

Cisco IQ 시작하기 가이드

소개

Cisco IQ™은 고객에게 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 사용자가 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.

이 문서에서는 Cisco IQ 및 해당 애플리케이션 시작에 대한 정보를 제공합니다. 자세한 내용은 [Cisco IQ 릴리스 정보](#) 또는 [Cisco IQ FAQ 문서](#)를 참조하십시오.

온보드


사전 요구 사항

Cisco IQ를 사용하기 전에 다음 전제 조건을 충족해야 합니다.

지원되는 브라우저

Cisco IQ는 다음 브라우저의 안정적인 최신 릴리스에서 지원됩니다.

- Google Chrome
- Microsoft Edge
- 애플 사파리
- Mozilla Firefox

 참고: 지원은 현재 브라우저 버전으로 제한되며 이전 버전에서는 전체 기능을 제공하지 않거나 새 업데이트가 릴리스될 때 지원되지 않을 수 있습니다.

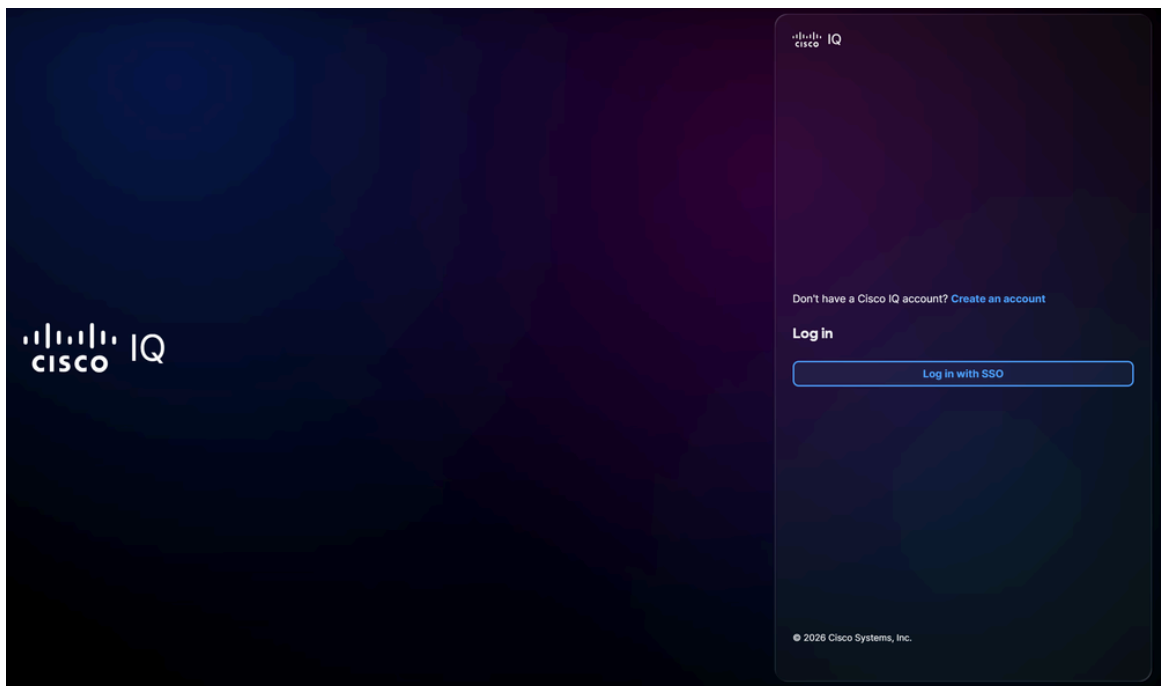
Cisco IQ에 액세스하려면 Cisco.com 계정이 있어야 합니다. Cisco [어카운트에](#) 대한 자세한 내용은 [로그인 및 어카운트 도움말](#)을 참조하십시오.

계정 생성

새 Cisco IQ 어카운트 생성

새 Cisco IQ 어카운트를 생성하려면

1. [Cisco IQ](#)로 이동합니다. Cisco Log in(Cisco 로그인) 페이지가 표시됩니다.



Cisco IQ 로그인

2. Create an account(어카운트 생성)를 클릭합니다.
3. Email(이메일) 필드에 CCO(Cisco Connection Online) ID 자격 증명을 입력합니다.
4. Next(다음)를 클릭합니다.
5. 비밀번호를 입력합니다.
6. Verify를 클릭합니다. Create a Cisco IQ Account(Cisco IQ 계정 생성) 페이지가 표시됩니다.

Create a Cisco IQ Account

Enter a company account name

Enter a preferred name for your organization Cisco IQ account

Select the primary data storage region

Choose the designated geographic data center where your data is securely stored and processed for this account.

US

EMEA


APJC

Create account

Cisco IQ 어카운트 생성


7. 회사 계정 이름 입력 필드에 조직의 Cisco IQ 계정에 사용할 고유 이름을 입력합니다.
8. 기본 데이터 저장 영역을 선택합니다.
9. Create account(어카운트 생성)를 클릭합니다. Cisco IQ 실행 패드로 리디렉션됩니다.

CX 클라우드 어카운트를 Cisco IQ로 마이그레이션

 참고: 어카운트 관리자만 기존 CX 클라우드 어카운트를 Cisco IQ로 마이그레이션할 수 있습니다.

기존 CX 클라우드 어카운트가 있는 경우 기존 CX 클라우드 데이터를 Cisco IQ로 마이그레이션할 수 있습니다. 다음 데이터는 기존 CX 클라우드 어카운트에서 자동으로 마이그레이션됩니다.

- 사용자 및 사용자 그룹(파트너 사용자 및 그룹 제외)
- 계약
- Intersight, Webex, SD-WAN(Software-Defined Wide Area Network), Meraki를 위한 클라우드 데이터 소스 추가

 참고: 원활한 전환을 보장하고 Cisco IQ의 맞춤형, 예측 가능한 사전 대응식 AI 기반 인텔리전스에서 더 정확한 통찰력을 얻으려면 마이그레이션 전에 CX 클라우드 계정 데이터를 검증하고 구성하는 것을 고려하십시오.

경고: CX 클라우드 데이터를 마이그레이션하지 않고 새 Cisco IQ 어카운트를 생성하는 경우 나중에 CX 클라우드 어카운트 데이터를 마이그레이션할 수 없습니다.

참고: CX 클라우드 어카운트는 한 번에 하나만 마이그레이션할 수 있습니다. 추가 어카운트를 마이그레이션해야 하는 경우 이 섹션에 설명된 단계를 반복합니다.

기존 CX 클라우드 어카운트를 마이그레이션하려면

1. [Cisco IQ](#)로 이동합니다. Cisco Log in(Cisco 로그인) 페이지가 표시됩니다.
2. Create an account(어카운트 생성)를 클릭합니다.
3. Email(이메일) 필드에 CCO(Cisco Connection Online) ID 자격 증명을 입력합니다.
4. Next(다음)를 클릭합니다.
5. 비밀번호를 입력합니다.
6. Verify를 클릭합니다. Create a Cisco IQ Account(Cisco IQ 계정 생성) 페이지가 표시됩니다.

Create a Cisco IQ Account

Migrate existing CX Cloud account?
If you create a new Cisco IQ account without migrating CX Cloud data, you will not be able to migrate CX Cloud account data later.

Select account to migrate [View account migration details](#)

CX Cloud account name	Region
<input checked="" type="radio"/> [Redacted]	APJC
<input type="radio"/> [Redacted]	EMEA
<input type="radio"/> [Redacted]	US

Enter a company account name
[Redacted]
Enter the name you want to use for your organization's Cisco IQ account.


Data storage region
APJC

Create account and migrate data

[Create a new Cisco IQ account without migrating data](#)

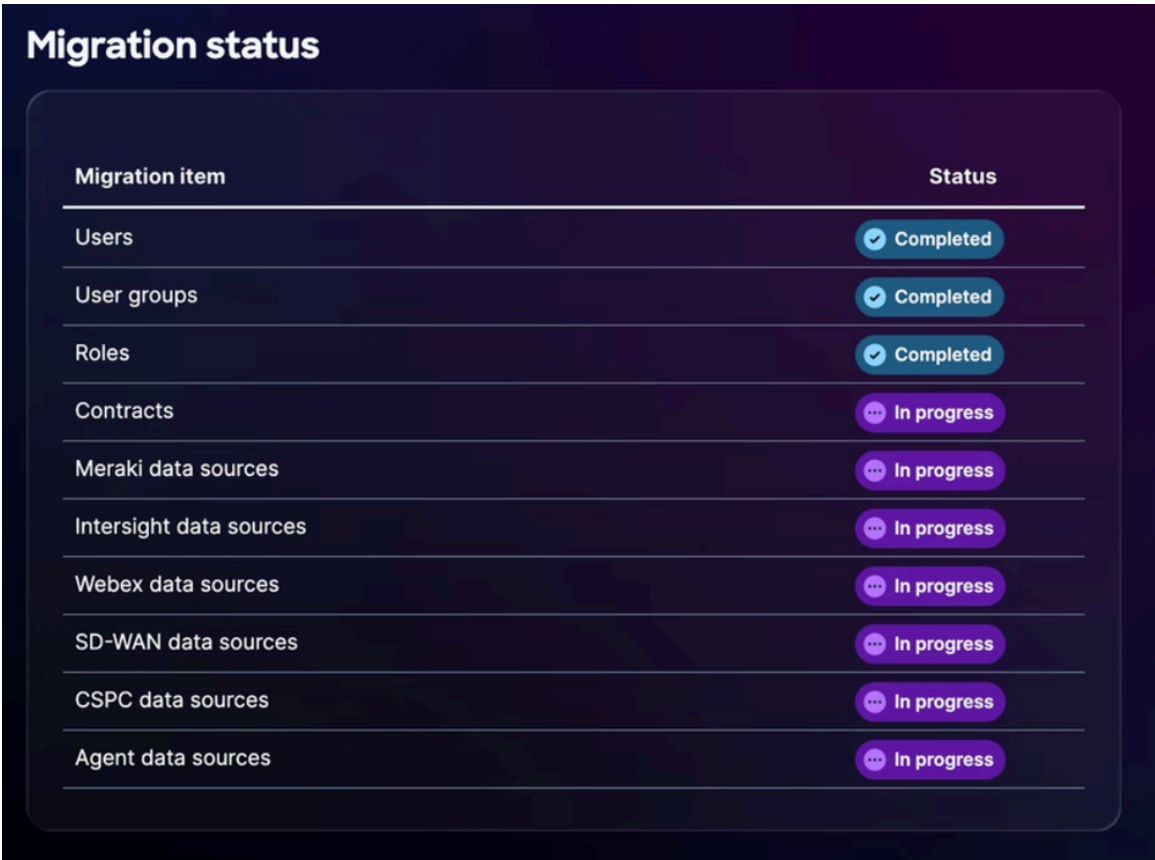
CX 클라우드 어카운트 선택

7. 데이터를 마이그레이션할 CX 클라우드 어카운트를 선택합니다.
8. 조직의 Cisco IQ 어카운트에 사용할 고유한 이름을 입력합니다.

 참고: 원래 어카운트의 데이터 스토리지 영역은 자동으로 채워지며 Cisco IQ 회사 어카운트로 마이그레이션됩니다. 데이터 스토리지 영역을 변경하려면 새 Cisco IQ 회사 어카운트를 생성해야 합니다.

9. Create account(어카운트 생성) 및 migrate data(데이터 마이그레이션)를 클릭합니다. Migration Status 페이지가 표시됩니다.

Migration Status 페이지는 Cisco IQ로 마이그레이션되는 데이터의 완료 상태를 표시합니다. 다음 상태를 사용할 수 있습니다.



Migration item	Status
Users	Completed
User groups	Completed
Roles	Completed
Contracts	In progress
Meraki data sources	In progress
Intersight data sources	In progress
Webex data sources	In progress
SD-WAN data sources	In progress
CSPC data sources	In progress
Agent data sources	In progress


마이그레이션 상태

- 진행 중: 데이터를 마이그레이션하는 중입니다.
- 완료됨: 마이그레이션 완료
- 마이그레이션할 수 없음: 데이터 마이그레이션이 완료되지 않아 Cisco IQ가 데이터를 마이그레이션할 수 없음

데이터를 마이그레이션할 수 없는 경우, 데이터를 새 Cisco IQ 회사 어카운트로 수동으로 마이그레이션해야 합니다. Cisco IQ에 추가 데이터를 추가하는 방법에 대한 자세한 내용은 [시스템](#) 설정을 참조하십시오.

10. 마이그레이션 프로세스가 완료되면 Continue(계속)를 클릭합니다. Cisco IQ 실행 패드로 리디렉션됩니다.

기존 어카운트에 로그인

 참고: 기존 Cisco IQ 어카운트가 있는 고객 중 회사 어카운트에 추가되지 않은 고객은 어카운트 관리자에게 어카운트 액세스를 요청해야 합니다.

기존 계정에 로그인하려면

1. [Cisco IQ](#)로 이동합니다. Cisco Log in(Cisco 로그인) 페이지가 표시됩니다.
2. Log in with SSO(SSO로 로그인)를 클릭합니다.
3. Email(이메일) 필드에 CCO ID 자격 증명을 입력합니다.
4. Next(다음)를 클릭합니다.
5. 비밀번호를 입력합니다.
6. Verify를 클릭합니다.

계정이 하나 있는 경우 Cisco IQ 실행 패드로 리디렉션됩니다.

둘 이상의 계정이 있는 경우 Cisco IQ 시작 페이지로 리디렉션됩니다.

Welcome to Cisco IQ!

Select an account below

Q Search

Account name

Region

US


US

US

US


계정 이름 선택

시작하기

 참고: 시작하기 전에 Cisco IQ에 완전히 합류했는지 확인하십시오. 자세한 [내용](#)은 온보딩을 참조하십시오.

지원 계층

Cisco IQ Support Tier 레벨은 Cisco IQ에서 귀하가 사용할 수 있는 액세스 및 기능을 정의하며, 귀하의 지원 및 전문 서비스 경험을 향상하도록 설계되었습니다. 이러한 레벨은 유효한 Cisco 지원 계약과 연결되어 AI 중심의 통찰력 및 문제 해결부터 자산 및 계약 관리에 이르기까지 활용할 수 있는 기능과 툴을 결정합니다. 레벨을 이해하면 Cisco IQ의 기능을 충분히 활용하는 동시에 계약 권한을 준수할 수 있습니다. 다음 표에는 각 레벨에서 사용할 수 있는 Cisco IQ 기능이 요약되어 있습니다.

 참고: 여러 지원 계층에 걸쳐 기능이 누적됩니다. 상위 레벨에는 하위 레벨의 모든 기능이 포함됩니다.

	기본 수준	표준 레벨	서명 레벨
	현재 상태 파악	운영 탄력성 우선 순위 지정	운영 효율성 가속화
완벽한 풍경 명료성	<p>다음 기능을 사용하여 동적 높은 신뢰도로 모든 Cisco 자산 및 하위 구성 요소를 추적합니다.</p> <ul style="list-style-type: none"> • 자산 인벤토리 • EOL(End-of-Life) 보고서 • 서비스 커버리지 보고서 • LDOS(Last Date of Support) 대시보드 	<p>다음 기능을 사용하여 네트워크의 성능을 분석하여 리소스를 할당할 위치를 결정하고 인프라 투자에 대한 현명한 결정을 내릴 수 있습니다.</p> <ul style="list-style-type: none"> • EOL 인사이트¹ • 서비스 커버리지 인사이트¹ • LDOS 인사이트¹ • 자산 중요도 인사이트¹ • 자산 태깅 	
사전 대응적 탄력성	<p>다음 기능을 사용하여 환경 내에서 잠재적 위험을 식별하고 해결하는 데 도움이 되는 중요한 알림에 대한 가시성을 확보합니다.</p> <ul style="list-style-type: none"> • 보안 자문 보고서 • Field Notice 보고서 	<p>Cisco IQ는 자산 위험의 상관관계를 분석함으로써 데이터를 통찰력으로 전환하여 가장 중요한 보안 위험을 식별하고 우선 순위를 지정할 수 있도록 합니다.</p> <ul style="list-style-type: none"> • 보안 자문 인사이트¹ • 보안 강화 인사이트¹ • Field Notice Insights¹ • 구성 인사이트¹ 	<p>다음 기능은 보안 상태를 개선하고 환경 내에서 구성을 최적화하는 데 도움이 되는 실행 가능한 권장 사항을 제공합니다.</p> <ul style="list-style-type: none"> • 구성 권장 사항¹ • 보안 강화 권장 사항¹
신속한 해결	<p>지원 사례를 관리하고 해결 상태를 한 곳에서 추적하여 다음 기능을 사용하여 문제를 더 빨리 해결하십시오.</p> <ul style="list-style-type: none"> • 사례 관리 	<p>다음 기능을 사용하여 케이스 트렌드 및 효율성 메트릭을 추적하여 지속적인 운영 개선 사항을 보여 주십시오. Cisco IQ는 활성 문제를 해결하고 근본적인 근본 원인을 조사하는 데 도움이 되는</p>	

	<ul style="list-style-type: none"> • 셀프 서비스 문제 해결¹ 	<p>상황 인식 해결 도우미를 제공합니다.</p> <ul style="list-style-type: none"> • 사례 인사이트¹ 	
--	--	---	--

¹ Cisco IQ Link, Intersight, Meraki, SD-WAN Manager 및 WebEx Control Hub를 통한 디바이스 및 텔레메트리 연결 지원

기본 기능

기본 지원 계층은 기술 제품 지원 전문가 액세스, 셀프 서비스 문제 해결, 중앙 집중식 사례 관리 등 신뢰할 수 있고 사후 대응적인 지원을 통해 기본적인 제어 기능을 제공합니다. Cisco IQ는 완벽한 가시성을 보장하기 위해 자산 텔레메트리, 계약 정보 및 지원 기록을 통합하여 자산 라이프사이클, 보안 권고 및 필드 알림에 대한 포괄적인 보기를 제공합니다. 또한 [Cisco U](#)를 통해 제공되는 기본적인 학습 리소스에 액세스하여 기술 전문성을 강화할 수 있습니다.

다음 표에는 기본 지원 계층에 사용할 수 있는 기능이 요약되어 있습니다.

기능	설명
자산 인벤토리	Asset Inventory는 하드웨어 제품, 모델 및 일련 번호, OS 버전, 설치 위치, 서비스 커버리지 세부사항에 대한 최신 목록 및 풍부한 시각화를 제공합니다. 또한 Cisco가 TAC(Technical Assistance Center) 케이스, 계약 갱신, 텔레메트리 등을 기준으로 자산이 활성 상태임을 알았을 때인 '마지막 신호'로 필터링하는 방법도 제공합니다.
EOL 보고서	EOL 보고서는 EoS(End of Sales)에서 LDOS로 EOL 중요 시점에 도달하거나 EOL 중요 시점을 넘긴 하드웨어 및 소프트웨어에 대한 최신 목록 및 풍부한 시각화를 제공하여 라이프사이클 및 기술 업데이트 계획을 가능하게 합니다.
서비스 커버리지 보고서	서비스 커버리지 보고서는 커버리지 및 지원 대상이 아닌 자산에 대한 최신 목록과 풍부한 시각화를 제공합니다.
LDOS 대시보드	LDOS 대시보드에서는 LDOS 주요 시점을 중앙에서 확인할 수 있으므로 하드웨어 또는 소프트웨어가 단종되기 전에 자산 계획 및 예산 예측이 개선되어 운영 위험을 줄일 수 있습니다.
보안 자문	보안 권고는 노출을 탐지하고, 위협의 심각도와 중요도를 기준으로 취약성의 우선 순위를 정하고, 경영진 수준의 통찰력을 제공하여 중요한 위협의

	완화를 가속화하여 진화하는 위협에 대한 전사적 탄력성을 강화하는 자동화된 솔루션을 제공합니다.
필드 알림	Field Notice는 보안 관련 제품이 아닌 문제를 감지하고, 영향 심각도와 중요도에 따라 문제의 우선 순위를 정하고, 임원급 통찰력을 제공하여 중요한 운영 문제를 신속하게 해결함으로써 기업 탄력성을 향상시키고 최적의 성능을 유지하는 자동화된 솔루션을 제공합니다.
사례 관리	Case Management는 케이스 수, 상태, 심각도 및 케이스와 관련된 RMA(Return Material Authorization)를 비롯한 최신 Cisco TAC 케이스 목록을 제공합니다. 또한 TAC 케이스를 열고(SCM(Support Case Manager) 에 대한 교차 실행을 통해) 신속하게 케이스 정보를 업데이트하여 문제 해결을 촉진할 수 있습니다.
셀프 서비스 문제 해결 ¹	셀프 서비스 문제 해결은 Cisco IQ AI Assistant를 사용하여 문제를 즉시 해결할 수 있는 방법을 제공합니다. 이 인터랙티브 툴은 Cisco의 검증된 지식 기반에서 직접 제공하는 실시간 컨텍스트 인식 문제 해결 및 전문가 권장 사항을 바탕으로 하므로 지원 케이스를 열지 않고도 문제를 해결할 수 있습니다.

¹ Cisco IQ Link, Intersight, Meraki, SD-WAN Manager 및 WebEx Control Hub를 통한 디바이스 및 텔레메트리 연결 지원

표준 기능

Standard 지원 계층은 솔루션 수준의 문제를 중앙 집중식으로 분류하고 필요한 기술 전문가와 조율하는 전담 케이스 소유자를 제공함으로써 운영 효율성을 향상시킵니다. 자산 데이터를 비즈니스 중요도와 연계하는 AI 기반 통찰력을 사용하여 위협을 사전에 완화할 수 있으며, 이를 통해 인벤토리, 보안, 구성 평가에 대한 명확한 가시성을 확보할 수 있습니다. 또한 [Cisco U](#)에서 제공되는 개별화된 학습 경로를 통해 팀의 전문성을 파트너의 특정 비즈니스 요구 사항에 맞출 수 있습니다.

다음 표에는 Standard 지원 계층에서 사용할 수 있는 기능이 요약되어 있습니다.

기능	설명
EOL 인사이트 ¹	EOL Insights는 EOL 주요 시점을 지능적으로 쿼리, 요약, 시각화 및 보고하여 라이프사이클 및 기술 업그레이드 계획에 대한 맞춤형 우선 순위를 제공합니다.

서비스 커버리지 인사이트 ¹	Service Coverage Insights는 서비스 커버리지 세부사항 및 갱신 시점을 시각화하고 분석함으로써 커버리지 업데이트 및 갱신 계획에 대한 맞춤형 우선순위 지정을 지원합니다.
자산 태깅	Asset Tagging을 사용하면 Asset Tags를 사용하여 비즈니스 요구에 따라 인벤토리를 구성할 수 있으므로, 부서, 위치 또는 프로젝트별로 하드웨어 및 소프트웨어 자산을 유연하게 구성할 수 있습니다.
LDOS 인사이트 ¹	LDOS Insights는 LDOS 이정표를 넘어서거나 다가가는 자산의 가시화 및 분석을 제공하여 라이프사이클 및 기술 업그레이드 계획에 대한 맞춤형 우선 순위를 제공합니다.
자산 중요도 인사이트 ¹	Asset Criticality Insights를 통해 자산 역할과 네트워크에서 자산 역할의 상대적 중요도를 평가 및 식별하여 위험 완화 노력의 우선 순위를 정하고 운영 탄력성을 개선할 수 있습니다.
보안 자문 인사이트 ¹	Security Advisory Insights는 Security Advisories의 영향을 받는 자산에 대한 지능적인 쿼리, 요약, 시각화 및 보고를 제공하여 위험 및 보안 사고 대응의 개인화된 우선 순위를 설정할 수 있도록 합니다.
보안 강화 인사이트 ¹	Security Hardening Insights는 장비 구성을 평가하고, 영향의 심각도와 중요도에 따라 보안 강화 허점을 파악하고, 임원급 통찰력을 제공하여 중요한 강화 조치를 신속하게 이행하는 자동화된 솔루션을 제공합니다. 지능형 쿼리, 요약, 시각화, 위험 자산 보고를 통해 향상된 보안 상태의 개인 맞춤형 우선 순위를 제공하는 동시에 엔터프라이즈 탄력성을 높이고 진화하는 위협에 대한 공격 표면을 줄입니다.
Field Notice Insights ¹	Field Notice Insights는 Field Notice의 영향을 받는 자산에 대한 지능적인 쿼리, 요약, 시각화 및 보고를 제공하여 위험 우선 순위를 맞춤화하고 알려진 문제에 대응할 수 있도록 지원합니다.
구성 인사이트 ¹	Configuration Insights는 현장에서 검증된 전문 지식을 바탕으로 Cisco가 권장하는 모범 사례와 비교하여 장치 구성을 평가하는 자동화된 솔루션을 제공합니다. 영향을 받는 자산의 지능적인 쿼리, 요약, 시각화 및 보고를 통해 개인화된 우선 순위를 지정하고 중요한 구성 차이를 신속하게 해결하여 인프라 탄력성을 높이고 네트워크 전반의 운영 위험을 줄일 수 있습니다.
사례 인사이트 ¹	Case Insights는 Cisco TAC 사례에 대한 지능적인 쿼리, 요약, 시각화 및 보고를 제공하여 운영 효율성에 대한 개별 맞춤형 모니터링을 지원합니다.

¹ Cisco IQ Link, Intersight, Meraki, SD-WAN Manager 및 WebEx Control Hub를 통한 디바이스 및 텔레메트리 연결 지원

시그니처 기능

시그니처 지원 계층은 표준 지원 계층을 기반으로 하며, 정의된 복구 SLA(Service Level Agreements)를 통해 운영 성과를 높이고 고객의 고유한 환경에 친숙한 전문가들로 구성된 전담 팀에 액세스할 수 있습니다. 이 등급은 운영 중단을 미연에 방지하는 데 중점을 둡니다. 사전 예방적 보안 강화, 체계적인 근본 원인 제거, 지속적인 전문가 중심 자산 분석을 통해 운영 중단을 예방합니다. 또한 고급 [Cisco U](#). 인증 교육 및 가상 실습 랩을 활용하여 수준 높은 기술 숙련도를 쌓을 수 있습니다.

다음 표에는 시그니처 지원 계층에 사용할 수 있는 기능이 요약되어 있습니다.

기능	설명
구성 권장 사항 ¹	Configuration Recommendation(컨피그레이션 권장 사항)은 잠재적 컨피그레이션 오류 및 불일치를 해결하기 위한 실행 가능한 권장 사항을 제공합니다.
보안 강화 권장 사항 ¹	Security Hardening Recommendations(보안 강화 권장 사항)는 각각의 실패한 강화 검사에 대한 일반적인 권장 사항을 제공하는 자동화된 솔루션을 제공하여 근본적인 보안 문제를 명확하고 간결하게 해결합니다.

¹ Cisco IQ Link, Intersight, Meraki, SD-WAN Manager 및 WebEx Control Hub를 통한 디바이스 및 텔레메트리 연결 지원

관리자를 위한 시작하기

새로 생성했거나 마이그레이션한 Cisco IQ 어카운트에 처음으로 로그인하면 시작 페이지에 시작 여정이 표시됩니다. Get Started(시작하기) 여정은 어카운트가 마이그레이션된 데이터를 사용하여 생성되었는지 또는 마이그레이션하지 않고 생성되었는지에 따라 달라집니다.


 참고: 시작하기 여정 환경은 RBAC(Role-Based Access Control) 권한에 따라 달라집니다.

생성을 통한 신규 어카운트

새로 생성된 어카운트의 시작하기 여정은 Cisco IQ 환경을 구성하고 Cisco IQ를 탐색하는 데 필요

한 초기 온보딩 단계를 안내합니다.


Cisco 클라우드 제품 연결

 참고: 이 단계를 완료하려면 하나 이상의 클라우드 제품을 연결해야 합니다.

Cisco 클라우드 제품 데이터를 Cisco IQ에 연결하는 것이 강력하고 개별화된 기능을 사용하는 가장 빠른 방법입니다. 데이터 연결을 설정한 후 몇 분 이내에 맞춤형 인사이트를 받을 수 있습니다.

Cisco 클라우드 제품에 연결하려면 [데이터](#) 커넥터를 [참조하십시오](#).


서비스 계약 연결

 참고: 이 단계를 완료하려면 하나 이상의 서비스 계약을 연결해야 합니다.

계약을 연결하면 서로 다른 팀 구성원과 연결된 계약의 데이터가 통합되고 텔레메트리를 통해 인벤토리에 연결되지 않은 자산이 통합되므로, 중앙 집중식 지원 커버리지 가시성이 확보되고 갱신 문제가 발생하지 않습니다.

서비스 계약을 연결하려면 서비스 계약을 [참조하십시오](#).


온프레미스 디바이스 연결

 참고: 이 단계를 완료하려면 하나 이상의 Cisco IQ Link를 등록해야 합니다.

온프레미스 디바이스와의 통신을 설정하려면 Cisco IQ Link를 구성해야 합니다. Cisco IQ Link는 Cisco 클라우드 플랫폼에서 아직 관리하지 않는 온프레미스 디바이스에 Cisco IQ의 모든 기능을 제공합니다. Cisco IQ Link는 데이터 센터에 VM(Virtual Machine)으로 설치하고 Cisco IQ 어카운트에 연결할 수 있습니다.

온프레미스 디바이스를 연결하려면 [데이터](#) 커넥터를 [참조하십시오](#).

사용자 액세스 관리

 참고: 이 단계를 완료하려면 두 명 이상의 사용자를 추가해야 합니다.

Cisco IQ의 간단한 액세스 제어 기능은 소규모 팀과 대규모 조직을 위해 설계되었습니다. 사용자를

추가하고 그룹 및 개인에게 관리자 또는 보기 전용 역할을 할당할 수 있습니다.

사용자를 추가하고 권한을 할당하려면 사용자를 [참조하십시오](#).

Cisco IQ 탐색

다음과 같은 Cisco IQ의 기능과 애플리케이션을 살펴보십시오.

- 실행 패드: 애플리케이션 액세스, 새로운 기능 검색, 대시보드 생성
- 자산 애플리케이션: 자세한 [내용은 Assets Application](#)을 참조하십시오
- 평가 애플리케이션: 자세한 [내용은](#) 평가 애플리케이션을 참조하십시오
- 지원 애플리케이션: 자세한 [내용은](#) 지원 애플리케이션을 참조하십시오
- Cisco IQ AI Assistant: 자세한 내용은 [AI Assistant](#)를 참조하십시오
- 시스템 설정: 계정 설정을 관리하고, 사용자에게 액세스 권한을 부여하고, 데이터 연결을 구성하고, 계정에 대한 활동 및 로그를 봅니다. 자세한 [내용은 시스템 설정](#) 참조

마이그레이션을 통한 신규 어카운트

마이그레이션을 통해 새 Cisco IQ 어카운트를 만든 경우 이전 어카운트의 정보를 이미 사용할 수 있습니다. 따라서 새로 마이그레이션된 어카운트의 시작하기 여정은 아래에 자세히 설명된 마이그레이션 검토로 제한됩니다.

마이그레이션 검토

마이그레이션을 검토하려면

- 계약이 성공적으로 마이그레이션되었는지 확인합니다. 홈 > 시스템 설정 > 서비스 계약
- 필요한 모든 데이터 연결이 홈 > 시스템 설정 > 데이터 커넥터에 올바르게 구성되어 있는지 확인합니다
- 사용자 데이터가 성공적으로 마이그레이션되었는지 확인하고, 홈 > 시스템 설정 > ID 및 액세스 > 사용자에서 계정을 활성화하여 마이그레이션된 사용자에게 액세스 권한을 부여합니다
- Home > Assets(자산) > Inventory(인벤토리)에서 자산이 성공적으로 마이그레이션되었는지 확인합니다.

일반 사용자를 위한 시작하기

Cisco IQ 계정에 처음으로 로그인하면 시작 페이지에 시작 여정이 표시됩니다. 이 과정에서는 Cisco IQ 기능 및 공통 워크플로에 대해 설명합니다.

 참고: 시작하기 여정 환경은 RBAC 권한에 따라 달라집니다.

Cisco IQ 탐색

다음과 같은 Cisco IQ의 기능과 애플리케이션을 살펴보십시오.

- 실행 패드: 애플리케이션 액세스, 새로운 기능 검색, 대시보드 생성
- 자산 애플리케이션: 자세한 [내용은 Assets Application](#)을 참조하십시오
- 평가 애플리케이션: 자세한 [내용은](#) 평가 애플리케이션을 참조하십시오
- 지원 애플리케이션: 자세한 [내용은](#) 지원 애플리케이션을 참조하십시오
- Cisco IQ AI Assistant: 자세한 내용은 [AI Assistant](#)를 참조하십시오

첫 번째 AI 보고서 생성

Cisco IQ의 AI 기반 분석 기능은 특정 비즈니스 요구 사항에 맞게 조정할 수 있는 선택된 자산을 기준으로 맞춤형 대상 보고서를 생성합니다.

첫 AI 보고서 [생성](#)에 대한 자세한 내용은 Assets 애플리케이션을 참조하십시오.

Cisco IQ AI Assistant에게 질문

시작하기 여정의 마지막 단계는 어디에서나 Cisco IQ AI Assistant를 시작하고 자산, 사례 또는 평가에 대해 질문을 하는 것입니다.

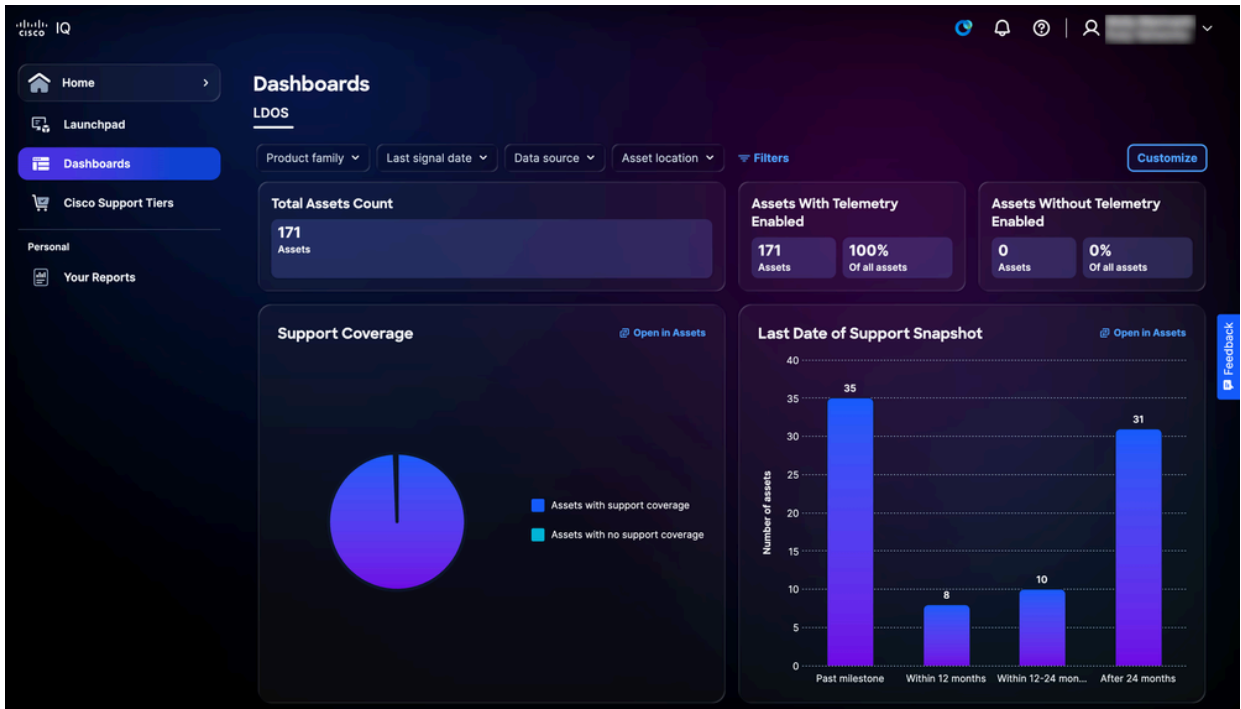
Cisco IQ [AI Assistant 사용](#)에 대한 자세한 내용은 AI Assistant를 참조하십시오.

대시보드

Dashboards 탭은 Cisco IQ에서 사용 가능한 다음 대시보드의 보기를 제공합니다.

LDOS 대시보드


LDOS 대시보드는 LDOS 메트릭스에 대한 포괄적이고 세부적인 정보를 제공하여 고객 가시성을 높이고, 사용자가 위험을 사전 대응적으로 관리할 수 있도록 하며, 보다 효율적이고 정확한 의사 결정을 지원합니다.




LDOS 대시보드

LDOS 대시보드에 대한 뷰 필터링

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

 참고: 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다.

 참고: 사용자의 역할 및 권한에 따라 서로 다른 필터를 사용할 수 있습니다.

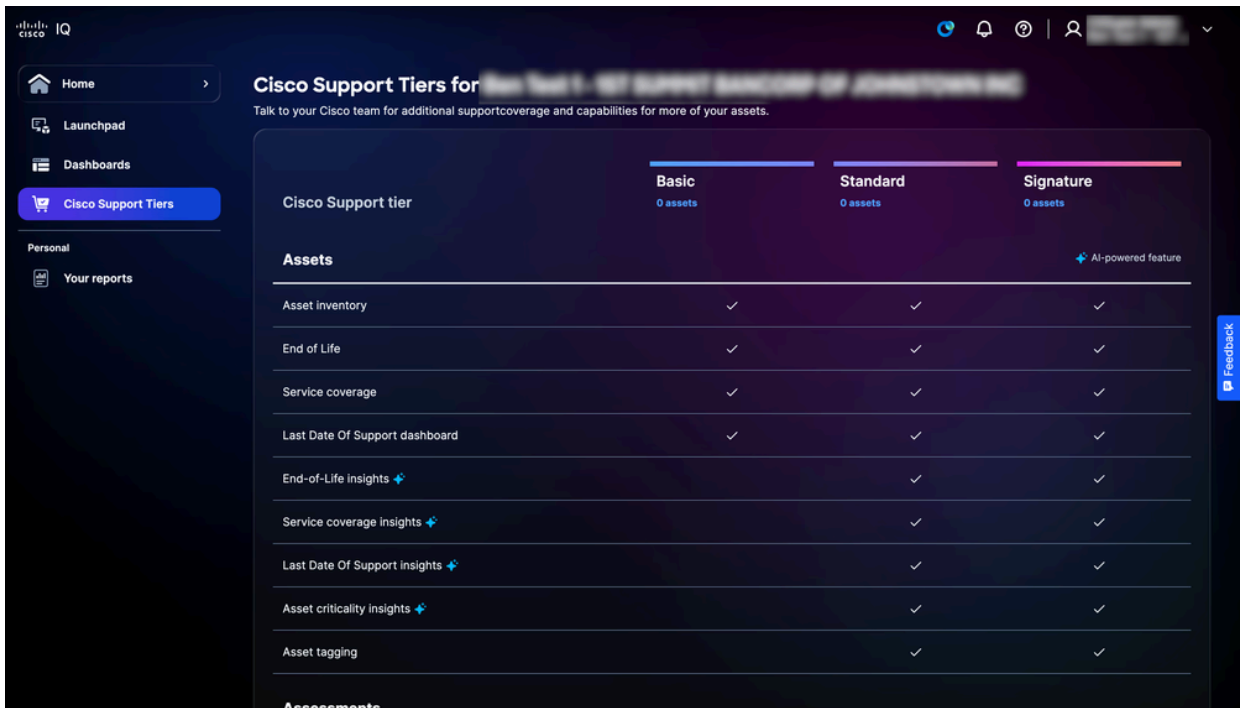
LDOS 대시보드에 대한 세부 정보 보기

Assets에서 Open(열기)을 클릭하면 페이지가 Inventory(인벤토리) 페이지로 리디렉션됩니다. 자세

한 [내용](#)은 인벤토리를 참조하십시오.

