Richtlinien für Administratorzugriff und RBAC auf der ISE verstehen

Inhalt

Einführung

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

Voraussetzungen

Anforderungen

Cisco empfiehlt, über die folgenden Themen zu verfügen:

- ISE
- Active Directory

- Lightweight Directory Access Protocol (LDAP)

Verwendete Komponenten

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

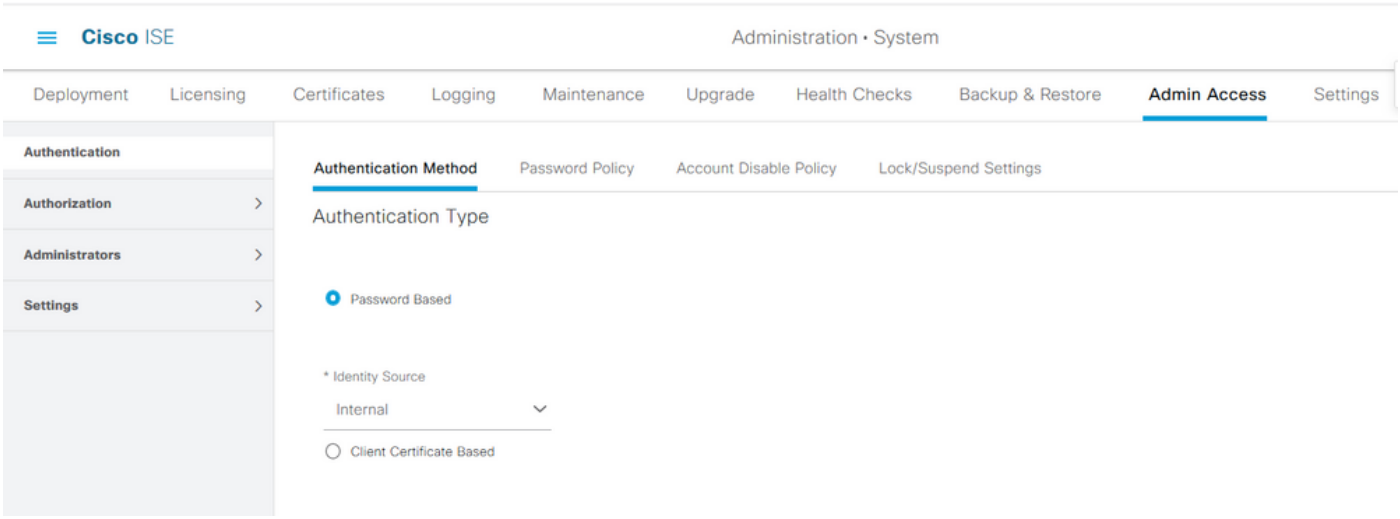
- Identity Services Engine 3.0
- Windows Server 2016

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

Konfigurieren

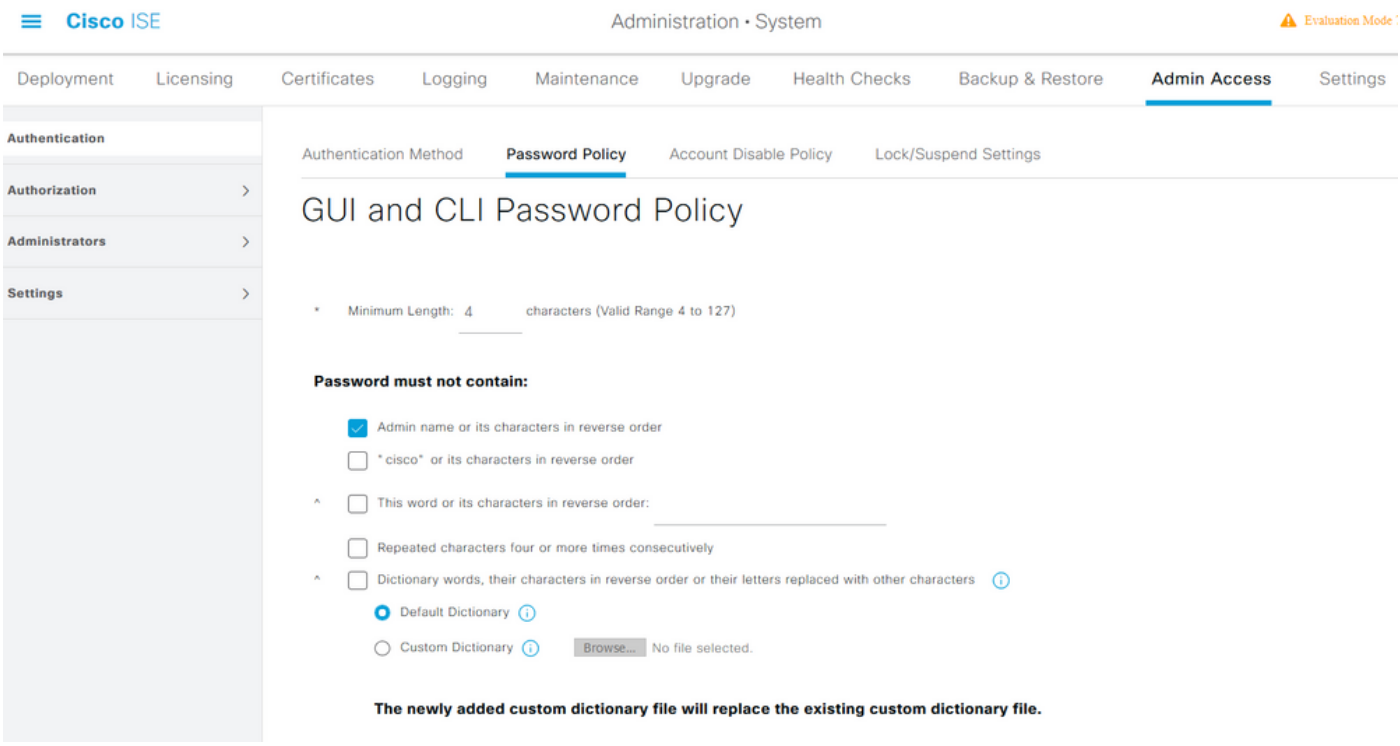
Authentifizierungseinstellungen

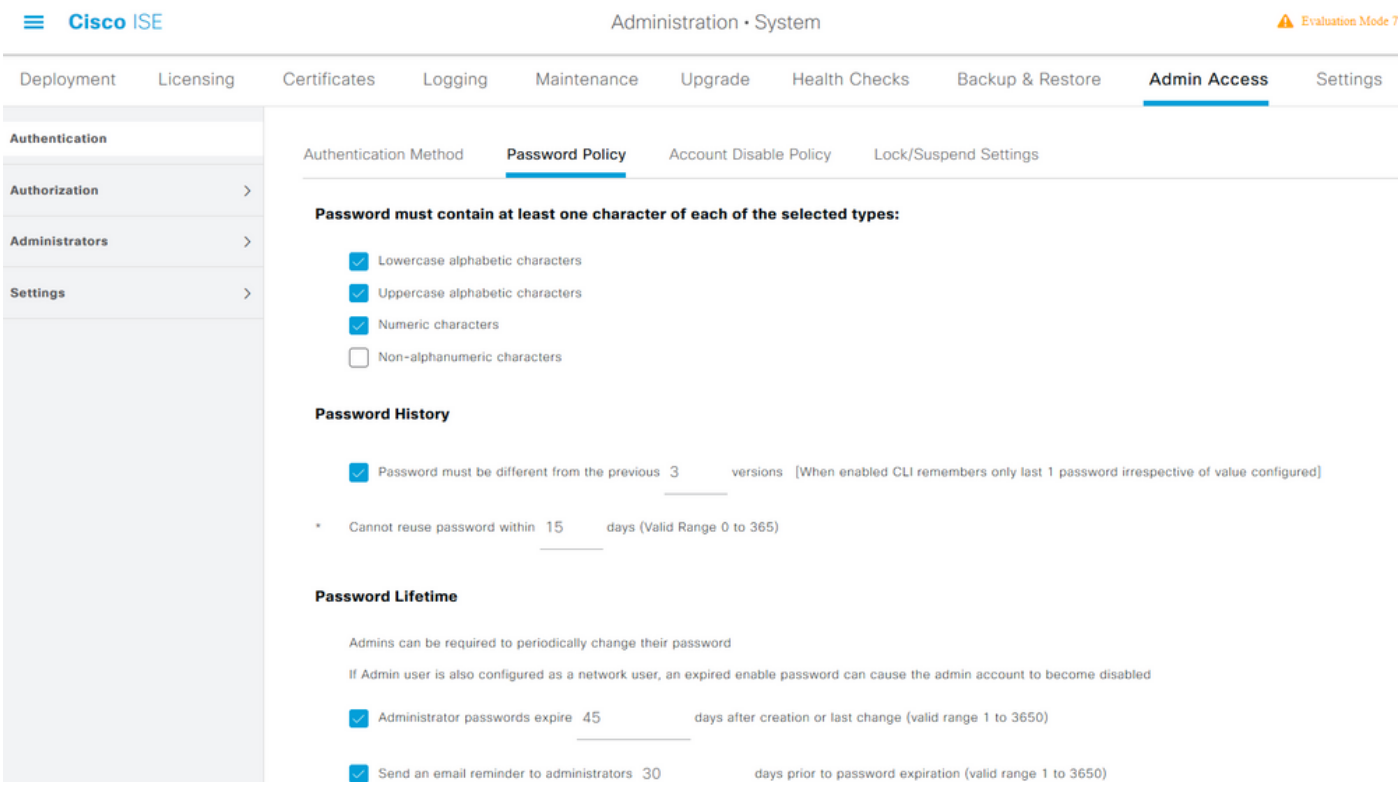
Admin-Benutzer müssen sich authentifizieren, um auf Informationen zur ISE zugreifen zu können. Die Identität von Admin-Benutzern kann mithilfe des ISE Internal Identity Store oder eines externen Identity Store überprüft werden. Die Authentizität kann entweder durch ein Kennwort oder ein Zertifikat überprüft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



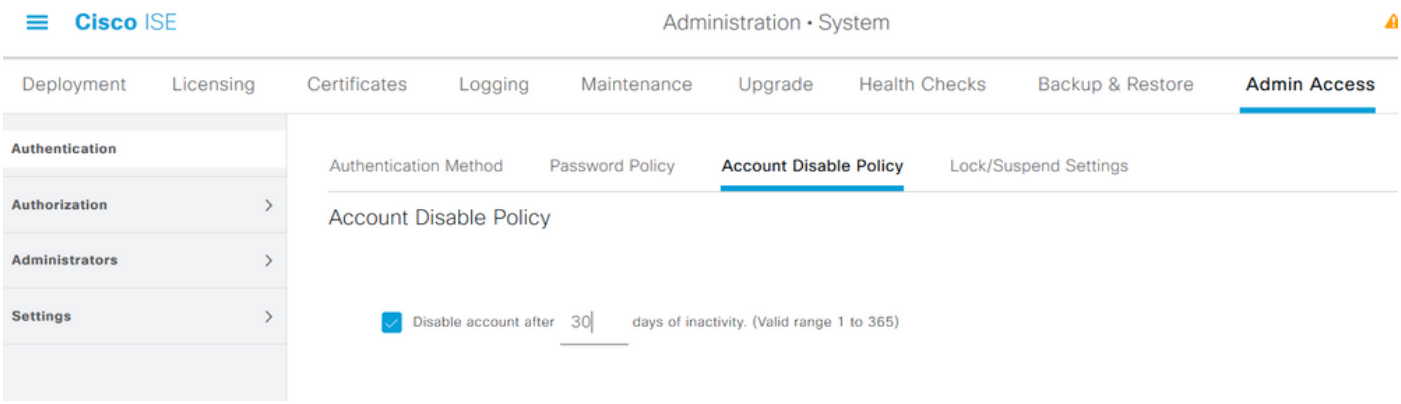
> **Hinweis**: Die kennwortbasierte Authentifizierung ist standardmäßig aktiviert. Wenn diese in Client Certificate-Based Authentication geändert wird, wird ein Neustart des Anwendungsservers auf allen Bereitstellungsknoten ausgelöst.

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

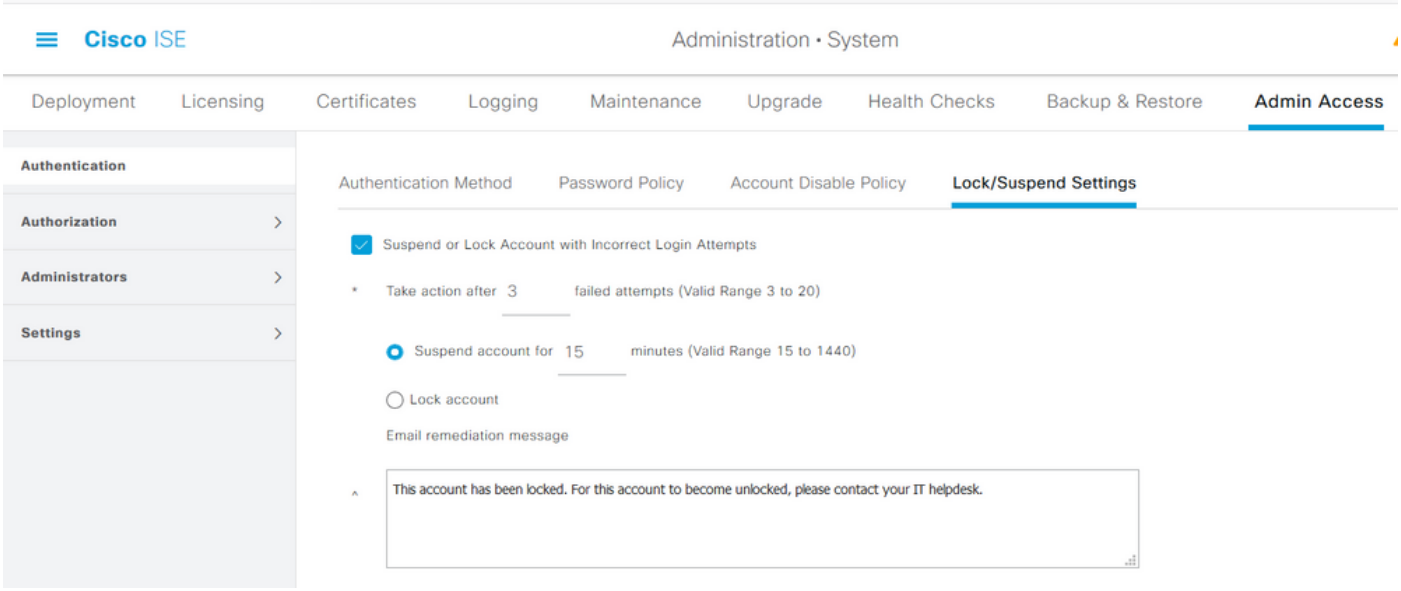




Die ISE bietet die Möglichkeit, inaktive Admin-Benutzer zu deaktivieren. Um dies zu konfigurieren, navigieren Sie zu **Administration > System > Admin Access > Authentication (Verwaltung > Administratorzugriff > Authentifizierung),** und navigieren Sie zur Registerkarte **Account Disable Policy (Kontodeaktivieren).**



