로운 로그 데이터 형식을 도입했습니다.

- ***PAN-OS 8.1***에서 ***PAN-OS 9.0***으로 업그레이드 - *PAN-OS 9.0*은 로컬 및 전용 *Log Collector*에 대한 새로운 로그 데이터 형식을 도입했습니다. *PAN-OS 11.0*으로의 업그레이드 경로에서 *PAN-OS 8.1*에서 *PAN-OS 9.0*으로 업그레이드하면 기존 로그 데이터가 새 형식으로 자동 마이그레이션됩니다.
- ***PAN-OS 10.0***에서 ***PAN-OS 10.1***로 업그레이드 - *PAN-OS 10.1*은 로컬 및 전용 *Log Collector*에 대한 새로운 로그 형식을 도입했습니다. *PAN-OS 11.0*으로의 업그레이드 경로에서는 *PAN-OS 8.1* 이전 버전에서 생성된 로그를 더 이상 사용할 수 없습니다. 여기에는 *PAN-OS 9.0*으로의 업그레이드의 일부로 마이그레이션된 로그가 포함됩니다. *PAN-OS 10.1*로 업그레이드한 후에는 이러한 로그를 복구하여 *PAN-OS 10.1* 로그 형식으로 마이그레이션할 수 있습니다.

로그 데이터 손실을 방지하려면 수집기 그룹의 모든 로그 수집기를 동시에 업그레이드해야 합니다. 수집기 그룹의 로그 수집기가 모두 동일한 PAN-OS 버전을 실행하지 않는 경우 로그 포워딩 또는 로그 수집이 발생하지 않습니다. 또한 수집기 그룹의 로그 수집기에 대한 로그 데이터는 모든 로그 수집기가 동일한 PAN-OS 버전을 실행할 때까지 **ACC** 또는 모니터 탭에 표시되지 않습니다. 예를 들어 수집기 그룹에 세 개의 로그 수집기가 있고 두 개의 로그 수집기를 업그레이드하는 경우 수집기 그룹의 로그 수집기로 로그가 포워딩되지 않습니다.

Panorama를 업그레이드하기 전에 PAN-OS® 11.0에 필요한 최소 콘텐츠 릴리스 버전은 릴리스 노트를 참조하십시오.

STEP 1 | 설치하려는 업데이트가 Panorama 배포에 적합한지 확인하십시오.

*Palo Alto Networks*는 *Panorama*, *Log Collectors* 및 모든 관리 방화벽이 동일한 콘텐츠 릴리스 버전을 실행할 것을 적극 권장합니다.

- ❑ Panorama 소프트웨어 릴리스를 위해 설치해야 하는 최소 콘텐츠 릴리스 버전은 릴리스 노트를 참조하십시오. 특정 릴리스로 로그 수집기 및 방화벽을 업그레이드하려는 경우 먼저 Panorama를 해당 릴리스(또는 이후 버전)로 업그레이드해야 합니다.
- ❑ Panorama 가상 어플라이언스의 경우 인스턴스가 Panorama 가상 어플라이언스 설정 전제 조건을 충족하는지 확인하십시오.

STEP 2 | PAN-OS 11.0으로의 업그레이드 경로 결정.

현재 실행 중인 PAN-OS 버전에서 PAN-OS 11.0으로 이동하는 경로에 있는 기능 릴리스 버전의 설치를 건너뛸 수 없습니다.

업그레이드 경로의 일부로 통과하는 각 릴리스에 대한 릴리스 노트 및 다운그레이드 고려 사항의 알려진 문제 및 기본 동작에 대한 변경 사항은 PAN-OS 업그레이드 점검표에서 확인할 수 있습니다.

STEP 3 | 업그레이드에 문제가 있는 경우 구성을 복원하는 데 사용할 수 있는 현재 Panorama 구성 파일의 백업을 저장하십시오.

*Panorama*는 구성의 백업을 자동으로 생성하지만 가장 좋은 방법은 업그레이드하기 전에 백업을 생성하고 외부에 저장하는 것입니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. 이름이 지정된 **Panorama** 구성 스냅샷 저장(**Panorama** > 설정 > 작업)을 수행하고, 이름 입력 구성을 선택한 후 확인을 클릭합니다.
3. 이름이 지정된 **Panorama** 구성 스냅샷 내보내기를 수행하고, 방금 저장한 구성의 이름을 선택한 다음 확인하고 내보낸 파일을 Panorama 외부 위치에 저장합니다.

STEP 4 | SCP 또는 HTTPS를 통해 Panorama에 콘텐츠를 연결하고 업로드할 수 있는 호스트에 최신 콘텐츠 업데이트를 다운로드합니다.

지금 콘텐츠 업데이트를 설치할 필요가 없으면 6으로 건너뜁니다.

1. 인터넷 액세스가 가능한 호스트를 사용하여https://www.paloaltonetworks.com/support/tabs/overview.html 에 로그인합니다.
2. 필요에 따라 콘텐츠 업데이트를 다운로드합니다.
   1. 리소스 섹션에서 업데이트 > 동적 업데이트를 클릭합니다.
   2. 적절한 콘텐츠 업데이트를 다운로드하고 파일을 호스트에 저장합니다. 업데이트해야 하는 각 콘텐츠 유형에 대해 이 단계를 수행합니다.

STEP 5 | 최신 콘텐츠 업데이트를 설치합니다.

소프트웨어 업데이트 전에 콘텐츠 업데이트를 설치해야 하며 *Panorama* 관리 서버에 설치하기 전에 먼저 방화벽을 Panorama에서 PAN-OS 11.0으로 업그레이드한 다음 Log Collector를 업그레이드해야 합니다.

애플리케이션 또는 애플리케이션 및 위협 업데이트를 먼저 설치한 다음 다른 업데이트(바이러스 백신, WildFire® 및 URL 필터링)를 한 번에 하나씩 순서에 관계없이 설치합니다.

구독에 애플리케이션 및 위협 콘텐츠가 모두 포함되어 있는지의 여부와 관계없이 *Panorama*는 애플리케이션 콘텐츠만 설치하고 이를 필요로 합니다. 자세한 내용은 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조합니다.

Panorama 웹 인터페이스에 로그인하고 각 콘텐츠 유형에 대해 다음 단계를 수행합니다.

1. **Panorama** > 동적 업데이트를 선택합니다.
2. 업로드를 클릭하고 콘텐츠 유형을 선택하고 업데이트를 다운로드한 호스트의 위치로 찾아보기한 다음 업데이트를 선택하고 확인을 클릭합니다.
3. 파일에서 설치, 패키지 유형을 선택하고 확인을 클릭합니다.

STEP 6 | 현재 Panorama에 설치된 모든 플러그인에 대해 PAN-OS 11.0에서 지원되는 플러그인 버전을 업로드합니다.

대상 PAN-OS 11.0 릴리스에 대해 지원되는 Panorama 플러그인 버전은 호환성 매트릭스를 참조하십시오.

이는 Panorama를 PAN-OS 10.2에서 PAN-OS 11.0으로 성공적으로 업그레이드하는 데 필요합니다. 지원되는 플러그인 버전을 다운로드하지 않으면 PAN-OS 11.0으로의 업그레이드가 차단됩니다.

*PAN-OS 11.0*으로 업그레이드하는 데 필요한 다운로드한 플러그인은 *PAN-OS 11.0*으로 성공적으로 업그레이드한 후 자동으로 설치됩니다. 다운로드한 플러그인이 자동으로 설치되지 않는 경우 *PAN-OS 11.0*으로 업그레이드 후 영향을 받는 플러그인을 수동으로 설치해야 합니다.

1. PAN-OS 11.0에서 지원하는 플러그인 버전을 다운로드합니다.
   1. Palo Alto Networks 지원 포털에 로그인합니다.
   2. 업데이트 > 소프트웨어 업데이트를 선택하고 드롭다운 메뉴에서 플러그인을 선택합니다.
   3. PAN-OS 10.2에서 지원되는 플러그인 버전을 다운로드합니다.
   4. 현재 Panorama에 설치된 모든 플러그인에 대해 이 단계를 반복합니다.
2. Panorama 웹 인터페이스에 로그인합니다.
3. **Panorama** > 플러그인을 선택하고 이전 단계에서 다운로드한 플러그인 버전을 업로드합니다.
   현재 Panorama에 설치된 모든 플러그인에 대해 이 단계를 반복합니다.

STEP 7 | PAN-OS 10.2로의 업그레이드 경로에 따라 Panorama를 PAN-OS 릴리스로 업그레이드합니다.

1. 인터넷에 연결되지 않은 경우 Panorama를 PAN-OS 8.1로 업그레이드합니다.
2. 인터넷에 연결되지 않은 경우 Panorama를 PAN-OS 9.0으로 업그레이드합니다.

   PAN-OS 9.0은 새로운 로그 형식을 도입했습니다. 로컬 로그 수집기가 구성된 경우 Panorama를 PAN-OS 9.0으로 성공적으로 업그레이드한 후 로그가 자동으로 새 형식으로 마이그레이션됩니다.

   자동 로그 마이그레이션이 성공적으로 완료되었는지 확인할 때까지 업그레이드 경로를 계속 진행하지 마십시오.
3. 인터넷에 연결되지 않은 경우 Panorama를 PAN-OS 9.1로 업그레이드합니다.
4. 인터넷에 연결되지 않은 경우 Panorama를 PAN-OS 10.0으로 업그레이드합니다.

   *(*레거시 모드의 *Panorama*만 해당*) PAN-OS 10.0.0*을 다운로드한 다음 다운로드하고 업그레이드 경로를 계속하기 전에 *PAN-OS 10.0.8* 이상 릴리스를 설치합니다.

   이는 *NFS* 스토리지 파티션에 저장된 모든 로그를 보존하는 데 필요합니다. *PAN-OS 10.0.7* 또는 이전 *PAN-OS 10.0* 릴리스를 설치하면 레거시 모드에서 *Panorama*의 *NFS* 스토리지 파티션에 저장된 일부 로그가 삭제됩니다.
5. 인터넷에 연결되지 않은 경우 Panorama를 PAN-OS 10.1로 업그레이드합니다.

   PAN-OS 10.1에는 새로운 로그 형식이 도입되었습니다. PAN-OS 10.0에서 PAN-OS 10.1로 업그레이드할 때 PAN-OS 8.1 또는 이전 릴리스에서 생성된 로그를 마이그레이션하도록 선택할 수 있습니다. 그렇지 않으면 이러한 로그는 PAN-OS 10.1로 성공적으로 업그레이드될 때 자동으로 삭제됩니다. 마이그레이션 중에는 ACC 또는 모니터 탭에 로그 데이터가 표시되지 않습니다. 마이그레이션이 진행되는 동안 로그 데이터는 적절한 Log Collector로 계속 포워딩되지만 성능에 약간의 영향을 미칠 수 있습니다.

   *(*레거시 모드의 *Panorama*만 해당*) PAN-OS 10.1.0*을 다운로드한 다음 *PAN-OS 10.1.3* 이상 릴리스를 다운로드하고 설치합니다.

   이는 *NFS* 스토리지 파티션에 저장된 모든 로그를 보존하는 데 필요합니다. *PAN-OS 10.1.2* 또는 이전 *PAN-OS 10.1* 릴리스를 설치하면 레거시 모드에서 *Panorama*의 *NFS* 스토리지 파티션에 저장된 일부 로그가 삭제됩니다.
6. 인터넷에 연결되지 않은 경우 Panorama를 PAN-OS 10.2로 업그레이드합니다.

STEP 8 | SCP 또는 HTTPS를 통해 콘텐츠를 Panorama에 연결하고 업로드할 수 있는 호스트에 최신 PAN-OS 11.0 릴리스 이미지를 다운로드합니다.

1. 인터넷에 액세스할 수 있는 호스트를 사용하여 Palo Alto Networks 고객 지원 웹사이트에 로그인합니다.
2. 소프트웨어 업데이트 다운로드:
   1. Palo Alto Networks 고객 지원 웹사이트의 기본 페이지에서 업데이트 > 소프트웨어 업데이트를 클릭합니다.
   2. 최신 PAN-OS 11.0 릴리스 이미지에 대한 모델별 이미지를 찾습니다. 예를 들어, M 시리즈 어플라이언스를 Panorama 11.0.0으로 업그레이드하려면 `Panorama_m-11.0.0` 이미지를 다운로드합니다. Panorama 가상 어플라이언스를 Panorama 11.0.0으로 업그레이드하려면 `Panorama_pc-11.0.0` 이미지를 다운로드합니다.

      필터링 기준 드롭다운에서 ***Panorama M*** 이미지*(M* 시리즈 어플라이언스*)* 또는 ***Panorama*** 업데이트*(*가상 어플라이언스*)*를 선택하여 *Panorama* 이미지를 빠르게 찾을 수 있습니다.
   3. 파일 이름을 클릭하고 파일을 호스트에 저장합니다.

STEP 9 | Panorama를 PAN-OS 11.0으로 업그레이드합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 소프트웨어를 선택하고 이전 단계에서 다운로드한 PAN-OS 11.0 이미지를 업로드합니다.
3. 업데이트를 다운로드한 호스트의 위치를 찾고, 업데이트를 선택한 다음 Panorama가 HA 구성에 있는 경우 동기화(소프트웨어 이미지를 보조 피어로 푸시)하고 확인을 클릭합니다.
4. 소프트웨어 이미지를 설치하고 재부팅하십시오.

   HA 구성의 경우, HA 구성에서 Panorama 업그레이드을(를) 수행하고, 그렇지 않으면 다음을 따릅니다.
   1. 업로드한 이미지를 설치합니다.
   2. 설치를 성공적으로 완료한 후 다음 방법 중 하나를 사용하여 재부팅하십시오.
      - 재부팅하라는 메시지가 표시되면 예를 클릭합니다. CMS 로그인 프롬프트가 표시되면 사용자명이나 암호를 입력하지 않고 Enter 키를 누릅니다. Panorama 로그인 프롬프트가 나타나면 초기 구성 중에 지정한 사용자명과 암호를 입력합니다.
      - 재부팅하라는 메시지가 표시되지 않으면 디바이스 작동 섹션에서 **Panorama**를 재부팅합니다(**Panorama** > **Setup** > **Operations**).

STEP 10 | Panorama 재부팅 후 Panorama 플러그인 버전이 PAN-OS 11.0을 지원하는지 확인합니다.

Panorama를 성공적으로 업그레이드한 후 PAN-OS 11.0에서 지원되는 Panorama 플러그인 버전을 확인하고 설치해야 합니다. PAN-OS 11.0에서 지원되는 Panorama 플러그인에 대한 자세한 내용은 호환성 매트릭스를 참조하십시오.

1. Panorama 웹 인터페이스에 로그인하고 대시보드의 일반 정보 위젯을 검토하여 PAN-OS 11.0 호환 플러그인 버전이 성공적으로 설치되었는지 확인합니다.

   Panorama CLI에 로그인하고 `show plugins installed` 명령을 입력하여 현재 설치된 플러그인 목록을 볼 수도 있습니다.
2. **Panorama** > 플러그인을 선택하고 설치되지 않은 플러그인을 검색합니다.
3. PAN-OS 11.0에서 지원되는 플러그인 버전을 설치합니다.
4. Panorama에 설치된 모든 플러그인이 PAN-OS 11.0에서 지원되는 버전을 실행할 때까지 위 단계를 반복합니다.

STEP 11 | (로컬 Log Collector가 수집기 그룹에 있는 경우) 수집기 그룹의 나머지 Log Collector를 업그레이드합니다.

- Panorama가 인터넷에 연결되어 있을 때 로그 수집기 업그레이드
- Panorama가 인터넷에 연결되어 있지 않을 때 로그 수집기 업그레이드

STEP 12 | (FIPS-CC 모드의 Panorama 및 관리형 디바이스)FIPS-CC 모드에서 Panorama 및 관리형 디바이스 업그레이드.

FIPS-CC 모드에서 Panorama 및 관리형 디바이스를 업그레이드하려면 PAN-OS 11.0 릴리스를 실행하는 동안 Panorama 관리에 추가된 경우 FIPS-CC 모드에서 디바이스의 보안 연결 상태를 재설정해야 합니다. 다음 관리형 디바이스를 Panorama 관리에 다시 온보딩해야 합니다. FIPS-CC 모드의

관리형 디바이스는 디바이스 등록 인증 키를 사용하여 Panorama에 추가됩니다.

디바이스 등록 인증 키를 사용하여 Panorama에 추가된 일반 작동 모드의 관리형 디바이스

관리형 디바이스가 PAN-OS 10.0 이하 릴리스를 실행하는 동안 Panorama 관리에 추가된 관리형 디바이스를 다시 온보딩할 필요가 없습니다.

STEP 13 | (PAN-OS 10.2 이상 릴리스) OpenSSL 보안 수준 2를 준수하려면 모든 인증서를 재생성하거나 다시 가져옵니다.

PAN-OS 10.1 또는 이전 릴리스에서 PAN-OS 11.0으로 업그레이드하는 경우 이 단계가 필요합니다. PAN-OS 10.2에서 업그레이드하고 이미 인증서를 재생성했거나 다시 가져온 경우 이 단계를 건너뜁니다.

모든 인증서는 다음 최소 요구 사항을 충족해야 합니다.

- RSA 2048비트 이상 또는 ECDSA 256비트 이상
- SHA256 이상의 다이제스트

인증서 재생성 또는 다시 가져오기에 대한 자세한 내용은 PAN-OS 관리자 가이드 또는 Panorama 관리자 가이드를 참조하십시오.

STEP 14 | (Panorama 모드에 권장) Panorama 가상 어플라이언스의 메모리를 64GB로 늘립니다.

Panorama 모드의 Panorama 가상 어플라이언스를 PAN-OS 11.0으로 성공적으로 업그레이드한 후, Palo Alto Networks는 부족 프로비저닝된 Panorama 가상 어플라이언스와 관련된 로깅, 관리 및 운영 성능 문제를 방지하기 위해 증가된 시스템 요구 사항을 충족하도록 Panorama 가상 어플라이언스의 메모리를 64GB로 늘릴 것을 권장합니다.

인터넷 연결 없이 Panorama 콘텐츠 업데이트 자동 설치

Panorama™ 관리 서버, 관리 방화벽, 로그 수집기 및 WildFire 어플라이언스가 인터넷에 연결되지 않은 에어 갭 네트워크에서 방화벽, 로그 수집기 및 WildFire® 장비에 대한 콘텐츠 업데이트를 자동으로 다운로드합니다. 이를 수행하려면 인터넷 액세스 및 SCP 서버가 있는 추가 Panorama를 배포해야 합니다. 인터넷 액세스로 Panorama를 배포한 후 SCP 서버에 콘텐츠 업데이트를 자동으로 다운로드하도록 인터넷이 연결된 Panorama를 구성합니다. SCP 서버에서 에어 갭 Panorama는 콘텐츠 업데이트 일정에 따라 콘텐츠 업데이트를 자동으로 다운로드하고 설치하도록 구성됩니다. Panorama는 인터넷에 액세스할 수 있는 Panorama가 콘텐츠 업데이트를 SCP 서버에 다운로드하거나 에어 갭 Panorama가 SCP 서버에서 콘텐츠 업데이트를 다운로드 및 설치할 때 시스템 로그를 생성합니다.

인터넷에 연결된 Panorama에서 인터넷이 연결되지 않은 Panorama로 다음 콘텐츠 업데이트 일정만 지원됩니다.

SCP 서버에 성공적으로 다운로드한 후 콘텐츠 업데이트 파일 이름을 조작하거나 변경하지 마십시오. *Panorama*는 파일 이름이 변경된 콘텐츠 업데이트를 다운로드 및 설치할 수 없습니다. 또한 자동 콘텐츠 업데이트가 성공하려면 *SCP* 서버에 충분한 디스크 공간이 있는지, 다운로드가 시작되려고 할 때 *SCP* 서버가 실행 중인지, 재부팅 중 두 *Panorama*의 전원이 켜져 있고 켜져 있지 않은지 확인해야 합니다.

이 예에서는 애플리케이션 및 위협 콘텐츠 업데이트에 대한 자동 콘텐츠 업데이트를 구성하는 방법을 보여줍니다.

STEP 1 | SCP 서버를 배포합니다.

관리 방화벽, 로그 수집기 및 WildFire 어플라이언스에 대한 콘텐츠 업데이트는 인터넷에 연결된 Panorama에서 다운로드합니다. 에어 갭 Panorama는 SCP 서버에서 콘텐츠 업데이트를 다운로드한 다음 관리 방화벽, WildFire 어플라이언스 및 로그 수집기에 업데이트를 설치합니다.

콘텐츠 업데이트를 위한 폴더 디렉터리를 만들 때 콘텐츠 업데이트 유형별로 폴더를 만드는 것이 가장 좋습니다. 이를 통해 대량의 콘텐츠 업데이트를 관리해야 하며 *SCP* 서버에서 삭제해서는 안 되는 콘텐츠 업데이트를 삭제할 가능성을 줄입니다.

STEP 2 | 인터넷에 연결된 Panorama를 배포합니다.

이 Panorama는 Palo Alto Networks 업데이트 서버와 통신하고 콘텐츠 업데이트를 SCP 서버에 다운로드합니다.

1. Panorama 관리 서버를 설정합니다.
   - M-시리즈 어플라이언스 설정
   - Panorama 가상 어플라이언스 설정
2. 초기 Panorama 구성을 수행합니다.
   - M-시리즈 어플라이언스의 초기 구성 수행
   - Panorama 가상 어플라이언스의 초기 구성 수행

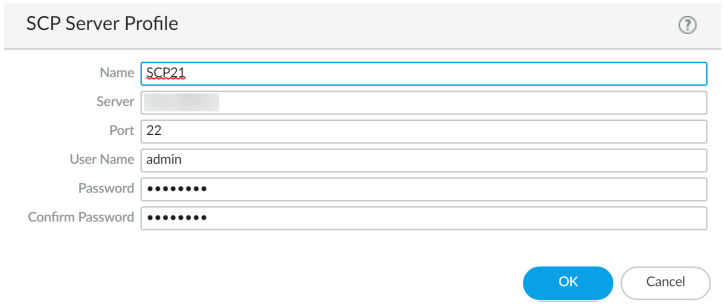
STEP 3 | 인터넷에 연결하지 않고 Panorama를 배포합니다.

이 Panorama는 SCP 서버와 통신하여 관리되는 방화벽, 로그 수집기 및 WildFire 어플라이언스에 콘텐츠 업데이트를 다운로드하고 설치합니다.

1. Panorama 관리 서버를 설정합니다.
   - M-시리즈 어플라이언스 설정
   - Panorama 가상 어플라이언스 설정
2. 초기 Panorama 구성을 수행합니다.
   - M-시리즈 어플라이언스의 초기 구성 수행
   - Panorama 가상 어플라이언스의 초기 구성 수행
3. 관리 방화벽, 로그 수집기 및 WildFire 어플라이언스를 추가하십시오.
   - 관리되는 디바이스로 방화벽 추가
   - 관리형 수집기 구성
   - Panorama로 관리할 독립 실행형 Wildfire 어플라이언스 추가

STEP 4 | SCP 서버에 콘텐츠 업데이트를 다운로드하도록 인터넷에 연결된 Panorama를 구성합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. SCP 서버 프로파일을 만듭니다.
   1. **Panorama** > 서버 프로파일 > **SCP**를 선택하고 새 SCP 서버 프로파일을 추가합니다.
   2. SCP 서버 프로파일에 대한 설명이 포함된 이름을 입력합니다.
   3. SCP 서버 IP 주소를 입력합니다.
   4. 포트를 입력합니다.
   5. SCP 서버 사용자명을 입력합니다.
   6. SCP 서버 비밀번호 및 비밀번호 확인을 입력합니다.
   7. 확인을 클릭하여 변경 사항을 저장합니다.



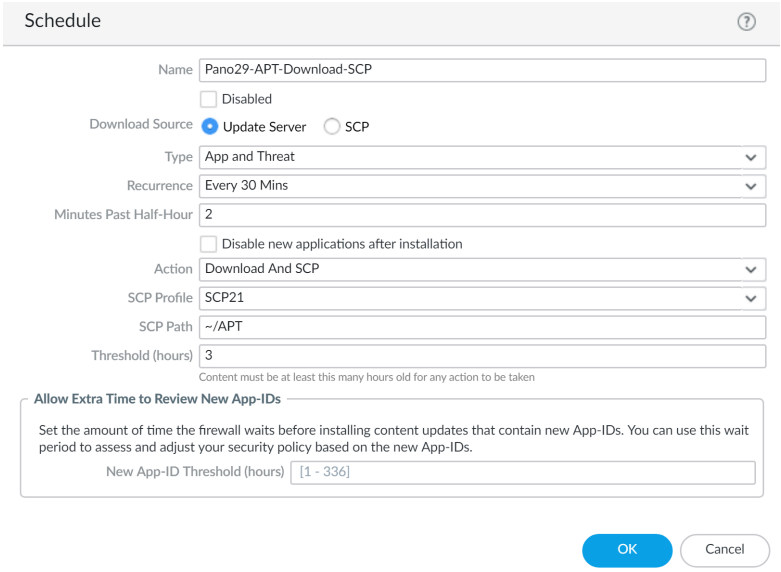
3. 콘텐츠 업데이트 일정을 만들어 SCP 서버에 콘텐츠 업데이트를 정기적으로 다운로드합니다.

   관리 방화벽, 로그 수집기 및 WildFire 어플라이언스에 자동으로 다운로드 및 설치하려는 각 콘텐츠 업데이트 유형에 대한 일정을 생성해야 합니다.

   1. **Panorama** > 디바이스 배포 > 동적 업데이트를 선택하고 일정을 선택한 다음 콘텐츠 업데이트 일정을 추가합니다.
   2. 콘텐츠 업데이트 일정을 설명하는 이름을 입력합니다.
   3. 다운로드 소스에 대해 업데이트 서버를 선택합니다.
   4. 콘텐츠 업데이트 유형을 선택합니다.
   5. Panorama가 Palo Alto Networks 업데이트 서버에서 새 콘텐츠 업데이트를 확인하는 인터벌을 설정하려면 반복을 선택합니다.

      더 정확한 반복 일정을 구성하려면 선택한 반복 인터벌 이후의 시간*(분)*을 입력합니다. 동일한 반복 인터벌을 사용하여 다운로드하도록 예약된 여러 콘텐츠 업데이트가 있는 경우 *Panorama* 및 *SCP* 서버에 과부하가 걸리지 않도록 시차를 두십시오.
   6. 작업에서 다운로드 및 **SCP**를 선택합니다.
   7. 이전 단계에서 구성한 **SCP** 프로파일을 선택합니다.
   8. 콘텐츠 업데이트 유형에 대해 **SCP** 경로를 입력합니다.

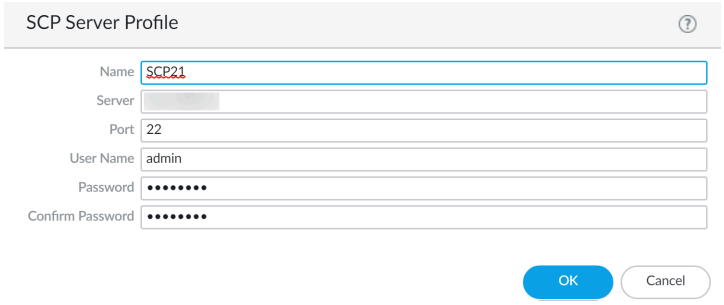
9. (선택 사항) 콘텐츠 업데이트에 대한 임계값을 시간 단위로 입력합니다. Panorama는 이 시간(또는 이전)이 지난 콘텐츠 업데이트만 다운로드합니다.
10. 확인을 클릭하여 변경 사항을 저장합니다.



4. 변경 사항을 커밋합니다.

STEP 5 | SCP 서버에서 콘텐츠 업데이트를 다운로드하도록 에어 갭 Panorama를 구성한 다음 관리 방화벽, 로그 수집기 및 WildFire 어플라이언스에 업데이트를 설치합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. SCP 서버 프로파일을 만듭니다.
   1. **Panorama** > 서버 프로파일 > **SCP**를 선택하고 새 SCP 서버 프로파일을 추가합니다.
   2. SCP 서버 프로파일에 대한 설명이 포함된 이름을 입력합니다.
   3. SCP 서버 IP 주소를 입력합니다.
   4. 포트를 입력합니다.
   5. SCP 서버 사용자명을 입력합니다.
   6. SCP 서버 비밀번호 및 비밀번호 확인을 입력합니다.
   7. 확인을 클릭하여 변경 사항을 저장합니다.



3. 콘텐츠 업데이트 일정을 만들어 SCP 서버에서 콘텐츠 업데이트를 정기적으로 다운로드하고 설치합니다.

   관리 방화벽, 로그 수집기 및 WildFire 어플라이언스에 자동으로 다운로드 및 설치하려는 각 콘텐츠 업데이트 유형에 대한 일정을 생성해야 합니다.

   1. **Panorama** > 디바이스 배포 > 동적 업데이트를 선택하고 일정을 선택한 다음 콘텐츠 업데이트 일정을 추가합니다.
   2. 콘텐츠 업데이트 일정을 설명하는 이름을 입력합니다.
   3. 다운로드 소스에 대해 **SCP**를 선택합니다.
   4. 이전 단계에서 구성한 **SCP** 프로파일을 선택합니다.
   5. 콘텐츠 업데이트 유형에 대해 **SCP** 경로를 입력합니다.
   6. 콘텐츠 업데이트 유형을 선택합니다.
   7. Panorama가 Palo Alto Networks 업데이트 서버에서 새 콘텐츠 업데이트를 확인하는 인터벌을 설정하려면 반복을 선택합니다.

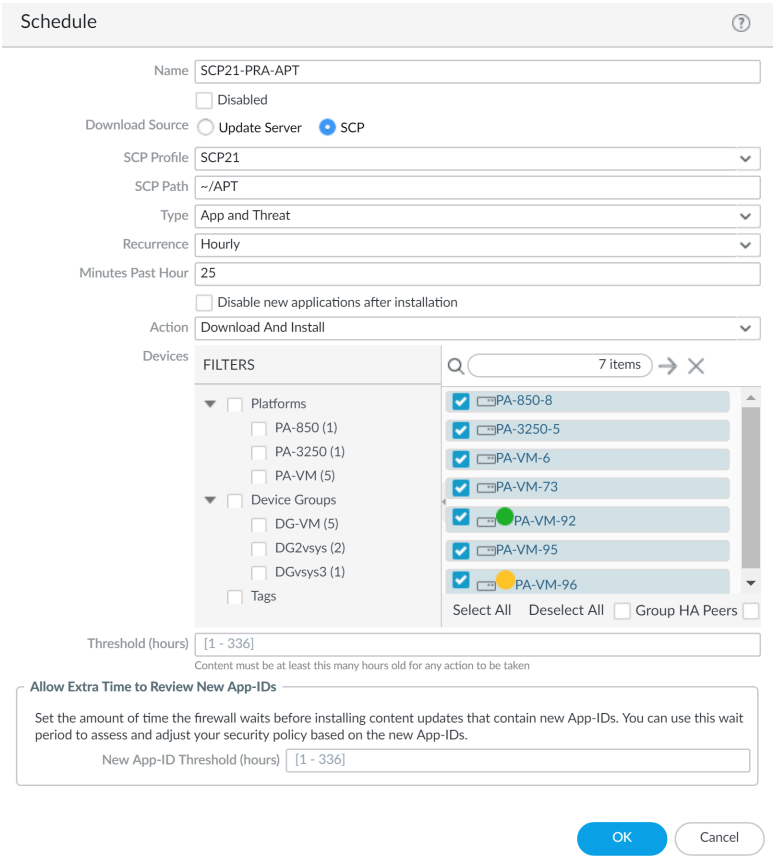
      더 정확한 반복 일정을 구성하려면 선택한 반복 인터벌 이후의 시간*(분)*을 입력합니다. 동일한 반복 인터벌을 사용하여 다운로드하도록 예약된 여러 콘텐츠 업데이트가 있는 경우 *Panorama* 및 *SCP* 서버에 과부하가 걸리지 않도록 시차를 두십시오.

8. 작업에서 다운로드 또는 다운로드 및 설치를 선택합니다.

   다운로드 소스가 ***SCP***인 경우 다운로드 및 다운로드 및 설치만 지원됩니다.

   다운로드를 선택하면 관리 방화벽에서 콘텐츠 업데이트 설치를 수동으로 시작해야 합니다.

9. 콘텐츠 업데이트를 설치할 디바이스를 선택합니다.
10. (선택 사항) 콘텐츠 업데이트에 대한 임계값을 시간 단위로 입력합니다. Panorama는 이 시간(또는 이전)이 지난 콘텐츠 업데이트만 다운로드합니다.
11. 확인을 클릭하여 변경 사항을 저장합니다.



4. 변경 사항을 커밋합니다.

HA 구성에서 Panorama 업그레이드

고가용성(HA) 구성에서 Panorama 소프트웨어를 업데이트할 때 원활한 페일오버를 보장하려면 능동형 및 수동형 Panorama 피어가 동일한 애플리케이션 데이터베이스 버전으로 동일한 Panorama 릴리스를 실행해야 합니다. 다음 예에서는 HA 쌍을 업그레이드하는 방법을 설명합니다(능동형 피어는 Primary_A이고 수동형 피어는 Secondary_B임).

Panorama 및 FIPS-CC 모드의 관리형 디바이스를 PAN-OS 10.2 또는 이전 릴리스에서 PAN-OS 11.0으로 업그레이드하는 경우, PAN-OS 10.2 릴리스를 실행하는 동안 Panorama 관리에 추가되었다면 FIPS-

CC 모드에서 디바이스의 보안 연결 상태를 재설정하는 추가 단계를 수행해야 합니다. FIPS-CC 모드에서 Panorama 및 FIPS-CC 디바이스를 업그레이드하는 방법에 대한 자세한 내용은 FIPS-CC 모드에서 Panorama 및 관리형 디바이스 업그레이드을(를) 참조하십시오.

Panorama를 업데이트하기 전에 PAN-OS 11.0에 필요한 최소 콘텐츠 릴리스 버전에 대한 릴리스 노트를 참조하십시오.

STEP 1 | Secondary_B(수동) 피어에서 Panorama 소프트웨어를 업그레이드합니다.

Secondary_B 피어에서 다음 작업 중 하나를 수행합니다. 인터넷 연결을 통해 Panorama 업그레이드

인터넷 연결 없이 Panorama 업그레이드

업그레이드 후 피어가 더 이상 동일한 소프트웨어 릴리스를 실행하지 않기 때문에 이 Panorama는 작동하지 않는 상태로 전환됩니다.

STEP 2 | (모범 사례) CDL(Cortex Data Lake)을 활용하는 경우 각 Panorama HA 피어에 Panorama 디바이스 인증서를 설치합니다.

Panorama는 PAN-OS 11.0으로 업그레이드할 때 CDL 수집 및 쿼리 엔드포인트 인증에 디바이스 인증서를 사용하도록 자동 전환됩니다.

*PAN-OS 11.0*으로 업그레이드하기 전에 디바이스 인증서를 설치하지 않으면 *Panorama*는 인증을 위해 기존 로깅 서비스 인증서를 계속 사용합니다.

STEP 3 | 페일오버를 강제 실행하려면 Primary_A 피어를 일시 중단합니다.

Primary_A 피어에서:

1. 작동 명령 섹션(**Panorama** > 고가용성)에서 로컬 **Panorama** 일시중단을 선택합니다.
2. 상태가 ## ###인지 확인합니다(웹 인터페이스의 오른쪽 하단 모서리에 표시됨).

   페일오버로 인해 Secondary_B 피어가 ## 상태로 전환되어야 합니다.

STEP 4 | Primary_A(현재 수동) 피어에서 Panorama 소프트웨어를 업그레이드합니다.

Primary_A 피어에서 다음 작업 중 하나를 수행합니다. 인터넷 연결을 통해 Panorama 업그레이드인터넷 연결 없이 Panorama 업그레이드

재부팅한 후 Primary_A 피어는 처음에 여전히 수동 상태입니다. 그런 다음 선점이 활성화된 경우(기본값) Primary_A 피어는 자동으로 활성 상태로 전환되고 Secondary_B 피어는 수동 상태로 되돌아갑니다.

선점을 비활성화한 경우 수동으로 기본 Panorama를 활성 상태로 복원합니다.

STEP 5 | 두 피어가 이제 새로 설치된 콘텐츠 릴리스 버전과 새로 설치된 Panorama 릴리스를 실행하고 있는지 확인합니다.

각 Panorama 피어의 대시보드에서 Panorama 소프트웨어 버전 및 애플리케이션 버전을 확인하고 두 피어에서 동일하며 실행 중인 구성이 동기화되었는지 확인합니다.

STEP 6 | (수집기 그룹의 로컬 Log Collector만) 수집기 그룹의 나머지 Log Collector를 업그레이드합니다.

Panorama가 인터넷에 연결되어 있을 때 로그 수집기 업그레이드Panorama가 인터넷에 연결되어 있지 않을 때 로그 수집기 업그레이드

STEP 7 | (FIPS-CC 모드의 Panorama 및 관리형 디바이스)FIPS-CC 모드에서 Panorama 및 관리형 디바이스 업그레이드.

FIPS-CC 모드에서 Panorama 및 관리형 디바이스를 업그레이드하려면 PAN-OS 11.0 릴리스를 실행하는 동안 Panorama 관리에 추가된 경우 FIPS-CC 모드에서 디바이스의 보안 연결 상태를 재설정해야 합니다. 다음 관리형 디바이스를 Panorama 관리에 다시 온보딩해야 합니다.

FIPS-CC 모드의 관리형 디바이스는 디바이스 등록 인증 키를 사용하여 Panorama에 추가됩니다.

디바이스 등록 인증 키를 사용하여 Panorama에 추가된 일반 작동 모드의 관리형 디바이스

관리형 디바이스가 PAN-OS 10.0 이하 릴리스를 실행하는 동안 Panorama 관리에 추가된 관리형 디바이스를 다시 온보딩할 필요가 없습니다.

STEP 8 | (PAN-OS 10.2 이상 릴리스) OpenSSL 보안 수준 2를 준수하려면 모든 인증서를 재생성하거나 다시 가져옵니다.

PAN-OS 10.1 또는 이전 릴리스에서 PAN-OS 11.0으로 업그레이드하는 경우 이 단계가 필요합니다. PAN-OS 10.2에서 업그레이드하고 인증서를 이미 재생성하거나 다시 가져온 경우 이 단계를 건너뛰십시오.

모든 인증서는 다음 최소 요구 사항을 충족해야 합니다.

RSA 2048비트 이상 또는 ECDSA 256비트 이상 SHA256 이상의 다이제스트

인증서 재생성 또는 다시 가져오기에 대한 자세한 내용은 PAN-OS 관리자 가이드 또는 Panorama 관리자 가이드를 참조하십시오.

STEP 9 | (Panorama 모드에 권장) Panorama 가상 어플라이언스의 메모리를 64GB로 늘립니다.

Panorama 모드의 Panorama 가상 어플라이언스를 PAN-OS 11.0으로 성공적으로 업그레이드한 후, Palo Alto Networks는 부족 프로비저닝된 Panorama 가상 어플라이언스와 관련된 로깅, 관리 및 운영 성능 문제를 방지하기 위해 증가된 시스템 요구 사항을 충족하도록 Panorama 가상 어플라이언스의 메모리를 64GB로 늘릴 것을 권장합니다.

Panorama 로그를 새 로그 형식으로 마이그레이션

Panorama 8.0 이상 릴리스로 업그레이드한 후 Panorama Log Collectors는 새로운 로그 저장 형식을 사용합니다. Panorama는 업그레이드 후 8.0 이전 릴리스 로그 형식의 로그에서 보고서 또는 ACC 데이터를 생성할 수 없으므로 Panorama 및 해당 로그 수집기를 PAN-OS® 7.1 또는 이전 릴리스에서 다음으로 업그레이드하는 즉시 기존 로그를 마이그레이션해야 합니다. PAN-OS 8.0 이상 릴리스이며 관리 방화벽을 업그레이드하기 전에 이 작업을 수행해야 합니다. Panorama는 로그 마이그레이션 중에 관리 디바이스에서 로그를 계속 수집하지만 PAN-OS 8.0 이상 릴리스로 업그레이드한 후에는 들어오는 로그를 새 로그 형식으로 저장합니다. 이러한 이유로 Panorama가 로그 마이그레이션 프로세스를 완료할 때까지 ACC 및 보고서에 부분 데이터만 표시됩니다.

새 형식으로의 로그 마이그레이션은 *PAN-OS 8.0* 이상 릴리스로 업그레이드할 때*(*또는 업그레이드 경로의 일부로 *PAN-OS 8.0*으로 업그레이드할 때*)* 수행해야 하는 일회성 작업입니다. 이후 *PAN-OS* 릴리스로 업그레이드할 때 이 마이그레이션을 다시 수행할 필요가 없습니다.

Panorama가 로그 마이그레이션 프로세스를 완료하는 데 걸리는 시간은 Panorama에 기록되는 새 로그의 양과 마이그레이션하려는 로그 데이터베이스의 크기에 따라 다릅니다. 로그 마이그레이션은 CPU를 많이 사용하는 프로세스이므로 로깅 속도가 낮은 시간에 마이그레이션을 시작하십시오. CPU 사용률이 높다는 것을 인지하게 되면 피크 시간에 마이그레이션을 중지하고 들어오는 로그 속도가 더 낮을 때 마이그레이션을 재개할 수 있습니다.

Panorama용 콘텐츠 및 소프트웨어 업데이트를 설치하고 로그 수집기를 업그레이드한 후 다음과 같이 로그를 마이그레이션합니다.

- 수신되는 로깅 속도를 봅니다.

  최상의 결과를 얻으려면 수신 로그 비율이 낮을 때 로그 마이그레이션을 시작하십시오. 속도를 확인하려면 Log Collector CLI에서 다음 명령을 실행하십시오.

  ```
  admin@FC-M500-1> debug log-collector log-collection-stats show
   incoming-logs
  ```

  로그 마이그레이션 중 높은 *CPU* 사용률*(100%*에 가까움*)*이 예상되며 작업은 계속해서 정상적으로 작동합니다. 리소스 경합이 발생할 경우 들어오는 로그 및 기타 프로세스를 위해 로그 마이그레이션이 제한됩니다.

- 각 로그 수집기의 로그를 새 형식으로 마이그레이션하기 시작합니다.

  마이그레이션을 시작하려면 각 Log Collector의 CLI에서 다음 명령을 입력하십시오.

  ```
  admin@FC-M500-1> request logdb migrate lc serial-number <ser_num>
   start
  ```

- 모든 기존 로그를 새 형식으로 마이그레이션하는 데 걸리는 시간을 예상하려면 로그 마이그레이션 상태를 확인하십시오.

  ```
  admin@FC-M500-1> request logdb migrate lc serial-number <ser_num>
   status Slot: all Migration State: ## # ###: 0.04 ## ## ##: 451##
   47#
  ```

- 로그 마이그레이션 프로세스를 중지합니다.

