

Intersight Virtual Appliance에서 LDAP 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[LDAP 기본 설정 컨피그레이션](#)

[사용자 및 그룹 구성](#)

[그룹 구성](#)

[사용자 구성](#)

[LDAPS\(Secure LDAP\) 컨피그레이션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[오류 1. 잘못된 액세스 세부 정보](#)

[오류 2. 잘못된 바인드 데이터](#)

[오류 3. 사용자를 찾을 수 없습니다.](#)

[오류 4. 잘못된 인증서](#)

[오류 5. 암호화 사용이 보안 포트와 함께 사용됩니다.](#)

[오류 6. 연결 매개 변수가 잘못되었습니다.](#)

[관련 정보](#)

소개

이 문서에서는 Intersight PVA(Private Virtual Appliance)에서 LDAP 인증을 구성하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- LDAP(Lightweight Directory Access Protocol) 프로토콜입니다.
- Intersight Private Virtual Appliance.
- DNS(도메인 이름 서버) 서버.

사용되는 구성 요소

- Intersight Private Virtual Appliance.
- 마이크로소프트 액티브 디렉토리.
- DNS 서버.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

LDAP는 네트워크를 통해 디렉토리에서 리소스에 액세스하는 데 사용되는 프로토콜입니다. 이러한 디렉토리에는 사용자, 조직 및 리소스에 대한 정보가 저장됩니다. LDAP는 인증 및 권한 부여 프로세스에 사용할 수 있는 정보에 액세스하고 이를 관리하는 표준 방법을 제공합니다.

이 문서에서는 LDAP를 통한 원격 인증을 Intersight PVA에 추가하는 컨피그레이션 프로세스를 보여줍니다.

구성

LDAP 기본 설정 컨피그레이션

1. System > Settings > AUTHENTICATION > LDAP/AD로 이동합니다.
2. LDAP 구성을 클릭합니다.
3. 필수 정보를 입력합니다. 다음 권장 사항을 고려하십시오.
 1. 이름은 임의로 설정되며 컨피그레이션에 영향을 주지 않습니다.
 2. BaseDN 및 BindDN의 경우 AD(Active Directory) 컨피그레이션에서 해당 값을 복사하여 붙여 넣습니다.
 3. Group Attribute의 기본값은 member입니다.



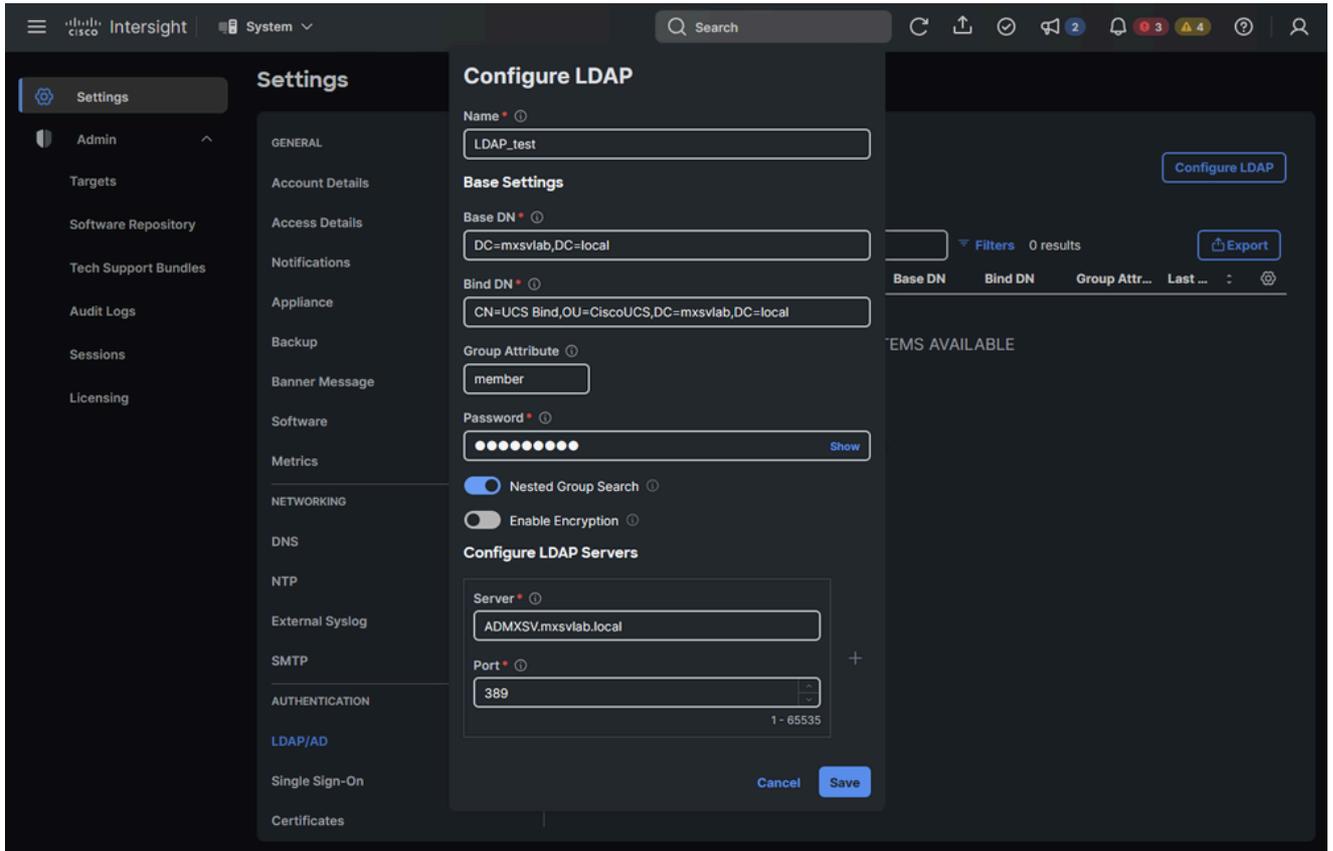
참고: UCSM 또는 CIMC와 같은 다른 UCS 관리 툴에서는 Group 특성이 memberOf로 설정됩니다. Intersight에서는 멤버로 두는 것이 좋습니다.

