

# Comprendere le policy RBAC e di accesso degli amministratori su ISE

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Impostazioni autenticazione](#)

[Configura gruppi amministrativi](#)

[Configura utenti amministratori](#)

[Configura autorizzazioni](#)

[Configura criteri RBAC](#)

[Configura impostazioni per accesso amministratore](#)

[Configura accesso al portale di amministrazione con credenziali AD](#)

[Partecipa ad ISE e AD](#)

[Seleziona gruppi di directory](#)

[Abilita accesso amministrativo per AD](#)

[Configurazione del mapping tra il gruppo di amministratori ISE e il gruppo AD](#)

[Impostare le autorizzazioni RBAC per il gruppo Admin](#)

[Accesso a ISE con credenziali AD e verifica](#)

[Configura accesso al portale di amministrazione con LDAP](#)

[Unisci ISE a LDAP](#)

[Abilita accesso amministrativo per utenti LDAP](#)

[Mappa il gruppo di amministratori ISE al gruppo LDAP](#)

[Impostare le autorizzazioni RBAC per il gruppo Admin](#)

[Accesso a ISE con credenziali LDAP e verifica](#)

## Introduzione

Questo documento descrive le funzionalità di ISE per gestire l'accesso amministrativo su Identity Services Engine (ISE).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ISE
- Active Directory

- Protocollo LDAP (Lightweight Directory Access Protocol)

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

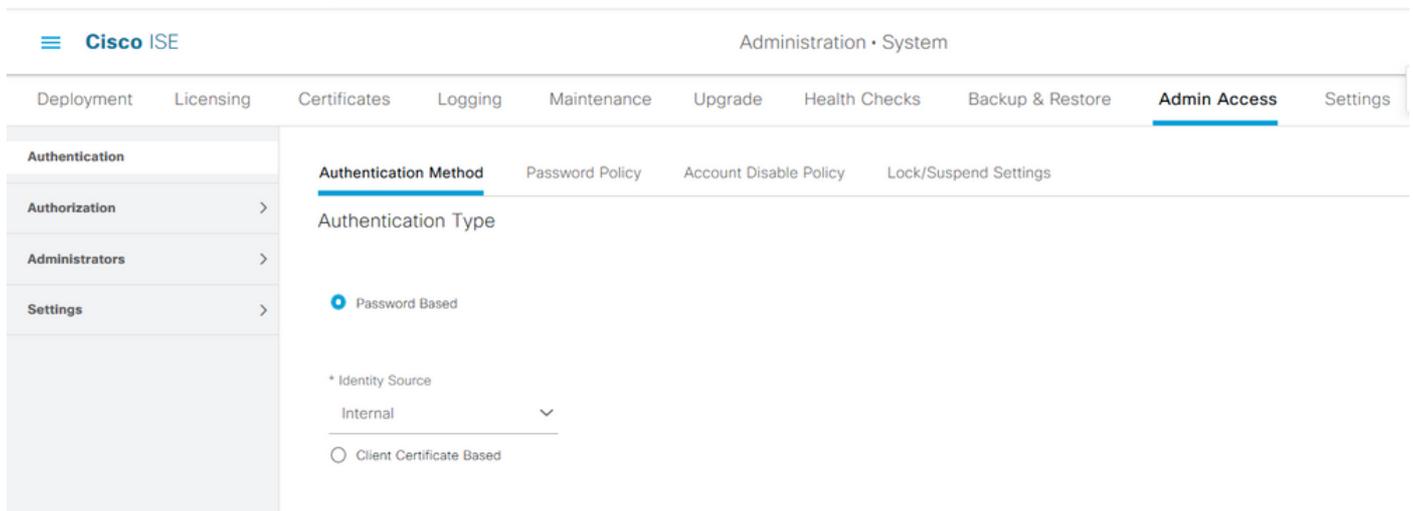
- Identity Services Engine 3.0
- Windows Server 2016

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Configurazione

### Impostazioni autenticazione

Gli utenti amministratori devono autenticarsi per accedere a qualsiasi informazione su ISE. L'identità degli utenti amministratori può essere verificata usando ISE Internal Identity Store o External Identity Store. L'autenticità può essere verificata mediante una password o un certificato. Per configurare queste impostazioni, selezionare **Amministrazione > Sistema > Accesso amministratore > Autenticazione**. Selezionare il tipo di autenticazione richiesto nella scheda **Metodo di autenticazione**.



**Nota:** L'autenticazione basata su password è abilitata per impostazione predefinita. Se questa opzione viene modificata in Autenticazione basata su certificati client, il server applicazioni verrà riavviato in tutti i nodi di distribuzione.

Identity Services Engine non consente di configurare i criteri password per l'interfaccia della riga di comando (CLI) dalla CLI. I criteri per la password sia per l'interfaccia utente grafica (GUI) che per la CLI possono essere configurati solo tramite la GUI di ISE. Per configurare questa impostazione, selezionare **Amministrazione > Sistema > Accesso amministratore > Autenticazione** e selezionare la scheda **Criteri password**.