  로그 마이그레이션 프로세스를 일시적으로 중지하려면 Log Collector CLI에서 다음 명령을 입력합니다.

  ```
  admin@FC-M500-1 request logdb migrate lc serial-number <ser_num>
   stop
  ```

향상된 디바이스 관리 용량을 위한 Panorama 업그레이드

M-600 어플라이언스의 기존 디바이스 관리 라이선스를 사용하여 최대 5,000개의 방화벽을 관리하거나 Panorama™ 가상 어플라이언스를 사용하여 최대 2,500개의 방화벽을 관리하려면 PAN-OS 9.1 이상 릴리스로 업그레이드하십시오.

STEP 1 | Panorama 가상 어플라이언스가 향상된 디바이스 관리를 위한 최소 리소스 요구사항을 아직 충족하지 않는 경우 Panorama 가상 어플라이언스의 CPU 및 메모리를 늘립니다.

업그레이드하기 전에 기존 Panorama 가상 어플라이언스가 최소 요구사항을 충족하는지 확인하려면 증가된 디바이스 관리 용량 요구사항을 검토하십시오.

STEP 2 | Panorama CLI에 로그인합니다.

STEP 3 | Panorama가 아직 이 모드에 있지 않은 경우 Panorama 관리 서버를 관리 전용으로 변경합니다.

- (M-600 어플라이언스만 해당) 5단계부터 시작하여 M-시리즈 어플라이언스를 관리 전용 모드로 설정합니다.

또는

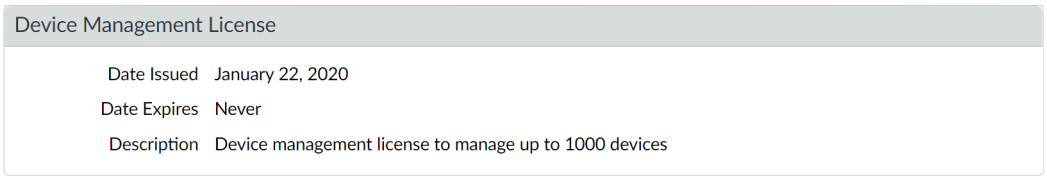
- 관리 전용 모드에서 Panorama 가상 어플라이언스를 설정합니다.

STEP 4 | Panorama 웹 인터페이스에 로그인합니다.

STEP 5 | Panorama 관리 서버를 업그레이드합니다.

- 인터넷 연결을 통해 Panorama 업그레이드.
- 인터넷 연결 없이 Panorama 업그레이드.
- HA 구성에서 Panorama 업그레이드.

STEP 6 | **Panorama** > 라이선스를 선택하고 디바이스 관리 라이선스가 성공적으로 활성화되었는지 확인합니다.



디바이스 관리 라이선스를 활성화한 다음 *PAN-OS 9.1* 이상 릴리스로 업그레이드한 경우, *M-600* 어플라이언스로 최대 *5,000*개의 방화벽을 관리하거나 *Panorama* 가상 어플라이언스로 최대 *2,500*개의 방화벽을 관리할 수 있지만 설명에는 여전히 *## 1000## ##### # ## # ## #### ## ####*가 표시됩니다.

FIPS-CC 모드에서 Panorama 및 관리형 디바이스 업그레이드

PAN-OS 11.0으로 성공적으로 업그레이드하면 FIPS-CC 모드의 모든 관리형 디바이스와 디바이스가 PAN-OS 11.0 릴리스를 실행할 때 Panorama에 추가된 모든 관리형 디바이스는 Panorama 관리에 다시 온보딩되어야 합니다. 이렇게 하려면 FIPS-CC 모드의 Panorama 및 FIPS-CC 모드의 모든 관리형 디바이스에 대한 보안 연결 상태를 재설정해야 합니다. 보안 연결 상태를 재설정한 후 디바이스 등록 인증 키를 사용하여 Panorama에 추가된 방화벽, Log Collector 및 WildFire 어플라이언스를 다시 Panorama 관리에 추가해야 합니다. 이 절차는 PAN-OS 10.0 또는 이전 릴리스를 실행하는 동안 Panorama에 추가된 관리형 디바이스에 필요하지 않으며 영향을 미치지 않습니다. 이는 FIPS-CC 모드에서 지원되는 모든 Panorama 모델 및 차세대 방화벽 하드웨어 및 VM 시리즈 모델에 필요합니다.

STEP 1 | FIPS-CC 모드에서 관리형 디바이스 목록을 만들고 디바이스 등록 인증 키를 사용하여 Panorama에 추가된 모든 관리형 디바이스를 만듭니다. 이렇게 하면 나중에 관리형 디바이스를 Panorama 관리에 다시 온보딩할 때 노력에 집중하는 데 도움이 됩니다.

STEP 2 | Panorama 및 관리형 디바이스를 PAN-OS 11.0으로 업그레이드합니다.

- 인터넷 연결을 통해 Panorama 업그레이드
- 인터넷 연결 없이 Panorama 업그레이드
- HA 구성에서 Panorama 업그레이드

STEP 3 | PAN-OS 11.0으로 성공적으로 업그레이드한 후 Panorama에서 시스템 로그를 검토하여 FIPS-CC 모드에서 Panorama에 연결할 수 없는 관리형 디바이스를 식별합니다.

STEP 4 | Panorama에서 보안 연결 상태를 재설정합니다.

이 단계는 PAN-OS 11.0 릴리스를 실행하는 동안 Panorama 관리에 추가된 모든 관리형 디바이스에 대한 연결을 재설정하며 되돌릴 수 없습니다. 이 단계는 PAN-OS 11.0으로 업그레이드된 PAN-OS 10.0 또는 이전 릴리스를 실행할 때 추가된 방화벽의 연결 상태에 영향을 미치지 않습니다.

1. Panorama CLI에 로그인합니다.
2. 보안 연결 상태를 재설정합니다.

```
admin> request sc3 reset
```

3. Panorama에서 관리 서버를 다시 시작합니다.

```
admin> ##### ### #### ## ##
```

4. (HA만 해당) 고가용성(HA) 구성의 각 피어에 대해 이 단계를 반복합니다.

STEP 5 | FIPS-CC 모드에서 관리형 디바이스의 보안 연결 상태를 재설정합니다.

이 단계는 관리형 디바이스 연결을 재설정하며 되돌릴 수 없습니다.

1. 관리 디바이스 CLI에 로그인합니다.
   - 방화벽 CLI에 로그인
   - Log Collector CLI에 로그인
   - WildFire 어플라이언스 CLI에 로그인
2. 보안 연결 상태를 재설정합니다.

```
admin> request sc3 reset
```

3. 관리되는 디바이스에서 관리 서버를 다시 시작합니다.

```
admin> ##### ### #### ## ##
```

STEP 6 | 영향을 받는 관리형 디바이스를 Panorama에 다시 추가합니다.

- 관리되는 디바이스로 방화벽 추가
- 관리형 수집기 구성
- Panorama로 관리할 독립형 WildFire 어플라이언스 추가

STEP 7 | OpenSSL 보안 수준 2를 준수하도록 모든 인증서를 재생성하거나 다시 가져옵니다.

PAN-OS 11.0으로 업그레이드할 때는 모든 인증서가 다음과 같은 최소 요구 사항을 충족해야 합니다.

- RSA 2048비트 이상 또는 ECDSA 256비트 이상
- SHA256 이상의 다이제스트

PAN-OS 관리자 가이드를 참조하거나 인증서 재생성 또는 다시 가져오기에 대한 자세한 내용은 Panorama 관리자 가이드를 참조하십시오.

Panorama 11.0에서 다운그레이드

PAN-OS® 11.0에는 Panorama 및 관리형 디바이스에 대한 인라인 딥 러닝, 단순화된 소프트웨어 업그레이드 및 다운그레이드를 활용하여 여러 PAN-OS 릴리스에서 관리형 디바이스를 업그레이드하는 운영 부담을 줄이는 제로 데이 익스플로잇 방지를 위한 고급 위협 방지 지원이 도입되었습니다. AIOps를 사용하는 BPA(Practice Assessment)를 통해 손상된 보안 상태로 인한 노출을 추가로 제거하고 온프레미스 웹 프록시를 사용하여 보안 또는 효율성을 희생하지 않고 클라우드로 전환하는 데 도움을 주며 IPv6 주소를 얻기 위한 상태 저장 DHCPv6 클라이언트에 대한 방화벽 지원, 사용자에 대한 가시성 향상 Cloud Identity Engine(CIE)에 대한 컨텍스트, 관리 액세스를 위한 TLSv1.3 지원, 향상된 IoT 보안 정책 규칙 권장 사항을 통해 정책 규칙 권장 사항을 더 쉽게 확장하고 관리할 수 있습니다. Panorama 11.0 릴리스를 실행하는 Log Collector 및 Panorama를 이전 기능 릴리스로 다운그레이드하기 전에 다음 워크플로를 사용하여 방화벽을 다운그레이드합니다. 이 절차는 로컬 Log Collector를 관리할 때 Panorama와 하나 이상의 Dedicated Log Collector를 관리할 때 Panorama에서 모두 작동합니다.

*PAN-OS 11.0*에서 이전 *PAN-OS* 릴리스로 다운그레이드하려면 대상 *PAN-OS* 릴리스로 다운그레이드 경로를 계속하기 전에 기본 *PAN-OS 10.2* 이상 *PAN-OS 10.2* 릴리스를 다운로드하여 설치해야 합니다. *PAN-OS 10.1* 또는 이전 *PAN-OS* 릴리스로 다운그레이드를 시도하면 *PAN-OS 11.0*에서 다운그레이드가 실패합니다.

Palo Alto Networks 호환성 매트릭스를 검토하여 다운그레이드하려는 방화벽 및 어플라이언스가 다운그레이드하려는 *PAN-OS* 릴리스와 호환되는지 확인하십시오. 다운그레이드할 수 있는 방화벽 및 어플라이언스의 경우 다운그레이드 고려 사항도 검토하여 다운그레이드 후 달라지거나 사용할 수 없는 모든 기능 및 구성 설정을 고려해야 합니다.

STEP 1 | Panorama 웹 인터페이스에 로그인합니다.

STEP 2 | Panorama 및 관리 디바이스에 대한 구성 파일의 백업을 저장합니다.

1. **Panorama** 및 디바이스 구성 스냅샷을 내보냅니다(**Panorama** > 설정 > 작업).
2. 내보낸 .tgz 파일을 Panorama, Log Collectors 및 방화벽 외부의 위치에 저장합니다. 다시 시작해야 하는 문제가 발생한 경우 이 백업을 사용하여 구성을 복원할 수 있습니다.

STEP 3 | 전용 Log Collector에 대한 인증을 구성하고 `admin` 관리자를 제거한 경우 새 `admin` 사용자를 구성하고 전용 Log Collector에 푸시합니다.

PAN-OS 9.1 및 이전 릴리스로 다운그레이드하려면 전용 로그 수집기에 `admin` 사용자가 구성되어 있어야 합니다.

STEP 4 | **Panorama** > **Plugins**를 선택하고 현재 Panorama에 설치된 모든 플러그인에 대해 PAN-OS 10.2에서 지원되는 플러그인 버전을 다운로드합니다.

PAN-OS 10.2 및 이전 릴리스에서 지원되는 Panorama 플러그인 버전은 Panorama 플러그인 호환성 매트릭스를 참조하십시오.

이는 Panorama를 PAN-OS 11.0에서 PAN-OS 10.2 및 이전 릴리스로 성공적으로 다운그레이드하는 데 필요합니다. 다운로드한 플러그인 버전은 PAN-OS 10.2로 다운그레이드하는 동안 자동으로 설치됩니다. 지원되는 플러그인 버전이 다운로드되지 않은 경우 PAN-OS 10.2로의 다운그레이드가 차단됩니다.

*(ZTP 플러그인만 해당) Panorama*를 *PAN-OS 10.2*로 성공적으로 다운그레이드하려면 다운그레이드 프로세스를 시작하기 전에 ZTP 플러그인을 제거해야 합니다. *PAN-OS 10.2*로 성공적으로 다운그레이드한 후 *Panorama*에 *ZTP* 플러그인을 다시 설치해야 합니다.

STEP 5 | PAN-OS 11.0 릴리스를 실행하는 각 방화벽을 다운그레이드합니다.

*PAN-OS 11.0*에서 이전 기능 릴리스로 다운그레이드하려면 먼저 기본 *PAN-OS 10.2* 릴리스 또는 이후 *PAN-OS 10.2* 릴리스로 다운그레이드해야 합니다. 기본 *PAN-OS 10.2* 이상 *PAN-OS 10.2* 릴리스로 다운그레이드한 후 대상 *PAN-OS* 버전으로 계속 다운그레이드할 수 있습니다.

*2*개 이상의 방화벽을 다운그레이드하는 경우 다운그레이드를 시작하기 전에 각 방화벽별 *PAN-OS 10.2* 이미지를 *Panorama*로 다운로드하여 프로세스를 간소화합니다. 예를 들어, *PA-220* 방화벽을 *PAN-OS 10.2*로 다운그레이드하려면 `PanOS_220-10.2.0` 또는 `PanOS_3000-10.2.0` 이미지를 다운로드합니다.

Panorama를 사용하려면 모든 방화벽이 동일하거나 이전 PAN-OS 릴리스를 실행해야 합니다. 따라서 Panorama를 다운그레이드하기 전에 환경에 따라 아래의 적절한 작업을 사용하고 반복하여 필요에 따라 모든 관리형 방화벽을 다운그레이드하십시오.

1. 사용 가능한 이미지를 지금 확인합니다(**Panorama** > 디바이스 배포 > 소프트웨어).
2. 다운그레이드할 각 모델 또는 일련의 방화벽에 대한 PAN-OS 10.2 이미지를 찾습니다. 이미지가 아직 다운로드되지 않은 경우 다운로드합니다.

비 **HA** 방화벽

설치(작업 열) 적절한 PAN-OS 10.2 버전을 다운그레이드할 모든 방화벽을 선택하고 설치 후 디바이스 재부팅을 선택한 다음 확인을 클릭합니다.

능동형/능동형 **HA** 방화벽

1. 설치를 클릭하고 그룹 **HA** 피어를 비활성화(지우기)하고 HA 피어 중 하나를 선택한 후 설치 후 디바이스 재부팅을 선택하고 확인을 클릭합니다. 계속하기 전에 방화벽이 재부팅을 마칠 때까지 기다리십시오.
2. 설치를 클릭하고 그룹 **HA** 피어를 비활성화(지우기)하고 이전 단계에서 업데이트하지 않은 HA 피어를 선택한 후 설치 후 디바이스 재부팅을 선택하고 확인을 클릭합니다.

능동형/수동형 **HA** 방화벽

이 예에서 능동형 방화벽의 이름은 fw1이고 수동 방화벽의 이름은 fw2입니다.

1. 적절한 업데이트를 설치(작업 열)하고, 그룹 **HA** 피어를 비활성화(지우기)한 다음, fw2를 선택하고, 설치 후 디바이스 재부팅을 선택한 후 확인을 클릭합니다.
2. fw2가 재부팅을 완료한 후 fw1(대시보드 > 고가용성 위젯)이 여전히 활성 피어이고 fw2가 여전히 수동 피어인지 확인합니다(로컬 방화벽 상태는 ##이고 피어(fw2)는 ##).
3. fw1에 액세스하고 로컬 디바이스 일시 중단(디바이스 > 고가용성 > 작동 명령).
4. fw2(대시보드 > 고가용성)에 액세스하고 로컬 방화벽 상태가 ##인지 확인하고 피어 방화벽(fw1)은 ## ##인지 확인합니다.

5. Panorama에 액세스하고 **Panorama** > 디바이스 배포 > 소프트웨어, 설치(Action 열) 적절한 업데이트를 선택하며 그룹 **HA** 피어를 비활성화(지우기)한 후 fw1을 선택하고 설치 후 디바이스 재부팅을 선택하며 확인을 클릭합니다. 계속하기 전에 fw1이 재부팅을 마칠 때까지 기다리십시오.
6. fw1(대시보드 > 고가용성 위젯)에 액세스하고 로컬 방화벽 상태가 ##이고 피어(fw2)가 ##인지 확인합니다.

   일렉션*(election)* 설정*(*디바이스 > 고가용성 > 일반*)*에서 선점을 활성화한 경우 재부팅 후 *fw1*이 활성 피어로 복원됩니다.

STEP 6 | Panorama 11.0을 실행하는 각 Log Collector를 다운그레이드합니다.

*PAN-OS 11.0*에서 이전 기능 릴리스로 다운그레이드하려면 먼저 기본 *PAN-OS 10.2* 이상 *PAN-OS 10.2* 릴리스로 다운그레이드해야 합니다. 기본 *PAN-OS 10.2* 이상 *PAN-OS 10.2* 릴리스로 다운그레이드한 후 대상 *PAN-OS* 버전으로 계속 다운그레이드할 수 있습니다.

1. 사용 가능한 이미지를 지금 확인합니다(**Panorama** > 디바이스 배포 > 소프트웨어).
2. Panorama 10.2 이미지를 찾습니다. 이미지가 아직 다운로드되지 않은 경우 다운로드합니다(작업 열).
3. 다운로드가 완료되면 Panorama 10.2를 실행하는 각 Log Collector에 이미지를 설치합니다. 업그레이드가 완료되면 디바이스를 자동으로 재부팅하려면 설치 후 디바이스 재부팅을 선택합니다.

STEP 7 | Panorama 다운그레이드.

*PAN-OS 11.0*에서 이전 기능 릴리스로 다운그레이드하려면 먼저 기본 *PAN-OS 10.2* 이상 *PAN-OS 10.2* 릴리스로 다운그레이드해야 합니다. 기본 *PAN-OS 10.2* 이상 *PAN-OS 10.2* 릴리스로 다운그레이드한 후 대상 *PAN-OS* 버전으로 계속 다운그레이드할 수 있습니다.

1. 사용 가능한 이미지를 보려면 **Panorama** > 소프트웨어 및 지금 확인을 선택합니다.
2. Panorama 10.2 이미지를 찾습니다. 이미지가 아직 다운로드되지 않은 경우 다운로드합니다.
3. 다운로드가 완료되면 Panorama에 이미지를 설치합니다.
4. 다음과 같이 Panorama를 재부팅합니다.
   - 재부팅하라는 메시지가 표시되면 예를 클릭합니다. **CMS** 로그인 프롬프트가 표시되면 사용자명이나 암호를 입력하지 않고 Enter 키를 누릅니다. Panorama 로그인 프롬프트가 나타나면 초기 구성 시 설정한 사용자명과 비밀번호를 입력합니다.
   - 재부팅하라는 메시지가 표시되지 않으면 **Panorama** > 설정 > 작업을 선택하고 **Panorama** 재부팅(디바이스 작업)을 클릭합니다.

STEP 8 | (ZTP 플러그인만 해당) ZTP 플러그인을 다시 설치합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. ZTP 플러그인을 설치합니다.
3. **Panorama** > 제로 터치 프로비저닝을 선택하고 **ZTP**를 선택(활성화)합니다.

Panorama 업그레이드 문제 해결

Panorama 업그레이드 문제를 해결하려면 다음 표를 사용하여 가능한 문제와 해결 방법을 검토하십시오.

증상	해결
소프트웨어 보증 라이선스가 만료되었습니다.	CLI에서 만료된 라이선스 키를 삭제합니다. 1. ## #### #입력 <software license key>. 2. **delete license key Software_Warranty<expiredate>.key**를 입력합니다.
최신 PAN-OS 소프트웨어 버전을 사용할 수 없습니다.	현재 설치된 버전보다 이전 릴리스인 소프트웨어 버전만 볼 수 있습니다. 예를 들어 8.1 릴리스가 설치된 경우 9.0 릴리스만 사용할 수 있습니다. 9.1 릴리스를 보려면 먼저 9.0으로 업그레이드해야 합니다.
(레거시 모드의 Panorama 가상 어플라이언스만 해당) 업그레이드 버전이 소프트웨어 관리자로 미리 로드하지 못했습니다.	이 문제는 사용 가능한 리소스가 충분하지 않을 때 발생합니다. 가상 머신 용량을 늘리거나 레거시 모드에서 Panorama 모드로 마이그레이션할 수 있습니다.

Panorama를 사용하여 방화벽, 로그 수집기 및 WildFire 어플라이언스에 대한 업그레이드 배포

Panorama™를 사용하면 나머지 관리 대상 디바이스에 업데이트를 설치하기 전에 방화벽, 전용 로그 수집기 또는 WildFire® 디바이스 및 디바이스 클러스터의 하위 집합에 배포하여 소프트웨어 및 콘텐츠 업데이트를 검증할 수 있습니다. 정기적인 콘텐츠 업데이트를 예약하려면 Panorama에 직접 인터넷 연결이 필요합니다. 요청 시(예약되지 않은) 소프트웨어 또는 콘텐츠 업데이트를 배포하는 절차는 Panorama가 인터넷에 연결되어 있는지의 여부에 따라 다릅니다. 예약된 업데이트 프로세스가 시작되었거나 5분 이내에 시작될 때 콘텐츠 업데이트를 수동으로 배포하면 Panorama에 경고가 표시됩니다.

업데이트를 배포할 때 Panorama는 관리 대상 디바이스(방화벽, 로그 수집기 및 WildFire 디바이스)에 업데이트가 있음을 알리고 디바이스는 Panorama에서 업데이트 패키지를 검색합니다. 기본적으로 관리 대상 디바이스는 Panorama의 관리(MGT) 인터페이스를 통해 업데이트를 검색합니다. 그러나 어플라이언스가 업데이트를 검색하도록 다른 인터페이스를 사용하여 MGT 인터페이스의 트래픽 부하를 줄이려면 다중 인터페이스를 사용하도록 Panorama를 구성할 수 있습니다.

Panorama를 사용하여 하나 이상의 방화벽에 대한 콘텐츠 버전을 이전에 설치된 콘텐츠 버전으로 빠르게 되돌릴 수 있습니다. 방화벽에 새 콘텐츠 버전이 설치된 후 새로 설치된 콘텐츠 버전이 네트워크 작업을 불안정하게 하거나 방해하는 경우 이전에 설치된 버전으로 되돌릴 수 있습니다.

기본적으로 각 유형의 소프트웨어 또는 콘텐츠 업데이트를 최대 *2*개까지 *Panorama*에 다운로드할 수 있습니다. 최대값을 초과하여 다운로드를 시작하면 *Panorama*는 선택한 유형의 가장 오래된 업데이트를 삭제합니다. 최대값을 변경하려면 소프트웨어 및 콘텐츠 업데이트를 위한 Panorama Storage 관리를 참조하십시오.

- Panorama가 다른 디바이스에 어떤 업데이트를 푸시할 수 있습니까?
- Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성
- Panorama를 사용하여 콘텐츠 업데이트 예약
- Panorama가 인터넷에 연결되어 있을 때 방화벽 업그레이드
- Panorama가 인터넷에 연결되어 있지 않을 때 방화벽 업그레이드
- Panorama가 인터넷에 연결되어 있을 때 로그 수집기 업그레이드
- Panorama가 인터넷에 연결되어 있지 않을 때 로그 수집기 업그레이드
- 인터넷 연결을 통해 Panorama에서 WildFire 클러스터 업그레이드
- 인터넷 연결 없이 Panorama에서 WildFire 클러스터 업그레이드
- ZTP 방화벽 업그레이드
- Panorama에서 콘텐츠 업데이트 되돌리기

Panorama가 다른 디바이스에 어떤 업데이트를 푸시할 수 있습니까?

설치할 수 있는 소프트웨어 및 콘텐츠 업데이트는 각 방화벽, Log Collector, WildFire® 어플라이언스 및 어플라이언스 클러스터에서 활성화된 구독에 따라 다릅니다.

어플라이언스 유형	소프트웨어 업데이트	콘텐츠 업데이트
로그 수집기	Panorama™	애플리케이션(로그 수집기는 위협 서명이 필요하지 않음) 바이러스 백신 WildFire®
방화벽	PAN-OS® GlobalProtect™ 에이전트/앱	애플리케이션 애플리케이션 및 위협 바이러스 백신 WildFire
WildFire	PAN-OS VM 이미지	WildFire

Panorama를 사용하여 콘텐츠 업데이트 예약

Panorama™는 방화벽, 로그 수집기, WildFire® 어플라이언스 및 어플라이언스 클러스터에서 지원되는 업데이트를 예약하려면 인터넷에 직접 연결해야 합니다. 그렇지 않으면 주문형 업데이트만 수행할 수 있습니다. (로그 수집기에 대한 바이러스 백신, WildFire 또는 BrightCloud URL 업데이트를 예약하려면 로그 수집기가 Panorama 7.0.3 이상의 버전을 실행하고 있어야 합니다.) 업데이트를 수신하는 각 방화벽, 로그 수집기 또는 WildFire 어플라이언스 또는 어플라이언스 클러스터는 설치 성공(구성 로그) 또는 실패(시스템 로그)를 나타내는 로그를 생성합니다. Panorama 관리 서버에서 업데이트를 예약하려면 인터넷 연결을 통해 Panorama 업데이트 설치를 참조하십시오.

업데이트를 배포하기 전에 콘텐츠 릴리스 버전 호환성에 대한 중요한 세부정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조합니다. *Panorama* 릴리스를 위해 설치해야 하는 최소 콘텐츠 릴리스 버전은 릴리스 노트를 참조하십시오.

*Panorama*는 동일한 유형의 업데이트에 대해 한 번에 하나의 업데이트만 다운로드할 수 있습니다. 동일한 유형의 업데이트를 같은 시간 반복 동안 여러 번 다운로드하도록 예약하면 첫 번째 다운로드만 성공합니다.

방화벽이 *Palo Alto Networks*® 업데이트 서버에 직접 연결되는 경우, *Panorama* 템플릿(디바이스 > 동적 업데이트)을 사용하여 콘텐츠 업데이트 일정을 방화벽에 푸시할 수도 있습니다. 업데이트가 릴리스된 후 일정 기간 동안 업데이트 설치를 지연시키려면 템플릿을 사용하여 일정을 배포해야 합니다. 드문 경우지만 콘텐츠 업데이트에 오류가 포함됩니다. 지연을 지정하면 *Palo Alto Networks*가 방화벽을 설치하기 전에 업데이트 서버에서 해당 업데이트를 식별하고 제거할 가능성이 높아집니다.

예약하려는 각 업데이트 유형에 대해 다음 단계를 수행합니다.

STEP 1 | **Panorama** > 디바이스 배포 > 동적 업데이트를 선택하고 일정을 클릭한 다음 일정을 추가합니다.

STEP 2 | 이름(일정 식별용), 업데이트 유형 및 업데이트 빈도(반복)를 지정합니다. 빈도 옵션은 업데이트 유형에 따라 다릅니다.

PAN-OS®는 업데이트 예약에 *Panorama* 시간대를 사용합니다.

유형을 앱 및 위협으로 설정하면 로그 수집기가 위협 콘텐츠가 아닌 애플리케이션 콘텐츠만 설치하고 이를 필요로 합니다. 방화벽은 애플리케이션과 위협 콘텐츠를 모두 사용합니다. 자세한 내용은 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조합니다.

STEP 3 | 다음 일정 작업 중 하나를 선택한 다음 방화벽 또는 로그 수집기를 선택합니다.

- 다운로드 및 설치(모범 사례) - 디바이스(방화벽), 로그 수집기 또는 **WildFire** 어플라이언스 및 클러스터를 선택합니다.
- 다운로드 전용 - Panorama는 업데이트를 다운로드하지만 설치하지는 않습니다.

STEP 4 | 확인을 클릭합니다.

STEP 5 | 커밋 > **Panorama**에 커밋을 선택한 다음 변경사항을 커밋합니다.

Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성

최상의 결과를 얻으려면 다음 Panorama™ 호환성 지침을 따르십시오.

- Panorama 관리 서버와 전용 로그 수집기 모두에 동일한 Panorama 릴리스를 설치합니다.
- Panorama는 관리하는 방화벽과 같거나 이후 버전의 PAN-OS를 실행해야 합니다. 자세한 내용은 Panorama 관리 호환성을 참조하십시오.

  방화벽을 PAN-OS 11.0으로 업그레이드하기 전에 먼저 Panorama를 11.0으로 업그레이드해야 합니다.
- PAN-OS 11.0을 실행하는 Panorama는 동일하거나 이전 PAN-OS 릴리스를 실행하는 WildFire® 어플라이언스 및 WildFire 어플라이언스 클러스터를 관리할 수 있습니다. 자세한 내용은 Panorama 관리 호환성을 참조하십시오.

  Panorama 관리 서버, Wildfire 어플라이언스 및 Wildfire 어플라이언스 클러스터는 동일한 PAN-OS 릴리스를 실행하는 것이 좋습니다.
- Panorama 관리 서버의 콘텐츠 릴리스 버전은 전용 로그 수집기 또는 관리되는 방화벽의 콘텐츠 릴리스 버전과 같거나 이전 버전이어야 합니다. 자세한 내용은 Panorama 관리 호환성을 참조하십시오.

  Palo Alto Networks®는 전용 로그 수집기 및 방화벽에서와 동일한 애플리케이션 데이터베이스 버전을 *Panorama*에 설치할 것을 권장합니다.

  구독에 애플리케이션 데이터베이스 또는 애플리케이션 및 위협 데이터베이스가 포함되는지의 여부와 관계없이 Panorama는 애플리케이션 데이터베이스만 설치합니다. Panorama 및 Dedicated Log Collectors는 정책 규칙을 적용하지 않으므로 위협 데이터베이스에서 위협 서명이 필요하지 않습니다. 애플리케이션 데이터베이스에는 관리되는 방화벽에 푸시할 정책 규칙을 정의하고 로그 및 보고서의 위협 정보를 해석할 때 Panorama 및 Dedicated Log Collectors에서 사용하는 위협 메타데이터(예: 위협 ID 및 이름)가 포함되어 있습니다. 그러나 방화벽은 로그에 기록된 식별자를 해당 위협, URL 또는 애플리케이션 이름과 일치시키기 위해 전체 애플리케이션 및 위협 데이터베이스가 필요합니다. Panorama 릴리스에 필요한 최소 콘텐츠 릴리스 버전은 릴리스 노트를 참조하십시오.

Panorama가 인터넷에 연결되어 있을 때 로그 수집기 업그레이드

Log Collector에 설치할 수 있는 소프트웨어 또는 콘텐츠 업데이트 목록은 지원되는 업데이트를 참조합니다.

*PAN-OS 8.1*에서 업그레이드하는 경우 *PAN-OS 9.0*은 로컬 및 전용 로그 수집기에 대한 새로운 로그 데이터 형식을 도입했습니다. *PAN-OS 10.1*로의 업그레이드 경로에서 기존 로그 데이터는 *PAN-OS 8.1*에서 *PAN-OS 9.0*으로 업그레이드할 때 자동으로 새 로그 데이터 형식으로 마이그레이션됩니다.

로그 데이터 손실을 방지하려면 수집기 그룹의 모든 로그 수집기를 동시에 업그레이드해야 합니다. 수집기 그룹의 로그 수집기가 모두 동일한 PAN-OS 버전을 실행하지 않는 경우 로그 포워딩 또는 로그 수집이 발생하지 않습니다. 또한 수집기 그룹의 로그 수집기에 대한 로그 데이터는 모든 로그 수집기가 동일한 PAN-OS 버전을 실행할 때까지 **ACC** 또는 모니터 탭에 표시되지 않습니다. 예를 들어 수집기 그룹에 세 개의 로그 수집기가 있고 두 개의 로그 수집기를 업그레이드하는 경우 수집기 그룹의 로그 수집기로 로그가 포워딩되지 않습니다.

Palo Alto Networks는 유지 관리 기간 동안 로그 수집기를 업그레이드할 것을 권장합니다. 로그 형식 마이그레이션으로 인해 전체 업그레이드 절차는 로컬 및 전용 로그 수집기의 로그 데이터 양에 따라 추가 시간이 걸립니다.

STEP 1 | Log Collector를 업그레이드하기 전에 Panorama 관리 서버에서 적절한 Panorama™ 소프트웨어 릴리스를 실행하고 있는지 확인하십시오.

Palo Alto Networks®는 *Panorama* 및 *Log Collector*가 동일한 소프트웨어 릴리스 버전을 실행하고 *Panorama*, *Log Collectors* 및 모든 관리 방화벽이 동일한 콘텐츠 릴리스 버전을 실행할 것을 적극 권장합니다. 중요한 소프트웨어 및 콘텐츠 호환성 세부정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조합니다.

Panorama는 Log Collectors와 동일한(또는 이후) 소프트웨어 릴리스를 실행해야 하지만 동일하거나 이후의 콘텐츠 릴리스 버전이 있어야 합니다.

- 소프트웨어 릴리스 버전 - Panorama 관리 서버에서 Log Collector를 업데이트할 릴리스와 같거나 이후의 소프트웨어 릴리스를 이미 실행하고 있지 않은 경우 Log Collector를 업데이트하기 전에 Panorama에 동일하거나 이후 버전의 Panorama 릴리스를 설치해야 합니다(Panorama용 콘텐츠 업데이트 및 소프트웨어 업그레이드 설치 참조).
- 콘텐츠 릴리스 버전 - 콘텐츠 릴리스 버전의 경우 모든 Log Collector가 최신 콘텐츠 릴리스 버전을 실행하고 있는지 또는 최소한 Panorama에서 실행되는 것보다 최신 버전을 실행하고 있는지 확인해야 합니다. Panorama 관리 서버에서 콘텐츠 릴리스 버전을 업데이트하기 전에 먼저 방화벽을 Panorama에서 PAN-OS 11.0으로 업그레이드한 다음 Log Collector를 업데이트합니다.

소프트웨어 및 콘텐츠 버전을 확인하려면:

- **Panorama** 관리 서버 - Panorama 관리 서버에서 실행 중인 소프트웨어 및 콘텐츠 버전을 확인하려면 Panorama 웹 인터페이스에 로그인하고 일반 정보 설정(대시보드)으로 이동합니다.
- 로그 수집기 - 로그 수집기에서 실행 중인 소프트웨어 및 콘텐츠 버전을 확인하려면 각 로그 수집기의 CLI에 로그인하고 **`show system info`** 명령을 실행합니다.

STEP 2 | PAN-OS 11.0으로의 업그레이드 경로 결정.

현재 실행 중인 PAN-OS 버전에서 PAN-OS 11.0.0으로의 경로에 있는 릴리스 버전의 설치를 건너뛸 수 없습니다.

업그레이드 경로의 일부로 통과하는 각 릴리스에 대한 릴리스 노트 및 다운그레이드 고려 사항의 알려진 문제 및 기본 동작에 대한 변경 사항은 PAN-OS 업그레이드 점검표에서 확인할 수 있습니다.

STEP 3 | 최신 콘텐츠 업데이트를 설치합니다.

Panorama 소프트웨어 릴리스에 필요한 최소 콘텐츠 릴리스 버전은 릴리스 노트를 참조하십시오.

1. Panorama 웹 인터페이스에 로그인합니다.
2. 최신 업데이트를 보려면 **Panorama** > 디바이스 배포 > 동적 업데이트 및 지금 확인을 선택합니다. 업데이트가 있으면 작업 열에 다운로드 링크가 표시됩니다.
3. 아직 설치하지 않은 경우 적절한 콘텐츠 업데이트를 다운로드합니다. 다운로드에 성공하면 작업 열의 링크가 다운로드에서 설치로 변경됩니다.
4. 다른 업데이트보다 먼저 콘텐츠 업데이트(애플리케이션 및 위협 업데이트)를 설치합니다.

   구독에 애플리케이션 및 위협 콘텐츠가 모두 포함되어 있는 경우 먼저 # 콘텐츠를 설치합니다. 그러면 애플리케이션 및 위협 콘텐츠가 모두 자동으로 설치됩니다.

   구독에 애플리케이션 및 위협 콘텐츠가 모두 포함되어 있는지의 여부와 관계없이 *Panorama*는 애플리케이션 콘텐츠만 설치하고 이를 필요로 합니다. 자세한 내용은 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조합니다.
5. 필요에 따라 다른 업데이트(바이러스 백신, WildFire 또는 URL 필터링)에 대해 위에서 명시한 하위 단계를 순서에 상관없이 한 번에 하나씩 반복합니다.

STEP 4 | PAN-OS 11.0으로의 업그레이드 경로에 따라 Log Collector를 PAN-OS 릴리스로 업그레이드합니다.

둘 이상의 *Log Collector*를 업그레이드하는 경우 이미지 다운로드를 시작하기 전에 업그레이드하려는 모든 *Log Collector*의 업그레이드 경로를 결정하여 프로세스를 간소화하십시오.

1. Panorama가 인터넷에 연결된 경우 Log Collector를 PAN-OS 8.1로 업그레이드합니다.
2. Panorama가 인터넷에 연결된 경우 Log Collector를 PAN-OS 9.0으로 업그레이드합니다.

   PAN-OS 9.0은 새로운 로그 형식을 도입했습니다. Log Collector를 PAN-OS 9.0으로 성공적으로 업그레이드하면 로그가 자동으로 새 형식으로 마이그레이션됩니다.

   자동 로그 마이그레이션이 성공적으로 완료되었는지 확인할 때까지 업그레이드 경로를 계속 진행하지 마십시오.
3. Panorama가 인터넷에 연결된 경우 Log Collector를 PAN-OS 9.1로 업그레이드합니다.
4. Panorama가 인터넷에 연결된 경우 Log Collector를 PAN-OS 10.0으로 업그레이드합니다.
5. Panorama가 인터넷에 연결된 경우 Log Collector를 PAN-OS 10.1로 업그레이드합니다.

   PAN-OS 11.0에서는 새로운 로그 형식이 도입되었습니다. PAN-OS 11.0에서 PAN-OS 10.1로 업그레이드할 때 PAN-OS 8.1 또는 이전 릴리스에서 생성된 로그를 마이그레이션하도록 선택할 수 있습니다. 그렇지 않으면 이러한 로그는 PAN-OS 10.1로 성공적으로 업그레이드될 때 자동으로 삭제됩니다. 마이그레이션 중에는 ACC 또는 모니터 탭에 로그 데이터가 표시되지 않습니다.

마이그레이션이 진행되는 동안 로그 데이터는 적절한 Log Collector로 계속 포워딩되지만 성능에 약간의 영향을 미칠 수 있습니다.

6. Panorama가 인터넷에 연결된 경우 Log Collector를 PAN-OS 10.2로 업그레이드합니다.

STEP 5 | Log Collector를 PAN-OS 11.0으로 업그레이드합니다.

1. Panorama에서 지금 확인(**Panorama** > 디바이스 배포 > 소프트웨어)에서 최신 업데이트를 확인합니다. 업데이트가 있으면 작업 열에 다운로드 링크가 표시됩니다.
2. PAN-OS 11.0 릴리스의 릴리스 버전에 대한 모델별 파일을 다운로드합니다. 예를 들어, M 시리즈 어플라이언스를 Panorama 11.0.0으로 업그레이드하려면 `Panorama_m-11.0.0` 이미지를 다운로드합니다.

   다운로드에 성공하면 해당 이미지에 대한 작업 열이 다운로드에서 설치로 변경됩니다.
3. PAN-OS 11.0을 설치하고 적절한 Log Collector를 선택합니다.
4. 필요에 따라 다음 중 하나를 선택하십시오.
   - 디바이스에만 업로드**(**설치하지 않음**)**.
   - 설치 후 기기 재부팅.
5. 확인을 클릭하여 업로드 또는 설치를 시작합니다.

STEP 6 | Log Collector에 설치된 소프트웨어 및 콘텐츠 업데이트 버전을 확인하십시오.

`show system info` 작동 명령을 입력합니다. 출력은 다음과 유사합니다.

```
sw-version: 11.0.0 app-version: 8270-6076 app-release-date:
 2020/05/08 18:21:51
```

STEP 7 | (FIPS-CC 모드만 해당)FIPS-CC 모드에서 Panorama 및 관리형 디바이스 업그레이드.

전용 Log Collector가 PAN-OS 11.0 릴리스를 실행하는 동안 전용 Log Collector를 Panorama 관리에 추가한 경우 FIPS-CC 모드에서 전용 Log Collector를 업그레이드하려면 보안 연결 상태를 재설정해야 합니다.

전용 Log Collector가 PAN-OS 10.0 이하 릴리스를 실행하는 동안 Panorama 관리에 추가된 전용 Log Collector를 다시 온보딩할 필요가 없습니다.

STEP 8 | (PAN-OS 10.2 이상 릴리스) OpenSSL 보안 수준 2를 준수하려면 모든 인증서를 재생성하거나 다시 가져옵니다.

PAN-OS 10.1 또는 이전 릴리스에서 PAN-OS 11.0으로 업그레이드하는 경우 이 단계가 필요합니다. PAN-OS 10.2에서 업그레이드하고 이미 인증서를 재생성했거나 다시 가져온 경우 이 단계를 건너뜁니다.

모든 인증서는 다음 최소 요구 사항을 충족해야 합니다.

- RSA 2048비트 이상 또는 ECDSA 256비트 이상
- SHA256 이상의 다이제스트

인증서 재생성 또는 다시 가져오기에 대한 자세한 내용은 PAN-OS 관리자 가이드 또는 Panorama 관리자 가이드를 참조하십시오.

STEP 9 | (Panorama 가상 어플라이언스에 권장됨) Panorama 가상 어플라이언스의 메모리를 64GB로 늘립니다.

Log Collector 모드에서 Panorama 가상 어플라이언스를 PAN-OS 11.0으로 성공적으로 업그레이드한 후, Palo Alto Networks는 부족 프로비저닝된 Panorama 가상 어플라이언스와 관련된 로깅, 관리 및 운영 성능 문제를 방지하기 위해 증가된 시스템 요구 사항을 충족하도록 Panorama 가상 어플라이언스의 메모리를 64GB로 늘릴 것을 권장합니다.

Panorama가 인터넷에 연결되어 있지 않을 때 로그 수집기 업그레이드

Log Collector에 설치할 수 있는 소프트웨어 또는 콘텐츠 업데이트 목록은 지원되는 업데이트를 참조합니다.

*PAN-OS 8.1*에서 업그레이드하는 경우 *PAN-OS 9.0*은 로컬 및 전용 로그 수집기에 대한 새로운 로그 데이터 형식을 도입했습니다. *PAN-OS 10.1*로의 업그레이드 경로에서 기존 로그 데이터는 *PAN-OS 8.1*에서 *PAN-OS 9.0*으로 업그레이드할 때 자동으로 새 형식으로 마이그레이션됩니다.

로그 데이터 손실을 방지하려면 수집기 그룹의 모든 로그 수집기를 동시에 업그레이드해야 합니다. 수집기 그룹의 로그 수집기가 모두 동일한 PAN-OS 버전을 실행하지 않는 경우 로그 포워딩 또는 로그 수집이 발생하지 않습니다. 또한 수집기 그룹의 로그 수집기에 대한 로그 데이터는 모든 로그 수집기가 동일한 PAN-OS 버전을 실행할 때까지 **ACC** 또는 모니터 탭에 표시되지 않습니다. 예를 들어 수집기 그룹에 세 개의 로그 수집기가 있고 두 개의 로그 수집기를 업그레이드하는 경우 수집기 그룹의 로그 수집기로 로그가 포워딩되지 않습니다.

Palo Alto Networks는 유지 관리 기간 동안 로그 수집기를 업그레이드할 것을 권장합니다. 로그 형식 마이그레이션으로 인해 전체 업그레이드 절차는 로컬 및 전용 로그 수집기의 로그 데이터 양에 따라 추가 시간이 걸립니다.

