

Conocer las políticas de acceso de administrador y RBAC en ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuración de autenticación](#)

[Configurar grupos de administradores](#)

[Configurar usuarios administradores](#)

[Configurar permisos](#)

[Configuración de políticas RBAC](#)

[Configuración de los parámetros de acceso de administrador](#)

[Configurar el acceso al portal de administración con credenciales de AD](#)

[Incorporación de ISE a AD](#)

[Elegir grupos de directorios](#)

[Habilitar acceso administrativo para AD](#)

[Configuración del grupo de administradores de ISE para la asignación de grupos de AD](#)

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

[Acceso a ISE con credenciales de AD y verificación](#)

[Configuración del acceso al portal de administración con LDAP](#)

[Conexión de ISE a LDAP](#)

[Habilitar el acceso administrativo para usuarios de LDAP](#)

[Asigne el grupo de administradores de ISE al grupo LDAP](#)

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

[Acceso a ISE con credenciales LDAP y verificación](#)

Introducción

Este documento describe las funciones de ISE para administrar el acceso administrativo en Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que conozca estos temas:

- ISE
- Directorio activo
- Protocolo ligero de acceso a directorios (LDAP)

Componentes Utilizados

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

- ISE 3.0
- Windows Server 2016


La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Configuración de autenticación

Los usuarios administrativos deben autenticarse para acceder a cualquier información de ISE. La identidad de los usuarios administradores se puede verificar mediante el almacén de identidades interno de ISE o un almacén de identidades externo. La autenticidad puede verificarse mediante una contraseña o un certificado. Para configurar estos ajustes, navegue hasta **Administration > System > Admin Access > Authentication**. Seleccione el tipo de autenticación necesario en la **Authentication Method** ficha.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb navigation is 'Administration · System'. The main navigation bar includes 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access' (highlighted), and 'Settings'. The left sidebar has 'Authentication', 'Authorization', 'Administrators', and 'Settings' with expandable arrows. 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 with a radio button. Below this, there is a section for '* Identity Source' with a dropdown menu currently set to 'Internal'. The 'Client Certificate Based' option is also visible but unselected.

 **Nota:** La autenticación basada en contraseña está activada de forma predeterminada. Si se cambia a la autenticación basada en certificados de cliente, se reinicia un servidor de aplicaciones en todos los nodos de implementación.

ISE no permite la configuración de la directiva de contraseñas de la interfaz de línea de comandos (CLI) desde la CLI. La política de contraseñas tanto para la interfaz gráfica de usuario (GUI) como

para la CLI solo se puede configurar mediante la GUI de ISE. Para configurarlo, vaya a Administration > System > Admin Access > Authentication y vaya a la Password Policy ficha.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE', 'Administration · System', and 'Evaluation Mode'. The main menu has 'Admin Access' selected. The left sidebar shows 'Authentication' selected. The breadcrumb trail is 'Authentication Method > Password Policy > Account Disable Policy > Lock/Suspend Settings'. The main content area is titled 'GUI and CLI Password Policy'. It features a 'Minimum Length' field set to 4 characters. Below this is a section 'Password must not contain:' with several checkboxes: 'Admin name or its characters in reverse order' (checked), '* cisco*' or its characters in reverse order' (unchecked), 'This word or its characters in reverse order:' (unchecked), 'Repeated characters four or more times consecutively' (unchecked), and 'Dictionary words, their characters in reverse order or their letters replaced with other characters' (unchecked). Under the last option, 'Default Dictionary' is selected. A note states: 'The newly added custom dictionary file will replace the existing custom dictionary file.'

This screenshot continues the configuration of the Password Policy. The breadcrumb trail is 'Authentication Method > Password Policy > Account Disable Policy > Lock/Suspend Settings'. The main content area is titled 'Password must contain at least one character of each of the selected types:'. It has four checkboxes: 'Lowercase alphabetic characters' (checked), 'Uppercase alphabetic characters' (checked), 'Numeric characters' (checked), and 'Non-alphanumeric characters' (unchecked). Below this is the 'Password History' section, which includes a checkbox for 'Password must be different from the previous 3 versions' (checked) and a note: '[When enabled CLI remembers only last 1 password irrespective of value configured]'. There is also a field for 'Cannot reuse password within 15 days' (checked). The 'Password Lifetime' section includes a note: 'Admins can be required to periodically change their password. If Admin user is also configured as a network user, an expired enable password can cause the admin account to become disabled'. It has two checkboxes: 'Administrator passwords expire 45 days after creation or last change' (checked) and 'Send an email reminder to administrators 30 days prior to password expiration' (checked).

ISE tiene una provisión para deshabilitar un usuario administrador inactivo. Para configurar esto, navegue hasta Administration > System > Admin Access > Authentication y navegue hasta la Account Disable Policy pestaña.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration - System' and a warning icon. Below it, a secondary navigation bar lists 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', and 'Admin Access'. The left sidebar contains 'Authentication', 'Authorization', 'Administrators', and 'Settings'. The main content area is titled 'Account Disable Policy' and features a checked checkbox for 'Disable account after 30 days of inactivity. (Valid range 1 to 365)'.