Cisco 지원 계층

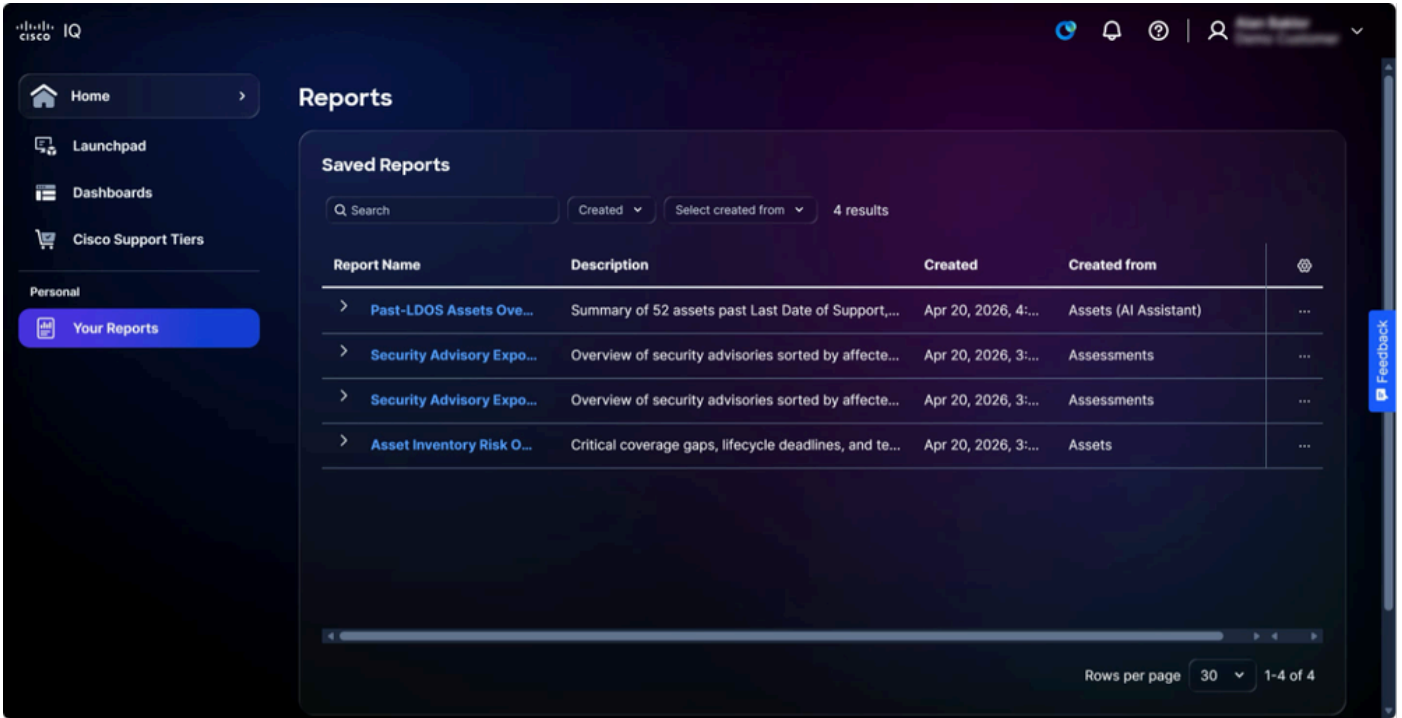
Cisco Support Tiers(Cisco 지원 계층) 페이지에서는 구매한 지원 계층에 사용할 수 있는 기능 및 연결된 지원 계약과 관련된 자산 수를 간략하게 살펴볼 수 있으므로, 포함된 지원 기능을 쉽게 이해하고 관리 및 검토하기 위한 조치를 취할 수 있습니다. 지원 [계층 기능](#)에 대한 자세한 내용은 지원 계층을 참조하십시오.



Cisco 지원 계층

보고서


보고서 기능을 사용하면 Cisco IQ에서 생성된 AI 정보를 개인 설정된 Your Reports 목록에 저장하여 중앙에서 관리할 수 있으므로 자신의 데이터에 빠르고 안전하게 액세스할 수 있습니다.



보고서

시스템 설정

System Settings(시스템 설정) 메뉴로 이동하려면 Home(홈) > System Settings(시스템 설정)를 선택합니다. Account Details(어카운트 세부 정보) 페이지가 표시됩니다.

 참고: 시스템 설정은 계정 관리자만 사용할 수 있습니다.

어카운트 세부 정보

시스템 설정 기능은 손쉬운 관리, 액세스 제어 및 데이터 할당을 지원하여 계정 관리자의 포괄적인 가시성과 액세스를 보장합니다. Account Details(어카운트 세부 정보) 페이지를 볼 때 Details(세부 정보) 섹션에는 다음 정보가 표시됩니다.

- 계정 이름
- 계정 유형
- 데이터 저장 영역
- 사용자
- 작성 날짜

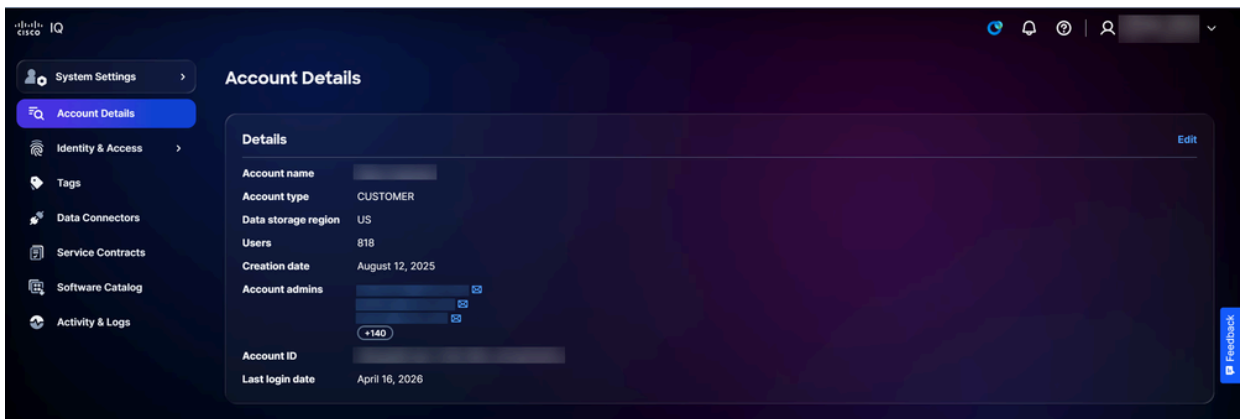
- 계정 관리자
- account id
- 마지막 로그인 날짜

계정 이름 수정

Account Details(어카운트 세부사항) 페이지에서 어카운트 이름만 변경할 수 있습니다.

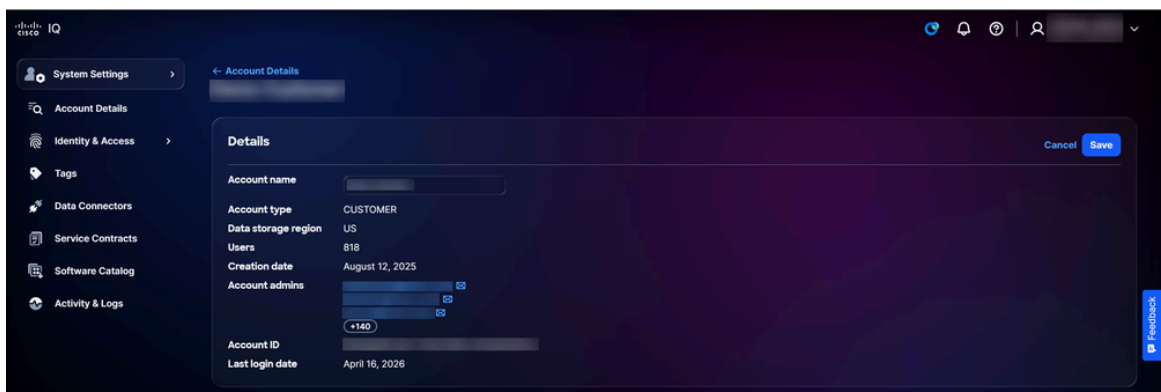
 참고: 데이터 저장소 영역과 같은 필드를 변경하려면 새 회사 계정을 만들어야 합니다.

계정 이름을 수정하려면



어카운트 세부 정보

1. Edit를 클릭합니다.



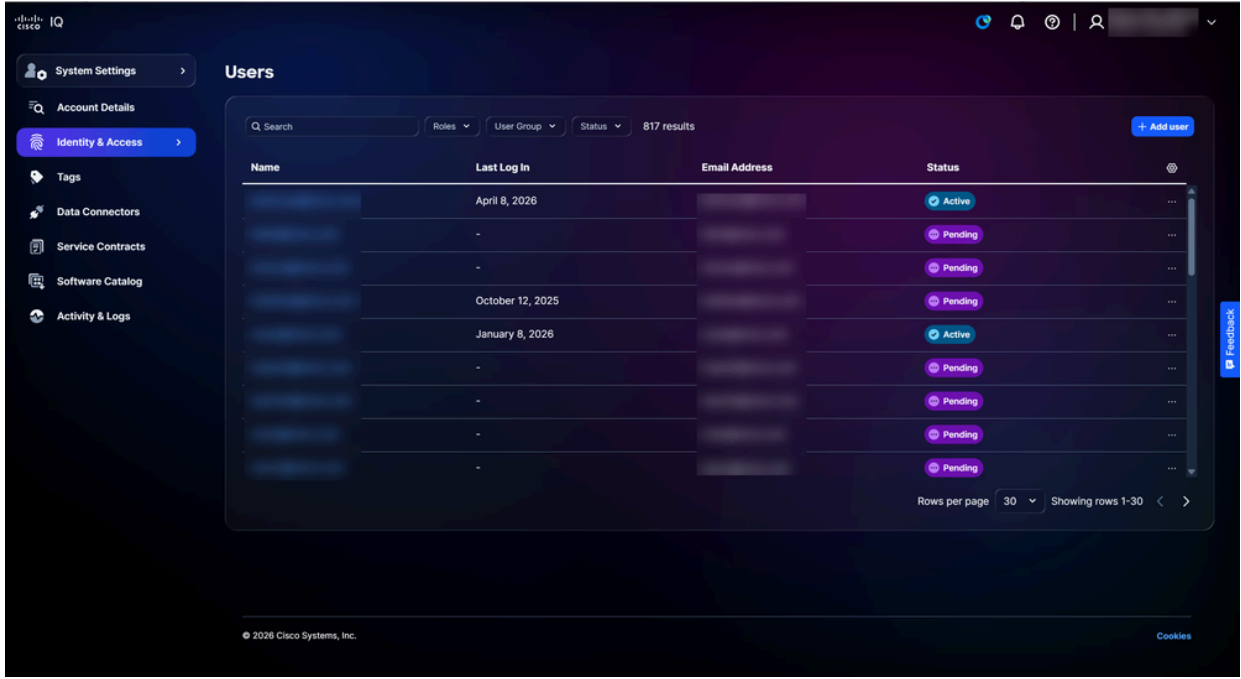
계정 이름 편집

2. 어카운트 이름을 수정합니다.

3. 저장을 클릭합니다.

사용자

사용자 계정은 Users(사용자) 페이지에서 생성, 수정 및 삭제됩니다. Users(사용자) 페이지로 이동하려면 System Settings(시스템 설정) > Identity & Access(ID 및 액세스) > Users(사용자)를 선택합니다. Users(사용자) 페이지가 표시됩니다.




사용자

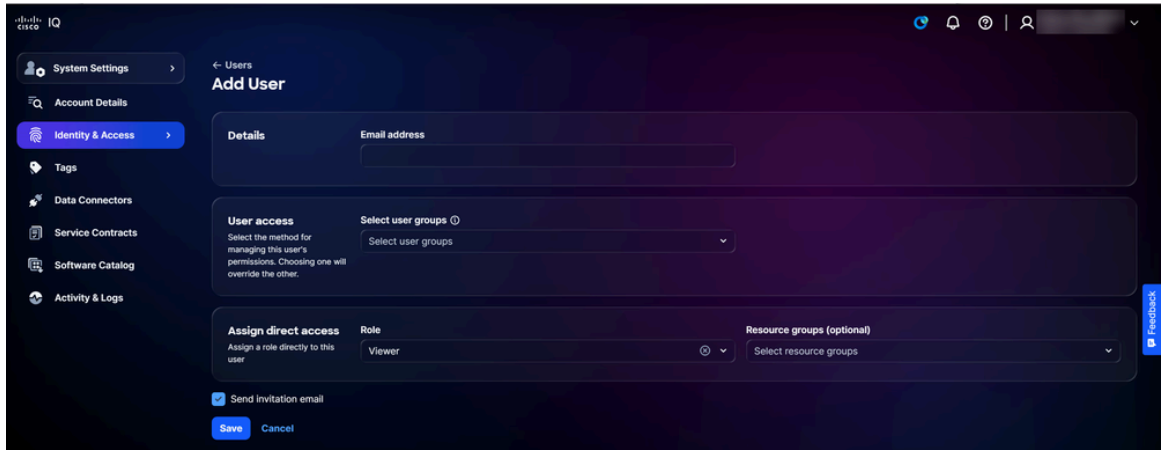
페이지 상단의 필드를 사용하여 목록을 좁히려면 검색 및 필터링할 수 있습니다.

새 사용자 추가

새 사용자를 추가하려면


 참고: 계정 관리자 또는 다른 인증된 사용자만 새 사용자를 추가할 수 있습니다.

1. Users(사용자) 페이지에서 Add User(사용자 추가)를 클릭합니다. Add User(사용자 추가) 페이지가 표시됩니다.




사용자 추가

2. 이메일 주소를 입력합니다.
3. 선택적으로, 사용자 그룹 선택 드롭다운 목록에서 사용자 그룹을 선택합니다.
4. 드롭다운 목록에서 역할을 선택합니다.

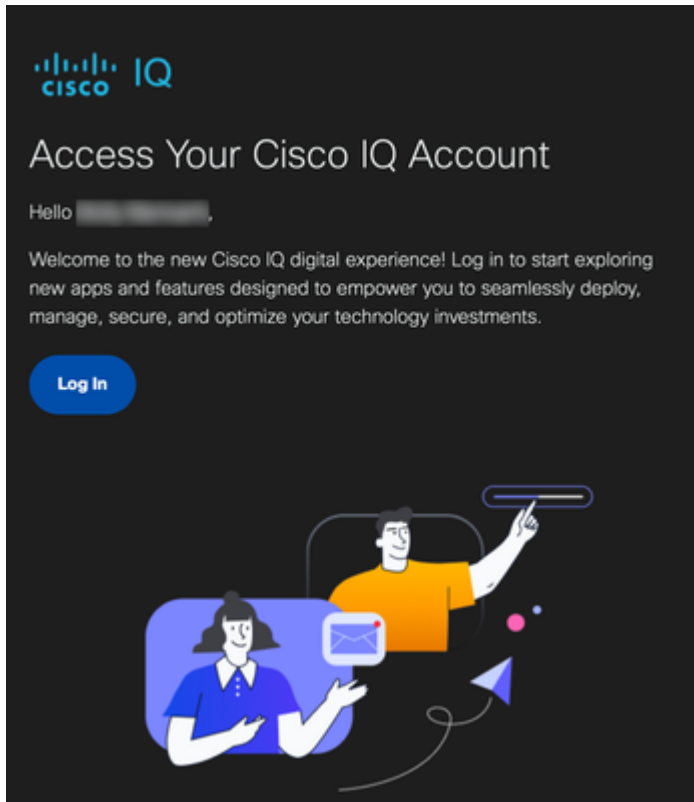
 참고: 사용자는 역할이 있는 하나 이상의 사용자 그룹에 속하거나 하나 이상의 역할이 할당되어야 합니다.

5. 선택적으로, 드롭다운 목록에서 리소스 그룹을 선택합니다.

 참고: 자원 그룹 드롭다운 목록은 선택한 역할에 대해서만 표시됩니다.

6. Send invitation email(초대 이메일 보내기) 확인란이 선택되어 있는지 확인합니다.
7. 저장을 클릭합니다. Users(사용자) 페이지에 확인 메시지가 표시됩니다.

사용자는 계정 관리자의 초대를 받은 후 이메일을 받습니다.

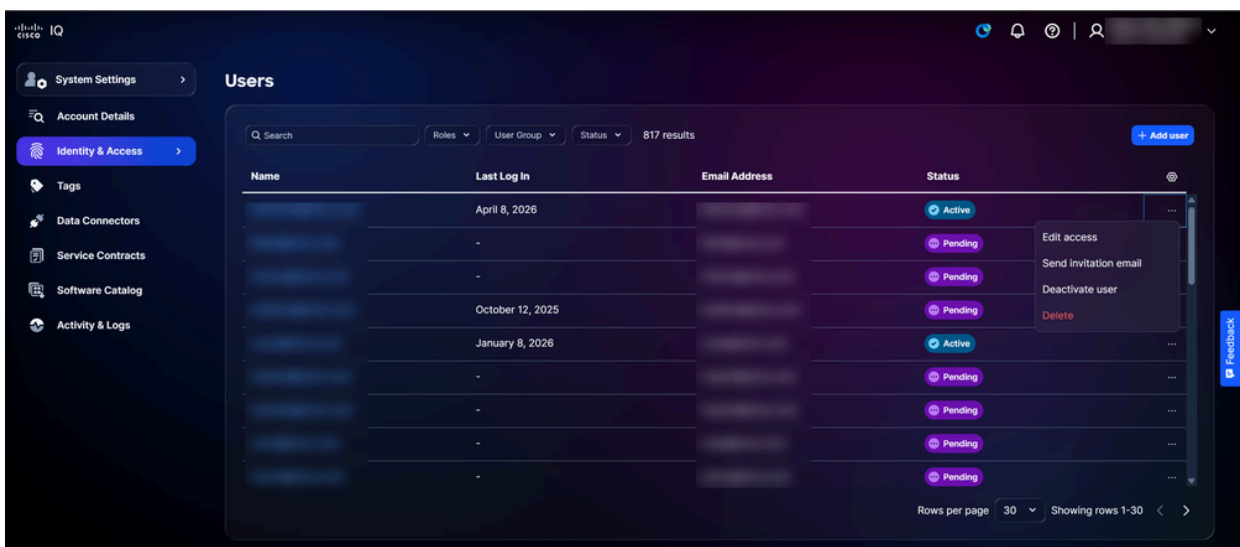


이메일 초대장

초대된 사용자는 이메일에서 Log In(로그인)을 클릭하여 계정에 로그인할 수 있습니다. 로그인 후 사용자의 상태가 Active(활성)가 됩니다.

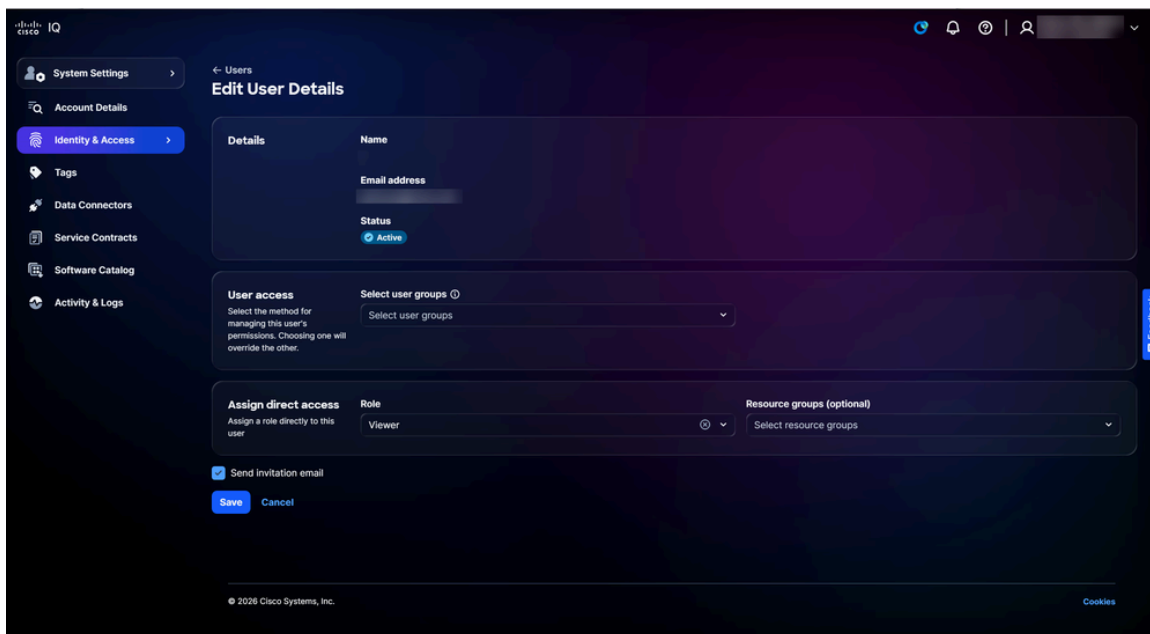
사용자 액세스 수정

사용자 계정의 사용자 그룹, 역할 또는 자원 그룹을 수정하려면




접속 권한 편집

1. Users(사용자) 페이지의 원하는 사용자에서 More Options(추가 옵션) 아이콘 > Edit access(액세스 수정)를 선택합니다. Edit User Details(사용자 세부사항 편집) 페이지가 표시됩니다.



사용자 세부 정보 편집

2. 원하는 사용자 그룹, 역할 및 리소스 그룹을 편집합니다.

 참고: 자원 그룹은 선택한 역할에 대해서만 표시됩니다.

3. 저장을 클릭합니다.

초대 이메일 보내기

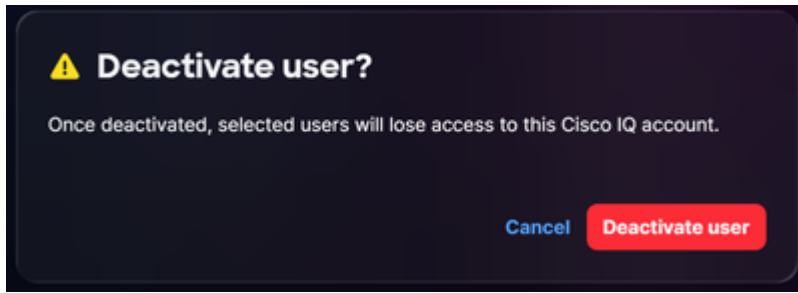
기존 사용자 계정에 초대 이메일을 보내려면

1. Users(사용자) 페이지로 이동합니다.
2. 원하는 사용자의 More Options(추가 옵션) 아이콘 > Send invitation email(초대 이메일 보내기)을 선택합니다. 확인 메시지가 표시됩니다.

사용자 비활성화

사용자 계정을 비활성화하려면


1. Users(사용자) 페이지의 원하는 사용자에서 More Options(추가 옵션) 아이콘 > Deactivate user(사용자 비활성화)를 선택합니다. Deactivate user(사용자 비활성화) 창이 열립니다.



사용자 비활성화 확인

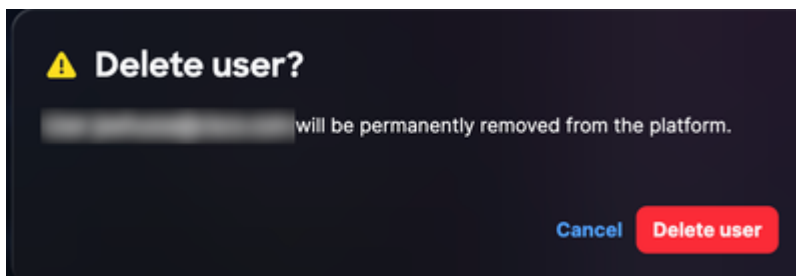
2. Deactivate user(사용자 비활성화)를 클릭하여 확인합니다. 확인 메시지가 표시됩니다.

사용자 삭제

 경고: 사용자 삭제는 되돌릴 수 없습니다.

사용자를 삭제하려면

1. Users(사용자) 페이지의 원하는 사용자에서 More Options(추가 옵션) 아이콘 > Delete(삭제)를 선택합니다. 사용자 삭제 창이 열립니다.



사용자 삭제 확인

2. 사용자 삭제를 클릭합니다. 사용자가 삭제됩니다.

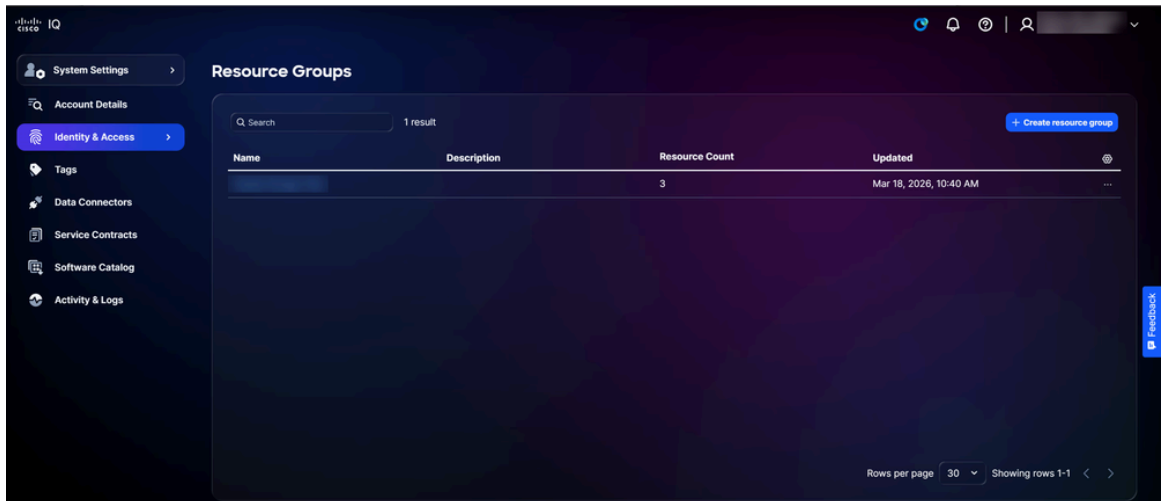
리소스 그룹

리소스 그룹은 유형과 속성을 기준으로 리소스를 지정하는 동적 컬렉션입니다. 리소스 그룹을 구성하면 그룹의 조건을 충족하는 리소스에 대한 역할의 데이터 액세스를 제한할 수 있습니다. 리소스는 여러 리소스 그룹에 속할 수 있습니다. 계정 관리자는 자원 그룹을 작성, 편집 및 삭제할 수 있습니다.

리소스 그룹을 보려면

1. System Settings(시스템 설정) > Identity & Access(ID 및 액세스) > Resource Groups(리소스

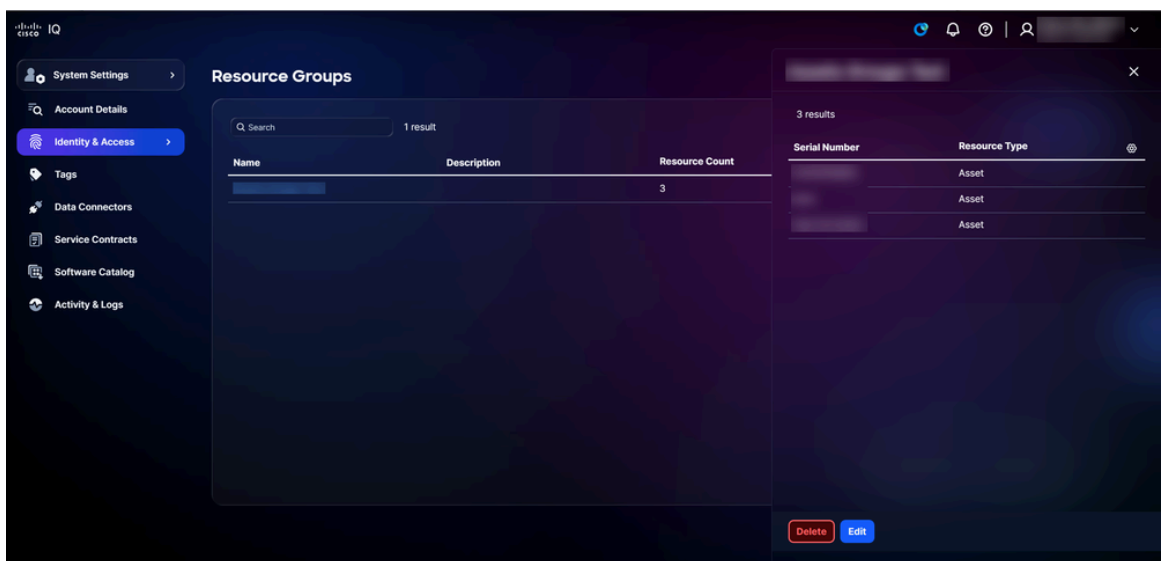
그룹)를 선택합니다. 리소스 그룹 페이지가 표시됩니다.



리소스 그룹

2. Search and Filter(검색 및 필터) 필드를 사용하여 목록의 범위를 좁힙니다.

3. 세부 정보를 표시하려면 리소스 그룹 이름을 클릭합니다.

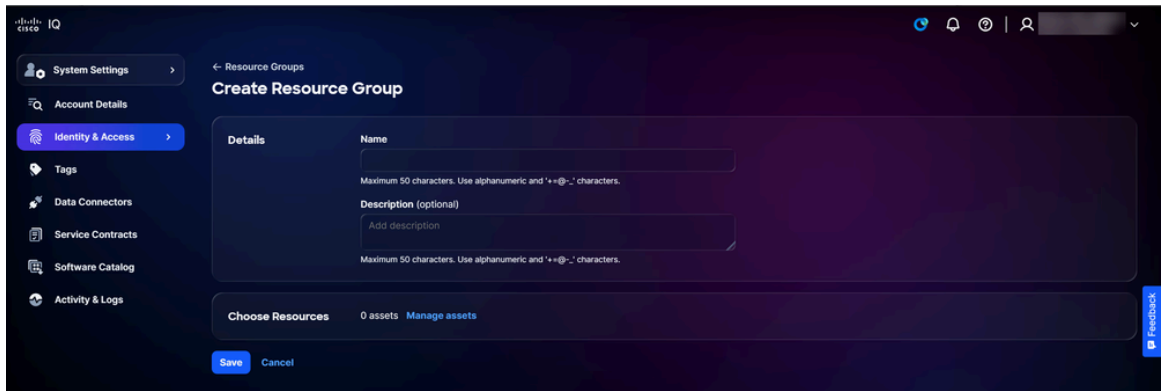


리소스 그룹 세부 정보

리소스 그룹 생성

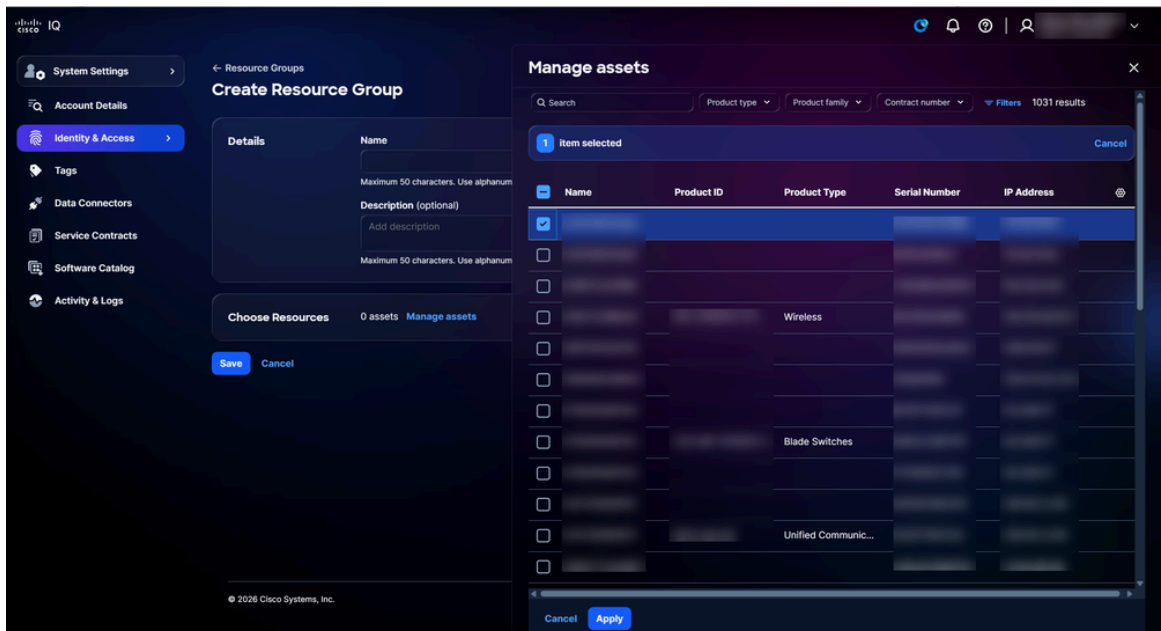
새 리소스 그룹을 생성하려면

1. Resource Groups(리소스 그룹) 페이지에서 Create resource group(리소스 그룹 생성)을 클릭합니다. 리소스 그룹 생성 페이지가 표시됩니다.



리소스 그룹 만들기

2. 자원 그룹의 이름을 입력합니다
3. 선택적으로, 설명을 입력합니다.
4. Manage assets(자산 관리)를 클릭합니다. 자산 관리 창이 열립니다.

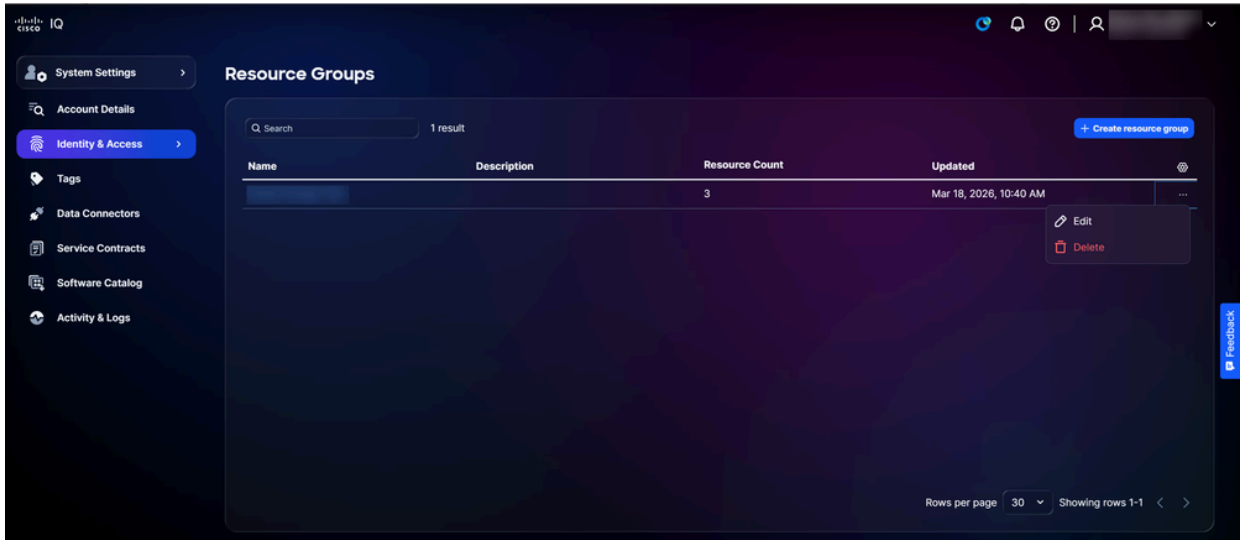


자산 관리

5. 원하는 에셋의 확인란을 선택합니다.
6. 적용을 클릭합니다.
7. 저장을 클릭합니다.

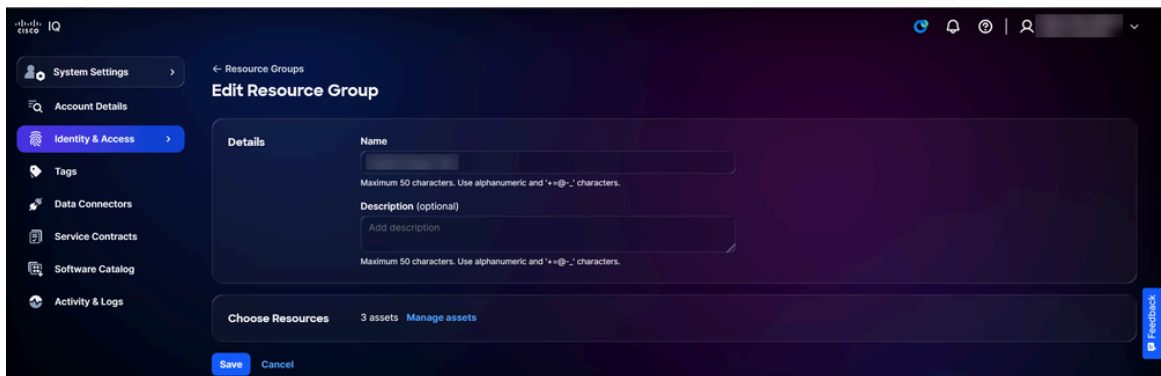
리소스 그룹 수정

리소스 그룹을 수정하려면



편집

1. Resource Groups(리소스 그룹) 페이지의 레코드에서 More Options(추가 옵션) 아이콘 > Edit(수정)를 선택합니다. 리소스 그룹 편집 페이지가 표시됩니다.



리소스 그룹 편집

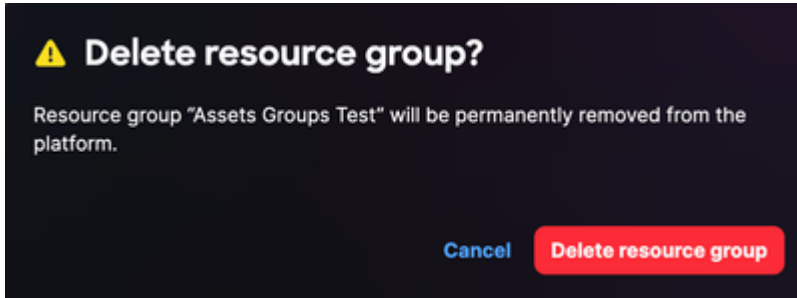
2. 원하는 대로 자원 그룹 속성을 편집합니다.
3. 저장을 클릭합니다.

리소스 그룹 삭제

경고: 리소스 그룹 삭제는 취소할 수 없습니다.

리소스 그룹을 삭제하려면

1. Resource Groups(리소스 그룹) 페이지의 레코드에서 More Options(추가 옵션) 아이콘 > Delete(삭제)를 선택합니다. 자원 그룹 삭제 창이 열립니다.




리소스 그룹 삭제

2. 리소스 그룹 삭제를 클릭합니다. 리소스 그룹이 삭제됩니다.

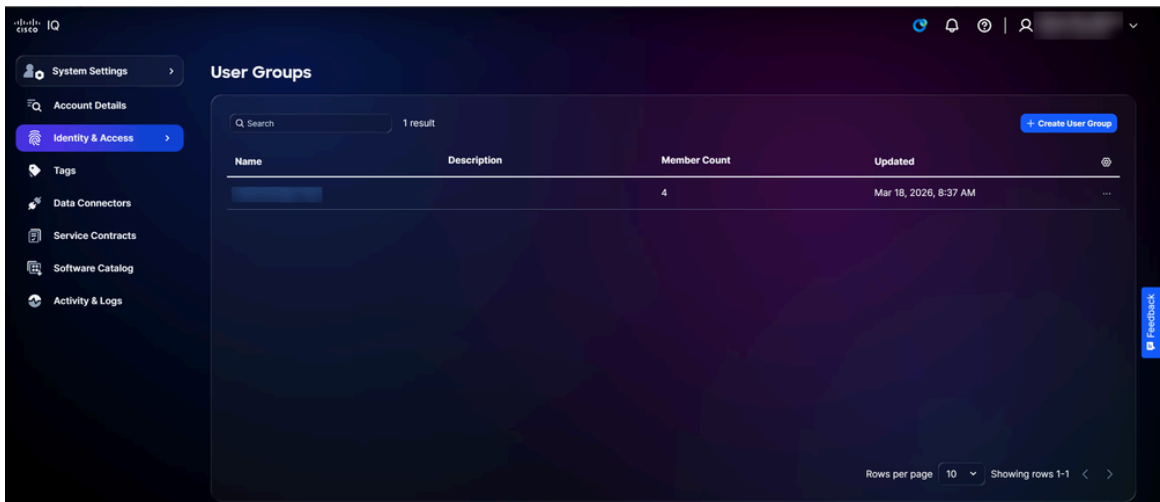
사용자 그룹

사용자 그룹을 사용하면 사용자 그룹을 생성, 편집 및 삭제하여 어카운트 전체에서 사용자를 효과적으로 제어할 수 있습니다.

 참고: All account users 사용자 그룹은 기본적으로 Cisco IQ의 모든 계정에 있으며 삭제하거나 편집할 수 없습니다. 항상 특정 유형의 모든 계정 사용자가 포함됩니다. 그 목적은 계정의 모든 사용자에게 역할을 적용하는 것입니다.