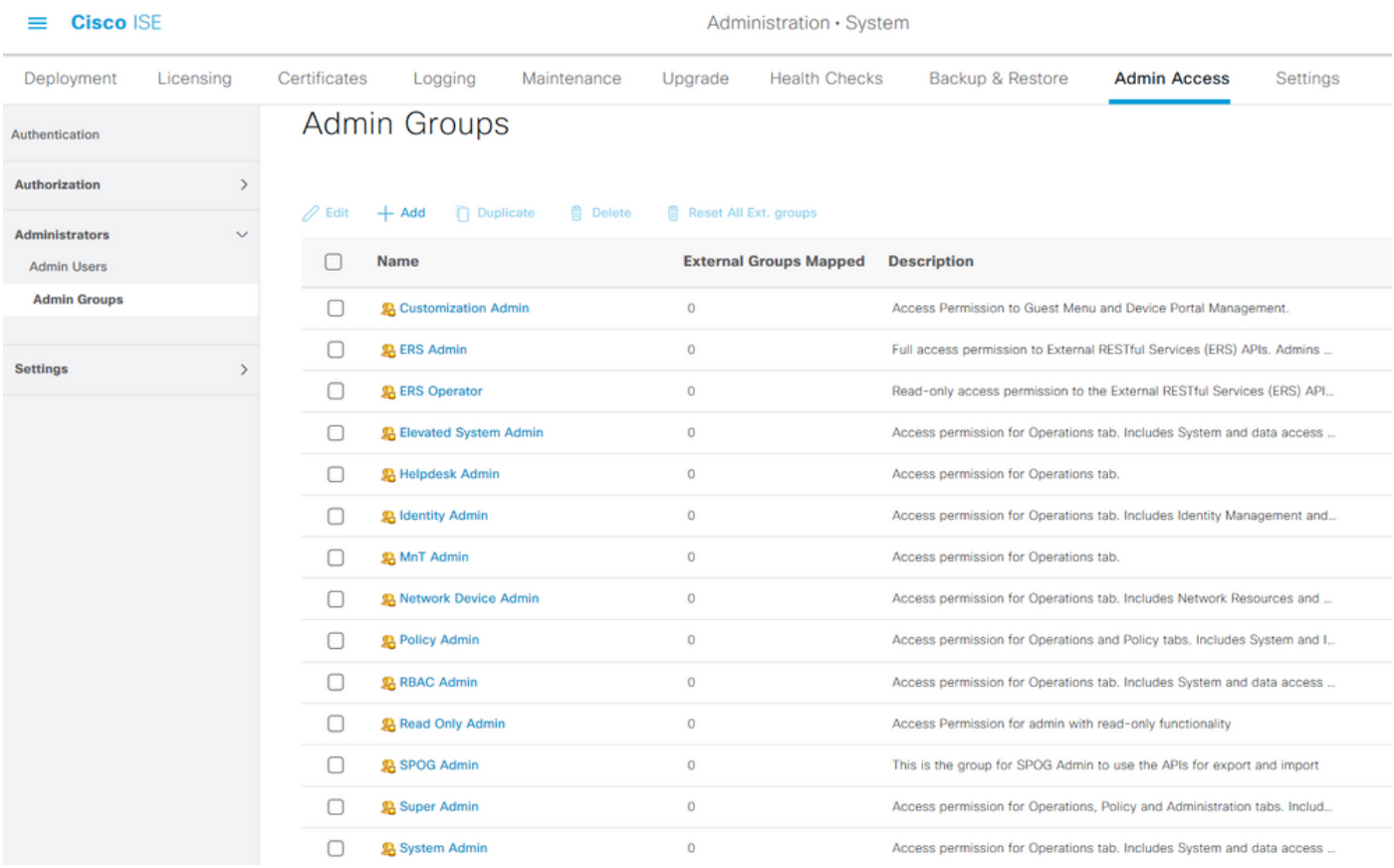
Die ISE bietet außerdem die Möglichkeit, ein Admin-Benutzerkonto basierend auf der Anzahl der fehlgeschlagenen Anmeldeversuche zu sperren oder auszusetzen. Um dies zu konfigurieren, navigieren Sie zu **Administration > System > Admin Access > Authentication (Verwaltung > Admin-Zugriff > Authentifizierung),**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



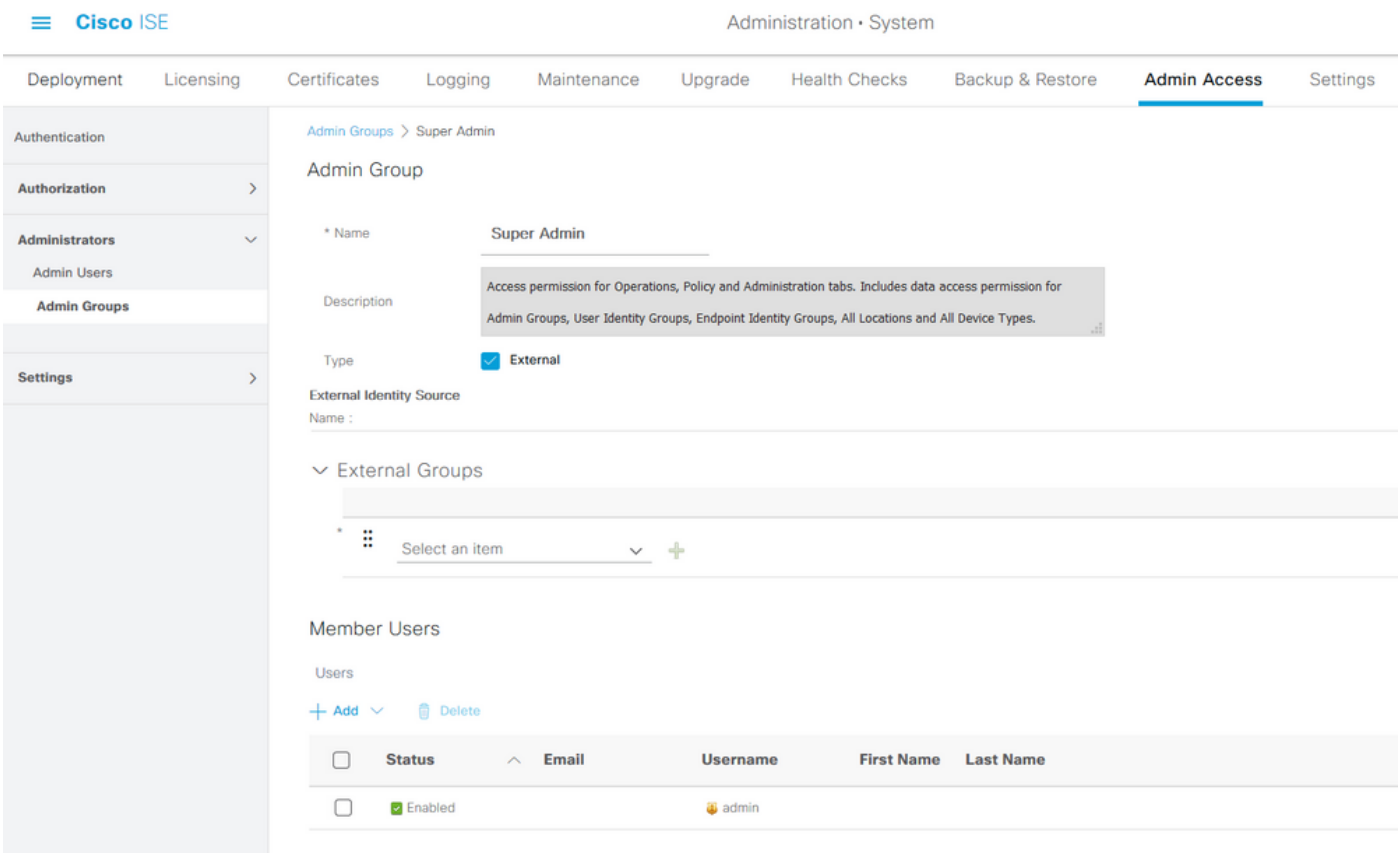
Für die Verwaltung des administrativen Zugriffs müssen Verwaltungsgruppen, Benutzer und verschiedene Richtlinien/Regeln ihre Berechtigungen steuern und verwalten.

Admin-Gruppen konfigurieren

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

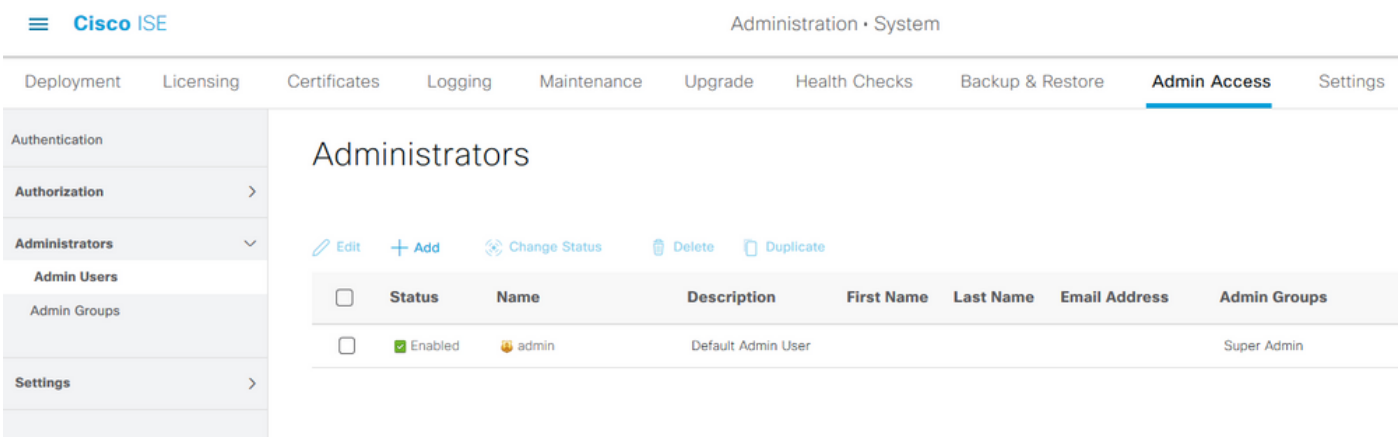


Wählen Sie nach dem Erstellen einer Gruppe die Gruppe aus, und klicken Sie auf Bearbeiten, um dieser Gruppe Administratorbenutzer hinzuzufügen. Es besteht die Möglichkeit, den Admin-Gruppen auf der ISE externe Identitätsgruppen zuzuordnen, sodass ein externer Admin-Benutzer die erforderlichen Berechtigungen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

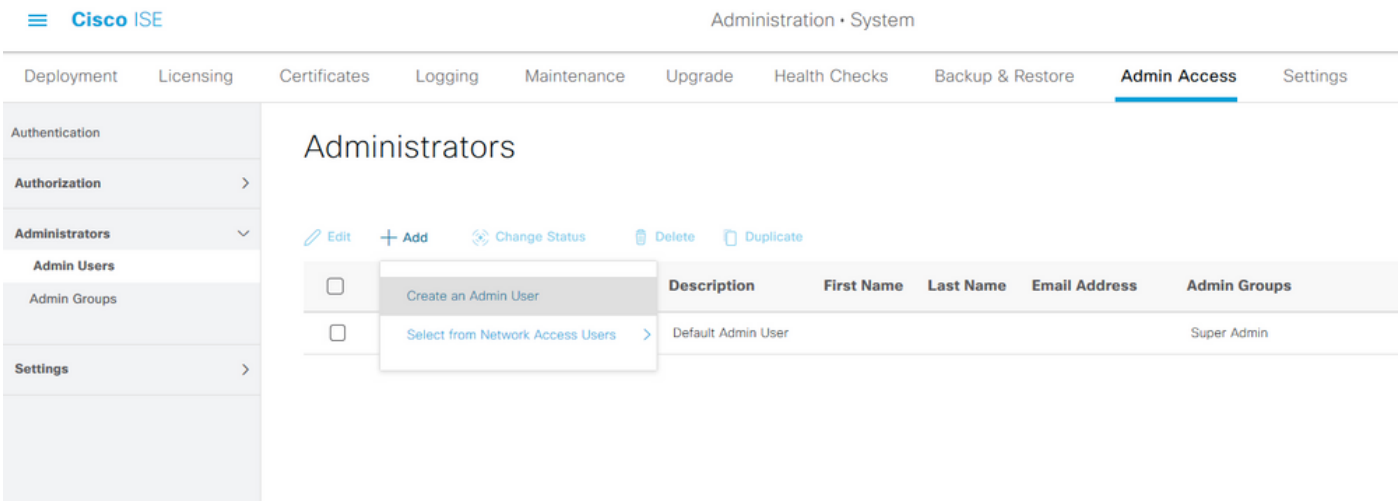


Admin-Benutzer konfigurieren

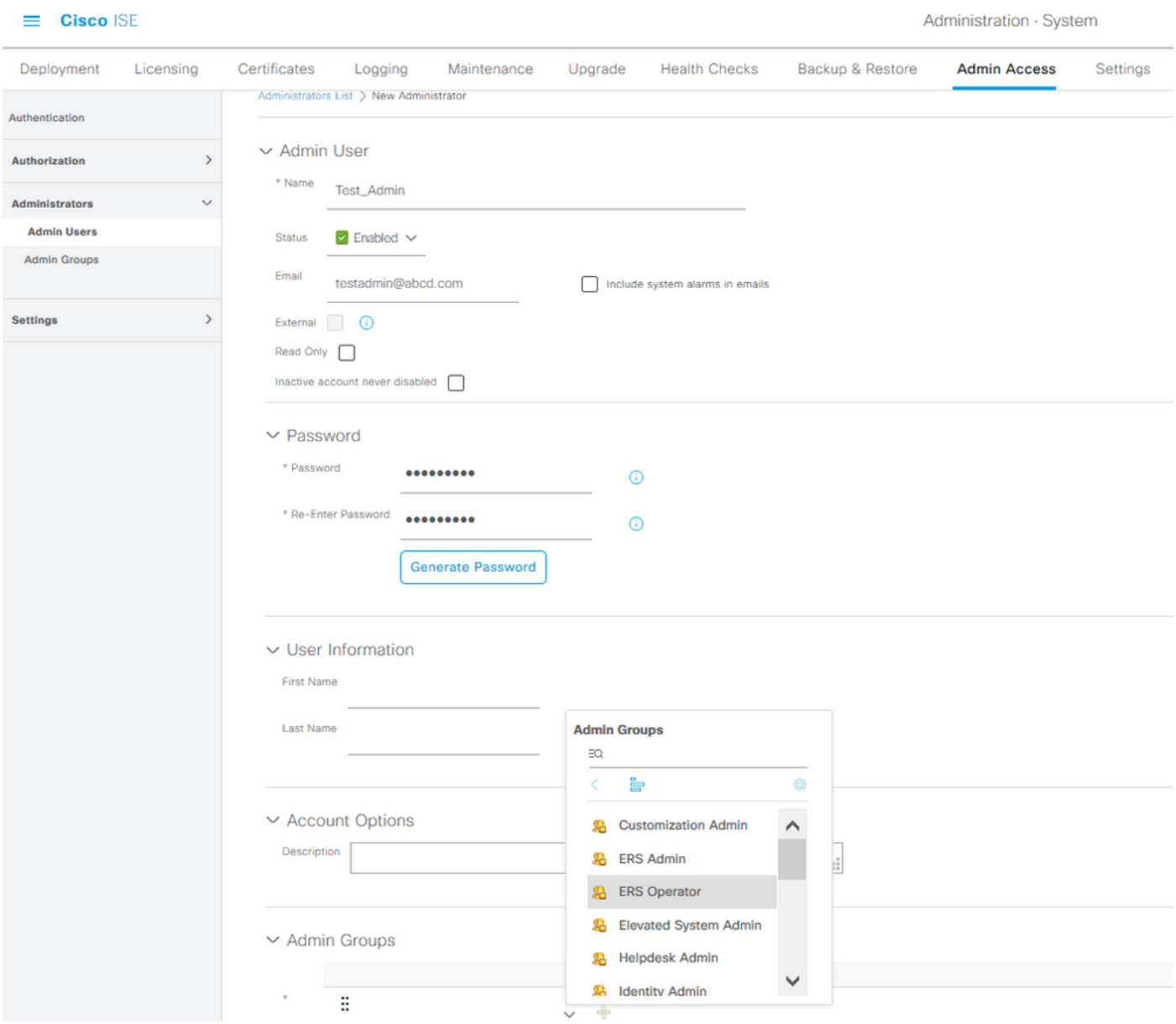
Um Admin-Benutzer zu konfigurieren, navigieren Sie zu **Administration > System > Admin Access > Administrator > Admin Users**.



