Intersight Manage Mode(HTTP Device Console 및 SSH)에서 Fabric Interconnect에 대한 보안 LDAP 액세스 구성

목차

소개

이 문서에서는 LDAP 정책을 사용하여 Intersight SaaS 인스턴스에서 도메인 LDAP 인증을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 항목에 대한 지식:

- LDAP(Lightweight Directory Access Protocol) 프로토콜입니다.
- DNS(도메인 이름 서버) 서버.
- Cisco Intersight

사용되는 구성 요소

- Cisco Intersight SaaS 인스턴스
- Microsoft Active Directory
- DNS 서버
- Microsoft AD CS(Active Directory 인증서 서비스)

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 잘 알려진 프로토콜입니다. 이러한 디렉토리에는 사용자, 조직 및 리소스에 대한 정보가 저장됩니다. LDAP는 인증 및 권한 부여 프로세스에 사용할 수 있는 정보에 액세스하고 이를 관리하기 위한 표준 프로세스를 제공합니다.

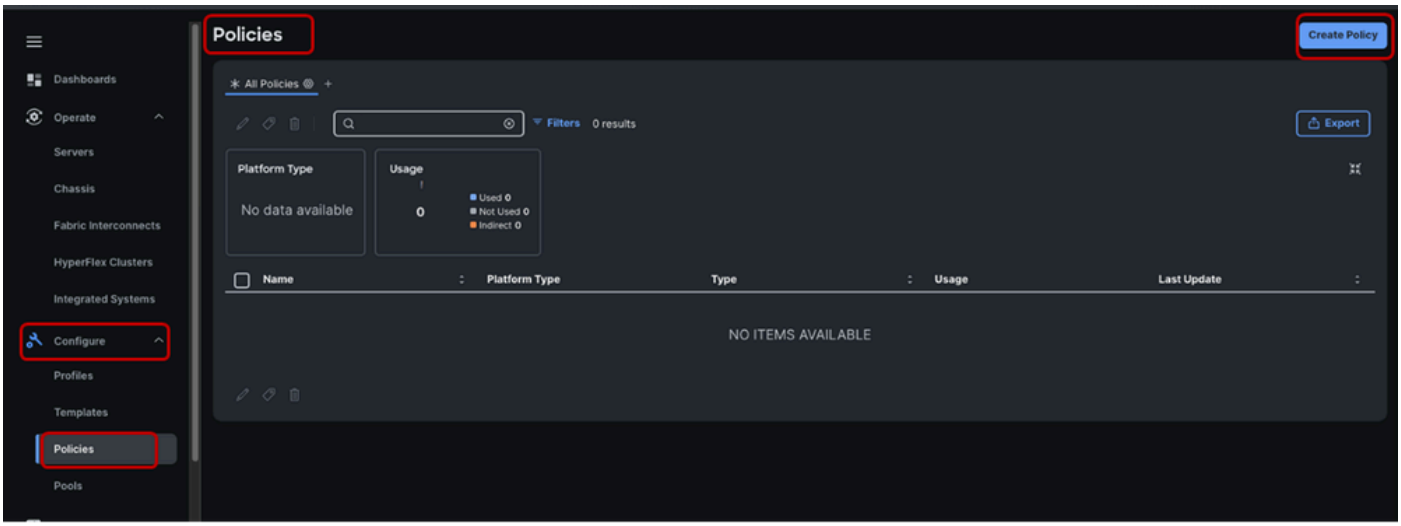
이 문서에서는 Intersight 관리 모드에서 Fabric Interconnect 피어의 디바이스 콘솔 또는 CLI(각각 HTTP 또는 SSH)에 대한 보안 LDAP를 통한 원격 인증을 위한 컨피그레이션 프로세스에 대해 설명합니다.

설정

LDAP 정책 구성

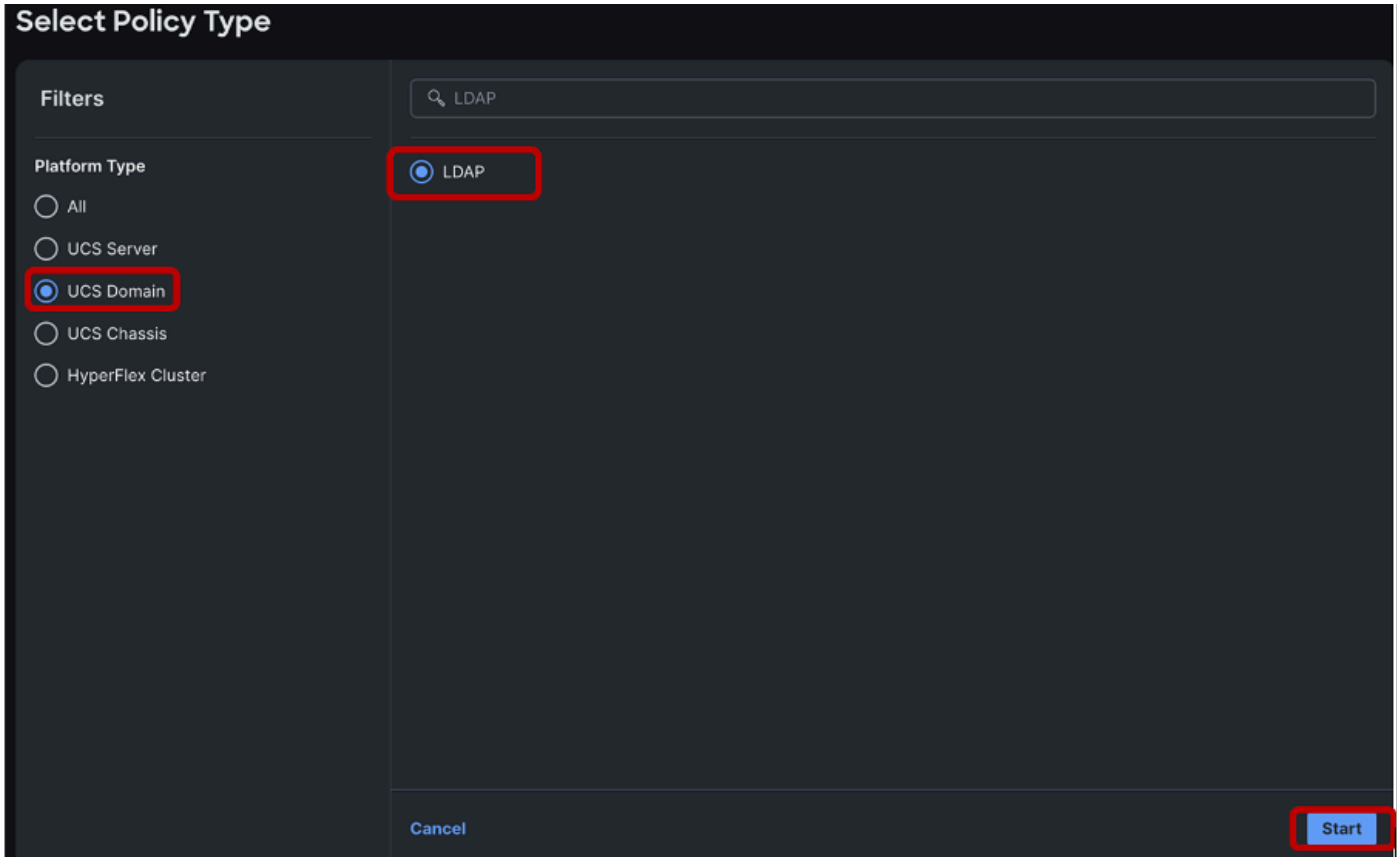
LDAP 정책을 구성하려면 Intersight SaaS 인스턴스에 로그인합니다.

Configure(구성) 섹션으로 이동하고 > Policies(정책)를 클릭합니다.
Policies(정책) 창 > Create Policy(정책 생성)로 이동합니다.