4. 이 LDAP 제공자의 비밀번호를 입력합니다.
5. 루트의 모든 그룹과 포함된 그룹에 대해 AD에서 재귀 검색을 허용하려면 중첩 그룹 검색 사용 토글을 설정합니다.
6. 일반 LDAP 컨피그레이션에 대해 Enable Encryption(암호화 활성화)을 비활성화한 상태로 둡니다. 보안 LDAP가 필요한 경우 이를 활성화하고 LDAPS(Secure LDAP) 컨피그레이션 섹션에서 구성해야 하는 보안 단계를 검토합니다.
4. 하나의 LDAP 서버에 대한 컨피그레이션을 추가합니다.
 1. 서버에서 LDAP 서버의 IP 또는 호스트 이름을 도입합니다.



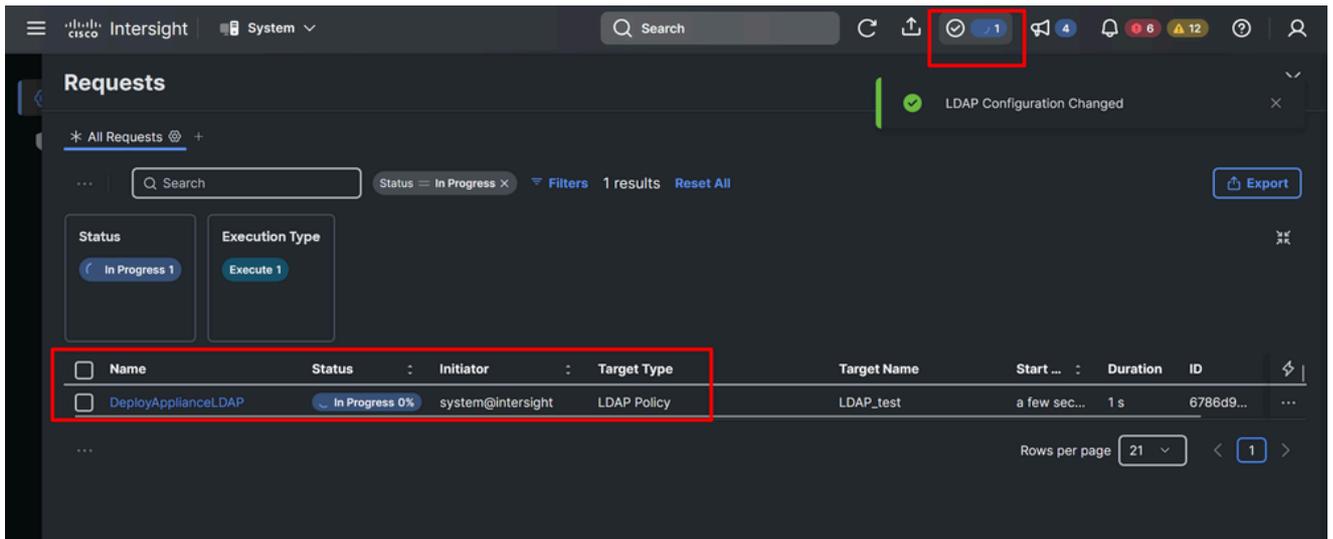
주의: 호스트 이름을 사용하는 경우 DNS에서 해당 호스트 이름을 올바르게 매핑할 수 있는지 확인합니다.

- LDAP의 기본 및 권장 포트는 389입니다.
- 저장을 클릭합니다.



기본 LDAP 설정의 컨피그레이션 예

- 상단 막대의 Requests에서 DeployApplianceLDAP 워크플로를 모니터링합니다.



