Cisco IQ Link Operations Guide v1.2.0

소개

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

Cisco IQ Link는 온프레미스 네트워크에서 자산 텔레메트리를 안전하게 수집하고 Cisco IQ로 전송하여 AI가 제공하는 예측 통찰력을 바탕으로 네트워크 가시성을 높이고 문제를 예측하며 운영 효율성을 높일 수 있습니다.

로컬 인증

계정 관리자는 다음 자격 증명을 사용하여 Cisco IQ Link에 로그인해야 합니다.

- 기본 사용자 이름: admin
- 기본 비밀번호: Cisco IQ Link 설치 프로세스 중에 설정된 비밀번호 자세한 내용은 Cisco IQ Link 시작 가이드를 참조하십시오
- 기본 계정 컨텍스트: 기본 고객

로그인 시 기본 사용자 "admin"과 계정 이름 "Default-Customer"가 홈 페이지에 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).

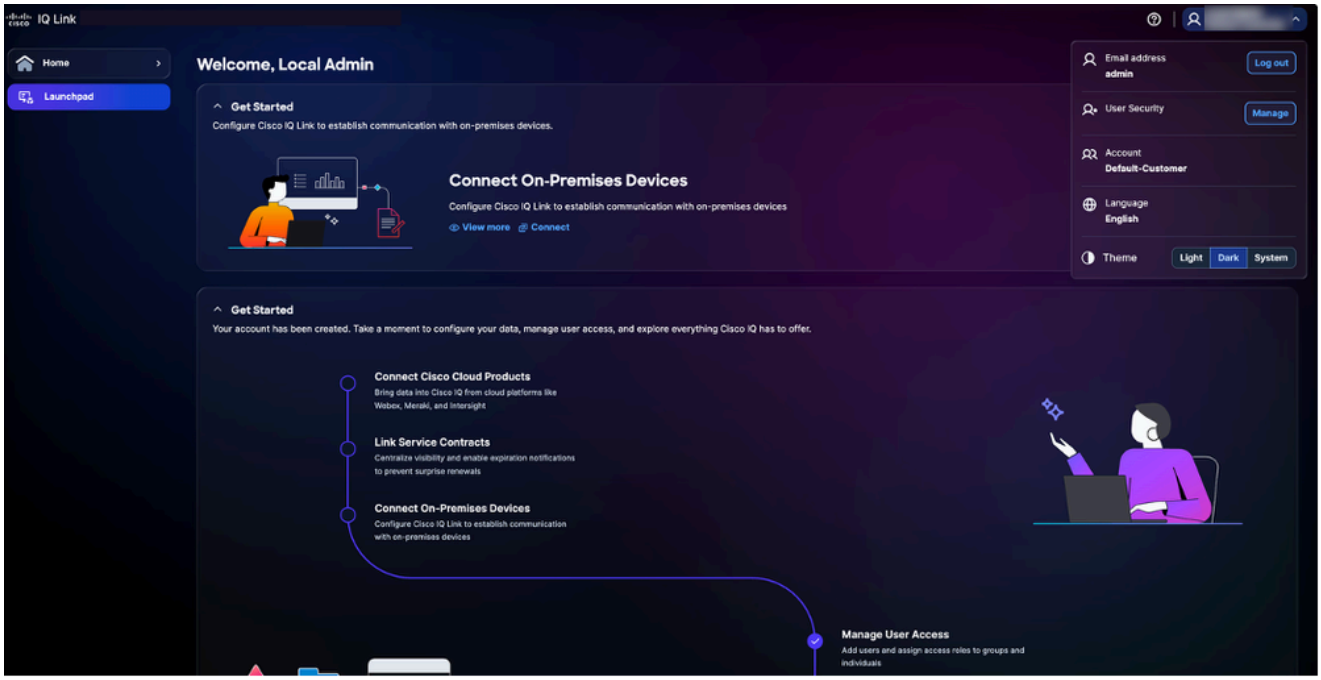
참고: 15분 내에 3회 시도하여 올바른 비밀번호를 입력하려고 합니다. 세 번의 시도가 모두 실패하면 보안을 위해 계정이 30분 동안 일시적으로 잠깁니다.
잠금 기간 중에는 로그인을 시도할 수 없습니다. 다음과 같은 메시지가 표시됩니다. "실패한 시도가 너무 많아 계정이 잠겼습니다. 잠금이 만료되는 시간을 포함하여 "나중에 다시 시도하십시오."
30분 후에 계정이 자동으로 잠금 해제되며, 이 때 로그인 또는 비밀번호 재설정을 시도할 수 있습니다.

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.

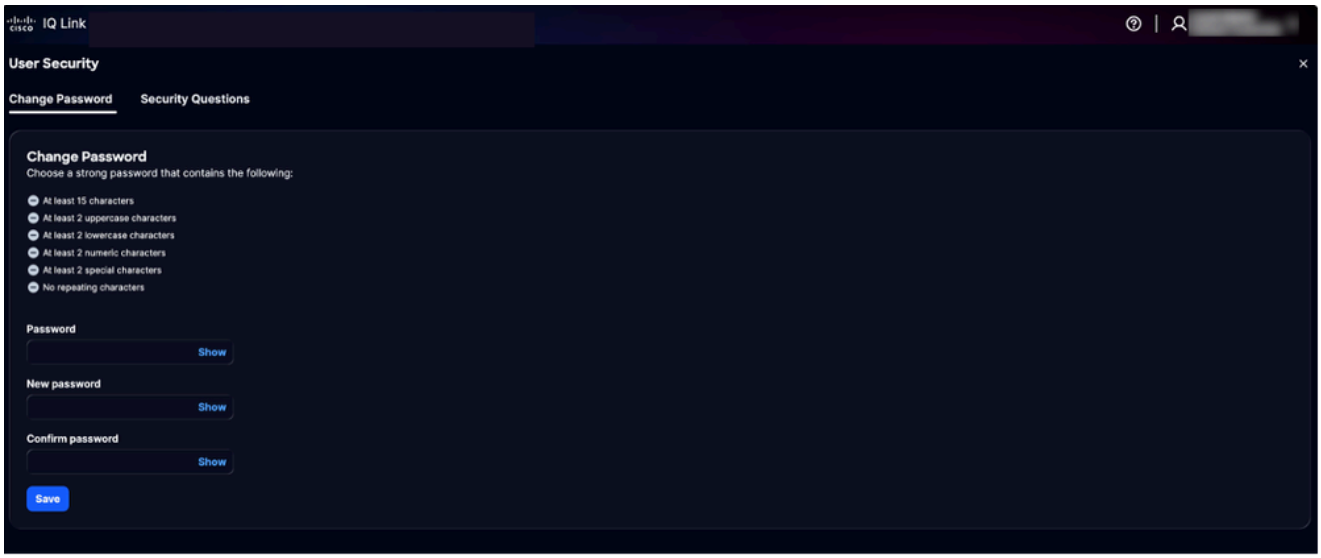
보안 질문을 설정하려면

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



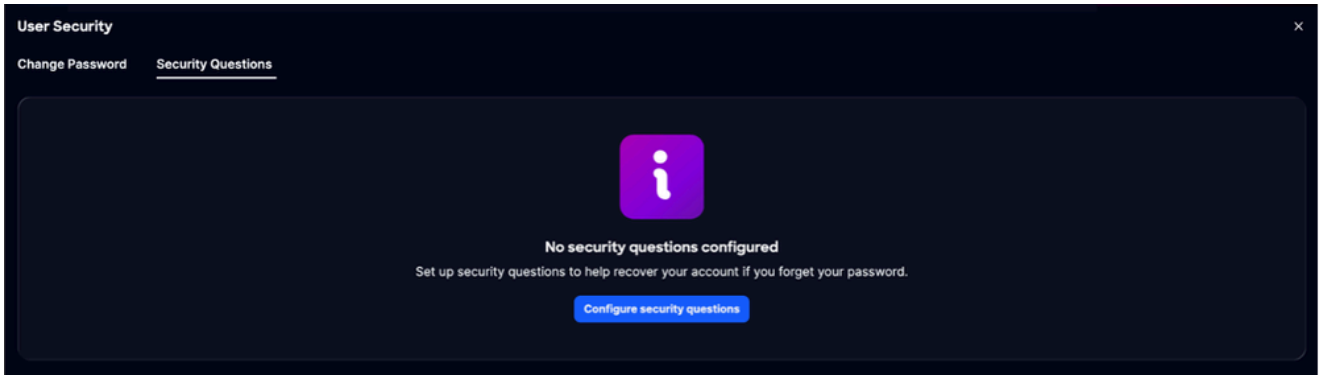
사용자 프로필 메뉴

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



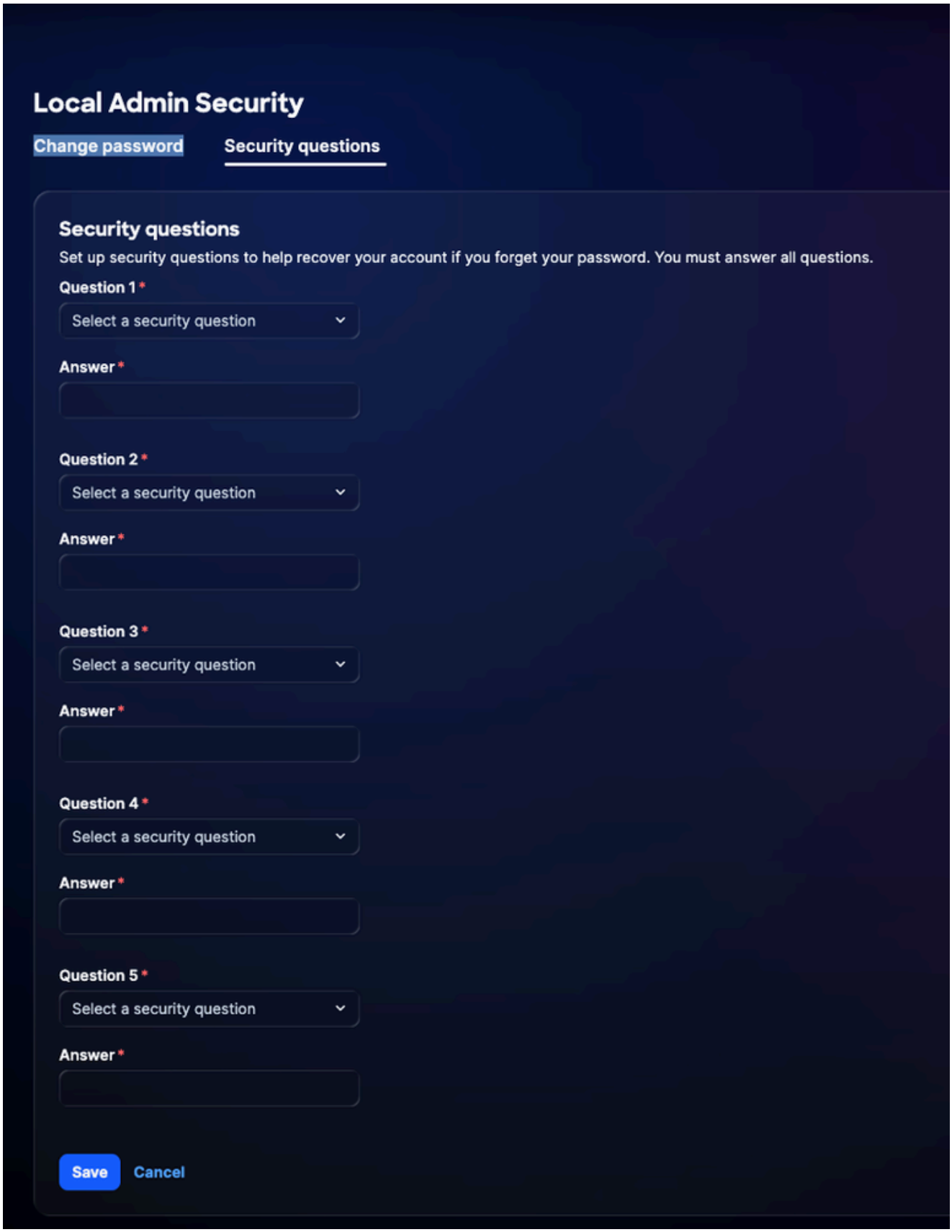
암호 변경

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



보안 질문

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



보안 질문

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. 예를 들어 " Smith" 및 "smith"는 동일한 것으로 간주됩니다.

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 이상이 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 비활성화됩니다.)

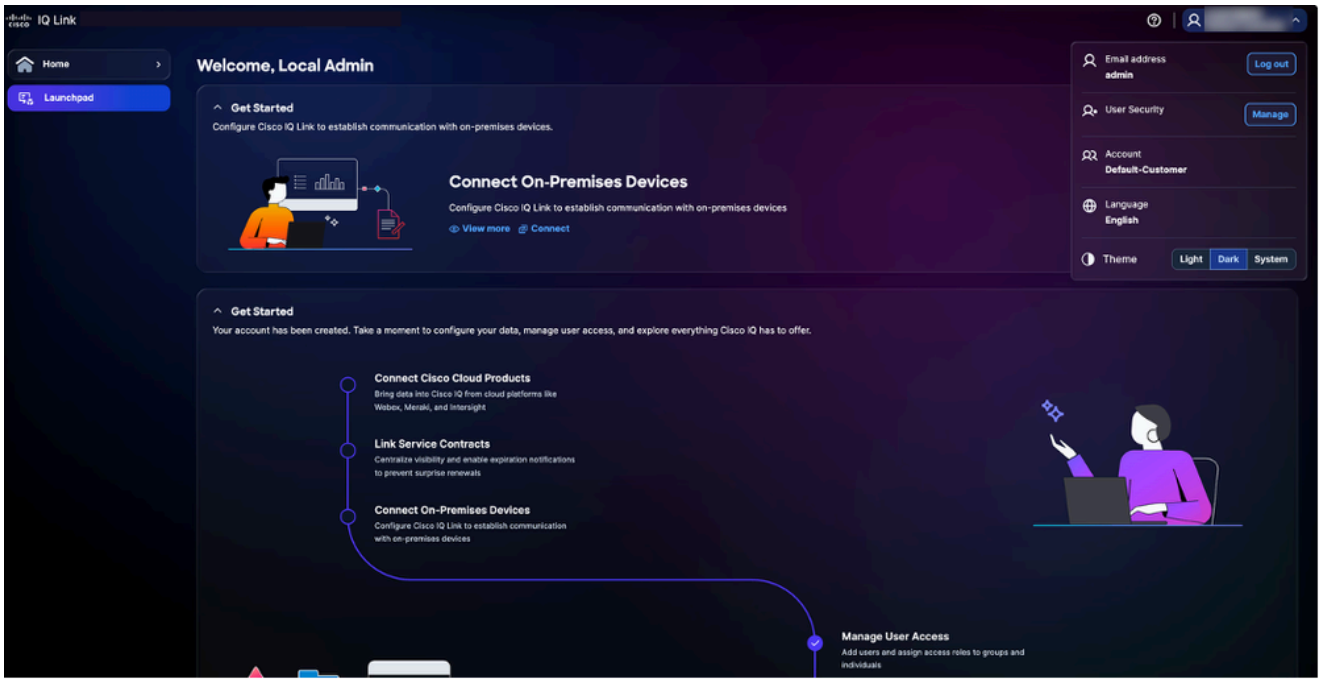
사전 요구 사항

비밀번호를 관리하려면 다음 조건을 충족해야 합니다.

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

비밀번호를 변경하려면

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



사용자 프로필 메뉴

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.

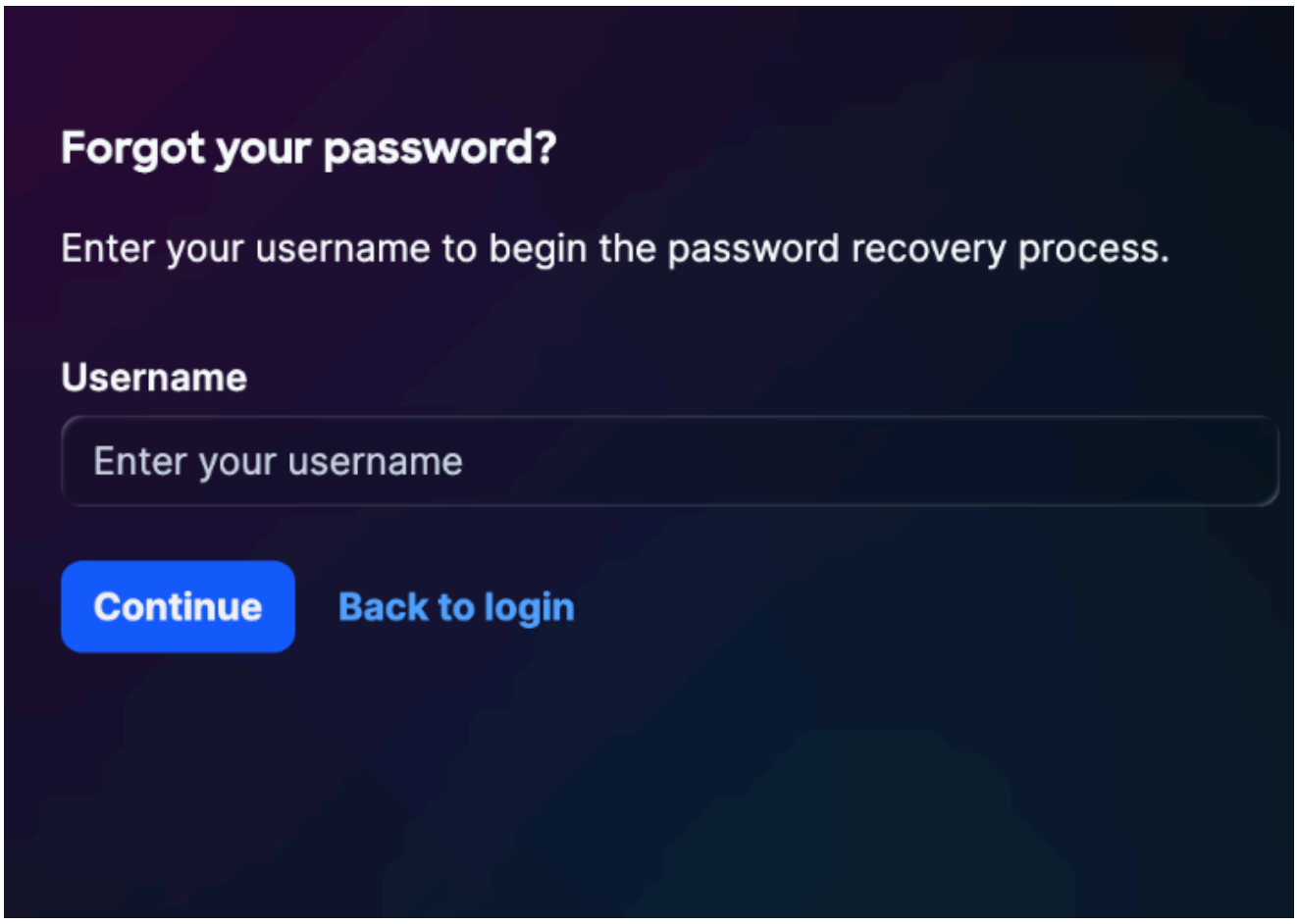
비밀번호는 Cisco IQ VM(Virtual Machine)을 비롯한 Cisco IQ 시스템에서 업데이트됩니다.

잊어버린 비밀번호 재설정

이전에 보안 질문을 설정한 경우 보안 질문 확인 프로세스를 사용하여 잊어버린 비밀번호를 재설정할 수 있습니다. 자세한 내용은 보안 Q&A 설정을 참조하십시오.

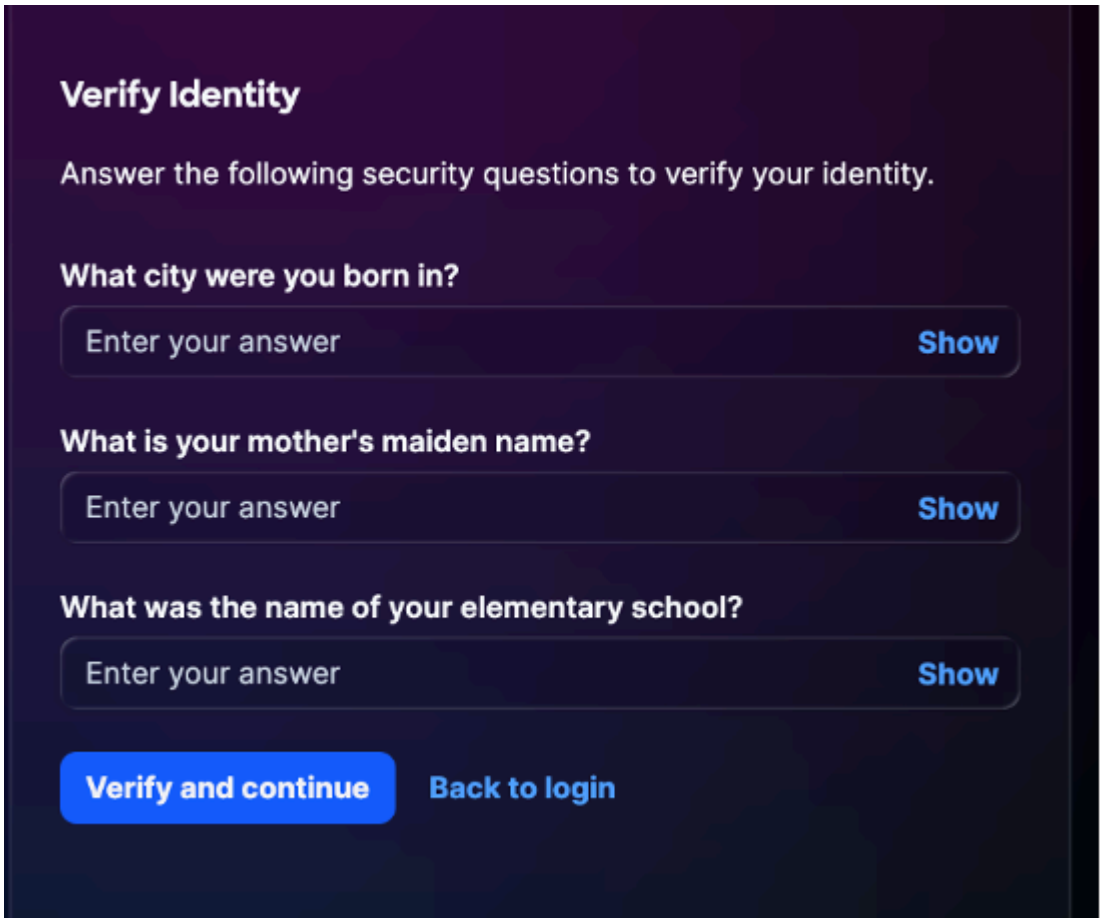
잊어버린 비밀번호를 재설정하려면

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



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.



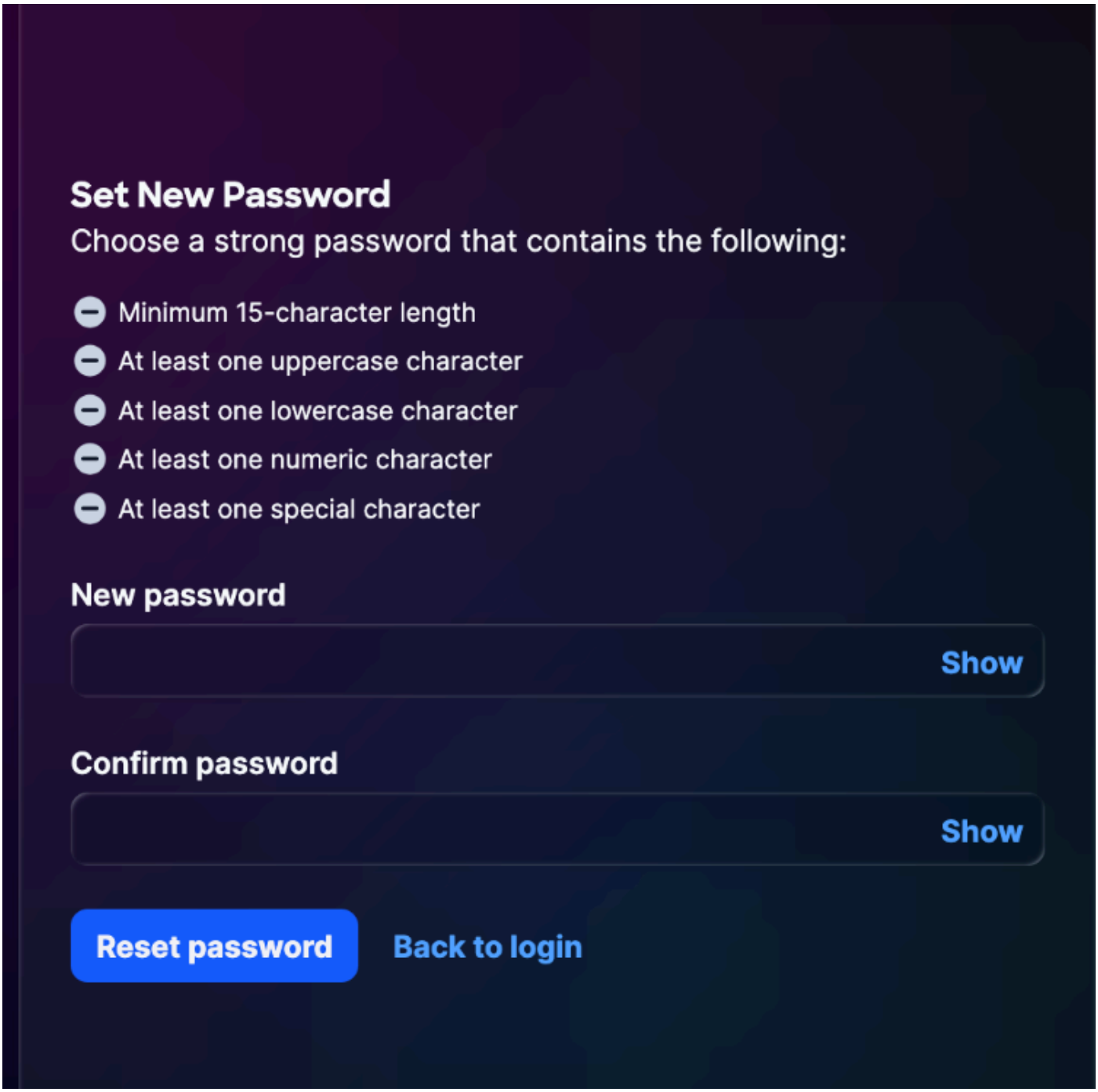
ID 확인

✎ 참고: 위에 표시된 보안 질문은 사용자별로 다르며 그에 따라 달라집니다.

---

5. 표시된 세 가지 질문 모두에 대한 응답을 입력합니다.

6. 확인과 계속을 클릭합니다. 전송된 응답이 이전에 저장된 응답과 일치하면 새 비밀번호를 입력하라는 메시지가 표시됩니다.



