

# 瞭解ISE上的管理員訪問許可權和RBAC策略

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[身份驗證設定](#)

[配置管理員組](#)

[配置管理員使用者](#)

[配置許可權](#)

[配置RBAC策略](#)

[配置管理員訪問許可權的設定](#)

[使用AD憑據配置管理員門戶訪問](#)

[將ISE加入AD](#)

[選擇目錄組](#)

[啟用AD的管理訪問](#)

[配置ISE管理員組到AD組的對映](#)

[設定管理員組的RBAC許可權](#)

[使用AD憑證訪問ISE並驗證](#)

[使用LDAP配置管理員門戶訪問](#)

[將ISE加入LDAP](#)

[為LDAP使用者啟用管理訪問](#)

[將ISE管理員組對映到LDAP組](#)

[設定管理員組的RBAC許可權](#)

[使用LDAP憑證訪問ISE並驗證](#)

## 簡介

本文檔介紹ISE的功能，用於管理身份服務引擎(ISE)上的管理訪問。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- ISE
- Active Directory
- 輕量型目錄存取通訊協定(LDAP)

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

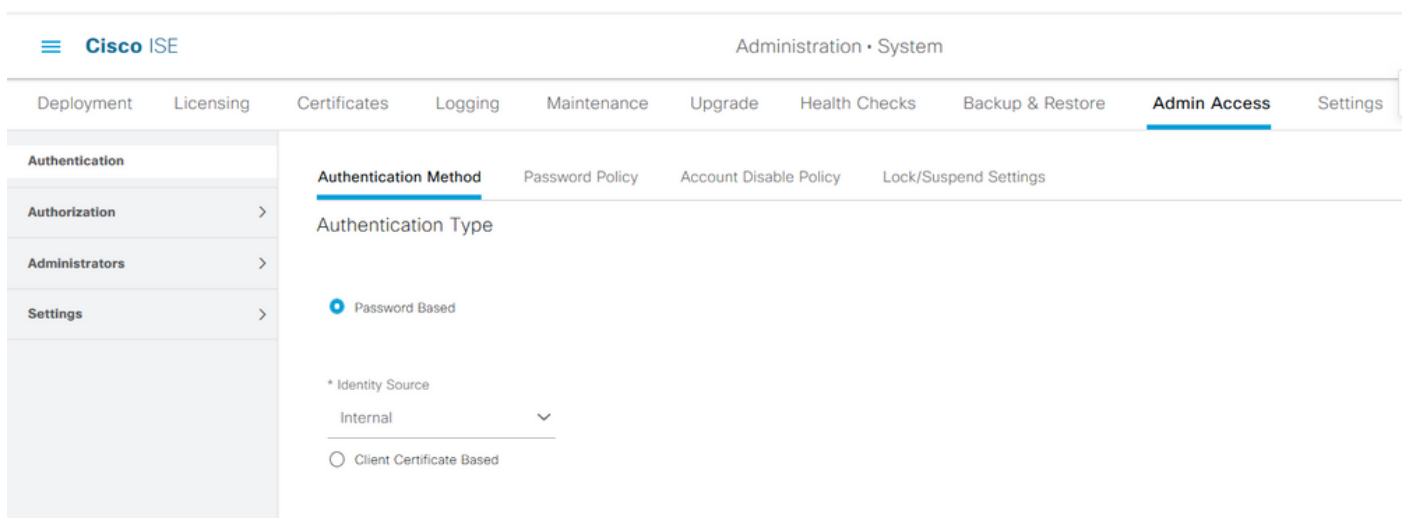
- 身分識別服務引擎3.0
- Windows Server 2016

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 設定

### 身份驗證設定

管理員使用者需要驗證自己才能訪問ISE上的任何資訊。管理員使用者的身份可通過ISE內部身份庫或外部身份庫進行驗證。可以通過密碼或證書來驗證真實性。要配置這些設定，請導航到**管理>系統>管理員訪問>身份驗證**。在**Authentication Method**頁籤下選擇所需的身份驗證型別。



