BPA 사용 설명서 OS 업그레이드 v5.1

소개

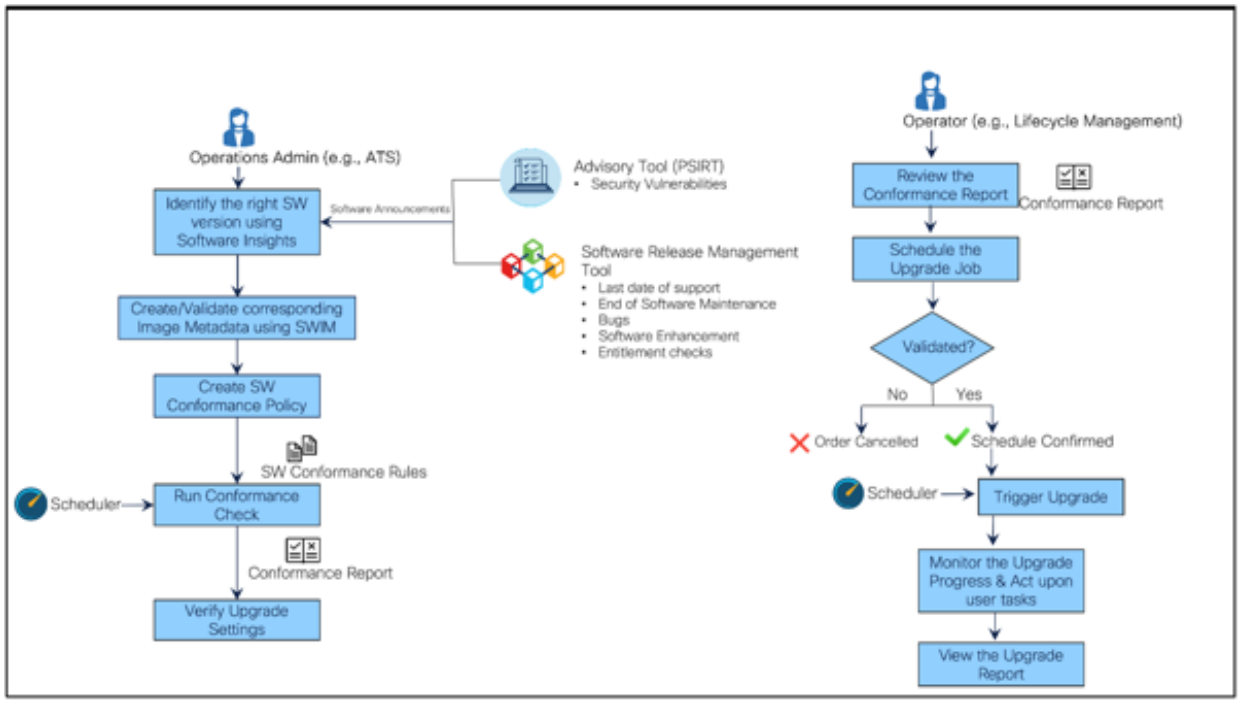
BPA(Business Process Automation)의 OS 업그레이드 애플리케이션은 여러 도메인에서 소프트웨어 적합성 및 네트워크 디바이스 업그레이드를 수행할 수 있는 포괄적인 자동화 솔루션을 제공합니다. 여러 도메인 컨트롤러를 지원하고 통합 사용자 환경을 제공합니다. 기본 OS(운영 체제) 업그레이드와 SMU(Software Maintenance Update) 또는 RPM(RPM Package Manager) 패치 업데이트를 모두 지원합니다.

주요 기능

OS 업그레이드 애플리케이션은 다음과 같은 주요 자동화 기능을 제공합니다.

- 소프트웨어 이미지 관리: 소프트웨어 업그레이드 프로세스에서 사용할 소프트웨어 이미지 및 해당 버전(모든 공급업체)의 중앙 집중식 목록
- 소프트웨어 인사이트: 네트워크 자산에 노출된 소프트웨어 위험 및 취약성을 파악하고 공급업체에서 권장하는 소프트웨어 버전에 대한 통찰력 확보
- 소프트웨어 적합성: 소프트웨어 이미지를 업그레이드해야 하는 네트워크의 모든 자산 식별
- MOP(프로시저 정의 업그레이드 방법): 각 벤더 디바이스 모델 또는 제품군에 대한 사전 및 사후 확인과 함께 업그레이드 프로세스를 사전 정의
- 업그레이드 작업: 모든 지역에 걸쳐 유지 보수 기간 동안 비준수 자산의 업그레이드 일정을 수립하고, 업그레이드 진행 상황을 모니터링하고, 자세한 보고서를 확보합니다.

엔드 투 엔드 흐름



엔드 투 엔드 흐름

위 그림에는 서로 다른 두 사용자 페르소나에 대한 OS 업그레이드 애플리케이션 통화 흐름이 나와 있습니다. OOB(Out-of-the-Box) 기능을 제공하는 운영 관리자 및 네트워크 운영자 OOB 역할 및 해당 권한에 대한 자세한 내용은 액세스 제어를 참조하십시오.

페르소나	설명	작업 공간
운영 관리자	네트워크 자산에 영향을 미치는 소프트웨어 취약성(예: 자문, 버그, 단종 게시물)을 검색합니다.	BPA: OS 업그레이드/소프트웨어 이미지 관리/자문
운영 관리자	영향을 받는 소프트웨어 버전 및 영향을 받는 자산을 식별하고 벤더가 제공한 제안을 기반으로 올바른 대	BPA: OS 업그레이드/소프트웨어 이미지 관리/통찰력

페르소나	설명	작업 공간
	상 버전을 결정합니다.	
운영 관리자	필요한 소프트웨어 이미지 메타데이터를 생성합니다.	BPA: OS 업그레이드/소프트웨어 이미지 관리/소프트웨어 이미지
운영 관리자	영향을 받는 디바이스 모델에 대한 의도를 생성하고 온디맨드 또는 예약된 정책 실행 시 정책을 실행합니다.	BPA: OS 업그레이드/소프트웨어 적합성 정책
운영 관리자	비적합 또는 영향을 받는 자산 식별	BPA: OS 업그레이드/소프트웨어 적합성/결과 보기
운영 관리자	업그레이드 MOP에 따라 업그레이드 정책을 만들거나 수정합니다. 여기에는 사전 확인 및 사후 확인, 배포 또는 활성화를 위한 워크플로, 트래픽 전환 또는 전환, 단일 또는 다중 단계 업그레이드를 위한 롤백 사전 정의가 포함됩니다	BPA: OS 업그레이드/업그레이드 정책
네트워크 운영자	모든 비준수 디바이스를 업그레이드하도록 작업 예약	BPA: OS 업그레이드/업그레이드 작업
네트워크 운영자	업그레이드 작업 진행률 모니터링	BPA: OS 업그레이드/업그레이드 작업/작업 세부 정보
네트워크 운영자	사용자 작업(있는 경우)에 대한 작업을 수행하여 문제를 정리하고 프로세스를 다음 단계로 진행합니다.	BPA: OS 업그레이드/업그레이드 작업/작업 세부 정보

가치 제안

OS 업그레이드 애플리케이션에서는 다음과 같은 부가 가치를 제공합니다.

- API - OSS(Northbound Operations Support Systems) 및 BSS(Business Support Systems)에서 보다 용이한 서비스 사용을 지원하는 첫 번째 접근 방식
- 다양한 도메인 컨트롤러로 관리되는 네트워크 전반에서 네트워크 디바이스의 소프트웨어 적합성을 신속하게 검증
- 운영자는 일괄 처리, 대기열 처리 및 예약 메커니즘을 사용하여 업그레이드 작업을 더 잘 제어할 수 있습니다
- 업그레이드 작업은 검토를 위해 일찍 생성하고 나중에 실행할 수 있습니다.
- 최소~0개의 장애로 더 빠르고 더 나은 처리량을 실현하는 대기열 처리 메커니즘
- 자동 컨피그레이션 백업 사전 업그레이드, 장애 발생 시 원활한 복원 지원
- 사전/사후 검사 실행, 서비스 중단 없이 성공적인 업그레이드 보장
- 사전 및 사후 검증 검사, 배포 또는 활성화, 트래픽 전환 또는 취소, 롤백 프로세스를 통해 업그레이드 MOP를 사전 정의할 수 있는 유연성을 제공하는 정책 중심의 접근 방식으로, 필요에

따라 사용자 정의할 수 있습니다.

지원되는 컨트롤러 및 디바이스 플랫폼

다음 플랫폼은 BPA에서 검증되었으며 지원되는 OOB입니다. 그러나 프레임워크는 일반적이며 새로운 플랫폼으로 확장할 수 있습니다. 추가 플랫폼에 대한 OOB 지원은 우선 순위를 기준으로 향후 릴리스에서 제공될 예정입니다.

도메인 컨트롤러	디바이스 플랫폼
Cisco Catalyst Center v2.3.7.5-70434	- Cisco IOS, Cisco IOS-XE
vManage v20.12.4	- Cisco IOS, Cisco IOS-XE 참고: 원격 서버 배포가 작동하려면 디바이스가 v17.9.x 이상이어야 합니다.
Nexus NDFC(Dashboard Fabric Controller) v12.1.2e 및 v12.2.2	- Cisco-NXOS(N9k)
FMC(Firewall Management Center) v7.4.1	- Firepower 3140
NSO(Network Services Orchestrator) v6.3	- Cisco-IOSXR(NCS540, NCS560, ASR9K) - Cisco-NXOS(N9K) 참고: NX-OS NED v5.25.17 이상이 필요합니다.
CNC(Cross Network Controller) v6.0	- Cisco-IOSXR(NCS540, ASR9K)
ANSIBLE v2.9.18(AWX - 17.1.0)	- Cisco-IOSXR(NCS540, ASR9K)
Direct-to-Device(Telnet(Teletype Network) 및 SSH(Secure Shell) 사용)	- Cisco-IOSXR(NCS540, ASR9K)

새로운 기능

이 릴리스의 OS 업그레이드 활용 사례에 사용할 수 있는 증분 기능에 대해서는 BPA 릴리스 정보를 참조하십시오.

사전 요구 사항

OS 업그레이드 애플리케이션을 사용하기 전에 다음 필수 조건을 충족해야 합니다.

- OS 업그레이드, 백업 및 복원, 스케줄러 서비스 및 모든 필수 플랫폼 서비스 또는 컨트롤러 에이전트 서비스가 실행 중입니다.
- 필수 객체(예: 워크플로, 프로세스 템플릿, 기본 업그레이드 정책 등)가 로드됩니다
- 필요한 컨트롤러가 추가되고 디바이스가 성공적으로 동기화됩니다. 자세한 내용은 지원되는 컨트롤러 및 디바이스 플랫폼을 참조하십시오

OS 업그레이드 애플리케이션 작업

OS 업그레이드 애플리케이션은 다음 구성 요소로 구성됩니다.

- 소프트웨어 이미지 관리(SWIM)
- 이미지 배포 서버 관리
- 소프트웨어 인사이트
- 소프트웨어 적합성
- 업그레이드 정책
- 업그레이드 작업
- 설정

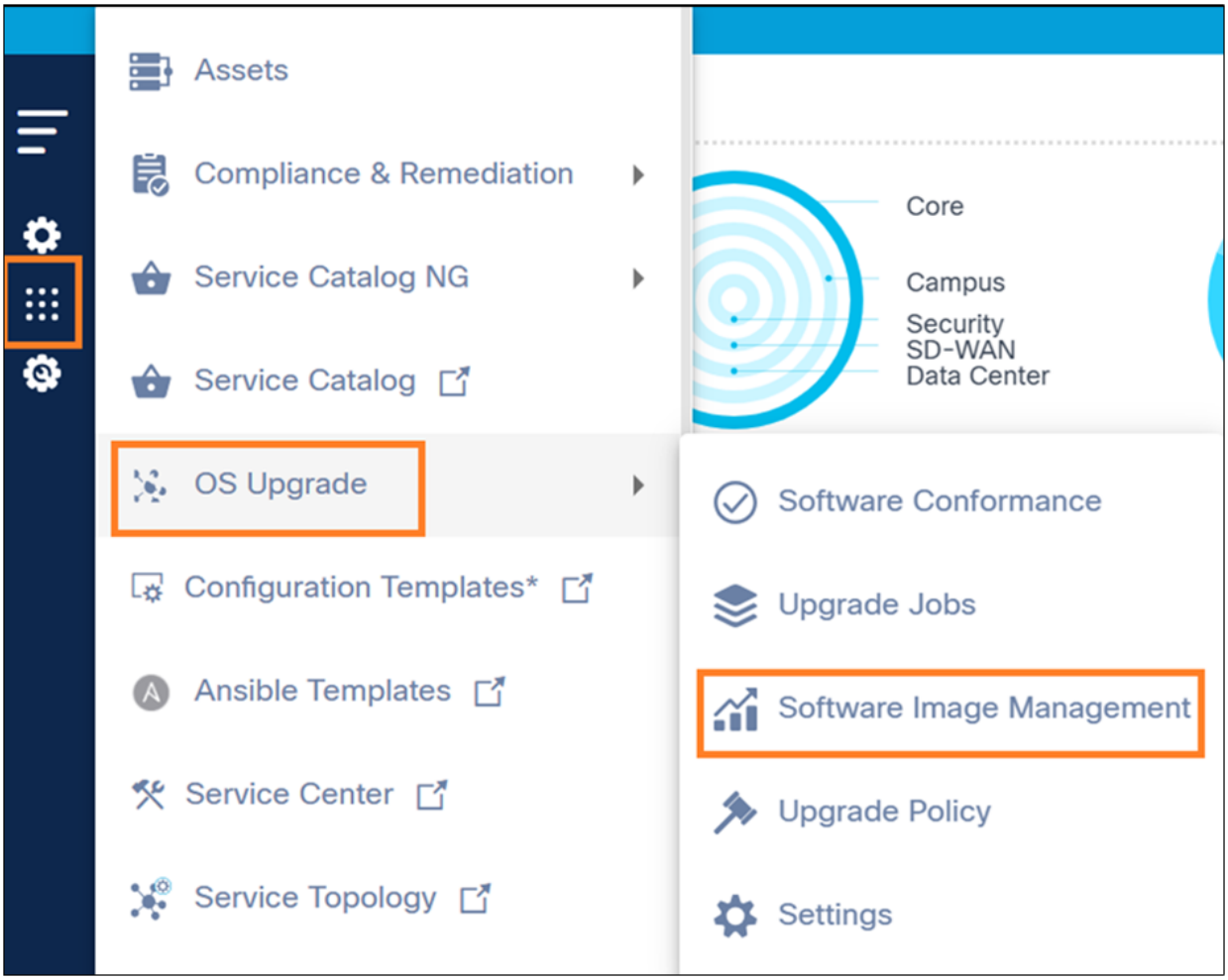
소프트웨어 이미지 관리

SWIM 구성 요소를 사용하면 운영 사용자가 OOB 이미지 관리를 지원하지 않는 NSO, ANSIBLE, CNC, FMC, Direct-to-Device 등의 컨트롤러에 대한 소프트웨어 이미지 세부 정보를 유지 관리할 수 있습니다. 또한 vManage, NDFC, Cisco Catalyst Center와 같은 컨트롤러에서 유지 관리하는 소프트웨어 이미지 세부 정보를 나열하며, 모든 도메인 컨트롤러에서 유지 관리되는 중앙 집중식 소프트웨어 목록을 제공합니다. 소프트웨어 이미지와 이미지 배포 서버는 SWIM 모듈 내의 두 가지 주요 하위 구성 요소입니다.

소프트웨어 이미지

Software Images 페이지에 액세스하려면

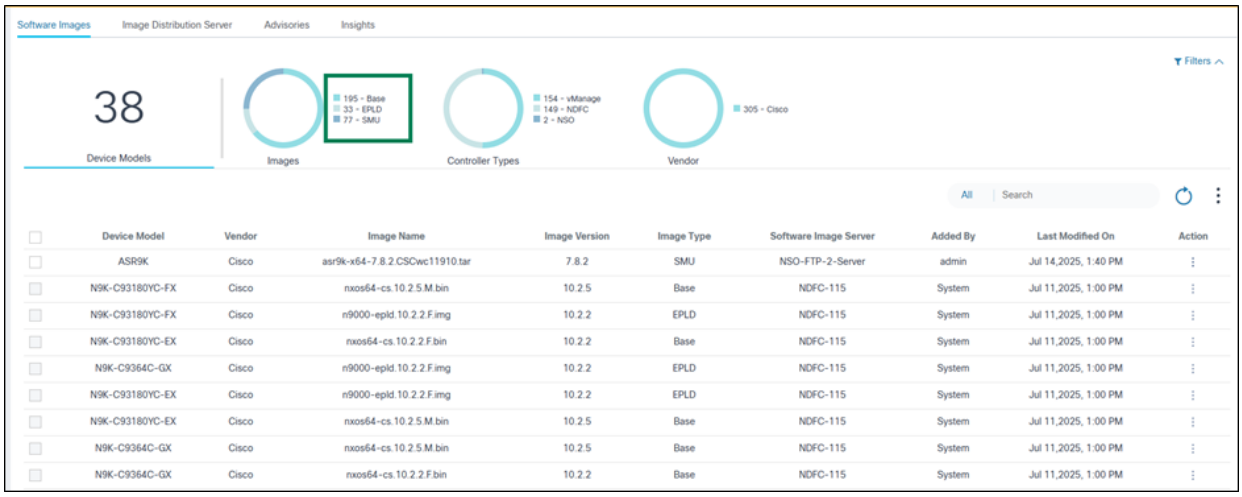
1. 소프트웨어 이미지 관리에 액세스할 수 있는 자격 증명을 사용하여 BPA에 로그인합니다.



소프트웨어 이미지 관리 탐색

2. OS Upgrade > Software Image Management를 선택합니다.

Image Management(이미지 관리) 페이지에는 다음 탭이 표시됩니다. 소프트웨어 이미지, 이미지 배포 서버, 자문 및 인사이트.



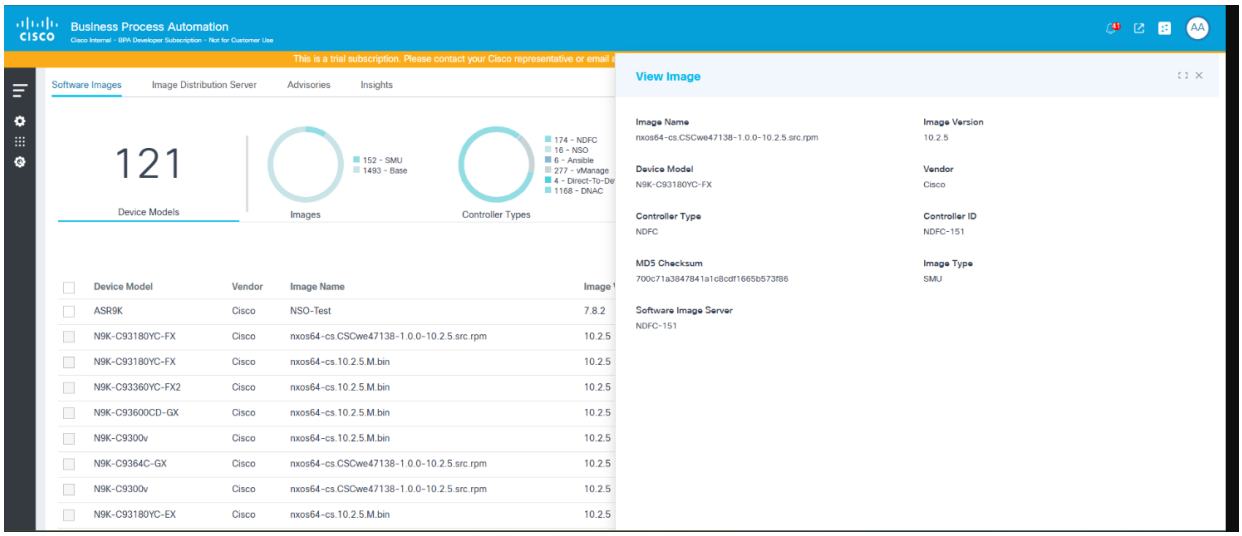
소프트웨어 이미지 탭

Software Images(소프트웨어 이미지) 탭에는 다음이 포함되어 있습니다.

- 다음을 제공하는 분석 섹션이 맨 위에 표시됩니다.
    - 총 장치 모델 및 관련 소프트웨어 이미지 수
    - 유형(예: 기본, SMU)에 따라 이미지를 필터링할 수 있는 이미지 빠른 필터 숫자는 각 이미지 유형과 연결된 이미지의 총 수를 나타냅니다
    - 이미지가 호스팅되는 컨트롤러 유형(예: Cisco Catalyst Center, vManage, NSO 또는 NDFC, Direct-to-Device, CNC, ANSIBLE, FMC)에 따라 이미지를 필터링할 수 있는 컨트롤러 유형 빠른 필터 숫자는 각 컨트롤러 유형과 연결된 총 이미지 수를 나타냅니다
    - 소프트웨어를 게시한 공급업체를 기준으로 이미지를 필터링할 수 있는 공급업체 빠른 필터
- 추가 옵션 아이콘은 다음 기능을 제공합니다.
    - 이미지 세부 정보 추가: 새 이미지 메타데이터 추가
    - 대량 업로드: 이미지 메타데이터를 .csv 형식으로 대량 업로드
    - 이미지 동기화: 컨트롤러(예: Cisco Catalyst Center, vManage, NDFC, FMC)에서 이미지 메타데이터 동기화
    - 모두 삭제: 선택한 이미지의 대량 삭제

참고: NSO, ANSIBLE, CNC 및 Direct-to-Device 컨트롤러에만 이미지 세부사항의 추가, 삭제 및 대량 업로드가 허용됩니다.

- 검색 필터는 이미지 검색에 사용할 수 있으며 다음과 같은 전용 검색 필터를 포함합니다.
    - 모두: 모든 필드 검색
    - 이미지 이름: 특정 이미지 이름으로 이미지 검색
    - 디바이스 모델: 지정된 모델이 있는 이미지 검색
    - 이미지 버전: 특정 소프트웨어 버전의 이미지 검색
    - 소프트웨어 이미지 서버: 특정 이미지 서버와 연결된 이미지 검색
- Refresh(새로 고침) 아이콘은 페이지를 새로 고치고 선택한 필터를 지웁니다.
- 기존 이미지는 다음 열이 있는 그리드 테이블에 표시됩니다.
    - 디바이스 모델: 이미지 세부 정보를 적용할 수 있는 장치 모델
    - 공급업체: 소프트웨어 이미지를 게시하는 벤더
    - 이미지 이름: 이미지의 파일 이름
    - 이미지 버전: 이미지의 소프트웨어 버전
    - 이미지 유형: 이미지 유형(예: 베이스, SMU, EPLD(Electronic Programmable Logic Device)) 결정
    - 소프트웨어 이미지 서버: 현재 이미지가 있는 이미지 서버
    - 추가자: 이미지 메타데이터를 추가한 사용자
    - 마지막 수정 날짜: 마지막 이미지 세부 정보 업데이트의 타임스탬프입니다.
    - 작업: 행별 작업(예: 편집, 삭제)을 선택할 수 있는 추가 옵션 아이콘을 제공합니다.
- 각 열 머리글을 클릭하여 이미지 정렬



이미지 보기

- 행을 클릭하면 이미지 보기 창이 열립니다

소프트웨어 이미지 메타데이터 동기화

소프트웨어 이미지의 온디맨드 동기화를 수행하려면

이미지 동기화

1. More Options(추가 옵션) 아이콘 > Sync Images(이미지 동기화)를 선택합니다. vManage, Cisco Catalyst Center, NDFC 및 FMC의 이미지 메타데이터 세부 정보는 BPA에서 검색 및 유지됩니다.

참고: FMC 컨트롤러의 경우 동기화가 실행될 때마다 기존 데이터가 보존됩니다. 새 이미지만 추가됩니다.

---

2. FMC 컨트롤러의 이미지 이름에 "FTD" 또는 "Firepower Threat_Defense"라는 단어가 포함된 경우 해당 이미지의 deviceModel은 FTD로 매핑됩니다.

또는

FMC 컨트롤러의 이미지 이름에 "FMC", "FW_Mgmt_Center" 또는 "Firewall_Management_Center"가 포함된 경우 해당 이미지의 deviceModel이 FMC로 매핑됩니다.

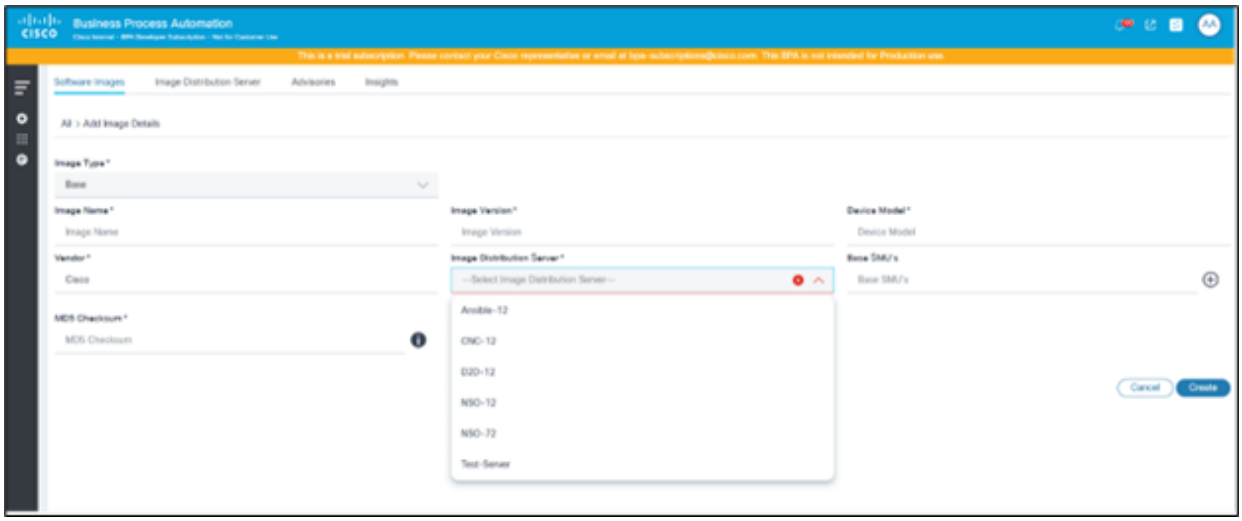
참고: FMC는 모델 정보를 이미지 메타데이터와 연결하지 않습니다. 동기화가 완료되면 각 이미지 메타데이터를 편집하고 필요에 따라 모델을 업데이트합니다. 모델 업데이트 없이는 FMC 업그레이드 프로세스가 예상대로 작동하지 않습니다.

---

3. 처음에는 vManage 원격 서버의 이미지에 UUID(Universally Unique Identifier)가 동기화 작업 후 Version 열에 매핑되어 있습니다. 운영자는 필요한 원격 서버 메타데이터를 수동으로 편집하고 적절한 이미지 버전으로 업데이트해야 합니다. 이 매핑을 수행하지 않으면 다른 OS 업그레이드 구성 요소(예: 소프트웨어 적합성, 업그레이드 정책, 업그레이드 작업 등)가 예상대로 작동하지 않습니다.
4. 정기적으로 자동 SWIM 메타 데이터 동기화를 예약하려면 구축 컨피그레이션을 참조하십시오.

소프트웨어 이미지 메타데이터 추가

1. More Options(추가 옵션) 아이콘 > Add Image Details(이미지 세부 정보 추가)를 선택합니다. Add Image Details(이미지 추가 세부 정보) 페이지가 표시됩니다.



이미지 세부 정보 추가

2. 다음 필드에 정보를 입력합니다.

- 이미지 유형: 이미지 유형(예: 베이스, SMU, EPLD)
- 이미지 이름: 이미지 파일의 이름; 사용자는 Name 필드에 이미지의 상대 경로 또는 절대 경로를 입력할 수 있습니다. 사용자가 절대 경로를 제공하면 해당 경로에서 직접 이미지를 가져옵

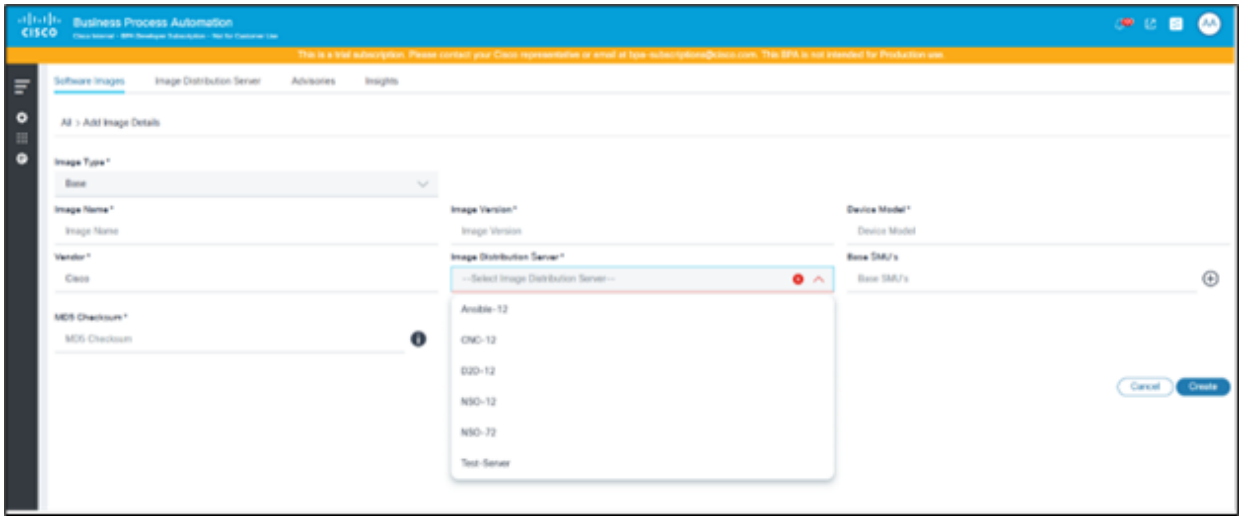
니다. 사용자가 상대 경로를 제공하는 경우, 시스템은 배포 중에 저장소 서버에 정의된 기본 경로를 추가하여 전체 경로를 확인합니다
- 이미지 버전: 이미지의 소프트웨어 버전
- 디바이스 모델: 이미지가 태깅되는 디바이스 모델

참고: 장치 모델은 해당 장치에 대해 CNC, NSO, Direct-To-Device 또는 ANSIBLE 컨트롤러에서 제공하는 모델 정보와 일치해야 합니다.

- 공급업체: 이미지를 게시한 공급업체 또는 제공업체 기본값은 Cisco이지만 필요에 따라 변경할 수 있습니다
- 이미지 배포 서버: Image Name(이미지 이름) 필드에 표시된 소프트웨어 파일을 호스팅하는 이미지 배포 서버를 선택합니다. 이미지 배포 서버를 선택하면 이미지 배포 서버 내에 정의된 지정된 컨트롤러 유형과 연결된 모든 컨트롤러 ID에 대해 이미지가 생성됩니다. 사용자가 이미지 배포 서버 아래에 컨트롤러 인스턴스를 추가하거나 제거하는 경우 해당 컨트롤러 인스턴스에 대한 해당 소프트웨어 이미지가 추가되거나 제거됩니다.
- 기본 SMU: 기본 골든 이미지에 있는 SMU 이 옵션은 이미지 유형이 베이스인 경우에만 적용됩니다
- MD5 체크섬: 확인을 위한 이미지 MD5 체크섬

3. Create(생성)를 클릭합니다. 진행률 알림과 확인 메시지가 표시됩니다.

참고: 업그레이드 정책에서 사용하기 전에 브리지 SMU에 대한 이미지 메타데이터를 추가해야 합니다. Bridge SMU를 추가하려면 Image Type 드롭다운 목록에서 SMU를 선택합니다.



브리지 SMU 이미지 메타데이터 추가

소프트웨어 이미지 메타데이터 벌크 업로드

	A	B	C	D	E	F	G
1	Device Model	Vendor	Image Name	Version	Image Type	Image Distribution Server	MD5 Checksum
2	NCS-540	Cisco	test22	1.1.1	Base	Ansible server	680fcd5f9f3558d6fd581edc0835ce2a
3	NCS-540	Cisco	test23	2.2.2	Base	Ansible server	b4eceaf95e419c63d8da124d214deaaf
4	NCS-540	Cisco	test33	2.2.2	Base	Ansible server	b4eceaf95e419c63d8da124d214deaaf
5	NCS-540	Cisco	test421	2.2.2	Base	Ansible server1	b4eceaf95e419c63d8da124d214deaaf

이미지 정보가 포함된 샘플 CSV 파일

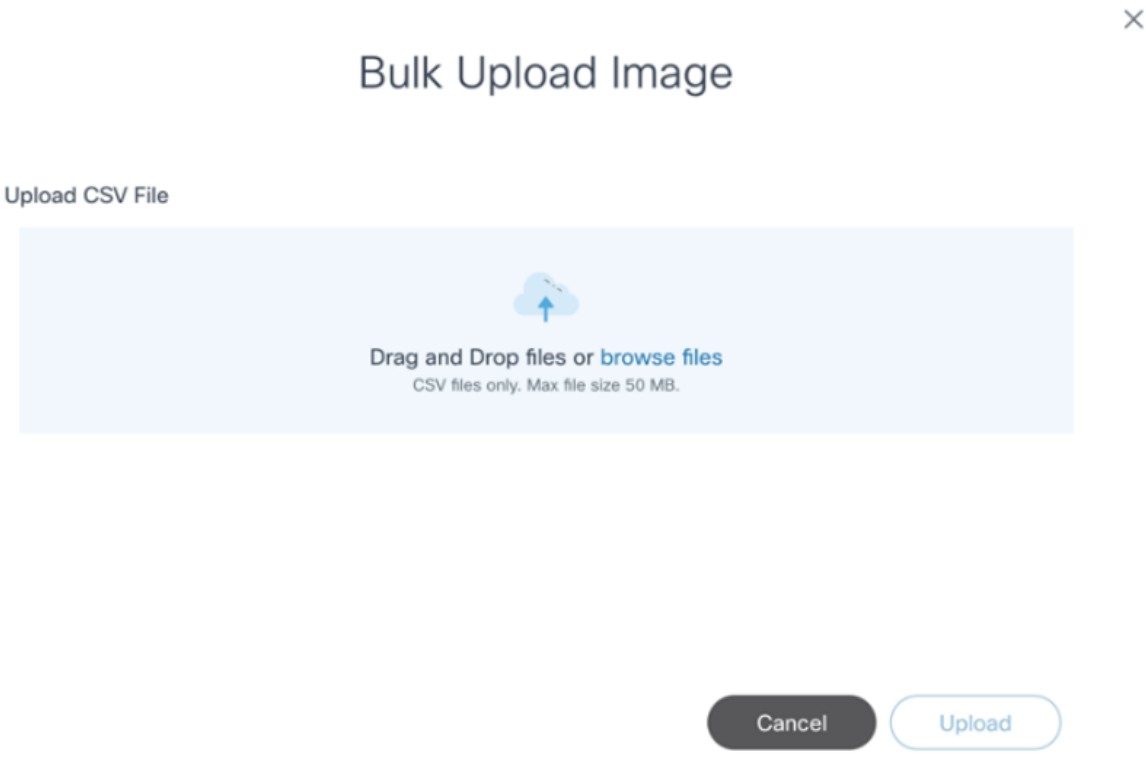
1. 필요한 이미지 세부 정보 및 다음 열 이름이 포함된 .csv 파일을 준비합니다.

- 이미지 이름
- 버전
- 디바이스 모델
- 공급업체
- 이미지 유형

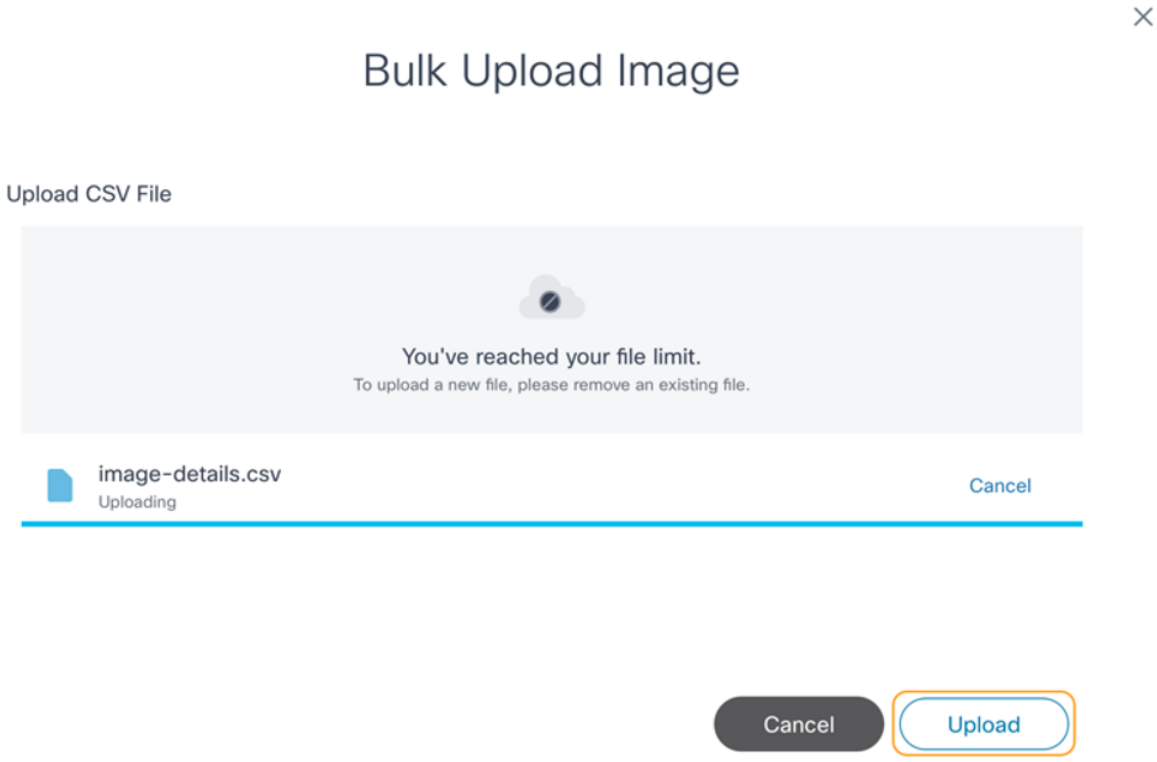
참고: Base, SMU 및 EPLD 값만 지원됩니다.

- 이미지 배포 서버
- MD5 체크섬

2. More Options(추가 옵션) 아이콘 > Bulk Upload(대량 업로드)를 선택합니다. Bulk Upload Image(이미지 대량 업로드) 창이 열립니다.

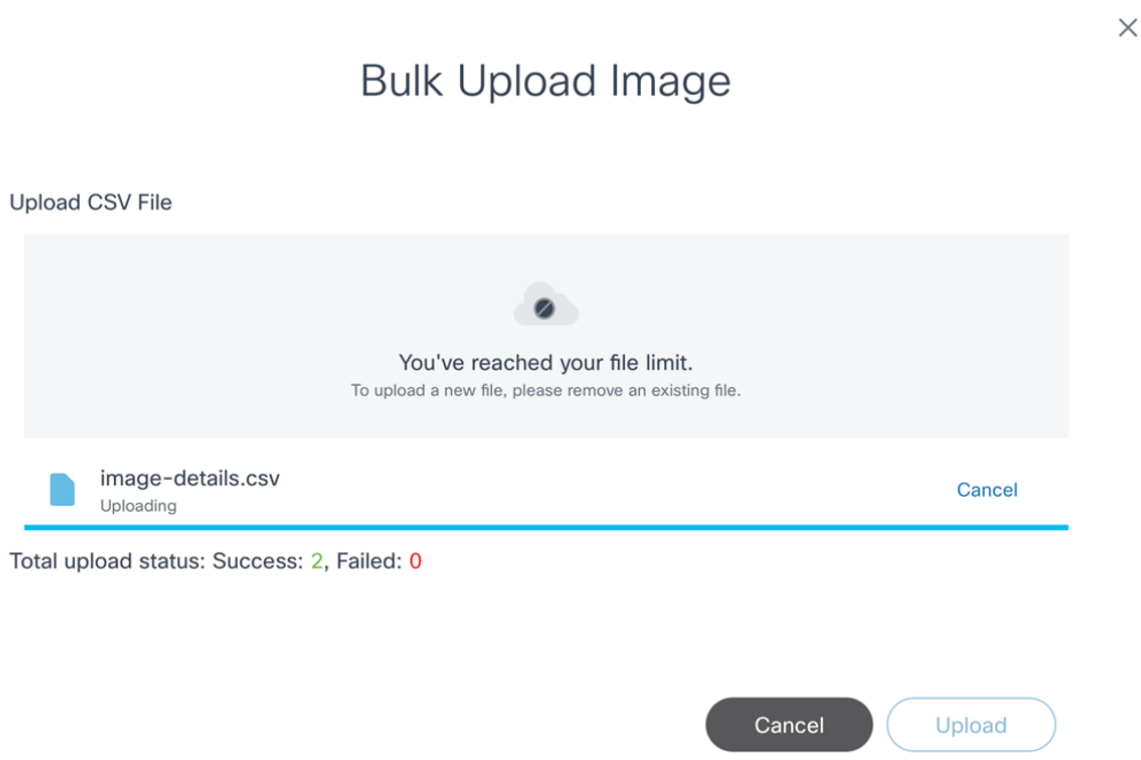


이미지 벌크 업로드



대량 업로드 이미지 - CSV 업로드

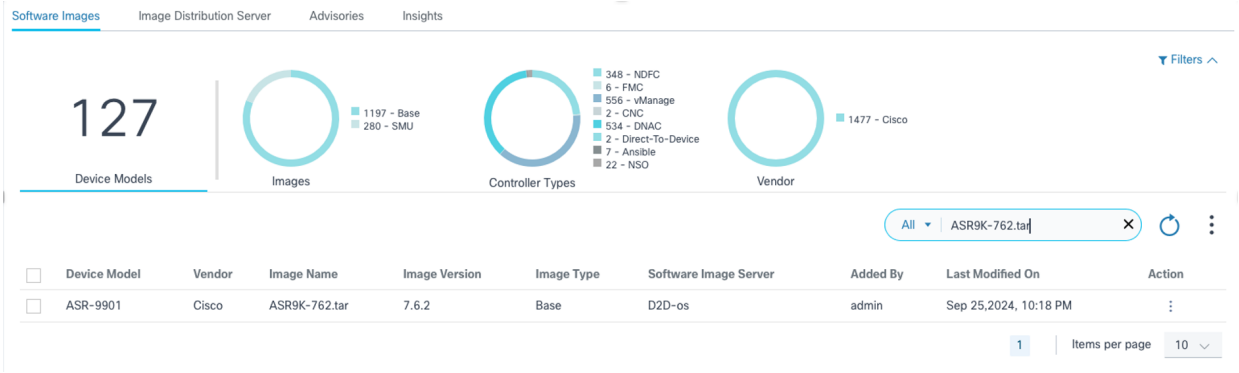
3. 준비된 .csv 파일을 선택하고 Upload(업로드)를 클릭합니다. .csv의 이미지 세부사항이 검증되고 처리됩니다. 파일이 업로드되면 최종 대량 업로드 상태가 표시됩니다.



대량 이미지 업로드 성공 상태

참고: 데이터 검증 오류(예: 중복 레코드 또는 잘못된 매개변수)가 발생하면 오류 메시지가 Bulk Upload Image(이미지 대량 업로드) 창에 그리드로 표시됩니다. 사용자는 .csv 파일의 값을 수정하고 다시 업로드할 수 있습니다.

기존 소프트웨어 이미지 메타데이터 편집

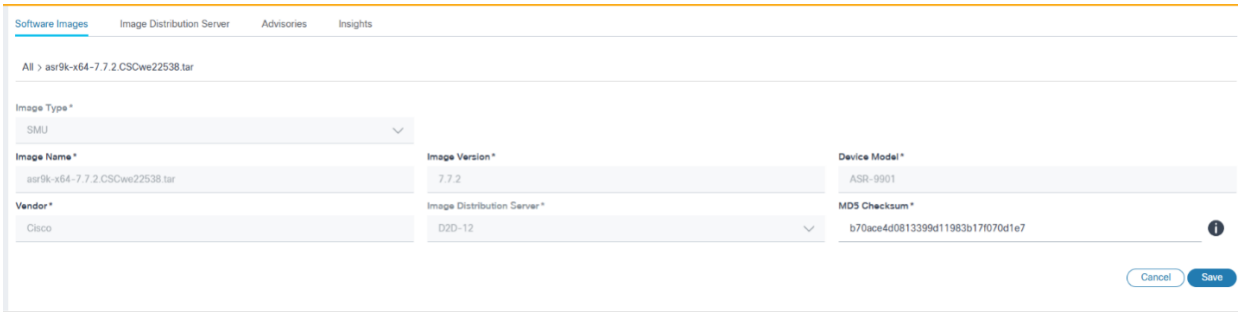


소프트웨어 이미지 메타데이터에서 검색

1. 검색 필터를 사용하여 업데이트해야 하는 이미지를 찾습니다.

편집

2. 원하는 이미지의 Action(작업) 열에서 More Options(추가 옵션) 아이콘 > Edit(편집)를 선택합니다.



소프트웨어 이미지 편집

3. 필수 매개변수를 업데이트하고 저장을 눌러 변경 사항을 저장하거나 취소를 눌러 변경 사항을 취소합니다. 진행률 알림이 표시되고 이미지 업데이트에 대한 확인 메시지가 표시됩니다.

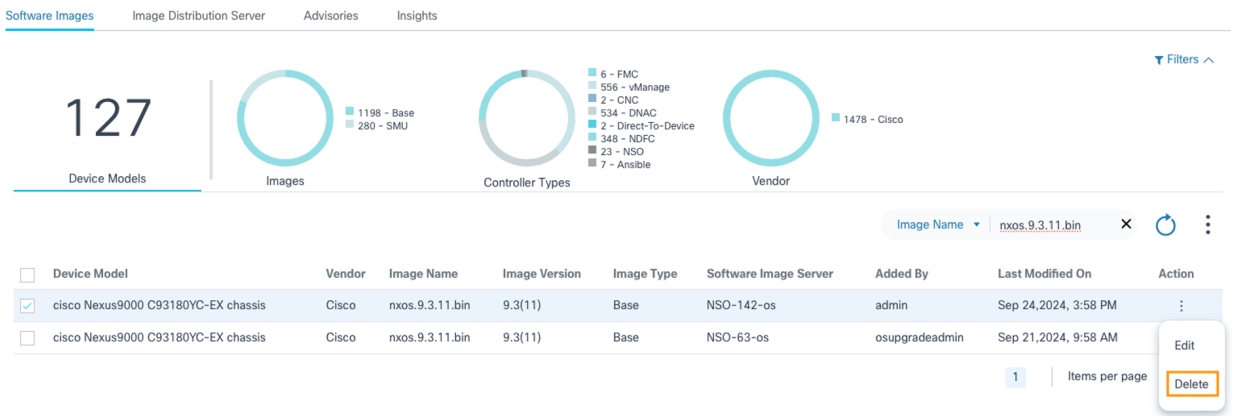
참고: 다음 목록에 유의해야 합니다.

- CNC, NSO, D2D, ANSIBLE, FMC 및 vManage 컨트롤러에서 수정 가능(원격 서버 이미지 메타데이터에만 적용)
- 장치 모델 업데이트는 vManage 원격 서버 이미지에 대해서만 지원됩니다
- vManage 원격 서버 이미지 메타데이터에 대해서는 Software Version 필드만 업데이트할 수 있습니다
- vManage 이미지의 경우 사용자는 컨트롤러 인스턴스 대신 소프트웨어 이미지 서버를 볼 수 있습니다

소프트웨어 이미지 메타데이터 삭제

소프트웨어 이미지 메타데이터에서 검색

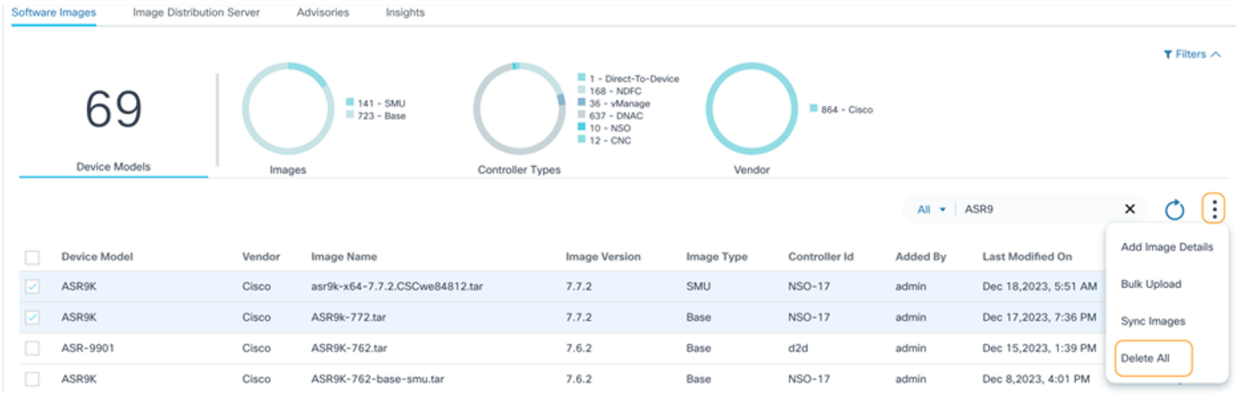
1. 원하는 이미지를 찾으려면 Search 필드를 사용합니다.



삭제

2. 원하는 이미지의 Action(작업) 열에서 More Options(추가 옵션) 아이콘 > Delete(삭제)를 선택하여 이미지를 삭제합니다.

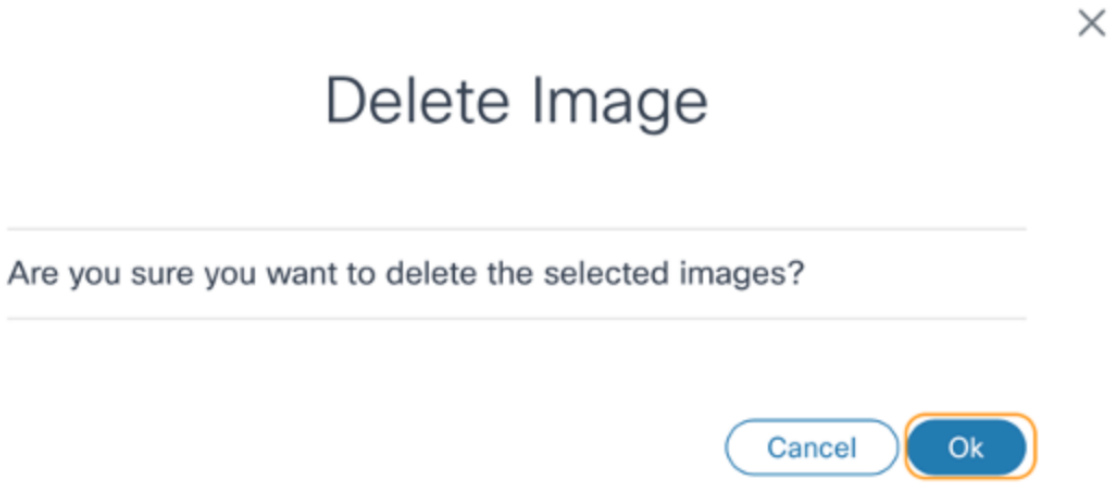
또는



모두 삭제

여러 이미지를 삭제하려면 원하는 이미지를 선택하고 추가 옵션 아이콘 > 모두 삭제를 선택합니다.

확인 메시지가 표시됩니다.



확인

3. OK(확인)를 클릭합니다. 진행 알림과 확인 메시지가 표시됩니다.

참고: 다음 목록에 유의해야 합니다.

- 이미지 메타데이터는 NSO, ANSIBLE, Direct-to-Device 및 CNC 컨트롤러에만 추가할 수 있습니다. 다른 모든 엔터프라이즈 컨트롤러의 경우 내장된 SWIM 기능이 활용되며, 각 컨트롤러에서 이미지가 검색됩니다
- NSO, ANSIBLE, Direct-to-Device 및 CNC 컨트롤러의 이미지 서버에서는 이미지 검색 기능이 지원되지 않습니다.
- 기본적으로 vManage 원격 서버 이미지 메타데이터는 버전 매개 변수 사후 동기화에 대한 UUID를 포함합니다. 사용자는 메타데이터를 수정하고 해당 버전으로 UUID를 업데이트해야 합니다. 해당 이미지 버전은 vManage 컨트롤러에서 식별하거나 이미지가 있는 디바이스에 로그인하여 식별할 수 있습니다.

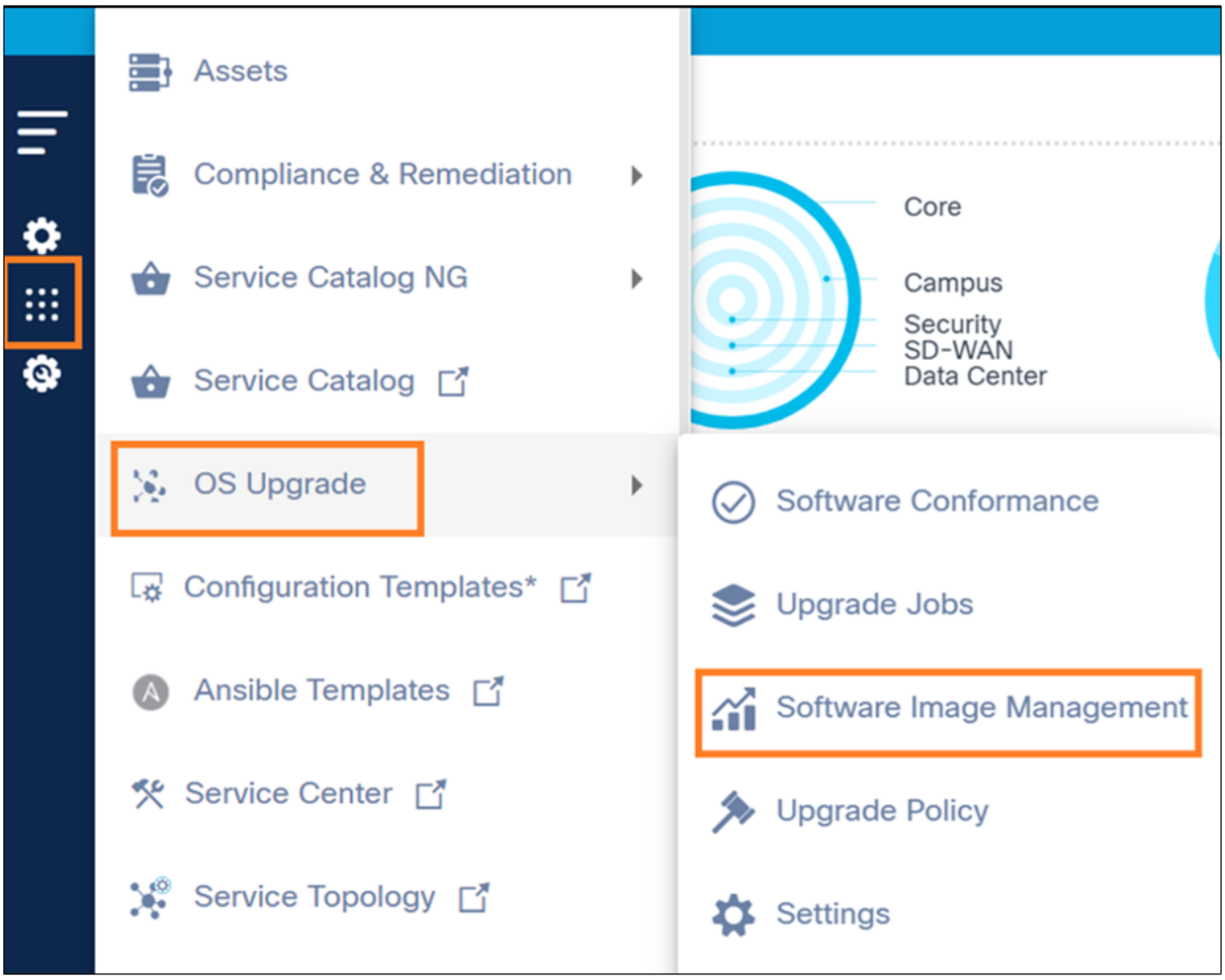
이미지 배포 서버 관리

이미지 배포 서버

이 구성 요소를 사용하면 운영 사용자가 OOB 이미지 저장소 관리를 지원하지 않는 CNC, NSO, ANSIBLE, FMC 및 Direct-To-Device 컨트롤러에 대한 이미지 저장소 서버 세부 정보를 유지 관리할 수 있습니다.