STEP 1 | Log Collector를 업그레이드하기 전에 Panorama 관리 서버에서 적절한 Panorama™ 소프트웨어 릴리스를 실행하고 있는지 확인하십시오.

*Palo Alto Networks®*는 *Panorama* 및 *Log Collector*가 동일한 소프트웨어 릴리스 버전을 실행하고 *Panorama, Log Collectors* 및 모든 관리 방화벽이 동일한 콘텐츠 릴리스 버전을 실행할 것을 적극 권장합니다. 중요한 소프트웨어 및 콘텐츠 호환성 세부정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조합니다.

Panorama는 Log Collectors와 동일한(또는 이후) 소프트웨어 릴리스를 실행해야 하지만 동일하거나 이후의 콘텐츠 릴리스 버전이 있어야 합니다.

- 소프트웨어 릴리스 버전 - Panorama 관리 서버가 Log Collector를 업데이트하려는 릴리스와 같거나 이후의 소프트웨어 릴리스를 실행하고 있지 않은 경우 로그 수집기를 업데이트하기 전에 Panorama(Panorama용 콘텐츠 및 소프트웨어 업데이트 설치 참조)에 동일하거나 이후의 Panorama 릴리스를 설치해야 합니다.
- 콘텐츠 릴리스 버전 - 콘텐츠 릴리스 버전의 경우 모든 Log Collector가 최신 콘텐츠 릴리스 버전을 실행 중인지, 최소한 설치하거나 Panorama에서 실행 중인 버전보다 최신 버전을 실행 중인지 확인해야 합니다. 그렇지 않은 경우 Panorama 관리 서버에서 콘텐츠 릴리스 버전을 업데이트하기 전에 먼저 방화벽을 Panorama에서 PAN-OS 11.0으로 업그레이드한 다음 Log Collector를 업데이트합니다(Panorama용 콘텐츠 업데이트 및 소프트웨어 업그레이드 설치 참조).

소프트웨어 및 콘텐츠 버전을 확인하려면:

- **Panorama** 관리 서버 - Panorama 관리 서버에서 실행 중인 소프트웨어 및 콘텐츠 버전을 확인하려면 Panorama 웹 인터페이스에 로그인하고 일반 정보 설정(대시보드)으로 이동합니다.
- 로그 수집기 - 로그 수집기에서 실행 중인 소프트웨어 및 콘텐츠 버전을 확인하려면 각 로그 수집기의 CLI에 로그인하고 **`show system info`** 명령을 실행합니다.

STEP 2 | PAN-OS 11.0으로의 업그레이드 경로 결정.

업그레이드 경로의 일부로 통과하는 각 릴리스에 대한 릴리스 노트 및 다운그레이드 고려 사항의 알려진 문제 및 기본 동작에 대한 변경 사항은 PAN-OS 업그레이드 점검표에서 확인할 수 있습니다.

둘 이상의 *Log Collector*를 업그레이드하는 경우 이미지 다운로드를 시작하기 전에 업그레이드하려는 모든 *Log Collector*의 업그레이드 경로를 결정하여 프로세스를 간소화하십시오.

STEP 3 | SCP 또는 HTTPS를 통해 Panorama에 연결하고 파일을 업로드할 수 있는 호스트에 최신 콘텐츠 및 소프트웨어 업데이트를 다운로드합니다.

Panorama 소프트웨어 릴리스에 필요한 최소 콘텐츠 릴리스 버전은 릴리스 노트를 참조하십시오.

1. 인터넷에 액세스할 수 있는 호스트를 사용하여 Palo Alto Networks 고객 지원 웹사이트에 로그인합니다.
2. 최신 콘텐츠 업데이트 다운로드:
   1. 리소스 섹션에서 동적 업데이트를 클릭합니다.
   2. 최신 콘텐츠 업데이트를 다운로드하고 파일을 호스트에 저장합니다. 업데이트할 각 콘텐츠 유형에 대해 이 단계를 수행합니다.
3. 소프트웨어 업데이트 다운로드:
   1. Palo Alto Networks® 고객 지원 웹사이트의 기본 페이지로 돌아가서 리소스 섹션에서 소프트웨어 업데이트를 클릭하십시오.
   2. 다운로드 열을 검토하여 설치할 버전을 결정하십시오. M 시리즈 어플라이언스의 업데이트 패키지 파일 이름은 "Panorama_m"으로 시작하고 그 뒤에 릴리스 번호가 옵니다. 예를 들어, M 시리즈 어플라이언스를 Panorama 11.0.0으로 업그레이드하려면 `Panorama_m-11.0.0` 이미지를 다운로드합니다.

      필터링 기준 드롭다운에서 ***Panorama M*** 이미지*(M* 시리즈 디바이스용*)*를 선택하면 *Panorama* 이미지를 빠르게 찾을 수 있습니다.
4. 적절한 파일 이름을 클릭하고 파일을 호스트에 저장합니다.

STEP 4 | 최신 콘텐츠 업데이트를 설치합니다.

콘텐츠 업데이트를 설치해야 하는 경우 소프트웨어 업데이트를 설치하기 전에 설치해야 합니다. 또한 *Panorama*에서 콘텐츠 릴리스 버전을 업데이트하기 전에 먼저 방화벽에 콘텐츠 업데이트를 설치한 다음 *Log Collectors*에 설치합니다.

애플리케이션 또는 애플리케이션 및 위협 업데이트를 먼저 설치한 다음 필요에 따라 다른 업데이트(바이러스 백신, WildFire® 또는 URL 필터링)를 한 번에 하나씩 순서에 관계없이 설치합니다.

구독에 애플리케이션 및 위협 콘텐츠가 모두 포함되어 있는지의 여부와 관계없이 *Panorama*는 애플리케이션 콘텐츠만 설치하고 이를 필요로 합니다. 자세한 내용은 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 디바이스 배포 > 동적 업데이트를 선택합니다.
3. 업로드를 클릭하고 업데이트 유형을 선택한 후 호스트에서 적절한 콘텐츠 업데이트 파일을 찾아보기하고 확인을 클릭합니다.
4. 파일에서 설치를 클릭하고 업데이트 유형을 선택한 다음 방금 업로드한 업데이트의 파일 이름을 선택합니다.
5. 로그 수집기를 선택합니다.
6. 확인을 클릭하여 설치를 시작합니다.
7. 각 콘텐츠 업데이트에 대해 이 단계를 반복합니다.

STEP 5 | PAN-OS 11.0으로의 업그레이드 경로에 따라 Log Collector를 PAN-OS 릴리스로 업그레이드합니다.

1. Panorama가 인터넷에 연결되지 않은 경우 Log Collector를 업그레이드하여 PAN-OS 8.1로 업그레이드합니다.
2. Panorama가 인터넷에 연결되지 않은 경우 Log Collector를 PAN-OS 9.0으로 업그레이드합니다.

   PAN-OS 9.0은 새로운 로그 형식을 도입했습니다. Log Collector를 PAN-OS 9.0으로 성공적으로 업그레이드하면 로그가 자동으로 새 형식으로 마이그레이션됩니다.

   자동 로그 마이그레이션이 성공적으로 완료되었는지 확인할 때까지 업그레이드 경로를 계속 진행하지 마십시오.
3. Panorama가 인터넷에 연결되지 않은 경우 Log Collector를 업그레이드하여 PAN-OS 9.1로 업그레이드합니다.
4. Panorama가 인터넷에 연결되지 않은 경우 Log Collector를 PAN-OS 10.0으로 업그레이드합니다.
5. Panorama가 인터넷에 연결되지 않은 경우 Log Collector를 PAN-OS 10.1로 업그레이드합니다.

   PAN-OS 10.0에서는 새로운 로그 형식이 도입되었습니다. PAN-OS 10.0에서 PAN-OS 10.1로 업그레이드할 때 PAN-OS 8.1 또는 이전 릴리스에서 생성된 로그를 마이그레이션하도록 선택할 수 있습니다. 그렇지 않으면 이러한 로그는 PAN-OS 10.1로 성공적으로 업그레이드될 때 자동으

로 삭제됩니다. 마이그레이션 중에는 ACC 또는 모니터 탭에 로그 데이터가 표시되지 않습니다. 마이그레이션이 진행되는 동안 로그 데이터는 적절한 Log Collector로 계속 포워딩되지만 성능에 약간의 영향을 미칠 수 있습니다.

6. Panorama가 인터넷에 연결되지 않은 경우 Log Collector를 PAN-OS 10.2로 업그레이드합니다.

STEP 6 | Log Collector를 PAN-OS 11.0으로 업그레이드합니다.

1. **Panorama** > 디바이스 배포 > 소프트웨어를 선택합니다.
2. 호스트에서 적절한 소프트웨어 업데이트 파일로 업로드, 찾아보기를 클릭하고 확인을 클릭합니다.
3. 방금 업로드한 릴리스의 작업 열에서 설치를 클릭합니다.
4. PAN-OS 11.0을 설치하고 적절한 Log Collector를 선택합니다.
5. 필요에 따라 다음 중 하나를 선택하십시오.
   - 디바이스에만 업로드**(**설치하지 않음**)**.
   - 설치 후 기기 재부팅.
6. 확인을 클릭하여 업로드 또는 설치를 시작합니다.

STEP 7 | 각 Log Collector에 설치된 소프트웨어 및 콘텐츠 버전을 확인합니다.

Log Collector CLI에 로그인하고 **`show system info`** 작업 명령을 입력합니다. 출력은 다음과 유사합니다.

```
sw-version: 11.0.0 app-version: 8270-6076 app-release-date:
 2020/05/08 18:21:51
```

STEP 8 | (FIPS-CC 모드만 해당)FIPS-CC 모드에서 Panorama 및 관리형 디바이스 업그레이드.

전용 Log Collector가 PAN-OS 11.0 릴리스를 실행하는 동안 전용 Log Collector를 Panorama 관리에 추가한 경우 FIPS-CC 모드에서 전용 Log Collector를 업그레이드하려면 보안 연결 상태를 재설정해야 합니다.

전용 Log Collector가 PAN-OS 10.0 이하 릴리스를 실행하는 동안 Panorama 관리에 추가된 전용 Log Collector를 다시 온보딩할 필요가 없습니다.

STEP 9 | (PAN-OS 10.2 이상 릴리스) OpenSSL 보안 수준 2를 준수하려면 모든 인증서를 재생성하거나 다시 가져옵니다.

PAN-OS 10.1 또는 이전 릴리스에서 PAN-OS 11.0으로 업그레이드하는 경우 이 단계가 필요합니다. PAN-OS 10.2에서 업그레이드하고 이미 인증서를 재생성했거나 다시 가져온 경우 이 단계를 건너뜁니다.

모든 인증서는 다음 최소 요구 사항을 충족해야 합니다.

- RSA 2048비트 이상 또는 ECDSA 256비트 이상
- SHA256 이상의 다이제스트

인증서 재생성 또는 다시 가져오기에 대한 자세한 내용은 PAN-OS 관리자 가이드 또는 Panorama 관리자 가이드를 참조하십시오.

STEP 10 | (Panorama 가상 어플라이언스에 권장됨) Panorama 가상 어플라이언스의 메모리를 64GB로 늘립니다.

Log Collector 모드에서 Panorama 가상 어플라이언스를 PAN-OS 11.0으로 성공적으로 업그레이드한 후, Palo Alto Networks는 부족 프로비저닝된 Panorama 가상 어플라이언스와 관련된 로깅, 관리 및 운영 성능 문제를 방지하기 위해 증가된 시스템 요구 사항을 충족하도록 Panorama 가상 어플라이언스의 메모리를 64GB로 늘릴 것을 권장합니다.

인터넷 연결을 통해 Panorama에서 WildFire 클러스터 업그레이드

클러스터의 WildFire 어플라이언스는 Panorama에서 관리할 때 병렬로 업그레이드할 수 있습니다. Panorama가 인터넷에 직접 연결되어 있는 경우 Panorama에서 직접 새 릴리스를 확인하고 다운로드할 수 있습니다.

*Panorama*는 동일한 소프트웨어 버전 또는 이후 소프트웨어 버전을 운영하는 *WildFire* 어플라이언스 및 어플라이언스 클러스터만 관리할 수 있습니다.

STEP 1 | Panorama를 WildFire 클러스터에 설치하려는 대상 소프트웨어 릴리스와 같거나 이후 릴리스로 업그레이드하십시오.

Panorama 업그레이드에 대한 자세한 내용은 Panorama용 콘텐츠 및 소프트웨어 업데이트 설치를 참조합니다.

STEP 2 | 샘플 분석을 일시적으로 중단합니다.

1. 방화벽이 새 샘플을 WildFire 어플라이언스로 포워딩하는 것을 중지합니다.
   1. 방화벽 웹 인터페이스에 로그인합니다.
   2. 디바이스 > 설정 > **WildFire**를 선택하고 일반 설정을 수정합니다.
   3. **WildFire Private Cloud** 필드를 지웁니다.
   4. 확인 및 커밋을 클릭합니다.
2. 어플라이언스에 이미 제출된 방화벽 샘플에 대한 분석이 완료되었는지 확인합니다.
   1. Panorama 웹 인터페이스에 로그인합니다.
   2. **Panorama** > 관리형 **WildFire** 클러스터를 선택하고 클러스터 분석 환경 사용률을 봅니다.
   3. 가상 머신 사용량에 진행 중인 샘플 분석이 표시되지 않는지 확인합니다.

   WildFire 어플라이언스가 최근 제출된 샘플 분석을 완료할 때까지 기다리지 않으려면 다음 단계를 계속할 수 있습니다. 그러나 *WildFire* 어플라이언스는 분석 대기열에서 보류 중인 샘플을 삭제합니다.

STEP 3 | 최신 WildFire 어플라이언스 콘텐츠 업데이트를 설치합니다.

이러한 업데이트는 어플라이언스에 최신 위협 정보를 제공하여 멀웨어를 정확하게 탐지합니다.

소프트웨어 업그레이드를 설치하기 전에 콘텐츠 업데이트를 설치해야 합니다. *Panorama* 릴리스를 위해 설치해야 하는 최소 콘텐츠 릴리스 버전은 릴리스 노트를 참조하십시오.

1. WildFire 콘텐츠 업데이트 다운로드:
   1. **Panorama** > 디바이스 배포 > 동적 업데이트를 선택합니다.
   2. WildFire 콘텐츠 업데이트 릴리스 패키지를 선택하고 다운로드를 클릭합니다.
2. 설치를 클릭합니다.
3. 업그레이드할 WildFire 클러스터 또는 개별 어플라이언스를 선택합니다.
4. 확인을 클릭하여 설치를 시작합니다.

STEP 4 | PAN-OS 소프트웨어 버전을 WildFire 어플라이언스에 다운로드합니다.

WildFire 어플라이언스를 업그레이드할 때 주요 릴리스 버전을 건너뛸 수 없습니다. 예를 들어, PAN-OS 9.1에서 PAN-OS 11.0으로 업그레이드하려면 먼저 PAN-OS 10.0, PAN-OS 10.1 및 PAN-OS 10.2를 다운로드하여 설치해야 합니다.

1. WildFire 소프트웨어 업그레이드 다운로드:
   1. **Panorama** > 디바이스 배포 > 소프트웨어를 선택합니다.
   2. 업데이트된 릴리스 목록을 검색하려면 지금 확인을 클릭하십시오.
   3. 설치하려는 WildFire 릴리스를 선택하고 다운로드를 클릭합니다.
   4. 닫기를 클릭하여 소프트웨어 다운로드 창을 종료합니다.
2. 설치를 클릭합니다.
3. 업그레이드할 WildFire 클러스터를 선택합니다.
4. 설치 후 디바이스 재부팅을 선택합니다.
5. 확인을 클릭하여 설치를 시작합니다.
6. (선택 사항) Panorama에서 설치 진행 상황을 모니터링합니다.

STEP 5 | (선택 사항) WildFire 컨트롤러 노드에서 재부팅 작업의 상태를 확인합니다.

WildFire 클러스터 컨트롤러에서 다음 명령을 실행하고 작업 유형 ## 및 상태 **FIN**을 찾습니다.

```
admin@WF-500(active-controller)> show cluster task pending
```

STEP 6 | WildFire 어플라이언스가 샘플 분석을 재개할 준비가 되었는지 확인하십시오.

1. sw-version 필드에 11.0.0이 표시되는지 확인합니다.

   ```
   admin@WF-500(passive-controller)> show system info | match sw-version
   ```

2. 모든 프로세스가 실행 중인지 확인합니다.

   ```
   admin@WF-500(passive-controller)> ### ##### ## ##
   ```

3. 자동 커밋(**AutoCom**) 작업이 완료되었는지 확인합니다.

   ```
   admin@WF-500(passive-controller)> show jobs all
   ```

인터넷 연결 없이 Panorama에서 WildFire 클러스터 업그레이드

클러스터의 WildFire 어플라이언스는 Panorama에서 관리할 때 병렬로 업그레이드할 수 있습니다. Panorama가 인터넷에 직접 연결되어 있지 않은 경우 Panorama에서 배포하기 전에 Palo Alto Networks 지원 사이트에서 소프트웨어 콘텐츠 및 업데이트를 다운로드하고 내부 서버에서 호스팅해야 합니다.

*Panorama*는 동일한 소프트웨어 버전 또는 이후 소프트웨어 버전을 운영하는 *WildFire* 어플라이언스 및 어플라이언스 클러스터만 관리할 수 있습니다.

STEP 1 | Panorama를 WildFire 클러스터에 설치하려는 대상 소프트웨어 릴리스와 같거나 이후 릴리스로 업그레이드하십시오.

Panorama 업그레이드에 대한 자세한 내용은 Panorama용 콘텐츠 및 소프트웨어 업데이트 설치를 참조합니다.

STEP 2 | 샘플 분석을 일시적으로 중단합니다.

1. 방화벽이 새 샘플을 WildFire 어플라이언스로 포워딩하는 것을 중지합니다.
   1. 방화벽 웹 인터페이스에 로그인합니다.
   2. 디바이스 > 설정 > **WildFire**를 선택하고 일반 설정을 수정합니다.
   3. **WildFire Private Cloud** 필드를 지웁니다.
   4. 확인 및 커밋을 클릭합니다.
2. 어플라이언스에 이미 제출된 방화벽 샘플에 대한 분석이 완료되었는지 확인합니다.
   1. Panorama 웹 인터페이스에 로그인합니다.
   2. **Panorama** > 관리형 **WildFire** 클러스터를 선택하고 클러스터 분석 환경 사용률을 봅니다.
   3. 가상 머신 사용량에 진행 중인 샘플 분석이 표시되지 않는지 확인합니다.

   WildFire 어플라이언스가 최근 제출된 샘플 분석을 완료할 때까지 기다리지 않으려면 다음 단계를 계속할 수 있습니다. 그러나 *WildFire* 어플라이언스는 분석 대기열에서 보류 중인 샘플을 삭제합니다.

STEP 3 | 인터넷에 액세스할 수 있는 호스트에 WildFire 콘텐츠 및 소프트웨어 업데이트를 다운로드합니다. Panorama는 호스트에 액세스할 수 있어야 합니다.

1. 인터넷 액세스가 가능한 호스트를 사용하여 Palo Alto Networks 고객 지원 웹사이트에 로그인합니다.
2. 콘텐츠 업데이트 다운로드:
   1. 도구 섹션에서 동적 업데이트를 클릭합니다.
   2. 원하는 콘텐츠 업데이트를 다운로드하고 파일을 호스트에 저장합니다. 업데이트할 각 콘텐츠 유형에 대해 이 단계를 수행합니다.
3. 소프트웨어 업데이트 다운로드:
   1. Palo Alto Networks 고객 지원 웹사이트의 기본 페이지로 돌아가서 도구 섹션에서 소프트웨어 업데이트를 클릭하십시오.
   2. 다운로드 열을 검토하여 설치할 버전을 결정하십시오. 업데이트 패키지의 파일 이름은 업그레이드 모델 및 릴리스를 나타냅니다. WildFire_<release>.
   3. 파일 이름을 클릭하고 파일을 호스트에 저장합니다.

STEP 4 | 최신 WildFire 어플라이언스 콘텐츠 업데이트를 설치합니다.

이러한 업데이트는 어플라이언스에 최신 위협 정보를 제공하여 멀웨어를 정확하게 탐지합니다.

소프트웨어 업그레이드를 설치하기 전에 콘텐츠 업데이트를 설치해야 합니다. *Panorama* 릴리스를 위해 설치해야 하는 최소 콘텐츠 릴리스 버전은 릴리스 노트를 참조하십시오.

1. WildFire 콘텐츠 업데이트 다운로드:
   1. **Panorama** > 디바이스 배포 > 동적 업데이트를 선택합니다.
   2. 업로드를 클릭하고, 콘텐츠 유형을 선택한 다음, WildFire 콘텐츠 업데이트 파일을 검색하고, 확인을 클릭합니다.
   3. 파일 설치를 클릭하고 업그레이드하려는 클러스터의 패키지 유형, 파일 이름 및 WildFire 어플라이언스를 선택한 다음, 확인을 클릭합니다.
2. 확인을 클릭하여 설치를 시작합니다.

STEP 5 | PAN-OS 소프트웨어 버전을 WildFire 어플라이언스에 다운로드합니다.

WildFire 어플라이언스를 업그레이드할 때 주요 릴리스 버전을 건너뛸 수 없습니다. 예를 들어, PAN-OS 9.1에서 PAN-OS 11.0으로 업그레이드하려면 먼저 PAN-OS 10.0, PAN-OS 10.1 및 PAN-OS 10.2를 다운로드하여 설치해야 합니다.

1. WildFire 소프트웨어 업그레이드 다운로드:
   1. **Panorama** > 디바이스 배포 > 소프트웨어를 선택합니다.
   2. 업데이트된 릴리스 목록을 검색하려면 지금 확인을 클릭하십시오.
   3. 설치하려는 WildFire 릴리스를 선택하고 다운로드를 클릭합니다.
   4. 닫기를 클릭하여 소프트웨어 다운로드 창을 종료합니다.
2. 설치를 클릭합니다.
3. 업그레이드할 WildFire 클러스터를 선택합니다.
4. 설치 후 디바이스 재부팅을 선택합니다.
5. 확인을 클릭하여 설치를 시작합니다.
6. (선택 사항) Panorama에서 설치 진행 상황을 모니터링합니다.

STEP 6 | (선택 사항) WildFire 컨트롤러 노드에서 재부팅 작업의 상태를 확인합니다.

WildFire 클러스터 컨트롤러에서 다음 명령을 실행하고 작업 유형 ## 및 상태 **FIN**을 찾습니다.

```
admin@WF-500(active-controller)> show cluster task pending
```

STEP 7 | WildFire 어플라이언스가 샘플 분석을 재개할 준비가 되었는지 확인하십시오.

1. sw-version 필드에 11.0.0이 표시되는지 확인합니다.

```
admin@WF-500(passive-controller)> show system info | match sw-version
```

2. 모든 프로세스가 실행 중인지 확인합니다.
   admin@WF-500(passive-controller)> ### ##### ## ##
3. 자동 커밋(**AutoCom**) 작업이 완료되었는지 확인합니다.

```
admin@WF-500(passive-controller)> show jobs all
```

Panorama가 인터넷에 연결되어 있을 때 방화벽 업그레이드

PAN-OS 11.0 출시 정보를 검토한 후 다음 절차를 사용하여 Panorama로 관리하는 방화벽을 업그레이드합니다. 이 절차는 독립 실행형 방화벽 및 고가용성(HA) 구성에 배포된 방화벽에 적용됩니다.

여러 기능 PAN-OS 릴리스에서 HA 방화벽을 업그레이드하는 경우 계속하기 전에 각 HA 피어를 업그레이드 경로에서 동일한 기능 PAN-OS 릴리스로 업그레이드해야 합니다. 예를 들어, PAN-OS 10.0에서 PAN-OS 11.0으로 HA 피어를 업그레이드하는 중입니다. 대상 PAN-OS 11.0 릴리스로 계속 업그레이드하려면 먼저 두 HA 피어를 모두 PAN-OS 10.1로 업그레이드해야 합니다. HA 피어가 2개 이상의 기능 릴리스와 떨어져 있는 경우 이전 릴리스가 설치된 방화벽은 ## ### ## ### 메시지와 함께 ## ### 상태가 됩니다.

*Panorama*가 업데이트 서버에 직접 연결할 수 없는 경우 Panorama가 인터넷에 연결되어 있지 않을 때 방화벽 업그레이드 절차에 따라 *Panorama*에 이미지를 수동으로 다운로드한 다음 방화벽에 배포할 수 있습니다.

새로운 소프트웨어 버전 업그레이드 건너뛰기 기능을 사용하면 PAN-OS 11.0의 Panorama 어플라이언스에서 PAN-OS 10.1 이상 버전의 방화벽으로 업그레이드를 배포할 때 최대 3개의 릴리스를 건너뛸 수 있습니다.

Panorama에서 방화벽을 업그레이드하려면 먼저 다음을 수행해야 합니다.

- Panorama가 업그레이드하려는 PAN-OS 버전과 같거나 이후 버전을 실행하고 있는지 확인하십시오. 관리형 방화벽을 이 버전으로 업그레이드하기 전에 Panorama를 업그레이드하고 해당 Log Collector를 11.0으로 업그레이드해야 합니다. 또한, Log Collector를 11.0으로 업그레이드할 때 로깅 인프라의 변경으로 인해 모든 Log Collector를 동시에 업그레이드해야 합니다.
- 방화벽이 안정적인 전원에 연결되어 있는지 확인하십시오. 업그레이드 중 전원이 손실되면 방화벽을 사용할 수 없게 될 수 있습니다.
- PAN-OS 11.0으로 업그레이드할 때 Panorama 가상 어플라이언스가 레거시 모드인 경우 레거시 모드를 유지할지 여부를 결정합니다. PAN-OS 9.1 이상의 버전을 실행하는 새 Panorama 가상 어플라이언스 배포에는 레거시 모드가 지원되지 않습니다. Panorama 가상 어플라이언스를 PAN-OS 9.0 또는 이전 릴리스에서 PAN-OS 11.0으로 업그레이드하는 경우, Palo Alto Networks는 Panorama 가상 어플라이언스

설정 전제 조건을 검토하고 필요에 따라 Panorama 모드 또는 관리 전용 모드로 변경할 것을 권장합니다.

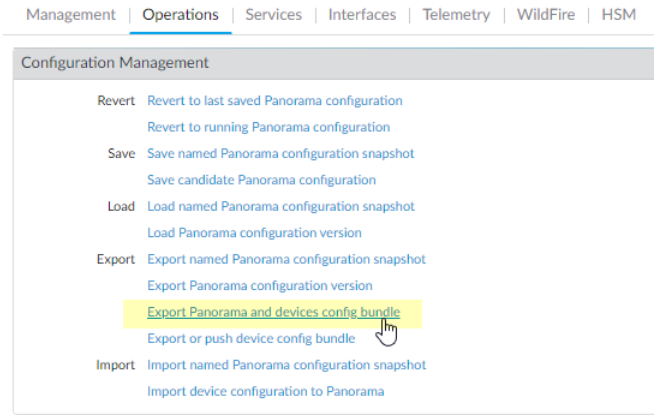
Panorama 가상 어플라이언스를 레거시 모드로 유지하려면 Panorama 가상 어플라이언스에 할당된 CPU 및 메모리를 최소 16개 CPU 및 32GB 메모리로 설정하여 성공적으로 PAN-OS 11.0으로 업그레이드합니다. 자세한 내용은 Panorama Virtual Appliance 설정 전제 조건을 참조하십시오.

STEP 1 | Panorama 웹 인터페이스에 로그인합니다.

STEP 2 | 업그레이드하려는 각 관리 방화벽에 현재 구성 파일의 백업을 저장합니다.

방화벽이 구성 백업을 자동으로 생성하지만 업그레이드하기 전에 백업을 생성하고 외부에 저장하는 것이 가장 좋습니다.

1. **Panorama** > 설정 > 작업을 선택하고 **Panorama** 및 디바이스 구성 번들 내보내기를 클릭하여 Panorama 및 각 관리 디바이스의 최신 구성 백업을 생성하고 내보냅니다.

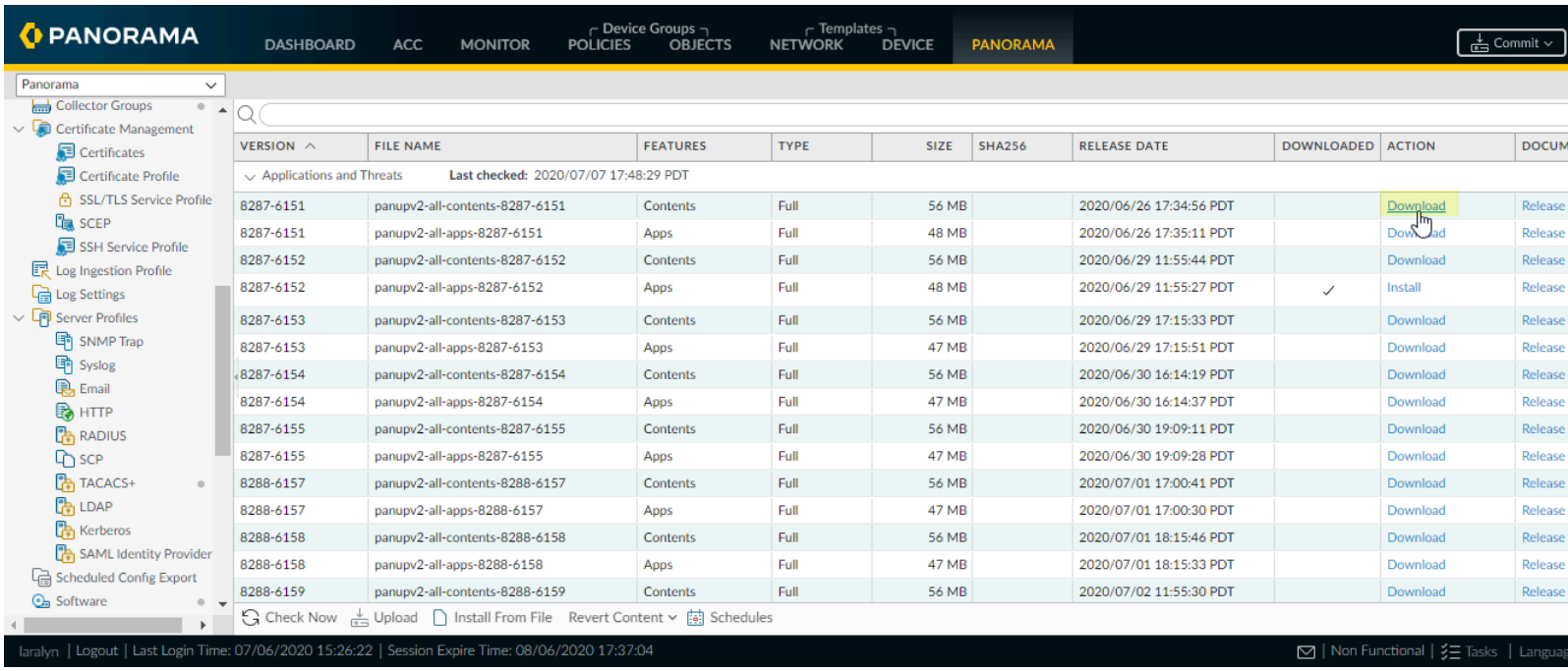


2. 내보낸 파일을 방화벽 외부 위치에 저장합니다. 업그레이드에 문제가 있는 경우 이 백업을 사용하여 구성을 복원할 수 있습니다.

STEP 3 | 최신 콘텐츠 업데이트를 설치합니다.

PAN-OS 11.0에 필요한 최소 콘텐츠 릴리스 버전은 릴리스 노트를 참조하십시오. Panorama 및 관리 방화벽에 콘텐츠 업데이트를 배포할 때 애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례을(를) 따릅니다.

1. 최신 업데이트를 보려면 **Panorama** > 디바이스 배포 > 동적 업데이트 및 지금 확인을 선택합니다. 업데이트가 있으면 작업 열에 다운로드 링크가 표시됩니다.



2. 설치를 클릭하고 업데이트를 설치할 방화벽을 선택합니다. HA 방화벽을 업그레이드하는 경우 두 피어 모두에서 콘텐츠를 업데이트해야 합니다.
3. 확인을 클릭합니다.

STEP 4 | PAN-OS 11.0으로의 업그레이드 경로 결정.

업그레이드 경로의 일부로 통과하는 각 릴리스에 대해 PAN-OS 업그레이드 체크리스트, 릴리스 노트 및 업그레이드/다운그레이드 고려 사항에서 알려진 문제 및 기본 동작의 변경 사항을 검토합니다.

둘 이상의 방화벽을 업그레이드하는 경우 이미지 다운로드를 시작하기 전에 모든 방화벽에 대한 업그레이드 경로를 결정하여 프로세스를 간소화하십시오.

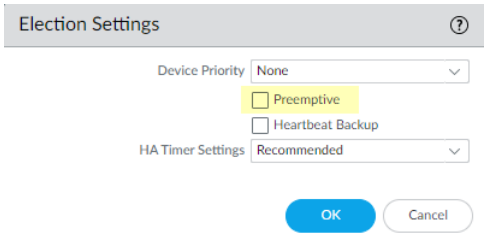
STEP 5 | (모범 사례) Cortex Data Lake(CDL)를 활용하는 경우 디바이스 인증서를 설치합니다.

방화벽은 PAN-OS 11.0으로 업그레이드할 때 CDL 수집 및 쿼리 엔드포인트 인증을 위해 디바이스 인증서를 사용하도록 자동으로 전환됩니다.

*PAN-OS 11.0*으로 업그레이드하기 전에 디바이스 인증서를 설치하지 않으면 방화벽은 인증을 위해 기존 로깅 서비스 인증서를 계속 사용합니다.

STEP 6 | (HA 방화벽 업그레이드만 해당) HA 쌍의 일부인 방화벽을 업그레이드할 경우 선점을 사용 중지합니다. 각 HA 쌍에 있는 하나의 방화벽에서만 이 설정을 비활성화하면 됩니다.

1. 디바이스 > 고가용성을 선택하고 일렉션**(election)** 설정을 편집합니다.
2. 활성화된 경우 선점 설정을 비활성화(지우기)하고 확인을 클릭합니다.



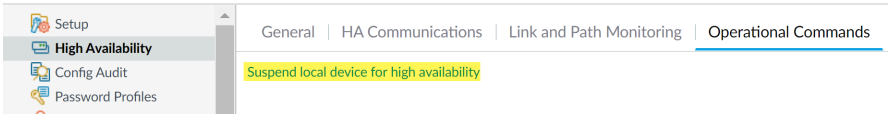
3. 변경사항을 커밋합니다. 업그레이드를 진행하기 전에 커밋이 성공했는지 확인합니다.

STEP 7 | (HA 방화벽 업그레이드만 해당) 기본 HA 피어를 일시 중단하여 강제 페일오버를 수행합니다.

(활성/수동 방화벽) 활성/수동 HA 구성의 방화벽의 경우 먼저 활성 HA 피어를 일시 중단하고 업그레이드합니다.

(활성/활성 방화벽) 활성/활성 HA 구성의 방화벽의 경우 활성-기본 HA 피어를 먼저 일시 중단하고 업그레이드합니다.

1. 활성 기본 방화벽 HA 피어의 방화벽 웹 인터페이스에 로그인합니다.
2. 디바이스 > 고가용성 > 작업 명령 및 고가용성을 위해 로컬 디바이스 일시중단을 선택합니다.



3. 오른쪽 하단에서 해당 상태가 ## ##인지 확인합니다.

   결과적인 장애 조치로 인해 보조 수동 HA 피어가 ## 상태로 전환되어야 합니다.

   결과적인 장애 조치는 업그레이드하기 전에 *HA* 장애 조치가 제대로 작동하는지 확인합니다.

STEP 8 | (선택 사항) 관리형 방화벽을 PAN-OS 10.1로 업그레이드합니다.

소프트웨어 버전 업그레이드 건너뛰기 기능은 PAN-OS 10.1 이상 릴리스를 실행하는 관리형 방화벽을 지원합니다. 관리형 방화벽의 릴리스가 PAN-OS 10.0 또는 이전인 경우 먼저 PAN-OS 10.1 이상 릴리스로 업그레이드합니다.

STEP 9 | (선택 사항) 구성된 SCP 서버로 파일을 내보냅니다.

PAN-OS 11.0에서는 관리형 방화벽에 업그레이드를 배포할 때 SCP 서버를 다운로드 소스로 사용할 수 있습니다. 다음 단계에서 소프트웨어 및 콘텐츠 이미지를 다운로드하기 전에 파일을 내보냅니다.

STEP 10 | 대상 릴리스에 필요한 소프트웨어 및 콘텐츠 버전을 확인하고 다운로드합니다.

이 단계에서는 PAN-OS 11.0으로 업그레이드하는 데 필요한 중간 소프트웨어 및 콘텐츠 이미지를 보고 다운로드할 수 있습니다.

다중 이미지 다운로드를 사용하여 소프트웨어 및 콘텐츠 이미지를 다운로드하는 것은 선택 사항입니다. 이미지는 한 번에 하나씩 다운로드할 수 있습니다.

1. **Panorama** > 디바이스 배포 > 소프트웨어 > 작업 > 검증을 클릭합니다.
2. 다운로드해야 하는 중간 소프트웨어 및 콘텐츠 버전을 확인합니다.
3. 업그레이드할 방화벽을 선택하고 배포를 클릭합니다.
4. 다운로드 소스를 선택하고 다운로드를 클릭합니다.

STEP 11 | 방화벽에 PAN-OS 11.0.0을 설치합니다.

(SD-WAN만 해당) SD-WAN 링크의 정확한 상태를 유지하려면 분기 방화벽을 업그레이드하기 전에 허브 방화벽을 *PAN-OS 11.0*으로 업그레이드해야 합니다. 허브 방화벽보다 먼저 브랜치 방화벽을 업그레이드하면 모니터링 데이터(***Panorama*** > ***SD-WAN*** > 모니터링)가 올바르지 않고 *down*으로 잘못 표시됩니다.

1. 업그레이드할 방화벽 모델에 해당하는 작업 열에서 설치를 클릭합니다. 예를 들어, PA-220 방화벽을 업그레이드하려면 PanOS_220-11.0.0에 해당하는 행에서 설치를 클릭합니다.
2. 소프트웨어 파일 배포 대화 상자에서 업그레이드할 모든 방화벽을 선택합니다.

   (HA 방화벽 업그레이드만 해당) 다운타임을 줄이려면 각 HA 쌍에서 하나의 피어만 선택합니다. 활성/수동 쌍의 경우 수동 피어를 선택합니다. 활성/활성 쌍의 경우 활성-보조 피어를 선택합니다.
3. (HA 방화벽 업그레이드만 해당) 그룹 **HA** 피어가 선택되지 않았는지 확인합니다.
4. 설치 후 디바이스 재부팅을 선택합니다.
5. 업그레이드를 시작하려면 확인을 클릭합니다.
6. 설치가 성공적으로 완료되면 다음 방법 중 하나를 사용하여 재부팅합니다.
   - 재부팅하라는 메시지가 표시되면 예를 클릭합니다.
   - 재부팅하라는 메시지가 표시되지 않으면 디바이스 > 설정 > 작업 및 디바이스 재부팅을 선택합니다.
7. 방화벽 재부팅이 완료되면 **Panorama** > 관리형 디바이스를 선택하고 업그레이드한 방화벽의 소프트웨어 버전이 11.0.0인지 확인합니다. 또한, 업그레이드한 수동 방화벽의 HA 상태가 여전히 수동인지 확인합니다.

STEP 12 | (HA 방화벽 업그레이드만 해당) HA 기능을 기본 HA 피어로 복원합니다.

1. 일시 중단된 기본 방화벽 HA 피어의 방화벽 웹 인터페이스에 로그인합니다.
2. 디바이스 > 고가용성 > 작업 명령 및 고가용성을 위해 로컬 디바이스 작동을 선택합니다.
3. 오른쪽 하단에서 상태가 ##인지 확인합니다. 활성/활성 구성의 방화벽의 경우 상태가 ##인지 확인합니다.
4. HA 피어 실행 구성이 동기화될 때까지 기다립니다.

   대시보드에서 고가용성 위젯에서 실행 중인 구성 상태를 모니터링합니다.

STEP 13 | (HA 방화벽 업그레이드만 해당) 보조 HA 피어를 일시 중단하여 기본 HA 피어로 강제 페일오버합니다.

1. 활성 보조 방화벽 HA 피어의 방화벽 웹 인터페이스에 로그인합니다.
2. 디바이스 > 고가용성 > 작업 명령 및 고가용성을 위해 로컬 디바이스 일시중단을 선택합니다.
3. 오른쪽 하단에서 해당 상태가 ## ##인지 확인합니다.

   그 결과 장애 조치로 인해 기본 수동 HA 피어가 ## 상태로 전환되어야 합니다.

   결과적인 장애 조치는 업그레이드하기 전에 *HA* 장애 조치가 제대로 작동하는지 확인합니다.

STEP 14 | (HA 방화벽 업그레이드만 해당) 각 HA 쌍에서 두 번째 HA 피어를 업그레이드합니다.

1. Panorama 웹 인터페이스에서 **Panorama** > 디바이스 배포 > 소프트웨어를 선택합니다.
2. 업그레이드 중인 HA 쌍의 방화벽 모델에 해당하는 작업 열에서 설치를 클릭합니다.
3. 소프트웨어 파일 배포 대화 상자에서 업그레이드할 모든 방화벽을 선택합니다. 이번에는 방금 업그레이드한 HA 방화벽의 피어만 선택합니다.
4. 그룹 **HA** 피어가 선택되지 않았는지 확인합니다.
5. 설치 후 디바이스 재부팅을 선택합니다.
6. 업그레이드를 시작하려면 확인을 클릭합니다.
7. 설치가 성공적으로 완료되면 다음 방법 중 하나를 사용하여 재부팅합니다.
   - 재부팅하라는 메시지가 표시되면 예를 클릭합니다.
   - 재부팅하라는 메시지가 표시되지 않으면 디바이스 > 설정 > 작업 및 디바이스 재부팅을 선택합니다.

STEP 15 | (HA 방화벽 업그레이드만 해당) HA 기능을 보조 HA 피어로 복원합니다.

1. 일시 중단된 보조 방화벽 HA 피어의 방화벽 웹 인터페이스에 로그인합니다.
2. 디바이스 > 고가용성 > 작업 명령 및 고가용성을 위해 로컬 디바이스 작동을 선택합니다.
3. 오른쪽 하단에서 상태가 ##인지 확인합니다. 활성/활성 구성의 방화벽의 경우 상태가 ##인지 확인합니다.
4. HA 피어 실행 구성이 동기화될 때까지 기다립니다.

   대시보드에서 고가용성 위젯에서 실행 중인 구성 상태를 모니터링합니다.

STEP 16 | (FIPS-CC 모드만 해당)FIPS-CC 모드에서 Panorama 및 관리형 디바이스 업그레이드.

FIPS-CC 모드에서 관리형 방화벽을 업그레이드하려면 관리형 방화벽이 PAN-OS 11.0 릴리스를 실행하는 동안 Panorama 관리에 전용 Log Collector를 추가한 경우 보안 연결 상태를 재설정해야 합니다.

