

Cisco IQ Virtual Appliance 운영 가이드 v1.2.0

소개

Cisco IQTM은 자산 가시성을 개선하고, 환경 전반에서 더 스마트한 통찰력을 제공하며, 케이스 관리를 능률화할 수 있도록 설계된 향상된 기능과 기능을 제공합니다. 또한, Cisco IQ AI Assistant와 같은 AI 기능은 사전 대응적이고 정보에 입각한 결정을 내리고 고객 참여와 성공을 위한 프로세스를 간소화할 수 있는 상황 인식 기능을 제공하여 운영 성과와 Cisco IQ 사용자 경험을 최적화합니다.

Cisco IQ On-Prem Air-Gapped는 Cisco IQ의 구축 모드 중 하나로, 엄격한 규정 준수, 데이터 주권, 보안 요구 사항을 가진 고도로 규제받는 업계의 고객을 위해 설계되었습니다. 이 모드에서 Cisco IQ는 Cisco IQ VA(Virtual Appliance)라고 하는 자체 내장 VM(Virtual Machine)으로 제공됩니다. VA는 전적으로 고객의 구내에서 실행되며 외부 네트워크와 완전히 격리되어 작동합니다. 이러한 격리를 유지하기 위해 소프트웨어 업데이트 및 유지 관리 패키지는 Cisco IQ SaaS에서 가져온 다음 승인된 수동 프로세스를 통해 VA로 전송됩니다.

Cisco IQ On-Prem Air-Gapped는 Cisco IQ SaaS의 주요 기능을 에어 갭(air-gapped) 환경으로 확장하여 미션 크리티컬 팀이 클라우드 연결 엔터프라이즈에 버금가는 속도와 진단 인텔리전스로 운영할 수 있도록 합니다.

Cisco IQ VA에 액세스하려면 지원되는 브라우저를 열고 <https://<fqdn-of-the-appliance>>로 이동합니다. 설치 과정에서 설정된 관리자 사용자 이름 및 비밀번호를 사용하여 로그인합니다.

 참고: Cisco IQ VA는 현재 Controlled Availability 프로그램에 등록된 고객만 사용할 수 있습니다. Cisco IQ 포털에서 VA 시스템 소프트웨어 및 추가 운영 패키지(모듈, 규칙, 자격)에 대한 다운로드 액세스는 일부 고객에게만 독점적으로 제공됩니다. 자세한 내용은 어카운트 담당자에게 문의하십시오.

연결 관리(데이터 수집)

Cisco IQ VA는 네트워크 데이터 수집을 위한 온프레미스 솔루션으로 인프라에 대한 심층적인 가시성을 제공합니다. Catalyst Center 및 Direct Connection을 통해 데이터를 수집합니다. 네트워크 인증 및 디바이스 검색을 관리하는 방법이 간소화됩니다. 데이터 수집 구성은 다음으로 구성됩니다.

- 크리덴셜 세트 생성: 네트워크 디바이스와 통신하기 위한 인증 프로토콜(예: SNMP(Simple Network Management Protocol) v1/v2c/v3)을 설정합니다. 보안 영역 또는 위치별로 자격 증명을 중앙 집중화하면(예: "SanJose-SNMPv3") 한 위치에서 비밀번호를 업데이트할 수 있으며, 변경 사항이 모든 관련 디바이스에 자동으로 전파됩니다.

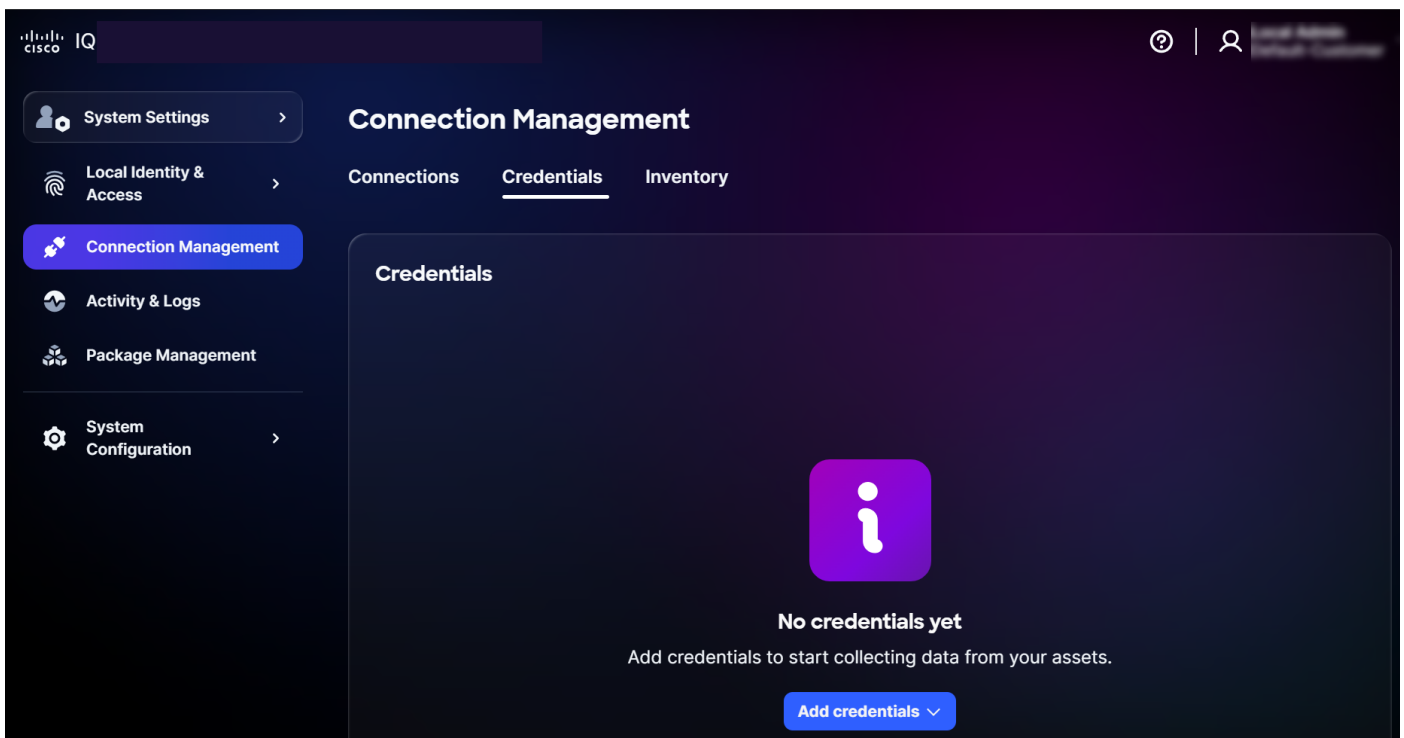
- 자격 증명을 인벤토리에 매핑: 인증 프로세스를 자동화하기 위해 크리덴셜 세트를 인벤토리 자산과 매핑합니다. 특정 IP 범위를 정의된 자격 증명 집합에 연결하는 규칙을 생성하면 시스템은 데이터 수집 중에 올바른 인증을 자동으로 적용합니다. 이렇게 하면 수동 입력 오류가 제거되고 네트워크 확장에 따라 컨피그레이션이 정확하게 유지됩니다.

 참고: 디바이스 검색을 위해서는 SNMPv2c/SNMPv3 및 SSH가 필요하며, Catalyst Center를 구성하기 전에 HTTP/HTTPS 자격 증명을 제공해야 합니다.

자격 증명 추가

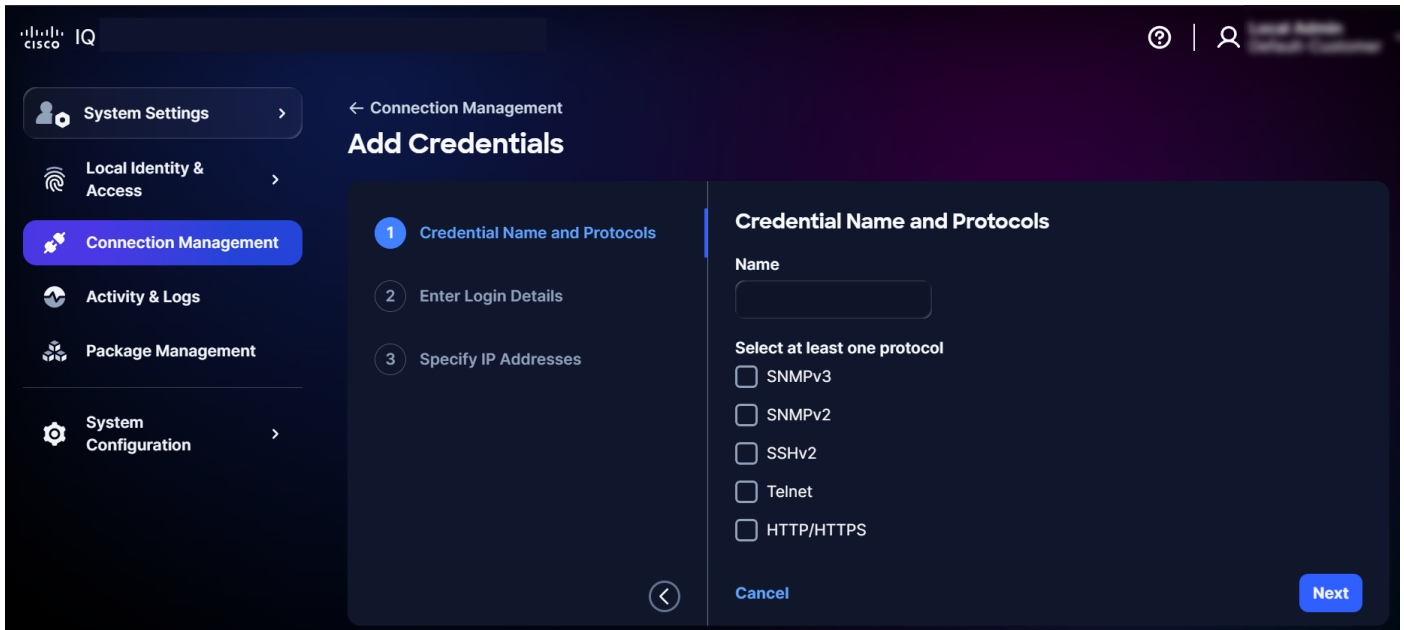
데이터 수집을 수행하려면 먼저 자격 증명을 추가해야 합니다. 자격 증명을 추가하려면

1. System Settings(시스템 설정)에서 Connection Management(연결 관리)를 선택합니다. Connection Management 페이지가 표시됩니다.
2. Credentials(자격 증명) 탭을 클릭합니다.



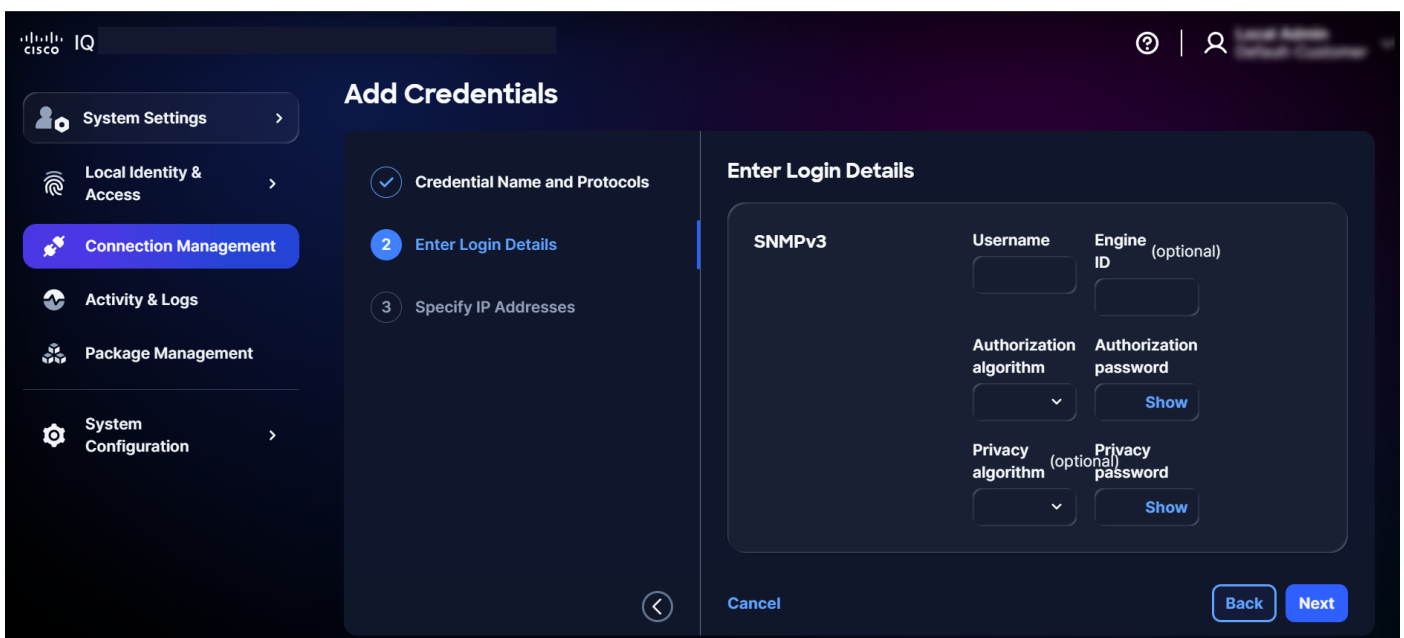
자격 증명 탭

3. Add credentials(자격 증명 추가)를 클릭합니다.



자격 증명 추가

4. 이름을 입력합니다.
5. 해당되는 모든 프로토콜 확인란을 선택합니다.
6. Next(다음)를 클릭합니다.



자격 증명 추가 세부 정보

 참고: 상기 이미지에 대해, 이전 단계에서 모든 프로토콜들이 선택될 때의 뷰가 예시된다. 인터페이스에는 선택한 프로토콜만 표시됩니다.

7. 선택한 각 프로토콜에 대한 로그인 세부 정보를 입력합니다.

8. Next(다음)를 클릭합니다.

IP 주소 지정

9. Included IPs(포함된 IP)를 입력합니다.

 참고: 이 필드는 접속 설정에 자격 증명을 사용할 수 있는 IP 주소 또는 IP 범위를 정의합니다. IP와 IP 마스크의 혼합을 지원합니다(와일드카드 표기법 사용). 지원되는 형식에 대한 자세한 내용은 자격 증명 [선택 및 일치 논리를 참조하십시오](#).

10. 저장을 클릭합니다. 확인 메시지가 표시되고 Credentials(자격 증명) 탭으로 리디렉션됩니다.

Name	Protocol	Included IPs
[Redacted]	HTTP/HTTPS	[Redacted]

추가된 자격 증명

Edit(수정) 아이콘을 클릭하여 자격 증명을 수정하고 Delete(삭제) 아이콘을 클릭하여 자격 증명을 삭제할 수 있습니다.

자격 증명 선택 및 일치 논리

텔레메트리 엔진은 우선순위 기반 일치 논리를 사용하여 검색 및 수집 중에 적용할 자격 증명을 결정합니다. 이 계층 구조를 이해하면 원하는 디바이스에 올바른 자격 증명이 사용됩니다.

- 우선 순위: 여러 자격 증명 집합이 디바이스에 적용되는 경우 Cisco IQ는 디바이스와 얼마나 정확하게 일치하는지를 기준으로 평가합니다. 시스템은 다음과 같은 우선순위를 적용하며, 더 구체적인 일치 항목이 우선합니다.
 - 정확한 IP 일치: 최우선 순위
 - 후행 와일드카드 일치: 우선순위는 후행 별의 수에 따라 달라집니다. 별이 적을수록 더 구체적인 일치를 나타내므로 우선순위가 높습니다.
- 와일드카드 서식 지정 규칙: 와일드카드(*)는 IP 주소에서 후행 문자로만 지원됩니다. 오른쪽에서 왼쪽으로 적용해야 합니다.
 - 지원되는 형식:
 - 1.2.3.*(가장 높은 우선 순위)
 - 1.2.*
 - 1.*.*
 - *.*.*(최저 우선 순위)
 - 지원되지 않는 형식:
 - 선행 와일드카드(예: *.1.2.3)
 - 옥텟 사이의 와일드카드(예: 10.10.*.20)
 - 대시 또는 기타 비표준 구분 기호 사용

자격 증명 선택 예:

다음 표에서는 디바이스가 여러 정의된 패턴과 일치하는 경우 텔레메트리 엔진이 가장 적합한 크리덴셜 세트를 선택하는 방법을 보여줍니다.

표 1: 자격 증명 선택 예

디바이스 IP	사용 가능한 자격 증명 집합	선택한 자격 증명 집합
10.10.1.5	10.10.1.5, 10.10.1., 10.10..*	10.10.1.5(정확히 일치)
10.10.2.15	10.10.2., 10.10..*	10.10.2.*(자세히)
10.10.5.50	10.10...	10.10... (자세히 설명)

 참고: 디바이스가 여러 개의 중복 카테고리에 속할 경우, 시스템은 항상 가장 높은 특이성(즉,

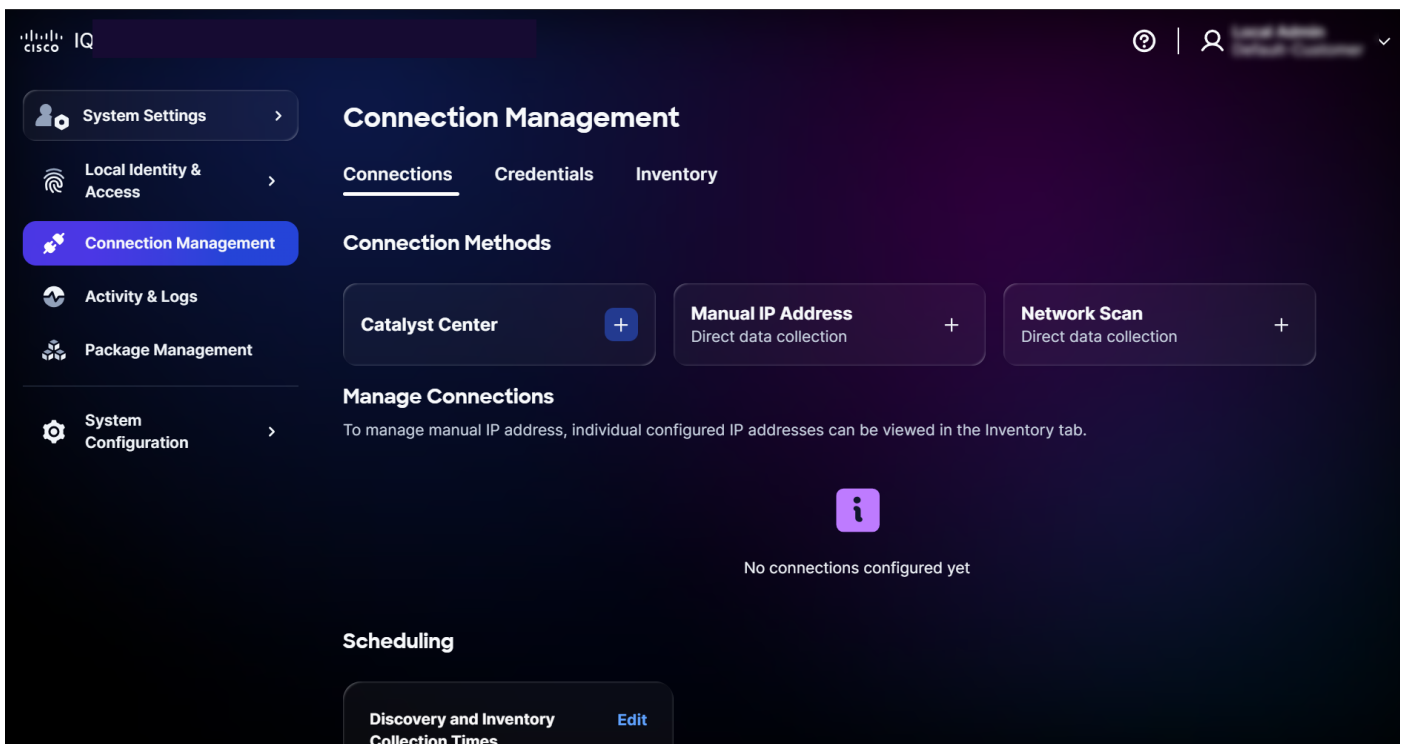
 가장 적은 후행 와일드카드)을 갖는 크리덴셜 세트를 선택합니다.

Catalyst Center를 사용한 데이터 수집

Cisco IQ VA의 각 인스턴스에 대해 최대 20개의 Catalyst Center(비클러스터)를 연결할 수 있습니다.

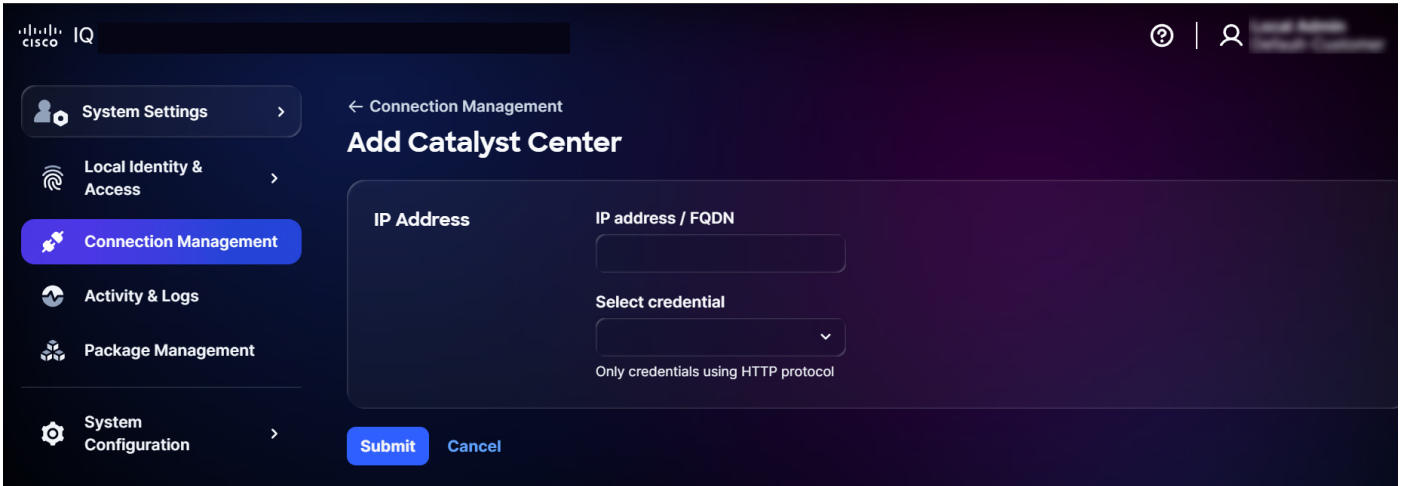
Catalyst Center를 사용한 데이터 수집:

1. System Settings(시스템 설정)에서 Connection Management(연결 관리)를 선택합니다.
Connection Management 페이지가 표시됩니다.



연결 관리

2. Catalyst Center 옵션을 클릭합니다.



Catalyst Center 추가

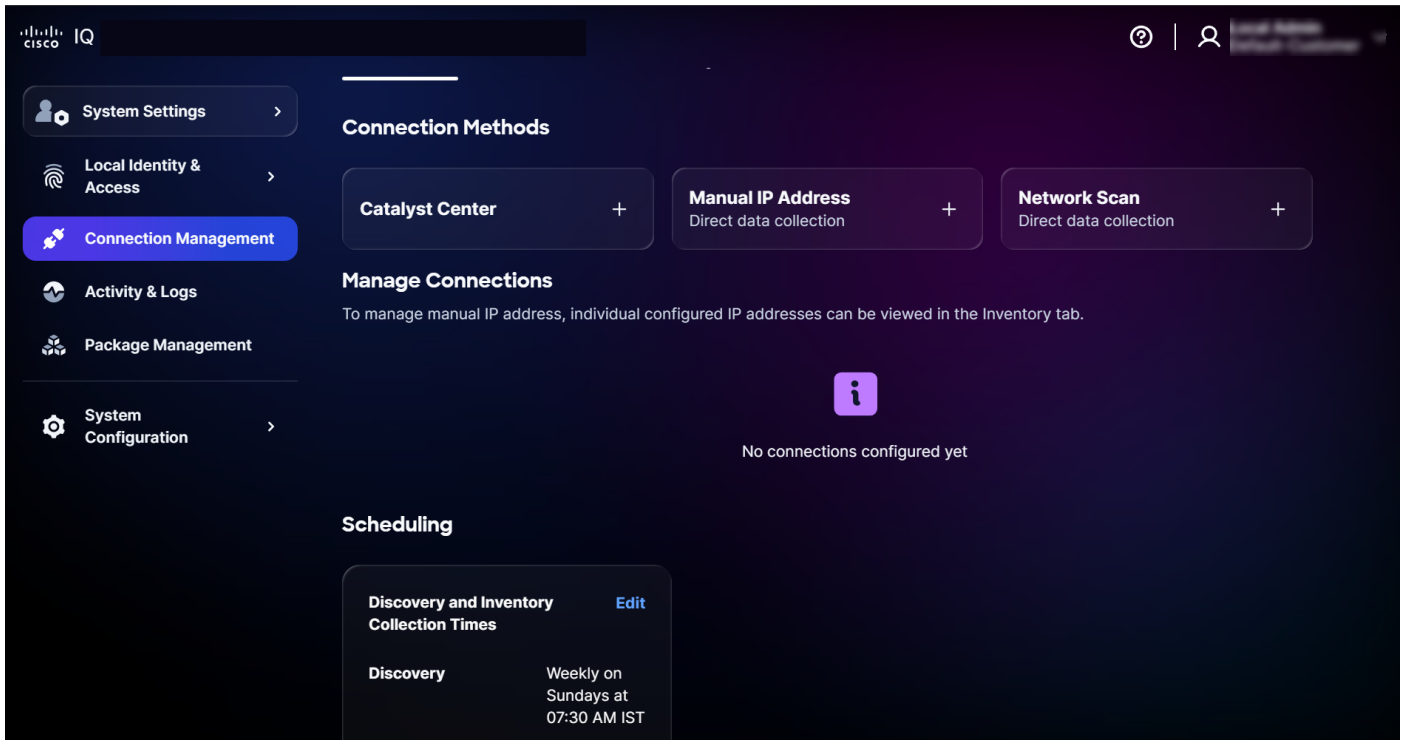
3. IP 주소 또는 FQDN을 입력합니다.
4. Select credential 드롭다운 목록에서 구성된 HTTP/HTTPS 자격 증명을 선택합니다.
5. Submit(제출)을 클릭합니다. 확인 메시지가 표시됩니다(최대 75분 정도 걸릴 수 있음). Configured Connections 아래에서 새로 추가된 Catalyst Center를 볼 수 있습니다.
6. 수집을 예약합니다. 자세한 [내용](#)은 예약을 참조하십시오.

 참고: Cisco IQ VA는 자동화된 스케줄링 설정으로 사전 구성되며 시스템은 기본 자동화된 수집 일정을 시작합니다. 조직의 요구 사항 및 유지 관리 기간에 맞게 일정을 수정하는 것이 좋습니다.

수동 데이터 수집

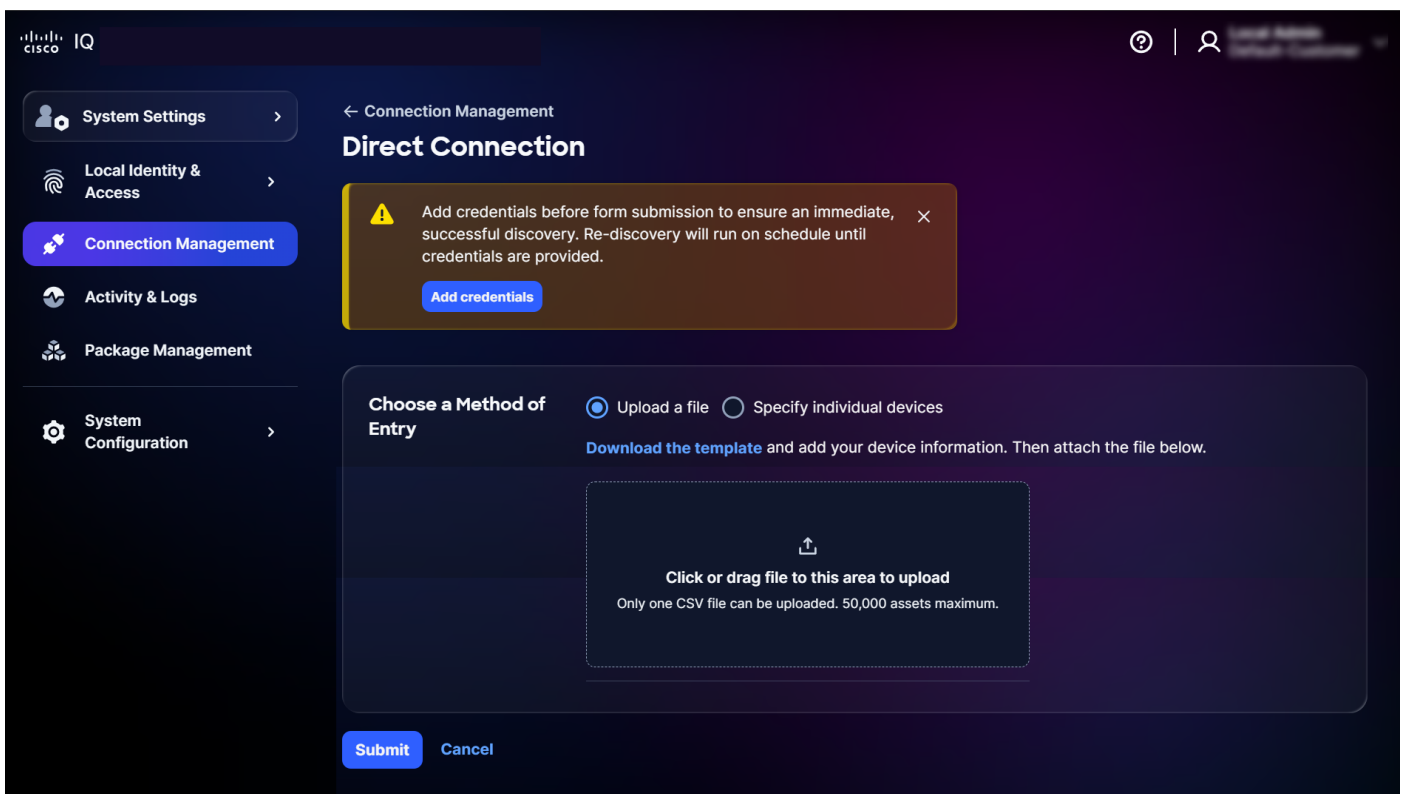
직접 데이터 연결을 위한 디바이스를 추가하려면

1. System Settings(시스템 설정)에서 Connection Management(연결 관리)를 선택합니다. Connection Management 페이지가 표시됩니다.



연결 관리

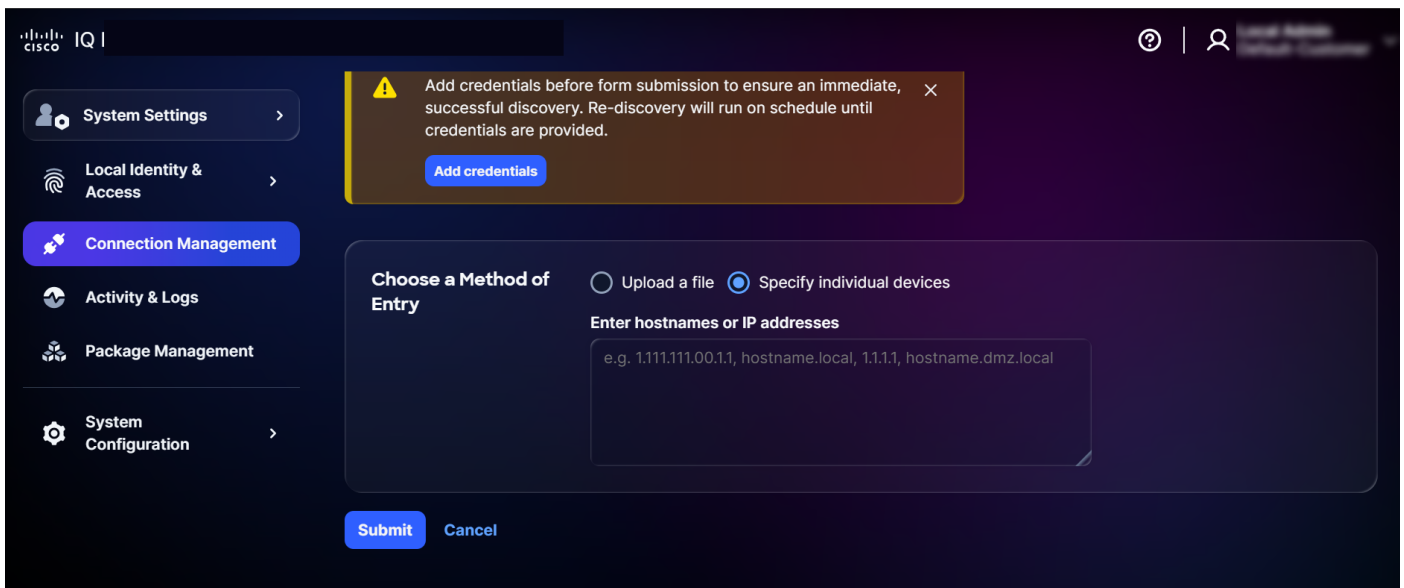
2. Manual IP Address(수동 IP 주소)를 클릭합니다. 데이터를 수집하기 위한 두 가지 옵션이 포함된 직접 연결 페이지가 표시됩니다.



파일 업로드

3. Choose a Method of Entry(입력 방법 선택)에서 preferred(기본) 옵션을 클릭하고 다음 방법 중 하나를 사용하여 장비 정보를 제공합니다.

- 파일 업로드: 파일을 클릭하거나 끌어서 놓습니다.



개별 디바이스 지정

- 개별 장치 지정: 단일 호스트 이름, IP 주소 또는 쉼표로 구분된 호스트 이름 및/또는 IP 주소 목록을 입력합니다

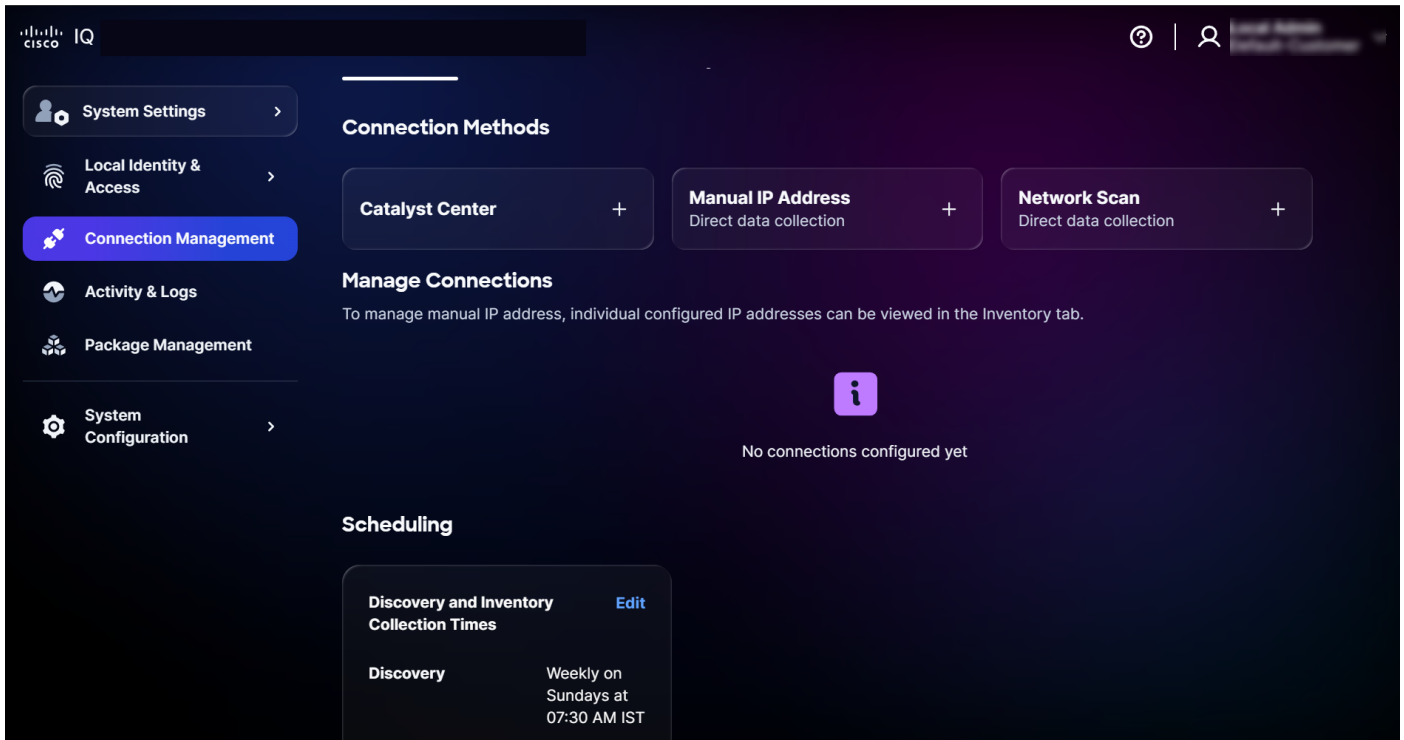
4. Submit(제출)을 클릭합니다. 전송이 성공하면 Assets 탭으로 리디렉션됩니다.

5. 수집을 예약합니다. 자세한 [내용](#)은 예약을 참조하십시오.

 참고: Cisco IQ VA는 자동화된 스케줄링 설정으로 사전 구성되며 시스템은 기본 자동화된 수집 일정을 시작합니다. 조직의 요구 사항 및 유지 관리 기간에 맞게 일정을 수정하는 것이 좋습니다.

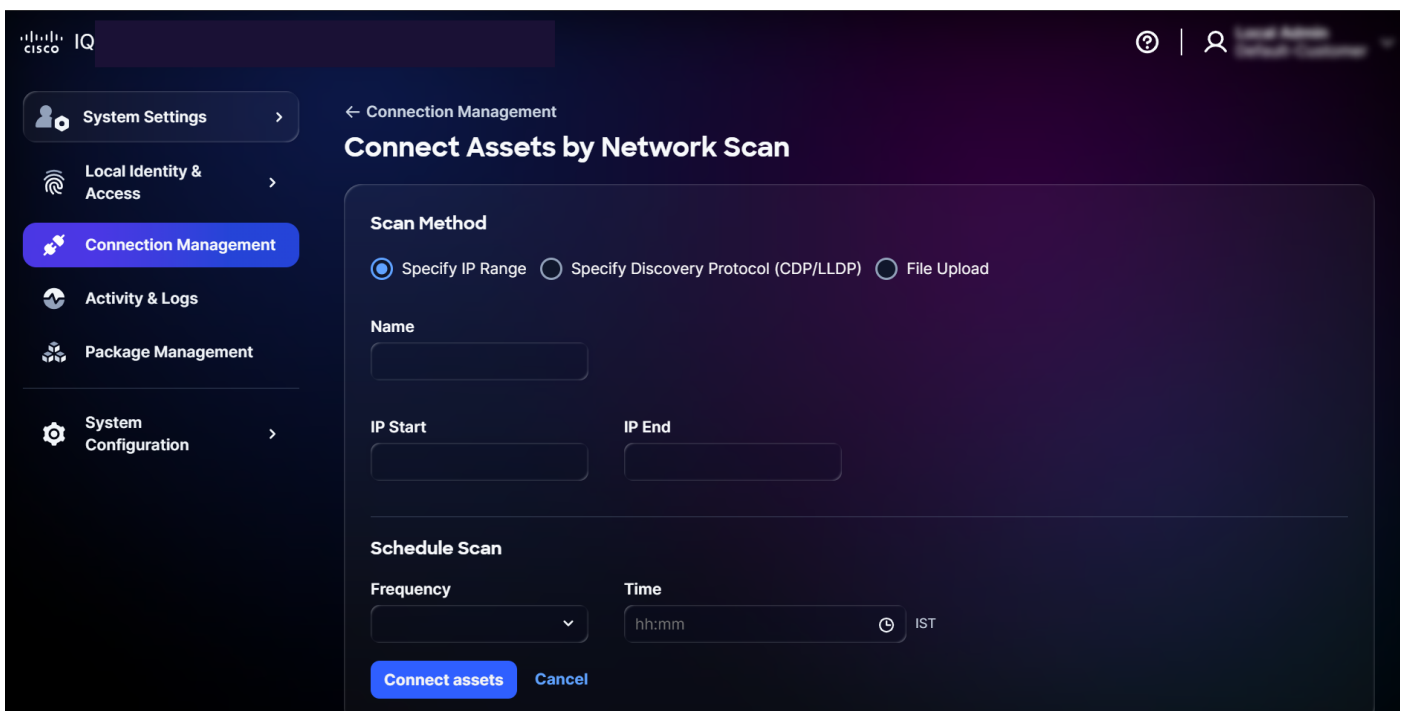
네트워크 검사

1. System Settings(시스템 설정)에서 Connection Management(연결 관리)를 선택합니다. Connection Management 페이지가 표시됩니다.



네트워크 검사

2. Network Scan(네트워크 스캔)을 클릭합니다. Connect Assets by Network Scan(네트워크 스캔별 자산 연결) 페이지가 3가지 옵션과 함께 표시됩니다.



- IP 범위 지정: 네트워크 검색 또는 관리 작업을 위해 해당 범위 내의 대상 장치에 대한 IP 주소 범위를 정의합니다.

- 검색 프로토콜(CDP/LLDP) 지정: 사용할 네트워크 검색 프로토콜 선택
- 파일 업로드: 컨피그레이션 파일 또는 데이터 등의 파일 업로드

3. Name을 입력합니다.

4. IP Start(IP 시작) 및 IP End(IP 종료)를 입력합니다.

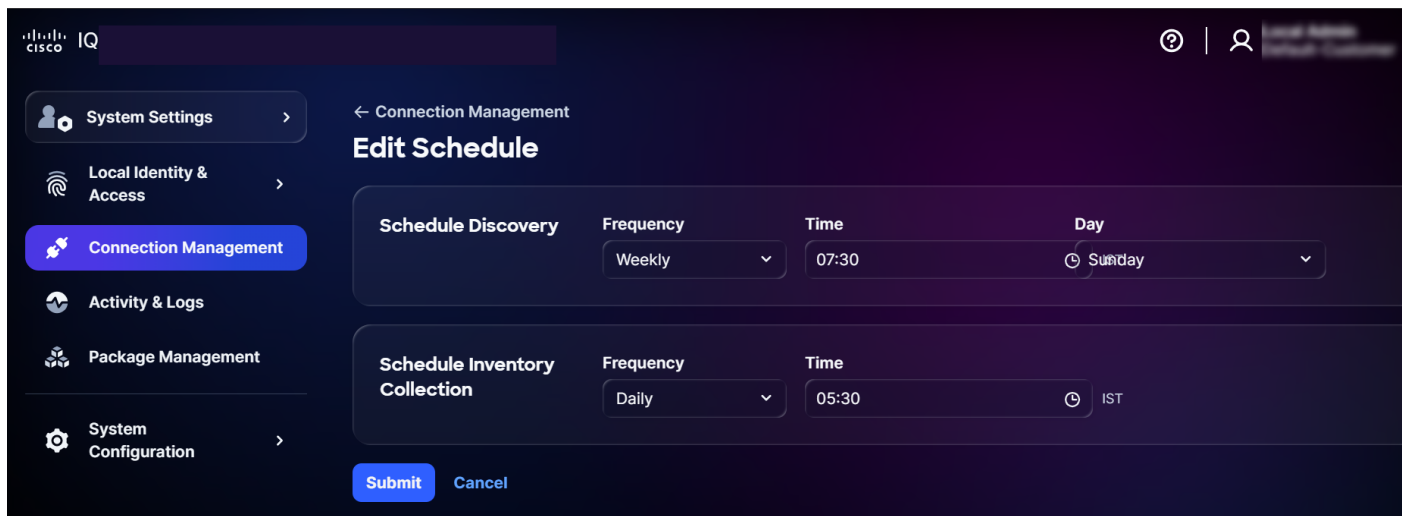
5. Schedule Scan(스캔 예약)에서 Frequency and Time(빈도 및 시간)을 선택합니다.

6. 에셋 연결을 클릭합니다.

예약

스케줄링은 Cisco IQ VA가 자동화된 데이터 수집을 수행하는 시기를 정의할 수 있도록 합니다. 수집을 예약하려면

1. Connection Management 페이지의 Scheduling 섹션에서 수정할 일정에 대해 Edit를 클릭합니다. 일정 편집 페이지가 표시됩니다.



일정 편집

2. Schedule Discovery(검색 예약) 섹션의 드롭다운 목록에서 원하는 빈도 및 일을 선택하고 원하는 시작 시간을 입력합니다.
3. Schedule Inventory Collection(인벤토리 수집 예약) 섹션의 드롭다운 목록에서 원하는 빈도를 선택하고 원하는 시작 시간을 입력합니다.
4. Submit(제출)을 클릭합니다.

 참고: 검색 또는 수집 일정에 대한 변경 사항이 Virtual Appliance 내에서 정확하게 동기화되고 반영될 수 있도록 5~10분 정도 기다립니다.

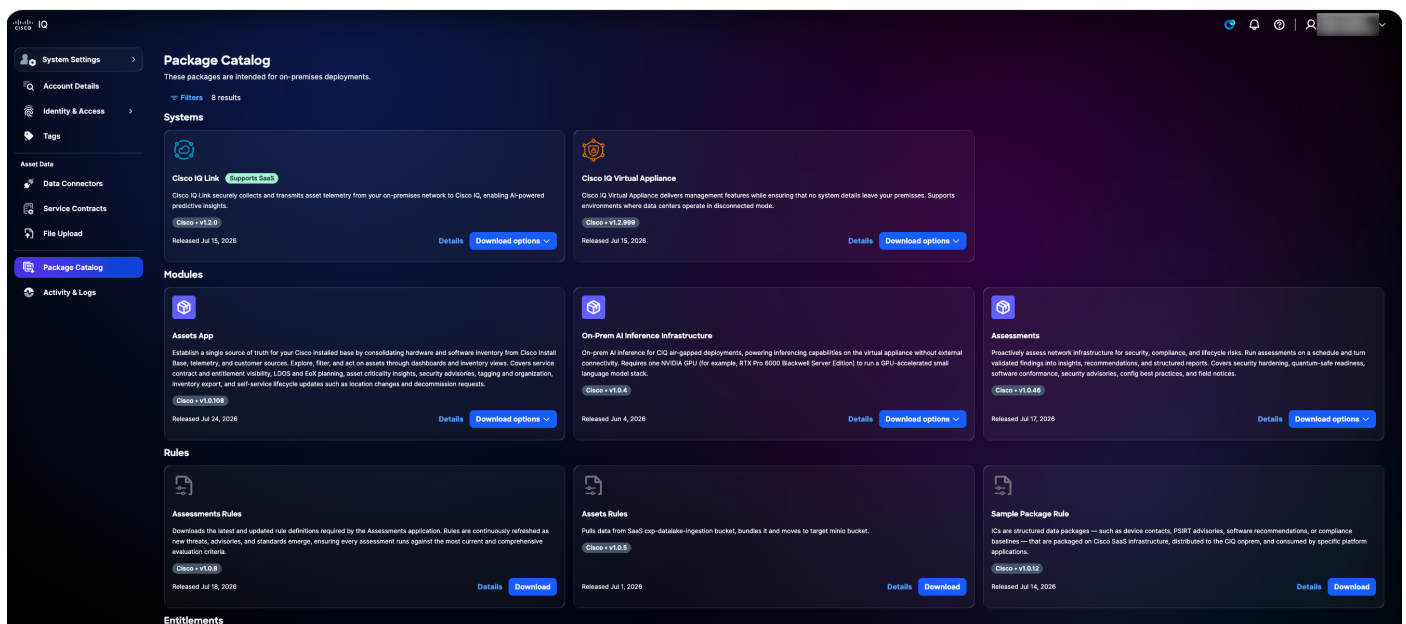
패키지 설치(모듈, 규칙 및 엔타이틀먼트)

VA 내에서 운영 모듈, 규칙, 자격, 특수 AI 기반 기능의 소프트웨어 라이프사이클(설치 및 컨피그레이션)을 관리할 수 있습니다. 패키지 카탈로그로 이동하여 Cisco IQ(SaaS)에서 최신 버전을 다운로드하여 설치할 수 있습니다. 패키지 카탈로그에는 사용 가능한 소프트웨어 인스턴스가 표시됩니다. 또한 업데이트를 원활하게 모니터링 및 관리하여 시스템 인스턴스를 효율적으로 추적 및 관리할 수 있습니다.

모듈 추가

모듈은 VA 내에서 핵심 기능을 제공하는 독립형 소프트웨어 패키지입니다. 자체 라이프사이클을 사용하는 독립적인 서비스로, 설치, 유지 보수, 크기 조정이 가능합니다. CPU, GPU(Graphics Processing Unit) 및 RAM을 비롯한 리소스 소비는 초기 설치 중에 선택한 배포 크기(Small, Medium 또는 Large)에 따라 동적으로 할당됩니다.

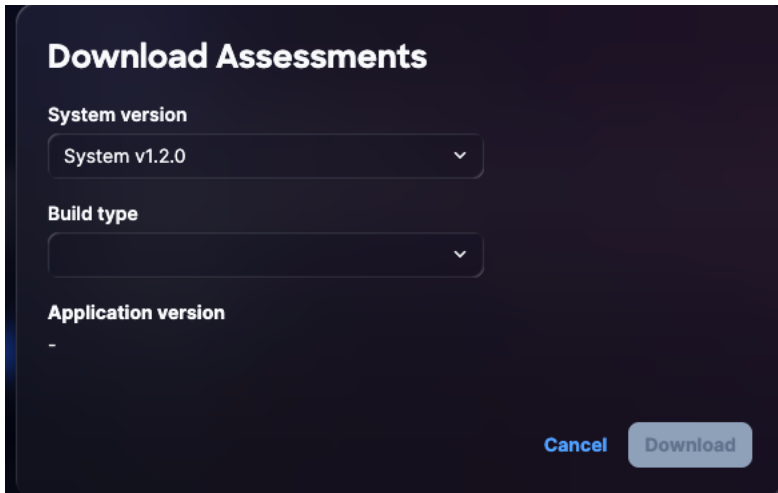
1. [Cisco IQ](#)에 [로그인합니다](#).
2. System Settings(시스템 설정) > Package Catalog(패키지 카탈로그)로 이동합니다.



패키지 카탈로그

3. 원하는 모듈 카드에서 다운로드 옵션 > 설치 패키지를 클릭합니다. 다운로드 창이 열립니다.

 참고: 평가 모듈은 이미지 예시에 사용됩니다.

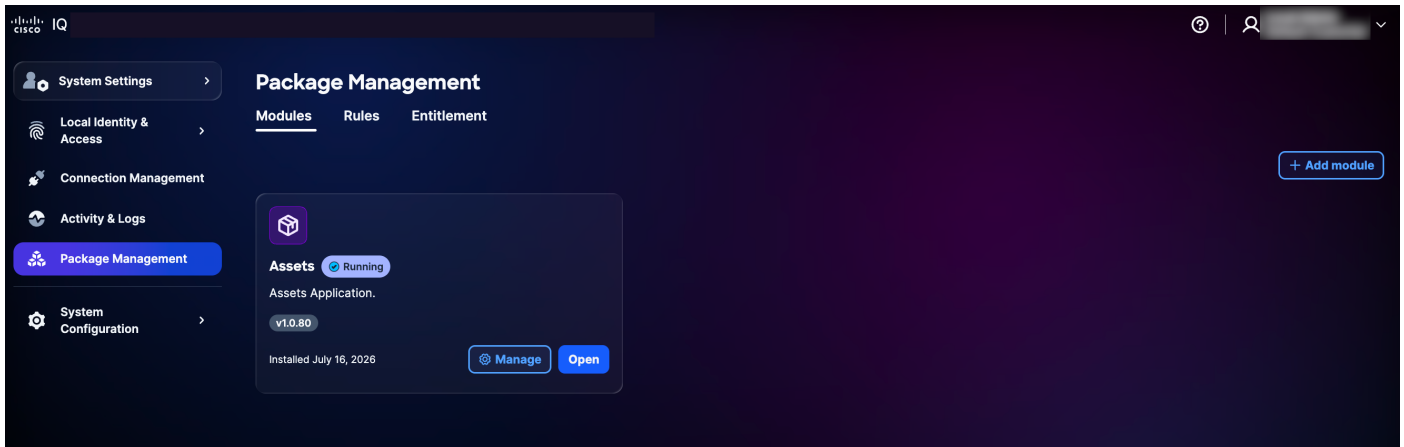


다운로드

4. 드롭다운 목록에서 시스템 버전을 선택합니다.
5. 드롭다운 목록에서 빌드 유형을 선택합니다.
6. 파일을 로컬로 저장하려면 Download(다운로드)를 클릭합니다.

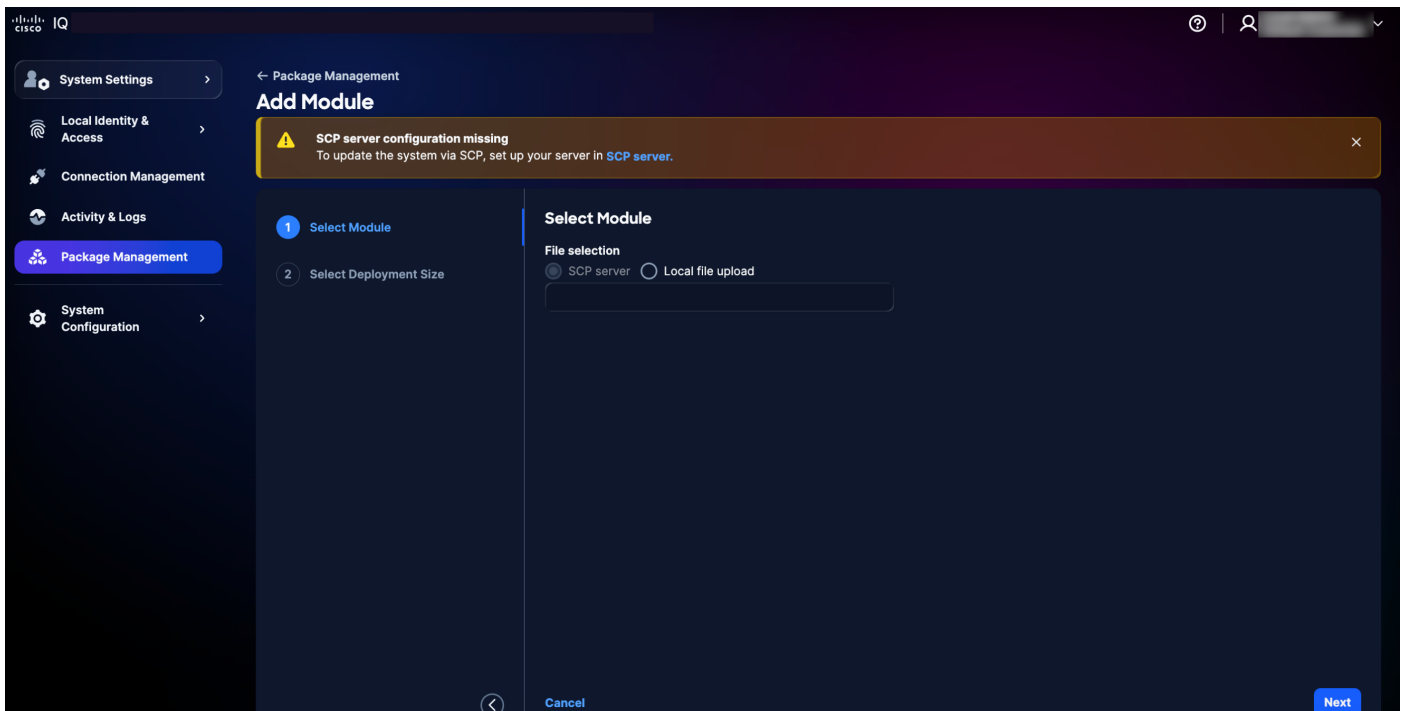
 참고: 설치 파일이 큼니다(10-25GB). 다운로드하기 전에 디스크 공간이 충분한지 확인하십시오.

7. VA로 이동합니다.
8. Home(홈) > System Settings(시스템 설정) > Package Management(패키지 관리)로 이동합니다. 패키지 관리 페이지는 다음 탭과 함께 표시됩니다.
 - 모듈
 - 규칙
 - 자격



모듈

9. 모듈 추가를 클릭합니다.

