

# 了解ISE上的管理员访问和RBAC策略

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[验证设置](#)

[配置管理员组](#)

[配置管理员用户](#)

[配置权限](#)

[配置RBAC策略](#)

[配置管理员访问设置](#)

[使用AD凭证配置管理员门户访问](#)

[将ISE加入AD](#)

[选择目录组](#)

[启用AD的管理访问](#)

[配置ISE管理组到AD组映射](#)

[为管理员组设置RBAC权限](#)

[使用AD凭证访问ISE并验证](#)

[使用LDAP配置管理员门户访问](#)

[将ISE加入LDAP](#)

[为LDAP用户启用管理访问](#)

[将ISE管理组映射到LDAP组](#)

[为管理员组设置RBAC权限](#)

[使用LDAP凭证访问ISE并验证](#)

## 简介

本文档介绍ISE管理身份服务引擎(ISE)上的管理访问的功能。

## 先决条件

### 要求

思科建议您了解以下主题：

- ISE
- Active Directory
- 轻量级目录访问协议(LDAP)

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

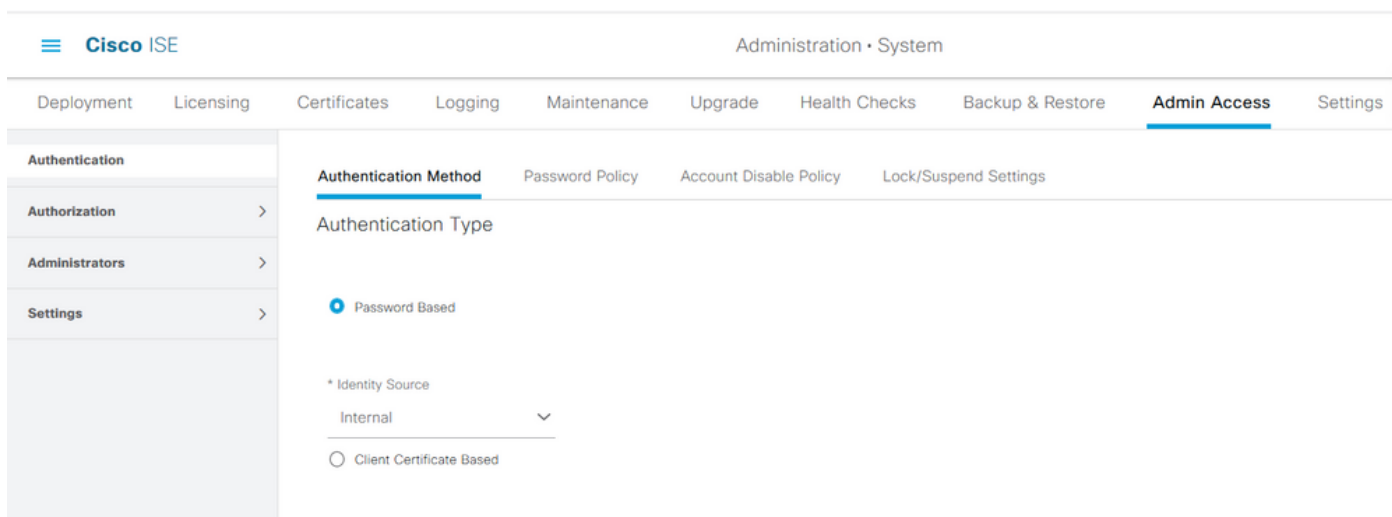
- 身份服务引擎3.0
- Windows Server 2016

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 配置

### 验证设置

管理员用户需要对自身进行身份验证才能访问ISE上的任何信息。管理员用户的身份可以通过使用ISE内部身份库或外部身份库进行验证。可通过密码或证书来验证真实性。要配置这些设置，请导航至**Administration > System > Admin Access > Authentication**。在Authentication Method选项卡下选择所需的**身份验证类型**。



**注意：**默认情况下启用基于密码的身份验证。如果更改为基于客户端证书的身份验证，则会导致所有部署节点上的应用服务器重新启动。

身份服务引擎不允许从CLI为命令行界面(CLI)配置密码策略。图形用户界面(GUI)和CLI的密码策略只能通过ISE的GUI进行配置。要配置此配置，请导航至**Administration > System > Admin Access > Authentication**，然后导航至**Password Policy**选项卡。

