

# LDS(Lightweight Directory Access Protocol)로 ISE 역할 기반 액세스 제어 구성

## 목차

---

### [소개](#)

### [사전 요구 사항](#)

#### [요구 사항](#)

### [설정](#)

#### [LDAP에 ISE 조인](#)

#### [LDAP 사용자에게 대한 관리 액세스 활성화](#)

#### [LDAP 그룹에 관리 그룹 매핑](#)

##### [메뉴 액세스에 대한 권한 설정](#)

##### [데이터 액세스에 대한 권한 설정](#)

##### [관리자 그룹에 대한 RBAC 권한 설정](#)

### [다음을 확인합니다.](#)

#### [AD 자격 증명으로 ISE 액세스](#)

### [문제 해결](#)

#### [일반 정보](#)

#### [패킷 캡처 분석](#)

#### [로그 분석](#)

##### [port-server.log 확인](#)

##### [ise-psc.log 확인](#)

---

## 소개

이 문서에서는 Cisco ISE(Identity Services Engine) 관리 GUI에 대한 관리 액세스를 위해 LDAP(Lightweight Directory Access Protocol)를 외부 ID 저장소로 사용하기 위한 컨피그레이션 예를 설명합니다.

## 사전 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE 버전 3.0 컨피그레이션
- LDAP

## 요구 사항

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE 버전 3.0
- Windows Server 2016

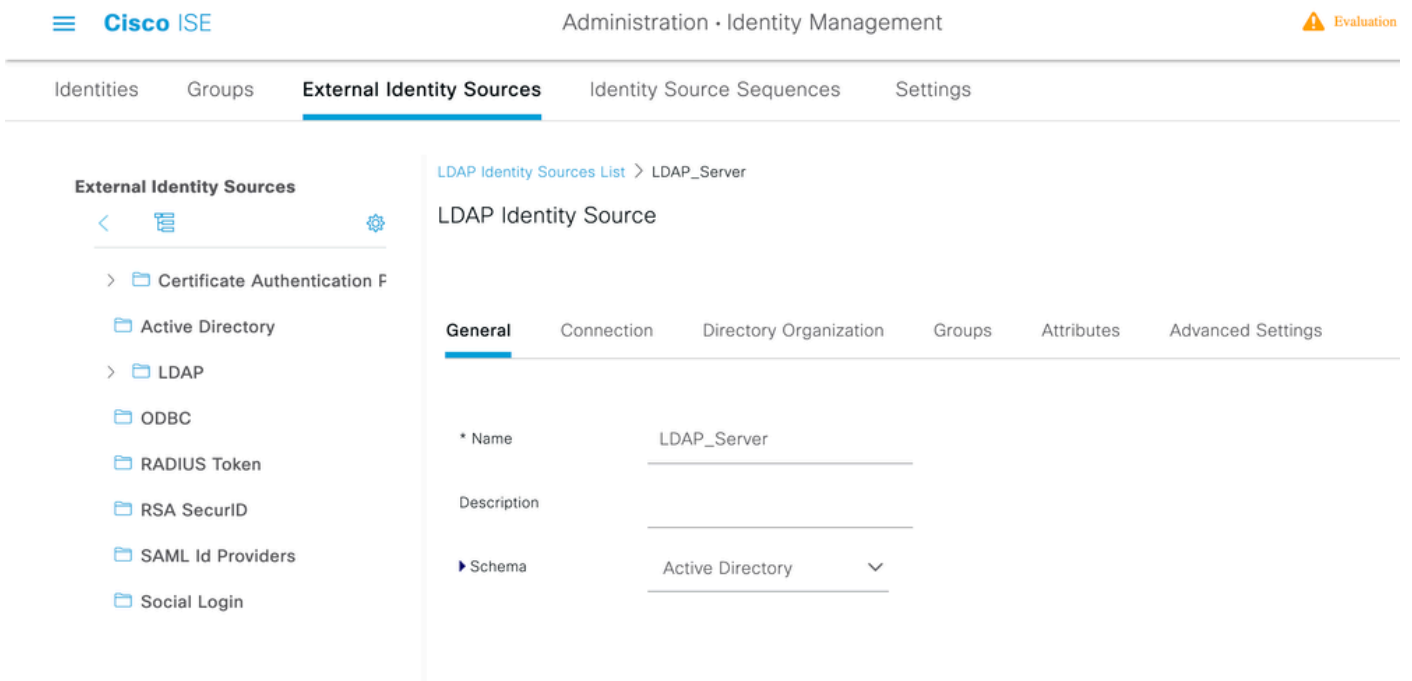
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 설정

