

# ISE Role Based Access Control with LDAP

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Configurations](#)

[Join ISE to LDAP](#)

[Enable Administrative Access for LDAP Users](#)

[Map the Admin Group to LDAP Group](#)

[Set Permissions for Menu Access](#)

[Set Permissions for Data Access](#)

[Set RBAC Permissions for the Admin Group](#)

[Verify](#)

[Access ISE with AD Credentials](#)

[Troubleshoot](#)

[General information](#)

[Packet Capture Analysis](#)

[Log Analysis](#)

[Verify the prrt-server.log](#)

[Verify the ise-psc.log](#)

## Introduction

This document describes a configuration example for the use of the Lightweight Directory Access Protocol (LDAP) as an external identity store for administrative access to the Cisco Identity Services Engine (ISE) management GUI.

## Prerequisites

Cisco recommends that you have knowledge of these topics:

- Configuration of Cisco ISE Versions 3.0
- LDAP (Lightweight Directory Access Protocol)

## Requirements

The information in this document is based on these software and hardware versions:

- Cisco ISE Version 3.0
- Windows Server 2016

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

# Configurations

Use the below section to configure an LDAP based user to get the administrative / custom based access to the ISE GUI . The below configuration uses the LDAP protocol queries in order to fetch the user from Active directory to perform the authentication.

## Join ISE to LDAP

1. Navigate to **Administration > Identity Management > External Identity Sources > Active Directory > LDAP.**
2. Under the **General** tab, enter the name of the LDAP and choose the schema Active Directory.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb navigation is Administration > Identity Management > External Identity Sources > LDAP\_Identity\_Sources\_List > LDAP\_Server. The left sidebar shows the navigation tree with 'External Identity Sources' expanded to 'LDAP'. The main content area is titled 'LDAP Identity Source' and has tabs for 'General', 'Connection', 'Directory Organization', 'Groups', 'Attributes', and 'Advanced Settings'. The 'General' tab is active, showing the following fields:

- \* Name: LDAP\_Server
- Description: (empty)
- Schema: Active Directory (dropdown menu)

## Configure Connection type and LDAP configuration

1. Navigate to **ISE > Administration > Identity Management > External Identity Sources > LDAP.**
2. Configure the Hostname of the Primary LDAP server along with the port 389(LDAP)/636 (LDAP-Secure) .
3. Enter the path for the Admin distinguished name (DN) with the admin password for the LDAP server .
4. Click on Test Bind Server to test the reachability of LDAP server from ISE .

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		<input type="checkbox"/> Enable Secondary Server	
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	

## Configure the Directory organization, Groups, and Attributes

1. Choose the correct Organization group of the user based on the hierarchy of users stored in the LDAP server .

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

\* 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

## Enable Administrative Access for LDAP Users

Complete these steps in order to enable password-based authentication.

1. Navigate to **ISE > Administration > System > Admin Access > Authentication**.
2. Under the **Authentication Method** tab, select the **Password-Based** option.
3. Select **LDAP** from the **Identity Source** drop-down menu.
4. Click **Save Changes**.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb trail is Administration > System > Admin Access > Authentication Method. The left sidebar contains a menu with Authentication, Authorization, Administrators, and Settings. The main content area has tabs for Authentication Method (selected), Password Policy, Account Disable Policy, and Lock/Suspend Settings. Under Authentication Method, the Authentication Type is set to Password Based. Below this, the Identity Source is set to LDAP:LDAP\_Server. There are Save and Reset buttons at the bottom right.

## Map the Admin Group to LDAP Group

Configure the Admin Group on the ISE and map it to the AD group. This allows the configured user to get access based on the authorization policies based on the configured RBAC permissions for the administrator based on group membership.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb trail is Administration > System > Admin Access > Admin Groups. The left sidebar contains a menu with Authentication, Authorization, Administrators, and Settings. The main content area has a breadcrumb trail Admin Groups > LDAP\_User\_Group. The Admin Group configuration page shows the Name set to LDAP\_User\_Group. The Type is set to External. The External Identity Source is set to LDAP\_Server. Under External Groups, there is a list of groups with one group selected: CN=employee,CN=Users,DC=a. Below this is a Member Users section with a table header: Status, Email, Username, First Name, Last Name. The table is currently empty with the message 'No data available'.

