

# Richtlinien für Administratorzugriff und RBAC auf der ISE verstehen

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Authentifizierungseinstellungen](#)

[Admin-Gruppen konfigurieren](#)

[Admin-Benutzer konfigurieren](#)

[Berechtigungen konfigurieren](#)

[RBAC-Richtlinien konfigurieren](#)

[Konfigurieren der Einstellungen für den Administratorzugriff](#)

[Konfigurieren des Admin-Portalzugriffs mit AD-Anmeldeinformationen](#)

[Werden Sie Teil der ISE](#)

[Verzeichnisgruppen auswählen](#)

[Administratorzugriff für AD aktivieren](#)

[Konfigurieren der ISE-Admin-Gruppe für AD-Gruppenzuordnung](#)

[RBAC-Berechtigungen für die Admin-Gruppe festlegen](#)

[Zugriff auf die ISE mit AD-Anmeldeinformationen und Überprüfung](#)

[Konfigurieren des Admin-Portalzugriffs mit LDAP](#)

[Beitritt zur ISE zum LDAP](#)

[Administratorzugriff für LDAP-Benutzer aktivieren](#)

[Zuordnung der ISE-Admin-Gruppe zur LDAP-Gruppe](#)

[RBAC-Berechtigungen für die Admin-Gruppe festlegen](#)

[Zugriff auf ISE mit LDAP-Anmeldeinformationen und Überprüfen](#)

## Einführung

Dieses Dokument beschreibt die Funktionen der ISE zur Verwaltung des administrativen Zugriffs auf die Identity Services Engine (ISE).

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über die folgenden Themen zu verfügen:

- ISE
- Active Directory

- Lightweight Directory Access Protocol (LDAP)

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

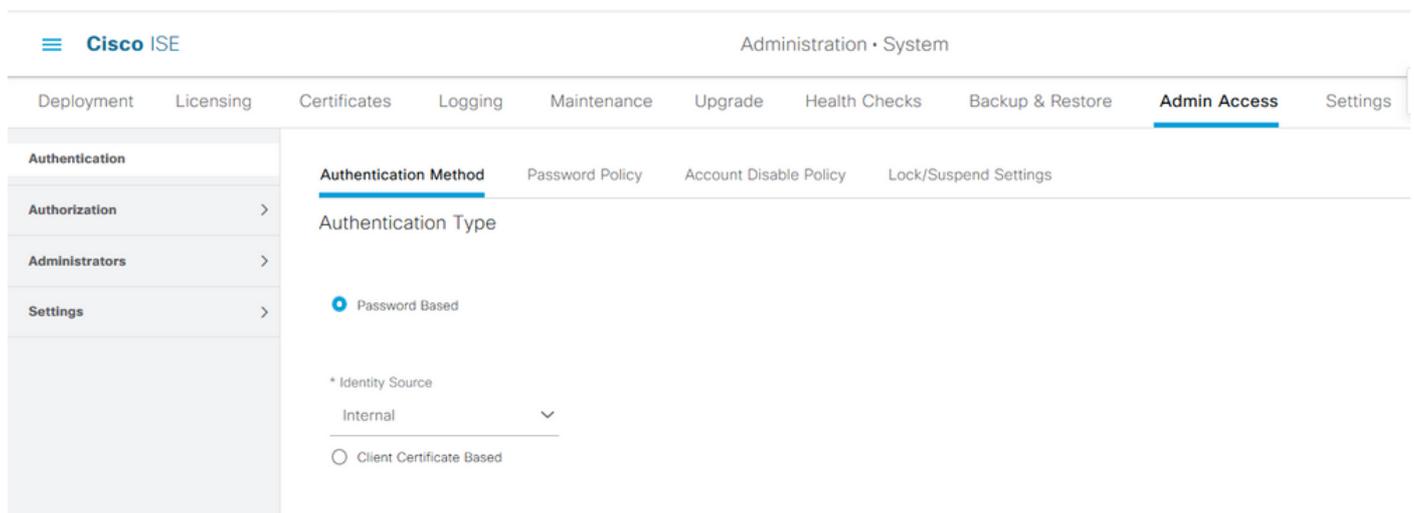
- Identity Services Engine 3.0
- Windows Server 2016

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konfigurieren

### Authentifizierungseinstellungen

Admin-Benutzer müssen sich authentifizieren, um auf Informationen zur ISE zugreifen zu können. Die Identität von Admin-Benutzern kann mithilfe des ISE Internal Identity Store oder eines externen Identity Store überprüft werden. Die Authentizität kann entweder durch ein Kennwort oder ein Zertifikat überprüft werden. Um diese Einstellungen zu konfigurieren, navigieren Sie zu **Administration > System > Admin Access > Authentication**. Wählen Sie auf der Registerkarte **Authentifizierungsmethode** den gewünschten Authentifizierungstyp aus.



