

Entender as políticas de acesso administrativo e RBAC no ISE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configurações de autenticação](#)

[Configurar grupos de administração](#)

[Configurar usuários administradores](#)

[Configurar permissões](#)

[Configurar políticas de RBAC](#)

[Definir configurações para acesso de administrador](#)

[Configurar o acesso do portal administrativo com credenciais do AD](#)

[Participe do ISE para o AD](#)

[Selecionar grupos de diretórios](#)

[Habilitar acesso administrativo para AD](#)

[Configurar o grupo administrativo do ISE para o mapeamento de grupo do AD](#)

[Definir permissões RBAC para o grupo de administração](#)

[Acesse o ISE com credenciais do AD e verifique](#)

[Configurar o acesso do portal administrativo com LDAP](#)

[Ingressar ISE em LDAP](#)

[Habilitar acesso administrativo para usuários LDAP](#)

[Mapear o grupo de administração do ISE para o grupo LDAP](#)

[Definir permissões RBAC para o grupo de administração](#)

[Acesse o ISE com credenciais LDAP e verifique](#)

Introduction

Este documento descreve os recursos do ISE para gerenciar o Acesso Administrativo no Identity Services Engine (ISE).

Prerequisites

Requirements

A Cisco recomenda que você conheça estes tópicos:

- ISE
- Active Directory

- LDAP (Lightweight Directory Access Protocol)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

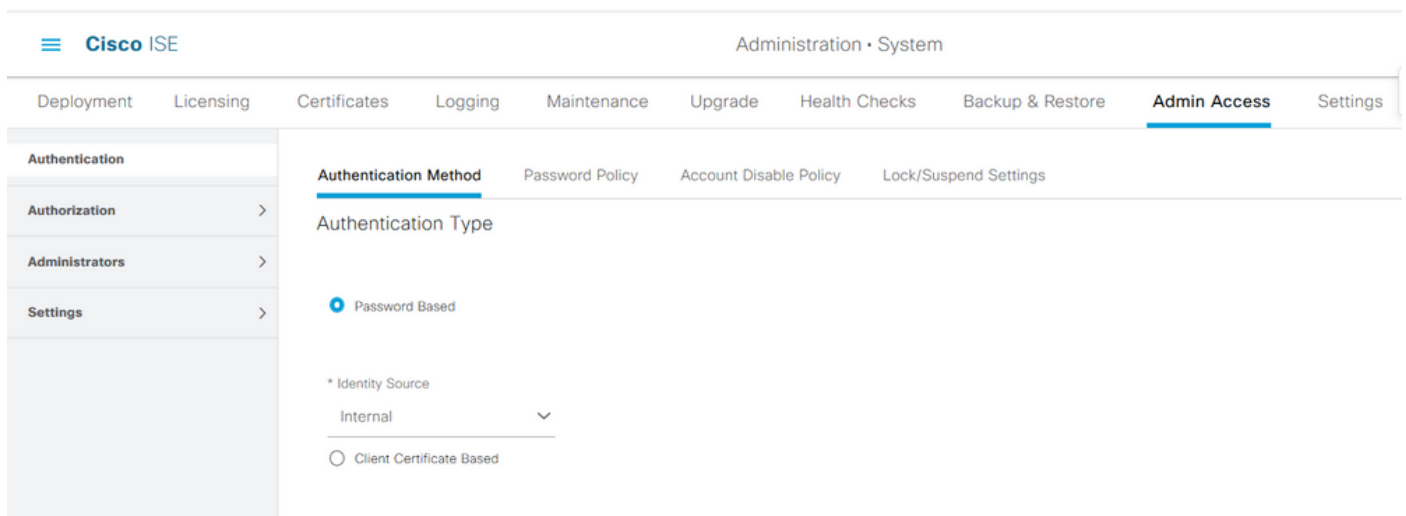
- Identity Services Engine 3.0
- Windows Server 2016

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Configurações de autenticação

Os usuários administrativos precisam se autenticar para acessar qualquer informação no ISE. A identidade dos usuários admin pode ser verificada usando o ISE Internal Identity Store ou um External Identity Store. A autenticidade pode ser verificada por uma senha ou um certificado. Para definir essas configurações, navegue para **Administration > System > Admin Access > Authentication**. Selecione o tipo de autenticação necessário na guia **Authentication Method**.



Note: A autenticação baseada em senha está habilitada por padrão. Se isso for alterado para a autenticação baseada em certificado do cliente, isso fará com que um servidor de aplicativos seja reiniciado em todos os nós de implantação.

O Identity Services Engine não permite configurar a política de senha para a CLI (Command Line Interface, interface de linha de comando) a partir da CLI. A política de senha para a Interface Gráfica de Usuário (GUI) e para a CLI só pode ser configurada através da GUI do ISE. Para configurar isso, navegue para **Administration > System > Admin Access > Authentication** e navegue até a guia **Password Policy**.

Authentication

Authorization >

Administrators >

Settings >

GUI and CLI Password Policy

* Minimum Length: 4 characters (Valid Range 4 to 127)

Password must not contain:

- Admin name or its characters in reverse order
- *cisco* or its characters in reverse order
- This word or its characters in reverse order: _____
- Repeated characters four or more times consecutively
- Dictionary words, their characters in reverse order or their letters replaced with other characters ⓘ
 - Default Dictionary ⓘ
 - Custom Dictionary ⓘ No file selected.

The newly added custom dictionary file will replace the existing custom dictionary file.

