BPA 사용 설명서 컨피그레이션 컴플라이언스 및 리미디에이션 v5.1

소개

CnR(Configuration Compliance and Remediation) 애플리케이션은 네트워크 운영자가 컨피그레이션 블록으로 구성된 사용자 정의 정책에 대해 디바이스 컨피그레이션 컴플라이언스 검사를 수행하도록 지원합니다. 운영자는 선택한 디바이스 컨피그레이션에서 시스템을 사용하여 컨피그레이션 블록을 수동으로 작성하거나 자동으로 생성합니다. 사용자는 RefD 애플리케이션에서 얻은 값에서 잠재적으로 파생되는 규칙 조건을 사용하여 이러한 블록에 적용되는 규칙을 설정할 수도 있습니다. 운영자는 일정에 따라 편리하게 컴플라이언스 점검을 실행하거나 점검을 즉시 시작할 수 있다.

이 애플리케이션은 직관적인 대시보드를 자랑하며, 컴플라이언스 위반에 대한 포괄적인 개요를 제공하고, 디바이스 및 컨피그레이션 블록 레벨에서 요약과 세부 보기를 모두 제공합니다.

이 애플리케이션에는 규정 준수 위반을 처리할 수 있는 강력한 교정 프레임워크가 포함되어 있습니다. 이 프레임워크는 GCT(Golden Configuration Templates)라고 하는 컨피그레이션 템플릿 및 프로세스 템플릿과 같은 워크플로와 템플릿을 활용하여 교정 프로세스를 간소화합니다. 규정 준수 확인과 마찬가지로, 교정 작업은 일정에 따라 실행되도록 프로그래밍하거나 즉시 트리거하여 위반을 신속하게 해결할 수 있습니다.

Next-Generation(Next-Gen) 포털의 Compliance and Remediation 대시보드에는 네트워크 보안 관리를 개선하고, 규정 준수 절차를 간소화하며, 교정 활동을 간소화하도록 설계된 기능이 있습니다. 대시보드는 자산 및 정책 준수에 대한 종합적인 요약을 제공하므로 네트워크 운영자가 네트워크 상태를 쉽게 평가하고 디바이스가 엄격한 보안 프로토콜을 준수하도록 할 수 있습니다.

구성 블록은 자동으로 생성된 다음 수동으로 편집하거나 추가할 수 있으므로 자동화와 사용자 지정 간의 균형을 유지할 수 있습니다. 기존 및 최신 인터페이스의 세부적인 사용자, 그룹 및 권한 설정을 포함하여 구성 블록 및 세분화된 액세스 제어 메커니즘을 정확하게 식별하는 시스템은 네트워크 구성이 신뢰할 수 있는 담당자의 손에 안전하게 유지되도록 합니다. 이러한 기능은 높은 네트워크 규정 준수 및 보안 표준을 유지하려는 조직에 강력한 툴셋을 제공합니다.

새로운 기능

다음과 같은 주요 기능이 도입되었습니다.

- 컴플라이언스 보고서를 생성, 확인 및 다운로드하는 포괄적인 보고 대시보드
- Asset Manager를 사용하여 디바이스를 온보딩하지 않고 디바이스 컨피그레이션을 업로드하여 오프라인 규정 준수 감사를 수행할 수 있습니다.
- 민감한 디바이스 컨피그레이션 데이터를 마스킹하기 위해 블록 컨피그레이션에서 패턴을 구성하는 기능
- 정책 및 자산 규정 준수 요약 그리드 데이터를 CSV 파일로 내보낼 수 있음
- 생성된 교정 컨피그레이션을 보고 디바이스 실행 컨피그레이션과 비교

- 컨피그레이션이 있는 경우 위반 증가를 지원하기 위한 블록 개선 사항
- 정책 생성 및 편집 페이지에서 연결된 사용자 경험을 활성화하여 블록 생성 페이지와 같은 하위 구성 요소로 교차 실행
- 규정 준수 작업의 개선 사항: 정책 수정 페이지로 교차 실행할 페이지를 만들고 편집합니다.

구성 요소

컴플라이언스 및 리미디에이션은 다음 컨트롤러 및 디바이스 유형을 지원합니다.

컨트롤러	OS 유형
NSO(6.5)	IOS XE, IOS XR, NX-OS, JunOS, Nokia SR-OS
CNC(6.0)	IOS XE, IOS XR, NX-OS
NDFC(3.2.0/패브릭 v12.2.2)	NX-OS
Cisco Catalyst Center(2.3.5)	IOS XE, IOS XR. 검증된 컴플라이언스 전용
FMC(7.2.5)	FX-OS(FTD). 검증된 컴플라이언스 전용
D2D(Direct To Device)	IOS XE, IOS XR, JunOS

참고: NSO 컨트롤러를 통한 Nokia SR-OS 지원은 컨피그레이션 컴플라이언스 기능에만 적용됩니다. Nokia 디바이스에는 교정이 지원되지 않습니다.

참고: 컴플라이언스 기능은 Cisco CLI(Command Line Interface) 형식 및 Juniper 및 Nokia 디바이스의 YAML 유사 형식으로 디바이스 컨피그레이션과 함께 작동합니다. 현재 프레임워크는 Netconf, JSON, XML 등과 같은 다른 형식을 지원하지 않습니다.

v5.0 릴리스의 일부로 CnR(Compliance and Remediation) 클래식 애플리케이션은 더 이상 사용되지 않습니다. 이제 모든 CnR 기능이 완전히 통합되어 차세대 포털에서 사용할 수 있습니다.

가정 및 전제 조건

CnR 활용 사례를 효과적으로 사용하려면 다음 전제 조건이 필요합니다.

- CnR 활용 사례에 대한 구독 자격 키를 업로드해야 합니다.
- 관련 컨트롤러 및 디바이스를 온보딩하여 BPA Asset Manager의 일부로 사용할 수 있어야 합니다. 자세한 내용은 BPA 사용 설명서의 Asset Manager 섹션을 참조하십시오.

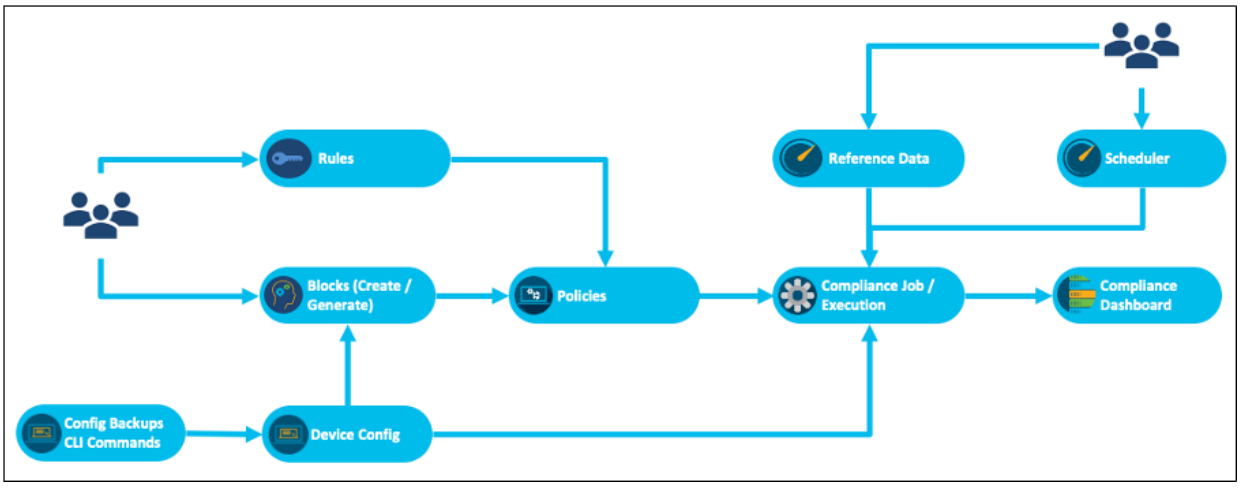
- 온보딩된 자산은 고객 요구 사항에 따라 Next-Gen 포털의 자산 그룹으로 그룹화해야 합니다.

규정 준수 대시보드

규정 준수 대시보드에서는 선택한 시간 동안 모든 디바이스의 위반을 요약하여 볼 수 있습니다. 현재 월의 데이터가 기본적으로 표시됩니다. 사용자는 규정 준수 위반에 대한 기록 데이터를 보기 위해 시간 창을 변경할 수 있습니다. 현재 월이 기본적으로 선택된 보기입니다.

참고: 클래식 UI에서 더 이상 사용되지 않는 규정 준수 대시보드가 제거되어 더 이상 사용할 수 없습니다. Next-Gen 포털에서 사용 가능한 대시보드를 사용해야 합니다.

구성 규정 준수 흐름도



구성 규정 준수 구성 요소 개요

자산 목록에 대한 정책에 대해 규정준수 작업이 실행되면 대시보드에 표시되는 규정준수 위반이 채워집니다. 필요한 규정준수 규칙과 함께 블록 컨피그레이션 목록을 추가하여 규정준수 정책을 생성합니다. 규정 준수 규칙은 RefD 애플리케이션에서 데이터를 가져오는 고정 값 또는 동적 변수를 확인할 수 있습니다. 규정 준수 작업은 온디맨드 방식으로 실행하거나 일회성 또는 반복 일정으로 실행할 수 있습니다.

컨피그레이션 컴플라이언스에는 다음과 같은 중요한 기능이 포함됩니다.

- 생성 차단: 블록은 수동으로 생성되거나 TTP(Template Text Parser) 템플릿을 사용하여 자동으로 생성됩니다. 정적 또는 동적(변수 포함)일 수 있습니다.
- 규칙 생성: 규칙은 블록의 변수를 검증합니다. 규칙 값은 정적으로 설정되거나 실행 시간 동안 RefD(Reference Data) 시스템에서 동적으로 검색될 수 있습니다.
- 정책 생성: 블록 목록과 해당 규칙을 선택하여 정책이 생성됩니다. 규칙의 데이터는 런타임에 RefD 프레임워크에서 동적으로 가져오는 고정 데이터일 수 있습니다.

- 규정 준수 작업 생성: 규정 준수 작업은 규정 준수 검사를 실행할 정책 및 자산 그룹(자산 목록 포함)을 선택하여 생성합니다. 사용자는 백업 프레임워크에서 디바이스 컨피그레이션을 검색하거나 실행 중에 디바이스에서 프로세스 템플릿을 통해 라이브 명령을 실행하도록 선택할 수 있습니다. 백업에서 컨피그레이션을 가져오면 라이브 디바이스에 연결할 필요 없이 디바이스를 오프라인으로 감사하는 데 도움이 됩니다. 작업을 예약하거나 온디맨드 방식으로 실행할 수 있습니다.
- 규정 준수 위반: 대시보드에서 규정준수 위반을 봅니다.

자산 규정 준수 요약

Asset Compliance Summary 탭은 네트워크 내의 모든 디바이스에서 규정준수 위반에 대한 포괄적인 개요를 제공하도록 설계된 필수 기능입니다. 이 탭에서는 사용자가 규정 준수 문제를 신속하게 파악하여 모든 장치가 설정된 정책 및 표준을 준수하도록 할 수 있습니다. 이 인터페이스에는 강력한 필터링 및 검색 기능이 포함되어 있으므로 컴플라이언스 데이터를 쉽게 탐색하고 분석할 수 있습니다.

주요 기능

- 디바이스별 위반 요약: 이 탭에는 각 디바이스의 컴플라이언스 위반에 대한 요약 보기가 표시되며, 사용자는 심각도 레벨(예: critical, high, medium, low)별로 범주화된 전반적인 컴플라이언스 상태를 빠르게 확인할 수 있습니다.
- 자세한 위반 정보: 각 디바이스에 대해 팝업 창은 위반된 정책에 대한 세부 정보를 제공하며 사용자는 위반을 일으킨 블록 및 컨피그레이션 라인으로 더 드릴다운할 수 있습니다.

자산 준수 요약 보기

- 고급 필터링 옵션: 탭 상단과 왼쪽에 있는 필터를 사용하면 그리드에 표시되는 데이터의 범위를 좁힐 수 있습니다. 사용자는 날짜 범위, 자산 그룹, 제품군 등을 기준으로 필터링하여 규정 준수 데이터를 중점적으로 분석할 수 있습니다.
- 검색 기능: 검색 필드를 사용하여 그리드의 데이터를 더 세분화할 수 있습니다. 사용자는 관련 키워드 또는 구를 입력하여 특정 디바이스를 빠르게 찾거나 컨트롤러로 관리할 수 있습니다.

- 사용자 지정 가능한 날짜 범위: 기본적으로 날짜 범위 필터에서 현재 월이 선택되어 최신 규정 준수 데이터를 제공합니다. 그러나 사용자는 날짜 범위를 사용자 지정하여 데이터를 볼 수 있습니다.
- 필터: 제품군, 자산 그룹, 감사 유형 등의 여러 필터를 사용할 수 있습니다. 필터를 적용하여 그리드를 새로 고칩니다.

자산 규정 준수 요약

- CSV로 내보내기: 사용자가 오프라인 분석, 보고 및 보관을 위해 자산 구성 규정 준수의 로컬 사본을 얻을 수 있도록 지원하는 기능입니다. 데이터를 CSV 파일로 내보내려면 More Options(추가 옵션) 아이콘에서 Export as CSV(CSV로 내보내기)를 선택합니다. 다운로드한 CSV 파일에는 적용된 모든 필터를 기준으로 현재 그리드에 표시된 데이터가 포함되어 있습니다.

자산 규정 준수 요약: CSV로 내보내기

자산 규정 준수를 위한 CSV 파일 세부사항

CSV 파일에는 디바이스 이름, 컨트롤러 인스턴스(관리자), 디바이스의 제품군, 디바이스 규정 준수 상태, 심각도별 위반 수(예: Critical, Major, Minor, Warning, Info, Unknown), 디바이스에 대한 규정 준수가 마지막으로 확인된 날짜 등 자산 규정 준수 요약 표에 표시되는 모든 열이 포함됩니다.

그리드에 페이지 매김 기능이 있는 경우 내보내기에는 보이는 페이지뿐 아니라 여러 페이지에 있는 모든 레코드도 포함됩니다.

자산 규정 준수를 위해 CSV 파일 열기 및 사용

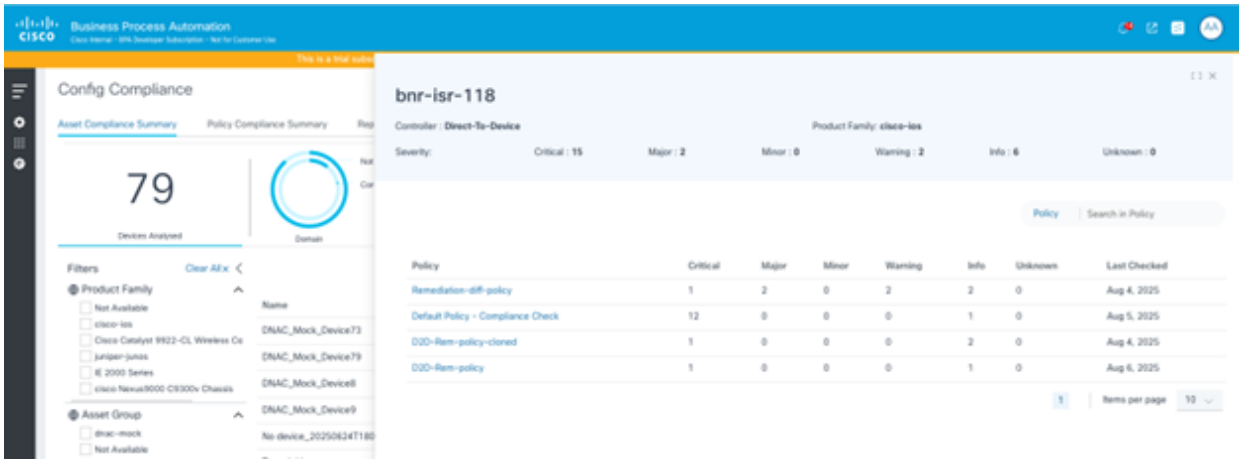
1. 다운로드한 CSV 파일을 Excel 또는 호환 가능한 스프레드시트 애플리케이션에서 엽니다.
2. 필터링된 결과를 포함하여 Asset Compliance Summary 표에 표시되는 내용과 일치해야 합니다.

	A	B	C	D	E	F	G	H	I	J	K
1	Device Name	Managed By	Product Family	Compliance	Critical	Major	Minor	Warning	Info	Unknown	Last Checked
2	CNC-bnr-asr-78	Direct-To-Device	IE 2000 Series	Non Compliant	1	0	0	0	0	0	04-Aug-25
3	D2d-118	Direct-To-Device	IE 2000 Series	Partially Compliant	0	1	0	1	1	0	04-Aug-25
4	D2d-juniper	Direct-To-Device	juniper-junos	Partially Compliant	0	0	0	2	2	1	06-Aug-25
5	DNAC_Mock_Device0	DNAC-Mock	Cisco Catalyst 9922-CL Wireless Controller for Cloud	Unknown	0	0	0	0	0	1	05-Aug-25
6	bnr-asr-78	cnc6		Partially Compliant	0	0	1	0	0	0	05-Aug-25
7	bnr-isr-118	Direct-To-Device	cisco-ios	Partially Compliant	15	2	0	2	6	0	06-Aug-25
8	bnr-n3k-44	NSO-166	cisco Nexus9000 C9300v Chassis	Partially Compliant	12	0	0	0	3	0	05-Aug-25
9											

자산 규정 준수 요약: Excel 애플리케이션에서 열린 CSV 파일

정책별 자산 준수 요약 보기

Asset Compliance Summary(자산 준수 요약) 그리드에서 행을 클릭하면 디바이스가 검증된 다른 정책에 따라 분류된 자산 위반의 세부 정보가 표시됩니다. 이는 사용자가 각 정책의 심각도를 기준으로 위반 수를 볼 수 있는 세부 보기 역할을 합니다.



자산 규정 준수 요약: 정책별 규정 준수 요약

참고: 다음 사항을 유의해야 합니다.

- Policy 열의 하이퍼링크는 Policy details 페이지로 연결됩니다.
- 행을 클릭하면 선택한 정책에 대한 Violation details(위반 세부사항) 페이지가 표시됩니다

위반 세부 정보 보기

Violation Details(위반 세부 정보) 페이지에는 디바이스 컨피그레이션에서 겹치는 블록 및 규칙 레벨 위반이 표시됩니다. 또한 사용자는 차단 컨피그레이션 및 권장 교정 컨피그레이션도 볼 수 있습니다.

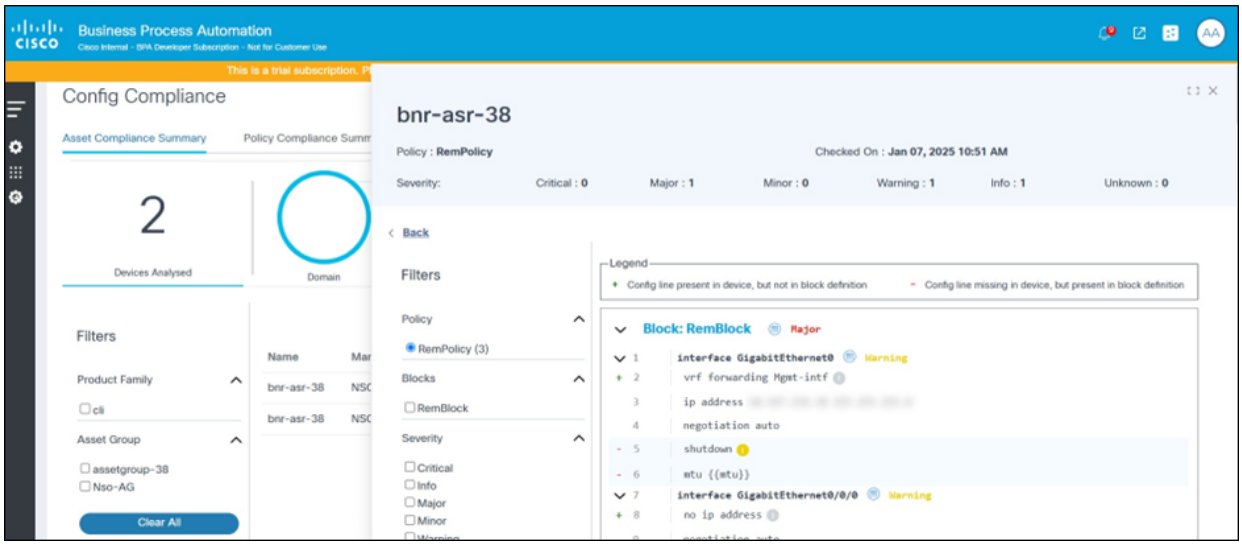
정책 레벨 분할과 함께 Asset Compliance Summary 페이지에서 Violation Details 페이지를 보려면 다음을 수행합니다.

1. Asset Compliance 그리드에서 행을 선택합니다. 팝업이 표시됩니다. 그리드에는 규정준수 세부사항이 정책별로 나뉘어 표시됩니다.
2. 그리드에서 행을 선택합니다. Violation Details(위반 세부사항) 페이지가 표시됩니다.

Policy Compliance Summary(정책 준수 요약) 그리드에서 Violations Details(위반 세부 정보) 페이지를 보려면

1. Policy Compliance Grid를 선택합니다.
2. 행 > 영향 받는 자산 그리드를 선택합니다.
3. 행을 선택합니다. 위반 세부 정보 페이지가 표시됩니다.

Violations Details(위반 세부사항) 페이지의 오른쪽에는 디바이스 컨피그레이션 블록이 표시되며 그 위에 위반이 오버레이됩니다. 해당 구성 라인에 대한 위반이 나열됩니다. 조건 실패의 경우 위반 리본은 규칙 이름, 조건 및 예상 컨피그레이션(규칙에 정의된 대로)과 디바이스 컨피그레이션에서 검색된 컨피그레이션의 세부 정보를 제공합니다.



자산 준수 위반

블록 기호

- 라인에 "+" 기호는 블록 컨피그레이션에 따라 컨피그레이션이 예상되지 않지만 디바이스 컨피그레이션에 추가로 존재함을 의미합니다.
- 라인에 "-" 기호는 컨피그레이션이 블록 컨피그레이션에 따라 예상되지만 디바이스 컨피그레이션에는 없음을 의미합니다.

필터

페이지 왼쪽의 필터 섹션에서는 다음 작업을 수행할 수 있습니다.

- 정책을 변경합니다. 이렇게 하면 페이지가 새로 고쳐지고 새로 선택한 정책에 대한 위반이 로드됩니다
- Blocks(블록) 확인란을 선택하여 선택한 블록과 관련된 위반을 봅니다
- 지정된 심각도 레벨의 위반을 보려면 Severity 확인란을 선택합니다
- 선택한 유형의 위반을 보려면 Violation Type 확인란을 선택합니다.
  - 순서 불일치: 장치 구성 라인의 순서가 블록 구성에 정의된 순서와 일치하지 않습니다
  - 누락된 구성: 블록 컨피그레이션에 따라 예상되지만 디바이스 컨피그레이션에는 없는 컨피그레이션 라인을 봅니다.
  - 추가 구성: 블록 컨피그레이션에 따라 예상되지는 않지만 디바이스 컨피그레이션에 추가로 표시되는 컨피그레이션 라인을 봅니다.
  - 규칙 실패: 규칙에서 하나 이상의 조건 실패.
  - 누락된 블록: 전체 디바이스 컨피그레이션 블록이 없거나 정의된 블록 컨피그레이션과 일치하지 않습니다.
  - 건너뛴 블록: 블록 필터 조건이 충족되지 않으므로 이 구성 블록을 건너뜁니다.

리미디에이션 컨피그레이션 보기 및 비교

Remediation Config 페이지에는 지정된 정책의 각 블록에 대해 선택한 디바이스에 대해 생성된 컨피그레이션이 표시됩니다. 컨피그레이션이 생성되고 정책에 있는 블록 및 규칙 세부사항과 컴플라이언스 실행 중에 검색된 디바이스 컨피그레이션을 고려합니다. 사용자는 동일한 페이지에서 컨피그레이션을 업데이트할 수 있습니다. 이렇게 생성된 컨피그레이션은 리미디에이션 작업 기능을 사용하여 디바이스에 푸시할 수 있습니다. 또한 이 페이지에서는 사용자가 생성된 컨피그레이션을 현재 실행 중인 컨피그레이션과 비교할 수 있는 옵션을 제공합니다. 사용자는 현재 디바이스 컨피그레이션을 검색하기 위해 하나 이상의 명령을 지정할 수 있습니다.

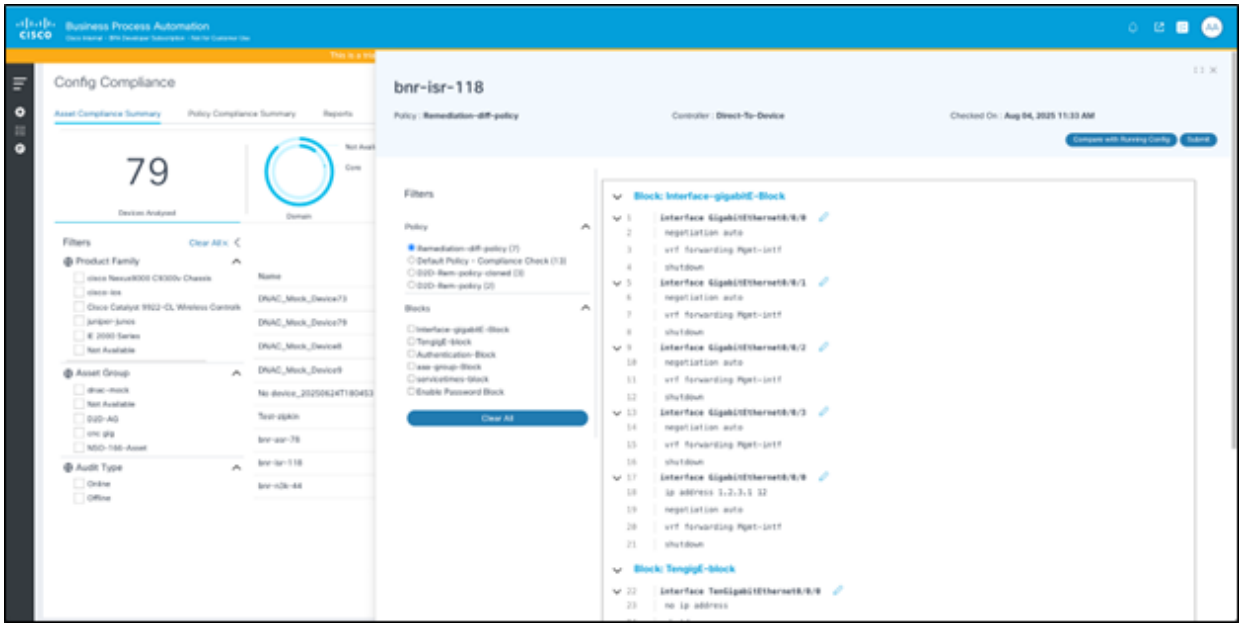
Asset Compliance 그리드에서 Remediation Config 페이지를 보려면 다음을 수행합니다.

1. Asset Compliance Summary(자산 준수 요약) 탭을 클릭합니다.

2. Action(작업) 열의 asset compliance grid(자산 규정 준수 그리드)에서 More Options(추가 옵션) 아이콘 > View Remediation Config(교정 컨피그레이션 보기)를 선택합니다. Remediation Config 페이지가 표시됩니다.

Policy Compliance 그리드에서 Remediation Config 페이지를 보려면

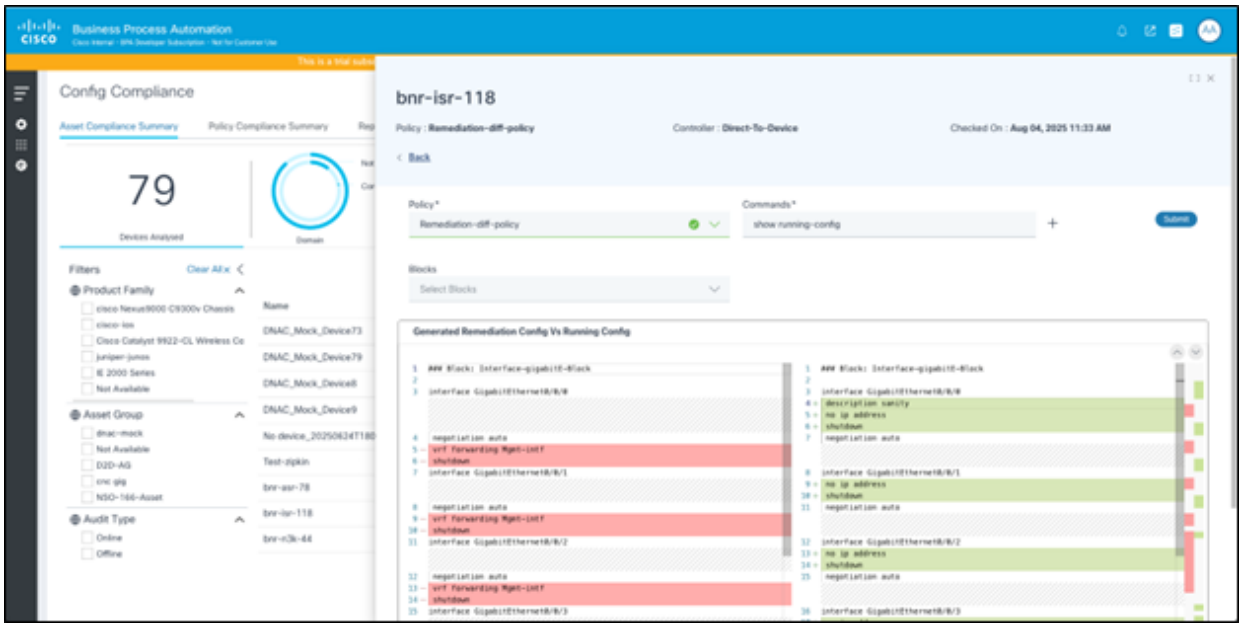
1. Policy Compliance Summary(정책 준수 요약) 탭을 클릭합니다.
2. 정책 규정준수 그리드에서 원하는 행을 선택합니다. 영향을 받는 자산 그리드가 표시됩니다.
3. Action(작업) 열에서 More Options(추가 옵션) 아이콘 > Select View Remediation Config(교정 컨피그레이션 보기)를 선택합니다. Remediation Config 페이지가 표시됩니다.



리미디에이션 구성 페이지

Remediation Config 페이지는 다음을 표시합니다.

- 생성된 리미디에이션 컨피그레이션: 생성된 컨피그레이션이 페이지의 오른쪽에 표시되며, 사용자가 컨피그레이션 블록을 수정하고 저장할 변경 사항을 제출할 수 있는 옵션도 함께 제공됩니다
- 필터: 필터는 정책을 선택한 다음 선택적으로 하나 이상의 블록을 선택하여 해당 생성된 컨피그레이션을 확인하는 데 사용할 수 있습니다
- 실행 중인 구성과 비교: Compare with Running Config를 클릭하여 사용자가 생성된 컨피그레이션을 디바이스 실행 컨피그레이션과 비교할 수 있는 자세한 페이지를 표시합니다



실행 중인 구성과 비교 페이지

실행 중인 구성과 비교 페이지는 다음을 표시합니다.

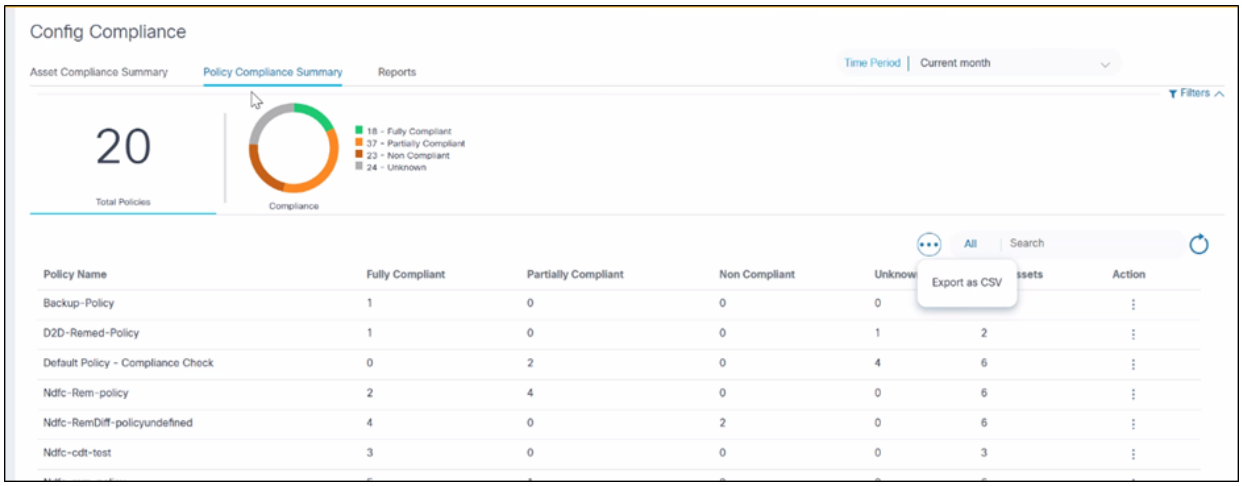
- 정책을 선택하는 옵션: 이전 페이지에서 선택한 정책이 미리 선택되어 있습니다.
- 디바이스에서 실행할 하나 이상의 명령을 입력할 수 있는 텍스트 상자
- 디바이스에서 명령을 실행하고 컨피그레이션을 검색하는 Submit(제출) 버튼
- 블록을 보고 필터링하는 옵션: 기본적으로 정책 내의 모든 블록이 표시됩니다. 사용자는 필요에 따라 개별 블록을 선택할 수 있습니다
- 생성된 컨피그레이션 및 디바이스 컨피그레이션을 나란히 표시하고 차이점을 강조 표시하는 컨피그레이션 차이 뷰어

정책 준수 요약

Policy Compliance Summary 탭은 정의된 정책에 대한 디바이스의 컴플라이언스 상태를 명확하고 간결하게 보여줍니다. 이 탭은 사용자가 규정 준수 환경을 신속하게 평가하고 관심 영역을 파악하는 데 도움이 됩니다. 이 탭에서는 컴플라이언스 상태를 기준으로 디바이스를 분류하므로 간단하게 이해하고 관리할 수 있습니다.

규정 준수 상태:

- 완전 호환: 모든 디바이스는 해당 정책에 대한 모든 규정 준수 규칙을 충족합니다.
- 부분적으로 호환: 일부 디바이스는 규칙을 준수하지만 다른 디바이스는 준수하지 않습니다.
- 규정 미준수: 어떤 디바이스도 정책을 준수하지 않습니다.
- 알 수 없음: 네트워크 연결에 문제가 있거나 백업을 사용할 수 없기 때문에 정책의 적합성을 확인할 수 없습니다.



CSV 내보내기를 통한 정책 준수 요약

정책 규정 준수를 위해 CSV로 내보내기

CSV로 내보내기 기능을 사용하면 오프라인 분석, 보고 및 보관을 위해 정책 규정준수의 로컬 사본을 얻을 수 있습니다. 데이터를 CSV 파일로 내보내려면 More Options(추가 옵션) 아이콘에서 Export as CSV(CSV로 내보내기)를 선택합니다. 다운로드한 CSV 파일에는 적용된 모든 필터를 기준으로 현재 그리드에 표시된 데이터가 포함되어 있습니다.

정책 규정 준수를 위한 CSV 파일 세부 정보

CSV 파일에는 정책 이름, 검증된 총 자산 수 및 규정 준수 상태(예: Fully Compliant, Partially Compliant, Non-Compliant 및 Unknown)별 수 분석이 포함됩니다. 그리드에 페이지 매김 기능이 있는 경우 내보내기에는 현재 페이지에 표시된 레코드뿐만 아니라 모든 페이지의 모든 레코드도 포함됩니다.

정책 준수를 위해 CSV 파일 열기 및 사용

1. 다운로드한 CSV 파일을 Excel 또는 호환 가능한 스프레드시트 애플리케이션에서 엽니다.
2. 콘텐츠가 정책 준수 요약 표(필터링된 결과 포함)에 표시된 것과 일치하는지 확인합니다.

	A	B	C	D	E	F
1	Policy Name	Fully Compliant	Partially Compliant	Non Compliant	Unknown	Total Assets
2	D2D-Juniper-policy	0	1	0	0	1
3	D2D-Raiseviolation-policy	0	1	0	0	1
4	D2D-Rem-policy	0	1	0	2	3
5	D2D-Rem-policy-cloned	0	1	0	0	1
6	Default Policy - Compliance Check	0	2	0	70	72
7	Policy Delete Issue	1	0	0	0	1
8	Policy Test	1	0	0	0	1
9	Remediation-diff-policy	0	1	0	0	1
10	cnc gig policy	0	1	0	0	1
11	cnc gigabit	0	2	1	1	4
12						

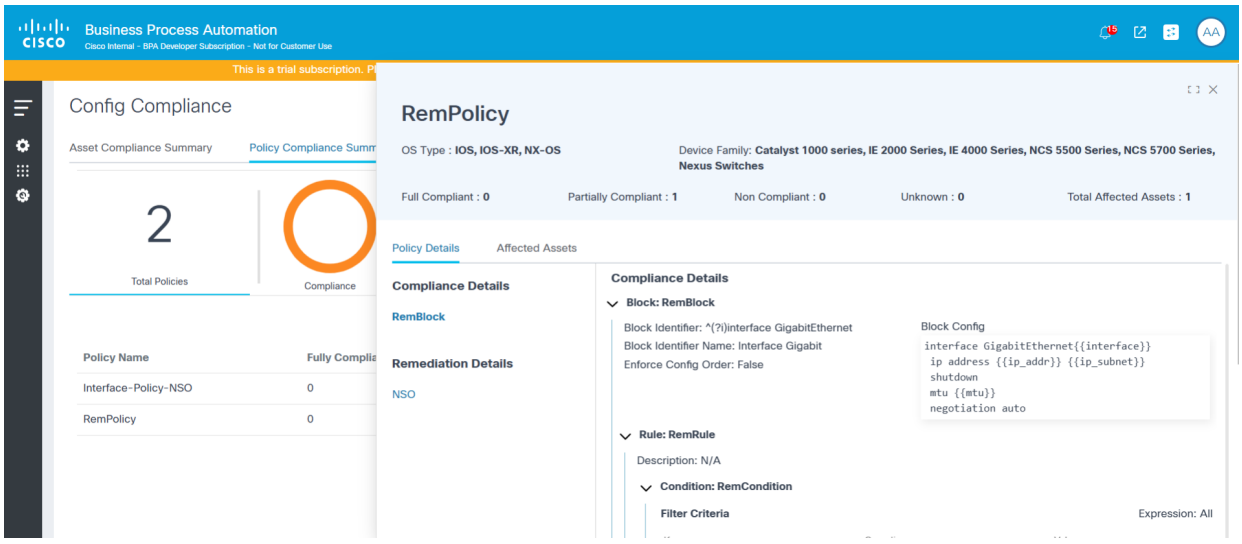
정책 준수: 정책 세부 정보

정책 세부 정보 보기

정책 세부 정보를 보려면

1. Action(작업) 열 아래의 More Options(추가 옵션) 아이콘에서 정책을 선택합니다.
2. View Policy Details를 선택합니다. Policy Details(정책 세부사항) 페이지가 표시됩니다.

참고: [정책 세부 정보] 페이지는 블록, 규칙 및 조건을 포함한 모든 정책 정보의 읽기 전용 보기입니다.사용자는 페이지 내에서 관련 블록으로 직접 이동하는 하이퍼링크를 누를 수 있습니다.