Authentication

Authorization >

Administrators >

Settings >

## GUI and CLI Password Policy

\* Minimum Length: 4 characters (Valid Range 4 to 127)

**Password must not contain:**

- Admin name or its characters in reverse order
- \* cisco\* or its characters in reverse order
- This word or its characters in reverse order: \_\_\_\_\_
- Repeated characters four or more times consecutively
- Dictionary words, their characters in reverse order or their letters replaced with other characters ⓘ
  - Default Dictionary ⓘ
  - Custom Dictionary ⓘ  No file selected.

**The newly added custom dictionary file will replace the existing custom dictionary file.**

Authentication

Authorization >

Administrators >

Settings >

**Password must contain at least one character of each of the selected types:**

- Lowercase alphabetic characters
- Uppercase alphabetic characters
- Numeric characters
- Non-alphanumeric characters

**Password History**

- Password must be different from the previous 3 versions [When enabled CLI remembers only last 1 password irrespective of value configured]

\* Cannot reuse password within 15 days (Valid Range 0 to 365)

**Password Lifetime**

Admins can be required to periodically change their password

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

- Administrator passwords expire 45 days after creation or last change (valid range 1 to 3650)
- Send an email reminder to administrators 30 days prior to password expiration (valid range 1 to 3650)

ISE prevede la disabilitazione di un utente amministratore inattivo. Per configurare questa impostazione, selezionare **Amministrazione > Sistema > Accesso amministratore > Autenticazione** e passare alla scheda **Criteri di disabilitazione account**.

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 contains 'Authentication', 'Authorization', 'Administrators', and 'Settings'. The main content area is titled 'Account Disable Policy' and features a sub-menu with 'Authentication Method', 'Password Policy', 'Account Disable Policy' (highlighted), and 'Lock/Suspend Settings'. The configuration shows a checked checkbox for 'Disable account after' followed by a text input field containing '30' and the label 'days of inactivity. (Valid range 1 to 365)'.

ISE offre anche la possibilità di bloccare o sospendere un account utente amministratore in base al numero di tentativi di accesso non riusciti. Per configurare questa impostazione, selezionare **Amministrazione > Sistema > Accesso amministratore > Autenticazione** e selezionare la scheda **Blocca/Sospendi impostazioni**.

The screenshot shows the Cisco ISE Administration interface for the 'Lock/Suspend Settings' configuration. 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 sub-menu with 'Authentication Method', 'Password Policy', 'Account Disable Policy', and 'Lock/Suspend Settings' (highlighted). The configuration shows a checked checkbox for 'Suspend or Lock Account with Incorrect Login Attempts'. Below this, there are two radio button options: 'Take action after 3 failed attempts (Valid Range 3 to 20)' and 'Suspend account for 15 minutes (Valid Range 15 to 1440)'. The 'Suspend account for' option is selected. There is also an unchecked radio button for 'Lock account'. Below these options, there is a text input field for 'Email remediation message' containing the text: 'This account has been locked. For this account to become unlocked, please contact your IT helpdesk.'

Per gestire l'accesso amministrativo, è necessario che i gruppi amministrativi, gli utenti e varie regole/policy controllino e gestiscano i propri privilegi.

## Configura gruppi amministrativi

Passare a **Amministrazione > Sistema > Accesso amministratore > Amministratori > Gruppi di amministratori** per configurare i gruppi di amministratori. Per impostazione predefinita, esistono pochi gruppi incorporati che non possono essere eliminati.

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

Authentication		Authorization		Administrators		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 ...

Una volta creato un gruppo, selezionarlo e fare clic su Modifica per aggiungere utenti amministratori al gruppo. È disponibile un'opzione per mappare i gruppi di identità esterni ai gruppi di amministratori su ISE in modo che un utente di External Admin ottenga le autorizzazioni necessarie. Per configurare questa opzione, selezionare il tipo come Esterno durante l'aggiunta dell'utente.

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

Authentication		Authorization		Administrators		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		

## Configura utenti amministratori

Per configurare gli utenti amministratori, selezionare **Amministrazione > Sistema > Accesso amministratore > Amministratori > Utenti amministratori**.

Cisco ISE 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

Fare clic su **Add**. Sono disponibili due opzioni. Uno consiste nell'aggiungere un nuovo utente. L'altro è quello di rendere un utente con accesso alla rete (ossia un utente configurato come utente interno per accedere alla rete/alle periferiche) un amministratore ISE.

Cisco ISE 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

- 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

Dopo aver selezionato un'opzione, è necessario fornire i dettagli richiesti e selezionare il gruppo di utenti in base al quale concedere le autorizzazioni e i privilegi all'utente.

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 ▼

## Configura autorizzazioni

Per un gruppo di utenti è possibile configurare due tipi di autorizzazioni:

1. Accesso al menu
2. Accesso ai dati

Menu Access controlla la visibilità di navigazione su ISE. È possibile configurare due opzioni per ogni scheda, Mostra o Nascondi. È possibile configurare una regola di accesso ai menu per visualizzare o nascondere le schede selezionate.

