Understand Admin Access and RBAC Policies on ISE

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Configure](#)
[Authentication Settings](#)
[Configure Admin Groups](#)
[Configure Admin Users](#)
[Configure Permissions](#)
[Configure RBAC policies](#)
[Configure Settings for Admin Access](#)
[Configure Admin Portal Access with AD Credentials](#)
[Join ISE to AD](#)
[Select Directory Groups](#)
[Enable Administrative Access for AD](#)
[Configure the ISE Admin Group to AD Group Mapping](#)
[Set RBAC Permissions for the Admin Group](#)
[Access ISE with AD Credentials and Verify](#)
[Configure Admin Portal Access with LDAP](#)
[Join ISE to LDAP](#)
[Enable Administrative Access for LDAP Users](#)
[Map the ISE Admin Group to LDAP Group](#)
[Set RBAC Permissions for the Admin Group](#)
[Access ISE with LDAP Credentials and Verify](#)

Introduction

This document describes the features of ISE to manage Administrative Access on Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recommends that you have the knowledge of these topics:

- ISE
- Active Directory

- Lightweight Directory Access Protocol (LDAP)

Components Used

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

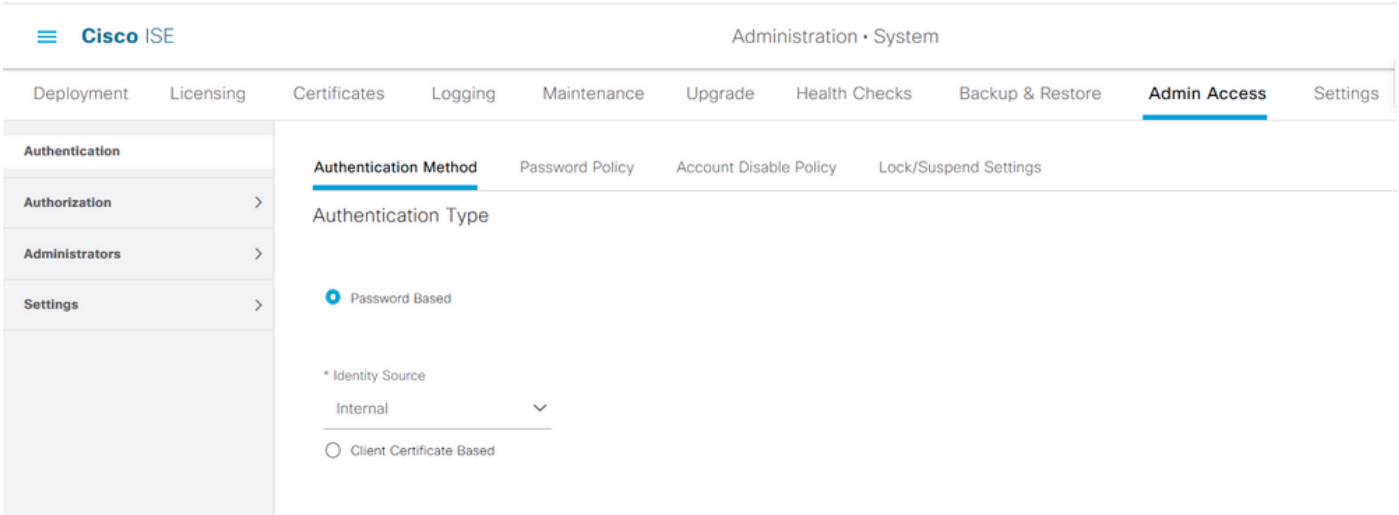
- Identity Services Engine 3.0
- Windows Server 2016

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, ensure that you understand the potential impact of any command.

Configure

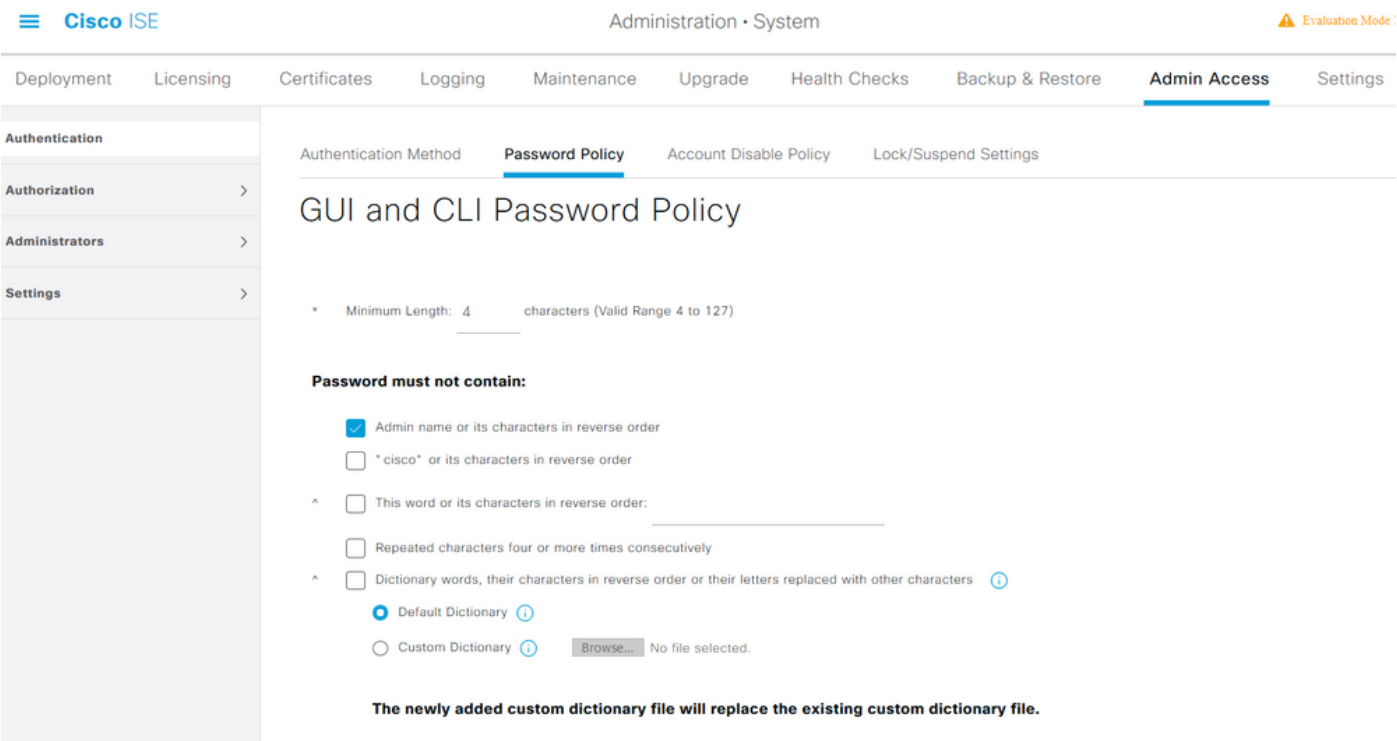
Authentication Settings

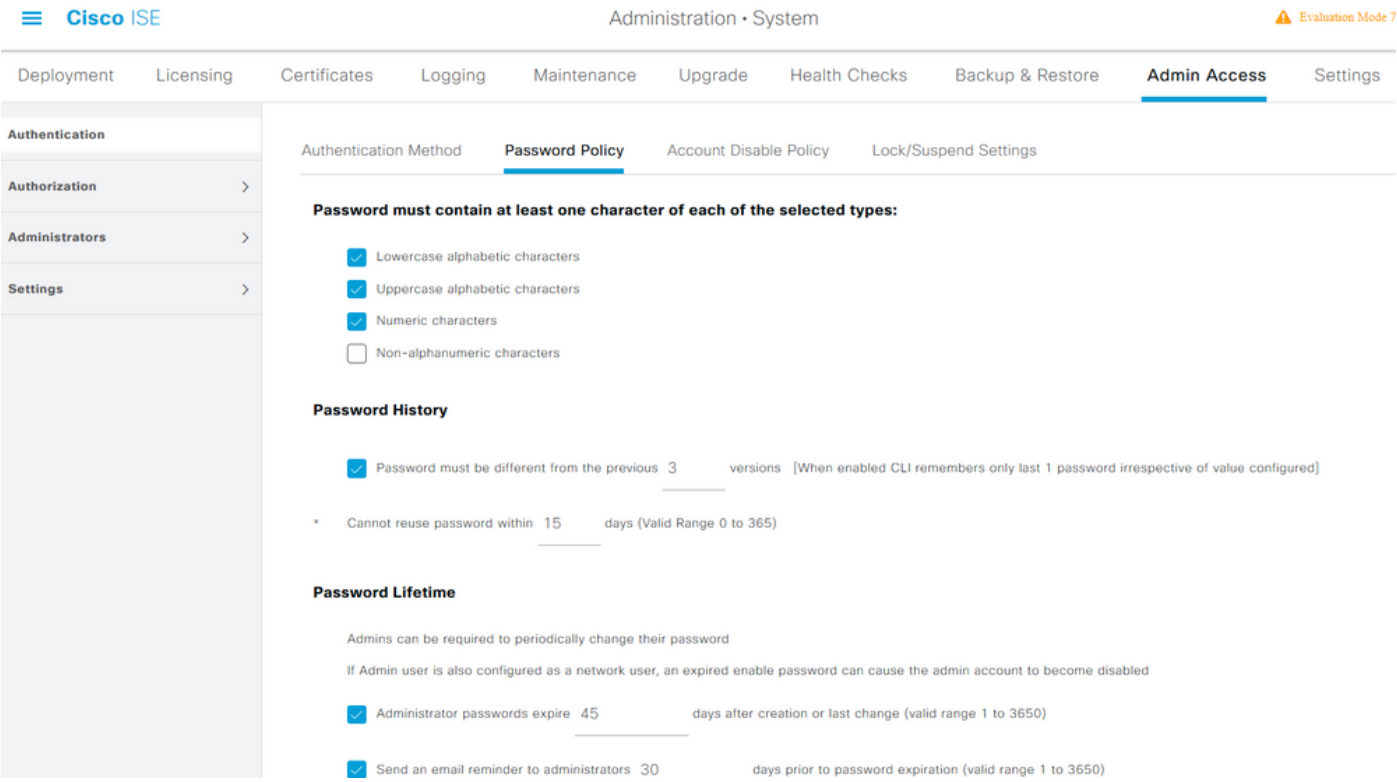
Admin Users need to authenticate themselves to access any information on ISE. The identity of admin users can be verified by using the ISE Internal Identity Store or an External Identity Store. The authenticity can be verified by either a password or a certificate. In order to configure these settings, navigate to **Administration > System> Admin Access > Authentication**. Select the required authentication type under the **Authentication Method** tab.



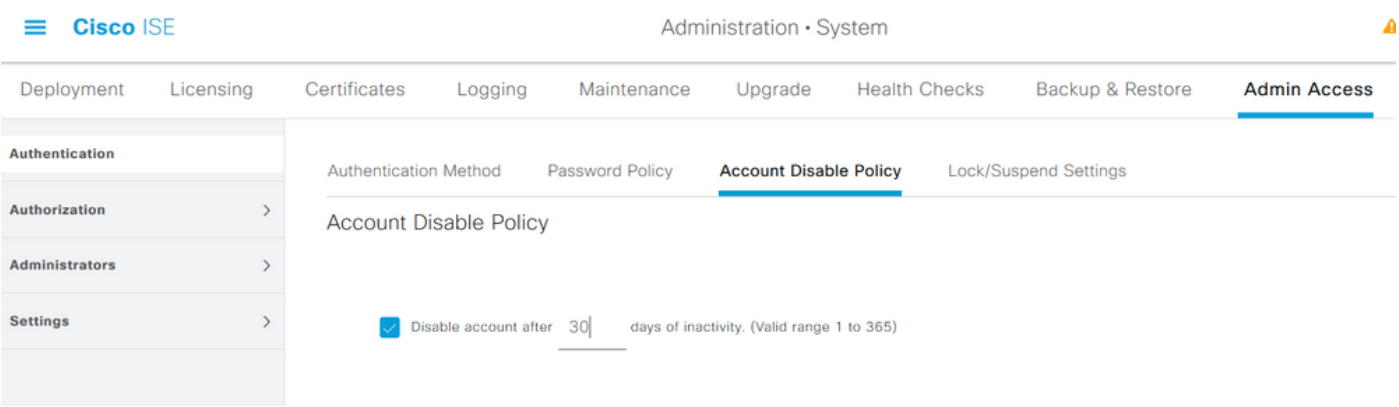
> **Note**: Password-Based authentication is enabled by default. If this is changed to Client Certificate-Based authentication, it causes an application server restart on all deployment nodes.

Identity Services Engine does not allow to configure the password policy for Command Line Interface (CLI) from the CLI. Password policy for both the Graphical User Interface (GUI) and the CLI can only be configured via the GUI of ISE. In order to configure this, navigate to **Administration > System > Admin Access > Authentication** and navigate to the **Password Policy** tab.

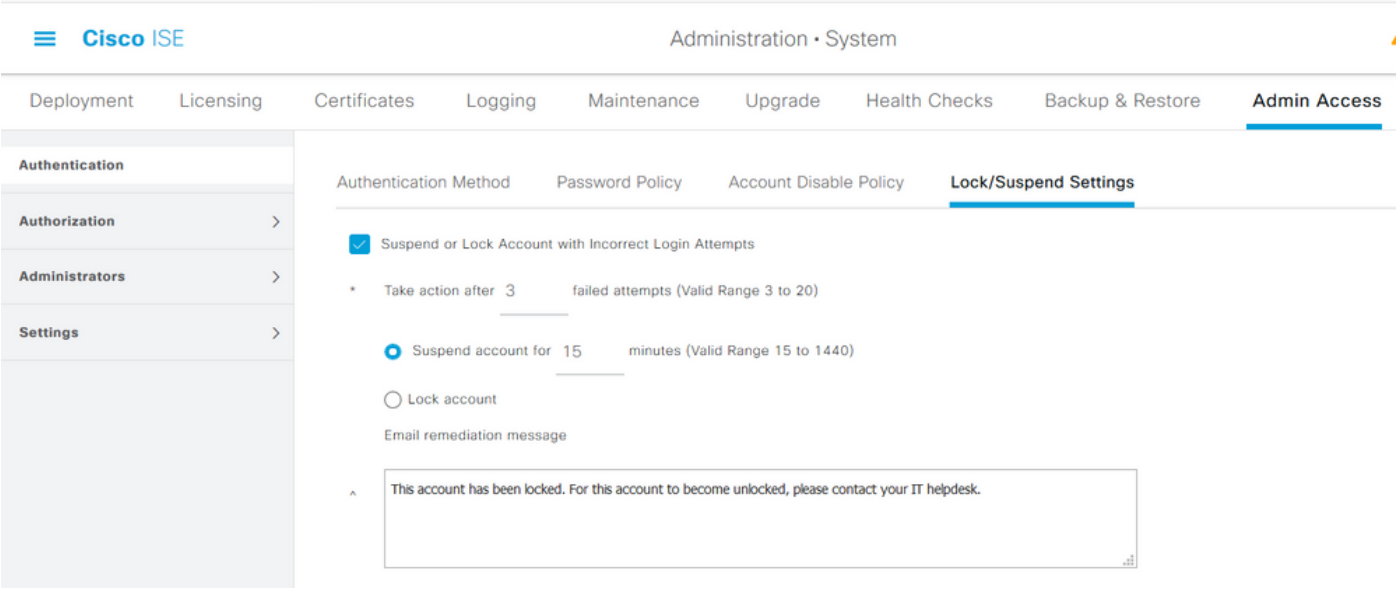




ISE has a provision to disable an inactive admin user. In order to configure this, navigate to **Administration > System > Admin Access > Authentication** and navigate to **Account Disable Policy** tab.