## Authentication

## Authorization &gt;

## Administrators &gt;

## Settings &gt;

## 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 &gt;

## Administrators &gt;

## Settings &gt;

**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)

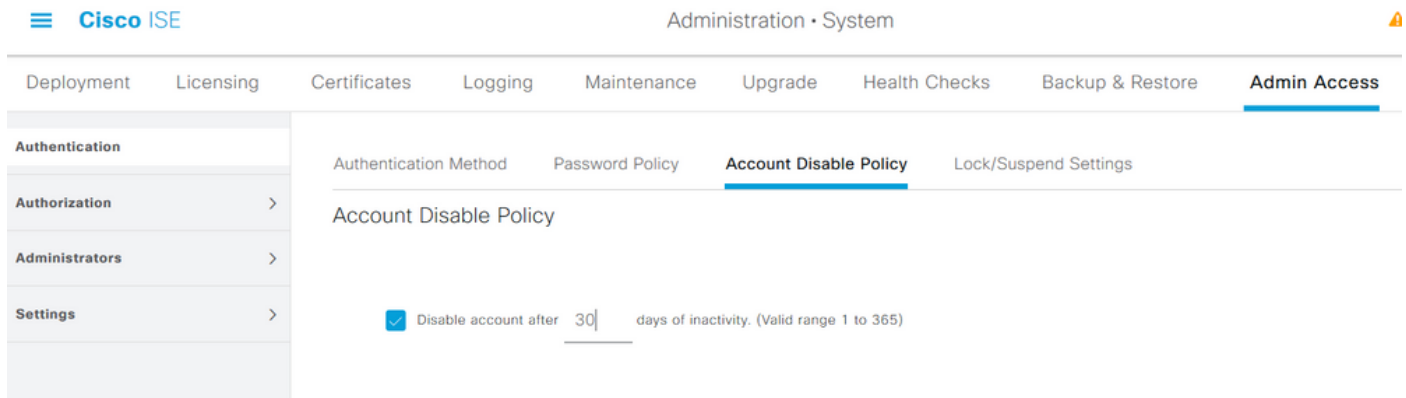
**Password Lifetime**

Admins can be required to periodically change their password

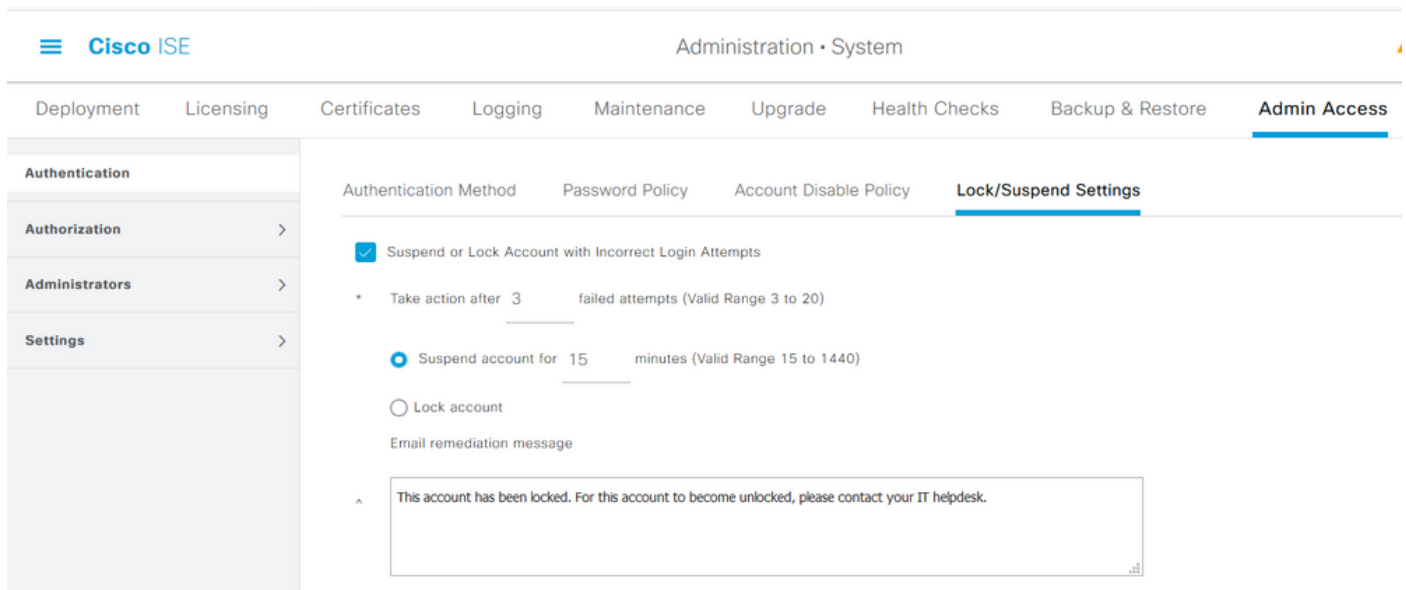
If Admin user is also configured as a network user, an expired enable password can cause the admin account to become disabled

- 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具有禁用非活动管理员用户的设置。要配置此项，请导航至管理>系统>管理员访问>身份验证，然后导航至帐户禁用策略选项卡。



ISE还根据失败登录尝试次数提供锁定或暂停管理员用户帐户的工具。要配置此设置，请导航至 **Administration > System > Admin Access > Authentication**，然后导航至**Lock/Suspend Settings**选项卡。



要管理管理访问，需要管理组、用户和各种策略/规则来控制和管理其权限。

## 配置管理员组

导航至**Administration > System > Admin Access > Administrators > Admin Groups**以配置管理员组。默认情况下，内置且无法删除的组很少。

- 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 ...

创建组后，选择该组，然后点击编辑将管理用户添加到该组。有一个调配将外部身份组映射到 ISE 上的管理员组，以便外部管理员用户获得所需权限。要配置此项，请在添加用户时选择类型为 External。

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

Admin Groups > Super Admin

### Admin Group

\* Name: Super Admin

Description: Access permission for Operations, Policy and Administration tabs. Includes data access permission for Admin Groups, User Identity Groups, Endpoint Identity Groups, All Locations and All Device Types.

