Configure ISE Role Based Access Control with Lightweight Directory Access Protocol

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 theprrt-server.log
  - Verify theise-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

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

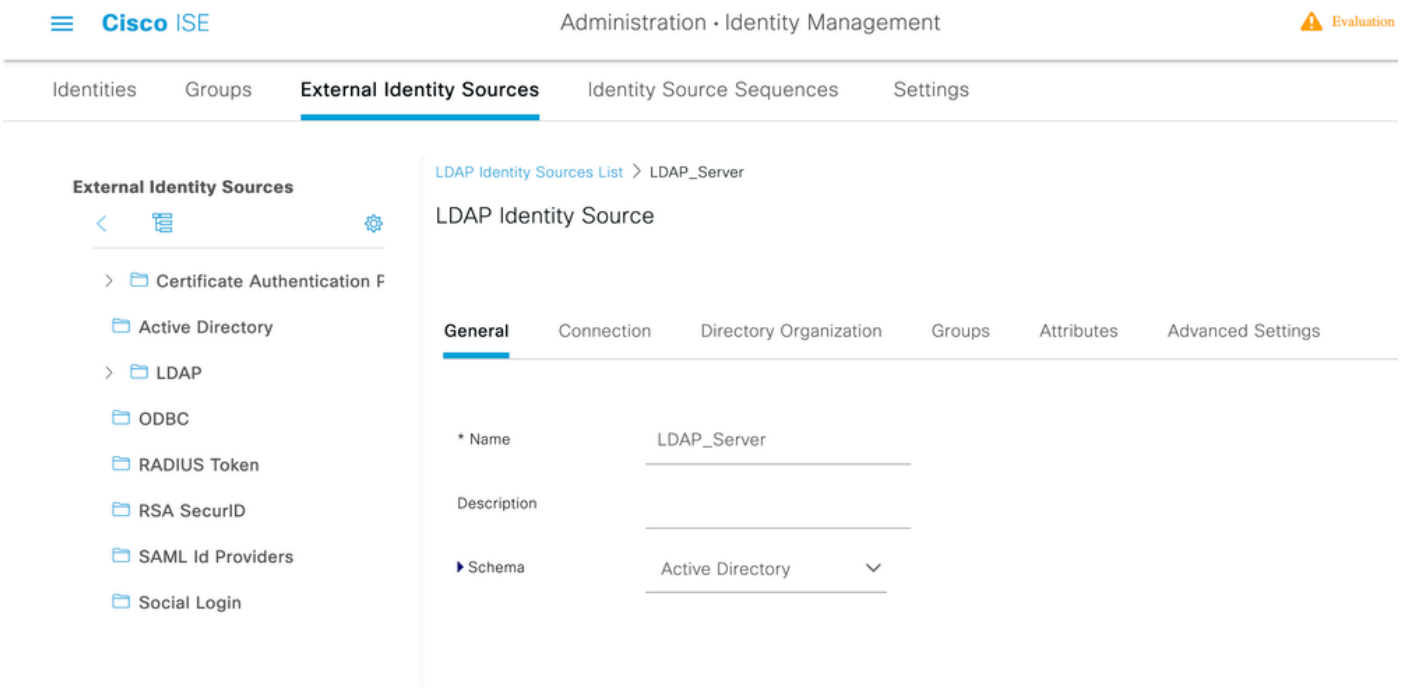
sure that you understand the potential impact of any command.