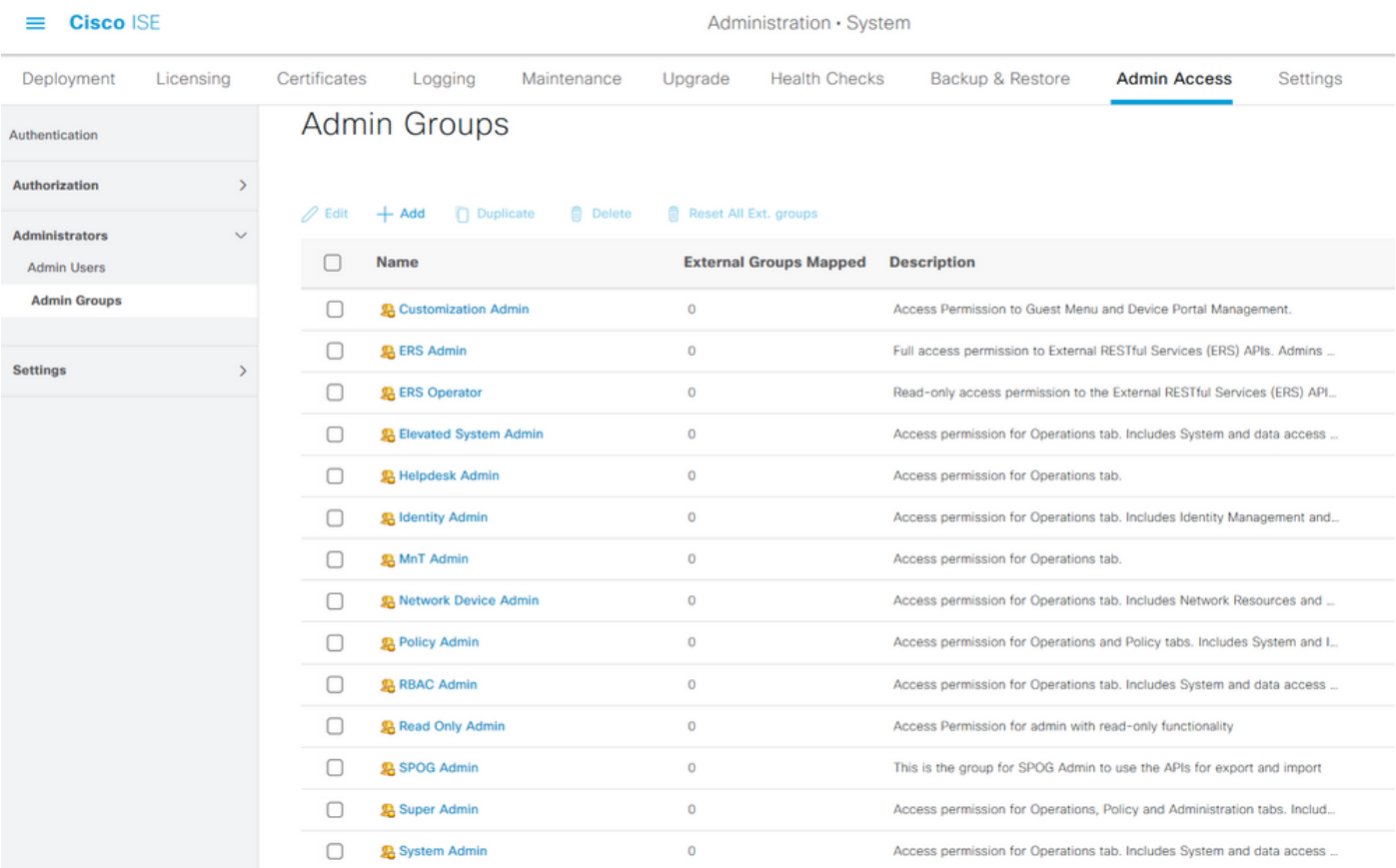
ISE also provides the facility to lock or suspend an admin user account based on the number of failed login attempts. In order to configure this, navigate to **Administration > System > Admin Access > Authentication** and navigate to the **Lock/Suspend Settings** tab.



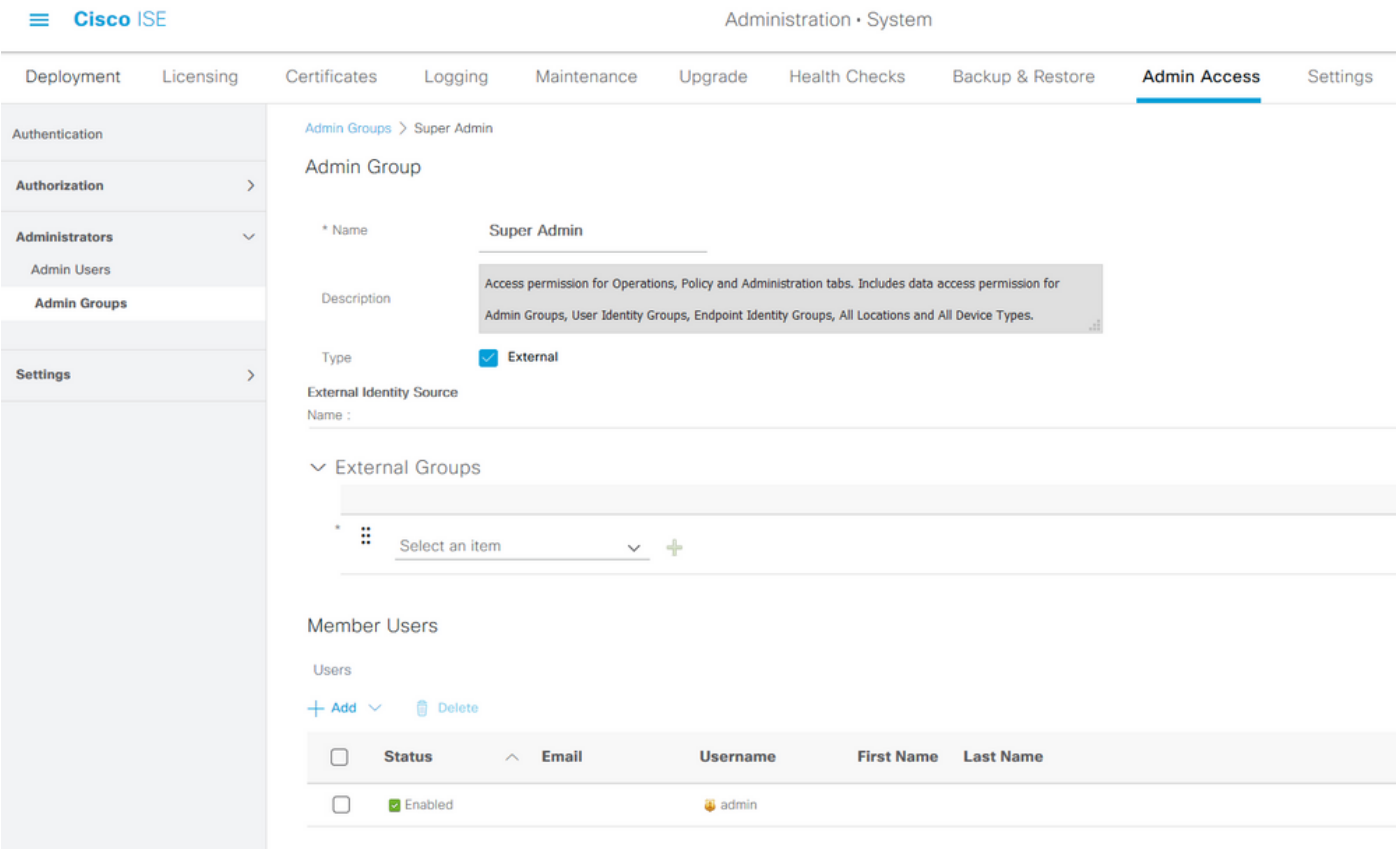
To manage administrative access, there is a need for administrative groups, users, and various policies/rules to control and manage their privileges.

Configure Admin Groups

Navigate to **Administration > System > Admin Access > Administrators > Admin Groups** to configure administrator groups. There are few groups that are built-in by default and cannot be deleted.

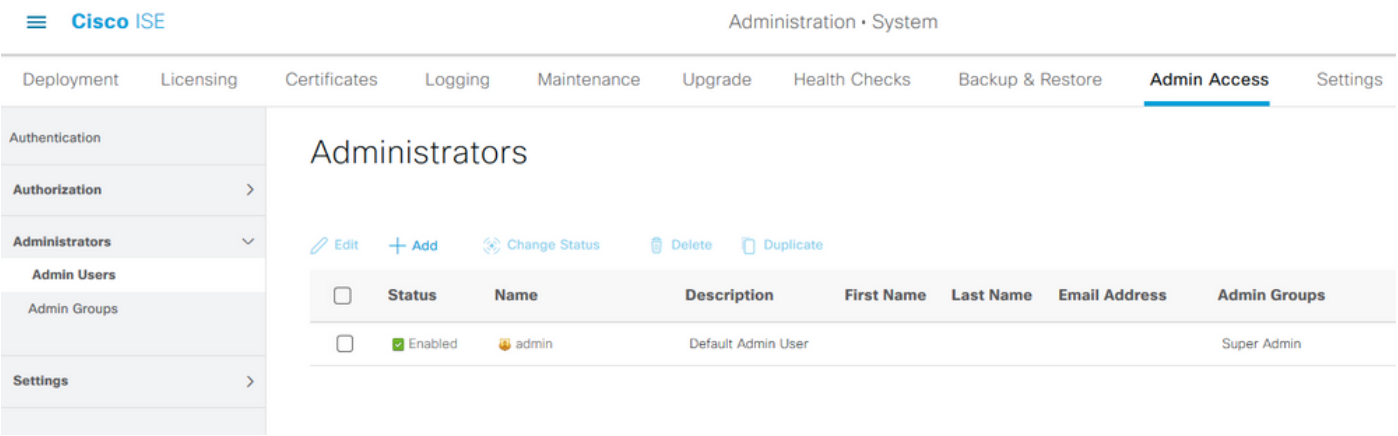


Once a group is created, select the group and click on edit to add administrative users to that group. There is a provision to map External Identity Groups to the Admin Groups on ISE so that an External Admin user gets the required permissions. In order to configure this, select the type as External while adding the user.

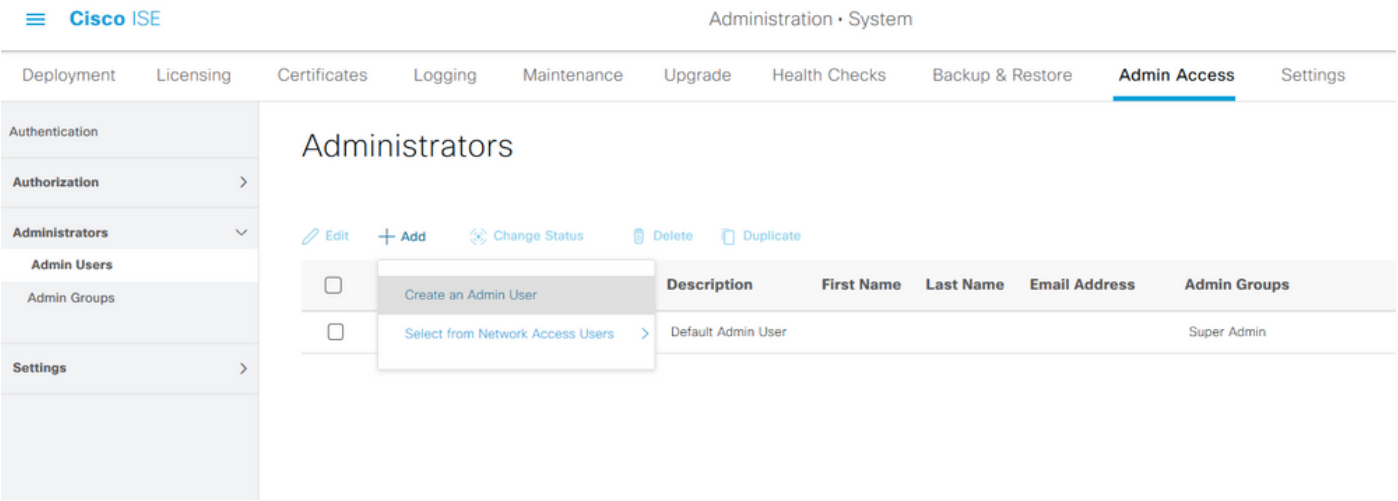


Configure Admin Users

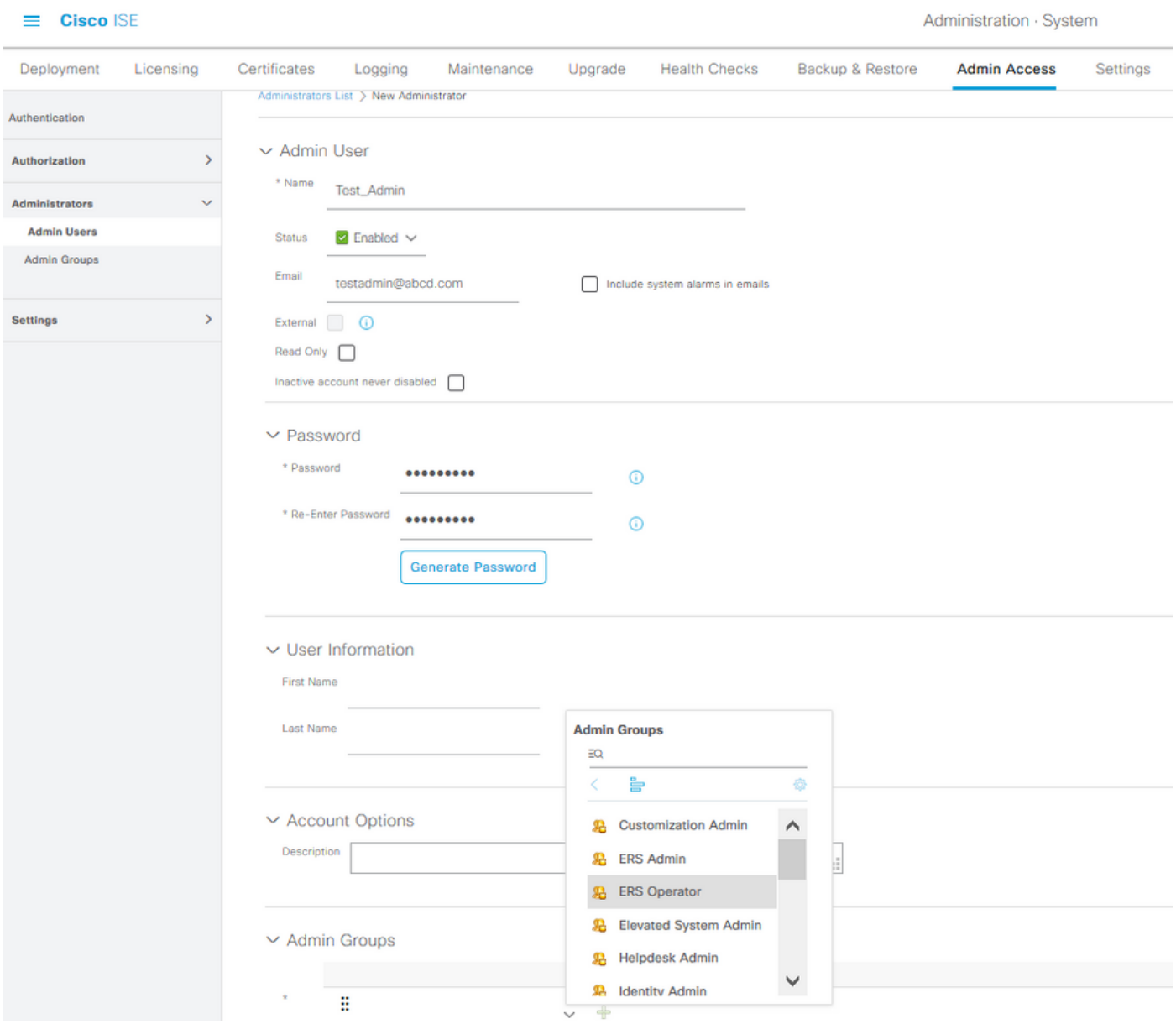
In order to configure Admin Users, navigate to **Administration > System > Admin Access > Administrators > Admin Users**.



Click **Add**. There are two options to choose from. One is to add a new user altogether. The other one is to make a Network Access User (i.e., a user-configured as an internal user to access the network/devices) as an ISE admin.



After you select an option, the required details must be provided and the user group must be selected based on which the permissions and privileges are given to the user.



