

# ISEでの管理アクセスおよびRBACポリシーの理解

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[認証設定](#)

[管理グループの設定](#)

[管理者ユーザの設定](#)

[権限の設定](#)

[RBACポリシーの設定](#)

[管理アクセスの設定](#)

[ADクレデンシャルを使用した管理ポータルアクセスの設定](#)

[AD への ISE の結合](#)

[ディレクトリグループの選択](#)

[AD 用管理アクセスの有効化](#)

[ISE管理グループのADグループマッピングへの設定](#)

[管理グループの RBAC アクセス許可の設定](#)

[ADクレデンシャルを使用したISEへのアクセスと確認](#)

[LDAPによる管理ポータルアクセスの設定](#)

[ISEからLDAPへの参加](#)

[LDAPユーザの管理アクセスの有効化](#)

[ISE管理グループをLDAPグループにマッピングします](#)

[管理グループの RBAC アクセス許可の設定](#)

[LDAPクレデンシャルによるISEへのアクセスと確認](#)

## 概要

このドキュメントでは、Identity Services Engine(ISE)の管理アクセスを管理するためのISEの機能について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- ISE
- Active Directory

- Lightweight Directory Access Protocol(LDAP)

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

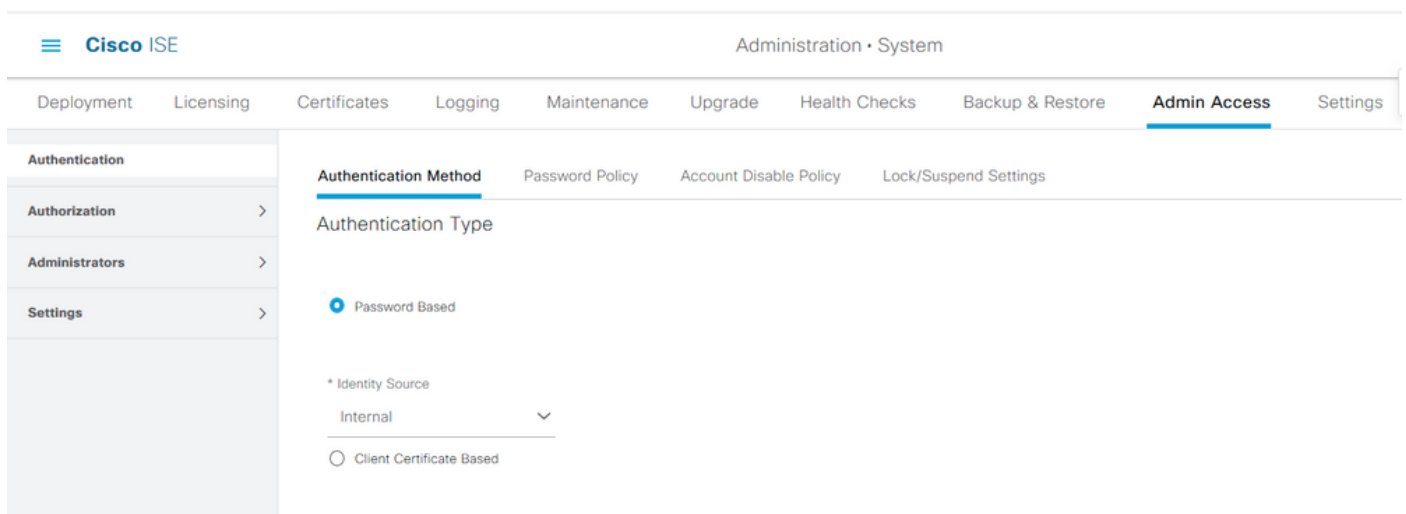
- Identity Services Engine 3.0
- Windows Server 2016

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 設定

### 認証設定

管理者ユーザは、ISEの情報にアクセスするために自身を認証する必要があります。管理者ユーザのIDは、ISE内部IDストアまたは外部IDストアを使用して確認できます。信頼性は、パスワードまたは証明書によって確認できます。これらの設定を構成するには、[Administration] > [System] > [Admin Access] > [Authentication]に移動します。[Authentication Method]タブで必要な認証タイプを選択します。



