

# Comprendre les politiques d'accès administrateur et RBAC sur ISE

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Paramètres d'authentification](#)

[Configurer les groupes d'administration](#)

[Configurer les utilisateurs admin](#)

[Configurer les autorisations](#)

[Configurer les stratégies RBAC](#)

[Configuration des paramètres d'accès administrateur](#)

[Configurer l'accès au portail Admin avec les informations d'identification AD](#)

[Rejoindre ISE à AD](#)

[Sélectionner des groupes de répertoires](#)

[Activer l'accès administratif pour AD](#)

[Configurer le mappage du groupe d'administration ISE sur le groupe AD](#)

[Définir les autorisations RBAC pour le groupe Admin](#)

[Accéder à ISE avec les identifiants AD et vérifier](#)

[Configurer l'accès au portail Admin avec LDAP](#)

[Rejoindre ISE à LDAP](#)

[Activer l'accès administratif pour les utilisateurs LDAP](#)

[Mapper le groupe d'administration ISE au groupe LDAP](#)

[Définir les autorisations RBAC pour le groupe Admin](#)

[Accéder à ISE avec les informations d'identification LDAP et vérifier](#)

## Introduction

Ce document décrit les fonctionnalités d'ISE pour gérer l'accès administratif sur ISE (Identity Services Engine).

## Conditions préalables

### Conditions requises

Cisco vous recommande de connaître ces sujets :

- ISE
- Active Directory

- LDAP (Lightweight Directory Access Protocol)

## Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

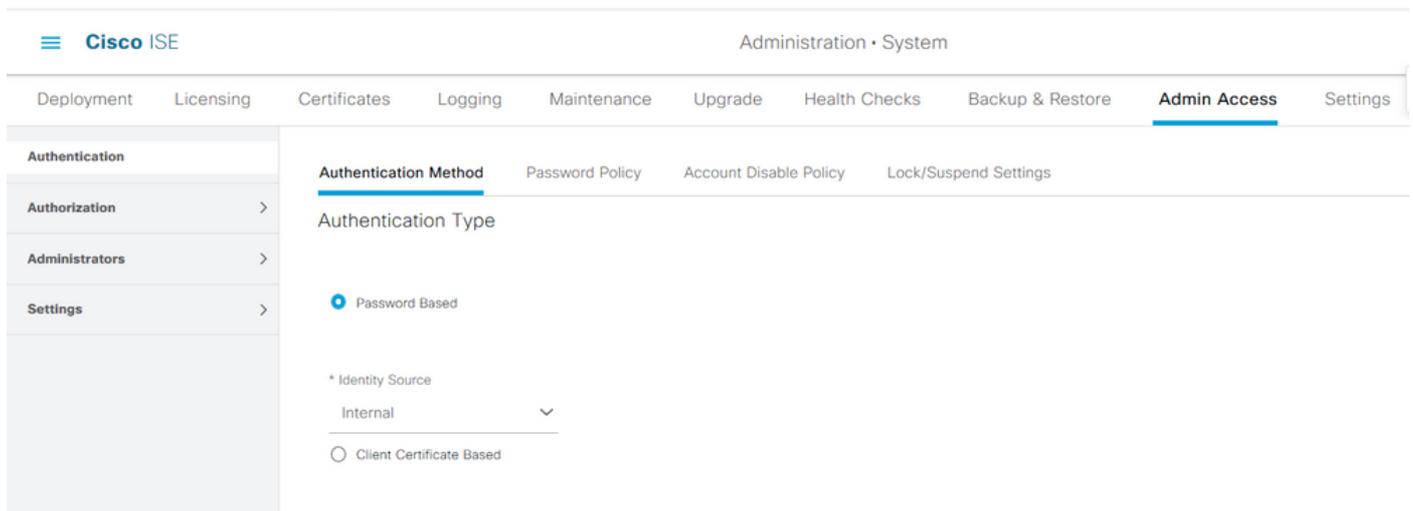
- Identity Services Engine 3.0
- Windows Server 2016

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Configuration

### Paramètres d'authentification

Les utilisateurs admin doivent s'authentifier pour accéder à toute information sur ISE. L'identité des utilisateurs admin peut être vérifiée à l'aide du magasin d'identités internes ISE ou d'un magasin d'identités externes. L'authenticité peut être vérifiée par un mot de passe ou un certificat. Afin de configurer ces paramètres, accédez à **Administration > System > Admin Access > Authentication**. Sélectionnez le type d'authentification requis sous l'onglet **Authentication Method**.



**Note:** L'authentification basée sur le mot de passe est activée par défaut. Si l'authentification basée sur le certificat client est modifiée, cela entraîne le redémarrage d'un serveur d'applications sur tous les noeuds de déploiement.

Identity Services Engine ne permet pas de configurer la stratégie de mot de passe pour l'interface de ligne de commande (CLI) à partir de l'interface de ligne de commande. La stratégie de mot de passe de l'interface graphique utilisateur (GUI) et de l'interface de ligne de commande ne peut être configurée que via l'interface utilisateur graphique d'ISE. Afin de configurer ceci, accédez à **Administration > System > Admin Access > Authentication** et accédez à l'onglet **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)

ISE dispose d'une provision pour désactiver un utilisateur administrateur inactif. Afin de configurer ceci, accédez à **Administration > System > Admin Access > Authentication** et accédez à l'onglet **Account Disable Policy**.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb trail 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)'.

ISE permet également de verrouiller ou de suspendre un compte d'utilisateur administrateur en fonction du nombre de tentatives de connexion ayant échoué. Afin de configurer ceci, accédez à **Administration > System > Admin Access > Authentication** et accédez à l'onglet **Lock/Suspend Settings**.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb trail 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.'

Pour gérer l'accès administratif, il est nécessaire que les groupes administratifs, les utilisateurs et les différentes politiques/règles contrôlent et gèrent leurs privilèges.

## Configurer les groupes d'administration

Accédez à **Administration > System > Admin Access > Administrators > Admin Groups** pour configurer les groupes d'administrateurs. Il y a peu de groupes intégrés par défaut et ne peuvent pas être supprimés.

- 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 ...