**Hinweis:** Die kennwortbasierte Authentifizierung ist standardmäßig aktiviert. Wenn diese in Client Certificate-Based Authentication geändert wird, wird ein Neustart des Anwendungsservers auf allen Bereitstellungsknoten ausgelöst.

Die Identity Services Engine ermöglicht es nicht, die Kennwortrichtlinie für die Befehlszeilenschnittstelle (CLI) über die CLI zu konfigurieren. Die Kennwortrichtlinie für die grafische Benutzeroberfläche (GUI) und die CLI kann nur über die GUI der ISE konfiguriert werden. Um dies zu konfigurieren, navigieren Sie zu **Administration > System > Admin Access > Authentication (Verwaltung > Administratorzugriff > Authentifizierung)**, und navigieren Sie zur Registerkarte **Password Policy (Kennwortrichtlinie)**.

## 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)

Die ISE bietet die Möglichkeit, inaktive Admin-Benutzer zu deaktivieren. Um dies zu konfigurieren, navigieren Sie zu **Administration > System > Admin Access > Authentication (Verwaltung > Administratorzugriff > Authentifizierung)**, und navigieren Sie zur Registerkarte **Account Disable Policy (Kontodeaktivieren)**.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration - System' and a warning icon. Below it, a secondary navigation bar lists various system functions: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, and Admin Access (which is highlighted). On the left, a sidebar menu shows 'Authentication' selected, with sub-items for Authorization, Administrators, and Settings. The main content area is titled 'Account Disable Policy' and contains a checkbox labeled 'Disable account after' which is checked. Next to it is a text input field containing the number '30', followed by the text 'days of inactivity. (Valid range 1 to 365)'.

Die ISE bietet außerdem die Möglichkeit, ein Admin-Benutzerkonto basierend auf der Anzahl der fehlgeschlagenen Anmeldeversuche zu sperren oder auszusetzen. Um dies zu konfigurieren, navigieren Sie zu **Administration > System > Admin Access > Authentication (Verwaltung > Admin-Zugriff > Authentifizierung)**, und navigieren Sie zur Registerkarte **Lock/Suspend Settings (Sperreinstellungen)**.

The screenshot shows the Cisco ISE Administration interface, specifically the 'Lock/Suspend Settings' configuration page. The top navigation bar is identical to the previous screenshot. The sidebar menu is also the same. The main content area is titled 'Lock/Suspend Settings' and features a checkbox labeled 'Suspend or Lock Account with Incorrect Login Attempts' which is checked. Below this, there are three radio button options: 'Take action after' (selected), 'Suspend account for', and 'Lock account'. The 'Take action after' option has a value of '3' and the text 'failed attempts (Valid Range 3 to 20)'. The 'Suspend account for' option has a value of '15' and the text 'minutes (Valid Range 15 to 1440)'. Below these options is a text area for 'Email remediation message' containing the text: 'This account has been locked. For this account to become unlocked, please contact your IT helpdesk.'

Für die Verwaltung des administrativen Zugriffs müssen Verwaltungsgruppen, Benutzer und verschiedene Richtlinien/Regeln ihre Berechtigungen steuern und verwalten.

## Admin-Gruppen konfigurieren

Navigieren Sie zu **Administration > System > Admin Access > Administrator Groups (Verwaltung > Administratorzugriff > Administratoren > Admin-Gruppen)**, um Administratorgruppen zu konfigurieren. Es gibt nur wenige Gruppen, die standardmäßig integriert sind und nicht gelöscht werden können.

- 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 ...

Wählen Sie nach dem Erstellen einer Gruppe die Gruppe aus, und klicken Sie auf Bearbeiten, um dieser Gruppe Administratorbenutzer hinzuzufügen. Es besteht die Möglichkeit, den Admin-Gruppen auf der ISE externe Identitätsgruppen zuzuordnen, sodass ein externer Admin-Benutzer die erforderlichen Berechtigungen erhält. Um dies zu konfigurieren, wählen Sie den Typ External aus, und fügen Sie den Benutzer hinzu.

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

Admin Groups > Super Admin

### Admin Group

\* Name

Description

Type  External

#### External Identity Source

Name :

#### External Groups

\*

#### Member Users

Users

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

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

## Admin-Benutzer konfigurieren

Um Admin-Benutzer zu konfigurieren, navigieren Sie zu **Administration > System > Admin Access > Administrator > Admin Users**.

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

Klicken Sie auf **Hinzufügen**. Es stehen zwei Optionen zur Auswahl. Eine besteht darin, einen neuen Benutzer ganz hinzuzufügen. Die andere Möglichkeit besteht darin, einen Netzwerkzugriffsbenuer (d. h. einen Benutzer, der als interner Benutzer für den Zugriff auf das Netzwerk/die Geräte konfiguriert ist) als ISE-Administrator festzulegen.

Administrators

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

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

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

Nachdem Sie eine Option ausgewählt haben, müssen die erforderlichen Details angegeben und die Benutzergruppe auf der Grundlage der Berechtigungen und Berechtigungen ausgewählt werden, die dem Benutzer erteilt werden.