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



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



Berechtigungen konfigurieren

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

1. Menüzugriff
2. Datenzugriff

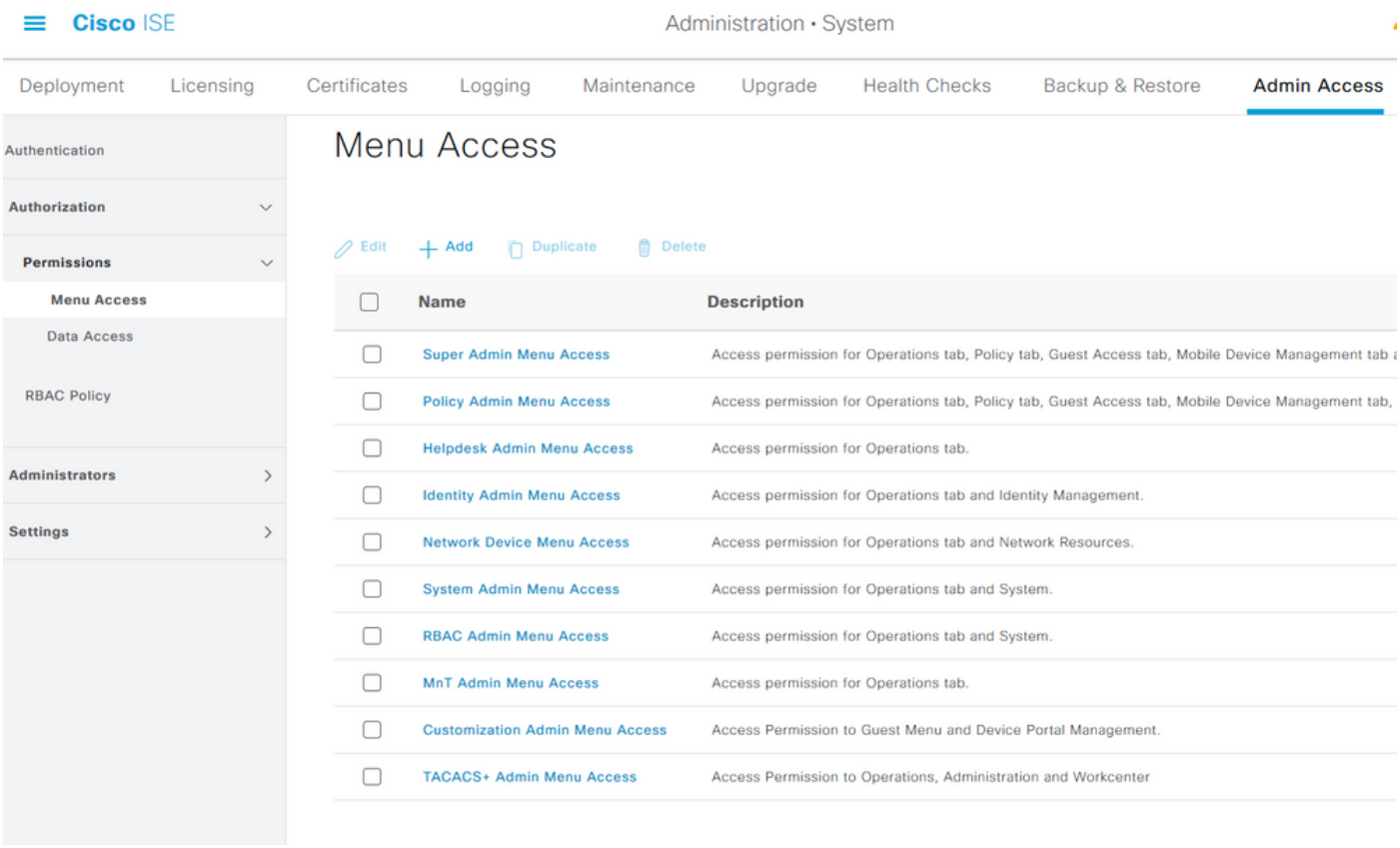
Über Menüzugriff wird die Navigationstransparenz auf der ISE gesteuert. Für jede Registerkarte gibt es zwei Optionen: Anzeigen oder Ausblenden, die konfiguriert werden können. Mit einer Regel für den Menüzugriff können ausgewählte Registerkarten ein- oder ausgeblendet werden.

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

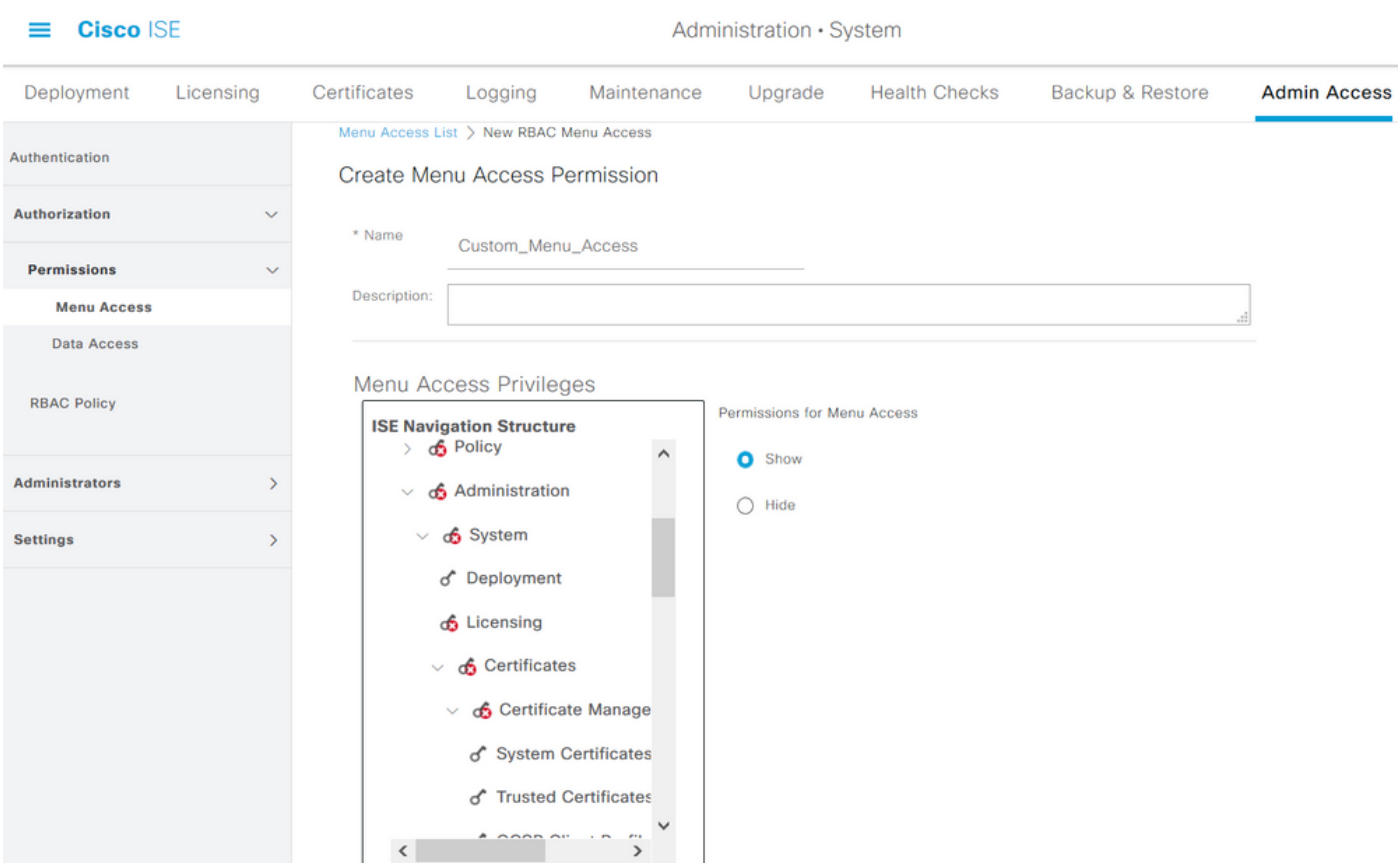
Menüzugriff und Datenzugriffsrichtlinien müssen erstellt werden, bevor sie auf eine beliebige

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

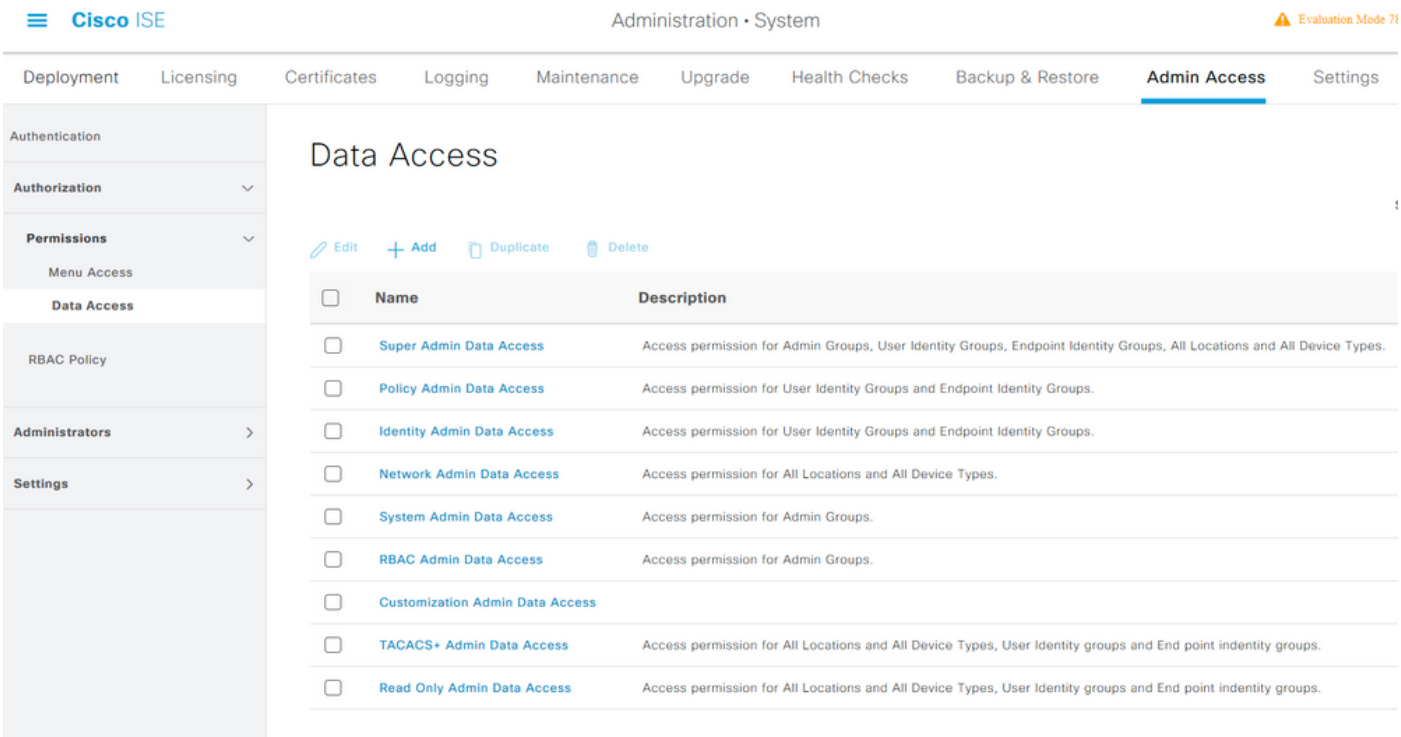
Um eine Menüzugriffsrichtlinie zu konfigurieren, navigieren Sie zu **Administration > System > Admin Access > Authorization > Permissions > Menu Access (Verwaltung > Administratorzugriff > Autorisierung > Berechtigungen > Menüzugriff)**.



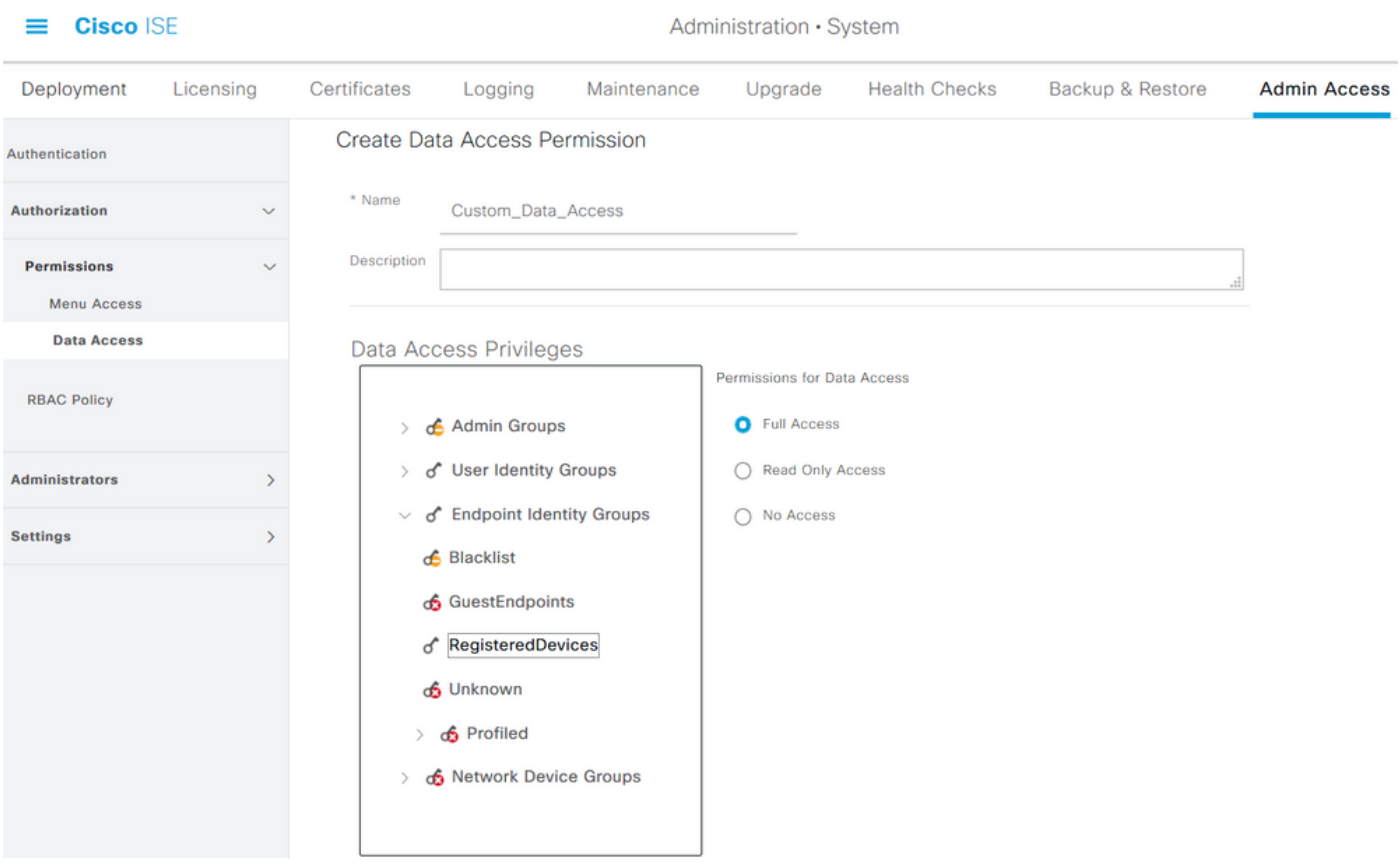
Klicken Sie auf **Hinzufügen**. Jede Navigationsoption in der ISE kann so konfiguriert werden, dass sie in einer Richtlinie angezeigt/ausgeblendet wird.