Configure Permissions

There are two types of permissions that can be configured for a user group:

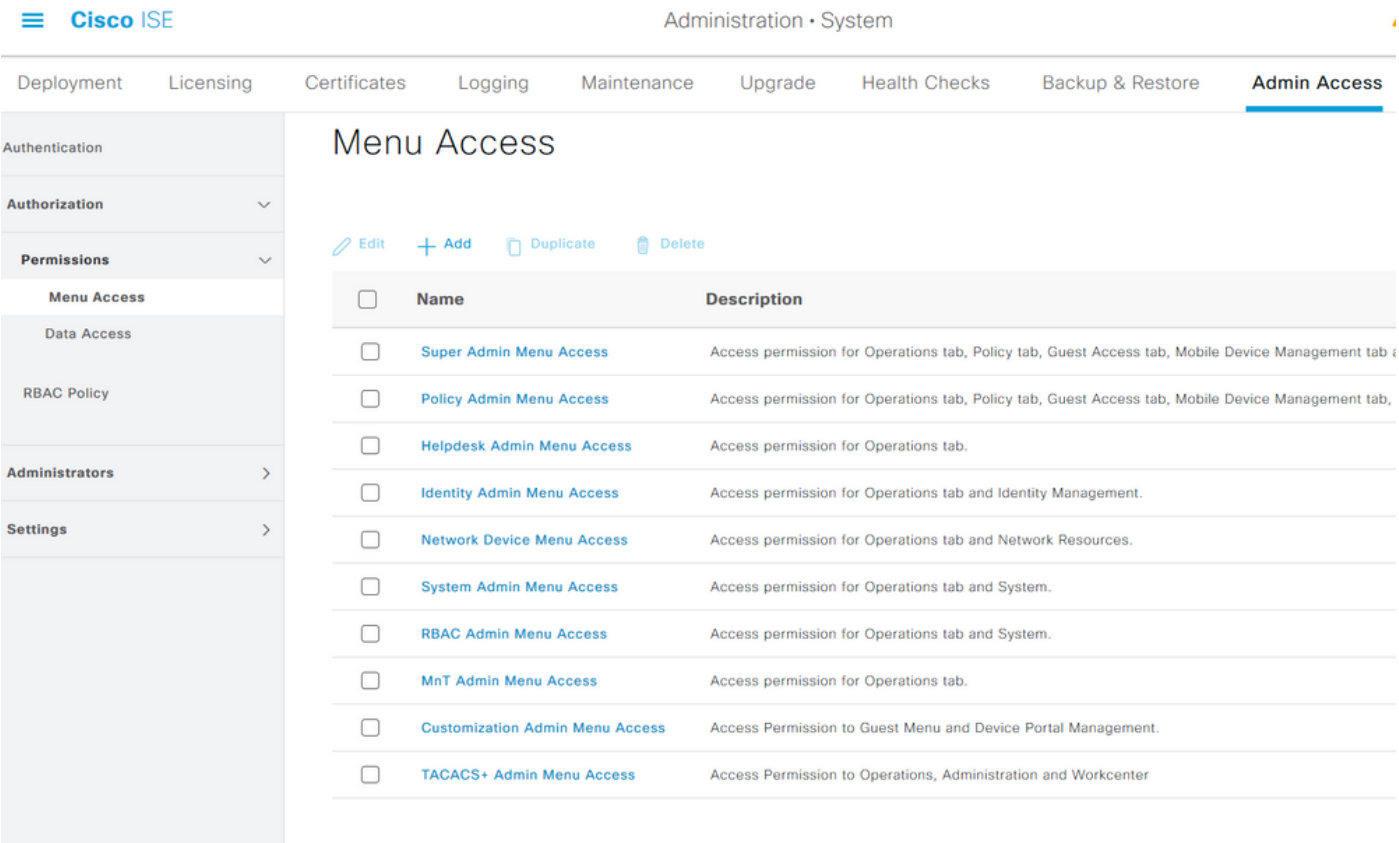
1. Menu Access
2. Data Access

Menu Access controls the navigational visibility on ISE. There are two options for every tab, Show or Hide, that can be configured. A Menu Access rule can be configured to show or hide selected tabs.

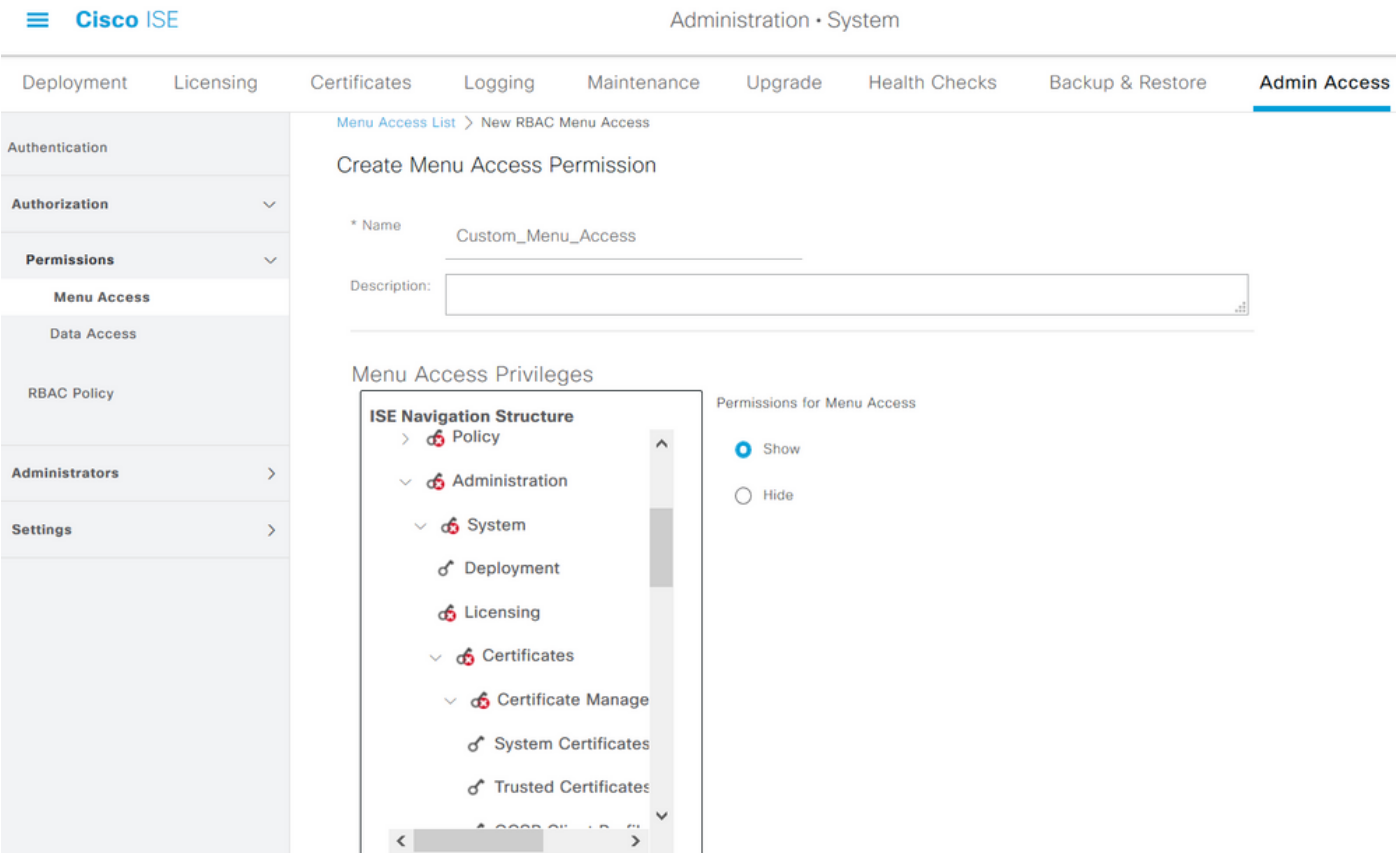
Data Access controls the ability to read/access/modify the Identity Data on ISE. Access permission can be configured only for Admin Groups, User Identity Groups, Endpoint Identity Groups, and Network Device Groups. There are three options for these entities on ISE which can be configured. They are Full Access, Read-Only Access, and No Access. A Data Access rule can be configured to choose one of these three options for each tab on ISE.

Menu Access and Data Access policies must be created before they can be applied to any admin group. There are a few policies that are built-in by default but they can always be customized or a new one can be created.

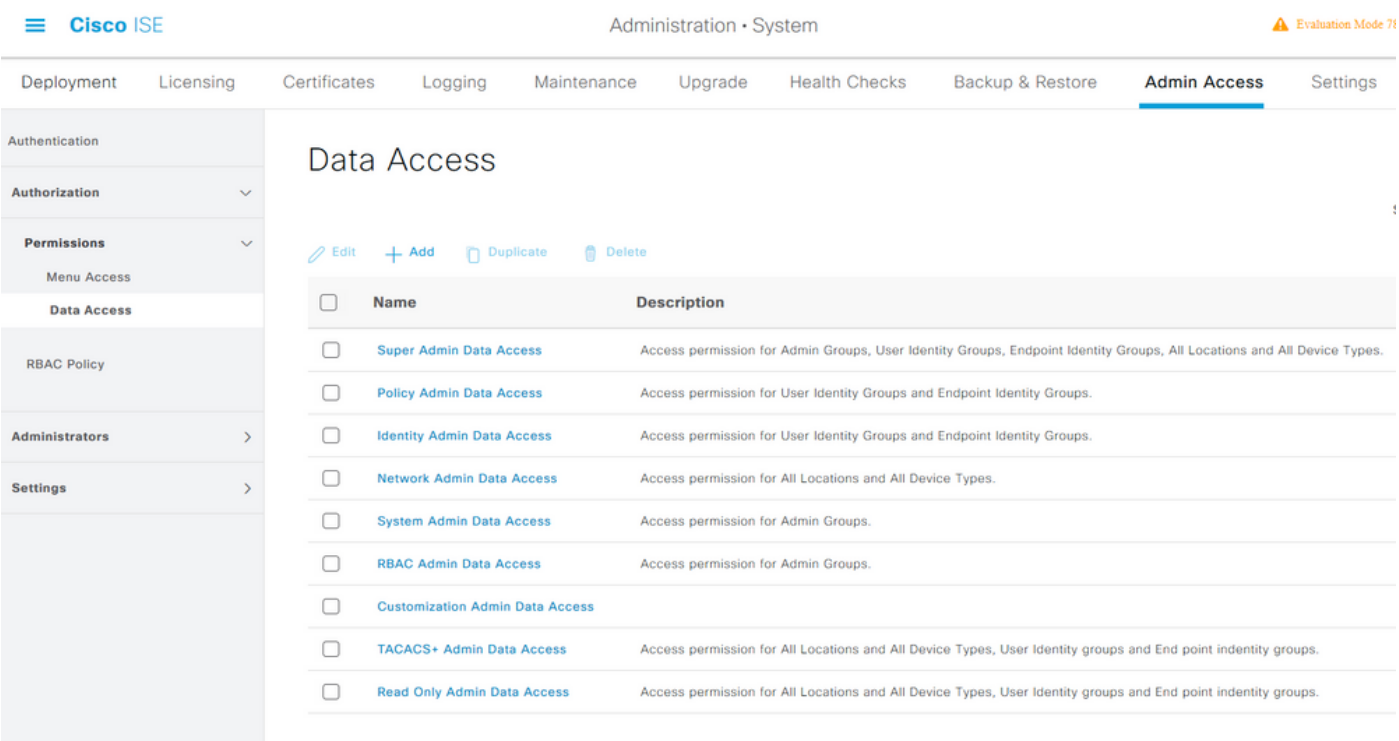
In order to configure a Menu Access policy, navigate to **Administration > System > Admin Access > Authorization > Permissions > Menu Access**.



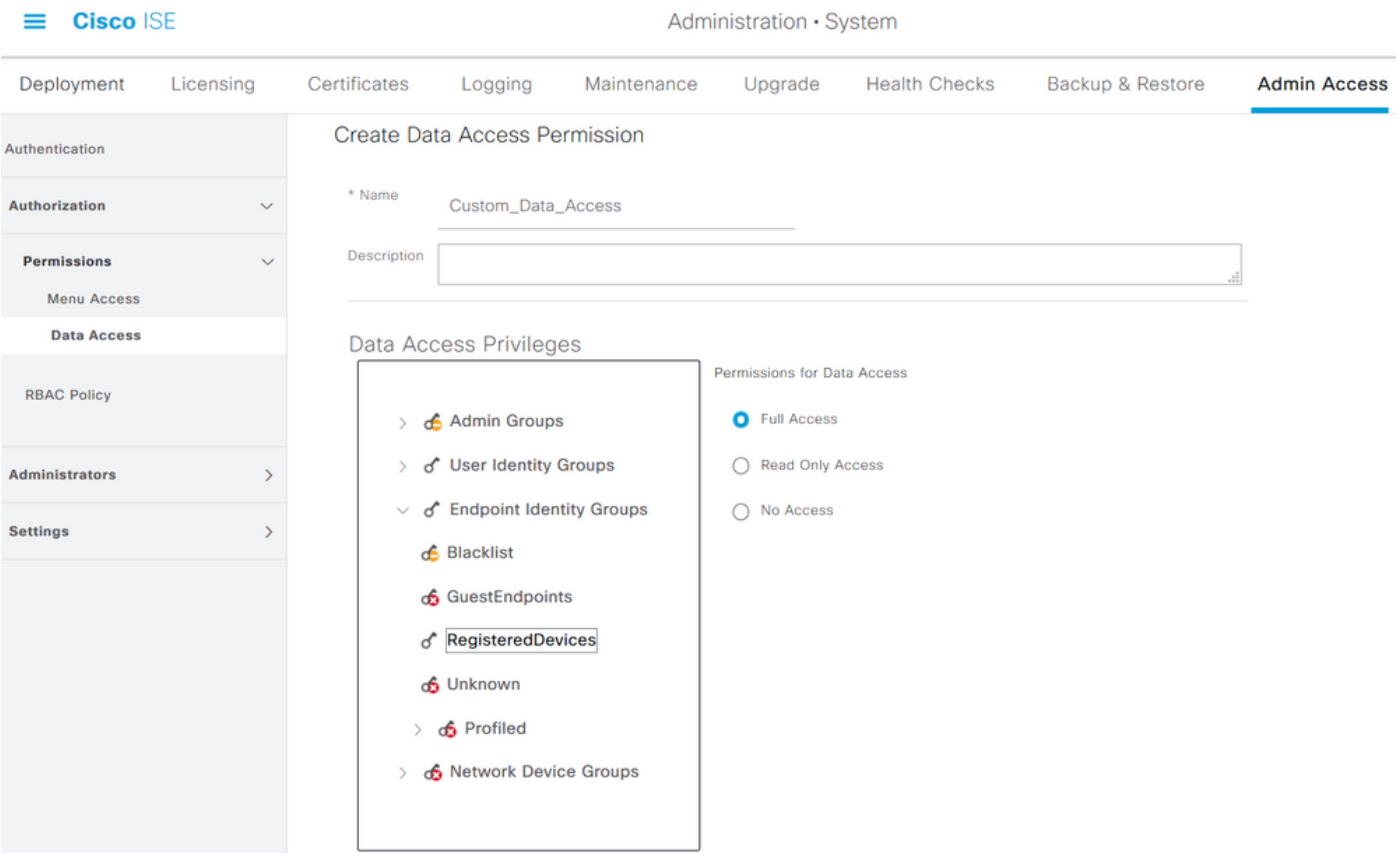
Click **Add**. Each navigational option in ISE can be configured to be shown/hidden in a policy.



In order to configure Data Access policy, navigate to **Administation > System > Admin Access > Authorization > Permissions > Data Access**.



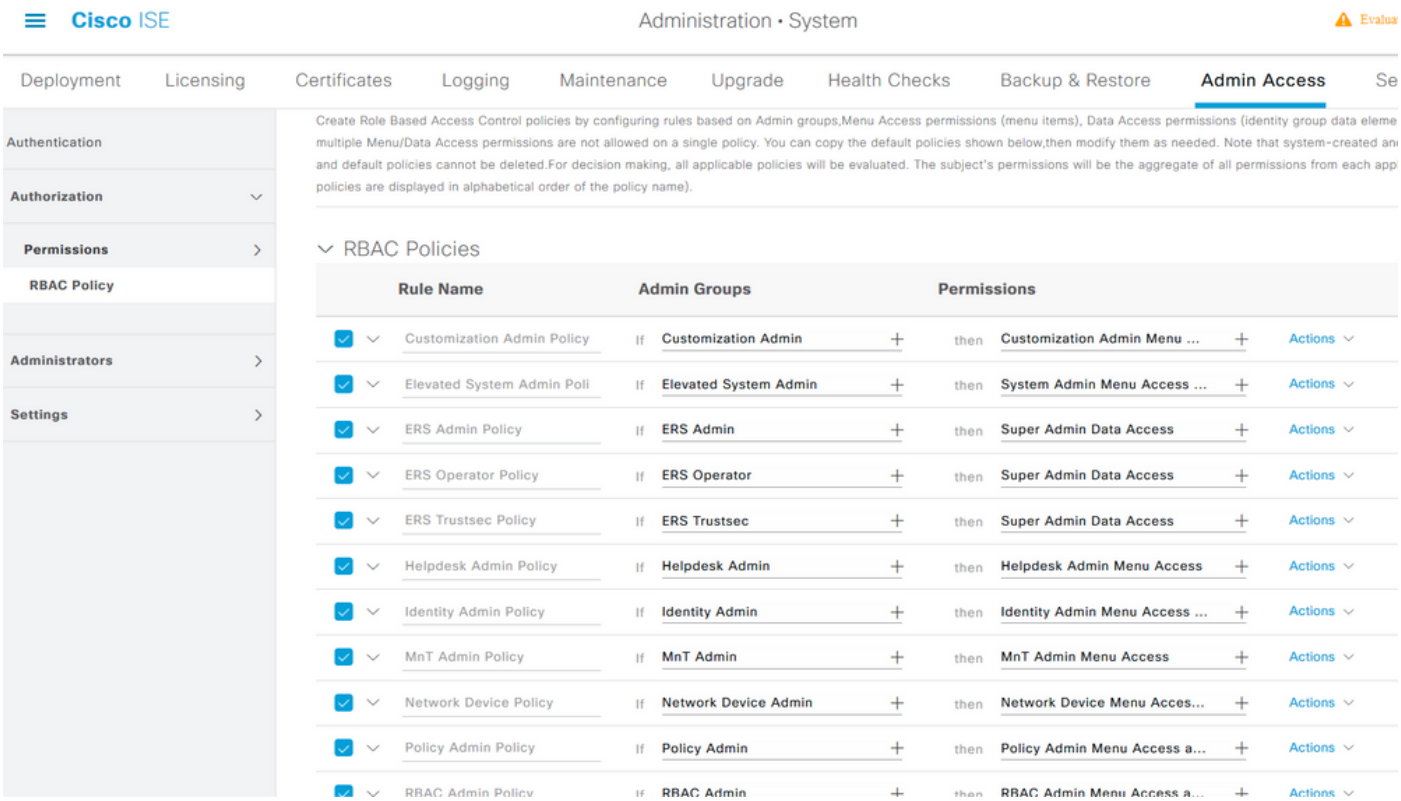
Click **Add** to create a new policy and configure permissions to access Admin/User Identity/Endpoint Identity/Network Groups.