정책 준수: 정책 세부 정보

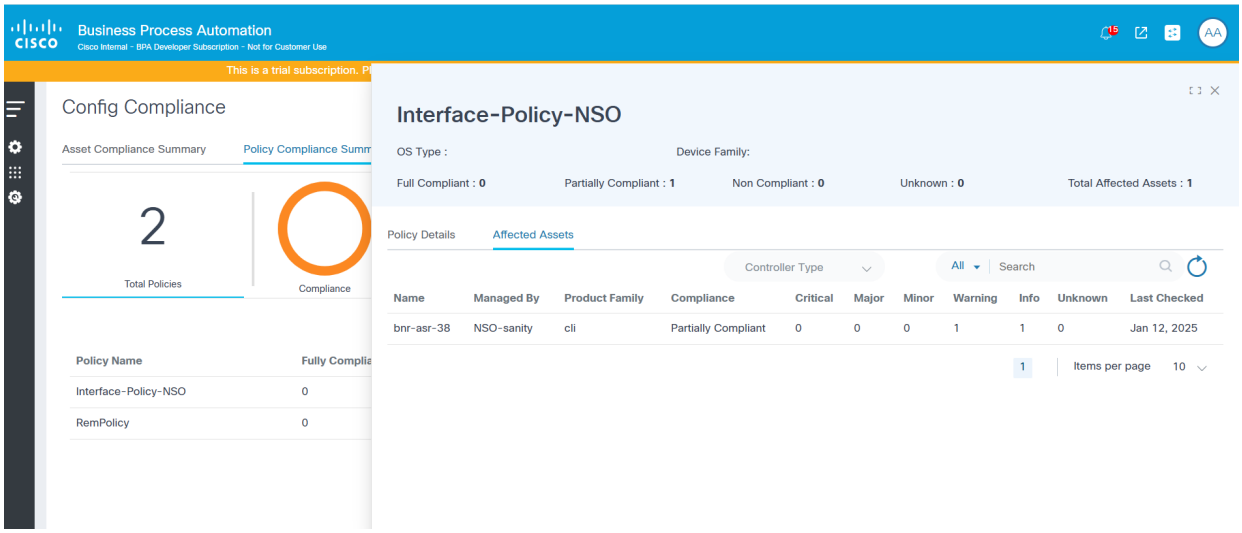
영향받는 자산 보기

Affected Assets(영향받는 자산) 탭에는 각 정책에서 분석된 자산 목록과 심각도로 구분된 위반 수

가 표시됩니다. Controller Type 드롭다운 목록 및 검색 상자를 사용하여 디바이스를 필터링할 수 있습니다.

Policy Compliance Summary(정책 준수 요약) 탭에서 영향받는 자산을 보려면

1. 행을 선택합니다. Compliance Policy 창이 열립니다.
2. Affected Assets(영향 받는 자산) 탭을 클릭합니다.



정책 준수: 영향을 받는 자산

참고: Affected Assets(영향받는 자산) 탭에서는 View Violation Details(위반 세부사항 보기) 페이지와 View Remediation Config(교정 컨피그레이션 보기) 페이지를 열 수 있는 작업을 제공합니다. 자세한 내용은 Asset Compliance Summary를 참조하십시오.

보고서

보고서 섹션에서는 디바이스 규정 준수에 대한 포괄적인 정보를 제공하고, 위반을 식별하며, 문제 해결 작업을 용이하게 합니다. 이 애플리케이션은 다양한 유형의 규정 준수 보고서를 생성, 보기, 다운로드 및 관리하기 위한 사용자 친화적인 인터페이스를 제공합니다.

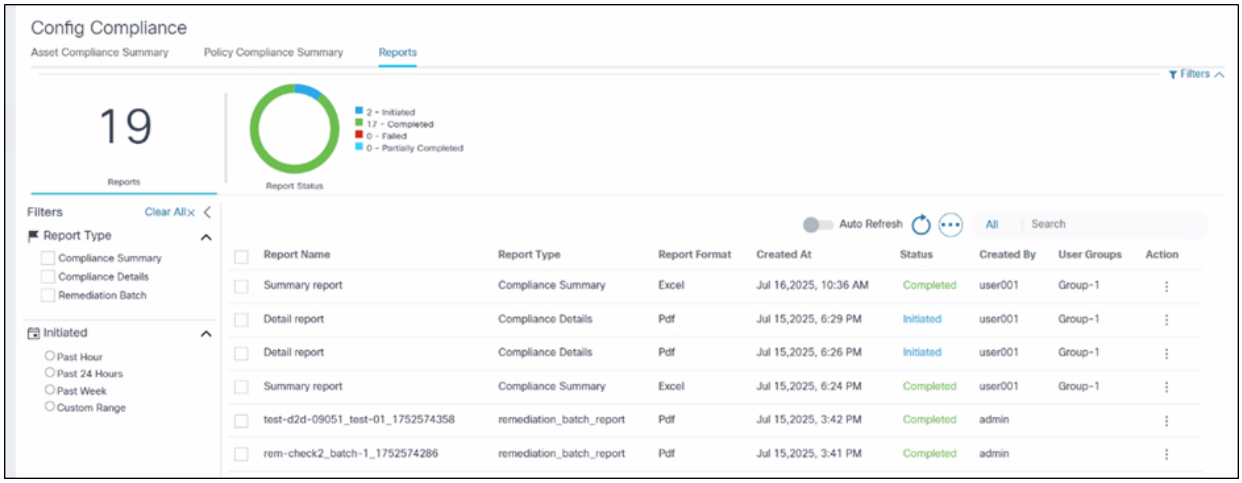
보고 대시보드

Reporting Dashboard(보고 대시보드)는 모든 규정 준수 보고 활동을 위한 중앙 허브 역할을 합니다. 사용자는 이 단일 인터페이스에서 보고서를 효율적으로 관리할 수 있습니다. Reports Dashboard(보고서 대시보드)에서 사용할 수 있는 주요 기능은 다음과 같습니다.

- 보고서 보기: 사용자는 이름, 유형, 관련 정책, 형식, 생성 날짜, 현재 상태(예: 시작됨, 완료됨,

실패, 부분적으로 완료됨)를 포함하여 생성된 모든 보고서의 목록을 볼 수 있습니다
- 보고서 다운로드: 보고서가 생성되면 오프라인 분석 또는 보관을 위해 다운로드할 수 있습니다. Action(작업) 열에는 다운로드 옵션이 제공됩니다
- 보고서 삭제: 사용자는 대시보드에서 오래되거나 불필요한 보고서를 제거할 수 있으므로 깨끗하고 체계적인 보고 환경을 유지하는 데 도움이 됩니다
- 필터링 및 검색: 대시보드는 광범위한 필터링 옵션을 제공하여 사용자가 보고서 유형(예: Compliance Details, Compliance Summary, Remediation Batch), 정책, 시작 상태(예: Past Hour, Past 24 Hours, Past Week, Custom Range) 등의 기준에 따라 특정 보고서를 신속하게 찾을 수 있도록 합니다. 검색 바도 이용하실 수 있습니다
- 보고서 상태 모니터링: 시각적 요약(즉, 파이 차트)은 시작, 완료, 실패 또는 부분적으로 완료된 보고서의 수를 표시하는 보고서의 상태를 나타냅니다.

Reporting(보고) 대시보드는 Compliance and Remediation(컴플라이언스 및 교정) 대시보드의 Reports(보고서) 탭 아래에 있는 랜딩 페이지입니다.



보고서 대시보드

- 사용 가능한 보고서 유형은 다음과 같습니다.
  - 규정 준수 요약 보고서
  - 규정 준수 세부 보고서
  - 리미디에이션 배치 보고서
- 필터를 사용하여 다음을 선택합니다.
  - 보고서 유형
  - 정책
  - 시작된 기간(보고서 목록은 선택한 기간을 기준으로 필터링됨)
- 보고서 목록을 자동으로 새로 고치는 옵션

보고 구성

보고 구성을 사용하면 관리자가 구축 및 비즈니스 요구 사항에 따라 주요 보고 관련 매개변수를 구성할 수 있습니다. 다음 매개변수를 컨피그레이션에 사용할 수 있습니다.

- 다음보다 오래된 보고서 자동 삭제(일): 이 기간보다 오래된 보고서는 시스템에서 삭제됩니다.
- Compliance Summary Report(컴플라이언스 요약 보고서)에서 정책별로 선택할 수 있는 최대 블록: Excel 파일의 탭 수를 읽기 가능한 한도로 유지하는 데 도움이 됩니다
- 규정 준수 세부 보고서에서 선택할 최대 자산: 지정된 상세 보고서에 대해 생성되는 PDF 파일 수를 제한하는 데 도움이 됩니다.

  규정 준수 작업 목록

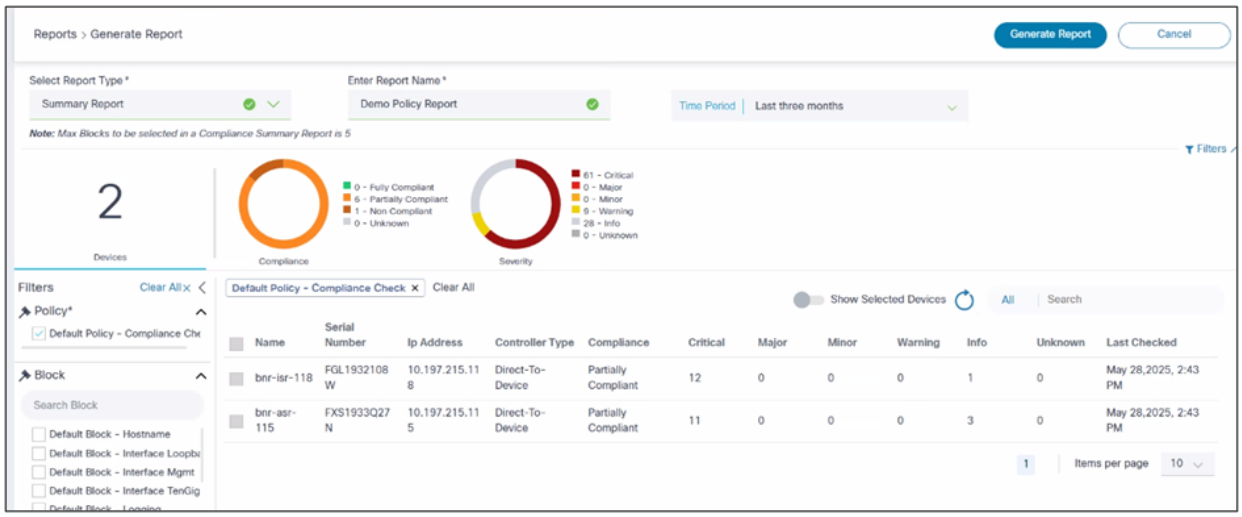
보고서 생성

이 애플리케이션은 사용자가 보고서 유형을 선택하고, 범위를 정의하고, 특정 필터를 적용할 수 있도록 새로운 규정 준수 보고서를 생성하기 위한 전용 인터페이스를 제공합니다. 보고서 생성 프로세스는 Reporting dashboard(보고 대시보드) 페이지 아래의 "Generate Report(보고서 생성)" 작업에서 시작됩니다.

보고서 생성의 주요 측면은 다음과 같습니다.

- 보고서 유형 선택: 사용자는 다음과 같은 서로 다른 보고서 유형 중에서 선택할 수 있습니다
  - 요약 보고서: 선택한 정책에 대한 모든 디바이스의 규정 준수에 대한 개요를 제공합니다.
  - 상세 보고서: 각 디바이스의 특정 위반에 대한 심층적인 정보를 제공하여 더욱 세부적인 뷰를 제공합니다.
- 보고서 이름 지정: 사용자는 생성된 보고서에 대한 관련 이름을 제공해야 합니다
- 기간 선택: 최근 규정 준수 데이터에 초점을 맞추기 위해 "현재 월" 또는 사용자 지정 범위와 같은 특정 기간에 대한 보고서를 생성할 수 있습니다.
- 필터 적용: 포괄적인 필터링 옵션을 통해 사용자는 보고서 범위를 좁힐 수 있습니다
  - 정책: 보고서에 포함할 규정준수 정책을 하나 이상 선택합니다. 정책 선택은 필수입니다.
  - 차단: 선택한 정책 내에서 보고서에 포함할 특정 컨피그레이션 블록을 선택합니다. 블록 선택은 선택 사항입니다.
  - 자산 그룹: 사용자는 하나 이상의 자산 그룹을 선택하여 범위에 있는 자산을 필터링할 수 있습니다
- 자산 선택: 이는 상세 보고서에만 적용됩니다
  - 사용자는 보고서를 생성해야 하는 특정 디바이스를 선택할 수 있습니다
  - 자산 테이블에는 이름, 일련 번호, IP 주소, 관리자, 현재 규정 준수 상태 등의 세부사항이 표시되며 심각도 레벨별 카운트가 포함됩니다

규정준수 요약 보고서를 생성하려면

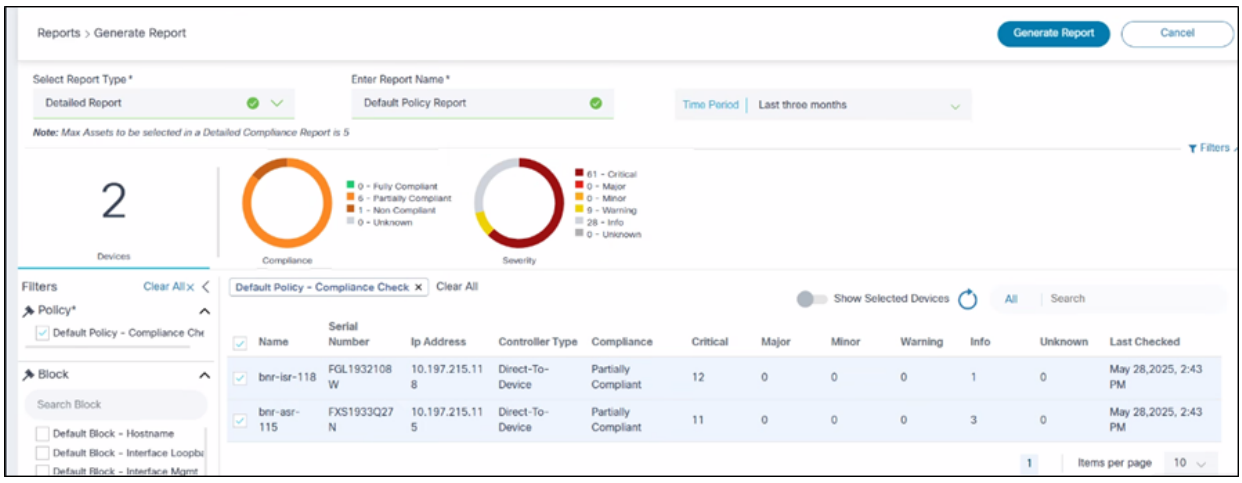


요약 보고서 생성

1. Select Report Type 드롭다운 목록에서 Summary Report를 선택합니다.
2. 보고서 이름을 입력합니다.
3. 시간 범위를 선택합니다. 이 선택에 따라 정책 및 블록이 나열됩니다.
4. 정책을 선택합니다. 추가 정책을 선택할 수도 있습니다.
5. 선택적으로, Blocks를 선택합니다. 선택하지 않으면 모든 블록이 포함됩니다.
6. 필수 자산 그룹, 규정 준수 상태 및 심각도 수준을 선택합니다.
7. Generate Report를 클릭합니다.

- 보고서 목록 페이지에서 보고서 상태가 시작됨으로 설정됩니다
- 완료되면 상태가 완료됨으로 변경됩니다. 하위 보고서 중 일부가 실패할 경우 상태가 Partially Completed(부분적으로 완료됨)로 변경됩니다
- 전체 보고서 생성에 실패하면 알림이 표시되고 상태가 Failed(실패)로 변경됩니다
- 완료되면 다운로드 옵션을 사용할 수 있습니다. Excel 보고서가 포함된 zip 파일을 다운로드할 수 있습니다.

규정 준수 세부 보고서를 생성하려면



세부 보고서 생성

1. Select Report Type 드롭다운 목록에서 Detailed Report를 선택합니다.
2. 보고서 이름을 입력합니다.
3. 시간 범위를 선택합니다. 이 선택에 따라 정책 및 블록이 나열됩니다.
4. 정책을 선택합니다. 추가 정책을 선택할 수도 있습니다.
5. 선택적으로, Blocks를 선택합니다. 선택하지 않으면 모든 블록이 포함됩니다.
6. 필수 자산 그룹, 규정 준수 상태 및 심각도 수준을 선택합니다.
7. 그리드에서 필요한 에셋을 선택합니다. 사용자는 "Select all(모두 선택)" 디바이스 및 "Show selected devices(선택한 디바이스 표시)"를 선택할 수 있습니다.
8. Generate Report를 클릭합니다.

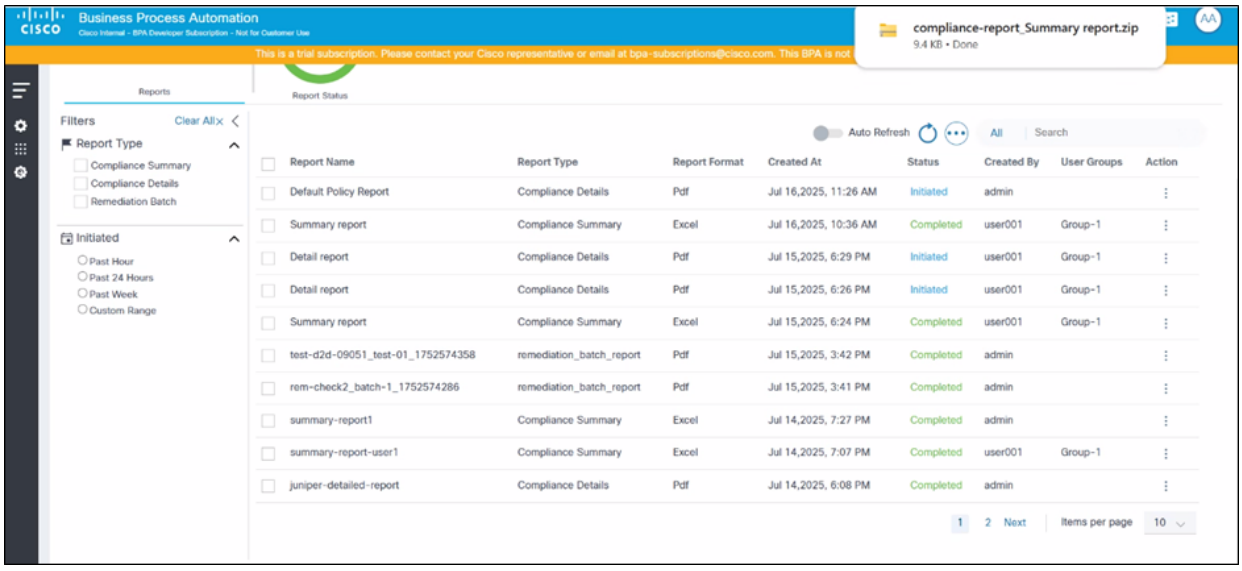
- 보고서 목록 페이지에서 보고서 상태가 시작됨으로 설정됩니다
- 완료되면 상태가 완료됨으로 변경됩니다. 하위 보고서 중 일부가 실패할 경우 상태가 Partially Completed(부분적으로 완료됨)로 변경됩니다
- 전체 보고서 생성에 실패하면 알림이 표시되고 상태가 Failed(실패)로 변경됩니다

보고서 다운로드 및 보기

완료된 보고서는 Reporting Dashboard(보고 대시보드) 그리드의 원하는 행에 있는 Download(다운로드) 아이콘을 사용하여 다운로드할 수 있습니다.

컨피그레이션 컴플라이언스 요약 보고서 이해

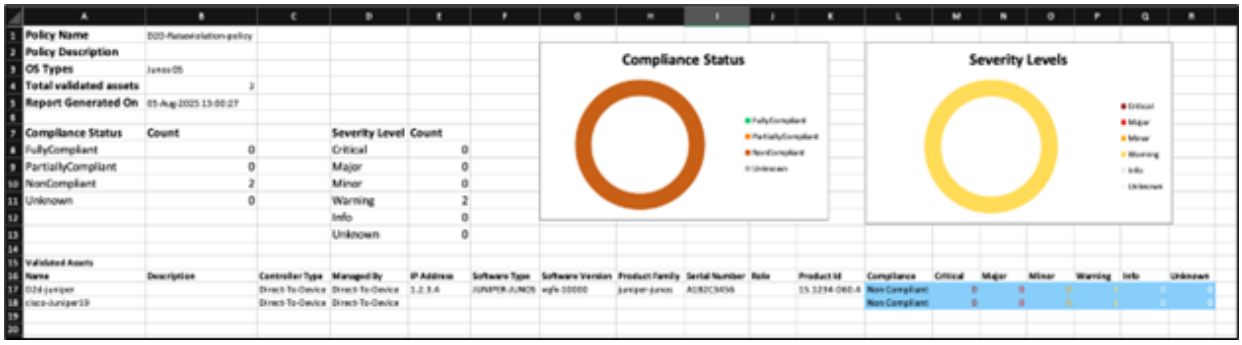
Compliance Summary 보고서는 개별 PDF 보고서가 포함된 zip 파일로, 디바이스당 하나의 PDF가 생성됩니다. 이 보고서 유형은 정책에 따른 컴플라이언스 위반의 개요와 디바이스에 대한 블록 레벨 드릴다운 매핑 위반 세부사항을 제공합니다.



규정 준수 요약 보고서

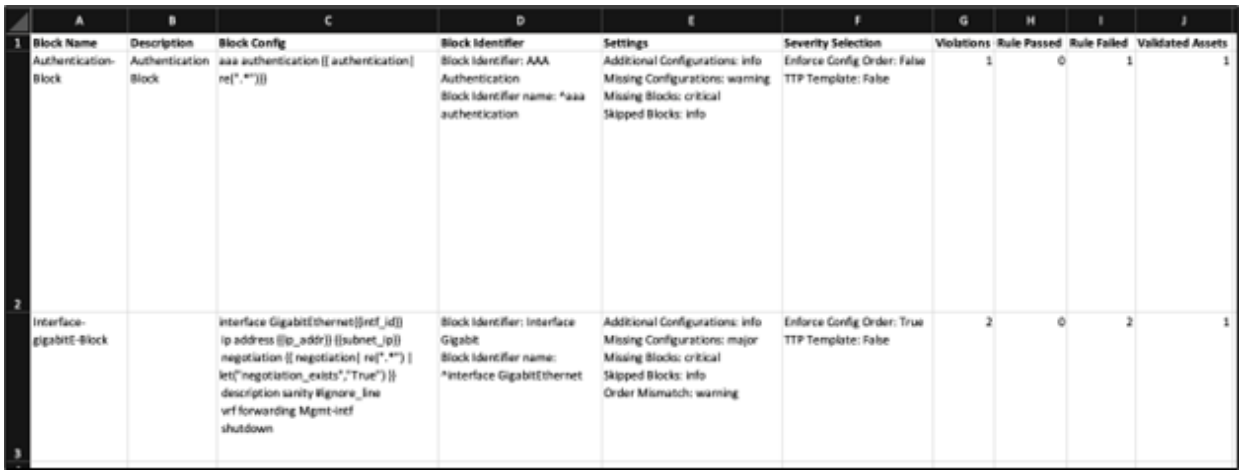
각 Excel 보고서에는 다음 시트가 포함되어 있으며 다음 정보를 제공합니다.

- 정책 요약:
  - 정책 이름, 설명, OS 유형, 검증된 총 자산 등 개요 세부 정보
  - 검증된 자산 카운트를 규정 준수 상태(예: Fully Compliant, Partially Compliant, Non-Compliant, Unknown)별로 분할한 그리드 및 차트 보기
  - 심각도 수준(예: Critical, Major, Minor, Warning Info, Unknown)별로 분할된 총 위반 수에 대한 그리드 및 차트 보기
  - 각 심각도 레벨에 대한 디바이스 세부 정보, 규정 준수 상태 및 위반 수가 포함된 자산 그리드



정책 요약 시트

- 차단 요약:
  - 블록 이름, 설명, 블록 구성, 블록 식별자 세부 정보 및 블록 위반 심각도 설정과 같은 블록 세부 정보
  - 지정된 블록에 대한 위반, 규칙 통과, 규칙 실패 및 자산 검증 횟수



Block Name	Description	Block Config	Block Identifier	Settings	Severity Selection	Violations	Rule Passed	Rule Failed	Validated Assets
Authentication-Block	Authentication Block	aaa authentication {{ authentication| re(".*")}}	Block Identifier: AAA Authentication Block Identifier name: *aaa authentication	Additional Configurations: info Missing Configurations: warning Missing Blocks: critical Skipped Blocks: info	Enforce Config Order: False TTP Template: False	1	0	1	1
Interface-gigabitE-Block		interface GigabitEthernet{{intf_id}} ip address {{ip_addr}} {{subnet_ip}} negotiation {{ negotiation| re(".*") | let("negotiation_exists","True") }} description sanity #ignore_line vrf forwarding Mgmt-intf shutdown	Block Identifier: Interface Gigabit Block Identifier name: ^interface GigabitEthernet	Additional Configurations: info Missing Configurations: major Missing Blocks: critical Skipped Blocks: info Order Mismatch: warning	Enforce Config Order: True TTP Template: False	2	0	2	1

블록 요약 시트

- 블록당 규칙 및 위반 세부사항:
- 위반 레벨 그리드에는 규칙 이름, 설명, 위반 이름, 설명 심각도 레벨, 전체 자산에 표시되는 위반 수, 영향을 받는 자산의 수가 나열됩니다
- 디바이스 레벨 그리드에는 규칙, 위반, 심각도, 디바이스 이름, 컨트롤러 이름(에서 관리) 간의

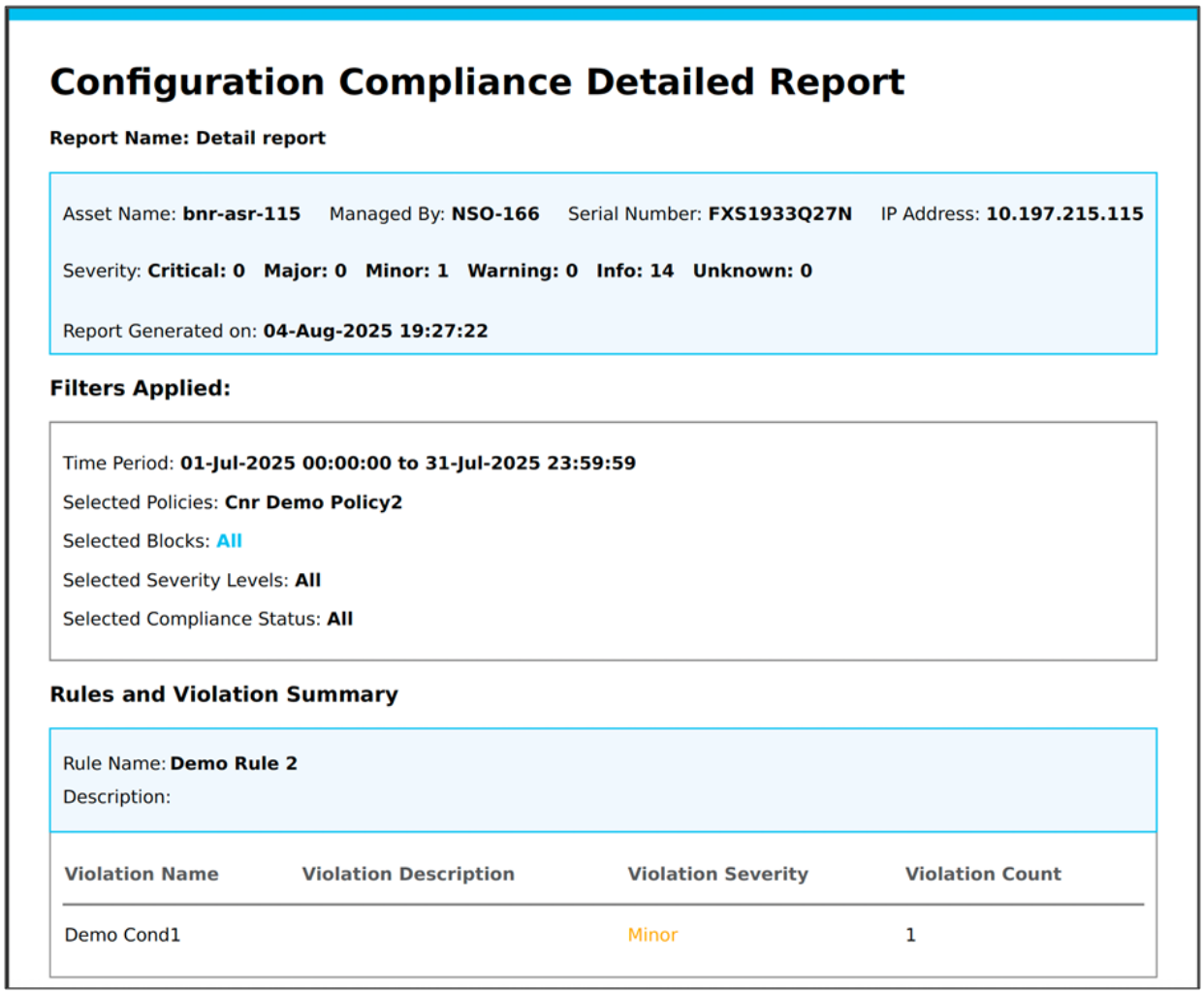
매핑이 표시됩니다

	A	B	C	D	E	F	G
1	**Rule Name**	**Rule Description**	**Violation Name**	**Description**	**Severity**	**Violation Count**	**Affected Assets Count**
2	Gigabit Rule	Rule to validate violations for Gigabit ethernet configuration	DescriptionCheck		warning	5	3
3	Gigabit Rule	Rule to validate violations for Gigabit ethernet configuration	IP-Address-Validation		critical	6	2
4	Gigabit Rule	Rule to validate violations for Gigabit ethernet configuration	No-Shutdown-check		compliant	0	0
5							
6							
7	**Rule Name**	**Violation Name**	**Severity**	**Device Name**	**Managed By**		
8	Gigabit Rule	DescriptionCheck	warning	bnr-isr-118	Direct-To-Device		
9	Gigabit Rule	DescriptionCheck	warning	bnr-isr-119	Direct-To-Device		
10	Gigabit Rule	DescriptionCheck	warning	bnr-isr-121	Direct-To-Device		
11	Gigabit Rule	IP-Address-Validation	critical	bnr-isr-118	Direct-To-Device		
12	Gigabit Rule	IP-Address-Validation	critical	bnr-isr-120	Direct-To-Device		
13							

컴플라이언스 세부사항 보고서

Compliance details(컴플라이언스 세부사항) 보고서에는 다음 정보가 포함됩니다.

- 보고서 이름: 보고서의 이름을 식별합니다
  - 자산 이름: 규정 준수 검사가 수행된 디바이스를 지정합니다
  - 기타 자산 세부사항: IP 주소 및 일련 번호(있는 경우)와 같은 세부사항이 포함됩니다.
  - 심각도: 심각도 수준별 위반 요약 수 제공
  - 보고서 생성 날짜: 보고서를 만든 시간의 타임스탬프를 나타냅니다.
- 적용된 필터: 특정 보고서를 생성하는 데 사용되는 특정 필터 기준의 세부 정보를 간략하게 보여 주며 투명성과 재현성을 보장합니다. 여기에는 기간, 선택한 정책, 블록, 심각도 레벨, 규정 준수 상태가 포함됩니다
- 규칙 및 위반 요약: 평가된 각 규칙을 나열하고 해당 규칙에 대해 발견된 위반의 요약을 제공합니다. 요약 그리드에는 위반 이름, 설명, 심각도 및 위반 횟수가 표시됩니다
- 위반 세부 정보: 선택한 블록의 각 디바이스 컨피그레이션 라인에 대한 명시적 세부사항과 각 라인의 위반 세부사항을 제공합니다.



Configuration Compliance Detailed Report

Report Name: Detail report

Asset Name: **bnr-asr-115** Managed By: **NSO-166** Serial Number: **FXS1933Q27N** IP Address: **10.197.215.115**

Severity: **Critical: 0** **Major: 0** **Minor: 1** **Warning: 0** **Info: 14** **Unknown: 0**

Report Generated on: **04-Aug-2025 19:27:22**

Filters Applied:

Time Period: **01-Jul-2025 00:00:00 to 31-Jul-2025 23:59:59**

Selected Policies: **Cnr Demo Policy2**

Selected Blocks: **All**

Selected Severity Levels: **All**

Selected Compliance Status: **All**

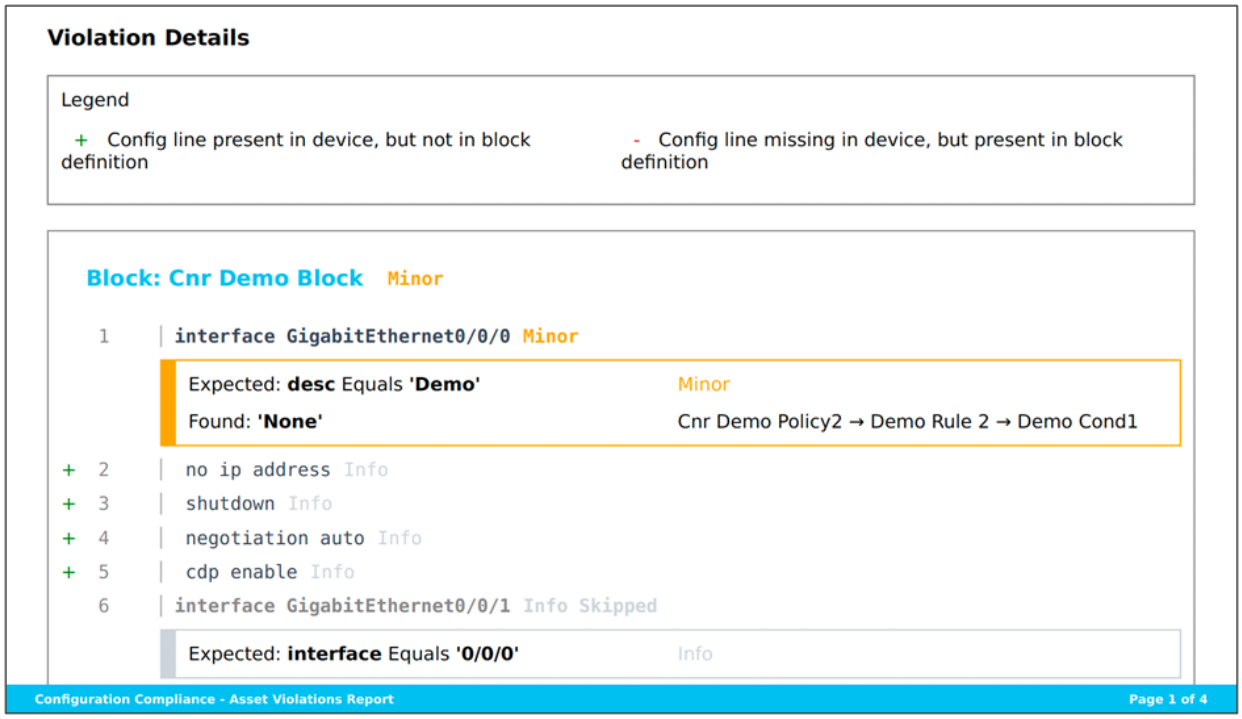
Rules and Violation Summary

Rule Name: **Demo Rule 2**

Description:

Violation Name	Violation Description	Violation Severity	Violation Count
Demo Cond1		Minor	1

규정 준수 세부 보고서 - 샘플 PDF 페이지 1



Violation Details

Legend

\+ Config line present in device, but not in block definition

\- Config line missing in device, but present in block definition

Block: Cnr Demo Block Minor

```
  1   interface GigabitEthernet0/0/0 Minor
```

Expected: **desc** Equals **'Demo'** Minor

Found: **'None'** Cnr Demo Policy2 → Demo Rule 2 → Demo Cond1

```
+ 2   no ip address Info
+ 3   shutdown Info
+ 4   negotiation auto Info
+ 5   cdp enable Info
  6   interface GigabitEthernet0/0/1 Info Skipped
```

Expected: **interface** Equals **'0/0/0'** Info

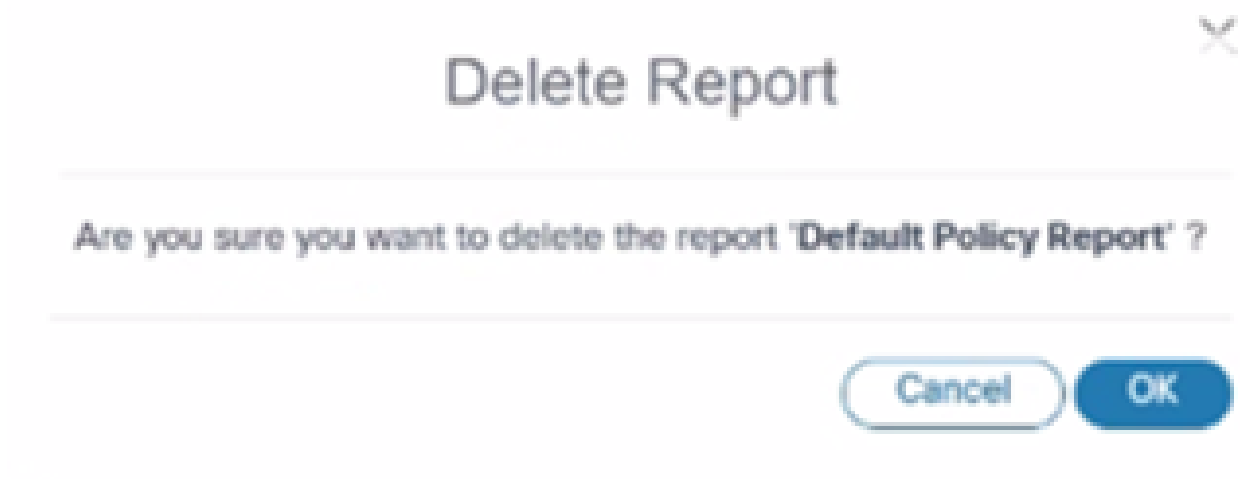
Configuration Compliance - Asset Violations Report Page 1 of 4

규정 준수 세부 보고서 - 샘플 PDF 2페이지

참고: Remediation batch(교정 배치) 페이지에서 생성된 교정 배치 PDF 보고서도 보고서 목록에서 다운로드하여 볼 수 있습니다.

보고서 삭제

보고서는 삭제 아이콘 을 선택하여 개별적으로 삭제할 수도 있고, 보고서의 확인란을 선택하고 추가 옵션 아이콘 > 삭제를 선택하여 대량으로 삭제할 수도 있습니다.



규정 준수 작업 목록

참고: 보고서를 삭제하면 보고 대시보드에서 보고서 파일 및 항목만 제거됩니다. 기본 규정 준수 실행 세부 정보가 유지됩니다.

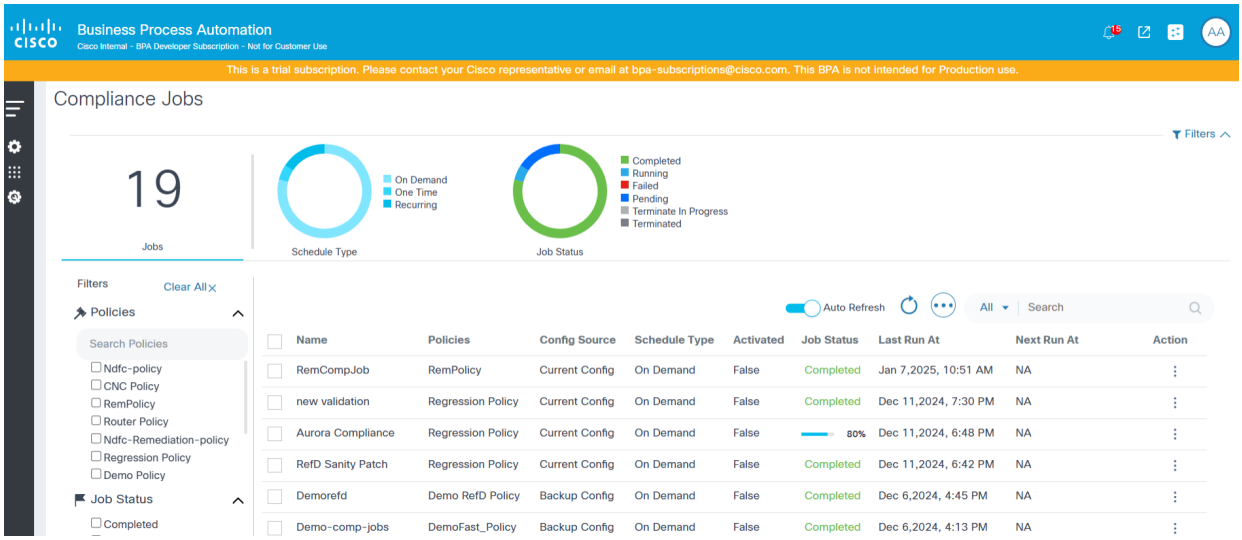
규정 준수 작업

차세대 포털의 규정 준수 작업 기능은 사용자가 선택한 정책 및 자산 그룹에서 규정 준수 작업을 생성, 관리 및 실행할 수 있도록 설계되었습니다. 이러한 작업은 일정 간격으로 실행되도록 예약하거나 온디맨드 방식으로 실행할 수 있으므로 모든 자산이 일관성 있게 규정을 준수하는지 점검할 수 있습니다.