이 섹션을 사용하여 LDAP 기반 사용자가 ISE GUI에 대한 관리/사용자 지정 기반 액세스를 얻도록 구성할 수 있습니다. 아래 컨피그레이션에서는 LDAP 프로토콜 쿼리를 사용하여 Active Directory에서 사용자를 가져와 인증을 수행합니다.

### LDAP에 ISE 조인

1. Administration(관리) > Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > Active Directory > LDAP로 이동합니다.
2. General(일반) 탭에서 LDAP의 이름을 입력하고 스키마 Active Directory를 선택합니다.



### 연결 유형 및 LDAP 구성 구성

1. ISE > Administration > Identity Management > External Identity Sources > LDAP로 이동합니다.
2. 포트 389(LDAP)/636(LDAP-Secure)과 함께 기본 LDAP 서버의 호스트 이름을 구성합니다.
3. LDAP 서버의 관리자 비밀번호와 함께 관리자 DN(고유 이름)의 경로를 입력합니다.
4. Test Bind Server(바인딩 서버 테스트)를 클릭하여 ISE에서 LDAP 서버 연결성을 테스트합니다.

Identities Groups **External Identity Sources** Identity Source Sequences Settings

> Certificate Authentication F

Active Directory

LDAP

ODBC

RADIUS Token

RSA SecurID

SAML Id Providers

Social Login

General **Connection** Directory Organization Groups Attributes Advanced Settings

Primary Server		Secondary Server	
* Hostname/IP	10.127.197.180	Hostname/IP	
* Port	389	Port	389
<input type="checkbox"/> Specify server for each ISE node			
Access	<input type="radio"/> Anonymous Access <input checked="" type="radio"/> Authenticated Access	Access	<input checked="" type="radio"/> Anonymous Access <input type="radio"/> Authenticated Access
Admin DN	* cn=Administrator,cn=Users,dc=	Admin DN	
Password	* .....	Password	

## 디렉토리 조직, 그룹 및 속성 구성

1. LDAP 서버에 저장된 사용자 계층에 따라 올바른 사용자 조직 그룹을 선택합니다.

Identities Groups **External Identity Sources** Identity Source Sequences Settings

> Certificate Authentication F

Active Directory

LDAP

ODBC

RADIUS Token

RSA SecurID

SAML Id Providers

Social Login

General **Directory Organization** Connection Groups Attributes Advanced Settings

\* Subject Search Base dc=anshsinh,dc=local [Naming Contexts...](#)

\* Group Search Base dc=anshsinh,dc=local [Naming Contexts...](#)