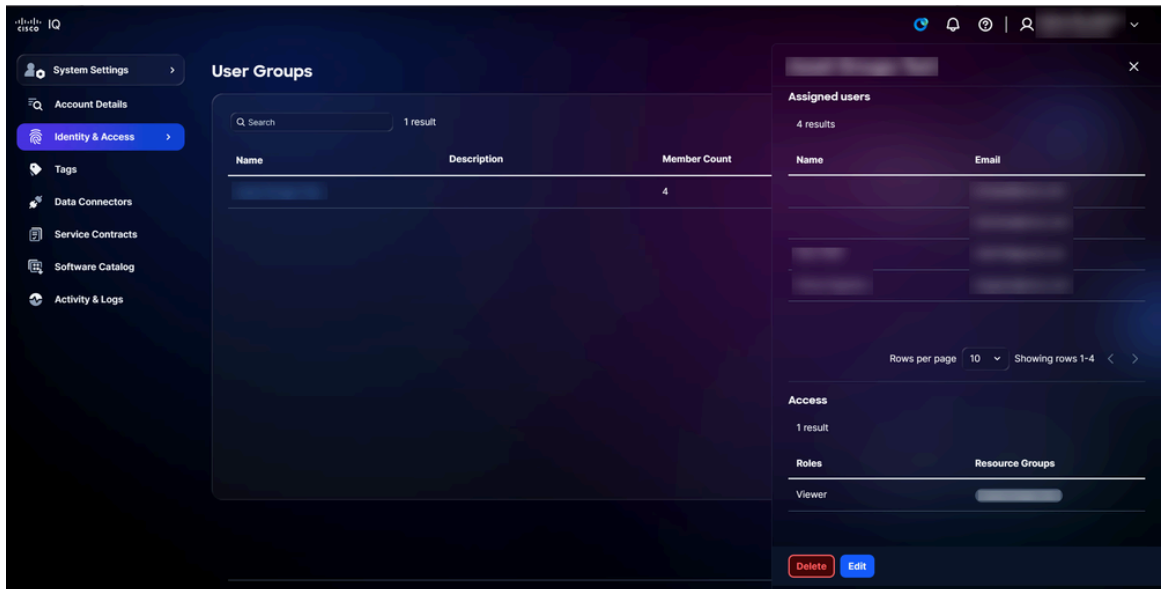
사용자 그룹을 보려면

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



사용자 그룹

2. Search and Filter(검색 및 필터) 필드를 사용하여 목록의 범위를 좁힙니다.
3. 세부 정보를 표시하려면 사용자 그룹 이름을 클릭합니다.

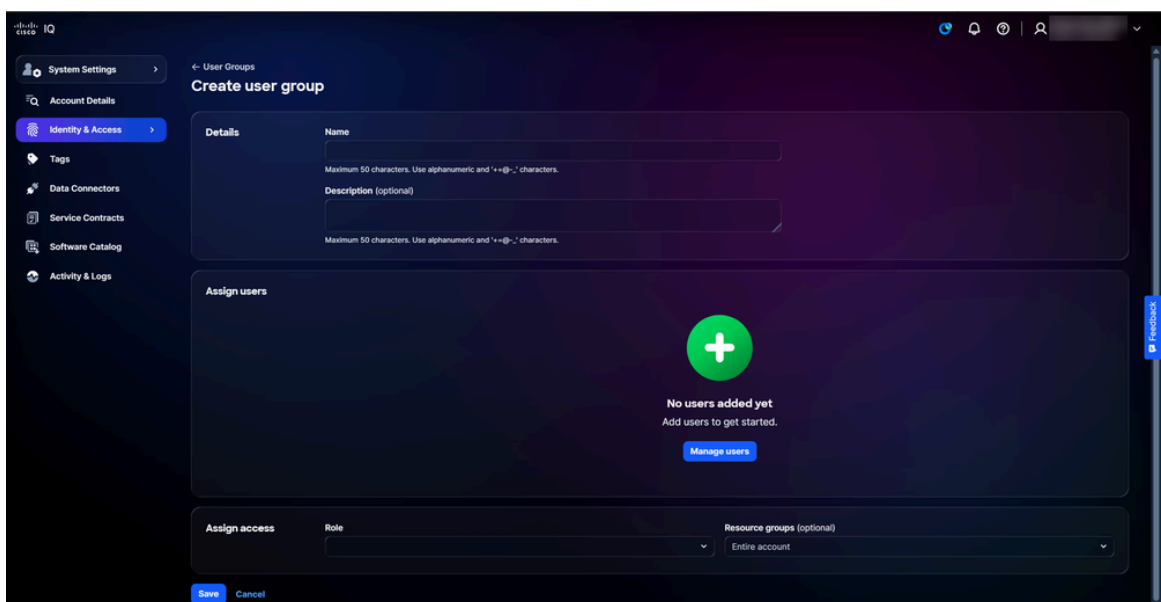


사용자 그룹 세부 정보

사용자 그룹 생성

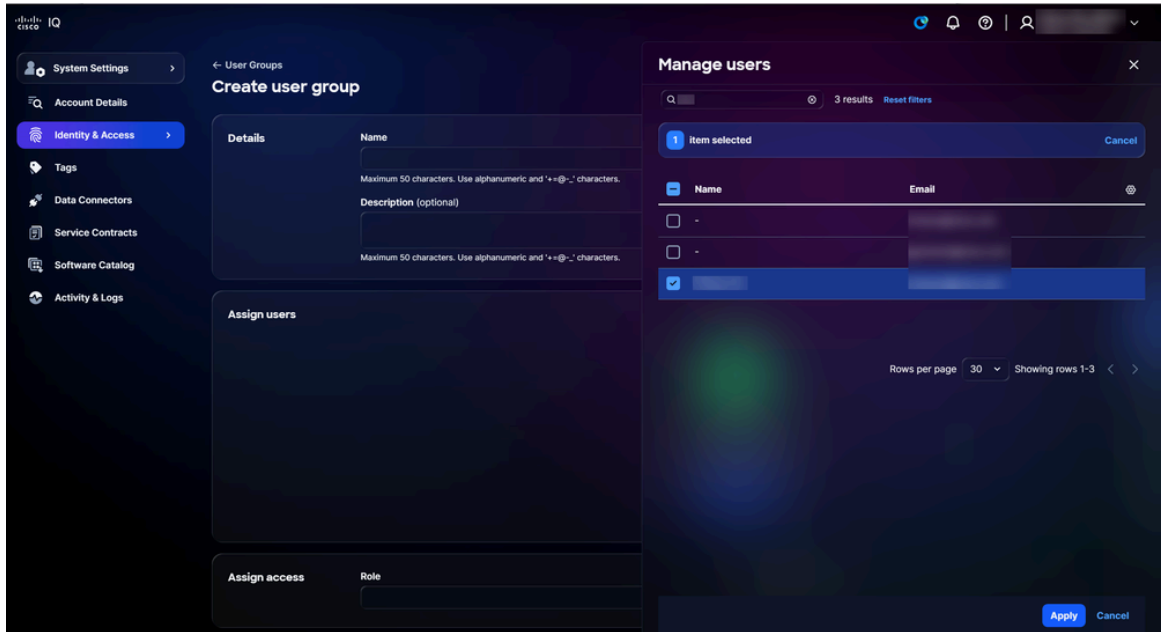
새 사용자 그룹을 생성하려면

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




사용자 그룹 생성

2. 사용자 그룹의 Name을 입력합니다.
3. 선택적으로, 설명을 입력합니다.
4. 사용자 관리를 클릭합니다. 사용자 관리 창이 열립니다.



사용자 관리

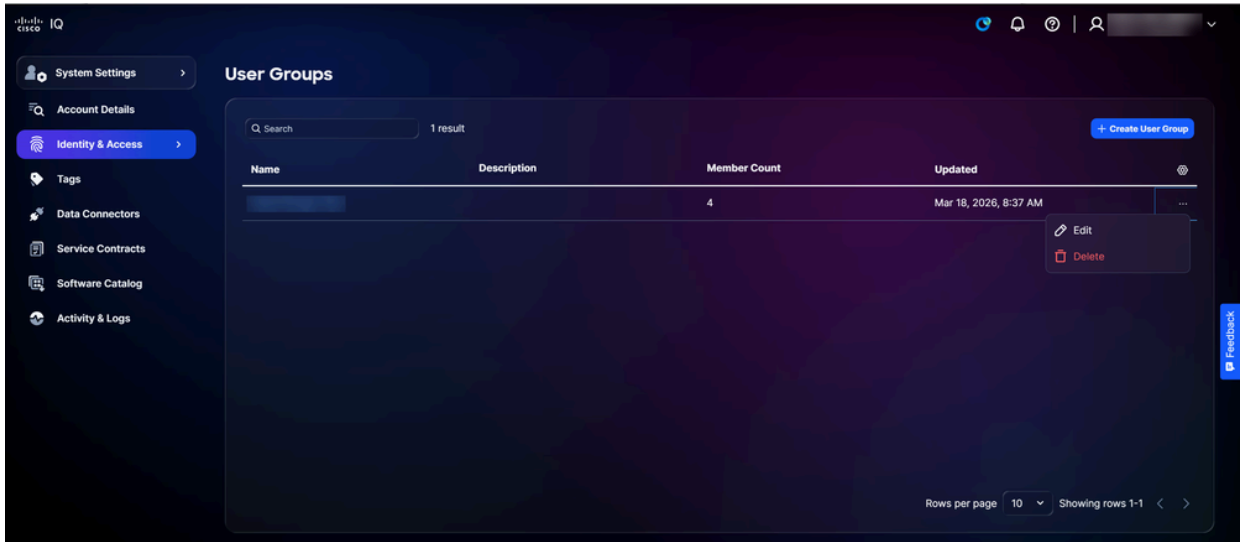
5. 원하는 사용자의 확인란을 선택합니다.
6. 적용을 클릭합니다.
7. 드롭다운 목록에서 역할을 선택합니다.
8. 선택적으로, 드롭다운 목록에서 리소스 그룹을 선택합니다.

 **참고:** 리소스 그룹을 추가하면 사용자 그룹이 액세스할 수 있는 리소스가 제한됩니다. 역할이 할당되었지만 자원 그룹이 선택되지 않은 경우, 역할은 계정의 역할과 관련된 모든 자원에 적용됩니다.

9. 저장을 클릭합니다. 새 사용자 그룹이 사용자 그룹 테이블에 표시됩니다.

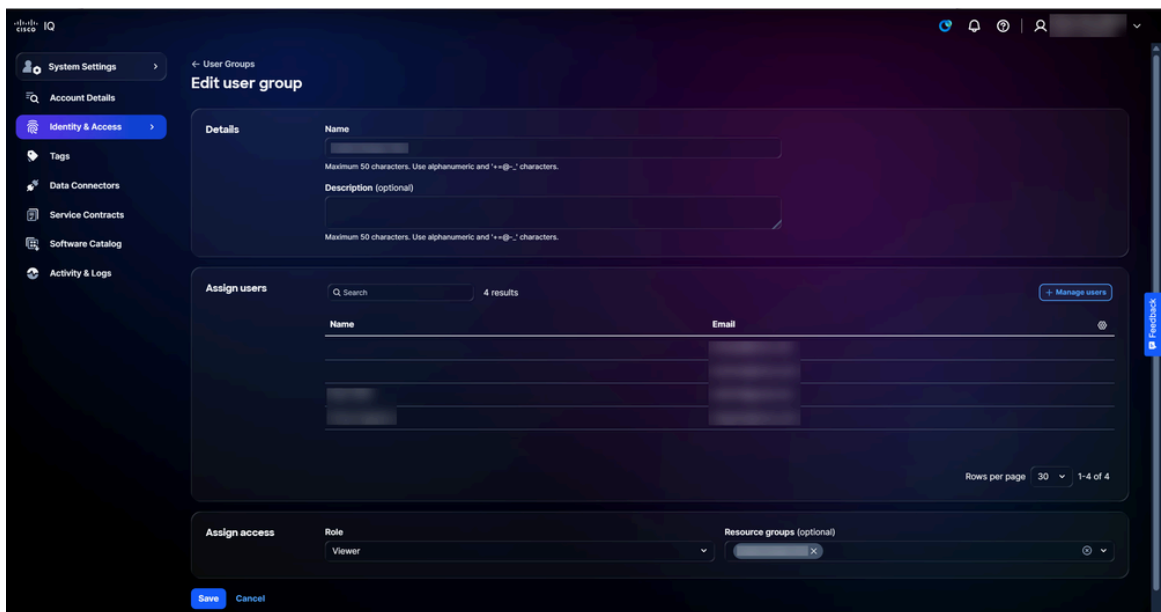
사용자 그룹 수정

사용자 그룹을 수정하려면



편집

1. User Groups(사용자 그룹) 페이지의 레코드에서 More Options(추가 옵션) 아이콘 > Edit(수정)를 선택합니다. 사용자 그룹 편집 페이지가 표시됩니다.



사용자 그룹 편집

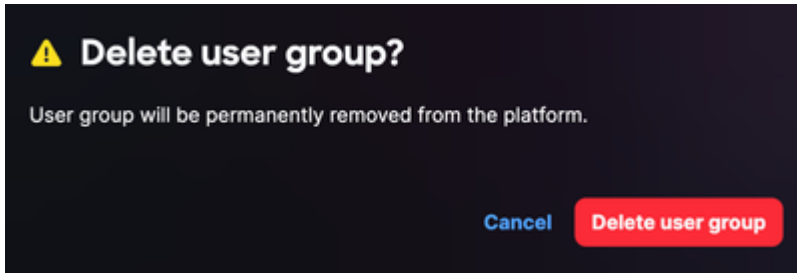
2. 사용자 그룹 특성을 원하는 대로 편집합니다.
3. 저장을 클릭합니다.

사용자 그룹 삭제

⚠ 경고: 사용자 그룹 삭제는 되돌릴 수 없습니다.

사용자 그룹을 삭제하려면

1. User Groups(사용자 그룹) 페이지의 레코드에서 More Options(추가 옵션) 아이콘 > Delete(삭제)를 선택합니다. 사용자 그룹 삭제 창이 열립니다.



사용자 그룹 삭제

2. 사용자 그룹 삭제를 클릭합니다. 사용자 그룹이 삭제됩니다.

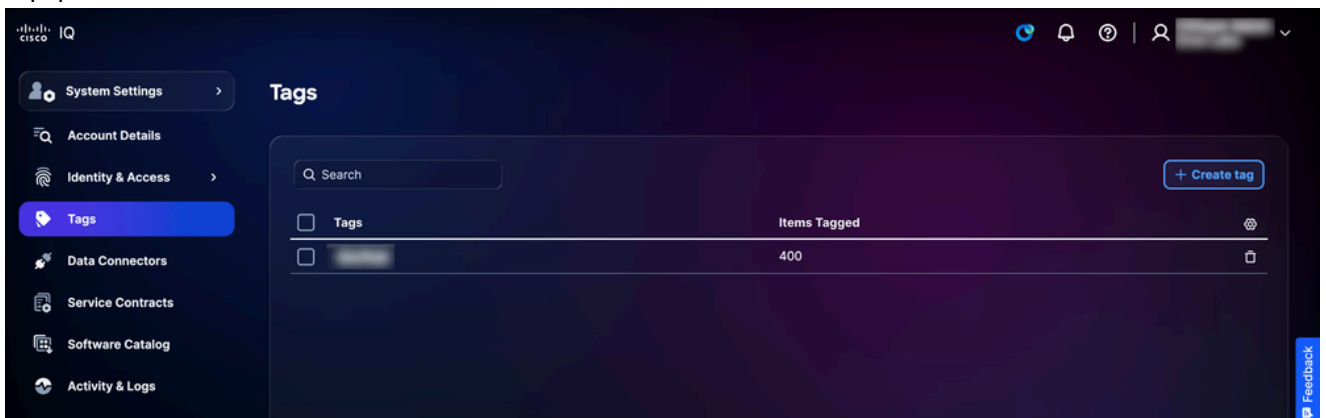
태그

자산 태그는 Cisco IQ의 인벤토리 자산에 할당하는 사용자 지정 라벨입니다. 태그는 사용자가 정의하는 키:값 쌍(예: Environment:Prod 또는 Label:Campus)입니다. 계정 관리자는 태그를 만들고 삭제할 수 있으며 사용자를 자원 그룹에 할당하여 자산 태그를 장치에 할당할 수 있습니다. 리소스 [그룹에 사용자](#)를 할당하는 방법에 대한 자세한 내용은 리소스 그룹을 참조하십시오.

자산 태그 생성

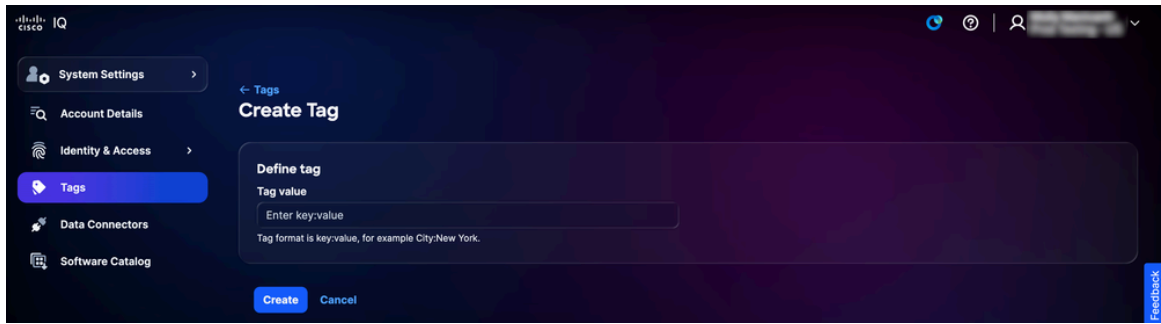
태그를 생성하려면 다음을 수행합니다.

1. Home(홈) > System Settings(시스템 설정) > Tags(태그)를 선택합니다. 태그 페이지가 표시됩니다.




태그

2. 태그 생성을 클릭합니다. 태그 생성 페이지가 표시됩니다.



태그 생성

3. Enter key:value 필드에 태그 값을 입력합니다.

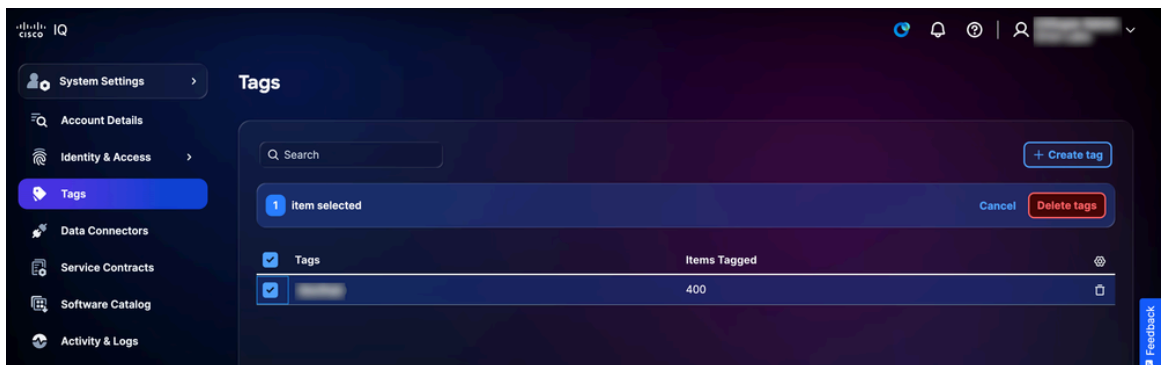
 참고: 태그 이름은 key:value 형식(예: City:NYC)입니다.

4. Create(생성)를 클릭합니다. 새 태그가 태그 페이지의 태그 목록에 표시됩니다.

자산 태그 삭제

태그를 삭제하려면

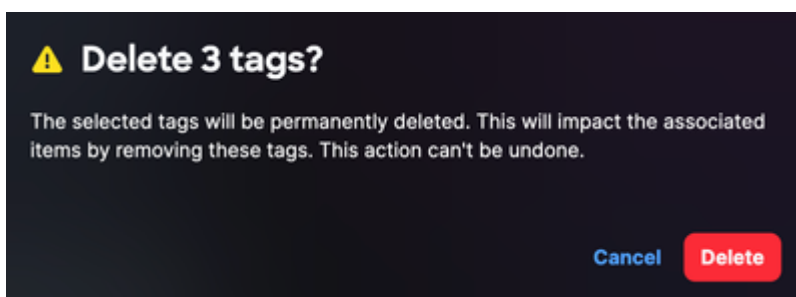
1. Home(홈) > System Settings(시스템 설정) > Tags(태그)를 선택합니다. 태그 페이지가 표시됩니다.



태그

2. 삭제할 태그의 확인란을 선택합니다.

3. 태그 삭제를 클릭합니다. 확인 메시지가 표시됩니다.



4. Delete(삭제)를 클릭하여 확인합니다.

데이터 커넥터

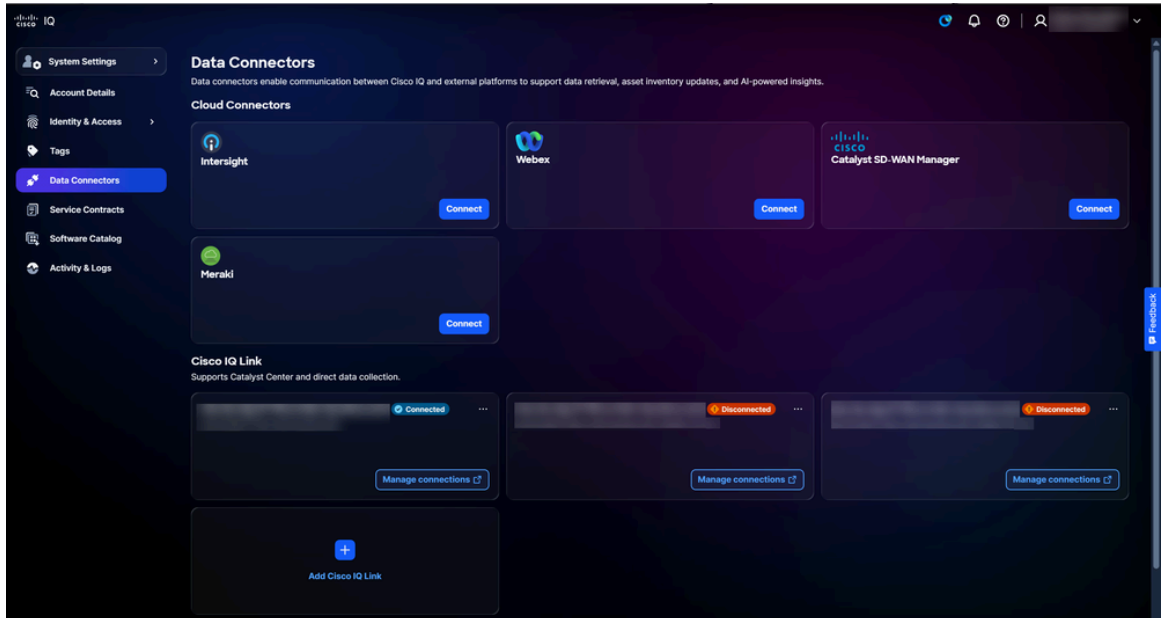
Cisco IQ는 멀티레이어 데이터 수집 접근 방식의 일환으로 데이터 커넥터를 사용하여 포괄적인 네트워크 통찰력을 제공합니다. Data Connectors는 네트워크의 자산으로부터 텔레메트리를 수집하여 Cisco IQ가 관련 통찰력과 신뢰할 수 있는 전문 지식을 제공할 수 있도록 합니다.

클라우드 커넥터 추가

Cisco 클라우드 제품 데이터를 Cisco IQ에 연결하는 것이 강력하고 개별화된 기능을 사용하는 가장 빠른 방법입니다. 다음 제품 컨트롤러에 대한 데이터 연결을 설정한 후 몇 분 이내에 맞춤형 정보를 얻을 수 있습니다. Intersight®, Meraki Dashboard, SD-WAN Manager, Webex® Control Hub

Cisco 클라우드 제품을 연결하려면

1. System Settings > Data Connectors를 선택합니다. 데이터 커넥터 페이지가 표시됩니다.

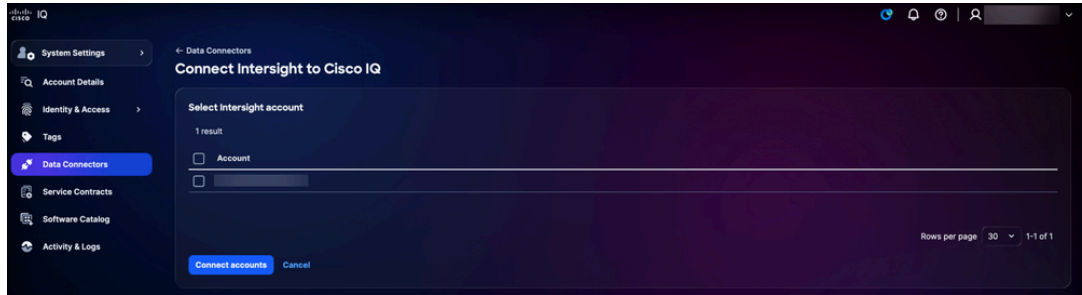


클라우드 커넥터

2. 원하는 클라우드 커넥터에 대해 Connect(연결)를 클릭합니다.

3. 선택한 클라우드 커넥터에 대해 다음 단계를 완료합니다.

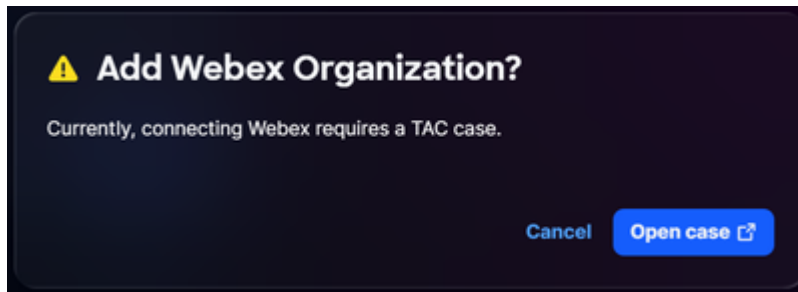
- Intersight



Intersight 연결

1. 원하는 어카운트의 확인란을 선택합니다.
2. Connect accounts(계정 연결)를 클릭합니다. Data Connectors(데이터 커넥터) 페이지로 리디렉션되고 확인 메시지가 표시됩니다.

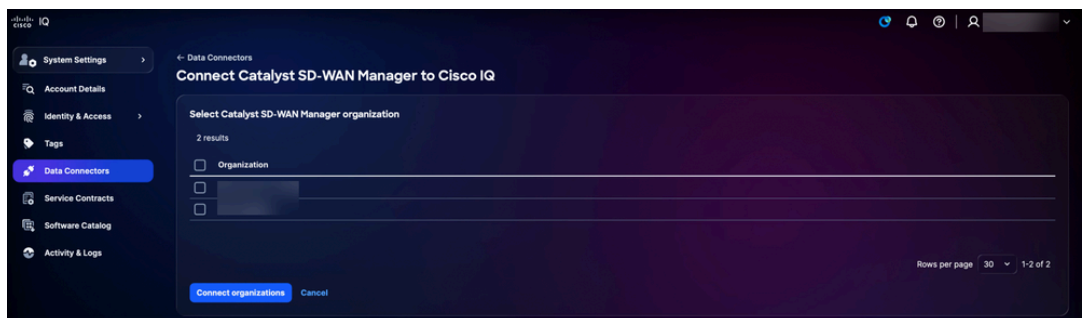
- Webex



Webex 연결

1. Add Webex Organization(Webex 조직 추가) 창에서 Open case(케이스 열기)를 클릭합니다. SCM으로 리디렉션됩니다.
2. SCM에서 지원 사례를 생성합니다.

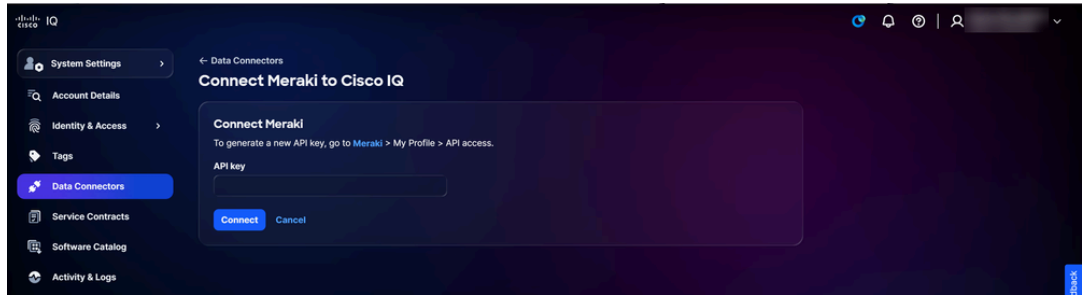
- Catalyst SD-WAN Manager



Catalyst SD-WAN Manager 연결

1. 원하는 조직의 확인란을 선택합니다.
2. Connect organizations(조직 연결)를 클릭합니다. Data Connectors(데이터 커넥터) 페이지로 리디렉션되고 확인 메시지가 표시됩니다.

- Meraki




Meraki 연결

1. 화면의 지침을 따릅니다.
2. API 키를 입력합니다.
3. 연결을 클릭합니다. Data Connectors(데이터 커넥터) 페이지로 리디렉션되고 확인 메시지가 표시됩니다.

Cisco IQ 링크 인스턴스 추가

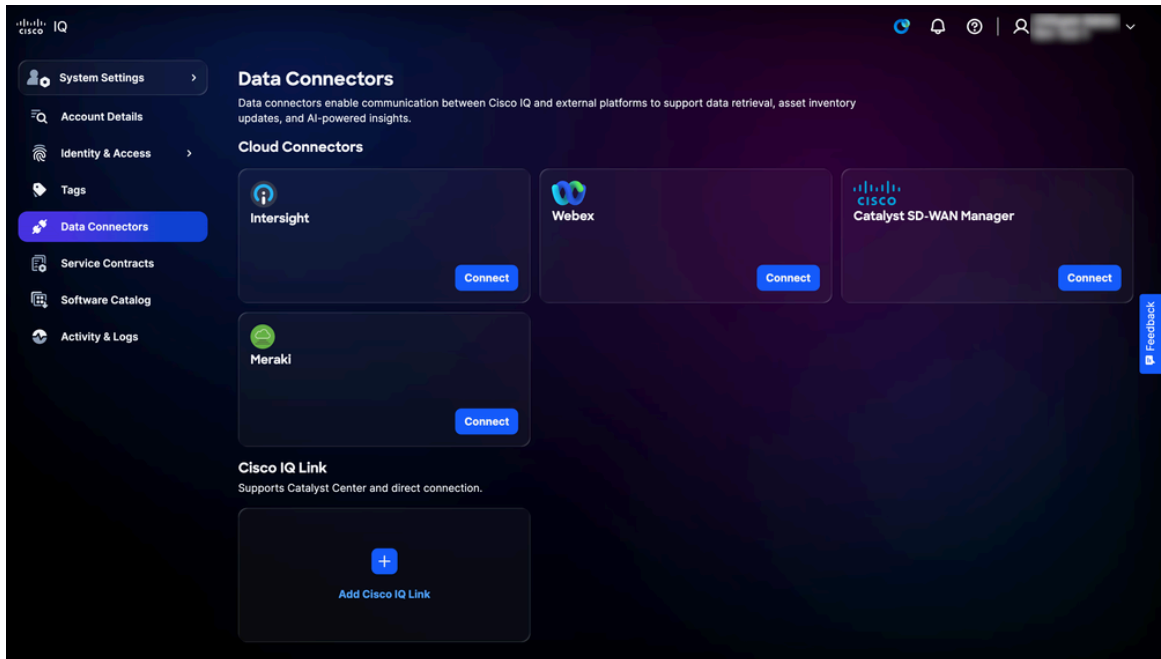
Cisco IQ Link는 Cisco IQ의 온프레미스 구성 요소로, 하드웨어 및 소프트웨어 라이프사이클 및 인벤토리 보고서와 같은 더욱 풍부하고 지능적인 통찰력을 제공하도록 설계되었습니다. 이전 컬렉터를 VM(Virtual Machine)에 설치하는 단일 커넥터로 통합하여 디바이스에서 자세한 텔레메트리 데이터를 수집합니다.

Cisco IQ Link는 자동화된 디바이스 검색 및 텔레메트리 수집을 수행하기 위해 온프레미스 네트워크 내에 구축됩니다. Cisco IQ Link는 Catalyst Center와 직접 연결 및 통합을 지원합니다. 또한 마이그레이션을 통해 계정을 생성한 경우 CX 에이전트 또는 CSPC를 활용하여 텔레메트리를 연결할 수 있습니다.

 참고: 클라우드 매니지드 컨트롤러의 경우 Cisco IQ Link가 필요하지 않습니다. Cisco Cloud를 통해 필요한 데이터에 직접 액세스할 수 있기 때문입니다.

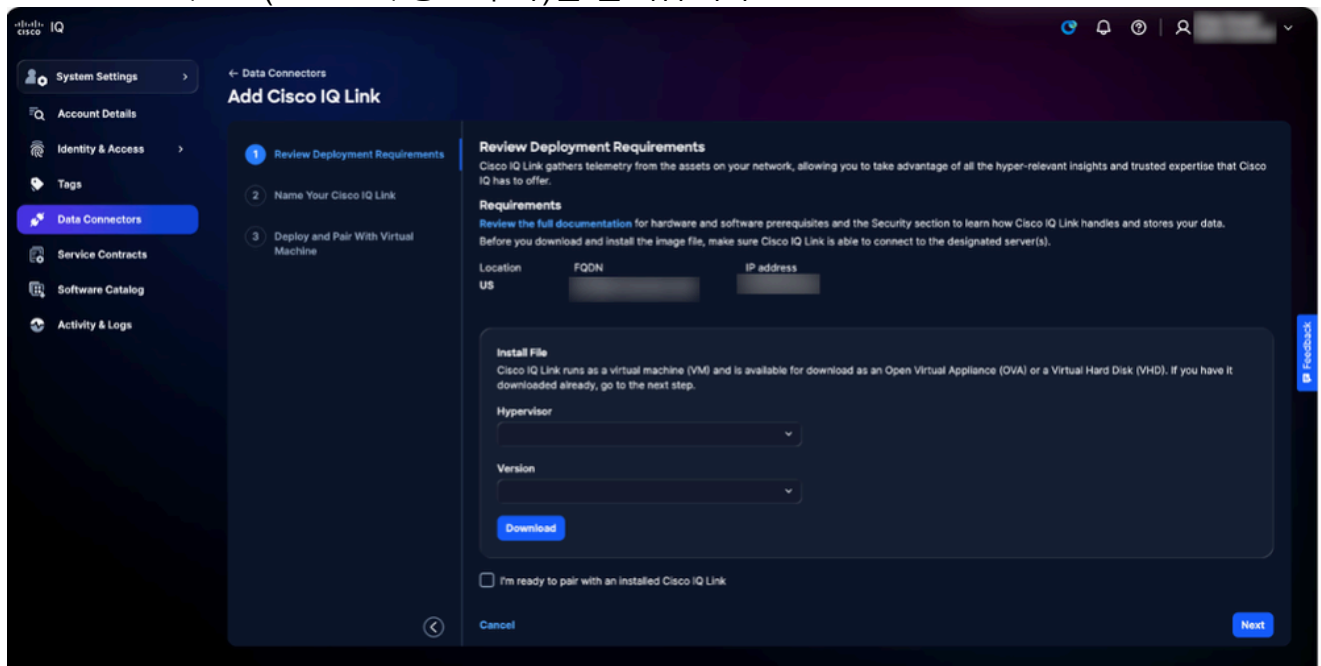
Cisco IQ에 Cisco IQ Link 인스턴스를 추가하려면

1. Data Connectors 페이지로 이동합니다.



Cisco IQ 링크 추가

2. Add Cisco IQ Link(Cisco IQ 링크 추가)를 클릭합니다.



OVA 또는 VHD 다운로드

3. OVA(Open Virtual Appliance) 또는 VHD(Virtual Hard Disk) 다운로드:

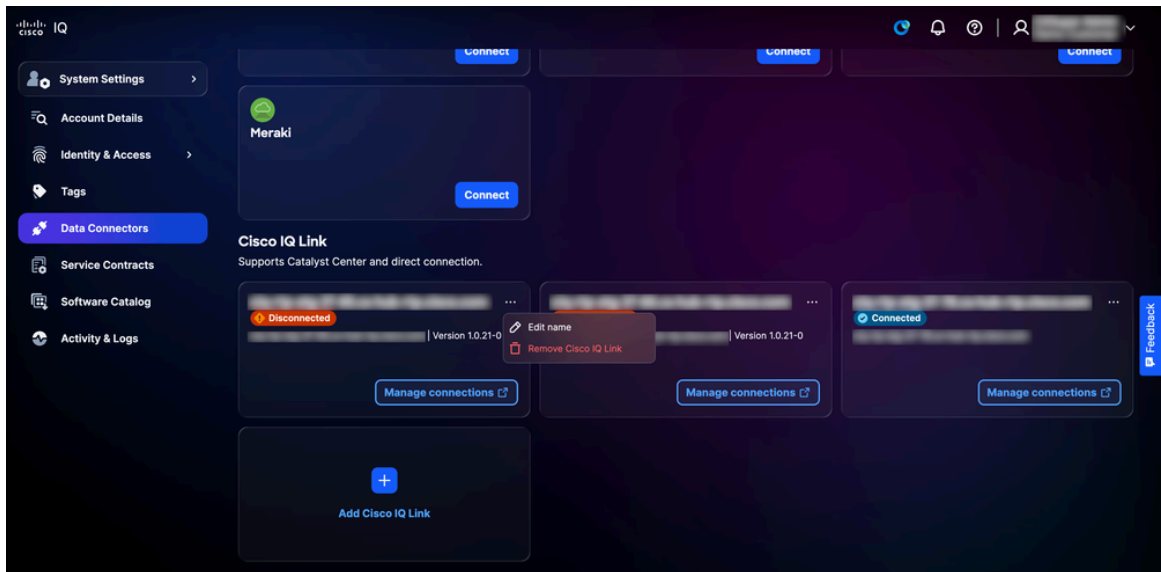
1. 드롭다운 목록에서 하이퍼바이저를 선택합니다.
 2. 드롭다운 목록에서 버전을 선택합니다.
 3. Download(다운로드)를 클릭합니다.
4. [Cisco IQ Link Getting Started Guide](#)에 액세스하려면 전체 [설명서 검토](#)를 클릭합니다. 이 문서에서는 이전 단계에서 다운로드한 파일을 사용하여 Cisco IQ Link를 설치하는 데 필요한 포

괄적인 단계별 지침을 제공합니다. Cisco IQ와 Cisco IQ Link 인터페이스 간의 모든 필수 전환을 포함하여 페어링과 컨피그레이션을 마무리하는 전체 구축 워크플로를 다룹니다.

Cisco IQ 링크 인스턴스 이름 수정

Cisco IQ Link 인스턴스 이름을 수정하려면

1. Data Connectors(데이터 커넥터) 페이지에서 원하는 Cisco IQ Link 인스턴스로 이동합니다.



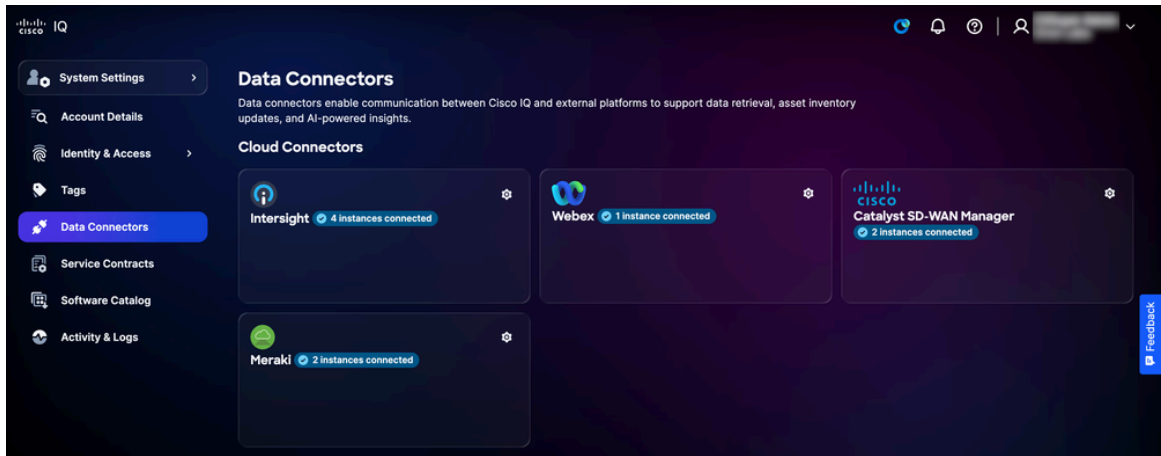
이름 편집

2. 추가 옵션 아이콘 > 이름 편집을 선택합니다.
3. 원하는 대로 이름을 편집합니다.
4. 업데이트를 클릭합니다.

