ISE에서 관리자 액세스 및 RBAC 정책 이해

목차

소개

이 문서에서는 ISE(Identity Services Engine)에서 관리 액세스를 관리하기 위한 ISE의 기능에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 주제에 대해 숙지할 것을 권장합니다.

- ISE
- Active Directory
- LDAP(Lightweight Directory Access Protocol)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

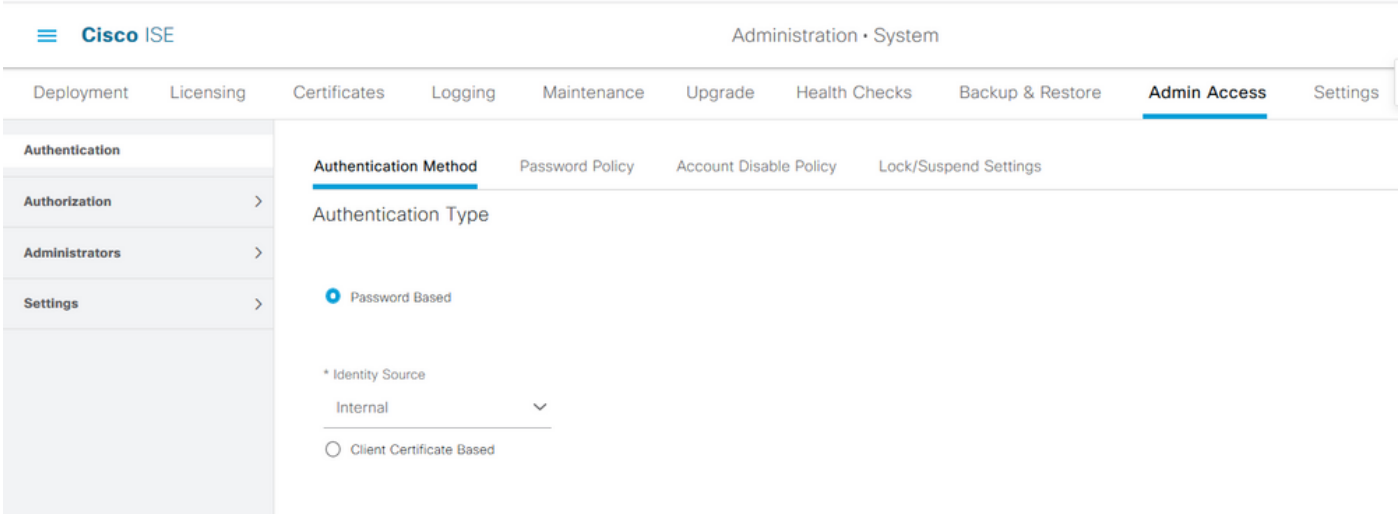
- Identity Services Engine 3.0
- Windows Server 2016

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

구성

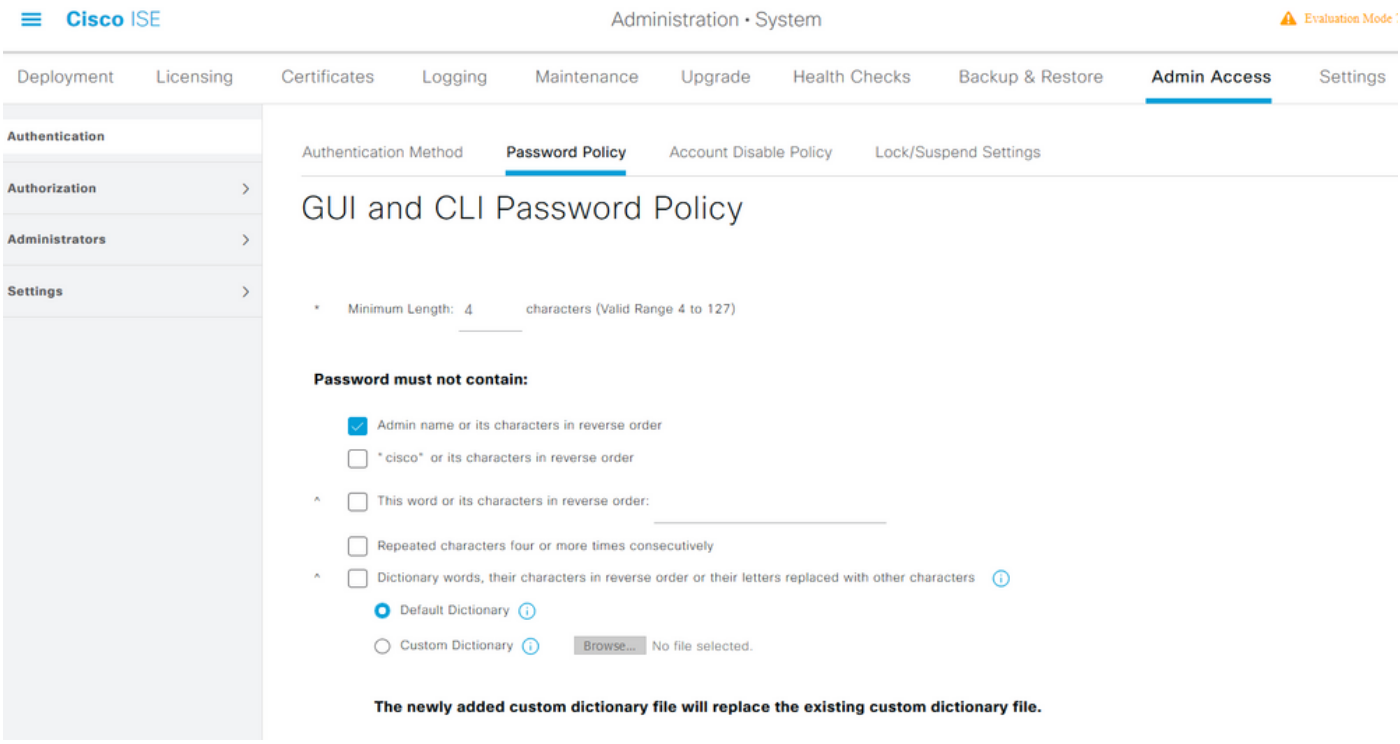
인증 설정

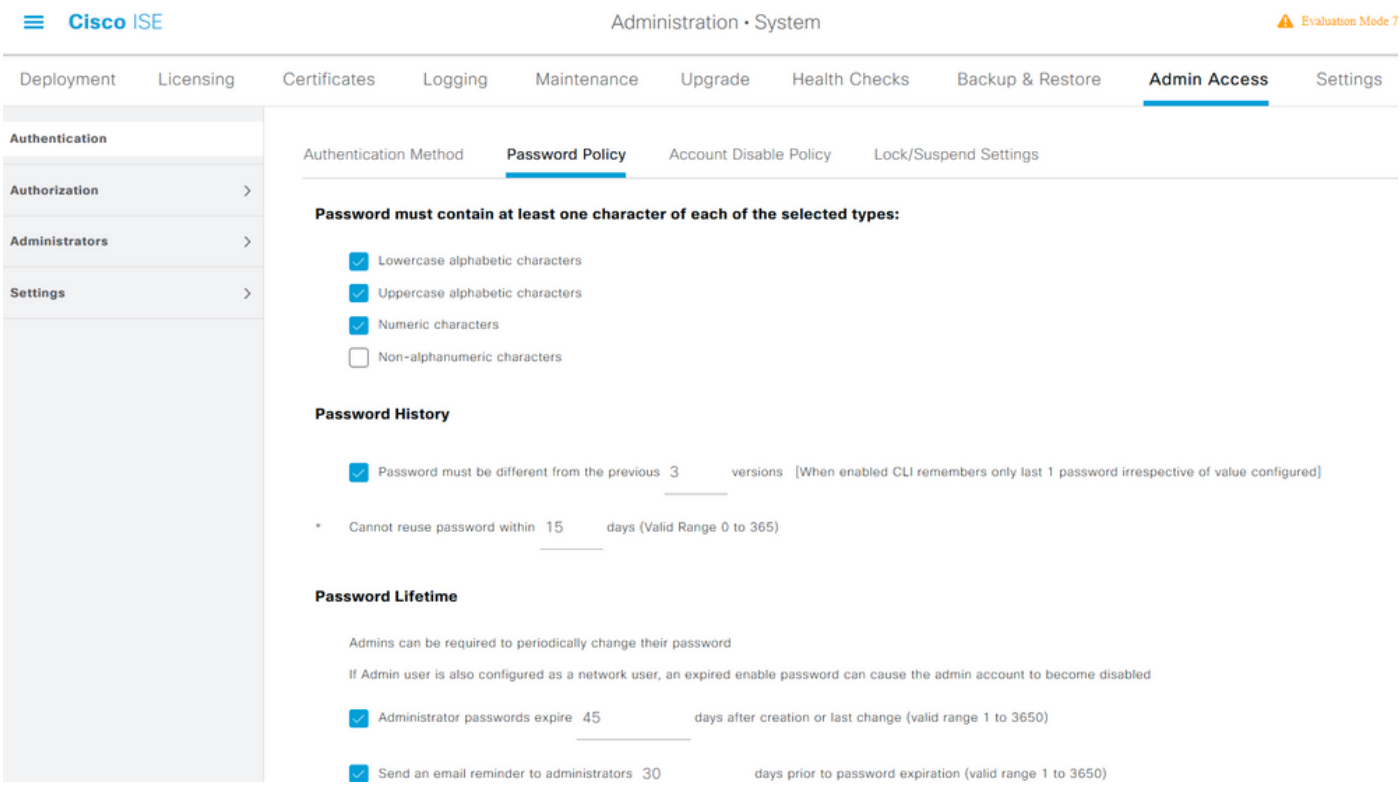
관리자 사용자는 ISE에 대한 모든 정보에 액세스하려면 자신을 인증해야 합니다.관리자 사용자의 ID는 ISE 내부 ID 저장소 또는 외부 ID 저장소를 사용하여 확인할 수 있습니다.신뢰성은 비밀번호 또는 인증서로 확인할 수 있습니다.이러한 설정을 구성하려면 Administration(관리) **> System(시스템) > Admin Access(관리 액세스) > Authentication(인증)으로 이동합니다**.Authentication Method(인증 방법) 탭 아래에서 필요한 인증 유형**을** 선택합니다.



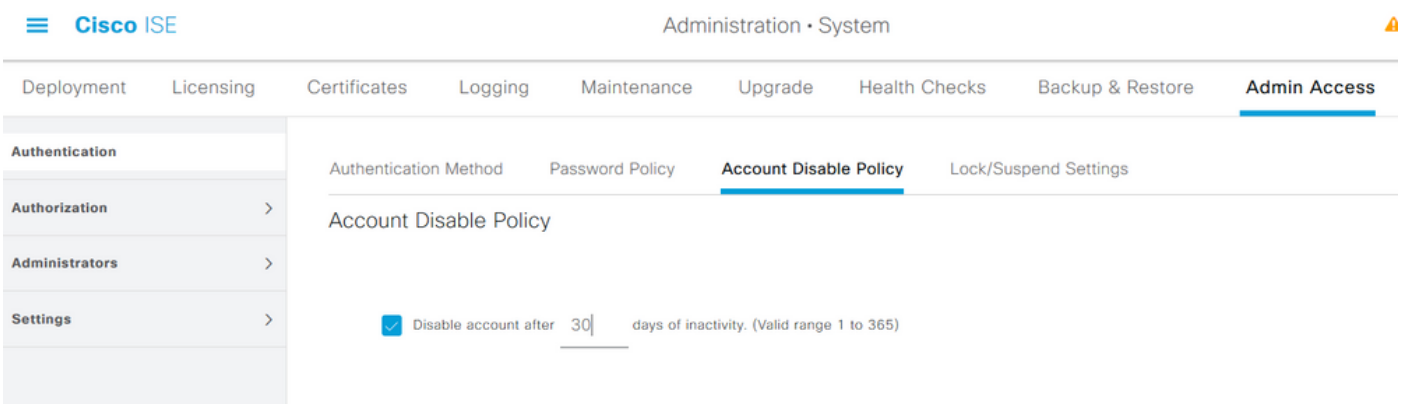
> **참고:**비밀번호 기반 인증은 기본적으로 활성화되어 있습니다.클라이언트 인증서 기반 인증으로 변경하면 모든 구축 노드에서 애플리케이션 서버가 재시작됩니다.

Identity Services Engine은 CLI에서 CLI(Command Line Interface)에 대한 비밀번호 정책을 구성할 수 없습니다.GUI 및 CLI 모두에 대한 비밀번호 정책은 ISE의 GUI를 통해서만 구성할 수 있습니다.이를 구성하려면 Administration(관리) **> System(시스템) > Admin Access(관리 액세스) > Authentication(인증)**으로 이동하고 **Password Policy(비밀번호 정책**) 탭으로 이동합니다.

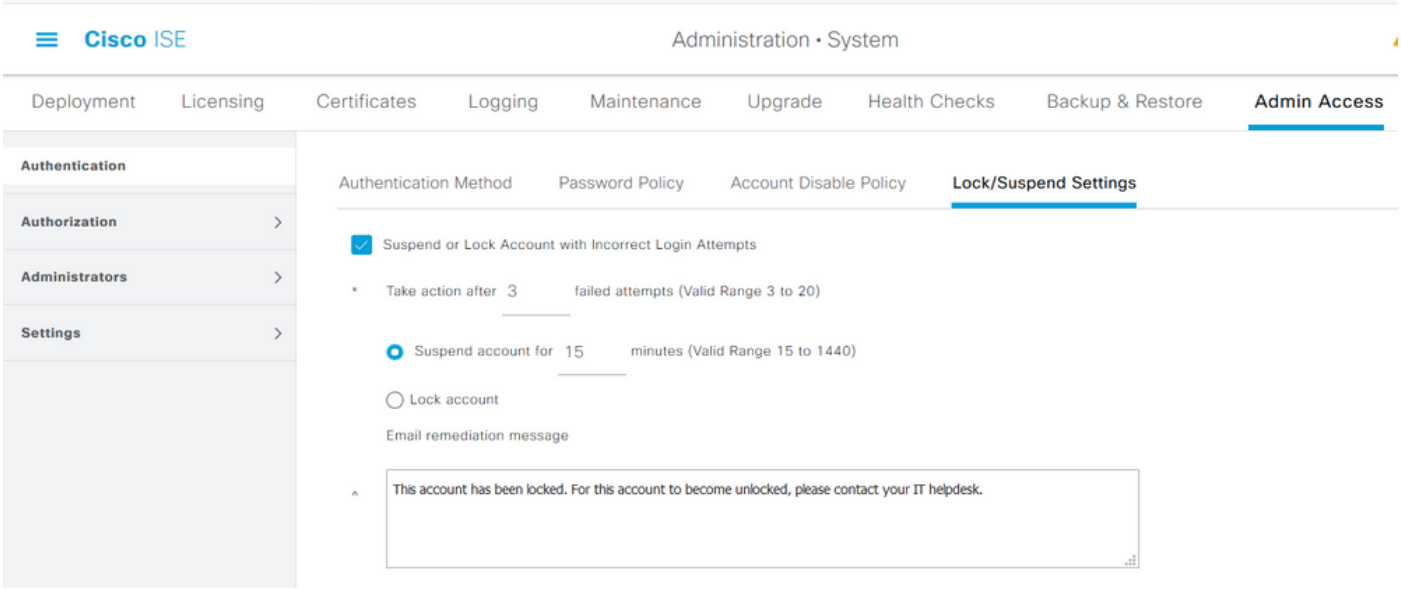




ISE에는 비활성 관리자 사용자를 비활성화하는 프로비저닝이 있습니다.이를 구성하려면 Administration(관리) **> System(시스템) > Admin Access(관리 액세스) > Authentication(인증)으로 이동하고 Account Disable Policy(계정 비활성화 정책)** 탭으로 이동합니다.



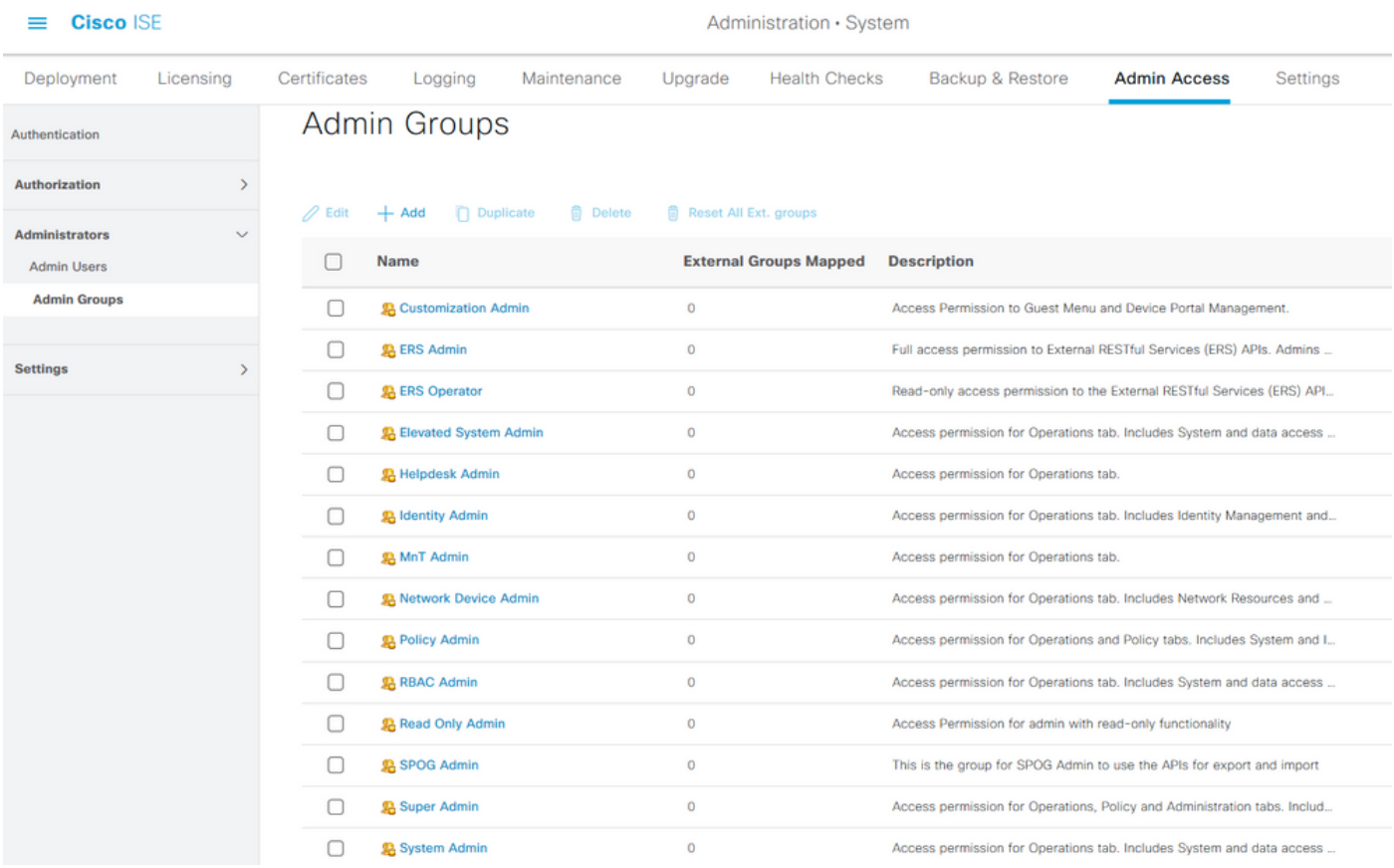
또한 ISE는 실패한 로그인 시도 횟수를 기반으로 관리자 사용자 계정을 잠그거나 일시 중단할 수 있는 기능을 제공합니다.이를 구성하려면 Administration(관리) **> System(시스템) > Admin Access(관리 액세스) > Authentication(인증)**으로 이동하고 **Lock/Suspend Settings(설정 잠금/일시 중단)** 탭으로 이동합니다.