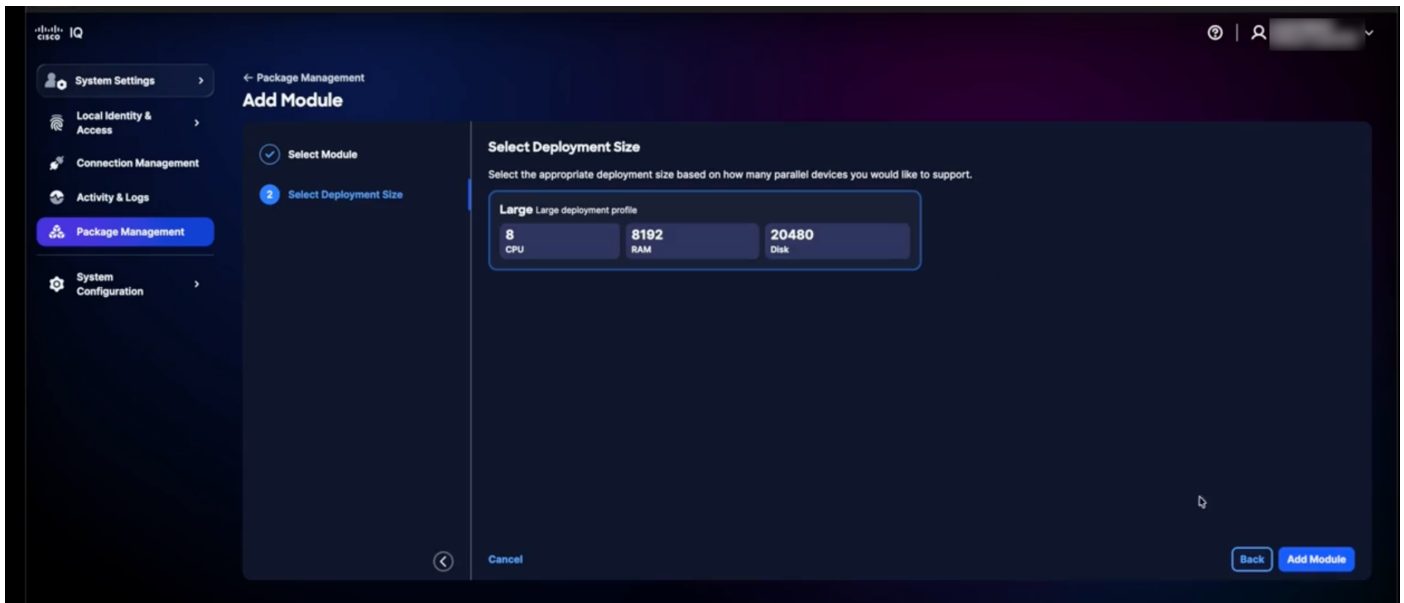


모듈 추가

10. 원하는 파일 선택 옵션을 선택합니다.

- SCP 서버: 설치 패키지의 정확한 파일 이름을 입력하십시오(대용량 파일에 권장됨).
- 로컬 파일 업로드: 다운로드한 설치 파일을 드래그 앤 드롭합니다(업로드 시간 때문에 30GB 이상의 파일에 권장되지 않음).

11. Next(다음)를 클릭합니다.



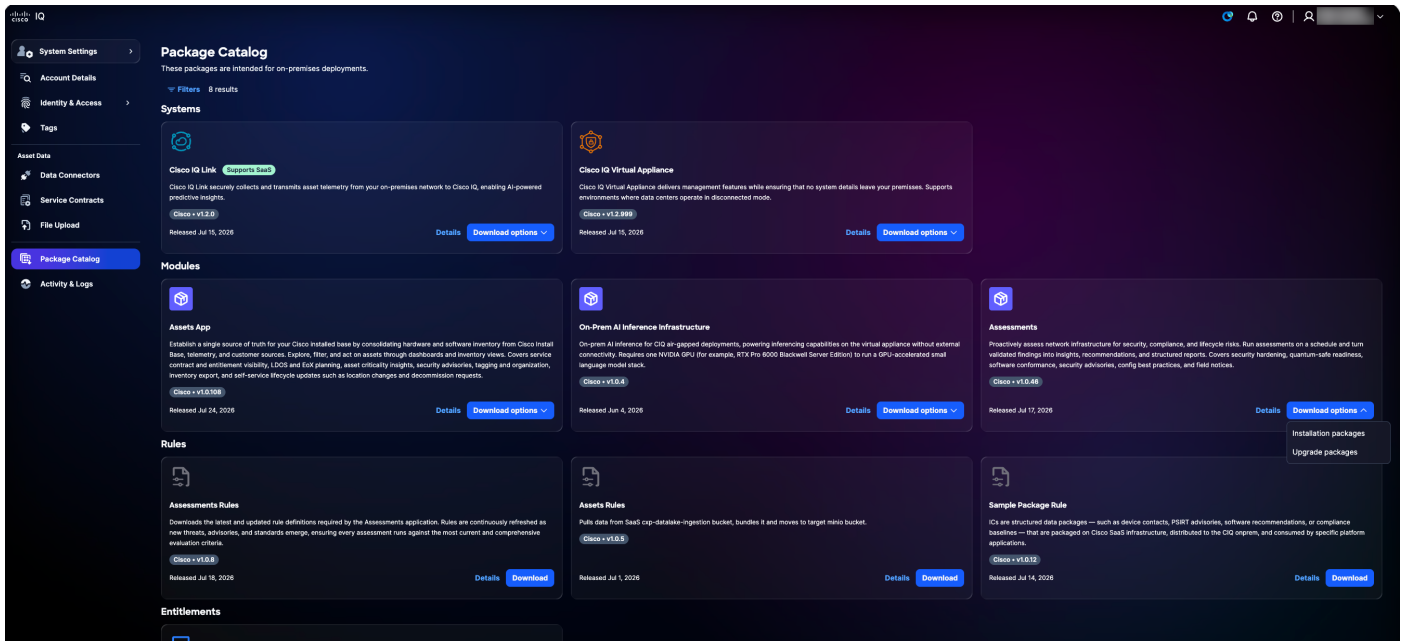
구축 크기

12. 배포 크기(예: Small, Medium 또는 Large)를 선택합니다. 이러한 크기는 미리 정의되어 있으며 리소스 요구 사항을 결정합니다.

13. Add Module(모듈 추가)을 클릭합니다. 새로 설치된 모듈이 패키지 관리의 Modules(모듈) 탭에 표시됩니다. 완료되면 모듈 상태가 "Running(실행 중)"으로 변경되고 Open(열기) 버튼을 사용할 수 있습니다.

모듈 업그레이드

최신 모듈은 패키지 카탈로그(Cisco IQ)에서 지속적으로 업데이트되고 있습니다. 최신 버전으로 업그레이드하려면



네트워크 검사로 자산 연결

- 원하는 모듈 카드에서 Download options(다운로드 옵션) > Upgrade packages(패키지 업그레이드)를 클릭합니다. 다운로드 창이 열립니다.



참고: Assessment 모듈은 이미지의 예로 사용됩니다.

Upgrade Assessments

System version

System v1.2.0



Current app version



Build type



Application version

-

Cancel

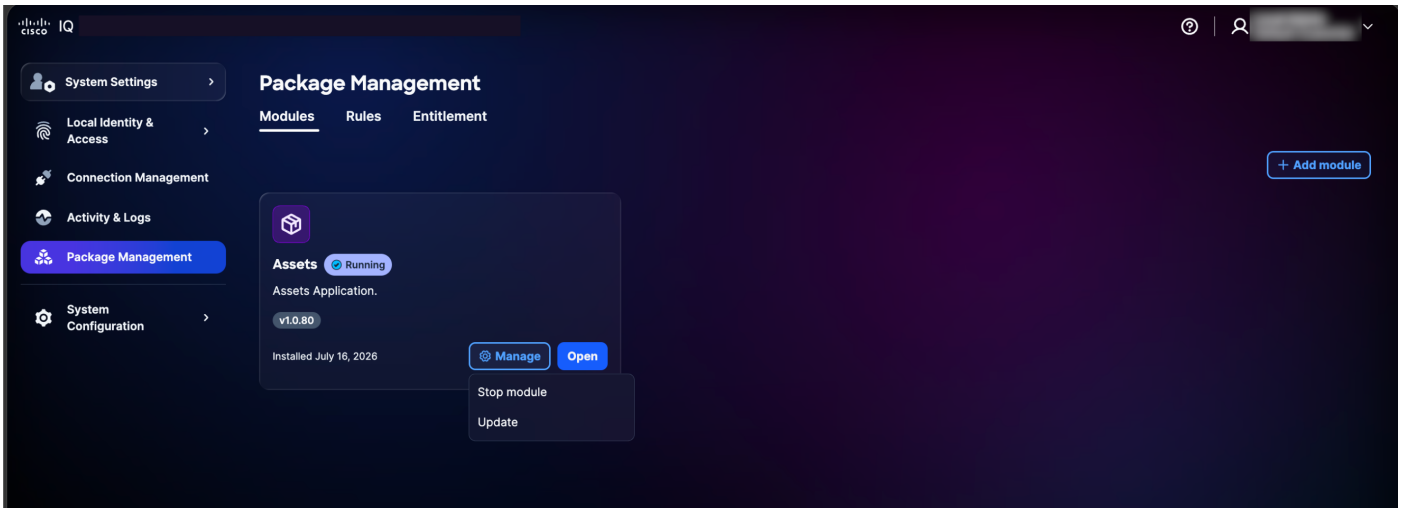
Download

다운로드

2. 드롭다운 목록에서 시스템 버전을 선택합니다.
3. 드롭다운 목록에서 현재 앱 버전을 선택합니다.
4. 드롭다운 목록에서 빌드 유형을 선택합니다.
5. 파일을 로컬로 저장하려면 Download(다운로드)를 클릭합니다.
6. VA로 이동하여 다운로드한 파일의 설치를 완료합니다.

모듈 관리

모듈을 추가한 후 Manage(관리)를 클릭하여 Package Management(패키지 관리) 페이지에서 모듈을 수정할 수 있습니다. 사용 가능한 수정 옵션에는 크기 조정 및 더 높은 버전으로 업그레이드가 포함됩니다. 모듈을 관리하려면



업데이트 유형

1. Package Management(패키지 관리) 페이지에서 Manage(관리) > Update(업데이트)를 클릭하여 원하는 모듈을 확인합니다.
2. 업데이트 유형을 선택합니다.

- 배포 크기만 변경
- 버전 업데이트

3. 구축 크기 변경을 선택한 경우 다음을 클릭하고 다음 페이지에서 새 구축 크기를 선택합니다.

또는

버전 업데이트를 선택하면 파일 선택 옵션이 표시됩니다. SCP Server(SCP 서버)를 선택하고 설치 패키지의 정확한 파일 이름을 입력하거나 Local file upload(로컬 파일 업로드)를 선택하고 다운로드한 설치 파일을 드래그 앤 드롭합니다.

4. Next(다음)를 클릭합니다. 업데이트 일정 선택 페이지가 표시됩니다.
5. 다음 라디오 버튼 옵션 중에서 선택하여 일정을 업데이트합니다.

- 지금 업데이트
- 나중에 업데이트



참고: 일부 모듈은 다운타임 없이 업데이트를 지원합니다. 다운타임이 필요한 경우 배너에 세부 정보가 표시됩니다.

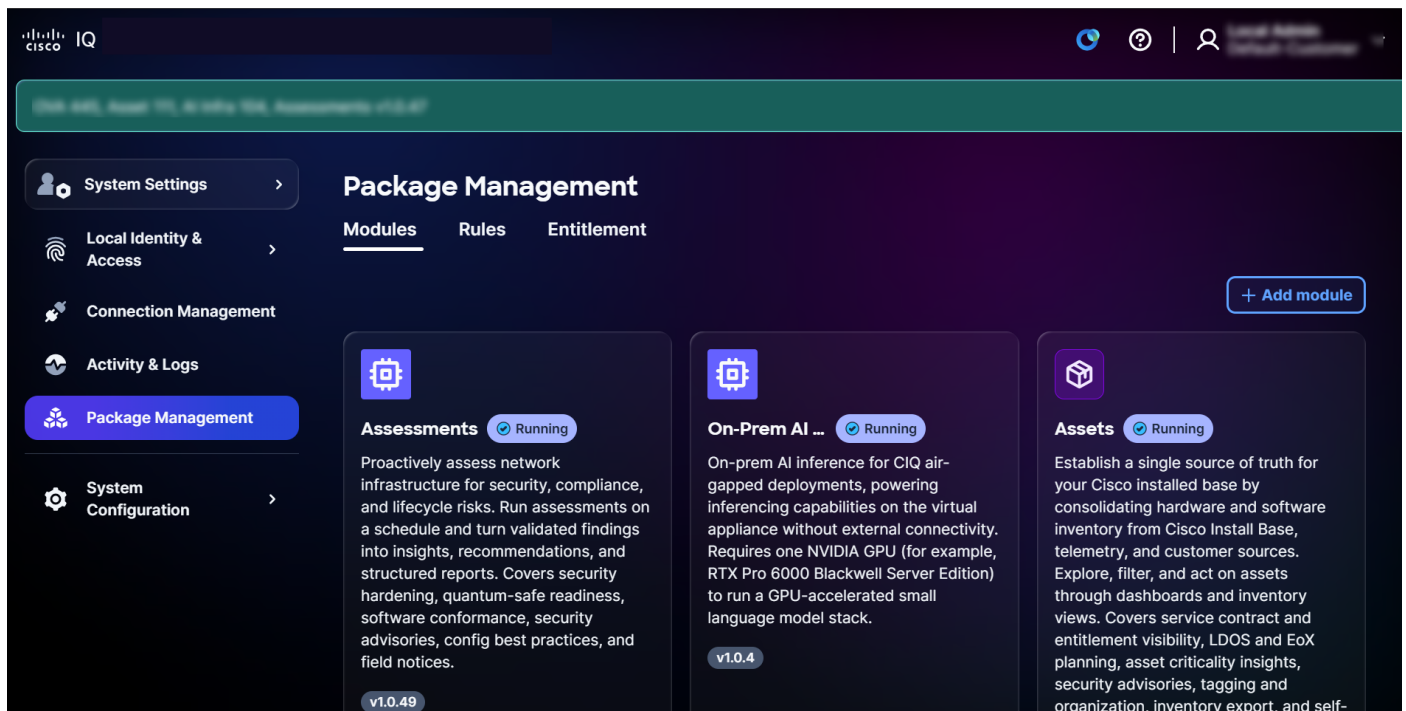
6. Update later(나중에 업데이트)를 선택한 경우 Date and Time(날짜 및 시간)을 입력합니다.
7. Next(다음)를 클릭합니다. 업데이트 요약이 표시됩니다.

 참고: 업데이트 요약에서 릴리스 정보에 액세스할 수 있습니다.

8. Update Module(모듈 업데이트)을 클릭하고 Module(모듈) 탭으로 이동합니다. 모듈은 "업데이트 예약" 상태를 표시합니다.

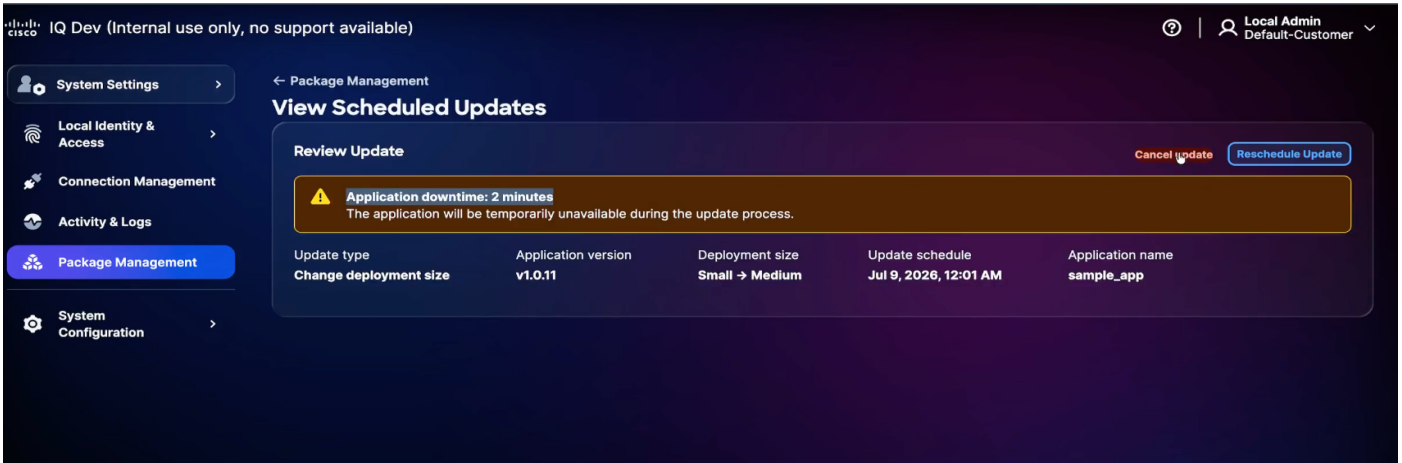
일정 수정

예약된 업데이트를 보거나 편집하거나 취소할 수도 있습니다. 예약된 업데이트를 편집하거나 취소하려면



일정 수정

1. Package Management(패키지 관리) 페이지에서 Manage(관리) > View Scheduled update of the desired module(원하는 모듈의 예약된 업데이트 보기)을 클릭합니다. 예약된 업데이트 보기 창이 표시됩니다.



업데이트 예약

- 필요에 따라 갱신 취소 또는 갱신 스케줄 조정을 클릭합니다.
- 화면의 지침에 따라 작업을 완료합니다.

 참고: 모듈 작업(예: 설치, 업그레이드 또는 크기 조정)이 실패할 경우 다음 옵션 중 하나를 선택합니다.

다시 시도: UI에는 작업을 다시 시도할 수 있는 Retry(재시도) 버튼이 표시됩니다. 로그: 오류가 지속되면 로그를 클릭하여 자세한 진단 정보를 확인합니다. 이는 설치 또는 런타임 오류의 원인을 식별하기 위한 기본 방법입니다.

규칙 설치

규칙은 기존 모듈의 기능을 확장하거나 수정하는 특수 구성 요소 또는 "추가 기능"입니다. 규칙은 독립 실행형 프로그램으로 실행되지 않습니다. 특정 규칙, 로직 또는 기능을 제공하기 위해 모듈에 "연결"됩니다. 규칙은 특정 모듈에 연결됩니다. 규칙이 설치되면 지원하는 모듈에 연결됩니다. 규칙을 사용하면 코어 모듈을 완전히 업그레이드하지 않고도 시스템을 업데이트하거나 사용자 지정할 수 있습니다. 새로운 규칙 또는 기능 집합이 필요한 경우 기존 모듈에 새 규칙을 추가하면 됩니다.

규칙을 다운로드하려면

- [Cisco IQ](#)에 [로그인](#)합니다.
- System Settings(시스템 설정) > Package Catalog(패키지 카탈로그)로 이동합니다.
- 원하는 규칙 카드에서 Download를 클릭합니다.

 참고: 다음 예제 이미지는 Assets 규칙에 대한 것입니다.

Download Assets Rules

Target app version

assets v1.0.0



Cancel

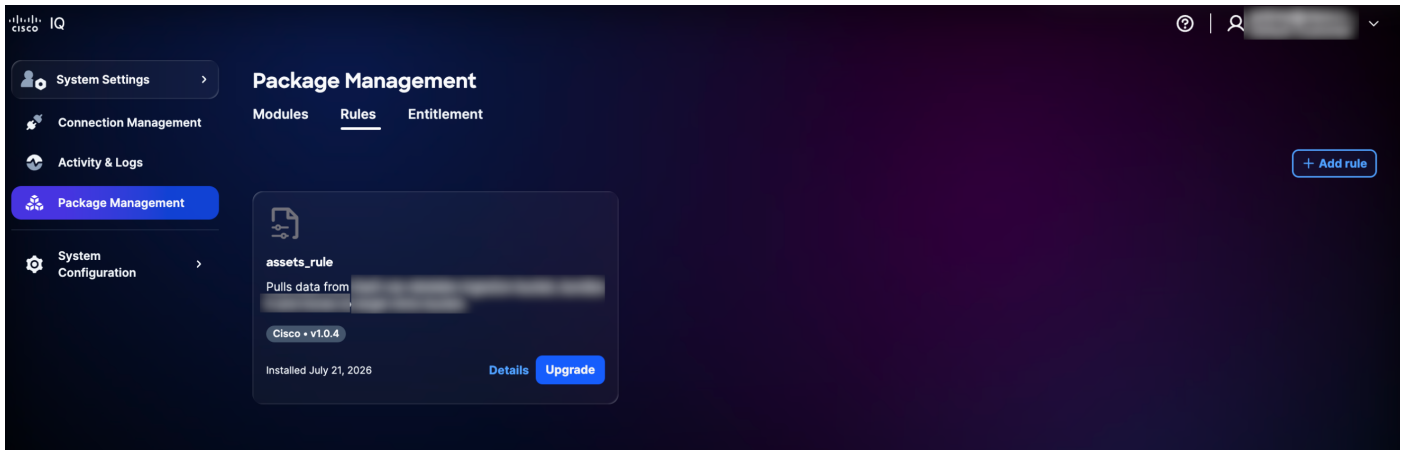
Download

다운로드

4. 드롭다운 목록에서 대상 앱 버전을 선택합니다.
5. 파일을 로컬로 저장하려면 Download(다운로드)를 클릭합니다.

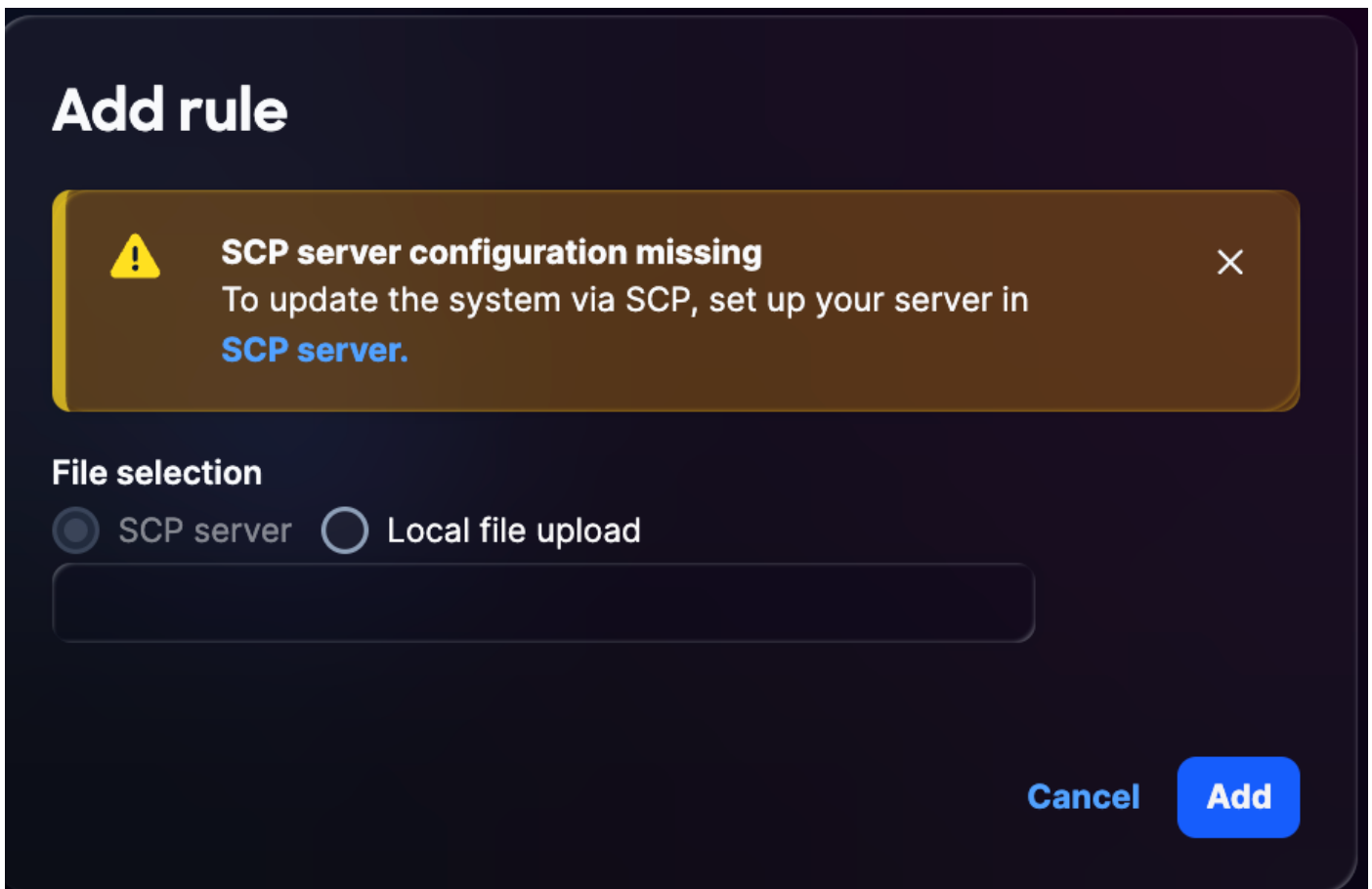
 참고: 설치 파일이 큼(10-25GB), 다운로드하기 전에 디스크 공간이 충분한지 확인하십시오.

6. VA로 이동합니다.
7. Home(홈) > System Settings(시스템 설정) > Package Management(패키지 관리)로 이동합니다. 패키지 관리 페이지는 다음 탭과 함께 표시됩니다.
 - 모듈
 - 규칙
 - 자격
8. Rules(규칙) 탭을 클릭합니다.



패키지 관리

9. Add rule(규칙 추가)을 클릭합니다.



규칙 추가

10. 원하는 파일 선택 옵션을 선택합니다.

- SCP(Secure Copy Protocol) 서버: 설치 패키지의 정확한 파일 이름을 입력합니다. 이 방법은

대용량 파일에 사용하는 것이 좋습니다.

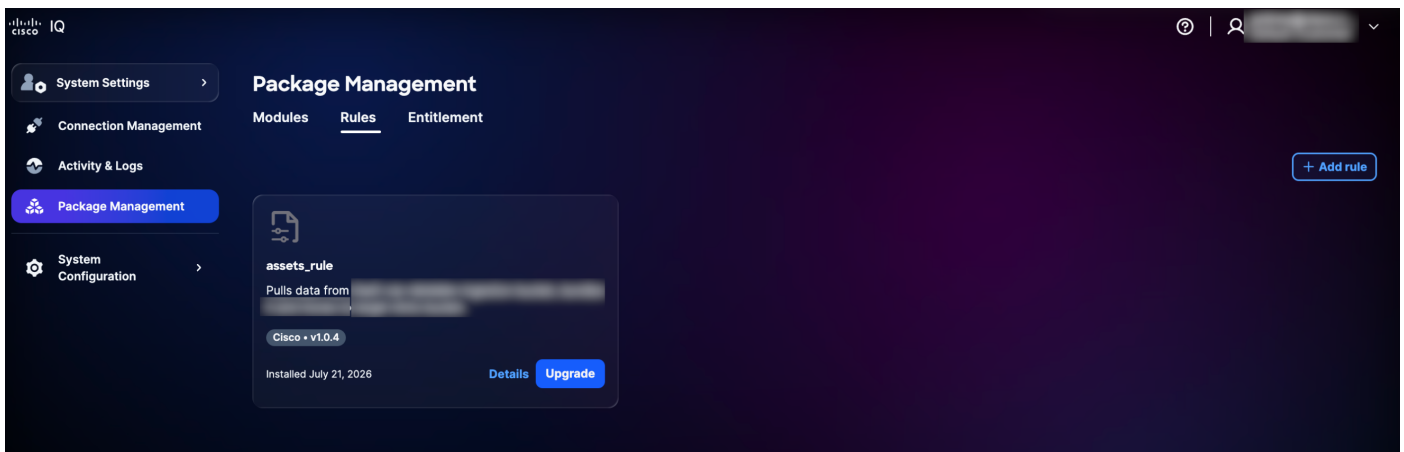
- 로컬 파일 업로드: 다운로드한 설치 파일을 드래그 앤 드롭합니다.

11. Add(추가)를 클릭합니다. 추가된 규칙이 패키지 관리에 표시됩니다.

규칙 업그레이드

규칙을 업그레이드하려면

1. VA에서 System Settings(시스템 설정) > Package Management(패키지 관리)로 이동합니다.



업그레이드

2. 원하는 규칙에서 Upgrade를 클릭합니다. Upgrade Rule 창이 열립니다.

Upgrade Rule

File selection

☒ SCP server ☐ Local file upload

Cancel

Add

업그레이드 규칙

3. 원하는 파일 선택 옵션을 선택합니다.

- SCP(Secure Copy Protocol) 서버: 설치 패키지의 정확한 파일 이름을 입력합니다. 이 방법은 대용량 파일에 사용하는 것이 좋습니다.
- 로컬 파일 업로드: 다운로드한 설치 파일을 드래그 앤 드롭합니다.

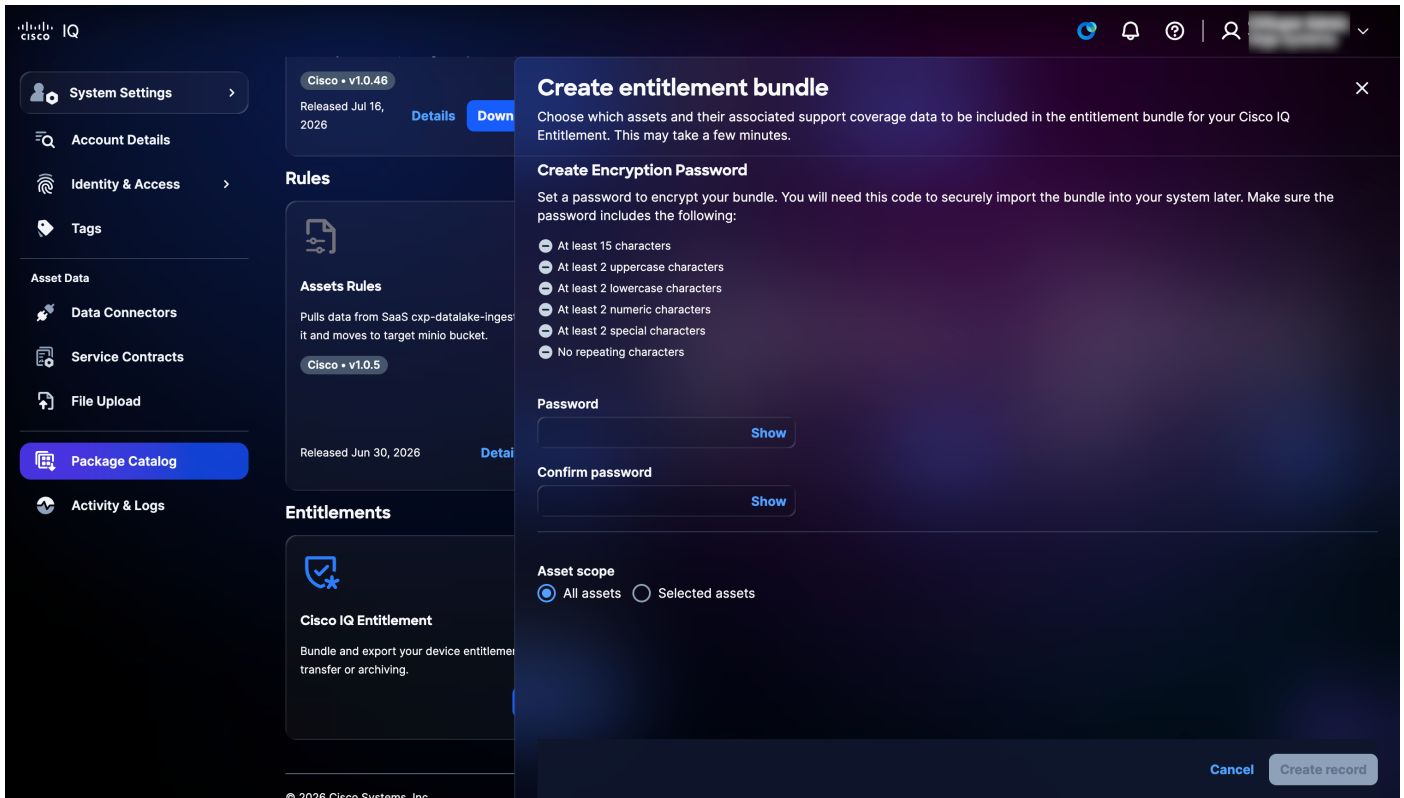
4. Add(추가)를 클릭합니다.

 참고: 이러한 규칙은 반복되는 예약된 디바이스 텔레메트리 수집에 적용됩니다. 즉각적인 애플리케이션을 위해 수동으로 디바이스 텔레메트리 수집을 시작할 수 있습니다.

자격 설치

엔타이틀먼트는 특정 소프트웨어 기능, 모듈 또는 서비스를 사용할 수 있는 조직의 권리를 검증합니다. 엔타이틀먼트를 설치하려면

1. [Cisco IQ](#)에 [로그인합니다](#).
2. System Settings(시스템 설정) > Package Catalog(패키지 카탈로그)로 이동합니다.
3. 자격 카드에서 레코드 만들기를 클릭합니다. Create entitlement bundle(자격 번들 생성) 창이 열립니다.



엔타이틀먼트 번들 생성

4. 비밀번호를 입력합니다. 화면에 표시되는 비밀번호 생성 규칙을 참조하십시오.
5. Confirm Password(비밀번호 확인)에 동일한 비밀번호를 다시 입력합니다.
6. 선호 자산 범위 라디오 버튼을 선택합니다.
 - 모든 자산: 연결된 모든 자산 포함
 - 선택한 자산: 사용자 환경에 맞는 특정 장치를 선택할 수 있습니다. 이 옵션을 선택한 경우 해당되는 모든 자산의 확인란을 선택합니다
7. 파일을 로컬로 저장하려면 레코드 만들기를 클릭합니다.

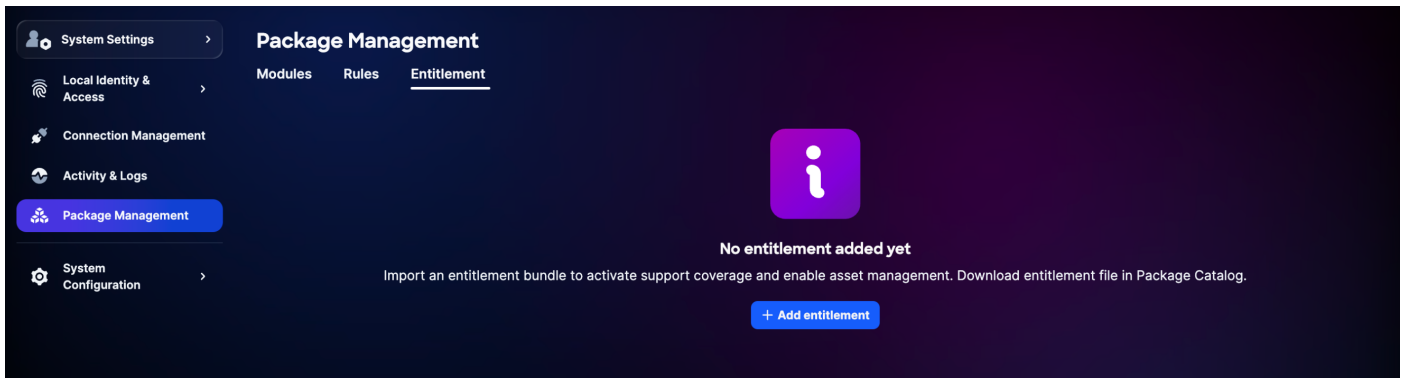
 참고: 엔타이틀먼트 번들을 생성한 후에는 현재 화면에서 이동하지 마십시오. 다른 페이지로 이동하면 번들이 무효화되며 다운로드 옵션을 활성화하려면 번들을 다시 생성해야 합니다.

 참고: 설치 파일이 큼(10-25GB), 다운로드하기 전에 디스크 공간이 충분한지 확인하십시오.

8. VA에 로그인합니다.
9. Home(홈) > System Settings(시스템 설정) > Package Management(패키지 관리)로 이동합니다. 패키지 관리 페이지는 다음 탭으로 구성됩니다.

- 모듈
- 규칙
- 자격

10. Entitlements(자격) 탭을 클릭합니다.



Entitlement(자격) 탭

11. Add Entitlement를 클릭합니다.

Add Entitlement

File selection

☒ SCP server
 ☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

Show

Cancel
Add

엔타이틀먼트 추가

12. 원하는 파일 선택 옵션을 선택합니다.

- SCP(Secure Copy Protocol) 서버: 설치 패키지의 정확한 파일 이름을 입력합니다. 이 방법은 대용량 파일에 권장됩니다.
- 로컬 파일 업로드: 다운로드한 설치 파일 드래그 앤 드롭

13. 비밀번호를 입력합니다.

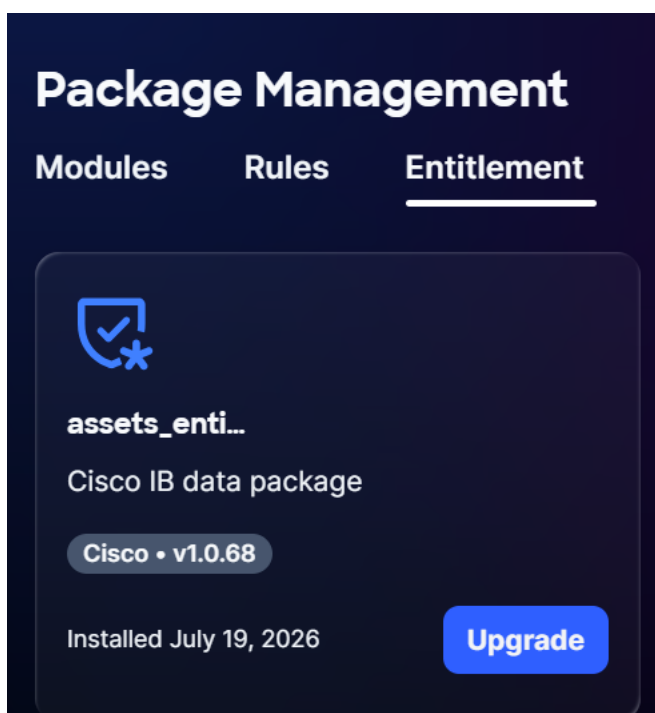
14. Add(추가)를 클릭합니다. 새로 설치된 엔타이틀먼트는 패키지 관리의 엔타이틀먼트 탭에 표시됩니다.

15. 엔타이틀먼트를 활성화하려면 엔타이틀먼트를 추가한 후 5~10분 정도 기다렸다가 디바이스 텔레메트리 수집을 시작합니다.

 참고: 엔타이틀먼트 프로세스에서 서비스 계약을 추가하면 해당 계약에 연결된 모든 디바이스가 온프레미스 디바이스 자산 인벤토리에 추가됩니다. 디바이스를 일련 번호로 필터링하거나, 여러 계정 ID를 사용하거나, 특정 디바이스를 선택하여 엔타이틀먼트를 관리할 수 있는 옵션이 있습니다.

자격 업그레이드

엔타이틀먼트를 업그레이드하려면



엔타이틀먼트 업그레이드

- 원하는 Entitlement(자격)에서 Upgrade(업그레이드)를 클릭합니다.

Upgrade Entitlement

File selection

☒ SCP server ☐ Local file upload

Decrypt Entitlement Bundle
Enter the entitlement decryption password.

Password *

Enter password

Show

Cancel

Add

자격 업그레이드

- 원하는 파일 선택 옵션을 선택합니다.
 - SCP(Secure Copy Protocol) 서버: 설치 패키지의 정확한 파일 이름을 입력합니다. 이 방법은 대용량 파일에 권장됩니다.
 - 로컬 파일 업로드: 다운로드한 설치 파일 드래그 앤 드롭
- 비밀번호를 입력합니다.
- Add(추가)를 클릭합니다.

AI 기반 기능

온프레미스 AI Inference Infrastructure 모듈은 VA에서 온프레미스 AI 전원 기능을 지원합니다. 로컬에서 SLM(Small Language Model)을 실행하여 시스템이 AI 전원 프롬프트에 응답할 수 있습니다. 설치가 완료되면 VA 인터페이스 내에서 직접 상호 작용할 수 있습니다.

다음 쿼리 유형이 지원됩니다.

- 자산: EoL 상태, 소프트웨어 통화 또는 부적합, 보안 취약성, 계약 커버리지 공백으로 인해 위험에 처한 자산 식별
- 인벤토리: 재고 자산에 대한 AI 기반 분석 요청

온프레미스 AI 추론 인프라 설치 패키지는 Cisco IQ Package Catalog에서 사용할 수 있으며 Assets와 같은 다른 모듈과 동일한 방식으로 배포됩니다.

 참고: 온프레미스 AI 추론 인프라는 한 번에 GPU당 하나만 실행할 수 있습니다. 설치를 완료하는 데 약 40-45분이 소요됩니다. 설치 파일이 큼니다(약 30GB). 다운로드하기 전에 디스크 공간이 충분한지 확인하십시오.

온프레미스 AI 추론 인프라의 전제 조건

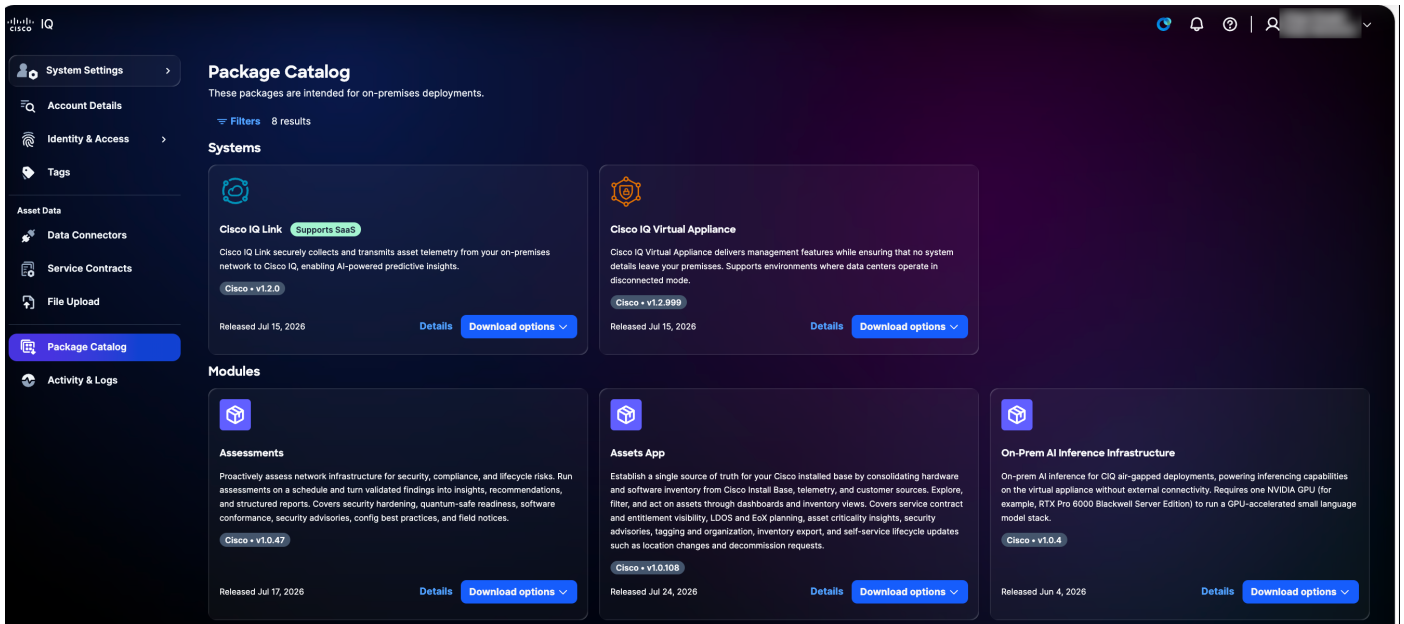
온프레미스 AI 추론 인프라를 설치하기 전에 다음 조건을 충족해야 합니다.

- VA에는 GPU 액세스 권한이 있는 VM이 포함되어야 합니다. slm은 GPU를 필요로 하며, GPU 없이는 실행될 수 없다
- GPU VM에는 80GB 이상의 GPU VRAM을 사용할 수 있어야 합니다

온프레미스 AI 추론 인프라 설치

VA에 온프레미스 AI 추론 인프라를 설치하려면 Cisco IQ SaaS에서 온프레미스 AI 추론 인프라 모듈을 다운로드합니다.

1. [Cisco IQ](#)에 [로그인합니다](#).
2. System Settings(시스템 설정) > Package Catalog(패키지 카탈로그)로 이동합니다.



패키지 설치

3. On-Prem AI Inference Infrastructure(온프레미스 AI 추론 인프라) 카드에서 Download options(다운로드 옵션) > Installation packages(설치 패키지)를 클릭합니다. 애플리케이션 다운로드 창이 열립니다.

Download On-Prem AI Inference Infrastructure

System version

System vv1.2.0



Build type

Release



Application version

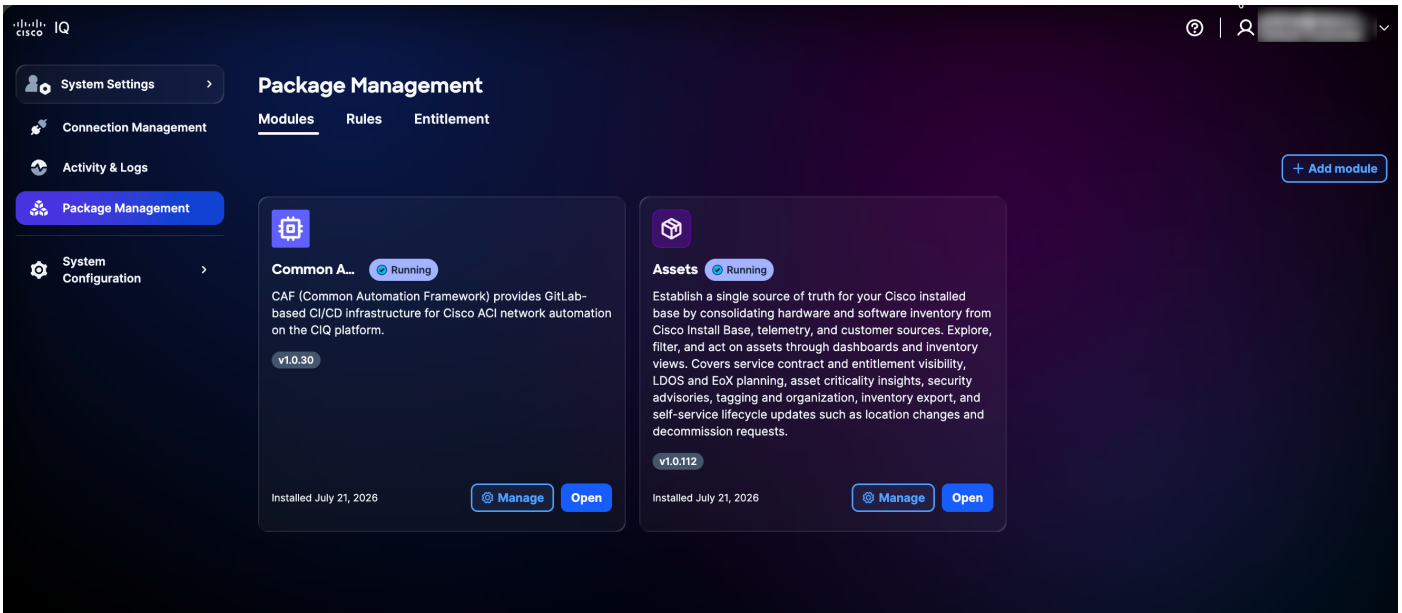
1.0.4

Cancel

Download

AI 추론 인프라 다운로드

4. 드롭다운 목록에서 시스템 버전을 선택합니다.
5. 드롭다운 목록에서 빌드 유형을 선택합니다.
6. Download(다운로드)를 클릭합니다.
7. VA로 이동합니다.

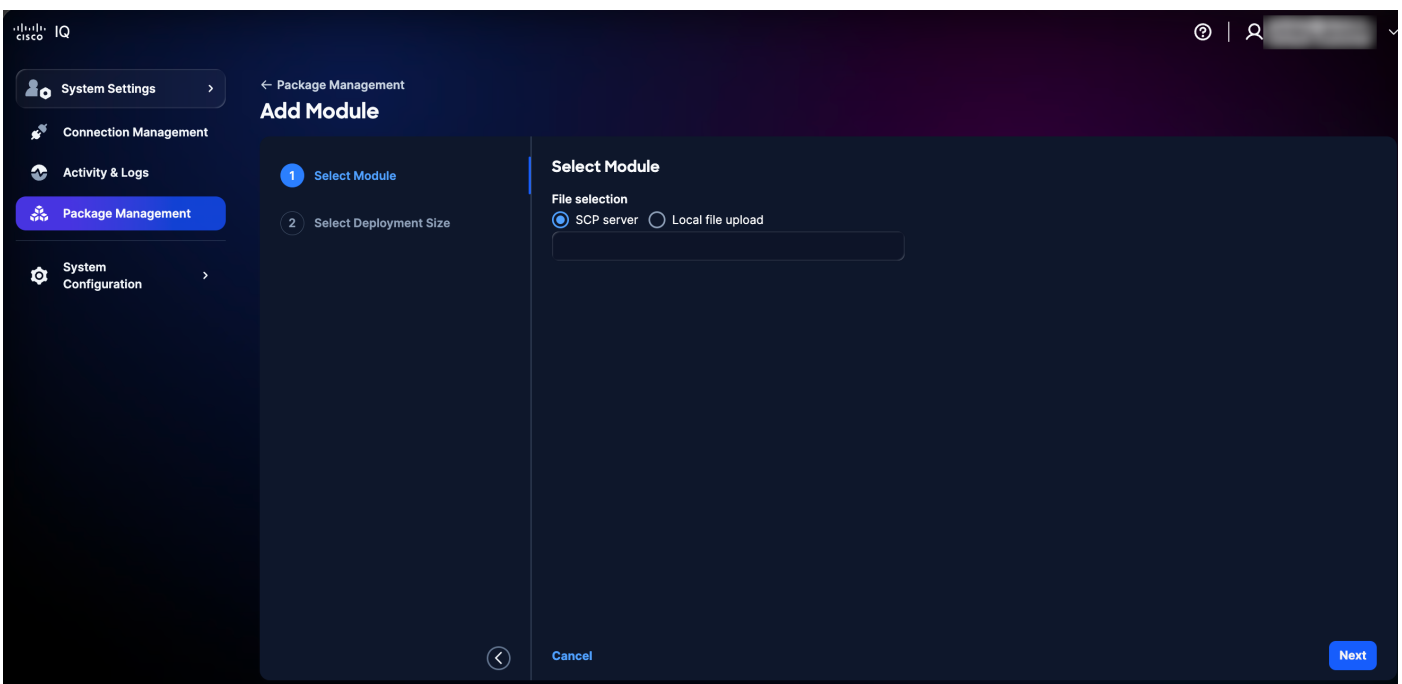


패키지 관리

8. Home(홈) > System Settings(시스템 설정) > Package Management(패키지 관리)로 이동합니다. 패키지 관리 페이지는 다음 탭과 함께 표시됩니다.

- 모듈
- 규칙
- 자격

9. Modules(모듈) 탭에서 Add modules(모듈 추가)를 클릭합니다.



모듈 선택

10. 원하는 파일 선택 옵션을 선택합니다.

- SCP 서버: 설치 패키지의 정확한 파일 이름을 입력합니다(대용량 파일에 권장됨).
- 로컬 파일 업로드: 다운로드한 설치 파일을 드래그 앤 드롭합니다(업로드 시간 때문에 30GB 이상의 파일에는 권장되지 않음). 참고: 로컬 파일 업로드 방법에 20분 임계값이 있습니다. 업로드 프로세스가 이 기간을 초과하면 설치가 실패합니다. SCP 서버를 사용하는 것이 성공적이고 안정적인 설치를 보장하기 위한 기본 방법입니다.

11. Next(다음)를 클릭합니다. 시스템에서 파일 업로드를 시작합니다.

12. 배포 크기(예: Small, Medium 또는 Large)를 선택합니다.

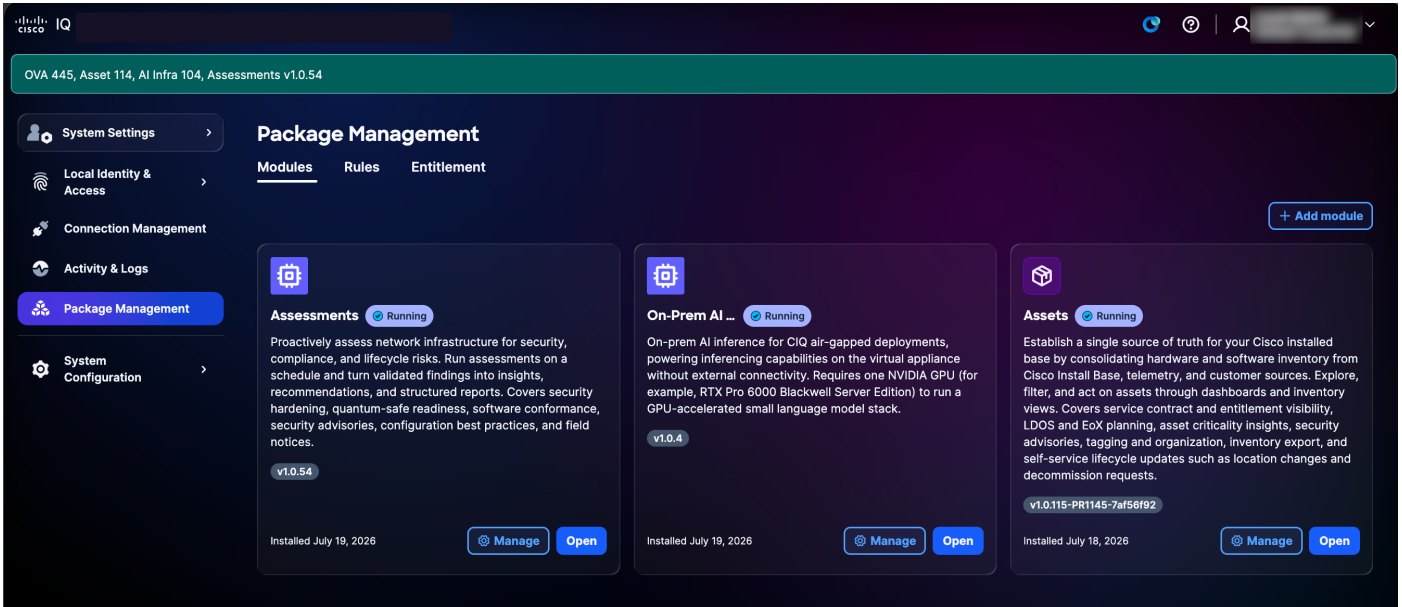
13. Add Module(모듈 추가)을 클릭합니다. 설치가 시작되며 완료하는 데 약 40-45분이 소요됩니다.

설치가 완료되면 Package Management(패키지 관리)의 Module(모듈) 탭에 On-Prem AI Inference Infrastructure(온프레미스 AI 추론 인프라)가 표시됩니다.

 참고: 온프레미스 AI 추론 인프라 모듈은 GPU당 하나만 실행할 수 있습니다. 이 모듈은 GPU VRAM의 약 90%를 사용합니다. 동일한 GPU에 추가 인스턴스를 설치하는 것은 지원되지 않습니다.

온프레미스 AI 추론 인프라 모듈 관리

온프레미스 AI 추론 인프라 모듈이 설치되면 패키지 관리의 애플리케이션 탭에서 관리할 수 있다.



AI 추론 인프라 수정

모듈을 관리하려면 온프레미스 AI 추론 인프라 모듈 옆에 있는 관리를 클릭합니다. 자세한 [내용](#)은 모듈 관리를 참조하십시오.