ISE también proporciona la posibilidad de bloquear o suspender una cuenta de usuario administrador en función del número de intentos de inicio de sesión fallidos. Para configurar esto, navegue hasta **Administration > System > Admin Access > Authentication** y navegue hasta la **Lock/Suspend Settings** pestaña.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration - System' and a warning icon. Below it, a secondary navigation bar lists 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', and 'Admin Access'. The left sidebar contains 'Authentication', 'Authorization', 'Administrators', and 'Settings'. The main content area is titled 'Lock/Suspend Settings' and features a checked checkbox for 'Suspend or Lock Account with Incorrect Login Attempts'. Below this, there are three radio button options: 'Take action after 3 failed attempts (Valid Range 3 to 20)', 'Suspend account for 15 minutes (Valid Range 15 to 1440)', and 'Lock account'. The 'Suspend account for 15 minutes' option is selected. Below these options is a text area for 'Email remediation message' containing the text: 'This account has been locked. For this account to become unlocked, please contact your IT helpdesk.'

Para administrar el acceso administrativo, es necesario que los grupos administrativos, los usuarios y varias políticas/reglas controlen y administren sus privilegios.

Configurar grupos de administradores

Desplácese hasta **Administration > System > Admin Access > Administrators > Admin Groups** para configurar grupos de administradores. Algunos grupos están integrados de forma predeterminada y no se pueden eliminar.

- Authentication
- Authorization >
- Administrators >
 - Admin Users
 - Admin Groups**
- Settings >

Admin Groups

[Edit](#) [+ Add](#) [Duplicate](#) [Delete](#) [Reset All Ext. groups](#)

<input type="checkbox"/>	Name	External Groups Mapped	Description
<input type="checkbox"/>	Customization Admin	0	Access Permission to Guest Menu and Device Portal Management.
<input type="checkbox"/>	ERS Admin	0	Full access permission to External RESTful Services (ERS) APIs. Admins ...
<input type="checkbox"/>	ERS Operator	0	Read-only access permission to the External RESTful Services (ERS) API...
<input type="checkbox"/>	Elevated System Admin	0	Access permission for Operations tab. Includes System and data access ...
<input type="checkbox"/>	Helpdesk Admin	0	Access permission for Operations tab.
<input type="checkbox"/>	Identity Admin	0	Access permission for Operations tab. Includes Identity Management and...
<input type="checkbox"/>	MnT Admin	0	Access permission for Operations tab.
<input type="checkbox"/>	Network Device Admin	0	Access permission for Operations tab. Includes Network Resources and ...
<input type="checkbox"/>	Policy Admin	0	Access permission for Operations and Policy tabs. Includes System and I...
<input type="checkbox"/>	RBAC Admin	0	Access permission for Operations tab. Includes System and data access ...
<input type="checkbox"/>	Read Only Admin	0	Access Permission for admin with read-only functionality
<input type="checkbox"/>	SPOG Admin	0	This is the group for SPOG Admin to use the APIs for export and import
<input type="checkbox"/>	Super Admin	0	Access permission for Operations, Policy and Administration tabs. Includ...
<input type="checkbox"/>	System Admin	0	Access permission for Operations tab. Includes System and data access ...

Una vez creado un grupo, selecciónelo y haga clic en editar para agregar usuarios administrativos a ese grupo. Existe una disposición para asignar grupos de identidad externos a los grupos de administradores en ISE, de modo que un usuario administrador externo obtenga los permisos necesarios. Para configurarlo, elija el tipo `External` mientras agrega el usuario.

- Authentication
- Authorization >
- Administrators >
 - Admin Users
 - Admin Groups**
- Settings >

[Admin Groups](#) > Super Admin

Admin Group

* Name

Description

Type External

External Identity Source
Name :

External Groups

+ +

Member Users

Users

[+ Add](#) [Delete](#)

<input type="checkbox"/>	Status	Email	Username	First Name	Last Name
<input type="checkbox"/>	✔ Enabled		admin		

Configurar usuarios administradores

Para configurar usuarios administrativos, vaya a **Administration > System > Admin Access > Administrators > Admin Users**.

Administrators

Status	Name	Description	First Name	Last Name	Email Address	Admin Groups
<input type="checkbox"/>	Enabled	admin				Super Admin

Haga clic en Add (Agregar). Hay dos opciones para elegir. Una es agregar un nuevo usuario. La otra es hacer de un usuario de acceso a la red (es decir, un usuario configurado como usuario interno para acceder a la red o los dispositivos) un administrador de ISE.

Administrators

Description	First Name	Last Name	Email Address	Admin Groups
Default Admin User				Super Admin

Después de elegir una opción, se deben proporcionar los detalles necesarios y se debe elegir el grupo de usuarios en función de los permisos y privilegios que se otorgan al usuario.

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Settings

Administrators List > New Administrator

Authentication

Authorization >

Administrators >

Admin Users

Admin Groups

Settings >

Admin User

* Name Test_Admin

Status Enabled

Email testadmin@abcd.com Include system alarms in emails

External ⓘ

Read Only

Inactive account never disabled

Password

* Password ●●●●●●●● ⓘ

* Re-Enter Password ●●●●●●●● ⓘ

Generate Password

User Information

First Name

Last Name

Account Options

Description

Admin Groups

* ⓘ

Admin Groups

EQ

< ⓘ ⚙

Customization Admin ▲

ERS Admin

ERS Operator

Elevated System Admin

Helpdesk Admin

Identity Admin ▼

Configurar permisos

Hay dos tipos de permisos que se pueden configurar para un grupo de usuarios:

1. Acceso al menú
2. Acceso a datos

Menu Access controla la visibilidad de navegación en ISE. Hay dos opciones para cada ficha, Mostrar u Ocultar, que se pueden configurar. Se puede configurar una regla de acceso al menú para mostrar u ocultar las fichas seleccionadas.

