Cisco IQ Link Operations Guide v1.1.1

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.

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

관리자는 다음 자격 증명을 사용하여 Cisco IQ 링크에 로그인해야 합니다.

- 기본 사용자 이름: admin
- 기본 암호: cisco IQ Link 설치 프로세스 중에 설정된 비밀번호 자세한 내용은 Cisco IQ Link 시작 가이드를 참조하십시오

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

로컬 관리자 보안 설정

시스템 구성의 로컬 관리자 보안 메뉴를 통해 비밀번호를 변경하고 보안 질문을 설정할 수 있습니다.

10분 내에 3회 시도에서 올바른 비밀번호를 입력하려고 합니다. 세 번의 시도가 모두 실패하면 보안을 위해 계정이 일시적으로 60분 동안 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."

60분 후에 계정이 자동으로 잠금 해제되며, 이 때 로그인 또는 비밀번호 재설정을 시도할 수 있습니

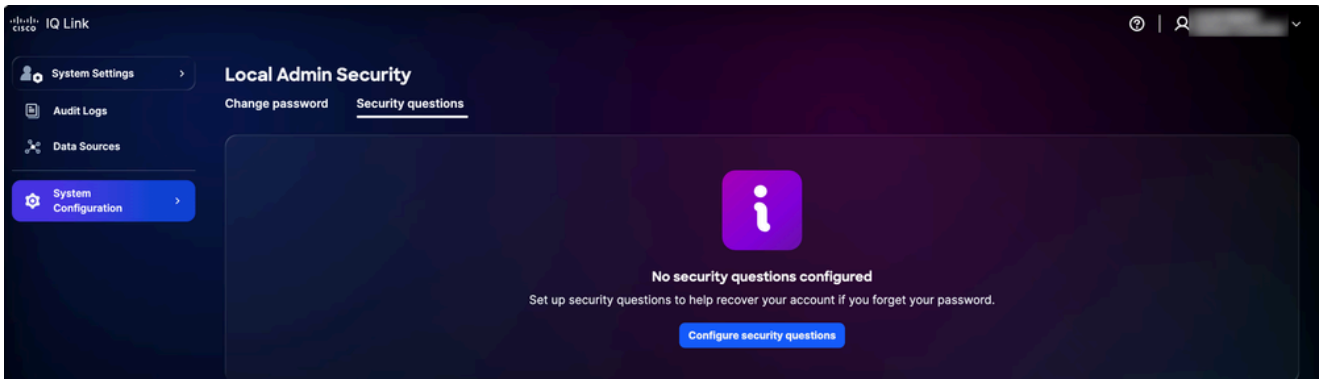
다.

보안 Q&A 설정

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

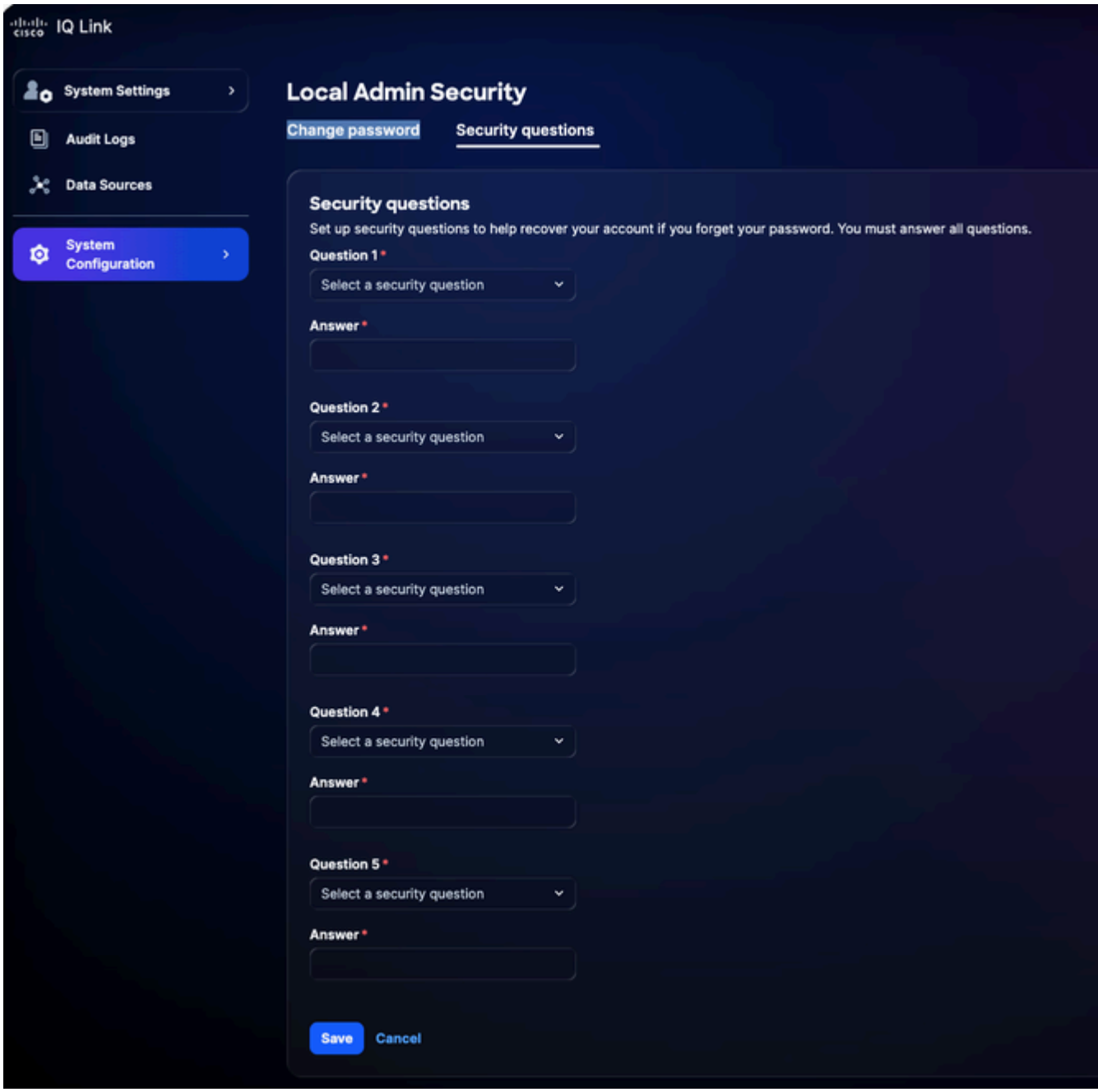
보안 질문을 설정하려면

1. System Settings(시스템 설정)에서 System Configuration(시스템 컨피그레이션) > Local Admin Security(로컬 관리자 보안) > Security Questions(보안 질문)를 선택합니다.



보안 질문

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



보안 질문

3. 드롭다운 목록에서 보안 질문 5개를 선택합니다.

4. 각 질문에 대한 응답을 입력합니다.

5. 저장을 클릭합니다.

참고:
· 답변은 대/소문자를 구분하지 않습니다. 예를 들어 "SMITH"와 "smith"는 동일한 것으로 간주됩니다.
· 추가 공백은 무시됩니다. 즉, "Smith"와 "Smith"는 동일하게 처리됩니다

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

로컬 관리자만 Cisco IQ의 비밀번호를 관리할 수 있습니다.

사전 요구 사항

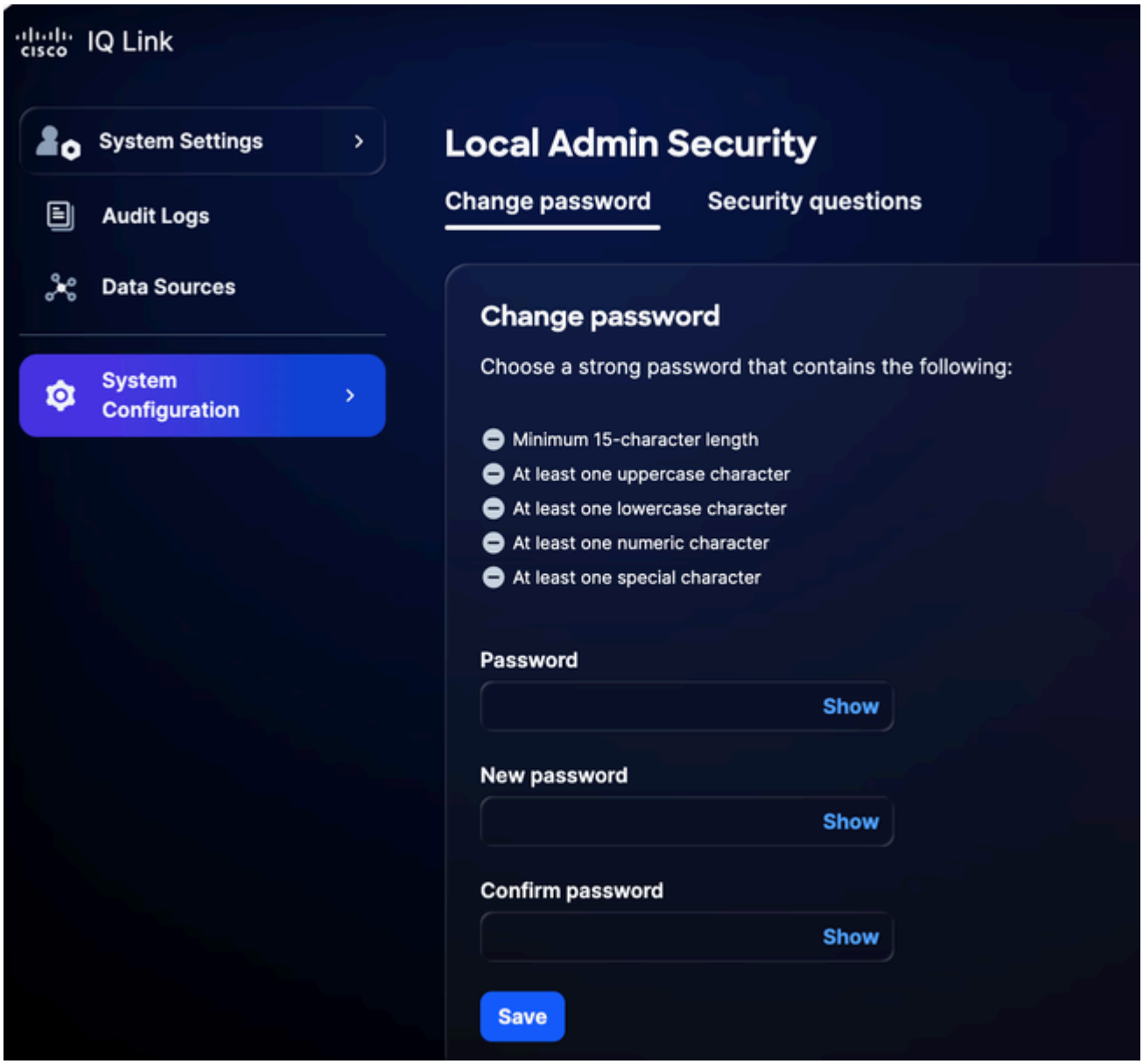
비밀번호를 관리하려면 다음 조건을 충족해야 합니다.

- 로컬 관리자
- 로컬 관리자 계정(SSO(Single Sign-On) 또는 외부 인증이 아님)을 사용하고 있습니다
- Cisco IQ에 로그인했습니다.
- 현재 비밀번호 확인

비밀번호 변경

비밀번호를 변경하려면

1. System Settings(시스템 설정)에서 System Configuration(시스템 컨피그레이션) > Local Admin Security(로컬 관리자 보안) > Change Password(비밀번호 변경)로 이동합니다.



암호 변경

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

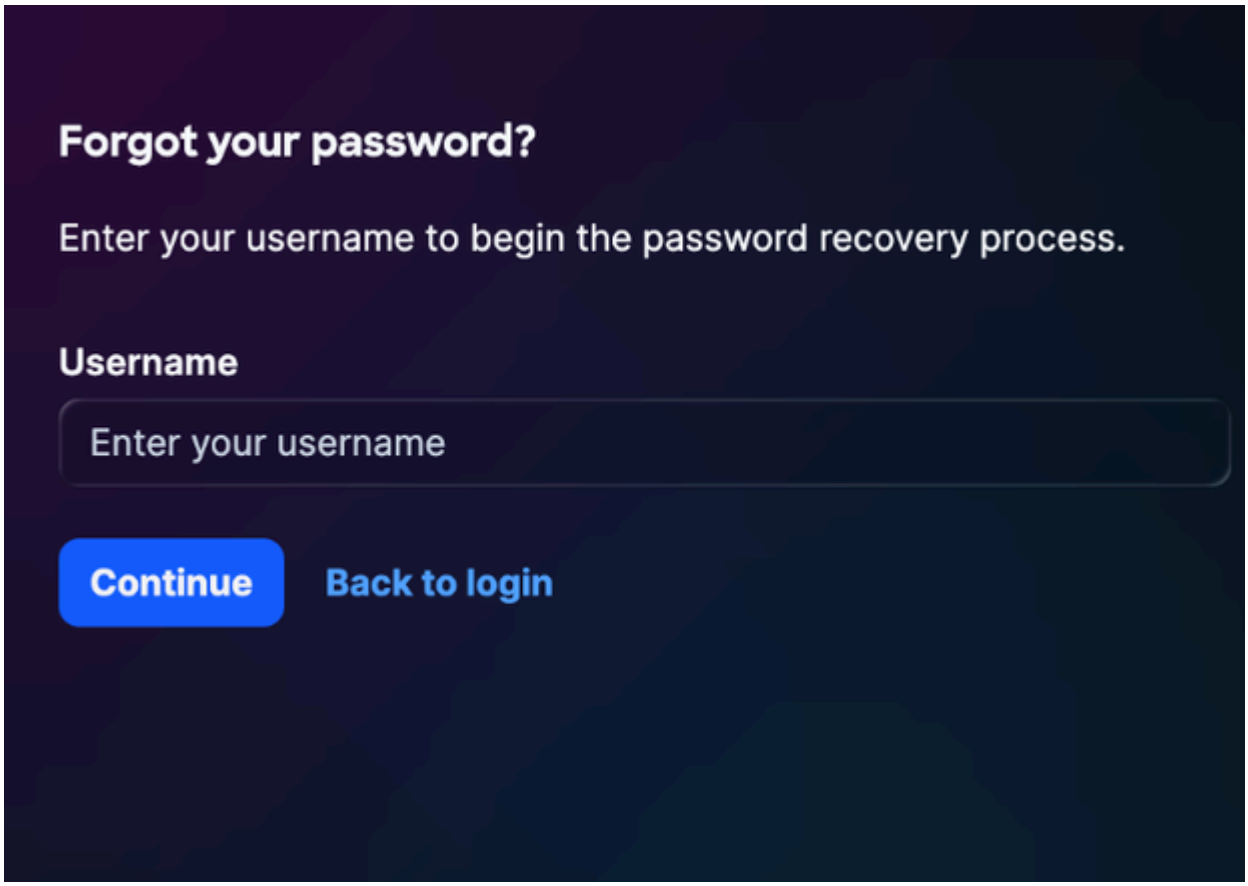
비밀번호는 Cisco IQ VM(Virtual Machine)을 비롯한 Cisco IQ 시스템에서 업데이트됩니다.

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.