Authentication

Authorization >

Administrators >

Settings >

Password must contain at least one character of each of the selected types:

- Lowercase alphabetic characters
- Uppercase alphabetic characters
- Numeric characters
- Non-alphanumeric characters

Password History

- Password must be different from the previous 3 versions [When enabled CLI remembers only last 1 password irrespective of value configured]

* Cannot reuse password within 15 days (Valid Range 0 to 365)

Password Lifetime

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

- Administrator passwords expire 45 days after creation or last change (valid range 1 to 3650)
- Send an email reminder to administrators 30 days prior to password expiration (valid range 1 to 3650)

O ISE tem uma provisão para desativar um usuário administrador inativo. Para configurar isso, navegue até **Administration > System > Admin Access > Authentication** e navegue até a guia **Account Disable Policy**.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb path is Administration > System > Admin Access > Authentication > Account Disable Policy. The 'Account Disable Policy' tab is selected. A checkbox labeled 'Disable account after' is checked, and the value '30' is entered in the adjacent input field, followed by the text 'days of inactivity. (Valid range 1 to 365)'.

O ISE também oferece o recurso de bloquear ou suspender uma conta de usuário admin com base no número de tentativas de login com falha. Para configurar isso, navegue para **Administration > System > Admin Access > Authentication** e navegue até a guia **Lock/Suspend Settings**.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb path is Administration > System > Admin Access > Authentication > Lock/Suspend Settings. The 'Lock/Suspend Settings' tab is selected. A checkbox labeled 'Suspend or Lock Account with Incorrect Login Attempts' is checked. Below it, 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 gerenciar o acesso administrativo, é necessário que grupos administrativos, usuários e várias políticas/regras controlem e gerenciem seus privilégios.

Configurar grupos de administração

Navegue até **Administration > System > Admin Access > Administrators > Admin Groups** para configurar grupos de administradores. Há poucos grupos que são incorporados por padrão e não podem ser excluídos.

- 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 ...

Depois que um grupo for criado, selecione o grupo e clique em editar para adicionar usuários administrativos a esse grupo. Há uma provisão para mapear grupos de identidade externos para grupos de administradores no ISE, de modo que um usuário de administrador externo obtenha as permissões necessárias. Para configurar isso, selecione o tipo como Externo ao adicionar o usuário.

- 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"/>	<input checked="" type="checkbox"/> Enabled		admin		

Configurar usuários administradores

Para configurar Usuários Admin, navegue para **Administração > Sistema > Acesso Admin > Administradores > Usuários Admin**.

Cisco ISE Administration - System

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

Authentication

Authorization >

Administrators ▾

Admin Users

Admin Groups

Settings >

Administrators

Edit + Add Change Status Delete Duplicate

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

Clique em Add. Há duas opções para escolher. Uma é adicionar um novo usuário completamente. O outro é fazer um usuário de acesso à rede (ou seja, um usuário configurado como um usuário interno para acessar a rede/dispositivos) como um administrador do ISE.

Cisco ISE Administration - System

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

Authentication

Authorization >

Administrators ▾

Admin Users

Admin Groups

Settings >

Administrators

Edit + Add Change Status Delete Duplicate

- Create an Admin User
- Select from Network Access Users >

<input type="checkbox"/>	Description	First Name	Last Name	Email Address	Admin Groups
<input type="checkbox"/>	Default Admin User				Super Admin

Depois de selecionar uma opção, os detalhes necessários devem ser fornecidos e o grupo de usuários deve ser selecionado com base no qual as permissões e os privilégios são dados ao usuário.

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

- Customization Admin
- ERS Admin
- ERS Operator
- Elevated System Admin
- Helpdesk Admin
- Identity Admin

Configurar permissões

Há dois tipos de permissões que podem ser configuradas para um grupo de usuários:

1. Acesso ao menu
2. Acesso a dados

O Menu Access controla a visibilidade de navegação no ISE. Há duas opções para cada guia, Mostrar ou Ocultar, que podem ser configuradas. Uma regra de Acesso a Menu pode ser configurada para mostrar ou ocultar guias selecionadas.

O acesso a dados controla a capacidade de ler/acessar/modificar os dados de identidade no ISE. A permissão de acesso pode ser configurada somente para grupos de administração, grupos de identidade de usuário, grupos de identidade de endpoint e grupos de dispositivos de rede. Há três opções para essas entidades no ISE que podem ser configuradas. Eles são acesso total, acesso somente leitura e sem acesso. Uma regra de acesso a dados pode ser configurada para escolher uma dessas três opções para cada guia no ISE.

As políticas de Acesso a Menu e Acesso a Dados devem ser criadas para que possam ser aplicadas a qualquer grupo de administradores. Há algumas políticas incorporadas por padrão,

mas elas sempre podem ser personalizadas ou podem ser criadas novas.

Para configurar uma política de acesso a menus, navegue para **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: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, and Admin Access (highlighted). 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 of existing menu access permissions. Each row has a checkbox, a name, and a description.

<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

Clique em Add. Cada opção de navegação no ISE pode ser configurada para ser mostrada/oculta em uma política.

The screenshot shows the 'Create Menu Access Permission' form in the Cisco ISE Administration console. The top navigation bar is the same as in the previous image. The left sidebar shows 'Permissions' expanded to 'Menu Access'. The main content area is titled 'Create Menu Access Permission' and contains a form with the following fields:

- * Name: Custom_Menu_Access
- Description: (empty text box)

Below the form is a section titled 'Menu Access Privileges'. It features a tree view of the 'ISE Navigation Structure' and a 'Permissions for Menu Access' section. The tree view shows the following structure:

- ISE Navigation Structure
 - > Policy
 - > Administration
 - > System
 - Deployment
 - Licensing
 - > Certificates
 - > Certificate Manage
 - System Certificates
 - Trusted Certificates

The 'Permissions for Menu Access' section has two radio buttons: 'Show' (selected) and 'Hide'.