Configurations

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



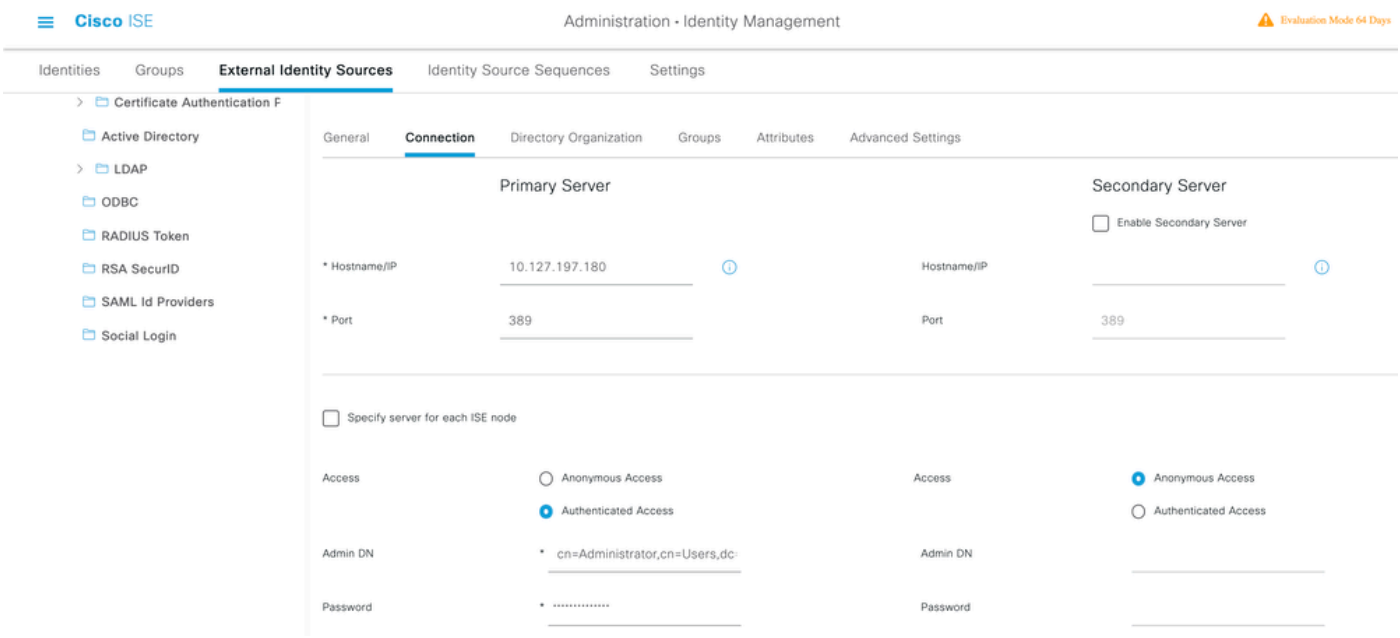
Configure Connection type and LDAP configuration

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) .

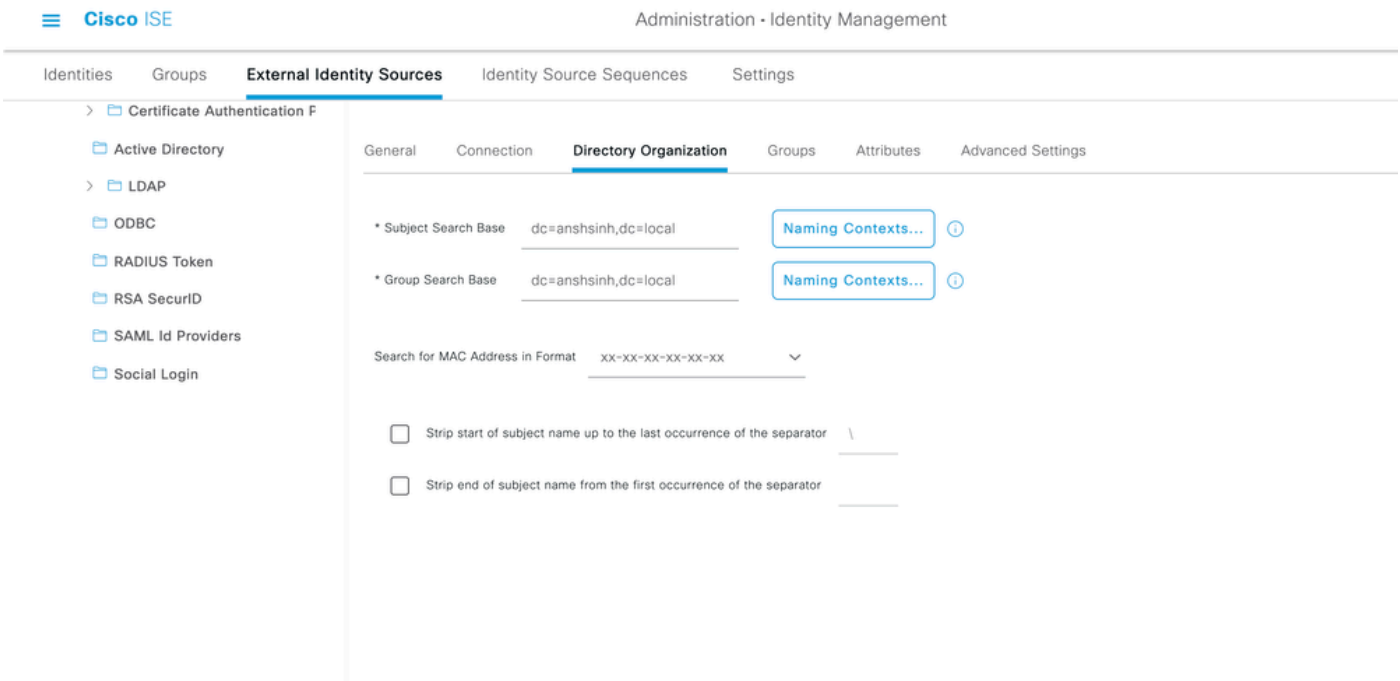
3. Enter the path for the Admin distinguished name (DN) with the admin password for the LDAP server .