Data Access controla la capacidad de leer/acceder/modificar los datos de identidad en ISE. El permiso de acceso sólo se puede configurar para grupos de administradores, grupos de identidad de usuarios, grupos de identidad de terminales y grupos de dispositivos de red. Hay tres opciones para estas entidades en ISE que se pueden configurar. Se trata de Acceso completo, Acceso de solo lectura y Sin acceso. Se puede configurar una regla de acceso a datos para elegir una de estas tres opciones para cada pestaña en ISE.

Se deben crear las directivas de acceso a menús y de acceso a datos para que se puedan aplicar a cualquier grupo de administradores. Hay algunas políticas integradas de forma predeterminada, pero siempre se pueden personalizar o se puede crear una nueva.

Para configurar una directiva de acceso a menús, vaya a **Administration > System > Admin Access > Authorization > Permissions > Menu Access**.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Administration · System' and a menu with options like 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', and 'Admin Access'. The left sidebar shows a tree view with 'Permissions' expanded to 'Menu Access'. The main content area is titled 'Menu Access' and contains a table with the following data:

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	Super Admin Menu Access	Access permission for Operations tab, Policy tab, Guest Access tab, Mobile Device Management tab
<input type="checkbox"/>	Policy Admin Menu Access	Access permission for Operations tab, Policy tab, Guest Access tab, Mobile Device Management tab,
<input type="checkbox"/>	Helpdesk Admin Menu Access	Access permission for Operations tab.
<input type="checkbox"/>	Identity Admin Menu Access	Access permission for Operations tab and Identity Management.
<input type="checkbox"/>	Network Device Menu Access	Access permission for Operations tab and Network Resources.
<input type="checkbox"/>	System Admin Menu Access	Access permission for Operations tab and System.
<input type="checkbox"/>	RBAC Admin Menu Access	Access permission for Operations tab and System.
<input type="checkbox"/>	MnT Admin Menu Access	Access permission for Operations tab.
<input type="checkbox"/>	Customization Admin Menu Access	Access Permission to Guest Menu and Device Portal Management.
<input type="checkbox"/>	TACACS+ Admin Menu Access	Access Permission to Operations, Administration and Workcenter

Haga clic en Add (Agregar). Cada opción de navegación de ISE se puede configurar para mostrarse u ocultarse en una política.

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access**

Authentication

Authorization

Permissions

Menu Access

Data Access

RBAC Policy

Administrators

Settings

Menu Access List > New RBAC Menu Access

Create Menu Access Permission

* Name: Custom_Menu_Access

Description:

Menu Access Privileges

ISE Navigation Structure

- > Policy
- Administration
 - System
 - Deployment
 - Licensing
 - Certificates
 - Certificate Manage
 - System Certificates
 - Trusted Certificates

Permissions for Menu Access

Show

Hide

Para configurar la directiva de acceso a datos, vaya a Administration > System > Admin Access > Authorization > Permissions > Data Access.

Cisco ISE Administration • System Evaluation Mode ?

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Settings

Authentication

Authorization

Permissions

Menu Access

Data Access

RBAC Policy

Administrators

Settings

Data Access

Edit Add Duplicate Delete

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	Super Admin Data Access	Access permission for Admin Groups, User Identity Groups, Endpoint Identity Groups, All Locations and All Device Types.
<input type="checkbox"/>	Policy Admin Data Access	Access permission for User Identity Groups and Endpoint Identity Groups.
<input type="checkbox"/>	Identity Admin Data Access	Access permission for User Identity Groups and Endpoint Identity Groups.
<input type="checkbox"/>	Network Admin Data Access	Access permission for All Locations and All Device Types.
<input type="checkbox"/>	System Admin Data Access	Access permission for Admin Groups.
<input type="checkbox"/>	RBAC Admin Data Access	Access permission for Admin Groups.
<input type="checkbox"/>	Customization Admin Data Access	
<input type="checkbox"/>	TACACS+ Admin Data Access	Access permission for All Locations and All Device Types, User Identity groups and End point identity groups.
<input type="checkbox"/>	Read Only Admin Data Access	Access permission for All Locations and All Device Types, User Identity groups and End point identity groups.

Haga clic en Agregar para crear una nueva política y configurar permisos para acceder a Admin/User Identity/Endpoint Identity/Network Groups.

The screenshot shows the 'Create Data Access Permission' configuration page in the Cisco ISE Admin Access interface. The page is divided into a sidebar on the left and a main content area on the right. The sidebar contains navigation options: Authentication, Authorization, Permissions, Data Access, RBAC Policy, Administrators, and Settings. The main content area is titled 'Create Data Access Permission' and contains a form for Name (Custom_Data_Access) and Description. Below the form is a 'Data Access Privileges' section with a tree view of data sources and a 'Permissions for Data Access' section with radio buttons for Full Access, Read Only Access, and No Access.