Type:  External

External Identity Source Name: \_\_\_\_\_

External Groups:   
 \*  +

Member Users

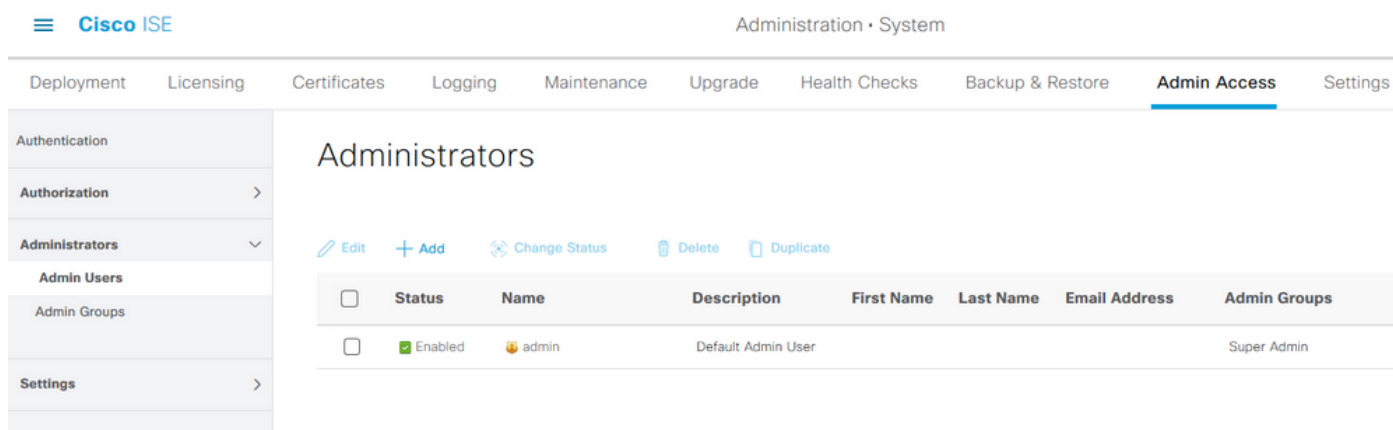
Users

+ Add  Delete

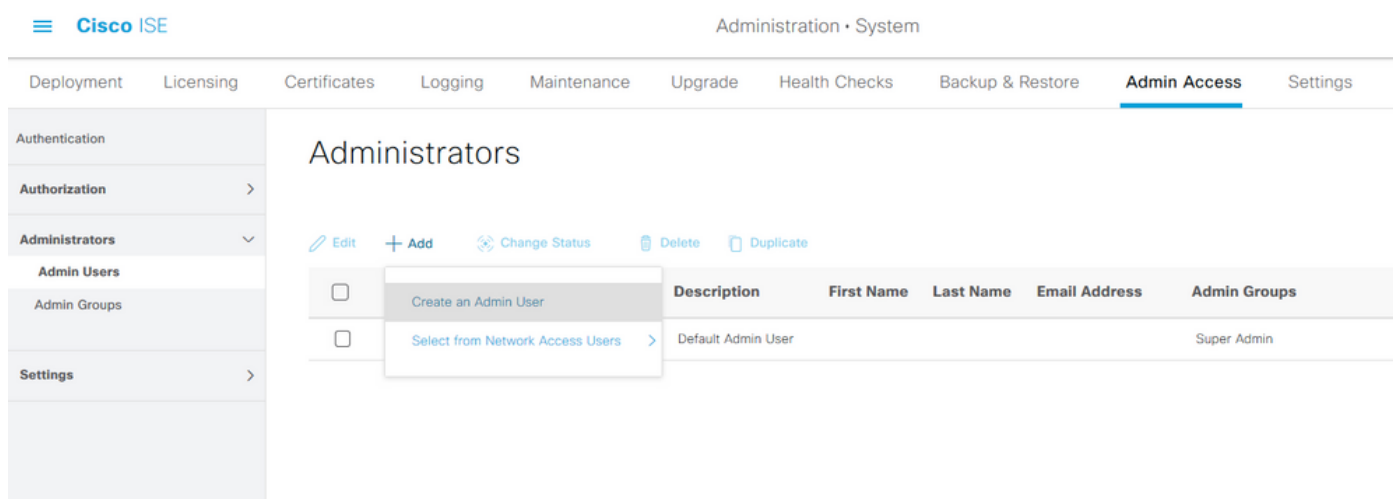
<input type="checkbox"/>	Status	Email	Username	First Name	Last Name
<input type="checkbox"/>	<input checked="" type="checkbox"/> Enabled		admin		

## 配置管理员用户

要配置管理员用户，请导航至Administration > System > Admin Access > Administrators > Admin Users。



单击 **Add**。有两个选项可供选择。一是添加一个新用户。另一个是将网络访问用户（即配置为内部用户以访问网络/设备的用户）作为ISE管理员。



选择选项后，必须提供所需的详细信息，并且必须根据向用户授予的权限和权限来选择用户组。

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

## 配置权限

可以为用户组配置两种权限：

1. 菜单访问
2. 数据访问

菜单访问控制ISE的导航可见性。每个选项卡都有两个选项，即显示或隐藏，可以配置。“菜单访问”(Menu Access)规则可配置为显示或隐藏选定的选项卡。

数据访问控制读取/访问/修改ISE上的身份数据的功能。只能为管理员组、用户身份组、终端身份组和网络设备组配置访问权限。ISE上的这些实体有三个可配置选项。它们是完全访问、只读访问和无访问。数据访问规则可配置为为ISE上的每个选项卡选择以下三个选项之一。

必须先创建菜单访问和数据访问策略，然后才能将它们应用到任何管理员组。默认情况下，有一些策略是内置的，但始终可以自定义或创建新策略。

要配置菜单访问策略，请导航至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

单击 **Add**。ISE 中的每个导航选项都可配置为在策略中显示/隐藏。

- 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

要配置数据访问策略，请导航至Administration > System > Admin Access > Authorization > Permissions > Data Access。



Cisco ISE Administration - System Evaluation Mode ?!

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

Authentication

Authorization

Permissions

Menu Access

**Data Access**

RBAC Policy

Administrators

Settings

## Data Access

Edit + Add Duplicate Delete

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.