Search for MAC Address in Format xx-xx-xx-xx-xx-xx

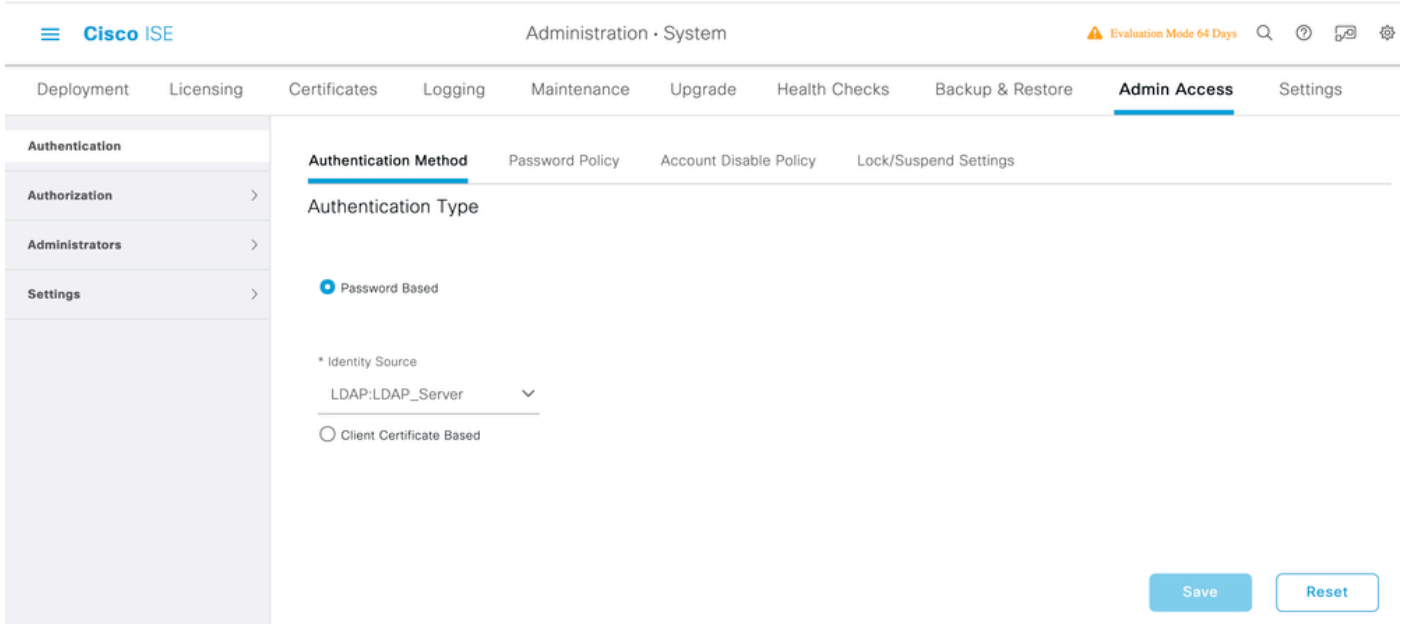
Strip start of subject name up to the last occurrence of the separator \

Strip end of subject name from the first occurrence of the separator

## LDAP 사용자에게 대한 관리 액세스 활성화

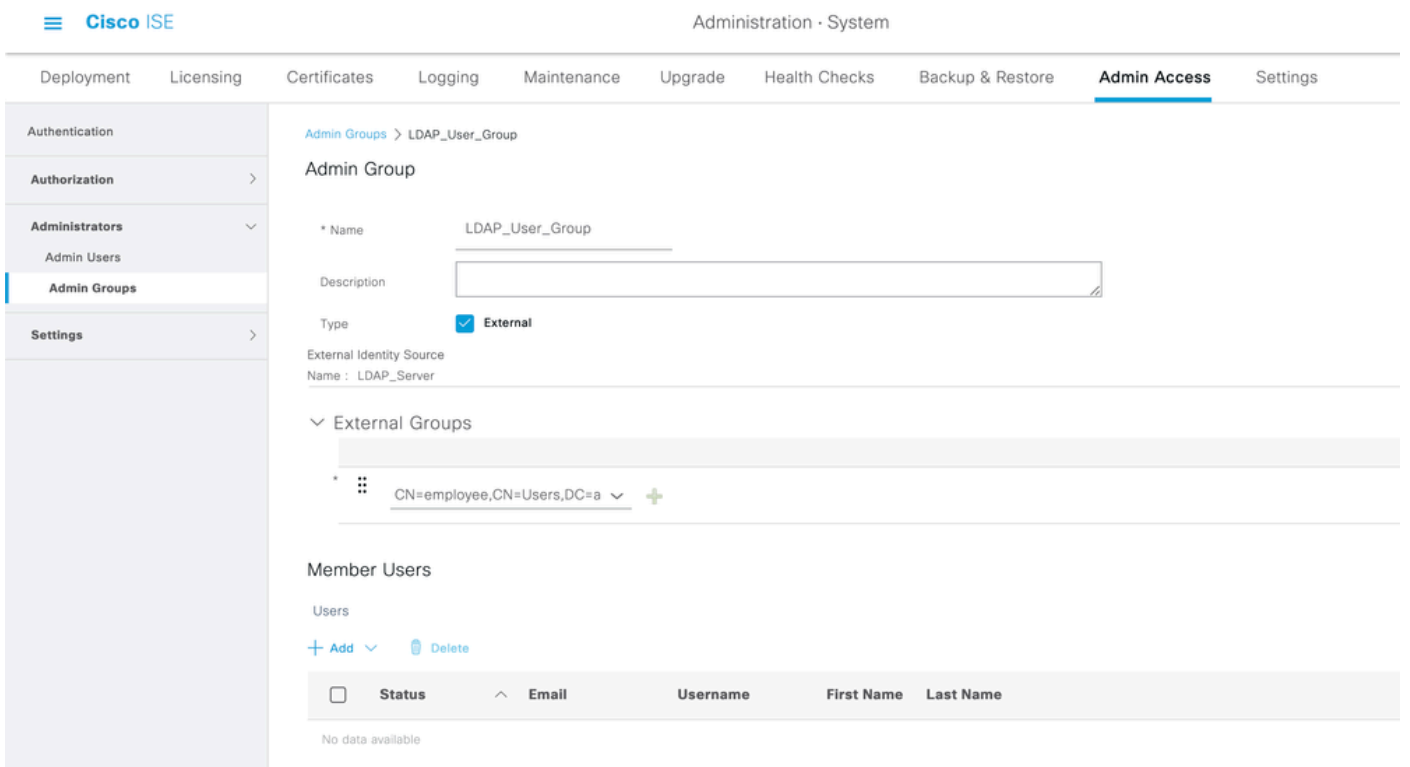
비밀번호 기반 인증을 활성화하려면 다음 단계를 완료하십시오.

