ISE Role Based Access Control with LDAP

Contents

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

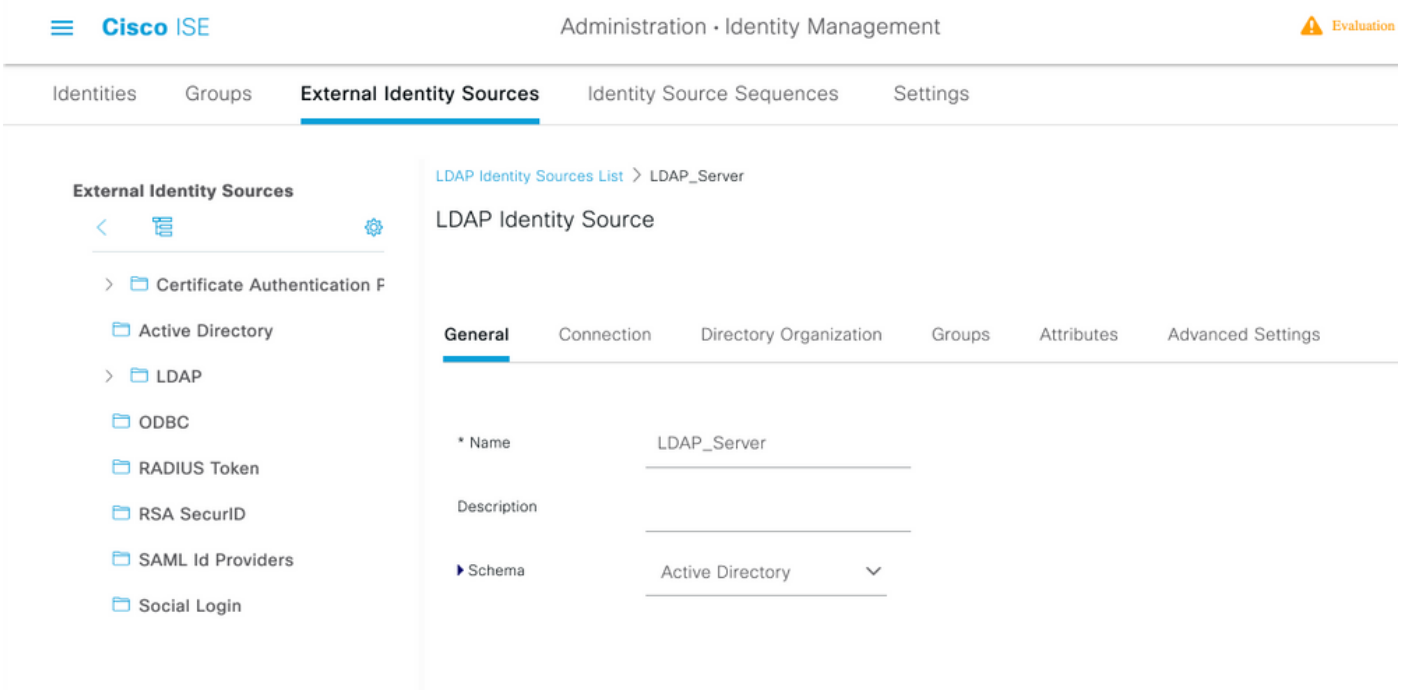
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

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.