单击Add 创建新策略，并配置权限以访问管理员/用户身份/终端身份/网络组。

Cisco ISE Administration - System

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

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代表基于角色的访问控制。用户所属的角色（管理员组）可以配置为使用所需的菜单和数据访问策略。可以为单个角色配置多个RBAC策略，或者可以在单个策略中配置多个角色以访问菜单和/或数据。当管理员用户尝试执行操作时，将评估所有这些适用策略。最终决定是适用于该角色的所有策略的总和。如果同时允许和拒绝的规则相互矛盾，则允许规则会覆盖拒绝规则。要配置这些策略，请导航至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

单击操作以复制/插入/删除策略。

**注意：**无法更新系统创建的策略和默认策略，且无法删除默认策略。

**注意：**不能在单个规则中配置多个菜单/数据访问权限。

## 配置管理员访问设置

除RBAC策略外，还可以配置一些对所有管理员用户通用的设置。

要配置GUI和CLI的Maximum Sessions Allowed、Pre-login和Post-login Banners的数量，请导航至Administration > System > Admin Access > Settings > Access。在“会话”选项卡下配置这些。

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  (Valid Range 1 to 20)

Pre-login banner

Welcome to ISE

Post-login banner

## CLI Sessions

Maximum Concurrent Sessions  (Valid Range 1 to 10)

Pre-login banner

要配置GUI和CLI可从中访问的IP地址列表，请导航至**Administration > System > Admin Access > Settings > Access**，然后导航至**IP Access**选项卡。

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

要配置节点列表，管理员可从其访问Cisco ISE中的MnT部分，请导航至**Administration > System > Admin Access > Settings > Access**，然后导航至**MnT Access**选项卡。

要允许部署内或部署外的节点或实体将系统日志发送到MnT，请单击**允许任何IP地址连接到MnT**单选按钮。要仅允许部署中的节点或实体将系统日志发送到MnT，请单击**仅允许部署中的节点连接到MnT**单选按钮。

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

**注意：**对于ISE 2.6补丁2及更高版本，默认启用“使用ISE消息服务”将UDP系统日志传输到MnT，这不允许来自部署外的任何其他实体的系统日志。

要配置由于会话处于非活动状态而导致的超时值，请导航至**Administration > System > Admin Access > Settings > Session**。在Session Timeout选项卡下**设置此值**。

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)

要查看/使当前活动会话无效，请导航至**Administration > Admin Access > Settings > Session**，然后单击**Session Info**选项卡。

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凭证配置管理员门户访问

## 将ISE加入AD

要将ISE加入到外部域，请导航至Administration > Identity Management > External Identity Sources > Active Directory。输入新的加入点名称和Active Directory域。输入可以添加和更改计算机对象的AD帐户的凭据，然后单击OK。

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. The main content area shows the 'Connection' tab for an Active Directory source. The 'Join Point Name' is 'AD' and the 'Active Directory Domain' is 'rinsantr.lab'. A 'Join Domain' dialog box is open in the foreground, asking for credentials to join ISE nodes to the Active Directory Domain. The dialog fields are: 'AD User Name' (Administrator), 'Password' (masked with dots), 'Specify Organizational Unit' (checkbox), and 'Store Credentials' (checkbox). 'Cancel' and 'OK' buttons are at the bottom right.

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

## 选择目录组

导航至**管理>身份管理>外部身份源>Active Directory**。单击所需的加入点名称并导航至“组”选项卡。单击“添加”>“从目录选择组”>“检索组”。至少导入一个管理员所属的AD组，然后单击“确定”，然后单击“保存”。

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

## 启用AD的管理访问

要启用使用AD的ISE基于密码的身份验证，请导航至**Administration > System > Admin Access > Authentication**。在Authentication Method选项卡中，选择**Password-Based**选项。从“身份源”下拉菜单中选择“AD”，然后单击“保存”。

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE', 'Administration · System', and 'Evaluation Mode 601'. The main navigation menu has tabs for 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The 'Admin Access' tab is selected. On the left, a sidebar menu shows 'Authentication', 'Authorization', 'Administrators', and 'Settings'. The main content area is titled 'Authentication Method' and includes sub-tabs for 'Password Policy', 'Account Disable Policy', and 'Lock/Suspend Settings'. Under 'Authentication Method', 'Authentication Type' is set to 'Password Based'. Below this, there is a section for '\* Identity Source' with a dropdown menu showing 'AD:AD' and a radio button for 'Client Certificate Based'. A 'Save' button is located at the bottom right.

## 配置ISE管理组到AD组映射

这允许授权根据AD中的组成员身份确定管理员的基于角色的访问控制(RBAC)权限。要定义思科ISE管理员组并将其映射到AD组，请导航至**Administration > System > Admin Access > Administrators > Admin Groups**。单击**Add**，然后输入新管理员组的名称。在“类型”字段中，选中“外部”复选框。从外部组下拉菜单中，选择此管理组要映射到的AD组（如上面的“选择目录组”部分中定义）。**提交更改**。

The screenshot shows the Cisco ISE Administration console for configuring an Admin Group. The top navigation bar is the same as the previous screenshot. The main navigation menu has 'Admin Access' selected. The sidebar menu shows 'Authentication', 'Authorization', 'Administrators', and 'Settings'. The main content area is titled 'Admin Groups > ISE AD Admin Group' and 'Admin Group'. It includes fields for '\* Name' (ISE AD Admin Group), 'Description', and 'Type' (External, checked). Below this is the 'External Identity Source' section with 'Name : AD'. The 'External Groups' section shows a dropdown menu with 'rinsantr.lab/Users/Test Group' selected. The 'Member Users' section has '+ Add' and 'Delete' buttons. At the bottom, there is a table with columns for 'Status', 'Email', 'Username', 'First Name', and 'Last Name', with the text 'No data available' below it.