**附註：**預設情況下啟用基於密碼的身份驗證。如果將其更改為基於客戶端證書的身份驗證，將導致應用程式伺服器在所有部署節點上重新啟動。

Identity Services Engine不允許從CLI為命令列介面(CLI)配置密碼策略。圖形使用者介面(GUI)和CLI的密碼策略只能通過ISE的GUI配置。若要配置此項，請導航到**Administration > System > Admin Access > Authentication**，然後導航到**Password Policy**頁籤。

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具有禁用非活動管理員使用者的設定。若要配置此項，請導航到Administration > System > Admin Access > Authentication，然後導航到Account Disable Policy頁籤。

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

ISE還提供根據登入嘗試失敗次數鎖定或暫停管理員使用者帳戶的工具。若要配置此功能，請導覽至Administration > System > Admin Access > Authentication，然後導覽至Lock/Suspend Settings索引標籤。

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration · System' and a warning icon. Below it, a menu bar contains 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', and 'Admin Access'. The left sidebar has 'Authentication', 'Authorization', 'Administrators', and 'Settings'. The main content area is titled 'Lock/Suspend Settings' and has sub-tabs for 'Authentication Method', 'Password Policy', 'Account Disable Policy', and 'Lock/Suspend Settings'. A checkbox is checked for 'Suspend or Lock Account with Incorrect Login Attempts'. 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' with the text: 'This account has been locked. For this account to become unlocked, please contact your IT helpdesk.'

要管理管理訪問，需要管理組、使用者和各種策略/規則來控制和管理其許可權。

## 配置管理員組

導航到Administration > System > Admin Access > Administrators > Admin Groups以配置管理員組。預設情況下，只有少陣列是內建的，無法刪除。

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

建立組後，選擇該組並按一下「編輯」將管理使用者新增到該組。存在將外部身份組對映到ISE上的管理員組的設定，以便外部管理員使用者獲得所需的許可權。要配置此型別，請在新增使用者時選擇型別為「外部」。

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

## Admin Groups > Super Admin

### Admin Group

\* Name

Description

Type  External

External Identity Source  
Name :

External Groups

\*

Member Users

Users

[+ Add](#)

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

## 配置管理員使用者

要配置管理員使用者，請導航到**管理>系統>管理員訪問許可權>管理員>管理員使用者**。

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 'Administrators' section expanded. The main content area is titled 'Administrators' and contains a table with the following data:

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

按一下「**Add**」。有兩種方法可以選擇。一種方法是完全新增新使用者。另一種方法是將網路訪問使用者（即配置為內部使用者以訪問網路/裝置的使用者）設定為ISE管理員。

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 'Super Admin' group.

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

選擇選項後，必須提供所需的詳細資訊，並且必須選擇使用者組，基於該使用者組授予使用者許可權和許可權。

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

## 配置許可權

可以為使用者組配置兩種型別的許可權：

1. 選單訪問
2. 資料存取

選單訪問控制ISE上的導航可見性。每個頁籤有兩個可配置的選項：「顯示」(Show)或「隱藏」(Hide)。可以配置選單訪問規則以顯示或隱藏選定的頁籤。

資料存取控制讀取/訪問/修改ISE上的身份資料的能力。只能為管理員組、使用者身份組、終端身份組和網路裝置組配置訪問許可權。ISE上有三個可以配置的實體選項。它們是「完全訪問」、「只讀訪問」和「無訪問」。可以配置資料存取規則為ISE上的每個頁籤選擇這三個選項之一。

必須先建立選單訪問和資料存取策略，然後才能將其應用於任何管理員組。有一些策略預設情況下是內建的，但可以始終對其進行自定義或建立新的策略。

要配置選單訪問策略，請導航到Administration > System > Admin Access > Authorization > Permissions > Menu Access。

- Authentication
- Authorization
- Permissions
  - Menu Access**
  - Data Access
  - RBAC Policy
- Administrators
- Settings

## Menu Access

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

<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

按一下「Add」。可以將ISE中的每個導航選項配置為在策略中顯示/隱藏。

- Authentication
- Authorization
- Permissions
  - Menu Access**
  - Data Access
  - RBAC Policy
- Administrators
- Settings

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

要配置資料存取策略，請導航到Administration > System > Admin Access > Authorization > Permissions > Data Access。



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.