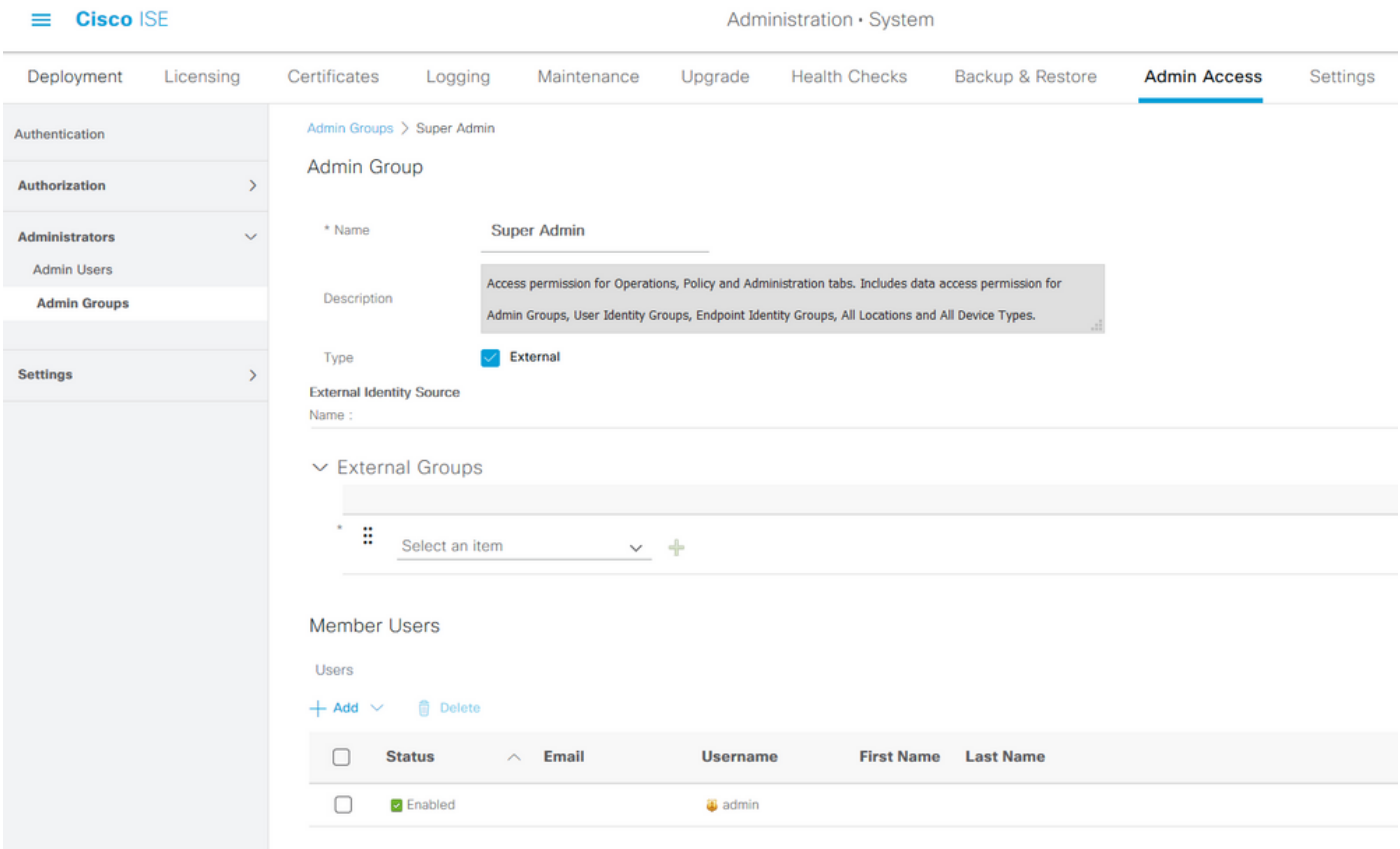
관리 액세스를 관리하려면 관리 그룹, 사용자 및 다양한 정책/규칙이 권한을 제어하고 관리해야 합니다.

관리 그룹 구성

Administration(관리) **> System(시스템) > Admin Access(관리 액세스) > Administrators(관리자) > Admin Groups(관리 그룹)로 이동하여 관리자 그룹**을 구성합니다.기본적으로 기본적으로 내장되어 있으며 삭제할 수 없는 그룹이 거의 없습니다.

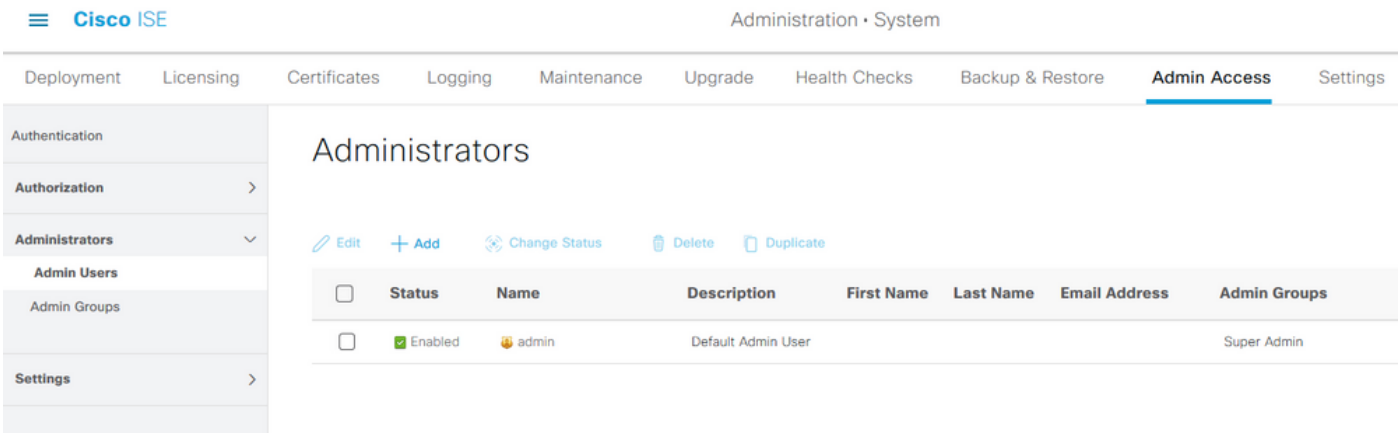


그룹이 생성되면 그룹을 선택하고 편집을 클릭하여 해당 그룹에 관리 사용자를 추가합니다.외부 관리자 사용자가 필요한 권한을 얻을 수 있도록 외부 ID 그룹을 ISE의 관리 그룹에 매핑하는 프로비저닝이 있습니다.이를 구성하려면 사용자를 추가하는 동안 유형을 External(외부)로 선택합니다.

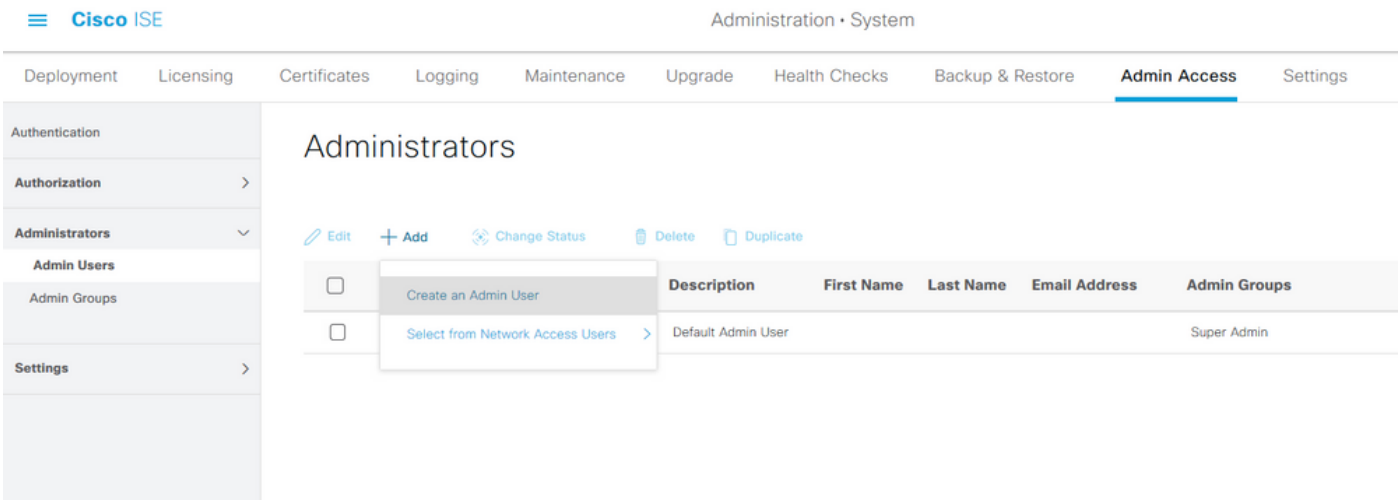


관리자 사용자 구성

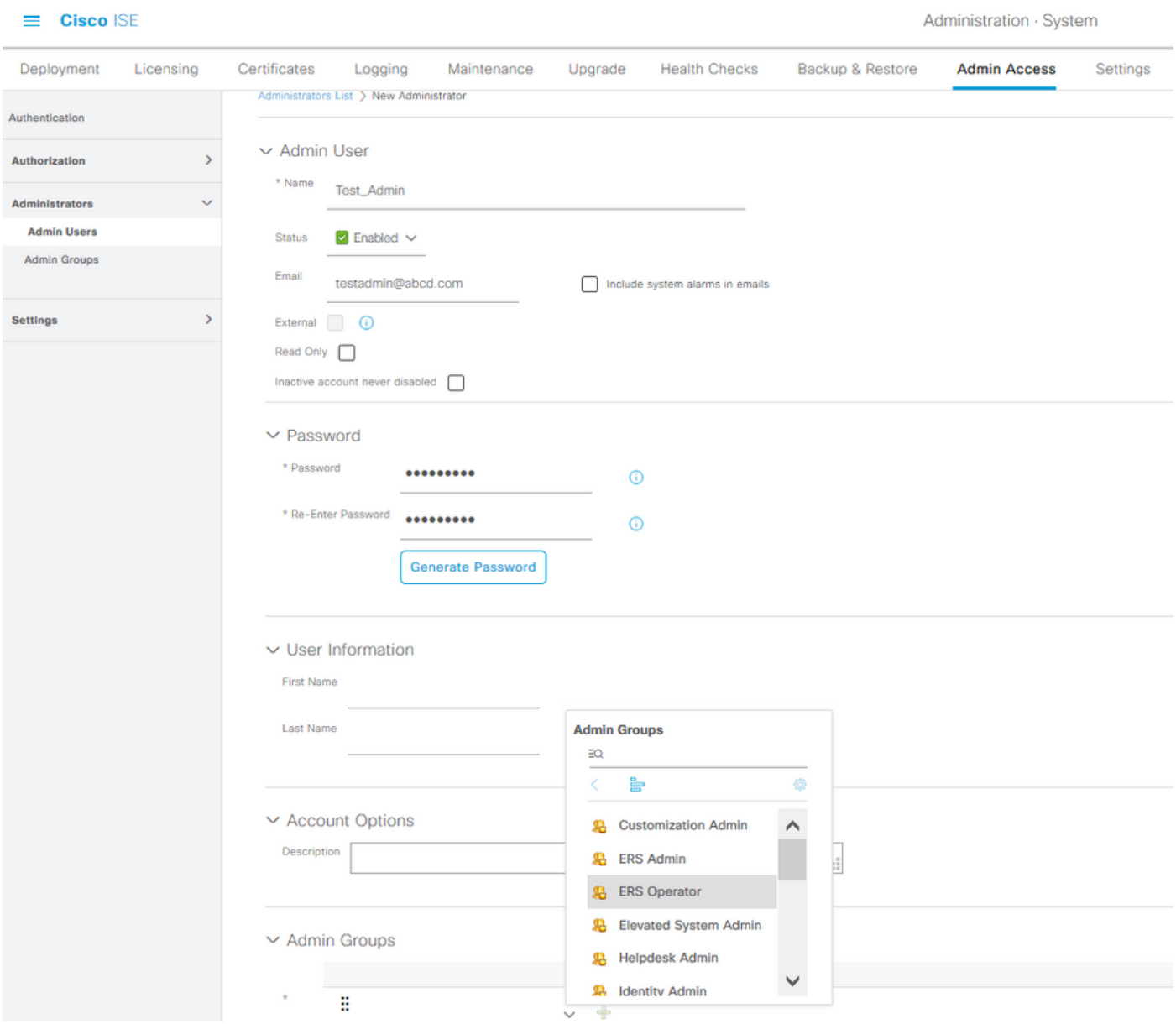
관리자 사용자를 구성하려면 Administration(관리) **> System(시스템) > Admin Access(관리자 액세스) > Administrators(관리자) > Admin Users(관리자 사용자)로 이동합니다**.



Add(**추가)를 클릭합니다**.두 가지 중에서 선택할 수 있습니다.한 가지는 새 사용자를 모두 추가하는 것입니다.다른 하나는 네트워크 액세스 사용자(즉, 네트워크/디바이스에 액세스하기 위해 내부 사용자로 구성된 사용자)를 ISE 관리자로 만드는 것입니다.



옵션을 선택한 후에는 필요한 세부 정보를 제공해야 하며 사용자에게 부여된 권한과 권한을 기준으로 사용자 그룹을 선택해야 합니다.



권한 구성

사용자 그룹에 대해 구성할 수 있는 두 가지 유형의 사용 권한이 있습니다.

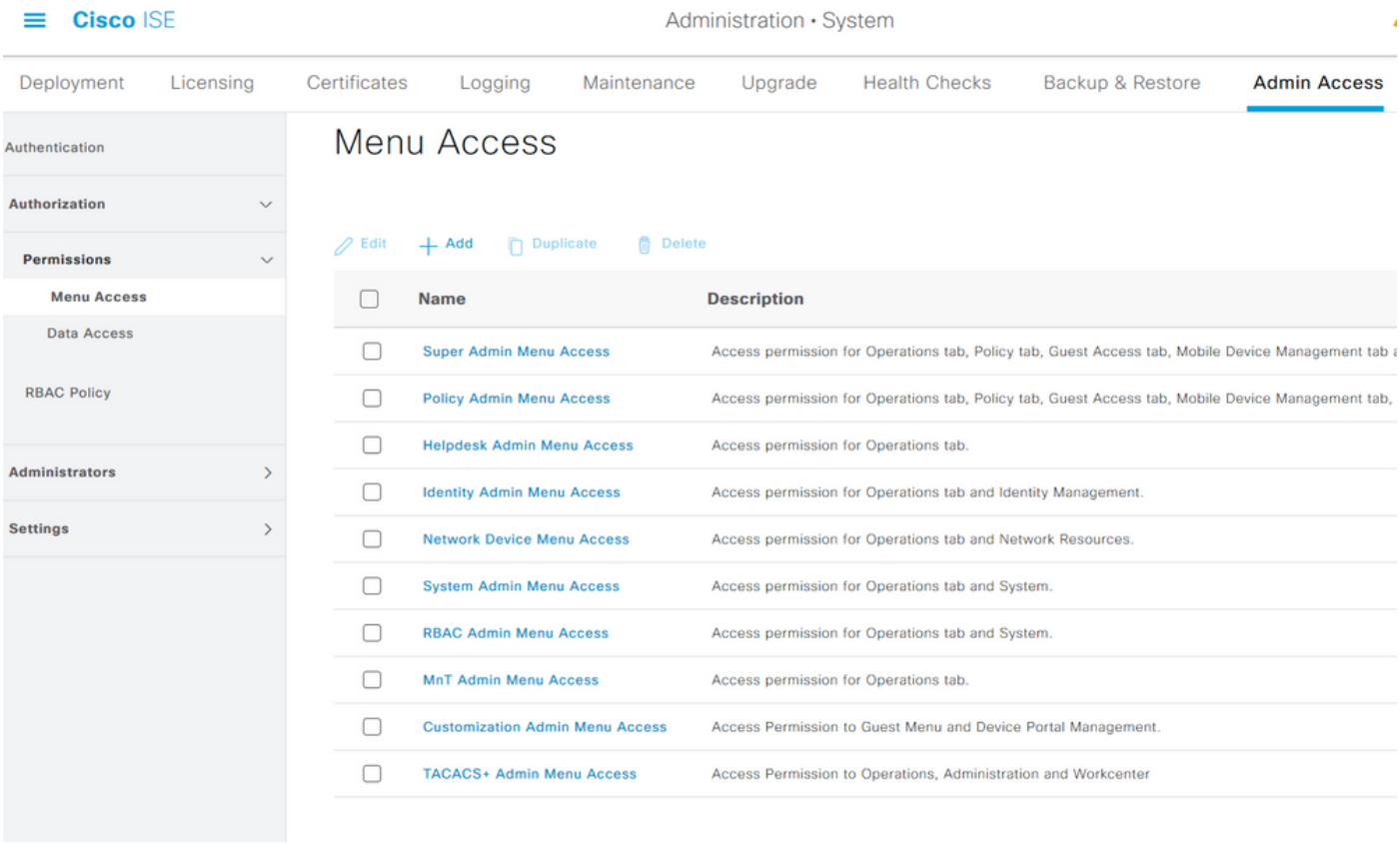
1. 메뉴 액세스
2. 데이터 액세스

Menu Access는 ISE에 대한 탐색 가시성을 제어합니다.표시 또는 숨기기라는 두 가지 옵션을 구성할 수 있습니다.선택한 탭을 표시하거나 숨기도록 메뉴 액세스 규칙을 구성할 수 있습니다.

