Comprendere le policy RBAC e di accesso degli amministratori su ISE

Sommario

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:

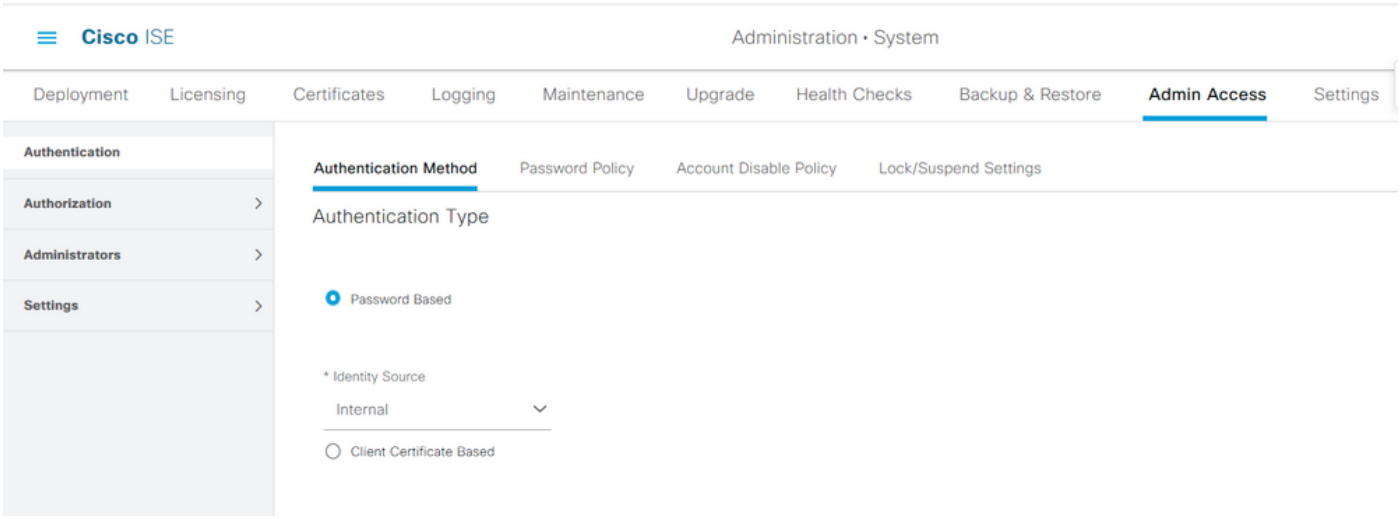
- Identity Services Engine 3.0
- Windows Server 2016

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

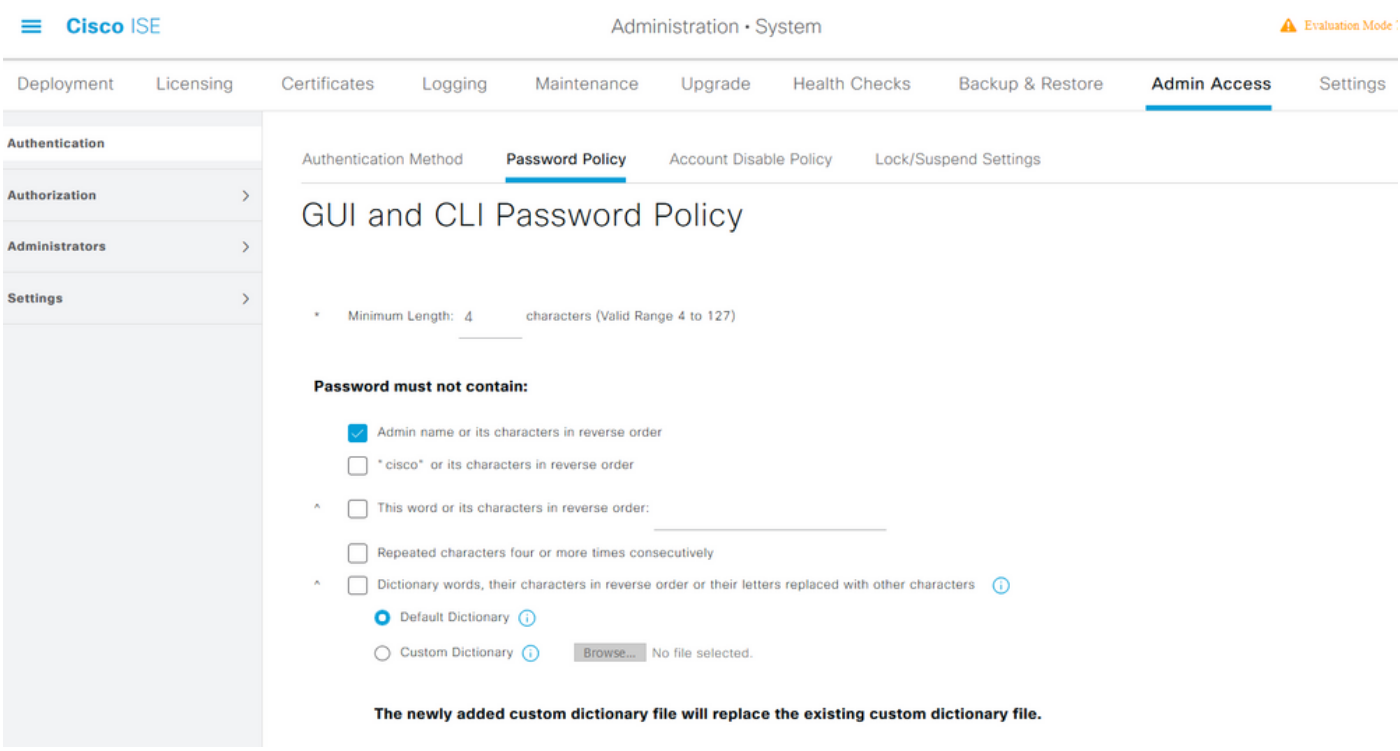
Impostazioni autenticazione

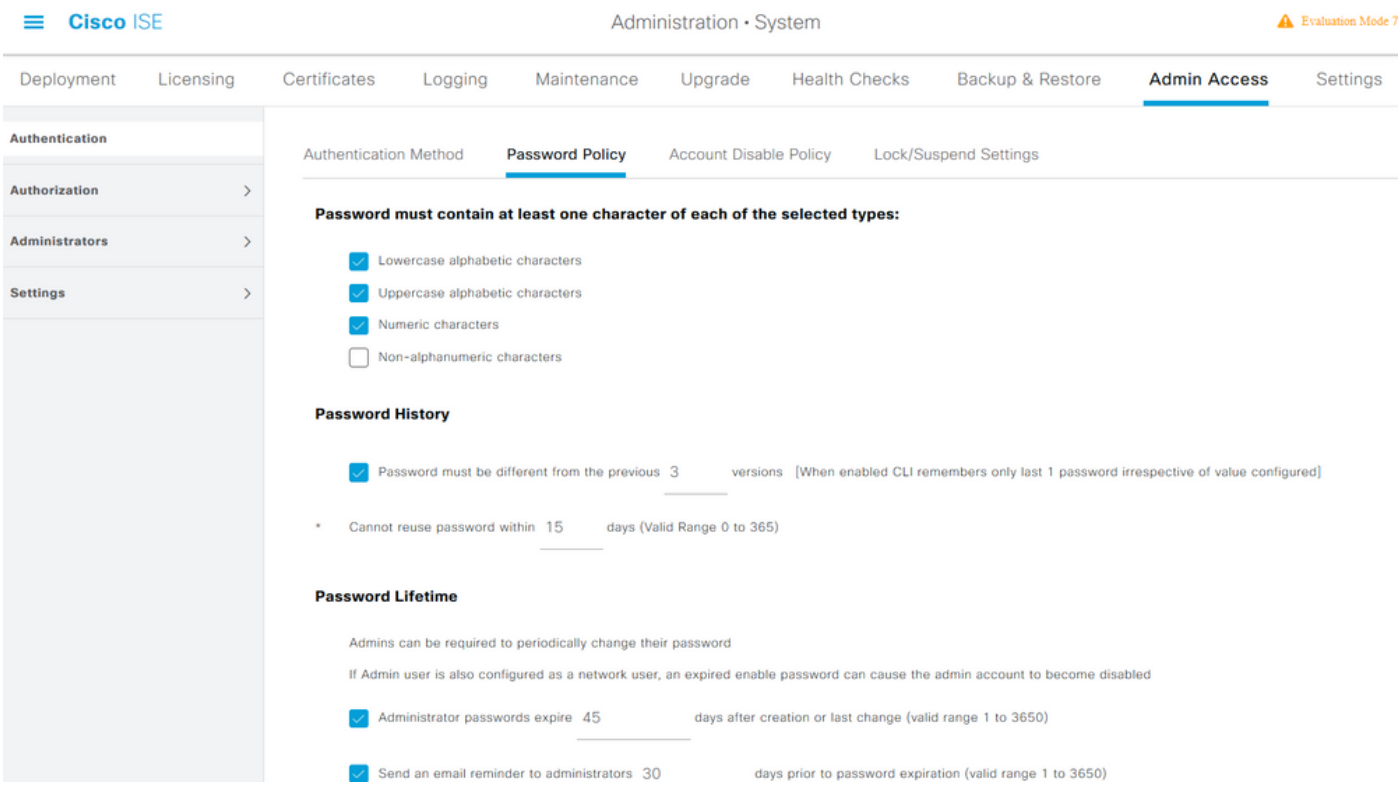
Gli utenti amministratori devono autenticarsi per accedere a qualsiasi informazione su ISE. L'identità degli utenti amministratori può essere verificata usando ISE Internal Identity Store o External Identity Store. L'autenticità può essere verificata mediante una password o un certificato. Per configurare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



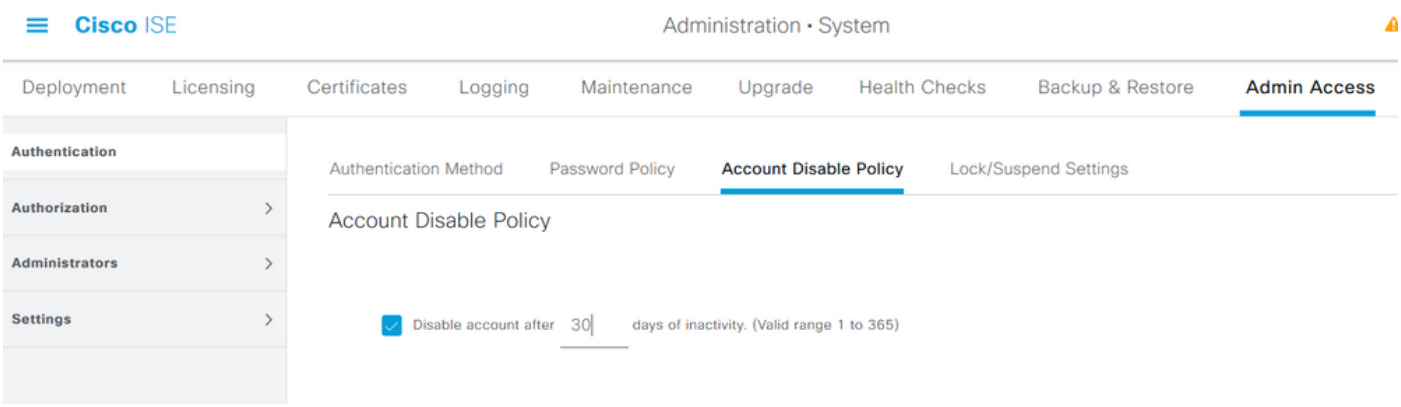
> **Nota:** L'autenticazione basata su password è abilitata per impostazione predefinita. Se questa opzione viene modificata in Autenticazione basata su certificati client, il server applicazioni verrà riavviato in tutti i nodi di distribuzione.

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**.

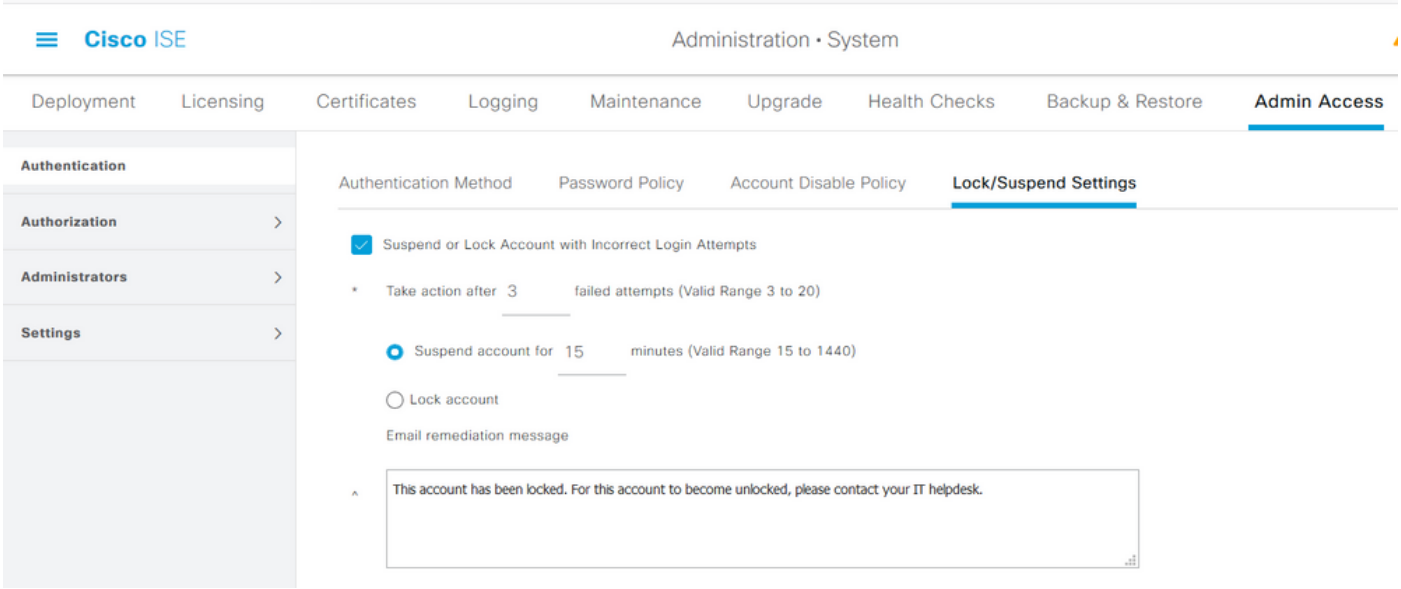




ISE prevede la disabilitazione di un utente amministratore inattivo. Per configurare questa impostazione, selezionare **Amministrazione > Sistema > Accesso amministratore > Autenticazione** e passare alla scheda **Criteri di disabilitazione account**.