비밀번호 재설정

15분 이내에 보안 질문에 올바르게 대답하려는 시도가 3회 있습니다. 세 번의 시도가 모두 실패하면 보안을 위해 계정이 30분 동안 일시적으로 잠깁니다. 잠금 기간 중에는 비밀번호를 재설정할 수 없습니다.
다음과 같은 메시지가 표시됩니다. "확인 시도가 너무 많이 실패하여 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. 신규 비밀번호를 입력합니다.

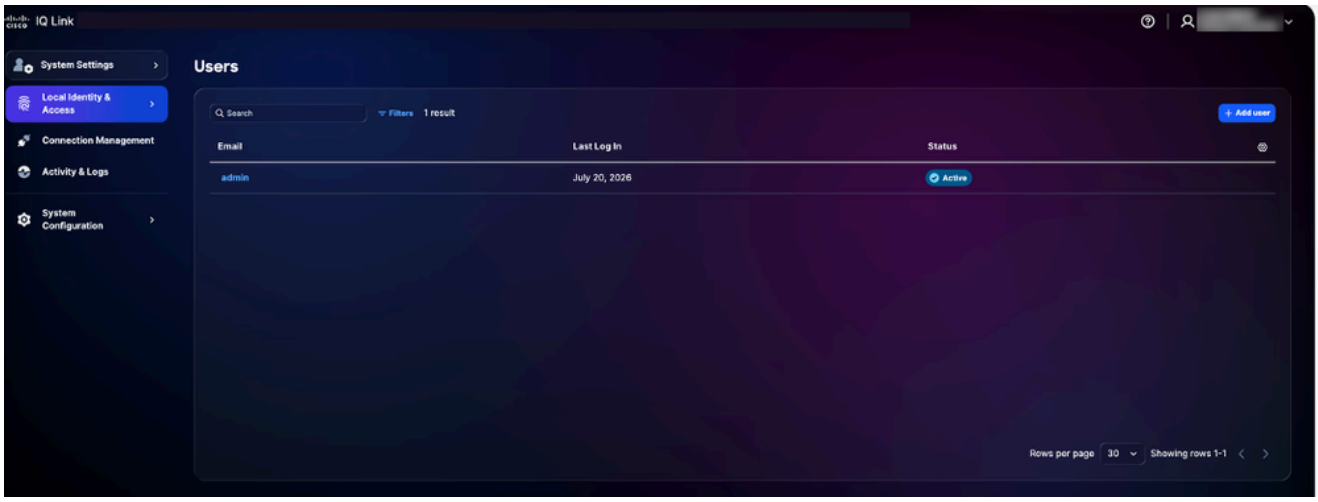
8. 비밀번호를 다시 입력하여 확인합니다.

9. 제출을 클릭합니다.

로컬 사용자 추가

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

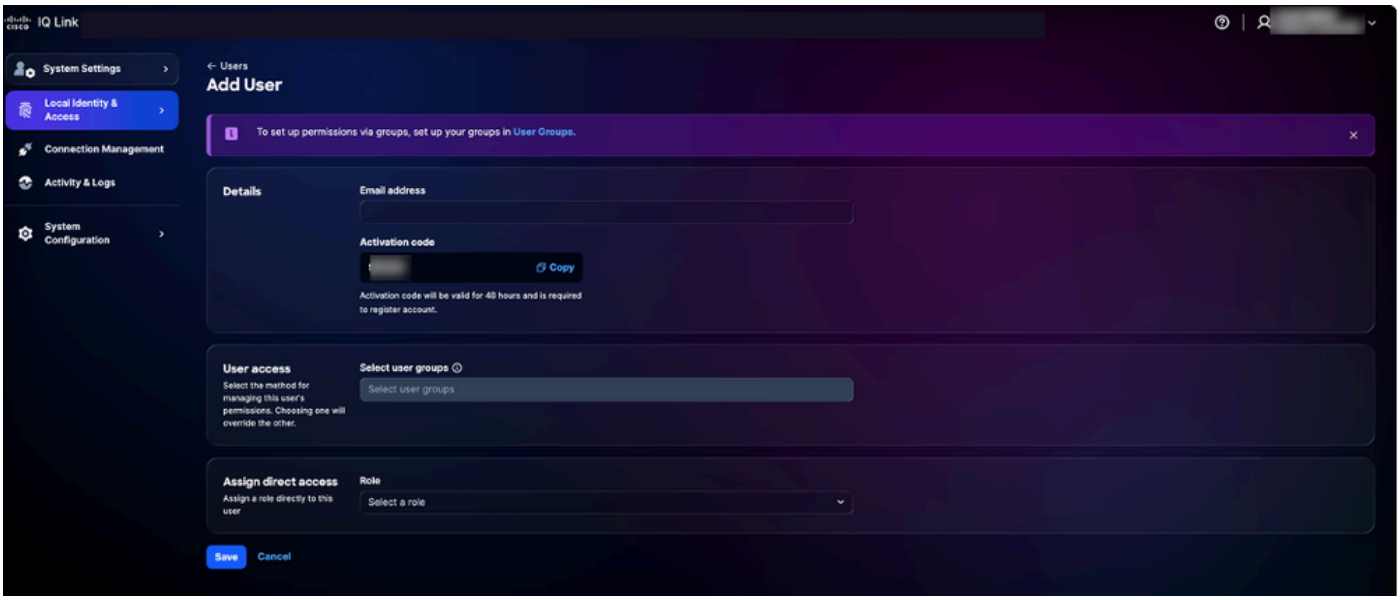
1. System Settings(시스템 설정) > Local Identity & Access(로컬 ID 및 액세스) > Users(사용자)로 이동합니다. Users(사용자) 페이지가 표시됩니다. 모든 기존 로컬 사용자를 상태와 함께 나열합니다.



사용자 페이지

참고: More Options(추가 옵션) 아이콘은 Account Administrators(어카운트 관리자)에 대해 표시되지 않습니다(위 이미지에 표시).

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



사용자 추가

3. 전자 메일 주소를 입력합니다.

4. 활성화 코드를 입력합니다.

참고: 활성화 코드는 기본적으로 표시됩니다. 등록을 완료해야 하므로 사용자와 공유합니다.

---

5. 사용자 액세스의 사용자 그룹 선택 드롭다운 목록에서 사용자 그룹을 선택합니다.

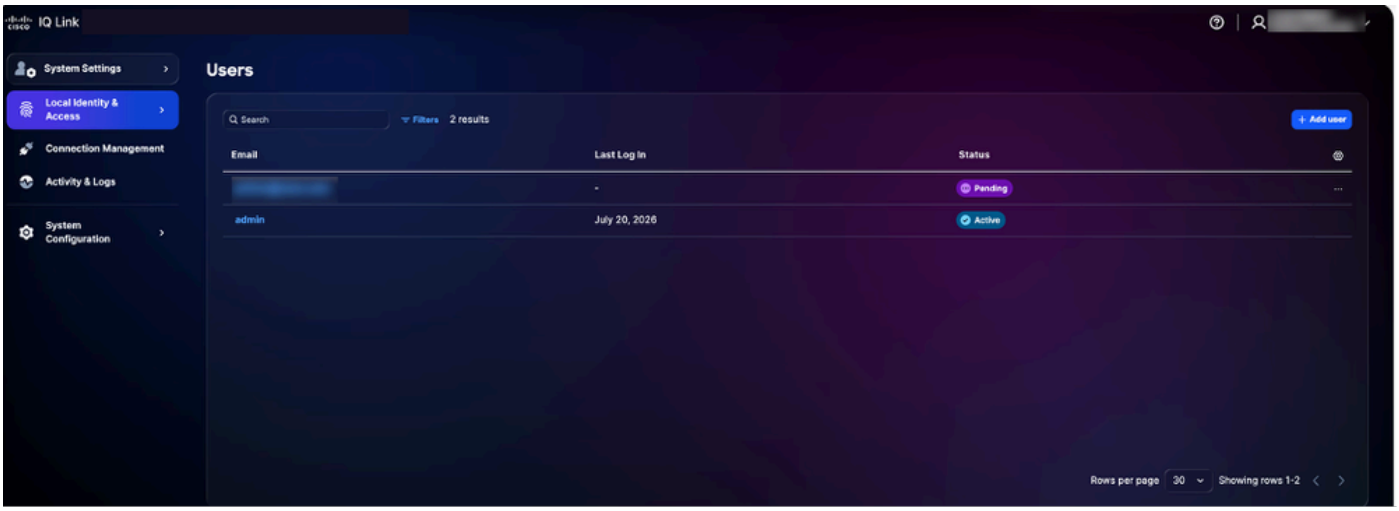
참고: 사용자는 선택한 그룹에서 액세스 권한을 상속합니다.

---

6. 직접 액세스 지정의 역할 드롭다운 목록에서 역할을 선택합니다. 다음 두 가지 역할을 사용할 수 있습니다.

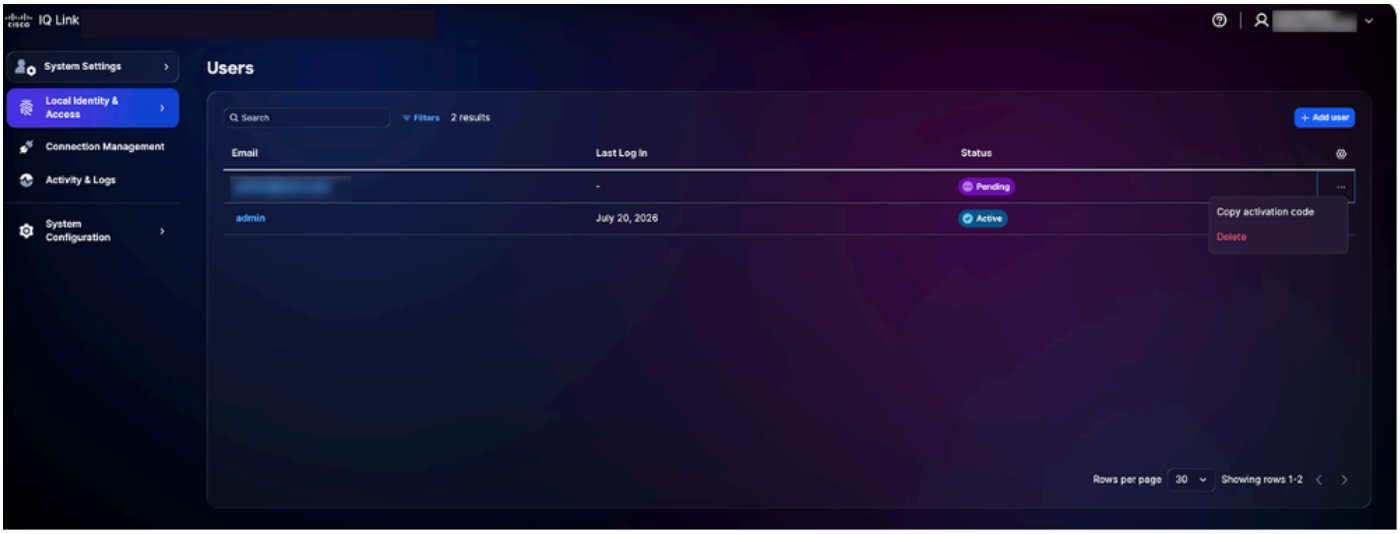
- 뷰어: 애플리케이션 보기 및 액세스
- 관리자: 애플리케이션 액세스 및 시스템 설정 관리(시스템 관리 및 IDP 제외)

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



새로 추가된 사용자

8. 목록에서 새로 생성된 사용자를 찾고 상태 열에 대기 중이 표시되는지 확인합니다.



활성화 코드 복사

9. 새로 생성된 사용자 옆에 있는 추가 옵션 아이콘 > 활성화 코드 복사를 클릭합니다. 활성화 코드가 클립보드에 복사됩니다.

10. 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

참고: 활성화 코드는 48시간 동안 유효합니다. 코드가 만료되면 계정 관리자에게 문의하여 새

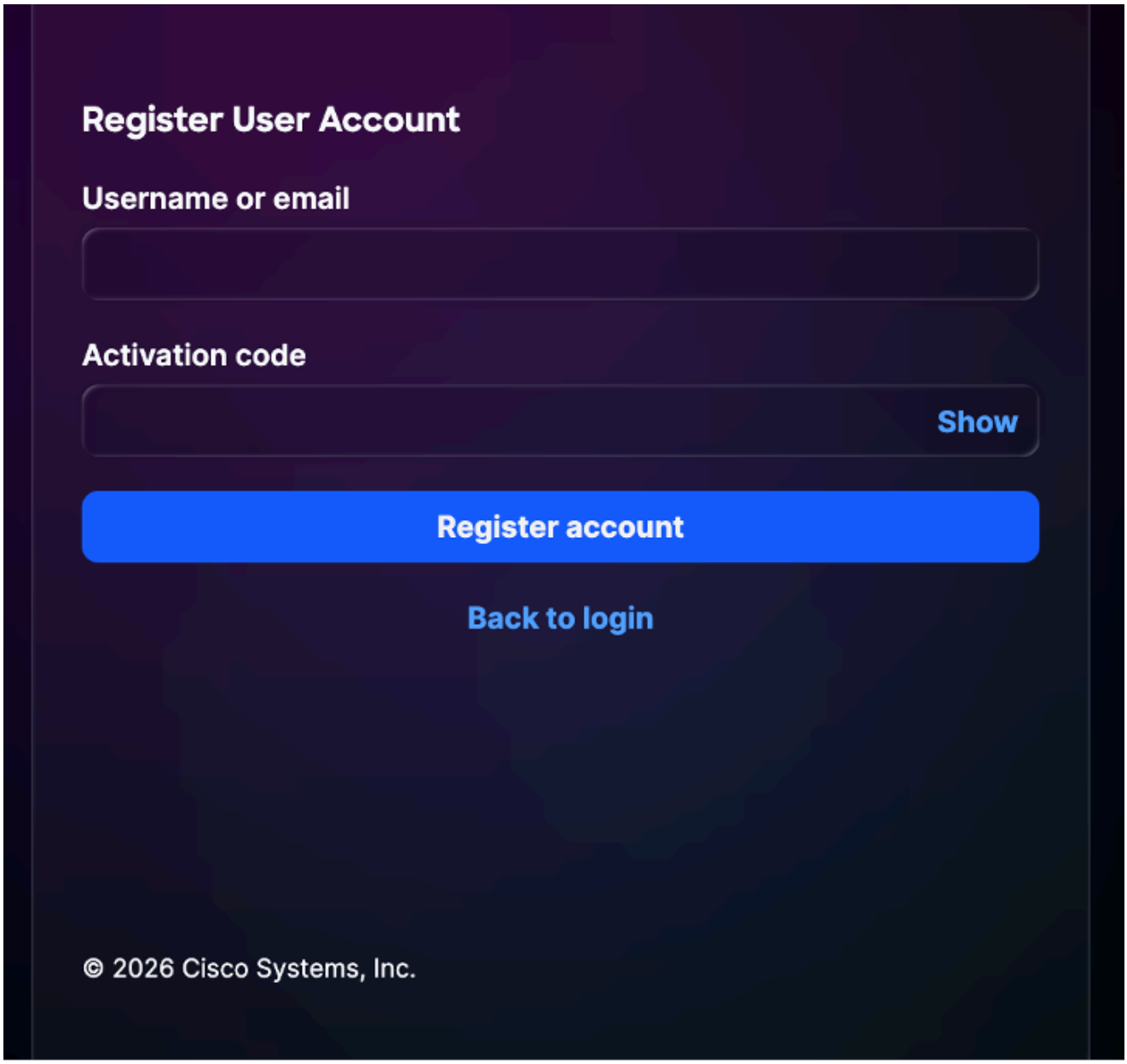
✎ 코드를 요청하십시오.

11. 로그아웃하려면 오른쪽 상단에 있는 사용자 아이콘을 클릭하고 로그아웃을 선택합니다. Cisco IQ 로그인 페이지로 돌아갑니다.

새 사용자 계정 등록

새 사용자 계정을 등록하려면

1. 로그인 페이지에서 새 사용자 계정 등록 링크를 클릭합니다.

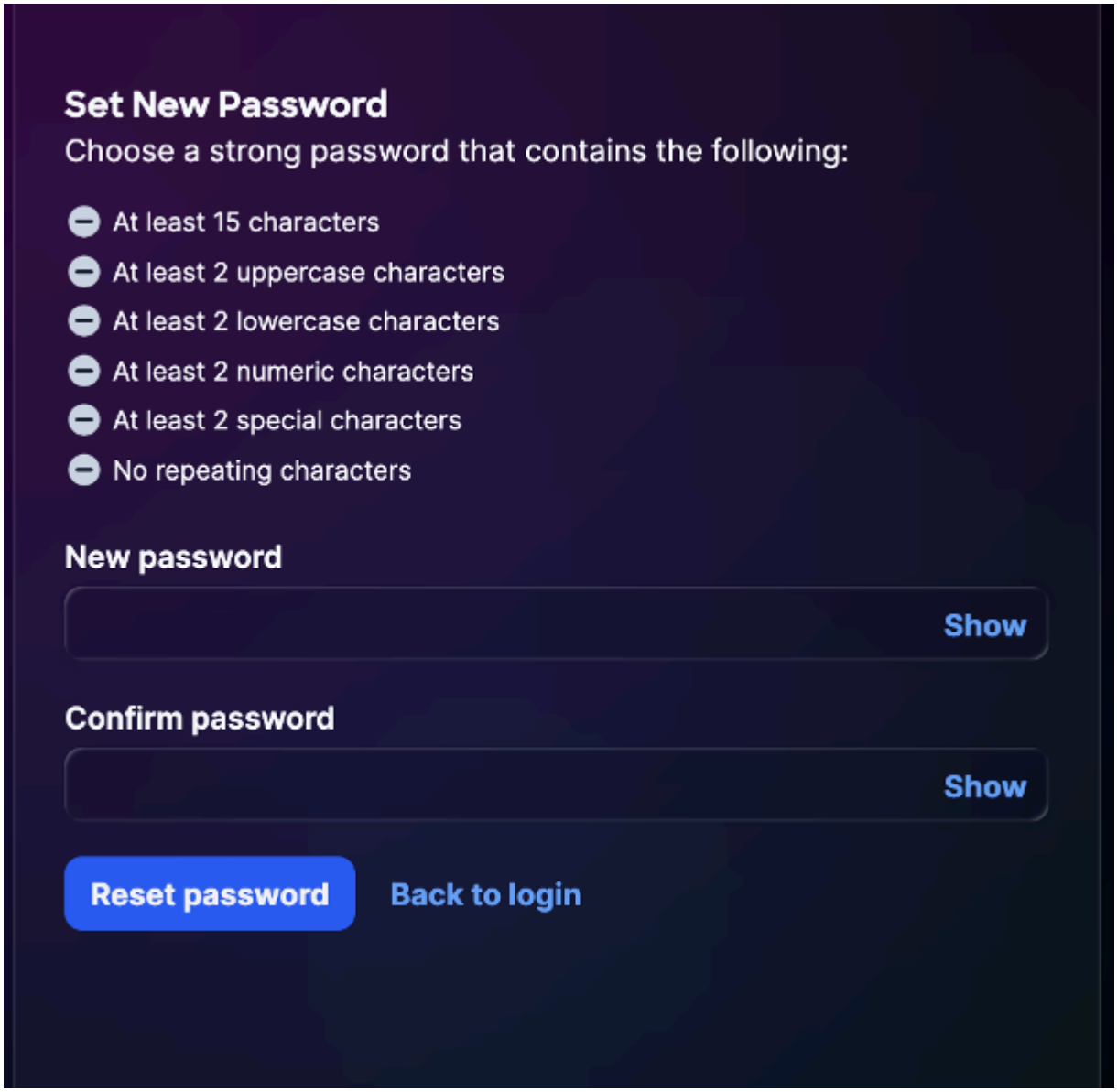


새 사용자 계정

2. 사용자를 생성할 때 사용한 사용자 이름 또는 이메일 주소를 입력합니다(예:

user1@abc.com).

3. 계정 관리자가 공유하는 활성화 코드를 입력합니다.
4. 계정 등록을 클릭합니다. 새 암호 설정 창이 표시됩니다.



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 (자세한 내용은 보안 질문 및 답변 설정 참조).

로컬 사용자 그룹 관리

User Groups(사용자 그룹)를 사용하면 계정 관리자가 여러 로컬 사용자에 대한 역할을 함께 관리할

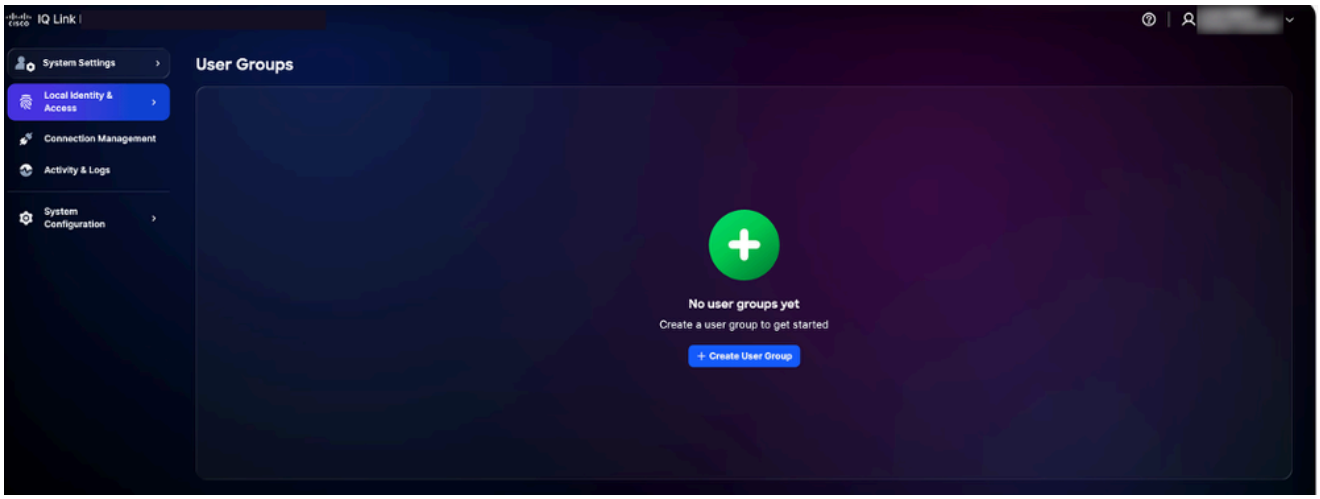
수 있습니다. 계정 관리자는 각 사용자에게 개별적으로 역할을 할당하는 대신 그룹을 만들고, 역할 및 사용자 집합을 여기에 연결하고, 역할 또는 멤버십을 한 곳에서 업데이트할 수 있습니다. 모든 사용자 그룹 관리는 Local Identity & Access(로컬 ID 및 액세스) 페이지에서 수행됩니다.

참고: 계정 관리자만 사용자 그룹을 생성, 편집 또는 삭제할 수 있습니다. 그룹은 기존 로컬 사용자로 구성됩니다. 사용자를 그룹에 추가하려면 먼저 사용자를 만들어야 합니다.

사용자 그룹 생성

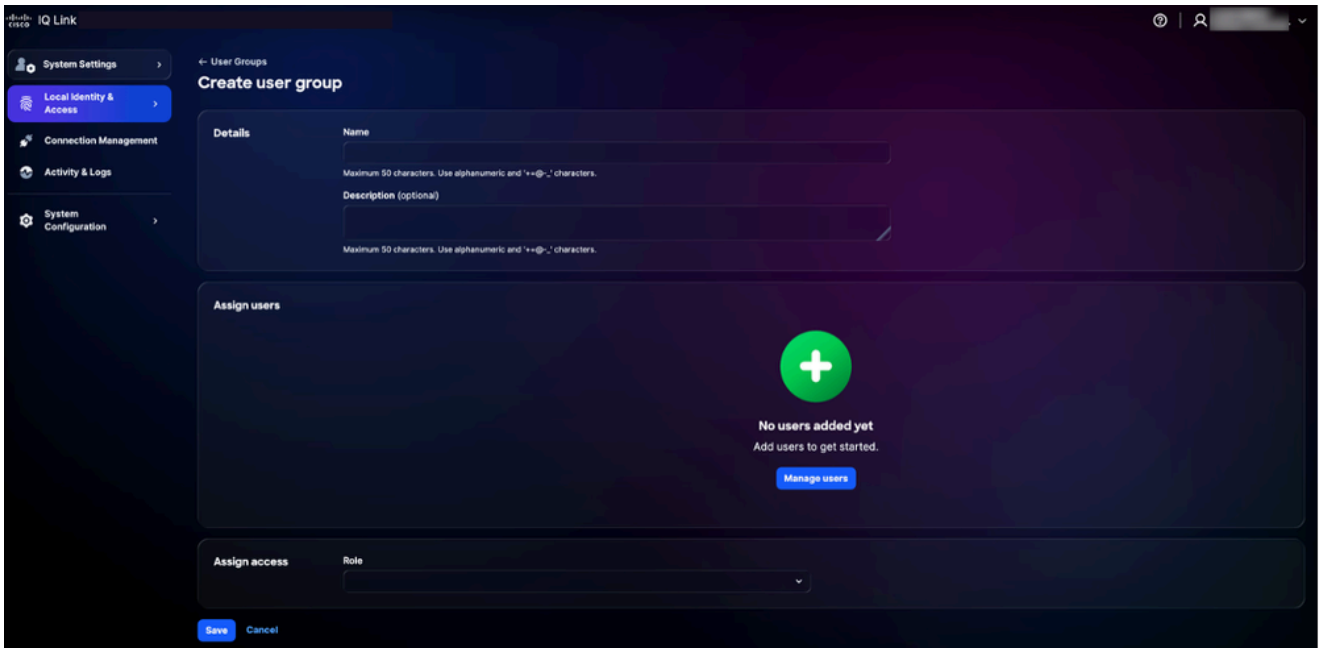
사용자 그룹을 생성하려면

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 허용됩니다.

- 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: 애플리케이션 보기 및 액세스(읽기 전용)
    - 관리자: 애플리케이션 액세스 및 시스템 설정 관리

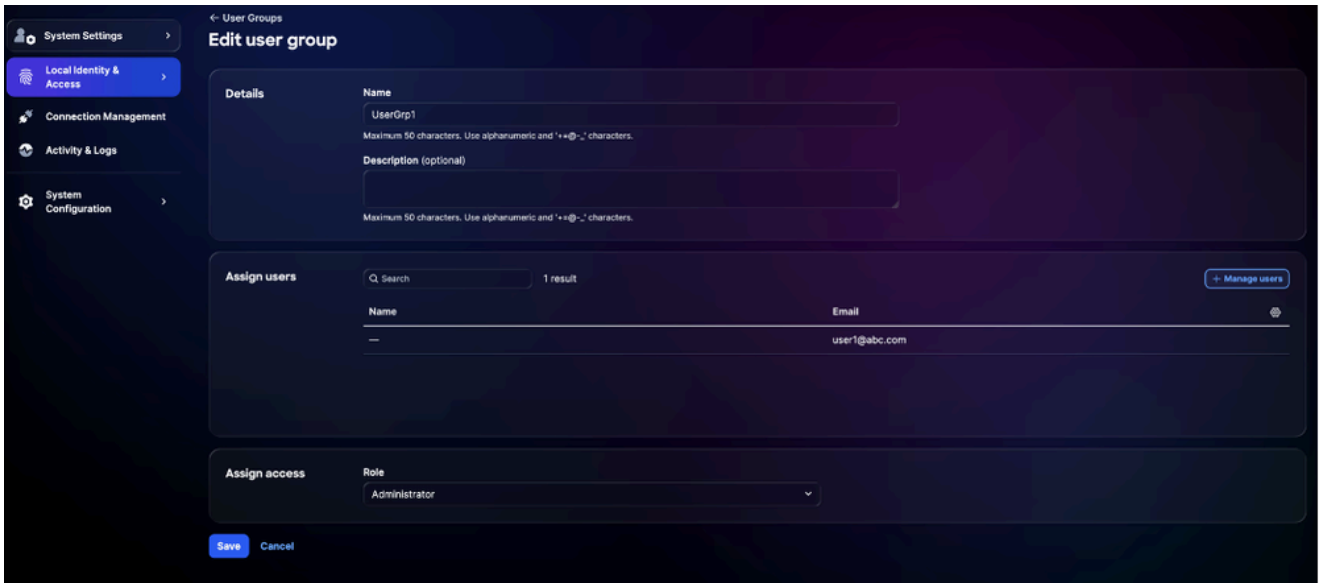
4. 저장을 클릭합니다.