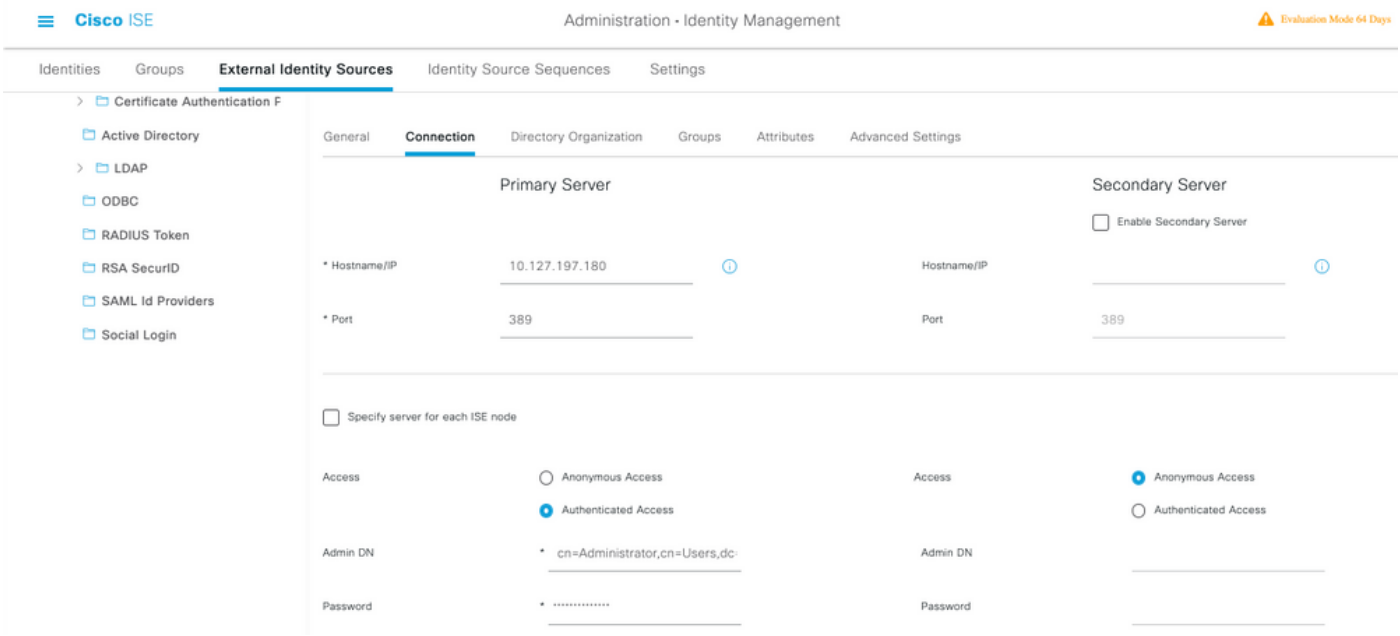
Configure Connection type and LDAP configuration

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) .

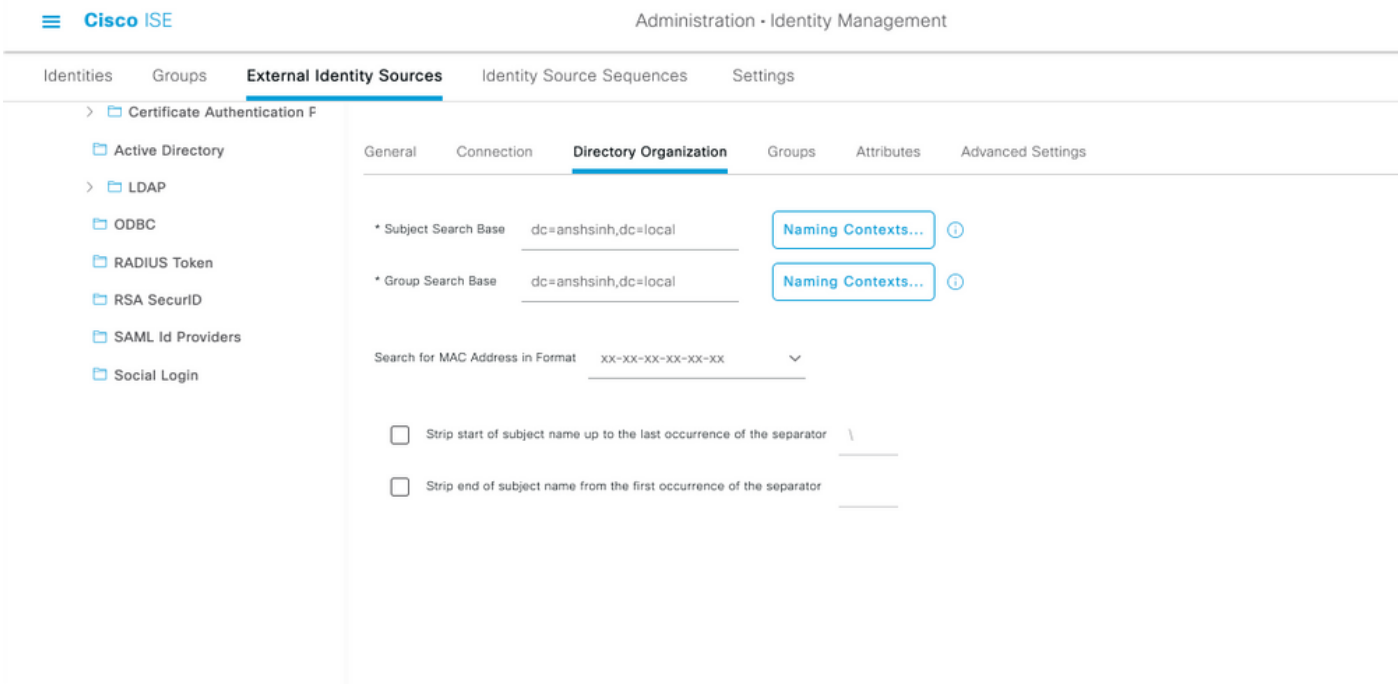
3. Enter the path for the Admin distinguished name (DN) with the admin password for the LDAP server .