관리형 방화벽이 PAN-OS 10.0 또는 이전 릴리스로 실행되는 경우에는 Panorama 관리에 추가된 관리형 방화벽을 다시 온보딩할 필요가 없습니다.

STEP 17 | 각 관리 방화벽에서 실행되는 소프트웨어 및 콘텐츠 릴리스 버전을 확인합니다.

1. Panorama에서 **Panorama** > 관리형 디바이스를 선택합니다.
2. 방화벽을 찾고 표에서 콘텐츠 및 소프트웨어 버전을 검토합니다.

   HA 방화벽의 경우 각 피어의 HA 상태가 예상대로인지 확인할 수도 있습니다.

	DEVICE NAME	MODEL	IP Address	TEMPLATE	Status				SOFTWARE VERSION	APPS AND THREAT	ANTIVIRUS
			IPV4		DEVICE STATE	HA STATUS	CERTIFICATE	L... M... D...			
	DG-VM (5/5 Devices Connected): Shared > DG-VM										
	PA-VM-6	PA-VM		Stack-VM	Connected		pre-defined		8.1.0	8320-6307	3881-4345
	PA-VM-73	PA-VM		Stack-Test73	Connected		pre-defined		9.1.3	8320-6307	3873-4337
	PA-VM-95	PA-VM		Stack-VM	Connected		pre-defined		10.0.0	8320-6307	3881-4345
	PA-VM-96	PA-VM		Stack-VM	Connected	Passive	pre-defined		10.0.0	8299-6216	3881-4345
	PA-VM			Stack-Test92	Connected	Active	pre-defined		10.0.0	8299-6216	3881-4345

STEP 18 | (HA 방화벽 업그레이드만 해당) 업그레이드하기 전에 HA 방화벽 중 하나에서 선점을 비활성화한 경우 일렉션**(election)** 설정(디바이스 > 고가용성) 해당 방화벽에 대해 선점 설정을 다시 활성화한 다음 변경 사항을 커밋합니다.

STEP 19 | Panorama 웹 인터페이스에서 전체 Panorama 관리 구성을 관리형 방화벽으로 푸시합니다.

이 단계는 Panorama에서 관리형 방화벽으로 디바이스 그룹 및 템플릿 스택 구성 변경 사항을 선택적으로 커밋하고 푸시할 수 있도록 하는 데 필요합니다.

이는 PAN-OS 10.1 또는 이전 릴리스에서 PAN-OS 11.0으로 성공적으로 업그레이드한 후 Panorama에서 관리하는 다중 vsys 방화벽에 구성 변경을 성공적으로 푸시하는 데 필요합니다. 자세한 내용은 Panorama에서 관리하는 multi-vsys 방화벽의 공유 구성 개체에 대한 기본 동작 변경을 참조하십시오.

1. 커밋 > 디바이스에 푸시를 선택합니다.
2. 푸시합니다.

STEP 20 | OpenSSL 보안 수준 2를 준수하도록 모든 인증서를 재생성하거나 다시 가져옵니다.

PAN-OS 10.2 이상 릴리스로 업그레이드할 때는 모든 인증서가 다음과 같은 최소 요구 사항을 충족해야 합니다. PAN-OS 10.2에서 업그레이드하고 인증서를 이미 재생성하거나 다시 가져온 경우 이 단계를 건너뛰십시오.

- RSA 2048비트 이상 또는 ECDSA 256비트 이상
- SHA256 이상의 다이제스트

PAN-OS 관리자 가이드를 참조하거나 인증서 재생성 또는 다시 가져오기에 대한 자세한 내용은 Panorama 관리자 가이드를 참조하십시오.

STEP 21 | 방화벽의 소프트웨어 업그레이드 기록을 볼 수 있습니다.

1. Panorama 인터페이스에 로그인합니다.
2. **Panorama** > 관리형 디바이스 > 요약으로 이동하여 디바이스 내역을 클릭합니다.

Panorama가 인터넷에 연결되어 있지 않을 때 방화벽 업그레이드

방화벽에 설치할 수 있는 소프트웨어 및 콘텐츠 업데이트 목록은 지원되는 업데이트를 참조하십시오.

새로운 소프트웨어 버전 업그레이드 건너뛰기 기능을 사용하면 PAN-OS 11.0의 Panorama 어플라이언스에서 PAN-OS 10.1 이상 버전의 방화벽으로 업그레이드를 배포할 때 최대 3개의 릴리스를 건너뛸 수 있습니다.

STEP 1 | 관리형 방화벽을 업그레이드하기 전에 Panorama 관리 서버와 Log Collector에서 Pan-OS 11.0이 실행되고 있는지 확인합니다.

*Palo Alto Networks®*는 *Panorama* 및 *Log Collectors*가 동일한 *Panorama* 소프트웨어 릴리스를 실행하고 *Panorama, Log Collectors* 및 모든 관리 방화벽이 동일한 콘텐츠 릴리스 버전을 실행할 것을 적극 권장합니다.

중요한 소프트웨어 및 콘텐츠 호환성 세부정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조합니다.

Panorama는 방화벽과 동일한(또는 이후 버전) 소프트웨어 릴리스를 실행해야 하지만 이와 동일하거나 이전 콘텐츠 릴리스 버전이 있어야 합니다.

- 소프트웨어 릴리스 버전 - Panorama 관리 서버 또는 로그 수집기가 방화벽을 업데이트하려는 릴리스와 같거나 이후의 소프트웨어 릴리스를 이미 실행하고 있지 않은 경우 동일한 또는 이후 버전의 Panorama를 설치해야 합니다. 방화벽을 업데이트하기 전에 Panorama 및 Log Collectors(Panorama용 콘텐츠 및 소프트웨어 업데이트 설치 참조)에서 릴리스하십시오.
- 콘텐츠 출시 버전 - 콘텐츠 릴리스 버전의 경우 모든 방화벽이 최신 콘텐츠 릴리스 버전을 실행 중이거나 최소한 Panorama 및 Log Collectors에서 실행되는 것보다 최신 버전을 실행하고 있는지 확인해야 합니다. 그렇지 않은 경우 Panorama 관리 서버에서 콘텐츠 릴리스 버전을 업데이트하기 전에 관리 방화벽을 업데이트한 다음 Panorama가 인터넷에 연결되어 있지 않을 때 로그 수집기를 업그레이드합니다(Panorama용 콘텐츠 및 소프트웨어 업데이트 설치 참조).

소프트웨어 및 콘텐츠 버전을 확인하려면:

- **Panorama** 관리 서버 - Panorama 웹 인터페이스에 로그인하고 일반 정보 설정(대시보드)으로 이동합니다.
- 로그 수집기 - 각 로그 수집기의 CLI에 로그인하고 **`show system info`** 명령을 실행합니다.

STEP 2 | 업그레이드하려는 각 관리 방화벽에 현재 구성 파일의 백업을 저장합니다.

방화벽이 구성 백업을 자동으로 생성하지만 업그레이드하기 전에 백업을 생성하고 외부에 저장하는 것이 가장 좋습니다.

1. **Panorama** 및 디바이스 구성 번들 내보내기(**Panorama** > 설정 > 작동)를 사용하여 Panorama 및 각 관리형 어플라이언스의 최신 구성 백업을 생성하고 내보낼 수 있습니다.
2. 내보낸 파일을 방화벽 외부 위치에 저장합니다. 업그레이드에 문제가 있는 경우 이 백업을 사용하여 구성을 복원할 수 있습니다.

STEP 3 | 어떤 콘텐츠 업데이트를 설치해야 하는지 결정합니다. PAN-OS® 릴리스에 설치해야 하는 최소 콘텐츠 릴리스 버전은 릴리스 노트를 참조하십시오.

*Palo Alto Networks*는 *Panorama, Log Collectors* 및 모든 관리 방화벽이 동일한 콘텐츠 릴리스 버전을 실행할 것을 적극 권장합니다.

각 콘텐츠 업데이트에 대해 업데이트가 필요한지 여부를 결정하고 다음 단계에서 다운로드해야 하는 콘텐츠 업데이트를 기록해 둡니다.

*Panorama*가 관리 방화벽 및 로그 수집기에서 실행되는 것과 동일하지만 이후 콘텐츠 릴리스 버전이 아니라 실행 중인지 확인합니다.

STEP 4 | Panorama 11.0으로 업데이트할 방화벽의 소프트웨어 업그레이드 경로를 결정합니다.

Panorama에 로그인하고 **Panorama** > 관리 디바이스를 선택한 다음 업그레이드하려는 방화벽의 현재 소프트웨어 버전을 확인합니다.

업그레이드 경로의 일부로 통과하는 각 릴리스에 대한 릴리스 노트 및 다운그레이드 고려 사항의 알려진 문제 및 기본 동작에 대한 변경 사항은 PAN-OS 업그레이드 점검표에서 확인할 수 있습니다.

STEP 5 | (선택 사항) 관리형 방화벽을 PAN-OS 10.1로 업그레이드합니다.

소프트웨어 버전 업그레이드 건너뛰기 기능은 PAN-OS 10.1 이상 릴리스를 실행하는 관리형 방화벽을 지원합니다. 관리형 방화벽의 릴리스가 PAN-OS 10.0 또는 이전인 경우 먼저 PAN-OS 10.1 이상 릴리스로 업그레이드합니다.

STEP 6 | 릴리스의 유효성 검사를 수행합니다.

이 단계에서는 11.0으로 업그레이드하는 데 필요한 중간 소프트웨어 및 콘텐츠 이미지를 설명합니다.

1. **Panorama** > 디바이스 배포 > 소프트웨어 > 작업 > 유효성 검사를 선택합니다.
2. 다운로드해야 하는 중간 소프트웨어 및 콘텐츠 버전을 확인합니다.

STEP 7 | SCP 또는 HTTPS를 통해 Panorama 또는 구성된 SCP 서버에 연결하고 파일을 업로드할 수 있는 호스트에 콘텐츠 및 소프트웨어 업데이트를 다운로드합니다.

기본적으로 각 유형의 소프트웨어 또는 콘텐츠 업데이트를 최대 2개까지 Panorama 어플라이언스에 업로드할 수 있으며 동일한 유형의 세 번째 업데이트를 다운로드하는 경우 Panorama는 해당 유형의 가장 오래된 버전에 대한 업데이트를 삭제합니다. 단일 유형의 소프트웨어 업데이트 또는 콘텐츠 업데이트를 2개 이상 업로드해야 하는 경우, **`set max-num-images count <number>`** CLI 명령을 사용하여 Panorama가 저장할 수 있는 최대 이미지 수를 늘립니다.

1. 인터넷에 액세스할 수 있는 호스트를 사용하여 Palo Alto Networks 고객 지원 웹사이트에 로그인합니다.

2. 콘텐츠 업데이트 다운로드:
   1. 리소스 섹션에서 동적 업데이트를 클릭합니다.
   2. 최신 콘텐츠 릴리스 버전(또는 최소한 Panorama 관리 서버에서 설치하거나 실행 중인 버전과 같거나 이후 버전)을 다운로드하고 파일을 호스트에 저장합니다. 업데이트해야 하는 각 콘텐츠 유형에 대해 반복합니다.
3. 소프트웨어 업데이트 다운로드:
   1. Palo Alto Networks 고객 지원 웹사이트의 기본 페이지로 돌아가서 리소스 섹션에서 소프트웨어 업데이트를 클릭하십시오.
   2. 다운로드 열을 검토하여 설치해야 하는 버전을 결정하십시오. 업데이트 패키지의 파일 이름은 모델을 나타냅니다. 예를 들어, PA-220 및 PA-5260 방화벽을 PAN-OS 11.0.0으로 업그레이드하려면 `PanOS_220-11.0.0`, `PanOS_3000-11.0.0` 및 `PanOS_5200-11.0.0` 이미지를 다운로드합니다.

      필터링 기준 드롭다운에서 ***PA***-<*series/model*>용 *PAN-OS*를 선택하여 특정 *PAN-OS* 이미지를 빠르게 찾을 수 있습니다.
4. 적절한 파일 이름을 클릭하고 파일을 호스트에 저장합니다.

STEP 8 | 중간 소프트웨어 버전과 최신 콘텐츠 버전을 다운로드합니다.

PAN-OS 11.0에서는 다중 이미지 다운로드 기능을 사용하여 여러 중간 릴리스를 다운로드할 수 있습니다.

1. 업그레이드할 방화벽을 선택합니다(필수 배포 > 배포).
2. 다운로드 소스를 선택하고 다운로드를 클릭합니다.

STEP 9 | 관리 방화벽에 콘텐츠 업데이트를 설치합니다.

소프트웨어 업데이트 전에 콘텐츠 업데이트를 설치해야 합니다.

애플리케이션 또는 애플리케이션 및 위협 업데이트를 먼저 설치한 다음 필요에 따라 다른 업데이트(바이러스 백신, WildFire® 또는 URL 필터링)를 한 번에 하나씩 순서에 관계없이 설치합니다.

1. **Panorama** > 디바이스 배포 > 동적 업데이트를 선택합니다.
2. 업로드를 클릭하고 업데이트 유형을 선택한 후 적절한 콘텐츠 업데이트 파일을 찾아보기하고 확인을 클릭합니다.
3. 파일에서 설치를 클릭하고 업데이트 유형을 선택한 다음 방금 업로드한 콘텐츠 업데이트의 파일 이름을 선택합니다.
4. 업데이트를 설치할 방화벽을 선택합니다.
5. 확인을 클릭하여 설치를 시작합니다.
6. 각 콘텐츠 업데이트에 대해 이 단계를 반복합니다.

STEP 10 | (GlobalProtect™ 포털 역할을 하는 방화벽만) 방화벽에서 GlobalProtect 에이전트/앱 소프트웨어 업데이트를 업로드하고 활성화합니다

사용자가 엔드포인트(클라이언트 시스템)에 업데이트를 다운로드할 수 있도록 방화벽에서 업데이트를 활성화합니다.

1. 인터넷에 액세스할 수 있는 호스트를 사용하여 Palo Alto Networks 고객 지원 웹사이트에 로그인합니다.
2. 적절한 GlobalProtect 에이전트/앱 소프트웨어 업데이트를 다운로드합니다.
3. Panorama에서 **Panorama** > 디바이스 배포 > **GlobalProtect** 클라이언트를 선택합니다.
4. 파일을 다운로드한 호스트에서 적절한 GlobalProtect 에이전트/앱 소프트웨어 업데이트로 업로드, 찾아보기를 클릭하고 확인을 클릭합니다.
5. 파일에서 활성화를 클릭하고 방금 업로드한 GlobalProtect 에이전트/앱 업데이트의 파일 이름을 선택합니다.

   한 번에 하나의 에이전트/앱 소프트웨어 버전만 활성화할 수 있습니다. 새 버전을 활성화했지만 일부 에이전트에 이전 버전이 필요한 경우 해당 에이전트가 이전 업데이트를 다운로드하려면 이전 버전을 다시 활성화해야 합니다.
6. 업데이트를 활성화할 방화벽을 선택합니다.
7. 확인을 클릭하여 활성화합니다.

STEP 11 | PAN-OS 11.0을 설치합니다.

고가용성*(HA)* 방화벽에서 소프트웨어를 업데이트할 때 다운타임을 방지하려면 한 번에 하나의 *HA* 피어를 업데이트하십시오.

능동형/능동형 방화벽의 경우 먼저 업데이트하는 피어가 중요하지 않습니다.

능동형/수동형 방화벽의 경우 먼저 수동 피어를 업데이트하고 활성 피어를 일시 중단*(*페일오버*)*하고 업데이트한 다음 기능 상태로 되돌려야 합니다*(*페일오버*).*

*(SD-WAN*만 해당*) SD-WAN* 링크의 정확한 상태를 유지하려면 분기 방화벽을 업그레이드하기 전에 허브 방화벽을 *PAN-OS 11.0*으로 업그레이드해야 합니다. 허브 방화벽보다 먼저 브랜치 방화벽을 업그레이드하면 모니터링 데이터*(**Panorama** > **SD-WAN** >* 모니터링*)*가 올바르지 않고 *down*으로 잘못 표시됩니다.

1. 방화벽 구성에 적용되는 단계를 수행하여 방금 업로드한 PAN-OS 소프트웨어 업데이트를 설치합니다.
   - 비 **HA** 방화벽 - 작업 열에서 설치를 클릭하고 업그레이드하려는 모든 방화벽을 선택한 다음 설치 후 디바이스 재부팅을 선택하고 확인을 클릭합니다. .
   - 능동형/능동형 **HA** 방화벽**:**
     1. 업그레이드할 첫 번째 피어에서 선점 설정이 비활성화되어 있는지 확인합니다(디바이스 > 고가용성 > 일렉션(Election) 설정). 활성화된 경우 일렉션**(election)** 설정을 편집하고 선점 설정을 비활성화(지우기)하고 변경 사항을 커밋합니다. 각 HA 쌍의 한 방화벽에서만 이 설정을 비활성화해야 하지만 계속하기 전에 커밋이 성공했는지 확인하십시오.
     2. 설치를 클릭하고 그룹 **HA** 피어를 비활성화(지우기)하고 HA 피어 중 하나를 선택하고 설치 후 디바이스 재부팅을 선택한 다음 확인을 클릭합니다. 계속하기 전에 방화벽이 재부팅을 마칠 때까지 기다리십시오.
     3. 설치를 클릭하고, 그룹 **HA** 피어를 비활성화(지우기)하고, 이전 단계에서 업데이트하지 않은 HA 피어를 선택하고, 설치 후 디바이스 재부팅, 확인을 클릭합니다.
   - 활성/수동 **HA** 방화벽 - 이 예에서 활성 방화벽의 이름은 fw1, 수동 방화벽의 이름은 fw2:
     1. 입니다. 업그레이드할 첫 번째 피어에서 선점 설정이 비활성화되어 있는지 확인합니다(디바이스 > 고가용성 > 일렉션 설정). 활성화된 경우 일렉션**(election)** 설정을 편집하고 선점 설정을 비활성화(지우기)하고 변경 사항을 커밋합니다. 각 HA 쌍의 한 방화벽에서만 이 설정을 비활성화해야 하지만 계속하기 전에 커밋이 성공했는지 확인합니다.
     2. 적절한 업데이트의 작업 열에서 설치를 클릭하고 그룹 **HA** 피어를 비활성화(지우기)한 후 fw2를 선택하고 설치 후 디바이스 재부팅, 확인을 클릭합니다. 계속하기 전에 fw2가 재부팅을 마칠 때까지 기다립니다.
     3. fw2가 재부팅을 완료한 후 fw1(대시보드 > 고가용성)에서 fw2가 여전히 수동 피어인지 확인합니다(로컬 방화벽 상태는 ##이고 피어(fw2)는 ##).

4. Fw1에 액세스하고 로컬 디바이스를 일시 중지합니다(디바이스 > 고가용성 > 작동 명령).
5. fw2(대시보드 > 고가용성)에 액세스하고 로컬 방화벽 상태가 ##이고 피어가 ## ###인지 확인합니다.
6. Panorama에 액세스하고 **Panorama** > 디바이스 배포 > 소프트웨어를 선택한 후 해당 릴리스에 대한 조치 열에서 설치를 클릭하고 그룹 **HA** 피어를 비활성화(지우기)한 후 fw1, 설치 후 디바이스 재부팅을 선택하고 확인을 클릭합니다. 계속하기 전에 fw1이 재부팅을 마칠 때까지 기다립니다.
7. fw1(디바이스 > 고가용성 > 작동 명령)에 액세스하고 로컬 디바이스 작동을 클릭한 후 계속 진행하기 전에 2분 정도 기다립니다.
8. fw1(대시보드> 고가용성)에서 로컬 방화벽 상태가 ##이고 피어(fw2)가 ##인지 확인합니다.

STEP 12 | (FIPS-CC 모드만 해당)FIPS-CC 모드에서 Panorama 및 관리형 디바이스 업그레이드.

FIPS-CC 모드에서 관리형 방화벽을 업그레이드하려면 관리형 방화벽이 PAN-OS 11.0 릴리스를 실행하는 동안 Panorama 관리에 전용 Log Collector를 추가한 경우 보안 연결 상태를 재설정해야 합니다.

관리형 방화벽이 PAN-OS 10.0 또는 이전 릴리스로 실행되는 경우에는 Panorama 관리에 추가된 관리형 방화벽을 다시 온보딩할 필요가 없습니다.

STEP 13 | 각 관리 방화벽에 설치된 소프트웨어 및 콘텐츠 버전을 확인합니다.

1. **Panorama** > 관리형 디바이스를 선택합니다.
2. 방화벽을 찾아 소프트웨어 버전, 앱 및 위협 요소, 바이러스 백신, URL 필터링 및 GlobalProtect 클라이언트 열의 값을 검토합니다.

STEP 14 | 업그레이드하기 전에 HA 방화벽 중 하나에서 선점을 비활성화한 경우, 그런 다음 일렉션 설정(디바이스 > 고가용성)을 편집하고 해당 방화벽에 대한 선점 설정을 다시 활성화합니다.

STEP 15 | Panorama 웹 인터페이스에서 전체 Panorama 관리 구성을 관리형 방화벽으로 푸시합니다.

이 단계는 Panorama에서 관리형 방화벽으로 디바이스 그룹 및 템플릿 스택 구성 변경 사항을 선택적으로 커밋하고 푸시할 수 있도록 하는 데 필요합니다.

이는 PAN-OS 11.0으로 성공적으로 업그레이드한 후 Panorama에서 관리하는 multi-vsys 방화벽에 구성 변경을 성공적으로 푸시하는 데 필요합니다. 자세한 내용은 Panorama에서 관리하는 multi-vsys 방화벽의 공유 구성 개체에 대한 기본 동작 변경을 참조하십시오.

1. 커밋 > 디바이스에 푸시를 선택합니다.
2. 푸시합니다.

STEP 16 | OpenSSL 보안 수준 2를 준수하도록 모든 인증서를 재생성하거나 다시 가져옵니다.

PAN-OS 11.0으로 업그레이드할 때는 모든 인증서가 다음과 같은 최소 요구 사항을 충족해야 합니다.

- RSA 2048비트 이상 또는 ECDSA 256비트 이상
- SHA256 이상의 다이제스트

PAN-OS 관리자 가이드를 참조하거나 인증서 재생성 또는 다시 가져오기에 대한 자세한 내용은 Panorama 관리자 가이드를 참조하십시오.

STEP 17 | 방화벽의 소프트웨어 업그레이드 기록을 볼 수 있습니다.

1. Panorama 인터페이스에 로그인합니다.
2. **Panorama** > 관리형 디바이스 > 요약으로 이동하여 디바이스 내역을 클릭합니다.

ZTP 방화벽 업그레이드

Panorama™ 관리 서버에 ZTP 방화벽을 성공적으로 추가한 후 ZTP 방화벽의 대상 PAN-OS 버전을 구성합니다. Panorama는 처음으로 Panorama에 성공적으로 연결한 후 ZTP 방화벽에 설치된 PAN-OS 버전이 구성된 대상 PAN-OS 버전보다 크거나 같은지 확인합니다. ZTP 방화벽에 설치된 PAN-OS 버전이 대상 PAN-OS 버전보다 낮으면 ZTP 방화벽은 대상 PAN-OS 버전이 설치될 때까지 업그레이드 사이클에 진입합니다.

STEP 1 | Panorama 웹 인터페이스에 관리자로 로그인합니다.

STEP 2 | Panorama에 ZTP 방화벽을 추가합니다.

STEP 3 | 최신 PAN-OS 릴리스를 보려면 **Panorama** > 디바이스 배포 > 업데이트 및 지금 확인을 선택합니다.

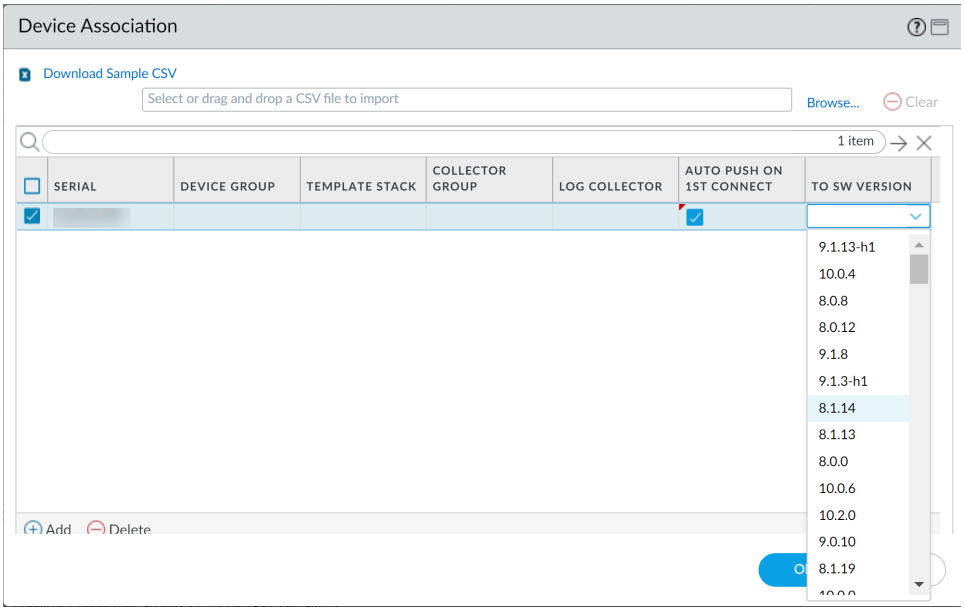
STEP 4 | **Panorama** > 관리 디바이스 > 요약을 선택하고 하나 이상의 ZTP 방화벽을 선택합니다.

STEP 5 | 선택한 ZTP 방화벽을 다시 연결합니다.

STEP 6 | 첫 번째 연결 시 자동 푸시를 선택(활성화)합니다.

STEP 7 | 대상 **SW** 버전 열에서 ZTP 방화벽의 대상 PAN-OS 버전을 선택합니다.

STEP 8 | 확인을 클릭하여 구성 변경 사항을 저장합니다.



STEP 9 | 커밋 및 **Panorama**에 커밋을 선택합니다.

STEP 10 | ZTP 방화벽의 전원을 켭니다.

ZTP 방화벽이 처음으로 Panorama에 연결되면 선택한 PAN-OS 버전으로 자동 업그레이드됩니다.

- **PAN-OS 11.0.0**을 실행하는 **Panorama** - PAN-OS 주요 또는 유지관리 릴리스에서 관리형 방화벽을 업그레이드하는 경우 대상 PAN-OS 릴리스가 설치되기 전에 업그레이드 경로의 중간 PAN-OS 릴리스가 먼저 설치됩니다.

  예를 들어, 관리형 방화벽에 대하여 원하는 대상 **SW** 버전을 PAN-OS 11.0.0으로 구성했고 방화벽에서 PAN-OS 10.1을 실행 중입니다. Panorama에 처음 연결할 때 PAN-OS 10.2.0이 관리형 방화벽에 먼저 설치됩니다. PAN-OS 10.2.0이 성공적으로 설치되면 방화벽이 대상 PAN-OS 11.0.0 릴리스로 자동 업그레이드됩니다.

- **PAN-OS 11.0.1** 이상 버전을 실행하는 **Panorama** - PAN-OS 주 또는 유지관리 릴리스에서 관리형 방화벽을 업그레이드하는 경우 업그레이드 경로에 중간 PAN-OS 주 릴리스가 설치되고 대상 PAN-OS 유지관리 릴리스가 설치되기 전에 기본 PAN-OS 주 릴리스가 다운로드됩니다.

  예를 들어, 관리형 방화벽에 대하여 원하는 대상 **SW** 버전을 PAN-OS 11.0.1로 구성했고 방화벽에서 PAN-OS 10.0을 실행 중입니다. Panorama에 처음 연결할 때 PAN-OS 10.1.0 및 PAN-OS 10.2.0이 관리형 방화벽에 설치됩니다. 관리형 방화벽이 재부팅되면 PAN-OS 11.0.0이 다운로드된 다음 방화벽이 대상 PAN-OS 11.0.1 릴리스에 자동으로 설치됩니다.

STEP 11 | ZTP 방화벽 소프트웨어 업그레이드를 확인합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 관리 디바이스 > 요약을 선택하고 ZTP 방화벽으로 이동합니다.
3. 소프트웨어 버전 열에 올바른 대상 PAN-OS 릴리스가 표시되는지 확인합니다.

STEP 12 | 향후의 모든 PAN-OS 업그레이드에 대해서는 방화벽을 Panorama에서 PAN-OS 11.0으로 업그레이드을(를) 참조하십시오.

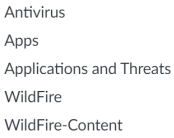
Panorama에서 콘텐츠 업데이트 되돌리기

Panorama™를 사용하면 Panorama에서 직접 하나 이상의 방화벽, 로그 수집기 또는 WildFire 어플라이언스에 있는 애플리케이션, 애플리케이션 및 위협, 안티바이러스, WildFire® 및 WildFire 콘텐츠 버전을 신속하게 되돌릴 수 있습니다. Panorama를 사용하여 관리되는 디바이스에 설치된 콘텐츠 버전을 되돌려 콘텐츠 업데이트에서 애플리케이션 또는 새로운 위협 서명의 도입 또는 수정과 관련된 위험을 완화하는 데 도움이 되는 중앙 집중식 워크플로를 활용합니다. Panorama는 콘텐츠를 되돌릴 때 각 디바이스에 대한 시스템 로그를 생성합니다. 관리형 디바이스에 콘텐츠 업데이트를 배포할 때 애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례을(를) 사용해야 합니다.

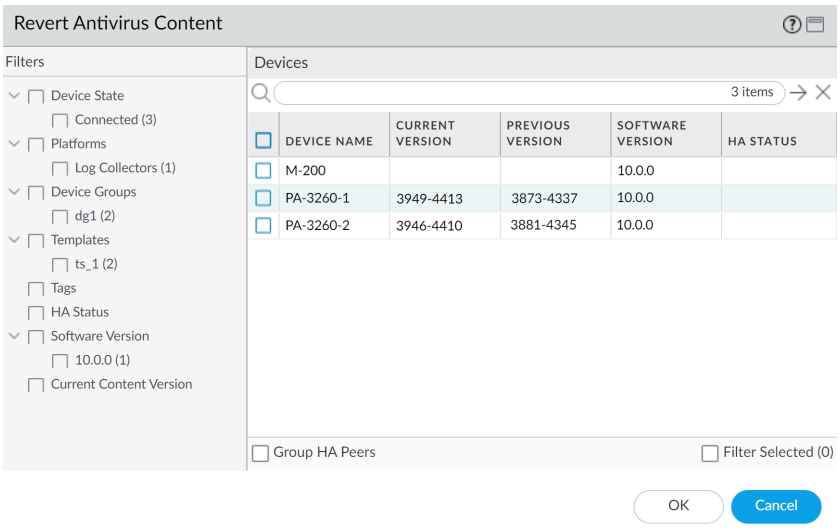
STEP 1 | Panorama 웹 인터페이스에 로그인합니다.

STEP 2 | **Panorama** > 디바이스 배포 > 동적 업데이트 및 콘텐츠 되돌리기를 선택합니다.

STEP 3 | 되돌릴 필요가 있는 콘텐츠 유형을 선택합니다.



STEP 4 | 콘텐츠를 되돌릴 하나 이상의 방화벽을 선택하고 확인을 클릭합니다. 되돌릴 콘텐츠 버전은 현재 디바이스에 설치된 버전보다 이전 버전이어야 합니다.



PAN-OS 업그레이드

PAN-OS 업그레이드 점검표

PAN-OS 업그레이드를 계획하면 Panorama 또는 방화벽에 대해 최신 버전의 PAN-OS로 원활하게 전환할 수 있습니다.

- 디바이스가 등록되고 라이선스가 부여되었는지 확인합니다.
- 사용 가능한 디스크 공간을 확인하십시오.

  필요한 디스크 공간은 PAN-OS 릴리스에 따라 다릅니다. 디바이스 > 소프트웨어를 선택하고 대상 PAN-OS 릴리스 크기를 검토하여 필요한 디스크 공간을 결정합니다.

  - **`show system disk-space`**를 실행합니다.
- 최소 콘텐츠 릴리스 버전을 확인하십시오.
- 기본하는 릴리스를 식별합니다.

  자세한 내용은 Palo Alto Networks 지원 소프트웨어 릴리스 지침 및 EOL(End of Life) Summary를 참조하십시오. 또한 대상 PAN-OS 릴리스에 대한 알려지고 해결된 문제, 업그레이드 및 다운그레이드 고려 사항, 제한 사항을 검토하여 PAN-OS 업그레이드가 사용자에게 미칠 수 있는 영향을 이해하십시오.
- 업그레이드 경로를 결정하십시오.

  하나의 *PAN-OS* 기능 릴리스 버전에서 이후 기능 릴리스로 업그레이드할 때 대상 릴리스 경로에 있는 기능 릴리스 버전 설치를 건너뛸 수 없습니다.
- 업그레이드 경로의 모든 릴리스에 대한 업그레이드/다운그레이드 고려 사항을 검토하십시오.
- (GlobalProtect에 필요) GlobalProtect 사용자가 VPN 연결을 잃지 않도록 하려면 최소 GlobalProtect™ 에이전트 버전을 확인하십시오. GlobalProtect는 최신 버전으로 직접 업그레이드할 수 있습니다.
- 설치한 플러그인의 대상 릴리스 버전에서 최소 플러그인 릴리스 버전을 확인하십시오.
- 관리 인터페이스에서 업데이트 서버로의 연결을 확인합니다.
  - 디바이스 > 문제 해결을 선택하고 업데이트 서버 연결을 테스트하여 DNS가 주소를 확인할 수 있는지 확인합니다.

    해결되지 않으면 DNS를 **`8.8.8.8`**로 변경하고(자체 DNS 서버가 아닌 공용 DNS 서버를 사용해야 함) 다시 핑(ping)합니다.

    그래도 해결되지 않으면 업데이트 서버를 **`staticupdates.paloaltonetworks.com`** 및 커밋으로 변경합니다.
- (SD-WAN만 해당) PAN-OS 10.2로 업그레이드할 허브 및 분기 방화벽을 식별합니다.

  SD-WAN 링크의 정확한 상태를 유지하려면 브랜치 방화벽을 업그레이드하기 전에 허브 방화벽을 PAN-OS 11.0으로 업그레이드해야 합니다. 허브 방화벽보다 먼저 브랜치 방화벽을 업그레이드하면 모니터링 데이터(**Panorama** > **SD-WAN** > 모니터링)가 올바르지 않고 `down`으로 잘못 표시됩니다.

- 현재 설치된 플러그인이 있는 경우 업그레이드하기 전에 현재 Panorama에 설치된 모든 플러그인(**Panorama** > 플러그인) 또는 방화벽(디바이스 > 플러그인)에 대해 PAN-OS 11.0에서 지원되는 플러그인 버전을 다운로드합니다.

  PAN-OS 10.2에서 지원되는 Panorama 플러그인 버전은 Panorama 플러그인 호환성 매트릭스를 참조하십시오.

  Panorama와 방화벽을 PAN-OS 11.0에서 PAN-OS 10.2로 성공적으로 업그레이드하는 데 필요합니다. 다운로드한 플러그인 버전은 PAN-OS 10.2로 업그레이드 시 자동으로 설치됩니다. 지원되는 플러그인 버전을 다운로드하지 않으면 PAN-OS 11.0으로의 업그레이드가 차단됩니다.

다운그레이드 고려 사항

다음 표에는 업그레이드 또는 다운그레이드에 영향을 주는 하드웨어 기능이 나열되어 있습니다. PAN-OS 11.0 릴리스로 업그레이드하거나 PAN-OS 11.0 릴리스에서 다운그레이드하기 전에 모든 업그레이드/다운그레이드 고려 사항을 이해해야 합니다. PAN-OS 11.0 릴리스에 대한 추가 정보는 PAN-OS 11.0 릴리스 노트를 참조하십시오.

기능	업그레이드 고려 사항	다운그레이드 고려 사항
클라우드 서비스 플러그인	최신 클라우드 서비스 플러그인 버전이 포함된 PAN-OS 11.0으로의 업그레이드는 지원되지 않습니다. 지원되지 않는 클라우드 서비스 플러그인 버전이 포함된 PAN-OS 11.0으로 업그레이드하면 Prisma Access 및 종속 플러그인 기능 모두에 영향을 미칠 수 있는 알 수 없거나 예기치 않은 문제가 발생할 수 있습니다.	없음.
Panorama 가상 어플라이언스에 대한 최소 시스템 메모리 요구 사항	Palo Alto Networks는 권장 Panorama 가상 어플라이언스 메모리 요구 사항을 32GB에서 최소 64GB로 늘렸습니다. 이는 Panorama 및 Log Collector 모드의 Panorama 가상 어플라이언스에 영향을 미쳐 프로비저닝이 부족한 Panorama 가상 어플라이언스와 관련된 로깅, 관리 및 운영 성능 문제를 방지합니다. 새로운 Panorama 가상 어플라이언스 배포의 경우 Palo Alto Networks는 최소 64GB의 가상 머신을 배포할 것을 권장합니다. 기존 Panroama 가상 디바이스 배포의 경우 PAN-OS 11.0으로 성공적으로 업그레이드한 후 기존 Panorama 가상 어플라이언스의 메모리를 늘리려면 Panorama 가상 디바이스의 CPU 및 메모리 늘리기를 참조하십시오.	없음.

기능	업그레이드 고려 사항	다운그레이드 고려 사항
관리 액세스를 위한 TLSv1.3 지원	방화벽을 업그레이드하면 방화벽이 관리 **TLS** 모드를 **excludetlsv1.3_only**로, 인증서를 없음으로 자동으로 설정합니다. 업그레이드 전에 SSL/TLS 서비스 프로필을 사용하여 관리 연결을 보호한 경우 프로필이 계속 작동합니다. 관리 액세스에 대한 TLSv1.3 지원을 사용 설정하려면 일반 설정(디바이스 > 설정 > 관리 > 일반 설정)으로 이동하여 관리 **TLS** 모드를 **tlsv1.3_only** 또는 혼합 모드로 설정한 다음 관리 서버 인증서를 선택해야 합니다. *TLSv1.3* 지원을 구성하면 업그레이드 전에 관리 연결에 사용되는 *SSL/TLS* 서비스 프로필이 비활성화됩니다.	PAN-OS 11.0에서 이전 PAN-OS 버전으로 다운그레이드하면 TLSv1.3 지원이 사라집니다. TLSv1.3 지원을 활성화했거나 관리 연결에 SSL/TLS 서비스 프로필을 사용하지 않은 경우 방화벽은 TLSv1.3(TLSv1.0-TLSv1.2) 및 관련 암호화 제품군을 제외한 모든 TLS 버전을 지원합니다. 그러나 다운그레이드하기 전에 SSL/TLS 서비스 프로필을 사용한 경우 방화벽은 해당 프로필을 계속 사용합니다.
사용자 지정 Syslog 형식	없음.	사용자 지정 syslog 형식(디바이스 > 서버 프로필 > **Syslog** 및 **Panorama** > 서버 프로필 > **Syslog**)를 최대 2,346자까지 늘려야 PAN-OS 10.2로 성공적으로 다운그레이드할 수 있습니다.
Cloud ID 엔진의 사용자 컨텍스트	Palo Alto Networks는 사용자 컨텍스트 클라우드 서비스를 활성화하기 전에 매핑 및 태그 재배포 아키텍처에 대한 자세한 기록을 생성할 것을 강력히 권장합니다. 다운그레이드가 필요한 경우 매핑 및 태그를 다시 채우도록 다운그레이드한 후 아키텍처 레코드	PANOS 11.0에서 이전 버전으로 다운그레이드한 후에는 사용자 컨텍스트 클라우드 서비스 옵션을 더 이상 사용할 수 없습니다. 또한, 다운그레이드는 다운그레이드된 디바이스에서 IP 주소-사용자 이름 매핑, IP 주소-포트 번호 매핑, 격리 목록, IP 주소-태그

기능	업그레이드 고려 사항	다운그레이드 고려 사항
	를 사용하여 해당 구성을 다시 만듭니다.	매핑 및 동적 사용자 그룹 태그를 지웁니다. 다운그레이드하기 전에 사용자 컨텍스트 클라우드 서비스 옵션을 활성화한 경우 다운그레이드 후 정보가 올바르게 다시 채워지도록 방화벽 또는 Panorama에서 매핑, 태그 및 격리 목록의 소스에 대해 이전 구성을 활성화합니다. Palo Alto Networks는 데이터의 기본 레코드를 설정하기 위해 다운그레이드하기 직전에 방화벽에서 다음 CLI 명령을 사용할 것을 권장합니다. 다운그레이드가 필요한 경우 다운그레이드 전후의 데이터를 비교하여 다운그레이드 후 방화벽에서 필요한 모든 데이터를 사용할 수 있는지 확인할 수 있습니다. • `show user ip-user-mapping all` 명령을 사용하여 현재 IP 주소-사용자 이름 매핑 수를 가져옵니다. • `show user ip-port-user-mapping all` 명령을 사용하여 현재 IP 주소-포트 번호 매핑 수를 가져옵니다. • 현재 IP 주소-태그 매핑 수를 얻으려면 `show object registered-ip all option count` 명령을 사용합니다. • `show object registered-user all`명령을 사용하여 태그-사용자 이름 매핑의 현재 수를 얻으십시오.

기능	업그레이드 고려 사항	다운그레이드 고려 사항
		• `debug user-id dump hip-profile-database` 명령을 사용하여 HIP 프로필과 연결된 모든 디바이스 목록을 가져옵니다. • 격리된 디바이스 목록을 PDF 또는 CSV로 내보냅니다. CLI 명령을 사용하여 다운그레이드 전후의 출력을 비교하여 데이터 양이 거의 동일한지 확인하고 방화벽을 사용하여 정책을 적용하기 전에 방화벽에서 필요한 데이터를 사용할 수 있는지 확인합니다. 격리 목록에 XML API 소스 및 수동으로 추가된 모든 디바이스에서 모든 매핑을 수동으로 복원해야 합니다. 격리 목록에 수동으로 추가된 XML API 및/또는 시스템을 사용하여 가져온 매핑 및 태그를 다시 가져오지 않고 다운그레이드 후 유효성을 검사하는 경우 이전에 격리된 사용자 및 디바이스가 더 이상 제한되지 않을 수 있으므로 보안 위험이 발생할 수 있습니다. 액세스 권한이 없는 리소스에 액세스합니다. 예를 들어, 검역을 위해 동적 사용자 그룹에 사용자를 추가한 XML API를 통해 특정 태그가 사용자에게 할당된 경우 해당 사용자는 다운그레이드 후 해당 사용자를 수동으로 추가할 때까지 더 이상 검역된 동적 사용자 그룹에 속하지 않습니다. 다운그레이드 전에 디바이스를 격리 목록에 수동으로 추가한 경우 다운그레이드 후 해당 디바이스를 수동으로 추가

기능	업그레이드 고려 사항	다운그레이드 고려 사항
		해야 합니다. 그렇지 않으면 디바이스가 더 이상 격리되지 않아 보안 위험이 발생할 수 있습니다.
NetBIOS 클라이언트 검색을 사용한 사용자 매핑	User-ID의 보안을 더욱 강화하고 구성 오류로 인한 잠재적인 보안 취약성을 제거하기 위한 지속적인 노력의 일환으로 사용자 매핑의 오래된 NetBIOS 클라이언트 검색 방법은 이 버전에서 더 이상 지원되지 않습니다. 현재 이 방법을 사용하여 사용자 매핑을 수집하는 경우 사용자 식별이 중단되지 않도록 업그레이드하기 전에 대체 방법을 구성해야 합니다. 대체 매핑 방법에 대한 자세한 내용은 PAN-OS 문서를 참조하십시오. 업그레이드 후에는 NetBIOS 클라이언트 프로빙(디바이스 > 사용자 식별 > 사용자 매핑 > **Palo Alto Networks User-ID** 에이전트 설정 > 클라이언트 프로빙)을 더 이상 사용할 수 없습니다. Windows User-ID 에이전트 버전 11.0에서는 NetBIOS 클라이언트 검색도 더 이상 사용할 수 없습니다.	없음.
HTTP 프록시를 통한 OCSP	없음.	PAN-OS 11.0 이전 버전으로 다운그레이드하는 경우 CRL(Certificate Revocation List) 방법을 사용하여 인증서 상태를 확인해야 합니다. OCSP 트래픽은 PAN-OS 11.0 이전 버전의 PAN-OS에서 HTTP 프록시를 통과할 수 없습니다.