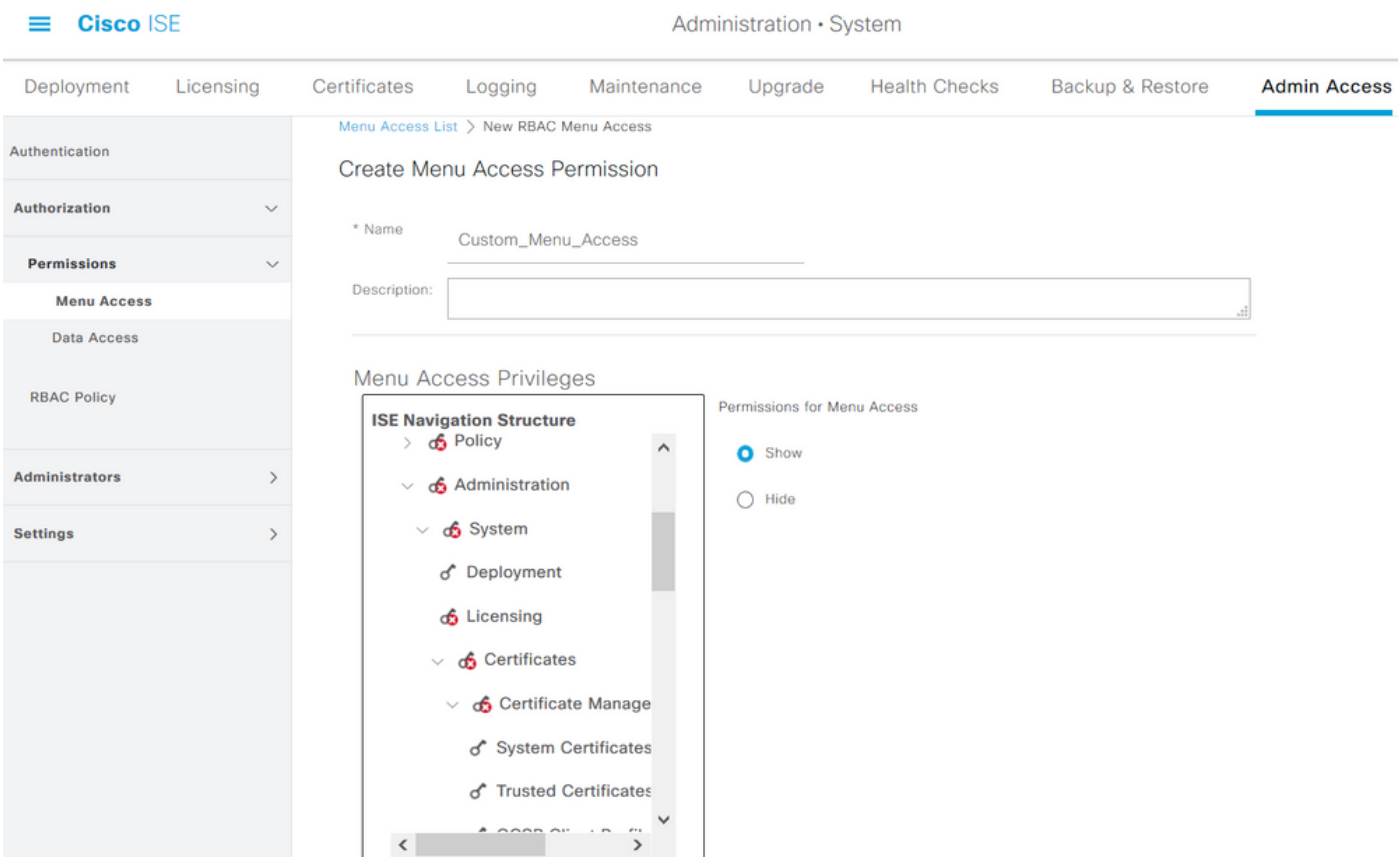
데이터 액세스는 ISE에서 ID 데이터를 읽기/액세스/수정하는 기능을 제어합니다.액세스 권한은 관리 그룹, 사용자 ID 그룹, 엔드포인트 ID 그룹 및 네트워크 장치 그룹에 대해서만 구성할 수 있습니다.ISE에서 이러한 엔티티에 대해 구성할 수 있는 세 가지 옵션이 있습니다.모든 액세스, 읽기 전용 액세스, 액세스 권한이 없습니다.데이터 액세스 규칙은 ISE의 각 탭에 대해 이 세 옵션 중 하나를 선택하도록 구성할 수 있습니다.

메뉴 액세스 및 데이터 액세스 정책은 관리자 그룹에 적용하려면 먼저 만들어야 합니다.기본적으로 기본적으로 제공되는 몇 가지 정책이 있지만 항상 사용자 지정할 수 있거나 새 정책을 만들 수 있습니다.

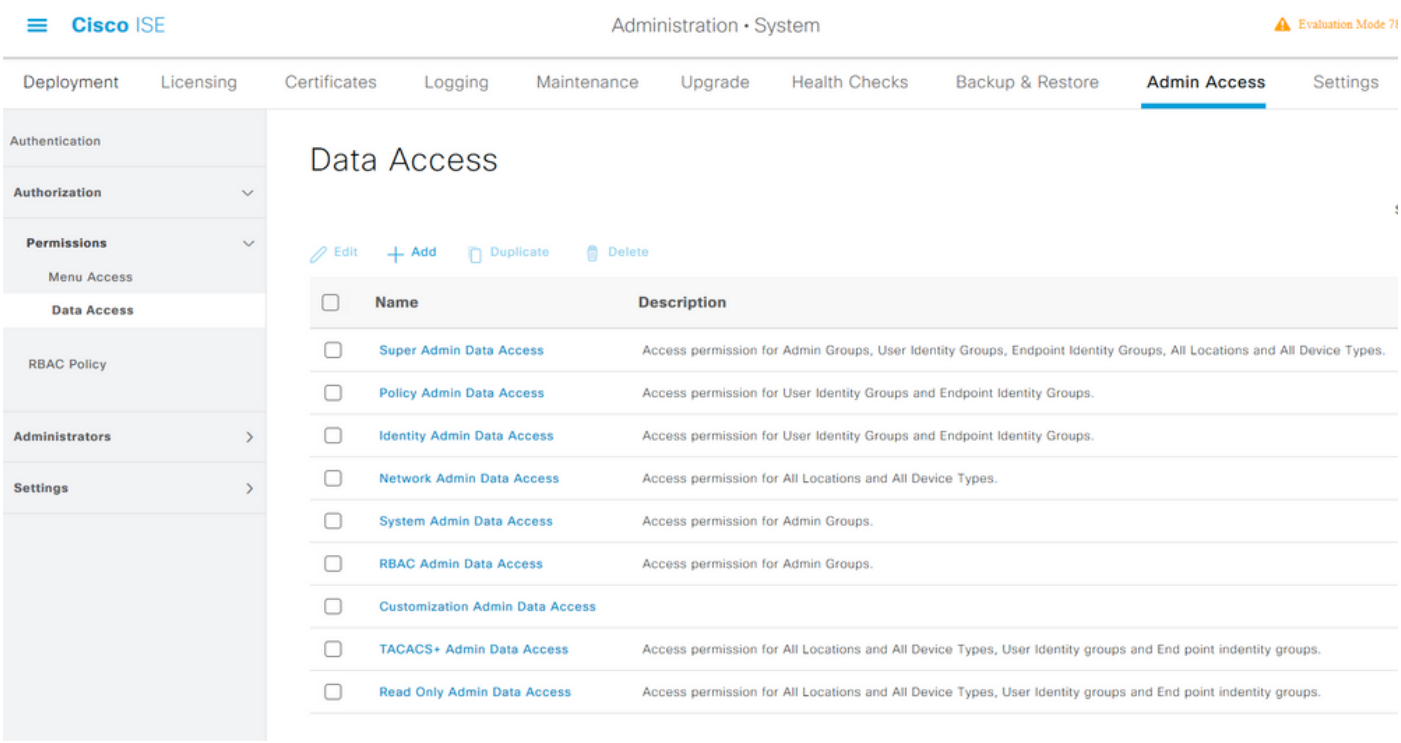
메뉴 액세스 정책을 구성하려면 Administration(관리) > System(시스템) > Admin Access(관리자 액세스) > Authorization(권한) > Permissions(권한) > Menu Access(메뉴 액세스)로 이동합니다.



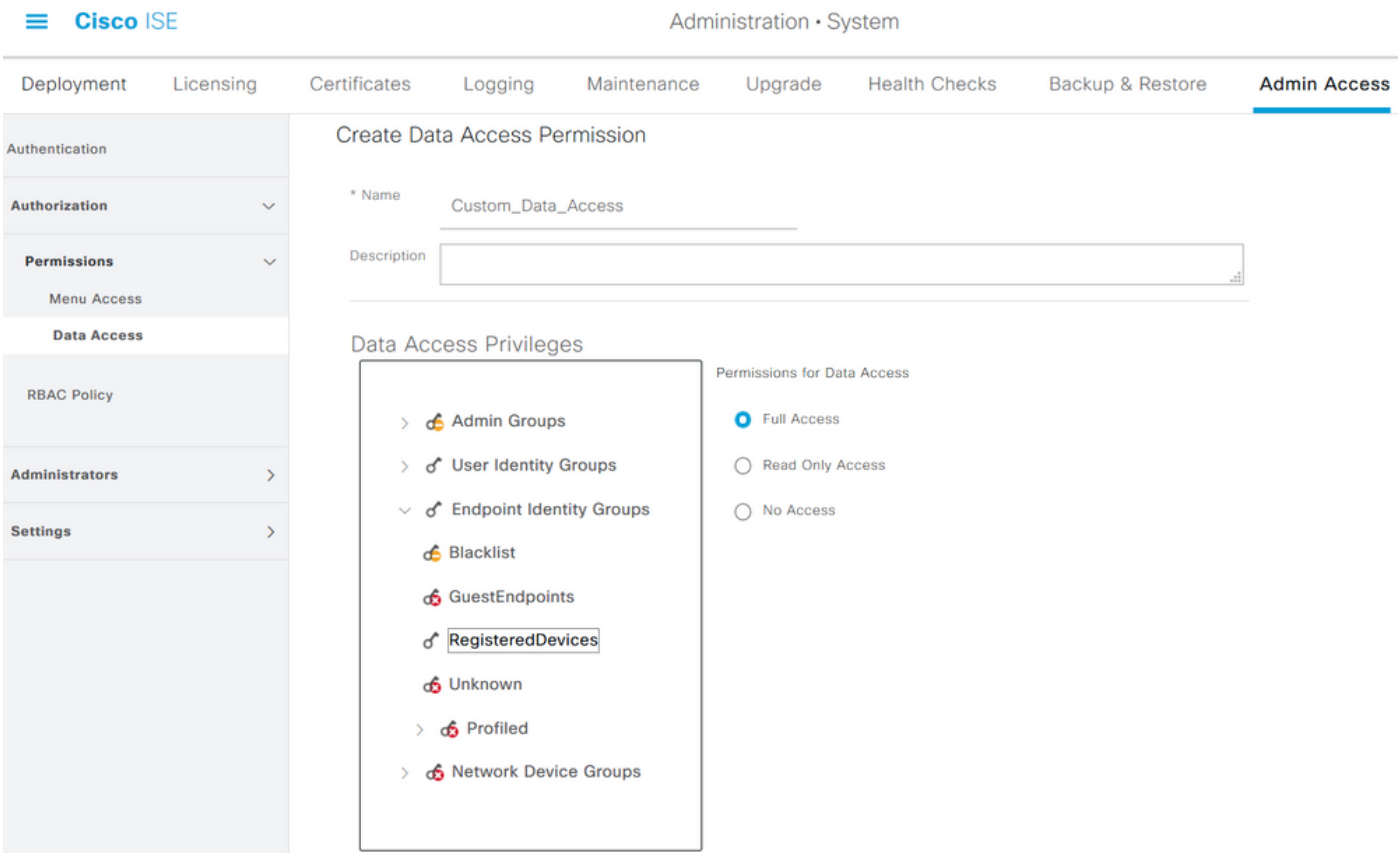
Add(**추가)를 클릭합니다**.ISE의 각 탐색 옵션은 정책에 표시/숨기도록 구성할 수 있습니다.



데이터 액세스 정책을 구성하려면 Administration(관리) > System(시스템) > Admin Access(관리자 액세스) > Authorization(권한) > Permissions(권한) > Data Access(데이터 액세스)로 이동합니다.



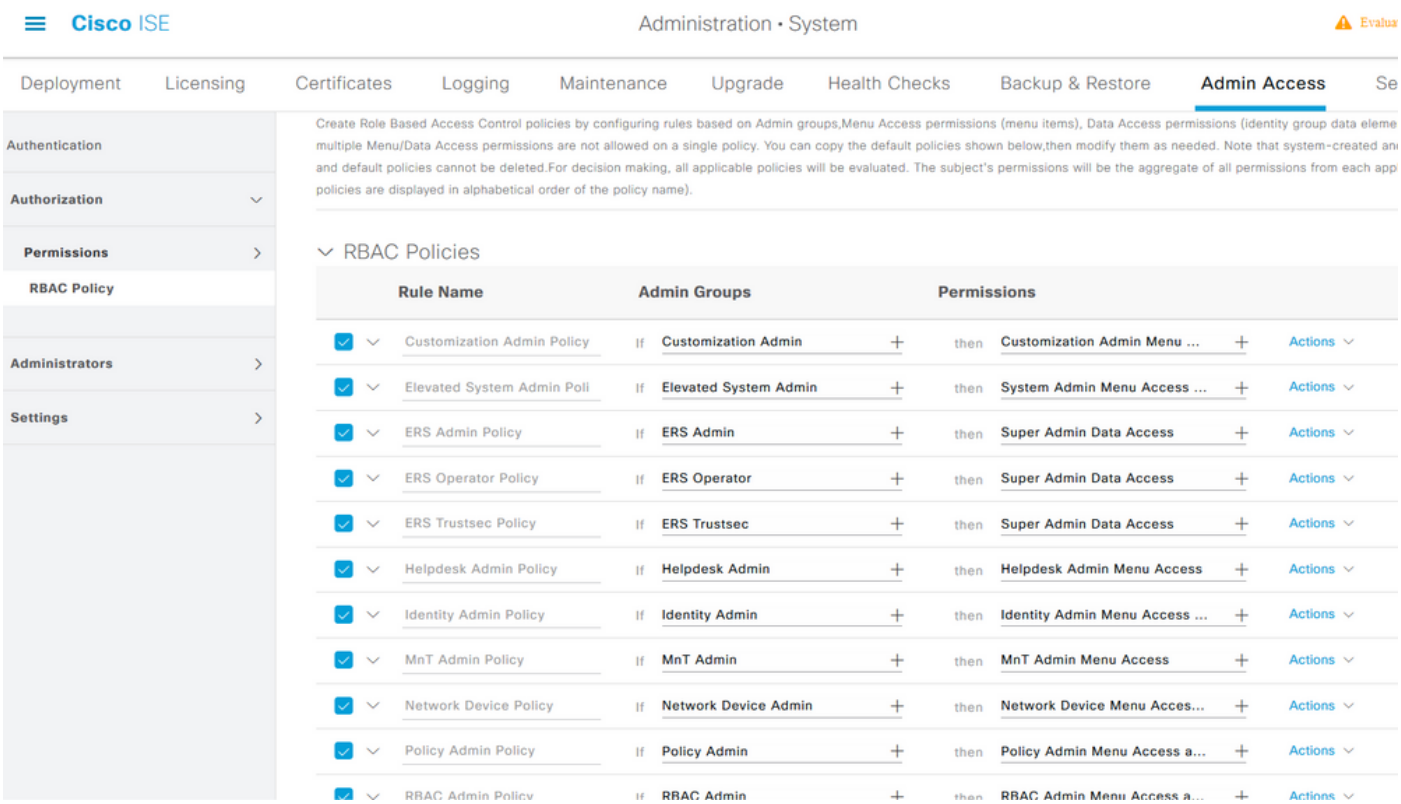
Add(**추가**)를 클릭하여 새 정책을 생성하고 Admin/User Identity/Endpoint Identity/Network Groups(관리자/사용자 ID/엔드포인트 ID/네트워크 그룹)에 액세스하기 위한 권한을 구성합니다.