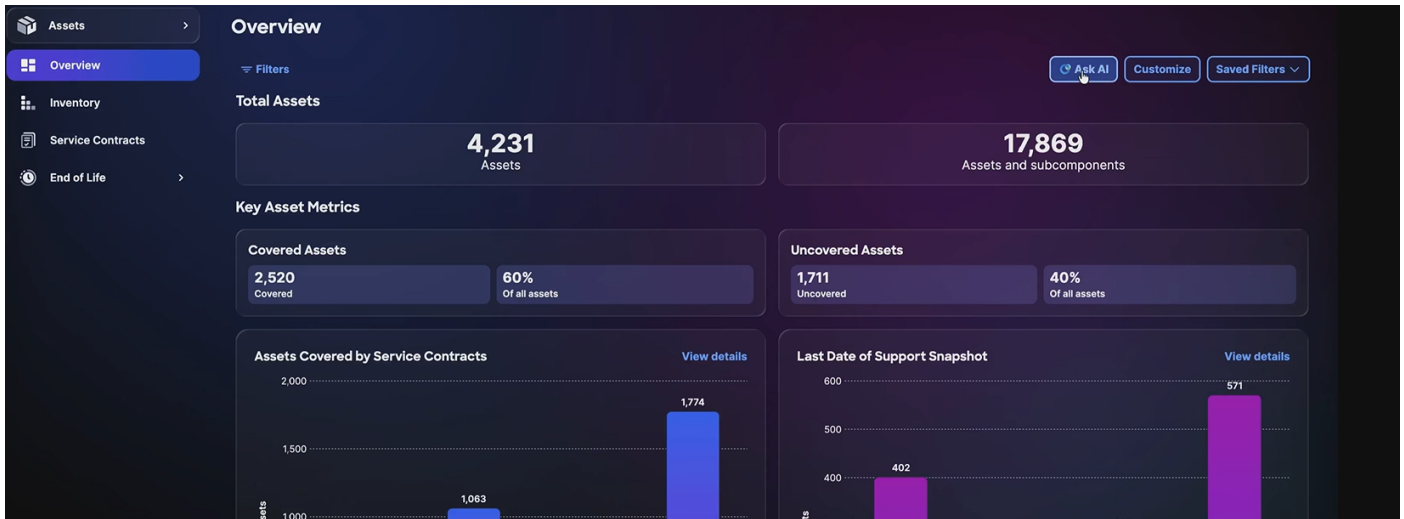
AI 기반 기능 사용

온프레미스 AI 추론 인프라 모듈이 성공적으로 설치되면 VA 인터페이스에서 Ask AI 버튼을 사용할 수 있게 된다.

AI에게 자산에 문의

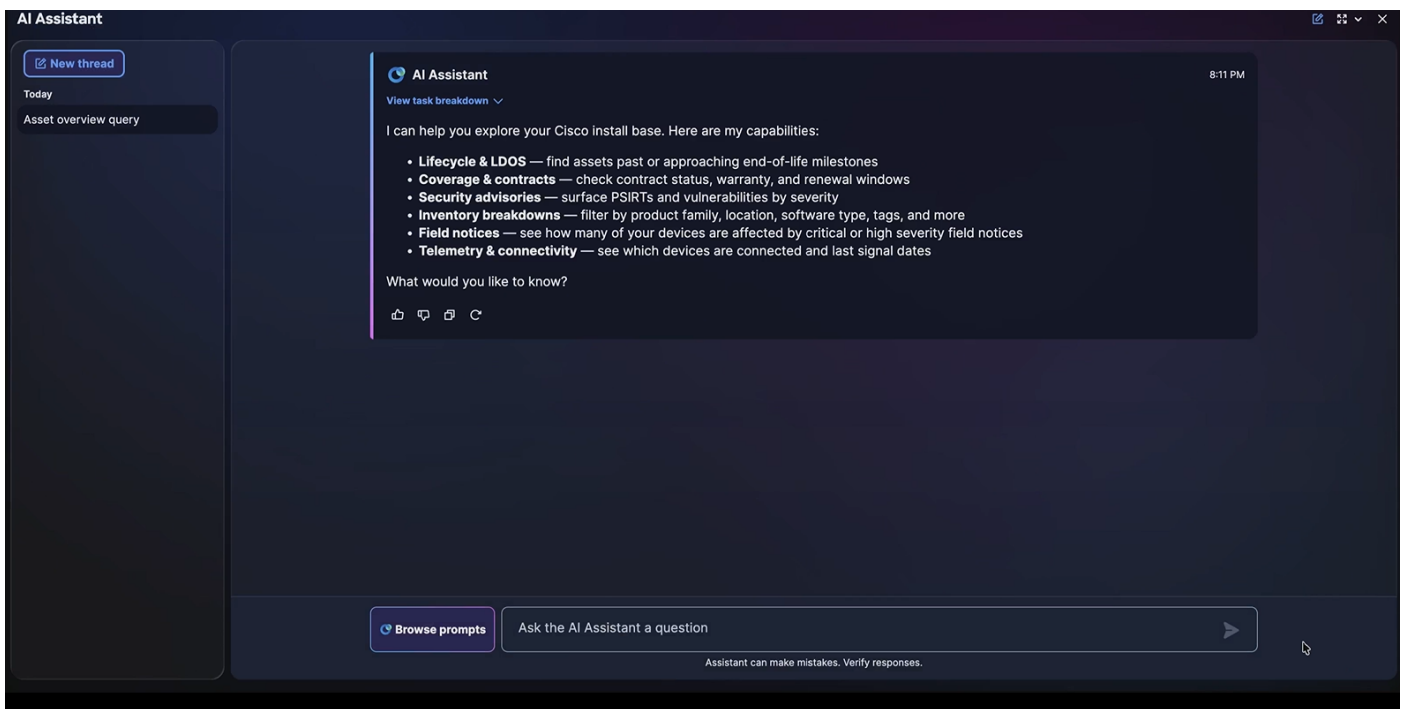
Assets에서 Ask AI를 사용하려면

1. 홈 메뉴 > 에셋을 선택합니다. 자산 페이지가 표시됩니다.



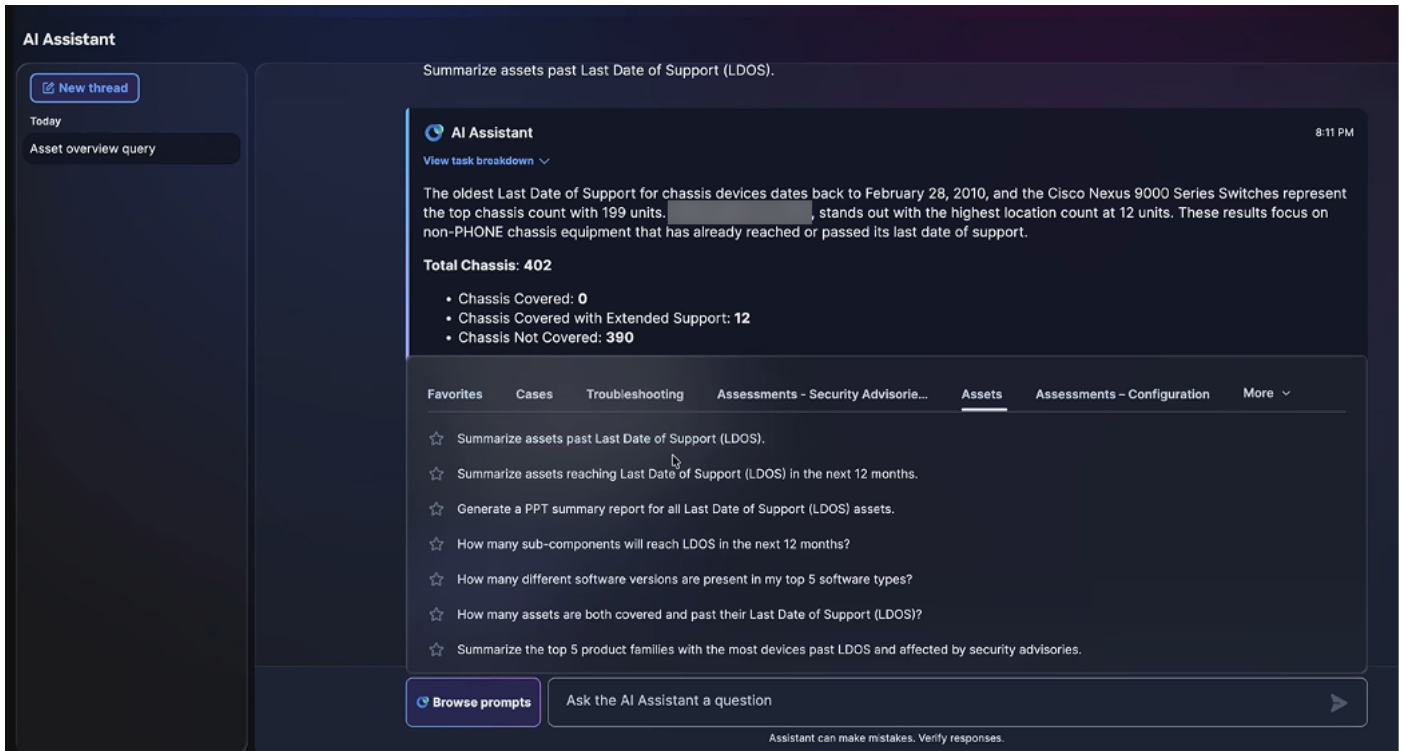
에셋 페이지

2. Ask AI(AI에 문의)를 클릭합니다. 온프레미스 AI 추론 인프라가 시작됩니다.



프롬프트 찾아보기

3. Browse prompts(프롬프트 찾아보기)를 클릭하여 사용 가능한 프롬프트를 보거나 Ask the AI Assistant a question(AI Assistant에 질문하기) 필드에 사용자 지정 질문을 입력합니다.



프롬프트 세트

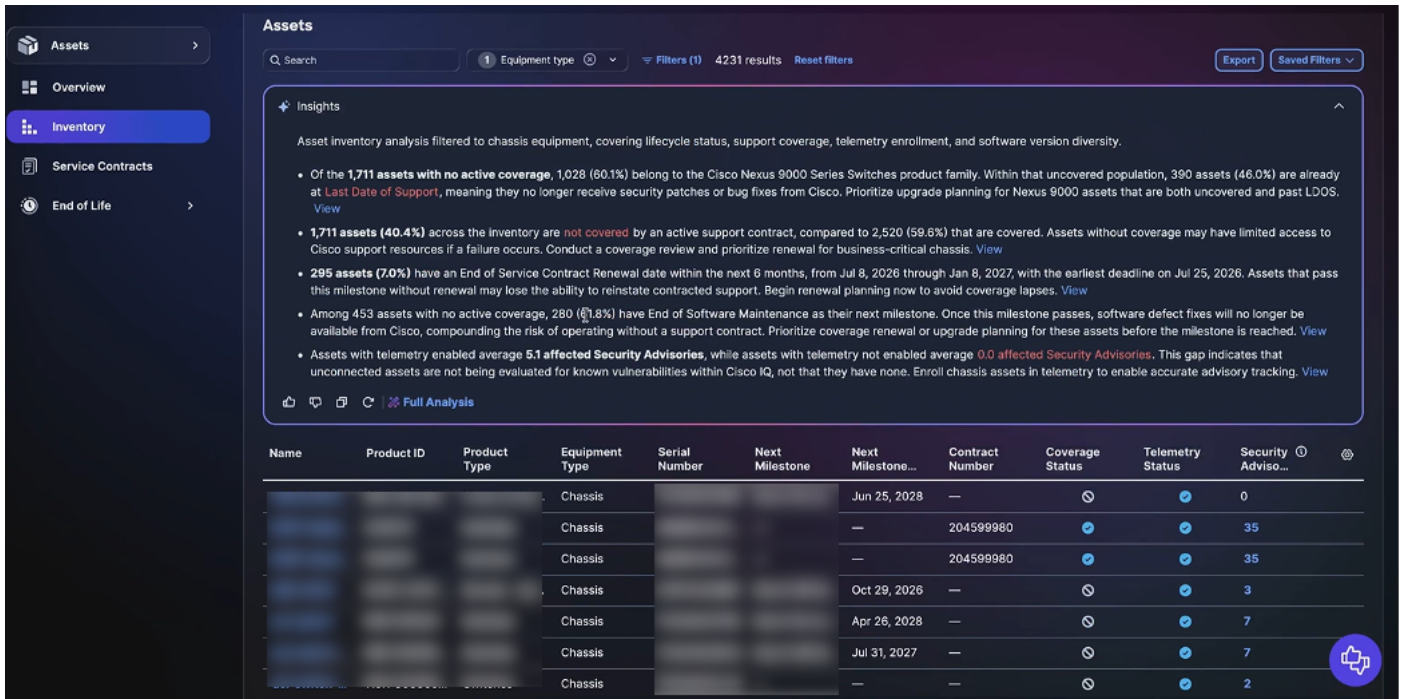
- 원하는 프롬프트를 클릭하거나 Enter를 누릅니다. 온-프레미스 SLM은 응답을 생성한다.

인벤토리의 AI 분석

온프레미스 AI 추론 인프라 모듈은 인벤토리 섹션에서 자동화된 AI 기반 분석을 제공합니다. 인벤토리 데이터가 채워지면 분석 결과가 자동으로 표시됩니다.

Inventory에서 AI 분석을 보려면

- 홈 메뉴 > 인벤토리를 선택합니다. Inventory(인벤토리) 페이지가 표시됩니다.



인벤토리

2. AI가 생성한 분석을 봅니다. 데이터를 사용할 수 있게 되면 결과가 인벤토리 보기에 표시됩니다.

 참고: 그래프, 대시보드, 차트와 같은 시각화를 위한 전체 분석을 클릭하여 추가적인 통찰력을 제공합니다.

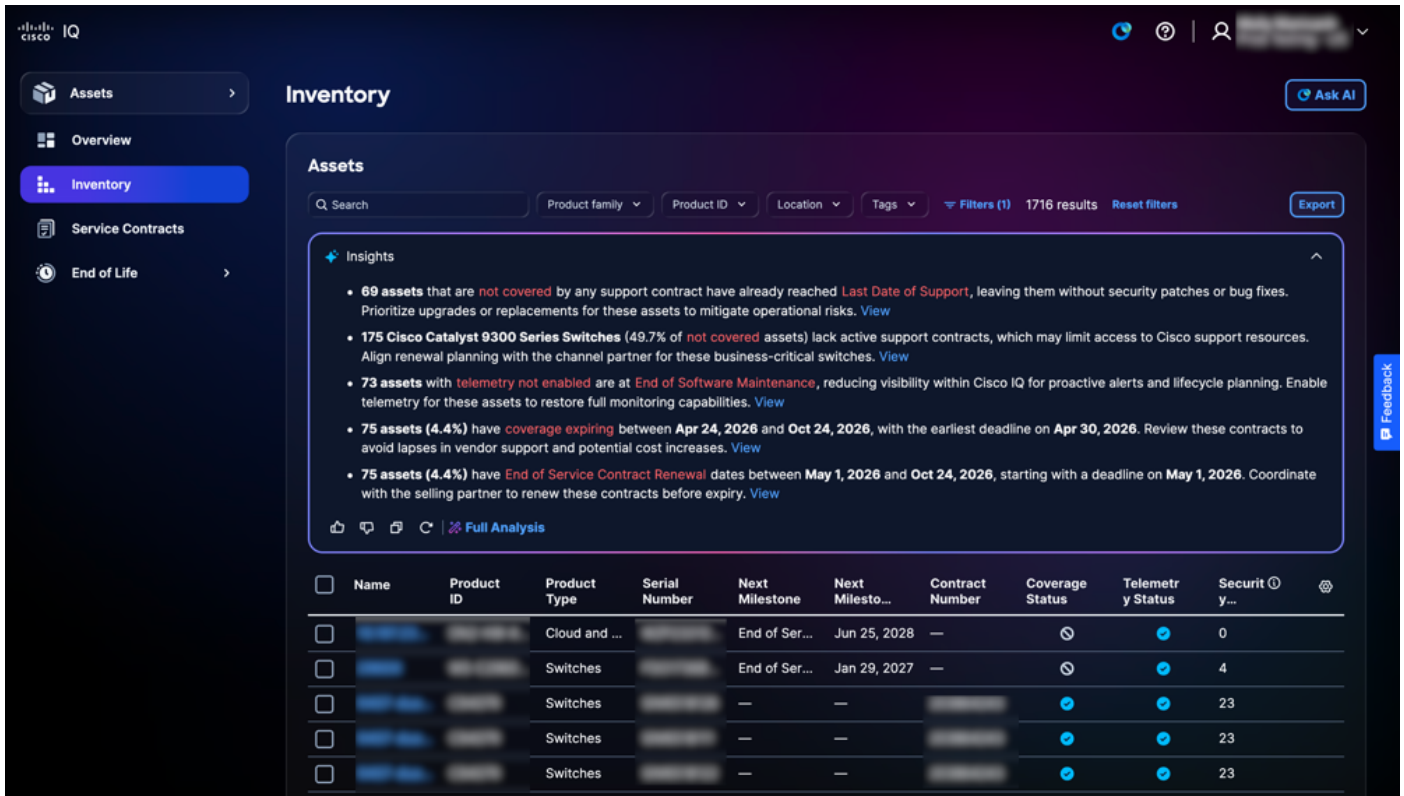
모듈의 공통 기능

이 섹션에서는 모든 모듈에서 공유하는 핵심 기능에 대해 자세히 설명합니다. 이러한 기능은 일관된 사용자 환경을 제공하고 시스템 성능을 최적화하며 관리 워크플로를 간소화합니다

데이터 분석

Insights 패널은 해당 페이지의 데이터에 대한 AI 기반 분석을 제공하여 네트워크 환경의 보안 및 상태를 개선하는 실행 가능한 통찰력을 제공합니다.

 참고: 분석 기능은 선택한 페이지에서만 사용할 수 있습니다.



인사이트 패널

Insights 패널 내에서 사용할 수 있는 옵션은 다음과 같습니다.

- 확장 아이콘을 클릭하여 패널을 확장하고 추가 정보를 표시합니다
- 엄지손가락 위로 또는 엄지손가락 아래로 아이콘을 클릭하여 AI가 생성한 정보에 대한 피드백을 제공합니다
- Full Analysis(전체 분석)를 클릭하여 추가 정보, 심층 분석, 그래프, 대시보드, 차트 등의 시각화를 표시합니다.

Security Advisories by Coverage Status

NOT COVERED: 6,046.00



COVERED: 20,757.00

This donut chart compares security advisories between devices with active coverage and those without.

KEY INSIGHT

Devices that are **NOT COVERED** account for **6,046 security advisories**, representing **23%** of the total exposure despite being a smaller portion of the inventory.



전체 분석

전체 분석 내에서 다음 옵션을 사용할 수 있습니다.

- PDF 다운로드를 클릭하여 기록 또는 협업을 위해 분석의 오프라인 사본을 저장합니다.

정보 내보내기

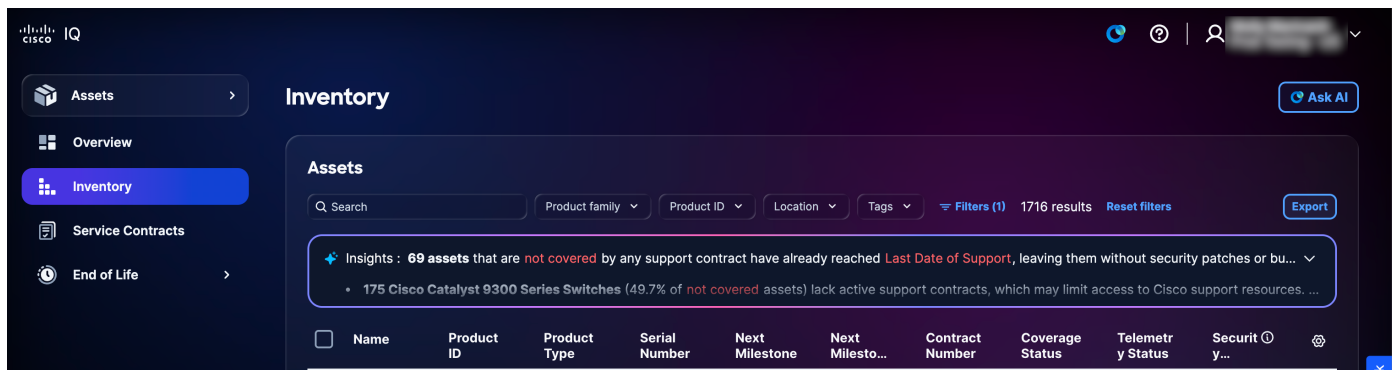
내보내기 기능을 사용하면 자산 및 보안 정보에 대한 사용자 지정 보기를 .xls 또는 .csv 형식으로 내보낼 수 있습니다.



참고: 내보내기 기능은 일부 페이지에서만 사용할 수 있습니다.

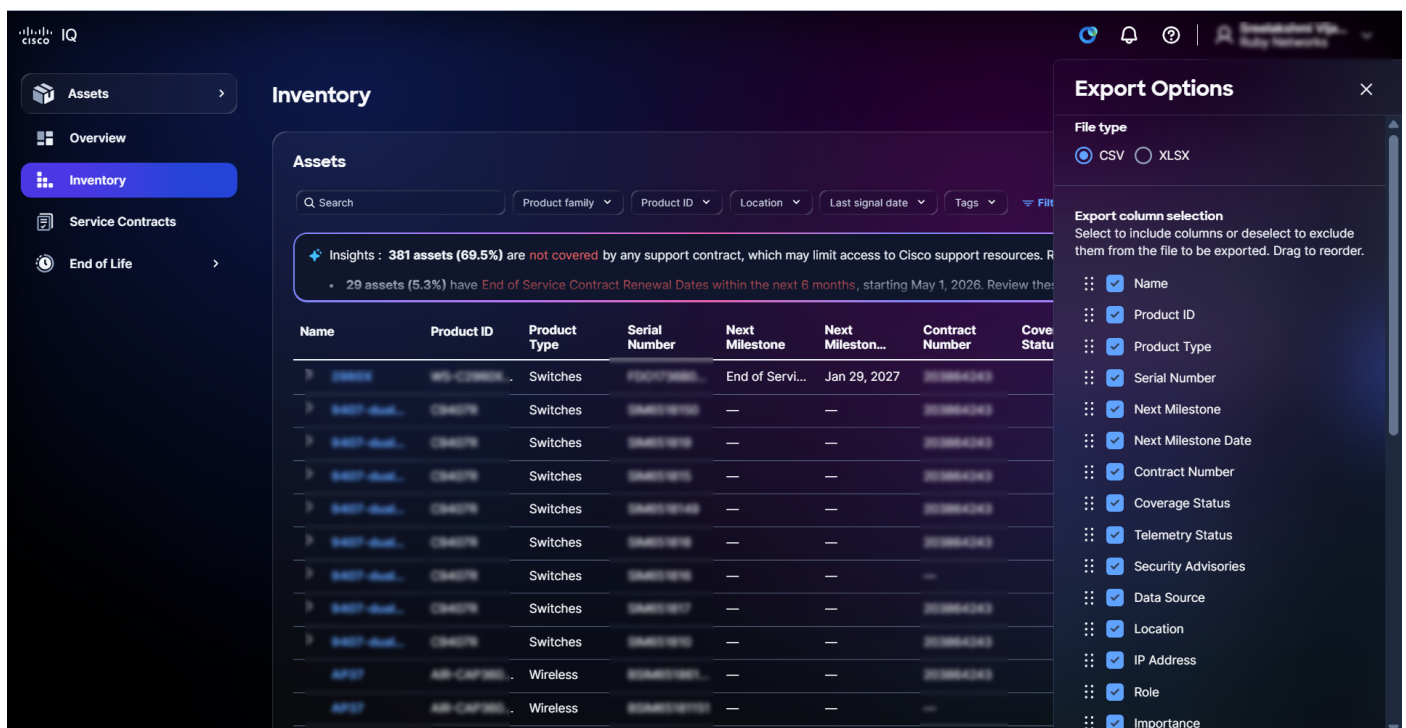
페이지에서 정보를 내보내려면 다음을 수행합니다.

1. 해당 페이지로 이동합니다.



Assets 모듈에서 인벤토리 내보내기

2. Export(내보내기)를 클릭합니다. 내보내기 옵션이 표시됩니다.



내보내기 옵션

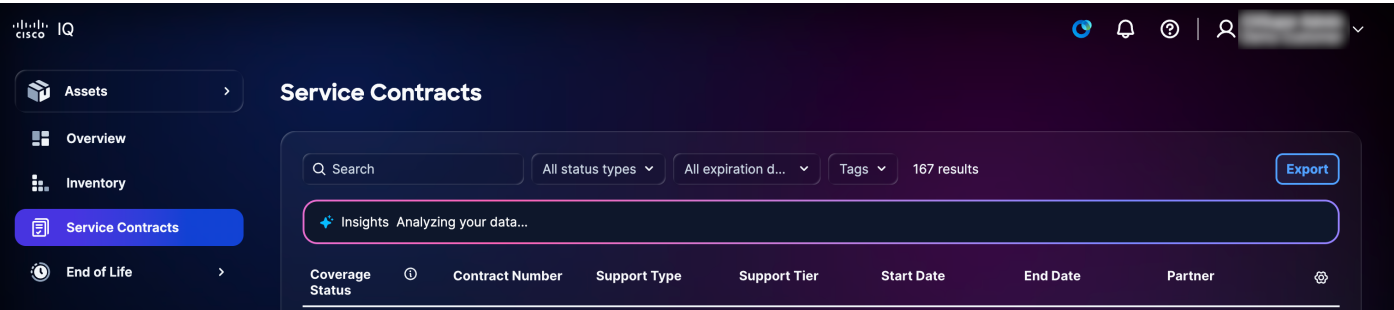
3. 파일 유형을 선택합니다.

4. 원하는 열의 확인란을 선택합니다.

5. Export(내보내기)를 클릭합니다. 파일이 브라우저의 로컬 다운로드 폴더로 다운로드됩니다.

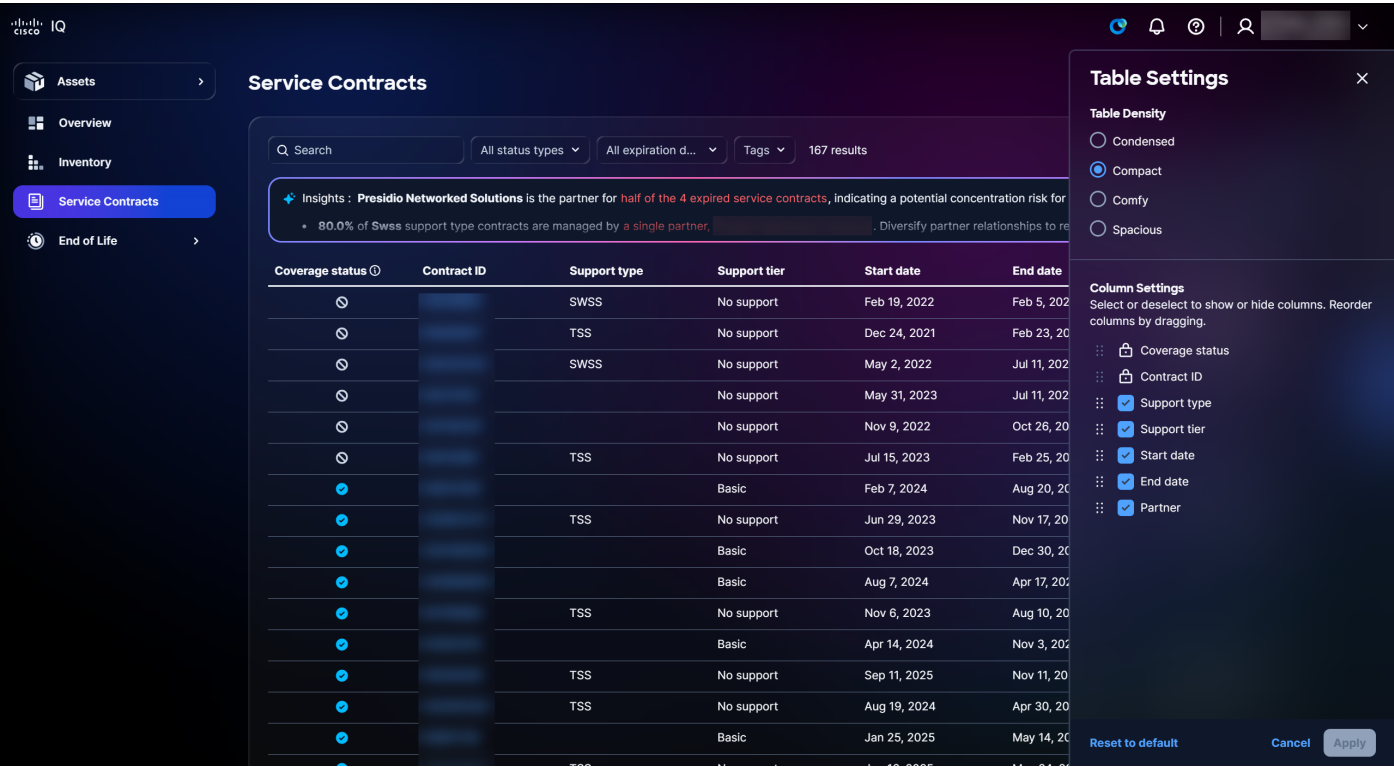
테이블 설정

서로 다른 모듈 기능에 대한 사용자 지정 보기 및 세분화된 보기를 생성하도록 테이블 설정을 구성할 수 있습니다.



테이블 설정

선택한 페이지에 표시되는 열을 변경하려면 테이블 설정 아이콘을 누릅니다. 테이블 설정이 표시됩니다.



테이블 설정 옵션

테이블 보기 변경

테이블 뷰를 변경하려면 다음을 수행합니다.

1. 다음 테이블 밀도 옵션 중 하나를 선택합니다.
 - 요약: 시각적 요소 및 간격을 최소화하여 추가 정보 표시
 - 컴팩트: 공백 감소 및 UI 요소 간 간격 강화
 - 편함: 더 많은 공백 및 요소 간 더 큰 간격 활용
 - 공간: 풍부한 공백 및 더 큰 UI 요소를 강조합니다.
2. 적용을 클릭합니다.

열 추가 및 제거

열을 추가하거나 제거하려면 다음을 수행합니다.

1. 열 설정 확인란을 선택하거나 선택 취소합니다.
2. 적용을 클릭합니다.



참고: 테이블 보기에서 이름 열을 제거할 수 없습니다.

열 순서 변경

열 순서를 변경하려면 다음을 수행합니다.

1. 열 이름을 끌어서 놓아 원하는 순서로 항목을 정렬합니다.
2. 적용을 클릭합니다.

대시보드 사용자 정의

Custom Dashboard(사용자 지정 대시보드) 기능을 사용하면 다음과 같은 다양한 직관적인 사용자 지정 옵션을 통해 표준 대시보드를 사용자 지정할 수 있습니다.

- 드래그 앤 드롭 기능을 사용하여 대시보드 위젯 또는 패널 재배포
- 워크플로와 관련이 없는 구성 요소를 모두 제거합니다.

- 개인화된 대시보드 레이아웃은 사용자 프로필에 안전하게 저장되며 모든 세션과 디바이스에 자동으로 적용됩니다
- 간단한 재설정 옵션으로 원래 대시보드 레이아웃 복원

대시보드를 사용자 정의하려면

1. 대시보드로 이동합니다.



사용자 지정

2. Customize를 클릭합니다.



대시보드 편집

3. 대시보드를 원하는 대로 변경합니다.

- 다시 정렬: 위젯을 원하는 레이아웃으로 드래그 앤 드롭
- 제거: 위젯을 제거하려면 삭제 아이콘을 클릭합니다
- 재설정: 대시보드를 원래 레이아웃으로 재설정하려면 기본값으로 재설정을 누릅니다

4. 저장을 클릭합니다. Dashboard Saved(대시보드 저장) 메시지가 표시됩니다.

대시보드 레이아웃은 모든 세션 및 디바이스에 자동으로 적용됩니다.

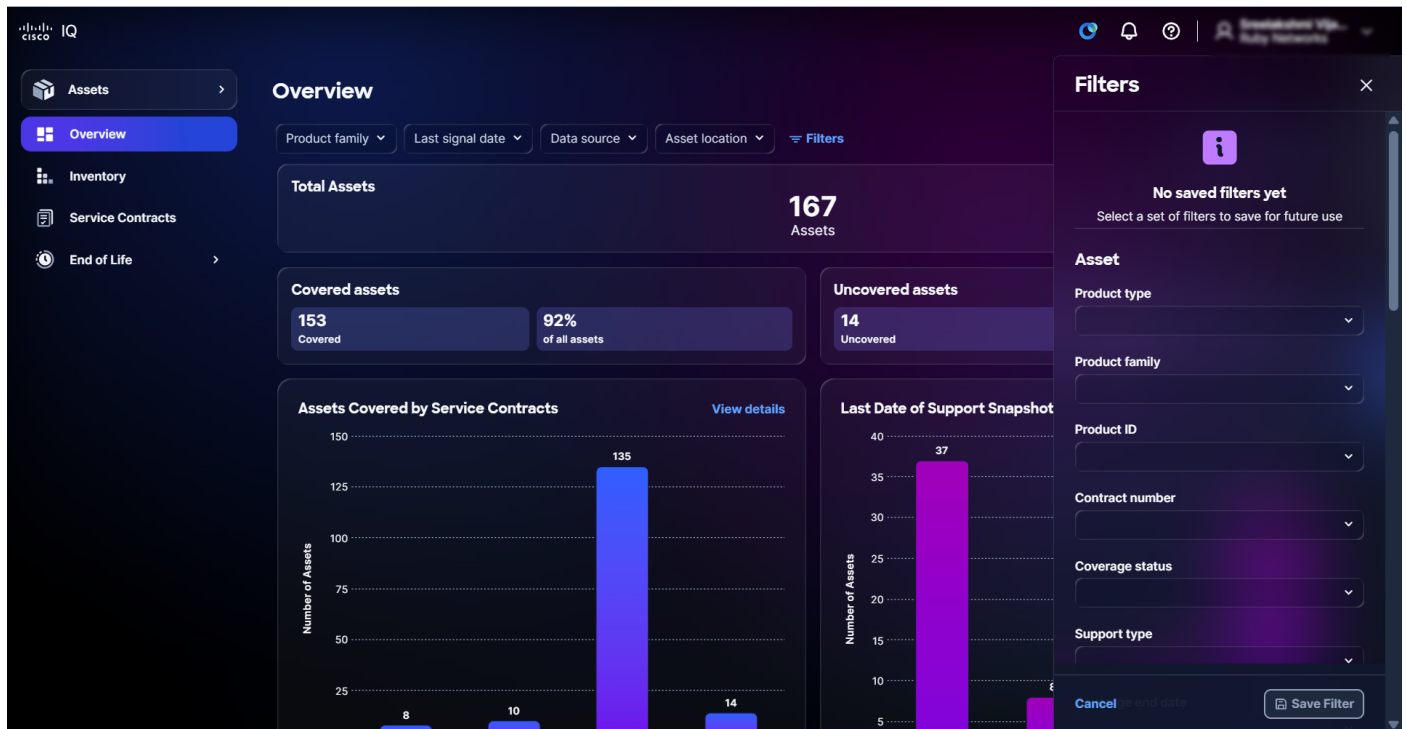
필터 사용자 정의

대시보드 보기의 사용자 지정 필터 구성을 저장할 수 있으므로 필요에 따라 원하는 설정으로 쉽게 돌아갈 수 있습니다. 모든 필터 기본 설정은 사용자별, 계정별로 안전하게 저장되므로 Cisco IQ에 액세스할 때마다 개별화되고 일관된 환경을 보장합니다.

필터 생성

사용자 지정 필터를 생성하려면

1. 대시보드로 이동합니다.
2. Filters를 클릭합니다.



필터

3. 드롭다운 목록에서 원하는 필터를 선택합니다.
4. Save Filter를 클릭합니다. Name Saved Filter 창이 열립니다.

Name saved Filter

Filter name *

Custom Filter |

Cancel

Save Filter

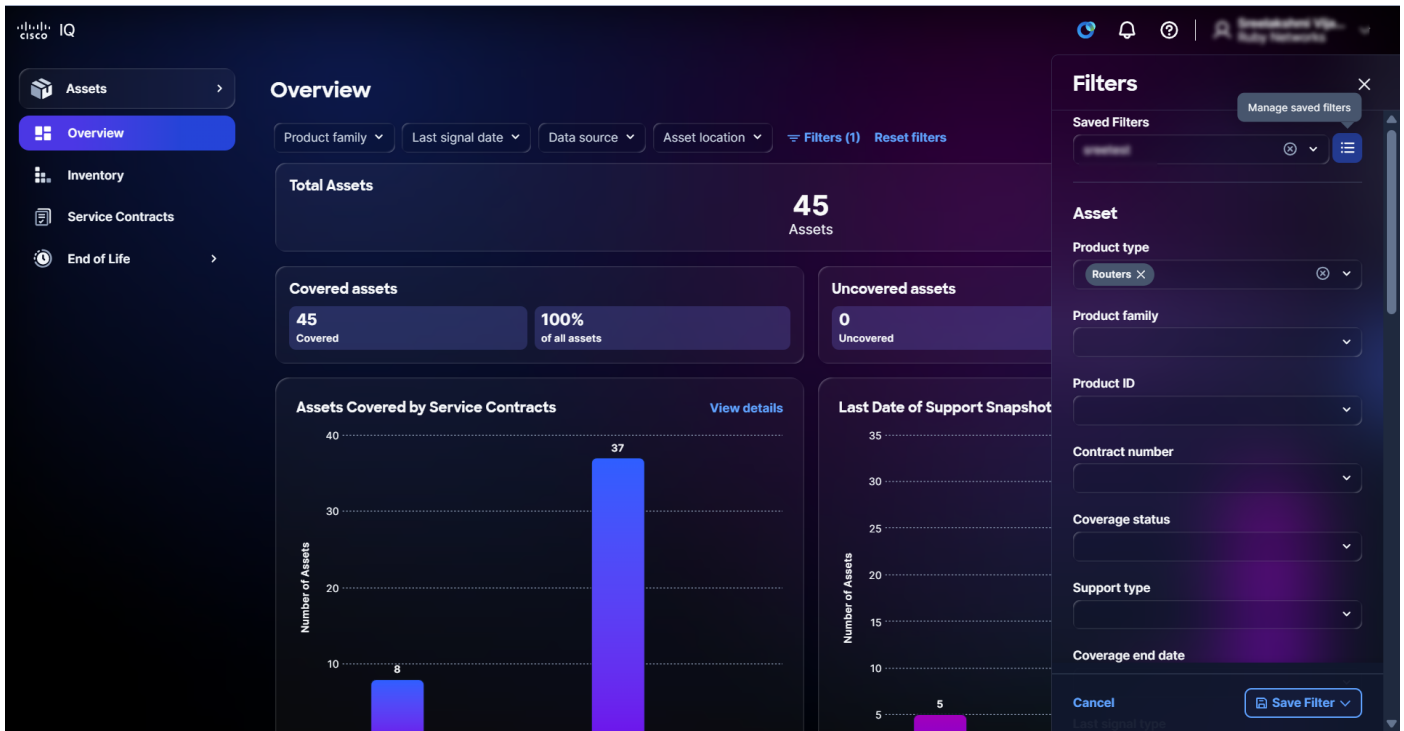
필터 이름

5. 필터 이름을 입력합니다.
6. Save Filter(필터 저장)를 클릭하여 확인합니다.

필터 이름 수정

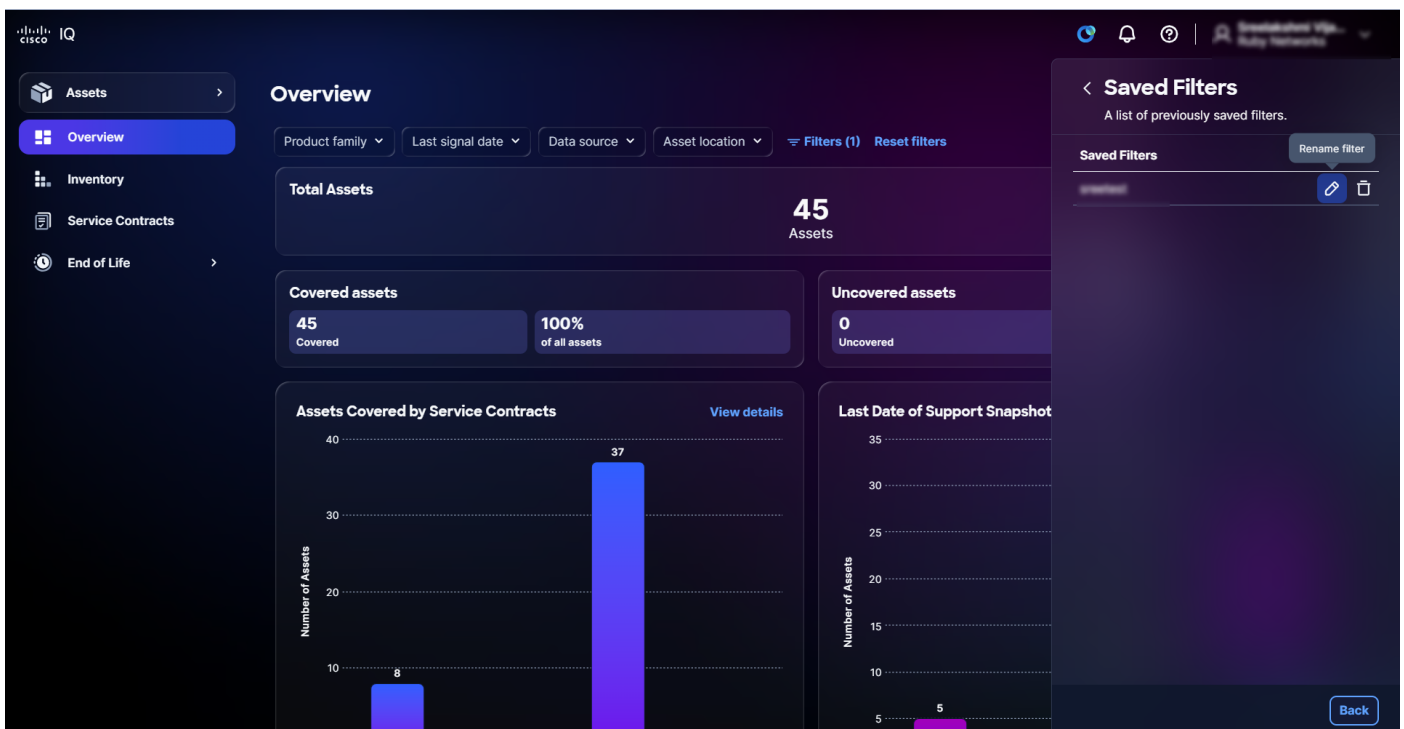
사용자 지정 필터를 수정하려면

1. Filters를 클릭합니다.



저장된 필터 관리

- 저장된 필터 관리 아이콘을 클릭합니다.
- 필터로 이동합니다.



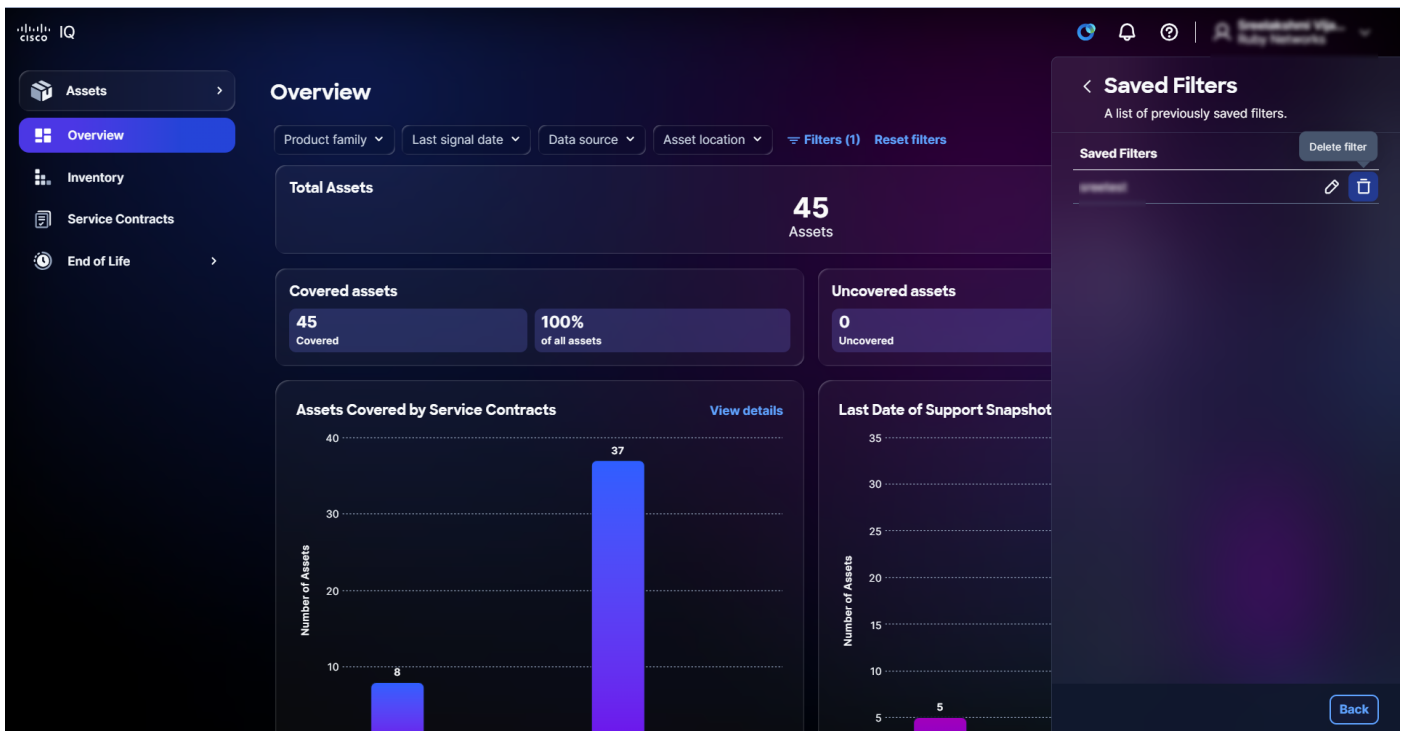
필터 편집

4. Edit(수정) 아이콘을 클릭합니다. Name saved Filter 창이 열립니다.
5. 필터 이름을 수정합니다.
6. Save Filter(필터 저장)를 클릭하여 확인합니다.

필터 삭제

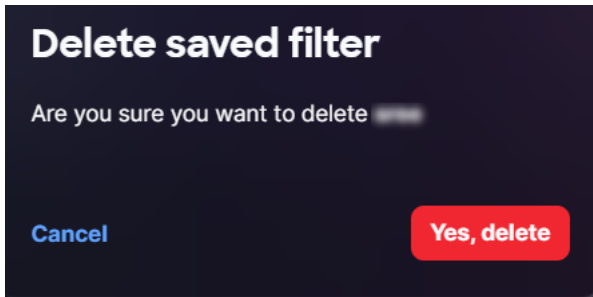
사용자 지정 필터를 삭제하려면

1. Filters를 클릭합니다.
2. 관리되는 저장된 필터 아이콘을 클릭합니다
3. 필터로 이동합니다.



저장된 필터 삭제

4. 삭제 아이콘을 클릭합니다. Delete saved filter 창이 열립니다.



저장된 필터 삭제 확인

5. 예, 삭제를 클릭하여 확인합니다.

Assets 모듈

Assets 모듈은 Cisco 자산에 대한 포괄적인 가시성 및 관리 기능을 제공하며 Cisco IQ의 기반으로 조직 내 모든 장치에 대한 중앙 집중식 목록을 제공합니다. 여러 소스에서 정보를 수집하므로 디바이스 인벤토리에 대한 단일 정보 소스 역할을 합니다. Cisco IQ 내의 다른 모듈(예: Assessments 모듈)은 이 데이터를 사용하여 디바이스의 상태 및 보안을 평가하는 것이므로 완전하고 정확한 자산 목록을 유지 관리하는 것이 중요합니다.

핵심 개념

Assets 모듈은 다음과 같은 핵심 개념을 기반으로 합니다.

- 자산: ID, 기능, 서비스 범위 및 라이프사이클을 상세하게 추적하여 Cisco의 서비스 제공의 일환으로 인벤토리 및 관리되는 모든 물리적 장치, 하드웨어 또는 소프트웨어
- 계약 소스 자산: 텔레메트리를 통하지 않고 연결된 서비스 계약 데이터에서 곧바로 인벤토리에 수집된 자산 Cisco IQ는 계약 데이터에서 다음 장비 유형을 수집합니다. 새시, 모듈, 전원 공급 장치 및 팬. 이러한 자산은 텔레메트리 연결이 없는 경우에도 인벤토리에 표시됩니다
- LDOS(Last Date of Support): Cisco 제품의 End-of-Life 및 End-of-Support 마일스톤 추적
- 서비스 커버리지: 특정 하드웨어 또는 소프트웨어와 관련된 활성 지원 계약, 보증 및 자격 레벨
- 자산 태그: 조직, 필터링 및 운영 워크플로를 위해 자산에 할당되는 사용자 정의 레이블
- 장치 신호: Cisco에서 장비 텔레메트리, 지원 사례 및 계약 갱신을 기반으로 (시리얼 번호로) 장비를 마지막으로 관찰한 시점을 가리킵니다. 멀티레이어 데이터 파이프라인을 통해 자산 텔레메트리 데이터 수집 및 보강

에셋 액세스 모듈

Cisco IQ의 자산 관리 기능에 액세스하려면 Home(홈) 메뉴 > Assets(자산)를 선택하거나 Home(홈) 페이지 > Launchpad(실행 패드) 탭의 Application(애플리케이션) 섹션에서 Assets(자산)를 클릭합니다. Overview(개요) 페이지가 표시됩니다.

자산 개요

Overview(개요) 페이지에는 디바이스의 상태 및 상태를 신속하게 평가할 수 있는 대시보드가 표시됩니다.

100% 400 Assets 100% 400 Assets 100% 400 Assets



Assets



Overview



Inventory



Service Contracts



End of Life



Overview

Filters

Ask AI

Customize

Saved Filters

Total Assets

199

Assets

928

Assets and subcomponents

Key Asset Metrics

Covered Assets

186

Covered

93%

Of all assets

Uncovered Assets

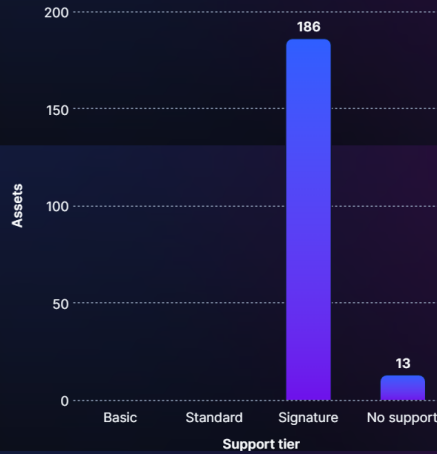
13

Uncovered

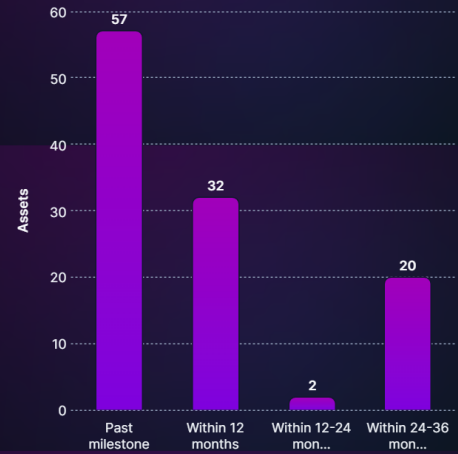
7%

Of all assets

Assets Covered by Service Contracts [View details](#)



Last Date of Support Snapshot [View details](#)



Assets With Telemetry Enabled

186

With telemetry

93%

Of all assets

Assets Without Telemetry Enabled

13

Without telemetry

7%

Of all assets

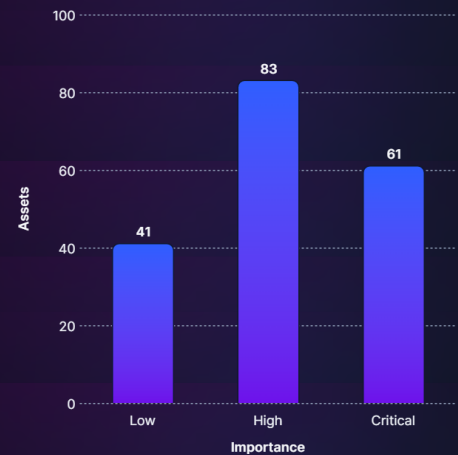
Assets With Critical or High Security Advisories [View details](#)



Of the 186 assets with telemetry enabled, 170 have critical or high Security Advisories

Assets by Importance [View details](#)

Importance can be evaluated for 185 assets.

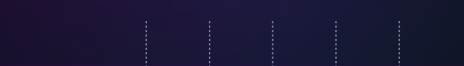


Asset Breakdown

Top 5 Product Families [View details](#)



Top 5 Install-At Locations [View details](#)



자산 개요

대시보드에는 다음 정보가 표시됩니다.

- 총 자산: Cisco IQ 어카운트 내 총 자산 수
- 주요 자산 메트릭: 텔레메트리 상태, 중요 보안 권고, LDOS 정보와 같은 추가 주요 메트릭
- 지원되는 자산: 서비스 계약으로 지원되는 자산의 총 수 및 비율
- 지원 대상이 아닌 자산: 서비스 계약이 적용되지 않는 자산의 총 수 및 비율
- 서비스 계약에서 다루는 자산: 서비스 계약에 포함되는 자산(하드웨어 또는 소프트웨어)의 수를 자격 수준별로 분류합니다.
- 지원 스냅샷 종료일: LDOS를 지나거나 LDOS에 도달한 자산 수 분석
- 텔레메트리 기능이 활성화된 자산: 텔레메트리 기능이 활성화된 자산의 총 수 및 비율
- 텔레메트리를 사용하지 않는 자산: 텔레메트리를 활성화하지 않은 자산의 총 수 및 비율
- 중요한 보안 권고 또는 높은 수준의 보안 권고를 받은 자산 텔레메트리를 사용하고 중요하거나 높은 수준의 보안 권고를 보유한 총 자산의 비율
- 중요도별 자산: 네트워크의 다른 디바이스에 상대적인 디바이스에 할당된 우선순위의 분석.
- 자산 분류: 제품군, 설치 위치, 소프트웨어 버전, 자산 역할 등 자산 정보의 자세한 표시

에셋 보기 필터링

드롭다운 목록에서 필터를 선택하거나 Filters(필터)를 클릭하고 사용 가능한 필터 목록에서 옵션을 선택하여 대시보드 보기를 필터링할 수 있습니다.

 참고: 화면 확대/축소 설정에 따라 일부 필터가 숨겨질 수 있습니다. 역할과 권한에 따라 서로 다른 필터를 사용할 수 있습니다.

에셋 세부사항 보기

View Details(세부 정보 보기)를 클릭하면 페이지가 Inventory(인벤토리) 페이지로 리디렉션됩니다. 자세한 [내용](#)은 인벤토리를 참조하십시오.

자산 중요도 인사이트

Cisco IQ에는 Assets 모듈의 새로운 기능인 Asset Criticality Insights가 포함되어 있습니다. 이 기능은 네트워크 장치의 기능적 역할과 비즈니스 중요성을 예측합니다. Asset Criticality Insights는 디바이스 컨피그레이션과 활성화된 기능을 분석하여 어떤 자산이 네트워크에 가장 큰 영향을 미치는지 파악할 수 있도록 합니다. 따라서 보안 리미디에이션, 소프트웨어 업그레이드, EOL(End-of-Life) 계획, 커버리지 결정에 있어 우선 순위를 지정할 수 있습니다.

 참고: Asset Criticality Insights는 활성 텔레메트리 연결이 있는 표준 또는 서명 수준의 자산에만 사용할 수 있습니다. 자산이 구성 요구 사항을 충족하는지 확인하여 대시보드에 이러한 정보를 입력해 주십시오.

Asset Criticality Insights는 다음 영역의 Assets 앱에서 사용할 수 있습니다.