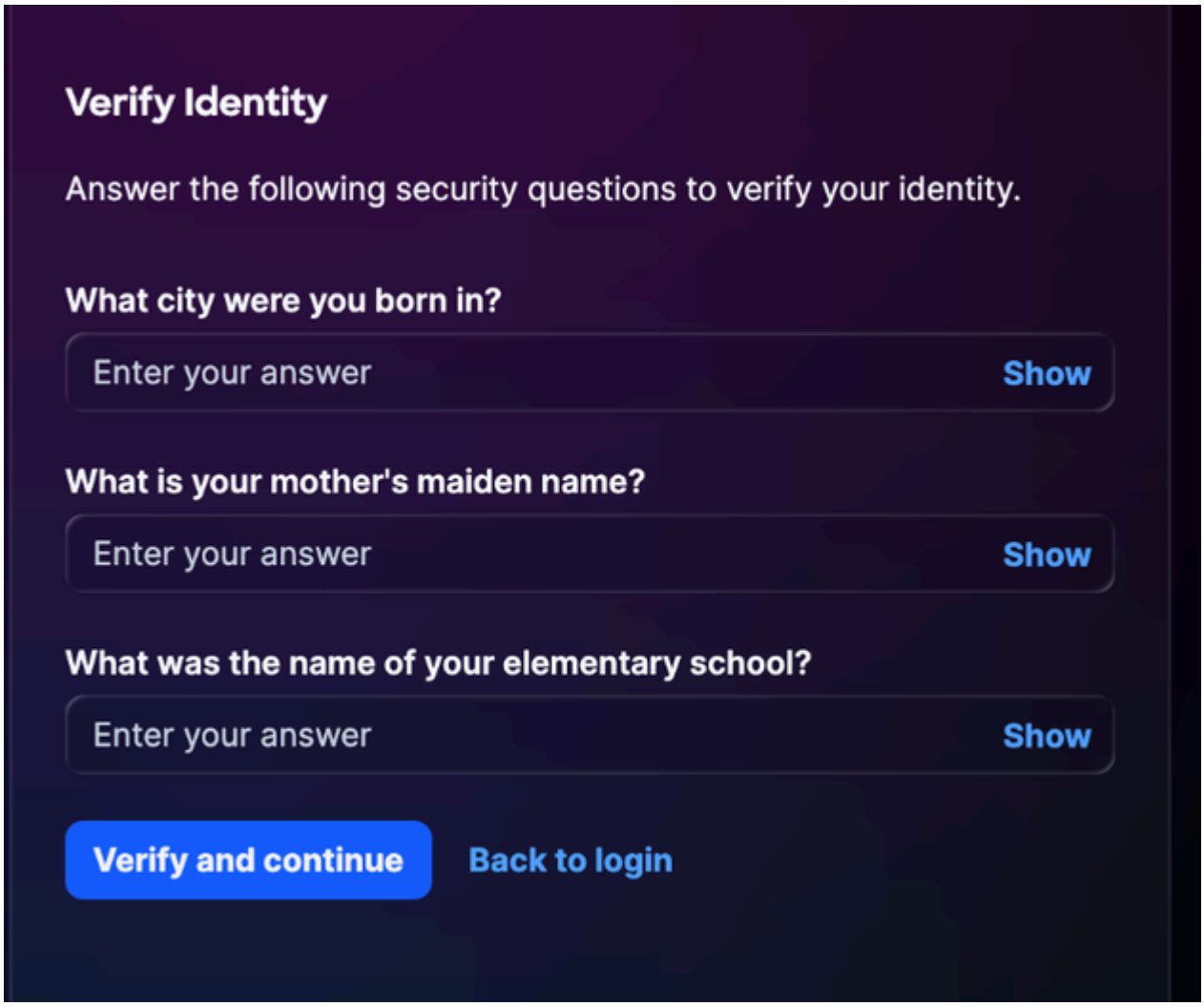
잊어버린 비밀번호를 재설정하려면

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



비밀번호 분실

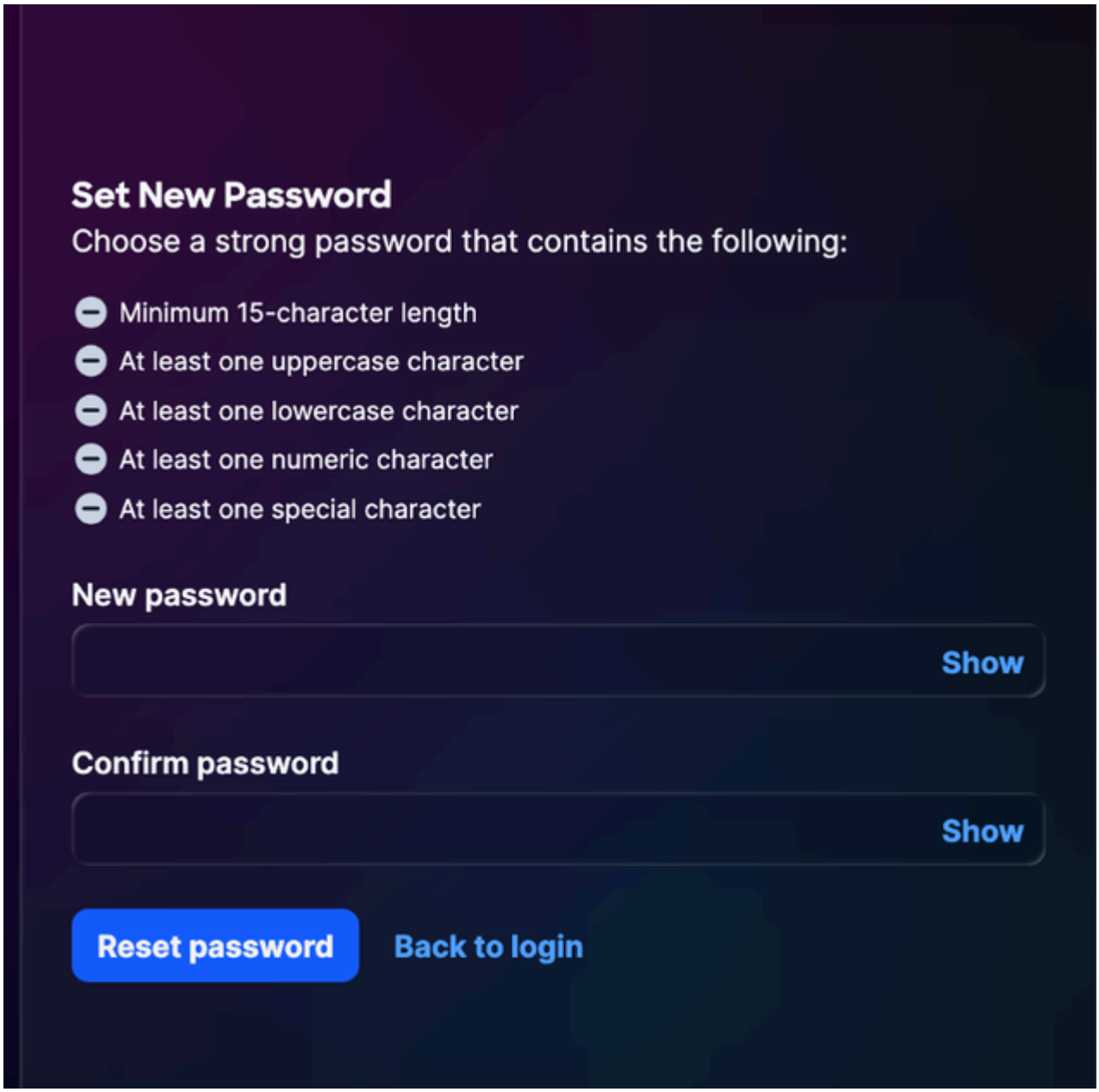
3. 사용자 이름을 입력합니다.
4. Continue(계속)를 클릭합니다. Verify Identity(ID 확인) 페이지에는 이전에 구성된 5개 질문 중 3개의 임의 보안 질문이 표시됩니다.



ID 확인

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

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



비밀번호 재설정

참고:
· 10분 이내에 보안 질문에 대한 답을 세 번 정확히 제시해야 합니다. 세 번의 시도가 모두 실패하면 보안을 위해 계정이 일시적으로 60분 동안 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."
· 60분 후에 계정이 자동으로 잠금 해제되며, 이 시점에서 로그인 또는 비밀번호 재설정을 시도할 수 있습니다.

---

7. 새 비밀번호를 입력합니다.

8. 비밀번호를 다시 입력하여 확인합니다.

9. Submit(제출)을 클릭합니다.

ID 공급자 구성

Cisco IQ Link에 로그인한 관리자는 다양한 설정을 구성할 수 있습니다. 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 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 특성을 설정합니다.

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

필드	가치
온보딩 범주	"New Onboarding(새 온보딩)"을 선택합니다.

SAML 컨피그레이션 매개변수

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

3. 다음 필수 특성 명령문을 구성합니다.

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

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

4. 애플리케이션에서 SLO(Single Logout) 설정을 구성합니다.

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

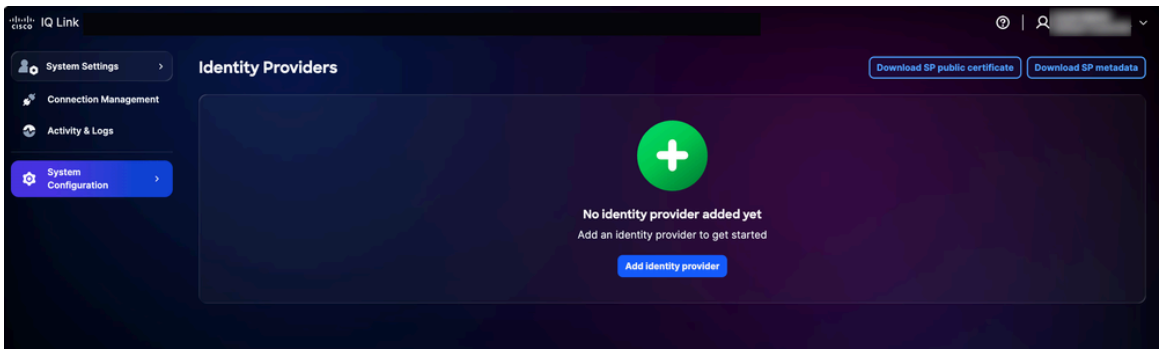
5. "SP 메타데이터" 파일을 다운로드하려면 다운로드 아이콘을 클릭합니다.

6. 공급자가 요구하는 대로 애플리케이션을 프로비저닝하거나 생성합니다.

IDP 추가

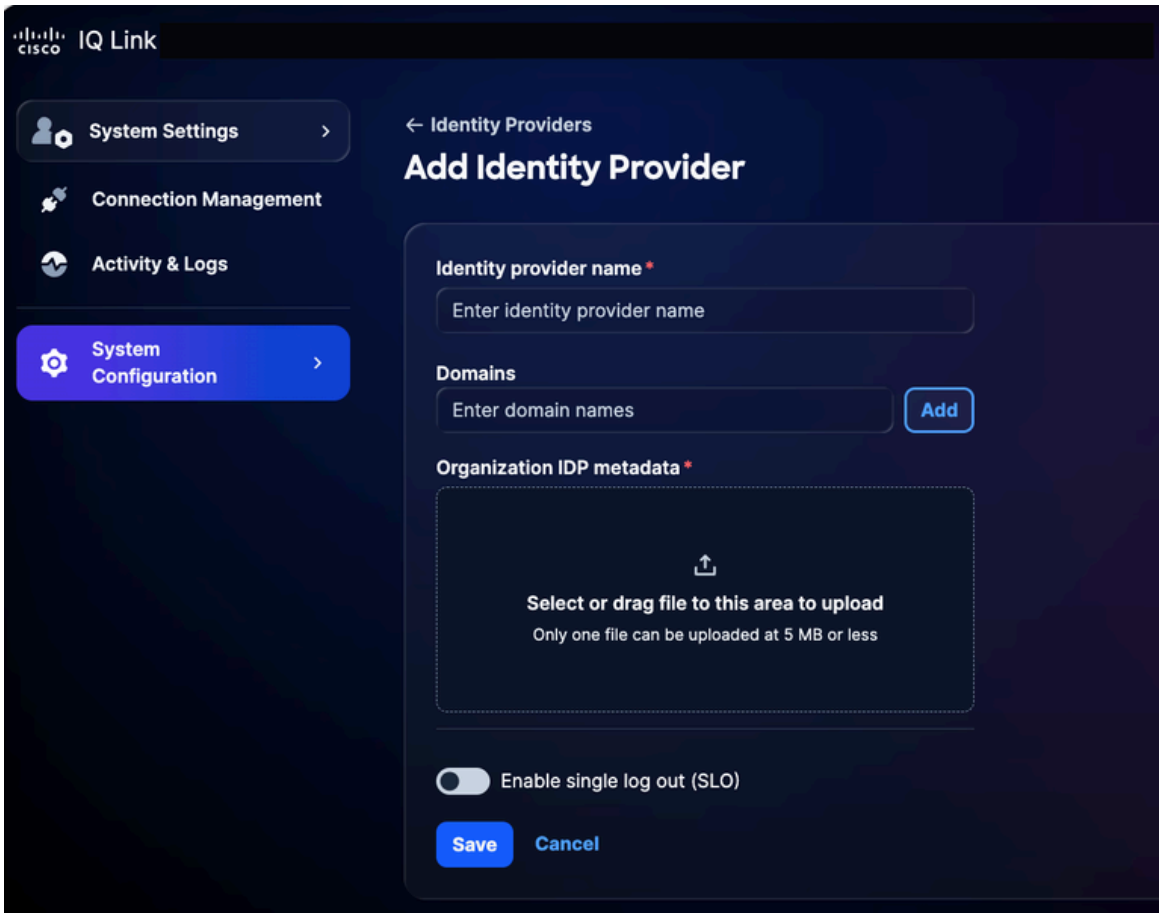
Cisco IQ Link에서 IDP를 추가하려면

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



IDP 홈 페이지

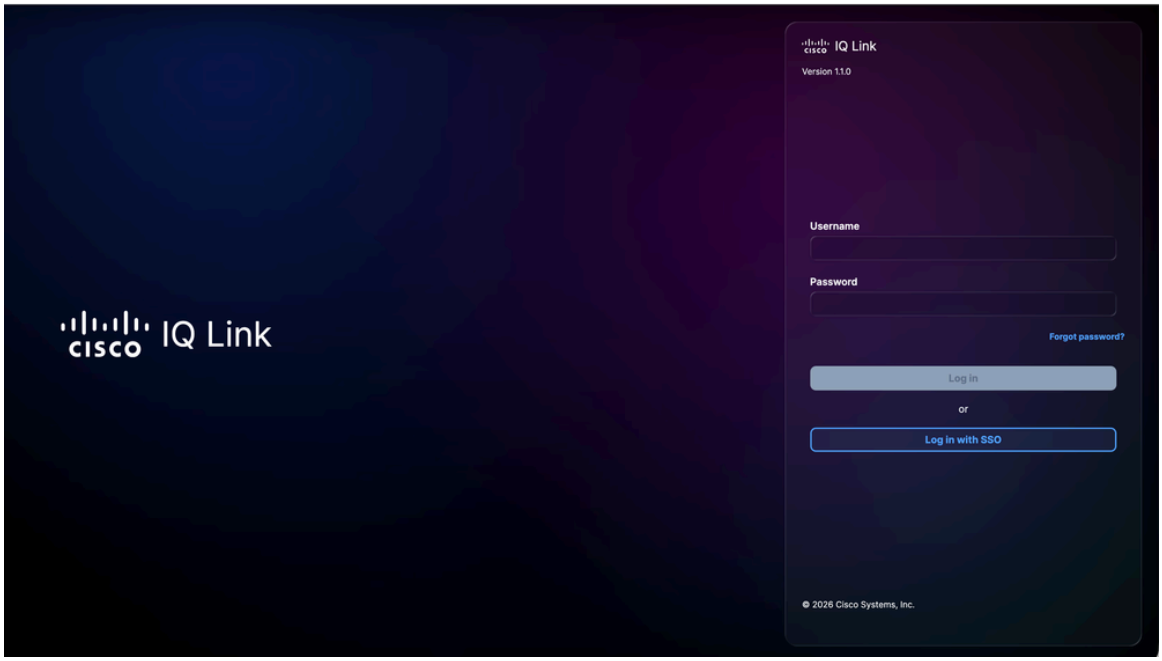
2. Add Identity Provider를 클릭합니다. Add Identity Provider 페이지가 표시됩니다.



ID 공급자 추가

참고: 지정된 시간에 하나의 IDP만 추가할 수 있습니다.

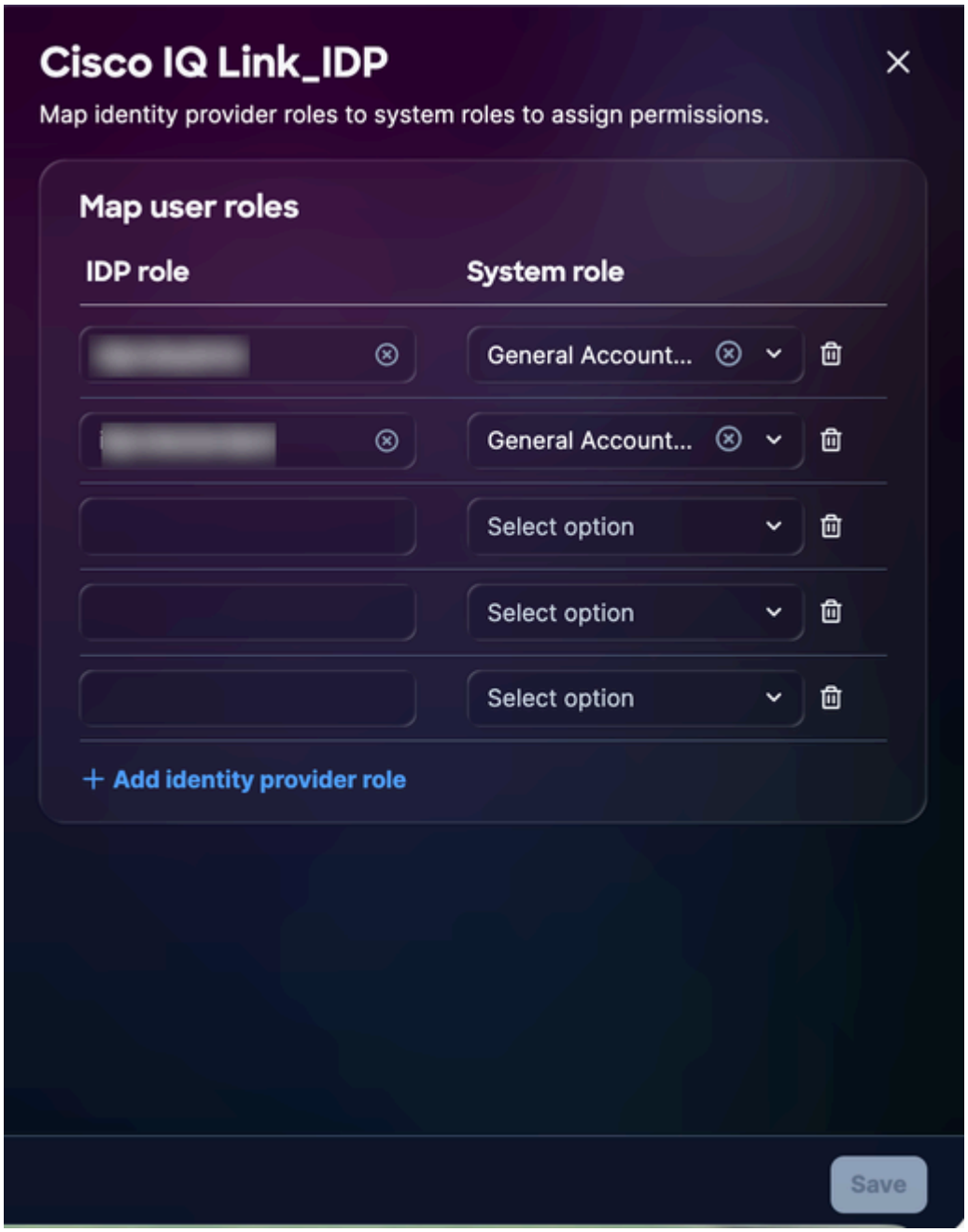
3. ID 공급자 이름을 입력합니다.
4. Add(추가)를 클릭하여 Cisco IQ Link에서 구성한 도메인 이름을 Domains(도메인) 필드에 추가합니다.
5. IDP 애플리케이션에서 얻은 SAML 메타데이터 파일을 Organization IDP metadata(조직 IDP 메타데이터) 필드에 끌어 놓거나 업로드하는 방법입니다. 이 파일에는 인증서 세부 정보 및 서비스 공급자(SP) 엔터티 세부 정보가 포함되어 있습니다.
6. (선택 사항) Enable single logout(단일 로그아웃 활성화) 토글 버튼을 켭니다. 나중에 SLO를 활성화할 수도 있습니다.
7. 저장을 클릭합니다.
8. 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.