按一下**Add**以建立新的策略並配置訪問管理員/使用者身份/終端身份/網路組的許可權。

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

Authentication

Authorization

Permissions

Menu Access

**Data Access**

RBAC Policy

Administrators

Settings

## Create 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

## 配置RBAC策略

RBAC代表基於角色的訪問控制。可以將使用者所屬的角色（管理員組）配置為使用所需的選單和資料存取策略。可以為單個角色配置多個RBAC策略，也可以在單個策略中配置多個角色以訪問選單和/或資料。當管理員使用者嘗試執行操作時，會評估所有這些適用的策略。最終決定是適用於該角色的所有策略的集合。如果同時存在允許和拒絕的衝突規則，則允許規則將覆蓋拒絕規則。要配置這些策略，請導航到Administration > System > Admin Access > Authorization > RBAC Policy。

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

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).

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 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

按一下 **Actions** 以複製/插入/刪除策略。

**附註：**無法更新系統建立的策略和預設策略，並且無法刪除預設策略。

**附註：**不能在單個規則中配置多個選單/資料存取許可權。

## 配置管理員訪問許可權的設定

除RBAC策略外，還可以配置一些對所有管理員使用者通用的設定。

要為GUI和CLI配置允許的最大會話數、登入前和登入後標語數，請導航到 **Administration > System > Admin Access > Settings > Access**。在 **Session** 頁籤下配置這些選項。

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

要配置可從中訪問GUI和CLI的IP地址清單，請導航到**Administration > System > Admin Access > Settings > Access**，然後導航到**IP Access**頁籤。

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

要配置管理員可從其訪問Cisco ISE的MnT部分的節點清單，請導航到**Administration > System > Admin Access > Settings > Access**，然後導航到**MnT Access**選項卡。

要允許部署內或部署外的節點或實體將系統日誌傳送到MnT，請按一下**Allow any IP address to connect to MNT**單選按鈕。要僅允許部署中的節點或實體將系統日誌傳送到MnT，請按一下**僅允許部署中的節點連線到MNT**單選按鈕。

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**

▼ MnT Access Restriction

Allow any IP address to connect to MNT

Allow only the nodes in the deployment to connect to MNT

**附註：**對於ISE 2.6補丁2及更高版本，預設情況下會啟用 *Use "ISE Messaging Service" for UDP Syslogs delivery to MnT*，這不允許來自部署外部任何其他實體的系統日誌。

要配置由於會話不活動而導致的超時值，請導航到 **Administration > System > Admin Access > Settings > Session**。在 **Session Timeout** 頁籤下設定此值。

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

Authentication

Authorization >

Administrators >

Settings >

Access

Session

Portal Customization

Session Timeout Session Info

\* Session Idle Timeout  minutes (Valid Range 6 to 100)

要檢視/使當前活動會話失效，請導航到 **Administration > Admin Access > Settings > Session**，然後點選 **Session Info** 選項卡。

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

Authentication

Authorization >

Administrators >

Settings >

Access

Session

Portal Customization

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

# 使用AD憑據配置管理員門戶訪問

## 將ISE加入AD

若要將ISE加入外部域，請導航到**管理>身份管理>外部身份源> Active Directory**。輸入新的加入點名稱和Active Directory域。輸入可以新增和更改電腦對象的AD帳戶的憑據，然後按一下**確定**。

The screenshot shows the Cisco ISE Administration console. The main navigation bar includes 'Administration • Identity Management'. The left sidebar shows 'External Identity Sources' with a tree view containing 'Certificate Authentication F', 'Active Directory', 'AD', 'LDAP', 'ODBC', 'RADIUS Token', 'RSA SecurID', 'SAML Id Providers', and 'Social Login'. The 'Active Directory' folder is expanded, and the 'AD' sub-item is selected. The main content area shows the 'Connection' tab for the selected source, with fields for 'Join Point Name' (AD) and 'Active Directory Domain' (rinsantr.lab). A 'Join Domain' dialog box is open in the foreground, titled 'Join Domain'. It contains the text: 'Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.' Below this are two input fields: '\* AD User Name' (Administrator) and '\* Password' (masked with dots). There are also two checkboxes: 'Specify Organizational Unit' and 'Store Credentials', both of which are unchecked. At the bottom right of the dialog are 'Cancel' and 'OK' buttons.

