Comprendre les politiques d'accès administrateur et RBAC sur ISE

Contenu

Introduction

Ce document décrit les fonctionnalités d'ISE pour gérer l'accès administratif sur ISE (Identity Services Engine).

Conditions préalables

Conditions requises

Cisco vous recommande de connaître ces sujets :

- ISE
- Active Directory

- LDAP (Lightweight Directory Access Protocol)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

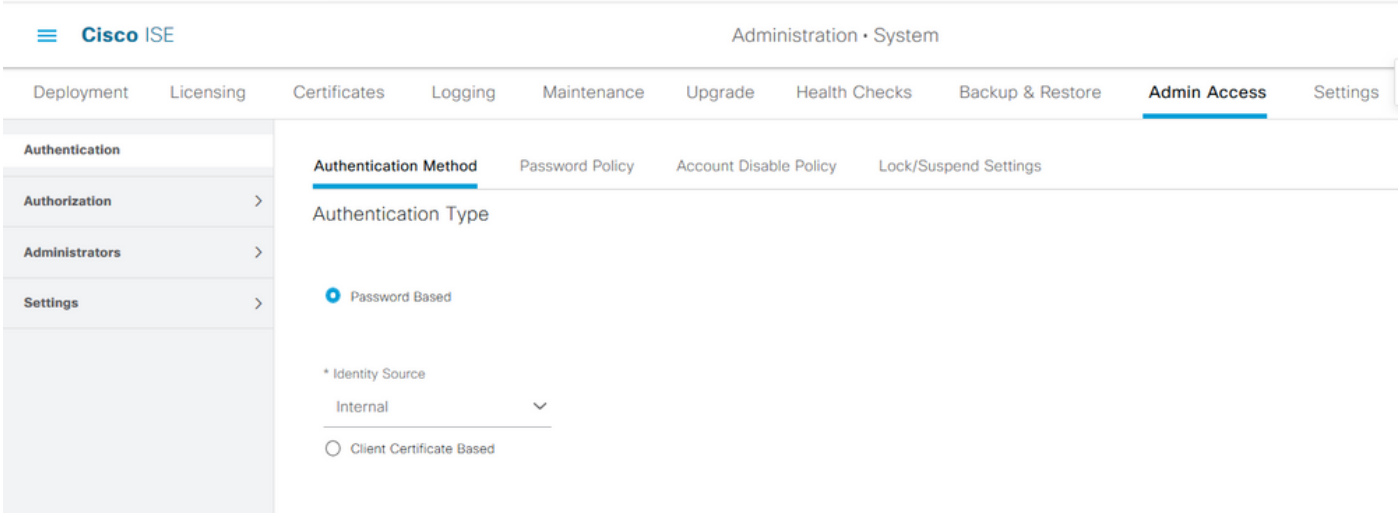
- Identity Services Engine 3.0
- Windows Server 2016

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

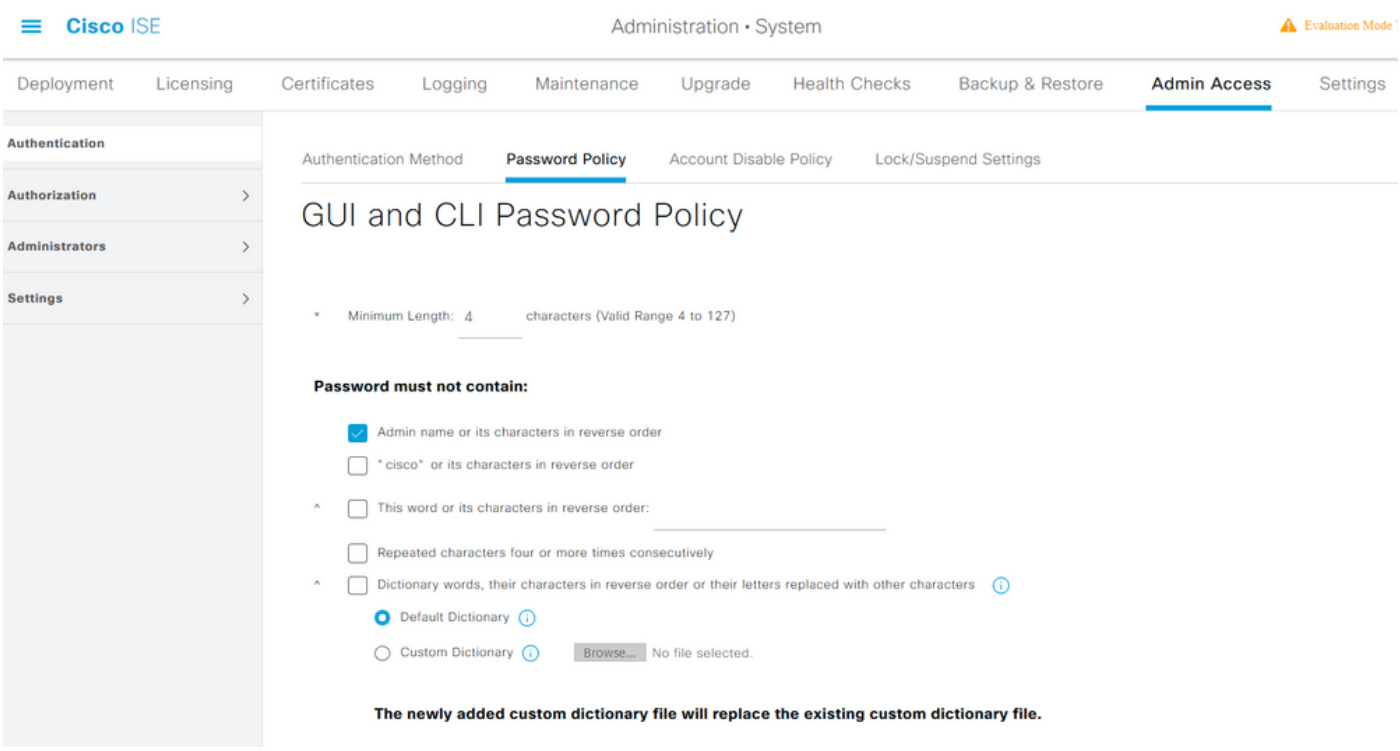
Paramètres d'authentification

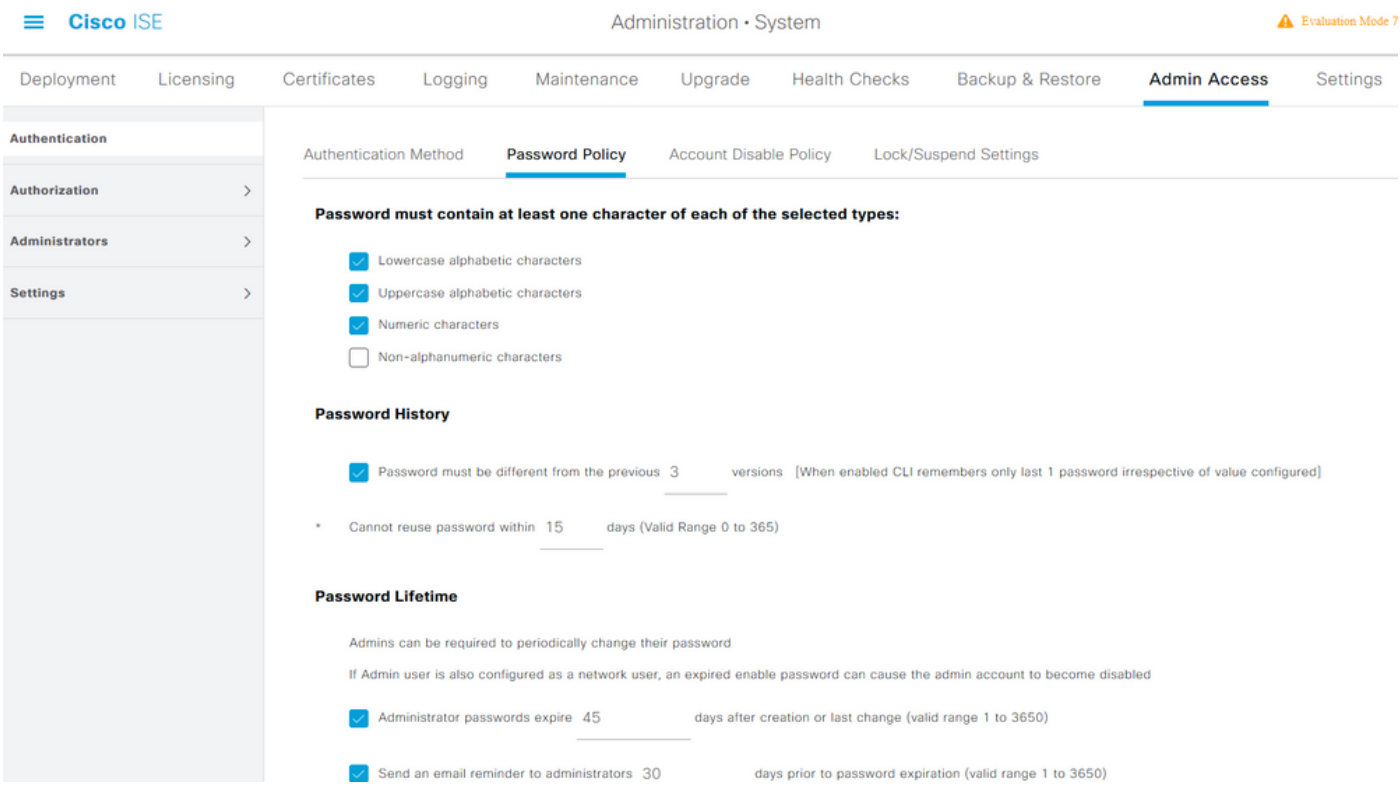
Les utilisateurs admin doivent s'authentifier pour accéder à toute information sur ISE. L'identité des utilisateurs admin peut être vérifiée à l'aide du magasin d'identités internes ISE ou d'un magasin d'identités externes. L'authenticité peut être vérifiée par un mot de passe ou un certificat. Afin de configurer ces paramètres, accédez à **Administration > System > Admin Access > Authentication**. Sélectionnez le type d'authentification requis sous l'onglet **Authentication Method**.



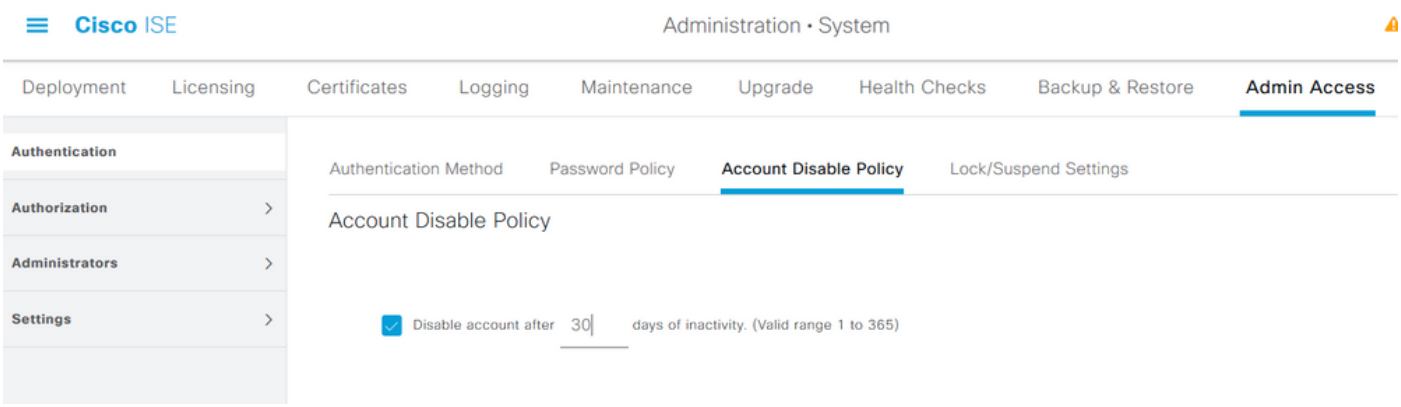
> **Note**: L'authentification basée sur le mot de passe est activée par défaut. Si l'authentification basée sur le certificat client est modifiée, cela entraîne le redémarrage d'un serveur d'applications sur tous les noeuds de déploiement.

Identity Services Engine ne permet pas de configurer la stratégie de mot de passe pour l'interface de ligne de commande (CLI) à partir de l'interface de ligne de commande. La stratégie de mot de passe de l'interface graphique utilisateur (GUI) et de l'interface de ligne de commande ne peut être configurée que via l'interface utilisateur graphique d'ISE. Afin de configurer ceci, accédez à **Administration > System > Admin Access > Authentication** et accédez à l'onglet **Password Policy**.

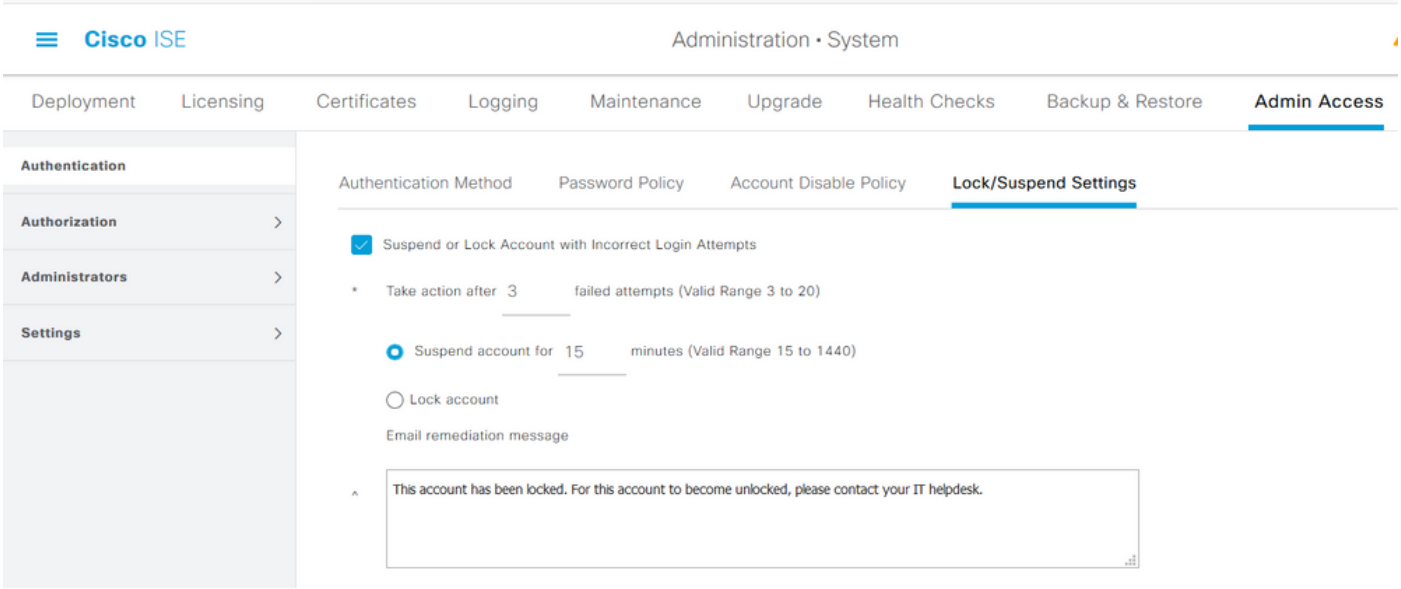




ISE dispose d'une provision pour désactiver un utilisateur administrateur inactif. Afin de configurer ceci, accédez à **Administration > System > Admin Access > Authentication** et accédez à l'onglet **Account Disable Policy**.