Une fois qu'un groupe est créé, sélectionnez-le et cliquez sur modifier pour ajouter des utilisateurs administratifs à ce groupe. Il existe une disposition permettant de mapper les groupes d'identité externes aux groupes d'administration sur ISE afin qu'un utilisateur d'administration externe obtienne les autorisations requises. Afin de configurer ceci, sélectionnez le type Externe lors de l'ajout de l'utilisateur.

- 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

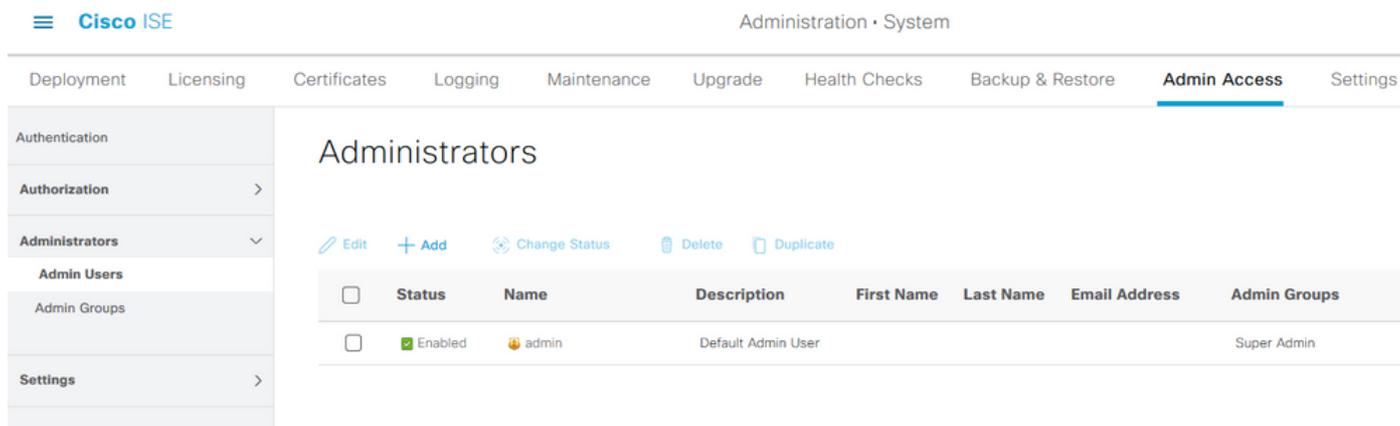
Users

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

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

## Configurer les utilisateurs admin

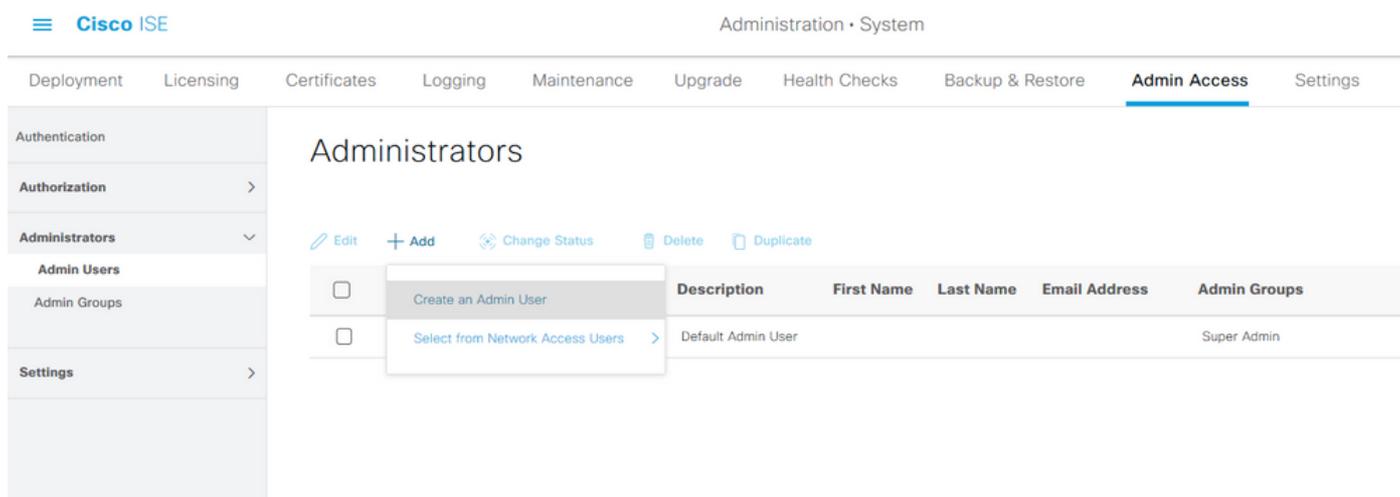
Afin de configurer les utilisateurs Admin, accédez à **Administration > System > Admin Access > Administrators > Admin Users**.



The screenshot shows the Cisco ISE Administration console. The navigation menu includes Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, **Admin Access**, and Settings. The left sidebar shows the navigation tree with 'Admin Users' selected. The main content area is titled 'Administrators' and contains a table of admin users.

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

Cliquez sur **Add**. Deux options s'offrent à vous. L'une consiste à ajouter un nouvel utilisateur. L'autre est de faire un utilisateur d'accès au réseau (c'est-à-dire un utilisateur configuré en tant qu'utilisateur interne pour accéder au réseau/aux périphériques) en tant qu'administrateur ISE.



The screenshot shows the Cisco ISE Administration console with the 'Add' dropdown menu open. The menu options are 'Create an Admin User' and 'Select from Network Access Users'. The table below shows the 'Default Admin User' with status 'Enabled' and group 'Super Admin'.

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

Une fois que vous avez sélectionné une option, les détails requis doivent être fournis et le groupe d'utilisateurs doit être sélectionné en fonction duquel les autorisations et privilèges sont accordés à l'utilisateur.

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

## Configurer les autorisations

Deux types d'autorisations peuvent être configurés pour un groupe d'utilisateurs :

1. Accès au menu
2. Accès aux données

Menu Access contrôle la visibilité de navigation sur ISE. Il existe deux options pour chaque onglet, Afficher ou Masquer, qui peuvent être configurées. Une règle d'accès au menu peut être configurée pour afficher ou masquer les onglets sélectionnés.