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



Configure the Directory organization, Groups, and Attributes

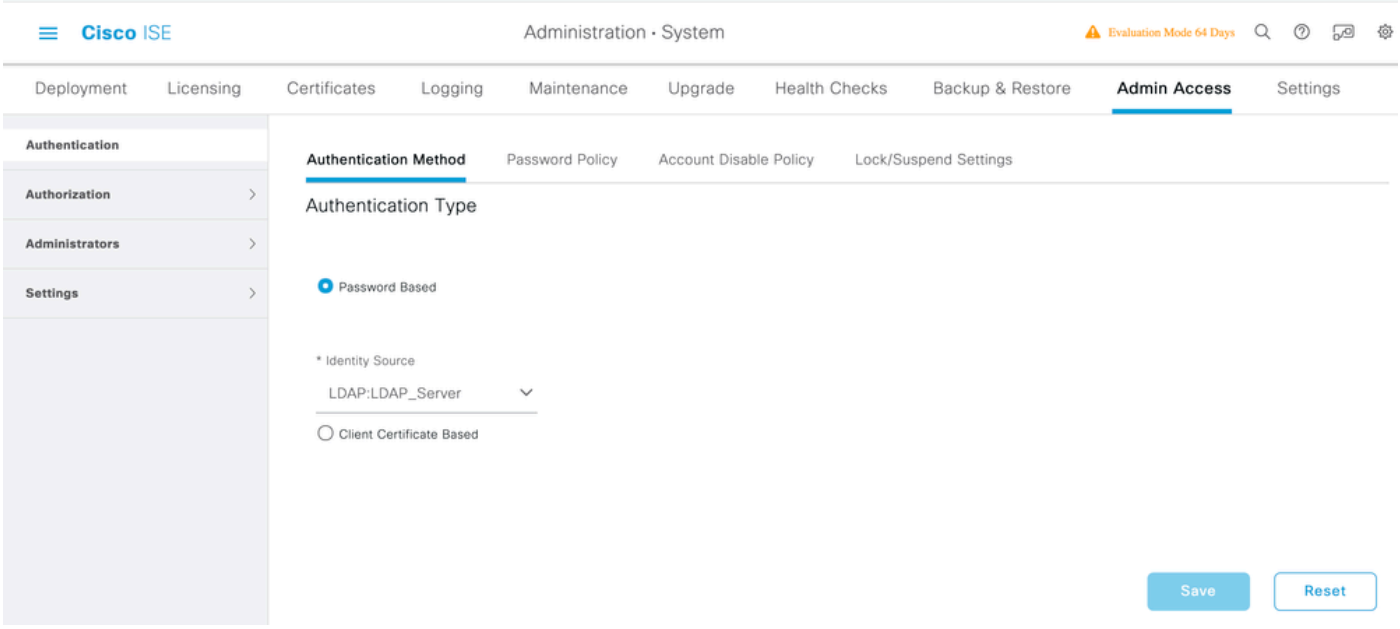
1. Choose the correct Organization group of the user based on the hierarchy of users stored in the LDAP server .