The screenshot shows the Cisco ISE Administration console, specifically the 'Connection' tab for the AD source. The main content area displays a table of ISE nodes. The table has the following columns: 'ISE Node', 'ISE Node R...', 'Status', 'Domain Controller', and 'Site'. There are also buttons for '+ Join', '+ Leave', 'Test User', 'Diagnostic Tool', and 'Refresh Table'.

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

## 選擇目錄組

導航到**管理>身份管理>外部身份源> Active Directory**。按一下所需的加入點名稱並導航到**組頁籤**。按一下**Add > Select Groups from Directory > Retrieve Groups**。至少匯入管理員所屬的一個AD組，然後按一下**確定**，然後按一下**儲存**。

Identity Sources

Connection

Edit +

Na

No data available

### Select Directory Groups

This dialog is used to select groups from the Directory.

Domain rinsantr.lab

Name Filter \* Retrieve Groups... SID Filter \* 50 Groups Retrieved. Type Filter ALL

<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

## 啟用AD的管理訪問

要使用AD啟用ISE的基於密碼的身份驗證，請導航到**Administration > System > Admin Access > Authentication**。在**Authentication Method**頁籤中，選擇**Password-Based**選項。從**Identity Source**下拉選單中選擇**AD**，然後按一下**Save**。

The screenshot shows the Cisco ISE Administration console. The breadcrumb trail is Administration > System > Admin Access. The left sidebar has Authentication selected. The main content area shows the Authentication Method configuration. The 'Password Based' radio button is selected. Below it, the 'Identity Source' dropdown is set to 'AD:AD'. There is a 'Save' button at the bottom right.

## 配置ISE管理員組到AD組的對映

這樣可授權基於AD中的組成員身份確定管理員的基於角色的訪問控制(RBAC)許可權。要定義Cisco ISE管理員組並將其對映到AD組，請導航到Administration > System > Admin Access > Administrators > Admin Groups。按一下Add，然後輸入新Admin組的名稱。在「型別」欄位中，選中External覈取方塊。從External Groups下拉選單中，選擇此管理員組要對映到的AD組（如上面的選擇目錄組部分中所定義）。提交更改。

The screenshot shows the Cisco ISE Administration console. The breadcrumb trail is Administration > System > Admin Access > Administrators > Admin Groups. The left sidebar has Admin Groups selected. The main content area shows the configuration for 'ISE AD Admin Group'. The 'Name' field contains 'ISE AD Admin Group'. The 'Type' dropdown is set to 'External'. The 'External Identity Source' is 'AD'. Under 'External Groups', there is a list with one entry: 'rinsantr.lab/Users/Test Group'. At the bottom, there is a table for 'Member Users' with columns for Status, Email, Username, First Name, and Last Name. The table is currently empty with the text 'No data available'.

## 設定管理員組的RBAC許可權

要將RBAC許可權分配給在上一部分中建立的管理員組，請導航到Administration > System > Admin Access > Authorization > RBAC Policy。從右側的Actions下拉選單中，選擇Insert new policy。建立一個新規則，將其與上面部分中定義的管理員組進行對映，然後為其分配所需的資料和選單訪問

許可權，然後按一下儲存。

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

## 使用AD憑證訪問ISE並驗證

從管理GUI註銷。從Identity Source下拉選單中選擇Join Point名稱。輸入AD資料庫中的使用者名稱和密碼，然後登入。

CISCO

Identity Services Engine

Intuitive network security

Username  
TestUser

Password  
●●●●●●●●

Identity Source  
AD

Login

要確認配置正常工作，請從ISE GUI右上角的Settings圖示驗證經過身份驗證的使用者名稱。導覽至Server Information，然後驗證使用者名稱。



## 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

## 使用LDAP配置管理員門戶訪問

### 將ISE加入LDAP

導航到**管理>身份管理>外部身份源> Active Directory > LDAP**。在**General**頁籤下，輸入LDAP的名稱，並選擇架構作為**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  ▼

接下來，要配置連線型別，請導航到**Connection**頁籤。在這裡，設定主LDAP伺服器的主機名/IP以及埠389(LDAP)/636(LDAP-Secure)。輸入管理員唯一判別名(DN)的路徑，並使用LDAP伺服器的管理員密碼。

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

General	<b>Connection</b>	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 text"="" type="text" 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		