RBAC 정책 구성

RBAC는 역할 기반 액세스 제어를 의미합니다.사용자가 속한 역할(관리 그룹)은 원하는 메뉴 및 데이터 액세스 정책을 사용하도록 구성할 수 있습니다.단일 역할에 대해 여러 RBAC 정책이 구성되거나 단일 정책에서 여러 역할을 구성하여 메뉴 및/또는 데이터에 액세스할 수 있습니다.해당 정책은 모두 관리자 사용자가 작업을 수행하려고 할 때 평가됩니다.최종 결정은 해당 역할에 적용할 수 있

는 모든 정책의 종합입니다.동시에 허용 및 거부하는 모순된 규칙이 있는 경우 허용 규칙은 거부 규칙을 재정의합니다.이러한 정책을 구성하려면 Administration(관리) **> System(시스템) > Admin Access(관리 액세스) > Authorization(권한 부여) > RBAC Policy(RBAC 정책)로 이동합니다**.



정책을 복제/삽입/삭제할 작업을 클릭합니다.

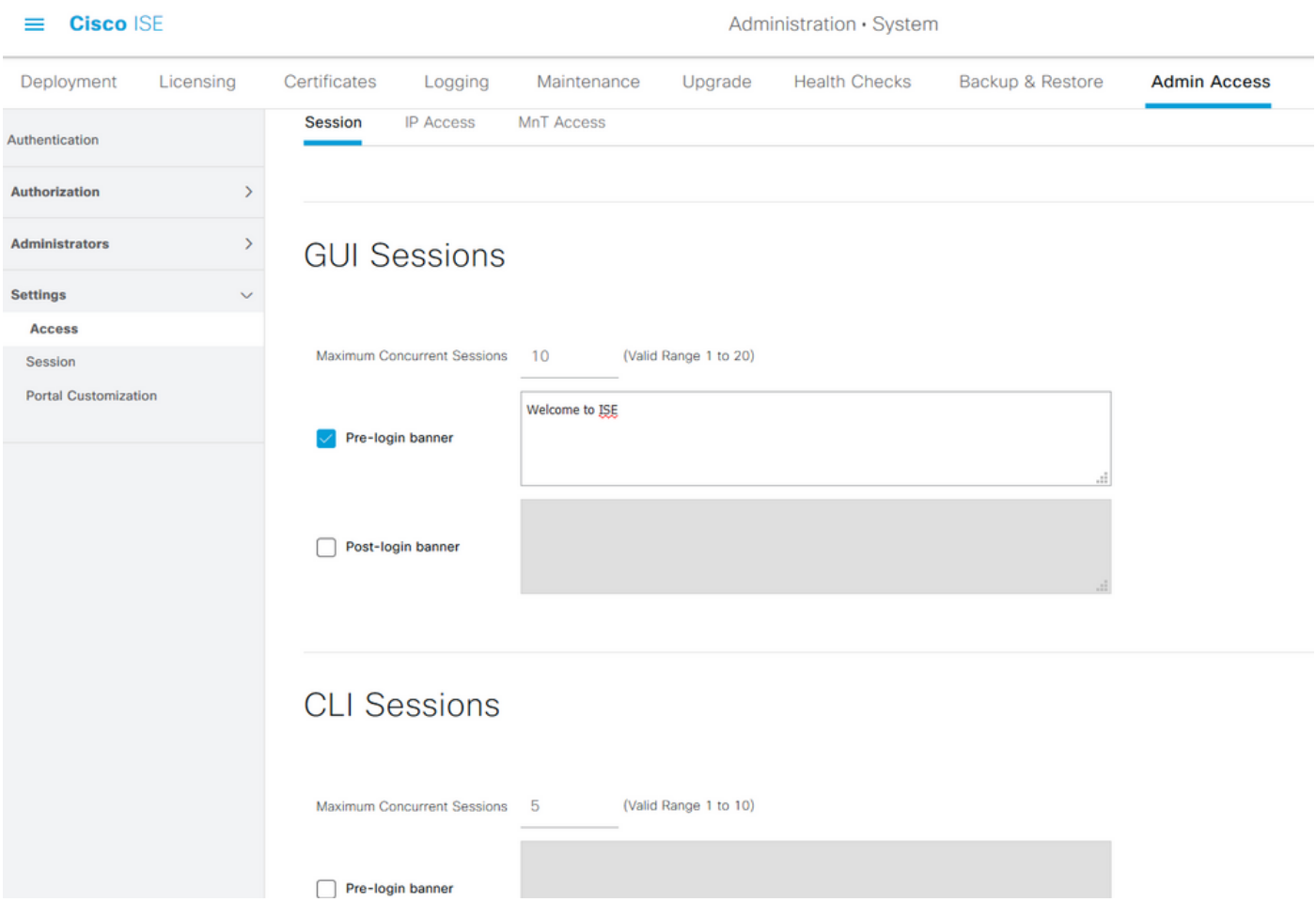
참고:시스템 생성 및 기본 정책은 업데이트할 수 없으며 기본 정책을 삭제할 수 없습니다.

참고:단일 규칙에서 다중 메뉴/데이터 액세스 권한을 구성할 수 없습니다.

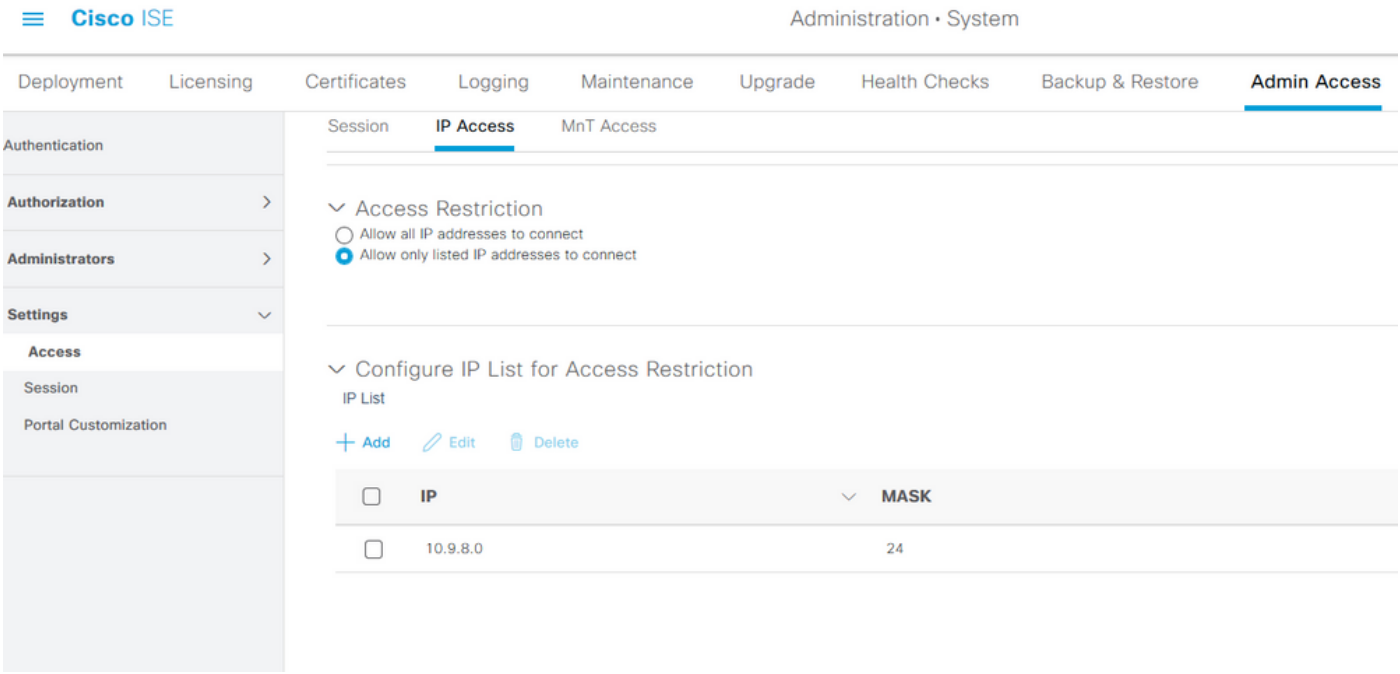
관리자 액세스에 대한 설정 구성

RBAC 정책 외에도 모든 관리자 사용자에게 공통된 몇 가지 설정을 구성할 수 있습니다.

GUI 및 CLI에 대해 Maximum Sessions Allowed, Pre-login, and Post-login Banners for GUI and CLI의 수를 구성하려면 **Administration > System > Admin Access > Settings > Access로 이동합니다**.Session(세션) 탭 아래에서 **구성합니다**.



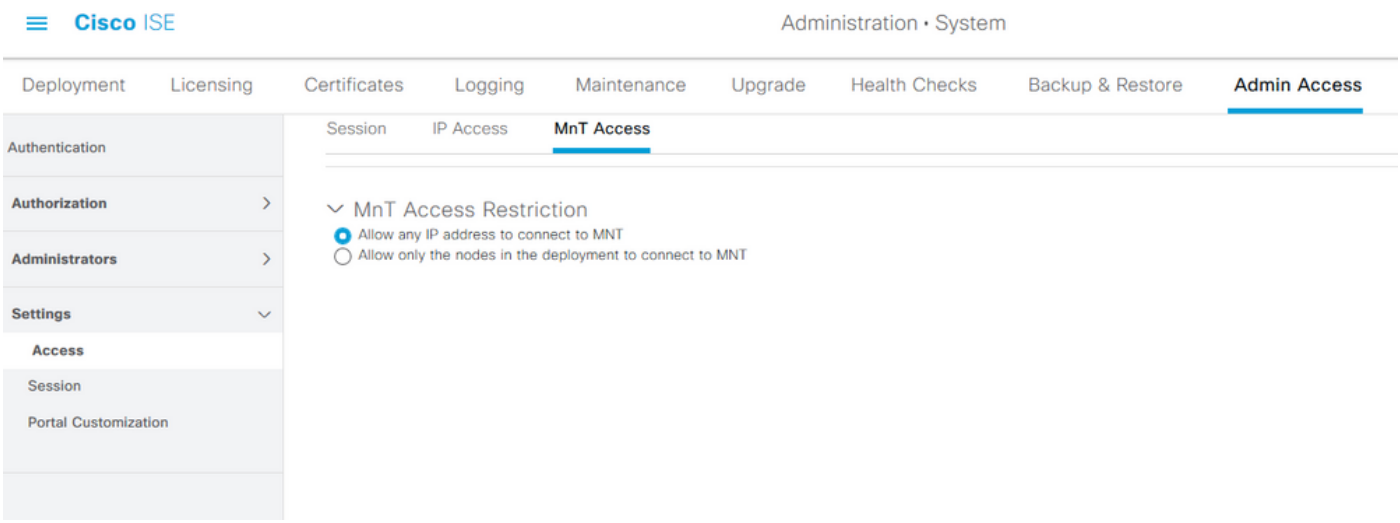
GUI 및 CLI에 액세스할 수 있는 IP 주소 목록을 구성하려면 **Administration(관리) > System(시스템) > Admin Access(관리 액세스) > Settings(설정) > Access(액세스)로 이동하여 IP Access(IP 액세스)** 탭으로 이동합니다.



관리자가 Cisco ISE에서 MnT 섹션에 액세스할 수 있는 노드 목록을 구성하려면 **Administration(관리) > System(시스템) > Admin Access(관리 액세스) > Settings(설정) > Access(액세스)**로 이동하고 **MnT Access(MnT 액세스)** 탭으로 이동합니다.

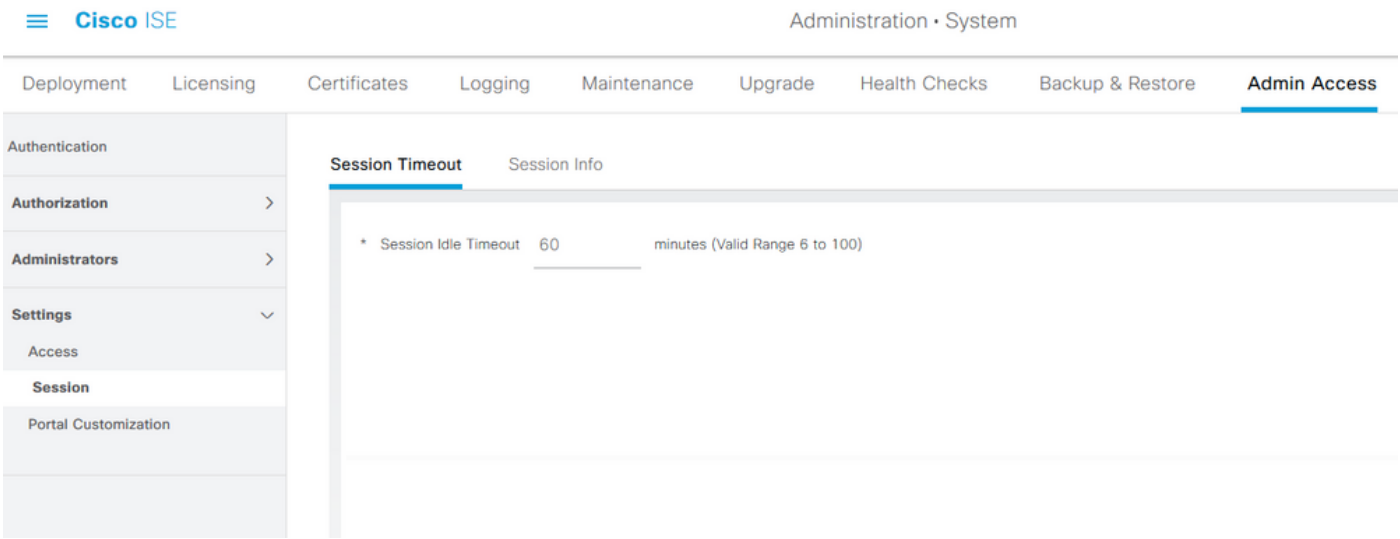
구축 내 또는 구축 외부의 노드 또는 엔티티가 syslog를 MnT로 전송하도록 허용하려면 Allow any

IP address to connect to MNT 라디오 버튼을 클릭합니다.구축 내의 노드 또는 엔티티만 syslog를 MnT로 전송하도록 허용하려면 Allow only the nodes to connect to MNT 라디오 버튼을 클릭합니다.

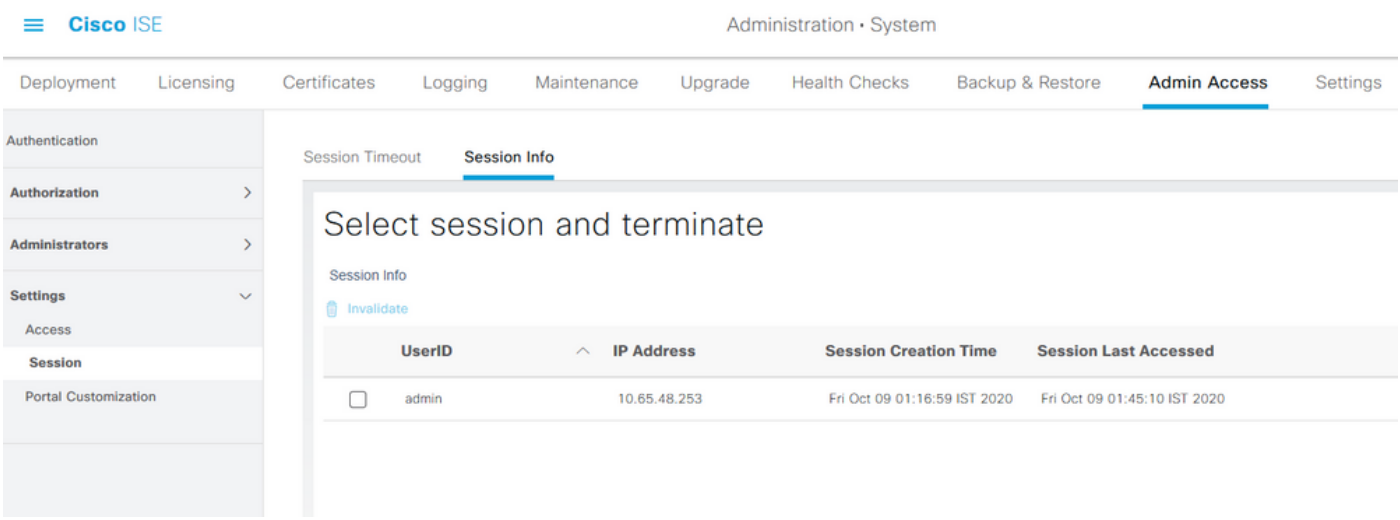


> **참고:**ISE 2.6 패치 2 이상의 경우 *MnT에 대한 UDP Syslogs 전달에 "ISE Messaging Service" 사용*이 기본적으로 설정되어 있으므로 구축 외부의 다른 엔티티로부터 syslog가 오는 것을 허용하지 않습니다.

세션이 비활성화되어 시간 초과 값을 구성하려면 Administration(관리) > System(시스템) **> Admin Access(관리 액세스) > Settings(설정) >** Session(**세션)으로 이동합니다.Session Timeout** 탭 아래에서 이 값을 설정합니다.



