

# Configureer ISE-rolgebaseerde toegangscontrole met lichtgewicht Directory Access Protocol

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Configuraties](#)

[Doe mee aan ISE naar LDAP](#)

[Administratieve toegang voor LDAP-gebruikers inschakelen](#)

[De Admin Group toewijzen aan LDAP Group](#)

[Rechten instellen voor menu-toegang](#)

[Rechten voor gegevenstoegang instellen](#)

[RBAC-toegangsrechten instellen voor de Admin-groep](#)

[Verifiëren](#)

[Toegang tot ISE met AD Credentials API](#)

[Problemen oplossen](#)

[Algemene informatie](#)

[Packet Capture Analysis](#)

[Analyse van logboeken](#)

[Controleer de rrt-server.log](#)

[Controleer theise-psc.log](#)

---

## Inleiding

Dit document beschrijft een configuratievoorbeeld voor het gebruik van het Lichtgewicht Directory Access Protocol (LDAP) als een extern identiteitsarchief voor administratieve toegang tot de Cisco Identity Services Engine (ISE)-beheerGUI.

## Voorwaarden

Cisco raadt kennis van de volgende onderwerpen aan:

- Configuratie van Cisco ISE-versies 3.0
- LDAP

## Vereisten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ISE versie 3.0
- Windows Server 2016

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Configuraties

Gebruik het vak om een op LDAP gebaseerde gebruiker te configureren voor toegang tot de ISE GUI op basis van beheer/aangepaste instellingen. In de onderstaande configuratie worden de LDAP-protocolvragen gebruikt om de gebruiker uit de Active Directory te halen voor het uitvoeren van de verificatie.

### Doe mee aan ISE naar LDAP

1. Ga naar Beheer > Identiteitsbeheer > Externe Identiteitsbronnen > Active Directory > LDAP.
2. Voer onder het tabblad Algemeen de naam van de LDAP in en kies het schema Active Directory.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb navigation is Administration > Identity Management. The main menu includes Identities, Groups, External Identity Sources (selected), Identity Source Sequences, and Settings. The left sidebar shows the External Identity Sources tree with folders for Certificate Authentication F, Active Directory, LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, and Social Login. The main content area displays the configuration for an LDAP Identity Source named 'LDAP\_Server'. The 'General' tab is active, showing fields for Name (LDAP\_Server), Description, and Schema (Active Directory).

### Verbindingstype en LDAP-configuratie configureren

1. Ga naar ISE > Administratie > Identiteitsbeheer > Externe identiteitsbronnen > LDAP.
2. Configureer de Hostname van de primaire LDAP-server samen met de poort 389(LDAP)/636 (LDAP-Secure).
3. Voer het pad in voor de Admin voornaam (DN) met het admin-wachtwoord voor de LDAP-server.
4. Klik op Test Bind Server om de bereikbaarheid van LDAP server van ISE te testen.

Cisco ISE Administration - Identity Management

External Identity Sources

Active Directory

Connection

Field	Primary Server	Secondary Server
* Hostname/IP	10.127.197.180	
* Port	389	389
Access	<input checked="" type="radio"/> Authenticated Access	<input type="radio"/> Authenticated Access
Admin DN	* cn=Administrator,cn=Users,dc=	
Password	* .....	

Specify server for each ISE node

Enable Secondary Server

De directoryorganisatie, groepen en kenmerken configureren

1. Kies de juiste organisatiegroep van de gebruiker op basis van de hiërarchie van gebruikers die zijn opgeslagen in de LDAP-server .

Cisco ISE Administration - Identity Management

External Identity Sources

LDAP

Directory Organization

\* 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

Administratieve toegang voor LDAP-gebruikers inschakelen

Voltooi deze stappen om op een wachtwoord gebaseerde verificatie in te schakelen.

1. Navigeer naar ISE > Administration > System > Admin Access > Verificatie.
2. Selecteer onder het tabblad Verificatiemethode de optie Wachtwoord gebaseerd.
3. Selecteer LDAP in het vervolgkeuzemenu Identity Source.
4. Klik op Wijzigingen opslaan.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Cisco ISE', 'Administration - System', and 'Evaluation Mode 64 Days'. The main navigation menu has 'Admin Access' selected. On the left, a sidebar contains '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'. There are 'Save' and 'Reset' buttons at the bottom right.

## De Admin Group toewijzen aan LDAP Group

Configureer de beheergroep op de ISE en wijs deze toe aan de AD-groep. Dit staat de gevormde gebruiker toe om toegang te krijgen die op het vergunningsbeleid wordt gebaseerd dat op de gevormde toestemmingen RBAC voor de beheerder op groepslidmaatschap wordt gebaseerd.

