

# ISE رودىل دن تسملا لوصولا في مكحتلا LDAP مادختساب

## تايوت حمل

[عمدق م](#)

[سياس الابلط م](#)

[تابلط م](#)

[تانيوك ت](#)

[LDAP لىل ISE مامض ن](#)

[LDAP مدمختسم ليرادال لوصولا نيكم ت](#)

[LDAP عمومج لىل قرادال عمومج نيي عت](#)

[عمئاق لىل لوصول تانوذ نيي عت](#)

[تانايبل لىل لوصول تانوذ نيي عت](#)

[قرادال عمومج ل RBAC تانوذ نيي عت](#)

[حصلا نم ققحت ل](#)

[AD دامتعا تانايبل مادختساب ISE لىل لوصول](#)

[اهجالص او عاطخال افاشكتسا](#)

[عماع تامول عم](#)

[عمزحل طاق ت ل ليلحت](#)

[لجسل ل ليلحت](#)

[prmt-server.log حص نم ققحت ل](#)

[ise-psc.log ل تقود](#)

## عمدق م

في (LDAP) ليلدل لىل لوصول لوكوتورب مادختسال نيوكتلل الاثم دن تسملا اذه فصي (GUI) عموسرلا مدمختسملا هجاو لىل يرادال لوصول ليجراخ عموه نزمك Lightweight عضولا Cisco نم عموهلا تامدخ كرحم قرادال

## سياس الابلط م

عمئالاتل عيضاوملاب عمفرعم كي دل نوكت نأب Cisco يصوت

- 3.0 رادصلال، Cisco ISE نيوكت
- (ليلدل لوصول ل في فخال لوكوتورب ل) LDAP

## تابلط م

عمئالاتل عمدملا تانوكملاو جماربل تارادصل لىل دن تسملا اذه في عمراول تامول عملا دن تست

- Cisco نم 3.0 رادصلال ISE
- Windows Server 2016 لىل عمشتل ماطن

عمصاخ عملمعم عمئب في عموجوملا زمجال نم دن تسملا اذه في عمراول تامول عملا عمشن م



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

Enable Secondary Server

\* Hostname/IP 10.127.197.180  ⓘ Hostname/IP  ⓘ

\* Port 389  Port 389

Specify server for each ISE node

Access  Anonymous Access  Authenticated Access Access  Anonymous Access  Authenticated Access

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

Password \* ..... Password

## تامس ل او تاعومجمل او ليلدل اسسؤم نيوكت

يلك يهل لسلسلت الى اذانتسا مدختسملل ءح يوصل اسسؤم ل ءومجم رتخأ .  
LDAP م داخ ي ف ني نزم ل ني مدختسملل

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 **Directory Organization** Connection Groups Attributes Advanced Settings

\* Subject Search Base dc=anshsinh,dc=local   ⓘ

\* Group Search Base dc=anshsinh,dc=local   ⓘ

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

## LDAP ي مدختسمل ي رادل ل ووصل ني كمت

رورم ل ءم لك الى ءدنتسمل ءق داصم ل ني كمتل تاوطل ل هءه لمكأ

1. ءق داصم ل > لوؤسمل الى ل ووصل > ماظنل > ءرادل ل > ISE الى ل لقتنا .
2. رورم ل ءم لك الى ءدنتسمل رايل دح ، ءق داصم ل بولسأ بيوبتل ءم ال ءحت .
3. ءي وهل رءصم ءلدسنم ل ءمائل ل نم LDAP دح .
4. تاريغتال ظفح قوف رقنا .

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration - System' and 'Evaluation Mode 64 Days'. The main navigation tabs are '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-tabs for 'Password Policy', 'Account Disable Policy', and 'Lock/Suspend Settings'. The 'Authentication Type' is 'Password Based'. Below this, there is a section for 'Identity Source' with a dropdown menu set to 'LDAP:LDAP\_Server' and a radio button for 'Client Certificate Based'. At the bottom right, there are 'Save' and 'Reset' buttons.

## LDAP ةومجم ىل ةرادال ةومجم نييعة

مدختسملل حمسي اذهو AD ةومجم ىل اهنبييعة تب مقو ISE ىل ةرادال ةومجم نييعة تب مق متي تال RBAC تانوذأ ىل ةانب ليوختال تاسايس ىل ةانب لوصولاب هنيوكت متي ذل ةومجم ل ةيوضع ىل اذانتسا لوؤسملل اهنبيوكت.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration - System' and 'Evaluation Mode 64 Days'. The main navigation tabs are '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 'Admin Group' and includes sub-tabs for 'Admin Groups' and 'LDAP\_User\_Group'. The 'Name' is 'LDAP\_User\_Group'. The 'Description' is empty. The 'Type' is 'External'. The 'External Identity Source' is 'LDAP\_Server'. Below this, there is a section for 'External Groups' with a dropdown menu set to 'CN=employee,CN=Users,DC=a'. There is a 'Member Users' section with 'Add' and 'Delete' buttons and a table with columns 'Status', 'Email', 'Username', 'First Name', and 'Last Name'. The table is empty with 'No data available'.