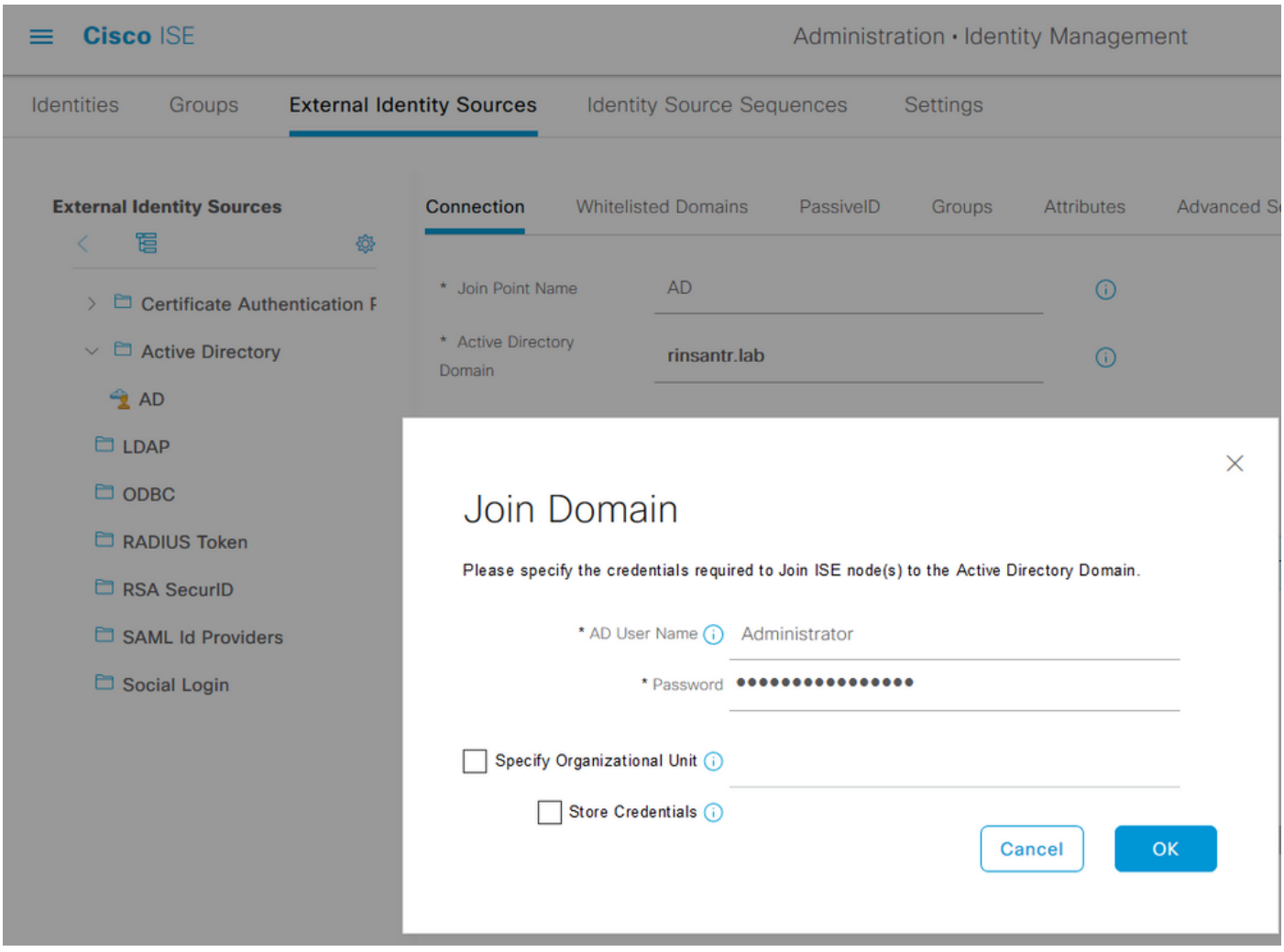
현재 활성 세션을 확인/무효화하려면 **Administration(관리) > Admin Access(관리 액세스) > Settings(설정) > Session(세션)으로 이동하고** Session Info(세션 정보) 탭을 클릭합니다.

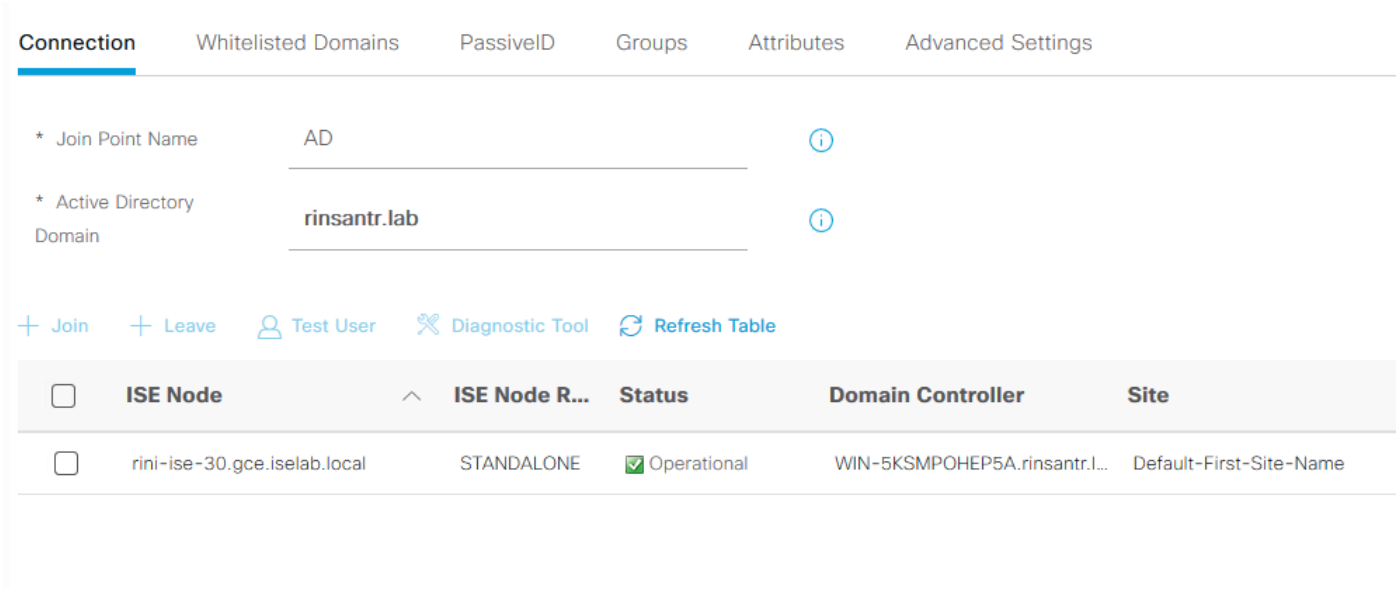


AD 자격 증명을 사용하여 관리 포털 액세스 구성

ISE를 AD에 조인

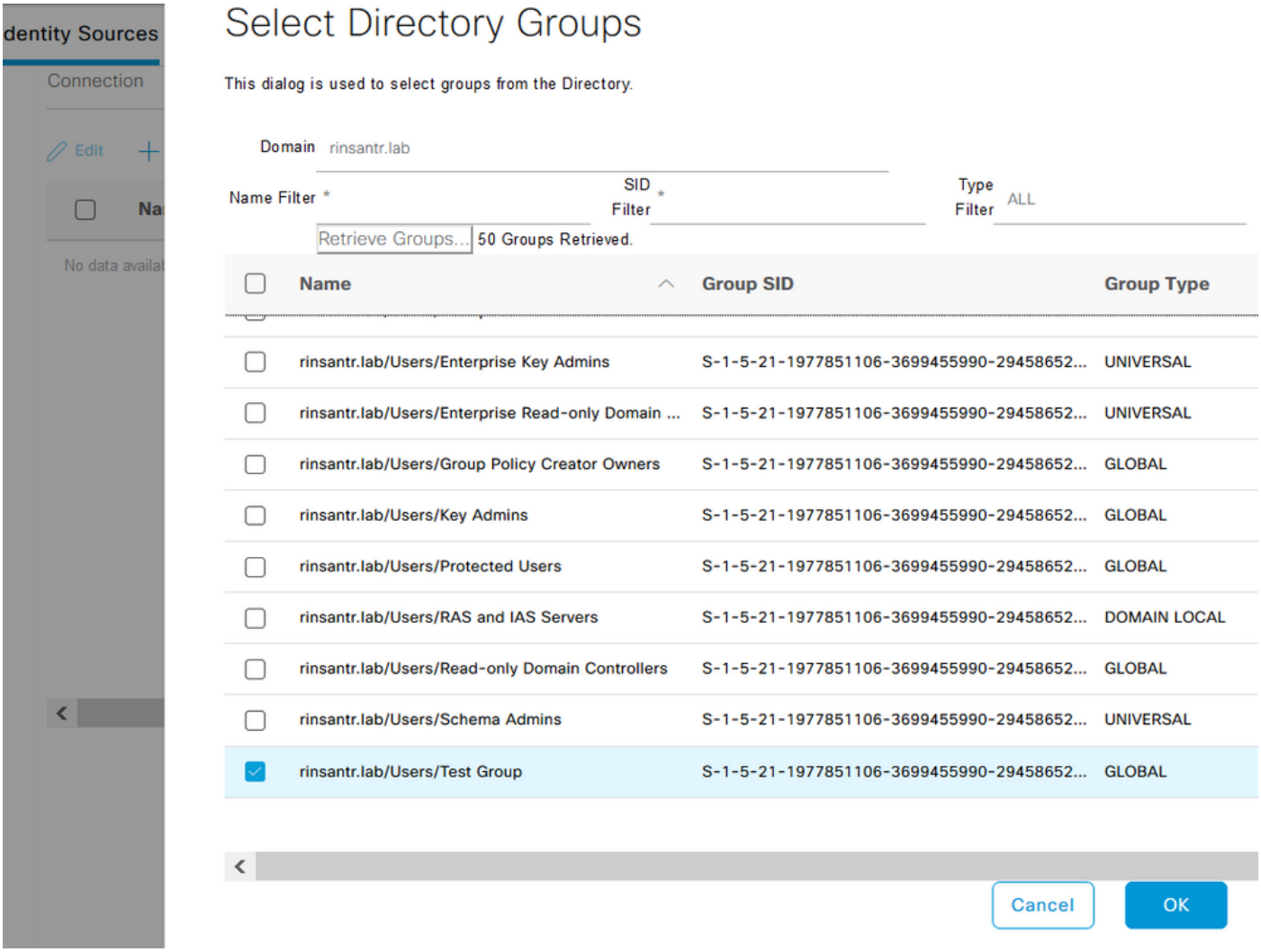
ISE를 외부 도메인에 가입시키려면 Administration(관리) **> Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > Active Directory로 이동합니다**.새 가입 포인트 이름 및 Active Directory 도메인을 입력합니다.컴퓨터 개체를 추가 및 변경할 수 있는 AD 계정의 자격 증명을 입력하고 [확인]을 클릭합니다.

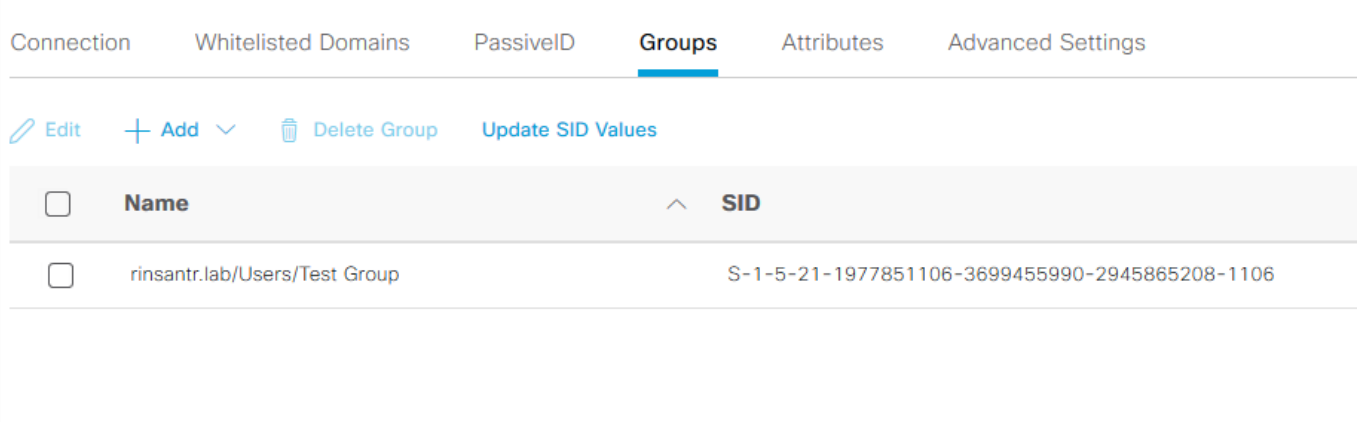




디렉터리 그룹 선택

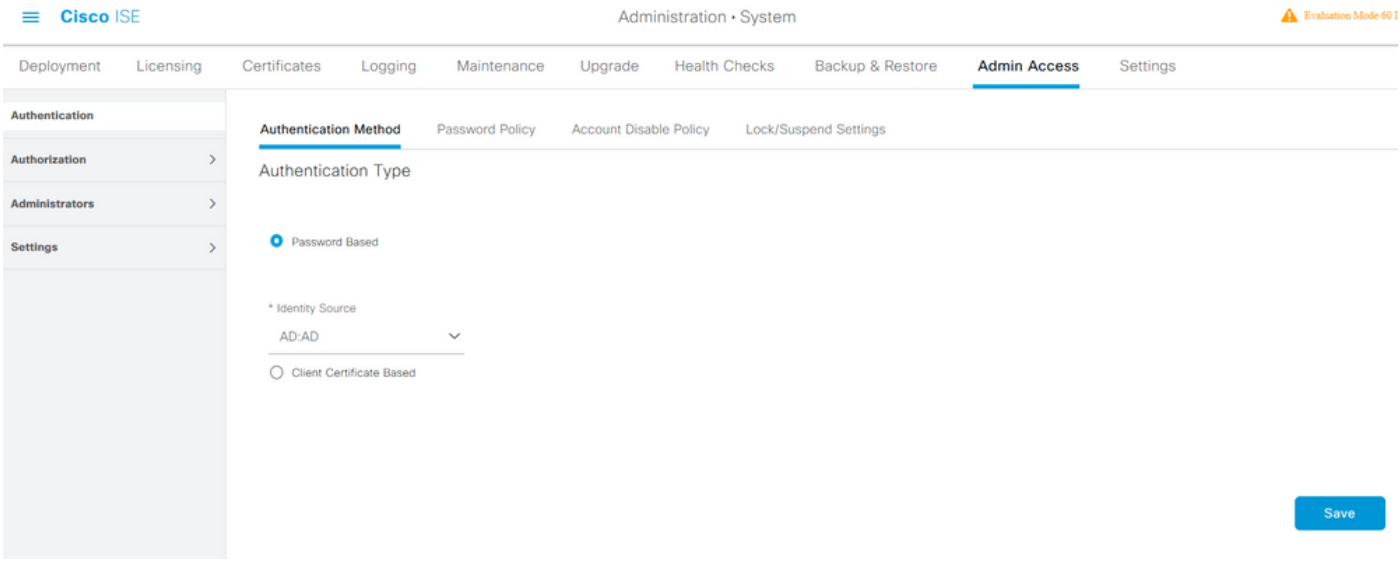
Administration(관리) **> Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > Active Directory로 이동합니다**.원하는 가입 포인트 이름을 클릭하고 **그룹** 탭으로 이동합니다 .Add(추가) **> Select Groups from Directory(디렉토리에서 그룹 선택) > Retrieve Groups(그룹 검색)를 클릭합니다**.관리자가 속한 AD 그룹을 하나 이상 가져오고 **OK**(확인)를 클릭한 다음 **Save(저장)**를 클릭합니다.





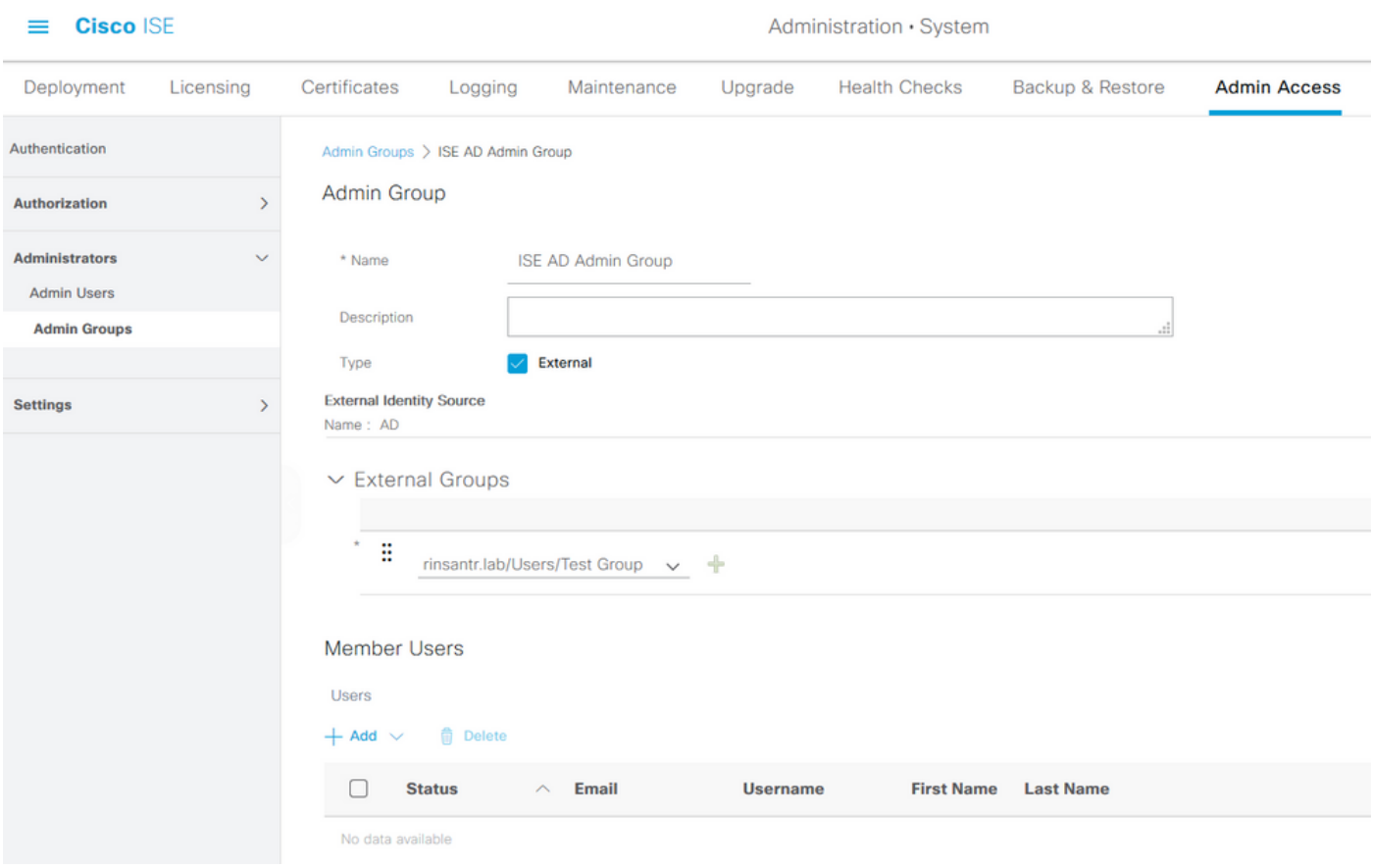
AD에 대한 관리 액세스 사용

AD를 사용하여 ISE의 비밀번호 기반 인증을 활성화하려면 Administration(관리) **> System(시스템) > Admin Access(관리 액세스) > Authentication(인증)으로 이동합니다**.Authentication Method(**인증 방법**) 탭에서 **Password-Based** 옵션**을** 선택합니다.Identity **Source(ID 소스**) 드롭다운 메뉴에서 **AD**를 선택하고 Save(저장)를 **클릭합니다**.