1. ISE > Administration > System > Admin Access > Authentication으로 이동합니다.
2. Authentication Method(인증 방법) 탭에서 Password-Based(비밀번호 기반) 옵션을 선택합니다.
3. Identity Source 드롭다운 메뉴에서 LDAP를 선택합니다.
4. Save Changes(변경 사항 저장)를 클릭합니다.



## LDAP 그룹에 관리 그룹 매핑

ISE에서 Admin Group(관리 그룹)을 구성하고 이를 AD 그룹에 매핑합니다. 이렇게 하면 구성된 사용자가 그룹 구성원 자격을 기반으로 한 관리자에 대해 구성된 RBAC 권한을 기반으로 하는 권한 부여 정책에 따라 액세스 권한을 얻을 수 있습니다.



## 메뉴 액세스에 대한 권한 설정

1. ISE > Administration > System > Authorization > Permissions > Menu access로 이동합니다
2. 관리자 사용자가 ISE GUI에 액세스할 수 있도록 메뉴 액세스를 정의합니다. 사용자가 필요한 경

우 일련의 작업만 수행할 수 있도록 사용자 지정 액세스를 위해 GUI에 표시하거나 숨기도록 하위 엔터티를 구성할 수 있습니다.

3. 저장을 클릭합니다.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Administration · System' and a menu with options like 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The left sidebar has a menu with 'Authentication', 'Authorization', 'Permissions', 'Menu Access', 'Data Access', 'RBAC Policy', 'Administrators', and 'Settings'. The main content area is titled 'Edit Menu Access Permission' and shows the configuration for 'LDAP\_Menu\_Access'. The 'Name' field is filled with 'LDAP\_Menu\_Access' and the 'Description' field is empty. Below this is the 'Menu Access Privileges' section, which includes a tree view of the 'ISE Navigation Structure' and radio buttons for 'Show' and 'Hide' permissions. The 'Show' option is selected.

데이터 액세스에 대한 권한 설정

1. ISE > Administration > System > Authorization > Permissions > Data access로 이동합니다.

2. ISE GUI의 ID 그룹에 대한 전체 액세스 또는 읽기 전용 액세스 권한을 가질 관리자 사용자의 데이터 액세스를 정의합니다.

3. 저장을 클릭합니다.