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. 그룹 옆의 More(추가) 아이콘을 클릭하고 Edit(편집)를 선택합니다. 사용자 그룹 편집 페이지가 표시됩니다.



사용자 그룹 편집

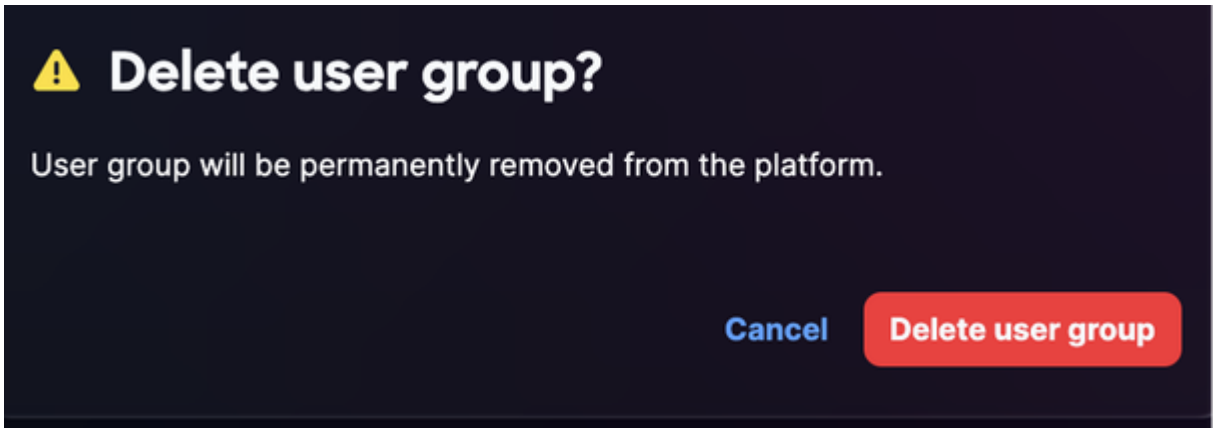
3. 원하는 대로 변경합니다.
4. 저장을 클릭합니다.

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

Cisco IQ Link에 로그인한 계정 관리자는 다양한 설정을 구성할 수 있습니다. 계정 관리자는 로컬 관리 또는 IDP(Identity Provider) 구성을 사용하여 Cisco IQ Link에 로그인할 수 있습니다.

SSO용 Okta IDP SAML 컨피그레이션

IDP SAML 구성 사전 요구 사항

- Cisco IQ 링크에 대한 로컬 계정 관리자 액세스
- IDP 포털 액세스

SSO에 대한 IDP SAML 컨피그레이션

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

1. IDP 포털로 이동합니다.

2. Cisco IQ Link 인스턴스에 대해 다음 속성을 설정합니다.
표 1: Cisco IQ 링크 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 2: SAML 컨피그레이션 매개변수

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

3. 다음 필수 속성 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: .*

4. 응용 프로그램에서 SLO(단일 로그아웃) 설정을 구성합니다.

표 3: 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 sp-public-key.crt로 저장합니다. 자세한 내용은 단일 로그아웃 컨피그레이션을 참조하십시오.
SP 메타데이터	SP 메타데이터는 AD FS 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

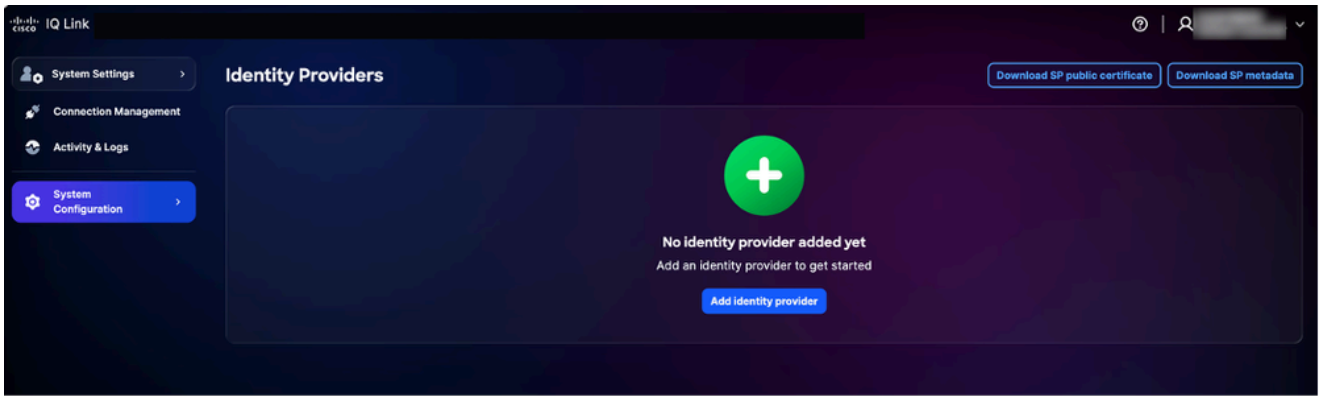
5. 다운로드 아이콘을 클릭하여 "SP 메타데이터" 파일을 다운로드합니다.

6. 제공자의 필요에 따라 신청서를 제공 또는 작성하는 행위

Okta IDP 추가

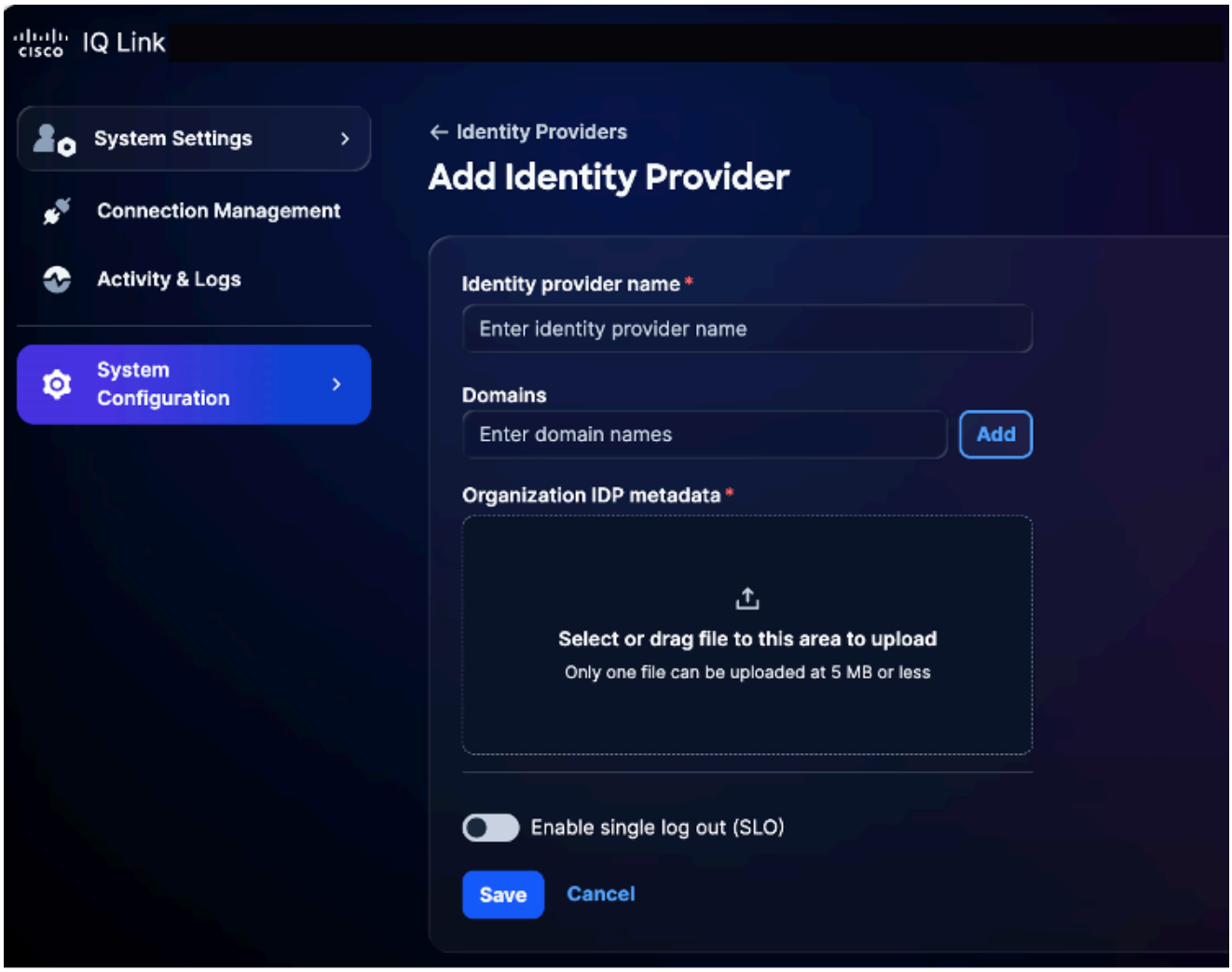
Cisco IQ Link에서 IDP를 추가하려면

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



IDP 홈 페이지

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



ID 공급자 추가

참고: 지정된 시간에 하나의 IDP만 추가할 수 있습니다.

3. ID 공급자 이름을 입력합니다.

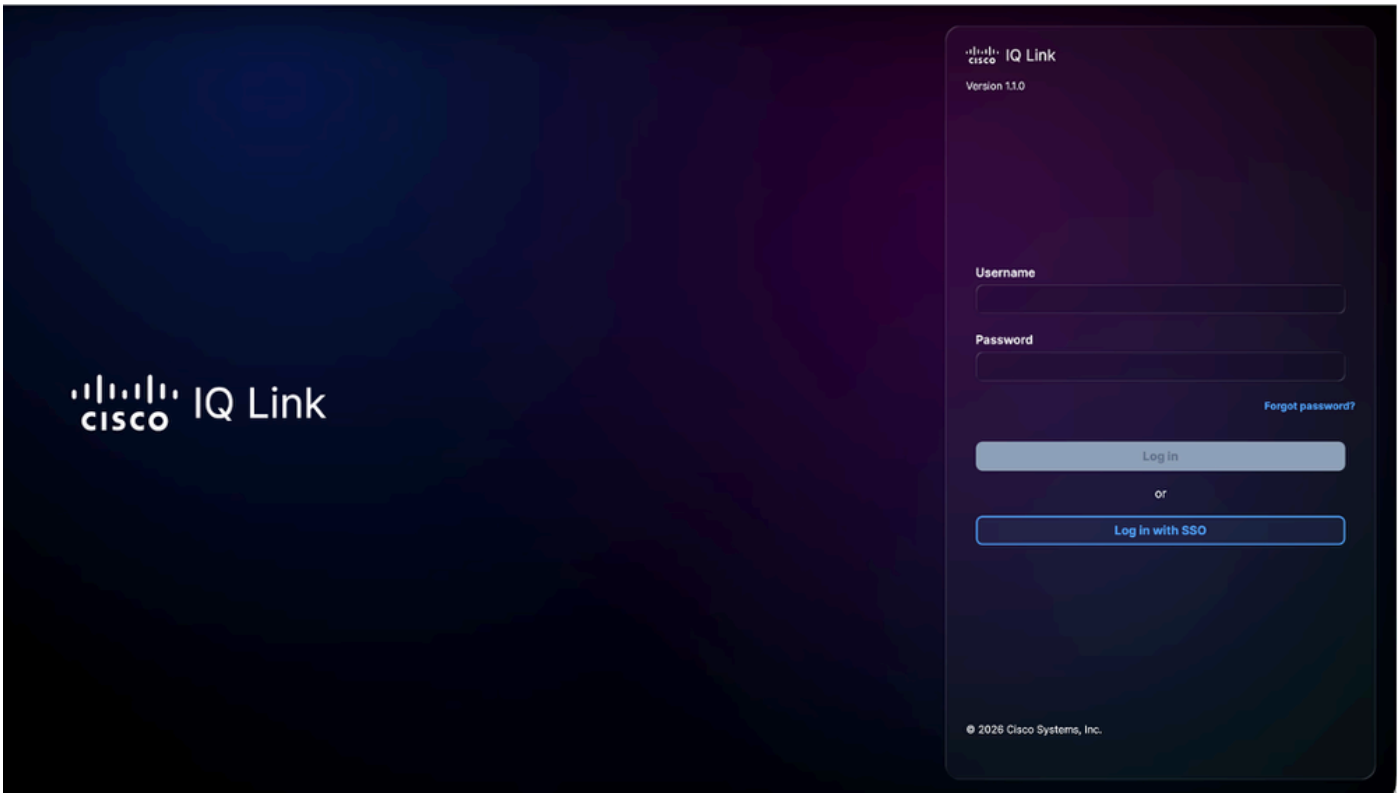
4. Cisco IQ Link에서 구성한 도메인 이름을 Domains(도메인) 필드에 추가하려면 Add(추가)를 클릭합니다.

5. IDP 애플리케이션에서 얻은 SAML 메타데이터 파일을 Organization IDP metadata(조직 IDP 메타데이터) 필드에 끌어 놓거나 업로드하는 방법 이 파일에는 인증서 세부 정보 및 서비스 공급자(SP) 엔터티 세부 정보가 포함되어 있습니다.

6. (선택 사항) Enable single logout(단일 로그아웃 활성화) 토글 버튼을 켭니다. 나중에 SLO를 활성화할 수도 있습니다.

7. 저장을 클릭합니다.

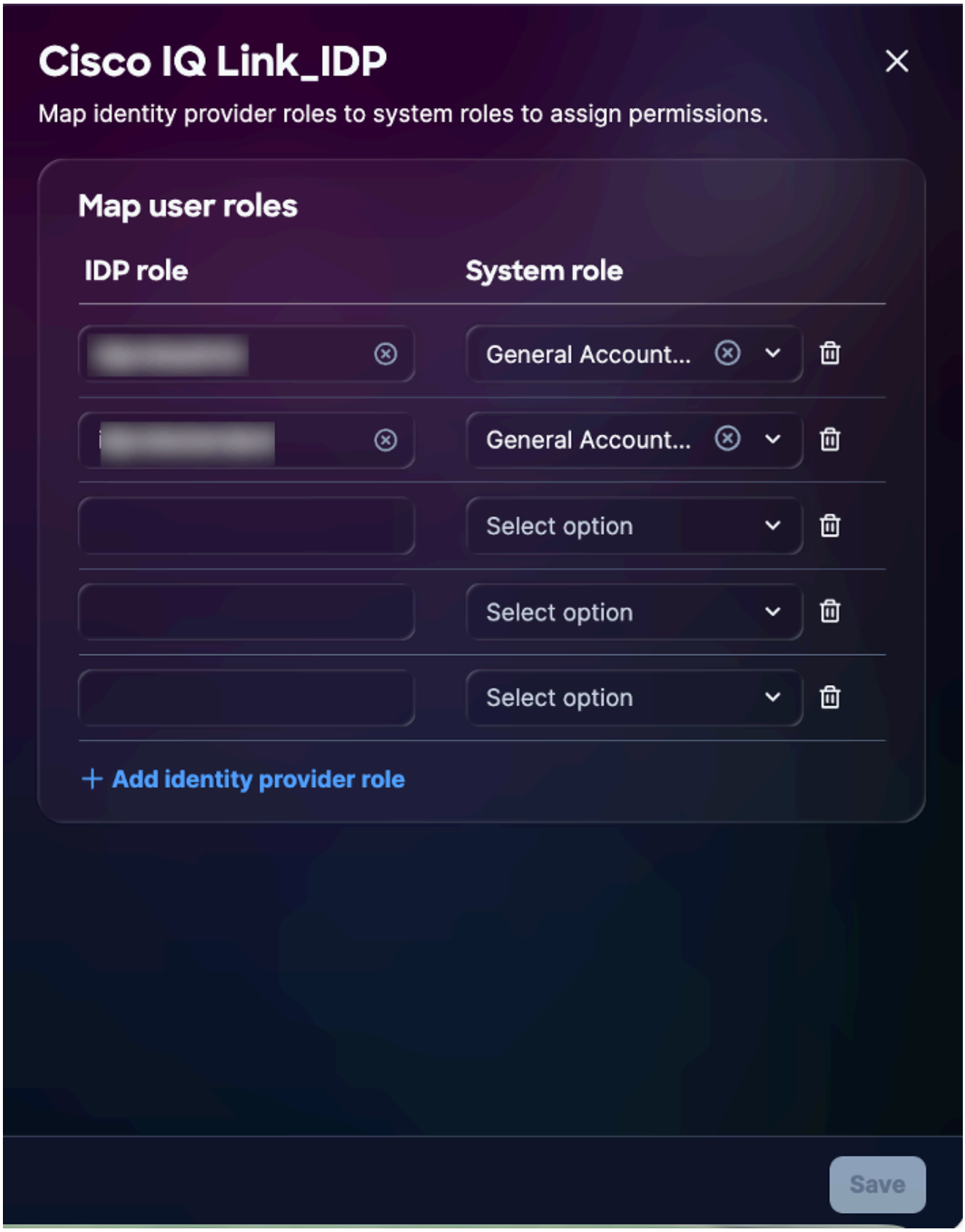
구성이 완료되면 로그인 페이지에 (IDP를 통해) SSO로 로그인할 수 있는 옵션이 표시됩니다.



Cisco IQ 링크 로그인

역할 매핑 컨피그레이션

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



사용자 역할 매핑

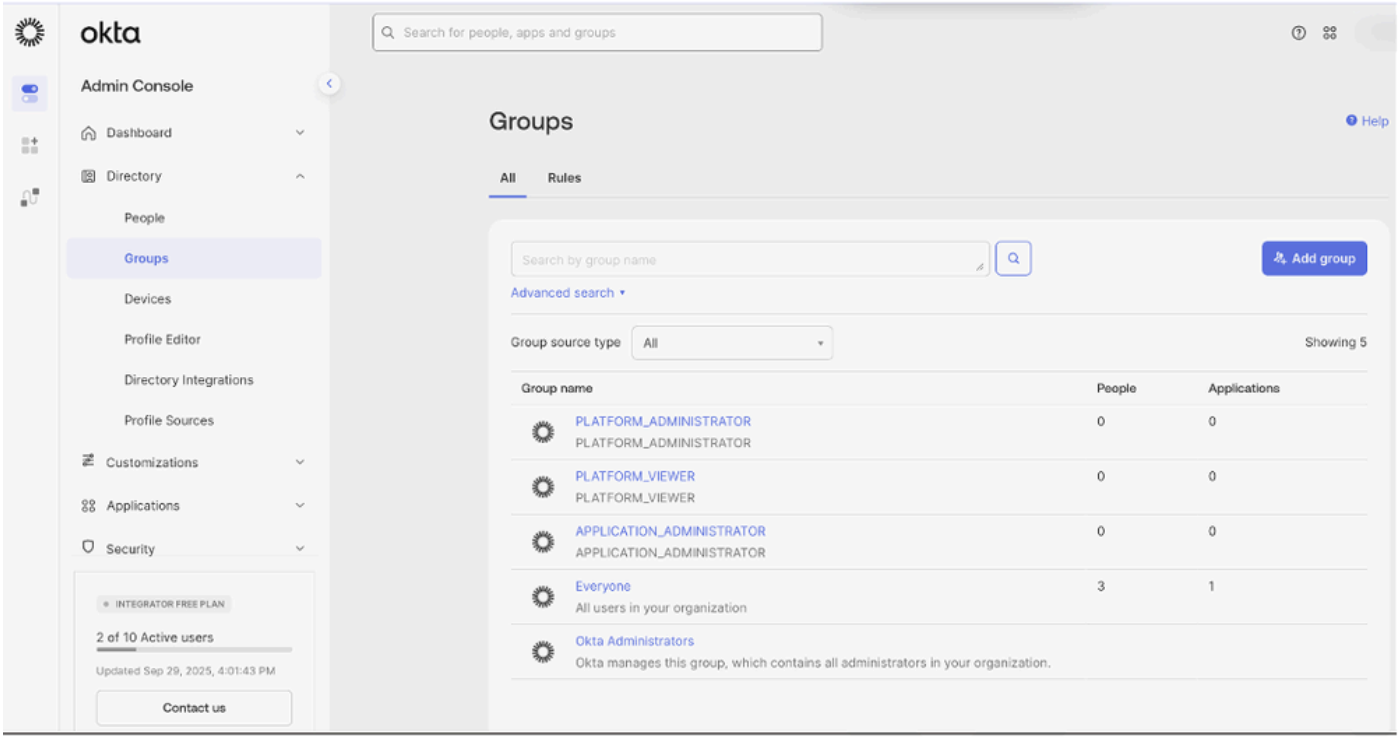
2. 선택한 시스템 역할에 대한 IDP 역할을 입력하십시오. 지원되는 시스템 역할은 다음과 같습니다.

- 일반 계정 관리자: 일반 계정 관리자는 제품의 모든 작업을 수행할 수 있는 모든 권한을 가집

니다

- 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. ID 제공자 역할 추가를 눌러 필요에 따라 추가 역할을 매핑합니다.

4. 저장을 클릭합니다.

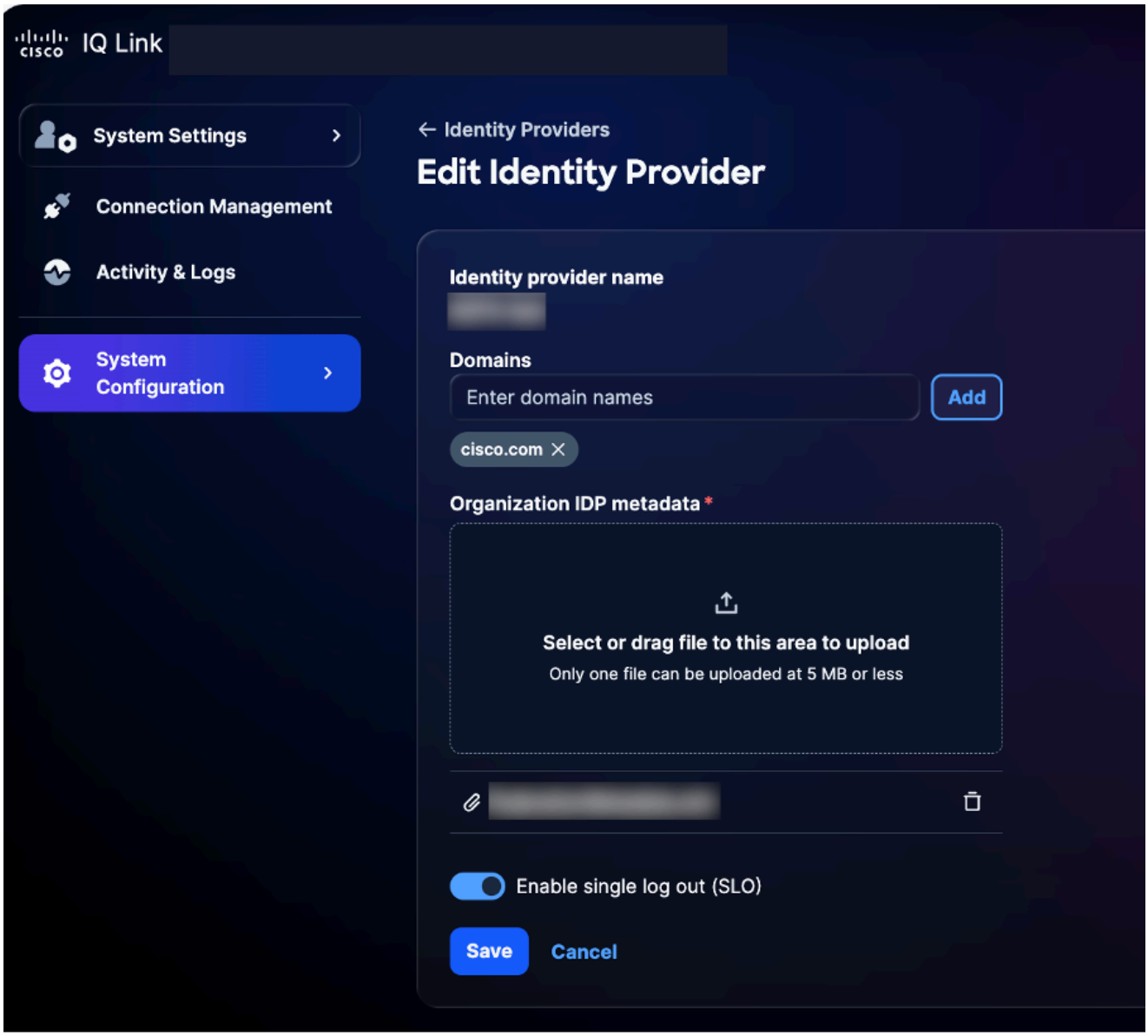
단일 로그아웃 컨피그레이션

SLO(Single Logout Configuration)를 활성화하도록 선택한 경우 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 제공자) 페이지에서 Download SP public certificate(SP 공용 인증서 다운로드)를 클릭합니다.

공용 인증서 다운로드

2. 다운로드 파일을 sp-public-key.crt로 저장합니다.
3. IDP 포털로 이동합니다.
4. SSO를 위한 IDP SAML 컨피그레이션에서 생성된 서명 인증서 파일을 업로드합니다.
5. IDP 메타데이터 파일을 다시 다운로드합니다.
6. Identity Providers(ID 제공자) 페이지에서 추가된 IDP의 More Options(추가 옵션) 아이콘 > Edit(수정)를 선택합니다.



ID 공급자 편집

7. Enable single log out (SLO)(단일 로그아웃(SLO) 활성화) 토글 버튼을 켭니다.
8. 새로 다운로드한 메타데이터 파일을 업로드합니다.
9. 다음 체크리스트를 사용하여 SSO 및 SLO 기능을 확인합니다.

확인 체크리스트:

- 로컬 계정 관리자 로그인 성공
- IDP 포털이 구성 및 프로비저닝됨
- IDP가 "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/SLO 흐름 테스트 성공

IDP 문제 해결

다음 목록에는 IDP 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 4: 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) ADFS(Federation Services)를 Cisco IQ용 SAML IDP로 구성하는 방법을 설명합니다.