- 자산 개요: Asset Criticality Insights 특성별로 요약 분석 필터링 및 보기
- 자산 인벤토리: 역할 및 중요도를 기준으로 디바이스를 표시, 검색, 필터링 및 정렬
- 자산 세부사항: 각 값을 설명하는 정보 툴팁과 함께 개별 디바이스의 역할 및 중요도 보기

역할 및 중요도 분류 재정의

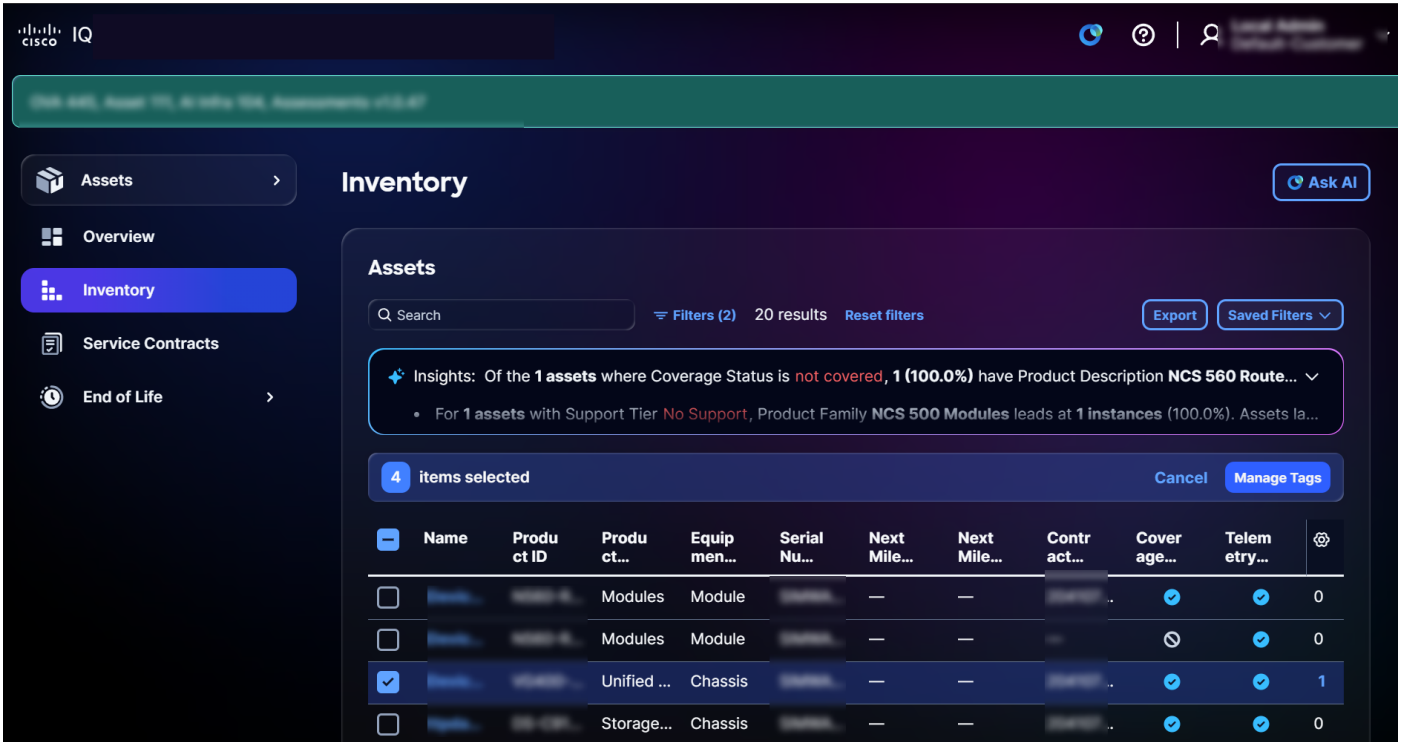
Cisco IQ는 텔레메트리 데이터를 기반으로 각 자산의 역할과 중요성을 자동으로 예측합니다. 자동화된 예측이 네트워크에 있는 자산의 기능이나 중요도를 정확하게 반영하지 못하는 경우 계정 관리자는 이러한 분류를 수동으로 수정할 수 있습니다.

 참고: 재정의 제어는 계정 관리자만 사용할 수 있습니다. 역할 및 중요도 값은 다른 모든 사용자 역할에 대해 읽기 전용입니다.

재고 테이블에서 분류 대체

하나 이상의 자산에 대한 역할 또는 중요도를 대체하려면

1. Assets > Inventory로 이동합니다.
2. 원하는 자산 행의 확인란을 클릭합니다. 여러 에셋을 동시에 업데이트하려면 여러 확인란을 선택합니다.



역할 및 중요성

3. Role 또는 Importance 열의 자산 행 드롭다운 목록에서 올바른 값을 선택합니다.
4. Apply(적용)를 클릭하여 재정의의 확인합니다.

수동으로 재정의된 값이 있는 에셋은 역할 또는 중요도 열에 시각적 표시기를 표시합니다.

 참고: 이전에 구성한 재정의의 제거하고 자동 예측으로 돌아가려면 Role 또는 Importance 드롭다운 목록에서 대시(—) 옵션을 선택합니다.

자산 상세내역에서 분류 대체

자산 상세내역 뷰에서 역할 또는 중요도를 대체하려면

1. Assets > Inventory로 이동하고 자산을 클릭합니다.
2. Asset details(자산 세부사항) 패널에서 Role(역할) 및 Importance(중요도) 필드를 찾습니다.
3. 업데이트할 필드의 드롭다운을 클릭하고 올바른 값을 선택합니다.
4. Apply(적용)를 클릭하여 확인합니다.

자산의 세부 정보 보기에는 원래의 자동화된 예측을 알려 주는 텔레메트리 속성에 대한 설명도 표

시되므로 재정의를 적절한지 여부를 판단하는 데 도움이 됩니다.

재정의 감사 추적 보기

모든 역할 및 중요도 재정의를 계정 레벨 감사 추적에 기록됩니다. 감사 추적에 액세스하려면

- 1. Home(홈) > System Settings(시스템 설정) > Activity & Logs(활동 및 로그)를 선택합니다.
- 2. Filters(필터) > Action Type(작업 유형) > override(재정의)를 선택하여 재정의를 이벤트만 표시합니다.

감사 추적에는 자산 이름, 이전 및 새 값, 변경한 사용자, 변경 날짜 및 시간이 표시됩니다. Export(내보내기) 옵션을 사용하여 감사 추적을 내보낼 수 있습니다.

 참고: 감사 추적은 날짜 범위, 사용자 및 자산 이름으로 필터링할 수 있습니다.

인벤토리

Inventory(인벤토리) 페이지는 Cisco IQ 어카운트에 속한 모든 Cisco 자산의 목록을 제공합니다.

 IQ

Assets

Overview

Inventory

Service Contracts

End of Life

Inventory

Assets

Search

1 Equipment type

Filters (1) Reset filters

Export Saved Filters

Insights: Among the 13 assets with Telemetry Status Not Connected, Support Tier NO SUPPORT is the most frequen...

With a Partition Key of "(empty)", 10 of the 13 assets have the Next Milestone as End Of Sale (40.0%). As these produc...

☐	Name	Produ ct ID	Produ ct...	Equip men...	Serial Nu...	Next Mile...	Next Mile...	Contr act...	Cover age...	Telem etry...	
☐			Cloud a...	Chassis		End of ...	Jun 25, ...	204107...			0
☐			Wireless	Chassis		—	—	204107...			0
☐			Wireless	Chassis		—	—	204107...			0
☐			Routers	Chassis		—	—	204107...			8
☐			Routers	Chassis		End of ...	Feb 19, ...	204107...			0
☐			Switches	Chassis		—	—	204107...			10

인벤토리

자산 인벤토리에 대한 뷰 검색 및 필터링

드롭다운 목록에서 필터를 선택하거나 Filters(필터)를 클릭하고 사용 가능한 필터 목록에서 옵션을 선택하여 목록 뷰를 필터링할 수 있습니다. 또한 Search(검색) 필드에 자산 이름을 입력하여 자산을 검색할 수도 있습니다.

참고:

- 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다.
- 역할과 권한에 따라 서로 다른 필터를 사용할 수 있습니다.

인벤토리 분석

Inventory 페이지의 Insights 패널은 지원 커버리지, 연결성, 주요 시점을 중심으로 자산 요약を提供하는 AI 기반 분석을 표시합니다. 그래프, 대시보드, 차트와 같은 시각화를 위한 전체 분석을 클릭하여 추가적인 통찰력을 제공합니다. 자세한 [내용은](#) 공통 모듈 기능의 데이터 분석을 참조하십시오.

인벤토리 내보내기

Export(내보내기)를 클릭하여 필터링된 인벤토리 목록을 .xls 또는 .csv 형식으로 저장합니다. 자세한 [내용은](#) 공통 모듈 기능의 정보 내보내기를 참조하십시오.

자산 상세내역 조회

자산 세부사항을 보려면 자산을 클릭합니다. 다음 탭과 함께 에셋의 세부사항 보기가 표시됩니다.

- 세부 정보: 제품, 신호 데이터, ID, 위치, 보증 및 커버리지 정보와 같은 자산 세부 정보를 표시합니다.

Assets

Overview

Inventory

Service Contracts

End of Life

← Inventory

10.197.236.131

Ask AI

Cisco Catalyst Center Appliance (Gen 2) - 44 Core

Details

Product Alerts

Hardware

Software

Product

Product ID

Product type

Product family

Last Date of Support

Identity

Serial number

IP address

Hostname

Software version

Role

Importance

Tags

Sold by

Location

Install-at

Signals

Last signal

Last signal type

Telemetry

Telemetry status

Last data collection

Data connector

Warranty

Warranty type

Warranty end date

Coverage

Coverage status

Contract number

Support tier

Coverage end date

자산 세부사항

- **제품 알림:** Security Advisories 및 Field Notice와 같은 관련 제품 경고를 표시합니다.

- 하드웨어: 하드웨어 EOL(예: End of Sale, Last Ship, Last Date of Support 날짜)에 대한 자세한 일정 보기 제공
- 소프트웨어: 소프트웨어 EOL에 대한 자세한 일정 보기 제공

자산 태그

자산 태그는 Cisco IQ의 인벤토리 자산에 할당하는 사용자 지정 라벨입니다. 태그는 사용자가 정의하는 키:값 쌍(예: Environment:Prod 또는 Label:Campus)입니다. 개별 자산 또는 여러 자산에 태그를 한 번에 할당할 수 있으며, 관심 있는 자산을 빠르게 찾기 위해 인벤토리를 태그별로 필터링할 수 있습니다.



참고: 어카운트 관리자가 태그를 생성하면 사용자는 자산에 태그를 할당할 수 있습니다.

태그 할당

인벤토리 보기에서 선택한 자산에 태그를 할당하면 향상된 필터링, 보고 및 관리를 위해 자산을 구성하고 분류할 수 있습니다.

자산에 태그를 지정하려면

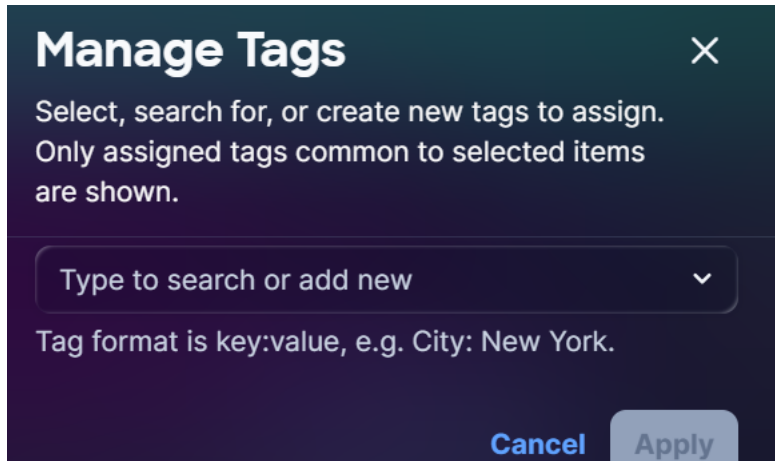
1. Assets > Inventory로 이동합니다.

The screenshot shows the Cisco IQ Inventory page. The left sidebar contains navigation links: Assets, Overview, Inventory (selected), Service Contracts, and End of Life. The main content area is titled 'Inventory' and includes a search bar, a 'Filters' button, and an 'Export' button. Below the search bar, there is an 'Insights' section with a dropdown menu showing 'Of the 27 assets with a Partition Key of "", Support Tier "NO SUPPORT" is the most common, with 27 (100.0...)'. Below the insights, there is a table with 2 items selected. The table has columns: Name, Product ID, Equipment, Serial Number, Next Mile, Contract, Coverage, and Telemetry. The first row is selected and shows 'Chassis' equipment. The second row is also selected and shows 'Chassis' equipment. The table is followed by a 'Manage Tags' button.

Name	Product ID	Equipment	Serial Number	Next Mile	Contract	Coverage	Telemetry
[selected]	[selected]	Chassis	[selected]	End of ...	Jun 25, ...	204107...	0
[selected]	[selected]	Chassis	[selected]	—	—	204107...	0

태그 지정 자산

- 원하는 에셋의 확인란을 선택합니다.
- Manage Tags(태그 관리)를 클릭합니다. Manage Tags 창이 열립니다.



태그 할당

- 텍스트 필드에 기존 옵션에서 태그 이름을 입력하거나 선택하고 Enter 키를 누릅니다.



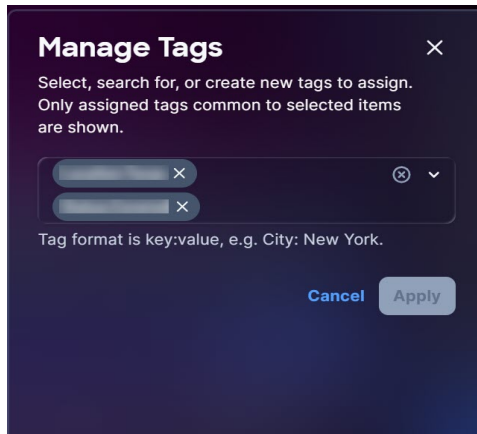
참고: 태그는 key:value 형식(예: City:NYC)입니다.

- 적용을 클릭합니다.

자산 태그 제거

하나 이상의 에셋에서 태그를 제거하려면

- Assets > Inventory로 이동합니다.
- 하나 이상의 에셋 옆에 있는 확인란을 선택합니다.
- 태그 관리를 클릭합니다. 태그 관리 창이 열립니다.



태그 제거

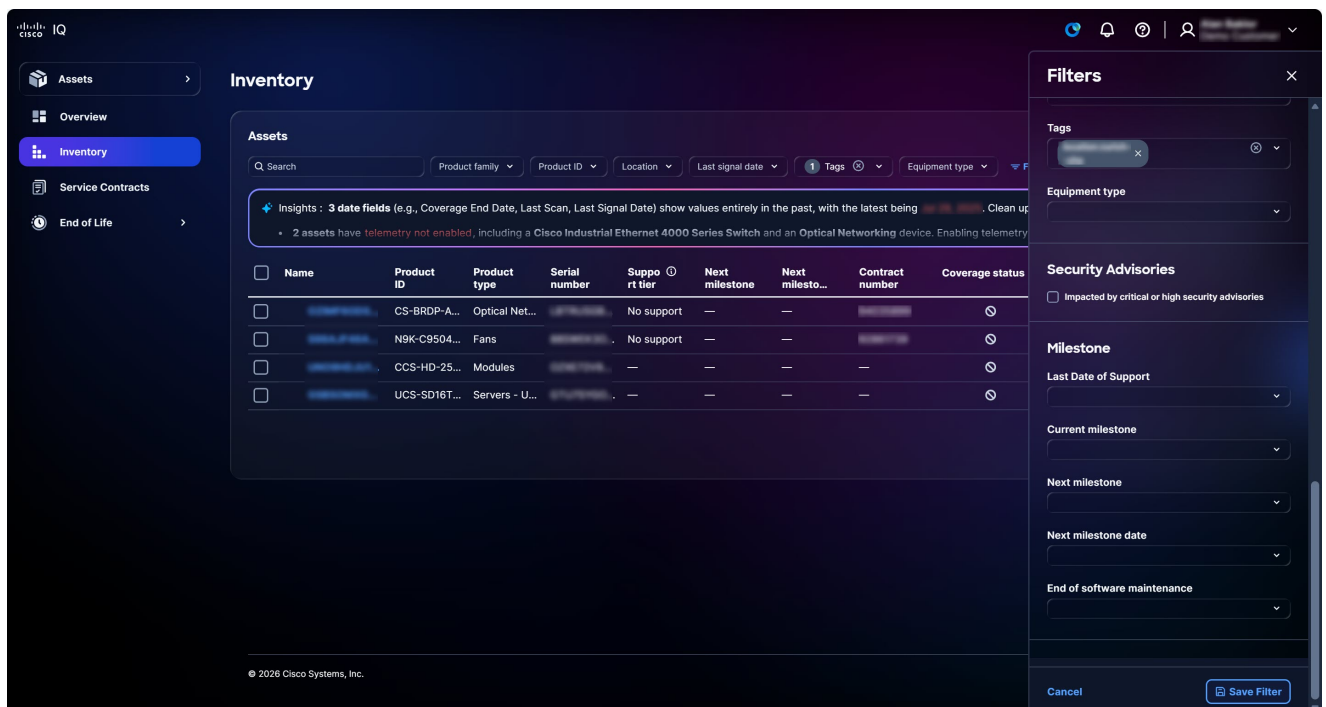
4. 선택 영역에서 제거하려면 임의의 태그에 X를 클릭합니다.
5. 적용을 클릭합니다.

자산 태그를 필터로 사용

태그를 생성한 후에는 해당 태그를 필터로 사용할 수 있습니다.

태그를 필터로 사용하려면

1. Inventory(인벤토리) 페이지로 이동합니다.
2. Filters를 클릭합니다. 필터 창이 열립니다.

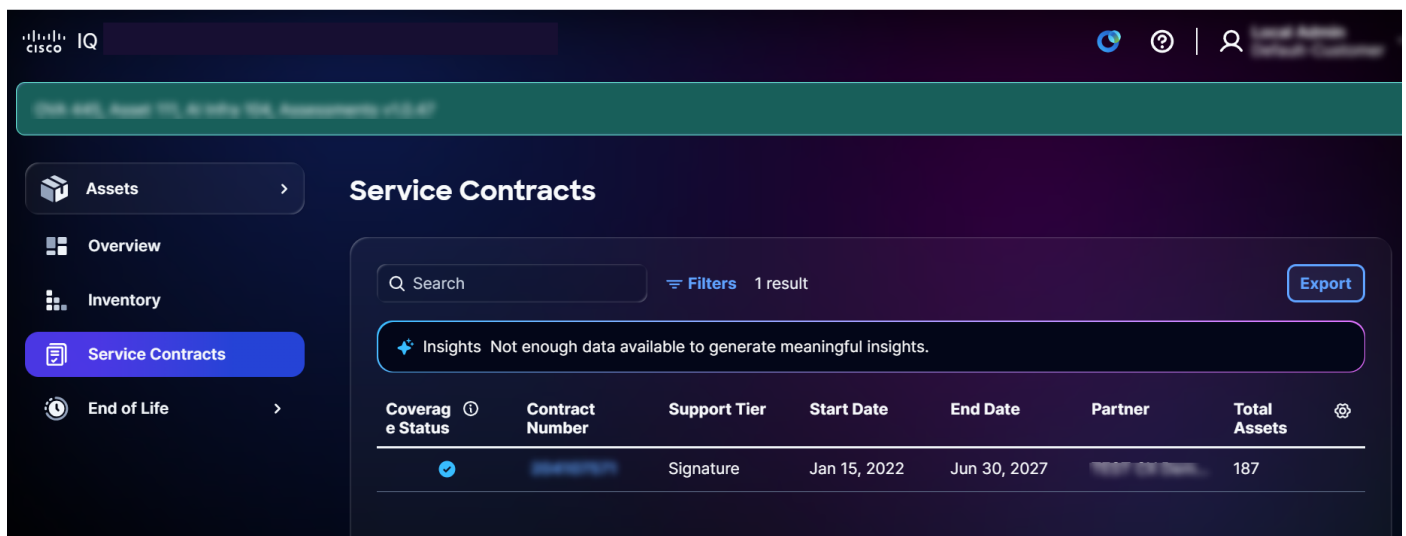


태그를 필터로 사용

3. Tags 드롭다운 목록에서 원하는 태그의 확인란을 선택합니다. 태그를 선택하면 Inventory(인벤토리) 페이지의 보기가 필터링된 보기로 업데이트됩니다.

서비스 계약

Service Contracts(서비스 계약) 페이지는 요약과 세부 계약 정보를 제공하여 효과적인 갱신 계획 및 커버리지 전략을 지원함으로써 계약 관리를 간소화합니다.



Coverage Status	Contract Number	Support Tier	Start Date	End Date	Partner	Total Assets
✓	██████████	Signature	Jan 15, 2022	Jun 30, 2027	██████████	187

서비스 계약

서비스 계약에 대한 뷰 검색 및 필터링

드롭다운 목록에서 필터를 선택하여 목록 보기를 필터링할 수 있습니다. Search(검색) 필드에 계약 번호를 입력하여 서비스 계약을 검색할 수도 있습니다.

서비스 계약 내보내기

Export(내보내기)를 클릭하여 필터링된 계약 목록을 .xls 또는 .csv 형식으로 저장합니다. 자세한 [내용은](#) 공통 모듈 기능의 정보 내보내기를 참조하십시오.

서비스 EA 요약

Services Enterprise Agreement (EA) Summary(서비스 기업 계약) 요약 페이지에서는 자산 포트폴

리오의 전체 Install Base 증가에 대한 통합 보기를 제공합니다. 데이터는 Cisco의 Install Base 레코드에서 직접 제공되므로 사용자와 어카운트 팀은 포트폴리오의 변화에 대해 시간의 경과에 따라 일관되게 파악할 수 있습니다.

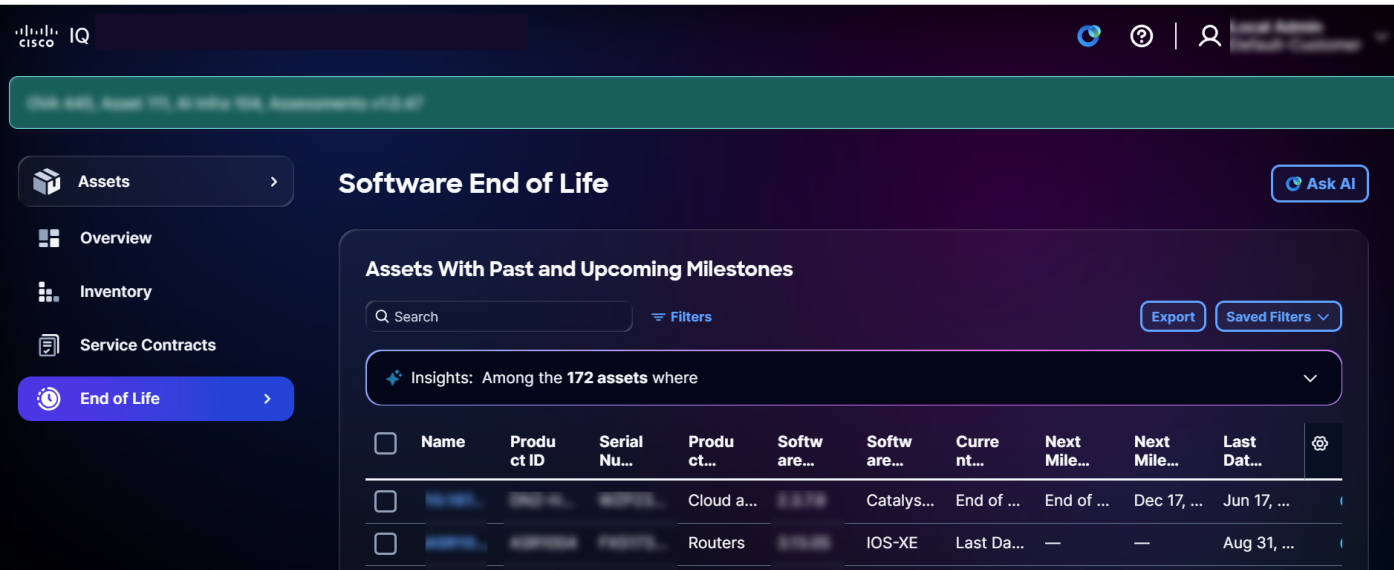
서비스 EA 요약 페이지는 다음 정보를 표시합니다.

- 추가된 자산: 보고 기간 동안 Install Base에 추가된 새 자산
- 순 변경: 보고 기간 동안 Install Base 규모의 전반적인 변경

 참고: 서비스 EA 요약 페이지에 대한 액세스는 역할 및 권한 요구 사항의 영향을 받을 수 있습니다. 이 페이지가 탐색에 표시되지 않으면 계정 관리자에게 문의하십시오.

단종

Hardware End of Life 및 Software End of Life 페이지는 제품 교체 주기 및 지원 범위를 사전 대응적으로 관리하는 데 필요한 지원을 사용자에게 제공함으로써 자세한 EOL 정보를 제공합니다. End of Life 페이지에서 자산을 누르면 Inventory 페이지의 관련 자산으로 리디렉션됩니다.



☐	Name	Product ID	Serial Number	Product Name	Software Version	Software Name	Current Milestone	Next Milestone	Next Milestone Date	Last Day of Support	
☐	Cloud a...			Cloud a...	2.2.18	Catalys...	End of ...	End of ...	Dec 17, ...	Jun 17, ...	
☐	Routers			Routers	2.2.18	IOS-XE	Last Da...	—	—	Aug 31, ...	

소프트웨어 단종

End of Life 분석

End of Life 페이지의 Insights 패널에는 AI 중심의 자산 개요와 정의된 Last Day of Support가 표시됩니다. 그래프, 대시보드, 차트와 같은 시각화를 위한 전체 분석을 클릭하여 추가적인 통찰력을 제공합니다. 자세한 내용은 [내용은](#) 공통 모듈 기능의 데이터 분석을 참조하십시오.

단종 내보내기

Export(내보내기)를 클릭하여 필터링된 EOL 자산 목록을 .xls 또는 .csv 형식으로 저장합니다. 자세한 [내용은](#) 공통 모듈 기능의 정보 내보내기를 참조하십시오.

평가 모듈

Assessments 모듈은 보안, 안정성, 용량, 규정 준수, 노후화와 관련된 위험을 사전에 조사하고 완화할 수 있는 평가 프레임워크를 제공하여 네트워크의 보안, 안정성, 안정성을 유지합니다.

핵심 개념

평가 모듈은 다음과 같은 핵심 개념을 기반으로 합니다.

- 평가: 성능, 규정 준수, 보안 또는 운영 능력을 측정하기 위해 사전 정의된 기준에 따라 인프라 엔터티를 체계적으로 평가 평가는 온디맨드, 일정 또는 이벤트에 의해 트리거됩니다
- 평가 실행: 평가 인스턴스 또는 단일 실행 각 실행은 범위, 트리거 메커니즘, 타임스탬프 및 평가에 의해 생성된 결과 데이터를 추적하는 새 실행 레코드를 생성합니다
- 찾기: 격차, 위험, 문제 또는 주목해야 할 상태를 식별하는 검증되고 실행 가능한 관찰. 조사 결과는 평가 과정에서 그라운드 레벨 데이터를 나타냅니다.
- 인사이트: 여러 연구 결과에 대한 패턴 또는 경향에서 파생된 더 높은 수준의 분석 결론. 통찰력은 조사 결과가 더 광범위한 비즈니스 또는 운영 맥락에서 무엇을 의미하는지 해석합니다.
- 권장 사항: 발견이나 통찰과 관련된 실행 가능한 구체적인 처방 권장 사항은 식별된 문제를 해결하거나 기회를 활용하기 위해 필요한 단계에 대한 명확한 지침을 제공합니다
- 보고서: 대상 고객에 대한 조사 결과, 통찰력 및 권장 사항을 종합하는 구조화된 문서 보고서는 고객, 경영진 및 기술 팀에 평가 결과를 전달하기 위한 주요 결과물입니다

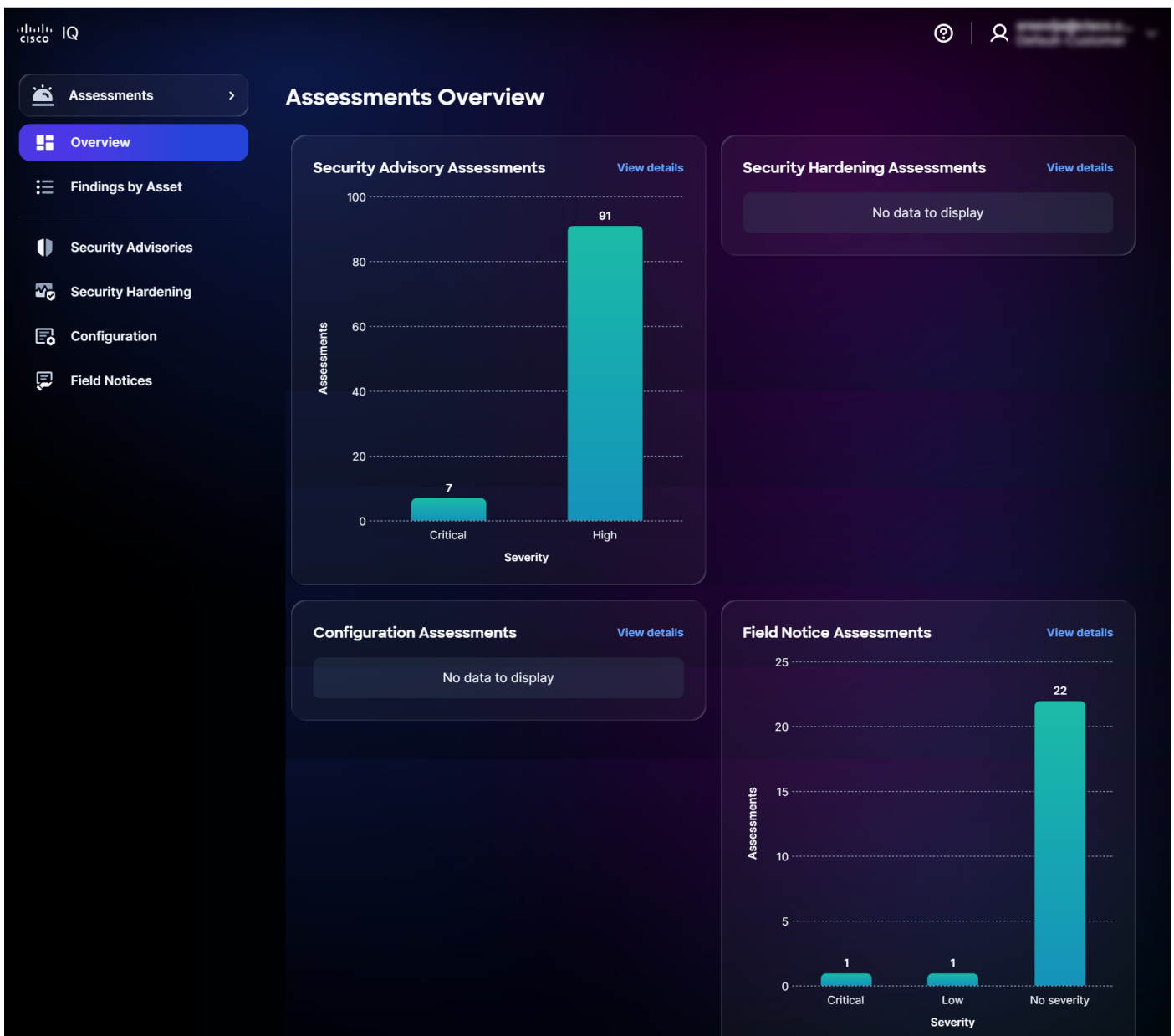
평가 모듈 액세스

Virtual Appliance의 보안 및 평가 기능에 액세스하려면 Home(홈) 메뉴 > Assessments(평가)를 선택하거나 Home(홈 페이지) > Launchpad(실행 패드) 탭의 Application(애플리케이션) 섹션에서 Assessments(평가)를 클릭합니다. 평가 개요 페이지가 표시됩니다.

 참고: System Configuration(시스템 컨피그레이션) > Package Management(패키지 관리)에서도 평가 모듈을 시작할 수 있습니다.

평가 개요

[평가 개요] 페이지에는 다음 대시보드가 표시됩니다.



평가 개요

대시보드에는 다음 정보가 표시됩니다.

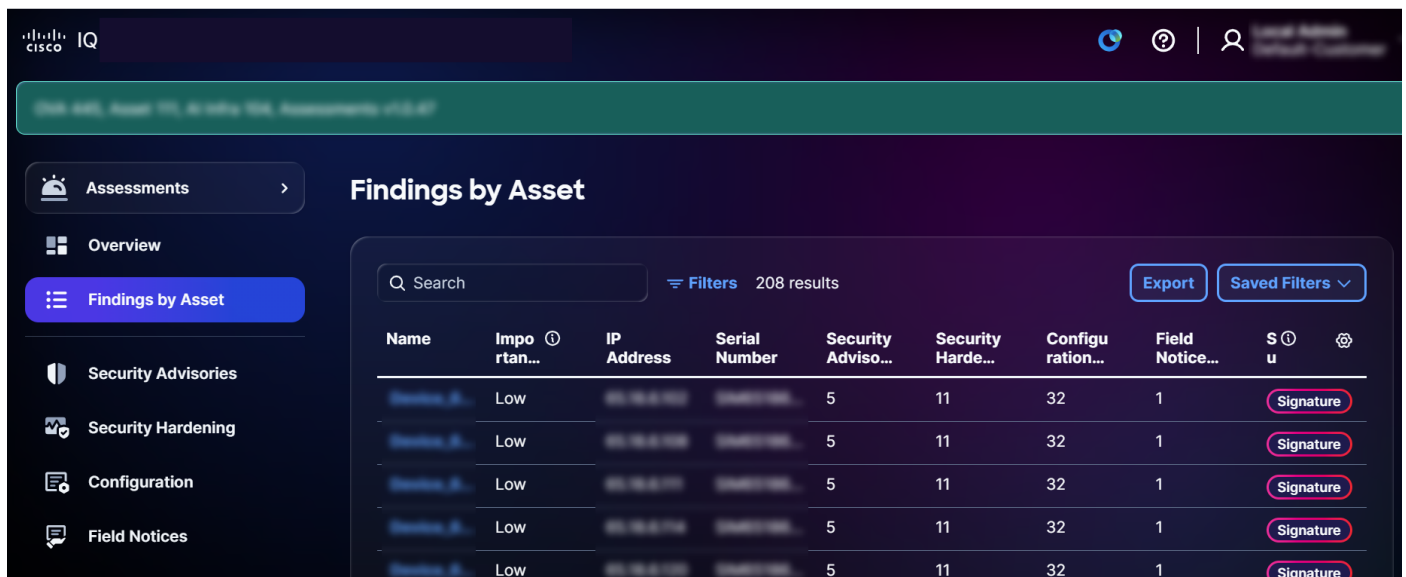
- 보안 자문 평가: 보안 권고에 대한 평가를 Critical(중대) 및 High(높음) 심각도별로 구분하여 표시합니다.
- 보안 강화 평가: 보안 강화 규칙에 실패한 자산을 High(높음), Medium(중간), Low(낮음) 및 Informational(정보) 심각도로 분류하여 표시합니다.

- 구성 평가: 컨피그레이션 규정 준수에 실패한 자산을 Critical(중대), High(높음), Medium(중간), Low(낮음) 및 Informational(정보) 심각도별로 분류하여 표시합니다.
- 필드 알림 평가: Critical(심각), High(높음) 및 Not applicable severity(해당 없음 심각도)별로 범주화된 필드 알림의 평가를 표시합니다.

 참고: 액세스 권한이 있는 자산만 볼 수 있습니다.

자산별 조사 결과

[자산별 검색 결과] 페이지는 다음 평가 중 하나 이상을 사용하여 평가된 자산 목록을 제공합니다. 보안 권고, 보안 강화, 구성 및 필드 알림



Name	Importance	IP Address	Serial Number	Security Advisory	Security Hardening	Configuration	Field Notice	Signature
...	Low	...	...	5	11	32	1	Signature
...	Low	...	...	5	11	32	1	Signature
...	Low	...	...	5	11	32	1	Signature
...	Low	...	...	5	11	32	1	Signature
...	Low	...	...	5	11	32	1	Signature

자산별 결과

자산별 검색 결과 보기 검색 및 필터링

드롭다운 목록에서 필터를 선택하거나 Filters(필터)를 클릭하고 사용 가능한 필터 목록에서 옵션을 선택하여 목록 뷰를 필터링할 수 있습니다. Search(검색) 필드에서 Findings by Asset(자산별 검색 결과)을 검색할 수도 있습니다.

 참고:

- 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다.
- 역할과 권한에 따라 서로 다른 필터를 사용할 수 있습니다.

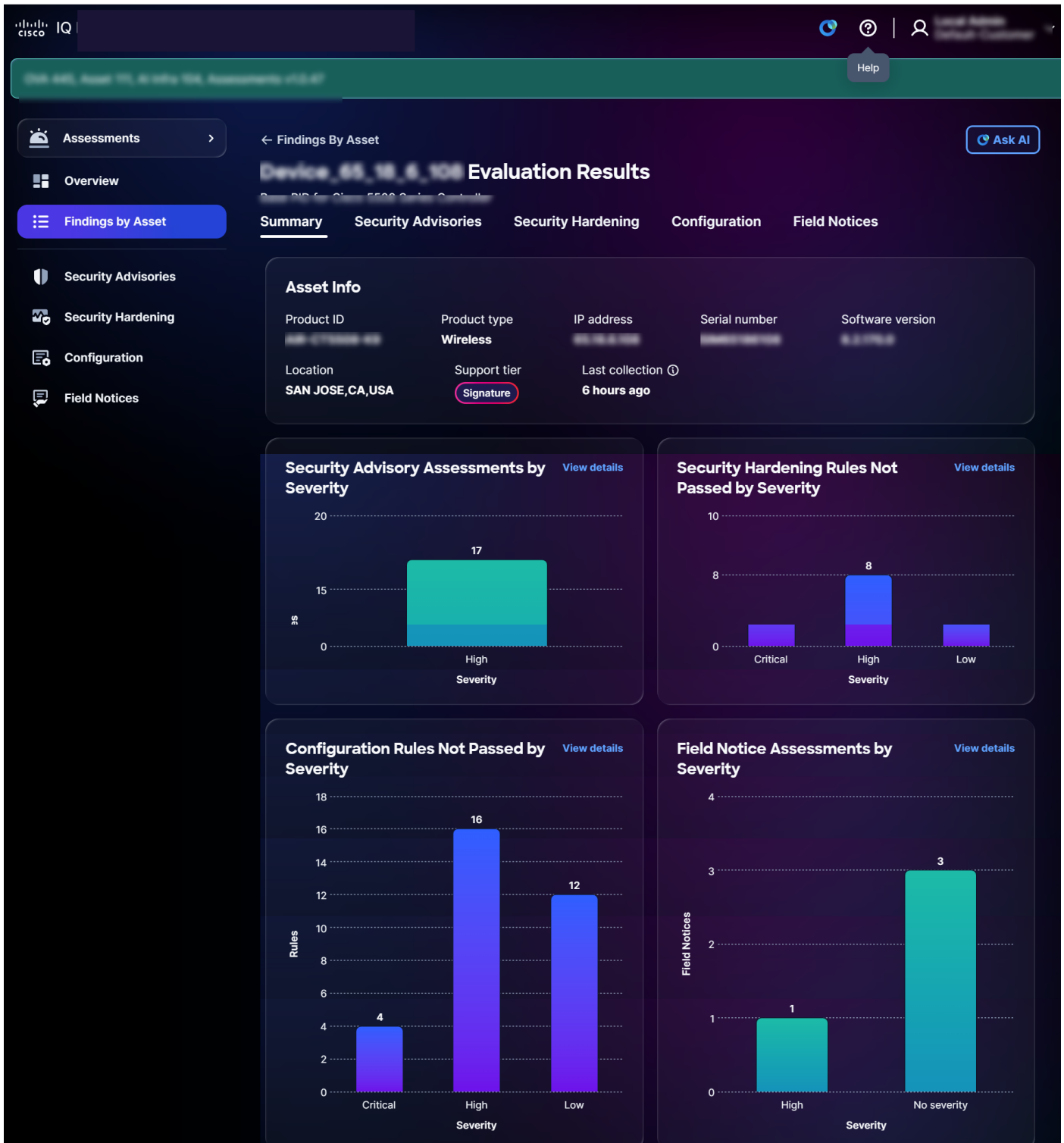
자산별 검색 결과 내보내기

Findings by Asset 목록 뷰를 내보내려면 Export를 클릭합니다. 자세한 [내용은 정보](#) 내보내기를 참조하십시오.

자산 상세내역별 결과 보기

자산 세부 정보로 검색 결과를 보려면 자산을 클릭합니다. 다음 탭에는 선택한 자산에 대한 세부사항이 표시됩니다.

- 요약: 보안 권고 사항, 보안 강화, 구성, 필드 알림의 수를 포함한 자세한 자산 정보를 제공합니다.
- 보안 권고: 관련 보안 자문 평가 목록 제공
- 보안 강화: 보안 강화 규칙에 실패한 자산 목록 제공
- 설정: 컨피그레이션 모범 사례 규칙에 실패한 자산 목록 제공
- 필드 알림: 관련 Field Notice 평가 목록 제공



자산 세부사항별 검색 결과

타일에서 View Details(세부 정보 보기)를 클릭하면 페이지가 모듈 내의 관련 페이지로 리디렉션됩니다.

전체 자산 세부 정보 보기를 클릭하면 자산 세부 정보 보기 페이지가 표시됩니다.

보안 자문

보안 자문 평가를 통해 취약점을 식별하고 위험도, 심각도, 심각도를 기준으로 우선 순위를 정함으로써 조직의 위험 관리 기능을 향상시킬 수 있습니다. Security Advisories는 취약성에 대한 세부적인 정보를 제공하고, 중요한 위협을 신속하게 완화하고, 규정 준수 및 비즈니스 목표에 부합하도록 보장합니다. 이를 통해 보안 상태를 강화하고, 리소스 할당을 최적화하며, 기업 전반에서 진화하는 위협에 대한 복원력을 강화할 수 있습니다. 보안 권고는 릴리스되는 즉시 Cisco IQ에서 자동으로 업데이트됩니다.

Security Advisories 페이지는 조직 내에서 탐지된 취약성이 있는 모든 Security Advisories 목록을 제공합니다. Security Advisory(보안 권고) 평가 목록에서 권고 사항을 클릭하면 해당 세부 정보 보기로 이동합니다.

Assessment	Severity	Affected Assets	Potentially Affected...	CVE	Last Updated
Cisco IOS and I...	High	0	12	Cisco IOS and I...	Oct 4, 2019
Cisco IOS and I...	High	0	1	Cisco IOS and I...	Sep 25, 2019
Cisco IOS and I...	High	1	0	Cisco IOS and I...	Mar 23, 2016
Multiple Vulner...	High	0	1	Multiple Vulner...	Jan 11, 2016
Cisco IOS and I...	High	0	1	Cisco IOS and I...	Jul 26, 2017
Cisco IOS and I...	High	1	0	Cisco IOS and I...	Sep 28, 2016

보안 자문

보안 권고 사항에 대한 뷰 검색 및 필터링

드롭다운 목록에서 필터를 선택하여 목록 보기를 필터링할 수 있습니다. 또한 Search(검색) 필드에 평가 이름을 입력하여 보안 자문 평가를 검색할 수도 있습니다.

 참고: 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다. 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다. 역할과 권한에 따라 서로 다른 필터를 사용할 수 있습니다. 누락된 심각도 값은 설명 도구 설명과 함께 "-"로 표시됩니다.

보안 권고 내보내기

보안 자문 평가를 내보내려면 내보내기를 클릭합니다. 자세한 [내용은 정보](#) 내보내기를 참조하십시오.

보안 자문 평가 세부 정보 보기

Assessment(평가)를 클릭하여 이에 대한 추가 세부 정보를 봅니다. 세부사항 페이지에는 CVSS(Common Vulnerability Scoring System) 점수, CVE(Common Vulnerabilities and Exposures), 심각도, 참조된 Cisco Security Advisory에 대한 링크와 같은 정보가 제공됩니다.

평가 결과 테이블에서 다음 유형의 결과를 볼 수 있습니다.

- 영향: 자산 또는 구성 요소에 공격자가 악용할 수 있는 확인된 취약성이 있어 교정이 필요함을 나타냅니다
- 영향을 받을 수 있음: 자산 또는 구성 요소에 취약성으로 이어질 수 있는 징후가 표시되지만 명확하게 확인되지 않음을 나타냅니다. 추가 조사가 필요할 수 있다

The screenshot displays the Cisco IQ interface for Security Advisories. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories (selected), Security Hardening, Configuration, and Field Notices. The main content area is titled 'Cisco IOS and IOS XE Software Session Initiation Protocol Denial of Service Vulnerability'. It includes an 'About the Assessment' section with a description of the vulnerability, a 'Show more' link, and a table with columns for Severity (High), CVE (CVE-2019-11904), CVSS score (9.8), Version (1.1), First published (Sep 25, 2019), and Last updated (Oct 4, 2019). Below this is a 'References' section with a link to the Security Advisory. The 'Asset Results' section shows a table with 12 results, all marked as 'Potentially Affected'. The table columns are Asset, Result, Product ID, IP Address, Serial Number, and Support Tier. Each row has a 'Signature' link.

Asset	Result	Product ID	IP Address	Serial Number	Support Tier
ISR44...	Potentially Affected				Signature
ISR43...	Potentially Affected				Signature
Isr4431	Potentially Affected				Signature
ISR43...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR43...	Potentially Affected				Signature

보안 자문 세부사항

자산 평가 결과에 대한 뷰 검색 및 필터링

드롭다운 목록에서 필터를 선택하거나 Filters(필터)를 클릭하고 사용 가능한 필터 목록에서 옵션을 선택하여 목록 뷰를 필터링할 수 있습니다. 또한 Search(검색) 필드에 자산 이름을 입력하여 자산을 검색할 수도 있습니다.



참고: 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다. 역할과 권한에 따라 다른 필터를 사용할 수 있습니다.

자산 평가 결과 보기

평가 결과의 세부 정보를 보려면 Assessment Outcome(평가 결과) 테이블에서 자산을 클릭합니다. 자산의 평가 결과 세부 정보 페이지가 표시됩니다.

The screenshot displays the Cisco IQ interface for a security advisory. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories (highlighted), Security Hardening, Configuration, and Field Notices. The main content area shows the 'Result' for a 'Cisco Secure Boot Hardware Tampering Vulnerability'. It includes a 'Result Details' section with a 'Potentially affected' warning, an 'Evidence' section listing matches on software type, chassis product ID, and module product ID, and an 'Additional Verification Needed' section with instructions. Below this is an 'About the Assessment' section detailing the vulnerability, its severity (High), CVE, CVSS score (6.7), and publication dates. The bottom section, 'About the Asset', provides details for the affected device, including Product ID, Product type (Switches), IP Address, Serial Number, Software version, Location (SAN JOSE, CA, USA), and Support tier (Signature).

결과 세부사항

보안 권고에 대한 자산 결과 내보내기

자산 결과를 내보내려면 내보내기를 누릅니다. 자세한 [내용은 정보](#) 내보내기를 참조하십시오.

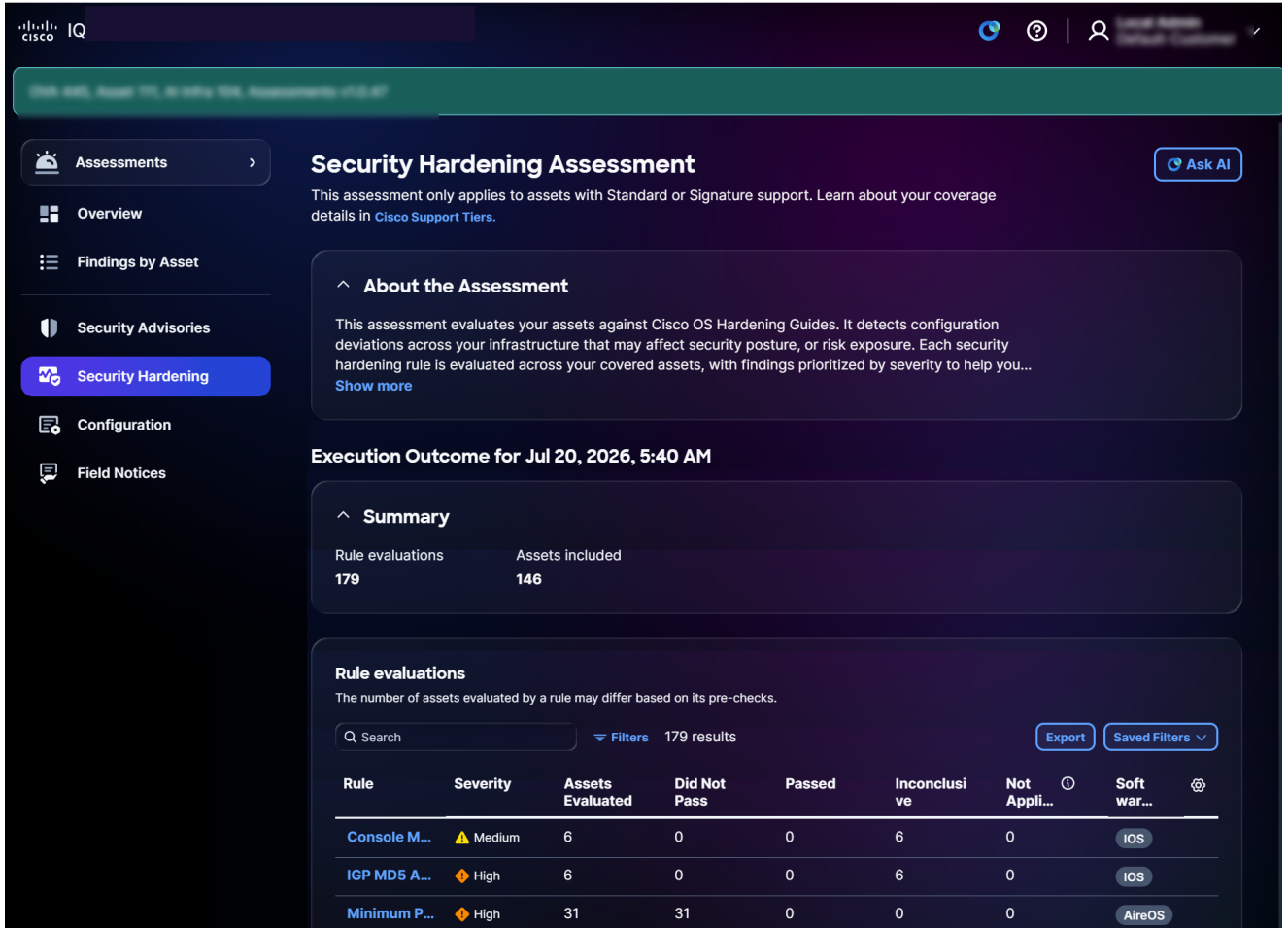
보안 강화

보안 강화(Security Hardening)는 업계 표준 벤치마크와 비교하여 라우터, 스위치 및 방화벽을 지속적으로 평가하여 네트워크 인프라의 보안 상태에 대한 거의 실시간으로 자동화된 가시성을 제공합니다. 구성 차이를 식별하고 실행 가능한 교정 지침을 제공하여 어카운트 관리자가 효과적으로 공격 표면을 줄이고 Cisco의 엄격한 보안 모범 사례에 일관된 조정을 유지할 수 있도록 합니다. 규정 준수 모니터링을 중앙 집중화하고 강화 프로세스를 간소화함으로써 보안 관리를 사후 대응적 작업에서 사전 대응적 데이터 중심 전략으로 전환하여 탄력적이고 안전한 엔터프라이즈 네트워크를 보장합니다.

 참고: 보안 강화 평가는 표준 지원 계층이 있는 자산에만 사용할 수 있습니다.

보안 강화 평가 보기

[보안 강화 평가] 페이지에는 다음 정보가 표시됩니다.



Security Hardening Assessment

This assessment only applies to assets with Standard or Signature support. Learn about your coverage details in [Cisco Support Tiers](#).

About the Assessment

This assessment evaluates your assets against Cisco OS Hardening Guides. It detects configuration deviations across your infrastructure that may affect security posture, or risk exposure. Each security hardening rule is evaluated across your covered assets, with findings prioritized by severity to help you... [Show more](#)

Execution Outcome for Jul 20, 2026, 5:40 AM

Summary

Rule evaluations	Assets included
179	146

Rule evaluations

The number of assets evaluated by a rule may differ based on its pre-checks.

Q Search Filters 179 results Export Saved Filters

Rule	Severity	Assets Evaluated	Did Not Pass	Passed	Inconclusive	Not Appli...	Soft war...
Console M...	Medium	6	0	0	6	0	IOS
IGP MD5 A...	High	6	0	0	6	0	IOS
Minimum P...	High	31	31	0	0	0	AireOS

보안 강화

- 평가 정보: 평가의 목적을 요약하여 추가 세부 정보를 제공합니다.
- 실행 결과: 전체 규칙 평가 수 및 포함된 자산을 포함하여 자산 평가 결과의 요약을 제공합니다.
- 규칙 평가: 심각도, 평가된 자산, 통과하지 않음, 통과됨, 불확실, 해당 사항 없음, Software 유형 등 규칙에 대한 자세한 정보를 제공합니다.
- 심각도: 규칙 평가의 중요도 또는 영향 수준을 제공합니다.
- 평가된 자산: 규칙 기준에 따라 평가된 총 자산 수를 제공합니다.
- 통과 안 함: 평가 중에 규칙 기준을 충족하지 못한 자산을 제공합니다.
- 통과: 평가 중에 규칙 기준을 충족한 자산을 제공합니다.

- 불확실: 평가에서 오류를 확인할 수 없는 자산을 제공합니다.
- 해당 없음: 규칙이 적용되지 않거나 관련이 없는 자산 또는 시나리오를 나타냅니다.
- 소프트웨어 유형: 소프트웨어 유형의 자산 제공

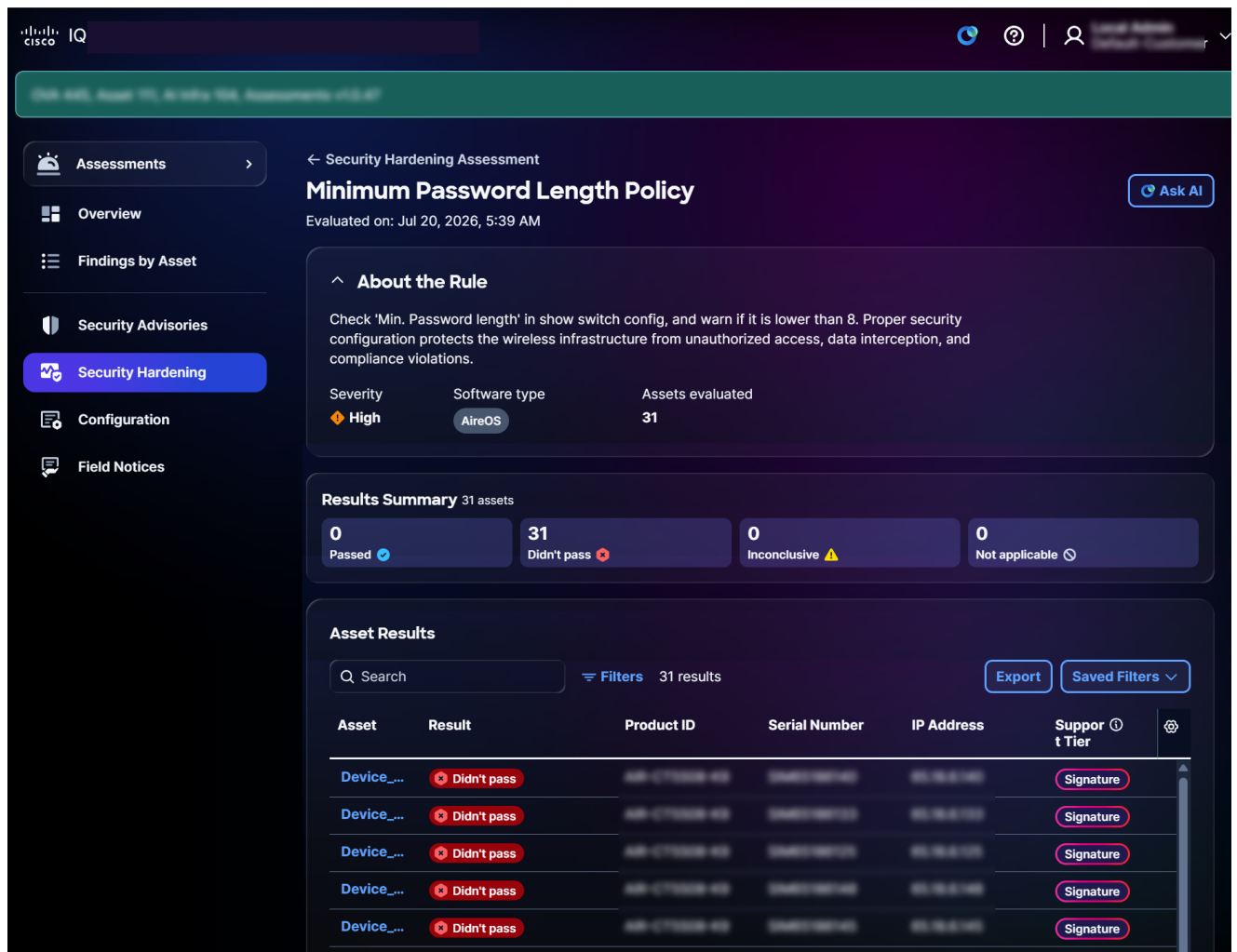
규칙 뷰 검색 및 필터링

드롭다운 목록에서 필터를 선택하거나 Filters(필터)를 클릭하고 사용 가능한 필터 목록에서 옵션을 선택하여 목록 뷰를 필터링할 수 있습니다. Search 필드에 규칙 이름을 입력하여 규칙을 검색할 수도 있습니다.