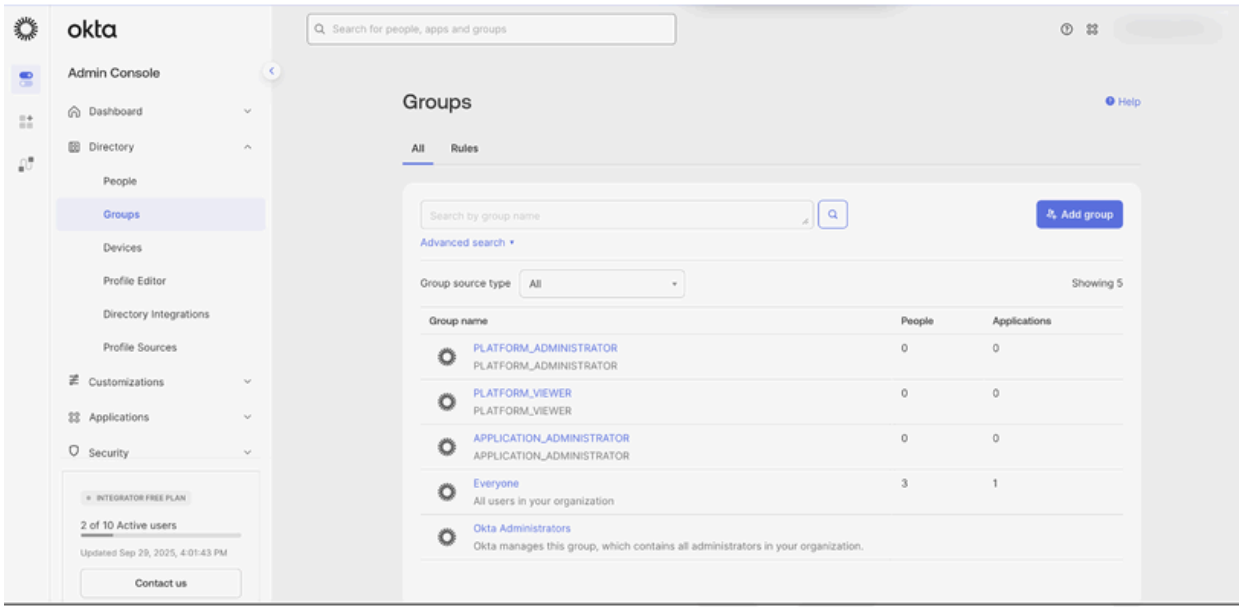


사용자 역할 매핑

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

    - general_account_administrator: 일반 계정 관리자는 제품의 모든 작업을 수행할 수 있는 모든 권한을 가집니다
    - general_account_viewer: 일반 계정 뷰어에는 읽기 전용 액세스 권한이 있습니다.

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



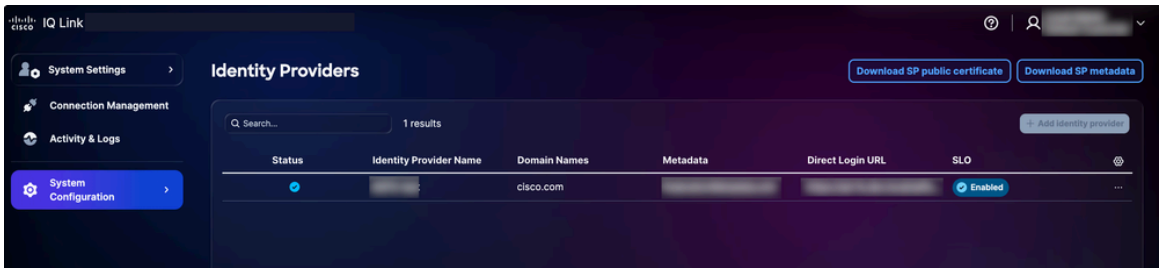
역할 매핑 참조

3. Add ID provider role(ID 제공자 역할 추가)을 클릭하여 필요에 따라 추가 역할을 매핑합니다.
4. 저장을 클릭합니다.

단일 로그아웃 컨피그레이션

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

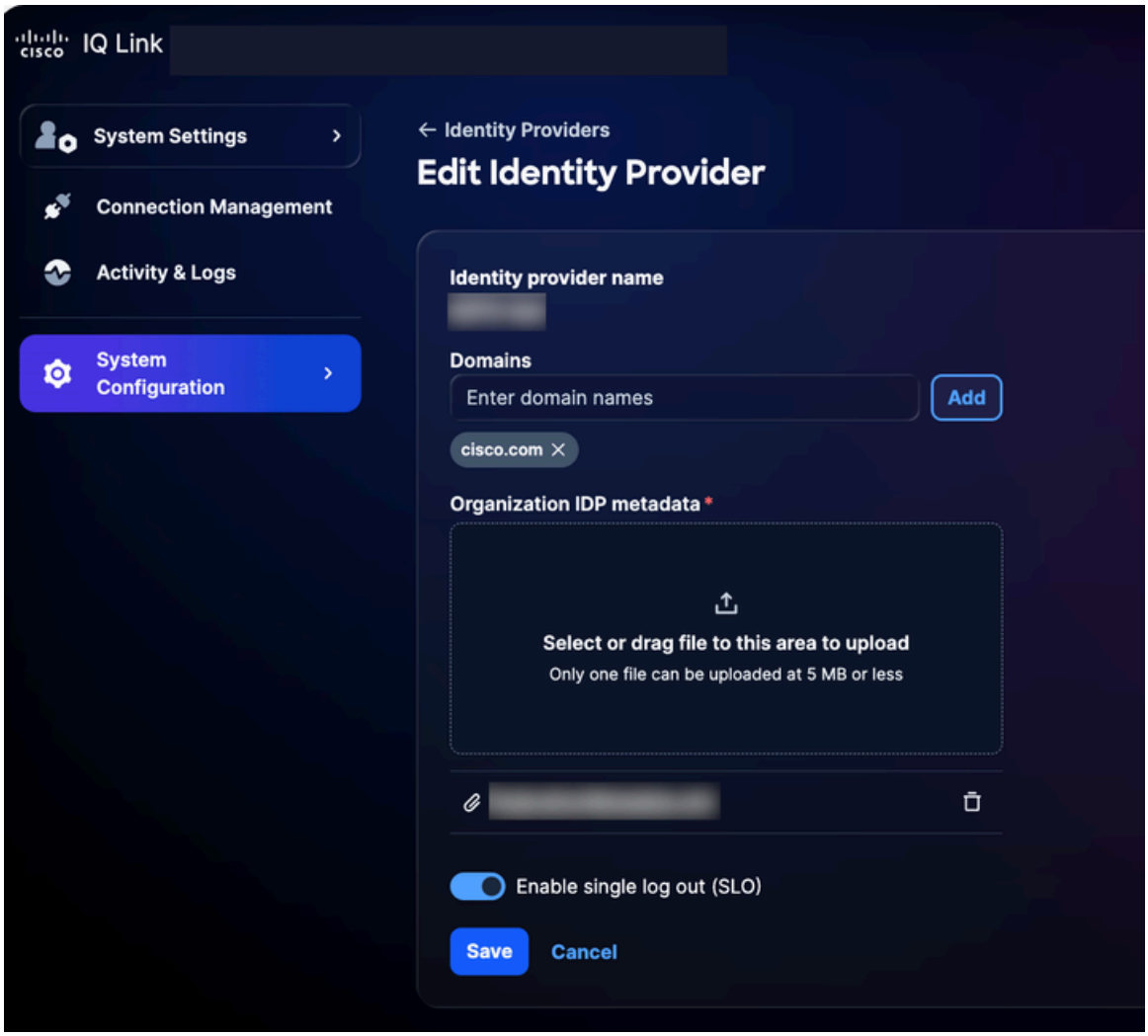
1. Identity Providers(ID 제공자) 페이지에서 Download SP public certificate(SP 공용 인증서 다운로드)를 클릭합니다.



공용 인증서 다운로드

2. 다운로드 파일을 sp-public-key.crt로 저장합니다.
3. IDP 포털로 이동합니다.
4. IDP SAML Configuration for SSO(SSO에 대한 IDP SAML 컨피그레이션) 섹션에서 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 메타 데이터 파일을 업로드합니다.
9. 다음 체크리스트를 사용하여 SSO 및 SLO 기능을 확인합니다.

확인 체크리스트:

- 로컬 관리자 로그인에 성공했습니다.
- 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.

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 ADFS(Active Directory 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 Active Directory 통합

- AD FS의 SSL/TLS 인증서
- Cisco IQ에 대한 관리자 액세스
- ADFS 서버(Windows Server)에 대한 관리 액세스
- AD FS 서버의 PowerShell 액세스
- AD FS와 Cisco IQ 간의 네트워크 연결
- AD FS 서버 컨피그레이션 세부 정보(아래 표 참조)

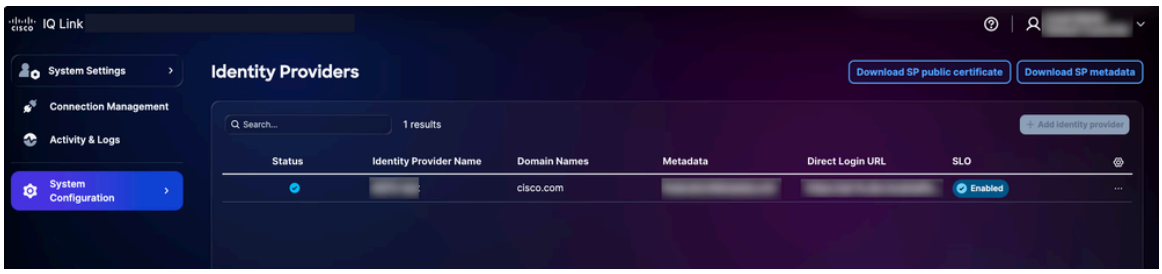
ADFS 서버 컨피그레이션

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	Active Directory 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 가져오기를 클릭합니다.
10. Browse(찾아보기)를 클릭하여 통신 사업자 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.

ADFS 클레임 규칙 구성

ADFS 클레임 규칙을 구성하려면 다음 섹션에 나열된 단계를 수행합니다.

필수 클레임

필요한 클레임은 다음 표를 참조하십시오.

필수 클레임

클레임	목적	소스
Email	사용자 식별자	AD 메일

클레임	목적	소스
표시 이름	사용자의 전체 이름	AD 표시 이름
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 A
=> issue(store = “Active Directory”, types = (“http://schemas.xmlsoap.org/ws/2005/05/identity/claims/ema

@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.Issu

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

3. 다음 명령을 실행하여 클레임 규칙을 적용합니다.

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

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 AD FS가 표준 신뢰 체인을 통해 검증할 수 없는 내부 인증 기관에서 발급합니다.

- 이 신뢰 당사자에 대해 전역적으로 체인 유효성 검사 사용 안 함

```
Set-AdfsRelyingPartyTrust `
    -TargetIdentifier “
     ” `
    -SigningCertificateRevocationCheck None `
    -EncryptionCertificateRevocationCheck None
```

또는

- 발급하는 CA 인증서를 신뢰할 수 있는 루트 인증 기관 저장소로 가져옵니다.

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

3. ADFS 서비스를 다시 시작하여 변경 사항을 적용합니다.

```
Restart-Service adfssrv
```

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.

