

# 基于ISE角色的LDAP访问控制

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[配置](#)

[将ISE加入LDAP](#)

[为LDAP用户启用管理访问](#)

[将管理组映射到LDAP组](#)

[设置菜单访问权限](#)

[设置数据访问权限](#)

[为管理员组设置RBAC权限](#)

[验证](#)

[使用AD凭证访问ISE](#)

[故障排除](#)

[一般信息](#)

[数据包捕获分析](#)

[日志分析](#)

[检验prrt-server.log](#)

[验证ise-psc.log](#)

## 简介

本文档介绍将轻量级目录访问协议(LDAP)用作外部身份库以管理访问思科身份服务引擎(ISE)管理GUI的配置示例。

## 先决条件

Cisco 建议您了解以下主题：

- 思科ISE版本3.0的配置
- LDAP ( 轻量级目录访问协议 )

## 要求

本文档中的信息基于以下软件和硬件版本：

- 思科ISE版本3.0
- Windows Server 2016

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始 ( 默认 ) 配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

# 配置

使用以下部分配置基于LDAP的用户，以获得对ISE GUI的基于管理/自定义的访问。以下配置使用LDAP协议查询从Active Directory获取用户以执行身份验证。

## 将ISE加入LDAP

1. 导航至**管理>身份管理>外部身份源> Active Directory > LDAP**。
2. 在**General**选项卡下，输入LDAP的名称并选择架构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 "External Identity Sources" sidebar is visible on the left, with "LDAP" selected. The main content area shows the configuration for the "LDAP Identity Source" with the "General" tab active. The configuration fields are as follows:

Field	Value
* Name	LDAP_Server
Description	
Schema	Active Directory

## 配置连接类型和LDAP配置

1. 导航至**ISE >管理>身份管理>外部身份源> LDAP**。
2. 配置主LDAP服务器的主机名以及端口389(LDAP)/636(LDAP-Secure)。
3. 输入管理员可分辨名称(DN)的路径和LDAP服务器的管理员密码。
4. 点击Test Bind Server以测试ISE中LDAP服务器的可达性。

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

Enable Secondary Server

Specify server for each ISE node

Access  Anonymous Access  Authenticated Access

Admin DN \* cn=Administrator,cn=Users,dc=

Password \* .....

## 配置目录组织、组和属性

1. 根据LDAP服务器中存储的用户的层次结构选择用户的正确组织组。

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

## 为LDAP用户启用管理访问

要启用基于密码的身份验证，请完成以下步骤。

1. 导航至ISE > Administration > System > Admin Access > Authentication。
2. 在Authentication Method选项卡下，选择Password-Based选项。
3. 从“身份源”下拉菜单中选择LDAP。
4. 点击Save Changes。

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Cisco ISE', 'Administration - System', and a warning for 'Evaluation Mode 64 Days'. The main navigation menu has 'Admin Access' selected. On the left, a sidebar lists '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', 'Password Based' is selected. The 'Identity Source' is set to 'LDAP:LDAP\_Server', and 'Client Certificate Based' is unselected. 'Save' and 'Reset' buttons are at the bottom right.

## 将管理组映射到LDAP组

在ISE上配置管理组并将其映射到AD组。这允许已配置用户根据基于组成员资格的管理员已配置的RBAC权限，根据授权策略获取访问权限。

The screenshot shows the Cisco ISE Administration interface for configuring an Admin Group. The top navigation bar is the same as the previous screenshot. The main navigation menu has 'Admin Access' selected. The left sidebar shows 'Admin Groups' selected. The main content area is titled 'Admin Group' and shows the configuration for 'LDAP\_User\_Group'. The 'Name' field contains 'LDAP\_User\_Group'. The 'Type' is set to 'External'. The 'External Identity Source' is 'LDAP\_Server'. Under 'External Groups', a group 'CN=employee,CN=Users,DC=a' is listed. The 'Member Users' section is empty, showing 'No data available'.

