

Control de acceso basado en roles ISE con LDAP

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Configuraciones](#)

[Unir ISE a LDAP](#)

[Habilitar acceso administrativo para usuarios LDAP](#)

[Asigne el Grupo Admin al Grupo LDAP](#)

[Establecer permisos para acceso a menús](#)

[Establecer permisos para acceso a datos](#)

[Establecer permisos RBAC para el grupo de administradores](#)

[Verificación](#)

[Acceso a ISE con credenciales AD](#)

[Troubleshoot](#)

[Información general](#)

[Análisis de captura de paquetes](#)

[Análisis de registro](#)

[Verifique el prrt-server.log](#)

[Verifique el ise-psc.log](#)

Introducción

Este documento describe un ejemplo de configuración para el uso del protocolo ligero de acceso a directorios (LDAP) como almacén de identidad externo para el acceso administrativo a la GUI de administración de Cisco Identity Services Engine (ISE).

Prerequisites

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de las versiones 3.0 de Cisco ISE
- LDAP (protocolo ligero de acceso a directorios)

Requirements

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ISE versión 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.

Configuraciones

Utilice la siguiente sección para configurar un usuario basado en LDAP para obtener el acceso administrativo/personalizado basado en la GUI de ISE . La siguiente configuración utiliza las consultas del protocolo LDAP para obtener al usuario del directorio activo para realizar la autenticación.

Unir ISE a LDAP

1. Vaya a **Administration > Identity Management > External Identity Sources > Active Directory > LDAP**.
2. Bajo la ficha **General**, ingrese el nombre del LDAP y elija el esquema 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", "Identity Source Sequences", and "Settings". The "External Identity Sources" section is expanded, showing a list of source types: Certificate Authentication F, Active Directory, LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, and Social Login. The "LDAP" option is selected, leading to the "LDAP Identity Sources List" page. The specific configuration page for "LDAP_Server" is shown, with the "LDAP Identity Source" title. The "General" tab is active, displaying the following fields: "Name" (LDAP_Server), "Description" (empty), and "Schema" (Active Directory). Other tabs include "Connection", "Directory Organization", "Groups", "Attributes", and "Advanced Settings".

Configurar el tipo de conexión y la configuración LDAP

1. Vaya a **ISE > Administration > Identity Management > External Identity Sources > LDAP**.
2. Configure el nombre de host del servidor LDAP primario junto con el puerto 389(LDAP)/636 (LDAP-Secure) .
3. Introduzca la ruta del nombre distinguido del administrador (DN) con la contraseña del administrador para el servidor LDAP .
4. Haga clic en Test Bind Server para probar el alcance del servidor LDAP desde ISE .

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 *

Configuración de la organización, grupos y atributos del directorio

1. Elija el grupo de organización correcto del usuario basado en la jerarquía de usuarios almacenados en el servidor LDAP .

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

Habilitar acceso administrativo para usuarios LDAP

Complete estos pasos para habilitar la autenticación basada en contraseña.

1. Vaya a ISE > Administration > System > Admin Access > Authentication.
2. En la ficha **Authentication Method**, seleccione la opción **Password-Based**.
3. Seleccione **LDAP** en el menú desplegable **Origen de identidad**.
4. Haga clic en **Guardar cambios**.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb trail is Administration > System > Admin Access > Authentication Method. The 'Authentication Method' sub-page is active, showing 'Authentication Type' with 'Password Based' selected. Below it, the 'Identity Source' is set to 'LDAP:LDAP_Server' via a dropdown menu. There are 'Save' and 'Reset' buttons at the bottom right.

Asigne el Grupo Admin al Grupo LDAP

Configure el grupo de administración en el ISE y asígnelo al grupo de AD. Esto permite al usuario configurado obtener acceso en función de las políticas de autorización basadas en los permisos RBAC configurados para el administrador en función de la pertenencia al grupo.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb trail is Administration > System > Admin Access > Admin Groups > LDAP_User_Group. The 'Admin Group' configuration page is active, showing 'Name' as 'LDAP_User_Group' and 'Type' as 'External'. The 'External Identity Source' is 'LDAP_Server'. Under 'External Groups', a group 'CN=employee,CN=Users,DC=a' is listed. At the bottom, there is a table for 'Member Users' which is currently empty with the message 'No data available'.