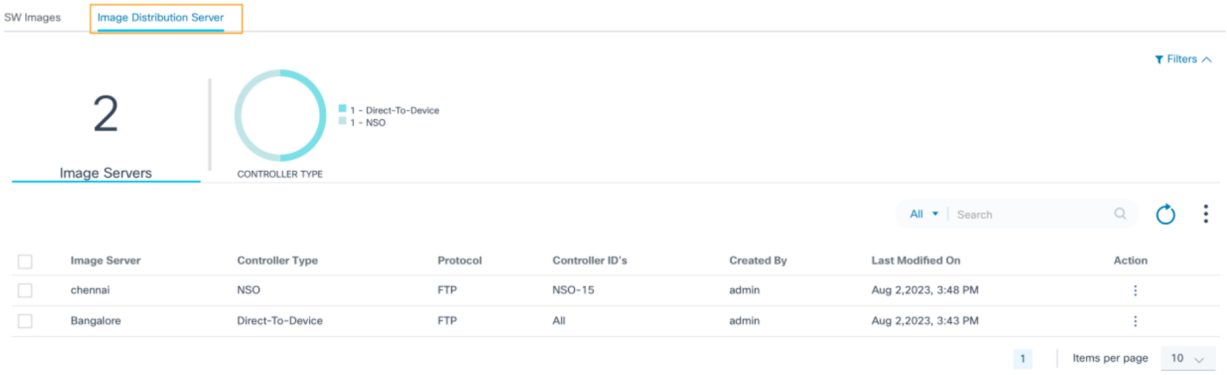
Image Distribution Server 페이지에 액세스하려면 다음을 수행합니다.

1. 이미지 배포 서버에 대한 액세스 권한을 관리하는 자격 증명을 사용하여 BPA에 로그인합니다 .



소프트웨어 이미지 관리

2. OS Upgrade > Software Image Management를 선택합니다.



이미지 배포 서버 탭

3. Image Distribution Server(이미지 배포 서버) 탭을 클릭합니다.

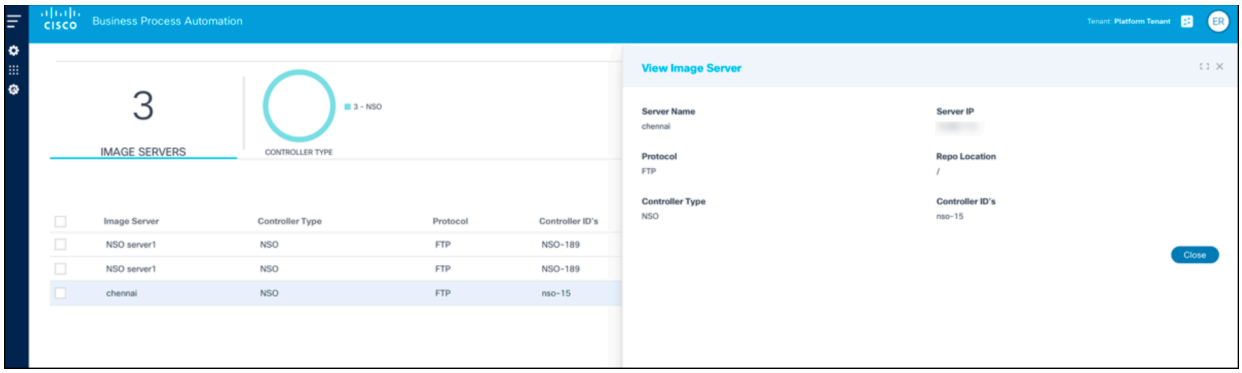
Image Distribution Server(이미지 배포 서버) 탭에는 다음이 포함되어 있습니다.

- 다음을 제공하는 분석 섹션이 맨 위에 표시됩니다.
  - 이 BPA 인스턴스에 온보딩된 총 이미지 서버 수
  - 컨트롤러 유형에 따라 이미지 서버를 필터링할 수 있는 컨트롤러 유형 빠른 필터(예: NSO, Direct-to-Device, CNC, ANSIBLE, FMC) 숫자는 해당 컨트롤러 유형과 연결된 이미지 배포 서버의 총 수를 나타냅니다.
- 다음 기능을 제공하는 추가 옵션 아이콘
  - 이미지 서버 추가: 새 이미지 배포 서버 추가
  - 모두 삭제: 선택한 배포 서버의 대량 삭제
- 배포 서버를 검색하는 데 사용할 수 있는 검색 필터로, 다음과 같은 전용 검색 필터를 포함합니다.
  - 모두: 모든 필드에서 검색
  - 이미지 서버: 특정 서버 이름의 서버를 검색합니다.
  - 컨트롤러 ID: 특정 컨트롤러 ID와 연결된 서버를 검색합니다.
- 페이지를 새로 고치고 선택한 필터를 지우는 데 사용할 수 있는 새로 고침 아이콘
- 기존 배포 서버는 다음 열이 있는 표 형태 테이블에 표시됩니다.
- 이미지 서버: 저장소 서버의 고유 이름
  - 컨트롤러 유형: 이 이미지 서버를 적용할 수 있는 컨트롤러 유형
  - 프로토콜: 저장소 서버에서 지원되는 복사 프로토콜

참고: FTP, SCP 및 SFTP(Secure File Transfer Protocol)만 지원됩니다

- 컨트롤러 ID: 현재 저장소 서버를 사용할 수 있거나 적용할 수 있는 컨트롤러 인스턴스 컨트롤러 인스턴스는 해당 컨트롤러를 통해 관리되는 디바이스를 나타냅니다
- 작성자(Created By): 저장소 서버에 온보딩한 사용자
- 마지막 수정 날짜: 서버 세부 정보가 마지막으로 업데이트된 시간의 타임스탬프입니다.

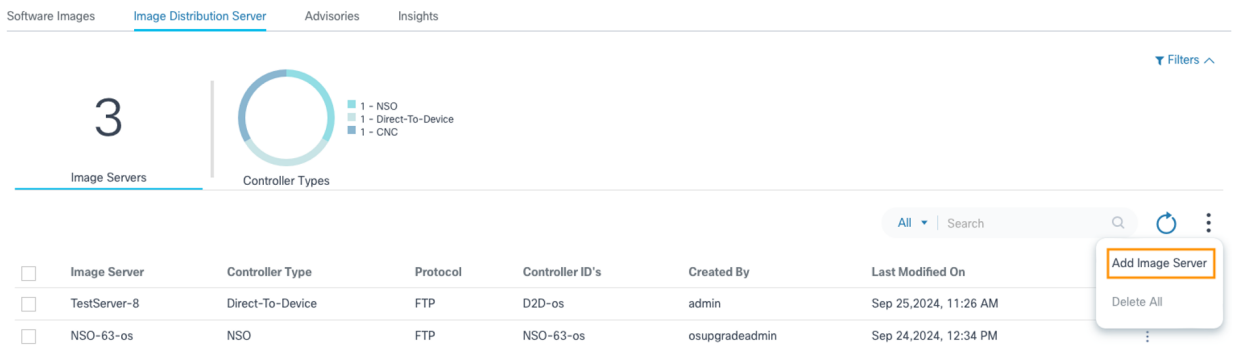
- 작업: Edit(수정) 및 Delete(삭제)와 같은 행별 작업을 제공합니다



이미지 서버 패널 보기

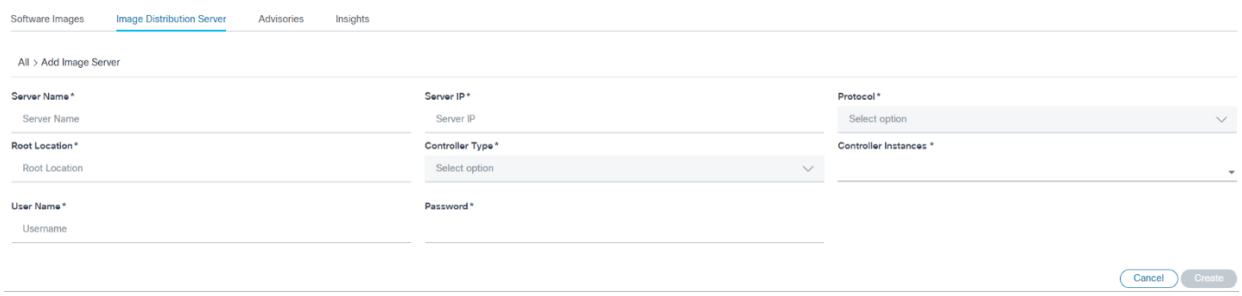
- 행을 클릭하면 View Image Server(이미지 서버 보기) 창이 열립니다

이미지 서버 세부 정보 추가

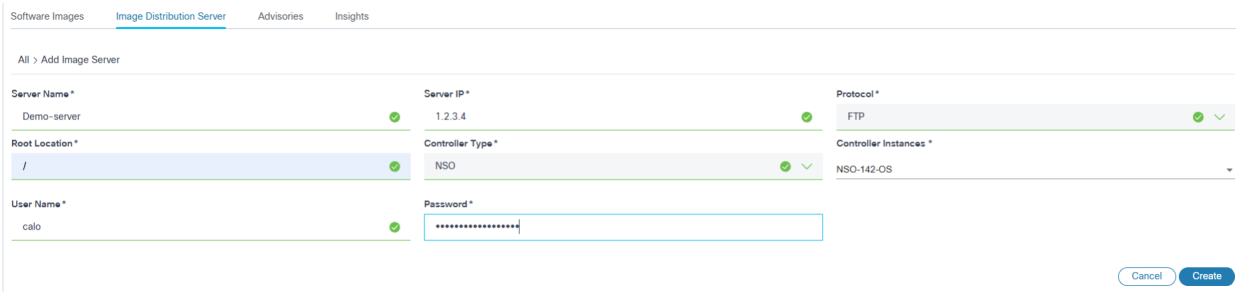


이미지 서버 추가

4. More Options(추가 옵션) 아이콘 > Add Image Server(이미지 서버 추가)를 선택합니다. Add Image Server(이미지 서버 추가) 페이지가 표시됩니다.



이미지 서버 세부 정보 추가



샘플 세부 정보가 포함된 이미지 서버 추가

5. 다음 필드에 정보를 입력합니다.

- 서버 이름: 이미지 저장소 서버의 고유 이름입니다.
- 서버 IP: 저장소 서버의 IPv4 주소

참고: 추가하기 전에 네트워크 디바이스에서 이 IP에 연결할 수 있는지 확인하십시오.

- 프로토콜: 이미지 복제본에 대해 이미지 저장소 서버에서 지원

참고: FTP, SCP 및 SFTP 프로토콜만 지원됩니다.

- Repo 위치: 저장소 서버에 있는 이미지 파일의 기본 경로

참고: 이미지 파일이 이미지 서버 저장소 폴더의 루트에 있는 경우 "/"는 값으로 작동합니다.

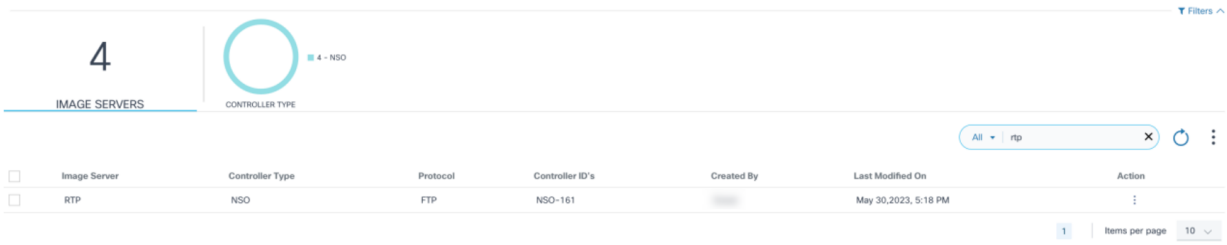
- 컨트롤러 유형: 현재 이미지 서버를 적용할 수 있는 컨트롤러 유형

참고: NSO, Direct-To-Device, CNC 및 ANSIBLE만 지원됩니다.

- 컨트롤러 인스턴스: 해당 이미지 저장소 서버를 사용하여 이미지를 복사해야 하는 관리되는 디바이스를 기반으로 하는 하나 이상의 적용 가능한 컨트롤러 인스턴스
- 사용자: 저장소에서 이미지 파일에 액세스하는 데 사용할 사용자 지정 자격 증명

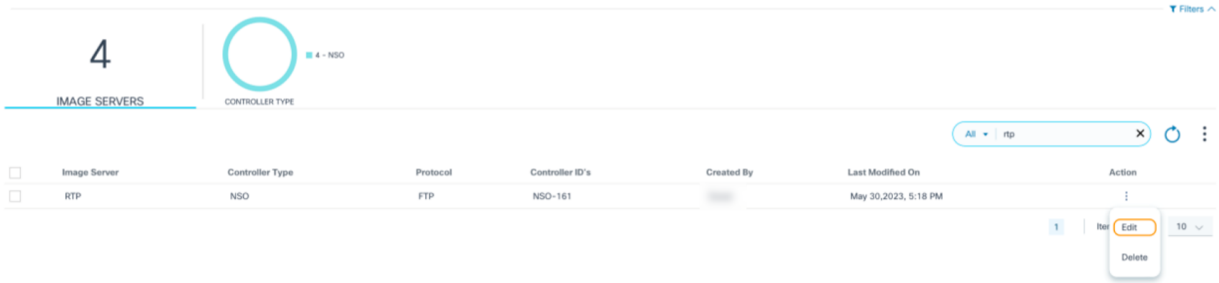
6. Create(생성)를 클릭합니다. 진행 알림이 표시되고 확인 메시지가 나타납니다.

이미지 서버 세부 정보 편집



이미지 서버 검색

7. Search(검색) 필드를 사용하여 업데이트해야 하는 배포 서버를 찾습니다.

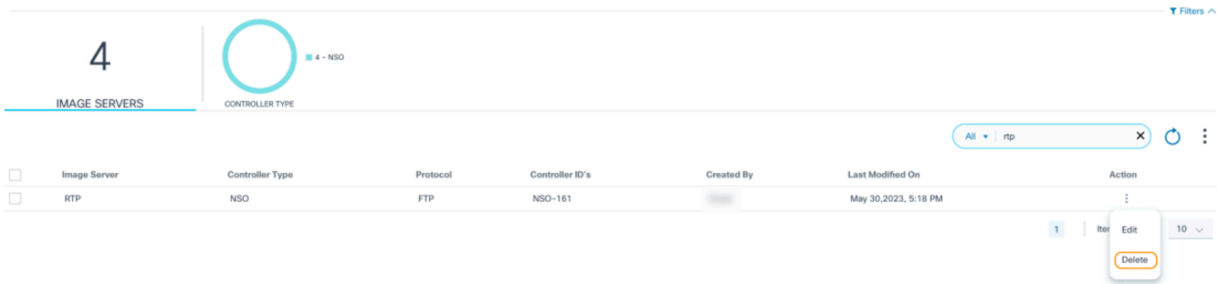


이미지 서버 편집

8. Action(작업) 열에서 More Options(추가 옵션) 아이콘 > Edit(수정)를 선택합니다.
9. 필수 매개변수를 업데이트합니다.
10. 저장을 클릭합니다. 진행률 알림과 확인 메시지가 표시됩니다.

이미지 서버 세부 정보 삭제

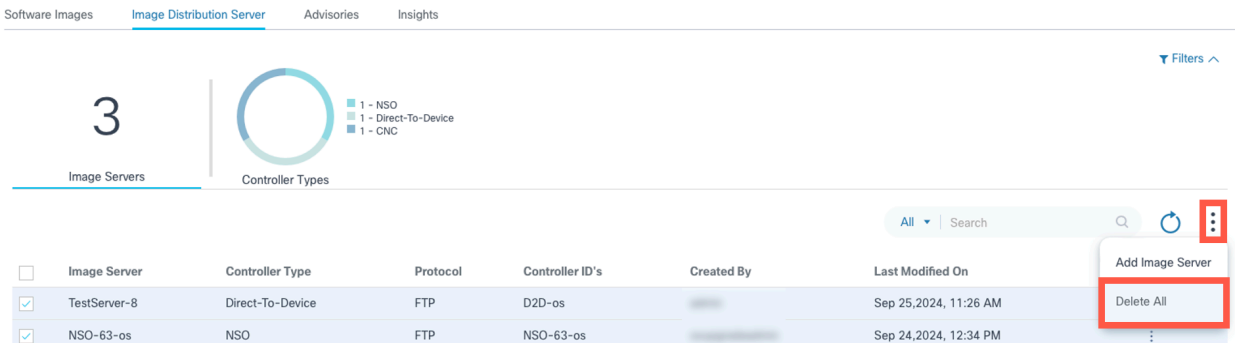
1. 검색 필터를 사용하여 원하는 서버를 찾습니다.



이미지 서버 삭제

2. 단일 배포 서버를 삭제하려면 Action(작업) 열에서 More Options(추가 옵션) 아이콘 > Delete(삭제)를 선택합니다.

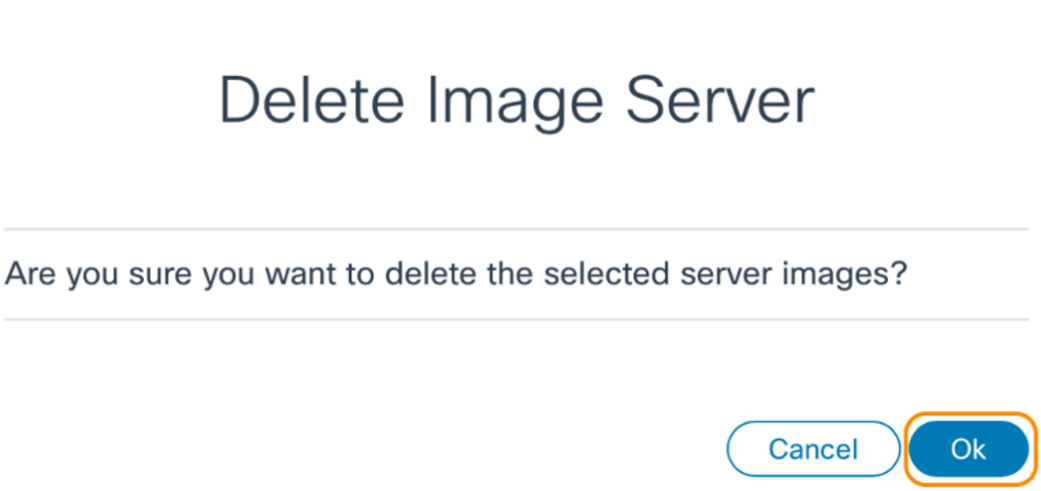
또는



여러 이미지 서버 삭제

여러 배포 서버를 삭제하려면 원하는 서버를 선택하고 추가 옵션 아이콘 > 모두 삭제를 선택합니다.

확인 메시지가 표시됩니다.



삭제 확인

3. OK(확인)를 클릭합니다. 진행 상황 알림 및 확인 메시지가 표시됩니다.

소프트웨어 인사이트

Software Insights는 보안 권고, 버그, 네트워크 자산에 노출된 소프트웨어 단종(end-of-life) 등 모든 보안 취약성을 검색합니다. 또한 Cisco Catalyst Center 및 NDFC 컨트롤러에서 관리하는 디바이스 모델에 대한 소프트웨어 제안도 제공합니다. 또한 네트워크 자산에 대해 제안된 소프트웨어 버전을 선택할 수 있으며, 제안 사항이 있는 경우 디바이스 모델에 대한 적합성 정책을 생성합니다.

사전 요구 사항

- Adapter for insights를 활성화합니다. "Cisco-Insights-Adapter"라는 Cisco Insights 서버용 어

댑터는 OOB에서 사용할 수 있습니다. 일부 외부 서드파티 Insights 서버와 통합하려면 해당 어댑터를 구축해야 합니다. 자세한 내용은 BPA Developer Guide에서 Insights Adapter 구성을 참조하십시오.

- BPA 시스템이 Cisco 클라우드에 연결하려면 인터넷 연결이 필요합니다.
- 동기화 작업을 진행하기 전에 client_id 및 client_secret이 어댑터 컨피그레이션에 있는지 확인합니다.
- 필요한 경우 아래 단계에 따라 인터넷용 프록시를 구성할 수 있습니다.
- IOS-XR OS 유형의 경우 필요에 따라 RefD(Reference Data Management)에서 사용자 지정 디바이스 시리즈-모델 매핑을 수행할 수 있습니다. 사용자 지정 시리즈-모델 매핑에 대한 자세한 내용은 BPA Developer Guide를 참조하십시오.
- BPA Kubernetes Pod에서 Cisco의 자문, 버그 및 End-of-Life 세부 정보를 수집하려면 인터넷에 액세스해야 합니다. BPA 네트워크에 직접 인터넷 액세스가 없지만 프록시를 통해 사용할 수 있는 경우 아래 단계를 사용하여 Kubernetes Pod에서 인터넷에 프록시를 사용하도록 하십시오.

1. **<<**http://proxy-domain.com:port**>>** 대신 실제 프록시 주소로 스크립트를 업데이트합니다.
2. 구축 YAML 또는 조타 차트에서 각 포드에 대한 환경 매개변수를 구성합니다.
3. NO_PROXY 또는 no_proxy 컨피그레이션의 모든 구축 이름을 추가하여 Kubernetes 노드에서 아래 스크립트를 실행합니다.

```
#!/bin/bash
# Define the environment variables
HTTP_PROXY=”<



     >”
HTTPS_PROXY=”<< http://proxy-domain.com:port>>”
http_proxy=”<



      >”
https_proxy=”<



       >”

NO_PROXY="*.svc,localhost,127.0.0.1,192.168.0.0/16,10.0.0.0/8,172.16 .0.0/12,adaptor-builder,agent-mana

no_proxy="*.svc,localhost,127.0.0.1,192.168.0.0/16,10.0.0.0/8,172.16 .0.0/12,adaptor-builder,agent-mana
# Get the list of deployments
deployments=$(kubectl get deployments -n bpa-ns | grep -v NAME | awk '{print $1}')

# Loop through each deployment and set the environment variables
for dp in $deployments;do
         kubectl set env deployment/$dp\
                     HTTP_PROXY=$HTTP_PROXY \
                     HTTPS_PROXY=$HTTPS_PROXY \
                    http_proxy=$http_proxy \
                     https_proxy=$https_proxy \
                     NO_PROXY=$NO_PROXY \
```

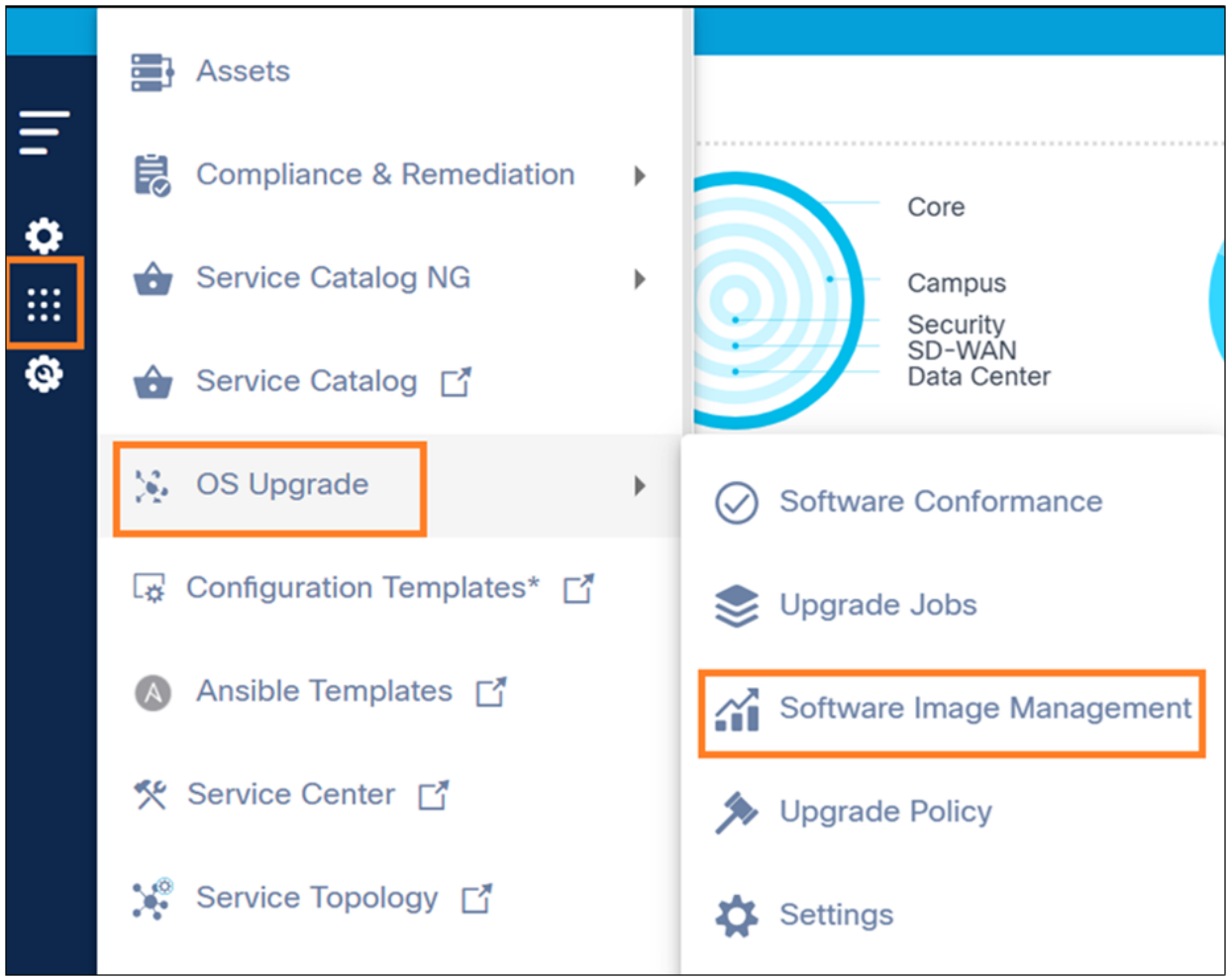
```
                    no_proxy=$no_proxy \
                   -n bpa-ns
done
```

참고: 위에서 설명한 대로 프록시를 설정하면 인사이트 어댑터가 Cisco 네트워크에 연결하고 필요한 Software Insights 데이터를 BPA로 다운로드할 수 있습니다. 프록시 없이 다른 외부 Insights 서버에 직접 연결하려면 no_proxy 변수에 추가해야 합니다.

BPA로 Software Insights 데이터 가져오기

소프트웨어 인사이트 데이터를 BPA에 동기화하려면

1. 소프트웨어 인사이트 데이터를 동기화할 수 있는 접속 정보를 사용하여 BPA에 로그인합니다.



소프트웨어 이미지 관리 탐색

2. 측면 패널에서 OS Upgrade(OS 업그레이드) > Software Image Management(소프트웨어 이미지 관리)를 선택합니다.

Advisories 탭

3. Advisories(권고 사항) 탭을 클릭합니다.

BPA에 소프트웨어 인사이트 가져오기 동기화

BPA에 소프트웨어 인사이트 가져오기 동기화

4. Sync를 클릭합니다.

이렇게 하면 인벤토리에 있는 자산과 관련된 모든 보안 권고, 우선 순위 버그, 단종 공보 및 소프트웨어 제안이 검색됩니다. 보안 권고 및 소프트웨어 단종 날짜는 OS 유형 및 소프트웨어 버전에 따라 결정됩니다. 우선 순위 버그와 소프트웨어 제안은 제품 ID 및 소프트웨어 버전에 따라 결정됩니다.

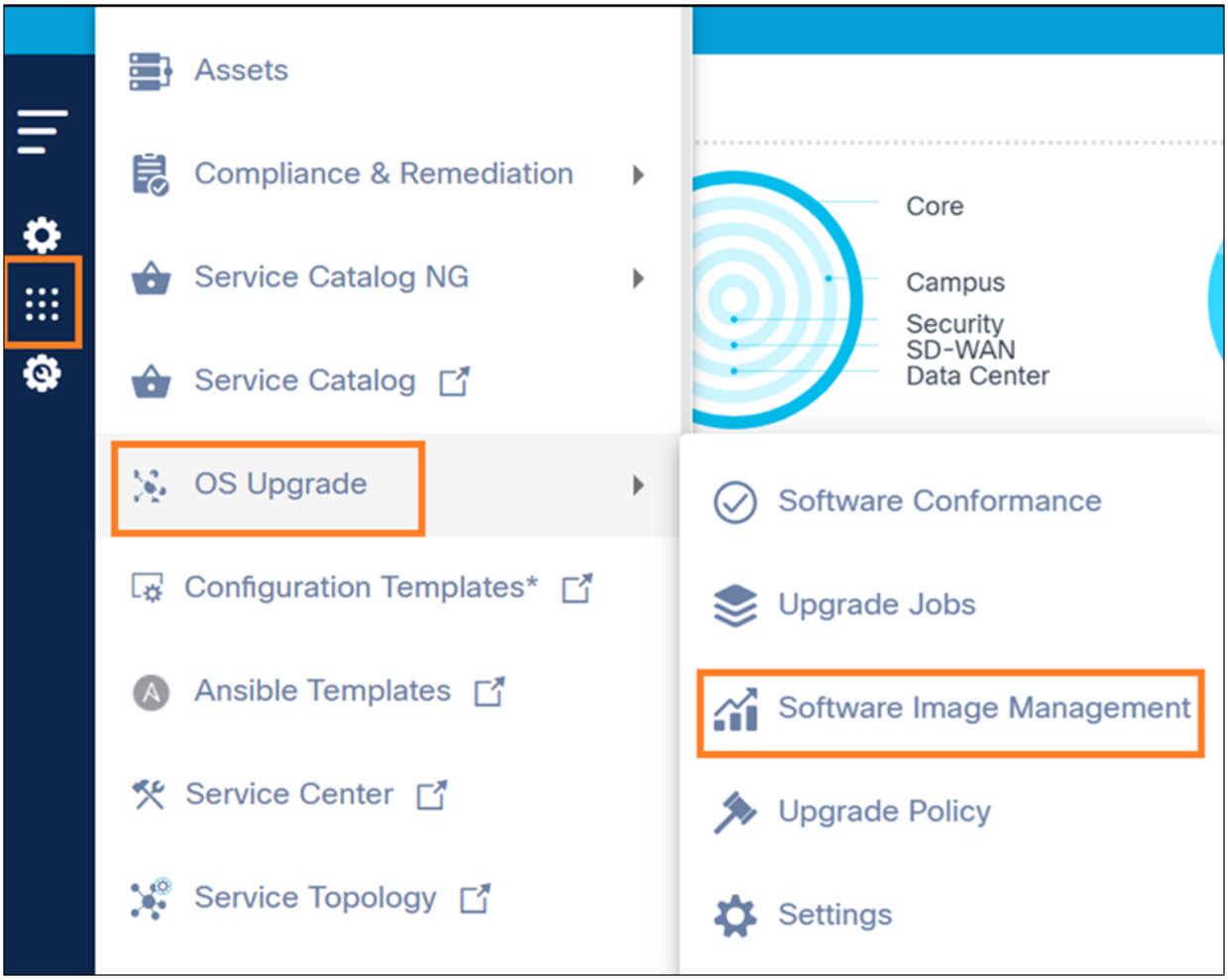
Last Updated(최종 업데이트)는 인사이트 데이터가 마지막으로 동기화된 날짜와 시간을 표시하며, Sync Status(동기화 상태) 필드에 마지막 동기화 상태가 표시됩니다.

참고: 해당되는 모든 권고, 버그, 릴리스 노트 및 제안은 "Cisco-Insights-Adapter" 파일을 통해 Cisco 클라우드에서 가져옵니다.

보안 권고 사항 보기 및 관리

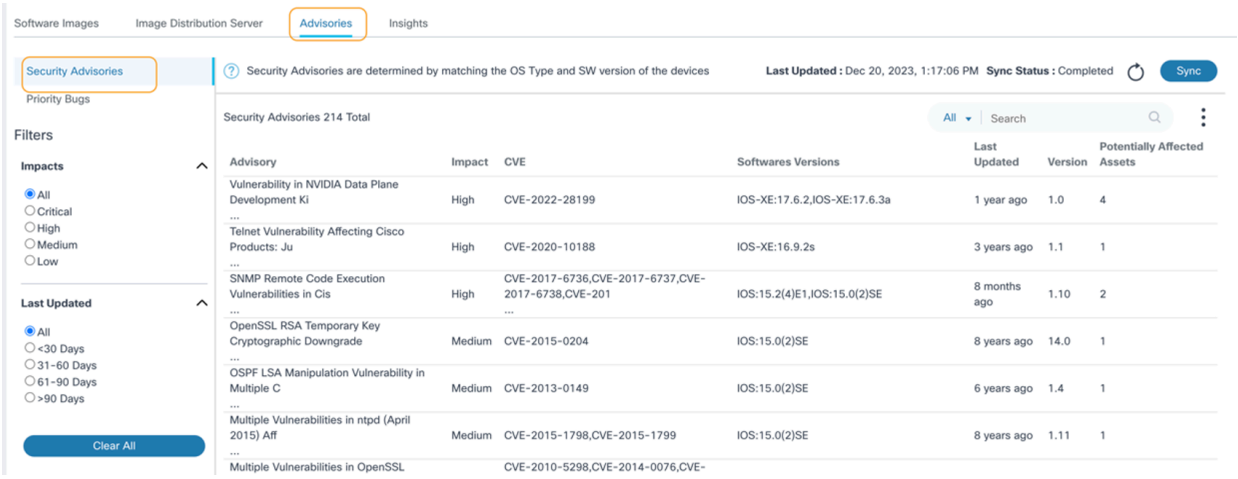
Advisories 페이지에 액세스하려면 다음을 수행합니다.

1. Advisories에 대한 액세스 권한을 관리하는 자격 증명을 사용하여 BPA에 로그인합니다.



소프트웨어 이미지 관리 탐색

2. OS Upgrade > Software Image Management를 선택합니다.



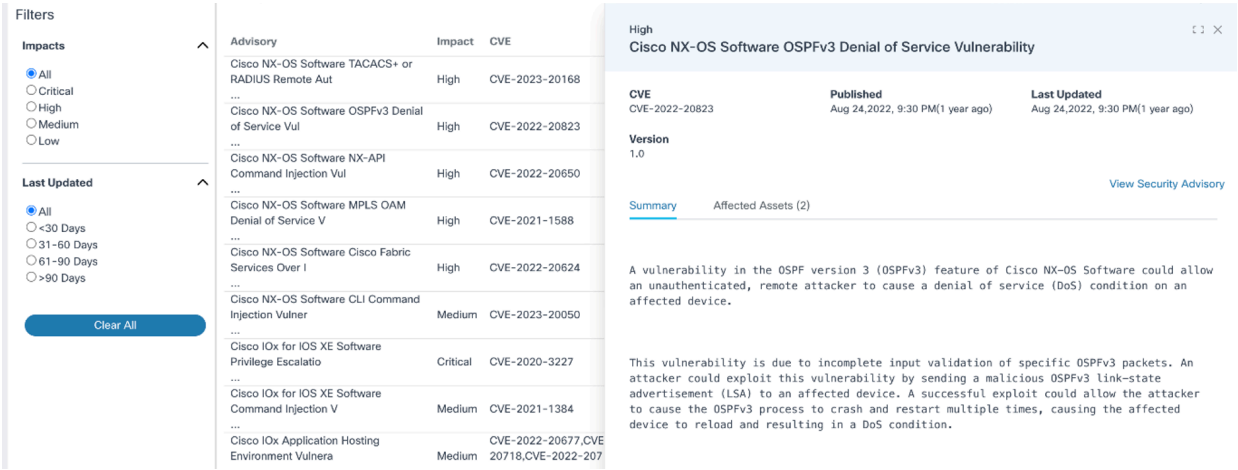
보안 자문

3. Advisories(권고 사항) 탭을 클릭합니다. Security Advisories 페이지는 기본적으로 열립니다.

권고 사항 데이터 필터링에 대해 다음 옵션이 표시됩니다.

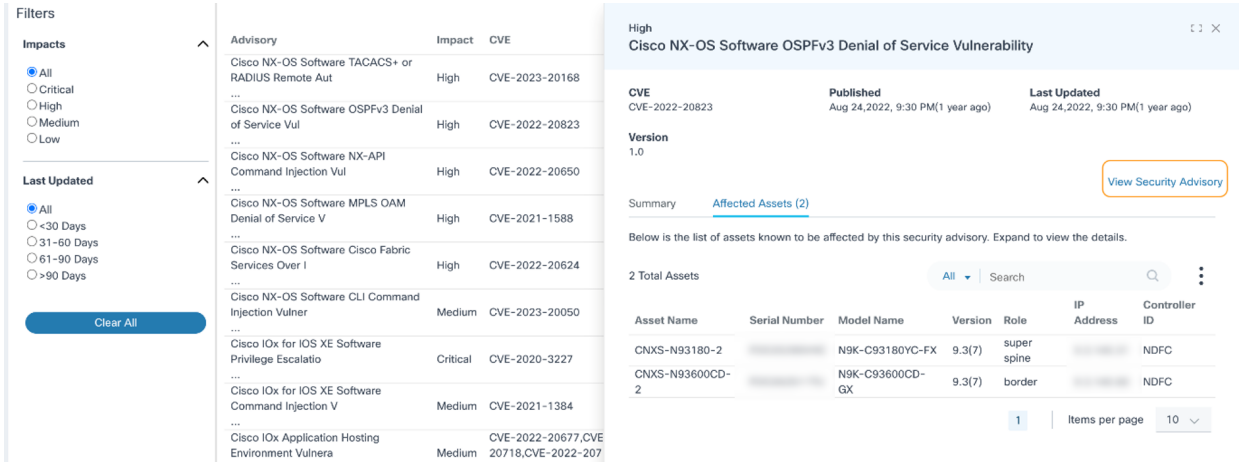
- 영향을 통해 권고 심각도를 기반으로 필터링할 수 있습니다. 기본적으로 모두 선택됨
- Last Updated는 권고자의 마지막 업데이트 날짜를 기준으로 필터링할 수 있습니다. 기본적으로 모두 선택됨
- 모두 지우기 선택한 필터를 재설정합니다
- 검색 필터는 권고 사항을 검색하는 데 사용되며 다음과 같은 전용 검색 필터를 포함합니다.
- 모두: Advisory, CVE, Software Versions와 같은 열을 검색합니다
- 권고: 검색에 지정된 용어로 권고 사항을 검색합니다.
- CVE: 특정 CVE(Common Vulnerabilities and Exposures)가 있는 권고 사항 검색
- 소프트웨어 버전: 특정 OS 유형 또는 소프트웨어 버전과 관련된 자문 검색
- Refresh(새로 고침) 아이콘은 페이지를 새로 고치고 선택한 필터를 지우는 데 사용됩니다
- 기존 권고는 다음 열과 함께 표시됩니다.
    - 권고: 권고 사항 요약
    - 영향: 권고 심각도
    - CVE: 할당된 CVE
    - 소프트웨어 버전: 영향을 받는 OS 유형 및 소프트웨어 버전
    - 최종 업데이트: 권고가 마지막으로 업데이트된 날짜 및 시간
    - 버전: 자문 버전
    - 영향을 받을 수 있는 자산: 권고의 영향을 받을 수 있는 자산 수
- 헤더 필드를 클릭하면 권고 사항이 정렬됩니다

참고: 분류는 영향을 받을 가능성이 있는 자산에 대한 옵션이 아닙니다.



권고 사항 세부 정보 보기

- 권고 행을 선택하면 다음 탭이 포함된 권고 사항의 세부 정보 보기가 열립니다.
    - 요약: 선택한 권고 사항의 요약을 표시합니다. 기본적으로 표시
    - 영향을 받는 자산: 자산 이름, 일련 번호, 모델 이름, 소프트웨어 버전, IP 주소, 컨트롤러 ID와 같은 잠재적으로 영향을 받는 자산 세부 정보를 표시합니다. 이 탭에서는 에셋 정렬 및 검색을 수행할 수 있습니다



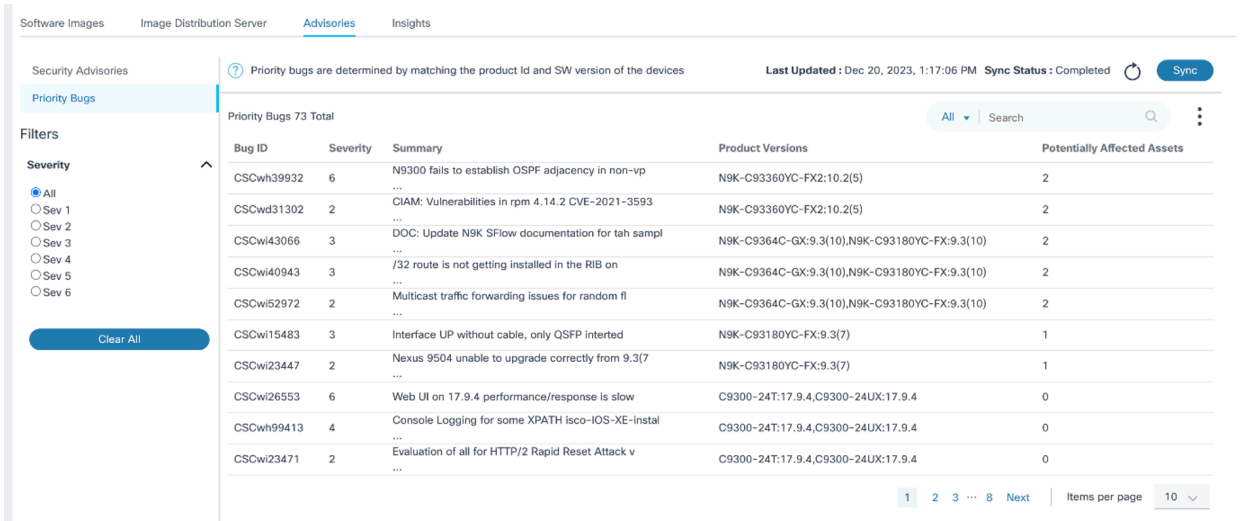
보안 권고 사항 보기

- 보안 권고 사항 보기 링크: 공식 자문 페이지로 이동합니다

우선순위 버그 보기 및 관리

우선 순위 버그 선택

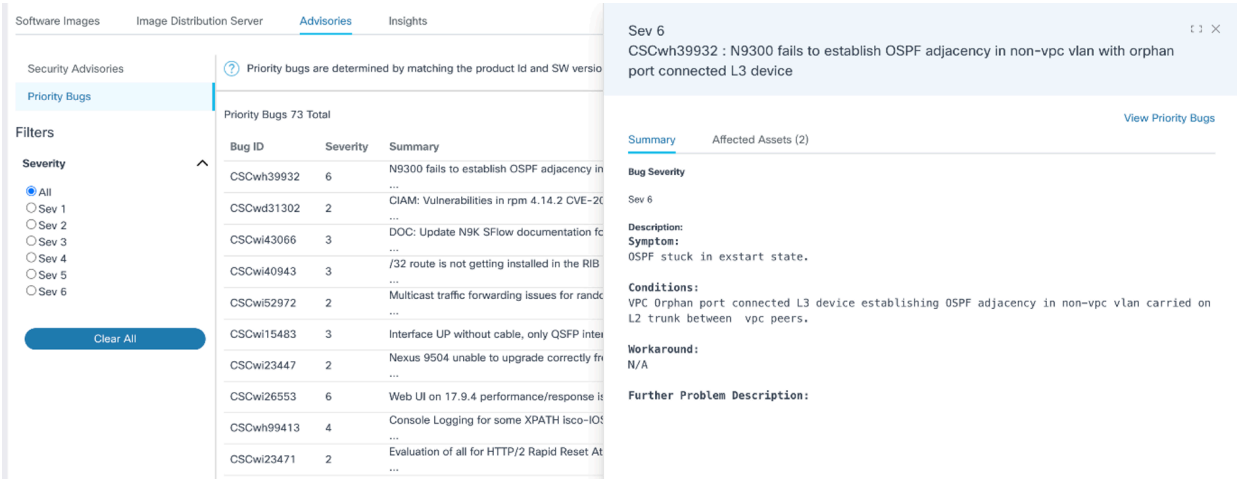
이전 섹션에 설명된 대로 Advisories 페이지를 연 후 Priority Bugs(우선순위 버그) 탭을 클릭합니다. Priority Bugs 페이지가 표시됩니다.



우선 순위 버그

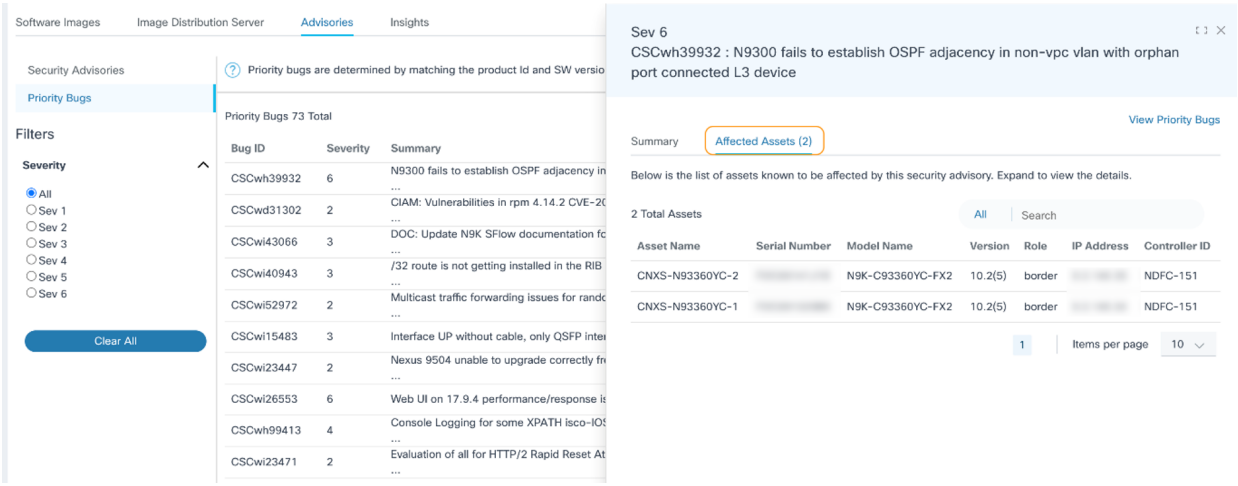
다음 옵션은 Priority Bugs(우선 순위 버그) 페이지에서 사용할 수 있습니다.

- 버그 심각도를 기반으로 필터링을 허용하는 심각도 필터 기본적으로 모두 선택됨
- 검색 필터는 버그를 검색하는 데 사용할 수 있으며 다음과 같은 전용 검색 필터를 포함합니다.
    - 모두: 모든 필드에서 검색
    - 버그 ID: 지정된 버그 ID의 버그를 검색합니다.
    - 요약: 요약에 특정 키워드가 있는 버그를 검색합니다.
    - 제품 버전: 특정 제품 ID 또는 소프트웨어 버전과 관련된 버그를 검색합니다.
- Refresh(새로 고침) 아이콘을 사용하여 페이지를 새로 고치고 선택한 필터를 지울 수 있습니다
- 우선순위 버그는 다음 열과 함께 테이블에 표시됩니다.
    - 버그 ID
    - 심각도: 버그 심각도
    - 요약: 버그의 요약 세부사항
    - 제품 버전: 영향을 받는 제품 ID 및 소프트웨어 버전
    - 영향을 받을 수 있는 자산: 버그의 영향을 받을 수 있는 자산 수
- Potentially Affected Assets(영향을 받을 수 있는 자산)를 제외한 열 머리글을 클릭하여 정렬할 수 있습니다.



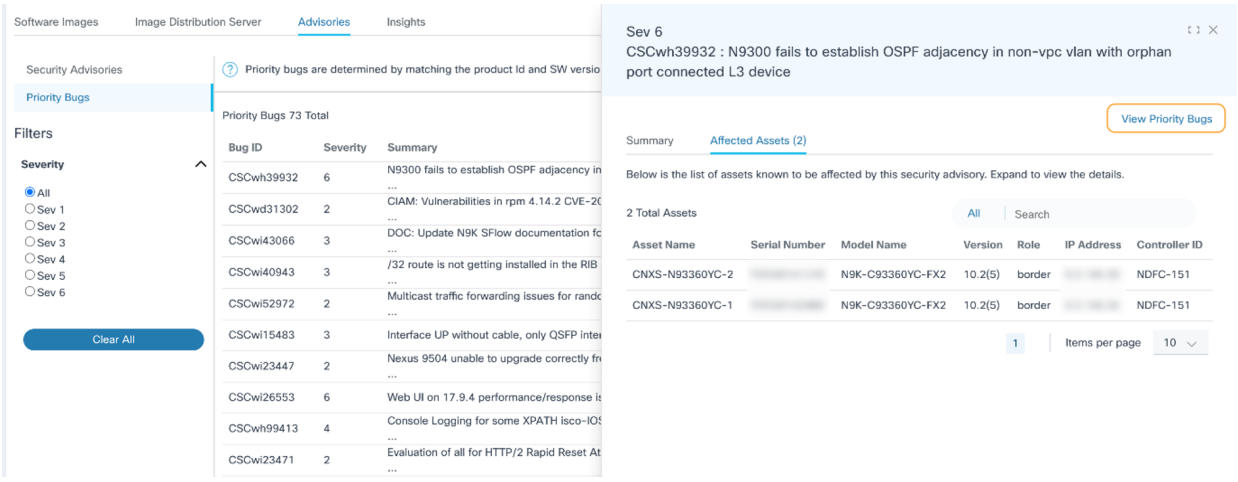
버그 세부사항 보기

- 버그를 클릭하면 다음을 포함하는 버그의 세부 보기가 열립니다.
    - 요약 탭: 버그 심각도, 설명 및 해결 정보 표시



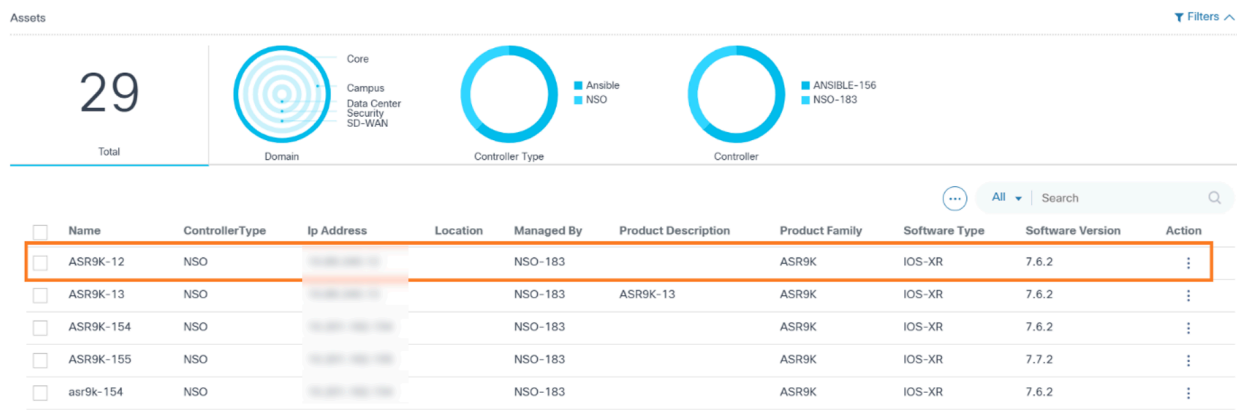
Affected Assets(영향을 받는 자산) 탭

- 영향을 받는 자산 탭: 자산 이름, 일련 번호, 모델 이름, 소프트웨어 버전, IP 주소, 컨트롤러 ID 등 영향을 받을 수 있는 모든 자산 세부사항을 표시합니다S; 이 탭에서는 에셋 정렬 및 검색을 수행할 수 있습니다



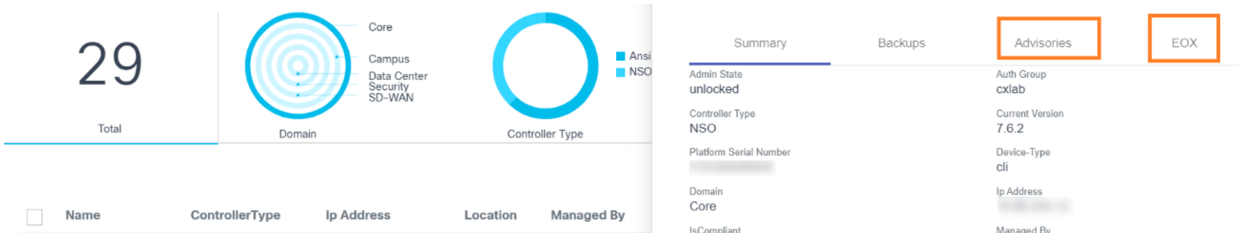
우선 순위 버그 보기

- 우선 순위 버그 보기 링크: 공식 버그 검색 도구로 이동



자산

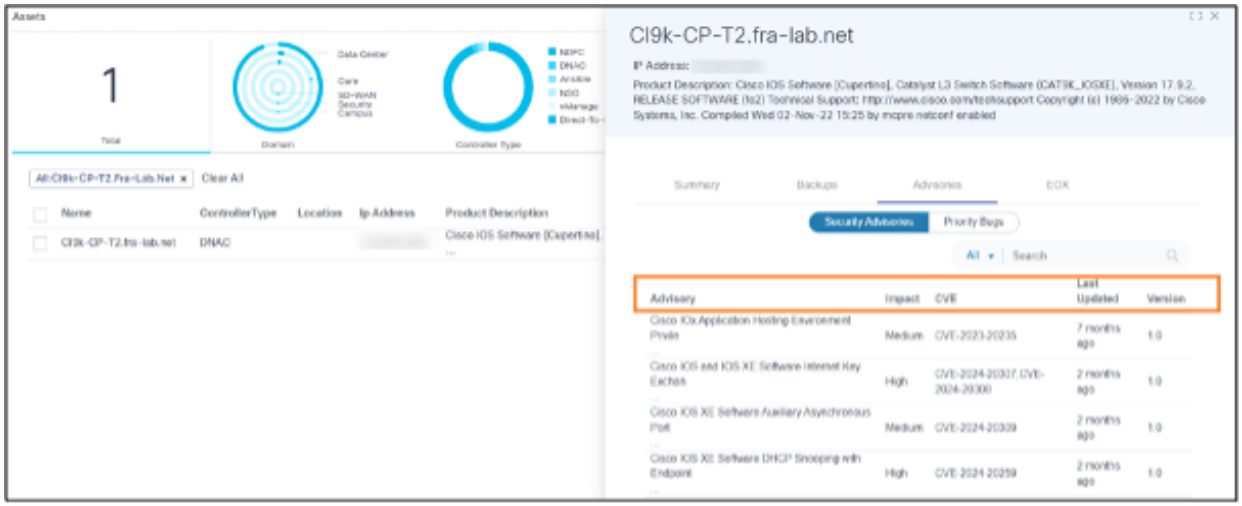
Asset Manager에서 사용자는 모든 자산의 목록을 볼 수 있습니다. 에셋을 선택하면 패널에 자산 레벨 정보가 표시됩니다. 여기에는 두 개의 탭으로 구성된 자산 소프트웨어 취약성 세부사항이 포함됩니다. 자문 및 EOX.