4.Click on Test Bind Server to test the reachability of LDAP server from ISE .



Configure the Directory organization, Groups, and Attributes

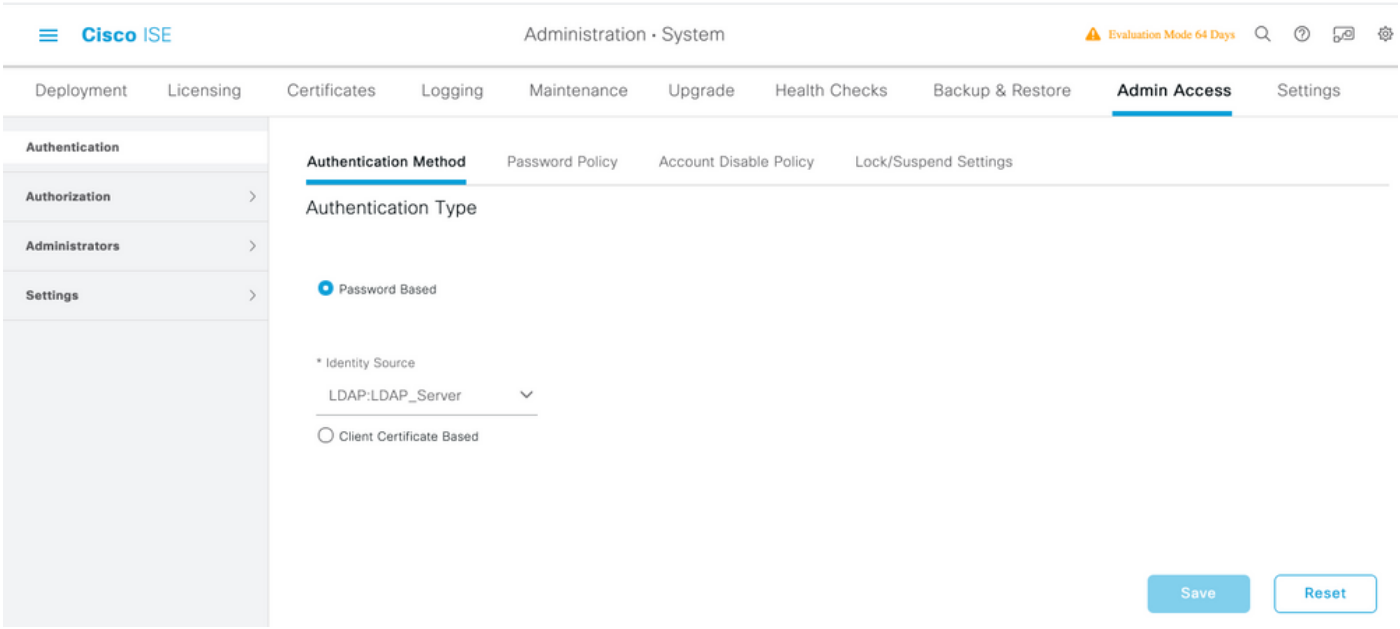
1. Choose the correct Organization group of the user based on the hierarchy of users stored in the LDAP server .