**注：**パスワードベースの認証は、デフォルトで有効になっています。これをクライアント証明書ベース認証に変更すると、すべての展開ノードでアプリケーションサーバが再起動します。

Identity Services Engineでは、CLIからコマンドラインインターフェイス(CLI)のパスワードポリシーを設定できません。グラフィカルユーザインターフェイス(GUI)とCLIの両方のパスワードポリシーは、ISEのGUIを介してのみ設定できます。これを設定するには、[Administration] > [System] > [Admin Access] > [Authentication]に移動し、[Password Policy]タブに移動します。

## 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には、非アクティブな管理者ユーザを無効にするプロビジョニングがあります。これを設定するには、[Administration] > [System] > [Admin Access] > [Authentication]に移動し、[Account Disable Policy]タブに移動します。

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Administration' and 'System'. Below it, a secondary navigation bar lists various system functions: 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', and 'Admin Access'. The 'Admin Access' tab is selected. On the left, a sidebar menu contains 'Authentication', 'Authorization', 'Administrators', and 'Settings'. The main content area is titled 'Account Disable Policy' and features a sub-tab 'Account Disable Policy'. A checkbox labeled 'Disable account after' is checked, with a value of '30' entered in the adjacent text box, followed by the text 'days of inactivity. (Valid range 1 to 365)'.

ISEには、失敗したログイン試行回数に基づいて、管理者ユーザアカウントをロックまたは一時停止する機能もあります。これを設定するには、[Administration] > [System] > [Admin Access] > [Authentication]に移動し、[Lock/Suspend Settings]タブに移動します。

This screenshot shows the 'Lock/Suspend Settings' configuration page in the Cisco ISE Administration console. The navigation and sidebar are identical to the previous screenshot. The 'Lock/Suspend Settings' sub-tab is selected. A checkbox '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. An 'Email remediation message' field is present, containing the text: 'This account has been locked. For this account to become unlocked, please contact your IT helpdesk.'

管理アクセスを管理するには、管理グループ、ユーザ、および権限を制御および管理するさまざまなポリシー/ルールが必要です。

## 管理グループの設定

[管理] > [システム] > [管理アクセス] > [管理者] > [管理グループ]に移動し、管理者グループを設定します。デフォルトで組み込まれているグループは少数であり、削除できません。

Admin 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 ...

グループが作成されたら、そのグループを選択し、[edit]をクリックしてそのグループに管理ユーザを追加します。外部IDグループをISE上の管理グループにマッピングして、外部管理者ユーザが必要な権限を取得できるようにするプロビジョニングがあります。これを設定するには、ユーザを追加するときにタイプとして[External]を選択します。

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	<input checked="" type="checkbox"/> External		
External Identity Source	Name :		
External Groups	Select an item		
Member Users	Users		
	<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled		
	admin		

## 管理者ユーザの設定

管理者ユーザを設定するには、[Administration] > [System] > [Admin Access] > [Administrators] > [Admin Users]に移動します。

Administration · System

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

Authentication

Authorization >

Administrators ▾

Admin Users

Admin Groups

Settings >

### Administrators

Edit + Add Change Status Delete Duplicate

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

[Add] をクリックします。選択するオプションは2つあります。1つは、新しいユーザを追加することです。もう1つの方法は、ISE管理者としてネットワークアクセスユーザ (内部ユーザとして設定されたユーザ) を作成することです。

Administration · System

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

Authentication

Authorization >

Administrators ▾

Admin Users

Admin Groups

Settings >

### Administrators

Edit + Add Change Status Delete Duplicate

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

オプションを選択した後は、必要な詳細を指定する必要があり、ユーザに与えられる権限と権限に基づいてユーザグループを選択する必要があります。

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

## 権限の設定

ユーザグループに設定できる権限には、次の2つのタイプがあります。

1. メニューアクセス
2. データアクセス

[Menu Access]は、ISEのナビゲーションの表示を制御します。[表示]または[非表示]タブごとに2つのオプションがあり、これらは設定可能です。メニューアクセスルールは、選択したタブの表示/非表示を設定できます。