방화벽을 PAN-OS 11.0으로 업그레이드

PAN-OS 11.0으로 업그레이드하는 방법은 고가용성(HA) 구성에 독립 실행형 방화벽이 있는지 또는 방화벽이 있는지 여부와 어느 시나리오에서든 Panorama를 사용하여 방화벽을 관리하는지 여부에 따라 다릅니다. PAN-OS 11.0 릴리스 노트를 검토한 다음 배포에 해당하는 절차를 따릅니다.

- PAN-OS 11.0으로의 업그레이드 경로 결정
- 방화벽을 Panorama에서 PAN-OS 11.0으로 업그레이드
- 독립 실행형 방화벽 업그레이드
- HA 방화벽 쌍 업그레이드

콘텐츠를 *WildFire* 어플라이언스로 포워딩하도록 구성된 *Panorama* 또는 방화벽으로 관리하는 방화벽을 업그레이드할 때는 먼저 Panorama 및 Log Collector를 업그레이드해야 하며, 그런 다음 방화벽을 업그레이드하기 전에 WildFire 어플라이언스를 업그레이드하십시오.

또한 *Panorama*보다 최신 유지 관리 릴리스를 실행하는 방화벽을 관리하는 것은 기능이 예상대로 작동하지 않을 수 있으므로 관리하지 않는 것이 좋습니다. 예를 들어 *Panorama*에서 *PAN-OS 10.1.0*을 실행 중인 경우 *PAN-OS 10.1.1* 이상의 유지 관리 릴리스를 실행하는 방화벽을 관리하지 않는 것이 좋습니다.

PAN-OS 11.0으로의 업그레이드 경로 결정

하나의 PAN-OS 기능 릴리스 버전에서 이후 기능 릴리스로 업그레이드할 때 대상 릴리스 경로에 있는 기능 릴리스 버전 설치를 건너뛸 수 없습니다. 또한, 권장되는 업그레이드 경로에는 다음 기능 릴리스 버전의 기본 이미지를 다운로드하기 전에 각 릴리스 버전에 최신 유지관리 릴리스를 설치하는 것이 포함됩니다. 사용자의 가동 중지 시간을 최소화하려면 업무 시간이 아닌 시간에 업그레이드를 수행하십시오.

수동 업그레이드의 경우 *Palo Alto Networks*는 업그레이드 경로에 따라 각 *PAN-OS* 릴리스에 대해 최신 유지관리 릴리스를 설치하고 업그레이드할 것을 권장합니다. 업그레이드할 대상 릴리스가 아니면 기능 릴리스용 *PAN-OS* 기본 이미지를 설치하지 마십시오.

다음과 같이 업그레이드 경로를 결정합니다.

STEP 1 | 현재 설치된 버전을 식별합니다.

- Panorama에서 **Panorama** > 관리 디바이스를 선택하고 업그레이드하려는 방화벽의 소프트웨어 버전을 확인합니다.
- 방화벽에서 디바이스 > 소프트웨어를 선택하고 현재 설치된 열에서 확인 표시가 있는 버전을 확인합니다.

STEP 2 | 업그레이드 경로 식별:

업그레이드 경로의 일부로 통과하는 각 릴리스에 대한 릴리스 정보 및 다운그레이드 고려 사항에서 알려진 문제 및 기본 동작에 대한 변경 사항을 검토합니다.

설치된 **PAN-OS** 버전	**PAN-OS 11.0**으로의 권장 업그레이드 경로
10.2.x	• 이미 PAN-OS 10.2 릴리스를 실행 중인 경우 PAN-OS 11.0으로 직접 업그레이드할 수 있습니다.
10.1.x	이제 소프트웨어 버전 업그레이드 건너뛰기 기능을 사용하여 PAN-OS 10.1 이상 릴리스에서 디바이스를 업그레이드할 때 소프트웨어 버전을 건너뛸 수 있습니다. • 이미 PAN-OS 10.1 릴리스를 실행 중인 경우 PAN-OS 11.0으로 직접 업그레이드할 수 있습니다.
10.0.x	• 최신 기본 PAN-OS 10.0 유지보수 릴리스를 다운로드하여 설치하고 재부팅하십시오. • PAN-OS 10.1.0을 다운로드합니다. • 최신 기본 PAN-OS 10.1 유지관리 릴리스를 다운로드 및 설치하고 재부팅합니다. • PAN-OS 10.2.0을 다운로드합니다. • 최신 기본 PAN-OS 10.2 유지관리 릴리스를 다운로드하여 설치하고 재부팅합니다. • 방화벽을 PAN-OS 11.0으로 업그레이드를 진행합니다.
9.1.x	• 최신 기본 PAN-OS 9.1 유지보수 릴리스를 다운로드하여 설치하고 재부팅하십시오. • PAN-OS 10.0.0 을 다운로드합니다. • 최신 기본 PAN-OS 10.0 유지보수 릴리스를 다운로드하여 설치하고 재부팅하십시오. • PAN-OS 10.1.0을 다운로드합니다. • 최신 기본 PAN-OS 10.1 유지관리 릴리스를 다운로드 및 설치하고 재부팅합니다. • PAN-OS 10.2.0을 다운로드합니다. • 최신 기본 PAN-OS 10.2 유지관리 릴리스를 다운로드하여 설치하고 재부팅합니다.

설치된 **PAN-OS** 버전	**PAN-OS 11.0**으로의 권장 업그레이드 경로
	• 방화벽을 PAN-OS 11.0으로 업그레이드를 진행합니다.
9.0.x	• 최신 기본 PAN-OS 9.0 유지보수 릴리스를 다운로드하여 설치하고 재부팅하십시오. 로그 수집기를 최신 *PAN-OS 9.0* 유지 관리 릴리스로 업그레이드하기 전에 업그레이드/다운그레이드 고려 사항을 검토합니다. • PAN-OS 9.1.0을 다운로드합니다. • 최신 기본 PAN-OS 9.1 유지보수 릴리스를 다운로드하여 설치하고 재부팅하십시오. • PAN-OS 10.0.0 을 다운로드합니다. • 최신 기본 PAN-OS 10.0 유지보수 릴리스를 다운로드하여 설치하고 재부팅하십시오. • PAN-OS 10.1.0을 다운로드합니다. • 최신 기본 PAN-OS 10.1 유지관리 릴리스를 다운로드 및 설치하고 재부팅합니다. • PAN-OS 10.2.0을 다운로드합니다. • 최신 기본 PAN-OS 10.2 유지관리 릴리스를 다운로드하여 설치하고 재부팅합니다. • 방화벽을 PAN-OS 11.0으로 업그레이드를 진행합니다.
8.1.x	• 최신 기본 PAN-OS 8.1 유지보수 릴리스를 다운로드하여 설치하고 재부팅하십시오. • 다운로드 PAN-OS 9.0.0 • 최신 기본 PAN-OS 9.0 유지보수 릴리스를 다운로드하여 설치하고 재부팅하십시오. 로그 수집기를 최신 *PAN-OS 9.0* 유지 관리 릴리스로 업그레이드하기 전에 업그레이드/다운그레이드 고려 사항을 검토합니다. • PAN-OS 9.1.0을 다운로드합니다.

설치된 **PAN-OS** 버전	**PAN-OS 11.0**으로의 권장 업그레이드 경로
	• 최신 기본 PAN-OS 9.1 유지보수 릴리스를 다운로드하여 설치하고 재부팅하십시오. • PAN-OS 10.0.0 을 다운로드합니다. • 최신 기본 PAN-OS 10.0 유지보수 릴리스를 다운로드하여 설치하고 재부팅하십시오. • PAN-OS 10.1.0을 다운로드합니다. • 최신 기본 PAN-OS 10.1 유지관리 릴리스를 다운로드 및 설치하고 재부팅합니다. • PAN-OS 10.2.0을 다운로드합니다. • 최신 기본 PAN-OS 10.2 유지관리 릴리스를 다운로드하여 설치하고 재부팅합니다. • 방화벽을 PAN-OS 11.0으로 업그레이드를 진행합니다.
8.0.x	• PAN-OS 8.0.20을 다운로드하여 설치하고 재부팅하십시오. • PAN-OS 8.1.0을 다운로드합니다. • 최신 기본 PAN-OS 8.1 유지보수 릴리스를 다운로드하여 설치하고 재부팅하십시오. • 다운로드 PAN-OS 9.0.0 • 최신 기본 PAN-OS 9.0 유지보수 릴리스를 다운로드하여 설치하고 재부팅하십시오. 로그 수집기를 최신 *PAN-OS 9.0* 유지 관리 릴리스로 업그레이드하기 전에 업그레이드/다운그레이드 고려 사항을 검토합니다. • PAN-OS 9.1.0을 다운로드합니다. • 최신 기본 PAN-OS 9.1 유지보수 릴리스를 다운로드하여 설치하고 재부팅하십시오. • PAN-OS 10.0.0 을 다운로드합니다. • 최신 기본 PAN-OS 10.0 유지보수 릴리스를 다운로드하여 설치하고 재부팅하십시오. • PAN-OS 10.1.0을 다운로드합니다. • 최신 기본 PAN-OS 10.1 유지관리 릴리스를 다운로드 및 설치하고 재부팅합니다.

설치된 **PAN-OS** 버전	**PAN-OS 11.0**으로의 권장 업그레이드 경로
	• 방화벽을 PAN-OS 11.0으로 업그레이드를 진행합니다.
7.1.x	• PAN-OS 7.1.26 유지 관리 릴리스를 다운로드하여 설치하고 재부팅합니다. • PAN-OS 8.0.0을 다운로드합니다. • PAN-OS 8.0.20을 다운로드하여 설치합니다. • PAN-OS 8.1.0을 다운로드합니다. • 최신 기본 PAN-OS 8.1 유지보수 릴리스를 다운로드하여 설치하고 재부팅하십시오. • 다운로드 PAN-OS 9.0.0 • 최신 기본 PAN-OS 9.0 유지보수 릴리스를 다운로드하여 설치하고 재부팅하십시오. 로그 수집기를 최신 *PAN-OS 9.0* 유지 관리 릴리스로 업그레이드하기 전에 업그레이드/다운그레이드 고려 사항을 검토합니다. • PAN-OS 9.1.0을 다운로드합니다. • 최신 기본 PAN-OS 9.1 유지보수 릴리스를 다운로드하여 설치하고 재부팅하십시오. • PAN-OS 10.0.0 을 다운로드합니다. • 최신 기본 PAN-OS 10.0 유지보수 릴리스를 다운로드하여 설치하고 재부팅하십시오. • PAN-OS 10.1.0을 다운로드합니다. • 최신 기본 PAN-OS 10.1 유지관리 릴리스를 다운로드 및 설치하고 재부팅합니다. • 방화벽을 PAN-OS 11.0으로 업그레이드를 진행합니다.

독립 실행형 방화벽 업그레이드

PAN-OS 11.0 릴리스 노트를 검토한 후 다음 절차에 따라 HA 구성에 없는 방화벽을 PAN-OS 11.0으로 업그레이드합니다.

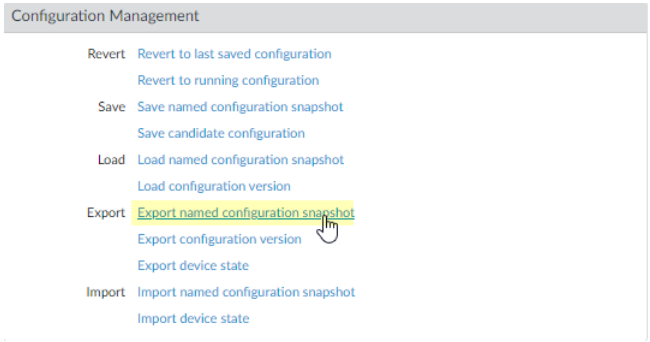
방화벽이 분석을 위해 샘플을 *WildFire* 어플라이언스로 포워딩하도록 구성된 경우 포워딩 방화벽을 업그레이드하기 전에 WildFire 어플라이언스를 업그레이드해야 합니다.

트래픽에 영향을 주지 않으려면 중단 기간 내에 업그레이드를 계획하십시오. 방화벽이 안정적인 전원에 연결되어 있는지 확인하십시오. 업그레이드 중 전원이 손실되면 방화벽을 사용할 수 없게 될 수 있습니다.

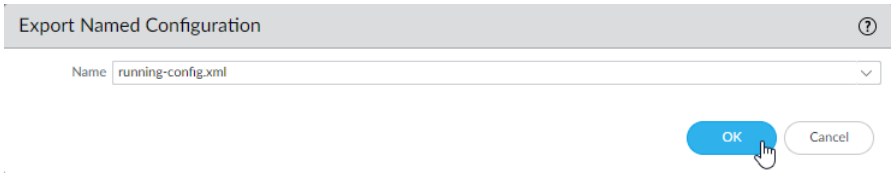
STEP 1 | 현재 구성 파일의 백업을 저장합니다.

방화벽이 구성 백업을 자동으로 생성하지만 업그레이드하기 전에 백업을 생성하고 외부에 저장하는 것이 가장 좋습니다.

1. 디바이스 > 설정 > 작업을 선택하고 이름이 지정된 구성 스냅샷 내보내기를 클릭합니다.



2. 실행 중인 구성이 포함된 XML 파일(예: **running-config.xml**)을 선택하고 확인을 클릭하여 구성 파일을 내보냅니다.



3. 내보낸 파일을 방화벽 외부 위치에 저장합니다. 업그레이드에 문제가 있는 경우 이 백업을 사용하여 구성을 복원할 수 있습니다.

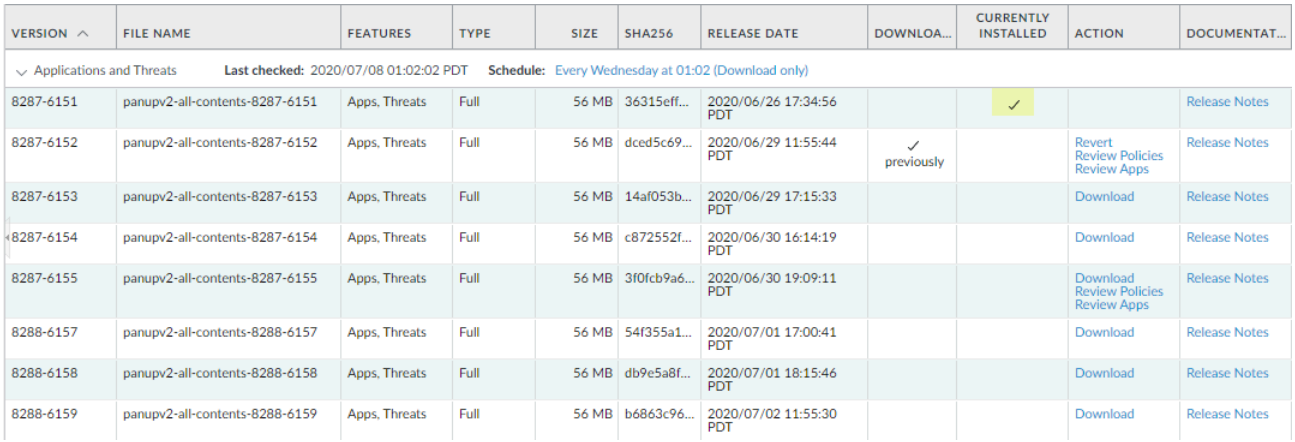
STEP 2 | (선택 사항) User-ID를 활성화한 경우 업그레이드 후 방화벽은 현재 IP 주소-사용자명 및 그룹 매핑을 지워 User-ID 소스의 속성으로 다시 채울 수 있습니다. 환경에서 매핑을 다시 채우는 데 필요한 시간을 예측하려면 방화벽에서 다음 CLI 명령을 실행합니다.

- IP 주소-사용자명 매핑의 경우:
  - `### User-ID #### ## ## ##`
  - `### ## ### ## ## ##`
- 그룹 매핑의 경우: `### ## ## ## ##`

STEP 3 | 방화벽이 최신 콘텐츠 릴리스 버전을 실행 중인지 확인하십시오.

PAN-OS 11.0 릴리스용으로 설치해야 하는 최소 콘텐츠 릴리스 버전은 릴리스 노트를 참조하십시오. 애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례을(를) 따릅니다.

1. 디바이스 > 동적 업데이트를 선택하고 현재 설치된 애플리케이션 또는 애플리케이션 및 위협 콘텐츠 릴리스 버전을 확인합니다.



VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOA...	CURRENTLY INSTALLED	ACTION	DOCUMENTAT...
Applications and Threats	**Last checked:** 2020/07/08 01:02:02 PDT	**Schedule:** Every Wednesday at 01:02 (Download only)								
8287-6151	panupv2-all-contents-8287-6151	Apps, Threats	Full	56 MB	36315eff...	2020/06/26 17:34:56 PDT		✓		Release Notes
8287-6152	panupv2-all-contents-8287-6152	Apps, Threats	Full	56 MB	dced5c69...	2020/06/29 11:55:44 PDT	✓ previously		Revert Review Policies Review Apps	Release Notes
8287-6153	panupv2-all-contents-8287-6153	Apps, Threats	Full	56 MB	14af053b...	2020/06/29 17:15:33 PDT			Download	Release Notes
8287-6154	panupv2-all-contents-8287-6154	Apps, Threats	Full	56 MB	c872552f...	2020/06/30 16:14:19 PDT			Download	Release Notes
8287-6155	panupv2-all-contents-8287-6155	Apps, Threats	Full	56 MB	3f0fcb9a6...	2020/06/30 19:09:11 PDT			Download Review Policies Review Apps	Release Notes
8288-6157	panupv2-all-contents-8288-6157	Apps, Threats	Full	56 MB	54f355a1...	2020/07/01 17:00:41 PDT			Download	Release Notes
8288-6158	panupv2-all-contents-8288-6158	Apps, Threats	Full	56 MB	db9e5a8f...	2020/07/01 18:15:46 PDT			Download	Release Notes
8288-6159	panupv2-all-contents-8288-6159	Apps, Threats	Full	56 MB	b6863c96...	2020/07/02 11:55:30 PDT			Download	Release Notes

2. 방화벽이 최소 필수 콘텐츠 릴리스 버전 또는 PAN-OS 11.0에 필요한 이후 버전을 실행하지 않는 경우 지금 확인하여 사용 가능한 업데이트 목록을 검색합니다.
3. 원하는 콘텐츠 릴리스 버전을 찾아 다운로드합니다.

   콘텐츠 업데이트 파일을 성공적으로 다운로드하면 작업 열의 링크가 해당 콘텐츠 릴리스 버전에 대해 다운로드에서 설치로 변경됩니다.
4. 업데이트를 설치합니다.

STEP 4 | PAN-OS 11.0으로의 업그레이드 경로 결정

업그레이드 경로의 일부로 통과하는 각 릴리스에 대한 릴리스 노트 및 다운그레이드 고려 사항의 알려진 문제 및 기본 동작에 대한 변경 사항은 PAN-OS 업그레이드 점검표에서 확인할 수 있습니다.

STEP 5 | (모범 사례) Cortex Data Lake(CDL)를 활용하는 경우 디바이스 인증서를 설치합니다.

방화벽은 PAN-OS 11.0으로 업그레이드할 때 CDL 수집 및 쿼리 엔드포인트 인증을 위해 디바이스 인증서를 사용하도록 자동으로 전환됩니다.

*PAN-OS 11.0*으로 업그레이드하기 전에 디바이스 인증서를 설치하지 않으면 방화벽은 인증을 위해 기존 로깅 서비스 인증서를 계속 사용합니다.

STEP 6 | PAN-OS 11.0으로 업그레이드합니다.

방화벽이 관리 포트에서 인터넷에 액세스할 수 없는 경우 Palo Alto Networks 고객 지원 포털에서 소프트웨어 이미지를 다운로드한 다음 방화벽에 수동으로 업로드할 수 있습니다.

1. 디바이스 > 소프트웨어를 선택하고 지금 확인을 클릭하여 최신 PAN-OS 업데이트를 표시합니다.

   사용 가능한 다음 PAN-OS 릴리스의 버전만 표시됩니다. 예를 들어, PAN-OS 11.0이 방화벽에 설치된 경우 PAN-OS 11.0 릴리스만 표시됩니다.
2. **Panorama** > 디바이스 배포 > 소프트웨어 > 작업 > 검증을 선택합니다.

   Panorama > 디바이스 배포 > 소프트웨어 > 작업 > 확인 모든 중간 소프트웨어 및 콘텐츠 이미지 보기 11.0.0으로 업그레이드해야 합니다.
3. 중간 소프트웨어 및 콘텐츠 이미지를 다운로드합니다.
4. 이미지를 다운로드한 후(또는 수동 업그레이드의 경우 이미지를 업로드한 후) 이미지를 설치합니다.
5. 설치가 성공적으로 완료되면 다음 방법 중 하나를 사용하여 재부팅합니다.
   - 재부팅하라는 메시지가 표시되면 예를 클릭합니다.
   - 재부팅하라는 메시지가 표시되지 않으면 디바이스 > 설정 > 작업을 선택하고 디바이스 재부팅을 클릭합니다.

   이 시점에서 방화벽은 *User-ID* 매핑을 지운 다음 *User-ID* 소스에 연결하여 매핑을 다시 채웁니다.
6. User-ID를 활성화한 경우 다음 CLI 명령을 사용하여 트래픽을 허용하기 전에 방화벽이 IP 주소-사용자명 및 그룹 매핑을 다시 채웠는지 확인합니다.
   - `### ip-user-mapping ## ##`
   - `### ## ## ##`

STEP 7 | OpenSSL 보안 수준 2를 준수하도록 모든 인증서를 재생성하거나 다시 가져옵니다.

PAN-OS 11.0으로 업그레이드할 때는 모든 인증서가 다음과 같은 최소 요구 사항을 충족해야 합니다.

- RSA 2048비트 이상 또는 ECDSA 256비트 이상
- SHA256 이상의 다이제스트

인증서 재생성 또는 다시 가져오기에 대한 자세한 내용은 PAN-OS 관리자 가이드를 참조하십시오.

STEP 8 | 방화벽이 트래픽을 전달하는지 확인합니다.

모니터 > 세션 브라우저를 선택하고 새 세션이 표시되는지 확인합니다.

	START TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATI...	FROM PORT	TO PORT	PROTOC...	APPLICATI...	RULE	INGRESS I/F	EGRESS I/F	BYTES	VIRTUAL SYSTEM
⊞	07/08 11:29:02	z1	z2			56622	44060	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	558	vsys1
⊞	07/08 11:29:00	z1	z2			44823	42573	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	277874	vsys1
⊞	07/08 11:29:10	z1	z2			60162	47273	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	580	vsys1
⊞	07/08 11:29:10	z1	z2			45751	6013	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	560	vsys1
⊞	07/08 11:29:00	z1	z2			52923	42559	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	111119	vsys1
⊞	07/08 11:29:12	z1	z2			45772	8348	6	ftp-data	rules6-clone-with-group	ethernet1/3	ethernet1/4	785	vsys1
⊞	07/08 11:29:10	z1	z2			39762	61408	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	554	vsys1
⊞	07/08 11:29:06	z1	z2			53948	56596	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	792	vsys1
⊞	07/08 11:28:11	z1	z2			38185	42186	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	3243	vsys1

STEP 9 | 방화벽에서 소프트웨어 업그레이드 기록을 볼 수 있습니다.

1. 방화벽 인터페이스에 로그인합니다.
2. 디바이스 > 요약 > 소프트웨어로 이동하여 디바이스 기록을 클릭합니다.

HA 방화벽 쌍 업그레이드

PAN-OS 11.0 릴리스 노트를 검토한 후 다음 절차를 사용하여 고가용성(HA) 구성에서 한 쌍의 방화벽을 업그레이드합니다. 이 절차는 능동형/수동형 및 능동형/능동형 구성 모두에 적용됩니다.

고가용성(HA) 구성에 있는 방화벽을 업그레이드할 때 가동 중지 시간을 방지하려면 한 번에 하나의 HA 피어를 업데이트하십시오. 활성/활성 방화벽의 경우 먼저 업그레이드하는 피어는 중요하지 않습니다(단순화를 위해 이 절차에서는 활성 기본 피어를 먼저 업그레이드하는 방법을 보여줍니다). 활성/수동 방화벽의 경우 먼저 활성(기본) 피어를 일시 중지(페일오버)하고 업그레이드해야 합니다. 기본 피어를 업그레이드한 후에는 기본 피어를 일시 중지를 해제하여 작동 상태(수동)로 되돌려야 합니다. 다음으로 수동(보조) 피어를 일시 중단하여 기본 피어를 다시 활성화해야 합니다. 기본 피어가 활성화되고 보조 피어가 일시 중단된 후 업그레이드를 계속할 수 있습니다. HA 피어 업그레이드 중 페일오버를 방지하려면 업그레이드를 진행하기 전에 선점이 비활성화되었는지 확인해야 합니다. 쌍의 한 피어에서만 선점을 비활성화하면 됩니다.

여러 기능 PAN-OS 릴리스에서 HA 방화벽을 업그레이드하는 경우 계속하기 전에 각 HA 피어를 업그레이드 경로에서 동일한 기능 PAN-OS 릴리스로 업그레이드해야 합니다. 예를 들어, PAN-OS 10.0에서 PAN-OS 11.0으로 HA 피어를 업그레이드하는 중입니다. 대상 PAN-OS 11.0 릴리스로 계속 업그레이드하려면 먼저 두 HA 피어를 모두 PAN-OS 10.1로 업그레이드해야 합니다. HA 피어가 2개 이상의 기능 릴리스와 떨어져 있는 경우 이전 릴리스가 설치된 방화벽은 ## ### ## ### 메시지와 함께 ## ### 상태가 됩니다.

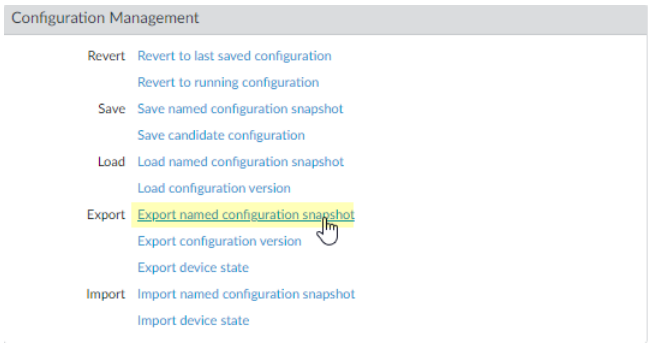
트래픽에 영향을 주지 않으려면 중단 기간 내에 업그레이드를 계획하십시오. 방화벽이 안정적인 전원에 연결되어 있는지 확인하십시오. 업그레이드 중 전원이 손실되면 방화벽을 사용할 수 없게 될 수 있습니다.

STEP 1 | 현재 구성 파일의 백업을 저장합니다.

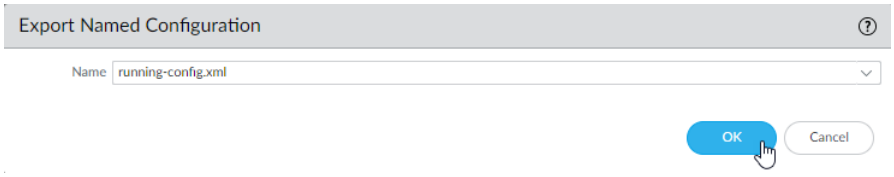
방화벽이 구성 백업을 자동으로 생성하지만 업그레이드하기 전에 백업을 생성하고 외부에 저장하는 것이 가장 좋습니다.

쌍의 각 방화벽에서 다음 단계를 수행하십시오.

1. 디바이스 > 설정 > 작업을 선택하고 이름이 지정된 구성 스냅샷 내보내기를 클릭합니다.



2. 실행 중인 구성이 포함된 XML 파일(예: **running-config.xml**)을 선택하고 확인을 클릭하여 구성 파일을 내보냅니다.



3. 내보낸 파일을 방화벽 외부 위치에 저장합니다. 업그레이드에 문제가 있는 경우 이 백업을 사용하여 구성을 복원할 수 있습니다.

STEP 2 | 디바이스 > 지원 및 기술 지원 파일 생성을 선택합니다.

기술 지원 파일을 생성하라는 메시지가 표시되면 예를 클릭합니다.

STEP 3 | HA 쌍의 각 방화벽이 최신 콘텐츠 릴리스 버전을 실행 중인지 확인하십시오.

PAN-OS 11.0 릴리스용으로 설치해야 하는 최소 콘텐츠 릴리스 버전은 릴리스 노트를 참조하십시오. 애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례을(를) 따릅니다.

1. 디바이스 > 동적 업데이트을 선택하고 애플리케이션 또는 애플리케이션 및 위협을 확인하여 현재 설치된 업데이트를 확인합니다.

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOA...	CURRENTLY INSTALLED	ACTION	DOCUMENTAT...
Applications and Threats	**Last checked:** 2020/07/08 01:02:02 PDT	**Schedule:** Every Wednesday at 01:02 (Download only)								
8287-6151	panupv2-all-contents-8287-6151	Apps, Threats	Full	56 MB	36315eff...	2020/06/26 17:34:56 PDT		✓		Release Notes
8287-6152	panupv2-all-contents-8287-6152	Apps, Threats	Full	56 MB	dced5c69...	2020/06/29 11:55:44 PDT	✓ previously		Revert Review Policies Review Apps	Release Notes
8287-6153	panupv2-all-contents-8287-6153	Apps, Threats	Full	56 MB	14af053b...	2020/06/29 17:15:33 PDT			Download	Release Notes
8287-6154	panupv2-all-contents-8287-6154	Apps, Threats	Full	56 MB	c872552f...	2020/06/30 16:14:19 PDT			Download	Release Notes
8287-6155	panupv2-all-contents-8287-6155	Apps, Threats	Full	56 MB	3f0fcb9a6...	2020/06/30 19:09:11 PDT			Download Review Policies Review Apps	Release Notes
8288-6157	panupv2-all-contents-8288-6157	Apps, Threats	Full	56 MB	54f355a1...	2020/07/01 17:00:41 PDT			Download	Release Notes
8288-6158	panupv2-all-contents-8288-6158	Apps, Threats	Full	56 MB	db9e5a8f...	2020/07/01 18:15:46 PDT			Download	Release Notes
8288-6159	panupv2-all-contents-8288-6159	Apps, Threats	Full	56 MB	b6863c96...	2020/07/02 11:55:30 PDT			Download	Release Notes

2. 방화벽이 최소 필수 콘텐츠 릴리스 버전 또는 PAN-OS 11.0에 필요한 이후 버전을 실행하지 않는 경우 지금 확인하여 사용 가능한 업데이트 목록을 검색합니다.
3. 원하는 콘텐츠 릴리스 버전을 찾아 다운로드합니다.

   콘텐츠 업데이트 파일을 성공적으로 다운로드하면 작업 열의 링크가 해당 콘텐츠 릴리스 버전에 대해 다운로드에서 설치로 변경됩니다.
4. 업데이트를 설치합니다. 두 피어 모두에 업데이트를 설치해야 합니다.

STEP 4 | PAN-OS 11.0으로의 업그레이드 경로 결정

현재 실행 중인 PAN-OS 버전에서 PAN-OS 11.0으로 이동하는 경로에 있는 기능 릴리스 버전의 설치를 건너뛸 수 없습니다.

업그레이드 경로의 일부로 통과하는 각 릴리스에 대한 릴리스 노트 및 다운그레이드 고려 사항의 알려진 문제 및 기본 동작에 대한 변경 사항은 PAN-OS 업그레이드 점검표에서 확인할 수 있습니다.

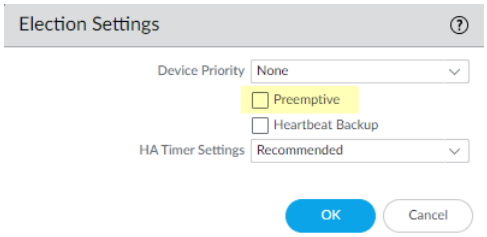
STEP 5 | (모범 사례) CDL(Cortex Data Lake)을 활용하는 경우 각 HA 피어에 디바이스 인증서를 설치합니다.

방화벽은 PAN-OS 11.0으로 업그레이드할 때 CDL 수집 및 쿼리 엔드포인트 인증을 위해 디바이스 인증서를 사용하도록 자동으로 전환됩니다.

*PAN-OS 11.0*으로 업그레이드하기 전에 디바이스 인증서를 설치하지 않으면 방화벽은 인증을 위해 기존 로깅 서비스 인증서를 계속 사용합니다.

STEP 6 | 각 쌍의 첫 번째 피어에서 선점을 비활성화합니다. HA 쌍의 한 방화벽에서만 이 설정을 비활성화해야 하지만 업그레이드를 진행하기 전에 커밋이 성공했는지 확인합니다.

1. 디바이스 > 고가용성을 선택하고 일렉션**(election)** 설정을 편집합니다.
2. 활성화된 경우 선점 설정을 비활성화(지우기)하고 확인을 클릭합니다.



3. 변경 사항을 커밋합니다.

STEP 7 | 페일오버를 강제 실행하려면 HA 피어를 일시 중단합니다.

(활성/수동 방화벽) 활성/수동 HA 구성의 방화벽의 경우 먼저 활성 HA 피어를 일시 중단하고 업그레이드합니다.

(활성/활성 방화벽) 활성/활성 HA 구성의 방화벽의 경우 활성-기본 HA 피어를 먼저 일시 중단하고 업그레이드합니다.

1. 디바이스 > 고가용성 > 작업 명령 및 고가용성을 위해 로컬 디바이스 일시중단을 선택합니다.
2. 오른쪽 하단에서 해당 상태가 ## ##인지 확인합니다.

   그 결과 장애 조치로 인해 보조 HA 피어가 ## 상태로 전환되어야 합니다.

   결과적인 장애 조치는 업그레이드하기 전에 *HA* 장애 조치가 제대로 작동하는지 확인합니다.

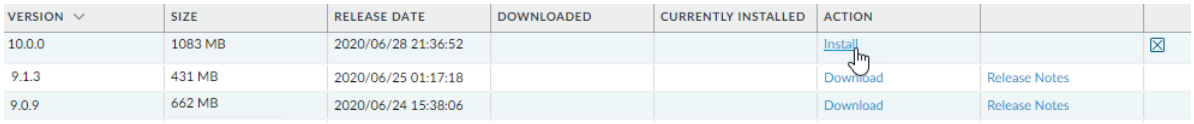
STEP 8 | 일시 중단된 HA 피어에 PAN-OS 11.0을 설치합니다.

1. 기본 HA 피어에서, 디바이스 > 소프트웨어를 선택하고 지금 확인을 클릭하여 최신 업데이트를 확인합니다.

   사용 가능한 다음 PAN-OS 릴리스의 버전만 표시됩니다. 예를 들어, PAN-OS 11.0이 방화벽에 설치된 경우 PAN-OS 11.0 릴리스만 표시됩니다.
2. PAN-OS 11.0.0을 찾아 다운로드합니다.

   방화벽이 관리 포트에서 인터넷에 액세스할 수 없는 경우 Palo Alto Networks 지원 포털에서 소프트웨어 이미지를 다운로드한 다음 방화벽에 수동으로 업로드할 수 있습니다.

   방화벽이 인터넷에 액세스할 수 있고 파일 다운로드 오류가 발생하면 지금 확인을 다시 클릭하여 *PAN-OS* 이미지 목록을 새로 고칩니다.
3. 이미지를 다운로드한 후(또는 수동 업그레이드의 경우 이미지를 업로드한 후) 이미지를 설치합니다.



4. 설치가 성공적으로 완료되면 다음 방법 중 하나를 사용하여 재부팅합니다.
   - 재부팅하라는 메시지가 표시되면 예를 클릭합니다.
   - 재부팅하라는 메시지가 표시되지 않으면 디바이스 > 설정 > 작업 및 디바이스 재부팅을 선택합니다.
5. 디바이스 재부팅이 완료되면 대시보드에서 고가용성 위젯을 보고 방금 업그레이드한 디바이스가 피어와 동기화되어 있는지 확인합니다.

STEP 9 | HA 기능을 기본 HA 피어로 복원합니다.

1. 디바이스 > 고가용성 > 작동 명령 및 고가용성을 위해 로컬 디바이스 작동을 선택합니다.
2. 오른쪽 하단에서 상태가 ##인지 확인합니다. 활성/활성 구성의 방화벽의 경우 상태가 ##인지 확인합니다.
3. HA 피어 실행 구성이 동기화될 때까지 기다립니다.

   대시보드에서 고가용성 위젯에서 실행 중인 구성 상태를 모니터링합니다.

STEP 10 | 보조 HA 피어에서 HA 피어를 일시 중단합니다.

1. 디바이스 > 고가용성 > 작업 명령 및 고가용성을 위해 로컬 디바이스 일시중단을 선택합니다.
2. 오른쪽 하단에서 해당 상태가 ## ##인지 확인합니다.

   그 결과 장애 조치로 인해 기본 HA 피어가 ## 상태로 전환되어야 합니다.

STEP 11 | 보조 HA 피어에 PAN-OS 11.0을 설치합니다.

1. 보조 피어에서, 디바이스 > 소프트웨어를 선택하고 지금 확인을 클릭하여 최신 업데이트를 확인합니다.
2. PAN-OS 11.0.0을 찾아 다운로드합니다.
3. 이미지를 다운로드한 후 설치합니다.
4. 설치가 성공적으로 완료되면 다음 방법 중 하나를 사용하여 재부팅합니다.
   - 재부팅하라는 메시지가 표시되면 예를 클릭합니다.
   - 재부팅하라는 메시지가 표시되지 않으면 디바이스 > 설정 > 작업 및 디바이스 재부팅을 선택합니다.

STEP 12 | HA 기능을 보조 HA 피어로 복원합니다.

1. 디바이스 > 고가용성 > 작동 명령 및 고가용성을 위해 로컬 디바이스 작동을 선택합니다.
2. 오른쪽 하단에서 상태가 ##인지 확인합니다. 활성/활성 구성의 방화벽의 경우 상태가 ##인지 확인합니다.
3. HA 피어 실행 구성이 동기화될 때까지 기다립니다.

   대시보드에서 실행 중인 구성 상태 고가용성 위젯을 모니터링합니다.

STEP 13 | 이전 단계에서 비활성화했던 HA 피어에서 선점을 다시 활성화합니다.

1. 디바이스 > 고가용성을 선택하고 일렉션**(election)** 설정을 편집합니다.
2. 선점 설정을 활성화(선택)하고 **OK**를 클릭합니다.
3. 변경 사항을 커밋합니다.

STEP 14 | OpenSSL 보안 수준 2를 준수하도록 모든 인증서를 재생성하거나 다시 가져옵니다.

PAN-OS 11.0으로 업그레이드할 때는 모든 인증서가 다음과 같은 최소 요구 사항을 충족해야 합니다.

- RSA 2048비트 이상 또는 ECDSA 256비트 이상
- SHA256 이상의 다이제스트

PAN-OS 관리자 가이드를 참조하거나 인증서 재생성 또는 다시 가져오기에 대한 자세한 내용은 Panorama 관리자 가이드를 참조하십시오.

STEP 15 | 두 피어가 예상대로 트래픽을 전달하는지 확인하십시오.

능동형/수동형 구성에서는 활성 피어만 트래픽을 전달해야 합니다. 두 피어 모두 능동형/능동형 구성에서 트래픽을 전달해야 합니다.

다음 CLI 명령을 실행하여 업그레이드가 성공했는지 확인합니다.

- (활성 피어만) 활성 피어가 트래픽을 전달하는지 확인하려면 **`show session all`** 명령을 실행합니다.
- 세션 동기화를 확인하려면 **`show high-availability interface ha2`** 명령을 실행하고 CPU 테이블의 하드웨어 인터페이스 카운터가 다음과 같이 증가하는지 확인합니다.
  - 활성/ 수동 구성, 활성 피어만 전송된 패킷을 표시합니다. 수동 피어는 수신된 패킷만 표시합니다.

    HA2 연결 유지를 활성화한 경우 수동 피어의 하드웨어 인터페이스 카운터는 전송 및 수신 패킷을 모두 표시합니다. 이는 *HA2* 연결 유지가 양방향이기 때문에 발생합니다. 즉, 두 피어 모두 *HA2* 연결 유지 패킷을 전송합니다.
  - 활성/활성 구성에서는 두 피어에서 수신된 패킷과 전송된 패킷을 볼 수 있습니다.

방화벽을 Panorama에서 PAN-OS 11.0으로 업그레이드

콘텐츠 업데이트를 배포하고 Panorama™ 관리 서버에서 관리 방화벽용 PAN-OS를 업그레이드합니다.

- Panorama가 인터넷에 연결되어 있을 때 방화벽 업그레이드
- Panorama가 인터넷에 연결되어 있지 않을 때 방화벽 업그레이드
- ZTP 방화벽 업그레이드

Panorama가 인터넷에 연결되어 있을 때 방화벽 업그레이드

PAN-OS 11.0 출시 정보를 검토한 후 다음 절차를 사용하여 Panorama로 관리하는 방화벽을 업그레이드합니다. 이 절차는 독립 실행형 방화벽 및 고가용성(HA) 구성에 배포된 방화벽에 적용됩니다.

여러 기능 PAN-OS 릴리스에서 HA 방화벽을 업그레이드하는 경우 계속하기 전에 각 HA 피어를 업그레이드 경로에서 동일한 기능 PAN-OS 릴리스로 업그레이드해야 합니다. 예를 들어, PAN-OS 10.0에서 PAN-OS 11.0으로 HA 피어를 업그레이드하는 중입니다. 대상 PAN-OS 11.0 릴리스로 계속 업그레이드하려면 먼저 두 HA 피어를 모두 PAN-OS 10.1로 업그레이드해야 합니다. HA 피어가 2개 이상의 기능 릴리스와 떨어져 있는 경우 이전 릴리스가 설치된 방화벽은 ## ### ## ### 메시지와 함께 ## ### 상태가 됩니다.

*Panorama*가 업데이트 서버에 직접 연결할 수 없는 경우 Panorama가 인터넷에 연결되어 있지 않을 때 방화벽 업그레이드 절차에 따라 *Panorama*에 이미지를 수동으로 다운로드한 다음 방화벽에 배포할 수 있습니다.