Configure RBAC policies

RBAC stands for Role-Based Access Control. Role (Admin Group) to which a user belongs can be configured to use the desired Menu and Data Access policies. There can be multiple RBAC policies configured for a single role OR multiple roles can be configured in a single policy to access Menu and/or Data. All of those applicable policies are evaluated when an admin user tries

to perform an action. The final decision is the aggregate of all policies applicable to that role. If there are contradictory rules which permit and deny at the same time, the permit rule overrides the deny rule. To configure these policies, navigate to **Administration > System > Admin Access > Authorization > RBAC Policy**.



Click **Actions** to Duplicate/Insert/Delete a policy.

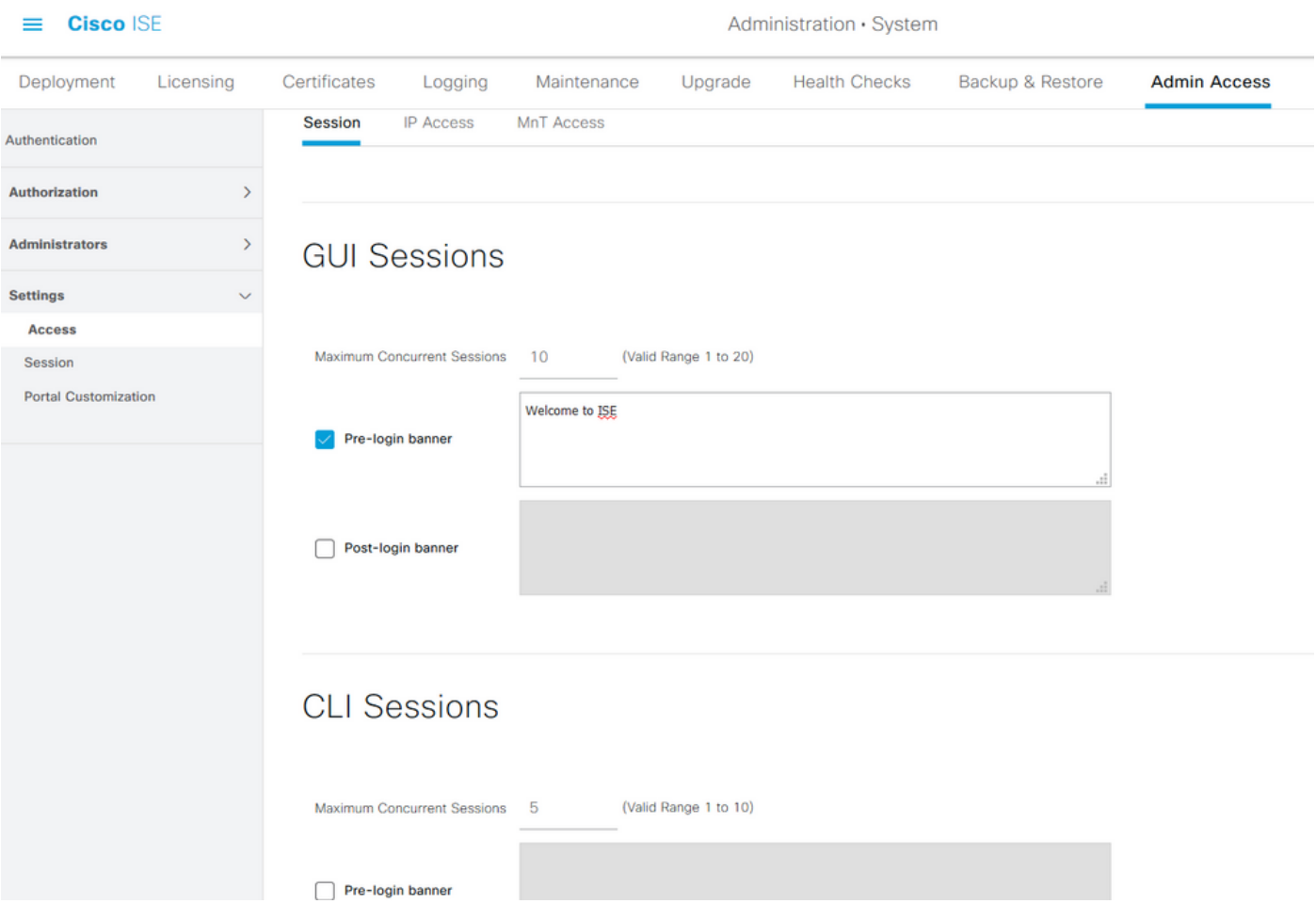
> **Note**: System-created and default policies cannot be updated, and default policies cannot be deleted.

> **Note**: Multiple Menu/Data Access permissions cannot be configured in a single rule.

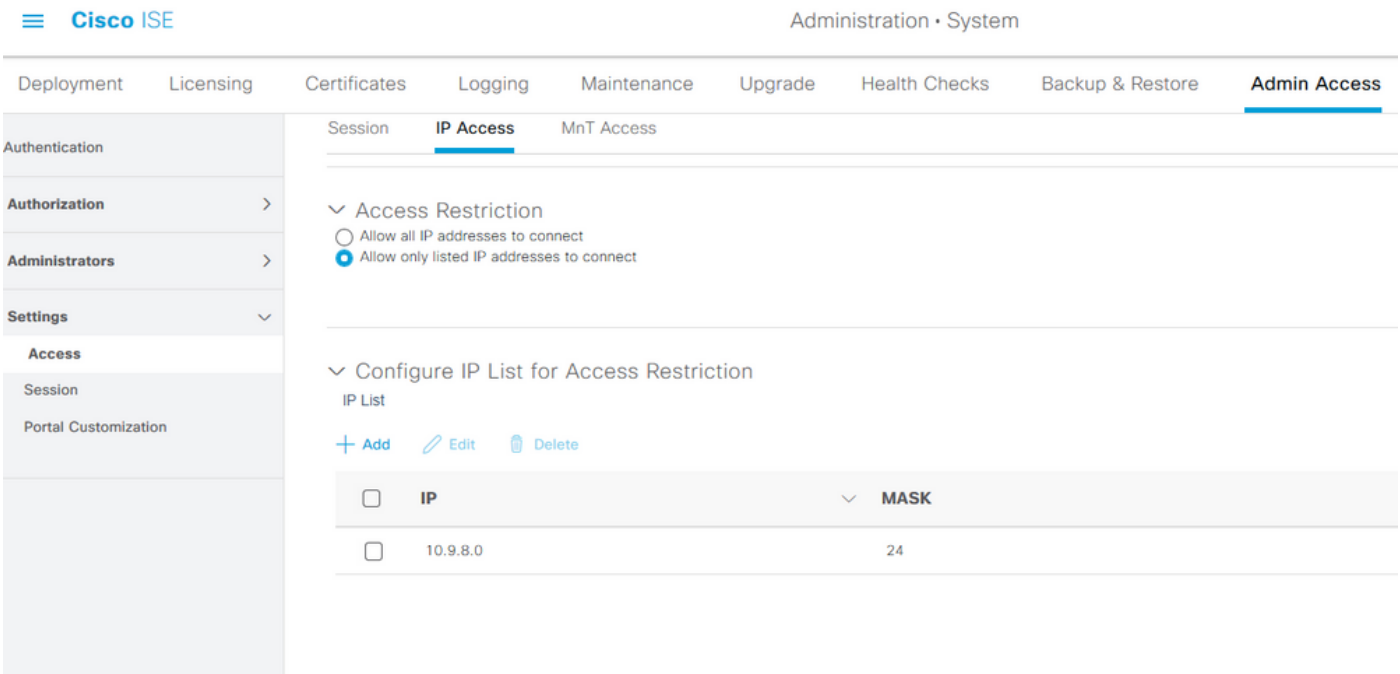
Configure Settings for Admin Access

In addition to the RBAC policies, there are a few settings that can be configured which are common to all the admin users.

In order to configure the number of Maximum Sessions Allowed, Pre-login, and Post-login Banners for GUI and CLI, navigate to **Administration > System > Admin Access > Settings > Access**. Configure these under the **Session** tab.



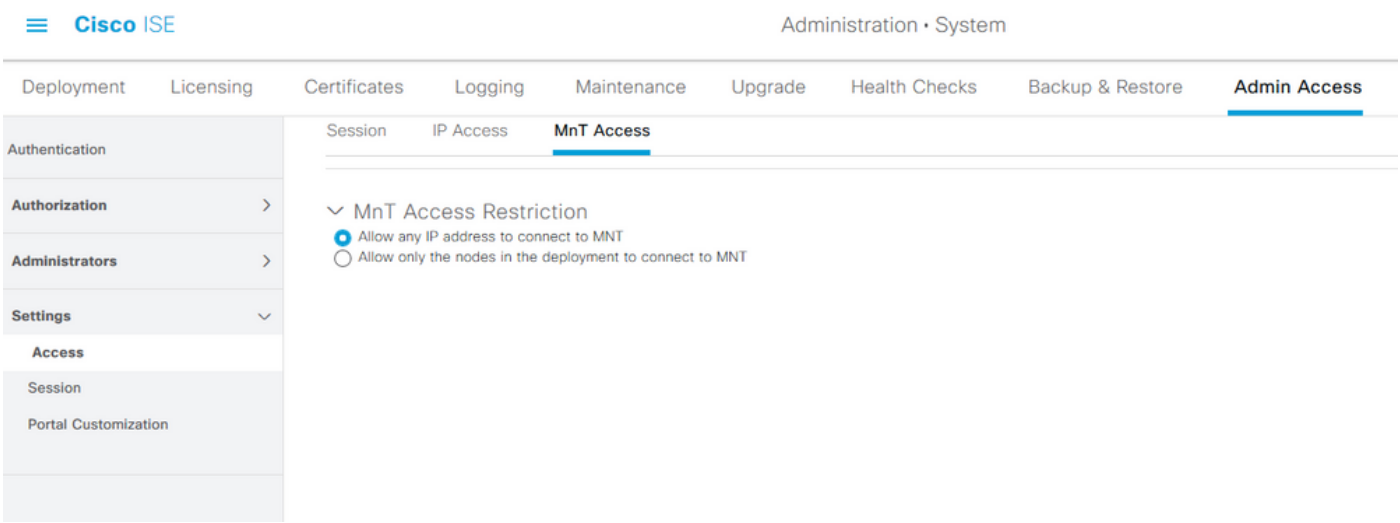
To configure the list of IP addresses from which the GUI and the CLI can be accessed, navigate to **Administration > System > Admin Access > Settings > Access** and navigate to the **IP Access** tab.



To configure a list of nodes from which administrators can access the MnT section in Cisco ISE, navigate to **Administration > System > Admin Access > Settings > Access** and navigate to the **MnT Access** tab.

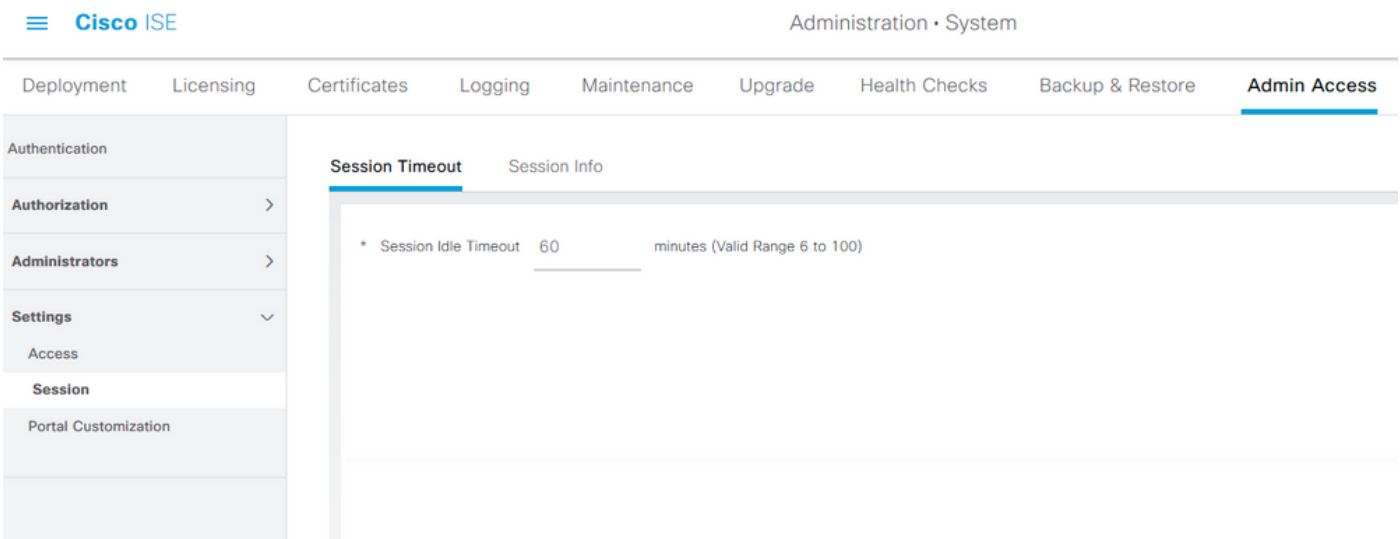
To allow nodes or entities either within the deployment or outside the deployment to send syslogs

to MnT, click the **Allow any IP address to connect to MNT** radio button. To allow only nodes or entities within the deployment to send syslogs to MnT, click **Allow only the nodes in the deployment to connect to MNT** radio button.

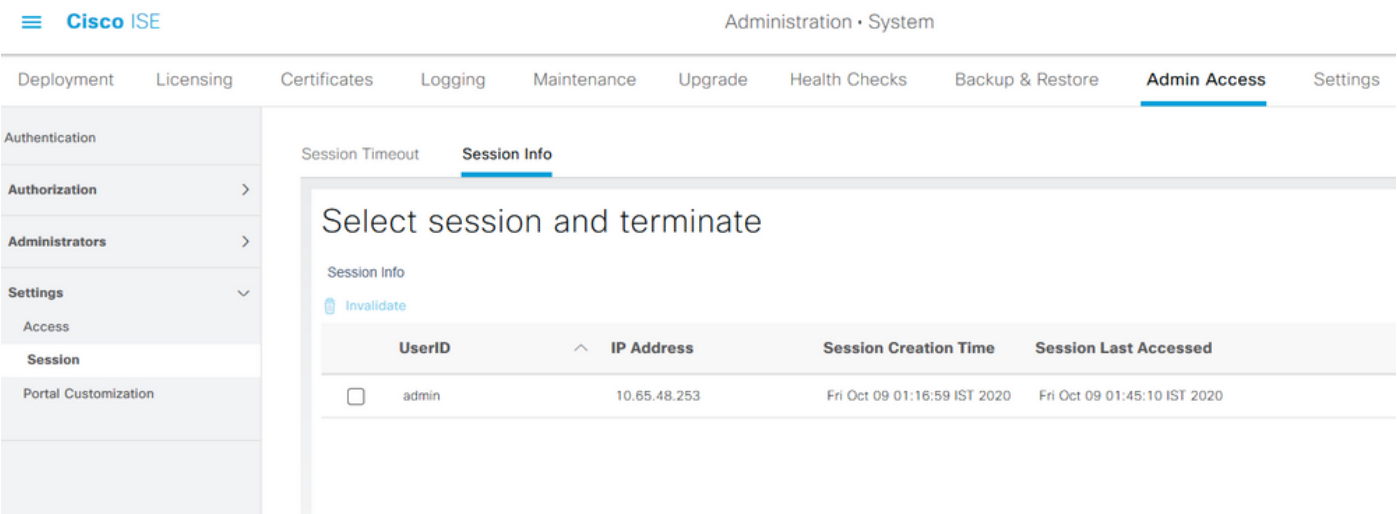


> **Note**: For ISE 2.6 patch 2 and later, *Use "ISE Messaging Service" for UDP Syslogs delivery to MnT* is turned on by default which doesn't allow syslogs coming from any other entities outside of deployment.

In order to configure a timeout value due to the inactivity of a session, navigate to **Administration > System > Admin Access > Settings > Session**. Set this value under the **Session Timeout** tab.