接下來，導航到**Directory Organization**頁籤，然後按一下**Naming Contexts**，以根據LDAP伺服器中儲存的使用者層次結構選擇使用者的正確組織組。

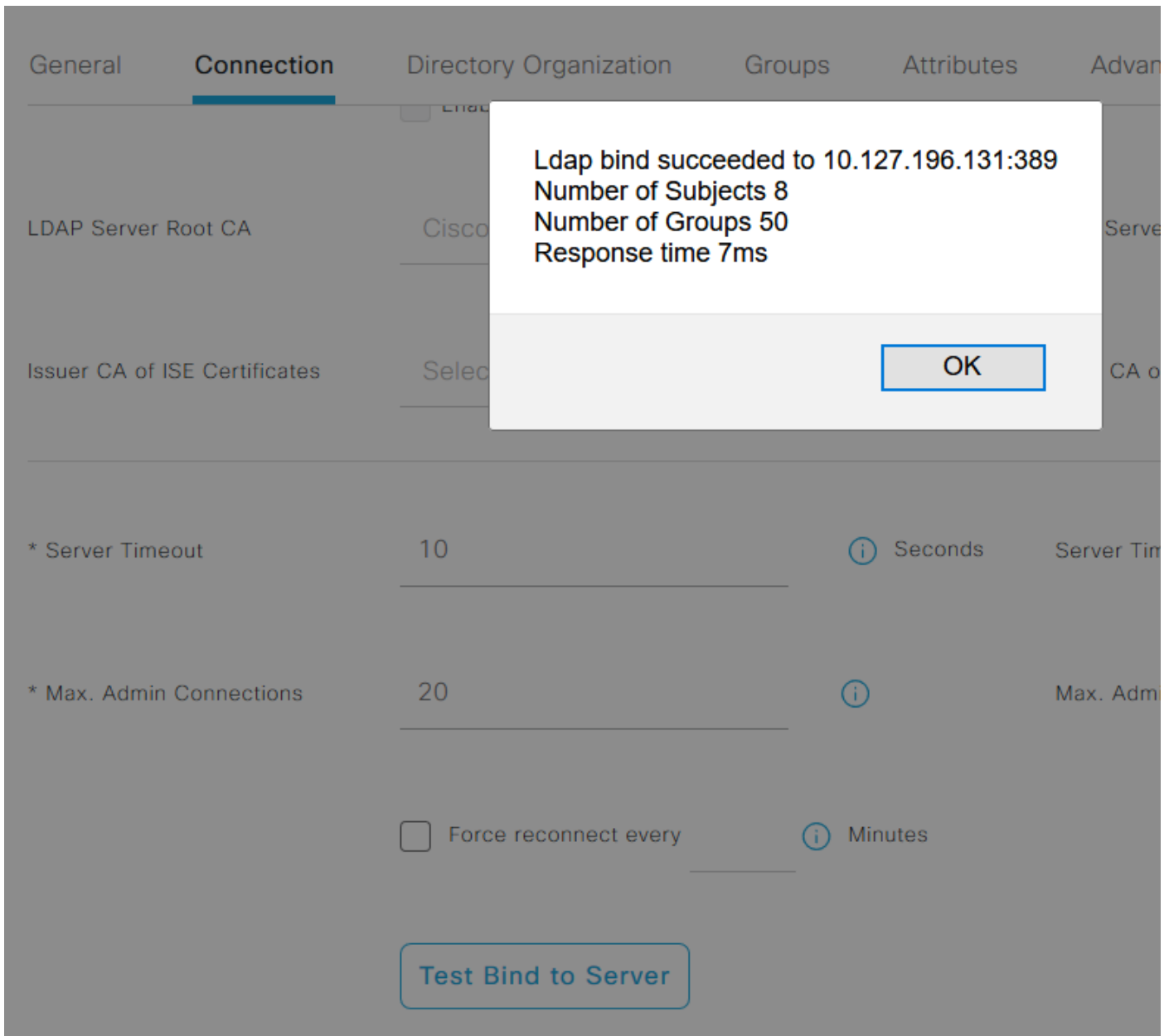
## External Identity Sources

[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 

按一下**Connection**頁籤下的**Test Bind to Server**，以測試從ISE訪問LDAP伺服器的能力。



現在，導航到**Groups**頁籤，然後按一下**Add > Select Groups From Directory > Retrieve Groups**。至少匯入一個管理員所屬的組，然後按一下**確定**，然後按一下**儲存**。