구축 요청

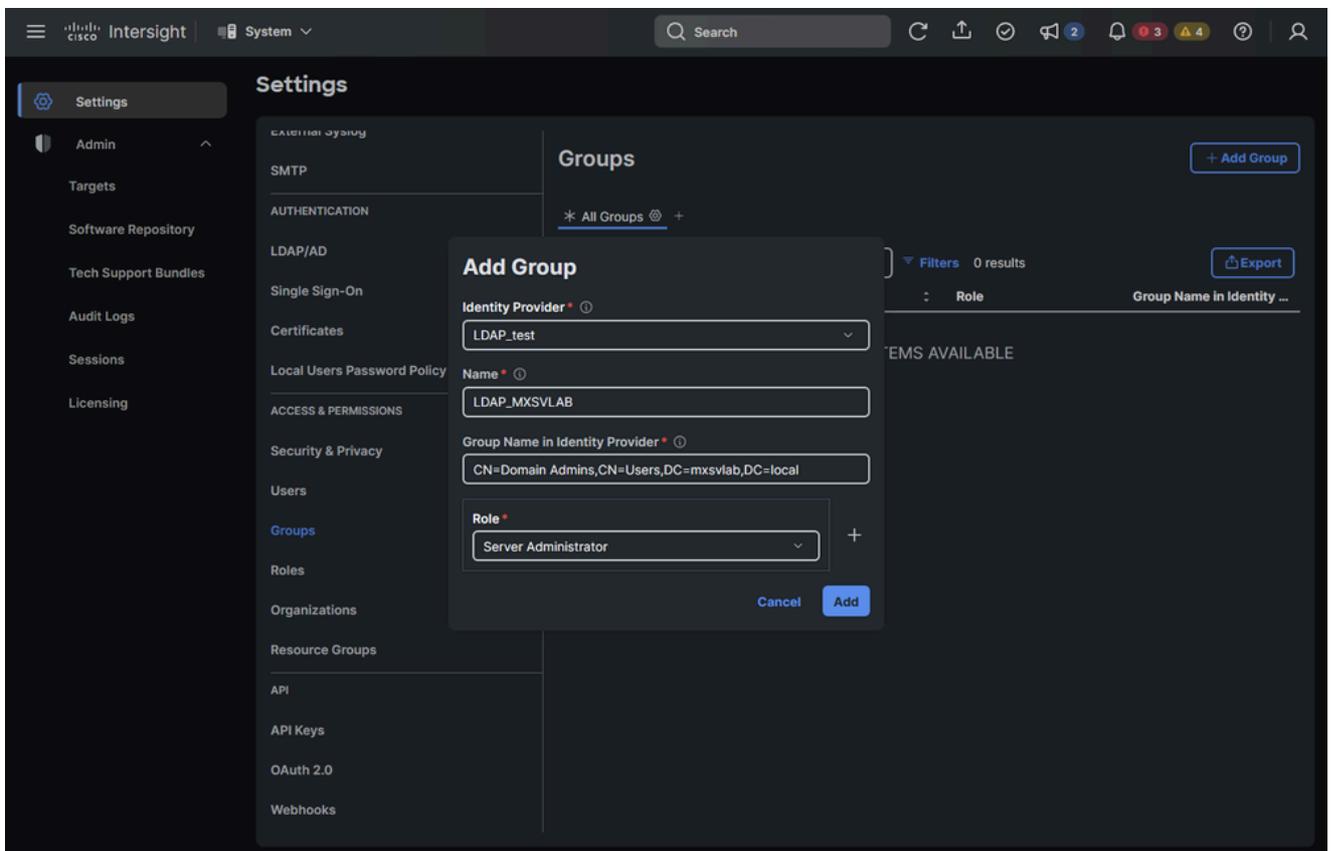
사용자 및 그룹 구성

워크플로 DeployApplianceLDAP가 완료되면 그룹 또는 개별 사용자를 구성할 수 있습니다.

그룹을 사용하기로 결정한 경우 해당 그룹에 속한 모든 사용자에게 권한이 제공됩니다. 개별 사용자를 사용하는 경우 고유한 권한 부여 역할을 가진 각 사용자를 추가해야 합니다.

그룹 구성

1. System(시스템) > Settings(설정) > ACCESS & PERMISSION(액세스 및 권한) > Groups(그룹)로 이동합니다.
2. Add Group(그룹 추가)을 클릭합니다.
3. ID 제공자를 선택합니다. LDAP 기본 설정 구성 섹션에서 설정한 이름입니다.
4. 그룹의 이름을 설정합니다.
5. ID 공급자에 그룹 이름 값을 입력합니다. LDAP 서버에 있는 그룹의 컨피그레이션과 일치해야 합니다.
6. 이 그룹의 사용자에게 제공하려는 액세스 레벨에 따라 역할을 선택합니다. [Intersight의 역할 및 권한을 참조하십시오.](#)



그룹의 컨피그레이션 예

사용자 구성

그룹 대신 개별 사용자를 구성하려는 경우 다음 지침을 따르십시오.

1. System(시스템) > Settings(설정) > ACCESS & PERMISSION(액세스 및 권한) > Users(사용자)로 이동합니다.
2. Add User(사용자 추가)를 클릭합니다.
3. Remote User(원격 사용자)를 선택합니다.
4. ID 제공자를 선택합니다. LDAP 기본 설정 구성 섹션에서 설정한 이름입니다.

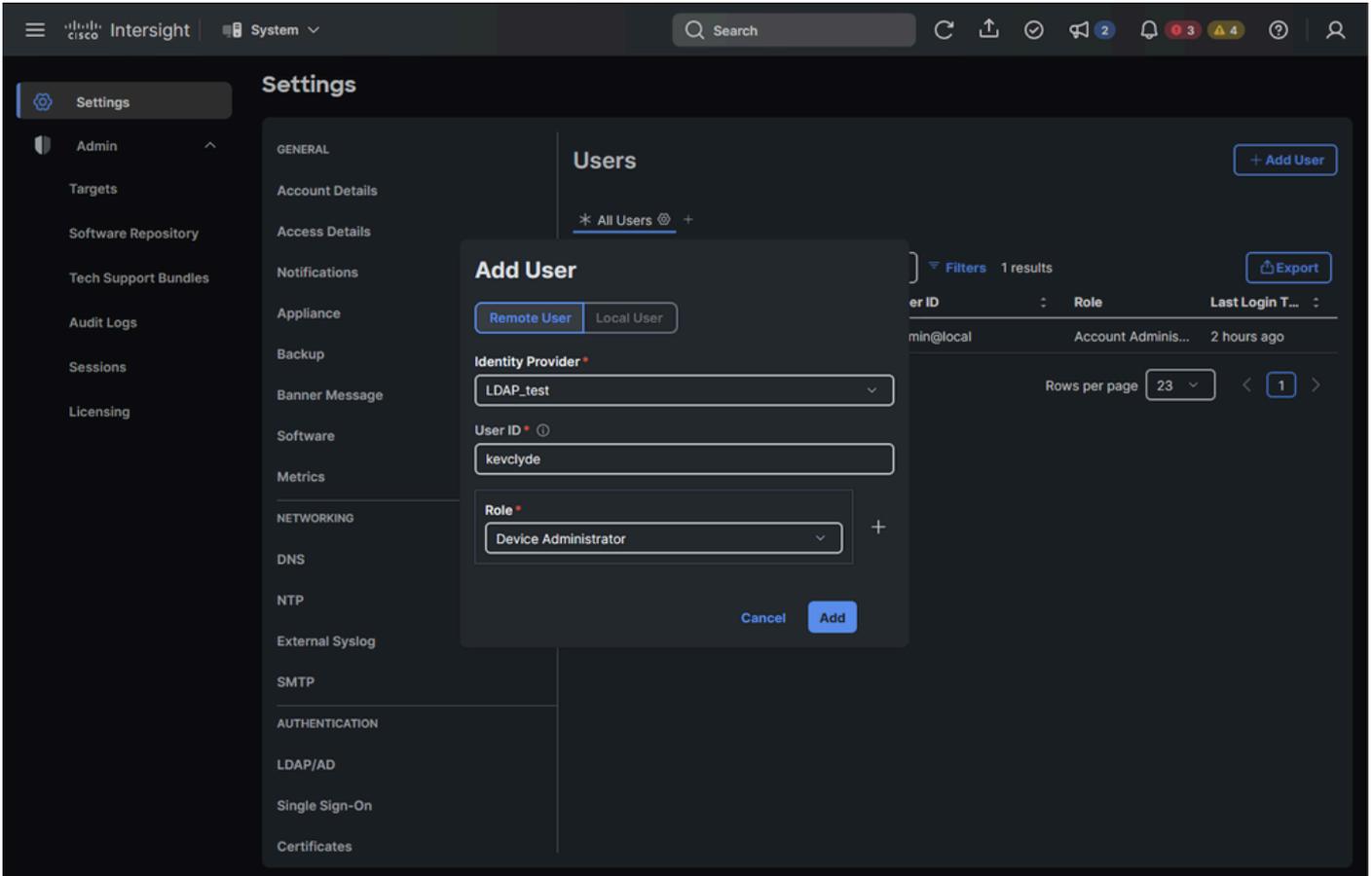
5. 사용자 ID를 설정합니다.