Data Access controlla la capacità di leggere/accedere/modificare i dati di identità su ISE. Le autorizzazioni di accesso possono essere configurate solo per i gruppi di amministratori, i gruppi di identità degli utenti, i gruppi di identità degli endpoint e i gruppi di dispositivi di rete. Ci sono tre opzioni per queste entità su ISE che possono essere configurate. Si tratta di Accesso completo, Accesso di sola lettura e Nessun accesso. Una regola di accesso ai dati può essere configurata in modo da scegliere una di queste tre opzioni per ciascuna scheda di ISE.

È necessario creare i criteri di accesso ai menu e ai dati prima di applicarli a qualsiasi gruppo amministrativo. Per impostazione predefinita, sono disponibili alcuni criteri predefiniti che possono

tuttavia essere personalizzati o creati.

Per configurare un criterio di accesso ai menu, selezionare **Amministrazione > Sistema > Accesso amministratore > Autorizzazione > Autorizzazioni > Accesso menu**.

The screenshot shows the Cisco ISE Administration interface for 'Menu Access'. The left sidebar has 'Menu Access' selected under 'Permissions'. The main area displays a table of 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

Fare clic su **Add**. Ogni opzione di navigazione in ISE può essere configurata per essere mostrata/nascosta in una policy.

The screenshot shows the 'Create Menu Access Permission' form. The 'Name' field is set to 'Custom\_Menu\_Access'. Below the form is the 'Menu Access Privileges' section, which includes 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

Per configurare i criteri di accesso ai dati, selezionare **Amministrazione > Sistema > Accesso amministratore > Autorizzazione > Autorizzazioni > Accesso ai dati**.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Administration • System' and 'Evaluation Mode 7!'. The main menu on the left has '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 buttons 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.

Fare clic su **Add** (Aggiungi) per creare un nuovo criterio e configurare le autorizzazioni di accesso ad Amministrazione/Identità utente/Identità endpoint/Gruppi di rete.

The screenshot shows the 'Create Data Access Permission' dialog in the Cisco ISE Administration console. The 'Name' field is filled with 'Custom\_Data\_Access'. The 'Description' field is empty. Below the form is a 'Data Access Privileges' section with a list of entities and their corresponding permissions.

**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

## Configura criteri RBAC

RBAC è l'acronimo di Role-Based Access Control (Controllo degli accessi basato sui ruoli). È

possibile configurare il ruolo (gruppo amministrativo) a cui appartiene un utente per l'utilizzo dei criteri di menu e di accesso ai dati desiderati. È possibile configurare più criteri RBAC per un singolo ruolo OPPURE configurare più ruoli in un singolo criterio per accedere a Menu e/o Dati. Tutti i criteri applicabili vengono valutati quando un utente amministratore tenta di eseguire un'azione. La decisione finale è l'aggregazione di tutte le politiche applicabili a quel ruolo. Se esistono regole contraddittorie che consentono e negano contemporaneamente, la regola di autorizzazione prevale sulla regola di negazione. Per configurare questi criteri, selezionare **Amministrazione > Sistema > Accesso amministratore > Autorizzazione > Criteri RBAC**.

The screenshot shows the Cisco ISE Administration console interface. The top navigation bar includes 'Cisco ISE', 'Administration · System', and an 'Evaluate' button. The main menu on the left lists 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Se'. The 'Admin Access' section is expanded to show 'Authentication', 'Authorization', 'Permissions', 'RBAC Policy', 'Administrators', and 'Settings'. The 'RBAC Policy' section is selected, displaying a table of RBAC Policies. The table has columns for 'Rule Name', 'Admin Groups', and 'Permissions'. Each row represents a policy with a checkbox, a dropdown arrow, the policy name, a condition (If), an admin group, a logical operator (+), a consequence (then), a permission name, another logical operator (+), and an 'Actions' dropdown.

Rule Name	Admin Groups	Permissions
Customization Admin Policy	Customization Admin	Customization Admin Menu ...
Elevated System Admin Poli	Elevated System Admin	System Admin Menu Access ...
ERS Admin Policy	ERS Admin	Super Admin Data Access
ERS Operator Policy	ERS Operator	Super Admin Data Access
ERS Trustsec Policy	ERS Trustsec	Super Admin Data Access
Helpdesk Admin Policy	Helpdesk Admin	Helpdesk Admin Menu Access
Identity Admin Policy	Identity Admin	Identity Admin Menu Access ...
MnT Admin Policy	MnT Admin	MnT Admin Menu Access
Network Device Policy	Network Device Admin	Network Device Menu Acces...
Policy Admin Policy	Policy Admin	Policy Admin Menu Access a...
RBAC Admin Policiv	RBAC Admin	RBAC Admin Menu Access a...

Fare clic su **Azioni** per duplicare/inserire/eliminare un criterio.

**Nota:** Impossibile aggiornare i criteri predefiniti e creati dal sistema e non è possibile eliminare i criteri predefiniti.