## 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

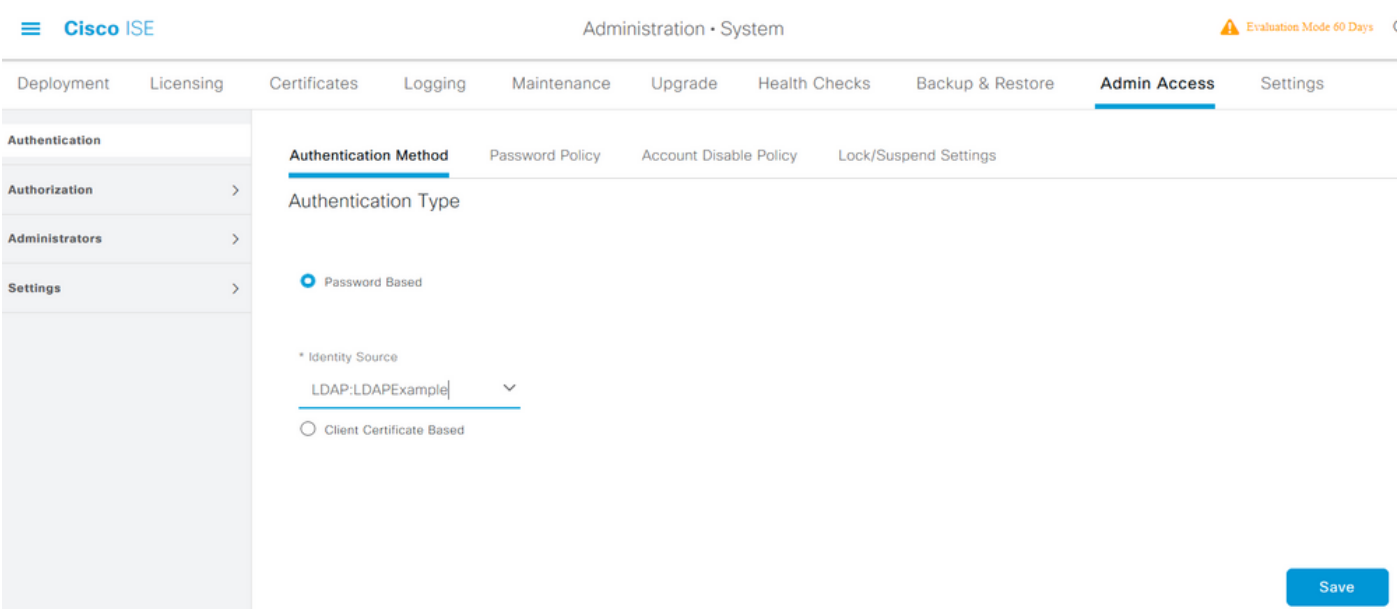
General   Connection   Directory Organization   **Groups**   Attributes   Advanced Settings