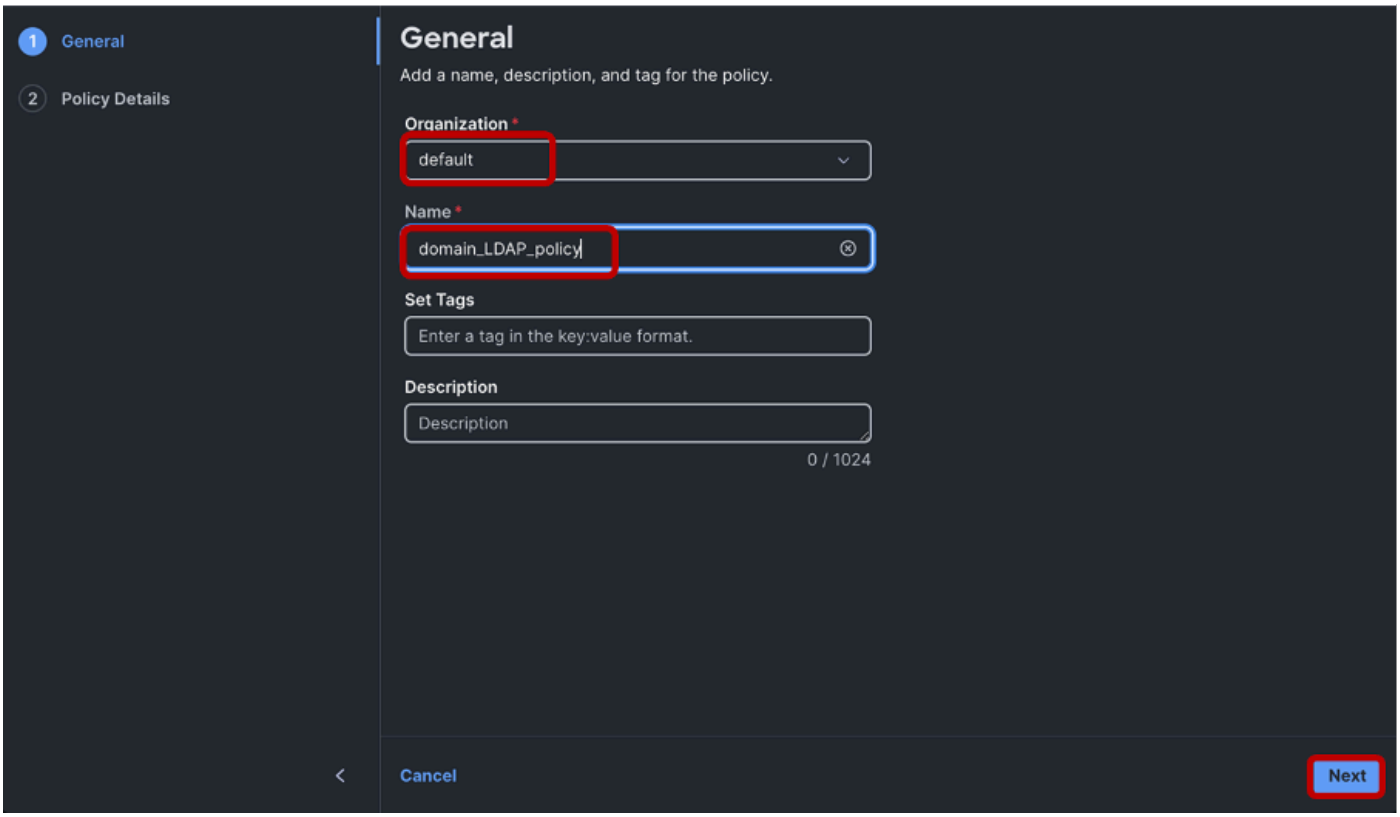


검색 막대에서 "LDAP"를 검색합니다.

LDAP 라디오 버튼을 선택하고 > Start(시작)를 클릭합니다.

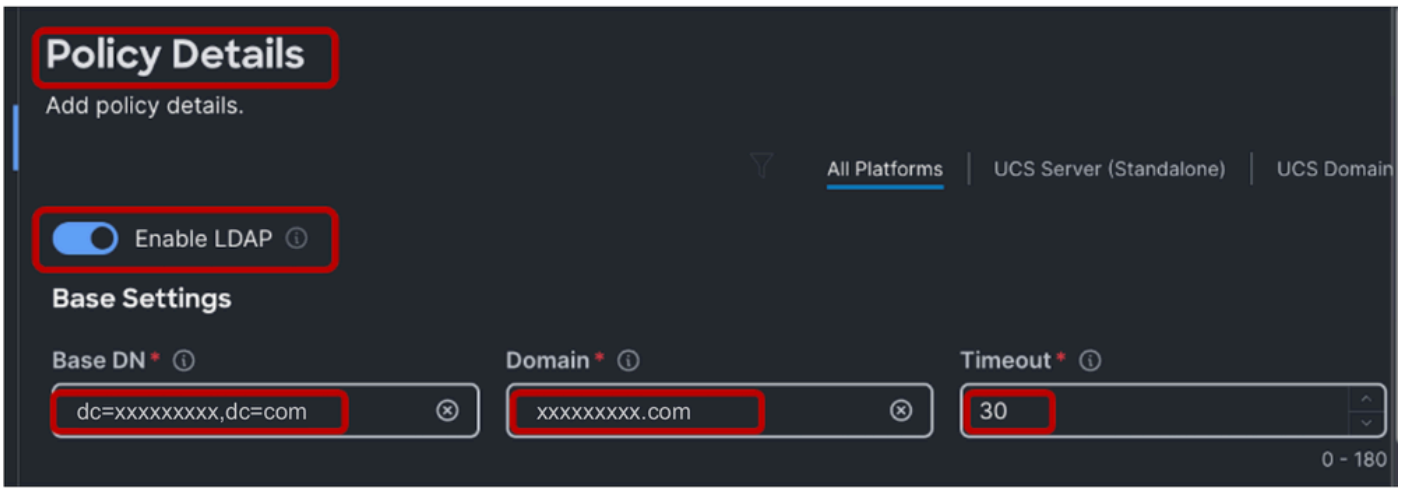


Create(생성) 창에서 > 원하는 Organization(조직)을 선택하고 > LDAP 정책의 이름을 지정하고 > Next(다음)를 클릭합니다.



Policy Details(정책 세부사항) 섹션에서 > Enable LDAP(LDAP 활성화) 슬라이더를 선택하고 Base DN, Domain(기본 DN), Timeout(시간 제한) 값을 채웁니다.

Timeout 값은 0~29로 설정된 경우 자동으로 30초로 설정됩니다. 이 데모에서 "xxxxxxxxx.com"은 LDAP 서버에 이미 구성된 도메인이며 30초 Timeout 값이 지정되었습니다.



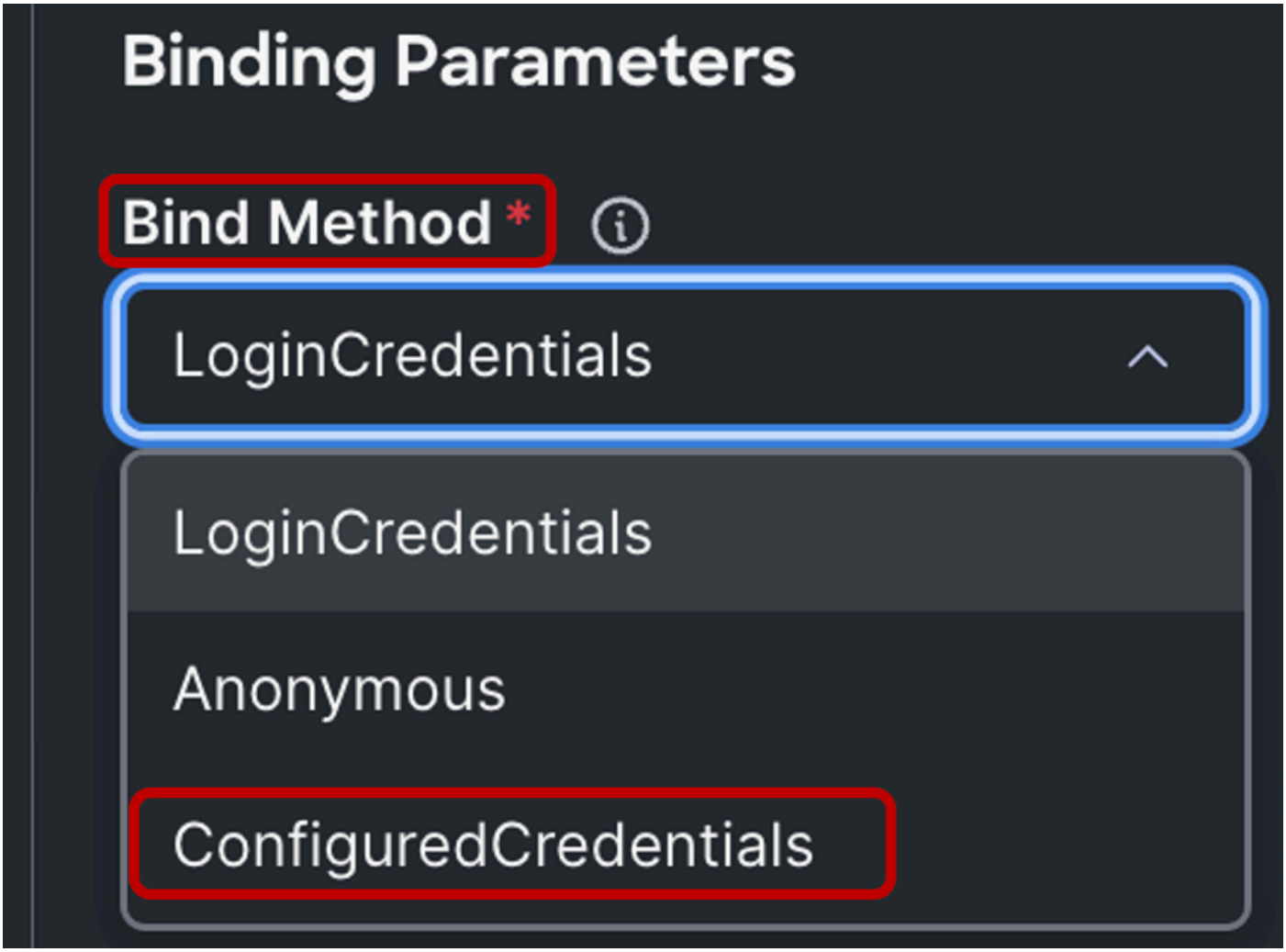
보안 LDAP를 구성하려면 Enable Encryption(암호화 활성화) 라디오 버튼을 활성화합니다.