## Set Permissions for Menu Access

1. Navigate to **ISE > Administration > System > Authorization > Permissions > Menu access**
2. Define the menu access for the admin user to access the ISE GUI. We can configure the sub-entities to be shown or hidden on the GUI for custom access for a user to perform only a set of operations if required.

### 3. Click on the **Save**.

The screenshot shows the Cisco ISE Administration interface for the 'System' section. The left sidebar contains navigation options: Authentication, Authorization, Permissions, Menu Access (selected), 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, the 'Menu Access Privileges' section displays a tree view of the 'ISE Navigation Structure' with the following items: Operations, Policy, Administration, Work Centers, Wizard, Settings, Home, and Context Visibility. To the right of the tree, there are radio buttons for 'Show' (selected) and 'Hide'.

### Set Permissions for Data Access

1. Navigate to **ISE > Administration > System > Authorization > Permissions > Data access**
2. Define the Data access for the admin user to have full access or read-only access to the identity groups on the ISE GUI.
3. Click on **Save**.

The screenshot shows the Cisco ISE Administration interface for the 'System' section. The left sidebar contains navigation options: Authentication, Authorization, Permissions, Menu Access, Data Access (selected), RBAC Policy, Administrators, and Settings. The main content area is titled 'Edit Data Access Permission' and shows the configuration for 'LDAP\_Data\_Access'. The 'Name' field is filled with 'LDAP\_Data\_Access' and the 'Description' field is empty. Below this, the 'Data Access Privileges' section displays a tree view of the 'Data Access Privileges' with the following items: Admin Groups, User Identity Groups, Endpoint Identity Groups, and Network Device Groups. To the right of the tree, there are radio buttons for 'Full Access' (selected), 'Read Only Access', and 'No Access'.

### Set RBAC Permissions for the Admin Group

1. Navigate to **ISE > Administration > System > Admin Access > Authorization > Policy**.

- From the **Actions** drop-down menu on the right, select **Insert New Policy Below** in order to add a new policy.
- Create a new rule called LDAP\_RBAC\_policy and map it with the Admin Group defined in the Enable Administrative Access for AD section, and assign it permissions for menu access and data access.
- Click **Save Changes**, and confirmation of the changes saved are displayed in the lower-right corner of the GUI.

Cisco ISE Administration - System

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
<input checked="" type="checkbox"/> Customization Admin Policy	If Customization Admin +	then Customization Admin Menu ... + Actions ▾
<input checked="" type="checkbox"/> Elevated System Admin Poli	If Elevated System Admin +	then System Admin Menu Access... + Actions ▾
<input checked="" type="checkbox"/> ERS Admin Policy	If ERS Admin +	then Super Admin Data Access + Actions ▾
<input checked="" type="checkbox"/> ERS Operator Policy	If ERS Operator +	then Super Admin Data Access + Actions ▾
<input checked="" type="checkbox"/> ERS Trustsec Policy	If ERS Trustsec +	then Super Admin Data Access + Actions ▾
<input checked="" type="checkbox"/> Helpdesk Admin Policy	If Helpdesk Admin +	then Helpdesk Admin Menu Access + Actions ▾
<input checked="" type="checkbox"/> Identity Admin Policy	If Identity Admin +	then Identity Admin Menu Access... + Actions ▾
<input checked="" type="checkbox"/> LDAP_RBAC_Rule	If LDAP_User_Group +	then LDAP_Menu_Access and L... X Actions ▾
<input checked="" type="checkbox"/> MnT Admin Policy	If MnT Admin +	then LDAP_Menu_Access ▾ +
<input checked="" type="checkbox"/> Network Device Policy	If Network Device Admin +	then LDAP_Data_Access ▾ +
<input checked="" type="checkbox"/> Policy Admin Policy	If Policy Admin +	then RBAC Admin Menu Access ... + Actions ▾
<input checked="" type="checkbox"/> RBAC Admin Policy	If RBAC Admin +	then RBAC Admin Menu Access ... + Actions ▾

## Verify

### Access ISE with AD Credentials

Complete these steps in order to access ISE with AD credentials:

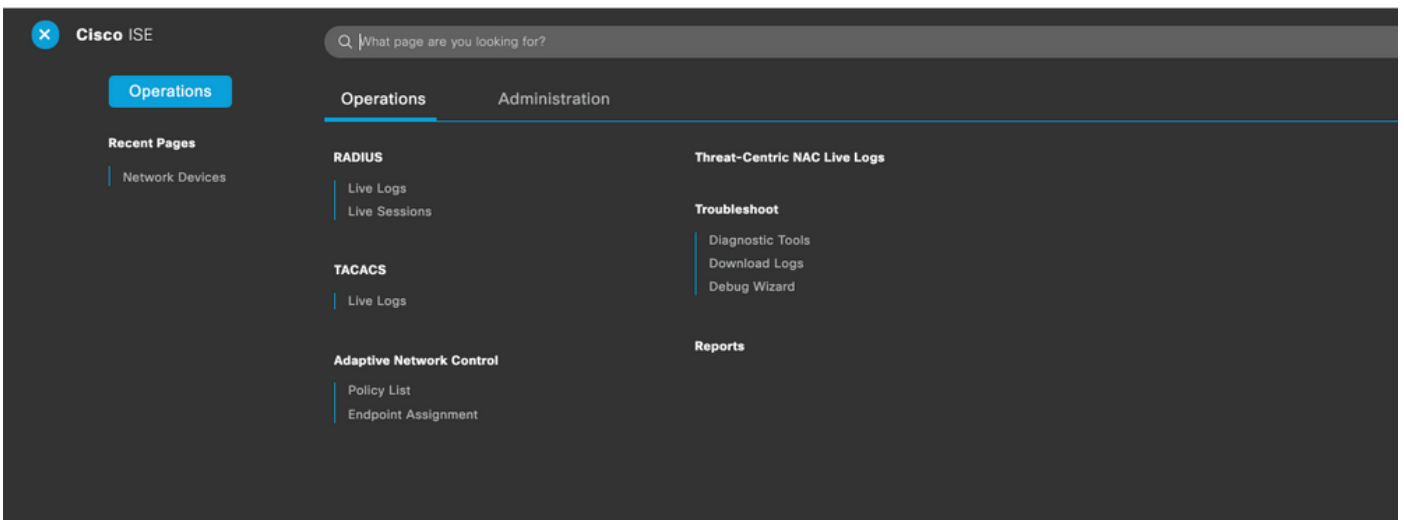
- Open ISE GUI to login with the LDAP user.
- Select LDAP\_Server from the **Identity Source** drop-down menu.
- Enter the username and password from the LDAP database, and log in.



Verify the login for the administrator logins in Audit Reports. Navigate to **ISE > Operations > Reports > Audit > Administrators Logins**.

Logged At	Administrator	IP Address	Server	Event	Event Details
Today	Administrator		Server		
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@anshsinh.local	10.65.37.52	ise30	Administrator logged off	User logged out
2020-10-10 10:56:47.668	admin2@anshsinh.local	10.65.37.52	ise30	Administrator authentication succeeded	Administrator authentication successful

In order to confirm that this configuration works properly, verify the authenticated username at the top-right corner of the ISE GUI. Define a custom based access which has limited access to the menu as shown here:



# Troubleshoot

## General information

In order to troubleshoot RBAC process, these ISE components have to be enabled in debug on the ISE Admin node :

RBAC - This will print the RBAC related message when we try to login ( ise-psc.log )

access-filter - This will print resource filter access (ise-psc.log )

runtime-AAA - This will print the logs for login and LDAP interaction messages (prtt-server.log )

## Packet Capture Analysis

The image shows a Wireshark packet capture analysis of LDAP traffic. A table at the top lists packets with columns for No., Time, Source, Destination, Protocol, Length, User-Name, and Off. Info. Three packets are highlighted in orange: packet 1043 (LDAP bind request), packet 1044 (LDAP search request), and packet 1045 (LDAP search response). Callout boxes provide context: 'Bind Request and response using LDAP for the administrator.' points to packets 1043 and 1044; 'Search request and response Entry for the username to the mapped LDAP group.' points to packets 1044 and 1045; 'Bind success for the username search' points to packet 1045. The packet details pane on the right shows the structure of the LDAP messages, including bindRequest, searchRequest, searchResEntry, and bindResponse.