## 为管理员组设置RBAC权限

要将RBAC权限分配给在上一节中创建的管理组，请导航至**Administration > System > Admin Access > Authorization > RBAC Policy**。从右侧的“操作”下拉菜单中，选择“插入新策略”。创建新规则，将其映射到上节中定义的管理组，并为其分配所需的数据和菜单访问权限，然后单击**Save**。

Authentication

Authorization

Permissions

RBAC Policy

Administrators

Settings

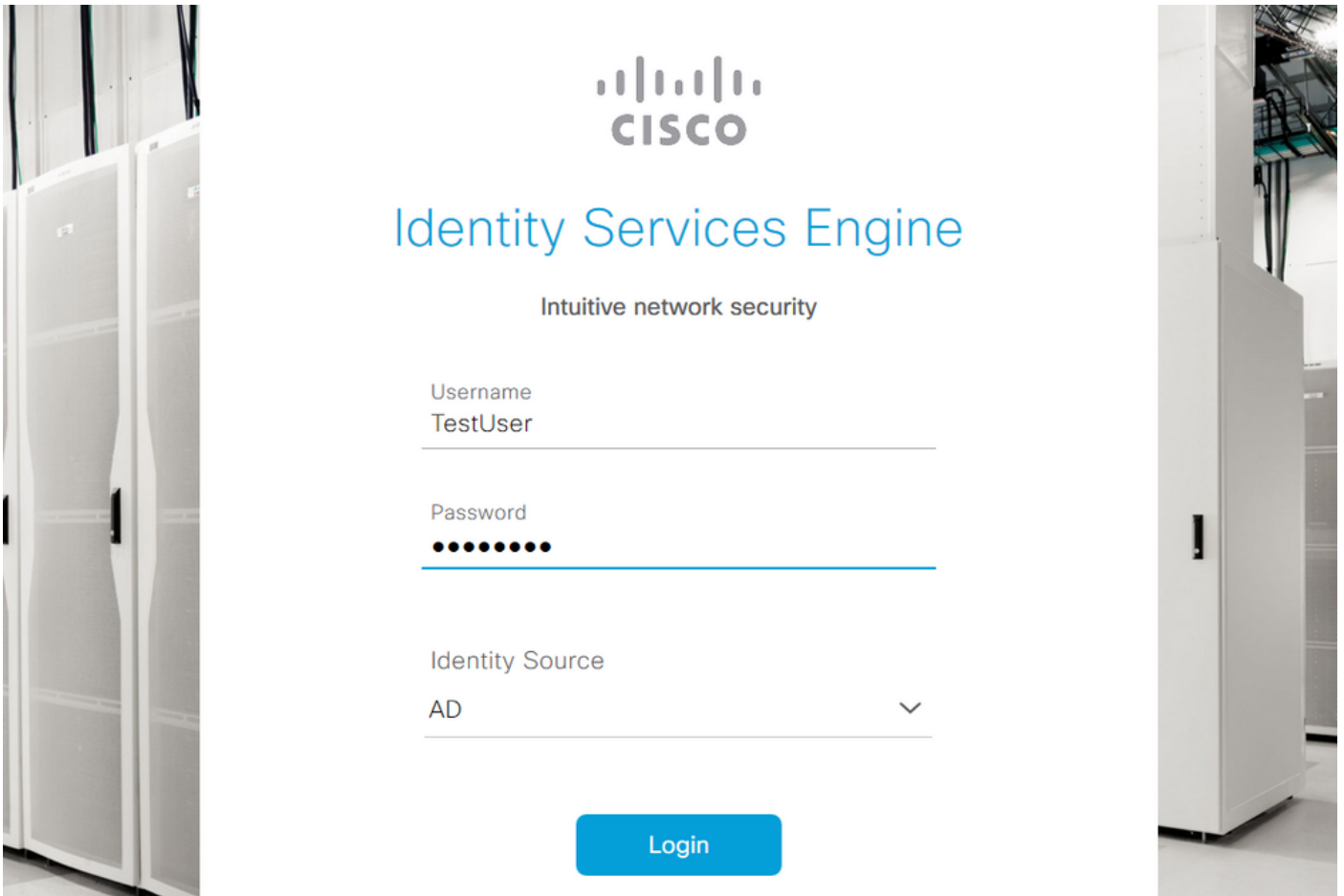
Create Role Based Access Control policies by configuring rules based on Admin groups, Menu Access permissions (menu items), Data Access permissions (identity group data elements) and other c allowed on a single policy. You can copy the default policies shown below, then modify them as needed. Note that system-created and default policies cannot be updated, and default policies cannot 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 Super Admin Menu Access +
<input checked="" type="checkbox"/> ERS Admin Policy	If ERS Admin	+ then Super Admin Data Access
<input checked="" type="checkbox"/> ERS Operator Policy	If ERS Operator	+ then

## 使用AD凭证访问ISE并验证

注销管理GUI。从“身份源”(Identity Source)下拉菜单中选择加入点名称。从AD数据库输入用户名和密码，然后登录。



要确认配置工作正常，请从ISE GUI右上角的**设置**图标验证经过身份验证的用户名。导航至“**Server Information**”并验证用户名。



## 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配置管理员门户访问

### 将ISE加入LDAP

导航至**管理>身份管理>外部身份源> Active Directory > LDAP**。在“常规”选项卡下，输入LDAP的名称，并选择架构作为**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  ▼