주요 기능

- 규정 준수 작업 나열: 오프라인 감사, 필터링, 생성, 편집, 삭제 및 실행 옵션과 함께 정의된 모든 규정준수 작업을 봅니다.
- 예약 및 온디맨드 작업: 예약된 간격으로 실행되도록 작업을 설정하거나 필요에 따라 즉시 실행할 수 있습니다.
- 세부적인 액세스 제어: 규정 준수 작업에 대한 액세스는 사용자 권한에 따라 제어되므로 사용

자가 액세스 권한이 있는 정책과 관련된 작업만 볼 수 있습니다.
- 필터링 옵션: 쉽게 탐색하고 관리할 수 있도록 정책, 작업 상태, 일정 유형 및 날짜 범위를 기준으로 작업을 필터링합니다.



규정 준수 작업 목록

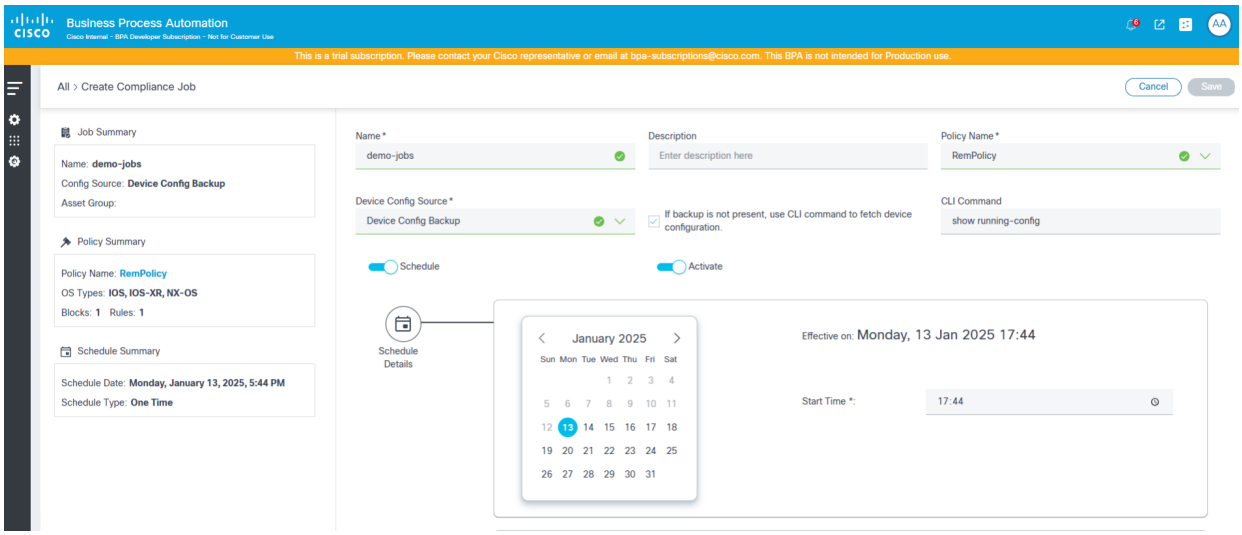
규정 준수 작업 생성

[규정준수 작업 생성] 페이지는 다음 속성을 포함합니다.

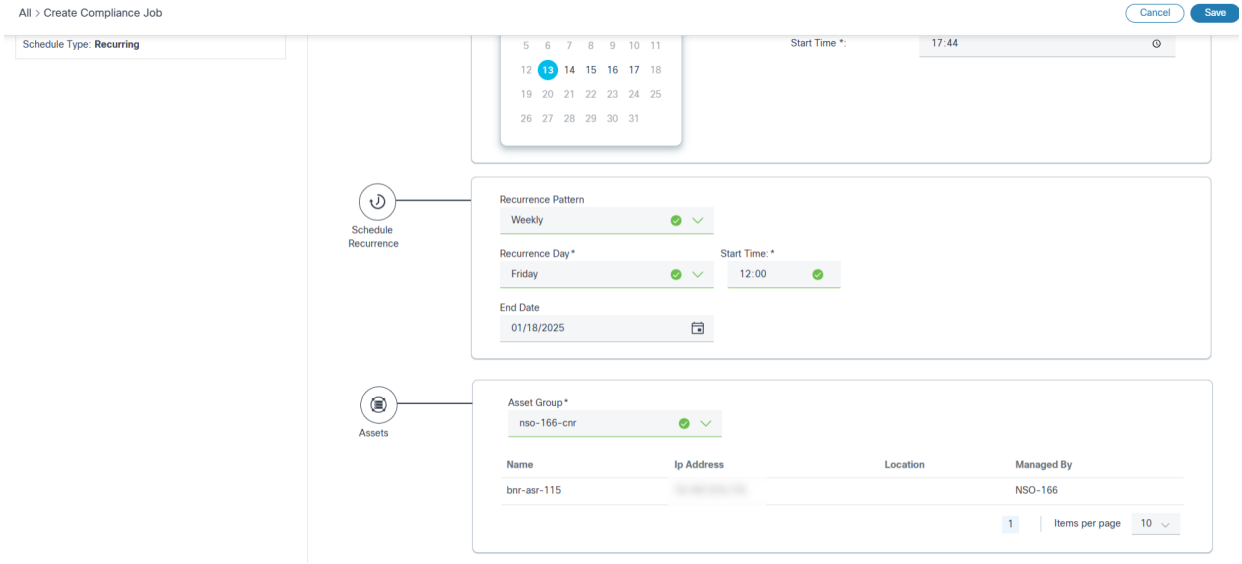
- 이름: 작업 이름
- 설명: 선택적 설명
- 정책 이름: 실행할 정책을 선택할 수 있는 드롭다운 목록입니다. 이 목록은 로그인한 사용자에 대해 구성된 액세스 정책에 따라 필터링될 수 있습니다
- 디바이스 컨피그레이션 소스: 규정 준수 작업을 실행하기 위한 디바이스 컨피그레이션(현재 컨피그레이션 또는 디바이스 컨피그레이션 백업)을 가져올 소스를 선택할 수 있는 드롭다운 목록과 백업이 없는 경우 CLI 명령으로 대체할지 여부를 나타내는 확인란이 있습니다.

참고: Device Config Backup 옵션은 기본 컨트롤러가 백업 기능을 지원하는 경우에만 작동합니다.

- 사용자 정의 변수: 선택한 정책에 사용자 정의 변수가 있는 경우 사용 가능한 네임스페이스에 대한 편집 가능한 텍스트 상자
- 일정 세부 정보: 시작 및 종료 날짜/시간, 되풀이 패턴 등 다양한 일정 매개 변수를 선택하는 섹션입니다.
- 자산: 규정 준수를 실행할 디바이스 목록을 식별할 자산 그룹을 선택하는 섹션
- 일정: 일정대로 작업 실행을 활성화 또는 비활성화하려면 토글합니다(1회 또는 반복). 비활성화된 경우 작업이 즉시 실행됩니다
- 활성 상태: 선택한 일정이 활성 상태인지 여부를 나타냅니다.



규정 준수 작업 생성



규정준수 작업 생성 2

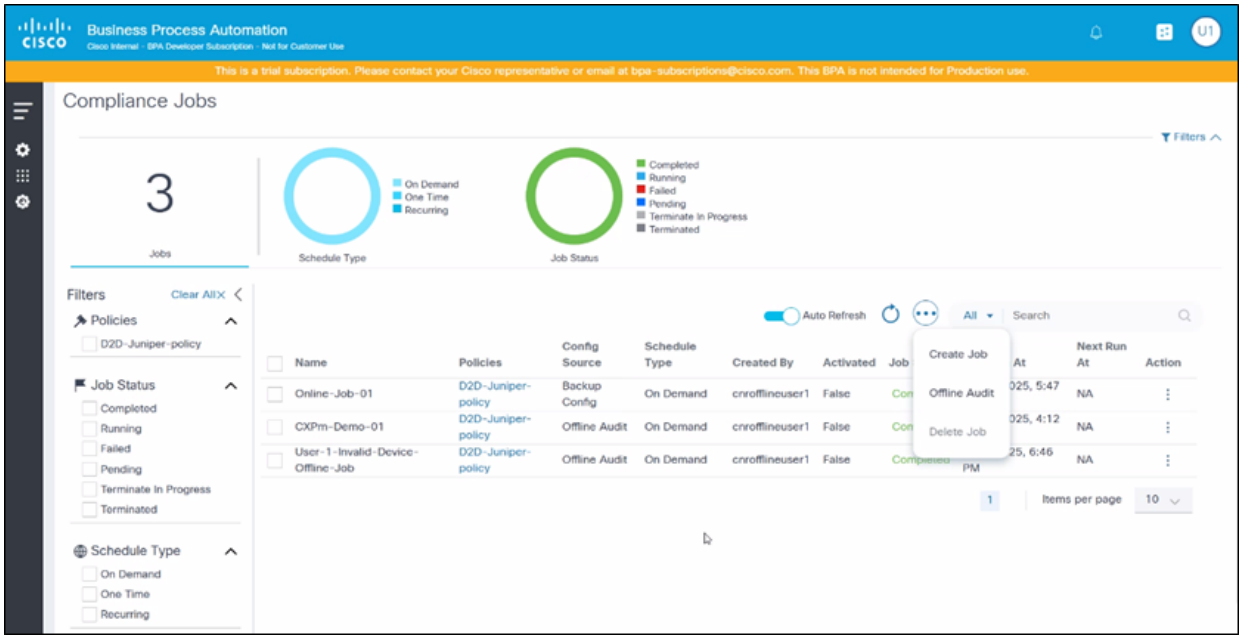
오프라인 감사 작업 생성

규정 준수 작업의 오프라인 감사 기능을 사용하면 디바이스를 BPA에 온보딩하지 않고도 디바이스 컨피그레이션에 대한 규정 준수 확인을 수행할 수 있습니다. 사용자는 디바이스 컨피그레이션을 파일로 수동으로 업로드할 수 있습니다. 여러 디바이스 컨피그레이션을 압축하여 zip 파일로 함께 업로드할 수 있습니다. 업로드되면 이러한 컨피그레이션 파일이 구문 분석되고 해당 파일 콘텐츠를 소스로 사용하여 컴플라이언스 작업을 생성할 수 있습니다. 오프라인 감사 결과는 온라인 감사 결과와 함께 규정 준수 대시보드에 표시됩니다.

오프라인 감사 페이지는 다음 속성을 포함합니다.

- 이름: 작업 이름
- 설명: 선택적 설명

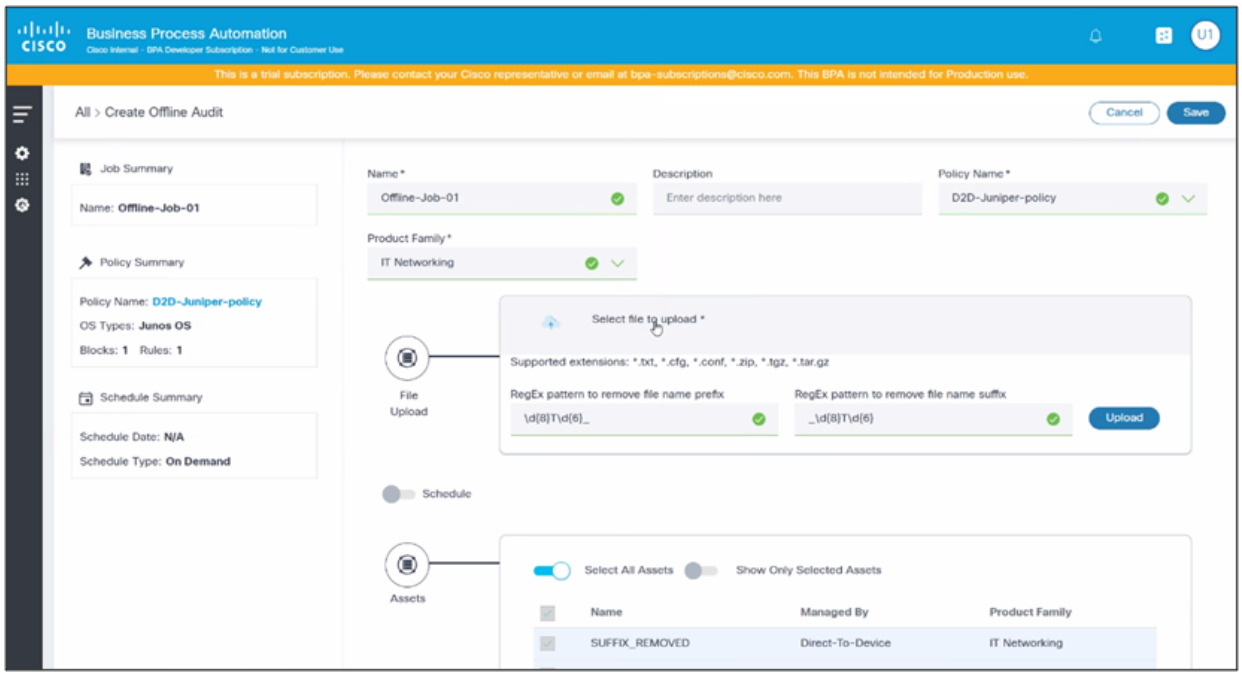
- 정책 이름: 실행할 정책을 선택할 수 있는 드롭다운 목록입니다. 이 목록은 로그인한 사용자에 대해 구성된 액세스 정책에 따라 필터링될 수 있습니다
- 제품군: 제품군을 선택할 수 있는 드롭다운 목록
- 파일 업로드: 오프라인 감사 기능을 사용하여 컨피그레이션 파일을 수동으로 업로드합니다. 이 작업은 로컬 시스템에서 파일을 선택하는 업로드 인터페이스를 통해 수행됩니다
- 일정: 일정을 설정하려면 토글
- 자산: 업로드된 파일 콘텐츠에 따라 디바이스 목록을 표시합니다.



오프라인 감사 선택

오프라인 감사 작업을 생성하려면

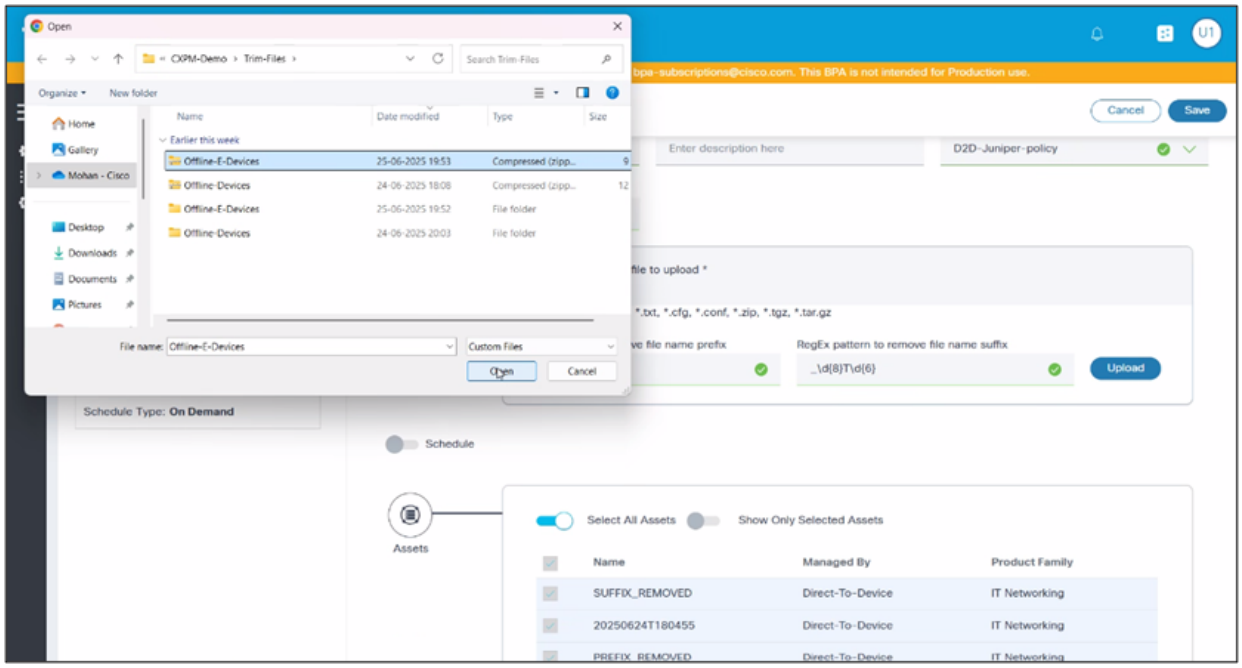
1. More Options(추가 옵션) 아이콘에서 Offline Audit(오프라인 감사)을 선택합니다.



파일 업로드

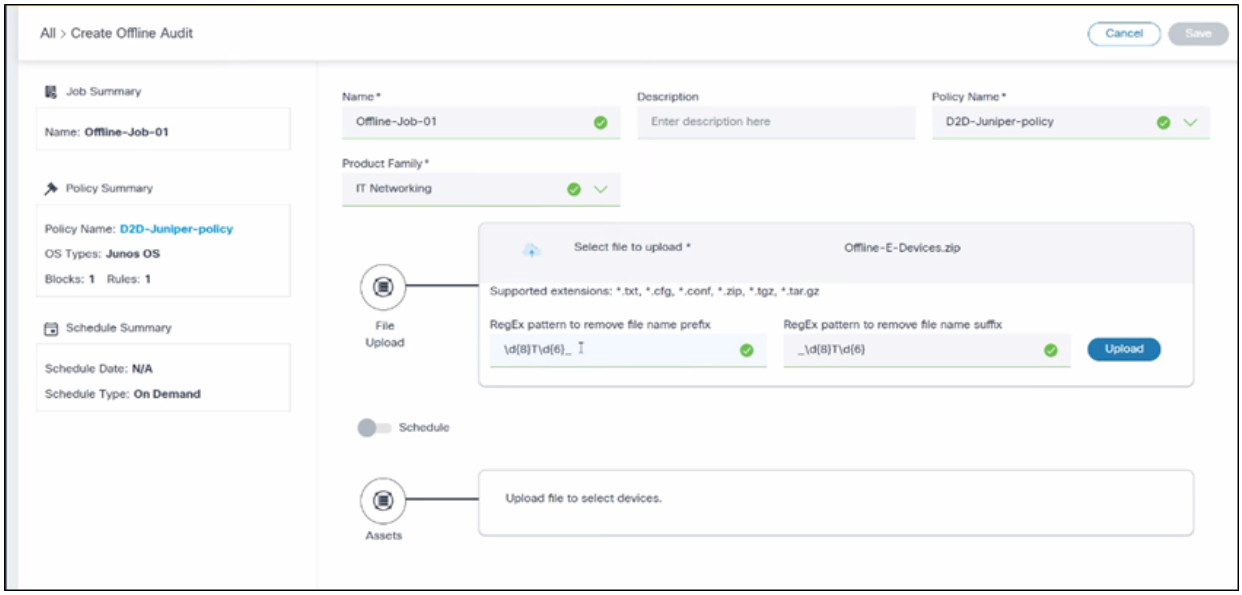
2. 컨피그레이션 파일을 업로드하기 위해 업로드할 파일 선택을 클릭합니다.

참고: 지원되는 파일 유형은 (.txt,.cfg,.conf,.zip,.tgz,.tar.gz)입니다.



데스크톱 파일

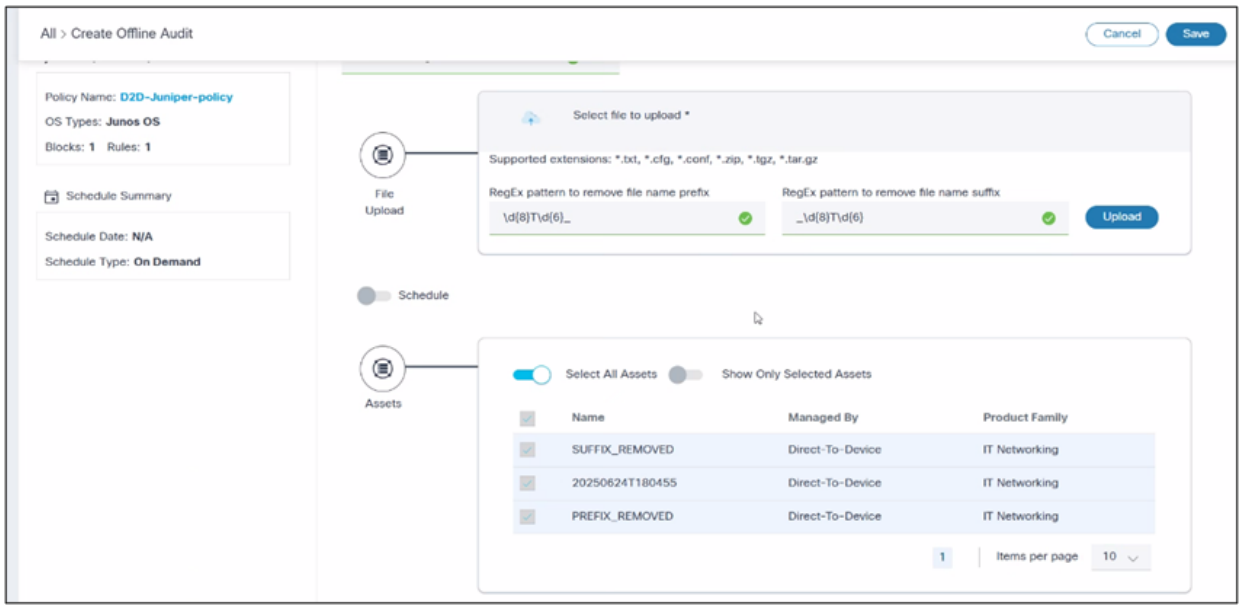
3. 컨피그레이션 파일이 폴더나 아카이브에서 압축된 경우 업로드하기 전에 파일의 압축을 풉니다.



Regex 패턴

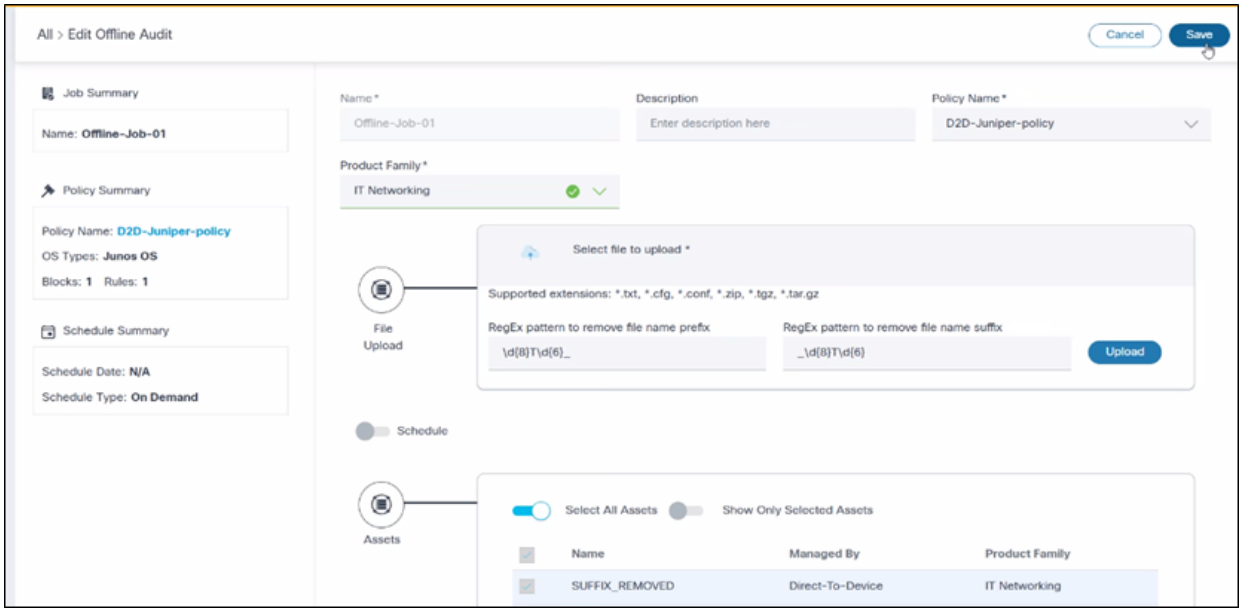
4. 파일 이름 트리밍에 Regex 패턴을 적용합니다(선택 사항).

참고: 접두사 또는 접미사 트리밍 패턴(regex)을 사용하여 업로드된 파일 이름을 표준화하거나 단순화하여 더 쉽게 처리할 수 있습니다.



파일 업로드

5. Upload를 클릭합니다. 파일이 데이터베이스에 저장되고 성공적으로 업로드되었음을 나타내는 확인 메시지가 표시됩니다.



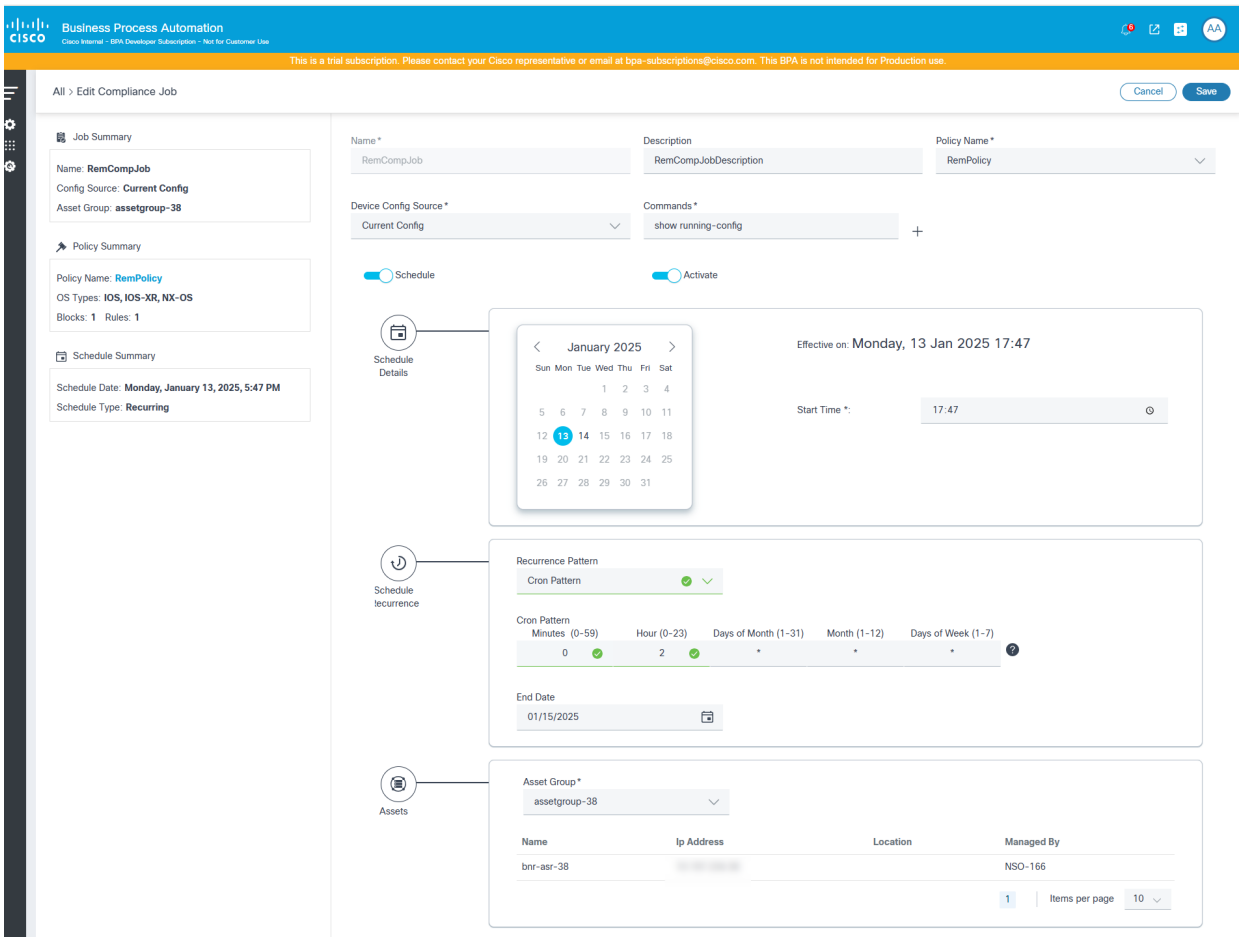
오프라인 감사 저장

6. 오프라인 감사 작업을 만들려면 저장을 클릭합니다.

규정준수 작업 편집

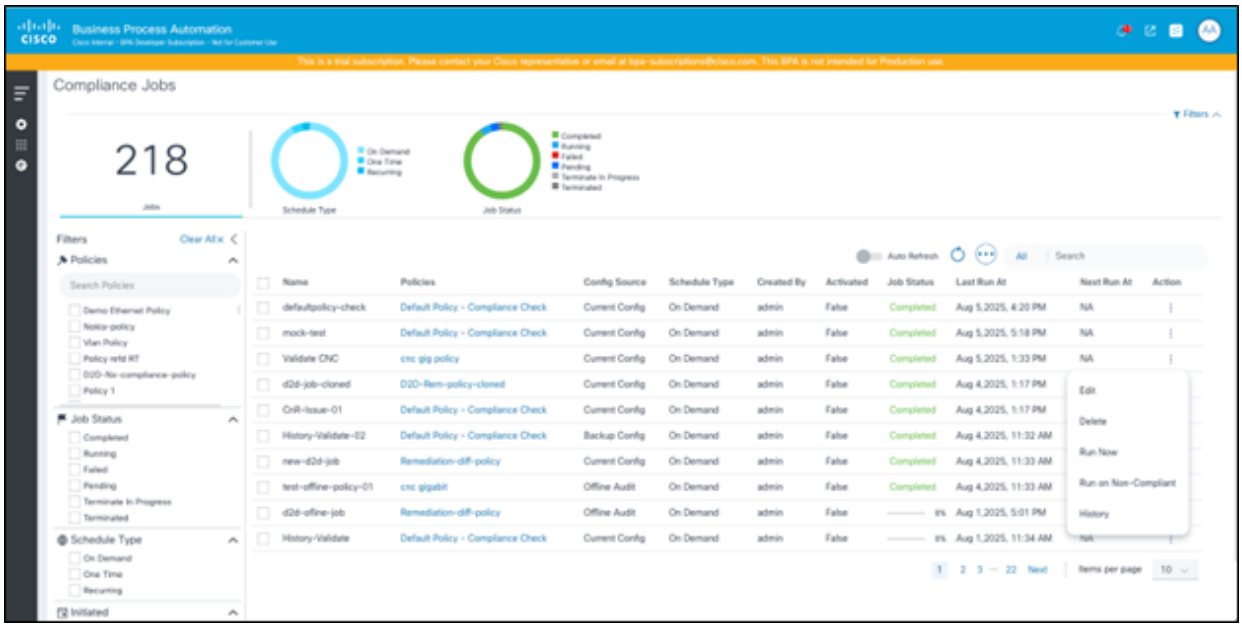
규정준수 작업을 편집하려면 규정준수 작업 생성에 제공된 단계를 수행합니다.

✎ 참고: 작업 이름을 편집할 수 없습니다.



규정준수 작업 편집

지금 실행 또는 컴플라이언스 작업 다시 실행



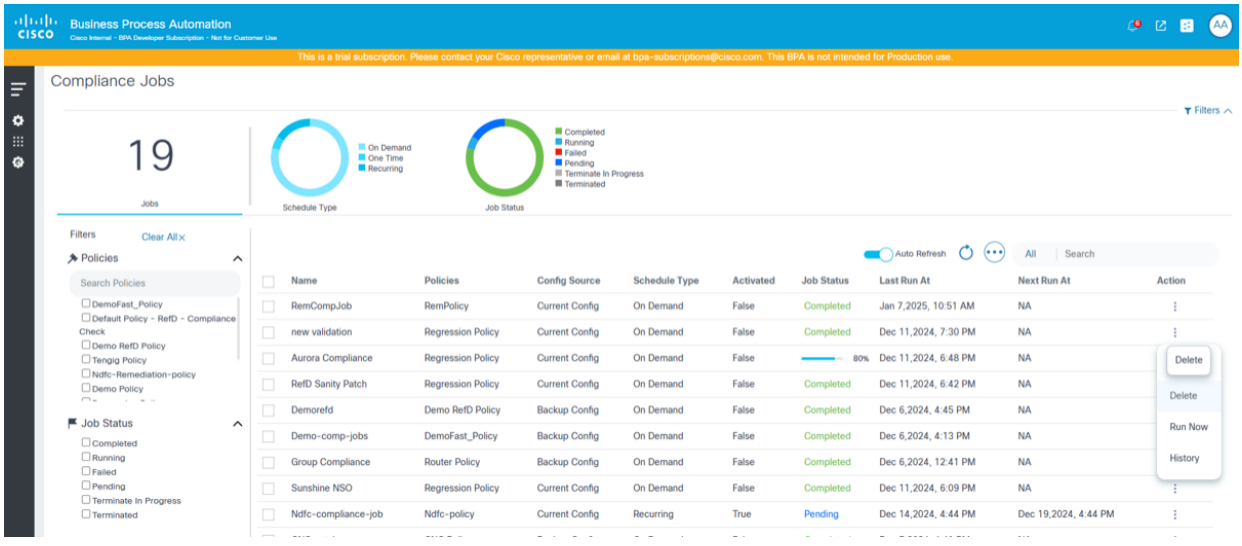
규정준수 작업 - 지금 실행 및 규정준수 위반 시 실행

규정 준수 작업 그리드에는 [추가 옵션] 아이콘에서 지금 실행을 선택하여 요청 시 작업을 실행할 수 있는 옵션이 있습니다. 작업에 기존 실행이 있는 경우 사용자는 추가 옵션 아이콘에서 규정 미준수에서 실행을 선택할 수 있습니다. 이 작업은 이전 실행에서 Fully Compliant로 표시되지 않은 자산 목록에서만 규정 준수 작업을 실행합니다.

규정준수 작업 삭제

포털에서는 사용자가 올바른 RBAC(역할 기반 액세스 제어) 역할을 가진 경우 하나 이상의 규정 준수 작업을 삭제할 수 있는 옵션을 제공합니다. 실행이 진행 중일 때는 작업을 삭제할 수 없습니다. 사용자는 단일 또는 다중 규정 준수 작업을 삭제하도록 선택할 수 있습니다.

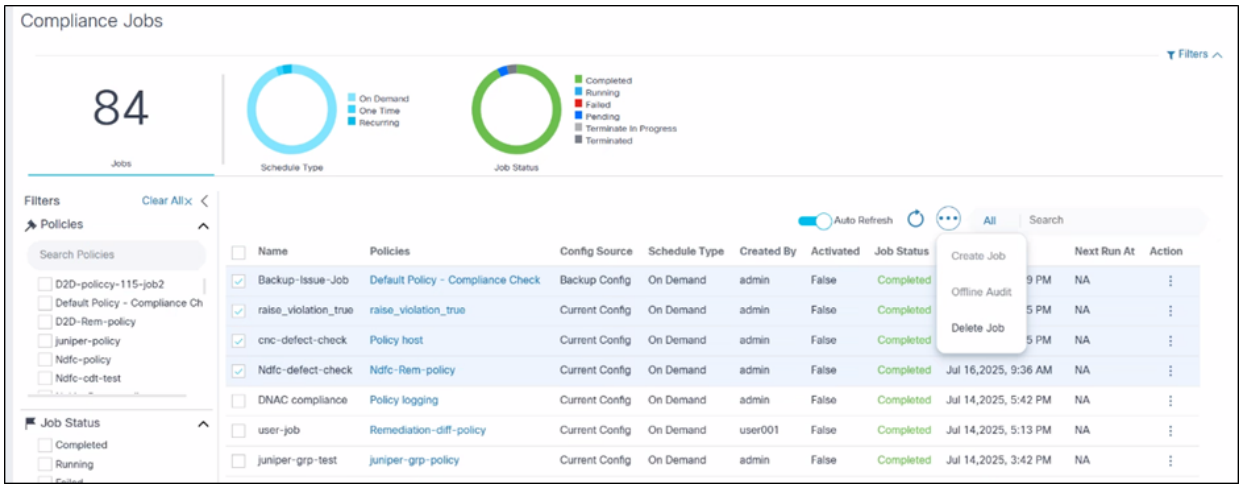
규정준수 작업을 삭제하려면



단일 규정 준수 작업 삭제

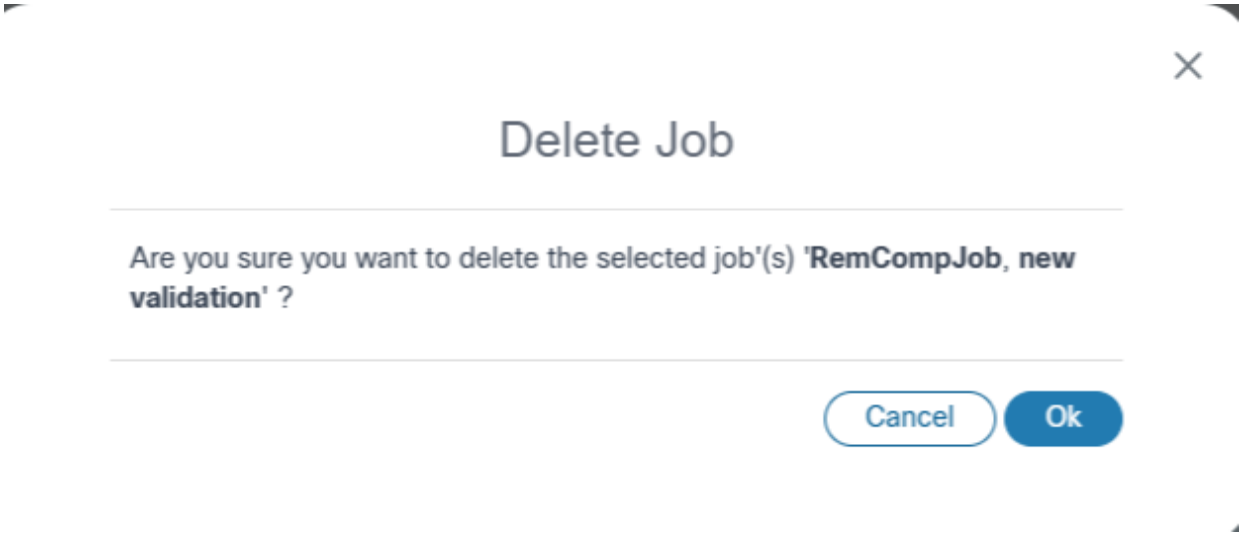
1. Compliance Jobs 페이지에서 삭제할 작업에서 추가 옵션 아이콘 > 삭제를 선택합니다.

또는



여러 규정 준수 작업 삭제

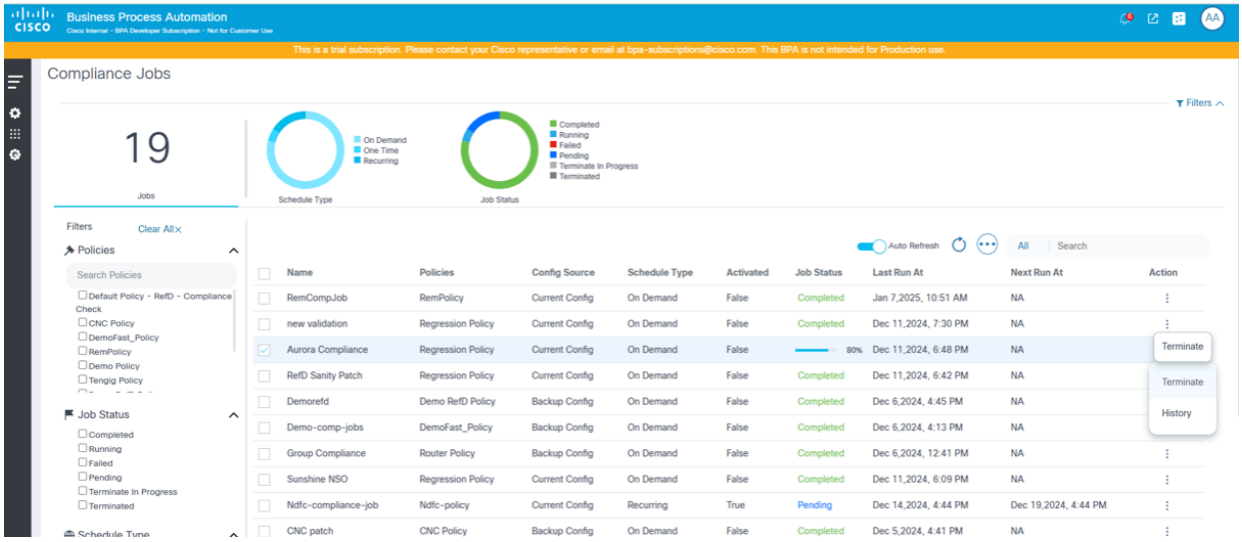
여러 준수 작업을 삭제하려면 삭제할 작업의 확인란을 선택하고 추가 옵션 > 작업 삭제를 선택합니다. 확인 메시지가 표시됩니다.