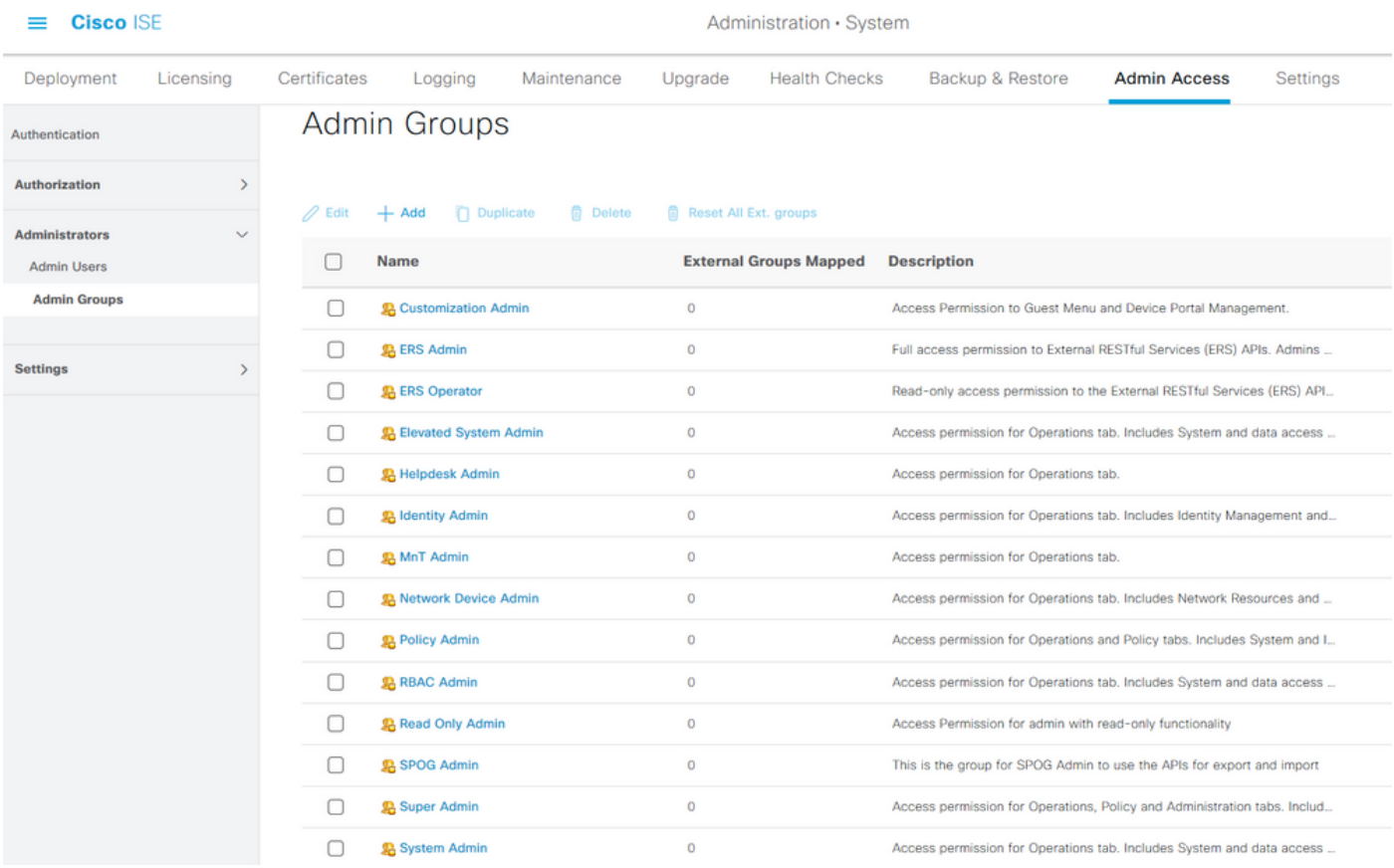
ISE offre anche la possibilità di bloccare o sospendere un account utente amministratore in base al numero di tentativi di accesso non riusciti. Per configurare questa impostazione, selezionare **Amministrazione > Sistema > Accesso amministratore > Autenticazione** e selezionare la scheda **Blocca/Sospendi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



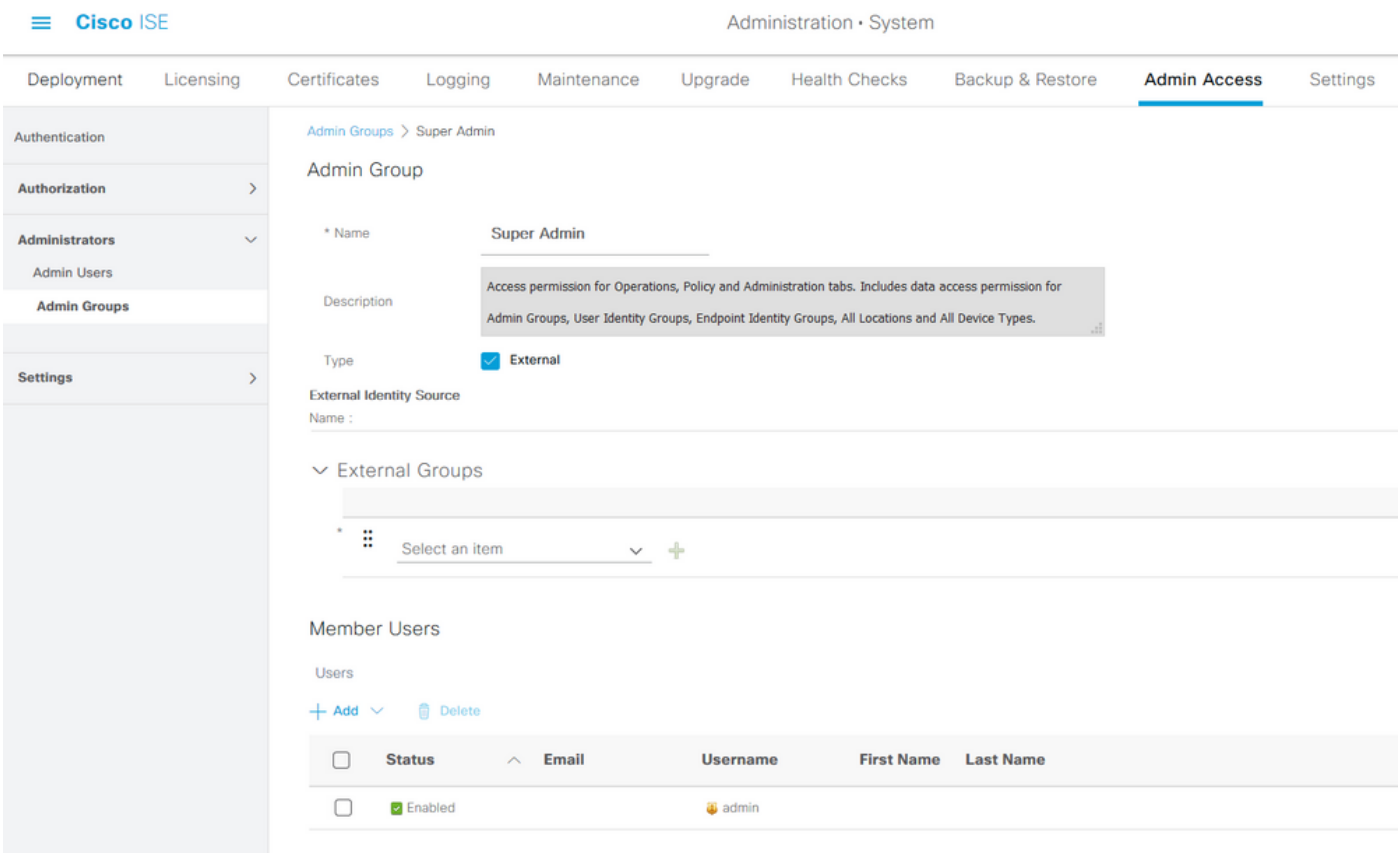
Per gestire l'accesso amministrativo, è necessario che i gruppi amministrativi, gli utenti e varie regole/policy controllino e gestiscano i propri privilegi.

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.

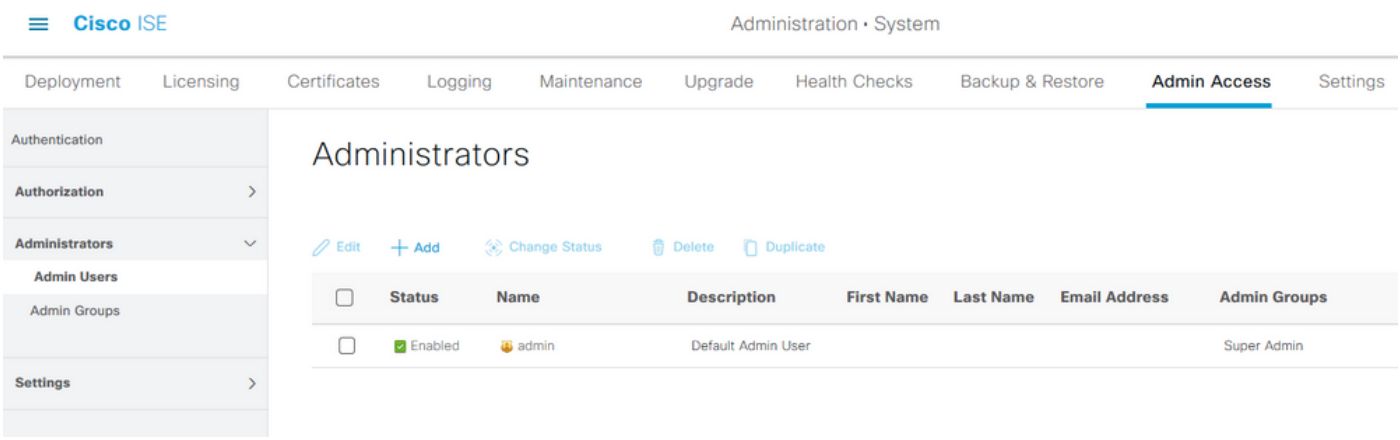


Una volta creato un gruppo, selezionarlo e fare clic su Modifica per aggiungere utenti amministratori al gruppo. È disponibile un'opzione per mappare i gruppi di identità esterni ai gruppi di amministratori su ISE in modo che un utente di External Admin ottenga le autorizzazioni necessarie. Per configurare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

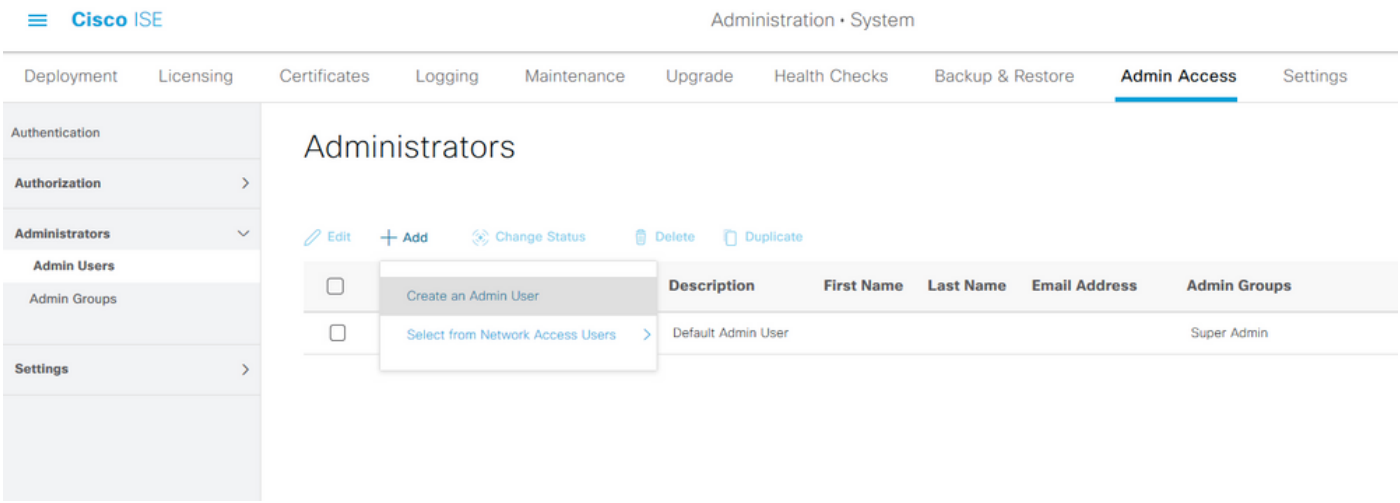


Configura utenti amministratori

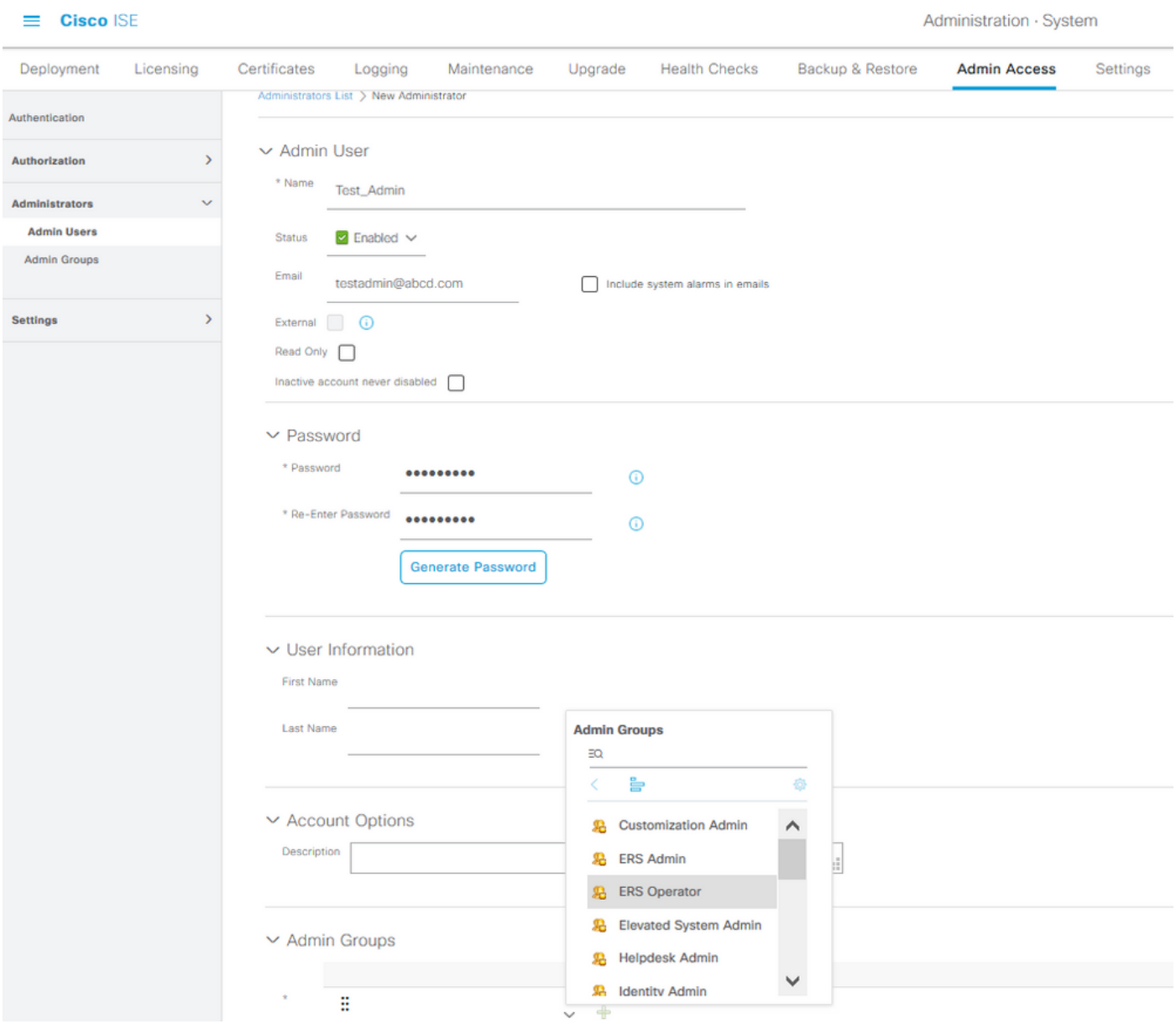
Per configurare gli utenti amministratori, selezionare **Amministrazione > Sistema > Accesso amministratore > Amministratori > Utenti amministratori**.



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.



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.