Establecer permisos para acceso a menús

1. Vaya a ISE > Administration > System > Authorization > Permissions > Menu access

2. Defina el acceso al menú para que el usuario administrador acceda a la GUI de ISE. Podemos configurar las subentidades que se mostrarán u ocultarán en la GUI para que un usuario pueda acceder a ellas de forma personalizada y realizar únicamente un conjunto de operaciones si es necesario.

3. Haga clic en **Guardar**.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb trail is Administration > System > Admin Access. The left sidebar shows the navigation menu with 'Permissions' expanded to 'Menu Access'. The main content area is titled 'Edit Menu Access Permission' for the object 'LDAP_Menu_Access'. It includes a 'Description' field and a 'Menu Access Privileges' section. The 'Menu Access Privileges' section contains 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 of this tree, under 'Permissions for Menu Access', the 'Show' radio button is selected, and the 'Hide' radio button is unselected.

Establecer permisos para acceso a datos

1. Vaya a ISE > Administration > System > Authorization > Permissions > Data Access

2. Defina el acceso a los datos para que el usuario administrador tenga acceso completo o acceso de sólo lectura a los grupos de identidad en la GUI de ISE.

3. Haga clic en **Guardar**.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb trail is Administration > System > Admin Access. The left sidebar shows the navigation menu with 'Permissions' expanded to 'Data Access'. The main content area is titled 'Edit Data Access Permission' for the object 'LDAP_Data_Access'. It includes a 'Description' field and a 'Data Access Privileges' section. The 'Data Access Privileges' section contains a tree view of the 'Data Access Privileges' with the following items: Admin Groups, User Identity Groups, Endpoint Identity Groups, and Network Device Groups. To the right of this tree, under 'Permissions for Data Access', the 'Full Access' radio button is selected, and the 'Read Only Access' and 'No Access' radio buttons are unselected.

Establecer permisos RBAC para el grupo de administradores

1. Vaya a ISE > Administration > System > Admin Access > Authorization > Policy.

- En el menú desplegable **Acciones** de la derecha, seleccione **Insertar nueva política abajo** para agregar una nueva política.
- Cree una nueva regla llamada LDAP_RBAC_policy y asígnela con el Grupo de Administración definido en la sección Habilitar acceso administrativo para AD, y asígnele permisos para acceso a menús y acceso a datos.
- Haga clic en **Guardar cambios**, y la confirmación de los cambios guardados se muestra en la esquina inferior derecha de la 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... X 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 ▾

Verificación

Acceso a ISE con credenciales AD

Complete estos pasos para acceder a ISE con credenciales AD:

- Abra la GUI de ISE para iniciar sesión con el usuario LDAP.
- Seleccione LDAP_Server en el menú desplegable **Identity Source**.
- Ingrese el nombre de usuario y la contraseña de la base de datos LDAP y conéctese.



Verifique el inicio de sesión del administrador en Informes de auditoría. Vaya a ISE > Operaciones > Informes > Auditoría > Logins de administradores.