새로운 소프트웨어 버전 업그레이드 건너뛰기 기능을 사용하면 PAN-OS 11.0의 Panorama 어플라이언스에서 PAN-OS 10.1 이상 버전의 방화벽으로 업그레이드를 배포할 때 최대 3개의 릴리스를 건너뛸 수 있습니다.

Panorama에서 방화벽을 업그레이드하려면 먼저 다음을 수행해야 합니다.

- Panorama가 업그레이드하려는 PAN-OS 버전과 같거나 이후 버전을 실행하고 있는지 확인하십시오. 관리형 방화벽을 이 버전으로 업그레이드하기 전에 Panorama를 업그레이드하고 해당 Log Collector를 11.0으로 업그레이드해야 합니다. 또한, Log Collector를 11.0으로 업그레이드할 때 로깅 인프라의 변경으로 인해 모든 Log Collector를 동시에 업그레이드해야 합니다.
- 방화벽이 안정적인 전원에 연결되어 있는지 확인하십시오. 업그레이드 중 전원이 손실되면 방화벽을 사용할 수 없게 될 수 있습니다.
- PAN-OS 11.0으로 업그레이드할 때 Panorama 가상 어플라이언스가 레거시 모드인 경우 레거시 모드를 유지할지 여부를 결정합니다. PAN-OS 9.1 이상의 버전을 실행하는 새 Panorama 가상 어플라이언스 배포에는 레거시 모드가 지원되지 않습니다. Panorama 가상 어플라이언스를 PAN-OS 9.0 또는 이전 릴리스에서 PAN-OS 11.0으로 업그레이드하는 경우, Palo Alto Networks는 Panorama 가상 어플라이언스

설정 전제 조건을 검토하고 필요에 따라 Panorama 모드 또는 관리 전용 모드로 변경할 것을 권장합니다.

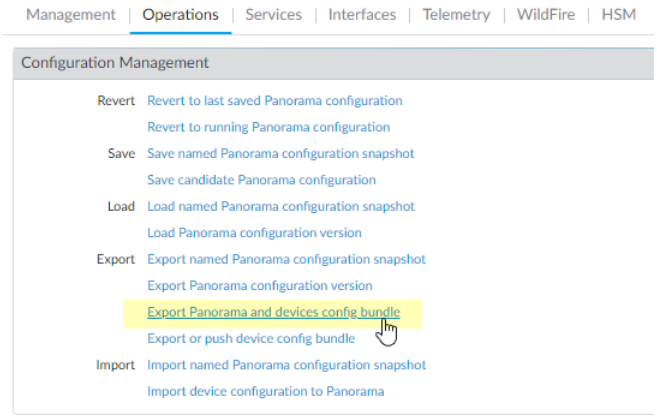
Panorama 가상 어플라이언스를 레거시 모드로 유지하려면 Panorama 가상 어플라이언스에 할당된 CPU 및 메모리를 최소 16개 CPU 및 32GB 메모리로 설정하여 성공적으로 PAN-OS 11.0으로 업그레이드합니다. 자세한 내용은 Panorama Virtual Appliance 설정 전제 조건을 참조하십시오.

STEP 1 | Panorama 웹 인터페이스에 로그인합니다.

STEP 2 | 업그레이드하려는 각 관리 방화벽에 현재 구성 파일의 백업을 저장합니다.

방화벽이 구성 백업을 자동으로 생성하지만 업그레이드하기 전에 백업을 생성하고 외부에 저장하는 것이 가장 좋습니다.

1. **Panorama** > 설정 > 작업을 선택하고 **Panorama** 및 디바이스 구성 번들 내보내기를 클릭하여 Panorama 및 각 관리 디바이스의 최신 구성 백업을 생성하고 내보냅니다.

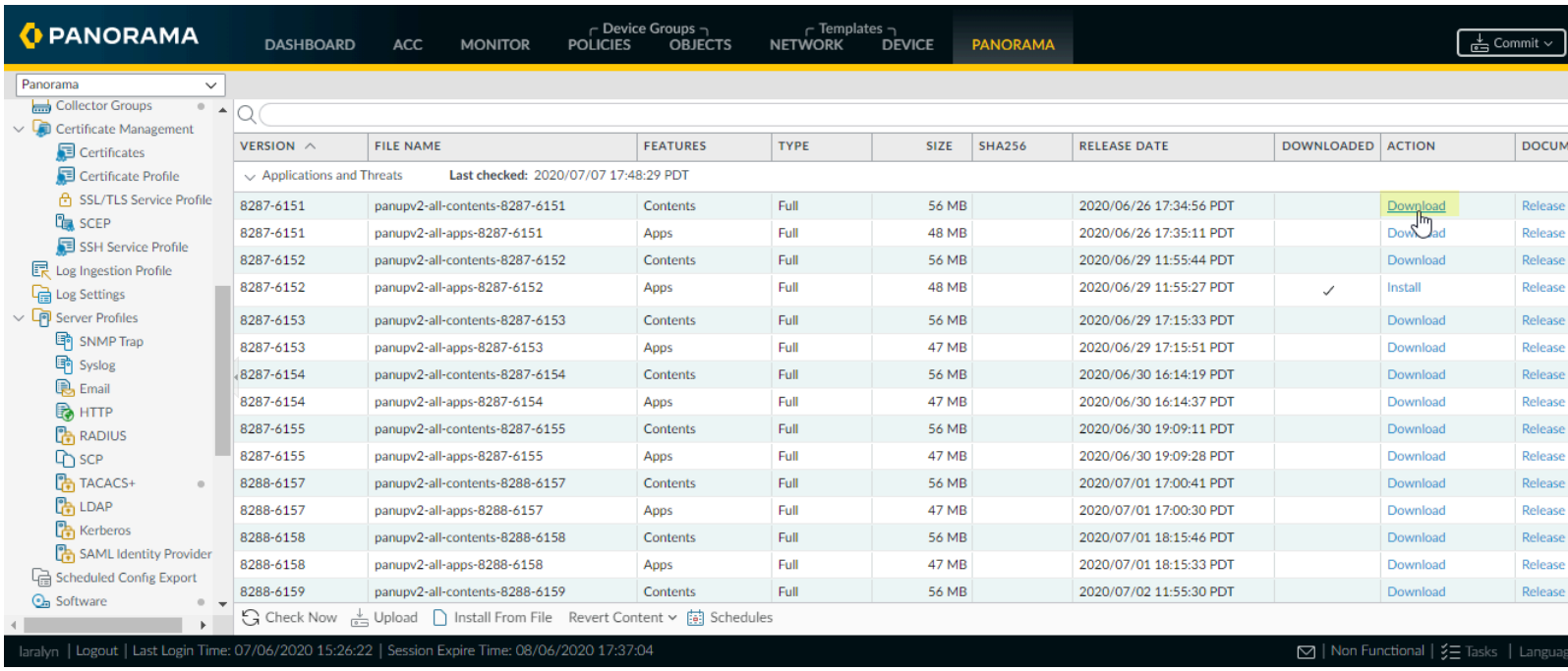


2. 내보낸 파일을 방화벽 외부 위치에 저장합니다. 업그레이드에 문제가 있는 경우 이 백업을 사용하여 구성을 복원할 수 있습니다.

STEP 3 | 최신 콘텐츠 업데이트를 설치합니다.

PAN-OS 11.0에 필요한 최소 콘텐츠 릴리스 버전은 릴리스 노트를 참조하십시오. Panorama 및 관리 방화벽에 콘텐츠 업데이트를 배포할 때 애플리케이션 및 위협 콘텐츠 업데이트에 대한 모범 사례을(를) 따릅니다.

1. 최신 업데이트를 보려면 **Panorama** > 디바이스 배포 > 동적 업데이트 및 지금 확인을 선택합니다. 업데이트가 있으면 작업 열에 다운로드 링크가 표시됩니다.



2. 설치를 클릭하고 업데이트를 설치할 방화벽을 선택합니다. HA 방화벽을 업그레이드하는 경우 두 피어 모두에서 콘텐츠를 업데이트해야 합니다.
3. 확인을 클릭합니다.

STEP 4 | PAN-OS 11.0으로의 업그레이드 경로 결정.

업그레이드 경로의 일부로 통과하는 각 릴리스에 대해 PAN-OS 업그레이드 체크리스트, 릴리스 노트 및 업그레이드/다운그레이드 고려 사항에서 알려진 문제 및 기본 동작의 변경 사항을 검토합니다.

둘 이상의 방화벽을 업그레이드하는 경우 이미지 다운로드를 시작하기 전에 모든 방화벽에 대한 업그레이드 경로를 결정하여 프로세스를 간소화하십시오.

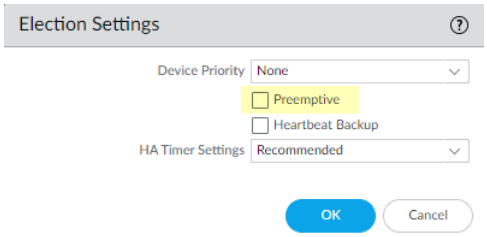
STEP 5 | (모범 사례) Cortex Data Lake(CDL)를 활용하는 경우 디바이스 인증서를 설치합니다.

방화벽은 PAN-OS 11.0으로 업그레이드할 때 CDL 수집 및 쿼리 엔드포인트 인증을 위해 디바이스 인증서를 사용하도록 자동으로 전환됩니다.

*PAN-OS 11.0*으로 업그레이드하기 전에 디바이스 인증서를 설치하지 않으면 방화벽은 인증을 위해 기존 로깅 서비스 인증서를 계속 사용합니다.

STEP 6 | (HA 방화벽 업그레이드만 해당) HA 쌍의 일부인 방화벽을 업그레이드할 경우 선점을 사용 중지합니다. 각 HA 쌍에 있는 하나의 방화벽에서만 이 설정을 비활성화하면 됩니다.

1. 디바이스 > 고가용성을 선택하고 일렉션**(election)** 설정을 편집합니다.
2. 활성화된 경우 선점 설정을 비활성화(지우기)하고 확인을 클릭합니다.



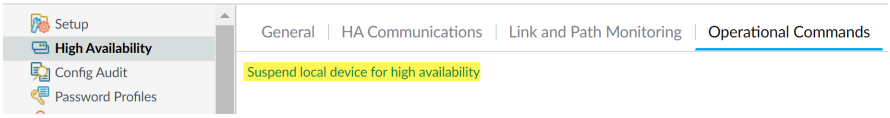
3. 변경사항을 커밋합니다. 업그레이드를 진행하기 전에 커밋이 성공했는지 확인합니다.

STEP 7 | (HA 방화벽 업그레이드만 해당) 기본 HA 피어를 일시 중단하여 강제 페일오버를 수행합니다.

(활성/수동 방화벽) 활성/수동 HA 구성의 방화벽의 경우 먼저 활성 HA 피어를 일시 중단하고 업그레이드합니다.

(활성/활성 방화벽) 활성/활성 HA 구성의 방화벽의 경우 활성-기본 HA 피어를 먼저 일시 중단하고 업그레이드합니다.

1. 활성 기본 방화벽 HA 피어의 방화벽 웹 인터페이스에 로그인합니다.
2. 디바이스 > 고가용성 > 작업 명령 및 고가용성을 위해 로컬 디바이스 일시중단을 선택합니다.



3. 오른쪽 하단에서 해당 상태가 ## ##인지 확인합니다.

   결과적인 장애 조치로 인해 보조 수동 HA 피어가 ## 상태로 전환되어야 합니다.

   결과적인 장애 조치는 업그레이드하기 전에 *HA* 장애 조치가 제대로 작동하는지 확인합니다.

STEP 8 | (선택 사항) 관리형 방화벽을 PAN-OS 10.1로 업그레이드합니다.

소프트웨어 버전 업그레이드 건너뛰기 기능은 PAN-OS 10.1 이상 릴리스를 실행하는 관리형 방화벽을 지원합니다. 관리형 방화벽의 릴리스가 PAN-OS 10.0 또는 이전인 경우 먼저 PAN-OS 10.1 이상 릴리스로 업그레이드합니다.

STEP 9 | (선택 사항) 구성된 SCP 서버로 파일을 내보냅니다.

PAN-OS 11.0에서는 관리형 방화벽에 업그레이드를 배포할 때 SCP 서버를 다운로드 소스로 사용할 수 있습니다. 다음 단계에서 소프트웨어 및 콘텐츠 이미지를 다운로드하기 전에 파일을 내보냅니다.

STEP 10 | 대상 릴리스에 필요한 소프트웨어 및 콘텐츠 버전을 확인하고 다운로드합니다.

이 단계에서는 PAN-OS 11.0으로 업그레이드하는 데 필요한 중간 소프트웨어 및 콘텐츠 이미지를 보고 다운로드할 수 있습니다.

다중 이미지 다운로드를 사용하여 소프트웨어 및 콘텐츠 이미지를 다운로드하는 것은 선택 사항입니다. 이미지는 한 번에 하나씩 다운로드할 수 있습니다.

1. **Panorama** > 디바이스 배포 > 소프트웨어 > 작업 > 검증을 클릭합니다.
2. 다운로드해야 하는 중간 소프트웨어 및 콘텐츠 버전을 확인합니다.
3. 업그레이드할 방화벽을 선택하고 배포를 클릭합니다.
4. 다운로드 소스를 선택하고 다운로드를 클릭합니다.

STEP 11 | 방화벽에 PAN-OS 11.0.0을 설치합니다.

(SD-WAN만 해당) SD-WAN 링크의 정확한 상태를 유지하려면 분기 방화벽을 업그레이드하기 전에 허브 방화벽을 *PAN-OS 11.0*으로 업그레이드해야 합니다. 허브 방화벽보다 먼저 브랜치 방화벽을 업그레이드하면 모니터링 데이터(***Panorama*** > ***SD-WAN*** > 모니터링)가 올바르지 않고 *down*으로 잘못 표시됩니다.

1. 업그레이드할 방화벽 모델에 해당하는 작업 열에서 설치를 클릭합니다. 예를 들어, PA-220 방화벽을 업그레이드하려면 PanOS_220-11.0.0에 해당하는 행에서 설치를 클릭합니다.
2. 소프트웨어 파일 배포 대화 상자에서 업그레이드할 모든 방화벽을 선택합니다.

   (HA 방화벽 업그레이드만 해당) 다운타임을 줄이려면 각 HA 쌍에서 하나의 피어만 선택합니다. 활성/수동 쌍의 경우 수동 피어를 선택합니다. 활성/활성 쌍의 경우 활성-보조 피어를 선택합니다.
3. (HA 방화벽 업그레이드만 해당) 그룹 **HA** 피어가 선택되지 않았는지 확인합니다.
4. 설치 후 디바이스 재부팅을 선택합니다.
5. 업그레이드를 시작하려면 확인을 클릭합니다.
6. 설치가 성공적으로 완료되면 다음 방법 중 하나를 사용하여 재부팅합니다.
   - 재부팅하라는 메시지가 표시되면 예를 클릭합니다.
   - 재부팅하라는 메시지가 표시되지 않으면 디바이스 > 설정 > 작업 및 디바이스 재부팅을 선택합니다.
7. 방화벽 재부팅이 완료되면 **Panorama** > 관리형 디바이스를 선택하고 업그레이드한 방화벽의 소프트웨어 버전이 11.0.0인지 확인합니다. 또한, 업그레이드한 수동 방화벽의 HA 상태가 여전히 수동인지 확인합니다.

STEP 12 | (HA 방화벽 업그레이드만 해당) HA 기능을 기본 HA 피어로 복원합니다.

1. 일시 중단된 기본 방화벽 HA 피어의 방화벽 웹 인터페이스에 로그인합니다.
2. 디바이스 > 고가용성 > 작업 명령 및 고가용성을 위해 로컬 디바이스 작동을 선택합니다.
3. 오른쪽 하단에서 상태가 ##인지 확인합니다. 활성/활성 구성의 방화벽의 경우 상태가 ##인지 확인합니다.
4. HA 피어 실행 구성이 동기화될 때까지 기다립니다.

   대시보드에서 고가용성 위젯에서 실행 중인 구성 상태를 모니터링합니다.

STEP 13 | (HA 방화벽 업그레이드만 해당) 보조 HA 피어를 일시 중단하여 기본 HA 피어로 강제 페일오버합니다.

1. 활성 보조 방화벽 HA 피어의 방화벽 웹 인터페이스에 로그인합니다.
2. 디바이스 > 고가용성 > 작업 명령 및 고가용성을 위해 로컬 디바이스 일시중단을 선택합니다.
3. 오른쪽 하단에서 해당 상태가 ## ##인지 확인합니다.

   그 결과 장애 조치로 인해 기본 수동 HA 피어가 ## 상태로 전환되어야 합니다.

   결과적인 장애 조치는 업그레이드하기 전에 *HA* 장애 조치가 제대로 작동하는지 확인합니다.

STEP 14 | (HA 방화벽 업그레이드만 해당) 각 HA 쌍에서 두 번째 HA 피어를 업그레이드합니다.

1. Panorama 웹 인터페이스에서 **Panorama** > 디바이스 배포 > 소프트웨어를 선택합니다.
2. 업그레이드 중인 HA 쌍의 방화벽 모델에 해당하는 작업 열에서 설치를 클릭합니다.
3. 소프트웨어 파일 배포 대화 상자에서 업그레이드할 모든 방화벽을 선택합니다. 이번에는 방금 업그레이드한 HA 방화벽의 피어만 선택합니다.
4. 그룹 **HA** 피어가 선택되지 않았는지 확인합니다.
5. 설치 후 디바이스 재부팅을 선택합니다.
6. 업그레이드를 시작하려면 확인을 클릭합니다.
7. 설치가 성공적으로 완료되면 다음 방법 중 하나를 사용하여 재부팅합니다.
   - 재부팅하라는 메시지가 표시되면 예를 클릭합니다.
   - 재부팅하라는 메시지가 표시되지 않으면 디바이스 > 설정 > 작업 및 디바이스 재부팅을 선택합니다.

STEP 15 | (HA 방화벽 업그레이드만 해당) HA 기능을 보조 HA 피어로 복원합니다.

1. 일시 중단된 보조 방화벽 HA 피어의 방화벽 웹 인터페이스에 로그인합니다.
2. 디바이스 > 고가용성 > 작업 명령 및 고가용성을 위해 로컬 디바이스 작동을 선택합니다.
3. 오른쪽 하단에서 상태가 ##인지 확인합니다. 활성/활성 구성의 방화벽의 경우 상태가 ##인지 확인합니다.
4. HA 피어 실행 구성이 동기화될 때까지 기다립니다.

   대시보드에서 고가용성 위젯에서 실행 중인 구성 상태를 모니터링합니다.

STEP 16 | (FIPS-CC 모드만 해당)FIPS-CC 모드에서 Panorama 및 관리형 디바이스 업그레이드.

FIPS-CC 모드에서 관리형 방화벽을 업그레이드하려면 관리형 방화벽이 PAN-OS 11.0 릴리스를 실행하는 동안 Panorama 관리에 전용 Log Collector를 추가한 경우 보안 연결 상태를 재설정해야 합니다.

관리형 방화벽이 PAN-OS 10.0 또는 이전 릴리스로 실행되는 경우에는 Panorama 관리에 추가된 관리형 방화벽을 다시 온보딩할 필요가 없습니다.

STEP 17 | 각 관리 방화벽에서 실행되는 소프트웨어 및 콘텐츠 릴리스 버전을 확인합니다.

1. Panorama에서 **Panorama** > 관리형 디바이스를 선택합니다.
2. 방화벽을 찾고 표에서 콘텐츠 및 소프트웨어 버전을 검토합니다.

   HA 방화벽의 경우 각 피어의 HA 상태가 예상대로인지 확인할 수도 있습니다.

	DEVICE NAME	MODEL	IP Address IPV4	TEMPLATE	Status DEVICE STATE	Status HA STATUS	Status CERTIFICATE	Status L... M... D...	SOFTWARE VERSION	APPS AND THREAT	ANTIVIRUS
	DG-VM (5/5 Devices Connected): Shared > DG-VM										
	PA-VM-6	PA-VM		Stack-VM	Connected		pre-defined		8.1.0	8320-6307	3881-4345
	PA-VM-73	PA-VM		Stack-Test73	Connected		pre-defined		9.1.3	8320-6307	3873-4337
	PA-VM-95	PA-VM		Stack-VM	Connected		pre-defined		10.0.0	8320-6307	3881-4345
	PA-VM-96	PA-VM		Stack-VM	Connected	Passive	pre-defined		10.0.0	8299-6216	3881-4345
	PA-VM			Stack-Test92	Connected	Active	pre-defined		10.0.0	8299-6216	3881-4345

STEP 18 | (HA 방화벽 업그레이드만 해당) 업그레이드하기 전에 HA 방화벽 중 하나에서 선점을 비활성화한 경우 일렉션**(election)** 설정(디바이스 > 고가용성) 해당 방화벽에 대해 선점 설정을 다시 활성화한 다음 변경 사항을 커밋합니다.

STEP 19 | Panorama 웹 인터페이스에서 전체 Panorama 관리 구성을 관리형 방화벽으로 푸시합니다.

이 단계는 Panorama에서 관리형 방화벽으로 디바이스 그룹 및 템플릿 스택 구성 변경 사항을 선택적으로 커밋하고 푸시할 수 있도록 하는 데 필요합니다.

이는 PAN-OS 10.1 또는 이전 릴리스에서 PAN-OS 11.0으로 성공적으로 업그레이드한 후 Panorama에서 관리하는 다중 vsys 방화벽에 구성 변경을 성공적으로 푸시하는 데 필요합니다. 자세한 내용은 Panorama에서 관리하는 multi-vsys 방화벽의 공유 구성 개체에 대한 기본 동작 변경을 참조하십시오.

1. 커밋 > 디바이스에 푸시를 선택합니다.
2. 푸시합니다.

STEP 20 | OpenSSL 보안 수준 2를 준수하도록 모든 인증서를 재생성하거나 다시 가져옵니다.

PAN-OS 10.2 이상 릴리스로 업그레이드할 때는 모든 인증서가 다음과 같은 최소 요구 사항을 충족해야 합니다. PAN-OS 10.2에서 업그레이드하고 인증서를 이미 재생성하거나 다시 가져온 경우 이 단계를 건너뛰십시오.

- RSA 2048비트 이상 또는 ECDSA 256비트 이상
- SHA256 이상의 다이제스트

PAN-OS 관리자 가이드를 참조하거나 인증서 재생성 또는 다시 가져오기에 대한 자세한 내용은 Panorama 관리자 가이드를 참조하십시오.

STEP 21 | 방화벽의 소프트웨어 업그레이드 기록을 볼 수 있습니다.

1. Panorama 인터페이스에 로그인합니다.
2. **Panorama** > 관리형 디바이스 > 요약으로 이동하여 디바이스 내역을 클릭합니다.

Panorama가 인터넷에 연결되어 있지 않을 때 방화벽 업그레이드

방화벽에 설치할 수 있는 소프트웨어 및 콘텐츠 업데이트 목록은 지원되는 업데이트를 참조하십시오.

새로운 소프트웨어 버전 업그레이드 건너뛰기 기능을 사용하면 PAN-OS 11.0의 Panorama 어플라이언스에서 PAN-OS 10.1 이상 버전의 방화벽으로 업그레이드를 배포할 때 최대 3개의 릴리스를 건너뛸 수 있습니다.

STEP 1 | 관리형 방화벽을 업그레이드하기 전에 Panorama 관리 서버와 Log Collector에서 Pan-OS 11.0이 실행되고 있는지 확인합니다.

*Palo Alto Networks®*는 *Panorama* 및 *Log Collectors*가 동일한 *Panorama* 소프트웨어 릴리스를 실행하고 *Panorama, Log Collectors* 및 모든 관리 방화벽이 동일한 콘텐츠 릴리스 버전을 실행할 것을 적극 권장합니다.

중요한 소프트웨어 및 콘텐츠 호환성 세부정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조합니다.

Panorama는 방화벽과 동일한(또는 이후 버전) 소프트웨어 릴리스를 실행해야 하지만 이와 동일하거나 이전 콘텐츠 릴리스 버전이 있어야 합니다.

- 소프트웨어 릴리스 버전 - Panorama 관리 서버 또는 로그 수집기가 방화벽을 업데이트하려는 릴리스와 같거나 이후의 소프트웨어 릴리스를 이미 실행하고 있지 않은 경우 동일한 또는 이후 버전의 Panorama를 설치해야 합니다. 방화벽을 업데이트하기 전에 Panorama 및 Log Collectors(Panorama용 콘텐츠 및 소프트웨어 업데이트 설치 참조)에서 릴리스하십시오.
- 콘텐츠 출시 버전 - 콘텐츠 릴리스 버전의 경우 모든 방화벽이 최신 콘텐츠 릴리스 버전을 실행 중이거나 최소한 Panorama 및 Log Collectors에서 실행되는 것보다 최신 버전을 실행하고 있는지 확인해야 합니다. 그렇지 않은 경우 Panorama 관리 서버에서 콘텐츠 릴리스 버전을 업데이트하기 전에 관리 방화벽을 업데이트한 다음 Panorama가 인터넷에 연결되어 있지 않을 때 로그 수집기를 업그레이드합니다(Panorama용 콘텐츠 및 소프트웨어 업데이트 설치 참조).

소프트웨어 및 콘텐츠 버전을 확인하려면:

- **Panorama** 관리 서버 - Panorama 웹 인터페이스에 로그인하고 일반 정보 설정(대시보드)으로 이동합니다.
- 로그 수집기 - 각 로그 수집기의 CLI에 로그인하고 **`show system info`** 명령을 실행합니다.

STEP 2 | 업그레이드하려는 각 관리 방화벽에 현재 구성 파일의 백업을 저장합니다.

방화벽이 구성 백업을 자동으로 생성하지만 업그레이드하기 전에 백업을 생성하고 외부에 저장하는 것이 가장 좋습니다.

1. **Panorama** 및 디바이스 구성 번들 내보내기(**Panorama** > 설정 > 작동)를 사용하여 Panorama 및 각 관리형 어플라이언스의 최신 구성 백업을 생성하고 내보낼 수 있습니다.
2. 내보낸 파일을 방화벽 외부 위치에 저장합니다. 업그레이드에 문제가 있는 경우 이 백업을 사용하여 구성을 복원할 수 있습니다.

STEP 3 | 어떤 콘텐츠 업데이트를 설치해야 하는지 결정합니다. PAN-OS® 릴리스에 설치해야 하는 최소 콘텐츠 릴리스 버전은 릴리스 노트를 참조하십시오.

*Palo Alto Networks*는 *Panorama, Log Collectors* 및 모든 관리 방화벽이 동일한 콘텐츠 릴리스 버전을 실행할 것을 적극 권장합니다.

각 콘텐츠 업데이트에 대해 업데이트가 필요한지 여부를 결정하고 다음 단계에서 다운로드해야 하는 콘텐츠 업데이트를 기록해 둡니다.

*Panorama*가 관리 방화벽 및 로그 수집기에서 실행되는 것과 동일하지만 이후 콘텐츠 릴리스 버전이 아니라 실행 중인지 확인합니다.

STEP 4 | Panorama 11.0으로 업데이트할 방화벽의 소프트웨어 업그레이드 경로를 결정합니다.

Panorama에 로그인하고 **Panorama** > 관리 디바이스를 선택한 다음 업그레이드하려는 방화벽의 현재 소프트웨어 버전을 확인합니다.

업그레이드 경로의 일부로 통과하는 각 릴리스에 대한 릴리스 노트 및 다운그레이드 고려 사항의 알려진 문제 및 기본 동작에 대한 변경 사항은 PAN-OS 업그레이드 점검표에서 확인할 수 있습니다.

STEP 5 | (선택 사항) 관리형 방화벽을 PAN-OS 10.1로 업그레이드합니다.

소프트웨어 버전 업그레이드 건너뛰기 기능은 PAN-OS 10.1 이상 릴리스를 실행하는 관리형 방화벽을 지원합니다. 관리형 방화벽의 릴리스가 PAN-OS 10.0 또는 이전인 경우 먼저 PAN-OS 10.1 이상 릴리스로 업그레이드합니다.

STEP 6 | 릴리스의 유효성 검사를 수행합니다.

이 단계에서는 11.0으로 업그레이드하는 데 필요한 중간 소프트웨어 및 콘텐츠 이미지를 설명합니다.

1. **Panorama** > 디바이스 배포 > 소프트웨어 > 작업 > 유효성 검사를 선택합니다.
2. 다운로드해야 하는 중간 소프트웨어 및 콘텐츠 버전을 확인합니다.

STEP 7 | SCP 또는 HTTPS를 통해 Panorama 또는 구성된 SCP 서버에 연결하고 파일을 업로드할 수 있는 호스트에 콘텐츠 및 소프트웨어 업데이트를 다운로드합니다.

기본적으로 각 유형의 소프트웨어 또는 콘텐츠 업데이트를 최대 2개까지 Panorama 어플라이언스에 업로드할 수 있으며 동일한 유형의 세 번째 업데이트를 다운로드하는 경우 Panorama는 해당 유형의 가장 오래된 버전에 대한 업데이트를 삭제합니다. 단일 유형의 소프트웨어 업데이트 또는 콘텐츠 업데이트를 2개 이상 업로드해야 하는 경우, **`set max-num-images count <number>`** CLI 명령을 사용하여 Panorama가 저장할 수 있는 최대 이미지 수를 늘립니다.

1. 인터넷에 액세스할 수 있는 호스트를 사용하여 Palo Alto Networks 고객 지원 웹사이트에 로그인합니다.

2. 콘텐츠 업데이트 다운로드:
   1. 리소스 섹션에서 동적 업데이트를 클릭합니다.
   2. 최신 콘텐츠 릴리스 버전(또는 최소한 Panorama 관리 서버에서 설치하거나 실행 중인 버전과 같거나 이후 버전)을 다운로드하고 파일을 호스트에 저장합니다. 업데이트해야 하는 각 콘텐츠 유형에 대해 반복합니다.
3. 소프트웨어 업데이트 다운로드:
   1. Palo Alto Networks 고객 지원 웹사이트의 기본 페이지로 돌아가서 리소스 섹션에서 소프트웨어 업데이트를 클릭하십시오.
   2. 다운로드 열을 검토하여 설치해야 하는 버전을 결정하십시오. 업데이트 패키지의 파일 이름은 모델을 나타냅니다. 예를 들어, PA-220 및 PA-5260 방화벽을 PAN-OS 11.0.0으로 업그레이드하려면 `PanOS_220-11.0.0`, `PanOS_3000-11.0.0` 및 `PanOS_5200-11.0.0` 이미지를 다운로드합니다.

      필터링 기준 드롭다운에서 ***PA-***<*series/model*>용 *PAN-OS*를 선택하여 특정 *PAN-OS* 이미지를 빠르게 찾을 수 있습니다.
4. 적절한 파일 이름을 클릭하고 파일을 호스트에 저장합니다.

STEP 8 | 중간 소프트웨어 버전과 최신 콘텐츠 버전을 다운로드합니다.

PAN-OS 11.0에서는 다중 이미지 다운로드 기능을 사용하여 여러 중간 릴리스를 다운로드할 수 있습니다.

1. 업그레이드할 방화벽을 선택합니다(필수 배포 > 배포).
2. 다운로드 소스를 선택하고 다운로드를 클릭합니다.

STEP 9 | 관리 방화벽에 콘텐츠 업데이트를 설치합니다.

소프트웨어 업데이트 전에 콘텐츠 업데이트를 설치해야 합니다.

애플리케이션 또는 애플리케이션 및 위협 업데이트를 먼저 설치한 다음 필요에 따라 다른 업데이트(바이러스 백신, WildFire® 또는 URL 필터링)를 한 번에 하나씩 순서에 관계없이 설치합니다.

1. **Panorama** > 디바이스 배포 > 동적 업데이트를 선택합니다.
2. 업로드를 클릭하고 업데이트 유형을 선택한 후 적절한 콘텐츠 업데이트 파일을 찾아보기하고 확인을 클릭합니다.
3. 파일에서 설치를 클릭하고 업데이트 유형을 선택한 다음 방금 업로드한 콘텐츠 업데이트의 파일 이름을 선택합니다.
4. 업데이트를 설치할 방화벽을 선택합니다.
5. 확인을 클릭하여 설치를 시작합니다.
6. 각 콘텐츠 업데이트에 대해 이 단계를 반복합니다.

STEP 10 | (GlobalProtect™ 포털 역할을 하는 방화벽만) 방화벽에서 GlobalProtect 에이전트/앱 소프트웨어 업데이트를 업로드하고 활성화합니다

사용자가 엔드포인트(클라이언트 시스템)에 업데이트를 다운로드할 수 있도록 방화벽에서 업데이트를 활성화합니다.

1. 인터넷에 액세스할 수 있는 호스트를 사용하여 Palo Alto Networks 고객 지원 웹사이트에 로그인합니다.
2. 적절한 GlobalProtect 에이전트/앱 소프트웨어 업데이트를 다운로드합니다.
3. Panorama에서 **Panorama** > 디바이스 배포 > **GlobalProtect** 클라이언트를 선택합니다.
4. 파일을 다운로드한 호스트에서 적절한 GlobalProtect 에이전트/앱 소프트웨어 업데이트로 업로드, 찾아보기를 클릭하고 확인을 클릭합니다.
5. 파일에서 활성화를 클릭하고 방금 업로드한 GlobalProtect 에이전트/앱 업데이트의 파일 이름을 선택합니다.

   한 번에 하나의 에이전트/앱 소프트웨어 버전만 활성화할 수 있습니다. 새 버전을 활성화했지만 일부 에이전트에 이전 버전이 필요한 경우 해당 에이전트가 이전 업데이트를 다운로드하려면 이전 버전을 다시 활성화해야 합니다.
6. 업데이트를 활성화할 방화벽을 선택합니다.
7. 확인을 클릭하여 활성화합니다.

STEP 11 | PAN-OS 11.0을 설치합니다.

고가용성*(HA)* 방화벽에서 소프트웨어를 업데이트할 때 다운타임을 방지하려면 한 번에 하나의 *HA* 피어를 업데이트하십시오.

능동형/능동형 방화벽의 경우 먼저 업데이트하는 피어가 중요하지 않습니다.

능동형/수동형 방화벽의 경우 먼저 수동 피어를 업데이트하고 활성 피어를 일시 중단*(*페일오버*)*하고 업데이트한 다음 기능 상태로 되돌려야 합니다*(*페일오버*).*

*(SD-WAN*만 해당*) SD-WAN* 링크의 정확한 상태를 유지하려면 분기 방화벽을 업그레이드하기 전에 허브 방화벽을 *PAN-OS 11.0*으로 업그레이드해야 합니다. 허브 방화벽보다 먼저 브랜치 방화벽을 업그레이드하면 모니터링 데이터*(**Panorama** > **SD-WAN** >* 모니터링*)*가 올바르지 않고 *down*으로 잘못 표시됩니다.

1. 방화벽 구성에 적용되는 단계를 수행하여 방금 업로드한 PAN-OS 소프트웨어 업데이트를 설치합니다.
   - 비 **HA** 방화벽 - 작업 열에서 설치를 클릭하고 업그레이드하려는 모든 방화벽을 선택한 다음 설치 후 디바이스 재부팅을 선택하고 확인을 클릭합니다. .
   - 능동형/능동형 **HA** 방화벽**:**
     1. 업그레이드할 첫 번째 피어에서 선점 설정이 비활성화되어 있는지 확인합니다(디바이스 > 고가용성 > 일렉션(Election) 설정). 활성화된 경우 일렉션**(election)** 설정을 편집하고 선점 설정을 비활성화(지우기)하고 변경 사항을 커밋합니다. 각 HA 쌍의 한 방화벽에서만 이 설정을 비활성화해야 하지만 계속하기 전에 커밋이 성공했는지 확인하십시오.
     2. 설치를 클릭하고 그룹 **HA** 피어를 비활성화(지우기)하고 HA 피어 중 하나를 선택하고 설치 후 디바이스 재부팅을 선택한 다음 확인을 클릭합니다. 계속하기 전에 방화벽이 재부팅을 마칠 때까지 기다리십시오.
     3. 설치를 클릭하고, 그룹 **HA** 피어를 비활성화(지우기)하고, 이전 단계에서 업데이트하지 않은 HA 피어를 선택하고, 설치 후 디바이스 재부팅, 확인을 클릭합니다.
   - 활성/수동 **HA** 방화벽 - 이 예에서 활성 방화벽의 이름은 fw1, 수동 방화벽의 이름은 fw2:
     1. 입니다. 업그레이드할 첫 번째 피어에서 선점 설정이 비활성화되어 있는지 확인합니다(디바이스 > 고가용성 > 일렉션 설정). 활성화된 경우 일렉션**(election)** 설정을 편집하고 선점 설정을 비활성화(지우기)하고 변경 사항을 커밋합니다. 각 HA 쌍의 한 방화벽에서만 이 설정을 비활성화해야 하지만 계속하기 전에 커밋이 성공했는지 확인합니다.
     2. 적절한 업데이트의 작업 열에서 설치를 클릭하고 그룹 **HA** 피어를 비활성화(지우기)한 후 fw2를 선택하고 설치 후 디바이스 재부팅, 확인을 클릭합니다. 계속하기 전에 fw2가 재부팅을 마칠 때까지 기다립니다.
     3. fw2가 재부팅을 완료한 후 fw1(대시보드 > 고가용성)에서 fw2가 여전히 수동 피어인지 확인합니다(로컬 방화벽 상태는 ##이고 피어(fw2)는 ##).

4. Fw1에 액세스하고 로컬 디바이스를 일시 중지합니다(디바이스 > 고가용성 > 작동 명령).
5. fw2(대시보드 > 고가용성)에 액세스하고 로컬 방화벽 상태가 ##이고 피어가 ## ###인지 확인합니다.
6. Panorama에 액세스하고 **Panorama** > 디바이스 배포 > 소프트웨어를 선택한 후 해당 릴리스에 대한 조치 열에서 설치를 클릭하고 그룹 **HA** 피어를 비활성화(지우기)한 후 fw1, 설치 후 디바이스 재부팅을 선택하고 확인을 클릭합니다. 계속하기 전에 fw1이 재부팅을 마칠 때까지 기다립니다.
7. fw1(디바이스 > 고가용성 > 작동 명령)에 액세스하고 로컬 디바이스 작동을 클릭한 후 계속 진행하기 전에 2분 정도 기다립니다.
8. fw1(대시보드> 고가용성)에서 로컬 방화벽 상태가 ##이고 피어(fw2)가 ##인지 확인합니다.

STEP 12 | (FIPS-CC 모드만 해당)FIPS-CC 모드에서 Panorama 및 관리형 디바이스 업그레이드.

FIPS-CC 모드에서 관리형 방화벽을 업그레이드하려면 관리형 방화벽이 PAN-OS 11.0 릴리스를 실행하는 동안 Panorama 관리에 전용 Log Collector를 추가한 경우 보안 연결 상태를 재설정해야 합니다.

관리형 방화벽이 PAN-OS 10.0 또는 이전 릴리스로 실행되는 경우에는 Panorama 관리에 추가된 관리형 방화벽을 다시 온보딩할 필요가 없습니다.

STEP 13 | 각 관리 방화벽에 설치된 소프트웨어 및 콘텐츠 버전을 확인합니다.

1. **Panorama** > 관리형 디바이스를 선택합니다.
2. 방화벽을 찾아 소프트웨어 버전, 앱 및 위협 요소, 바이러스 백신, URL 필터링 및 GlobalProtect 클라이언트 열의 값을 검토합니다.

STEP 14 | 업그레이드하기 전에 HA 방화벽 중 하나에서 선점을 비활성화한 경우, 그런 다음 일렉션 설정(디바이스 > 고가용성)을 편집하고 해당 방화벽에 대한 선점 설정을 다시 활성화합니다.

STEP 15 | Panorama 웹 인터페이스에서 전체 Panorama 관리 구성을 관리형 방화벽으로 푸시합니다.

이 단계는 Panorama에서 관리형 방화벽으로 디바이스 그룹 및 템플릿 스택 구성 변경 사항을 선택적으로 커밋하고 푸시할 수 있도록 하는 데 필요합니다.

이는 PAN-OS 11.0으로 성공적으로 업그레이드한 후 Panorama에서 관리하는 multi-vsys 방화벽에 구성 변경을 성공적으로 푸시하는 데 필요합니다. 자세한 내용은 Panorama에서 관리하는 multi-vsys 방화벽의 공유 구성 개체에 대한 기본 동작 변경을 참조하십시오.

1. 커밋 > 디바이스에 푸시를 선택합니다.
2. 푸시합니다.

STEP 16 | OpenSSL 보안 수준 2를 준수하도록 모든 인증서를 재생성하거나 다시 가져옵니다.

PAN-OS 11.0으로 업그레이드할 때는 모든 인증서가 다음과 같은 최소 요구 사항을 충족해야 합니다.

- RSA 2048비트 이상 또는 ECDSA 256비트 이상
- SHA256 이상의 다이제스트

PAN-OS 관리자 가이드를 참조하거나 인증서 재생성 또는 다시 가져오기에 대한 자세한 내용은 Panorama 관리자 가이드를 참조하십시오.

STEP 17 | 방화벽의 소프트웨어 업그레이드 기록을 볼 수 있습니다.

1. Panorama 인터페이스에 로그인합니다.
2. **Panorama** > 관리형 디바이스 > 요약으로 이동하여 디바이스 내역을 클릭합니다.

ZTP 방화벽 업그레이드

Panorama™ 관리 서버에 ZTP 방화벽을 성공적으로 추가한 후 ZTP 방화벽의 대상 PAN-OS 버전을 구성합니다. Panorama는 처음으로 Panorama에 성공적으로 연결한 후 ZTP 방화벽에 설치된 PAN-OS 버전이 구성된 대상 PAN-OS 버전보다 크거나 같은지 확인합니다. ZTP 방화벽에 설치된 PAN-OS 버전이 대상 PAN-OS 버전보다 낮으면 ZTP 방화벽은 대상 PAN-OS 버전이 설치될 때까지 업그레이드 사이클에 진입합니다.

STEP 1 | Panorama 웹 인터페이스에 관리자로 로그인합니다.

STEP 2 | Panorama에 ZTP 방화벽을 추가합니다.

STEP 3 | 최신 PAN-OS 릴리스를 보려면 **Panorama** > 디바이스 배포 > 업데이트 및 지금 확인을 선택합니다.