자문 및 EOX

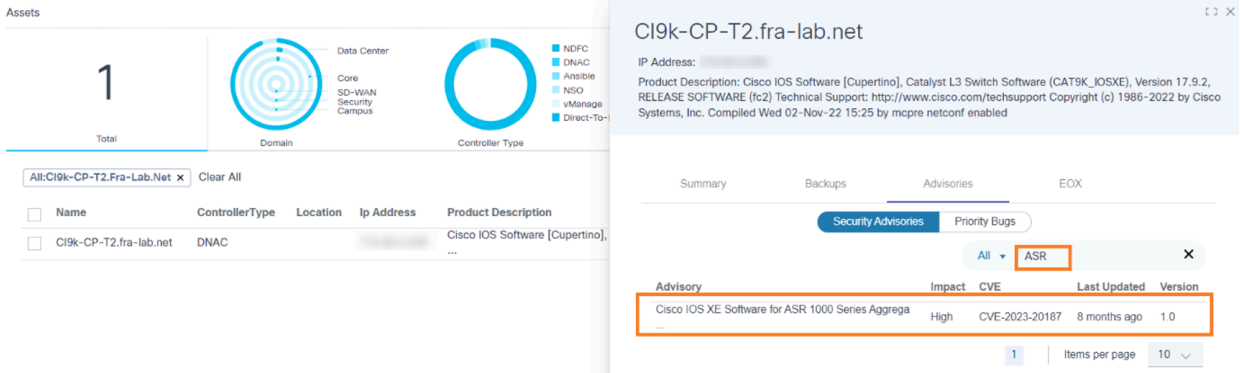
Advisories 탭에는 Security Advisories(보안 권고 사항) 및 Priority Bug(우선 순위 버그)의 두 가지 하위 탭이 있습니다. 이러한 탭에 대한 자세한 내용은 아래 섹션에 나와 있습니다.

보안 자문

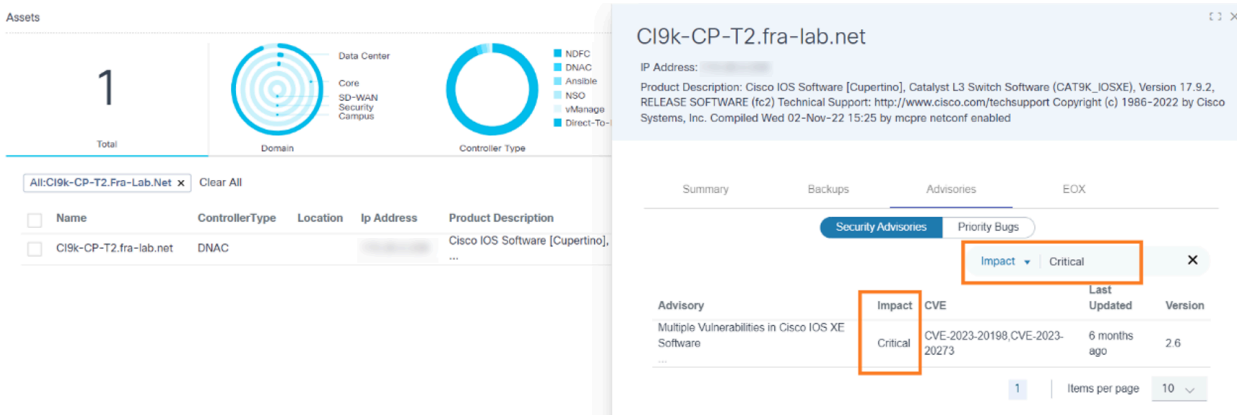


선택한 자산의 보안 권고

사용자는 Security Advisories 하위 탭에서 선택한 자산에 영향을 주는 모든 보안 Advisories를 볼 수 있습니다. 보안 권고 테이블의 열에는 Advisories, Impact, CVE, Last Updated 및 Version이 포함됩니다¶.



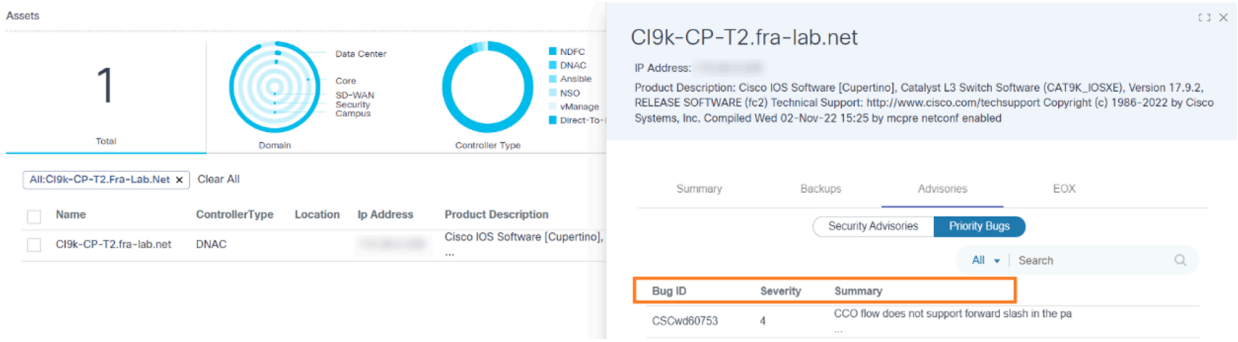
보안 권고 사항 검색



보안 권고 사항 검색 - 영향 옵션

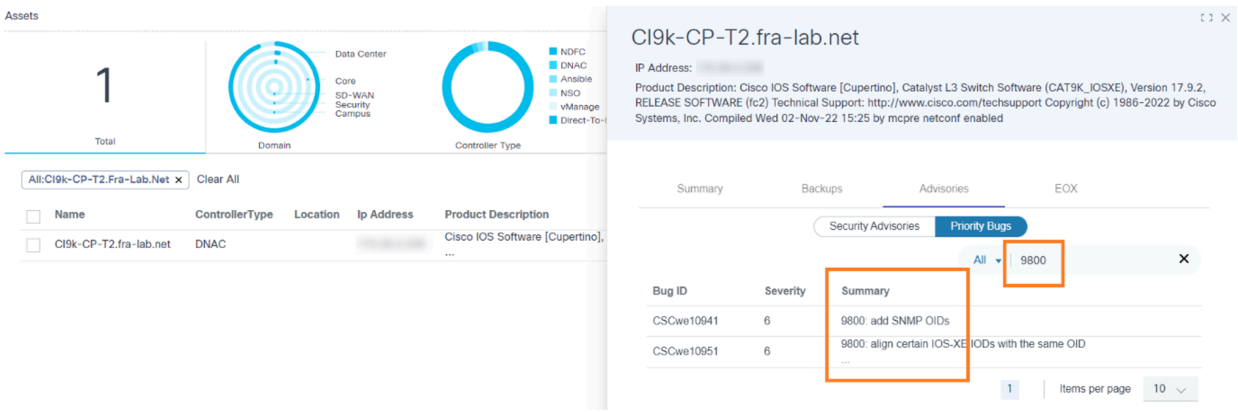
사용자는 Advisories, Impact, CVE, Last Updated, Version 열의 값을 기반으로 Advisories를 검색할 수 있습니다. 페이지 매기기를 사용하면 페이지 사이를 이동할 수 있습니다.

우선 순위 버그

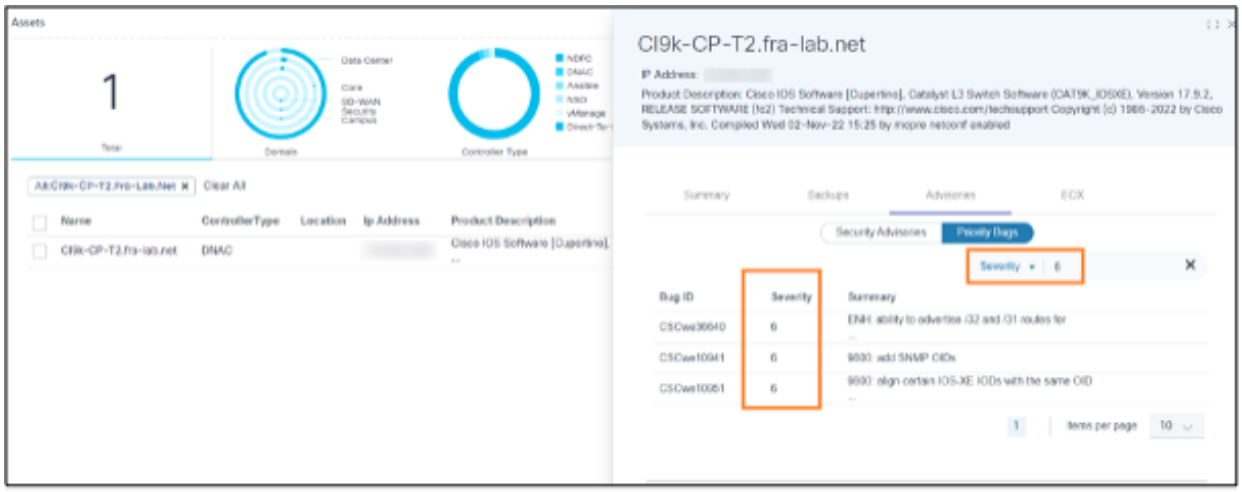


선택한 자산에 영향을 주는 우선 순위 버그

Priority Bugs 하위 탭에서 사용자는 지정된 자산에 영향을 주는 모든 우선순위 버그에 액세스할 수 있습니다. 이 탭의 열에는 버그 ID, 심각도 및 요약이 포함됩니다.



요약으로 우선 순위 버그 검색



심각도별 우선 순위 버그 검색

사용자는 Bug ID, Severity, Summary 열의 값을 기반으로 우선순위 버그를 검색할 수 있습니다. 페이지를 매기면 페이지 간 탐색이 용이해집니다.

EOX

EOX 탭

EOX 탭은 세 가지 중요한 날짜를 비롯하여 자산에 대한 소프트웨어 단종 데이터를 표시합니다.

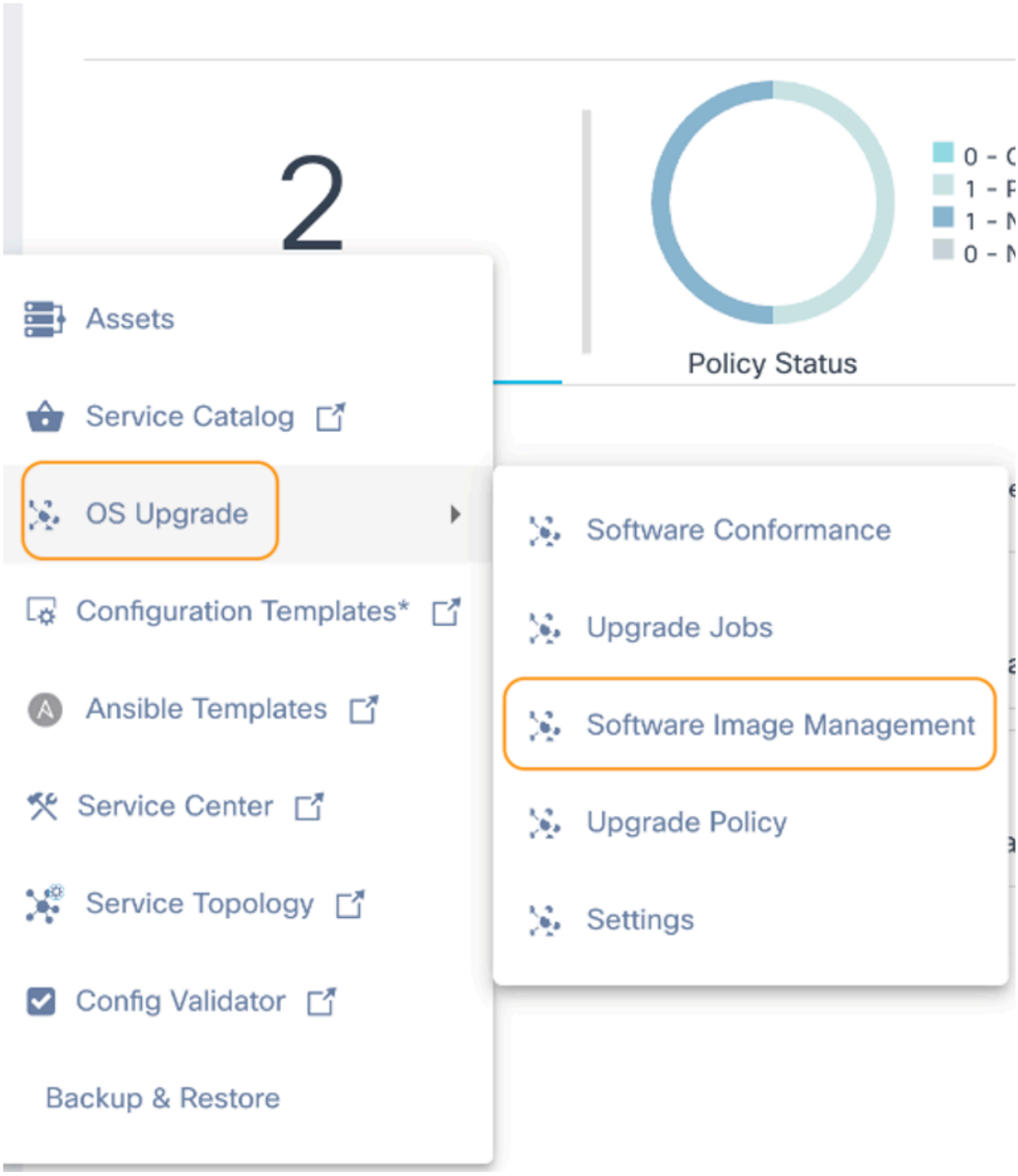
- 소프트웨어 유지 보수 종료
- 보안 지원 종료
- 지원 종료일

소프트웨어 인사이트 보기

Software Insights는 Cisco Catalyst Center 및 NDFC 컨트롤러에서 관리하는 디바이스 모델에 대한 소프트웨어 제안 사항을 제공하며, 제안 사항이 있는 경우 관리자 사용자는 디바이스 모델에 대한 적합성 정책을 생성할 수 있습니다.

Software Insights에 액세스하려면

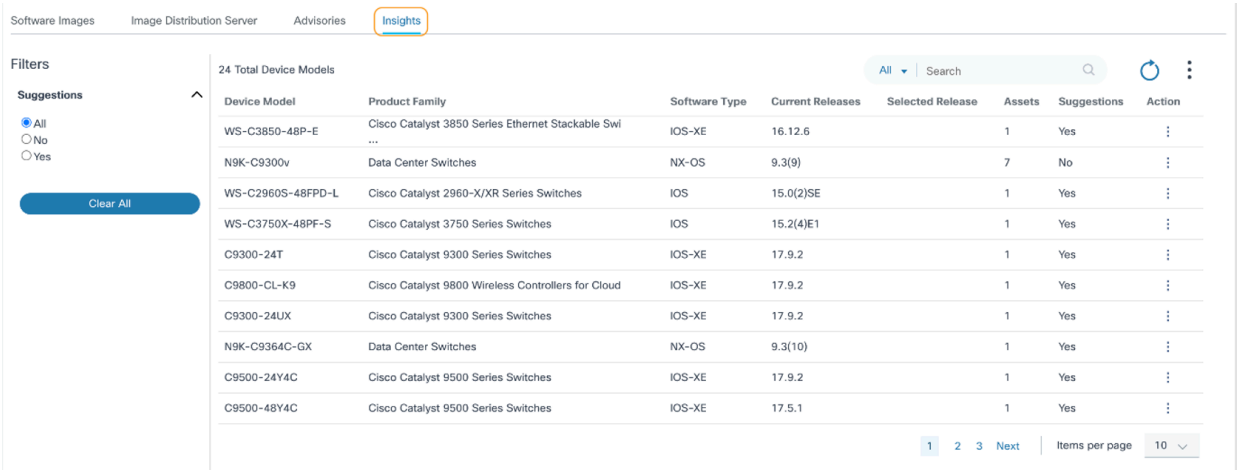
1. Insights에 대한 액세스 권한을 관리하는 자격 증명으로 BPA에 로그인합니다.



소프트웨어 이미지 관리

2. 측면 패널에서 OS Upgrade(OS 업그레이드) > Software Image Management(소프트웨어 이

미지 관리)를 선택합니다.



Insights 탭

3. Insights 탭을 클릭합니다.

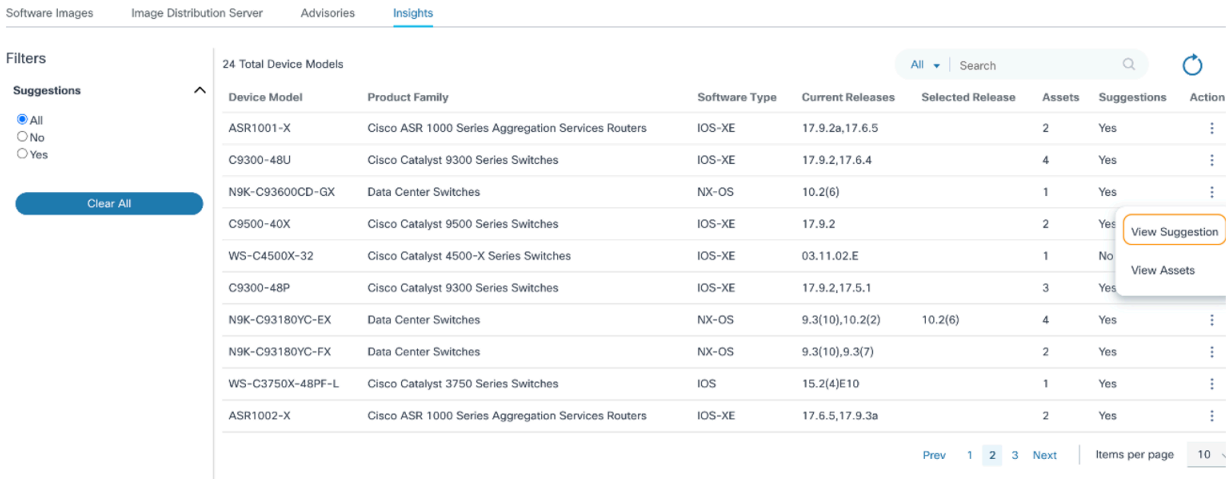
Insights 탭은 다음과 같습니다.

- 사용자가 제안을 기반으로 데이터를 필터링할 수 있도록 하는 필터입니다. 기본적으로 모두(All)가 선택됩니다.
    - 예를 선택하면 장치 모델에 대한 데이터가 권장 사항으로 필터링됩니다.
    - 제안 없이 디바이스 모델의 데이터를 필터링하지 않음

CSV로 내보내기

- More Options(추가 옵션) 아이콘은 페이지에 표시된 데이터를 내보낼 수 있는 Export to CSV(CSV로 내보내기) 옵션을 제공합니다
    - Refresh(새로 고침) 아이콘은 페이지를 새로 고치고 선택한 필터를 지웁니다
    - 검색 필터는 데이터 검색에 사용되며 다음과 같은 전용 검색 필터를 포함합니다.
- 모두: 모든 열(예: 장치 모델, 제품군, 소프트웨어 유형)에서 검색
- 디바이스 모델: 특정 디바이스 모델 이름으로 데이터 검색
- 제품군 특정 제품군 이름의 데이터를 검색합니다.
- 소프트웨어 유형: 특정 소프트웨어 유형 이름의 데이터 검색

- 기존 디바이스 모델은 다음 열과 함께 표시됩니다.
- 디바이스 모델: 디바이스 모델의 이름
- 제품군: 디바이스 모델이 속한 제품군의 이름
- 소프트웨어 유형: 디바이스 모델이 속한 소프트웨어 유형의 이름
- 현재 릴리스: 디바이스 모델의 인벤토리에 현재 있는 고유한 소프트웨어 버전 목록
- 선택한 릴리스: Cisco에서 제공하는 제안 중에서 선택적 버전으로 선택된 권장 릴리스 버전입니다.
- 자산: 장치 모델의 Asset Manager에 있는 에셋 수입니다.
- 제안: 장치 모델에 사용할 수 있는 제안에 대해 Yes(예) 또는 No(아니요)를 표시합니다

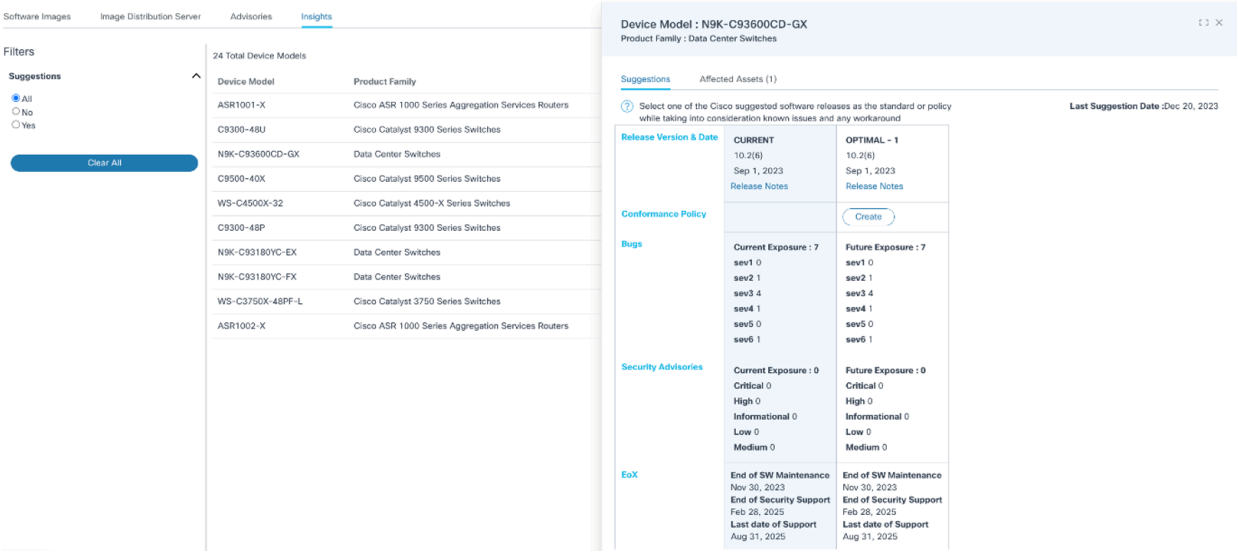


제안 탐색 보기

- 작업: 추가 옵션 아이콘(예: 제안 보기 및 자산 보기)을 통해 행별 작업을 제공합니다.

참고: 장치 모델에 제안 사항이 없으면 제안 사항 보기를 사용할 수 없습니다.

공급업체 제안 소프트웨어 버전 보기 및 선택

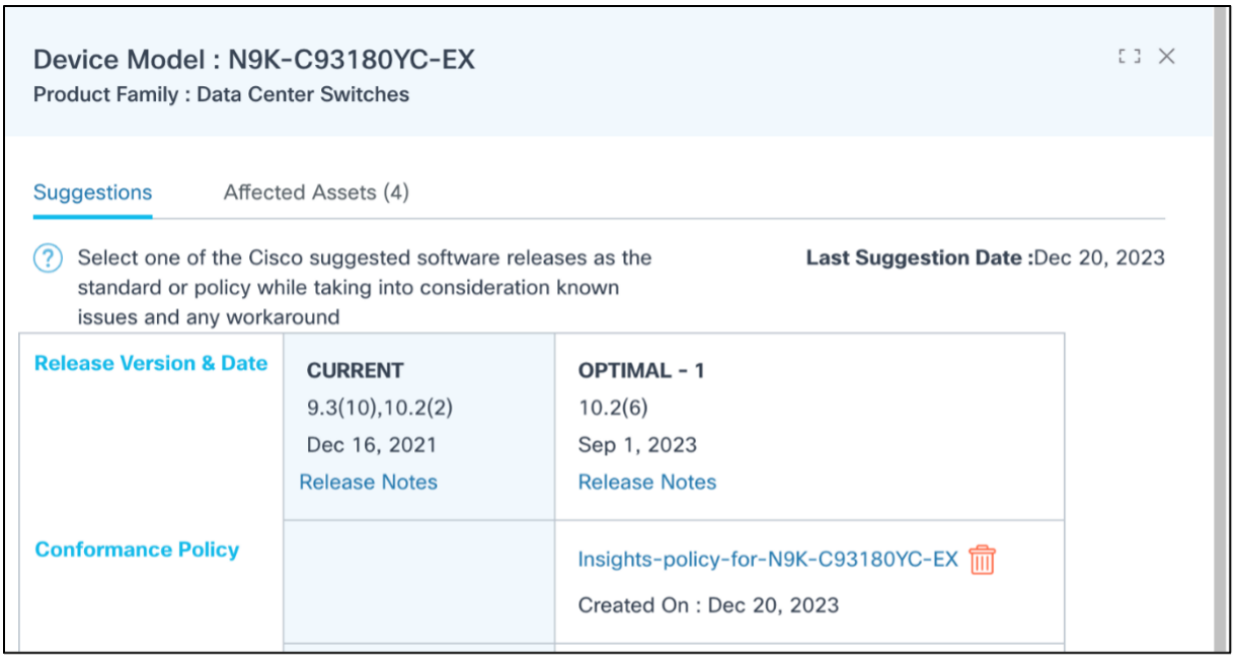


제안 탭

작업 열에서 추가 옵션 아이콘 > 제안 보기를 선택하면 모든 통찰력 세부 정보가 포함된 측면 패널이 열립니다. Suggestions(제안) 탭에는 선택한 디바이스 모델에 대한 현재 및 제안된 릴리스 세부 사항이 있습니다. 디바이스 모델에 두 개 이상의 제안이 있을 수 있습니다. 다음 데이터를 사용할 수 있습니다.

- 릴리스 버전 및 날짜: 릴리스 버전, 날짜 및 메모 세부사항은 Cisco 클라우드에서 사용 가능한 경우 현재 및 제안된 릴리스에 대해 표시됩니다. 인벤토리의 에셋이 둘 이상의 버전에 속하는 경우, 해당되는 모든 버전은 Current 열에 쉼표로 구분된 값으로 표시됩니다
- 준수 정책 생성: 관리자가 디바이스 역할을 Any로 사용하여 특정 버전에 대한 적합성 정책을 생성할 수 있음

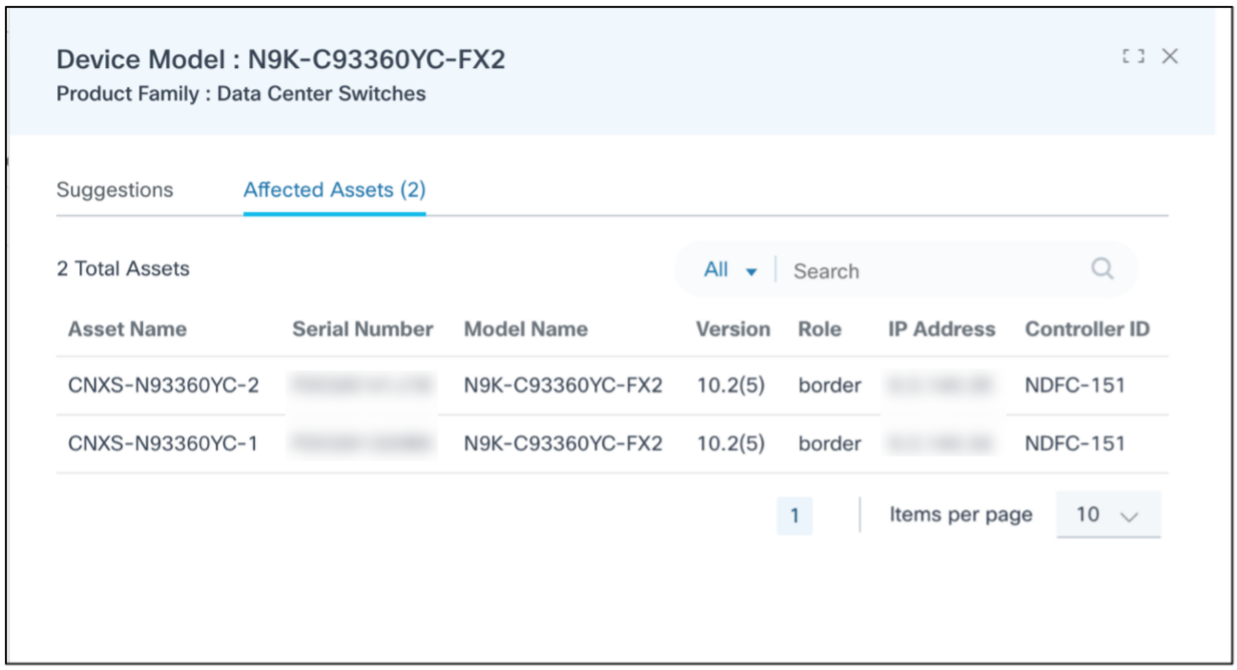
참고: 적합성 정책 생성은 NDFC 컨트롤러 디바이스 모델에 대해서만 지원됩니다



정책 삭제 옵션

참고: 디바이스 모델에 대한 정책이 이미 있는 경우 오류가 표시됩니다. 정책이 없으면 Enabled(활성화됨) 상태로 정책이 생성됩니다. Insights에서 정책이 생성된 경우 사용자는 정책을 삭제할 수 있습니다.

- 버그: 각 릴리스에 대한 통합 버그 수를 표시합니다.
- 보안 권고: 각 릴리스에 대한 통합 권고 사항 수를 표시합니다.
- EoX: 각 릴리스의 소프트웨어 유지 관리 종료, 보안 지원 종료 및 지원 종료일을 표시합니다.



Affected Assets(영향을 받는 자산) 탭

작업 열에서 추가 옵션 아이콘 > 에셋 보기를 선택하면 기본적으로 영향 받는 에셋 탭이 표시되는 측면 패널이 열립니다. Affected Assets(영향받는 자산) 탭에는 Asset Name(자산 이름), Serial Number(일련 번호), Model Name(모델 이름), Software Version(소프트웨어 버전), IP Address(IP 주소), Controller ID(컨트롤러 ID) 등의 열에 영향을 받을 수 있는 자산 세부 정보가 표시됩니다. 이 탭에서는 에셋 정렬 및 검색을 수행할 수 있습니다.

소프트웨어 업그레이드가 필요한 장비 식별

자세한 내용은 소프트웨어 적합성을 참조하십시오.

소프트웨어 적합성

Software Conformance는 네트워크에서 의도한 대상 소프트웨어 버전과 호환되지 않는 자산을 식별하는 데 도움이 됩니다. 검증은 소프트웨어 적합성 의도가 정의된 정책과 규칙을 기반으로 합니다. 이러한 정책은 예약 또는 온디맨드 방식으로 실행할 수 있습니다. 적합성 정책을 성공적으로 실행하면 적용 가능한 자산의 상태를 제공하는 적합성 결과가 생성됩니다. 적합성 범위는 디바이스 역할, 컨트롤러 인스턴스 관리 등과 같은 다양한 기준에 따라 달라집니다.

사전 요구 사항

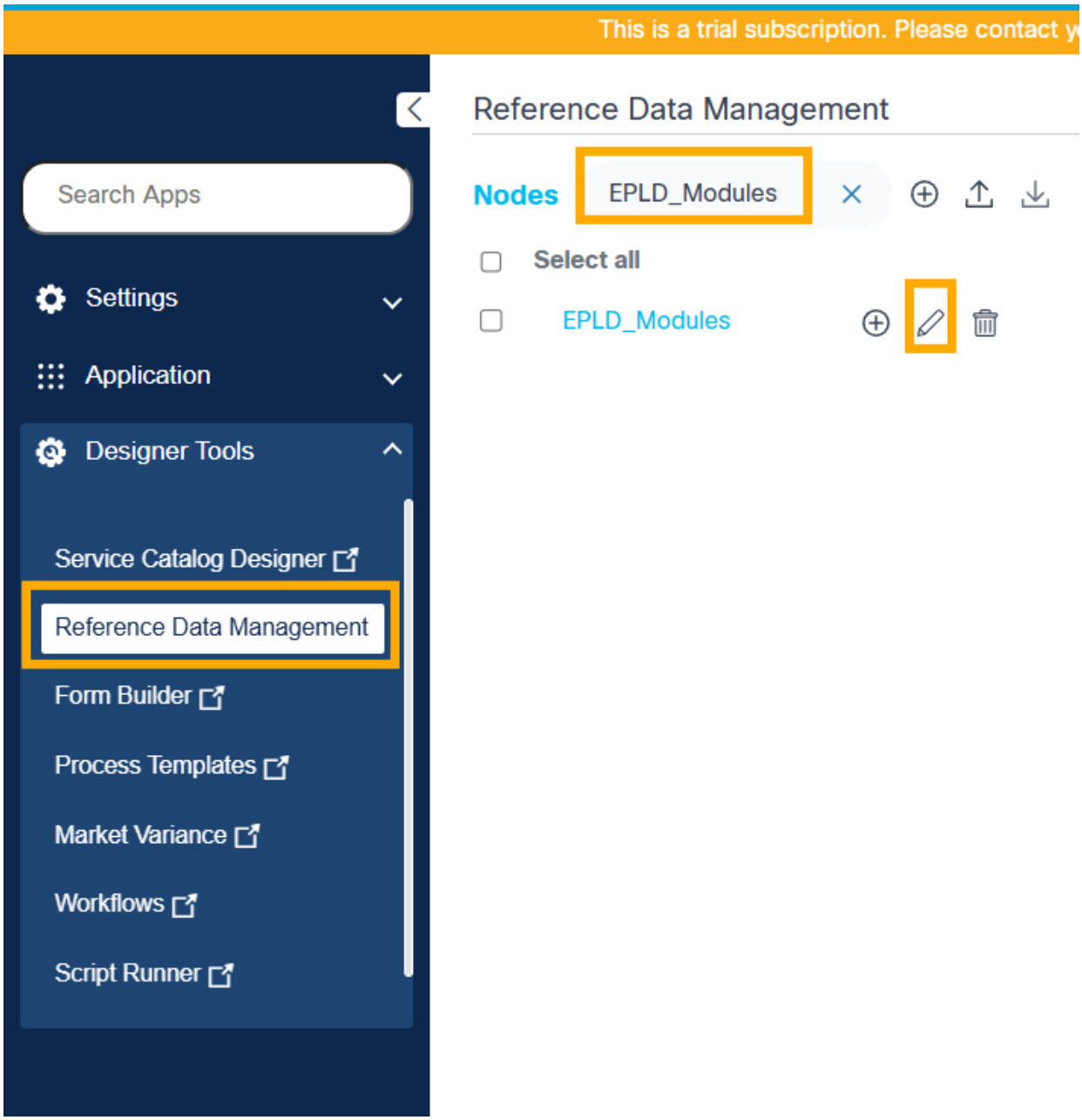
- Cisco Catalyst Center, vManage, NDFC 및 FMC와 같은 컨트롤러의 소프트웨어 이미지가 동기화되어 있어야 합니다. 자세한 내용은 소프트웨어 이미지 메타데이터 동기화를 참조하십시오.

- NSO, CNC, Direct-to-Device, ANSIBLE 등의 컨트롤러에 필요한 소프트웨어 이미지 메타데이터를 추가해야 합니다. 자세한 내용은 소프트웨어 이미지 메타데이터 추가를 참조하십시오.
- 사용자는 EPLD 모듈 데이터를 관리하기 위해 RefD 애플리케이션에 액세스할 수 있어야 합니다.
- 필수 릴리스에 대한 EPLD 모듈 정보는 RefD 응용 프로그램에서 미리 채워져야 합니다
- OOB를 사용할 수 없는 경우 사용자는 RefD 응용 프로그램에서 EPLD 모듈 정보를 수동으로 추가해야 합니다

참조 데이터 관리 응용 프로그램에서 EPLD 모듈 데이터 생성

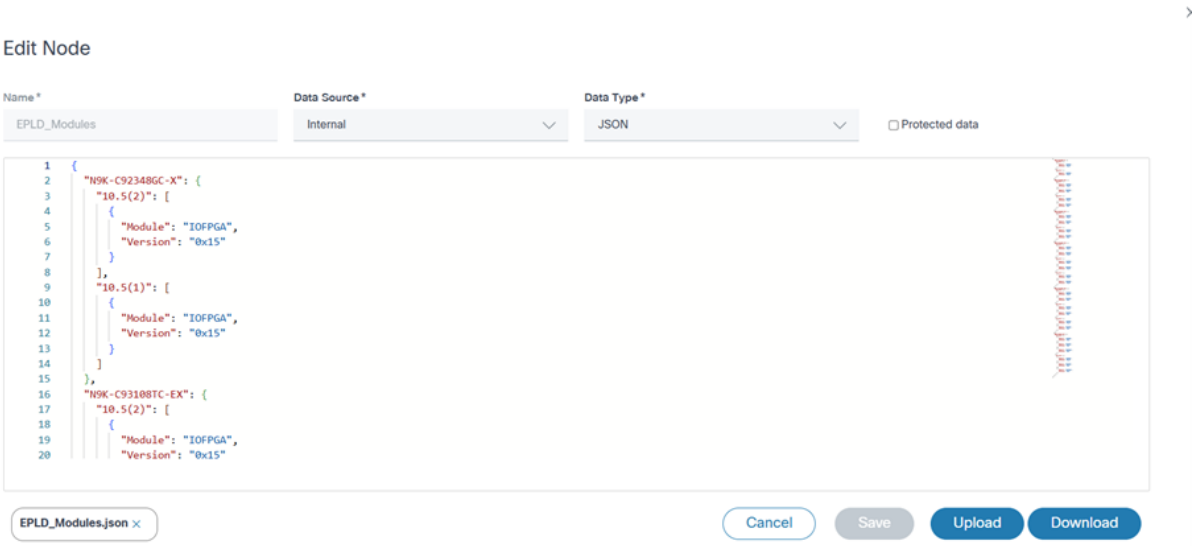
적합성 정책을 생성하기 전에 RefD 응용 프로그램에서 EPLD 모듈 참조 데이터를 생성합니다. RefD 애플리케이션에는 Nexus 소프트웨어 버전 v10.2(8) 및 v10.4(5)에 대한 EPLD 모듈 정보가 각각 포함됩니다. 다른 디바이스 버전의 경우 EPLD 모델 정보를 RefD 응용 프로그램에서 수동으로 추가해야 합니다.

EPLD 모듈 메타데이터에 다른 릴리스를 추가하려면 다음 단계를 완료합니다.



참조 데이터 관리

1. Reference Data Management 응용 프로그램으로 이동하여 "EPLD_Modules"를 검색합니다.
2. "EPLD_Modules" 파일을 선택하고 Edit(편집) 아이콘을 선택합니다.



노드 편집

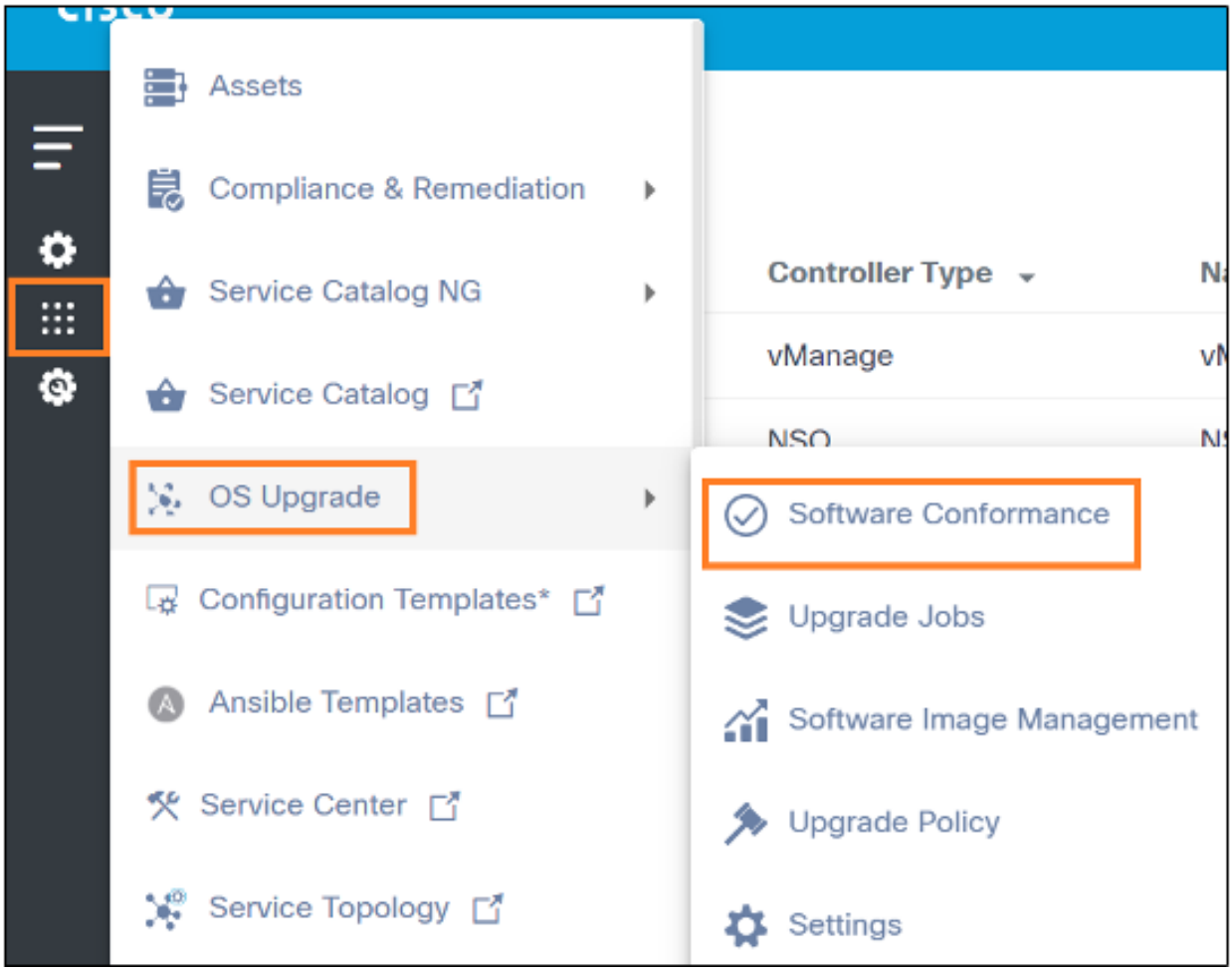
3. 다음 구조의 새 엔트리를 추가하여 새 릴리스 EPLD 모듈 메타데이터를 추가합니다.

```
structure:
  "N9K-C92348GC-X": {
    "10.5(2)": [
      {
        "Module": "IOFPGA",
        "Version": "0x15"
      }
    ]
  }
```

4. Save(저장)를 클릭하고 적합성 정책에서 선택할 수 있는 새 EPLD 모듈 메타데이터를 검증합니다. 지원되는 릴리스에 대한 EPLD 데이터가 미리 채워집니다.

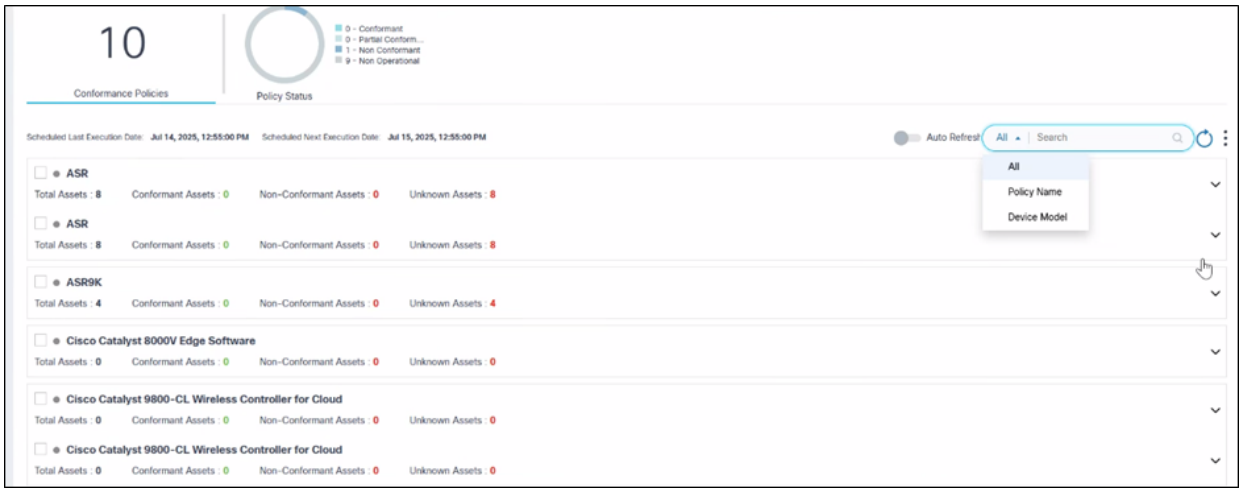
소프트웨어 적합성 보기 및 관리

1. Software Conformance(소프트웨어 적합성)에 액세스할 수 있는 자격 증명을 사용하여 BPA에 로그인합니다.



소프트웨어 적합성 탐색

2. OS Upgrade(OS 업그레이드) > Software Conformance(소프트웨어 적합성)를 선택합니다. Software Conformance 페이지가 표시됩니다.



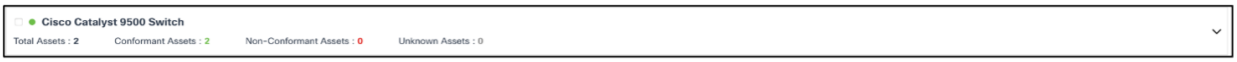
소프트웨어 적합성

Software Conformance 페이지는 다음을 포함합니다.

- 다음을 제공하는 분석 섹션이 맨 위에 표시됩니다.

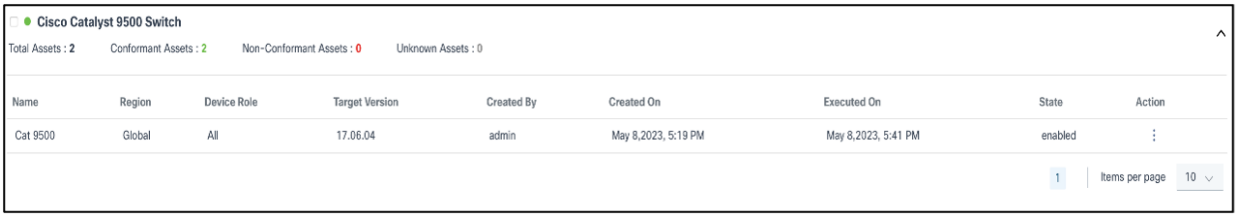
- 시스템에 존재하는 총 적합성 정책 수
- 다음 기준에 따라 필터링할 정책 상태 빠른 필터
    - 준수: 지정된 모델이 있는 모든 BPA 관리 디바이스는 정의된 소프트웨어 버전에 있습니다
    - 부분 적합성: 지정된 모델이 있는 일부 BPA 관리 디바이스는 정의된 소프트웨어 버전에 있습니다. 나머지 디바이스는 서로 다른 소프트웨어 버전에 있습니다
    - 비준수: 지정된 모델이 있는 모든 BPA 관리 디바이스는 지정된 소프트웨어 버전과 비교할 때 서로 다른 소프트웨어 버전에 있습니다
    - 비작동: 정책에 지정된 디바이스 모델을 기반으로 적용 가능한 디바이스를 찾을 수 없습니다
- 이전에 실행된 스케줄링된 적합성 확인의 일자와 시간 및 다음 스케줄링된 적합성 확인이 모든 정책에 대해 이루어지는 시기를 나타내는 스케줄링된 마지막 실행 일자 및 스케줄링된 다음 실행 일자
- 디바이스 모델, 정책 이름 또는 모두를 기반으로 정책을 필터링하는 데 사용되는 검색 필드 사용자는 All(모두)을 선택하여 모든 매개변수를 검색할 수 있습니다.
- Auto Refresh 토글을 사용하면 활성화된 경우 사용자 정의 간격으로 In-Progress 적합성 정책을 자동으로 새로 고칠 수 있습니다. 토글을 활성화하려면
    - 새로 고침 간격을 변경하려면 OS 업그레이드 > 설정으로 이동합니다.
    - 자동 새로 고침 간격을 원하는 값으로 수정합니다
    - Save(저장)를 클릭합니다.
- Auto Refresh(자동 새로 고침) 토글 기능이 활성화된 경우 소프트웨어 적합성 정책 대시보드가 새 간격으로 새로 고쳐집니다.
- 페이지를 새로 고치고 선택한 필터를 지울 수 있는 [새로 고침] 아이콘
- 다음 옵션을 제공하는 추가 옵션 아이콘
    - 정책 생성
    - 모든 정책 실행
    - 선택한 여러 정책 삭제

정책은 장치 모델에 따라 그룹화되고 확장 가능한 패널로 표시되므로 서로 다른 컨트롤러에서 관리하는 장치 모델 전체에 대한 단일 보기를 제공합니다.



컴플라이언스 정책의 축소된 보기

축소된 보기에서는 디바이스 모델 및 Total Assets, Conformant Assets, Non-Conformant Assets , Unknown Assets와 같은 빠른 통계가 표시됩니다.

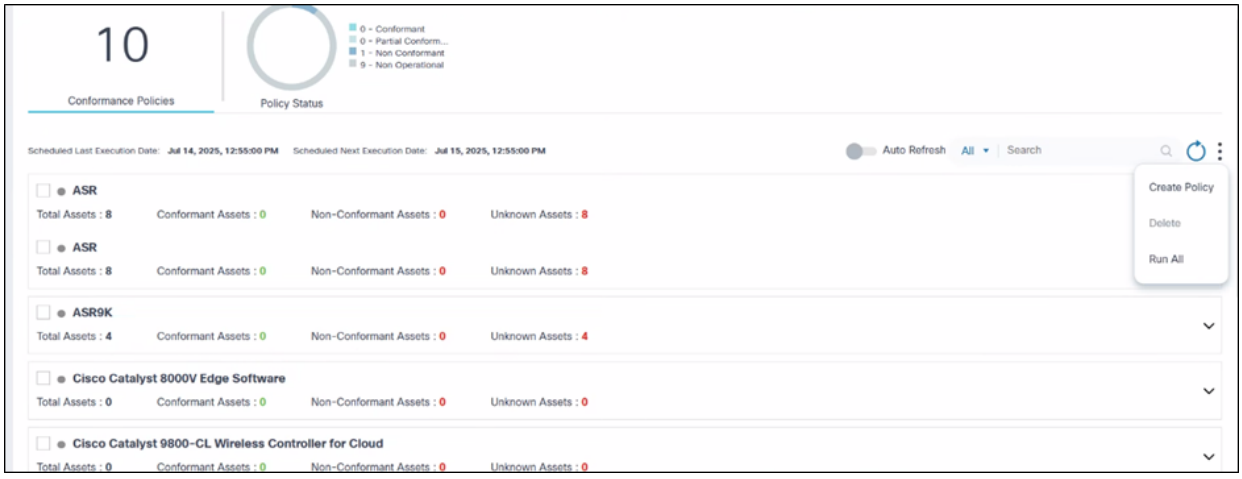


규정 준수 정책의 확장된 보기

확장된 보기에는 디바이스 모델과 관련된 모든 정책이 표시됩니다. 각 정책에 대해 Action(작업) 열에서 More Options(추가 옵션) 아이콘을 선택하여 Run(실행), Edit Policy(정책 수정), View Results(결과 보기) 등의 추가 작업을 수행할 수 있습니다.

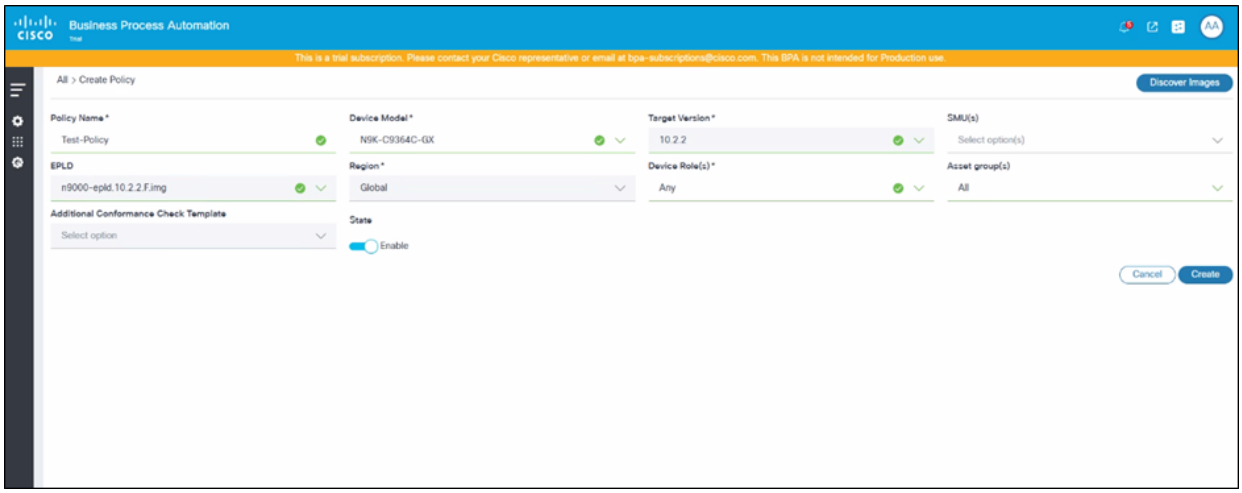
소프트웨어 적합성 정책 생성

1. Software Conformance(소프트웨어 적합성)에 대한 액세스 권한을 관리하는 자격 증명을 사용하여 BPA에 로그인합니다.
2. OS Upgrade(OS 업그레이드) > Software Conformance(소프트웨어 적합성)를 선택합니다. Software Conformance 페이지가 표시됩니다.