Data Access contrôle la capacité à lire/accéder/modifier les données d'identité sur ISE. L'autorisation d'accès ne peut être configurée que pour les groupes d'administration, les groupes d'identité d'utilisateur, les groupes d'identité de point de terminaison et les groupes de périphériques réseau. Il existe trois options pour ces entités sur ISE qui peuvent être configurées. Il s'agit de l'accès complet, de l'accès en lecture seule et de l'absence d'accès. Une règle d'accès aux données peut être configurée pour choisir l'une de ces trois options pour chaque onglet de l'ISE.

Les stratégies d'accès aux menus et d'accès aux données doivent être créées avant de pouvoir

être appliquées à n'importe quel groupe d'administrateurs. Il existe quelques stratégies intégrées par défaut, mais elles peuvent toujours être personnalisées ou une nouvelle peut être créée.

Afin de configurer une stratégie d'accès au menu, accédez à **Administration > System > Admin Access > Authorization > Permissions > Menu Access**.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb path is Administration > System > Admin Access > Authorization > Permissions > Menu Access. The left sidebar is expanded to show the 'Menu Access' section under 'Permissions'. The main content area displays a table of permissions 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

Cliquez sur **Add**. Chaque option de navigation dans ISE peut être configurée pour être affichée/masquée dans une stratégie.

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

Menu Access List > New RBAC Menu Access

### Create Menu Access Permission

\* Name:

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

Afin de configurer la stratégie d'accès aux données, accédez à **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

### 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.

Cliquez sur **Add** pour créer une nouvelle stratégie et configurer les autorisations d'accès aux groupes Admin/User Identity/Endpoint Identity/Network.

Authentication

**Authorization** ▾

**Permissions** ▾

Menu Access

**Data Access**

RBAC Policy

**Administrators** >

**Settings** >

### Create Data Access Permission

\* Name

Description

#### 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

## Configurer les stratégies RBAC

RBAC est l'acronyme de Role-Based Access Control. Le rôle (groupe d'administration) auquel appartient un utilisateur peut être configuré pour utiliser les stratégies Menu et Accès aux données souhaitées. Plusieurs stratégies RBAC peuvent être configurées pour un seul rôle OU plusieurs rôles peuvent être configurés dans une seule stratégie pour accéder au menu et/ou aux données. Toutes ces stratégies applicables sont évaluées lorsqu'un utilisateur admin tente d'exécuter une action. La décision finale est l'ensemble de toutes les politiques applicables à ce rôle. S'il existe des règles contradictoires qui autorisent et refusent en même temps, la règle d'autorisation remplace la règle de refus. Pour configurer ces stratégies, accédez à **Administration > System > Admin Access > Authorization > RBAC Policy**.

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

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). 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).

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 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

Cliquez sur **Actions** pour dupliquer/Insérer/Supprimer une stratégie.

**Note:** Les stratégies créées par le système et les stratégies par défaut ne peuvent pas être mises à jour et les stratégies par défaut ne peuvent pas être supprimées.

**Note:** Impossible de configurer plusieurs autorisations d'accès aux menus/données dans une seule règle.

## Configuration des paramètres d'accès administrateur

Outre les stratégies RBAC, il existe quelques paramètres qui peuvent être configurés et qui sont communs à tous les utilisateurs admin.

Afin de configurer le nombre maximal de sessions autorisées, de sessions préalables et de bannières postérieures à la connexion pour l'interface utilisateur graphique et l'interface de ligne de commande, accédez à **Administration > System > Admin Access > Settings > Access**. Configurez-les sous l'onglet **Session**.

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

Pour configurer la liste des adresses IP à partir desquelles l'interface utilisateur graphique et l'interface de ligne de commande sont accessibles, accédez à **Administration > System > Admin Access > Settings > Access** et accédez à l'onglet **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

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

Pour configurer une liste de noeuds à partir desquels les administrateurs peuvent accéder à la section MnT de Cisco ISE, accédez à **Administration > System > Admin Access > Settings > Access** et accédez à l'onglet **MnT Access**.

Pour autoriser les noeuds ou les entités du déploiement ou en dehors du déploiement à envoyer

des syslogs à MnT, cliquez sur la case d'option **Autoriser toute adresse IP à se connecter à MNT**. Pour autoriser uniquement les noeuds ou entités du déploiement à envoyer des syslogs à MnT, cliquez sur la case d'option **Autoriser uniquement les noeuds du déploiement à se connecter à MNT**.

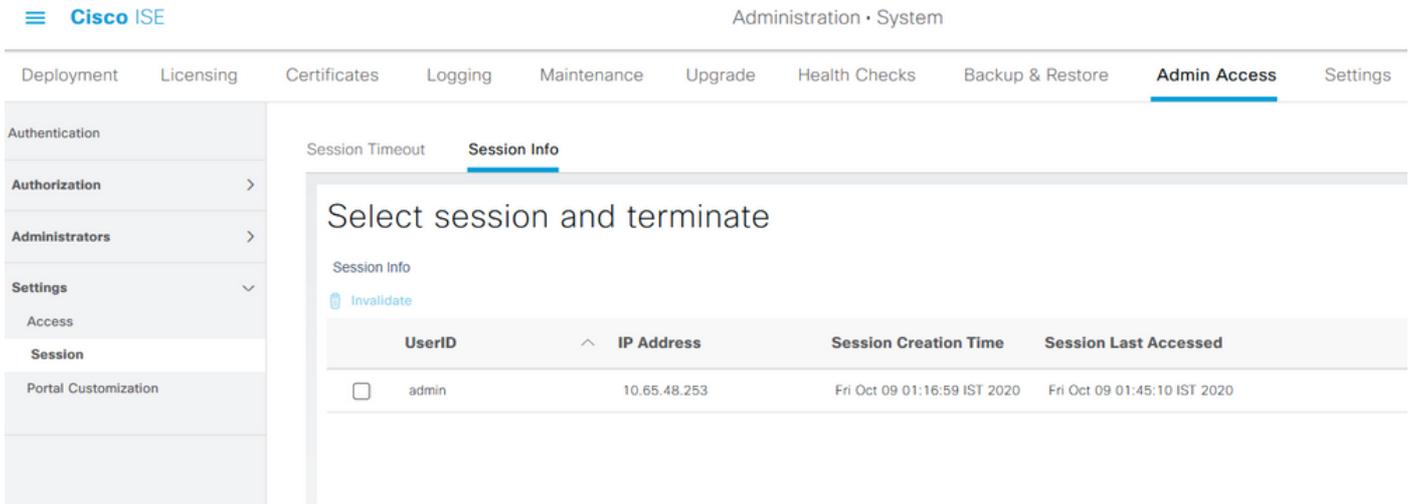
The screenshot shows the Cisco ISE Administration interface. The breadcrumb path is Administration > System > Admin Access. The 'Admin Access' tab is selected. Under 'MnT Access', the 'MnT Access Restriction' section is expanded, showing two radio button options: 'Allow any IP address to connect to MNT' (which is selected) and 'Allow only the nodes in the deployment to connect to MNT'. A left-hand navigation menu is visible with categories like Authentication, Authorization, Administrators, and Settings.