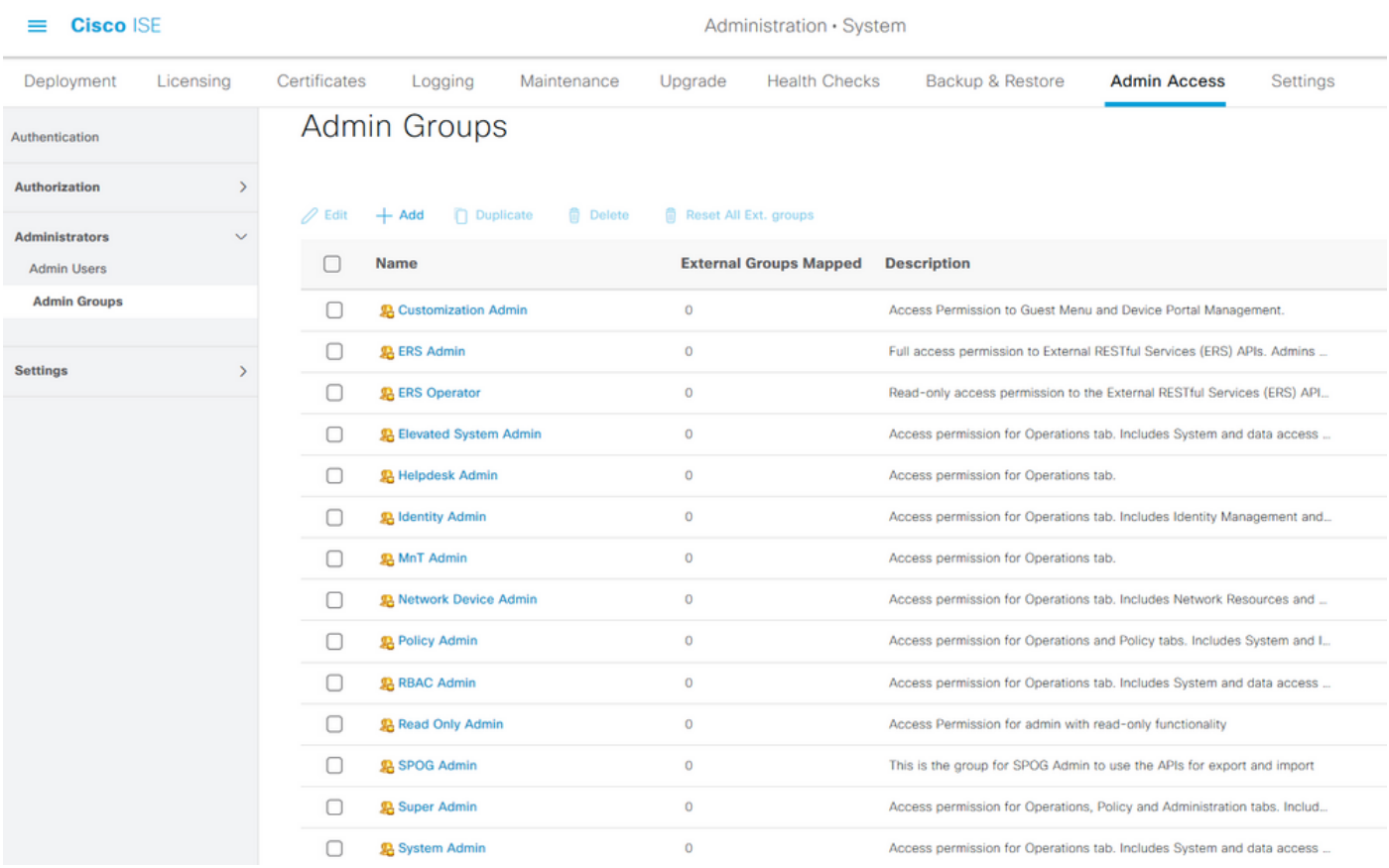
ISE permet également de verrouiller ou de suspendre un compte d'utilisateur administrateur en fonction du nombre de tentatives de connexion ayant échoué. Afin de configurer ceci, accédez à **Administration > System > Admin Access > Authentication** et accédez à l'onglet **Lock/Suspend Settings**.



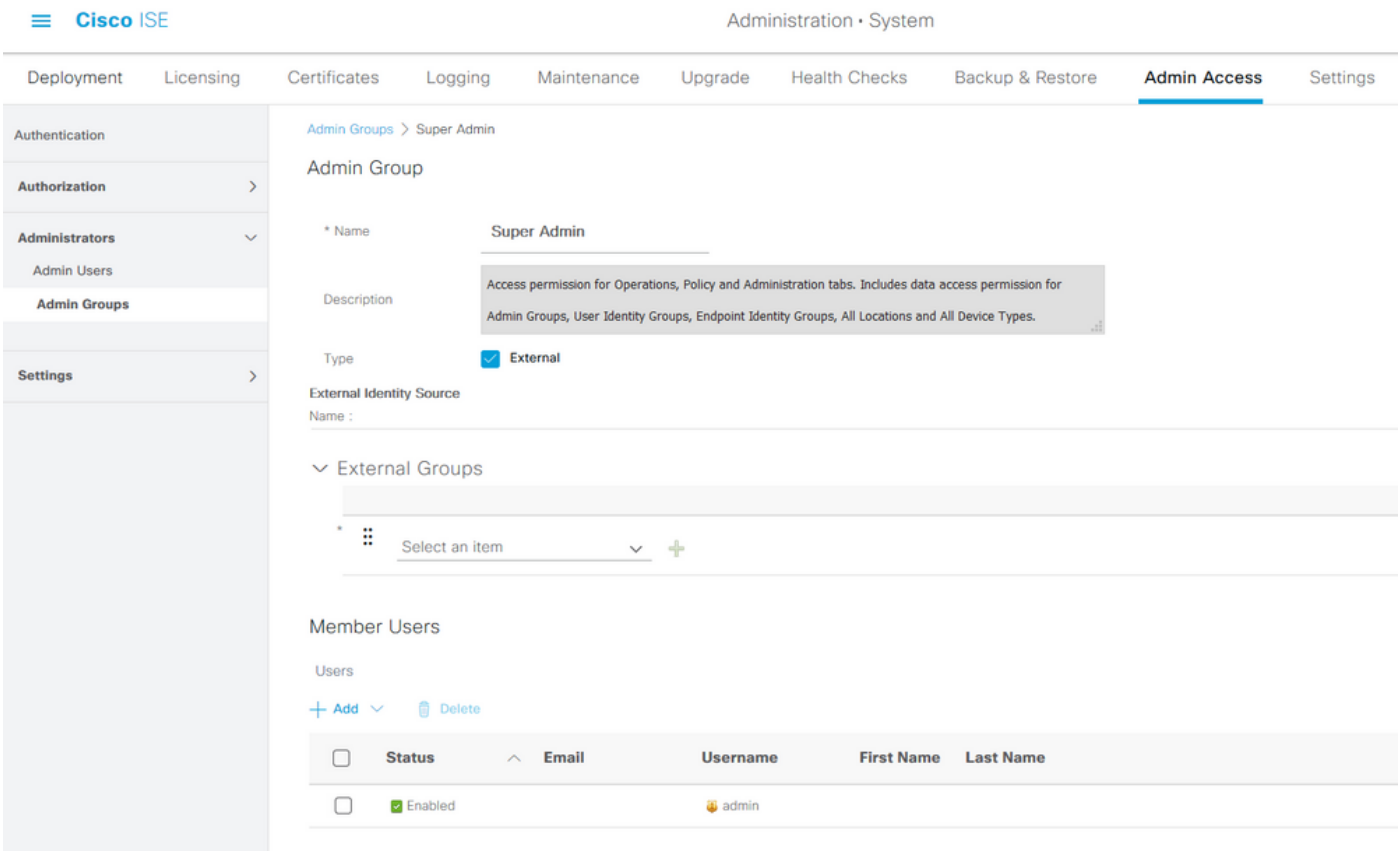
Pour gérer l'accès administratif, il est nécessaire que les groupes administratifs, les utilisateurs et les différentes politiques/règles contrôlent et gèrent leurs privilèges.

Configurer les groupes d'administration

Accédez à **Administration > System > Admin Access > Administrators > Admin Groups** pour configurer les groupes d'administrateurs. Il y a peu de groupes intégrés par défaut et ne peuvent pas être supprimés.

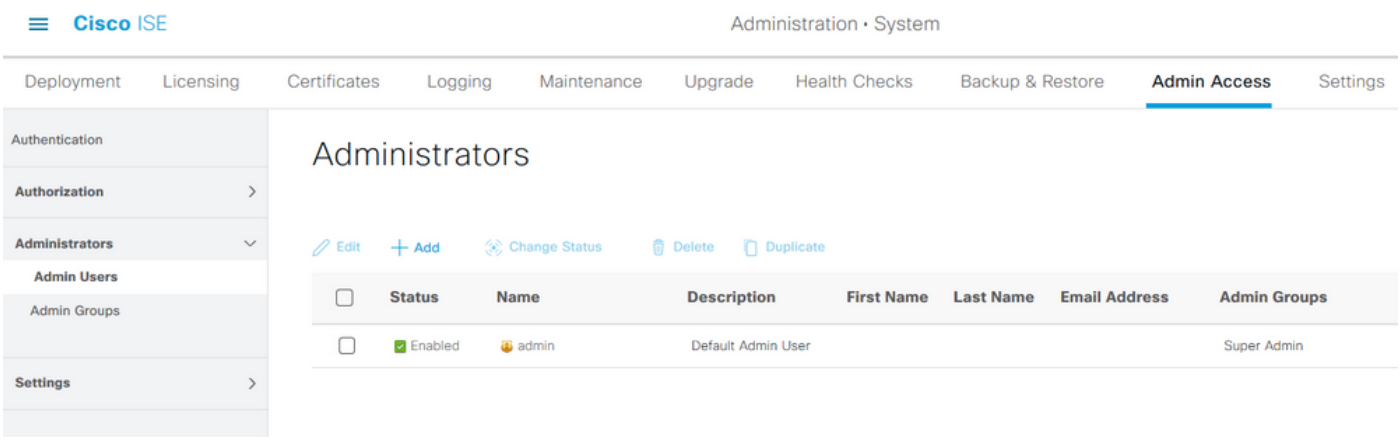


Une fois qu'un groupe est créé, sélectionnez-le et cliquez sur modifier pour ajouter des utilisateurs administratifs à ce groupe. Il existe une disposition permettant de mapper les groupes d'identité externes aux groupes d'administration sur ISE afin qu'un utilisateur d'administration externe obtienne les autorisations requises. Afin de configurer ceci, sélectionnez le type Externe lors de l'ajout de l'utilisateur.

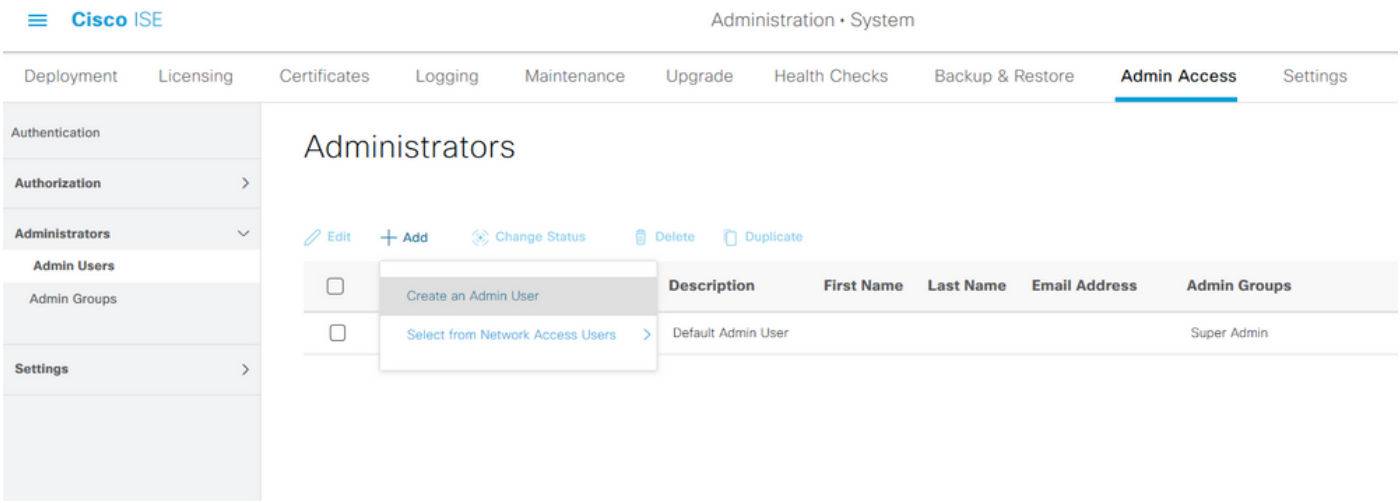


Configurer les utilisateurs admin

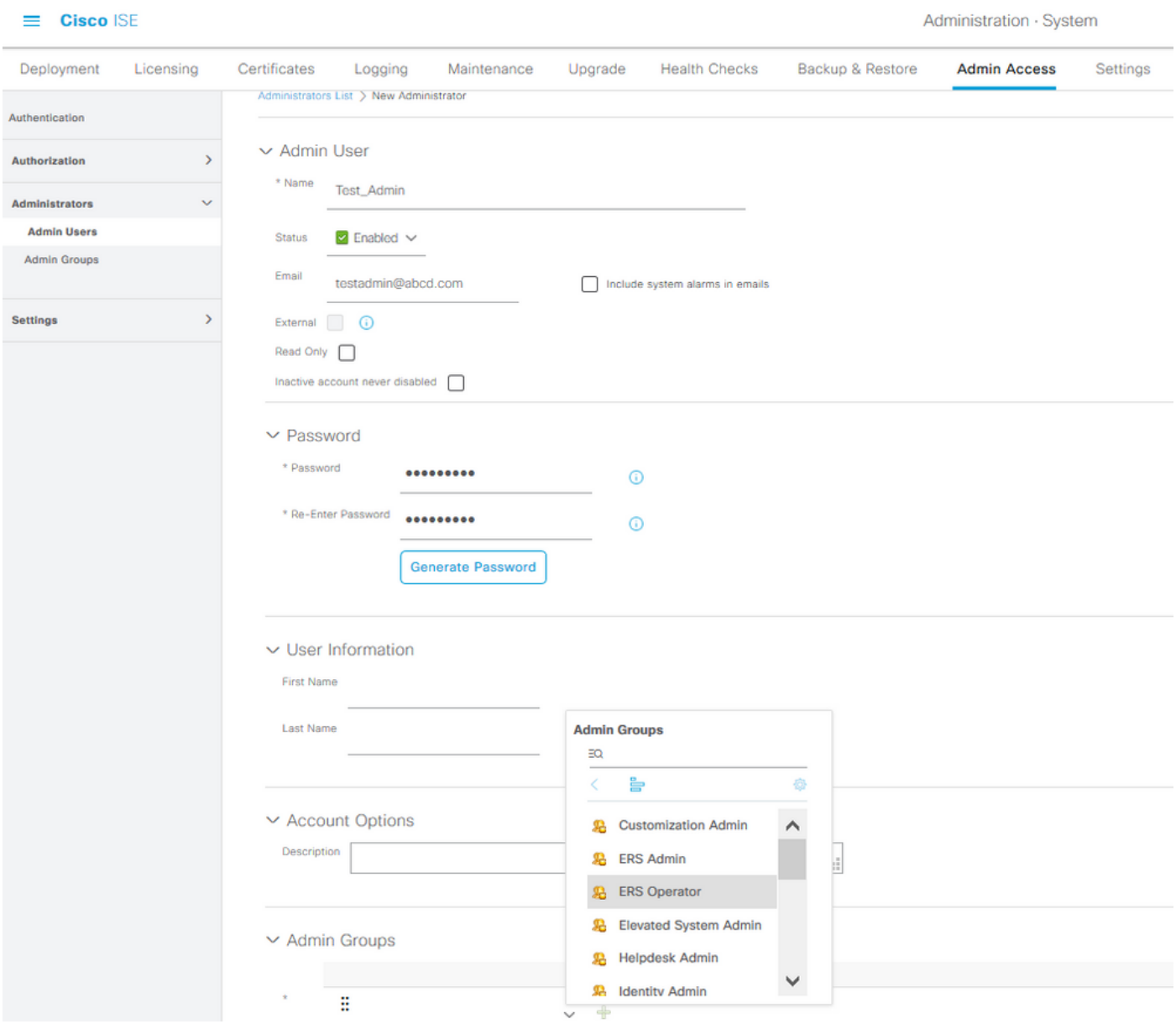
Afin de configurer les utilisateurs Admin, accédez à **Administration > System > Admin Access > Administrators > Admin Users**.



Cliquez sur **Add**. Deux options s'offrent à vous. L'une consiste à ajouter un nouvel utilisateur. L'autre est de faire un utilisateur d'accès au réseau (c'est-à-dire un utilisateur configuré en tant qu'utilisateur interne pour accéder au réseau/aux périphériques) en tant qu'administrateur ISE.



Une fois que vous avez sélectionné une option, les détails requis doivent être fournis et le groupe d'utilisateurs doit être sélectionné en fonction duquel les autorisations et privilèges sont accordés à l'utilisateur.