Para configurar a política de acesso a dados, navegue para **Administração > Sistema > Acesso de administração > Autorização > Permissões > Acesso a dados**.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE', 'Administration • System', and 'Evaluation Mode 7!'. The main menu on the left lists 'Authentication', 'Authorization', 'Permissions', 'Menu Access', 'Data Access', 'RBAC Policy', 'Administrators', and 'Settings'. The 'Data Access' section is active, displaying a table of existing permissions. Above the table are buttons for 'Edit', '+ Add', 'Duplicate', and '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.

Clique em **Adicionar** para criar uma nova política e configurar permissões para acessar Admin/User Identity/Endpoint Identity/Network Groups.

The screenshot shows the 'Create Data Access Permission' form in the Cisco ISE Administration console. The form has a 'Name' field with the value 'Custom_Data_Access' and an empty 'Description' field. Below the form is a 'Data Access Privileges' section with a tree view of groups. The 'RegisteredDevices' group is selected. To the right, there are radio buttons for 'Full Access' (selected), 'Read Only Access', and 'No Access'.

Data Access Privileges

- > Admin Groups
- > User Identity Groups
- > Endpoint Identity Groups
 - Blacklist
 - GuestEndpoints
 - RegisteredDevices
 - Unknown
 - > Profiled
 - > Network Device Groups

Permissions for Data Access

- Full Access
- Read Only Access
- No Access

Configurar políticas de RBAC

RBAC significa Role-Based Access Control (Controle de acesso baseado em função). A função

(Grupo Admin) à qual um usuário pertence pode ser configurada para usar as políticas desejadas de Menu e Acesso a Dados. Pode haver várias políticas RBAC configuradas para uma única função OU várias funções podem ser configuradas em uma única política para acessar Menu e/ou Dados. Todas essas políticas aplicáveis são avaliadas quando um usuário administrador tenta executar uma ação. A decisão final é o conjunto de todas as políticas aplicáveis a essa função. Se existirem regras contraditórias que permitem e negam ao mesmo tempo, a regra de permissão substitui a regra de negação. Para configurar essas políticas, navegue para **Administration > System > Admin Access > Authorization > RBAC Policy**.

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is Administration > System > Admin Access > Authorization > RBAC Policy. The left sidebar contains a navigation menu with options: Authentication, Authorization (selected), Permissions, RBAC Policy, Administrators, and Settings. The main content area displays a table of RBAC Policies. Above the table, there is a note: "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). 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)."

Rule Name	Admin Groups	Permissions	Actions
<input checked="" type="checkbox"/> Customization Admin Policy	If Customization Admin	+ then Customization Admin Menu ...	+ Actions
<input checked="" type="checkbox"/> Elevated System Admin Policy	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 Access...	+ 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

Clique em **Ações** para Duplicar/Inserir/Excluir uma diretiva.

Note: As políticas criadas pelo sistema e padrão não podem ser atualizadas, e as políticas padrão não podem ser excluídas.

Note: Não é possível configurar várias permissões de Acesso a Dados/Menu em uma única regra.

Definir configurações para acesso de administrador

Além das políticas de RBAC, há algumas configurações que podem ser configuradas comuns a todos os usuários admin.

Para configurar o número máximo de sessões permitidas, pré-login e banners pós-login para GUI e CLI, navegue para **Administration > System > Admin Access > Settings > Access**. Configure-os na guia **Sessão**.

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

Authentication
 Authorization >
 Administrators >
 Settings ▾
 Access
 Session
 Portal Customization

Session IP Access MnT Access

GUI Sessions

Maximum Concurrent Sessions: 10 (Valid Range 1 to 20)

Pre-login banner

Welcome to ISE

Post-login banner

CLI Sessions

Maximum Concurrent Sessions: 5 (Valid Range 1 to 10)

Pre-login banner

Para configurar a lista de endereços IP dos quais a GUI e a CLI podem ser acessadas, navegue para **Administration > System > Admin Access > Settings > Access** e navegue até a guia **IP Access**.

Cisco ISE Administration • System

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

Authentication
 Authorization >
 Administrators >
 Settings ▾
 Access
 Session
 Portal Customization

Session **IP Access** MnT Access

▼ 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	MASK
<input type="checkbox"/>	10.9.8.0	24

Para configurar uma lista de nós a partir dos quais os administradores podem acessar a seção MnT no Cisco ISE, navegue até **Administração > Sistema > Acesso de Administrador > Configurações > Acesso** e navegue até a guia **Acesso MnT**.

Para permitir que nós ou entidades dentro ou fora da implantação enviem syslogs para MnT,

clique no botão de opção **Allow any IP address to connect to MNT**. Para permitir que apenas nós ou entidades na implantação enviem syslogs para MnT, clique em **Permitir que somente os nós na implantação se conectem ao botão de opção MNT**.