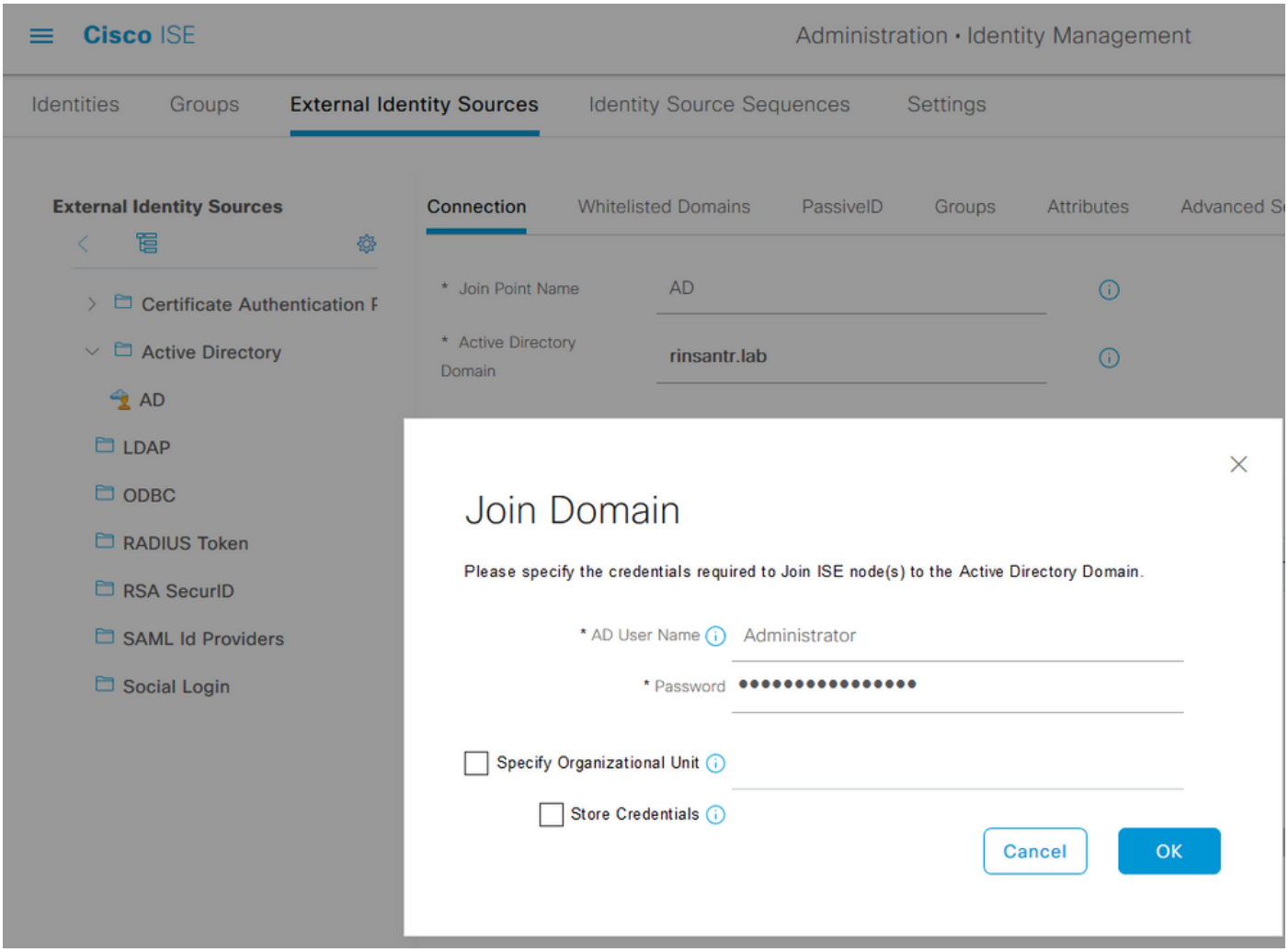
In order to view/invalidate the current active sessions, navigate to **Administration > Admin Access > Settings > Session** and click the **Session Info** tab.

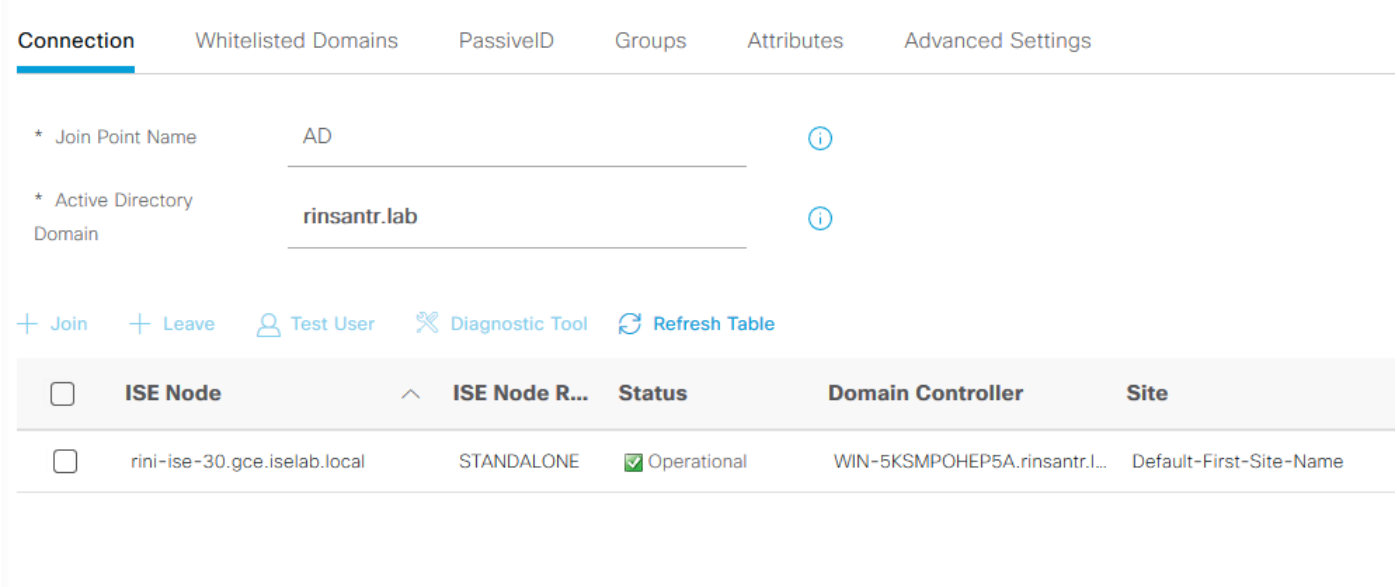


Configure Admin Portal Access with AD Credentials

Join ISE to AD

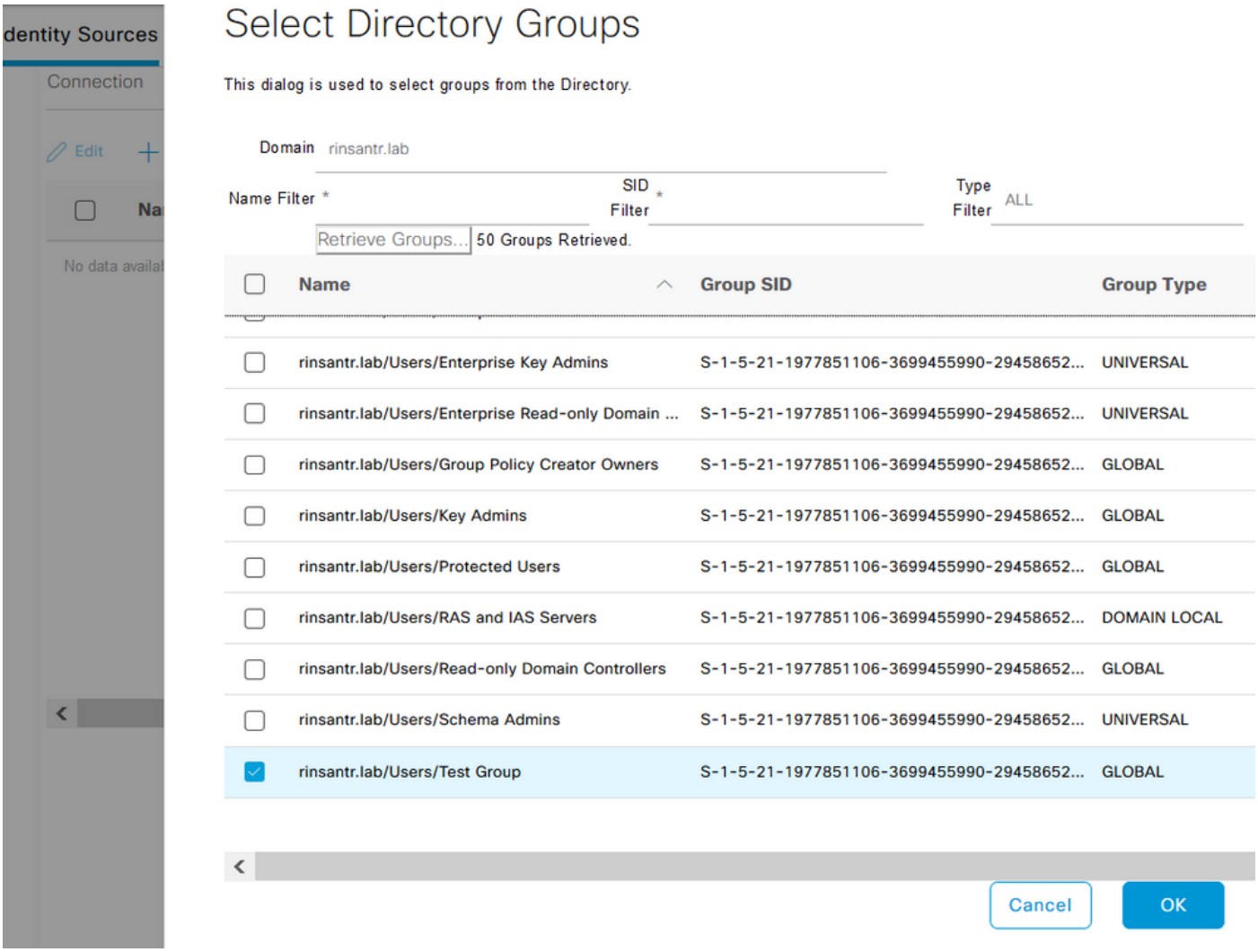
In order to join ISE to an external domain, navigate to **Administration > Identity Management > External Identity Sources > Active Directory**. Enter the new join point name and active directory domain. Enter the credentials of the AD account that can add and make changes to computer objects, and click **OK**.

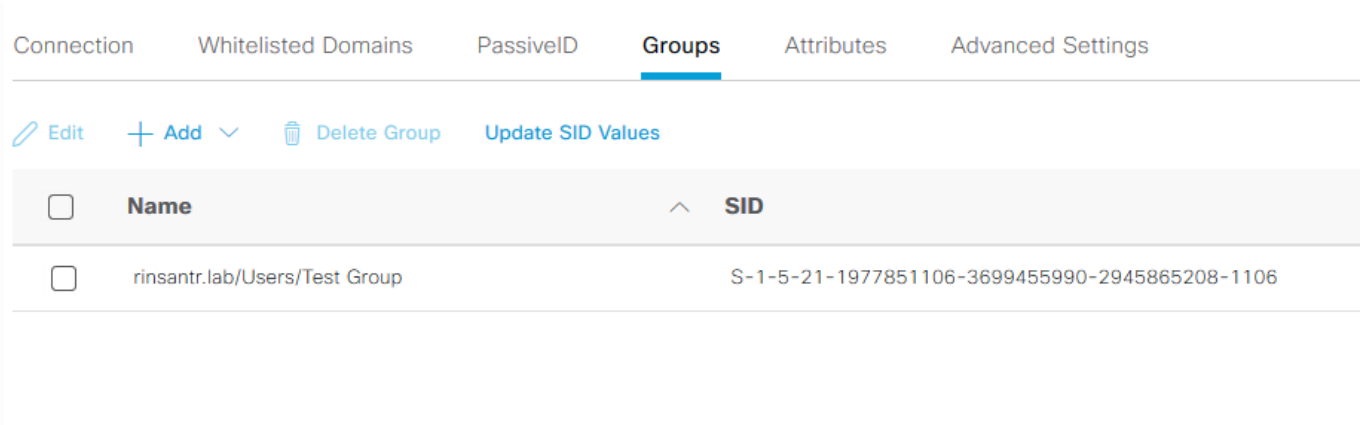




Select Directory Groups

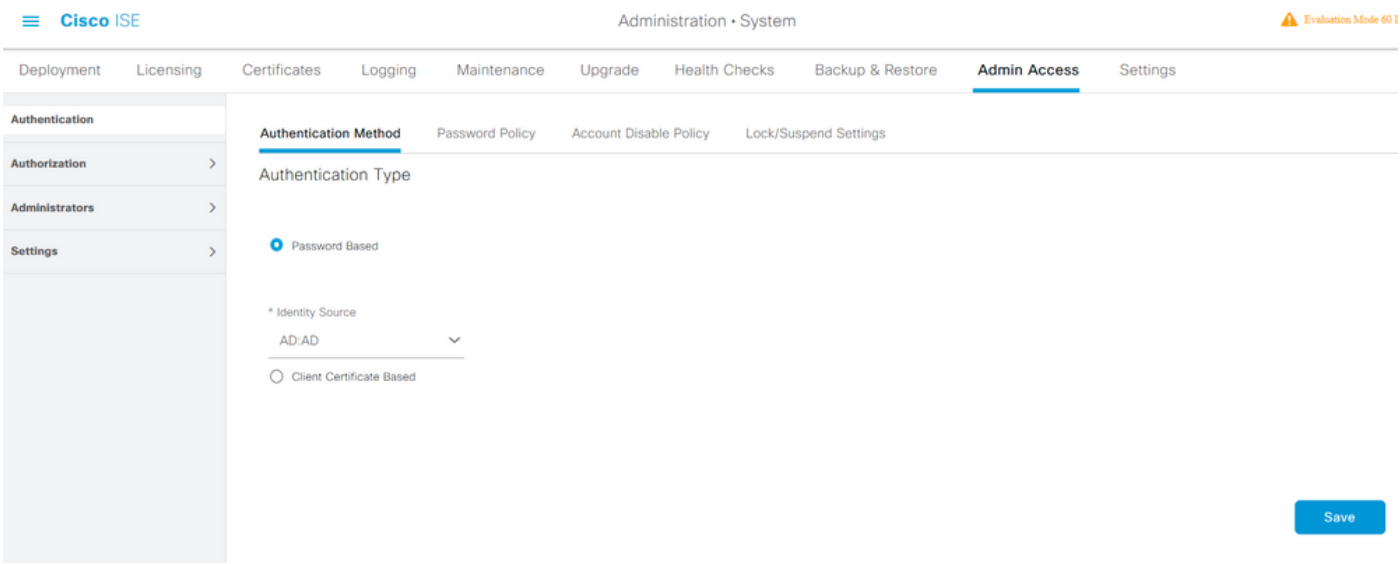
Navigate to **Administration > Identity Management > External Identity Sources > Active Directory**. Click on the desired Join Point Name and navigate to the **Groups** tab. Click on **Add > Select Groups from Directory > Retrieve Groups**. Import at least one AD Group to which your administrator belongs, and click **OK**, then click **Save**.





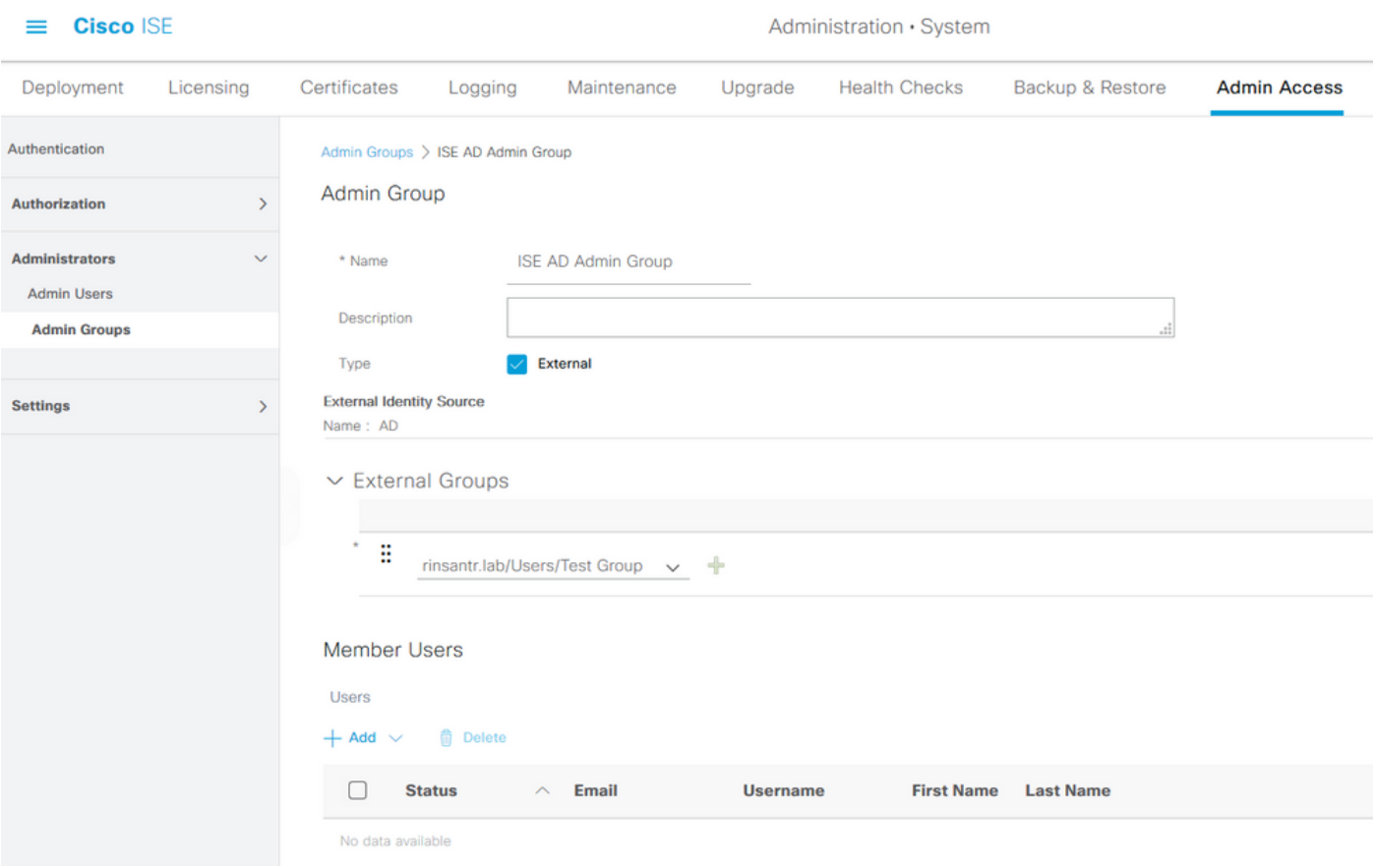
Enable Administrative Access for AD

In order to enable password-based authentication of ISE using AD, navigate to **Administration> System > Admin Access > Authentication**. In the **Authentication Method** tab, select the **Password-Based** option. Select **AD** from the **Identity Source** drop-down menu and click **Save**.