팁: 사용자 이름을 로그인 방법으로 사용하려면 User ID 필드에 LDAP 서버에서 sAMAccountName으로 구성된 값을 복사합니다.

이메일을 사용하려면 LDAP 서버의 mail 특성에서 사용자의 이메일을 설정해야 합니다.

6. 사용자에게 제공하려는 액세스 레벨에 따라 역할을 선택합니다. [Intersight의 역할 및 권한을 참조하십시오.](#)

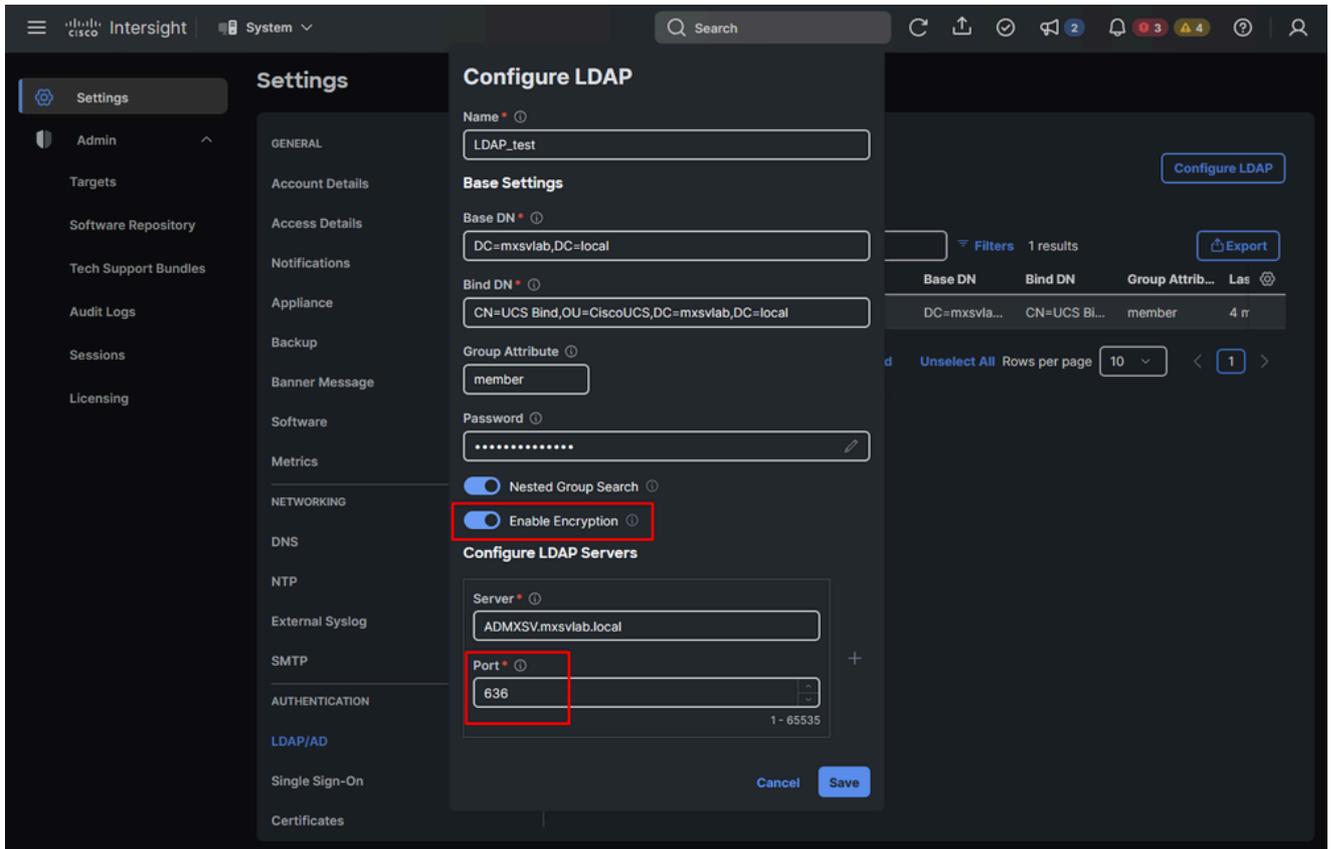


사용자에 대한 컨피그레이션 예

LDAPS(Secure LDAP) 컨피그레이션

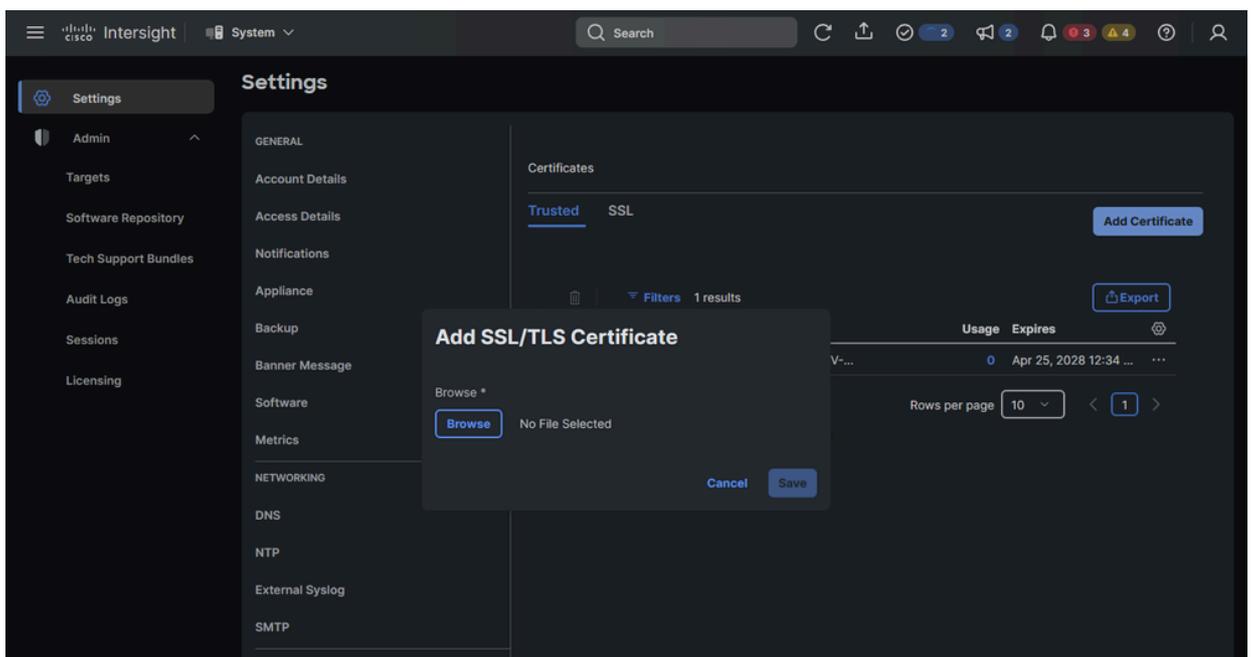
LDAP 통신을 암호화로 보호하려면 CA에서 서명한 인증서가 있어야 합니다. 이러한 변경 사항을 구성에 적용해야 합니다.

1. LDAP Basic Settings(LDAP 기본 설정) 컨피그레이션의 단계를 완료하되 Enable Encryption(암호화 활성화) 슬라이더를 오른쪽으로 이동합니다(3단계 g).