Configura autorizzazioni

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

1. Accesso al menu
2. Accesso ai dati

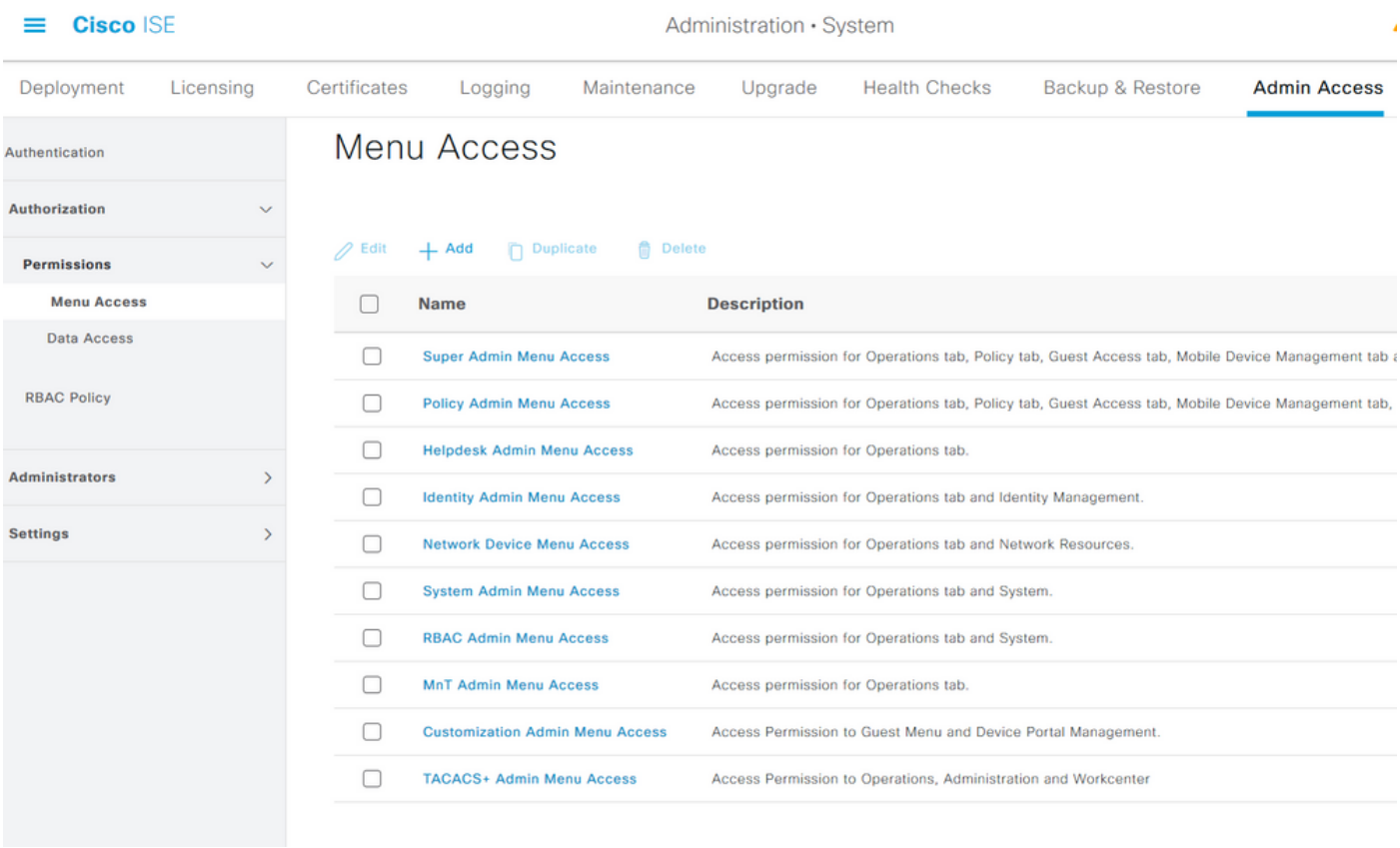
Menu Access controlla la visibilità di navigazione su ISE. È possibile configurare due opzioni per ogni scheda, Mostra o Nascondi. È possibile configurare una regola di accesso ai menu per visualizzare o nascondere le schede selezionate.

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.

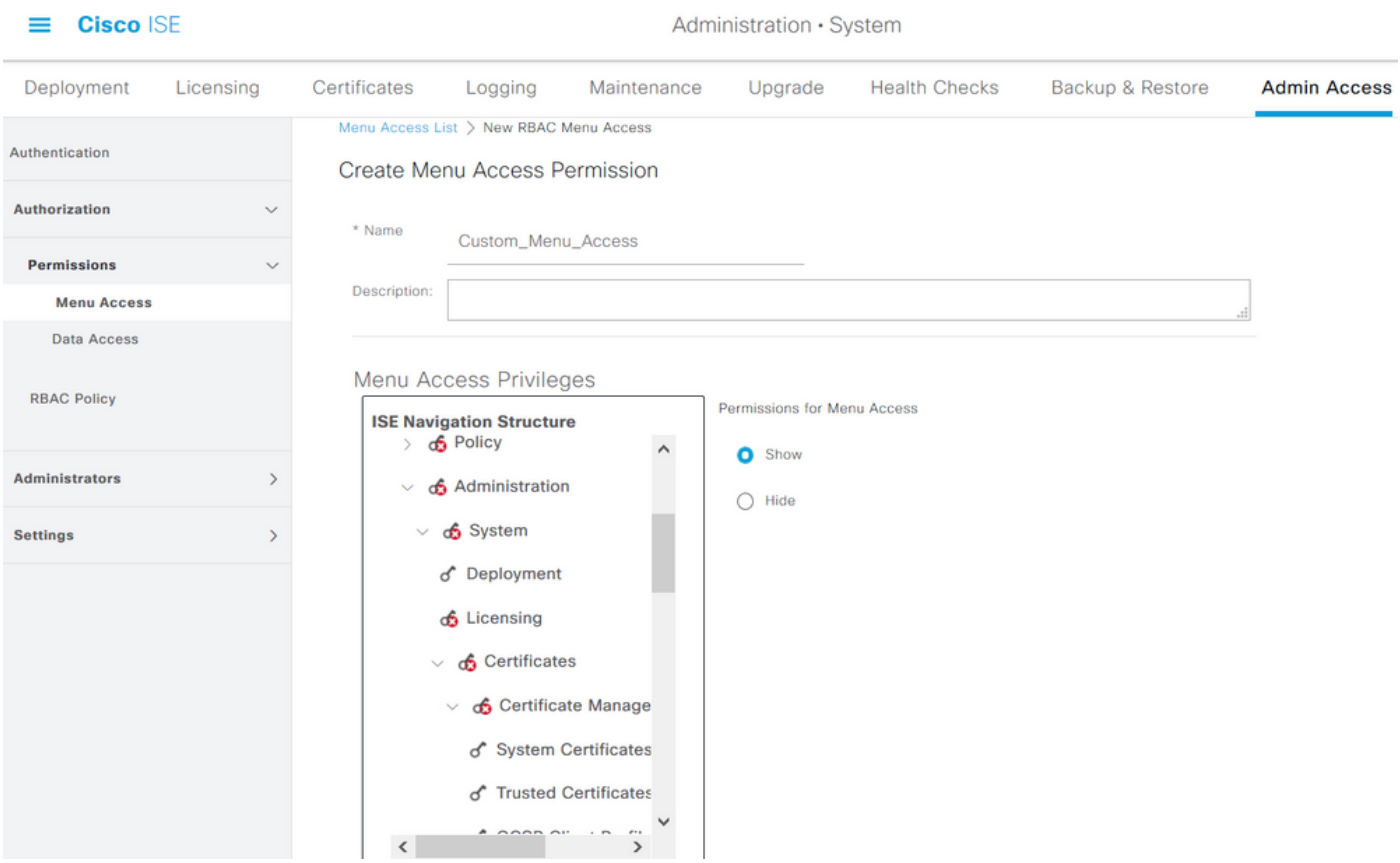
Ènecessario creare i criteri di accesso ai menu e ai dati prima di applicarli a qualsiasi gruppo amministrativo. Per impostazione predefinita, sono disponibili alcuni criteri predefiniti che possono

tuttavia essere personalizzati o creati.

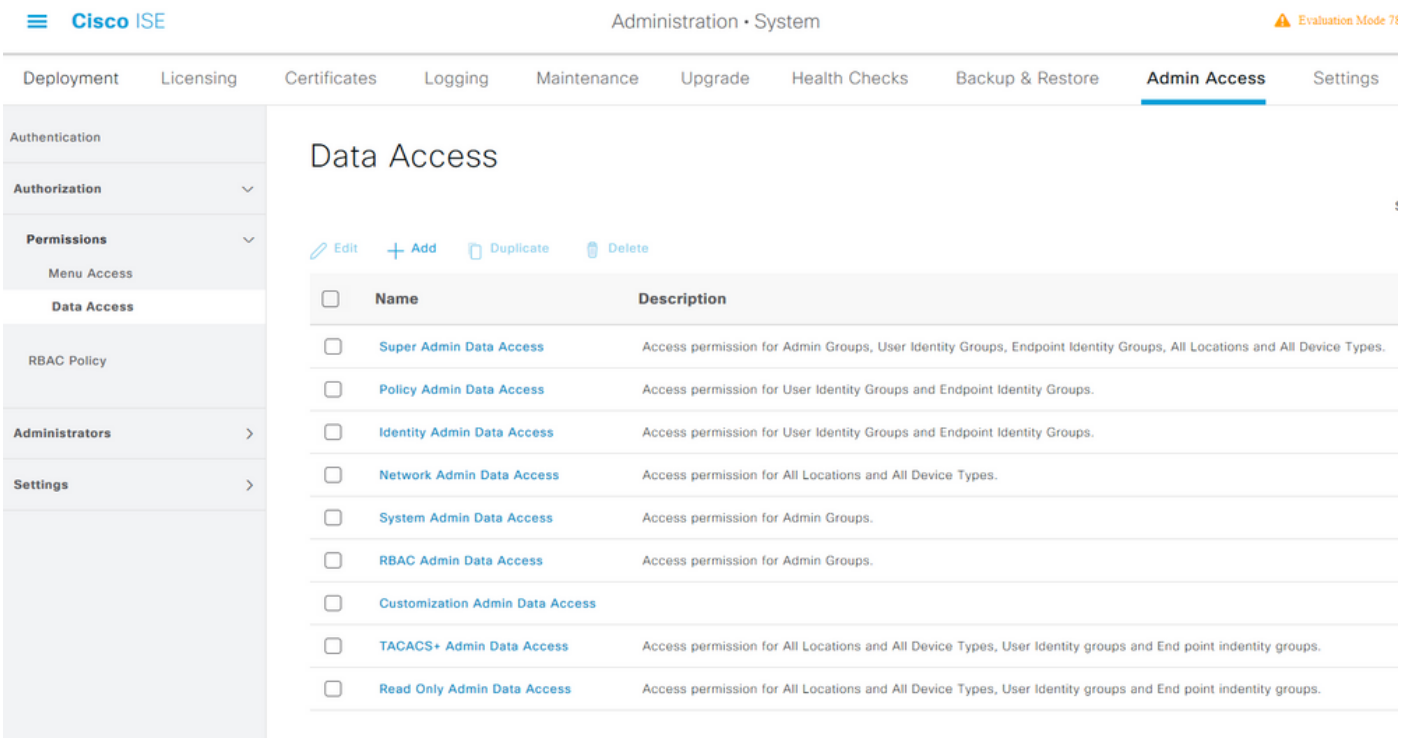
Per configurare un criterio di accesso ai menu, selezionare **Amministrazione > Sistema > Accesso amministratore > Autorizzazione > Autorizzazioni > Accesso menu**.



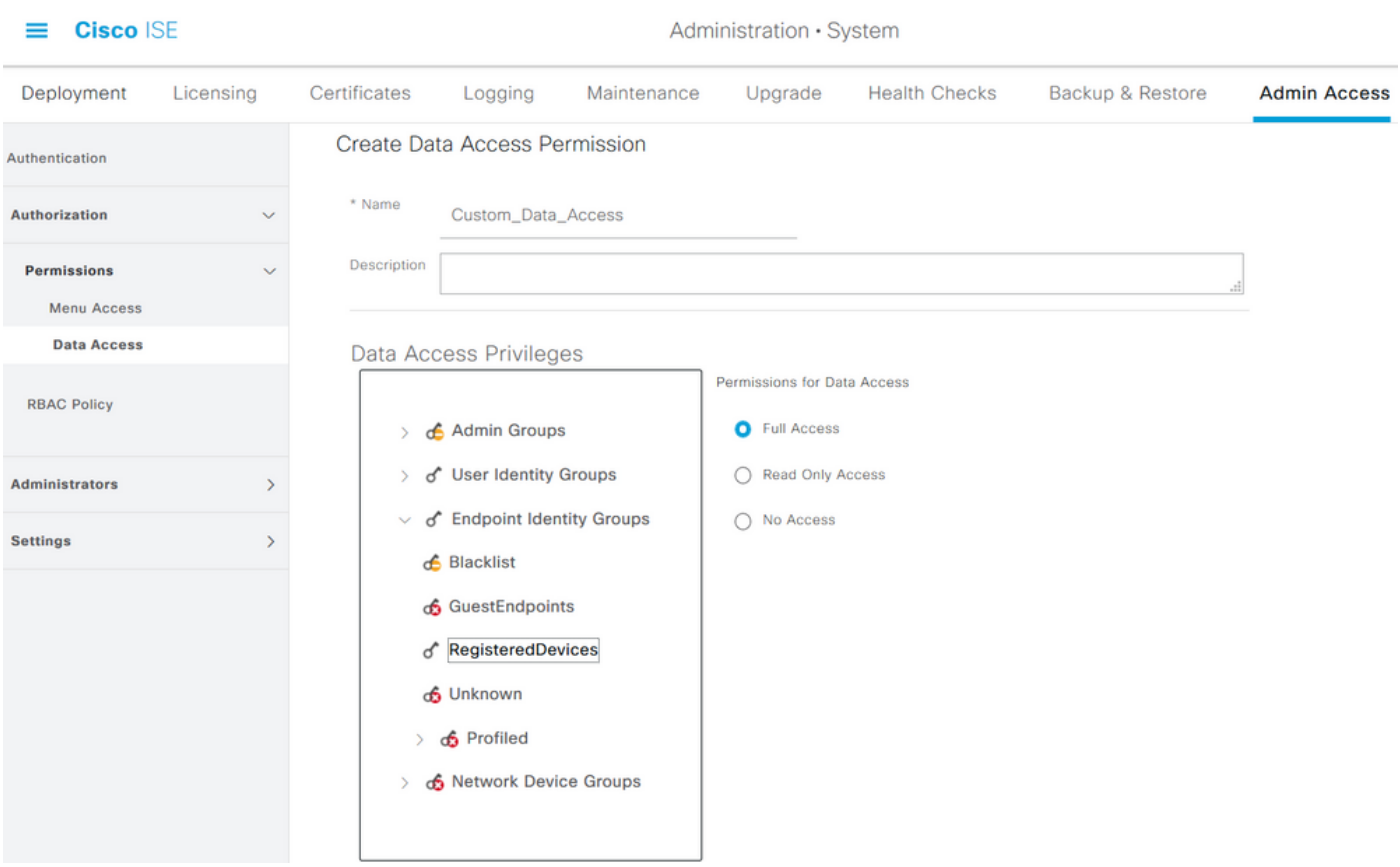
Fare clic su **Add**. Ogni opzione di navigazione in ISE può essere configurata per essere mostrata/nascosta in una policy.