참고: 일반적인 LDAP 컨피그레이션에서는 IP 주소 또는 FQDN을 사용할 수 있지만 서명된

인증서는 필요하지 않습니다. 따라서 "표준" LDAP를 구성할 때 Enable Encryption(암호화 활성화) 옵션, DNS Server Network Connectivity Policy(DNS 서버 네트워크 연결 정책) 및 인증서 관리 정책 컨피그레이션의 인증서를 무시할 수 있습니다. 보안 LDAP를 사용하려면 LDAP 서버 이름 확인 및 루트 인증서에 대해 구성된 DNS 서버가 필요합니다.

Binding Parameters(바인딩 매개변수) 섹션에서 기본 설정은 LoginCredentials(바인드 작업에 대해 사용자 LDAP 자격 증명을 인증하는 개별 사용자를 활용함)입니다. 이렇게 하면 전용 바인드 사용자를 구성할 필요가 없습니다.

이 데모에서는 Bind 사용자가 구성됩니다. 따라서 "Bind Method(바인드 메서드)"가 "ConfiguredCredentials(구성된 자격 증명)"로 변경됩니다.

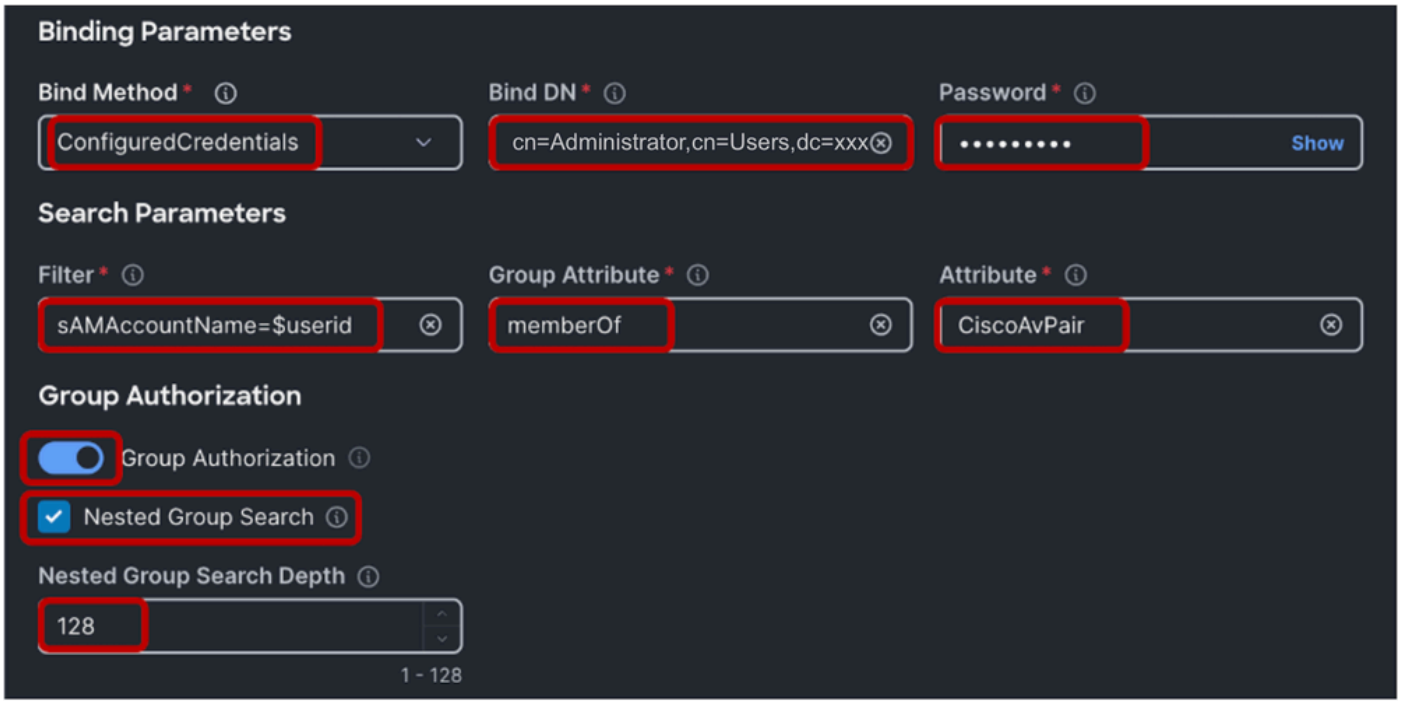


그런 다음 Bind DN(Bind User) 및 Bind User Password를 추가합니다. Windows Active Directory에서 구성하는 모든 사용자가 될 수 있습니다. 이 데모에서는 Administrator 사용자가 사용됩니다.

'cn=Administrator,cn=Users,dc=xxxxxxxxx,dc=com'입니다.

Search Parameters(매개변수 검색) 섹션의 Filter(필터)에 "sAMAccountName=$userid"를 입력합니다.

Group Attributes(그룹 특성)에 "memberOf"를 추가하고 Attribute(특성) 필드에 "CiscoAvPair"를 추가합니다. LDAP 서버 컨피그레이션에 따라 Group Authorization(그룹 권한 부여) 및 Nested Group Search(중첩 그룹 검색)를 활성화할 수 있습니다. 이 데모에서는 기본 Nested Group Search Depth at 128이 사용됩니다.



"Configure LDAP Servers(LDAP 서버 구성)" 섹션 > LDAP 서버 IP 주소 또는 FQDN(Secure LDAP에 필요) 및 포트 번호(389)를 입력합니다.

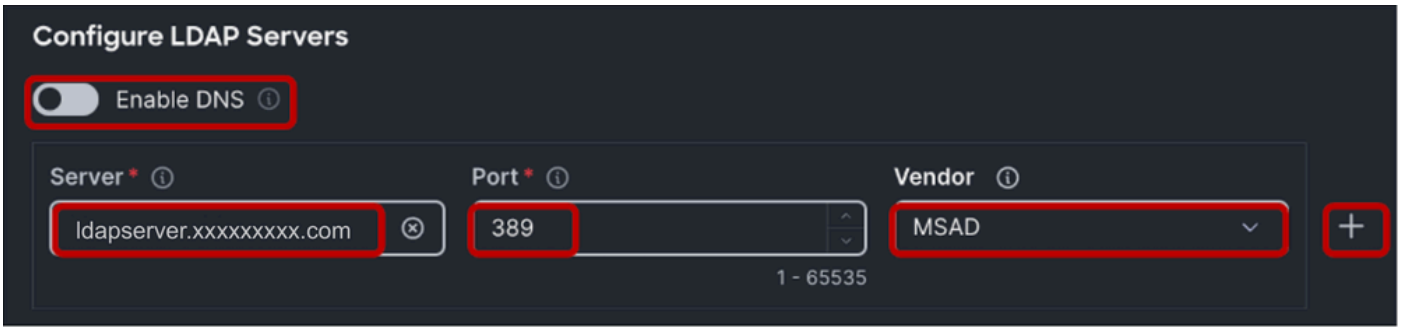
UCS의 보안 LDAP는 STARTTLS를 사용하여 포트 389를 사용하는 암호화된 통신을 활성화합니다.

포트를 389에서 636으로 수정하면 인증 오류가 발생할 수 있습니다. Cisco UCS는 SSL을 위해 포트 636에서 TLS 협상을 수행합니다. 그러나 초기 연결은 항상 포트 389에서 암호화되지 않은 상태로 설정됩니다.

LDAP Server Vendor를 선택합니다. 사용 가능한 공급업체 옵션은 OpenLDAP 및 MSAD(Microsoft Active Directory)입니다. 이 데모에서는 사용 중인 LDAP 서버가 Windows Server 2019이므로 MSAD가 사용됩니다.

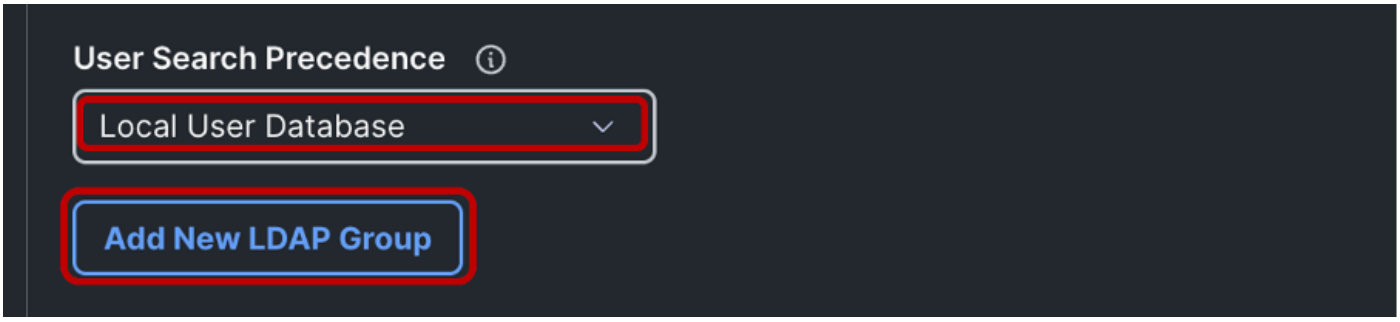
UCS 도메인의 LDAP 컨피그레이션에는 이 옵션을 적용할 수 없으므로 Enable DNS(DNS 활성화) 버튼을 OFF(끄기)로 둡니다.