클라우드 커넥터에서 연결된 어카운트 제거

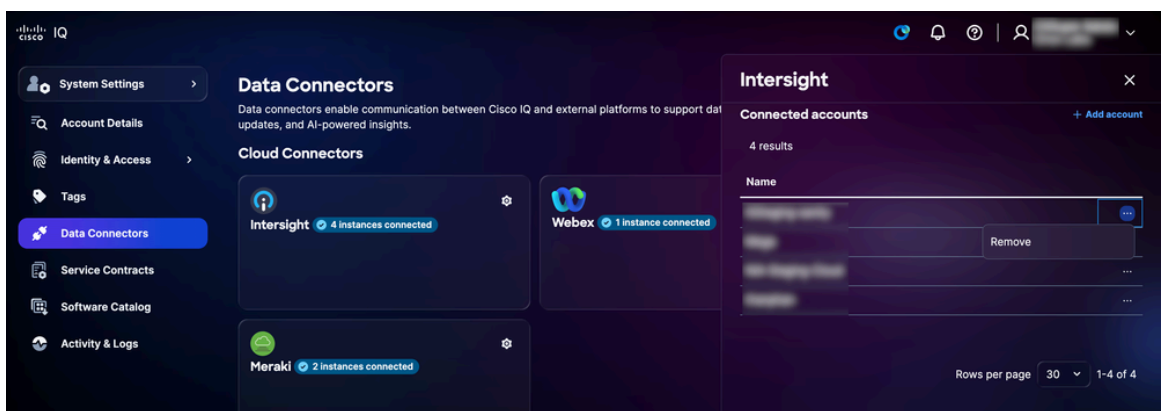
클라우드 커넥터에서 연결된 어카운트를 제거하려면

1. Data Connectors 페이지에서 원하는 클라우드 커넥터로 이동합니다.



클라우드 커넥터 설정

2. Settings(설정) 아이콘을 클릭합니다. Connected Accounts 창이 열립니다.



클라우드 커넥터 연결 계정 제거

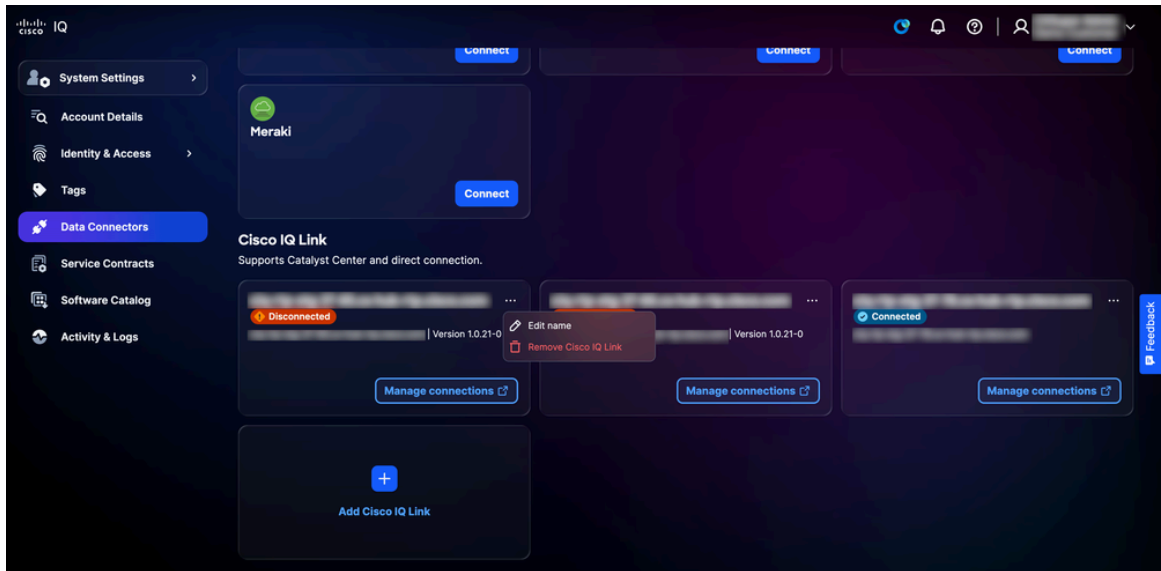
3. 원하는 계정에서 추가 옵션 아이콘 > 제거를 선택합니다. 확인 메시지가 표시됩니다.

4. Remove(제거)를 클릭하여 확인합니다.

Cisco IQ 링크 인스턴스 제거

데이터 커넥터에서 Cisco IQ Link 인스턴스를 제거하려면


1. Data Connectors(데이터 커넥터) 페이지에서 원하는 Cisco IQ Link 인스턴스로 이동합니다.



Cisco IQ 링크 제거

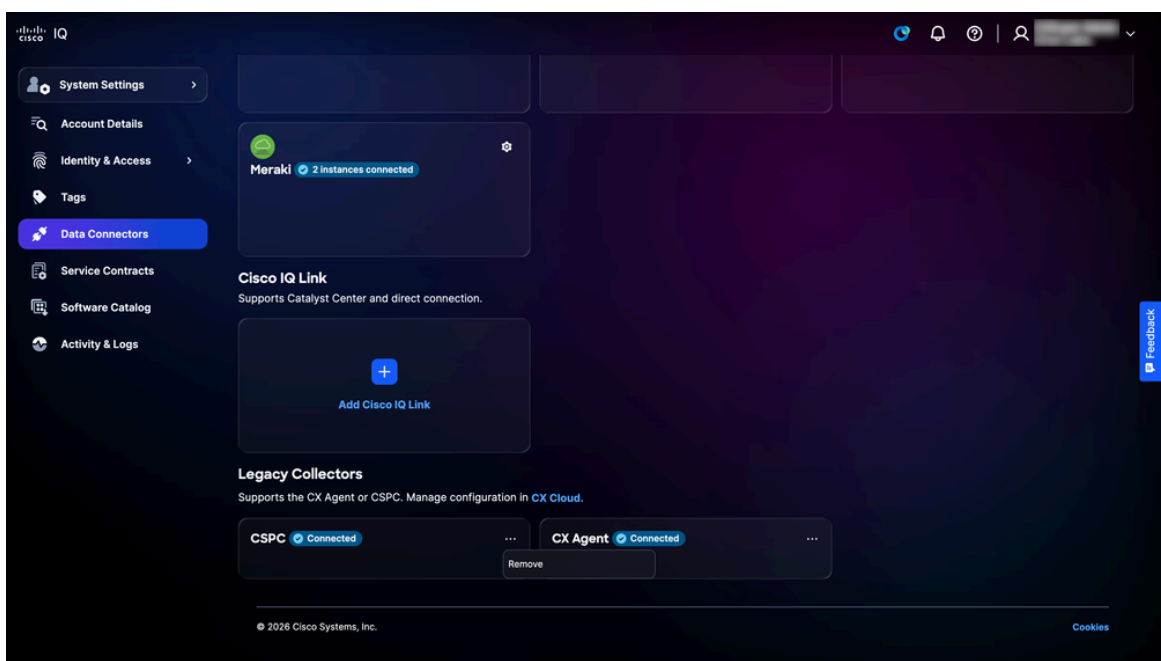
2. 추가 옵션 아이콘 > Cisco IQ Link 제거를 선택합니다. 확인 메시지가 표시됩니다.
3. Cisco IQ Link를 제거하기 위해 지원 케이스를 열려면 Open case(케이스 열기)를 클릭합니다.

레거시 컬렉터 제거

 참고: 레거시 컬렉터는 CX Cloud에서 마이그레이션된 어카운트에만 표시됩니다.

연결된 레거시 커넥터를 제거하려면


1. Data Connectors 페이지에서 원하는 레거시 컬렉터로 이동합니다.



2. 추가 옵션 아이콘 > 제거를 선택합니다. 확인 메시지가 표시됩니다.
3. 기존 컬렉터를 제거하기 위해 지원 케이스를 열려면 Open case(케이스 열기)를 클릭합니다.

서비스 계약

계약을 연결하면 서로 다른 팀 구성원과 연결된 계약의 데이터가 통합되며, 텔레메트리를 통해 인벤토리에 연결되지 않은 장치가 통합되어 지원 커버리지 가시성이 중앙 집중화되고 갱신 문제가 발생하지 않습니다. 계약을 연결하려면 지원 케이스를 여는 데 사용되는 계약 번호가 필요합니다.

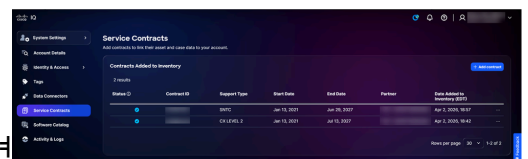
 참고: 계약 번호 지원은 파트너 또는 Cisco 영업 담당자에게 문의하십시오.

서비스 계약의 주요 이점은 다음과 같습니다.

- 조직의 지원 범위에 대한 중앙 집중식 뷰 생성
- 갱신 월을 앞설 수 있는 맞춤형 대시보드
- 텔레메트리 또는 에어 갭(air-gapped) 환경의 일부에 연결되지 않은 자산을 포함하도록 인벤토리 가시성 확장


계약 연결

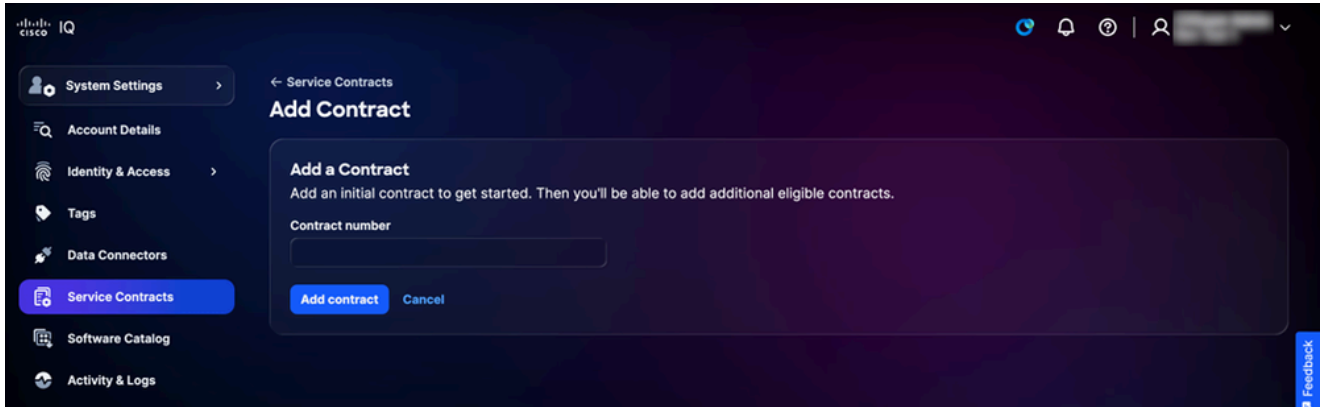
Service Contracts(서비스 계약) 페이지에서 계약을 연결하려면



계약 추가

1. 계약 추가를 클릭합니다. 계약 추가 페이지가 표시됩니다.

 참고: 최초 계약이 어카운트에 추가된 후 추가 계약을 추가할 수 있습니다.



계약 번호 입력

2. 계약 번호를 입력합니다.
3. 계약 추가를 클릭합니다. 계약이 어카운트에 추가됩니다.

소프트웨어 카탈로그

Software Catalog(소프트웨어 카탈로그)에는 사용 가능한 소프트웨어 인스턴스가 표시됩니다. 또한 업데이트를 원활하게 모니터링 및 관리하여 시스템 인스턴스를 효율적으로 추적 및 관리할 수 있습니다.

소프트웨어 카탈로그에 액세스하려면 홈 > 시스템 설정 > 소프트웨어 카탈로그로 이동합니다. 소프트웨어 카탈로그 페이지가 표시됩니다. 이 페이지에서는 사용 가능한 소프트웨어 인스턴스가 링크 컬렉터 가용성 카드로 표시됩니다. 각 링크 컬렉터 가용성 카드에는 소프트웨어 인스턴스의 이름, 설명, 게시자 및 버전이 표시됩니다.

소프트웨어 인스턴스에 대한 세부사항 보기

소프트웨어 인스턴스에 대한 릴리스 정보를 보려면 Details를 클릭합니다. 인스턴스의 최신 릴리스 정보가 포함된 창이 열립니다. 이전 릴리스 정보를 보려면 드롭다운 목록에서 릴리스 버전을 선택합니다.

새 소프트웨어 인스턴스에 대한 패키지 설치


새 인스턴스를 만들기 위해 설치 프로그램을 다운로드하려면

1. 원하는 Link collector availability card(링크 컬렉터 가용성 카드)에서 Download options(다운로드 옵션) > Install packages(패키지 설치)를 선택합니다. 패키지 설치 창이 열립니다.
2. 드롭다운 목록에서 다음 하이퍼바이저 옵션 중 하나를 선택합니다.

- ESXi: 가상 시스템 및
- Hyper-V: Microsoft Hyper-V용
- KVM: Linux 커널 기반 가상 머신(KVM)용

3. 드롭다운 목록에서 버전을 선택합니다.

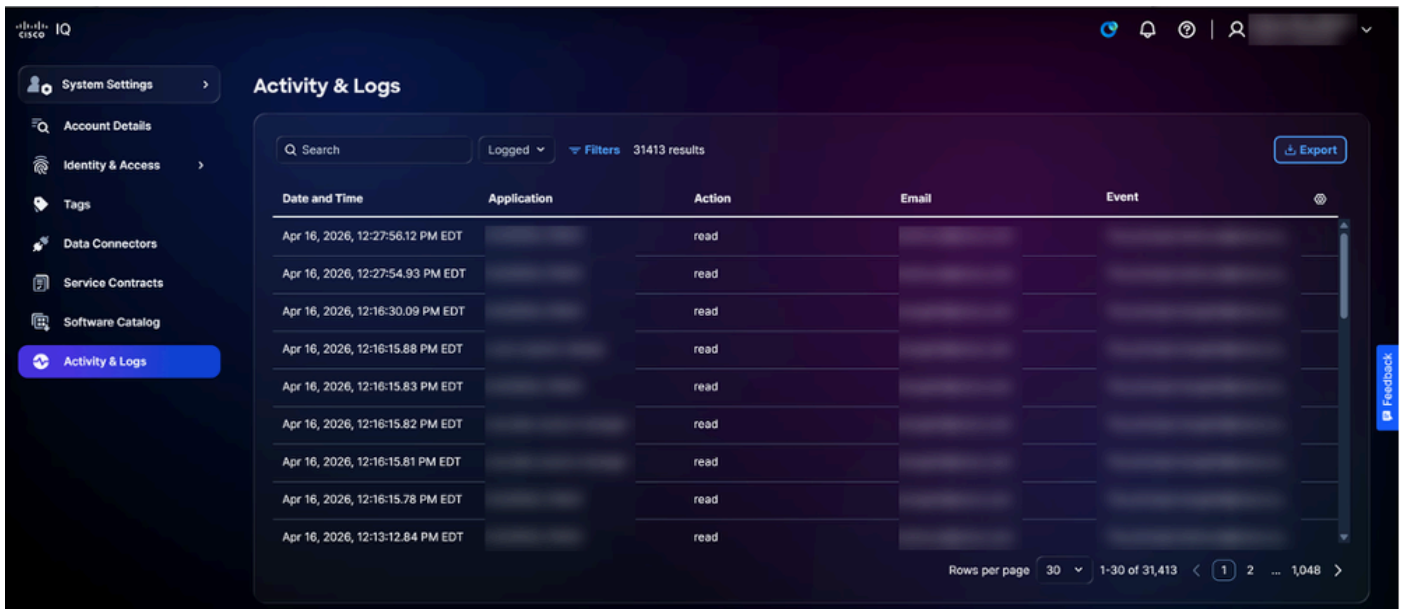
4. 파일을 로컬로 저장하려면 Download(다운로드)를 클릭합니다.

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

5. 데이터 센터에 파일을 구축합니다. 자세한 내용은 [Cisco IQ Link 시작 가이드](#)를 참조하십시오.

활동 및 로그

Activity & Logs 서비스는 규정 준수, 문제 해결 및 모니터링을 위해 Cisco IQ에서 모든 사용자 작업 및 시스템 이벤트를 중앙 집중식으로 추적합니다. 사용자 ID, 타임스탬프, 소스 IP 주소, 영향을 받는 리소스 등 세부 컨텍스트로 인증 이벤트, 권한 부여 결정, 리소스 액세스, 컨피그레이션 변경, 관리 작업에 대한 불변의 감사 레코드를 캡처합니다. Activity & Logs는 보존 정책을 시행하고 시간 범위 검색, 사용자 기반 필터 및 리소스별 활동 추적을 지원하여 감사 이벤트를 유연하게 쿼리하고 필터링할 수 있게 합니다.

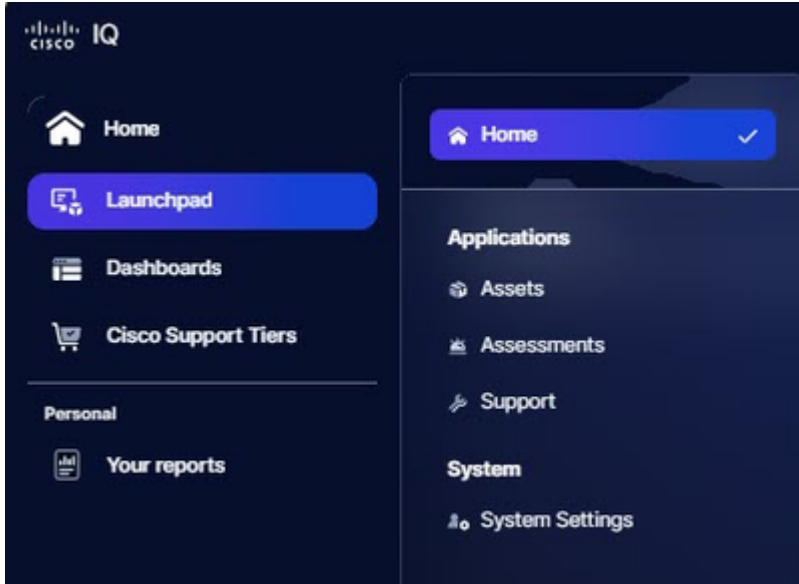


Date and Time	Application	Action	Email	Event
Apr 16, 2026, 12:27:56.12 PM EDT		read		
Apr 16, 2026, 12:27:54.93 PM EDT		read		
Apr 16, 2026, 12:16:30.09 PM EDT		read		
Apr 16, 2026, 12:16:15.88 PM EDT		read		
Apr 16, 2026, 12:16:15.83 PM EDT		read		
Apr 16, 2026, 12:16:15.82 PM EDT		read		
Apr 16, 2026, 12:16:15.81 PM EDT		read		
Apr 16, 2026, 12:16:15.78 PM EDT		read		
Apr 16, 2026, 12:13:12.84 PM EDT		read		

활동 및 로그

자산 애플리케이션

Assets 애플리케이션은 Cisco 자산에 대한 포괄적인 가시성 및 관리 기능을 제공하며 Cisco IQ의 기초가 되어 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 애플리케이션 (예: Assessments 애플리케이션)은 이 데이터를 사용하여 디바이스의 상태 및 보안을 평가하는 것이므로 완전하고 정확한 자산 목록을 유지 관리하는 것이 중요합니다.



홈 메뉴

핵심 개념

Assets 애플리케이션은 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
- 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. 자산 텔레메트리 데이터는 멀티레이어 데이터 파이프라인을 통해 수집 및 보강됩니다.

Assets 애플리케이션 액세스

Cisco IQ의 자산 관리 기능에 액세스하려면 Home 메뉴 > Assets를 선택합니다. Overview(개요) 페이지가 표시됩니다.

자산 개요

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

- Assets
- Overview**
- Inventory
- Service Contracts
- End of Life

Overview

Product family Last signal date Data source Asset location Filters

Ask AI Customize

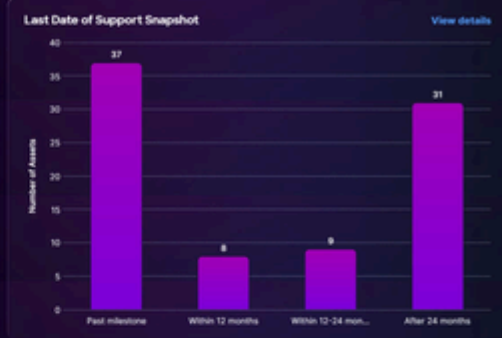
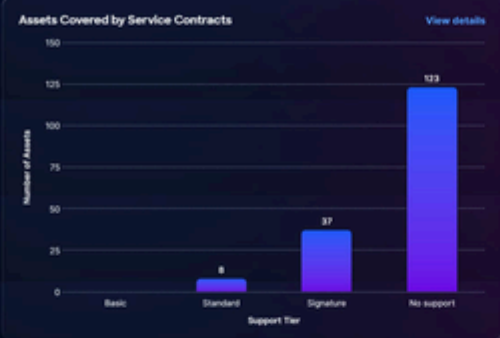
Total Assets 168 Assets

Covered assets 97% of all assets

58 Covered

Uncovered assets 3% of all assets

2 Uncovered



Key Asset Metrics

Assets with telemetry 100% of all assets

168 with telemetry

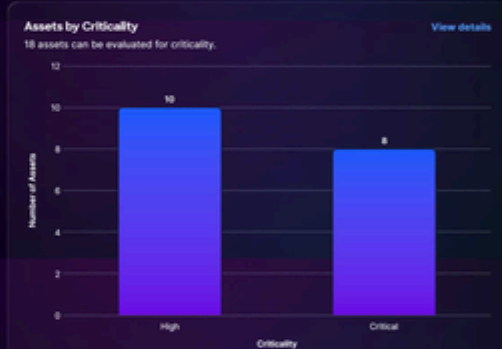
Assets without telemetry 0% of all assets

0 without telemetry

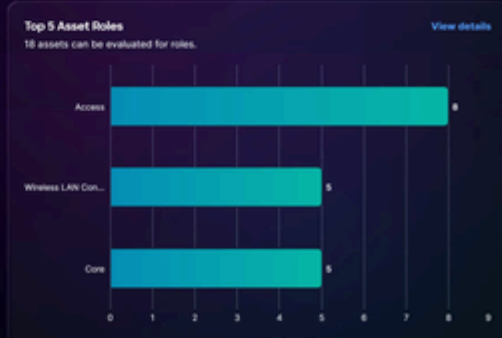
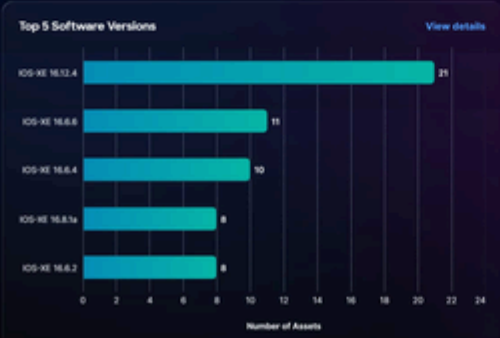
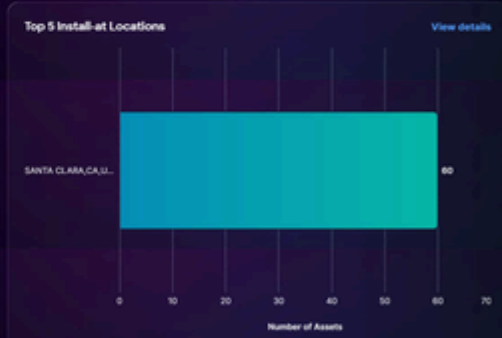
Assets With Critical or High Security Advisories View details

85%

Of the 168 assets with telemetry enabled, 142 have critical or High Security Advisories



Asset Breakdown




대시보드에는 다음 정보가 표시됩니다.

- 총 자산: Cisco IQ 어카운트 내 총 자산 수
- 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
- 주요 자산 메트릭: 텔레메트리 상태, 중요 보안 권고, LDOS 정보와 같은 추가 주요 메트릭
 - 텔레메트리를 사용하는 자산: 텔레메트리 기능이 활성화된 자산의 총 수 및 비율
 - 텔레메트리 없는 자산: 텔레메트리를 활성화하지 않은 자산의 총 수 및 비율
 - 중요한 보안 권고 또는 높은 수준의 보안 권고를 받은 자산 텔레메트리를 사용하고 중요 또는 높은 보안 권고 사항이 있는 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: 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다.


 참고: 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 앱의 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 지원하므로 보안 리미디에이션, 소프트웨어 업그레이드, EOL 계획, 커버리지 결정에 있어 우선 순위를 지정할 수 있습니다.

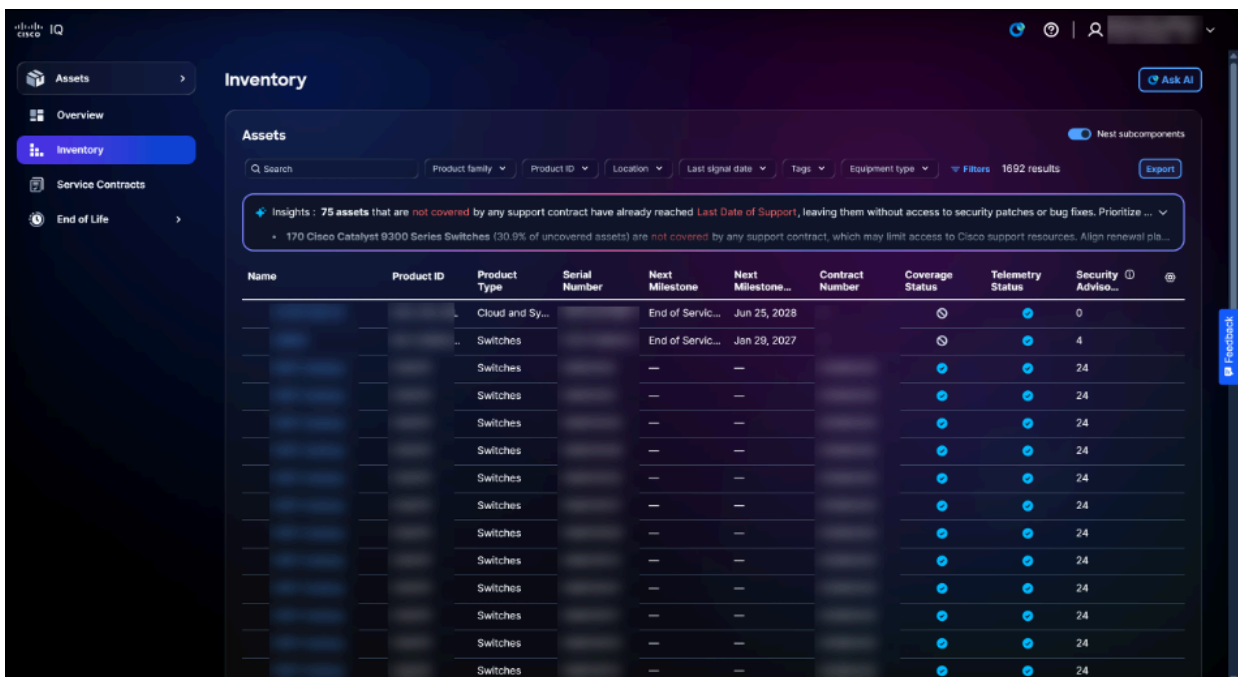
 참고: Asset Criticality Insights는 활성 텔레메트리 연결이 있는 표준 또는 서명 수준의 자산에만 사용할 수 있습니다. 자산이 구성 요구 사항을 충족하는지 확인하여 대시보드에 이러한 정보를 입력해 주십시오.

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 톨팁과 함께 개별 디바이스의 역할 및 중요도 보기

인벤토리

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





Name	Product ID	Product Type	Serial Number	Next Milestone	Next Milestone...	Contract Number	Coverage Status	Telemetry Status	Security Advisory...
		Cloud and Sy...		End of Servic...	Jun 25, 2028		🟡	🟢	0
		Switches		End of Servic...	Jan 29, 2027		🟡	🟢	4
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24
		Switches		—	—		🟢	🟢	24

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.

 참고: 역할과 권한에 따라 서로 다른 필터를 사용할 수 있습니다.

인벤토리 분석

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

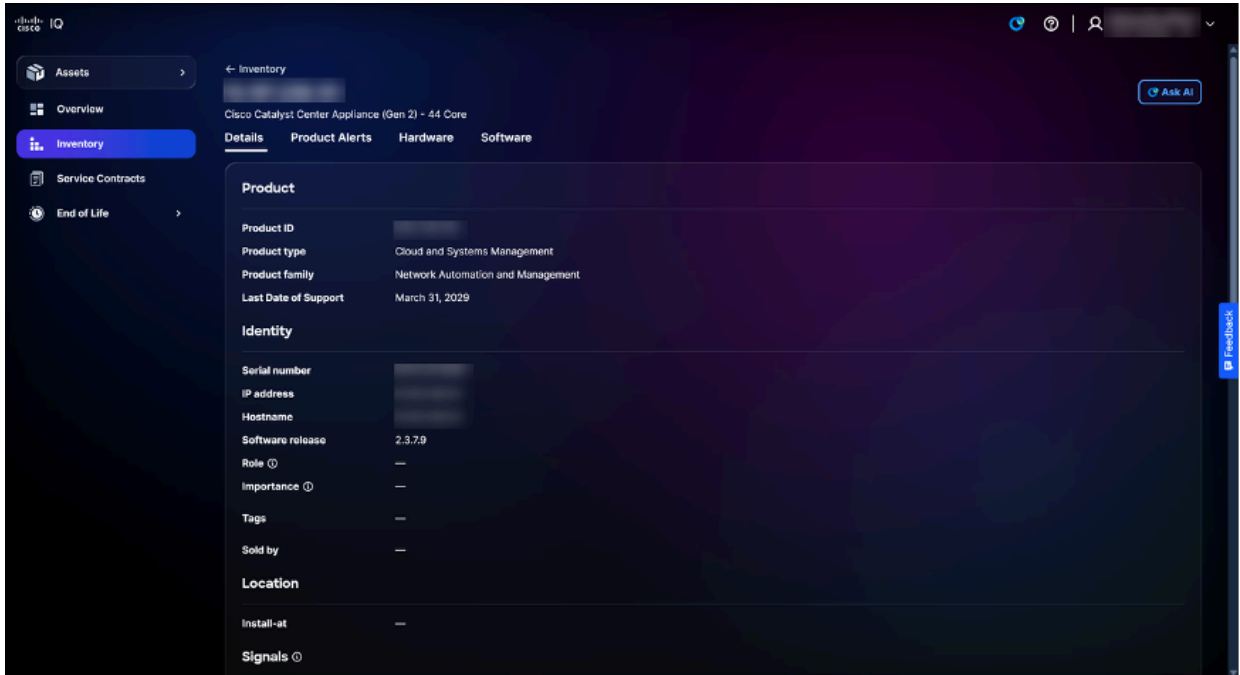
인벤토리 내보내기

Export(내보내기)를 클릭하여 필터링된 인벤토리 목록을 .xls 또는 .csv 형식으로 저장합니다. 자세한 [내용은](#) 일반 응용 프로그램 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.




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 key:value 정의하는 쌍(예: Environment:Prod 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.

자산 태그 생성 및 삭제

자산 [태그](#) 생성 및 삭제에 대한 자세한 내용은 시스템 설정의 태그를 참조하십시오.

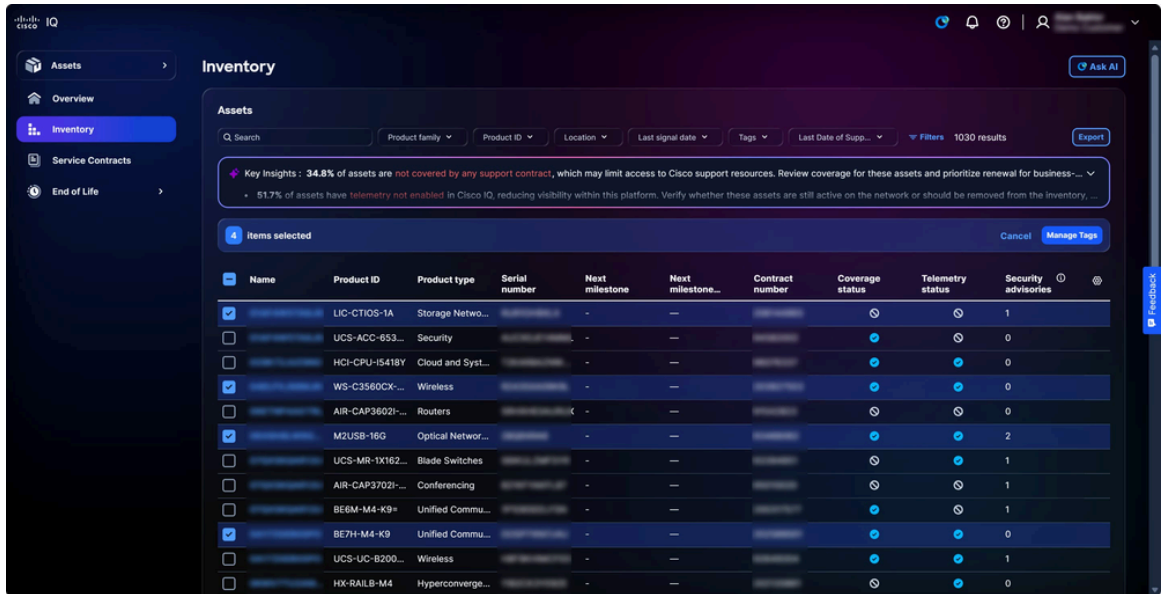
 참고: 계정 관리자만 태그를 만들고 삭제할 수 있습니다.

태그 할당

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

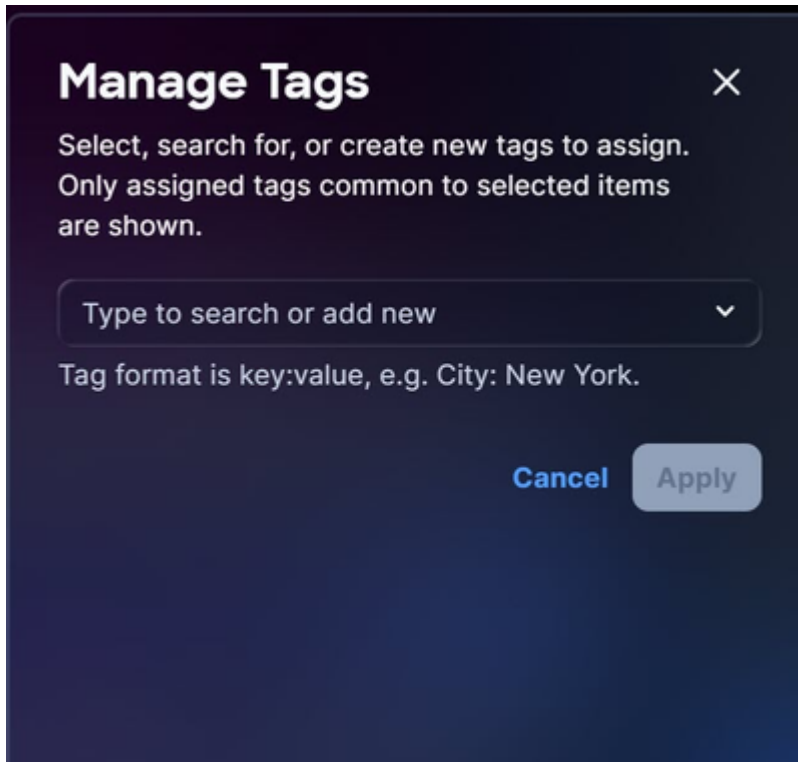
자산에 태그를 지정하려면

1. Assets > Inventory로 이동합니다.



태그 지정 자산

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



태그 할당

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

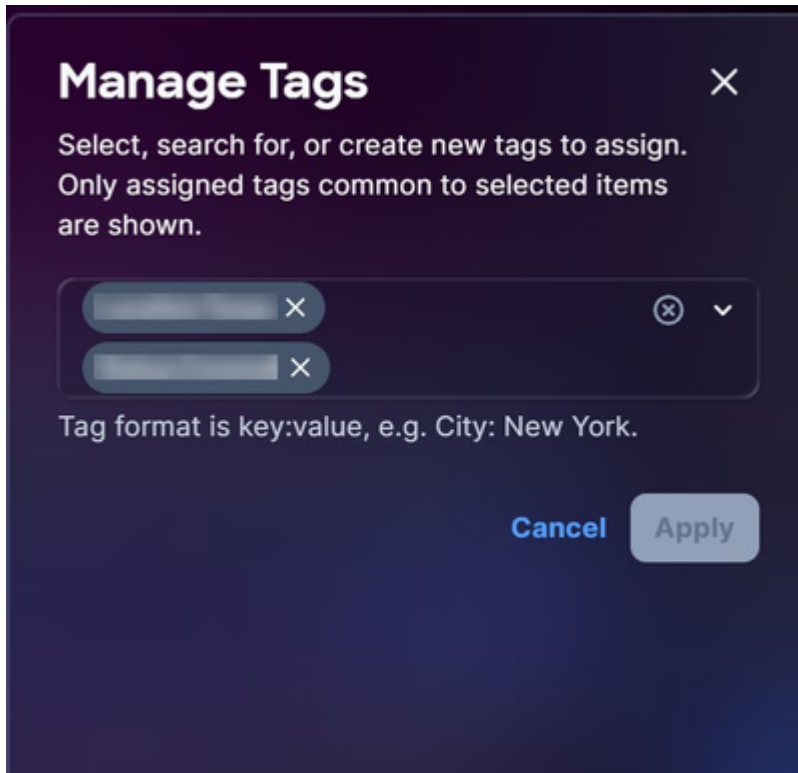
 참고: 태그는 key:value 형식(예: City:NYC)입니다.

5. 적용을 클릭합니다.

자산 태그 제거

하나 이상의 에셋에서 태그를 제거하려면

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



태그 제거

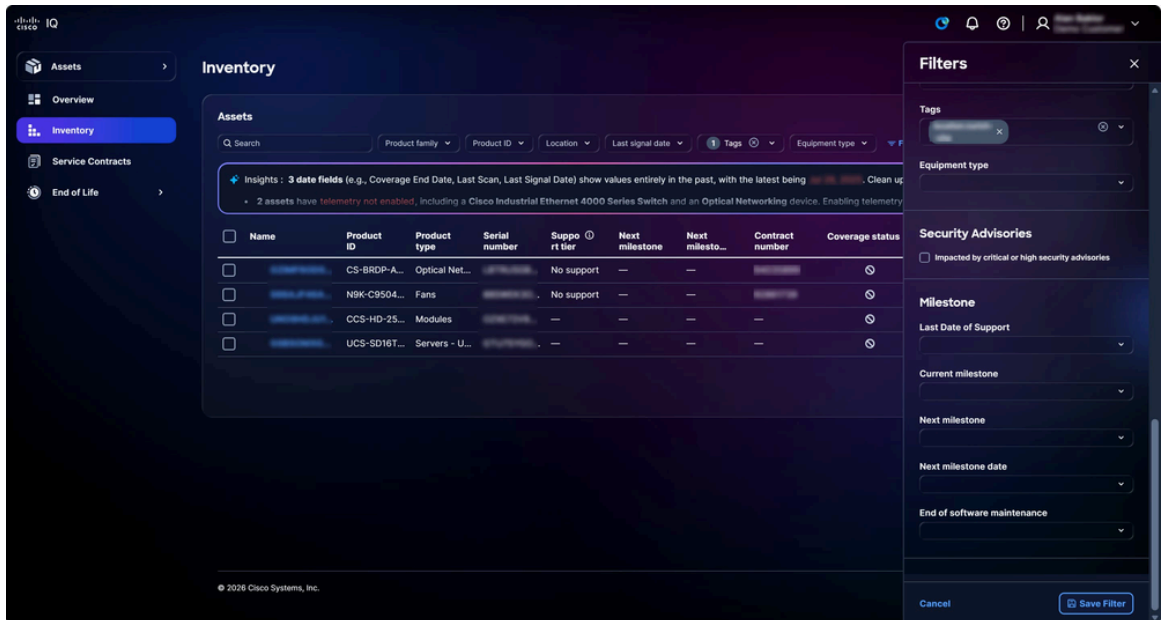
4. 선택 영역에서 제거하려면 임의의 태그에 X를 클릭합니다.
5. 적용을 클릭합니다.

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.

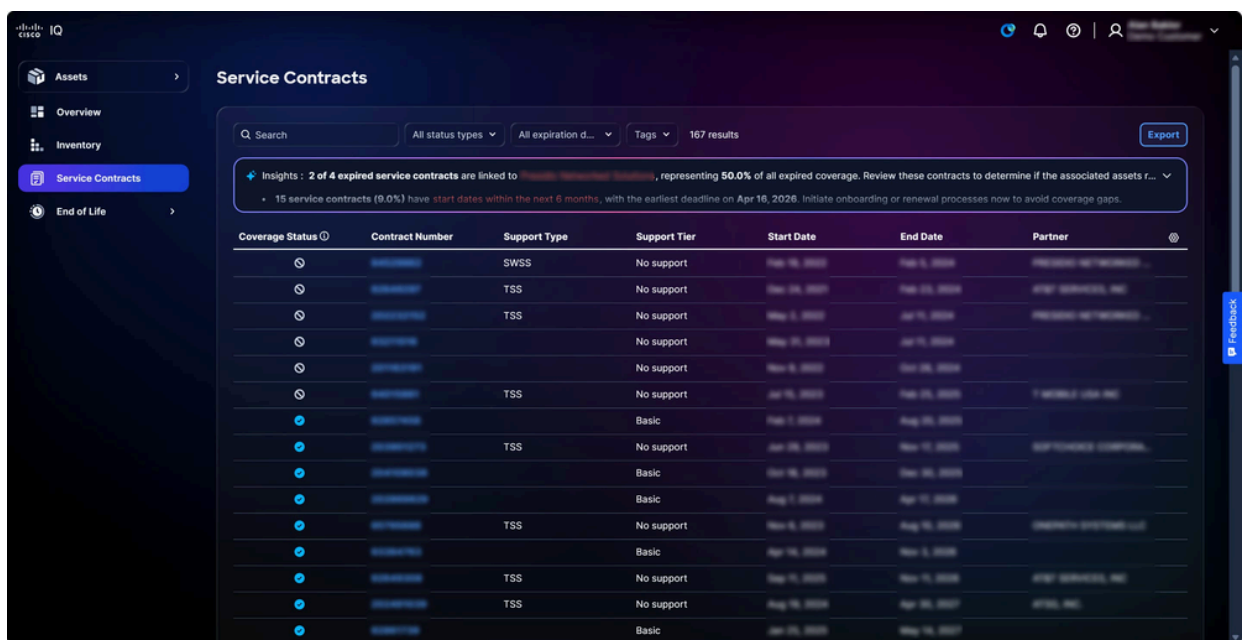


태그를 필터로 사용

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.