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



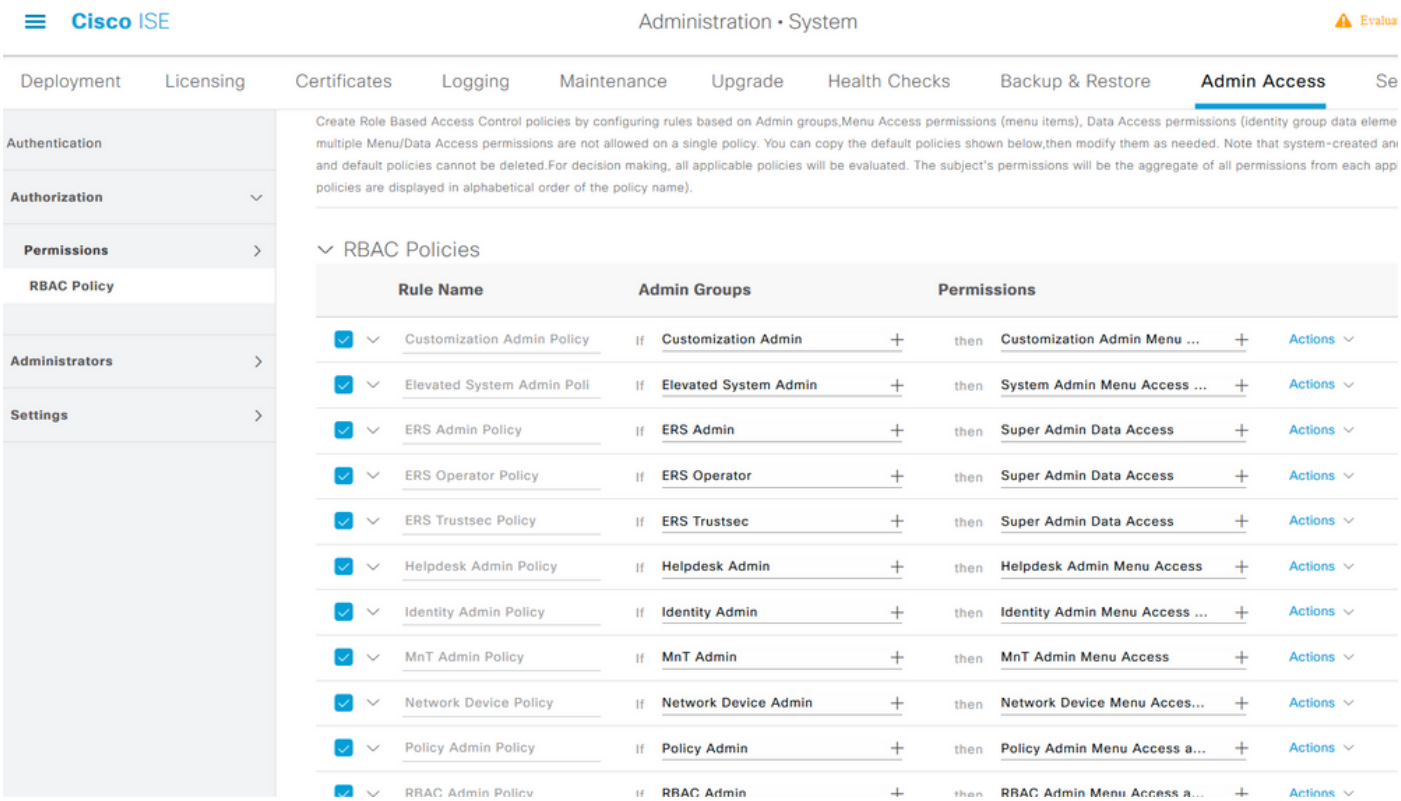
Fare clic su **Add** (Aggiungi) per creare un nuovo criterio e configurare le autorizzazioni di accesso ad Amministrazione/Identità utente/Identità endpoint/Gruppi di rete.



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**.



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

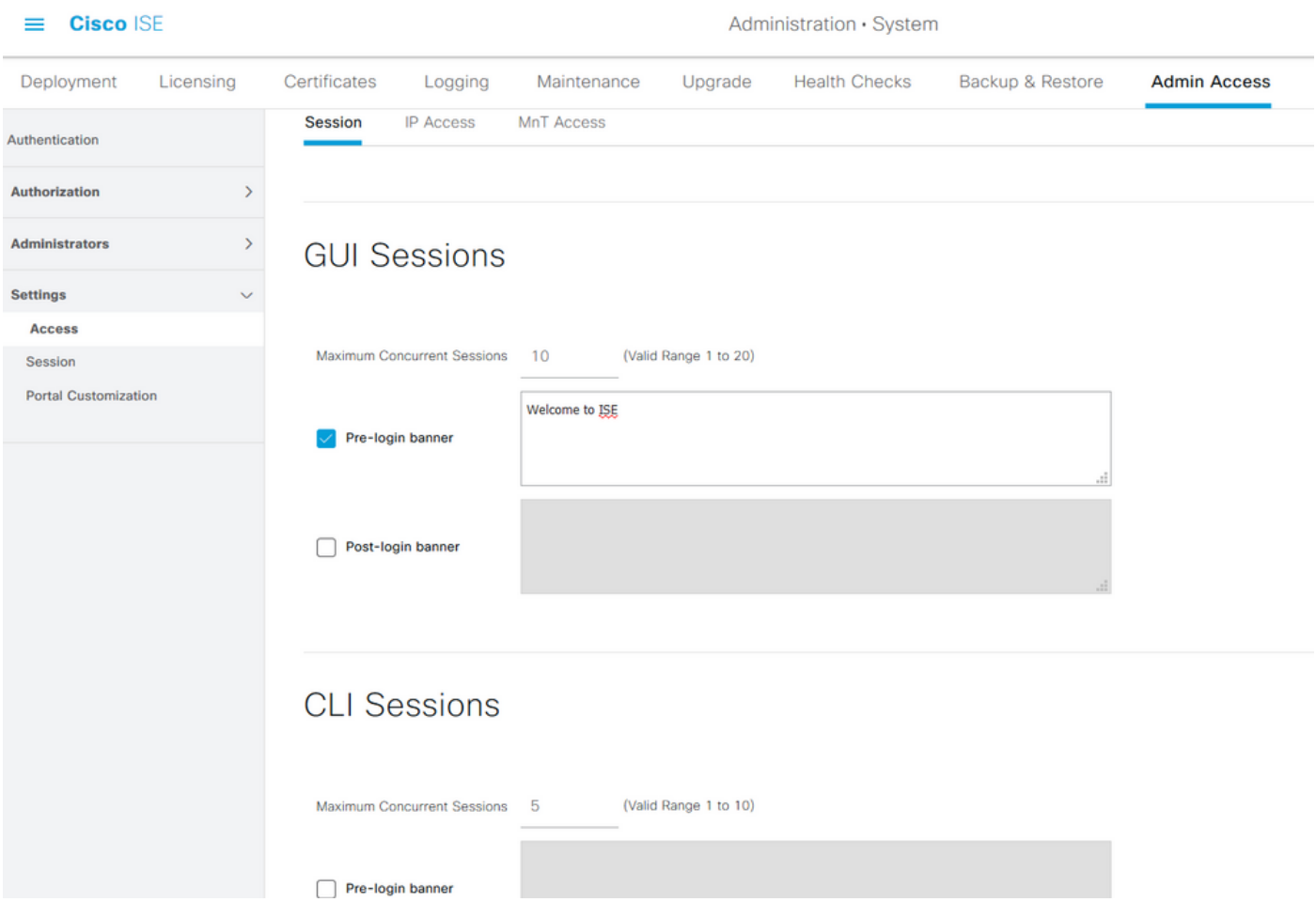
> **Nota:** Impossibile aggiornare i criteri predefiniti e creati dal sistema e non è possibile eliminare i criteri predefiniti.

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

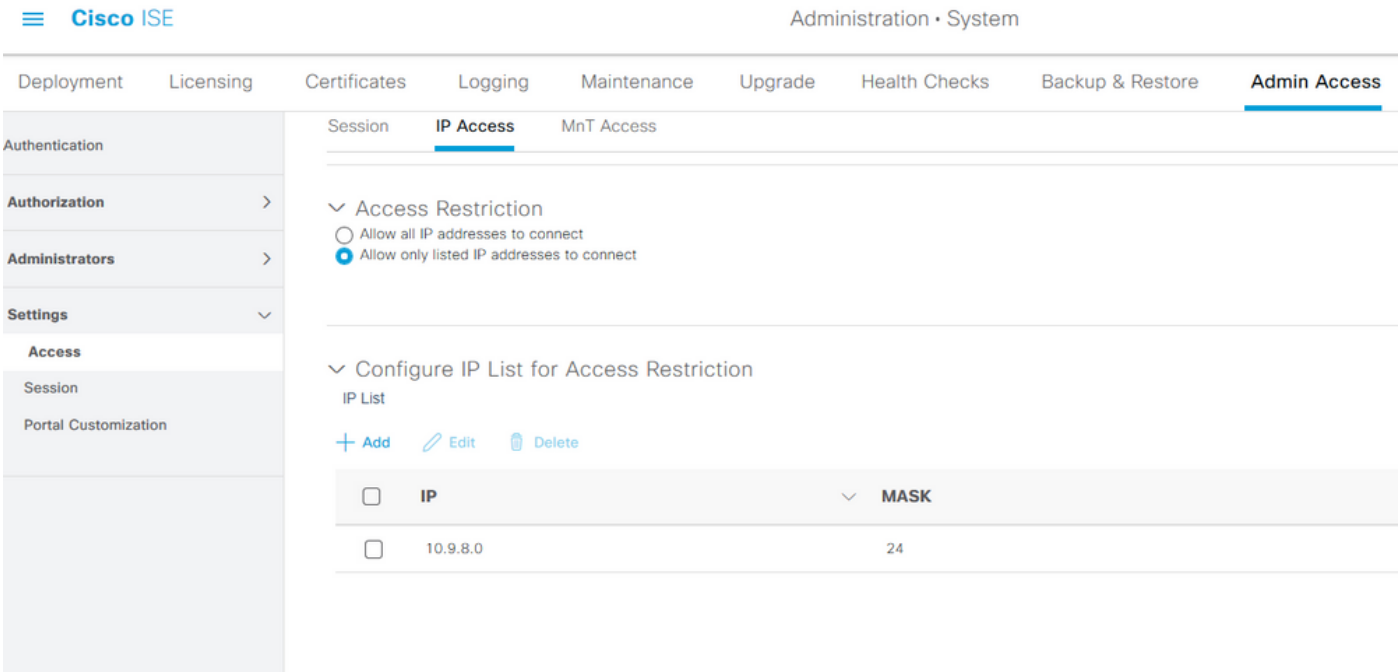
Configura impostazioni per accesso amministratore

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**.



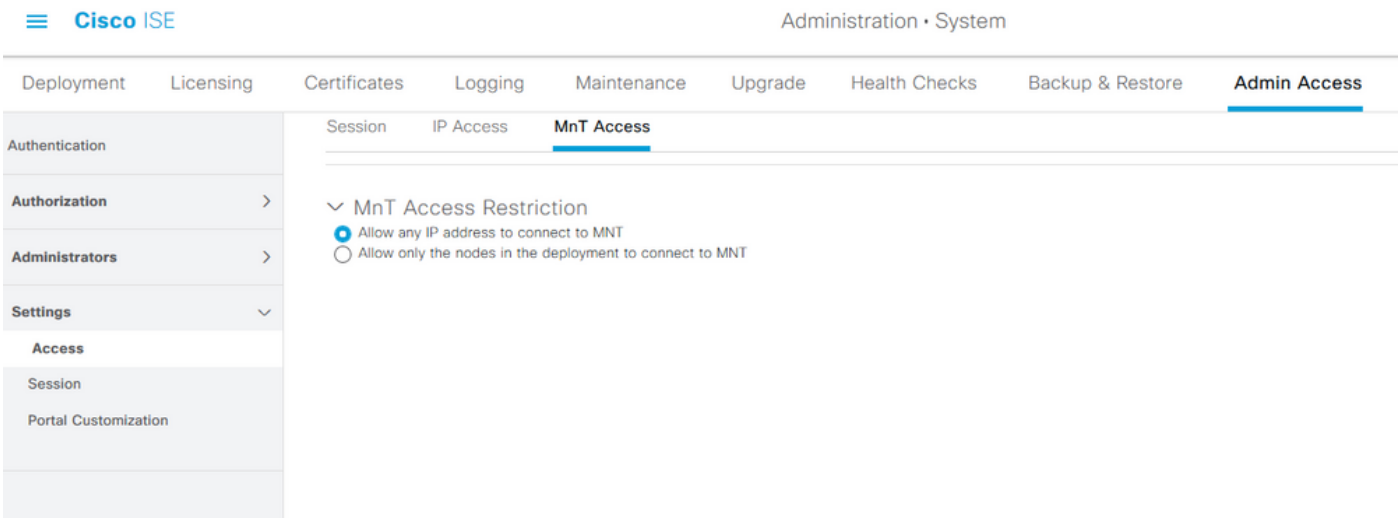
Per configurare la lista di indirizzi IP da cui è possibile accedere alla GUI e alla CLI, selezionare **Amministrazione > Sistema > Accesso amministratore > Impostazioni > Accesso** e selezionare la scheda **Accesso IP**.



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**.

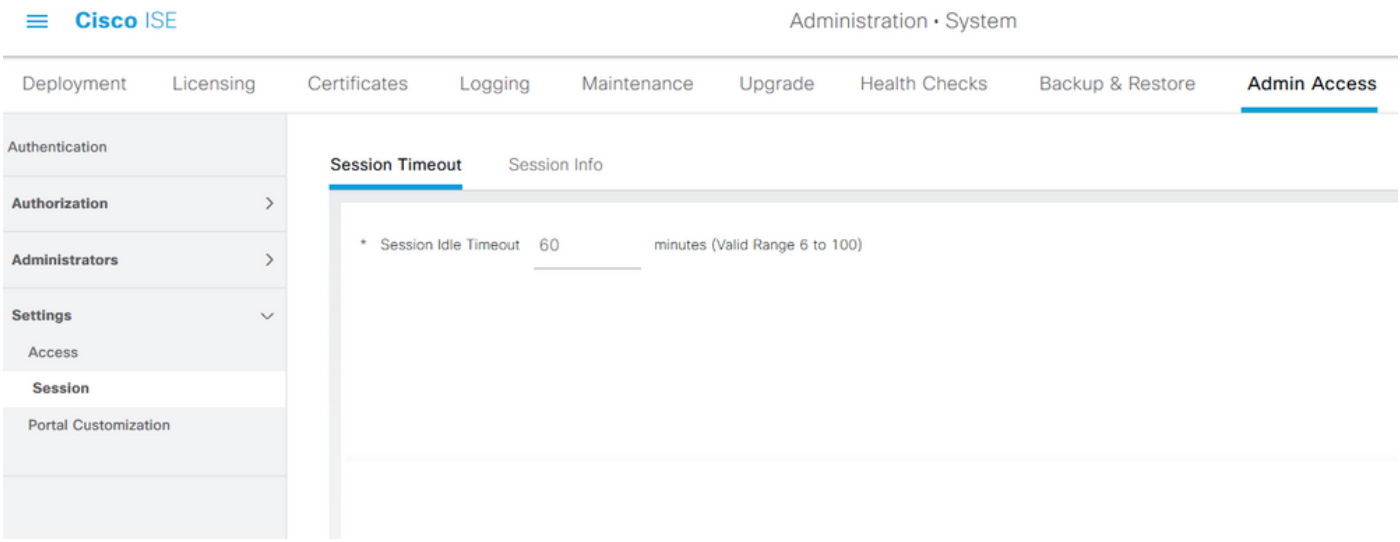
Per consentire ai nodi o alle entità all'interno o all'esterno della distribuzione di inviare syslog a

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**.

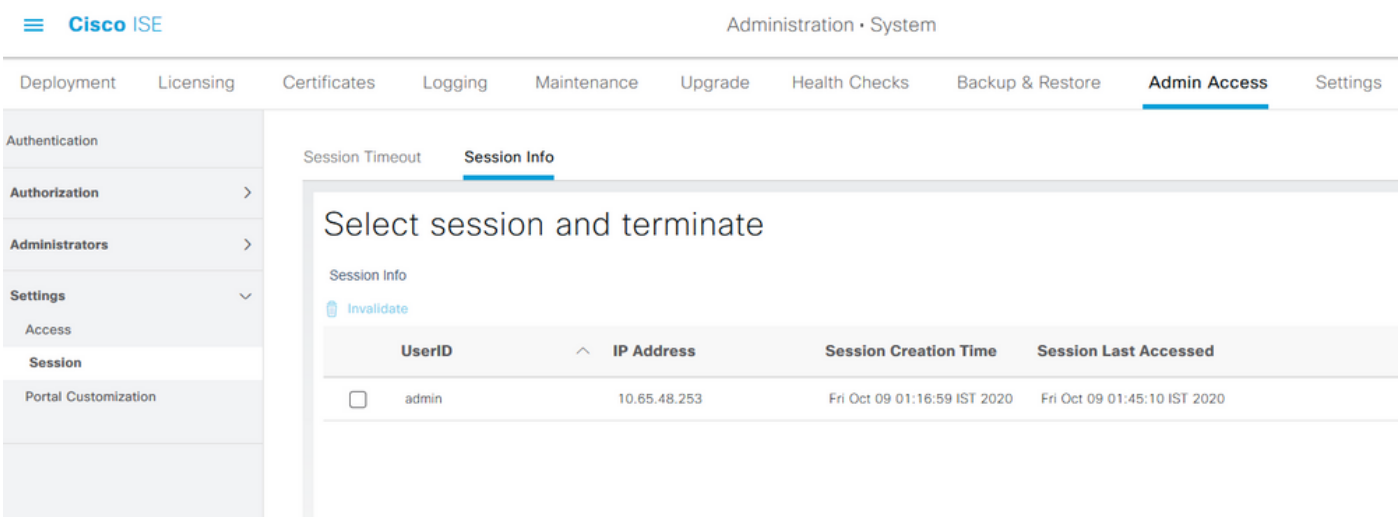


> **Nota:** Per ISE 2.6 patch 2 e versioni successive, l'opzione *Use "ISE Messaging Service" for UDP Syslogs delivery to MnT* è attivata per impostazione predefinita e non consente syslog provenienti da altre entità esterne all'implementazione.