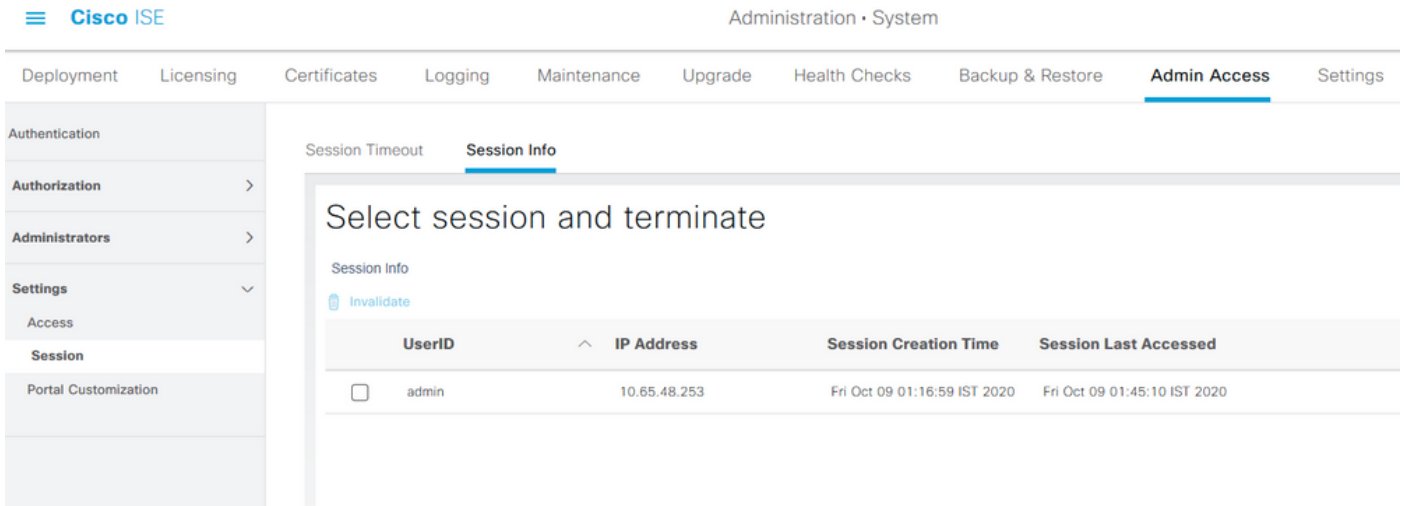
The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration • System' and a menu with options: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, and Admin Access. The 'Admin Access' tab is selected. On the left, a sidebar menu shows 'Authentication', 'Authorization', 'Administrators', and 'Settings' (expanded to show 'Access', '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'.

Note: Para o ISE 2.6 patch 2 e posterior, o uso do "ISE Messaging Service" para a entrega de Syslogs UDP ao MnT é ativado por padrão, o que não permite syslogs provenientes de outras entidades fora da implantação.

Para configurar um valor de tempo limite devido à inatividade de uma sessão, navegue para **Administração > Sistema > Acesso de Administrador > Configurações > Sessão**. Defina esse valor na guia **Session Timeout**.

The screenshot shows the Cisco ISE Administration interface for the 'Session Timeout' configuration. The top navigation bar is the same as in the previous screenshot. The 'Admin Access' tab is selected. The left sidebar menu is the same, with 'Settings' expanded to 'Session'. The main content area has two tabs: 'Session Timeout' (selected) and 'Session Info'. Under the 'Session Timeout' tab, there is a configuration field for 'Session Idle Timeout' set to '60' minutes, with a note '(Valid Range 6 to 100)'. The field is a text input with a dropdown arrow on the right.

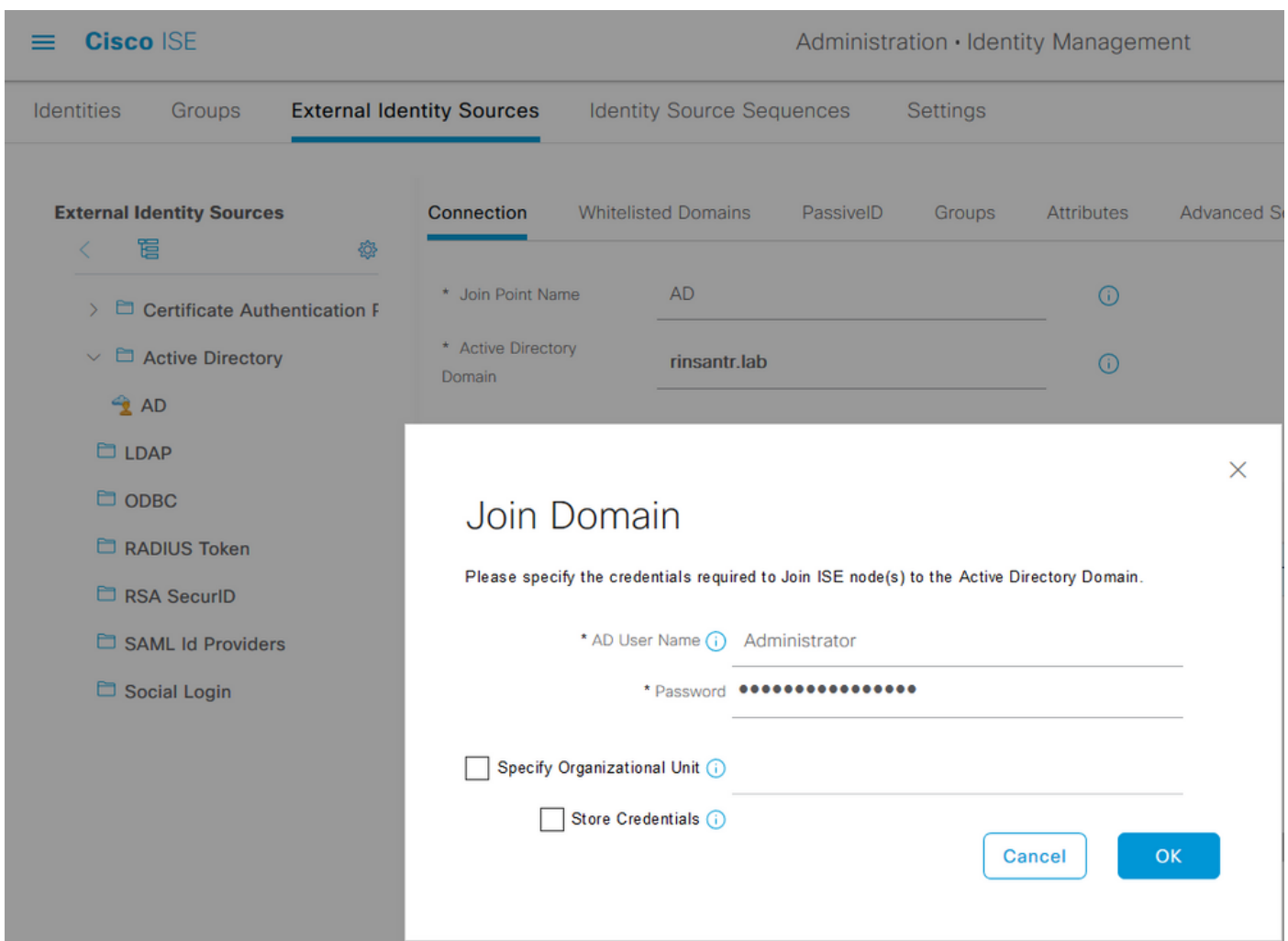
Para visualizar/invalidar as sessões ativas atuais, navegue para **Administração > Acesso de Administrador > Configurações > Sessão** e clique na guia **Informações da Sessão**.