データアクセスは、ISE上のアイデンティティデータの読み取り/アクセス/変更を制御します。アクセス権限は、管理グループ、ユーザIDグループ、エンドポイントIDグループ、およびネットワークデバイスグループに対してのみ設定できます。ISE上のこれらのエンティティには3つのオプションがあり、これらは設定可能です。フルアクセス、読み取り専用アクセス、およびアクセスなし。ISEの各タブに対して、次の3つのオプションのいずれかを選択するようにデータアクセスルールを設定できます。

メニューのアクセスポリシーとデータアクセスポリシーは、任意の管理グループに適用する前に作成する必要があります。デフォルトで組み込まれているポリシーはいくつかありますが、常に

カスタマイズすることも、新しいポリシーを作成することもできます。

メニューアクセスポリシーを設定するには、[Administration] > [System] > [Admin Access] > [Authorization] > [Permissions] > [Menu Access]に移動します。

The screenshot shows the Cisco ISE Administration console. The breadcrumb path is Administration > System > Admin Access > Menu Access. The left sidebar shows the navigation menu with 'Menu Access' selected. The main content area displays a table of existing menu access permissions.

<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

[Add] をクリックします。ISEの各ナビゲーションオプションは、ポリシーに表示/非表示を設定できます。

The screenshot shows the 'Create Menu Access Permission' form in the Cisco ISE Administration console. The breadcrumb path is Administration > System > Admin Access > Menu Access List > New RBAC Menu Access. The form includes a 'Name' field with the value 'Custom\_Menu\_Access' and a 'Description' field. Below the form is a 'Menu Access Privileges' section with a tree view of the ISE navigation structure and radio buttons for 'Show' and 'Hide' permissions.

ISE Navigation Structure

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

Permissions for Menu Access

Show  
 Hide



データアクセスポリシーを設定するには、[管理(Administration)] > [システム(System)] > [管理アクセス(Admin Access)] > [許可(Authorization)] > [権限(Permissions)] > [データアクセス(Data Access)]に移動します。

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Administration · System' and 'Evaluation Mode ?!'. The main navigation tabs are 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The left sidebar shows a tree view with 'Data Access' selected. The main content area is titled 'Data Access' and contains a table of existing permissions. At the top of the table are icons for 'Edit', '+ Add', 'Duplicate', and 'Delete'.

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

[Add]をクリックして新しいポリシーを作成し、管理/ユーザアイデンティティ/エンドポイントアイデンティティ/ネットワークグループにアクセスするためのアクセス許可を設定します。

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

- \* Name: Custom\_Data\_Access
- Description: (empty text box)

Below the form is a section titled 'Data Access Privileges' which contains a list of groups and their corresponding permissions:

- Admin Groups: Full Access (selected)
- User Identity Groups: Read Only Access
- Endpoint Identity Groups: No Access
- Blacklist: (no permission selected)
- GuestEndpoints: (no permission selected)
- RegisteredDevices: (no permission selected)
- Unknown: (no permission selected)
- Profiled: (no permission selected)
- Network Device Groups: (no permission selected)

## RBACポリシーの設定

RBACは、Role-Based Access Control ( ロールベースアクセスコントロール ) の略です。ユーザが属するロール ( 管理グループ ) は、必要なメニューポリシーとデータアクセスポリシーを使用するように設定できます。1つのロールに対して複数のRBACポリシーを設定することも、1つのポリシーに複数のロールを設定してメニューやデータにアクセスすることもできます。これらの適用可能なポリシーはすべて、管理者ユーザがアクションを実行しようとしたときに評価されます。最終的な決定は、そのロールに適用されるすべてのポリシーの集約です。同時に許可と拒否を行う矛盾したルールがある場合、許可ルールによって拒否ルールが上書きされます。これらのポリシーを設定するには、[Administration] > [System] > [Admin Access] > [Authorization] > [RBAC Policy]に移動します。