구성된 LDAP 서버의 맨 오른쪽에 있는 "+" 아이콘을 클릭하여 여러 LDAP 서버를 구성할 수 있습니다.

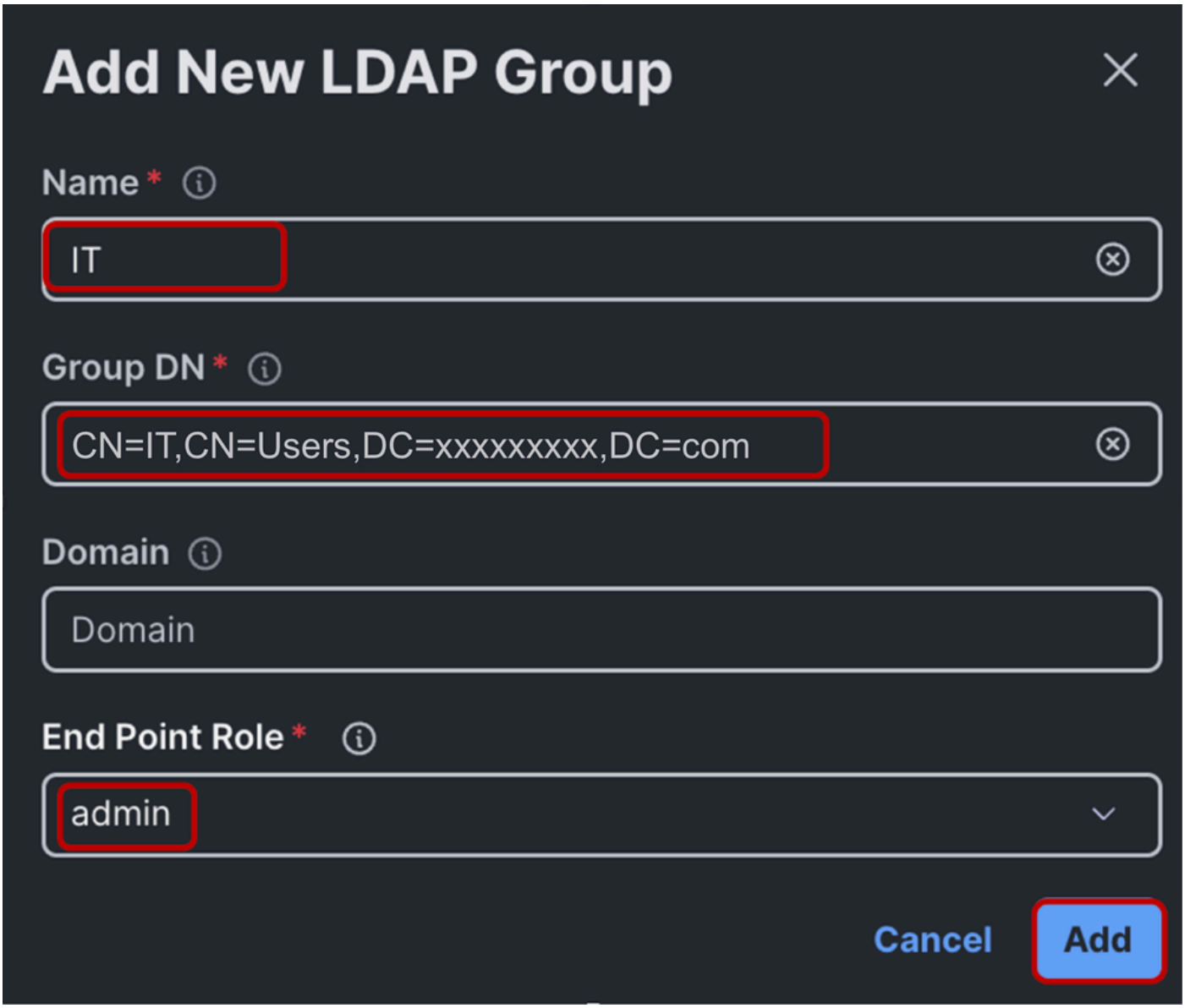


참고: 사용자 검색 우선 순위를 로컬 사용자 데이터베이스로 유지하거나 사용 사례에 따라 LDAP 사용자 데이터베이스로 변경할 수 있습니다.

그런 다음 Add New LDAP Group(새 LDAP 그룹 추가) 버튼을 클릭하여 LDAP 서버에 구성된 그룹에 해당하는 그룹 DN을 추가합니다.



그룹의 이름을 지정하고 LDAP 서버에서 받은 그룹 DN을 추가한 다음 원하는 엔드포인트 역할을 선택합니다.