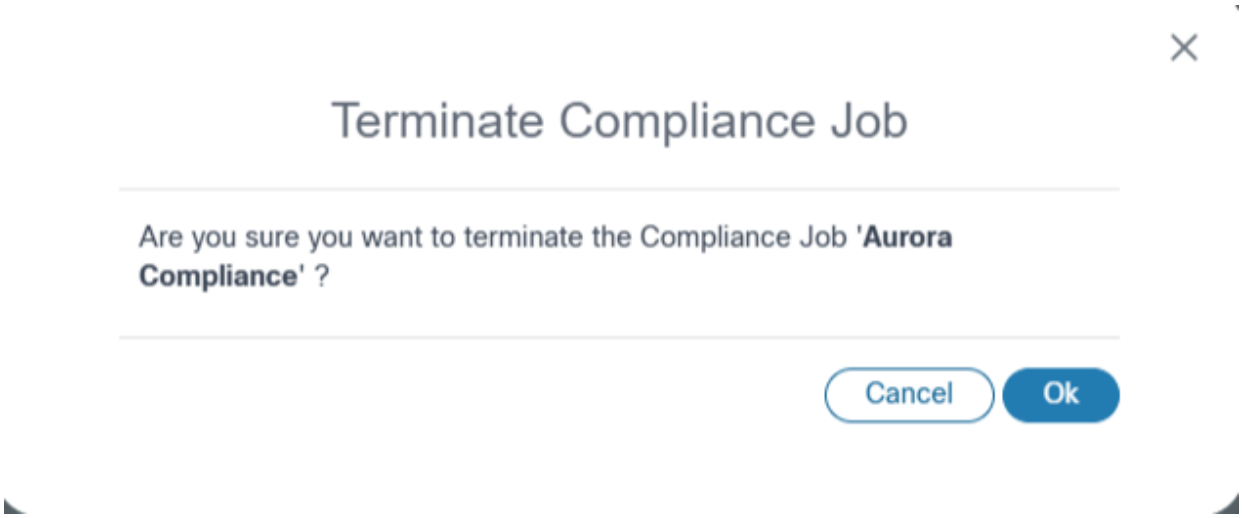
규정 준수 작업 삭제 확인

규정 준수 작업 종료

포털은 사용자에게 지정된 작업의 실행 중인 실행을 종료할 수 있는 옵션을 제공합니다. 작업이 종료되면 현재 실행 중인 디바이스가 실행을 완료하고 대기열에 추가된 모든 디바이스 실행을 취소합니다.



규정 준수 작업 종료

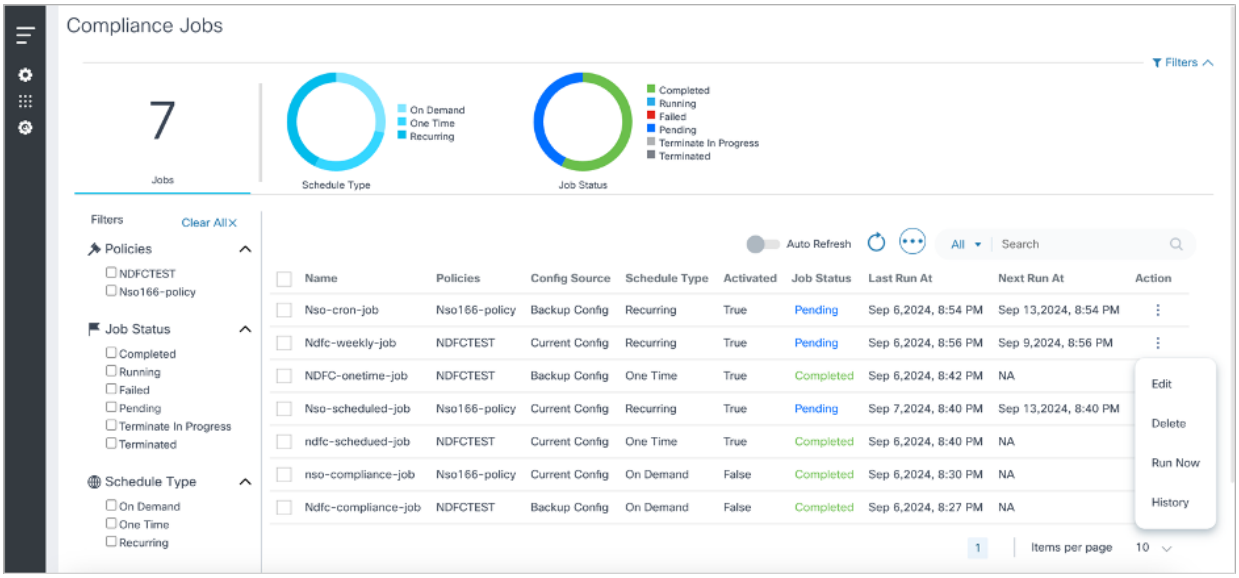


규정 준수 작업 종료 확인

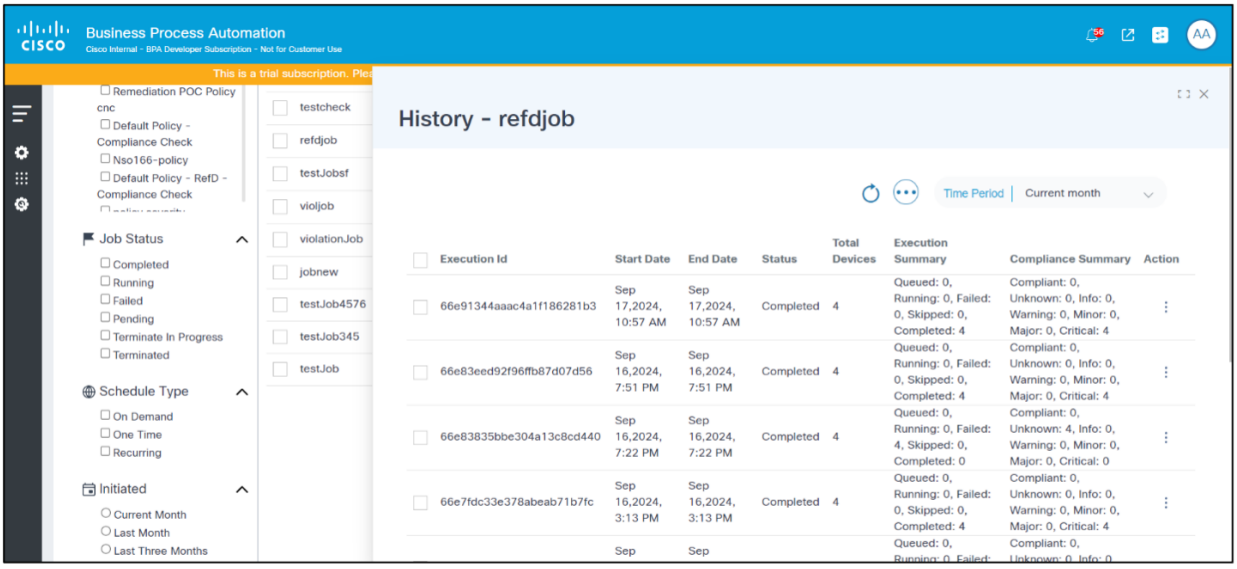
규정 준수 작업 기록

[규정 준수 작업]의 [기록] 옵션은 일정 날짜 범위를 기준으로 필터링된 선택한 작업의 실행 목록을 표시합니다.

규정준수 작업 기록을 보려면 [규정준수 작업] 페이지에서 추가 옵션 아이콘 > 기록을 선택합니다. 기록 페이지가 표시됩니다.



규정 준수 작업 기록

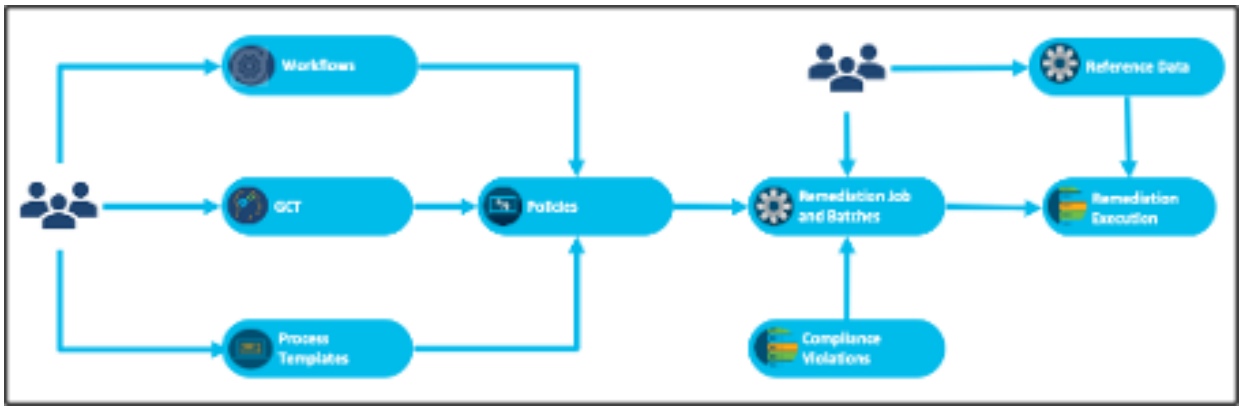


기록 페이지

교정 작업

Remediation Framework를 통해 운영자는 컴플라이언스 대시보드에 나열된 컴플라이언스 위반을 해결할 수 있습니다. 이 프레임워크는 워크플로, GCT 및 프로세스 템플릿을 사용합니다.

컨피그레이션 리미디에이션 흐름도



컨피그레이션 교정 개요

컨피그레이션 교정 활용 사례를 통해 운영자는 교정 작업을 사용하여 디바이스에서 컨피그레이션 위반을 수정할 수 있습니다. 규정 준수 정책은 먼저 컨트롤러 유형별 적절한 워크플로, GCT 템플릿 및 프로세스 템플릿으로 구성됩니다. 영향 받는 자산 목록에 대한 정책에 대해 교정 작업이 실행됩니다. 교정 중에 디바이스에 적용할 값은 규정 준수 실행 결과, RefD 애플리케이션 및 기존 디바이스 컨피그레이션을 비롯한 다양한 데이터 소스에서 가져올 수 있습니다. 특정 고객 요구 사항에 따라 워크플로를 맞춤화하여 교정 중에 추가 단계를 수용할 수 있습니다.

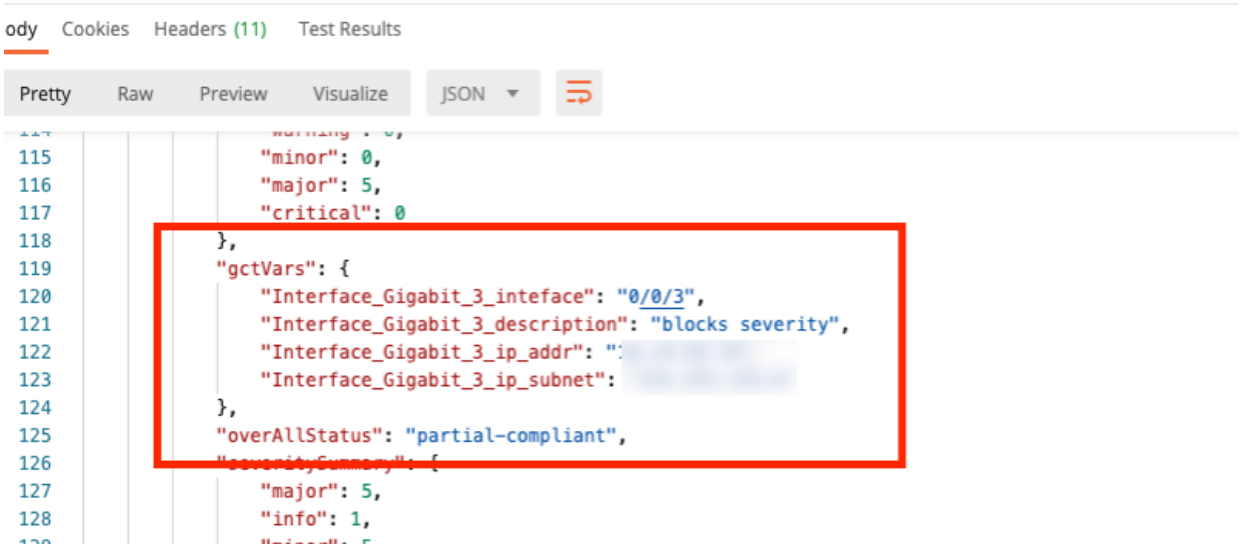
교정 기능의 가장 중요한 단계는 다음과 같습니다.

GCT 템플릿

GCT는 컨트롤러별 템플릿을 사용하여 디바이스에 컨피그레이션 변경 사항을 적용하는 데 사용되는 BPA 핵심 기능입니다.

- 디바이스 컨피그레이션을 업데이트하는 GCT 템플릿 생성, 컴플라이언스 위반 해결
- GCT 템플릿 내의 변수가 다음 구문을 준수하는 경우 프레임워크는 자동 변수 매핑을 지원합니다.
  - 단일 디바이스 컨피그레이션 블록의 경우: <>_<>. 예: management_interface_ipv4_addr, management_interface_ipv4_subnet
  - 여러 디바이스 컨피그레이션 블록이 향후 릴리스에 계획됨
- "Block Identifier Name" 및 "Variable Name from block"에 공백이 포함된 경우 이러한 공백은 밑줄("_")로 대체해야 합니다. 예를 들어, If"Block Identifier Name"은 "Management Interface"이고 "Variable Name"은 "IPV4_ADDR"이면 GCT의 변수 이름은 "Management_Interface_IPV4_ADDR"이어야 합니다.
- 사용자는 규정 준수 디바이스 실행의 "gctVars" 출력을 확인하여 GCT 변수 구문 및 매핑이 올바른지 확인할 수 있습니다. 규정 준수 디바이스 실행을 가져오려면 다음 REST API를 사용합니다.
  - 실행 ID를 찾기 위해 실행 가져오기
    - URL: /api/v1.0/compliance-remediation/compliance-executions
    - 방법: 가져오기
  - 실행 ID를 사용하여 장치 실행 가져오기
    - URL: https://<>/bpa/api/v1.0/compliance-remediation/compliance-device-

execution?executionId=<>
    - 방법: 가져오기



GCT 변수 - gctVar

- 블록에서 변수를 검색하려면 다음 REST API를 사용합니다.
    - URL: https://<>/bpa/api/v1.0/compliance-remediation/utils/schema
    - 방법: POST
    - 본문: {"blockName": "<< 블록 이름 >>" }
- 디바이스에 템플릿을 적용하여 GCT 템플릿을 검증하여 dry run 및 commit 모두 수행
- 규정 준수 정책에서 위의 GCT 템플릿을 구성합니다

워크플로

교정 프레임워크는 다음과 같은 기본 참조 워크플로를 제공합니다.

- 교정 프로세스: 이 워크플로에는 교정 실행과 관련된 일반적인 단계 집합이 있습니다.
- 교정 하위 프로세스: 이 워크플로에는 요건에 따라 다른 팀에서 사용자 지정할 수 있는 변수 할당, GCT dry run 및 GCT commit 작업이 포함되어 있습니다.

두 워크플로 모두 현재 상태 그대로 사용하거나, 고객의 필요에 따라 업데이트하거나, 교체할 수 있습니다.

프로세스 템플릿

정책에 대해 프로세스 템플릿 및 분석 템플릿을 구성하여 사전 및 사후 검사를 실행하고 출력을 비교할 수 있습니다.

정책

CnR 정책은 작업을 사용하여 컨피그레이션을 교정하는 데 사용할 수 있는 워크플로, GCT 템플릿 및 디바이스 유형별 프로세스 템플릿을 모두 포함합니다.

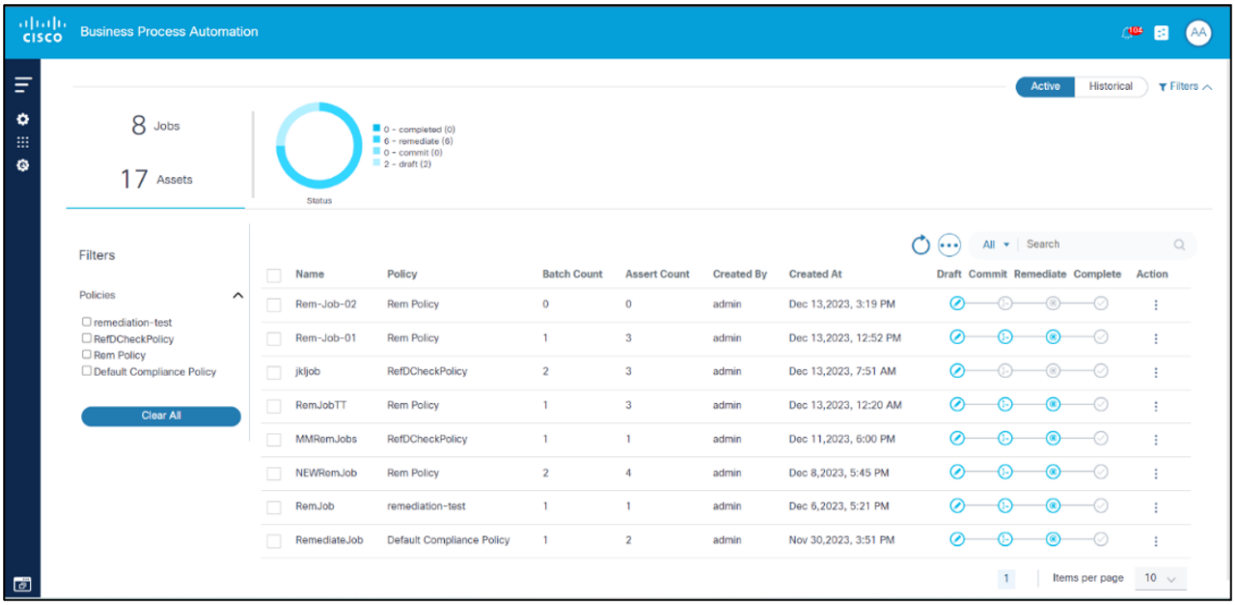
교정 작업

리미디에이션 작업은 운영자가 영향을 받는 자산의 선택된 목록에 대해 리미디에이션 정책을 적용할 수 있도록 지원합니다. 수정 작업은 온디맨드 또는 일정에 따라 실행할 수 있습니다. 런타임에 리미디에이션 워크플로는 디바이스 세부 정보, 컴플라이언스 실행 세부 정보, RefD 프레임워크를 비롯한 다양한 소스에서 데이터를 가져올 수 있습니다.

교정 작업 목록

사용자는 다음과 같이 대시보드에서 생성된 교정 작업을 필터링, 정렬 및 볼 수 있습니다.

- 작업: 생성된 총 작업을 표시합니다.
- 자산: 생성된 총 자산을 표시합니다.
- 상태: 상태별 작업 표시
- 활성 및 기록: 선택 사항에 따라 활성 또는 기록(비활성) 작업을 표시합니다.
- 정책: 정책에 따라 교정 작업을 필터링합니다.
- 주 눈금: 헤더를 클릭하여 정렬할 수 있는 작업의 기본 목록을 표시하며, 페이지 이름이 있는 이름 및 정책별 검색을 포함합니다.
- 작업: 작업이 초안 또는 완료 상태에 있을 때 보관하거나 삭제할 수 있습니다. 실행 중인 작업은 보관하거나 삭제할 수 없습니다.

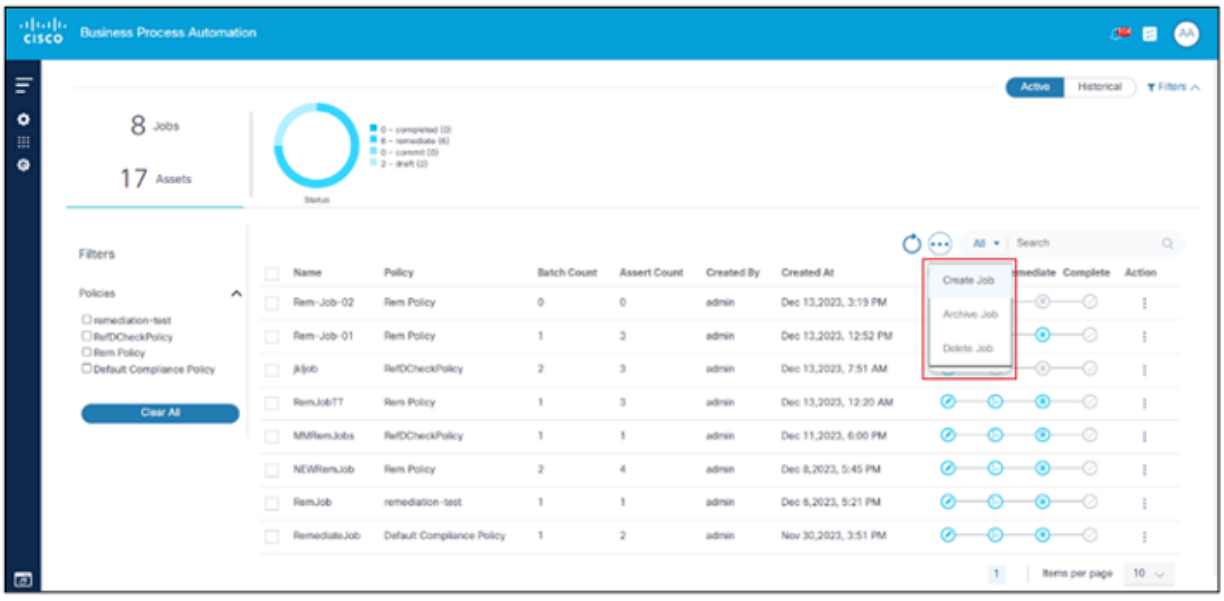


교정 작업 목록

교정 작업 생성 및 편집

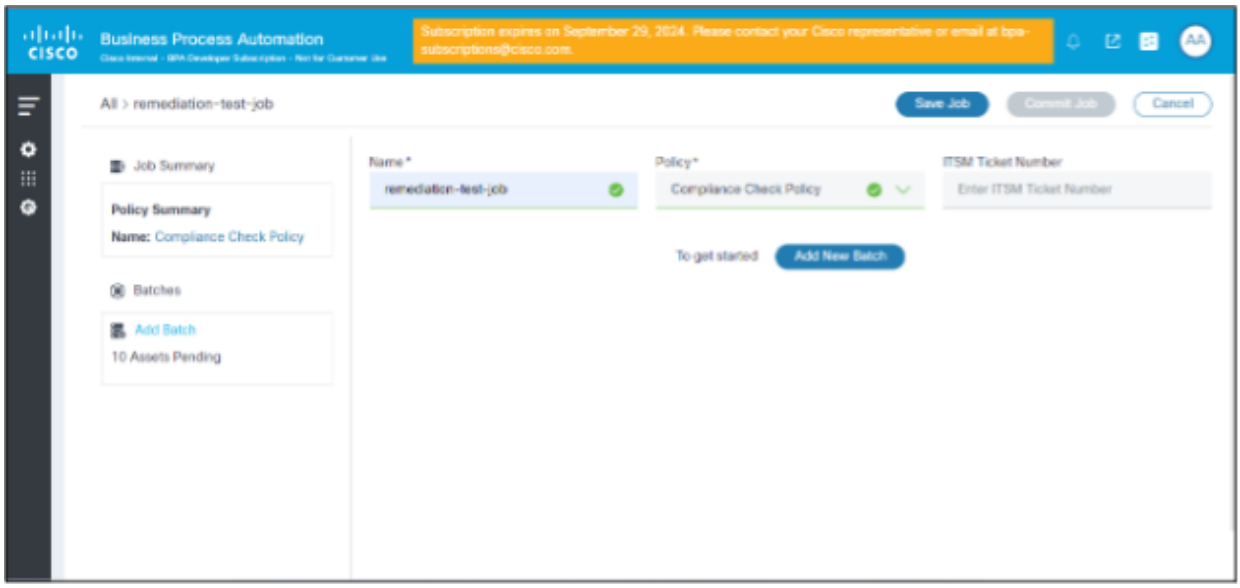
교정 작업은 작업 목록 페이지에서 생성되며 다음 단계를 수행하여 생성할 수 있습니다.

1. 추가 옵션 아이콘 > 작업 생성을 선택합니다. [작업 생성] 페이지가 표시됩니다.



교정 작업 옵션

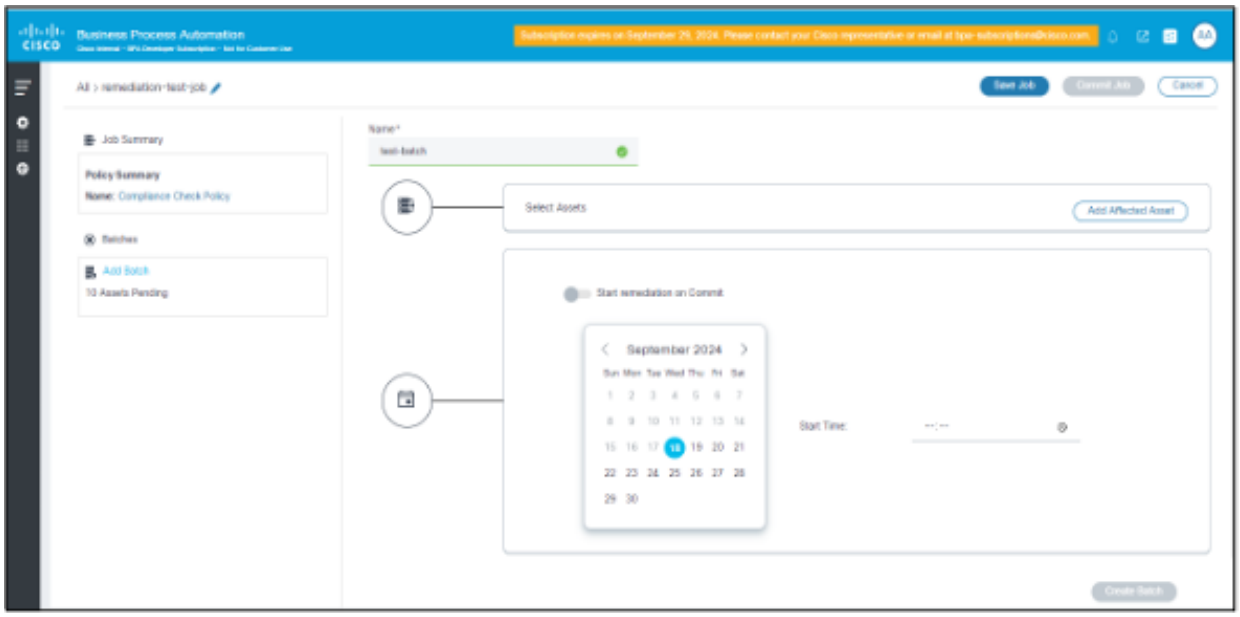
2. 세부 정보를 완료하거나 수정합니다.



교정 작업: 세부사항

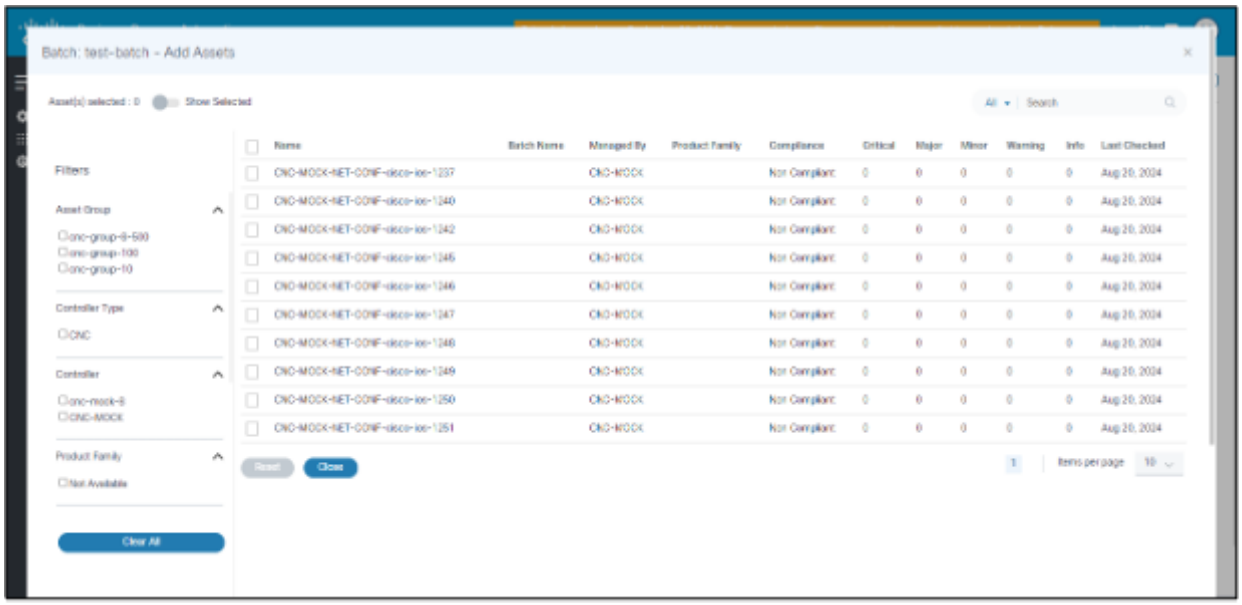
3. 작업 저장을 클릭합니다.

[작업 생성] 페이지에서 작업에 배치를 추가하려면



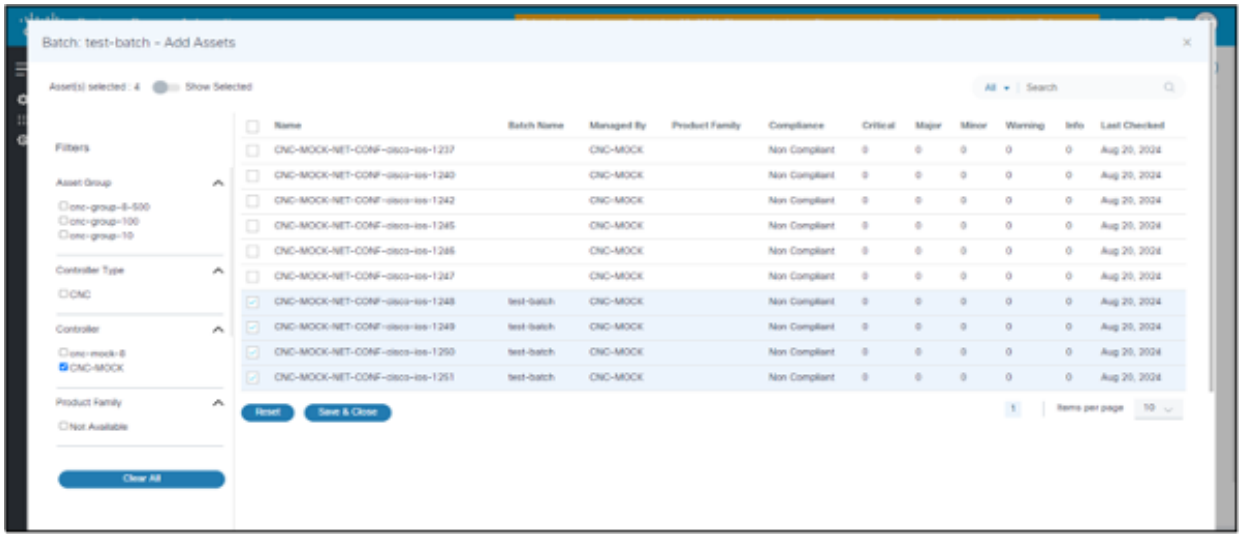
교정 작업: 배치 추가

1. Add New Batch를 클릭합니다.
2. 이름, 영향 받는 자산 상세내역 및 스케줄 상세내역을 입력합니다.
3. Add Affected Assets를 클릭합니다.
4. Assets Details(자산 세부사항) 페이지에서 영향을 받은 자산 목록을 선택하고 Save Job(작업 저장)을 클릭합니다.
5. 컨트롤러 유형, 컨트롤러, 자산 그룹, 제품군을 기준으로 자산을 필터링합니다.
6. 에셋을 선택한 후 저장 및 닫기를 클릭하여 이전 페이지로 돌아갑니다.



교정 작업: 영향을 받는 자산 추가

참고: 사용자는 Affected Assets 페이지에서 필터를 적용할 수 있습니다.



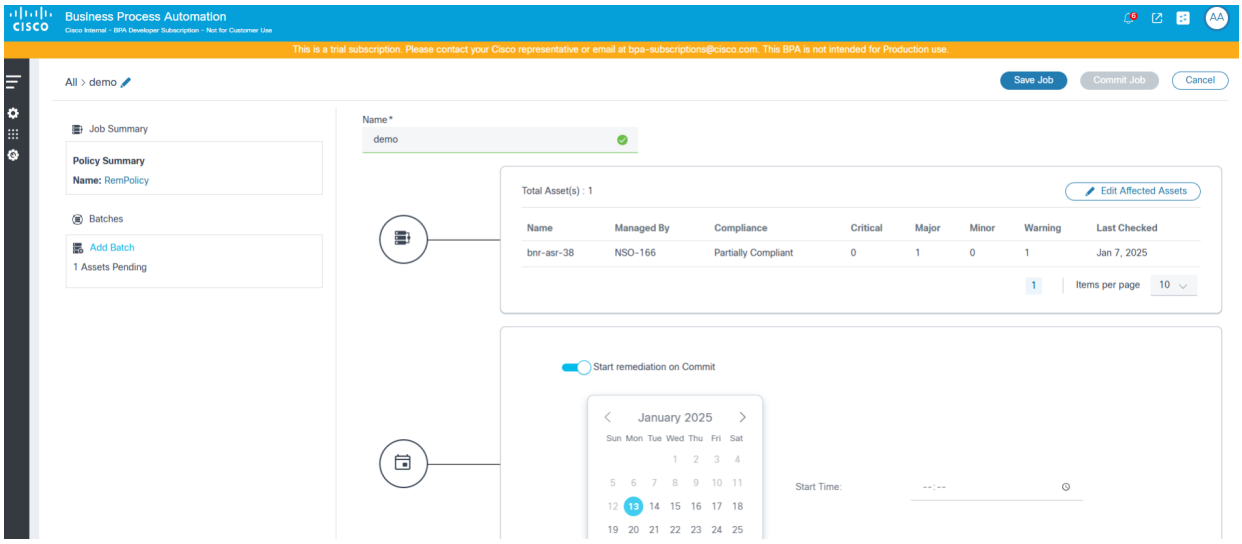
교정 작업: 영향 받는 필터 추가

영향을 받는 자산이 추가되면 저장 시 또는 예약된 미래 시간에 배치를 한 번 실행할 수 있습니다.

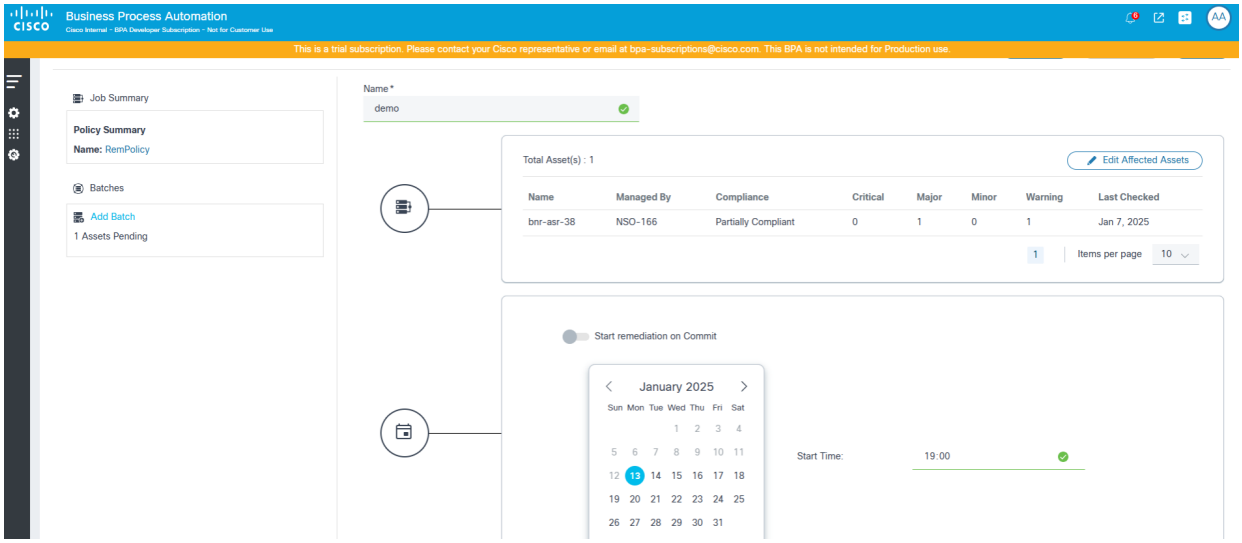
참고: 온디맨드로 작업을 실행하려면 Start remediation on Commit(커밋 시 교정 시작) 토글을 활성화합니다. 사용자가 이 옵션을 선택하면 날짜와 시간이 필요하지 않습니다. 사용자가 One-Time 옵션을 선택하는 경우 작업을 실행하려면 날짜와 시간을 제공해야 합니다.

단일 교정 작업에 둘 이상의 일괄 처리가 있습니다. 각 배치는 커밋 시 또는 예약된 날짜 및 시간에 시작할 수 있습니다.

온커밋(on-commit) 교정 배치는 온디맨드 또는 예약으로 실행할 수 있습니다.



교정 작업: 온디맨드



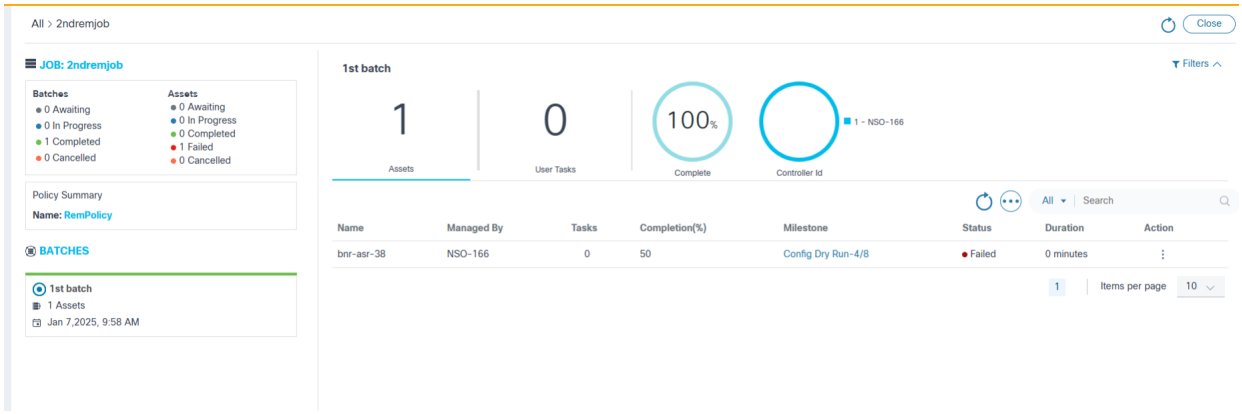
교정 작업: 1회/예약됨

교정 실행: 장치 목록

교정 작업이 커밋되면 실행이 트리거되고, 작업 상태가 [장치 목록] 페이지의 [교정 작업] 아래에 표시됩니다. 사용자는 컨트롤러 ID, 이름, 관리자, 제품군 별로 필터를 적용할 수 있습니다.

- 작업: 배치 및 자산의 상태 세부 정보 및 교정 작업을 실행하도록 선택한 정책의 이름을 표시합니다
- 배치: 현재 교정 작업의 일부로 배치 목록을 표시합니다.
- 자동 새로 고침: 작업이 실행 중 상태인 경우 30초마다 페이지를 자동으로 새로 고치거나, 페이지를 새로 고치거나, 취소를 수행하여 이전 페이지로 돌아갈 수 있는 옵션을 표시합니다
- 배치 레벨 세부 정보: 총 자산 수, 사용자 작업 수, 완료 퍼센트 및 컨트롤러 세부 정보를 포함한 배치 레벨 요약 세부 정보를 표시합니다

- 자산 그리드: 각 자산에 대한 사용자 작업, 완료율 및 현재 중요 시점을 포함하는 자산 그리드 뷰를 표시합니다



교정 실행: 장치 목록

교정 실행: 인라인 사용자 작업 세부 정보

디바이스 목록에서 Tasks 열은 사용자에게 수행할 작업이 있는지 여부를 나타냅니다.