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**.



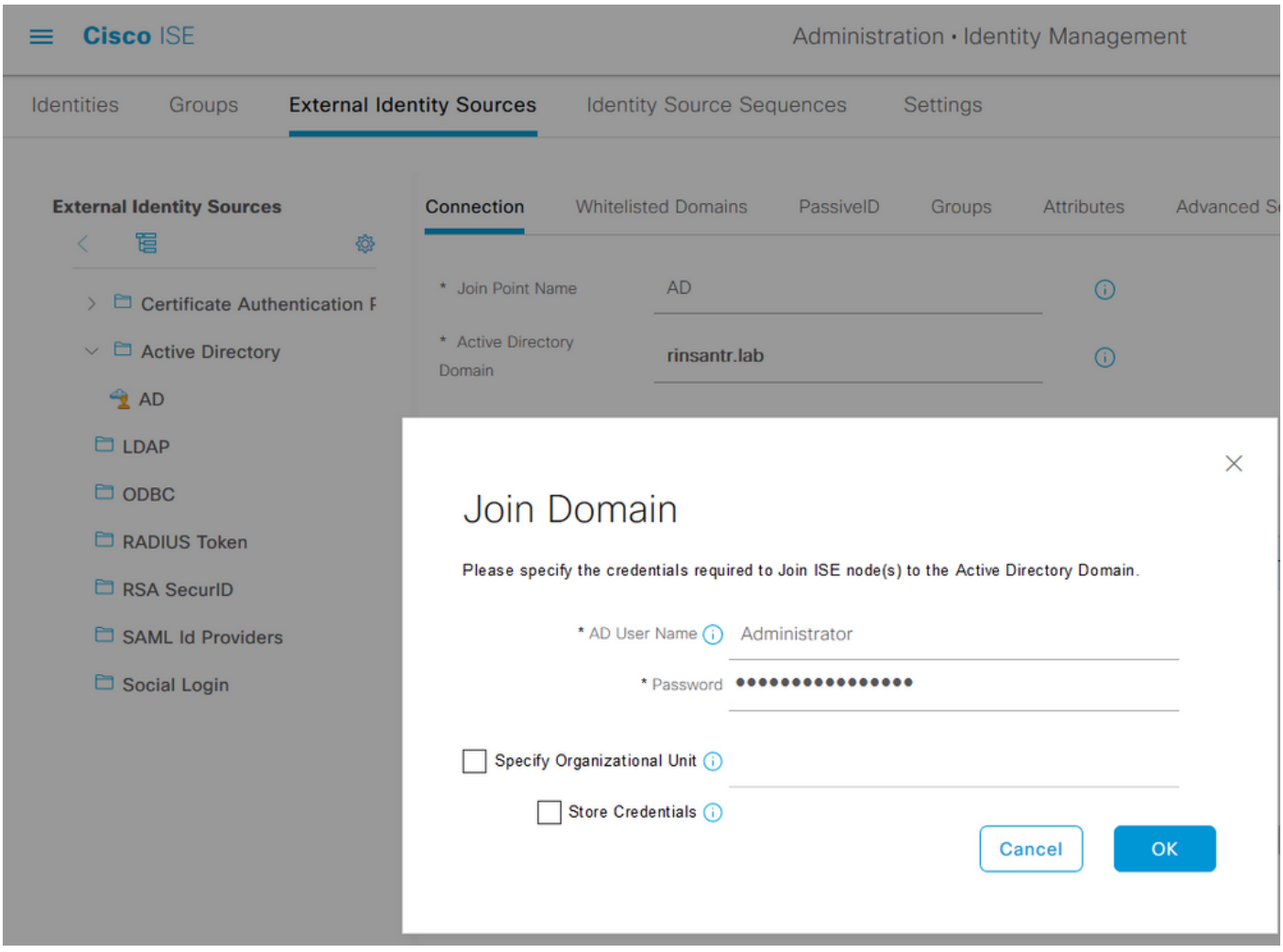
Per visualizzare/invalidare le sessioni attive correnti, selezionare **Amministrazione > Accesso amministratore > Impostazioni > Sessione** e fare clic sulla scheda **Informazioni sessione**.

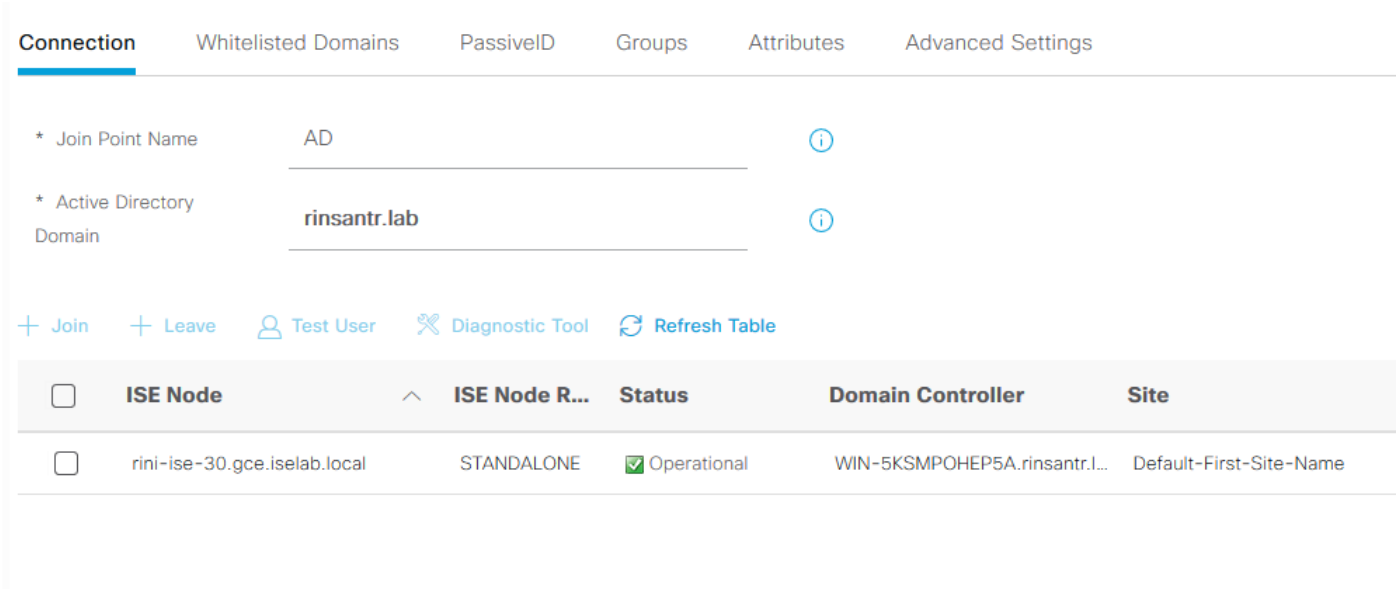


Configura accesso al portale di amministrazione con credenziali AD

Partecipa ad ISE e AD

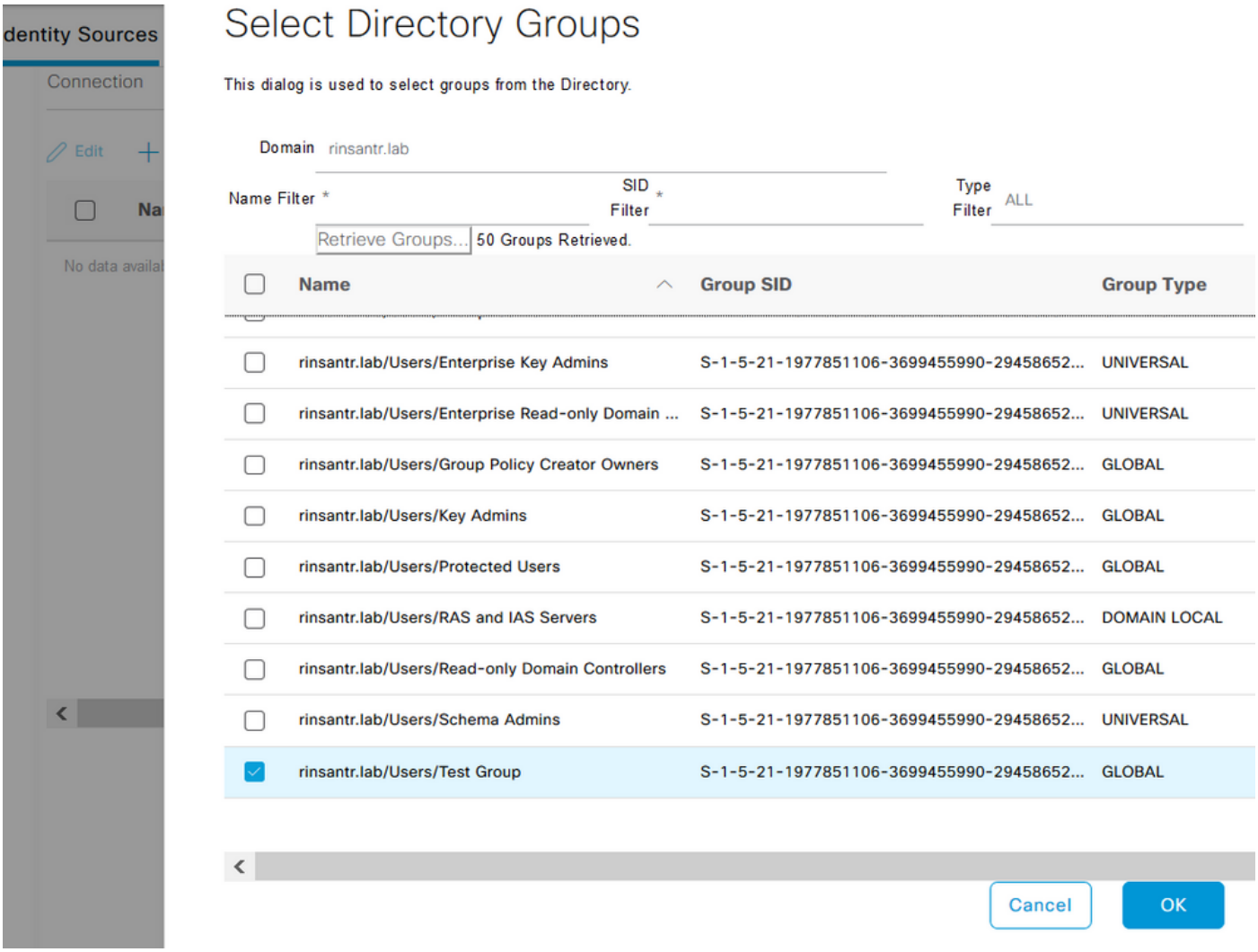
Per aggiungere ISE a un dominio esterno, selezionare **Amministrazione > Gestione delle identità > Origini identità esterne > Active Directory**. Immettere il nuovo nome del punto di join e il dominio di Active Directory. Immettere le credenziali dell'account AD che consente di aggiungere e modificare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

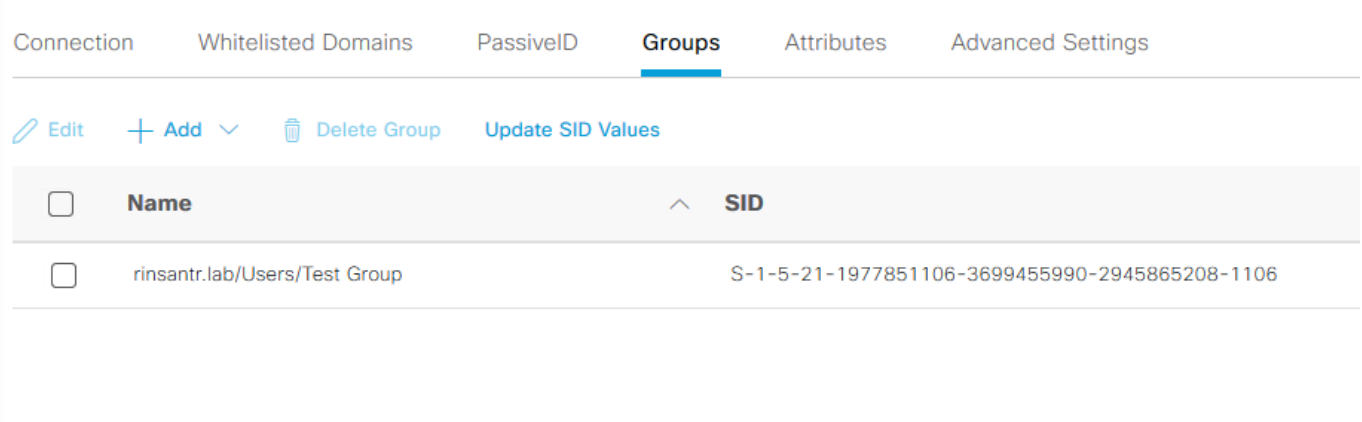




Seleziona gruppi di directory

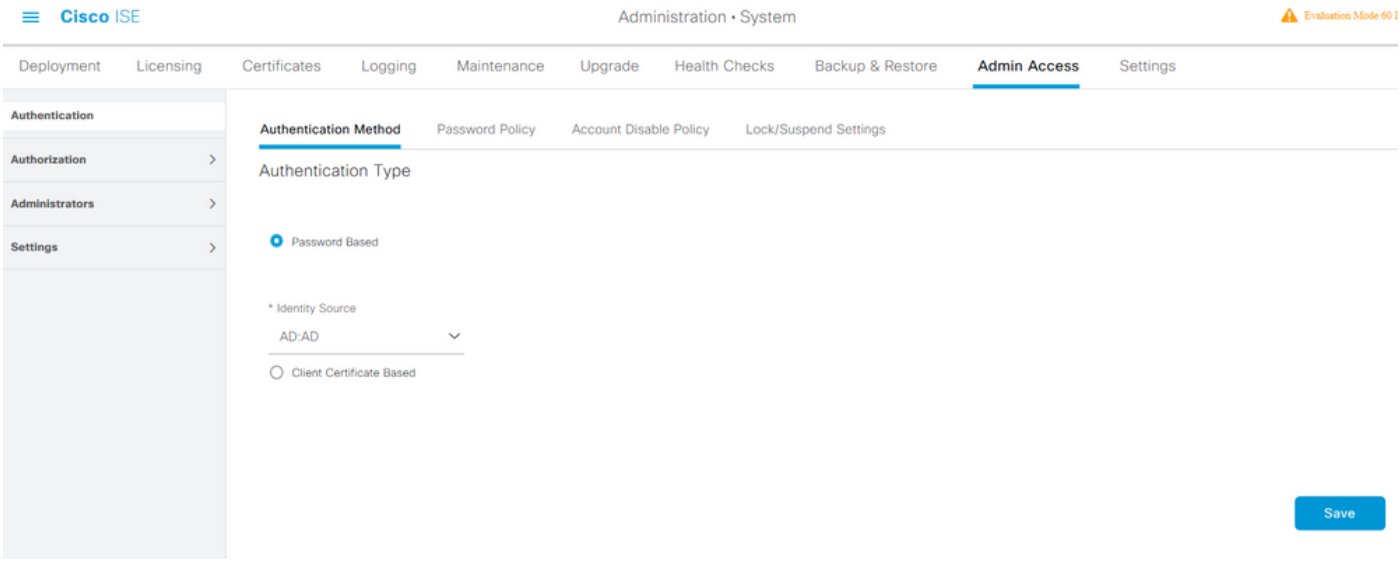
Passare a **Amministrazione > Gestione delle identità > Origini identità esterne > Active Directory**. Fare clic sul nome del punto di join desiderato e passare alla scheda **Gruppi**. Fare clic su **Aggiungi > Seleziona gruppi dalla directory > Recupera gruppi**. Importare almeno un gruppo AD al quale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