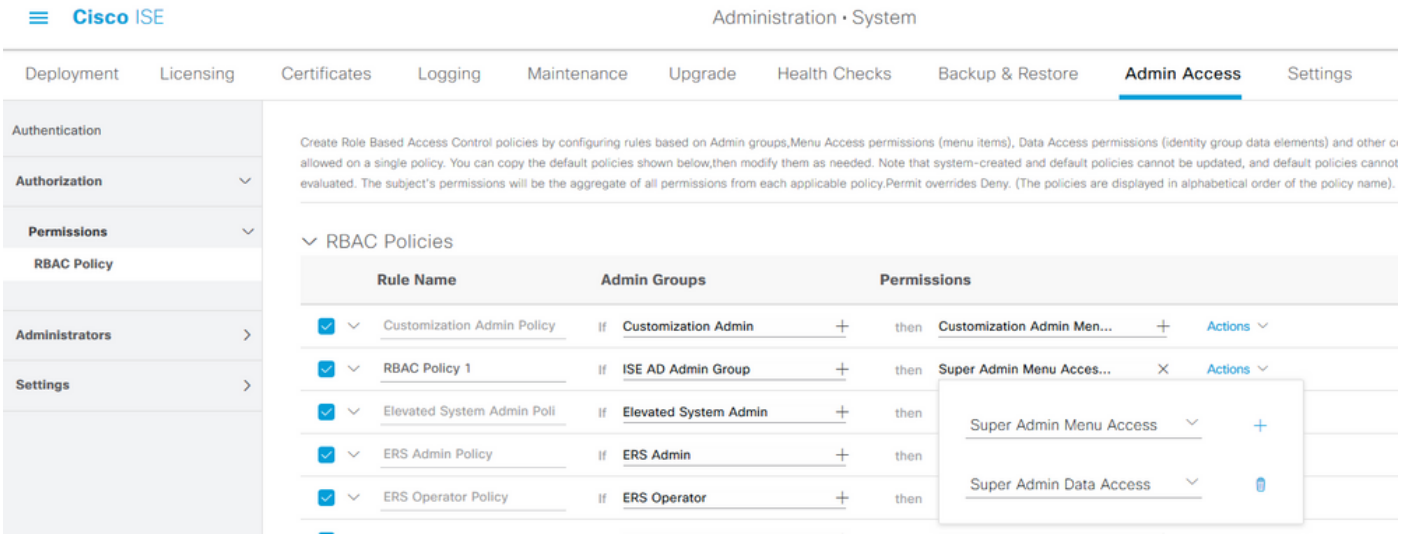
ISE 관리 그룹을 AD 그룹 매핑에 구성

이렇게 하면 권한 부여가 AD의 그룹 구성원 자격을 기반으로 관리자에 대한 RBAC(Role Based Access Control) 권한을 결정할 수 있습니다.Cisco ISE 관리 그룹을 정의하고 이를 AD 그룹에 매핑하려면 Administration(관리) **> System(시스템) > Admin Access(관리 액세스) > Administrators(관리자) > Admin Groups(관리 그룹)로 이동합니다**.Add(**추가**)를 클릭하고 새 Admin 그룹의 이름을 입력합니다.유형 필드에서 **외부** 확인란을 선택합니다.External **Groups(외부 그룹**) 드롭다운 메뉴에서 이 관리 그룹을 매핑할 AD 그룹을 선택합니다(위의 Select Directory Groups(디렉토리 그룹 선택) 섹션에 정의됨). 변경 사항을 제출합니다.



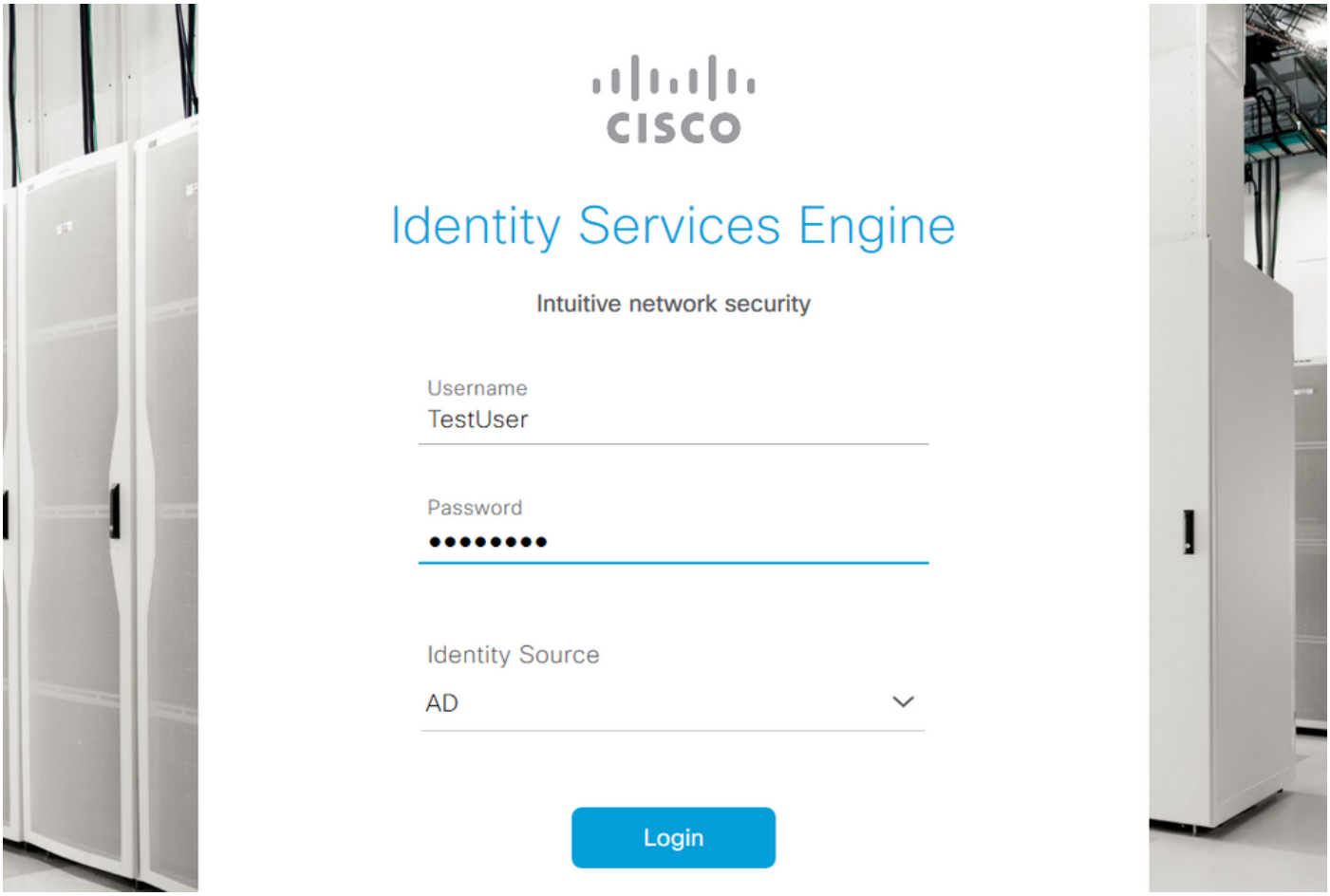
관리 그룹에 대한 RBAC 권한 설정

이전 섹션에서 생성한 관리 그룹에 RBAC 권한을 할당하려면 **Administration > System > Admin Access > Authorization > RBAC Policy로 이동합니다**.오른쪽 **Actions** 드롭다운 메뉴에서 Insert **new policy를 선택합니다**.새 규칙을 생성하고 위의 섹션에 정의된 관리 그룹과 매핑한 다음 원하는 데이터 및 메뉴 액세스 권한을 사용하여 할당한 다음 **Save**를 클릭합니다.

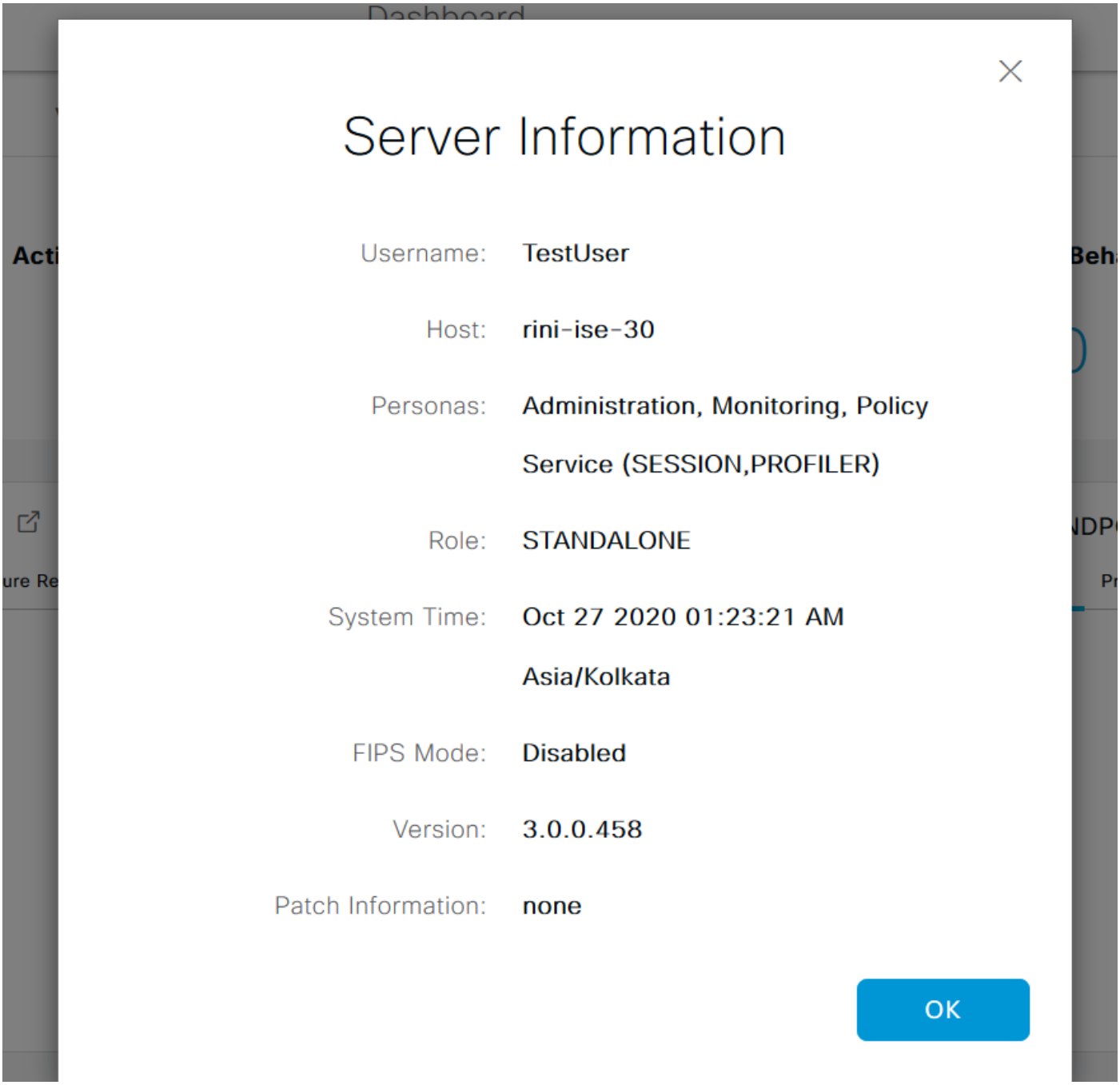


AD 자격 증명을 사용하여 ISE에 액세스하고 확인

관리 GUI에서 로그아웃합니다.**Identity Source** 드롭다운 메뉴에서 Join Point 이름을 선택합니다 .AD 데이터베이스의 사용자 이름과 암호를 입력하고 로그인합니다.



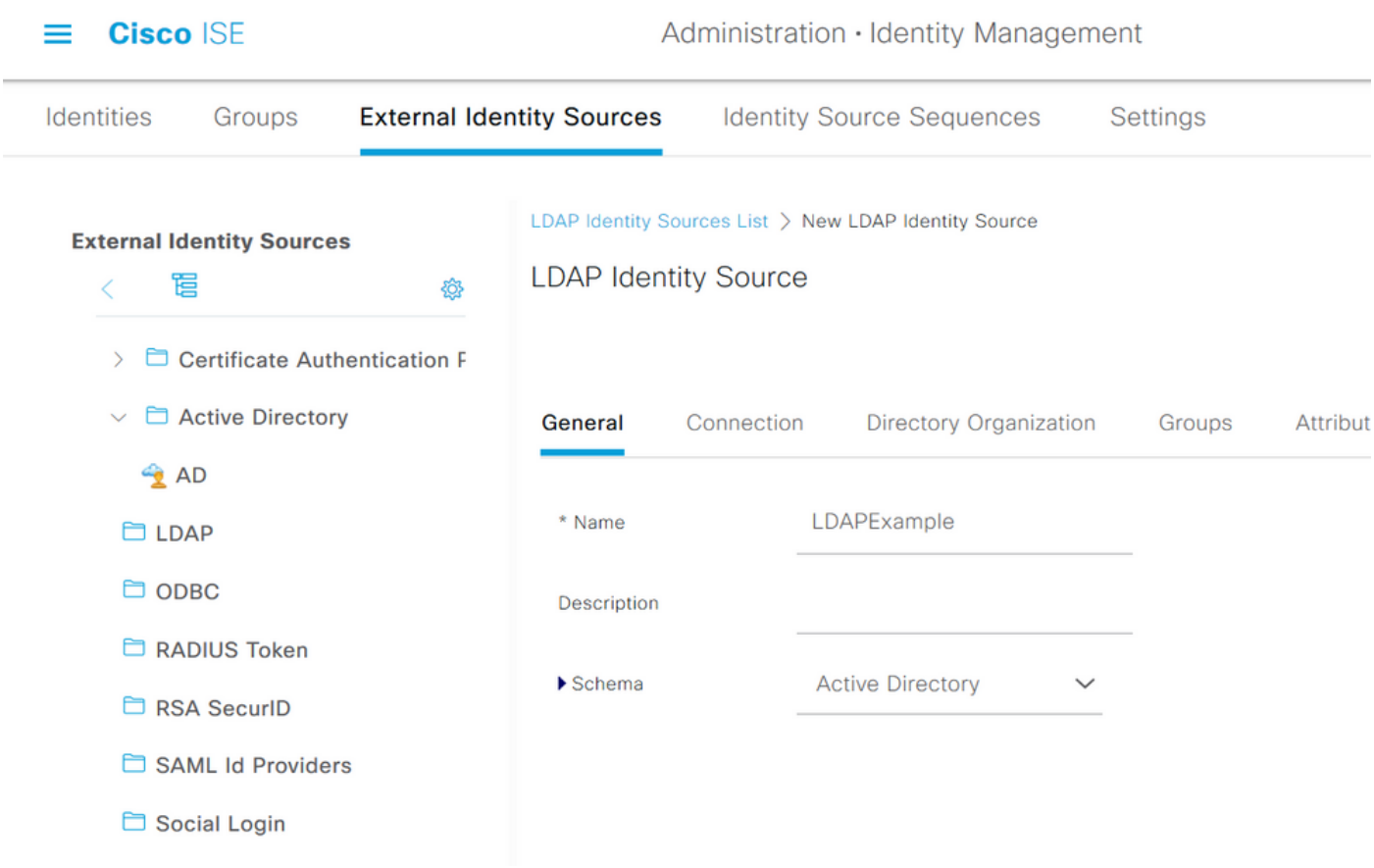
컨피그레이션이 제대로 작동하는지 확인하려면 ISE GUI의 오른쪽 상단 모서리에 있는 **Settings** 아이콘에서 인증된 사용자 이름을 확인합니다.Server Information(**서버 정보**)으로 이동하고 사용자 이름을 확인합니다.