 참고: 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다. 역할과 권한에 따라 서로 다른 필터를 사용할 수 있습니다.

규칙 평가 세부 정보 보기

규칙 평가에 대한 추가 세부 정보를 보려면 규칙을 클릭합니다. 규칙의 평가 세부사항 페이지가 다음 정보와 함께 표시됩니다.



The screenshot shows the Cisco IQ interface for a Security Hardening Assessment. The main heading is "Minimum Password Length Policy", evaluated on Jul 20, 2026, at 5:39 AM. The assessment is categorized as "High" severity and applies to "AireOS" software type, with 31 assets evaluated.

Results Summary (31 assets):

- 0 Passed (blue checkmark)
- 31 Didn't pass (red X)
- 0 Inconclusive (yellow triangle)
- 0 Not applicable (grey circle)

Asset Results:

Search: [Q Search] Filters: 31 results [Export] [Saved Filters v]

Asset	Result	Product ID	Serial Number	IP Address	Support Tier
Device_...	Didn't pass	...	...	...	Signature
Device_...	Didn't pass	...	...	...	Signature
Device_...	Didn't pass	...	...	...	Signature
Device_...	Didn't pass	...	...	...	Signature
Device_...	Didn't pass	...	...	...	Signature

규칙 보기

- 규칙 정보: 심각도, 소프트웨어 유형, 버전, 평가된 자산 등 규칙에 대한 세부 정보를 제공하며 관련 소스 문서에 대한 설명적 레이블 링크를 포함합니다.
- 결과 요약: Passed(통과), Did not pass(통과하지 않음), Inconclusive(결정되지 않음), Not applicable(해당 사항 없음)과 같은 규칙과 관련된 자산 결과의 요약을 제공합니다.
- 자산 결과: 자산 목록 제공 - 자산, 결과, 제품 ID, 일련 번호, IP 주소, 지원 계층과 같은 세부 정보

 참고: Cisco IQ는 평가 결과가 "불확실"할 때 명확한 지침을 제공하여 원인(예: 텔레메트리 누락, 지원되지 않는 OS)을 설명하고 데이터 수집 확인, 자격 증명 업데이트, 데이터 새로 고침 등의 단계를 권장합니다. 문제 해결에 도움이 되도록 관련 문서에 대한 레이블이 지정된 링크도 제공됩니다.

자산 규칙에 대한 뷰 검색 및 필터링

드롭다운 목록에서 필터를 선택하거나 Filters(필터)를 클릭하고 사용 가능한 필터 목록에서 옵션을 선택하여 목록 뷰를 필터링할 수 있습니다. 또한 검색 필드에 자산 이름을 입력하여 자산 평가 결과를 검색할 수 있습니다.

 참고: 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다. 역할과 권한에 따라 서로 다른 필터를 사용할 수 있습니다.

자산 결과 내보내기

규칙에 대한 평가 결과를 내보내려면 Export를 클릭합니다. 자세한 [내용은 정보](#) 내보내기를 참조하십시오.

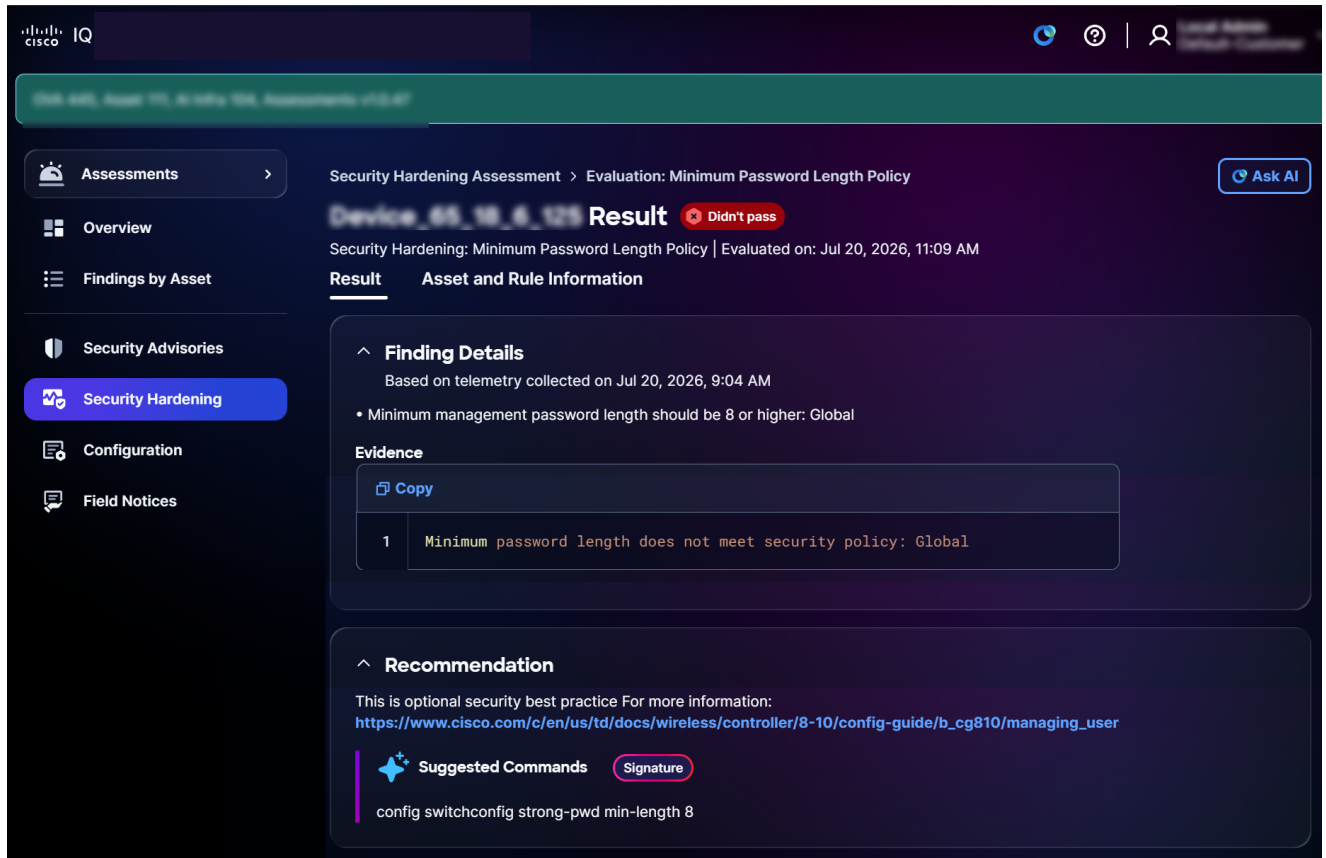
자산 결과에 대한 뷰 검색 및 필터링

드롭다운 목록에서 필터를 선택하거나 Filters(필터)를 클릭하고 사용 가능한 필터 목록에서 옵션을 선택하여 목록 뷰를 필터링할 수 있습니다. 검색 필드에 자산 이름을 입력하여 자산 결과를 검색할 수도 있습니다.

 참고: 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다. 역할과 권한에 따라 서로 다른 필터를 사용할 수 있습니다.

보안 강화를 위한 자산 결과 보기

자산 결과에서 자산을 눌러 해당 상세내역을 조회합니다. 에셋의 결과 세부사항 페이지에는 자격 레벨 또는 계층에 따른 정보가 표시됩니다.



보안 강화 표준 계층

- 표준 계층
- 찾기 세부 정보: 증거 로그와 함께 평가 중에 확인된 구성 편차에 대한 정보를 제공합니다.
- 권장 사항: 조사 결과를 해결하고 컨피그레이션 일관성을 보장하는 지침 제공

보안 강화를 위한 자산 및 규칙 정보 보기

에셋 및 해당 규칙의 세부사항을 보려면 에셋 및 규칙 정보 탭을 클릭합니다. Asset and Rule Info 페이지가 표시됩니다.

자산 정보: 제품 ID, 제품 유형, IP 주소, 일련 번호, 소프트웨어 버전, 위치, 지원 계층과 같은 자산의 세부 정보를 제공합니다.

- 규칙 정보: 규칙 세부사항(심각도 및 소프트웨어 유형 포함) 및 특정 강화 검사의 중요성 제공

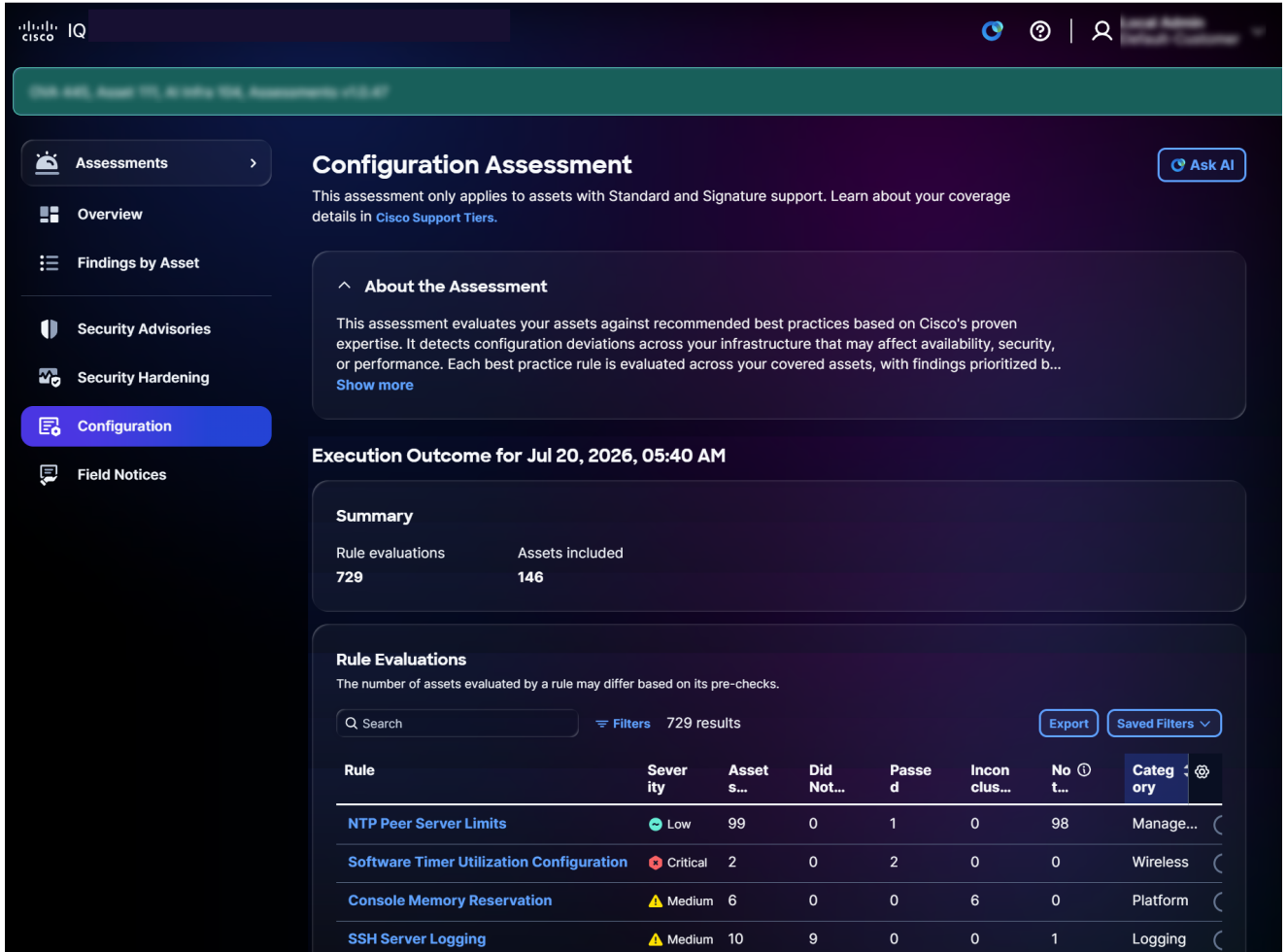
설정

구성 평가는 인프라 전반의 가용성, 보안 또는 성능에 영향을 미칠 수 있는 구성 편차를 탐지하기 위해 Cisco의 검증된 전문성을 기반으로 권장 모범 사례와 비교하여 자산을 평가합니다. 각 모범 사례 규칙은 지원되는 자산 전반에 걸쳐 평가되며, 구성 일관성, 향상된 탄력성 및 운영 위험 감소를 보장하기 위해 심각도별로 검색 결과의 우선 순위를 지정합니다.

 참고: 구성 평가는 표준 지원 계층이 있는 자산에만 사용할 수 있습니다.

구성 평가 보기

Configuration Assessment(컨피그레이션 평가) 페이지에는 다음 정보가 표시됩니다.



Configuration Assessment

This assessment only applies to assets with Standard and Signature support. Learn about your coverage details in [Cisco Support Tiers](#).

About the Assessment

This assessment evaluates your assets against recommended best practices based on Cisco's proven expertise. It detects configuration deviations across your infrastructure that may affect availability, security, or performance. Each best practice rule is evaluated across your covered assets, with findings prioritized b...

Execution Outcome for Jul 20, 2026, 05:40 AM

Summary

Rule evaluations	Assets included
729	146

Rule Evaluations

The number of assets evaluated by a rule may differ based on its pre-checks.

Search Filters 729 results Export Saved Filters

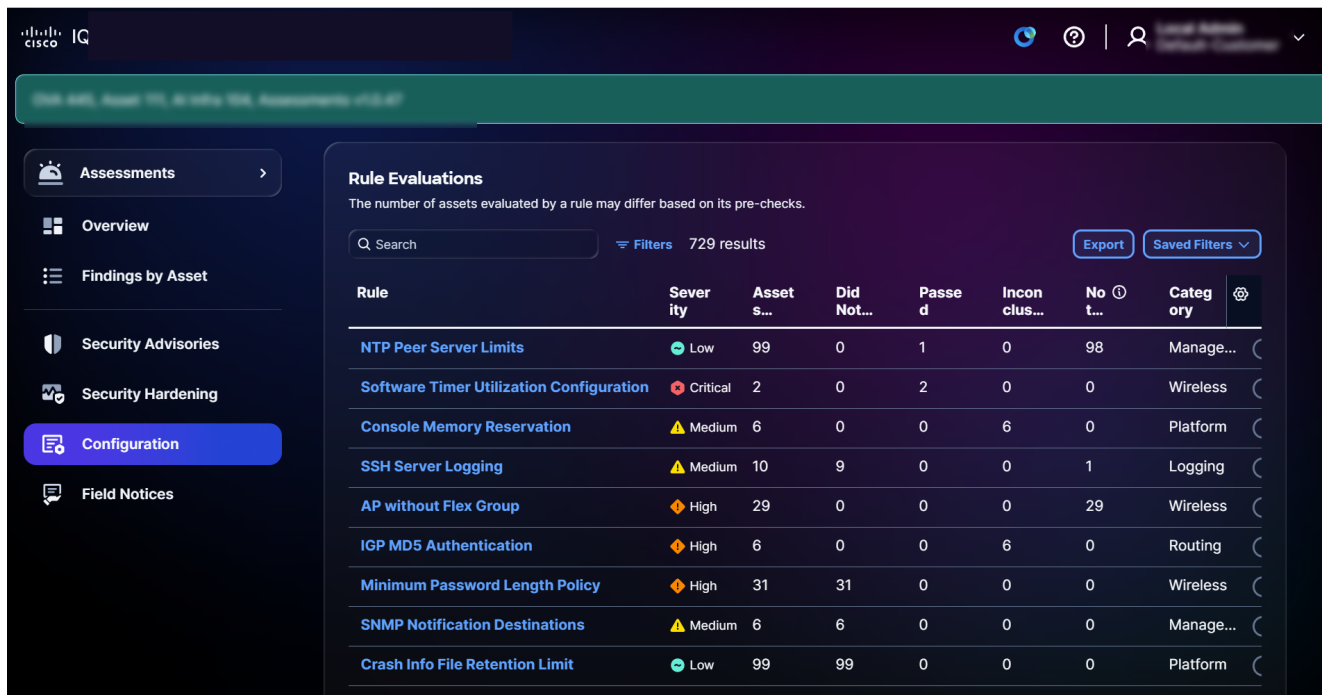
Rule	Severity	Asset s...	Did Not...	Passed	Inconclus...	No t...	Category
NTP Peer Server Limits	Low	99	0	1	0	98	Manage...
Software Timer Utilization Configuration	Critical	2	0	2	0	0	Wireless
Console Memory Reservation	Medium	6	0	0	6	0	Platform
SSH Server Logging	Medium	10	9	0	0	1	Logging

구성 평가

- 평가 정보: 평가의 목적을 요약하여 추가 세부 정보를 제공합니다.
- 요약: 평가된 규칙 및 평가된 자산과 같은 구성 실행의 요약 제공
- 인사이트: 패턴 분석을 통해 파악된 구성 허점에 대한 통찰력 및 조사 결과의 상관관계를 제공합니다. 지능적으로 그룹화된 키 카드로 표시되어 주의가 필요한 가장 중요한 영역을 강조 표시합니다
- 규칙 평가: 심각도, 평가된 자산, 통과하지 않음, 통과됨, 불확정, 해당 사항 없음, 범주, Software 유형 등 규칙에 대한 자세한 정보를 제공합니다.
- 심각도: 규칙 평가의 중요도 또는 영향 수준을 제공합니다.
- 평가된 자산: 규칙 기준에 따라 평가된 총 자산 수를 제공합니다.

- 통과 안 함: 평가 중에 규칙 기준을 충족하지 못한 총 자산 수를 제공합니다.
- 불확실: 평가를 실행할 수 없는 총 자산 수를 제공합니다.
- 통과: 평가 중에 규칙 기준을 충족한 자산을 제공합니다.
- 해당 없음: 규칙이 적용되지 않거나 관련이 없는 자산 또는 시나리오를 나타냅니다.
- 범주: 규칙이 속한 도메인 영역을 제공합니다.
- 소프트웨어 유형: 규칙이 적용되는 소프트웨어 자산의 유형을 나타냅니다.

규칙 뷰 검색 및 필터링



Rule	Severity	Asset s...	Did Not...	Passe d	Incon clus...	No t...	Categ ory	
NTP Peer Server Limits	Low	99	0	1	0	98	Manage...	
Software Timer Utilization Configuration	Critical	2	0	2	0	0	Wireless	
Console Memory Reservation	Medium	6	0	0	6	0	Platform	
SSH Server Logging	Medium	10	9	0	0	1	Logging	
AP without Flex Group	High	29	0	0	0	29	Wireless	
IGP MD5 Authentication	High	6	0	0	6	0	Routing	
Minimum Password Length Policy	High	31	31	0	0	0	Wireless	
SNMP Notification Destinations	Medium	6	6	0	0	0	Manage...	
Crash Info File Retention Limit	Low	99	99	0	0	0	Platform	

규칙 평가

드롭다운 목록에서 필터를 선택하거나 Filters(필터)를 클릭하고 사용 가능한 필터 목록에서 옵션을 선택하여 목록 뷰를 필터링할 수 있습니다. Search 필드에 규칙 이름을 입력하여 규칙을 검색할 수도 있습니다.

 참고: 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다. 역할과 권한에 따라 서로 다른 필터를 사용할 수 있습니다.

규칙 평가 세부 정보 보기

규칙 평가에 대한 추가 세부 정보를 보려면 규칙을 클릭합니다. 규칙의 평가 세부사항 페이지가 다음 정보와 함께 표시됩니다.

평가

- 규칙 정보: 심각도, 카테고리, 소프트웨어 유형, 평가된 자산과 같은 규칙에 대한 세부 정보를 제공하며 관련 소스 문서에 대한 설명적 링크를 포함합니다.
- 결과 요약: Passed(통과됨), Did not pass(통과하지 않음), Inconclusive(결정되지 않음) 및 Not applicable(해당 없음) 상태의 자산 수를 표시하여 전반적인 자산 결과를 제공합니다.
- 자산 결과: 선택한 규칙의 영향을 받는 에셋 목록을 결과 상태와 함께 제공합니다.

 참고: Cisco IQ는 평가 결과가 "불확실" 상태일 때 명확한 지침을 제공하여 원인(예: 텔레메트리 누락, 지원되지 않는 OS)을 설명하고 데이터 수집 확인, 자격 증명 업데이트, 데이터 새로 고침 등의 단계를 권장합니다. 문제 해결에 도움이 되도록 관련 문서에 대한 레이블이 지정된 링크도 제공됩니다. Assessment 모듈은 규칙에 대한 다중 카테고리 선택을 지원하므로, 여러 규칙 카테고리에 걸쳐 동시에 처리 및 평가가 가능합니다.

자산 결과 내보내기

규칙에 대한 자산 결과를 내보내려면 내보내기를 누릅니다. 자세한 [내용은 정보](#) 내보내기를 참조하십시오.

자산 결과에 대한 뷰 검색 및 필터링

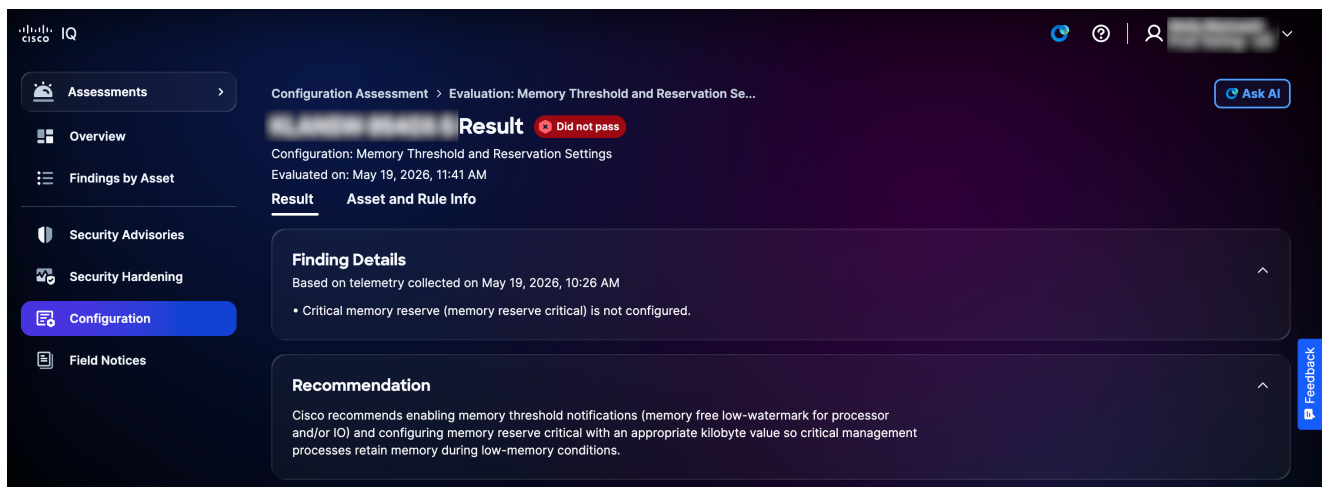
드롭다운 목록에서 필터를 선택하거나 Filters(필터)를 클릭하고 사용 가능한 필터 목록에서 옵션을 선택하여 목록 뷰를 필터링할 수 있습니다. 검색 필드에 자산 이름을 입력하여 자산 결과를 검색할 수도 있습니다.

 참고: 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다. 역할과 권한에 따라 서로 다른 필터를 사용할 수 있습니다.

구성 평가에 대한 자산 결과 보기

자산 결과의 상세내역을 조회하려면 자산 결과에서 자산을 누릅니다.

에셋의 결과 세부사항 페이지에는 자격 레벨 또는 계층에 따른 정보가 표시됩니다.

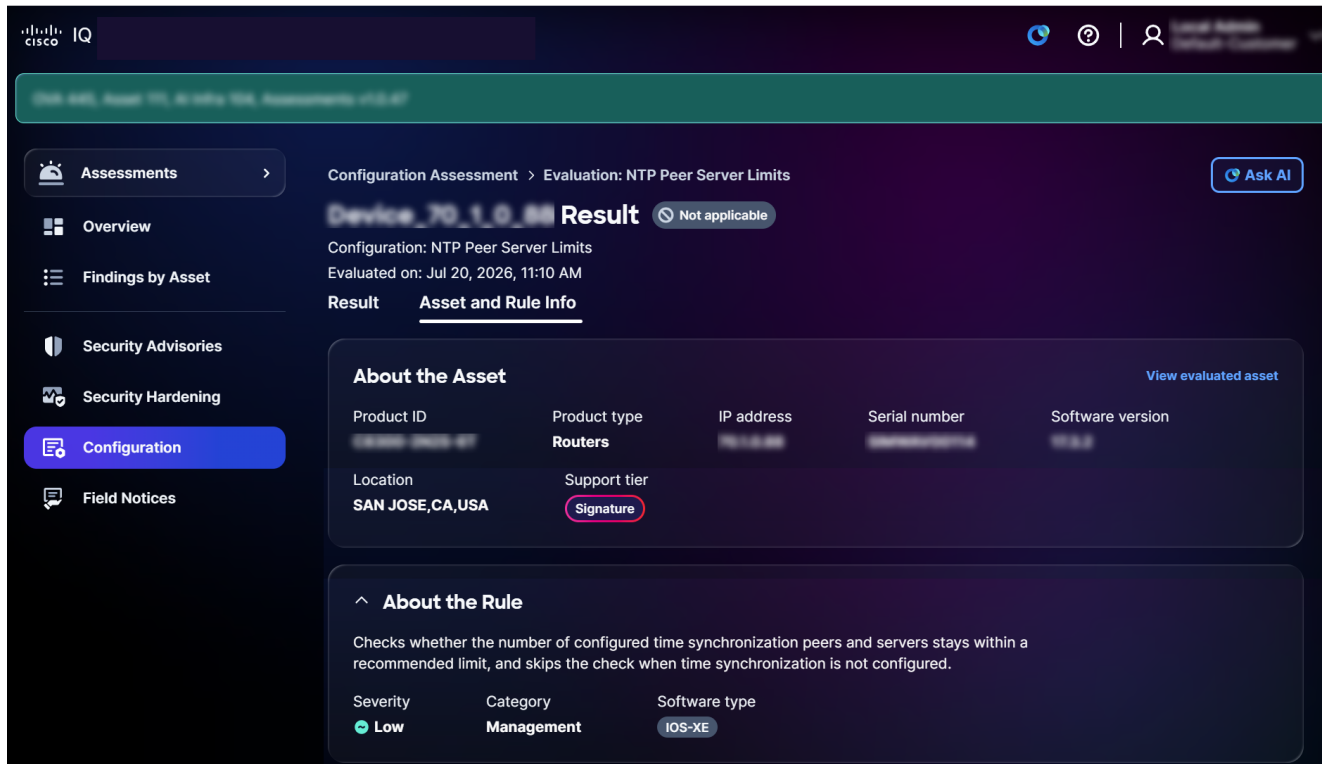


구성 표준 계층

- 표준 계층
- 찾기 세부 정보: 증거 로그와 함께 평가 중에 확인된 구성 편차에 대한 정보를 제공합니다.
- 권장 사항: 조사 결과를 해결하고 컨피그레이션 일관성을 보장하는 지침 제공

구성 평가를 위한 자산 및 규칙 정보 보기

자산 및 규칙 정보 세부사항을 보려면 Asset and Rule Info 탭을 클릭합니다.



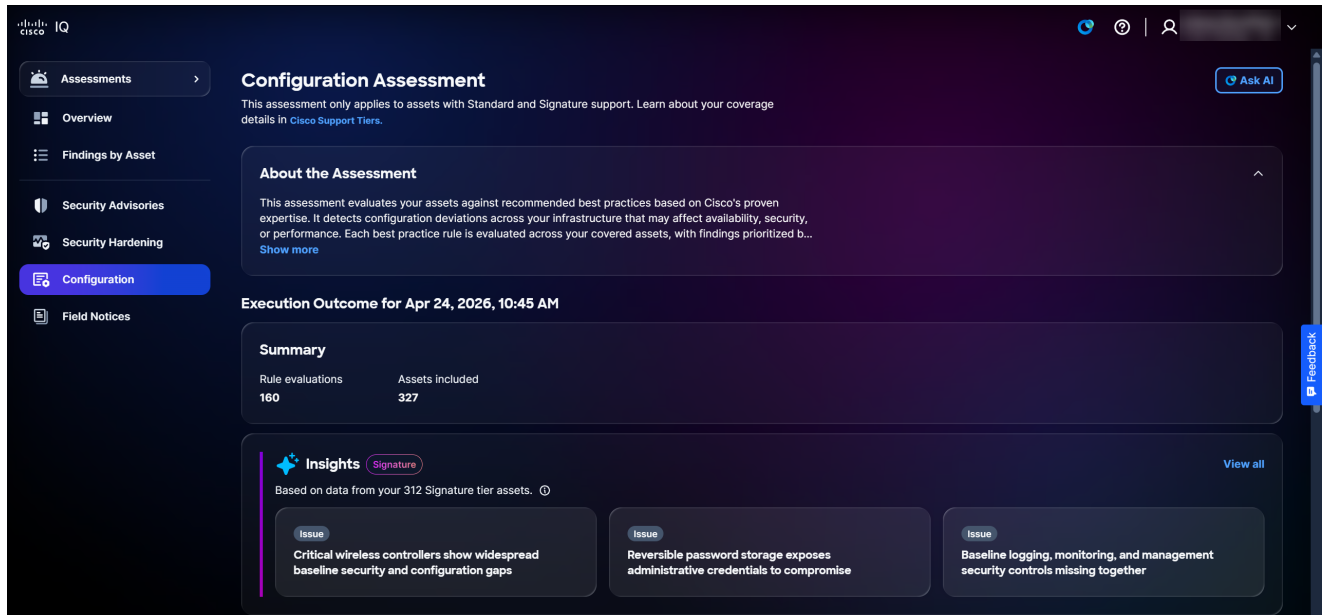
자산 및 규칙 정보

자산 및 규칙 정보 페이지는 다음 정보와 함께 표시됩니다.

- 자산 정보: 제품 ID, 제품 유형, IP 주소, 일련 번호, 소프트웨어 버전, 위치 및 지원 계층과 같은 자산의 세부 정보를 제공합니다.
- 규칙 정보: 심각도, 카테고리, 소프트웨어 유형 등 규칙의 세부 정보를 제공합니다

인사이트 보기

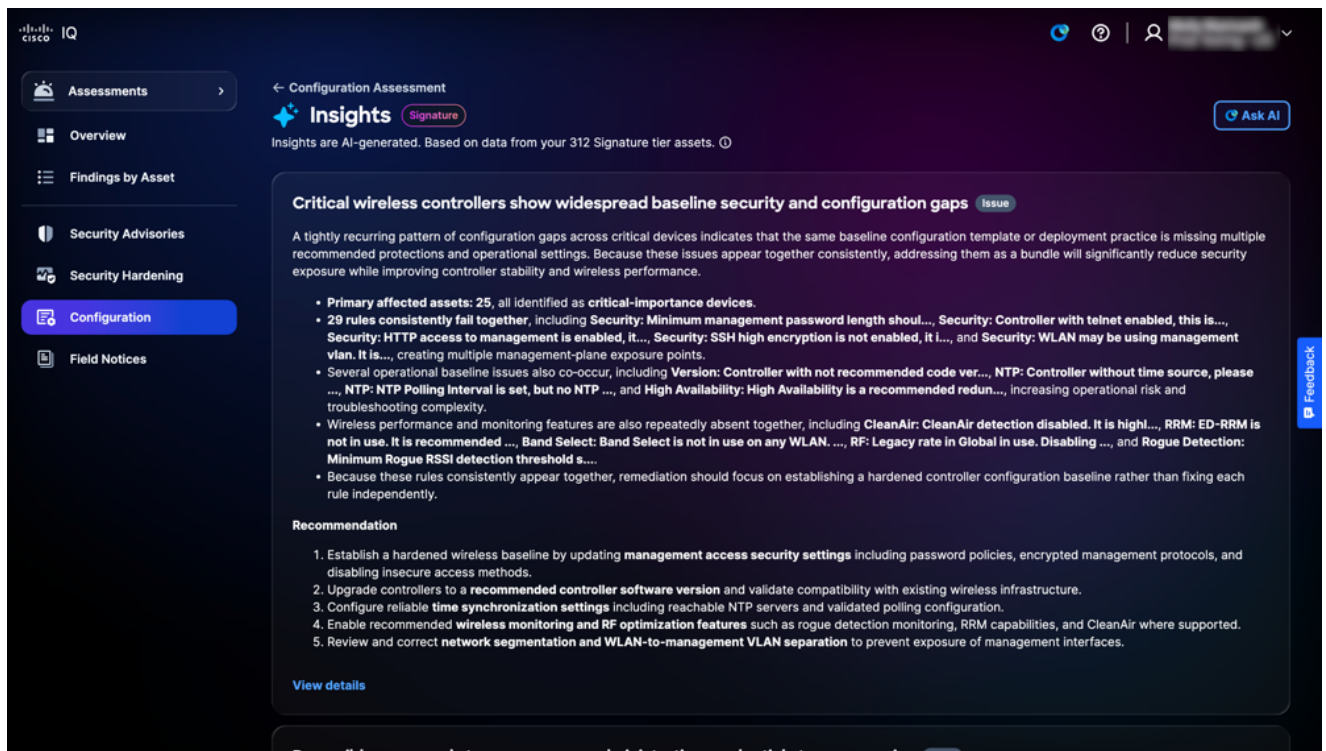
통찰력은 AI에서 생성되며, 우선 순위가 지정된 주요 카드에 평가 데이터를 종합하여 여러 조사 결과에 걸쳐 중요한 구성 차이를 강조하는 지능형 대시보드의 역할을 합니다. 이러한 시급한 영역에 집중함으로써 가장 큰 영향을 미치는 인프라 위험을 효율적으로 해결할 수 있습니다. 또한 Best Practice에 따라 인프라가 잘 작동하는 영역을 파악하여 장점을 강조합니다.



통찰력

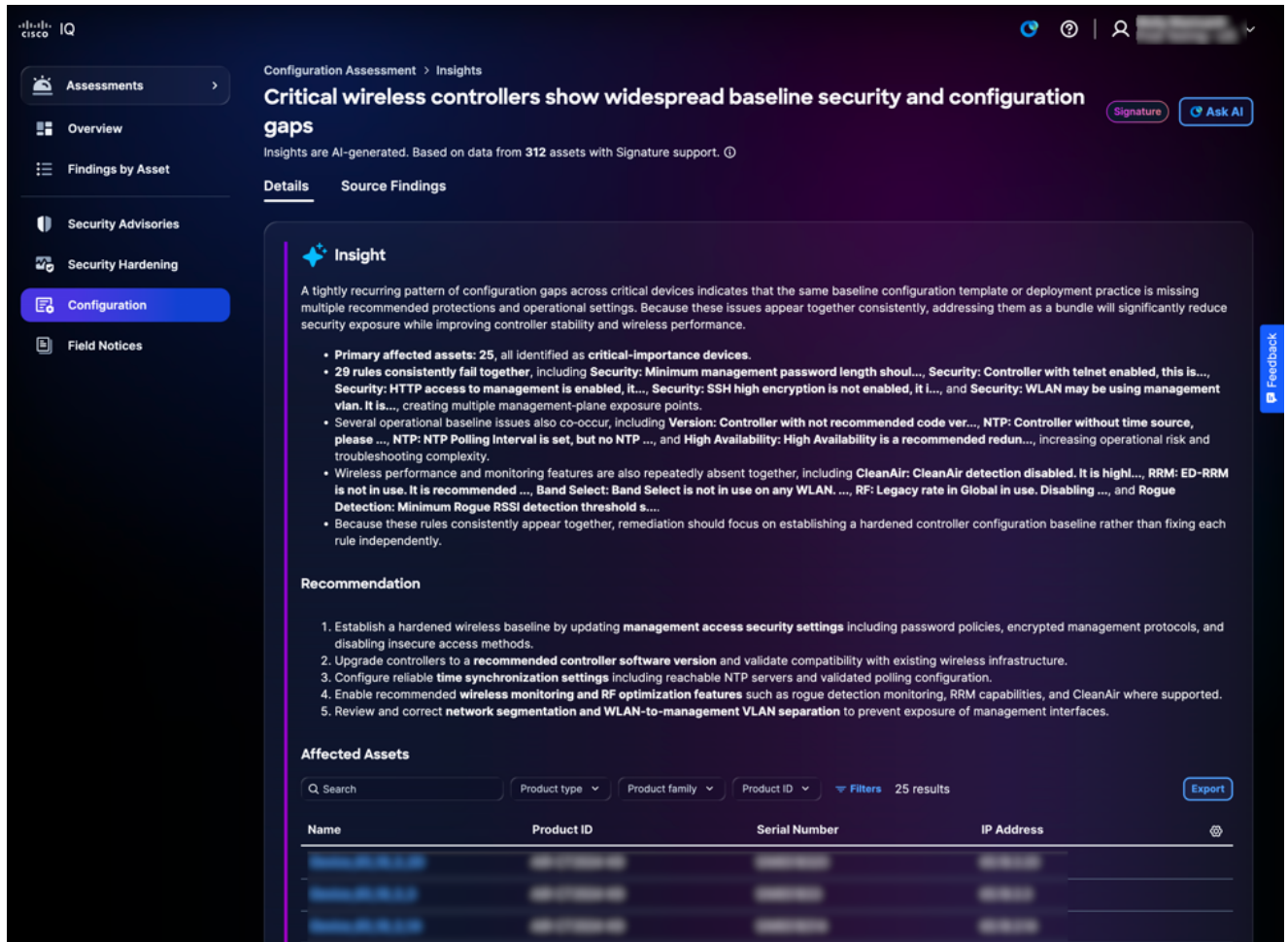
Insights 세부 정보를 보려면

1. Insights 패널에서 View all(모두 보기)을 클릭합니다. Insights 페이지에는 모든 인사이트가 표시됩니다.



인사이트 페이지

2. View details(세부사항 보기)를 클릭하거나 임의의 카드를 클릭합니다. 다음 정보와 함께 Insights 세부 정보 페이지가 표시됩니다.



인사이트 세부 정보

- 인사이트: 여러 조사 결과에 대한 종합적인 분석을 통해 파악된 구성 편차의 반복적인 패턴 및 구성이 모범 사례와 일치하는 인프라의 탁월성 영역을 조명하는 요약を提供합니다.
 - 권장 사항: 식별된 구성 차이를 해결하기 위한 실행 가능한 단계 제공
 - 영향을 받는 자산: 컨피그레이션 편차가 Insight 섹션에 정의된 대로 식별된 특정 디바이스의 목록을 제공합니다.
3. Source Findings(소스 검색 결과)를 클릭합니다. Source Findings(소스 결과) 페이지에는 통찰력을 지원하는 세부적인 개별 결과가 표시됩니다.

The screenshot shows the Cisco IQ Configuration Assessment Insights page. The main heading is "Critical wireless controllers show widespread baseline security and configuration gaps". Below this, it states "Insights are AI-generated. Based on data from 312 assets with Signature support." The page has a sidebar with navigation options: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration (selected), and Field Notices. The main content area shows a table of findings with columns: Asset, Rule, Severity, Serial Number, and Result. The table is filtered to show 725 results. The first few rows show findings related to "High Availability: High Availa..." with a severity of "Low" and a result of "Did not pass".

Asset	Rule	Severity	Serial Number	Result
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass

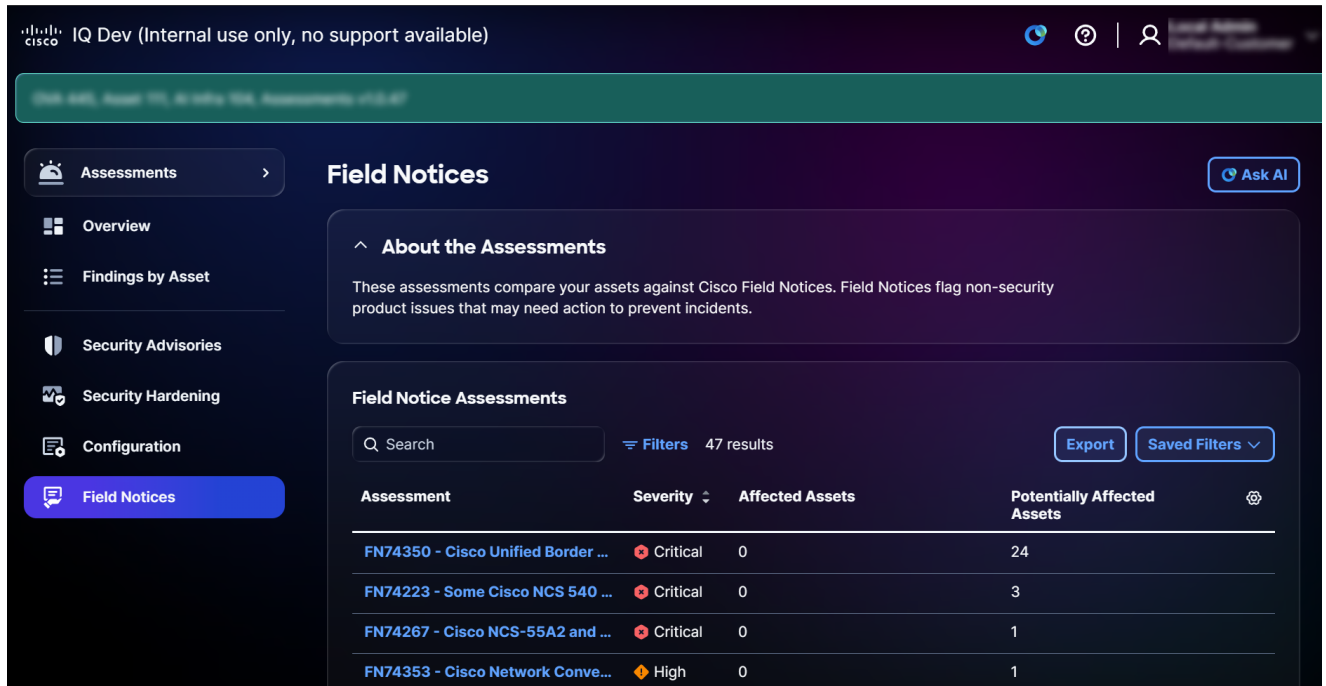
출처 조사 결과

Severity and Result 드롭다운 목록에서 필터를 선택하여 테이블 보기를 필터링할 수 있습니다.

참고: 권장 사항 및 영향을 받는 자산은 각 통찰력의 결과에 따라 선택 사항입니다.

필드 알림

Field Notice는 보안 관련 제품이 아닌 주요 문제를 식별하여 그 영향의 심각도와 중요도를 기준으로 구성함으로써 조직의 제품 위험 관리 능력을 향상시킵니다. Field Notice는 제품 결함에 대한 실행 가능한 통찰력을 제공하고, 권장 업그레이드 또는 해결 방법을 통해 완화를 가속화하며, 운영 및 비즈니스 목표와의 조율을 보장합니다. 이를 통해 제품 안정성을 강화하고, 리소스 할당을 최적화하며, 기업 전반에서 진화하는 제품 과제에 대한 탄력성을 강화할 수 있습니다.



필드 노트

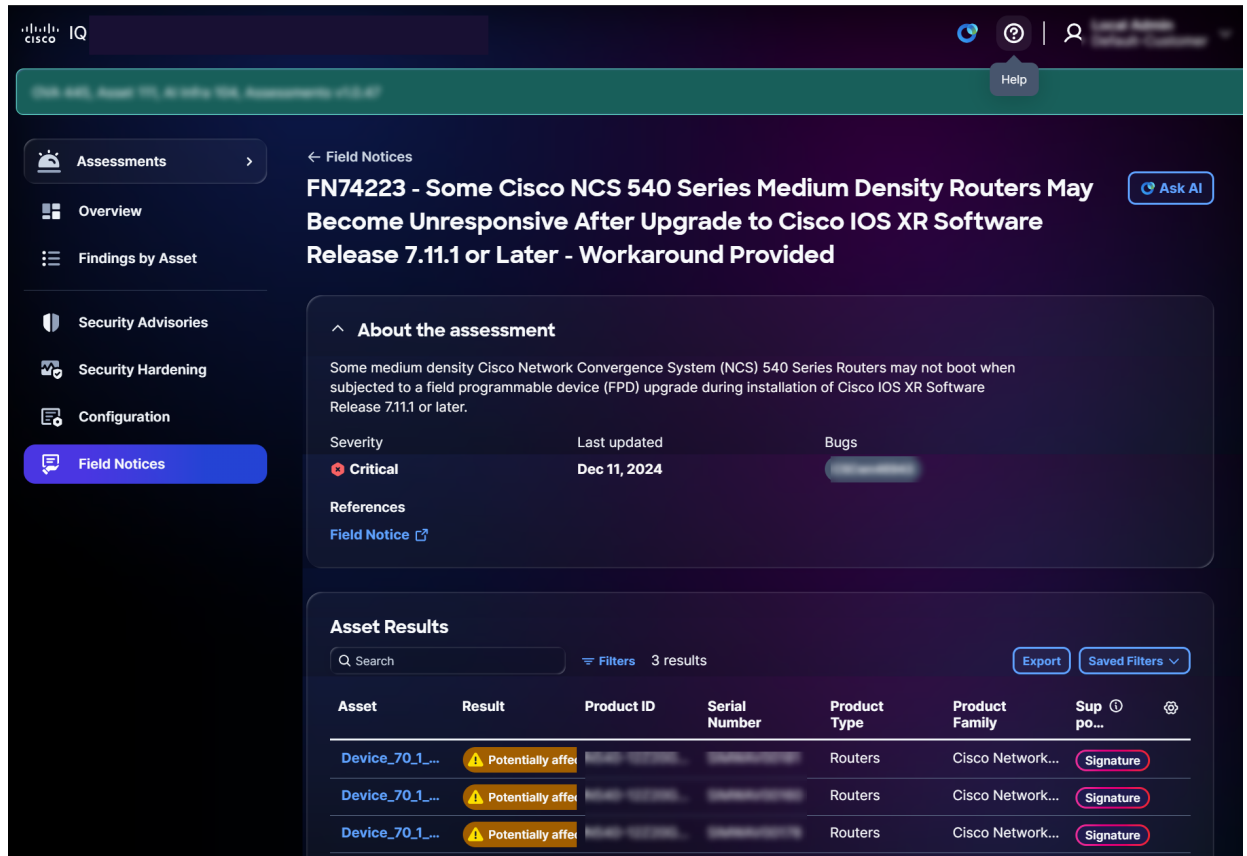
필드 알림에 대한 뷰 검색 및 필터링

드롭다운 목록에서 필터를 선택하여 목록 보기를 필터링할 수 있습니다. 검색 필드에 평가 이름을 입력하여 필드 알림 평가를 검색할 수도 있습니다.

Field Notice에 대한 평가 보기

필드 알림에 대한 추가 세부 정보를 보려면 평가를 클릭합니다. 다음 평가 세부사항이 표시됩니다.

- 평가 정보: 평가의 목적을 요약하여 추가 세부 정보를 제공합니다.
- Field Notice 평가: 취약성이 탐지된 자산을 포함하여 선택한 필드 알림의 영향을 받는 자산 목록을 표시합니다



Field Notice에 대한 평가 보기

필드 알림에 대한 자산 결과 검색 및 필터링 보기

드롭다운 목록에서 필터를 선택하거나 Filters(필터)를 클릭하고 사용 가능한 필터 목록에서 옵션을 선택하여 목록 뷰를 필터링할 수 있습니다. 검색 필드에 자산 이름을 입력하여 자산 결과를 검색할 수도 있습니다.

 참고: 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다. 역할과 권한에 따라 서로 다른 필터를 사용할 수 있습니다.

Field Notice에 대한 자산 결과 내보내기

필드 알림에 대한 평가 자산 결과를 내보내려면 내보내기를 클릭합니다. 자세한 [내용은 정보](#) 내보내기를 참조하십시오.

Field Notice에 대한 자산 평가 결과 보기

자산의 평가 결과 세부사항을 보려면 Asset Assessment Results(자산 평가 결과)에서 자산을 클릭합니다. 자산의 평가 결과 세부사항 페이지가 표시됩니다.

다음 유형의 결과를 볼 수 있습니다.

- 영향: Field Notice에 대해 자동으로 확인된 모든 기준을 충족하며 영향을 받았는지 확인하기 위해 추가 수동 확인이 필요하지 않은 자산을 나타냅니다.

- 영향을 받을 수 있음: Field Notice에 대해 자동으로 확인된 모든 기준을 충족하지만 실제 영향을 받았는지 확인하기 위해 추가 수동 확인이 필요한 자산을 나타냅니다.

Assessments - Security Hardening(평가 - 보안 강화) 탭에서 다음 프롬프트를 사용할 수 있습니다.

- 네트워크 장치에 대한 Cisco 보안 강화 모범 사례는 무엇입니까?
- Cisco IOS XE 디바이스를 어떻게 강화합니까?
- 라우터 및 스위치의 주요 보안 강화 단계를 나열합니다.
- Cisco 디바이스에 권장되는 기본 강화 설정은 무엇입니까?
- 보안 강화 모범 사례를 위반하는 자산은 몇 개입니까?

로컬 인증

계정 관리자는 다음 자격 증명을 사용하여 VA에 로그인해야 합니다.

- 기본 사용자 이름: admin
- 기본 비밀번호: VA 설치 프로세스 중에 설정되는 비밀번호. 자세한 내용은 시작 가이드를 참조하십시오
- 기본 계정 컨텍스트: 기본 고객

로그인 시 홈 페이지에 기본 사용자 "admin" 및 계정 이름 "Default-Customer"가 표시됩니다.

로컬 관리자 보안 설정

홈 페이지의 User Profile 메뉴를 통해 비밀번호를 변경하고 보안 질문을 설정할 수 있습니다.

잠금 설정

다음 계정 잠금 설정은 배포 중에 구성할 수 있습니다.

- 잠금 상태: 계정 잠금 기능을 활성화하거나 비활성화합니다.
- Maximum Login Attempts(최대 로그인 시도 횟수): 계정이 잠기기 전에 허용되는 연속 실패 횟수의 최대값을 설정합니다(기본값: 3; 범위: 0~10).
- 롤링 시간 창: 실패한 시도를 추적할 기간을 정의합니다(기본값: 15분; 범위: 0~60분).
- 기간: 최대 시도 횟수에 도달한 후 계정이 잠긴 상태를 유지하는 기간을 설정합니다(기본값: 30분; 범위: 0~60분).

 참고: 15분 내에 3회 시도하여 올바른 비밀번호를 입력하려고 합니다. 세 번의 시

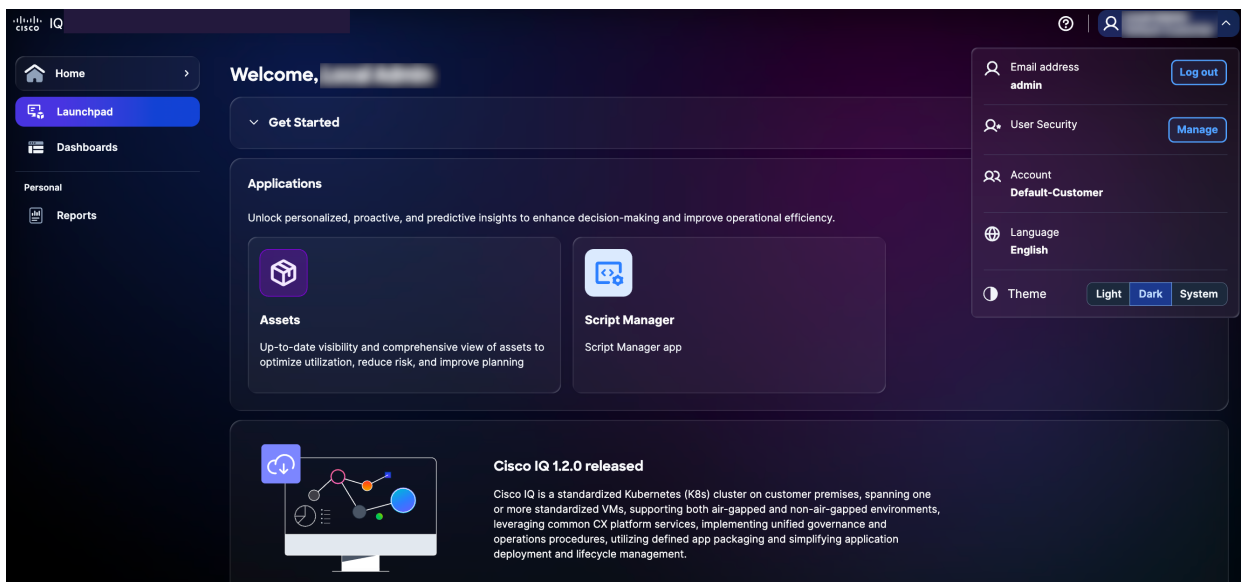
 도가 모두 실패하면 보안을 위해 계정이 30분 동안 일시적으로 잠깁니다. 잠금 기간 중에는 로그인을 시도할 수 없습니다. 다음과 같은 메시지가 표시됩니다. "실패한 시도가 너무 많아 계정이 잠겼습니다. 잠금이 만료되는 시간을 포함하여 "나중에 다시 시도하십시오." 30분 후에 계정이 자동으로 잠금 해제되며, 이 때 로그인 또는 비밀번호 재설정을 시도할 수 있습니다."

보안 Q&A 설정

비밀번호를 잊어버린 경우 보안 질문을 통해 ID를 확인할 수 있습니다. 계정 관리자는 비밀번호 재설정 기능을 활성화하기 위해 5개의 보안 질문에 대한 답변을 설정해야 합니다. 이것은 1회 설정입니다.

보안 질문을 설정하려면

1. 홈 페이지에서 사용자 프로필 아이콘을 클릭합니다. 드롭다운 메뉴가 열립니다.



보안 사용

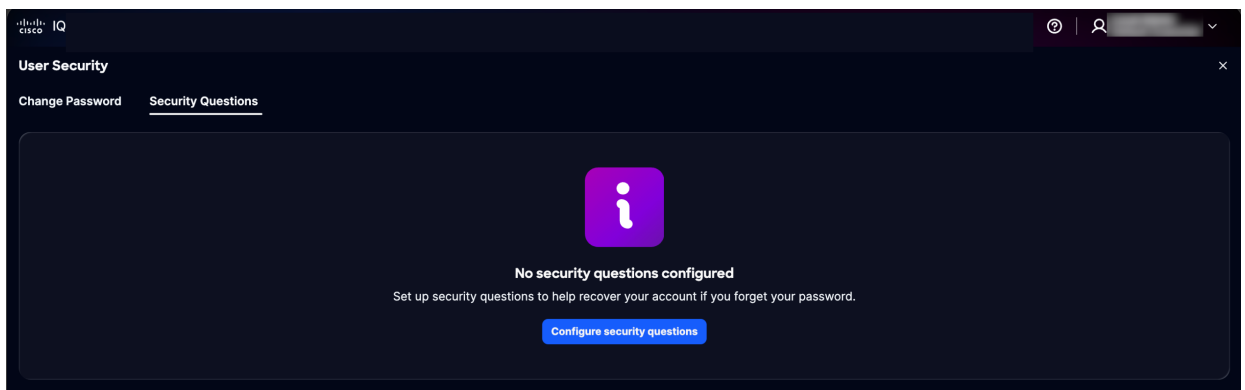
2. 사용자 보안에서 관리를 클릭합니다. User Security 페이지가 표시됩니다.



The screenshot shows the 'User Security' interface in Cisco IQ. The 'Change Password' tab is selected. It lists password requirements: at least 15 characters, at least 2 uppercase characters, at least 2 lowercase characters, at least 2 numeric characters, at least 2 special characters, and no repeating characters. There are input fields for 'Password', 'New password', and 'Confirm password', each with a 'Show' button. A 'Save' button is at the bottom.

보안 질문

3. Security Questions(보안 질문)를 클릭하여 탭을 엽니다.



The screenshot shows the 'User Security' interface in Cisco IQ. The 'Security Questions' tab is selected. It displays a message: 'No security questions configured. Set up security questions to help recover your account if you forget your password.' Below the message is a blue button labeled 'Configure security questions'.

보안 질문 탭

4. Configure security questions(보안 질문 구성)를 클릭합니다.

User Security

Change Password

Security Questions

Security Questions

Set up security questions to help recover your account if you forget your password. You must answer all questions.

Question 1 *

Select a security question



Answer *

Question 2 *

Select a security question



Answer *

Question 3 *

Select a security question



Answer *

Question 4 *

Select a security question



Answer *

Question 5 *

Select a security question



Answer *

보안 질문 구성

5. 드롭다운 목록에서 보안 질문 5개를 선택합니다.
6. 각 질문에 대한 응답을 입력합니다.
7. 저장을 클릭합니다.



참고: 대답은 대/소문자를 구분하지 않습니다. 예를 들어 "SMITH"와 "smith"는 동일한 것으로 간주됩니다. 추가 공백은 무시됩니다. 즉, "Smith"와 "Smith"는 동일하게 처리됩니다. 답을 입력한 방법(예: 전체 이름 대 별명)을 기억하십시오. 몇 년 후에 기억하게 될 솔직한 대답을 사용하세요. 시간이 지나도 변하지 않는 답변이 포함된 질문을 선택합니다.