정책 생성

3. More Options(추가 옵션) 아이콘 > Create Policy(정책 생성)를 선택합니다.



정책 양식 만들기

4. Policy Name(정책 이름), Device Model(디바이스 모델), Target Version(대상 버전), SMU, EPLD, Device Role(디바이스 역할), Asset Groups(자산 그룹) 및 Additional Conformance Check Template(추가 적합성 확인 템플릿) 필드에 정보를 입력합니다. SMU, 자산 그룹 및 추가 적합성 확인 템플릿은 선택 필드입니다.

참고: 이제 사용자는 Create Conformance Policy(적합성 정책 생성) 양식에서 둘 이상의 디바이스 모델을 선택할 수 있습니다.

참고: 소프트웨어 적합성 프레임워크는 디바이스를 관리하는 특정 모델, 역할 또는 컨트롤러 인스턴스의 디바이스에 대해 기본 OS 버전 및 SMU 패치에 대한 적합성 확인을 실행할 수 있습니다. 추가 사용자 지정 확인이 필요한 경우 Additional Conformance Check Template(추가 적합성 확인 템플릿) 필드에 매핑할 수 있는 필수 명령 및 검증 규칙을 사용하여 프로세스 템플릿을 생성할 수 있습니다.

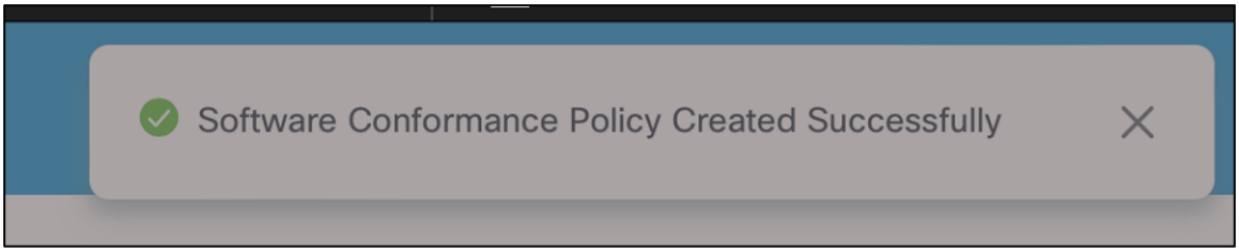
---

5. Create(생성)를 클릭합니다. 확인 메시지가 표시됩니다.

참고: 다음 목록에 유의해야 합니다.

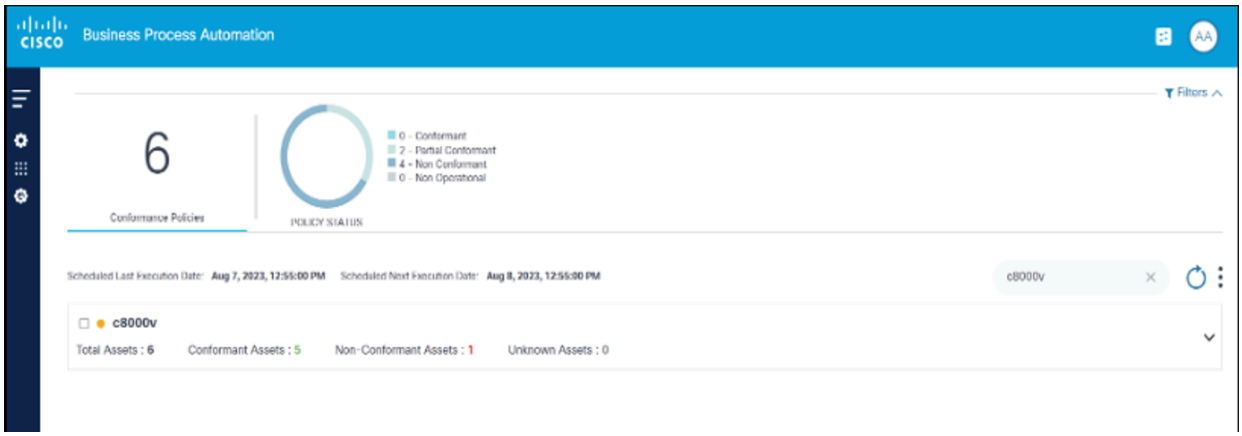
- 활용 사례 관리자는 선택한 장치 모델에 대해 서로 다른 장치 역할로 여러 정책을 유연하게 생성할 수 있습니다. 단일 정책에서 둘 이상의 역할을 선택할 수 있습니다.
- Device Role(s) 드롭다운 목록에서 Any(모두)를 선택하면 다른 모든 디바이스 역할(예: Access, Core 등)이 비활성화됩니다. 다른 디바이스 역할이 선택된 경우 Any가 비활성화됩니다.
- CNC, NSO, ANSIBLE, Direct-to-Device 등의 컨트롤러에서 관리되는 디바이스의 경우 디바이스에 역할 정보가 없으므로 Device Role 드롭다운 목록에서 선택한 Any 역할을 사용하여 규정 준수 확인을 수행할 수 있습니다.
- FMC의 Device Role(s)(디바이스 역할) 드롭다운 목록에서 Any(모두)를 선택하면 독립형, 제어 및 데이터 디바이스를 비롯한 모든 디바이스에서 소프트웨어 적합성이 실행됩니다.

- SMU 적합성 및 업그레이드는 CNC, NSO, ANSIBLE, FMC, Direct-to-Device 및 NDFC 컨트롤러에서만 지원됩니다.
- 이 릴리스에서는 Region 드롭다운 목록의 Global만 지원됩니다
- 사용자는 드롭다운 목록에서 자산 그룹을 선택할 수 있습니다. 기본적으로 모두(All)가 선택됩니다. 사용자는 하나 이상의 자산 그룹을 선택할 수 있습니다. 특정 자산 그룹을 선택하면 선택한 자산 그룹의 디바이스에 대해서만 정책이 실행됩니다.
- Device Model, Target Version, SMU(s) 필드에 대한 예상 값이 표시되지 않으면 Discover Images(이미지 검색)를 클릭하고 다시 시도하십시오.
- Device Model, Asset Group(s) 및 Role 필드가 함께 고유한 정책을 형성합니다. 중복 정책은 허용되지 않습니다.
- EPLD 필드는 선택된 디바이스 모델 및 대상 버전에 대해 EPLD 이미지 메타데이터를 사용할 수 있는 경우에만 값을 채웁니다.
- 정책 이름은 고유하며 중복 정책 이름은 허용되지 않습니다.



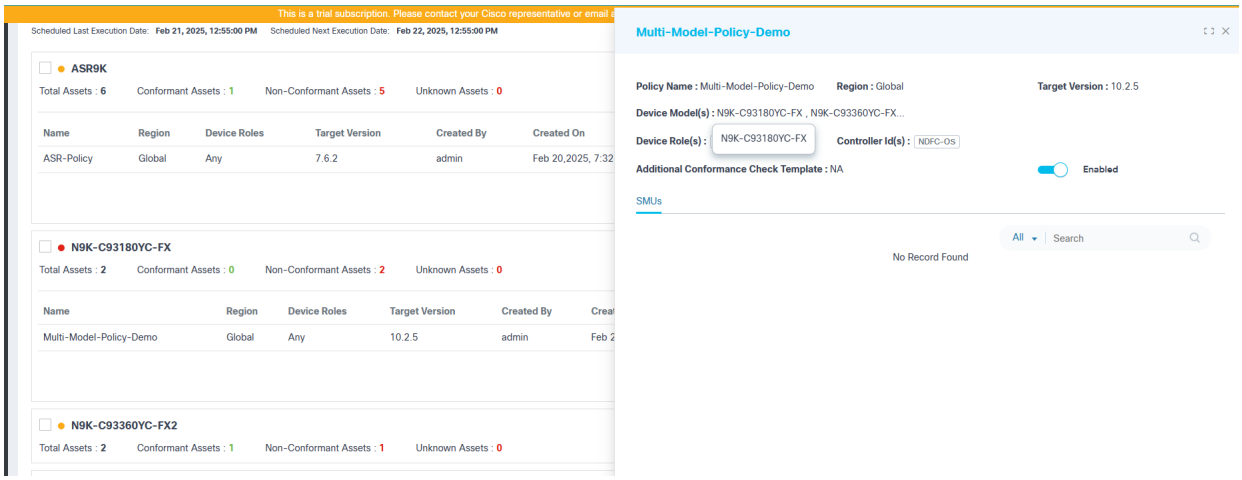
적합성 정책 생성 확인

- OS Upgrade Next Generation(Next-Gen) 태그가 지정된 프로세스 템플릿이 Additional Conformance Check Template(추가 적합성 확인 템플릿) 필드에 표시됩니다.



적합성 정책의 검색 결과

6. Search(검색) 필드에 디바이스 모델을 입력하여 생성된 정책을 찾습니다.

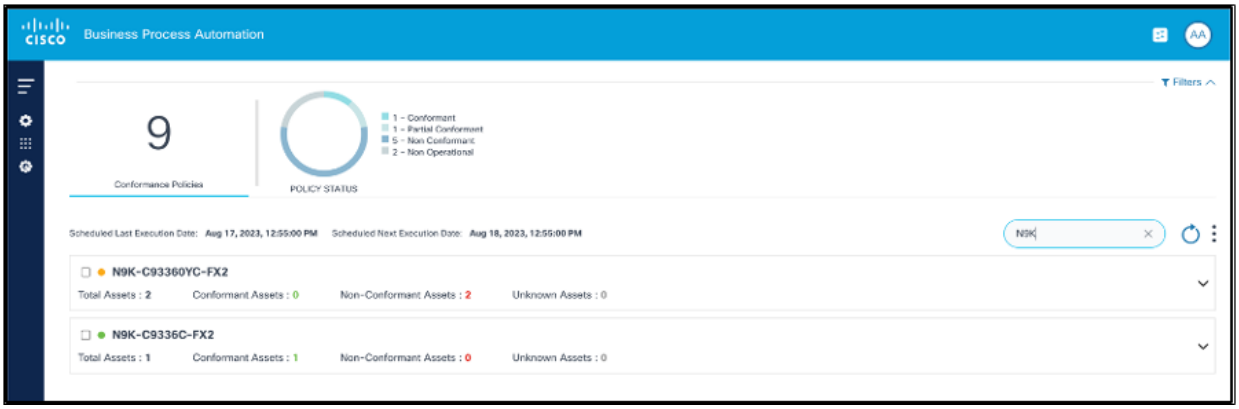


적합성 정책 보기

7. 정책의 세부사항 보기를 보려면 Policy를 클릭합니다.

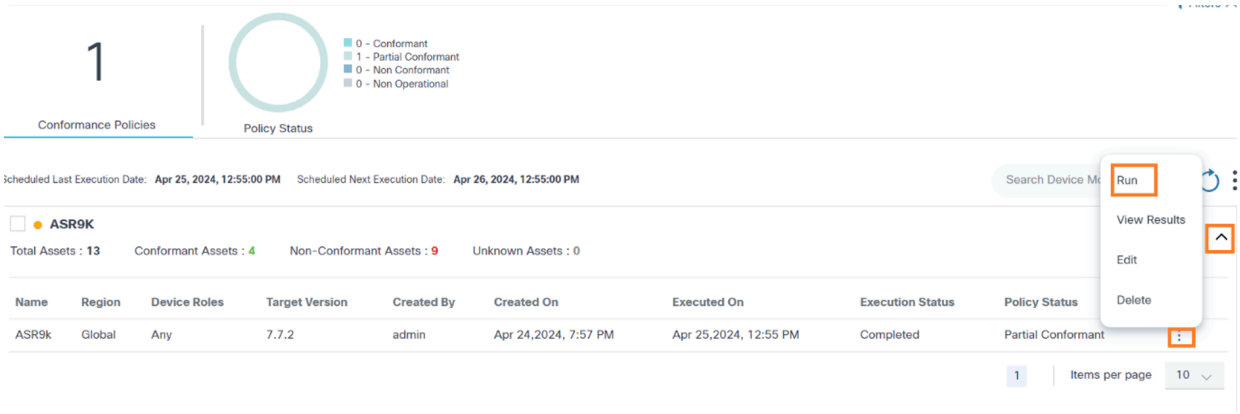
온디맨드 방식으로 소프트웨어 적합성 확인 실행

1. 실행 액세스 권한이 있는 자격 증명으로 BPA에 로그인합니다.
2. OS Upgrade(OS 업그레이드) > Software Conformance(소프트웨어 적합성)를 선택합니다. Software Conformance 페이지가 표시됩니다.



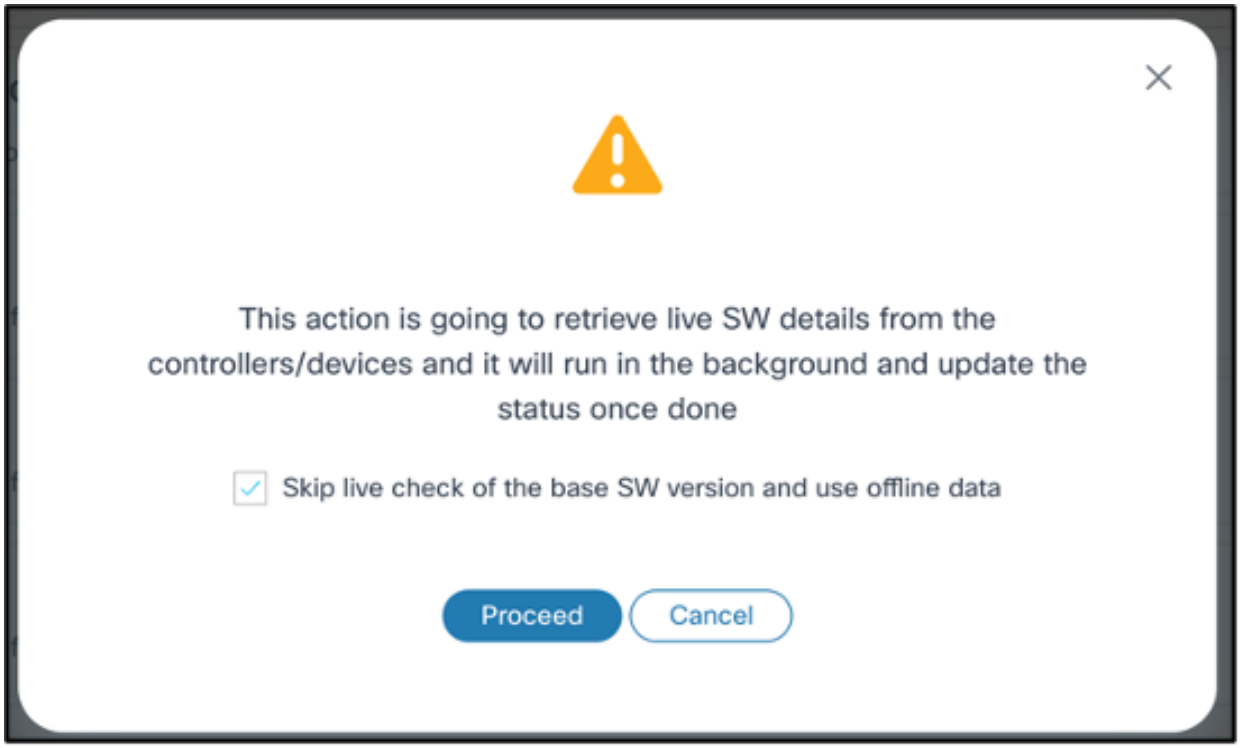
정책 검색

3. Search(검색) 필드를 사용하여 온디맨드 방식으로 실행할 정책을 찾습니다.



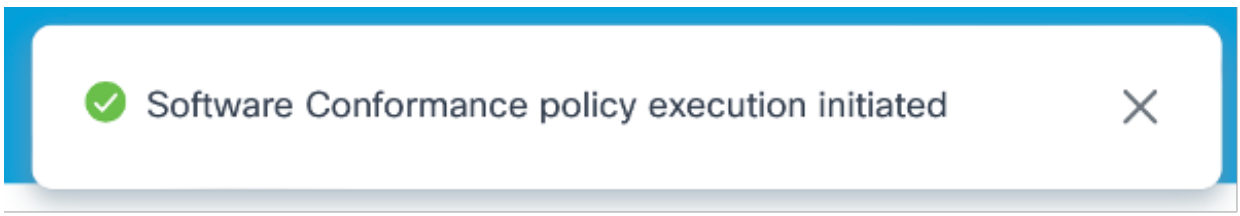
실행

4. 정책의 Action(작업) 열에서 More Options(추가 옵션) > Run(실행)을 선택합니다. 디바이스에 대해 라이브 인벤토리 검사를 수행해야 하는지 여부를 확인하는 확인 메시지가 표시됩니다.



적합성 정책 실행 확인

5. 적합성 확인을 실행하기 전에 실시간 인벤토리 동기화가 필요한 경우 Base SW Version and use offline data 확인란의 Skip Live Check를 지우고 Proceed(계속)를 클릭합니다. 이 경우 적합성 확인은 사후 동기화만 실행됩니다. 오른쪽 상단 모서리에 알림이 표시됩니다.



적합성 정책 실행 알림

참고: 다음 목록에 유의해야 합니다.

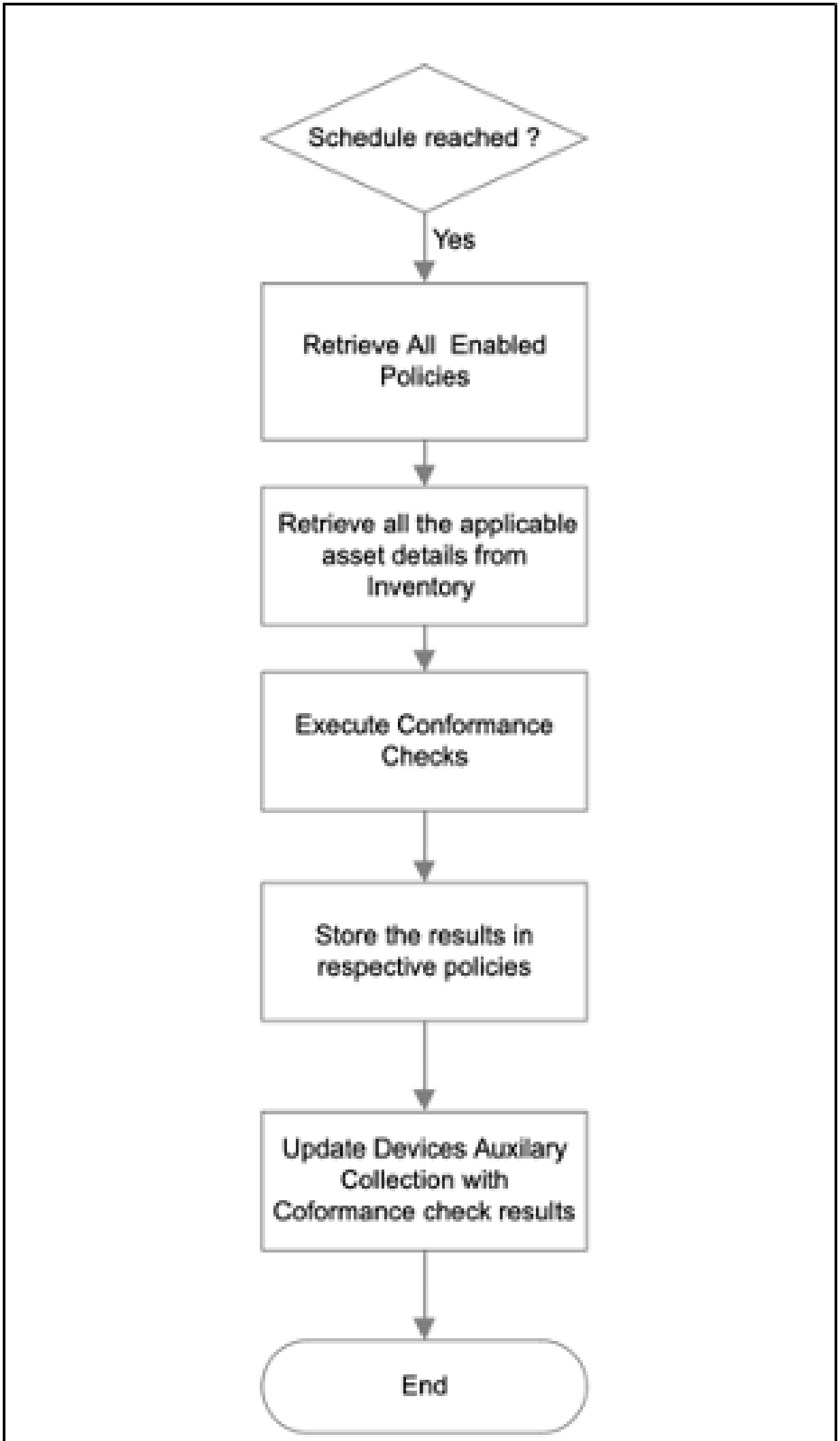
- 적합성 확인은 기본적으로 자산 재고 데이터를 사용하여 수행됩니다.
- 이 프로세스 중에 인벤토리 또는 디바이스 동기화가 실패할 경우 해당 정책 디바이스는 Unknown(알 수 없음)으로 표시되고 SMU 확인을 건너뜁니다.
- SMU의 경우 적합성 검사를 수행하기 전에 디바이스에서 실시간 데이터를 검색한 다음 Base SW Version and use offline data 확인란의 Skip Live Check(기본 SW 버전 및 오프라인 데이터 사용) 확인란을 선택합니다.
- 정책이 여러 디바이스 모델을 포함하는 경우, 디바이스 모델에 대해 해당 정책을 실행하면 모든 관련 정책의 실행이 시작됩니다.

소프트웨어 적합성 확인 실행 예약

일정 관리기 서비스를 사용하여 정기적으로 소프트웨어 적합성 검사를 자동으로 수행할 수 있습니다. 예약된 적합성 확인을 구성하여 다음을 실행할 수 있습니다.

- 매일
- 하루에 두 번
- 매주
- 한 번

일정에 도달하면 Enabled(활성화됨) 상태의 모든 정책이 자동으로 실행되고 적합성 결과가 해당 정책에 저장됩니다.

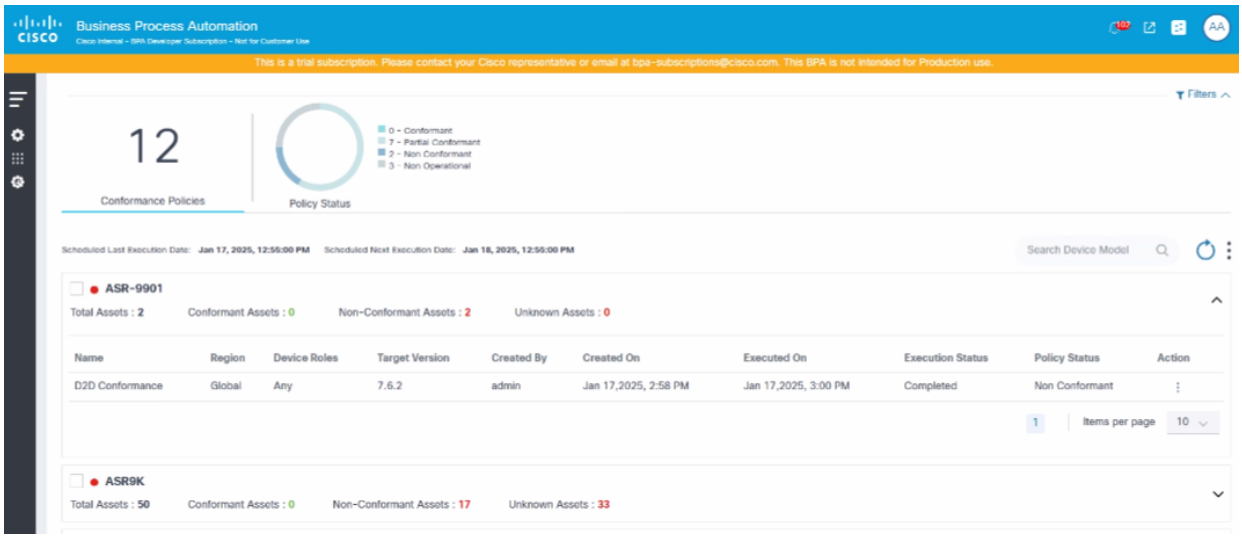

Schedule reached ?
Yes
Retrieve All Enabled Policies
Retrieve all the applicable asset details from Inventory
Execute Conformance Checks
Store the results in respective policies
Update Devices Auxilary Collection with Coformance check results
End

소프트웨어 적합성 검사 예약 실행 통화 흐름

자세한 내용은 [소프트웨어](#) 적합성을 참조하십시오.

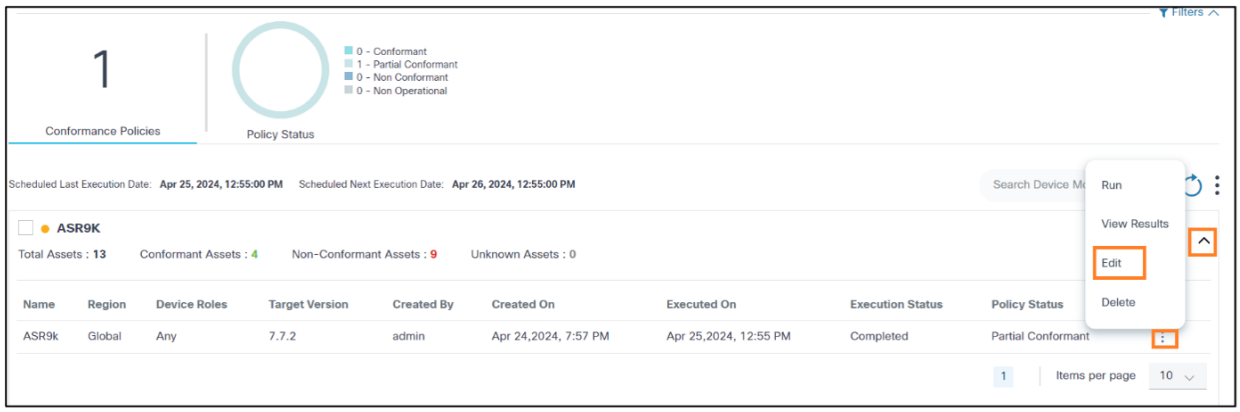
소프트웨어 적합성 정책 업데이트

1. Manage access for Software Conformance(소프트웨어 적합성 관리) 액세스 권한이 있는 자격 증명을 사용하여 BPA에 로그인합니다.
2. OS Upgrade(OS 업그레이드) > Software Conformance(소프트웨어 적합성)를 선택합니다. Software Conformance 페이지가 표시됩니다.



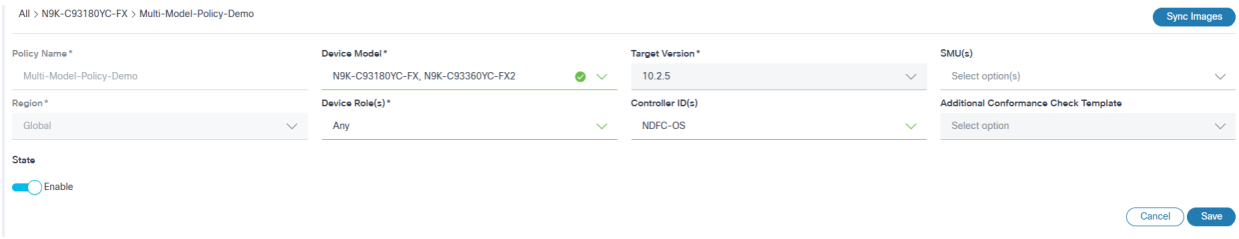
소프트웨어 적합성

3. 원하는 정책을 찾으려면 Search 필드를 사용합니다.



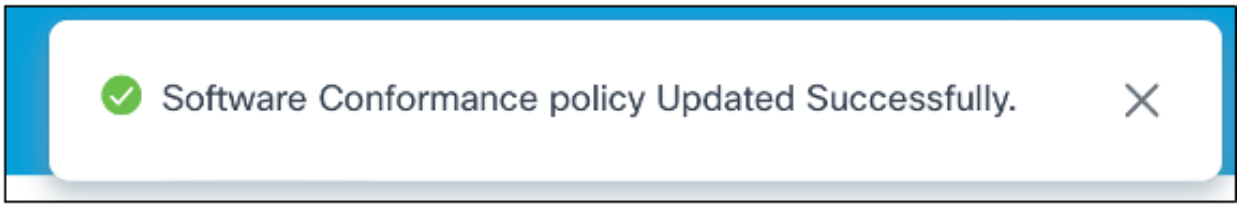
편집

4. 정책의 Action(작업) 열에서 More Options(추가 옵션) 아이콘 > Edit(수정)를 선택합니다.



세부 정보가 채워진 적합성 정책 편집

5. 필요에 따라 대상 버전, SMU, 디바이스 역할, 컨트롤러 ID, 정책 상태 및 추가 적합성 확인 템플릿 필드를 편집합니다.
6. 저장을 클릭합니다. 확인 메시지가 표시됩니다.

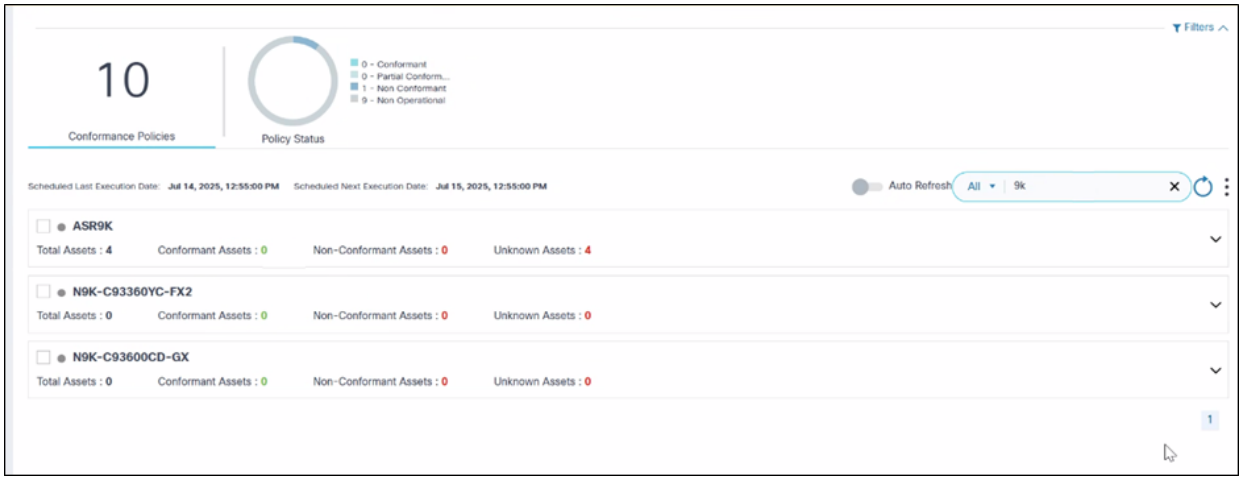


업데이트 성공 확인

참고: 소프트웨어 적합성 정책이 진행 중인 업그레이드 작업에 사용되는 경우 정책을 편집할 수 없습니다.

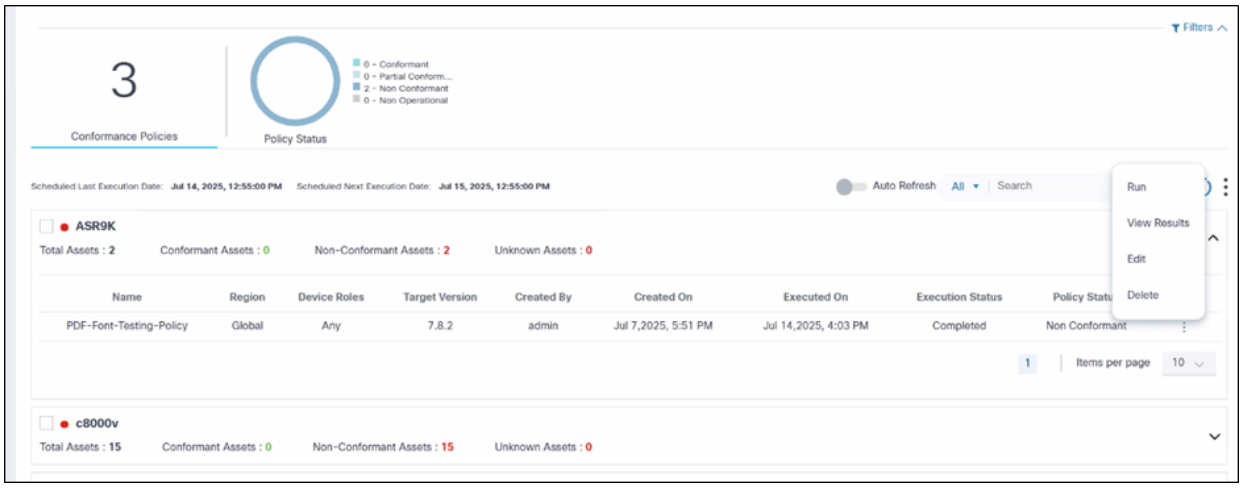
소프트웨어 적합성 정책 삭제

1. 관리 액세스 권한이 있는 자격 증명으로 BPA에 로그인합니다.
2. OS Upgrade(OS 업그레이드) > Software Conformance(소프트웨어 적합성)를 선택합니다. Software Conformance 페이지가 표시됩니다.



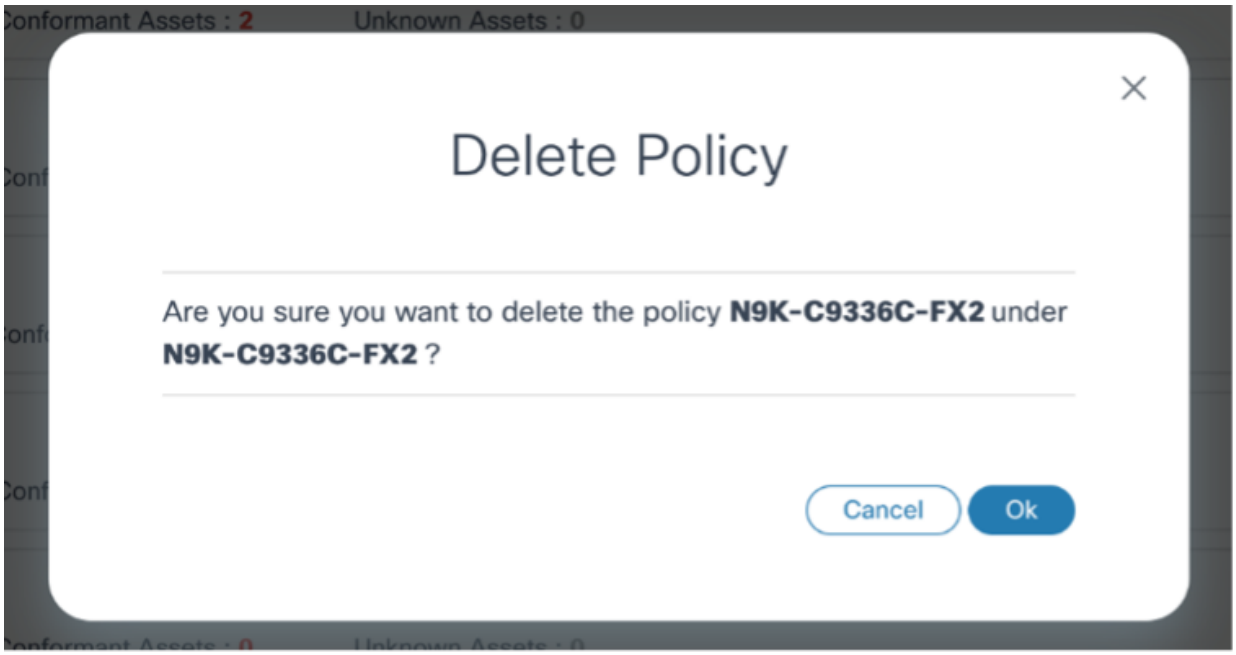
적합성 정책의 검색 결과

3. 원하는 정책을 찾으려면 Search 필드를 사용합니다.

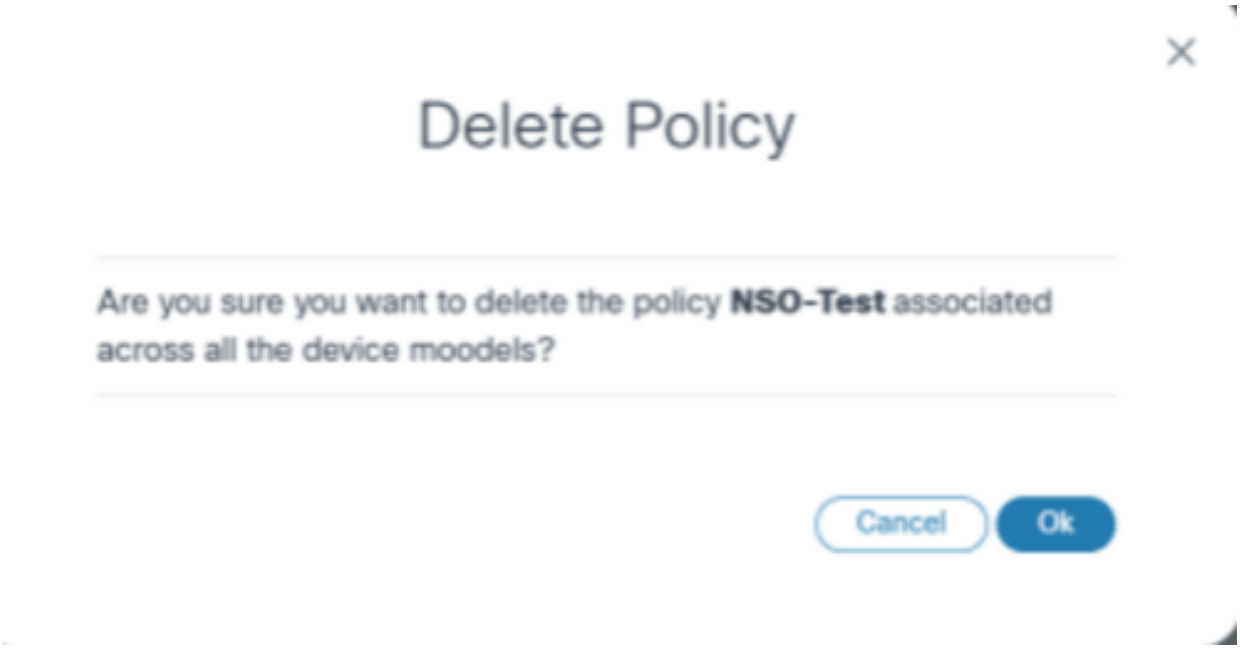


삭제

4. 정책의 Action(작업) 열에서 More Options(추가 옵션) 아이콘 > Delete(삭제)를 선택합니다. 확인 창이 열립니다.



정책 삭제 확인



정책 삭제 확인(정책이 여러 모델과 연결된 경우)

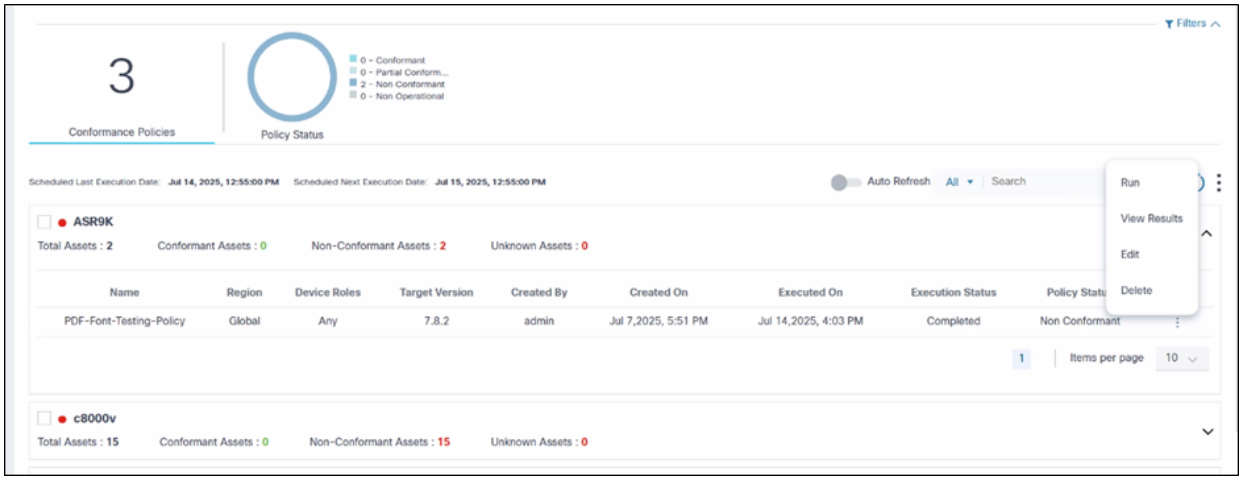
5. OK(확인)를 클릭합니다. 정책이 삭제됩니다.

참고: 다음 목록에 유의해야 합니다.

- 정책이 둘 이상의 디바이스 모델과 연결된 경우, 정책을 삭제하면 연결된 각 모델에 대한 모든 관련 정책이 제거됩니다.
- 진행 중인 업그레이드 작업에 소프트웨어 적합성 정책을 사용하면 해당 정책을 삭제할 수 없습니다.

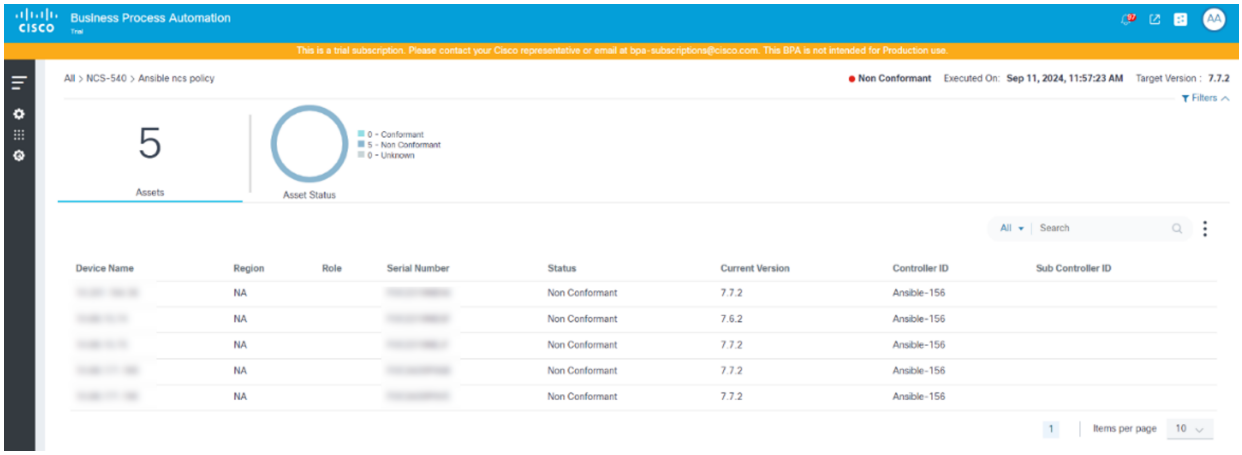
적합성 결과 보기 및 다운로드

정책이 실행되면

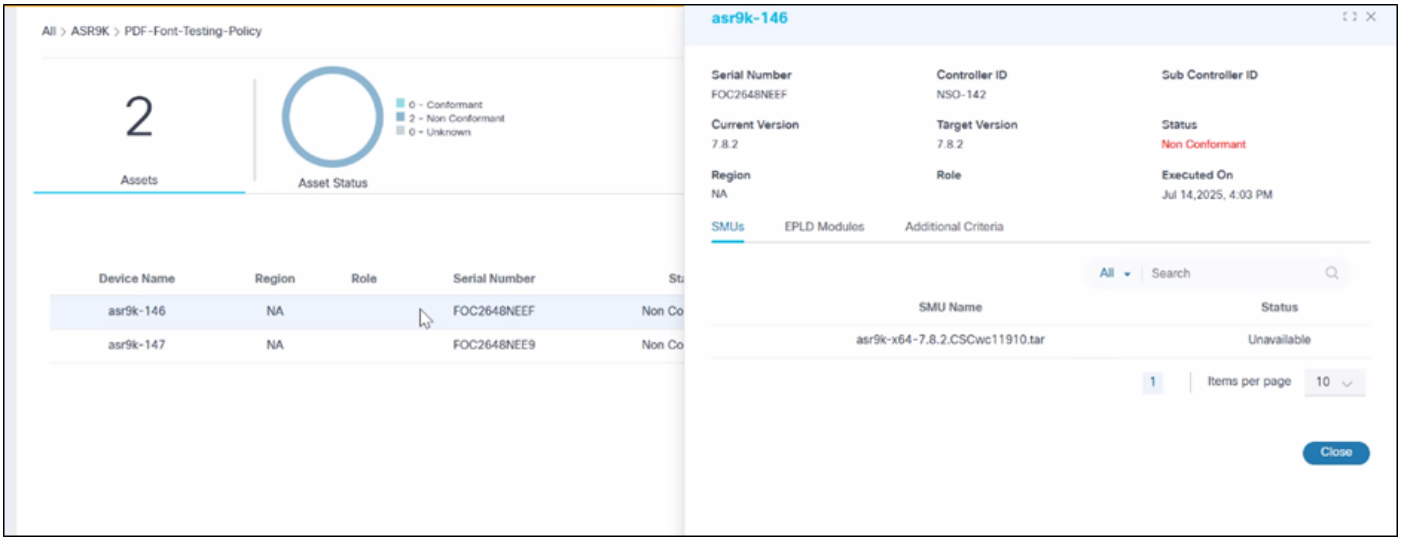


결과 보기 옵션

1. Software Conformance 페이지에서 More Options(추가 옵션) 아이콘 > View Results(결과 보기)를 선택합니다. 사용자가 디바이스의 적합성 상태를 볼 수 있는 Results 페이지가 표시됩니다.



결과 보기



Command Output:

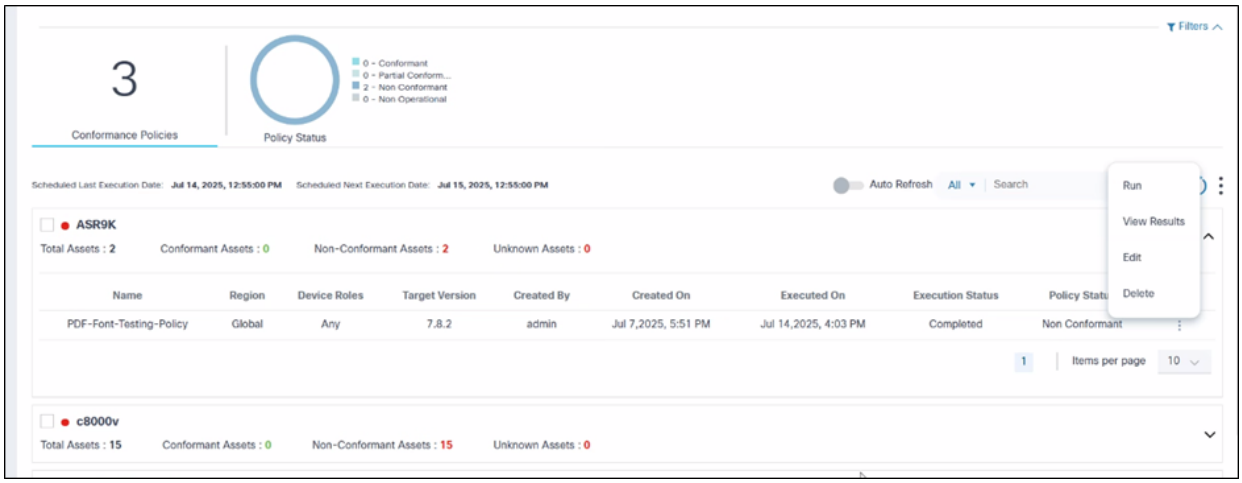
```
Label : 7.7.2

Node 0/RP0/CPU0 [RP]
  Boot Partition: xr_lv32
  Active Packages: 11
        ncs540-xr-7.7.2 version=7.7.2 [Boot image]
        ncs540-lictrl-1.0.0.0-r772
        ncs540-mpls-1.0.0.0-r772
        ncs540-li-1.0.0.0-r772
        ncs540-mgbl-1.0.0.0-r772
        ncs540-isis-1.0.0.0-r772
        ncs540-ospf-1.0.0.0-r772
        ncs540-k9sec-1.0.0.0-r772
        ncs540-mcast-1.0.0.0-r772
        ncs540-mpls-te-rsvp-1.0.0.0-r772
        ncs540-eigrp-1.0.0.0-r772

Node 0/0/CPU0 [LC]
  Boot Partition: xr_lcp_lv32
  Active Packages: 11
        ncs540-xr-7.7.2 version=7.7.2 [Boot image]
        ncs540-lictrl-1.0.0.0-r772
        ncs540-mpls-1.0.0.0-r772
        ncs540-li-1.0.0.0-r772
        ncs540-mgbl-1.0.0.0-r772
```

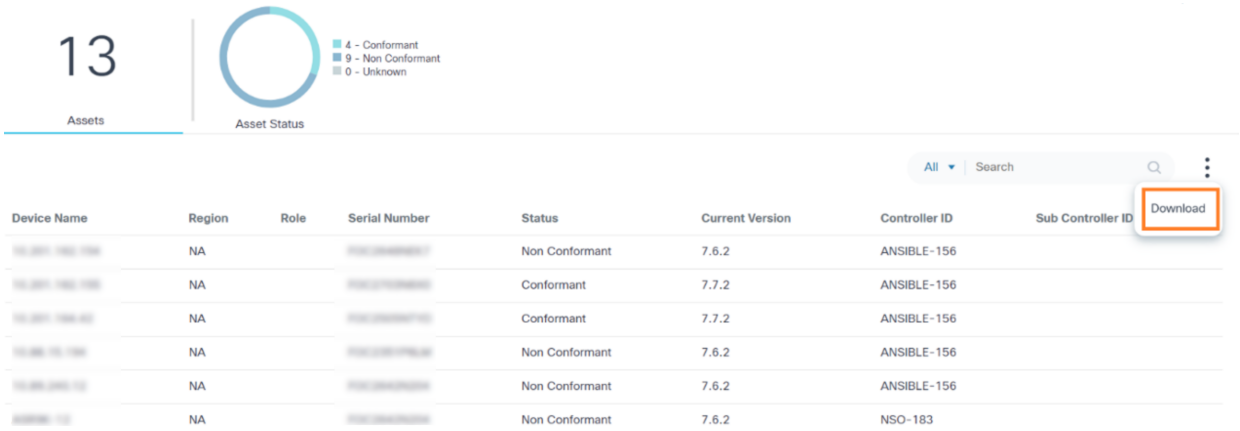
2. 행을 선택하여 SMU 상태 및 추가 기준과 함께 특정 자산 상세내역을 표시합니다.

참고: NSO, CNC, ANSIBLE, Direct-to-Device 및 NDFC 컨트롤러 자산에 대해서만 SMU 세부 사항이 표시됩니다. EPLD 모듈은 NDFC 컨트롤러에만 표시됩니다.



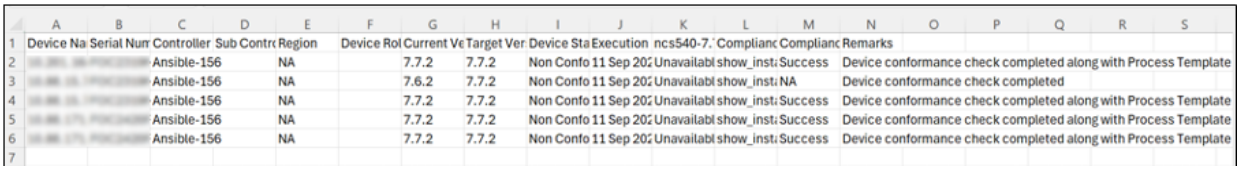
결과 보기

3. 디바이스의 Action(작업) 열에서 More Options(추가 옵션) 아이콘 > View Results(결과 보기)를 선택합니다.



다운로드

4. More Options(추가 옵션) 아이콘 > Download(다운로드)를 선택하여 SMU 가용성 상태의 결과를 .csv 형식으로 다운로드합니다.



Excel 시트 보기

참고: 결과 조회는 가장 최근에 실행된 적합성 검사의 결과만 표시합니다. 사용자는 액세스 권한이 있는 자산만 볼 수 있습니다. 비운영 정책의 경우 View Results(결과 보기)가 비활성화됩니다.

가능한 장치 상태:

- 준수: 디바이스가 정의된 정책을 준수함을 나타냅니다.
- 비준수: 다음 조건을 충족하면 디바이스가 적합하지 않음을 나타냅니다.

대상 버전	스무	컴플라이언스 검사	상태
부적합	해당 없음	해당 없음	부적합
적합하	사용할 수 없음	규칙 실패	부적합
적합하	사용 가능	규칙 실패	부적합
적합하	사용할 수 없음	규칙 성공	부적합

- 알 수 없음: 디바이스에 현재 소프트웨어 버전 정보가 없기 때문에 디바이스 소프트웨어 적합성 검사를 수행할 수 없음을 나타냅니다.

알 수 없음 상태의 기준은 다음과 같습니다.

대상 버전	스무	EPLD	컴플라이언스 검사	상태
부적합	해당 없음	해당 없음	해당 없음	부적합
적합하	사용할 수 없음	부적합	규칙 실패	부적합
적합하	사용할 수 없음	적합하	규칙 실패	부적합
적합하	사용 가능	적합하	규칙 실패	부적합
적합하	사용 가능	부적합	규칙 실패	부적합
적합하	사용할 수 없음	적합하	규칙 성공	부적합
적합하	사용할 수 없음	적합하	규칙 성공	부적합

가능한 SMU 상태:

- 사용 가능: SMU가 디바이스에 있고 활성 상태임을 나타냅니다.
- 사용할 수 없음: SMU가 없거나 있지만 비활성 상태임을 나타냅니다.