Configuración de políticas RBAC

RBAC significa control de acceso basado en roles. El rol (grupo de administradores) al que pertenece un usuario se puede configurar para utilizar las directivas de acceso a datos y menú deseadas. Puede haber varias políticas RBAC configuradas para un solo rol o pueden configurarse varios roles en una sola política para acceder a Menú y/o Datos. Todas estas políticas aplicables se evalúan cuando un usuario administrador intenta realizar una acción. La decisión final es la suma de todas las políticas aplicables a esa función. Si hay reglas contradictorias que permiten y deniegan al mismo tiempo, la regla de permiso anula la regla de denegación. Para configurar estas directivas, vaya a [Administration > System > Admin Access > Authorization > RBAC 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). Note that multiple Menu/Data Access permissions are 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 deleted. For decision making, all applicable policies will be evaluated. The subject's permissions will be the aggregate of all permissions from each applicable policy (policies are displayed in alphabetical order of the policy name).

Authentication

Authorization

Permissions

RBAC Policy


Administrators

Settings

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"/> MnT Admin Policy	If MnT Admin	+ then MnT Admin Menu Access + Actions
<input checked="" type="checkbox"/> Network Device Policy	If Network Device Admin	+ then Network Device Menu Acces... + Actions
<input checked="" type="checkbox"/> Policy Admin Policy	If Policy Admin	+ then Policy Admin Menu Access a... + Actions
<input checked="" type="checkbox"/> RBAC Admin Policy	If RBAC Admin	+ then RBAC Admin Menu Access a... + Actions

Haga clic **Actions** para duplicar/insertar/eliminar una política.

 Nota: Las políticas creadas por el sistema y las políticas por defecto no se pueden actualizar y las políticas por defecto no se pueden eliminar.

 Nota: No se pueden configurar varios permisos de menú/acceso a datos en una sola regla.

Configuración de los parámetros de acceso de administrador

Además de las políticas de RBAC, hay algunas configuraciones que se pueden configurar que son comunes a todos los usuarios administradores.

Para configurar el número máximo de sesiones permitidas, banners previos y posteriores al inicio de sesión para GUI y CLI, vaya a **Administration > System > Admin Access > Settings > Access**. Configúrelos en la pestaña **Session**.

- Authentication
- Authorization >
- Administrators >
- Settings ▾
 - Access**
 - Session
 - Portal Customization

GUI Sessions

Maximum Concurrent Sessions (Valid Range 1 to 20)

Pre-login banner

Welcome to ISE

Post-login banner

CLI Sessions

Maximum Concurrent Sessions (Valid Range 1 to 10)

Pre-login banner

Administration > System > Admin Access > Settings > Access **Para configurar la lista de direcciones IP desde las cuales se puede acceder a la GUI y la CLI, navegue hasta la IP Access pestaña y navegue hasta ella.**

- Authentication
- Authorization >
- Administrators >
- Settings ▾
 - Access**
 - Session
 - Portal Customization

Access Restriction

- Allow all IP addresses to connect
- Allow only listed IP addresses to connect

Configure IP List for Access Restriction

IP List


+ Add Edit Delete

<input type="checkbox"/> IP	<input type="text" value="MASK"/>
<input type="checkbox"/> 10.9.8.0	24

Para configurar una lista de nodos desde los cuales los administradores pueden acceder a la sección MnT en Cisco ISE, desplácese hasta Administration > System > Admin Access > Settings > Access la MnT Access pestaña y desplácese hasta ella.

Para permitir que los nodos o entidades de la implementación o de fuera de ella envíen registros del sistema a MnT, haga clic en el botón de opción **Allow any IP address to connect to MNT**. Para permitir que sólo los nodos o entidades de la implementación envíen registros del sistema a MnT, haga clic en el botón de opción **Allow only the nodes in the deployment to connect to MNT**.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb trail is Administration > System. The main navigation tabs include Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, and Admin Access. The left sidebar shows a tree view with Authentication, Authorization, Administrators, and Settings. Under Settings, the Access section is expanded to show Session and Portal Customization. The main content area is titled MnT Access and contains a section for MnT Access Restriction with two radio button options: 'Allow any IP address to connect to MNT' (selected) and 'Allow only the nodes in the deployment to connect to MNT'.

 Nota: Para ISE 2.6 parche 2 y versiones posteriores, el servicio de mensajería de ISE está habilitado de forma predeterminada para entregar registros del sistema UDP a MnT. Esta configuración restringe la aceptación de registros del sistema de entidades externas más allá de la implementación.

Para configurar un valor de tiempo de espera debido a la inactividad de una sesión, vaya a **Administration > System > Admin Access > Settings > Session**. Establezca este valor en la **Session Timeout** ficha.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb trail is Administration > System. The main navigation tabs include Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, and Admin Access. The left sidebar shows a tree view with Authentication, Authorization, Administrators, and Settings. Under Settings, the Session section is expanded to show Portal Customization. The main content area is titled Session Timeout and contains a form field for Session Idle Timeout set to 60 minutes (Valid Range 6 to 100).

Para ver/invalidar las sesiones activas actualmente, navegue hasta **Administration > Admin Access > Settings > Session** y haga clic en la **Session Info** pestaña.