인라인 사용자 작업 세부 정보를 보려면

1. 작업 수를 선택합니다. 사용자 작업 목록 창이 열립니다.
2. 작업을 선택합니다. 사용자 작업 세부 정보 창이 열립니다.

인라인에서 다음 작업을 수행할 수 있습니다.

- 완료
- 재시도
- 취소

교정 실행: 인라인 중요 시점 세부 정보

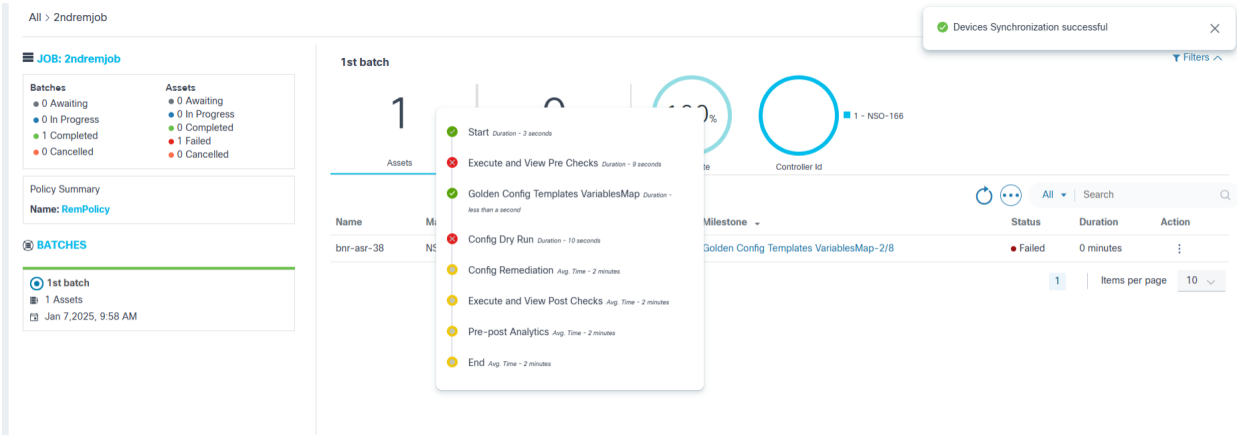
디바이스 목록에서 Milestone 열은 지정된 디바이스의 교정에 관련된 현재 이정표를 나타냅니다.

인라인 중요 시점 세부 정보를 보려면 열을 선택합니다. 이정표 상세내역 창이 열립니다.

이정표에 대해 사용할 수 있는 상태는 다음과 같습니다.

- 시작되지 않음
- 실행 중

- 완료됨
- 실패



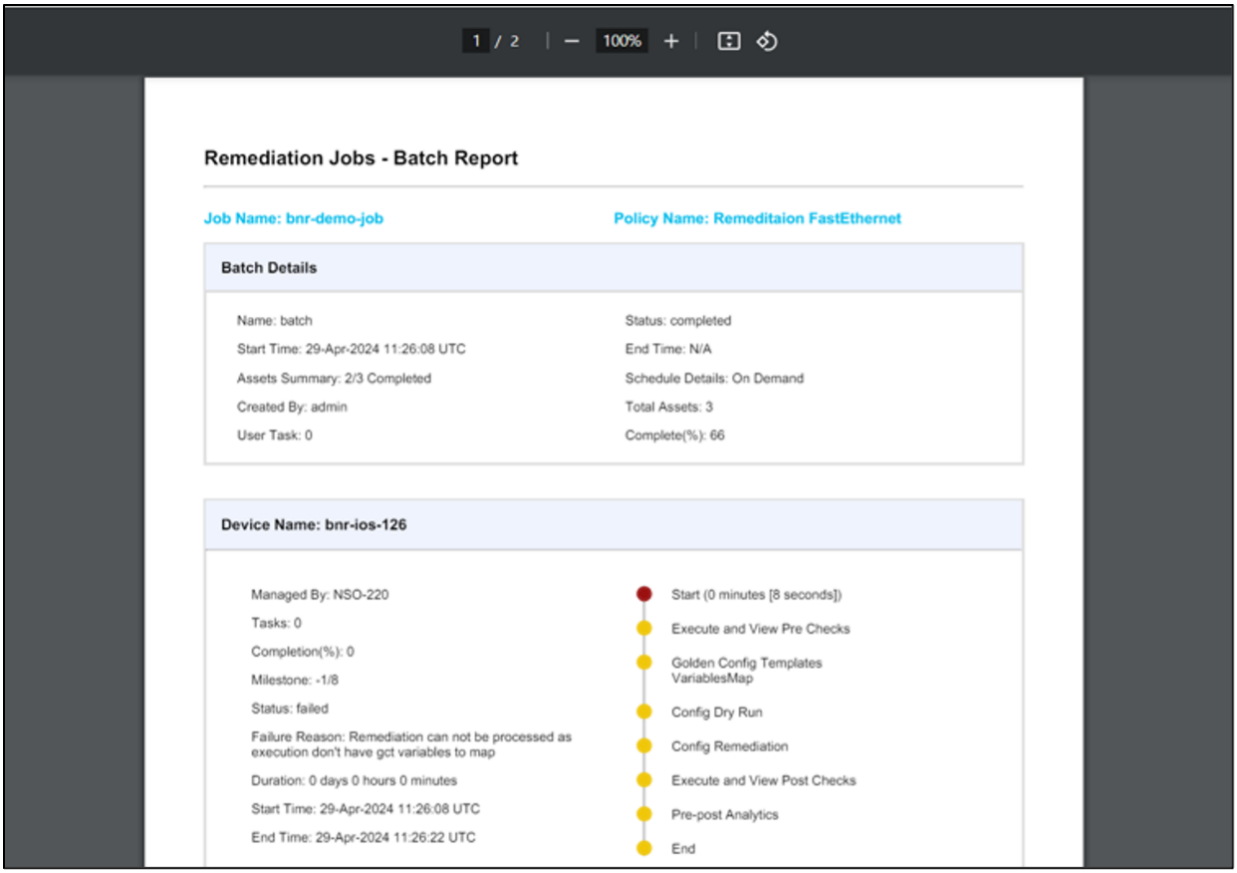
교정 실행: 인라인 중요 시점 세부 정보

교정 실행: 배치 요약 PDF 보고서 생성 및 다운로드

배치 요약은 생성 및 다운로드할 수 있습니다.

일괄 처리당 요약 보고서를 PDF로 다운로드하려면 다음을 수행합니다.

1. More Options(추가 옵션) 아이콘 > Generate Report(보고서 생성)를 선택합니다. 시스템에서 내부적으로 보고서가 준비되었는지 확인합니다. 보고서가 준비되면 보고서 다운로드 옵션이 활성화됩니다.
2. More Options(추가 옵션) 아이콘 > Download Report(보고서 다운로드)를 선택합니다. PDF 다운로드



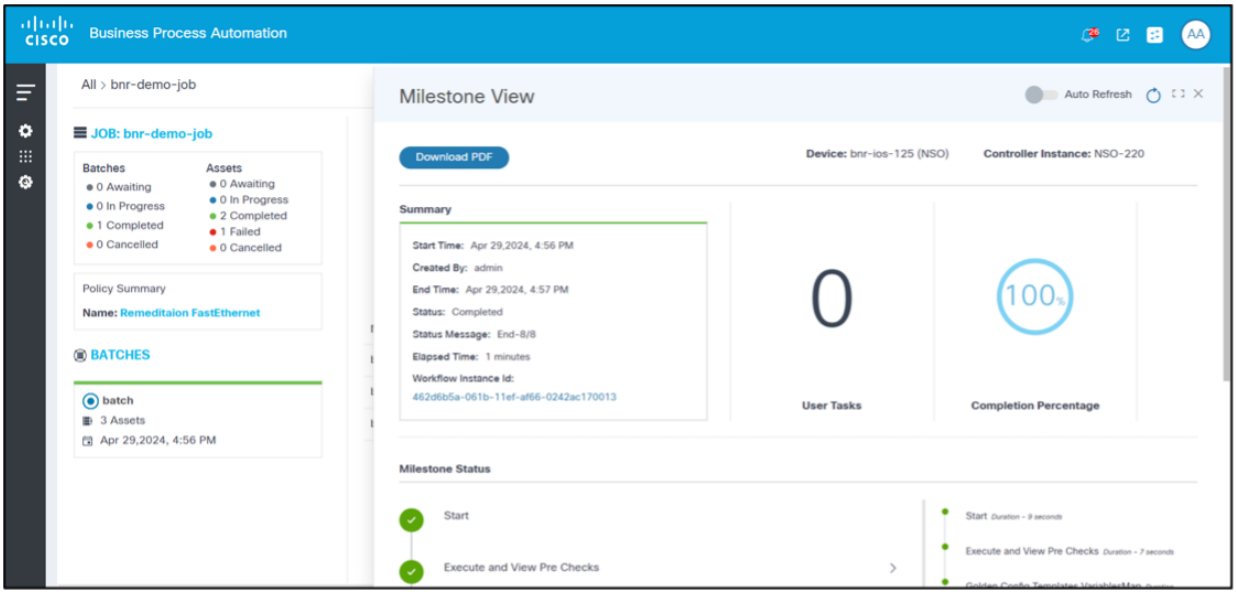
배치 요약 보고서 PDF

교정 작업 배치 보고서에는 작업 이름, 배치명, 시작 및 종료 시간, 총 자산, 전체 상태 등 교정 배치의 요약을 제공하는 배치 세부 정보 섹션이 포함되어 있습니다. 그 다음에는 디바이스 이름, 디바이스별 교정 상태, 타임라인, 기간 및 이정표 목록, 상태가 포함된 Device Detail 섹션(디바이스당 섹션 하나)이 표시됩니다.

교정 실행: 디바이스 세부 정보

이정표에 대한 장비 세부사항을 보려면 Device Details(장비 세부사항) 페이지를 선택합니다. 이정표 보기 페이지가 표시됩니다.

완료된 주요 이정표의 명령 출력을 포함하여 세부 이정표 상태의 지정된 디바이스에 대한 교정 요약이 표시됩니다. 예를 들어, process template 명령 출력, GCT dry run 출력 및 분석 차이 출력 내용을 볼 수 있습니다.



교정 실행: 중요 시점 보기

교정 실행: 장비 세부사항 - 마일스톤 보고서

이정표 보고서를 보려면

1. Device Details(디바이스 세부사항) 페이지를 선택합니다. 이정표 보기 페이지가 표시됩니다.
2. PDF 다운로드를 클릭합니다. 이정표 보기 보고서는 아래와 같이 생성 및 다운로드됩니다.

이 보고서는 선택한 디바이스 교정에 대한 보다 정교한 이정표 세부사항 및 해당 콘텐츠를 제공합니다.

Device Name: bnr-asr-38

Milestones

Start

Milestone:	Start	**Execution Start:**	Tue Jan 07 2025 04:28:29 +0000 (GMT)
Status:	Complete	**Completed On:**	Tue Jan 07 2025 04:28:32 +0000 (GMT)

Execute and View Pre Checks

Milestone:	Execute and View Pre Checks	**Execution Start:**	Tue Jan 07 2025 04:28:33 +0000 (GMT)
Status:	Failed	**Completed On:**	Tue Jan 07 2025 04:28:42 +0000 (GMT)

Template id : **nso_prepostFail** **Device Name :** **bnr-asr-38** **Commands Evaluation Result :** **Fail**

dir harddisk: location all | include free Rules Evaluation Result : **Pass**

Execution Start Time: 01/07/25, 04:28:37:498 AM GMT - End Time: 01/07/25, 04:28:39:589 AM GMT- Duration: 2091ms

#Rule : **1** **Operation :** **Contains** **Result :** **Pass**

Rule : **Invalid input detected**

설정: 블록 및 규칙

블록의 기능

컨피그레이션 블록은 네트워크 관리 시스템에서 컴플라이언스 정책을 생성하고 시행하기 위한 필수 요소입니다. 인터페이스, 라우터 BGP(Border Gateway Protocol) 등에 대한 디바이스 CLI 컨피그레이션을 나타냅니다. 다음은 컨피그레이션 블록의 주요 기능입니다.

- 모듈 구조: 컨피그레이션 블록에서는 모듈형 정책 생성이 가능하므로 관리자가 디바이스 컨피그레이션의 개별 섹션을 독립적으로 정의하고 관리할 수 있습니다. 이러한 모듈 구조는 규정 준수 정책의 업데이트 및 유지 관리 프로세스를 간소화합니다.
- 세분화: 관리자는 디바이스 구성을 더 작고 관리하기 쉬운 부분으로 분할함으로써 정확한 컴플라이언스 검사를 수행하고 특정 표준을 적용할 수 있습니다. 이렇게 하면 디바이스 컨피그레이션의 모든 부분이 필요한 정책을 따르게 됩니다.
- 재사용 가능성: 컨피그레이션 블록이 정의되면 여러 컴플라이언스 정책 및 디바이스에서 재사용할 수 있습니다. 이러한 재사용 가능성을 통해 이중화가 줄어들고 컨피그레이션 관리의 일관성이 보장됩니다.
- 정적 구성 블록: 고정 컨피그레이션 블록은 변수가 없는 원시 디바이스 컨피그레이션을 나타냅니다.

  예: 다음 블록은 TwentyFiveGigE0/0/0/31 인터페이스에서 규정 준수 확인을 실행하는 데 사용할 수 있습니다

```
interface TwentyFiveGigE0/0/0/31
  description au01-inv-5g-08 enp94s0f0
  no shutdown
  load-interval 30
  l2transport
```

- 동적 구성 블록: 동적 컨피그레이션 블록은 더 적응성 있고 재사용이 가능한 변수를 포함하는 디바이스 컨피그레이션을 나타냅니다. 이러한 블록은 TTP 템플릿처럼 작동하여 디바이스 컨피그레이션에 적용하고 변수에 대한 값을 가져옵니다. 이러한 변수를 검증하기 위해 규칙에 조건을 추가할 수 있습니다. TTP에 대한 자세한 내용은 https://ttp.readthedocs.io/en/latest/Overview.html을 참조하십시오.

  예: 다음 블록은 모든 TwentyFiveGigE 인터페이스에서 컴플라이언스 검사를 실행하는 데 사용할 수 있습니다

```
interface TwentyFiveGigE{{INTERFACE_ID}}
  description {{DESCRIPTION}}
```

```
        no shutdown
        load-interval {{LOAD_INTERVAL}}
        l2transport
```

하위 계층이 있는 동적 구성 블록: 이 블록은 동적 컨피그레이션 블록과 같은 기능을 하며 여러 계층이 있는 디바이스 컨피그레이션에서 값을 검색하는 데 사용됩니다.

예: 다음 예에서는 디바이스 컨피그레이션 및 계층적 구조에서 값을 검색하는 데 사용되는 해당 동적 블록을 보여 줍니다.

계층 구조를 가진 장치 구성:

```
router bgp 12.34
address-family ipv4 unicast
  router-id 1.1.1.X
!
vrf CT2S2
  rd 102:103
  !
  neighbor 10.1.102.XXX
  remote-as 102.XXX
  address-family ipv4 unicast
    send-community-ebgp
    route-policy vCE102-link1.102 in
    route-policy vCE102-link1.102 out
  !
  !
  neighbor 10.2.102.XXX
  remote-as 102.XXX
  address-family ipv4 unicast
    route-policy vCE102-link2.102 in
    route-policy vCE102-link2.102 out
  !
  !
vrf AS65000
  rd 102:XXX
  !
  neighbor 10.1.37.X
  remote-as 65000
  address-family ipv4 labeled-unicast
    route-policy PASS-ALL in
    route-policy PASS-ALL out
```

위 컨피그레이션을 구문 분석할 동적 블록 컨피그레이션입니다.

```
router bgp {{ ASN }}




address-family ipv4 unicast {{ _start_ }}
  router-id {{ bgp_rid }}









vrf {{ vrf }}
  rd {{ rd }}









  neighbor {{ neighbor }}
  remote-as {{ neighbor_asn }}









  address-family ipv4 unicast {{ _start_ }}
    send-community-ebgp {{ send_community_ebgp }}
    route-policy {{ RPL_IN }} in
    route-policy {{ RPL_OUT }} out
```

규칙의 기능

규칙을 사용하면 구성 블록에 있는 변수에 대해 검증할 조건을 정의할 수 있습니다. 실행 과정에서 규정 준수 엔진은 디바이스 컨피그레이션을 구문 분석하고, 디바이스 블록 인스턴스의 일치하는 인스턴스를 찾고, 라인에서 값을 읽고, 규칙에 정의된 조건을 값에 대해 실행합니다. 컨피그레이션 라인에 위반이 있는지 여부에 관계없이 결과는 대시보드에 표시하기 위해 저장됩니다.

구성 규칙은 이제 블록 생성 라이프사이클의 일부입니다. 따라서 규칙을 볼 수 있는 별도의 페이지가 없습니다. 해당 block create 또는 update 페이지에서 규칙을 나열하고 생성하고 업데이트할 수 있습니다.

CnR 프레임워크에서 규칙은 지정된 조건에 대해 컨피그레이션을 검증하는 데 중요한 역할을 합니다. 이 섹션에서는 시스템 내에서 규칙이 어떻게 통합되고 관리되는지에 대한 개요를 제공합니다.

- 목적: 규칙을 통해 사용자는 구성 블록 내에 있는 변수를 검증하는 데 사용되는 조건을 정의할 수 있습니다
- 실행 프로세스:
    - 컴플라이언스 엔진이 디바이스 컨피그레이션을 구문 분석합니다
    - 디바이스 블록 인스턴스의 일치하는 인스턴스 식별
    - 구성 행에서 값을 추출합니다.
    - 규칙에 정의된 조건을 이러한 값에 적용합니다
    - 위반을 나타내는 결과가 대시보드에 저장 및 표시됩니다

블록 라이프사이클과의 통합

- 라이프사이클 통합: 이제 구성 규칙이 블록 생성 주기에 필수적입니다.
- 관리:
    - 규칙은 블록 생성 또는 업데이트에 사용되는 페이지 내에서 직접 나열, 생성 및 업데이트됩니다
    - 별도의 전용 페이지 없이 규칙을 조회하여 블록 라이프사이클 내에서 효율적으로 관리할 수 있습니다.

이러한 통합으로 컴플라이언스 검사가 컨피그레이션 관리 프로세스에 원활하게 통합되므로 사전 정의된 규칙에 대해 디바이스 컨피그레이션을 효율적으로 모니터링하고 관리할 수 있습니다.

목록 블록

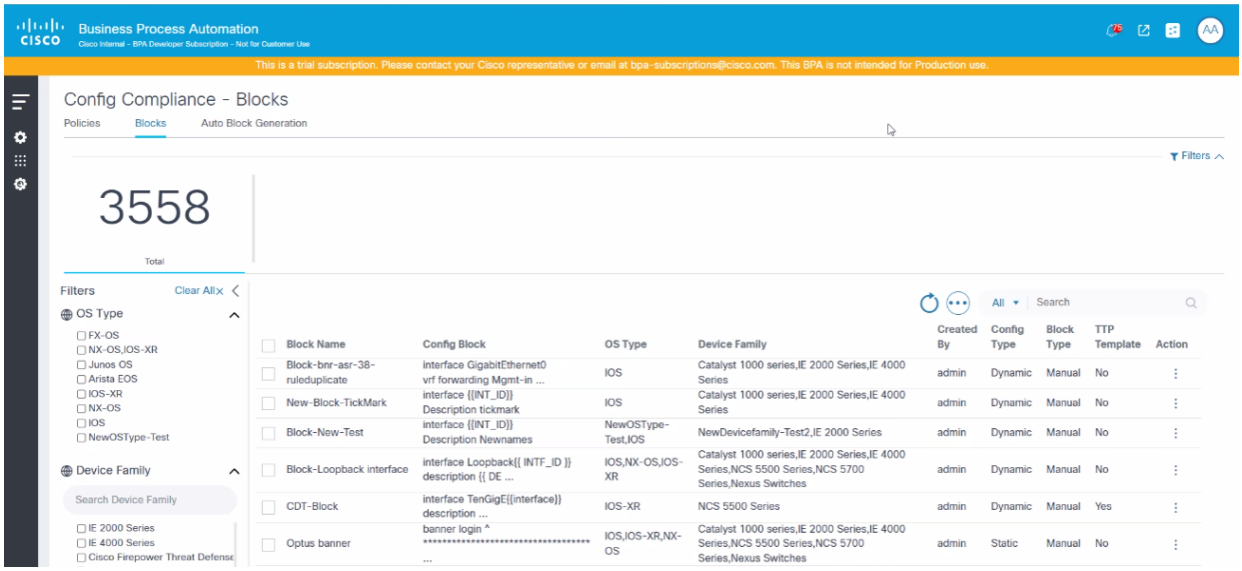
Blocks(블록) 페이지에는 모든 컨피그레이션 블록이 나열되며 블록을 생성, 추가, 수정, 삭제, 가져오기 및 내보내는 작업이 제공됩니다. 사용자는 블록 세부사항을 필터링, 정렬 및 볼 수 있습니다.

기능 블록 세부 정보

- 총 개수: 생성된 총 블록 수를 표시합니다
- 필터 옵션:
    - OS 유형 및 장치 제품군: 사용자가 선택한 기준에 따라 블록을 필터링할 수 있습니다.
- 주 눈금:
    - 기본 블록 목록을 표시합니다.

- 사용자는 열 헤더를 클릭하여 목록을 정렬할 수 있습니다
- 사용자가 모든 속성 또는 특히 블록 이름으로 검색할 수 있는 검색 기능이 포함되어 있습니다.
- 목록을 쉽게 탐색할 수 있도록 페이지 번호 매기기 지원

- 작업:
  - 편집: 사용자는 기존 블록을 수정할 수 있음
  - 삭제: 사용자는 목록에서 블록을 제거할 수 있습니다



컨피그레이션 블록 목록

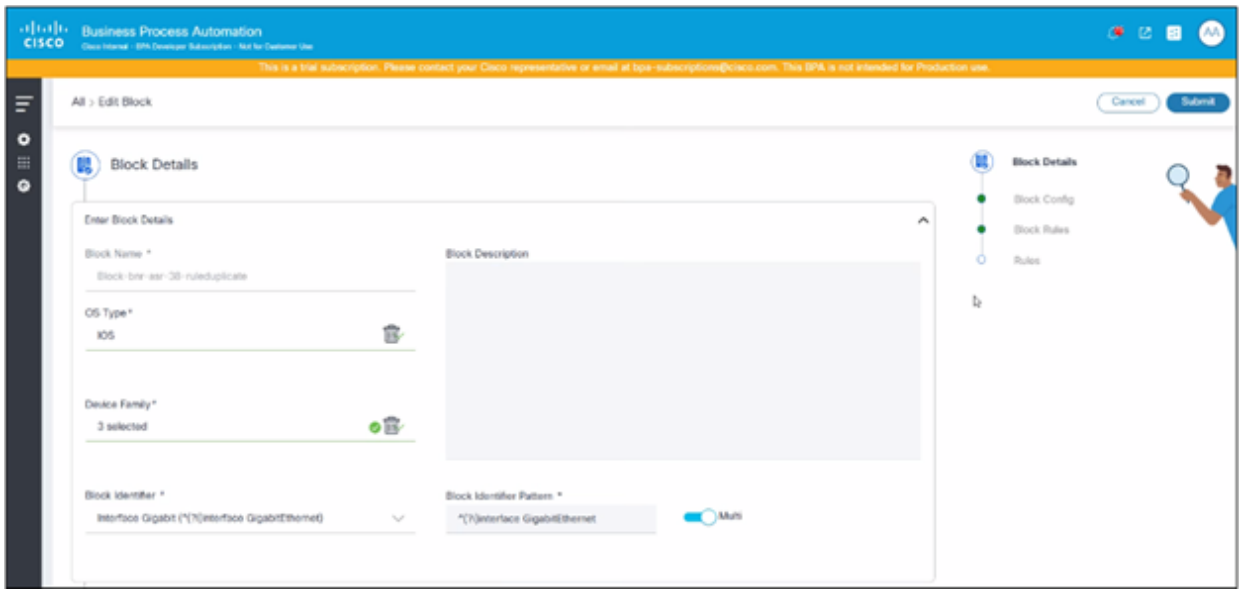
블록 및 규칙 추가 또는 편집

Add or Edit Block(블록 추가 또는 수정) 페이지는 블록에 대한 필수 정보를 캡처하고 관리하도록 설계되었습니다. 이 페이지에서는 다음 섹션을 간략하게 설명합니다.

- 기본 차단 세부 정보:

  Basic Details(기본 세부사항) 섹션에는 다음이 포함됩니다.

  - 블록 이름: 블록의 지정된 이름
  - 설명: 블록의 목적 또는 기능에 대한 간략한 개요 또는 설명
  - OS 유형: 블록과 연결된 운영 체제 유형
  - 장치 제품군: 블록과 호환되는 디바이스 범주 또는 그룹
  - 블록 식별자 선택: 블록의 고유 식별자를 선택하기 위한 옵션
  - 블록 식별자 세부 정보 추가 또는 편집: 적합한 블록 식별자가 없는 경우 사용자는 동일한 필드를 사용하여 다음 블록 식별자 세부 정보를 추가하거나 편집할 수 있습니다.
    - 블록 식별자 이름: 블록 식별자에 지정된 특정 이름
    - 패턴: 블록 식별자가 따르는 패턴 또는 형식
    - 다중: 컨피그레이션 블록을 다중 라인 컨피그레이션으로 처리할지 여부를 나타내려면 전환합니다.

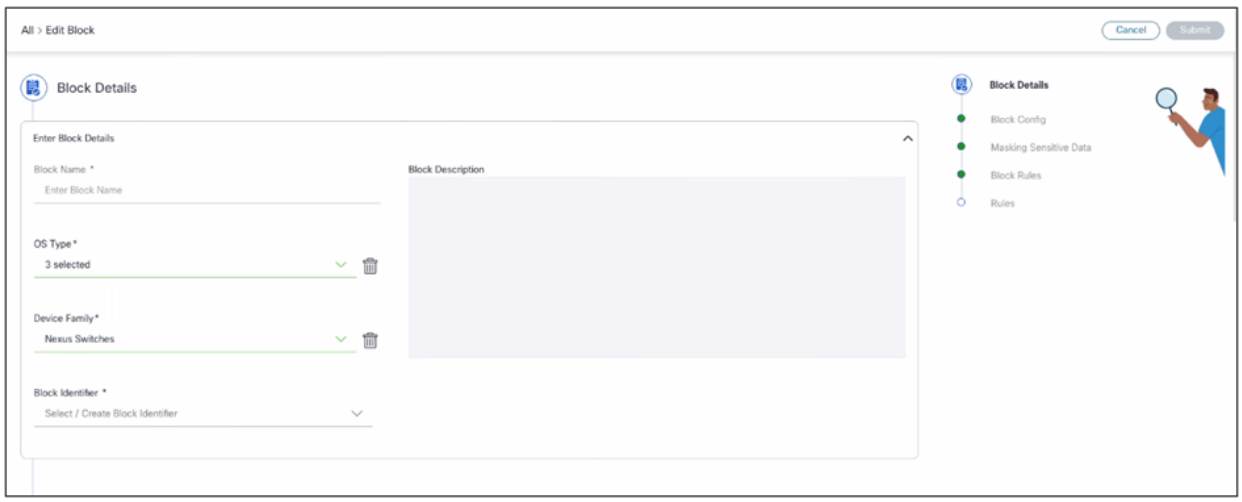


블록 추가 또는 편집 - 블록 세부사항

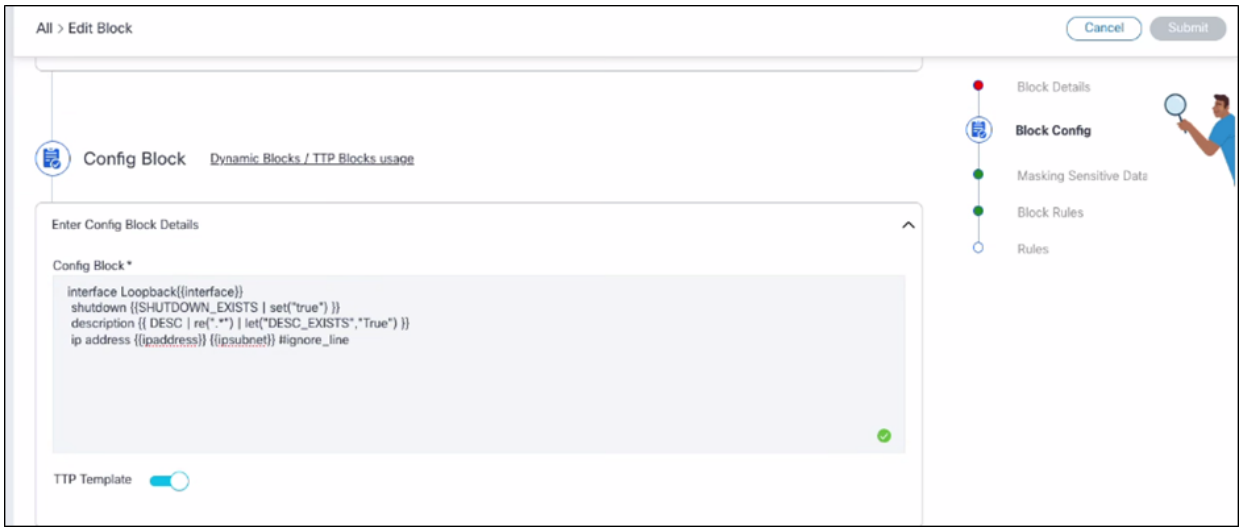
- 블록 구성:

Block Config(컨피그레이션 차단) 섹션에는 다음이 포함됩니다.

- 구성 블록: 서로 다른 변수를 포함하는 디바이스의 컨피그레이션을 나타냅니다. 이 컨피그레이션에서는 시스템 내에서 디바이스를 설정하고 관리하는 방법을 간략하게 설명합니다.
- TTP 템플릿: 블록이 TTP(Template Transformation Protocol) 템플릿으로 지정되었는지 여부를 나타내며, 이는 여러 디바이스에서 컨피그레이션을 변환 또는 표준화하기 위한 템플릿으로 사용되는 블록을 식별하는 데 도움이 됩니다.



차단 세부 정보



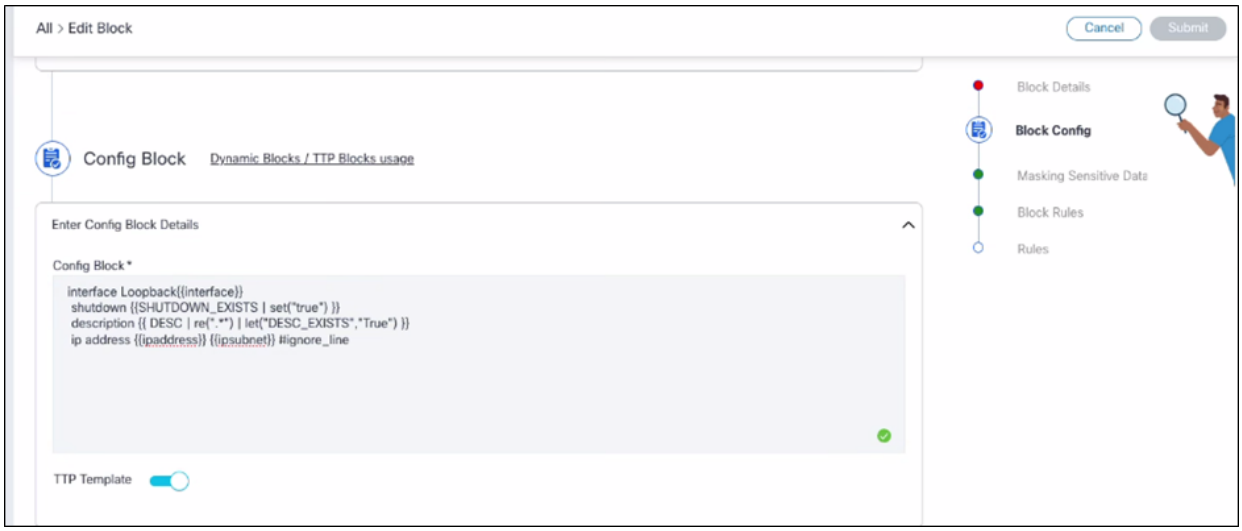
구성 차단

무시 라인 구문 사용

Ignore Line Syntax(라인 무시 구문)를 사용하면 사용자가 특정 구성 라인의 끝에 코멘트를 추가하여 해당 라인의 규정 준수 확인 또는 위반을 건너뛰도록 시스템에 지시할 수 있습니다. 이렇게 하면 보고서 또는 대시보드에서 행이 위반으로 표시되지 않습니다.

Ignore Line Syntax를 사용하려면 다음 단계를 완료합니다.

1. 규정 준수 검사에서 제외할 구성 행을 찾습니다(예: ip 주소).



줄 구문 무시

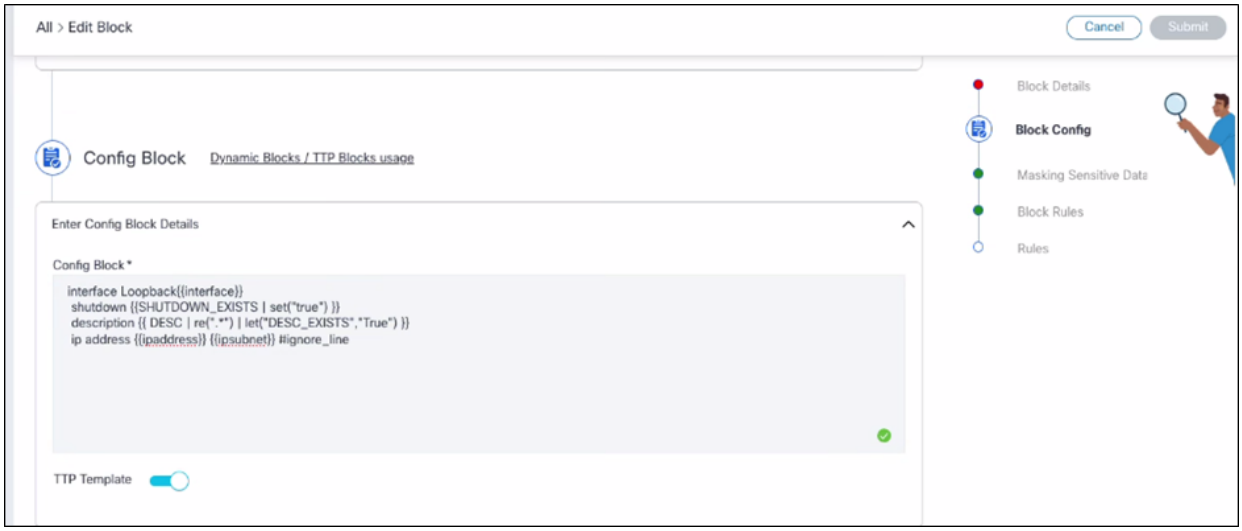
2. 해당 줄의 끝에 주석 구문 "#ignore_line"를 사용하여 줄을 추가합니다. 예: ip 주소 {{ipAddress}} {{ipSubnet}} #ignore_line

위반 제기

블록 구성의 이 TTP(Template Text Parser) 기능은 특정 행이 있는 경우 위반이 발생해야 하는지 여부를 나타내는 데 사용할 수 있습니다.

TTP 기능을 사용하려면 다음 단계를 완료하십시오.

1. 블록 생성 또는 편집 페이지의 블록 구성 섹션에서 제어할 구성 라인을 찾습니다.
2. 다음과 같이 set 또는 let 명령을 사용하여 TTP 변수를 정의합니다.
   - config line shutdown이 존재하는 경우 set 명령을 사용하여 다음과 같이 변수를 정의합니다.
     셧다운 | {{SHUTDOWN_FLAG | set("true")}"
   - 사용자에게 설명 {{DESC}}과(와) 같은 config 라인에 기존 변수가 있는 경우 다음과 같이 let 명령을 사용합니다.
     설명 {{ DESC | re(".*") | let("DESC_EXISTS", "True") }}
3. 규칙에서 이러한 변수(위의 샘플에 SHUTDOWN_FLAG 또는 DESC_EXISTS)를 사용하여 위반을 제기합니다.



위반 제기

효과:

디바이스 컨피그레이션에서 "shutdown" 또는 "description config" 행을 사용할 수 있는 경우 대시보드 페이지에 위반이 표시됩니다. 위반의 심각도는 규칙 생성 시 선택한 사항에 따라 달라집니다.

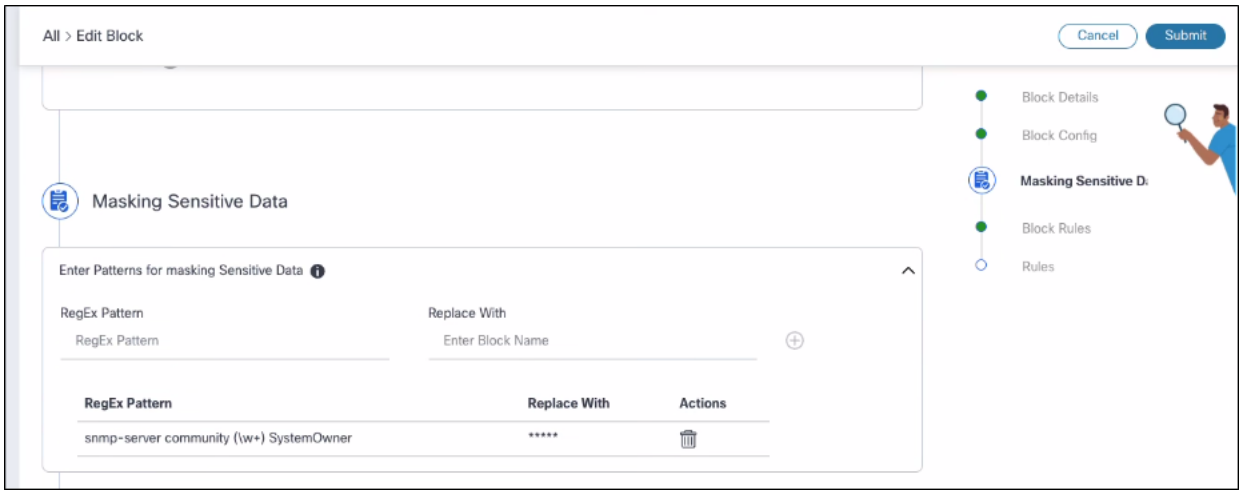
- 민감한 데이터 마스크:

Mask Sensitive Data는 사용자가 디바이스 컨피그레이션에서 암호 또는 키와 같은 민감한 정보를 식별하고 마스킹하기 위해 정규식을 사용하여 패턴을 정의할 수 있는 기능입니다. 이렇게 하면 일

치하는 데이터를 지정된 마스크(예: "***")로 대체하여 중요한 데이터가 위반 보기 또는 교정 컨피그레이션 차이에서 표시되지 않습니다.

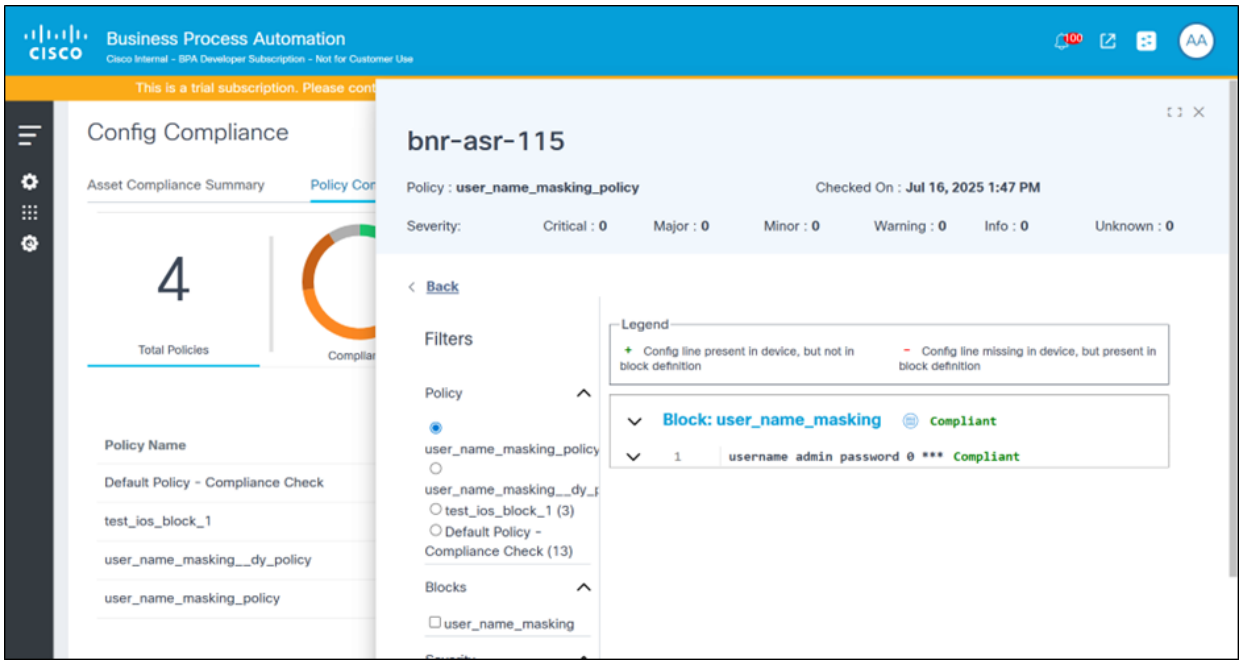
민감한 데이터를 마스킹하는 절차는 다음과 같습니다.