가능한 EPLD 모듈 상태:

- 준수: EPLD 모듈이 예상 대상 버전과 함께 장치에 있음을 나타냅니다.
- 비준수: EPLD 모듈이 예기치 않은 대상 버전을 가진 장치에 있음을 나타냅니다.
- 누락된 모듈: EPLD 모듈이 장치에서 구성되거나 가입되지 않았음을 나타냅니다.

가능한 규정 준수 검사 템플릿 상태:

- 성공: 디바이스가 유효한 명령 및 규칙으로 프로세스 템플릿을 성공적으로 실행했음을 나타냅니다.
- 실패: 디바이스가 프로세스 템플릿을 실행하지 못했음을 나타냅니다(예: 명령이 잘못된 경우).
- 해당 없음: 디바이스가 프로세스 템플릿을 실행할 자격이 없음을 나타냅니다(예: 디바이스가 정의된 대상 버전과 호환되지 않는 경우).

참고: 다음 목록에 유의해야 합니다.

- 소프트웨어 적합성 확인은 기본 테넌트에 속한 디바이스에서만 작동합니다
- 소프트웨어 적합성 확인은 디바이스의 현재 소프트웨어 버전에 대한 진실의 소스로서 자산 인벤토리를 사용합니다. 자산 인벤토리 데이터가 오래된 경우 소프트웨어 적합성 확인 결과가 오래된 것입니다. 부실 데이터 문제를 방지하려면 적합성 정책 실행을 시작할 때 실시간 인벤토리 확인 기능을 사용합니다
- OS Upgrade > Settings > Software Conformance에서 기본 일정을 변경할 수 있습니다
- BPA 5.1로 업그레이드한 후에는 기존의 모든 정책이 비활성화 상태로 이동됩니다. 사용자는 각 정책을 수정하고 적절한 값을 선택하고 활성화한 다음 추가 사용을 위해 변경 사항을 저장해야 합니다

업그레이드 정책

업그레이드 정책 구성 요소는 두 가지 유형의 정책을 지원합니다.

- 단일 단계 정책:
  - 모두
  - <특정 소스 버전(7.7.1)> - <특정 대상 버전(7.7.2)>
- 다단계 정책:
  - v7.7.1 - 7.7.2
  - v7.7.2 - 7.7.8
- 다단계 업그레이드에는 아래 예제와 같이 Bridge SMU가 포함될 수 있습니다.
  - v7.7.1 - v7.7.1[브리지 SMU]
  - V7.7.1[브리지 SMU] - 7.7.8

업그레이드 정책 구성 요소는 다음 플랫폼별 아티팩트를 사전 정의할 수 있는 유연성을 제공합니다
.

- 업그레이드 경로
- 사전/사후 검증 템플릿 또는 워크플로
- 배포 워크플로
- 활성화 워크플로
- 백업 워크플로
- 시간 초과 값
- 롤백 워크플로
- 유효한 사전 및 사후 차이
- 트래픽 전환 워크플로 또는 트래픽 전환 워크플로

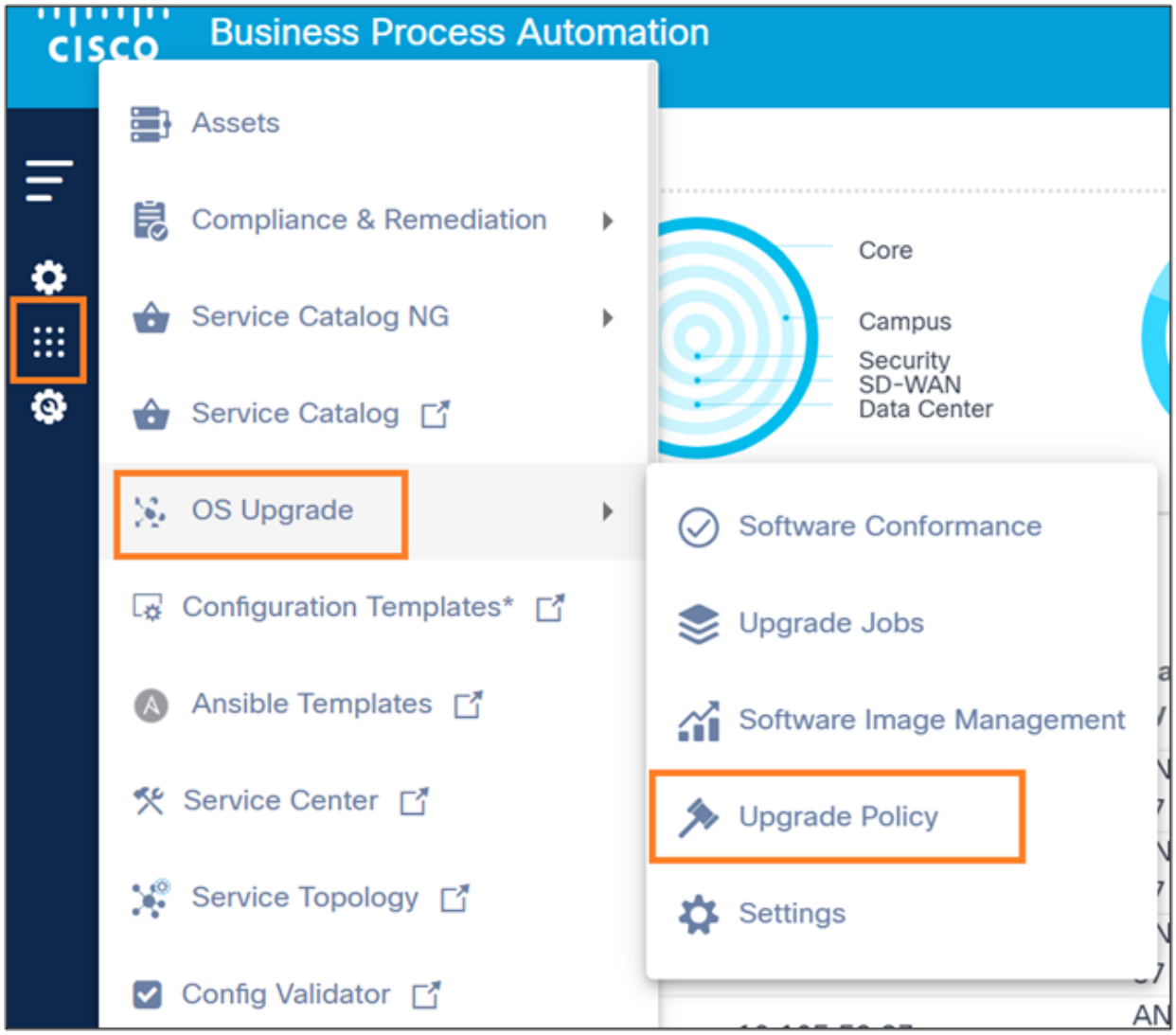
사전 요구 사항

- 필수 사전/사후 검증 프로세스 템플릿 또는 워크플로
- 필요한 백업, 배포, 활성화 및 롤백 워크플로
- 필요한 이미지 메타데이터

업그레이드 정책 보기 및 관리

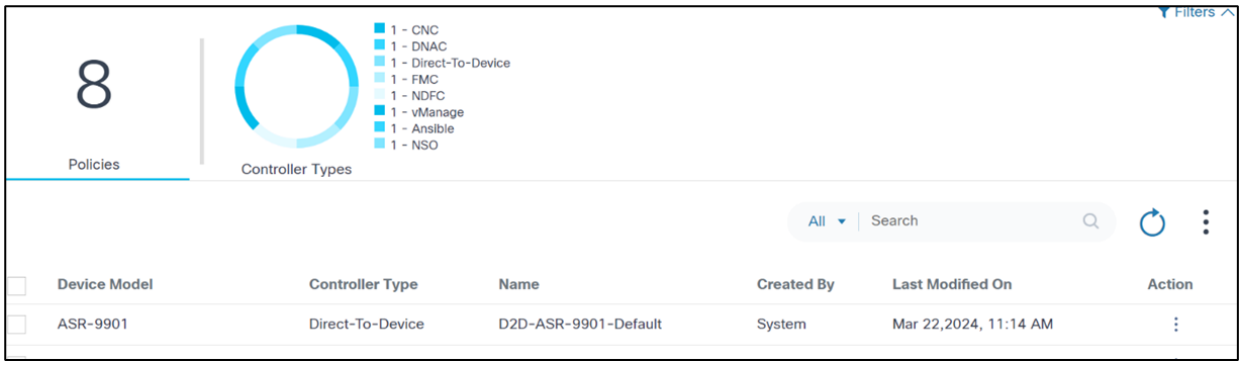
Upgrade Policy(업그레이드 정책) 페이지에 액세스하려면 다음을 수행합니다.

1. 업그레이드 정책에 액세스할 수 있는 자격 증명을 사용하여 BPA에 로그인합니다.



업그레이드 정책 탐색

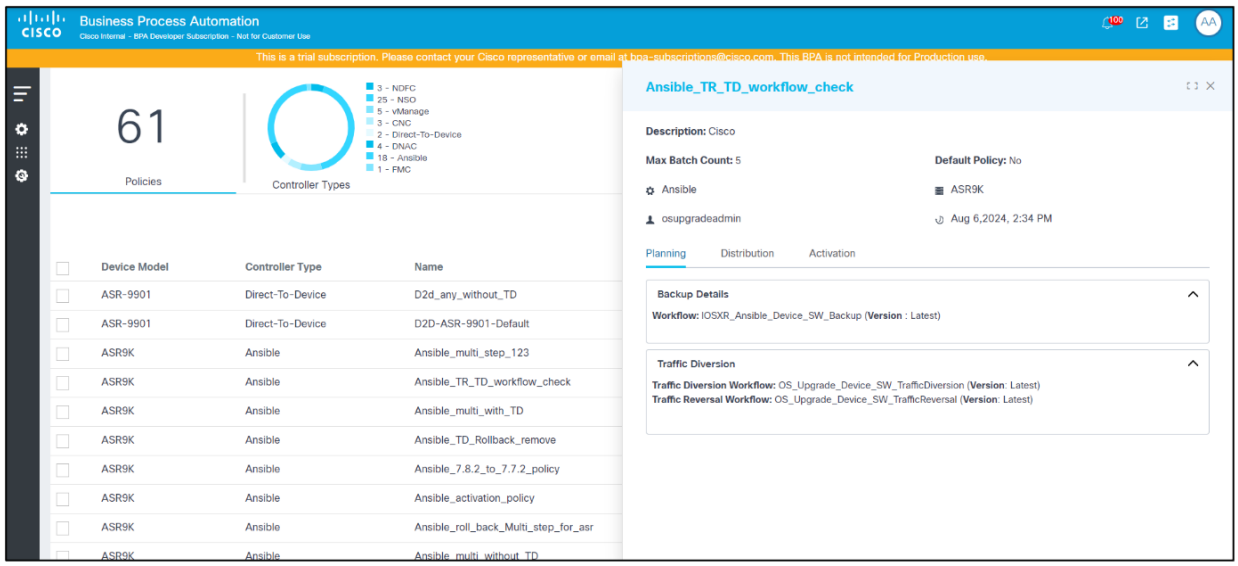
2. OS Upgrade > Upgrade Policy를 선택합니다. Upgrade Policy 페이지가 표시됩니다.



업그레이드 정책

Upgrade Policy 페이지는 다음을 포함합니다.

- 다음을 제공하는 분석 섹션이 맨 위에 표시됩니다.
  - 시스템의 총 업그레이드 정책 수
  - 컨트롤러 유형별로 필터링할 수 있는 기능을 제공하는 컨트롤러 유형 빠른 필터
- More Options(추가 옵션) 아이콘 - Create Policy(정책 생성) 및 Delete All Selected Policies(선택한 모든 정책 삭제)와 같은 대량 처리 작업에 대한 옵션을 제공합니다.
- 검색 필터는 다음과 같이 필터링할 수 있는 정책을 검색합니다.
  - 모두: 모든 필드 검색
  - 디바이스 모델: 지정된 모델이 있는 정책 검색
  - 이름: 지정된 정책 이름의 정책 검색
  - 작성자: 지정된 사용자로 정책 검색
- 해당 열 이름 또는 테이블 필드를 클릭하여 정책을 정렬합니다.



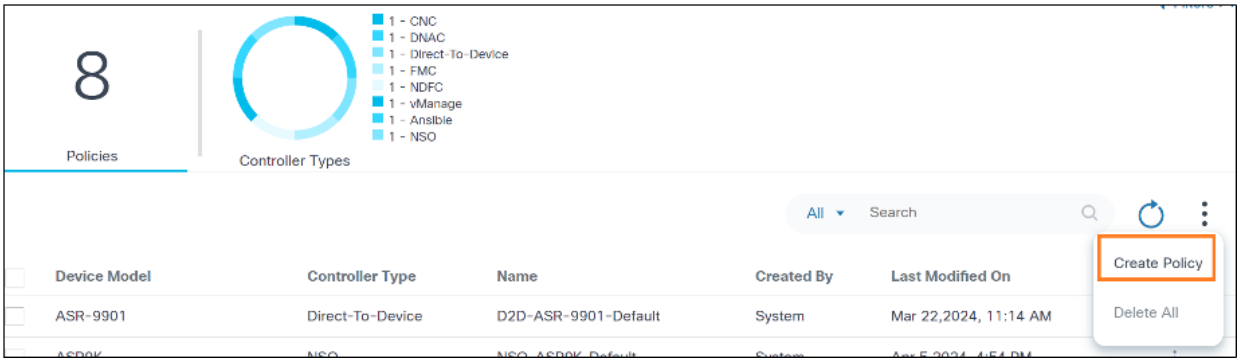
정책 세부 정보 보기

- 특정 정책 또는 정책의 세부 정보 보기 행 클릭

참고: 정책 이름이 고유한 경우 동일한 디바이스 모델 및 컨트롤러 유형에는 원하는 수의 정책이 있을 수 있습니다.

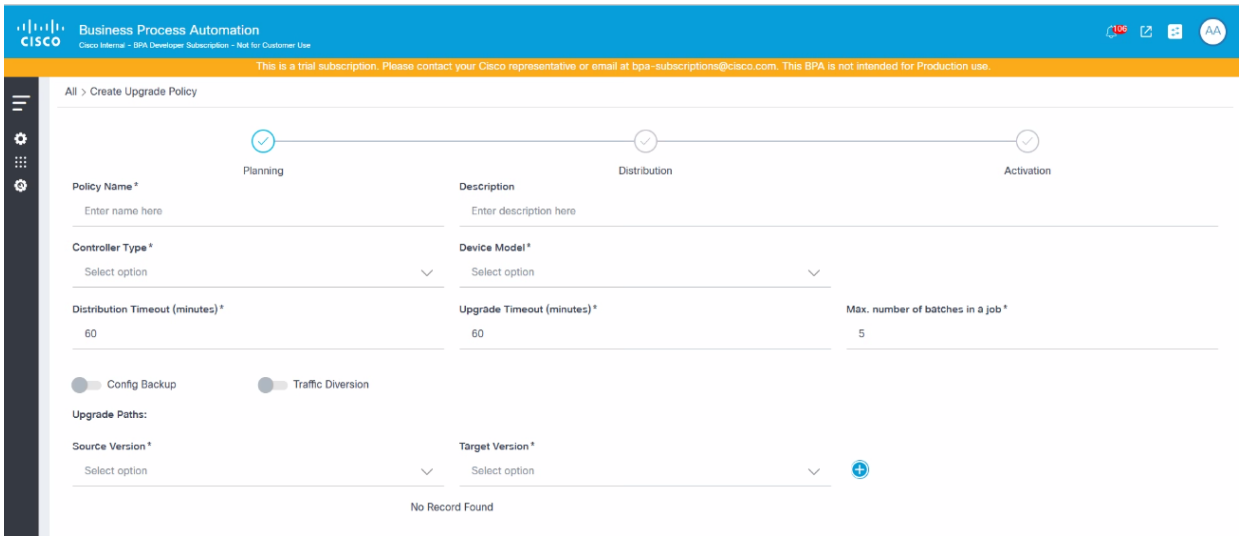
업그레이드 정책 생성

1. 업그레이드 정책에 대한 관리 액세스 권한이 있는 자격 증명으로 BPA에 로그인합니다.
2. OS Upgrade > Upgrade Policy를 선택합니다. Upgrade Policy 페이지가 표시됩니다.



정책 생성

3. More Options(추가 옵션) > Create Policy(정책 생성)를 선택합니다. Create Upgrade Policy 페이지가 표시됩니다.



업그레이드 정책 생성

계획

1. 전체 정책과 관련된 매개변수를 구성합니다. 아래 표에는 각 필드에 대한 간략한 설명이 나와 있습니다.

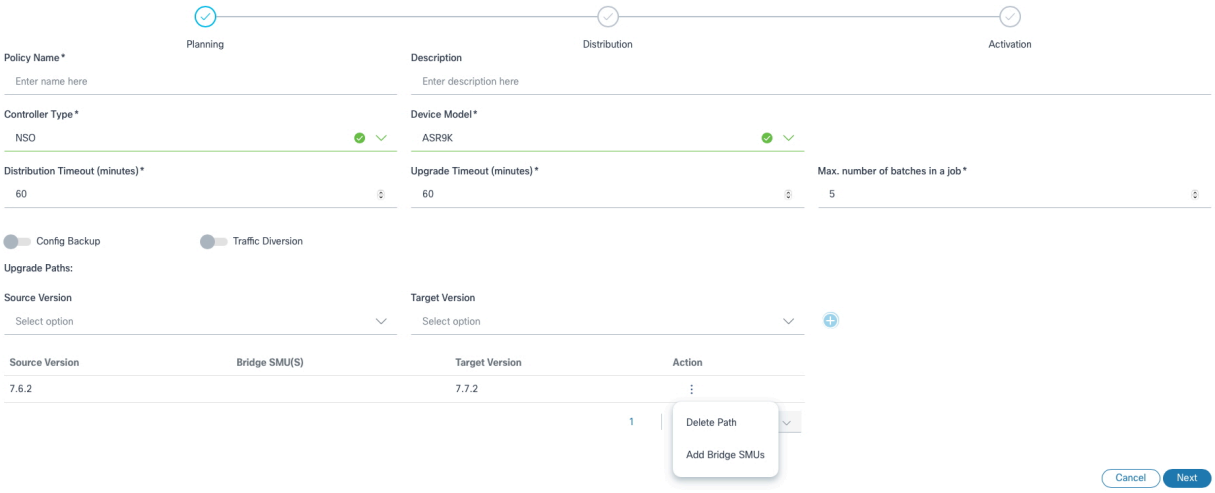
필드	설명
정책 이름	정책의 이름
설명	정책에 대한 간략한 설명
컨트롤러 유형	OS 업그레이드를 수행하는 데 사용되는 적절한 컨트롤러
디바이스 모델	OS 업그레이드를 수행하는 데 사용되는 디바이스 모델
배포 시간 초과(분)	이미지 배포 작업의 최대 대기 시간(분)
업그레이드 시간 초과(분)	이미지 활성화 활동의 최대 대기 시간(분)
작업의 최대 일괄 처리 수	작업에 추가할 수 있는 일괄 처리 수 허용되는 최대 배치 수는 20개입니다.
구성 백업 토글	백업이 필요한 경우 이 토글을 활성화하고 vManage 및 Direct-to-Device 컨트롤러에 대한 창에서 다음 필드를 완료합니다. - 워크플로 이름: 해당 백업 워크플로 참고: 워크플로를 찾을 수 없는 경우 워크플로에 OS 업그레이드 NextGen 태그가 올바르게 지정되었는지 확인합니다 - 최신 워크플로 사용: 이 옵션을 선택하면 선택한 워크플로의 최신 버전이 사용됩니다 - 워크플로 버전: 맞춤형 워크플로 버전; 최신 워크플로 사용을 선택하지 않은 경우에만 선택할 수 있습니다. NDFC, NSO, CNC 및 Cisco Catalyst Center 컨트롤러의 경우 백업 및 복원 서비스를 통해 백업이 수행됩니다. 따라서 백업 및 복원 정책은 Backup details(백업 세부 정보) 창에서 선택해야 합니다. 참고: 사용자는 컨트롤러 유형에 적합한 정책을 선택해야 합니다. 백업 및 복원 정책에 대한 자세한 내용은 백업 및 복원 섹션을 참조하십시오.
트래픽 전환 토글	Nexus 디바이스에 대한 백업을 활성화하려면 대상 디바이스에 기능 scp-server 컨피그레이션이 있어야 합니다. 트래픽 전용이 필요한 경우 이 토글을 활성화하고 Traffic Diversion(트래픽 전용) 창에서 다음 필드를 완료합니다.

필드	설명
업그레이드 경로	- 트래픽 전환 워크플로: 적용 가능한 트래픽 전환 워크플로입니다. 참고: 워크플로를 찾을 수 없는 경우 워크플로에 OS 업그레이드 NextGen 태그가 올바르게 지정되었는지 확인합니다 - 트래픽 전환 워크플로: 적용 가능한 트래픽 전환 워크플로입니다. 참고: 워크플로를 찾을 수 없는 경우 워크플로에 OS 업그레이드 NextGen 태그가 올바르게 지정되었는지 확인합니다 - 최신 워크플로 사용: 위에서 선택한 워크플로의 최신 버전 - 워크플로 버전: 맞춤형 워크플로 버전; 최신 워크플로 사용을 선택하지 않은 경우에만 선택할 수 있습니다. 업그레이드 경로는 적용 가능한 단계 업그레이드 경로를 정의합니다. 다양한 수요를 수용하기 위해 다음 필드에 여러 소스 및 대상 버전을 추가할 수 있습니다 - 소스 버전: 업그레이드 경로의 시작 버전 - 대상 버전: 업그레이드 경로의 끝 버전 - 소스 버전(Any)에서 대상 버전(Any)으로: 이 옵션은 Source Version 및 Target Version 필드에 대해 모두 Any를 선택하여 사용할 수 있습니다. 이는 모든 디바이스 모델의 기본값입니다. 이 시나리오에서는 Distribution and Activation 페이지에서 업그레이드를 위한 통합 프로세스를 제공합니다 - 소스 버전(특정 버전)에서 대상 버전(특정 버전)으로: 디바이스 모델에 사용할 수 있는 특정 이미지 버전을 선택하여 사용할 수 있습니다. 여러 소스 및 대상 버전을 추가할 수 있습니다. 배포 및 활성화 업그레이드 프로세스 입력 수는 추가된 소스 및 대상 버전 수와 일치하며, 각각은 해당 소스 및 대상 버전으로 레이블이 지정된 축소 가능한 섹션으로 표시됩니다. 업그레이드 경로를 사용하려면 소스 버전에 필수 SMU를 적용한 후 해당 업그레이드 경로에 Bridge SMU로 추가하여 타겟 버전으로 업그레이드해야 합니다. 브리지 SMU에 대한 자세한 내용은 다음 섹션을 참조하십시오.

브리지 SMU

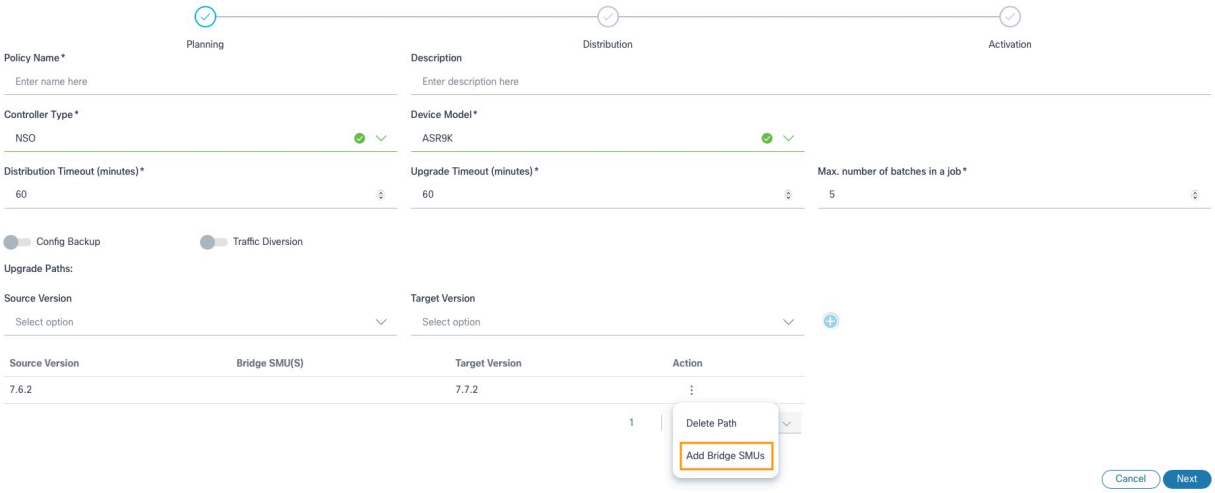
필수 업그레이드 또는 다운그레이드 SMU라고도 하는 Bridge SMU는 필수 구성 요소이며, 동일한 플랫폼이나 모델의 다른 소프트웨어 릴리스로 업그레이드하거나 다운그레이드하기 전에 설치해야 합니다.

업그레이드 경로에 브리지 SMU 추가



업그레이드 경로 옵션

1. 업그레이드 경로를 추가한 후 More Options(추가 옵션) 아이콘을 선택합니다. Delete Path(경로 삭제) 및 Add Bridge SMUs(브리지 SMU 추가) 옵션이 표시됩니다.



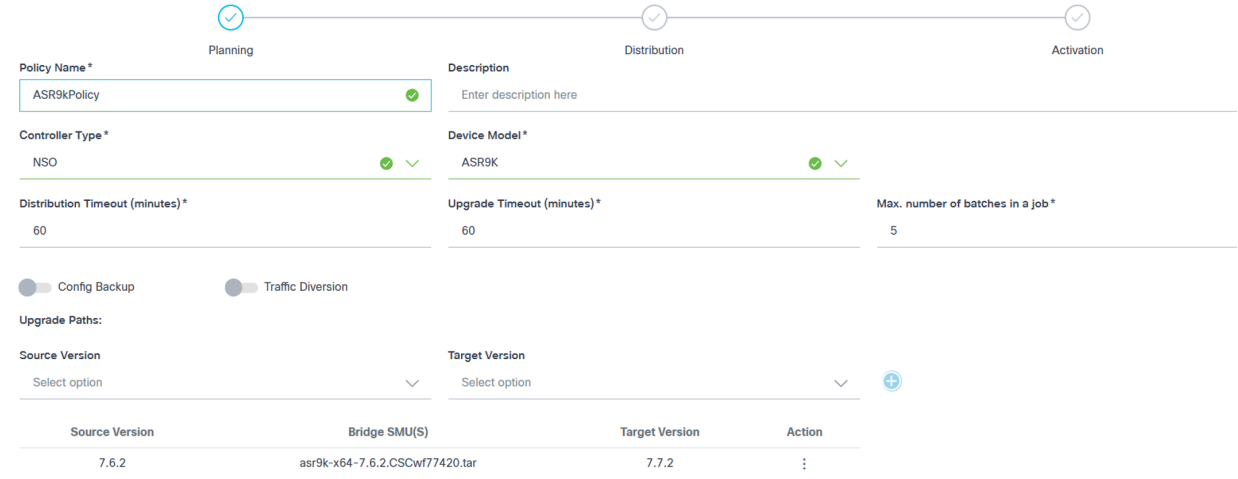
브리지 SMU 추가

2. Add Bridge SMUs(브리지 SMU 추가)를 선택합니다. Add Bridge SMUs 창이 열립니다. 지정

된 업그레이드 경로에 대해 사용 가능한 모든 브리지 SMU가 표시됩니다.

브리지 SMU 추가

3. Add Bridge SMUs(브리지 SMU 추가) 창에서 브리지 SMU를 추가할 확인란을 선택하거나 제거할 확인란을 선택 취소합니다. 브리지 SMU를 추가하면 업그레이드 경로가 선택한 브리지 SMU 세부 정보로 업데이트됩니다.



Bridge SMU를 사용한 업그레이드 경로

참고: Bridge SMU가 포함된 각 업그레이드 경로는 업그레이드 과정에서 2단계 업그레이드로 간주됩니다. 위 그림에 나와 있는 업그레이드 경로의 최종 업그레이드 경로는 다음과 같습니다.

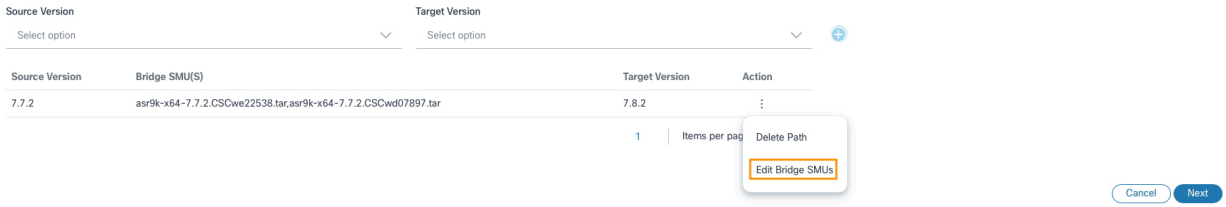
- 7.6.2 - 7.6.2 [브리지 SMU]

이 경로는 Bridge SMU를 사용하여 v7.6.2에서 실행 중인 디바이스를 업데이트하는 것을 나타냅니다.

- 7.6.2 [브리지 SMU] - 7.7.2

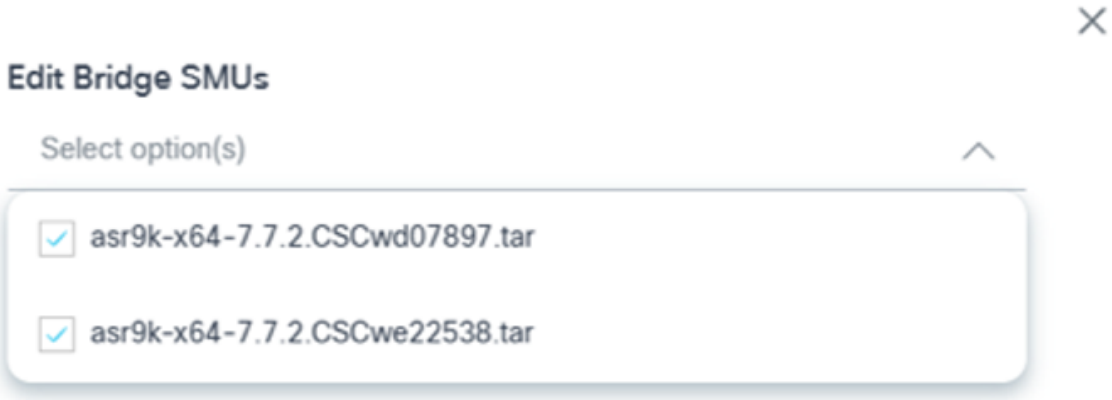
이 경로는 디바이스를 v7.6.2에서 v7.7.2로 업그레이드함을 나타냅니다. 이 경우 디바이스의 소스 버전은 Bridge SMU가 적용된 7.6.2입니다.

브리지 SMU 편집



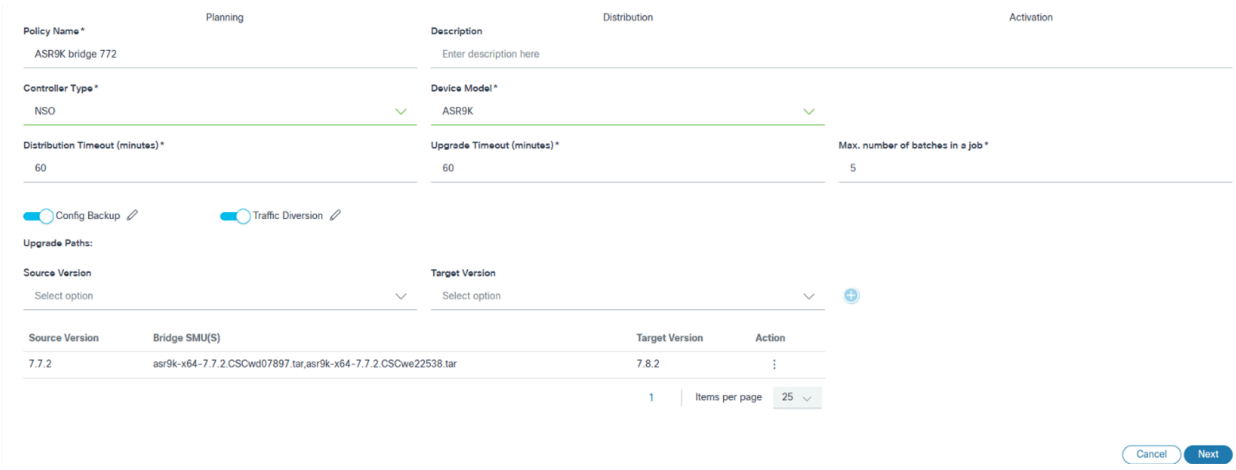
Bridge SMU를 사용한 업그레이드 경로

1. Upgrade Paths(업그레이드 경로) 섹션에서 More Options(추가 옵션) 아이콘 > Edit Bridge SMUs(브리지 SMU 편집)를 선택합니다. Edit Bridge SMUs 창이 열립니다.



브리지 SMU 편집

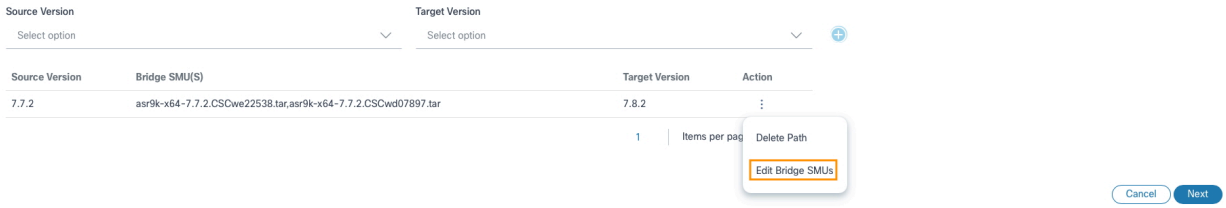
2. 브리지 SMU를 업데이트하려면 해당 확인란을 선택하거나 선택 취소합니다.
3. OK(확인)를 클릭합니다. 변경 사항의 요약이 표시됩니다.



변경 사항 요약

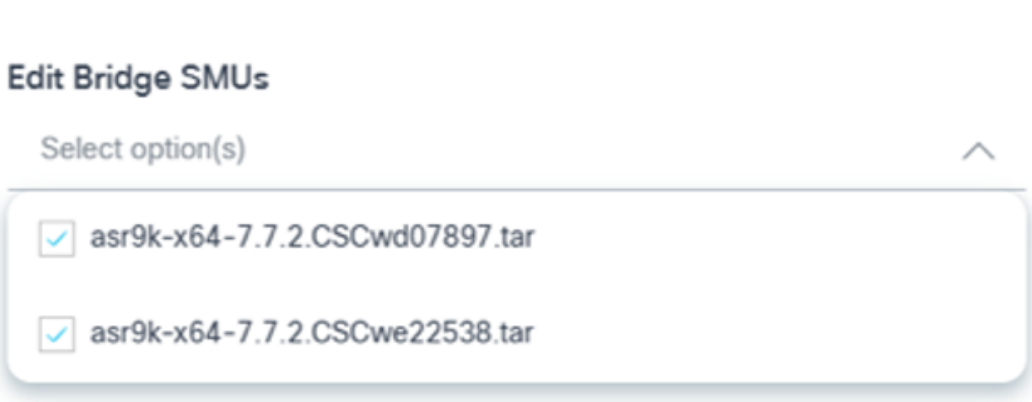
4. 변경 사항의 요약을 확인하고 Next(다음)를 클릭합니다.

브리지 SMU 삭제



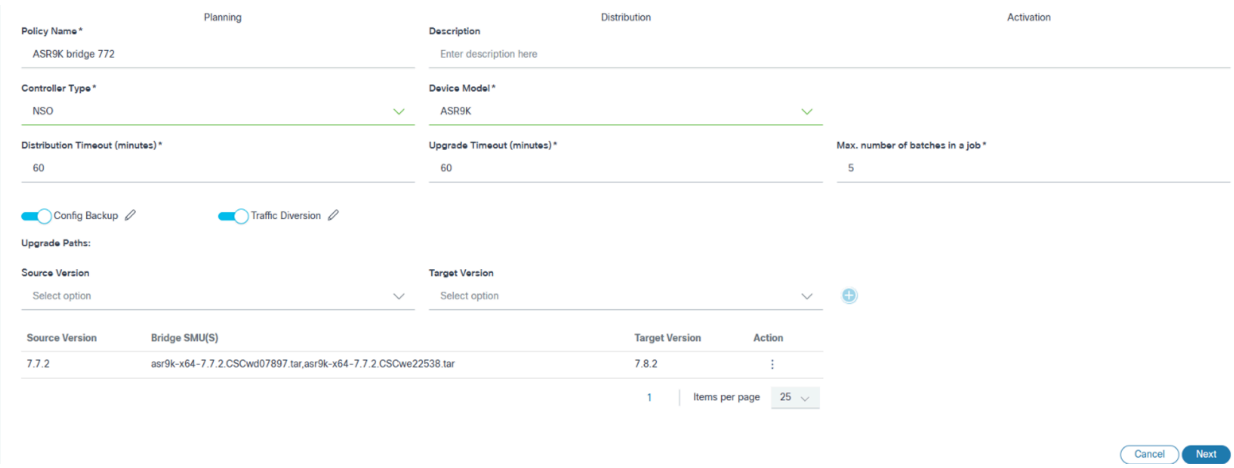
브리지 SMU 편집

1. Upgrade Paths(업그레이드 경로) 섹션에서 More Options(추가 옵션) 아이콘 > Edit Bridge SMUs(브리지 SMU 편집)를 선택합니다. Edit Bridge SMUs 창이 열립니다.



브리지 SMU 편집

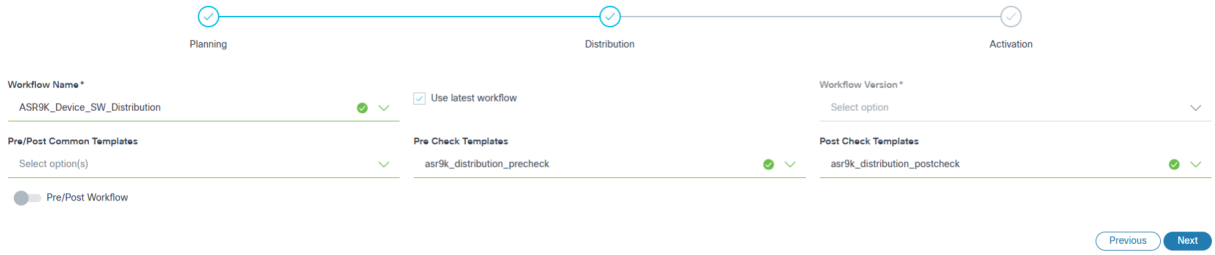
2. 브리지 SMU를 제거하려면 해당 확인란의 선택을 취소합니다.
3. OK(확인)를 클릭합니다. 변경 사항의 요약이 표시됩니다.



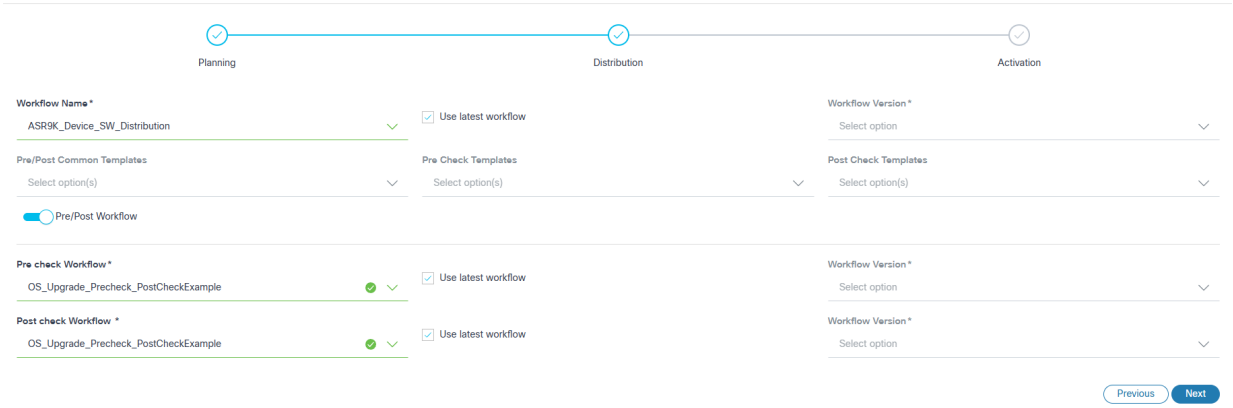
변경 사항 요약

배포

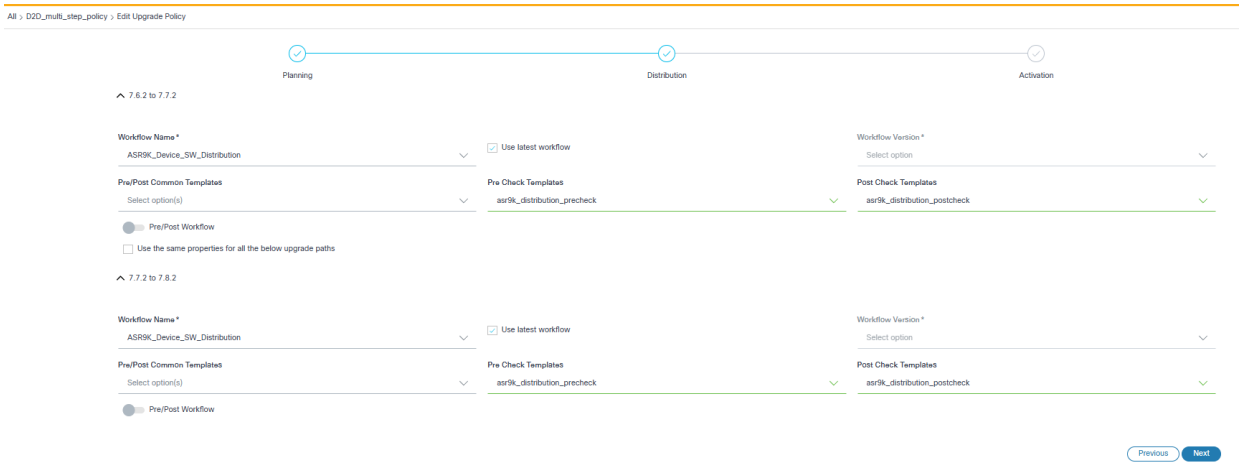
분배는 이미지 분배(즉, 이미지 카피)와 관련된 입력 파라미터들을 취한다. 다음 이미지는 각 업그레이드 경로 유형에 필요한 입력 매개변수입니다.



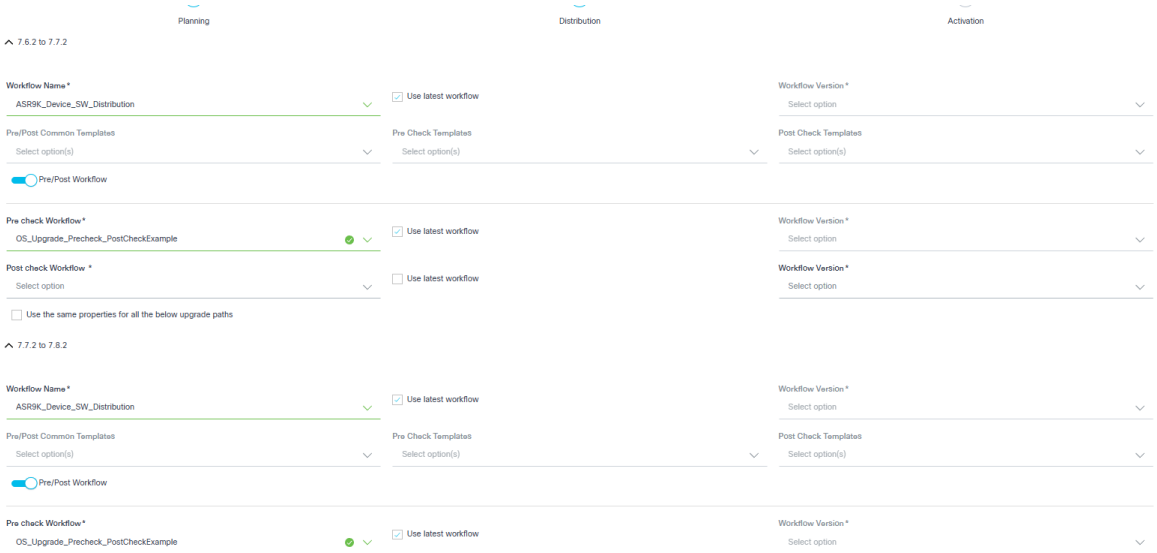
이미지 배포 섹션 - 단일 단계 업그레이드



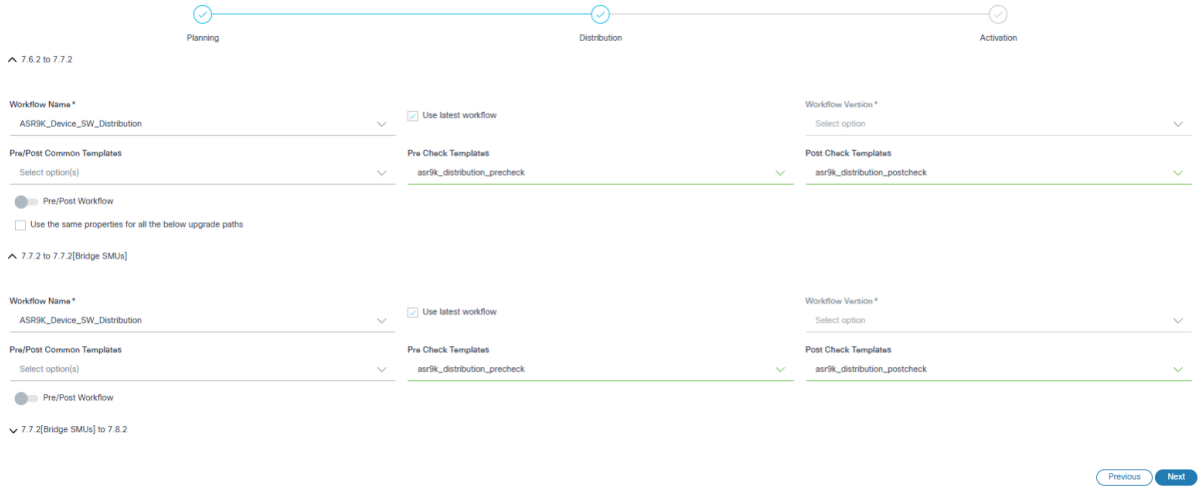
이미지 배포 섹션 - 사전/사후 워크플로우가 포함된 단일 단계 업그레이드 토글



배포 섹션 - 다단계 업그레이드



배포 섹션 - 다단계 업그레이드



배포 섹션 - 브리지 SMU 업그레이드

1. 이미지 배포와 관련된 매개변수를 구성합니다.
2. 다음 표에서는 각 필드에 대한 간단한 설명을 제공합니다.

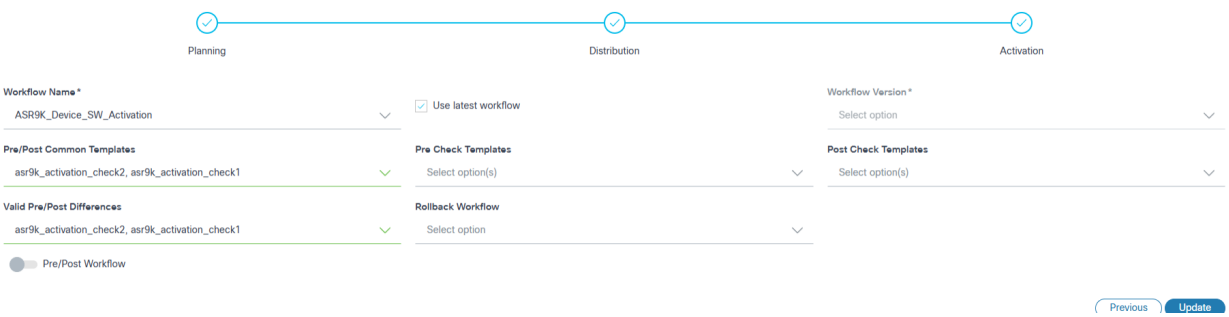
필드	설명
워크플로 이름	적용 가능한 배포 워크플로
최신 워크플로 사용	선택한 워크플로의 최신 버전 선택
워크플로 버전	맞춤형 워크플로 버전; 이 옵션은 최신 워크플로 사용 확인란이 선택되지 않은 경우에만 선택할 수 있습니다
사전/사후 공통 템플릿	두 단계(즉, 사전 확인 및 사후 확인)에서 실행되는 프로세스 템플릿 참고: 점검은 배포 중요 시점에만 해당됩니다. 자세한 내용은 [프로세스 템플릿]을 참조하십시오

필드	설명
사전/사후 워크플로 토글	사용자가 Distribution Milestone 내에서 사전 또는 사후 확인 워크플로의 실행을 선택할 수 있습니다. 토글이 켜져 있으면 사전 확인 또는 사후 확인 워크플로만 구성할 수 있습니다.
워크플로 사전 확인	사전 검사 단계 동안에만 실행되는 명령을 포함합니다. 참고: 이러한 점검은 배포 중요 시점에만 적용됩니다.
사후 검사 워크플로	사후 검사 워크플로는 사후 검사 단계 동안 고유하게 실행되는 명령으로 구성됩니다. 참고: 이러한 점검은 배포 중요 시점에만 적용됩니다.
사전 검사 템플릿	배타적 사전 검사 명령이 포함된 프로세스 템플릿 템플릿은 사전 검사 단계에서만 실행됩니다. 참고: 점검은 배포 중요 시점에만 해당됩니다.
사후 점검 템플릿	독점 post-check 명령이 포함된 프로세스 템플릿 템플릿은 사후 검사 단계에서만 실행됩니다. 참고: 점검은 배포 중요 시점에만 해당됩니다.
아래의 모든 업그레이드 경로에 동일한 속성 사용	다중 선택 업그레이드의 모든 업그레이드 경로에 일관된 속성이 적용됩니다. 참고: 이 옵션을 선택하면 다중 선택 업그레이드의 모든 업그레이드 경로에 동일한 속성이 적용됩니다.

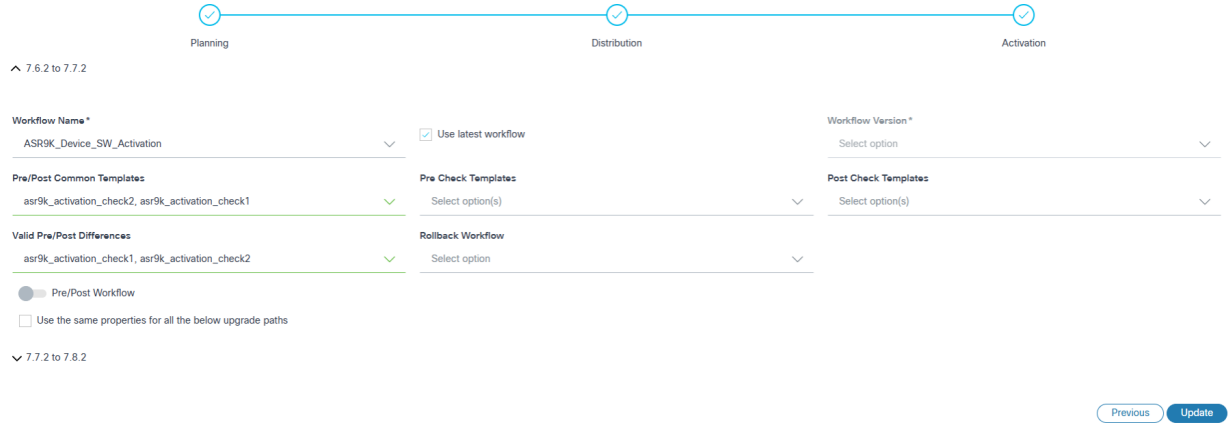
참고: 워크플로 또는 프로세스 템플릿에는 OS Upgrade Next-Gen 태그가 올바르게 지정되어 있어야 합니다.

3. Next(다음)를 클릭하여 Activation(활성화) 섹션으로 이동합니다.

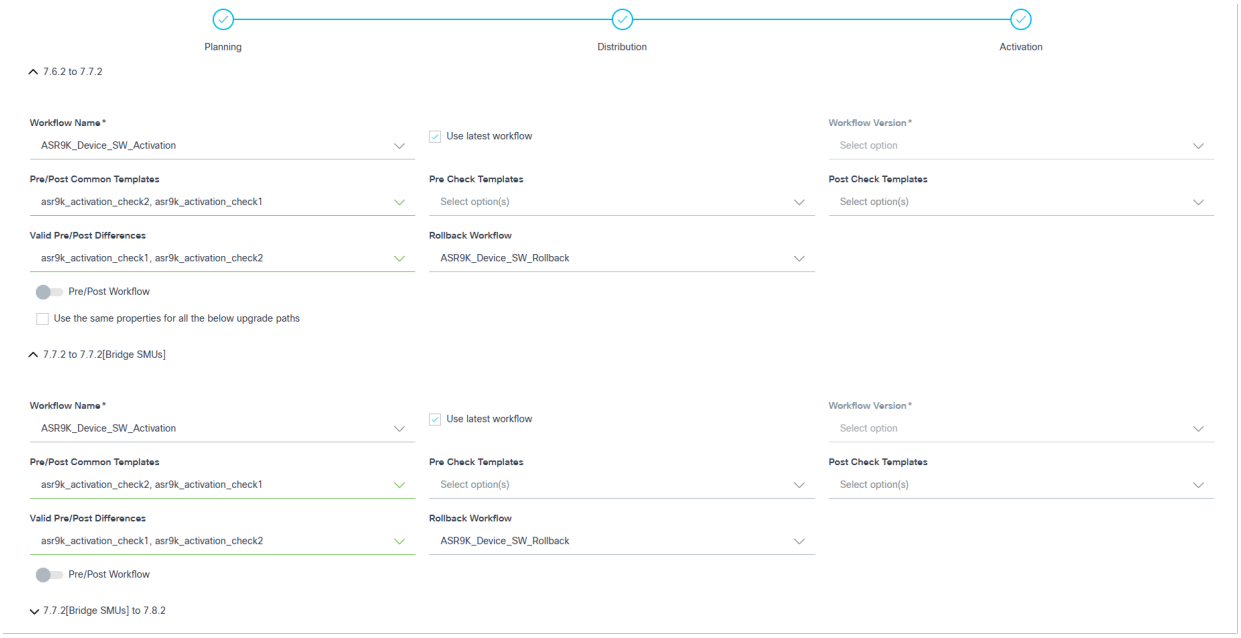
활성화



활성화 섹션 - 단일 단계 업그레이드



활성화 섹션 - 다단계 업그레이드



활성화 섹션 - 브리지 SMU 업그레이드

1. 이미지 활성화와 관련된 매개변수를 구성합니다.
2. 아래 표에는 각 필드에 대한 간략한 설명이 나와 있습니다.