Enable Administrative Access for LDAP Users

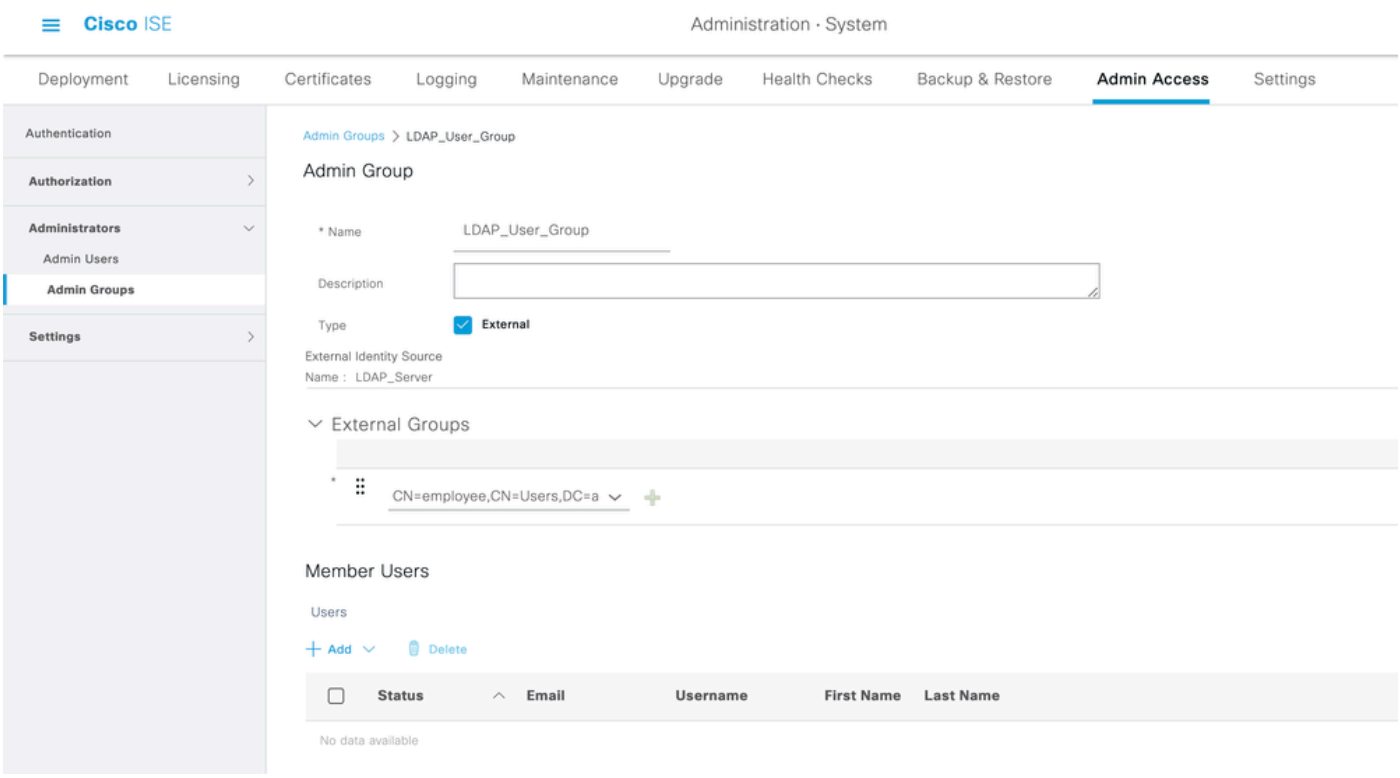
Complete these steps in order to enable password-based authentication.

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.