1. Mask Sensitive Data 섹션에서 다음을 수행합니다.
   - 민감한 데이터를 식별하기 위한 여러 정규식(regex) 패턴 추가
   - 일치 데이터(예: "")를 마스크 처리하려면 대체 문자열을 지정합니다. 예를 들어, Regex 패턴은 암호로 채울 수 있으며(암호로 시작하는 텍스트 및 단어 뒤에 오는 텍스트 일치) 대체 문자열은 다음과 같아야 합니다.
2. 필요한 만큼 regex 패턴을 추가합니다. 격자선 형식으로 표시됩니다.



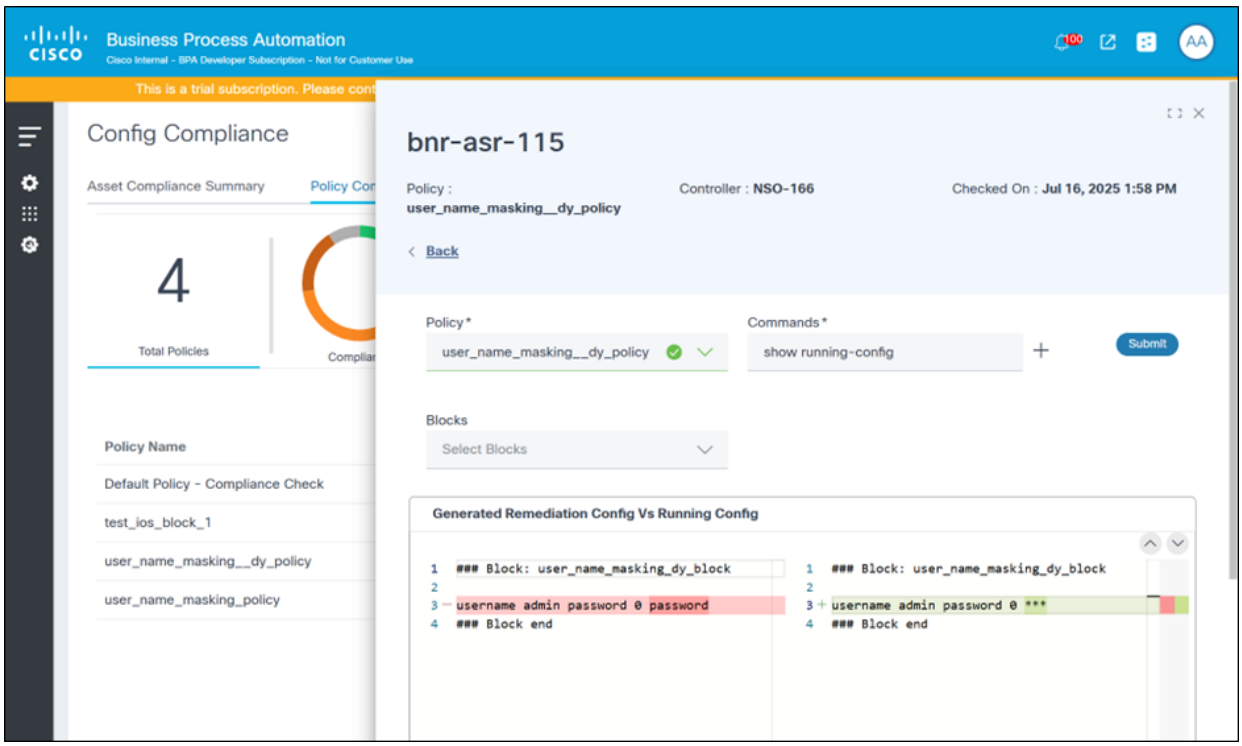
민감한 데이터 마스크

3. 더 이상 필요하지 않으면 목록에서 패턴을 삭제합니다.
4. 시스템은 정규식을 사용하여 일치하는 중요한 디바이스 컨피그레이션 데이터를 찾고 이를 지정된 마스크(예: "***")로 대체합니다. 이 마스킹은 다음 페이지에서 사용됩니다.
   - Compliance dashboard(규정준수 대시보드) > Affected Assets(영향을 받는 자산) > View violations(위반 보기) 페이지: UI에 표시되는 컨피그레이션 데이터 및 이러한 위반 세부사항을 기반으로 생성된 자산 준수 보고서



[위반 보기] 페이지에서 민감한 데이터 마스크

- Compliance dashboard(규정준수 대시보드) > View Remediation Config(교정 구성 보기) > View Remediation Diff(교정 차이 보기) 페이지: 디바이스 컨피그레이션 데이터는 블록의 마스크 설정에 따라 마스킹된 민감한 데이터를 표시합니다

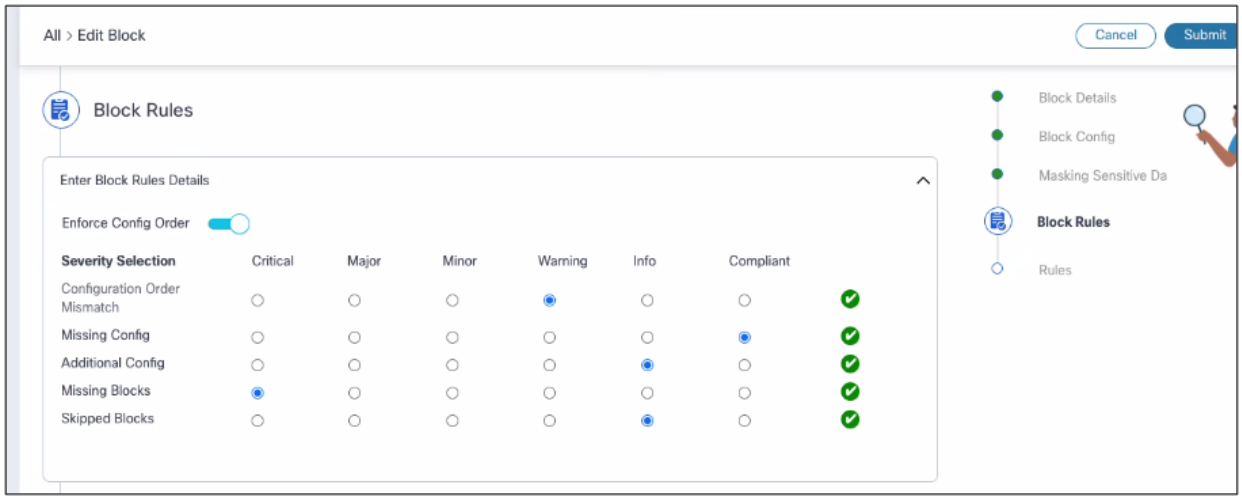


교정 diff 페이지에서 민감한 데이터 마스크

- 차단 규칙(심각도 선택):

  Block Rules 섹션에는 다음이 포함됩니다.

- 컨피그레이션 순서 적용: 규정 준수 확인 과정에서 구성 행이 올바른 순서로 표시되는지 확인합니다. 규정 준수 엔진은 예상 주문에 대해 구성 라인의 순서를 확인합니다.
- 심각도 선택: 사용자가 블록 내의 위반에 심각도 수준을 할당할 수 있습니다. 심각도 수준은 규정 준수 문제의 우선 순위를 정하고 효과적으로 관리하는 데 도움이 됩니다.
- 구성 순서 불일치: 컨피그레이션 라인 순서의 불일치를 식별하고 디바이스 컨피그레이션 라인 순서가 예상 주문과 일치하지 않을 경우 알림을 제공합니다.
- 누락된 구성:
  - 누락된 컨피그레이션 라인 탐지
  - 디바이스 컨피그레이션에 없는 예상 컨피그레이션 라인을 강조 표시합니다
  - 전체 디바이스 컨피그레이션 블록이 누락되었거나 정의된 블록 컨피그레이션과 일치하지 않는지 확인합니다
- 추가 구성:
  - 예기치 않은 컨피그레이션 행을 식별합니다.
  - 디바이스 컨피그레이션에 있지만 블록 컨피그레이션에 따라 예상하지 못한 컨피그레이션 라인을 표시합니다
- 건너뛴 블록:
  - 검사되지 않은 컨피그레이션 블록을 나타냅니다
  - 블록이 지정된 필터 조건을 충족하지 않으면 건너뜁니다



블록-블록 규칙 추가 또는 편집

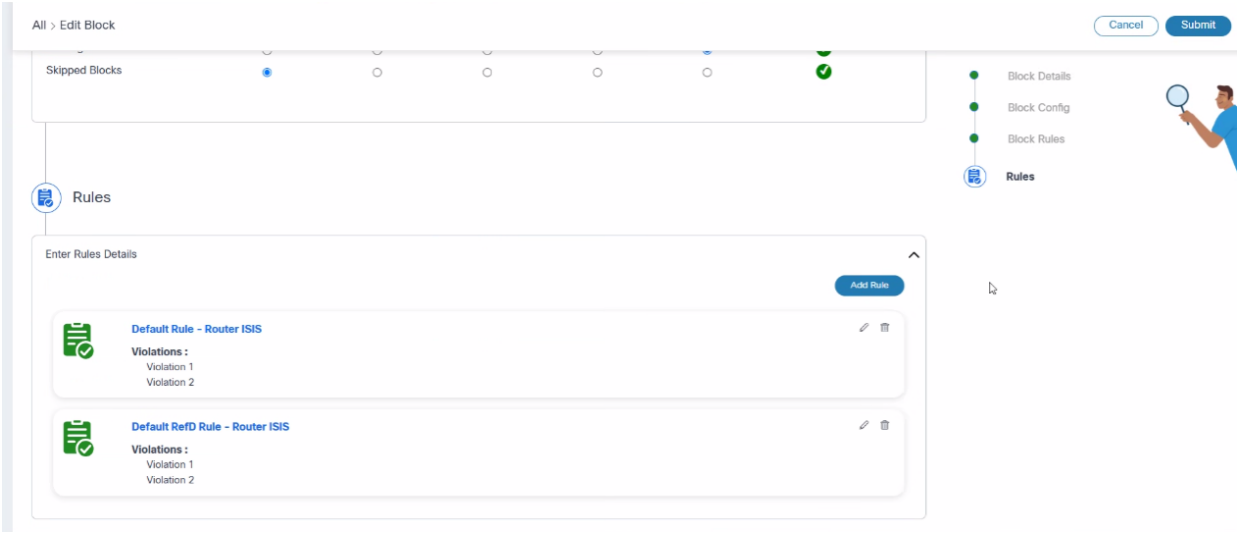
규칙 관리

CnR 프레임워크에서 사용자는 "Add or Edit Blocks(블록 추가 또는 수정)" 인터페이스를 통해 블록 규칙을 관리할 수 있습니다. 이 기능은 아래 섹션과 같이 구성됩니다.

✎ 참고: 사용자가 특정 블록 레벨 위반을 제기하지 않으려는 경우 심각도 레벨 "Compliant"를 선택할 수 있습니다.

- 규칙 컨피그레이션:
  - 사용자는 규정 준수 엔진이 구성을 검증하는 데 사용하는 규칙을 설정하고 관리할 수 있

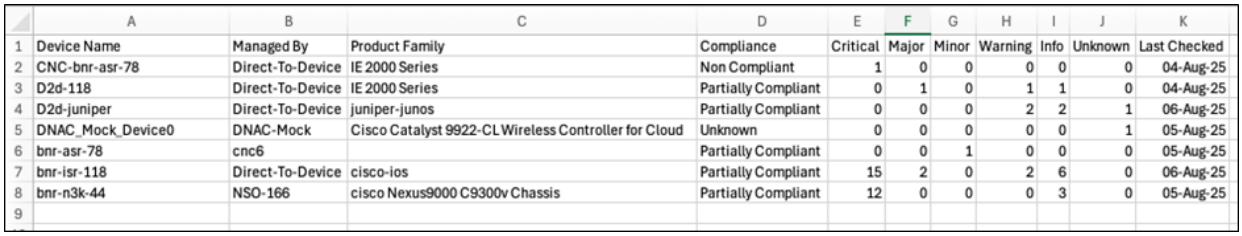
습니다
    - 사용자는 필요에 따라 규칙을 생성, 수정 또는 삭제할 수 있습니다
- 규칙 목록:
    - 생성된 모든 규칙의 포괄적인 목록을 제공하여 세부 사항을 파악할 수 있습니다.
    - 사용자는 기존 규칙을 수정하거나 더 이상 필요하지 않은 규칙을 삭제할 수 있습니다



구성 블록 추가 및 편집

규칙 세부사항 추가 또는 수정

- 규칙 이름:
    - 식별을 위해 규칙에 고유한 이름 할당
    - 이 필드는 각 규칙을 명확하게 인식할 수 있도록 하는 필수 필드입니다
- 기본 규칙:
    - 규칙을 기본 규칙으로 설정할지 여부를 지정합니다
    - 사용자는 이 설정을 사용하여 규칙을 규정 준수 프레임워크 내에서 기본값으로 설정할 수 있습니다
- 설명:
    - 규칙에 대한 추가 컨텍스트 또는 정보를 제공합니다.
    - 이 필드는 선택 사항이지만 설명서와 명확성을 위해 유용할 수 있습니다
- 위반:
    - 규칙과 관련된 위반 목록을 관리합니다.
    - 사용자는 필요에 따라 위반을 추가, 수정 또는 삭제할 수 있습니다



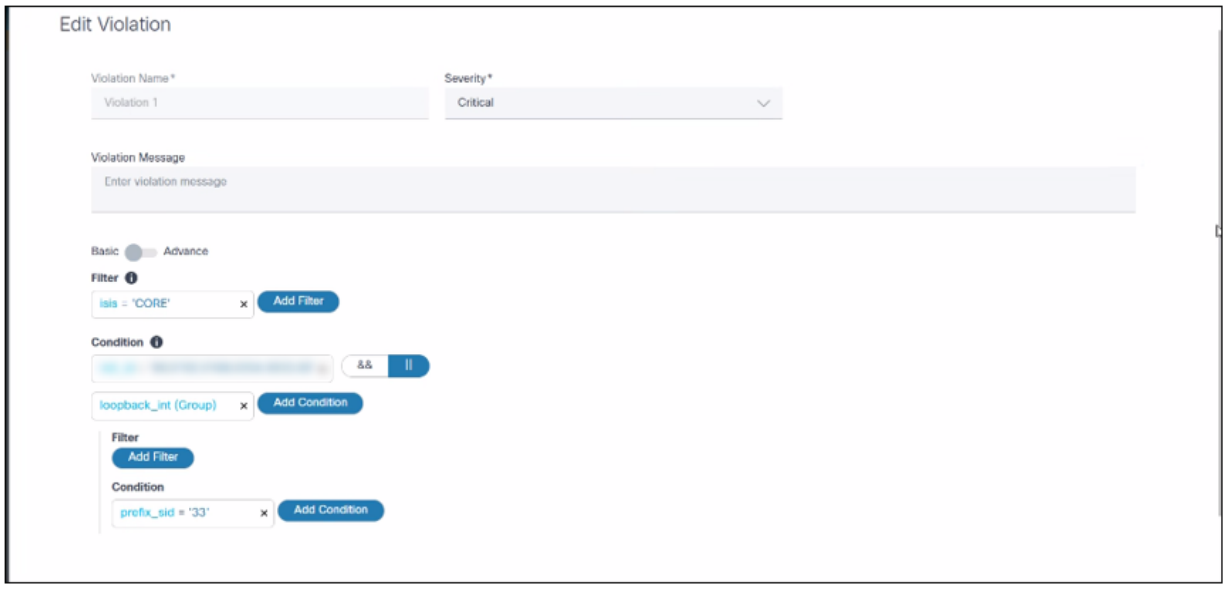
	A	B	C	D	E	F	G	H	I	J	K
1	Device Name	Managed By	Product Family	Compliance	Critical	Major	Minor	Warning	Info	Unknown	Last Checked
2	CNC-bnr-asr-78	Direct-To-Device	IE 2000 Series	Non Compliant	1	0	0	0	0	0	04-Aug-25
3	D2d-118	Direct-To-Device	IE 2000 Series	Partially Compliant	0	1	0	1	1	0	04-Aug-25
4	D2d-juniper	Direct-To-Device	juniper-junos	Partially Compliant	0	0	0	2	2	1	06-Aug-25
5	DNAC_Mock_Device0	DNAC-Mock	Cisco Catalyst 9922-CL Wireless Controller for Cloud	Unknown	0	0	0	0	0	1	05-Aug-25
6	bnr-asr-78	cnc6		Partially Compliant	0	0	1	0	0	0	05-Aug-25
7	bnr-isr-118	Direct-To-Device	cisco-ios	Partially Compliant	15	2	0	2	6	0	06-Aug-25
8	bnr-n3k-44	NSO-166	cisco Nexus9000 C9300v Chassis	Partially Compliant	12	0	0	0	3	0	05-Aug-25
9											

Add or Edit Blocks-Rules(블록 규칙 추가 또는 수정): 규칙 추가 또는 수정

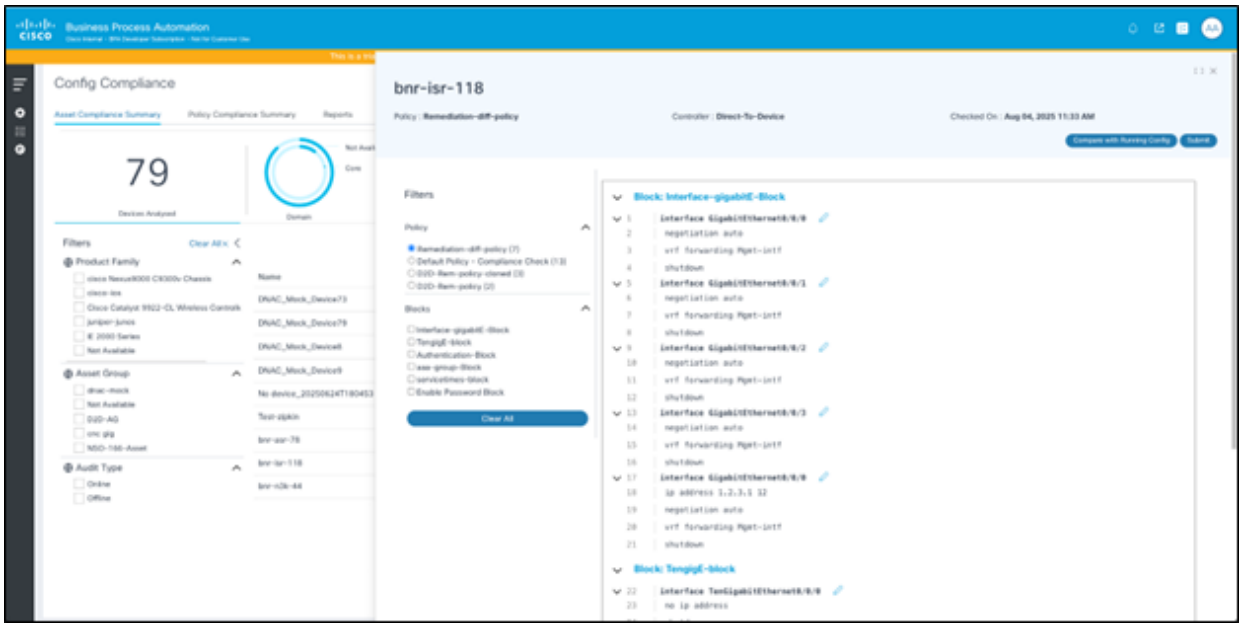
규칙 위반 추가 또는 수정

규칙 위반은 규정준수 실행에서 중요한 구성 요소로, 수행해야 할 특정 검사에 대해 자세히 설명합니다. 다음은 규칙 위반을 생성 및 관리하는 방법에 대한 개요입니다.

- 기본 모드:
  - 사용자 인터페이스 요소: 이 모드에서는 사용자가 GUI(Graphical User Interface)를 사용하여 규칙 위반을 생성할 수 있습니다. 이 접근법은 전형적으로 더 사용자 친화적이고 코딩에 관여하고 싶어하지 않는 사람들을 위해 접근 가능하다.
  - 단계별 지침: 사용자는 사전 정의된 UI 요소를 사용하여 검사를 정의하는 프로세스를 안내받습니다.
- 고급 모드:
  - JSON 유사 코드 형식: 코딩에 익숙한 사용자의 경우 이 모드에서는 JSON과 같은 구조화된 형식으로 입력하여 규칙 위반을 생성할 수 있습니다.
  - 유연성 및 정밀도: 이 방법을 사용하면 복잡한 규칙 확인을 정의할 수 있는 유연성과 정확성이 향상됩니다.



규칙 위반 생성 또는 편집 - 기본 모드



규칙 위반 생성 또는 편집 - 고급 모드

규칙 위반에는 다음 섹션이 있습니다.

- 위반 이름: 위반의 이름
- 심각도: 실행 중 이 위반이 실패하는 경우 규정 준수 심각도를 정의합니다.
- 위반 메시지: 위반 확인에 실패할 경우 메시지가 표시됩니다
- 위반 필터 기준: 그룹이 아닌 스키마 변수를 사용할 수 있는 위반 조건을 적용합니다.
  - 필터 기준에서 그룹의 일부가 아닌 개별 데이터 요소를 기반으로 조건을 설정하는 데 사용됩니다.
  - 사용자가 데이터의 계층 및 구조에 따라 기준을 선택할 수 있도록 하여 정확하고 관련 있는 필터링을 보장합니다.
- 규칙 조건: Group 및 Non-Group 스키마 변수를 모두 사용할 수 있는 경우 규정 준수를 확인하기 위한 실제 조건입니다.
  - 두 유형의 변수 모두 규칙에 사용되어 포괄적 조건을 생성합니다
  - 그룹 변수: 관련 데이터 수집에 조건을 적용할 수 있도록 하여 구조화된 그룹 내에서 철저한 확인 보장
  - 그룹 외 변수: 독립적인 데이터 요소에 조건을 적용할 수 있도록 하여 규칙 적용의 유연성 제공

동적 사용자 정의 블록 - 모범 사례

- 변수 이름이 각 블록 내에서 고유한지 확인합니다.
- 그룹 이름에 변수를 사용하지 마십시오.
- 하위 계층 구성의 경우 블록에서 "<group>"을 사용합니다.

예:
https://ttp.readthedocs.io/en/latest/Writing%20templates/How%20to%20parse%20hierarchical%20(config

[to-parse-hierarchical-configuration-data]

- 유사한 컨피그레이션 라인의 값을 단일 변수로 캡처하려면 다음과 같이 변수를 사용합니다. `{{ <<var-name>> | 선 | joinmatches(',') }}`. 다음 예에서 보여주는 것처럼 `{{ start }}` 및 `{{ end }}`} 내에 구성 행을 묶습니다.

디바이스 컨피그레이션	구성 차단
ip 도메인 목록 vrf Mgmt-intf core.cisco.com ip 도메인 목록 cisco.com ip 도메인 목록 east.cisco.com ip 도메인 목록 west.cisco.com	{{_start_}} ip 도메인 목록 {{ domains | _line_ | joinmatches(‘,') }} {{ _end_ }} ip 도메인 목록 vrf {{ vrf_name }} {{ vrf_domain }}

- 구성 행에서 공백이 포함된 값을 캡처하려면 아래 표에 나와 있는 것처럼 블록의 변수를 사용합니다. `{{ <<var-name>> | re(".*") }}`

디바이스 컨피그레이션	구성 차단
인터페이스 HundredGigE0/0/1/31 설명 인터페이스: 12년 01Hg0/0/1/31 mtu 9216	인터페이스 {{ INTF_ID }} 설명 {{ INTF_DESC | re(".*") }} mtu 9216

규칙 및 비 RefD 규칙에서 규칙 계층 구조 및 RefD 통합 이해

동적 블록 TTP에는 컨피그레이션이 구조화되고 검증되는 방법을 결정하는 두 가지 스키마가 있습니다.

- 그룹 기반 스키마:
  - 이 스키마는 계층적 방식으로 구성을 구성하여 요소 간에 상위-하위 관계를 설정합니다
  - 요소가 논리적으로 중첩되고 상호 연관된 복잡한 컨피그레이션에 이상적
  - 서로 다른 구성 요소 간의 계층적 관계 및 종속성을 검증하도록 규칙을 정의할 수 있습니다
- 비그룹 기반 스키마:
  - 구성은 계층 관계 없이 모든 요소가 동일한 레벨에 존재하는 플랫 형식으로 구성됩니다
  - 계층 구조가 필요 없는 간단한 구성에 적합

    - 각 구성 요소가 특정 기준을 충족하도록 규칙을 설정할 수 있습니다

RefD 통합

- RefD의 목적:
    - 역할: BPA 프레임워크 내에서 지역 및 외부 변수를 관리하기 위한 도구 역할을 함
    - 기능:
        - 동적 가져오기: 가변 데이터의 동적 검색 및 관리를 지원하여 규정 준수 확인이 실시간 데이터 변화에 적응할 수 있도록 합니다.
        - API 상호 작용: BPA 활용 사례를 위한 API를 제공하여 이러한 동적 변수와 값에 액세스하고 이를 관리함으로써 규정 준수 워크플로에 원활하게 통합됩니다.

규정준수 규칙 값 구문

CnR 활용 사례는 RefD 프레임워크와 통합되어 규정 준수 확인 및 교정 워크플로 내에서 데이터를 동적으로 활용합니다. 특히 사용된 변수의 구문과 유형에 초점을 맞추어 이러한 통합이 어떻게 작동하는지에 대한 자세한 설명은 다음과 같습니다.

- 키워드로 패킷 암호화를 허용하기 때문입니다: 구문은 "RefD"로 시작해야 합니다.
- 매개변수: 구문에서 "key" 매개변수는 필수 항목입니다
- 예:

```
plaintext
Copy Code
RefD:ns={$SITE}&key={{#device.deviceIdentifier}}.interfaces.MgmtEth{{ INT_ID }}.ipv4_addr
```

변수 유형

- 사용자 정의 변수:
    - 규정준수 작업을 생성하는 동안 구성되었습니다.
    - 범위: 지정된 작업의 모든 실행에 적용 가능
    - 구문: `{$VarName}`
    - 예: `{$SITE}`
- 시스템 변수
    - 실행 중 사용 가능한 상황 데이터를 기반으로 프레임워크에서 사전 정의
    - 현재 프레임워크는 디바이스 객체에 대한 액세스를 제공합니다
    - 구문: `{{#VarName}}`
    - 예:
        - `{{#device.deviceIdentifier}}` - 디바이스 식별자를 나타냅니다.
        - `{{#device.additionalAttributes.serialNumber}}` - 장치 일련 번호를 나타냅니다.

- TTP 변수
  - 블록 구성에 있음
  - 구문: `{{ VarName }}`
  - 예: `{{ INT_ID }}`

비 RefD 규칙

- 이러한 규칙은 RefD 규칙과 같지만 "RefD" 키워드로 시작하지 않습니다
- 예:

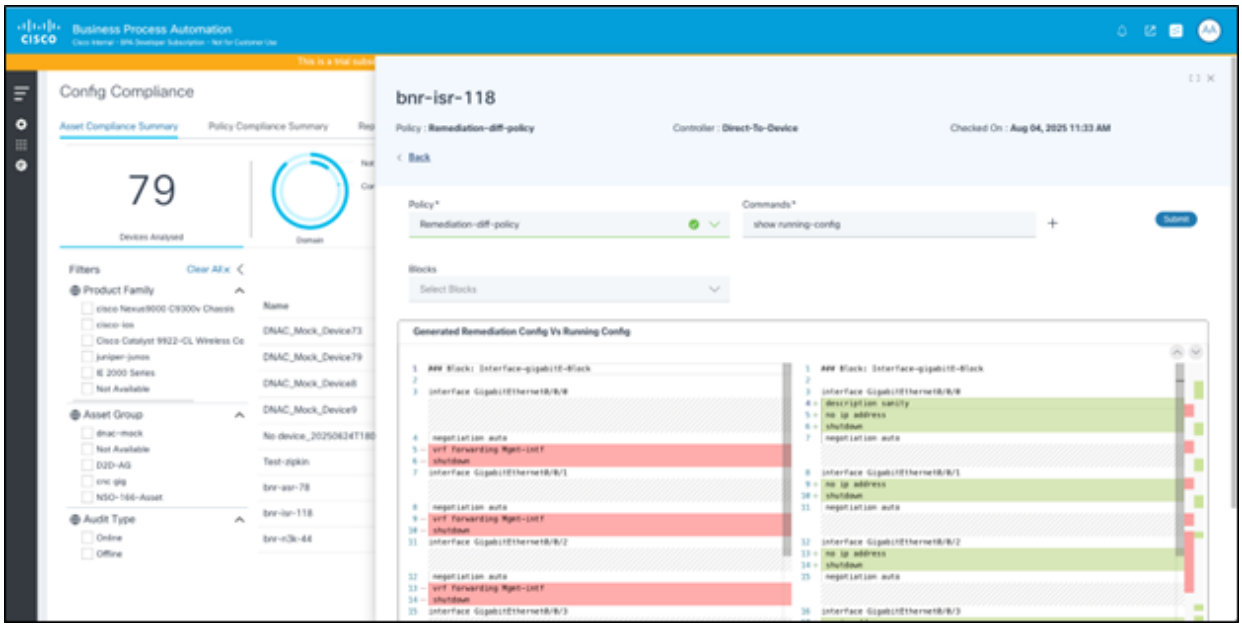
```
plaintext
Copy Code
{$int_id}.{{#device}}.{{ mtu_val }}
```

변수 사용

- 사용자 정의 변수: {$Var}(으)로 표시됨
- 시스템 변수: deviceIdentifier, controllerId, `controllerType` 등의 특성을 노출하는 `{{#Var}}`로 표시됩니다.
- TTP 변수: 이중 중괄호 안에 `{{var}}`(으)로 표시됨

실행

- 작업을 생성하는 동안 $ 변수가 지정된 경우 해당 값을 설정할 수 있습니다
- 변수의 결합된 값을 가져온 디바이스 컨피그레이션과 비교하여 규정 준수 보장



디바이스 컨피그레이션

	A	B	C	D	E	F
1	Policy Name	Fully Compliant	Partially Compliant	Non Compliant	Unknown	Total Assets
2	D2D-Juniper-policy	0	1	0	0	1
3	D2D-Raiseviolation-policy	0	1	0	0	1
4	D2D-Rem-policy	0	1	0	2	3
5	D2D-Rem-policy-cloned	0	1	0	0	1
6	Default Policy - Compliance Check	0	2	0	70	72
7	Policy Delete Issue	1	0	0	0	1
8	Policy Test	1	0	0	0	1
9	Remediation-diff-policy	0	1	0	0	1
10	cnc gig policy	0	1	0	0	1
11	cnc gigabit	0	2	1	1	4
12						

구성 규칙: 참조D

블록 세부 정보 보기

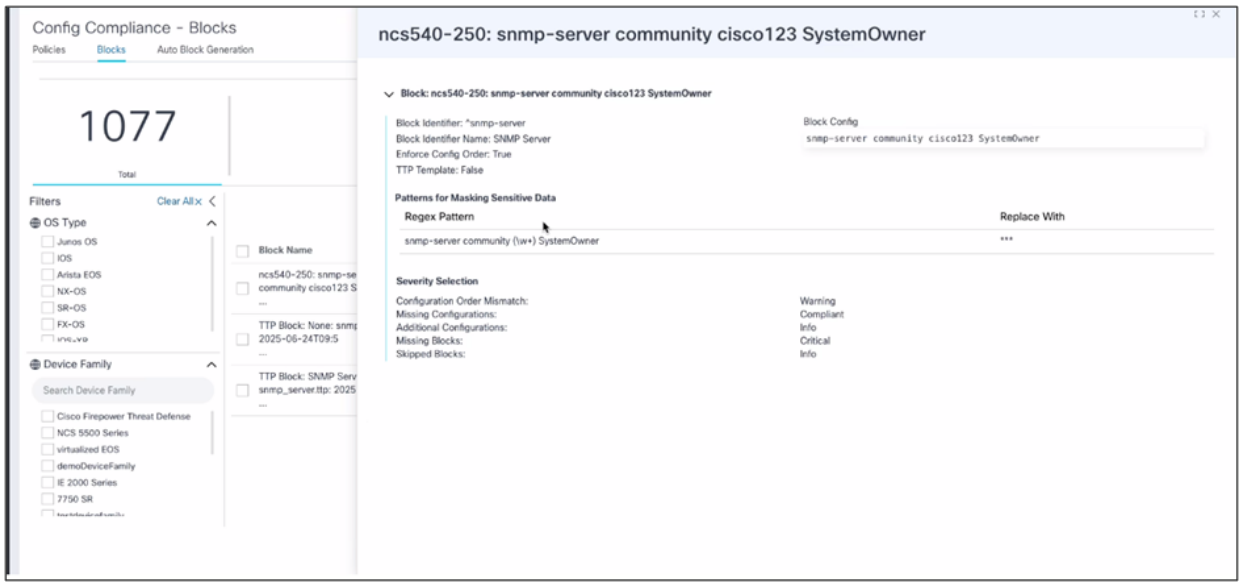
블록 세부 정보에 액세스하려면

1. Blocks 페이지로 이동합니다.
2. 그리드에서 행을 선택하거나 눌러 특정 블록의 세부 정보를 봅니다. 화면 오른쪽에 블록 세부 정보 페이지가 표시됩니다.

참고: 이 페이지는 연관된 블록, 규칙 및 모든 위반을 포함하여 블록과 관련된 모든 정보의 읽기 전용 보기를 제공합니다.

하이퍼링크가 있는 경우 세부 정보 내에서 클릭하면 사용자가 관련 블록 또는 관련 정보로 리디렉

션됩니다.



차단 세부 정보 보기

블록 삭제

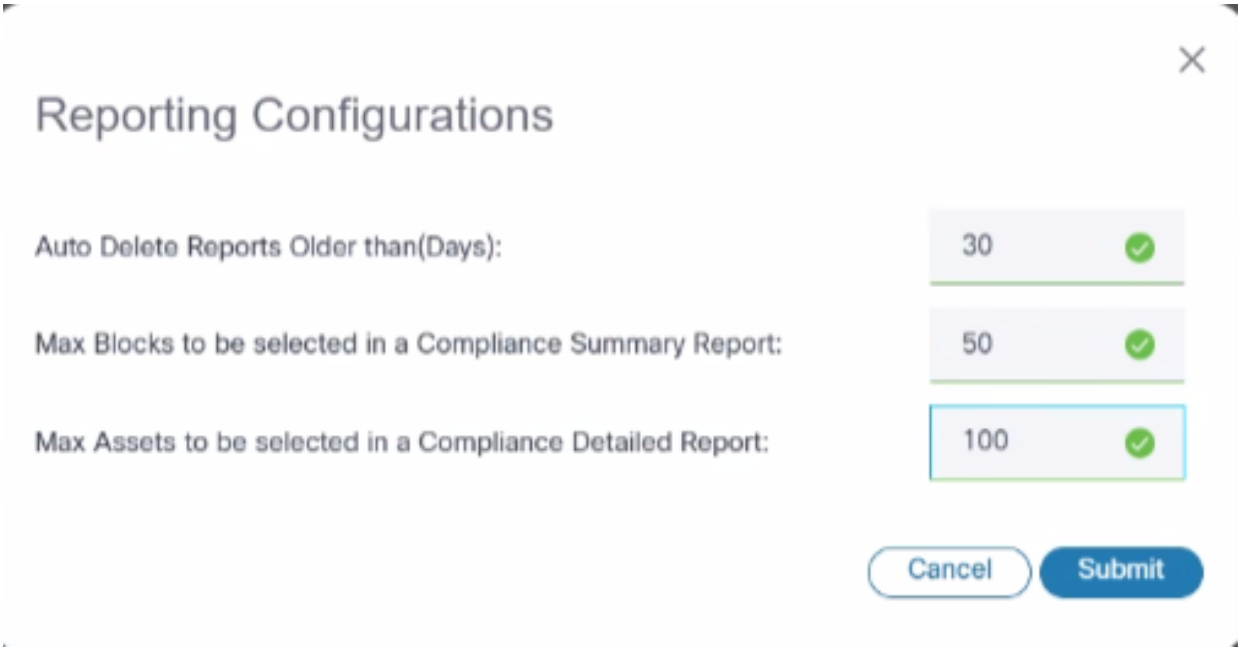
포털에서는 사용자가 적절한 RBAC 권한이 있는 경우 하나 이상의 블록을 삭제할 수 있습니다. 사용자는 다음 단계를 완료하여 이러한 작업을 수행할 수 있습니다.

단일 블록 삭제:

1. Blocks 페이지로 이동합니다.
2. 삭제할 블록 옆에 있는 More Options(추가 옵션) 아이콘을 클릭합니다.
3. 삭제 옵션을 선택합니다. 확인 메시지가 표시됩니다.

다중 블록 삭제:

1. Blocks 페이지로 이동합니다.
2. 삭제할 각 블록 옆에 있는 확인란을 선택합니다.
3. 추가 옵션 아이콘을 클릭하고 삭제를 선택합니다. 확인 메시지입니다.

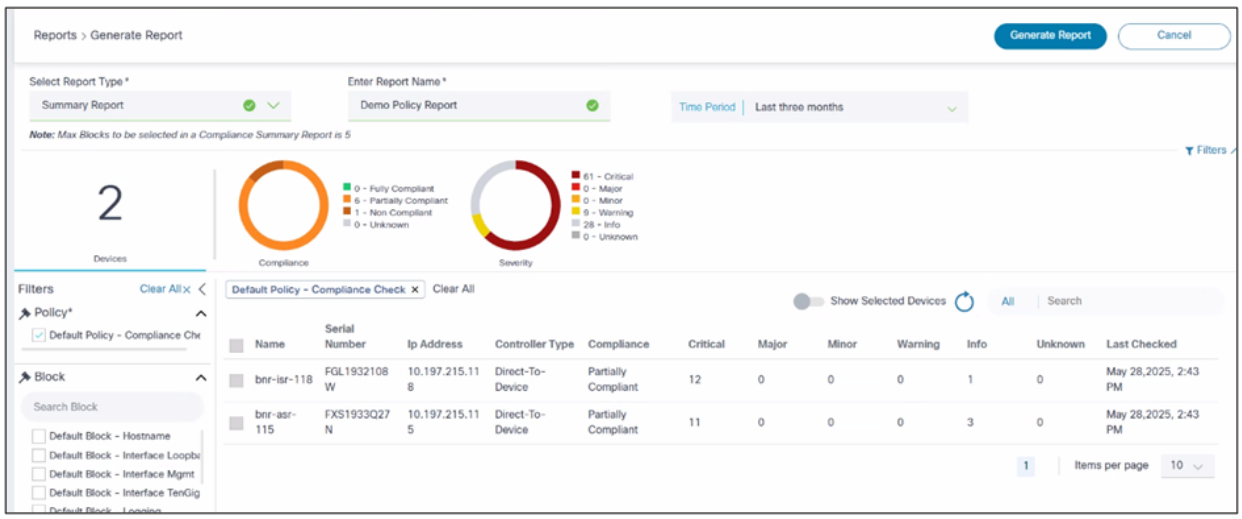


블록 삭제

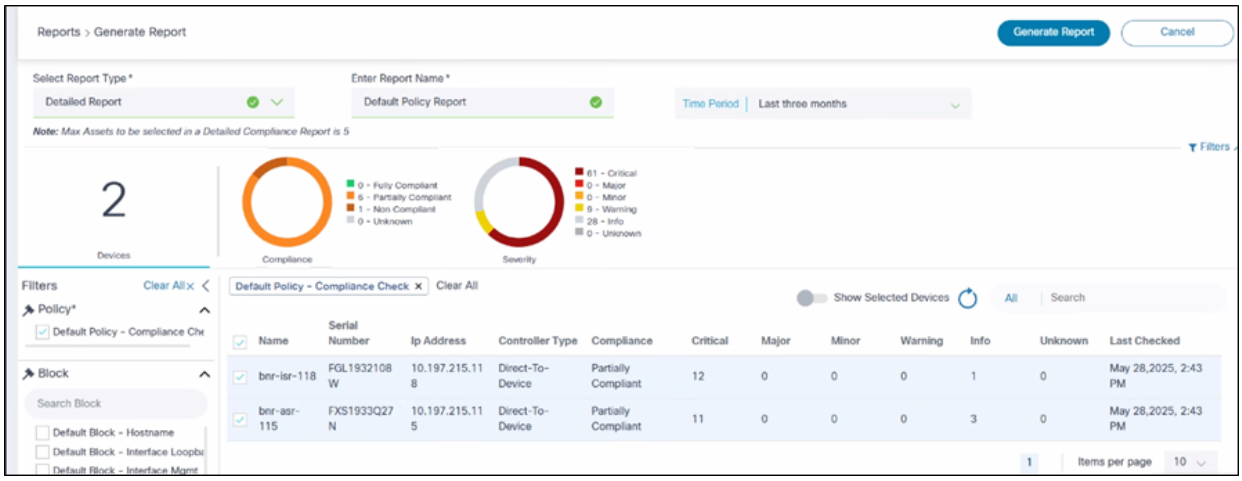
설정: 자동 블록 생성

블록 생성은 사용자가 디바이스의 컨피그레이션을 기반으로 블록을 자동으로 생성할 수 있게 합니다. 이러한 자동화는 수동 생성에 필요한 시간과 노력을 줄이고, 사용자가 처음부터 시작하는 대신 변수를 추가하거나 제거하여 블록을 쉽게 편집할 수 있도록 합니다.