참고: 필요한 경우 나중에 답변을 업데이트할 수 있습니다. 답변을 업데이트할 때 이전 답변이 모두 교체되므로 변경하려는 질문뿐 아니라 5개 질문 모두에 대한 답변을 다시 제공해야 합니다.

비밀번호 관리

계정 관리자 및 로컬 사용자는 Cisco IQ의 비밀번호를 관리할 수 있습니다.

계정의 보안을 위해 다음 비밀번호 정책이 적용됩니다.

- 재사용 제한: 새 비밀번호는 이전 5개 비밀번호와 일치하지 않습니다. 이 정책은 등록, 비밀번호 분실 및 비밀번호 변경 흐름에 적용됩니다.
- 문자 변형: 인증된 상태에서 비밀번호를 변경할 경우 현재 비밀번호에서 8자 이상 이 새 비밀번호와 달라야 합니다.
- 최소 변경 간격: 기본적으로 비밀번호를 다시 변경하기 전에 24시간을 기다려야 합니다. 다른 간격이 구성된 경우 해당 시간이 경과할 때까지 비밀번호를 업데이트할 수 없습니다.
- 암호 만료: 비밀번호는 60일마다 만료됩니다. 만료일 이후 처음 로그인하면 시스템에 액세스하기 전에 새 비밀번호를 설정해야 합니다(0으로 구성된 경우 비밀번호 만료는 비활성화됨).

사전 요구 사항

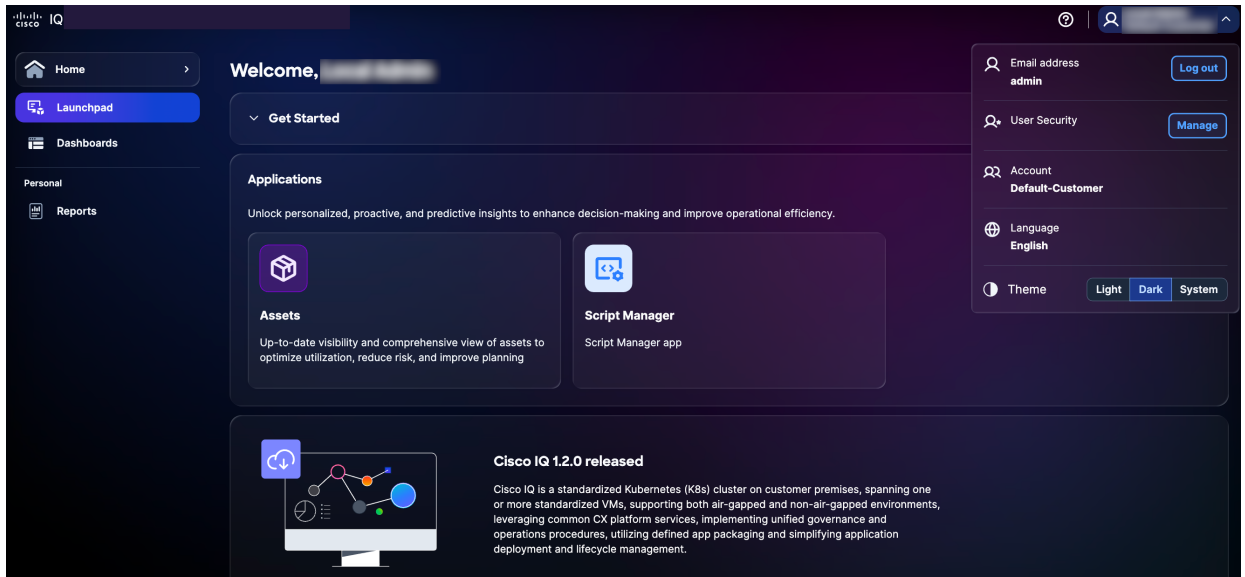
비밀번호를 관리하려면 다음 조건을 충족해야 합니다.

- 로컬 계정 관리자 또는 사용자입니다.
- 로컬 계정을 사용 중입니다(SSO(Single Sign-On) 또는 외부 인증이 아님).
- Cisco IQ에 로그인했습니다.
- 현재 비밀번호 확인

비밀번호 변경

비밀번호를 변경하려면

1. 홈 페이지에서 사용자 프로필 아이콘을 클릭합니다. 드롭다운 메뉴가 열립니다.



사용자 보안 관리

2. 사용자 보안에서 관리를 클릭합니다. User Security 페이지가 표시됩니다.



암호 변경

3. 현재 비밀번호를 입력합니다.
4. 새 비밀번호를 입력합니다.
5. 새 비밀번호를 다시 입력하여 확인합니다.
6. 저장을 클릭합니다.

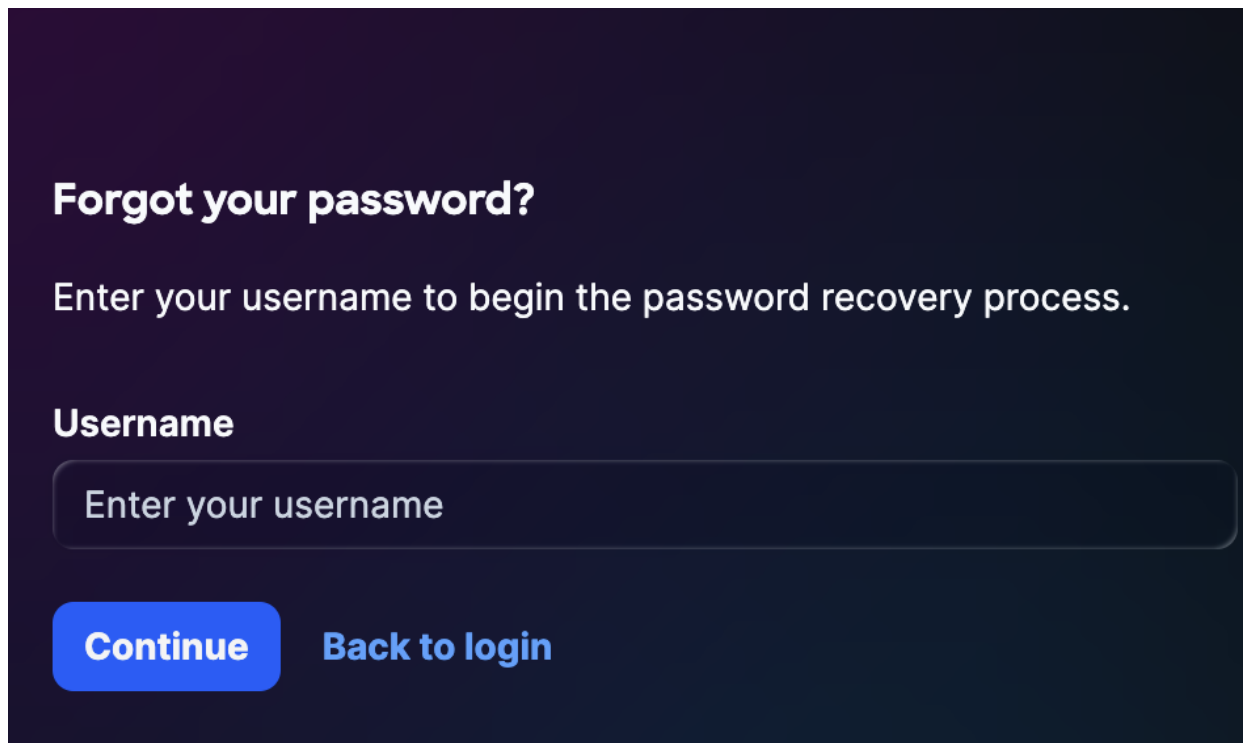
비밀번호는 Cisco IQ VM을 비롯한 Cisco IQ 시스템에서 업데이트됩니다.

잊어버린 비밀번호 재설정

보안 질문 확인 프로세스를 사용하여 비밀번호를 재설정할 수 있습니다.

잊어버린 비밀번호를 재설정하려면

1. Cisco IQ VA 로그인 페이지로 이동합니다.
2. Forgot Password(비밀번호 분실)를 클릭합니다.



Forgot your password?

Enter your username to begin the password recovery process.

Username

Enter your username

Continue [Back to login](#)

비밀번호 분실

3. 사용자 이름을 입력합니다.
4. Continue(계속)를 클릭합니다. Verify Identity(ID 확인) 페이지에는 이전에 구성된 5개 질문 중 3개의 임의 보안 질문이 표시됩니다.

Verify Identity

Answer the following security questions to verify your identity.

What city were you born in?

Enter your answer

Show

What is your mother's maiden name?

Enter your answer

Show

What was the name of your elementary school?

Enter your answer

Show

Verify and continue

Back to login

ID 확인

5. 표시된 세 가지 질문 모두에 대한 응답을 입력합니다.
6. Verify and continue(확인 및 계속)를 클릭합니다. 전송된 응답이 이전에 저장된 응답과 일치하면 새 비밀번호를 입력하라는 메시지가 표시됩니다.

Set New Password

Choose a strong password that contains the following:

- At least 15 characters
- At least 2 uppercase characters
- At least 2 lowercase characters
- At least 2 numeric characters
- At least 2 special characters
- No repeating characters

New password

Show

Confirm password

Show

Reset password

Back to login

비밀번호 재설정

 참고: 15분 내에 3회 시도하여 올바른 비밀번호를 입력하려고 합니다. 세 번의 시도가 모두 실패하면 보안을 위해 계정이 30분 동안 일시적으로 잠깁니다. 잠금 기간 중에는 로그인을 시도할 수 없습니다. 다음과 같은 메시지가 표시됩니다. "실패한 시도가 너무 많아 계정이 잠겼습니다. 잠금이 만료되는 시간을 포함하여 "나중에 다시 시도하십시오." 30분 후에 계정이 자동으로 잠금 해제되며, 이 때 로그인 또는 비밀번호 재설정을 시도할 수 있습니다.

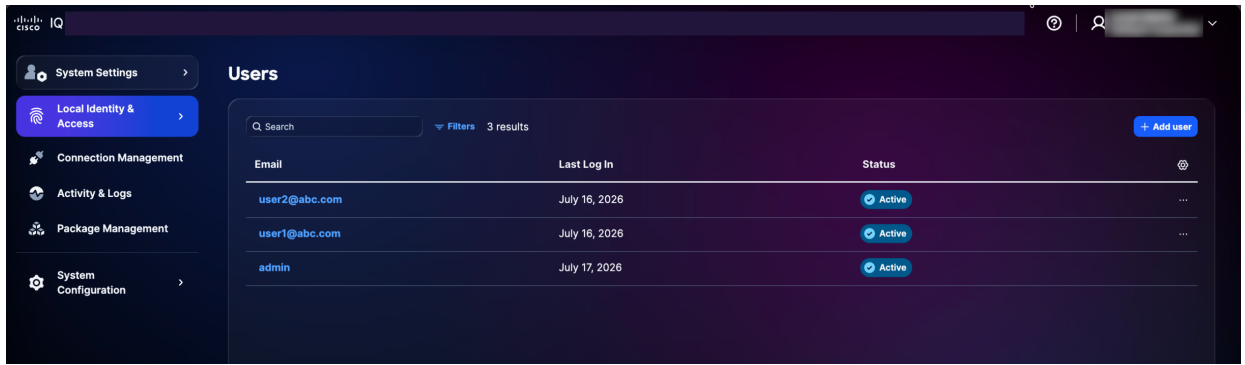
7. 새 비밀번호를 입력합니다.
8. 비밀번호를 다시 입력하여 확인합니다.
9. Submit(제출)을 클릭합니다.

로컬 사용자 추가

계정 관리자는 Cisco IQ 계정에 사용자를 추가할 수 있습니다. 새 사용자를 추가하려면

1. System Settings(시스템 설정) > Local Identity & Access(로컬 ID 및 액세스) > Users(사용자)로 이동합니다. Users(사용자) 페이지가 표시됩니다. 모든 기존 로컬

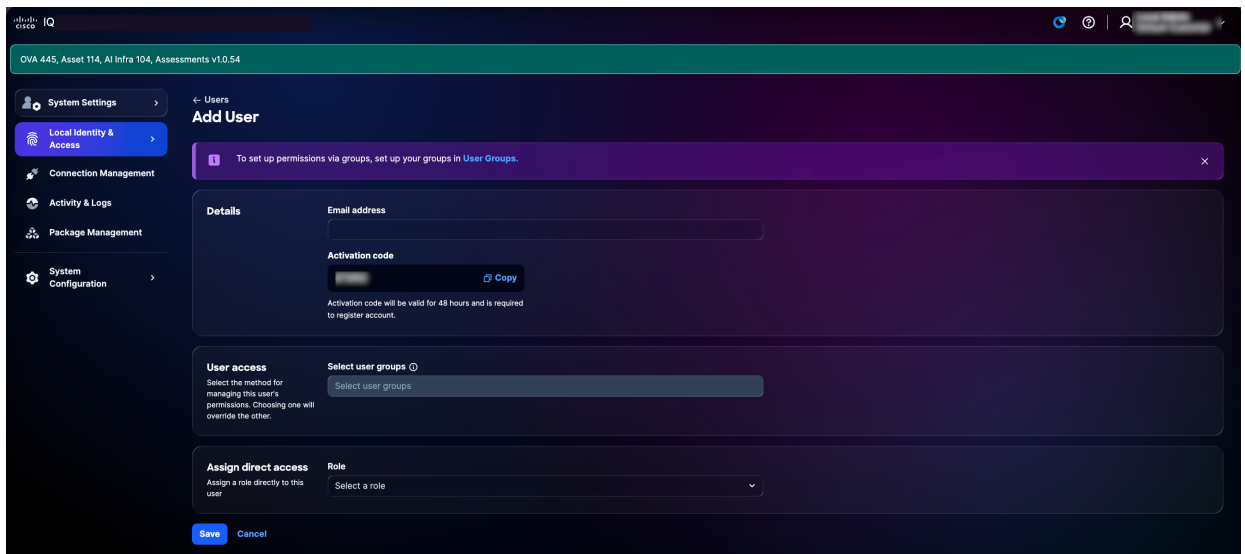
사용자를 상태와 함께 나열합니다.



사용자 페이지

 참고: 안전하지 않은 채널을 통해 활성화 코드를 공유하지 마십시오. 코드가 손실되거나 손상된 경우 메뉴 아이콘을 사용하여 이전 활성화 코드를 무효화하는 새 활성화 코드를 다시 생성합니다. 활성화 코드는 48시간 동안 유효합니다. 코드가 만료되면 계정 관리자에게 문의하여 새 코드를 요청하십시오.

- 사용자 추가를 클릭합니다. Add User(사용자 추가) 페이지가 표시됩니다.



사용자 추가

3. 이메일 주소를 입력합니다.

4. 활성화 코드를 입력합니다.

 참고: 활성화 코드는 기본적으로 표시됩니다. 등록에 필요한 대로 표시된 활성화 코드를 사용자와 공유합니다.

5. User access(사용자 액세스)의 Select user groups(사용자 그룹 선택) 드롭다운 목록에서 사용자 그룹을 선택합니다.



참고: 사용자는 선택한 그룹에서 액세스 권한을 상속합니다.

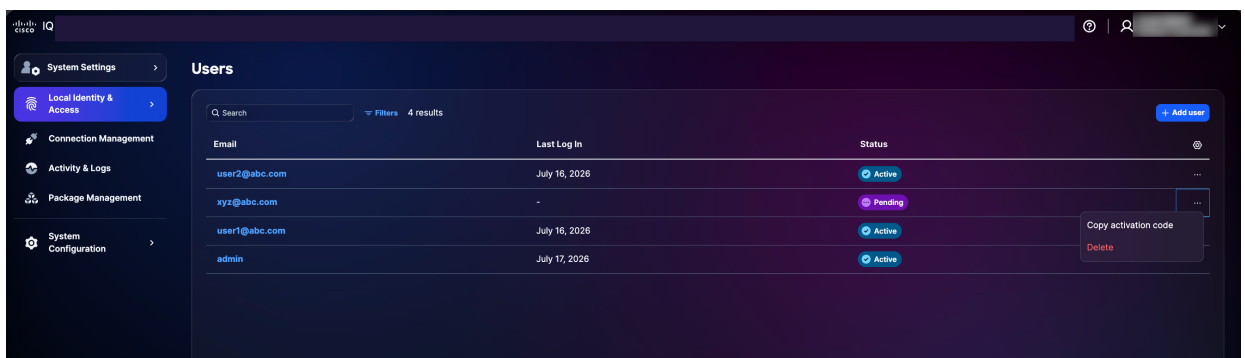
6. Assign direct access(직접 액세스 할당)의 Role(역할) 드롭다운 목록에서 역할을 선택합니다. 다음 두 가지 역할을 사용할 수 있습니다.

- 뷰어: 애플리케이션 보기 및 액세스
- 계정 관리자: 액세스 모듈 및 IDP(System Management and Identity Provider)를 제외한 시스템 설정 관리

7. 저장을 클릭합니다. 새 사용자가 생성되어 사용자 목록에 보류 중 상태로 표시됩니다. Pending(보류 중)은 사용자가 아직 자동 활성화를 완료하지 않았음을 나타냅니다.

8. 목록에서 새로 생성된 사용자를 찾고 Status 열에 Pending(보류 중)이 표시되는지 확인합니다.

9. 새로 생성된 사용자 옆에 있는 More Options(추가 옵션) 아이콘을 클릭합니다.



활성화 코드 복사

10. 드롭다운 목록에서 활성화 코드 복사를 선택합니다. 활성화 코드가 클립보드에 복사됩니다.

11. 이 코드를 사용자와 안전하게(예: 안전한 내부 채널을 통해) 공유합니다. 활성화 코드는 1회용이며 등록을 완료하는 데 필요합니다.



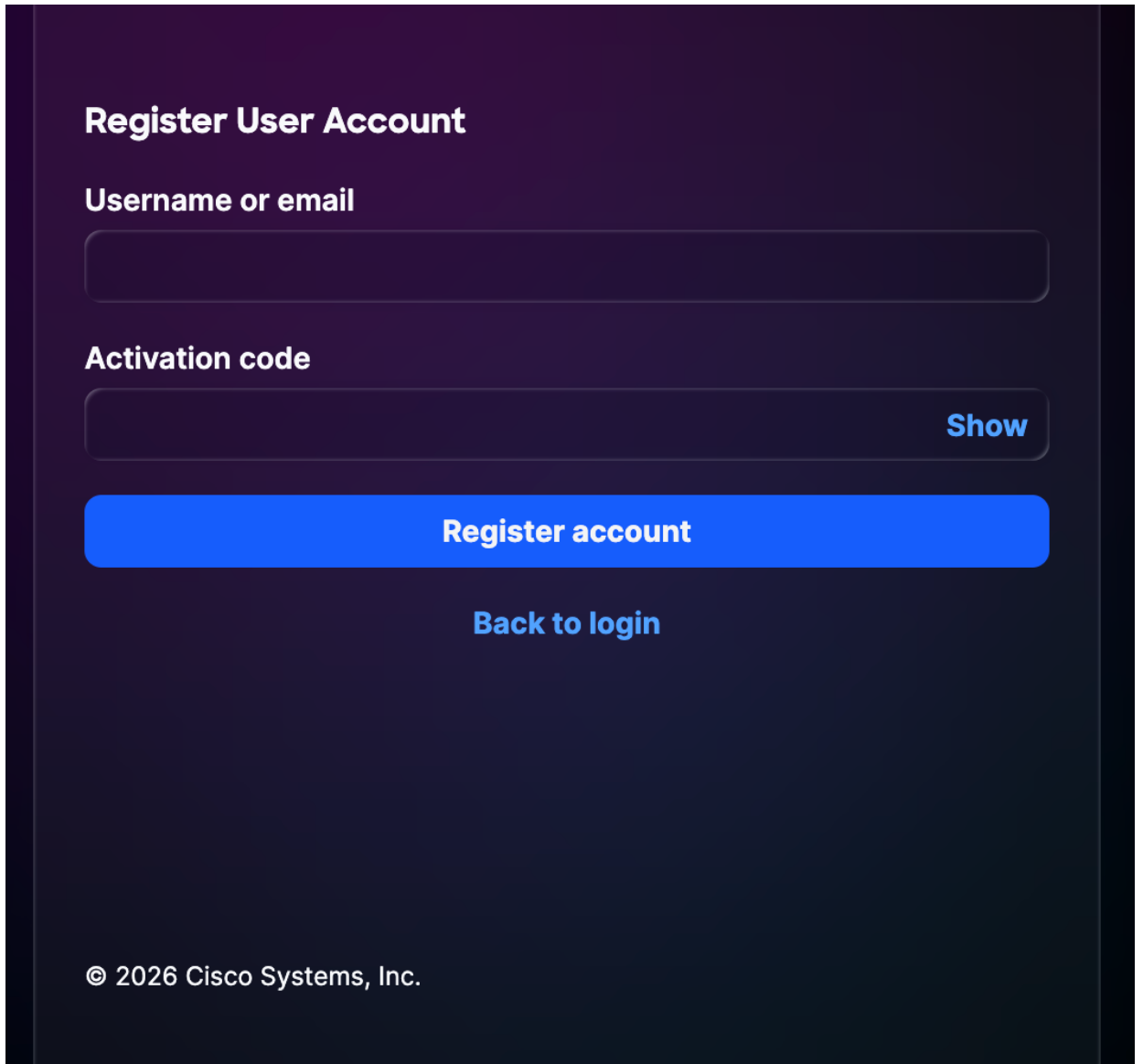
참고: 안전하지 않은 채널을 통해 활성화 코드를 공유하지 마십시오. 코드가 손실되거나 손상된 경우 메뉴 아이콘을 사용하여 이전 활성화 코드를 무효화하는 새 활성화 코드를 다시 생성합니다. 활성화 코드는 48시간 동안 유효합니다. 코드가 만료되면 계정 관리자에게 문의하여 새 코드를 요청하십시오.

12. 로그아웃하려면 오른쪽 상단 모서리에 있는 사용자 프로필 아이콘을 클릭하고 Logout(로그아웃)을 선택합니다. Cisco IQ 로그인 페이지로 돌아갑니다.

새 사용자 계정 등록

새 사용자 계정을 등록하려면

1. 로그인 페이지에서 새 사용자 계정 등록 링크를 클릭합니다.

A registration form titled "Register User Account" on a dark purple background. It features two input fields: "Username or email" and "Activation code". The "Activation code" field has a "Show" button to its right. Below the fields is a large blue "Register account" button, and below that is a blue "Back to login" link. At the bottom left, the copyright notice "© 2026 Cisco Systems, Inc." is displayed.

Register User Account

Username or email

Activation code

 Show

Register account

Back to login

© 2026 Cisco Systems, Inc.

새 사용자 계정

2. 사용자를 만들 때 사용한 사용자 이름 또는 이메일 주소(예: user1@abc.com)를 입력합니다.
3. 계정 관리자가 공유하는 활성화 코드를 입력합니다.
4. 계정 등록을 클릭합니다. 새 암호 설정 창이 표시됩니다.

Set New Password

Choose a strong password that contains the following:

- At least 15 characters
- At least 2 uppercase characters
- At least 2 lowercase characters
- At least 2 numeric characters
- At least 2 special characters
- No repeating characters

New password

Show

Confirm password

Show[Reset password](#)[Back to login](#)

새 사용자 계정 암호

5. 새 비밀번호를 입력합니다.
6. 비밀번호 확인에 비밀번호를 다시 입력합니다.
7. 첫 번째 로그인에 성공하면 사용자에게 5개의 보안 질문을 구성하라는 메시지가 표시됩니다. ([보안 질문 설정 참조](#)).

로컬 사용자 그룹 관리

사용자 그룹을 사용하면 계정 관리자가 여러 로컬 사용자의 역할을 동시에 관리할 수 있습니다. 각 사용자에게 개별적으로 역할을 할당하는 대신 그룹을 만들고, 여기에 역할과 사용자 집합을 연결하고, 역할 또는 멤버십을 한 곳에서 업데이트할 수 있습니다. 모든 사용자 그룹 관리는 Local Identity & Access(로컬 ID 및 액세스) 페이지에서 수행됩니다.



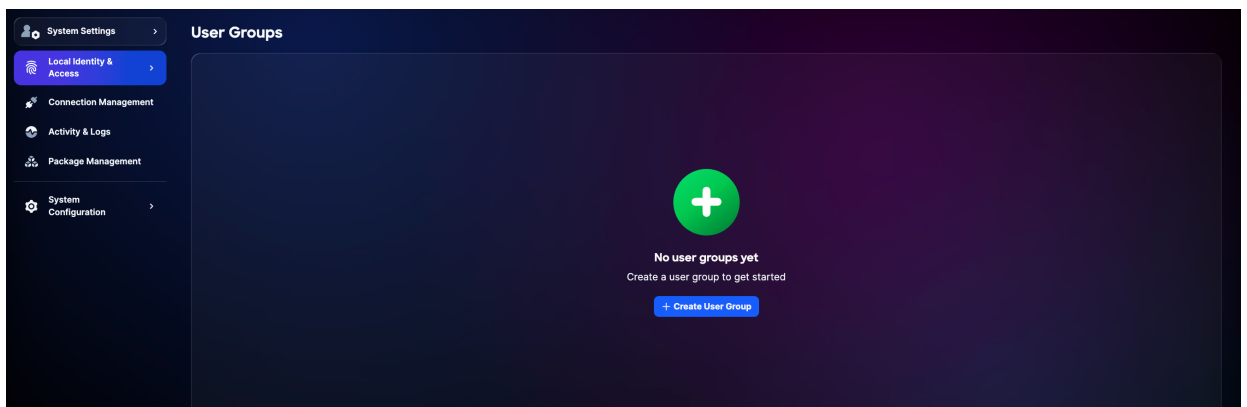
참고: 계정 관리자만 사용자 그룹을 생성, 편집 또는 삭제할 수 있습니다. 그룹은

 기존 로컬 사용자로 구성됩니다. 사용자를 그룹에 추가하려면 먼저 사용자를 만들어야 합니다. 자세한 내용은 [로컬 사용자](#) 추가를 참조하십시오.

사용자 그룹 생성

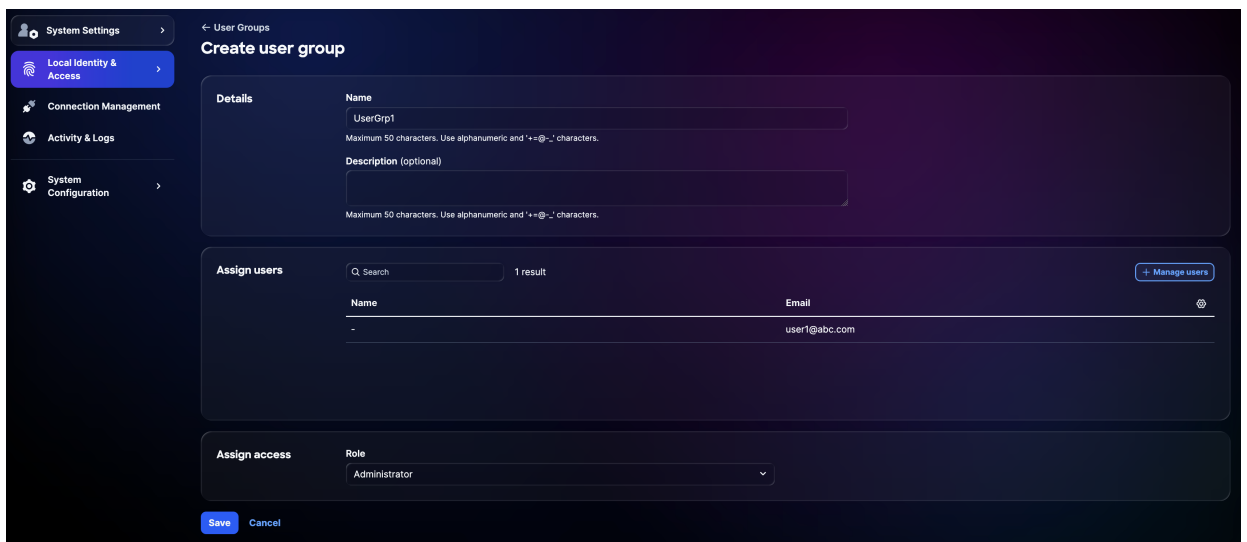
사용자 그룹을 생성하려면

1. System Settings(시스템 설정)에서 Local Identity & Access(로컬 ID 및 액세스) > User Groups(사용자 그룹)를 선택합니다. User Groups(사용자 그룹) 페이지가 표시됩니다.



사용자 그룹

2. Create User Group(사용자 그룹 생성)을 클릭합니다. Create user group(사용자 그룹 생성) 페이지가 표시됩니다.



사용자 그룹 생성

3. 다음 섹션을 완료합니다.

- 세부사항
- 이름: 그룹의 고유한 이름을 입력합니다(예: 읽기 전용 연산자)

- 설명(선택 사항): 그룹에 대한 간단한 설명(최대 50자; 영숫자 및 + = @ - _ 문자는 허용)
- 사용자 할당: 그룹에 추가할 기존 로컬 사용자를 하나 이상 검색하고 선택합니다. 참고: 아직 나열되지 않은 사용자를 추가하려면 사용자 관리를 클릭합니다.
- 액세스 권한 할당
- 역할: 이 그룹의 모든 구성원에 할당할 시스템 역할을 선택합니다. 다음 역할을 사용할 수 있습니다.
- 뷰어: 모듈 보기 및 액세스(읽기 전용)
- 관리자: 모듈 액세스 및 시스템 설정 관리

4. 저장을 클릭합니다.

새 사용자 그룹이 할당된 역할 및 구성원 수와 함께 사용자 그룹 목록에 표시됩니다.

사용자 그룹 수정

사용자 그룹을 수정하려면

1. User Groups(사용자 그룹) 목록에서 수정할 그룹을 찾습니다.
2. 추가 옵션 아이콘 > 원하는 그룹의 편집을 선택합니다. 사용자 그룹 편집 페이지가 표시됩니다.

사용자 그룹 편집

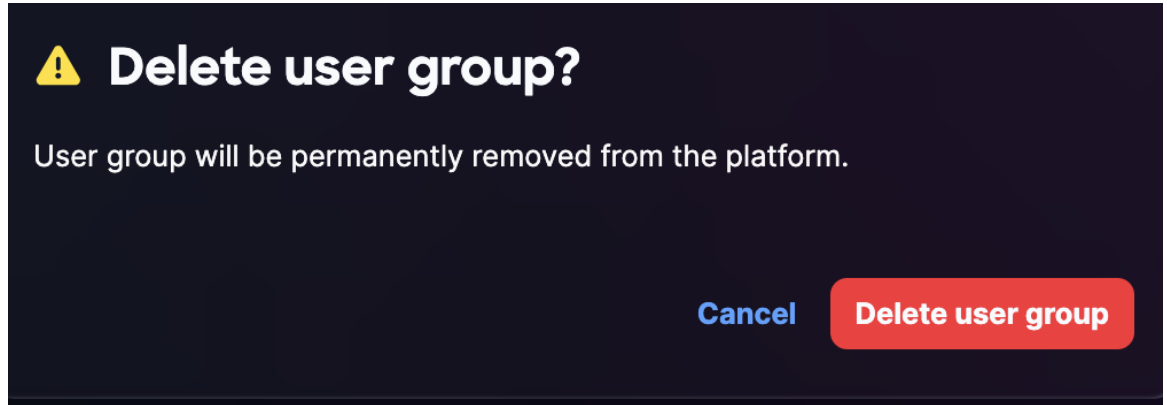
3. 원하는 대로 변경합니다.
4. 저장을 클릭합니다.

업데이트된 그룹이 사용자 그룹 목록에 표시됩니다. 새 역할은 그룹의 모든 구성원에 대해 적용됩니다.

사용자 그룹 삭제

사용자 그룹을 삭제하려면

1. User Groups(사용자 그룹) 목록에서 삭제할 그룹을 찾습니다.
2. 그룹 옆의 More Options 아이콘을 클릭하고 Delete를 선택합니다.



사용자 그룹 삭제

3. 프롬프트가 표시되면 삭제를 확인합니다.

사용자 그룹 목록에서 그룹이 제거됩니다.



참고: 사용자 그룹을 삭제하면 모든 구성원에서 그룹 기반 역할 할당이 제거됩니다. 개별 사용자 계정은 삭제되지 않습니다.

ID 공급자 구성

VA에 로그인하면 계정 관리자가 다양한 설정을 구성할 수 있습니다. 계정 관리자는 로컬 관리 또는 IDP 컨피그레이션을 사용하여 로그인할 수 있습니다.

SSO용 Okta IDP SAML 컨피그레이션

IDP SAML 구성 사전 요구 사항

- Cisco IQ에 대한 로컬 관리자 액세스
- IDP 포털 액세스

SSO에 대한 IDP SAML 컨피그레이션

SSO에 대해 IDP SAML(Security Assertion Markup Language)을 구성하려면

1. IDP 포털로 이동합니다.

표 2: Cisco IQ 특성

필드	가치
애플리케이션 이름	<응용 프로그램 이름>
환경	ESP 비즈니스 애플리케이션
애플리케이션 소유자 그룹	IDP 설정의 소유자
팀 메일러	팀용 메일러
대상	비인력
온보딩 범주	"New Onboarding(새 온보딩)"을 선택합니다.

표 3: SAML 컨피그레이션 매개변수

매개변수	설정	예
대상(엔티티 ID)	FQDN(정규화된 도메인 이름)	mymanagementhost.mydomain.com
Single Sign-On URL	SAML Assertion ACS(고객 서비스) 엔드포인트	https://mymanagementhost.mydomain.com/saml/acs
이름 ID 형식	이메일 주소	해당 없음
애플리케이션 사용자 이름	사용자 이름	해당 없음

5. 특성 명령문을 구성합니다.

 참고: IDP 특성 변경 사항은 특정 공급자 및 컨피그레이션에 따라 달라집니다. Cisco IDP와 그 특성은 아래를 예로 들어 공유됩니다.

- 1차 진입
 - 이름: 사용자 이름
 - 가치: 사용자 로그인
- 두 번째 항목
 - 이름: 기본 이메일
 - 가치: 사용자 이메일
- Group Attribute 문
 - 이름: 그룹
 - 필터: 레젝스
 - 가치: *

6. 애플리케이션에서 SLO(Single Logout) 설정을 구성합니다.

표 4: SLO 구성 설정

필드	가치
서명 인증서	Okta의 경우 이 인증서는 SLO를 활성화하도록 선택한 경우에만 필요합니다. ID 공급자에서 SP 인증서 다운로드를 사용하여 서명 인증서를 다운로드합니다. 파일을

필드	가치
	sp-public-key.crt로 저장합니다. 자세한 내용은 단일 로그아웃 컨피그레이션을 참조하십시오.
SP 메타데이터	SP(서비스 공급자) 메타데이터는 ADFS IDP에만 필요하며 Okta에는 필요하지 않습니다.
단일 로그아웃을 사용하시겠습니까?	예 또는 아니요
단일 로그아웃 URL	https://mymanagementhost.mydomain.com/saml/logout
SP 발급자(대상/엔티티 ID 또는 ACS URL)	https://mymanagementhost.mydomain.com

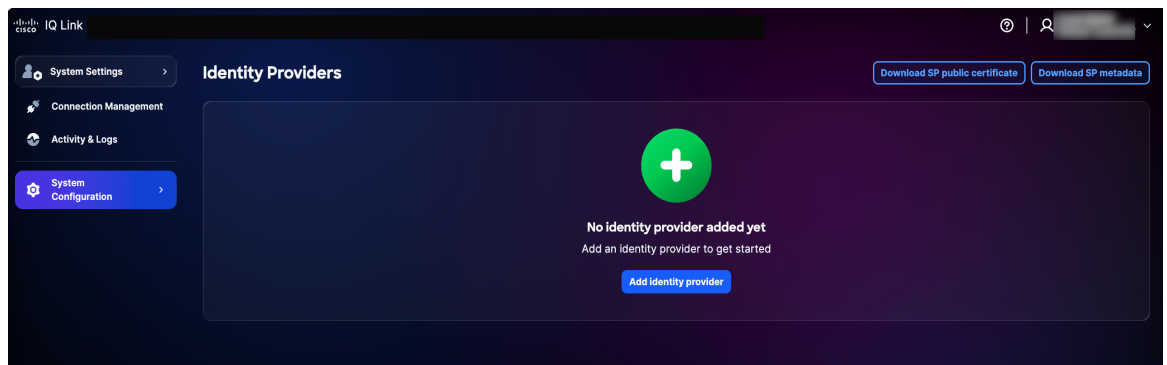
8. "IDP Metadata XML" 파일을 다운로드하려면 다운로드 아이콘을 클릭합니다.

9. 공급자가 요구하는 대로 애플리케이션을 프로비저닝하거나 생성합니다.

Okta IDP 추가

Cisco IQ에서 IDP를 추가하려면

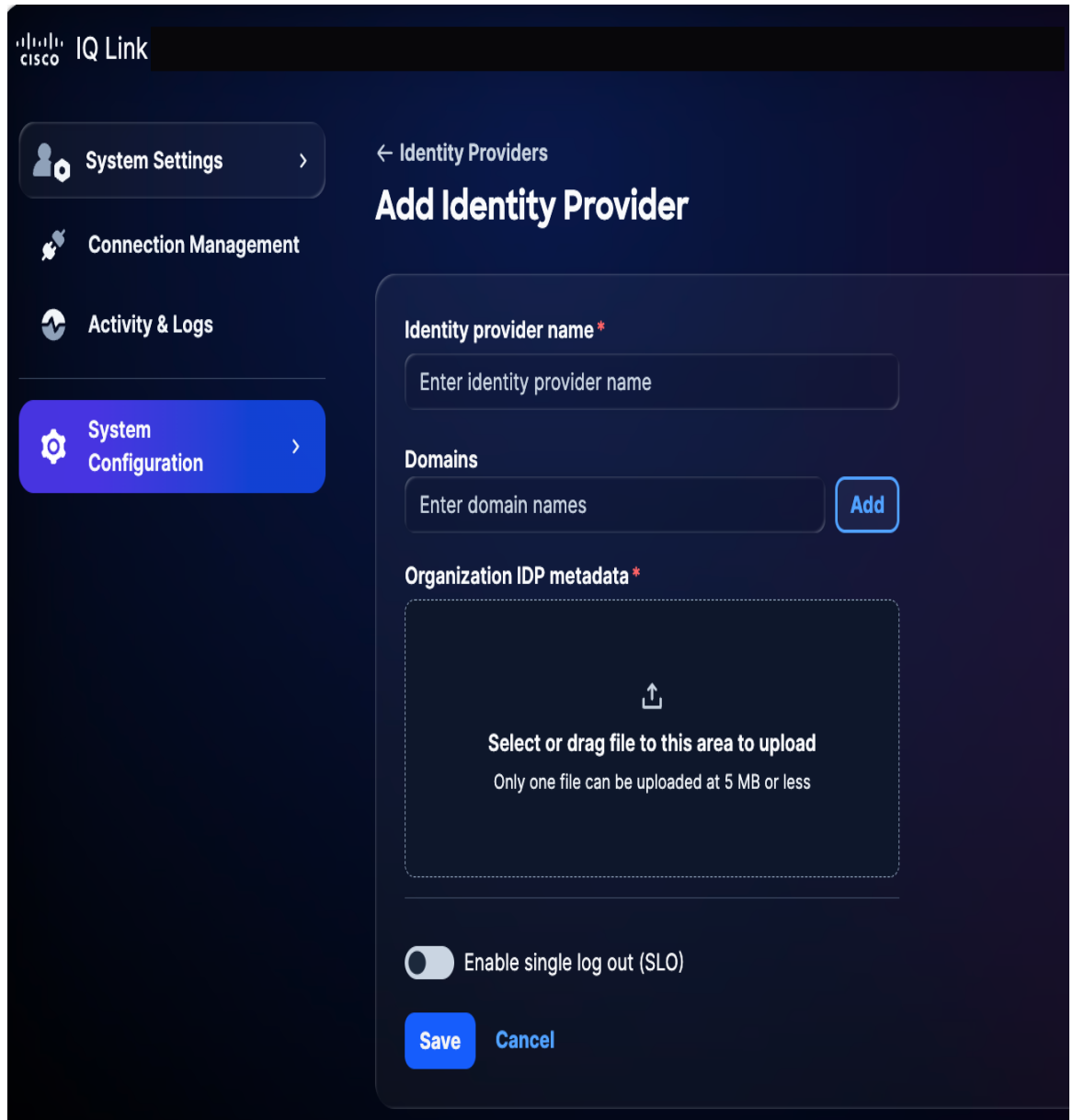
1. System Settings(시스템 설정)에서 System Configuration(시스템 컨피그레이션) > Identity Providers(ID 제공자)를 선택합니다. ID 제공자 페이지가 표시됩니다.



IDP 홈 페이지

참고: 지정된 시간에 하나의 IDP만 추가할 수 있습니다.

2. Add Identity Provider를 클릭합니다. Add Identity Provider 페이지가 표시됩니다.



ID 공급자 추가

3. ID 공급자 이름을 입력합니다.
4. Add(추가)를 클릭하여 Cisco IQ로 구성된 도메인 이름을 Domain(s) 필드에 추가합니다.
5. IDP 애플리케이션에서 얻은 SAML 메타데이터 파일을 Organization IDP metadata(조직 IDP 메타데이터) 필드에 끌어 놓거나 업로드하는 방법입니다. 이 파일에는 인증서 세부사항 및 SP 엔티티 세부사항이 포함되어 있습니다.
6. (선택 사항) Enable single logout(단일 로그아웃 활성화) 토글 버튼을 켭니다. 나중에 SLO를 활성화할 수도 있습니다.
7. 저장을 클릭합니다.

역할 매핑 컨피그레이션

1. 추가된 IDP에서 More Options(추가 옵션) 아이콘 > Map Roles(역할 매핑)를 선택합니다. [사용자 역할 매핑] 페이지가 표시됩니다.

×

Map identity provider roles to system roles to assign permissions.

Map User Roles

IDP Role	System Role
iq-demo-user ⊗	General Account... ⊗ ▾ ⊗
	▾ ⊗
	▾ ⊗
	▾ ⊗
	▾ ⊗

+ Add identity provider role

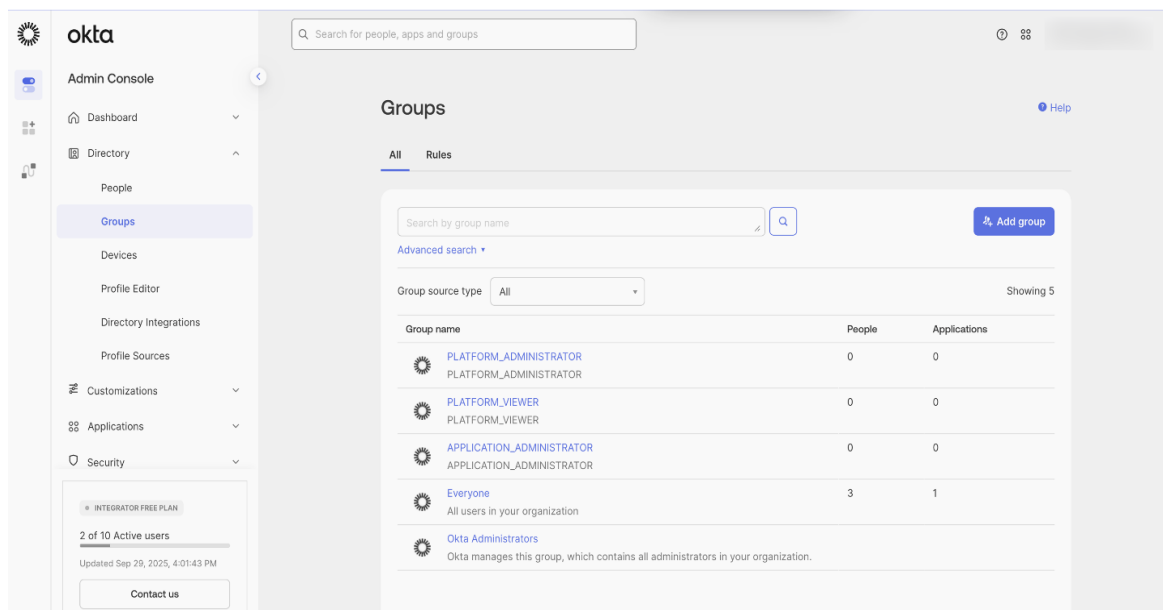
Save

사용자 역할 매핑

2. 선택한 시스템 역할에 대한 IDP 역할을 입력하십시오. 지원되는 시스템 역할은 다음과 같습니다.

- 일반 계정 관리자: 일반 계정 관리자는 제품의 모든 작업을 수행할 수 있는 모든 권한을 가집니다
- 일반 계정 뷰어: 일반 계정 뷰어에는 읽기 전용 액세스 권한이 있습니다

 참고: IDP 역할은 열린 텍스트 필드입니다. 조직의 IDP에 구성된 그룹 또는 역할 이름과 정확히 일치해야 합니다. Okta 그룹의 예는 아래에 공유됩니다.



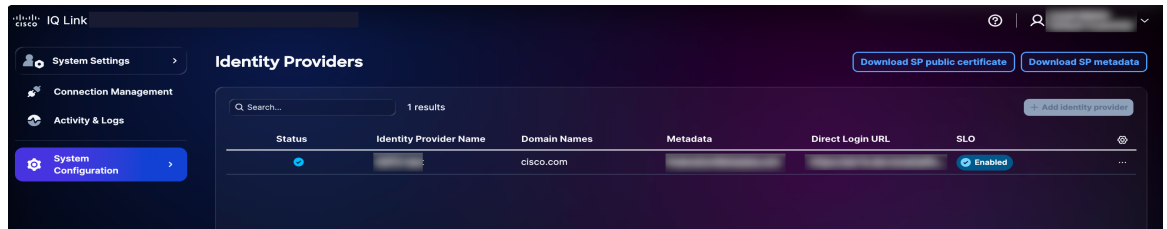
역할 매핑 참조

3. Add ID provider role(ID 제공자 역할 추가)을 클릭하여 필요에 따라 추가 역할을 매핑합니다.
4. 저장을 클릭합니다. 구성이 완료되면 로그인 페이지에 (IDP를 통해) SSO로 로그인할 수 있는 옵션이 표시됩니다.

단일 로그아웃 컨피그레이션

SLO를 활성화하려면 SLO URL이 포함된 메타데이터를 업로드해야 합니다. ID 공급자 설정을 편집하고 단일 로그아웃 사용 토글을 켜면 이를 구성할 수 있습니다. SLO 컨피그레이션을 완료하려면

1. Identity Providers(ID 공급자) 홈 페이지에서 Download SP public certificate(SP 공용 인증서 다운로드)를 클릭합니다.



SP 공용 인증서

2. 다운로드한 파일을 sp-public-key.crt로 저장합니다.
3. IDP 포털로 이동합니다.
4. [SSO를 위한](#) IDP SAML 컨피그레이션에서 생성된 서명 인증서 [파일을 업로드합니다](#).
5. SLO URL(예: https://ciq-xxx-xxx-37-160.cx-hub-rtp.cisco.com/saml/logout)을 입력합니다.
6. SP 발급자(예: ciq-xxx-xxx-37-160.cx-hub-rtp.cisco.com)를 입력합니다.
7. Submit(제출)을 클릭합니다.
8. IDP 메타데이터 파일을 다시 다운로드합니다.
9. Identity Providers(ID 제공자) 페이지에서 추가된 IDP의 More Options(추가 옵션) 아이콘 > Edit(수정)를 선택합니다.
10. Enable single log out (SLO)(단일 로그아웃(SLO) 활성화) 토글 버튼을 켭니다.
11. 새로 다운로드한 메타데이터 파일을 업로드합니다.
12. 다음 체크리스트를 사용하여 SSO 및 SLO 기능을 확인합니다.

확인 체크리스트:

- 로컬 관리자 로그인에 성공했습니다.
- IDP 포털이 구성 및 프로비저닝됨
- IDP는 "성공" 상태로 Cisco IQ에 추가됩니다
- 역할 매핑이 구성되고 테스트됨
- SP 메타데이터가 다운로드되고 인증서가 추출됨
- SLO가 활성화된 경우 SLO 컨피그레이션이 실제 서명 인증서로 완료됩니다
- 엔드 투 엔드 SSO 및 SLO 흐름 테스트 성공

IDP 문제 해결

다음 표에는 IDP 상태, 인증서 오류, SSO 로그인 실패 및 SLO 컨피그레이션과 관련된 문제를 신속하게 파악하고 해결하는 데 도움이 되는 일반적인 문제 및 가능한 솔루션이 나열되어 있습니다.

표 5: 문제 해결

문제	솔루션
IDP 상태가 "Incomplete(미완료)"로 표시됩니다.	역할 매핑 컨피그레이션 확인
인증서 오류	인증서 형식 및 유효성 확인
SSO 로그인 실패	특성 매핑 및 그룹 할당 검증
SLO가 예상대로 작동하지 않음	인증서가 제대로 업로드되고 SLO URL이 구성되었는지 확인합니다.

AD FS IDP SAML SSO 컨피그레이션

이 섹션에서는 Microsoft AD(Active Directory) FS(Federation Services)를 Cisco IQ용 SAML IDP로 구성하여 비밀번호 기반 및 PKI(Public Key Infrastructure) 또는 인증서 기반 인증을 지원하는 방법에 대해 설명합니다.

AD FS IDP SAML을 SSO에 구성하기 위한 사전 요구 사항

- AD FS 6.0 이상이 권장됨
- Windows Server 2016 + (권장 2019)
- 구성된 AD와 사용자 계정 통합
- AD FS 서버의 SSL/TLS 인증서
- Cisco IQ에 대한 관리자 액세스
- ADFS 서버(Windows Server)에 대한 관리 액세스
- AD FS 서버의 PowerShell 액세스
- AD FS와 Cisco IQ 간의 네트워크 연결
- 엔터프라이즈 CA(Certificate Authority)(설치되었거나 연결 가능)
- 도메인 관리자 또는 기업 관리자 권한(PKI에만 필요)
- AD FS 서버 컨피그레이션 세부 정보(아래 표 참조)

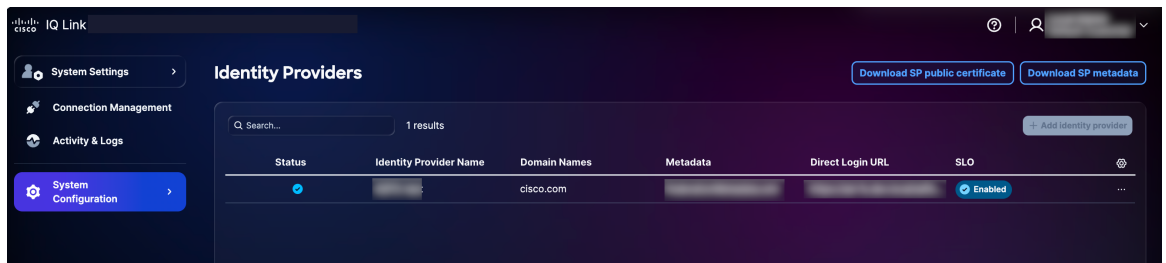
표 6: 인증 흐름 개요

항목	설명	예
Cisco IQ FQDN	사용자 배포 호스트 이름	<Your-CIQ-FQDN> 예: dev35-23.cx-xxx-xxx.cisco.com
ADFS 서버 URL	사용자 AD FS 서버 주소	https://<Your-ADFS-HOSTNAME> 예: https://ad-fs.dev.local
회사 도메인	이메일 도메인	<사용자-도메인>
AD 그룹	Active Directory 그룹 DN(도메인 이름)	CN=역할 - CXIQ 개발자 OU=그룹, DC=dev, DC=로컬
CA 이름(PKI)	엔터프라이즈 CA 이름	<Your-CA-Name>
인증서 인증 포트(PKI)	AD FS 대체 TLS 포트	49443
SSL 인증서 지문	AD FS 서버 SSL 인증서	<Your-SSL-CERT-THUMBPRINT>

기본 AD FS SAML 구성

AD FS를 구성하려면

1. System Settings(시스템 설정)에서 System Configuration(시스템 컨피그레이션) > Identity Providers(ID 제공자)를 선택합니다. ID 제공자 페이지가 표시됩니다.



다운로드 옵션

2. Download SP public certificate and Download SP metadata(SP 공용 인증서 다운로드 및 SP 메타데이터 다운로드)를 클릭하여 이러한 파일을 다운로드합니다.
3. service-provider-metadata.xml 및 service-provider-certificate.crt 파일을 복사하여 ADFS 서버(예: C:\)에 저장합니다.
4. AD FS 서버에 로그인합니다.
5. AD FS Management(AD FS 관리) 메뉴에서 Relying Party Trust(당사자 Trust)를 클릭합니다.
6. Relying Party Trust 메뉴에서 Add Relying Party Trust를 클릭합니다. 새 마

법사가 열립니다.

7. Claims Aware 라디오 버튼을 클릭합니다.
8. Start(시작)를 클릭하여 컨피그레이션을 진행합니다.
9. 파일에서 신뢰 당사자에 대한 데이터 가져오기를 클릭하여 3단계의 일부로 저장된 파일에서 세부 정보를 가져옵니다.
10. Browse(찾아보기)를 클릭하여 통신 사업자 메타데이터 파일을 선택하고 파일 업로드를 완료합니다.
11. Next(다음)를 클릭합니다.
12. 표시 이름(예: "Cisco IQ")을 입력하고 관련 메모를 추가한 후 Next(다음)를 클릭합니다.
13. Choose Access Control Policy(액세스 제어 정책 선택) 페이지에서 Permit everyone(모두 허용)(또는 조직의 보안 컨피그레이션에 필요한 정책)을 클릭합니다.
14. 나머지 화면에서 Next(다음)를 클릭합니다.
15. Close(닫기)를 클릭하여 당사자 Trust 컨피그레이션을 완료합니다.



참고: AD FS 서버에 등록된 MFA(Multi-Factor Authentication) 어댑터(예: Azure MFA, 구성된 시간 기반 TOTP(One-Time Password)).

이 정책이 구성된 MFA 제공자 없이 활성화된 경우 ADFS는 사용자를 인증하지만 궁극적으로 urn:oasis:names:tc:SAML:2.0:status:RequestDenied 상태의 요청을 거부합니다. SAML 응답에 어설션이 포함되어 있지 않으므로 플러그인이 실패하고 "이메일 누락" 오류를 보고합니다.

문제: "Permit Everyone with MFA(MFA로 모든 사용자 허용)"가 선택됩니다.

해결 방법: PowerShell에서 다음 명령을 실행하여 현재 정책을 확인합니다.

```
Get-AdfsRelyingPartyTrust -Name
```

“

```
”).AccessControlPolicyName
```

To set “Permit everyone” (no MFA requirement), run the following command:

```
Set-AdfsRelyingPartyTrust -TargetName “
```

”

```
-AccessControlPolicyName “Permit everyone”
```

You can also create the trust through PowerShell:

```
-Add-AdfsRelyingPartyTrust `
-Name "
" `
-Identifier "
" `
-SamlEndpoint (New-AdfsSamlEndpoint -Binding POST -Protocol
SAMLAssertionConsumer -Uri "
") `
-AccessControlPolicyName "Permit everyone" `
-IssuanceAuthorizationRules '=> issue(Type =
"http://schemas.microsoft.com/authorization/claims/permit", Value =
"true");
```

ADFS 클레임 규칙 구성

ADFS 클레임 규칙을 구성하려면 다음 섹션에 나열된 단계를 수행합니다.

필수 클레임

필요한 클레임은 다음 표를 참조하십시오.

표 7: 필수 클레임

클레임	목적	소스
Email	사용자 식별자	AD 메일
표시 이름	사용자의 전체 이름	AD 표시 이름
UPN	PKI/인증서 인증	ADFS는 UPN을 통해 클라이언트 인증서를 AD 사용자에게 매핑합니다
이름 ID	SAML 제목	이메일 변형
그룹	역할 기반 액세스	AD 그룹 구성원(memberOf)

클레임 규칙 적용

1. 당사자 Trust의 이름을 정의합니다(예: "Cisco IQ - Production").

```
$relyingPartyName = "Your-RP-Name"
```

2. 사용자 정보 및 그룹 멤버십을 Cisco IQ에 전송하도록 클레임 규칙을 정의합니다.

```
$claimRules = @'
@RuleTemplate = "LdapClaims"
@RuleName = "Send Email and Name"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"),
@RuleTemplate = "LdapClaims"
@RuleName = "Send UPN"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"),
query = ";userPrincipalName;{0}", param = c.Value);
@RuleName = "Transform Email to NameID"
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "email");
@RuleName = "Send Group Membership"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/group"),
query = ";memberOf;{0}", param = c.Value);
'@
```

3. 다음 명령을 실행하여 클레임 규칙을 적용합니다.

```
Set-AdfsRelyingPartyTrust -TargetName $relyingPartyName
-IssuanceTransformRules $claimRules
```

Write-Host "클레임 규칙이 성공적으로 구성되었습니다!" -ForegroundColor Green

경고: 각 AD 사용자 계정에는 메일 특성이 채워져 있어야 합니다. 이 특성이 없으면 SAML assertion에 이메일 클레임이 포함되지 않으므로 인증이 거부됩니다.