AD FS IDP SAML을 SSO에 구성하기 위한 사전 요구 사항

- AD FS 6.0 이상이 권장됨
- Windows Server 2012 R2+
- 구성된 AD 통합
- AD FS의 SSL/TLS(Transport Layer Security) 인증서
- 계정 관리자가 Cisco IQ에 액세스
- ADFS 서버(Windows Server)에 대한 관리 액세스
- AD FS 서버의 PowerShell 액세스
- AD FS와 Cisco IQ 간의 네트워크 연결

- AD FS 서버 컨피그레이션 세부 정보(아래 표 참조)

표 5: ADFS 서버 컨피그레이션

항목	설명	예
Cisco IQ FQDN	사용자 배포 호스트 이름	devxx-23.cx-xxx-xxx.cisco.com
ADFS 서버 URL	사용자 AD FS 서버 주소	https://ad-fs.dev.local
회사 도메인	이메일 도메인	company.com
AD 그룹	AD 그룹 DN(도메인 이름)	CN=역할 - CXIQ 개발자

AD FS 서버 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 디렉토리(예: C:-certificate.crt)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 마법사가 열립니다.

7. Claims Aware 라디오 버튼을 클릭합니다.
8. Start(시작)를 클릭하여 컨피그레이션을 진행합니다.
9. 파일에서 신뢰 당사자에 대한 데이터 가져오기(Import data from a file)를 클릭하여 3단계의 일부로 저장된 파일에서 세부 정보를 가져옵니다.
10. Browse(찾아보기)를 클릭하여 SP 메타데이터 파일을 선택하고 파일 업로드를 완료합니다.
11. Next(다음)를 클릭합니다.
12. 표시 이름(예: "CIQ-Stage")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 또는 *TOTP(Time-Based One-Time Password)가 구성되어 있음)가 없으면 "Permit Everyone with MFA"를 선택하지 마십시오.
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
```

"Permit everyone"(MFA 요건 없음)을 설정하려면 다음 명령을 실행합니다.

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

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

PowerShell을 통해 신뢰 당사자 트러스트를 만들 수도 있습니다.

```
Add-AdfsRelyingPartyTrust `
    -Name “


     ” `
    -Identifier “


      ” `
-SamlEndpoint (New-AdfsSamlEndpoint -Binding POST -Protocol SAMLAssertionConsumer -Uri “


       ”) `
    -AccessControlPolicyName “Permit everyone” `
    -IssuanceAuthorizationRules ’=> issue(Type = “http://schemas.microsoft.com/authorization/claims/per
```

ADFS 클레임 규칙 구성

ADFS 클레임 규칙을 구성하려면 다음 섹션에 나열된 단계를 수행합니다.

필수 클레임

필요한 클레임은 다음 표를 참조하십시오.

표 6: 필수 클레임

클레임	목적	소스
Email	사용자 식별자	AD 메일
표시 이름	사용자의 전체 이름	AD 표시 이름
UPN	PKI(공개 키 인프라)/인증서 인증	ADFS는 UPN(User Principal Name)을 통해 클라이언트 인증서를 AD

클레임	목적	소스
		사용자에게 매핑합니다
이름 ID	SAML 제목	이메일 변형
그룹	역할 기반 액세스	AD 그룹 구성원 (memberOf)

클레임 규칙 적용

1. 당사자 트러스트의 이름(예: "Cisco IQ - Stage")을 정의합니다.

```
$relyingPartyName = “Cisco IQ - Stage”
```

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 ”, Issuer == “AD
=> issue(store = “Active Directory”, types = (“http://schemas.xmlsoap.org/ws/2005/05/identity/claims/em

@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.Iss

@RuleName = “Send Group Membership”
c:[Type == “http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname ”, Issuer == “AD
=> issue(store = “Active Directory”, types = (“http://schemas.xmlsoap.org/claims/Group”), query = “;mem
’@@
```

3. 다음 명령을 실행하여 클레임 규칙을 적용합니다.

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

Write-Host “Claim rules configured successfully!” -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. 사용자 이름을 설정하여 사용자의 그룹 멤버십을 확인합니다.

```
$username = “testuser”
```

2. 다음 명령을 실행하여 사용자 계정을 찾습니다.

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

3. 사용자가 속한 그룹을 표시합니다.

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

출력 예:

```
CN=Role - CXIQ Developers,OU=Role Groups,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 내부 CA(Certificate Authority)에 의해 발급되며 AD FS는 표준 신뢰 체인을 통해 유효성을 검사할 수 없습니다.

- 이 신뢰 당사자에 대해 전역적으로 체인 유효성 검사 사용 안 함

```
Set-AdfsRelyingPartyTrust `
    -TargetIdentifier “


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

또는

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

```
Import-Certificate -FilePath “C:-iq-onprem-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 추가

하는 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.

```
Install-AdcsCertificationAuthority `
    -CAType EnterpriseRootCA `
    -CACommonName “



     ” `
    -KeyLength 2048 `
    -HashAlgorithmName SHA256 `
    -CryptoProviderName “RSA#Microsoft Software Key Storage Provider” `
    -ValidityPeriod Years `
    -ValidityPeriodUnits 10 `
    -Force
```

4. 다음 명령을 실행하여 설치하는 방법

```
certutil -ca
```

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

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

인증서 템플릿 구성

클라이언트 인증 EKU(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 EKU가 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 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, Thumbprint, NotAfter -AutoSize
```

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 장치로 전송합니다.

3. 다음 명령을 실행하여 인증서를 Mac 키 체인으로 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.

```
Enable-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 AddressPath, Enabled, Proxy -AutoSize
```

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", "FormsAu
-PrimaryExtranetAuthenticationProvider @("CertificateAuthentication", "FormsAuthentication", "Microsoft
```

2. 다음 명령을 사용하여 두 목록에 모두 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 포트를 업데이트하고 다음 명령을 사용하여 ADFS 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 만듭니다.

```
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.

```
netsh 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:
Write-Host “Moved $($bad.Count) cert(s) from Root to Intermediate CA store” -ForegroundColor Green
```

3. 다음 명령을 실행하여 자체 서명되지 않은 인증서가 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 7: Channel 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 올바르게 인식되도록 SystemCertificates 저장소에 있어야 합니다.

---

1. 다음 명령을 사용하여 CA 인증서의 지문을 정의합니다.

```
$caThumbprint = “

    ”
```

2. 다음 명령을 사용하여 CA 인증서가 LocalMachinestore에 이미 있는지 확인합니다.

```
$exists = Test-Path “HKLM:\caThumbprint”
```

인증서를 찾을 수 없는 경우 LocalMachinestore로 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 Metadata”}).FullUrl

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.xml으로 이동합니다.
2. <your-adfs-server>를 ADFS 서버의 호스트 이름으로 바꿉니다.
3. 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 표시됩니다. 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.

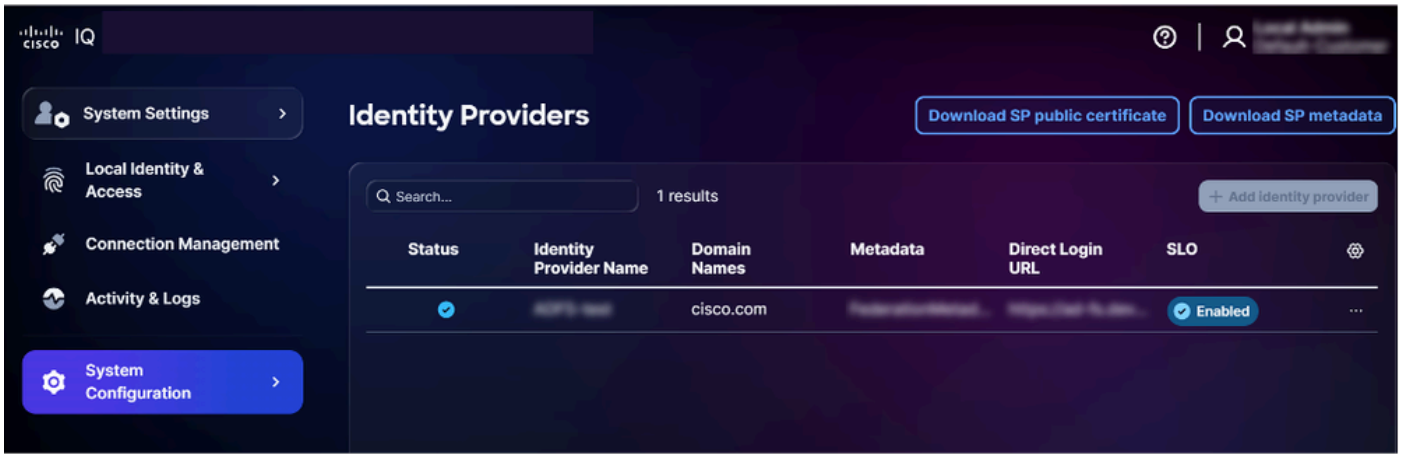
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = “(&(objectClass=group)(cn=Role - CXIQ*))”
$searcher.PropertiesToLoad.Add(“distinguishedName”) | Out-Null
$searcher.PropertiesToLoad.Add(“cn”) | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties[“distinguishedname”]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

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

CN=역할 - CXIQ 개발자,OU=그룹,DC=dev,DC=예,DC=com CN=역할 - CXIQ 뷰어,OU=그룹,DC=dev,DC=예,DC=com

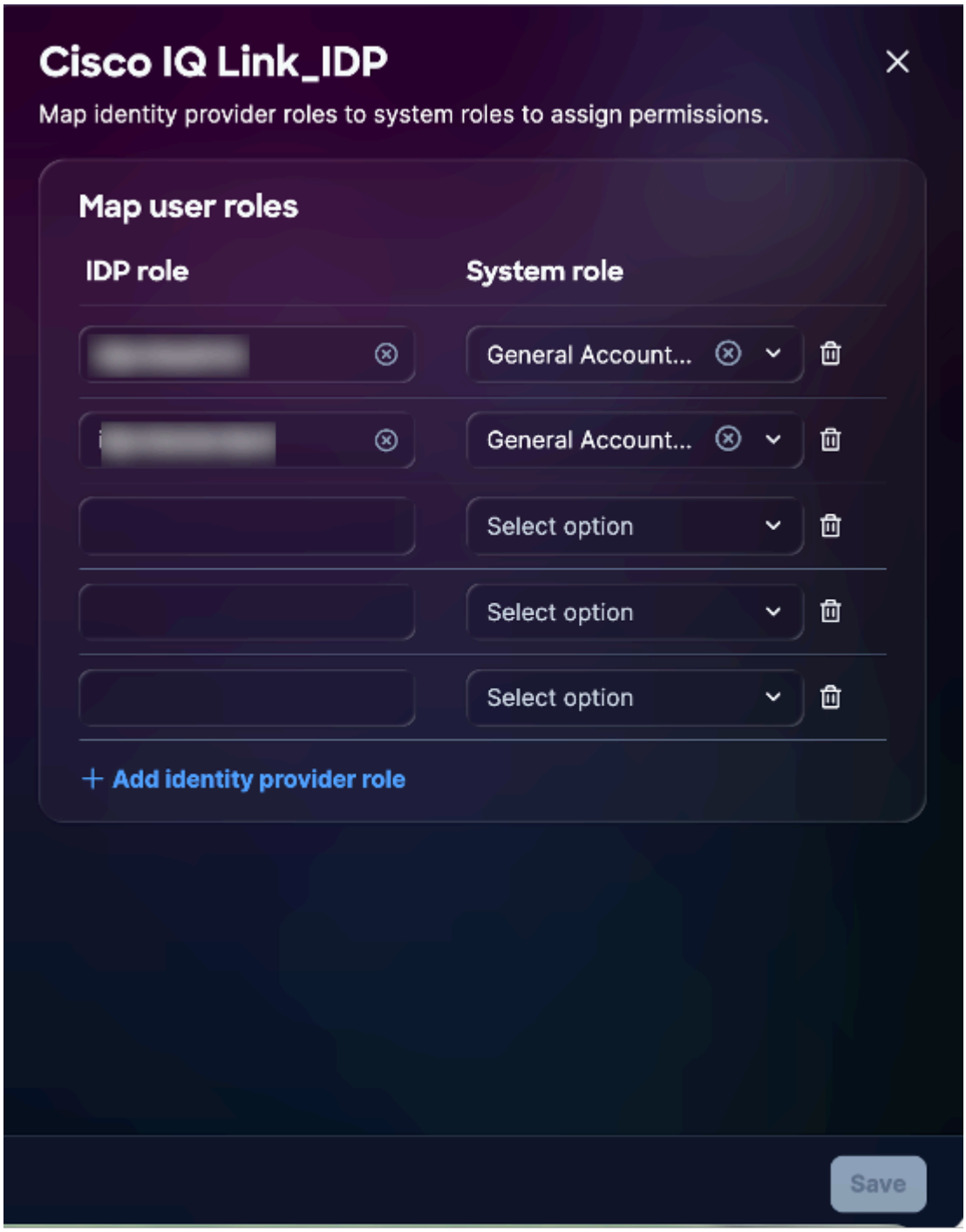
필수 그룹이 나열되지 않으면 계정 관리자가 AD에서 생성해야 AD FS 역할 매핑을 완료할 수 있습니다.

역할 매핑을 구성하려면



역할 매핑

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



역할 매핑

2. 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: 전체 도메인 이름이 아닌 구문 분석된 이름(예: CXIQ Developers)을 사용합니다.

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(자세한 내용은 인증서 기반 인증 구성 아래의 macOS(클라이언트 머신)에서 사용자 인증서 가져오기를 참조하십시오).

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. 로그인에 성공했는지 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 8: 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 • 잘못된 그룹 특성: http://schemas.xmlsoap.org/cla ims/Group이어야 합니다. • 사용자가 AD 그룹에 없습니다.
암호 해독 실패	로그의 "어설션 해독 실패"	AD FS 인증서 컨피그레이션에 대한 컨피그레이션 확인
로그인 루프	인증 또는 로그인 루프에 고착	• 잘못된 ACS URL: 확인: https://your-fqdn/saml/acs • 쿠키 불일치: 올바른 도메인에 대한 브라우저 쿠키 확인

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 - Stage” | 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 - Stage” | 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/CBA(Certificate-Based Authentication)를 모두 지원하는 방법에 대해 설명합니다.

SSO를 위한 Entra ID SAML 구성 사전 요구 사항

- Microsoft 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 9: 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>
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 센터에 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. 갤러리에서 찾을 수 없는 다른 모든 응용 프로그램 통합(비갤러리)을 선택합니다.
6. Create(생성)를 클릭합니다.

SAML Single Sign-On 구성

SAML SSO(Single Sign-On)를 구성하려면 SP 메타데이터 파일을 업로드해야 합니다. VA(Virtual Appliance)에서 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. 메타데이터 파일 업로드 버튼을 클릭하여 SP 메타데이터 파일을 업로드합니다. 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

1. Enterprise Application(엔터프라이즈 애플리케이션)에서 Single Sign-On(단일 로그인)으로 이동하고 SAML을 선택합니다.

2. Basic SAML Configuration(기본 SAML 컨피그레이션) 섹션에서 Edit(편집)를 클릭하고 다음을 입력합니다.

   a. 식별자(엔터티 ID): <YOUR-CIQ-FQDN>

   b. 회신 URL(ACS URL): https://<YOUR-CIQ-FQDN>/saml/acs

   c. 로그온 URL: https://<YOUR-CIQ-FQDN>/saml/login

   d. 로그아웃 URL: https://<YOUR-CIQ-FQDN>/saml/logout

3. 저장을 클릭합니다.

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

---

4. SAML 속성 및 클레임을 구성하려면 [속성 및 클레임] 섹션에서 [편집]을 클릭합니다.

5. 다음 클레임을 구성합니다.

표 10: 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/claims
명사	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
성	user.surname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
이름	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
그룹	user.assignedroles	(비어 있음 — 네임스페이스 지우기)

참고: 그룹 클레임의 경우
- user.assignedroles를 소스로 사용 — user.groups
- 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(애플리케이션 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 관리자, CXIQ 개발

✎ 자, CXIQ 뷰어).

앱 역할은 다음과 같은 이유로 그룹 클레임 대신 사용됩니다.

- 클라우드 전용 테넌트는 P1 또는 P2 라이센스가 없으면 그룹 표시 이름을 보낼 수 없습니다.
- sAMAccountName은 온-프레미스 AD에서 동기화된 그룹에 대해서만 작동합니다.
- 그룹 ID 소스에서 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) 섹션으로 이동합니다.
2. 페더레이션 메타데이터 XML 다운로드(entra-id-metadata.xml로 저장)

   또는

   수동 인증서 입력을 위해 인증서 다운로드(Base64).
3. 설정 섹션에서 다음 값을 기록해 둡니다.

- 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 11: 시스템 역할

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

참고: Entra ID에 구성된 것과 동일하게 App Role Value 문자열을 사용합니다(자세한 내용은 Entra ID SAML 애플리케이션 구성의 App Roles 구성 참조).

3. 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/login으로 이동합니다.
3. Microsoft 로그인 페이지로 리디렉션되었는지 확인합니다.
4. 자격 증명으로 인증합니다(구성된 경우 MFA).
5. 인증 후 /saml/acs로 다시 리디렉션되고 Cisco IQ 애플리케이션이 표시되는지 확인합니다.
6. 다음 명령을 실행하여 그룹 추출을 확인합니다.

```
kubectl -ncxue logs deployment/apisix -since=5m | grep -E “authentication successful|Extracted group|To
```

예상 출력

```
SAML 2.0 compliant authentication successful for user: user@domain.com with full name: N/A and 1 groups
Extracted group: CXIQ Admins (original: CXIQ Admins)
Total groups extracted: 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

- 엔터프라이즈 CA가 구성된 AD CS(Certificate Services)가 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.msc를 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. 요청을 CA에 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 -P “

    ”
```

- 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 센터에 로그인합니다.
2. Protection > Security > Certificate authorities로 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 Subject Alternative Name(주체 대체 이름)에 있는 UPN이 Entra ID 사용자에게 매핑됩니다.

CBA 플로우 확인

1. 익명 또는 전용 모드로 브라우저를 엽니다.
2. https://<YOUR-CIQ-FQDN>/saml/login으로 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 12: 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 Entra ID SAML 애플리케이션 구성의 SAML Single Sign-On 구성 참조). 사용자에게 메일 특성이 채워져 있는지 확인합니다.
추출된 총 그룹: 0	그룹 클레임이 구성되지 않았거나 잘못된 원본	user.assignedroles를 소스로 사용합니다. 사용자가 앱 역할에 할당되었는지 확인합니다(자세한 내용은 Entra ID SAML 애플리케이션 구성에서 앱 역할에 사용자 할당 참조).
중복된 그룹 클레임	user.groups 및 user.assignedroles 모두 활성	user.groups 클레임을 제거합니다. user.assignedroles만 유지합니다.
UUID로 표시되는 그룹	소스 특성은 "Group ID"입니다.	App Roles(앱 역할) 접근 방식을 사용합니다(자세한 내용은 Configuring Entra ID SAML Application(Entra ID SAML 애플리케이션 구성)의 앱 역할 구성을 참조하십시오).
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 서명 CA 접근 방식을 사용합니다(자세한 내용은 랩 환경의 CRL 해결 방법 참조).
인증서를 묻는 메시지가 표시되지 않음	인증서가 키 체인에 없거나, CA가 클라이언트에서 신뢰되지 않거나, CBA가 활성화되지 않음	사용자 인증서가 macOS 키 체인 액세스에서 가져왔는지 확인합니다(자세한 내용은 macOS(클라이언트 머신)에서 사용자 인증서 가져오기 구성 인증서 기반 인증의 아래 참조), CBA가 필요한 설정으로 Entra ID에서 활성화되었는지 확인합니다(자세한 내용은 인증서 기반 인증 구성의 Entra ID 인증 방법에서 CBA 활성화 참조). Chrome이 다시 시작되어 변경 사항이 적용되었는지 확인합니다.
SAML 어설션이 만료되었습니다.	시스템 간 클럭 스큐	플러그인 컨피그레이션에서 clock_skew_seconds를 늘립니다(기본값 300, 실습에 30000 사용).
VA의 상태 "Incomplete"	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 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

- Enttra ID에서 엔터프라이즈 애플리케이션 생성(비갤러리)
- SP 메타데이터를 수동으로 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 ID 제공자 추가
- 앱 역할 값을 Cisco IQ 시스템 역할에 매핑하도록 역할 매핑 구성
- 비밀번호 기반 로그인이 엔드 투 엔드로 작동하는지 확인
- 로그에서 그룹이 올바르게 추출되었는지 확인합니다.

인증서 기반 인증(선택 사항)

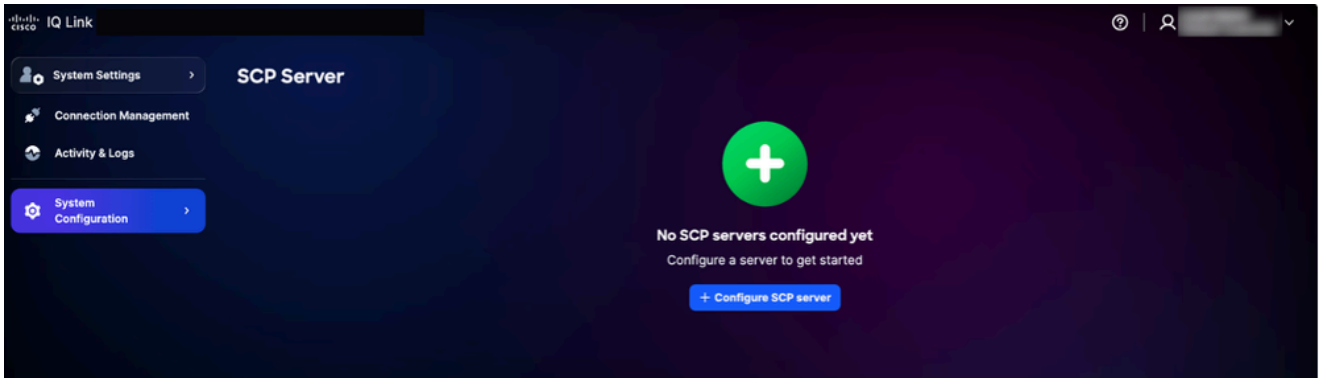
- 클라이언트 인증 EKU를 사용하여 AD CS에 인증서 템플릿 생성
- UPN이 Entra ID 사용자와 일치하는 사용자 인증서 발급
- 사용자 인증서를 PFX로 내보내고 클라이언트 컴퓨터에 설치
- 클라이언트 머신의 CA 인증서 신뢰
- Protection > Certificate authorities(인증 기관)에서 CA 루트 인증서를 Entra ID에 업로드합니다.
- 인증 방법에서 CBA 활성화
- 사용자 이름 바인딩 구성(PrincipalName 및 userPrincipalName)
- CBA 로그인이 엔드 투 엔드로 작동하는지 확인

SCP 서버 추가

이 SCP(Secure Copy Protocol) 서버는 Cisco IQ 설치를 추가, 업그레이드 또는 패치하는 데 필수적인 업그레이드 파일을 가져오기 위한 사전 요구 사항입니다.

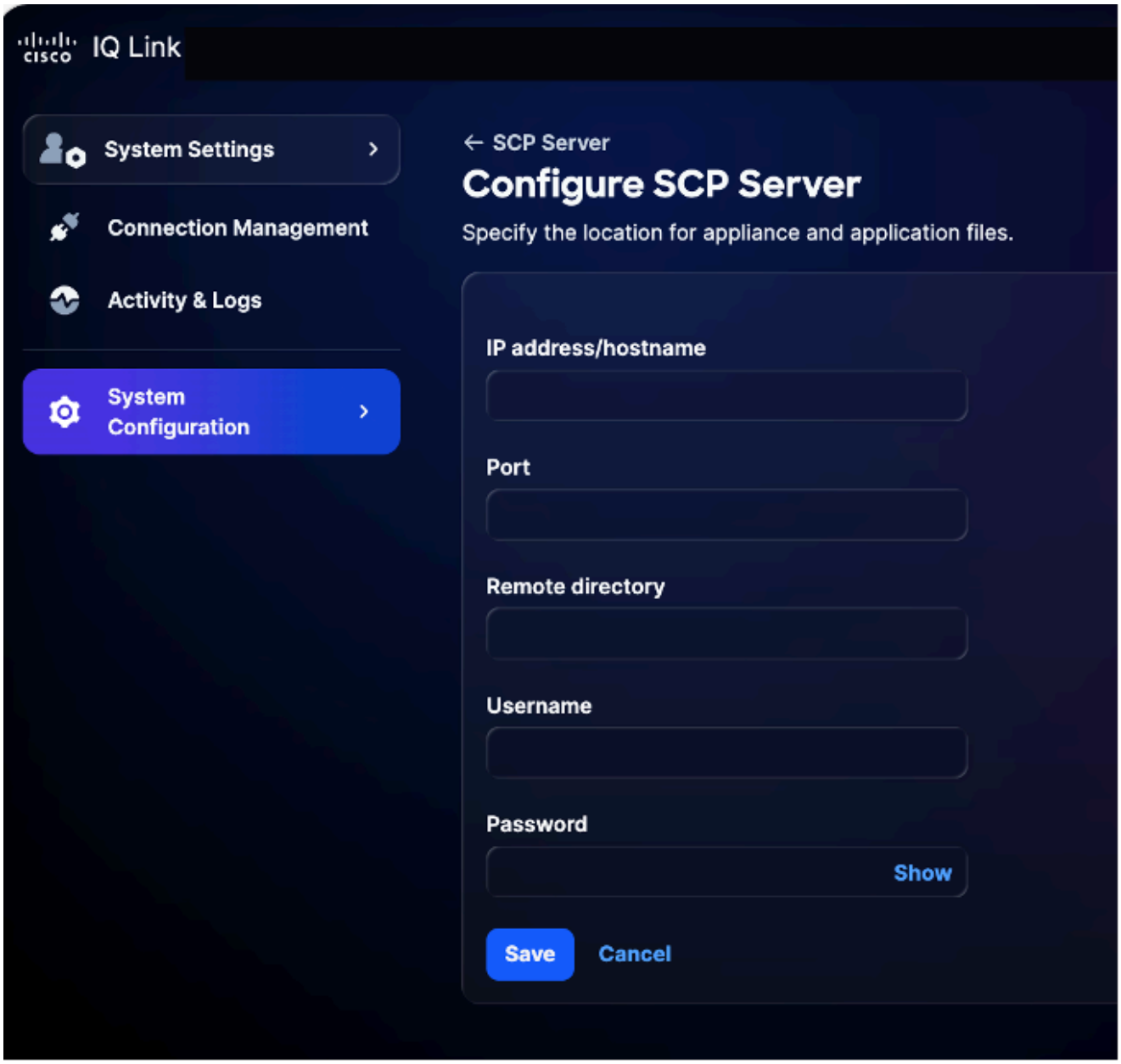
SCP 서버를 추가하려면

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 Server(SCP 서버 구성)를 클릭합니다.



SCP 서버 구성

3. IP 주소/호스트 이름을 입력합니다.
4. 포트 번호를 입력합니다.
5. Remote 디렉터리를 입력합니다.
6. 사용자 이름을 입력합니다.
7. 비밀번호를 입력합니다.
8. 저장을 클릭합니다. 확인 메시지가 표시됩니다.