**Nota:** Impossibile configurare più autorizzazioni di accesso ai dati o ai menu in un'unica regola.

## Configura impostazioni per accesso amministratore

Oltre ai criteri RBAC, è possibile configurare alcune impostazioni comuni a tutti gli utenti amministratori.

Per configurare il numero massimo di sessioni consentite, banner di pre-accesso e post-accesso per GUI e CLI, selezionare **Amministrazione > Sistema > Accesso amministratore > Impostazioni > Accesso**. Configurarle nella scheda **Sessione**.

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

Per configurare la lista di indirizzi IP da cui è possibile accedere alla GUI e alla CLI, selezionare **Amministrazione > Sistema > Accesso amministratore > Impostazioni > Accesso** e selezionare la scheda **Accesso IP**.

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

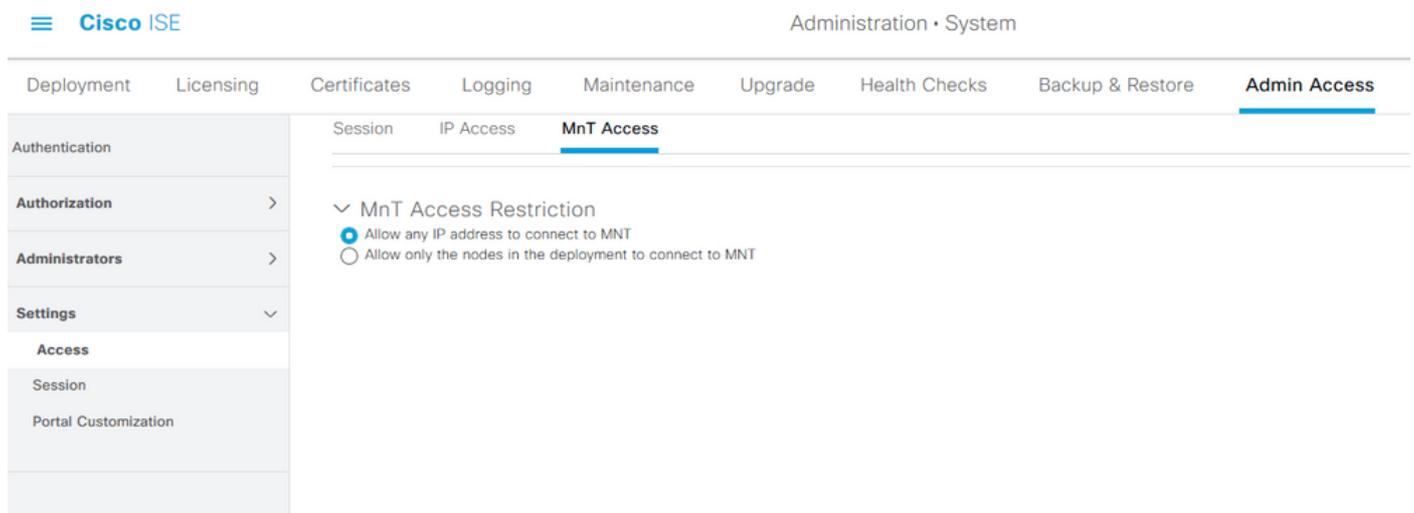
+ Add Edit Delete

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

Per configurare un elenco di nodi da cui gli amministratori possono accedere alla sezione MnT in Cisco ISE, selezionare **Amministrazione > Sistema > Accesso amministratore > Impostazioni > Accesso** e selezionare la scheda **Accesso MnT**.

Per consentire ai nodi o alle entità all'interno o all'esterno della distribuzione di inviare syslog a