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 Active Directory에서 매핑에 사용할 그룹을 찾을 수 있는지 확인합니다. Active Directory에서 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”] }
```

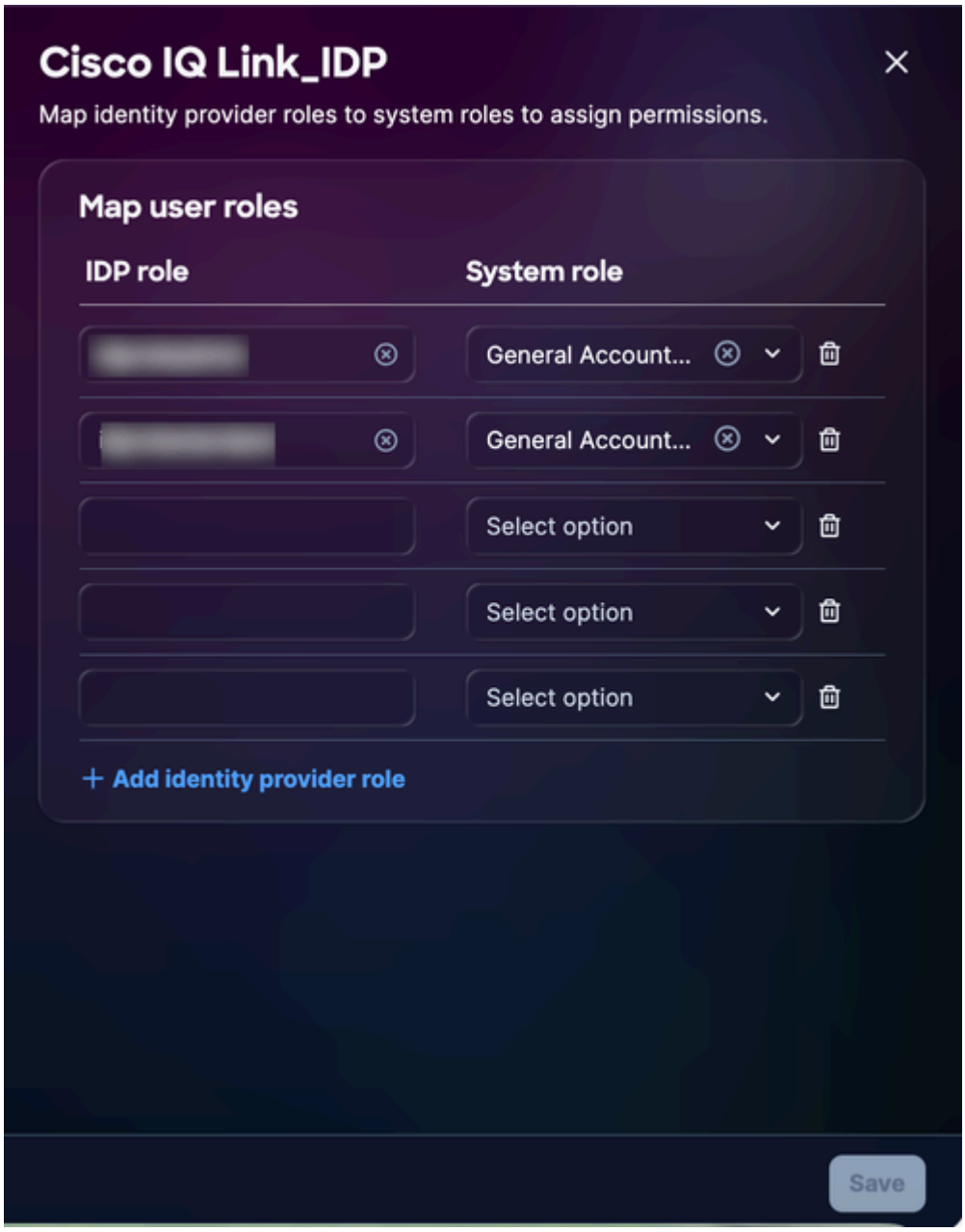
시스템은 LDAP를 통해 직접 Active Directory를 쿼리하므로 추가 모듈이 필요 없습니다. 그룹 정보는 전체 DN(Distinguished Name) 형식으로 반환됩니다. 예:

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 않은 경우 관리자가 Active Directory에서 만들어야 AD FS 역할 매핑을 완료할 수 있습니다.

역할 매핑을 구성하려면

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 입력하십시오. 지원되는 시스템 역할은 다음과 같습니다.

    - general_account_administrator: 일반 계정 관리자는 제품의 모든 작업을 수행할 수 있는 모든 권한을 가집니다. IDP 역할(구문 분석된 이름)은 CXIQ Admins입니다.
    - general_account__viewer: 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.

검증 및 테스트

인증 테스트

1. Incognito 또는 Private 모드 브라우저에서 https://your-cisco-iq-domain.com/login으로 이동합니다.
2. domain\username 또는 user@domain.local 형식의 Active Directory 자격 증명을 사용하여 로그인합니다.
3. 인증 성공 후에 Cisco IQ 홈 페이지로 리디렉션되는지 확인합니다.
4. 할당된 역할이 사용자 프로필에 올바른 구문 분석된 그룹 이름(예: CXIQ Developers)을 표시하는지 확인합니다.

로그아웃 테스트

로그아웃을 테스트하려면 Cisco IQ에서 로그아웃을 클릭합니다. "Logging out, please wait..." 메시지가 표시되고 Cisco IQ 로그인 페이지로 리디렉션됩니다. 시스템은 AD FS 세션도 종료합니다. AD FS에 직접 액세스하려고 하면 다시 로그인하라는 메시지가 표시됩니다.

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.

AD FS 문제

문제	증상/설명	원인/검사/해결 방법 및 수정
추출되지 않은 그룹	로그인 후 역할 없음	● 클레임 규칙: AD FS 클레임 규칙 구성의 지침을 다시 실행합니다 ● 그룹 특성: http://schemas.xmlsoap.org/claims/Group이어야 합니다. ● 사용자가 AD 그룹에 없습니다.

문제	증상/설명	원인/검사/해결 방법 및 수정
암호 해독 실패	로그에서 "어설션 해독 실패"	AD FS 인증서 컨피그레이션에 대한 컨피그레이션 확인
로그인 루프	인증 또는 로그인 루프에 고착	● 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.

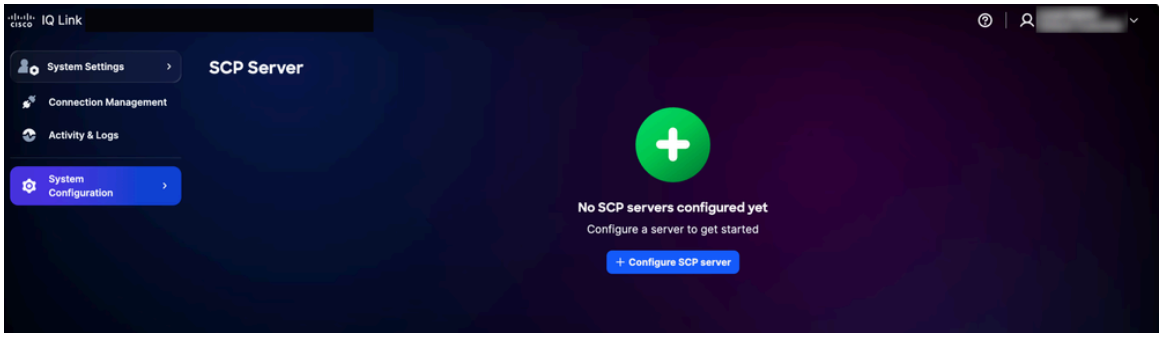
```
Get-AdfsRelyingPartyTrust -Name “Cisco IQ - Stage” | Select-Object SamlEndpoints
```

SCP 서버 추가

이 SCP(Secure Copy Protocol) 서버는 Cisco IQ 설치를 추가, 업그레이드 또는 수정하는 데 필수적인 업그레이드 파일을 가져오기 위한 필수 구성 요소입니다.

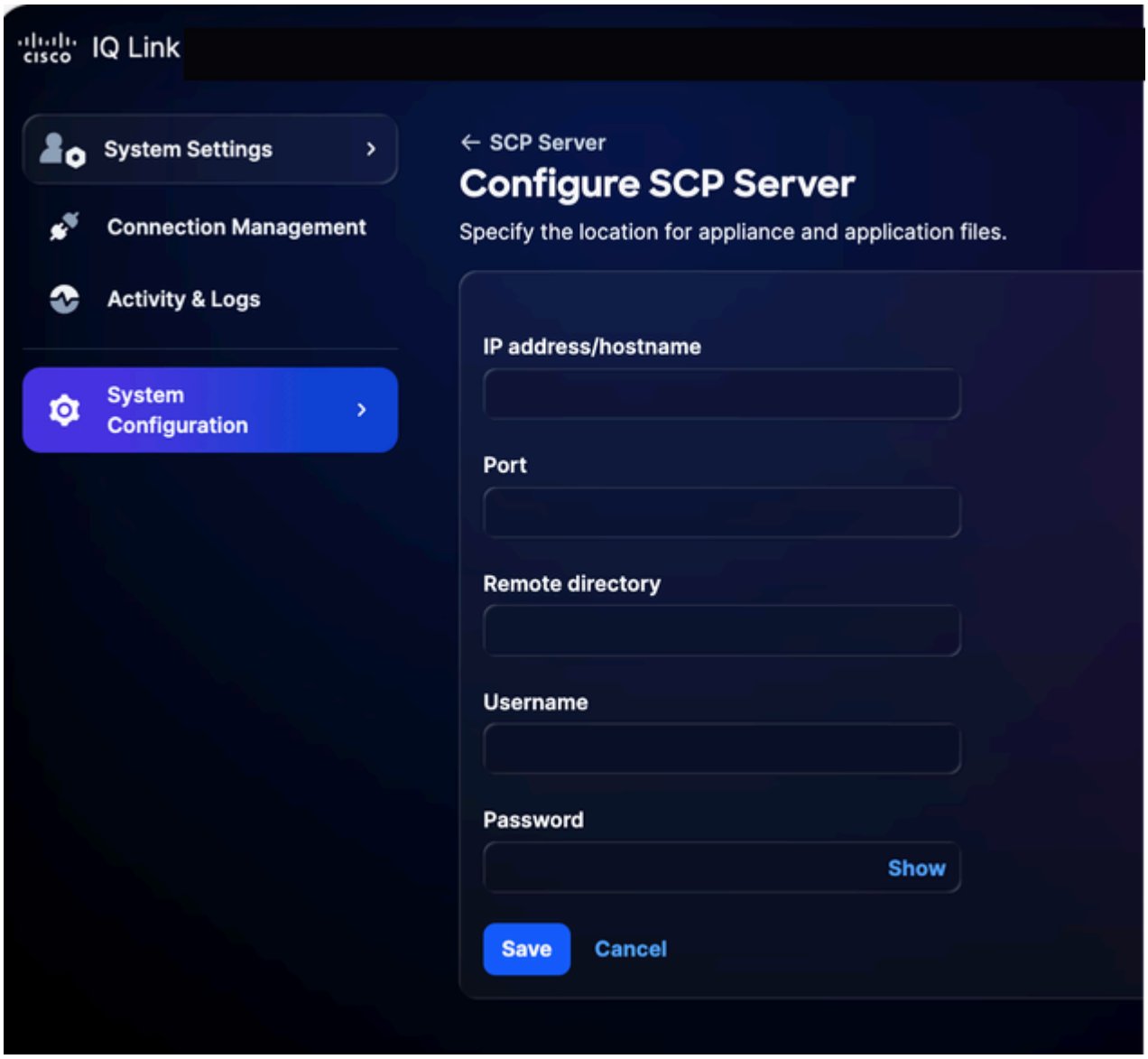
SCP 서버를 추가하려면

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