2. 사용된 포트가 LDAPS(보안)를 지원하는 포트인 636 또는 3269인지 확인합니다. 다른 모든 포트는 TLS를 통한 LDAP를 지원합니다.



보안 LDAP에 대한 컨피그레이션 변경

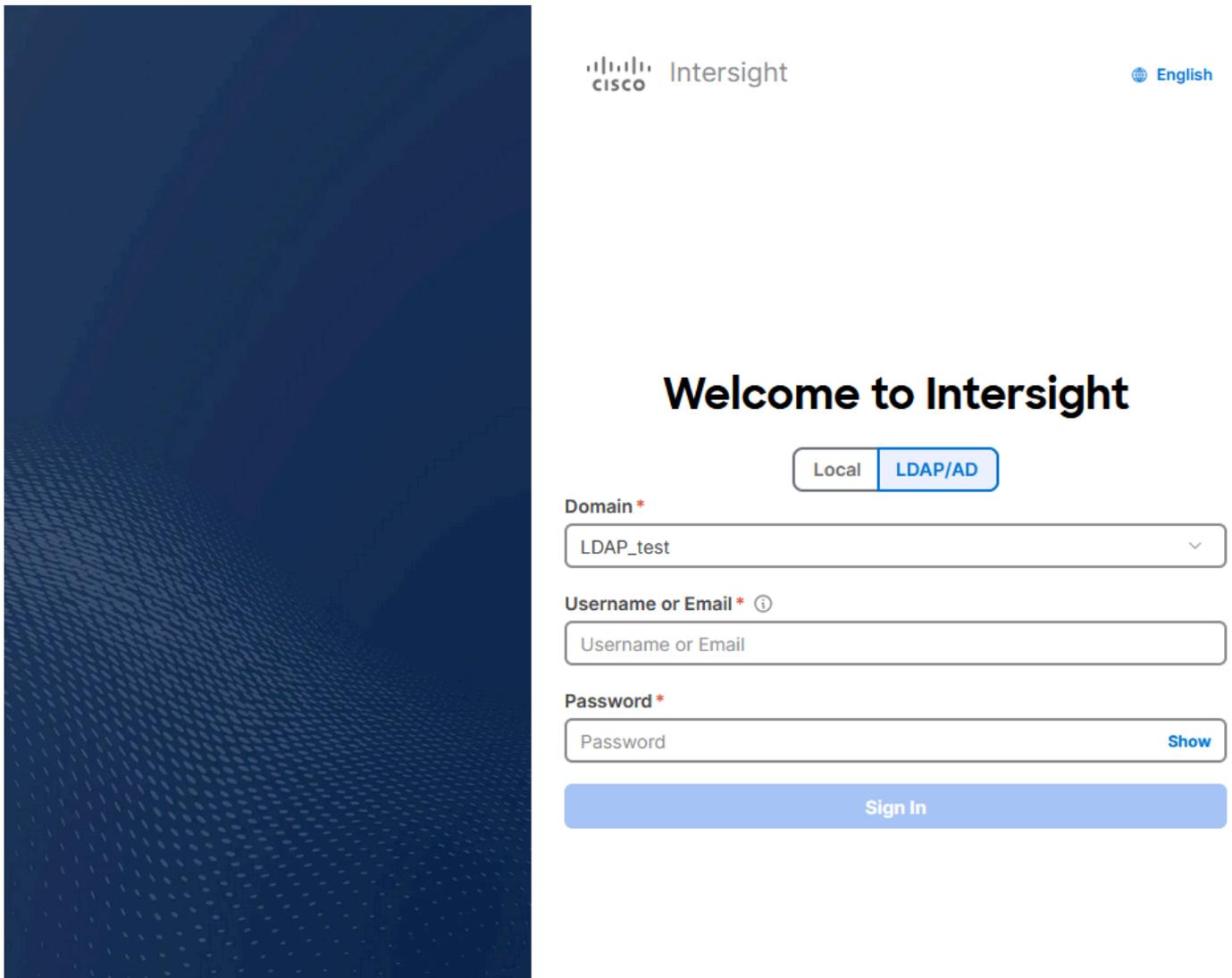
3. 컨피그레이션을 저장하고 워크플로 DeployApplianceLDAP가 완료될 때까지 기다립니다.
4. 다음 단계로 인증서를 추가합니다.
 1. System > Settings > AUTHENTICATION >으로 이동합니다. Certificates(인증서) > Trusted(신뢰할 수 있음).
 2. Add Certificate(인증서 추가)를 클릭합니다.
 3. Browse(찾아보기)를 클릭하고 CA에서 발급한 인증서가 포함된 .pem 파일을 선택합니다.