사용자의 이메일 주소를 업데이트하려면 다음 PowerShell 명령을 실행합니다.

```
Set-ADUser -Identity "
```

```
" -EmailAddress
```

“

”

사용자 그룹 확인

1. 다음 명령을 실행하여 사용자의 그룹 멤버십을 확인하도록 사용자 이름을 설정합니다.

```
$username = "username"
```

2. 다음 명령을 실행하여 사용자 계정을 찾습니다.

```
$searcher = [adsisearcher]"(samaccountname=$username)"  
$user = $searcher.FindOne()
```

3. 다음 명령을 사용하여 사용자가 속한 그룹을 표시합니다.

```
$user.Properties.memberof
```

출력 예:

CN=역할 - CXIQ 개발자,OU=역할 그룹,DC=dev,DC=local

SP 서명 인증서를 신뢰하도록 AD FS 구성

1. AD FS 서버에서 SP 인증서를 TrustedPeople 저장소로 가져옵니다.

```
Import-Certificate -FilePath "C:-provider-certificate.crt"  
-CertStoreLocation "Cert:"
```

2. 다음 옵션 중 하나를 선택합니다.



참고: SP 인증서는 AD FS가 표준 신뢰 체인을 통해 검증할 수 없는 내부 CA에서 발급됩니다.

- 이 신뢰 당사자에 대해 전역적으로 체인 유효성 검사 사용 안 함

```
Set-AdfsRelyingPartyTrust `
-TargetIdentifier “
```

```
” `
```

```
-SigningCertificateRevocationCheck None `
-EncryptionCertificateRevocationCheck None
```

- SP 인증서가 자체 서명되지 않은 CA에서 발급된 경우 발급된 CA 인증서를 루트 인증서 저장소로 가져옵니다

```
Import-Certificate -FilePath “C:-ca.cer” -CertStoreLocation
“Cert:”
```

3. ADFS 서비스를 다시 시작하여 변경 사항을 적용합니다.

```
Restart-Service adfssrv
```

PKI/인증서 인증 설정

이 섹션에서는 비밀번호와 함께 인증서 기반(즉, 스마트 카드 또는 소프트웨어 인증서) 인증을 추가하는 방법에 대해 설명합니다. 비밀번호 전용 인증만으로 충분할 경우 이 섹션을 건너뛸 수 있습니다.

AD CS CA 역할 설치

AD CS(인증서 서비스) CA 역할을 설치하려면

1. 다음 명령을 실행하여 도메인에 엔터프라이즈 CA가 이미 있는지 확인합니다.

```
certutil -config - -ping
```

명령이 유효한 응답을 반환하는 경우 이 섹션의 나머지 부분을 건너뛸 수 있습니다. 환경이 이미 구성되었습니다. CA를 찾을 수 없음을 나타내는 경우 2단계로 진행합니다.

2. 다음 명령을 실행하여 CA 역할을 설치합니다.


```
install-WindowsFeature AD-Certificate -IncludeManagementTools
```

3. 다음 명령을 실행하여 CA 역할을 구성합니다.

```
nstall-AdcsCertificationAuthority `
-CAType EnterpriseRootCA `
-CACommonName "
`
-KeyLength 2048 `
-HashAlgorithmName SHA256 `
-CryptoProviderName "RSA#Microsoft Software Key Storage Provider" `
-ValidityPeriod Years `
-ValidityPeriodUnits 10 `
-Force
```

4. 다음 명령을 실행하여 설치를 확인합니다.

```
certutil -ca
```

5. 다음 명령을 실행하여 서비스가 활성 상태이고 연결할 수 있는지 확인합니다

```
certutil -config - -ping
```

인증서 템플릿 구성

클라이언트 인증 ECU(Enhanced Key Usage)를 사용하여 인증서 템플릿을 구성하려면

1. certsrv.msc를 열고 CA 노드를 확장합니다.
2. Certificate Templates(인증서 템플릿) > Manage(관리)를 마우스 오른쪽 버튼으로 클릭합니다.
3. 사용자 템플릿을 복제합니다.



참고: 기본 제공 사용자 템플릿은 해당 템플릿에서 발급된 인증서에 클라이언트 인증 ECU가 포함된 경우에만 유효하거나 작동합니다.

4. 다음 탭에서 설정을 구성합니다.

- 일반: Name(이름) 필드에 유효 기간이 1년인 "CIQ 사용자 인증"을 입력합니다
- 요청 처리: Purpose 드롭다운 목록에서 Signature and encryption을 선택하고 Allow private key to exported(개인 키를 내보냄 허용) 확인란을 선택합니다
- 주체 이름: Build from Active Directory Information(Active Directory 정보에서 빌드)을 선택하고 Subject(제목) 및 SAN(SAN) 필드에 이메일을 포함합니다

경고: Subject(제목) 및 SAN 필드에는 사용자의 UPN(User Principal Name) 또는 AD 계정과 일치하는 이메일이 포함되어야 합니다. AD FS는 이러한 필드를 사용하여 AD 사용자에게 인증서를 매핑합니다.

- 내선 번호: 애플리케이션 정책에 "클라이언트 인증 (1.3.6.1.5.5.7.3.2)"이 포함되어 있는지 확인합니다.
- Security: 도메인 사용자 추가 및 읽기 및 등록 권한 부여

5. 다음 명령을 사용하여 템플릿을 게시합니다.

```
Add-CATemplate -Name "CIQUserAuthentication" -Force
```

사용자 인증서 등록

1. 대상 사용자로 로그인합니다.
2. 다음 명령을 실행하여 인증서를 등록합니다.

```
certreq -enroll -user "CIQUserAuthentication"
```

3. 다음 명령을 실행하여 인증서 설치를 확인합니다.

```
Get-ChildItem Cert:| Where-Object {
    $_.EnhancedKeyUsageList.ObjectId -contains "1.3.6.1.5.5.7.3.2"} | Format-Table Subject,
```

Windows에서 사용자 인증서 내보내기 및 클라이언트에 설치(Mac)

Windows에서 Mac으로 사용자 인증서를 내보내려면

1. 다음 명령을 실행하여 Windows의 인증서를 PFX 파일로 내보냅니다.

```
$cert = Get-ChildItem Cert:| Where-Object { $_.Subject -like "*"
    *"}
$password = ConvertTo-SecureString -String "
    " -Force -AsPlainText
Export-PfxCertificate -Cert $cert -FilePath "C:-cert.pfx" -Password $password
```

2. user-cert.pfx 파일을 Mac 디바이스로 전송합니다.

3. 다음 명령을 실행하여 Mac 키 체인으로 인증서를 가져옵니다.

```
security import user-cert.pfx -k ~/Library/Keychains/login.keychain-db -P "
    "
```



참고: 인증서를 가져온 후에는 브라우저를 닫았다가 다시 열어야 인증서가 인식됩니다.

4. 다음을 실행하여 Mac에서 CA를 신뢰합니다.

```
sudo security add-trusted-cert -d -r trustRoot \
-k /Library/Keychains/System.keychain ca-certificate.cer
```

AD FS 인증서 인증 엔드포인트 활성화

AD FS 인증서 인증 엔드포인트를 활성화하려면

1. 다음 명령을 실행하여 필요한 ADFS 인증서 엔드포인트를 활성화합니다.

```
EEnable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/2005/certificate
```

```
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/2005/certificatetransport
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certificate
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certificatetransport
```

2. 다음 명령을 실행하여 모든 엔드포인트가 활성화되었는지 확인합니다.

```
Get-AdfsEndpoint | Where-Object { $_.AddressPath -like "*cert*" } | Format-Table Address
```

기본 인증서 인증 활성화

인증서 인증을 기본으로 활성화하려면

1. 다음 명령을 사용하여 인트라넷 및 엑스트라넷 액세스를 위한 기본 인증 공급자를 구성합니다.

```
Set-AdfsGlobalAuthenticationPolicy `
-PrimaryIntranetAuthenticationProvider @"CertificateAuthentication", "WindowsAuthentication"
-PrimaryExtranetAuthenticationProvider @"CertificateAuthentication", "FormsAuthentication"
```

2. 다음 명령을 사용하여 두 목록에 CertificateAuthentication 및 FormsAuthentication이 포함되어 있는지 확인합니다.

```
(Get-AdfsGlobalAuthenticationPolicy).PrimaryIntranetAuthenticationProvider
(Get-AdfsGlobalAuthenticationPolicy).PrimaryExtranetAuthenticationProvider
```

3. 다음 명령을 사용하여 현재 TLS 클라이언트 포트 컨피그레이션을 확인합니다.

```
Get-AdfsProperties | Select-Object HostName, HttpsPort, TlsClientPort
```

4. TlsClientPort가 49443 않으면 다음 명령을 사용하여 포트를 업데이트하고 AD FS 서비스를 다시 시작합니다.

```
Set-AdfsProperties -TlsClientPort 49443
Restart-Service adfssrv
```

SChannel/TLS 수정(PKI에 중요)

다음 절의 단계에서는 인증서 인증이 작동하지 않도록 하는 CERT_E_UNTRUSTEDROOT(0x800B0109) 오류를 해결합니다.

포트 49443에서 SSL 인증서 바인딩

포트 49443에서 SSL 인증서를 바인딩하려면

1. 다음 명령을 사용하여 포트 49443에서 기존 SSL 인증서 바인딩을 제거합니다.

```
>netsh http delete sslcert  
hostnameport=
```

:49443

2. 다음 명령을 사용하여 활성화된 클라이언트 인증서 협상을 사용하여 새 바인딩을 생성합니다.

```
netsh http add sslcert hostnameport=
```

```
:49443 `  
certhash=
```

```
appid="{5d89a20c-beab-4389-9447-324788eb944a}" `  
certstorename=MY `  
clientcertnegotiation=enable `  
verifyclientcertrevocation=disable
```

3. 다음 명령을 사용하여 클라이언트 인증서 협상이 활성화되었는지 확인합니다.

```
http show sslcert  
hostnameport=
```

:49443

인증서 저장소 정리(CRITICAL)

인증서 저장소를 정리하려면

경고: Windows SChannel은 신뢰할 수 있는 루트 저장소에 자체 서명되지 않은 인증서가 있는 경우 모든 클라이언트 인증서를 거부합니다. 이는 PKI 장애의 주요 근본 원인입니다.

1. 다음 명령을 실행하여 신뢰할 수 있는 루트 저장소에서 자체 서명되지 않은 인증서를 식별합니다.

```
$bad = Get-ChildItem Cert: | Where-Object { $_.Issuer -ne $_.Subject }  
$bad | ForEach-Object { Write-Host "PROBLEM: $( $_.Subject ) | Issuer: $( $_.Issuer )" -ForegroundColor Red }
```

2. 다음 명령을 실행하여 이러한 인증서를 중간 CA 저장소로 이동합니다.

```
$bad | Move-Item -Destination Cert:\IntermediateCA  
Write-Host "Moved $($bad.Count) cert(s) from Root to Intermediate CA store" -ForegroundColor Green
```

3. 다음 명령을 실행하여 자체 서명되지 않은 인증서가 트러스트된 루트 저장소에 남아 있지 않은지 확인합니다.

```
Get-ChildItem Cert: | Where-Object { $_.Issuer -ne $_.Subject }
```

SChannel 레지스트리 수정(중요)

올바른 인증서 인증을 보장하기 위해 SChannel 레지스트리 설정을 구성하려면

1. 다음 명령을 사용하여 레지스트리 경로 변수를 정의합니다.

```
$regPath = "HKLM:"
```

2. 다음 명령을 사용하여 아래 표에 정의된 레지스트리 설정을 적용합니다.

```
Set-ItemProperty -Path $regPath -Name "ClientAuthTrustMode" -Value 2 -Type DWord  
Set-ItemProperty -Path $regPath -Name "SendTrustedIssuerList" -Value 0 -Type DWord
```

표 8: 채널 레지스트리 설정

설정	가치	목적
ClientAuthTrustMode	2	배타적 CA 신뢰를 활성화하여 기본 검증 경로를 수정합니다.
트러스트된 발급자 목록 보내기	0	TLS 핸드셰이크 중에 서버가 신뢰할 수 있는 전체 발급자 목록을 전송하지 못하게 합니다.

CA 인증서 저장소 확인

CA 인증서 저장소를 확인하려면



참고: 사용자 인증서를 발급하는 CA 인증서가 SystemCertificates 저장소에 있어야 올바르게 인식됩니다.

1. 다음 명령을 사용하여 CA 인증서의 지문을 정의합니다.

```
$caThumbprint = "
```

```
"
```

2. 다음 명령을 사용하여 CA 인증서가 LocalMachinestore*에 이미 있는지 확인합니다.

```
$exists = Test-Path "HKLM:\caThumbprint"
```

인증서를 찾을 수 없는 경우 LocalMachine 저장소로 가져옵니다.

```
if (-not $exists) {
    Import-Certificate -FilePath "C:\YOUR-CA-CERT>.cer" `
        -CertStoreLocation "Cert:"
}
```

ADFS 서버 재부팅(필수)

다음 명령을 사용하여 ADFS 서버를 다시 시작합니다.

```
Restart-Computer -Force
```



참고: ClientAuthTrustMode 레지스트리 변경 사항은 서버가 다시 시작된 후에만 적용됩니다.

AD FS 메타데이터 내보내기

PowerShell 또는 웹 브라우저를 사용하여 ADFS 메타데이터를 다운로드할 수 있습니다.

PowerShell

PowerShell을 사용하여 AD FS 메타데이터를 내보내려면

1. AD FS 서버에서 PowerShell을 엽니다.
2. 다음 명령을 실행하여 메타데이터 파일을 다운로드합니다.

```
$metadataUrl = (Get-AdfsEndpoint | Where-Object {$_.Protocol -eq "Federation Meta  
Invoke-WebRequest -Uri $metadataUrl.AbsoluteUri -OutFile "C:-metadata.xml"  
Write-Host "ADFS metadata exported to C:-metadata.xml" -ForegroundColor Green
```

명령을 실행하면 메타데이터 파일이 C:-metadata.xml에 저장됩니다.

웹 브라우저

웹 브라우저를 사용하여 ADFS 메타데이터를 내보내려면

1. <https://<your-adfs-server>/FederationMetadata/2007-06/FederationMetadata.xml>으로 이동하여 "<your-adfs-server>"를 ADFS 서버의 호스트 이름으로 바꿉니다.
2. 메시지가 표시되면 메타데이터 XML 파일을 컴퓨터에 저장합니다.

Cisco IQ에서 구성

Cisco IQ에서 구성하려면

1. ad fs-metadata.xml을 워크스테이션에 전송합니다.
2. Cisco IQ에서 System Settings(시스템 설정) > System Configuration(시스템 컨피그레이션) > Identity Providers(ID 제공자)로 이동합니다.
3. IDP 인증서, 엔티티 ID 및 SSO URL을 자동으로 추출하려면 ADFS 메타데이터 파일을 업로드합니다.

4. 설정 저장.

 참고: AD FS에서 자동 토큰 서명 인증서 롤오버를 수행하는 경우 메타데이터 파일을 다시 내보내고 Cisco IQ에 업로드하여 지속적인 인증을 유지해야 합니다.

AD FS IDP 추가

1. Identity Providers(ID 제공자) 페이지에서 Add ID provider(ID 제공자 추가)를 클릭합니다.
2. ID 공급자 이름을 입력합니다.
3. 도메인(예: company.com)을 입력합니다.
4. (선택 사항) 필요한 경우 Enable single logout(단일 로그아웃 활성화) 토글 버튼을 켭니다.
5. IDP 애플리케이션에서 얻은 SAML 메타데이터 파일을 Upload IDP Metadata(IDP 메타데이터 업로드) 필드에 끌어 놓거나 업로드합니다.
6. 저장을 클릭합니다.

 참고: 역할 매핑이 완료될 때까지 상태가 "Incomplete(미완료)"로 표시 됩니다. 이는 정상적인 동작입니다.

역할 매핑 구성

역할 매핑을 구성하기 전에 매핑에 사용할 그룹을 AD에서 찾을 수 있는지 확인하십시오. AD에서 그룹을 찾으려면 다음 PowerShell 명령을 실행합니다.

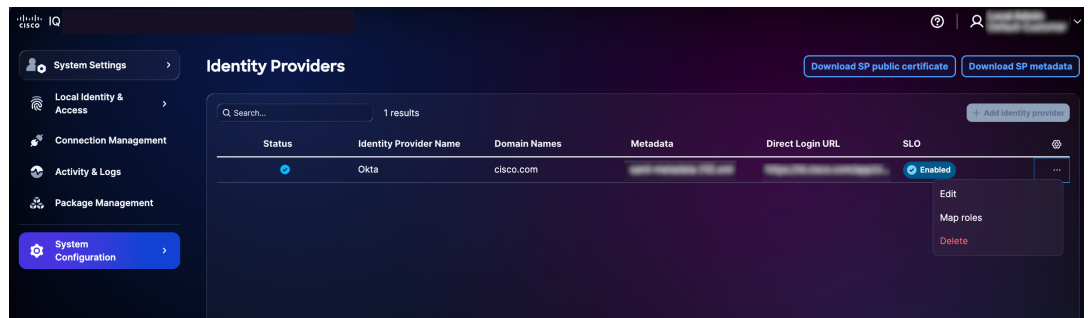
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = "(&(objectClass=group)(cn=Role - CXIQ*))"
$searcher.PropertiesToLoad.Add("distinguishedName") | Out-Null
$searcher.PropertiesToLoad.Add("cn") | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties["distinguishedname"] }
```

시스템은 LDAP(Lightweight Directory Access Protocol)를 통해 AD를 직접 쿼리하므로 추가 모듈이 필요하지 않습니다. 다음과 같이 그룹 정보가 전체 DN 형식으로 반환됩니다.

```
CN=Role - CXIQ Developers, OU=Groups, DC=dev, DC=example,
DC=com
CN=Role - CXIQ Viewers, OU=Groups, DC=dev, DC=example,
DC=com
```

필수 그룹이 나열되지 않으면 계정 관리자가 AD에서 생성해야 AD FS 역할 매핑을 완료할 수 있습니다.

역할 매핑을 구성하려면



역할 매핑

1. 추가된 IDP에서 More Options(추가 옵션) 아이콘 > Map Roles(역할 매핑)를 선택합니다. [사용자 역할 매핑] 페이지가 표시됩니다.

Cisco IQ Link_IDP

X

Map identity provider roles to system roles to assign permissions.

Map user roles

IDP role	System role
	General Account...
	General Account...
	Select option
	Select option
	Select option

+ Add identity provider role

Save

역할 매핑

- 선택한 시스템 역할에 대한 IDP 역할을 입력합니다. 지원되는 시스템 역할은 다음과 같습니다.
 - 일반 계정 관리자: 일반 계정 관리자는 제품의 모든 작업을 수행할 수 있는 모든 권한을 가집니다. IDP 역할(구문 분석된 이름)은 CXIQ Admins입니다.
 - 일반 계정 뷰어: 일반 계정 뷰어에는 읽기 전용 액세스 권한이 있습니다. IDP 역할(구문 분석된 이름)은 CXIQ Developers 및 CXIQ Viewer입니다.



참고: 구문 분석된 이름(예: CXIQ Developers)을 사용하고 전체 DN을 사용하지 않습니다.

3. 저장을 클릭합니다. 상태가 Success(성공)로 업데이트됩니다.

SChannel 클라이언트 인증서 테스트

클라이언트 인증서를 허용하도록 SChannel이 올바르게 구성되었는지 확인하려면 새 PowerShell 창을 열고 다음 명령을 실행합니다.

```
curl.exe -insecure `
-cert "CurrentUser\YOUR-USER-CERT-THUMBPRINT;" `
-v "https://

:49443/adfs/ls/"
```

예상되는 출력은 HTTP 응답(예: 리디렉션 또는 ADFS 페이지)입니다. TLS 핸드셰이크 오류가 발생하면 연결에 실패했습니다.

PKI 플로우에 대한 엔드 투 엔드 브라우저 테스트

PKI 플로우에 대한 엔드 투 엔드 브라우저 테스트를 시작하기 전에 사용자 인증서가 MacOS 키 체인에 설치되어 있는지 확인합니다(MacOS([Client Machine](#))에서 [사용자 인증서 가져오기 참조](#)). 테스트하려면

1. 애플리케이션 SAML 로그인 URL로 이동합니다. AD FS는 인증서 및 비밀번호 옵션을 제공합니다.
2. Certificate Authentication(인증서 인증)을 선택합니다. 브라우저에서 인증서를 묻는 프롬프트가 표시됩니다.
3. 인증서를 업로드합니다. AD FS는 사용자를 인증하고, SAML 응답으로 요청을 리디렉션하고, 새 세션을 설정합니다.

암호 흐름에 대한 엔드 투 엔드 브라우저 테스트

암호 흐름에 대한 엔드 투 엔드 브라우저 테스트를 시작하기 전에 다음을 수행합니다.

1. 애플리케이션 SAML 로그인 URL로 이동합니다. AD FS는 인증서 및 비밀번호 옵션을 제공합니다.

2. 비밀번호/양식 인증을 선택합니다.
3. 사용자 이름을 입력합니다.
4. 비밀번호 입력.
5. 성공적으로 로그인했는지 확인합니다.



참고: 두 흐름이 동시에 작동해야 합니다.

AD FS 문제 해결

다음 목록에는 ADFS 상태, 인증서 오류, SSO 로그인 실패 및 SLO 컨피그레이션과 관련된 문제를 신속하게 파악하고 해결하는 데 도움이 되는 일반적인 문제 및 가능한 솔루션이 설명되어 있습니다.

표 9: AD FS 문제

문제	증상/설명	원인/검사/해결 방법 및 수정
추출되지 않은 그룹	로그인 후 역할 없음	클레임 규칙 누락: AD FS 클레임 규칙 구성의 지침을 다시 실행합니다
암호 해독 실패	로그의 "어설션 해독 실패"	AD FS 인증서 컨피그레이션에 대한 컨피그레이션 확인 - 잘못된 ACS URL: 확인: https://your-fqdn/saml/acs - 쿠키 불일치: 올바른 도메인에 대한 브라우저 쿠키 확인
로그인 루프	인증 또는 로그인 루프에 고착	

문제 해결을 위한 진단 명령

AD FS 환경과 Cisco IQ 간의 성공적인 통합을 보장하려면 다음 진단 명령을 사용하십시오. 이러한 명령은 메타데이터 액세스 가능성, 인증서 컨피그레이션 및 엔드포인트 설정을 확인하는 데 도움이 됩니다.

- ADFS 메타데이터 액세스 가능성 확인: ADFS 페더레이션 메타데이터에 접근할 수 있으며 공개적으로 액세스할 수 있는지 확인합니다. 이는 초기 신뢰를 설정하기 위한 중요한 단계입니다.

```
curl -k https://
```

/FederationMetadata/2007-06/FederationMetadata.xml

- 암호화 인증서 검증: 올바른 암호화 인증서가 Cisco IQ Relying Party Trust와 연결되었는지 확인

```
Get-AdfsRelyingPartyTrust -Name "Cisco IQ - Production" |  
Select-Object EncryptionCertificate | Format-List
```

- SAML 엔드포인트 컨피그레이션 검토: Cisco IQ 트러스트에 대한 SAML 엔드포인트가 올바르게 구성되어 있고 인증 요청 및 어설션이 예상 URL로 라우팅되는지 확인합니다.

```
Get-AdfsRelyingPartyTrust -Name "Cisco IQ - Production" |  
Select-Object SamlEndpoints
```

SSO용 Microsoft Entra ID SAML 컨피그레이션

이 섹션에서는 Microsoft Entra ID(Entra ID)를 Cisco IQ용 SAML IDP로 구성하여 비밀번호 기반 및 PKI 또는 CBA(Certificate-Based Authentication)를 모두 지원하는 방법에 대해 설명합니다.

SSO를 위한 Entra ID SAML 구성 사전 요구 사항

- Centera ID 테넌트(예: "ciqtestdev.onmicrosoft.com")
- Cisco IQ에 대한 전역 관리자 또는 애플리케이션 관리자 역할 액세스
- Entra ID(클라우드)와 Cisco IQ 간의 연결
- 엔터프라이즈 CA가 설치되었거나 연결 가능(PKI에만 필요)
- 인터넷에서 연결할 수 있는 CRL(Certificate Revocation List) 배포 지점(PKI에만 필요)

표 10: Entra ID 서버 컨피그레이션

항목	설명	예
테넌트 ID	Entra ID 테넌트 식별자	37352d8f-0ebe-4762-8161-8775ffe897cb
Cisco IQ FQDN	배포 호스트 이름	<YOUR-CIQ-FQDN>

항목	설명	예
IDP 엔티티 ID	Entra ID 발급자 URL	https://sts.windows.net/<TENANT-ID>/
IDP SSO URL	SAML 로그인 끝점	https://login.microsoftonline.com/<TENANT-ID>/saml2
회사 도메인	사용자용 이메일 도메인	<사용자-도메인>

Entra ID SAML 애플리케이션 구성

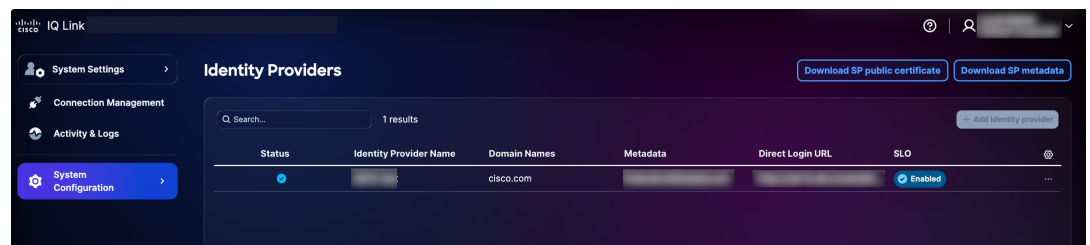
엔터프라이즈 응용 프로그램 생성

1. [Microsoft](#) Entra 관리 [센터](#)에 [로그인합니다](#).
2. Identity(ID) > Applications(애플리케이션) > Enterprise applications(엔터프라이즈 애플리케이션)로 이동합니다.
3. New application(새 애플리케이션) > Create your own application(고유한 애플리케이션 생성)을 클릭합니다.
4. 이름(예: "Cisco IQ")을 입력합니다.
5. 갤러리(갤러리가 아닌)에서 찾을 수 없는 다른 모든 응용 프로그램 통합을 선택합니다.
6. Create(생성)를 클릭합니다.

SAML Single Sign-On 구성

SAML SSO(Single Sign-On)를 구성하려면 SP 메타데이터 파일을 업로드해야 합니다. VA에서 다음 단계를 수행하여 얻을 수 있습니다.

1. System Settings(시스템 설정)에서 System Configuration(시스템 컨피그레이션) > Identity Providers(ID 제공자)를 선택합니다. ID 제공자 페이지가 표시됩니다.



다운로드 옵션

2. 다운로드할 SP 메타데이터 다운로드를 클릭합니다. 다운로드한 이 SP 메타데이터 파일은 SAML SSO(Single Sign-On) 구성을 완료하기 위해 업로드됩니다.

3. SP 메타데이터 파일을 업로드하려면 메타데이터 파일 업로드 버튼을 클릭합니다. 업로드 성공 후 SP 메타데이터 파일의 데이터가 SAML 기반 Single Sign-on 화면에 자동으로 입력됩니다.

Single Sign-On 설정을 구성하기 위해 이러한 세부 정보를 수동으로 입력하도록 선택할 수도 있습니다. SAML Single Sign-On을 수동으로 구성하려면

4. Enterprise Application(엔터프라이즈 애플리케이션)에서 Single Sign-On(단일 로그인)으로 이동하고 SAML을 선택합니다.
5. Basic SAML Configuration(기본 SAML 컨피그레이션) 섹션에서 Edit(편집)를 클릭하고 다음을 입력합니다.
 - 식별자(엔티티 ID): <YOUR-CIQ-FQDN>
 - 회신 URL(ACS URL): https://<YOUR-CIQ-FQDN>/saml/acs
 - 로그인 URL: https://<YOUR-CIQ-FQDN>/saml/login
 - 로그아웃 URL: https://<YOUR-CIQ-FQDN>/saml/logout
6. 저장을 클릭합니다.



참고: 엔티티 ID는 Cisco IQ가 SP 엔티티 ID로 사용하는 것과 정확히 일치해야 합니다. 일반적으로 구축의 FQDN입니다.

7. SAML 특성 및 클레임을 구성하려면 Attributes and Claims(특성 및 클레임) 섹션에서 Edit(수정)를 클릭합니다.
8. 다음 클레임을 구성합니다.

표 11: 필수 SAML 클레임

클레임	소스 특성	네임스페이스
고유 사용자 식별자 (NameID)	user.userprincipalname (기본값)	
이메일 주소	사용자.메일	http://schemas.xmlsoap.org/ws/2005/05/identity/
명사	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/
성	user.surname	http://schemas.xmlsoap.org/ws/2005/05/identity/
이름	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity/
그룹	user.assignedroles	(비어 있음 — 네임스페이스 지우기)



참고: 그룹 클레임의 경우

- user.groups가 아니라 user.assignedroles를 소스로 사용합니다.

- 네임스페이스 필드는 비어 있어야 합니다. 이렇게 하면 SAML assertion의 특성 이름이 전체 URI(Uniform Resource Identifier) 대신 단순히 그룹으로 설정됩니다
- 충돌이 발생하므로 user.groups와 중복된 그룹 클레임을 추가하지 마십시오

앱 역할 구성

애플리케이션 역할은 애플리케이션 등록(엔터프라이즈 애플리케이션 아님)에서 구성됩니다. 애플리케이션 역할을 구성하려면

1. Identity(ID) > Applications(애플리케이션) > App registrations(앱 등록)로 이동합니다.
2. 애플리케이션을 찾아 선택합니다.
3. App roles(앱 역할) > Create app role(앱 역할 생성)로 이동합니다.
4. 필요한 각 역할에 대해 다음을 구성합니다.
 - 표시 이름: 예: Cisco IQ Admins
 - 허용되는 멤버 유형: 사용자/그룹
 - 가치: 예: Cisco IQ Admins
 - 설명: 예를 들어, Cisco IQ Administrators
5. 적용을 클릭합니다.



참고: Cisco IQ 역할 매핑 요구 사항에 맞는 역할을 생성합니다(예: CXIQ Admins, CXIQ Developers 또는 CXIQ Viewer).

앱 역할은 다음과 같은 이유로 그룹 클레임 대신 사용됩니다.

- 클라우드 전용 테넌트는 P1 또는 P2 라이선스가 없으면 그룹 표시 이름을 보낼 수 없습니다.
- sAMAccountName은 온-프레미스 AD에서 동기화된 그룹에 대해서만 작동합니다
- 그룹 ID 원본에서 매핑하기 어려운 UUID(Universally Unique Identifier)를 보냅니다.
- 앱 역할은 Cisco IQ 역할 기대치에 맞는 정확한 문자열 값을 전송합니다.

앱 역할에 사용자 할당

사용자를 앱 역할에 할당하려면 다음을 수행합니다.

1. Enterprise Application > Users and groups로 돌아갑니다.
2. Add user/group(사용자/그룹 추가)을 클릭합니다.
3. 사용자를 선택하고 적절한 앱 역할을 할당합니다.
4. Assign(할당)을 클릭합니다. 역할 값은 SAML assertion groups 속성에서 읽을 수 있는 문자열로 표시됩니다.

IDP 메타데이터 및 인증서 다운로드

IDP 메타데이터 및 인증서를 다운로드하려면

1. Enterprise Application(엔터프라이즈 애플리케이션)에서 Single Sign-On(단일 로그인) > SAML Signing Certificate(SAML 서명 인증서)를 선택합니다.
2. 페더레이션 메타데이터 XML 다운로드(entra-id-metadata.xml로 저장)
또는
수동 인증서 입력을 위해 인증서 다운로드(Base64).
3. Set up(설정) 섹션에서 다음 값을 확인합니다.
 - 로그인 URL(IDP SSO URL)
 - Azure AD 식별자(IDP 엔터티 ID)
 - 로그아웃 URL(IDP SLO URL)



참고: Entra ID가 서명 인증서를 주기적으로 순환하므로, 중단 없는 SSO 서비스를 보장하려면 활성 인증서가 변경될 때마다 메타데이터를 다시 다운로드하고 VA에 업로드해야 합니다.

Entra ID IDP 추가



참고: SAML에 대한 APISIX 경로는 Cisco IQ에 IDP가 추가되면 자동으로 생성되므로 수동 경로 컨피그레이션이 필요하지 않습니다.

Entra ID IDP를 추가하려면

1. VA에 계정 관리자로 로그인합니다.
2. System Settings(시스템 설정) > System Configuration(시스템 컨피그레이션) > Identity Providers(ID 제공자)로 이동합니다.

3. Add ID provider(ID 제공자 추가)를 클릭합니다.
4. IDP의 이름(예: "Entra ID")을 입력합니다.
5. 도메인(예: "ciqtestdev.onmicrosoft.com" 또는 회사 도메인)을 입력합니다.
6. (선택 사항) 필요한 경우 Enable single logout(단일 로그아웃 활성화) 토글 버튼을 켭니다.
7. Entra ID에서 가져온 entra-id-metadata.xml 파일을 Upload IDP Metadata(IDP 메타데이터 업로드) 필드에 끌어서 놓거나 업로드합니다.
8. 저장을 클릭합니다.

 참고: 역할 매핑이 완료될 때까지 상태는 "Incomplete(미완료)"로 유지됩니다. 이는 정상적인 동작입니다.

역할 매핑 구성

역할 매핑을 구성하려면

1. 추가된 IDP에서 More Options(추가 옵션) 아이콘 > Map Roles(역할 매핑)를 선택합니다. [사용자 역할 매핑] 페이지가 표시됩니다.
2. 각 시스템 역할에 대한 IDP 역할을 입력합니다. 지원되는 시스템 역할은 다음과 같습니다.

표 12: 시스템 역할

시스템 역할	IDP 역할(앱 역할 값)	설명
general_account_administrator	CXIQ 관리자	모든 작업에 대한 전체 권한
general_account_viewer	CXIQ 개발자	읽기 전용 액세스
general_account_viewer	CXIQ 뷰어	읽기 전용 액세스

 참고: Entra ID에 구성된 것과 동일하게 애플리케이션 역할 값 문자열을 사용합니다(자세한 [내용은 애플리케이션 역할 구성 참조](#)).

4. 저장을 클릭합니다. 상태가 Success(성공)로 업데이트됩니다.

SAML 플로우 확인(비밀번호 인증)

SAML 플로우를 확인하려면

1. 익명 또는 전용 모드로 브라우저를 엽니다.

2. `https://<YOUR-CIQ-FQDN>/saml/login`으로 이동합니다.
3. Microsoft 로그인 페이지로 리디렉션되었는지 확인합니다.
4. 자격 증명으로 인증합니다(구성된 경우 MFA).
5. 인증 후 `/saml/acs`로 다시 리디렉션되고 Cisco IQ 애플리케이션이 표시되는지 확인합니다.
6. 다음 명령을 실행하여 그룹 추출을 확인합니다.

```
kubectl -ncxue logs deployment/apisix -since=5m | grep -E "authentication success"
```

예상 출력

사용자에 대한 SAML 2.0 호환 인증 성공: user@domain.com(전체 이름): 해당 없음 및 그룹 1개

추출된 그룹: CXIQ 관리자(원본: CXIQ 관리자)

추출된 총 그룹: 1

인증서 기반 인증 구성

이 섹션에서는 비밀번호와 함께 CBA를 추가하는 방법에 대해 설명합니다. 비밀번호 전용 인증만으로 충분할 경우 이 섹션을 건너뛸 수 있습니다.

CBA의 전제 조건

- Enterprise CA가 구성된 AD CS가 있는 Windows Server(예: "DEV-ADCS-CA")
- CA 서버의 PowerShell 관리자 액세스
- 인증서 UPN은 Entra ID userPrincipalName과 일치해야 합니다.
- CRL 배포 지점은 인터넷에서 액세스할 수 있어야 합니다.

AD CS에서 인증서 템플릿 생성

1. CA 서버에서 `certtmpl.msc`를 엽니다.
2. 사용자 템플릿을 복제하고 이름을 "EntraUserCert"로 지정합니다.
3. 템플릿을 구성합니다.
 - 일반: 표시 이름 EntraUserCert, 유효 기간 1-2년

- 요청 처리: 목적 = 서명 및 암호화
- 주체 이름: 요청에서 공급 선택
- 내선 번호: 애플리케이션 정책은 클라이언트 인증 (1.3.6.1.5.5.7.3.2)을 포함해야 합니다.
- Security: 인증된 사용자에게 읽기 및 등록 권한 부여

4. 다음 명령을 사용하여 템플릿을 게시합니다.

```
Add-CATemplate -Name "EntraUserCert" -Force
```

사용자 인증서 요청 및 발급

1. 다음 PowerShell 스크립트를 사용하여 INF(인증서 컨피그레이션) 파일 (예: C:-cert.inf)을 만듭니다.

```
@”
[Version]
Signature = “`$Windows NT`$”
[NewRequest]
Subject = “CN=

”

KeyLength = 2048
KeySpec = 1
KeyUsage = 0xa0
MachineKeySet = FALSE
ProviderName = “Microsoft RSA SChannel Cryptographic Provider”
RequestType = PKCS10
[RequestAttributes]
CertificateTemplate = EntraUserCert
[EnhancedKeyUsageExtension]
OID = 1.3.6.1.5.5.7.3.2
OID = 1.3.6.1.4.1.311.20.2.2
[Extensions]
2.5.29.17 = “{text}”
_continue_ = “upn=

”

_continue_ = “email=

”

”
"@ | Out-File -FilePath C:-cert.inf -Encoding ASCII
```

2. <USER-UPN>을 Entra ID UPN(예: user@ciqtestdev.onmicrosoft.com)으로 바꿉니다.
3. 인증서를 생성하려면 다음 명령을 실행합니다.

```
certreq -new C:-cert.inf C:-cert.csr
```

4. CA에 요청을 제출하려면 다음 명령을 실행합니다.

```
certreq -submit -config “
```

```
  \CA-NAME>” C:-cert.csr C:-cert.cer
```

5. CA에 인증서를 설치하려면 다음 명령을 실행합니다.

```
certreq -accept C:-cert.cer
```

인증서 내보내기

사용자 인증서를 PFX 파일(클라이언트용)로 내보내려면 다음 스크립트를 실행합니다.

```
$cert = Get-ChildItem Cert:| Where-Object { $_.Subject -like “*
```

```
  *” }
```

```
$password = ConvertTo-SecureString -String “
```

```
  ” -Force -AsPlainText
```

```
Export-PfxCertificate -Cert $cert -FilePath C:-cert.pfx -Password $password
```

CA 루트 인증서(Entra ID용)를 내보내려면 다음 스크립트를 실행합니다.

```
Get-ChildItem Cert:| Where-Object { $_.Subject -like "*"
    *"} |
Select-Object -First 1 | Export-Certificate -FilePath C:-root.cer -Type CERT
```

클라이언트 컴퓨터에서 사용자 인증서 가져오기(MacOS)

사용자 인증서(PFX)를 가져오려면 다음 명령을 실행합니다.

```
security import /path/to/entra-cert.pfx -k ~/Library/Keychains/login.keychain-db
"
```

CA 루트 인증서를 가져오려면 다음 명령을 실행합니다.

```
security import /path/to/ca-root.cer -k ~/Library/Keychains/login.keychain-db
```

CA 인증서를 Always Trust in Keychain Access로 설정하려면

1. 키 체인 액세스를 엽니다.
2. CA 인증서를 찾아 Get Info(정보 가져오기)를 클릭합니다.
3. Trust(신뢰)에서 "Always Trust(항상 신뢰)"로 설정합니다.

 참고: 가져온 다음 브라우저를 종료했다가 다시 열어 인증서를 인식합니다.

CA 루트 인증서를 Entra ID에 업로드

1. [Microsoft](#) Entra 관리 [센터](#)에 [로그인합니다](#).
2. Protection(보호) > Security(보안) > Certificate authorities(인증 기관)로 이동합니다.
3. Upload(업로드)를 클릭하고 ca-root.cer 파일을 선택합니다.
4. 루트 CA 인증서로 표시합니다.
5. CRL 배포 지점 URL을 입력합니다(공개적으로 연결 가능해야 함).

Entra ID 인증 방법에서 CBA 활성화

1. Protection > Authentication methods > Policies로 이동합니다.
2. 구성하려면 Certificate-based authentication(인증서 기반 인증)을 클릭합니다.
3. CBA를 활성화하고 대상 사용자 또는 그룹을 추가합니다.
4. Configure(구성)에서 보호 수준을 Single-factor authentication으로 설정합니다.

사용자 이름 바인딩 구성

CBA 컨피그레이션에서 Username binding(사용자 이름 바인딩) 탭으로 이동하여 다음 바인딩을 설정합니다.

- 인증서 필드: 사용자 이름
- 사용자 특성: 사용자 계정 이름

이렇게 하면 인증서의 SAN(Subject Alternative Name)에 있는 UPN이 Entra ID 사용자에게 매핑됩니다.

CBA 플로우 확인

1. 익명 또는 전용 모드로 브라우저를 엽니다.
2. <https://<YOUR-CIQ-FQDN>/saml/login>으로 이동합니다.
3. Microsoft 로그인 페이지에서 사용자의 이메일을 입력하고 다음을 클릭합니다.
4. Use a certificate or smart card(인증서 또는 스마트 카드 사용)(또는 자동 프롬프트 가능)를 선택합니다.
5. 브라우저에서 인증서 선택 프롬프트를 표시할 때 해당 사용자 인증서를 선택합니다.

6. Centera ID가 인증서를 검증하고 SAML 응답으로 리디렉션하며 세션을 생성하는지 확인합니다.

 참고: 올바른 클라이언트 인증서를 선택했는지 확인합니다. 잘못된 인증서(예: 다른 사용자의 인증서 또는 만료된 인증서)를 선택하면 인증이 실패합니다.

Entra ID 문제 해결

다음 목록에는 Entra ID SAML 컨피그레이션과 관련된 문제를 신속하게 파악하고 해결하는 데 도움이 되는 일반적인 문제 및 가능한 솔루션이 요약되어 있습니다.

표 13: 문제 해결

문제	원인	수정
유효하지 않은 SAML 응답 - 이메일 누락	SAML assertion에 NameID 또는 이메일 특성이 없습니다.	Entra ID 클레임 컨피그레이션을 확인합니다(자세한 내용은 SAML Single Sign-On 구성 참조). 사용자에게 메일 특성이 채워져 있는지 확인합니다.
추출된 총 그룹: 0	그룹이 구성되지 않았거나 잘못된 출처라고 주장함	user.assignedroles를 소스로 사용합니다. 사용자가 앱 역할에 할당되었는지 확인합니다(자세한 내용은 앱 역할에 사용자 할당 참조).
중복 그룹 클레임	user.groups 및 user.assignedroles 모두 활성화	user.groups 클레임을 제거합니다. user.assignedroles만 유지합니다.
UUID로 표시되는 그룹	소스 특성은 "Group ID"입니다.	앱 역할 접근 방식을 사용합니다(자세한 내용은 앱 역할 구성 참조).
특성 이름에 긴 URI 표시	네임스페이스 필드가 비어 있지 않습니다.	그룹 클레임 설정에서 Namespace 필드를 지웁니다.
잘못된 SAML 서명	IdP 인증서가 회전되거나 일치하지 않음	Entra ID에서 메타데이터를 다시 다운로드하고 Cisco IQ에 다시 업로드합니다.
ADSTS500191	인터넷에서 CRL에 연결할 수 없음	공개적으로 액세스 가능한 URL에 CRL을 게시하거나 자체 서명된 CA 접근 방식을 사용합니다(자세한 내용은 CRL 연결 문제 해결 방법 참조).
인증서를 묻는 메시지	인증서가 키 체인	MacOS 키 체인 액세스에서 사용

문제	원인	수정
가 표시되지 않음	에 없거나, CA가 클라이언트에서 신뢰되지 않거나, CBA가 활성화되지 않음	자 인증서를 가져왔는지 확인합니다(자세한 내용은 MacOS(클라이언트 컴퓨터에서 사용자 인증서 가져오기) 참조), CBA가 필요한 설정으로 Entra ID에서 활성화되었는지 확인합니다(자세한 내용은 Entra ID 인증 방법 에서 CBA 활성화 참조), Chrome이 다시 시작되어 변경 사항이 적용되었는지 확인합니다. 플러그인 컨피그레이션에서 clock_skew_seconds를 늘립니다(기본값은 300; 실습에 30000 사용).
SAML 어설션이 만료되었습니다.	시스템 간 클럭 스큐	
가상 어플라이언스의 상태 "미완료"	역할 매핑이 아직 구성되지 않았습니다.	역할 매핑을 완료합니다(자세한 내용은 역할 매핑 구성 참조).

연결 가능성 문제에 대한 CRL 해결 방법

인터넷에서 CA의 CRL 배포 지점에 연결할 수 없는 경우(실험실 설정에서 흔히 사용됨) CRL 요구 사항 없이 자체 서명된 CA를 사용합니다.

```
powershell
# Create self-signed CA
$rootCA = New-SelfSignedCertificate `
-Subject "CN=CIQ-Test-CA" `
-CertStoreLocation "Cert:" `
-KeyUsage CertSign, CRLSign `
-KeyLength 2048 `
-NotAfter (Get-Date).AddYears(5) `
-TextExtension @"(2.5.29.19={text}ca=TRUE)"
# Create user cert signed by the CA
$userCert = New-SelfSignedCertificate `
-Subject "CN=