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

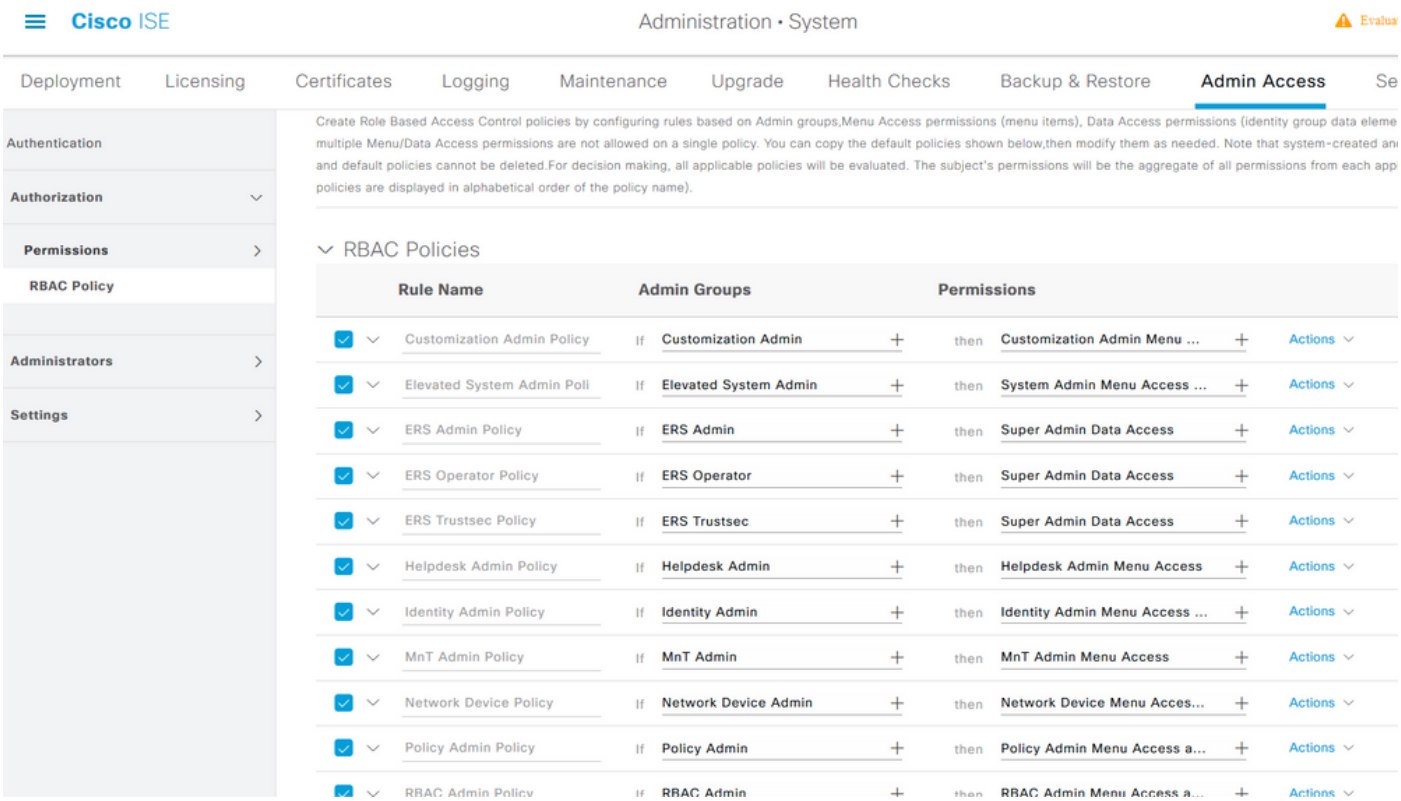


Klicken Sie auf **Hinzufügen**, um eine neue Richtlinie zu erstellen und Berechtigungen für den Zugriff auf die Identität von Admin/Benutzer/Endpunkt/Netzwerkgruppen zu konfigurieren.



RBAC-Richtlinien konfigurieren

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



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

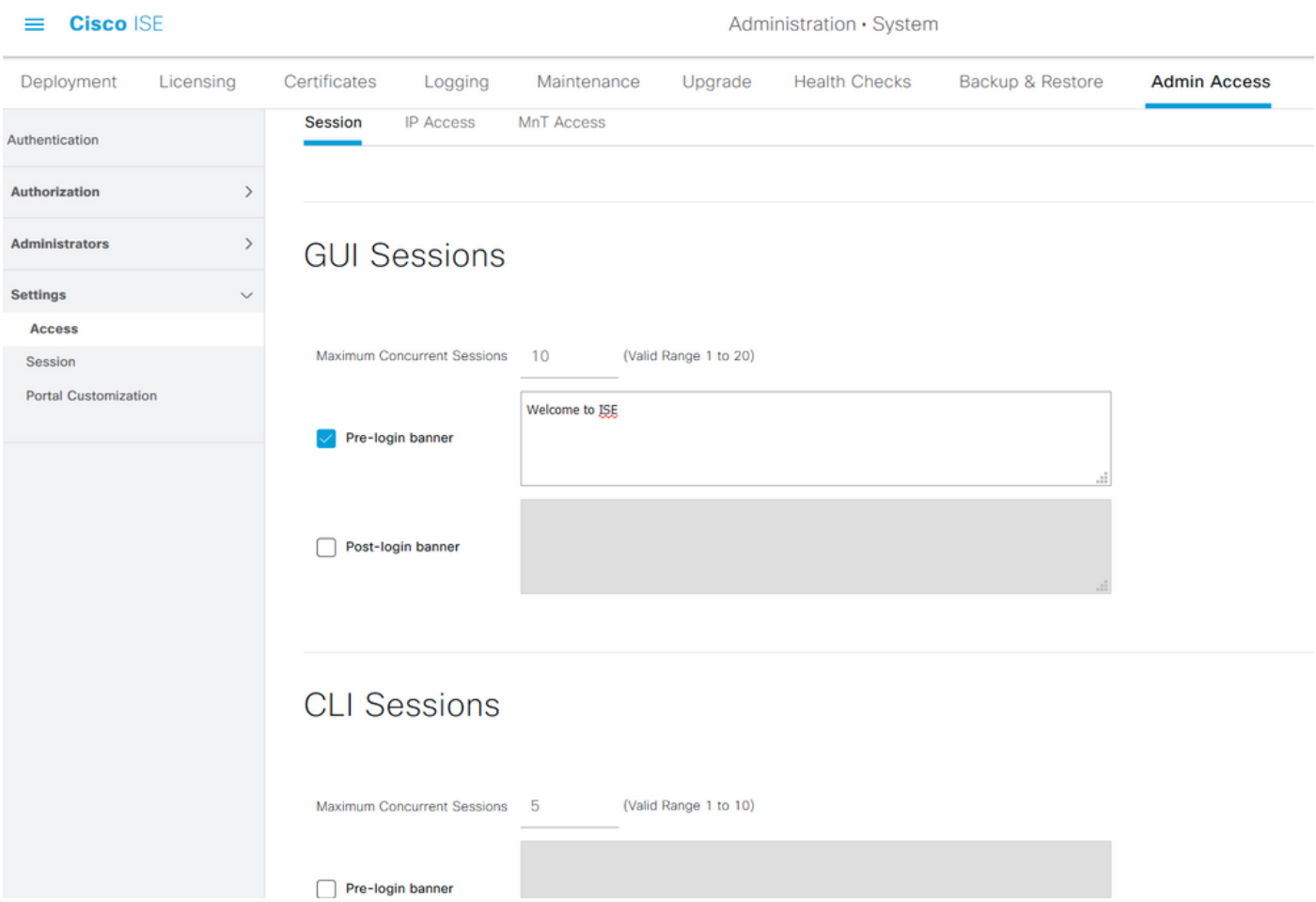
> **Hinweis**: Vom System erstellte und Standard-Richtlinien können nicht aktualisiert werden, und Standardrichtlinien können nicht gelöscht werden.

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

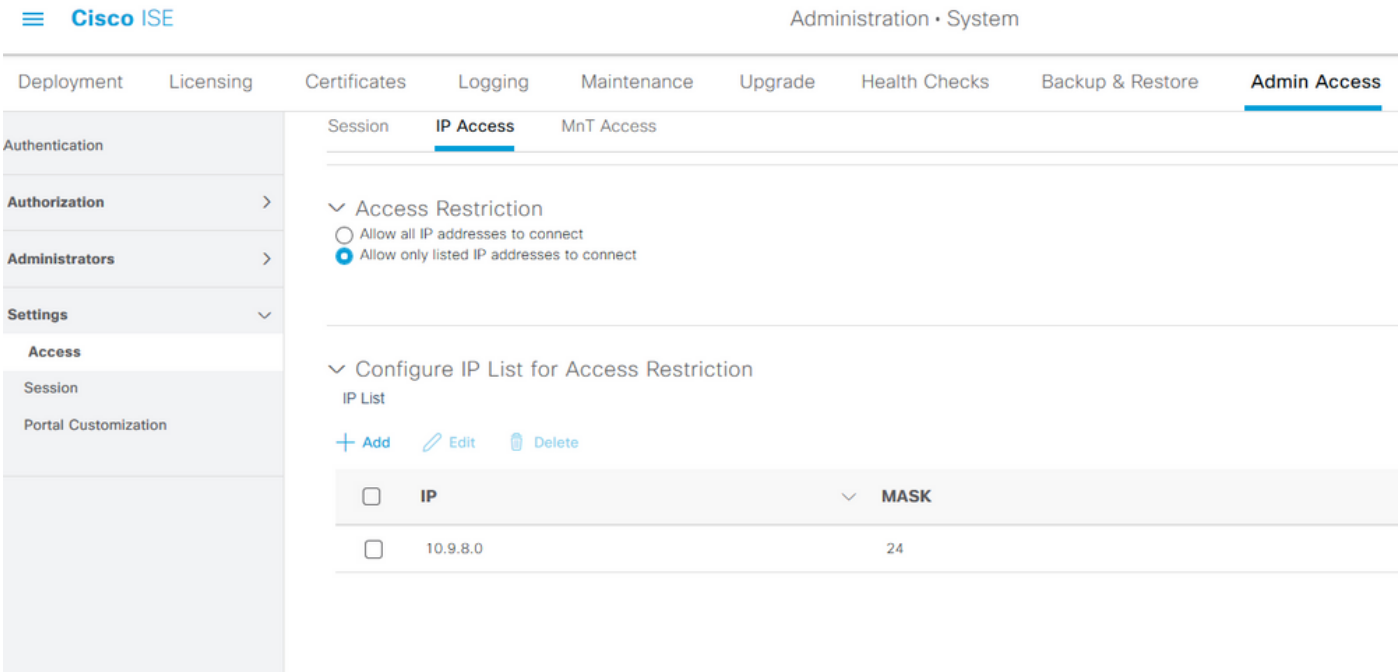
Konfigurieren der Einstellungen für den Administratorzugriff

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

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

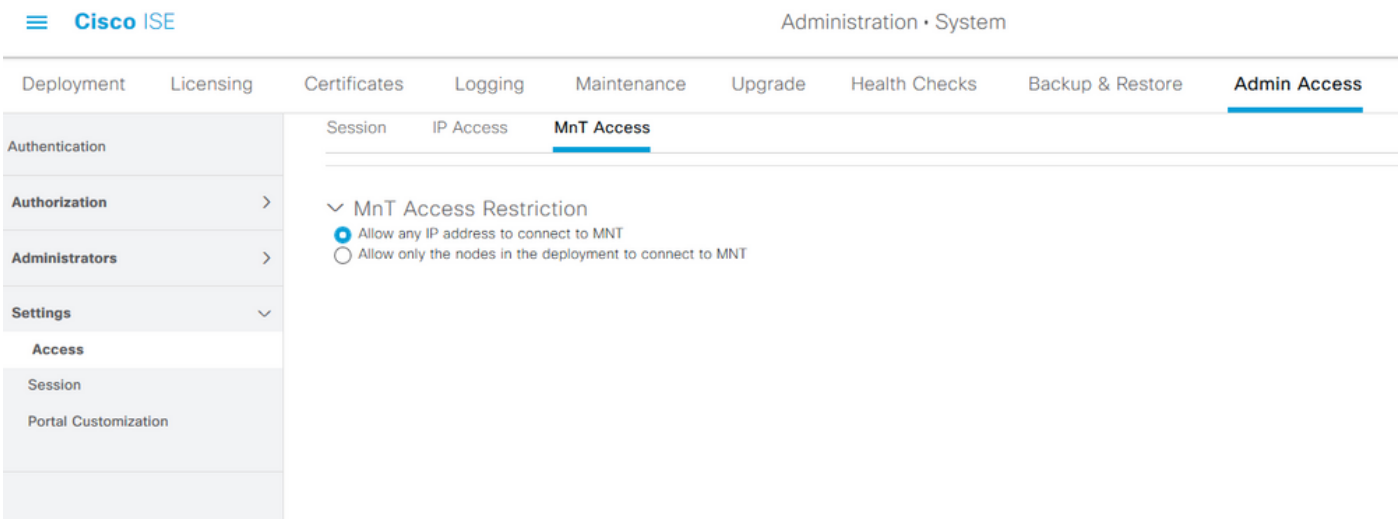


Um die Liste der IP-Adressen zu konfigurieren, von denen aus auf die GUI und die CLI zugegriffen werden kann, navigieren Sie zu **Administration > System > Admin Access > Settings > Access** und navigieren Sie zur Registerkarte **IP Access (IP-Zugriff)**.