## 设置菜单访问权限

1. 导航至ISE > 管理 > 系统 > 授权 > 权限 > 菜单访问

2. 定义管理员用户访问ISE GUI的菜单访问权限。我们可以配置要在GUI上显示或隐藏的子实体，以使用户在需要时仅执行一组操作时进行自定义访问。

3. 单击“保存”。

The screenshot shows the Cisco ISE Admin Access configuration page for editing a Menu Access Permission. The breadcrumb is "Menu Access List > LDAP\_Menu\_Access". The page title is "Edit Menu Access Permission". The "Name" field is "LDAP\_Menu\_Access" and the "Description" field is empty. Below, the "Menu Access Privileges" section shows 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, "Permissions for Menu Access" has the "Show" radio button selected and the "Hide" radio button unselected.

## 设置数据访问权限

1. 导航至ISE > Administration > System > Authorization > Permissions > Data access
2. 定义管理员用户对ISE GUI上的身份组具有完全访问权限或只读访问权限的数据访问权限。
3. 单击“保存”。

The screenshot shows the Cisco ISE Admin Access configuration page for editing a Data Access Permission. The breadcrumb is "Data Access List > LDAP\_Data\_Access". The page title is "Edit Data Access Permission". The "Name" field is "LDAP\_Data\_Access" and the "Description" field is empty. Below, the "Data Access Privileges" section shows a tree view of the ISE Navigation Structure with the following items: Admin Groups, User Identity Groups, Endpoint Identity Groups, and Network Device Groups. To the right, "Permissions for Data Access" has the "Full Access" radio button selected, and the "Read Only Access" and "No Access" radio buttons unselected.

## 为管理员组设置RBAC权限

1. 导航至ISE > Administration > System > Admin Access > Authorization > Policy。
2. 从右侧的“操作”下拉菜单中，选择Insert New Policy Below 以添加新策略。
3. 创建名为LDAP\_RBAC\_policy的新规则，并将其与在“启用AD的管理访问”部分中定义的管理组

进行映射，并为其分配菜单访问和数据访问权限。

4. 单击**Save Changes**,GUI右下角将显示保存的更改的确认。

The screenshot shows the Cisco ISE Administration console interface. The top navigation bar includes tabs for Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access (selected), and Settings. The left sidebar contains a navigation menu with categories: Authentication, Authorization, Permissions (Menu Access, Data Access, RBAC Policy), Administrators, and Settings. The main content area displays 'RBAC Policies' with a table of existing policies and a modal window for editing the 'LDAP\_RBAC\_Rule' policy.

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).

Rule Name	Admin Groups	Permissions
Customization Admin Policy	Customization Admin	Customization Admin Menu ...
Elevated System Admin Poli	Elevated System Admin	System Admin Menu Access...
ERS Admin Policy	ERS Admin	Super Admin Data Access
ERS Operator Policy	ERS Operator	Super Admin Data Access
ERS Trustsec Policy	ERS Trustsec	Super Admin Data Access
Helpdesk Admin Policy	Helpdesk Admin	Helpdesk Admin Menu Access
Identity Admin Policy	Identity Admin	Identity Admin Menu Access...
LDAP_RBAC_Rule	LDAP_User_Group	LDAP_Menu_Access and L...
MnT Admin Policy	MnT Admin	
Network Device Policy	Network Device Admin	
Policy Admin Policy	Policy Admin	
RBAC Admin Policy	RBAC Admin	RBAC Admin Menu Access ...

The modal window for 'LDAP\_RBAC\_Rule' shows a dropdown menu with 'LDAP\_Menu\_Access' and 'LDAP\_Data\_Access' options, each with a plus sign to add it to the policy's permissions.