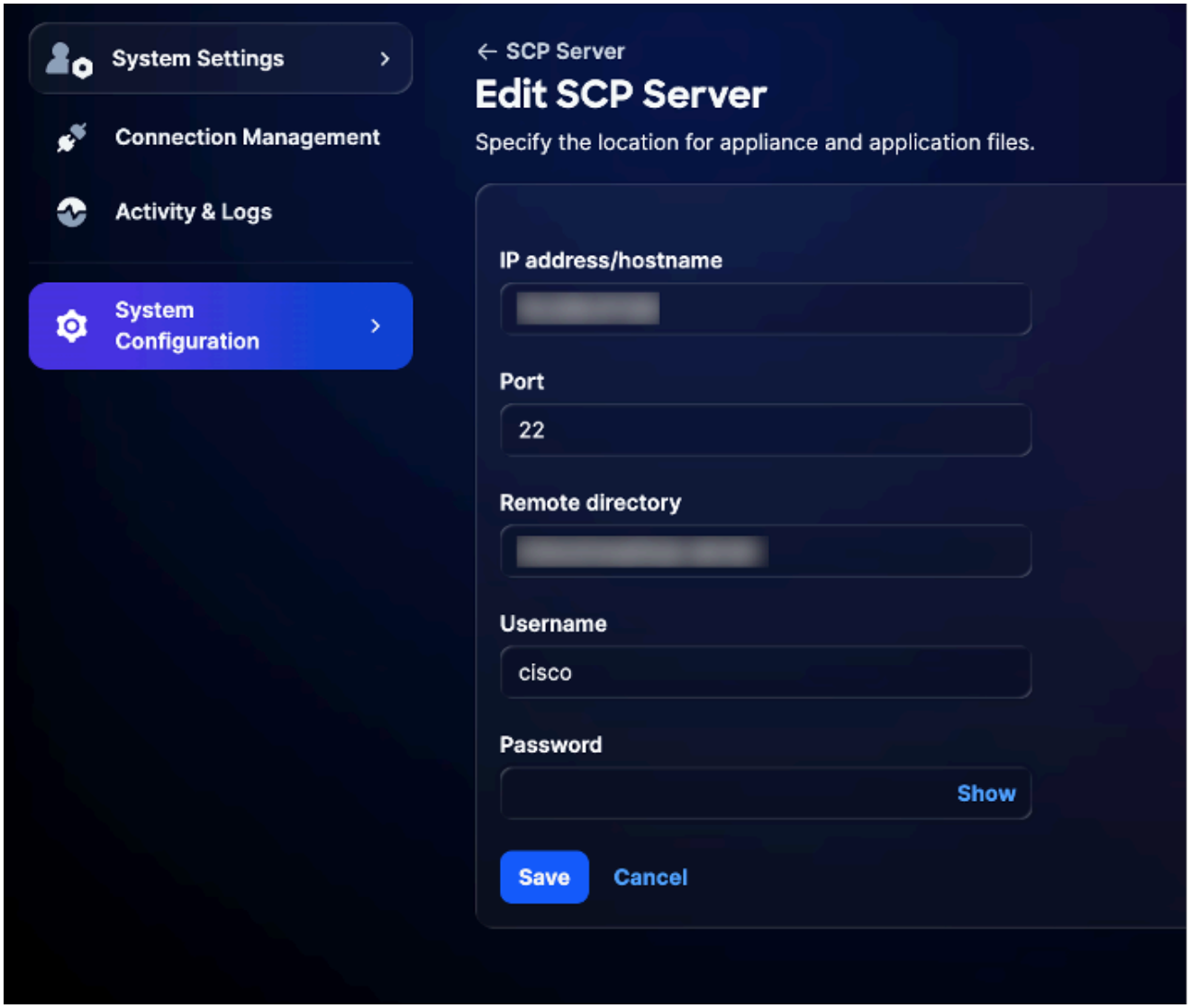
기존 SCP 서버 수정

기존 SCP 서버를 수정하려면

1. SCP 서버 페이지로 이동합니다.

SCP 서버

2. 원하는 기존 SCP 서버에 대해 Edit를 클릭합니다.



SCP 서버 편집

3. 필요에 따라 세부 정보를 수정합니다.

4. 저장을 클릭합니다.

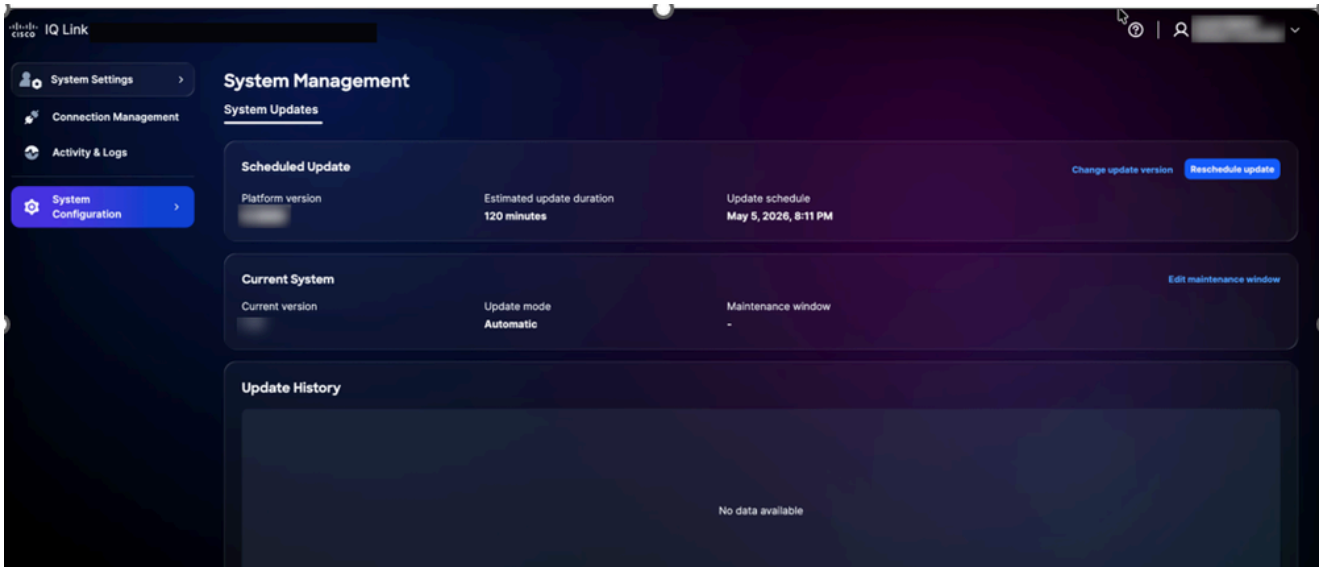
시스템 관리

UI를 통해 최신 Cisco IQ Link 버전으로 업그레이드할 수 있습니다. Cisco IQ Data Connectors 페이지에서 확인할 수도 있습니다.

시스템 업데이트 다시 예약

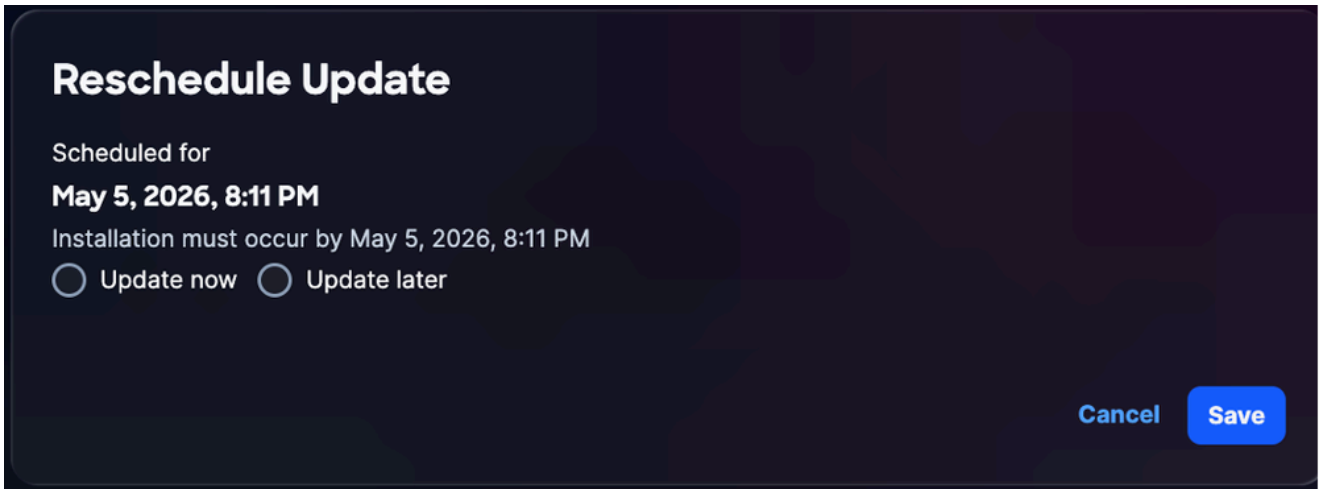
시스템 갱신 스케줄을 조정하려면

1. Administration(관리)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.



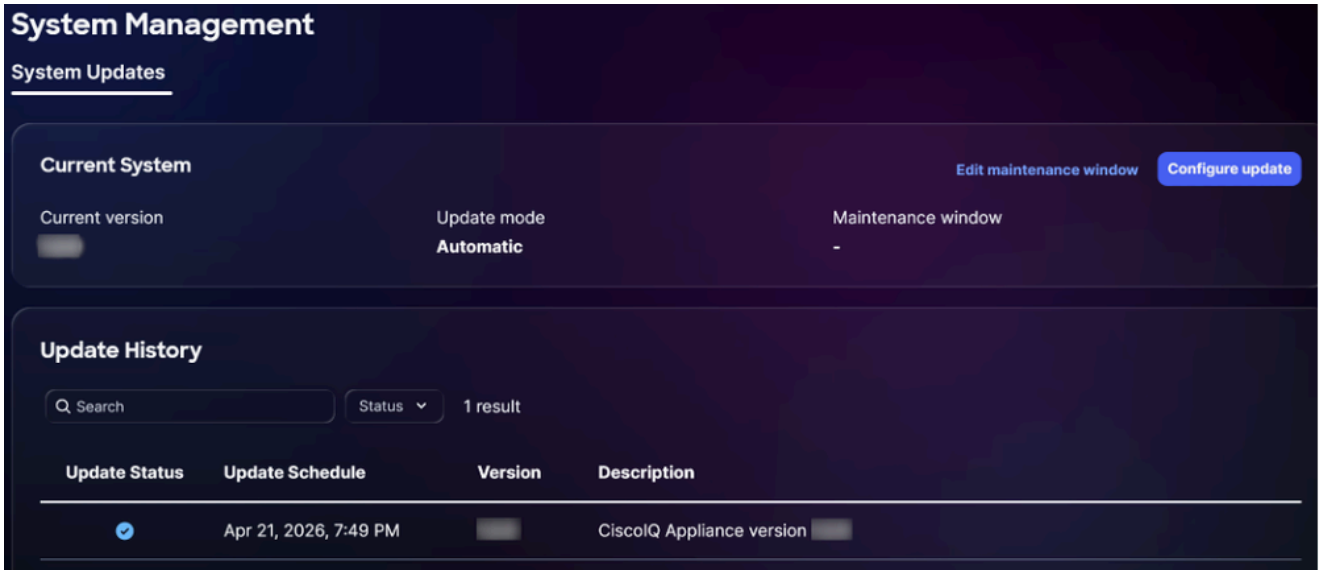
시스템 업그레이드

2. Reschedule update(업데이트 다시 예약)를 클릭합니다.



업그레이드 다시 예약

3. 즉시 일정을 재설정하려면 지금 업데이트 라디오 버튼을 선택하고 다른 시간을 예약하려면 나중에 업데이트 라디오 버튼을 선택합니다.
4. 저장을 클릭합니다. 확인 메시지가 표시되고 System Update 홈 페이지로 리디렉션됩니다.

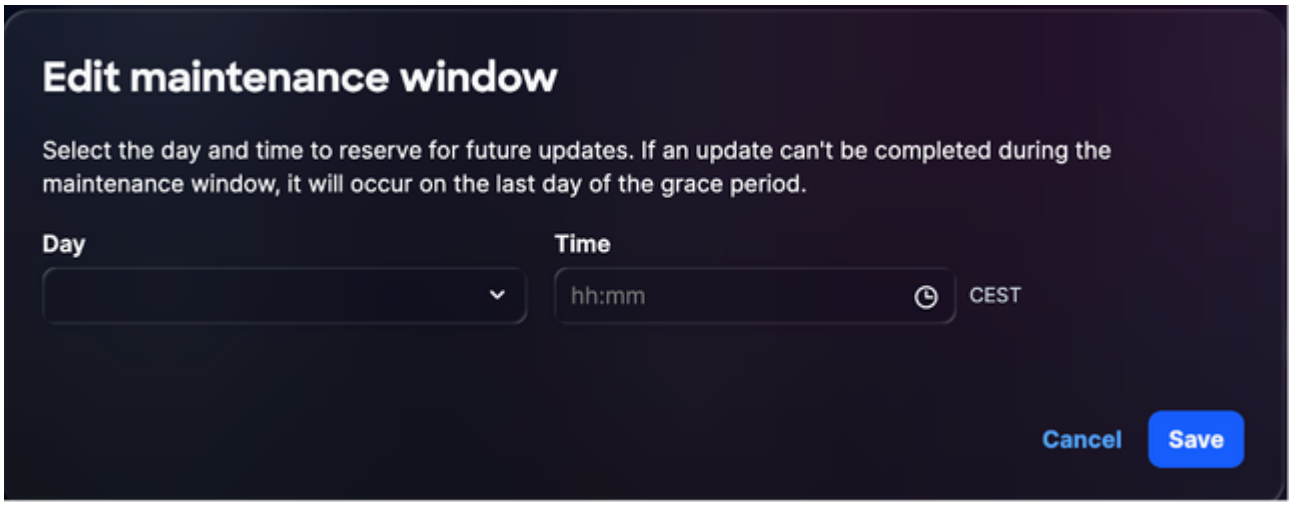


업그레이드 성공

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

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.

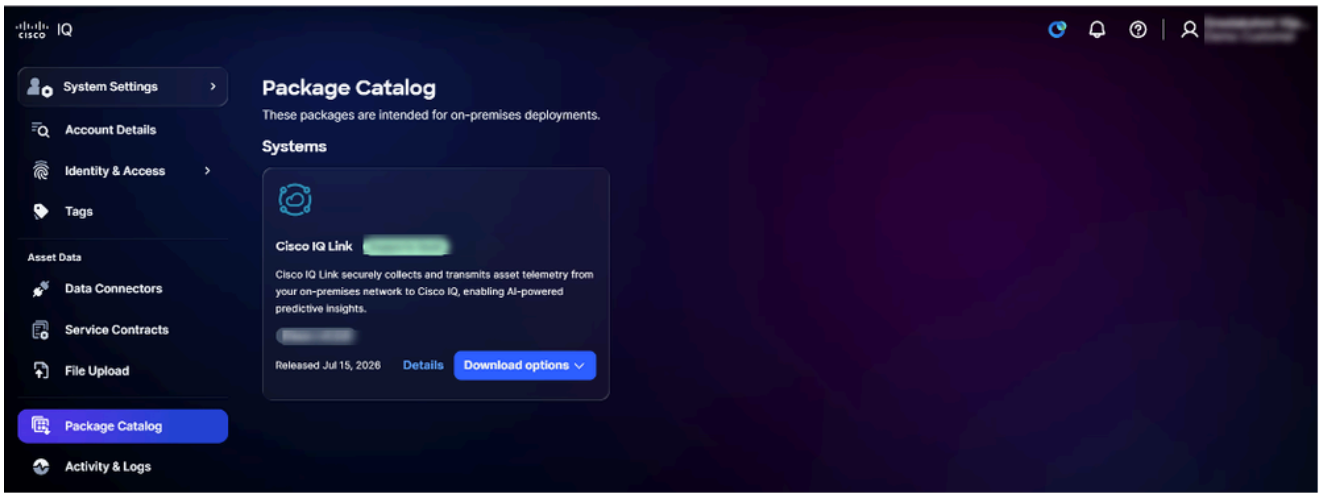
3. 저장을 누릅니다. 유지 관리 창이 성공적으로 예약되었습니다. 업데이트는 표시된 일정에 따라 트리거됩니다.

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.

수동으로 시스템 업그레이드

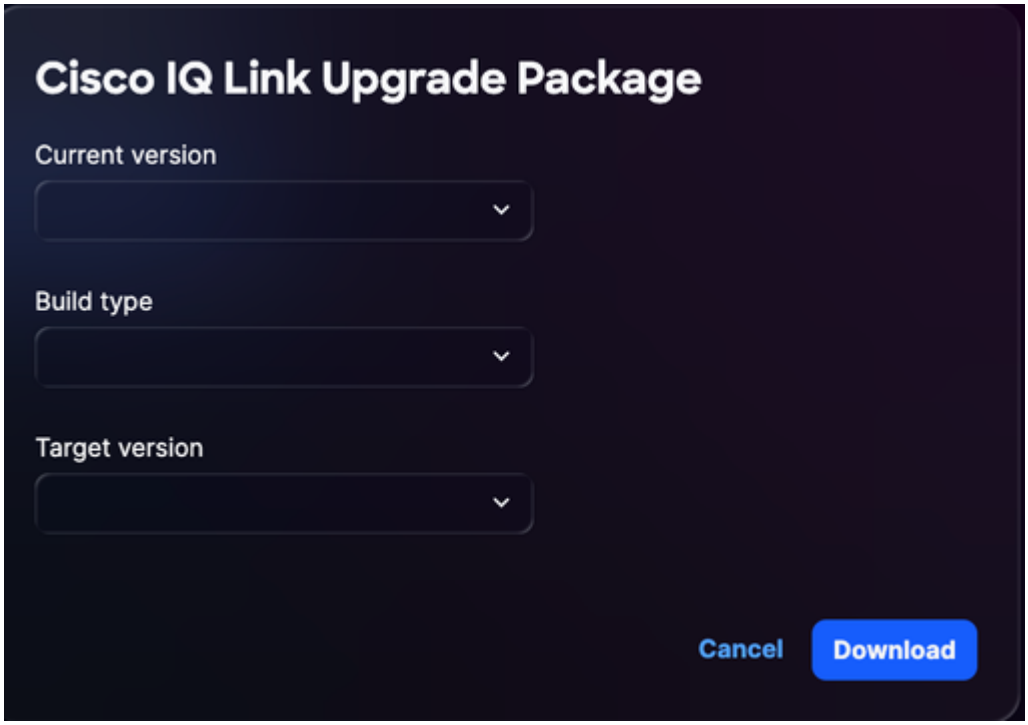
Cisco IQ SaaS에서 자동 배포를 사용할 수 없거나 지연되는 시나리오에서는 Cisco IQ SaaS에서 직접 업그레이드 번들을 다운로드하여 수동으로 시스템 업그레이드를 수행할 수 있습니다. 시스템을 수동으로 업그레이드하려면

1. Cisco IQ SaaS에 로그인하고 Home(홈) > System Settings(시스템 설정) > Package Catalog(패키지 카탈로그)를 선택합니다.



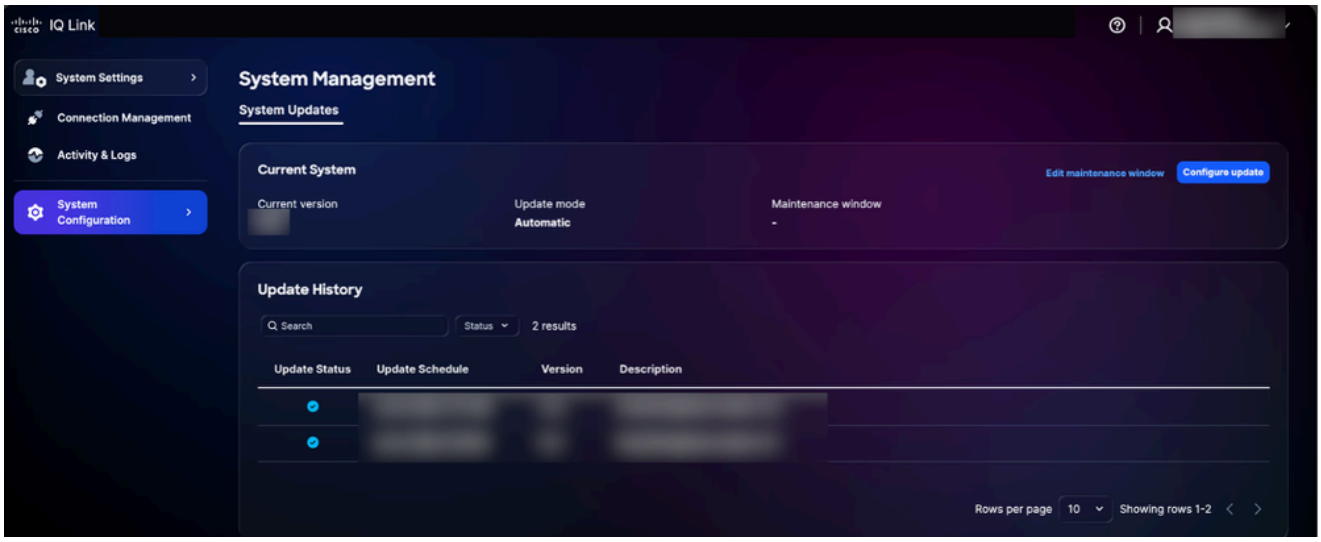
패키지 카탈로그

2. Cisco IQ Link 섹션에서 Download options(다운로드 옵션) > Upgrade packages(업그레이드 패키지)를 클릭합니다.



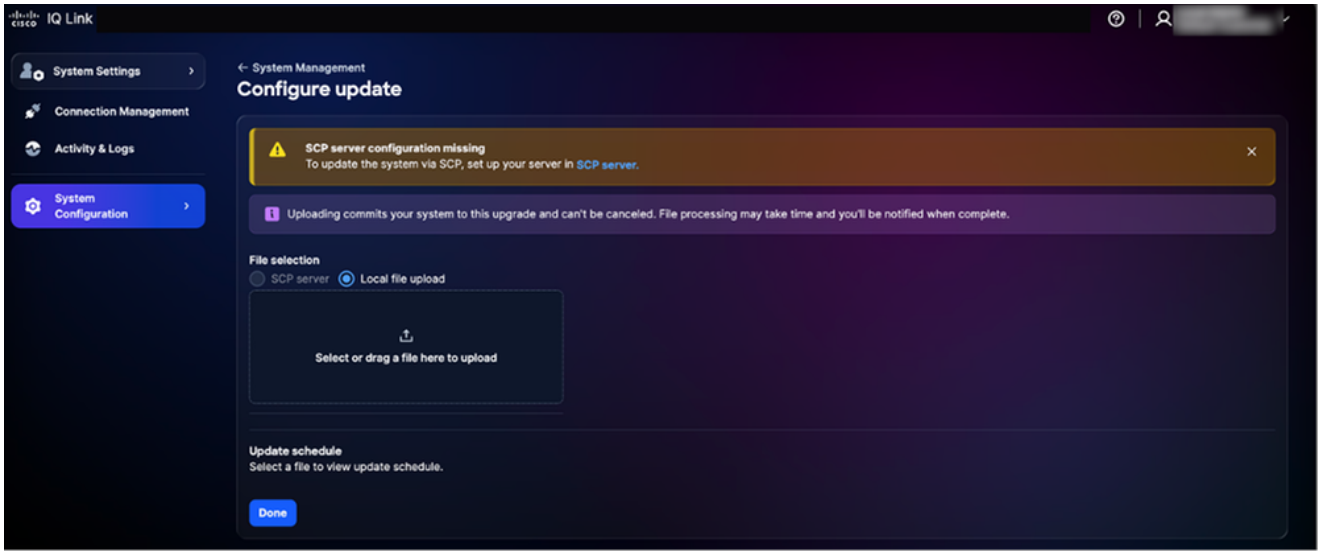
패키지 업그레이드

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



업데이트 구성

9. 업데이트 구성을 클릭합니다.



로컬 파일 업로드

10. Local file upload(로컬 파일 업로드) 라디오 버튼을 클릭합니다.

11. 다운로드한 업그레이드 번들 파일을 선택하거나 업로드 필드로 끌어옵니다.
12. 완료를 클릭합니다. 시스템이 성공적으로 업데이트된 후 확인 메시지가 표시됩니다.

SSL 인증서 컨피그레이션

기본 자체 서명 인증서는 Cisco IQ에 사전 설치되어 활성화되지만 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.

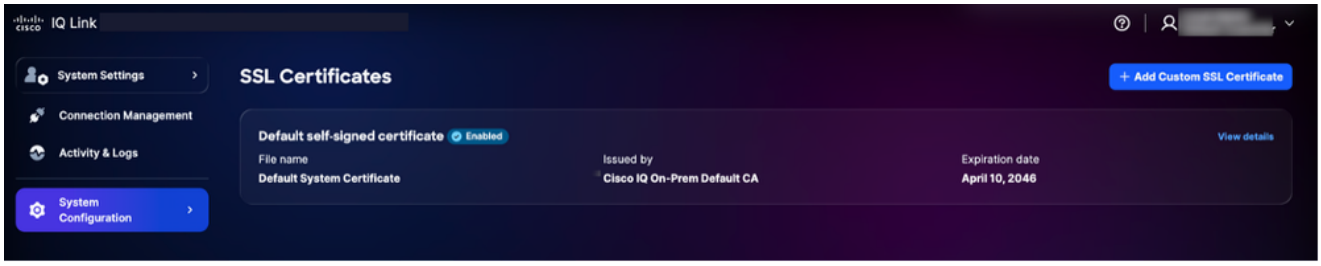
참고: 인증서의 유효 기간이 90일 이상 남아 있어야 합니다. 인증서가 만료될 때까지 남은 기간이 90일 미만일 경우 "만료 임박"으로 간주됩니다.

SSL 인증서를 추가, 수정 또는 삭제한 후 Okta IDP 또는 ADFS IDP에 대한 Single Logout Configuration(단일 로그아웃 컨피그레이션)에 설명된 대로 새 SSL 인증서를 업로드해야 합니다.