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Settings

Authentication

Authorization

Permissions

Menu Access

**Data Access**

RBAC Policy

Administrators

Settings

Data Access List > LDAP\_Data\_Access

Edit Data Access Permission

\* Name LDAP\_Data\_Access

Description

Data Access Privileges

- Admin Groups
- User Identity Groups
- Endpoint Identity Groups
- Network Device Groups

Permissions for Data Access

Full Access

Read Only Access

No Access

### 관리자 그룹에 대한 RBAC 권한 설정

1. ISE > Administration > System > Admin Access > Authorization > Policy로 이동합니다.
2. 오른쪽의 Actions 드롭다운 메뉴에서 Insert New Policy를 선택하여 새 정책을 추가합니다.
3. LDAP\_RBAC\_policy라는 새 규칙을 생성하고 Enable Administrative Access for AD(AD에 대한 관리 액세스 활성화) 섹션에 정의된 Admin Group(관리 그룹)에 매핑하고 메뉴 액세스 및 데이터 액세스에 대한 권한을 할당합니다.
4. Save Changes(변경 사항 저장)를 클릭하면 GUI의 오른쪽 아래 모서리에 저장된 변경 사항이 표시됩니다.

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Settings

Authentication

Authorization

Permissions

Menu Access

Data Access

**RBAC Policy**


Administrators


Settings

Create Role Based Access Control policies by configuring rules based on Admin groups, Menu Access permissions (menu items), Data Access permissions (identity group data elements) and other condition not allowed on a single policy. You can copy the default policies shown below, then modify them as needed. Note that system-created and default policies cannot be updated, and default policies cannot be evaluated. The subject's permissions will be the aggregate of all permissions from each applicable policy. Permit overrides Deny. (The policies are displayed in alphabetical order of the policy name).

RBAC Policies

Rule Name	Admin Groups	Permissions
Customization Admin Policy	Customization Admin	Customization Admin Menu ...
Elevated System Admin Poli	Elevated System Admin	System Admin Menu Access...
ERS Admin Policy	ERS Admin	Super Admin Data Access
ERS Operator Policy	ERS Operator	Super Admin Data Access
ERS Trustsec Policy	ERS Trustsec	Super Admin Data Access
Helpdesk Admin Policy	Helpdesk Admin	Helpdesk Admin Menu Access
Identity Admin Policy	Identity Admin	Identity Admin Menu Access...
LDAP_RBAC_Rule	LDAP_User_Group	LDAP_Menu_Access and L...
MnT Admin Policy	MnT Admin	LDAP_Menu_Access
Network Device Policy	Network Device Admin	LDAP_Data_Access
Policy Admin Policy	Policy Admin	
RBAC Admin Policy	RBAC Admin	RBAC Admin Menu Access ...

 참고: 슈퍼 관리자 사용자는 기본 시스템 생성 RBAC 정책 및 권한을 수정할 수 없습니다. 이렇게 하려면 필요에 따라 필요한 권한으로 새 RBAC 정책을 생성하고 이러한 정책을 관리자 그룹에 매핑해야 합니다.

 참고: 기본 슈퍼 관리자 그룹의 관리자 사용자만 다른 관리자 사용자를 수정하거나 삭제할 수 있습니다. 슈퍼 관리자 그룹의 메뉴 및 데이터 액세스 권한으로 복제된 관리자 그룹의 일부인 외부 매핑 사용자라도 관리자 사용자를 수정하거나 삭제할 수 없습니다.

## 다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

### AD 자격 증명으로 ISE 액세스

AD 자격 증명으로 ISE에 액세스하려면 다음 단계를 완료하십시오.