## 验证

### 使用AD凭证访问ISE

要使用AD凭证访问ISE，请完成以下步骤：

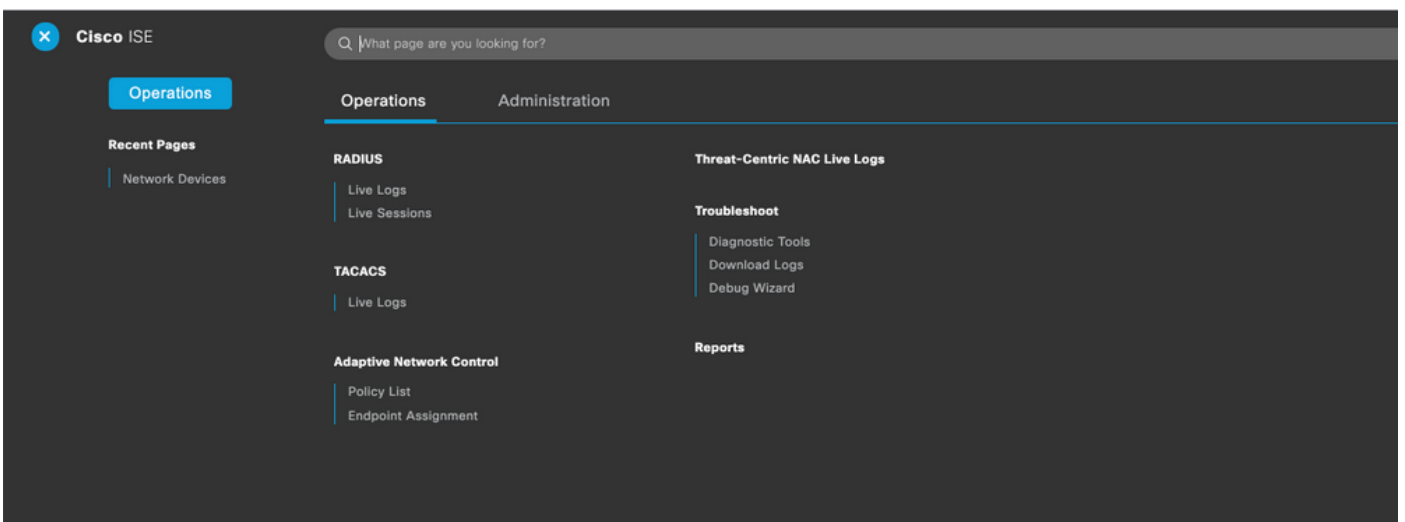
1. 打开ISE GUI以使用LDAP用户登录。
2. 从Identity Source下拉菜单中选择**LDAP\_Server**。
3. 从LDAP数据库输入用户名和密码，然后登录。



在审核报告中验证管理员登录的登录。导航至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

要确认此配置工作正常，请在ISE GUI右上角验证经过身份验证的用户名。定义基于自定义的访问权限，该权限对菜单的访问受限，如下所示：



## 故障排除

## 一般信息

要排除RBAC进程故障，必须在ISE管理节点的调试中启用这些ISE组件：

RBAC — 当我们尝试登录时(ise-psc.log)，此操作将打印RBAC相关消息

access-filter — 将打印资源过滤器访问(ise-psc.log)

runtime-AAA — 这将打印登录和LDAP交互消息的日志(prrt-server.log)

## 数据包捕获分析

The image shows a Wireshark capture of LDAP traffic. A table at the top lists packets with columns for No., Time, Source, Destination, Protocol, Length, Username, and Content. Three packets are highlighted in yellow: packet 1843 (bindRequest), packet 1844 (searchRequest), and packet 1848 (bindRequest). Callout boxes provide context: 'Bind Request and response using LDAP for the administrator.' points to packet 1843; 'Search request and response Entry for the username to the mapped LDAP group.' points to packet 1844; and 'Bind success for the username search' points to packet 1848. The packet details pane on the right shows the structure of these LDAP messages, including bindRequest, searchRequest, searchResEntry, and bindResponse.

## 日志分析

### 检验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
```

## 验证ise-psc.log

从这些日志中，您可以验证在尝试访问网络设备资源时用于admin2用户的RBAC策略 —

```
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
```