사용자 지정 SSL 인증서 추가

사용자 지정 SSL 인증서를 추가하려면

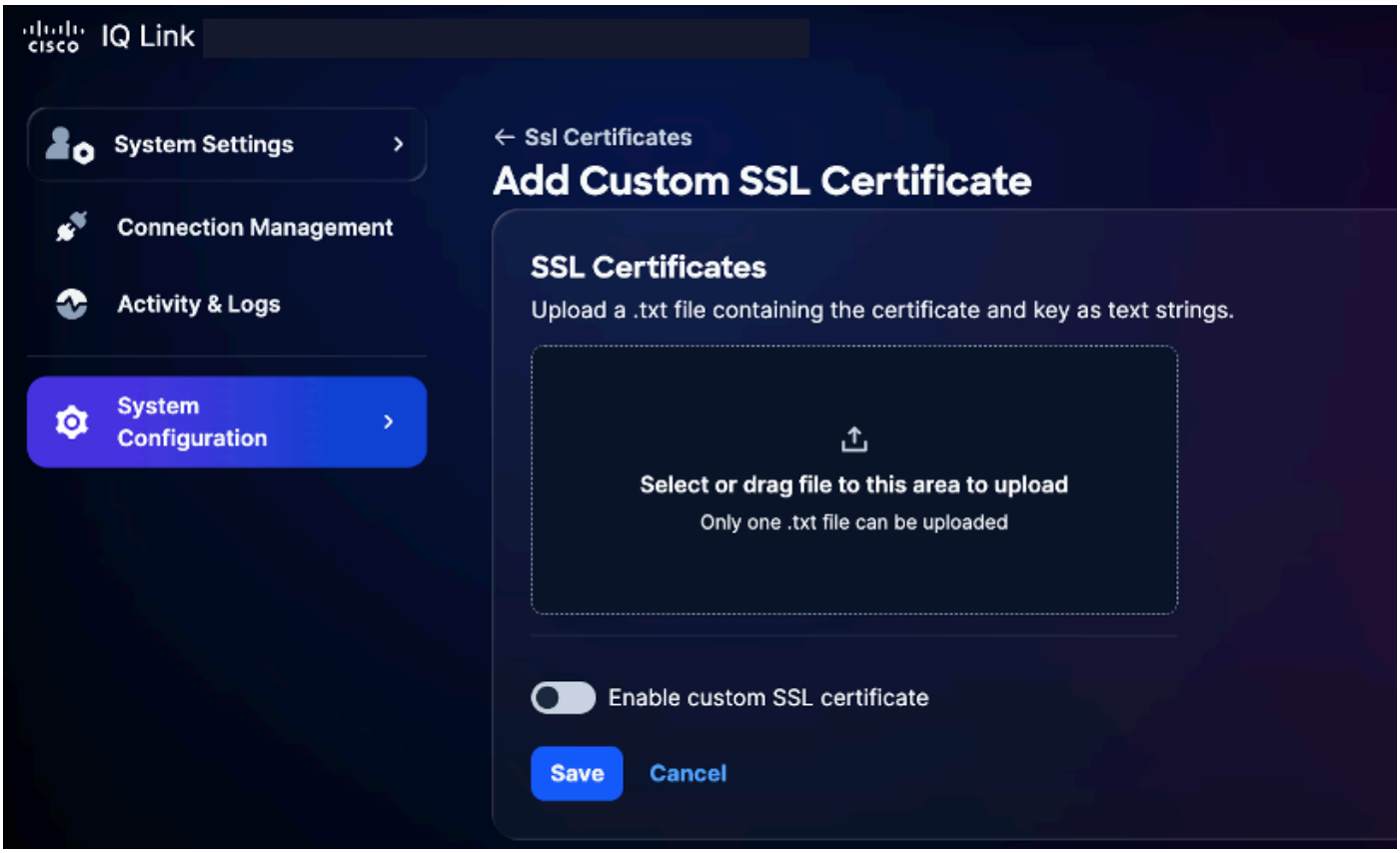
1. System Settings(시스템 설정)에서 System Configuration(시스템 컨피그레이션) > SSL Certificates(SSL 인증서)를 선택합니다. 시스템의 모든 SSL 인증서를 나열하는 SSL Certificates 페이지가 표시됩니다.



SSL 인증서 추가

2. Add Custom SSL Certificate를 클릭합니다.

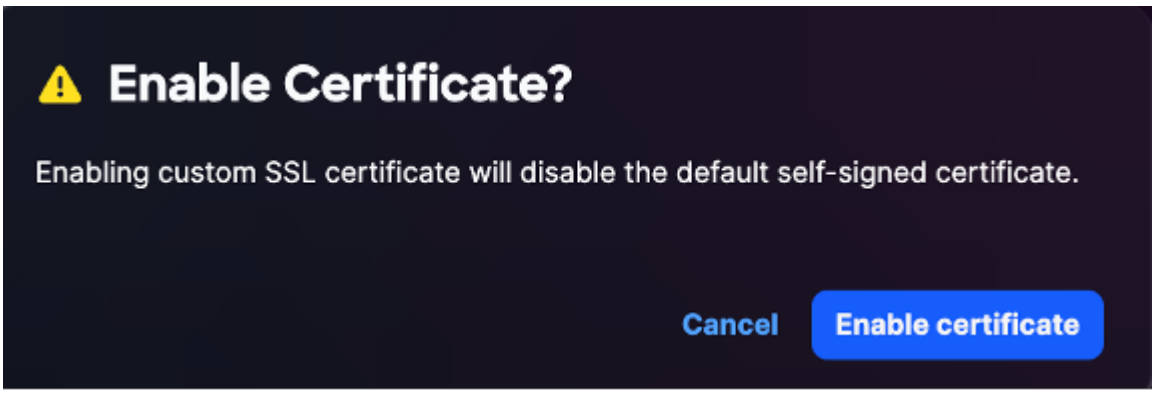
참고:
- Privacy-Enhanced Mail 인코딩 인증서 및 키가 모두 포함된 .txt 파일을 텍스트 문자열로 업로드합니다.
- 한 번에 하나의 .txt 파일만 업로드할 수 있습니다.
- 파일에 인증서와 개인 키가 모두 포함되어야 합니다.



SSL 인증서 업로드

3. 사용자 지정 SSL 인증서를 SSL Certificate(SSL 인증서) 필드에 끌어서 놓거나 업로드합니다.

4. Enable custom SSL certificate(사용자 지정 SSL 인증서 활성화) 토글 버튼을 켭니다.



SSL 인증서 편집

참고: 인증서를 즉시 활성화하지 않고 업로드하려면 토글을 끄지 않습니다.

5. Enable certificate(인증서 활성화)를 클릭합니다.

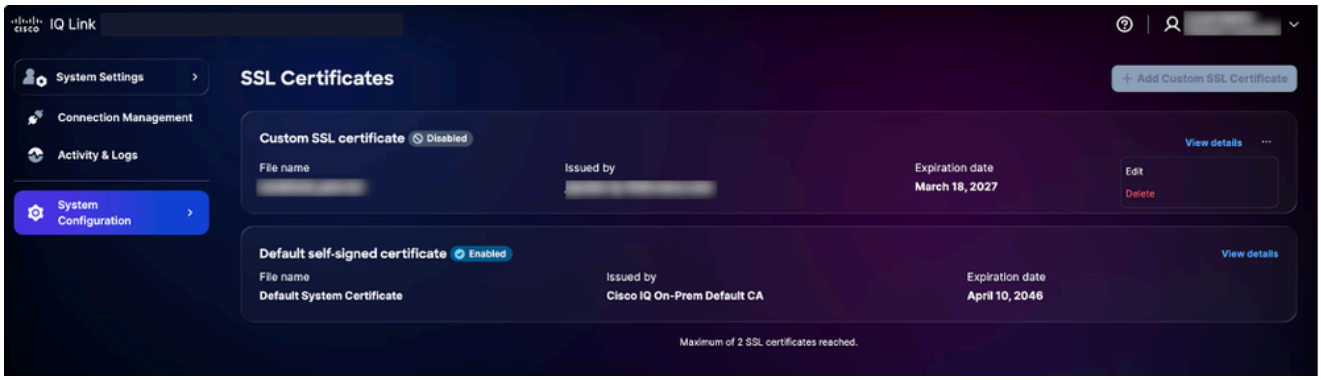
6. 저장을 클릭합니다.

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.



SSL 인증서 편집

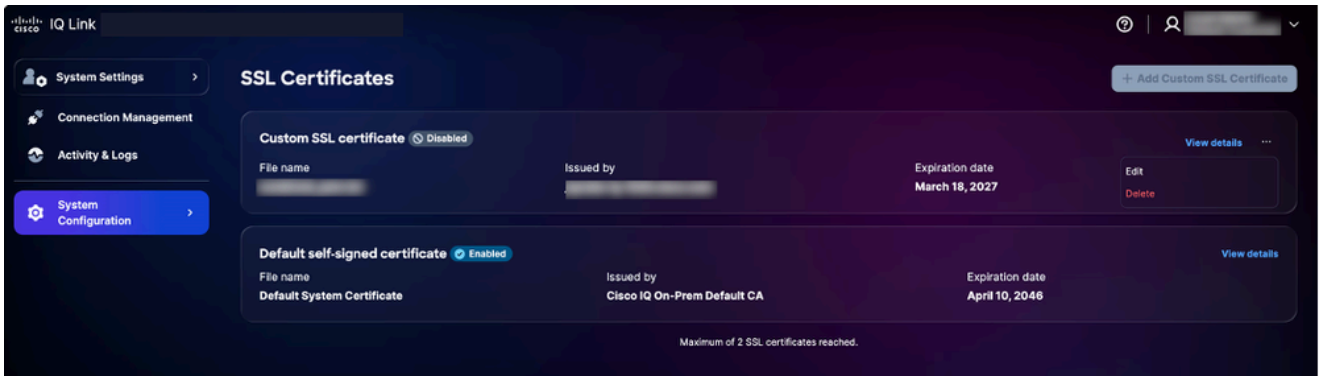
2. 추가 옵션 아이콘 > 편집을 선택합니다. Edit SSL Certificate 페이지가 표시됩니다.
3. 필요에 따라 인증서 세부사항을 수정합니다.
4. 저장을 클릭합니다.

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 사용자 지정 SSL 인증서로 이동합니다.



SSL 인증서 삭제

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

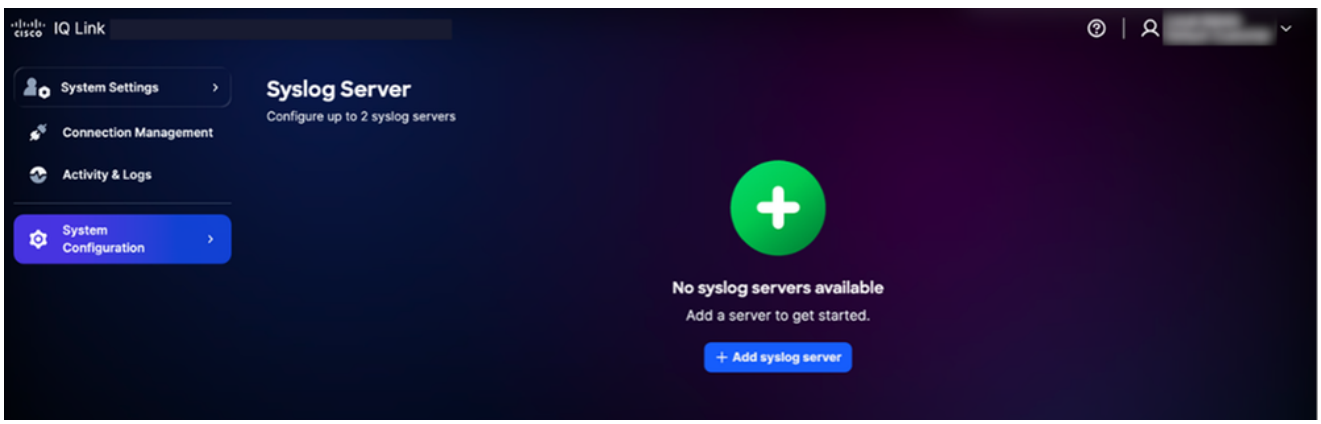
계정 관리자 역할의 사용자는 외부 syslog 서버가 시스템 로그를 내보내도록 구성할 수 있습니다. 최대 2개의 syslog 서버를 구성할 수 있습니다.

참고: Syslog 서버는 FQDN이 아니라 IP 주소로 지정해야 합니다.

Syslog 서버 추가

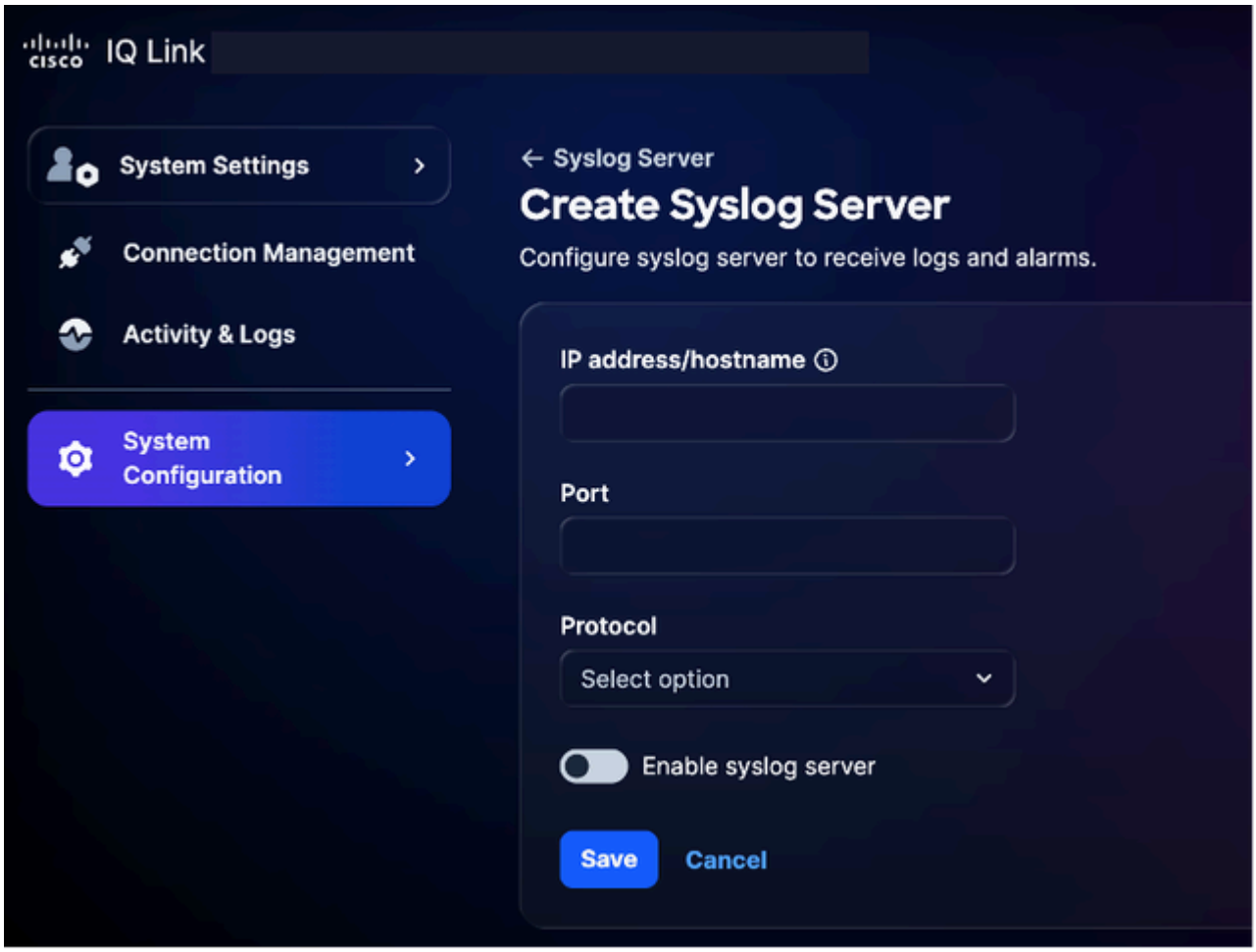
syslog 서버를 추가하려면

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

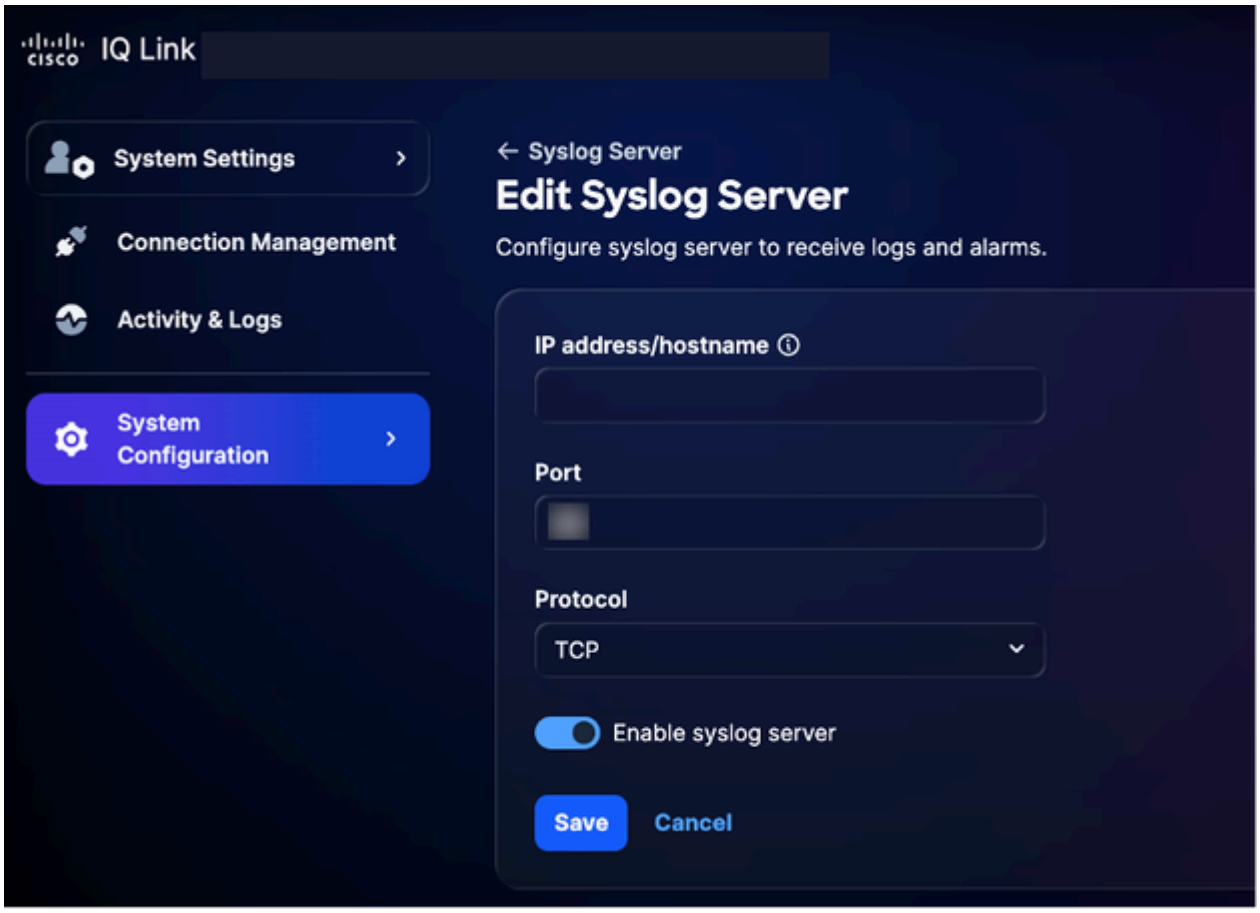
3. IP 주소/호스트 이름을 입력합니다.
4. 포트 번호를 입력합니다.
5. Protocol 드롭다운 목록에서 해당 프로토콜(예: UDP 또는 TCP)을 선택합니다.
6. Enable syslog server 토글 버튼을 켭니다.
7. 저장을 클릭합니다. 확인 메시지가 표시되고 새로 추가된 syslog 서버가 Syslog 서버 홈 페이지에 표시됩니다.

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 표시

됩니다.



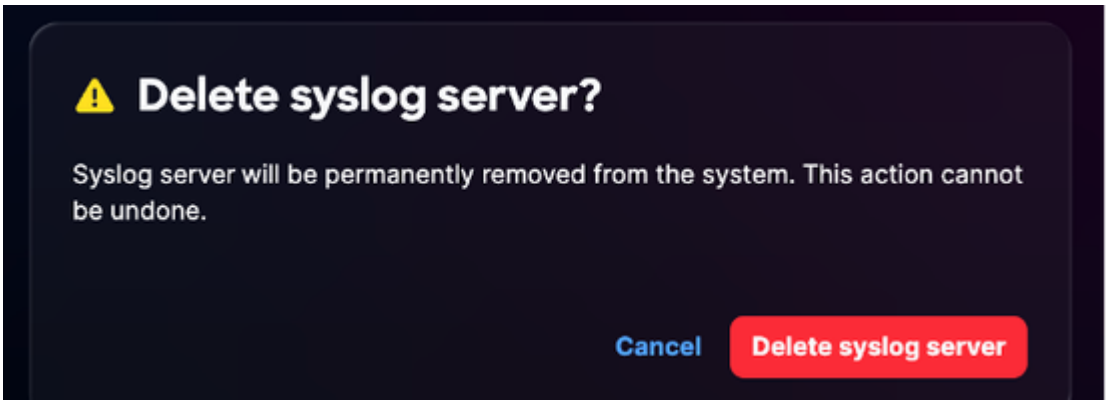
Syslog 서버 편집

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.

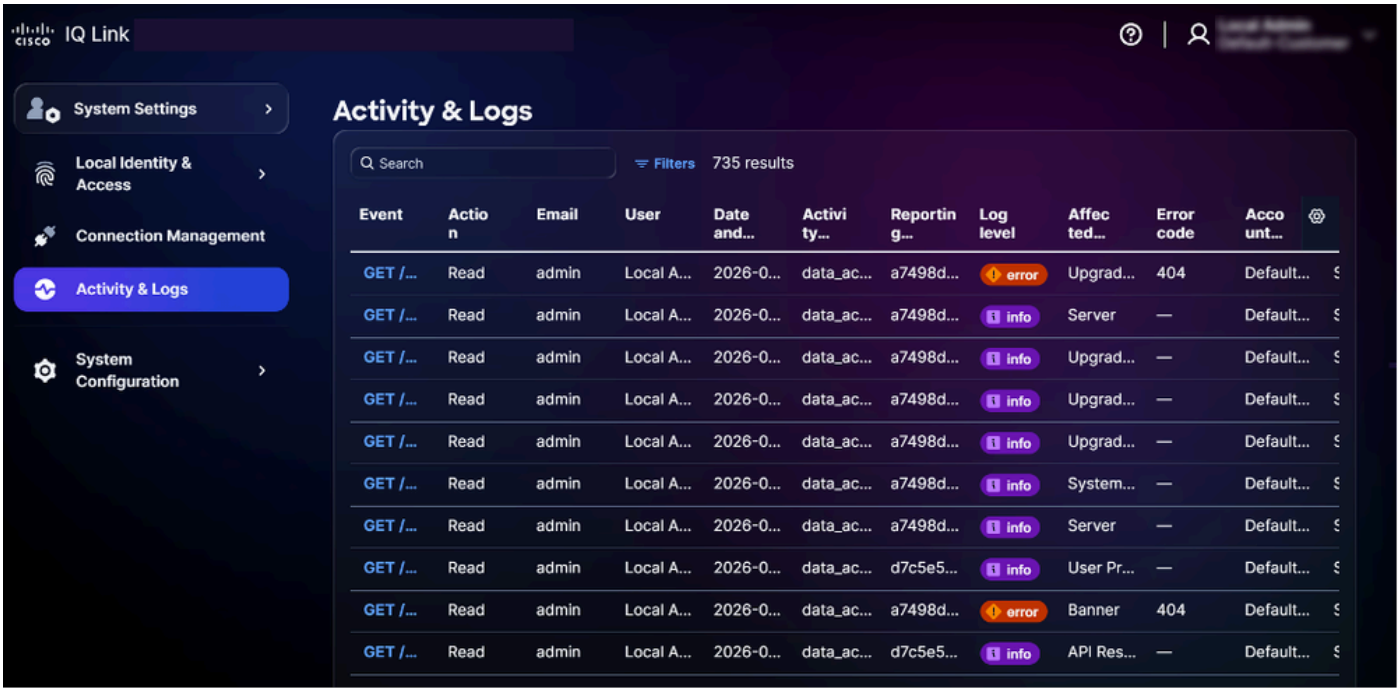


확인

3. Delete syslog server(syslog 서버 삭제)를 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.



작업 및 로그

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

작업 및 로그:

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

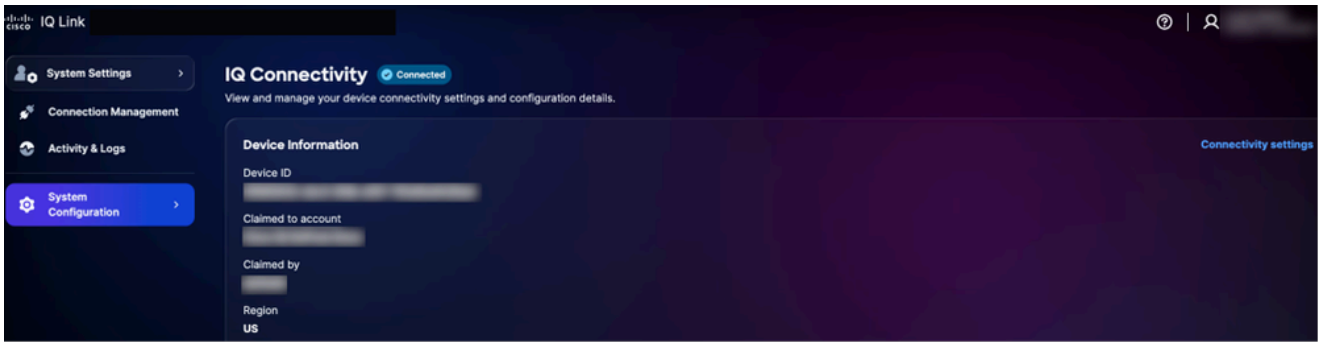
다음 필터 옵션을 사용할 수 있습니다.

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

IQ 연결

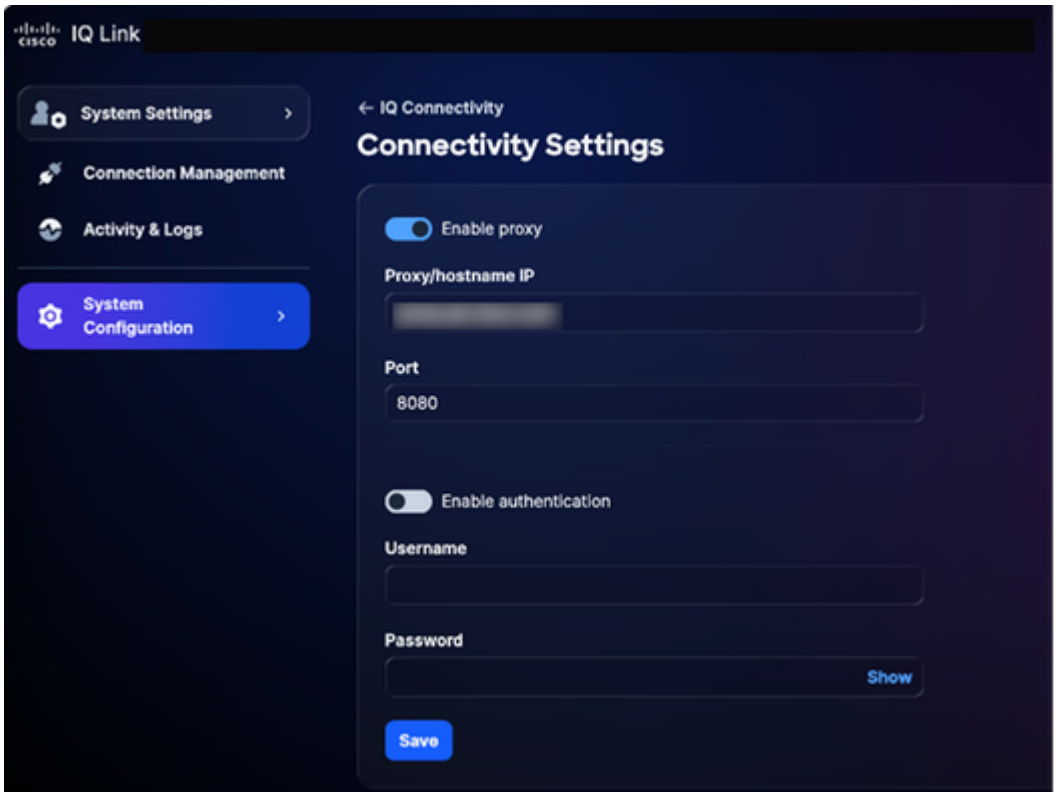
디바이스 연결 설정 및 컨피그레이션 세부사항을 보고 관리하려면

1. System Settings(시스템 설정)에서 System Configuration(시스템 컨피그레이션) > IQ Connectivity(IQ 연결)를 선택합니다. IQ Connectivity(IQ 연결) 페이지가 표시됩니다.