**Note:** Pour le correctif 2.6 ISE et versions ultérieures, *utilisez « ISE Messaging Service » pour la livraison des Syslogs UDP à MnT* est activée par défaut, ce qui n'autorise pas les Syslogs provenant d'autres entités en dehors du déploiement.

Afin de configurer une valeur de délai d'attente en raison de l'inactivité d'une session, accédez à **Administration > System > Admin Access > Settings > Session**. Définissez cette valeur sous l'onglet **Temporisation de session**.

The screenshot shows the Cisco ISE Administration interface. The breadcrumb path is Administration > System > Admin Access > Settings > Session. The 'Session Timeout' tab is selected. A configuration field for 'Session Idle Timeout' is visible, set to '60 minutes (Valid Range 6 to 100)'. A left-hand navigation menu is visible with categories like Authentication, Authorization, Administrators, and Settings.

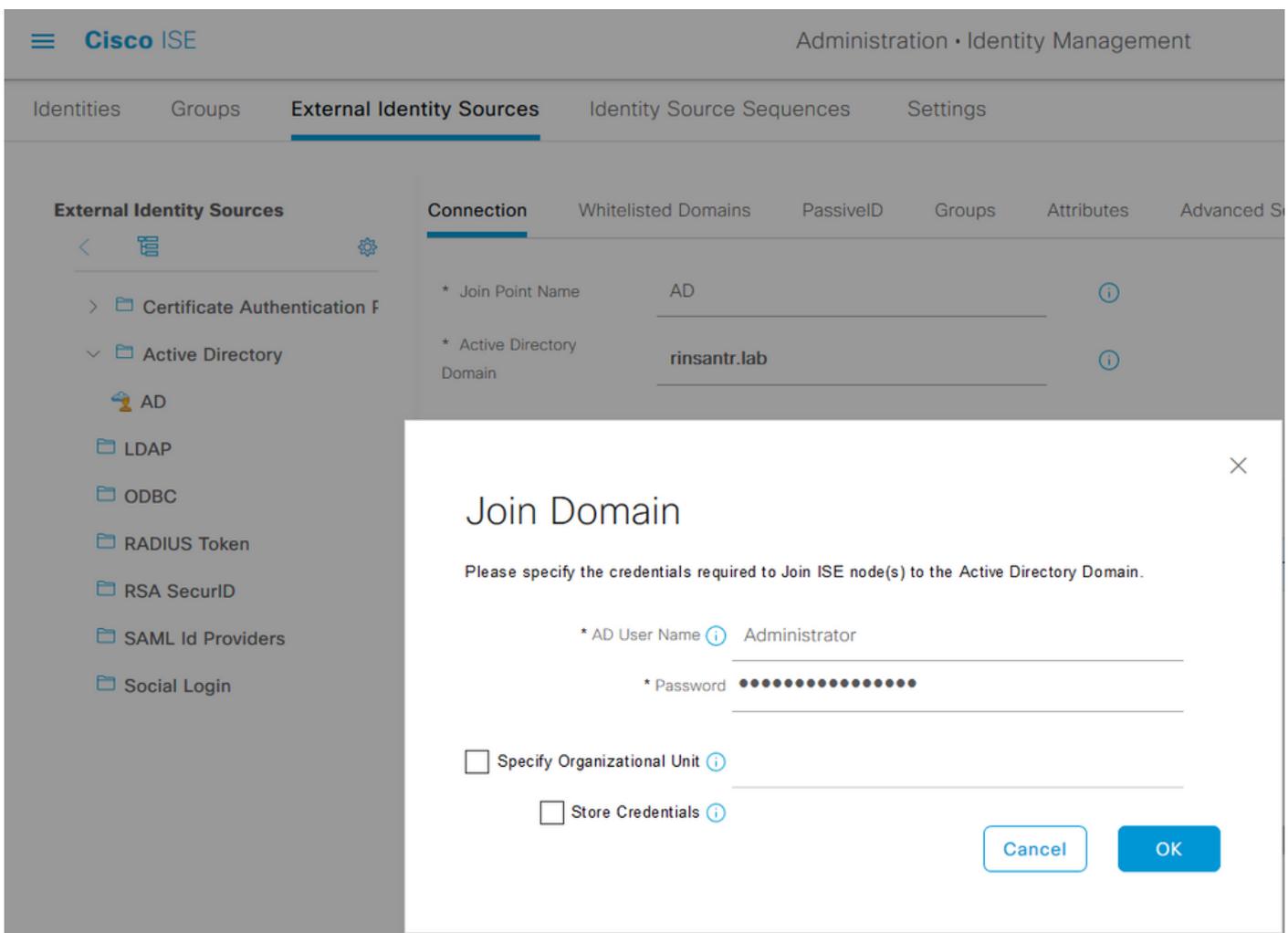
Afin d'afficher/d'invalider les sessions actives en cours, accédez à **Administration > Admin Access > Settings > Session** et cliquez sur l'onglet **Session Info**.