Session Timeout **Session Info**

Select session and terminate

Session Info

[Invalidate](#)

	UserID	IP Address	Session Creation Time	Session Last Accessed
<input type="checkbox"/>	admin	10.65.48.253	Fri Oct 09 01:16:59 IST 2020	Fri Oct 09 01:45:10 IST 2020

Configurar el acceso al portal de administración con credenciales de AD

Incorporación de ISE a AD

Para unir ISE a un dominio externo, vaya a **Administration > Identity Management > External Identity Sources > Active Directory**. Introduzca el nuevo nombre del punto de unión y el dominio de Active Directory. Escriba las credenciales de la cuenta de AD que puede agregar, realice cambios en los objetos del equipo y haga clic en **Aceptar**.

Cisco ISE Administration • Identity Management

Identities Groups **External Identity Sources** Identity Source Sequences Settings

External Identity Sources Connection Whitelisted Domains PassivID Groups Attributes Advanced S

< [Icon] [Icon]
 > Certificate Authentication F
 v Active Directory
 AD
 LDAP
 ODBC
 RADIUS Token
 RSA SecurID
 SAML Id Providers
 Social Login

* Join Point Name AD

* Active Directory Domain rinsantr.lab

Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name Administrator

* Password ●●●●●●●●●●

Specify Organizational Unit

Store Credentials

Connection Whitelisted Domains PassivID Groups Attributes Advanced Settings

* Join Point Name AD

* Active Directory Domain rinsantr.lab

+ Join + Leave [Icon] Test User [Icon] Diagnostic Tool [Icon] Refresh Table

<input type="checkbox"/>	ISE Node	ISE Node R...	Status	Domain Controller	Site
<input type="checkbox"/>	rini-ise-30.gce.iselab.local	STANDALONE	<input checked="" type="checkbox"/> Operational	WIN-5KSMPOHEP5A.rinsantr.l...	Default-First-Site-Name

Elegir grupos de directorios

Desplácese hasta Administration > Identity Management > External Identity Sources > Active Directory. Haga clic en el nombre del punto de unión que desee y desplácese a la ficha Grupos. Haga clic en Add > Select Groups from Directory > Retrieve Groups. Importe al menos un grupo de AD al que pertenezca el administrador, haga clic en Aceptar y, a continuación, haga clic en Guardar.

Identity Sources

Connection

Edit +

Na

No data available

<

Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

Name Filter * SID Filter * Type Filter

<input type="checkbox"/>	Name	Group SID	Group Type
<input type="checkbox"/>	rinsantr.lab/Users/Enterprise Key Admins	S-1-5-21-1977851106-3699455990-29458652...	UNIVERSAL
<input type="checkbox"/>	rinsantr.lab/Users/Enterprise Read-only Domain ...	S-1-5-21-1977851106-3699455990-29458652...	UNIVERSAL
<input type="checkbox"/>	rinsantr.lab/Users/Group Policy Creator Owners	S-1-5-21-1977851106-3699455990-29458652...	GLOBAL
<input type="checkbox"/>	rinsantr.lab/Users/Key Admins	S-1-5-21-1977851106-3699455990-29458652...	GLOBAL
<input type="checkbox"/>	rinsantr.lab/Users/Protected Users	S-1-5-21-1977851106-3699455990-29458652...	GLOBAL
<input type="checkbox"/>	rinsantr.lab/Users/RAS and IAS Servers	S-1-5-21-1977851106-3699455990-29458652...	DOMAIN LOCAL
<input type="checkbox"/>	rinsantr.lab/Users/Read-only Domain Controllers	S-1-5-21-1977851106-3699455990-29458652...	GLOBAL
<input type="checkbox"/>	rinsantr.lab/Users/Schema Admins	S-1-5-21-1977851106-3699455990-29458652...	UNIVERSAL
<input checked="" type="checkbox"/>	rinsantr.lab/Users/Test Group	S-1-5-21-1977851106-3699455990-29458652...	GLOBAL

<

Cancel OK

Connection Whitelisted Domains PassivID **Groups** Attributes Advanced Settings

Edit + Add Delete Group Update SID Values

<input type="checkbox"/>	Name	SID
<input type="checkbox"/>	rinsantr.lab/Users/Test Group	S-1-5-21-1977851106-3699455990-2945865208-1106

Habilitar acceso administrativo para AD

Para habilitar la autenticación basada en contraseñas de ISE mediante AD, vaya a **Administration > System > Admin Access > Authentication**. En la **Authentication Method** ficha, elija la **Password-Based** opción. Elija AD en el **Identity Source** menú desplegable y haga clic en **Guardar**.

Cisco ISE Administration - System Evaluation Mode 601

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Settings

Authentication

Authentication Method Password Policy Account Disable Policy Lock/Suspend Settings

Authorization >

Administrators >

Settings >

Authentication Method

Authentication Type

Password Based

* Identity Source

AD:AD

Client Certificate Based

Save

Configuración del grupo de administradores de ISE para la asignación de grupos de AD

Esto permite la autorización para determinar los permisos RBAC para el administrador en función de la pertenencia al grupo en AD. Para definir un grupo de administradores de Cisco ISE y asignarlo a un grupo de AD, vaya a **Administration > System > Admin Access > Administrators > Admin Groups**. Haga clic en **Agregar** e ingrese un nombre para el nuevo grupo de administradores. En el campo **Tipo**, marque la casilla de verificación **Externo**. En el menú desplegable **Grupos externos**, elija el grupo AD al que se asignará este grupo de administradores (como se define en la **Select Directory Groups** sección). Envíe los cambios.