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 ▼

## Berechtigungen konfigurieren

Es gibt zwei Arten von Berechtigungen, die für eine Benutzergruppe konfiguriert werden können:

1. Menüzugriff
2. Datenzugriff

Über Menüzugriff wird die Navigationstransparenz auf der ISE gesteuert. Für jede Registerkarte gibt es zwei Optionen: Anzeigen oder Ausblenden, die konfiguriert werden können. Mit einer Regel für den Menüzugriff können ausgewählte Registerkarten ein- oder ausgeblendet werden.

Der Datenzugriff kontrolliert die Möglichkeit, die Identitätsdaten der ISE zu lesen, darauf zuzugreifen und zu ändern. Die Zugriffsberechtigung kann nur für Admin-Gruppen, Benutzeridentitätsgruppen, Endpunkt-Identitätsgruppen und Netzwerkgerätegruppen konfiguriert werden. Für diese Entitäten auf der ISE stehen drei Optionen zur Verfügung, die konfiguriert werden können. Es handelt sich um uneingeschränkten Zugriff, schreibgeschützten Zugriff und keinen Zugriff. Eine Datenzugriffsregel kann so konfiguriert werden, dass sie für jede Registerkarte der ISE eine dieser drei Optionen auswählt.

Menüzugriff und Datenzugriffsrichtlinien müssen erstellt werden, bevor sie auf eine beliebige

Admin-Gruppe angewendet werden können. Es gibt einige Richtlinien, die standardmäßig integriert sind, aber immer angepasst oder neu erstellt werden können.

Um eine Menüzugriffsrichtlinie zu konfigurieren, navigieren Sie zu **Administration > System > Admin Access > Authorization > Permissions > Menu Access (Verwaltung > Administratorzugriff > Autorisierung > Berechtigungen > Menüzugriff)**.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Cisco ISE' and 'Administration · System'. Below this, a secondary navigation bar lists various system functions: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, and Admin Access (which is currently selected). On the left side, there is a sidebar menu with categories like Authentication, Authorization, Permissions, Menu Access, Data Access, RBAC Policy, Administrators, and Settings. The main content area is titled 'Menu Access' and contains a table of permissions. Above the table are action buttons: Edit, Add, Duplicate, and Delete. The table has two columns: 'Name' and 'Description'. Each row in the table starts with a checkbox in the Name column.

<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

Klicken Sie auf **Hinzufügen**. Jede Navigationsoption in der ISE kann so konfiguriert werden, dass sie in einer Richtlinie angezeigt/ausgeblendet wird.

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

Authentication

Authorization

Permissions

**Menu Access**

Data Access

RBAC Policy

Administrators

Settings

Menu Access List > New RBAC Menu Access

### Create Menu Access Permission

\* Name: Custom\_Menu\_Access

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

Um die Datenzugriffsrichtlinie zu konfigurieren, navigieren Sie zu **Administration > System > Admin Access > Authorization > Permissions > Data Access (Verwaltung > System > Administratorzugriff > Autorisierung > Berechtigungen > Datenzugriff)**.

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.

Klicken Sie auf **Hinzufügen**, um eine neue Richtlinie zu erstellen und Berechtigungen für den Zugriff auf die Identität von Admin/Benutzer/Endpunkt/Netzwerkgruppen zu konfigurieren.

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

## RBAC-Richtlinien konfigurieren

RBAC steht für rollenbasierte Zugriffskontrolle. Die Rolle (Admin-Gruppe), der ein Benutzer angehört, kann für die Verwendung des gewünschten Menüs und der Datenzugriffsrichtlinien konfiguriert werden. Es können mehrere RBAC-Richtlinien für eine einzelne Rolle konfiguriert werden, ODER es können mehrere Rollen in einer einzelnen Richtlinie konfiguriert werden, um auf Menü und/oder Daten zuzugreifen. Alle diese geltenden Richtlinien werden ausgewertet, wenn ein Administrator versucht, eine Aktion auszuführen. Die endgültige Entscheidung ist die Gesamtheit aller für diese Rolle geltenden Richtlinien. Wenn es widersprüchliche Regeln gibt, die gleichzeitig zulassen und verweigern, überschreibt die Genehmigungsregel die Deny-Regel. Um diese Richtlinien zu konfigurieren, navigieren Sie zu **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). 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).

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

Klicken Sie auf **Aktionen**, um eine Richtlinie zu duplizieren/einzufügen/zu löschen.

**Hinweis:** Vom System erstellte und Standard-Richtlinien können nicht aktualisiert werden, und Standardrichtlinien können nicht gelöscht werden.

**Hinweis:** Mehrere Menü-/Datenzugriffsberechtigungen können nicht in einer Regel konfiguriert werden.

## Konfigurieren der Einstellungen für den Administratorzugriff

Zusätzlich zu den RBAC-Richtlinien können einige Einstellungen konfiguriert werden, die allen Admin-Benutzern gemeinsam sind.