## Configurer l'accès au portail Admin avec les informations d'identification AD

### Rejoindre ISE à AD

Pour rejoindre ISE à un domaine externe, accédez à **Administration > Identity Management > External Identity Sources > Active Directory**. Entrez le nouveau nom de point de jointure et le domaine Active Directory. Entrez les informations d'identification du compte AD qui peut ajouter et apporter des modifications aux objets de l'ordinateur, puis cliquez sur **OK**.



[Connection](#)
[Whitelisted Domains](#)
[PassiveID](#)
[Groups](#)
[Attributes](#)
[Advanced Settings](#)

\* Join Point Name  ⓘ

\* Active Directory Domain  ⓘ

[+ 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

## Sélectionner des groupes de répertoires

Accédez à **Administration > Identity Management > External Identity Sources > Active Directory**. Cliquez sur le nom du point de jointure souhaité et accédez à l'onglet **Groupes**. Cliquez sur **Add > Select Groups from Directory > Retrieve Groups**. Importez au moins un groupe AD auquel votre administrateur appartient, puis cliquez sur **OK**, puis sur **Enregistrer**.

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

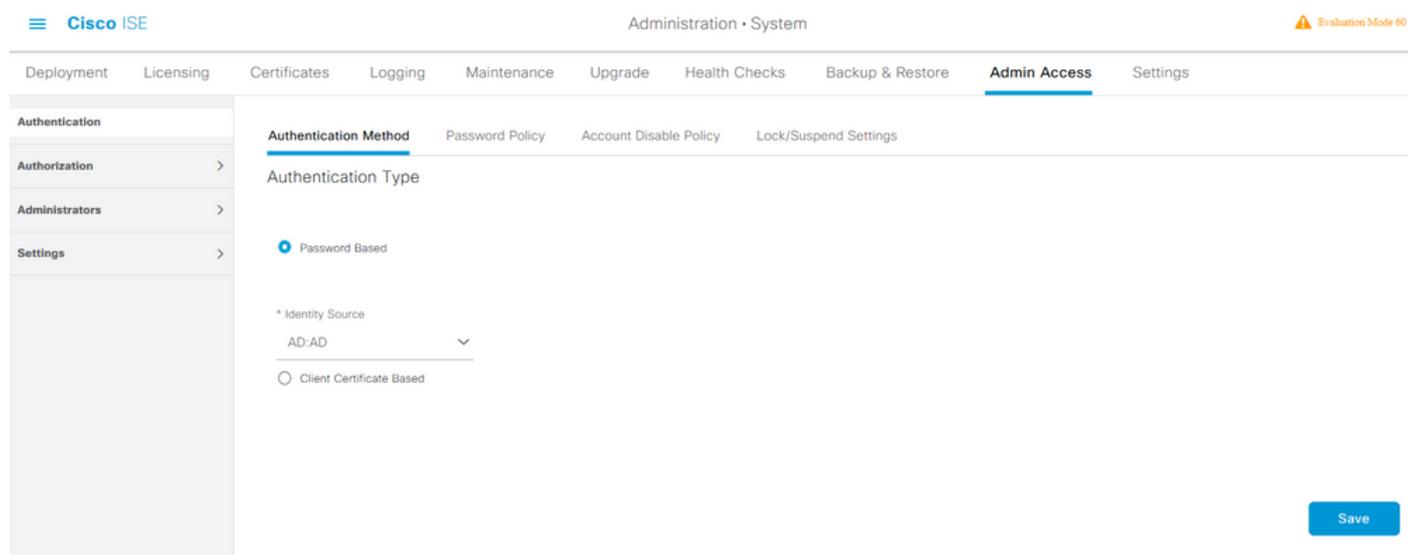
<input type="checkbox"/>	Name	Group SID	Group Type
<input type="checkbox"/>	rinsantr.lab/Users/Enterprise Key Admins	S-1-5-21-1977851106-3699455990-29458652...	UNIVERSAL
<input type="checkbox"/>	rinsantr.lab/Users/Enterprise Read-only Domain ...	S-1-5-21-1977851106-3699455990-29458652...	UNIVERSAL
<input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

## Activer l'accès administratif pour AD

Afin d'activer l'authentification basée sur un mot de passe d'ISE à l'aide d'AD, accédez à **Administration > System > Admin Access > Authentication**. Dans l'onglet **Authentication Method**, sélectionnez l'option **Password-Based**. Sélectionnez **AD** dans le menu déroulant **Source d'identité** et cliquez sur **Enregistrer**.



## Configurer le mappage du groupe d'administration ISE sur le groupe AD

Cela permet d'autoriser la détermination des autorisations RBAC (Role Based Access Control) pour l'administrateur en fonction de l'appartenance au groupe dans AD. Pour définir un groupe d'administrateurs Cisco ISE et le mapper à un groupe AD, accédez à **Administration > System > Admin Access > Administrators > Admin Groups**. Cliquez sur **Add** et saisissez un nom pour le nouveau groupe Admin. Dans le champ Type, cochez la case **Externe**. Dans le menu déroulant **Groupes externes**, sélectionnez le groupe AD auquel ce groupe d'administration doit être mappé (tel que défini dans la section Sélectionner les groupes de répertoires ci-dessus). **Soumettez** les modifications.

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					

## Définir les autorisations RBAC pour le groupe Admin

Pour attribuer des autorisations RBAC au groupe d'administration créé dans la section précédente, accédez à **Administration > System > Admin Access > Authorization > RBAC Policy**. Dans le menu déroulant **Actions** à droite, sélectionnez **Insérer une nouvelle stratégie**. Créez une nouvelle règle, mappez-la avec le groupe d'administrateurs défini dans la section ci-dessus, puis affectez-la avec les autorisations d'accès aux données et au menu souhaitées, puis cliquez sur **Enregistrer**.