Configurar o acesso do portal administrativo com credenciais do AD

Participe do ISE para o AD

Para ingressar no ISE em um domínio externo, navegue para **Administration > Identity Management > External Identity Sources > Active Directory**. Insira o novo nome do ponto de junção e o domínio do active directory. Insira as credenciais da conta do AD que pode adicionar e fazer alterações em objetos de computador e clique em **OK**.



Connection Whitelisted Domains PassiveID Groups Attributes Advanced Settings

* Join Point Name AD ⓘ

* Active Directory Domain rinsantr.lab ⓘ

+ Join + Leave 👤 Test User 🔧 Diagnostic Tool ↻ Refresh Table

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

Selecionar grupos de diretórios

Navegue até **Administration > Identity Management > External Identity Sources > Ative Diretory**. Clique no nome do ponto de união desejado e navegue até a guia **Grupos**. Clique em **Adicionar > Selecionar grupos em Diretório > Recuperar grupos**. Importe pelo menos um grupo AD ao qual o administrador pertence, clique em **OK** e em **Salvar**.

Identity Sources

Connection

Edit +

Na

No data availa

Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

Name Filter * SID * Type Filter ALL

50 Groups Retrieved.

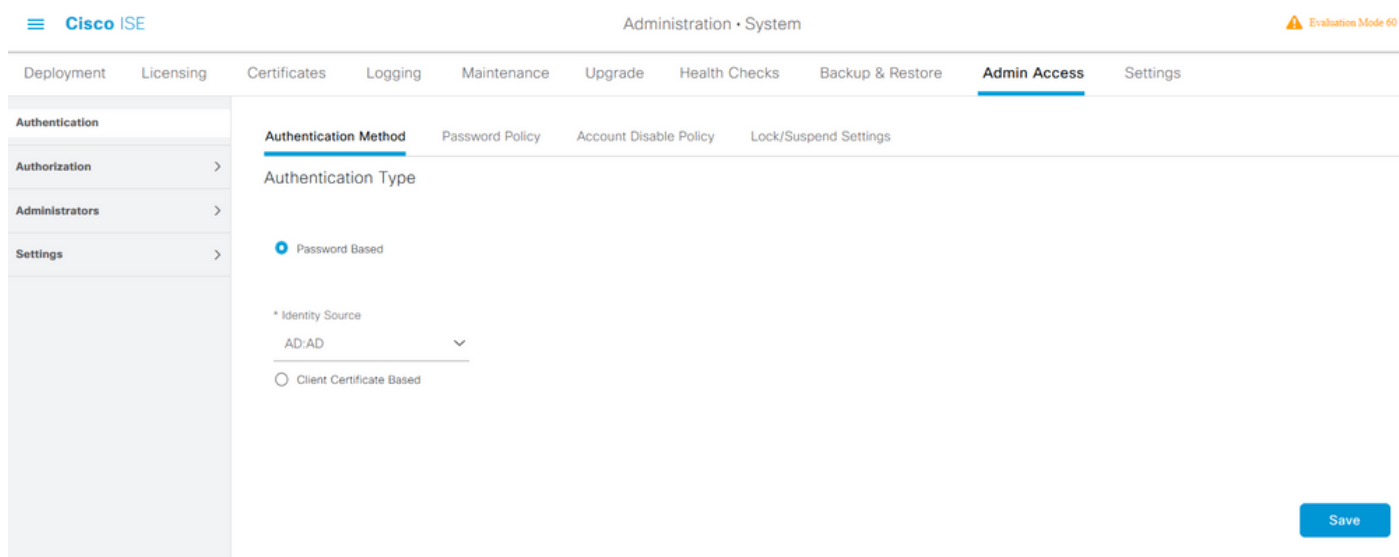
<input type="checkbox"/>	Name	Group SID	Group Type
<input type="checkbox"/>	rinsantr.lab/Users/Enterprise Key Admins	S-1-5-21-1977851106-3699455990-29458652...	UNIVERSAL
<input type="checkbox"/>	rinsantr.lab/Users/Enterprise Read-only Domain ...	S-1-5-21-1977851106-3699455990-29458652...	UNIVERSAL
<input 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

[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 acesso administrativo para AD

Para habilitar a autenticação baseada em senha do ISE usando o AD, navegue para **Administration > System > Admin Access > Authentication (Administração > Sistema > Acesso de Administrador > Autenticação)**. Na guia **Authentication Method**, selecione a opção **Password-Based**. Selecione **AD** no menu suspenso **Origem da identidade** e clique em **Salvar**.