Cisco ISE Administration - System Evaluate

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

Authentication

Authorization  v

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 v
<input checked="" type="checkbox"/> Elevated System Admin Poli	If Elevated System Admin	+ then System Admin Menu Access ... + Actions v
<input checked="" type="checkbox"/> ERS Admin Policy	If ERS Admin	+ then Super Admin Data Access + Actions v
<input checked="" type="checkbox"/> ERS Operator Policy	If ERS Operator	+ then Super Admin Data Access + Actions v
<input checked="" type="checkbox"/> ERS Trustsec Policy	If ERS Trustsec	+ then Super Admin Data Access + Actions v
<input checked="" type="checkbox"/> Helpdesk Admin Policy	If Helpdesk Admin	+ then Helpdesk Admin Menu Access + Actions v
<input checked="" type="checkbox"/> Identity Admin Policy	If Identity Admin	+ then Identity Admin Menu Access ... + Actions v
<input checked="" type="checkbox"/> MnT Admin Policy	If MnT Admin	+ then MnT Admin Menu Access + Actions v
<input checked="" type="checkbox"/> Network Device Policy	If Network Device Admin	+ then Network Device Menu Acces... + Actions v
<input checked="" type="checkbox"/> Policy Admin Policy	If Policy Admin	+ then Policy Admin Menu Access a... + Actions v
<input checked="" type="checkbox"/> RBAC Admin Policy	If RBAC Admin	+ then RBAC Admin Menu Access a... + Actions v

ポリシーを複製/挿入/削除するには、[アクション]をクリックします。

注：システム作成およびデフォルトポリシーは更新できず、デフォルトポリシーは削除できません。

注：1つのルールで複数のメニュー/データアクセス権限を設定することはできません。

## 管理アクセスの設定

RBACポリシーに加えて、すべての管理者ユーザに共通の設定を設定できます。

GUIおよびCLIの[Maximum Sessions Allowed]、[Pre-login]、および[Post-login Banners]の数を設定するには、[Administration] > [System] > [Admin Access] > [Settings] > [Access]に移動します。[セッション]タブでこれらを設定します。

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

GUIおよびCLIにアクセスできるIPアドレスのリストを設定するには、[Administration] > [System] > [Admin Access] > [Settings] > [Access]に移動して、[IP Access]タブに移動します。

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

管理者がCisco ISEのMnTセクションにアクセスできるノードのリストを設定するには、[Administration] > [System] > [Admin Access] > [Settings] > [Access]に移動し、[MnT Access]タブに移動します。

展開内または展開外のノードまたはエンティティがMnTにsyslogを送信できるようにするには、[Allow any IP address to connect to MNT]オプションボタンをクリックします。展開内のノードま

またはエンティティのみがMnTにsyslogを送信できるようにするには、[展開内のノードのみがMNTに接続することを許可する]ラジオボタンをクリックします。

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

注：ISE 2.6パッチ2以降では、MnTへのUDP Syslog配信に「ISE Messaging Service」を使用するが、デフォルトでオンになっています。これは、展開外の他のエンティティからのsyslogを許可しません。

セッションの非アクティブによるタイムアウト値を設定するには、[Administration] > [System] > [Admin Access] > [Settings] > [Session]に移動します。この値は、[Session Timeout]タブで設定します。

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Administration · System'. Below it, a menu bar contains 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', and 'Admin Access'. The left sidebar has a tree view with 'Authentication', 'Authorization', 'Administrators', and 'Settings' (expanded to show 'Access', 'Session', and 'Portal Customization'). The main content area is titled 'Session Timeout' and shows a field for 'Session Idle Timeout' set to '60 minutes (Valid Range 6 to 100)'.

現在のアクティブなセッションを表示または無効にするには、[Administration] > [Admin Access] > [Settings] > [Session]に移動し、[Session Info]タブをクリックします。

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

## ADクレデンシャルを使用した管理ポータルアクセスの設定

### AD への ISE の結合

ISEを外部ドメインに参加させるには、[Administration] > [Identity Management] > [External Identity Sources] > [Active Directory]に移動します。新しい参加ポイント名とActive Directoryドメインを入力します。コンピュータオブジェクトを追加および変更できるADアカウントの資格情報を入力し、[OK]をクリックします。