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 c 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

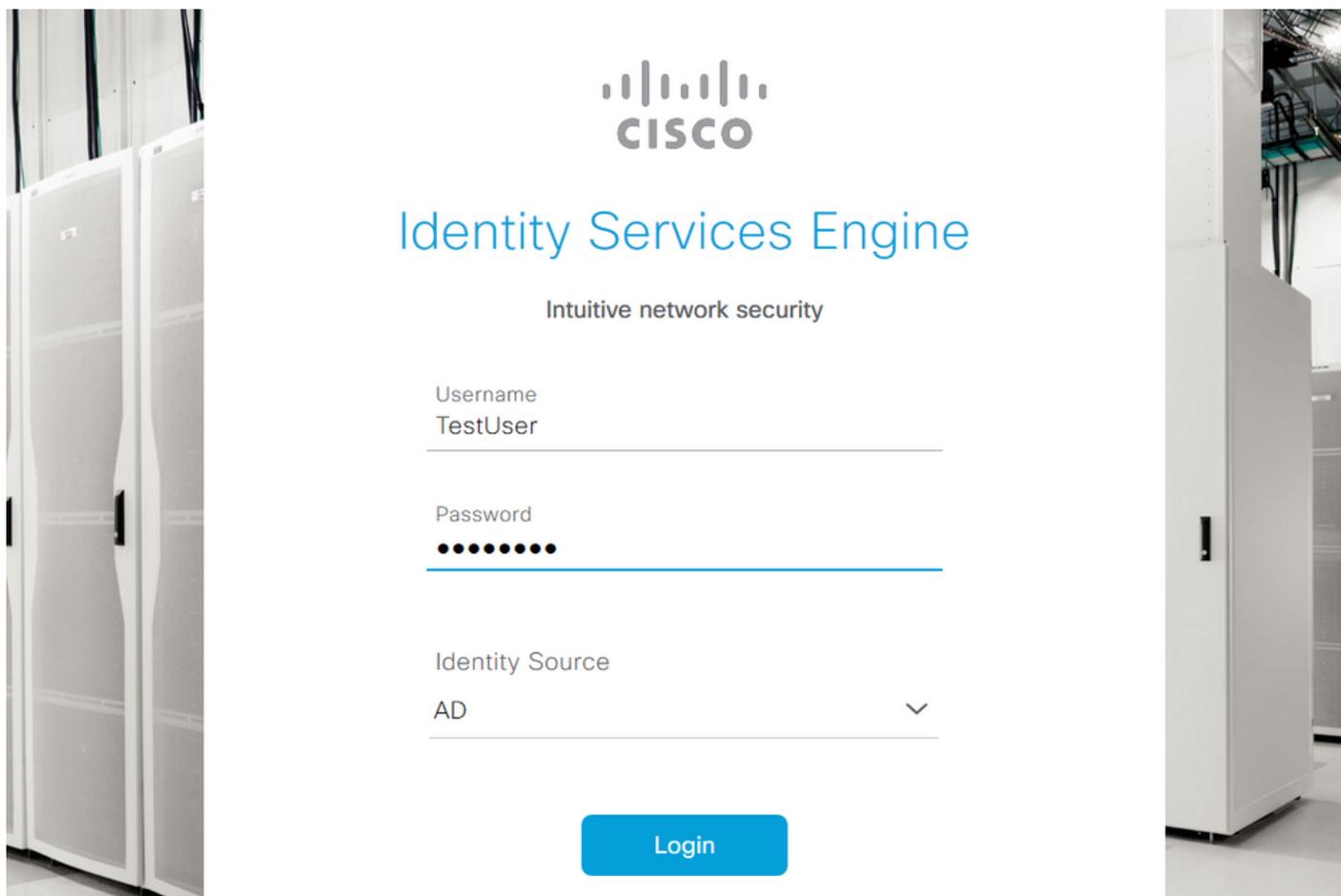
Super Admin Menu Access  +

Super Admin Data Access  +

## Accéder à ISE avec les identifiants AD et vérifier

Déconnectez-vous de l'interface utilisateur graphique d'administration. Sélectionnez le nom du point de jointure dans le menu déroulant **Source d'identité**. Saisissez le nom d'utilisateur et le mot

de passe de la base de données AD, puis connectez-vous.



  
**Identity Services Engine**  
Intuitive network security

Username  
TestUser

Password  
●●●●●●●●

Identity Source  
AD

Login

Pour vérifier que la configuration fonctionne correctement, vérifiez le nom d'utilisateur authentifié à partir de l'icône **Paramètres** dans le coin supérieur droit de l'interface utilisateur graphique ISE. Accédez à **Informations sur le serveur** et vérifiez le nom d'utilisateur.

## 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

## Configurer l'accès au portail Admin avec LDAP

### Rejoindre ISE à LDAP

Accédez à **Administration > Identity Management > External Identity Sources > Active Directory > LDAP**. Sous l'onglet **Général**, entrez un nom pour LDAP et choisissez le schéma en tant qu'**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  ▼

Ensuite, pour configurer le type de connexion, accédez à l'onglet **Connexion**. Définissez ici le nom d'hôte/l'adresse IP du serveur LDAP principal avec le port 389(LDAP)/636 (LDAP-Secure). Entrez le chemin d'accès du nom unique d'administrateur (DN) avec le mot de passe d'administrateur du serveur 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 password"="" type="password" value="* .....&lt;/td&gt; &lt;td&gt;Password&lt;/td&gt; &lt;td&gt;&lt;input type="/>		
Secure Authentication	<input type="checkbox"/> Enable Secure Authentication	Secure Authentication	<input type="checkbox"/> Enable Secure Authentication

Ensuite, accédez à l'onglet **Organisation du répertoire** et cliquez sur **Contextes de noms** pour choisir le groupe d'organisations correct de l'utilisateur en fonction de la hiérarchie des utilisateurs stockés dans le serveur LDAP.