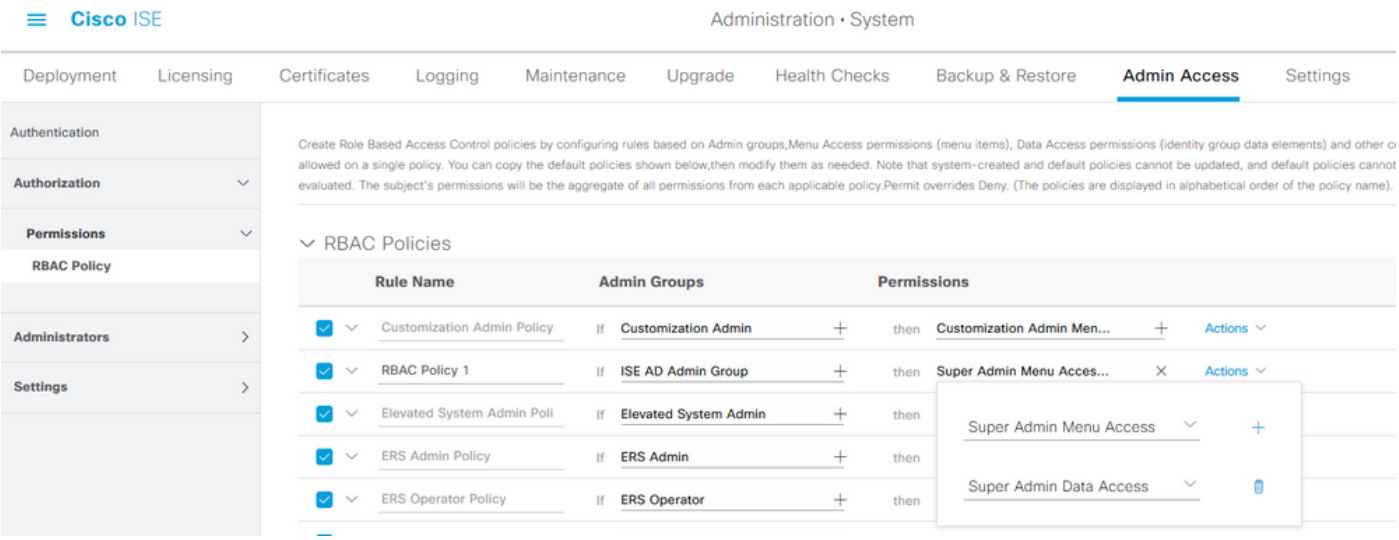
Configure the ISE Admin Group to AD Group Mapping

This allows authorization to determine the Role Based Access Control (RBAC) permissions for the administrator based on group membership in AD. To define a Cisco ISE Admin Group and map that to an AD group, navigate to **Administration > System > Admin Access > Administrators > Admin Groups**. Click **Add** and enter a name for the new Admin group. In the Type field, check the **External** check box. From the **External Groups** drop-down menu, select the AD group to which this Admin Group is to be mapped (as defined in the Select Directory Groups section above). **Submit** the changes.



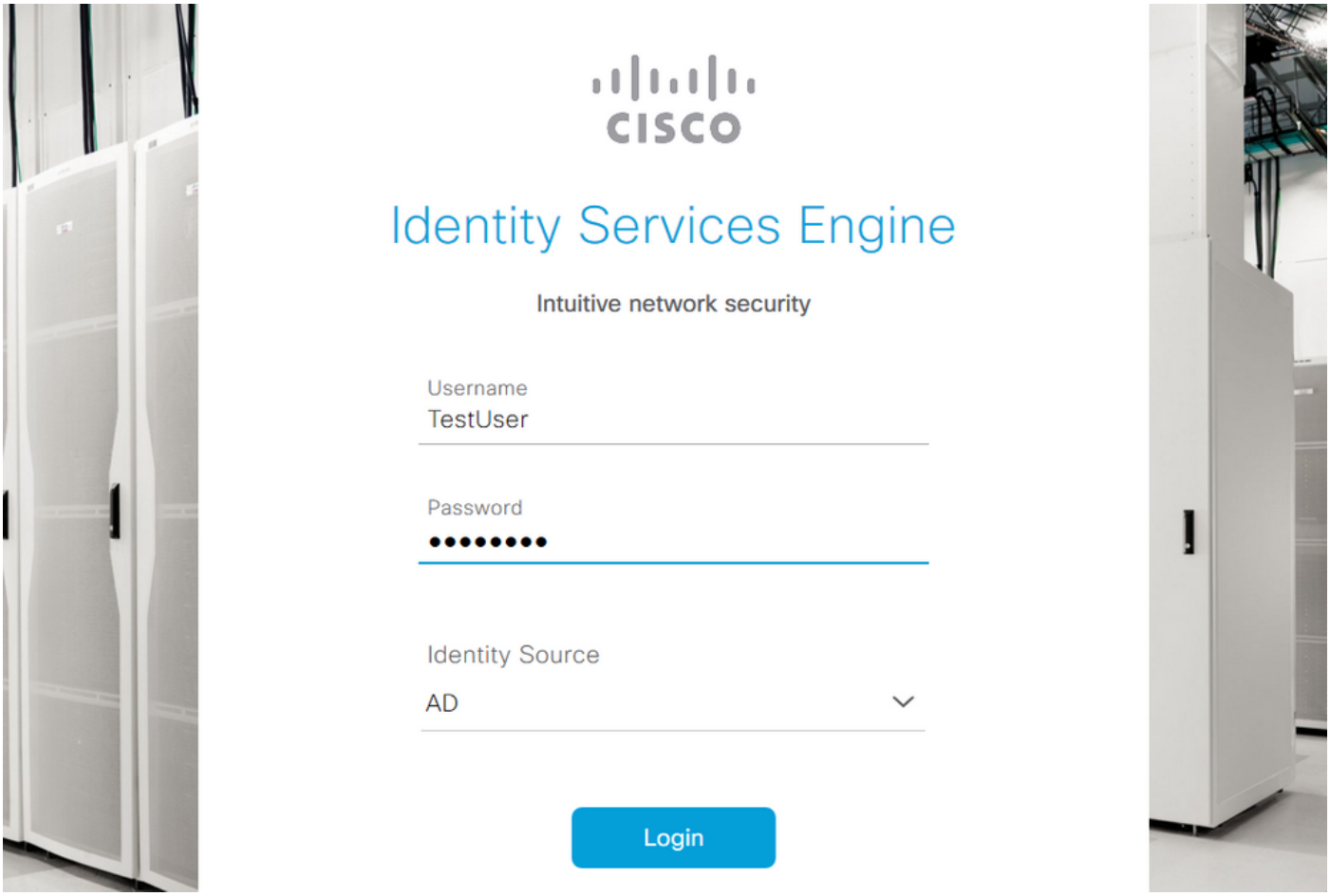
Set RBAC Permissions for the Admin Group

To assign RBAC permissions to the Admin Group created in the previous section, navigate to **Administration > System > Admin Access > Authorization > RBAC Policy**. From the **Actions** drop-down menu on the right, select **Insert new policy**. Create a new rule, map it with the Admin Group defined in the above section, and assign it with desired data and menu access permissions, then click **Save**.

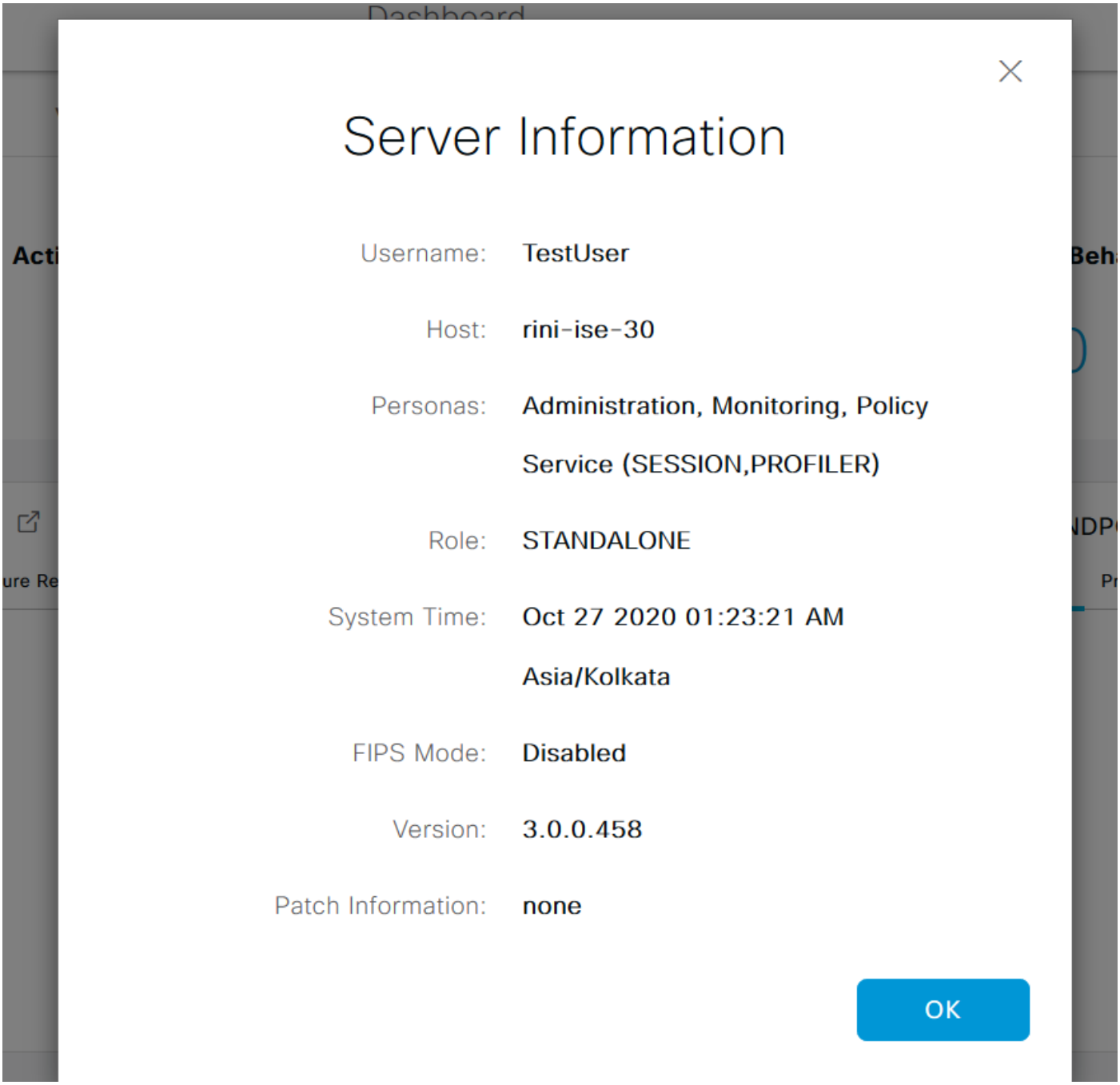


Access ISE with AD Credentials and Verify

Log out of the administrative GUI. Select the Join Point name from the **Identity Source** drop-down menu. Enter the username and password from the AD database, and log in.



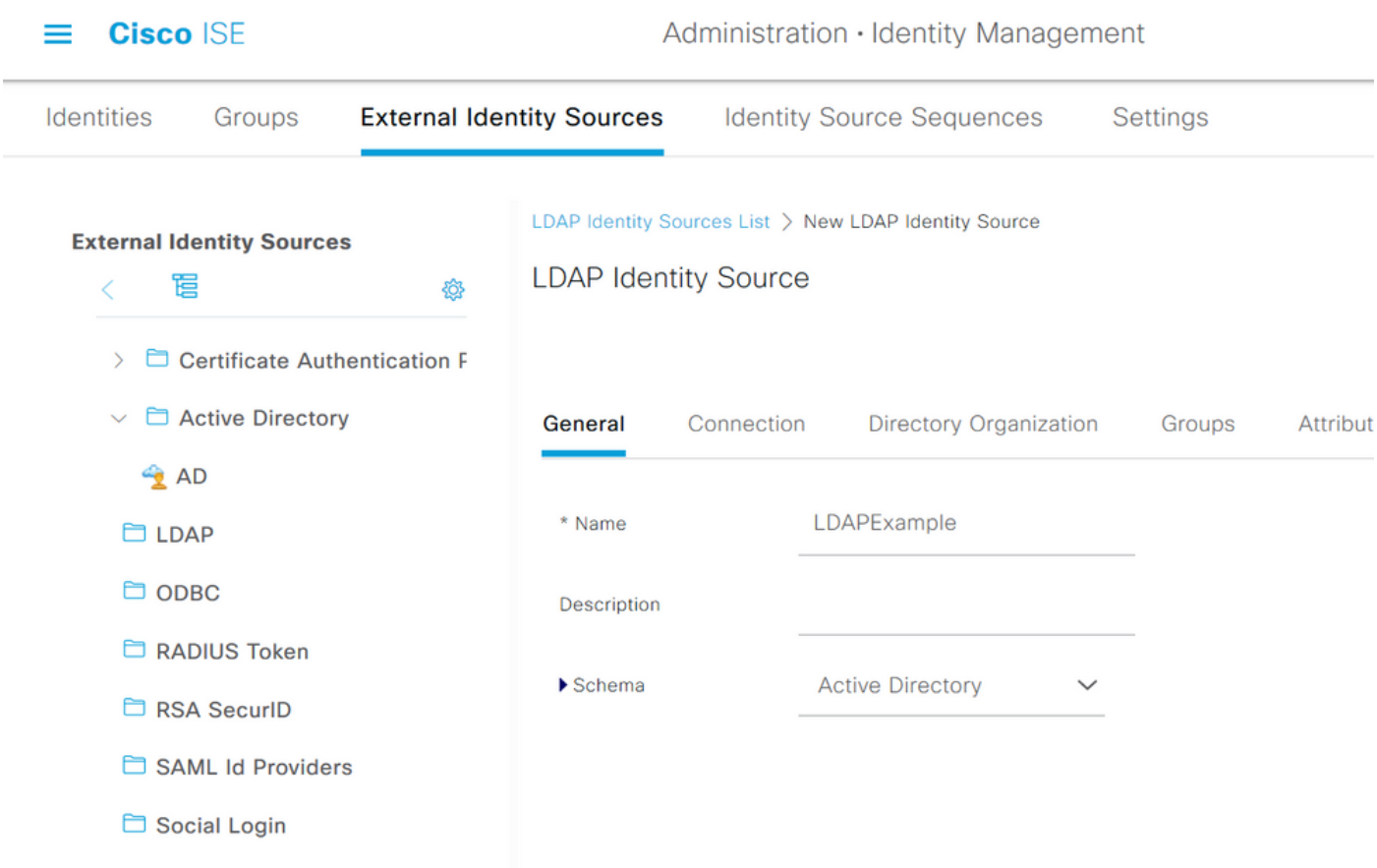
To confirm that the configuration works properly, verify the authenticated username from **Settings** icon on the top right corner of the ISE GUI. Navigate to **Server Information** and verify the Username.