서비스 계약

서비스 계약에 대한 뷰 검색 및 필터링

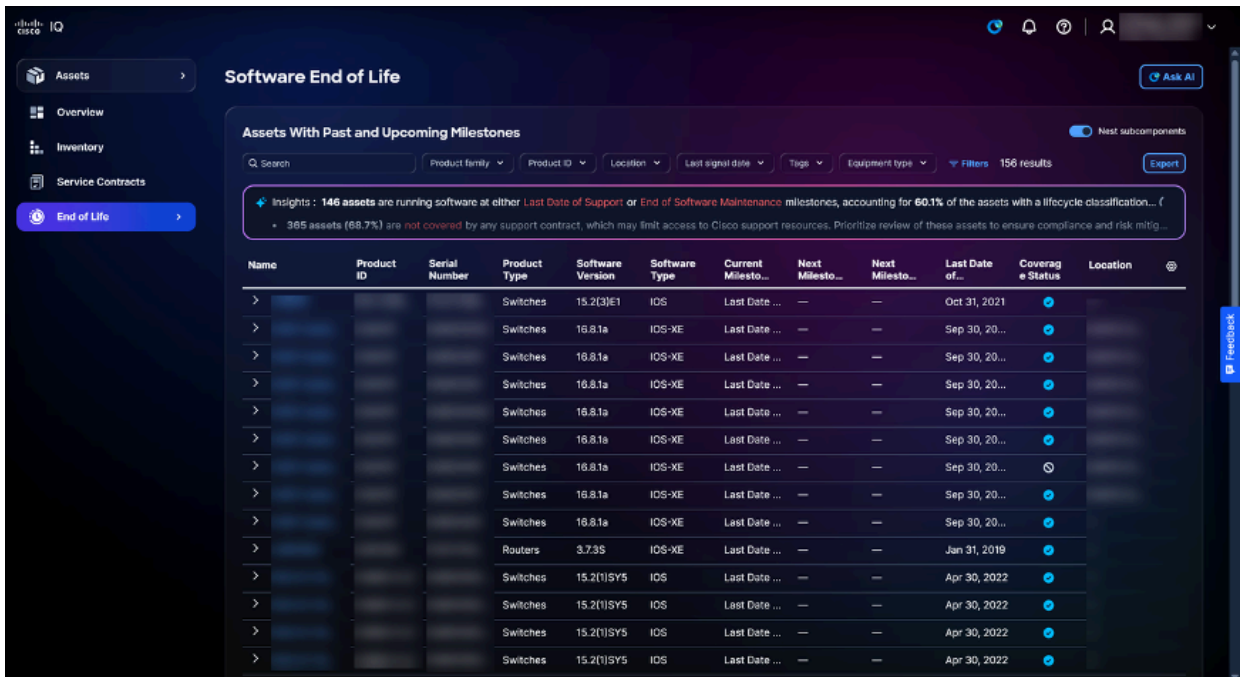
드롭다운 목록에서 필터를 선택하여 목록 보기를 필터링할 수 있습니다. Search(검색) 필드에 계약 번호를 입력하여 서비스 계약을 검색할 수도 있습니다.

서비스 계약 내보내기

Export(내보내기)를 클릭하여 필터링된 계약 목록을 .xls 또는 .csv 형식으로 저장합니다. 자세한 [내용](#)은 일반 응용 프로그램 기능의 정보 내보내기를 참조하십시오.

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.



The screenshot displays the 'Software End of Life' interface in Cisco IQ. It features a sidebar with navigation options: Assets, Overview, Inventory, Service Contracts, and End of Life. The main content area is titled 'Assets With Past and Upcoming Milestones' and includes a search bar and various filters. An insights panel at the top states: '146 assets are running software at either Last Date of Support or End of Software Maintenance milestones, accounting for 60.1% of the assets with a lifecycle classification... 365 assets (68.7%) are not covered by any support contract, which may limit access to Cisco support resources. Prioritize review of these assets to ensure compliance and risk mitigation.' Below this is a table with columns: Name, Product ID, Serial Number, Product Type, Software Version, Software Type, Current Milestone, Next Milestone, Next Milestone, Last Date of..., Coverage Status, and Location. The table lists several switches and routers with their respective software versions and end-of-life dates.

Name	Product ID	Serial Number	Product Type	Software Version	Software Type	Current Milesto...	Next Milesto...	Next Milesto...	Last Date of...	Coverag e Status	Location
>			Switches	15.2(3)E1	IOS	Last Date ...	—	—	Oct 31, 2021	🟢	
>			Switches	16.8.1a	IOS-XE	Last Date ...	—	—	Sep 30, 20...	🟢	
>			Switches	16.8.1a	IOS-XE	Last Date ...	—	—	Sep 30, 20...	🟢	
>			Switches	16.8.1a	IOS-XE	Last Date ...	—	—	Sep 30, 20...	🟢	
>			Switches	16.8.1a	IOS-XE	Last Date ...	—	—	Sep 30, 20...	🟢	
>			Switches	16.8.1a	IOS-XE	Last Date ...	—	—	Sep 30, 20...	🟢	
>			Switches	16.8.1a	IOS-XE	Last Date ...	—	—	Sep 30, 20...	🟢	
>			Switches	16.8.1a	IOS-XE	Last Date ...	—	—	Sep 30, 20...	🟢	
>			Routers	3.7.3S	IOS-XE	Last Date ...	—	—	Jan 31, 2019	🟢	
>			Switches	15.2(1)SY5	IOS	Last Date ...	—	—	Apr 30, 2022	🟢	
>			Switches	15.2(1)SY5	IOS	Last Date ...	—	—	Apr 30, 2022	🟢	
>			Switches	15.2(1)SY5	IOS	Last Date ...	—	—	Apr 30, 2022	🟢	
>			Switches	15.2(1)SY5	IOS	Last Date ...	—	—	Apr 30, 2022	🟢	

소프트웨어 단종

End of Life 분석

End of Life 페이지의 Insights 패널에는 AI 중심의 자산 개요와 정의된 Last Day of Support가 표시 됩니다. 그래프, 대시보드, 차트와 같은 시각화를 위한 전체 분석을 클릭하여 추가적인 통찰력을 제 공합니다. 자세한 [내용](#)은 공통 애플리케이션 기능의 데이터 분석을 참조하십시오.

단종 내보내기

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

평가 애플리케이션

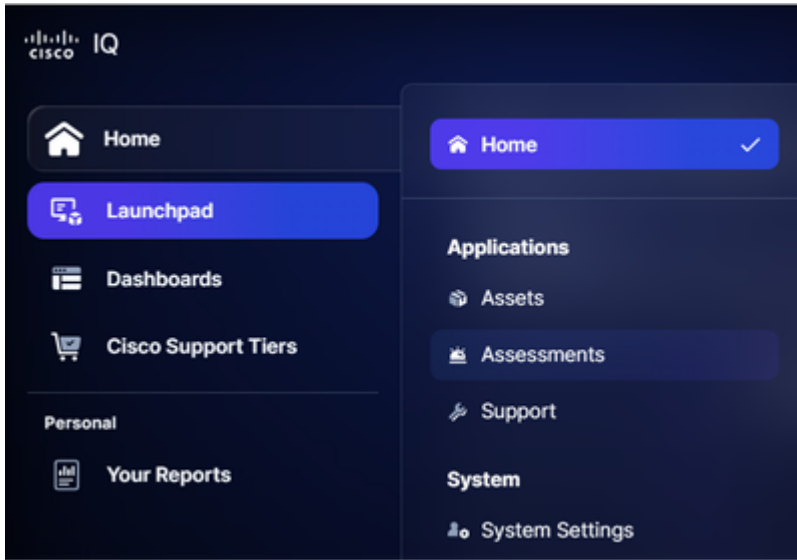
Assessments 애플리케이션은 사용자가 보안, 안정성, 용량, 규정 준수 및 노후화와 관련된 위험을 사전에 조사하고 완화할 수 있도록 하는 평가 프레임워크를 제공하여 네트워크의 보안, 안정성 및 안정성을 유지합니다.

핵심 개념

평가 애플리케이션은 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 애플리케이션 액세스



평가

Cisco IQ의 보안 및 평가 기능에 액세스하려면 Home 메뉴 > Assessments를 선택합니다. 평가 개요 페이지가 표시됩니다.

평가 개요


[평가 개요] 페이지에는 다음 대시보드가 표시됩니다.



평가 개요

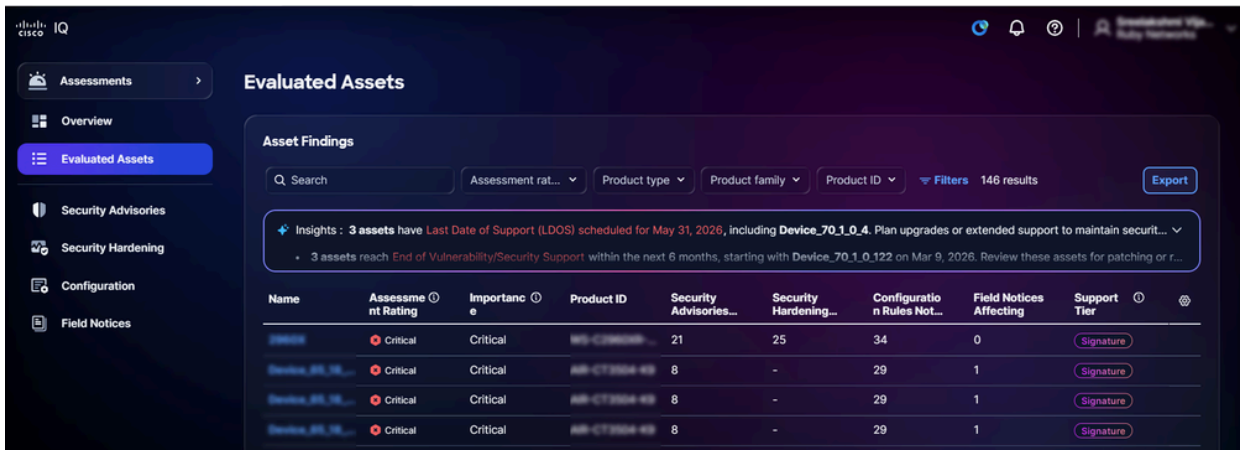
대시보드에는 다음 정보가 표시됩니다.

- 보안 자문 평가: 보안 권고에 대한 평가를 Critical(중대) 및 High(높음) 심각도별로 구분하여 표시합니다.
- 통과되지 않은 자산으로 보안 강화 규칙: 보안 강화 규칙에 실패한 자산을 High(높음), Medium(중간), Low(낮음) 및 Informational(정보) 심각도로 분류하여 표시합니다.
- 통과되지 않은 에셋이 포함된 컨피그레이션 규칙: 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), Medium(중간) 및 No severity(심각도 없음)별로 범주화된 필드 알림의 평가를 표시합니다.

 참고: 고객은 액세스 권한이 있는 자산만 볼 수 있습니다.

자산별 조사 결과

Findings by Asset(자산별 조사 결과) 페이지는 Security Advisories(보안 권고), Security Hardening(보안 강화), Configuration(컨피그레이션) 및 Field Notice(필드 알림)를 포함한 다음 평가 중 하나 이상을 사용하여 평가된 자산 목록을 제공합니다.




Name	Assessment Rating	Importance	Product ID	Security Advisories...	Security Hardening...	Configuration Rules Not...	Field Notices Affecting	Support Tier
Device_70_1_0_4	Critical	Critical	98-CT3004-08	21	25	34	0	Signature
Device_70_1_0_4	Critical	Critical	98-CT3004-08	8	-	29	1	Signature
Device_70_1_0_4	Critical	Critical	98-CT3004-08	8	-	29	1	Signature
Device_70_1_0_4	Critical	Critical	98-CT3004-08	8	-	29	1	Signature

자산별 조사 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.

 참고: 역할과 권한에 따라 서로 다른 필터를 사용할 수 있습니다.

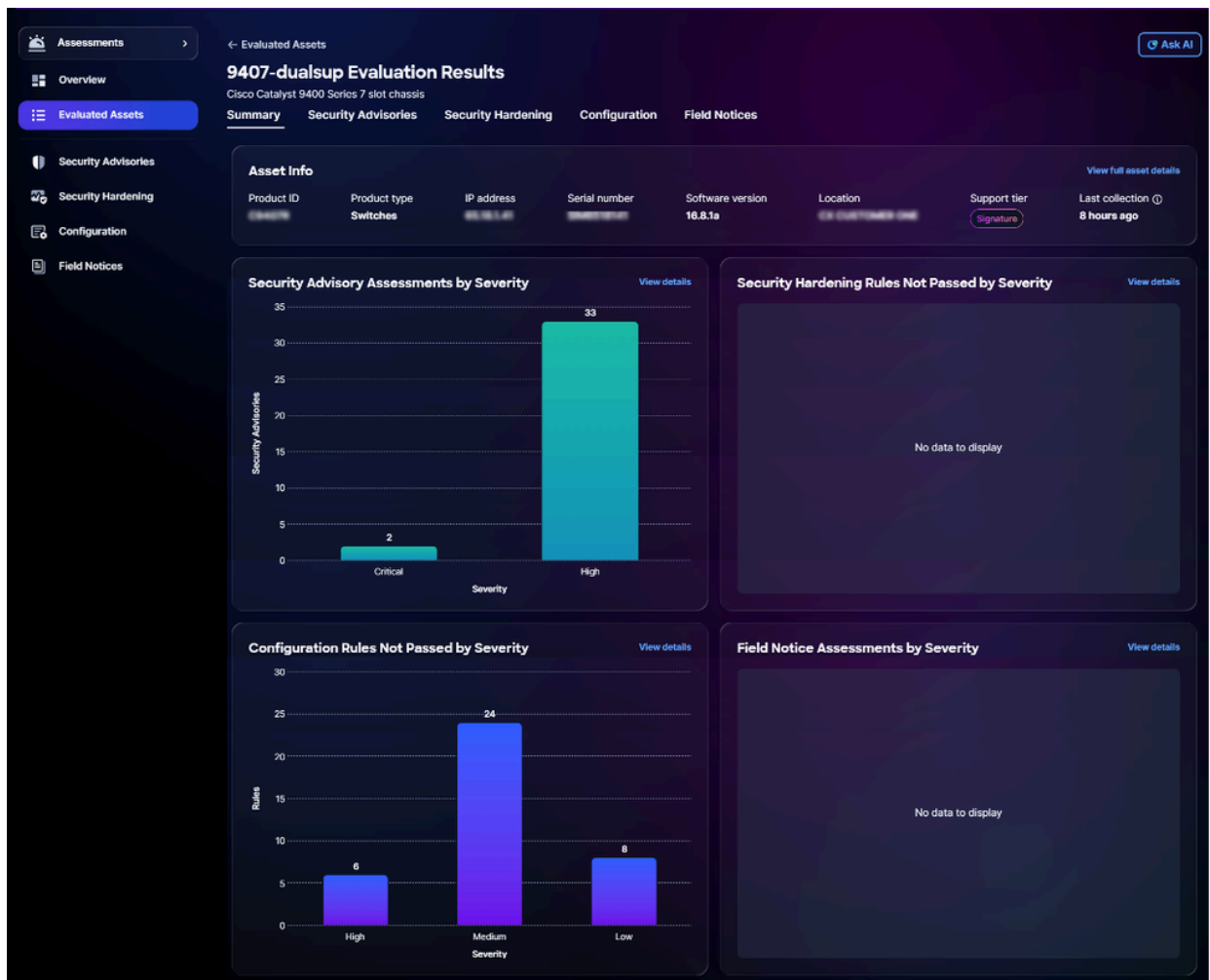
자산별 검색 결과 내보내기

Finding by Asset 목록 뷰를 내보내려면 Export를 클릭합니다. 내보내기^에 대한 자세한 내용은 정보 내보내기를 참조하십시오.

자산 상세내역별 결과 보기

Findings by Asset details(자산별 검색 결과)를 보려면 Asset(자산)을 클릭합니다. 다음 탭에는 선택한 자산에 대한 세부사항이 표시됩니다.

- 요약: 보안 권고 사항 수, 보안 강화, 컨피그레이션 및 Field Notice를 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 세부 정보 보기를 클릭하면 응용 프로그램 내의 관련 페이지로 페이지가 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.

The screenshot shows the Cisco IQ Security Advisories interface. It includes a sidebar with navigation options like Assessments, Overview, Evaluated Assets, Security Advisories (selected), Security Hardening, Configuration, and Field Notices. The main content area is titled 'Security Advisories' and contains an 'About the Assessments' section and a table of 'Security Advisory Assessments With Vulnerabilities Detected'. The table has 7 columns: Assessment, Severity, Assets at Risk, Assets Potentially at Risk, CVE, and Last Updated. There are 10 rows of data, each representing a different security advisory with its severity, the number of assets at risk, and the associated CVE ID.

Assessment	Severity	Assets at Risk	Assets Potentially at Risk	CVE	Last Updated
Cisco IOS XE Software ...	High	987	0	CVE-2025-20197 (+4)	May 7, 2025
Cisco IOS XE Software ...	High	942	0	CVE-2020-3417	Nov 2, 2020
Cisco IOS and IOS XE S...	High	882	13	CVE-2025-20352	Oct 6, 2025
Cisco IOS XE Software ...	High	881	11	CVE-2021-1403	Mar 24, 2021
Multiple Vulnerabilities...	Critical	881	11	CVE-2023-20198 (+1)	Nov 1, 2023
Cisco IOS XE Software ...	High	881	11	CVE-2021-1442	Mar 24, 2021
Cisco IOS XE Software ...	High	881	11	CVE-2020-3141 (+1)	Sep 24, 2020
Cisco IOS XE Software ...	High	794	0	CVE-2020-3209	Jun 3, 2020
Cisco IOS XE Software ...	High	740	11	CVE-2020-3219	Jun 3, 2020

보안 자문

보안 권고 사항에 대한 필터링 뷰 검색

드롭다운 목록에서 필터를 선택하여 목록 뷰를 필터링할 수 있습니다. 또한 검색 필드에 평가 이름을 입력하여 보안 권고 평가를 검색할 수도 있습니다.

참고: 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다.

참고: 역할과 권한에 따라 서로 다른 필터를 사용할 수 있습니다.

참고: 누락된 심각도 값은 설명 도구 설명과 함께 "-"로 표시됩니다.

보안 권고 내보내기

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

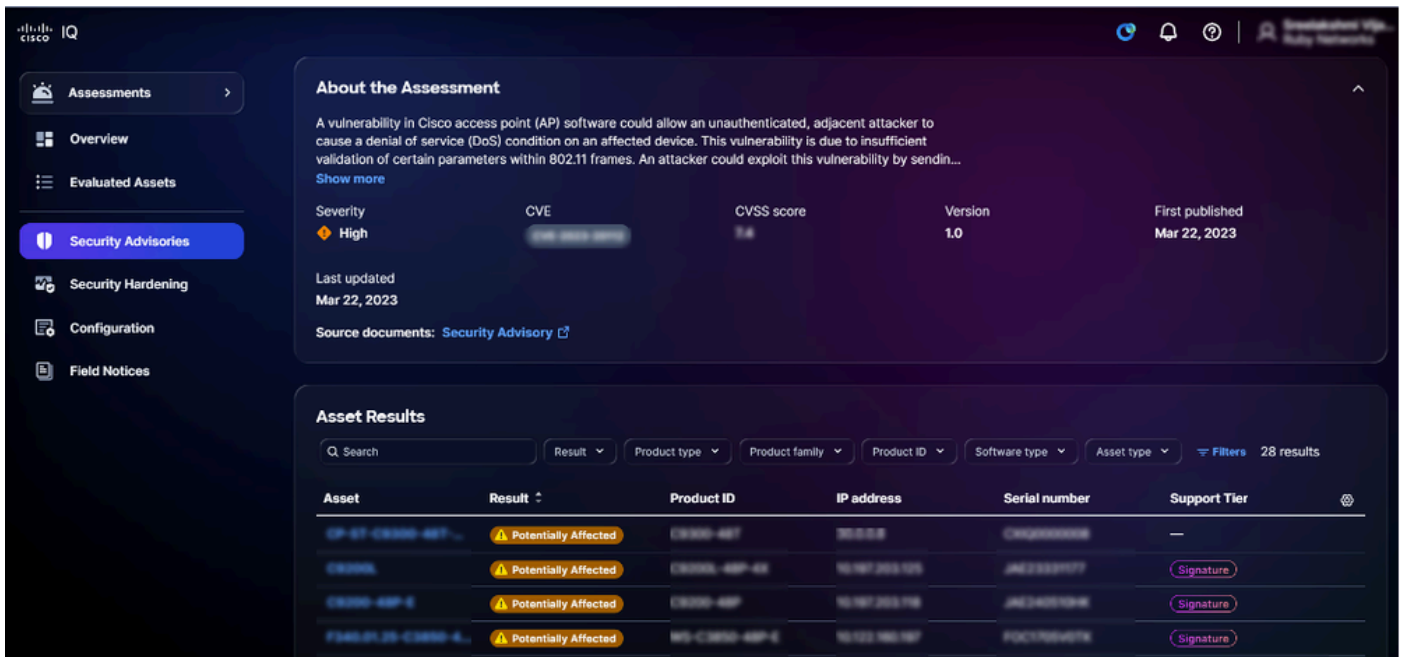
보안 자문 평가 세부 정보 보기

평가에 대한 추가 세부 정보를 보려면 Advisory(권고)를 클릭합니다. 이 세부사항 페이지는 CVSS(Common Vulnerability Scoring System) 점수, CVE(Common Vulnerabilities and

Exposures), 심각도, 참조된 Cisco Security Advisory에 대한 링크와 같은 정보를 제공합니다.

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



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.

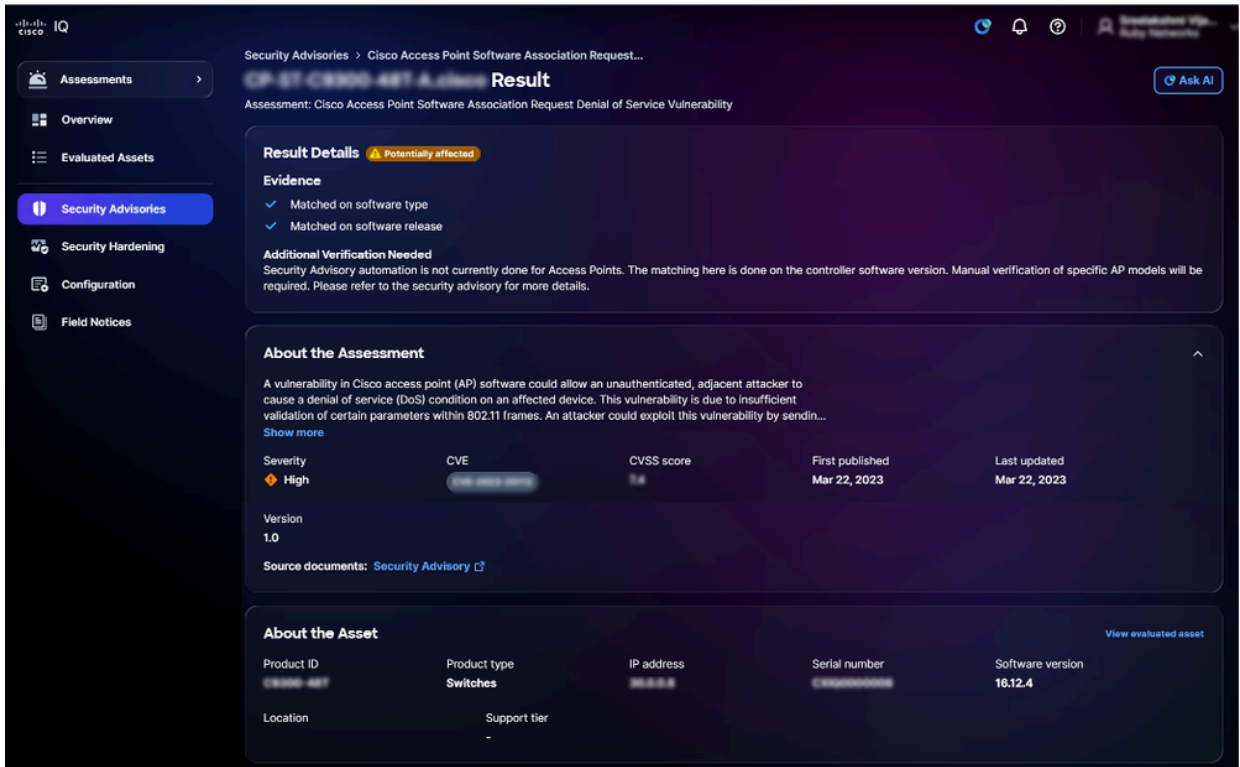
 참고: 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다.

 참고: 역할과 권한에 따라 서로 다른 필터를 사용할 수 있습니다.

자산 평가 결과 보기

평가 결과의 세부 정보를 보려면 Asset Assessment Results 테이블에서 자산을 클릭합니다. 평가

결과 세부사항 페이지가 표시됩니다.




결과 세부사항

보안 권고에 대한 자산 결과 내보내기

자산 결과를 내보내려면 내보내기를 누릅니다. 내보내기^에 대한 자세한 내용은 정보 내보내기를 참조하십시오.

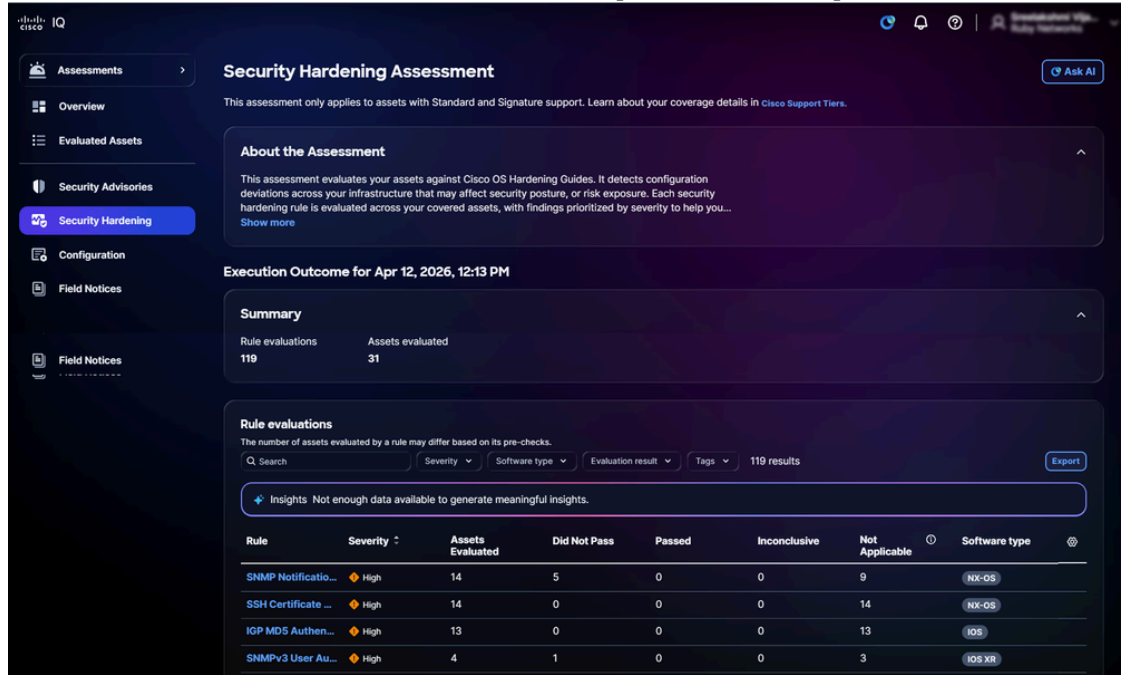
보안 강화

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 관리자가 효과적으로 공격 표면을 줄이고 Cisco의 엄격한 보안 모범 사례에 일관되게 대응할 수 있도록 합니다. 규정 준수 모니터링을 중앙 집중화하고 강화 프로세스를 간소화함으로써 애플리케이션은 사후 대응적 작업에서 사전 대응적 데이터 중심 전략으로 보안 관리를 전환하여 탄력적이고 안전한 엔터프라이즈 네트워크를 보장합니다.

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

보안 강화 평가 보기

보안 강화에 대한 추가 세부 정보를 보려면 평가를 클릭합니다. [보안 강화 평가] 페이지에는 다음




정보가 표시됩니다.

보안 강화

- 평가 정보: 평가의 목적을 요약하여 추가 세부 정보를 제공합니다.
- 실행 요약: 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

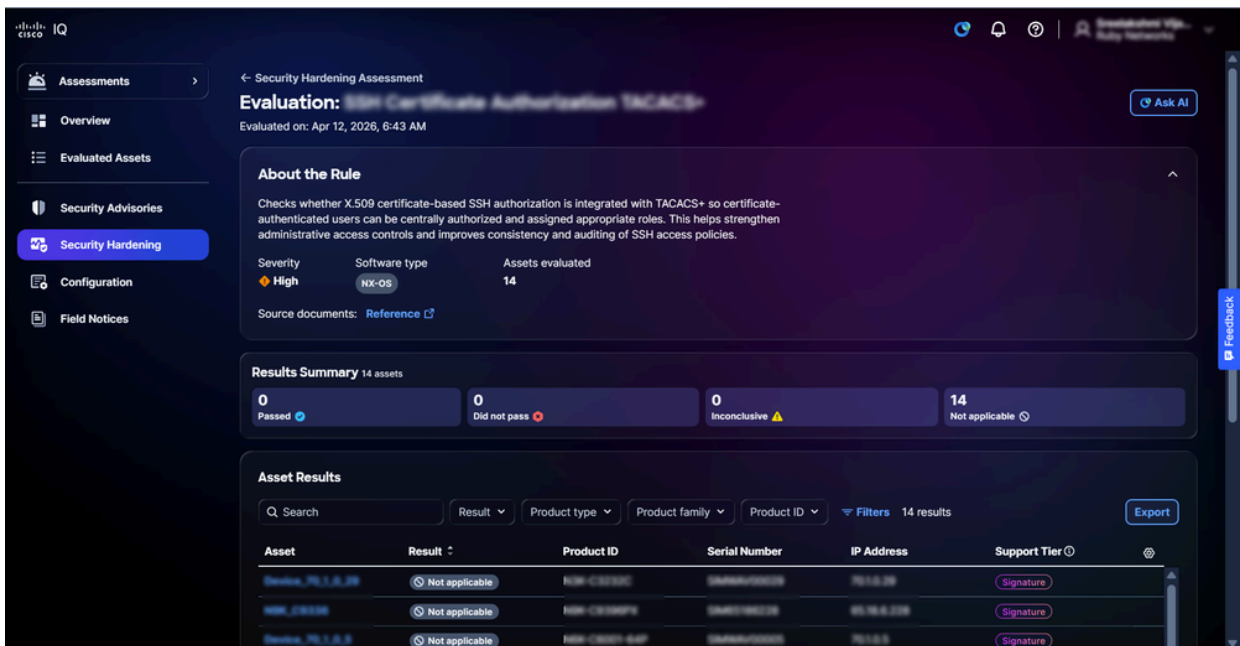
드롭다운 목록에서 필터를 선택하거나 Filters(필터)를 클릭하고 사용 가능한 필터 목록에서 옵션을 선택하여 목록 뷰를 필터링할 수 있습니다. Search 필드에 규칙 이름을 입력하여 규칙을 검색할 수도 있습니다.

 참고: 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다.

 참고: 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.




Asset	Result	Product ID	Serial Number	IP Address	Support Tier
Device, 78.1.0.20	Not applicable	IOS-120200	12020000000000000000	78.1.0.20	Signature
Device, 78.1.0.21	Not applicable	IOS-120200	12020000000000000000	78.1.0.21	Signature
Device, 78.1.0.2	Not applicable	IOS-120200-001	12020000000000000000	78.1.0.2	Signature

규칙 보기

- 규칙 정보: 심각도, 소프트웨어 유형, 버전 및 평가된 자산과 같은 규칙에 대한 세부 정보를 제공합니다.
- 결과 요약: Passed(통과), Did not pass(통과 안 함), Inconclusive(결론 없음), Not applicable(해당 없음)과 같은 규칙과 관련된 자산 결과의 요약을 제공합니다
- 자산 결과: 자산 목록 및 자산(예: 자산, 결과, 제품 ID, 일련 번호, IP 주소, 지원 계층)을 제공합니다.

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.


 참고: 역할과 권한에 따라 서로 다른 필터를 사용할 수 있습니다.

자산 결과 내보내기

규칙에 대한 평가 결과를 내보내려면 Export를 클릭합니다. 내보내기^에 대한 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.

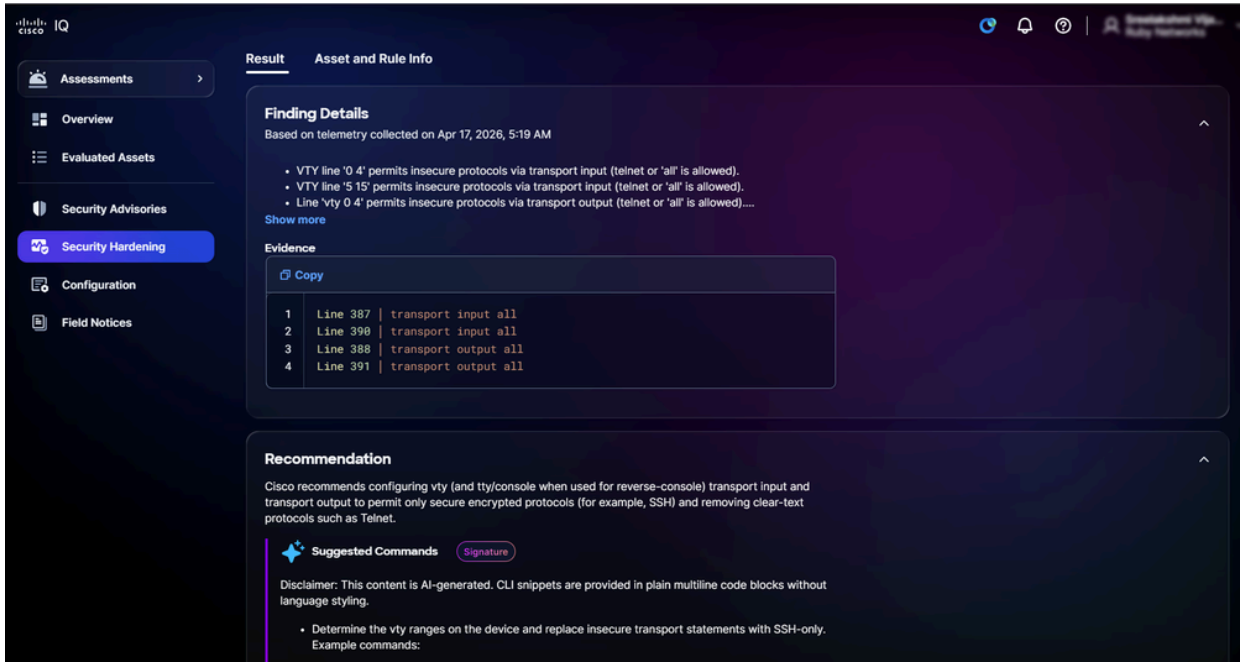
 참고: 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다.

 참고: 역할과 권한에 따라 서로 다른 필터를 사용할 수 있습니다.

보안 강화를 위한 자산 결과 보기

자산 결과의 상세내역을 조회하려면 자산 결과에서 자산을 누릅니다. 자산 결과의 세부사항 페이지에는 자격 레벨 또는 계층에 따른 정보가 표시됩니다.

- 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



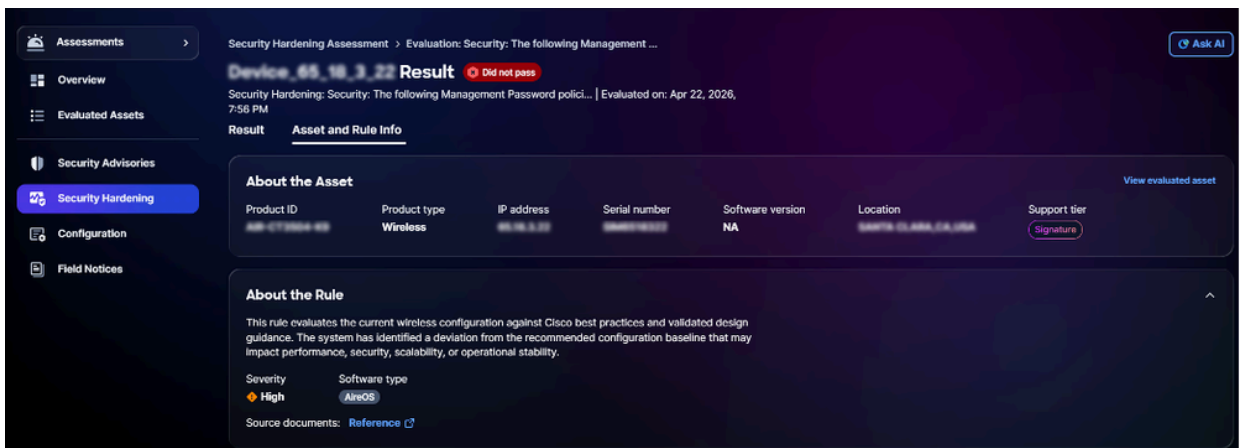
보안 강화 시그니처 계층

- 서명 계층

- 찾기 세부 정보: 증거 로그와 함께 평가 중에 확인된 구성 편차에 대한 정보를 제공합니다.
- 권장 사항: 구성 일관성을 보장하기 위해 코드 조각과 함께 장치 수준의 실행 가능한 지침을 제공합니다.

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 및 규칙 정보

- 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

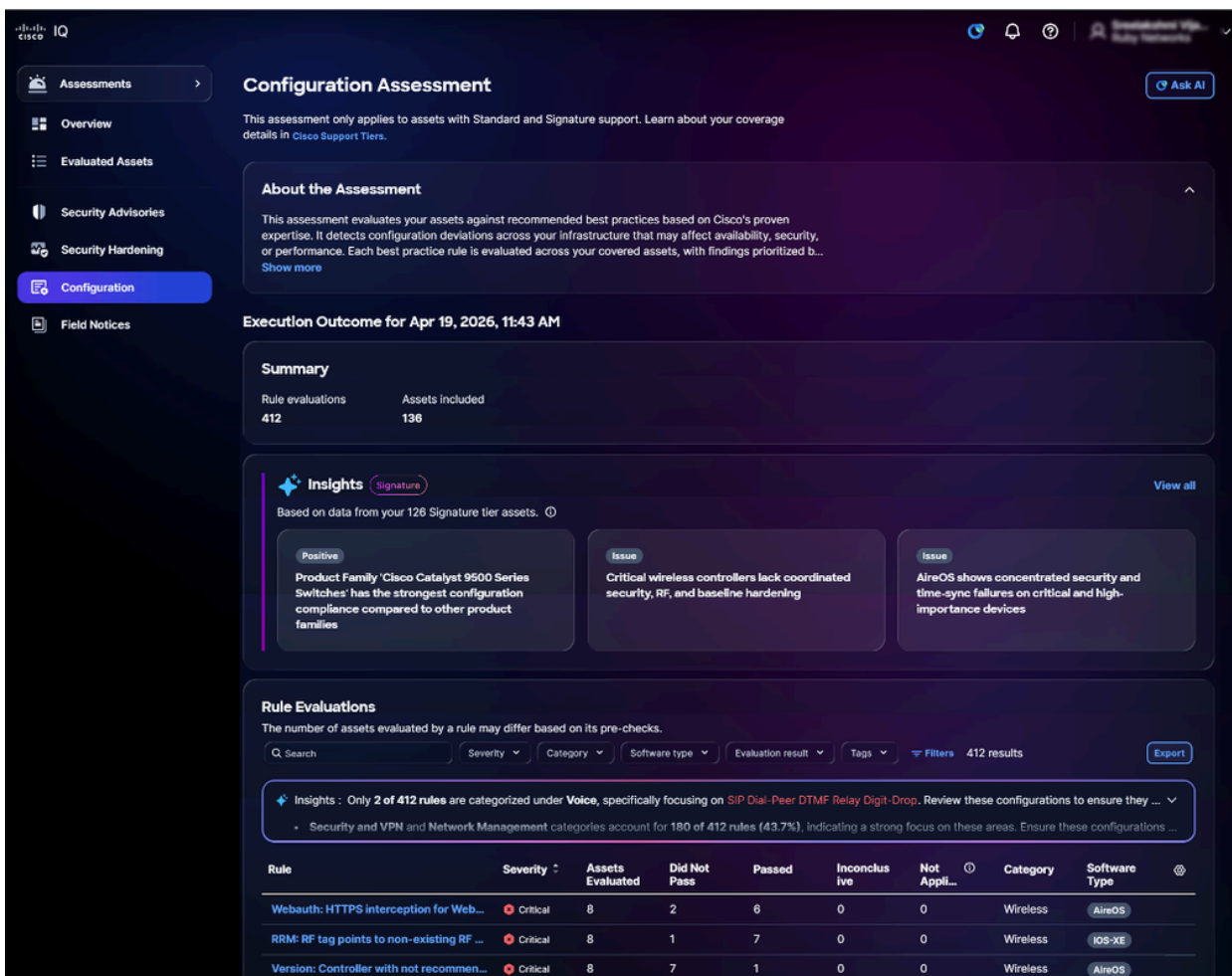
설정

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 Best Practice 규칙은 지원 대상 자산 및 심각도에 따라 우선 순위가 지정된 결과를 평가하여 구성 일관성, 향상된 복원력, 운영 위험 감소를 보장합니다.