Enable Administrative Access for LDAP Users

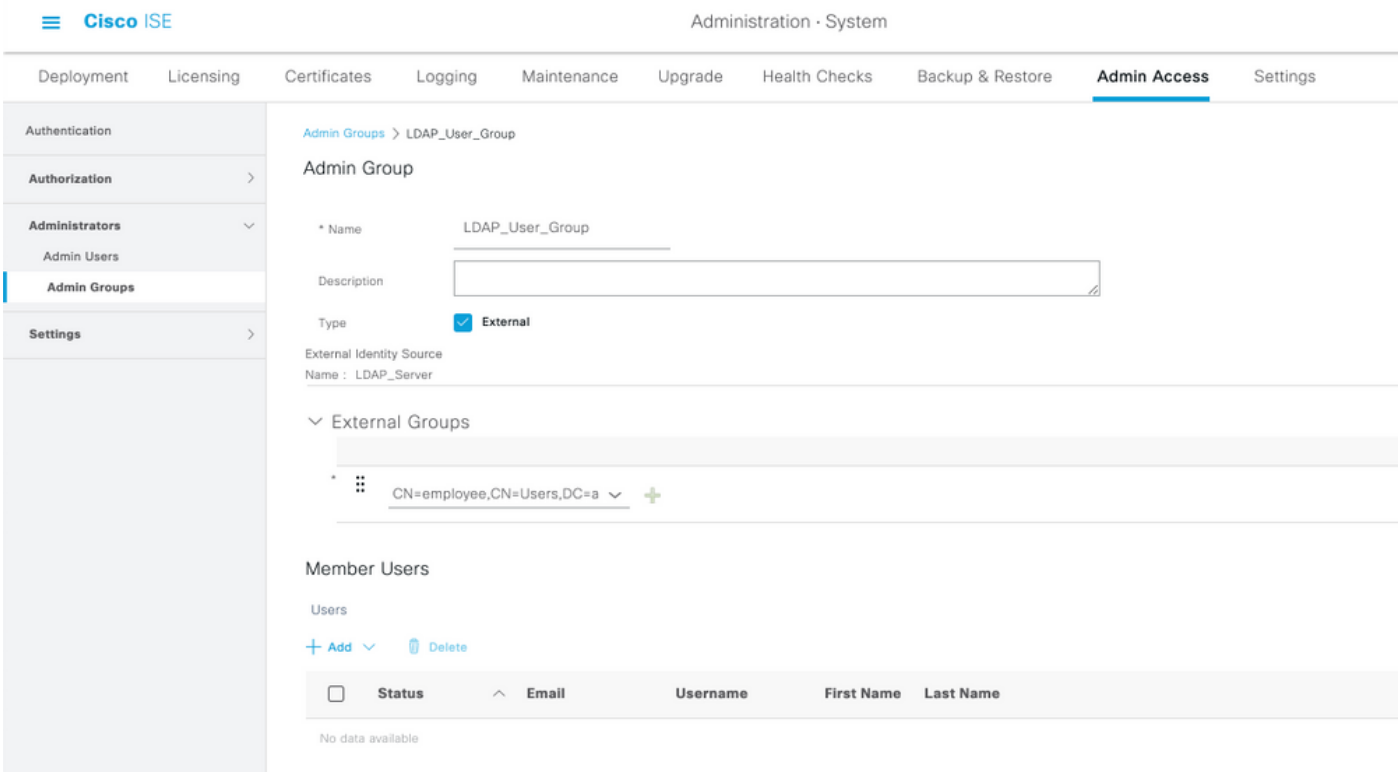
Complete these steps in order to enable password-based authentication.

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**.



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.