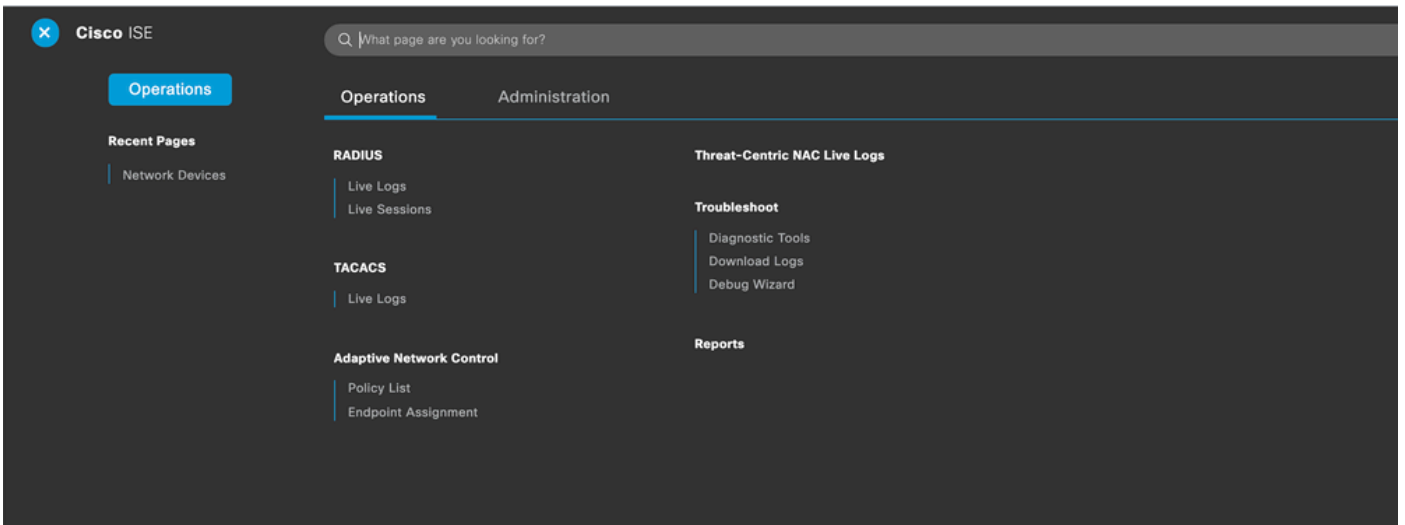
1. LDAP 사용자로 로그인하려면 ISE GUI를 엽니다.
2. Identity Source 드롭다운 메뉴에서 LDAP\_Server를 선택합니다.
3. LDAP 데이터베이스의 UPN 및 비밀번호를 입력하고 로그인합니다.



감사 보고서에서 관리자 로그인에 대한 로그인을 확인합니다. ISE > Operations > Reports > Audit > Administrators Logins로 이동합니다.

Logged At	Administrator	IP Address	Server	Event	Event Details
2020-10-10 10:57:41.217	admin	10.65.37.52	ise30	Administrator authentication succeeded	Administrator authentication successful
2020-10-10 10:57:32.098	admin2@anshshinh.local	10.65.37.52	ise30	Administrator logged off	User logged out
2020-10-10 10:56:47.668	admin2@anshshinh.local	10.65.37.52	ise30	Administrator authentication succeeded	Administrator authentication successful

이 컨피그레이션이 제대로 작동하는지 확인하려면 ISE GUI의 오른쪽 상단 모서리에서 인증된 사용자 이름을 확인합니다. 다음과 같이 메뉴에 대한 액세스가 제한된 사용자 지정 기반 액세스를 정의합니다.



## 문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

### 일반 정보

RBAC 프로세스의 문제를 해결하려면 ISE 관리 노드에서 이러한 ISE 구성 요소를 디버깅할 때 활성화해야 합니다.

RBAC - 로그인을 시도할 때 RBAC 관련 메시지가 인쇄됩니다(ise-psc.log).

access-filter - 리소스 필터 액세스(ise-psc.log)를 인쇄합니다.

runtime-AAA - 로그인 및 LDAP 상호 작용 메시지에 대한 로그를 인쇄합니다(prrt-server.log).