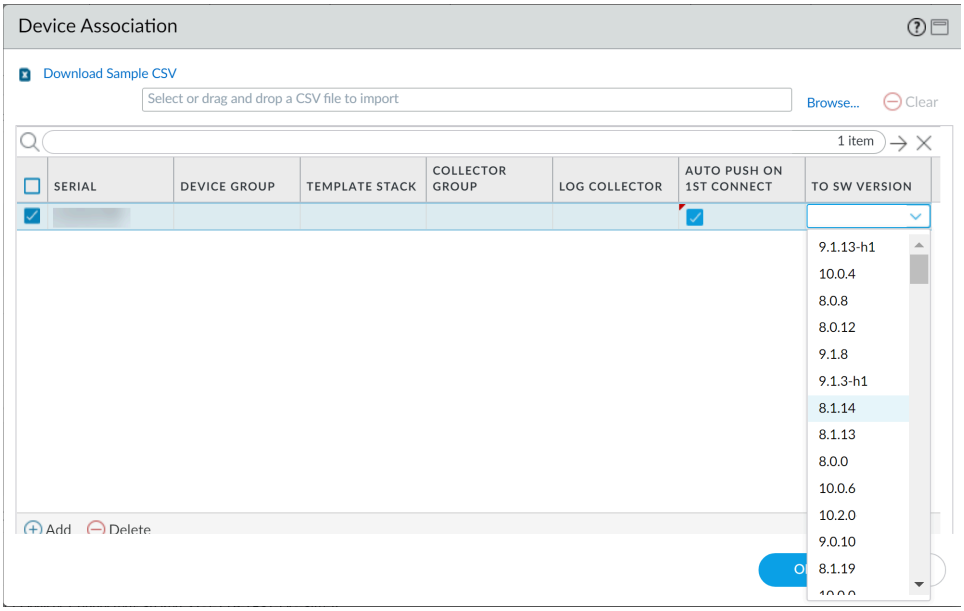
STEP 4 | **Panorama** > 관리 디바이스 > 요약을 선택하고 하나 이상의 ZTP 방화벽을 선택합니다.

STEP 5 | 선택한 ZTP 방화벽을 다시 연결합니다.

STEP 6 | 첫 번째 연결 시 자동 푸시를 선택(활성화)합니다.

STEP 7 | 대상 **SW** 버전 열에서 ZTP 방화벽의 대상 PAN-OS 버전을 선택합니다.

STEP 8 | 확인을 클릭하여 구성 변경 사항을 저장합니다.



STEP 9 | 커밋 및 **Panorama**에 커밋을 선택합니다.

STEP 10 | ZTP 방화벽의 전원을 켭니다.

ZTP 방화벽이 처음으로 Panorama에 연결되면 선택한 PAN-OS 버전으로 자동 업그레이드됩니다.

- **PAN-OS 11.0.0**을 실행하는 **Panorama** - PAN-OS 주요 또는 유지관리 릴리스에서 관리형 방화벽을 업그레이드하는 경우 대상 PAN-OS 릴리스가 설치되기 전에 업그레이드 경로의 중간 PAN-OS 릴리스가 먼저 설치됩니다.

  예를 들어, 관리형 방화벽에 대하여 원하는 대상 **SW** 버전을 PAN-OS 11.0.0으로 구성했고 방화벽에서 PAN-OS 10.1을 실행 중입니다. Panorama에 처음 연결할 때 PAN-OS 10.2.0이 관리형 방화벽에 먼저 설치됩니다. PAN-OS 10.2.0이 성공적으로 설치되면 방화벽이 대상 PAN-OS 11.0.0 릴리스로 자동 업그레이드됩니다.

- **PAN-OS 11.0.1** 이상 버전을 실행하는 **Panorama** - PAN-OS 주 또는 유지관리 릴리스에서 관리형 방화벽을 업그레이드하는 경우 업그레이드 경로에 중간 PAN-OS 주 릴리스가 설치되고 대상 PAN-OS 유지관리 릴리스가 설치되기 전에 기본 PAN-OS 주 릴리스가 다운로드됩니다.

  예를 들어, 관리형 방화벽에 대하여 원하는 대상 **SW** 버전을 PAN-OS 11.0.1로 구성했고 방화벽에서 PAN-OS 10.0을 실행 중입니다. Panorama에 처음 연결할 때 PAN-OS 10.1.0 및 PAN-OS 10.2.0이 관리형 방화벽에 설치됩니다. 관리형 방화벽이 재부팅되면 PAN-OS 11.0.0이 다운로드된 다음 방화벽이 대상 PAN-OS 11.0.1 릴리스에 자동으로 설치됩니다.

STEP 11 | ZTP 방화벽 소프트웨어 업그레이드를 확인합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 관리 디바이스 > 요약을 선택하고 ZTP 방화벽으로 이동합니다.
3. 소프트웨어 버전 열에 올바른 대상 PAN-OS 릴리스가 표시되는지 확인합니다.

STEP 12 | 향후의 모든 PAN-OS 업그레이드에 대해서는 방화벽을 Panorama에서 PAN-OS 11.0으로 업그레이드을(를) 참조하십시오.

PAN-OS 다운그레이드

PAN-OS 11.0에서 방화벽을 다운그레이드하는 방법은 이전 기능 릴리스(여기서 PAN-OS 버전의 첫 번째 또는 두 번째 숫자는 9.1.2에서 9.0.8로 또는 9.0.3에서 8.1.14로 변경됨)로 다운그레이드하는지 아니면 동일한 기능 릴리스(여기서 릴리스 버전의 세 번째 숫자가 8.1.2에서 8.1.0으로 변경됨) 내에서 유지관리 릴리스 버전으로 다운그레이드하는지에 따라 다릅니다. 한 기능 릴리스에서 이전 기능 릴리스로 다운그레이드할 때 새 기능을 수용하기 위해 최신 릴리스에서 구성을 마이그레이션할 수 있습니다. PAN-OS 11.0 구성을 이전 PAN-OS 릴리스로 마이그레이션하려면 먼저 다운그레이드할 기능 릴리스의 구성을 복원합니다. 동일한 기능 릴리스 내에서 한 유지 관리 릴리스에서 다른 릴리스로 다운그레이드할 때 구성을 복원할 필요가 없습니다.

- 방화벽을 이전 유지 관리 릴리스로 다운그레이드
- 방화벽을 이전 기능 릴리스로 다운그레이드
- Windows 에이전트 다운그레이드

항상 소프트웨어 버전과 일치하는 구성으로 다운그레이드하십시오. 일치하지 않는 소프트웨어 버전 및 구성은 다운그레이드에 실패하거나 시스템을 유지 관리 모드로 강제 전환할 수 있습니다. 이것은 한 기능 릴리스에서 다른 기능 릴리스로의 다운그레이드*(예: 9.0.0*에서 *8.1.3*으로*)*에만 적용되며 동일한 기능 릴리스 버전*(예: 8.1.3*에서 *8.1.1*으로*)* 내의 유지 관리 릴리스로의 다운그레이드에는 적용되지 않습니다.

다운그레이드에 문제가 있는 경우 유지 관리 모드로 들어가 디바이스를 공장 기본값으로 재설정한 다음 업그레이드 전에 내보낸 원래 구성 파일에서 구성을 복원해야 할 수 있습니다.

방화벽을 이전 유지 관리 릴리스로 다운그레이드

유지 관리 릴리스에는 새로운 기능이 도입되지 않으므로 이전 구성을 복원할 필요 없이 동일한 기능 릴리스에서 이전 유지 관리 릴리스로 다운그레이드할 수 있습니다. 유지 관리 릴리스는 릴리스 버전의 세 번째 숫자가 변경되는 릴리스입니다. 예를 들어 릴리스 버전의 세 번째 숫자만 다르기 때문에 8.1.6에서 8.1.4로의 다운그레이드는 유지 관리 릴리스 다운그레이드로 간주됩니다.

동일한 기능 릴리스 내에서 이전 유지 관리 릴리스로 다운그레이드하려면 다음 절차를 따르십시오.

STEP 1 | 현재 구성 파일의 백업을 저장합니다.

방화벽이 구성 백업을 자동으로 생성하지만 다운그레이드하고 외부에 저장하기 전에 백업을 생성하는 것이 가장 좋습니다.

1. 명명된 구성 스냅샷을 내보냅니다(디바이스 > 설정 > 작업).
2. 실행 중인 구성이 포함된 XML 파일(예: **running-config.xml**)을 선택하고 확인을 클릭하여 구성 파일을 내보냅니다.
3. 내보낸 파일을 방화벽 외부 위치에 저장합니다. 다운그레이드에 문제가 있는 경우 이 백업을 사용하여 구성을 복원할 수 있습니다.

STEP 2 | 이전 유지 관리 릴리스 이미지를 설치합니다.

방화벽이 관리 포트에서 인터넷에 액세스할 수 없는 경우 Palo Alto Networks 지원 포털에서 소프트웨어 업데이트를 다운로드할 수 있습니다. 그런 다음 방화벽에 수동으로 업로드할 수 있습니다.

1. 지금 확인(디바이스 > 소프트웨어)에서 사용 가능한 이미지를 확인합니다.
2. 다운그레이드할 버전을 찾습니다. 이미지가 아직 다운로드되지 않은 경우 다운로드합니다.
3. 다운로드가 완료되면 이미지를 설치합니다.
4. 설치가 성공적으로 완료되면 다음 방법 중 하나를 사용하여 재부팅합니다.
   - 재부팅하라는 메시지가 표시되면 예를 클릭합니다.
   - 재부팅하라는 메시지가 표시되지 않으면 디바이스 작업(디바이스 > 설정 > 작업) 및 디바이스 재부팅으로 이동합니다.

방화벽을 이전 기능 릴리스로 다운그레이드

다음 워크플로우를 사용하여 다른 기능 릴리스로 업그레이드하기 전에 실행 중이던 구성을 복원하십시오. 업그레이드 이후의 모든 변경 사항은 손실됩니다. 따라서 최신 기능 릴리스로 돌아갈 때 변경 사항을 복원할 수 있도록 현재 구성을 백업하는 것이 중요합니다. 방화벽을 이전 기능 릴리스로 다운그레이드하기 전에 다운그레이드 고려 사항을(를) 검토합니다.

*PAN-OS 11.0*에서 이전 *PAN-OS* 릴리스로 다운그레이드하려면 대상 *PAN-OS* 릴리스로 다운그레이드 경로를 계속 진행하기 전에 *PAN-OS 10.1.3* 또는 이후 *PAN-OS 11.0* 릴리스를 다운로드하여 설치해야 합니다. *PAN-OS 10.1.2* 또는 이전 *PAN-OS 11.0* 릴리스로 다운그레이드를 시도하면 *PAN-OS 11.0*에서 다운그레이드가 실패합니다.

이전 기능 릴리스로 다운그레이드하려면 다음 절차를 따르십시오.

STEP 1 | 현재 구성 파일의 백업을 저장합니다.

방화벽이 구성의 백업을 자동으로 생성하지만 업그레이드하기 전에 백업을 생성하고 외부에 저장하는 것이 가장 좋습니다.

1. 명명된 구성 스냅샷을 내보냅니다(디바이스 > 설정 > 작업).
2. 실행 중인 구성이 포함된 XML 파일(예: **running-config.xml**)을 선택하고 확인을 클릭하여 구성 파일을 내보냅니다.
3. 내보낸 파일을 방화벽 외부 위치에 저장합니다. 다운그레이드에 문제가 있는 경우 이 백업을 사용하여 구성을 복원할 수 있습니다.

STEP 2 | 이전 기능 릴리스 이미지를 설치합니다.

새 릴리스로 업그레이드하면 자동 저장 버전이 생성됩니다.

1. 지금 확인(디바이스 > 소프트웨어)에서 사용 가능한 이미지를 확인합니다.
2. PAN-OS 10.1을 설치합니다.

   PAN-OS 11.0에서 이전 기능 릴리스로 다운그레이드하려면 먼저 PAN-OS 10.1.3 또는 이후 PAN-OS 11.0 릴리스로 다운그레이드해야 합니다. PAN-OS 10.1.3 또는 이후 PAN-OS 11.0 릴리스로 성공적으로 다운그레이드한 후 대상 PAN-OS 버전으로 계속 다운그레이드할 수 있습니다.

   1. PAN-OS 11.0 이미지를 찾아 다운로드합니다.
   2. PAN-OS 11.0 이미지를 설치합니다.
3. 다운그레이드할 대상 PAN-OS 이미지를 찾습니다. 이미지가 아직 다운로드되지 않은 경우 다운로드합니다.
4. 다운로드가 완료되면 이미지를 설치합니다.
5. 다운그레이드를 위한 구성 파일 선택합니다. 디바이스를 재부팅하면 방화벽이 로드됩니다. 대부분의 경우 현재 다운그레이드 중인 릴리스에서 업그레이드할 때 자동으로 저장된 구성을 선택해야 합니다. 예를 들어, PAN-OS 11.0을 실행 중이고 PAN-OS 10.2.2로 다운그레이드하는 경우 `autosave-10.2.2`를 선택합니다.
6. 설치가 성공적으로 완료되면 다음 방법 중 하나를 사용하여 재부팅합니다.
   - 재부팅하라는 메시지가 표시되면 예를 클릭합니다.
   - 재부팅하라는 메시지가 표시되지 않으면 디바이스 작업(디바이스 > 설정 > 작업) 및 디바이스 재부팅으로 이동합니다.

Windows 에이전트 다운그레이드

PAN-OS 11.0 Windows 기반 User-ID 에이전트를 설치 제거한 후 이전 에이전트 릴리스를 설치하기 전에 다음 단계를 수행합니다.

STEP 1 | Windows 시작 메뉴를 열고 관리 도구를 선택합니다.

STEP 2 | 컴퓨터 관리 > 서비스 및 애플리케이션 > 서비스를 선택하고 사용자 **ID** 에이전트를 두 번 클릭합니다.

STEP 3 | 로그온을 선택하고 이 계정을 선택한 다음 User-ID 에이전트 계정의 사용자 이름을 지정합니다.

STEP 4 | 암호 및 암호 확인을 입력합니다.

STEP 5 | 확인을 클릭하여 변경 사항을 저장합니다.

PAN-OS 업그레이드 문제 해결

PAN-OS 업그레이드 문제를 해결하려면 다음 표를 사용하여 가능한 문제와 해결 방법을 검토하십시오.

증상	해결
소프트웨어 보증 라이선스가 만료되었습니다.	CLI에서 만료된 라이선스 키를 삭제합니다. 1. ## #### #입력 <software license key>. 2. **delete license key Software_Warranty<expiredate>.key**를 입력합니다.
최신 PAN-OS 소프트웨어 버전을 사용할 수 없습니다.	현재 설치된 버전보다 이전 릴리스인 소프트웨어 버전만 볼 수 있습니다. 예를 들어 8.1 릴리스가 설치된 경우 9.0 릴리스만 사용할 수 있습니다. 9.1 릴리스를 보려면 먼저 9.0으로 업그레이드해야 합니다.
동적 업데이트를 확인하지 못했습니다.	이 문제는 네트워크 연결 오류로 인해 발생합니다. 지금 확인 버튼을 클릭한 후 동적 업데이트 표시 오류에 대한 지식베이스 문서를 참조하십시오.
유효한 디바이스 인증서를 찾을 수 없습니다.	PAN-OS 9.1.3 이상 버전에서는 Palo Alto Networks 클라우드 서비스를 활용하는 경우 디바이스 인증서를 설치해야 합니다. 디바이스 인증서를 설치하려면: 1. 고객 지원 포털에 로그인합니다. 2. **OTP** 생성(자산 > 디바이스 인증서)을 선택합니다. 3. 디바이스 유형에서 차세대 방화벽용 **OTP** 생성을 선택합니다. 4. PAN-OS 디바이스 일련번호를 선택하십시오. 5. **OTP**를 생성하고 일회용 비밀번호를 복사합니다. 6. 방화벽에 관리자로 로그인합니다. 7. 디바이스 인증서(디바이스 > 설정 > 관리 > 디바이스 > 인증서)를 선택하고 인증서를 받습니다.

증상	해결
	8. OTP를 붙여넣고 확인을 클릭합니다.
이미지 인증 오류로 인해 소프트웨어 이미지 파일을 소프트웨어 관리자에 로드하지 못했습니다.	소프트웨어 이미지 목록을 업데이트하려면 지금 확인을 클릭합니다. 이렇게 하면 업데이트 서버에 대한 새 연결이 설정됩니다.
VMware NSX 플러그인 버전이 새 소프트웨어 버전과 호환되지 않습니다.	VMware NSX 플러그인은 8.0으로 업그레이드할 때 자동으로 설치되었습니다. 플러그인을 사용하지 않는 경우 제거할 수 있습니다.
PAN-OS 9.1로 업그레이드한 후 재부팅 시간이 예상보다 길었습니다.	애플리케이션 및 위협 콘텐츠 릴리스 버전 8221 이상으로 업그레이드하십시오. 최소 소프트웨어 및 콘텐츠 버전에 대한 자세한 내용은 <xref to 11.0 Associated Software and Content Versions>을(를) 참조하십시오.
라이선스가 활성화된 경우에도 디바이스가 지원되지 않았습니다.	디바이스 > 소프트웨어에서 지금 확인을 클릭합니다. 업데이트 서버에 대한 새 연결을 설정하여 방화벽의 라이선스 정보를 업데이트합니다. 웹 인터페이스에서 작동하지 않으면 ### ##### ## ##을 사용합니다.
방화벽에는 DHCP 서버에서 할당한 DHCP 주소가 없습니다.	ISP DHCP 서버에서 내부 네트워크로의 트래픽을 허용하는 보안 정책 규칙을 구성합니다.
방화벽이 유지관리 모드로 계속 부팅됩니다.	CLI에서 유지관리 복구 도구(MRT)에 액세스합니다. MRT 창에서 계속 > 디스크 이미지를 선택합니다. 재설치 **<current version>** 또는 **<previous version>**(으)로 되돌리기를 선택합니다. 되돌리기 또는 재설치 작업이 완료되면 재부팅을 선택합니다.
HA 구성에서 방화벽이 너무 오래되었다는 오류와 함께 피어 방화벽을 업그레이드하면 방화벽이 일시 중단된 상태로 전환됩니다.	하나의 방화벽을 두 개 이상의 주요 릴리스가 출시된 버전으로 업그레이드하면 네트워크가 중단됩니다. 다음 메이저 릴리스로 업그레이드하기 전에 한 번의 메이저 릴리스만 먼저 두 방화벽을 업그레이드해야 합니다. 피어 방화벽을 일시 중단된 방화벽이 중지된 버전으로 다운그레이드합니다.

VM 시리즈 방화벽 업그레이드

VM 시리즈 PAN-OS 소프트웨어 업그레이드(독립 실행형)

새로운 기능, 해결된 문제 및 알려진 문제를 검토한 후 다음 절차에 따라 HA 구성에 없는 방화벽을 업그레이드합니다.

트래픽에 영향을 주지 않으려면 중단 기간 내에 업그레이드를 계획하십시오. 방화벽이 안정적인 전원에 연결되어 있는지 확인하십시오. 업그레이드 중 전원이 손실되면 방화벽을 사용할 수 없게 될 수 있습니다.

STEP 1 | VM 시리즈 방화벽에 충분한 하드웨어 리소스를 사용할 수 있는지 확인하십시오.

각 VM 시리즈 모델의 리소스 요구 사항을 보려면VM 시리즈 시스템 요구 사항을참조하세요. 업그레이드 프로세스를 계속하기 전에 추가 하드웨어 리소스를 할당하십시오. 추가 하드웨어 리소스를 할당하는 프로세스는 하이퍼바이저마다 다릅니다.

VM-시리즈 방화벽에 해당 모델에 필요한 리소스가 없는 경우 VM-50과 관련된 용량이 기본값으로 설정됩니다.

STEP 2 | 웹 인터페이스에서장치 > 라이센스로 이동하여 올바른 VM-시리즈 방화벽 라이센스가 있고 라이센스가 활성화되었는지 확인하십시오.

VM-시리즈 방화벽 독립 실행형 버전에서는장치 > 지원으로 이동하여 지원 라이센스를 활성화했는지 확인하십시오.

STEP 3 | 현재 구성 파일의 백업을 저장합니다.

방화벽이 구성 백업을 자동으로 생성하지만 업그레이드하기 전에 백업을 생성하고 외부에 저장하는 것이 가장 좋습니다.

1. 디바이스 > 설정 > 작업을 선택하고 이름이 지정된 구성 스냅샷 내보내기를 클릭합니다.
2. 실행 중인 구성이 포함된 XML 파일(예: **running-config.xml**)을 선택하고 확인을 클릭하여 구성 파일을 내보냅니다.
3. 내보낸 파일을 방화벽 외부 위치에 저장합니다. 업그레이드에 문제가 있는 경우 이 백업을 사용하여 구성을 복원할 수 있습니다.

STEP 4 | (선택 사항) User-ID를 활성화한 경우 업그레이드 후 방화벽은 현재 IP 주소-사용자명 및 그룹 매핑을 지워 User-ID 소스의 속성으로 다시 채울 수 있습니다. 환경에서 매핑을 다시 채우는 데 필요한 시간을 예측하려면 방화벽에서 다음 CLI 명령을 실행합니다.

- IP 주소-사용자명 매핑의 경우:
  - **### User-ID #### ## ## ##**
  - **### ## ### ## ## ##**
- 그룹 매핑의 경우: **### ## ## ## ##**

STEP 5 | 방화벽이 최신 콘텐츠 릴리스 버전을 실행 중인지 확인하십시오.

1. 디바이스 > 동적 업데이트를 선택하고 현재 설치된 애플리케이션 또는 애플리케이션 및 위협 콘텐츠 릴리스 버전을 확인합니다.
2. 방화벽이 최소 필수 콘텐츠 릴리스 버전 또는 PAN-OS 11.0에 필요한 이후 버전을 실행하지 않는 경우 지금 확인하여 사용 가능한 업데이트 목록을 검색합니다.
3. 원하는 콘텐츠 릴리스 버전을 찾아 다운로드합니다.

   콘텐츠 업데이트 파일을 성공적으로 다운로드하면 작업 열의 링크가 해당 콘텐츠 릴리스 버전에 대해 다운로드에서 설치로 변경됩니다.
4. 업데이트를 설치합니다.

STEP 6 | VM 시리즈 플러그인을 업그레이드하세요.

1. 업그레이드하기 전에 새로운 VM 시리즈 플러그인이 환경에 영향을 미치는지 여부에 대한 자세한 내용을 최신 릴리스 노트에서 확인하세요.

   예를 들어, 새로운 VM-Series 플러그인 버전에 AWS 기능만 포함되어 있다고 가정해 보겠습니다. 새로운 기능을 활용하려면 AWS의 VM 시리즈 방화벽 인스턴스에서 플러그인을 업데이트해야 합니다.

   사용자 환경에 적용되지 않는 업그레이드를 설치하지 마십시오.
2. VM 시리즈 방화벽에 로그인하고 대시보드를 확인하여 플러그인 버전을 확인하세요.
3. 플러그인 버전을 보려면장치 > 플러그인을선택하세요. 지금 확인을사용하여 업데이트를 확인하세요.
4. 플러그인 버전을 선택한 다음 작업 열에서 설치를 클릭하여 플러그인을 설치합니다.

STEP 7 | PAN-OS 업그레이드

방화벽이 관리 포트에서 인터넷에 액세스할 수 없는 경우 Palo Alto Networks 고객 지원 포털에서 소프트웨어 이미지를 다운로드한 다음 방화벽에 수동으로 업로드할 수 있습니다.

1. 디바이스 > 소프트웨어를 선택하고 지금 확인을 클릭하여 최신 PAN-OS 업데이트를 표시합니다.
2. 대상 PAN-OS 버전을 찾아다운로드합니다.
3. 이미지를 다운로드한 후(또는 수동 업그레이드의 경우 이미지를 업로드한 후) 이미지를 설치합니다.
4. 설치가 성공적으로 완료되면 다음 방법 중 하나를 사용하여 재부팅합니다.
   - 재부팅하라는 메시지가 표시되면 예를 클릭합니다.
   - 재부팅하라는 메시지가 표시되지 않으면 디바이스 > 설정 > 작업을 선택하고 디바이스 재부팅을 클릭합니다.

   이 시점에서 방화벽은 *User-ID* 매핑을 지운 다음 *User-ID* 소스에 연결하여 매핑을 다시 채웁니다.
5. User-ID를 활성화한 경우 다음 CLI 명령을 사용하여 트래픽을 허용하기 전에 방화벽이 IP 주소-사용자명 및 그룹 매핑을 다시 채웠는지 확인합니다.
   - **### ip-user-mapping ## ##**
   - **### ## ## ##**
6. 처음으로 XFR 릴리스로 업그레이드하는 경우 이 단계를 반복하여 해당 XFR 릴리스로 업그레이드하십시오.

STEP 8 | 방화벽이 트래픽을 전달하는지 확인합니다.

모니터 > 세션 브라우저를 선택하고 새 세션이 표시되는지 확인합니다.

VM 시리즈 PAN-OS 소프트웨어 업그레이드(HA 쌍)

다음 절차를 사용하여 고가용성(HA) 구성에서 한 쌍의 방화벽을 업그레이드합니다. 이 절차는 능동형/수동형 및 능동형/능동형 구성 모두에 적용됩니다.

고가용성(HA) 구성에 있는 방화벽을 업그레이드할 때 가동 중지 시간을 방지하려면 한 번에 하나의 HA 피어를 업데이트하십시오. 능동형/능동형 방화벽의 경우 어떤 피어를 먼저 업그레이드하는지는 중요하지 않습니다(이 절차에서는 간단하게 능동형-보조 피어를 먼저 업그레이드하는 방법을 보여줍니다). 능동형/수동형 방화벽의 경우 먼저 수동형 피어를 업그레이드하고 능동형 피어를 일시 중단(페일오버)하고 활성 피어를 업데이트한 다음 해당 피어를 기능 상태로 되돌려야 합니다(페일백). HA 피어 업그레이드 중 페일오버를 방지하려면 업그레이드를 진행하기 전에 선점이 비활성화되었는지 확인해야 합니다. 쌍의 한 피어에서만 선점을 비활성화하면 됩니다.

트래픽에 영향을 주지 않으려면 중단 기간 내에 업그레이드를 계획하십시오. 방화벽이 안정적인 전원에 연결되어 있는지 확인하십시오. 업그레이드 중 전원이 손실되면 방화벽을 사용할 수 없게 될 수 있습니다.

STEP 1 | VM-Series 방화벽에 사용할 수 있는 하드웨어 리소스가 충분한지 확인합니다.

를 참조하십시오. VM-Series 시스템 요구 사항 을 클릭하여 각 VM 시리즈 모델에 대한 리소스 요구 사항을 확인합니다. 업그레이드 프로세스를 계속하기 전에 추가 하드웨어 리소스를 할당하십시오. 추가 하드웨어 리소스를 할당하는 프로세스는 각 하이퍼바이저마다 다릅니다.

VM-Series 방화벽에 모델에 필요한 리소스가 없는 경우 기본적으로 VM-50과 연결된 용량으로 설정됩니다.

STEP 2 | 웹 인터페이스에서 다음으로 이동합니다. 장치 > 라이센스 올바른 VM-Series 방화벽 라이센스가 있고 라이센스가 활성화되어 있는지 확인합니다.

VM-Series 방화벽 독립 실행형 버전에서 장치 > 지원 그리고 지원 라이선스를 활성화했는지 확인합니다.

STEP 3 | 현재 구성 파일의 백업을 저장합니다.

방화벽이 구성 백업을 자동으로 생성하지만 업그레이드하기 전에 백업을 생성하고 외부에 저장하는 것이 가장 좋습니다.

쌍의 각 방화벽에서 다음 단계를 수행하십시오.

1. 디바이스 > 설정 > 작업을 선택하고 이름이 지정된 구성 스냅샷 내보내기를 클릭합니다.
2. 실행 중인 구성이 포함된 XML 파일(예: **running-config.xml**)을 선택하고 확인을 클릭하여 구성 파일을 내보냅니다.
3. 내보낸 파일을 방화벽 외부 위치에 저장합니다. 업그레이드에 문제가 있는 경우 이 백업을 사용하여 구성을 복원할 수 있습니다.

STEP 4 | (선택 사항) User-ID를 활성화한 경우 업그레이드 후 방화벽은 현재 IP 주소-사용자명 및 그룹 매핑을 지워 User-ID 소스의 속성으로 다시 채울 수 있습니다. 환경에서 매핑을 다시 채우는 데 필요한 시간을 예측하려면 방화벽에서 다음 CLI 명령을 실행합니다.

- IP 주소-사용자명 매핑의 경우:
  - **### User-ID #### ## ## ##**
  - **### ## ### ## ## ##**
- 그룹 매핑의 경우: **### ## ## ## ##**

STEP 5 | HA 쌍의 각 방화벽이 최신 콘텐츠 릴리스 버전을 실행 중인지 확인하십시오.

PAN-OS 11.0 릴리스용으로 설치해야 하는 최소 콘텐츠 릴리스 버전은 릴리스 노트를 참조하십시오. 다음을 따르십시오. Best Practices for Application and Threat Updates(응용 프로그램 및 위협 업데이트에 대한 모범 사례).

1. 디바이스 > 동적 업데이트을 선택하고 애플리케이션 또는 애플리케이션 및 위협을 확인하여 현재 설치된 업데이트를 확인합니다.
2. 방화벽이 설치하려는 소프트웨어 버전에 필요한 최소 콘텐츠 릴리스 버전 또는 이후 버전을 실행하지 않는 경우 지금 확인 을 클릭하여 사용 가능한 업데이트 목록을 검색합니다.
3. 원하는 콘텐츠 릴리스 버전을 찾아 다운로드합니다.

   콘텐츠 업데이트 파일을 성공적으로 다운로드하면 작업 열의 링크가 해당 콘텐츠 릴리스 버전에 대해 다운로드에서 설치로 변경됩니다.
4. 업데이트를 설치합니다. 두 피어 모두에 업데이트를 설치해야 합니다.

STEP 6 | VM-Series 플러그인을 업그레이드합니다.

1. 업그레이드하기 전에 최신 릴리스 정보에서 새 VM-Series 플러그인이 환경에 영향을 미치는지 여부에 대한 자세한 내용을 확인하십시오.

   예를 들어 새 VM 시리즈 플러그인 버전에 AWS 기능만 포함되어 있다고 가정합니다. 새로운 기능을 활용하려면 AWS의 VM-Series 방화벽 인스턴스에서 플러그인을 업데이트해야 합니다.

   사용자 환경에 적용되지 않는 업그레이드를 설치하지 마십시오.
2. VM-Series 방화벽에 로그인하고 대시보드를 확인하여 플러그인 버전을 확인합니다.
3. 고르다 장치 > 플러그인플러그인 버전을 봅니다. 쓰다 지금 확인 업데이트를 확인합니다.
4. 플러그인 버전을 선택한 다음 작업 열에서 설치를 클릭하여 플러그인을 설치합니다.

   HA 쌍의 VM-Series 방화벽에 플러그인을 설치할 때 액티브 피어보다 먼저 패시브 피어에 플러그인을 설치합니다. 패시브 피어에 플러그인을 설치하면 비기능 상태로 전환됩니다. 액티브 피어에 플러그인을 설치하면 패시브 피어가 기능 상태로 돌아갑니다.

STEP 7 | 각 쌍의 첫 번째 피어에서 선점을 비활성화합니다. HA 쌍의 한 방화벽에서만 이 설정을 비활성화해야 하지만 업그레이드를 진행하기 전에 커밋이 성공했는지 확인합니다.

1. 디바이스 > 고가용성을 선택하고 일렉션**(election)** 설정을 편집합니다.
2. 활성화된 경우 선점 설정을 비활성화(지우기)하고 확인을 클릭합니다.
3. 변경 사항을 커밋합니다.

STEP 8 | 첫 번째 피어에 PAN-OS 릴리스를 설치합니다.

능동형/수동형 구성에서 가동 중지 시간을 최소화하려면 먼저 수동 피어를 업그레이드하십시오. 능동형/능동형 구성의 경우 먼저 보조 피어를 업그레이드하십시오. 모범 사례로 능동형/능동형 구성을 사용하는 경우 동일한 유지 관리 기간 동안 두 피어를 모두 업그레이드하는 것이 좋습니다.

업그레이드하기 전에 *HA*가 제대로 작동하는지 테스트하려면 먼저 능동형/수동형 구성에서 활성 피어를 업그레이드하여 장애 없이 페일오버가 발생하는지 확인하십시오.

1. 첫 번째 피어에서 > 디바이스 > 소프트웨어 > 를 선택하고 최신 업데이트를 보려면 지금 확인을 클릭합니다**.**
2. Locate 및 다운로드 대상 PAN-OS 버전입니다.

   방화벽이 관리 포트에서 인터넷에 액세스할 수 없는 경우 Palo Alto Networks 지원 포털에서 소프트웨어 이미지를 다운로드한 다음 방화벽에 수동으로 업로드할 수 있습니다.
3. 이미지를 다운로드한 후(또는 수동 업그레이드의 경우 이미지를 업로드한 후) 이미지를 설치합니다.
4. 설치가 성공적으로 완료되면 다음 방법 중 하나를 사용하여 재부팅합니다.
   - 재부팅하라는 메시지가 표시되면 예를 클릭합니다.
   - 재부팅하라는 메시지가 표시되지 않으면 디바이스 > 설정 > 작업 및 디바이스 재부팅을 선택합니다.
5. 디바이스 재부팅이 완료되면 대시보드에서 고가용성 위젯을 보고 방금 업그레이드한 디바이스가 여전히 **HA** 구성에서 수동형 또는 능동형**-**보조 피어인지 확인합니다**.**

STEP 9 | 두 번째 피어에 PAN-OS 릴리스를 설치합니다.

1. (액티브/패시브 구성만 해당) HA가 방금 업그레이드한 피어로 장애 조치(failover)되도록 활성 피어를 일시 중단합니다.
   1. 활성 피어에서 장치 > 고가용성 > 운영 명령 을 클릭하고 로컬 장치 일시 중단.
   2. 대시보드에서 고가용성 위젯을 보고 상태가 수동으로 변경되는지 확인합니다.
   3. 다른 피어에서 활성 상태이고 트래픽을 전달하고 있는지 확인합니다(모니터 > 세션 브라우저).
2. 두 번째 피어에서 디바이스 > 소프트웨어 > 를 선택하고 최신 업데이트를 보려면 지금 확인을 클릭합니다.
3. Locate 및 다운로드 대상 PAN-OS 버전입니다.
4. 이미지를 다운로드한 후 설치합니다.
5. 설치가 성공적으로 완료되면 다음 방법 중 하나를 사용하여 재부팅합니다.
   - 재부팅하라는 메시지가 표시되면 예를 클릭합니다.
   - 재부팅하라는 메시지가 표시되지 않으면 디바이스 > 설정 > 작업 및 디바이스 재부팅을 선택합니다.
6. (능동형/수동형 구성만 해당) 방금 업그레이드한 피어의 CLI에서 다음 명령을 실행하여 방화벽이 다시 작동하도록 합니다.

   `request high-availability state functional`

STEP 10 | 두 피어가 예상대로 트래픽을 전달하는지 확인하십시오.

능동형/수동형 구성에서는 활성 피어만 트래픽을 전달해야 합니다. 두 피어 모두 능동형/능동형 구성에서 트래픽을 전달해야 합니다.

다음 CLI 명령을 실행하여 업그레이드가 성공했는지 확인합니다.

- (활성 피어만) 활성 피어가 트래픽을 전달하는지 확인하려면 **`show session all`** 명령을 실행합니다.
- 세션 동기화를 확인하려면 **`show high-availability interface ha2`** 명령을 실행하고 CPU 테이블의 하드웨어 인터페이스 카운터가 다음과 같이 증가하는지 확인합니다.
  - 활성/ 수동 구성, 활성 피어만 전송된 패킷을 표시합니다. 수동 피어는 수신된 패킷만 표시합니다.

    HA2 연결 유지를 활성화한 경우 수동 피어의 하드웨어 인터페이스 카운터는 전송 및 수신 패킷을 모두 표시합니다. 이는 *HA2* 연결 유지가 양방향이기 때문에 발생합니다. 즉, 두 피어 모두 *HA2* 연결 유지 패킷을 전송합니다.
  - 활성/활성 구성에서는 두 피어에서 수신된 패킷과 전송된 패킷을 볼 수 있습니다.

STEP 11 | 업그레이드 전에 선점을 비활성화했다면 지금 다시 활성화하십시오.

1. 디바이스 > 고가용성을 선택하고 일렉션**(election)** 설정을 편집합니다.
2. 선점을 선택하고 확인을 클릭합니다**.**
3. 변경 사항을 커밋합니다.

Panorama를 사용하여 VM 시리즈 PAN-OS 소프트웨어 업그레이드

다음 절차를 사용하여 Panorama로 관리하는 방화벽을 업그레이드합니다. 이 절차는 독립 실행형 방화벽 및 고가용성(HA) 구성에 배포된 방화벽에 적용됩니다.

*Panorama*가 업데이트 서버에 직접 연결할 수 없는 경우 Panorama가 인터넷에 연결되어 있지 않을 때 방화벽에 업데이트 배포 절차에 따라 *Panorama*에 이미지를 수동으로 다운로드한 다음 방화벽에 배포할 수 있습니다.

Panorama에서 방화벽을 업그레이드하려면 먼저 다음을 수행해야 합니다.

- Panorama가 업그레이드하려는 PAN-OS 버전과 같거나 이후 버전을 실행하고 있는지 확인하십시오. 관리형 방화벽을 이 버전으로 업그레이드하기 전에 Panorama를 업그레이드하고 해당 Log Collector를 11.0으로 업그레이드해야 합니다. 또한, Log Collector를 11.0으로 업그레이드할 때 로깅 인프라의 변경으로 인해 모든 Log Collector를 동시에 업그레이드해야 합니다.
- Panorama를 9.1로 업그레이드할 때 최대 6시간의 유지 보수 기간을 확장하십시오. 이 릴리즈에는 중요한 인프라 변경 사항이 포함되어 있습니다. 따라서 이전 릴리즈보다 Panorama 업그레이드 시간이 더 오래 걸립니다.
- 방화벽이 안정적인 전원에 연결되어 있는지 확인하십시오. 업그레이드 중 전원이 손실되면 방화벽을 사용할 수 없게 될 수 있습니다.

STEP 1 | Panorama를 업그레이드한 후 업그레이드할 방화벽에 구성을 커밋하고 푸시합니다.

STEP 2 | VM-시리즈 방화벽에 충분한 하드웨어 리소스가 제공되는지 확인합니다.

각 VM 시리즈 모델에 대한 리소스 요구 사항을 확인하려면 VM 시리즈 시스템 요구 사항을 참조하십시오. 업그레이드 프로세스를 계속하기 전에 추가 하드웨어 리소스를 할당하십시오. 추가 하드웨어 리소스를 할당하는 프로세스는 각 하이퍼바이저마다 다릅니다.

VM 시리즈 방화벽에 모델에 필요한 리소스가 없으면 기본적으로 VM-50과 관련된 용량으로 설정됩니다.

STEP 3 | 웹 인터페이스에서 **Device** > **Licenses** 으로 이동하여 올바른 VM-Series 방화벽 라이센스를 사용하고 라이센스를 활성화했는지 확인합니다.

VM 시리즈 방화벽 독립 버전에서 **Device** > **Support** 으로 이동하여 지원 라이센스를 활성화했는지 확인합니다.

STEP 4 | 업그레이드하려는 각 관리 방화벽에 현재 구성 파일의 백업을 저장합니다.

방화벽이 구성 백업을 자동으로 생성하지만 업그레이드하기 전에 백업을 생성하고 외부에 저장하는 것이 가장 좋습니다.

1. Panorama 웹 인터페이스에서 **Panorama** > 설정 > 작동을 선택하고 **Panorama** 및 디바이스 구성 번들 내보내기를 클릭하여 Panorama 및 각 관리 어플라이언스의 최신 구성 백업을 생성하고 내보냅니다.
2. 내보낸 파일을 방화벽 외부 위치에 저장합니다. 업그레이드에 문제가 있는 경우 이 백업을 사용하여 구성을 복원할 수 있습니다.

STEP 5 | 업그레이드하려는 방화벽에서 콘텐츠 릴리스 버전을 업데이트합니다.

PAN-OS 11.0에 필요한 최소 콘텐츠 릴리스 버전은 릴리스 노트를 참조하십시오. Panorama 및 관리된 방화벽에 콘텐츠 업데이트를 배포할 때 사용 프로그램 및 위협 업데이트의 Best Practice를 준수해야 합니다.

1. 최신 업데이트를 보려면 **Panorama** > 디바이스 배포 > 동적 업데이트 및 지금 확인을 선택합니다. 업데이트가 있으면 작업 열에 다운로드 링크가 표시됩니다.
2. 아직 설치하지 않은 경우 최신 콘텐츠 릴리스 버전을 다운로드합니다.
3. 설치를 클릭하고 업데이트를 설치할 방화벽을 선택한 다음 확인을 클릭합니다. HA 방화벽을 업그레이드하는 경우 두 피어 모두에서 콘텐츠를 업데이트해야 합니다.

STEP 6 | (HA 방화벽 업그레이드만 해당) HA 쌍의 일부인 방화벽을 업그레이드할 경우 선점을 비활성화합니다. 각 HA 쌍에 있는 하나의 방화벽에서만 이 설정을 비활성화하면 됩니다.

1. 디바이스 > 고가용성을 선택하고 일렉션**(election)** 설정을 편집합니다.
2. 활성화된 경우 선점 설정을 비활성화(지우기)하고 확인을 클릭합니다.
3. 변경사항을 커밋합니다. 업그레이드를 진행하기 전에 커밋이 성공했는지 확인합니다.

STEP 7 | 대상 PAN-OS 11.0 릴리스 이미지를 다운로드합니다.

1. 최신 릴리스 버전을 보려면 **Panorama** > 디바이스 배포 > 소프트웨어 및 지금 확인을 선택합니다.
2. 업그레이드할 릴리스 버전의 방화벽 관련 파일을 다운로드합니다. 업그레이드할 각 방화벽 모델(또는 방화벽 시리즈)에 대해 별도의 설치 파일을 다운로드해야 합니다.

STEP 8 | 방화벽에 PAN-OS 소프트웨어 업데이트를 설치합니다.

1. 업그레이드할 방화벽 모델에 해당하는 작업 열에서 설치를 클릭합니다.
2. 소프트웨어 파일 배포 대화 상자에서 업그레이드할 모든 방화벽을 선택합니다. 가동 중지 시간을 줄이려면 각 HA 쌍에서 피어를 하나만 선택하십시오. 활성/수동 쌍의 경우 수동 피어를 선택합니다. 활성/활성 쌍의 경우 활성-보조 피어를 선택합니다.
3. (HA 방화벽 업그레이드만 해당) 그룹 **HA** 피어가 선택되지 않았는지 확인합니다.
4. 설치 후 디바이스 재부팅을 선택합니다.
5. 업그레이드를 시작하려면 확인을 클릭합니다.
6. 설치가 성공적으로 완료되면 다음 방법 중 하나를 사용하여 재부팅합니다.
   - 재부팅하라는 메시지가 표시되면 예를 클릭합니다.
   - 재부팅하라는 메시지가 표시되지 않으면 디바이스 > 설정 > 작업 및 디바이스 재부팅을 선택합니다.
7. 방화벽 재부팅이 완료되면 **Panorama** > 관리형 디바이스를 선택하고 업그레이드한 방화벽의 소프트웨어 버전이 11.0.0인지 확인합니다. 또한, 업그레이드한 수동 방화벽의 HA 상태가 여전히 수동인지 확인합니다.

STEP 9 | (HA 방화벽 업그레이드만 해당) 각 HA 쌍에서 두 번째 HA 피어를 업그레이드합니다.