Um die Anzahl der maximal zulässigen Sitzungen, Banner vor der Anmeldung und Banner nach der Anmeldung für die GUI und die CLI zu konfigurieren, navigieren Sie zu **Administration > System > Admin Access > Settings > Access (Verwaltung > Administratorzugriff > Einstellungen > Zugriff)**. Konfigurieren Sie diese auf der Registerkarte **Sitzung**.

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

Um die Liste der IP-Adressen zu konfigurieren, von denen aus auf die GUI und die CLI zugegriffen werden kann, navigieren Sie zu **Administration > System > Admin Access > Settings > Access** und navigieren Sie zur Registerkarte **IP Access (IP-Zugriff)**.

Cisco ISE

Administration • System

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

Authentication

Authorization >

Administrators >

Settings ▾

Access

Session

Portal Customization

Session   **IP Access**   MnT Access

▼ Access Restriction

Allow all IP addresses to connect

Allow only listed IP addresses to connect

▼ Configure IP List for Access Restriction

IP List

+ Add   Edit   Delete

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

Um eine Liste von Knoten zu konfigurieren, von denen Administratoren auf den MnT-Bereich in der Cisco ISE zugreifen können, navigieren Sie zu **Administration > System > Admin Access > Settings > Access (Verwaltung > Administratorzugriff > Einstellungen > Zugriff)** und navigieren Sie zur Registerkarte **MnT Access (Zugriff auf MnT)**.

Wenn Knoten oder Einheiten innerhalb oder außerhalb der Bereitstellung Syslogs an MnT senden möchten, klicken Sie auf das Optionsfeld **Allow any IP address to connect to MNT (IP-Adresse darf mit MNT verbunden werden)**. Wenn nur Knoten oder Entitäten innerhalb der Bereitstellung Syslogs an MnT senden möchten, klicken Sie auf das Optionsfeld **Nur die Knoten in der Bereitstellung können eine Verbindung mit dem MNT herstellen**.

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

**Hinweis:** Für ISE 2.6 Patch 2 und höher ist *"ISE Messaging Service"* für die Bereitstellung von UDP-Syslogs an MnT standardmäßig aktiviert, sodass Syslogs von anderen Einheiten außerhalb der Bereitstellung nicht zugelassen werden.

Um einen Timeout-Wert aufgrund der Inaktivität einer Sitzung zu konfigurieren, navigieren Sie zu **Administration > System > Admin Access > Settings > Session**. Legen Sie diesen Wert auf der Registerkarte **Session Timeout** fest.

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

Um die aktuellen aktiven Sitzungen anzuzeigen/für ungültig zu erklären, navigieren Sie zu **Administration > Admin Access > Settings > Session** und klicken Sie auf die Registerkarte **Session Info (Sitzungsinformationen)**.

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

## Konfigurieren des Admin-Portalzugriffs mit AD-Anmeldeinformationen

### Werden Sie Teil der ISE

Um der ISE zu einer externen Domäne beizutreten, navigieren Sie zu **Administration > Identity Management > External Identity Sources > Active Directory**. Geben Sie den neuen Join-Punktnamen und die Active Directory-Domäne ein. Geben Sie die Anmeldeinformationen des AD-Kontos ein, das Computerobjekte hinzufügen und ändern kann, und klicken Sie auf **OK**.

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 PassiveID 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

## Verzeichnisgruppen auswählen

Navigieren Sie zu **Administration > Identity Management > External Identity Sources > Active Directory**. Klicken Sie auf den gewünschten Join Point-Namen, und navigieren Sie zur Registerkarte **Groups**. Klicken Sie auf **Hinzufügen > Gruppen aus Verzeichnis auswählen > Gruppen abrufen**. Importieren Sie mindestens eine AD-Gruppe, der Ihr Administrator angehört, und klicken Sie auf **OK**, und klicken Sie dann auf **Speichern**.

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 Filter \*    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

Connection	Whitelisted Domains	PassiveID	<b>Groups</b>	Attributes	Advanced Settings
<a href="#">Edit</a>	<a href="#">+ Add</a>	<a href="#">Delete Group</a>	<a href="#">Update SID Values</a>		
<input type="checkbox"/>	Name			SID	
<input type="checkbox"/>	rinsantr.lab/Users/Test Group			S-1-5-21-1977851106-3699455990-2945865208-1106	

## Administratorzugriff für AD aktivieren

Um die kennwortbasierte Authentifizierung der ISE über AD zu aktivieren, navigieren Sie zu **Administration > System > Admin Access > Authentication (Verwaltung > Admin-Zugriff > Authentifizierung)**. Wählen Sie auf der Registerkarte **Authentication Method** die Option **Password-Based (Kennwortbasiert)** aus. Wählen Sie **AD** aus dem Dropdown-Menü **Identitätsquelle** aus, und klicken Sie auf **Speichern**.