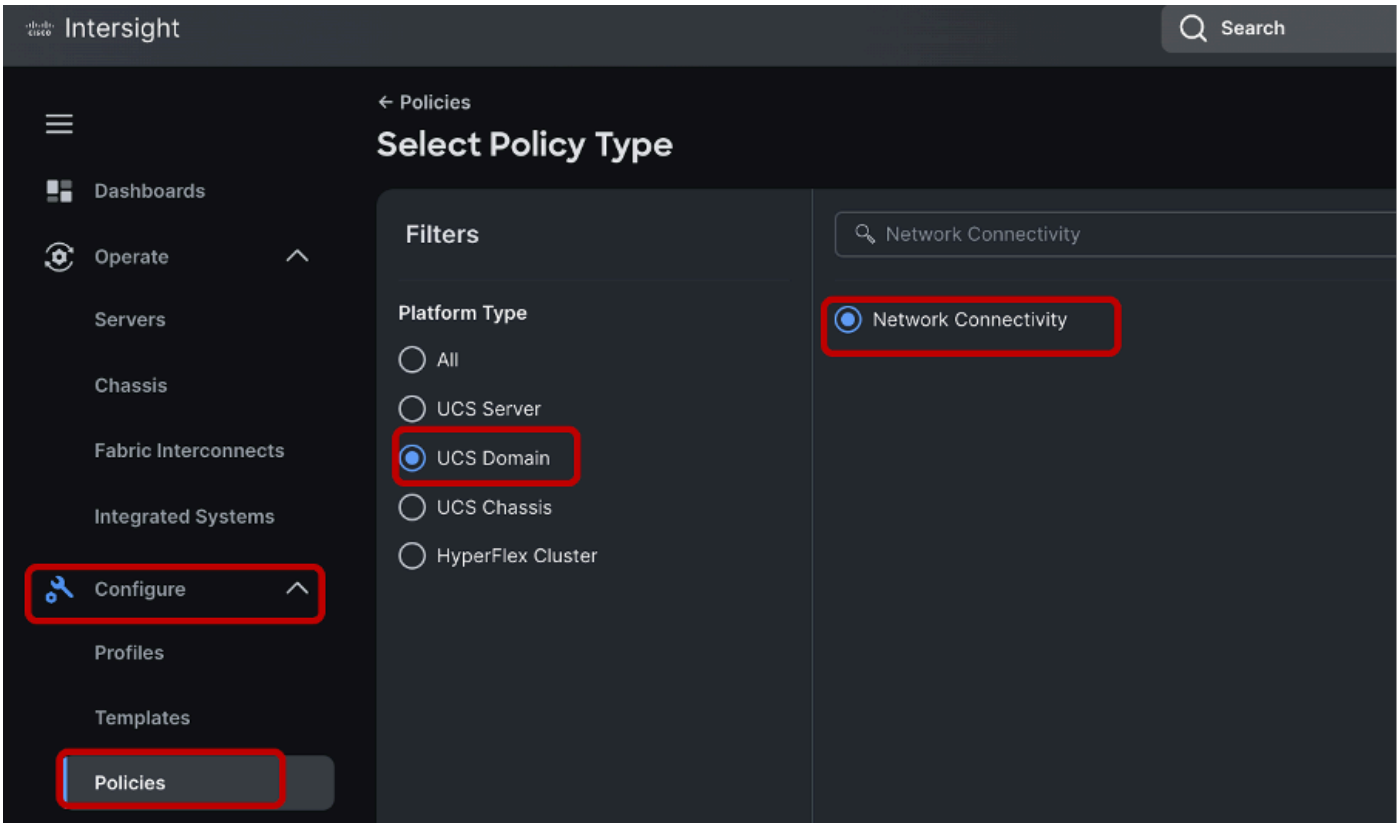


Add(추가) > Select Create(생성 선택)를 클릭하여 LDAP 정책을 생성합니다

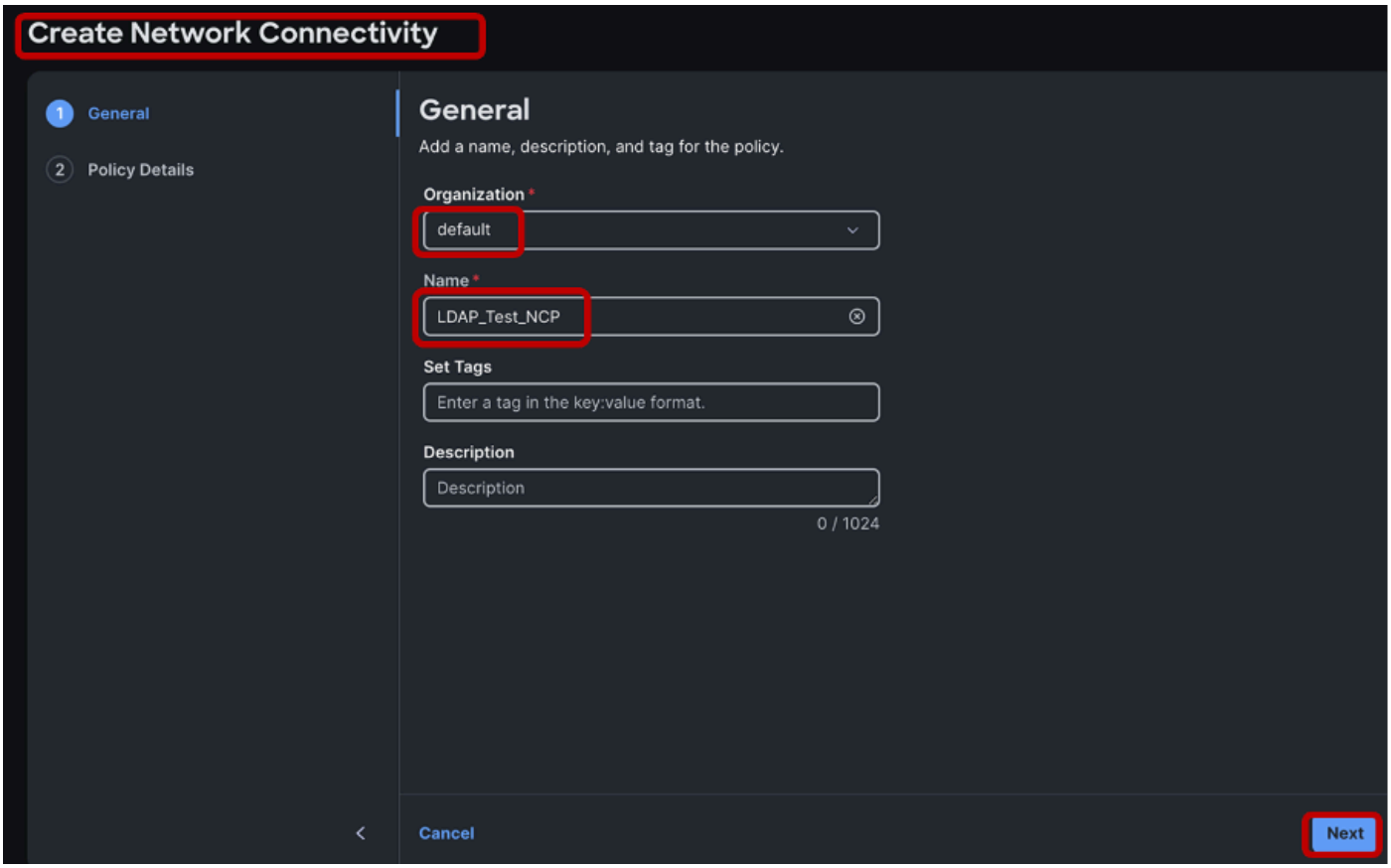
참고: 도메인 LDAP 정책 컨피그레이션의 경우 이 문서를 생성할 때 "admin"만 엔드포인트 역할로 지원됩니다.

네트워크 연결 정책 구성

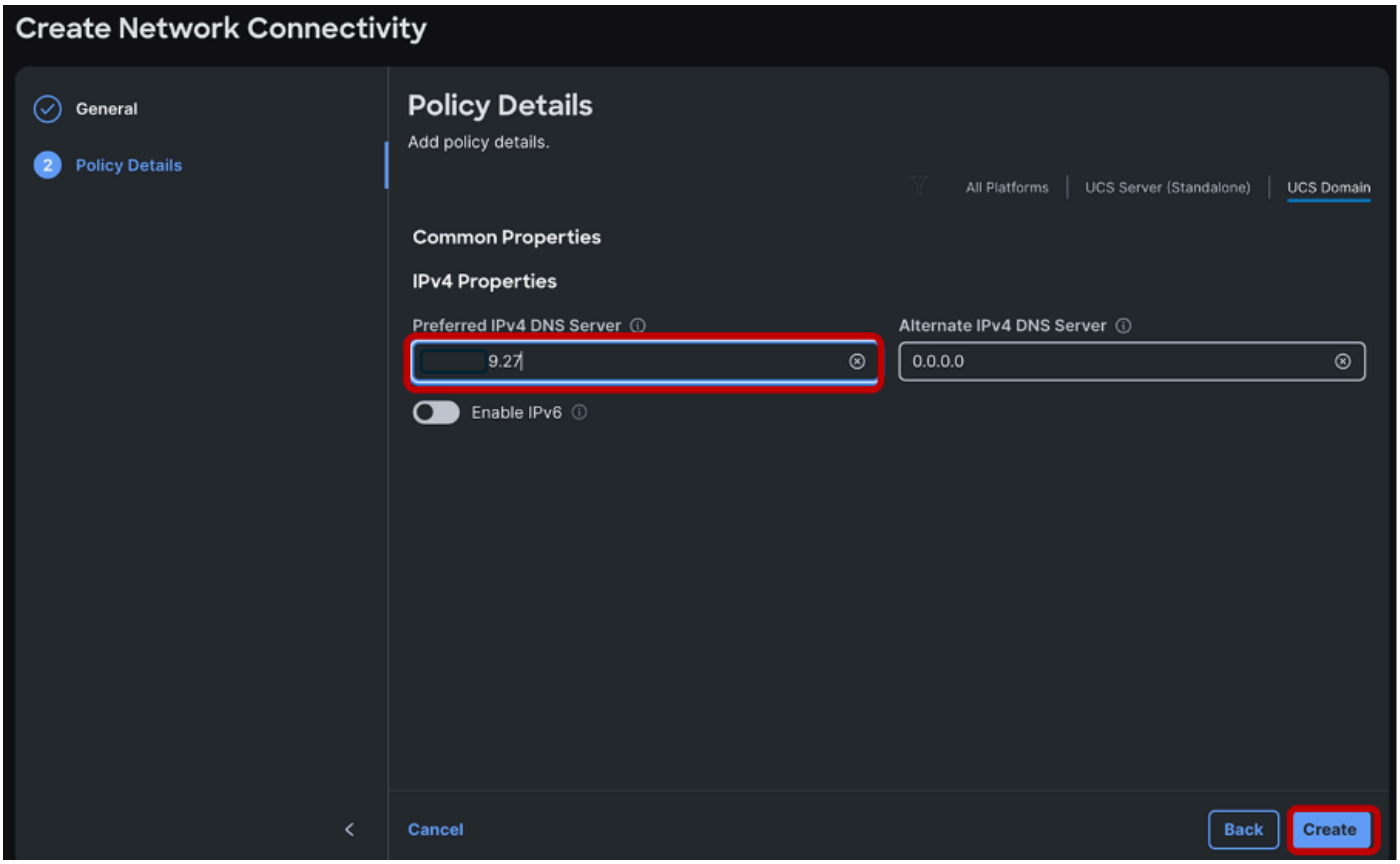
네트워크 연결 정책을 생성하여 UCS 도메인에 대한 DNS 서버를 구성합니다.



적절한 조직을 선택하고 > 정책의 이름을 입력하고 > 다음을 클릭합니다.