Cisco ISE Administration • Identity Management

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

**External Identity Sources**

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

**Connection** Whitelisted Domains PassivelD Groups Attributes Advanced S

\* Join Point Name AD ⓘ

\* Active Directory Domain **rinsantr.lab** ⓘ

**Join Domain** ⓘ

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

\* AD User Name ⓘ Administrator

\* Password ⓘ ●●●●●●●●●●

Specify Organizational Unit ⓘ

Store Credentials ⓘ

Cancel OK

Connection    Whitelisted Domains    PassiveID    Groups    Attributes    Advanced Settings

---

\* Join Point Name    AD    ⓘ

---

\* Active Directory Domain    rinsantr.lab    ⓘ

---

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

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

## ディレクトリグループの選択

[Administration] > [Identity Management] > [External Identity Sources] > [Active Directory] を順に選択します。目的の結合点名をクリックし、「グループ」タブに移動します。[Add] > [Select Groups from Directory] > [Retrieve Groups]をクリックします。管理者が属するADグループを少なくとも1つインポートし、[OK]をクリックし、[保存]をクリックします。

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 \*    SID \*    Type Filter ALL

Retrieve Groups...    50 Groups Retrieved.

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

[Edit](#) [+ Add](#) [Delete Group](#) [Update SID Values](#)

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

## AD 用管理アクセスの有効化

ADを使用してISEのパスワードベース認証を有効にするには、[Administration] > [System] > [Admin Access] > [Authentication]に移動します。[Authentication Method]タブで、[Password-Based]オプションを選択します。[IDソース]ドロップダウンメニューから[AD]を選択し、[Save]をクリックします。

The screenshot shows the Cisco ISE Administration console. The navigation path is Administration > System > Admin Access > Authentication Method. The 'Authentication Method' is set to 'Password Based'. The 'Identity Source' dropdown menu is set to 'AD:AD'. There is a 'Save' button at the bottom right.

## ISE管理グループのADグループマッピングへの設定

これにより認証において、ADのグループメンバーシップに基づいて管理者の役割ベースアクセス制御 (RBAC) 権限が判別されます。Cisco ISE管理グループを定義し、それをADグループにマッピングするには、[Administration] > [System] > [Admin Access] > [Administrators] > [Admin Groups]に移動します。[Add]をクリックし、新しい管理グループの名前を入力します。[Type]フィールドで [External check box] をオンにします。[External Groups]ドロップダウンメニューから、この管理グループをマッピングするADグループを選択します (上記の[Select Directory Groups]セクションで定義されています)。変更を送信します。



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					

## 管理グループの RBAC アクセス許可の設定

前のセクションで作成した管理グループにRBAC権限を割り当てるには、[Administration] > [System] > [Admin Access] > [Authorization] > [RBAC Policy]に移動します。右側の[アクション]ドロップダウンメニューから、[新しいポリシーの挿入]を選択します。新しいルールを作成し、上のセクションで定義した管理グループにマッピングし、必要なデータおよびメニューアクセス権限を割り当て、[Save]をクリックします。

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

Authentication

Authorization >

Permissions >

**RBAC Policy**

Administrators >

Settings >

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

RBAC Policies

Rule Name	Admin Groups	Permissions
<input checked="" type="checkbox"/> Customization Admin Policy	If Customization Admin	+ then Customization Admin Men... + Actions
<input checked="" type="checkbox"/> RBAC Policy 1	If ISE AD Admin Group	+ then Super Admin Menu Acces... X Actions
<input checked="" type="checkbox"/> Elevated System Admin Poli	If Elevated System Admin	+ then
<input checked="" type="checkbox"/> ERS Admin Policy	If ERS Admin	+ then
<input checked="" type="checkbox"/> ERS Operator Policy	If ERS Operator	+ then

Super Admin Menu Access +

Super Admin Data Access +

## ADクレデンシャルを使用したISEへのアクセスと確認

管理 GUI からログアウトします。[IDソース]ドロップダウンメニューから結合ポイント名を選択します。AD データベースからユーザ名とパスワードを入力し、ログインします。





# Identity Services Engine

Intuitive network security

Username  
TestUser

Password  
●●●●●●●●

Identity Source  
AD

Login

設定が正常に動作していることを確認するには、ISE GUIの右上隅にある[Settings]アイコンから認証されたユーザ名を確認します。[サーバ情報]に移動し、ユーザ名を確認します。