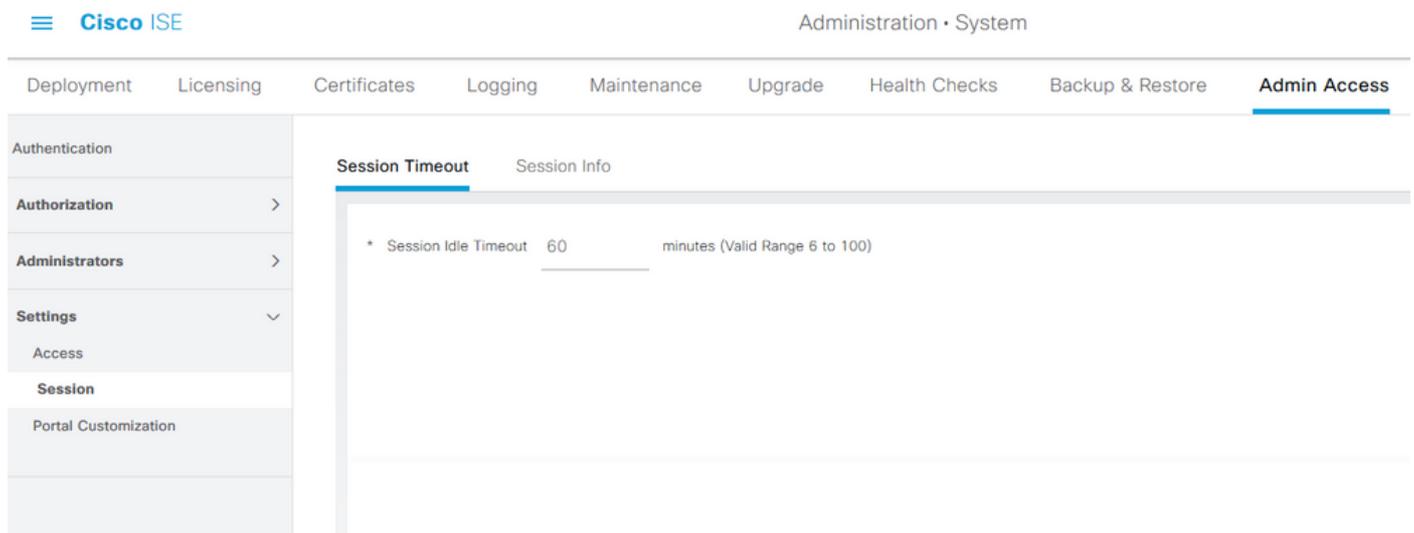
MnT, fare clic sul pulsante di opzione **Consenti a qualsiasi indirizzo IP di connettersi a MNT**. Per consentire solo ai nodi o alle entità della distribuzione di inviare syslog a MnT, fare clic sul pulsante di opzione **Consenti solo ai nodi della distribuzione di connettersi a MNT**.



The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Administration • System' and a menu with options: 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'. Under 'Settings', 'Access' is expanded to show 'Session' and 'Portal Customization'. The main content area is titled 'MnT Access' and contains 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'.

**Nota:** Per ISE 2.6 patch 2 e versioni successive, l'opzione *Use "ISE Messaging Service" for UDP Syslogs delivery to MnT* è attivata per impostazione predefinita e non consente syslog provenienti da altre entità esterne all'implementazione.

Per configurare un valore di timeout a causa dell'inattività di una sessione, selezionare **Amministrazione > Sistema > Accesso amministratore > Impostazioni > Sessione**. Impostare questo valore nella scheda **Timeout sessione**.



The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Administration • System' and a menu with options: 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'. Under 'Settings', 'Access' is expanded to show 'Session' and 'Portal Customization'. The main content area is titled 'Session Timeout' and shows a configuration field for 'Session Idle Timeout' set to '60 minutes (Valid Range 6 to 100)'.

Per visualizzare/invalidare le sessioni attive correnti, selezionare **Amministrazione > Accesso amministratore > Impostazioni > Sessione** e fare clic sulla scheda **Informazioni sessione**.

Cisco ISE Administration - System

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

Authentication  
 Authorization >  
 Administrators >  
 Settings v  
 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

## Configura accesso al portale di amministrazione con credenziali AD

### Partecipa ad ISE e AD

Per aggiungere ISE a un dominio esterno, selezionare **Amministrazione > Gestione delle identità > Origini identità esterne > Active Directory**. Immettere il nuovo nome del punto di join e il dominio di Active Directory. Immettere le credenziali dell'account AD che consente di aggiungere e modificare gli oggetti computer e fare clic su **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 ⓘ

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

## Seleziona gruppi di directory

Passare a **Amministrazione > Gestione delle identità > Origini identità esterne > Active Directory**. Fare clic sul nome del punto di join desiderato e passare alla scheda **Gruppi**. Fare clic su **Aggiungi > Seleziona gruppi dalla directory > Recupera gruppi**. Importare almeno un gruppo AD al quale appartiene l'amministratore, fare clic su **OK**, quindi su **Salva**.

Identity Sources

Connection

Edit +

Na

No data available

### Select Directory Groups

This dialog is used to select groups from the Directory.

Domain

Name Filter \*    SID Filter \*    Type Filter ALL

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	

## Abilita accesso amministrativo per AD

Per abilitare l'autenticazione basata su password di ISE con AD, selezionare **Amministrazione > Sistema > Accesso amministratore > Autenticazione**. Nella scheda **Metodo di autenticazione** selezionare l'opzione **Basato su password**. Selezionare **AD** dal menu a discesa **Origine identità** e fare clic su **Salva**.

The screenshot shows the Cisco ISE Administration console. The navigation menu includes: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, **Admin Access**, and Settings. Under 'Admin Access', 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.

## Configurazione del mapping tra il gruppo di amministratori ISE e il gruppo AD

In questo modo viene concessa l'autorizzazione per determinare le autorizzazioni RBAC (Role Based Access Control) per l'amministratore in base all'appartenenza ai gruppi in Active Directory. Per definire un gruppo Cisco ISE Admin e mapparlo a un gruppo AD, selezionare **Amministrazione > Sistema > Accesso amministratore > Amministratori > Gruppi amministrativi**. Fare clic su **Add** (Aggiungi) e immettere un nome per il nuovo gruppo Admin. Nel campo Tipo selezionare la casella di controllo **Esterno**. Dal menu a discesa **Gruppi esterni**, selezionare il gruppo AD a cui deve essere mappato questo gruppo amministrativo (come definito nella sezione Seleziona gruppi di directory sopra). **Inviare** le modifiche.