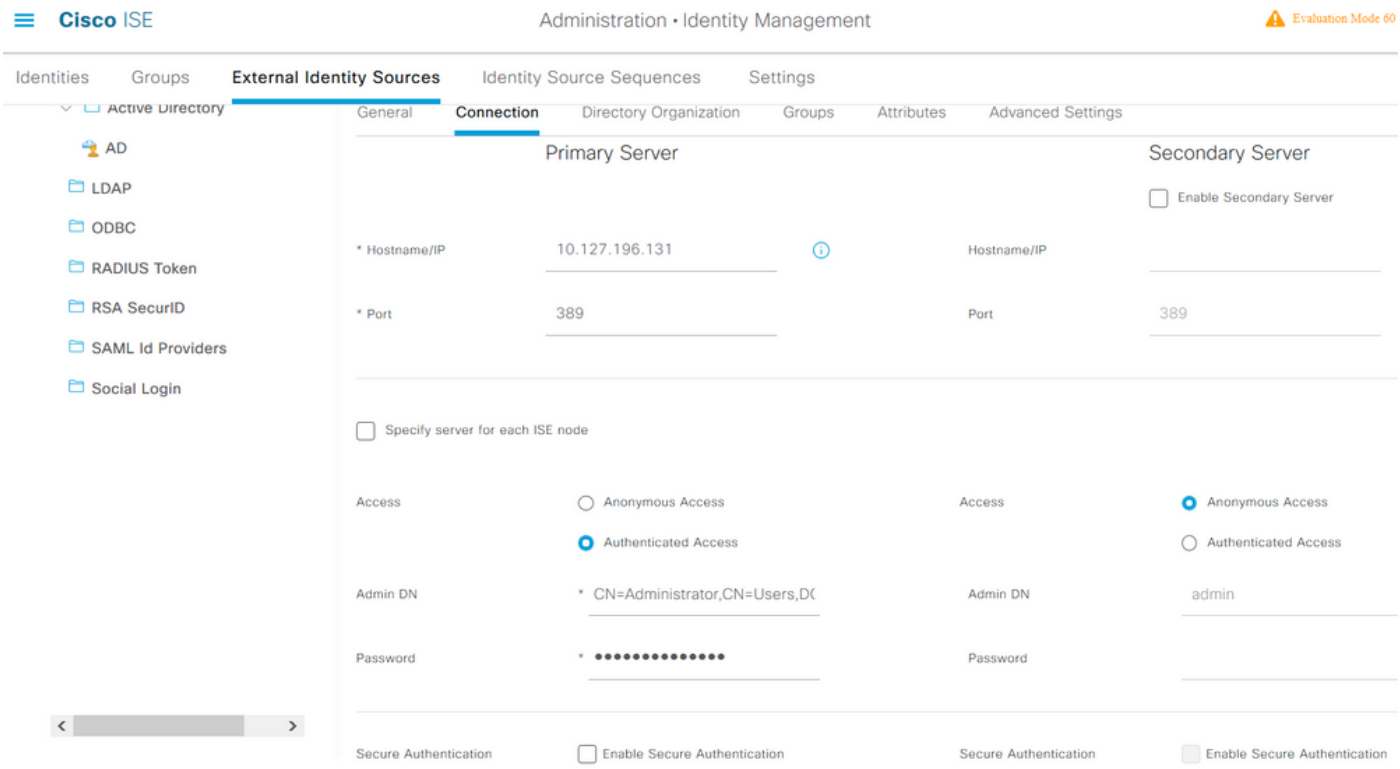
LDAP로 관리 포털 액세스 구성

LDAP에 ISE 조인

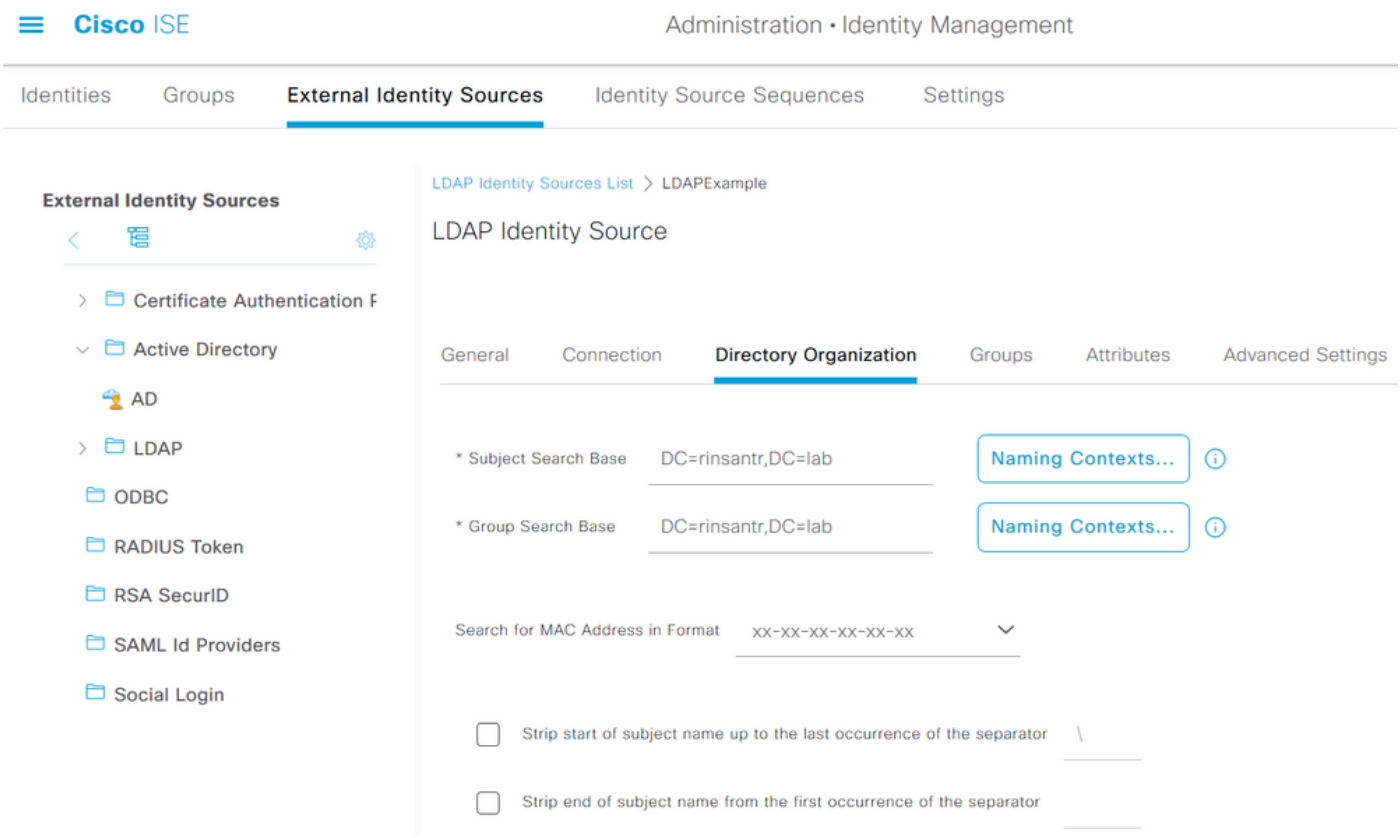
Administration(관리) > **Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > Active Directory > LDAP로 이동합니다**.General(**일반**) 탭에서 LDAP의 이름을 입력하고 스키마를 **Active Directory**로 선택합니다.



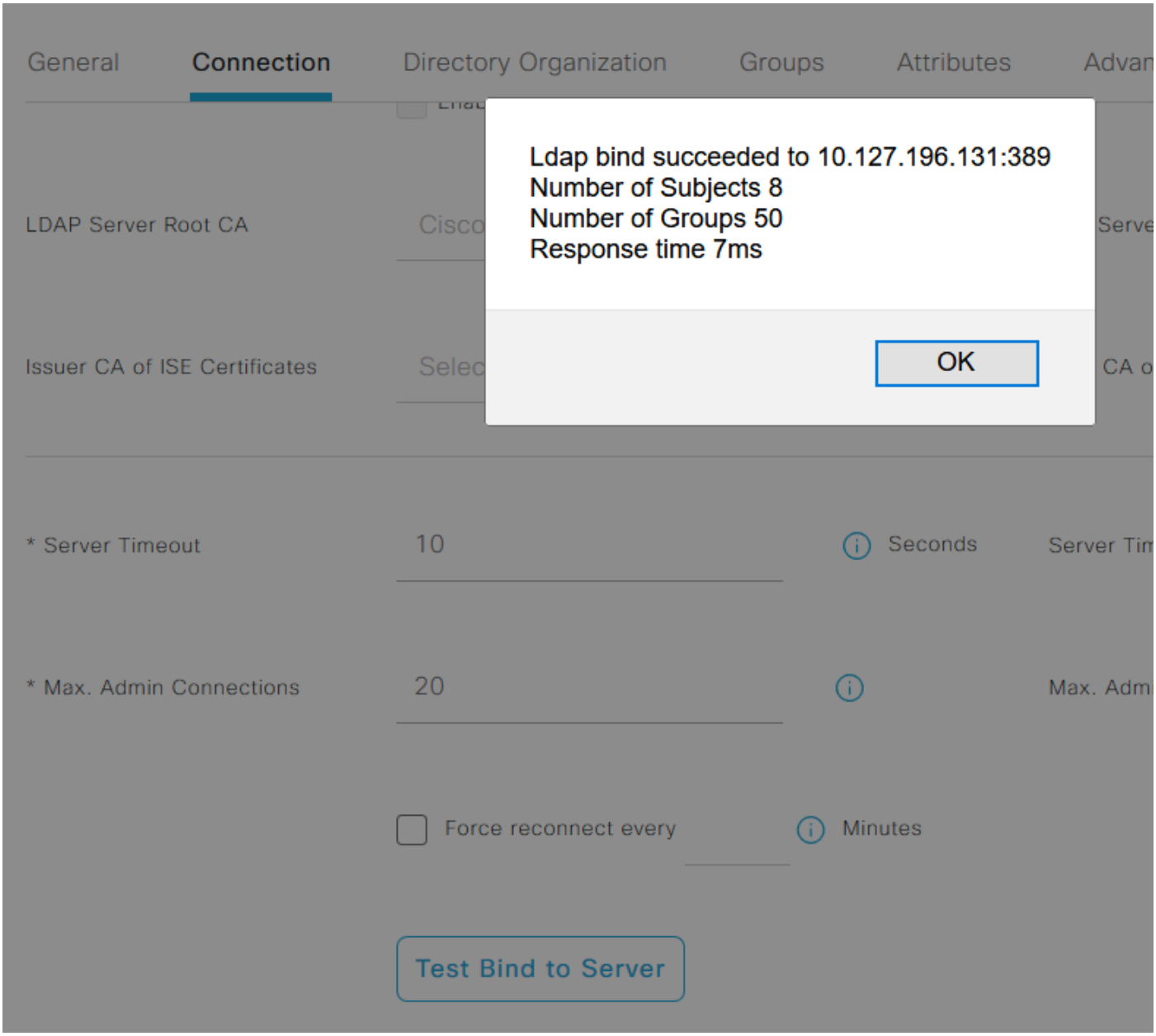
다음으로 연결 유형을 구성하려면 **Connection** 탭으로 이동합니다.여기서는 포트 389(LDAP)/636(LDAP-Secure)과 함께 기본 LDAP 서버의 호스트 이름/IP를 설정합니다. LDAP 서버의 관리자 비밀번호와 함께 DN(Admin Distinguished Name)의 경로를 입력합니다.



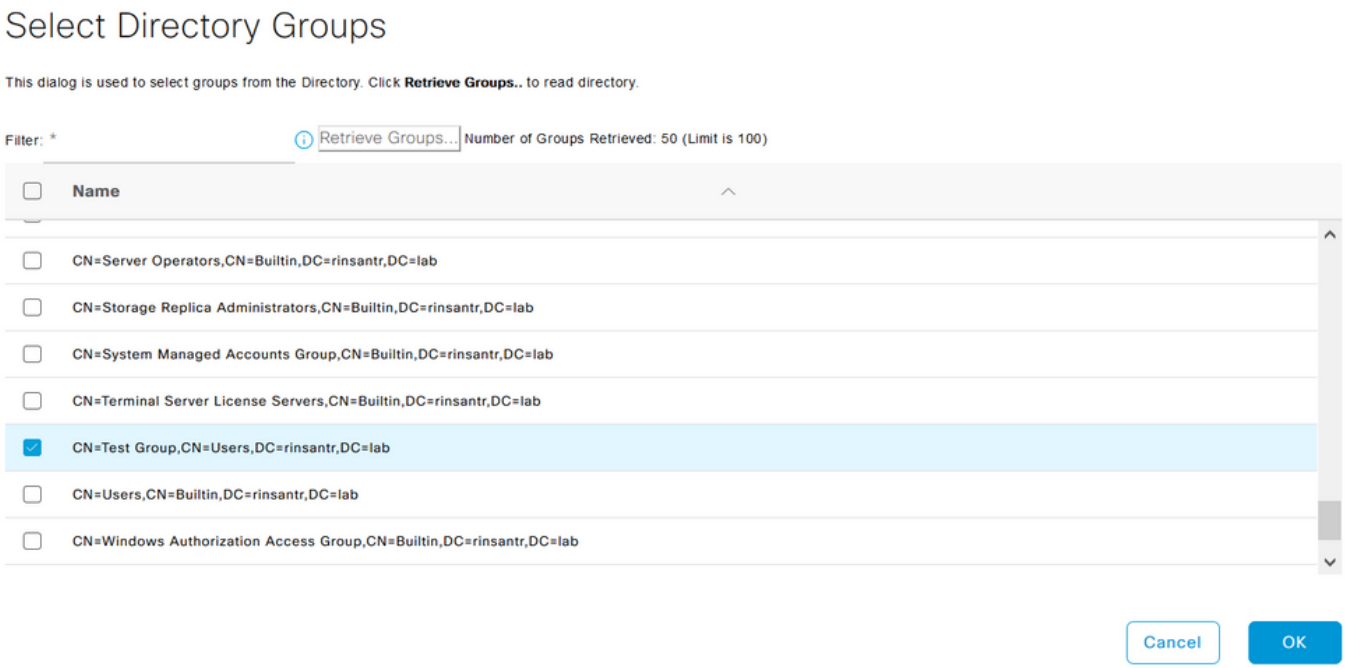
다음으로, **Directory Organization(디렉토리 조직)** 탭으로 이동하고 **Naming Contexts(명명 컨텍스트)**를 클릭하여 LDAP 서버에 저장된 사용자 계층 구조를 기반으로 올바른 사용자 조직 그룹을 선택합니다.

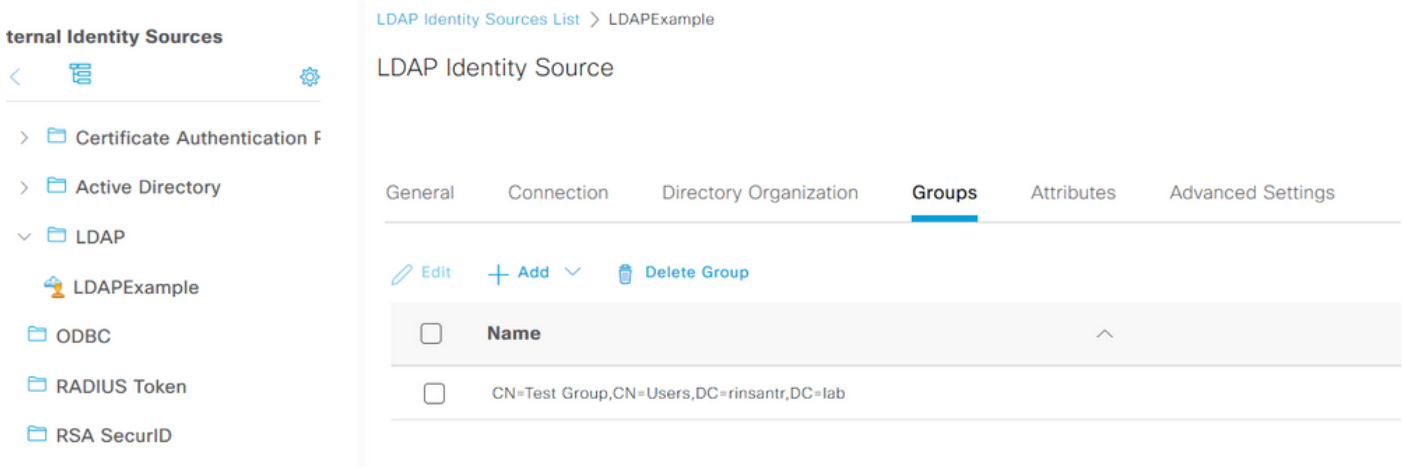


ISE에서 **LDAP** 서버**의 연결**을 테스트하려면 Connection(**연결**) 탭 아래의 Test Bind to Server(서버에 바인딩 테스트)를 클릭합니다.