Configurar o grupo administrativo do ISE para o mapeamento de grupo do AD

Isso permite autorização para determinar as permissões RBAC (Role Based Access Control, Controle de Acesso Baseado em Função) para o administrador com base na associação de grupo no AD. Para definir um grupo de administração do Cisco ISE e mapeá-lo para um grupo do AD, navegue para **Administration > System > Admin Access > Administrators > Admin Groups**. Clique em **Adicionar** e insira um nome para o novo grupo Admin. No campo Tipo, marque a caixa de seleção **Externo**. No menu suspenso **Grupos externos**, selecione o grupo do AD ao qual esse Grupo de administração deve ser mapeado (conforme definido na seção **Selecionar grupos de diretórios** acima). **Envie** as alterações.

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

* +

Member Users

Users

+ Add Delete

<input type="checkbox"/>	Status	Email	Username	First Name	Last Name
No data available					

Definir permissões RBAC para o grupo de administração

Para atribuir permissões de RBAC ao Grupo Admin criado na seção anterior, navegue para **Administration > System > Admin Access > Authorization > RBAC Policy**. No menu suspenso **Ações** à direita, selecione **Inserir nova política**. Crie uma nova regra, mapeie-a com o grupo de administração definido na seção acima, atribua-a com os dados desejados e as permissões de acesso ao menu e clique em **Salvar**.

Cisco ISE Administration • System

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

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 elements) and other ci 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 Men... + Actions
<input checked="" type="checkbox"/> RBAC Policy 1	If ISE AD Admin Group	+ then Super Admin Menu Acces... X Actions
<input checked="" type="checkbox"/> Elevated System Admin Poli	If Elevated System Admin	+ then
<input checked="" type="checkbox"/> ERS Admin Policy	If ERS Admin	+ then
<input checked="" type="checkbox"/> ERS Operator Policy	If ERS Operator	+ then

Super Admin Menu Access +

Super Admin Data Access +

Acesse o ISE com credenciais do AD e verifique

Fazer logoff da GUI administrativa. Selecione o nome do ponto de junção no menu suspenso **Origem da identidade**. Insira o nome de usuário e a senha do banco de dados do AD e faça logon.



Identity Services Engine

Intuitive network security

Username
TestUser

Password
●●●●●●●●

Identity Source
AD

Login

Para confirmar se a configuração funciona corretamente, verifique o nome de usuário autenticado no ícone **Settings (Configurações)** no canto superior direito da GUI do ISE. Navegue até **Informações do servidor** e verifique o Nome de usuário.

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

Configurar o acesso do portal administrativo com LDAP

Ingressar ISE em LDAP

Navegue até **Administration > Identity Management > External Identity Sources > Ative Directory > LDAP**. Na guia **Geral**, insira um nome para o LDAP e escolha o esquema como **Ative 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 ▼

Em seguida, para configurar o tipo de conexão, navegue até a guia **Conexão**. Aqui, defina o nome de host/IP do servidor LDAP principal junto com a porta 389(LDAP)/636 (LDAP-Secure). Insira o caminho do DN (nome distinto) do administrador com a senha de administrador do servidor LDAP.

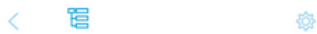
- ▼  Active Directory
 -  AD
 -  LDAP
 -  ODBC
 -  RADIUS Token
 -  RSA SecurID
 -  SAML Id Providers
 -  Social Login

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="text" value="*"/>	Password	<input type="text"/>
Secure Authentication	<input type="checkbox"/> Enable Secure Authentication	Secure Authentication	<input type="checkbox"/> Enable Secure Authentication

Em seguida, navegue até a guia **Directory Organization** e clique em **Naming Context** para escolher o grupo de organização correto do usuário com base na hierarquia de usuários armazenados no servidor LDAP.