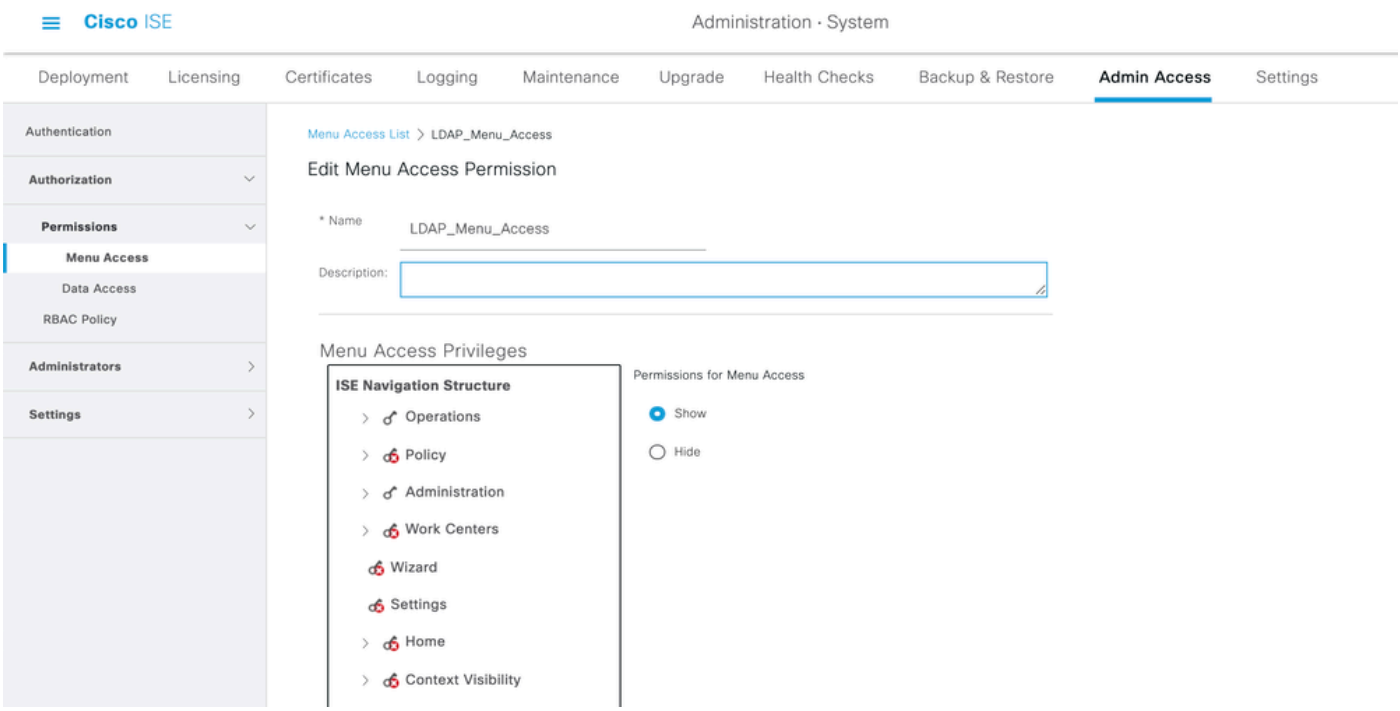


Set Permissions for Menu Access

1. Navigate to **ISE > Administration > System > Authorization > Permissions > Menu access**

2. Define the menu access for the admin user to access the ISE GUI. You 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**.