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

구성 평가 보기

구성에 대한 추가 세부 정보를 보려면 평가를 클릭합니다. 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... [Show more](#)

Execution Outcome for Apr 19, 2026, 11:43 AM

Summary

Rule evaluations	Assets Included
412	136

Insights Signature [View all](#)

Based on data from your 126 Signature tier assets. ⓘ

- Positive**: Product Family 'Cisco Catalyst 9500 Series Switches' has the strongest configuration compliance compared to other product families
- Issue**: Critical wireless controllers lack coordinated security, RF, and baseline hardening
- Issue**: AireOS shows concentrated security and time-sync failures on critical and high-importance devices

Rule Evaluations

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

Search: Severity: ▼ Category: ▼ Software type: ▼ Evaluation result: ▼ Tags: ▼ Filters: 412 results [Export](#)

Insights: Only 2 of 412 rules are categorized under Voice, specifically focusing on SIP Dial-Peer DTMF Relay Digit-Drop. Review these configurations to ensure they ...

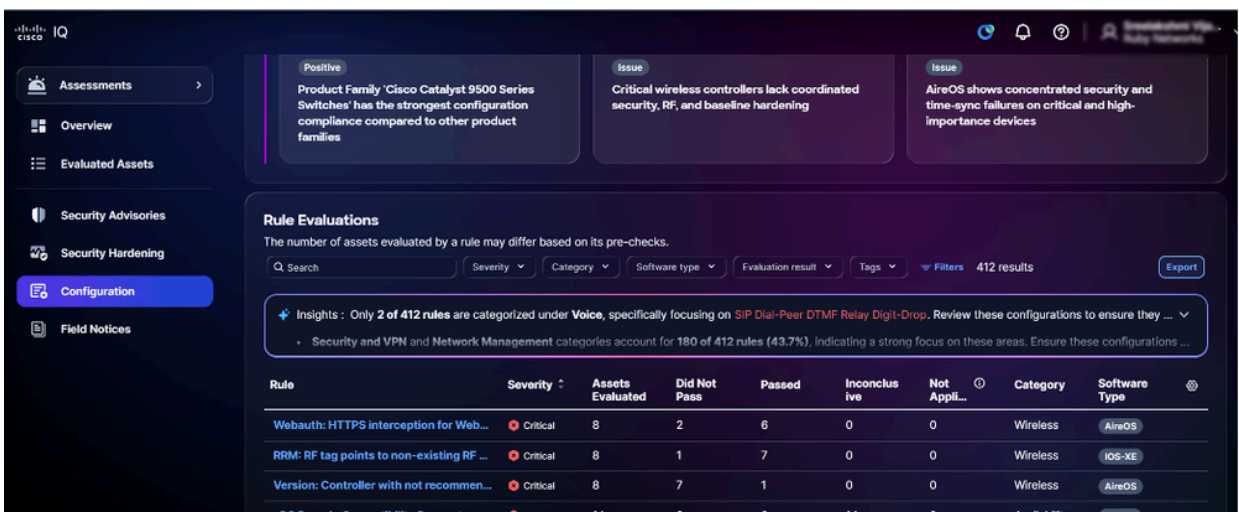
- Security and VPN and Network Management categories account for 180 of 412 rules (43.7%), indicating a strong focus on these areas. Ensure these configurations ...

Rule	Severity	Assets Evaluated	Did Not Pass	Passed	Inconclusive	Not Appli...	Category	Software Type
Webauth: HTTPS interception for Web...	Critical	8	2	6	0	0	Wireless	AireOS
RRM: RF tag points to non-existing RF ...	Critical	8	1	7	0	0	Wireless	IOS-XE
Version: Controller with not recommen...	Critical	8	7	1	0	0	Wireless	AireOS

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




The screenshot displays the Cisco IQ Rule Evaluations interface. It features a sidebar with navigation options like Assessments, Overview, Evaluated Assets, Security Advisories, Security Hardening, Configuration, and Field Notices. The main content area shows a 'Rule Evaluations' section with a search bar and filters. Below this, there are insights and a table of rule evaluations.


Rule	Severity	Assets Evaluated	Did Not Pass	Passed	Inconclusive	Not Appli...	Category	Software Type
Webauth: HTTPS interception for Web...	Critical	8	2	6	0	0	Wireless	AireOS
RRM: RF tag points to non-existing RF ...	Critical	8	1	7	0	0	Wireless	IOS-XE
Version: Controller with not recommen...	Critical	8	7	1	0	0	Wireless	AireOS
UPC Domain Compatibility Parameters	Critical	14	0	0	14	0	Availability	IOS-XE

규칙 평가

드롭다운 목록에서 필터를 선택하거나 Filters(필터)를 클릭하고 사용 가능한 필터 목록에서 옵션을

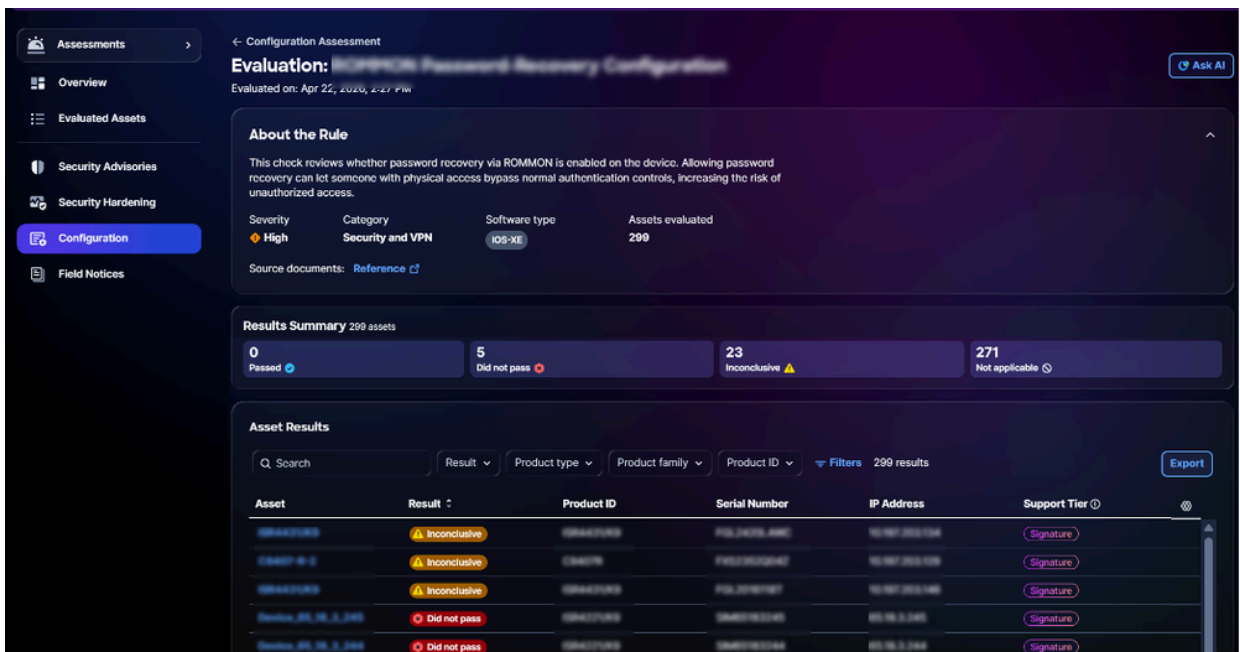
선택하여 목록 뷰를 필터링할 수 있습니다. Search 필드에 규칙 이름을 입력하여 규칙을 검색할 수도 있습니다.

 참고: 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다.

 참고: 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 자산 같은 규칙에 대한 세부 정보를 제공하며 관련 소스 문서에 대한 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.


자산 결과 내보내기


규칙에 대한 자산 결과를 내보내려면 내보내기를 누릅니다. 내보내기 [에](#) 대한 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.

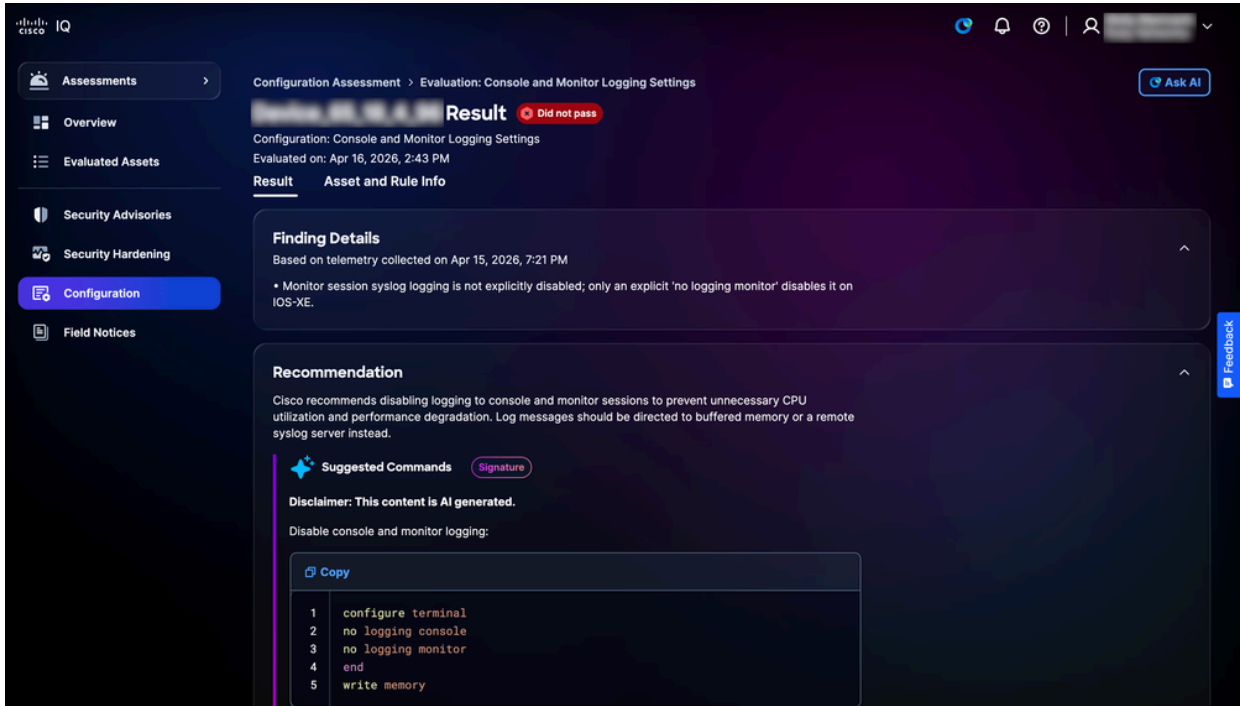
 참고: 역할과 권한에 따라 서로 다른 필터를 사용할 수 있습니다.

구성 평가에 대한 자산 결과 보기

자산 결과의 상세내역을 조회하려면 자산 결과에서 자산을 누릅니다.

자산 결과의 세부사항 페이지에는 자격 레벨 또는 계층에 따른 정보가 표시됩니다.

- 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



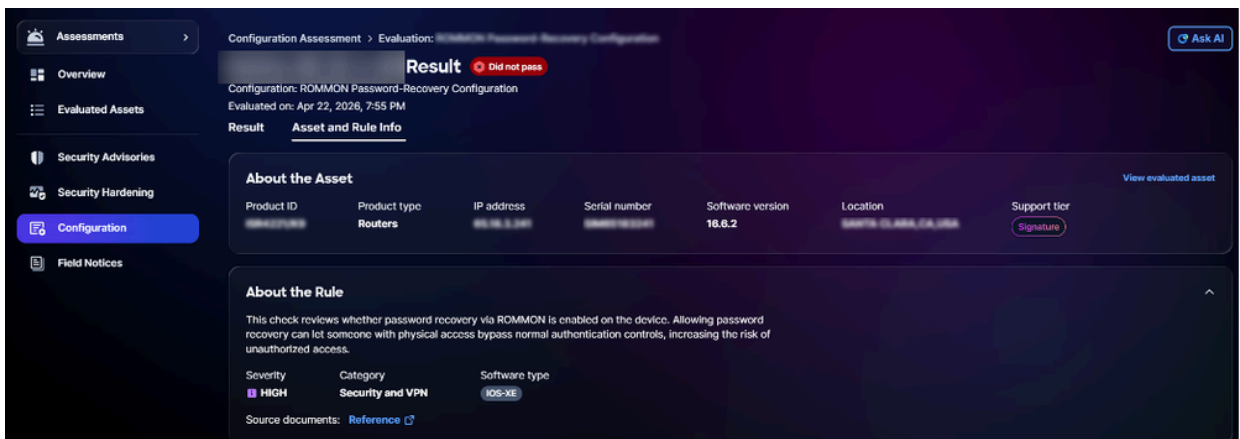
구성 서명 계층

• 서명 계층

- 찾기 세부 정보: 증거 로그와 함께 평가 중에 확인된 구성 편차에 대한 정보를 제공합니다.
- 권장 사항: 장치 레벨의 실행 가능한 지침을 코드 조각과 함께 제공하여 검색 결과를 해결하고 컨피그레이션 일관성을 보장합니다.

구성 평가를 위한 자산 및 규칙 정보 보기

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



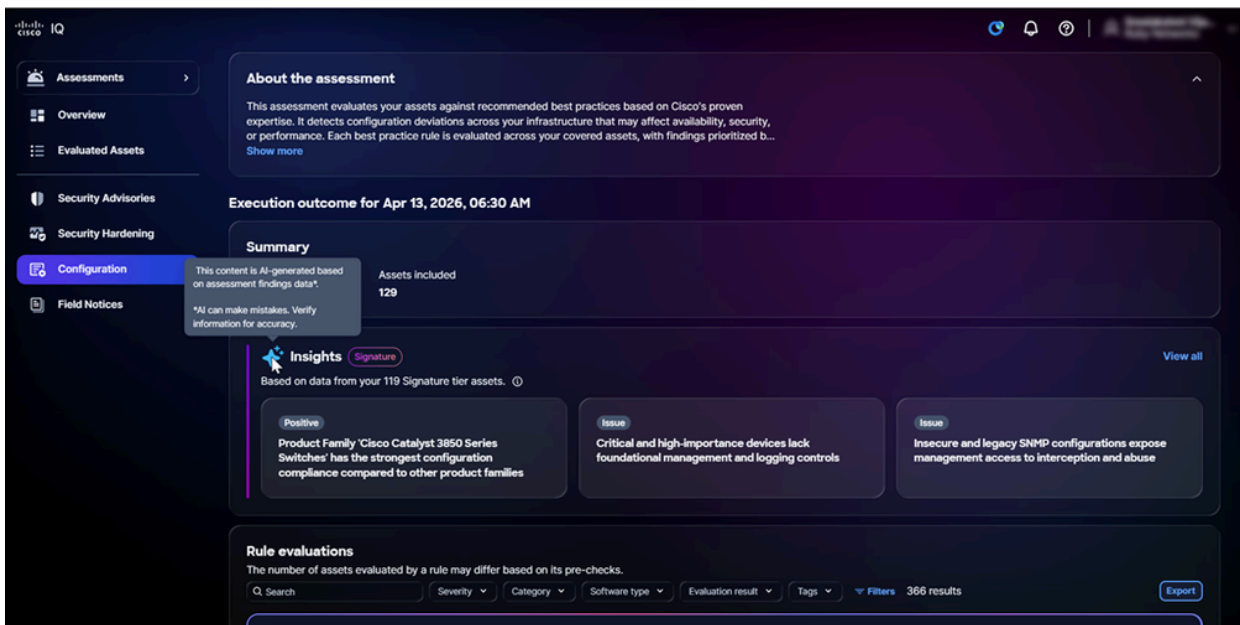
자산 및 규칙 정보

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

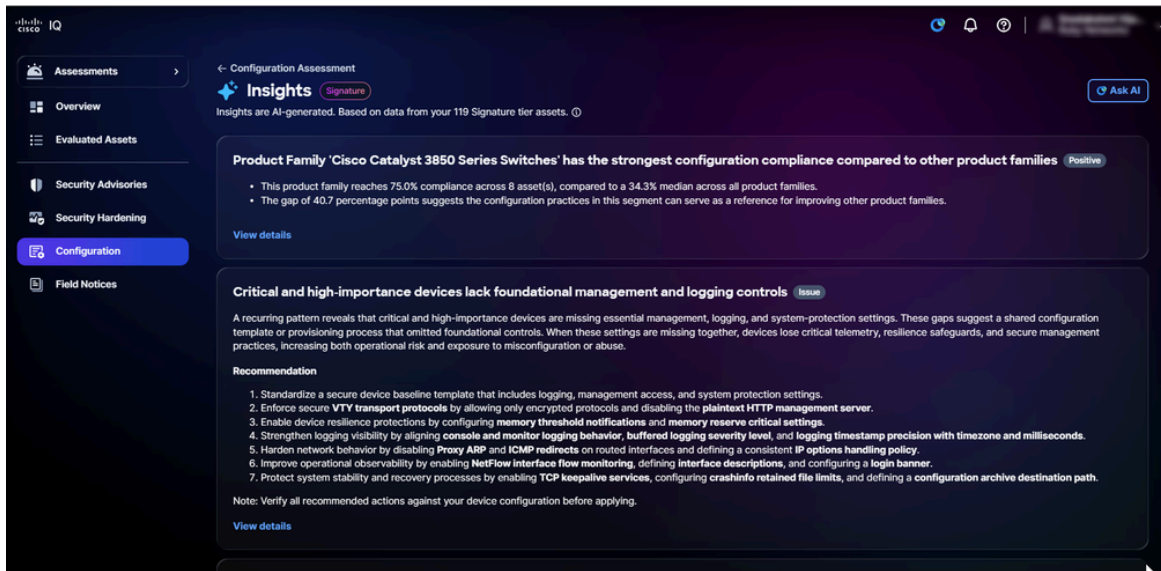
통찰력은 AI에서 생성되며, 우선 순위가 지정된 주요 카드에 평가 데이터를 종합하여 여러 조사 결과에 걸쳐 중요한 구성 차이를 강조하는 지능형 대시보드의 역할을 합니다. 이러한 시급한 영역에 집중함으로써 가장 큰 영향을 미치는 인프라 위험을 효율적으로 해결할 수 있습니다. 또한 Best Practice에 따라 인프라가 잘 작동하는 영역을 파악하여 장점을 강조합니다.



통찰력

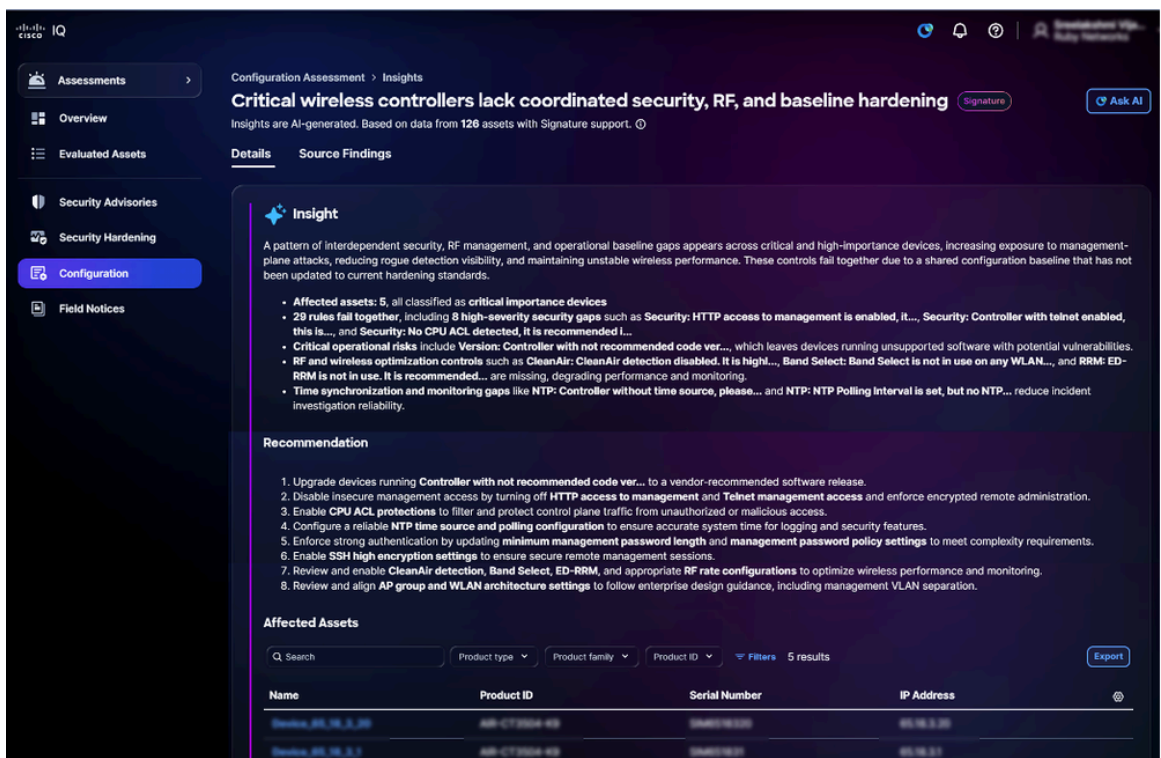
Insights 세부 정보를 보려면

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



인사이트 페이지

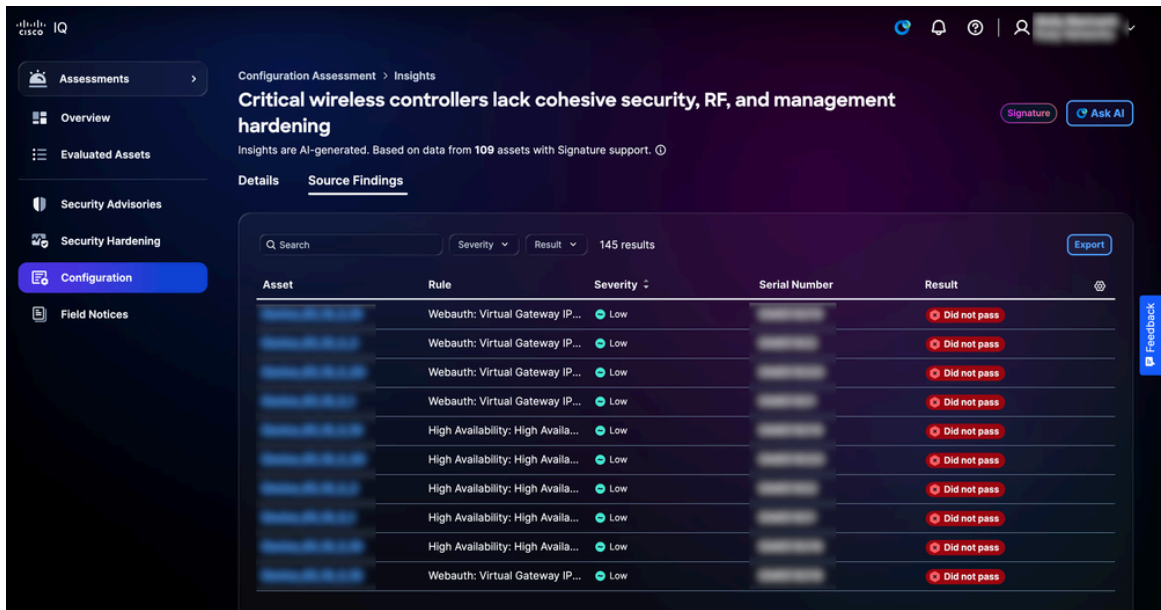
2. 세부 정보 보기를 클릭합니다. 다음 정보와 함께 Insights 세부 정보 페이지가 표시됩니다. 카드를 클릭하여 세부사항 페이지를 열 수도 있습니다.



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 제공
- 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 검색 결과) 페이지에는 통찰력을 지원하는 세부적인 개별 검색 결과가 표시됩니다.



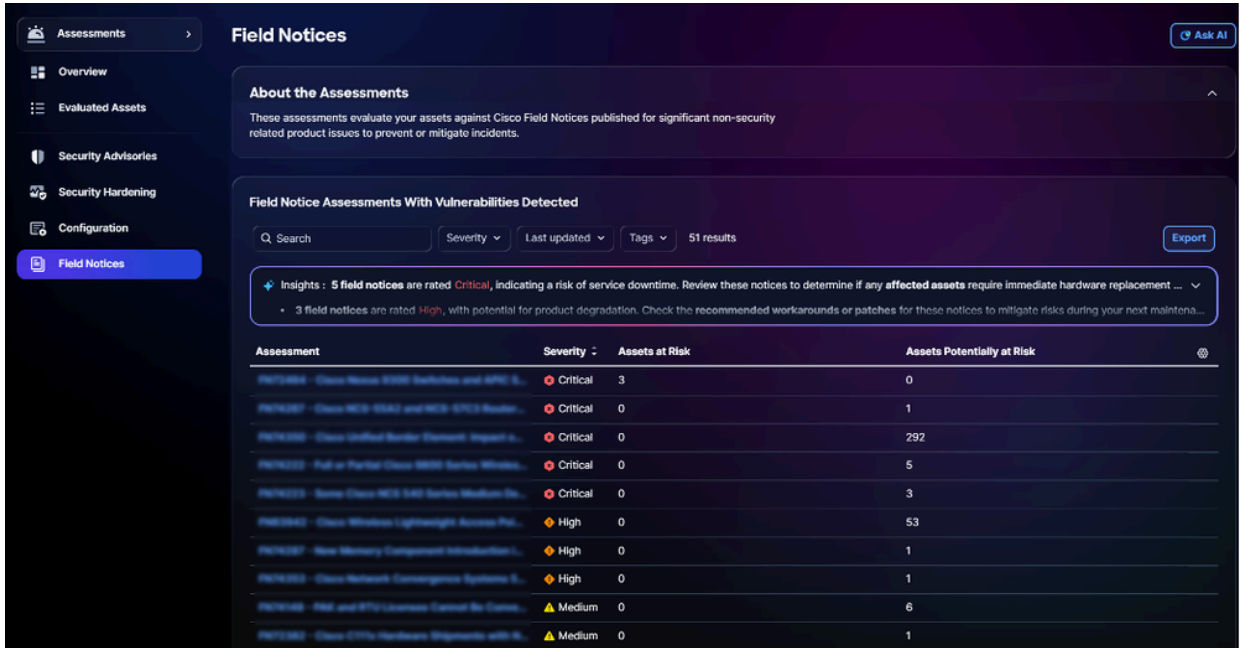
출처 조사 결과

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 알림

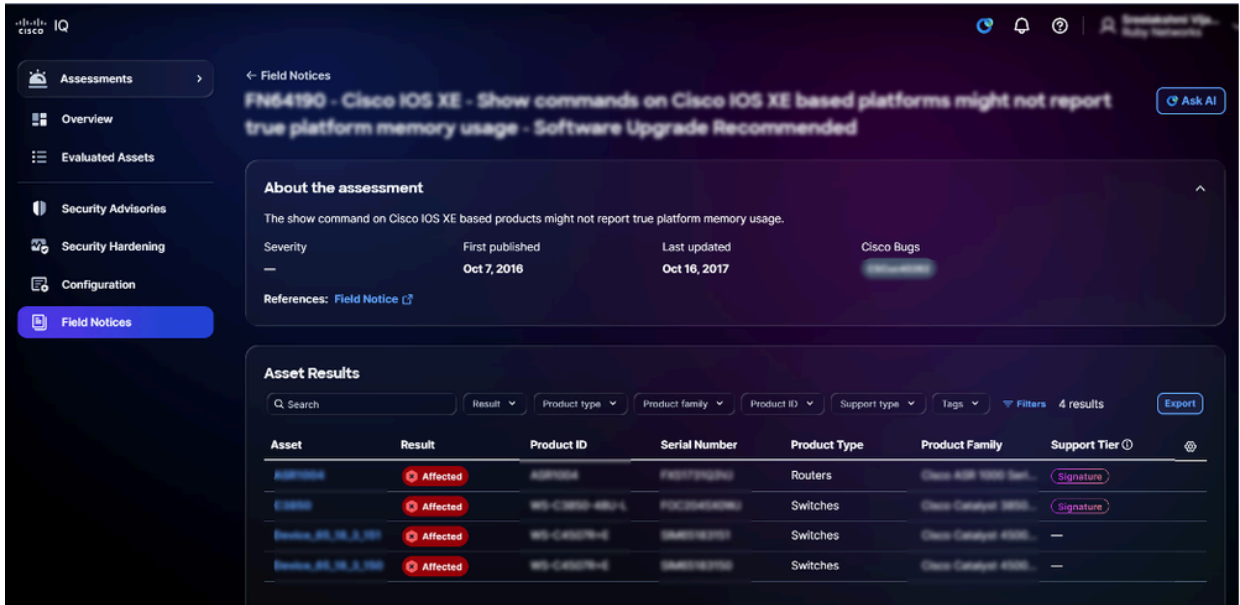
필드 알림에 대한 뷰 검색 및 필터링

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 자산 평가 세부사항이 표시됩니다.


- 평가 정보: 평가의 목적을 요약하여 추가 세부 정보를 제공합니다.
- 탐지된 취약성이 있는 필드 알림 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.

 참고: 역할과 권한에 따라 서로 다른 필터를 사용할 수 있습니다.

Field Notice에 대한 평가 자산 결과 내보내기

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

Field Notice에 대한 평가 자산 결과 보기

평가 자산 결과의 세부 정보를 보려면 Asset Assessment Results에서 자산을 클릭합니다. 평가 자산 결과의 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.

지원 애플리케이션

Support 애플리케이션은 고객 지원 사례에 대한 통합 보기를 제공합니다. 케이스 목록 보기를 필터링, 정렬 및 맞춤화할 수 있으며, 액세스 권한이 있는 미결 케이스와 마감된 케이스 모두에 대한 가시성을 제공합니다.

Cisco IQ에서 Support 애플리케이션에 액세스하려면 Home > Support를 선택합니다. Support Overview(지원 개요) 페이지가 표시됩니다.

지원 개요



지원 개요

Support Overview(지원 개요) 페이지는 다음 정보가 포함된 대화형 그래프 대시보드입니다.

- 심각도별 미결 케이스: 지난 90일 동안 S1~S4 심각도로 분류된 모든 미결 케이스
- 케이스 상태별 케이스 열기: 지난 90일 동안 케이스 상태에 따라 분류된 모든 미결 케이스
- 상태별 RMA: 지난 90일 동안의 모든 RMA를 상태에 따라 분류

- 심각도별 마감된 케이스: 지난 90일 동안 심각도별로 분류되어 종결된 총 사례 수

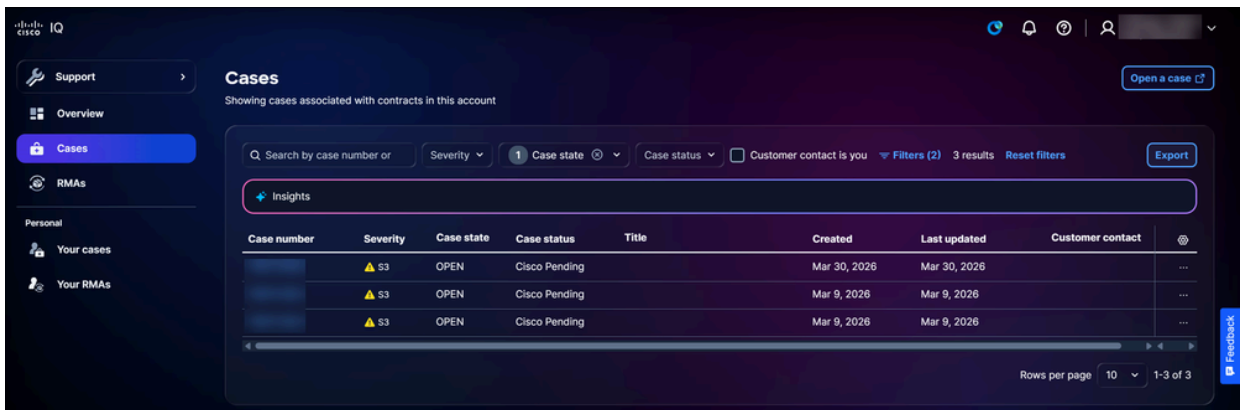
케이스 세부사항 보기

View details(세부 정보 보기)를 클릭하면 페이지가 어카운트의 Cases(케이스) 페이지로 리디렉션됩니다. Overview 페이지 그래프에서 막대를 클릭하면 관련 필터가 적용된 계정의 Cases 페이지로 리디렉션됩니다. 예를 들어, Open Cases by Severity(심각도별 Open Cases) 그래프에서 S1 심각도 막대를 클릭하면 Case status(케이스 상태)가 "Open(열기)"으로, Severity(심각도)가 "S1(S1)"로 설정된 어카운트의 Cases(케이스) 페이지로 리디렉션됩니다. 자세한 내용은 [내용](#)을 케이스를 참조하십시오.

케이스

어카운트 케이스

왼쪽 패널에서 Cases(케이스)를 클릭하여 Cases(케이스) 페이지로 이동합니다.



케이스

Cases(케이스) 페이지에는 Cisco IQ 어카운트의 계약과 관련된 모든 케이스의 통합 목록이 표시됩니다. 설정 아이콘을 클릭하고 원하는 열의 확인란을 선택한 다음 적용을 클릭하여 목록에 표시되는 열을 구성할 수 있습니다. Case number(케이스 번호), Severity(심각도), Case state(케이스 상태), Case status(케이스 상태), Title(제목) 및 Created(생성됨) 열은 항상 표시되며 선택 취소할 수 없습니다.


사용 가능한 작업

Cases(케이스) 페이지에서 다음 작업을 수행할 수 있습니다.

- 케이스 열기: Open a case(케이스 열기)를 클릭하여 [SCM](#)을 교차 실행하고 케이스를 생성함

니다.


- 데이터 내보내기: 대시보드에 현재 표시된 모든 데이터를 CSV 파일로 다운로드하려면 Export(내보내기)를 클릭합니다
- 케이스 세부사항 보기: 케이스 번호 또는 테이블 행을 클릭하여 케이스의 세부사항 보기를 엽니다(자세한 내용은 [케이스 세부사항 보기](#) 참조).
- 케이스 닫기: Open case's More Options 아이콘 > Close case를 선택하여 Close case 창을 엽니다. 이 창에서 마감 이유를 입력하고 케이스를 마감할 수 있습니다
- 케이스 다시 열기: 마감된 케이스의 추가 옵션 아이콘 > 케이스 재개설을 선택하여 케이스 재개설 창을 엽니다. 이 창에서는 재개설 사유를 입력하고 케이스를 열 수 있습니다

 참고: 마감된 케이스는 마감 후 14일 이내에 재접수 가능하다.

케이스 보기 필터링

드롭다운 목록에서 필터를 선택하거나 Customer contact is you 확인란을 선택하여 목록 보기를 필터링할 수 있습니다. 선택적으로, Filters를 클릭하고 사용 가능한 필터 옵션 목록에서 선택합니다. 필터 및 선택 항목은 세션 및 로그인 전반에 걸쳐 유지되어 대시보드를 개인 설정합니다. 적용되는 기본 필터는 다음과 같습니다.

- 케이스 상태: 열림
- 생성됨: 90일 이내에 생성됨

 참고: 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다.

케이스

왼쪽 패널에서 Your Cases를 클릭하여 Your Cases 페이지로 이동합니다.

The screenshot shows the 'Your cases' page in Cisco IQ. The page title is 'Your cases' and it includes a sub-header 'Includes all cases you are authorized to view.' There is a search bar for 'Search by case number' and several filters: 'Severity', 'Case state' (set to 1), 'Case status', and 'Customer contact is you'. The page shows 9 results. Below the filters is an 'Insights' section with the text 'Analyzing your data...'. The main content is a table with the following columns: Case number, Severity, Case state, Case status, Title, Created, Last updated, Customer contact, and an action menu icon. The table contains 9 rows of data. At the bottom right, there is a 'Feedback' button and a footer indicating 'Rows per page 30' and '1-9 of 9'.

Case number	Severity	Case state	Case status	Title	Created	Last updated	Customer contact	
	▲ S3	OPEN	Cisco Pending		Apr 11, 2026	Apr 13, 2026		...
	▲ S3	OPEN	Cisco Pending		Apr 8, 2026	Apr 11, 2026		...
	▲ S3	OPEN	Cisco Pending		Apr 8, 2026	Apr 11, 2026		...
	▲ S3	OPEN	Cisco Pending		Apr 8, 2026	Apr 8, 2026		...
	▲ S3	OPEN	Cisco Pending		Jan 29, 2026	Apr 2, 2026		...
	▲ S3	OPEN	Cisco Pending		Jan 27, 2026	Mar 4, 2026		...
	● S4	OPEN	Cisco Pending		Jan 27, 2026	Feb 24, 2026		...
	● S4	OPEN	Cisco Pending		Jan 27, 2026	Feb 24, 2026		...
	● S4	OPEN	Cisco Pending		Jan 27, 2026	Jan 30, 2026		...

케이스

Your Cases(케이스) 페이지에는 보고 관리할 수 있는 통합 케이스 목록이 표시됩니다. 설정 아이콘을 클릭하고 원하는 열의 확인란을 선택한 다음 적용을 클릭하여 목록에 표시되는 열을 구성할 수 있습니다. Case number(케이스 번호), Severity(심각도), Case state(케이스 상태), Case status(케이스 상태), Title(제목) 및 Created(생성됨) 열은 항상 표시되며 선택 취소할 수 없습니다.

사용 가능한 작업

Your Cases(케이스) 페이지에서 다음 작업을 수행할 수 있습니다.


- 케이스 열기: 케이스 열기: Open a case(케이스 열기)를 클릭하여 SCM을 교차 실행하고 케이스를 생성합니다.
- 데이터 내보내기: 대시보드에 현재 표시된 모든 데이터를 CSV 파일로 다운로드하려면 Export(내보내기)를 클릭합니다
- 케이스 세부사항 보기: 케이스 번호 또는 테이블 행을 클릭하여 케이스의 세부사항 보기를 엽니다(자세한 내용은 [케이스 세부사항 보기](#) 참조).
- 케이스 닫기: Open case's More Options 아이콘 > Close case를 선택하여 Close case 창을 엽니다. 이 창에서 마감 이유를 입력하고 케이스를 마감할 수 있습니다
- 케이스 다시 열기: 마감된 케이스의 추가 옵션 아이콘 > 케이스 재개설을 선택하여 케이스 재개설 창을 엽니다. 이 창에서는 재개설 사유를 입력하고 케이스를 열 수 있습니다

참고: 마감된 케이스는 마감 후 14일 이내에 재접수 가능하다.