### 패킷 캡처 분석



**Bind Request and response using LDAP for the administrator.**

No.	Time	Source	Destination	Protocol	Length	Username	Content
579	2028-09-30 01:21:08.848523	10.106.32.184	10.127.197.188	LDAP	73		unbindRequest(4)
1040	2028-09-30 01:21:13.346421	10.106.32.184	10.127.197.188	LDAP	140		bindRequest(1) "CN=Administrator,CN=Users,DC=anshshinh,DC=local" simple
1041	2028-09-30 01:21:13.348424	10.127.197.188	10.106.32.184	LDAP	88		bindResponse(1) success
1043	2028-09-30 01:21:13.348757	10.106.32.184	10.127.197.188	LDAP	191		searchRequest(2) "dc=anshshinh,dc=local" wholeSubtree
1044	2028-09-30 01:21:13.349581	10.127.197.188	10.106.32.184	LDAP	475		searchResEntry(2) "CN=admin2,CN=Users,DC=anshshinh,DC=local"   searchRes
1048	2028-09-30 01:21:13.351026	10.106.32.184	10.127.197.188	LDAP	127		bindRequest(1) "CN=admin2,CN=Users,DC=anshshinh,DC=local" simple
1049	2028-09-30 01:21:13.352809	10.127.197.188	10.106.32.184	LDAP	88		bindResponse(1) success
15320	2028-09-30 01:21:40.068100	10.106.32.184	10.127.197.188	LDAP	191		searchRequest(3) "dc=anshshinh,dc=local" wholeSubtree
15325	2028-09-30 01:21:40.069045	10.127.197.188	10.106.32.184	LDAP	475		searchResEntry(3) "CN=admin2,CN=Users,DC=anshshinh,DC=local"   searchRes
15330	2028-09-30 01:21:40.069756	10.106.32.184	10.127.197.188	LDAP	127		bindRequest(2) "CN=admin2,CN=Users,DC=anshshinh,DC=local" simple
15337	2028-09-30 01:21:40.071344	10.127.197.188	10.106.32.184	LDAP	88		bindResponse(2) success

Search request and response Entry for the username to the mapped LDAP group.

Bind success for the username search

## 로그 분석

### prrt-server.log 확인

PAPAuthenticator,2020-10-10 08:54:00,621,DEBUG,0x7f852bee3700,cntx=0002480105,sesn=ise30/389444264/3178

IdentitySequence,2020-10-10 08:54:00,627,DEBUG,0x7f852c4e9700,cntx=0002480105,sesn=ise30/389444264/3178

LDAPIDStore,2020-10-10 08:54:00,628,DEBUG,0x7f852c4e9700,cntx=0002480105,sesn=ise30/389444264/3178,CPMS

Server,2020-10-10 08:54:00,634,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessi

Connection,2020-10-10 08:54:00,634,DEBUG,0x7f85293b8700,LdapConnectionContext::sendSearchRequest(id = 1

Server,2020-10-10 08:54:00,635,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessi

Server,2020-10-10 08:54:00,635,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessi

Server,2020-10-10 08:54:00,636,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessi

Server,2020-10-10 08:54:00,636,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessi

Connection,2020-10-10 08:54:00,636,DEBUG,0x7f85293b8700,LdapConnectionContext::sendBindRequest(id = 122

Server,2020-10-10 08:54:00,640,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessi

## ise-psc.log 확인

이 로그에서 네트워크 장치 리소스에 액세스를 시도 할 때 admin2 사용자에게 사용된 RBAC 정책을 확인 할 수 있습니다.

```
2020-10-10 08:54:24,474 DEBUG [admin-http-pool51][] com.cisco.cpm.rbacfilter.AccessUtil -:admin2@anshs
2020-10-10 08:54:24,524 INFO [admin-http-pool51][] cpm.admin.ac.actions.NetworkDevicesLPInputAction -
2020-10-10 08:54:24,524 DEBUG [admin-http-pool51][] cisco.ise.rbac.authorization.RBACAuthorization -:a
2020-10-10 08:54:24,526 DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImp
2020-10-10 08:54:24,526 DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImp
2020-10-10 08:54:24,528 DEBUG [admin-http-pool51][] cisco.ise.rbac.authorization.RBACAuthorization -:a
2020-10-10 08:54:24,528 INFO [admin-http-pool51][] cpm.admin.ac.actions.NetworkDevicesLPInputAction -
2020-10-10 08:54:24,534 INFO [admin-http-pool51][] cisco.cpm.admin.license.TrustSecLicensingUIFilter
2020-10-10 08:54:24,593 DEBUG [admin-http-pool51][] cisco.ise.rbac.authorization.RBACAuthorization -:a
2020-10-10 08:54:24,595 DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImp
2020-10-10 08:54:24,597 DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImp
2020-10-10 08:54:24,604 INFO [admin-http-pool51][] cisco.cpm.admin.license.TrustSecLicensingUIFilter
```

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.