接下来，要配置连接类型，请导航至“连接”选项卡。在此，设置主LDAP服务器的主机名/IP以及端口389(LDAP)/636(LDAP-Secure)。使用LDAP服务器的管理员密码输入管理员可分辨名称(DN)的路径。

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

然后，导航至“目录组织”选项卡，然后单击命名上下文，根据存储在LDAP服务器中的用户的层次结构选择用户的正确组织组。

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...](#) ⓘ

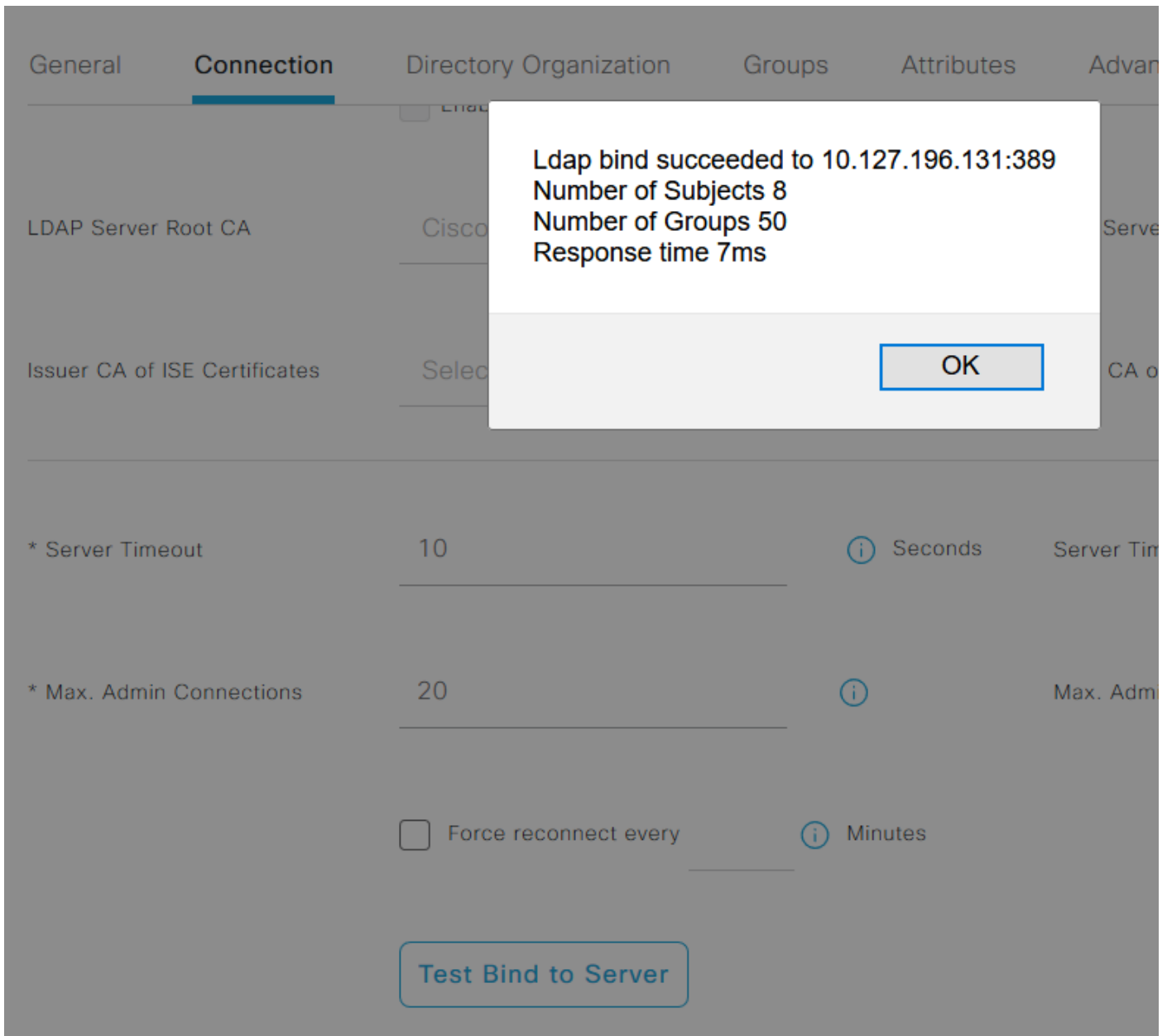
\* Group Search Base DC=rinsantr,DC=lab [Naming Contexts...](#) ⓘ