No.	Time	Source	Destination	Protocol	Length	User-Name	Off. Info
579	2020-09-30 01:21:08.848523	10.106.32.184	10.127.197.188	LDAP	73		bindRequest(4)
1040	2020-09-30 01:21:13.346421	10.106.32.184	10.127.197.188	LDAP	140		bindRequest(1) "CN=Administrator,CN=Users,DC=anshsinh,DC=local" simple
1041	2020-09-30 01:21:13.348424	10.127.197.188	10.106.32.184	LDAP	88		bindResponse(1) success
1043	2020-09-30 01:21:13.348757	10.106.32.184	10.127.197.188	LDAP	191		searchRequest(2) "dc=anshsinh,dc=local" wholeSubtree
1044	2020-09-30 01:21:13.349581	10.127.197.188	10.106.32.184	LDAP	475		searchResEntry(2) "CN=admin2,CN=Users,DC=anshsinh,DC=local"   searchRes
1045	2020-09-30 01:21:13.351026	10.106.32.184	10.127.197.188	LDAP	127		bindRequest(1) "CN=admin2,CN=Users,DC=anshsinh,DC=local" simple
1049	2020-09-30 01:21:13.352089	10.127.197.188	10.106.32.184	LDAP	88		bindResponse(1) success
15320	2020-09-30 01:21:40.068100	10.106.32.184	10.127.197.188	LDAP	191		searchRequest(3) "dc=anshsinh,dc=local" wholeSubtree
15325	2020-09-30 01:21:40.069045	10.127.197.188	10.106.32.184	LDAP	475		searchResEntry(3) "CN=admin2,CN=Users,DC=anshsinh,DC=local"   searchRes
15330	2020-09-30 01:21:40.069756	10.106.32.184	10.127.197.188	LDAP	127		bindRequest(2) "CN=admin2,CN=Users,DC=anshsinh,DC=local" simple
15337	2020-09-30 01:21:40.071044	10.127.197.188	10.106.32.184	LDAP	88		bindResponse(2) success

## Log Analysis

### Verify the prtt-server.log

PAPAuthenticator,2020-10-10

```
08:54:00,621,DEBUG,0x7f852bee3700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u  
serauth286,user=admin2@anshsinh.local,validateEvent: Username is [admin2@anshsinh.local]  
bIsMachine is [0] isUtf8Valid is [1],PAPAuthenticator.cpp:86 IdentitySequence,2020-10-10
```

```
08:54:00,627,DEBUG,0x7f852c4e9700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u  
serauth286,user=admin2@anshsinh.local,***** Authen
```

```
IDStoreName:LDAP_Server,IdentitySequenceWorkflow.cpp:377 LDAPIDStore,2020-10-10
```

```
08:54:00,628,DEBUG,0x7f852c4e9700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u  
serauth286,user=admin2@anshsinh.local,Send event to LDAP_Server_924OqzxSbv_199_Primary  
server,LDAPIDStore.h:205 Server,2020-10-10
```

```
08:54:00,634,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u  
serauth286,user=admin2@anshsinh.local,LdapServer::onAcquireConnectionResponse: succeeded to  
acquire connection,LdapServer.cpp:724 Connection,2020-10-10
```

```
08:54:00,634,DEBUG,0x7f85293b8700,LdapConnectionContext::sendSearchRequest(id = 1221): base =  
dc=anshsinh,dc=local, filter =  
((&(objectclass=Person)(userPrincipalName=admin2@anshsinh.local)),LdapConnectionContext.cpp:516  
Server,2020-10-10
```

```
08:54:00,635,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u  
serauth286,user=admin2@anshsinh.local,LdapSubjectSearchAssistant::processAttributes: found  
CN=admin2,CN=Users,DC=anshsinh,DC=local entry matching admin2@anshsinh.local  
subject,LdapSubjectSearchAssistant.cpp:268 Server,2020-10-10
```

```
08:54:00,635,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u  
serauth286,user=admin2@anshsinh.local,LdapSubjectSearchAssistant::processGroupAttr: attr =  
memberOf, value = CN=employee,CN=Users,DC=anshsinh,DC=local,LdapSubjectSearchAssistant.cpp:389
```



```
Server, 2020-10-10
08:54:00, 636, DEBUG, 0x7f85293b8700, cntx=0002480105, sesn=ise30/389444264/3178, CPMSessionID=ise30:u
serauth286, user=admin2@anshsinh.local, LdapServer::onAcquireConnectionResponse: succeeded to
acquire connection, LdapServer.cpp:724 Server, 2020-10-10
08:54:00, 636, DEBUG, 0x7f85293b8700, cntx=0002480105, sesn=ise30/389444264/3178, CPMSessionID=ise30:u
serauth286, user=admin2@anshsinh.local, LdapServer::authenticate: user = admin2@anshsinh.local, dn
= CN=admin2, CN=Users, DC=anshsinh, DC=local, LdapServer.cpp:352 Connection, 2020-10-10
08:54:00, 636, DEBUG, 0x7f85293b8700, LdapConnectionContext::sendBindRequest(id = 1223): dn =
CN=admin2, CN=Users, DC=anshsinh, DC=local, LdapConnectionContext.cpp:490 Server, 2020-10-10
08:54:00, 640, DEBUG, 0x7f85293b8700, cntx=0002480105, sesn=ise30/389444264/3178, CPMSessionID=ise30:u
serauth286, user=admin2@anshsinh.local, LdapServer::handleAuthenticateSuccess: authentication of
admin2@anshsinh.local user succeeded, LdapServer.cpp:474 LDAPIDStore, 2020-10-10
08:54:00, 641, DEBUG, 0x7f852c6eb700, cntx=0002480105, sesn=ise30/389444264/3178, CPMSessionID=ise30:u
serauth286, user=admin2@anshsinh.local, LDAPIDStore::onResponse:
LdapOperationStatus=AuthenticationSucceeded -> AuthenticationResult=Passed, LDAPIDStore.cpp:336
```