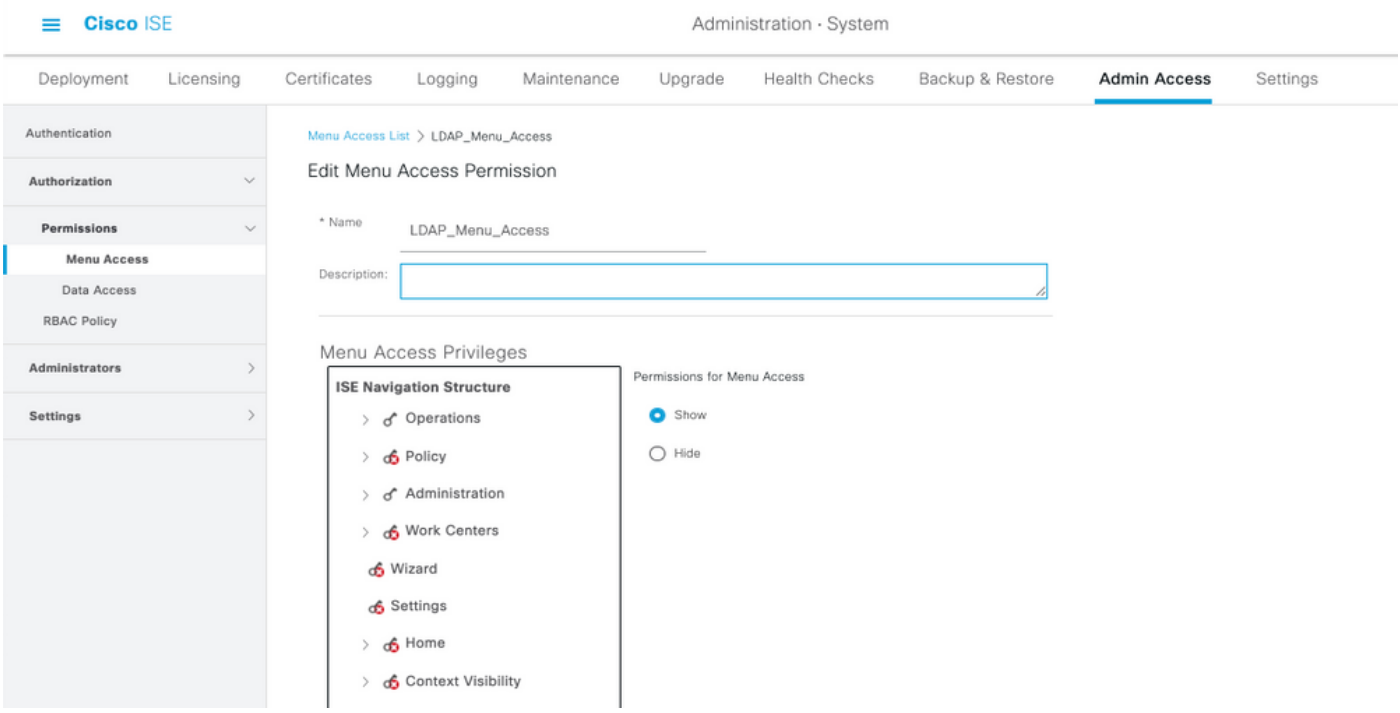


Set Permissions for Menu Access

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**.

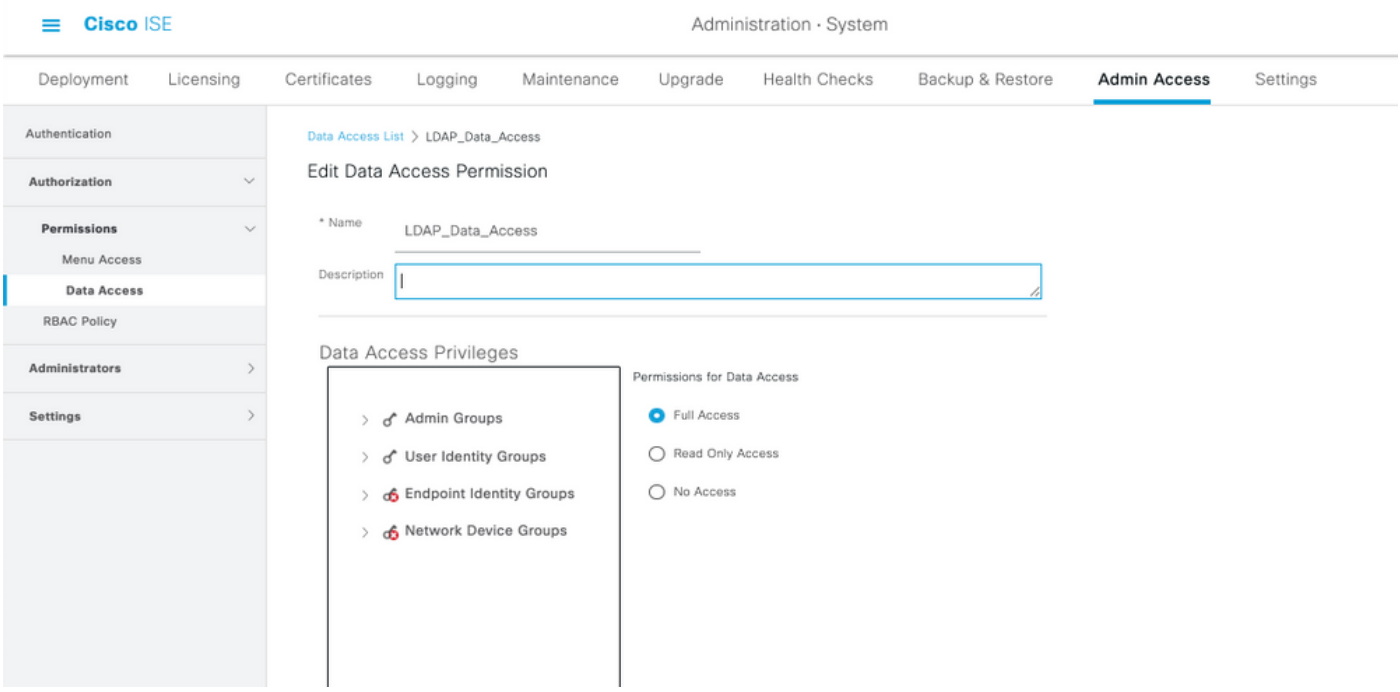


Set Permissions for Data Access

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.

