

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 the prrt-server.log](#)

[Verify these-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.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes the Cisco ISE logo, the current page title 'Administration - Identity Management', and an 'Evaluation' warning icon. Below the navigation bar, there are tabs for 'Identities', 'Groups', 'External Identity Sources' (which is selected), 'Identity Source Sequences', and 'Settings'. On the left side, there is a sidebar menu for 'External Identity Sources' with various categories like Certificate Authentication F, Active Directory, LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, and Social Login. The main content area shows the configuration for an 'LDAP Identity Source' named 'LDAP_Server'. The 'General' tab is selected, and the configuration fields are as follows:

Field	Value
* Name	LDAP_Server
Description	
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 .

Cisco ISE Administration - Identity Management Evaluation Mode 64 Days

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 .

Cisco ISE Administration - Identity Management

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 top navigation bar includes 'Administration - System' and a warning for 'Evaluation Mode 64 Days'. The main menu has tabs for 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The 'Admin Access' tab is selected. On the left, a sidebar menu shows 'Authentication', 'Authorization', 'Administrators', and 'Settings'. The main content area is titled 'Authentication Method' and includes sub-sections for 'Password Policy', 'Account Disable Policy', and 'Lock/Suspend Settings'. Under 'Authentication Type', the 'Password Based' option is selected. Below this, there is a field for '* Identity Source' with a dropdown menu currently showing 'LDAP:LDAP_Server'. There is also an unselected radio button for 'Client Certificate Based'. At the bottom right, there are 'Save' and 'Reset' buttons.

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 for configuring an Admin Group. The top navigation bar is the same as in the previous screenshot. The main menu has 'Admin Access' selected. The left sidebar menu shows 'Admin Groups' selected. The main content area is titled 'Admin Groups > LDAP_User_Group' and 'Admin Group'. It contains the following fields and sections:

- * Name: LDAP_User_Group
- Description: (empty text box)
- Type: External
- External Identity Source Name: LDAP_Server
- External Groups: A section with a dropdown menu showing 'CN=employee,CN=Users,DC=a' and a plus sign to add more groups.
- Member Users: A section with 'Users' and '+ Add' and 'Delete' buttons.
- A table with columns: Status, Email, Username, First Name, Last Name. Below the table, it says '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. 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**.

The screenshot shows the Cisco ISE Administration interface for the 'System' section. The left sidebar contains a navigation menu with 'Menu Access' selected under the 'Permissions' section. 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 is visible, showing a tree view of the 'ISE Navigation Structure' with options 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 a navigation menu with 'Data Access' selected under the 'Permissions' section. 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 is visible, showing a tree view of the 'Data Access Privileges' with options 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**.
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.

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... × 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 ▾

 **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:

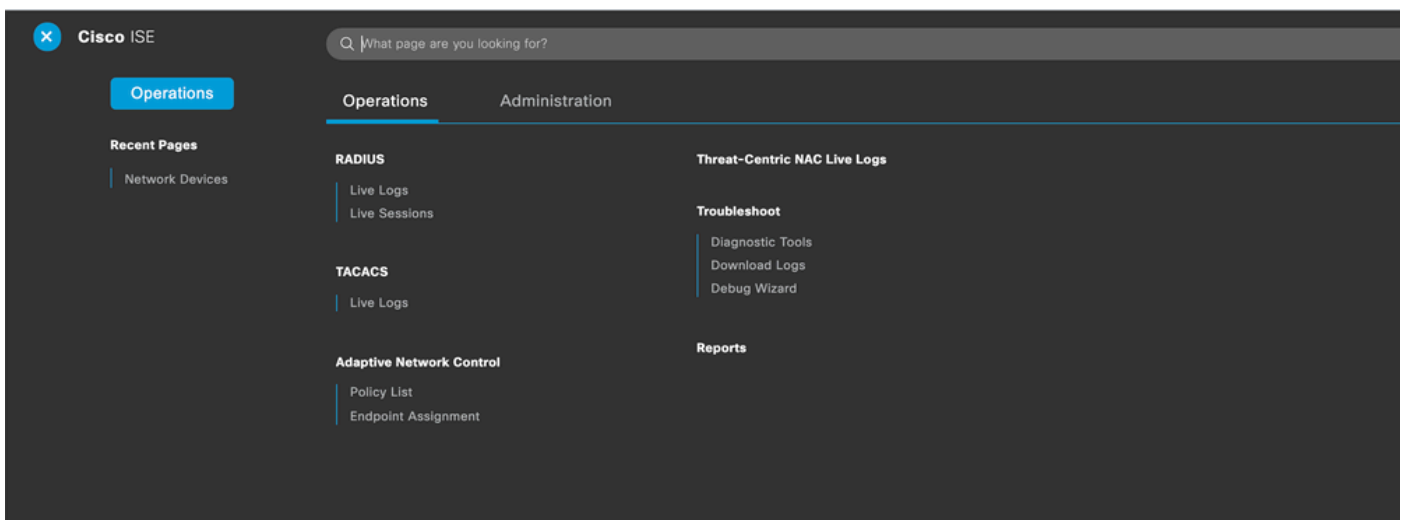
1. Open ISE GUI to log in with the LDAP user.
2. Select LDAP_Server from the **Identity Source** drop-down menu.
3. Enter the UPN and password from the LDAP database, and log in.



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

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@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

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

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, Username, and Content. Below the table, three callout boxes provide context:

- Bind Request and response using LDAP for the administrator.** Points to packets 140 and 88.
- Search request and response Entry for the username to the mapped LDAP group.** Points to packets 191 and 475.
- Bind success for the username search** Points to packets 127 and 88.

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=anshshih,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=anshshih,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=anshshih,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=anshshih,DC=local" simple
1049	2028-09-30 01:21:13.352089	10.127.197.188	10.106.32.184	LDAP	88		bindResponse(1) success
15320	2028-09-30 01:21:40.968108	10.106.32.184	10.127.197.188	LDAP	191		searchRequest(3) "dc=anshshih,dc=local" wholeSubtree
15325	2028-09-30 01:21:40.968845	10.127.197.188	10.106.32.184	LDAP	475		searchResEntry(3) "CN=admin2,CN=Users,DC=anshshih,DC=local" searchRes
15330	2028-09-30 01:21:40.969756	10.106.32.184	10.127.197.188	LDAP	127		bindRequest(2) "CN=admin2,CN=Users,DC=anshshih,DC=local" simple
15337	2028-09-30 01:21:40.971044	10.106.32.184	10.127.197.188	LDAP	88		bindResponse(2) success

Log Analysis

Verify the prrt-server.log

PAPAAuthenticator,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,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
```