Configurer les autorisations

Deux types d'autorisations peuvent être configurés pour un groupe d'utilisateurs :

1. Accès au menu
2. Accès aux données

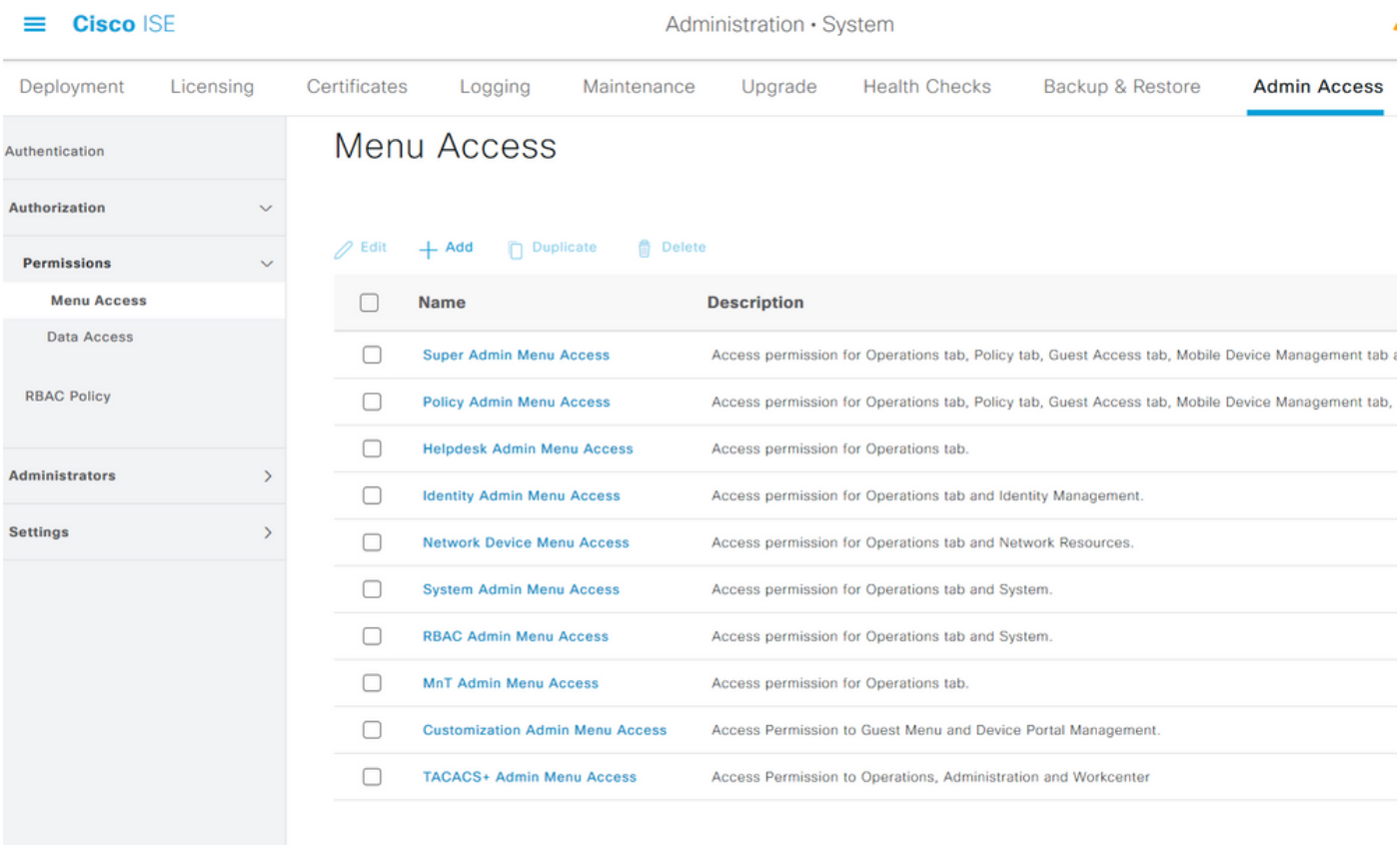
Menu Access contrôle la visibilité de navigation sur ISE. Il existe deux options pour chaque onglet, Afficher ou Masquer, qui peuvent être configurées. Une règle d'accès au menu peut être configurée pour afficher ou masquer les onglets sélectionnés.

Data Access contrôle la capacité à lire/accéder/modifier les données d'identité sur ISE. L'autorisation d'accès ne peut être configurée que pour les groupes d'administration, les groupes d'identité d'utilisateur, les groupes d'identité de point de terminaison et les groupes de périphériques réseau. Il existe trois options pour ces entités sur ISE qui peuvent être configurées. Il s'agit de l'accès complet, de l'accès en lecture seule et de l'absence d'accès. Une règle d'accès aux données peut être configurée pour choisir l'une de ces trois options pour chaque onglet de l'ISE.

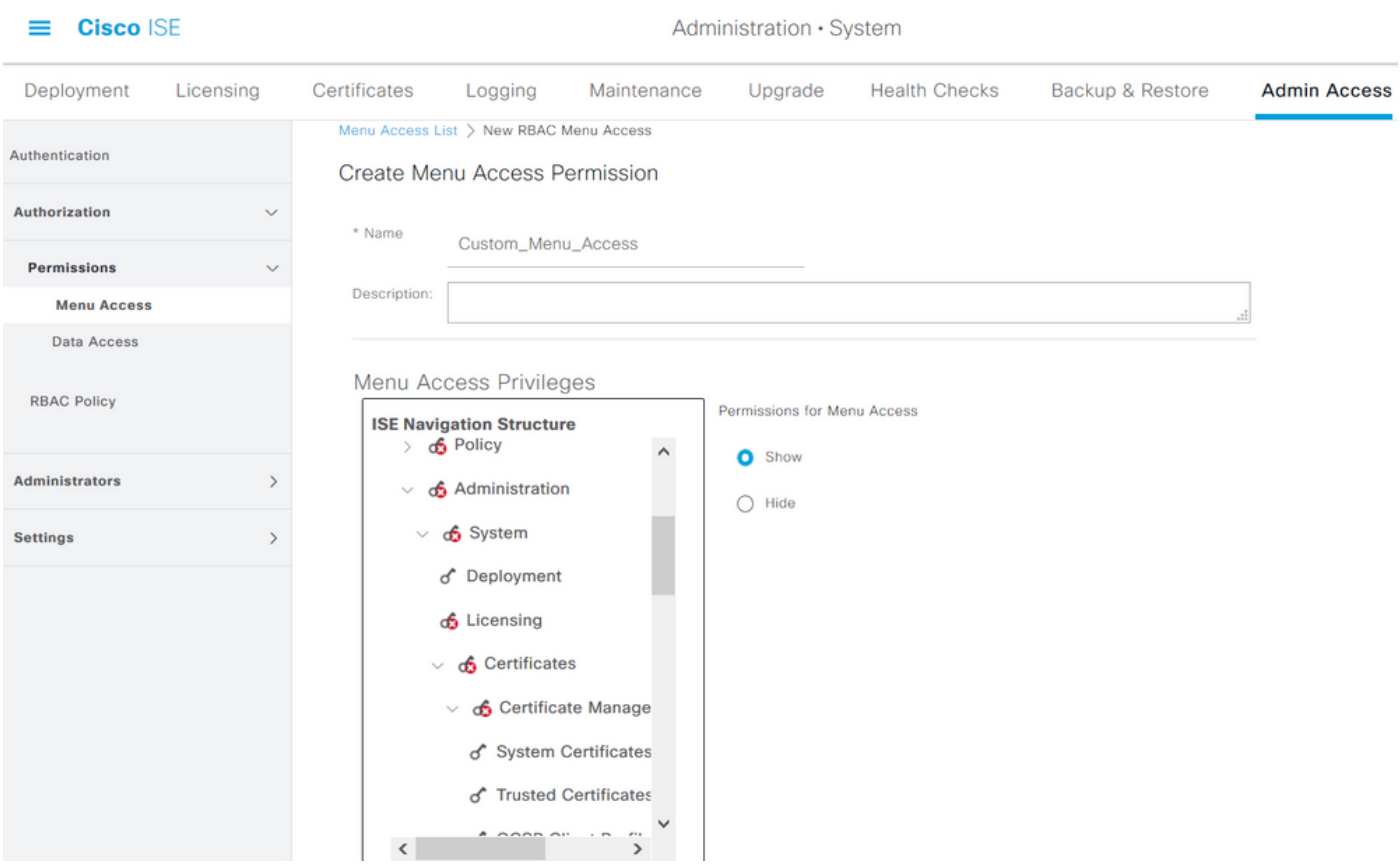
Les stratégies d'accès aux menus et d'accès aux données doivent être créées avant de pouvoir

être appliquées à n'importe quel groupe d'administrateurs. Il existe quelques stratégies intégrées par défaut, mais elles peuvent toujours être personnalisées ou une nouvelle peut être créée.

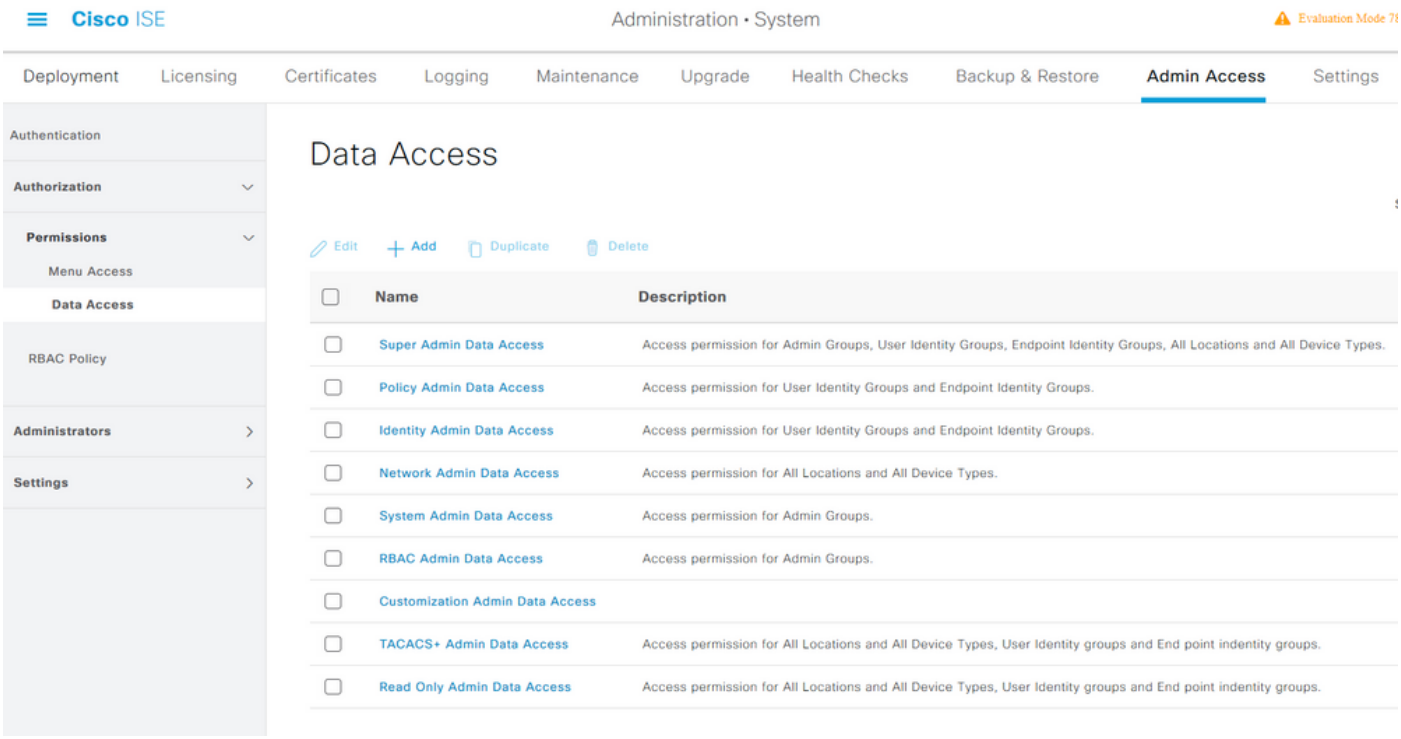
Afin de configurer une stratégie d'accès au menu, accédez à **Administration > System > Admin Access > Authorization > Permissions > Menu Access**.



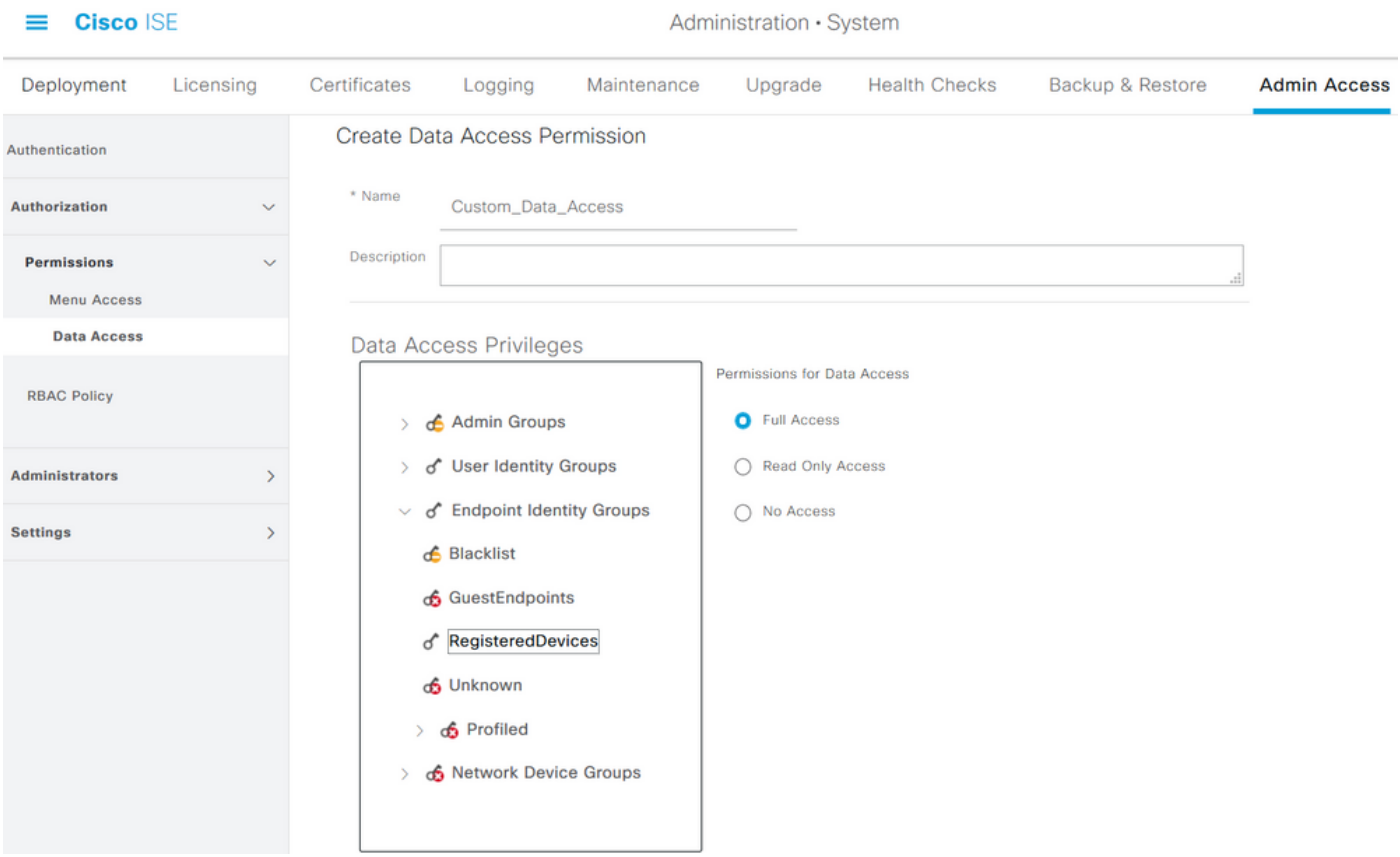
Cliquez sur **Add**. Chaque option de navigation dans ISE peut être configurée pour être affichée/masquée dans une stratégie.



Afin de configurer la stratégie d'accès aux données, accédez à **Administration > System > Admin Access > Authorization > Permissions > Data Access**.

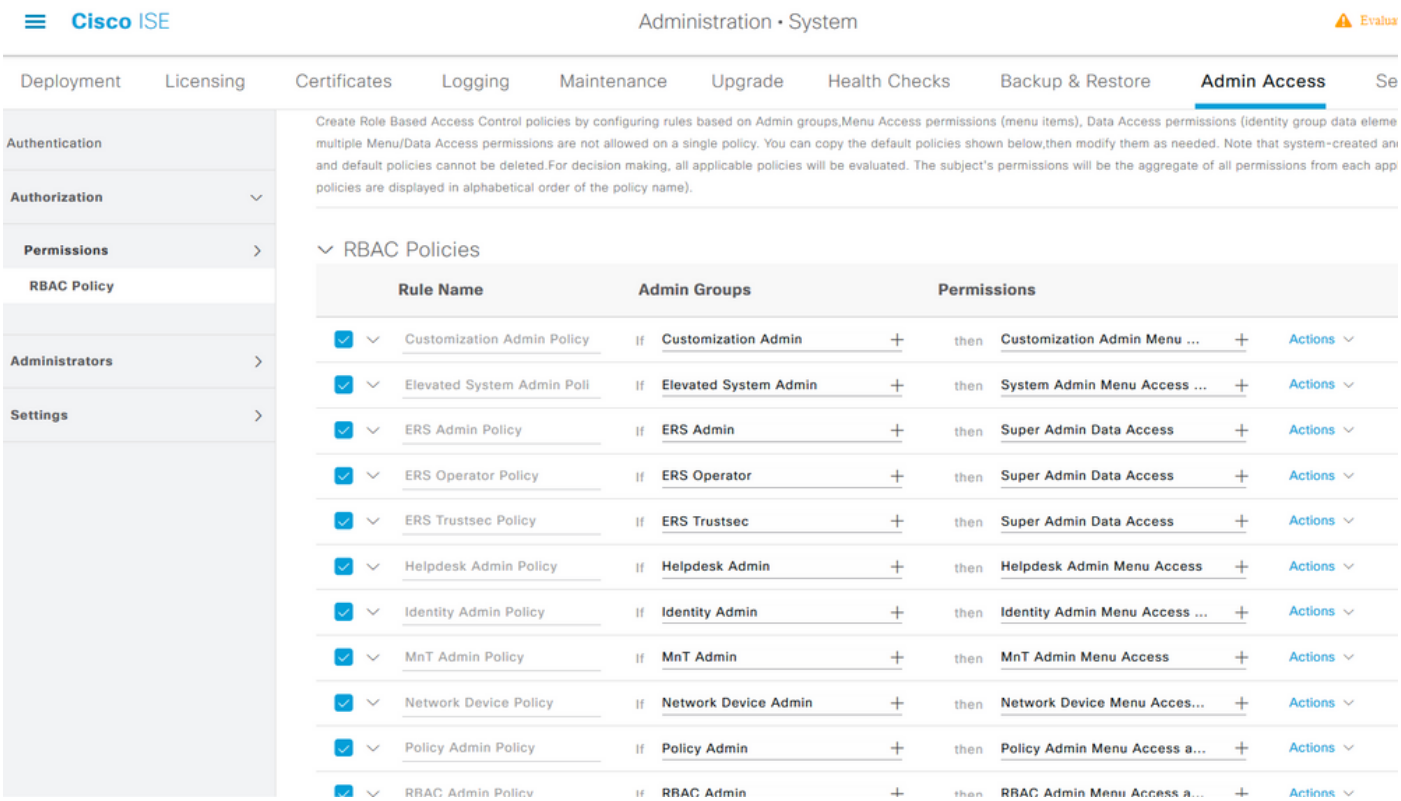


Cliquez sur **Add** pour créer une nouvelle stratégie et configurer les autorisations d'accès aux groupes Admin/User Identity/Endpoint Identity/Network.