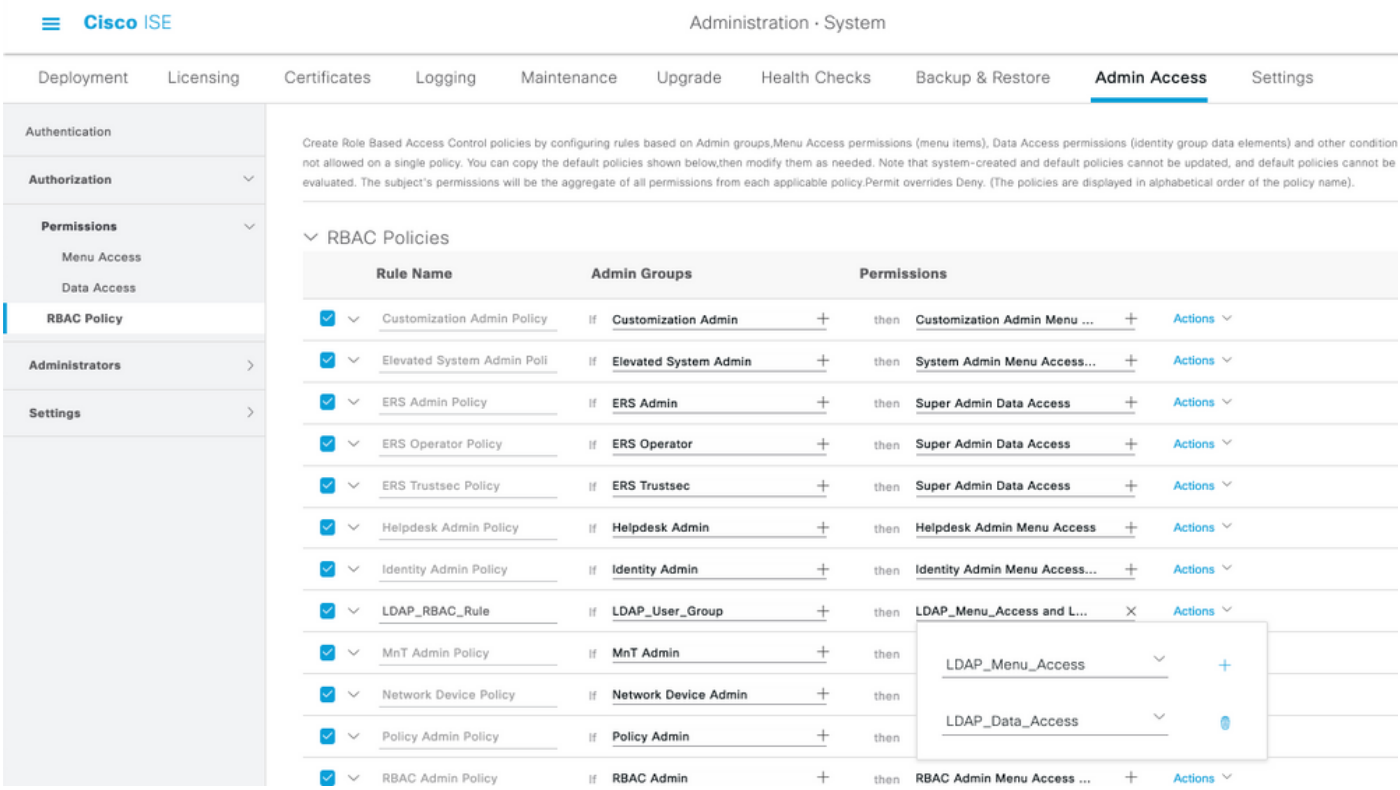
3. Click on **Save**.



Set RBAC Permissions for the Admin Group

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

2. From the **Actions** drop-down menu on the right, select **Insert New Policy Below** in order to add a new policy.
3. 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.
4. Click **Save Changes**, and confirmation of the changes saved are displayed in the lower-right corner of the GUI.