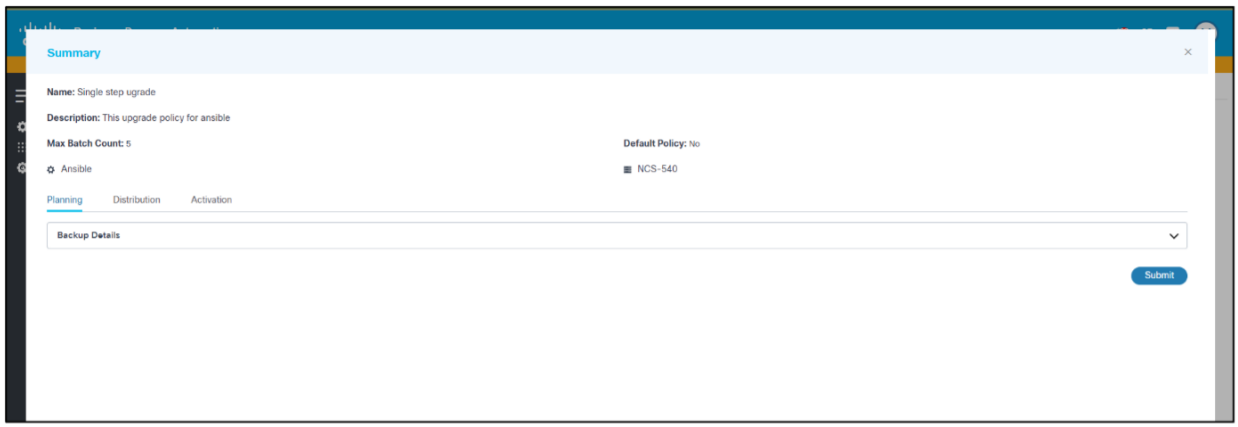
필드	설명
워크플로 이름	해당 활성화 워크플로
최신 워크플로 사용	선택한 워크플로의 최신 버전 선택
워크플로 버전	맞춤형 워크플로 버전; 최신 워크플로 사용 확인란을 선택하지 않은 경우에만 선택할 수 있습니다
사전/사후 공통 템플릿	두 단계(즉, 사전 검사 및 사후 검사)에서 실행되는 프로세스 템플릿입니다. 참고: 검사는 활성화 중요 시점에만 해당됩니다.

필드	설명
사전 검사 템플릿	자세한 내용은 프로세스 템플릿을 참조하십시오 배타적 사전 검사 명령이 포함된 프로세스 템플릿 템플릿은 사전 검사 단계에서만 실행됩니다. 참고: 검사는 활성화 중요 시점에만 해당됩니다.
수표 템플릿 게시	독점 post-check 명령이 포함된 프로세스 템플릿 템플릿은 사후 검사 단계에서만 실행됩니다. 참고: 검사는 활성화 중요 시점에만 해당됩니다.
유효한 사전/사후 차이	차이를 무시하도록 선택된 프로세스 템플릿입니다. 참고: 검사는 활성화 중요 시점에만 해당됩니다.
롤백 워크플로	적용 가능한 롤백 워크플로입니다. 참고: 다중 선택 업그레이드에서 롤백 워크플로가 있는 업그레이드 경로 중 하나를 선택한 경우, 다른 모든 업그레이드 단계는 기본적으로 롤백 워크플로와 함께 선택됩니다.
워크플로 사전 확인	이 맞춤형 사전 검사 워크플로는 실행 결과를 선택하고 검토할 수 있는 특정 명령으로 구성됩니다. 사전 점검 단계에서만 실시됩니다. 참고: 이 검사는 활성화 중요 시점에만 해당됩니다.
사후 검사 워크플로	이 맞춤형 사후 검사 워크플로는 실행 결과를 선택하고 검토할 수 있는 특정 명령으로 구성됩니다. 사후 점검 단계에서만 수행됩니다. 참고: 이 검사는 활성화 중요 시점에만 해당됩니다.
아래의 모든 업그레이드 경로에 동일한 속성 사용	다중 선택 업그레이드의 모든 업그레이드 경로에 일관된 속성이 적용됩니다. 참고: 이 옵션을 선택하면 다중 선택 업그레이드의 모든 업그레이드 경로에 동일한 속성이 적용됩니다.

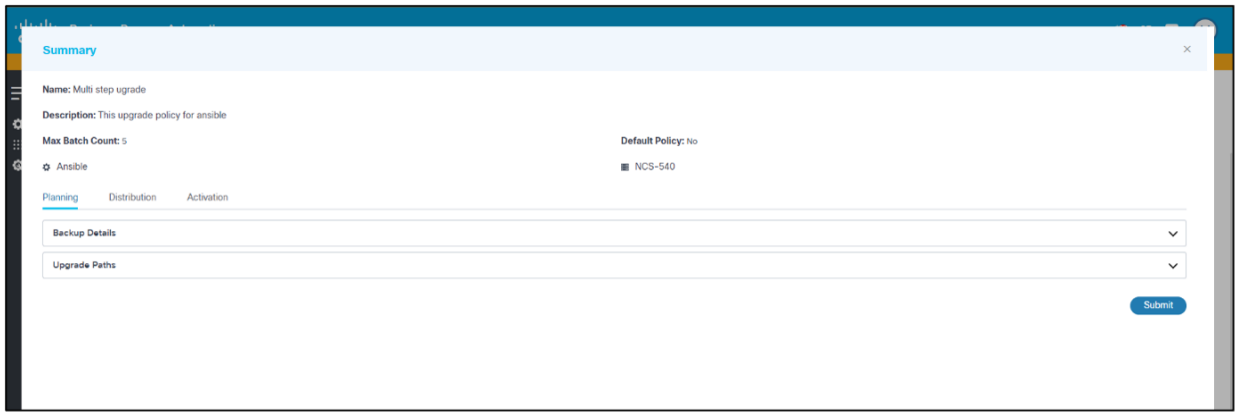
✎ 참고: 다음에 유의해야 합니다.

- Nexus 디바이스에 필요한 공개 키 알고리즘은 NSO에서 구성해야 합니다.
- Nexus 디바이스에서 사전 및 사후 검사 템플릿을 실행하도록 bgp, bfd 및 hsrp의 기능을 구성합니다.

3. Create(생성)를 클릭합니다. 필드 요약이 표시됩니다.



요약 - 단일 단계 업그레이드 정책



요약 - 다단계 업그레이드 정책

4. 필드의 요약을 확인하고 Submit(제출)을 클릭합니다. 진행 알림과 확인 메시지가 표시됩니다. 정책이 성공적으로 생성되면 페이지에 표시됩니다.

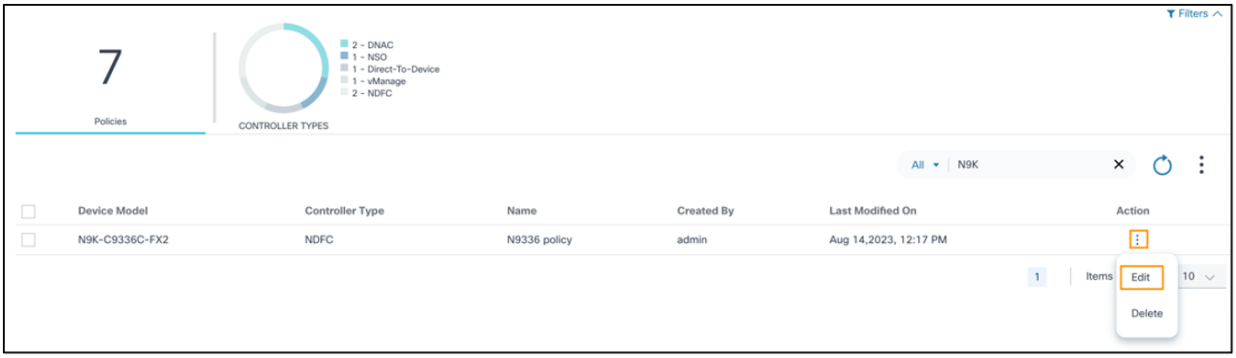
필요에 따라 다른 디바이스 모델에 대한 추가 업그레이드 정책을 생성할 수 있습니다.

업그레이드 정책 수정

업그레이드 정책의 검색 결과

1. Upgrade Policy(업그레이드 정책) 페이지에서 Search(검색) 필드를 사용하여 원하는 정책을

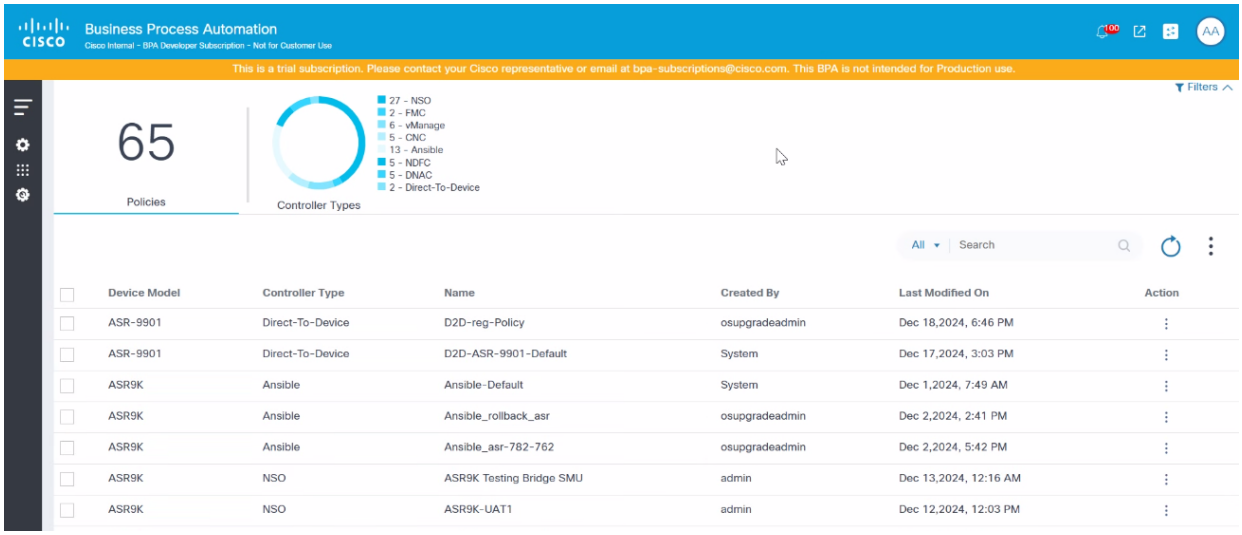
찾습니다.



업그레이드 정책 편집

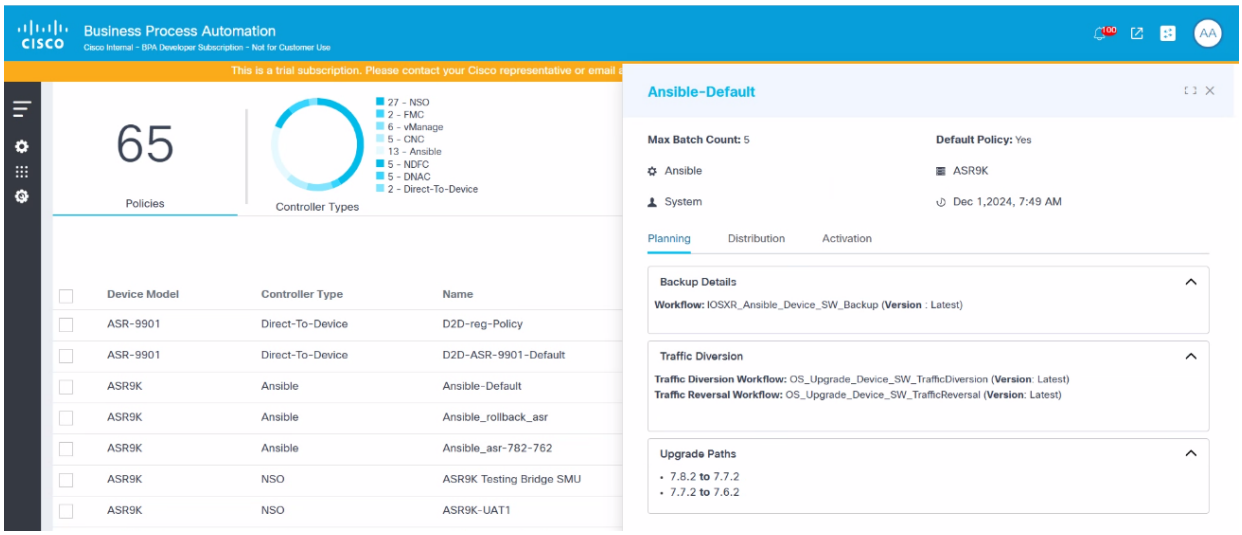
2. 정책의 Action(작업) 열에서 More Options(추가 옵션) 아이콘 > Edit(수정)를 선택합니다.
3. 관련 필드를 업데이트하고 업데이트를 클릭합니다. 변경 사항의 요약이 표시됩니다.
4. 변경 사항의 요약을 확인하고 Submit(제출)을 클릭합니다. 진행 상황 알림 및 확인 메시지가 표시됩니다.

업그레이드 정책 보기



업그레이드 정책

1. Upgrade Policy 페이지에서 원하는 업그레이드 정책의 행을 선택합니다. 정책의 세부사항 보기가 열립니다.



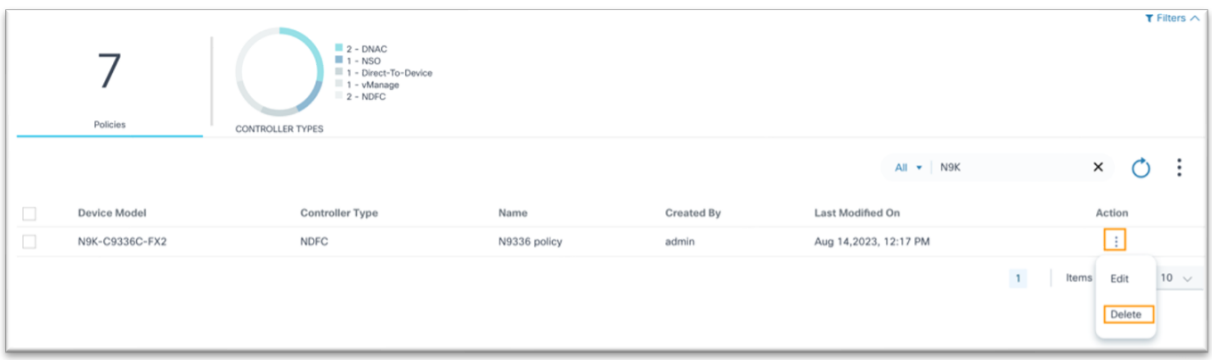
업그레이드 정책 세부 정보 보기

업그레이드 정책 삭제

참고: 기본 정책은 삭제할 수 없지만 프로세스 템플릿과 워크플로는 사용자가 편집할 수 있습니다.

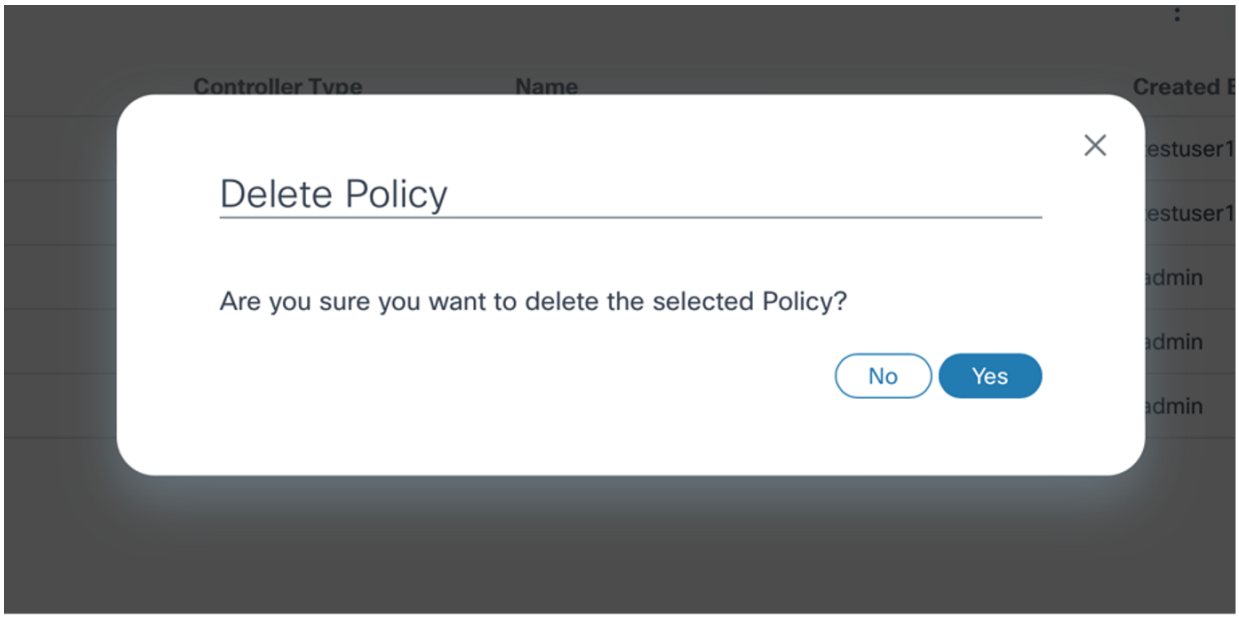
업그레이드 정책

1. Upgrade Policies(업그레이드 정책) 페이지에서 Search(검색) 필드를 사용하여 원하는 정책을 **.



업그레이드 정책 삭제

2. 정책의 Action(작업) 열에서 More Options(추가 옵션) > Delete(삭제)를 선택합니다. 확인 창이 열립니다



정책 삭제 확인

3. Yes(예)를 클릭합니다.

업그레이드 정책에 대한 액세스 제어

이 기능은 업그레이드 정책에 대한 액세스 제어를 제공하여 권한이 없는 사용자가 OS 업그레이드 애플리케이션에 정의된 정책을 업데이트할 수 없도록 제한합니다. 관리자는 액세스 가능한 정책으로 리소스 그룹을 정의하여 액세스를 제한할 수 있습니다.

리소스 그룹을 생성하려면

1. Settings(설정) > Resource Groups(리소스 그룹)로 이동합니다.
2. 관리자가 아닌 사용자가 액세스할 수 있는 정책으로 리소스 그룹을 만듭니다. 이 사용자 그룹에 속한 비관리자 사용자는 이제 이 리소스 그룹에서 사용할 수 있는 정책에만 액세스할 수 있습니다.
3. 리소스 그룹을 사용자 그룹과 연결하는 액세스 정책을 생성합니다.

자세한 내용은 액세스 제어를 참조하십시오.

✎ 참고: 다음 사항을 유의해야 합니다.

- 사용자가 배포 및 활성화에 대해 잘못된 워크플로를 선택할 수 있으므로 의도하지 않은 동작이 발생합니다. 워크플로를 올바르게 매핑하고 배포, 활성화, 롤백 및 장치 모델과 같은 중요 시점에 대한 적용 가능성을 확인하는 것은 사용자의 책임입니다.
- 워크플로 및 프로세스 템플릿은 OS Upgrade Next-Gen 태그와 매핑되어야 정책을 생성하거나 업데이트할 때 선택할 수 있습니다.
- 시스템 사용자가 만든 기본 OOB 정책은 삭제할 수 없지만 프로세스 템플릿과 워크플로는 사용자가 편집할 수 있습니다.

업그레이드 작업

소프트웨어 업그레이드는 업그레이드 작업 응용 프로그램을 사용하여 관리됩니다. 이 응용 프로그램은 각 배치에 하나 이상의 네트워크 장치가 있는 하나 이상의 배치로 구성됩니다. 초안 모드에서 작업을 생성하고 여러 번 저장할 수 있습니다. 업그레이드는 작업을 커밋한 후에만 시작할 수 있으므로 운영자는 사전에 변경 계획을 세울 수 있습니다.

사전 요구 사항

- 업그레이드를 위한 예약된 유지 보수 기간
- 업그레이드 변경 요청에 대한 사전 승인
- 구성 백업 및 복원 서비스가 실행 중이어야 합니다.
- 스케줄러 서비스가 실행 중이어야 합니다.
- 외부 시스템용 BPA 어댑터(예: 티켓팅 시스템)가 있는 경우 온보딩해야 합니다

업그레이드 작업 보기 및 관리

1. 업그레이드 작업에 액세스할 수 있는 자격 증명을 사용하여 BPA에 로그인합니다.
2. OS Upgrade(OS 업그레이드) > Upgrade Jobs(업그레이드 작업)를 선택합니다. [업그레이드 작업] 페이지가 표시됩니다.

업그레이드 작업

[업그레이드 작업] 페이지는 다음 항목을 포함합니다.

참고: 기본적으로 10개의 작업이 표시됩니다. 페이지 번호를 사용하여 다른 작업 페이지로 이동할 수 있습니다.

- 활성 작업과 보관된 작업은 활성 작업과 보관된 작업 간에 전환하는 데 사용할 수 있습니다
- 다음을 제공하는 분석 섹션이 맨 위에 표시됩니다.
    - 작업에 연결된 총 작업 및 자산
    - 다음 필터가 포함된 단계 차트:
        - 초안: 작업이 초안 단계에 있으며 아직 커밋되지 않았습니다.
        - 커밋: 작업이 일정에 도달할 때까지 필요한 모든 장치, 배치 또는 일정과 함께 커밋됩니다
        - 구축: 하나 이상의 일괄 처리에 대한 업그레이드 작업이 시작되었습니다.
        - 완료: 모든 배치에 속한 모든 디바이스에 대한 업그레이드 작업이 완료되었습니다.
    - 컨트롤러 유형 차트: Cisco Catalyst Center, vManage, NSO, NDFC, Direct-to-Device, CNC, ANSIBLE 및 FMC 컨트롤러 유형을 통한 작업 필터링 허용
    - 다음 필터가 있는 작업 유형 차트:
        - 배포: 컨트롤러에서 디바이스로 이미지를 스테이징하거나 복사하는 작업
        - 활성화: 장치 소프트웨어의 활성화 또는 업그레이드를 수행하는 작업
        - 배포 및 활성화: 장치 소프트웨어의 스테이징 또는 복사 및 활성화 또는 업그레이드를 수행하는 작업
- 모든 메타데이터에 대해 일반 검색을 수행하거나 작업 이름 및 생성자 필드를 기준으로 일반 검색을 수행하는 데 사용할 수 있는 검색 필드입니다
- 작업 요약을 새로 고치고 [검색] 필드에서 차트 필터 또는 사용자 지정 검색을 지우는 데 사용할 수 있는 [새로 고침] 아이콘입니다.
- 추가 옵션 아이콘 - 새 업그레이드 작업 생성 및 선택한 작업을 보관 또는 삭제하는 옵션을 제공합니다. 사용자는 모두 선택 또는 선택 취소할 수 있습니다.
- 작업은 패널로 표시되며 다음 정보를 빠르게 볼 수 있습니다.
    - 사용 가능한 사용자 작업이 있는 경우 사용자 작업 아이콘이 사용자 작업 수와 함께 표시됩니다
    - 작업을 생성한 사용자
    - 작업 생성 날짜
    - 배치 및 자산 수
    - 컨트롤러 유형(예: Cisco Catalyst Center, vManage, NDFC, Direct-to-Device, CNC, ANSIBLE 또는 FMC)
    - 대상 버전
    - 해당 디바이스 모델
    - 각 이정표에 대한 색상 범례가 있는 작업 단계(초안, 커밋, 배치 및 완료)의 이정표 보기:

- 회색: 이정표가 시작되지 않았습니다.
- 파란색: 이정표가 진행 중입니다.
- 빨간색: 중요 시점 문제
- 초록색: 이정표 완료

- 작업 상태를 표시하는 중요 시점 끝의 색 범례입니다.

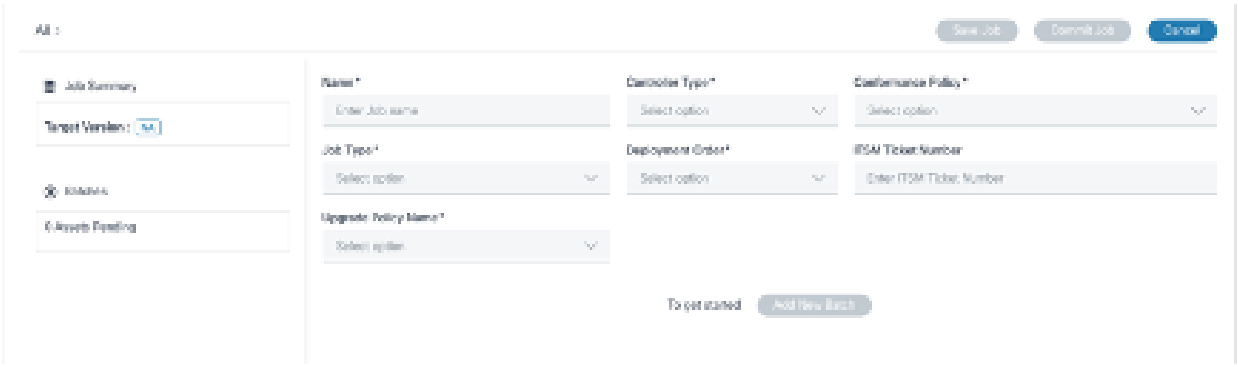
  - 초록색: 작업 완료
  - 빨간색: 작업에 문제가 있습니다.
  - 파란색: 작업 진행 중

업그레이드 작업 예약

작업을 생성하려면 다음을 수행합니다.

업그레이드 작업 생성 옵션

1. [업그레이드 작업] 페이지에서 [추가 옵션] 아이콘 > [작업 생성]을 선택합니다. [업그레이드 작업 생성] 페이지가 표시됩니다.



업그레이드 작업 생성

2. 이름 필드에 작업 이름을 입력합니다.
3. 컨트롤러 유형(예: Cisco Catalyst Center, vManage, NDFC, Direct-to-Device, CNC, FMC, ANSIBLE 또는 NSO)을 선택합니다.
4. 부적합 디바이스가 있는 적합성 정책을 선택합니다.

참고: 정책을 선택한 후 사용할 해당 업그레이드 정책을 자동으로 식별하여, 한 번 이상 실행되며 하나 이상의 비준수 디바이스가 있는 적합성 정책만 목록에서 사용할 수 있습니다.

다음 세부 정보는 [작업 요약] 아래의 [작업 생성] 양식 왼쪽에 표시됩니다.

- 영향을 받는 디바이스 모델

참고: 선택한 적합성 정책에 연결된 디바이스 모델이 두 개 이상 있는 경우 여러 디바이스 모델이 표시됩니다.

- 대상 버전
- 기존 릴리스 버전 및 해당 개수 집계
- 허용되는 최대 배치 수
- 부적합 자산의 총 수

참고: 선택한 적합성 정책이 여러 디바이스 모델과 연관된 경우, 연관된 모든 모델에 대한 비적합성 자산의 합계가 표시됩니다.

- 일괄 처리 추가 옵션

5. 다음 업그레이드 작업 유형 중 하나를 선택합니다.

- 배포: 배포 전용 작업은 실제 정품 인증 전에 소프트웨어 이미지를 스테이징하는 경우에 유용합니다
- 활성화: 활성화 전용 작업은 배포 전용 작업을 통해 배포가 이미 완료된 장치의 업그레이드를 수행하는 데 유용합니다
- 배포 및 활성화: 이미지 배포 또는 스테이징과 활성화는 모두 동일한 작업 내에서 수행되므로 이미지를 장치에 복사하고 업그레이드하는 데 필요한 충분한 유지 관리 기간을 사용할 수 있는 경우에 유용합니다

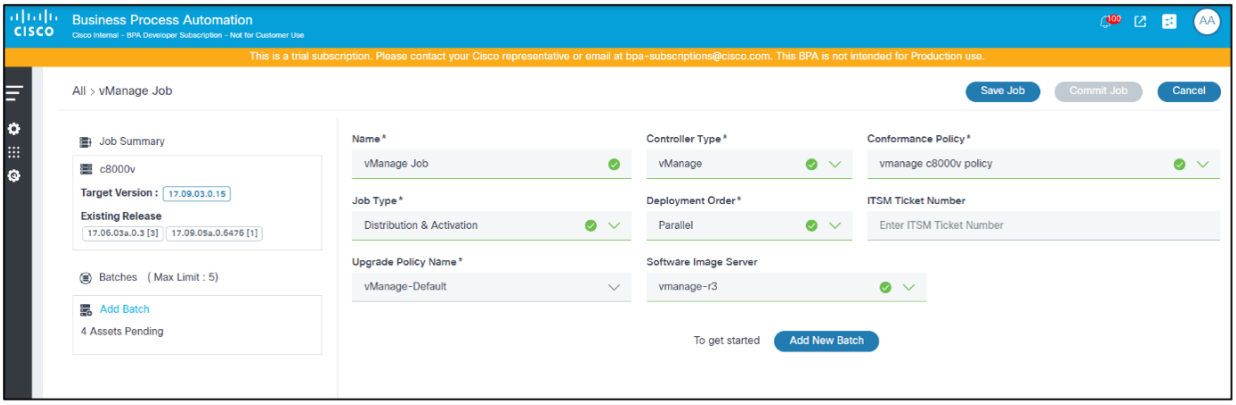
6. 업그레이드 주문을 선택합니다. 병렬 모드에서는 여러 디바이스가 동시에 처리되지만 순차 모드에서는 디바이스가 하나씩 처리됩니다.

참고: 병렬 모드에서 처리할 수 있는 최대 디바이스 수는 구축 컨피그레이션에 따라 다릅니다. 선택한 업그레이드 순서는 전체 작업에 적용되지만 필요에 따라 특정 일괄 처리 내에서 재정의할 수 있습니다.

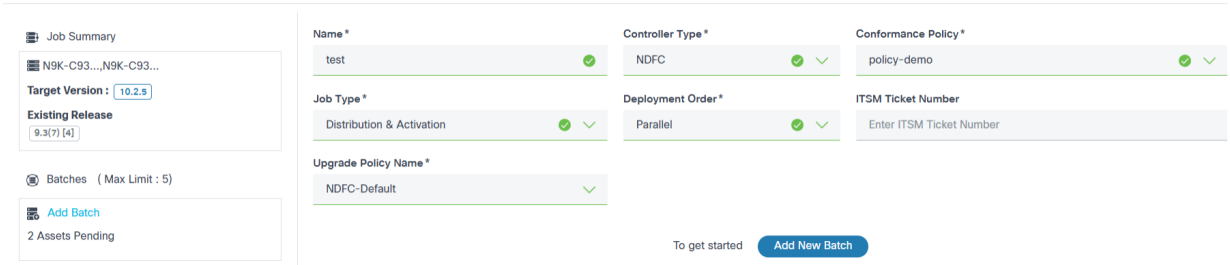
7. ITSM(IT Service Management) Ticket Number(IT 서비스 관리) Ticket Number(티켓 번호) 필드에 변경 요청 번호를 추가합니다.

8. Upgrade Policy Name(업그레이드 정책 이름)을 선택합니다. 컨트롤러 유형 및 적합성 정책 디바이스 모델에 따라 적용 가능한 업그레이드 정책만 표시됩니다. 사용자는 업그레이드 정책 중 하나를 선택할 수 있습니다. 소프트웨어 적합성 정책에 둘 이상의 연결된 모델이 있는 경우 각 모델과 연결된 모든 관련 업그레이드 정책이 표시됩니다. 사용자는 모든 모델에 적용되는 업그레이드 정책을 신중하게 선택해야 합니다.
9. Software Image Server(소프트웨어 이미지 서버)를 선택하여 어떤 vManage 이미지 저장소(예: 로컬 또는 원격)를 사용할지 지정합니다.

참고: 이 입력은 vManage 컨트롤러 유형에만 적용됩니다.

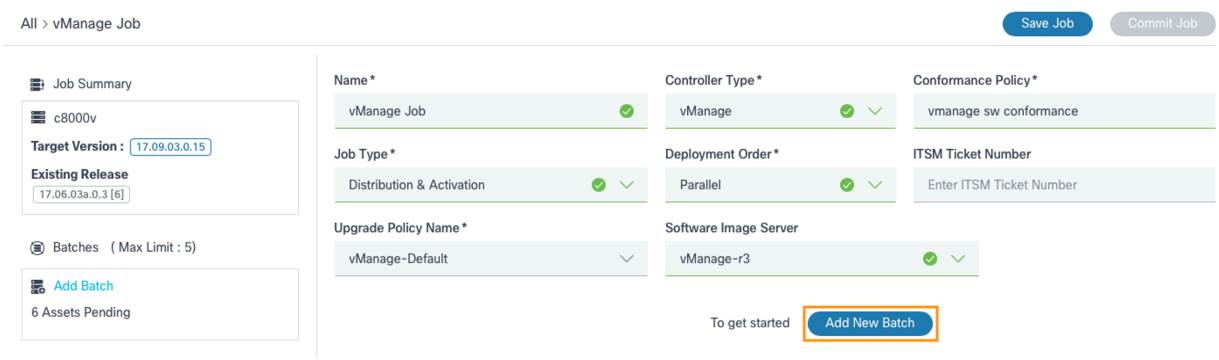


세부 정보가 채워진 업그레이드 작업 생성(적합성 정책에는 하나의 모델이 있음)



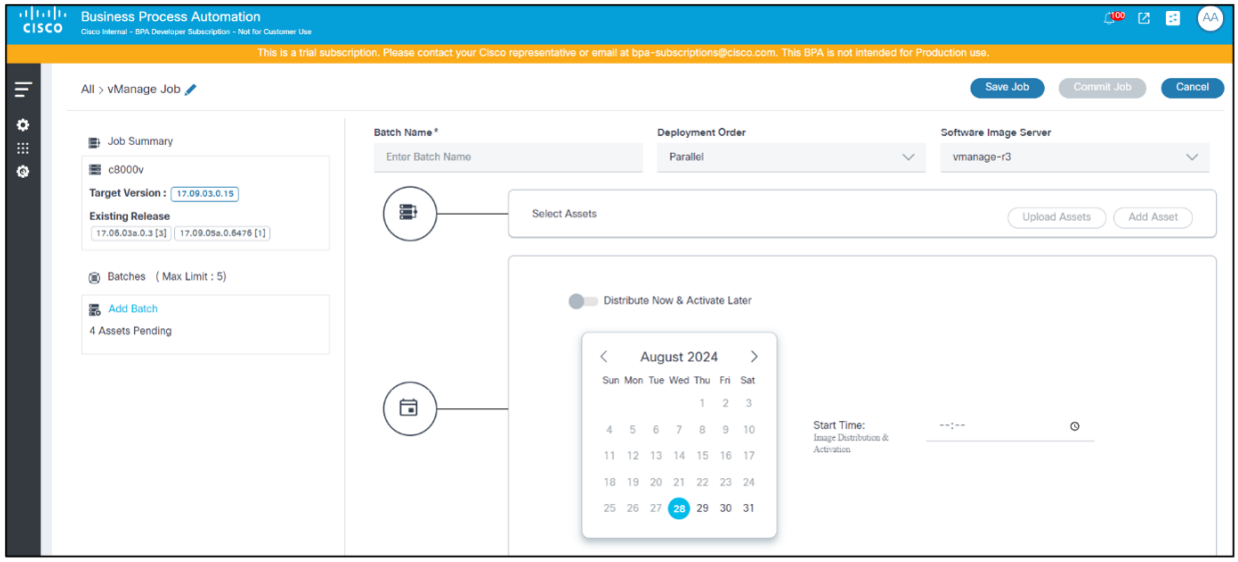
세부 정보가 채워진 업그레이드 작업 생성(적합성 정책에 여러 모델이 있음)

10. 작업 저장을 클릭하여 작업을 커밋할 준비가 될 때까지 초안을 저장합니다.



배치 추가 및 새 배치 추가

11. 배치를 추가하려면 Add Batch(배치 추가) 링크 또는 Add New Batch(새 배치 추가)를 클릭합니다. 배치 생성 창이 열립니다.



배치 생성

12. 관련 배치명을 입력하고 배치 순서를 선택합니다.

참고: 여기서 선택한 업그레이드 유형은 [작업 생성] 페이지에서 선택한 업그레이드 유형보다 우선합니다

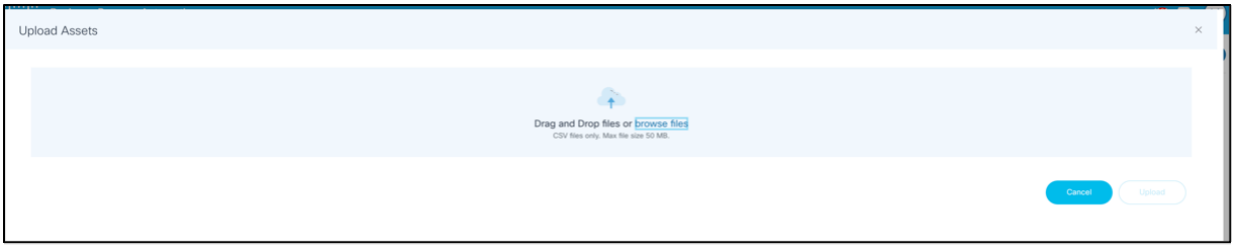
---

13. Software Image Server(소프트웨어 이미지 서버)를 선택하여 어떤 vManage 리포지토리(예: 로컬 또는 원격)를 사용할지 지정합니다.

참고: 이 필드는 vManage 컨트롤러 유형에만 적용됩니다. 여기서 선택한 소프트웨어 이미지 서버는 [작업 생성] 페이지에서 선택한 서버보다 우선합니다

---

14. 배치에 자산을 추가합니다. 자산은 두 가지 방법으로 배치에 추가할 수 있습니다.



자산 업로드

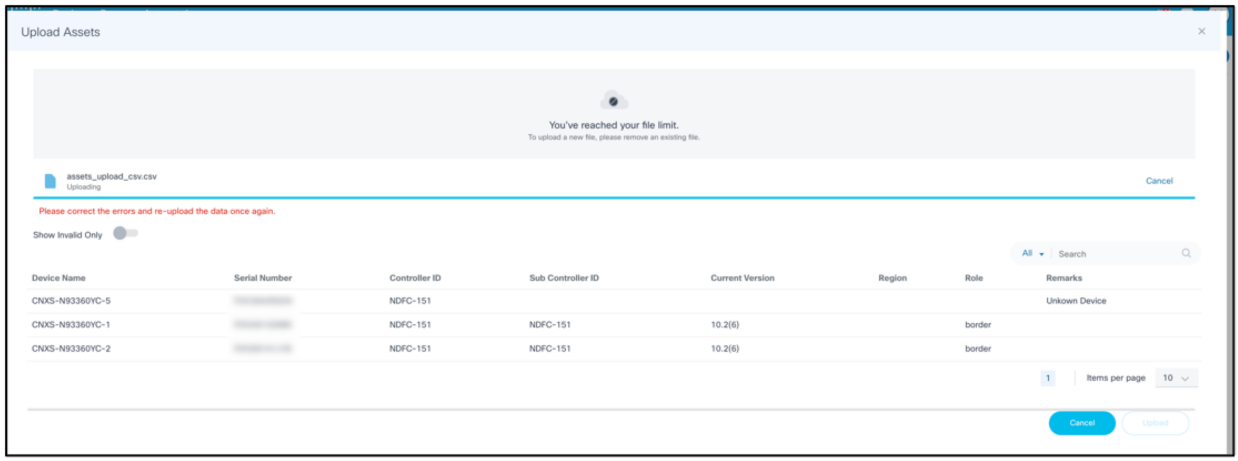
옵션 1:

a. Upload Assets(자산 업로드)를 클릭합니다. 자산 업로드 창이 열립니다.
b. 업로드할 .csv 파일을 선택합니다.

참고: .csv 파일에는 다음 세부 정보가 있어야 합니다.

- 장치 이름: 디바이스 또는 자산의 이름
- 일련 번호: 디바이스의 일련 번호
- 컨트롤러 ID: 디바이스를 관리하는 컨트롤러의 이름
- 하위 컨트롤러 ID: 디바이스를 관리하는 하위 컨트롤러 ID의 이름

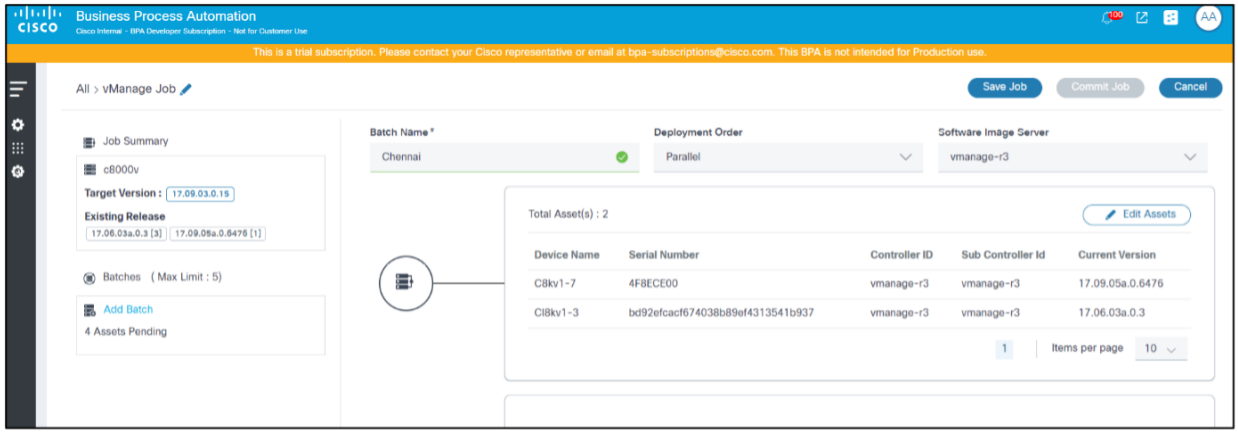
c. Upload를 클릭합니다. .csv 파일 데이터의 유효성을 검사하고 유효한 데이터와 유효하지 않은 데이터가 모두 표시됩니다. Show Invalid Only(유효하지 않은 항목만 표시) 토글은 업로드된 자산 세부사항에서 유효하지 않은 디바이스를 필터링하는 데 사용할 수 있습니다.



CSV 파일을 통해 업로드된 샘플 자산

d. 업로드한 파일에 오류가 있는 경우 오류를 수정하고 다시 업로드합니다.

참고: 사용자는 업로드된 모든 디바이스가 유효한 경우에만 자산 선택을 진행할 수 있습니다.



배치 추가 - 선택한 자산

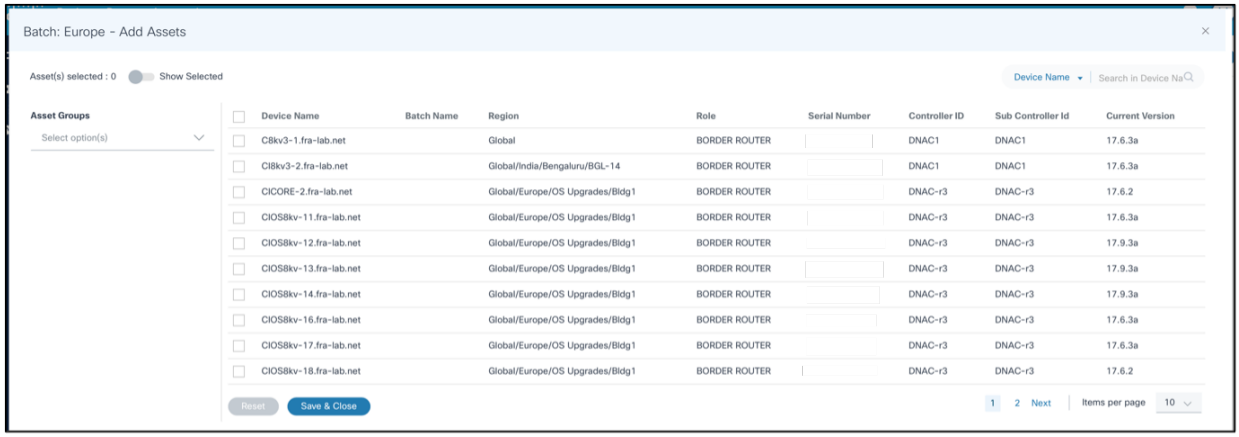
옵션 2:

a. Add Assets(에셋 추가)를 클릭합니다. 자산 선택 창이 열립니다.

참고: 자산 업로드 및 자산 추가는 동시에 사용할 수 없습니다.

b. FMC 컨트롤러 유형의 경우에만 업그레이드를 수행할 제어 노드 또는 독립형 노드를 선택합니다.

참고: 데이터 노드의 업그레이드는 해당 제어 노드에서 처리되므로 업그레이드 작업에서 데이터 장치를 사용할 수 없습니다.



장치 선택

c. 현재 배치에 포함할 장치를 선택합니다.

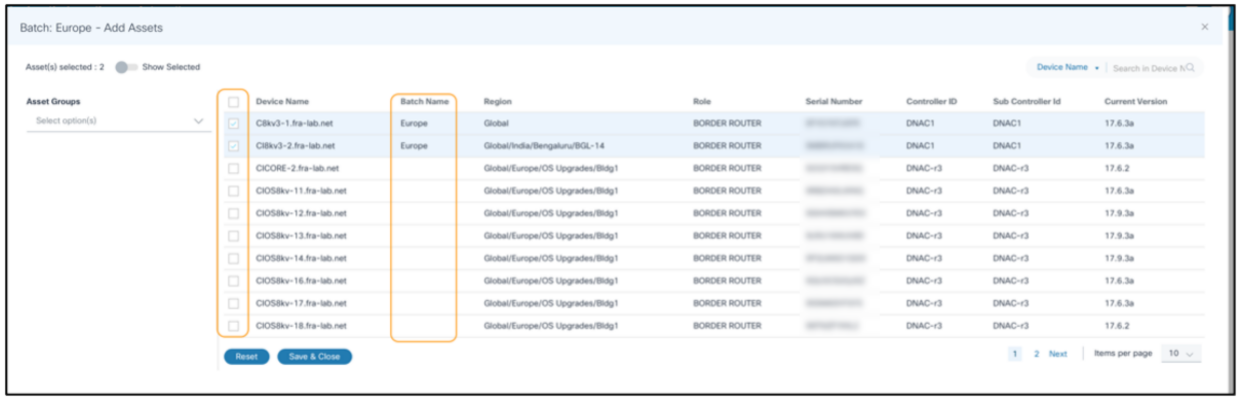
검색 필터는 다른 특성을 기준으로 장치를 필터링하는 데 사용할 수 있으며, Device Name(장치 이름) 열 헤더에서 확인란을 선택하여 필터링 기준에 일치하는 모든 장치를 대량으로 선택할 수 있습니다. 사용자는 자산 그룹별로 필터링할 수도 있습니다.

선택한 에셋만 보려면 선택한 항목 표시 토글을 활성화할 수 있습니다.

참고: 선택 항목 표시 토글이 활성화되면 자산 그룹 필터가 비활성화됩니다.

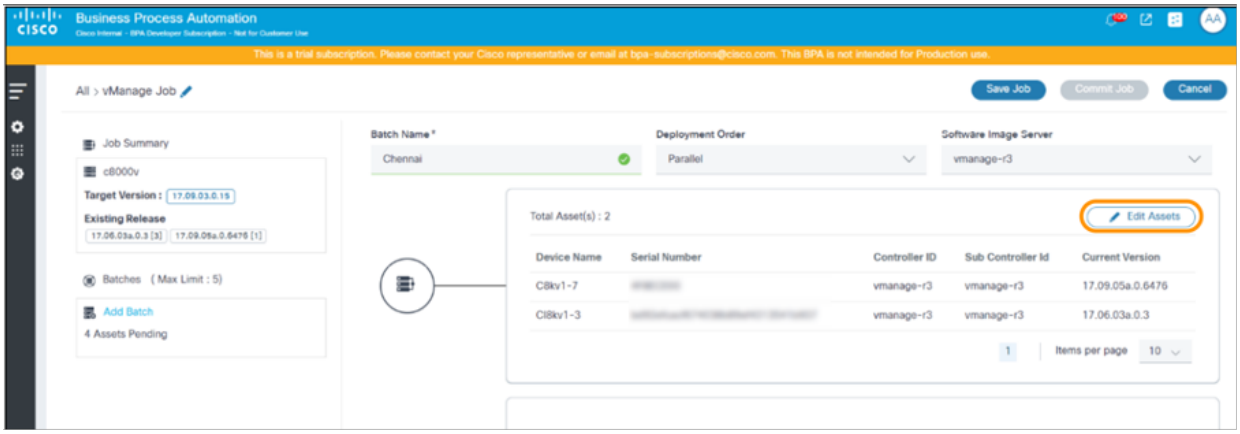
d. 저장 및 닫기를 클릭합니다.

재설정을 클릭하면 선택 항목이 취소되고 자산 선택 항목의 원래 상태가 유지됩니다.



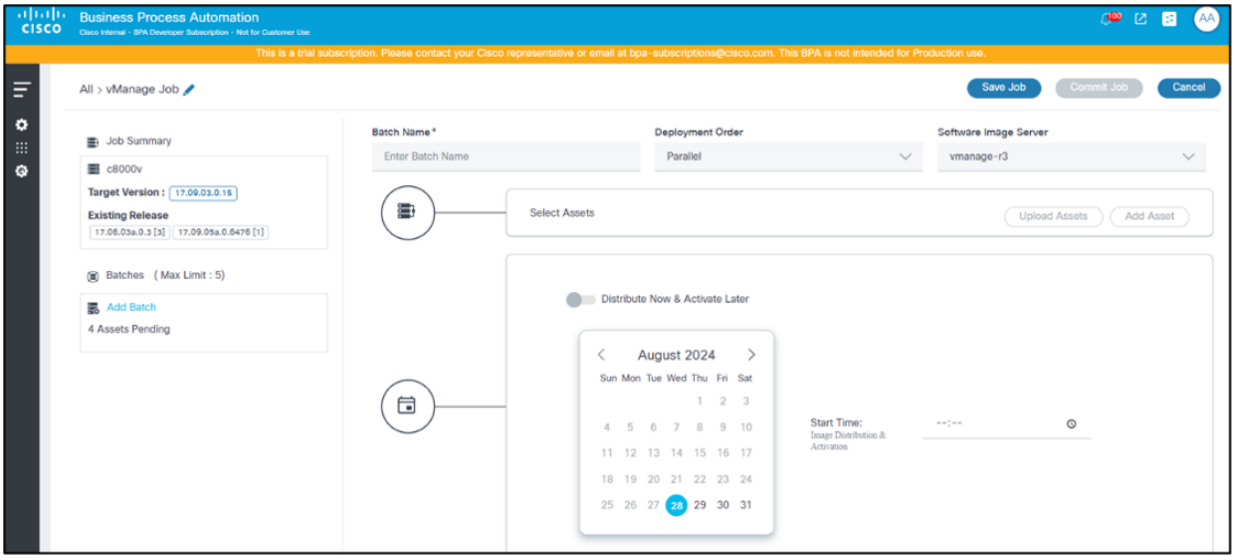
재설정

e. 자산 선택을 수정해야 하는 경우 자산 편집을 클릭합니다.



에셋 일괄 편집

f. 필요한 사항을 변경하려면 에셋을 선택하거나 지우고 저장 및 닫기를 클릭합니다. 배치 자산을 편집하는 동안 다른 작업과 배치의 일부인 현재 선택된 자산은 체크 표시와 배치명 열에 표시된 배치명을 사용하여 식별할 수 있습니다.



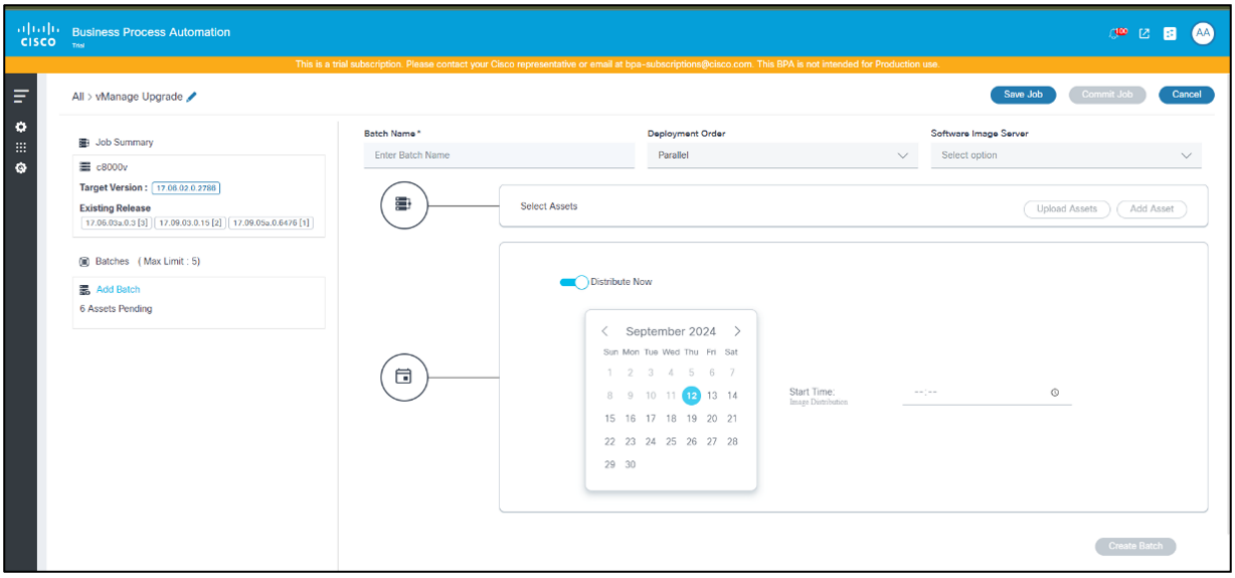
업그레이드 작업 스케줄러

15. 현재 배치에 대해 선택한 업그레이드 유형을 트리거할 시간을 예약하려면 날짜 선택에서 날짜를 선택하고 시간 선택에서 시간을 선택합니다.