Configurer les stratégies RBAC

RBAC est l'acronyme de Role-Based Access Control. Le rôle (groupe d'administration) auquel appartient un utilisateur peut être configuré pour utiliser les stratégies Menu et Accès aux données souhaitées. Plusieurs stratégies RBAC peuvent être configurées pour un seul rôle OU plusieurs rôles peuvent être configurés dans une seule stratégie pour accéder au menu et/ou aux données. Toutes ces stratégies applicables sont évaluées lorsqu'un utilisateur admin tente d'exécuter une action. La décision finale est l'ensemble de toutes les politiques applicables à ce rôle. S'il existe des règles contradictoires qui autorisent et refusent en même temps, la règle d'autorisation remplace la règle de refus. Pour configurer ces stratégies, accédez à **Administration > System > Admin Access > Authorization > RBAC Policy**.



Cliquez sur **Actions** pour dupliquer/Insérer/Supprimer une stratégie.

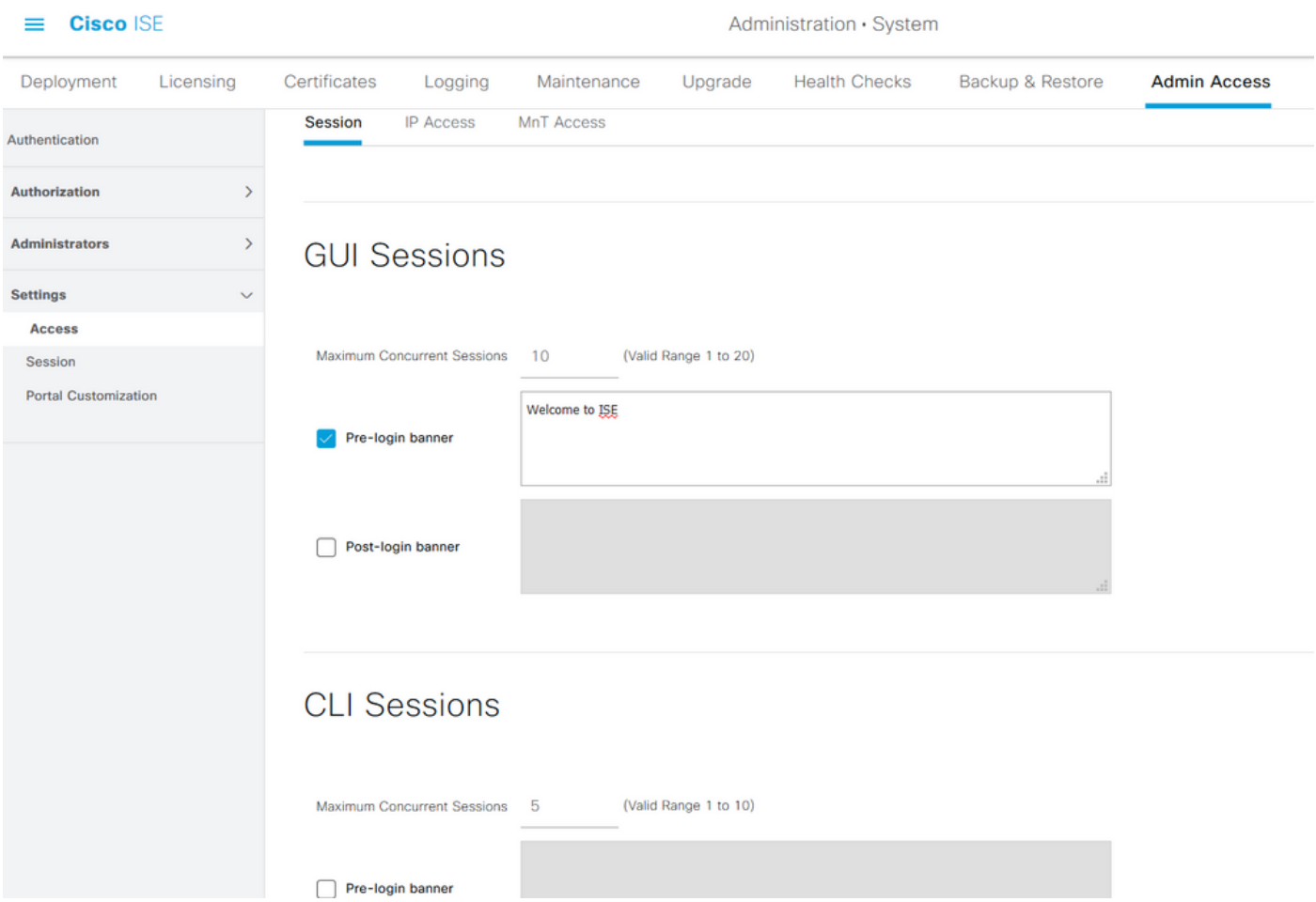
> **Note**: Les stratégies créées par le système et les stratégies par défaut ne peuvent pas être mises à jour et les stratégies par défaut ne peuvent pas être supprimées.

> **Note**: Impossible de configurer plusieurs autorisations d'accès aux menus/données dans une seule règle.

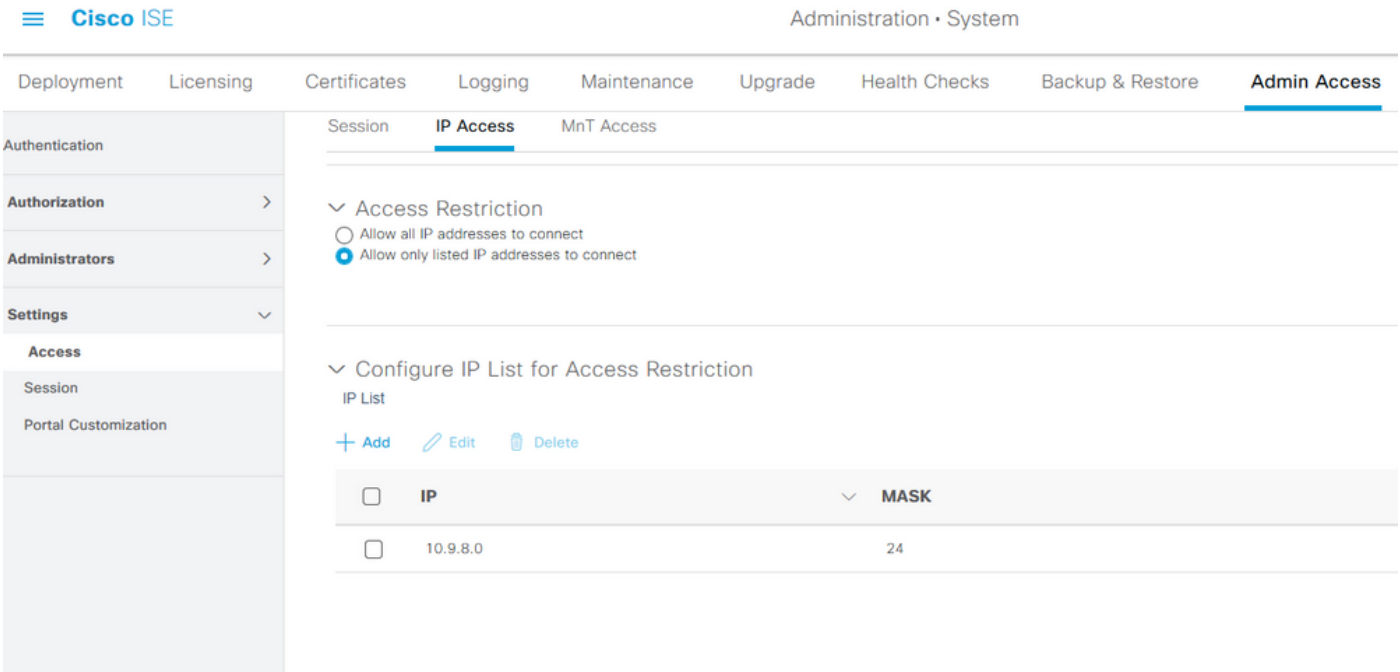
Configuration des paramètres d'accès administrateur

Outre les stratégies RBAC, il existe quelques paramètres qui peuvent être configurés et qui sont communs à tous les utilisateurs admin.

Afin de configurer le nombre maximal de sessions autorisées, de sessions préalables et de bannières postérieures à la connexion pour l'interface utilisateur graphique et l'interface de ligne de commande, accédez à **Administration > System > Admin Access > Settings > Access**. Configurez-les sous l'onglet **Session**.



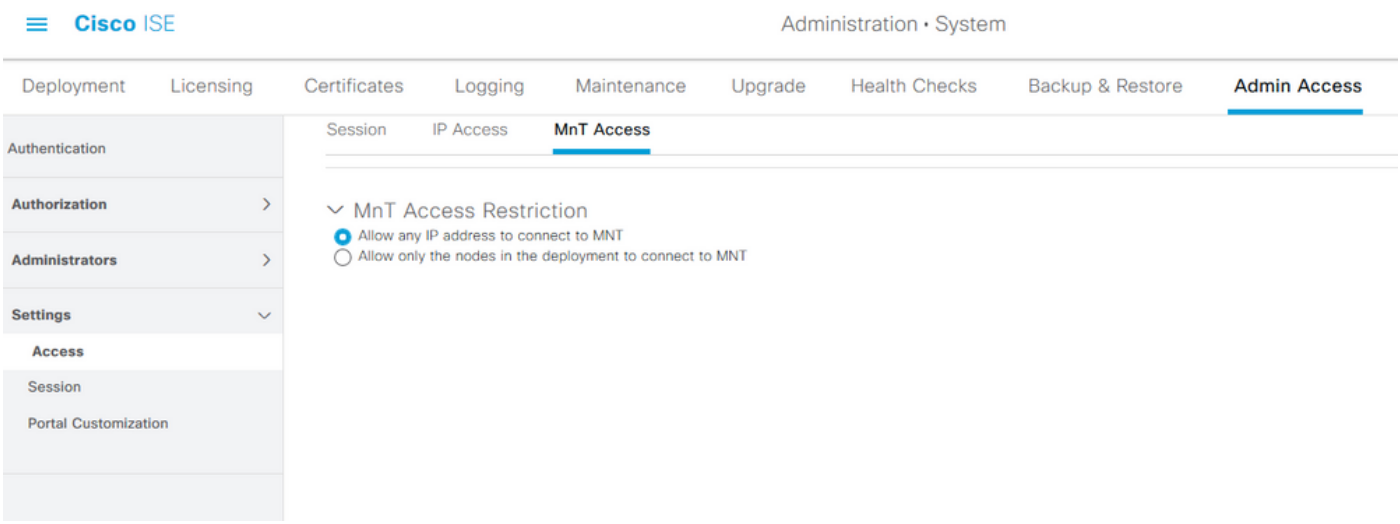
Pour configurer la liste des adresses IP à partir desquelles l'interface utilisateur graphique et l'interface de ligne de commande sont accessibles, accédez à **Administration > System > Admin Access > Settings > Access** et accédez à l'onglet **IP Access**.



Pour configurer une liste de noeuds à partir desquels les administrateurs peuvent accéder à la section MnT de Cisco ISE, accédez à **Administration > System > Admin Access > Settings > Access** et accédez à l'onglet **MnT Access**.

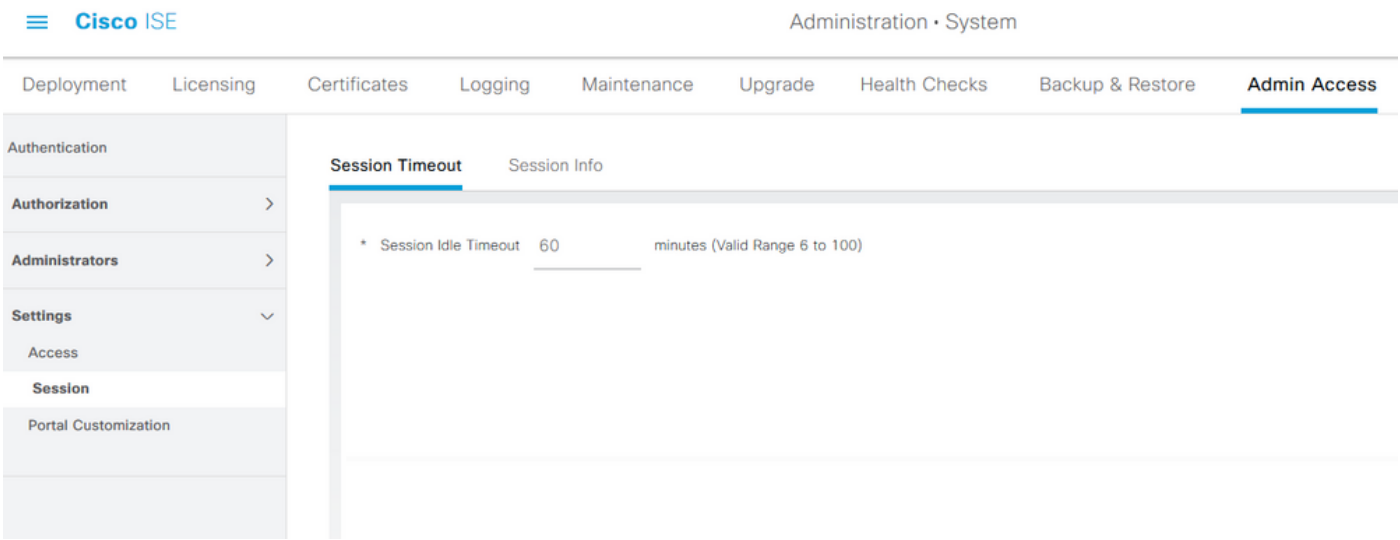
Pour autoriser les noeuds ou les entités du déploiement ou en dehors du déploiement à envoyer

des syslogs à MnT, cliquez sur la case d'option **Autoriser toute adresse IP à se connecter à MNT**. Pour autoriser uniquement les noeuds ou entités du déploiement à envoyer des syslogs à MnT, cliquez sur la case d'option **Autoriser uniquement les noeuds du déploiement à se connecter à MNT**.

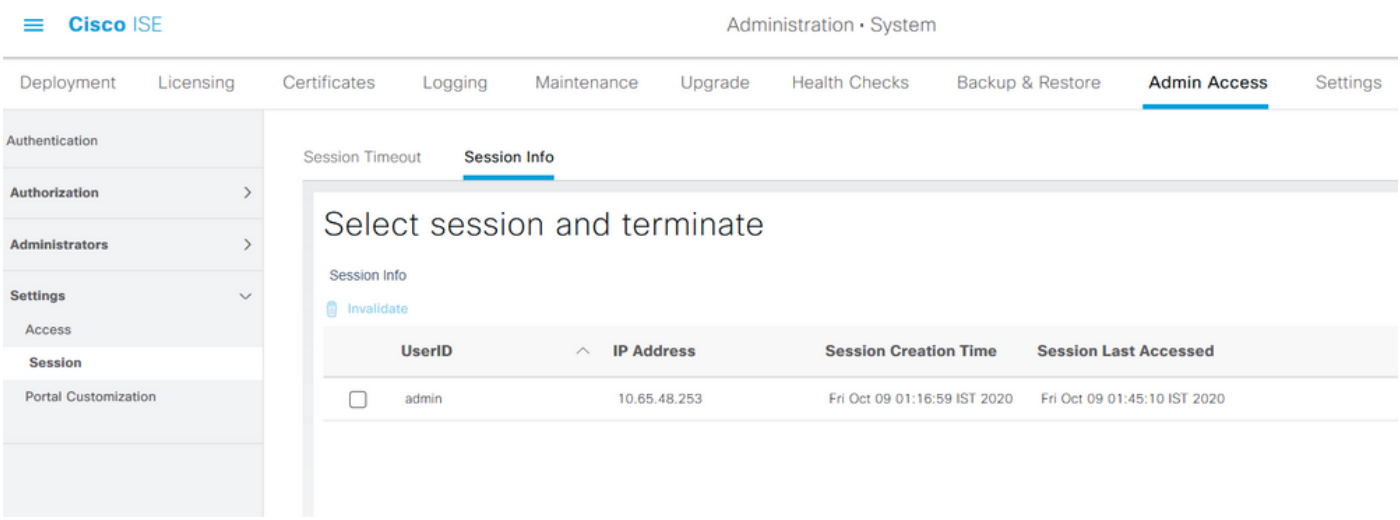


> **Note**: Pour le correctif 2.6 ISE et versions ultérieures, *utilisez « ISE Messaging Service » pour la livraison des Syslogs UDP à MnT* est activée par défaut, ce qui n'autorise pas les Syslogs provenant d'autres entités en dehors du déploiement.