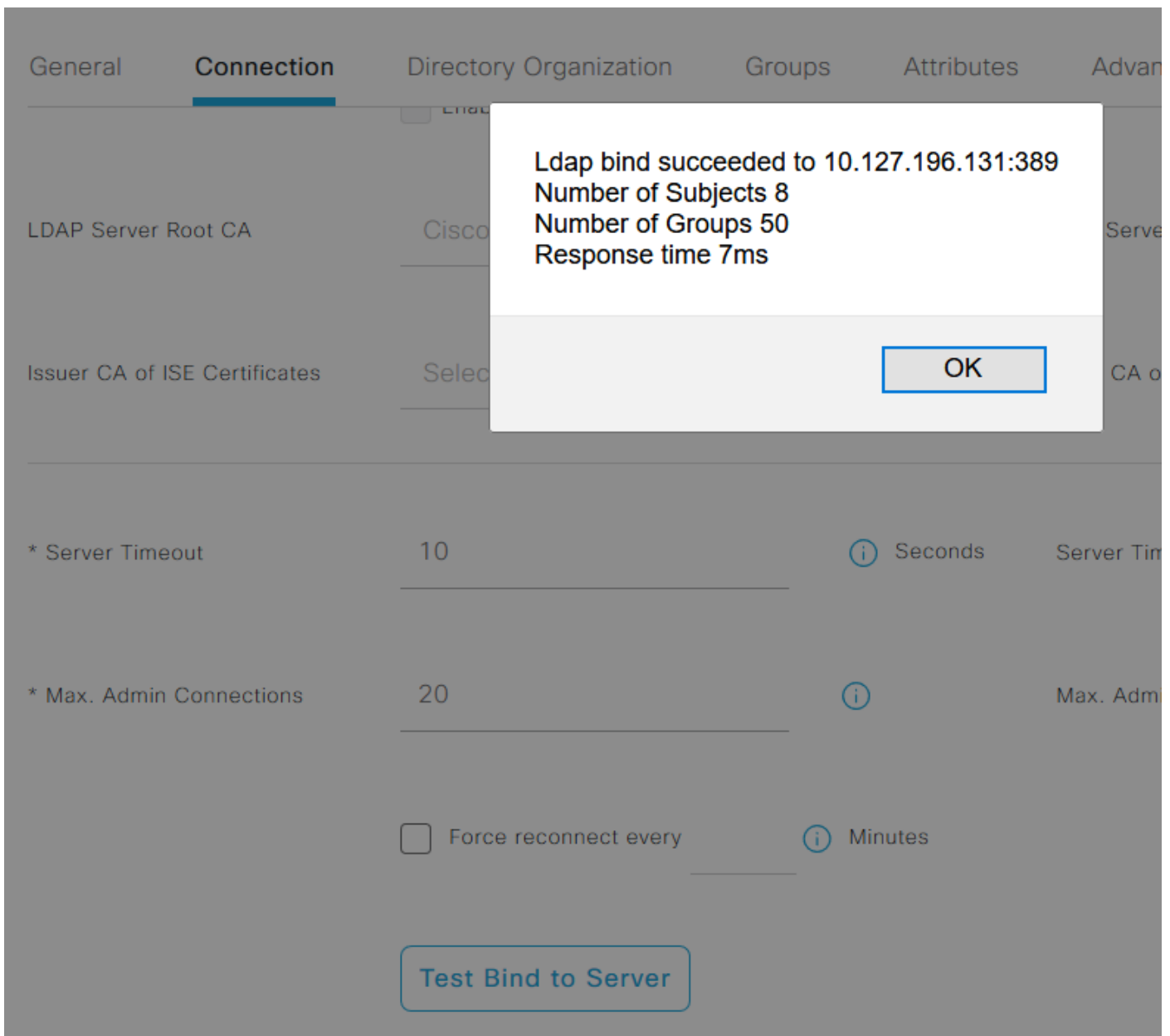
External Identity Sources

[Certificate Authentication F](#)[Active Directory](#)[AD](#)[LDAP](#)[ODBC](#)[RADIUS Token](#)[RSA SecurID](#)[SAML Id Providers](#)[Social Login](#)[LDAP Identity Sources List](#) > LDAPExample

LDAP Identity Source

General Connection **Directory Organization** Groups Attributes Advanced Settings* Subject Search Base DC=rinsantr,DC=lab [Naming Contexts...](#) ⓘ* Group Search Base DC=rinsantr,DC=lab [Naming Contexts...](#) ⓘSearch for MAC Address in Format ▼ 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

Clique em **Test Bind to Server** na guia **Connection** para testar a acessibilidade do servidor LDAP do ISE.



Agora, navegue até a guia **Grupos** e clique em **Adicionar > Selecionar grupos do diretório > Recuperar grupos**. Importe pelo menos um grupo ao qual o administrador pertence, clique em **OK** e em **Salvar**.

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




Internal Identity Sources

- <  
- > Certificate Authentication F
- > Active Directory
- ✓ LDAP
 -  LDAPExample
 - ODBC
 - RADIUS Token
 - RSA SecurID

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 acesso administrativo para usuários LDAP

Para habilitar a autenticação baseada em senha do ISE usando LDAP, navegue para **Administration > System > Admin Access > Authentication** (Administração > Sistema > Acesso de Administrador > Autenticação). Na guia **Authentication Method**, selecione a opção **Password-Based**. Selecione **LDAP** no menu suspenso **Origem da identidade** e clique em **Salvar**.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration - System' and 'Evaluation Mode 60 Days'. The main navigation menu has 'Admin Access' selected. The left sidebar shows 'Authentication' selected. The main content area is titled 'Authentication Method' and 'Authentication Type'. The 'Password Based' radio button is selected. Below it, the 'Identity Source' dropdown is set to 'LDAP:LDAPExample|'. There is also an unselected 'Client Certificate Based' radio button. A 'Save' button is located at the bottom right.

Mapear o grupo de administração do ISE para o grupo LDAP

Isso permite que o usuário configurado obtenha acesso de Administrador com base na autorização das políticas de RBAC, que por sua vez se baseia na associação de grupo LDAP do usuário. Para definir um grupo de administração do Cisco ISE e mapeá-lo para um grupo LDAP, navegue para **Administration > System > Admin Access > Administrators > Admin Groups**. Clique em **Adicionar** e insira um nome para o novo grupo Admin. No campo Tipo, marque a caixa de seleção **Externo**. No menu suspenso **Grupos externos**, selecione o grupo LDAP para o qual esse grupo de administração deve ser mapeado (como recuperado e definido anteriormente). **Envie** as alterações.

The screenshot shows the Cisco ISE Administration interface for creating a new admin group. The top navigation bar includes 'Administration - System'. The main navigation menu has 'Admin Access' selected. The left sidebar shows 'Admin Groups' selected. The main content area is titled 'Admin Group' and 'New Admin Group'. The 'Name' field is 'ISE LDAP Admin Group'. The 'Description' field is empty. The 'Type' is set to 'External' (checked). The 'External Identity Source' is 'LDAPExample'. The 'External Groups' section shows a dropdown menu with 'CN=Test Group,CN=Users,DC=' selected. A 'Save' button is located at the bottom right.