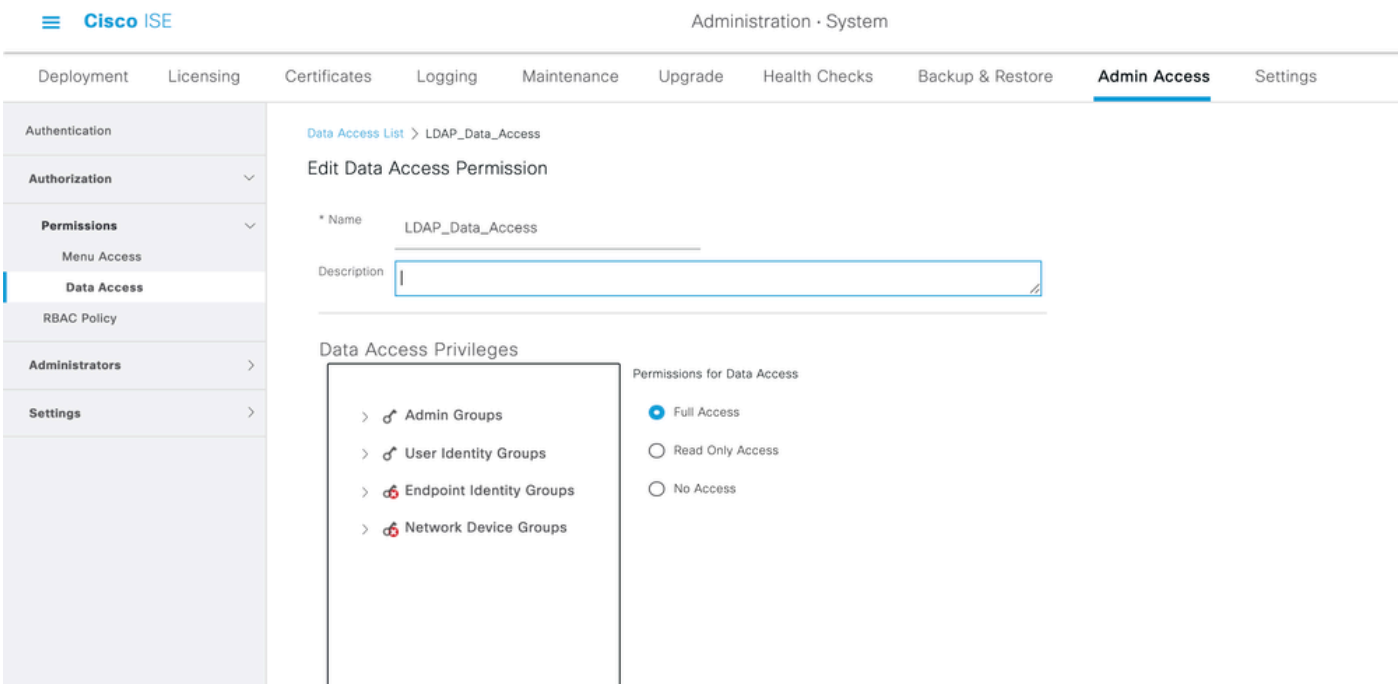


Set Permissions for Data Access

1. Navigate to **ISE > Administration > System > Authorization > Permissions > Data access**.

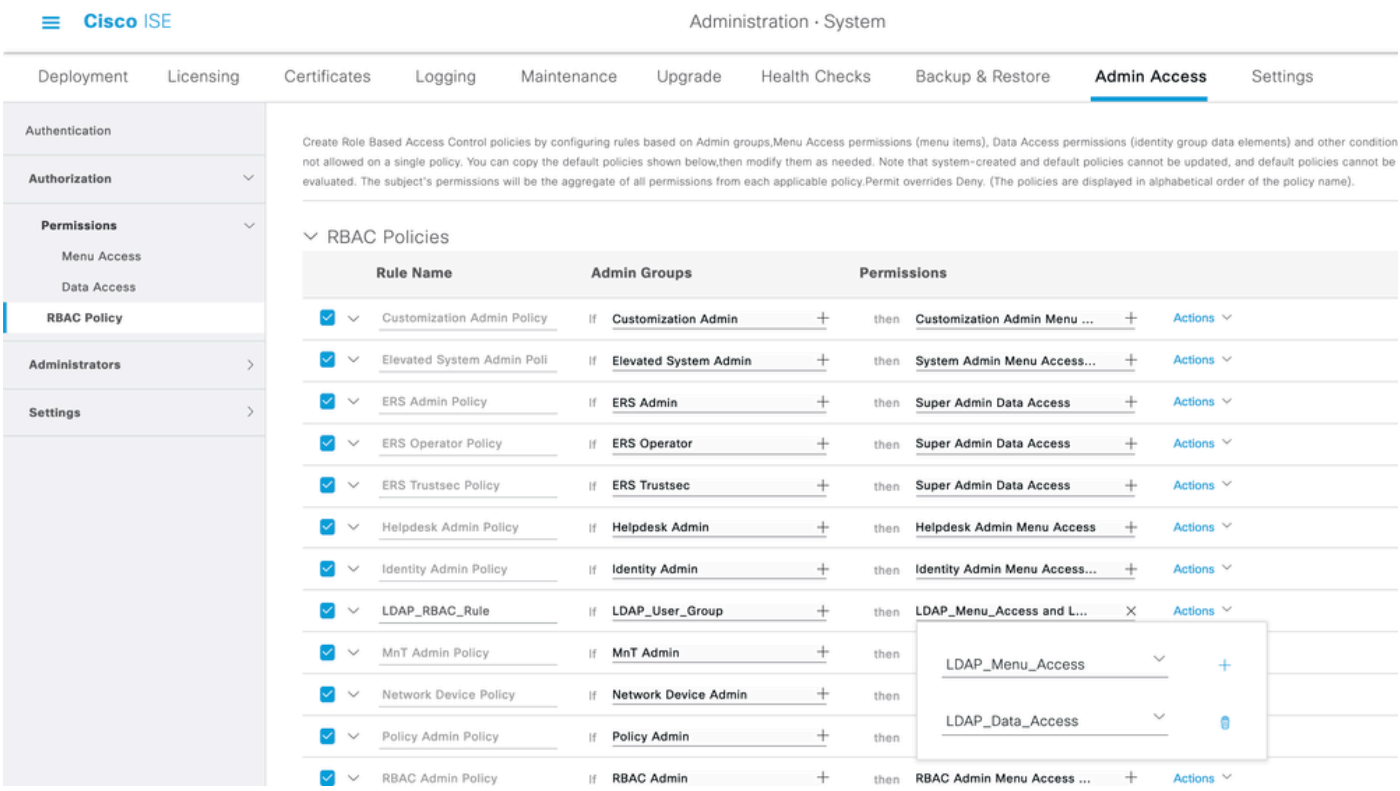
2. Define the Data access for the admin user to have full access or read-only access to the identity groups on the ISE GUI.

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** to add a new policy.
3. Create a new rule called LDAP_RBAC_policy 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.



Note: The super admin user cannot modify the default system-generated RBAC policies and permissions. To do this, you must create new RBAC policies with the necessary permissions based on your needs, and map these policies to an admin group.

Note: Only an admin user from the default Super Admin Group can modify or delete other admin users. Even an externally mapped user who is part of an Admin Group cloned with the Menu and Data Access privileges of the Super Admin Group cannot modify or delete an admin user.