Afin de configurer une valeur de délai d'attente en raison de l'inactivité d'une session, accédez à **Administration > System > Admin Access > Settings > Session**. Définissez cette valeur sous l'onglet **Temporisation de session**.



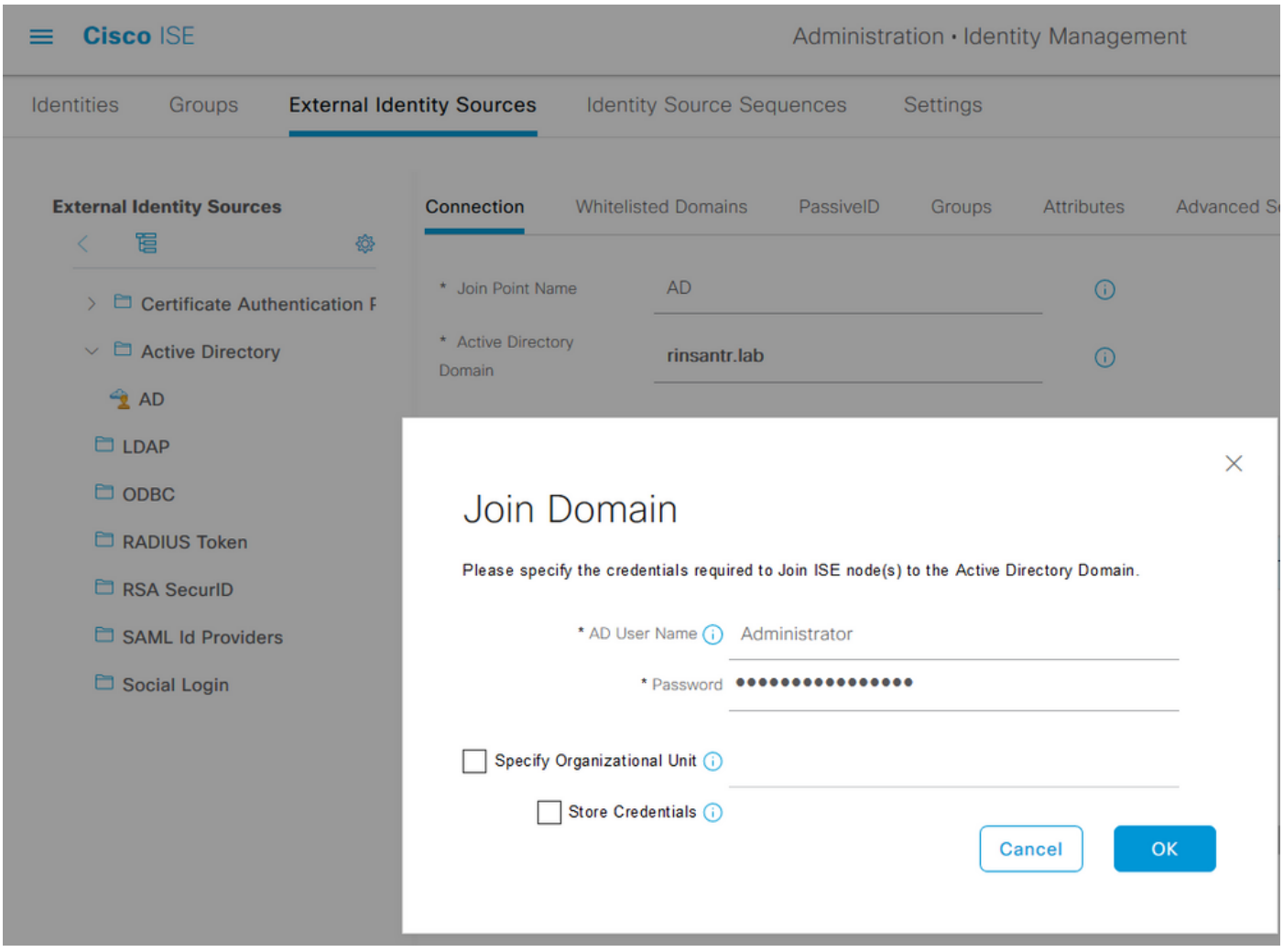
Afin d'afficher/d'invalider les sessions actives en cours, accédez à **Administration > Admin Access > Settings > Session** et cliquez sur l'onglet **Session Info**.

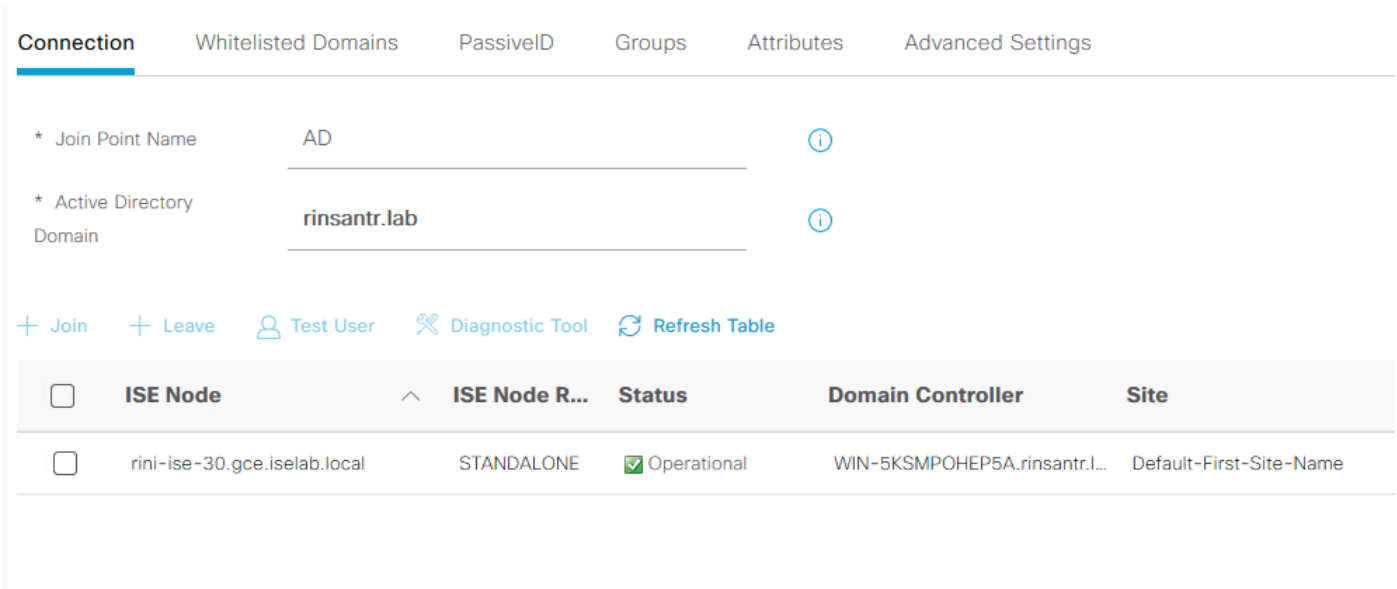


Configurer l'accès au portail Admin avec les informations d'identification AD

Rejoindre ISE à AD

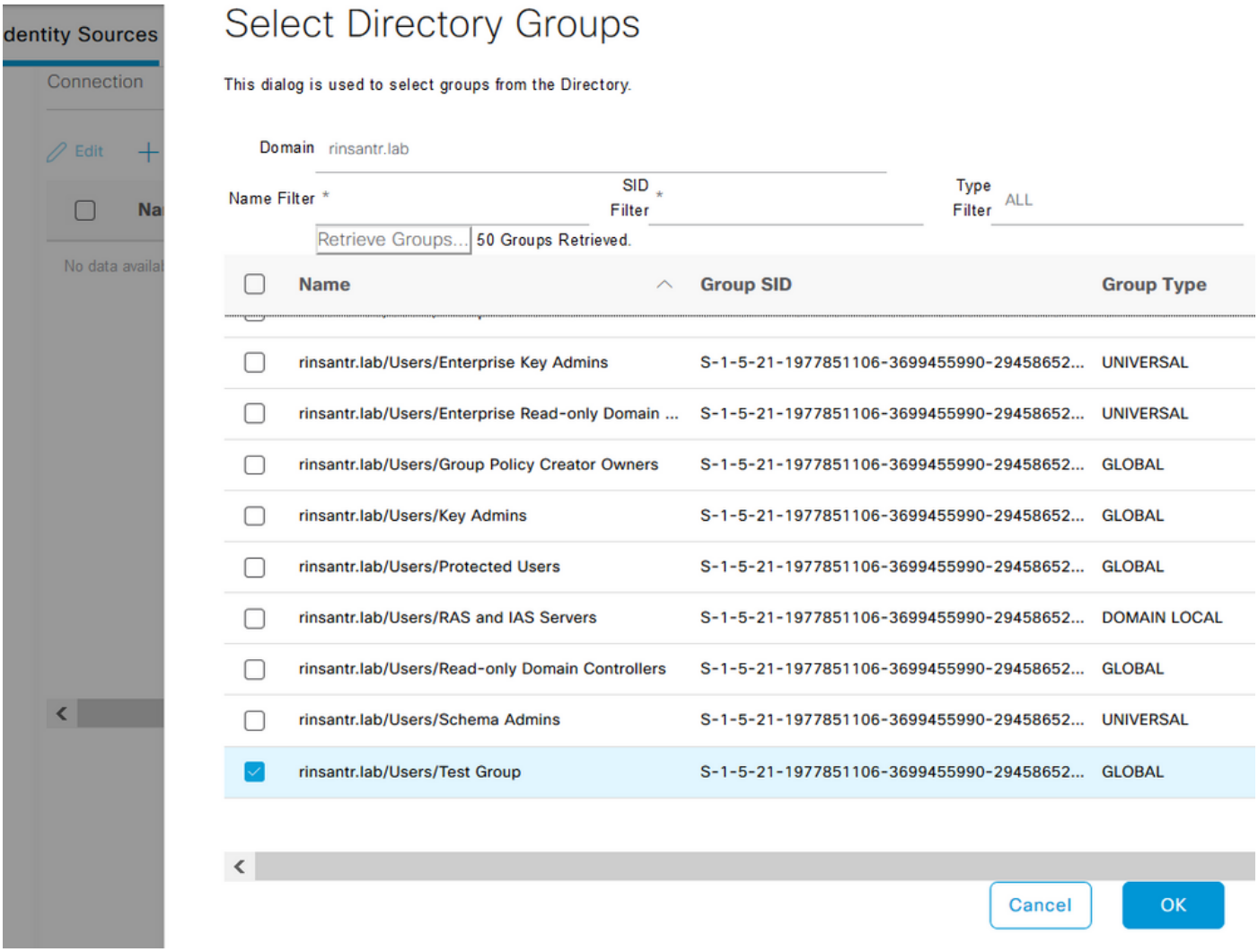
Pour rejoindre ISE à un domaine externe, accédez à **Administration > Identity Management > External Identity Sources > Active Directory**. Entrez le nouveau nom de point de jointure et le domaine Active Directory. Entrez les informations d'identification du compte AD qui peut ajouter et apporter des modifications aux objets de l'ordinateur, puis cliquez sur **OK**.

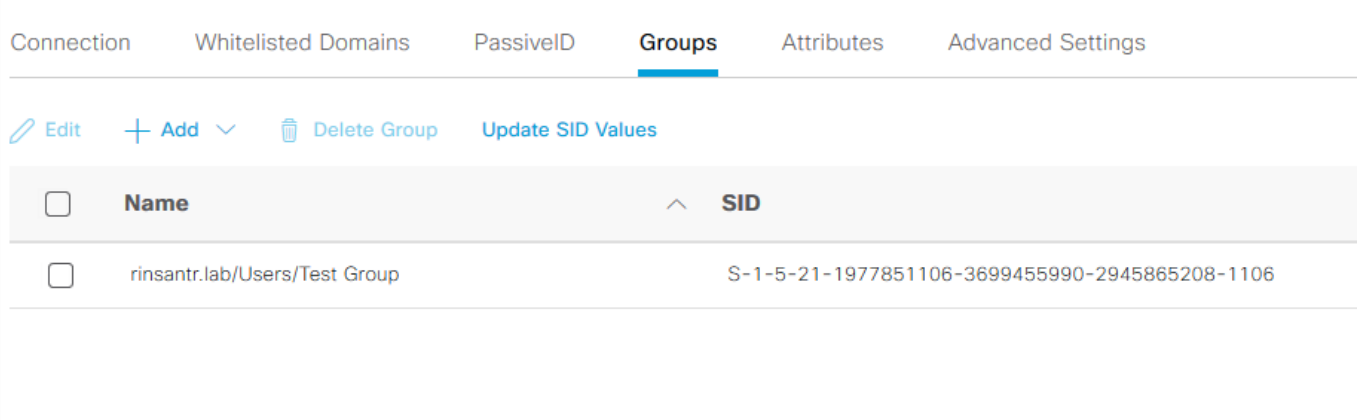




Sélectionner des groupes de répertoires

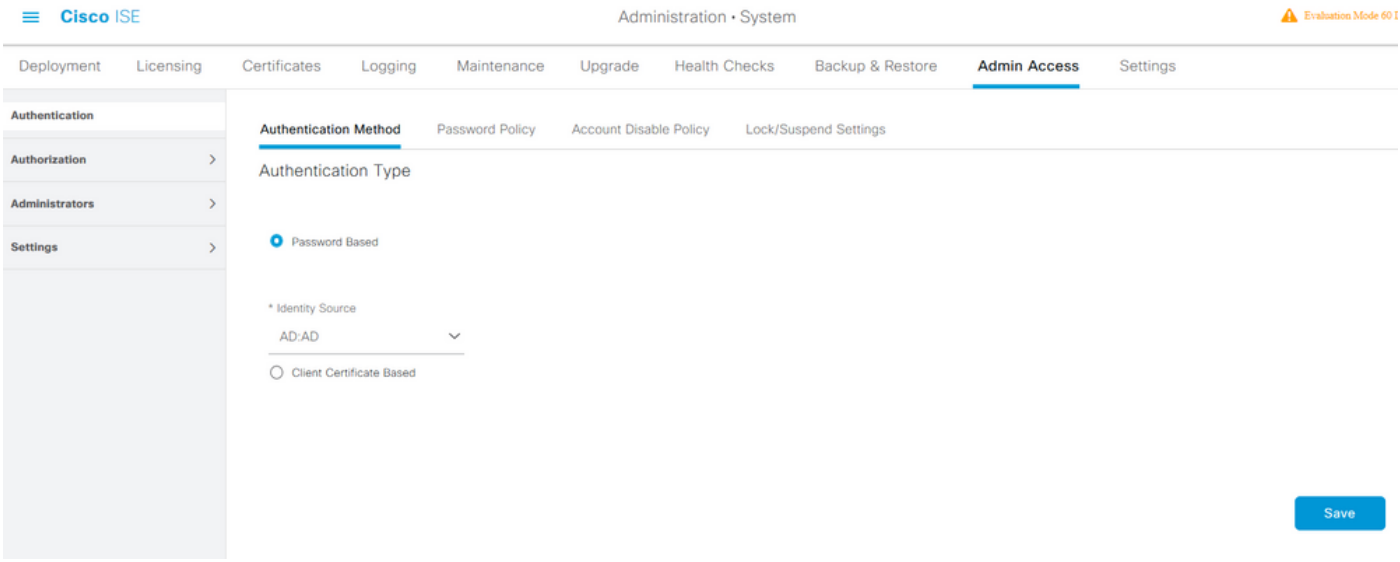
Accédez à **Administration > Identity Management > External Identity Sources > Active Directory**. Cliquez sur le nom du point de jointure souhaité et accédez à l'onglet **Groupes**. Cliquez sur **Add > Select Groups from Directory > Retrieve Groups**. Importez au moins un groupe AD auquel votre administrateur appartient, puis cliquez sur **OK**, puis sur **Enregistrer**.