블록 생성 세부 정보를 보려면 행을 클릭합니다.

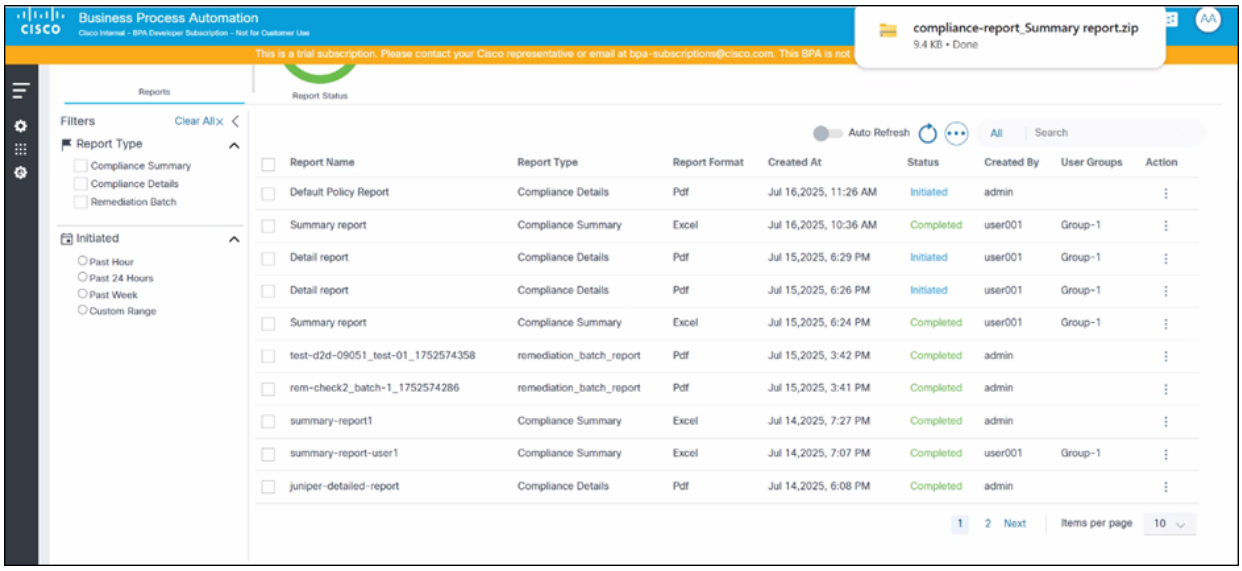


자동 차단 생성 목록 - 보기



자동 차단 생성 세부 정보

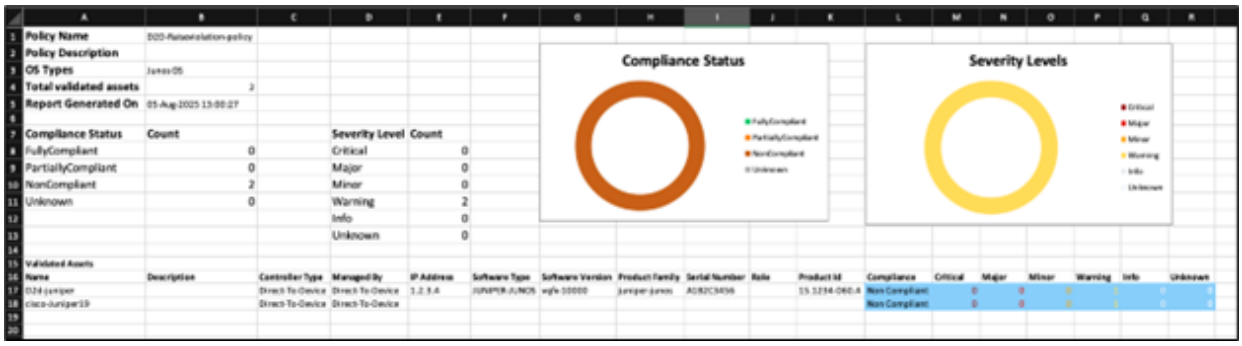
자동 블록 생성



자동 차단 생성 목록

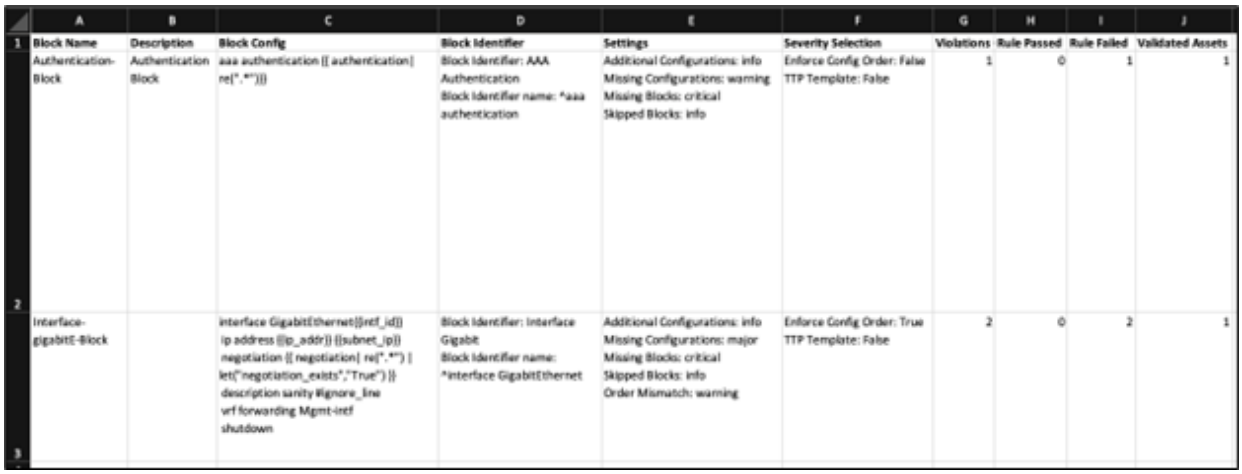
Automatic Block Generation(자동 블록 생성) 페이지에는 다음 필드가 포함되어 있습니다.

- 생성 출처: 블록이 생성되는 소스입니다. 다음과 같은 세 가지 옵션이 있습니다.
  - 디바이스 컨피그레이션 백업: 시스템은 백업 활용 사례에서 디바이스 컨피그레이션을 선택합니다



디바이스 컨피그레이션 백업

- 파일 업로드: 사용자가 디바이스 컨피그레이션을 업로드할 수 있는 File Upload 창이 열립니다



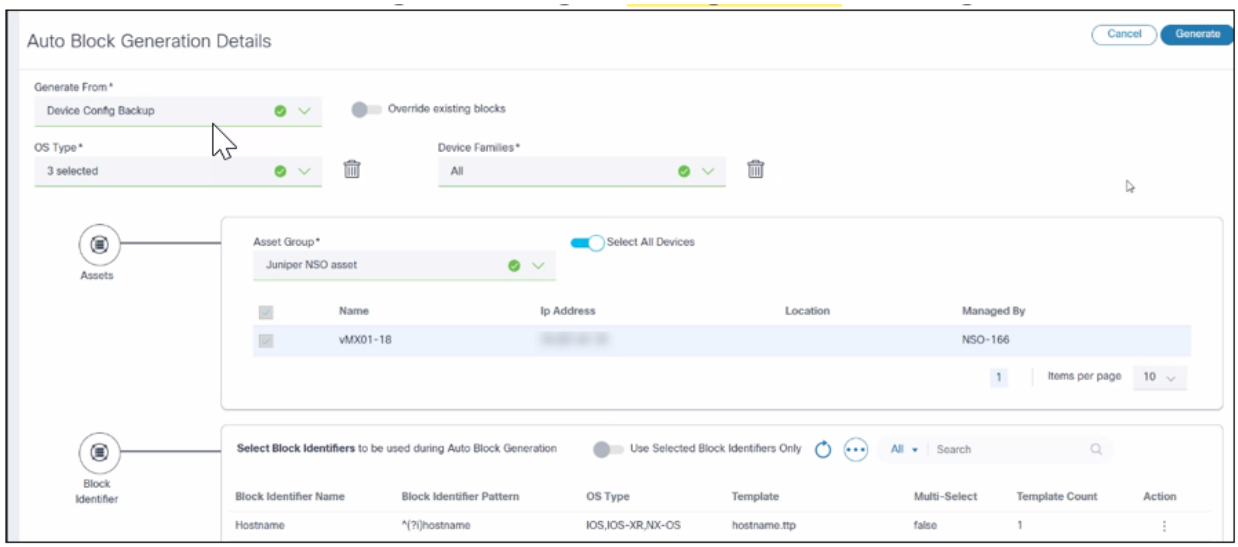
파일 업로드

- 현재 구성: 시스템이 디바이스 컨피그레이션을 가져오기 위해 사용하는 CLI 컨피그레이션 명령을 입력합니다.

	A	B	C	D	E	F	G
1	**Rule Name**	**Rule Description**	**Violation Name**	**Description**	**Severity**	**Violation Count**	**Affected Assets Count**
2	Gigabit Rule	Rule to validate violations for Gigabit ethernet configuration	DescriptionCheck		warning	5	3
3	Gigabit Rule	Rule to validate violations for Gigabit ethernet configuration	IP-Address-Validation		critical	6	2
4	Gigabit Rule	Rule to validate violations for Gigabit ethernet configuration	No-Shutdown-check		compliant	0	0
5							
6							
7	**Rule Name**	**Violation Name**	**Severity**	**Device Name**	**Managed By**		
8	Gigabit Rule	DescriptionCheck	warning	bnr-isr-118	Direct-To-Device		
9	Gigabit Rule	DescriptionCheck	warning	bnr-isr-119	Direct-To-Device		
10	Gigabit Rule	DescriptionCheck	warning	bnr-isr-121	Direct-To-Device		
11	Gigabit Rule	IP-Address-Validation	critical	bnr-isr-118	Direct-To-Device		
12	Gigabit Rule	IP-Address-Validation	critical	bnr-isr-120	Direct-To-Device		
13							

현재 구성

- OS 유형: 이 블록과 관련된 OS 유형의 목록입니다.
- 장치 제품군: 이 블록과 관련된 디바이스 제품군 목록입니다.
- 자산: Assets 기능은 동적 블록을 생성하기 위한 장치를 선택하는 구조화된 접근 방식을 제공합니다
    - 자산 그룹 선택:
        - 사용자가 동적 블록을 생성하는 데 사용되는 자산 그룹이라고 하는 사전 정의된 디바이스 그룹을 선택할 수 있습니다
        - 위치, 유형 또는 기능과 같은 특정 기준에 따라 디바이스를 그룹화하여 디바이스를 쉽게 관리하고 구성할 수 있습니다.
    - 하위 집합 장치 선택:
        - 사용자는 선택한 자산 그룹 내에서 특정 장비 하위 집합을 선택할 수 있습니다.
        - 사용자가 특정 디바이스 세그먼트에 집중할 수 있도록 하여 더 많은 대상 블록 생성 및 관리 지원



블록 생성

- 블록 식별자: 사용자가 블록 생성 중에 사용되는 블록 식별자 목록을 선택할 수 있는 옵션을 제공합니다. 또한 블록 식별자 관리 기능도 인라인으로 제공합니다.

블록 식별자

블록 식별자는 CiscoConfParser를 사용하여 전체 디바이스 컨피그레이션에서 컨피그레이션 블록을 추출합니다. 각 블록 식별자는 regex 패턴과 연결되어야 합니다. 사용자는 UI 또는 API를 사용하여 자신의 블록 식별자를 생성하거나 기존의 블록 식별자를 업데이트할 수 있다. 이 플랫폼은 현재 약 55~60개의 기본 블록 식별자를 제공합니다. 각 식별자는 OS 유형에 고유하며 Ingester 서비스를 통해 BPA 애플리케이션 구축 중에 로드됩니다. TTP 템플릿은 각 블록 식별자와 연관될 수 있습니다. 블록 식별자의 이름과 패턴은 모두 고유해야 합니다.

블록 식별자에 대해 Multi 옵션이 활성화된 경우, 규정준수 프레임워크는 일치하는 컨피그레이션에서 여러 컨피그레이션 블록을 생성합니다. 그렇지 않으면 일치하는 모든 컨피그레이션을 단일 블록

으로 취급합니다.

Multi 옵션 True의 블록 식별자 예: 인터페이스, 라우터 bgp, vrf, l2vpn 등

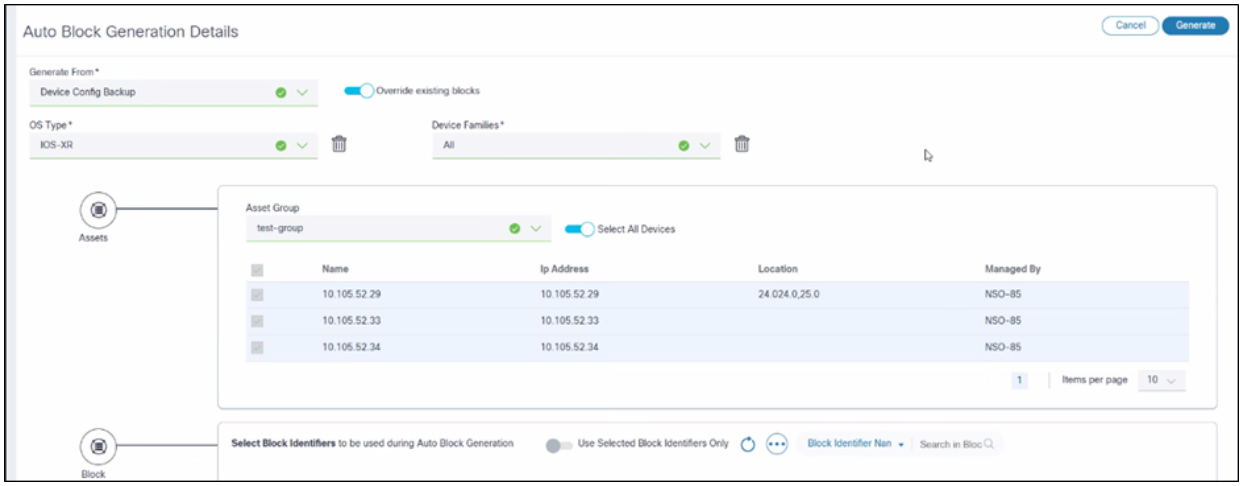
Multi option False가 있는 블록 식별자의 예: 로깅, snmp-server, domain 등

예:

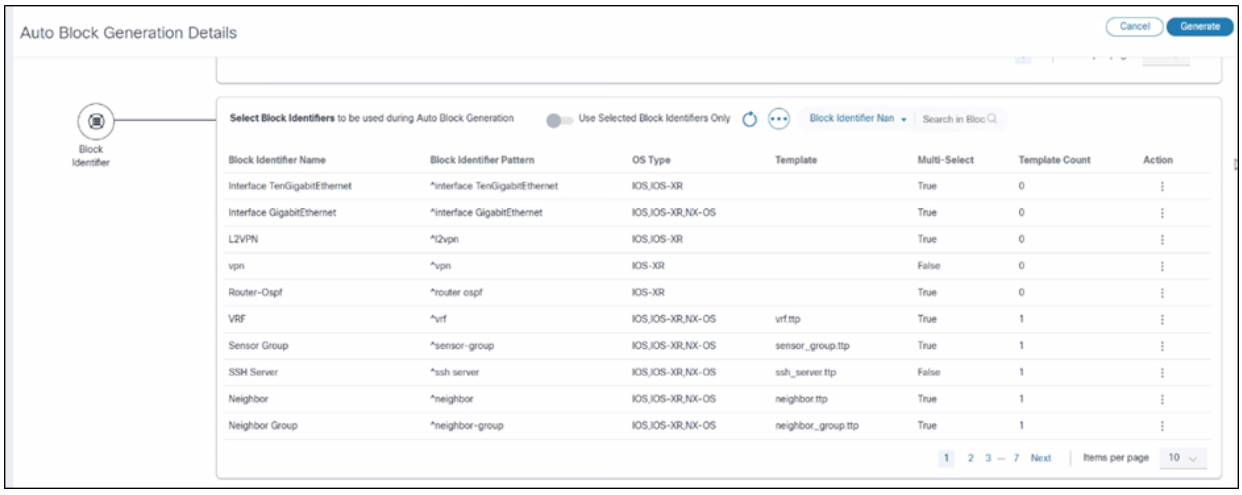
```
{
  “name”: “BundleEthernet Interface”,
  “osType”: [“IOS”, “IOS-XR”, “NX-OS”],
  “multi”: true,
  “blockIdentifier”: “^(?i)interface Bundle-Ether”,
  “templates”: [“parent_interface.ttp”]
}

{
  “name”: “Loopback Interface”,
  “osType”: [“IOS”, “IOS-XR”, “NX-OS”],
  “multi”: true,
  “blockIdentifier”: “^(?i)interface Loopback”,
  “templates”: [“parent_interface.ttp”]
}
```

목록 블록 식별자

목록 블록 식별자를 사용하면 검색 및 정렬 기능과 함께 블록 식별자 목록을 볼 수 있습니다. 이 기능은 Generate Blocks(블록 생성) 페이지에서 사용할 수 있습니다.

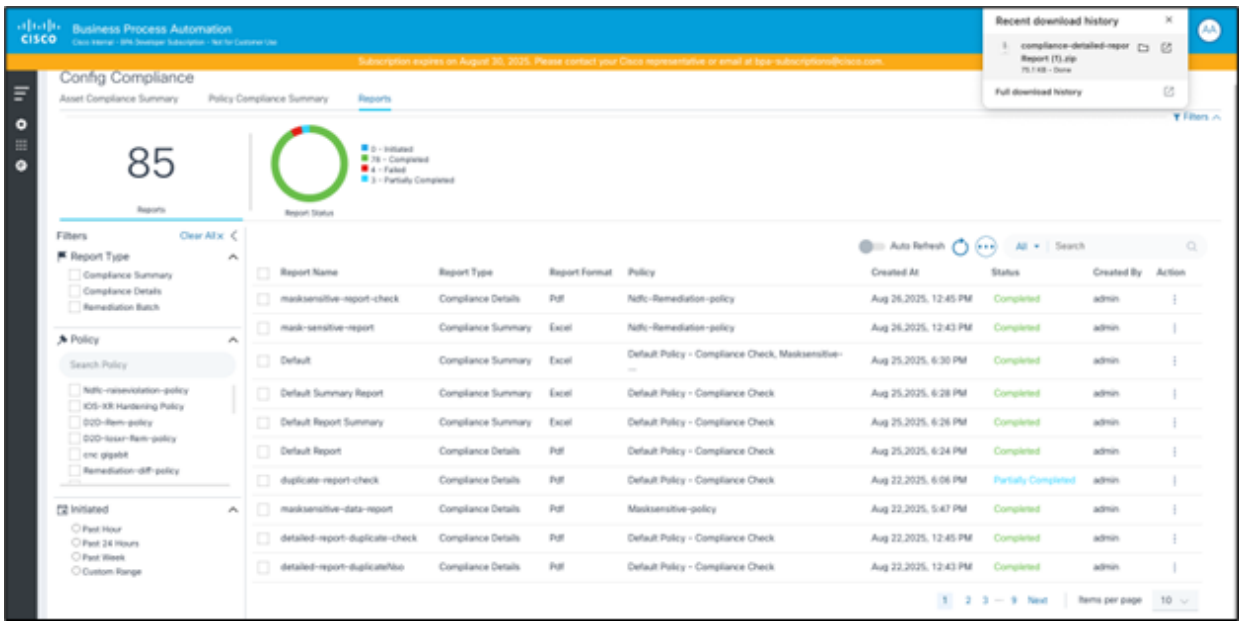


블록 식별자 목록



블록 식별자

블록 식별자 만들기 또는 편집

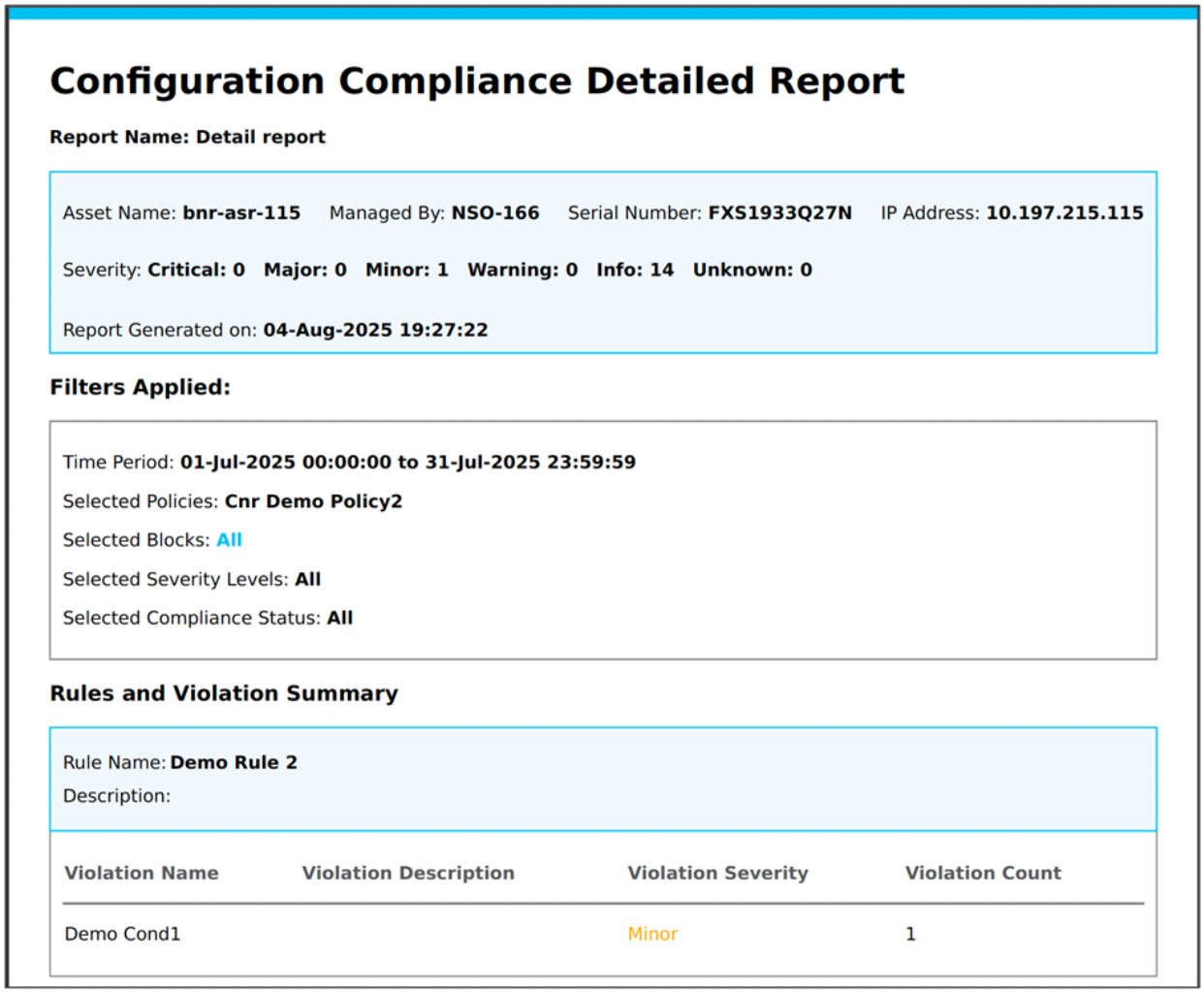


블록 식별자 편집

Auto Block Generation(자동 블록 생성) 페이지의 Block Identifier List(블록 식별자 목록) 섹션에서는 블록 식별자를 효과적으로 관리할 수 있는 툴을 제공합니다. 기능은 다음과 같습니다.

- 블록 식별자 만들기
  - 사용자는 목록에 새 블록 식별자를 추가할 수 있습니다
  - 이것은 블록을 조직하고 구별하기 위해 사용될 수 있는 고유 식별자를 도입할 수 있게 한다
- 블록 식별자 편집
  - 기존 블록 식별자를 수정할 수 있습니다.
  - 식별자를 업데이트하거나 수정할 수 있도록 하여 정확하고 해당 블록의 연관성을 유지합니다.

- 블록 식별자 삭제
  - 사용자는 목록에서 블록 식별자를 제거할 수 있습니다
  - 더 이상 필요하지 않거나 적용할 수 없는 식별자를 제거할 수 있도록 하여 식별자 관리를 용이하게 합니다.



Configuration Compliance Detailed Report

Report Name: Detail report

Asset Name: bnr-asr-115 Managed By: NSO-166 Serial Number: FXS1933Q27N IP Address: 10.197.215.115

Severity: Critical: 0 Major: 0 Minor: 1 Warning: 0 Info: 14 Unknown: 0

Report Generated on: 04-Aug-2025 19:27:22

Filters Applied:

Time Period: 01-Jul-2025 00:00:00 to 31-Jul-2025 23:59:59

Selected Policies: Cnr Demo Policy2

Selected Blocks: All

Selected Severity Levels: All

Selected Compliance Status: All

Rules and Violation Summary

Rule Name: Demo Rule 2

Description:

Violation Name	Violation Description	Violation Severity	Violation Count
Demo Cond1		Minor	1

블록 식별자 삭제

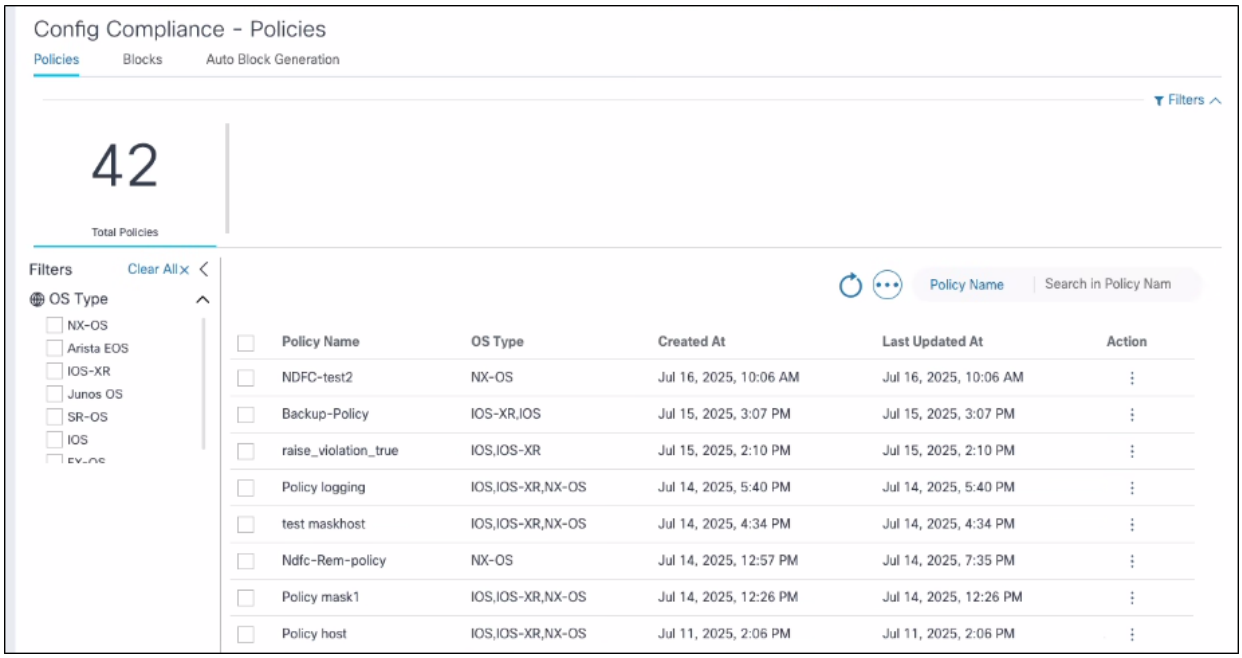
설정: 정책

Policies(정책) 탭에서 규정 준수 실행을 활성화하는 정책, 규칙 및 블록의 집합을 정의할 수 있습니다. 정책은 컨피그레이션 블록 및 규칙으로 구성된 사용자 정의 템플릿입니다. 정책을 생성하기 위한 구성 블록들의 리스트 및 각 구성 블록에 대한 규칙들의 리스트가 선택될 수 있다.

정책 나열

Policies(정책) 탭에는 정책 목록이 표시될 수 있습니다. 이는 정책의 추가, 수정, 삭제, 가져오기 및 내보내기에 대한 작업도 제공합니다.

참고: 관련 블록 및 규칙과 함께 정책을 가져오거나 내보냅니다.



정책 나열

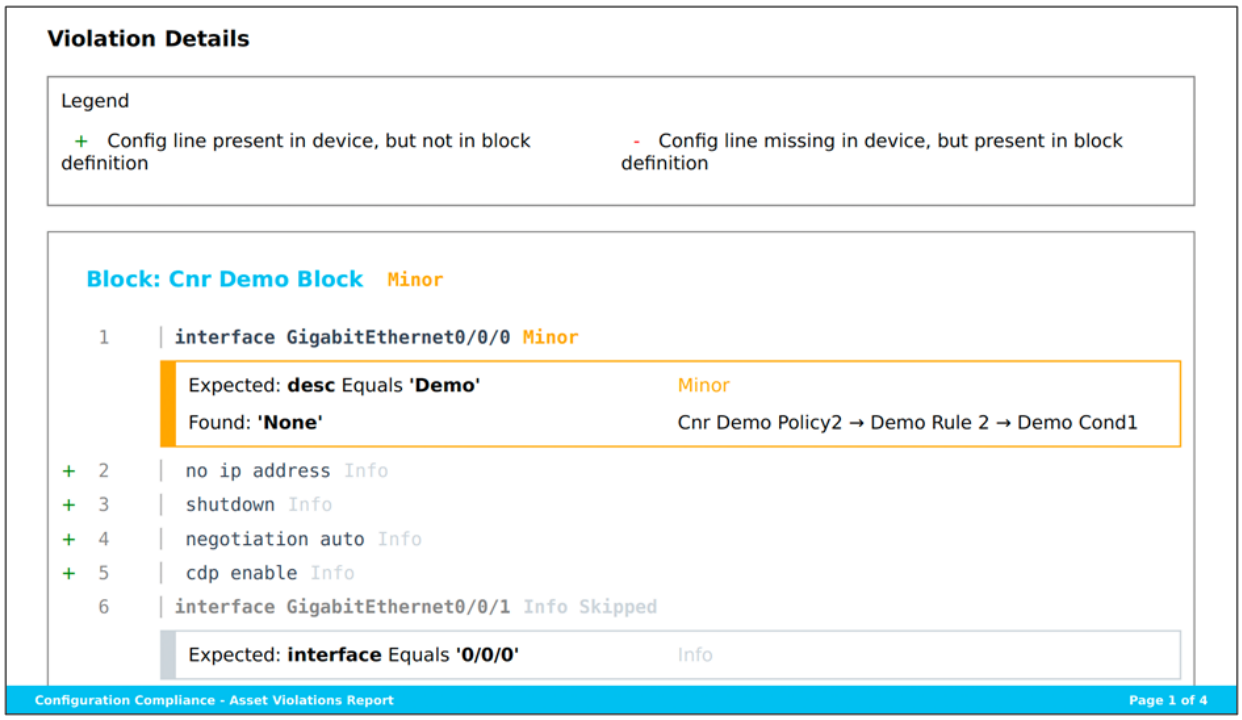
정책 추가 및 수정

이 섹션에서는 Add Policy and Edit Policy 페이지에 대해 간략하게 설명합니다.

정책 세부 정보

- 정책 이름: 정책 이름
- OS 유형: 이 정책에 대해 지원되는 OS 유형 목록
- 장치 제품군: 이 정책에 대해 지원되는 디바이스 제품군 목록
- 정책 설명(선택 사항): 정책에 대해 간략하게 설명합니다.

OS Type 및 Device Family 필드는 다음 섹션에서 선택한 블록을 기준으로 자동으로 채워집니다.

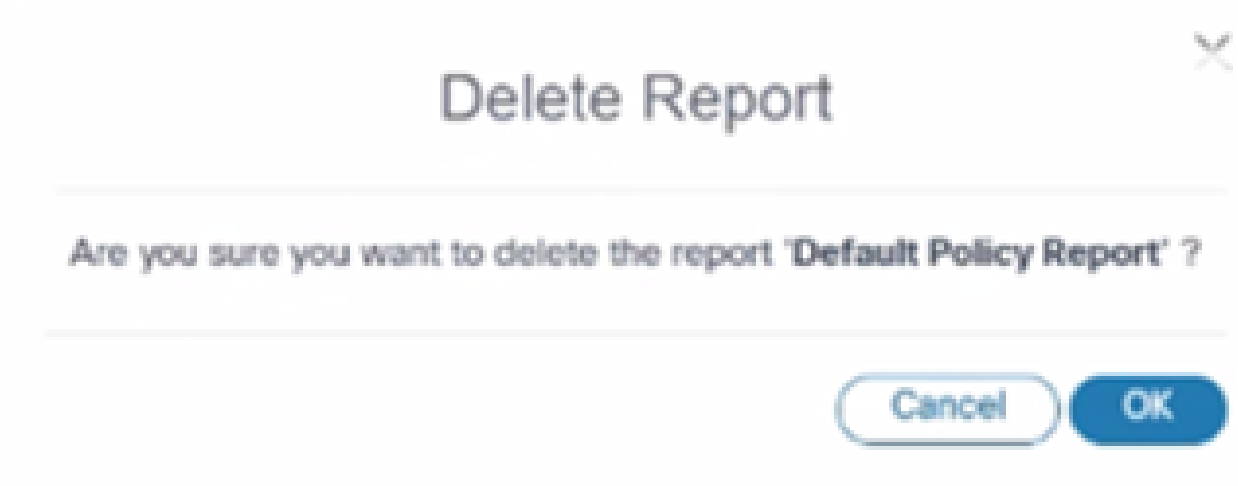


구성 정책: 정책 세부 정보

블록 선택 대화 상자

"Select Blocks(블록 선택)" 기능은 사용자가 정책에 포함할 컨피그레이션 블록을 선택할 수 있도록 설계된 사용자 친화적 인터페이스입니다. 이 섹션에는 해당 기능이 나열되어 있습니다.

- 팝업 대화 상자
  - 목적: 사용자가 현재 페이지를 벗어나지 않고도 구성 블록을 선택할 수 있는 전용 공간을 제공합니다.
  - 사용자 상호 작용: 초점을 맞춘 별도의 대화 상자에 옵션을 표시하여 직관적인 선택 프로세스 보장
- 옵션 추가 및 선택
  - 다중 선택: 사용자는 정책에 포함할 하나 이상의 컨피그레이션 블록을 선택할 수 있습니다
  - 유연성: 사용자의 특정 정책 요구 사항에 따라 다양한 블록을 포함할 수 있도록 지원
- 탐색 기능
  - 필터: 사용자가 특정 기준에 따라 사용 가능한 블록 목록을 좁힐 수 있으므로 관련 블록을 더 쉽게 찾을 수 있습니다.
  - 페이지 매김: 블록을 관리 가능한 페이지로 구성하여 대용량 데이터 집합을 통한 탐색 향상
  - 검색 기능: 이름 또는 기타 식별자로 블록을 빠르게 배치할 수 있으므로 선택 프로세스가 간소화됩니다



블록 선택

사용자는 Block Selection(블록 선택) 섹션에서 Create(생성)를 클릭하여 새 블록을 생성할 수 있습니다. 새 브라우저 탭이 교차 시작되고 사용자가 새 블록을 생성할 수 있습니다. 제출된 사용자는 원래 탭으로 돌아가 새로 생성된 블록을 선택하여 정책에 추가할 수 있습니다.

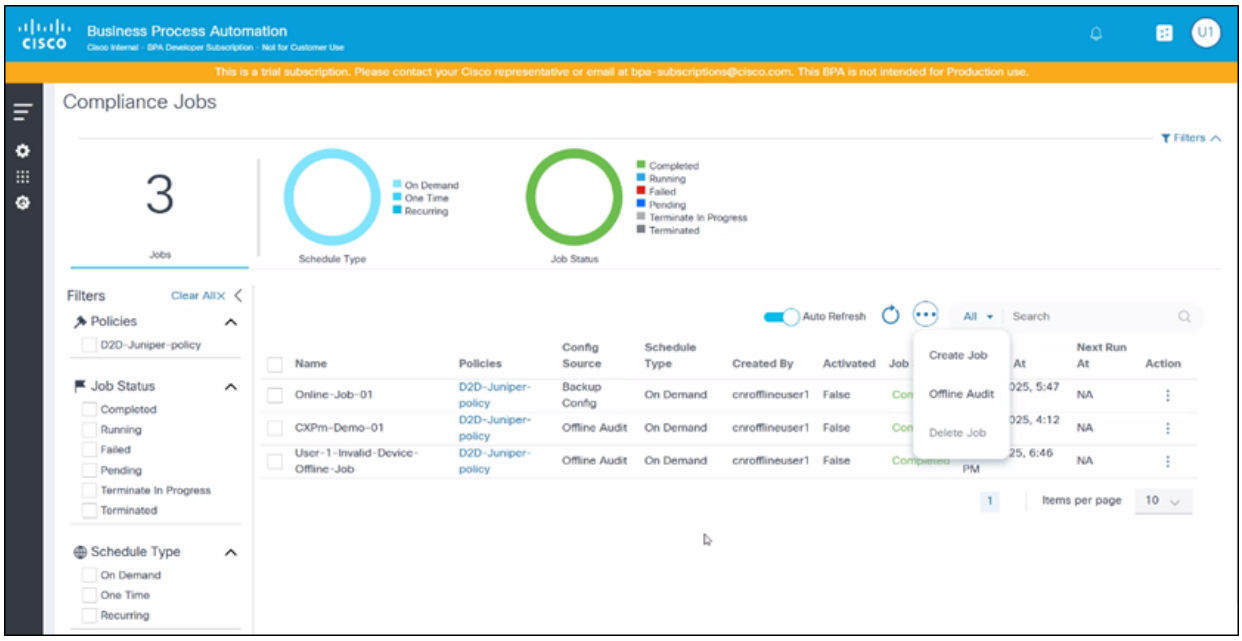
조건 필터

Conditional Filters(조건부 필터) 기능은 사용자가 컨피그레이션 블록에 특정 기준을 적용할 수 있는 고급 툴로서, 정확하고 대상이 지정된 컴플라이언스 검사를 보장합니다.