The screenshot shows the Cisco ISE Administration console. The navigation path is **Administration > System > Admin Access > Authentication**. 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.

## Konfigurieren der ISE-Admin-Gruppe für AD-Gruppenzuordnung

Dadurch kann der Administrator anhand der Gruppenmitgliedschaft in AD die Berechtigungen für die rollenbasierte Zugriffskontrolle (Role Based Access Control, RBAC) festlegen. Um eine Cisco ISE-Admin-Gruppe zu definieren und einer AD-Gruppe zuzuordnen, navigieren Sie zu **Administration > System > Admin Access > Administrator Groups**. Klicken Sie auf **Hinzufügen**, und geben Sie einen Namen für die neue Admin-Gruppe ein. Aktivieren Sie im Feld Typ das Kontrollkästchen **Extern**. Wählen Sie im Dropdown-Menü **Externe Gruppen** die AD-Gruppe aus, der diese Admin-Gruppe zugeordnet werden soll (wie im Abschnitt **Select Directory Groups (Verzeichnisgruppen auswählen)** oben definiert). **Senden Sie** die Änderungen.

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					

## RBAC-Berechtigungen für die Admin-Gruppe festlegen

Um der im vorherigen Abschnitt erstellten Admin Group RBAC-Berechtigungen zuzuweisen, navigieren Sie zu **Administration > System > Admin Access > Authorization > RBAC Policy**. Wählen Sie im Dropdown-Menü **Aktionen** rechts die Option **Neue Richtlinie einfügen aus**. Erstellen Sie eine neue Regel, ordnen Sie sie der im oben genannten Abschnitt definierten Administratorgruppe zu, und weisen Sie ihr die gewünschten Daten- und Menüzugriffsberechtigungen zu. Klicken Sie anschließend auf **Speichern**.