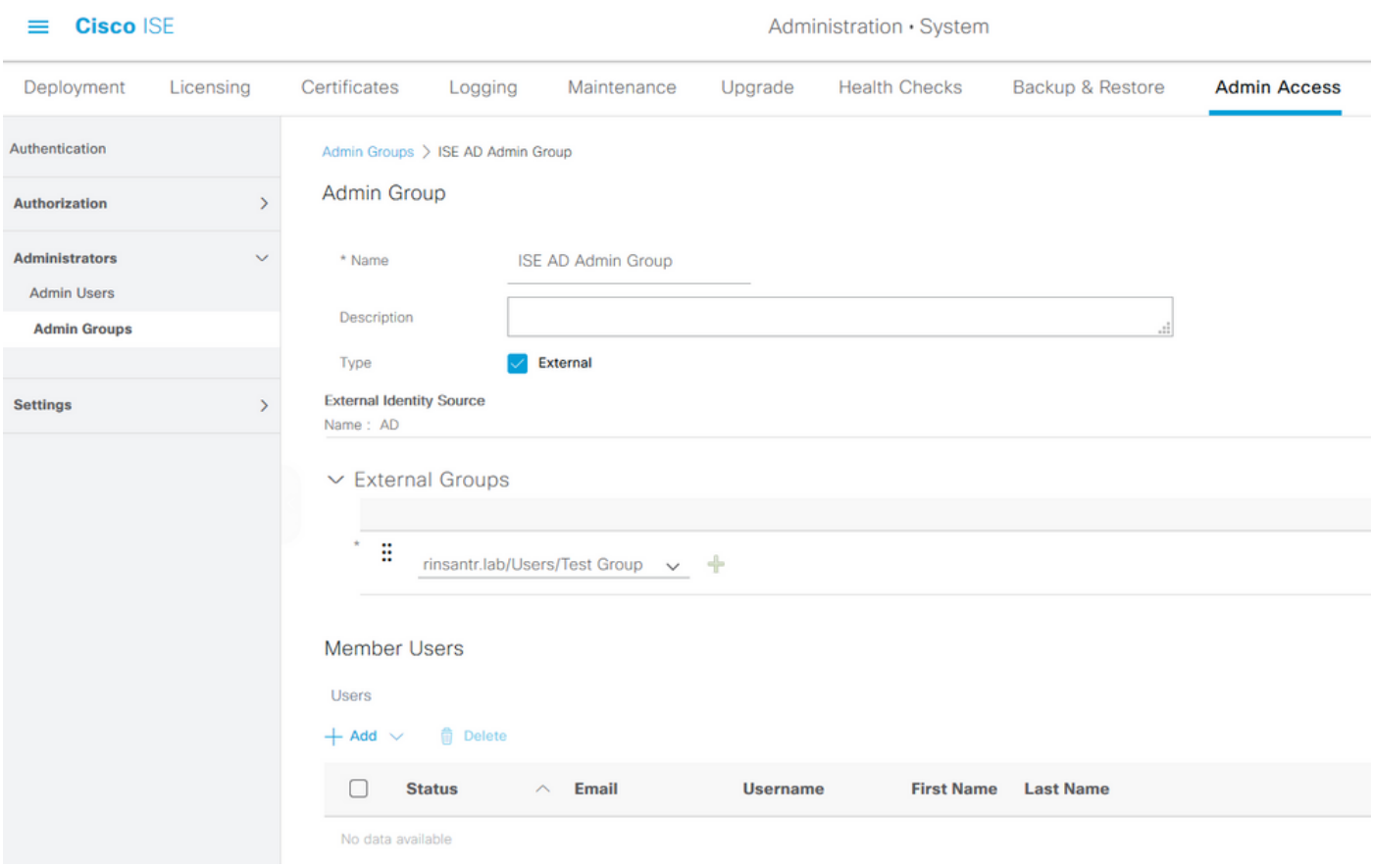
Abilita accesso amministrativo per AD

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**.



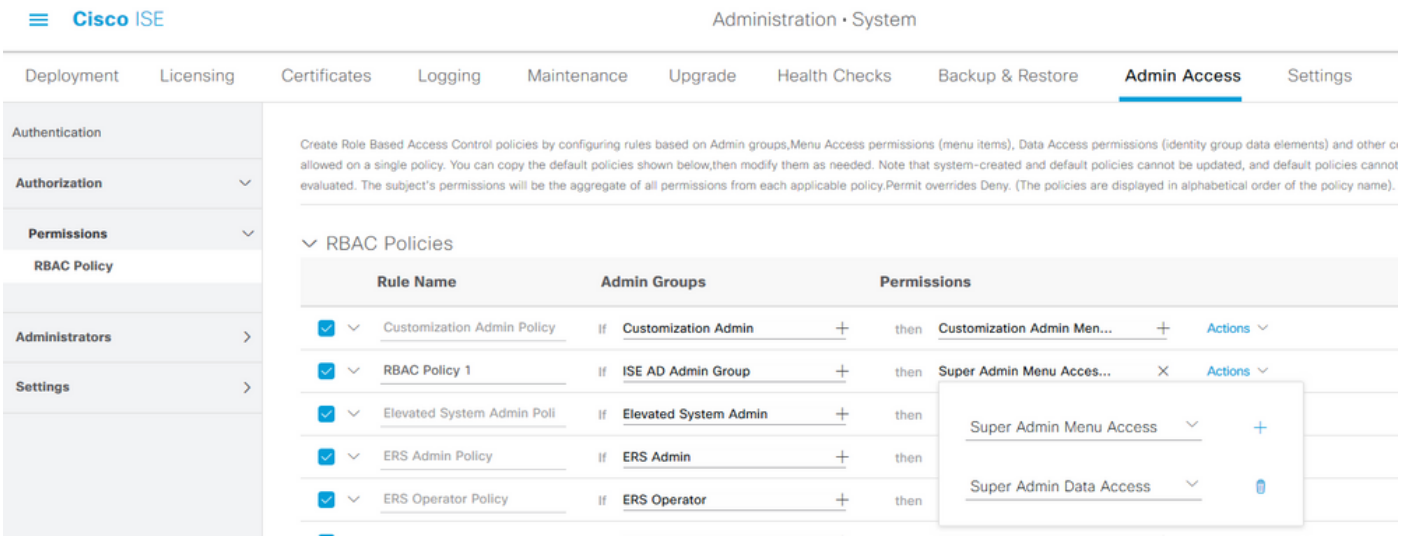
Configurazione del mapping tra il gruppo di amministratori ISE e il gruppo AD

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.



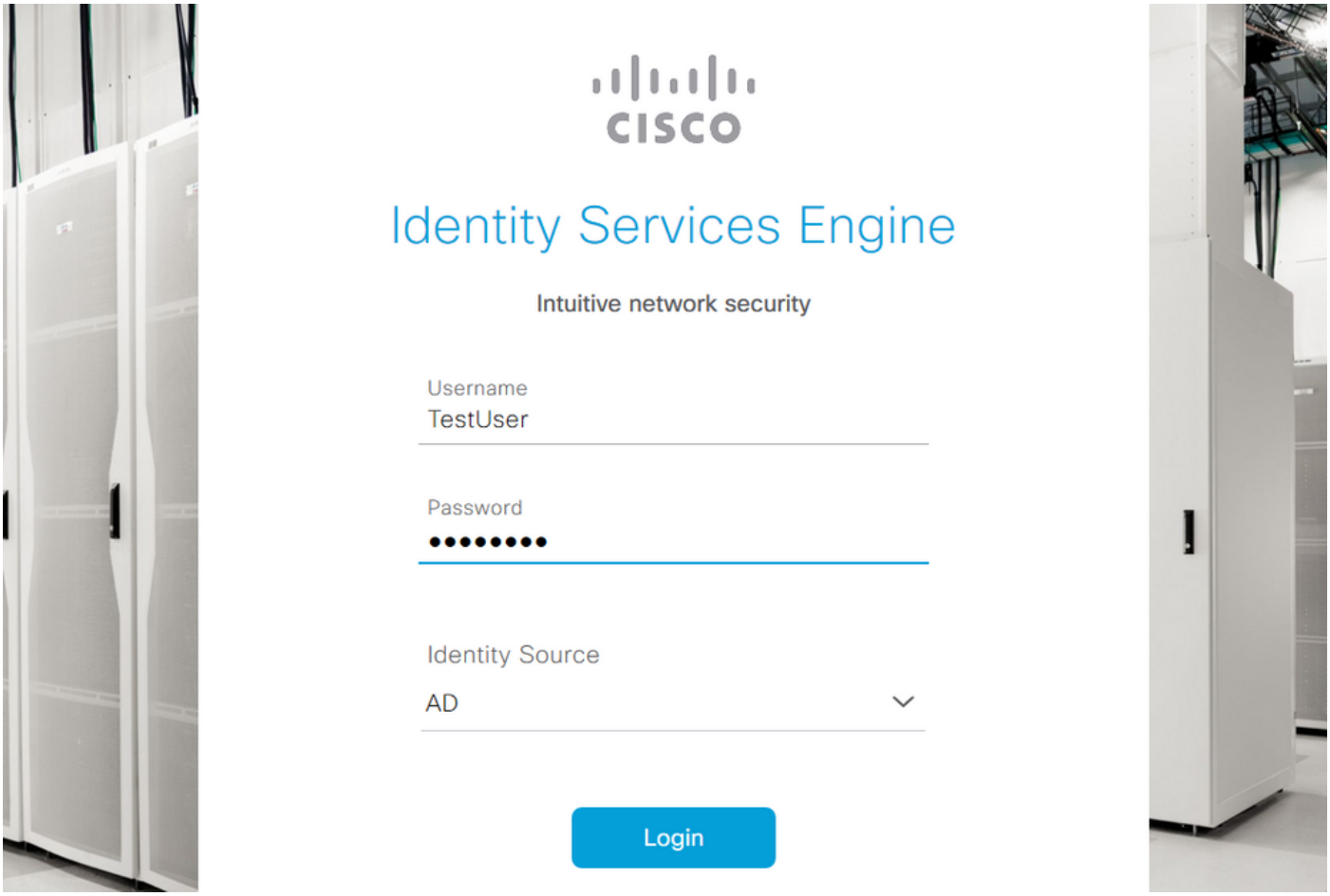
Impostare le autorizzazioni RBAC per il gruppo Admin

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**.

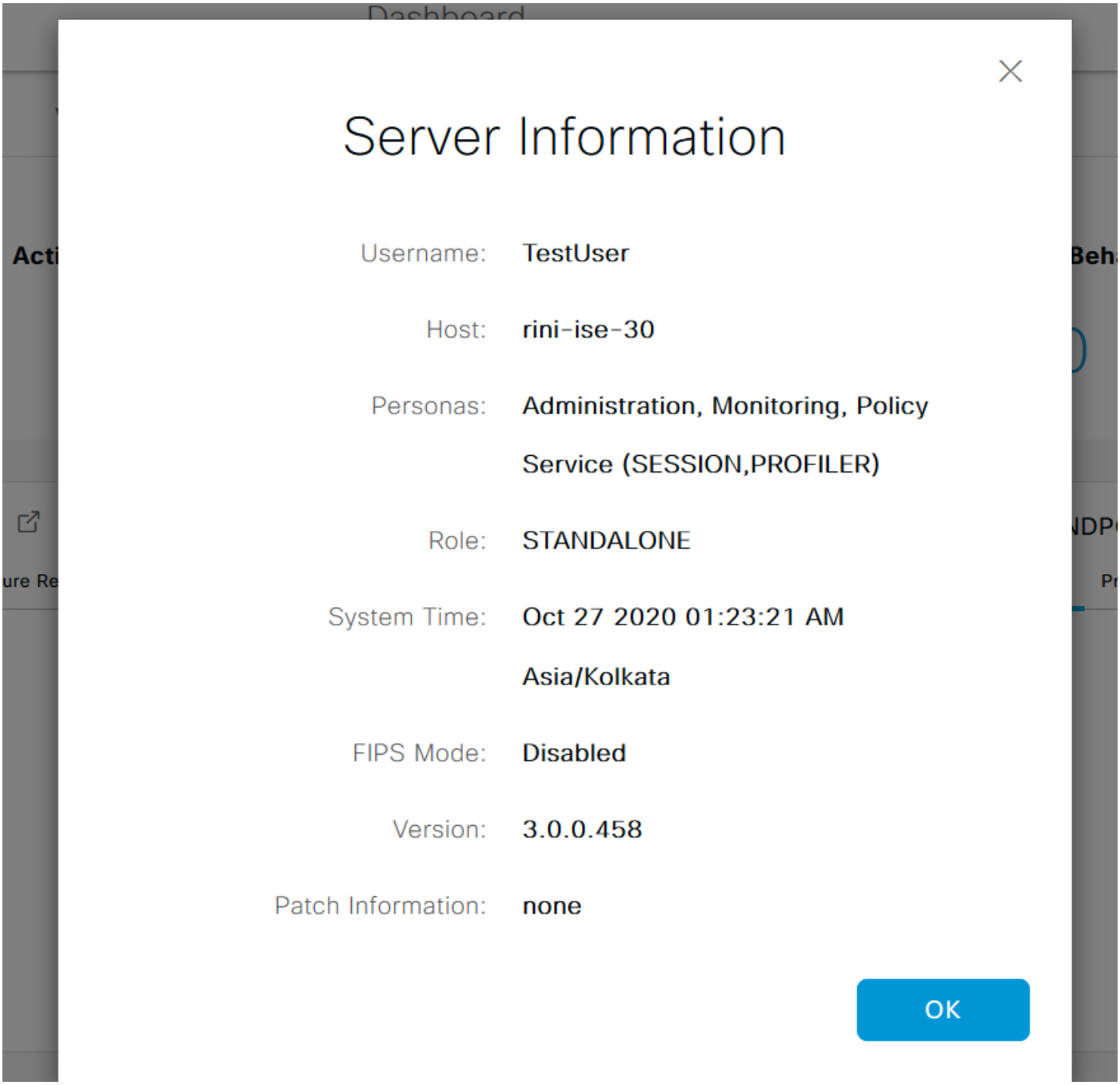


Accesso a ISE con credenziali AD e verifica

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.



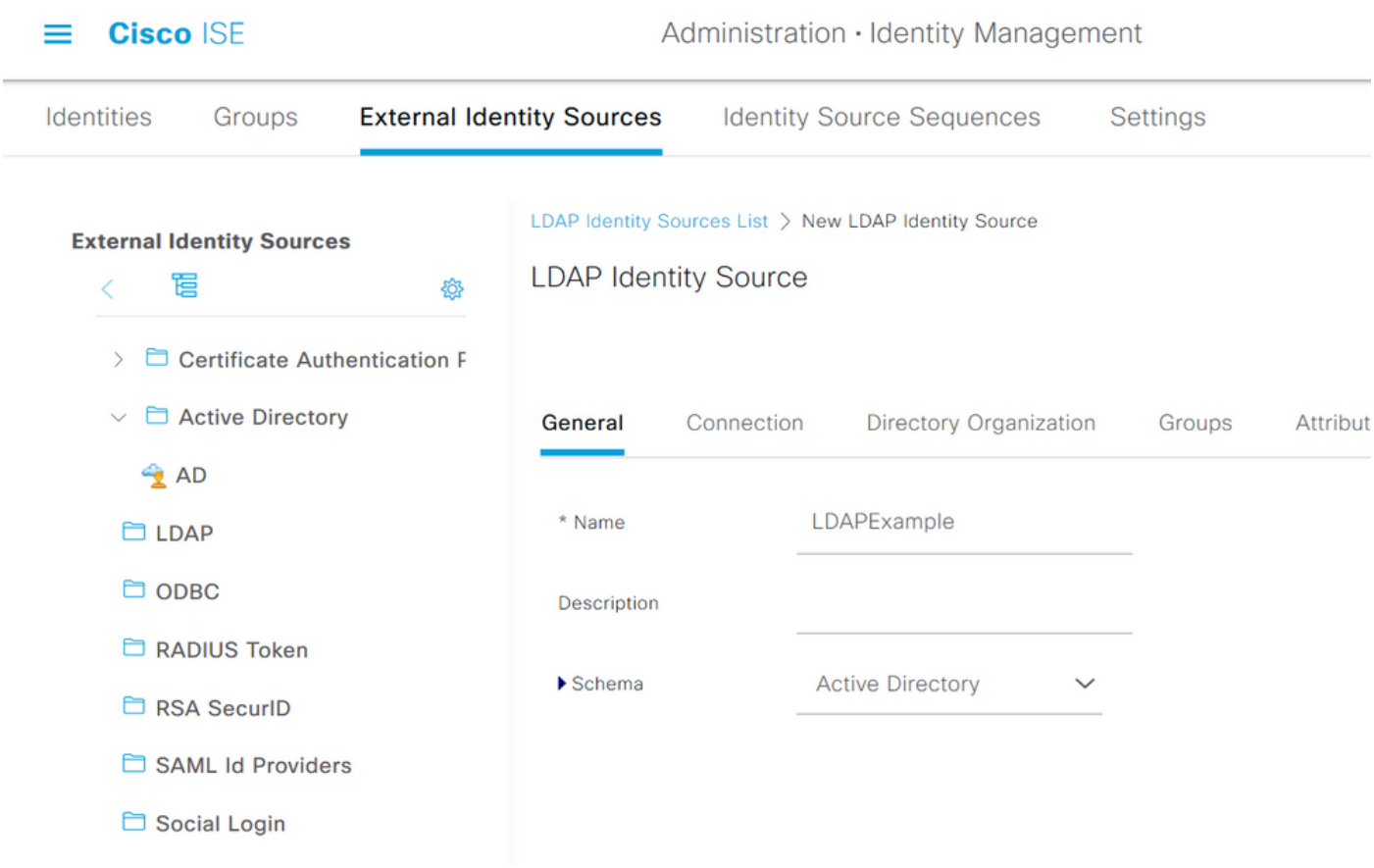
Per verificare che la configurazione funzioni correttamente, verificare il nome utente autenticato usando l'icona **Settings** nell'angolo in alto a destra dell'interfaccia grafica di ISE. Passare a **Informazioni server** e verificare il nome utente.