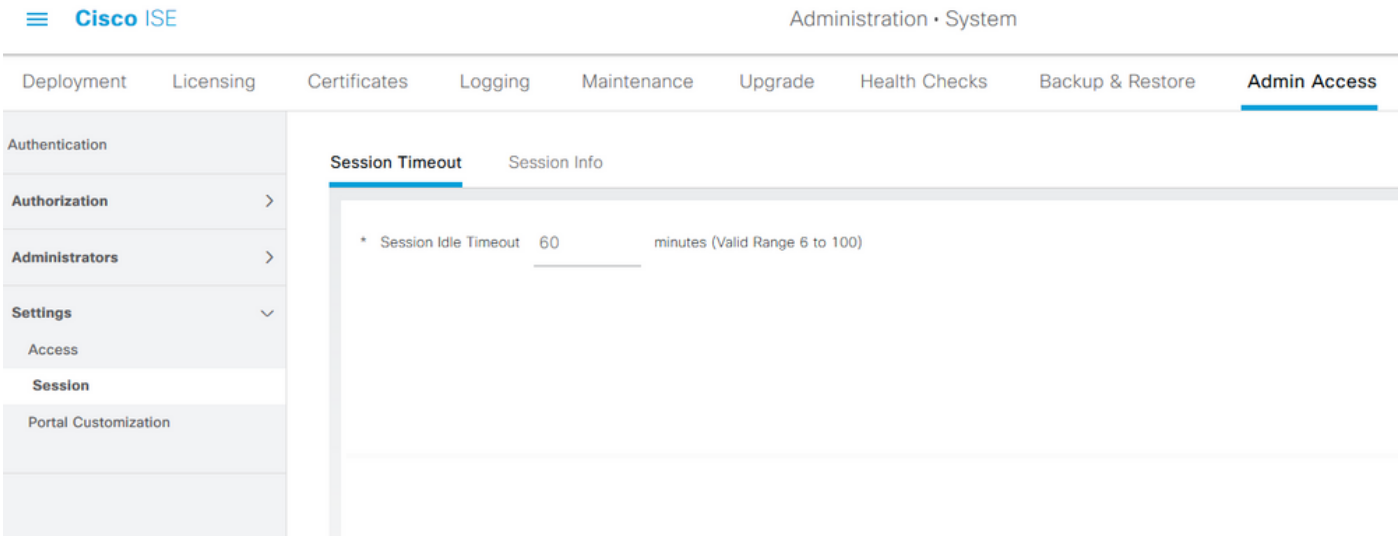
Um eine Liste von Knoten zu konfigurieren, von denen Administratoren auf den MnT-Bereich in der Cisco ISE zugreifen können, navigieren Sie zu **Administration > System > Admin Access > Settings > Access (Verwaltung > Administratorzugriff > Einstellungen > Zugriff)** und navigieren Sie zur Registerkarte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

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

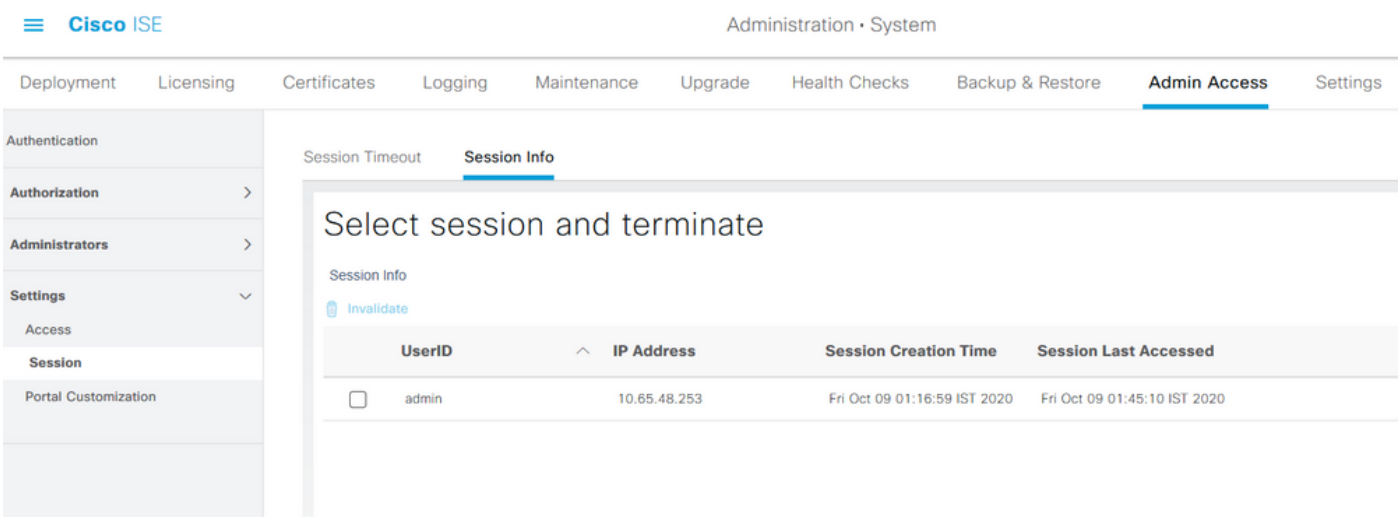


> **Hinweis**: Für ISE 2.6 Patch 2 und höher ist *"ISE Messaging Service" für die Bereitstellung von UDP-Syslogs an MnT* standardmäßig aktiviert, sodass Syslogs von anderen Einheiten außerhalb der Bereitstellung nicht zugelassen werden.

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



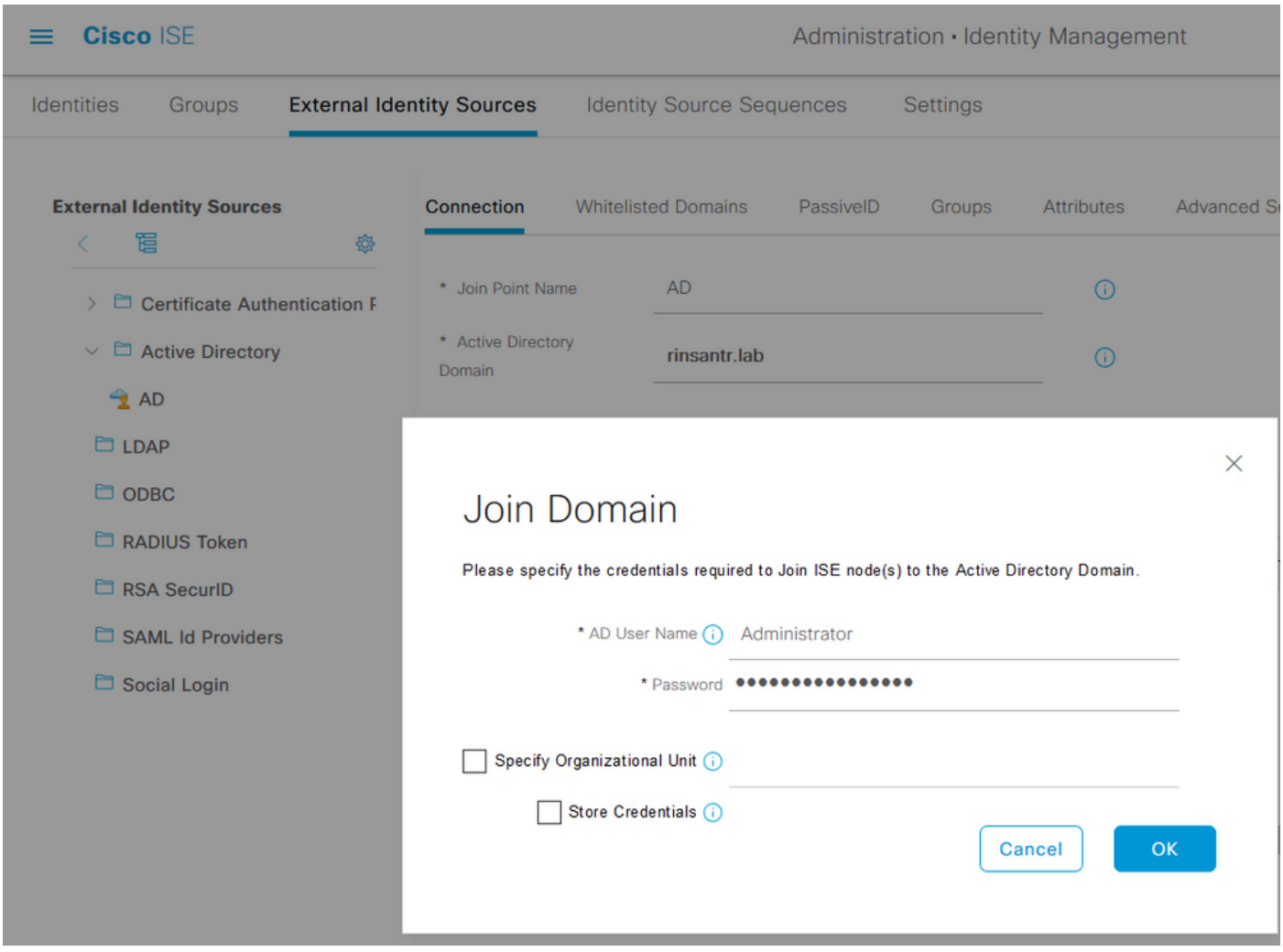
Um die aktuellen aktiven Sitzungen anzuzeigen/für ungültig zu erklären, navigieren Sie zu **Administration > Admin Access > Settings > Session** und klicken Sie auf die Registerkarte **Session Info (Sitzungsinformationen)**.

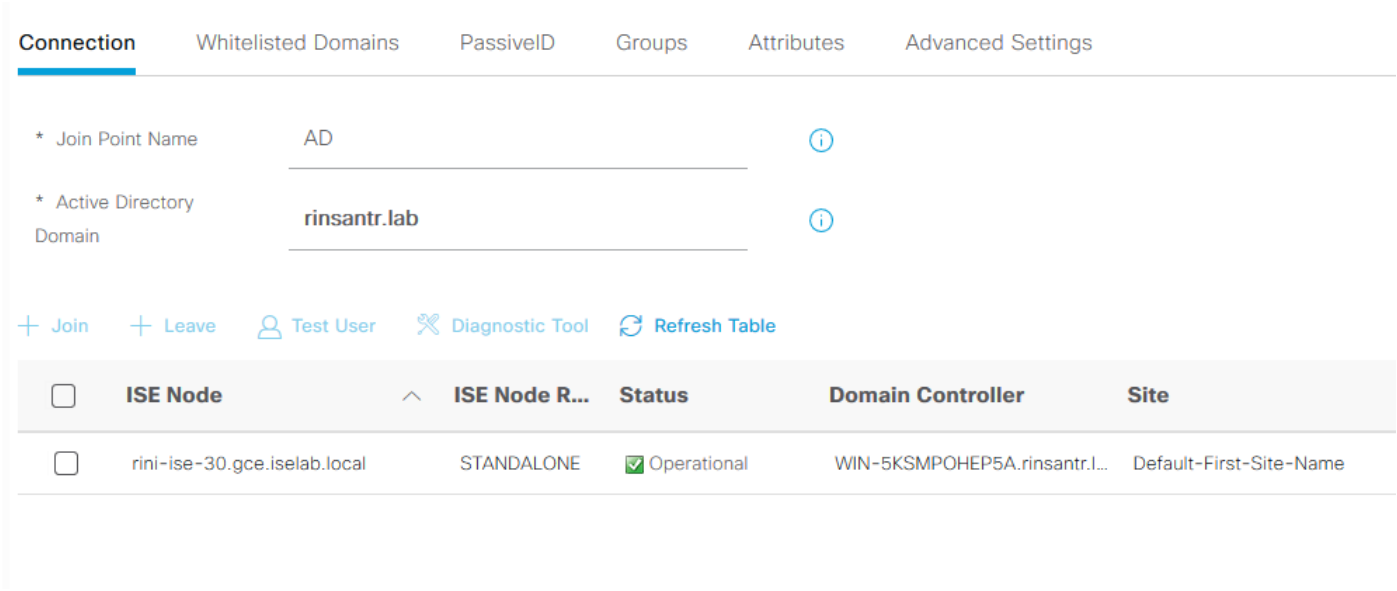


Konfigurieren des Admin-Portalzugriffs mit AD-Anmeldeinformationen

Werden Sie Teil der ISE

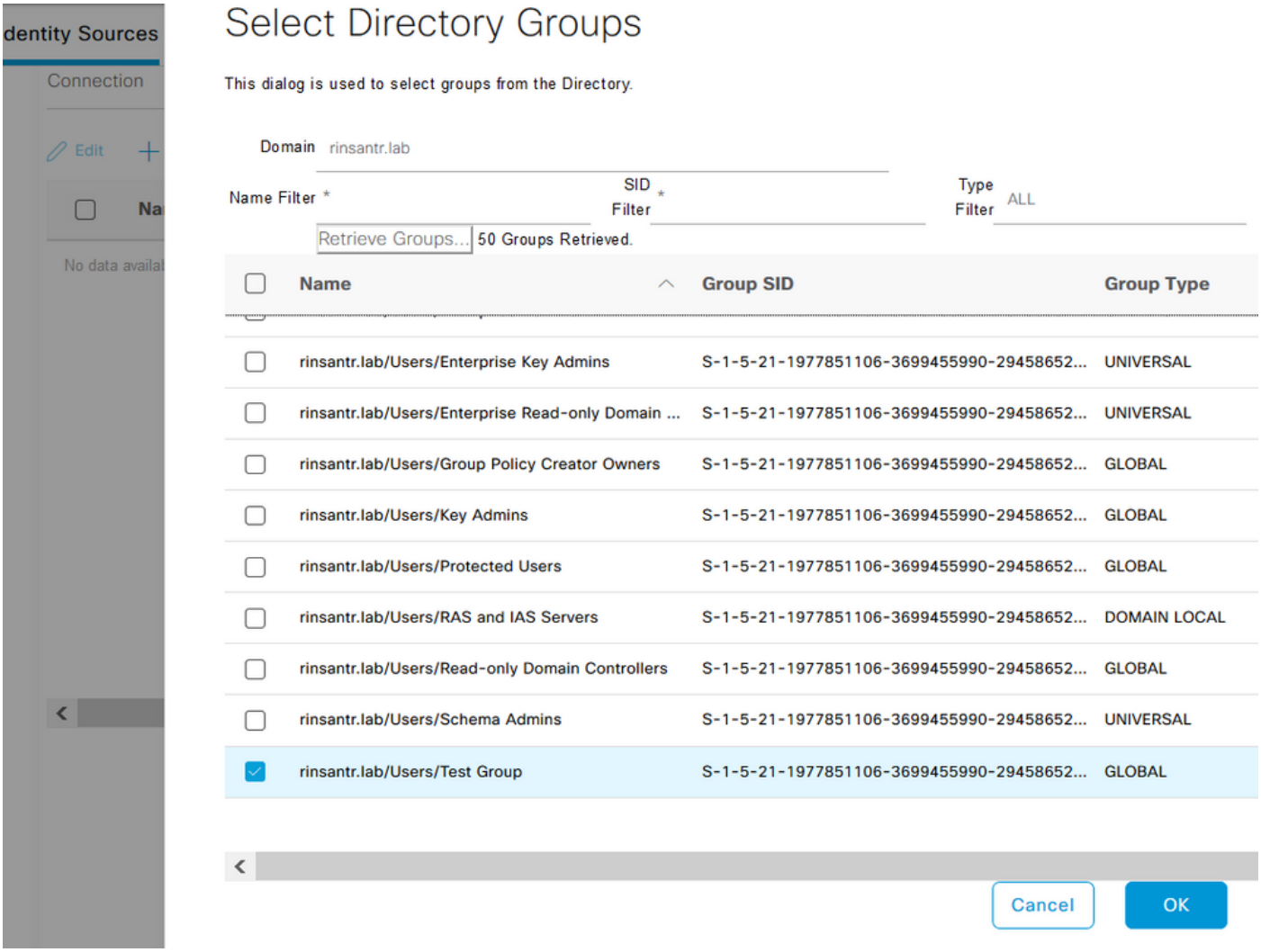
Um der ISE zu einer externen Domäne beizutreten, navigieren Sie zu **Administration > Identity Management > External Identity Sources > Active Directory**. Geben Sie den neuen Join-Punktnamen und die Active Directory-Domäne ein. Geben Sie die Anmeldeinformationen des AD-Kontos ein, das Computerobjekte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