케이스 보기 필터링

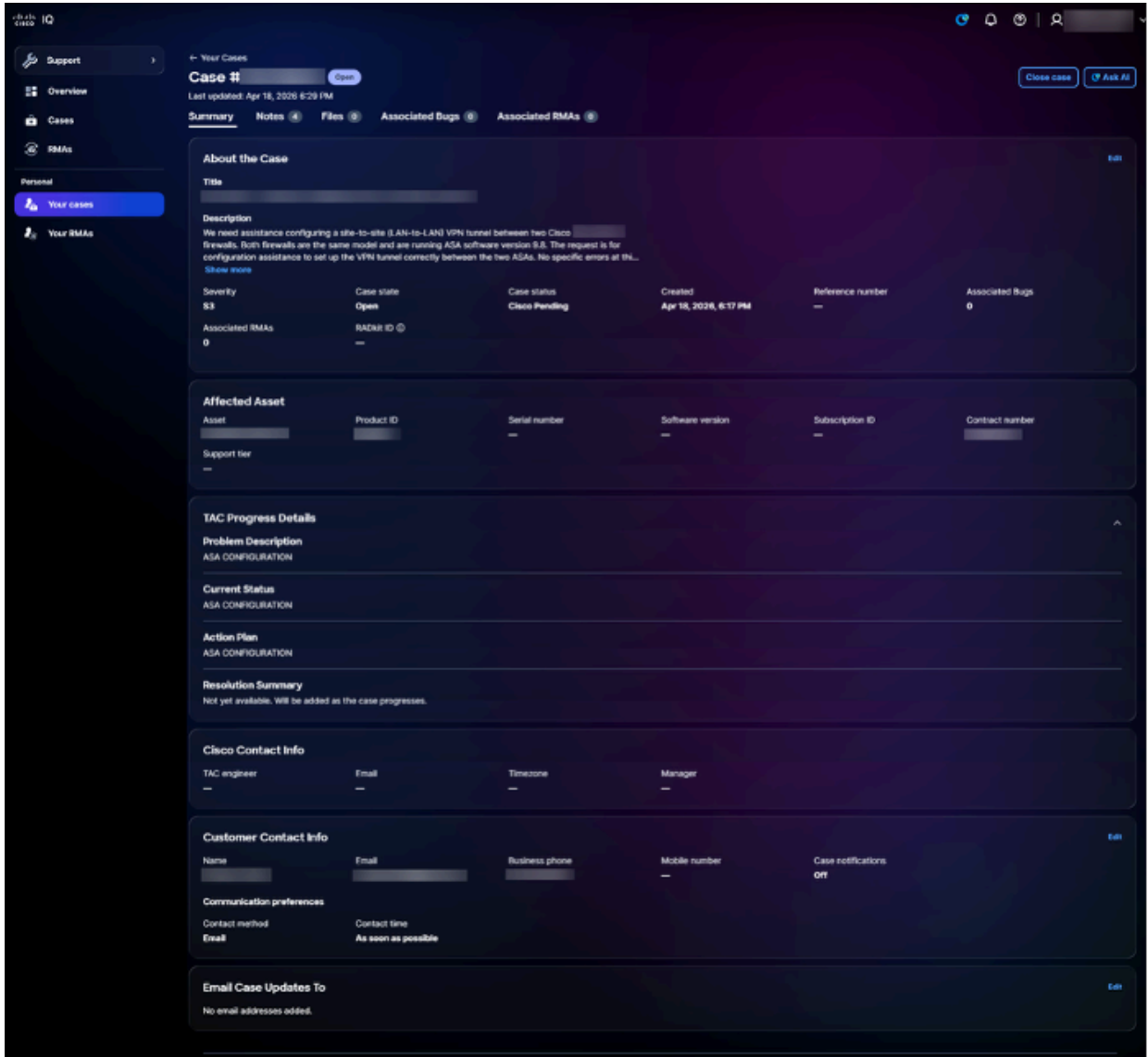
드롭다운 목록에서 필터를 선택하거나 Customer contact is you 확인란을 선택하여 목록 보기를 필터링할 수 있습니다. 선택적으로, Filters를 클릭하고 사용 가능한 필터 옵션 목록에서 선택합니다. 필터 및 선택 항목은 세션 및 로그인 전반에 걸쳐 유지되어 대시보드를 개인 설정합니다. 적용되는 기본 필터는 다음과 같습니다.

- 케이스 상태: 열림
- Customer contact is you 확인란
- 생성됨: 90일 이내에 생성됨

 참고: 일부 필터는 화면 확대/축소 설정에 따라 숨겨질 수 있습니다.


케이스 세부사항 보기

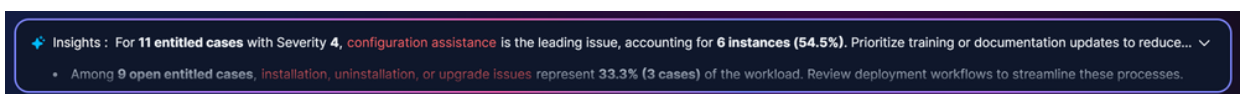
케이스의 세부사항을 보려면 목록에서 케이스를 클릭합니다.



케이스 세부사항 보기

케이스 세부사항 보기에는 지원 케이스의 중앙 집중식 보기가 표시되며, 이를 통해 케이스 정보, 영향을 받은 자산 정보를 검토하고 TAC 진행 상황을 추적하고 사용 가능한 케이스 작업에 액세스할 수 있습니다. 활용 가능한 작업으로는 마감된 케이스를 Reopen(재개설)을 클릭하여 재개설하고, 케이스 마감을 클릭하여 마감한 케이스를 마감하며, 케이스의 컨텍스트가 있는 AI Assistant를 Ask AI(AI에게 문의)를 클릭하여 실행하는 작업 등이 있습니다. 사용 가능한 탭은 아래 섹션에 설명되어 있습니다.

 참고: AI가 생성한 필드는 해당하는 경우 Star 아이콘으로 표시됩니다.

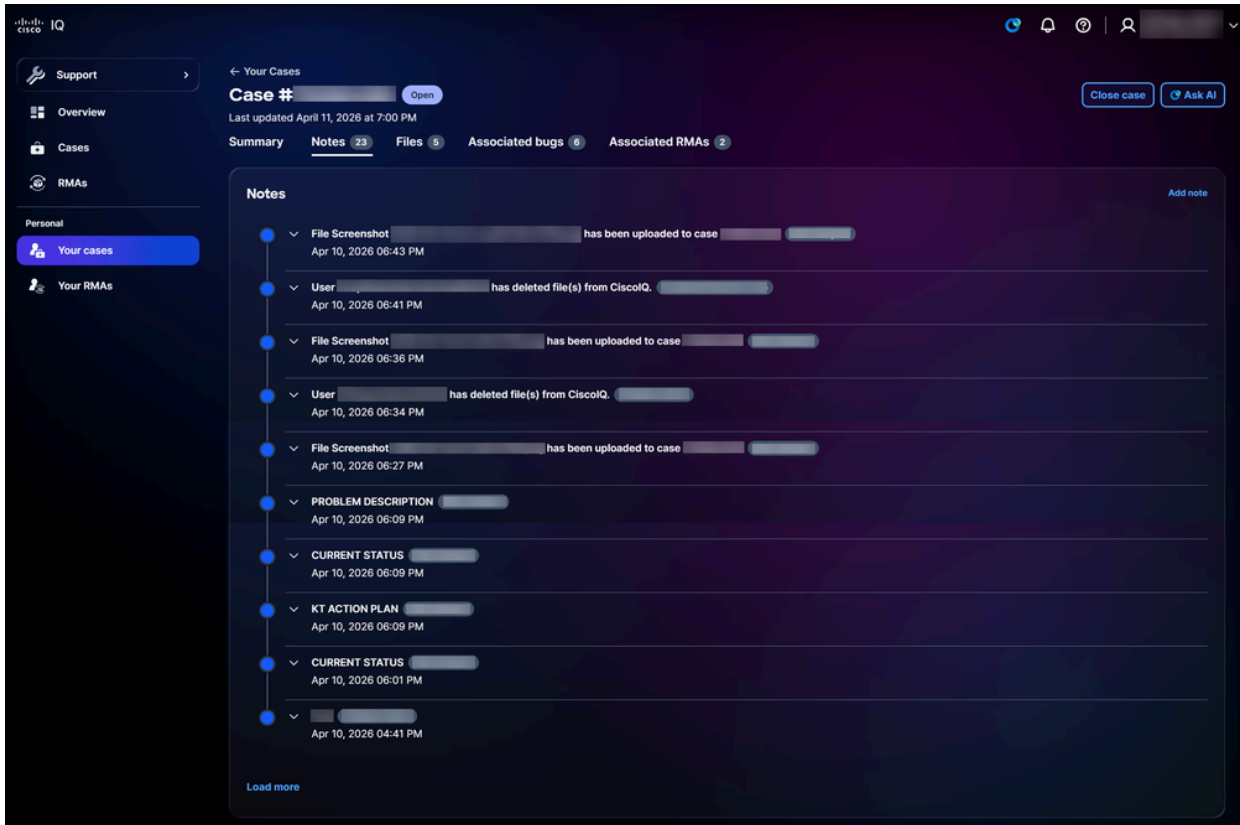


별 아이콘

요약

Summary 탭에는 주요 케이스 정보가 표시되므로 개별 지원 케이스의 현재 상태, 컨텍스트 및 진행 상황을 신속하게 파악할 수 있습니다. 케이스 세부사항 및 영향을 받는 자산을 검토하고, TAC 진행 세부사항을 통해 케이스의 라이프사이클을 모니터링하고, 연락처 정보를 수정하고, 케이스 업데이트 알림을 수신할 이메일 주소를 지정할 수 있습니다. 선택 필드만 편집할 수 있습니다.


참고



참고

메모 탭을 클릭하면 메모 페이지가 열립니다. 고객 또는 시스코 엔지니어가 케이스를 제출했는지 여부와 관련된 모든 메모를 볼 수 있습니다.

새 메모를 추가하려면

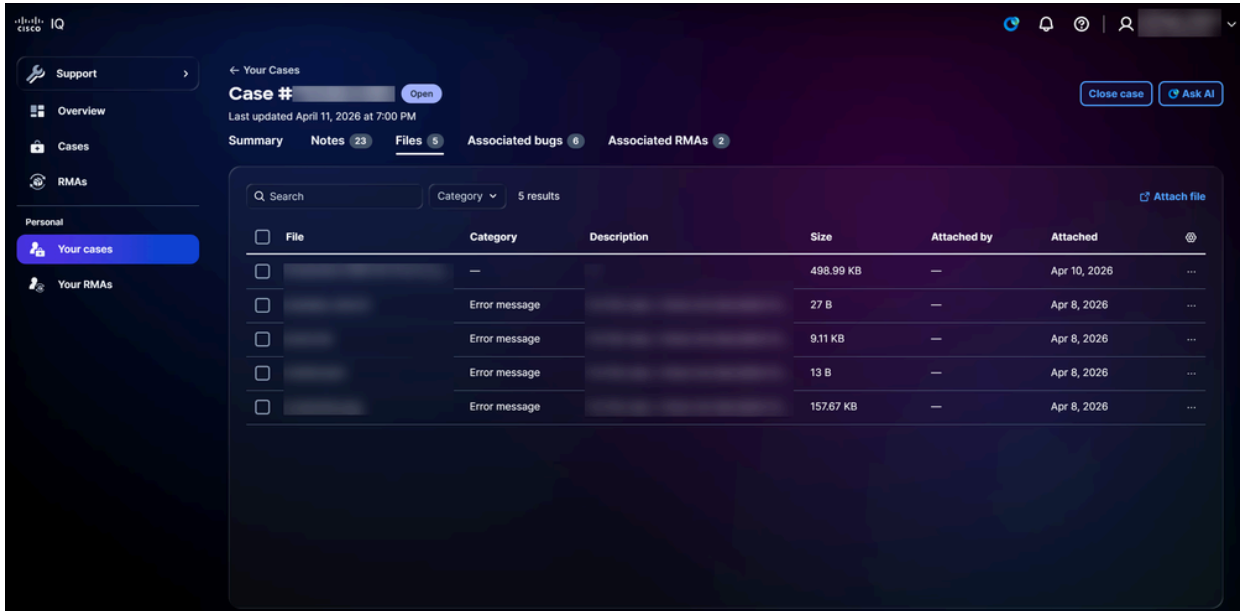
 경고: 메모를 삭제할 수 없습니다.

1. 메모 추가를 클릭합니다. 메모 추가 창이 열립니다.
2. 제목을 입력합니다.

3. Details(세부사항)를 입력합니다.

4. Add(추가)를 클릭합니다.

파일




파일

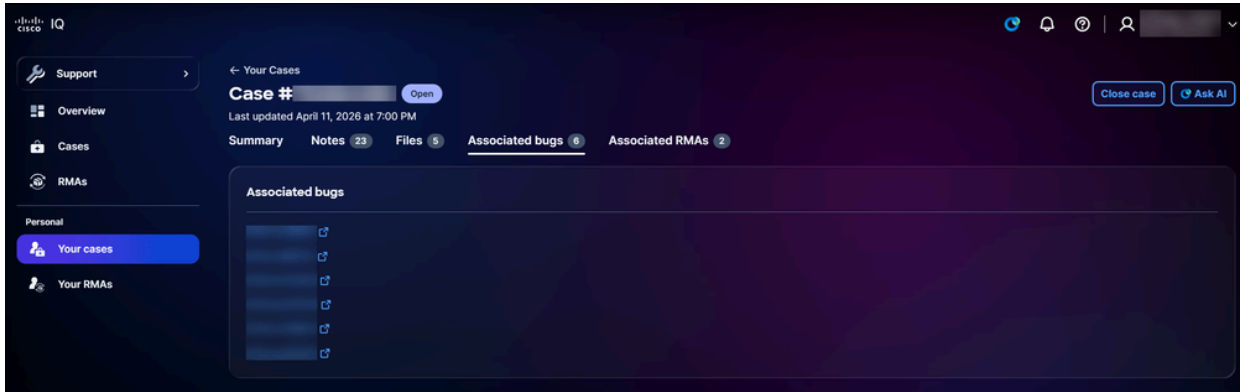
파일 탭을 클릭하면 파일 페이지가 열립니다. 케이스 파일의 이름, 크기 및 날짜를 보고 추가 또는 삭제할 수 있습니다. Category 드롭다운 목록에서 옵션을 선택하여 파일을 필터링합니다. 선택적으로, Filters(필터)를 클릭하고 사용 가능한 필터 옵션 중에서 선택합니다. 설정 아이콘 을 클릭하고 원하는 열의 확인란을 선택한 다음 적용을 클릭하여 목록에 표시되는 열을 구성할 수도 있습니다.

파일을 추가하려면 파일 첨부를 클릭합니다. 케이스에 대한 파일을 업로드할 수 있는 SCM으로 리디렉션됩니다.

파일을 삭제하려면 원하는 파일의 확인란을 선택하고 삭제를 클릭합니다. 파일 삭제 창이 열립니다. Delete file(s)(파일 삭제)을 클릭합니다.

 참고: 파일 다운로드 는 지원되지 않습니다.

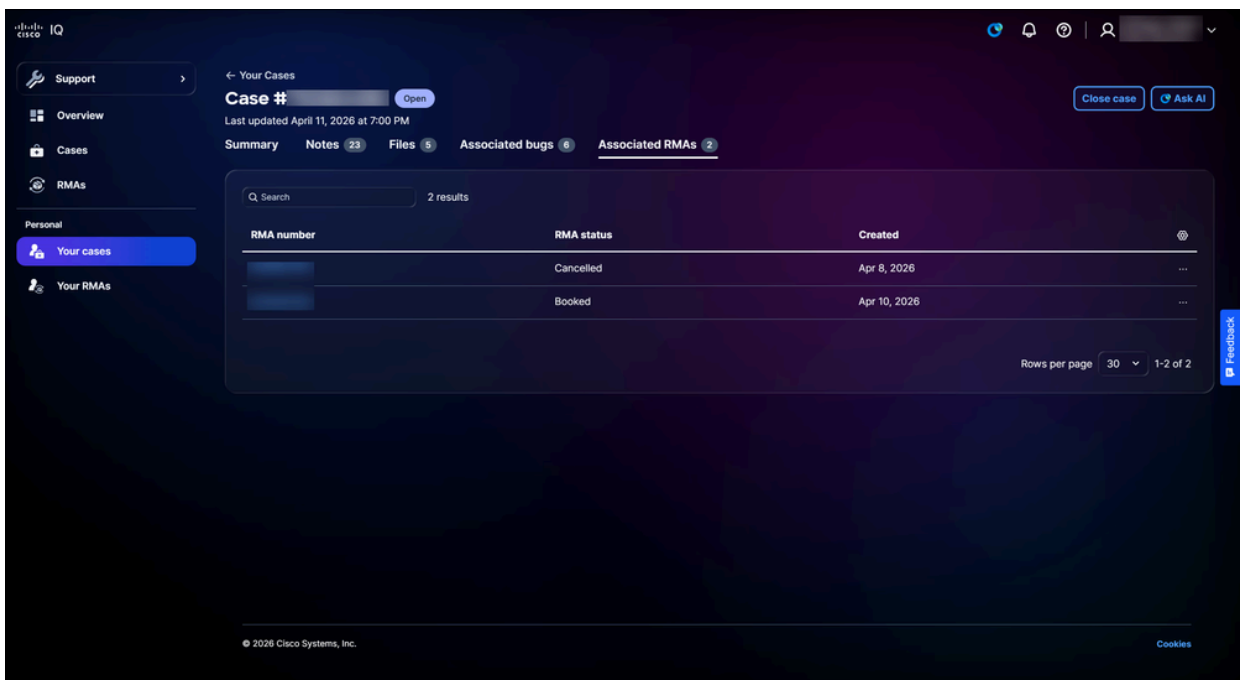
연결된 버그



연결된 버그

Associated bugs(연결된 버그) 탭을 클릭하면 Associated bugs(연결된 버그) 페이지가 열립니다. 버그의 ID를 클릭하면 Cisco.com의 Bug [Search](#) Tool에서 자세한 버그 정보를 교차 실행할 수 있습니다.

관련 RMA



관련 RMA

Associated RMAs(연결된 RMA) 탭을 클릭하면 Associated RMAs(연결된 RMA) 페이지가 열립니다. 설정 아이콘을 클릭하고 원하는 열의 확인란을 선택한 다음 적용을 클릭하여 목록에 표시되는 열을 구성할 수 있습니다. 관련 RMA 페이지에서 다음 작업을 수행할 수 있습니다.

- 케이스 닫기: 케이스 닫기를 클릭하여 케이스 닫기 창을 엽니다. 이 창에서는 케이스 닫기 이유를 제공하고 케이스를 닫을 수 있습니다
- RMA 세부사항 보기: RMA 번호 또는 테이블 행을 클릭하여 RMA의 세부사항 보기를 엽니다

(자세한 내용은 [RMA 세부사항 보기](#) 참조).

- Cisco 물류 팀에 문의: 행의 More Options(추가 옵션) 아이콘 > Contact Cisco logistics(Cisco 물류 팀에 문의)를 선택하여 Cisco 물류 팀에 문의하십시오.

RMA

계정 RMA

RMA number	RMA status	Associated case number	Created
	Booked		Apr 10, 2026
	Cancelled		Apr 8, 2026
	Cancelled		Apr 8, 2026
	Closed		Jan 26, 2026
	Closed		Dec 11, 2025
	Closed		Oct 22, 2025
	Closed		Oct 7, 2025
	Closed		Oct 1, 2025
	Closed		Sep 15, 2025
	Closed		Sep 8, 2025

RMA 목록

왼쪽 패널에서 RMA를 클릭하여 RMA 페이지로 이동합니다. RMA 페이지는 Cisco IQ 어카운트의 케이스와 관련된 모든 RMA의 통합 목록을 표시합니다. 설정 아이콘 을 클릭하고 원하는 열의 확인란을 선택한 다음 적용을 클릭하여 목록에 표시되는 열을 구성할 수 있습니다.

사용 가능한 작업

RMA 페이지에서 다음 작업을 수행할 수 있습니다.

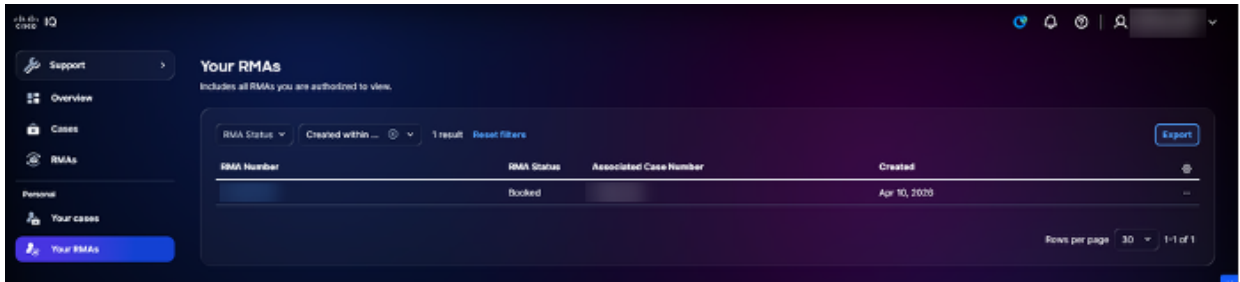
- 데이터 내보내기: 현재 CSV 파일로 표시된 모든 데이터를 다운로드하려면 Export를 클릭합니다.
- RMA 세부사항 보기: RMA 번호 또는 테이블 행을 클릭하여 RMA의 세부사항 보기를 엽니다 (자세한 내용은 [RMA 세부사항 보기](#) 참조).
- Cisco 물류 팀에 문의: 행의 More Options(추가 옵션) 아이콘 > Contact Cisco logistics(Cisco 물류 팀에 문의)를 선택하여 Cisco 물류 팀에 문의하십시오.

어카운트 RMA 보기 필터링

드롭다운 목록에서 필터를 선택하여 목록 보기를 필터링할 수 있습니다.

RMA

왼쪽 패널에서 Your RMAs(RMA)를 클릭하여 Your RMAs(RMA) 페이지로 이동합니다.



RMA

Your RMAs (RMA) 페이지에는 보고 관리하는 데 필요한 엔타이틀먼트를 보유한 RMA의 통합 목록이 표시됩니다. 설정 아이콘을 클릭하고 원하는 열의 확인란을 선택한 다음 적용을 클릭하여 목록에 표시되는 열을 구성할 수 있습니다.

사용 가능한 작업

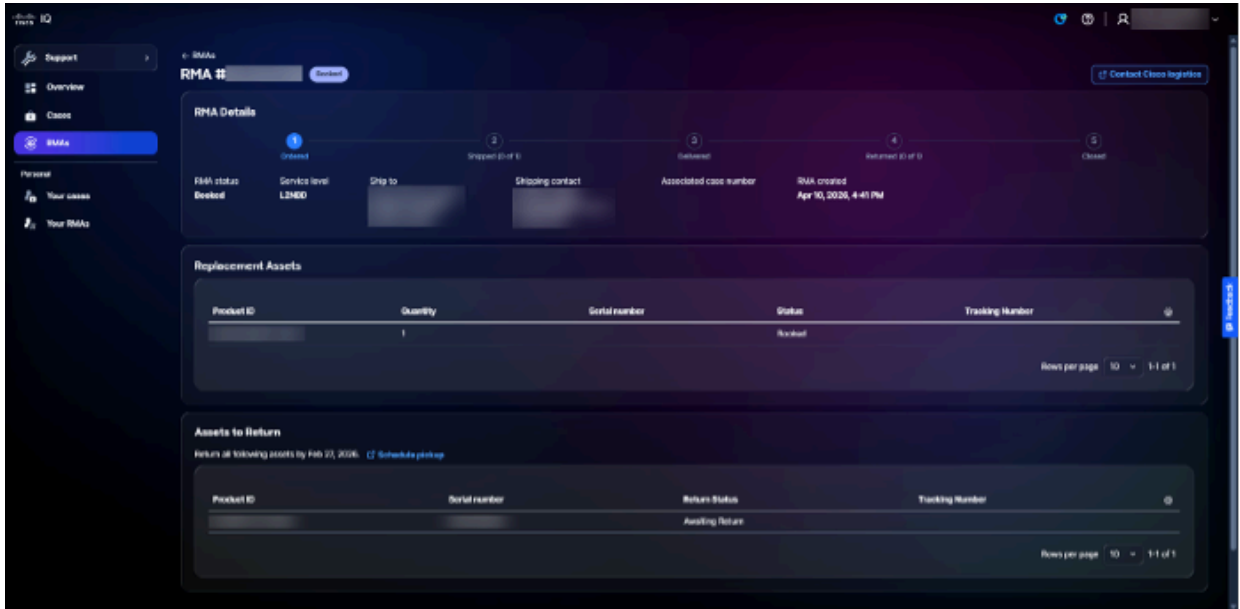
RMA 페이지에서 다음 작업을 수행할 수 있습니다.

- 데이터 내보내기: 현재 CSV 파일로 표시된 모든 데이터를 다운로드하려면 Export를 클릭합니다.
- RMA 세부사항 보기: RMA 번호 또는 테이블 행을 클릭하여 RMA의 세부사항 보기를 엽니다 (자세한 내용은 [RMA 세부사항 보기](#) 참조).
- Cisco 물류 팀에 문의: 행의 More Options(추가 옵션) 아이콘 > Contact Cisco logistics(Cisco 물류 팀에 문의)를 선택하여 Cisco 물류 팀에 문의하십시오.

RMA 보기 필터링

작성된 드롭다운 목록에서 옵션을 선택하여 목록 보기를 필터링할 수 있습니다.

RMA 세부사항 보기




RMA 세부사항 보기

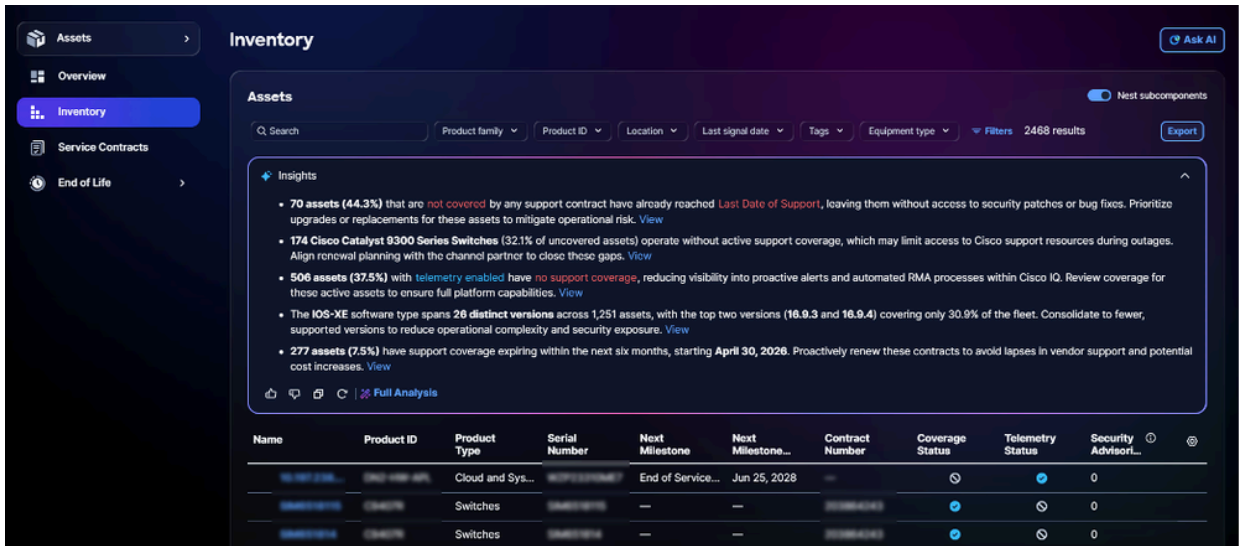
RMA 세부사항 보기는 RMA의 중앙 집중식 보기를 제공하므로 RMA 정보를 검토하고, 진행 상황을 추적하고, 사용 가능한 RMA 작업에 액세스할 수 있습니다. Cisco 물류 팀에 문의, 추적 번호 액세스, 자산 픽업 예약 등의 작업을 수행할 수 있습니다.

공통 애플리케이션 기능

데이터 분석

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

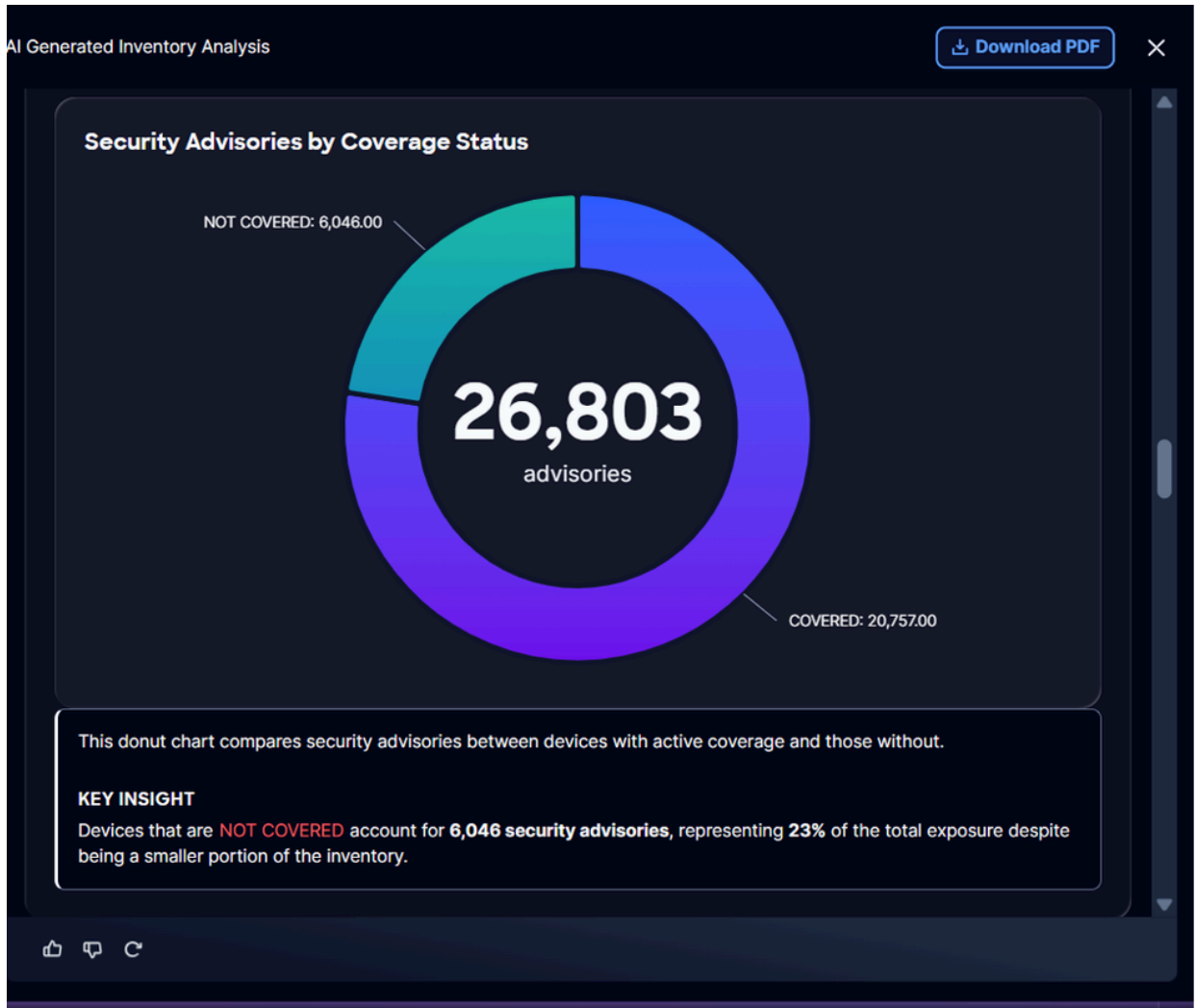
 참고: 분석 기능은 선택한 페이지에서만 사용할 수 있습니다.



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 시가 생성한 정보에 대한 피드백을 제공합니다
- Full Analysis(전체 분석)를 클릭하여 추가 정보, 심층 분석, 그래프, 대시보드, 차트 등의 시각화를 표시합니다.




전체 분석

전체 분석 내에서 다음 옵션을 사용할 수 있습니다.

- 기록 또는 협업을 위해 분석의 오프라인 사본을 저장하려면 Download PDF(PDF 다운로드)를 클릭합니다

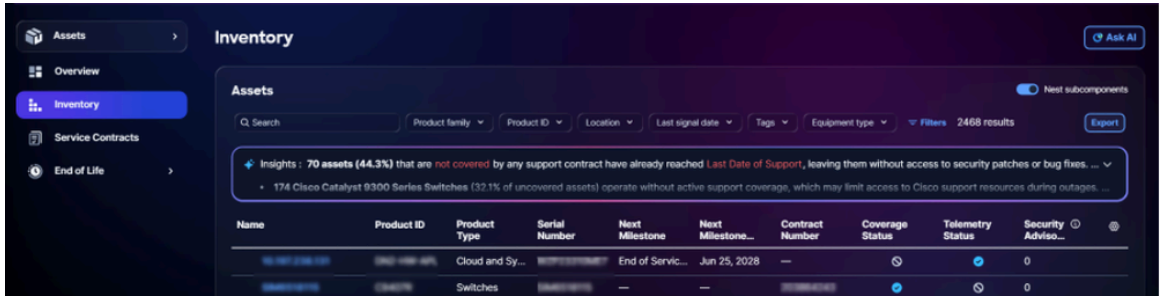
정보 내보내기

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.

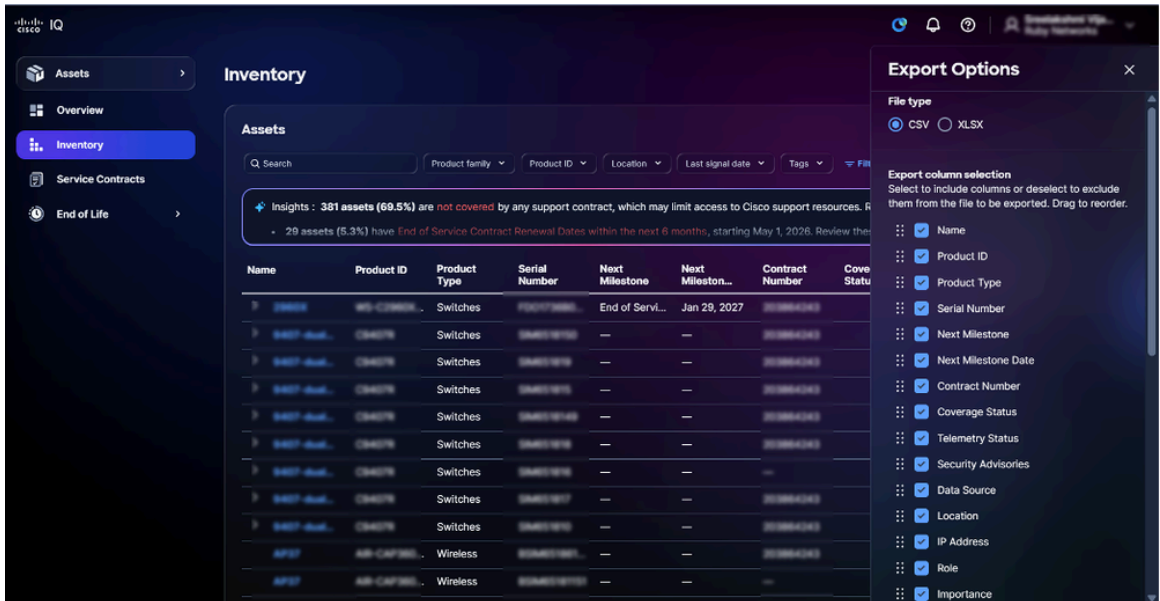
페이지에서 정보를 내보내려면 다음을 수행합니다.

1. 해당 페이지로 이동합니다.



Assets 애플리케이션에서 인벤토리 내보내기

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



내보내기 옵션

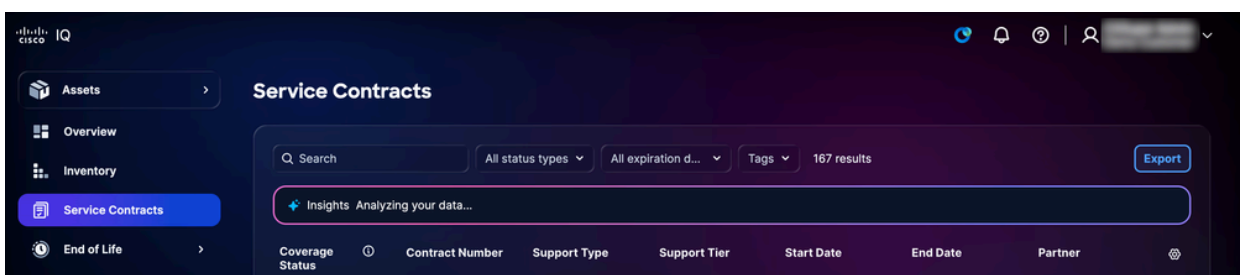
3. 파일 유형을 선택합니다.

4. 원하는 열의 확인란을 선택합니다.

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

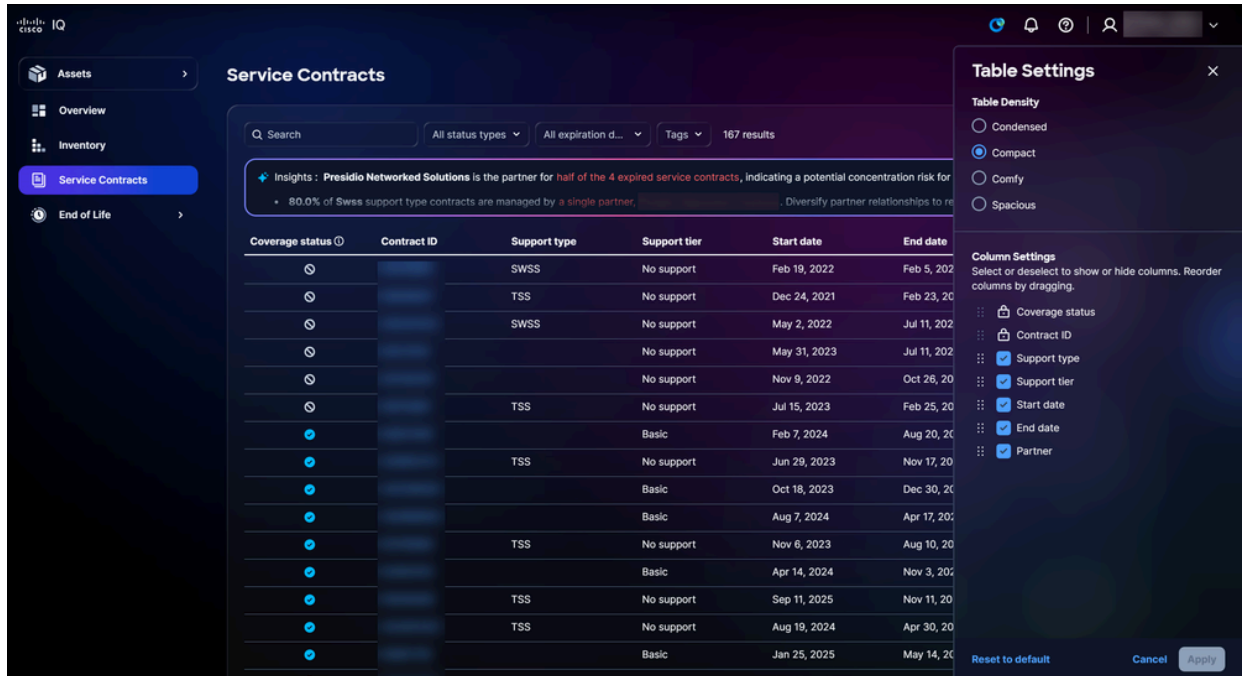
테이블 설정

서로 다른 응용 프로그램 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 재배열
- 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.



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.

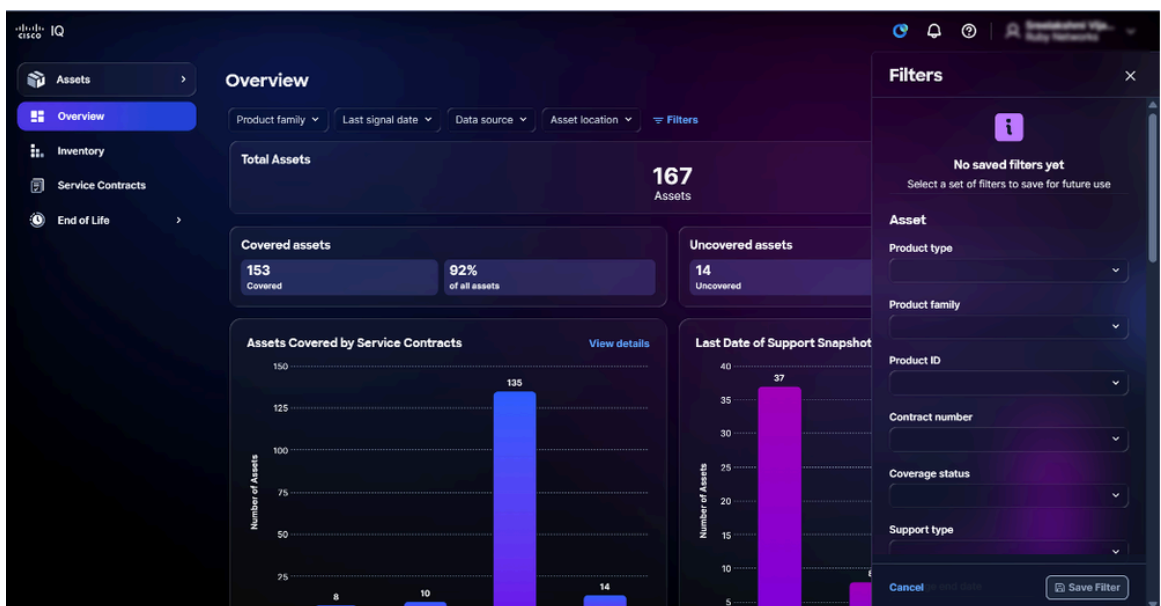
필터 사용자 정의

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.

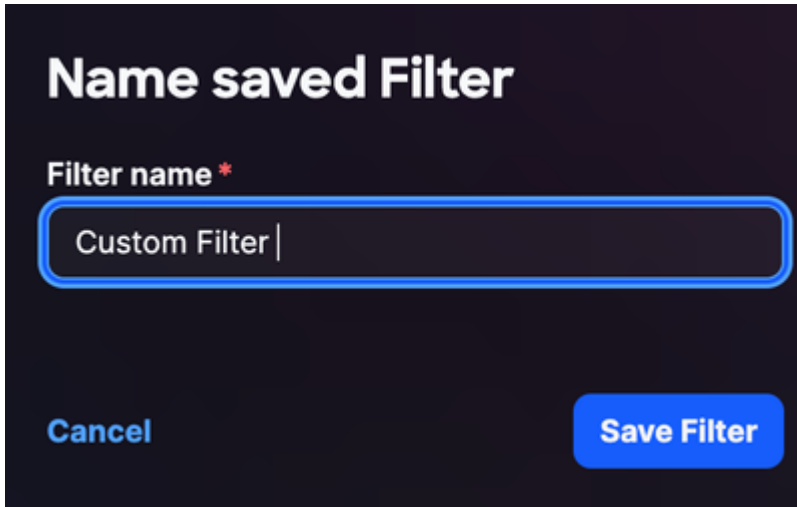
필터 생성

사용자 지정 필터를 생성하려면

1. 대시보드로 이동합니다.
2. Filters를 클릭합니다.