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 navigation menu has 'Admin Access' selected. The left sidebar has 'Admin Groups' selected. The main content area is titled 'Admin Group' and shows the configuration for 'LDAP\_User\_Group'. The 'Name' field is 'LDAP\_User\_Group'. The 'Type' is 'External'. The 'External Identity Source' is 'LDAP\_Server'. Under 'External Groups', a group is added with the name 'CN=employee,CN=Users,DC=a'. The 'Member Users' section is empty, showing a table with columns for 'Status', 'Email', 'Username', 'First Name', and 'Last Name'. There are '+ Add' and 'Delete' buttons above the table.

## Rechten instellen voor menutoegang

1. Navigeer naar ISE > Beheer > Systeem > autorisatie > Rechten > Menutoegang
2. Definieer de menutoegang voor de beheerder om toegang te krijgen tot de ISE GUI. U kunt de

subentiteiten die moeten worden weergegeven of verborgen op de GUI configureren voor aangepaste toegang voor een gebruiker om desgewenst alleen een set bewerkingen uit te voeren.

3. Klik op Opslaan.

The screenshot shows the Cisco ISE Administration console interface. The top navigation bar includes 'Administration · System' and a menu with options: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, **Admin Access**, and Settings. The left sidebar shows a navigation tree with 'Menu Access' selected. 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 list of 'ISE Navigation Structure' items: Operations, Policy, Administration, Work Centers, Wizard, Settings, Home, and Context Visibility. To the right of this list, under 'Permissions for Menu Access', there are two radio buttons: 'Show' (which is selected) and 'Hide'.

## Rechten voor gegevenstoegang instellen

1. Ga naar ISE > Beheer > Systeem > autorisatie > Rechten > Toegang tot gegevens.
2. Definieer de gegevenstoegang voor de beheerder om volledige toegang of alleen-lezen toegang te hebben tot de identiteitsgroepen op de ISE GUI.
3. Klik op Opslaan.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, **Admin Access**, and Settings. The left sidebar menu is expanded to show: Authentication, Authorization, Permissions, Menu Access, **Data Access**, RBAC Policy, Administrators, and Settings. The main content area displays the 'Edit Data Access Permission' page for 'LDAP\_Data\_Access'. The page title is 'Data Access List > LDAP\_Data\_Access'. The form fields are: '\* Name' (LDAP\_Data\_Access) and 'Description' (empty). Below the form is the 'Data Access Privileges' section, which includes a list of groups: Admin Groups, User Identity Groups, Endpoint Identity Groups, and Network Device Groups. To the right of this list are the 'Permissions for Data Access' options: Full Access (selected), Read Only Access, and No Access.

## RBAC-toegangsrechten instellen voor de Admin-groep

1. Blader naar ISE > Administration > System > Admin Access > Authorisation > Policy.
2. Selecteer in het vervolgkeuzemenu Acties rechts de optie Nieuw beleid invoegen om een nieuw beleid toe te voegen.
3. Maak een nieuwe regel met de naam LDAP\_RBAC\_policy en wijs deze toe met de Admin Group die is gedefinieerd in de sectie Administratieve toegang inschakelen voor AD en wijs deze toegangsrechten toe voor menu-toegang en gegevenstoegang.
4. Klik op Wijzigingen opslaan en bevestig als de opgeslagen wijzigingen in de rechterbenedenhoek van de GUI worden weergegeven.

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

 **Opmerking:** de super admin gebruiker kan het standaard systeem-gegenereerde RBAC beleid en de rechten niet wijzigen. Om dit te doen, moet u nieuwe RBAC-beleid maken met de nodige rechten op basis van uw behoeften, en dit beleid toewijzen aan een beheergroep.

 **Opmerking:** alleen een admin-gebruiker uit de standaard Super Admin Group kan andere admin-gebruikers wijzigen of verwijderen. Zelfs een extern toegewezen gebruiker die deel uitmaakt van een Admin-groep die is gekloond met de rechten Menu en Data Access van de Super Admin-groep kan een beheerder niet wijzigen of verwijderen.

## Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

### Toegang tot ISE met AD Credentials API

Voltooi de volgende stappen om toegang te krijgen tot ISE met AD-referenties:

1. Open ISE GUI om in te loggen met de LDAP-gebruiker.
2. Selecteer LDAP\_Server in het vervolgkeuzemenu Identity Source.
3. Voer het UPN en het wachtwoord in uit de LDAP-database en log in.



Controleer de login voor de beheerder logins in Auditrapporten. Blader naar ISE > Operations > Rapporten > Audit > Administrators Logins.