Definir permissões RBAC para o grupo de administração

Para atribuir permissões de RBAC ao Grupo Admin criado na seção anterior, navegue para **Administration > System > Admin Access > Authorization > RBAC Policy**. No menu suspenso **Ações** à direita, selecione **Inserir nova política**. Crie uma nova regra, mapeie-a com o grupo de administração definido na seção acima, atribua-a com os dados desejados e as permissões de

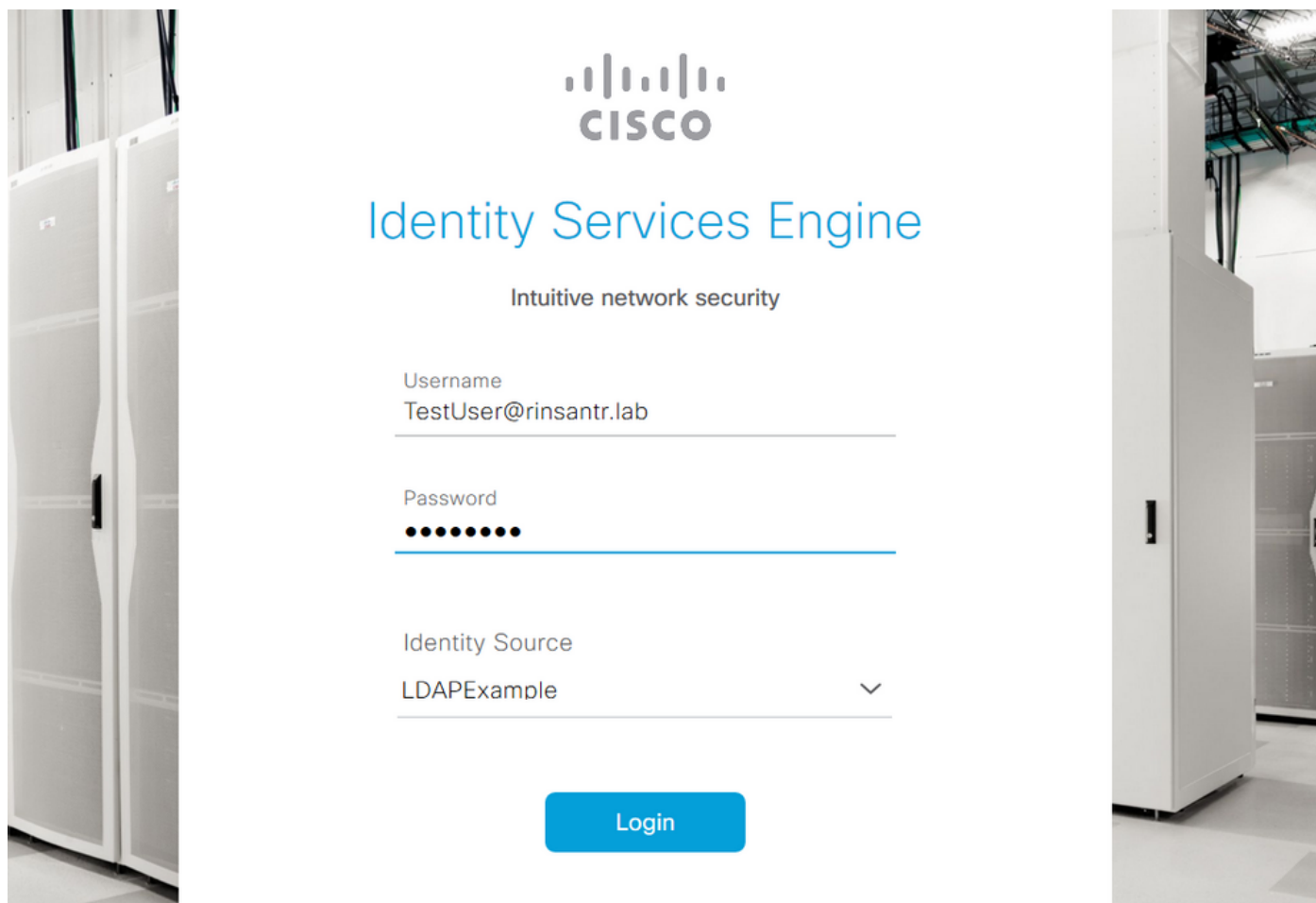
acesso ao menu e clique em **Salvar**.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration · System' and an 'Evaluate' button. The left sidebar contains menu items: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, **Admin Access**, and Set. The main content area is titled 'RBAC Policies' and contains a table of policies. A dropdown menu is open over the 'Super Admin Menu Access' permission, showing options like 'Super Admin Menu Access' and 'Read Only Admin Data Access'.

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
Maintenance Admin Policy	Maintenance Admin	Maintenance Admin Menu Access

Acesse o ISE com credenciais LDAP e verifique

Fazer logoff da GUI administrativa. Selecione o nome LDAP no menu suspenso **Origem da identidade**. Insira o nome de usuário e a senha do banco de dados LDAP e faça login.



Para confirmar se a configuração funciona corretamente, verifique o nome de usuário autenticado no ícone **Configurações** no canto superior direito da GUI do ISE. Navegue até **Informações do**

servidor e verifique o Nome de usuário.

Dashboard

Guests

Acti

Beha

NDPC

Pr

Failure Re

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