", `
-CertStoreLocation "Cert:" `
-Signer $rootCA `
-KeyUsage DigitalSignature `
-KeyLength 2048 `
-NotAfter (Get-Date).AddYears(2) `
-TextExtension @(
"2.5.29.37={text}1.3.6.1.5.5.7.3.2",
"2.5.29.17={text}upn="
```

&email=

”

)

루트 CA 인증서만 Entra ID에 업로드합니다. CDP(Cisco Discovery Protocol) 없이 자체 서명되므로 Entra ID는 CRL 검증을 시도하지 않습니다.

설정 체크리스트 완료

이 섹션에서는 Microsoft Entra ID SAML 애플리케이션 및 선택적 CBA로 VA를 구성하기 위한 전체 설정 체크리스트에 대해 설명합니다.

Entra ID SAML 애플리케이션 설정

- Entra ID에서 엔터프라이즈 애플리케이션(비갤러리) 생성
- 수동으로 SP 메타데이터를 입력하여 기본 SAML 구성 구성
- 특성 및 클레임 구성(이메일, 이름, user.assignedroles가 있는 그룹 포함)
- 앱 등록에서 앱 역할 만들기
- 앱 역할에 사용자 할당
- 페더레이션 메타데이터 XML 다운로드

Cisco IQ 컨피그레이션

- Entra ID 메타데이터를 업로드하여 Cisco IQ에 IDP 추가
- 앱 역할 값을 Cisco IQ 시스템 역할에 매핑하도록 역할 매핑 구성
- 비밀번호 기반 로그인 이 엔드 투 엔드로 작동하는지 확인
- 로그에서 그룹이 올바르게 추출되었는지 확인합니다.

인증서 기반 인증(선택 사항)

- 클라이언트 인증 ECU를 사용하여 AD CS에 인증서 템플릿 생성

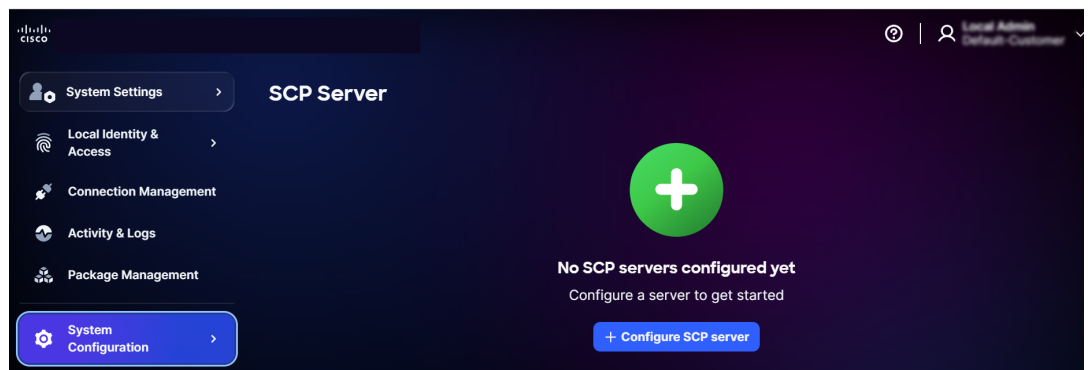
- Entra ID 사용자와 일치하는 UPN으로 사용자 인증서 발급
- 사용자 인증서를 PFX 파일로 내보내고 클라이언트 컴퓨터에 설치합니다
- 클라이언트 머신의 CA 인증서 신뢰
- Protection(보호) > Certificate authorities(인증 기관)에서 CA 루트 인증서를 Entra ID에 업로드합니다.
- 인증 방법에서 CBA 활성화
- 사용자 이름 바인딩 구성(PrincipalName 및 userPrincipalName)
- CBA 로그인이 엔드 투 엔드로 작동하는지 확인

SCP 서버 추가

SCP 서버는 Cisco IQ 설치를 추가, 업그레이드 또는 수정하는 데 필수적인 업그레이드 파일을 가져오기 위한 필수 구성 요소입니다.

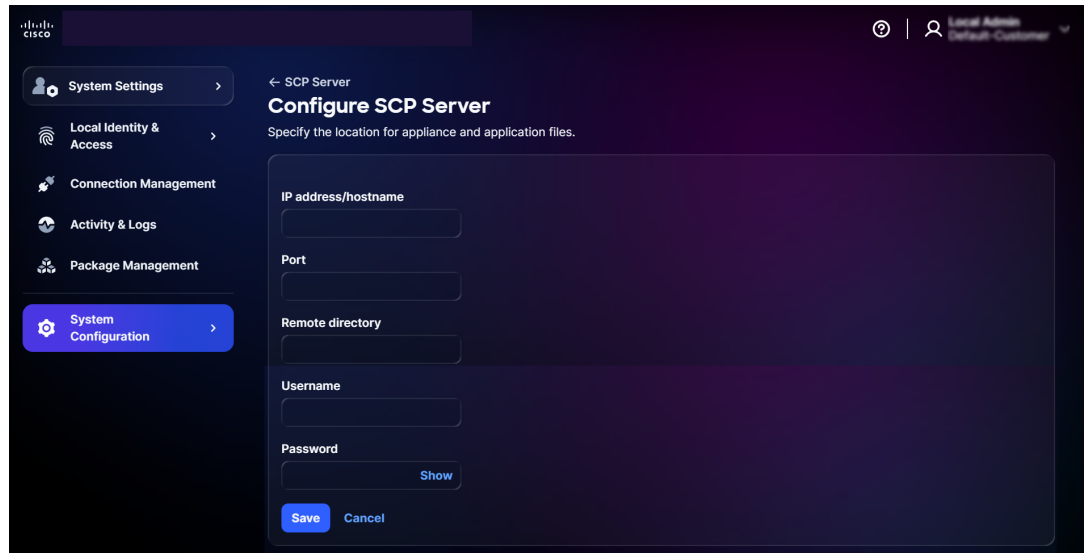
SCP 서버를 추가하려면

1. System Settings(시스템 설정)에서 System Configuration(시스템 컨피그레이션) > SCP Server(SCP 서버)를 선택합니다. SCP Server(SCP 서버) 페이지가 표시됩니다.



SCP 서버 홈 페이지

2. Configure SCP server를 클릭합니다. Configure SCP Server(SCP 서버 구성) 페이지가 표시됩니다.



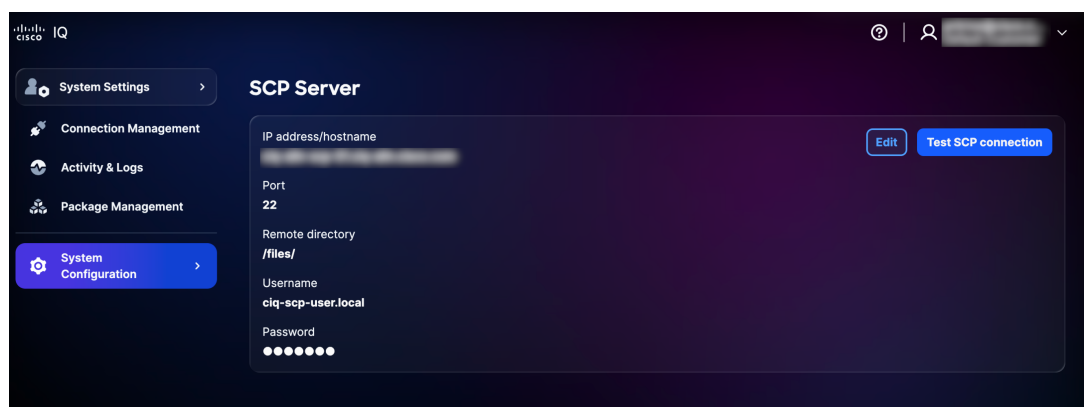
SCP 서버 구성

3. IP 주소/호스트 이름을 입력합니다.
4. 포트를 입력합니다.
5. 원격 디렉토리를 입력합니다.
6. 사용자 이름을 입력합니다.
7. 비밀번호를 입력합니다.
8. 저장을 클릭합니다. 확인 메시지가 표시됩니다.

기존 SCP 서버 수정

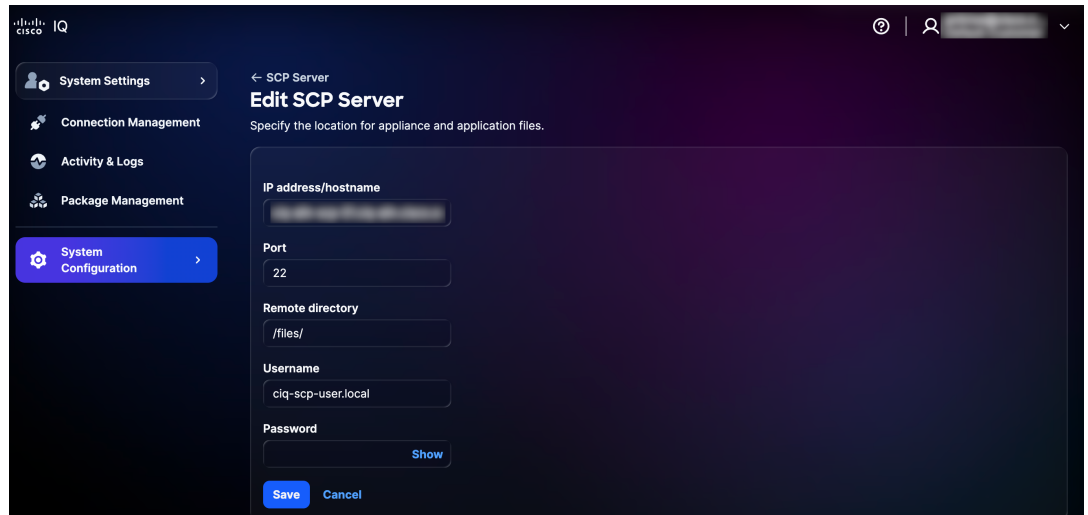
기존 SCP 서버를 수정하려면

1. SCP 서버 페이지로 이동합니다.



추가된 SCP 서버

2. 원하는 기존 SCP 서버의 Edit를 클릭합니다.



SCP 서버 편집

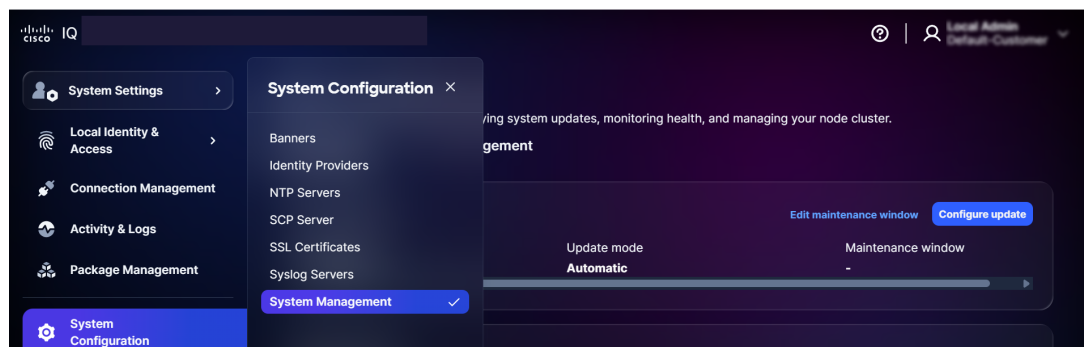
3. 필요에 따라 세부 정보를 수정합니다.
4. 저장을 클릭합니다.

시스템 관리

UI를 통해 최신 Cisco IQ VA 버전으로 업그레이드할 수 있습니다. Cisco IQ Data Connectors(Cisco IQ 데이터 커넥터) 페이지에서 확인할 수도 있습니다.

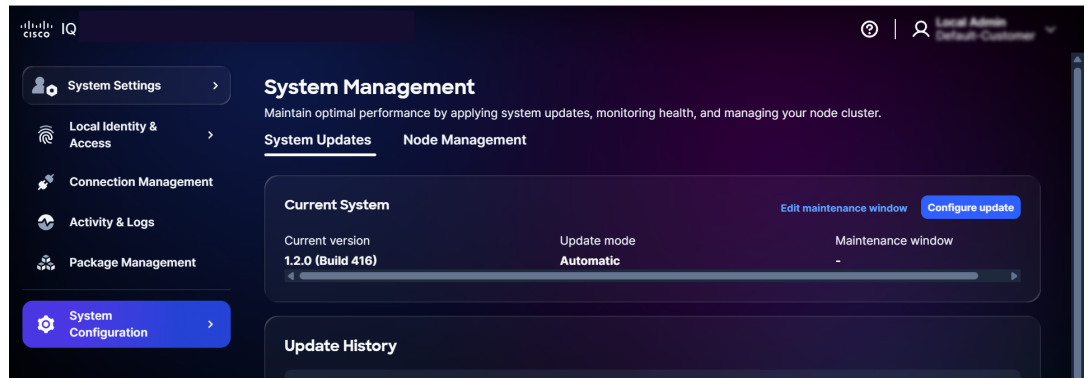
시스템 업데이트 다시 예약

시스템 갱신 스케줄을 조정하려면



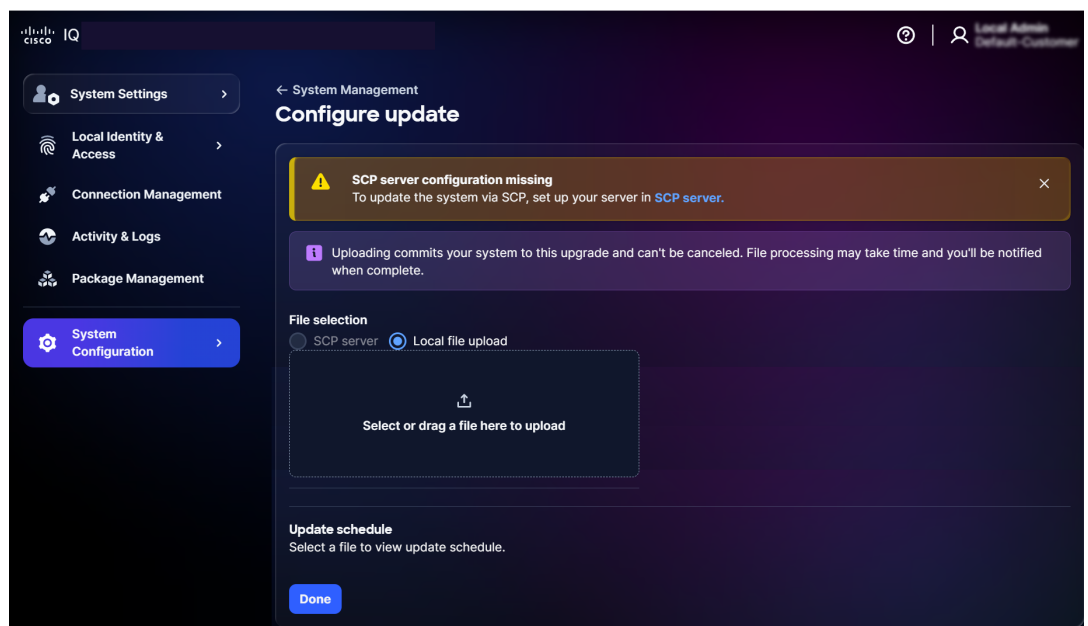
시스템 관리

1. System Settings(시스템 설정)에서 System Configuration(시스템 컨피그레이션) > System Management(시스템 관리)를 선택합니다. System Management 페이지가 표시됩니다. 이 페이지에는 현재 실행 중인 시스템 버전이 표시됩니다. 구성된 업데이트가 없으면 Update History 섹션이 비어 있습니다.



시스템 업그레이드

2. 업데이트 구성을 클릭합니다. Configure update 페이지가 표시됩니다.



업그레이드 구성

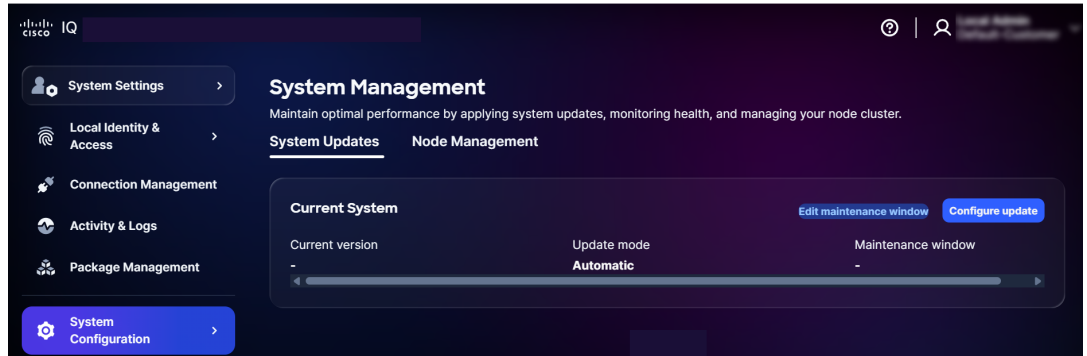
3. 다른 시간을 예약하려면 업데이트 일정을 선택합니다.

4. 파일 업로드가 완료될 때까지 기다립니다. 기간은 번들 크기 및 네트워크 속도에 따라 다릅니다.

Update Status(업데이트 상태) 열 아래에 표시된 확인 표시 아이콘을 확인하여 업데이트에 성공했음을 확인합니다.

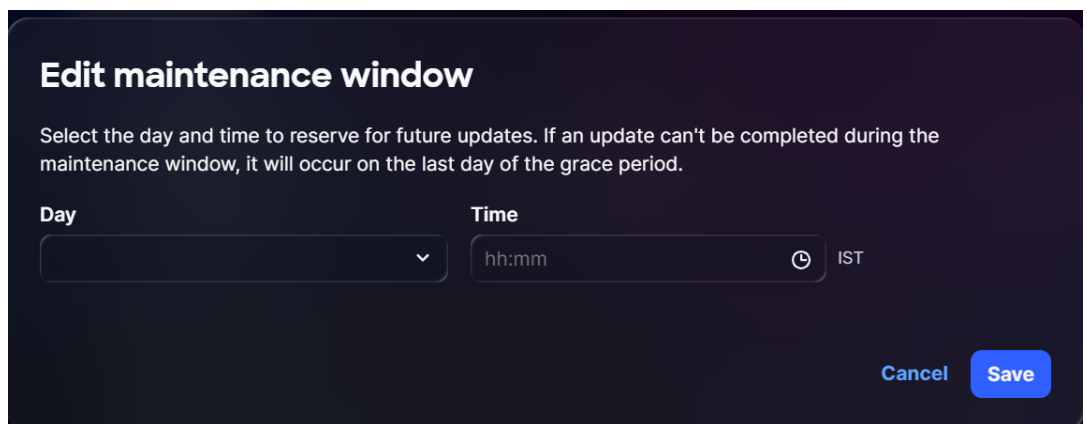
시스템 업그레이드 일정 수정

시스템 업그레이드에 대한 사용자 지정 일정을 생성할 수 있습니다. 사용자 지정 일정이 구성된 경우 최대 유예 기간 내에 유지되면 사용자 정의 날짜에 업그레이드가 수행됩니다. 시스템 업그레이드 일정을 생성하려면



유지 관리 편집

1. System Management(시스템 관리) 페이지의 Current System(현재 시스템) 섹션에서 Edit maintenance(유지 관리 편집) 창을 클릭합니다.



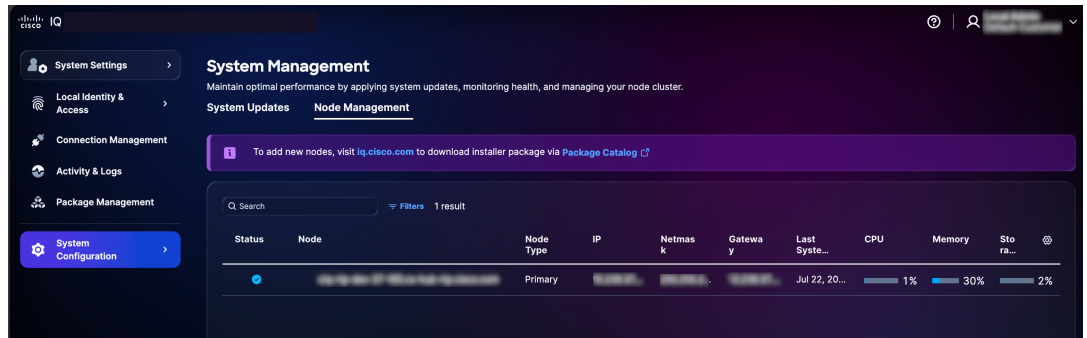
유지 관리 창 편집

2. Day and Time 드롭다운 목록에서 옵션을 선택합니다.
3. 저장을 누릅니다. 유지 관리 창이 성공적으로 예약되었습니다. 업데이트는 표시된 일정에 따라 트리거됩니다.

 참고: 업그레이드 일정이 구성되지 않은 경우, 시스템은 기본적으로 비재부팅 업그레이드의 경우 2주, 재부팅이 필요한 업그레이드의 경우 4주의 유예 기간을 설정합니다. 이러한 유예 기간이 지나면 수동으로 업데이트를 수행해야 합니다. 업그레이드가 실패할 경우 시스템은 최대 2회의 자동 재시도를 수행합니다. 세 번째 시도는 예약되었지만 수동으로 시작해야 합니다.

노드 관리

1. System Configuration(시스템 컨피그레이션) > System Management(시스템 관리) > Node Management(노드 관리)로 이동하여 클러스터의 노드를 보고 관리합니다.



노드 관리

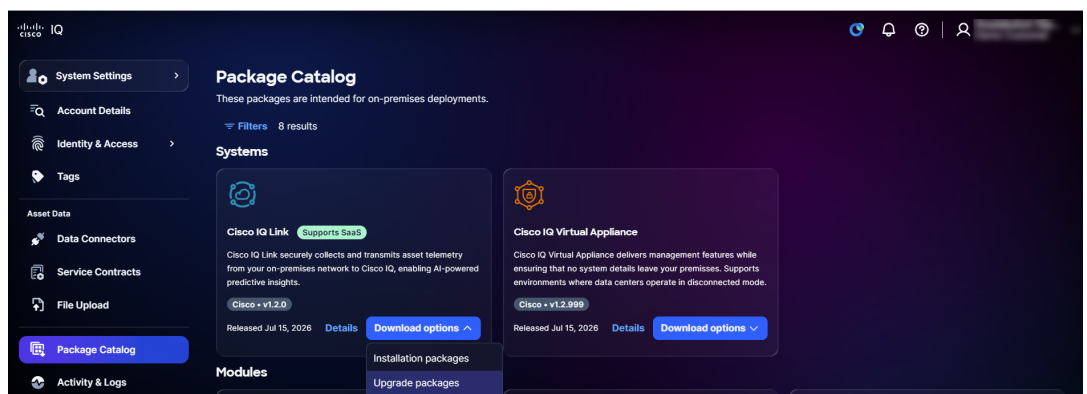
2. 노드 목록에는 각 노드의 상태, 호스트 이름, 노드 유형, IP 주소, 넷마스크, 게이트웨이 및 마지막 동기화 시간이 표시됩니다.

 참고: 상태 열의 파란색 확인 표시는 노드가 활성 상태임을 나타냅니다.

수동으로 시스템 업그레이드

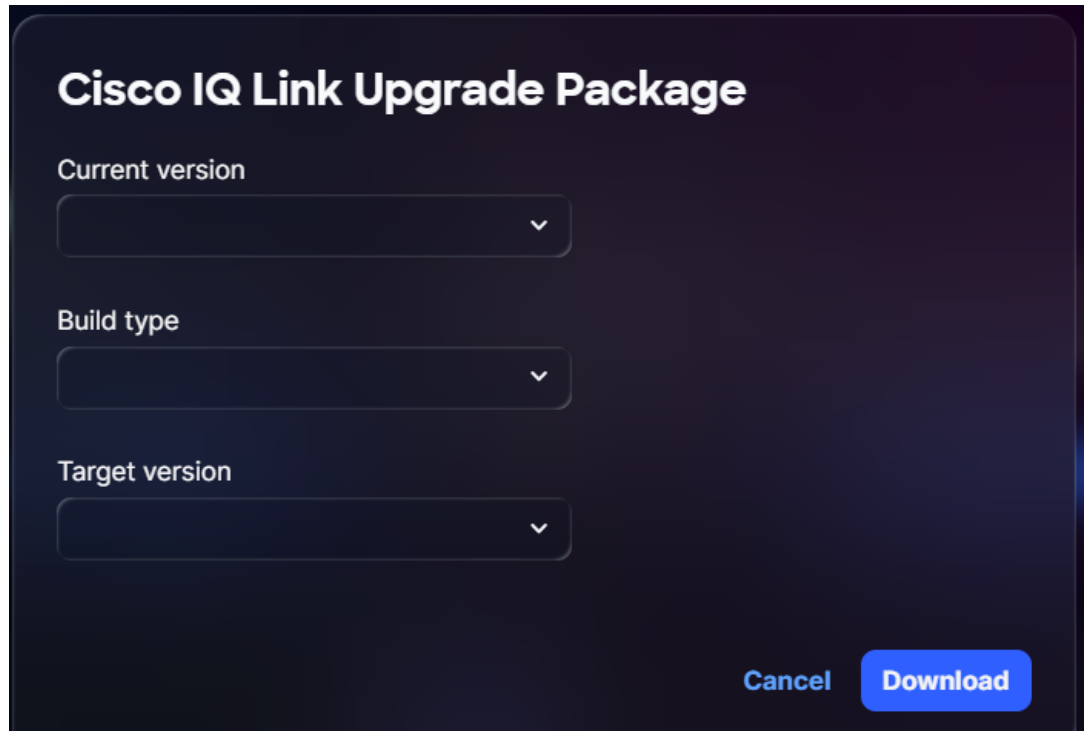
Cisco IQ SaaS에서 자동 배포를 사용할 수 없거나 지연되는 시나리오에서는 Cisco IQ SaaS에서 직접 업그레이드 번들을 다운로드하여 수동으로 시스템 업그레이드를 수행할 수 있습니다. 시스템을 수동으로 업그레이드하려면

1. [Cisco IQ](#) SaaS에 [로그인합니다](#).
2. Home > System Settings > Package Catalog로 이동합니다.



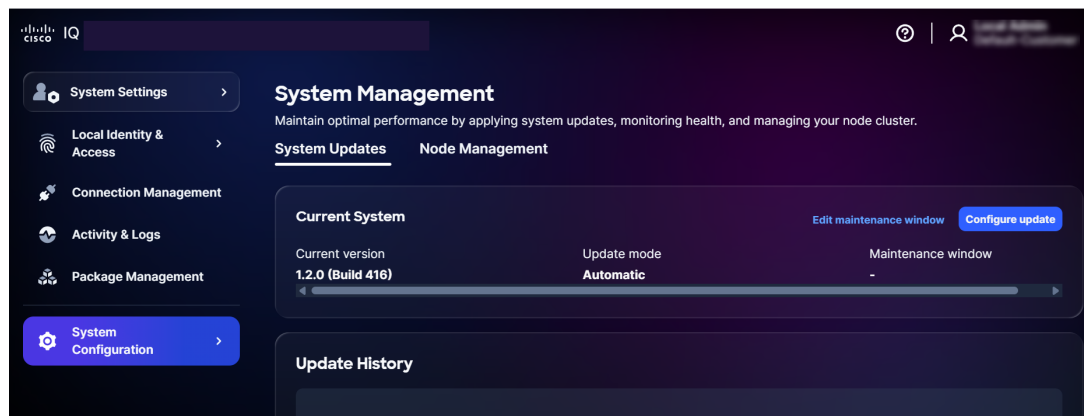
소프트웨어 카탈로그

3. Cisco IQ Virtual Appliance 카드에서 Download options(다운로드 옵션) > Upgrade packages(업그레이드 패키지)를 클릭합니다.



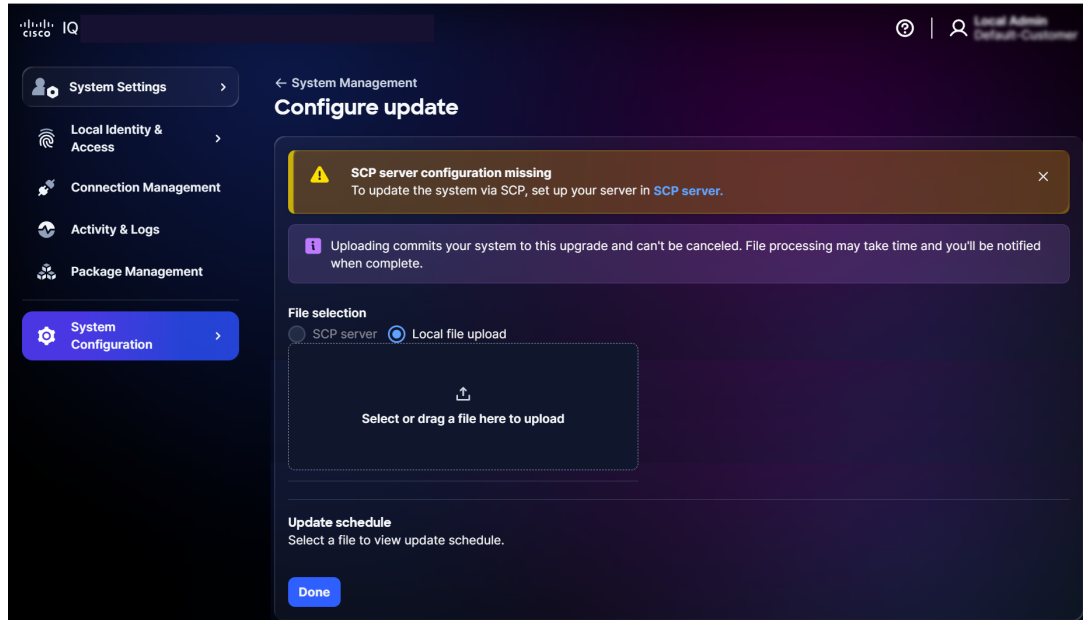
패키지 업그레이드

4. 드롭다운 목록에서 현재 버전을 선택합니다.
5. 드롭다운 목록에서 빌드 유형을 선택합니다.
6. 드롭다운 목록에서 대상 버전을 선택합니다.
7. Download(다운로드)를 클릭합니다. 업그레이드 번들이 다운로드됩니다.
8. Cisco IQ VA로 이동합니다.
9. System Settings(시스템 설정)에서 System Configuration(시스템 컨피그레이션) > System Management(시스템 관리)를 선택합니다.



업데이트 구성

10. 업데이트 구성을 클릭합니다.



로컬 파일 업로드

11. Local file upload(로컬 파일 업로드) 라디오 버튼을 클릭합니다.
12. 다운로드한 업그레이드 번들 파일을 선택하거나 업로드 필드로 끌어옵니다.
13. 파일 업로드가 완료될 때까지 기다립니다. 기간은 번들 크기 및 네트워크 속도에 따라 다릅니다.

SSL 인증서 컨피그레이션

기본 자체 서명 인증서는 Cisco IQ에 사전 설치되어 활성화되지만, 선택적으로 사용자 지정 SSL 인증서를 업로드할 수 있습니다. 사용자 지정 SSL 인증서가 활성화되면 HTTPS 연결에 사용됩니다. 인증서가 비활성화되거나 삭제되면 시스템은 자동으로 기본 인증서로 돌아갑니다. 기본 SSL 인증서는 편집하거나 삭제할 수 없습니다.

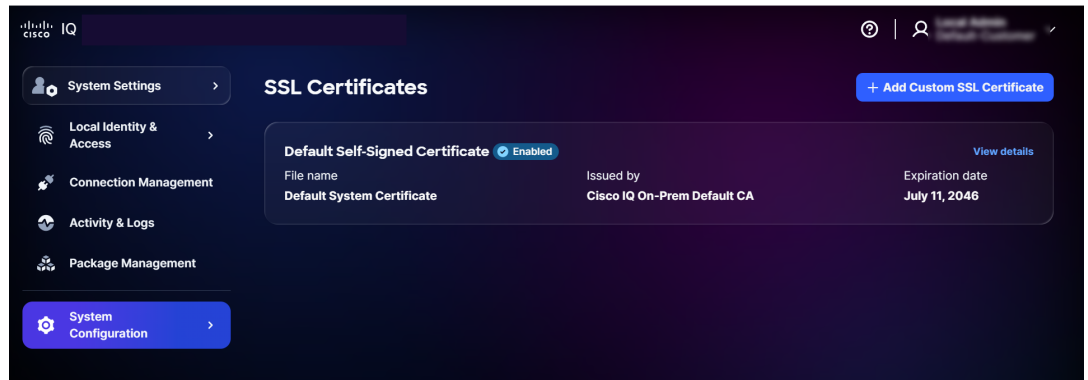
 참고: 인증서의 유효 기간이 90일 이상 남아 있어야 합니다. 인증서가 만료될 때까지 남은 기간이 90일 미만일 경우 "만료 임박"으로 간주됩니다. SSL 인증서를 추가, 편집 또는 삭제한 후에는 Okta IDP 또는 ADFS IDP에 대한 SLO 컨피그레이션 완료에 설명된 대로 새 SSL [인증서](#)를 업로드해야 합니다.

사용자 지정 SSL 인증서 추가

사용자 지정 SSL 인증서를 추가하려면

1. System Settings(시스템 설정)에서 System Configuration(시스템 컨피그레이션) > SSL Certificates(SSL 인증서)를 선택합니다. 시스템의 모

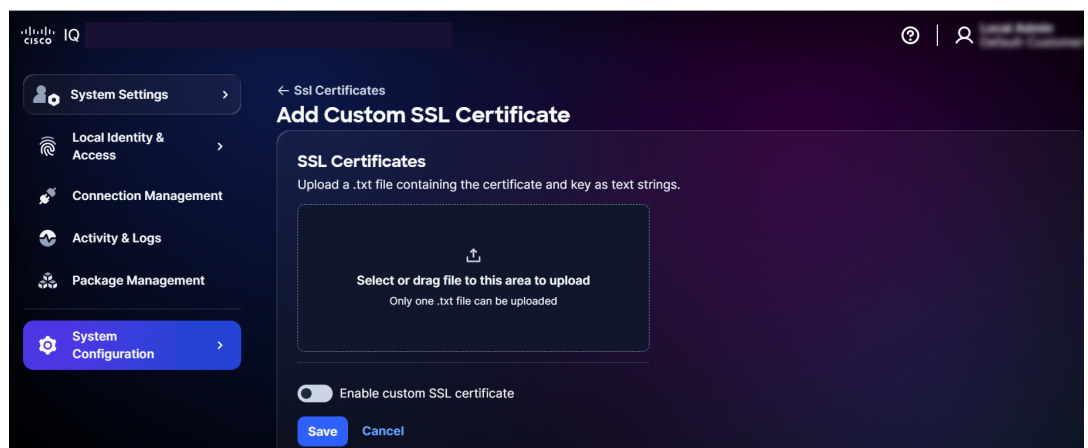
든 SSL 인증서를 나열하는 SSL Certificates 페이지가 표시됩니다.



SSL 인증서 추가

2. Add Custom SSL Certificate를 클릭합니다.

 참고: Privacy-Enhanced Mail 인코딩 인증서 및 키가 모두 포함된 .txt 파일을 텍스트 문자열로 업로드합니다. .txt 파일은 한 번에 하나만 업로드할 수 있습니다. 파일에는 인증서와 개인 키가 모두 포함되어야 합니다.



SSL 인증서 업로드

3. SSL Certificate(SSL 인증서) 섹션에서 사용자 지정 SSL 인증서를 끌어
서 놓거나 업로드합니다.

4. Enable custom SSL certificate(맞춤형 SSL 인증서 활성화) 토글 버튼
을 켭니다.

Enable Certificate?

Enabling custom SSL certificate will disable the default self-signed certificate.

Cancel

Enable certificate

인증서 사용

 참고: 인증서를 즉시 활성화하지 않고 업로드하려면 토글을 끄지 않습니다.

5. Enable certificate를 클릭합니다.

6. 저장을 클릭합니다.

맞춤형 SSL 인증서가 활성화되고 활성화됩니다. 기본 시스템 인증서는 자동으로 비활성화됩니다.

사용자 지정 SSL 인증서 수정

사용자 지정 SSL 인증서를 수정하여 새 인증서를 업로드하거나 현재 활성화된 인증서를 비활성화할 수 있습니다. 편집하려면 다음을 수행합니다.

1. 원하는 사용자 지정 SSL 인증서로 이동합니다.
2. 추가 옵션 아이콘 > 편집을 선택합니다. Edit SSL Certificate 페이지가 표시됩니다.
3. 필요에 따라 인증서 세부사항을 수정합니다.
4. 저장을 클릭합니다.

사용자 지정 SSL 인증서 삭제

경고: 사용자 지정 SSL 인증서는 언제든지 삭제할 수 있지만 취소할 수 없는 작업입니다. 삭제 후 언제든지 새 사용자 지정 인증서를 업로드할 수 있습니다.

삭제하려면

1. 원하는 개인 SSL 인증서로 이동합니다.
2. 추가 옵션 아이콘 > 삭제를 선택합니다.

3. Delete Certificate(인증서 삭제)를 클릭합니다. 사용자 지정 인증서가 삭제되고 기본 인증서가 자동으로 다시 활성화됩니다.

Syslog 서버 컨피그레이션

계정 관리자 역할의 사용자는 외부 syslog 서버가 시스템 로그를 내보내도록 구성할 수 있습니다. 최대 2개의 syslog 서버를 구성할 수 있습니다.

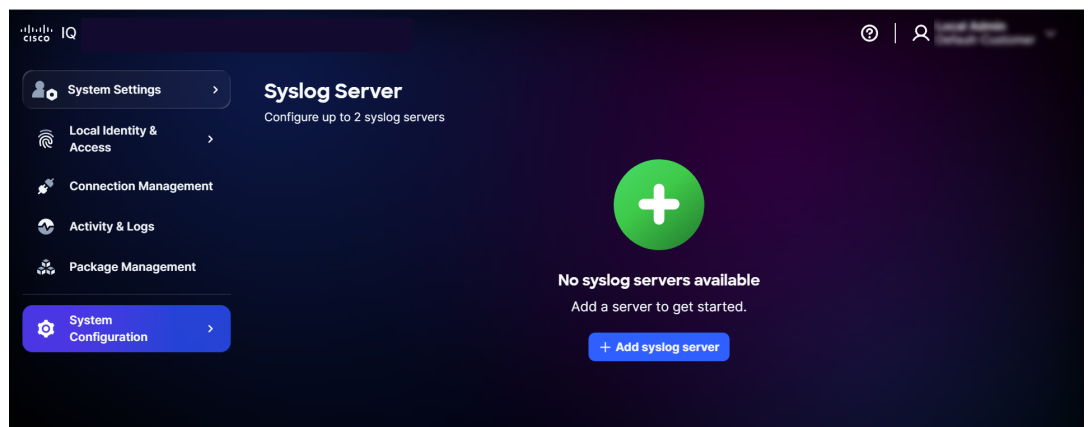


참고: Syslog 서버는 FQDN(Fully Qualified Domain Name)이 아니라 IP 주소로 지정해야 합니다.

Syslog 서버 추가

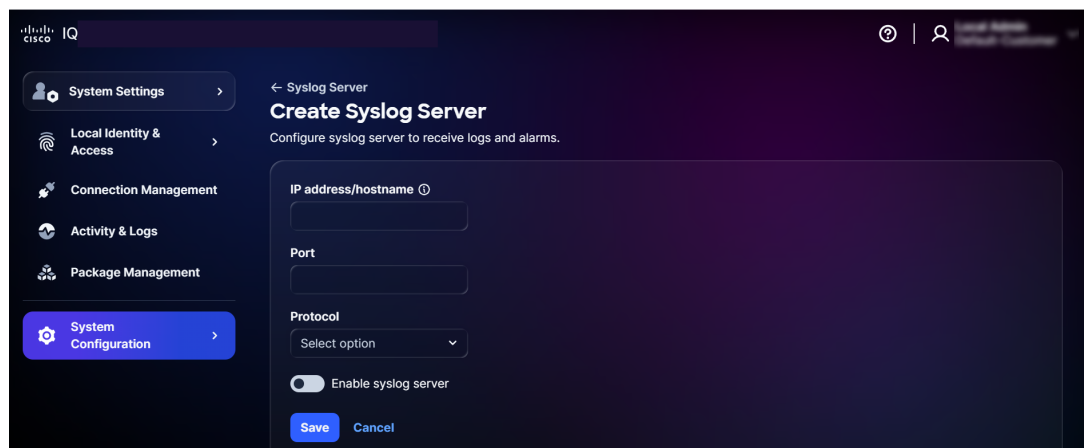
syslog 서버를 추가하려면

1. System Settings(시스템 설정)에서 System Configuration(시스템 컨피그레이션) > Syslog Server(Syslog 서버)를 선택합니다. Syslog Server 페이지가 표시됩니다.



Syslog 서버 추가

2. Add syslog server(syslog 서버 추가)를 클릭합니다. Create Syslog Server(Syslog 서버 생성) 페이지가 표시됩니다.



Syslog 서버 생성

3. IP 주소/호스트 이름을 입력합니다.
4. Port를 입력합니다.
5. Protocol 드롭다운 목록에서 해당 프로토콜(예: UDP, TCP)을 선택합니다.
6. Enable syslog server 토글 버튼을 켭니다.
7. 저장을 클릭합니다. 확인 메시지가 표시되고 새로 추가된 syslog 서버가 Syslog 서버 홈 페이지에 표시됩니다.

구성된 Syslog 서버 수정

구성된 syslog 서버를 수정하려면

1. 원하는 syslog 서버로 이동합니다.
2. 추가 옵션 아이콘 > 편집을 선택합니다. Edit Syslog Server(Syslog 서버 수정) 페이지가 표시됩니다.
3. 필요에 따라 세부 정보를 편집하거나 Enable syslog server 토글을 끕니다.
4. 저장을 클릭합니다.

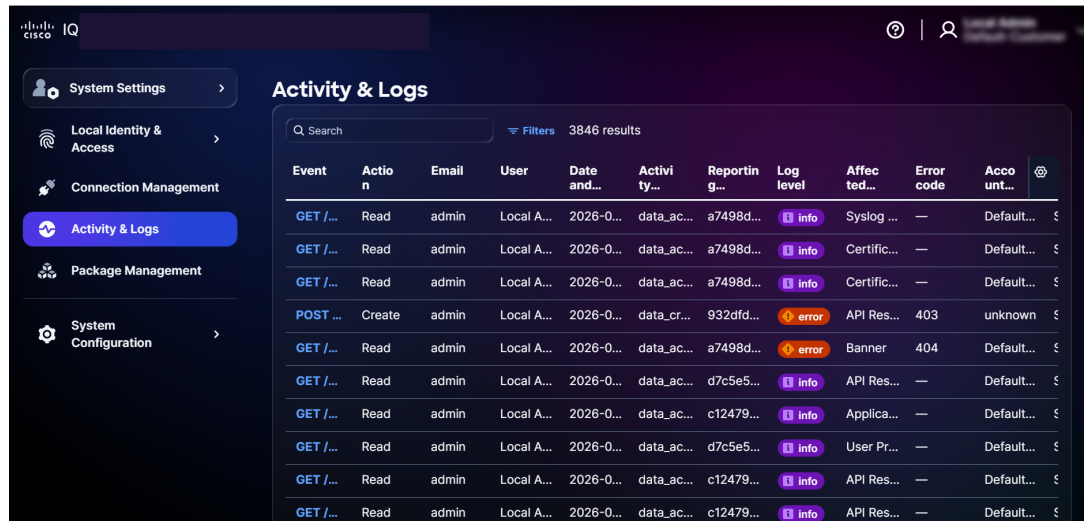
구성된 Syslog 서버 삭제

구성된 syslog 서버를 삭제하려면

1. 원하는 syslog 서버로 이동합니다.
2. 추가 옵션 아이콘 > 삭제를 선택합니다. 확인 메시지가 표시됩니다.
3. Delete syslog server를 클릭합니다.

활동 및 로그

활동 및 로그는 Cisco IQ의 사용자 작업 및 변경 사항에 대한 자세한 기록을 제공하여 계정 관리자가 사용자 활동을 추적하고 투명성을 유지할 수 있도록 합니다.



활동 및 로그

활동 및 로그를 보려면 System Settings(시스템 설정) 메뉴에서 Activity & Logs(활동 및 로그)를 선택합니다.

작업 및 로그:

- 게이트웨이 레벨에서 모든 API 작업 기록
- 필터, 페이지 매김 및 검색 기능을 지원하여 정보를 쉽게 찾고 관리할 수 있습니다.

다음 필터 옵션을 사용할 수 있습니다.

- 최종 로그 날짜: 로그를 특정 시간 범위로 필터링
- 로그 수준: 심각도(예: 오류, 경고 및 정보)별로 로그를 필터링합니다.
- 활동 유형: 시스템 활동 유형별로 로그를 필터링합니다.
- 오류 코드: 특정 오류 코드에 대한 필터

배너

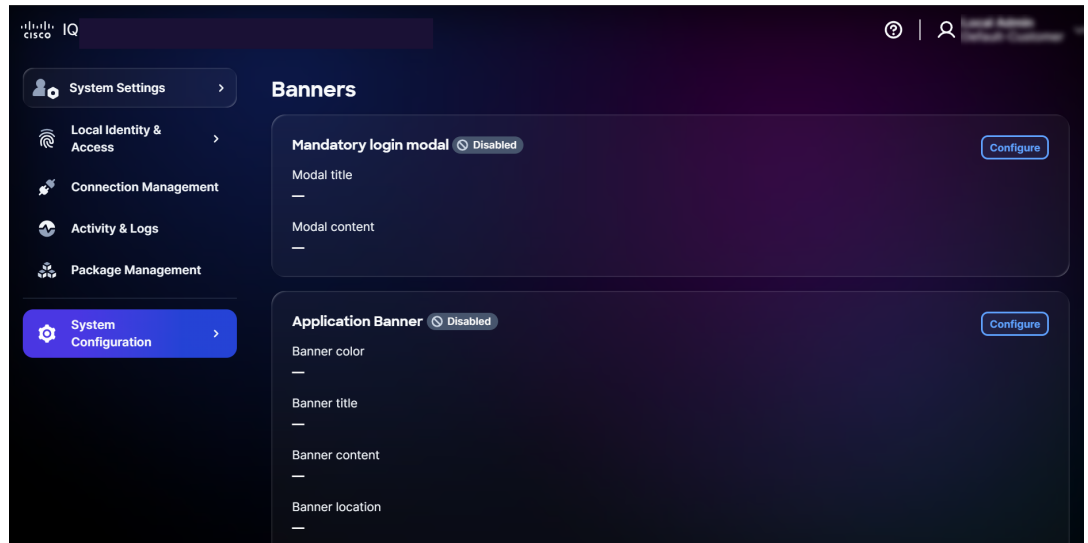
계정 관리자는 보안 및 규정 준수 표준을 충족하도록 시스템 전체 배너를 구성할 수 있습니다.

- 필수 로그인 모드: 로그인 화면으로 진행하기 전에 필수 배너를 승인해야 합니다.
- 애플리케이션 배너: 이러한 배너는 인증에 성공한 후 애플리케이션 전체에 표시되는 사용자 지정 배너입니다.

필수 로그인 모달 배너 구성

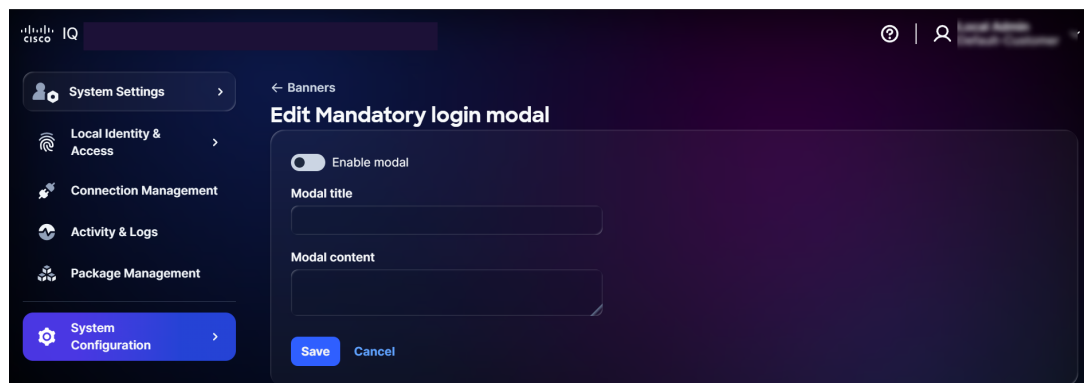
필수 배너를 구성하려면

1. System Settings(시스템 설정)에서 System Configuration(시스템 컨피그레이션) > Banners(배너)를 선택합니다. Banners(배너) 페이지가 표시됩니다.



필수 배너 구성

2. 필수 로그인 모드에서 Configure를 클릭합니다. 필수 로그인 모달 편집 페이지가 표시됩니다.



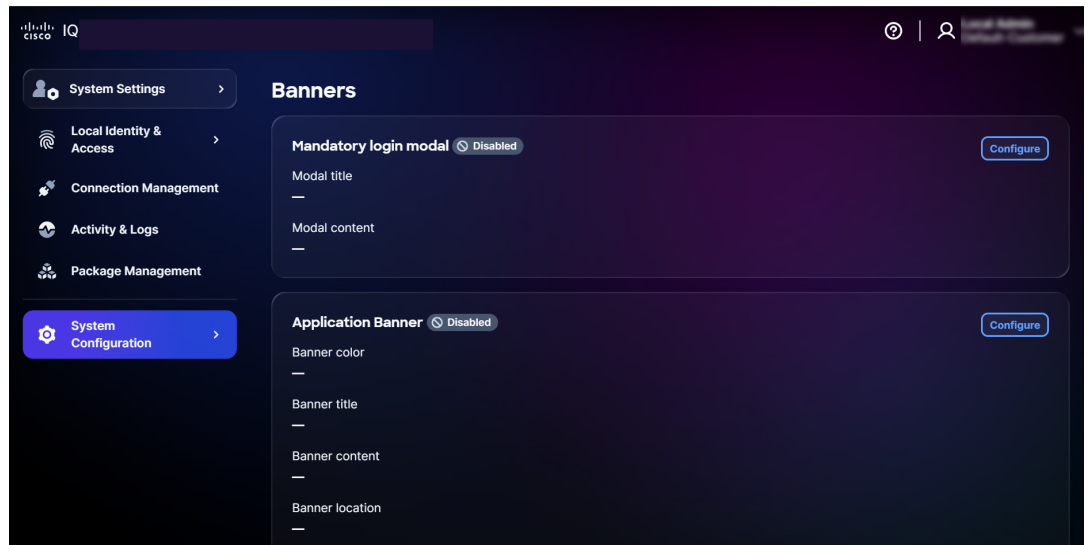
필수 로그인 모달 배너 편집

3. 배너를 활성화 또는 비활성화하려면 토글을 클릭합니다.
4. 모달 제목을 입력합니다.
5. 모달 내용을 입력합니다.
6. 저장을 클릭합니다. 필수 로그인 모달이 저장됩니다.

애플리케이션 배너 구성

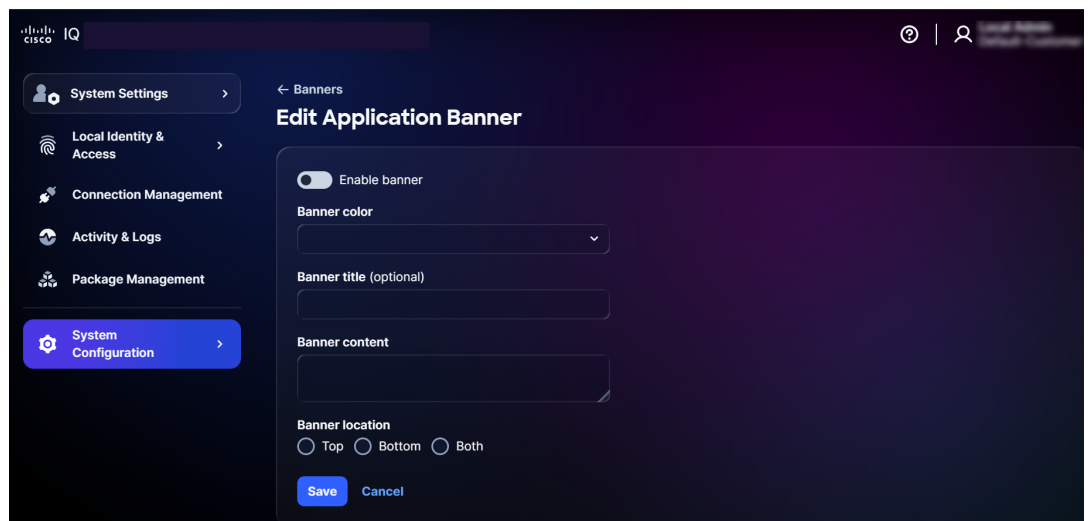
애플리케이션 배너를 구성하려면

1. System Settings(시스템 설정)에서 System Configuration(시스템 컨피그레이션) > Banners(배너)를 선택합니다. Banners(배너) 페이지가 표시됩니다.



배너 구성

2. 애플리케이션 배너에서 구성을 클릭합니다. 애플리케이션 배너 편집 페이지가 표시됩니다.



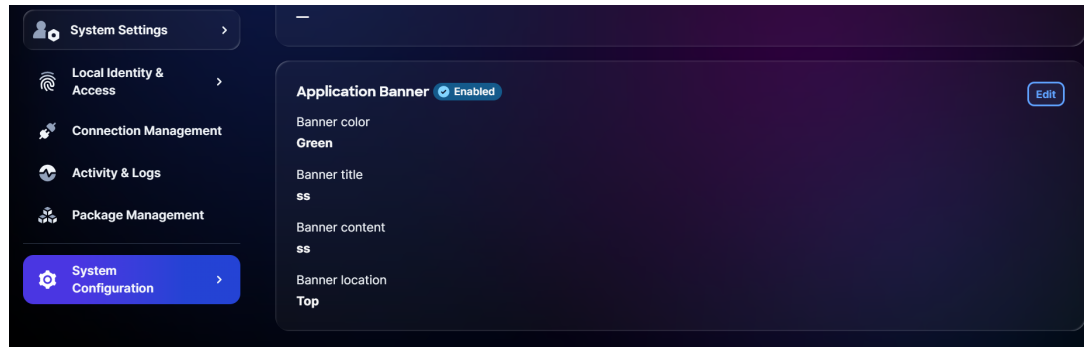
애플리케이션 배너 편집

3. 배너를 활성화 또는 비활성화하려면 토글을 클릭합니다.
4. 배너 색상을 선택합니다.
5. 배너 제목을 입력합니다.
6. 배너 콘텐츠를 입력합니다.
7. 배너 위치를 선택합니다.
8. 저장을 클릭합니다. 배너가 애플리케이션 전체에 표시됩니다.

배너 수정

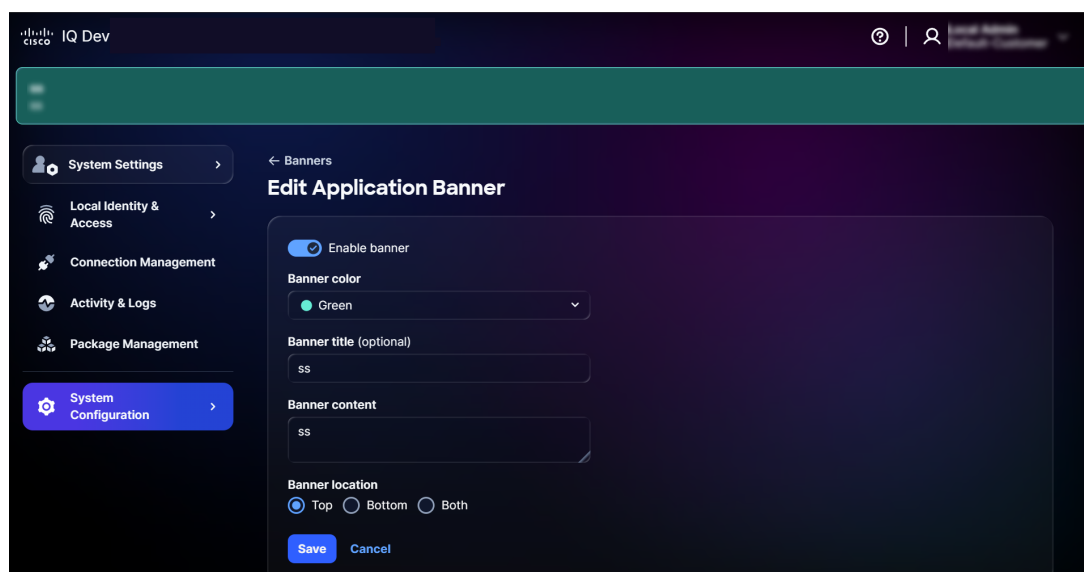
배너를 수정하려면

1. System Settings(시스템 설정)에서 System Configuration(시스템 컨피그레이션) > Banners(배너)를 선택합니다. Banners(배너) 페이지가 표시됩니다.



배너 편집

2. Edit를 클릭합니다. 애플리케이션 배너 편집 페이지가 표시됩니다.



애플리케이션 배너 편집

3. 원하는 세부 정보를 편집합니다.
4. 배너를 활성화 또는 비활성화하려면 토글을 클릭합니다.
5. 저장을 클릭합니다.

문제 해결

Cisco IQ 시스템에서 진단 및 로그 파일을 수집하고 SCP 서버로 안전하게 전송할 수 있습니다. 문제를 보고할 때 이러한 파일을 지원 팀과 공유하여 중

요한 컨텍스트를 제공하고 문제 해결을 지원할 수 있습니다.

진단 및 로그 파일을 수집하려면

1. Cisco IQ에 로그인합니다.

```
CISCO IQ

Navigation Main Menu

SYSTEM STATUS
Cisco IQ On-Prem Installed

CONFIGURATION SETTINGS
IP Address/Mask
Gateway IP
DNS List
Search Domain
NTP List
Hostname

MAIN MENU
[1] Configure Network Settings DISABLED because the platform is installed
[2] Configure System Orchestrator DISABLED because the platform is installed
[3] System Diagnostics
[4] Help
[5] About
[q] Quit
```

주 메뉴

2. Cisco IQ Main(Cisco IQ 주) 메뉴에서 "3"을 입력하고 Enter 키를 눌러 System Diagnostics(시스템 진단)를 선택합니다.

```
CISCO IQ

Navigation Main Menu > System Diagnostics

Please provide the following server connection details:

[Enter SCP/SFTP Server Address: ]
Valid IP address ✓
[Enter SCP/SFTP Server Port (e.g. 22): ]
Valid port ✓
[Enter SCP/SFTP Server Path (e.g. /var/log/support/): ]
Valid server path ✓

PROTOCOL SELECTION
[1] SCP (Secure Copy Protocol) - Default
[2] SFTP (SSH File Transfer Protocol)

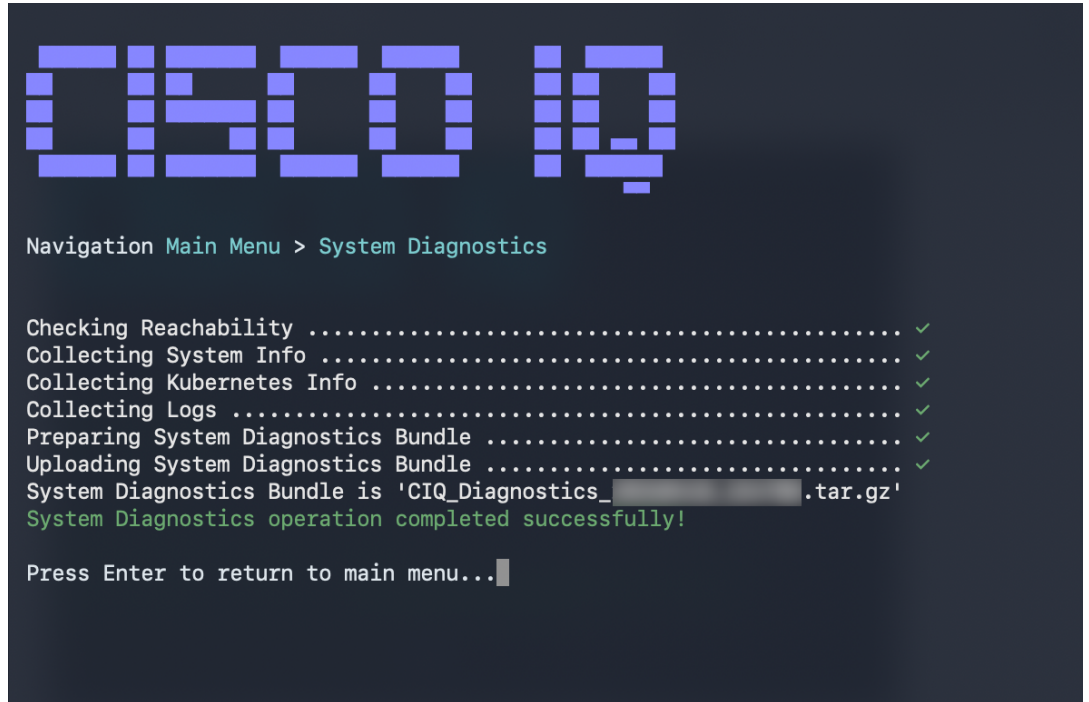
[Select protocol [1]/[2] (default: SCP): 1]
scp
✓ Selected protocol: SCP
[Enter Username: ]
Valid username ✓
[Enter Password: ]

Continue with System Diagnostics? ([c]ontinue/[B]ack):
```

시스템 진단

3. SCP/SFTP 서버 주소를 입력합니다.

4. SCP/SFTP 서버 포트를 입력합니다.
5. SCP/SFTP 서버 경로를 입력합니다.
6. 프로토콜을 선택합니다.
7. 사용자 이름을 입력합니다.
8. Password(비밀번호)를 입력합니다.
9. "C"를 입력하고 Enter를 눌러 시스템 진단을 계속합니다.

A terminal window with a dark background and light blue text. At the top, there is a large, stylized logo made of small squares. Below the logo, the text "Navigation Main Menu > System Diagnostics" is displayed. A list of diagnostic steps follows, each with a green checkmark at the end: "Checking Reachability", "Collecting System Info", "Collecting Kubernetes Info", "Collecting Logs", "Preparing System Diagnostics Bundle", and "Uploading System Diagnostics Bundle". Below this list, a message states "System Diagnostics Bundle is 'CIQ_Diagnostics_...tar.gz'" and "System Diagnostics operation completed successfully!". At the bottom, it says "Press Enter to return to main menu..." with a cursor.

```
Navigation Main Menu > System Diagnostics

Checking Reachability ..... ✓
Collecting System Info ..... ✓
Collecting Kubernetes Info ..... ✓
Collecting Logs ..... ✓
Preparing System Diagnostics Bundle ..... ✓
Uploading System Diagnostics Bundle ..... ✓
System Diagnostics Bundle is 'CIQ_Diagnostics_...tar.gz'
System Diagnostics operation completed successfully!

Press Enter to return to main menu...
```

시스템 진단 작업 완료

시스템에서 진단 프로세스를 시작하고 다음 작업을 수행합니다.

- 연결성 확인
- 시스템 정보 수집
- Kubernetes 정보 수집
- 로그 수집
- 시스템 진단 번들 준비
- 시스템 진단 번들 업로드

완료되면 생성된 번들 이름을 나타내는 확인 메시지가 표시됩니다.

지원 모듈

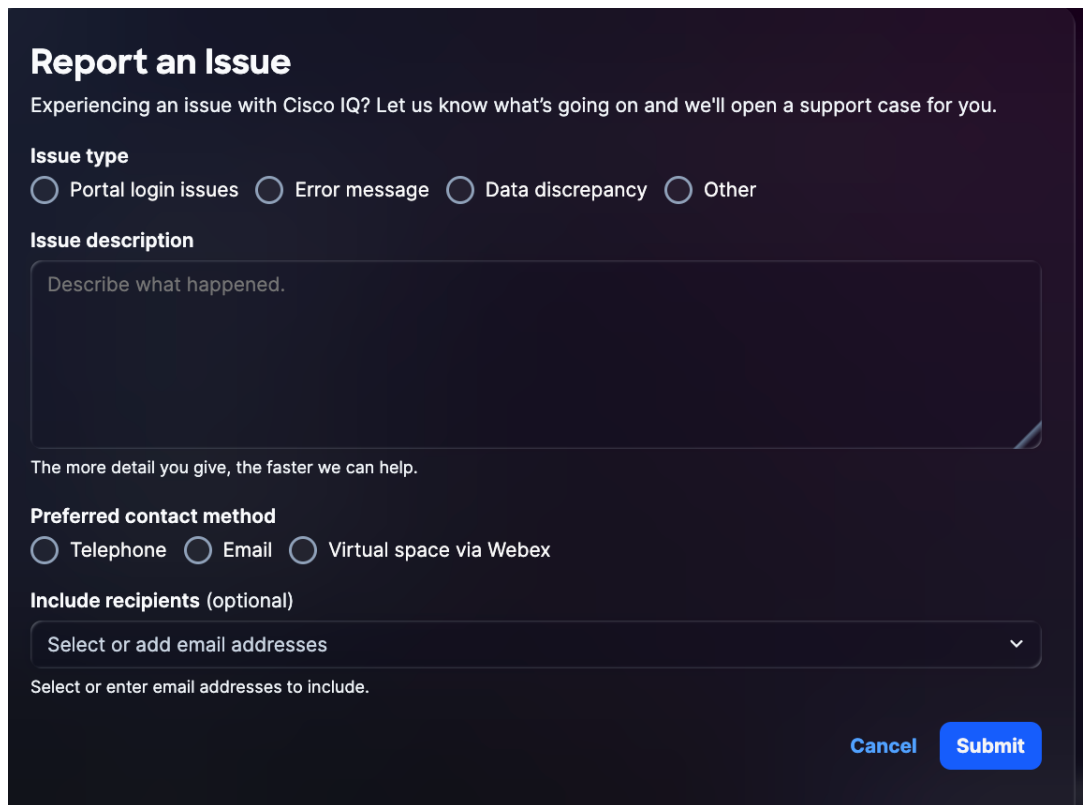
Cisco IQ SaaS에서 VA 및 모듈별 지원 사례를 생성할 수 있습니다. 지원 모듈은 Cisco IQ SaaS에서 사용할 수 있으며 지원 케이스를 통합적으로 볼 수 있습니다. 케이스 목록 보기를 필터링, 정렬 및 맞춤화할 수 있으며, 액세스 권한이 있는 미결 케이스와 마감된 케이스 모두에 대한 가시성을 제공합니다. Cisco IQ SaaS의 지원 모듈에 대한 자세한 내용은 [Cisco IQ SaaS 시작 설명서를 참조하십시오](#).

 참고: Cisco IQ VA 고객은 Cisco IQ VA 및 해당 모듈과 관련된 TAC(Technical Assistance Center) 케이스 접수, 제품 케이스 생성 및 관리 등 대부분의 Cisco IQ SaaS 지원 모듈 기능에 액세스할 수 있습니다.

지원 케이스 생성

Cisco IQ SaaS에서 VA 및 모듈별 케이스를 생성할 수 있습니다. 케이스를 생성하려면

1. SaaS([Cisco IQ](#))에 로그인합니다.
2. Help(도움말) 아이콘 > Report an Issue(문제 보고)를 클릭합니다. 문제 보고 창이 열립니다.



Report an Issue

Experiencing an issue with Cisco IQ? Let us know what's going on and we'll open a support case for you.

Issue type

☐ Portal login issues ☐ Error message ☐ Data discrepancy ☐ Other

Issue description

Describe what happened.

The more detail you give, the faster we can help.

Preferred contact method

☐ Telephone ☐ Email ☐ Virtual space via Webex

Include recipients (optional)

Select or add email addresses

Select or enter email addresses to include.

Cancel Submit

문제 보고

3. 필요한 세부 정보를 제공합니다.
4. Submit(제출)을 클릭합니다.

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.