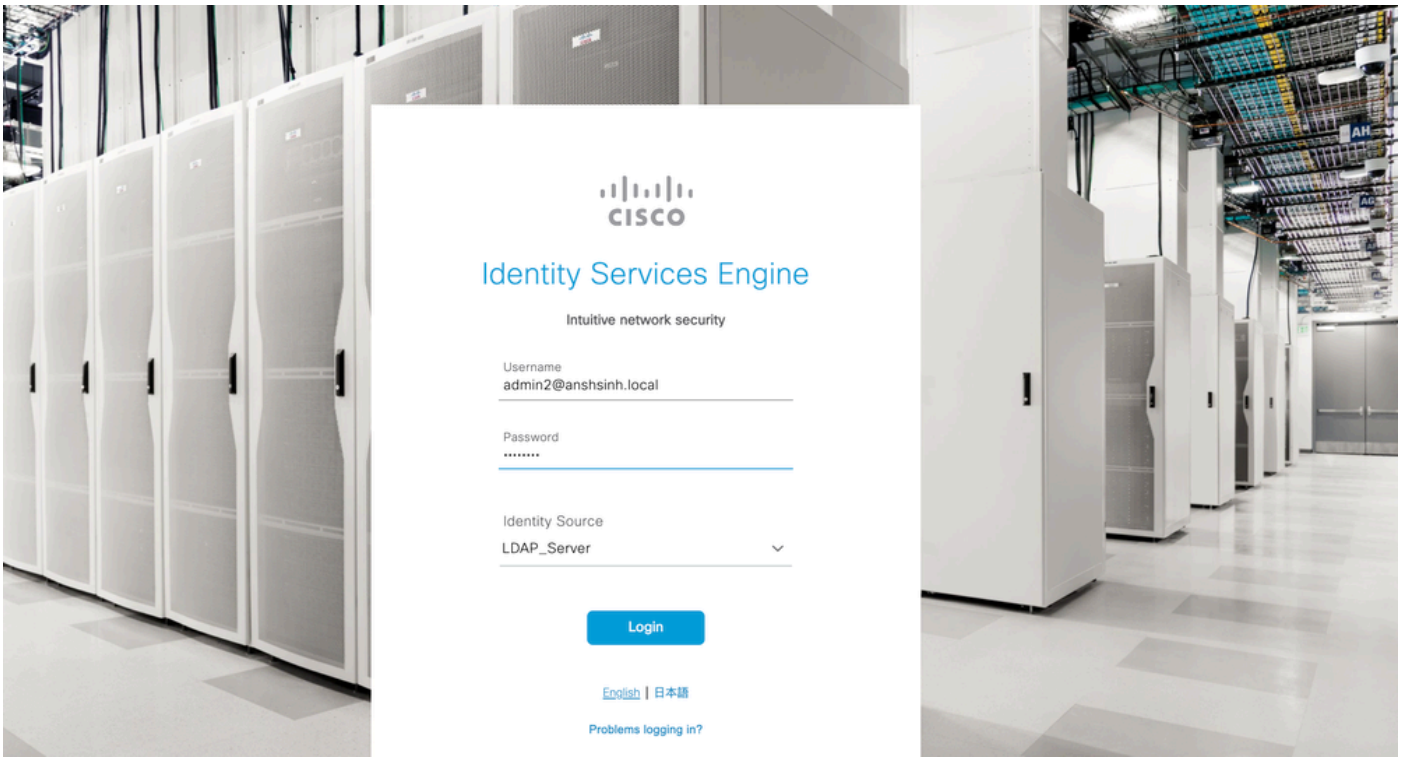
Verify

Use this section in order to confirm that your configuration works properly.

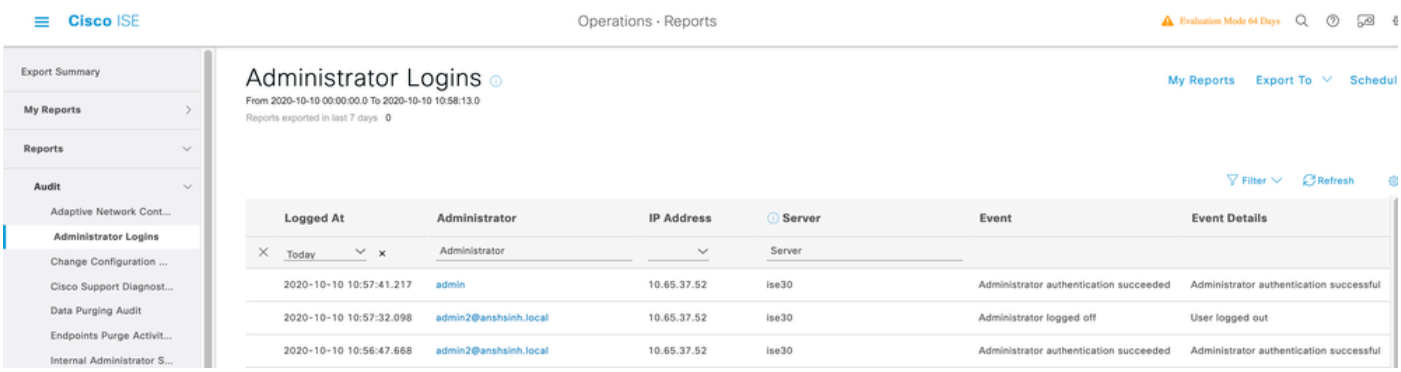
Access ISE with AD Credentials

Complete these steps to access ISE with AD credentials:

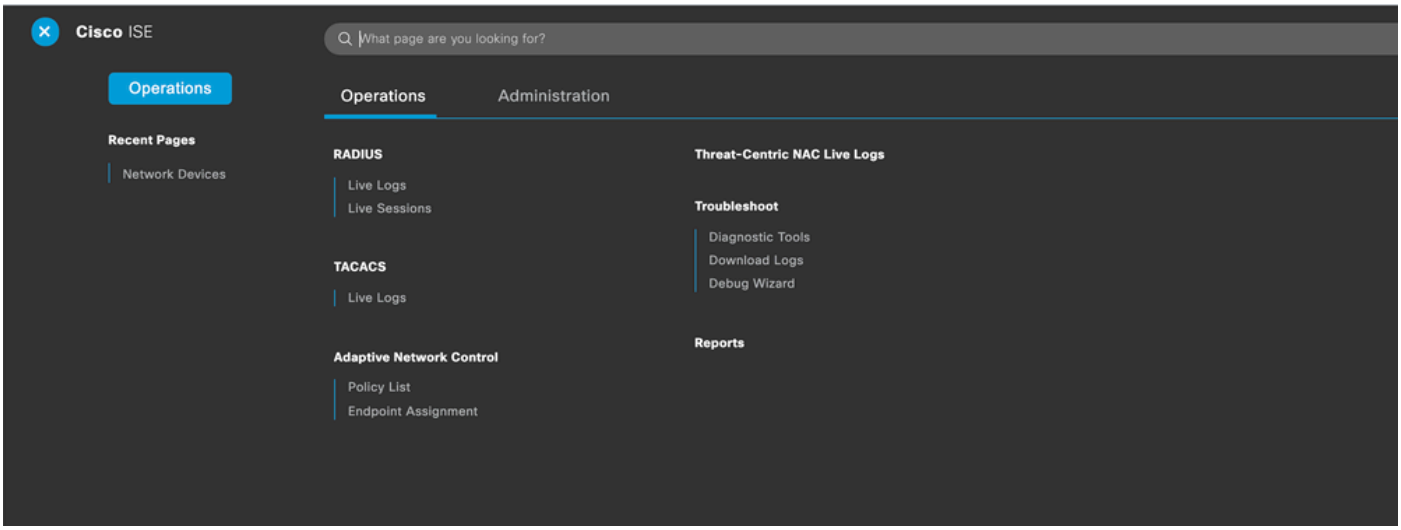
1. Open ISE GUI to log in with the LDAP user.
2. Select LDAP_Server from the **Identity Source** drop-down menu.
3. Enter the UPN and password from the LDAP database, and log in.



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



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

This section provides information you can use in order to troubleshoot your configuration.

General Information

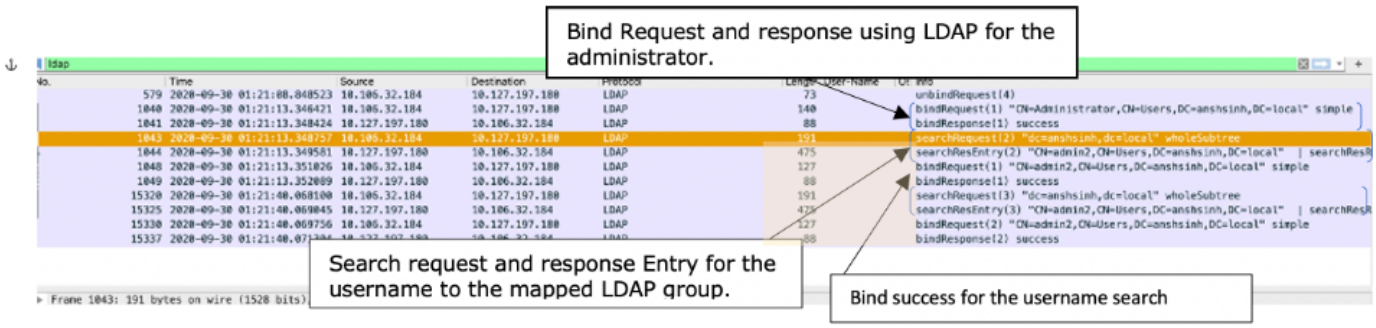
To troubleshoot the RBAC process, these ISE components have to be enabled in debugging on the ISE Admin node :

RBAC - This prints the RBAC-related message when we try to log in (ise-psc.log)

access-filter - This prints resource filter access (ise-psc.log)

runtime-AAA - This prints 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

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,CPMSessio

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,CPMSessio
```

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

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

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

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,CPMSessio



LDAPIDStore,2020-10-10 08:54:00,641,DEBUG,0x7f852c6eb700,cntx=0002480105,sesn=ise30/389444264/3178,CPMS
```

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@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
```