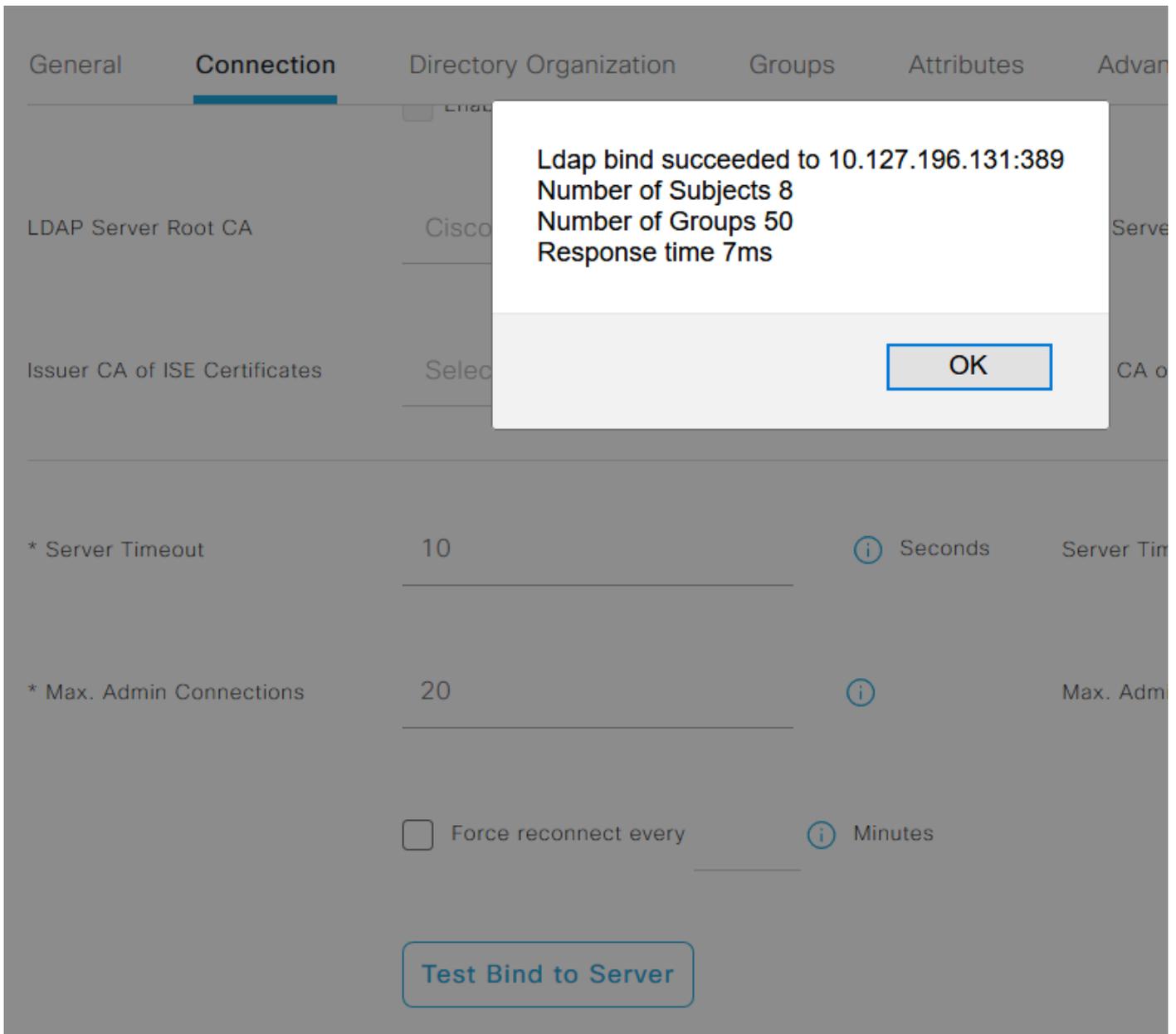
## External Identity Sources

[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 

Cliquez sur **Test Bind to Server** sous l'onglet **Connection** pour tester l'accessibilité du serveur LDAP à partir d'ISE.



Accédez maintenant à l'onglet **Groupes** et cliquez sur **Ajouter > Sélectionner des groupes dans le répertoire > Récupérer des groupes**. Importez au moins un groupe auquel votre administrateur appartient, puis cliquez sur **OK**, puis sur **Enregistrer**.

## 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

## Activer l'accès administratif pour les utilisateurs LDAP

Afin d'activer l'authentification basée sur un mot de passe d'ISE à l'aide de LDAP, accédez à **Administration > System > Admin Access > Authentication**. Dans l'onglet **Authentication Method**, sélectionnez l'option **Password-Based**. Sélectionnez **LDAP** dans le menu déroulant **Source d'identité** et cliquez sur **Enregistrer**.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, **Admin Access**, and Settings. The left sidebar has: Authentication, Authorization, Administrators, and Settings. The main content area is titled 'Authentication Method' and includes sub-tabs: Password Policy, Account Disable Policy, and Lock/Suspend Settings. Under 'Authentication Type', the 'Password Based' radio button is selected. Below it, the 'Identity Source' dropdown menu is set to 'LDAP:LDAPExample|'. The 'Client Certificate Based' radio button is unselected. A blue 'Save' button is located at the bottom right of the configuration area.

## Mapper le groupe d'administration ISE au groupe LDAP

Cela permet à l'utilisateur configuré d'obtenir l'accès Administrateur en fonction de l'autorisation des stratégies RBAC, qui à son tour est basé sur l'appartenance au groupe LDAP de l'utilisateur. Pour définir un groupe d'administrateurs Cisco ISE et le mapper à un groupe LDAP, accédez à **Administration > System > Admin Access > Administrators > Admin Groups**. Cliquez sur **Add** et saisissez un nom pour le nouveau groupe Admin. Dans le champ Type, cochez la case **Externe**. Dans le menu déroulant **Groupes externes**, sélectionnez le groupe LDAP auquel ce groupe d'administration doit être mappé (tel que récupéré et défini précédemment). **Soumettez** les modifications.

The screenshot shows the Cisco ISE Administration console for the 'Admin Groups' configuration. The top navigation bar is the same as in the previous screenshot. The left sidebar has: Authentication, Authorization, Administrators (with a dropdown arrow), and Settings. The main content area is titled 'Admin Groups > New Admin Group'. The 'Admin Group' configuration form includes: 'Name' field with 'ISE LDAP Admin Group', an empty 'Description' field, 'Type' with the 'External' checkbox checked, and 'External Identity Source' with 'Name : LDAPExample'. Below this, there is a section for 'External Groups' with a dropdown menu showing 'CN=Test Group,CN=Users,DC=' and a plus sign to add more groups.