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

<input type="checkbox"/>	Status	Email	Username	First Name	Last Name
No data available					

## Impostare le autorizzazioni RBAC per il gruppo Admin

Per assegnare le autorizzazioni RBAC al gruppo di amministratori creato nella sezione precedente, selezionare **Amministrazione > Sistema > Accesso amministratore > Autorizzazione > Criteri RBAC**. Dal menu a discesa **Azioni** a destra, selezionare **Inserisci nuovo criterio**. Creare una nuova regola, eseguirne il mapping con il gruppo Amministratori definito nella sezione precedente e assegnarle i dati e le autorizzazioni di accesso ai menu desiderati, quindi fare clic su **Salva**.

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 criteria 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 +

## Accesso a ISE con credenziali AD e verifica

Uscire dalla GUI amministrativa. Selezionare il nome del punto di join dal menu a discesa **Origine identità**. Immettere il nome utente e la password del database di Active Directory ed eseguire l'accesso.



# Identity Services Engine

Intuitive network security

Username  
TestUser

Password  
●●●●●●●●

Identity Source  
AD

Login

Per verificare che la configurazione funzioni correttamente, verificare il nome utente autenticato usando l'icona **Settings** nell'angolo in alto a destra dell'interfaccia grafica di ISE. Passare a **Informazioni server** e verificare il nome utente.

## 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

## Configura accesso al portale di amministrazione con LDAP

### Unisci ISE a LDAP

Passare a **Amministrazione > Gestione delle identità > Origini identità esterne > Active Directory > LDAP**. Nella scheda **Generale**, immettere un nome per il server LDAP e scegliere lo schema come **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  ▼

Quindi, per configurare il tipo di connessione, passare alla scheda **Connessione**. Qui, impostare il nome host/IP del server LDAP principale insieme alla porta 389(LDAP)/636 (LDAP-Secure). Immettere il percorso del DN (nome distinto) dell'amministratore con la password Admin del server LDAP.

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

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

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

Passare quindi alla scheda **Organizzazione directory** e fare clic su **Contesti di denominazione** per scegliere il gruppo di organizzazioni corretto dell'utente in base alla gerarchia degli utenti memorizzati nel server LDAP.