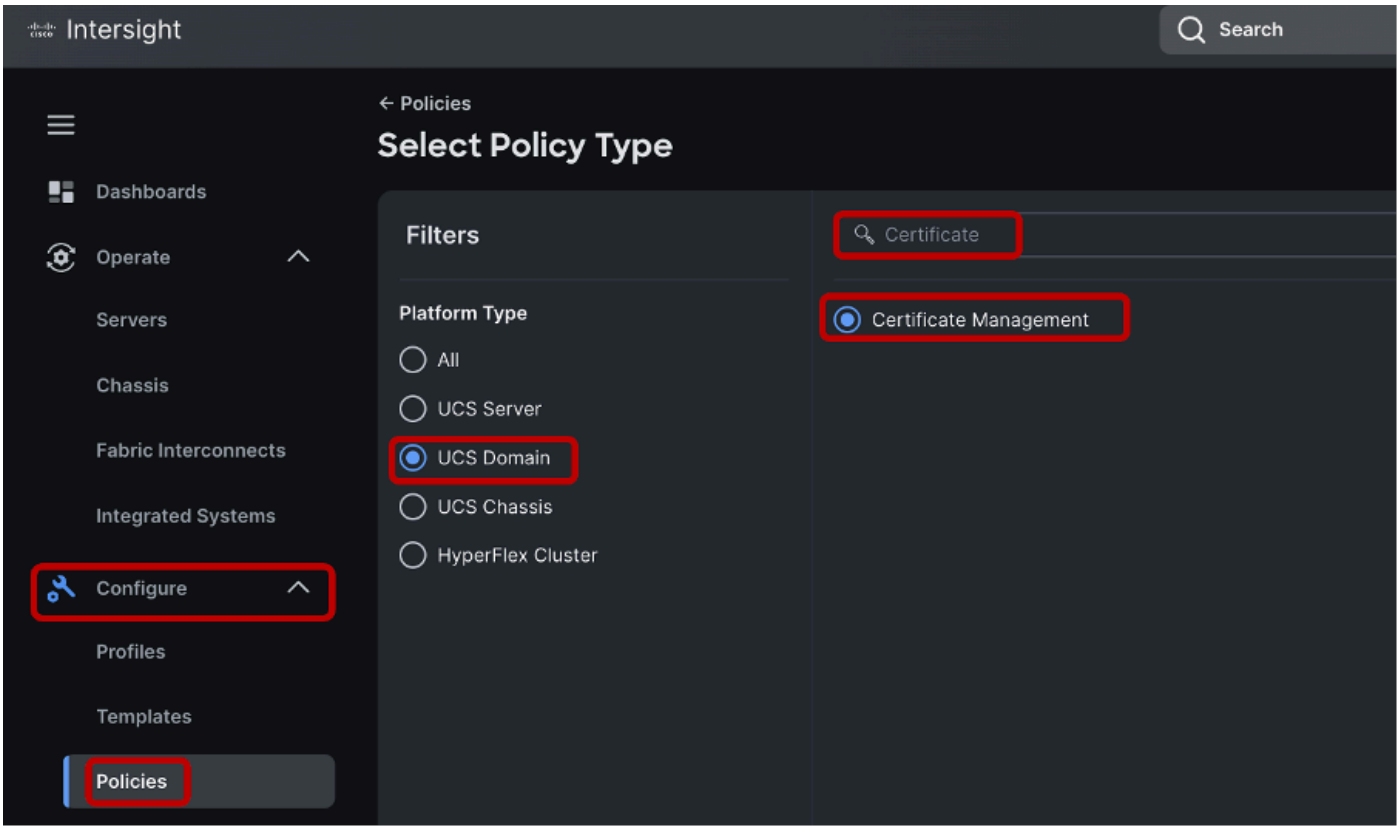
Preferred DNS server IPv4 주소를 정의하고 Create(생성)를 클릭하여 정책을 저장합니다.



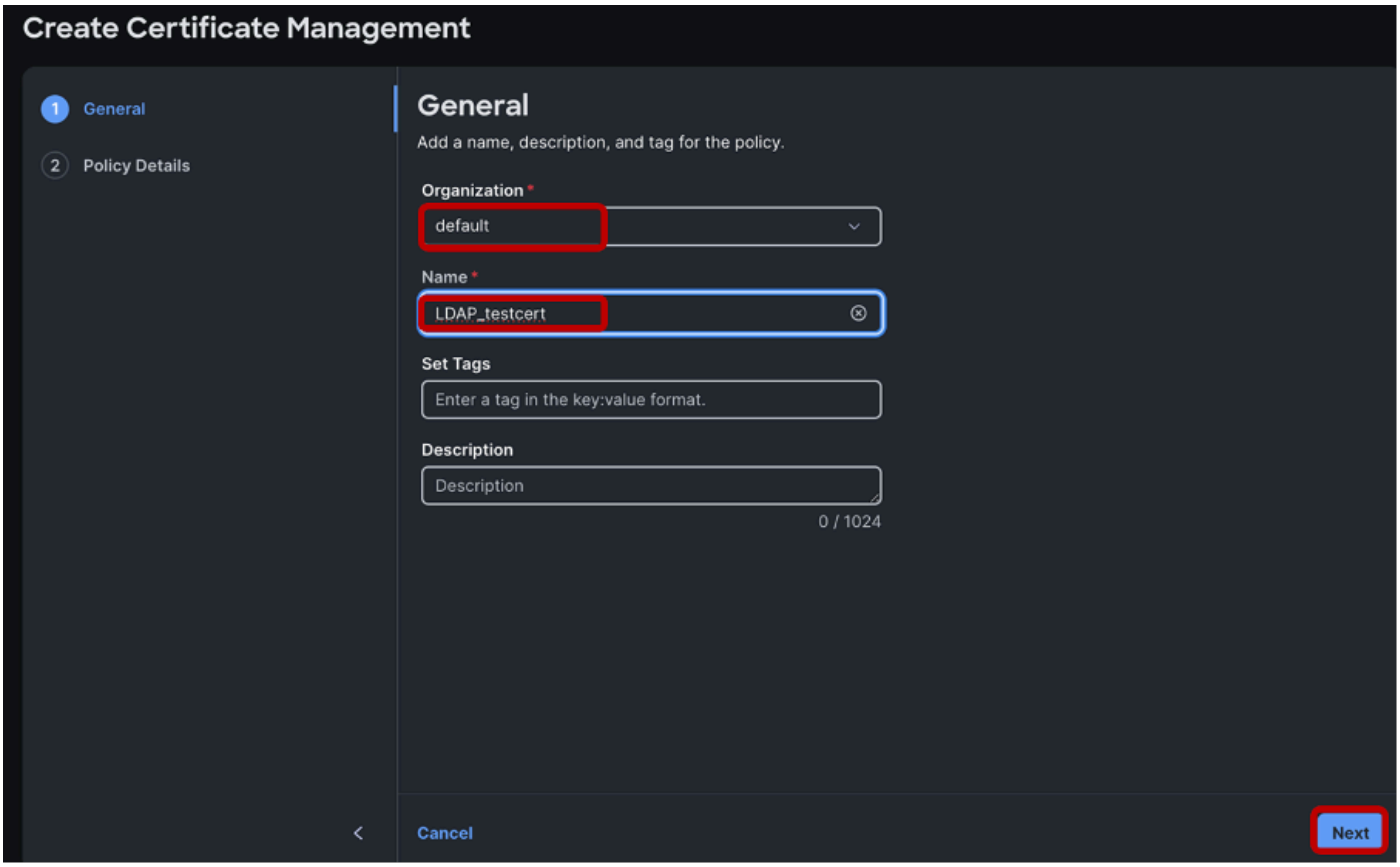
DNS 서버 IP 주소가 구성되어 있고 이름 확인을 위해 연결할 수 있는지 확인합니다. 이름 확인이 도메인 내의 LDAP 서버 및 Fabric Interconnect에서 작동하는지 확인합니다. 이 데모에서는 DNS 서버가 LDAP 서버와 동일한 Windows 시스템 인스턴스에 있습니다.

인증서 관리 정책 구성

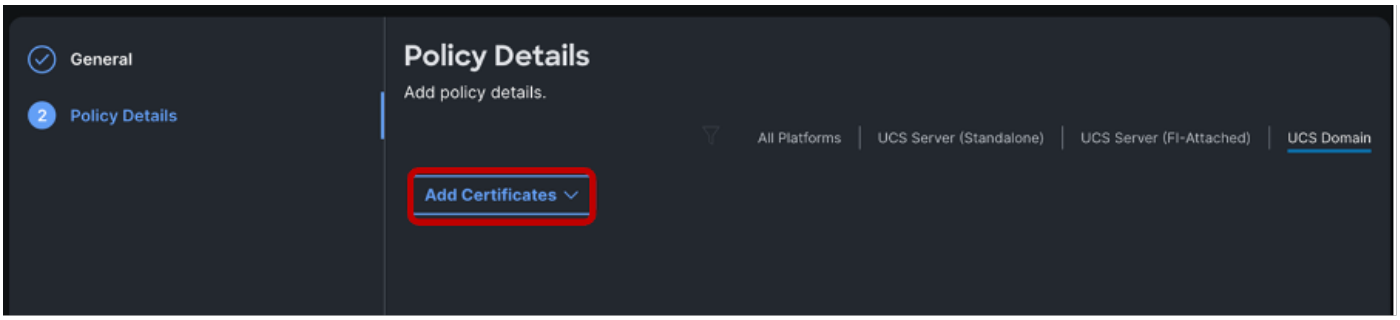
다음으로 인증서 관리 정책을 구성합니다. 이는 LDAP 암호화가 작동하기 위해 필요합니다.



적절한 조직을 선택하고 정책의 이름을 지정한 후 Next(다음)를 클릭합니다.