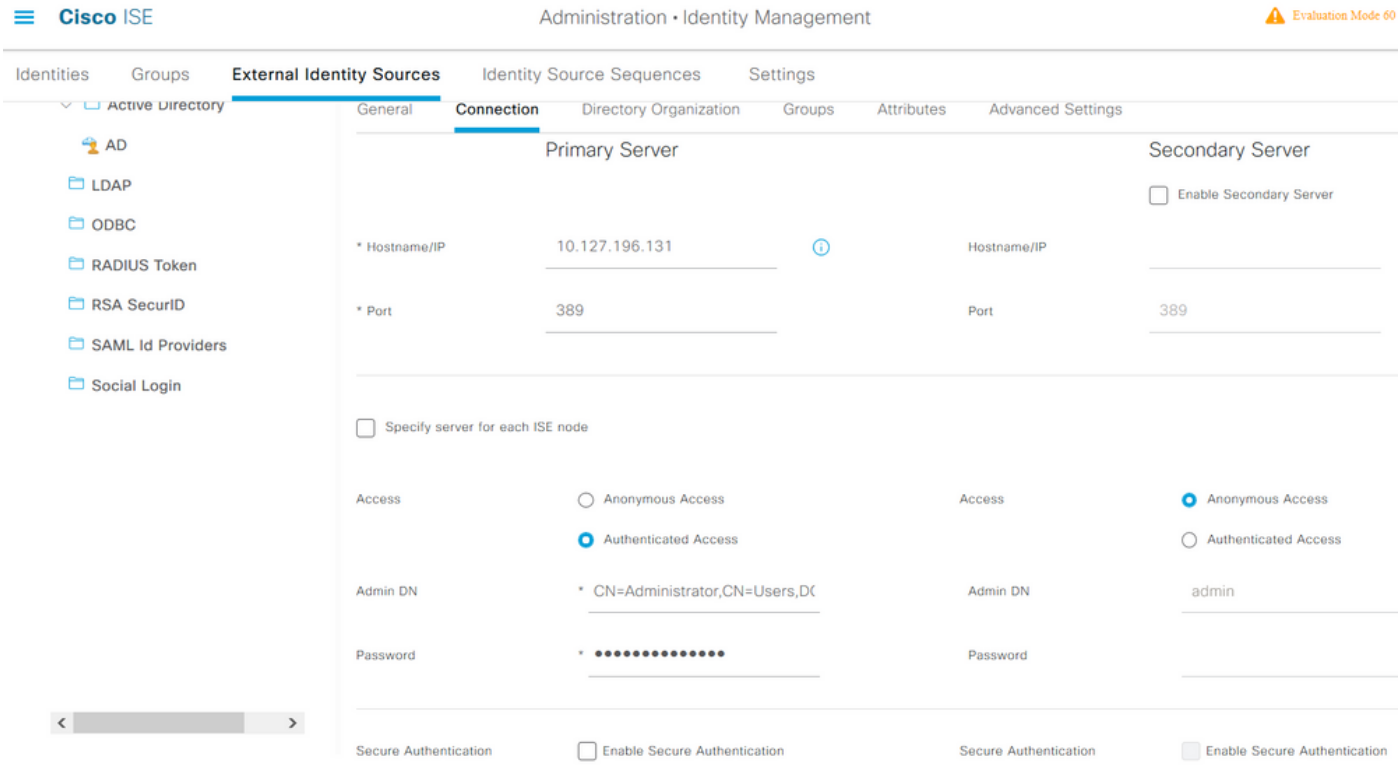
Configura accesso al portale di amministrazione con LDAP

Unisci ISE a LDAP

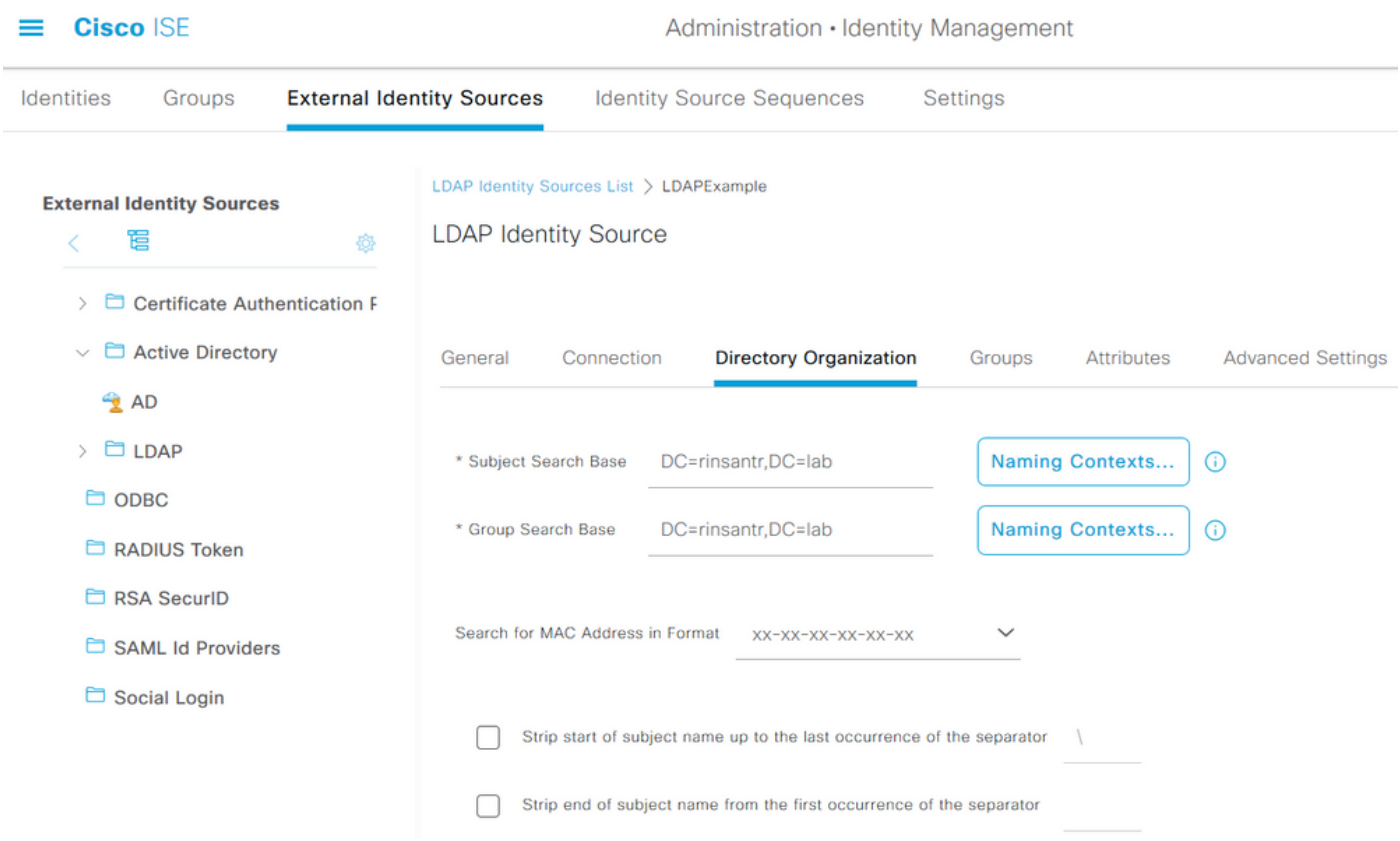
Passare a **Amministrazione > Gestione delle identità > Origini identità esterne > Active Directory > LDAP**. Nella scheda **Generale**, immettere un nome per il server LDAP e scegliere lo schema come **Active Directory**.



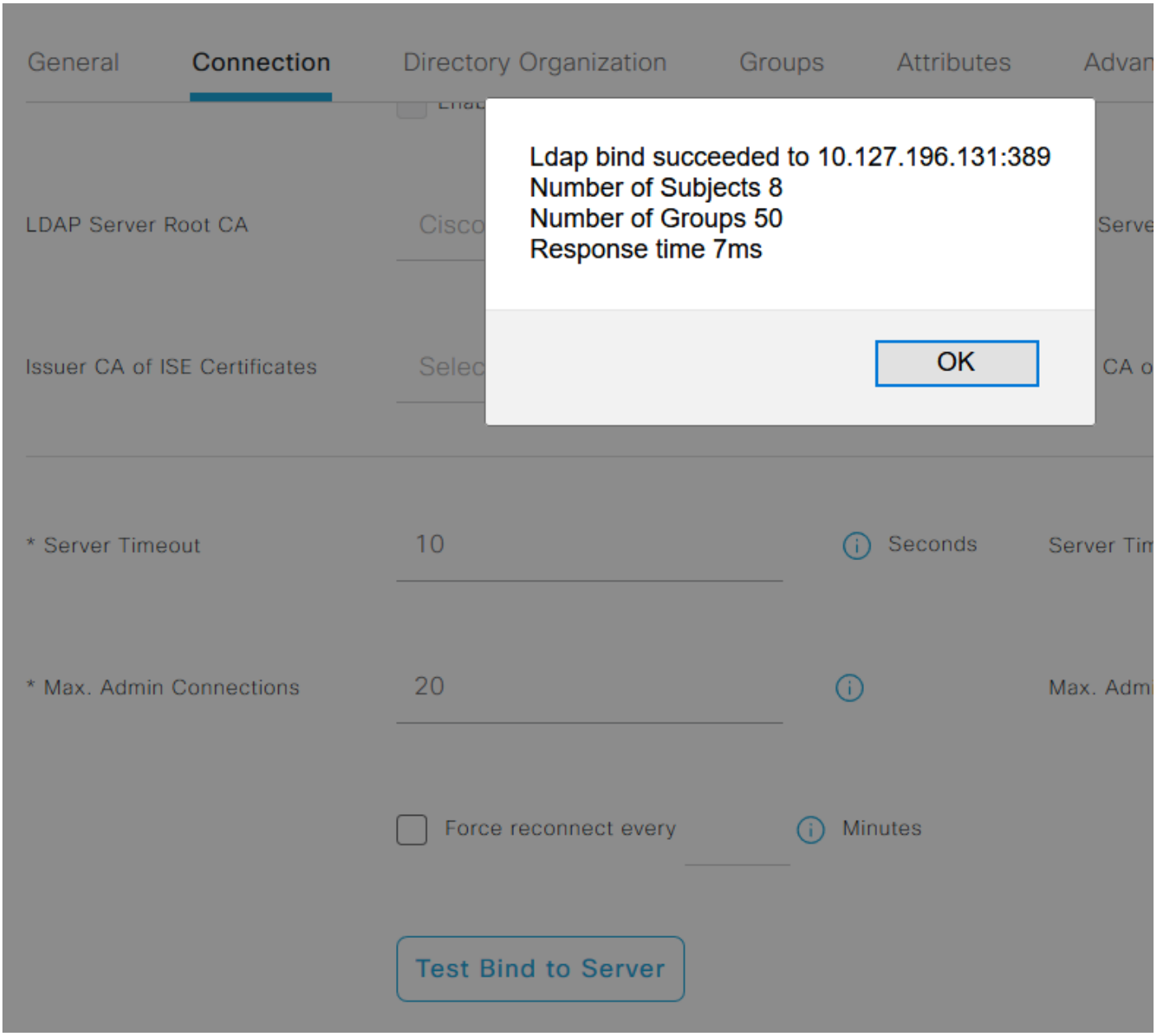
Quindi, per configurare il tipo di connessione, passare alla scheda **Connessione**. Qui, impostare il nome host/IP del server LDAP principale insieme alla porta 389(LDAP)/636 (LDAP-Secure). Immettere il percorso del DN (nome distinto) dell'amministratore con la password Admin del server LDAP.



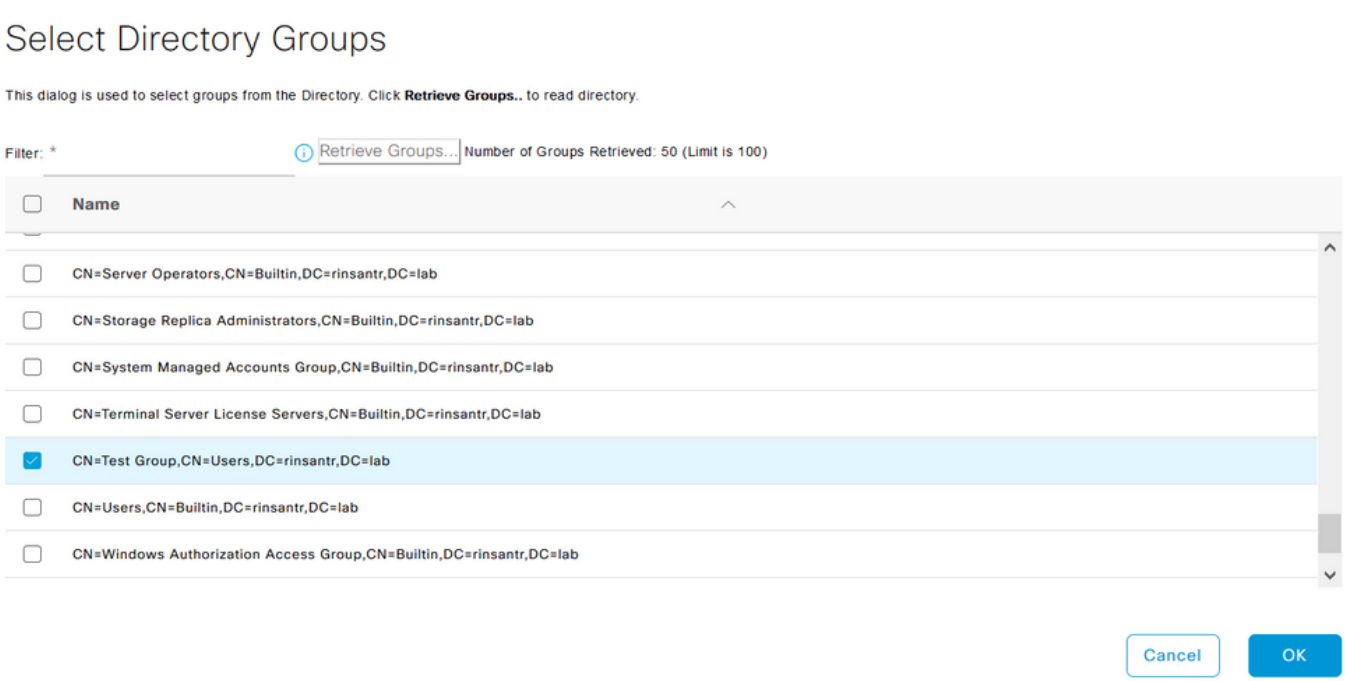
Passare quindi alla scheda **Organizzazione directory** e fare clic su **Contesti di denominazione** per scegliere il gruppo di organizzazioni corretto dell'utente in base alla gerarchia degli utenti memorizzati nel server LDAP.