인증서를 추가하기 위한 구성

다음을 확인합니다.

브라우저에서 Intersight Virtual Appliance URL로 이동합니다. 이제 화면에 LDAP 자격 증명으로 로그인하는 옵션이 표시됩니다.



The screenshot shows the Intersight login interface. At the top left is the Cisco Intersight logo, and at the top right is a language selector set to 'English'. The main heading is 'Welcome to Intersight'. Below this, there are two tabs: 'Local' and 'LDAP/AD', with 'LDAP/AD' being the active tab. The 'Domain *' field is a dropdown menu with 'LDAP_test' selected. The 'Username or Email *' field has an information icon and contains the placeholder text 'Username or Email'. The 'Password *' field has a 'Show' button and contains the placeholder text 'Password'. At the bottom is a large blue 'Sign In' button.

로그인 화면에서 활성화된 LDAP 컨피그레이션

문제 해결

로그인이 실패하는 경우 오류 메시지는 무엇이 잘못되었을 수 있는지에 대한 힌트를 제공합니다.

오류 1. 잘못된 액세스 세부 정보

Notification Details



✖ LDAP login failed.

LDAP Authentication failed with the given credentials, LDAP Result Code 49. Check your username or password and try again.

Close

잘못된 암호 오류에 대한 오류 메시지

이 오류는 액세스 데이터가 잘못되었음을 의미합니다.

1. 사용자 이름 및 비밀번호가 올바른지 확인합니다.

오류 2. 잘못된 바인드 데이터

Notification Details



✖ LDAP login failed.

LDAP Authentication failed with the given bind credentials, LDAP Result Code 49. Check your BindDN and Bind password and try again.

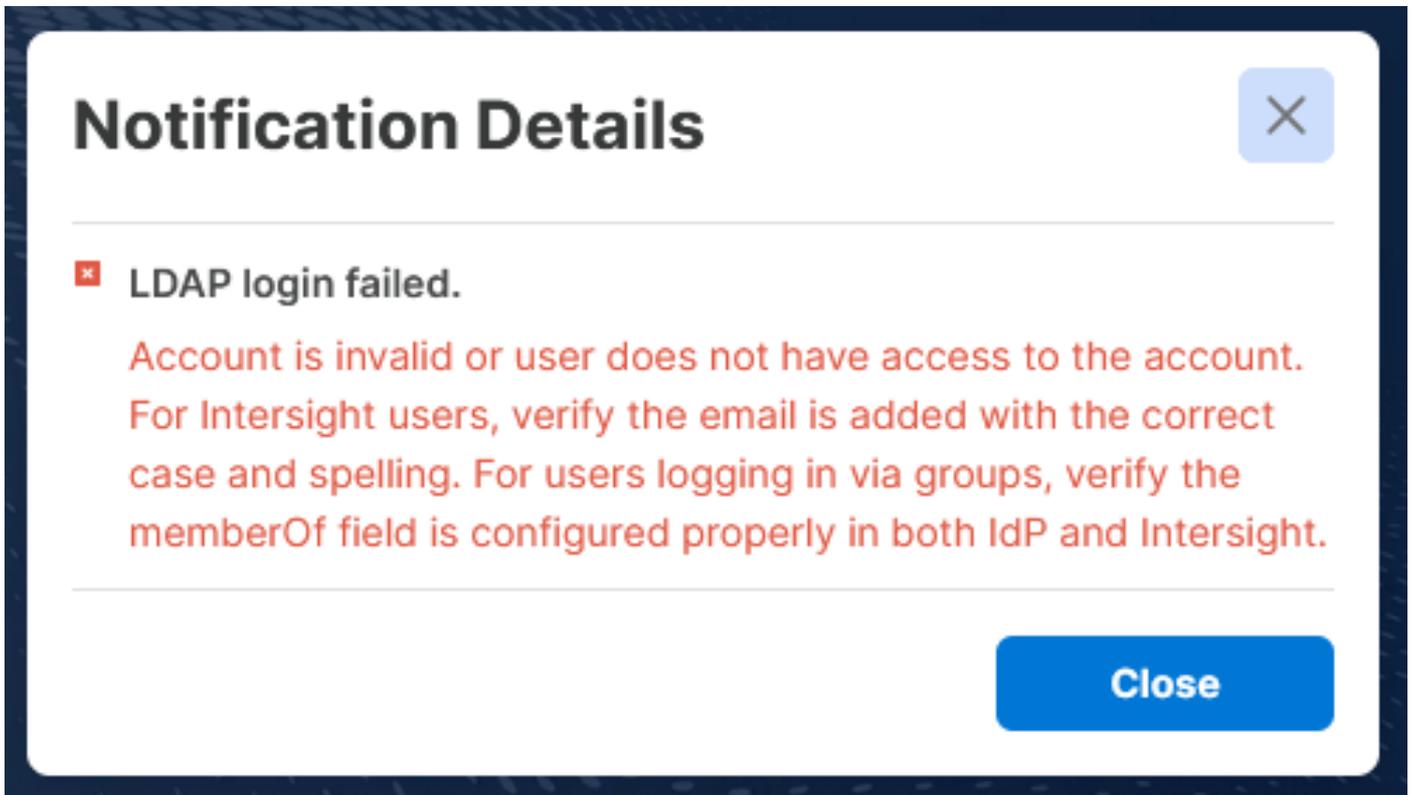
Close

잘못된 바인드 데이터에 대한 오류 메시지

이 오류는 바인드 데이터가 잘못되었음을 의미합니다.

1. BindDN을 확인합니다.
2. LDAP 설정에 구성된 바인드 비밀번호를 확인합니다.

오류 3. 사용자를 찾을 수 없습니다.