IQ 연결

2. Connectivity settings(연결 설정)를 클릭합니다.



연결 설정

3. 필요에 따라 세부사항을 업데이트합니다.
4. 저장을 클릭합니다.

연결 관리(데이터 수집)

Cisco IQ Link는 네트워크 데이터 수집을 위한 온프레미스 솔루션으로 인프라에 대한 심층적인 가시성을 제공하도록 설계되었습니다. Catalyst Center 및 Direct Connection을 통해 데이터를 수집합니다. 네트워크 인증 및 디바이스 검색을 관리하는 방법이 간소화됩니다. 데이터 수집 구성은 아래에 요약되어 있습니다.

- 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.

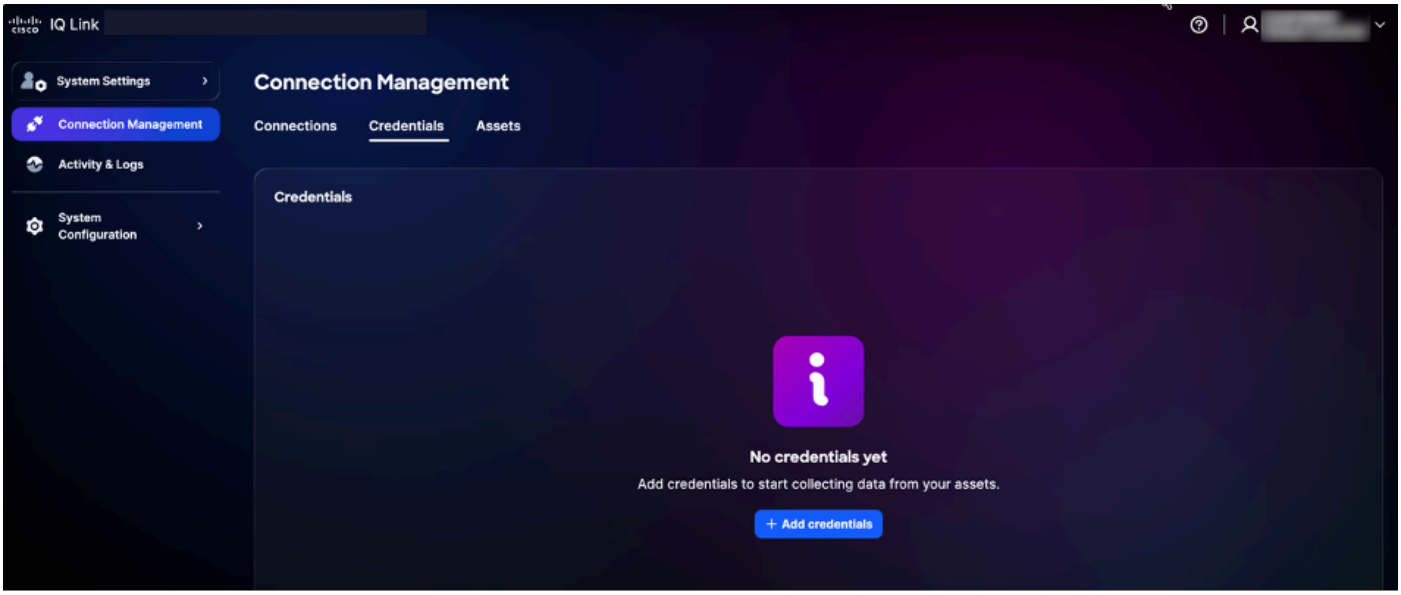
참고: 디바이스 검색을 위해서는 SNMPv2c/SNMPv3 및 SSH가 필요하며, Catalyst Center를

구성하기 전에 HTTP/HTTPS 자격 증명을 제공해야 합니다.

자격 증명 추가

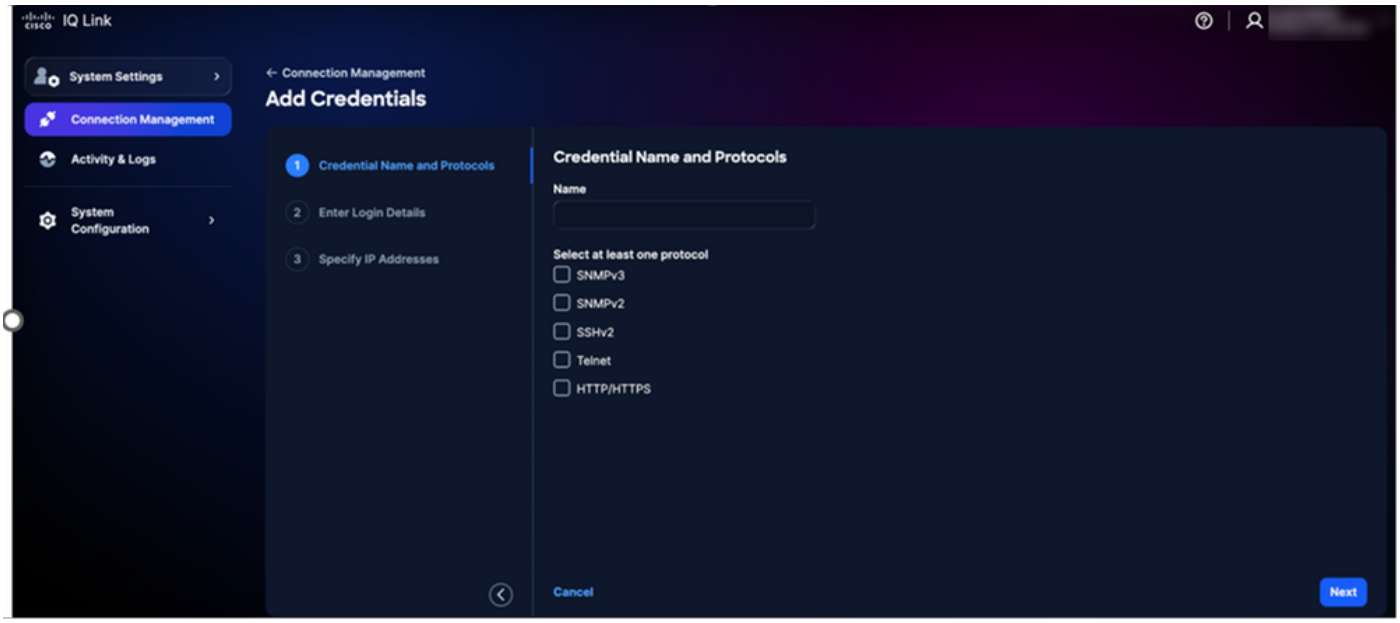
데이터 수집을 수행하려면 먼저 자격 증명을 추가해야 합니다. 자격 증명을 추가하려면

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. 자격 증명 추가를 클릭합니다.

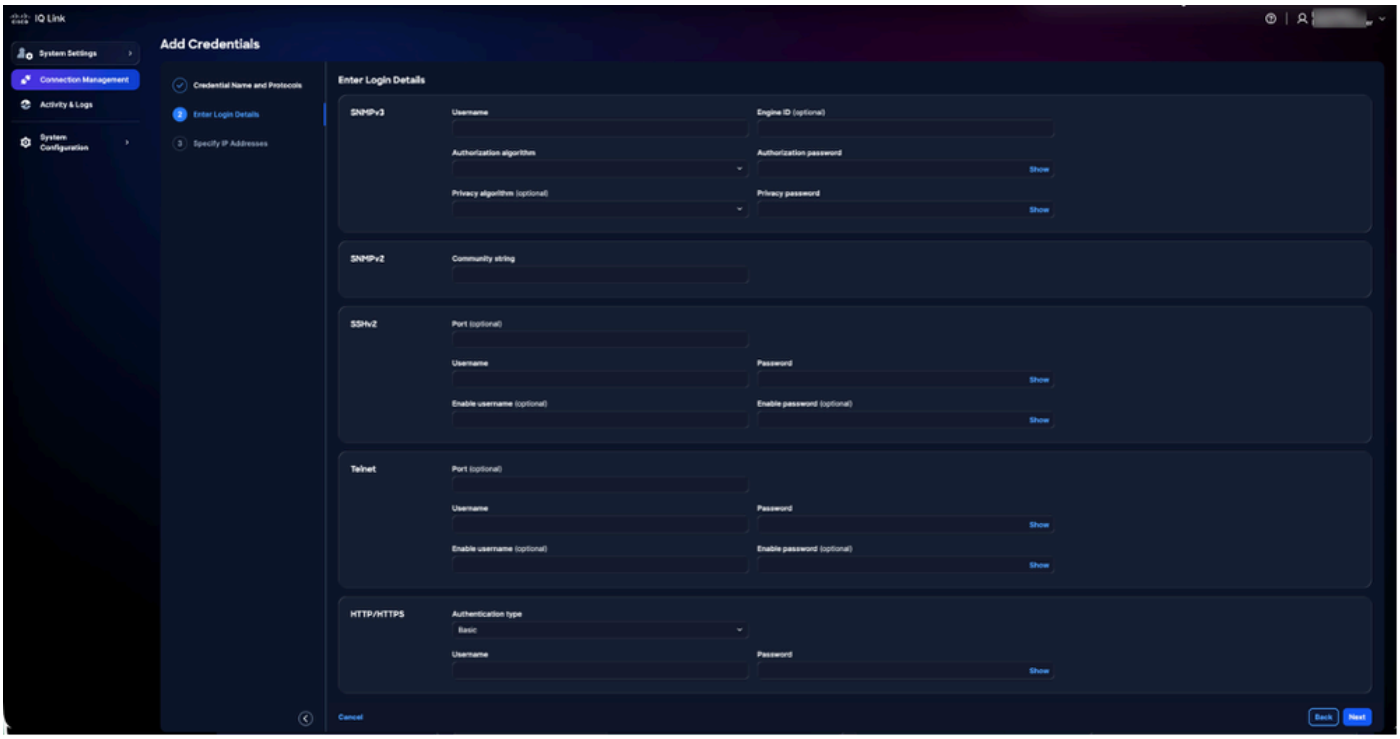


자격 증명 추가

4. 이름을 입력합니다.

5. 해당되는 모든 프로토콜 체크박스를 선택합니다.

6. 다음을 클릭합니다.

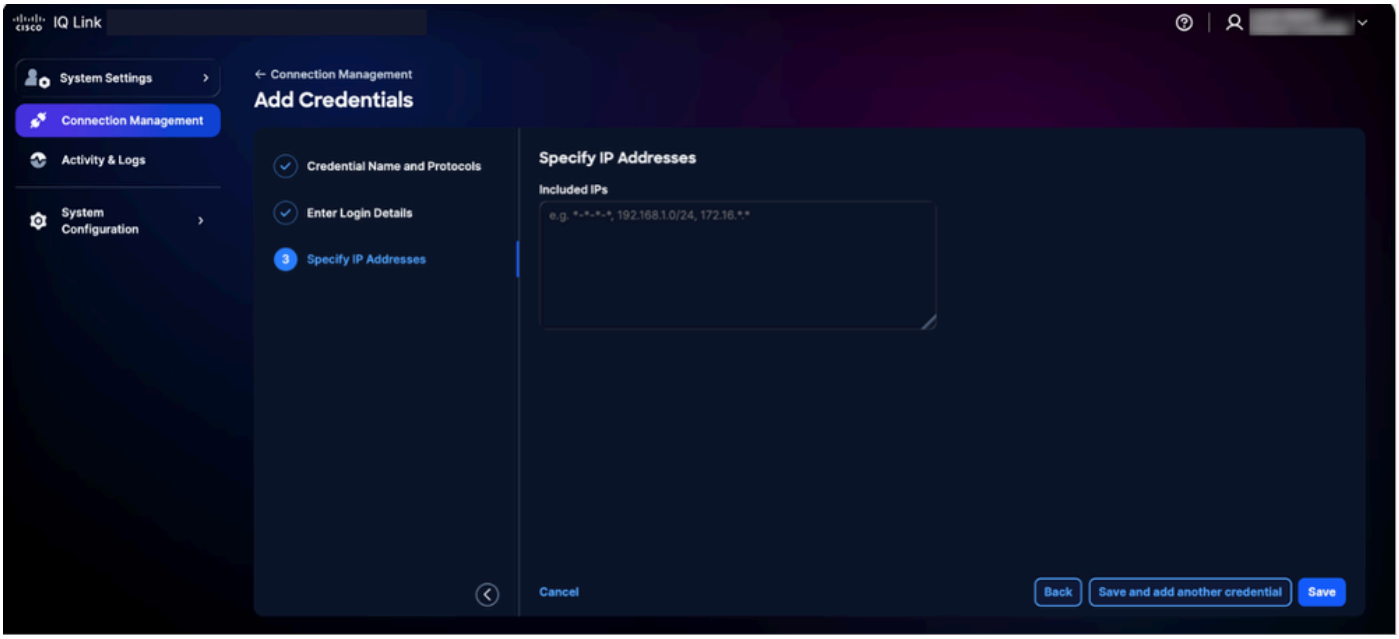


자격 증명 추가 세부 정보

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

7. 선택한 각 프로토콜에 대한 로그인 상세내역을 입력합니다.

8. 다음을 클릭합니다.

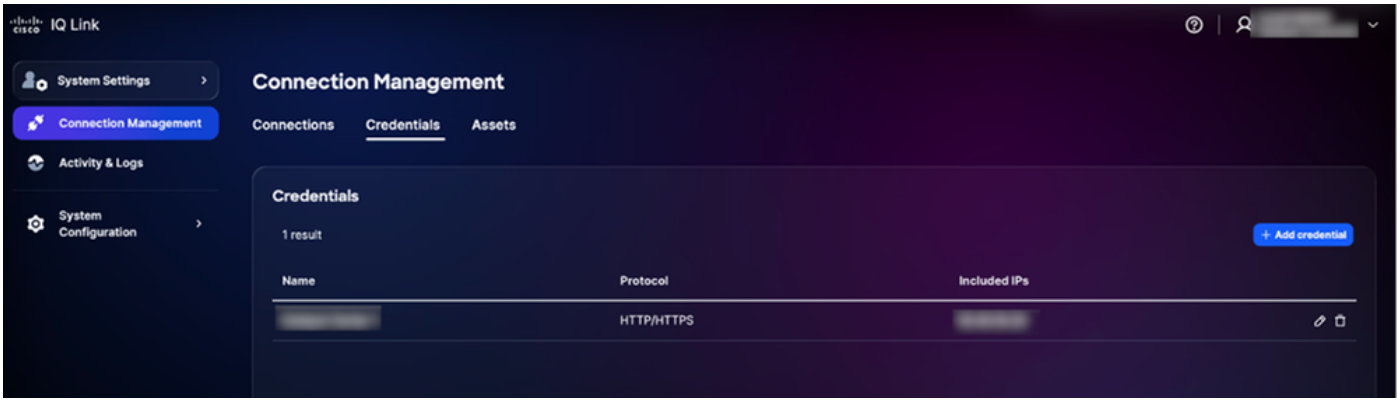


IP 주소 지정

9. 포함된 IP를 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.



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:우선 순위는 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.*(와일드카드 중 가장 높은 우선 순위)

    1.2.*

    1.*.*.*

    ..*.*(최저 우선순위)

  - 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 13: 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)

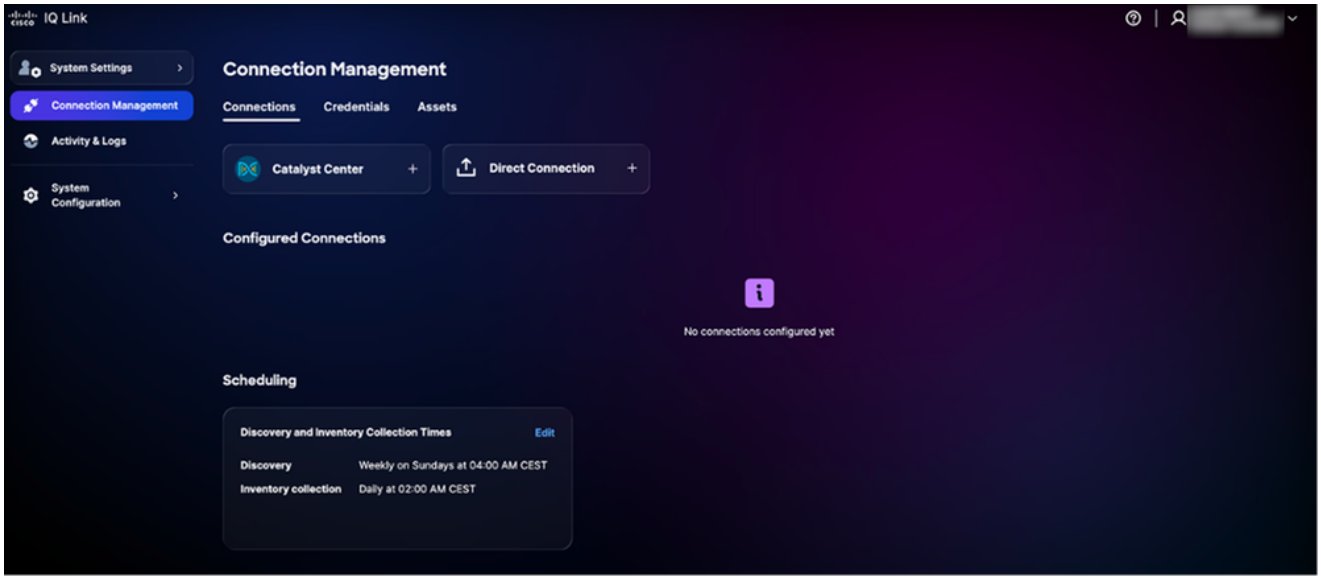
참고: 디바이스가 여러 개의 중복 카테고리에 속할 경우, 시스템은 항상 가장 높은 특이성(즉, 가장 적은 후행 와일드카드)을 갖는 크리덴셜 세트를 선택합니다.

Catalyst Center를 사용한 데이터 수집

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

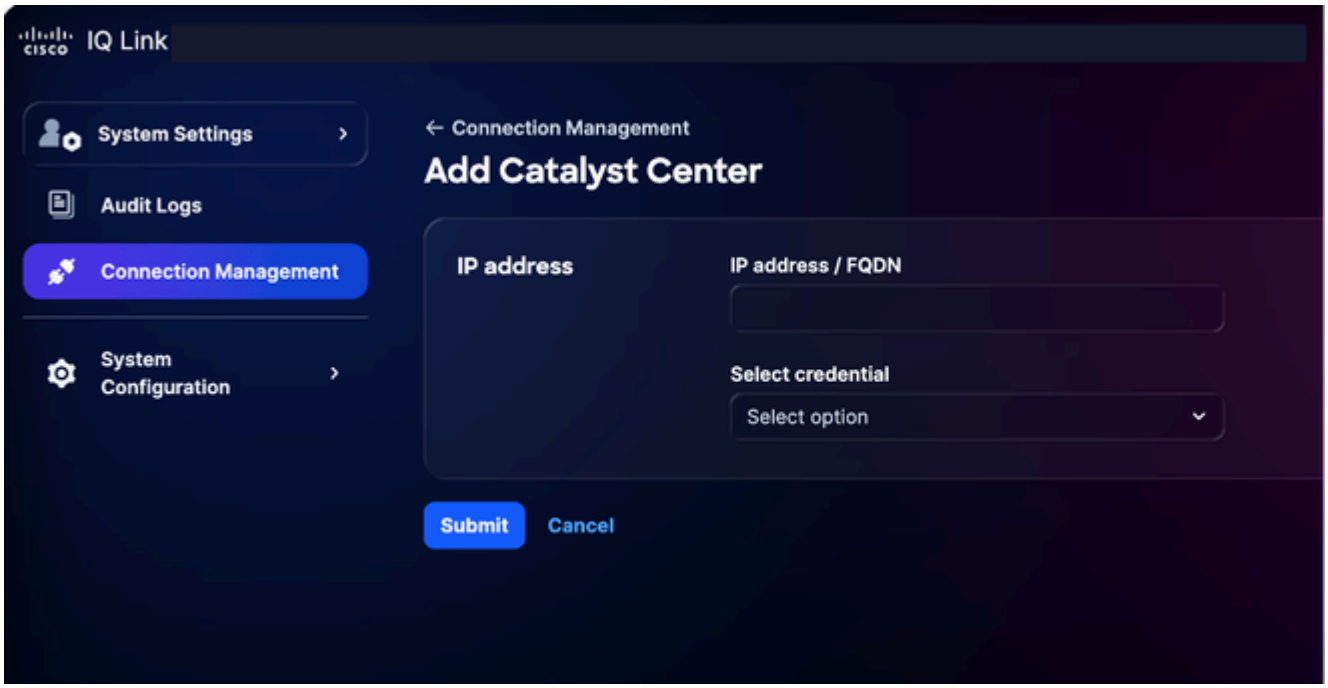
Catalyst Center를 사용한 데이터 수집:

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



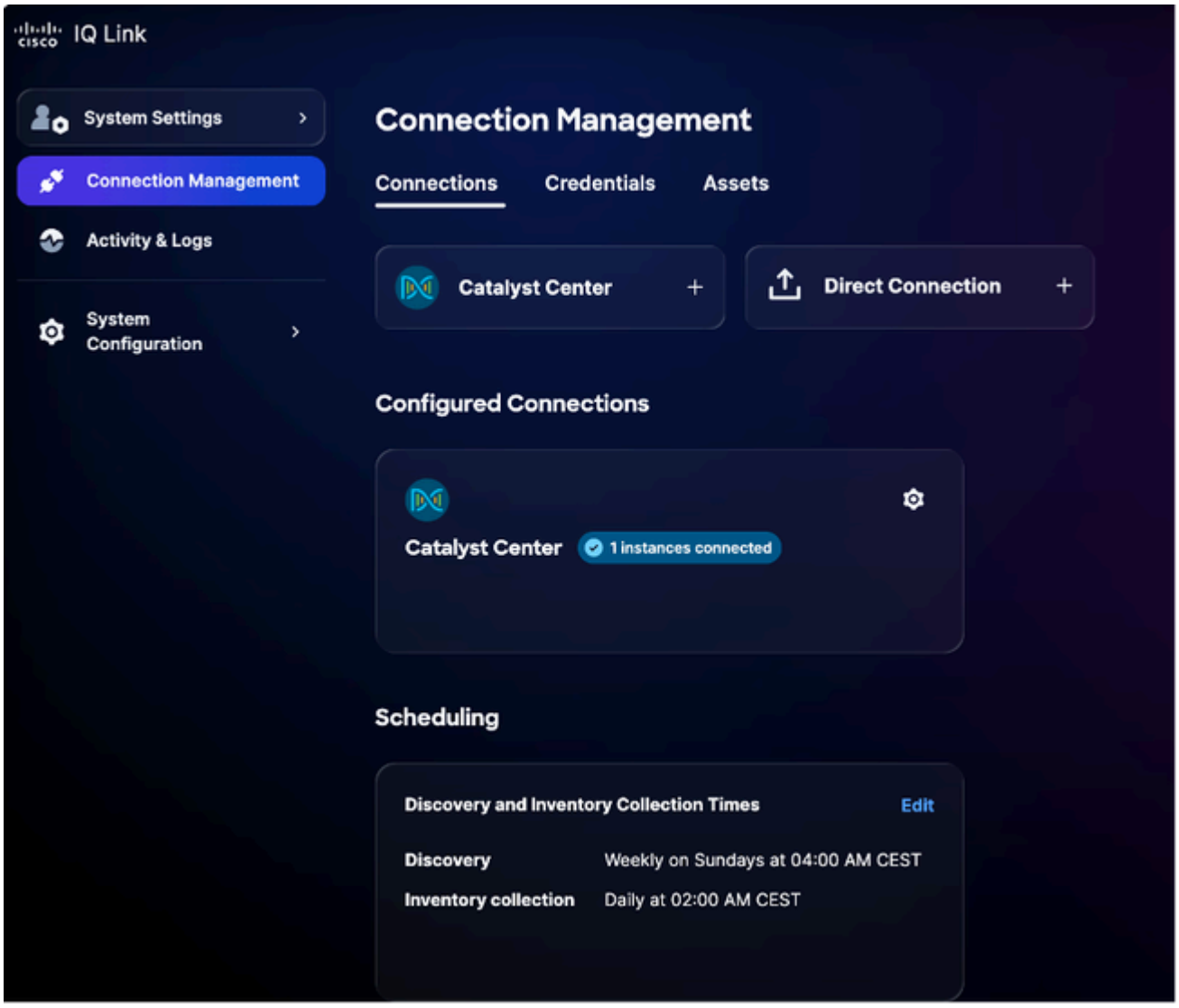
연결 관리

2. Catalyst Center 옵션을 클릭합니다.



Catalyst Center 추가

3. IP 주소 또는 FQDN을 입력합니다.
4. 드롭다운 목록에서 구성된 HTTP/HTTPS 자격 증명을 선택합니다.
5. Submit(제출)을 클릭합니다. 확인 메시지가 표시됩니다(최대 75분이 소요될 수 있음). Configured Connections 아래에서 새로 추가된 Catalyst Center를 볼 수 있습니다.



Catalyst Center가 추가되었습니다.