## Verify the ise-psc.log

From these logs, you can verify the RBAC policy used for the admin2 user when tries to access Network Device resource -

```
2020-10-10 08:54:24, 474 DEBUG [admin-http-pool51][] com.cisco.cpm.rbacfilter.AccessUtil -
:admin2@anshsinh.local::- For admin2@anshsinh.local on /NetworkDevicesLPInputAction.do --
ACCESS ALLOWED BY MATCHING administration_networkresources_devices 2020-10-10 08:54:24, 524 INFO
[admin-http-pool51][] cpm.admin.ac.actions.NetworkDevicesLPInputAction -
:admin2@anshsinh.local::- In NetworkDevicesLPInputAction container method 2020-10-10
08:54:24, 524 DEBUG [admin-http-pool51][] cisco.ise.rbac.authorization.RBACAuthorization -
:admin2@anshsinh.local::- :::::::::::Inside RBACAuthorization.getDataEntityDecision:::::
userName admin2@anshsinh.local dataType RBAC_NETWORK_DEVICE_GROUP permission ALL 2020-10-10
08:54:24, 526 DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImpl -
:admin2@anshsinh.local::- In DataPermissionEvaluator:hasPermission 2020-10-10 08:54:24, 526
DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImpl -
:admin2@anshsinh.local::- Data access being evaluated:LDAP_Data_Access 2020-10-10 08:54:24, 528
DEBUG [admin-http-pool51][] cisco.ise.rbac.authorization.RBACAuthorization -
:admin2@anshsinh.local::- :::::::::::Inside RBACAuthorization.getDataEntityDecision:::::
permission retrieved false 2020-10-10 08:54:24, 528 INFO [admin-http-pool51][]
cpm.admin.ac.actions.NetworkDevicesLPInputAction -:admin2@anshsinh.local::- Finished with rbac
execution 2020-10-10 08:54:24, 534 INFO [admin-http-pool51][]
cisco.cpm.admin.license.TrustSecLicensingUIFilter -:admin2@anshsinh.local::- Should TrustSec be
visible :true 2020-10-10 08:54:24, 593 DEBUG [admin-http-pool51][]
cisco.ise.rbac.authorization.RBACAuthorization -:admin2@anshsinh.local::- :::::::::::Inside
RBACAuthorization.getPermittedNDG::::: userName admin2@anshsinh.local 2020-10-10 08:54:24, 595
DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImpl -
:admin2@anshsinh.local::- In DataPermissionEvaluator:getPermittedNDGMap 2020-10-10 08:54:24, 597
DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImpl -
:admin2@anshsinh.local::- processing data Access :LDAP_Data_Access 2020-10-10 08:54:24, 604 INFO
[admin-http-pool51][] cisco.cpm.admin.license.TrustSecLicensingUIFilter -
:admin2@anshsinh.local::- Should TrustSec be visible :true
```