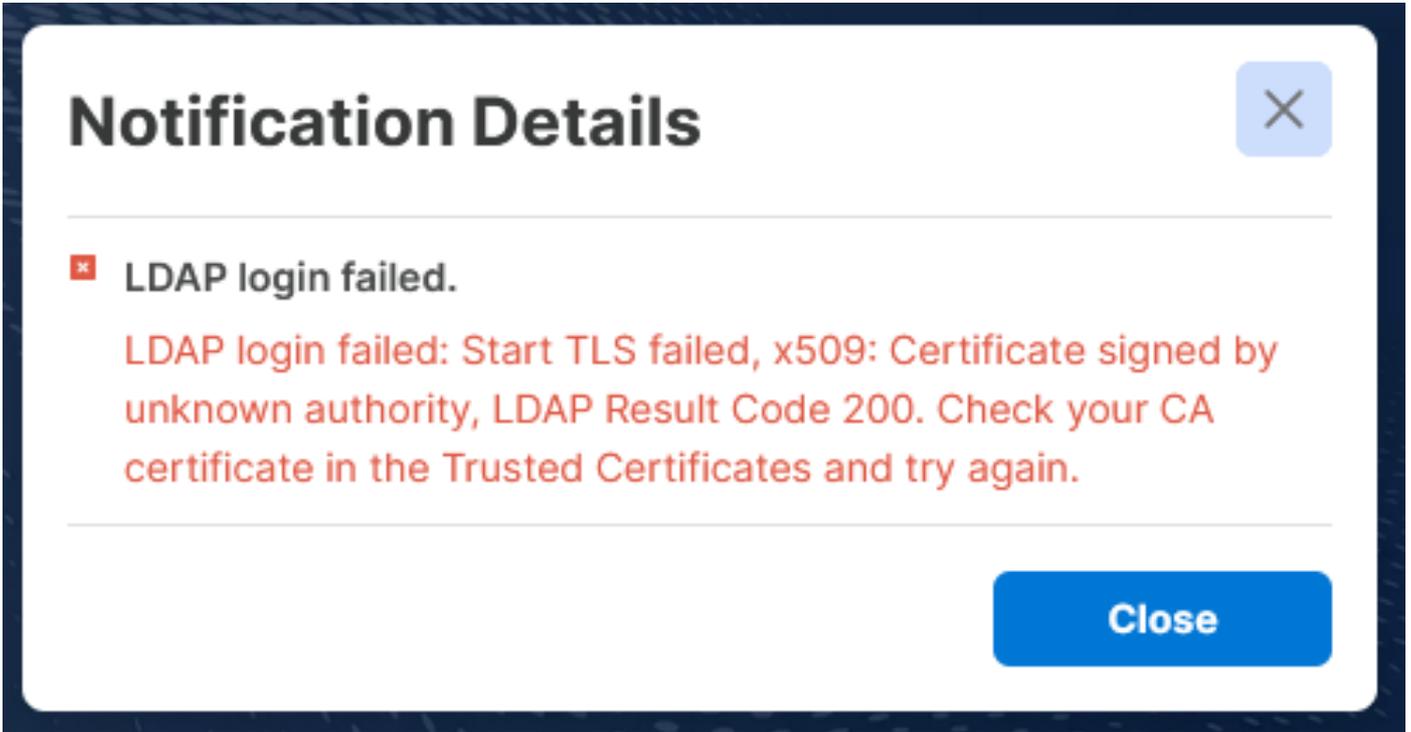


사용자에 대한 오류 메시지를 찾을 수 없음

이는 LDAP 서버의 검색이 인증된 사용자를 반환하지 않을 때 트리거됩니다. 다음 설정이 올바른지 확인합니다.

1. BaseDN을 선택합니다. 사용자를 찾는 데 사용된 매개변수가 잘못되었습니다.
2. 그룹 특성이 memberOf 대신 member로 설정되어 있는지 확인합니다.
3. 그룹 컨피그레이션의 ID 공급자에서 그룹 이름이 올바른지 확인합니다. 이는 그룹을 통해 권한 부여가 제공되는 경우에만 적용됩니다.
4. 사용자의 이메일이 사용자에 대한 AD 컨피그레이션의 mail 필드에 제대로 설정되어 있는지 확인합니다. 이는 개별 사용자에게 권한 부여가 제공되는 경우에만 적용됩니다.