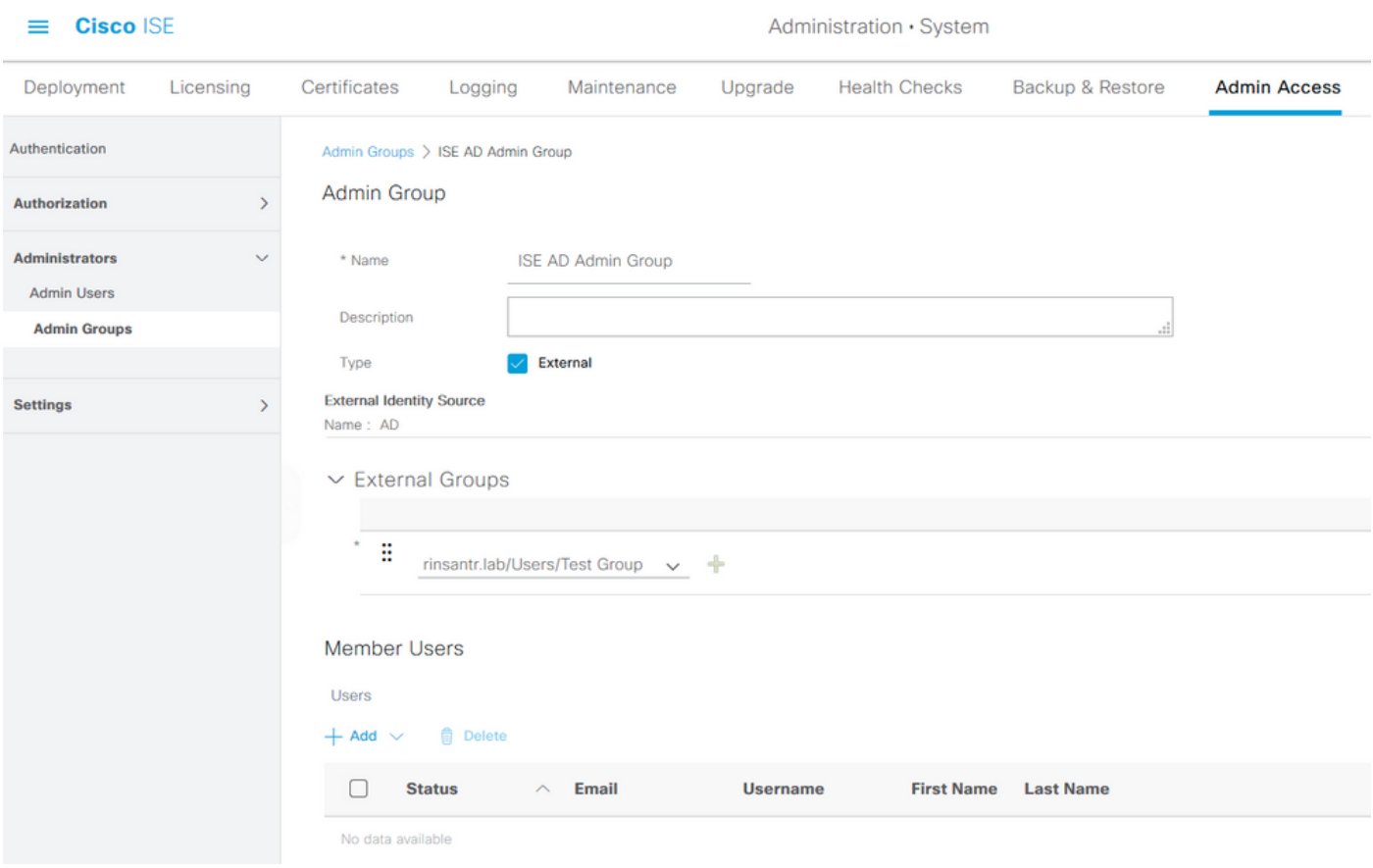
Activer l'accès administratif pour AD

Afin d'activer l'authentification basée sur un mot de passe d'ISE à l'aide d'AD, accédez à **Administration> System > Admin Access > Authentication**. Dans l'onglet **Authentication Method**, sélectionnez l'option **Password-Based**. Sélectionnez **AD** dans le menu déroulant **Source d'identité** et cliquez sur **Enregistrer**.



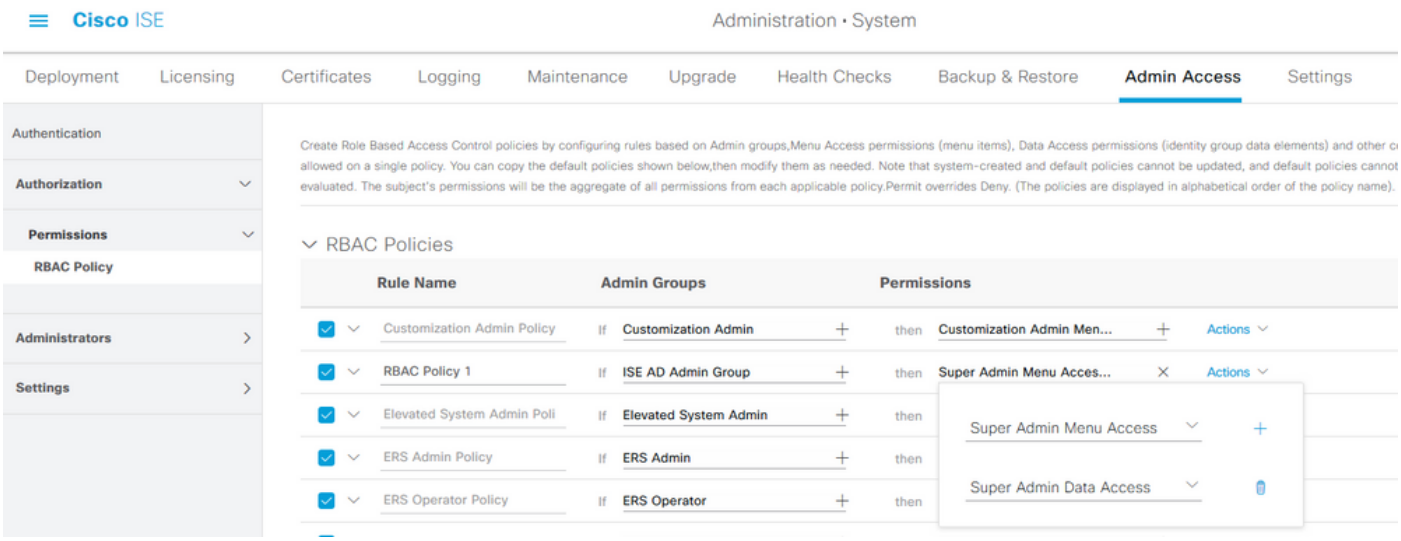
Configurer le mappage du groupe d'administration ISE sur le groupe AD

Cela permet d'autoriser la détermination des autorisations RBAC (Role Based Access Control) pour l'administrateur en fonction de l'appartenance au groupe dans AD. Pour définir un groupe d'administrateurs Cisco ISE et le mapper à un groupe AD, accédez à **Administration > System > Admin Access > Administrators > Admin Groups**. Cliquez sur **Add** et saisissez un nom pour le nouveau groupe Admin. Dans le champ Type, cochez la case **Externe**. Dans le menu déroulant **Groupes externes**, sélectionnez le groupe AD auquel ce groupe d'administration doit être mappé (tel que défini dans la section Sélectionner les groupes de répertoires ci-dessus). **Soumettez** les modifications.



Définir les autorisations RBAC pour le groupe Admin

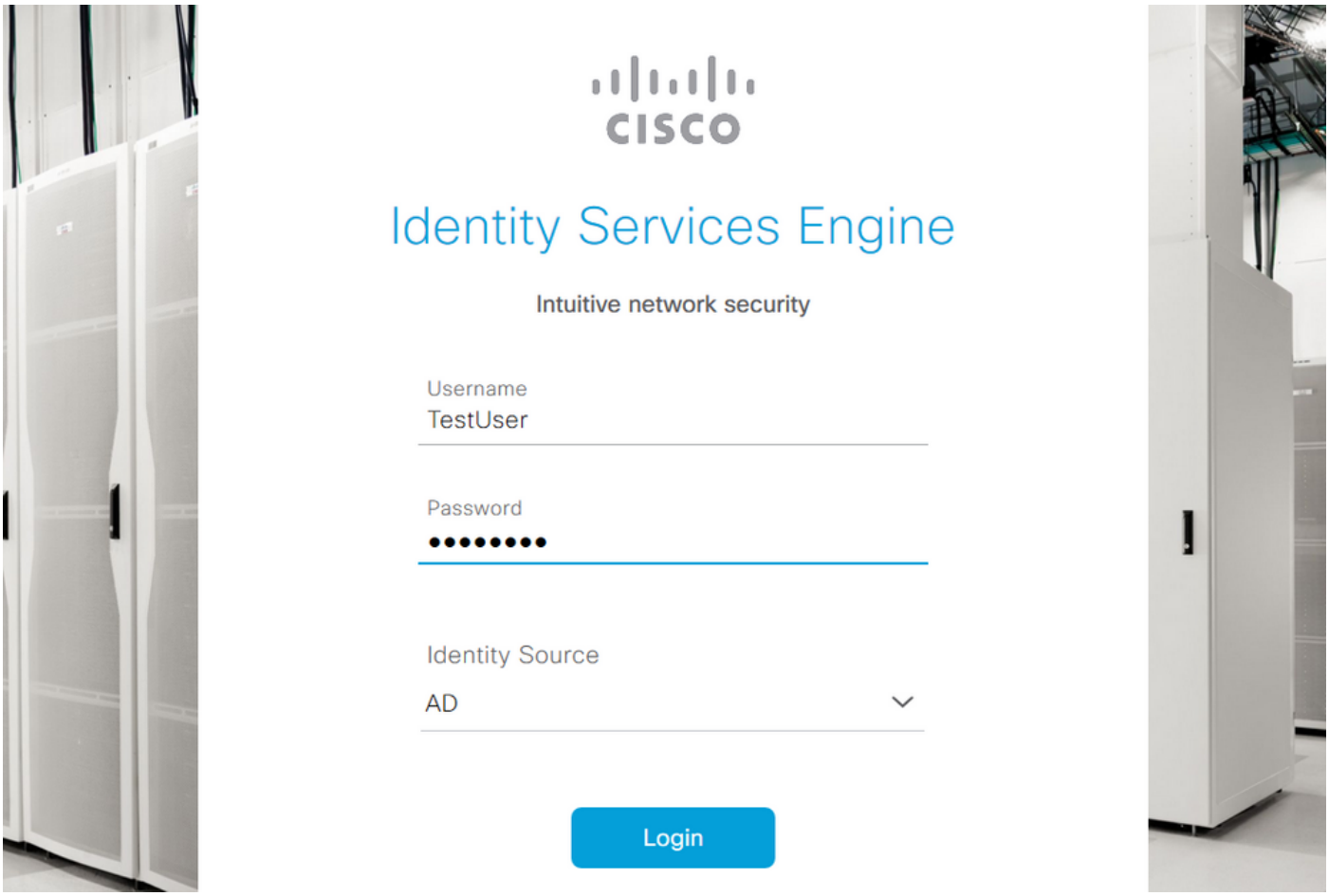
Pour attribuer des autorisations RBAC au groupe d'administration créé dans la section précédente, accédez à **Administration > System > Admin Access > Authorization > RBAC Policy**. Dans le menu déroulant **Actions** à droite, sélectionnez **Insérer une nouvelle stratégie**. Créez une nouvelle règle, mappez-la avec le groupe d'administrateurs défini dans la section ci-dessus, puis affectez-la avec les autorisations d'accès aux données et au menu souhaitées, puis cliquez sur **Enregistrer**.



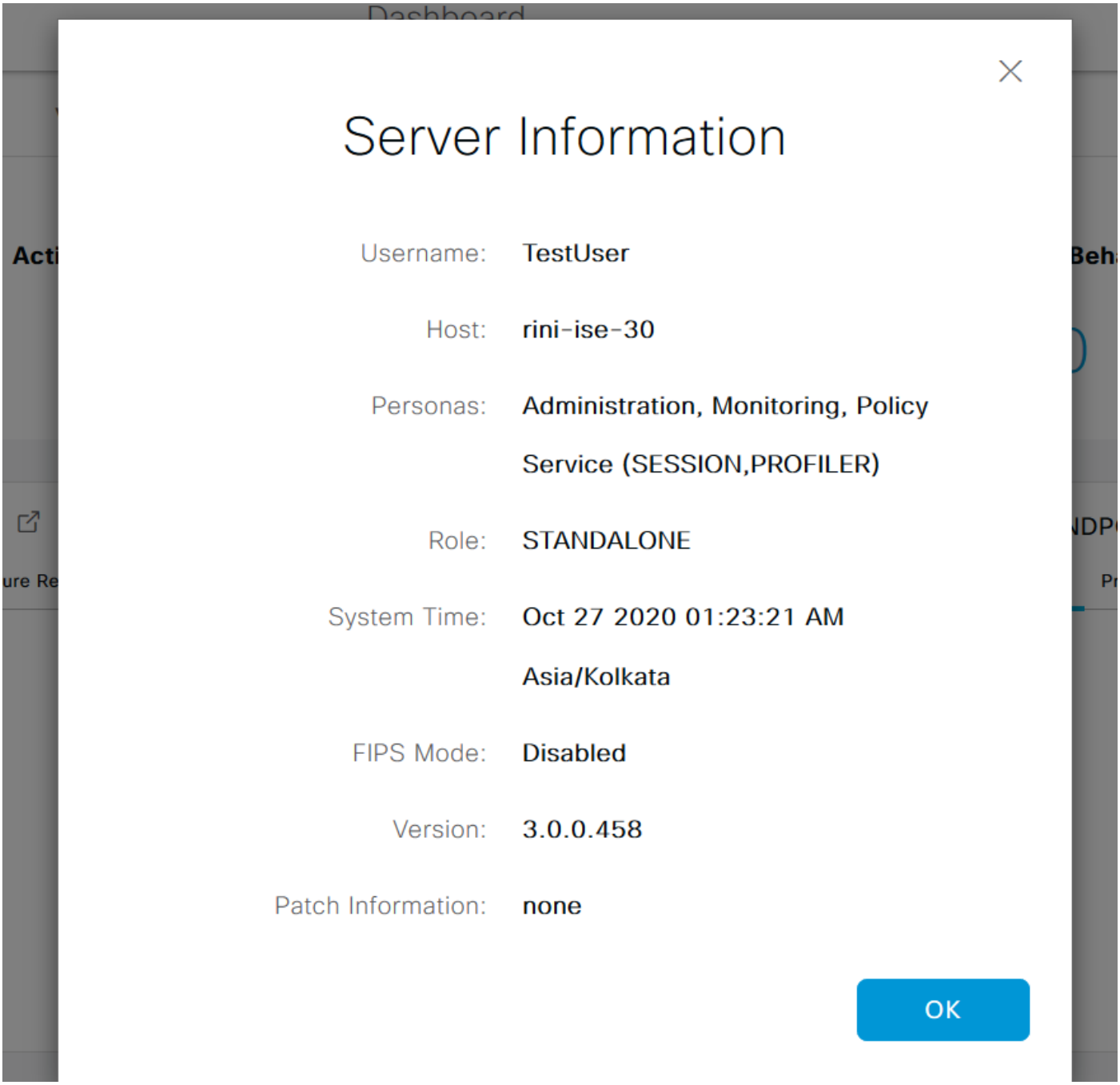
Accéder à ISE avec les identifiants AD et vérifier

Déconnectez-vous de l'interface utilisateur graphique d'administration. Sélectionnez le nom du point de jointure dans le menu déroulant **Source d'identité**. Saisissez le nom d'utilisateur et le mot

de passe de la base de données AD, puis connectez-vous.