## ةمئاقلا ىل لوصول تانوذأ نييعة

1. ةمئاقلا ىل لوصول > تانوذأ > ليوختال > ماظنلا > ةرادال > ISE ىل لقتنا.

2. ةيموسرلا مدختسملل ةهجاو ىل لوصول لوؤسملل ةمئاقلا لوصول ديذحت تب مق. مدختسملل ةهجاو ىل ةافخا واهضرع متيل ةيعةرفال تانايكلال نيوكت اننكمي. ISE ل (GUI) مزل اذا طقف تايلمعال نم ةومجم ةارجال مدختسملل صصخملل لوصول (GUI) ةيموسرلا رمال.



2. ديدج جهن ةفاضال هاندأ ديدج جهن چاردإ ددح، نيميللا ىلع تاءارجإ ةلدسننملا ةمئاقلا نم.
  3. ةرادإلا ةعومجم عم اهطيطختب مقو LDAP\_RBAC\_POLICY ىمست ةديج ةدعاق ءاشناب مق ىلإ لوصولل اهل تانوذأ نيينعتب مقو، ل يرادإلا لوصولل نيكمت مسق يف ةفرعمل تانايبلا ىلإ لوصولل ةمئاقلا.
  4. ةيوازلا يف ةظوفحملل تارييغتلل ديكأت ضرع متي و، تارييغتلل ظفح قوف رونا.
- ةيموسرلا مدختسملل ةهجاو نم ىنمىللا ىلفلل

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
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	LDAP_Menu_Access
Network Device Policy	Network Device Admin	LDAP_Data_Access
Policy Admin Policy	Policy Admin	
RBAC Admin Policy	RBAC Admin	RBAC Admin Menu Access ...

## ةحصللا نم ققحتلا

### AD دامتعا تانايب مادختساب ISE ىلإ لوصولل

AD تاغوسم مادختساب ISE ىلإ لوصولل ةيلتلا تاوطخل لمكأ:

1. LDAP مدختسم مادختساب لوخدلا ليچستل ISE (GUI) ةيموسرلا مدختسملل ةهجاوحتفا.
2. ةيوهل رصم ةلدسننملا ةمئاقلا نم LDAP\_Server ددح.
3. لوخدلا لچسو، LDAP تانايب ةدعاق نم رورملا ةمك و مدختسملل مسالخدأ.



> تاي لم عمل > ISE الى لقتنا. قي قددتلا ريراقت يف لوؤس ملل لوخذلا ليچست نم ققحت  
 ني لوؤس ملل لوخذ ليچست تاي لم عمل > قي قددتلا > ريراقتلا

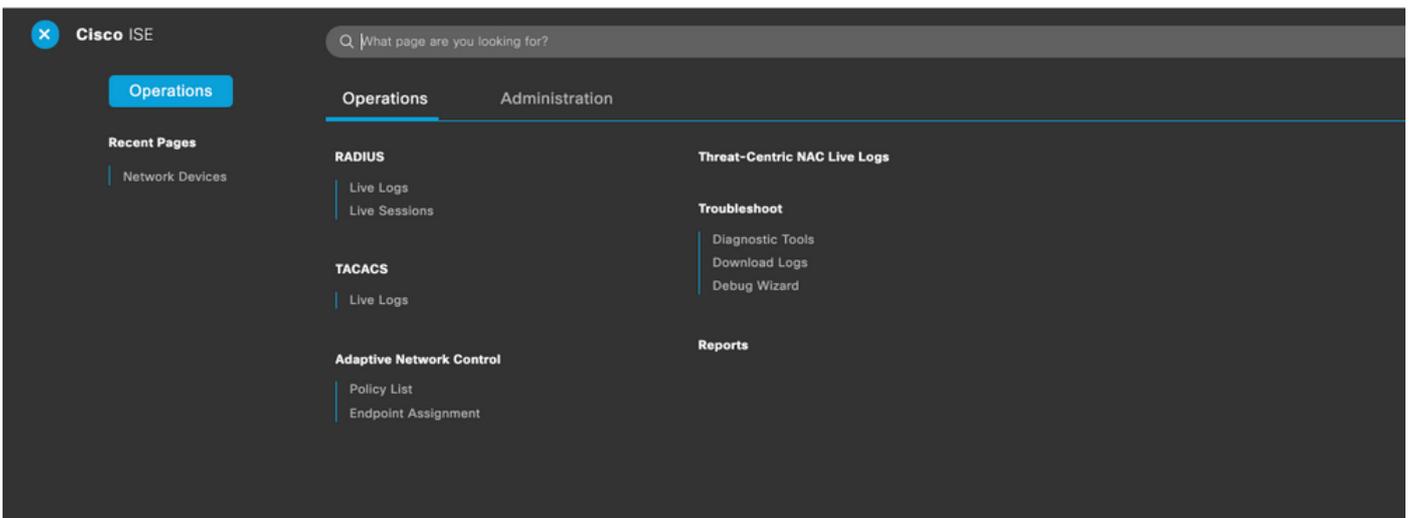
Cisco ISE Operations - Reports Evaluation Mode 64 Days