Cisco ISE Administration - System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access**

Authentication

Authorization >

Administrators >

Admin Users

Admin Groups

Settings >

Admin Groups > ISE AD Admin Group

Admin Group

* Name ISE AD Admin Group

Description

Type External

External Identity Source

Name : AD

External Groups

* rinsantr.lab/Users/Test Group

Member Users

Users

+ Add Delete

Status	Email	Username	First Name	Last Name
No data available				

Establecer permisos RBAC para el grupo de administradores

Para asignar permisos RBAC al grupo de administradores creado en la sección anterior, vaya a **Administration > System > Admin Access > Authorization > RBAC Policy**. En el menú desplegable **Actions** de la derecha, seleccione **Insert new policy**. Cree una nueva regla, asígnela al grupo de administradores definido en la sección anterior y asígnele los datos y permisos de acceso al menú que desee. A continuación, haga clic en **Guardar**.

The screenshot shows the Cisco ISE Administration console. 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 has a tree view with 'RBAC Policy' selected under 'Permissions'. The main content area displays a table of RBAC Policies with columns for Rule Name, Admin Groups, and Permissions. A dropdown menu is open for the 'RBAC Policy 1' row, showing options for 'Super Admin Menu Access' and 'Super Admin Data Access'.

Rule Name	Admin Groups	Permissions
Customization Admin Policy	If Customization Admin	then Customization Admin Men... + Actions
RBAC Policy 1	If ISE AD Admin Group	then Super Admin Menu Acces... X Actions
Elevated System Admin Poli	If Elevated System Admin	then
ERS Admin Policy	If ERS Admin	then
ERS Operator Policy	If ERS Operator	then

Acceso a ISE con credenciales de AD y verificación

Cierre la sesión de la GUI administrativa. Seleccione el nombre del punto de unión en el **Identity Source** menú desplegable. Introduzca el nombre de usuario y la contraseña de la base de datos de AD e inicie sesión.



Identity Services Engine

Intuitive network security

Username
TestUser

Password
●●●●●●●●

Identity Source
AD

Login

Para confirmar que la configuración funciona correctamente, verifique el nombre de usuario autenticado desde el icono Settings en la esquina superior derecha de la GUI de ISE. Navegue hasta Información del servidor y verifique el Nombre de usuario.

Dashboard

Acti

Beh

ure Re

IDP

Pr

×

Server Information

Username: TestUser

Host: rini-ise-30

Personas: Administration, Monitoring, Policy
Service (SESSION,PROFILER)

Role: STANDALONE

System Time: Oct 27 2020 01:23:21 AM
Asia/Kolkata

FIPS Mode: Disabled

Version: 3.0.0.458

Patch Information: none












OK

Configuración del acceso al portal de administración con LDAP

Conexión de ISE a LDAP

Desplácese hasta **Administration > Identity Management > External Identity Sources > Active Directory > LDAP**. En la **General** ficha, introduzca un nombre para LDAP y elija el esquema como **Active Directory**.

External Identity Sources

- <  
- >  Certificate Authentication F
- ▼  Active Directory
 -  AD
 -  LDAP
 -  ODBC
 -  RADIUS Token
 -  RSA SecurID
 -  SAML Id Providers
 -  Social Login

[LDAP Identity Sources List](#) > New LDAP Identity Source

LDAP Identity Source









General Connection Directory Organization Groups Attribut

* Name

Description

▶ Schema ▼

A continuación, para configurar el tipo de conexión, vaya a la **Connection** ficha . Aquí, configure el nombre de host/IP del servidor LDAP principal junto con el puerto 389 (LDAP)/636 (LDAP-Secure). Introduzca la ruta del nombre distinguido (DN) de administrador con la contraseña de administrador del servidor LDAP.