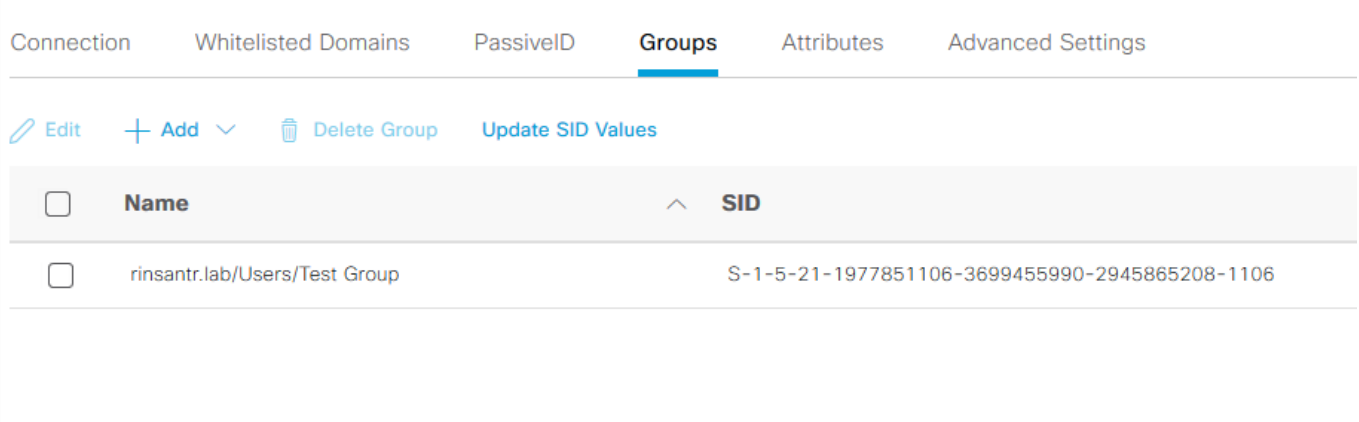




Verzeichnisgruppen auswählen

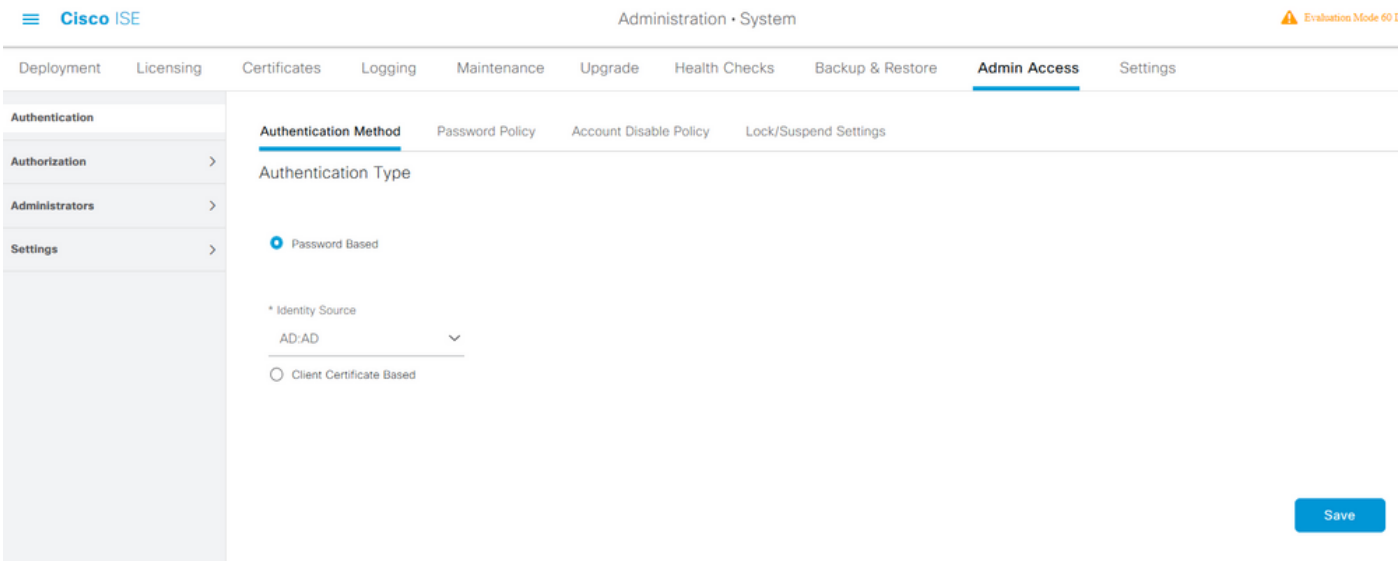
Navigieren Sie zu **Administration > Identity Management > External Identity Sources > Active Directory**. Klicken Sie auf den gewünschten Join Point-Namen, und navigieren Sie zur Registerkarte **Groups**. Klicken Sie auf **Hinzufügen > Gruppen aus Verzeichnis auswählen > Gruppen abrufen**. Importieren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





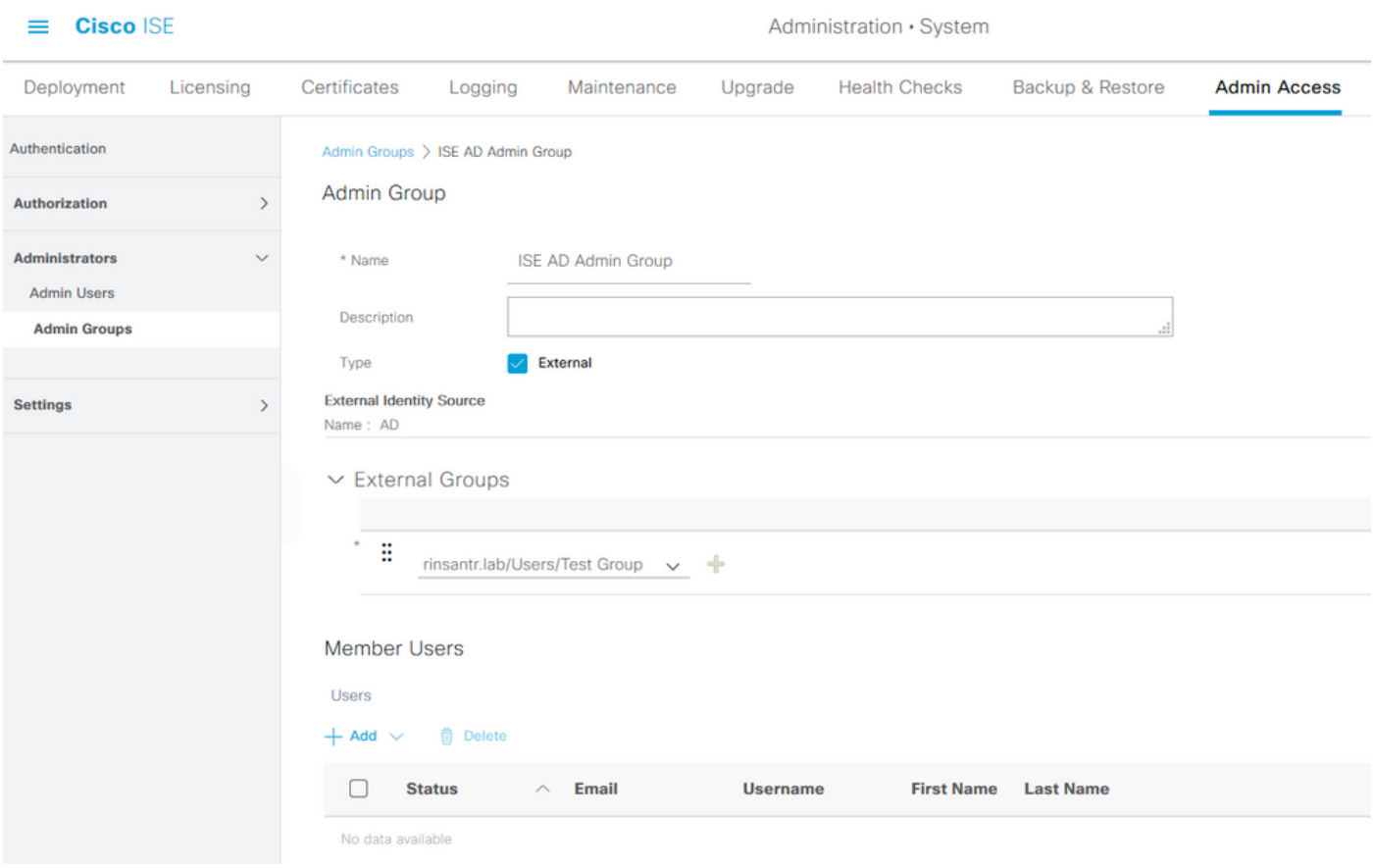
Administratorzugriff für AD aktivieren

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



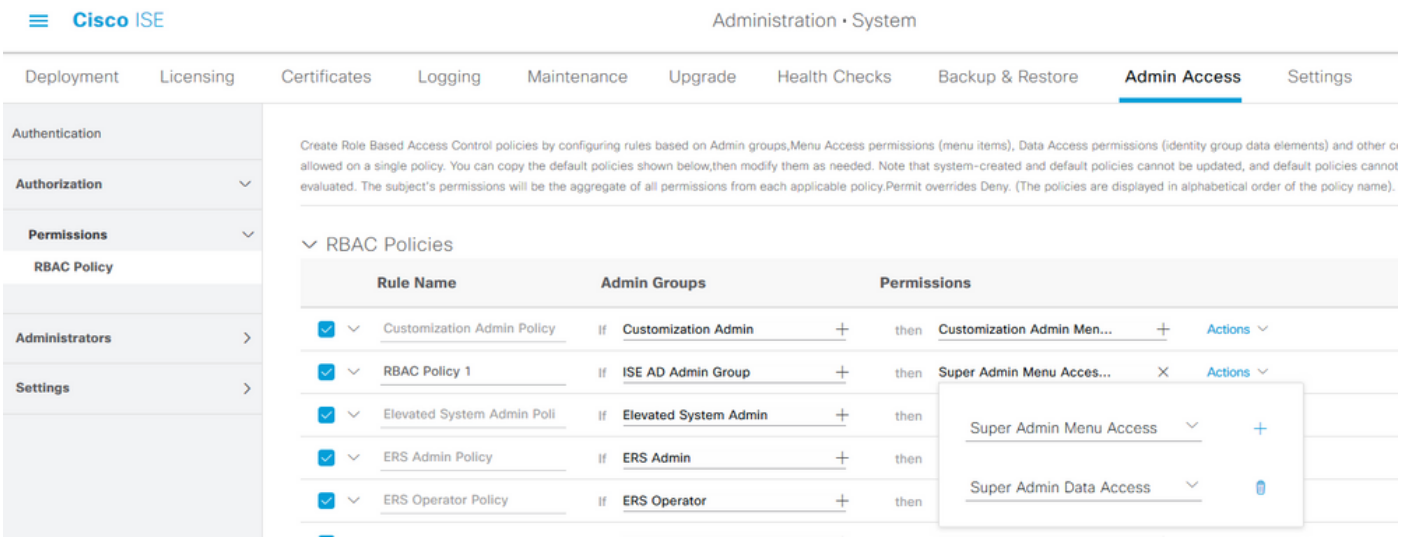
Konfigurieren der ISE-Admin-Gruppe für AD-Gruppenzuordnung

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



RBAC-Berechtigungen für die Admin-Gruppe festlegen

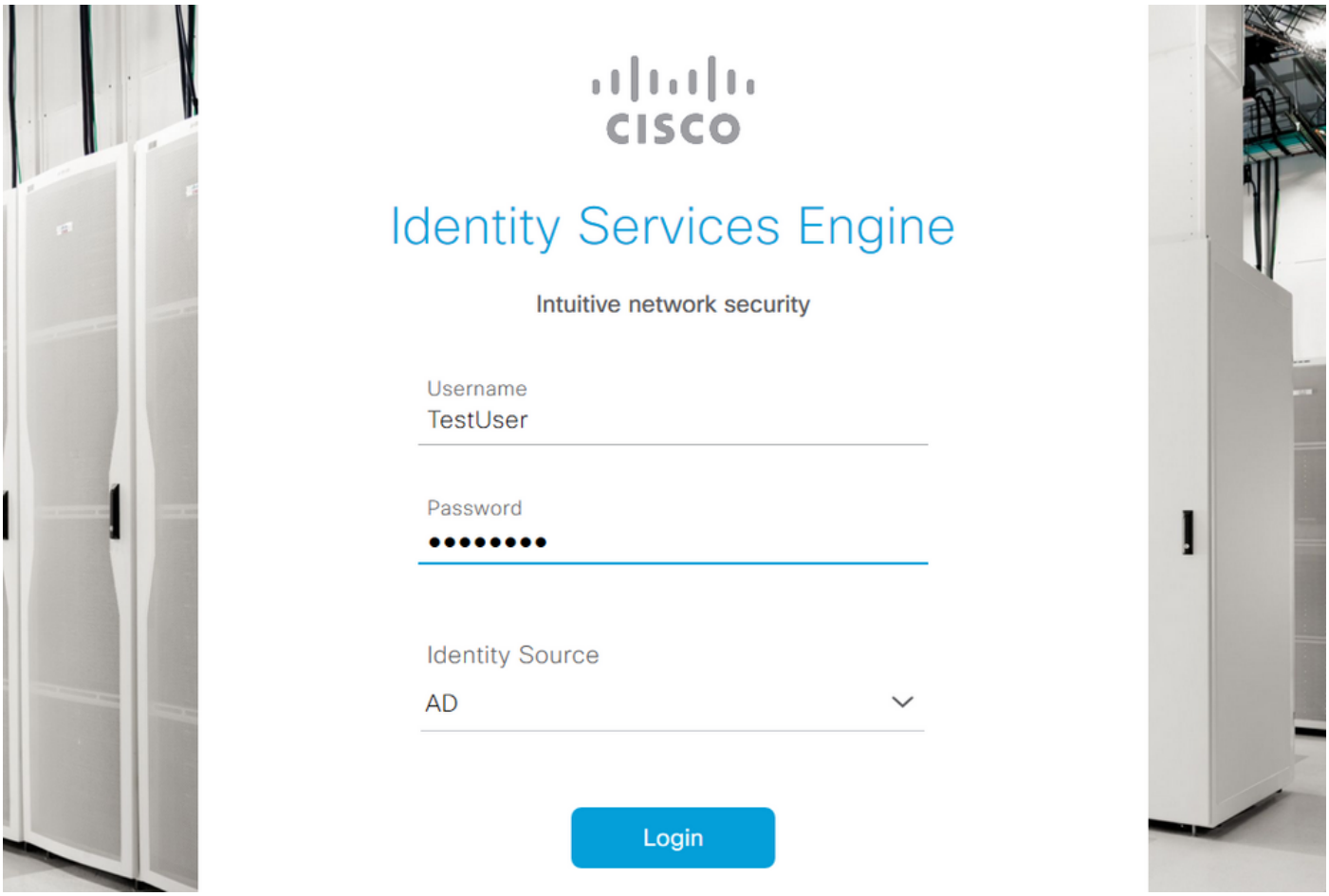
Um der im vorherigen Abschnitt erstellten Admin Group RBAC-Berechtigungen zuzuweisen, navigieren Sie zu **Administration > System > Admin Access > Authorization > RBAC Policy**. Wählen Sie im Dropdown-Menü **Aktionen** rechts die Option **Neue Richtlinie einfügen aus**. Erstellen Sie eine neue Regel,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