Cisco ISE Administration • System

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

Authentication

**Authorization** >

Permissions >

**RBAC Policy**

Administrators >

Settings >

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

> RBAC Policies

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

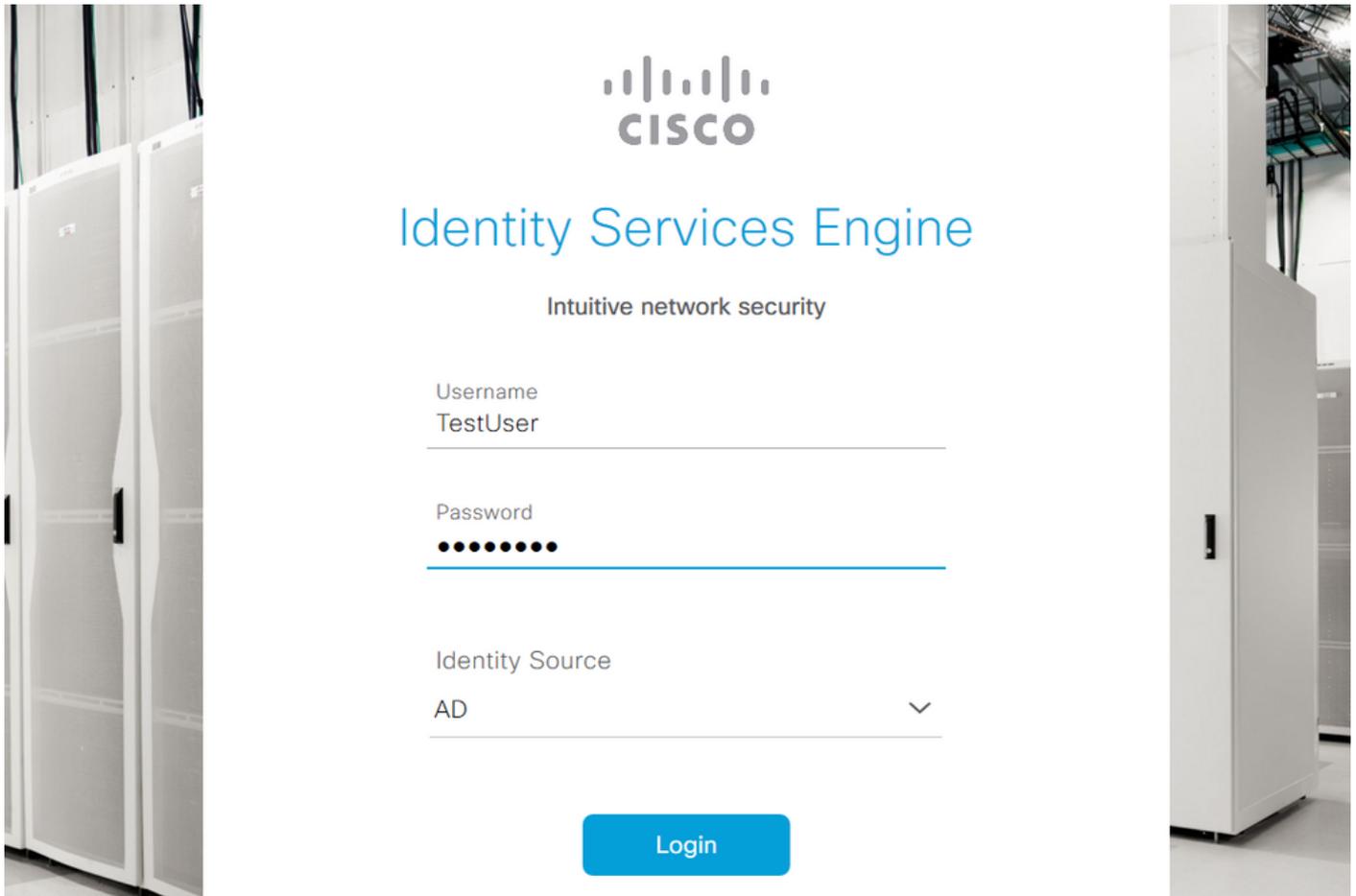
Super Admin Menu Access > +

Super Admin Data Access > +

## Zugriff auf die ISE mit AD-Anmeldeinformationen und Überprüfung

Melden Sie sich von der Verwaltungs-GUI ab. Wählen Sie im Dropdown-Menü **Identitätsquelle** den Namen des Join Point aus. Geben Sie den Benutzernamen und das Kennwort aus der AD-

Datenbank ein, und melden Sie sich an.



**CISCO**

## Identity Services Engine

Intuitive network security

Username  
TestUser

Password  
●●●●●●●●

Identity Source  
AD

Login

Um zu überprüfen, ob die Konfiguration ordnungsgemäß funktioniert, überprüfen Sie den authentifizierten Benutzernamen über das Symbol **Einstellungen** oben rechts in der ISE-GUI. Navigieren Sie zu **Serverinformationen**, und überprüfen Sie den Benutzernamen.

## 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

## Konfigurieren des Admin-Portalzugriffs mit LDAP

### Beitritt zur ISE zum LDAP

Navigieren Sie zu **Administration > Identity Management > External Identity Sources > Active Directory > LDAP**. Geben Sie auf der Registerkarte **Allgemein** einen Namen für das LDAP ein, und wählen Sie das Schema als **Active Directory** aus.

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  ▼

Navigieren Sie anschließend zur Registerkarte **Verbindung**, um den Verbindungstyp zu konfigurieren. Legen Sie hier den Hostnamen/die IP-Adresse des primären LDAP-Servers zusammen mit dem Port 389(LDAP)/636 (LDAP-Secure) fest. Geben Sie den Pfad des DN's mit dem Administratorkennwort des LDAP-Servers ein.

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

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

	Primary Server		Secondary Server
			<input type="checkbox"/> Enable Secondary Server
* Hostname/IP	<input type="text" value="10.127.196.131"/> ⓘ	Hostname/IP	<input type="text"/>
* Port	<input type="text" value="389"/>	Port	<input type="text" value="389"/>
<input type="checkbox"/> Specify server for each ISE node			
Access	<input type="radio"/> Anonymous Access <input checked="" type="radio"/> Authenticated Access	Access	<input checked="" type="radio"/> Anonymous Access <input type="radio"/> Authenticated Access
Admin DN	<input type="text" value="* CN=Administrator,CN=Users,DC"/>	Admin DN	<input type="text" value="admin"/>
Password	<input type="text" value="* ....."/>	Password	<input type="text"/>
Secure Authentication	<input type="checkbox"/> Enable Secure Authentication	Secure Authentication	<input type="checkbox"/> Enable Secure Authentication

Navigieren Sie anschließend zur Registerkarte **Verzeichnisorganisation**, und klicken Sie auf **Naming Contexts**, um die richtige Organisationsgruppe des Benutzers auf Basis der Hierarchie der auf dem LDAP-Server gespeicherten Benutzer auszuwählen.

## 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

Klicken Sie auf **Test Bind to Server** unter der Registerkarte **Connection (Verbindung)**, um die Erreichbarkeit des LDAP-Servers von der ISE zu testen.

The screenshot shows a configuration page with tabs: General, **Connection**, Directory Organization, Groups, Attributes, and Advanced. The 'Connection' tab is active. A white dialog box is centered on the screen with the following text:

Ldap bind succeeded to 10.127.196.131:389  
Number of Subjects 8  
Number of Groups 50  
Response time 7ms

At the bottom right of the dialog box is an 'OK' button. Below the dialog box, the configuration page shows fields for:

- \* Server Timeout: 10 (Seconds)
- \* Max. Admin Connections: 20
- Force reconnect every (Minutes)

At the bottom of the configuration page is a 'Test Bind to Server' button.