SCP 서버 홈 페이지

2. Configure SCP Server(SCP 서버 구성)를 클릭합니다.



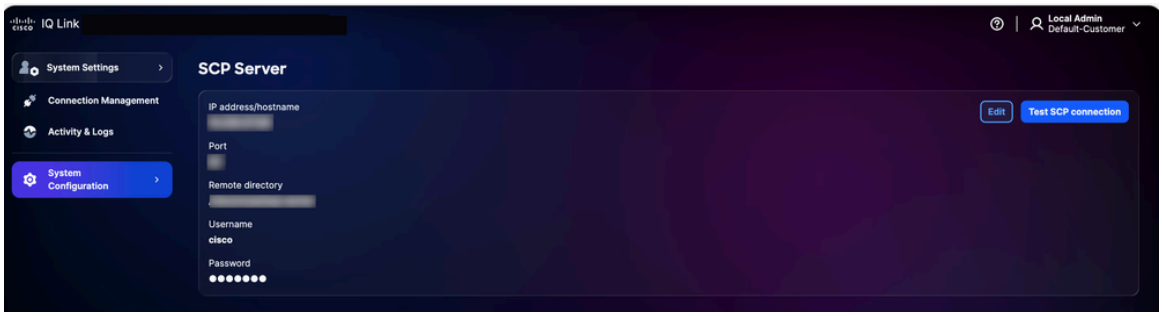
SCP 서버 구성

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

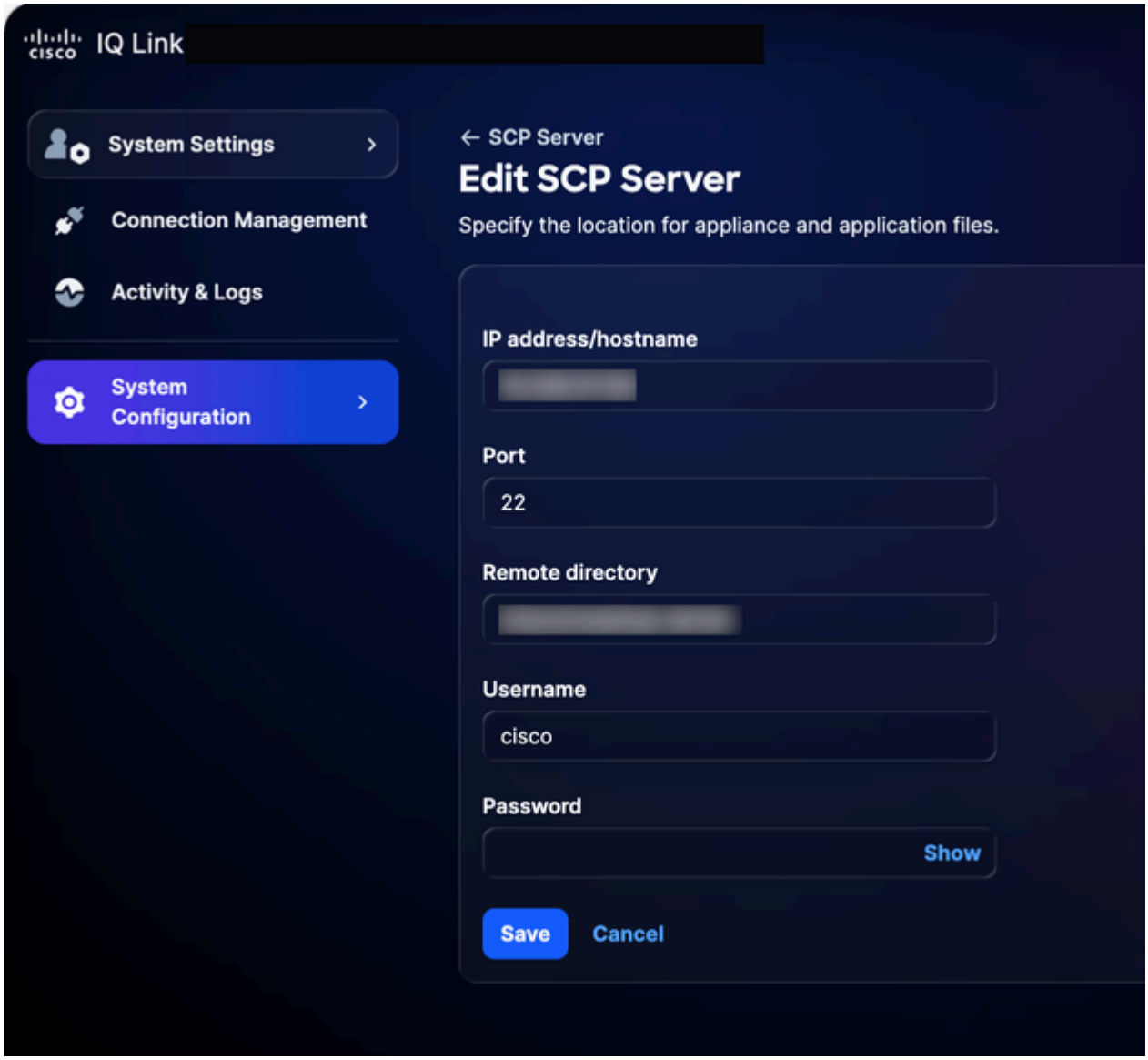
기존 SCP 서버를 수정하려면

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.

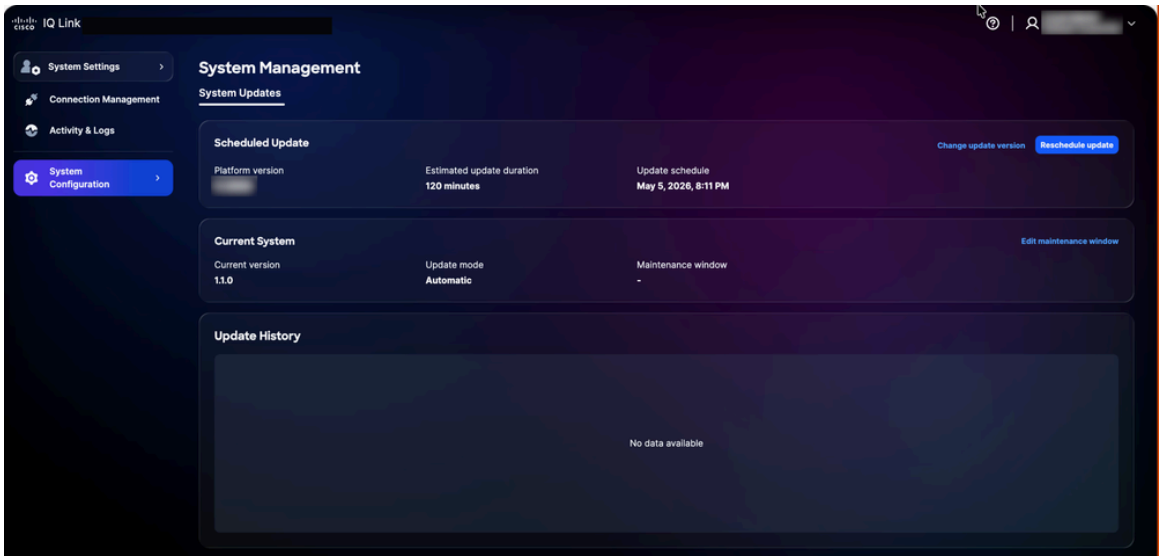
시스템 관리 업데이트

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

스케줄 조정 시스템

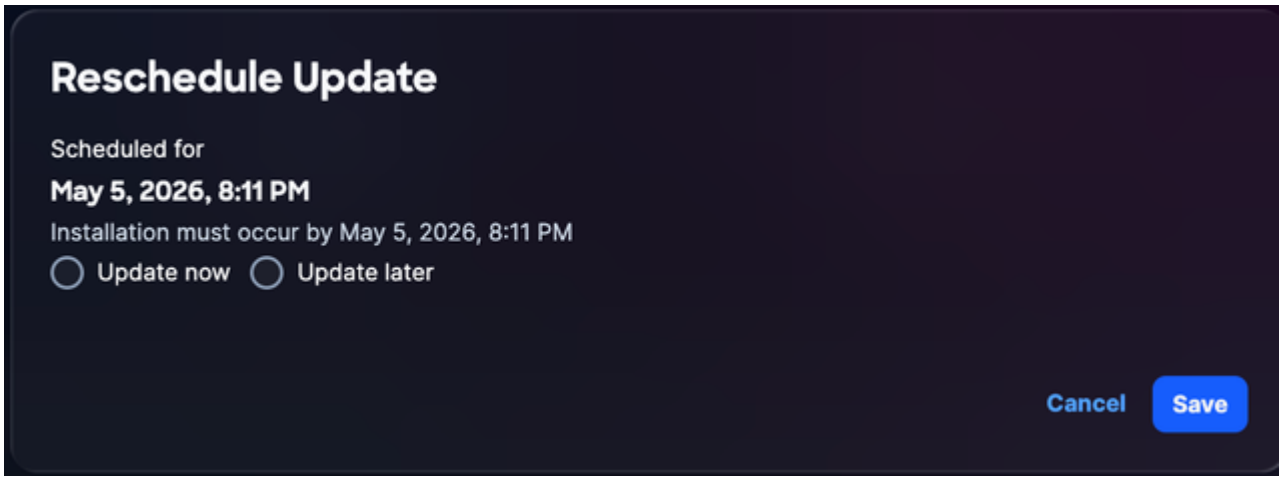
시스템 갱신 스케줄을 조정하려면

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

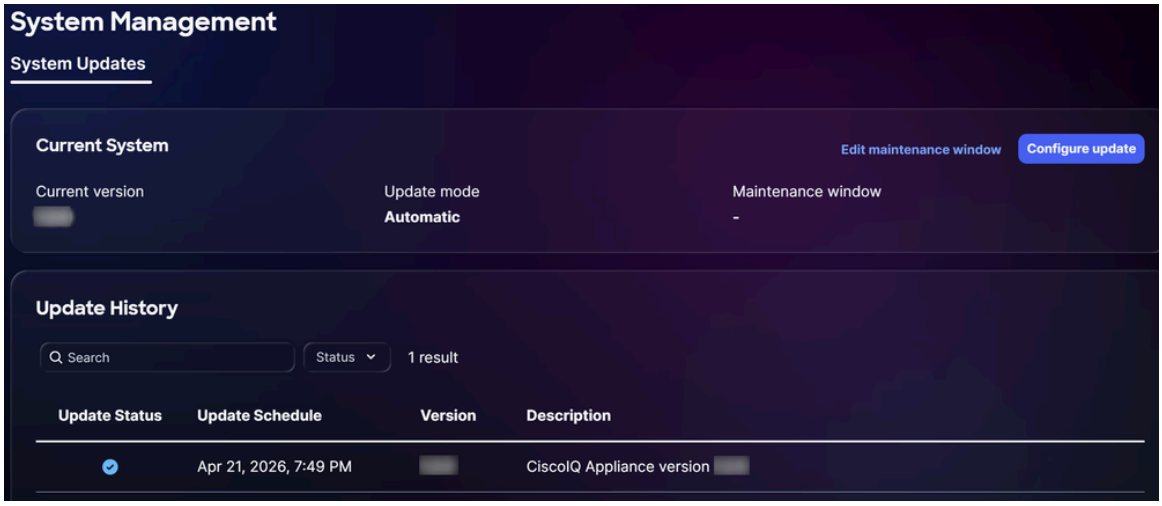
2. Reschedule update(업데이트 다시 예약)를 클릭합니다.



업그레이드 다시 예약

3. 즉시 스케줄 조정을 위해 지금 갱신을 누르거나 다른 시간을 예약하려면 나중에 갱신을 누릅니다.

4. 저장을 클릭합니다. 확인 메시지가 표시되고 System Update Home(시스템 업데이트 홈) 페이지로 리디렉션됩니다.



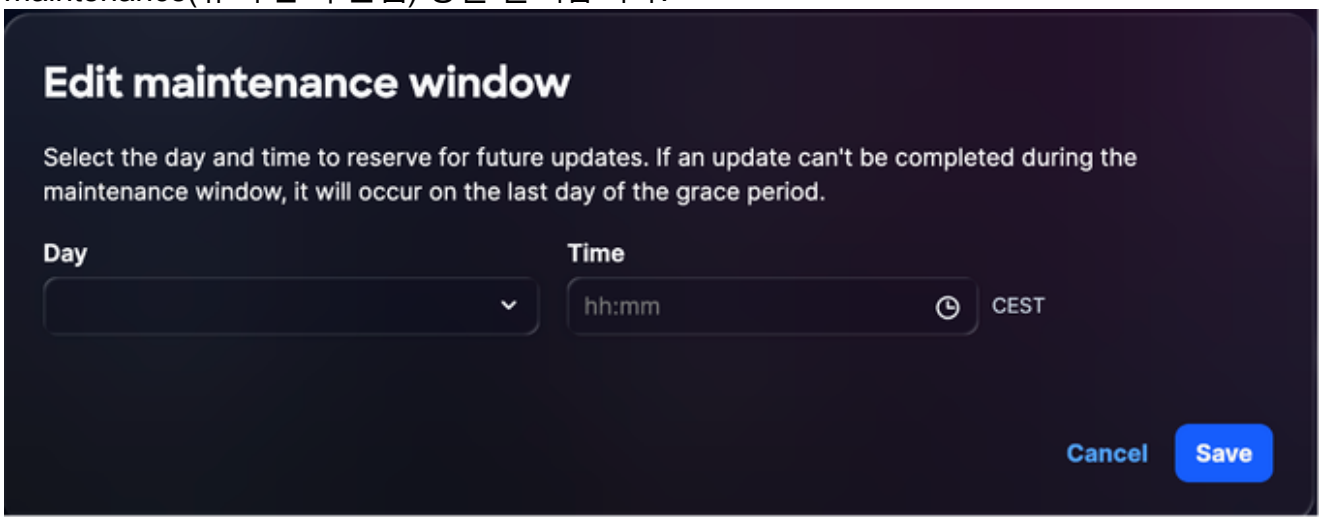
업그레이드 성공

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.

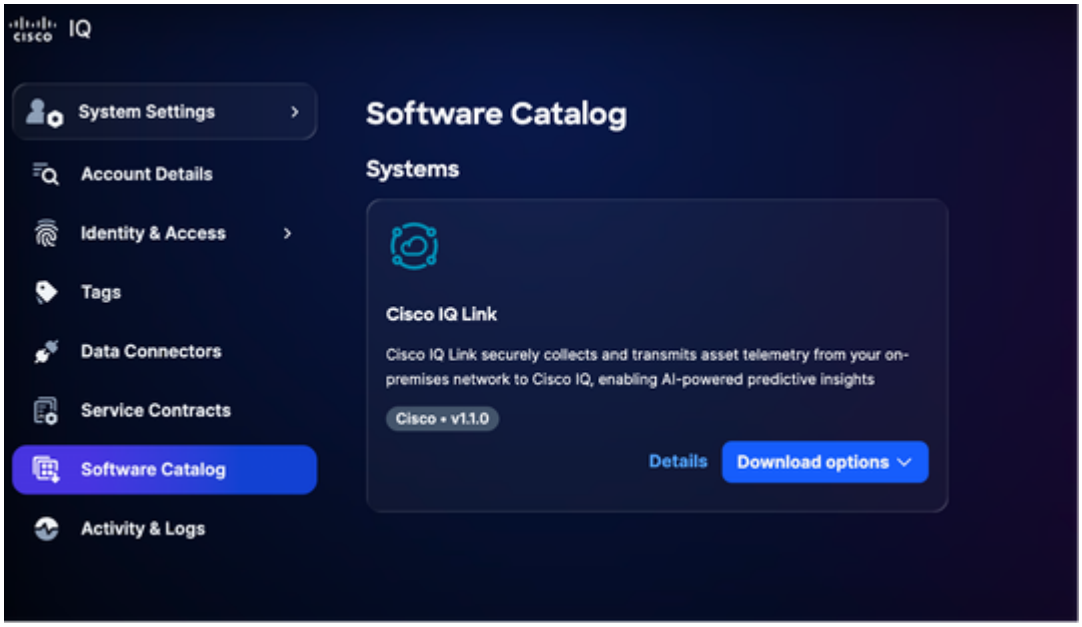
참고:
· 업그레이드 일정이 구성되지 않은 경우, 시스템은 기본적으로 비재부팅 업그레이드의 경우 2주, 재부팅이 필요한 업그레이드의 경우 4주의 유예 기간을 설정합니다. 이러한 유예 기간이 지나면 수동으로 업데이트를 수행해야 합니다.
· 업그레이드가 실패할 경우 시스템은 최대 2회의 자동 재시도를 수행합니다. 세 번째 시도는 예약되었지만 수동으로 시작해야 합니다.

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.

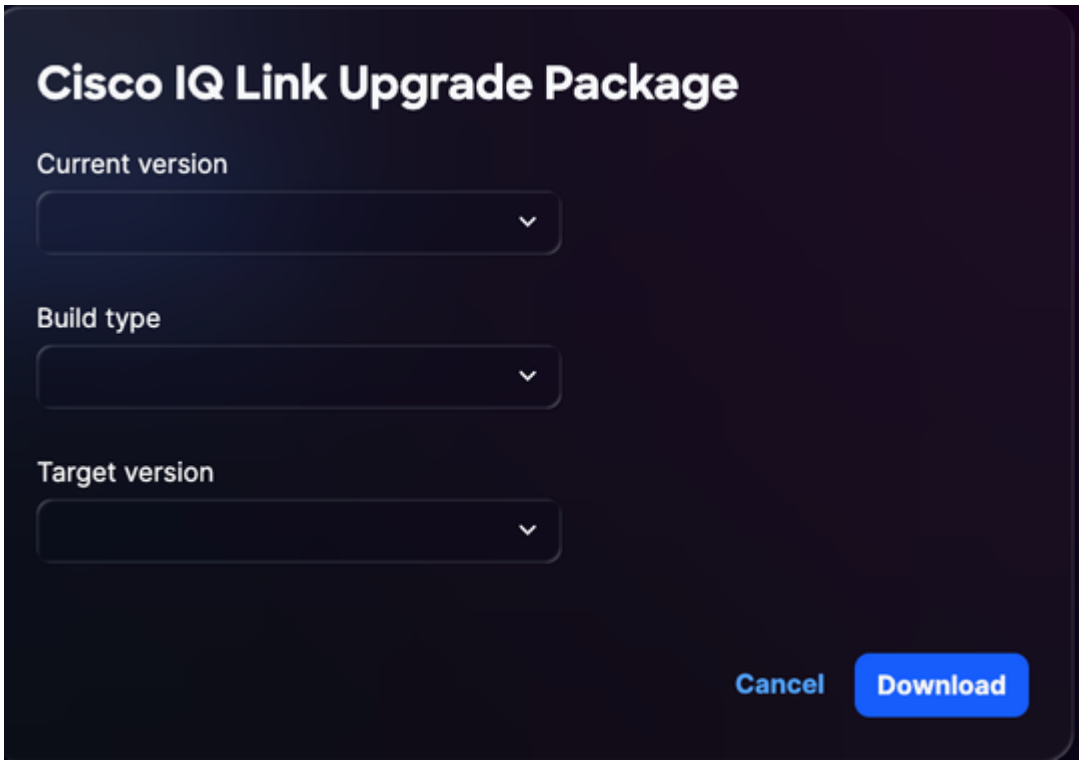
시스템을 수동으로 업그레이드하려면

1. Cisco IQ SaaS에 로그인합니다.
2. Home(홈) > System Settings(시스템 설정) > Software Catalog(소프트웨어 카탈로그)를 선택합니다.



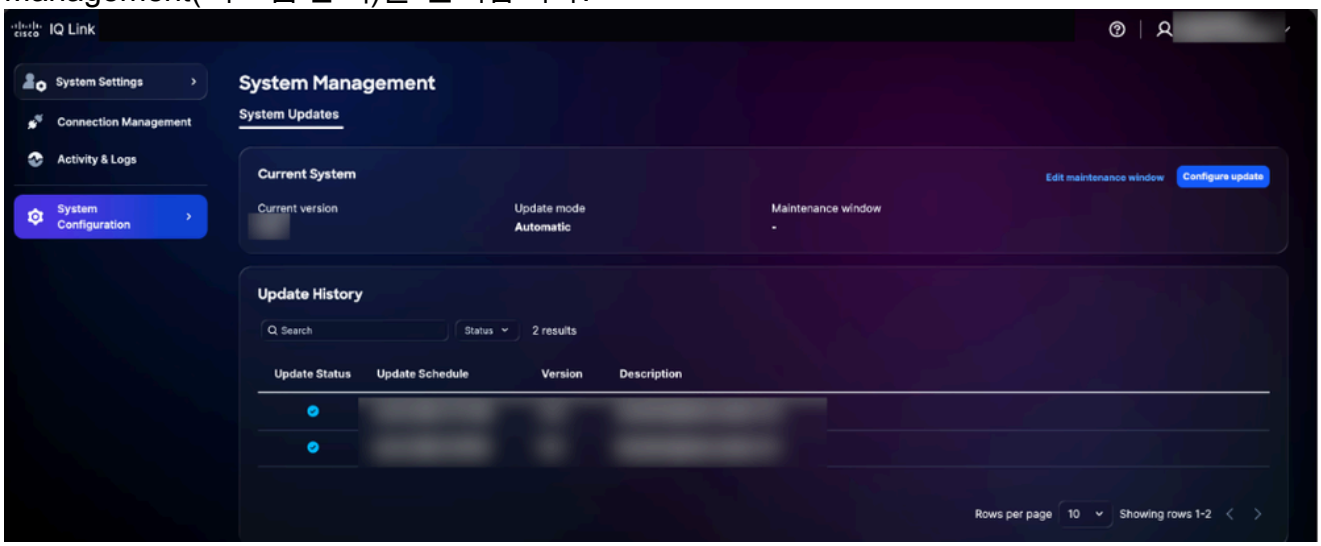
소프트웨어 카탈로그

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



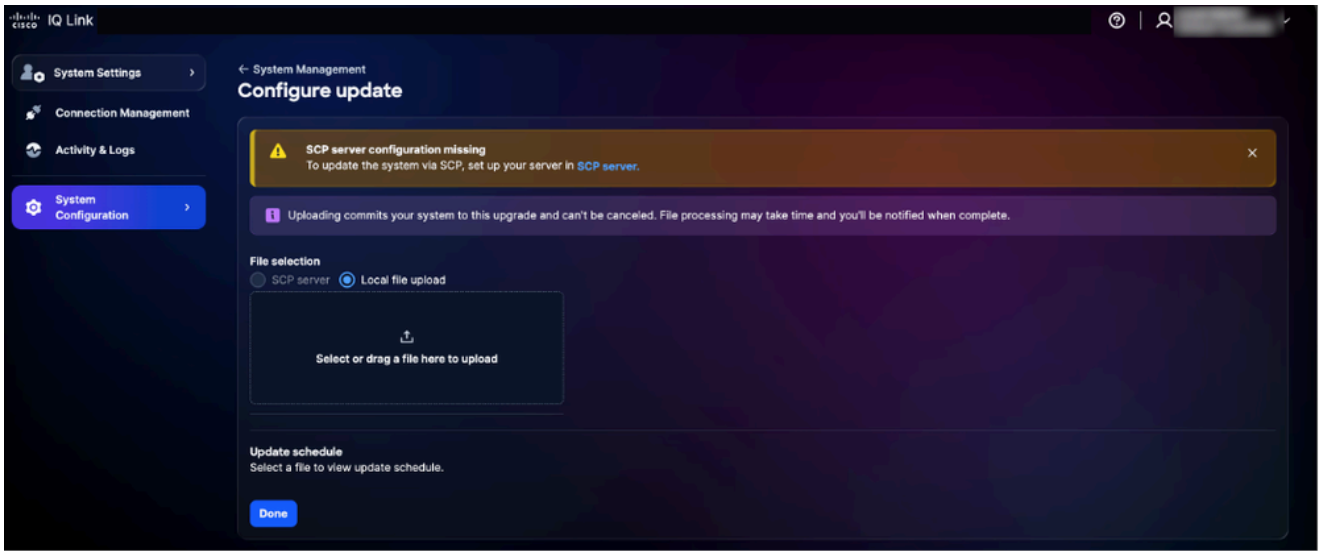
패키지 업그레이드

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



업데이트 구성

10. 업데이트 구성을 클릭합니다.



로컬 파일 업로드

11. Local file upload(로컬 파일 업로드) 라디오 버튼을 클릭합니다.
12. 다운로드한 업그레이드 번들 파일을 선택하거나 업로드 필드로 끌어옵니다.
13. 완료를 클릭합니다. 시스템이 성공적으로 업데이트된 후 확인 메시지가 표시됩니다.

SSL 인증서 컨피그레이션

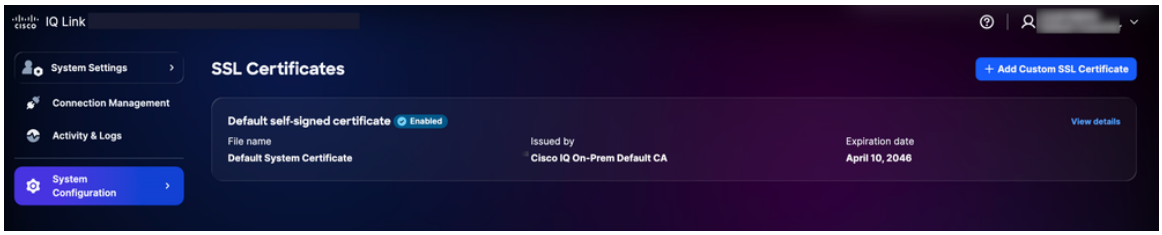
기본 자체 서명 인증서는 Cisco IQ에 사전 설치되어 활성화되지만 사용자는 사용자 지정 SSL 인증서를 업로드할 수 있습니다. 사용자 지정 SSL 인증서가 활성화되면 HTTPS 연결에 사용됩니다. 인증서가 비활성화되거나 삭제되면 시스템은 자동으로 기본 인증서로 돌아갑니다.