## 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

## LDAPによる管理ポータルアクセスの設定

### ISEからLDAPへの参加

[Administration] > [Identity Management] > [External Identity Sources] > [Active Directory] > [LDAP]に移動します。[General]タブで、LDAPの名前を入力し、スキーマを[Active Directory]として選択します。

## External Identity Sources

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

LDAP Identity Sources List &gt; New LDAP Identity Source

## LDAP Identity Source

General Connection Directory Organization Groups Attribut

\* Name

Description

▶ Schema  ▼

次に、接続の種類を構成するには、[接続]タブに移動します。ここで、プライマリLDAPサーバのホスト名/IPを、ポート389(LDAP)/636(LDAP-Secure)とともに設定します。LDAPサーバの管理パスワードを使用して、管理識別名(DN)のパスを入力します。

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

次に、[Directory Organization] タブに移動し、[Naming Contexts]をクリックして、LDAPサーバに保存されているユーザの階層に基づいてユーザの正しい組織グループを選択します。

## External Identity Sources

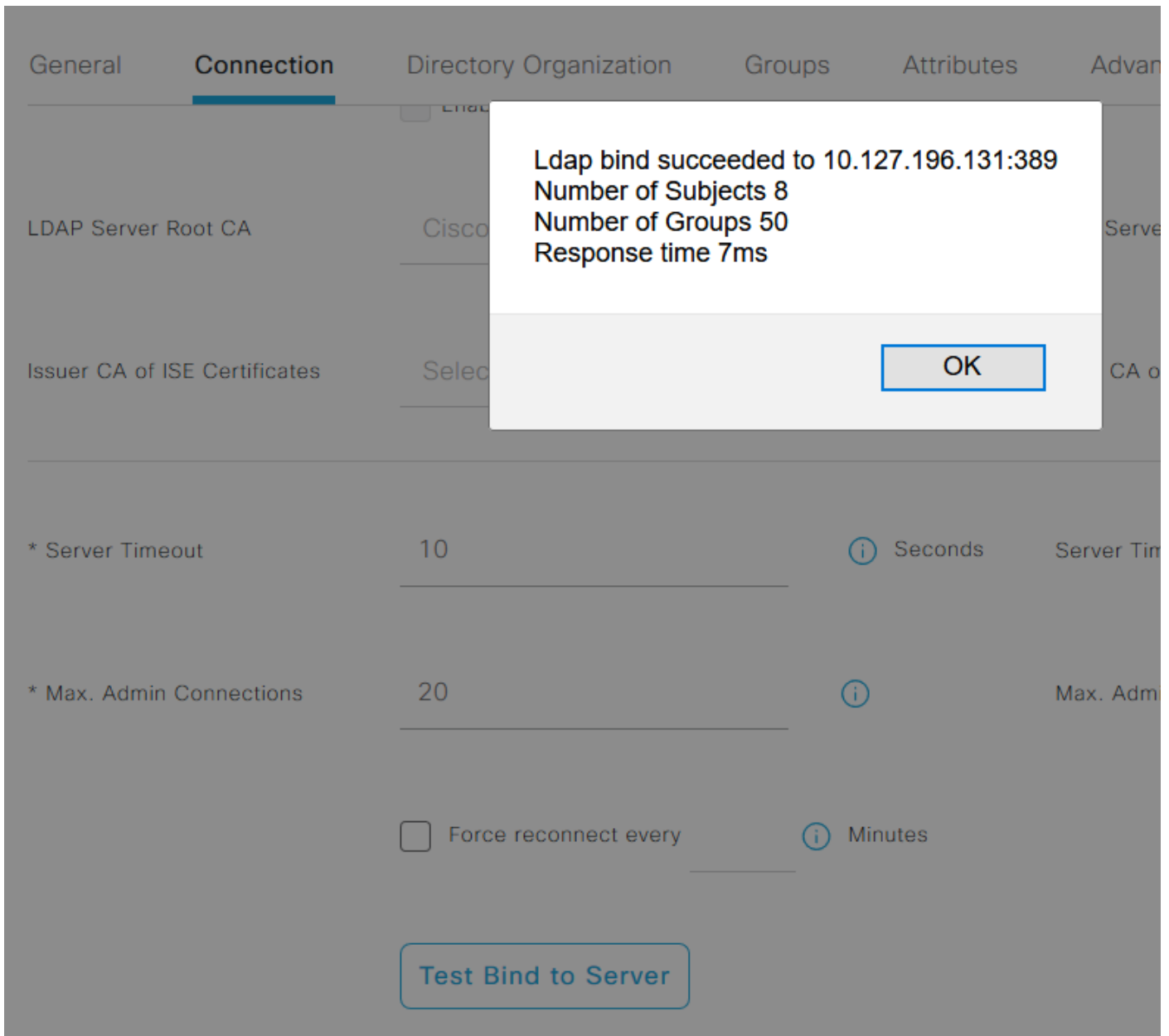
[Certificate Authentication F](#)[Active Directory](#)[AD](#)[LDAP](#)[ODBC](#)[RADIUS Token](#)[RSA SecurID](#)[SAML Id Providers](#)[Social Login](#)