- 사용자가 미리 정의된 조건에 따라 선택된 구성 블록에 컨피그레이션을 적용하거나 규정 준수 확인을 실행할 수 있습니다.
- 지정된 기준에 부합하지 않는 것을 필터링하여 관련 블록에 리소스와 노력을 집중
- 사용자는 컨피그레이션 블록이 충족해야 컴플라이언스 검사 또는 기타 프로세스에 포함될 조건을 정의할 수 있습니다
- 이러한 조건과 일치하는 블록만 실행되지만 다른 블록은 무시되므로 더 정밀한 제어가 가능합니다

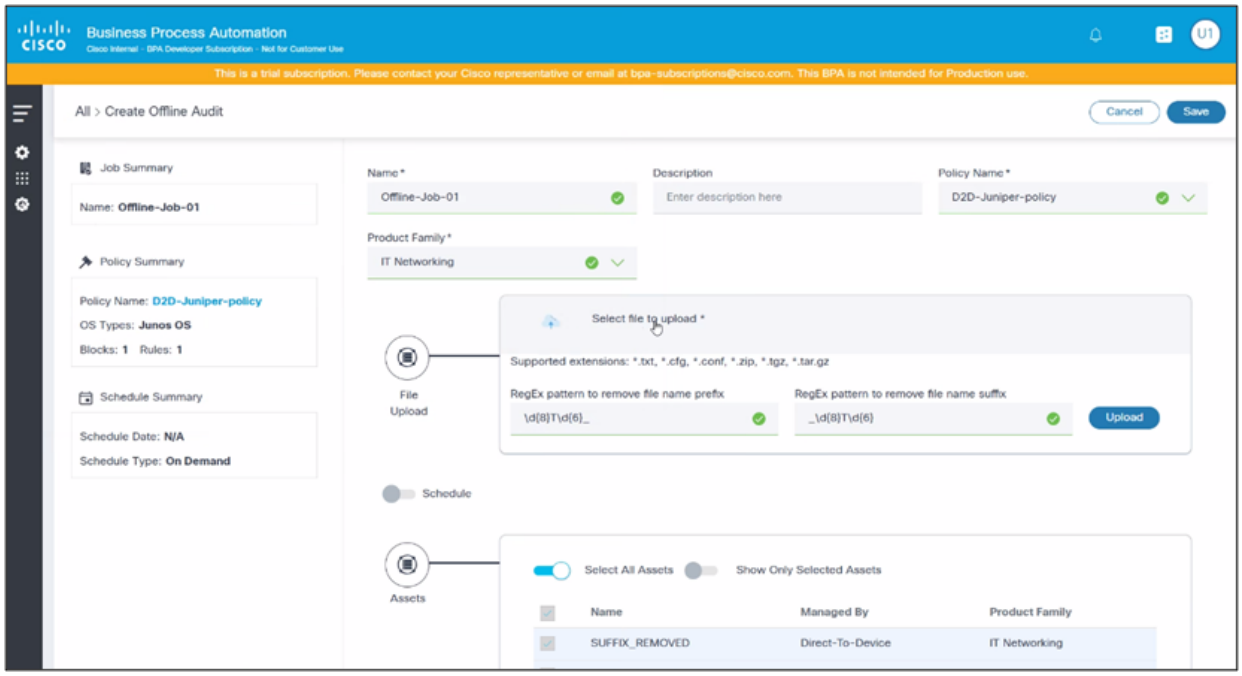
활용 사례:

- 선택적 컴플라이언스 검사: 정책이 사용 가능한 20개 인터페이스 중 2개의 특정 인터페이스에서만 컨피그레이션을 확인하려는 경우 사용자는 조건을 설정하여 규정 준수 확인을 2개의 인터페이스로만 제한할 수 있습니다.



조건 필터

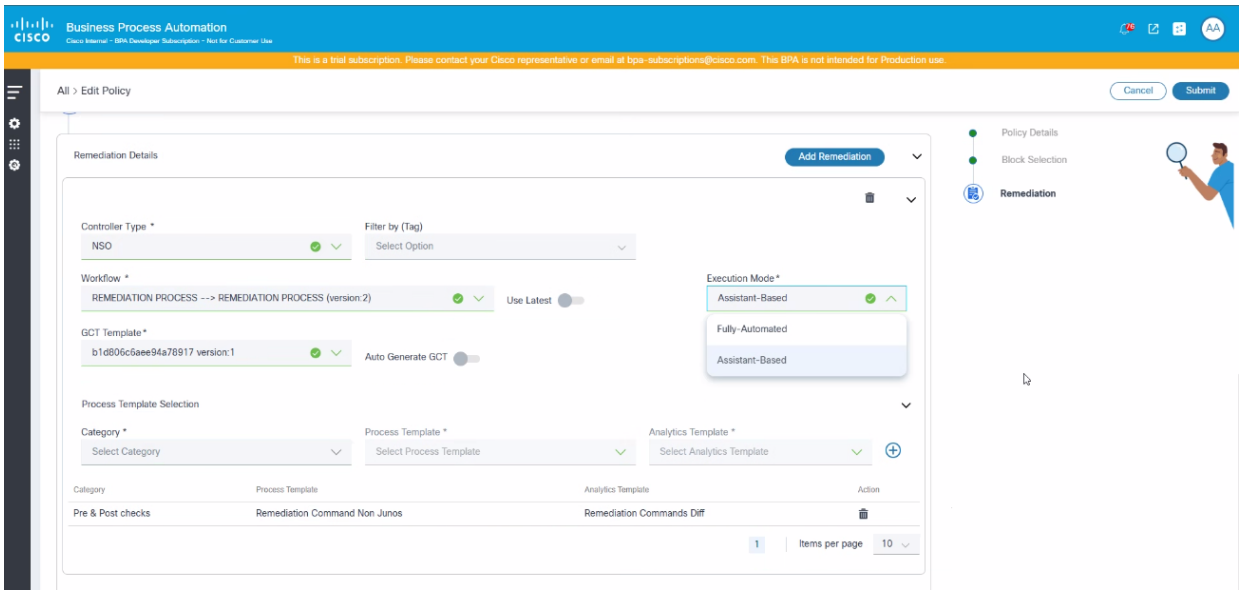
- 규칙 선택: 지정된 구성 블록에 대해 하나 이상의 규칙을 선택하는 옵션입니다.



규칙 선택

리미디에이션 섹션

Policies(정책) 페이지는 컨트롤러 유형별 교정 세부사항을 정의하는 선택적 섹션을 제공합니다.



구성 정책: 교정 세부 정보

- 컨트롤러 유형: 보안정책 교정을 지원하는 컨트롤러 유형 목록
- 교정 워크플로: 선택한 컨트롤러 유형의 디바이스에 대해 실행할 워크플로
- GCT 템플릿: 적용할 하나 이상의 GCT 템플릿
- 프로세스 템플릿: 사전 점검 및 사후 점검의 일부로서 해당 분석 템플릿과 함께 실행될 하나 이상의 프로세스 템플릿.
- 사전 검사 템플릿: 사전 확인을 위해서만 실행할 프로세스 템플릿의 선택적 목록
- 사후 검사 템플릿: 사후 확인을 위해서만 실행할 프로세스 템플릿의 선택적 목록
- 실행 모드:
  - 완전 자동: 교정 프로세스는 수동 개입 또는 사용자 작업 없이 자동으로 실행됩니다
  - 보조자 기반: 시스템은 교정 프로세스 중에 수동 지원이 필요한 사용자 작업을 생성합니다

GCT 기능 자동 생성

GCT 자동 생성 기능은 교정에 필요한 GCT 템플릿을 생성하는 프로세스를 간소화하도록 설계되었습니다. 아래에 자세히 설명되어 있습니다.

- 규정 준수 실행의 결과 및 세부사항을 기반으로 GCT 템플릿을 자동으로 생성
- 템플릿 생성 프로세스 자동화
- 생성된 템플릿은 규정 준수 확인 과정에서 파악된 문제를 해결하도록 맞춤화되어, 규정 준수 요구 사항에 부합하는 교정 작업을 보장합니다

역할 및 액세스 제어

정적 권한 목록

Next-Gen 포털의 Configuration Compliance 대시보드는 BPA의 RBAC 기능을 지원하며, 다음과 같은 권한을 통해 규칙과 조건을 처리하기 위해 GUI 표현에서 구성의 동적 텍스트 블록이 어떻게 표시되는지를 나타냅니다.

그룹	작업	설명
ui-app	complianceDashboard.show	규정 준수 대시보드 앱 표시/숨기기
ui-app	교정Dashboard.show	교정 작업 앱 표시
ui-app	complianceJobs.show	규정 준수 작업 앱 표시
ui-app	규정준수 구성.표시	규정 준수 구성 앱 표시
규정준수대시보드	에셋컴플라이언스 요약	자산 규정 준수 요약 보기
규정준수대시보드	정책규정준수요약	정책 준수 요약 보기
규정준수대시보드	보기위반	위반 세부 정보 보기
규정준수대시보드	정책규정준수 자산요약	영향을 받는 자산 보기
규정준수대시보드	보고서보기	보고 대시보드, 보고서 설정 보기 및 보고서 다운로드
규정준수대시보드	보고서관리	보고서 생성 및 삭제
규정준수대시보드	보고서설정 관리	보고서 설정 수정
리미디에이션 대시보드	보기교정작업	교정 작업 보기
리미디에이션 대시보드	보기교정 이정표	교정 이정표 보기
리미디에이션 대시보드	관리개선작업	사용자 작업 생성, 삭제, 보관 및 처리와 같은 교정 작업 관리
규정준수 작업	규정준수 작업 보기	규정 준수 작업 및 실행 보기
규정준수 작업	규정준수작업 관리	규정 준수 작업 관리
규정준수구성	규정준수구성 보기	정책, 블록, 규칙, 블록 생성, 블록 식별자 및 TTP 템플릿과 같은 규정 준수 컨피그레이션 보기
규정준수구성	규정준수정책 관리	규정 준수 정책 관리
규정준수구성	컴플라이언스블록 관리	컴플라이언스 블록 및 규칙 및 블록 식별자 관리
규정준수구성	컴플라이언스블록생성 관리	컴플라이언스 블록 생성 및 TTP 템플릿 관리

사전 정의된 역할

컨피그레이션 컴플라이언스 및 리미디에이션 활용 사례에는 아래 표에 나열된 사전 정의된 역할이 있습니다.

✎ 참고: 관리자는 고객 요구 사항에 따라 역할을 생성하거나 업데이트할 수 있습니다.

역할	설명	권한
규정 준수 관리자	모든 규정 준수 관련 권한이 있는 관리자 역할	UI 애플리케이션: 자산 관리자 표시 - 자산 그룹 표시 - 규정 준수 대시보드 보기 - 규정 준수 작업 표시 - 규정 준수 구성 표시 자산: 자산 목록 보기 - 자산에 대한 백업 구성 보기 - 백업 구성 - 컨트롤러 지원 디바이스 작업 수행 자산 그룹: - 자산 그룹 보기 - 자산 그룹 관리 - 동적 자산 그룹 생성 백업 구성: 디바이스 컨피그레이션 백업 보기, 비교 및 다운로드 백업 복원 정책: 백업 복원 정책 보기 규정 준수 대시보드: - 자산의 규정 준수 요약 보기 - 정책의 컴플라이언스 요약 보기 - 위반 보기

역할	설명	권한
		- 영향을 받는 자산 보기 보고서 생성 및 삭제 보고 대시보드, 보고서 설정 보기 및 보고서 다운로드 보고서 설정 수정: 규정 준수 작업 규정 준수 작업 및 실행 보기 - 규정 준수 작업 관리 규정 준수 구성: - 정책, 블록, 규칙 등의 규정 준수 구성 보기 - 규정 준수 정책 관리 - 컴플라이언스 블록, 규칙 및 블록 식별자 관리 - 컴플라이언스 블록 생성 및 TTP 템플릿 관리 UI 애플리케이션: - Asset Manager 표시 - 자산 그룹 표시 - 규정 준수 대시보드 보기 - 규정 준수 작업 표시 - 규정 준수 구성 표시
컴플라이언스 연산자	컨피그레이션 관리를 제외한 모든 컴플라이언스 권한이 있는 운영자 역할	자산: 자산 목록 보기 - 자산에 대한 백업 구성 보기 - 백업 구성 - 컨트롤러 지원 디바이스 작업 수행 자산 그룹: - 자산 그룹 보기 - 자산 그룹 관리 - 동적 자산 그룹 생성 백업 구성: 디바이스 컨피그레이션 백

역할	설명	권한
규정 준수 읽기 전용	규정 준수 활용 사례와 관련된 모든 읽기 전용 권한을 제공합니다.	업 보기, 비교 및 다운로드 백업 복원 정책: 백업 복원 정책 보기 규정 준수 대시보드: - 자산 규정 준수 요약 보기 - 정책 준수 요약 보기 - 위반 보기 - 영향을 받는 자산 보기 보고서 생성 및 삭제 보고 대시보드, 보고서 설정 보기 및 보고서 다운로드 규정 준수 작업: 규정 준수 작업 및 실행 보기 - 규정 준수 작업 관리 규정 준수 구성: 정책, 블록, 규칙과 같은 규정 준수 컨피그레이션 보기 UI 애플리케이션: - Asset Manager 표시 - 자산 그룹 표시 - 규정 준수 대시보드 보기 - 규정 준수 작업 표시 - 규정 준수 구성 표시 자산: 자산 목록 보기 - 자산에 대한 백업 구성 보기 - 컨트롤러 지원 디바이스 작업 수행 자산 그룹: - 자산 그룹 보기 백업 구성: 디바이스 컨피그레이션 백업 보기, 비교 및 다운로드

역할	설명	권한
리미디에이션 관리자/리미디에이션 운영자	모든 리미디에이션 관련 권한이 있는 운영자 역할	백업 복원 정책: 백업 복원 정책 보기 규정 준수 대시보드: 자산 규정 준수 요약 보기 - 정책 준수 요약 보기 - 위반 보기 - 영향을 받는 자산 보기 보고 대시보드, 보고서 설정 보기 및 보고서 다운로드 규정 준수 작업: 규정 준수 작업 및 실행 보기 규정 준수 구성: 정책, 블록, 규칙과 같은 규정 준수 컨피그레이션 보기 UI 애플리케이션: - Asset Manager 표시 - 자산 그룹 표시 - 교정 대시보드 보기 자산: - 자산 목록 보기 자산 그룹: - 자산 그룹 보기 자산 그룹 관리 - 동적 자산 그룹 생성 교정 대시보드: - 교정 작업 보기 - 교정 이정표 보기 - 자산 규정 준수 요약 보기 - 생성, 삭제, 아카이브, 사용자 작업 처리와 같은 교정 작업 관리

역할	설명	권한
교정 읽기 전용	교정 사용 사례와 관련된 모든 읽기 전용 권한을 제공합니다.	- 영향을 받는 자산 보기 UI 애플리케이션: - Asset Manager 표시 - 자산 그룹 표시 - 교정 대시보드 보기 자산: - 자산 목록 보기 자산 그룹: - 자산 그룹 보기 동적 자산 그룹 생성 교정 대시보드: - 교정 작업 보기 - 교정 이정표 보기 - 자산 규정 준수 요약 보기 - 영향을 받는 자산 보기

액세스 정책

액세스 정책 기능을 사용하면 사용자가 특정 규정 준수 정책 및 자산 그룹에 적절히 액세스할 수 있습니다. 이 기능은 관리자가 사용자 역할 및 책임을 기반으로 액세스 제어를 정의하고 적용할 수 있도록 함으로써 보안 및 운영 효율성을 향상시킵니다. 액세스 정책은 Access Policy 페이지를 통해 관리됩니다. 이 페이지에서 관리자는 정책을 생성, 수정 및 사용자 또는 그룹에 할당할 수 있습니다. 관리자는 각 사용자 또는 그룹이 보거나 편집하거나 관리할 수 있는 규정 준수 정책 및 자산 그룹을 지정하여 세분화된 권한을 정의할 수 있습니다. 이러한 수준의 세부 정보를 통해 민감한 정보 및 중요한 작업에 대한 엄격한 제어를 유지할 수 있습니다.

액세스 정책이 정의되면 현재 사용자가 액세스할 수 있는 CnR 정책 및 자산 목록을 기반으로 Next-Gen UI의 모든 컴플라이언스 및 리미디에이션 페이지에서 데이터가 제한됩니다.

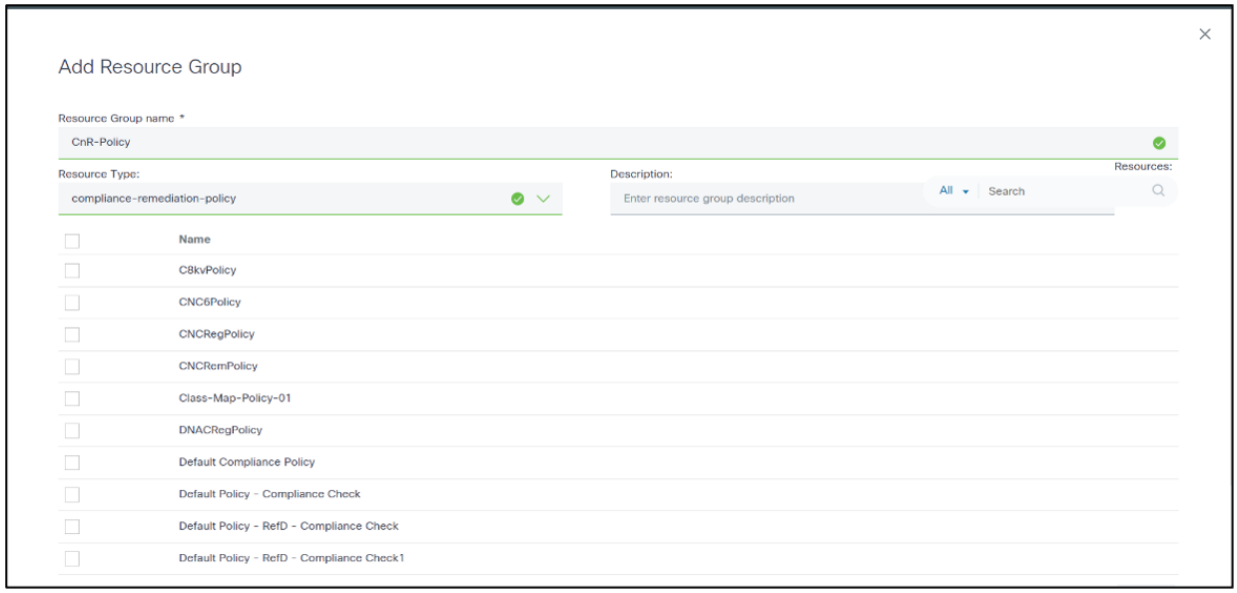
사용자 액세스를 제공하려면

참고: 권한은 관리자만 제공할 수 있습니다.

1. 사용자를 생성하고 사용자 그룹에 할당합니다.
2. 사용자 역할을 생성하고 생성된 사용자 그룹에 할당합니다.
3. 자산 그룹에 자산을 추가합니다.
4. 규정 준수 정책 리소스를 할당할 리소스 그룹을 만듭니다.
5. 액세스 정책을 생성하고 관련 사용자 그룹, 자산 그룹 및 리소스 그룹을 선택합니다.

리소스 그룹 생성

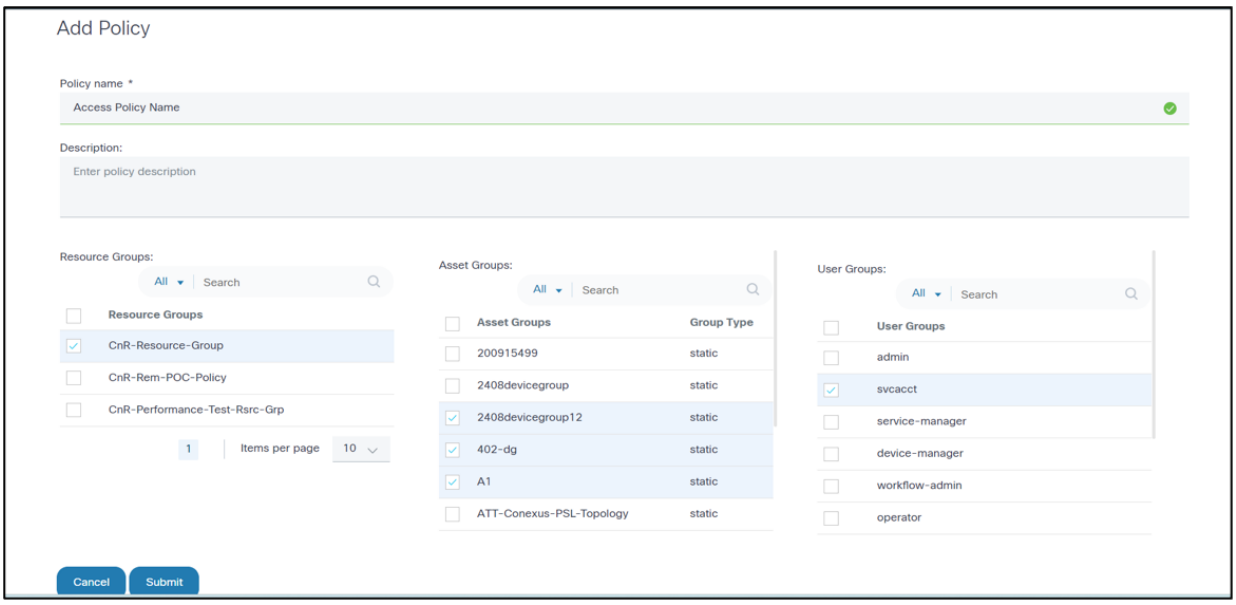
Resource Type(리소스 유형) 드롭다운 목록에서 규정준수 교정 정책을 사용하여 리소스 그룹을 생성하고 각 사용자 그룹에 대한 액세스 권한을 부여해야 하는 규정준수 정책을 선택합니다.



리소스 그룹 만들기

액세스 정책 생성

사용자 그룹에 권한을 부여할 필요가 있는 리소스 그룹 및 자산 그룹으로 액세스 정책을 생성합니다.



액세스 정책 생성

오프라인 규정 준수

오프라인 규정 준수 기능을 사용하면 사용자가 자산 인벤토리의 활성 디바이스를 통해 사용할 수 없는 디바이스 컨피그레이션에 대해 규정 준수 확인을 실행할 수 있습니다.

사용자는 디바이스 백업 구성을 사용하거나 규정 준수 작업에서 오프라인 감사를 생성하여 오프라인 규정 준수를 실행할 수 있습니다. 실행 결과는 규정 준수 대시보드에서 볼 수 있습니다.

디바이스 백업 컨피그레이션 사용

관리자는 원하는 디바이스 세트에 대한 실행 컨피그레이션이 포함된 zip 파일을 수동으로 업로드할 수 있습니다. 이 기능은 Backup & Restore(백업 및 복원) 애플리케이션의 Device Config - Upload(디바이스 구성 - 업로드) 섹션에서 사용할 수 있습니다. 디바이스 컨피그레이션이 업로드되면 디바이스 백업 컨피그레이션을 디바이스 컨피그레이션의 소스로 선택하여 원하는 디바이스에 대한 규정 준수 작업을 생성할 수 있습니다. 실행 중에 업로드된 디바이스 컨피그레이션이 백업 애플리케이션에서 검색되고 해당 컨피그레이션에서 컴플라이언스 검사가 실행됩니다.

규정준수 작업에서 오프라인 감사 생성 기능 사용

오프라인으로 디바이스 컨피그레이션에 대한 컴플라이언스를 실행하려면 사용자는 Compliance Jobs(컴플라이언스 작업) 페이지의 More Options(추가 옵션) 아이콘에서 Offline Audit(오프라인 감사)을 선택할 수 있습니다. 이를 통해 사용자는 실행 중인 컨피그레이션이 포함된 zip 파일을 Compliance 애플리케이션에서 직접 업로드할 수 있습니다. 실행 중에 업로드된 디바이스 컨피그레이션이 구문 분석되고 컴플라이언스 검사가 실행됩니다.

Ingester를 통한 구성 구축

Ingester 프레임워크를 사용하여 규정 준수 구성 아티팩트의 로드를 자동화할 수 있습니다. 아티팩트가 개발되면 다음 단계를 통해 대상 환경으로 내보내고 패키지화하여 구축할 수 있습니다.

- 다음 명령을 사용하여 NPM 패키지를 만듭니다.

```
mkdir <


      >
cd  <


       >
npm init (press "enter" for all prompts)
```

- BPA 포털에서 컨피그레이션 내보내기(기본 UI)
    - BPA Classic UI(BPA 클래식 UI) > Configuration Compliance & Remediation(컨피그레이션 규정 준수 및 교정) > Configurations(컨피그레이션)로 이동합니다
    - "TTP 템플릿/블록 식별자/블록/규칙/정책" 내보내기
- 내보낸 파일의 이름을 다음과 같이 바꿉니다.
    - TTP 템플릿: <<filename>>.cnrttptemplate.json
    - 블록 식별자: <<filename>>.cnrblockidentifier.json
    - 블록: <<filename>>.cnrblock.json
    - 규칙: <<filename>>.cnrrule.json
    - 정책: <<filename>>.cnrpolicy.json
- 패키지 ingester 데이터(.tgz)
    - 내보낸 모든 파일을 "1단계"에서 생성한 npm 패키지에 복사
    - npm 패키지 내에서 npm pack 명령을 실행하여 ".tgz" 파일을 만듭니다
- BPA 단일 노드 환경 내에 인제스터 데이터(.tgz) 구축
    - .tgz 파일을 BPA 번들이 구축된 서버의 <<BPA core bundle>/packages/data 폴더에 복사합니다.
    - Ingester 서버를 다시 시작합니다(docker ingester-service 다시 시작).
- BPA 다중 노드 환경에 인제스터 데이터(.tgz) 구축
    - .tgz 파일을 키 차트가 배포된 서버의 /opt/bpa/packages/data 폴더에 복사합니다.

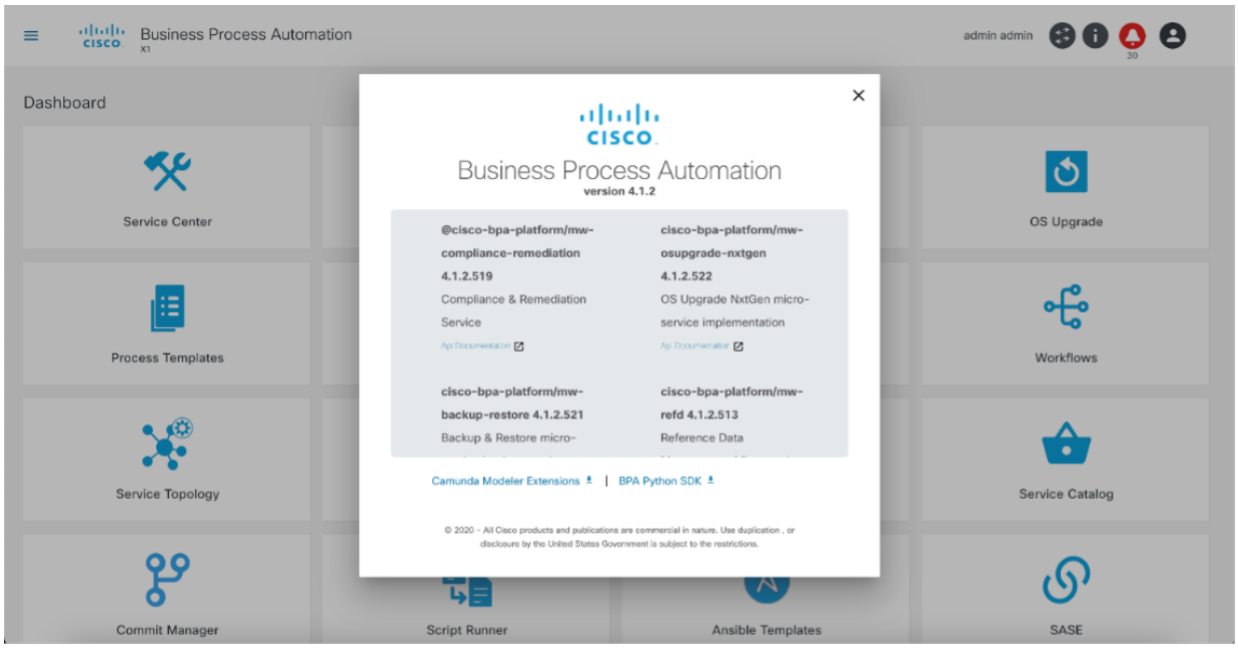
- Ingester pod 재배포(`kubectl 배포 재시작 배포 ingester-service -n bpa-ns`)

참조

이름	설명
TTP	컨피그레이션 블록에 사용되는 템플릿 텍스트 파서
전화회의 파서	CLI 장치 구성을 구문 분석하는 데 사용되는 구성 필드 파서

API 설명서

규정 준수 및 교정에 대한 API 설명서 세부 정보는 클래식 UI About(정보) 팝업에서 확인할 수 있습니다.



BPA 정보(클래식 UI)

문제 해결

대시보드

최근 준수 작업 결과가 표시되지 않음

관찰: 최신 규정 준수 작업 결과는 Next-Gen 포털 대시보드에 표시되지 않습니다.

잠재적 원인 1: 대시보드에는 "Current Month(현재 월)"로 기본 설정된 날짜 범위가 선택되어 있습니다. 새 월이 최근에 시작된 경우(예: 오늘이 월의 첫 번째 날), 어제(이전 달의 마지막 날) 이전에 실행된 실행이 표시되지 않습니다.

분석: 대시보드에서 올바른 날짜 범위(필요한 경우 전월 날짜 포함)가 선택되어 있는지 확인하여 적절한 위반 데이터를 표시합니다.

잠재적 원인 2: 다른 사용자가 동일한 정책 및/또는 자산 조합에서 규정 준수 작업을 실행했을 수 있습니다. 대시보드에는 선택한 날짜 범위 내에서 최근 실행 중에 발견된 위반이 표시됩니다.

분석: 관리자(또는 모든 규정 준수 작업에 대한 액세스 권한이 있는 사용자)는 규정 준수 작업 목록 및 해당 기록을 검토하여 어떤 정책 또는 자산 그룹 조합이 실행되는지 확인합니다.

규정 준수 작업

전체 실행 상태가 "Skipped"로 설정됨

관찰: 규정 준수 작업을 실행하는 동안 전체 실행 상태가 "건너뜀"으로 표시됩니다. 위반 사항은 보고되지 않습니다.

잠재적 원인: 동일한 작업에 대한 기존 실행이 아직 실행 중입니다.

분석: 규정 준수 작업은 특정 시점에서 실행 중 상태로 하나의 실행만 수행할 수 있습니다. 이전 실행이 여전히 실행 중인지 확인합니다. 장기간 중단되거나 실행 중인 실행은 종료할 수 있습니다.

디바이스 상태가 "Skipped"로 설정됨

관찰: 규정 준수 작업 실행에서 일부 디바이스의 상태가 "Skipped(건너뜀)"로 표시됩니다.

잠재적 원인: 해당 장치가 속한 컨트롤러 유형에 대해 규정준수 기능이 활성화되지 않았습니다.

분석: 규정 준수 정책은 기능이 활성화된 자산 그룹 내의 디바이스에만 적용됩니다.

디바이스 상태가 "Failed(실패)"로 설정됨

관찰: 규정 준수 작업 실행에서 일부 디바이스의 상태가 "실패"로 표시됩니다.

잠재적 원인: 규정 준수 실행 프로세스 중에 발생한 런타임 오류입니다. 이러한 오류는 코드 오류이

거나 정책, 블록, 규칙, 블록 식별자 등의 잘못된 구성일 수 있습니다.

분석:

런타임 오류의 이유를 찾는 API:

1. 실행 ID를 찾기 위해 실행 가져오기

   API: /api/v1.0/compliance-remediation/

   컴플라이언스 실행

   방법: 가져오기
2. 실행 ID를 사용하여 장치 실행 가져오기

   API: /api/v1.0/compliance-remediation/

   컴플라이언스 디바이스 실행 여부

   executionId=<< execution-id >>

   방법: 가져오기

규정 준수 규칙

규칙 표시 빈 값

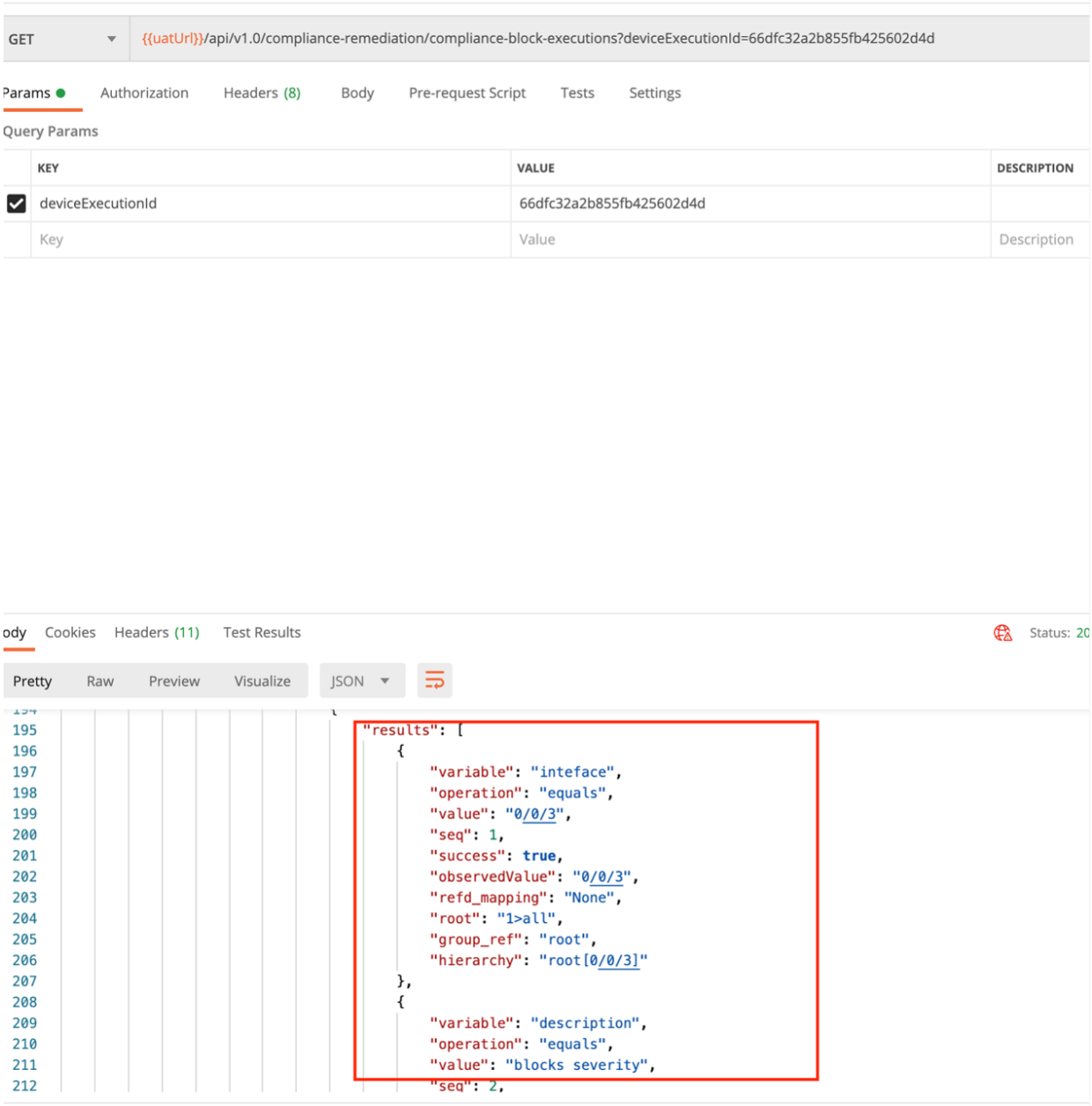
관찰: 규정 준수 작업을 실행하는 동안 규칙 변수에 빈 값이 표시됩니다.

분석:

1. RefD 애플리케이션에서 데이터를 검색하는 경우 RefD 키가 올바른 형식인지 확인합니다. 해당하는 경우 RefD 응용 프로그램에 규칙의 규정 준수 변수에 연결된 키에 대한 데이터가 있는지 확인합니다. 또한 규정 준수 서비스 로그를 확인하여 규정 준수 앱에서 올바른 RefD 키를 보내고 있는지 확인합니다. 규칙 및 비 RefD 규칙에서 규칙 계층 구조 및 RefD 통합 이해를 참조하십시오.
2. 다음 API를 사용하여 컴플라이언스 블록 실행 결과를 확인합니다.

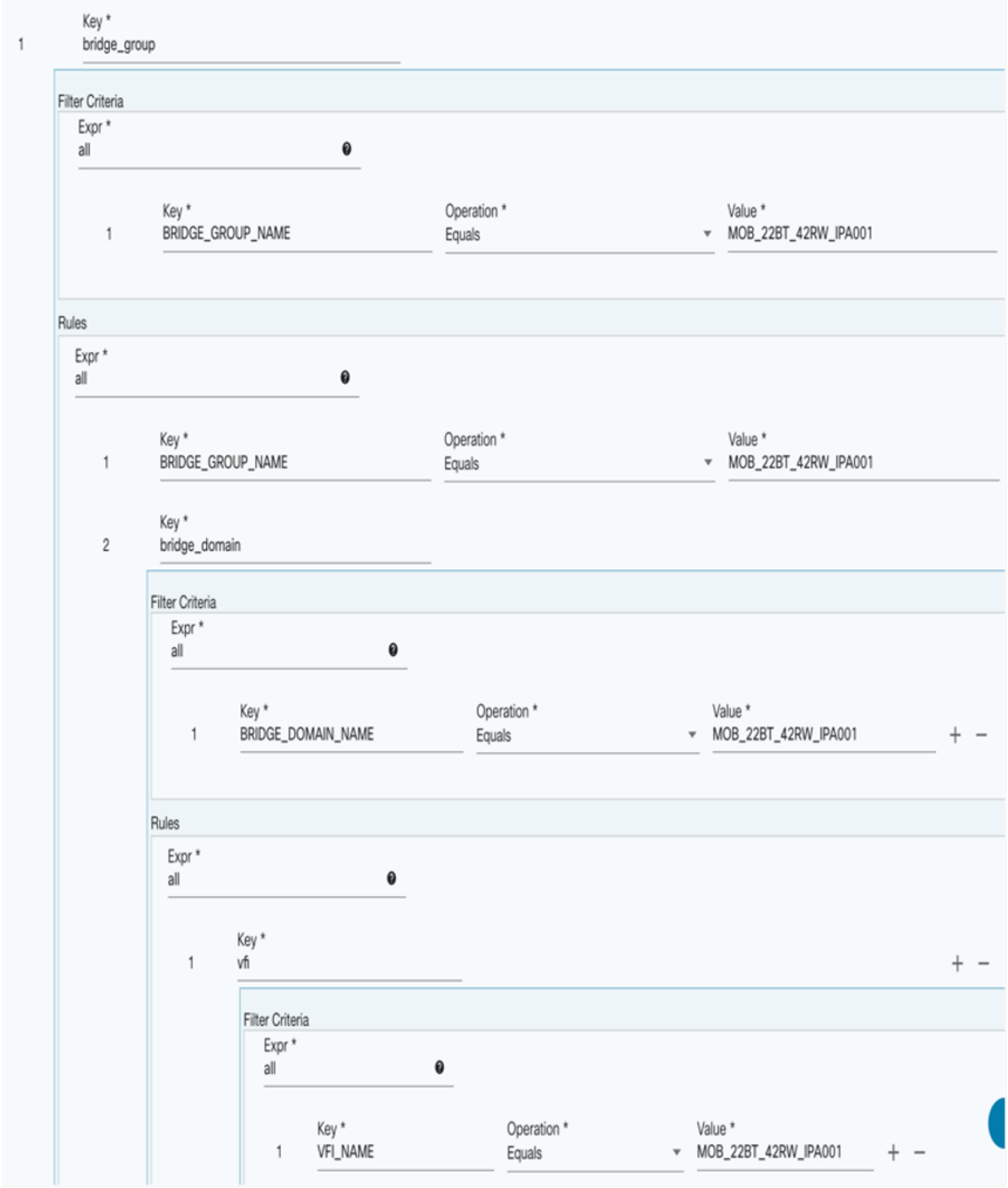
   URL: /api/v1.0/compliance-remediation/compliance-block-execution?deviceExecutionId=<>

   방법: 가져오기



컴플라이언스 블록 실행 결과

3. 블록에 하위 계층이 있는지 아니면 단일 계층이 있는지 확인하고 계층에 따라 규칙이 구성되었는지 확인합니다.



컴플라이언스 블록 실행 결과

4. 다음 python 스크립트를 실행하여 TTP 파서가 디바이스 컨피그레이션에서 값을 추출하는지 확인합니다.

```
from ttp import ttp
### Provide device config inside the below variable
data_to_parse = """
"""

### Provide block config inside the below variable
ttp_template = """
```

```
"""

### Create parser object and parse data using template:
parser = ttp(data=data_to_parse, template=ttp_template)
parser.parse()

### Check results and see if TTP parser extracts the value or not
results = parser.result()
print(results)
```

규정 준수 로그 모니터링

단일 노드 환경:

```
docker logs -f compliance-remediation-service
```

다중 노드 Kubernetes 환경:

```
kubectl logs -f services/compliance-remediation-service -n bpa-ns
```

Kibana 로그 모니터링:

```
https://<< BPA 호스트 >>:30401
```

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.