참고: 인증서의 유효 기간이 90일 이상 남아 있어야 합니다. 인증서는 만료일까지 남은 기간이 90일 미만일 때 "만료가 임박함"으로 간주됩니다. SSL 인증서를 추가, 수정 또는 삭제한 후 고객은 Okta IDP 또는 ADFS IDP에 대한 Completing SLO Configuration(SLO 컨피그레이션 완료) 섹션에 설명된 대로 새 SSL을 업로드해야 합니다.

사용자 지정 SSL 인증서 추가

사용자 지정 SSL 인증서를 추가하려면

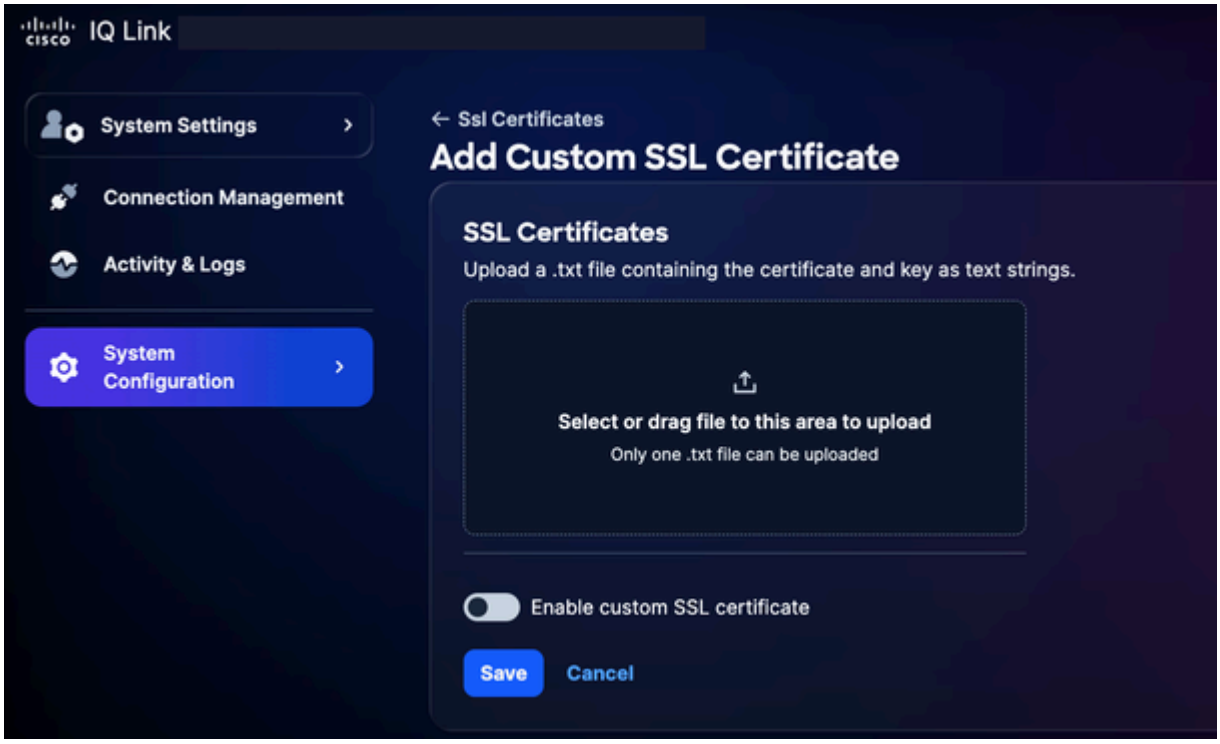
1. System Settings(시스템 설정)에서 System Configuration(시스템 컨피그레이션) > SSL Certificates(SSL 인증서)를 선택합니다. 시스템의 모든 SSL 인증서를 나열하는 SSL Certificates 페이지가 표시됩니다.



SSL 인증서 추가

2. Add Custom SSL Certificate를 클릭합니다.

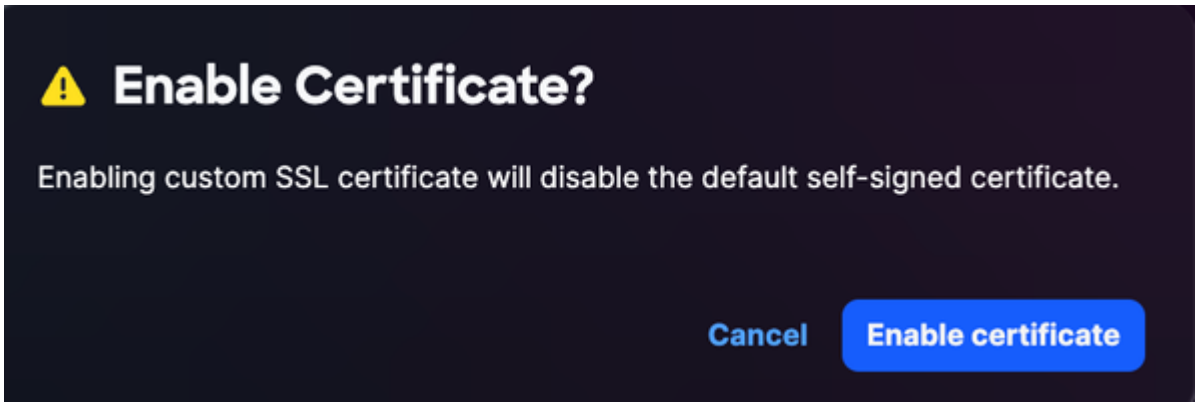
참고:
· Privacy-Enhanced Mail 인코딩 인증서 및 키가 모두 포함된 .txt 파일을 텍스트 문자열로 업로드합니다.
· 한 번에 하나의 .txt 파일만 업로드할 수 있습니다.
· 파일에 인증서와 개인 키가 모두 있어야 합니다.



SSL 인증서 업로드

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

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



인증서 사용

참고: 인증서를 즉시 활성화하지 않고 업로드하려면 토글을 끄지 않습니다.

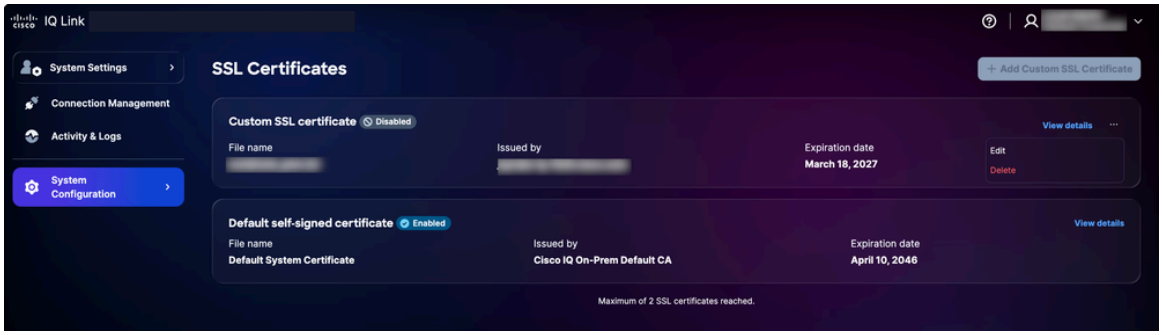
5. Enable certificate(인증서 활성화)를 클릭합니다.
6. 저장을 클릭합니다.

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

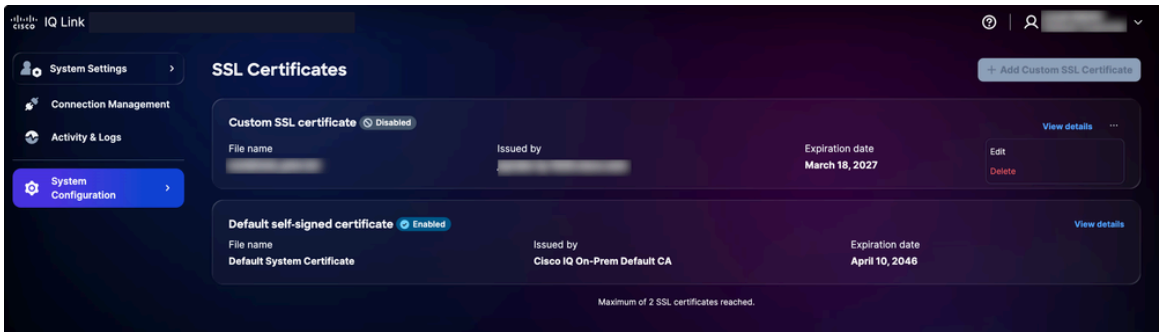
2. 추가 옵션 아이콘 > 편집을 선택합니다. Edit SSL Certificate 페이지가 표시됩니다.
3. 필요에 따라 인증서 세부사항을 수정합니다.
4. 저장을 클릭합니다.

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 개인 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

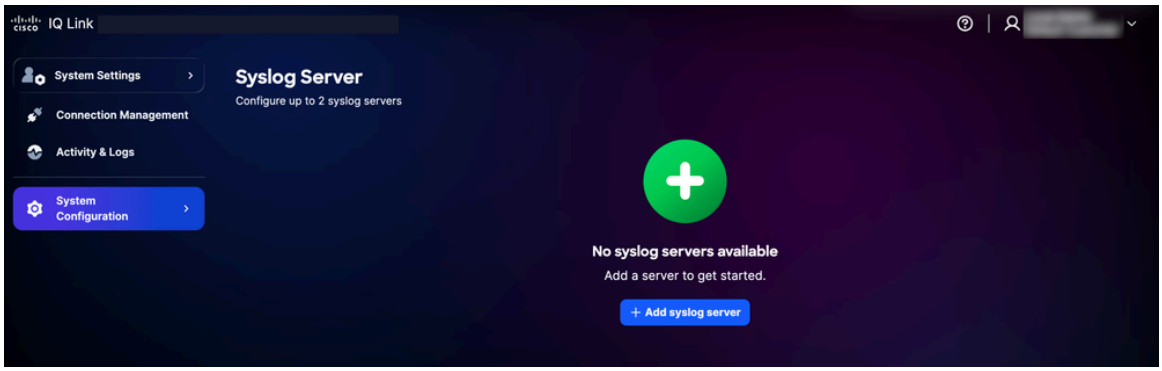
Administrator 역할의 사용자는 외부 syslog 서버를 구성하여 시스템 로그를 내보낼 수 있습니다. 최대 2개의 syslog 서버를 구성할 수 있습니다.

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

Syslog 서버 추가

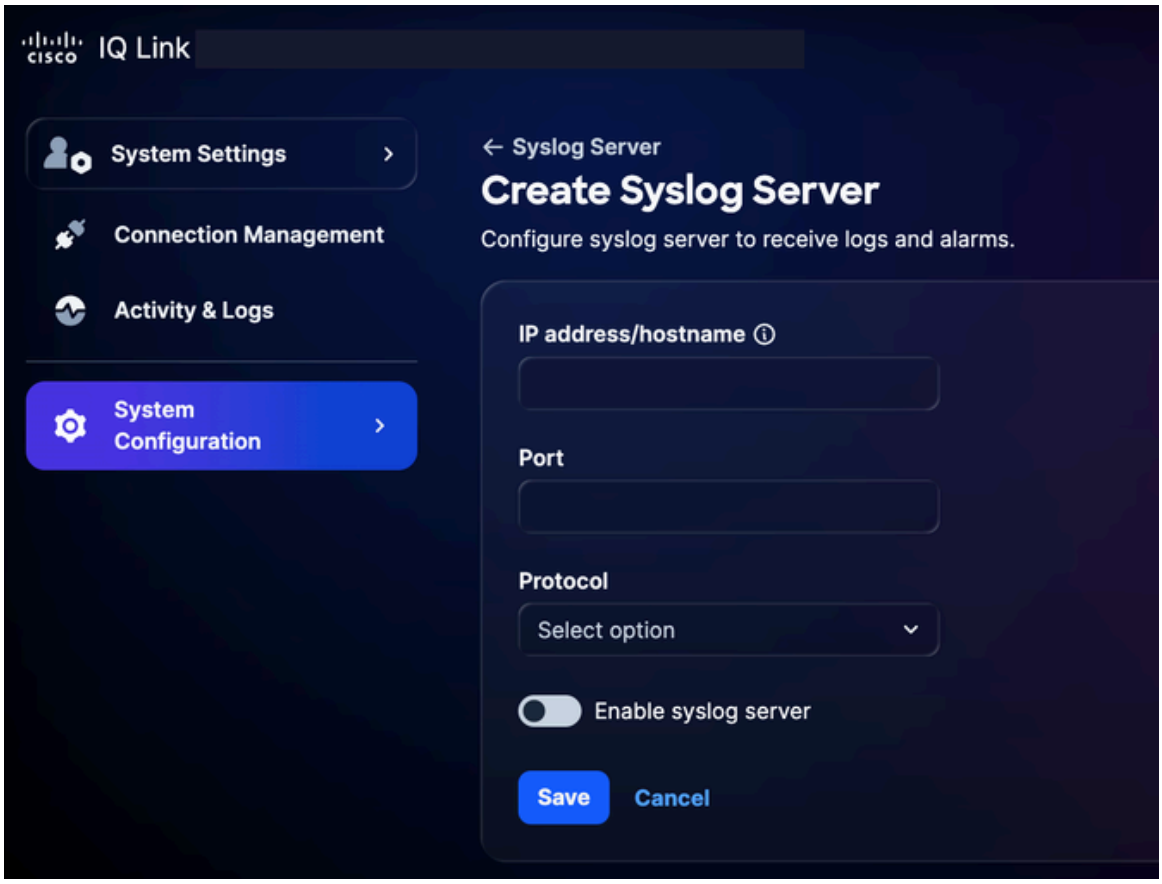
syslog 서버를 추가하려면

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



Syslog 서버 추가

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



Syslog 서버 생성

3. IP 주소/호스트 이름을 입력합니다.

4. 포트 번호를 입력합니다.

5. Protocol 드롭다운 목록에서 해당 프로토콜(예: UDP 또는 TCP)을 선택합니다.

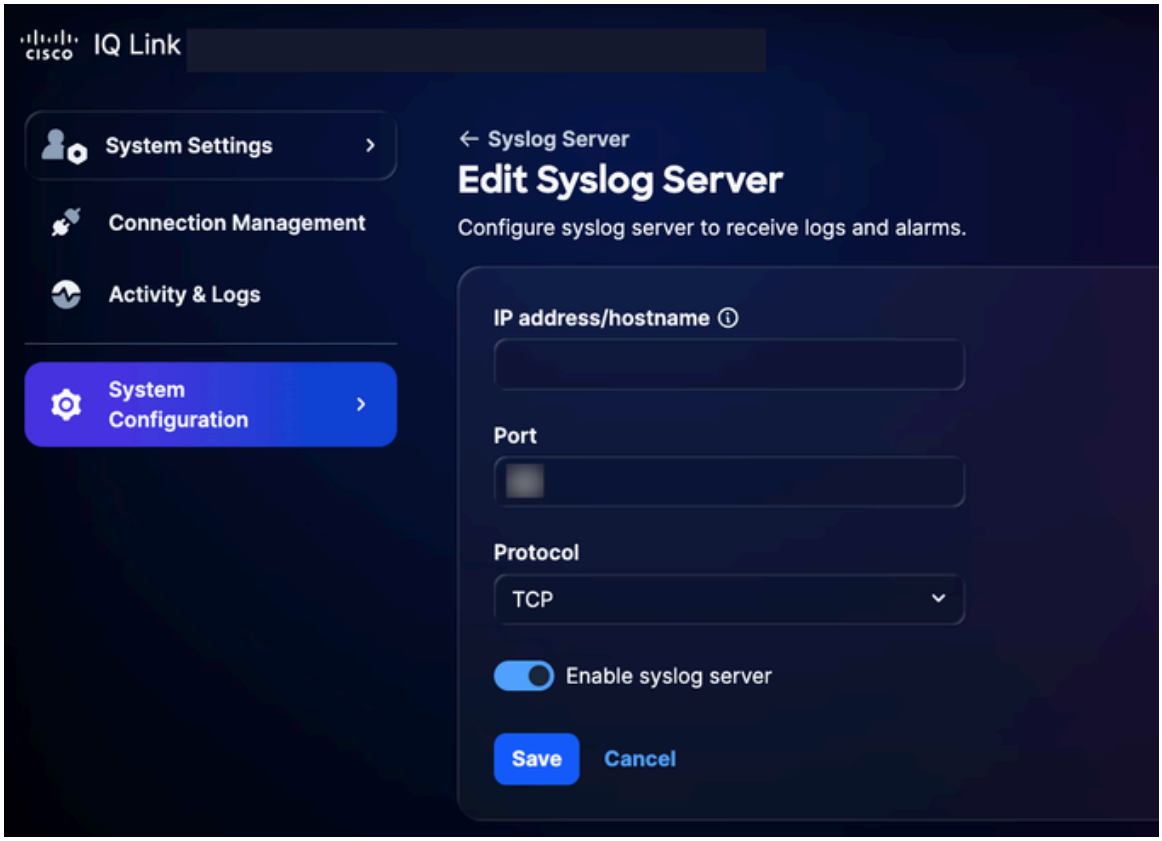
6. Enable syslog server 토글 버튼을 켭니다.

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 표시됩니다.



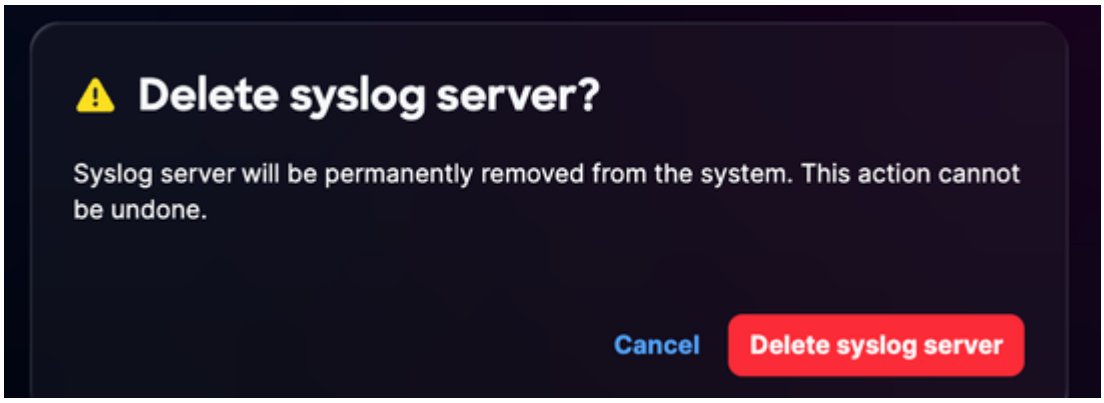
Syslog 서버 편집

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.