Navigieren Sie jetzt zur Registerkarte **Gruppen**, und klicken Sie auf **Hinzufügen > Gruppen aus Verzeichnis auswählen > Gruppen abrufen**. Importieren Sie mindestens eine Gruppe, der Ihr Administrator angehört, und klicken Sie auf **OK**, und klicken Sie dann auf **Speichern**.

## Select Directory Groups

This dialog is used to select groups from the Directory. Click **Retrieve Groups..** to read directory.

Filter: \* Retrieve Groups... Number of Groups Retrieved: 50 (Limit is 100)

<input type="checkbox"/>	Name
<input type="checkbox"/>	CN=Server Operators,CN=Builtin,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=Storage Replica Administrators,CN=Builtin,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=System Managed Accounts Group,CN=Builtin,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=Terminal Server License Servers,CN=Builtin,DC=rinsantr,DC=lab
<input checked="" type="checkbox"/>	CN=Test Group,CN=Users,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=Users,CN=Builtin,DC=rinsantr,DC=lab
<input type="checkbox"/>	CN=Windows Authorization Access Group,CN=Builtin,DC=rinsantr,DC=lab

Cancel OK

**Internal Identity Sources**

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

LDAP Identity Sources List > LDAPExample

### LDAP Identity Source

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

 Edit    Add    Delete Group

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

## Administratorzugriff für LDAP-Benutzer aktivieren

Um die kennwortbasierte Authentifizierung der ISE über LDAP zu aktivieren, navigieren Sie zu **Administration > System > Admin Access > Authentication**. Wählen Sie auf der Registerkarte **Authentication Method** die Option **Password-Based (Kennwortbasiert)** aus. Wählen Sie **LDAP** aus dem Dropdown-Menü **Identitätsquelle** aus, und klicken Sie auf **Speichern**.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The 'Admin Access' tab is active. 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 'LDAP:LDAPExample|'. There is also an option for 'Client Certificate Based' which is not selected. A 'Save' button is located at the bottom right of the configuration area.

## Zuordnung der ISE-Admin-Gruppe zur LDAP-Gruppe

Auf diese Weise erhält der konfigurierte Benutzer Administratorzugriff, basierend auf der Autorisierung der RBAC-Richtlinien, die wiederum auf der LDAP-Gruppenmitgliedschaft des Benutzers basieren. Um eine Cisco ISE-Admin-Gruppe zu definieren und einer LDAP-Gruppe zuzuordnen, navigieren Sie zu **Administration > System > Admin Access > Administrator Groups**. Klicken Sie auf **Hinzufügen**, und geben Sie einen Namen für die neue Admin-Gruppe ein. Aktivieren Sie im Feld Typ das Kontrollkästchen **Extern**. Wählen Sie im Dropdown-Menü **Externe Gruppen** die LDAP-Gruppe aus, der diese Admin-Gruppe zugeordnet werden soll (wie zuvor abgehört und definiert). **Senden Sie** die Änderungen.

The screenshot shows the Cisco ISE Administration console for creating a new admin group. The top navigation bar is the same as in the previous screenshot. The 'Admin Access' tab is active, and the 'Administrator Groups' sub-tab is selected. The main content area is titled 'Admin Group' and includes the following fields: '\* Name' (ISE LDAP Admin Group), 'Description' (empty text area), 'Type' (checked 'External'), and 'External Identity Source' (Name: LDAPExample). Below these fields is a section for 'External Groups' with a dropdown menu showing 'CN=Test Group,CN=Users,DC=' and a plus sign to add more groups. A 'Save' button is located at the bottom right of the configuration area.

## RBAC-Berechtigungen für die Admin-Gruppe festlegen

Um der im vorherigen Abschnitt erstellten Admin Group RBAC-Berechtigungen zuzuweisen, navigieren Sie zu **Administration > System > Admin Access > Authorization > RBAC Policy**. Wählen Sie im Dropdown-Menü **Aktionen** rechts die Option **Neue Richtlinie einfügen aus**. Erstellen Sie eine neue Regel, ordnen Sie sie der im oben genannten Abschnitt definierten

Administratorgruppe zu, und weisen Sie ihr die gewünschten Daten- und Menüzugriffsberechtigungen zu. Klicken Sie anschließend auf **Speichern**.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Administration · System' and an 'Evaluate' warning icon. The left sidebar contains navigation options: Authentication, Authorization (selected), Permissions, RBAC Policy, Administrators, and Settings. The main content area displays 'RBAC Policies' with a table of existing policies and a context menu for editing permissions.