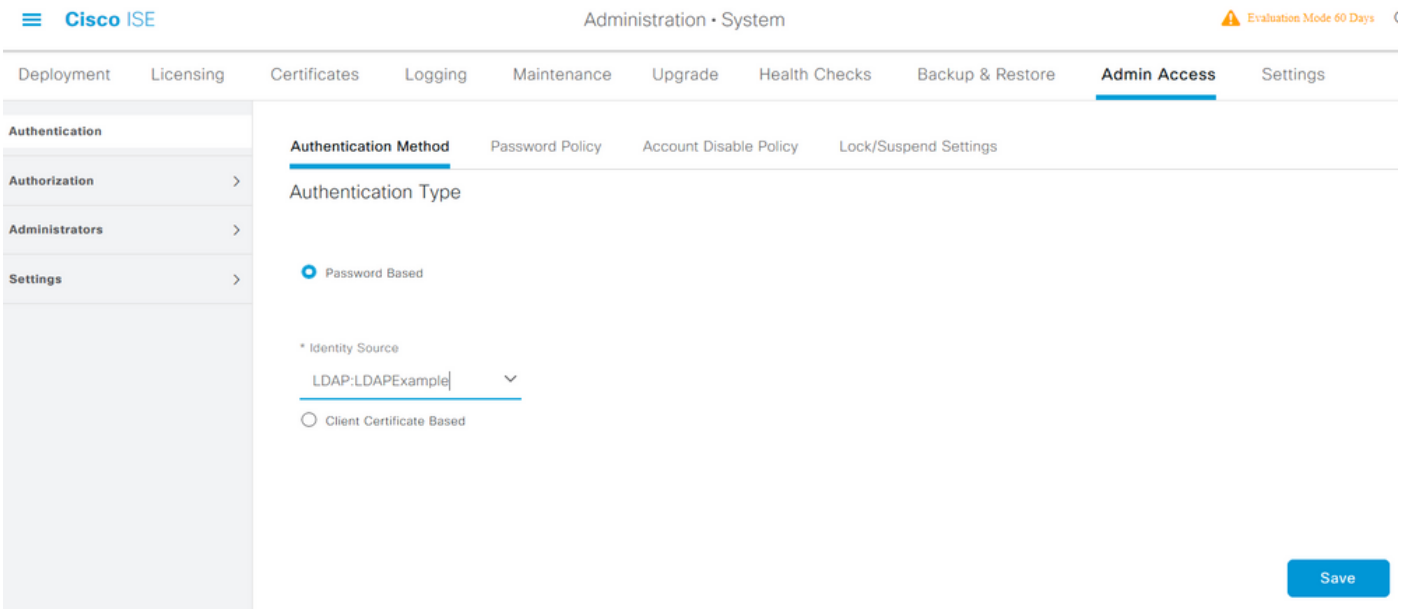
이제 **그룹** 탭으로 이동하고 Add(추가) **> Select Groups From Directory(디렉토리에서 그룹 선택) > Retrieve Groups(그룹 검색)를 클릭합니다**.관리자가 속한 그룹을 하나 이상 가져오고 **OK**(확인)를 클릭한 다음 **Save(저장)**를 클릭합니다.





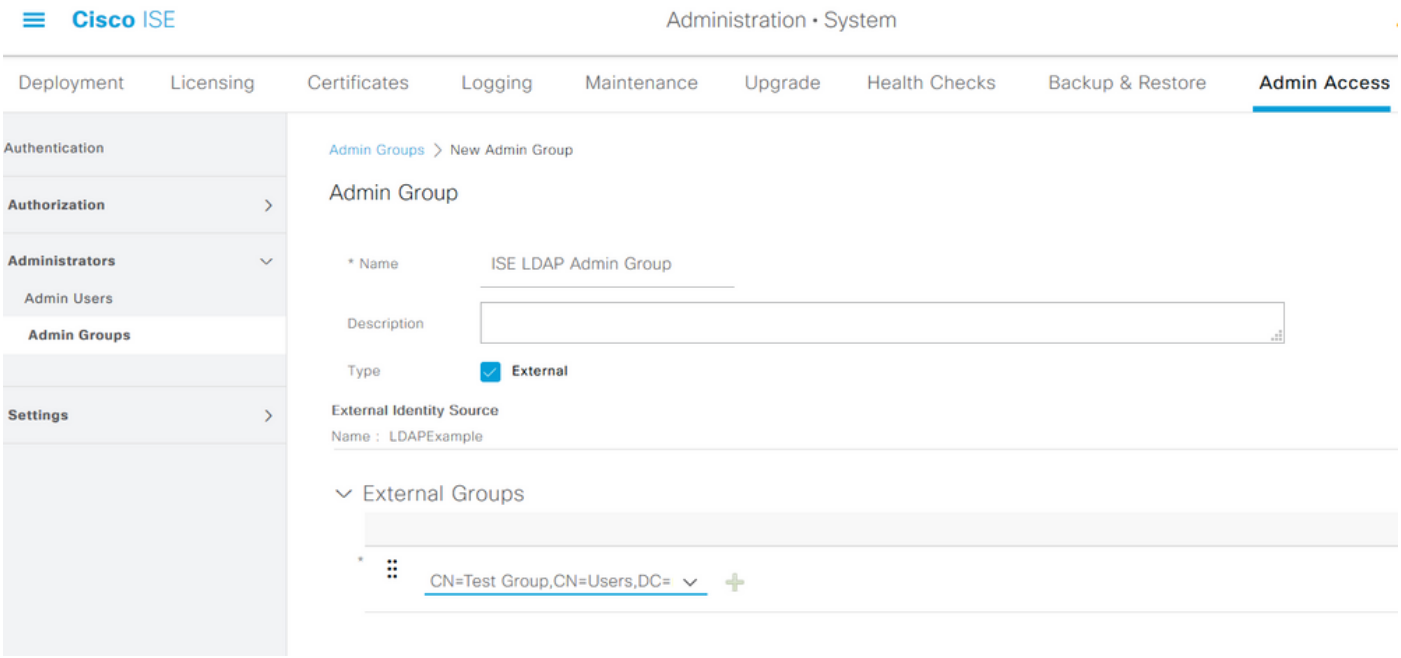
LDAP 사용자에 대한 관리 액세스 활성화

LDAP를 사용하여 ISE의 비밀번호 기반 인증을 활성화하려면 Administration(관리) **> System(시스템) > Admin Access(관리 액세스) > Authentication(인증)으로 이동합니다**.Authentication Method(**인증 방법**) 탭에서 **Password-Based** 옵션을 선택합니다.Identity **Source**(ID 소스) 드롭다운 메뉴에서 LDAP를 선택하고 Save(저장)를 **클릭합니다**.



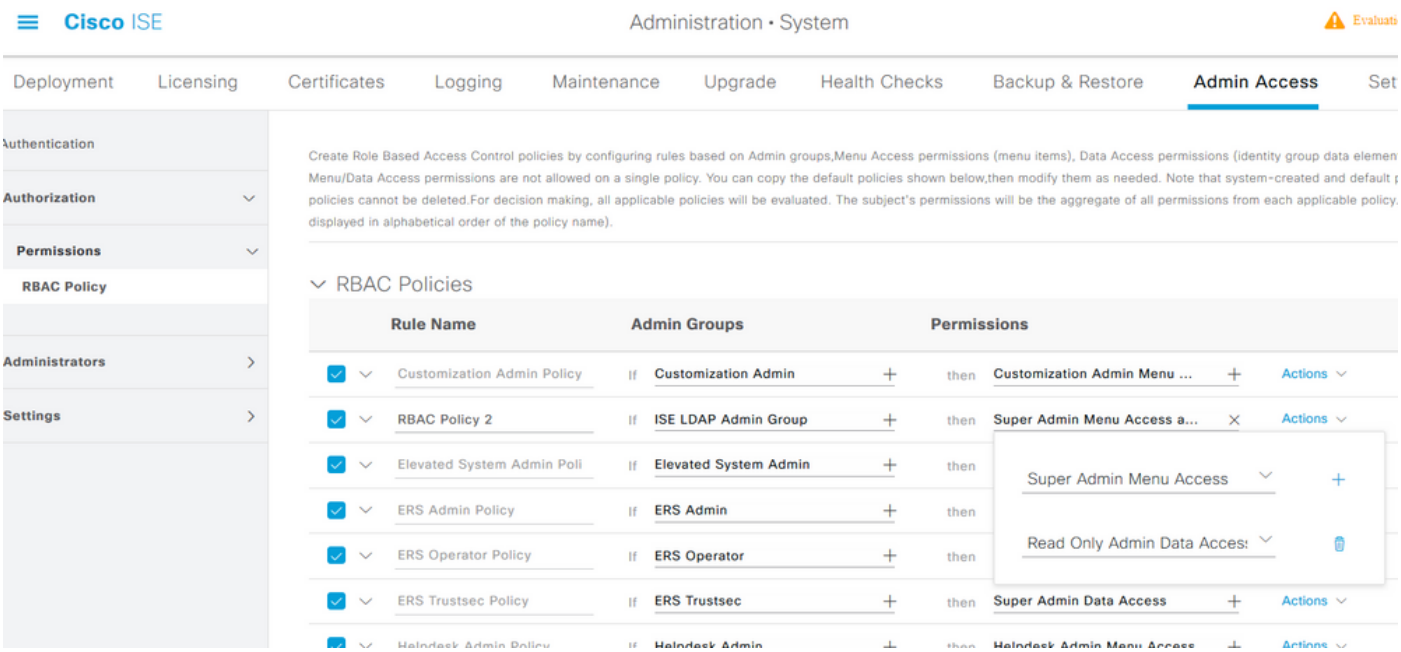
ISE 관리 그룹을 LDAP 그룹에 매핑

이렇게 하면 구성된 사용자가 RBAC 정책의 권한 부여를 기반으로 관리자 액세스 권한을 얻을 수 있으며, 이는 사용자의 LDAP 그룹 구성원 자격을 기반으로 합니다.Cisco ISE 관리 그룹을 정의하고 이를 LDAP 그룹에 매핑하려면 **Administration > System > Admin Access > Administrators > Admin Groups로 이동합니다**.Add(**추가**)를 클릭하고 새 Admin 그룹의 이름을 입력합니다.유형 필드에서 **외부** 확인란을 선택합니다.External **Groups(외부 그룹**) 드롭다운 메뉴에서 이 관리 그룹이 매핑될 LDAP 그룹을 선택합니다(이전에 검색되고 정의됨). 변경 사항을 제출합니다.



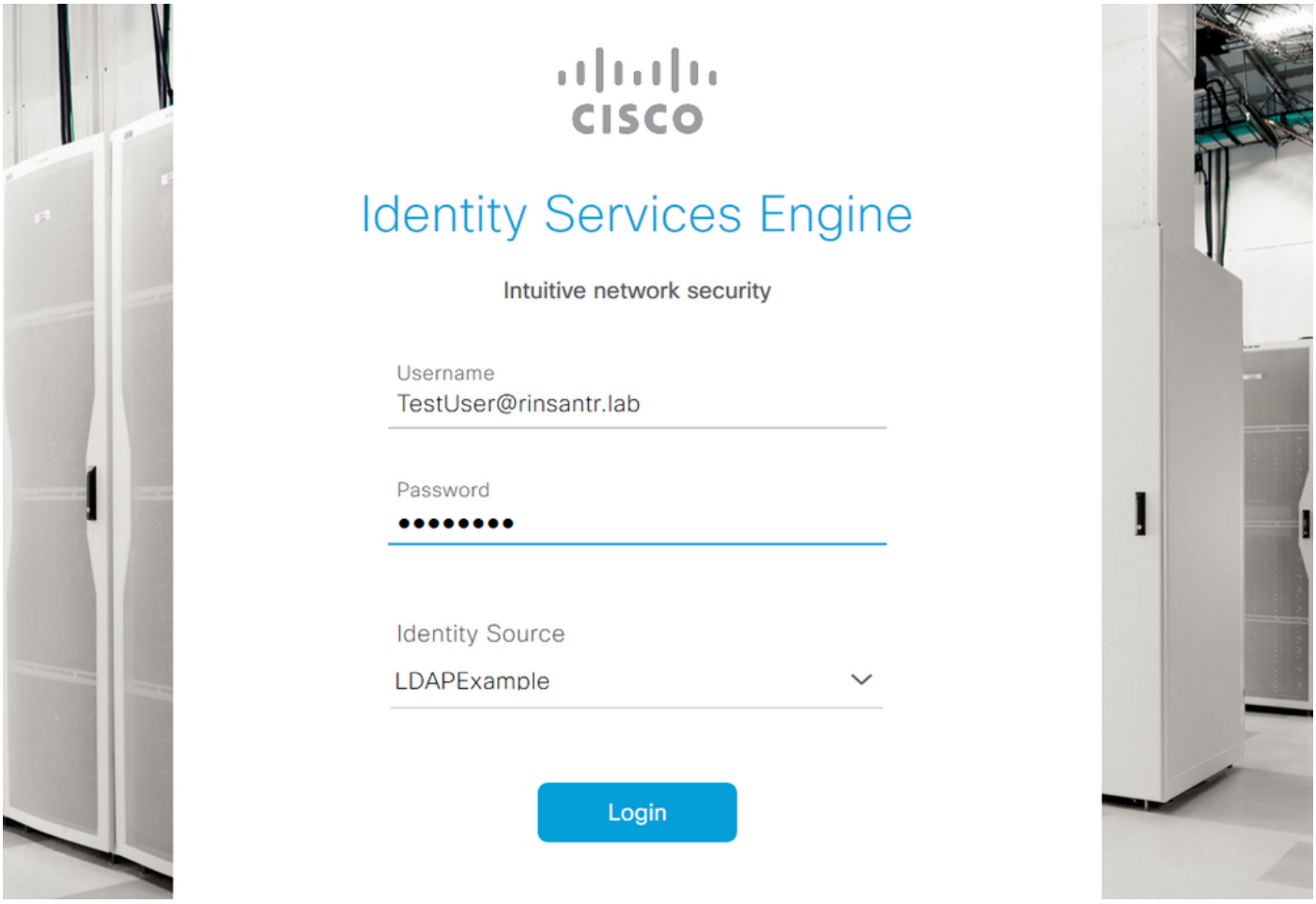
관리 그룹에 대한 RBAC 권한 설정

이전 섹션에서 생성한 관리 그룹에 RBAC 권한을 할당하려면 **Administration > System > Admin Access > Authorization > RBAC Policy로 이동합니다**.오른쪽 **Actions** 드롭다운 메뉴에서 Insert **new policy를 선택합니다**.새 규칙을 생성하고 위의 섹션에 정의된 관리 그룹과 매핑한 다음 원하는 데이터 및 메뉴 액세스 권한을 사용하여 할당한 다음 **Save**를 클릭합니다.

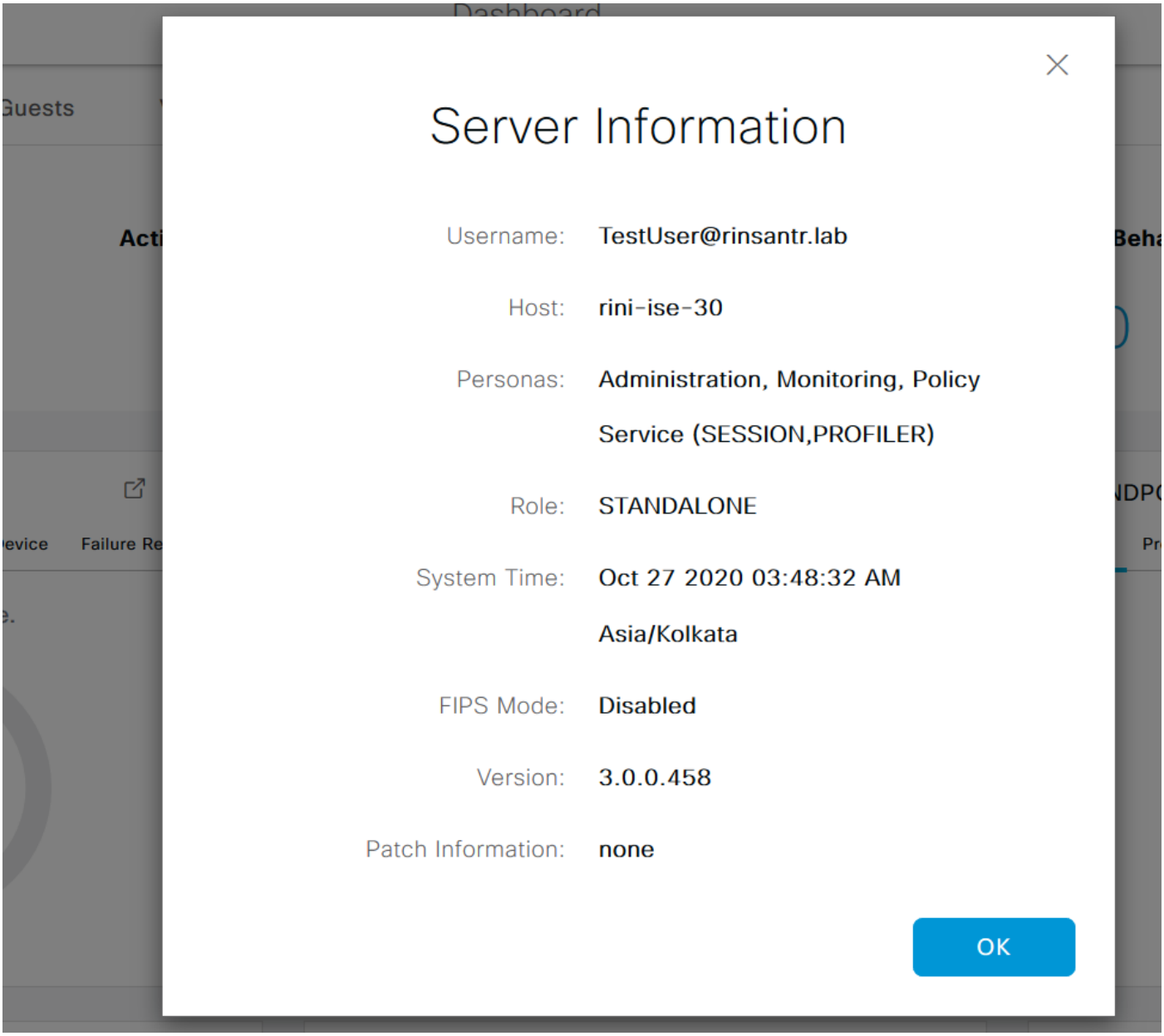


LDAP 자격 증명을 사용하여 ISE에 액세스하고 확인

관리 GUI에서 로그아웃합니다.**Identity Source** 드롭다운 메뉴에서 LDAP 이름을 선택합니다.LDAP 데이터베이스의 사용자 이름과 비밀번호를 입력하고 로그인합니다.



컨피그레이션이 제대로 작동하는지 확인하려면 ISE GUI 오른쪽 상단 모서리에 있는 **Settings** 아이콘에서 인증된 사용자 이름을 확인합니다.Server Information(**서버 정보**)으로 이동하고 사용자 이름을 확인합니다.


Server Information
Username: TestUser@rinsantr.lab
Host: rini-ise-30
Personas: Administration, Monitoring, Policy Service (SESSION,PROFILER)
Role: STANDALONE
System Time: Oct 27 2020 03:48:32 AM Asia/Kolkata
FIPS Mode: Disabled
Version: 3.0.0.458
Patch Information: none
OK