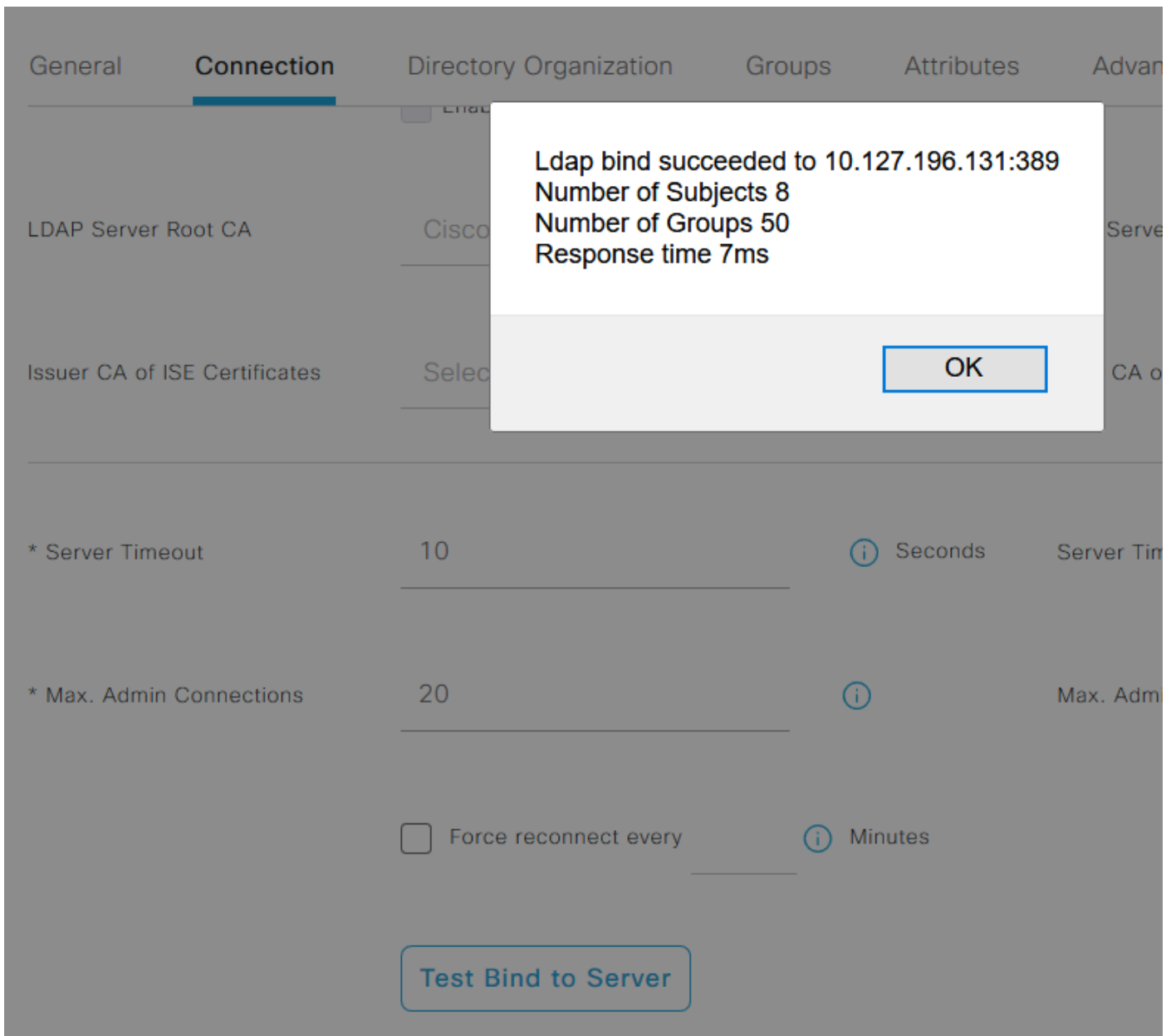
- ▼  Active Directory
 -  AD
 -  LDAP
 -  ODBC
 -  RADIUS Token
 -  RSA SecurID
 -  SAML Id Providers
 -  Social Login

General	Connection	Directory Organization	Groups	Attributes	Advanced Settings
	Primary Server				Secondary Server
					<input type="checkbox"/> Enable Secondary Server
* Hostname/IP	<input type="text" value="10.127.196.131"/> ⓘ			Hostname/IP	<input type="text"/>
* Port	<input type="text" value="389"/>			Port	<input type="text" value="389"/>
<input type="checkbox"/> Specify server for each ISE node					
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	* <input type="text" value="CN=Administrator,CN=Users,DC"/>			Admin DN	<input type="text" value="admin"/>
Password	* <input type="password" value="••••••••"/>			Password	<input type="password"/>
Secure Authentication	<input type="checkbox"/> Enable Secure Authentication			Secure Authentication	<input type="checkbox"/> Enable Secure Authentication

A continuación, vaya a la [Directory Organization](#) ficha y haga clic en [Naming Contexts](#) para elegir el grupo de organización correcto del usuario en función de la jerarquía de usuarios almacenada en el servidor LDAP.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration • Identity Management'. Below it, a secondary navigation bar has 'Identities', 'Groups', 'External Identity Sources' (highlighted), 'Identity Source Sequences', and 'Settings'. On the left, a sidebar titled 'External Identity Sources' lists various authentication methods, with 'LDAP' selected. The main content area is titled 'LDAP Identity Sources List > LDAPExample' and 'LDAP Identity Source'. It features several tabs: 'General', 'Connection', 'Directory Organization' (active), 'Groups', 'Attributes', and 'Advanced Settings'. Under the 'Directory Organization' tab, there are two rows for search bases: '* Subject Search Base' and '* Group Search Base', both set to 'DC=rinsantr,DC=lab'. Each row has a 'Naming Contexts...' button with an information icon. Below these, there is a 'Search for MAC Address in Format' field with the value 'XX-XX-XX-XX-XX-XX' and a dropdown arrow. At the bottom, there are two unchecked checkboxes: 'Strip start of subject name up to the last occurrence of the separator \\' and 'Strip end of subject name from the first occurrence of the separator \\'.

Haga clic en [Test Bind to Server](#) en la [Connection](#) pestaña para probar la disponibilidad del servidor LDAP desde ISE.



Ahora desplácese a la pestaña **Groups** y haga clic en **Add > Select Groups From Directory > Retrieve Groups**.
Importe al menos un grupo al que pertenezca el administrador, haga clic en **Aceptar** y, a continuación, haga clic en **Guardar**.