## Définir les autorisations RBAC pour le groupe Admin

Pour attribuer des autorisations RBAC au groupe d'administration créé dans la section précédente, accédez à **Administration > System > Admin Access > Authorization > RBAC Policy**. Dans le menu déroulant **Actions** à droite, sélectionnez **Insérer une nouvelle stratégie**. Créez une nouvelle règle, mappez-la avec le groupe d'administrateurs défini dans la section ci-dessus, puis

affectez-la avec les autorisations d'accès aux données et au menu souhaitées, puis cliquez sur **Enregistrer**.

The screenshot shows the Cisco ISE Administration System interface. The top navigation bar includes 'Administration · System' and an 'Evaluate' button. The main navigation menu has 'Admin Access' selected. The left sidebar shows 'Authentication', 'Authorization', 'Permissions', 'RBAC Policy', 'Administrators', and 'Settings'. 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 'Super Admin Menu Access' permission, showing options like 'Super Admin Menu Access' and 'Read Only Admin Data Access'.

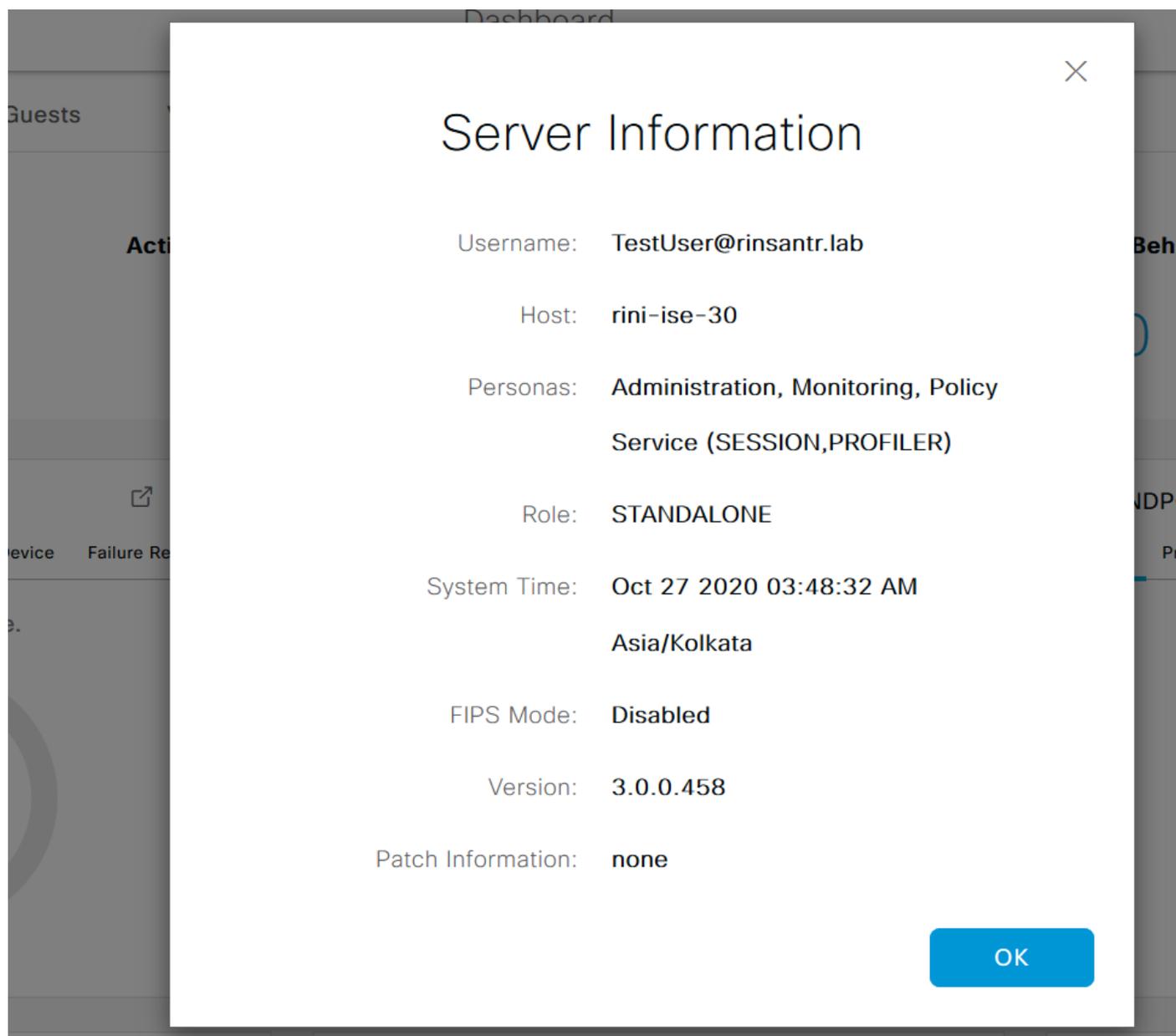
Rule Name	Admin Groups	Permissions
Customization Admin Policy	Customization Admin	Customization Admin Menu ...
RBAC Policy 2	ISE LDAP Admin Group	Super Admin Menu Access a...
Elevated System Admin Poli	Elevated System Admin	
ERS Admin Policy	ERS Admin	
ERS Operator Policy	ERS Operator	
ERS Trustsec Policy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

## Accéder à ISE avec les informations d'identification LDAP et vérifier

Déconnectez-vous de l'interface utilisateur graphique d'administration. Sélectionnez le nom LDAP dans le menu déroulant **Source d'identité**. Saisissez le nom d'utilisateur et le mot de passe de la base de données LDAP, puis connectez-vous.

The screenshot shows the Cisco Identity Services Engine login page. The page features the Cisco logo and the text 'Identity Services Engine' and 'Intuitive network security'. The login form includes fields for 'Username' (TestUser@rinsantr.lab), 'Password' (masked with dots), and 'Identity Source' (LDAPExample). A blue 'Login' button is at the bottom.

Afin de vérifier que la configuration fonctionne correctement, vérifiez le nom d'utilisateur authentifié à partir de l'icône **Paramètres** dans le coin supérieur droit de l'interface utilisateur graphique ISE. Accédez à **Informations sur le serveur** et vérifiez le nom d'utilisateur.



The screenshot shows a 'Server Information' dialog box overlaid on the ISE GUI. The dialog contains the following 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

An 'OK' button is located at the bottom right of the dialog.