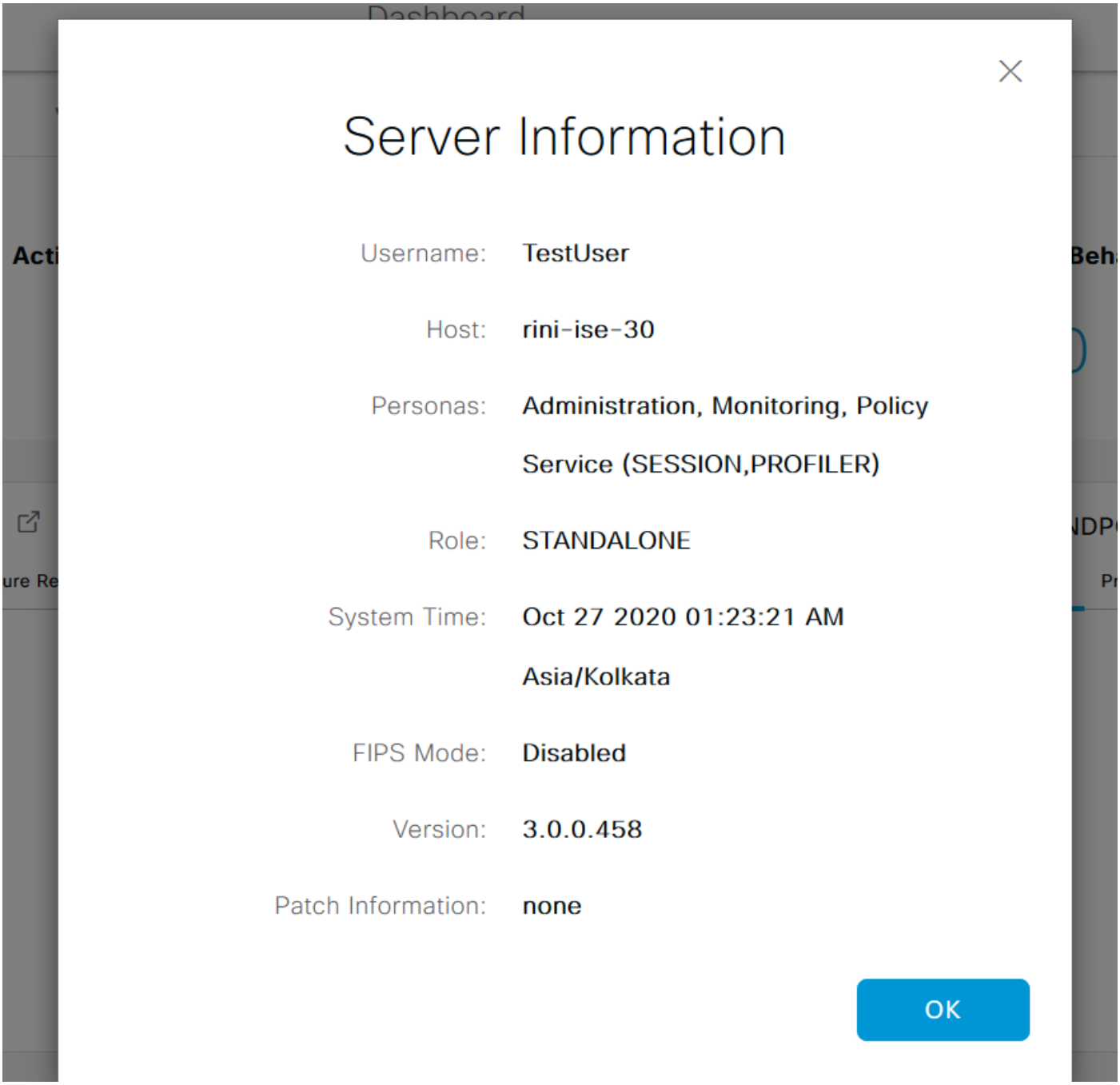
Zugriff auf die ISE mit AD-Anmeldeinformationen und Überprüfung

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

Datenbank ein, und melden Sie sich an.



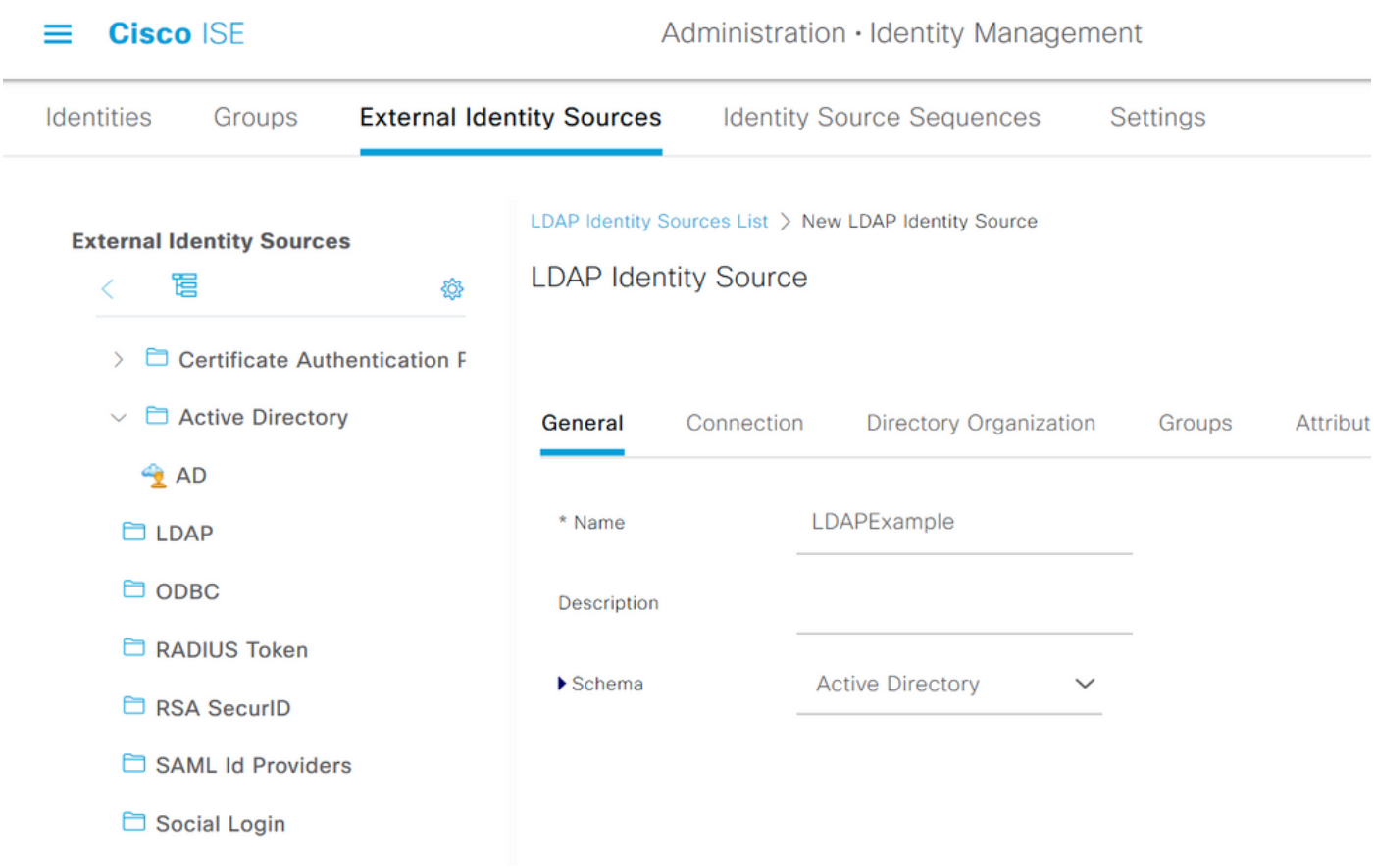
Um zu überprüfen, ob die Konfiguration ordnungsgemäß funktioniert, überprüfen Sie den authentifizierten Benutzernamen über das Symbol **Einstellungen** oben rechts in der ISE-GUI. Navigieren Sie zu **Serverinformationen**, und überprüfen Sie den Benutzernamen.



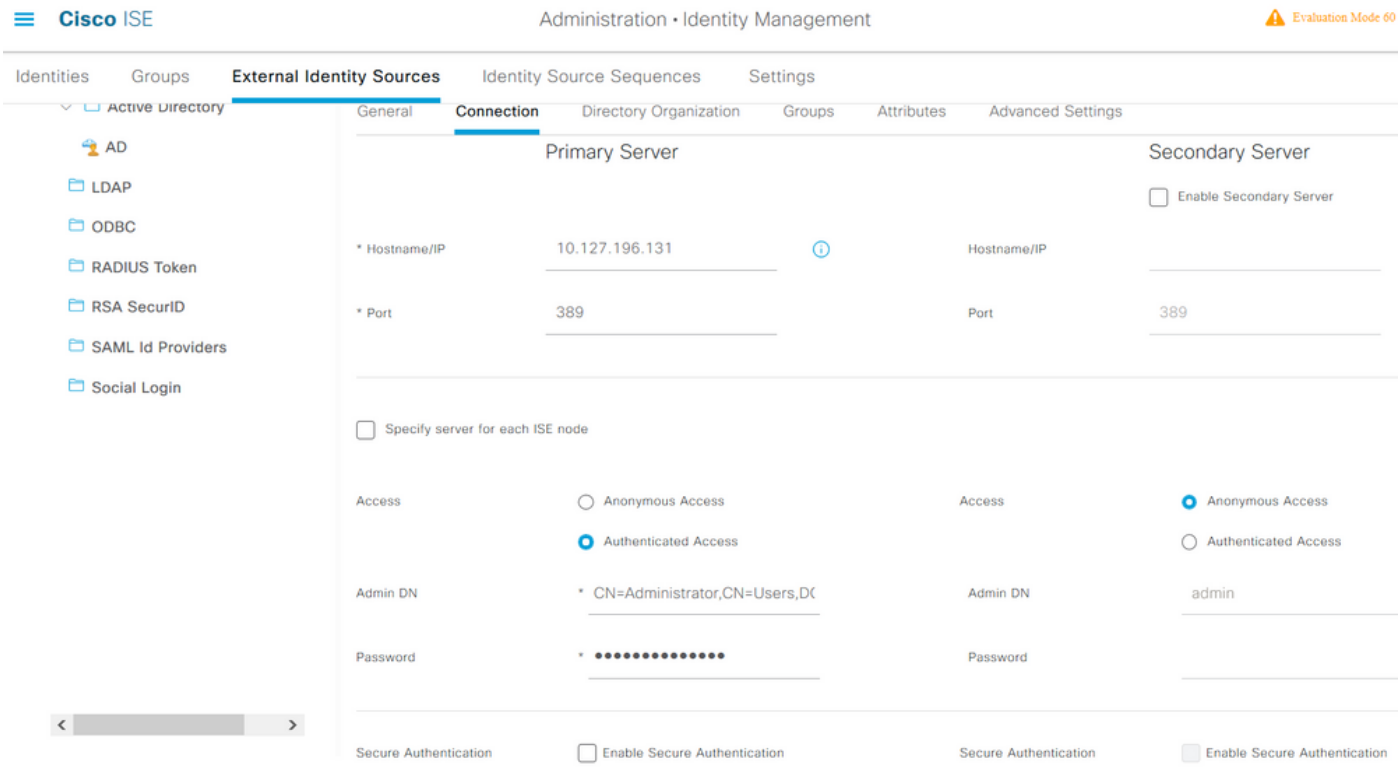
Konfigurieren des Admin-Portalzugriffs mit LDAP

Beitritt zur ISE zum LDAP

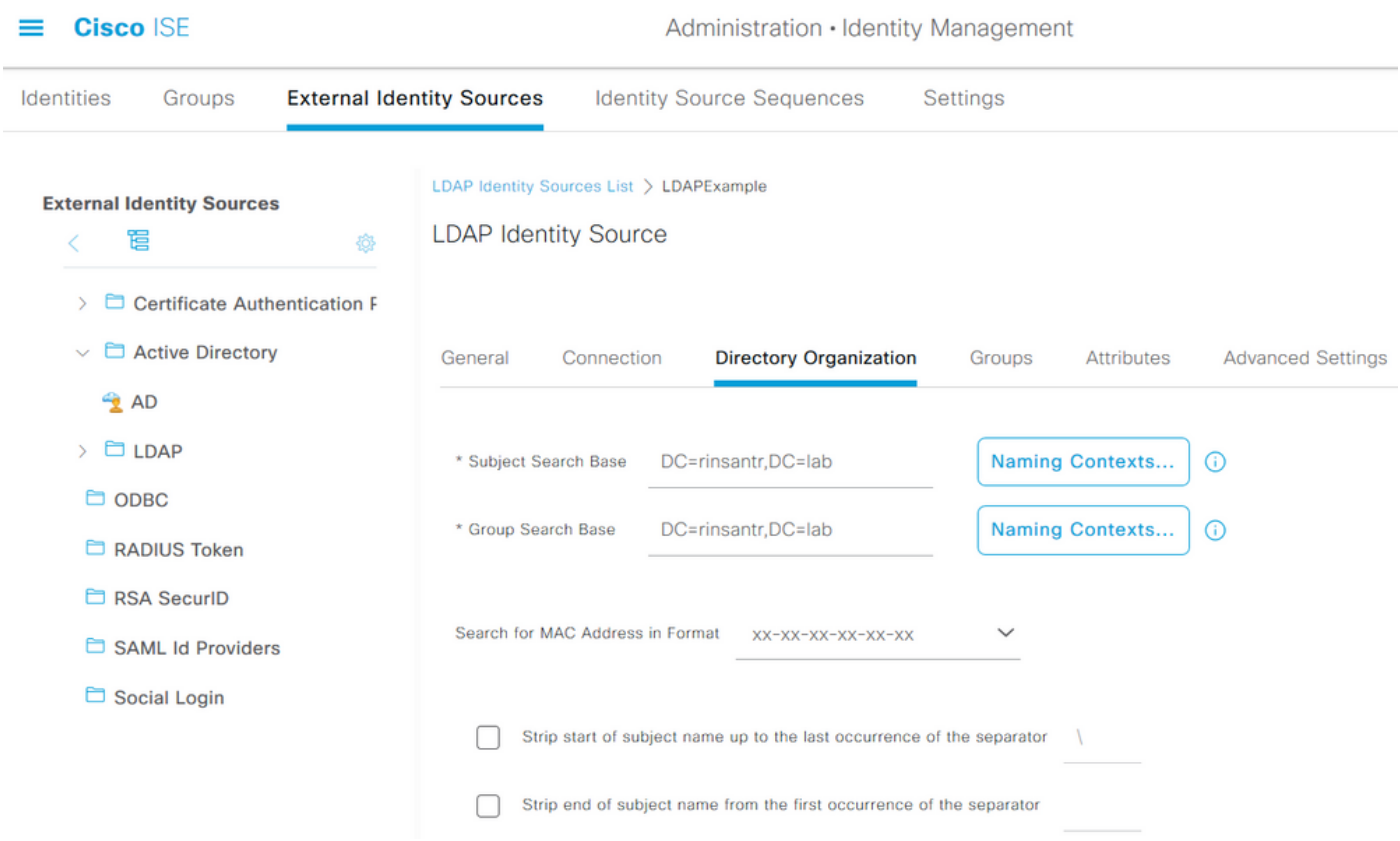
Navigieren Sie zu **Administration > Identity Management > External Identity Sources > Active Directory > LDAP**. Geben Sie auf der Registerkarte **Allgemein** einen Namen für das LDAP ein, und wählen Sie das Schema als **Active Directory aus**.