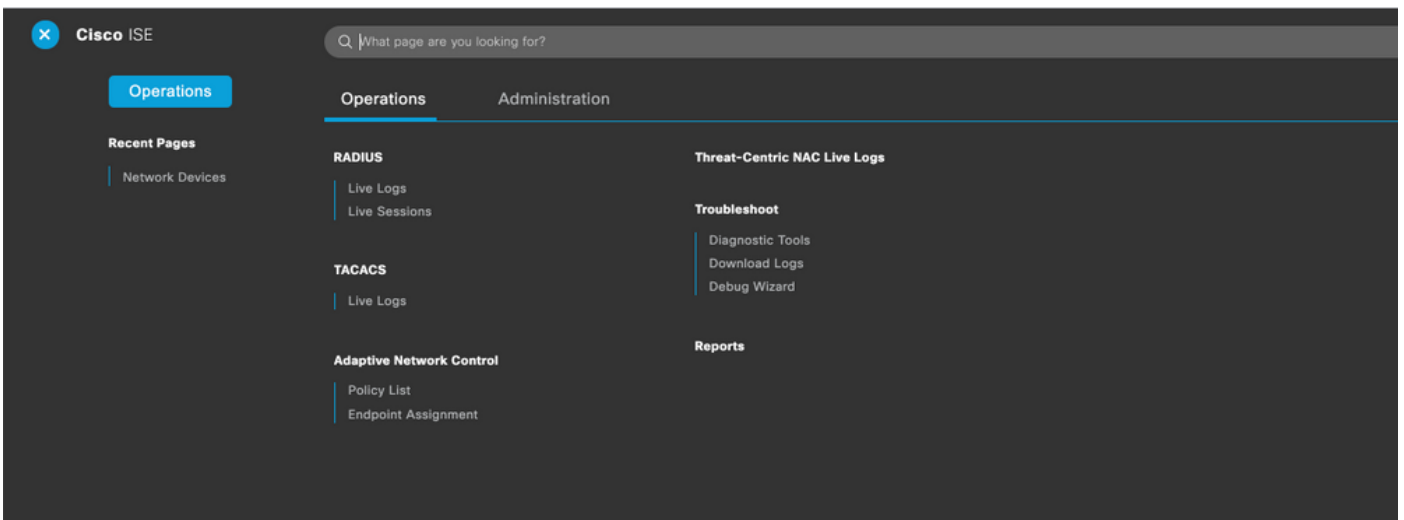
Cisco ISE Operations - Reports Evaluation Mode 64 Days

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

Para confirmar que esta configuración funciona correctamente, verifique el nombre de usuario autenticado en la esquina superior derecha de la GUI de ISE. Defina un acceso basado en el cliente que tenga acceso limitado al menú como se muestra aquí:



Troubleshoot

Información general

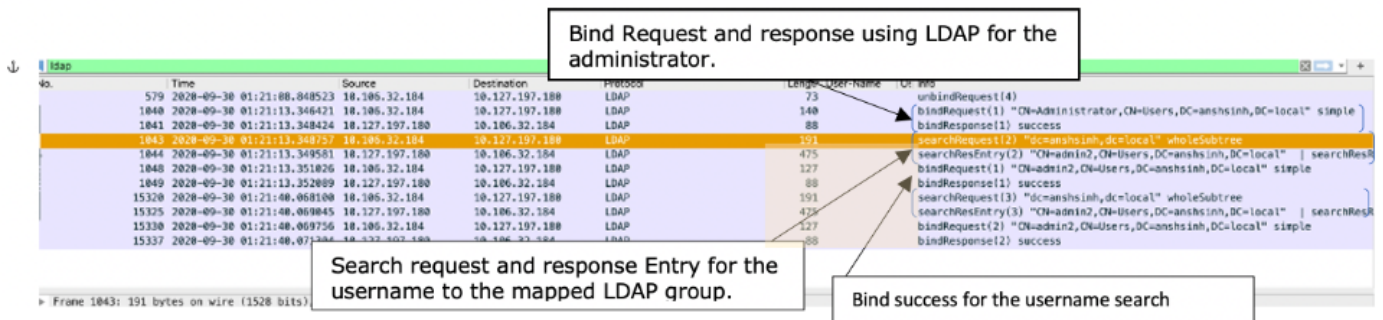
Para resolver problemas del proceso RBAC, estos componentes ISE deben estar habilitados en debug en el nodo de administrador ISE :

RBAC - Esto imprimirá el mensaje relacionado con RBAC cuando intentemos iniciar sesión (ise-psc.log)

access-filter - Esto imprimirá el acceso al filtro de recursos (ise-psc.log)

Runtime-AAA - Esto imprimirá los registros para los mensajes de interacción de login y LDAP (prtt-server.log)

Análisis de captura de paquetes



Análisis de registro

Verifique el prtt-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_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
```

Verifique el ise-psc.log

Desde estos registros, puede verificar la política RBAC utilizada para el usuario admin2 cuando intente acceder al recurso de dispositivo de red -

```
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
```