### Administrator Logins

From 2020-10-10 00:00:00.0 To 2020-10-10 10:58:13.0  
 Reports exported in last 7 days 0

Logged At	Administrator	IP Address	Server	Event	Event Details
Today	Administrator		Server		
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

تمت يذلا مدختس ملل مسا نم ققحت، حيحص لكشب لمعي نيوكتلا اذه نأ نم دكأتلل  
 ديحتب مق (ISE) ةيموسرلا مدختس ملل ةهجاو نم ينم يلا ايلعلا ةيوازلا يف هتقداصم  
 انه حضورم وه امك ةمئاقلا الى ةدودحم لووصو ةينكام الى دن تسي صصخم لووصو



# اهحال صإو عاطخأل فاشكتسا

## ةماع تامولعم

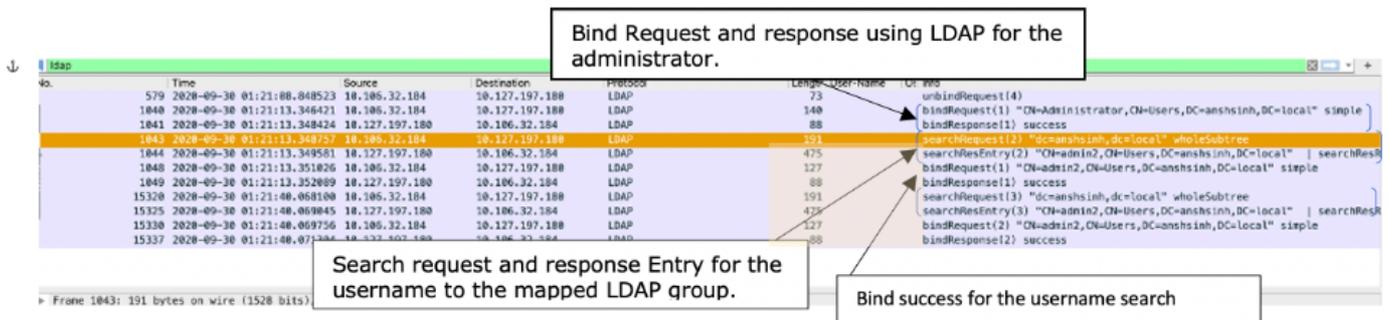
عاطخأل ححصت يف هذه ISE تانوكم نيكمت بجي ،اهحال صإو RBAC ةي لمع عاطخأ فاشكتسا ل ISE لوؤسم ةدقع ىلع :

RBAC ( ise-psc.log ) لوخدلا ليجست ةلواجم دنع RBAC ةلصللا تاذ ةلاس رللا ةعابطب اذه موقيس - RBAC

( ise-psc.log ) دراوملا ةيفصت لماع ىلإ لوصوللا ةعابطب اذه موقيس - filter لوصوللا

LDAP لعافات لئاسرو لوخدلا ليجستب ةصاخلا لالجسلا ةعابطب اذه موقيس - Runtime-AAA ( prrt-server.log )

## ةمزلحلا طاقنلا ليجلت



## لجسلا ليجلت

## prrt-server.log ةحص نم ققحتلا

```
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_9240qzxSbv_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
```

## دقيق ل ise-psc.log

دع admin2 مخدمتس ملل ةم دختس مل RBAC ةسايس نم ققحتل ك نكمي ،تال جسل هذه نم  
- ةكبشل زا هج دروم يل لوصول ةل واهج -

```
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
```

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت  
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او  
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل متهتبل ب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىلإ أمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقدنع اهتيلوئسم Cisco  
Systems (رفوتم طبارل) ي لصلأل يزي لچنل دن تسمل