Edit + Add Delete Group

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

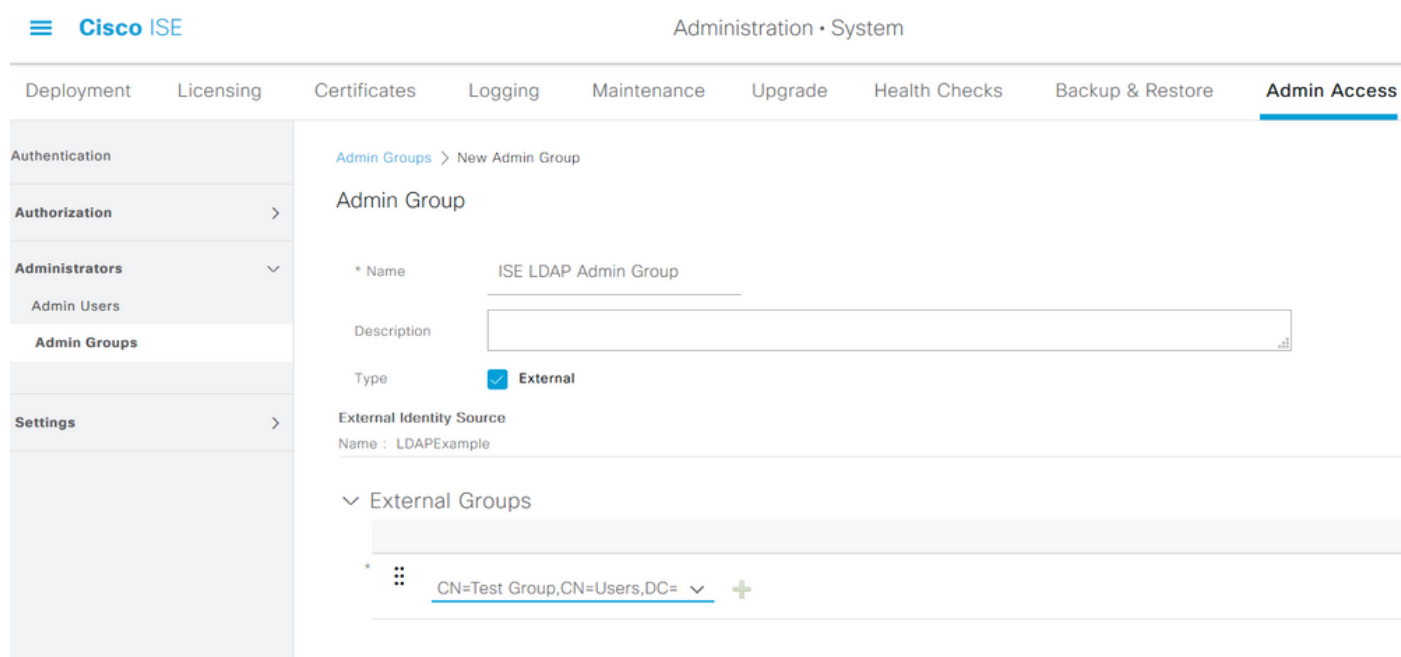
## 為LDAP使用者啟用管理訪問

要使用LDAP啟用ISE的基於密碼的身份驗證，請導航到Administration > System > Admin Access > Authentication。在Authentication Method頁籤中，選擇Password-Based選項。從Identity Source下拉選單中選擇LDAP，然後按一下Save。



## 將ISE管理員組對映到LDAP組

這允許配置的使用者根據RBAC策略的授權獲得管理員訪問許可權，這反過來又基於使用者的LDAP組成員資格。要定義Cisco ISE管理員組並將其對映到LDAP組，請導航到**Administration > System > Admin Access > Administrators > Admin Groups**。按一下**Add**，然後輸入新Admin組的名稱。在「型別」欄位中，選中**External**覈取方塊。從**External Groups**下拉選單中，選擇此管理員組要對映到的LDAP組（如之前檢索和定義的）。**提交更改**。



## 設定管理員組的RBAC許可權

要將RBAC許可權分配給在上一部分中建立的管理員組，請導航到**Administration > System > Admin Access > Authorization > RBAC Policy**。從右側的**Actions**下拉選單中，選擇**Insert new policy**。建立一個新規則，將其與上面部分中定義的管理員組進行對映，然後為其分配所需的資料和選單訪問許可權，然後按一下**儲存**。