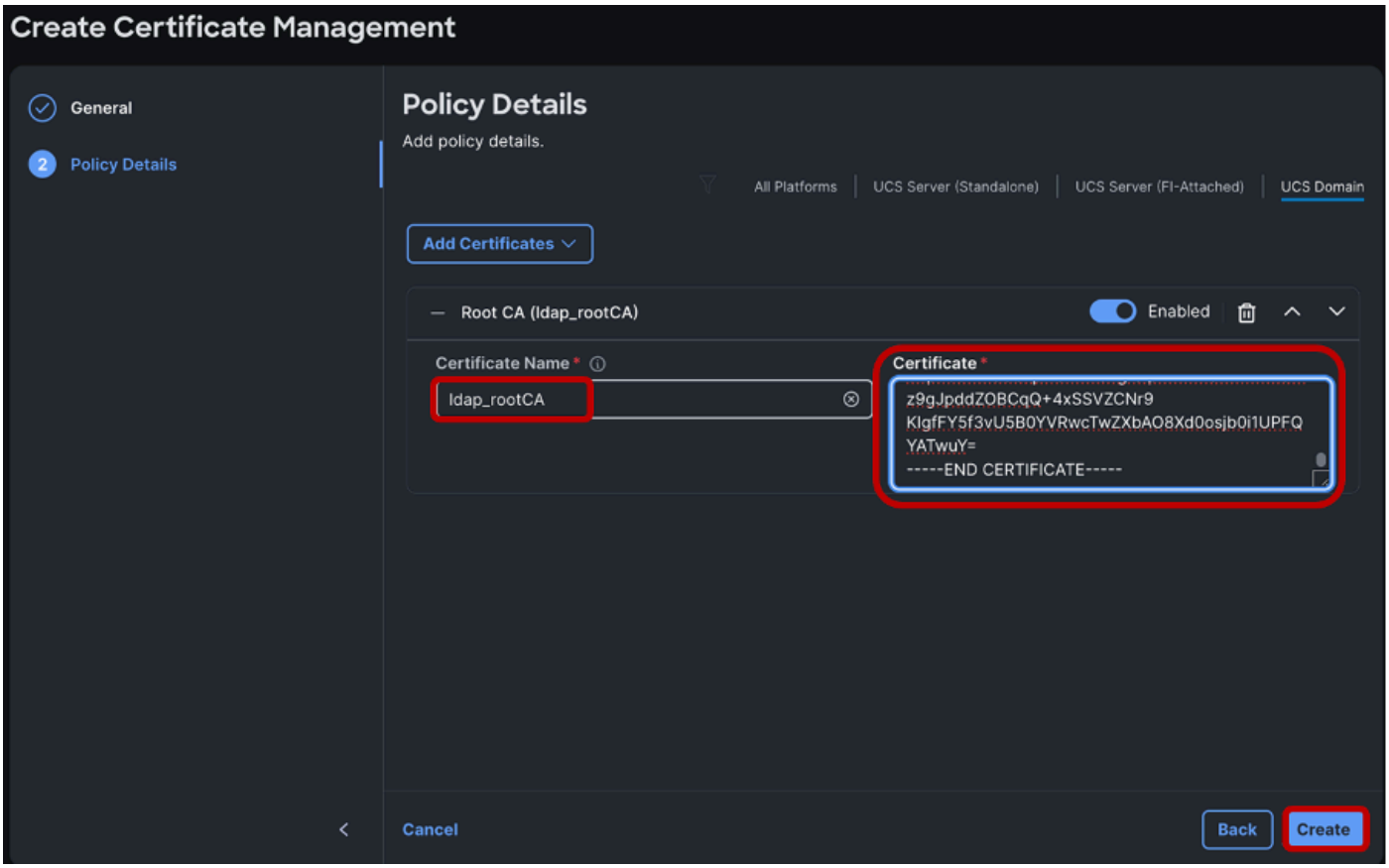


Add Certificates를 클릭합니다.

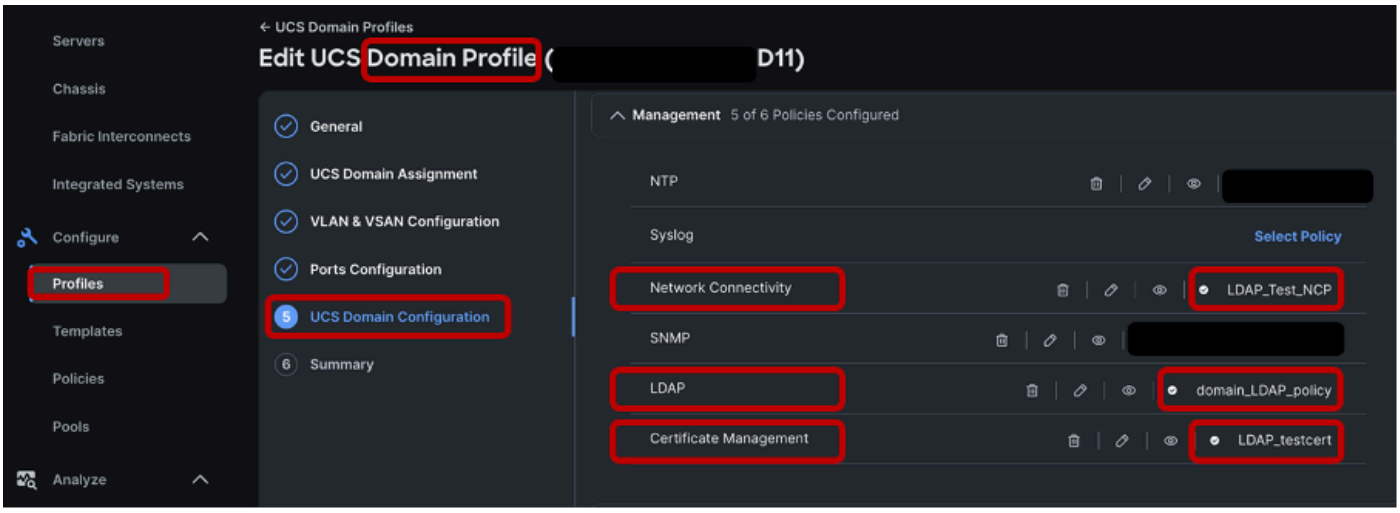


인증서의 이름을 지정하고 Microsoft Active Directory 인증서 서비스의 루트 인증서에 붙여넣습니다 .

Create(생성)를 클릭합니다.



LDAP, 네트워크 연결 및 인증서 관리 정책이 생성된 후, 그림과 같이 "UCS Domain Configuration(UCS 도메인 컨피그레이션)" 섹션의 원하는 도메인 프로필에서 새로 생성된 정책을 참조하십시오.



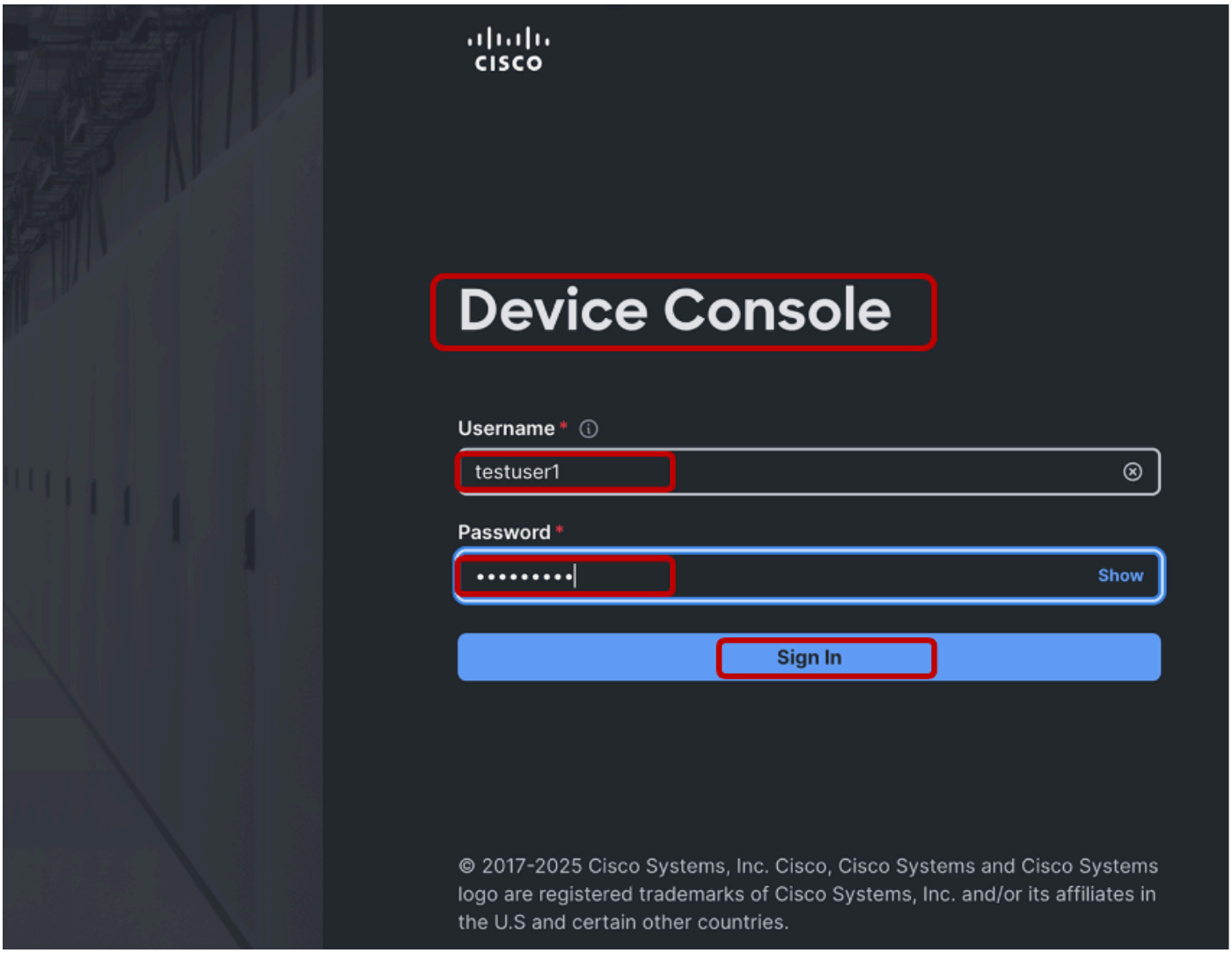
Next(다음), Save and Deploy the domain profile(도메인 프로필 저장 및 구축)을 클릭합니다.