1. (활성/수동 업그레이드만 해당) 업그레이드 중인 각 활성/수동 쌍에서 활성 디바이스를 일시 중지합니다.
   1. 컨텍스트를 능동형 방화벽으로 전환합니다.
   2. 대시보드의 고가용성 위젯에서 **Local** 방화벽 상태가 **Active**이고 **Peer**가 **Passive**인지 확인합니다.
   3. 디바이스 > 고가용성 > 작동 명령 > 로컬 디바이스 일시 중단을 선택합니다.
   4. 대시보드의 고가용성 위젯으로 돌아가서 **Local**이 **Passive**로, **Peer**가 **Active**로 변경되었는지 확인합니다.
2. Panorama 컨텍스트로 돌아가서 **Panorama** > 디바이스 배포 > 소프트웨어를 선택합니다.
3. 업그레이드 중인 HA 쌍의 방화벽 모델에 해당하는 작업 열에서 설치를 클릭합니다.
4. 소프트웨어 파일 배포 대화 상자에서 업그레이드할 모든 방화벽을 선택합니다. 이번에는 방금 업그레이드한 HA 방화벽의 피어만 선택합니다.
5. 그룹 **HA** 피어가 선택되지 않았는지 확인합니다.
6. 설치 후 디바이스 재부팅을 선택합니다.
7. 업그레이드를 시작하려면 확인을 클릭합니다.
8. 설치가 성공적으로 완료되면 다음 방법 중 하나를 사용하여 재부팅합니다.
   - 재부팅하라는 메시지가 표시되면 예를 클릭합니다.
   - 재부팅하라는 메시지가 표시되지 않으면 디바이스 > 설정 > 작업 및 디바이스 재부팅을 선택합니다.
9. (활성/수동 업그레이드만 해당)방금 업그레이드한 피어의 CLI에서 다음 명령을 실행하여 방화벽이 다시 작동하도록 합니다.

   ```
   request high-availability state functional
   ```

STEP 10 | (PAN-OS XFR 업그레이드만) 단계 8 및 단계 9을 반복하여 첫 번째 피어 및 두 번째 피어를 PAN-OS XFR로 업그레이드합니다.

STEP 11 | 각 관리 방화벽에서 실행되는 소프트웨어 및 콘텐츠 릴리스 버전을 확인합니다.

1. Panorama에서 **Panorama** > 관리형 디바이스를 선택합니다.
2. 방화벽을 찾고 표에서 콘텐츠 및 소프트웨어 버전을 검토합니다.

   HA 방화벽의 경우 각 피어의 HA 상태가 예상대로인지 확인할 수도 있습니다.

STEP 12 | (HA 방화벽 업그레이드만 해당) 업그레이드하기 전에 HA 방화벽 중 하나에서 선점을 비활성화한 경우 일렉션**(election)** 설정(디바이스 > 고가용성) 해당 방화벽에 대해 선점 설정을 다시 활성화한 다음 변경 사항을 커밋합니다.

PAN-OS 소프트웨어 버전 업그레이드(NSX용 VM 시리즈)

배포에 가장 적합한 업그레이드 방법을 선택합니다.

- 유지 관리 기간 중 NSX용 VM 시리즈 업그레이드 - 이 옵션을 사용하면 서비스 정의의 OVF URL을 변경하지 않고 유지 관리 기간 중에 VM 시리즈 방화벽을 업그레이드할 수 있습니다.
- 트래픽 중단 없이 NSX용 VM 시리즈 업그레이드 - 이 옵션을 사용하면 게스트 VM에 대한 서비스를 중단하거나 서비스 정의의 OVF URL을 변경하지 않고도 VM 시리즈 방화벽을 업그레이드할 수 있습니다.

다음 그래픽은 현재 지원되는 Panorama와 VMware NSX용 Panorama 플러그인 조합과 성공적으로 업그레이드하기 위해 따라야 하는 업그레이드 경로를 보여줍니다.

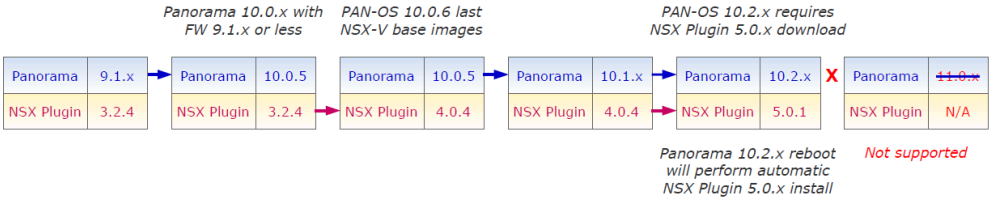
- 아래의 각 상자는 지원되는 조합을 나타냅니다.
- HA 쌍에서 NSX 또는 Panorama용 Panorama 플러그인을 업그레이드하는 경우 패시브 파노라마 피어를 먼저 업그레이드한 다음 액티브 HA 피어를 업그레이드하십시오.

VMware NSX 배포용 VM 시리즈를 업그레이드하기 전에 아래에 표시된 업그레이드 경로를 검토하여 환경에 가장 적합한 플러그인과 PAN-OS 조합을 찾기 위한 업그레이드 단계를 이해하십시오.

Panorama and PAN NSX Plugin Upgrade Paths

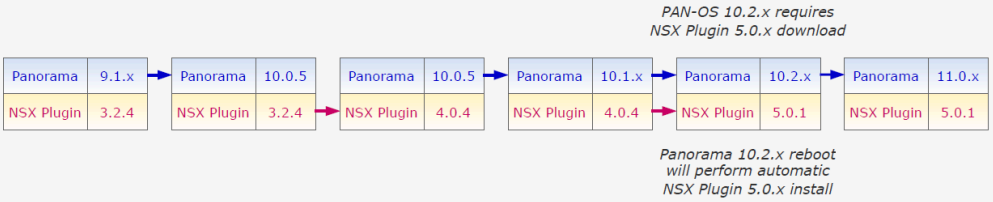
- For Panorama upgrades, first upgrade Panorama HA Passive, then Panorama HA Active
- For NSX Plugin upgrades, first upgrade Panorama HA Passive, then Panorama HA Active
- Best practice is always upgrade one at a time (either Panorama or NSX Plugin)

VM-Series for NSX-V



IMPORTANT! PAN-OS 10.0.6 are the last available base images for VM-Series for NSX-V.

VM-Series for NSX (formerly NSX-T)



IMPORTANT! VMware NSX-T has been renamed to VMware NSX as of version 4.0.x.

유지 관리 기간 동안 NSX용 VM 시리즈 업그레이드

VM 시리즈 방화벽 NSX 버전의 경우 Panorama를 사용하여 방화벽의 소프트웨어 버전을 업그레이드하십시오.

STEP 1 | VMware NSX용 VM 시리즈업그레이드 경로를검토합니다.

STEP 2 | VM-시리즈 방화벽에 추가 하드웨어 리소스를 할당하십시오.

VM 시리즈 방화벽에 충분한 하드웨어 리소스를 사용할 수 있는지 확인하십시오. 각 VM 시리즈 모델에 대한 새로운 리소스 요구 사항을 보려면VM 시리즈 시스템 요구 사항을참조하세요. 업그레이드 프로세스를 계속하기 전에 추가 하드웨어 리소스를 할당하십시오. 추가 하드웨어 리소스를 할당하는 프로세스는 하이퍼바이저마다 다릅니다.

STEP 3 | 업그레이드하려는 각 관리 방화벽에 현재 구성 파일의 백업을 저장합니다.

방화벽이 구성의 백업을 자동으로 생성하지만 업그레이드하기 전에 백업을 생성하고 외부에 저장하는 것이 가장 좋습니다.

1. 장치 > 설정 > 작업을선택하고파노라마 및 장치 구성 번들 내보내기를클릭합니다. 이 옵션은 Panorama 및 각 관리 장치 구성 백업의 최신 버전을 수동으로 생성하고 내보내는 데 사용됩니다.
2. 내보낸 파일을 방화벽 외부 위치에 저장합니다. 업그레이드에 문제가 있는 경우 이 백업을 사용하여 구성을 복원할 수 있습니다.

STEP 4 | PAN-OS 버전에 필요한 콘텐츠 릴리스 버전을 확인하려면 릴리스 노트를 확인하세요.

업그레이드하려는 방화벽은 PAN-OS 버전에 필요한 콘텐츠 릴리스 버전을 실행해야 합니다.

1. **Panorama** > 디바이스 배포 > 동적 업데이트를 선택합니다.
2. 최신 업데이트를 확인하세요. 지금 확인(창의 왼쪽 하단에 위치)을 클릭하여 최신 업데이트를 확인하세요. 작업 열의 링크는 업데이트가 있는지의 여부를 나타냅니다. 버전을 사용할 수 있으면다운로드링크가 표시됩니다.
3. 선택한 버전을 다운로드하려면다운로드를클릭하세요. 다운로드에 성공하면 **Action** 열의 링크가 **Download**에서 **Install**로 변경됩니다.
4. 설치를 클릭하고 업데이트를 설치할 방화벽을 선택합니다. 설치가 완료되면 현재 설치됨 열에 확인 표시가 나타납니다.

STEP 5 | 선택한 방화벽에 소프트웨어 업데이트를 배포합니다.

방화벽이 *HA*로 구성된 경우그룹 ***HA*** 피어확인란을 선택 취소하고 한 번에 하나의 *HA* 피어를 업그레이드해야 합니다.

1. **Panorama** > 디바이스 배포 > 소프트웨어를 선택합니다.
2. 최신 업데이트를 확인하세요. 지금 확인(창의 왼쪽 하단에 있음)을 클릭하여 최신 업데이트를 확인하세요. 작업 열의 링크는 업데이트가 있는지의 여부를 나타냅니다.
3. 파일 이름을검토하고다운로드 를클릭합니다. 다운로드하는 소프트웨어 버전이 네트워크에 배포된 방화벽 모델과 일치하는지 확인하십시오. 다운로드에 성공하면 **Action** 열의 링크가 **Download**에서 **Install**로 변경됩니다.
4. 설치를클릭하고 소프트웨어 버전을 설치하려는 장치를 선택합니다.
5. 설치 후 디바이스 재부팅을 선택합니다.
6. HA에 장치가 구성되어 있는 경우그룹 **HA** 피어확인란을 선택 취소하고 한 번에 하나의 HA 피어를 업그레이드합니다.

STEP 6 | 각 관리 방화벽에서 실행되는 소프트웨어 및 콘텐츠 릴리스 버전을 확인합니다.

1. **Panorama** > 관리형 디바이스를 선택합니다.
2. 방화벽을 찾고 표에서 콘텐츠 및 소프트웨어 버전을 검토합니다.

트래픽 중단 없이 NSX용 VM 시리즈 업그레이드

다음 절차를 사용하여 VMware NSX 환경에서 PAN-OS 버전의 VM 시리즈 방화벽을 업그레이드할 수 있습니다. 이 절차를 통해 VM을 다른 ESXi 호스트로 마이그레이션하여 트래픽을 방해하지 않고 PAN-OS 업그레이드를 수행할 수 있습니다.

STEP 1 | VMware NSX 업그레이드 경로를 위한 VM 시리즈를 검토하십시오.

STEP 2 | 업그레이드하려는 각 관리 방화벽에 현재 구성 파일의 백업을 저장합니다.

방화벽이 구성의 백업을 자동으로 생성하지만 업그레이드하기 전에 백업을 생성하고 외부에 저장하는 것이 가장 좋습니다.

1. [장치 > 설정 > 작업] 을 선택하고 파노라마 및 장치 구성 번들 내보내기를 클릭합니다. 이 옵션은 Panorama 및 각 관리 장치의 컨피그레이션 백업의 최신 버전을 수동으로 생성하고 내보내는 데 사용됩니다.
2. 내보낸 파일을 방화벽 외부 위치에 저장합니다. 업그레이드에 문제가 있는 경우 이 백업을 사용하여 구성을 복원할 수 있습니다.

STEP 3 | 릴리스 노트를 확인하여 PAN-OS 버전에 필요한 콘텐츠 릴리스 버전을 확인하십시오.

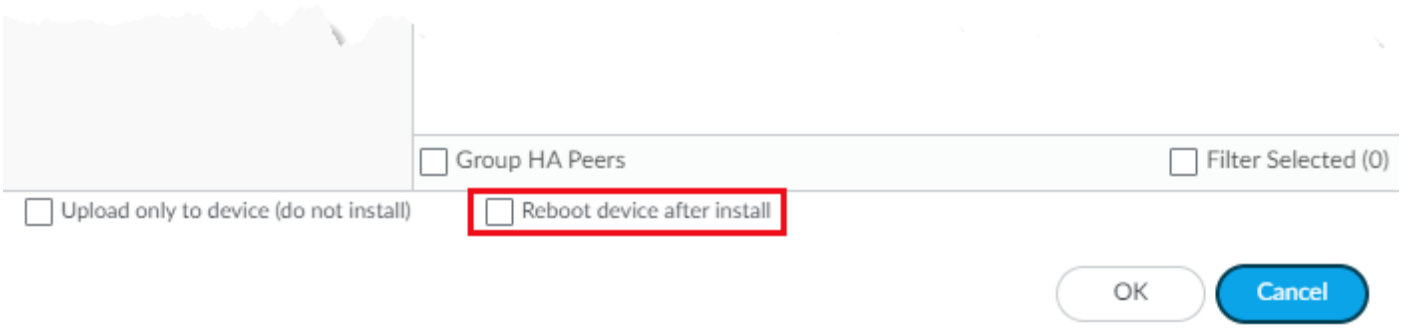
업그레이드하려는 방화벽에는 PAN-OS 버전에 필요한 콘텐츠 릴리스 버전이 실행되고 있어야 합니다.

1. **Panorama** > 디바이스 배포 > 동적 업데이트를 선택합니다.
2. 최신 업데이트를 확인하세요. Check Now (창의 왼쪽 하단 모서리에 있음) 를 클릭하여 최신 업데이트를 확인합니다. 작업 열의 링크는 업데이트가 있는지의 여부를 나타냅니다. 사용 가능한 버전이 있는 경우 다운로드 링크가 표시됩니다.
3. 다운로드를 클릭하여 선택한 버전을 다운로드합니다. 다운로드에 성공하면 **Action** 열의 링크가 **Download**에서 **Install**로 변경됩니다.
4. 설치를 클릭하고 업데이트를 설치할 방화벽을 선택합니다. 설치가 완료되면 현재 설치됨 열에 확인 표시가 나타납니다.

STEP 4 | PAN-OS 이미지를 클러스터의 모든 VM 시리즈 방화벽에 다운로드합니다.

1. 파노라마에 로그인합니다.
2. **Panorama** > 디바이스 배포 > 소프트웨어를 선택합니다.
3. 새로 고침을 클릭하여 최신 소프트웨어 릴리스를 확인하고 릴리스 노트를 검토하여 릴리스의 변경 사항에 대한 설명을 확인하고 소프트웨어를 설치하기 위한 마이그레이션 경로를 확인하십시오.
4. 다운로드를 클릭하여 소프트웨어를 검색한 다음 설치를 클릭합니다.

   새 소프트웨어 이미지를 설치한 후에는 *VM* 시리즈 방화벽을 재부팅하지 마십시오.
5. 업그레이드할 관리 대상 장치를 선택합니다.
6. 설치 후 장치 재부팅 확인란의 선택을 취소합니다.



7. 확인을 클릭합니다.

STEP 5 | 클러스터의 첫 번째 ESXi 호스트에서 VM 시리즈 방화벽을 업그레이드합니다.

1. vCenter에 로그인합니다.
2. 호스트 및 클러스터를 선택합니다.
3. 호스트를 마우스 오른쪽 버튼으로 클릭하고 유지 보수 모드를 > 선택합니다. > 유지 보수 모드로 전환합니다.
4. VM 시리즈 방화벽을 제외한 모든 VM을 호스트 외부로 (자동 또는 수동) 마이그레이션합니다.
5. VM 시리즈 방화벽의 전원을 끕니다. 이는 호스트에서 유지 보수 모드로 전환되면 자동으로 발생해야 합니다.
6. (선택 사항) 업그레이드 프로세스를 계속하기 전에 VM 시리즈 방화벽에 추가 CPU 또는 메모리를 할당합니다.

   VM 시리즈 방화벽에 사용할 수 있는 하드웨어 리소스가 충분한지 확인합니다. 각 VM 시리즈 모델에 대한 새로운 리소스 요구 사항을 보려면 VM 시리즈 모델을 참조하십시오.
7. 호스트를 마우스 오른쪽 버튼으로 클릭하고 유지 보수 모드를 선택합니다. 유지 > 보수 모드 종료를 선택합니다. 유지 보수 모드를 종료하면 NSX ESX Agent Manager (EAM) 에서 VM 시리즈 방화벽의 전원이 켜집니다. 새 PAN-OS 버전으로 방화벽이 재부팅됩니다.
8. 모든 VM을 (자동 또는 수동) 원래 호스트로 다시 마이그레이션합니다.

STEP 6 | 각 ESXi 호스트의 각 VM 시리즈 방화벽에 대해 이 프로세스를 반복합니다.

STEP 7 | 각 관리 방화벽에서 실행되는 소프트웨어 및 콘텐츠 릴리스 버전을 확인합니다.

1. **Panorama** > 관리형 디바이스를 선택합니다.
2. 디바이스를 찾고 테이블에 있는 콘텐츠 및 소프트웨어 버전을 검토합니다.

VM 시리즈 모델 업그레이드

VM 시리즈 방화벽의 라이센스 프로세스에서는 UUID와 CPU ID를 사용하여 각 VM 시리즈 방화벽에 대한 고유 일련 번호를 생성합니다. 따라서 라이센스를 생성하면 해당 라이센스는 VM 시리즈 방화벽의 특정 인스턴스에 매핑되며 수정할 수 없습니다.

다음과 같은 경우에는 이 섹션의 지침을 따르십시오.

- 평가판 라이센스에서 프로덕션 라이센스로 마이그레이션합니다.
- 용량을 늘릴 수 있도록 모델을 업그레이드합니다. 예를 들어 VM-100에서 VM-300 모델로 업그레이드하려고 합니다.

- 방화벽에서 일부 중요한 프로세스를 다시 시작하는 용량 업그레이드. 서비스 중단을 최소화하려면 *HA* 구성을 권장합니다. *HA* 쌍의 용량을 업그레이드하려면HA 쌍의 VM 시리즈 모델 업그레이드를참조하십시오.
- 프라이빗 또는 퍼블릭 클라우드 배포에서 방화벽에 *BYOL* 옵션 라이선스가 부여된 경우 인스턴스 유형이나 *VM* 유형을 변경하기 전에VM을 비활성화해야 합니다. 모델이나 인스턴스를 업그레이드하면 *UUID*와 *CPU ID*가 변경되므로 .

STEP 1 | VM-시리즈 방화벽에 추가 하드웨어 리소스를 할당하십시오.

용량 업그레이드를 시작하기 전에 VM 시리즈 방화벽에서 새 용량을 지원하기에 충분한 하드웨어 리소스를 사용할 수 있는지 확인해야 합니다. 추가 하드웨어 리소스를 할당하는 프로세스는 하이퍼바이저마다 다릅니다.

새로운 VM 시리즈 모델의 하드웨어 요구 사항을 확인하려면VM 시리즈 모델 을참조하십시오.

용량 업그레이드에는 VM 시리즈 방화벽을 재부팅할 필요가 없지만 하드웨어 할당을 변경하려면 가상 머신의 전원을 꺼야 합니다.

STEP 2 | 고객 지원포털에서 라이선스 API 키를 검색하세요.

1. 고객 지원 포털에 로그인합니다.

   초기 라이센스를 등록하는 데 사용한 것과 동일한 계정을 사용하고 있는지 확인하십시오.

2. 왼쪽 메뉴에서자산 > **API** 키 관리를선택합니다.
3. API 키를 복사합니다.

STEP 3 | 방화벽에서 CLI를 사용하여 이전 단계에서 복사한 API 키를 설치합니다.

```
#### API # ## # ## <key>
```

STEP 4 | (인터넷에 접속할 수 있는 경우)장치 > 설정 > 서비스에서업데이트 서버 **ID**를 확인하려면 방화벽을 활성화하십시오.

STEP 5 | 변경 사항을 커밋합니다. 방화벽에 로컬로 구성된 사용자가 있는지 확인하십시오. 구성이 라이센스가 없는 PA-VM 개체 제한을 초과하는 경우 비활성화 후 파노라마 푸시 사용자를 사용하지 못할 수 있습니다.

STEP 6 | 용량을 업그레이드하세요.

Device > **Licenses**를 선택한 후 다음 방법 중 하나로 라이선스 및 구독을 활성화합니다.

- 라이선스 서버에서 라이선스 키 검색 - 고객 지원 포털에서 라이선스를 활성화한 경우 이 옵션을 사용합니다.
- (인터넷) 인증 코드 사용 -지원 포털에서 이전에 활성화되지 않은 라이선스에 대한 인증 코드를 사용하여 VM 시리즈 용량을 업그레이드하려면 이 옵션을 사용합니다. 메시지가 표시되면 인증 코드를 입력한 다음 확인을 클릭합니다.
- (인터넷 없음) 라이선스 키 수동 업로드- 방화벽이고객 지원포털에 인터넷으로 연결되어 있지 않은 경우 이 옵션을 사용합니다. 인터넷이 연결된 컴퓨터에서 CSP에 로그인하고 라이선스 키 파일을 다운로드한 후 방화벽과 동일한 네트워크에 있는 컴퓨터로 전송하고 방화벽에 업로드합니다.

STEP 7 | 방화벽에 라이선스가 성공적으로 부여되었는지 확인하세요.

장치 > 라이선스페이지에서 라이선스가 성공적으로 활성화되었는지 확인합니다.

HA 쌍의 VM 시리즈 모델 업그레이드

VM 시리즈 방화벽을 업그레이드하면 방화벽의 용량을 늘릴 수 있습니다. 용량은 VM 시리즈 방화벽이 처리하도록 최적화된 세션, 규칙, 보안 영역, 주소 개체, IPsec VPN 터널 및 SSL VPN 터널의 수로 정의됩니다. VM 시리즈 방화벽에 새 용량 라이센스를 적용하면 모델 번호 및 관련 용량이 방화벽에 구현됩니다.

업그레이드하기 전에 방화벽 모델의 VM 시리즈 시스템 요구 사항을 확인하십시오. 방화벽의 메모리가 *5.5GB* 미만인 경우 방화벽의 용량 *(*세션 수, 규칙, 보안 영역, 주소 개체 수 등*)* 이 *VM-50 Lite*의 용량으로 제한됩니다.

이 프로세스는 HA 구성에 있는 하드웨어 기반 방화벽 쌍을 업그레이드하는 프로세스와 유사합니다. 세션 동기화를 활성화한 경우 용량 업그레이드 프로세스 중에도 세션 동기화가 계속됩니다. 고가용성(HA) 구성에 있는 방화벽을 업그레이드할 때 가동 중지 시간을 방지하려면 한 번에 하나의 HA 피어를 업데이트하십시오.

업그레이드 프로세스 중에 방화벽의 구성을 변경하지 마십시오. 업그레이드 프로세스 중에 용량 불일치가 감지되면 구성 동기화가 자동으로 비활성화되고 두 *HA* 피어의 용량 라이센스가 일치하면 다시 활성화됩니다.

HA 쌍의 방화벽이 주요 소프트웨어 버전 *(*예*: 9.1* 및 *9.0)* 이 다르고 용량이 다른 경우 두 디바이스 모두 일시 중단된 *HA* 상태가 됩니다. 따라서 용량을 업그레이드하기 전에 두 방화벽이 모두 동일한 버전의 *PAN-OS*를 실행하는지 확인하는 것이 좋습니다.

STEP 1 | 패시브 방화벽에서 용량 라이센스를 업그레이드합니다.

절차를 따라 VM 시리즈 모델을 업그레이드합니다.

일부 프로세스가 이 패시브 피어에서 다시 시작되면 새 VM 시리즈 모델이 대시보드에 표시됩니다. 이 업그레이드된 피어는 활성 피어와의 용량 불일치로 인해 이제 작동하지 않는 상태입니다.

세션 동기화를 활성화한 경우 다음 단계를 계속하기 전에 HA 피어 간에 세션이 동기화되었는지 확인하십시오. 세션 동기화를 확인하려면 show high-availability interface ha2 명령을 실행하고 CPU 테이블의 하드웨어 인터페이스 카운터가 다음과 같이 증가하는지 확인합니다.활성/ 수동 구성, 활성 피어만 전송된 패킷을 표시합니다. 수동 피어는 수신된 패킷만 표시합니다.**HA2 ## ### #### ## ## ### ## ## ##### #### ## # ## ### ## #####. ## HA2 ## ### ##### ### #####. #, # ## ## HA2 ## ## ### #####.**

활성/활성 구성에서는 두 피어에서 수신된 패킷과 전송된 패킷을 볼 수 있습니다.

STEP 2 | 활성 방화벽에서 용량 라이센스를 업그레이드합니다.

절차를 따라 VM 시리즈 모델을 업그레이드합니다.

새로운 VM 시리즈 모델은 중요한 프로세스가 재시작된 후 대시보드에 표시됩니다. 패시브 방화벽이 활성 상태가 되고 이 피어 (이전의 활성 방화벽) 는 초기 상태에서 HA 쌍의 패시브 피어가 됩니다.

VM 시리즈 방화벽을 이전 릴리스로 다운그레이드

다음 워크플로우를 사용하여 다른 기능 릴리스로 업그레이드하기 전에 실행 중이던 구성을 복원하십시오. 업그레이드 이후의 모든 변경 사항은 손실됩니다. 따라서 최신 기능 릴리스로 돌아갈 때 변경 사항을 복원할 수 있도록 현재 구성을 백업하는 것이 중요합니다.

다음 절차에 따라 이전 릴리스로 다운그레이드합니다.

STEP 1 | 현재 구성 파일의 백업을 저장합니다.

방화벽이 구성의 백업을 자동으로 생성하지만 업그레이드하기 전에 백업을 생성하고 외부에 저장하는 것이 가장 좋습니다.

1. 명명된 구성 스냅샷을 내보냅니다(디바이스 > 설정 > 작업).
2. 실행 중인 구성이 포함된 XML 파일(예: **running-config.xml**)을 선택하고 확인을 클릭하여 구성 파일을 내보냅니다.
3. 내보낸 파일을 방화벽 외부 위치에 저장합니다. 다운그레이드에 문제가 있는 경우 이 백업을 사용하여 구성을 복원할 수 있습니다.

STEP 2 | 이전 기능 릴리스 이미지를 설치합니다.

새 릴리스로 업그레이드하면 자동 저장 버전이 생성됩니다.

1. 지금 확인(디바이스 > 소프트웨어)에서 사용 가능한 이미지를 확인합니다.
2. 다운그레이드할 이미지를 찾습니다. 이미지가 아직 다운로드되지 않은 경우 다운로드합니다.
3. 다운로드가 완료되면 이미지를 설치합니다.
4. 다운그레이드를 위한 구성 파일 선택합니다. 디바이스를 재부팅하면 방화벽이 로드됩니다. 대부분의 경우 현재 다운그레이드 중인 릴리스에서 업그레이드할 때 자동으로 저장된 구성을 선택해야 합니다. 예를 들어, PAN-OS 11.0을 실행 중이고 PAN-OS 10.2.2로 다운그레이드하는 경우 autosave-10.2.2를 선택합니다.
5. 설치가 성공적으로 완료되면 다음 방법 중 하나를 사용하여 재부팅합니다.
   - 재부팅하라는 메시지가 표시되면 예를 클릭합니다.
   - 재부팅하라는 메시지가 표시되지 않으면 디바이스 작업(디바이스 > 설정 > 작업) 및 디바이스 재부팅으로 이동합니다.

Panorama 플러그인 업그레이드

Panorama 플러그인 업그레이드/다운그레이드 고려 사항

다음 표에는 업그레이드 또는 다운그레이드에 영향을 주는 하드웨어 기능이 나열되어 있습니다. PAN-OS 11.0 릴리스로 업그레이드하거나 다운그레이드하기 전에 가을 업그레이드/다운그레이드 고려 사항을 이해해야 합니다. PAN-OS 11.0 릴리스에 대한 추가 정보는 PAN-OS 11.0 릴리스 노트를 참조하십시오.

표 **1: Panorama** 플러그인 업그레이드**/**다운그레이드 고려 사항

기능	업그레이드 고려 사항	다운그레이드 고려 사항
Panorama 플러그인 • AWS 플러그인 • Azure 플러그인 • Kubernetes 플러그인 • 소프트웨어 방화벽 라이선스 플러그인 • PAN-OS SD-WAN 플러그인 • IPS 서명 변환기 플러그인 • ZTP 플러그인 • 엔터프라이즈 DLP 플러그인 • Openconfig 플러그인 • GCP 플러그인 • Cisco ACI 플러그인 • Nutanix 플러그인 • VCenter 플러그인	PAN-OS 11.0으로 업그레이드하기 전에 Panorama에 설치된 모든 플러그인에 대해 PAN-OS 11.0에서 지원되는 Panorama 플러그인 버전을 다운로드해야 합니다. 이는 PAN-OS 11.0으로 성공적으로 업그레이드하는 데 필요합니다. 자세한 내용은 호환성 매트릭스를 참조하십시오.	PAN-OS 11.0에서 다운그레이드하려면 Panorama에 설치된 모든 플러그인에 대해 PAN-OS 10.2 및 이전 릴리스에서 지원되는 Panorama 플러그인 버전을 다운로드해야 합니다. 자세한 내용은 Panorama 플러그인 호환성 매트릭스를 참조하십시오.
	(Enterprise DLP) Panorama를 PAN-OS 10.2로 업그레이드한 후 PAN-OS 11.0 또는 이전 릴리스를 실행하는 모든 관리 방화벽에 애플리케이션 및 위협 콘텐츠 릴리스 버전 8520을 설치해야 합니다. 이는 PAN-OS 10.2로 업그레이드하지 않은 Enterprise DLP를 활용하는 관리형 방화벽에 구성 변경 사항을 성공적으로 푸시하는 데 필요합니다.	
	(Enterprise DLP) Shared Enterprise DLP 구성이 포함된 Panorama 구성 백업을 로드하면 파일 기반이 아닌 트래픽을 스캔하는 데 필요한 공유 앱 제외 필터가 삭제됩니다.	
	(SD-WAN) SD-WAN 2.2 및 이전 릴리스용 Panorama 플러그인은 PAN-OS 11.0에서 지원되지 않습니다.	

기능	업그레이드 고려 사항	다운그레이드 고려 사항
	Panorama 관리 서버를 PAN-OS 11.0으로 업그레이드하면 SD-WAN용 Panorama 플러그인 2.2 이하 릴리스가 설치되어 SD-WAN 플러그인이 Panorama 웹 인터페이스에서 숨겨지거나 SD-WAN 구성이 삭제됩니다. 두 경우 모두 새 SD-WAN 플러그인 버전을 설치하거나 SD-WAN 플러그인을 제거할 수 없습니다.	
PAN-OS SD-WAN	Panorama를 PAN-OS 11.0으로 성공적으로 업그레이드하고 Panorama 플러그인을 SD-WAN 버전 2.0.0에서 SD-WAN 버전 3.0으로 성공적으로 업그레이드한 후에는 기존 SD-WAN 배포에 대해서만 Panorama에서 SD-WAN 캐시를 지워야 합니다. SD-WAN 캐시를 지우면 기존 SD-WAN 구성이 삭제되지 않지만 SD-WAN용 Panorama 플러그인 버전 3.0에 도입된 새 형식에 대한 IP 주소, 터널 및 게이트웨이 명명 규칙이 삭제됩니다. SD-WAN의 새 배포의 경우 PAN-OS 11.0으로 업그레이드한 후 Panorama에 SD-WAN 버전 3.0용 Panorama 플러그인을 설치하면 Panorama에서 SD-WAN 캐시를 지울 필요가 없습니다. 1. Panorama CLI에 로그인합니다. 2. Panorama에서 SD-WAN 캐시를 지웁니다. `admin> debug plugins sd_wan drop-config-cache all`	없음.

엔터프라이즈 DLP 플러그인 업그레이드

Panorama™ 관리 서버에 설치된 엔터프라이즈 데이터 손실 방지(DLP) 플러그인 버전을 업그레이드합니다.

Palo Alto Networks Panorama 플러그인 호환성 매트릭스를 참조하고 대상 Enterprise DLP 플러그인 버전에 필요한 최소 PAN-OS 버전을 검토합니다.

STEP 1 | Panorama 웹 인터페이스에 로그인합니다.

STEP 2 | Panorama에서 엔터프라이즈 DLP 플러그인 버전을 업그레이드합니다.

고가용성(HA) 구성의 Panorama의 경우 Panorama HA 피어에서 이 단계를 반복합니다.

1. 최신 **dlp** 플러그인 버전에 대해 **Panorama** > 플러그인 및 지금 확인을 선택합니다.
2. 최신 버전의 Enterprise DLP 플러그인을 다운로드 및 설치합니다.
3. 새 플러그인 버전이 성공적으로 설치되면 Panorama 대시보드를 보고 일반 정보 위젯에서 #### DLP 버전이 업그레이드한 Enterprise DLP 플러그인 버전을 표시하는지 확인합니다.

STEP 3 | (4.0.0으로 업그레이드만 해당) Enterprise DLP 데이터 필터링 설정을 편집하여 최대 파일 크기를 20MB 이하로 줄입니다.

이 플러그인 버전은 대용량 파일 크기 검사를 지원하지 않으므로 Enterprise DLP 3.0.3 이상 릴리스용 Panorama 플러그인을 Enterprise DLP 4.0.0으로 업그레이드할 때 필요합니다.

Panorama Interconnect 플러그인 업그레이드

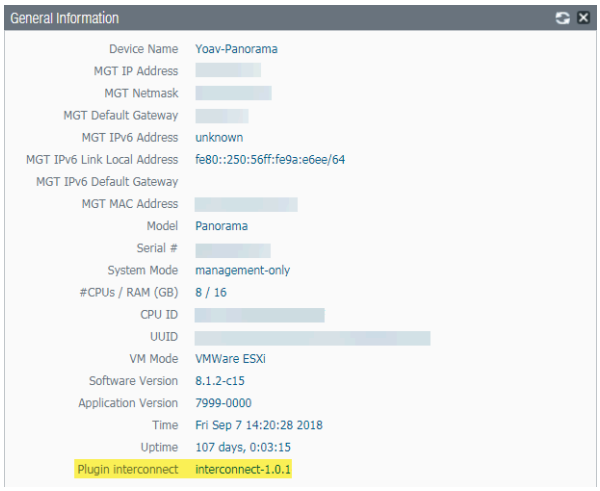
Panorama 컨트롤러 및 Panorama 노드에서 Panorama™ Interconnect 플러그인을 업그레이드하려면 다음 절차를 따르십시오. Panorama Interconnect 플러그인을 업그레이드할 때 Panorama 노드를 컨트롤러와 동일한 플러그인 버전으로 업그레이드하기 전에 Panorama 컨트롤러를 업그레이드해야 합니다. Panorama 노드에 다운로드하여 설치하는 새 플러그인 버전은 Panorama 컨트롤러에 설치한 플러그인 버전과 같아야 Panorama 컨트롤러와 선택한 Panorama 노드의 플러그인 버전이 동기화된 상태로 유지됩니다.

플러그인을 처음 설치하는 경우 Panorama Interconnect 플러그인 설정을 참조합니다.

STEP 1 | Panorama 컨트롤러의 Panorama 웹 인터페이스에 로그인합니다.

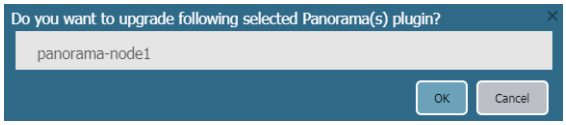
STEP 2 | Panorama Controller에서 Panorama Interconnect 플러그인을 업그레이드하십시오.

1. **Panorama** > 플러그인을 선택하고 ## ##을 검색합니다.
2. 새 Interconnect 플러그인 버전을 다운로드하고 설치합니다. 설치가 완료된 후 알려주는 프롬프트가 표시됩니다.
3. 대시보드에 새로 설치된 Interconnect 플러그인 버전이 표시되는지 확인합니다.

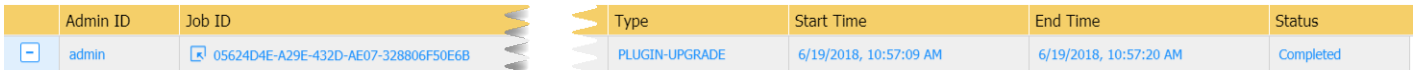


STEP 3 | Panorama Node에서 Panorama Interconnect 플러그인을 업그레이드합니다.

1. **Panorama** > 상호 연결 > **Panorama** 노드를 선택하고 하나 이상의 Panorama 노드를 선택하고 플러그인 업그레이드를 선택합니다.
2. 선택한 Panorama 노드를 확인하고 확인을 클릭하여 플러그인 업그레이드를 시작합니다.



3. 플러그인 업그레이드 작업이 ##될 때까지 기다리십시오. 작업 진행 상황을 보려면 **Panorama** > 상호 연결 > 작업을 클릭합니다.



4. 업그레이드가 성공적으로 완료되면 **Panorama** > 상호 연결 > **Panorama** 노드을 선택하여 선택한 Panorama 노드에 플러그인 버전이 올바른지 확인합니다.

SD-WAN 플러그인 업그레이드

Panorama™ 관리 서버 및 SD-WAN을 활용하는 방화벽에 설치된 SD-WAN 플러그인 버전을 업그레이드하십시오.

Palo Alto Networks Panorama 플러그인 호환성 매트릭스를 참조하고 대상 SD-WAN 플러그인 버전에 필요한 최소 PAN-OS 버전을 검토합니다.

STEP 1 | Panorama 웹 인터페이스에 로그인합니다.

STEP 2 | Panorama에서 SD-WAN 플러그인 버전을 업그레이드합니다.

고가용성(HA) 구성의 Panorama의 경우 Panorama HA 피어에서 이 단계를 반복합니다.

1. 최신 **sd_wan** 플러그인 버전에 대해 **Panorama** > 플러그인 및 지금 확인을 선택합니다.
2. 최신 버전의 SD-WAN 플러그인을 다운로드하고 설치합니다.

STEP 3 | 새 플러그인 버전이 성공적으로 설치되면 Panorama 대시보드를 보고 일반 정보 위젯에서 SD-WAN ####이 업그레이드한 SD-WAN 플러그인 버전을 표시하는지 확인합니다.

업그레이드를 위한 CLI 명령

업그레이드 작업에 CLI 명령 사용

다음 CLI 명령을 사용하여 업그레이드 작업을 수행합니다.

원하는 경우...	다음을 사용합니다...
방화벽의 현재 버전 확인	
• 방화벽 소프트웨어 및 콘텐츠의 현재 버전을 확인하십시오.	`show system info`
사용 가능한 동적 업데이트에 액세스하고 방화벽의 콘텐츠 버전을 업그레이드합니다.	
• Palo Alto Networks 서버에서 직접 동적 업데이트의 사용 가능한 콘텐츠 버전을 확인하십시오.	`### ##### ## ##`
• 방화벽에서 직접 동적 업데이트의 사용 가능한 콘텐츠 버전을 확인합니다.	`### ##### ## ##`
• 콘텐츠 버전을 방화벽에 직접 다운로드합니다.	`### ##### #### ## <content version>`
• 콘텐츠 버전을 설치합니다.	`### ##### ## ## <content version>`

원하는 경우...	다음을 사용합니다...
사용 가능한 소프트웨어 버전에 액세스하고 방화벽을 업그레이드하십시오.	
• 다운로드할 수 있는 사용 가능한 소프트웨어 버전을 확인하십시오.	### ##### ## ##
• 방화벽에 로드된 사용 가능한 버전을 확인합니다.	### ##### ## ##
• 특정 버전의 소프트웨어를 다운로드합니다.	### ##### #### ## ## **<version>**
• 특정 다운로드 작업의 상태를 확인합니다.	**Show job id <jobid>**
• 다운로드한 소프트웨어를 설치합니다.	### ##### ## ## **10.1.0** ##
• 방화벽을 다시 시작합니다.	### ### ##

방화벽에 사용 가능한 소프트웨어 패치에 액세스:

패치 기능은 현재 미리보기 모드로 제공됩니다. 이 기능은 전체 지원이 제공되지 않습니다.

원하는 경우...	다음을 사용합니다...
• 다운로드할 수 있는 사용 가능한 소프트웨어 패치를 확인합니다.	## ### ## ##
• 현재 설치된 방화벽 버전에 사용 가능한 패치를 확인합니다.	### ## ## ##
• 특정 패치 버전을 다운로드합니다.	## ### ## #### ## **<version>**
• 특정 패치 버전에 대한 자세한 정보를 확인합니다.	### ## ## ## ## **<version>**
• 다운로드한 패치를 설치합니다.	### ## ## ## ## **<version>**
• 설치된 패치를 적용합니다.	## ### ## ##

업그레이드를 위한 API

업그레이드 작업에 API 사용

다음 CLI 명령을 사용하여 업그레이드 작업을 수행합니다.

원하는 경우...	다음을 사용합니다...
방화벽의 현재 버전 확인	
• 방화벽 소프트웨어 및 콘텐츠의 현재 버전을 확인하십시오.	**https://firewall/api/?type=op&cmd=<request><system><software><chec check></software></system>**
사용 가능한 동적 업데이트에 액세스하고 방화벽의 콘텐츠 버전을 업그레이드합니다.	
• Palo Alto Networks 서버에서 직접 동적 업데이트의 사용 가능한 콘텐츠 버전을 확인하십시오.	**https://firewall/api/?type=op&cmd=<request><content><upgrade><chec check></upgrade></content></request>**
• 방화벽에서 직접 동적 업데이트의 사용 가능한 콘텐츠 버전을 확인합니다.	**https://firewall/api/?type=op&cmd=<request><content><upgrade><info info></upgrade></content></request>**
• 최신 콘텐츠 버전을 방화벽에 직접 다운로드합니다.	**https://firewall/api/?type=op&cmd=<request><content><upgrade><down latest></download></upgrade></content></request>**
• 특정 콘텐츠 버전을 방화벽에 직접 다운로드합니다.	**https://firewall/api/?type=op&cmd=<request><content><upgrade><down ## ## ## ### #####.<file></download></upgrade></content></request>**
• 콘텐츠 버전을 설치합니다.	**https://firewall/api/?type=op&cmd=<request><content><upgrade><inst <content version></version></install></upgrade></content></request>**
사용 가능한 소프트웨어 버전에 액세스하고 방화벽을 업그레이드하십시오.	

원하는 경우...	다음을 사용합니다...
• 다운로드할 수 있는 사용 가능한 소프트웨어 버전을 확인하십시오.	**https://firewall/api/?type=op&cmd=<request><system><software><info info></software></system></request>**
• 방화벽에 로드된 사용 가능한 버전을 확인합니다.	**https://firewall/api/?type=op&cmd=<request><system><software><chec check></software></system></request>**
• 특정 버전의 소프트웨어를 다운로드합니다.	**https://firewall/api/?type=op&cmd=request><system><software><downl version></download></software></system></request>**
• 특정 다운로드 작업의 상태를 확인합니다.	**https://firewall/api/?type=op&cmd=<show><jobs></jobs></show>**
• 다운로드한 소프트웨어를 설치합니다.	**https://firewall/api/?type=op&cmd=<request><system><software><inst version></install></software></system></request>**
• 방화벽을 다시 시작합니다.	**https://firewall/api/?type=op&cmd=<request><restart><system></system></restart></request>**