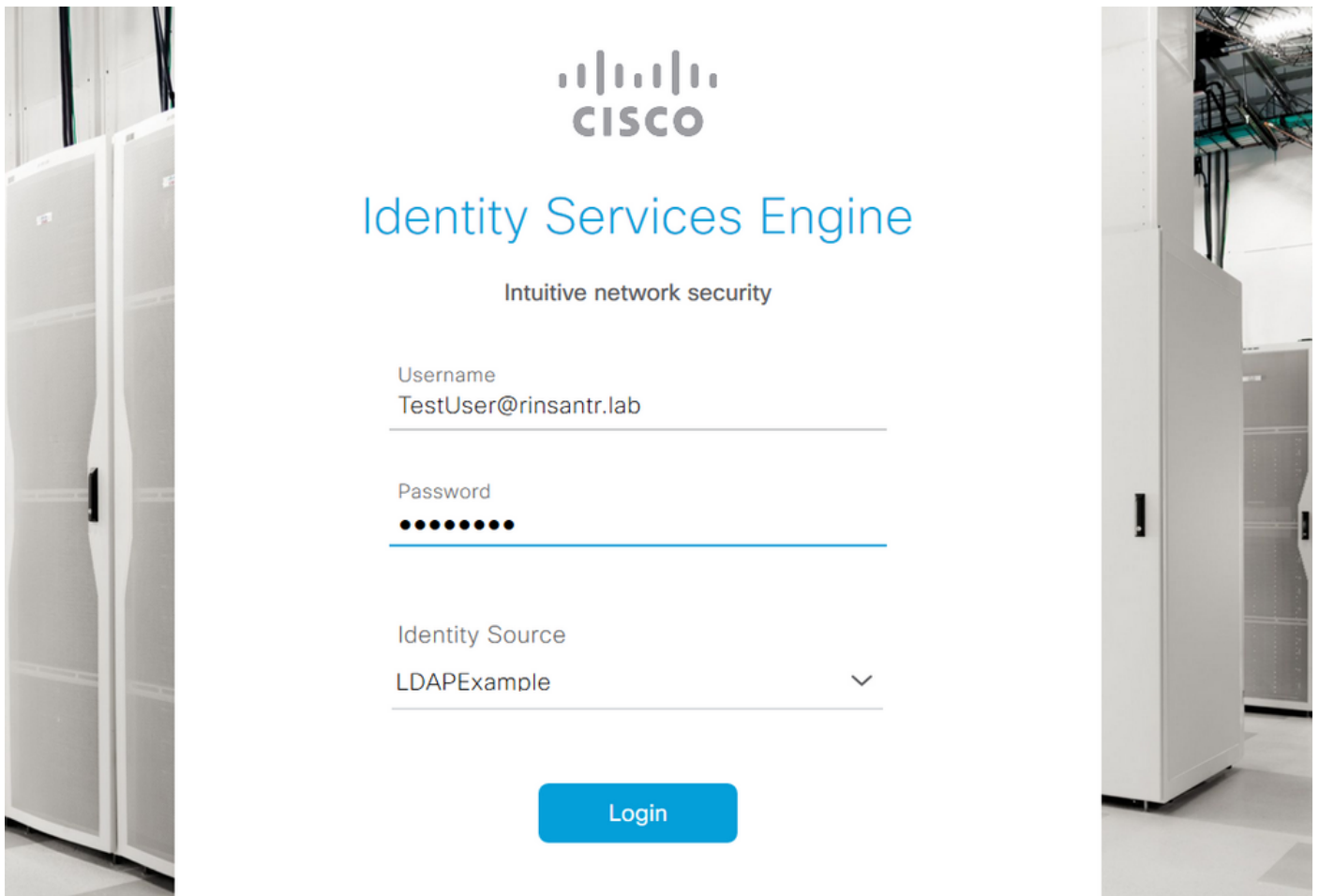
Create Role Based Access Control policies by configuring rules based on Admin groups, Menu Access permissions (menu items), Data Access permissions (identity group data element Menu/Data Access permissions are not allowed on a single policy. You can copy the default policies shown below, then modify 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
<input checked="" type="checkbox"/> Customization Admin Policy	If Customization Admin	+ then Customization Admin Menu ... + Actions
<input checked="" type="checkbox"/> RBAC Policy 2	If ISE LDAP Admin Group	+ then Super Admin Menu Access a... × Actions
<input checked="" type="checkbox"/> Elevated System Admin Poli	If Elevated System Admin	+ then Super Admin Menu Access +
<input checked="" type="checkbox"/> ERS Admin Policy	If ERS Admin	+ then Read Only Admin Data Acces: +
<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 Haldrack Admin Menu Access + Actions
<input checked="" type="checkbox"/> Haldrack Admin Policy	If Haldrack Admin	+ then Haldrack Admin Menu Access + Actions

## 使用LDAP憑證訪問ISE並驗證

從管理GUI註銷。從身份源下拉選單中選擇LDAP名稱。從LDAP資料庫輸入使用者名稱和密碼，然後登入。



若要確認組態是否正常運作，請從ISE GUI右上角的**Settings**圖示驗證經過驗證的使用者名稱。導覽至**Server Information**，然後驗證使用者名稱。



# 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**