도메인 프로파일 구축에 성공하면 IMM 도메인에 대한 보안 LDAP 컨피그레이션이 완료됩니다.

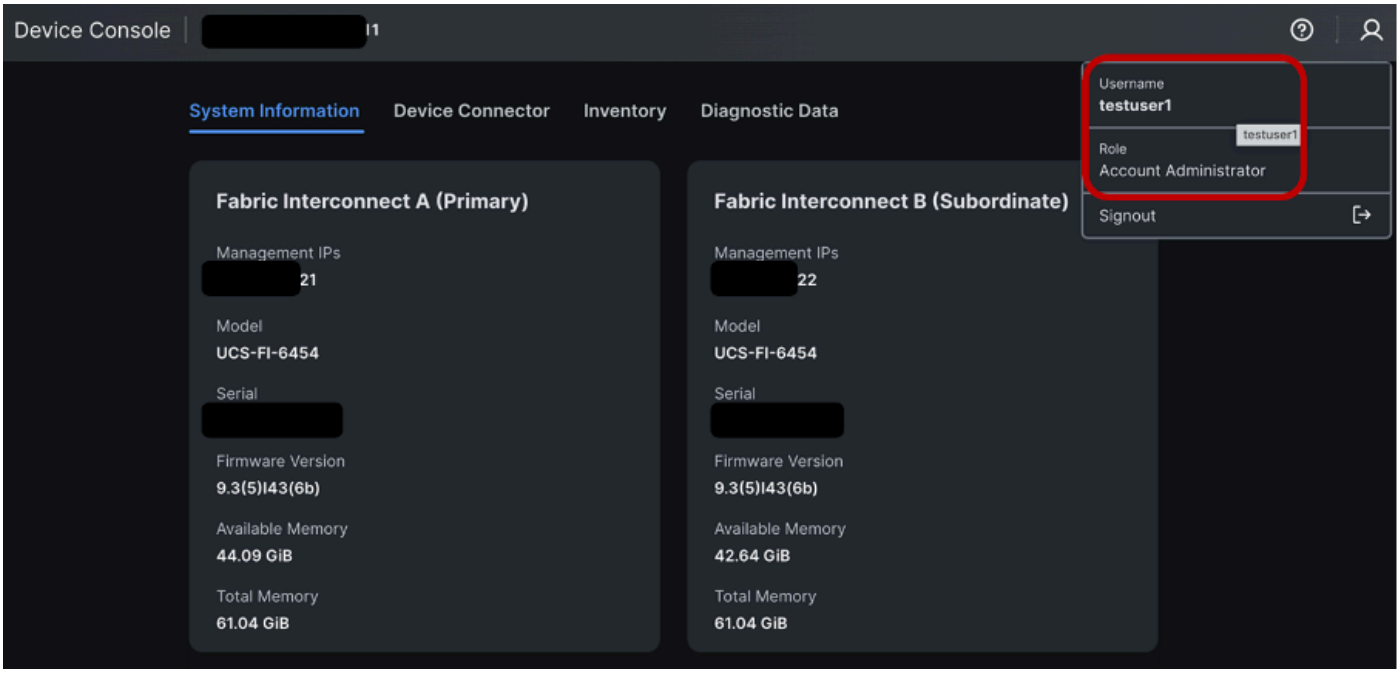
확인

확인하려면 구성된 LDAP/Active Directory 사용자 중 하나를 사용하여 Device Console GUI 및 Fabric Interconnect CLI에 로그인을 시도합니다.

디바이스 콘솔 로그인 테스트

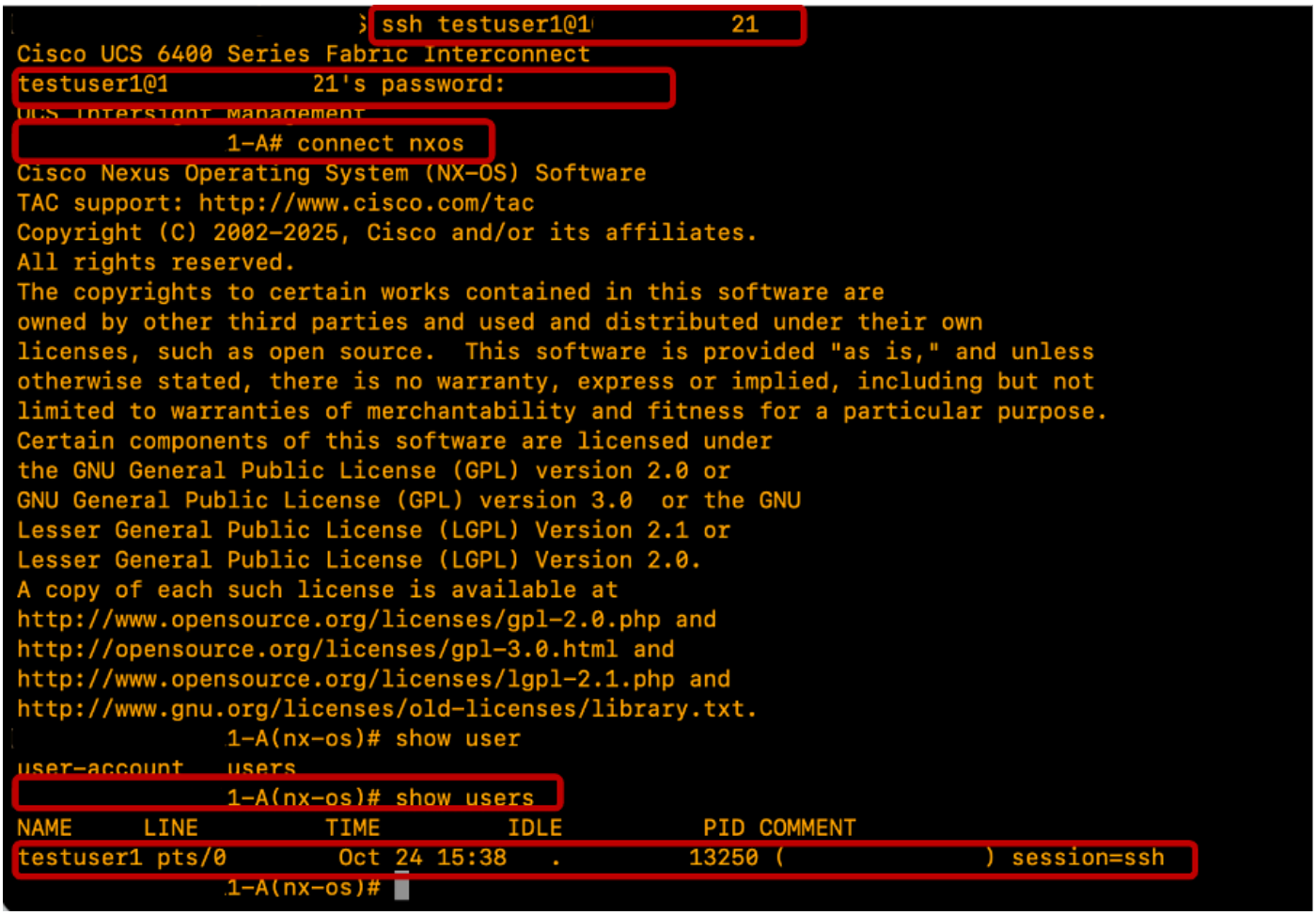


Testuser1 디바이스 콘솔 로그인에 성공했습니다.



테스트 FI SSH 로그인

Testuser1 SSH 로그인에 성공했습니다.



관련 정보

- Intersight 도움말 센터
- Cisco Intersight Managed Mode Fabric Interconnect 관리 설명서

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.