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

单击**Connection**选项卡下的**Test Bind to Server(测试绑定到服务器)**，以测试LDAP服务器从ISE的可达性。



现在导航至“组”选项卡，然后单击“添加”>“从目录选择组”>“检索组”。至少导入一个管理员所属的组，然后单击“确定”，然后单击“保存”。

## 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

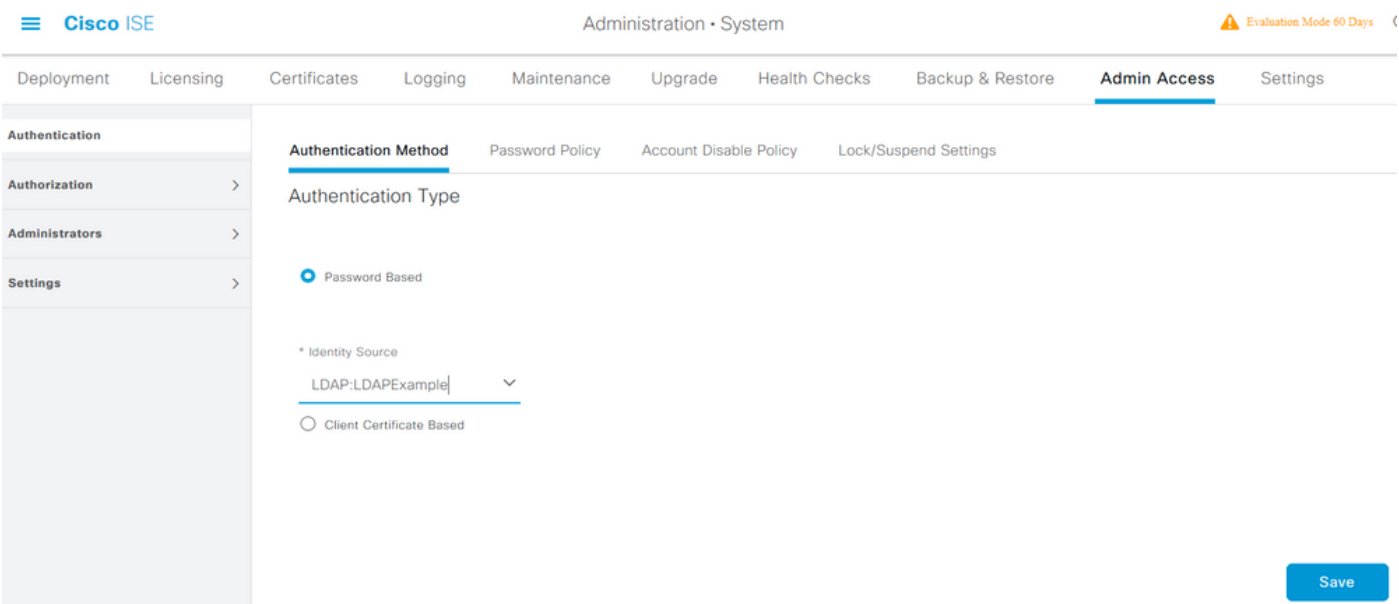
General   Connection   Directory Organization   **Groups**   Attributes   Advanced Settings

Edit + Add Delete Group

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

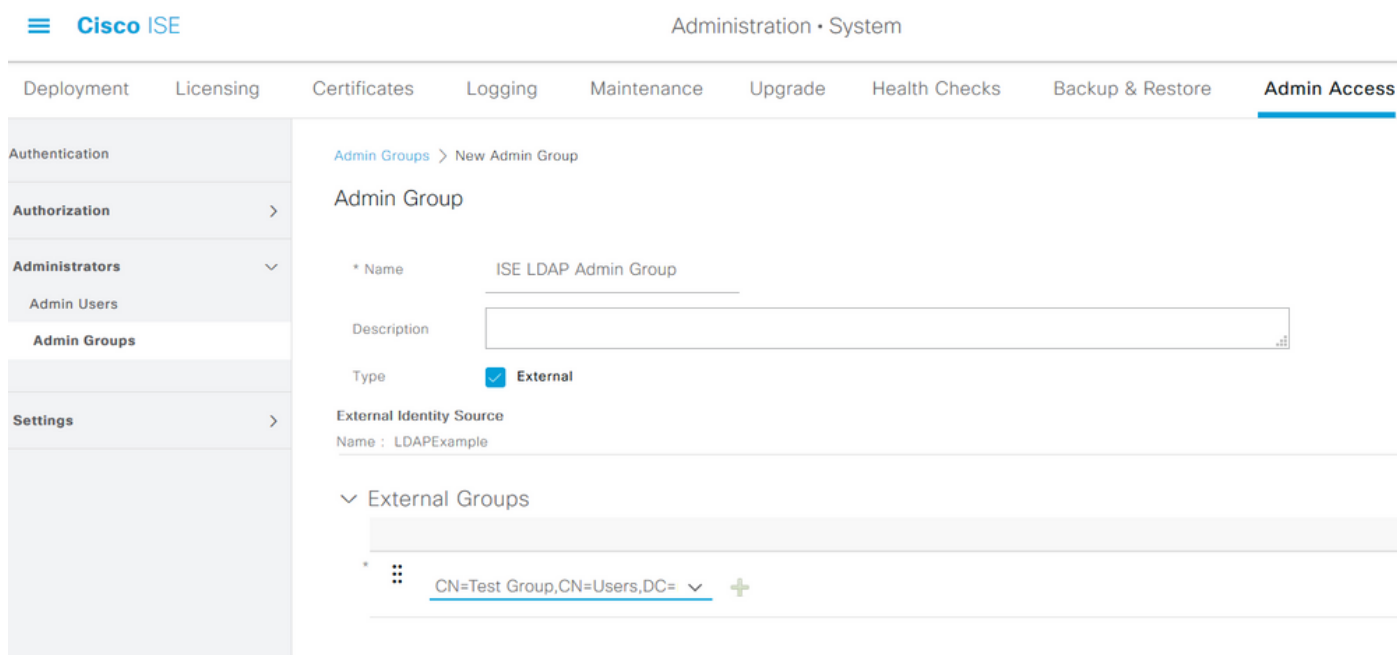
## 为LDAP用户启用管理访问

要启用使用LDAP的ISE基于密码的身份验证，请导航至**Administration > System > Admin Access > Authentication**。在Authentication Method选项卡中，选择**Password-Based**选项。从“身份源”下拉菜单中选择“LDAP”，然后单击“保存”。