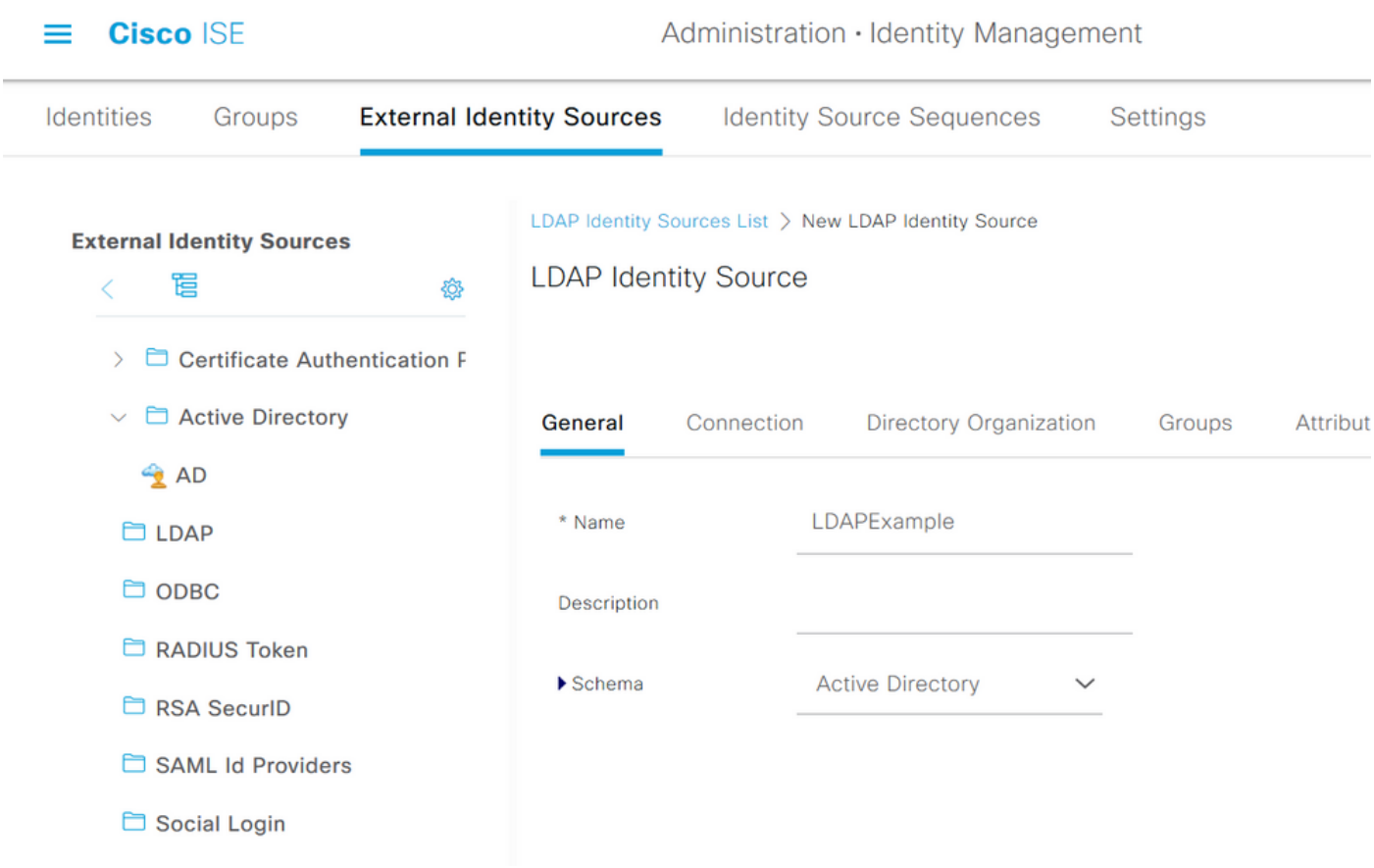
Pour vérifier que la configuration fonctionne correctement, vérifiez le nom d'utilisateur authentifié à partir de l'icône **Paramètres** dans le coin supérieur droit de l'interface utilisateur graphique ISE. Accédez à **Informations sur le serveur** et vérifiez le nom d'utilisateur.



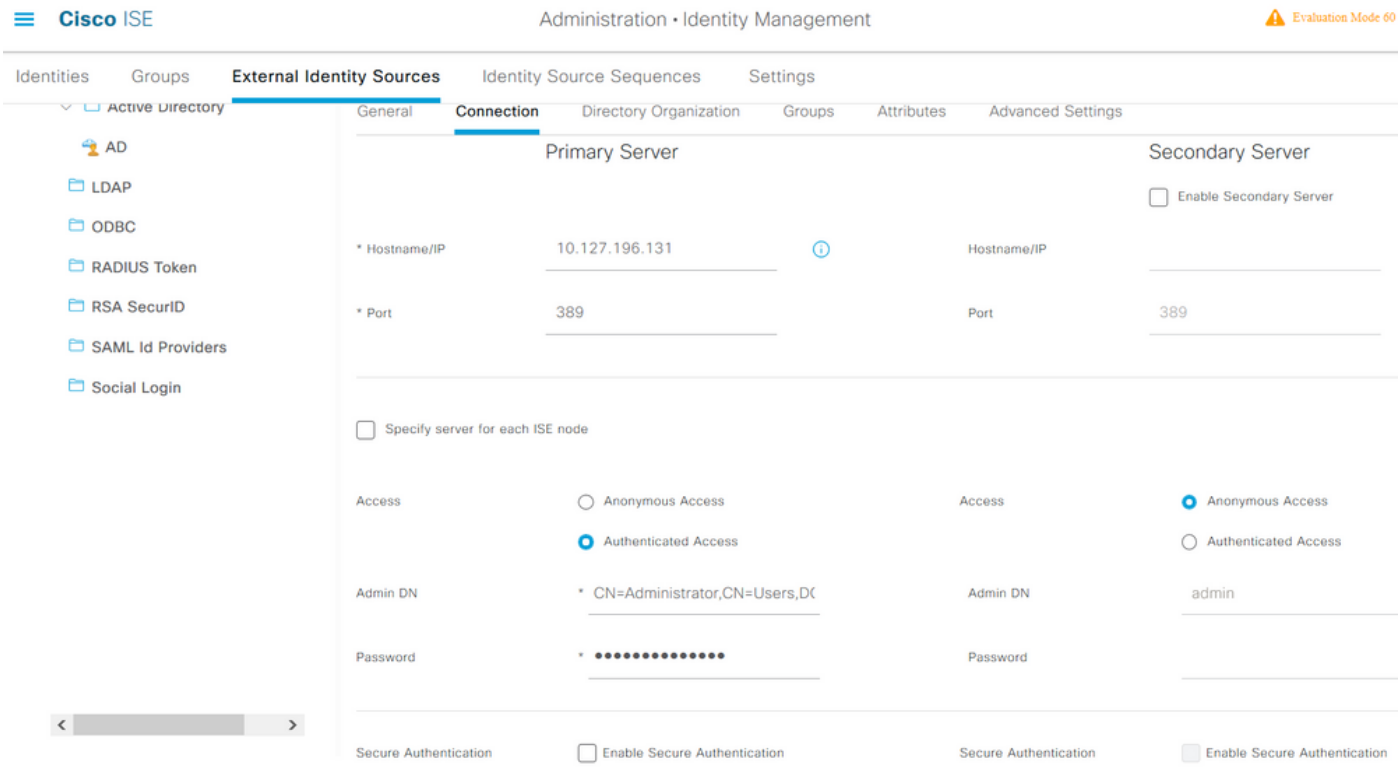
Configurer l'accès au portail Admin avec LDAP

Rejoindre ISE à LDAP

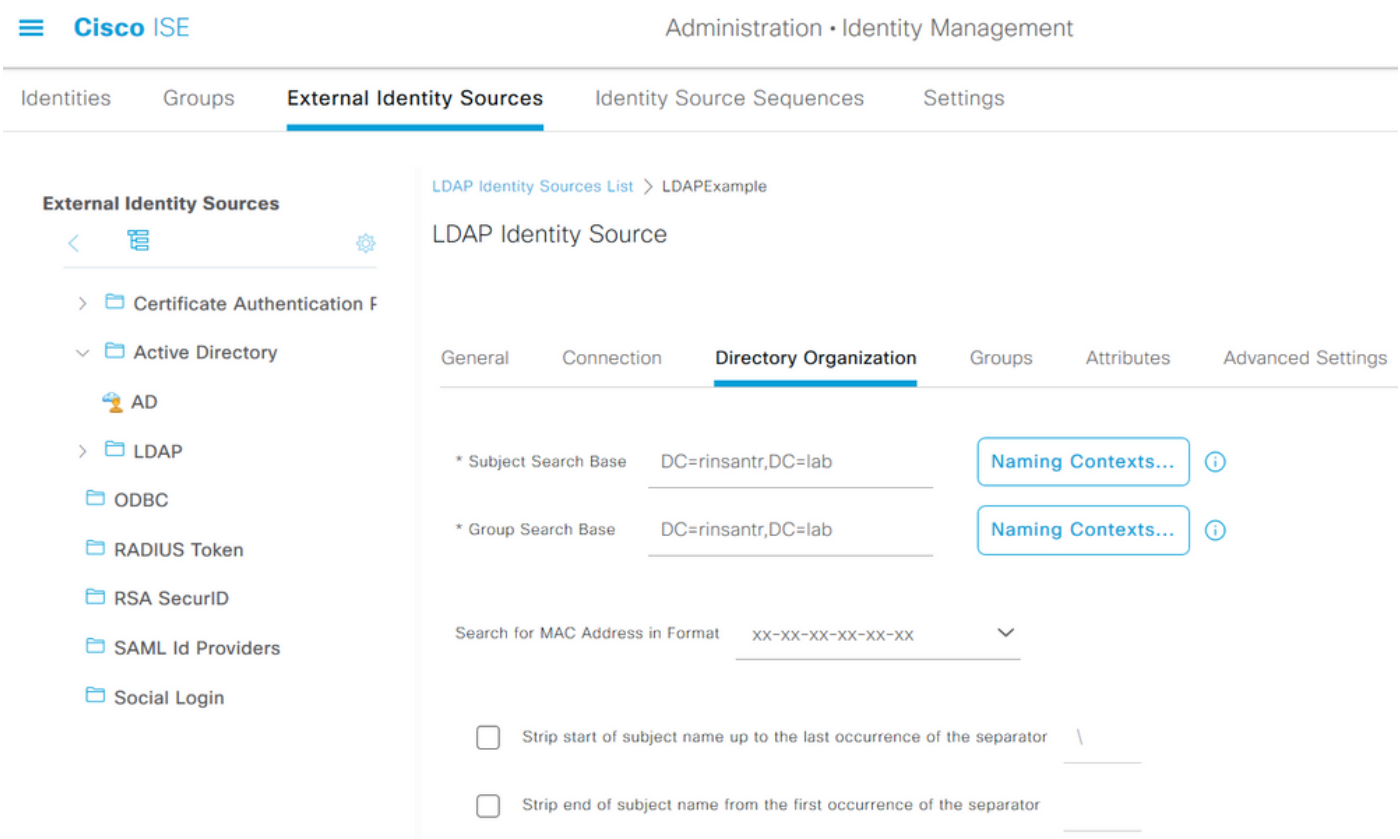
Accédez à **Administration > Identity Management > External Identity Sources > Active Directory > LDAP**. Sous l'onglet **Général**, entrez un nom pour LDAP et choisissez le schéma en tant qu'**Active Directory**.



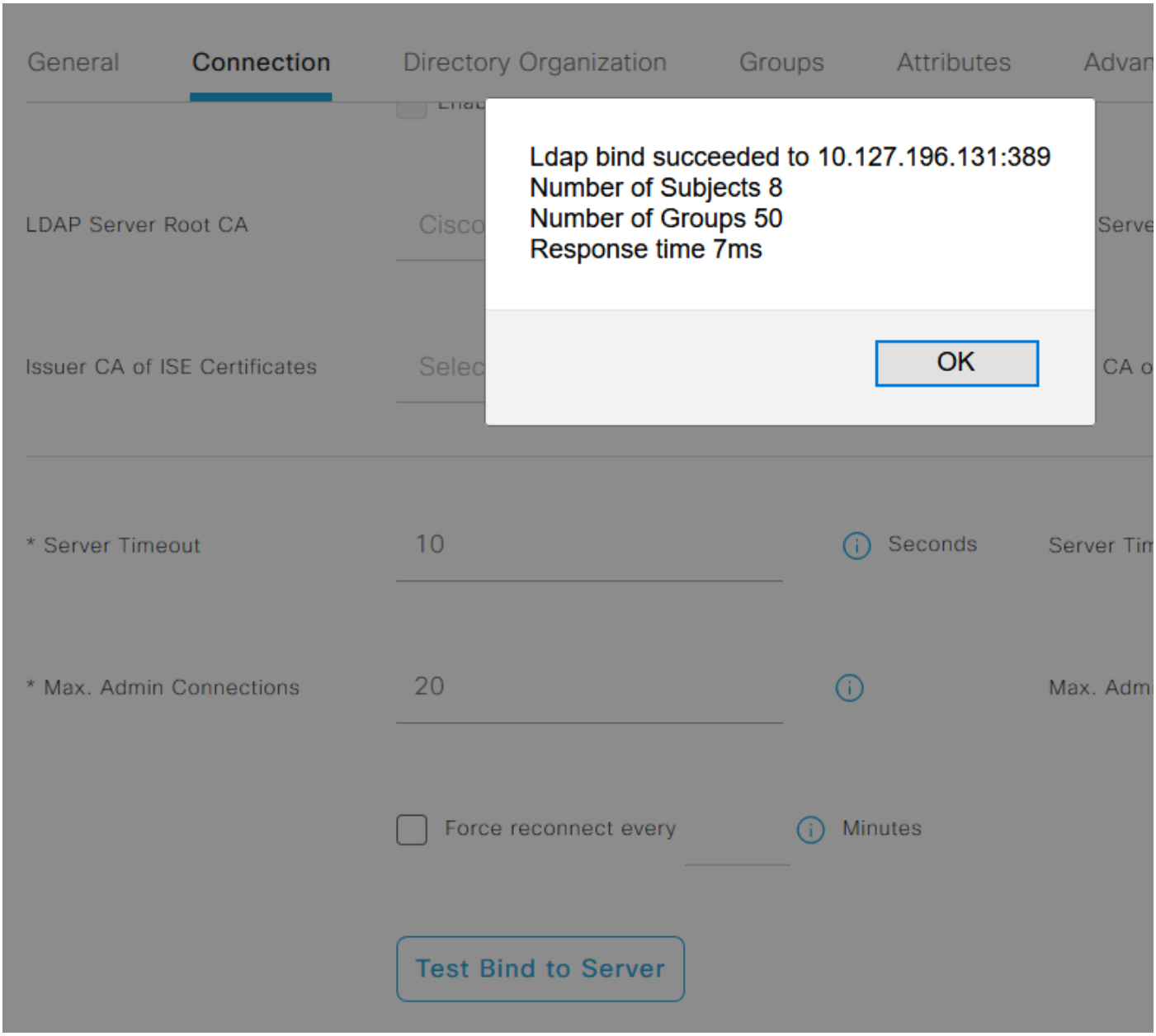
Ensuite, pour configurer le type de connexion, accédez à l'onglet **Connexion**. Définissez ici le nom d'hôte/l'adresse IP du serveur LDAP principal avec le port 389(LDAP)/636 (LDAP-Secure). Entrez le chemin d'accès du nom unique d'administrateur (DN) avec le mot de passe d'administrateur du serveur LDAP.



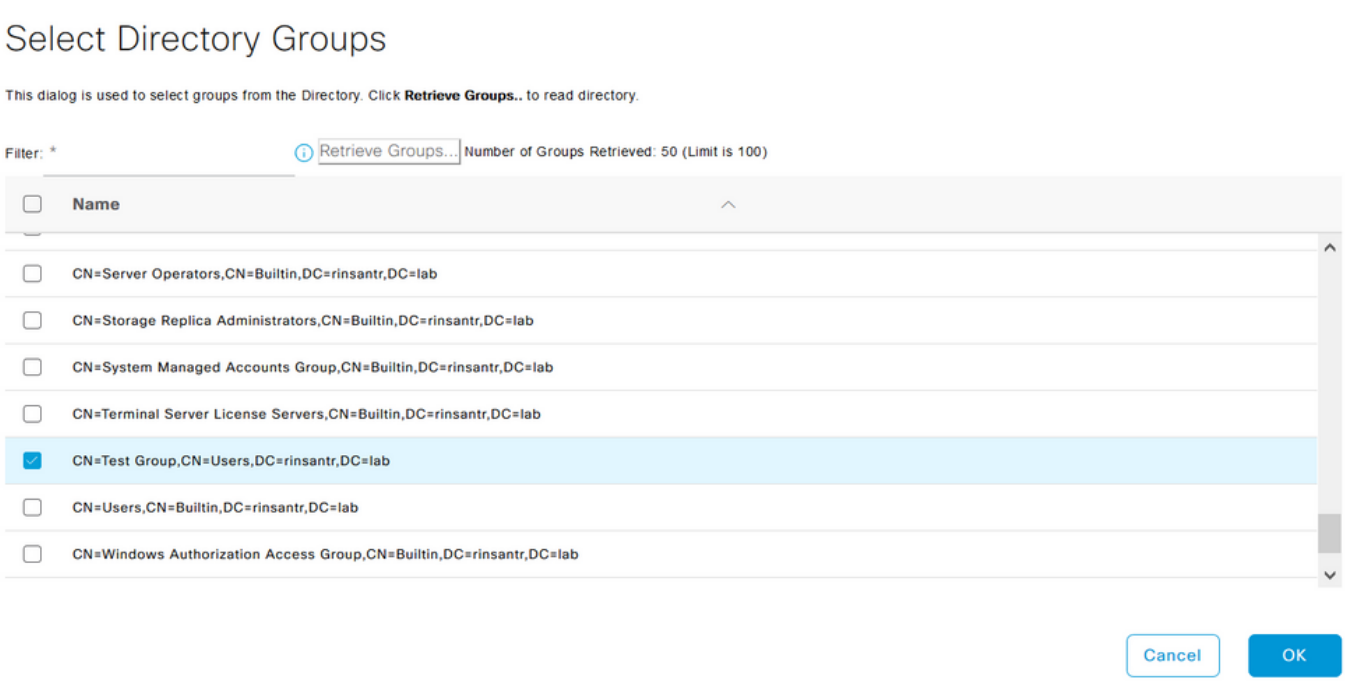
Ensuite, accédez à l'onglet **Organisation du répertoire** et cliquez sur **Contextes de noms** pour choisir le groupe d'organisations correct de l'utilisateur en fonction de la hiérarchie des utilisateurs stockés dans le serveur LDAP.