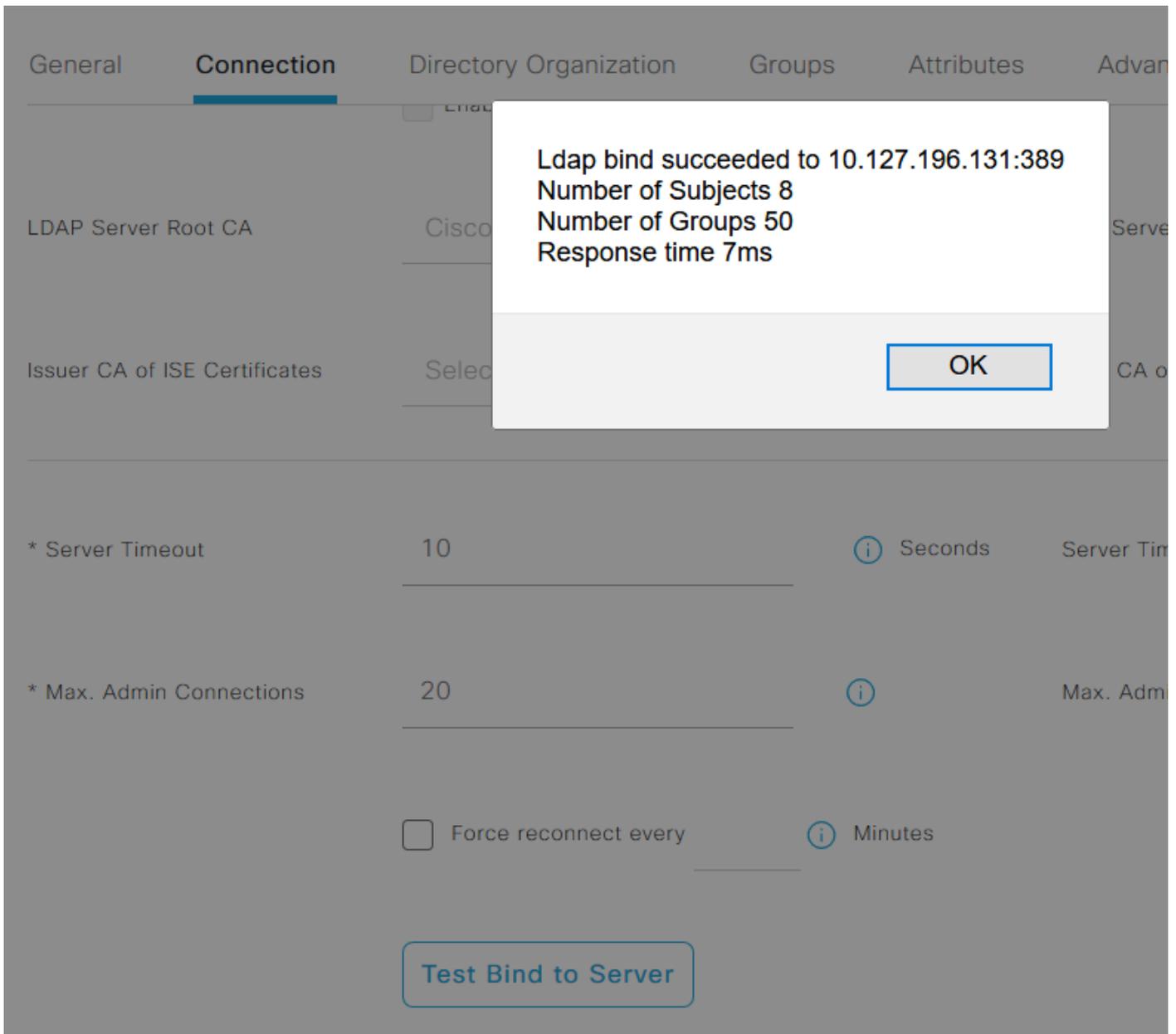
## External Identity Sources

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

## LDAP Identity Source

General Connection **Directory Organization** Groups Attributes Advanced Settings\* Subject Search Base DC=rinsantr,DC=lab [Naming Contexts...](#) ⓘ\* Group Search Base DC=rinsantr,DC=lab [Naming Contexts...](#) ⓘSearch for MAC Address in Format  ▼ Strip start of subject name up to the last occurrence of the separator  Strip end of subject name from the first occurrence of the separator 

Fare clic su **Test Bind to Server** nella scheda **Connection** per verificare la raggiungibilità del server LDAP da ISE.



Passare alla scheda **Gruppi** e fare clic su **Aggiungi > Seleziona gruppi da directory > Recupera gruppi**. Importare almeno un gruppo a cui appartiene l'amministratore, fare clic su **OK**, quindi su **Salva**.

## 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

## Abilita accesso amministrativo per utenti LDAP

Per abilitare l'autenticazione basata su password di ISE utilizzando LDAP, selezionare **Amministrazione > Sistema > Accesso amministratore > Autenticazione**. Nella scheda **Metodo di autenticazione** selezionare l'opzione **Basato su password**. Selezionare **LDAP** dal menu a discesa **Origine identità** e fare clic su **Salva**.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Cisco ISE' and 'Administration - System'. The main navigation menu has 'Admin Access' selected. On the left, a sidebar menu shows 'Authentication', 'Authorization', 'Administrators', and 'Settings'. The main content area is titled 'Authentication Method' and includes sub-sections for 'Password Policy', 'Account Disable Policy', and 'Lock/Suspend Settings'. Under 'Authentication Type', the 'Password Based' radio button is selected. Below it, the 'Identity Source' dropdown is set to 'LDAP:LDAPExample'. The 'Client Certificate Based' radio button is unselected. A blue 'Save' button is located at the bottom right of the configuration area.

## Mappa il gruppo di amministratori ISE al gruppo LDAP

Questo consente all'utente configurato di ottenere l'accesso come amministratore in base all'autorizzazione dei criteri RBAC, che a sua volta si basa sull'appartenenza dell'utente al gruppo LDAP. Per definire un Cisco ISE Admin Group e mapparlo a un gruppo LDAP, selezionare **Amministrazione > Sistema > Accesso amministratore > Amministratori > Gruppi amministrativi**. Fare clic su **Add** (Aggiungi) e immettere un nome per il nuovo gruppo Admin. Nel campo Tipo selezionare la casella di controllo **Esterno**. Dal menu a discesa **Gruppi esterni** (External Groups), selezionate il gruppo LDAP a cui il gruppo amministrativo deve essere mappato (come recuperato e definito in precedenza). **Inviare** le modifiche.

The screenshot shows the 'New Admin Group' configuration page in Cisco ISE. The breadcrumb navigation is 'Admin Groups > New Admin Group'. The main heading is 'Admin Group'. The 'Name' field contains 'ISE LDAP Admin Group'. The 'Description' field is empty. The 'Type' is set to 'External' with a checked checkbox. The 'External Identity Source' is 'LDAPExample'. Under the 'External Groups' section, a dropdown menu shows 'CN=Test Group,CN=Users,DC=' selected. A blue 'Save' button is visible at the bottom right.

## Impostare le autorizzazioni RBAC per il gruppo Admin

Per assegnare le autorizzazioni RBAC al gruppo di amministratori creato nella sezione precedente, selezionare **Amministrazione > Sistema > Accesso amministratore > Autorizzazione > Criteri RBAC**. Dal menu a discesa **Azioni** a destra, selezionare **Inserisci nuovo criterio**. Creare una nuova regola, eseguirne il mapping con il gruppo Amministratori definito nella sezione precedente

e assegnarle i dati e le autorizzazioni di accesso ai menu desiderati, quindi fare clic su **Salva**.