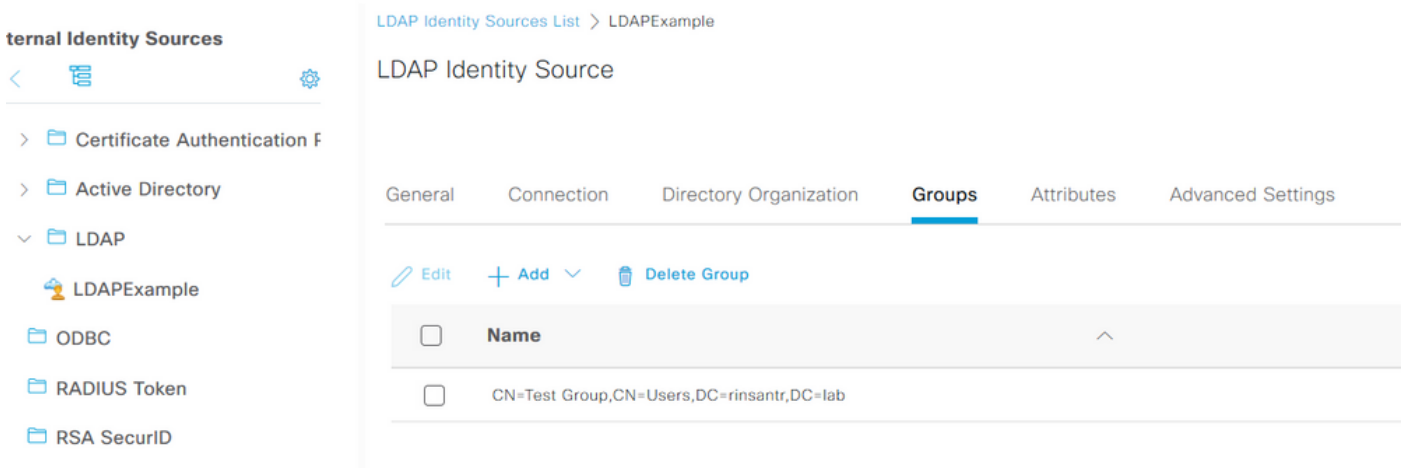


Fare clic su **Test Bind to Server** nella scheda **Connection** per verificare la raggiungibilità del server LDAP da ISE.



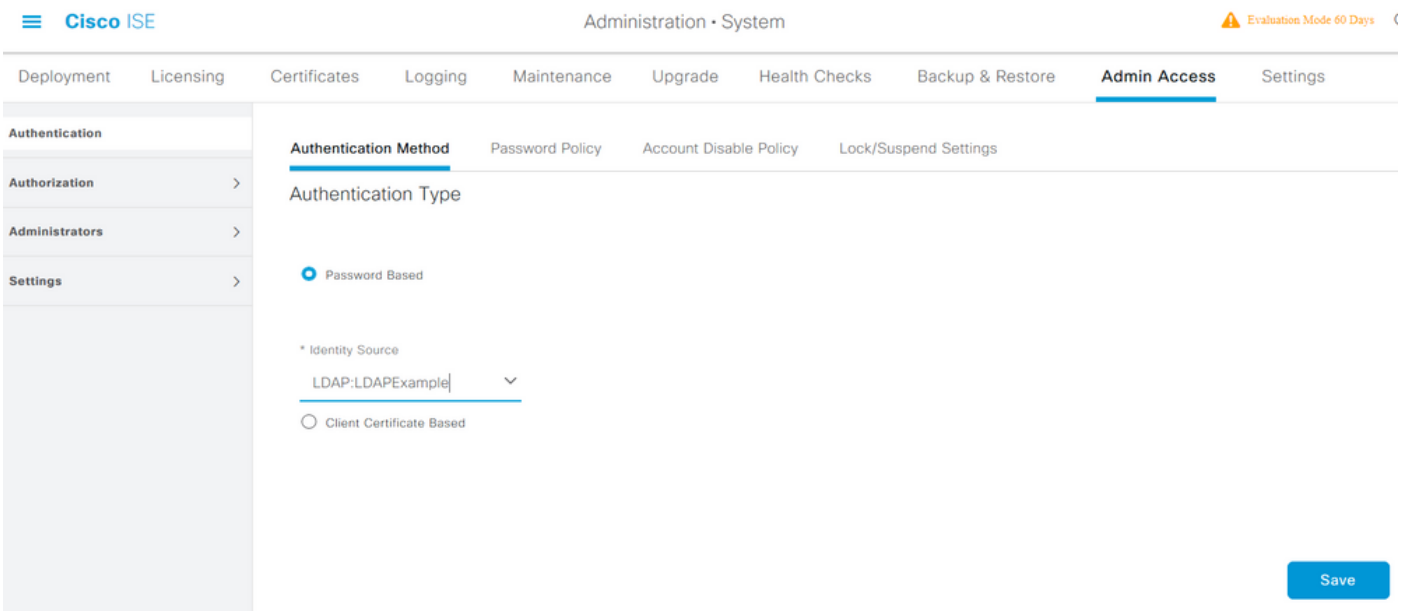
Passare alla scheda **Gruppi** e fare clic su **Aggiungi > Seleziona gruppi da directory > Recupera gruppi**. Importare almeno un gruppo a cui appartiene l'amministratore, fare clic su **OK**, quindi su **Salva**.





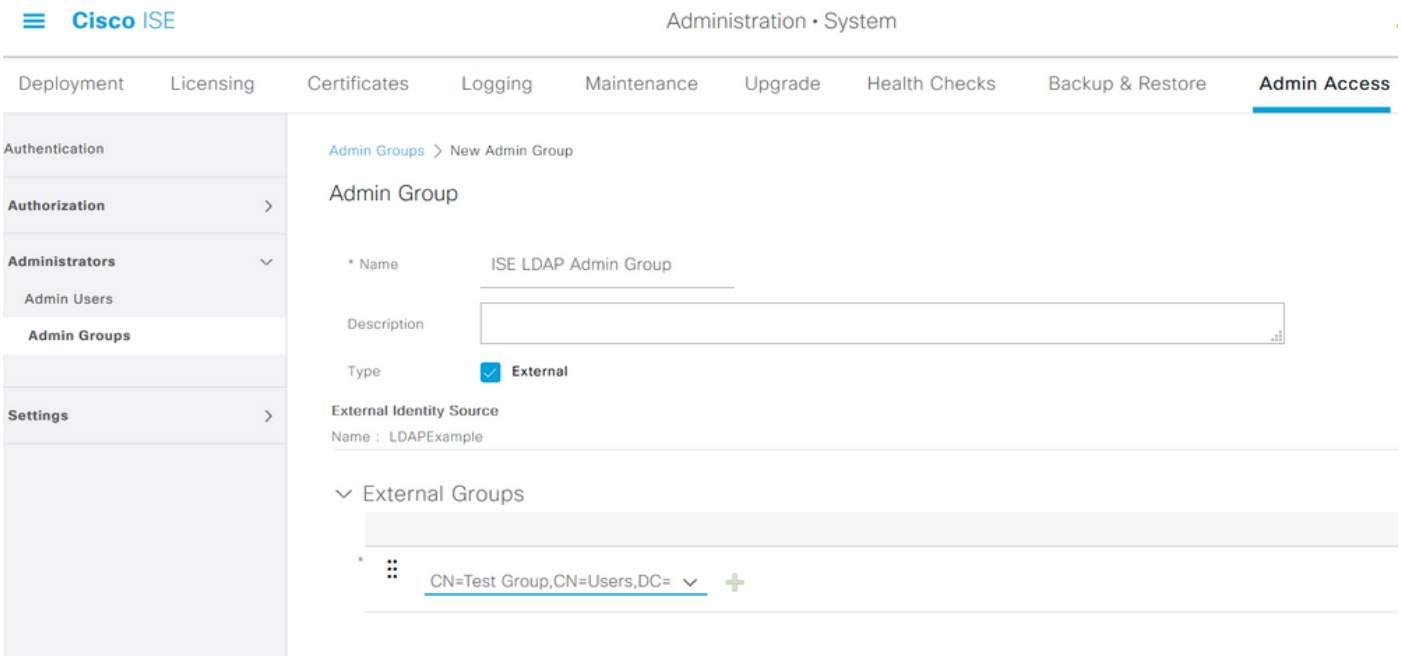
Abilita accesso amministrativo per utenti LDAP

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**.



Mappa il gruppo di amministratori ISE al gruppo LDAP

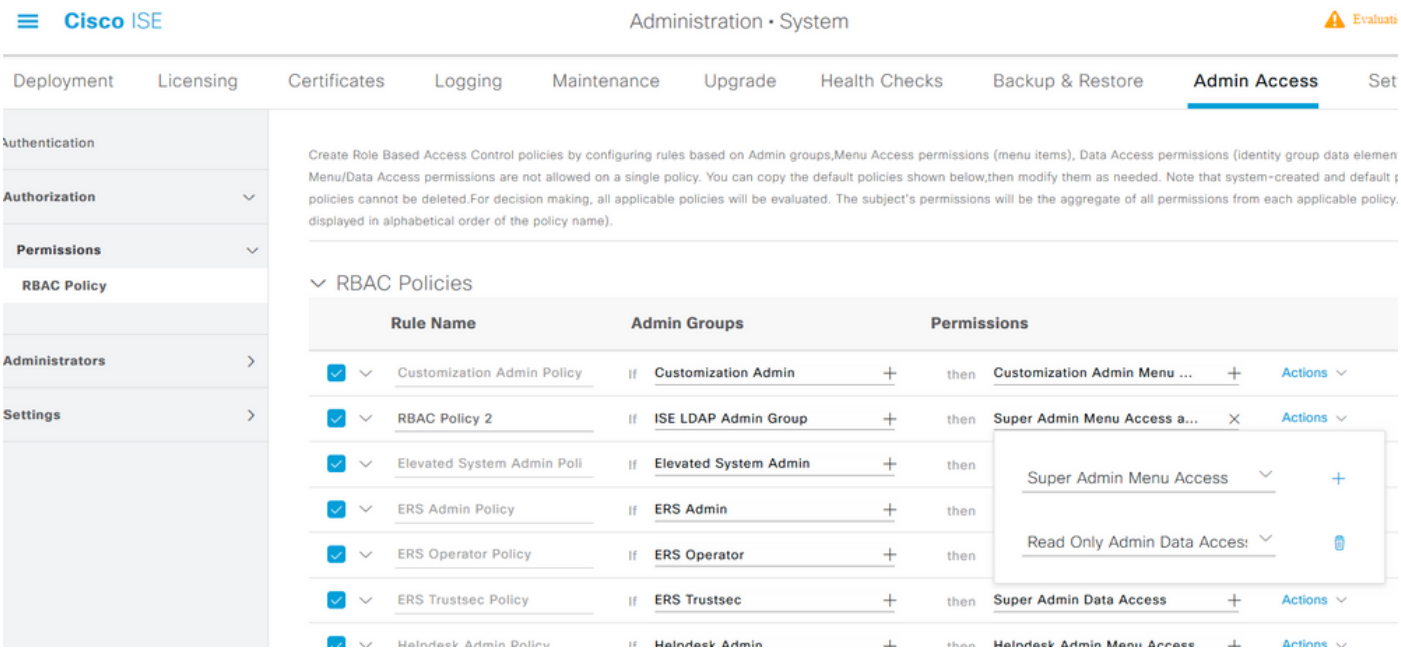
Questo consente all'utente configurato di ottenere l'accesso come amministratore in base all'autorizzazione dei criteri RBAC, che a sua volta si basa sull'appartenenza dell'utente al gruppo LDAP. Per definire un Cisco ISE Admin Group e mapparlo a un gruppo LDAP, selezionare **Amministrazione > Sistema > 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.



Impostare le autorizzazioni RBAC per il gruppo Admin

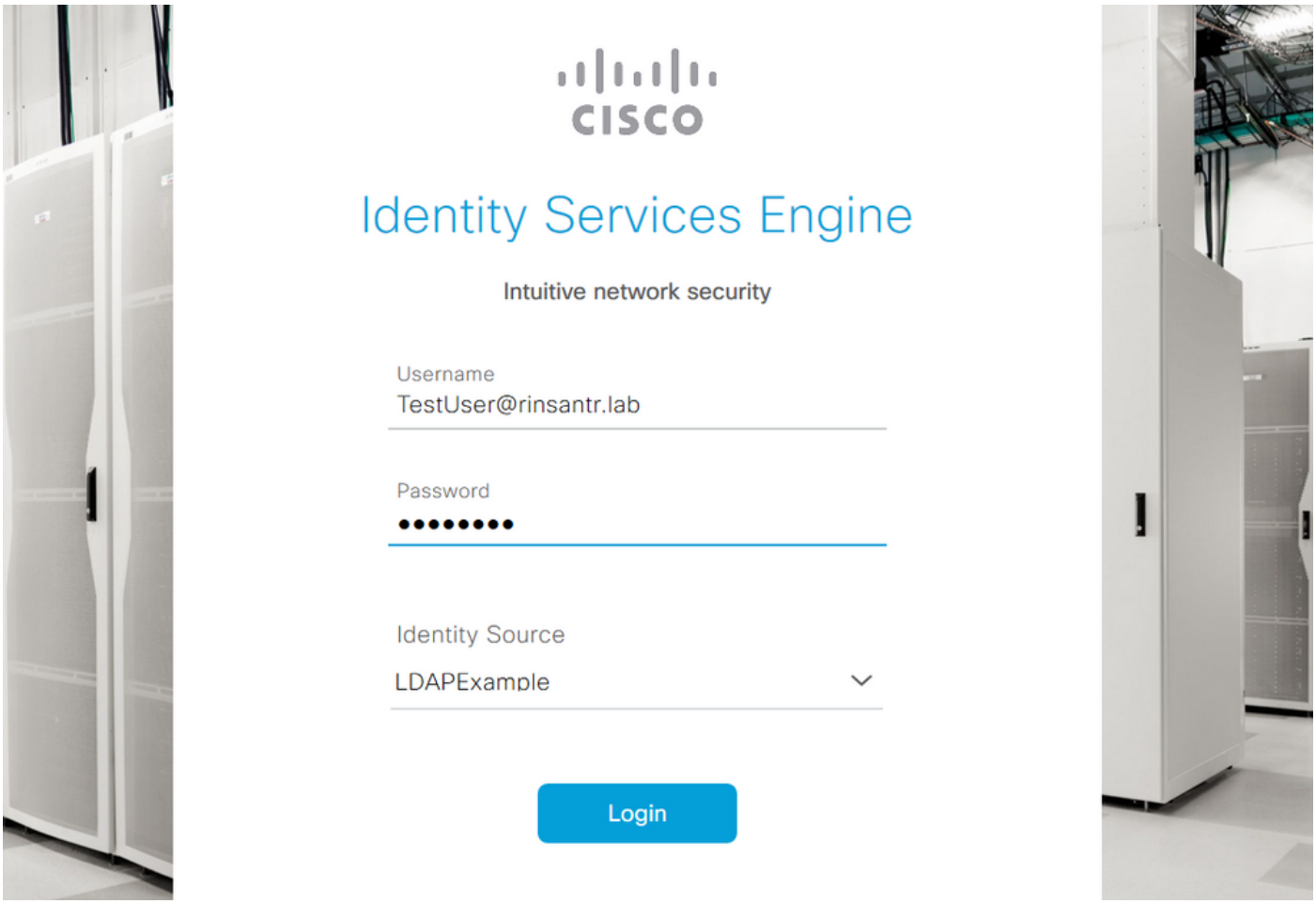
Per assegnare le autorizzazioni RBAC al gruppo di amministratori creato nella sezione precedente, selezionare **Amministrazione > Sistema > Accesso amministratore > Autorizzazione > Criteri RBAC**. Dal menu a discesa **Azioni** a destra, selezionare **Inserisci nuovo criterio**. Creare una nuova regola,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



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.