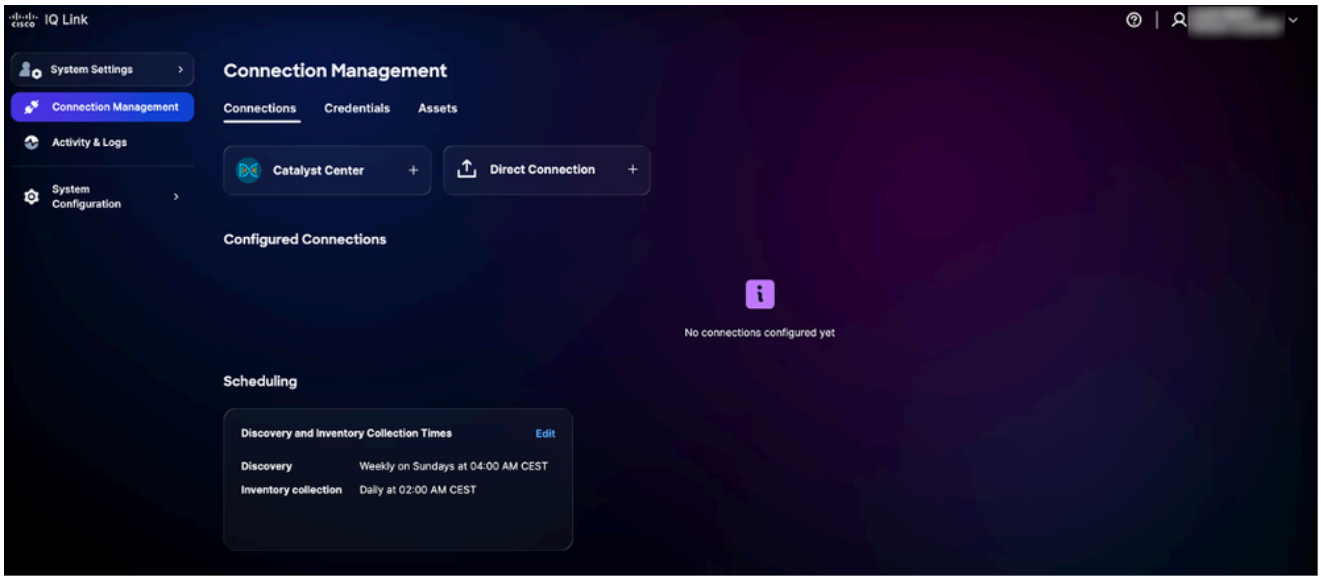
6. 수집을 예약합니다. 자세한 내용은 예약을 참조하십시오.

참고: Cisco IQ Link는 자동화된 스케줄링 설정으로 미리 구성되어 있으며 시스템은 기본 자동화된 수집 일정을 시작합니다. 조직의 요구 사항 및 유지 관리 기간에 맞게 일정을 수정하는 것이 좋습니다.

직접 연결

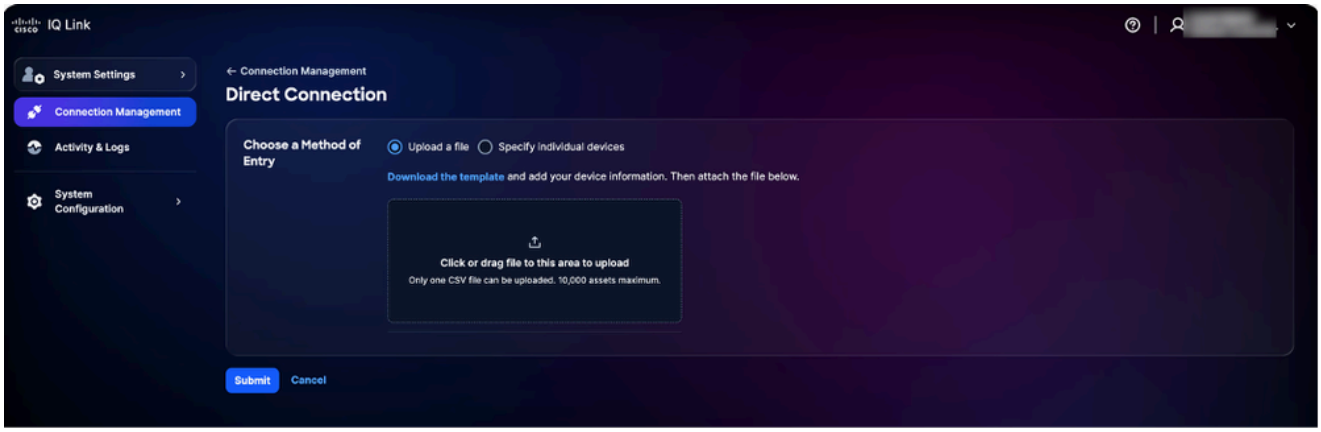
직접 연결을 위해 디바이스를 추가하려면

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



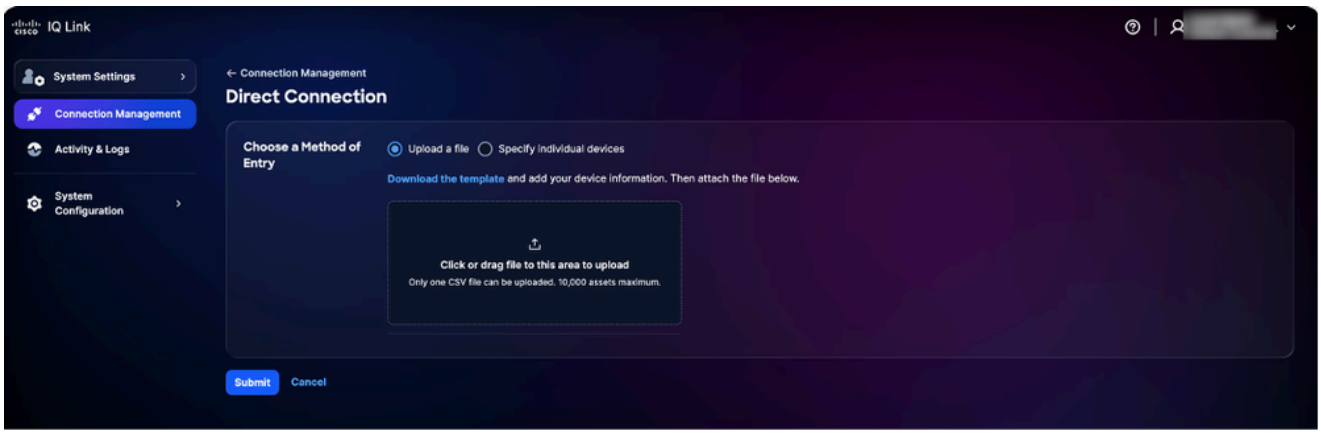
연결 관리

2. 직접 연결을 클릭합니다. 데이터를 수집하기 위한 두 가지 옵션이 포함된 직접 연결 페이지가 표시됩니다.



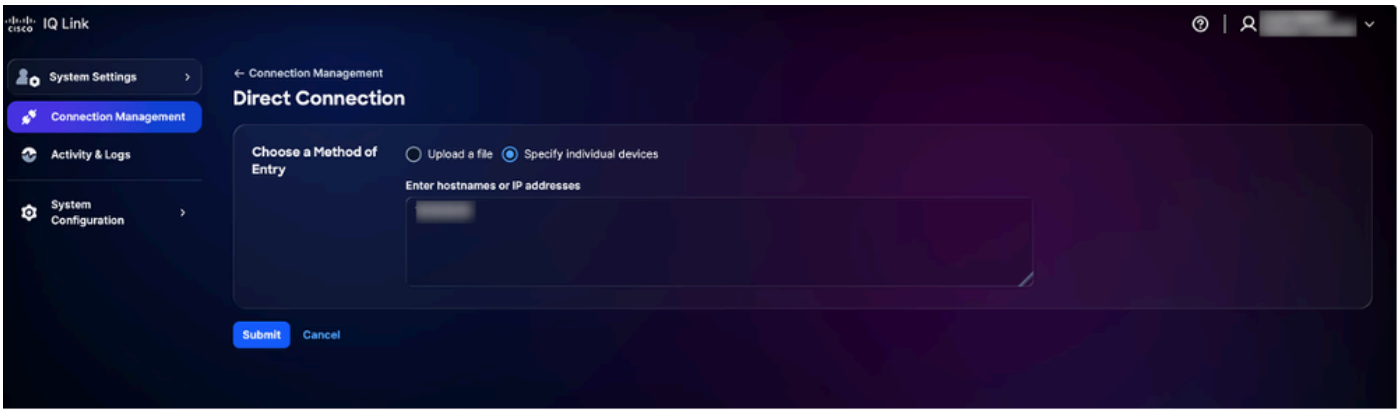
파일 업로드

3. Choose a Method of Entry(입력 방법 선택)에 대한 기본 옵션을 클릭하고 다음 방법 중 하나를 사용하여 디바이스를 제출합니다.



파일 업로드

- 파일 업로드: 파일을 클릭하거나 끌어서 놓고 Submit(제출)을 클릭합니다.



개별 디바이스 지정

- 개별 장치 지정: 단일 호스트 이름, IP 주소 또는 쉼표로 구분된 호스트 이름 및/또는 IP 주소 목록을 입력한 다음 Submit(제출)을 클릭합니다.

전송이 성공하면 Assets 탭으로 리디렉션됩니다.

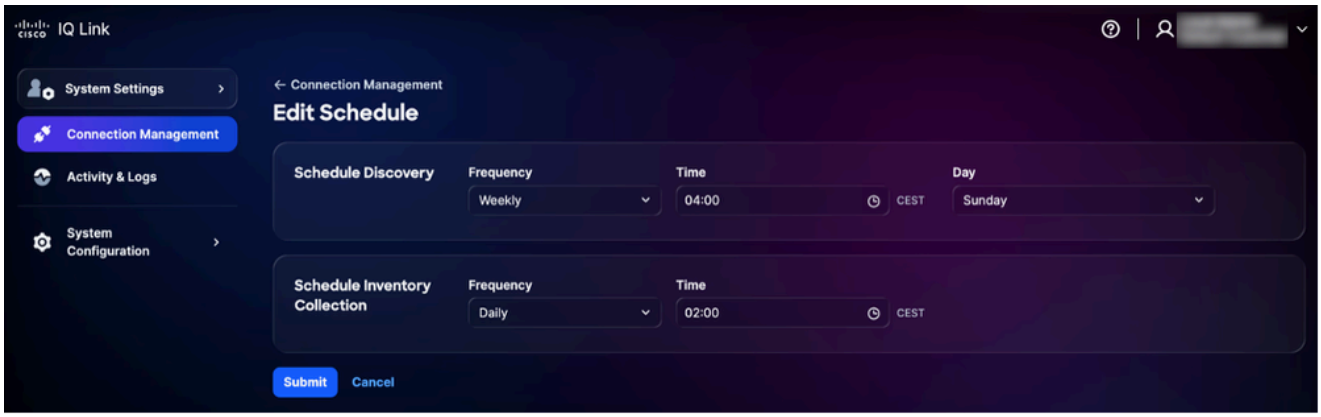
4. 수집을 스케줄링합니다. 자세한 내용은 예약을 참조하십시오.

참고: Cisco IQ Link는 자동화된 스케줄링 설정으로 미리 구성되어 있으며 시스템은 기본 자동화된 수집 일정을 시작합니다. 조직의 요구 사항 및 유지 관리 기간에 맞게 일정을 수정하는 것이 좋습니다.

예약

예약을 통해 Cisco IQ Link에서 자동화된 데이터 수집을 수행하는 시기를 정의할 수 있습니다. 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 Cisco IQ Link 내에서 정확하게 동기화되고 반영될 수 있도록 5~10분 정도 기다립니다.

배너

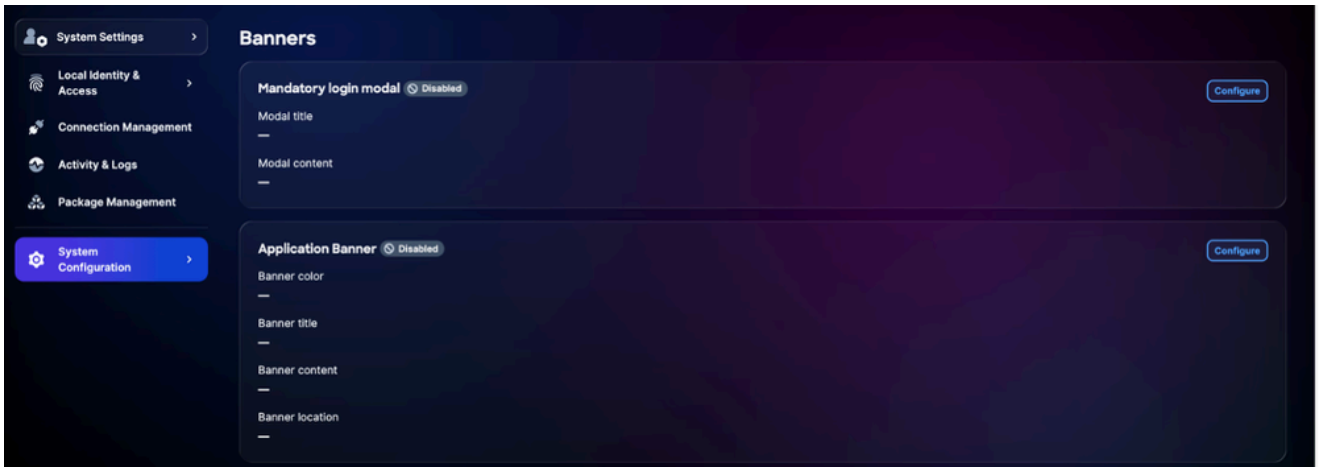
계정 관리자는 보안 및 규정 준수 표준을 충족하도록 시스템 전체 배너를 구성할 수 있습니다.

- 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

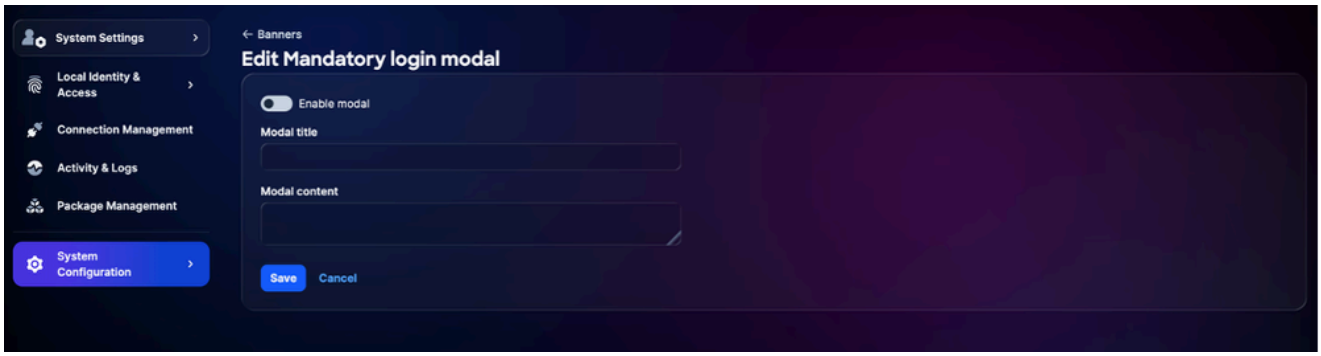
필수 배너를 구성하려면

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.



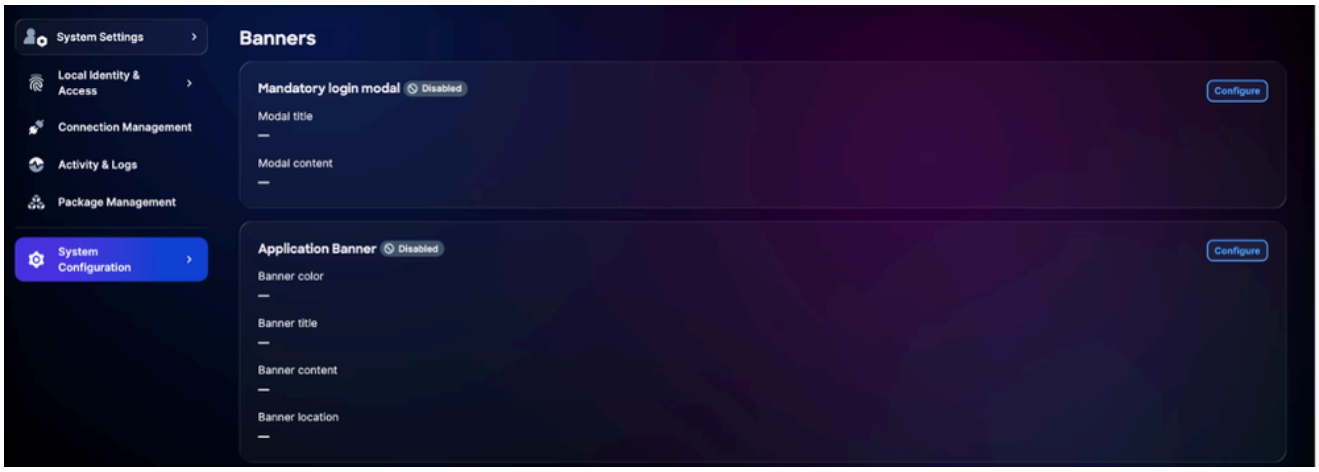
필수 로그인 모달 배너 편집

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

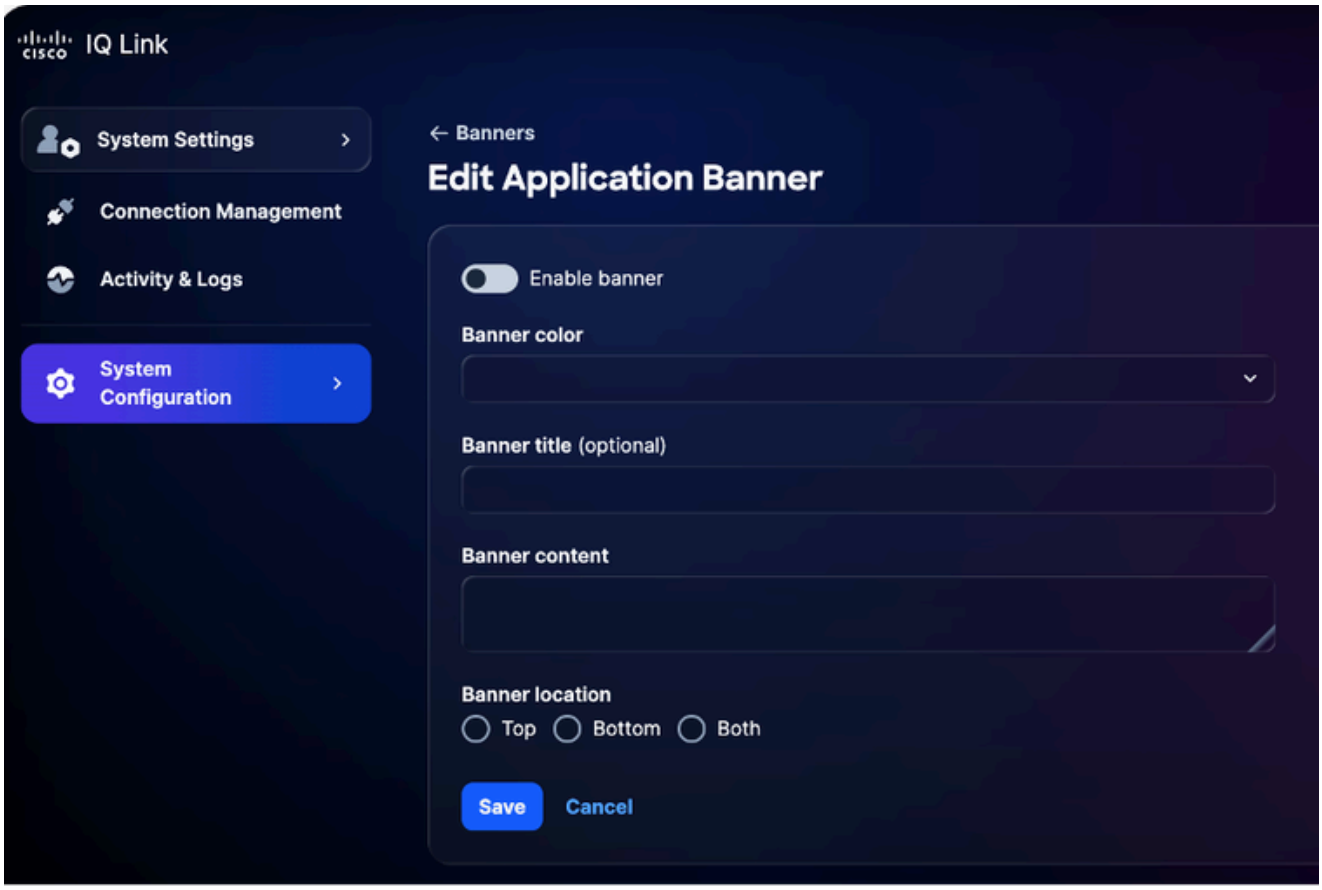
애플리케이션 배너를 구성하려면

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.

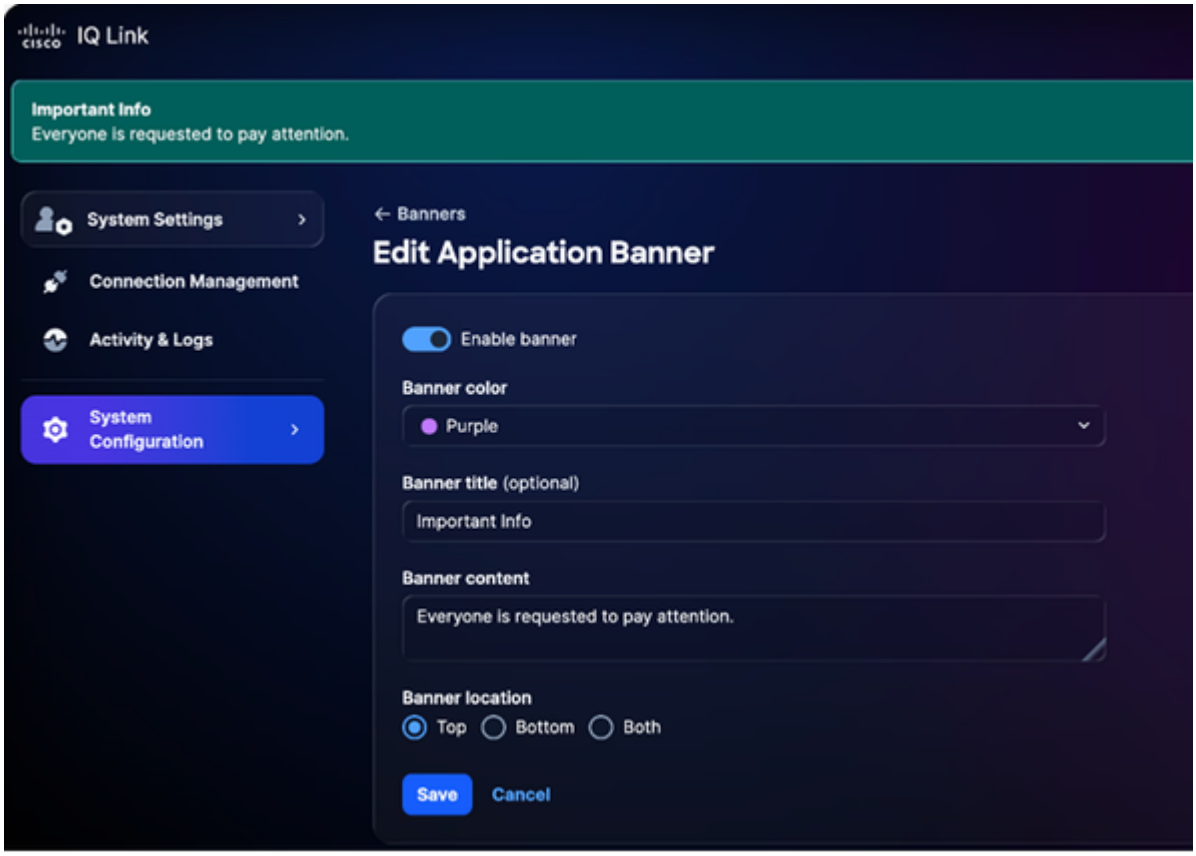
8. 저장을 클릭합니다. 배너가 애플리케이션 전체에 표시됩니다.

배너 수정

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

애플리케이션 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 중요한 컨텍스트를 제공하고 문제 해결을 지원할 수 있습니다.

진단 및 로그 파일을 수집하려면

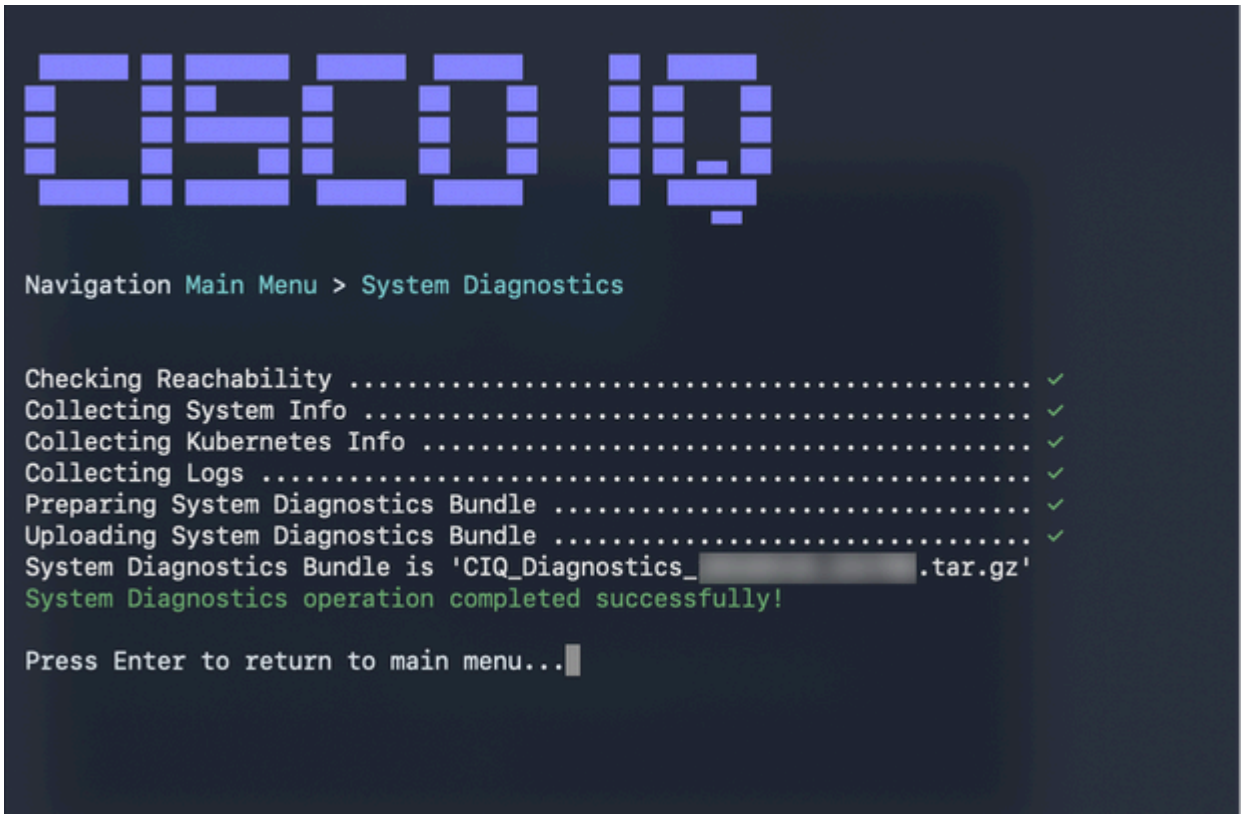
1. Cisco IQ에 로그인합니다.

주 메뉴

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

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.



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.

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.