오류 4. 잘못된 인증서

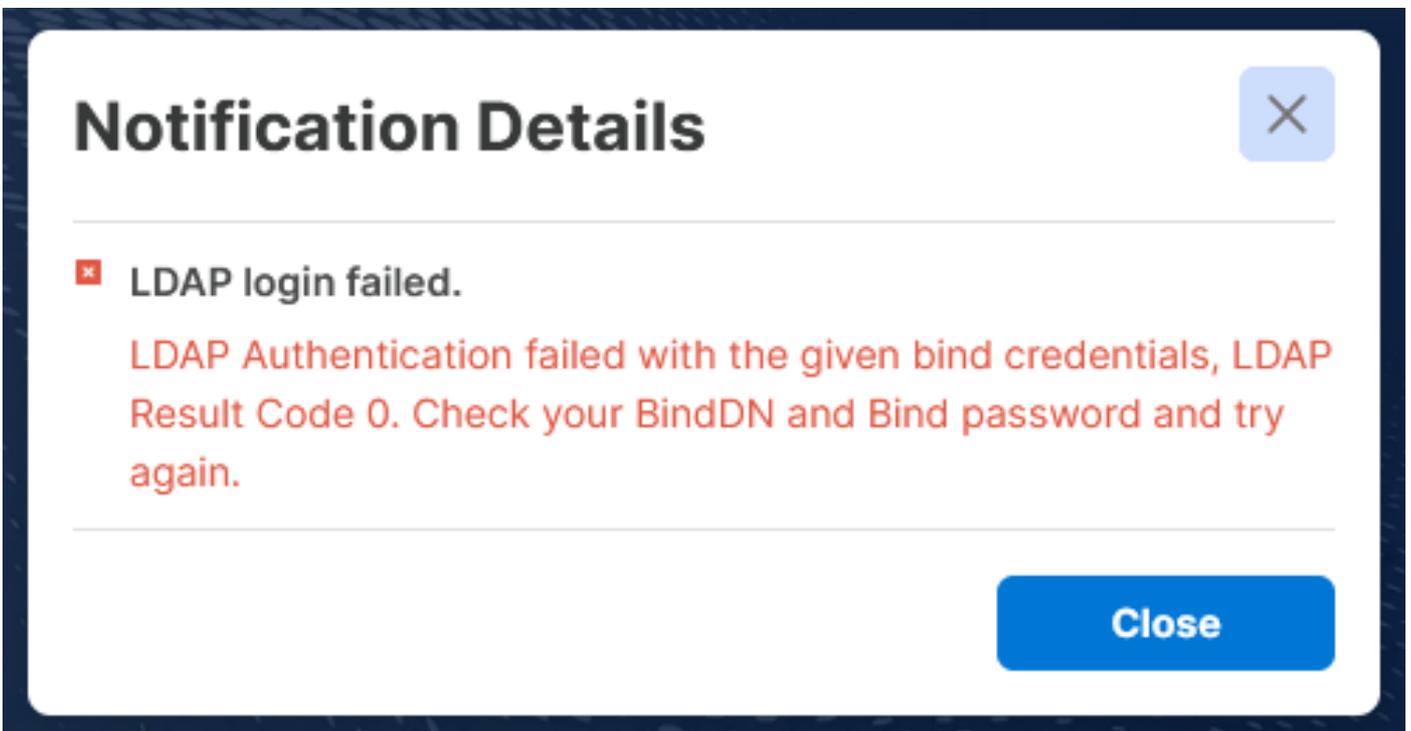


잘못된 인증서에 대한 오류 메시지

암호화된 LDAP가 활성화된 경우

1. 인증서가 구성되어 있고 올바른 전체 인증서가 포함되어 있는지 확인합니다.

오류 5. 암호화 사용이 보안 포트와 함께 사용됩니다.

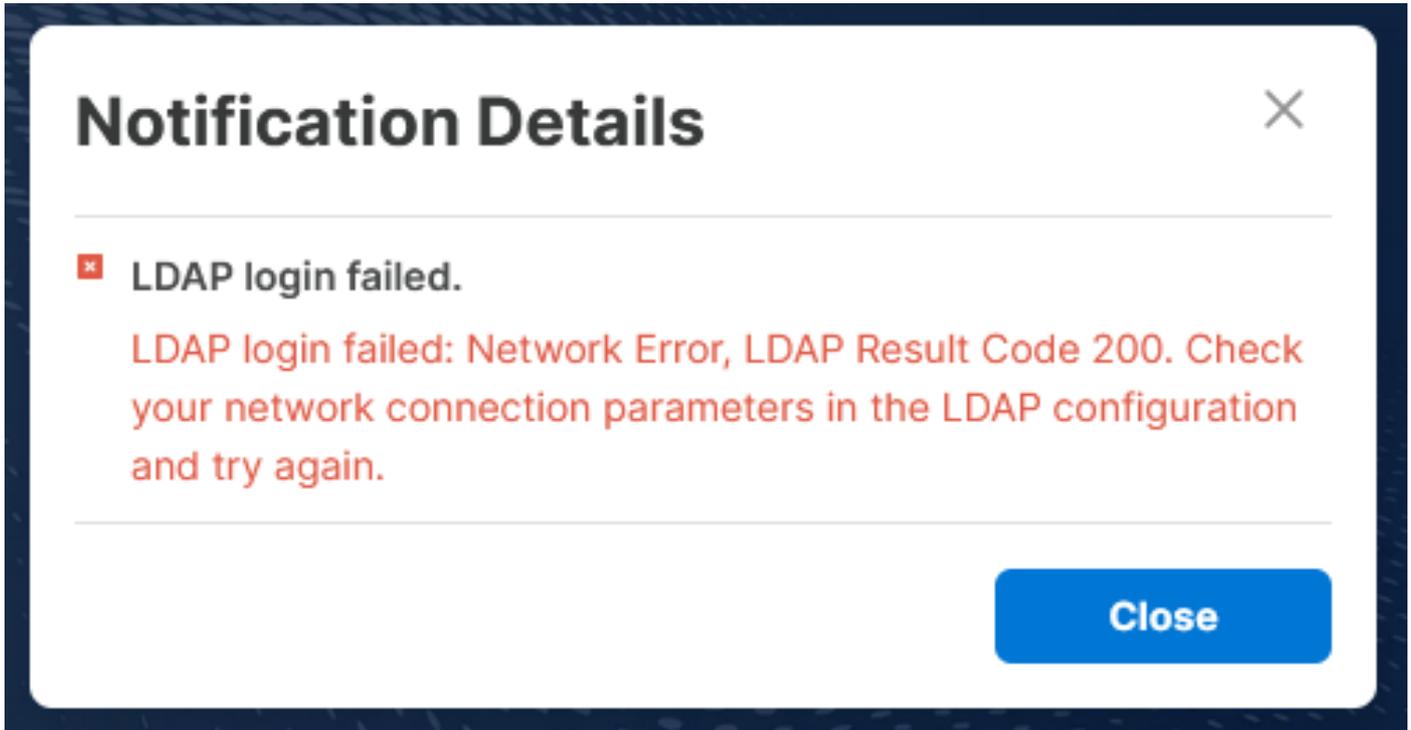


암호화 사용 오류 메시지 사용 안 함

이 오류는 암호화 사용이 활성화되지 않았지만 보안 LDAP용 포트가 구성된 경우에 나타납니다.

1. 암호화가 활성화되지 않은 경우 포트 389를 사용해야 합니다.

오류 6. 연결 매개 변수가 잘못되었습니다.



잘못된 포트에 대한 오류 메시지

이 오류는 LDAP 서버에 성공적으로 연결할 수 없었음을 의미합니다. 다음을 확인하십시오.

1. DNS 서버는 LDAP 서버의 호스트 이름을 올바른 IP로 확인해야 합니다.
2. Intersight 어플라이언스에서 LDAP 서버에 연결할 수 있습니다.
3. 포트 389가 암호화되지 않은 LDAP에 사용되는지, 636 또는 3269가 보안 LDAP(LDAPS)에 사용되는지, 기타 포트가 TLS에 사용되는지 확인합니다(암호화를 활성화하고 인증서 설정).

관련 정보

- [Cisco Intersight Virtual Appliance와 LDAP 통합\(비디오\)](#)
- [Intersight Appliance에서 LDAP 설정 구성](#)
- [Intersight의 역할 및 권한](#)
- [UCSM의 LDAP에 대한 샘플 컨피그레이션](#)

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.