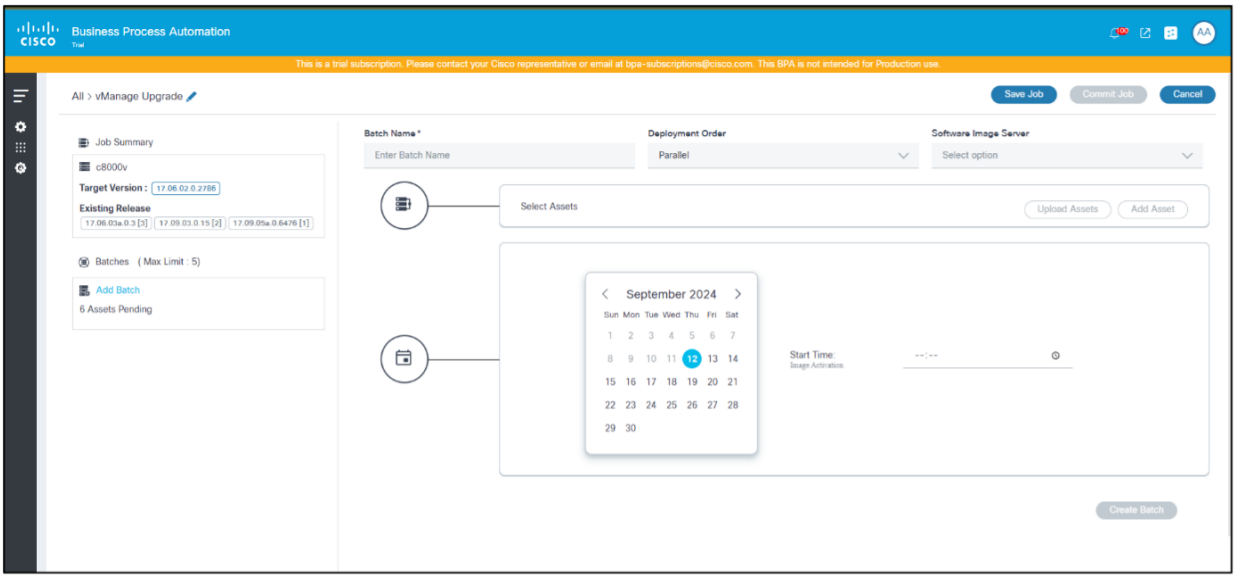
참고: 선택한 작업 유형이 사용 가능한 스케줄의 유형을 변경합니다.

가능한 시나리오는 다음과 같습니다.

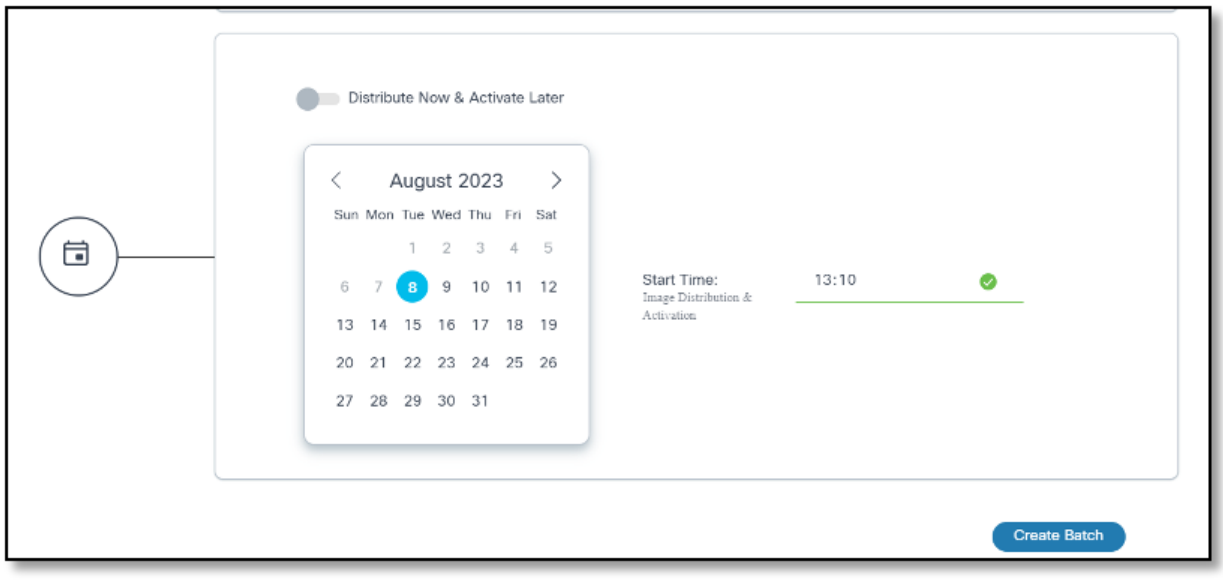
작업 유형	지금 배포 토글	예약 날짜 및 시간	배포 세부 정보
배포	기본적으로 비활성화됨	활성	지정된 예약 날짜 및 시간에 배포가 발생합니다.
배포	활성화됨	비활성화됨	작업 커밋 후 배포가 발생합니다.
활성화	해당 없음	활성	지정된 날짜 및 시간에 활성화
배포 및 활성화	기본적으로 비활성화됨	활성	배포 및 활성화는 지정된 날짜 및 시간에 수행됩니다.
배포 및 활성화	활성화됨	활성	배포는 작업 커밋 후 발생하며, 지정된 예약 날짜 및 시간에 활성화 트리거됩니다.



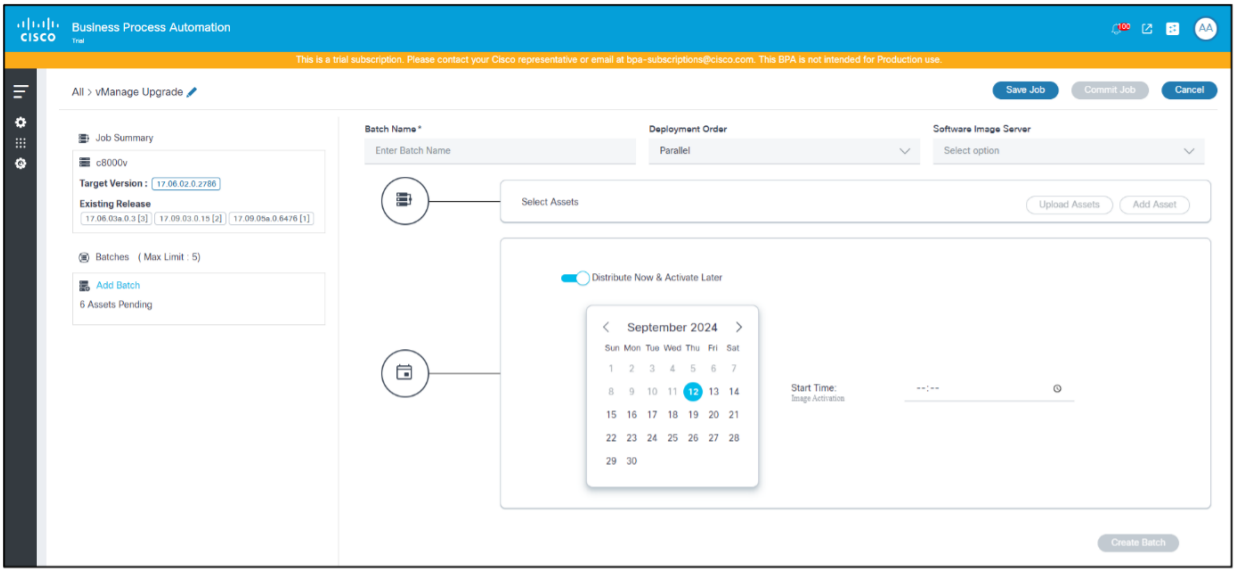
배포 작업 유형 일정 옵션



활성화 작업 유형 일정 옵션



배포 및 활성화 작업 유형 일정 옵션

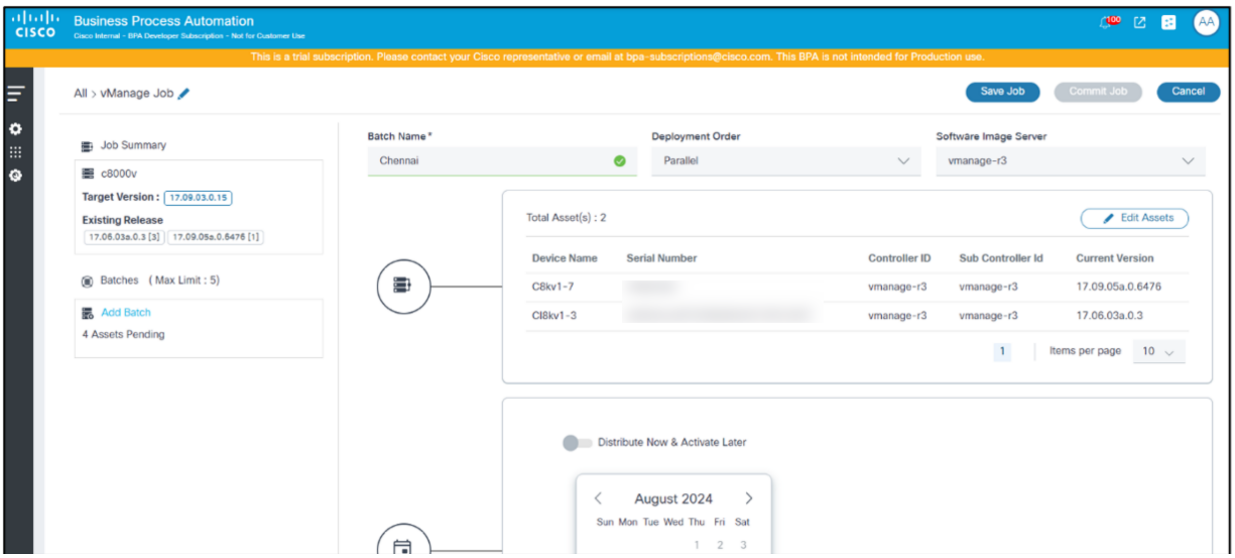


배포 및 활성화 작업 유형 일정 옵션 - 지금 배포 및 나중에 활성화 전환

참고: 다음 목록에 유의해야 합니다.

- 여러 배치를 스케줄링할 때 시스템 과부하를 방지할 수 있도록 두 배치 간의 시간 간격을 제공합니다. 여러 배치가 겹치는 경우 단일 배치에 추가하는 것이 좋습니다.
- [지금 배포] 및 [나중에 활성화] 토글이 활성화된 경우 작업 커밋 시간과 활성화 일정 사이에 시간 간격을 제공합니다. 그렇지 않은 경우 활성화 워크플로는 수동 개입이 필요한 사용자 작업을 생성할 수 있습니다. 즉, 사용자는 배포가 완료될 때까지 기다렸다가 다시 시도해야 합니다.

16. 배치 생성을 누릅니다. 배치는 페이지 왼쪽에서 볼 수 있습니다.



작업 생성 - 작업 커밋

필요한 만큼 배치를 생성합니다. 필요한 모든 정보를 사용할 수 있을 때까지 작업이 초안 상태가 될 수 있습니다.

참고: 작업 저장을 눌러 초안을 저장하면 작업 데이터가 손실되지 않습니다.

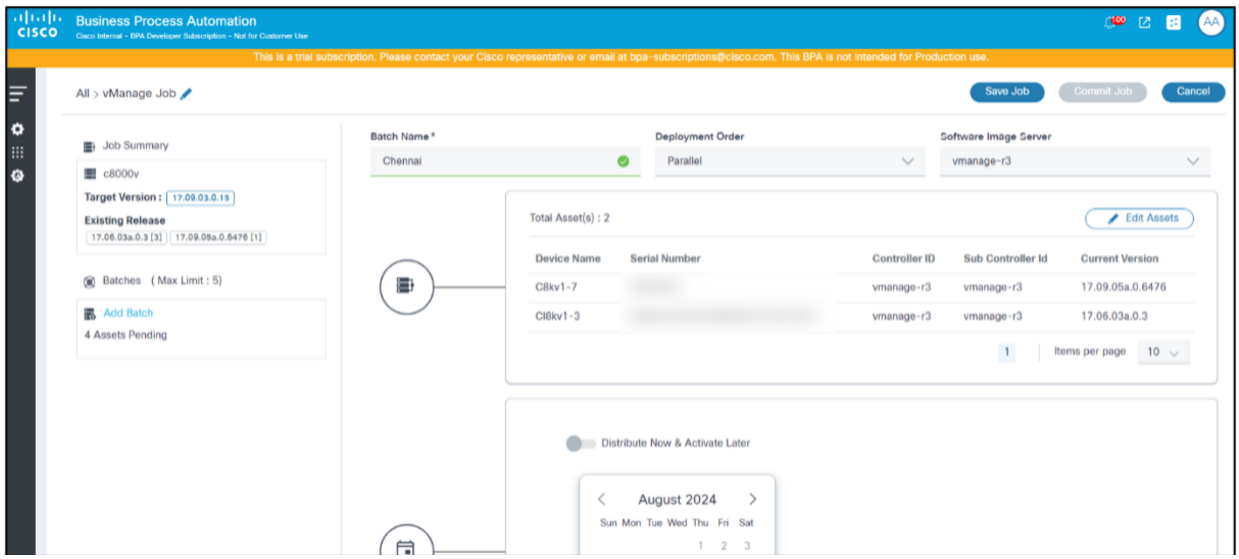
17. 작업 생성을 완료하려면 작업 커밋을 클릭합니다. 일괄 처리에 대해 일정이 트리거되면 작업은 배포 상태로 전환됩니다.

참고: 최대 배치 수에 대한 임계값은 Upgrade Policy(업그레이드 정책) 페이지에서 확장하거나 업데이트할 수 있습니다.

작업에서 배치 편집

참고: 작업이 초안 단계에 있는 경우에만 배치를 업데이트할 수 있습니다.

1. 왼쪽 패널에서 원하는 배치를 선택합니다.



에셋 편집

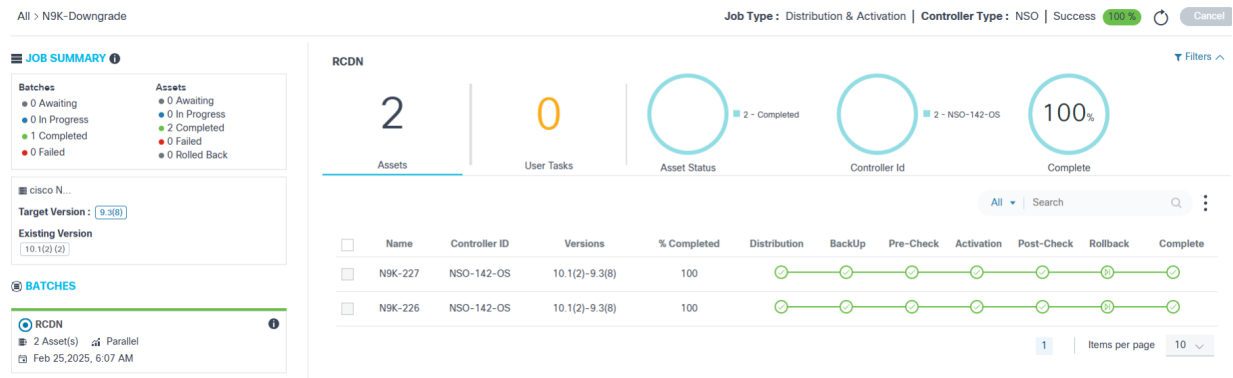
2. Edit Assets(에셋 편집)를 클릭합니다.
3. 자산 추가 또는 자산 업로드에서 자산을 선택 또는 정산하거나 일자 또는 시작 시간을 변경하여 배치 스케줄을 수정하여 필요한 변경을 수행합니다.
4. 배치 갱신을 누릅니다.

업그레이드 작업 실행 및 진행률 모니터링

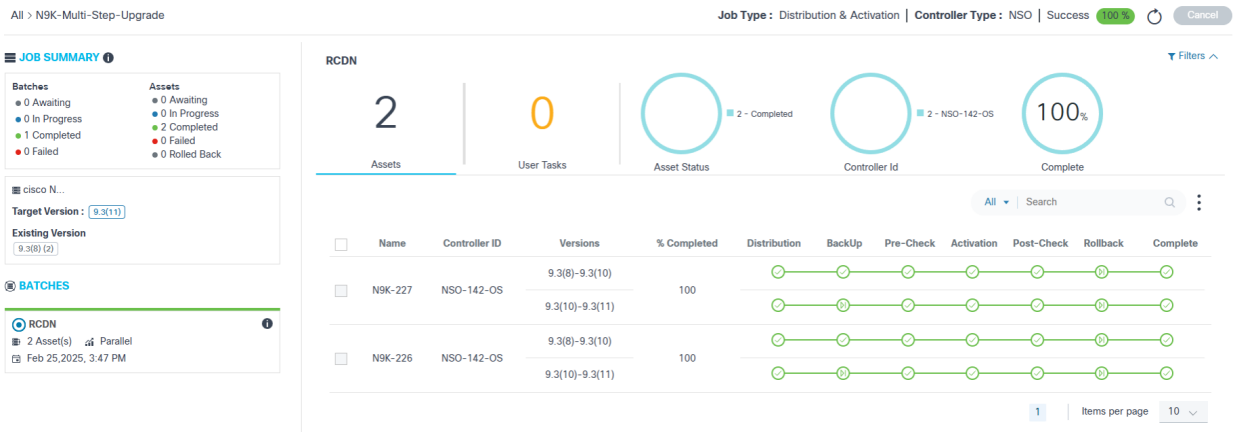
1. 업그레이드 작업에 액세스할 수 있는 자격 증명을 사용하여 BPA에 로그인합니다.
2. OS Upgrade(OS 업그레이드) > Upgrade Jobs(업그레이드 작업)를 선택합니다. [업그레이드 작업] 페이지가 표시됩니다.

업그레이드 작업

3. 작업을 신속하게 필터링하려면 검색 필터를 사용 가능한 차트 필터와 함께 사용합니다.
4. 원하는 작업을 클릭합니다. [작업 요약] 페이지가 표시됩니다.

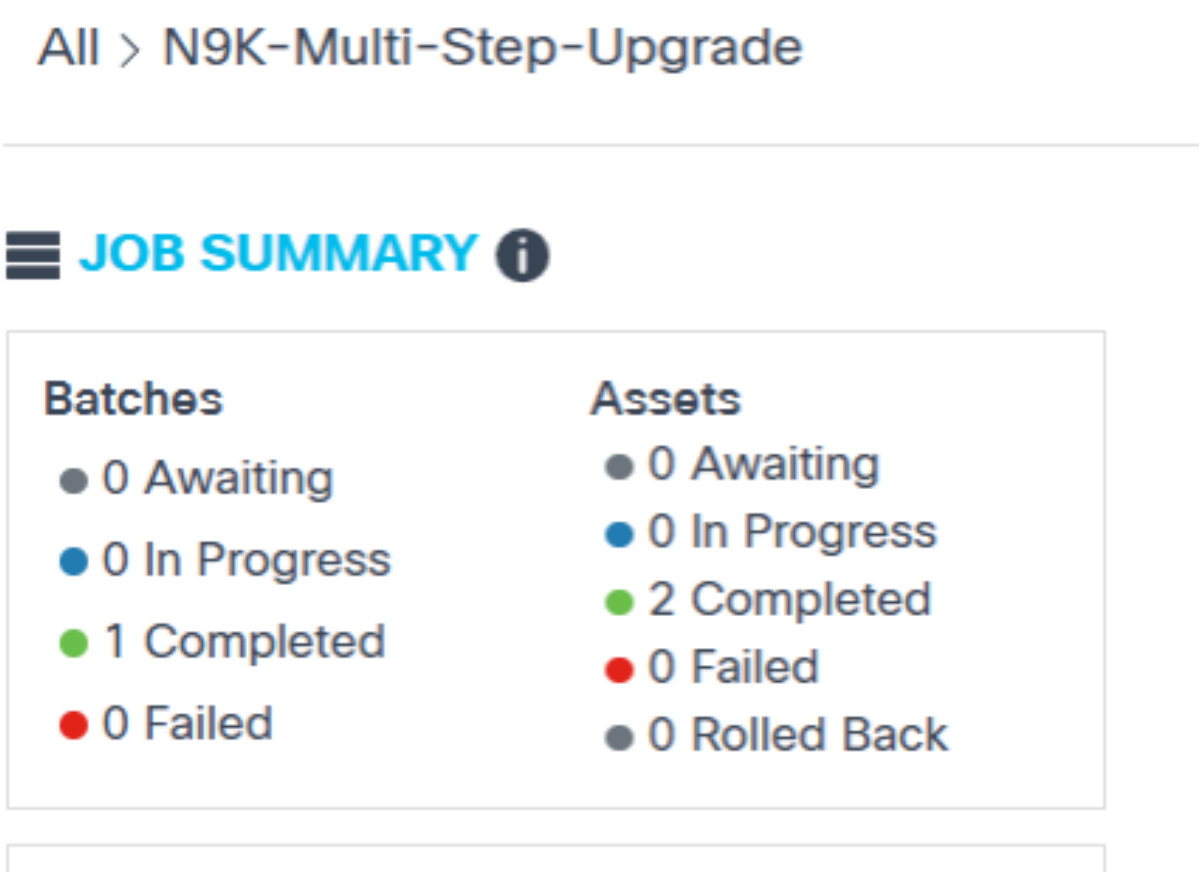


단일 단계 업그레이드



다단계 업그레이드

왼쪽 패널에서는 다음 정보를 제공합니다.



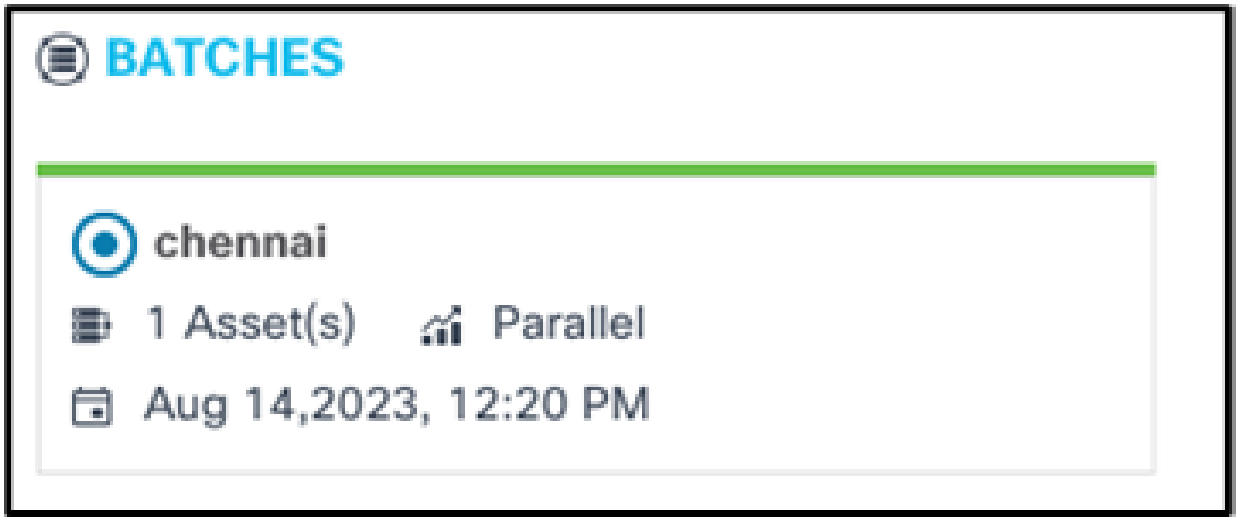
작업 요약

- 배치 및 개별 자산의 빠른 요약

적합성 정책 세부사항(정책에 모델이 하나인 경우)

적합성 정책 세부 정보(정책에 여러 모델이 있는 경우)

- 작업의 영향을 받는 장치 모델, 대상 소프트웨어 버전 및 기존 릴리스 버전
- 이 작업의 일부인 배치 목록



배치 세부 정보

- 배치 세부 정보:
  - 회색 위쪽 테두리는 배치가 일정을 기다리고 있음을 나타냅니다.
  - 파란색 위쪽 테두리는 배치 배포가 진행 중임을 나타냅니다.
  - 녹색 위쪽 테두리는 배치 구축이 완료되었음을 나타냅니다.

[작업 요약] 페이지의 맨 위에 다음 정보가 표시됩니다.

최상위 작업 요약

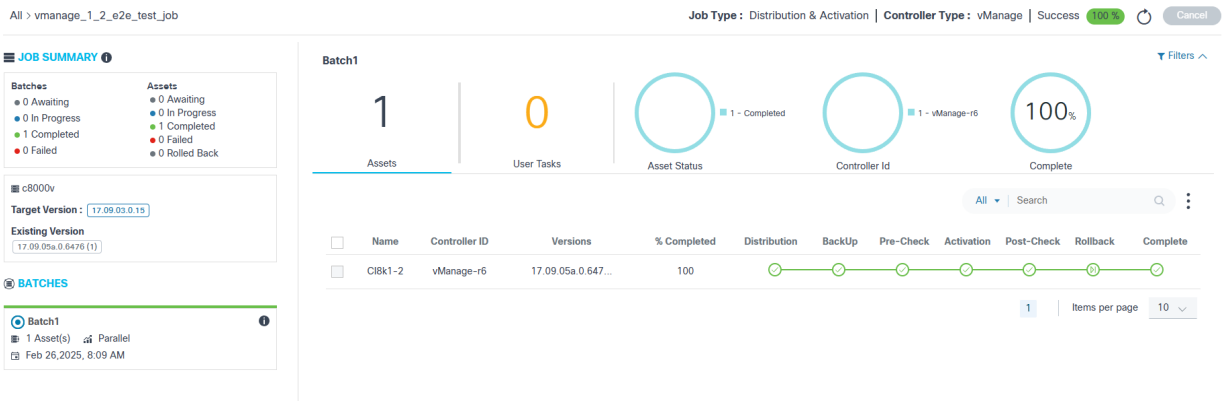
- 현재 작업의 이동 경로 탐색(예: All > vmanage_1_2_e2e). All 옵션이 Jobs Dashboard로 전환

됩니다
- 작업 유형
- 컨트롤러 유형
- 완료 백분율의 작업 상태:

    - 성공: 업그레이드 작업 성공
    - 실패: 어떤 이유로 인해 업그레이드 작업이 실패했습니다.
    - 진행 중: 업그레이드 작업이 진행 중입니다.

참고: 한 배치의 스케줄에 도달한 경우에도 작업 상태가 진행 중으로 이동됩니다.

- 대기 중: 작업이 커밋되었지만 하나 이상의 배치 스케줄에 도달할 때까지 대기 중입니다.



작업 요약

[작업 요약] 페이지에서는 다음 옵션을 사용할 수 있습니다.

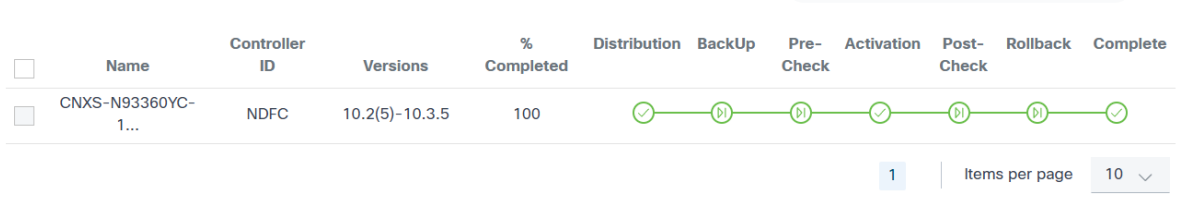
- Refresh(새로 고침) 아이콘을 사용하면 온디맨드 방식으로 업데이트를 검색할 수 있습니다
- 취소는 배치에 대한 일정에 도달하지 않는 한 초안 및 커밋 단계의 작업을 취소하는 데 사용됩니다
- 활성화를 선택하면 이전에 완료된 작업의 일부였던 것과 동일한 배치 및 에셋을 사용하여 초안 상태에서 새 활성화 작업이 생성됩니다

    - 활성화는 작업 유형이 배포이고 성공적으로 완료된 경우에만 사용할 수 있습니다
    - 활성화 작업이 이미 만들어져 있고 활성화를 클릭하면 이전에 만든 작업의 상태와 함께 메시지가 표시되고 이미 만든 작업을 리디렉션할 수 있는 옵션이 제공됩니다. 새로 생성된 작업에서 사용자는 배치나 에셋을 편집하거나 삭제할 수 있는 옵션이 있지만 작업 유형, 컨트롤러 유형 및 적합성 정책은 편집할 수 없습니다.
- 분석 섹션 아래에 페이지별로 구분된 자산 목록이 표시됩니다
- 검색 필드는 다음과 같은 열에 대한 일반 및 필드별 검색을 허용합니다.

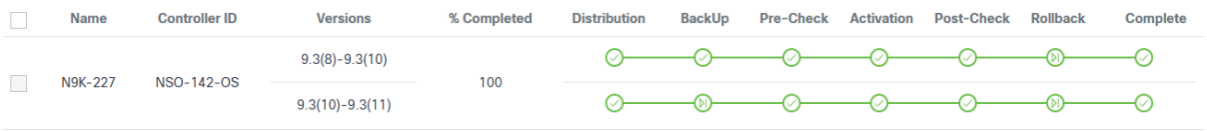
    - 디바이스 이름
    - 컨트롤러 ID
    - 일련 번호

배치 보고서 다운로드

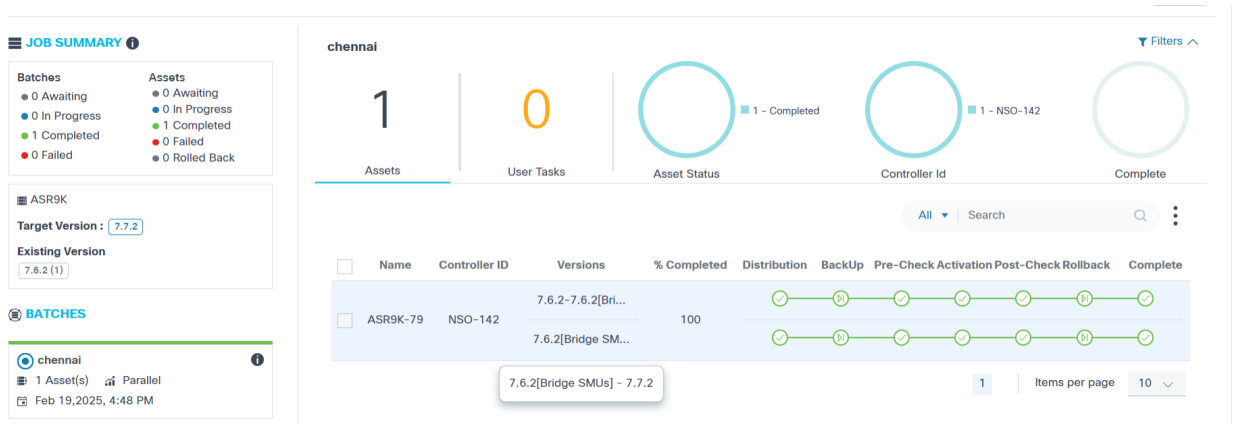
- 추가 옵션 아이콘 > 다운로드를 선택하여 배치 레벨 보고서를 다운로드하는 옵션입니다. 이 보고서는 장비 세부사항이 포함된 배치 레벨 세부사항으로 구성됩니다



정렬 - 단일 단계 업그레이드



정렬 - 다단계 업그레이드



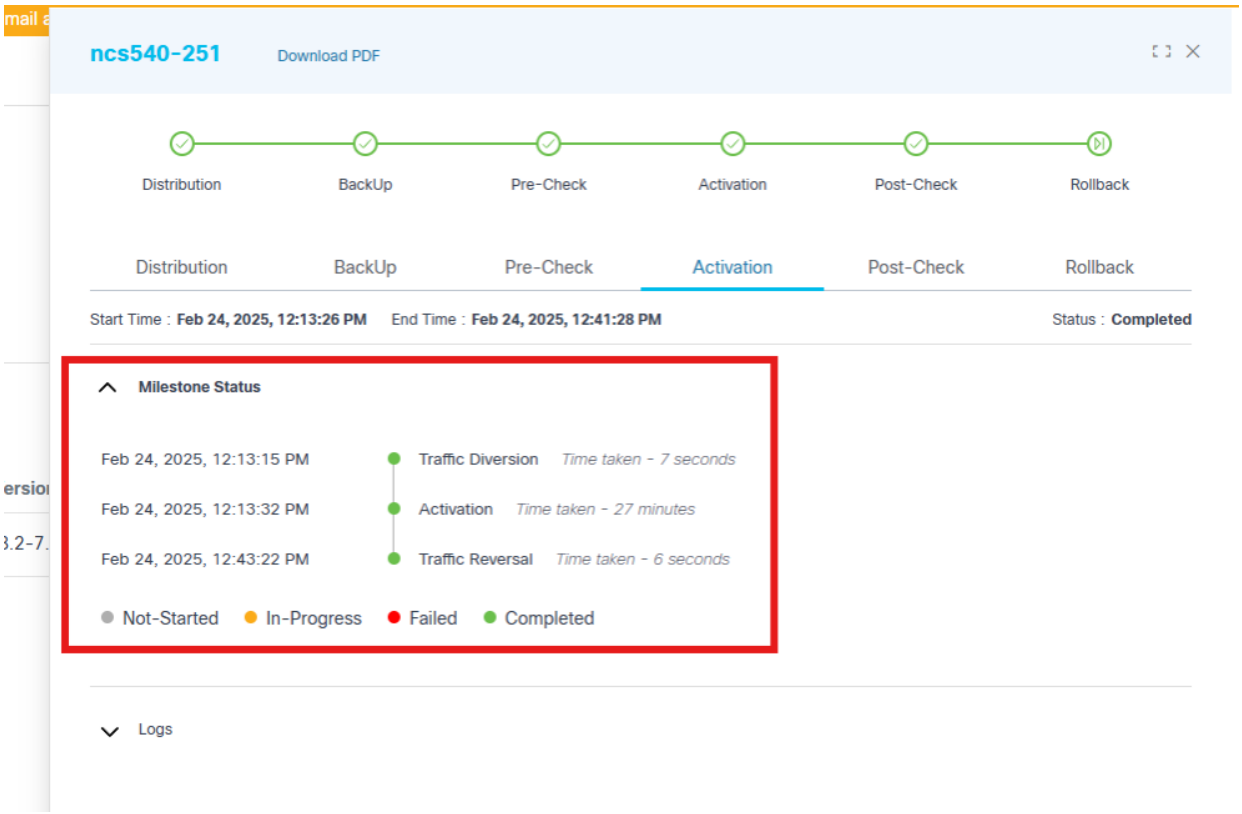
정렬 - 브리지 SMU 업그레이드

- 열 이름을 클릭하여 정렬할 수 있습니다.
- 이름, 컨트롤러 ID, 버전, % 완료됨과 함께 각 디바이스에 대해 다음 업그레이드 이정표가 표시됩니다.
    - 배포
    - 백업

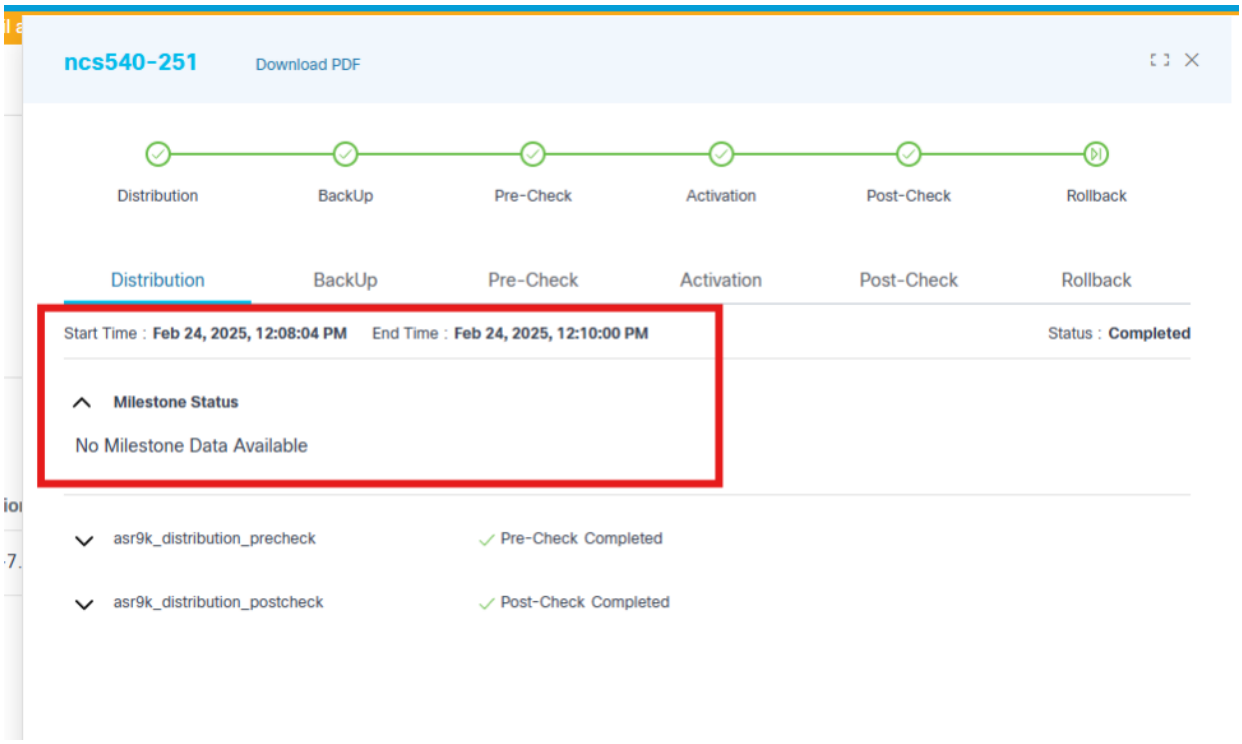
- 사전 점검
- 트래픽 전용
- 활성화
- 사후 점검
- 트래픽 반전
- 롤백
- 완료

참고: % 완료됨은 디바이스에 대해 완료된 이정표의 수를 기준으로 진행률을 표시합니다. 배치 내의 모든 장치 레벨 완료 퍼센트가 합산되어 배치 완료 퍼센트가 계산됩니다. 차례로 모든 배치 완료 백분율을 합산하여 작업 레벨 완료 백분율을 계산합니다.

사용자 지정 이정표라고도 하는 하위 이정표는 표준 이정표 아래에서 추가 시 실행되고 표시되는 중간의 중요 단계입니다. 사용자 지정 이정표 추가에 대한 자세한 내용은 BPA Developer Guide를 참조하십시오.



하위 이정표 보기(표준 이정표 이름 아래에 하위 이정표가 추가된 경우)

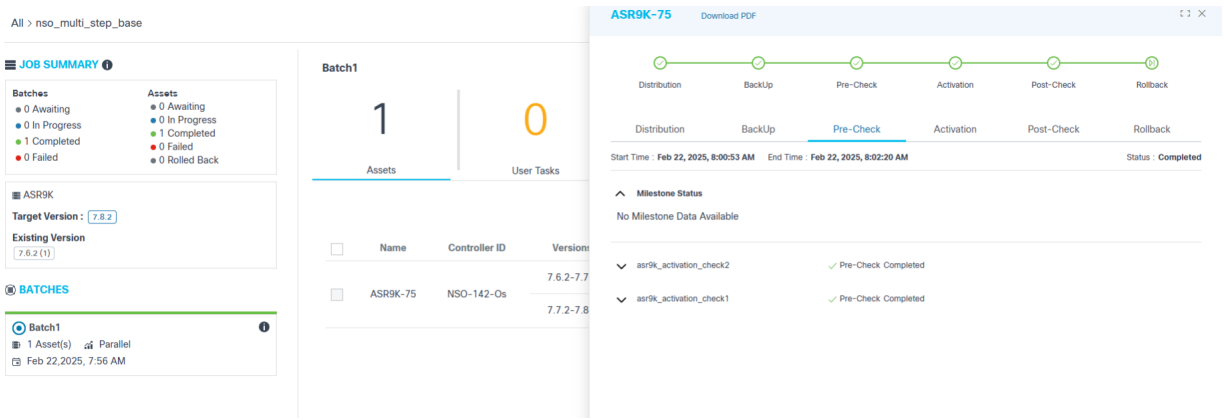


하위 이정표 보기(표준 이정표 이름 아래에 하위 이정표가 추가되지 않은 경우)

참고: 이정표는 선택한 작업 유형에 따라 달라집니다. TrafficReversal 중요 시점은 배포 작업에 사용할 수 없습니다.

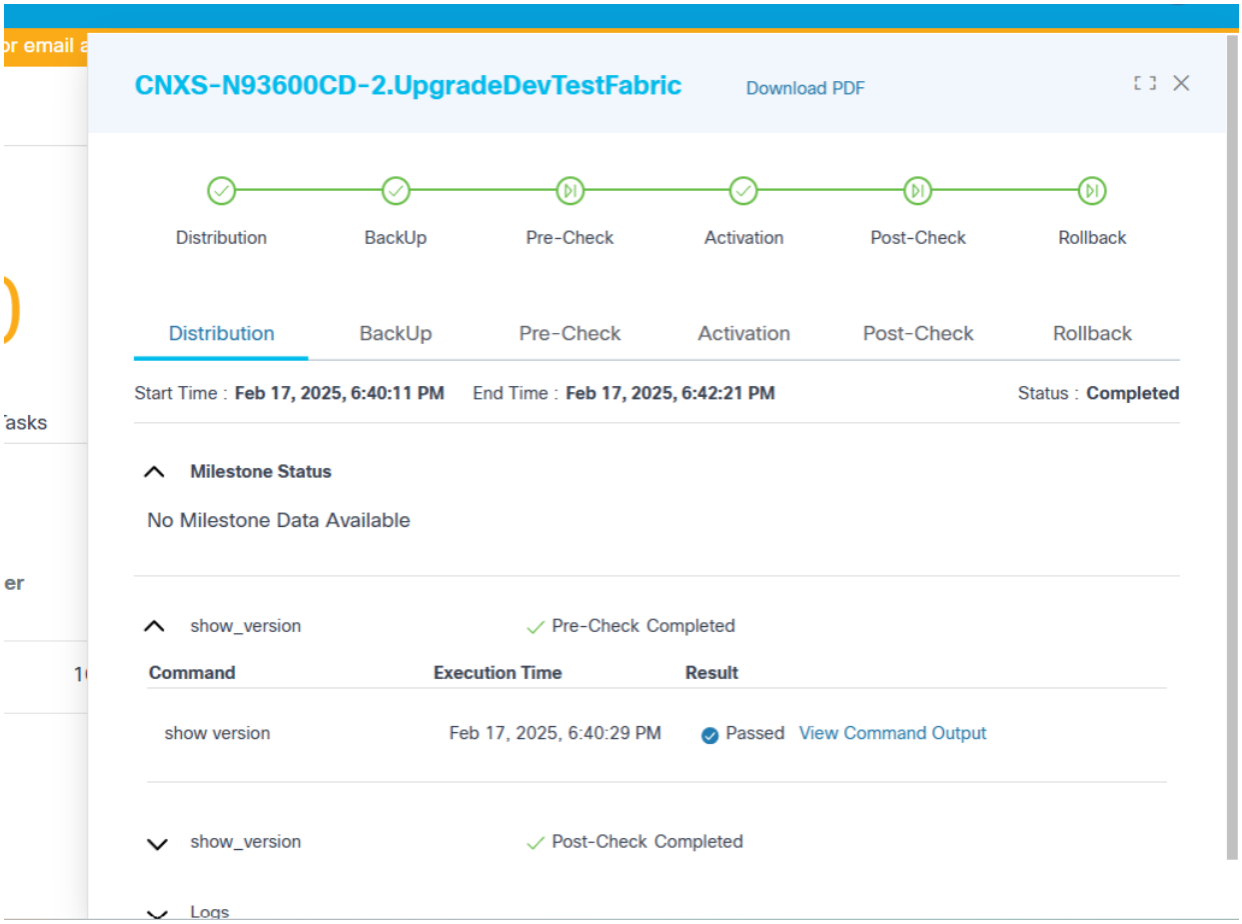
트래픽 전환 및 트래픽 전환은 활성화 이정표에 따라 이동됩니다.

- 다음으로 구성된 이정표 색 범례입니다.
  - 회색 체크: 보류 중
  - 파란색 검사: 진행 중
  - 녹색 플래그: 건너뜀
  - 녹색 확인: 완료됨
  - 주황색 확인: 사용자 작업
  - 빨간색 체크: 실패



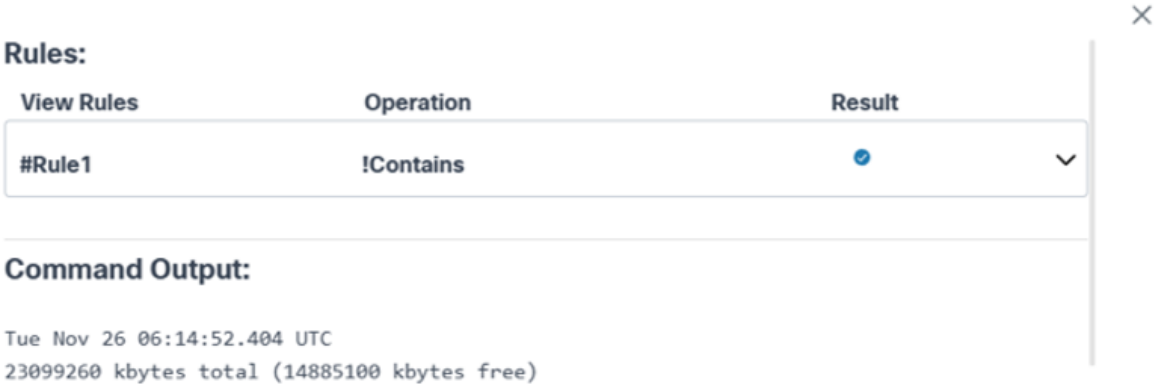
사전 확인 및 사후 확인 중요 시점 보기

사전 확인 또는 사후 확인 실행 이정표의 경우, 사용자는 각 프로세스 템플릿에 구성된 모든 명령에 대한 검증 규칙 및 상태와 함께 전체 명령 출력을 볼 수 있습니다.



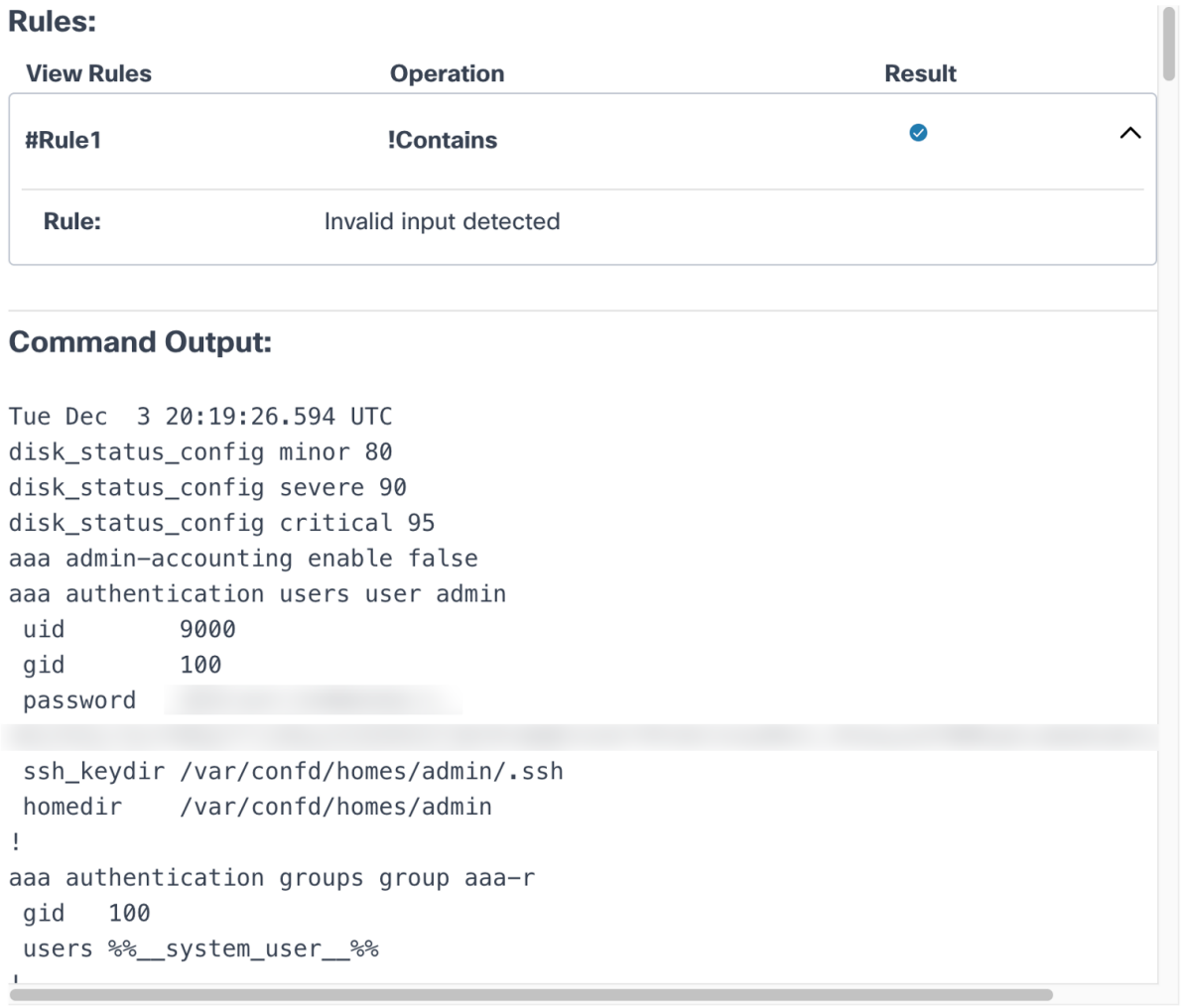
사전 검사 명령 출력이 있는 배포 중요 시점 보기

1. 명령 출력 및 pre- 및 post-check 명령과 연결된 규칙을 보려면 View Command Output(명령 출력 보기) 링크를 클릭합니다.

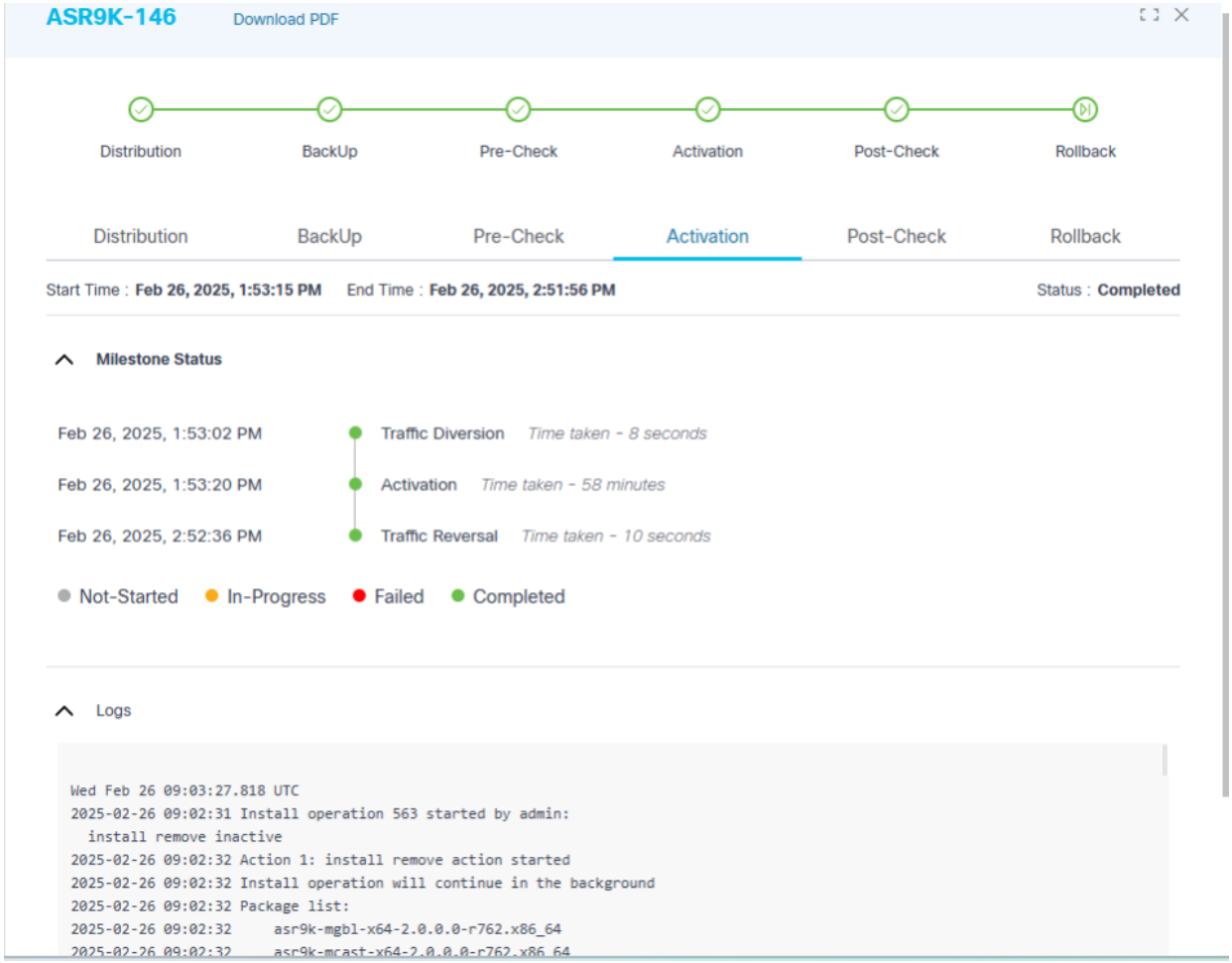


사전 및 사후 검사 명령 출력 및 관련 규칙

2. 각 규칙의 전체 세부사항을 보려면 Expand(확장) 아이콘을 선택합니다.



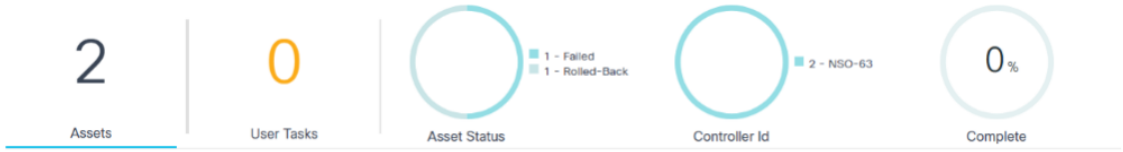
유효성 검사 규칙이 있는 사전 검사 및 사후 검사 명령 출력



라이브 로그가 있는 활성화 중요 시점 보기

위 그림에는 특정 디바이스의 소프트웨어 활성화 진행 상황을 모니터링하는 데 도움이 되는 라이브 로그가 포함된 활성화 이정표의 세부 정보가 나와 있습니다.

이정표가 시작되거나 완료되면 이정표를 클릭하면 자세한 정보가 표시됩니다.