## 将ISE管理组映射到LDAP组

这允许已配置用户根据RBAC策略的授权（这反过来又基于用户的LDAP组成员身份）获取管理员访问权限。要定义思科ISE管理组并将其映射到LDAP组，请导航至**Administration > System > Admin Access > Administrators > Admin Groups**。单击**Add**，然后输入新管理员组的名称。在“类型”字段中，选中“外部”复选框。从外部组下拉菜单中，选择此管理组要映射到的LDAP组（如之前检索和定义的）。**提交更改**。



## 为管理员组设置RBAC权限

要将RBAC权限分配给在上一节中创建的管理组，请导航至**Administration > System > Admin Access > Authorization > RBAC Policy**。从右侧的“操作”下拉菜单中，选择“插入新策略”。创建新规则，将其映射到上节中定义的管理组，并为其分配所需的数据和菜单访问权限，然后单击**Save**。

Authentication

Authorization

Permissions

RBAC Policy

Administrators

Settings

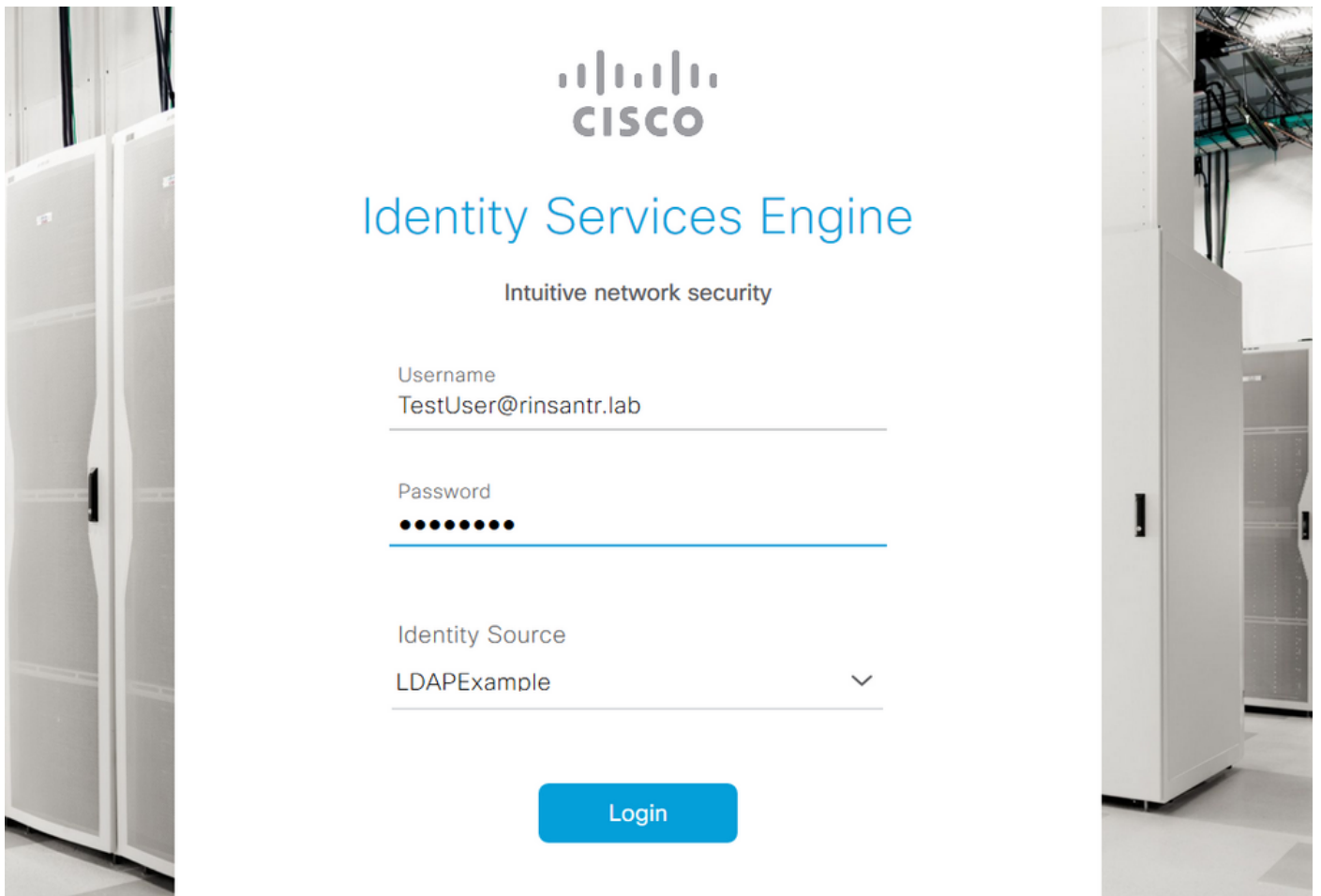
Create Role Based Access Control policies by configuring rules based on Admin groups, Menu Access permissions (menu items), Data Access permissions (identity group data element Menu/Data Access permissions are not allowed on a single policy. You can copy the default policies shown below, then modify them as needed. Note that system-created and default policies cannot be deleted. For decision making, all applicable policies will be evaluated. The subject's permissions will be the aggregate of all permissions from each applicable policy, displayed in alphabetical order of the policy name).

RBAC Policies

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

## 使用LDAP凭证访问ISE并验证

注销管理GUI。从Identity Source下拉菜单中选择LDAP名称。从LDAP数据库输入用户名和密码，然后登录。



要确认配置是否正常工作，请从ISE GUI右上角的**设置**图标验证经过身份验证的用户名。导航至“Server Information”并验证用户名。



## 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