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



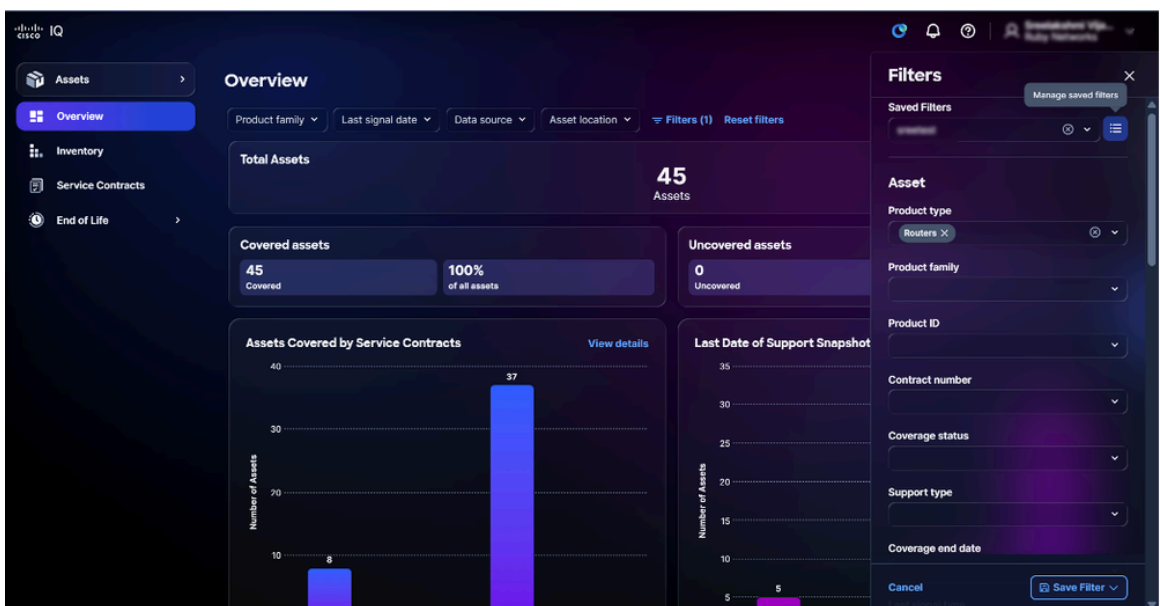
필터 이름

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

필터 이름 수정

사용자 지정 필터를 수정하려면

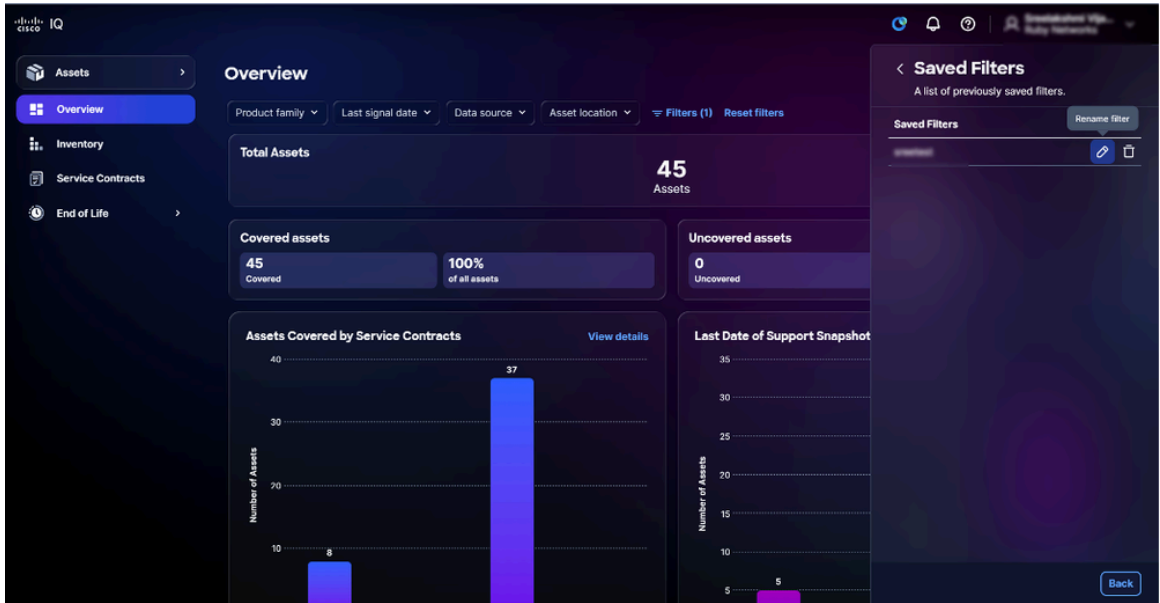
1. Filters를 클릭합니다.



저장된 필터 관리

2. Managed saved filters(관리되는 저장된 필터) 아이콘을 클릭합니다.

3. 필터로 이동합니다.



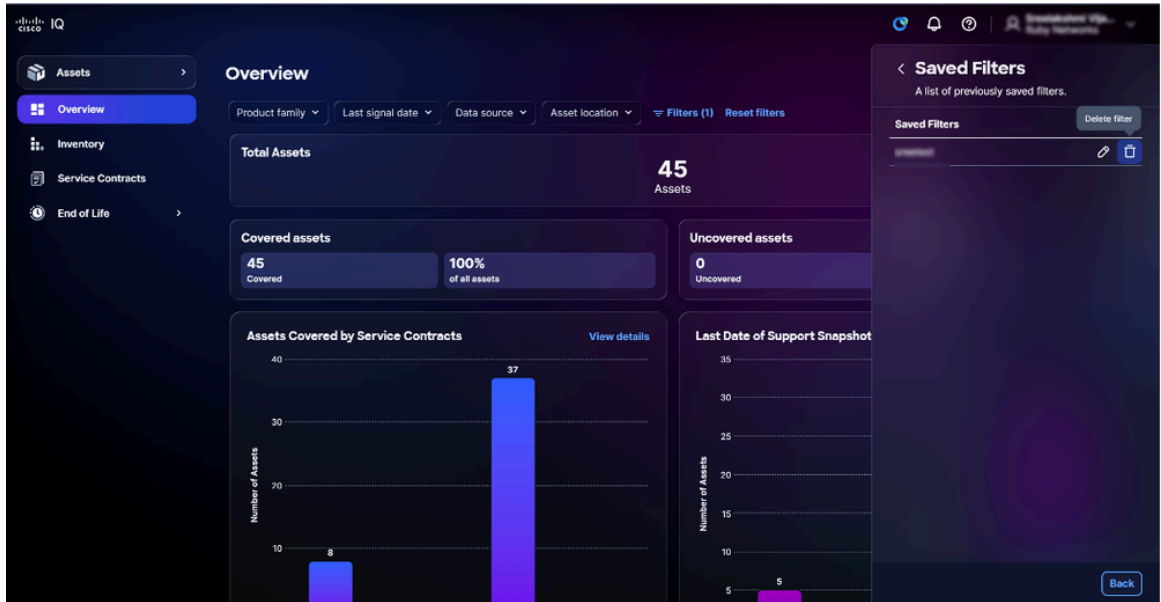
필터 편집

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. Managed Saved Filters(관리되는 저장된 필터) 아이콘을 클릭합니다
3. 필터로 이동합니다.



저장된 필터 삭제

4. 삭제 아이콘을 클릭합니다. Delete saved filter 창이 열립니다.
5. 예, 삭제를 클릭하여 확인합니다.

AI Assistant


개요

Cisco IQ AI Assistant는 원시 데이터를 실행 가능한 통찰력, 권장 사항 및 안내된 작업으로 변환하여 Cisco IQ에 대한 이해와 사용을 향상하도록 설계되었습니다. 또한 개별 데이터 소스를 활용하고 여러 데이터 스트림 전반에 걸쳐 인텔리전스를 종합하여 실시간 제안을 제공하는 기존 틀에 통합됩니다. Cisco IQ AI Assistant는 사용자가 사전 대응적이고 정보에 근거한 결정을 내리고 고객 참여와 성공을 위한 프로세스를 간소화할 수 있도록 상황에 맞는 이해를 제공함으로써 운영 성과를 최적화하고 Cisco IQ 사용자 경험을 향상시킵니다.

Cisco IQ AI Assistant의 기능은 다음과 같습니다.

- 강력한 에지 케이스 처리: 투명한 설명과 명확한 방향 전환을 통해 원활한 지원 환경과 더 높은 사용자 만족도 보장
- 스트리밍 기능: 생성된 응답 보기
- 향상된 상황 데이터: 동적 상황 정보를 통해 애플리케이션, 페이지, 세션 간에 원활한 상호 작용 지원
- 케이스 관리 지원: Cases(케이스) 목록 보기에 표시되는 케이스 생성, 보기 및 관리

- 자산 재고 관리: 조직의 자산 또는 리소스에 대한 보고서 추적, 관리 및 생성
- 자산 중요도: 네트워크 내에서 자산의 역할과 중요도에 따라 위험 완화 활동을 위한 자산의 우선 순위 지정
- 위험 평가 및 관리: 조직의 자산과 관련된 잠재적 위험 평가 및 관리
- 보안 강화: 지원되는 장치에 대한 고객의 장치 실행 컨피그레이션을 관련 Cisco 및 CISA(Cybersecurity and Infrastructure Security Agency) 강화 지침과 비교
- 설정: 권장 모범 사례와 비교하여 고객 디바이스 실행 컨피그레이션을 평가하고 컨피그레이션 편차를 파악하고 실행 가능한 권장 사항을 제공합니다.

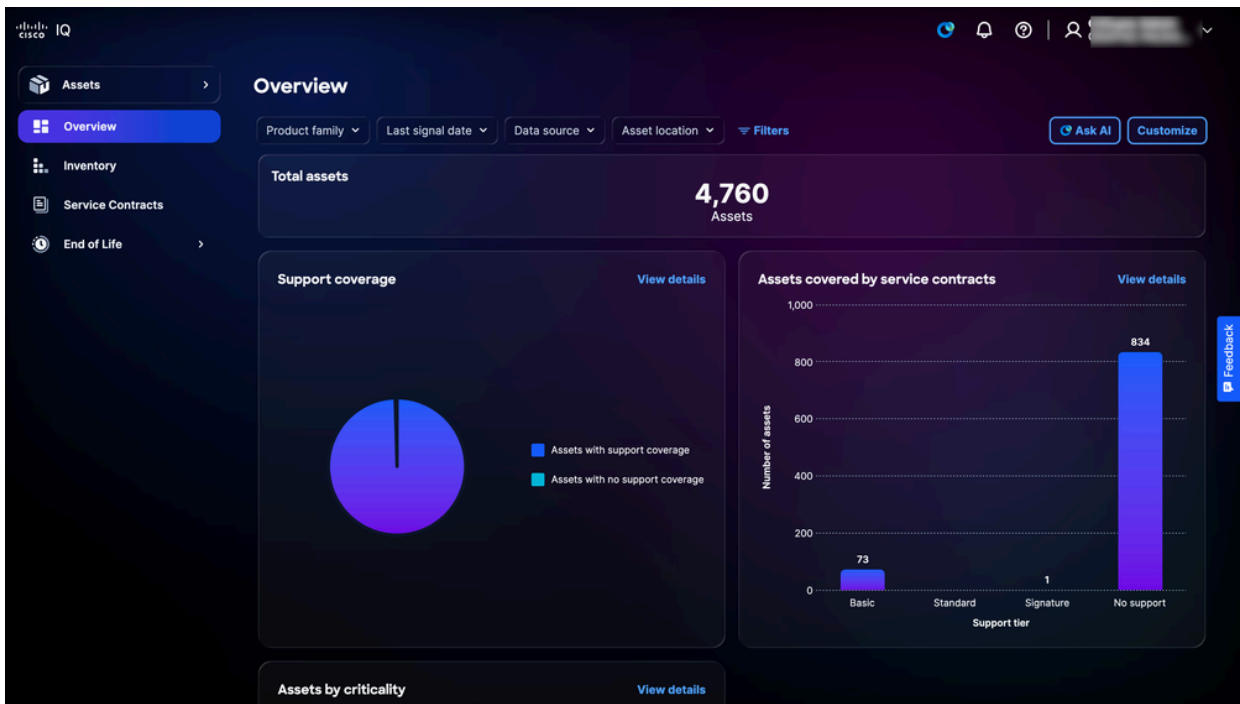
 참고: Cisco IQ AI Assistant는 Cisco IQ 내 어디서나 실행할 수 있습니다. 모든 사용자가 사용할 수 있지만 제공되는 기능은 지원 계층 레벨(기본, 표준 또는 서명)에 따라 다릅니다.

Cisco IQ AI Assistant 액세스


Cisco IQ AI Assistant를 사용하려면

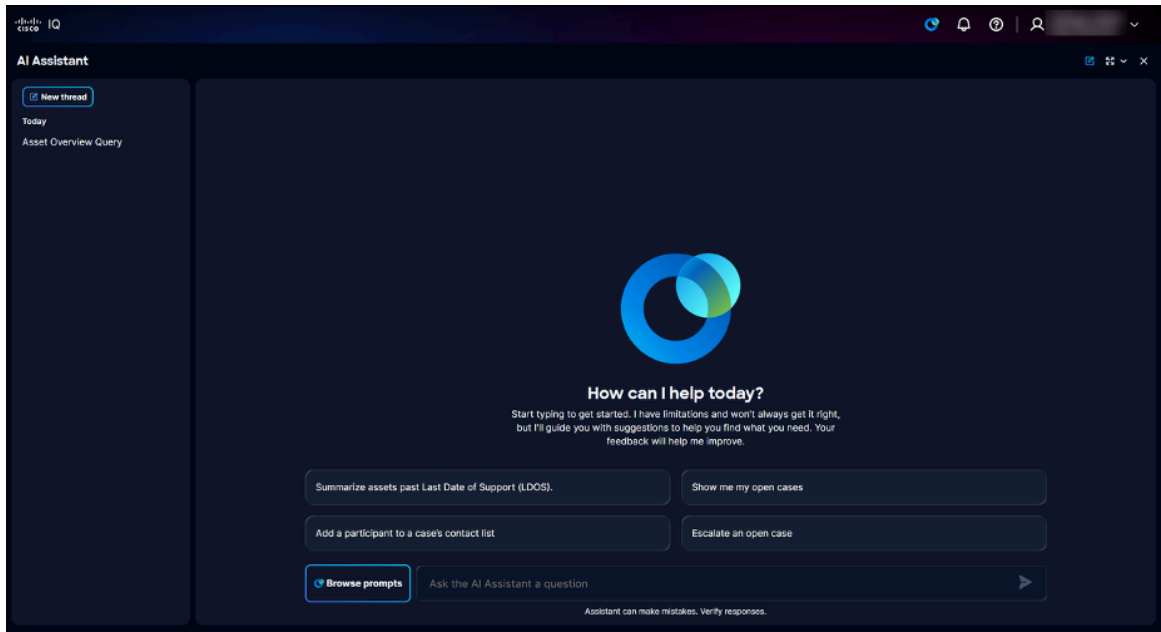


AI Assistant 아이콘




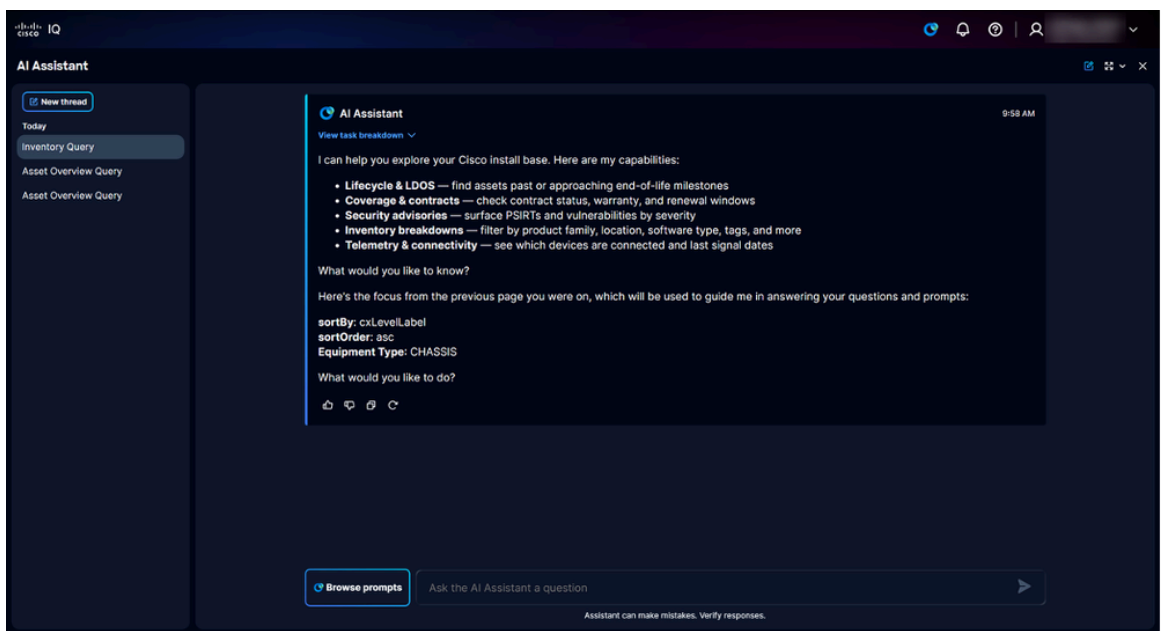
1. AI Assistant 아이콘을 클릭하거나 Ask AI(AI에게 묻기)를 클릭하여 Cisco IQ AI Assistant를 시작합니다.


 참고: Cisco IQ 내의 아무 곳에서도 이 두(2) 옵션을 클릭하여 Cisco IQ AI Assistant에 액세스할 수 있습니다. 사용자가 실행하는 특정 페이지의 데이터와 컨텍스트를 활용하여 관련성이 높은 통찰력과 권장 사항을 제공할 수 있도록 합니다. 현재 작업을 이해하여 맞춤형 지침, 문제 해결 단계 및 효율성 향상을 제공합니다.



랜딩 페이지

 참고: 새 프롬프트를 입력하거나 미리 만든 프롬프트 라이브러리를 찾아볼 수 있습니다.



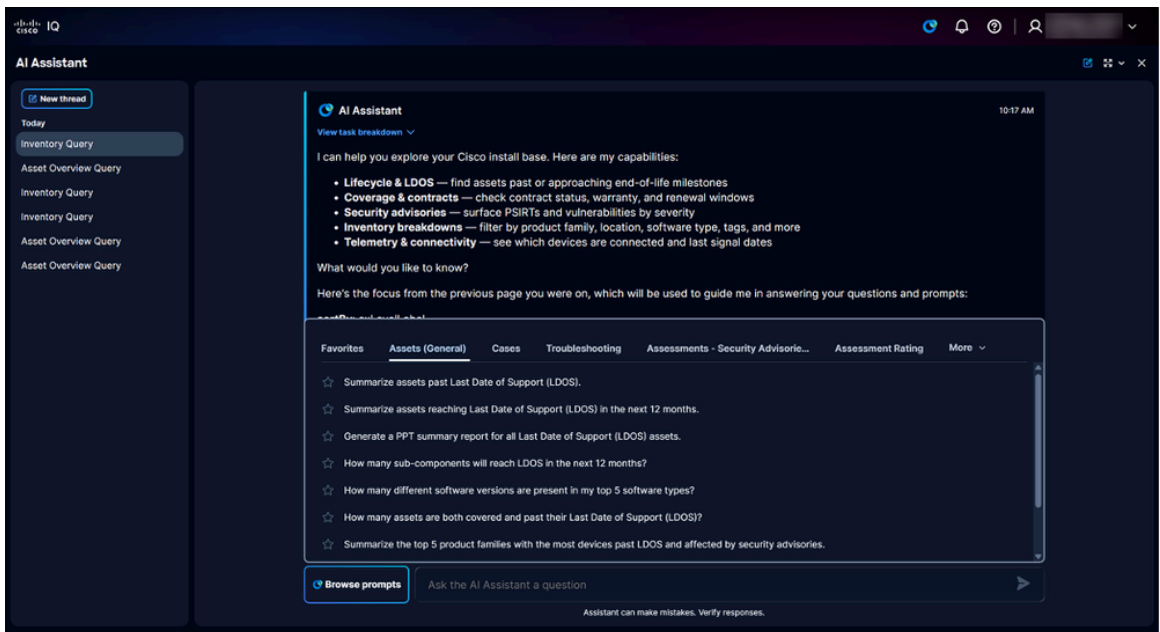
 참고: 기본적으로 Cisco IQ AI Assistant의 보기는 전체 화면으로 설정됩니다. 새 보기를 선택하면 Cisco IQ AI Assistant는 이전에 선택한 보기를 유지합니다.

Cisco IQ AI Assistant에는 다음과 같은 사용 가능한 옵션이 표시됩니다.

- 이전 스레드: 30일간의 프롬프트 기록을 제공합니다.
- 찾아보기 프롬프트: 프롬프트 라이브러리를 엽니다. [부록 A](#)를 참조하십시오. [Cisco IQ AI Assistant 프롬프트 라이브러리](#)에서 사용 가능한 모든 질문의 목록을 묻는 프롬프트
- AI Assistant에게 질문 필드를 요청합니다. AI Assistant에게 질문을 할 텍스트 필드; 더 나은 응답을 받기 위해 서술적인 문장 전체 사용

2. 다음 방법 중 하나를 사용하여 프롬프트를 선택합니다.

- AI Assistant에게 질문하기 필드에 하나 이상의 키워드를 입력하여 프롬프트를 검색하고 프롬프트를 클릭합니다
- AI Assistant에게 질문하기 필드에 설명 문장과 전체 문장을 사용하여 자유 형식 질문을 입력합니다



프롬프트 라이브러리

- 프롬프트 라이브러리를 열고 다음 프롬프트 범주 탭 중 하나를 선택 하려면 프롬프트 찾아보기를 클릭 합니다.
 - 자산(일반): LDOS 및 일반 인벤토리 쿼리를 비롯한 자산 라이프사이클과 관련된 프롬프트
 - 사례: 케이스 보기, 업데이트, 에스컬레이션, 마감과 같은 케이스 관리 작업을 지원하라는 메시지가 표시되므로 효율적인 추적 및 Cisco 지원 엔지니어

와의 연결이 가능합니다.

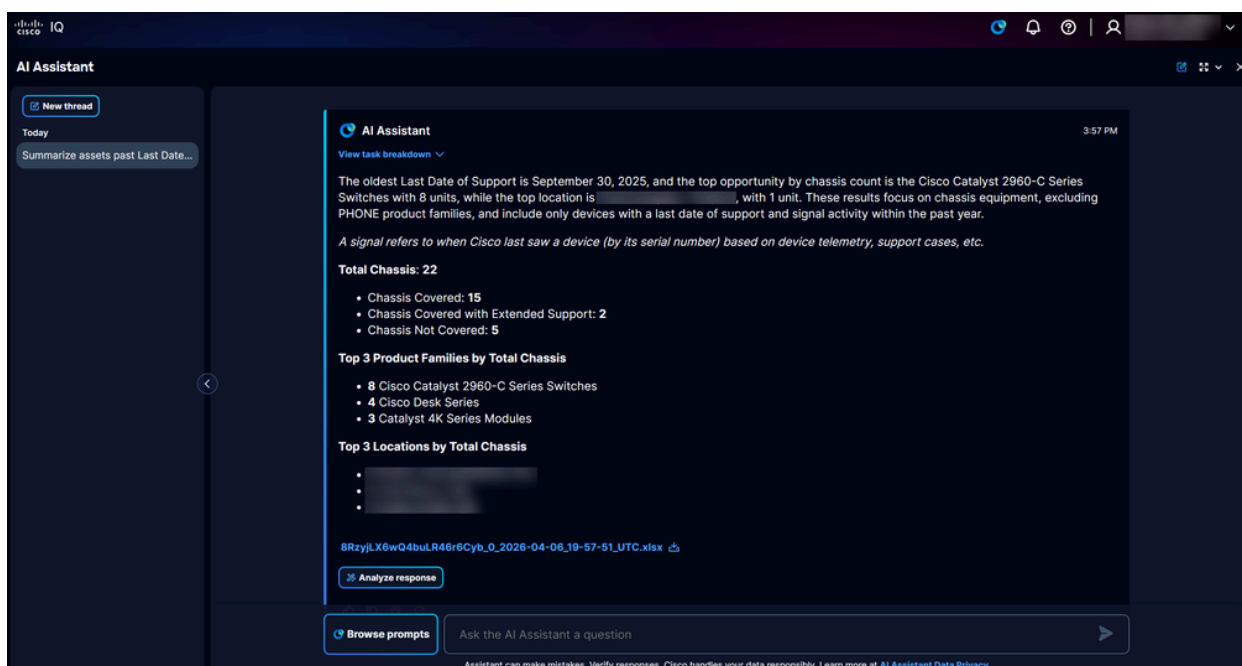
- 문제 해결: 오류 syslog 메시지 또는 컨피그레이션 질문에 대한 지원을 요청하는 메시지
- 평가 - 보안 권고: 전반적인 네트워크 보안 상태 평가, 주요 취약성 파악, 심각도가 높은 보안 위협 또는 컨피그레이션 취약성의 영향을 받는 특정 자산 나열과 관련된 프롬프트
- 자산 중요도: 네트워크 내에서 자산의 역할과 중요도에 따라 위험 완화 활동을 위한 자산의 우선순위를 정하는 것에 관한 프롬프트
- 평가 - 구성: 컨피그레이션 평가 결과 요약, 권장 모범 사례에 대한 컨피그레이션 편차 식별, 실행 가능한 권장 사항 생성과 관련된 프롬프트
- 평가 - 보안 강화: 권장 보안 기준 구성, 장치 강화에 대한 모범 사례, Cisco 네트워크 인프라 보안을 위한 단계별 절차 확인과 관련된 프롬프트

3. 프롬프트를 클릭합니다. 응답이 생성됩니다.

AI Assistant를 위한 향상된 상황 데이터

Cisco IQ AI Assistant는 컨텍스트가 동적임을 보장하여 애플리케이션, 페이지 및 세션 간에 원활한 상호 작용을 지원합니다. 이를 통해 모든 응답에서 상황 데이터를 활용하여 질문에 맞는 관련성이 높은 응답을 제공할 수 있습니다.

LDOS 요약 및 우선 순위 지정



LDOS 요약 및 우선순위 지정 기능을 사용하면 네트워크 자산과 관련된 위협을 신속하게 식별하고 해결할 수 있습니다. 이 기능은 예상 네트워크 역할 및 보안 취약성 상태에 따라 자산을 분류하여 취약성 교정을 지원하고 전반적인 서비스 품질을 향상시킵니다.

주요 이점

LDOS 요약 및 우선순위 지정 기능의 주요 이점은 다음과 같습니다.

- 우선순위가 지정된 위협 보기
- 운영 영향 분석
- 실행 가능한 통찰력

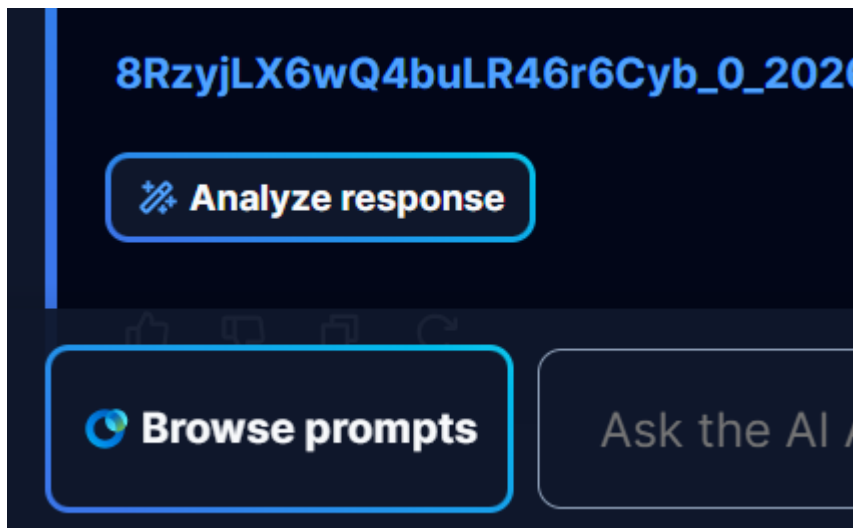
이 기능의 일환으로, 사용자 인터페이스에서 또는 LDOS 통찰력을 볼 때 사전 초기 설정된 제한된 질문 집합("*"로 표시됨)을 볼 수 있습니다.

보고서

LDOS 보고서 생성

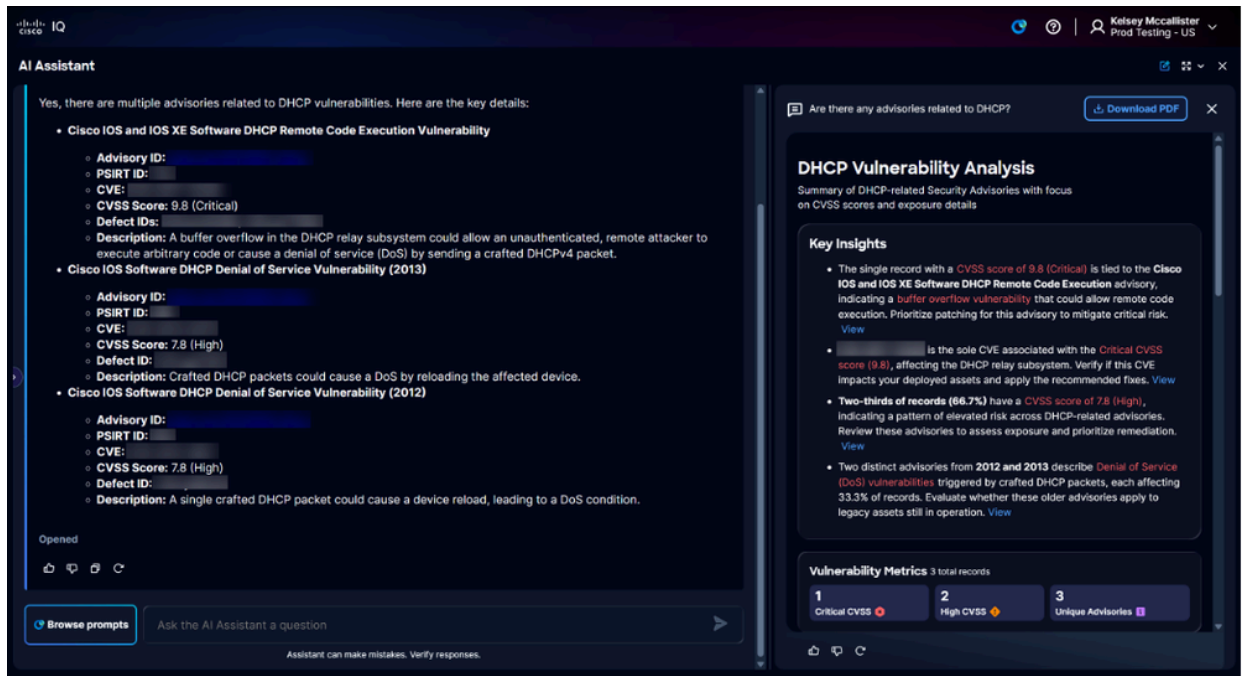
AI가 생성하고 큐레이션된 LDOS 보고서는 LDOS에 접근하거나 지난 자산에 대한 요약을 제공합니다. 또한 네트워크의 위협 환경을 신속하게 파악하는 데 도움이 되는 보안 권고 사항 및 취약성을 파악할 수 있을 뿐만 아니라, 새로 고침 옵션도 중점적으로 살펴봅니다.

응답 분석



응답 분석

응답 분석을 클릭하면 데이터가 요약된 AI 기반 요약이 수신되고 그래프, 대시보드, 차트 등 다양한 시각화가 생성돼 통찰력 있는 정보를 제공한다.



AI 요약

AI 기반 요약에는 보고서를 PDF로 다운로드할 수 있는 Download PDF(PDF 다운로드) 버튼이 포함되어 있습니다.

LDOS 요약 및 보고서 생성을 위한 데이터 소스

LDOS 요약 및 우선순위 지정 기능에서는 다음 주요 데이터 소스를 활용합니다.

- Install Base 자산 및 계약
- 텔레메트리 자산 및 계약
- CX 신호 데이터
- 하드웨어 및 소프트웨어 자산에 대한 EOL 이정표

Cisco IQ AI Assistant로 문제 해결

Cisco IQ는 Cisco IQ AI Assistant를 사용하여 장비 문제를 독립적으로 해결할 수 있도록 지원합니다. Cisco의 인증된 문제 해결 도구 및 입증된 지식 베이스를 기반으로 하는 이 직관적인 대화형 도

우미는 상황별 실시간 권장 사항을 제공합니다.

일상적인 문제 해결 시나리오에 맞게 설계되었으며 네트워크 엔지니어가 Cisco 제품 문제를 조사하고 증상을 검토하고 실행 가능한 다음 단계를 파악할 수 있도록 지원합니다. 오류 메시지, syslog, 소프트웨어 결함, 릴리스 지침, 구성 관련 질문 등의 기술적 세부 사항을 해석합니다. 문제를 즉시 해결함으로써 지원 케이스를 열지 않고도 문제를 해결하여 최적의 성능을 유지하고 시간을 절약할 수 있습니다.

모범 사례

트러블슈팅을 위해 Cisco IQ AI Assistant를 사용하는 경우 다음 모범 사례를 사용하십시오.

- 가능한 한 구체적이어야 합니다. 첫 번째 메시지에 플랫폼, 제품군 및 소프트웨어 버전 포함



참고: Asset에서 Cisco IQ AI Assistant를 시작할 때 이미 이 정보가 있습니다.

- 패러프레이징하는 대신 정확한 오류, 경보 또는 syslog 텍스트를 붙여넣습니다.
- 업그레이드, 컨피그레이션 업데이트 또는 토폴로지 변경과 같이 문제가 시작되기 전에 변경된 사항을 설명합니다.
- 문제가 장치 1대, 사이트 1대 또는 여러 사용자에게 영향을 미치는지 등 그 영향을 명확하게 공유


케이스

Cases Management(케이스 관리) 기능을 사용하면 셀프 서비스를 통해 지원 케이스를 관리할 수 있으므로 비즈니스 애플리케이션 및 서비스가 신속하게 복원됩니다. 이 기능을 사용하면 케이스를 효율적으로 관리하고 지원 환경을 간소화할 수 있습니다. 케이스 [관리](#)에 대한 자세한 내용은 지원 애플리케이션을 참조하십시오.

Cases Management를 사용하면 지원 케이스를 한 곳에서 신속하게 확인하고 추적할 수 있습니다. 또한 케이스 상태 확인, 업데이트 검토, 진행 상황 준수, 다음 단계에 대한 정보 전달을 지원하므로 더 간편하게 문제를 관리하고 더 신속하게 지원을 받을 수 있습니다.

부록 A: Cisco IQ AI Assistant 프롬프트

이 부록에서는 Cisco IQ AI Assistant에서 사용할 수 있는 프롬프트에 대한 자세한 개요를 제공하며, 질문 테마별로 글머리 기호 목록으로 구성됩니다.

 참고: 프롬프트 라이브러리가 사용자 입력에 따라 옵션을 좁힐 때 관련 제안을 선택하여 사용할 수 있는 가능한 프롬프트를 찾아보거나 사용자 지정 프롬프트를 제출할 수 있습니다. Cisco IQ AI Assistant는 자연어 입력을 기반으로 하며 드롭다운 메뉴와 같은 입력 양식을 포함하지 않으므로 원활한 사용자 환경이 보장됩니다.

Assets(일반) 탭 아래에서 다음 프롬프트를 사용할 수 있습니다.

- LDOS(Last Date of Support) 이후의 자산을 요약합니다.
- 향후 12개월 내에 LDOS(Last Date of Support)에 도달한 자산을 요약합니다.
- 모든 LDOS(Last Date of Support) 자산에 대한 PPT 요약 보고서를 생성합니다.
- 향후 12개월 동안 LDOS에 도달할 하위 구성 요소는 몇 개입니까?
- 상위 5개 소프트웨어 유형에는 몇 개의 다른 소프트웨어 버전이 있습니까?
- LDOS(Last Date of Support)가 지났거나 서비스가 지원되는 자산은 몇 개입니까?
- LDOS를 지나 보안 권고의 영향을 받는 디바이스가 가장 많은 상위 5개 제품군을 요약합니다.
- LDOS를 지나 보안 권고의 영향을 받는 카드 및 모듈을 요약합니다.
- 몇 개의 하위 구성 요소가 상위 새시보다 EoL 중요 시점을 앞당기고 있습니까?

Cases(케이스) 탭에서 다음 프롬프트를 사용할 수 있습니다.

- 열려 있는 내 케이스 표시
- 케이스 요약
- RMA 상태 표시
- 버그 상태 표시
- 사건에 대한 최신 정보를 알려 주세요
- 케이스에 대한 최신 업데이트 및 보류 중인 작업 항목 제공
- 열려 있는 케이스 닫기
- 케이스의 연락처 목록에 참가자 추가
- 케이스에 대한 Webex 스페이스 통신 만들기
- 케이스를 처리하는 엔지니어와 연결
- 미결 케이스의 심각도 수준 올리기
- 미결 케이스 에스컬레이션
- 새 엔지니어에게 케이스 요청
- 열려 있는 케이스 다시 대기열 지정
- 케이스에 메모 추가

Troubleshooting(문제 해결) 탭에서 다음 프롬프트를 사용할 수 있습니다.

- Syslog 오류 [Error](오류)를 해결하고 근본 원인을 파악하려면 어떻게 해야 합니까?
- 구성 문제를 해결하고 [ABCD]의 근본 원인을 파악하려면 어떻게 해야 합니까?
- 제품 ID [ABCD]에 [XYZ]을(를) 구성하려면 어떻게 합니까?

Assessments - Security Advisories 탭 아래에서 다음 프롬프트를 사용할 수 있습니다.

- DHCP와 관련된 권고 사항이 있습니까?
- Salt Typhoon과 관련된 webUI 권한 에스컬레이션 취약점을 확인할 수 있는 보안 권고 사항이 있습니까?
- HTTP를 활성화하기 전에 HTTP 활성화와 관련된 알려진 보안 권고 또는 취약성을 확인할 수 있습니까?
- 내 네트워크에서 취약한 보안 자문 수는 몇 개입니까?
- 보안 권고에 취약한 디바이스는 몇 개입니까?

Asset Criticality 탭 아래에서 다음 프롬프트를 사용할 수 있습니다.

- 역할과 중요도에 따라 가장 중요한 자산은 무엇입니까?
- 보안 권고의 영향을 받는 핵심 장치는 몇 대입니까?
- 커버리지가 향후 12개월 내에 만료될 예정인 중요도가 높은 핵심 장비 요약
- 역할과 중요도에 따라 LDOS 자산의 우선 순위를 새로 고칩니다.
- 역할과 중요도에 따라 갱신할 지원 대상이 아닌 자산 또는 곧 지원 대상이 될 자산의 우선 순위를 지정합니다.
- 지원 대상 자산의 역할과 중요도에 따라 갱신 시 만료 예정인 계약의 우선 순위를 지정합니다.
- 심각도, 역할, 영향을 받는 자산의 중요도를 기준으로 PSIRT 취약성의 우선 순위를 지정합니다.

Assessments(평가) - Configuration(컨피그레이션) 탭에서 다음 프롬프트를 사용할 수 있습니다.

- 최근 구성 평가에 대한 요약을 제공할 수 있습니까?
- 평가된 구성 모범 사례 규칙은 몇 개이며, 최소 한 개의 자산이 통과하지 못한 결과는 몇 개입니까?
- 네트워크 전체에서 가장 일반적인 컨피그레이션 편차는 무엇입니까?
- 어떤 Cisco 제품군이 컨피그레이션 모범 사례와 가장 많이 다르습니까?
- 평가된 자산은 몇 개이며, 몇 퍼센트가 지나지 않았습니까?
- 컨피그레이션 모범 사례와 가장 많이 차이가 나는 범주는 무엇입니까?
- 네트워크에 가장 큰 위협을 초래하는 구성 편차는 무엇이며, 어떤 시정 조치가 권장됩니까?
- 심각도가 높은 최대 구성 편차가 있는 자산은 무엇입니까? 권장되는 시정 조치는 무엇입니까?
- 자산 중요도를 기준으로 심각도가 높은 심각도 구성 편차 분석 표시
- 심각도, 카테고리, 소프트웨어 유형별 컨피그레이션 모범 사례 규칙 편차 분석 표시

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?

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.