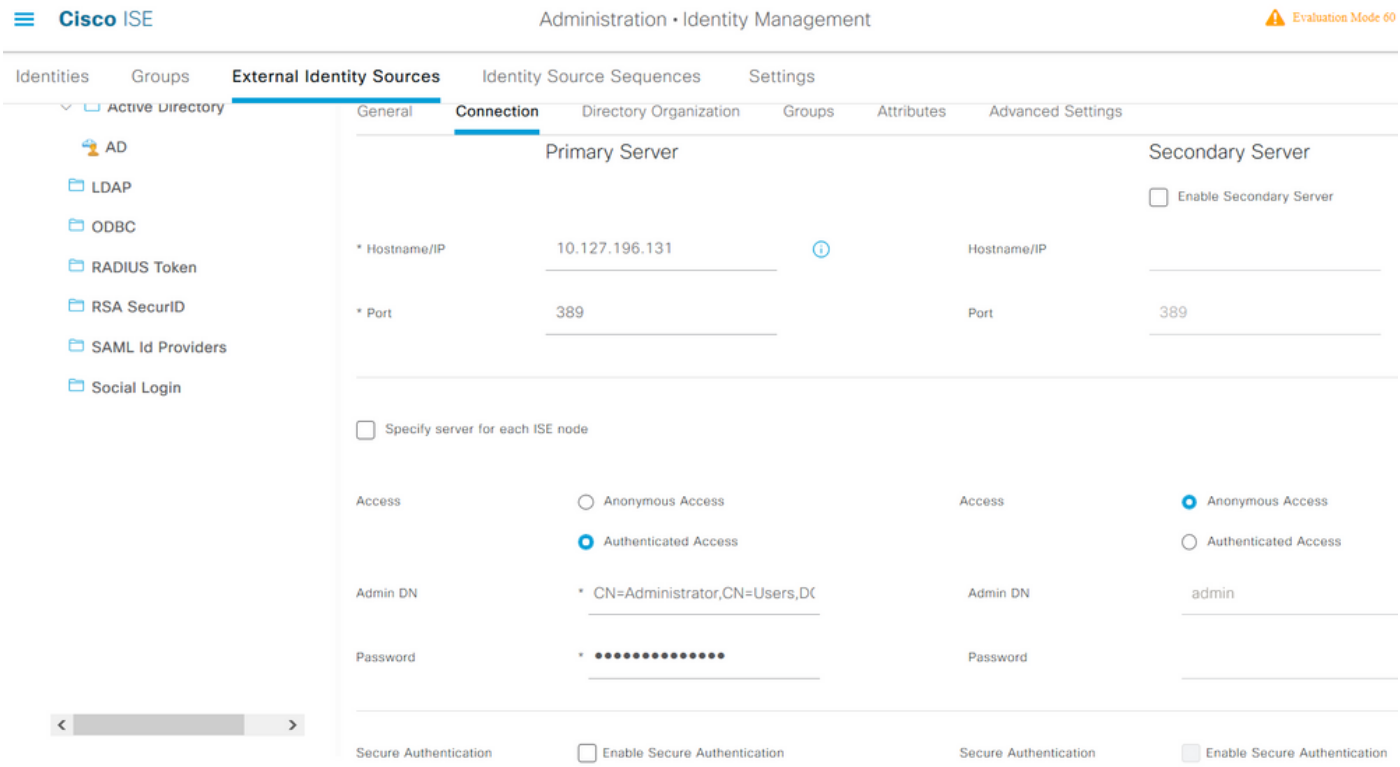
Configure Admin Portal Access with LDAP

Join ISE to LDAP

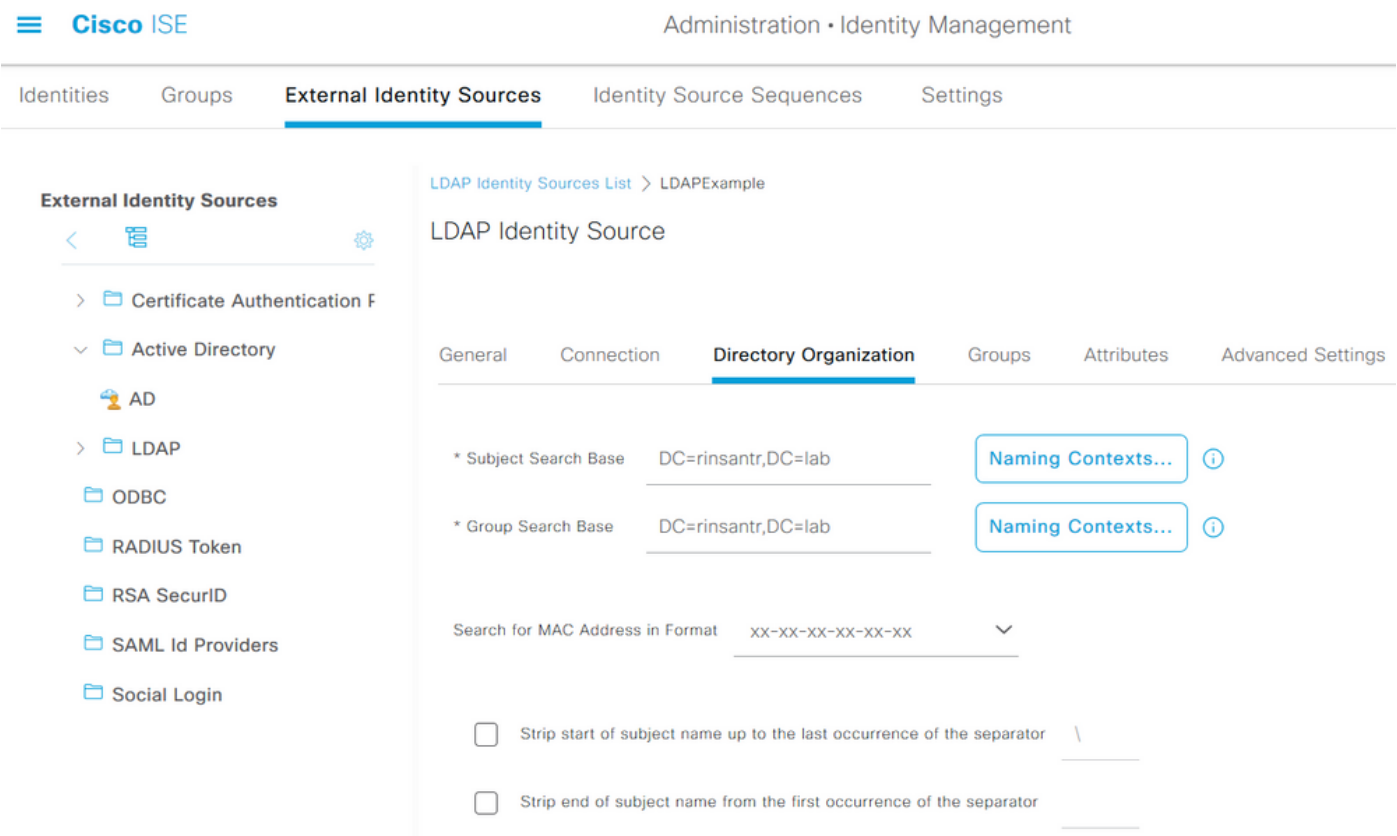
Navigate to **Administration > Identity Management > External Identity Sources > Active Directory > LDAP**. Under the **General** tab, enter a name for the LDAP and choose the schema as **Active Directory**.



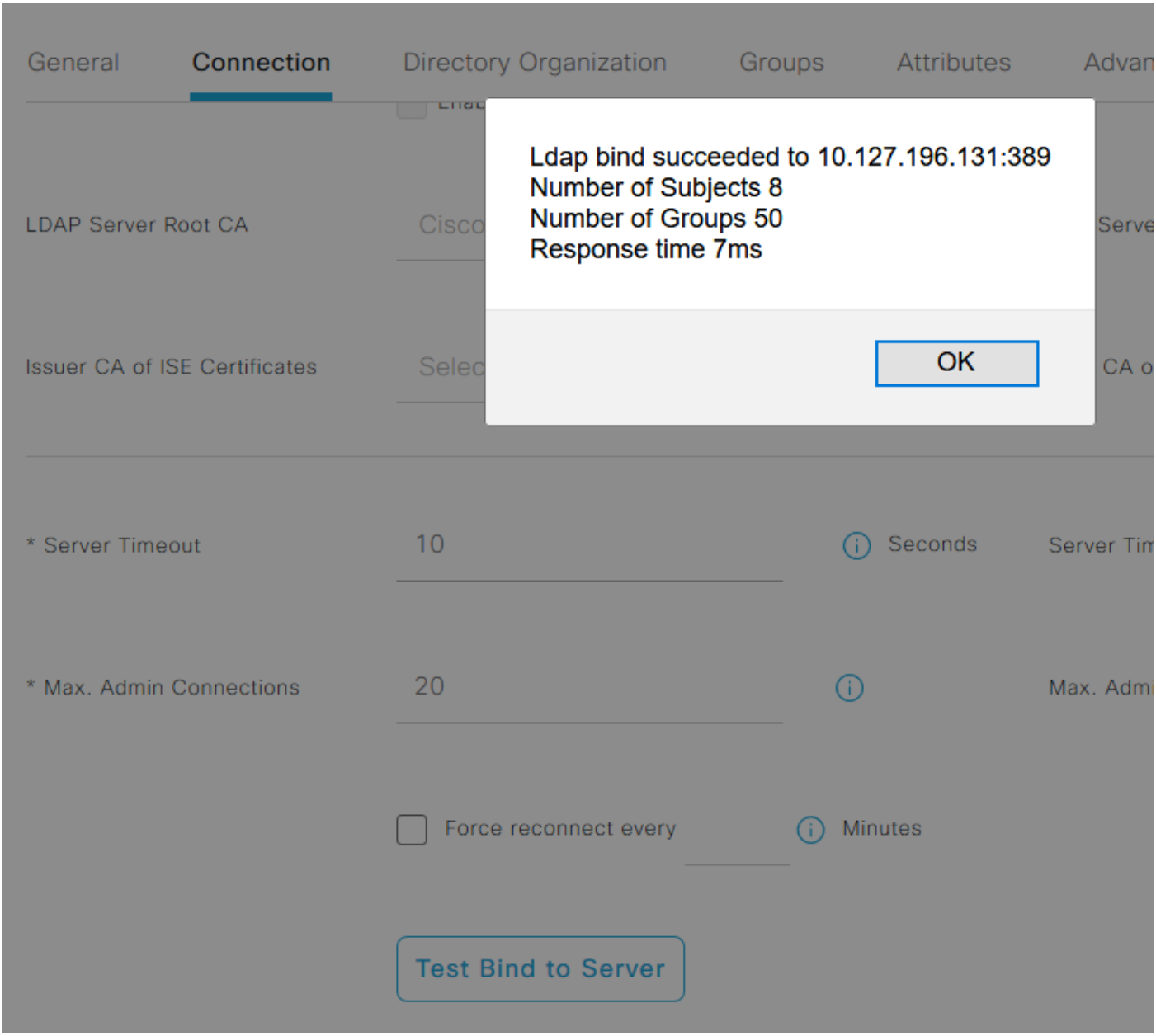
Next, to configure the connection type, navigate to the **Connection** tab. Here, set the Hostname/IP of the Primary LDAP server along with the port 389(LDAP)/636 (LDAP-Secure). Enter the path of the Admin distinguished name (DN) with the Admin password of the LDAP server.



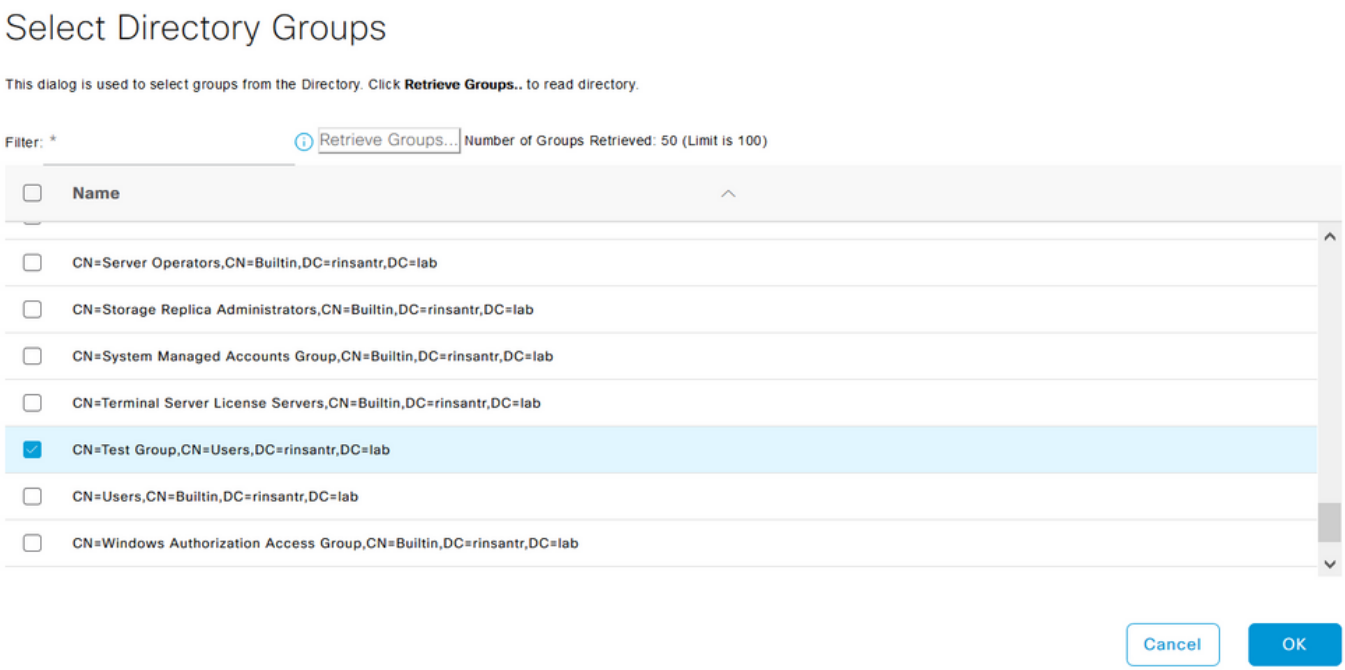
Next, navigate to the **Directory Organization** tab and click on **Naming Contexts** to choose the correct organization group of the user based on the hierarchy of users stored in the LDAP server.

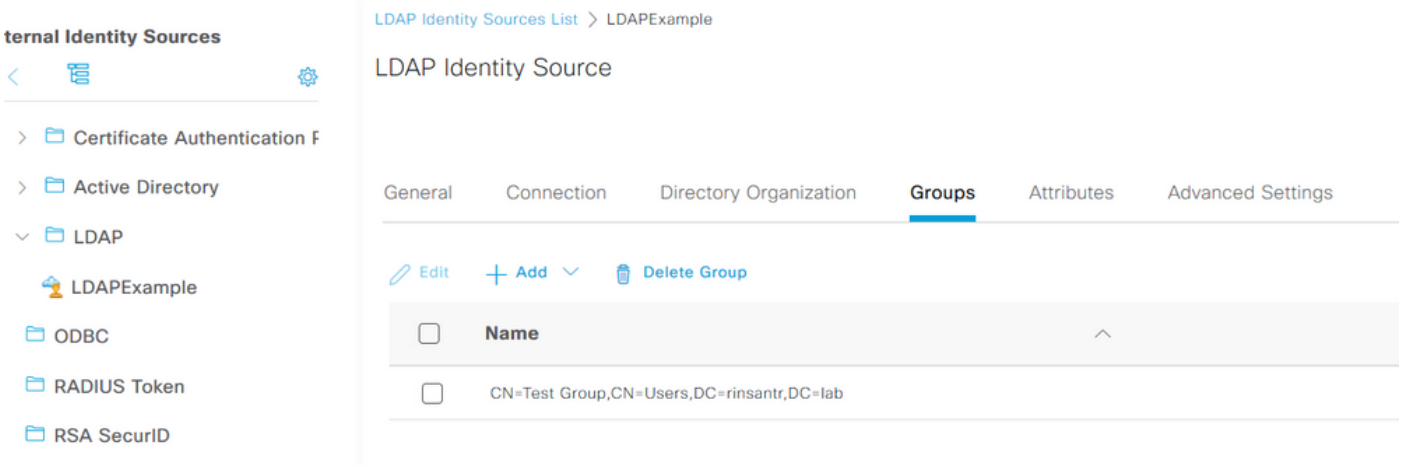


Click on **Test Bind to Server** under the **Connection** tab to test the reachability of the LDAP server from ISE.