LDAP Identity Sources List &gt; 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 

[Connection]タブの[Test Bind to Server]をクリックし、ISEからLDAPサーバへの到達可能性をテストします。



次に、[グループ]タブに移動し、[追加]>[ディレクトリからグループを選択]>[グループの取得]をクリックします。管理者が属するグループを少なくとも1つインポートし、「OK」をクリックし、「保存」をクリックします。

## 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

## LDAPユーザの管理アクセスの有効化

LDAPを使用してISEのパスワードベース認証を有効にするには、**[Administration] > [System] > [Admin Access] > [Authentication]**に移動します。**[Authentication Method]**タブで、**[Password-Based]**オプションを選択します。**[IDソース]**ドロップダウンメニューから**[LDAP]**を選択し、**[Save]**をクリックします。

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

Authentication

Authorization >

Administrators >

Settings >

**Authentication Method** Password Policy Account Disable Policy Lock/Suspend Settings

Authentication Type

Password Based

\* Identity Source

LDAP:LDAPExample | v

Client Certificate Based

Save

## ISE管理グループをLDAPグループにマッピングします

これにより、設定されたユーザはRBACポリシーの許可に基づいて管理者アクセスを取得できます。この権限は、ユーザのLDAPグループメンバーシップに基づいて取得されます。Cisco ISE管理グループを定義してLDAPグループにマッピングするには、[Administration] > [System] > [Admin Access] > [Administrators] > [Admin Groups]に移動します。[Add]をクリックし、新しい管理グループの名前を入力します。[Type] フィールドで [External check box] をオンにします。[外部グループ]ドロップダウンメニューから、この管理グループがマッピングされるLDAPグループを選択します（以前に取得および定義した場合）。変更を送信します。

Cisco ISE Administration · System

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

Authentication

Authorization >

Administrators >

Admin Users

**Admin Groups**

Settings >

Admin Groups > New Admin Group

Admin Group

\* Name ISE LDAP Admin Group

Description

Type  External

External Identity Source

Name : LDAPExample

External Groups

\* CN=Test Group,CN=Users,DC= v +

## 管理グループの RBAC アクセス許可の設定

前のセクションで作成した管理グループにRBAC権限を割り当てるには、[Administration] > [System] > [Admin Access] > [Authorization] > [RBAC Policy]に移動します。右側の[アクション]ドロップダウンメニューから、[新しいポリシーの挿入]を選択します。新しいルールを作成し、上のセクションで定義した管理グループにマッピングし、必要なデータおよびメニューアクセス権限を割り当て、[Save]をクリックします。