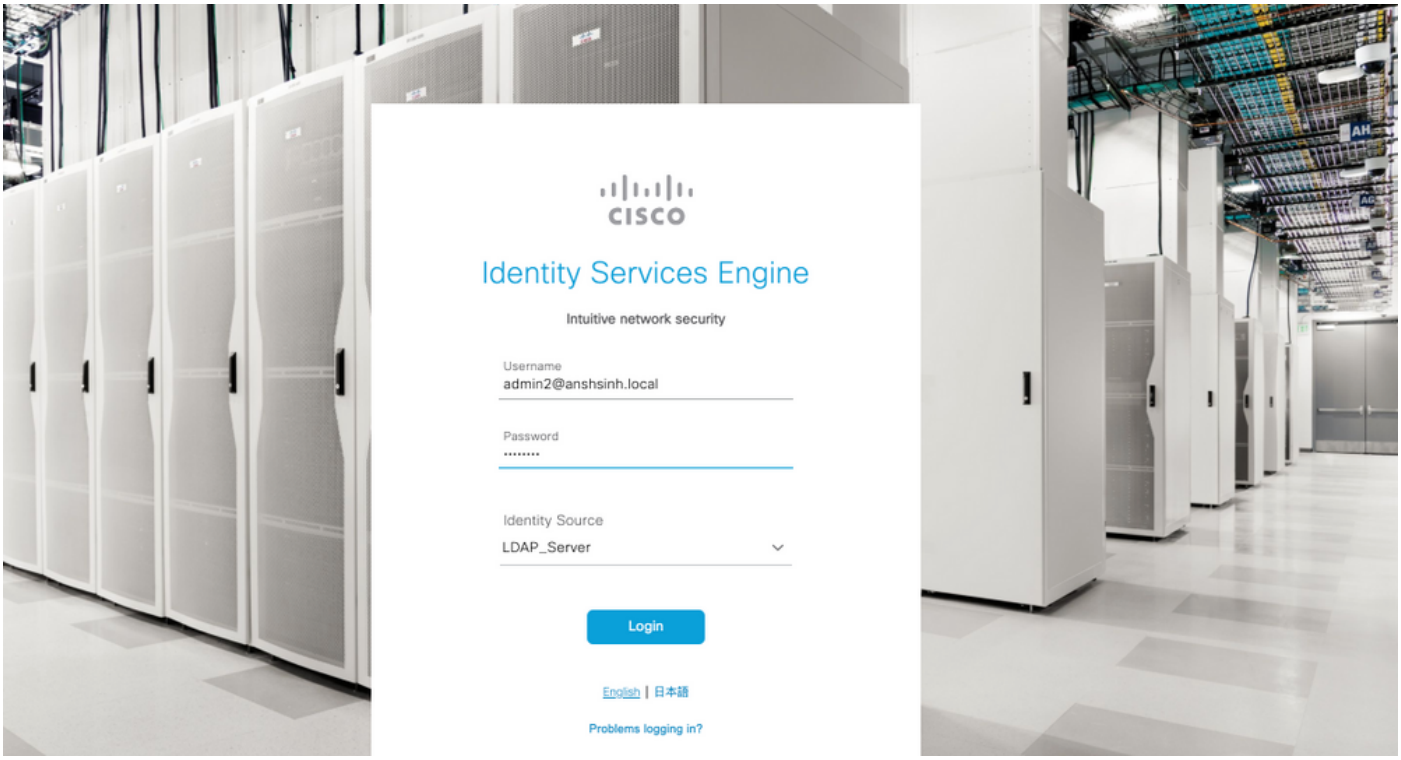


Verify

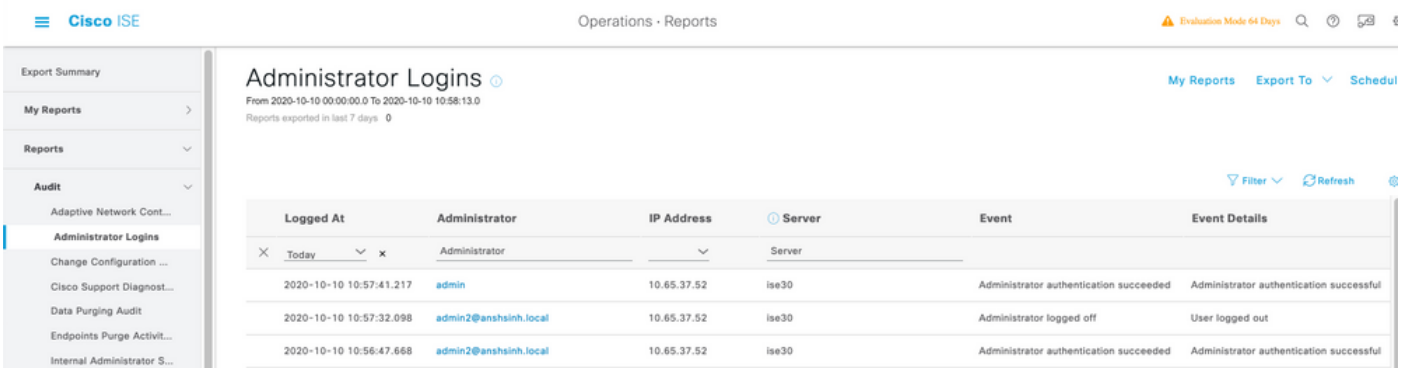
Access ISE with AD Credentials

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

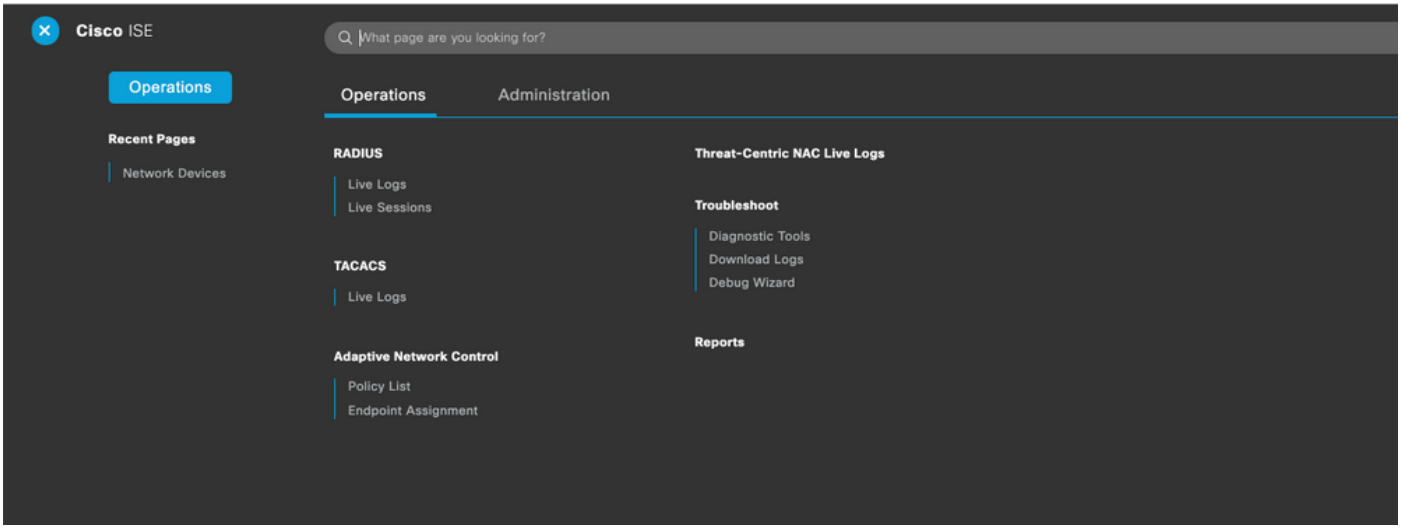
1. Open ISE GUI to login with the LDAP user.
2. Select LDAP_Server from the **Identity Source** drop-down menu.
3. Enter the username and password from the LDAP database, and log in.



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