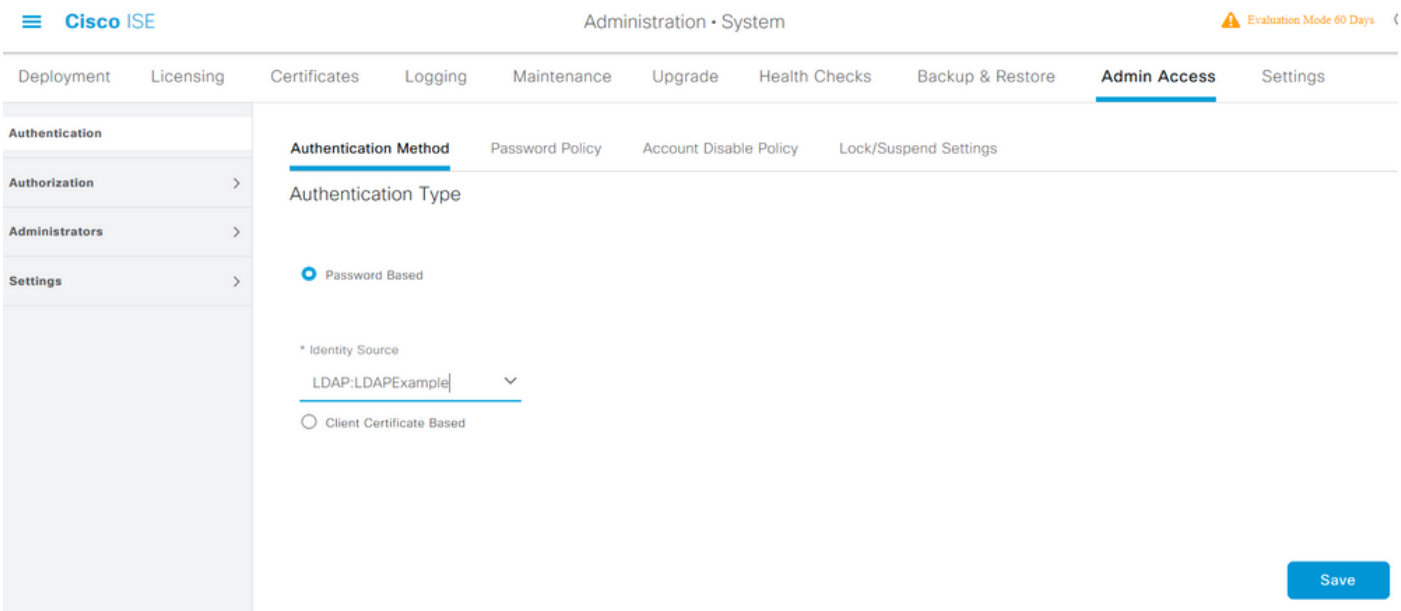
Now navigate to the **Groups** tab and click **Add > Select Groups From Directory > Retrieve Groups**. Import at least one group to which your administrator belongs, and click **OK**, then click **Save**.





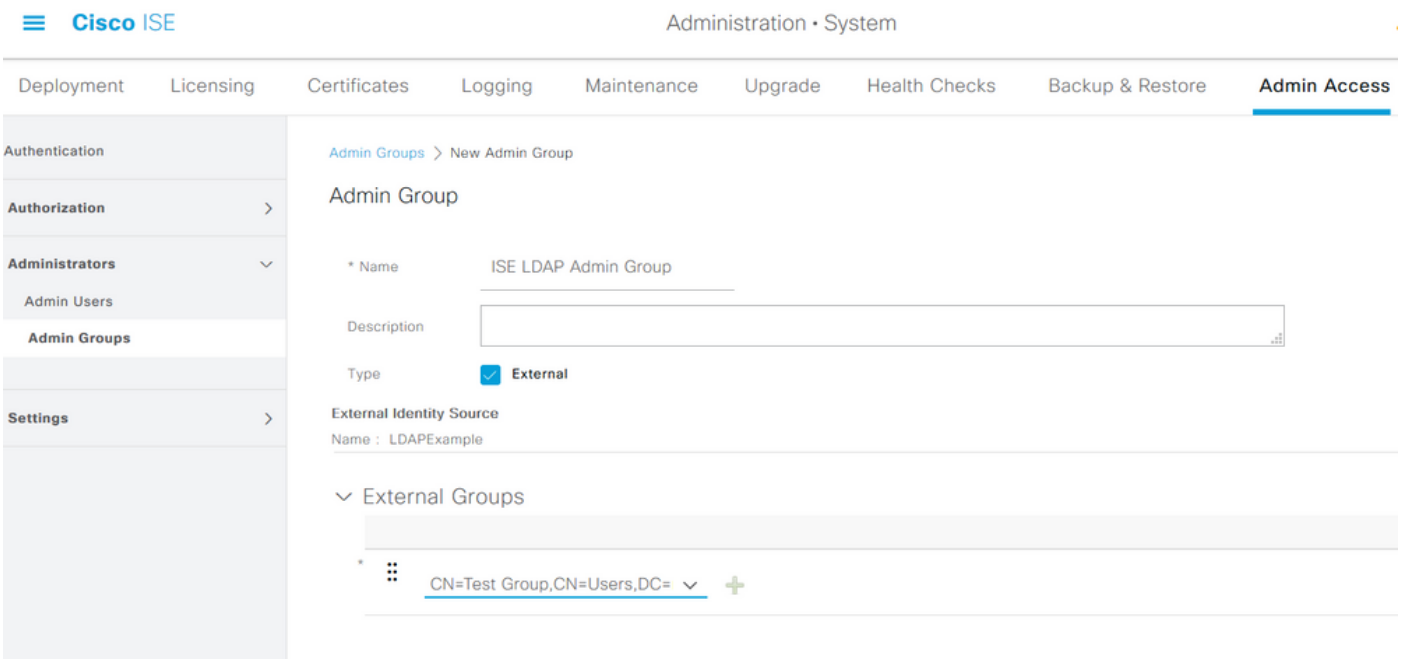
Enable Administrative Access for LDAP Users

In order to enable password-based authentication of ISE using LDAP, navigate to **Administration> System > Admin Access > Authentication**. In the **Authentication Method** tab, select the **Password-Based** option. Select **LDAP** from the **Identity Source** drop-down menu and Click **Save**.



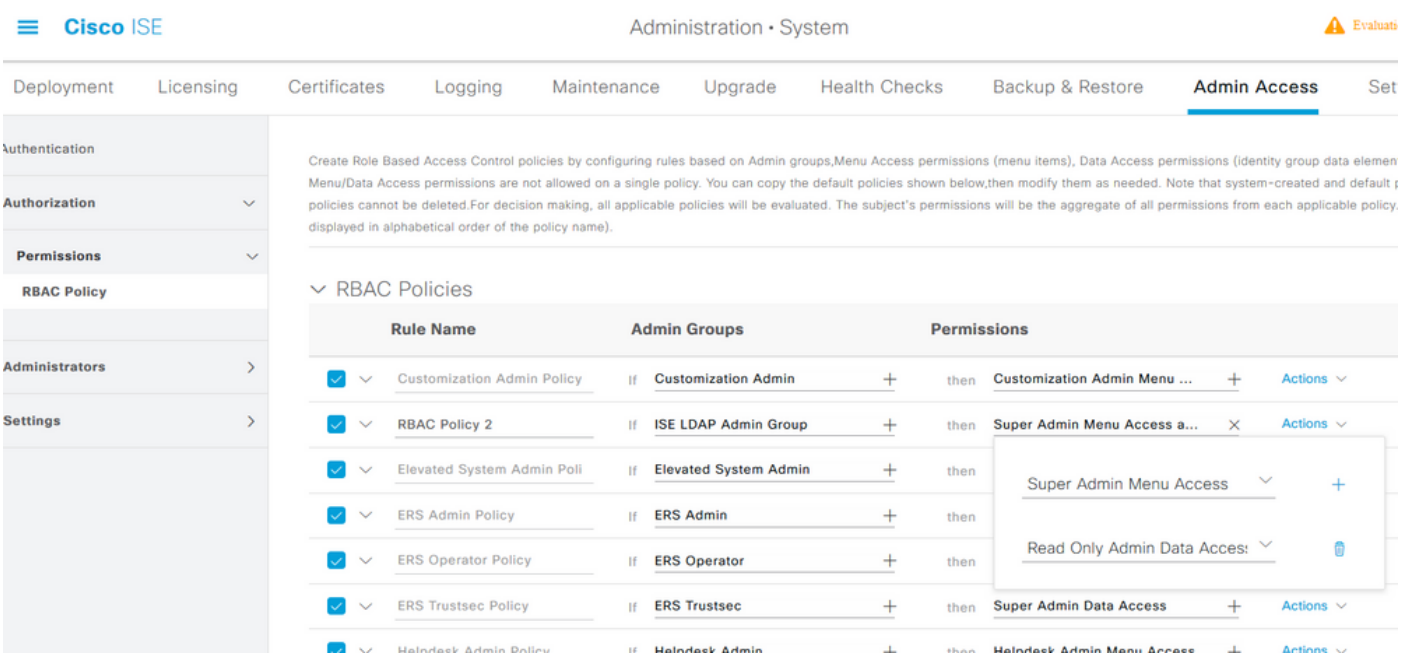
Map the ISE Admin Group to LDAP Group

This allows the configured user to get Administrator access based on the authorization of the RBAC policies, which in turn is based on the LDAP group membership of the user. To define a Cisco ISE Admin Group and map it to an LDAP group, navigate to **Administration > System > Admin Access > Administrators > Admin Groups**. Click **Add** and enter a name for the new Admin group. In the Type field, check the **External** check box. From the **External Groups** drop-down menu, select the LDAP group to which this Admin Group is to mapped (as retrived and defined previously). **Submit** the changes.



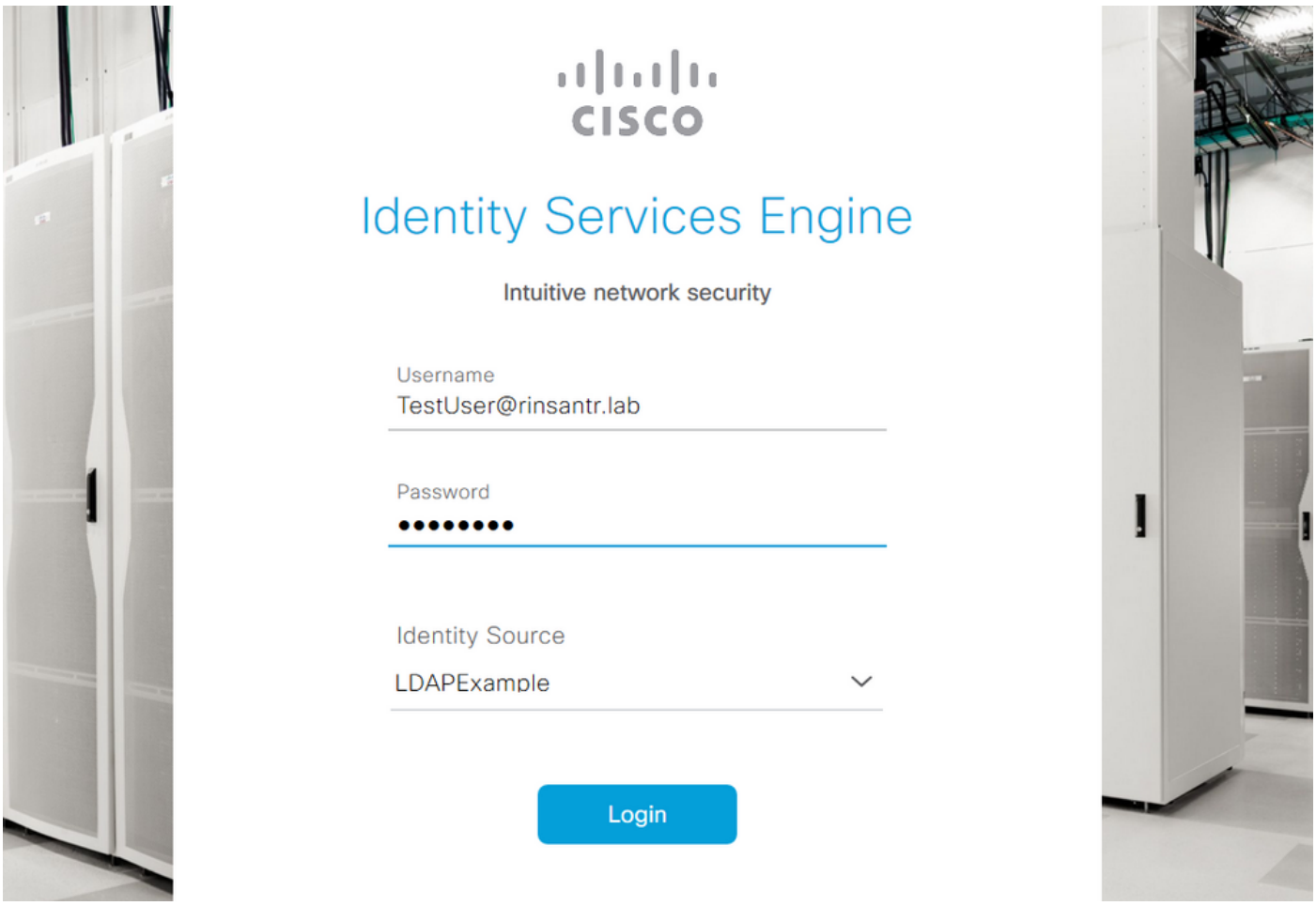
Set RBAC Permissions for the Admin Group

To assign RBAC permissions to the Admin Group created in the previous section, navigate to **Administration > System > Admin Access > Authorization > RBAC Policy**. From the **Actions** drop-down menu on the right, select **Insert new policy**. Create a new rule, map it with the Admin Group defined in the above section, and assign it with desired data and menu access permissions, then click **Save**.

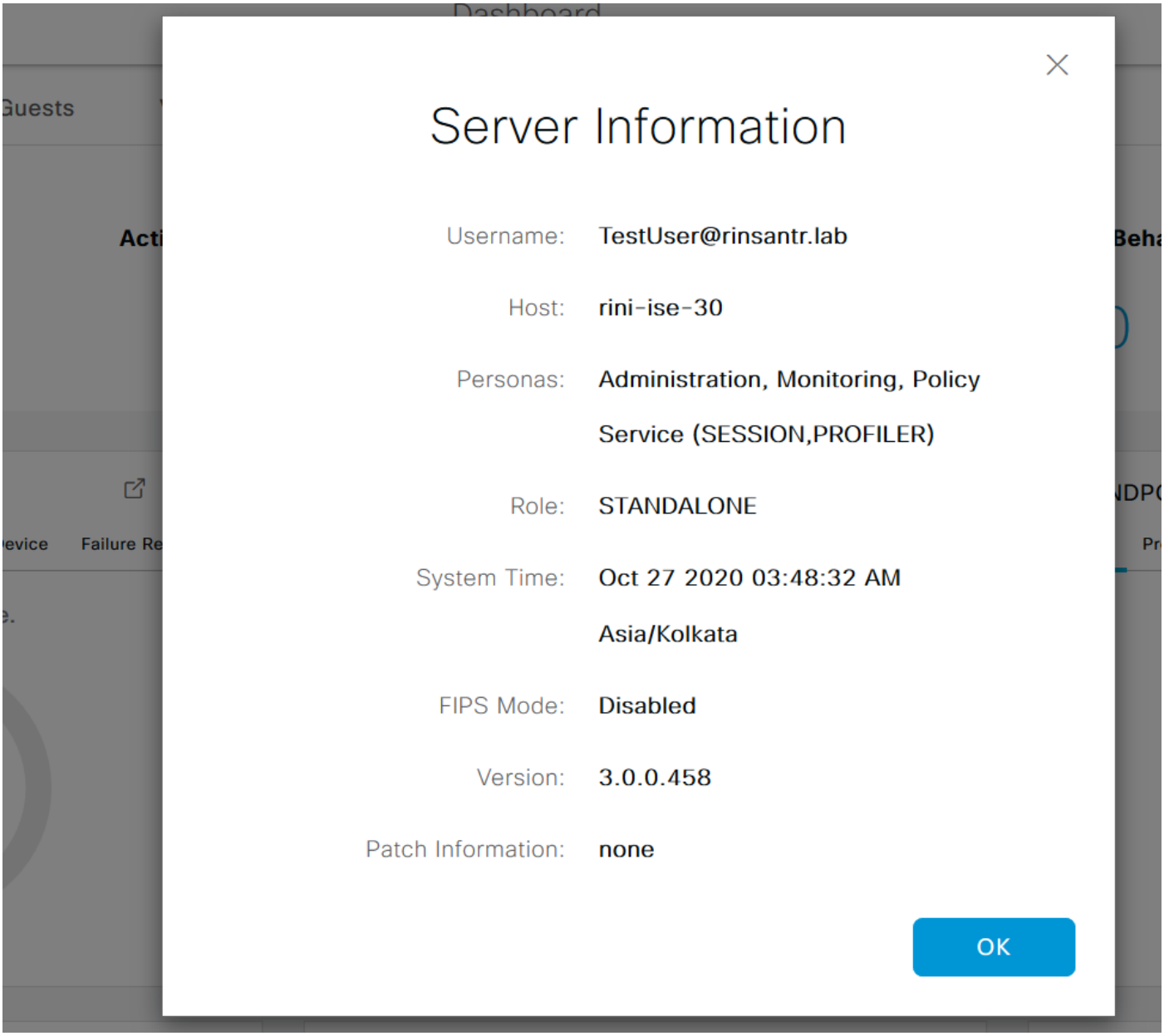


Access ISE with LDAP Credentials and Verify

Log out of the administrative GUI. Select the LDAP name from the **Identity Source** drop-down menu. Enter the username and password from the LDAP database, and log in.



In order to confirm that the configuration works properly, verify the authenticated username from the **Settings** icon on the top right corner of the ISE GUI. Navigate to **Server Information** and verify the Username.


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