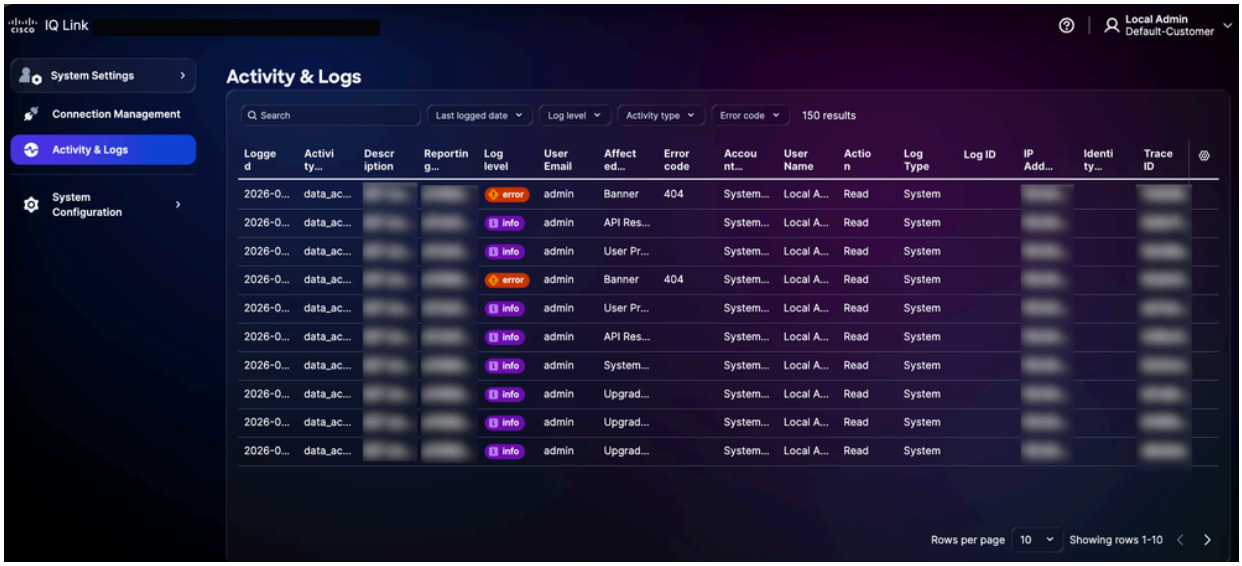


확인

3. Delete syslog server를 클릭합니다.

활동 및 로그

Activity & Logs(활동 및 로그)는 Cisco IQ의 사용자 작업 및 변경 사항에 대한 자세한 기록을 제공하여 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

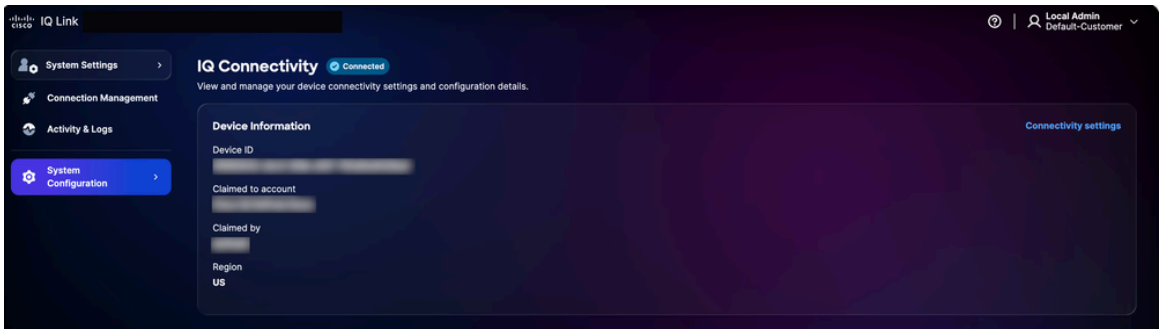
다음 필터 옵션을 사용할 수 있습니다.

- 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

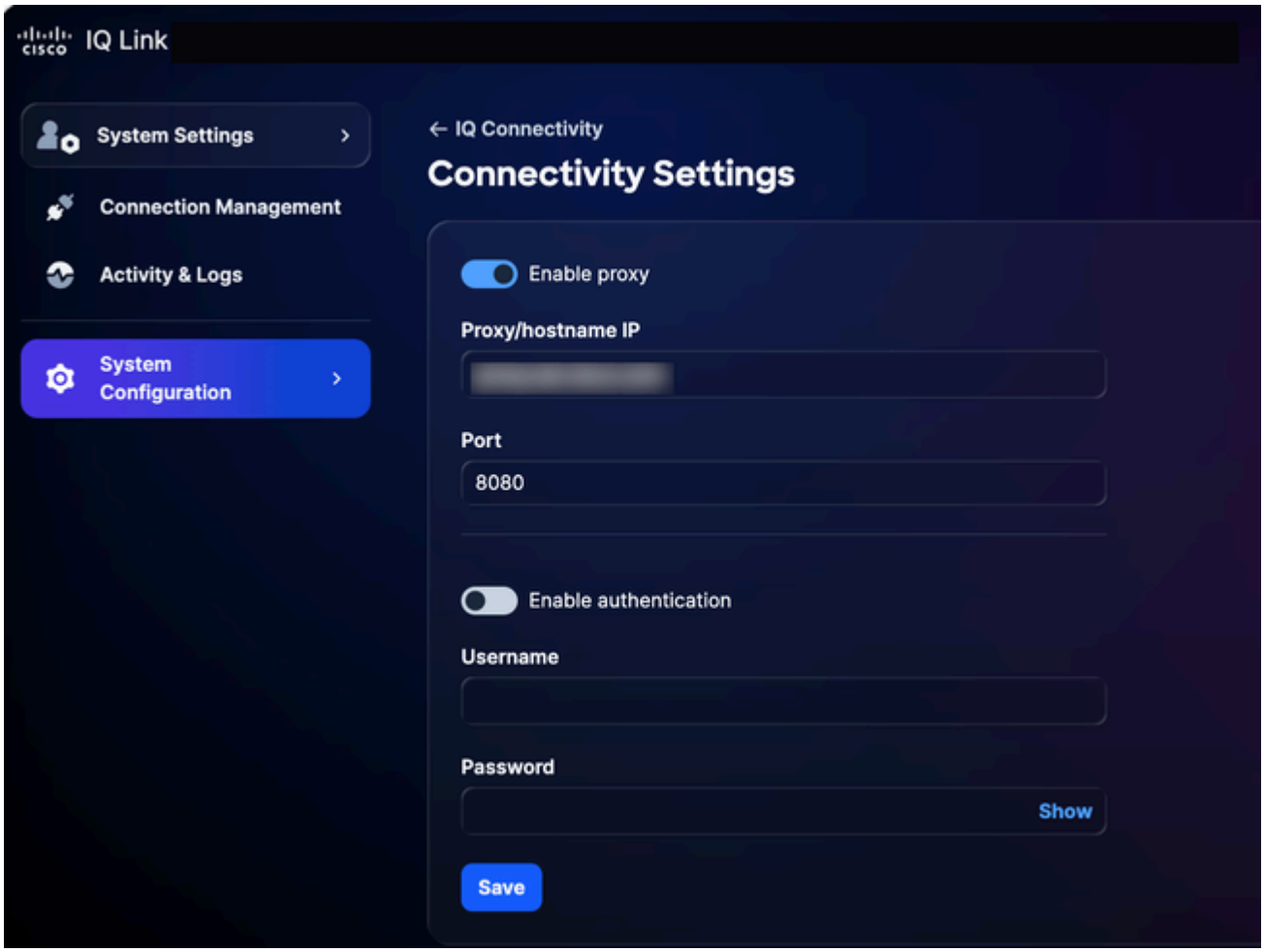
디바이스 연결 설정 및 컨피그레이션 세부사항을 보고 관리하려면

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 구축 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 다음과 같이 요약할 수 있습니다.

- 크리덴셜 세트 생성: 네트워크 디바이스와 통신하기 위해 인증 프로토콜(예: SNMP 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 시스

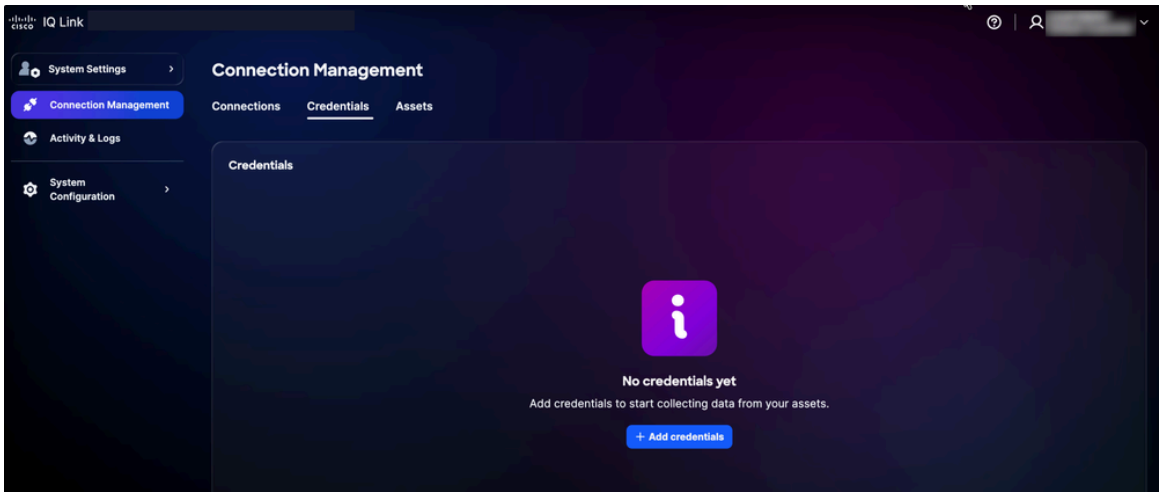
템은 데이터 수집 중에 올바른 인증을 자동으로 적용합니다. 이렇게 하면 수동 입력 오류가 제거되고 네트워크 확장에 따라 컨피그레이션이 정확하게 유지됩니다.

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

자격 증명 추가

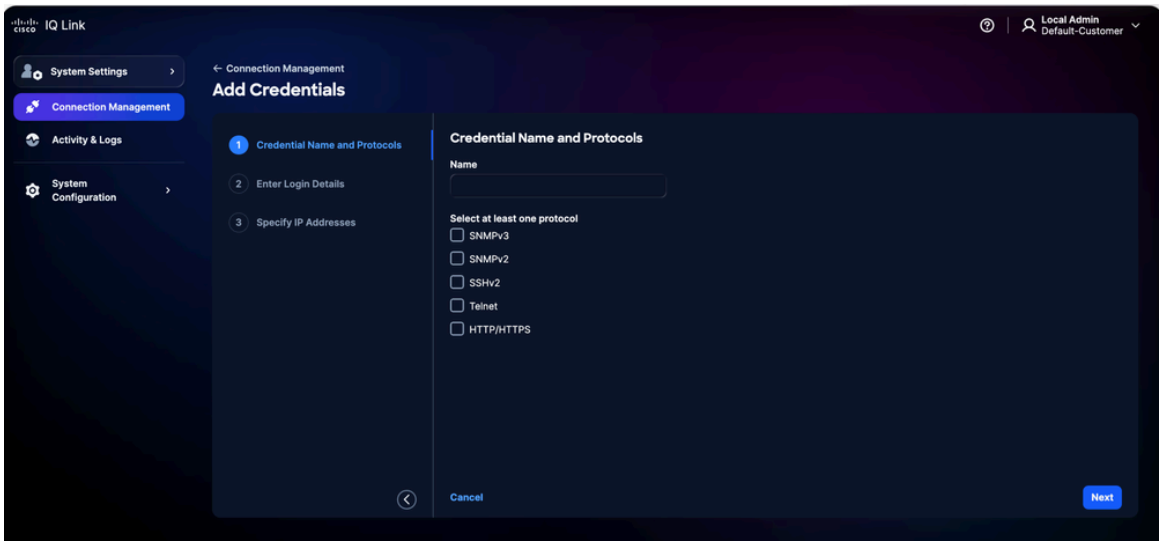
데이터 수집을 수행하려면 먼저 자격 증명을 추가해야 합니다. 자격 증명을 추가하려면

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



자격 증명 탭

3. Add credentials(자격 증명 추가)를 클릭합니다.

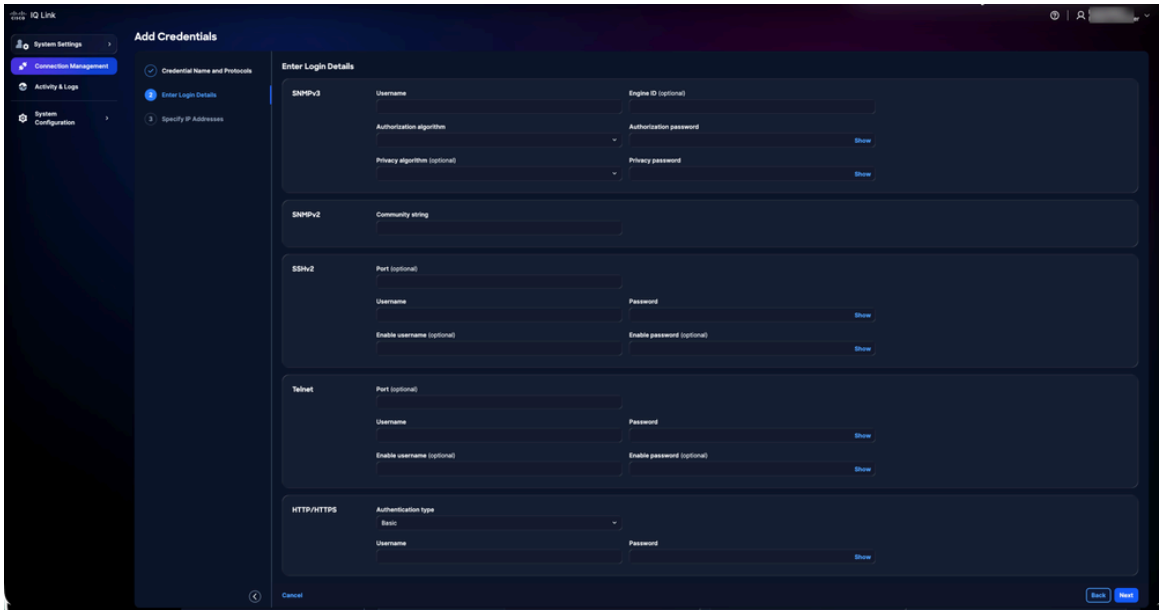


자격 증명 추가

4. Name을 입력합니다.

5. 해당되는 모든 프로토콜 확인란을 선택합니다.

6. Next(다음)를 클릭합니다.

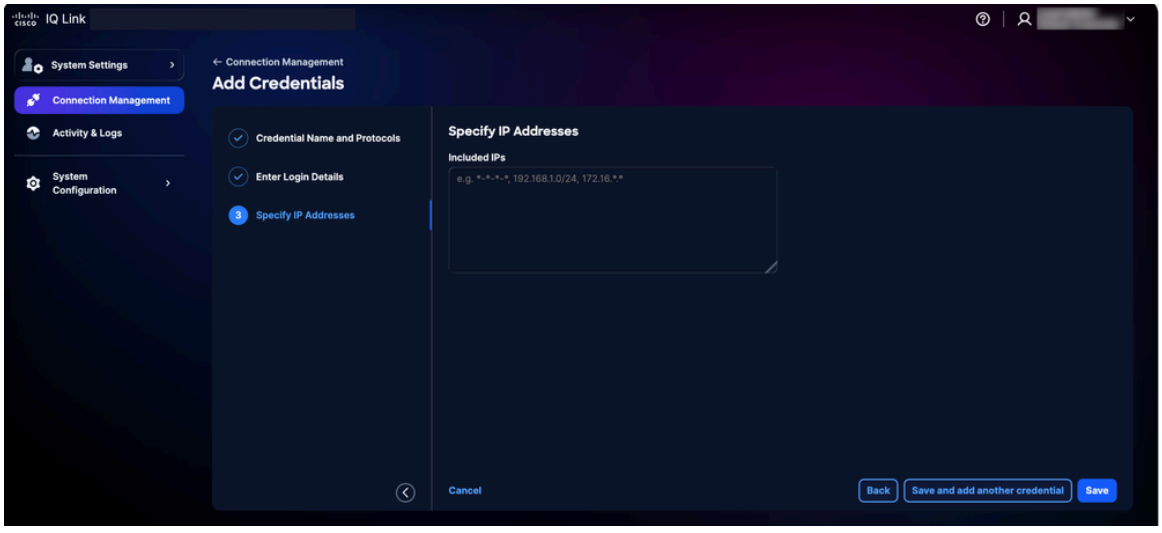


자격 증명 추가 세부 정보

참고: 위 그림에서는 이전 단계에서 모든 프로토콜이 선택된 경우의 보기를 보여 줍니다. 선택한 특정 프로토콜만 인터페이스에 표시됩니다.

7. 선택한 각 프로토콜에 대한 로그인 세부 정보를 입력합니다.

8. Next(다음)를 클릭합니다.

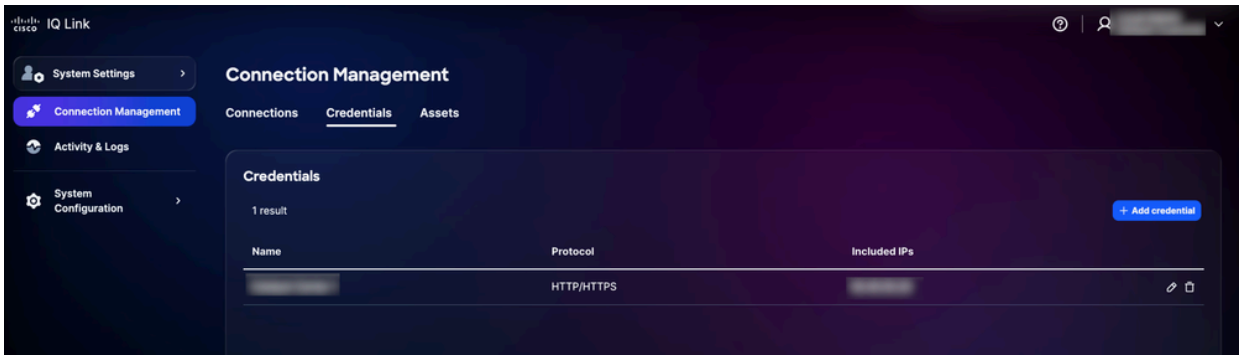


IP 주소 지정

9. Included IPs(포함된 IP)를 입력합니다.

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

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



추가된 자격 증명

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

자격 증명 선택 및 일치 논리

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

- 우선 순위: 여러 자격 증명 집합이 디바이스에 적용되는 경우 Cisco IQ는 디바이스와 얼마나 정확하게 일치하는지를 기준으로 평가합니다. 시스템은 다음과 같은 우선순위를 적용하며, 더 구체적인 일치 항목이 우선합니다.
  - 정확한 IP 일치: 최우선 순위
  - 후행 와일드카드 일치:** **우선순위는 후행 별의 수에 따라 달라집니다. 별이 적을수록 더 구체적인 일치를 나타내므로 우선순위가 높습니다.
- 와일드카드 서식 지정 규칙: 와일드카드(*)는 IP 주소에서 후행 문자로만 지원됩니다. 오른쪽에서 왼쪽으로 적용해야 합니다.