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

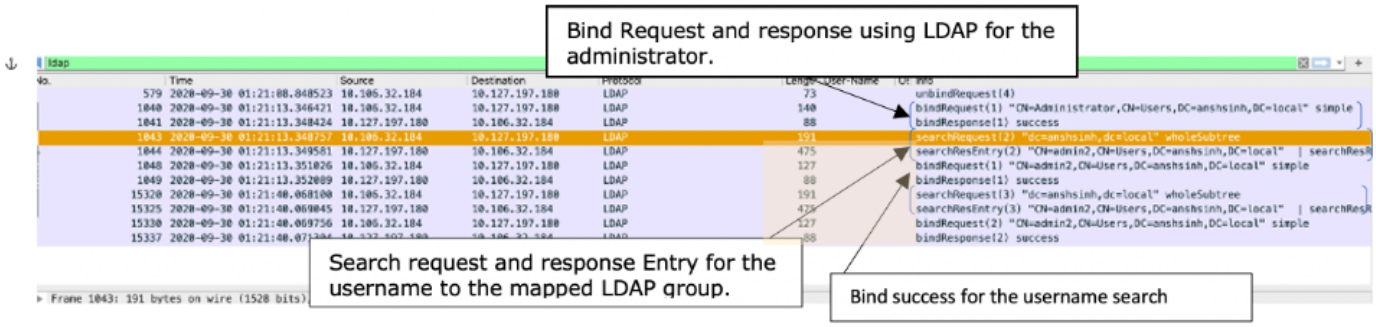
In order to troubleshoot RBAC process, these ISE components have to be enabled in debug on the ISE Admin node :

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

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

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

Packet Capture Analysis



Log Analysis

Verify the prrt-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
```