Authentication

Authorization

Permissions

RBAC Policy

Administrators

Settings

Administration • System

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

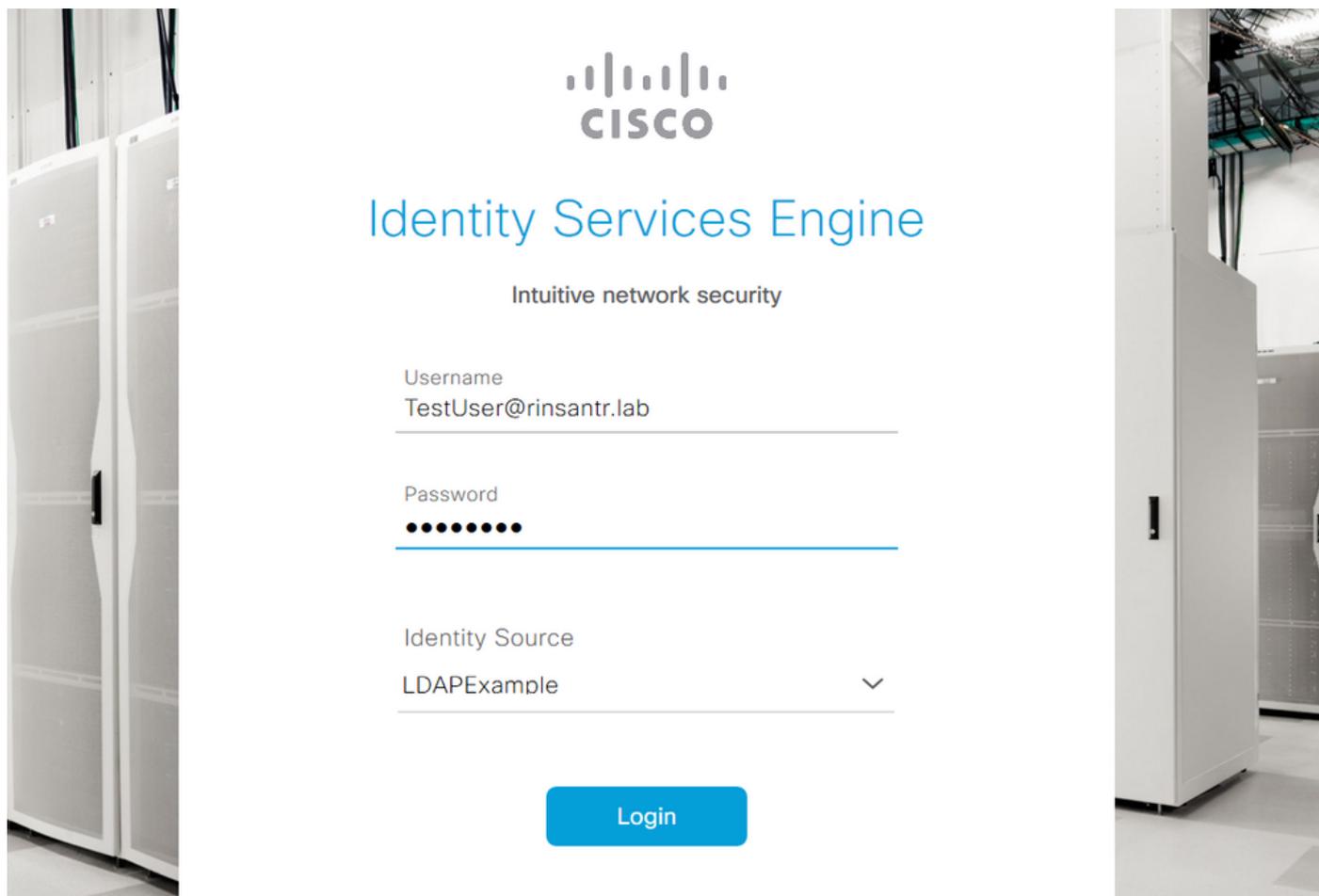
Create Role Based Access Control policies by configuring rules based on Admin groups, Menu Access permissions (menu items), Data Access permissions (identity group data elements). Menu/Data Access permissions are not allowed on a single policy. You can copy the default policies shown below, then modify 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
Maintenance Admin Policy	Maintenance Admin	Maintenance Admin Menu Access

## Accesso a ISE con credenziali LDAP e verifica

Uscire dalla GUI amministrativa. Selezionare il nome LDAP dal menu a discesa **Origine identità**. Immettere il nome utente e la password dal database LDAP ed effettuare l'accesso.



Per verificare che la configurazione funzioni correttamente, verificare il nome utente autenticato usando l'icona **Settings** (Impostazioni) nell'angolo in alto a destra dell'interfaccia grafica di ISE.

Passare a **Informazioni server** e verificare il nome utente.

Dashboard

Guests

Acti

Beha

NDPC

Pr

Failure Re

## 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