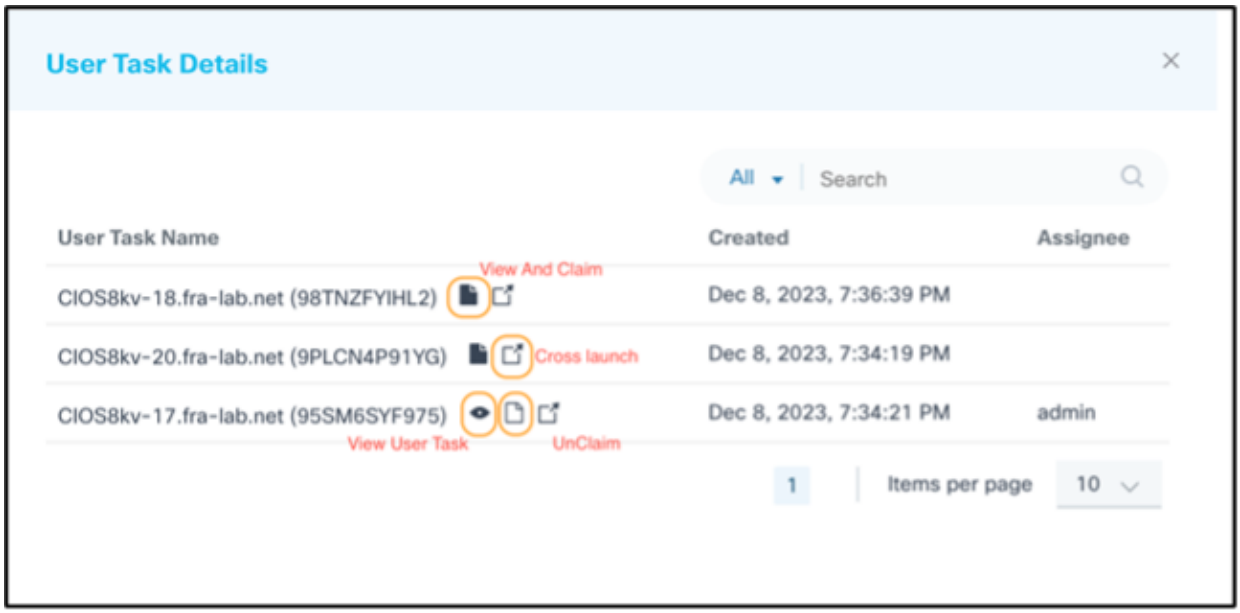
분석 섹션

작업 요약 페이지 상단에 표시되는 분석 섹션에는 현재 선택한 작업과 관련된 다음 정보가 표시됩니다.

- 배치 이름(예: 아시아)
- ^을(를) 필터링하여 분석 섹션을 확장합니다.
- 다음 배치 상세내역이 순서대로 표시됩니다.
    - 자산: 총 자산 수

- 사용자 작업: 작업 사용자 또는 관리자의 입력을 대기하는 총 사용자 작업 수
- 자산 상태: 상태에 따라 배치 디바이스를 필터링합니다. 성공적으로 롤백된 디바이스를 식별하는 데 도움이 되도록 Rollback(롤백) 필터가 추가되었습니다.
- 컨트롤러 ID: 선택한 컨트롤러 ID에 속하는 배치 디바이스를 필터링합니다.
- 완료: 전체 배치 완료 퍼센트

사용자 작업에 대해 작업을 수행하려면 사용자 작업 수를 클릭합니다. 다음과 함께 사용자 작업 세부 정보 창이 열립니다.



사용자 작업 세부 정보

- 주의가 필요한 각 장치에 해당하는 사용자 작업 목록
- 사용자 작업 옵션에 대한 다음 아이콘:

  - 보기 및 클레임: 사용자 작업 세부 정보 보기
  - 교차 실행: 기본 UI에서 BPA 워크플로 작업 보기
  - 클레임 취소: 사용자 작업 할당 제거
  - 사용자 작업 보기: 사용자 작업 세부 정보 보기

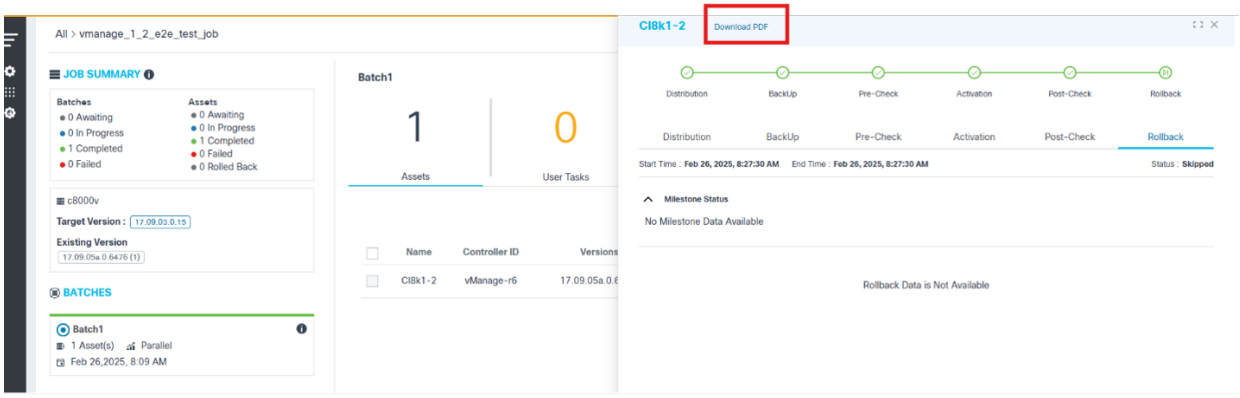
사용자 작업

사용자 작업의 보기 옵션

- 다음 옵션은 작업 컨텍스트에 따라 표시됩니다.
    - 다시 시도: 작업 다시 실행
    - 모두 다시 시도: 모든 사전 및 사후 검사를 다시 실행합니다.
    - 계속: 다음 작업으로 계속 진행
    - 롤백: 이전 버전으로 롤백합니다. 이 옵션은 활성화 또는 사후 검사에 실패하거나 사전 /사후 검사 사이에 잘못된 차이가 있을 때 사용할 수 있습니다
    - 취소: 현재 작업을 취소합니다.
    - 닫기: 사용자 작업 창을 닫습니다.
- 사용자 작업(있는 경우)에 대해 작업을 수행하고 새로 고침 아이콘을 선택하여 총 사용자 작업 수를 새로 고칩니다
- 총 배치 완료 퍼센트
- 컨트롤러 ID로 필터링할 수 있는 클릭 가능한 차트

참고: 컨트롤러 ID 앞의 숫자는 각 컨트롤러에서 관리하는 디바이스의 총 수를 나타냅니다.

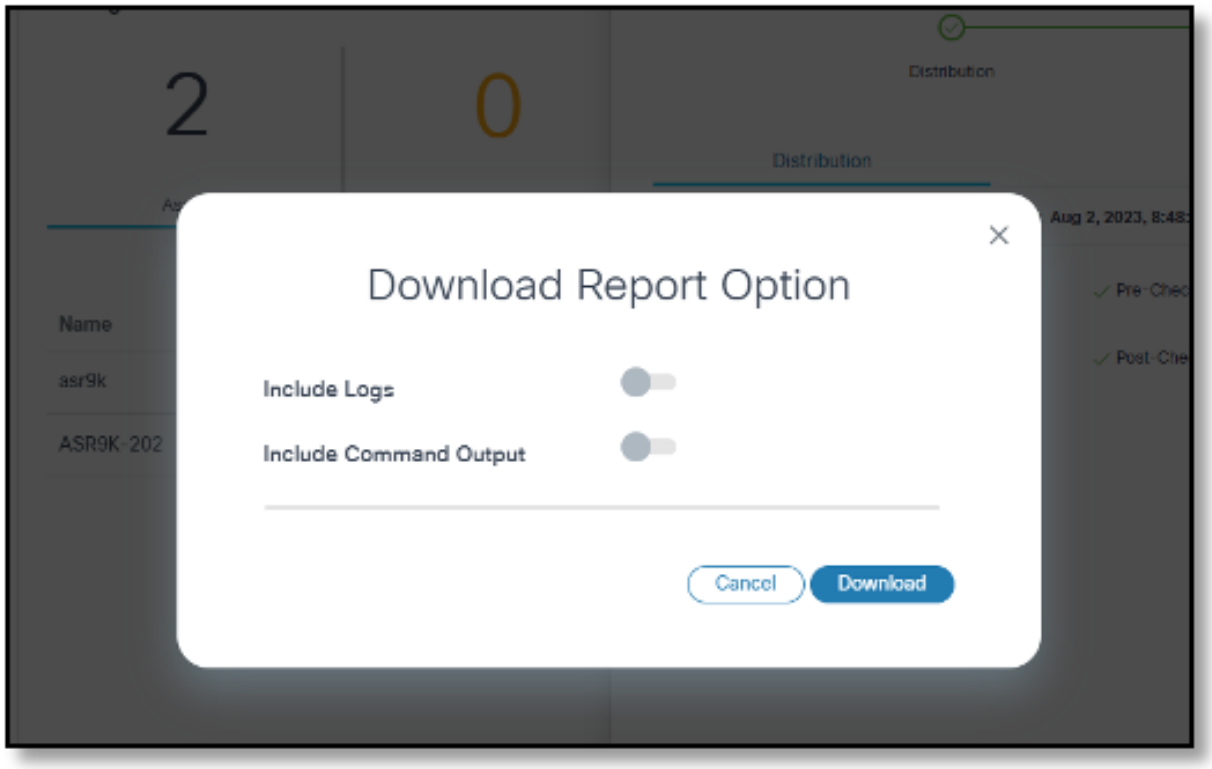
소프트웨어 업그레이드 보고서 다운로드



PDF 다운로드

디바이스 이름이 표시되고 세부 정보 보기의 헤더에 Download PDF(PDF 다운로드)가 표시됩니다. 사용자는 현재 선택한 디바이스에 대한 업그레이드 보고서를 PDF 형식으로 생성하고 다운로드할 수 있습니다. 업그레이드 보고서를 PDF 형식으로 다운로드하려면

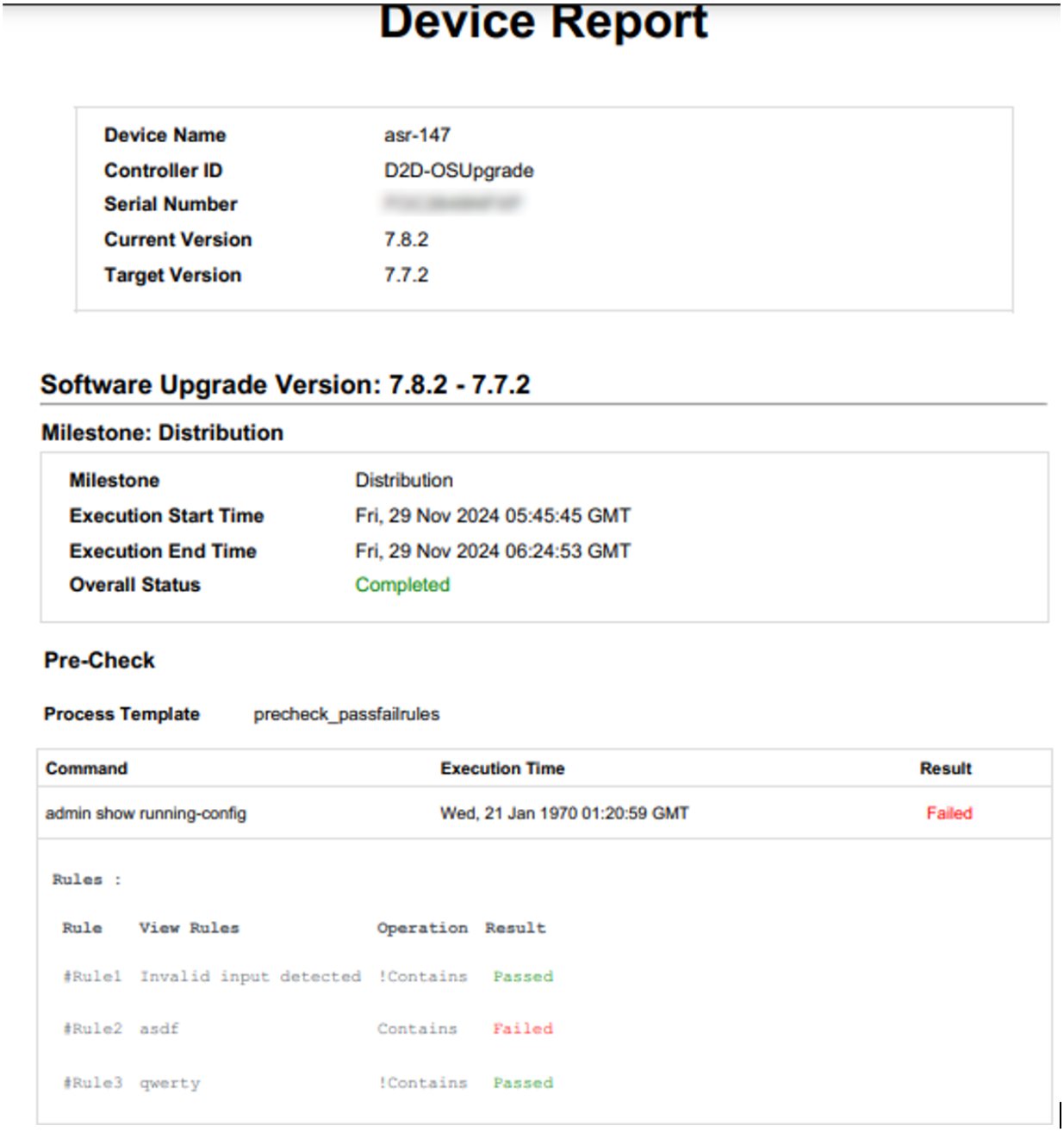
1. PDF 다운로드를 클릭합니다. 보고서 다운로드 옵션 창이 열립니다.



보고서 다운로드 옵션

2. Include Logs(로그 포함) 및 Include Command Outputs(명령 출력 포함) 토글을 활성화합니다 .
    - 로그 포함: 보고서에 라이브 로그(있는 경우) 포함
    - 명령 출력 포함: 보고서에 사전 확인 및 사후 확인의 명령 출력을 포함합니다. 이 경우, 규칙 뒤에 명령 출력이 옵니다
3. Download(다운로드)를 클릭합니다. 보고서 생성이 시작됩니다.

참고: Include Logs 및 Include Command Output 토글을 모두 활성화하면 보고서 생성 및 보고서 크기의 처리 시간이 늘어납니다. 자세한 보고서가 필요한 경우에만 이 토글을 사용하십시오. 명령 규칙은 명령 출력 토글이 On 또는 Off인지에 관계없이 보고서에 포함됩니다.



Device Report

Device Name	asr-147
Controller ID	D2D-OSUpgrade
Serial Number	
Current Version	7.8.2
Target Version	7.7.2

Software Upgrade Version: 7.8.2 - 7.7.2

Milestone: Distribution

Milestone	Distribution
Execution Start Time	Fri, 29 Nov 2024 05:45:45 GMT
Execution End Time	Fri, 29 Nov 2024 06:24:53 GMT
Overall Status	Completed

Pre-Check

Process Template precheck_passfailrules

Command	Execution Time	Result
admin show running-config	Wed, 21 Jan 1970 01:20:59 GMT	Failed

Rules :

Rule	View Rules	Operation	Result
#Rule1	Invalid input detected	!Contains	Passed
#Rule2	asdf	Contains	Failed
#Rule3	qwerty	!Contains	Passed

장치 보고서

보관 작업

1. 업그레이드 작업에 액세스할 수 있는 자격 증명을 사용하여 BPA에 로그인합니다.
2. OS Upgrade(OS 업그레이드) > Upgrade Jobs(업그레이드 작업)를 선택합니다. [업그레이드 작업] 페이지가 표시됩니다.
3. 검색 필터를 사용 가능한 차트 필터와 함께 사용하여 작업을 필터링합니다.
4. 작업을 하나 이상 선택합니다.

아카이브 작업

5. More Options(추가 옵션) 아이콘 > Archive(아카이브)를 선택합니다.

참고: 완료된 작업만 보관할 수 있습니다.

작업 삭제

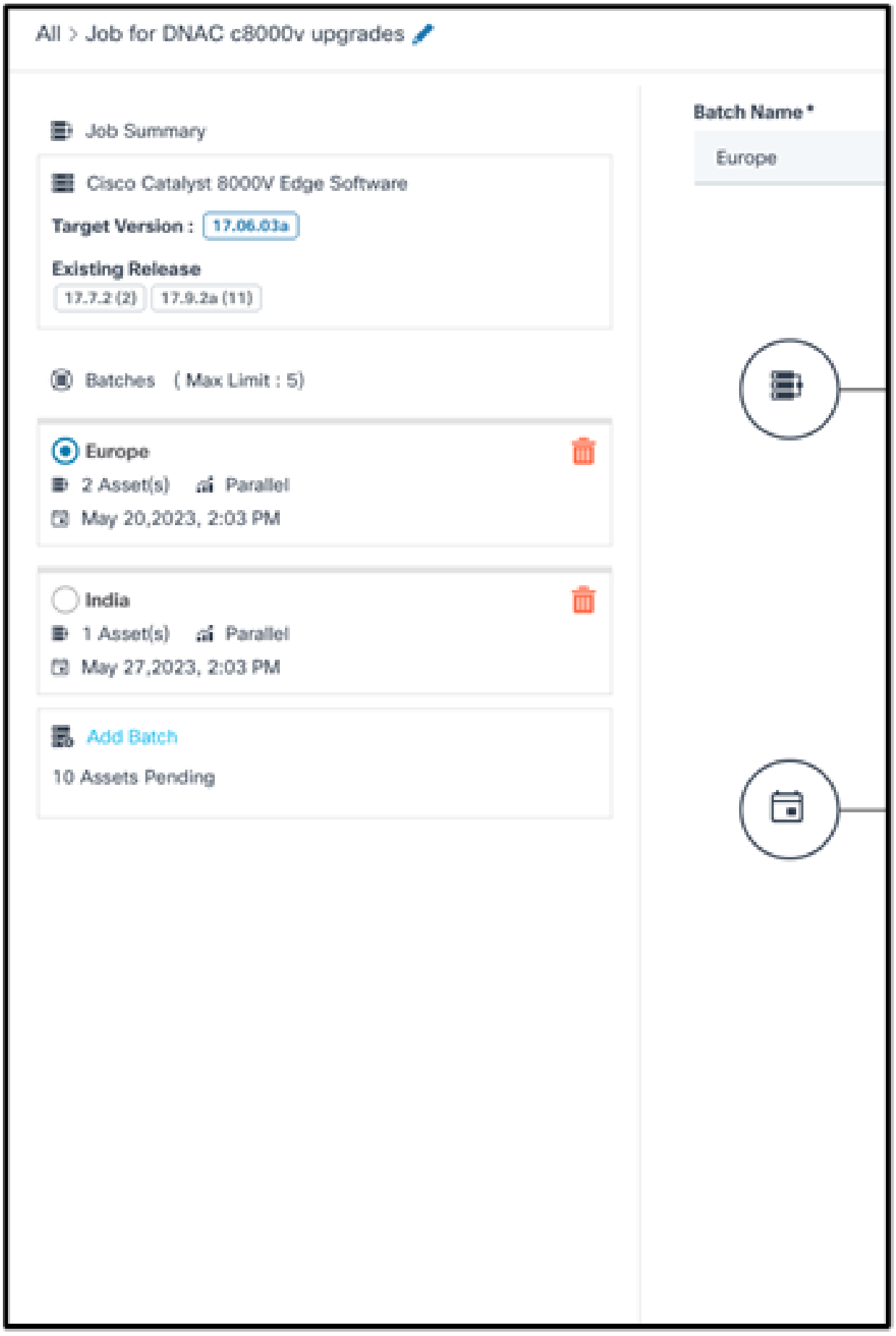
1. 업그레이드 작업에 액세스할 수 있는 자격 증명을 사용하여 BPA에 로그인합니다.
2. OS Upgrade(OS 업그레이드) > Upgrade Jobs(업그레이드 작업)를 선택합니다. [업그레이드 작업] 페이지가 표시됩니다.
3. 검색 필터를 사용 가능한 차트 필터와 함께 사용하여 작업을 필터링합니다.
4. 작업을 하나 이상 선택합니다.

작업 삭제

5. 추가 옵션 아이콘 > 작업 삭제를 선택합니다.

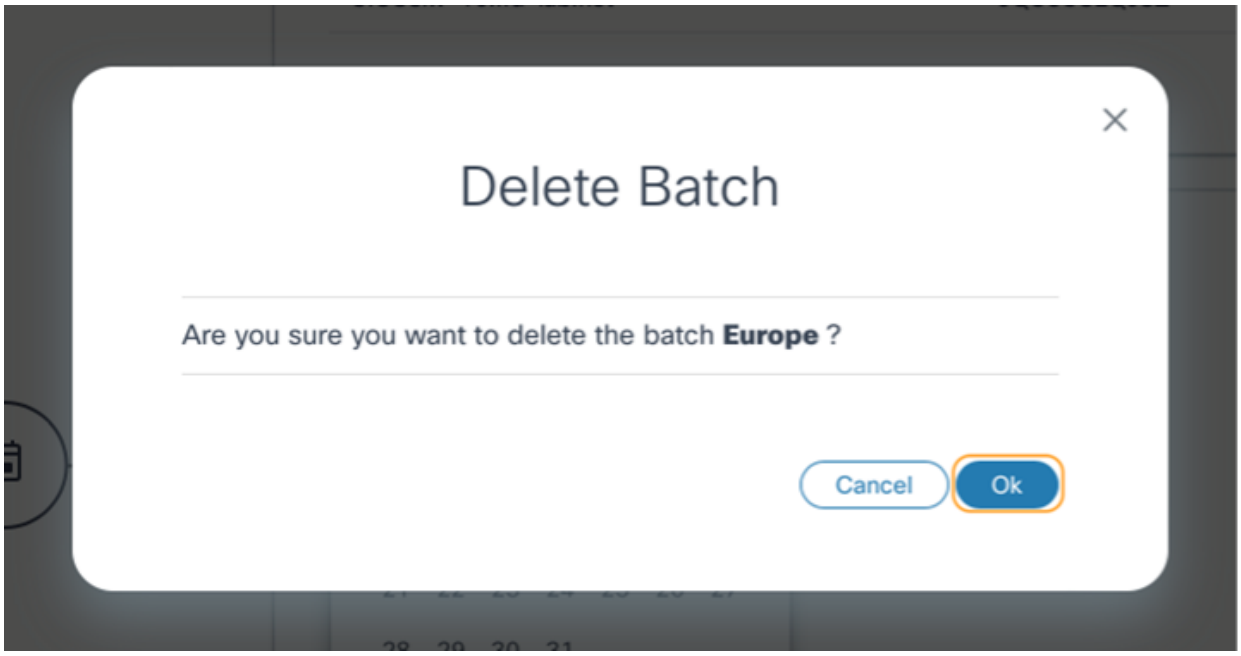
참고: 작업은 초안 단계에 있을 때만 삭제할 수 있습니다.

작업에서 배치 삭제


All > Job for DNAC c8000v upgrades
Job Summary
Cisco Catalyst 8000V Edge Software
Target Version : 17.06.03a
Existing Release
17.7.2 (2)
17.9.2a (11)
Batches (Max Limit : 5)
Europe
2 Asset(s)
Parallel
May 20,2023, 2:03 PM
India
1 Asset(s)
Parallel
May 27,2023, 2:03 PM
Add Batch
10 Assets Pending
Batch Name *
Europe

작업에서 배치 삭제

1. 측면 패널에서 원하는 배치의 삭제 아이콘을 선택합니다. 확인 창이 열립니다.



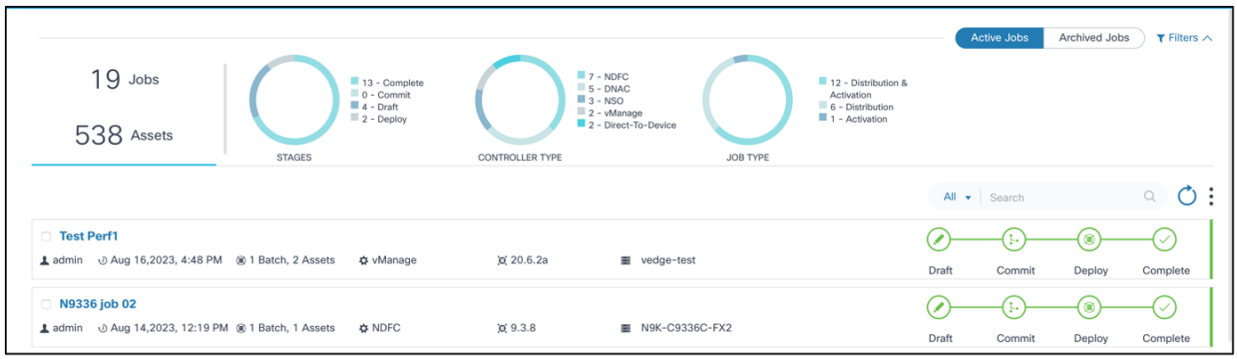
배치 삭제 확인

2. OK(확인)를 클릭합니다.

삭제된 배치와 연관된 자산은 보류 중인 자산 풀로 반환되며 신규 또는 기존 배치에서 선택할 수 있습니다.

작업 취소

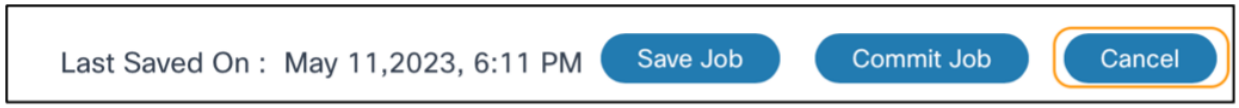
1. 업그레이드 작업에 액세스할 수 있는 자격 증명을 사용하여 BPA에 로그인합니다.
2. OS Upgrade(OS 업그레이드) > Upgrade Jobs(업그레이드 작업)를 선택합니다. [업그레이드 작업] 페이지가 표시됩니다.



업그레이드 작업

3. 원하는 작업을 필터링하려면 검색 필터를 사용 가능한 차트 필터와 함께 사용합니다.

4. 원하는 작업을 클릭합니다. [작업 요약] 페이지가 표시됩니다.



취소

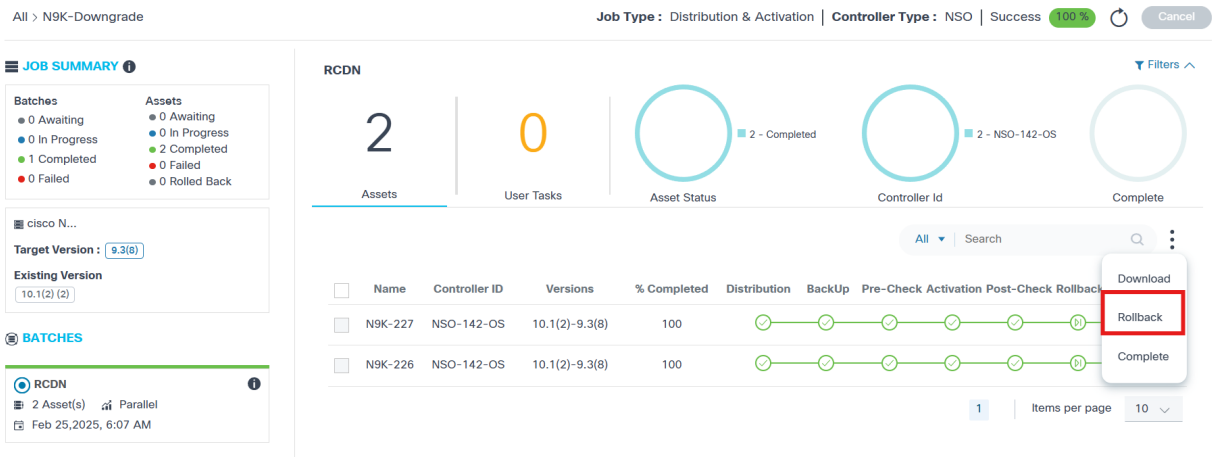
5. 취소를 클릭합니다.

완료된 작업 또는 업그레이드 롤백

1. 업그레이드 작업에 액세스할 수 있는 자격 증명을 사용하여 BPA에 로그인합니다.
2. OS Upgrade(OS 업그레이드) > Upgrade Jobs(업그레이드 작업)를 선택합니다. [업그레이드 작업] 페이지가 표시됩니다.

업그레이드 작업

3. 원하는 작업을 필터링하려면 검색 필터를 사용 가능한 차트 필터와 함께 사용합니다.
4. 원하는 작업을 클릭합니다. [작업 요약] 페이지가 표시됩니다. 왼쪽 창에서 필요한 배치를 선택하고 오른쪽 창에서 Complete confirmation/Rollback이 필요한 원하는 디바이스를 선택합니다
5. More Options(추가 옵션) 아이콘을 선택하고 요건에 따라 Rollback(롤백) 또는 Complete(완료) 메뉴 작업을 클릭합니다.



롤백

참고: 디바이스는 다음 전제 조건을 충족하는 경우에만 선택할 수 있습니다.

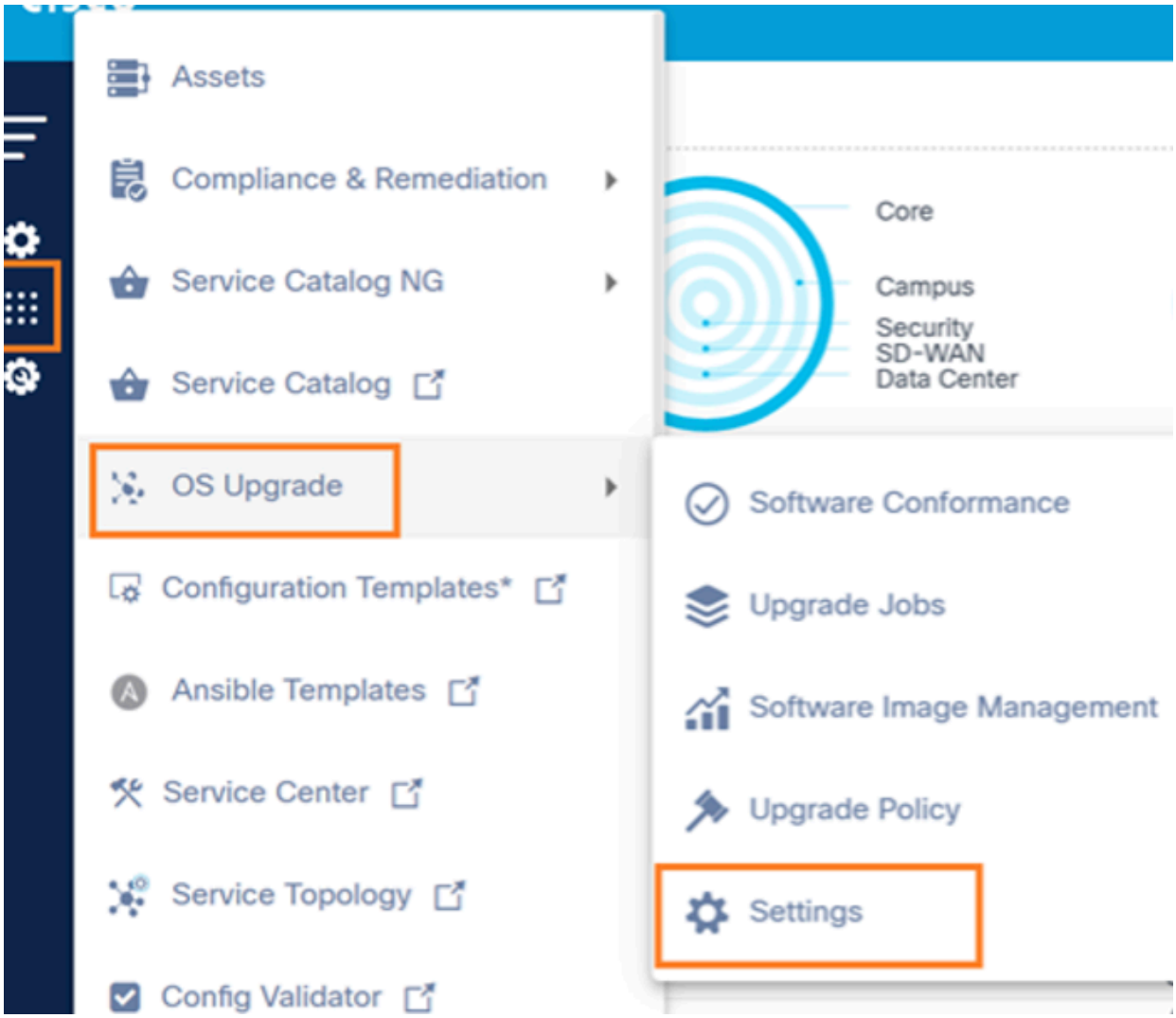
- 완료된 업그레이드된 작업의 롤백 옵션을 사용하도록 설정하려면 설정을 구성해야 합니다. 자세한 내용은 설정을 참조하십시오.
- 시간 내에 아무 조치도 취하지 않으면 디바이스가 자동으로 Complete(완료) 상태로 전환됩니다
- 이전에 롤백이 완료되었거나 롤백 이정표가 대기 중인 상태이면 온디맨드 롤백 작업에 디바이스를 사용할 수 있습니다

설정

OS 업그레이드 설정에서는 OS 업그레이드 응용 프로그램의 다른 구성 요소에 사용되는 공통 설정을 보관할 자리 표시자를 제공합니다.

설정 페이지에 액세스하려면 다음을 수행합니다.

1. 설정에 대한 액세스 권한을 관리하는 자격 증명을 사용하여 BPA에 로그인합니다.



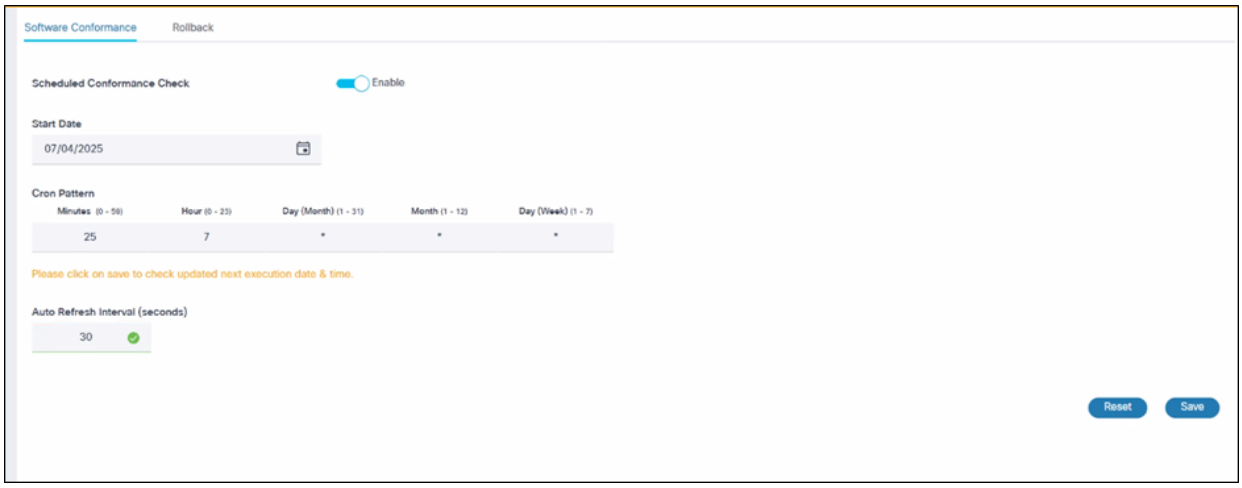
설정

2. OS Upgrade(OS 업그레이드) > Settings(설정)를 선택합니다. 설정 페이지가 열립니다.

Settings(설정) 페이지에는 다음 두 개의 탭이 있습니다.

- 소프트웨어 적합성: 이 탭에서 자동 적합성 실행 일정을 허용하는 구성을 업데이트할 수 있습니다
- 롤백: 전체 디바이스 업그레이드의 롤백을 허용하는 컨피그레이션은 이 탭에서 업데이트할 수 있습니다

소프트웨어 적합성



Software Conformance 탭

Software Conformance 탭은 다음을 제공합니다.

- 예약된 적합성 확인: 일정 사용 또는 사용 안 함
- 시작 날짜: MM/DD/YYYY를 선택합니다.

참고: 시작 날짜는 미래 날짜여야 합니다.

- Cron 패턴: 다음 세부 정보를 제공합니다.
  - 분(0-59)
  - 시간(0-23)
  - 일(월) (1-31)
  - 월(1-12)
  - 일(주)(1-7)
- 자동 새로 고침 간격 추가: 기본값은 30초입니다
- 저장: 변경 내용 저장

롤백

롤백 탭

롤백 탭은 다음을 제공합니다.

- 사용자 확인 토글: 사용자 확인 사용 또는 사용 안 함
    - 사용 상태: 업그레이드 작업의 디바이스는 구성 임계값 시간(시간)에 구성된 임계값 시간에 도달할 때까지 롤백하거나 업그레이드를 완료하기 위한 사용자 확인을 기다립니다. 도달 시 디바이스는 자동으로 완료됨 상태로 전환됩니다
    - 사용 안 함 상태: 업그레이드 작업의 디바이스는 사용자 확인을 기다리지 않고 자동으로 업그레이드를 완료합니다
- 확인 임계값 시간: 시간 단위로 대기할 임계값 시간 추가
- 저장: 변경 내용 저장

구축 컨피그레이션

- 적합성 정책 확인 및 SWIM 메타데이터의 기본 일정은 현지 시간으로 매일 오전 7시 25분에 구성됩니다.
- SWIM 이미지 메타데이터 동기화의 기본 일정을 변경하려면 BPA 설치 디렉토리 "<BPA install directory>/conf/@cisco-bpa-platform/mw-osupgrade-nxtgen/config.json"으로 이동하여 schedule.swimSchedule 등록 정보를 Cron 표현식으로 업데이트합니다. 구축 후 일정을 업데이트할 수 있습니다. 자세한 내용은 소프트웨어 적합성을 참조하십시오.
- 서로 다른 컨트롤러 유형에 대해 병렬 모드로 처리되는 최대 디바이스 수를 늘리거나 줄이려면 다음을 수행합니다.

1. 다음 파일을 업데이트합니다.
    - Cisco Catalyst Center 파일: "<BPA_INSTALL_DIRECTORY>/conf/@cisco-bpa-platform/mw-dnac-agent/config.json"
    - vManage 파일: "<BPA_INSTALL_DIRECTORY>/conf/@cisco-bpa-platform/mw-vmanage-agent/config.json"
    - NDFC 파일: "<BPA_INSTALL_DIRECTORY>/conf/@cisco-bpa-platform/mw-ndfc-agent/config.json"
    - FMC 파일: "<BPA_INSTALL_DIRECTORY>/conf/@cisco-bpa-platform/mw-fmc-agent/config.json"
2. 동시 활성화 또는 배포 제한을 늘리려면 Update throttling(조절 업데이트) > capabilities(기능) > image-activation, image-distribute(이미지 활성화, 이미지 배포)로 이동합니다.

참고: 이러한 제한을 업데이트하기 전에 지원되는 컨트롤러 및 디바이스 플랫폼을 참조하십시오.

액세스 제어

역할 기반 액세스 제어

BPA는 RBAC(Roles Based Access Control)를 지원합니다. RBAC 모델에서 역할은 사용자가 수행할 수 있는 권한 집합(즉, 작업)을 캡슐화합니다. 액세스 제어의 경우 관리자는 사용자 그룹에 대한 사용 권한이 있는 미리 정의된 역할 또는 새로 생성된 역할을 할당할 수 있습니다. 사용자는 하나 이상의 사용자 그룹에 속할 수 있으며 각 사용자 그룹은 해당 그룹의 사용자에게 특정 액세스 권한을 부여하는 하나 이상의 역할에 할당될 수 있습니다.

아래 표에는 OOB OS 업그레이드 역할 및 관련 권한이 요약되어 있습니다.

서비스	그룹	의도	슈퍼 관리자	활용 사례 관리자	읽기 전용 사용자(OS 업그레이드 사용 사례 읽기 전용 사용자)	운영자
OSU업그레이드 서비스	ui_app	업그레이드 작업 응용 프로그램 표시 또는 숨기기	예	예	예	예
OSU업그레이드 서비스	ui_app	소프트웨어 적합성 응용 프로그램 표시 또는 숨기기	예	예	예	예
OSU업그레이드 서비스	ui_app	SWIM 응용 프로그램 표시 또는 숨기기	예	예	예	예
OSU업그레이드 서비스	ui_app	소프트웨어 업그레이드 정책 응용 프로그램 표시 또는 숨기기	예	예	예	예
OSU업그레이드 서비스	ui_app	소프트웨어 업그레이드 설정 표시 또는 숨기기	예	예	예	예
OSU업그레이드 서비스	업그레이드 작업	업그레이드 작업 관리(예: 생성, 업데이트, 삭제 및 커밋)	예	예	아니요	예
OSU업그레이드 서비스	업그레이드 작업	업그레이드 작업 취소	예	예	아니요	예
OSU업그레이드 서비스	업그레이드 작업	작업의 온디맨드 보관	예	예	아니요	예
OSU업그레이드 서비스	업그레이드 작업	수동 승인	예	예	아니요	예

서비스	그룹	의도	슈퍼 관리자	활용 사례 관리자	읽기 전용 사용자(OS 업그레이드 사용 사례 읽기 전용 사용자)	운영자
OSU업그레이드 서비스	소프트웨어 적합성 정책	소프트웨어 적합성 정책 및 실행 결과 보기	예	예	예	예
OSU업그레이드 서비스	소프트웨어 적합성 정책	소프트웨어 적합성 정책 생성, 업데이트 및 삭제	예	예	아니요	아니요
OSU업그레이드 서비스	소프트웨어 적합성 정책	소프트웨어 적합성 정책의 온디맨드 실행	예	예	아니요	예
OSU업그레이드 서비스	업그레이드 정책	OS 업그레이드 정책 보기	예	예	예	예
OSU업그레이드 서비스	업그레이드 정책	OS 업그레이드 정책 관리	예	예	아니요	아니요
OSU업그레이드 서비스	스윔이미지 관리	소프트웨어 이미지 생성, 업데이트 및 삭제	예	예	아니요	예
OSU업그레이드 서비스	스윔이미지 관리	수영 보기	예	예	예	예
OSU업그레이드 서비스	스윔이미지 관리	소프트웨어 이미지 동기화	예	예	아니요	예
OSU업그레이드 서비스	소프트웨어 권장 사항	소프트웨어 권장 메타데이터 동기화	예	예	아니요	아니요
OSU업그레이드 서비스	소프트웨어 권장 사항	권고 사항 또는 통찰력 보기	예	예	예	예
OSU업그레이드 서비스	소프트웨어 권장 사항	적합성 정책 관리	예	예	아니요	아니요
OSU업그레이드 서비스	소프트웨어 적합성 설정	소프트웨어 적합성 설정 보기	예	예	예	예
OSU업그레이드 서비스	소프트웨어 적합성 설정	소프트웨어 적합성 설정 관리	예	예	아니요	아니요

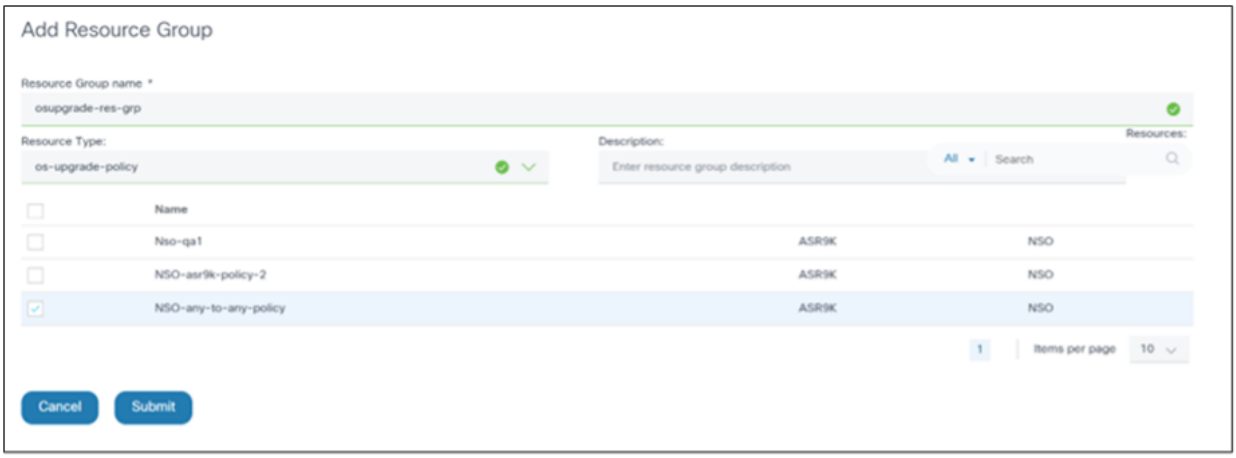
참고: 사용자 지정 역할 및 권한 매핑은 요구 사항에 따라 수행할 수 있습니다. 리소스 그룹을 참조하십시오.

리소스 그룹

이 기능은 BPA 리소스에 대한 세분화된 액세스 제어 기능(예: 업그레이드 정책)을 제공하여 권한이 없는 사용자가 OS 업그레이드 애플리케이션에 정의된 정책을 업데이트할 수 없도록 제한합니다. 관리자는 액세스 가능한 정책으로 리소스 그룹을 정의하여 액세스를 제한할 수 있습니다.

리소스 그룹을 생성하려면

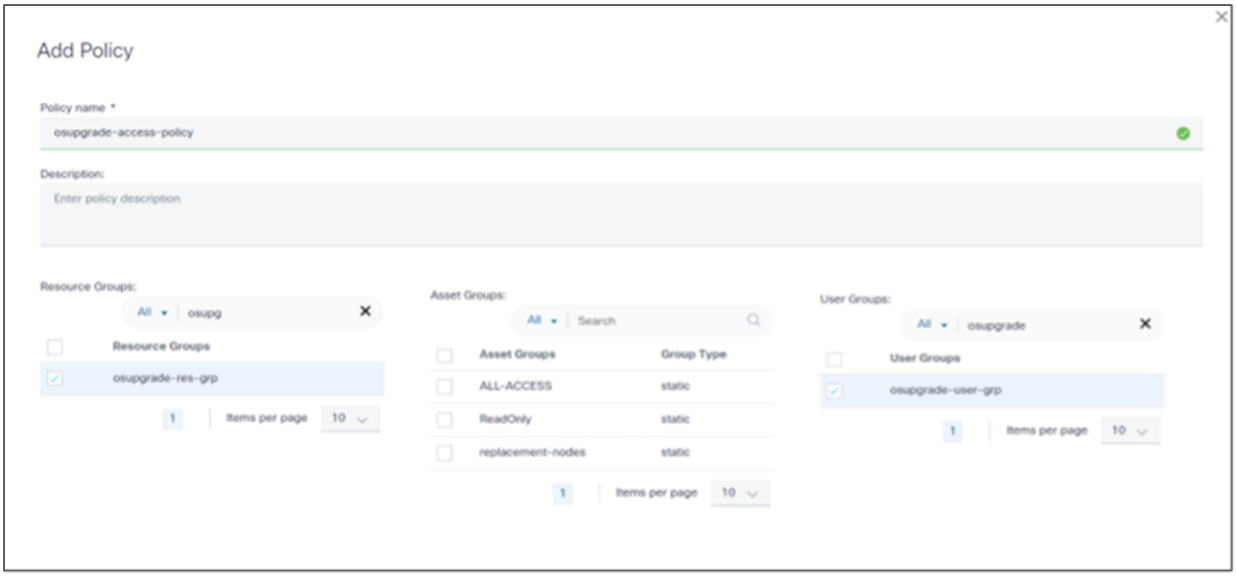
1. Settings(설정) > Resource Groups(리소스 그룹)로 이동합니다.



리소스 그룹 추가

2. 관리자가 아닌 사용자가 액세스할 수 있는 정책으로 리소스 그룹을 만듭니다.
3. 리소스 유형으로 os-upgrade-policy를 선택합니다. 해당 리소스가 표시됩니다.
4. 필요한 업그레이드 정책을 선택합니다.
5. Submit(제출)을 클릭합니다. 이 사용자 그룹에 속한 비관리자 사용자는 이제 선택한 리소스 그룹에서만 사용 가능한 정책에 액세스할 수 있습니다.

리소스 그룹을 사용자 그룹과 연결하려면 액세스 정책을 생성합니다.

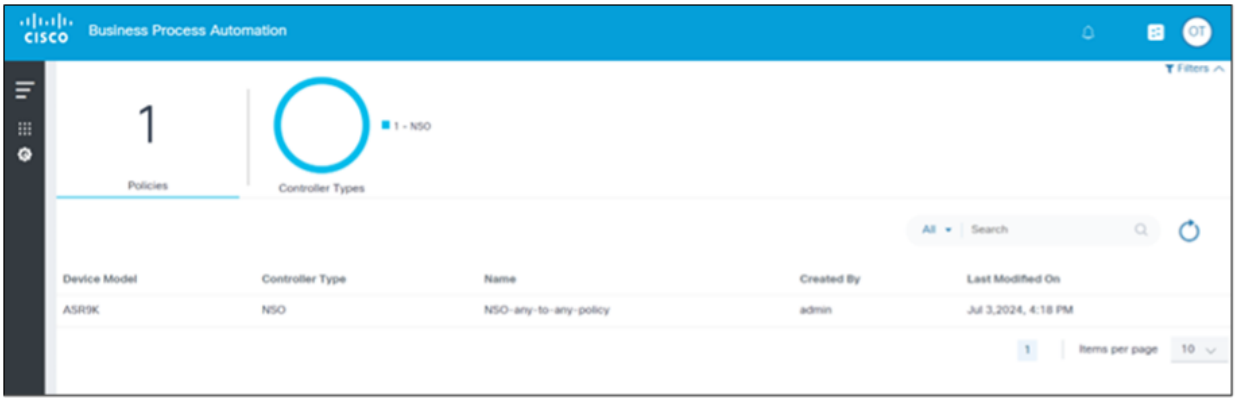


액세스 정책 추가

참고: 리소스 그룹이 생성되면 액세스 정책을 통해 사용자 그룹과 연결되어야 합니다. 다음에 대한 자세한 내용은 액세스 제어를 참조하십시오.

- 사용자
- 역할
- 사용자 그룹
- 액세스 정책
- 리소스 그룹
- 자산 그룹

다음은 관리자가 아닌 사용자가 제한된 리소스에 액세스할 수 있는 예입니다.



리소스 제한이 있는 비관리자 사용자

제로 트러스트 플래그 설정

사용자가 액세스할 수 있는 리소스는 제로 트러스트 플래그 설정에 따라 달라질 수 있습니다. 제로

트러스트 플래그는 true 또는 false로 설정할 수 있습니다. 다음 표에는 제로 트러스트 플래그 설정을 기반으로 하는 리소스 액세스 가능성이 요약되어 있습니다.

사용자	사용자 그룹	액세스 정책	리소스 그룹	리소스	제로 트러스트	활성화됨
사용자 1	UG1	AP1	RG1	리소스 2개	리소스 2개	리소스 2개
사용자 1	UG1	AP2	RG2	0개 리소스	0개 리소스	0개 리소스
사용자 1	UG1	AP3	없음		0개 리소스	모든 리소스
사용자 1	UG1	없음	없음		0개 리소스	모든 리소스

제로 트러스트 플래그를 활성화하거나 비활성화하려면

1. 다음 컨피그레이션 경로로 이동합니다.

```
cd /opt/bpa/bpa-helm-chart-

        /charts/cisco-bpa-platform-mw-auth/public_conf/config.json
```

2. zeroTrustPolicies 값을 수정합니다.
3. 다음 코어 번들로 이동합니다.

```
cd /opt/bpa/bpa-helm-chart-
```

4. 다음 명령을 실행하여 코어 키를 삭제합니다.

```
helm delete bpa-rel -n bpa-ns
```

5. 다음 명령을 실행하여 포드의 상태를 확인합니다

```
kubectl get pods -n bpa-ns
```

6. 모든 Pod가 종료된 후 다음 명령을 실행하여 코어 Helm을 설치합니다.

```
helm install bpa-rel --create-namespace --namespace bpa-ns
```

7. 다음 명령을 실행하여 나타나는 포드의 상태를 확인합니다.

```
kubectl get pods -n bpa-ns
```

OS 업그레이드 문제 해결

이 섹션에서는 BPA의 OS 업그레이드 애플리케이션에서 관찰된 문제와 관련된 트러블슈팅 팁을 제공합니다.

적합성 정책을 생성할 때 대상 장치 모델을 볼 수 없습니다.

해당 이미지 메타데이터를 SWIM 아래의 Software Images에서 사용할 수 있는지 확인합니다. 찾을 수 없는 경우 다음 옵션 중 하나를 수행합니다.

- 이미지를 동기화하여 Cisco Catalyst Center, NDFC, vManage 및 FMC와 같은 컨트롤러에서 이미지 메타데이터 검색
- NSO, CNC, Direct-to-Device, ANSIBLE 등의 컨트롤러에 필요한 이미지 메타데이터 생성

소프트웨어 적합성에 작동 안 함 상태 표시

이는 다음과 같은 이유 때문일 수 있습니다.

- 소프트웨어 적합성 정책을 생성할 때 선택한 모델의 에셋을 찾을 수 없습니다.
- SWIM의 모델 이름이 모든 디바이스의 디바이스 인벤토리에 있는 적합성 디바이스 모델과 일치하지 않습니다
- SMU가 소프트웨어 적합성 생성의 일부로 선택되었고 모든 디바이스에 대해 SMU 검색이 실

패한 경우
- 규정 준수 검사 템플릿 실행을 위해 선택한 프로세스 템플릿을 찾을 수 없거나 실패했습니다.
- 소프트웨어 적합성을 생성할 때 선택한 모델의 모든 디바이스에서 일련 번호 또는 현재 버전을 사용할 수 없습니다

특정 디바이스의 소프트웨어 적합성 결과 상태를 알 수 없음

이는 다음과 같은 이유 때문일 수 있습니다.

- SWIM의 모델 이름이 디바이스 인벤토리의 적합성 디바이스 모델과 일치하지 않습니다
- SMU가 소프트웨어 적합성 생성의 일부로 선택되었고 디바이스에 대한 SMU 검색이 실패한 경우
- 규정 준수 검사 템플릿 실행을 위해 선택한 프로세스 템플릿을 찾을 수 없거나 실패했습니다.
- 일련 번호 또는 현재 버전을 디바이스에서 사용할 수 없습니다.

업그레이드 작업 완료 진행률

업그레이드가 완료되었지만 업그레이드 작업 완료 진행률이 100 미만인 경우 OS Upgrade > Settings > Rollback(OS 업그레이드) 아래에서 Wait for Rollback(롤백 대기 설정)이 활성화되어 있고 User Verification(사용자 확인) 토글이 설정되었는지 확인합니다. 전체 완료율이 100 미만이면 롤백 또는 완료를 선택합니다.

작업 일정 도달, 디바이스가 대기 중 상태로 고정됨

예약된 작업이 시작된 후 디바이스가 대기 중 상태로 유지되면 Kafka, Camunda, Scheduler, OS Upgrade 마이크로 서비스를 다시 시작해 보십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.