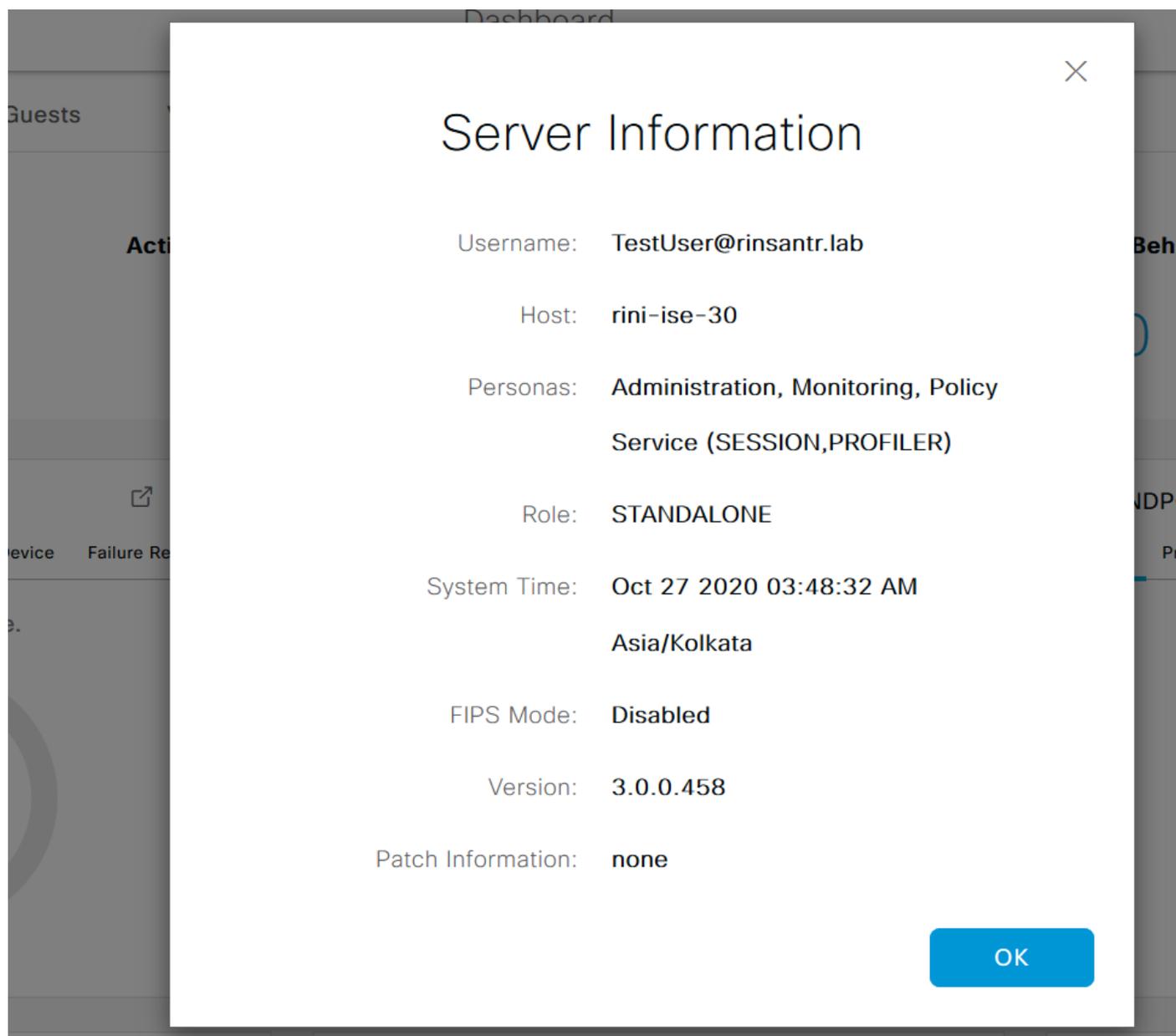
Rule Name	Admin Groups	Permissions
Customization Admin Policy	Customization Admin	Customization Admin Menu ...
RBAC Policy 2	ISE LDAP Admin Group	Super Admin Menu Access a...
Elevated System Admin Poli	Elevated System Admin	
ERS Admin Policy	ERS Admin	
ERS Operator Policy	ERS Operator	
ERS Trustsec Policy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

## Zugriff auf ISE mit LDAP-Anmeldeinformationen und Überprüfen

Melden Sie sich von der Verwaltungs-GUI ab. Wählen Sie den LDAP-Namen aus dem Dropdown-Menü **Identitätsquelle** aus. Geben Sie den Benutzernamen und das Kennwort aus der LDAP-Datenbank ein, und melden Sie sich an.

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

Um zu überprüfen, ob die Konfiguration ordnungsgemäß funktioniert, überprüfen Sie den authentifizierten Benutzernamen über das Symbol **Einstellungen** oben rechts in der ISE-GUI. Navigieren Sie zu **Serverinformationen**, und überprüfen Sie den Benutzernamen.



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

- Username: TestUser@rinsantr.lab
- Host: rini-ise-30
- Personas: Administration, Monitoring, Policy Service (SESSION,PROFILER)
- Role: STANDALONE
- System Time: Oct 27 2020 03:48:32 AM Asia/Kolkata
- FIPS Mode: Disabled
- Version: 3.0.0.458
- Patch Information: none

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