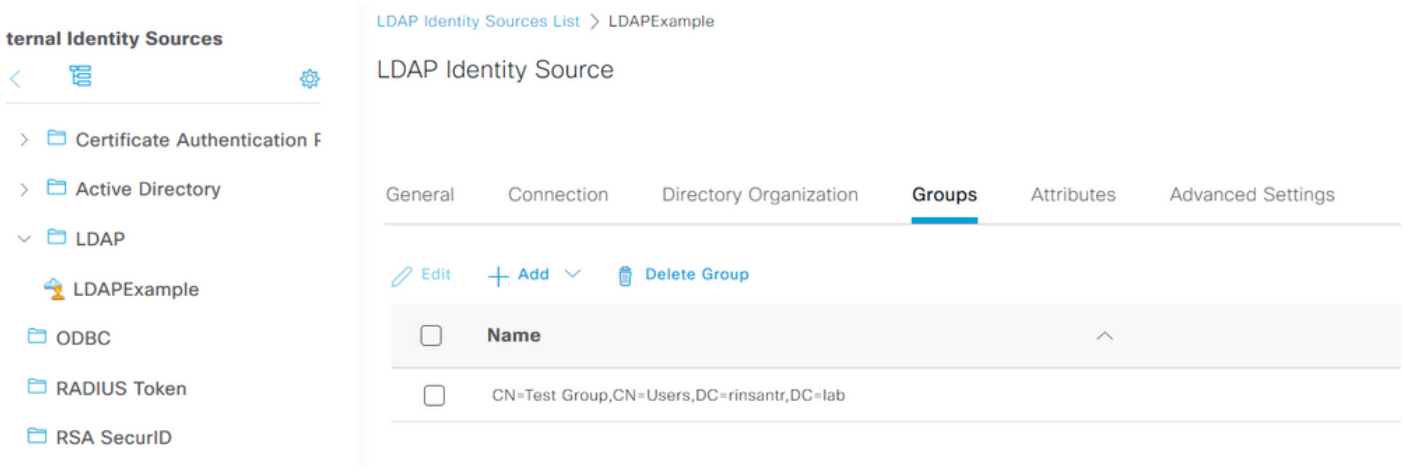


Cliquez sur **Test Bind to Server** sous l'onglet **Connection** pour tester l'accessibilité du serveur LDAP à partir d'ISE.



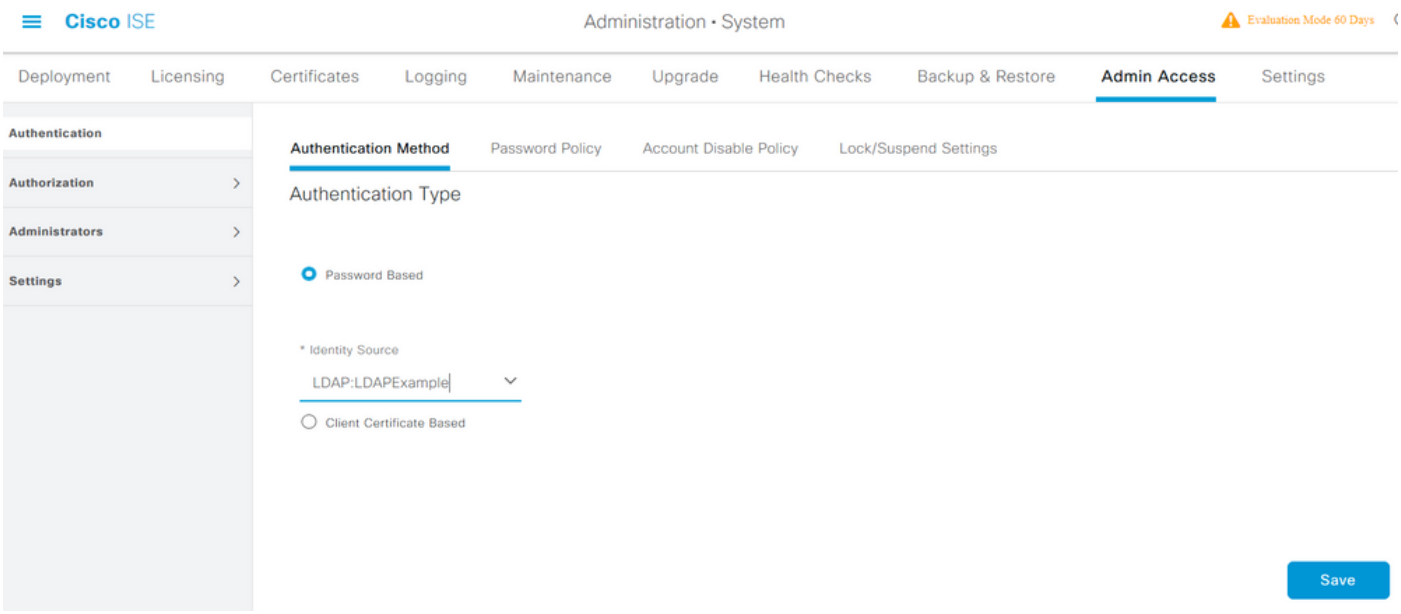
Accédez maintenant à l'onglet **Groupes** et cliquez sur **Ajouter > Sélectionner des groupes dans le répertoire > Récupérer des groupes**. Importez au moins un groupe auquel votre administrateur appartient, puis cliquez sur **OK**, puis sur **Enregistrer**.





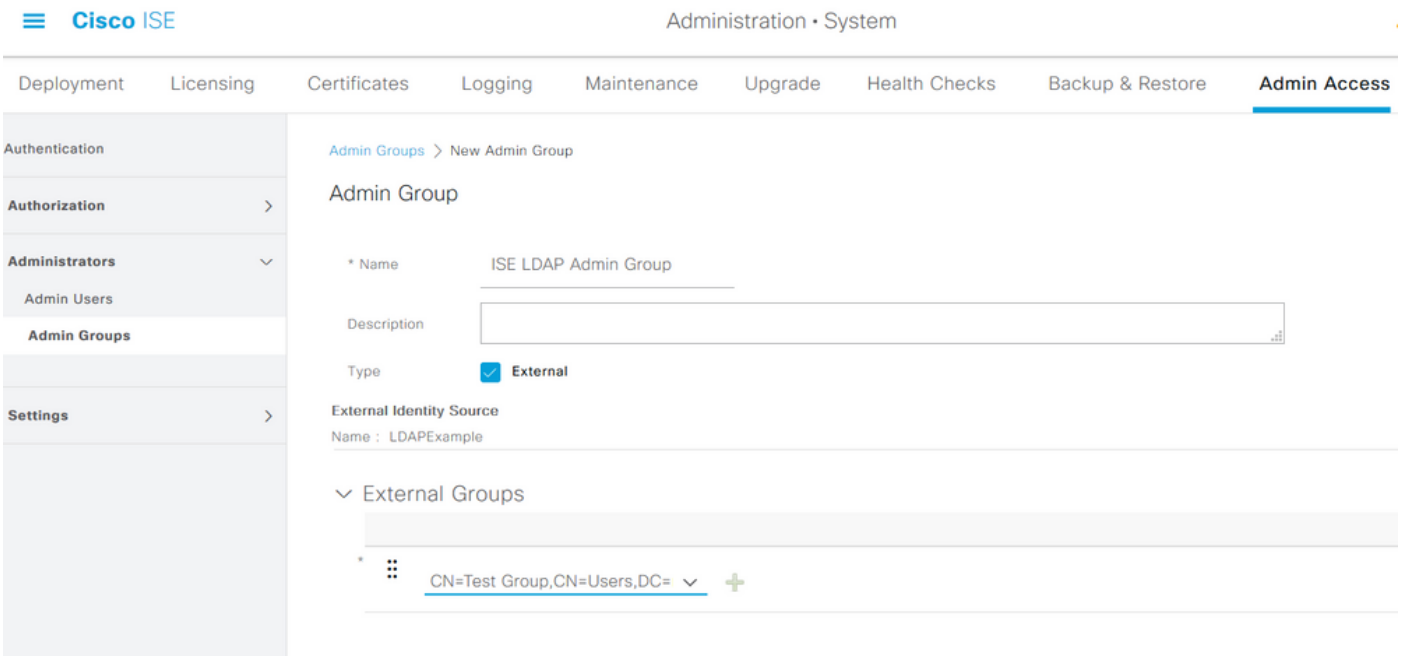
Activer l'accès administratif pour les utilisateurs LDAP

Afin d'activer l'authentification basée sur un mot de passe d'ISE à l'aide de LDAP, accédez à **Administration > System > Admin Access > Authentication**. Dans l'onglet **Authentication Method**, sélectionnez l'option **Password-Based**. Sélectionnez **LDAP** dans le menu déroulant **Source d'identité** et cliquez sur **Enregistrer**.



Mapper le groupe d'administration ISE au groupe LDAP

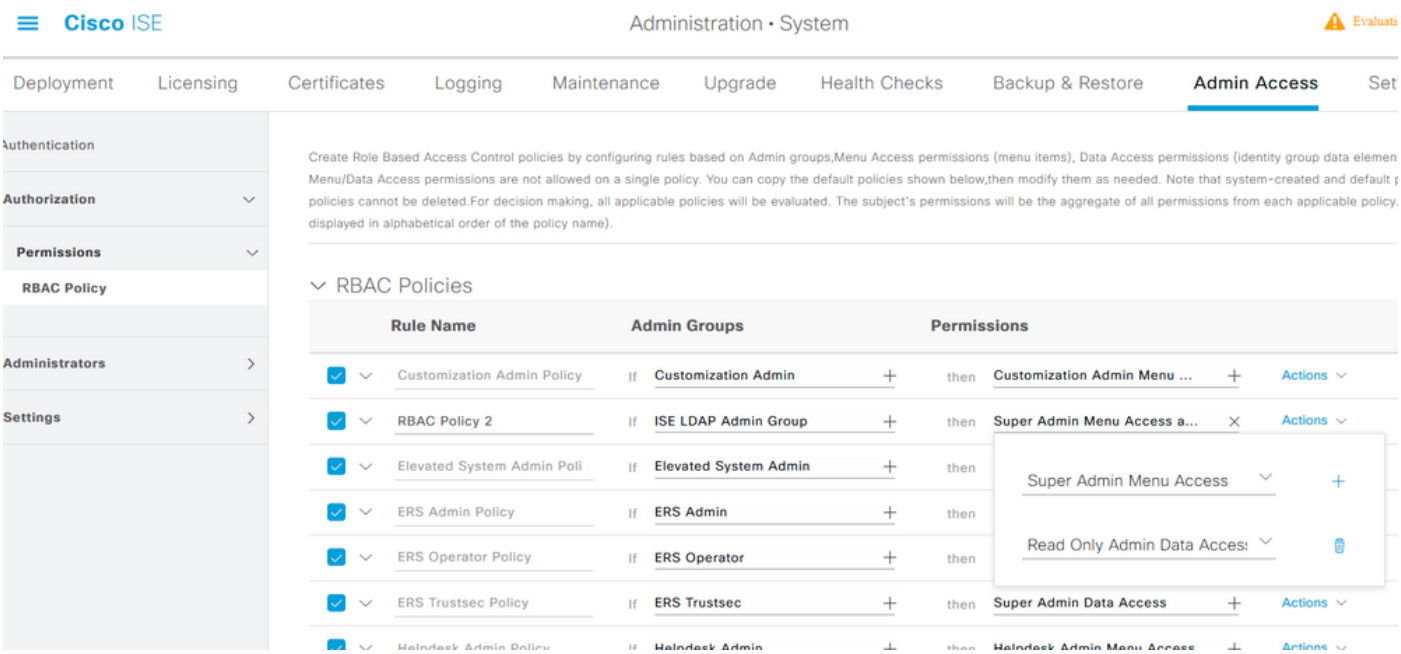
Cela permet à l'utilisateur configuré d'obtenir l'accès Administrateur en fonction de l'autorisation des stratégies RBAC, qui à son tour est basé sur l'appartenance au groupe LDAP de l'utilisateur. Pour définir un groupe d'administrateurs Cisco ISE et le mapper à un groupe LDAP, accédez à **Administration > System > Admin Access > Administrators > Admin Groups**. Cliquez sur **Add** et saisissez un nom pour le nouveau groupe Admin. Dans le champ Type, cochez la case **Externe**. Dans le menu déroulant **Groupes externes**, sélectionnez le groupe LDAP auquel ce groupe d'administration doit être mappé (tel que récupéré et défini précédemment). **Soumettez** les modifications.



Définir les autorisations RBAC pour le groupe Admin

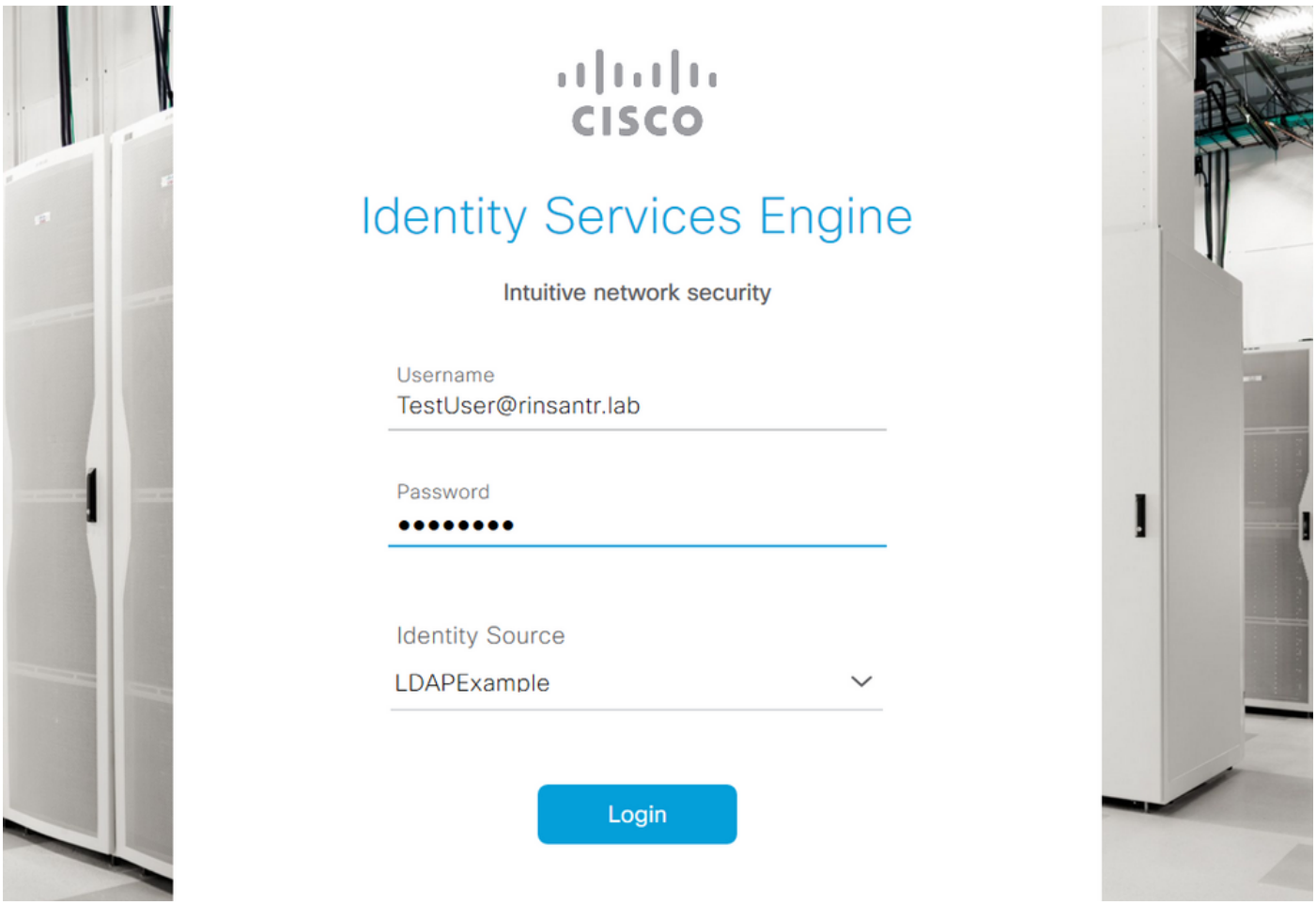
Pour attribuer des autorisations RBAC au groupe d'administration créé dans la section précédente, accédez à **Administration > System > Admin Access > Authorization > RBAC Policy**. Dans le menu déroulant **Actions** à droite, sélectionnez **Insérer une nouvelle stratégie**. Créez une nouvelle règle, mappez-la avec le groupe d'administrateurs défini dans la section ci-dessus, puis

affectez-la avec les autorisations d'accès aux données et au menu souhaitées, puis cliquez sur **Enregistrer**.



Accéder à ISE avec les informations d'identification LDAP et vérifier

Déconnectez-vous de l'interface utilisateur graphique d'administration. Sélectionnez le nom LDAP dans le menu déroulant **Source d'identité**. Saisissez le nom d'utilisateur et le mot de passe de la base de données LDAP, puis connectez-vous.



Afin de vérifier que la configuration fonctionne correctement, vérifiez le nom d'utilisateur authentifié à partir de l'icône **Paramètres** dans le coin supérieur droit de l'interface utilisateur graphique ISE. Accédez à **Informations sur le serveur** et vérifiez le nom d'utilisateur.