Cisco ISE Operations · Reports Evaluation Mode 64 Days

Administrator Logins My Reports Export To Schedule

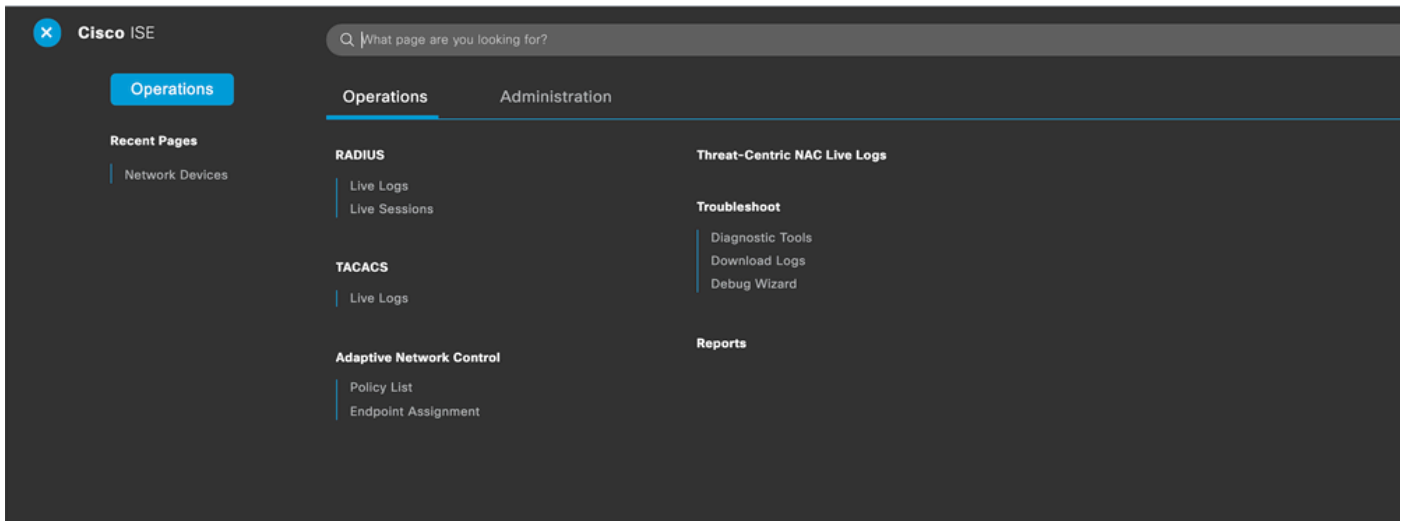
From 2020-10-10 00:00:00.0 To 2020-10-10 10:58:13.0  
Reports exported in last 7 days 0

Filter Refresh

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

Om te bevestigen dat deze configuratie correct werkt, verifieert u de geverifieerde gebruikersnaam rechtsboven in de ISE GUI. Definieer een op maat gebaseerde toegang die beperkte toegang tot het menu heeft zoals hier wordt getoond:





## Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

### Algemene informatie

Om problemen op te lossen tijdens het RBAC-proces, moeten deze ISE-componenten worden ingeschakeld in het debuggen op de ISE-beheerknoppunt:

RBAC - Dit drukt het RBAC-gerelateerde bericht af wanneer we proberen in te loggen (ise-psc.log)

access-filter - Hiermee wordt de toegang tot resourcefilters afgedrukt (ise-psc.log)

runtime-AAA - Hiermee worden de logbestanden voor login en LDAP-interfaceberichten afgedrukt (prt-server.log)

### Packet Capture Analysis

No.	Time	Source	Destination	Protocol	Length	User-Name	Ct. Info
579	2028-09-30 01:21:08.848523	10.106.32.184	10.127.197.188	LDAP	73		unbindRequest(4)
1840	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
1841	2028-09-30 01:21:13.348424	10.127.197.188	10.106.32.184	LDAP	88		bindResponse(1) success
1842	2028-09-30 01:21:13.348723	10.106.32.184	10.127.197.188	LDAP	171		searchRequest(1) "dc=anshshih,dc=local" wholesubtree
1844	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
1848	2028-09-30 01:21:13.351826	10.106.32.184	10.127.197.188	LDAP	127		bindRequest(1) "CN=admin2,CN=Users,DC=anshshih,DC=local" simple
1849	2028-09-30 01:21:13.352889	10.127.197.188	10.106.32.184	LDAP	88		bindResponse(1) success
15320	2028-09-30 01:21:40.068100	10.106.32.184	10.127.197.188	LDAP	191		searchRequest(3) "dc=anshshih,dc=local" wholesubtree
15325	2028-09-30 01:21:40.069045	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 01:21:40.069756	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 01:21:40.071884	10.127.197.188	10.106.32.184	LDAP	88		bindResponse(2) success

### Analyse van logboeken

Controleer de prt-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

Controleer het bestand ise-psc.log

Van deze logbestanden kunt u het RBAC-beleid controleren dat wordt gebruikt voor de admin2-gebruiker wanneer wordt geprobeerd om toegang te krijgen tot de netwerkapparaatbron.

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

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.