Select Directory Groups

This dialog is used to select groups from the Directory. Click **Retrieve Groups..** to read directory.

Filter: * Retrieve Groups... Number of Groups Retrieved: 50 (Limit is 100)

<input type="checkbox"/>	Name
<input type="checkbox"/>	CN=Server Operators,CN=Builtin,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=Storage Replica Administrators,CN=Builtin,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=System Managed Accounts Group,CN=Builtin,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=Terminal Server License Servers,CN=Builtin,DC=rinsantr,DC=lab
<input checked="" type="checkbox"/>	CN=Test Group,CN=Users,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=Users,CN=Builtin,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=Windows Authorization Access Group,CN=Builtin,DC=rinsantr,DC=lab

Cancel OK

LDAP Identity Sources List > LDAPExample

LDAP Identity Source

General Connection Directory Organization **Groups** Attributes Advanced Settings

Edit + Add Delete Group

<input type="checkbox"/>	Name
<input type="checkbox"/>	CN=Test Group,CN=Users,DC=rinsantr,DC=lab

Habilitar el acceso administrativo para usuarios de LDAP

Para habilitar la autenticación basada en contraseña de ISE mediante LDAP, vaya a **Administration > System > Admin Access > Authentication**. En la **Authentication Method** ficha, elija la **Password-Based** opción. Elija LDAP del **Identity Source** menú desplegable y haga clic en **Save**.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb trail is Administration > System > Admin Access > Authentication Method. The 'Authentication Method' is set to 'Password Based'. Under 'Identity Source', a dropdown menu is open showing 'LDAP:LDAPExample' selected. There is a 'Save' button at the bottom right.

Asigne el grupo de administradores de ISE al grupo LDAP

Esto permite al usuario configurado obtener acceso de administrador basado en la autorización de las políticas RBAC, que a su vez se basa en la pertenencia al grupo LDAP del usuario. Para definir un grupo de administradores de Cisco ISE y asignarlo a un grupo LDAP, vaya a [Administration > System > Admin Access > Administrators > Admin Groups](#). Haga clic en **Agregar** e ingrese un nombre para el nuevo grupo de administradores. En el campo **Tipo**, marque la casilla de verificación **Externo**. En el menú desplegable **External Groups**, elija el grupo LDAP al que se asignará este grupo de administración (como se recuperó y definió anteriormente). Envíe los cambios.

The screenshot shows the Cisco ISE Administration interface for creating a new admin group. The breadcrumb trail is Administration > System > Admin Access > Admin Groups > New Admin Group. The 'Name' field contains 'ISE LDAP Admin Group'. The 'Type' is set to 'External'. Under 'External Identity Source', the name is 'LDAPExample'. In the 'External Groups' section, a dropdown menu is open showing 'CN=Test Group,CN=Users,DC=' selected. There is a '+' button next to the dropdown.

Establecer permisos RBAC para el grupo de administradores

Para asignar permisos RBAC al grupo de administradores creado en la sección anterior, vaya a [Administration > System > Admin Access > Authorization > RBAC Policy](#). En el menú desplegable **Actions** de la

derecha, seleccione **Insert new policy**. Cree una nueva regla, asígnela al grupo de administradores definido en la sección anterior y asígnele los datos y permisos de acceso al menú que desee. A continuación, haga clic en **Guardar**.

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Set

Authentication

Authorization

Permissions

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 element). Menu/Data Access permissions are 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 deleted. For decision making, all applicable policies will be evaluated. The subject's permissions will be the aggregate of all permissions from each applicable policy, displayed in alphabetical order of the policy name).

RBAC Policies

Rule Name	Admin Groups	Permissions
Customization Admin Policy	Customization Admin	Customization Admin Menu ...
RBAC Policy 2	ISE LDAP Admin Group	Super Admin Menu Access a...
Elevated System Admin Poli	Elevated System Admin	
ERS Admin Policy	ERS Admin	
ERS Operator Policy	ERS Operator	
ERS Trustsec Policy	ERS Trustsec	Super Admin Data Access
Healthcheck Admin Policy	Healthcheck Admin	Healthcheck Admin Menu Access

Acceso a ISE con credenciales LDAP y verificación

Cierre la sesión de la GUI administrativa. Elija el nombre LDAP en el menú desplegable Origen de identidad. Introduzca el nombre de usuario y la contraseña de la base de datos LDAP e inicie sesión.



Identity Services Engine

Intuitive network security

Username

TestUser@rinsantr.lab

Password

●●●●●●●●

Identity Source

LDAPExample



Login

Para confirmar que la configuración funciona correctamente, verifique el nombre de usuario autenticado desde el icono Settings en la esquina superior derecha de la GUI de ISE. Navegue hasta Información del servidor y verifique el Nombre de usuario.



Server Information

Username: **TestUser@rinsantr.lab**

Host: **rini-ise-30**

Personas: **Administration, Monitoring, Policy
Service (SESSION,PROFILER)**

Role: **STANDALONE**

System Time: **Oct 27 2020 03:48:32 AM
Asia/Kolkata**

FIPS Mode: **Disabled**

Version: **3.0.0.458**

Patch Information: **none**

OK

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).