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

Authentication

Authorization

Permissions

RBAC Policy

Administrators

Settings

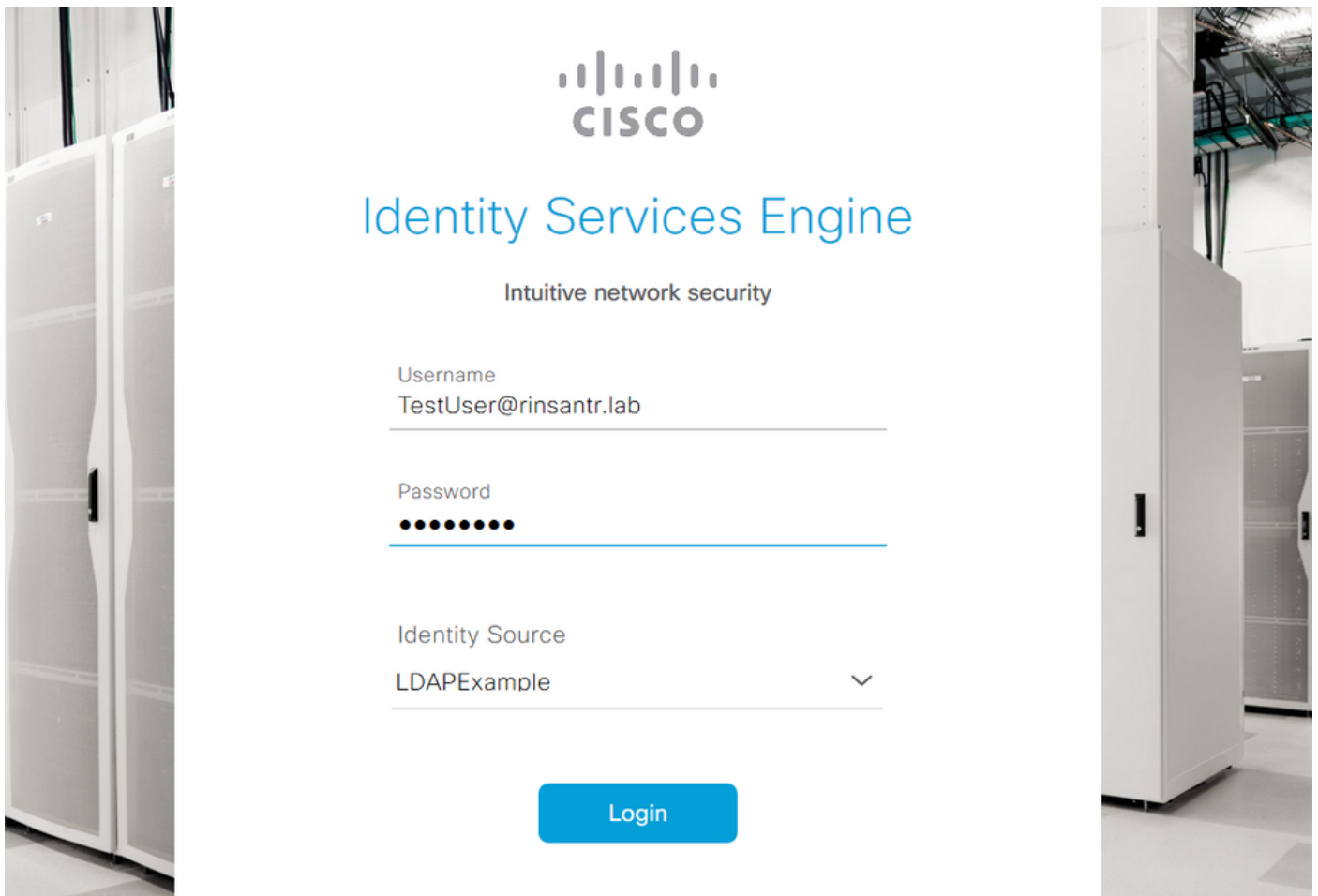
Create Role Based Access Control policies by configuring rules based on Admin groups, Menu Access permissions (menu items), Data Access permissions (identity group data element). Menu/Data Access permissions are not allowed on a single policy. You can copy the default policies shown below, then modify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

RBAC Policies

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

## LDAPクレデンシャルによるISEへのアクセスと確認

管理 GUI からログアウトします。[IDソース]ドロップダウンメニューからLDAP名を選択します。LDAPデータベースからユーザ名とパスワードを入力し、ログインします。



設定が正常に動作していることを確認するには、ISE GUIの右上隅にある[Settings] アイコンから認証されたユーザ名を確認します。[サーバ情報]に移動し、ユーザ名を確認します。





## 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**