  - 지원되는 형식:

    1.2.3.*(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.

자격 증명 선택 예

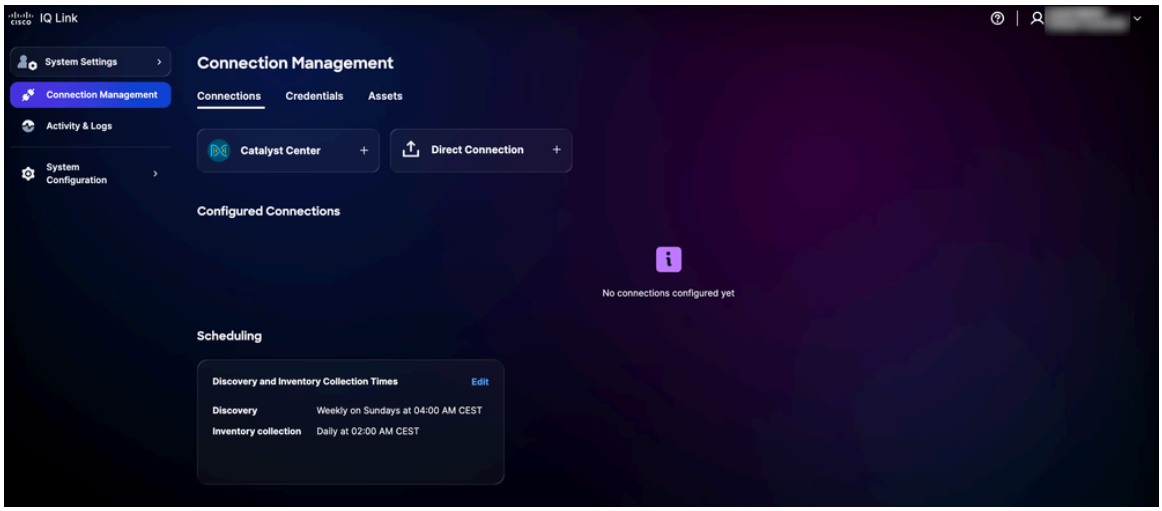
디바이스 IP	사용 가능한 자격 증명 집합	선택한 자격 증명 집합
10.10.1.5	10.10.1.5, 10.10.1., 10.10..*	10.10.1.5(정확히 일치)
10.10.2.15	10.10.2., 10.10..*	10.10.2.*(자세히)
10.10.5.50	10.10...	10.10... (자세히 설명)

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

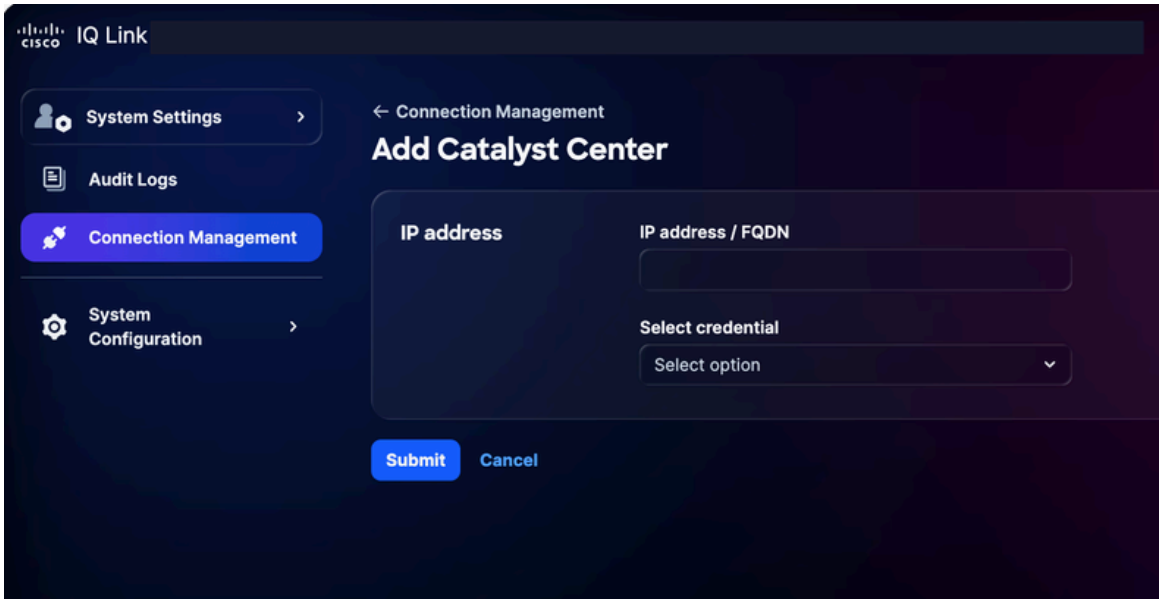
Catalyst Center를 사용한 데이터 수집:

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



연결 관리

2. Catalyst Center 옵션을 클릭합니다.

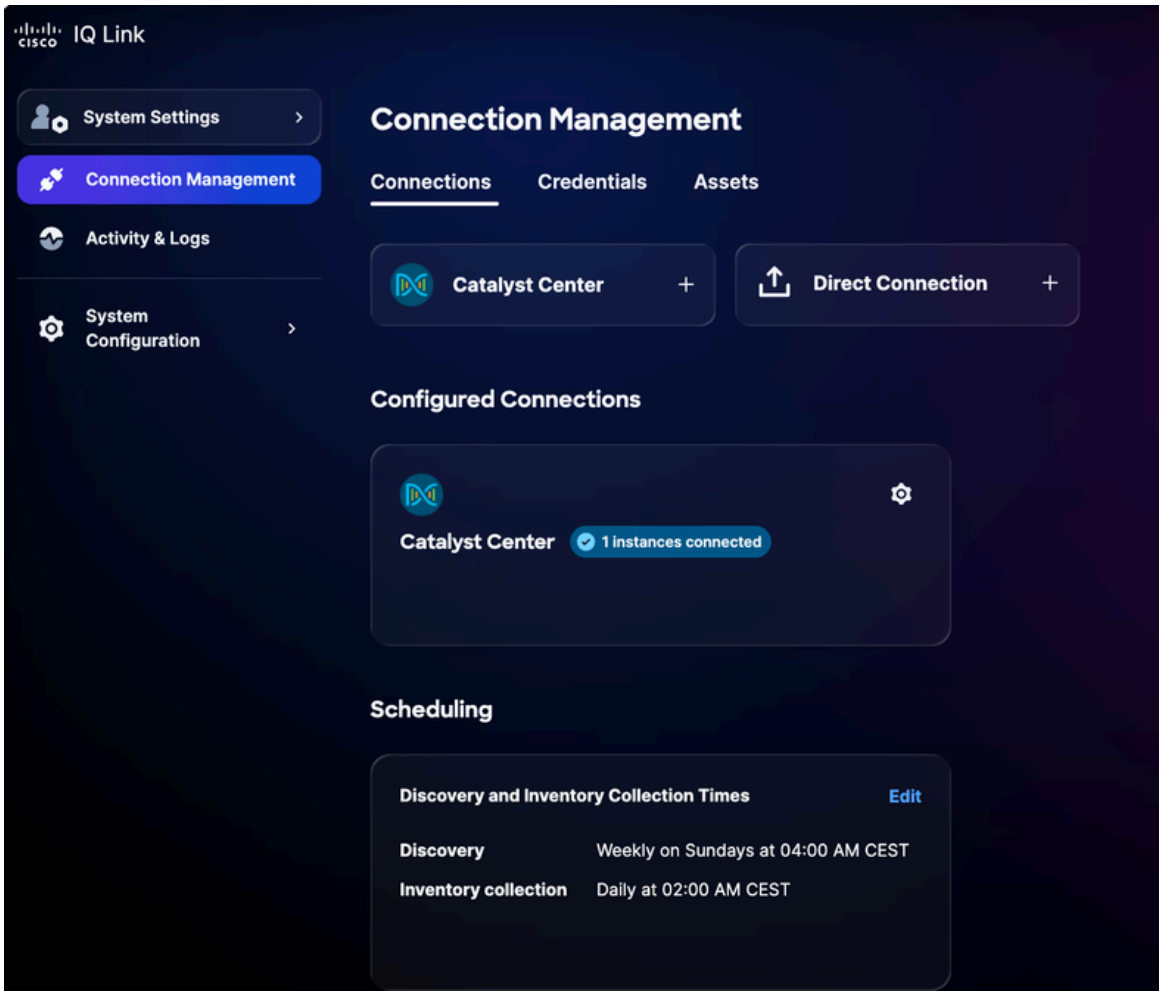


Catalyst Center 추가

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.

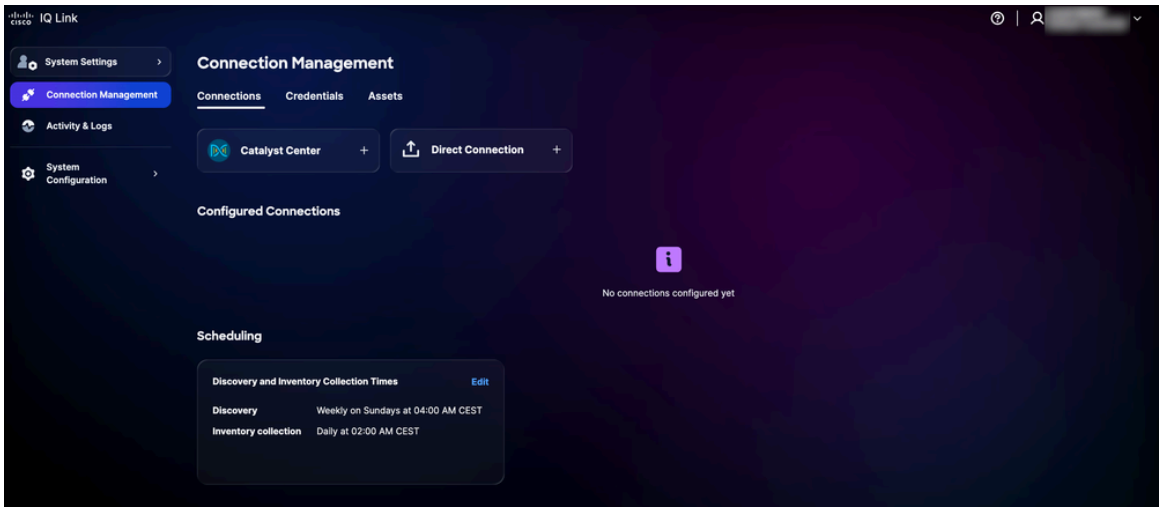
6. 수집을 예약합니다. 자세한 내용은 예약을 참조하십시오.

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

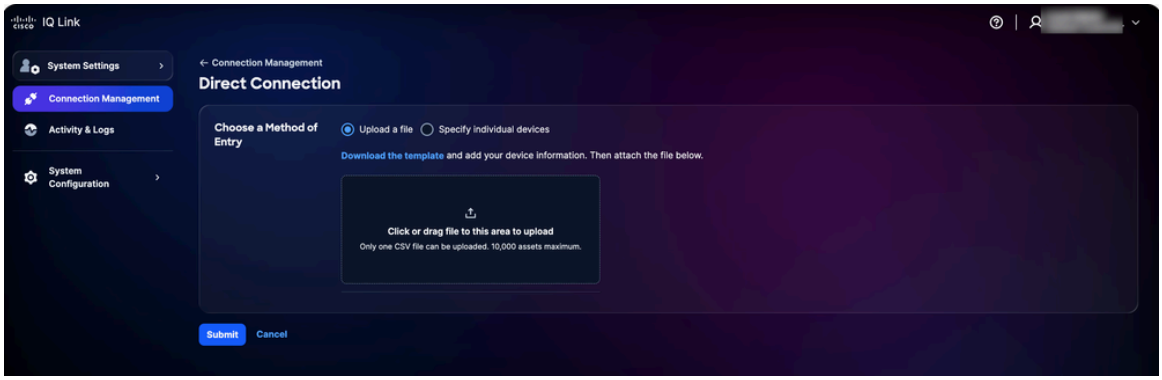
직접 연결을 위해 디바이스를 추가하려면

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



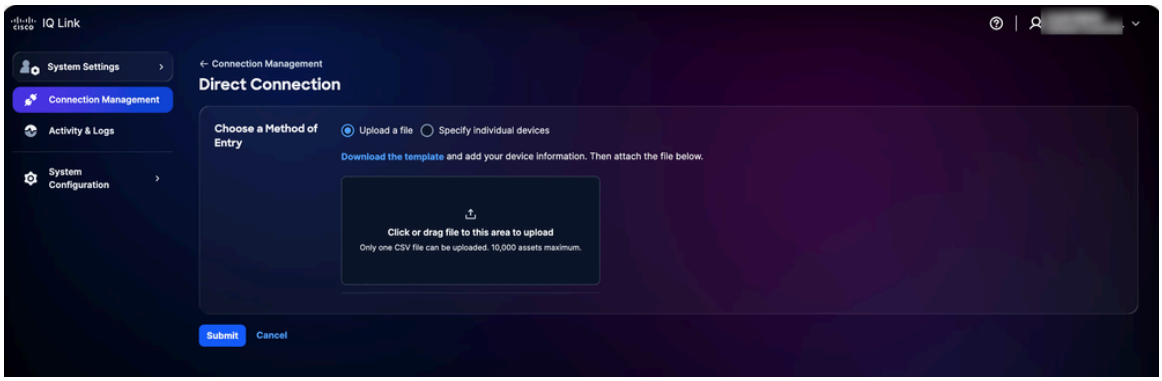
연결 관리

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



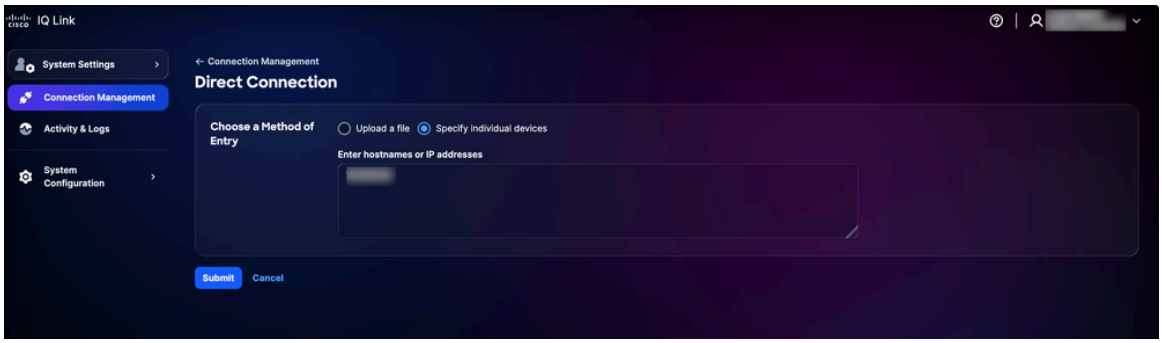
파일 업로드

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.

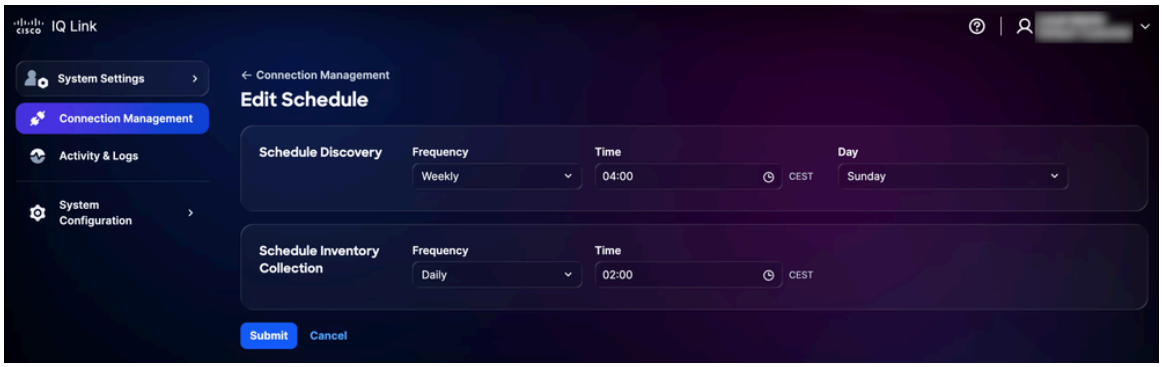
4. 수집을 예약합니다. 자세한 내용은 예약을 참조하십시오.

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.

예약

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

관리자는 애플리케이션 전체에 표시되는 사용자 지정 배너를 구성할 수 있습니다.

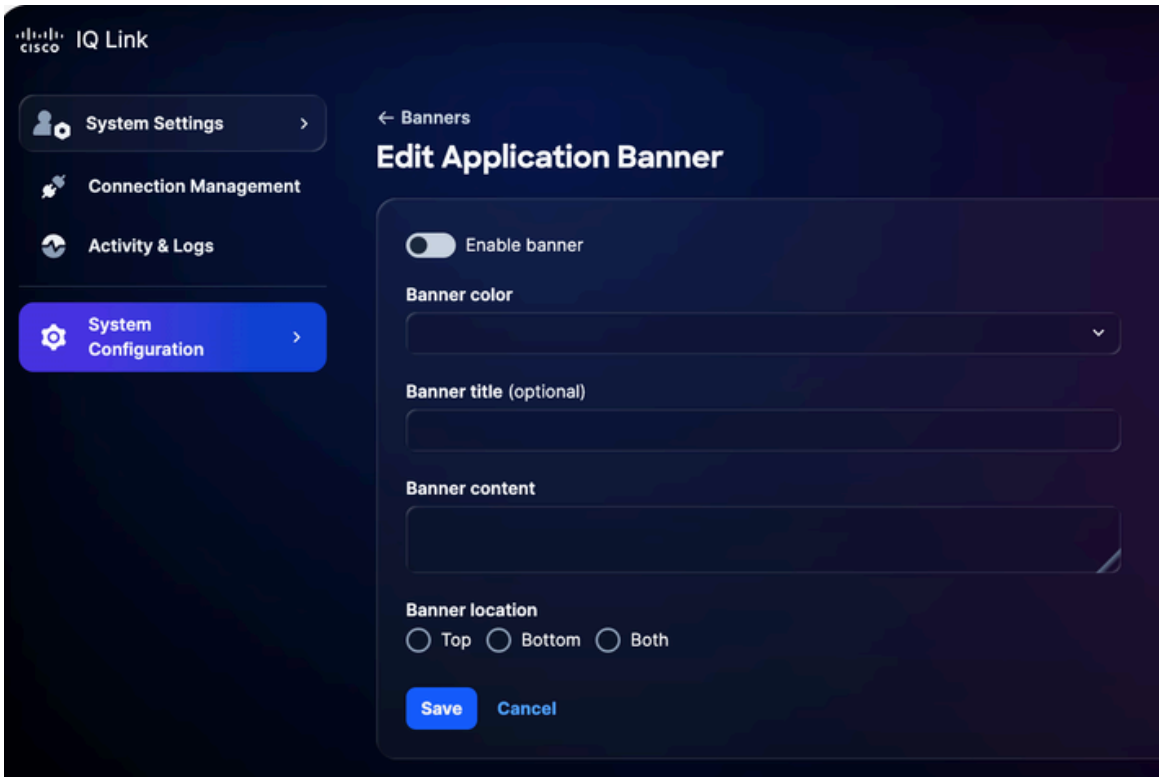
배너 구성

배너를 구성하려면

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

배너 구성

2. Configure를 클릭합니다. 애플리케이션 배너 편집 페이지가 표시됩니다.



애플리케이션 배너 편집

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

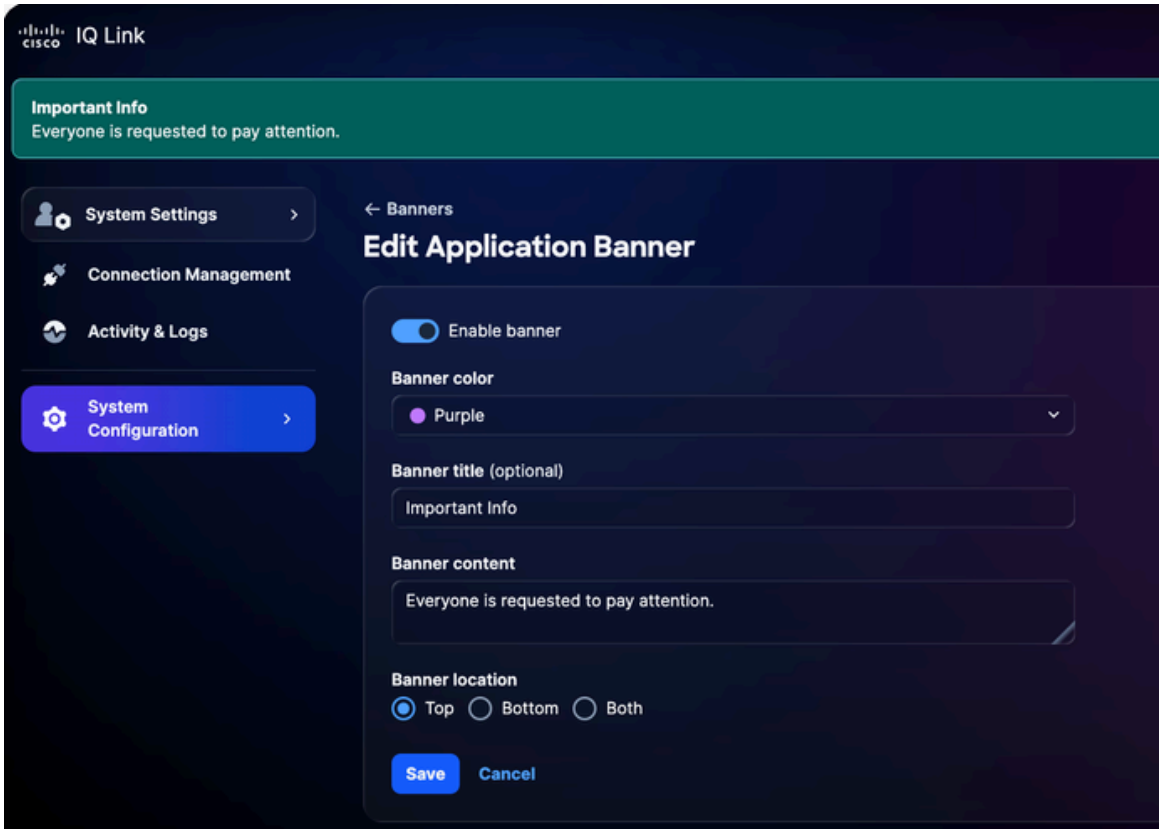
배너 수정

배너를 수정하려면

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

배너 편집

2. Edit를 클릭합니다. 애플리케이션 배너 편집 페이지가 표시됩니다.



애플리케이션 배너 편집

3. 원하는 세부 정보를 편집합니다.

4. 배너를 활성화 또는 비활성화하려면 토글을 클릭합니다.

5. 저장을 클릭합니다.

문제 해결

고객은 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 Co시스템 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.