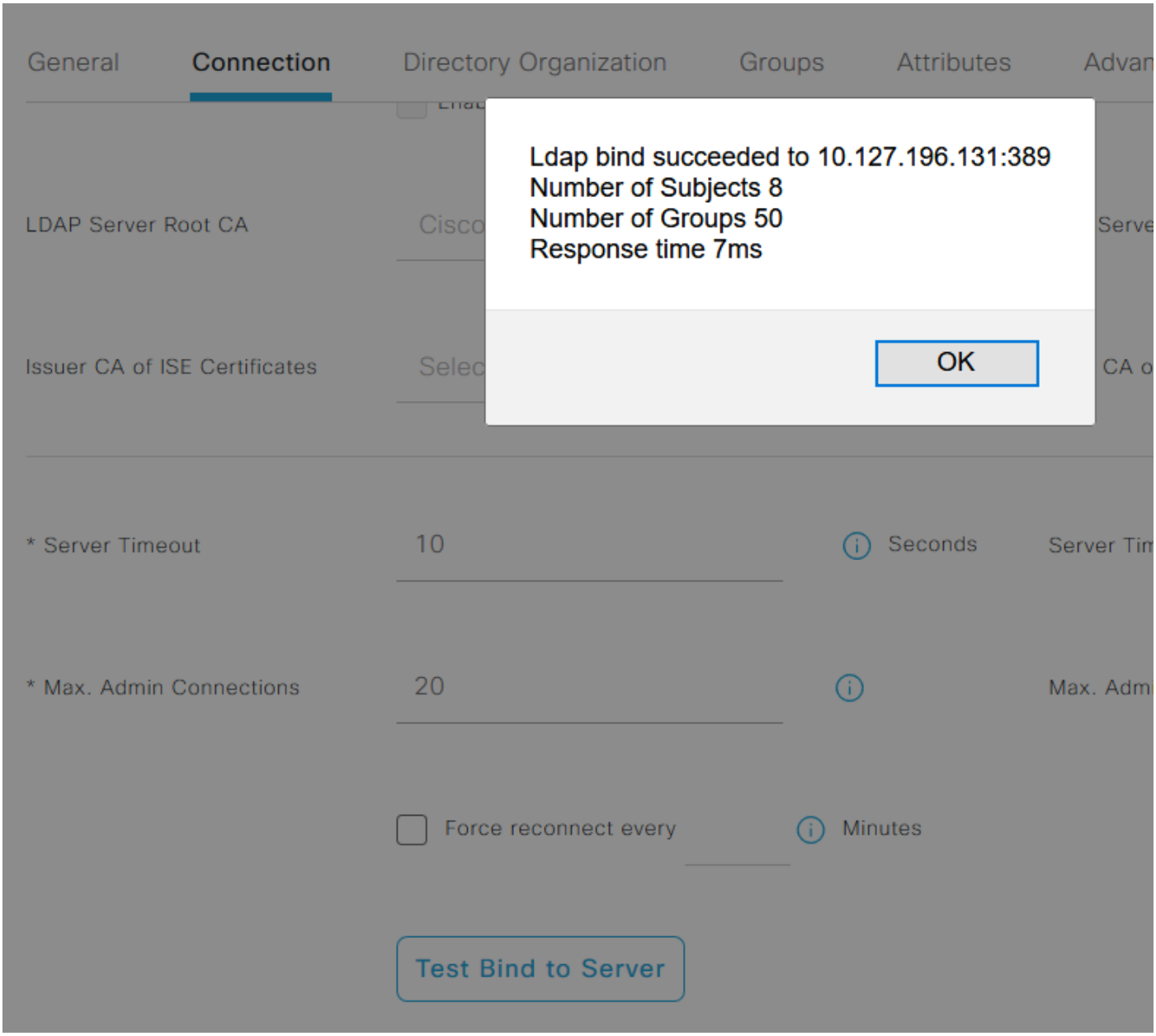
Navigieren Sie anschließend zur Registerkarte **Verbindung**, um den Verbindungstyp zu konfigurieren. Legen Sie hier den Hostnamen/die IP-Adresse des primären LDAP-Servers zusammen mit dem Port 389(LDAP)/636 (LDAP-Secure) fest. Geben Sie den Pfad des DNs mit dem Administratorkennwort des LDAP-Servers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



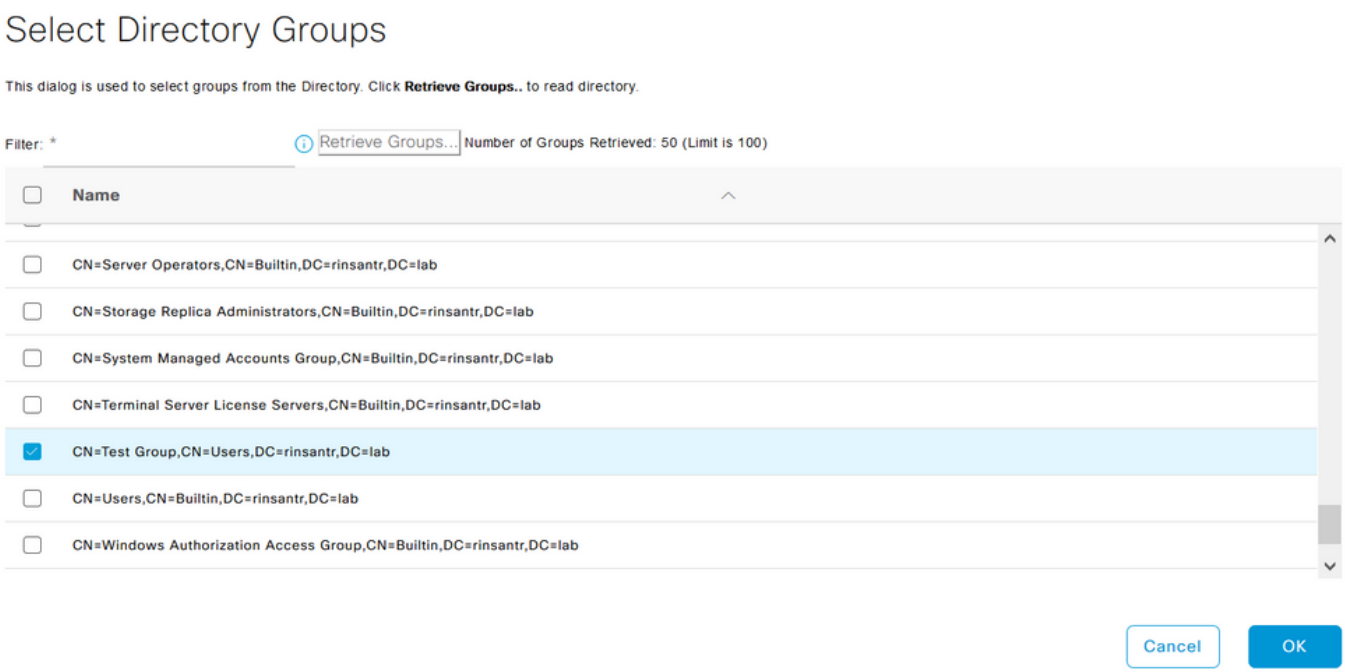
Navigieren Sie anschließend zur Registerkarte **Verzeichnisorganisation**, und klicken Sie auf **Naming Contexts**, um die richtige Organisationsgruppe des Benutzers auf Basis der Hierarchie der auf dem LDAP-Server gespeicherten Benutzer auszuwählen.

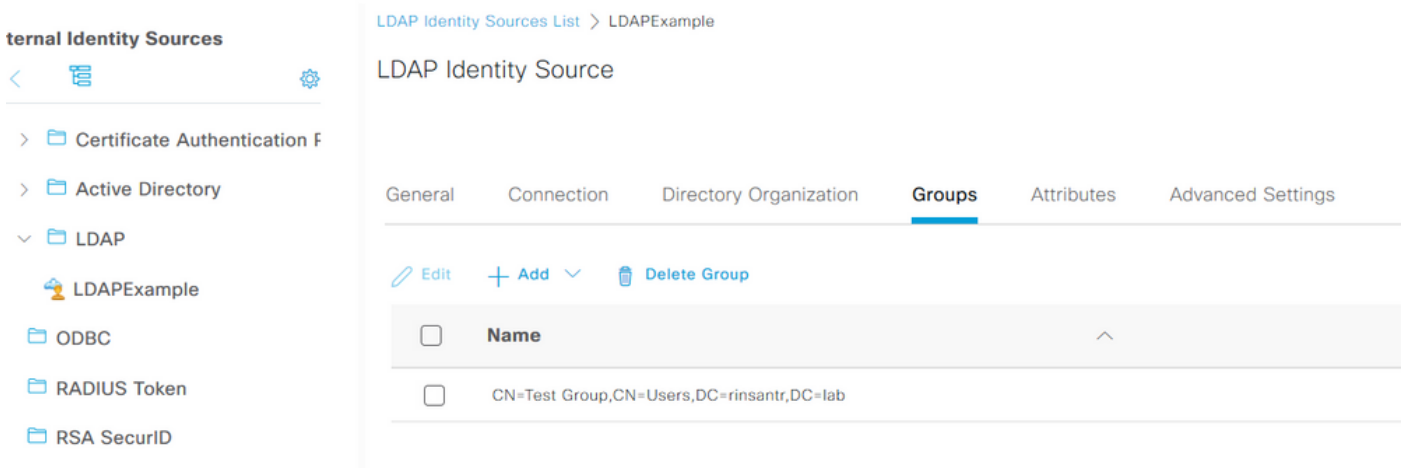


Klicken Sie auf **Test Bind to Server** unter der Registerkarte **Connection (Verbindung)**, um die Erreichbarkeit des LDAP-Servers von der ISE zu testen.



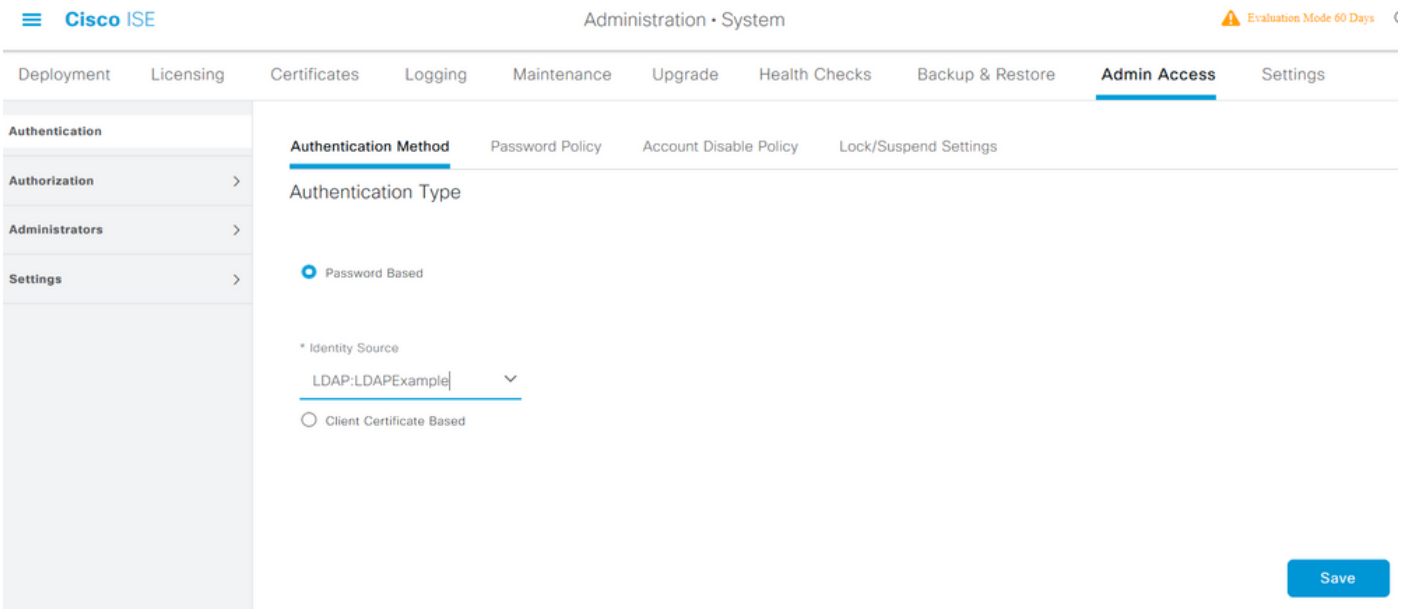
Navigieren Sie jetzt zur Registerkarte **Gruppen**, und klicken Sie auf **Hinzufügen > Gruppen aus Verzeichnis auswählen > Gruppen abrufen**. Importieren Sie mindestens eine Gruppe, der Ihr Administrator angehört, und klicken Sie auf **OK**, und klicken Sie dann auf **Speichern**.





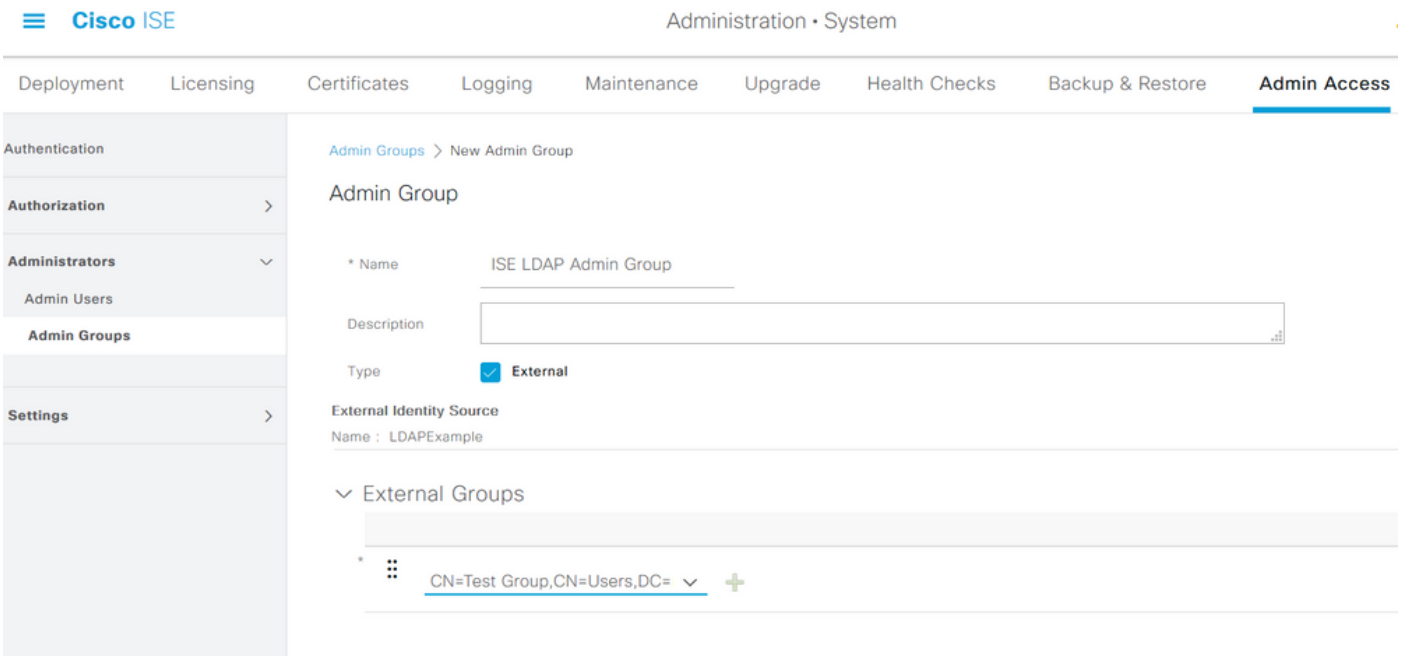
Administratorzugriff für LDAP-Benutzer aktivieren

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



Zuordnung der ISE-Admin-Gruppe zur LDAP-Gruppe

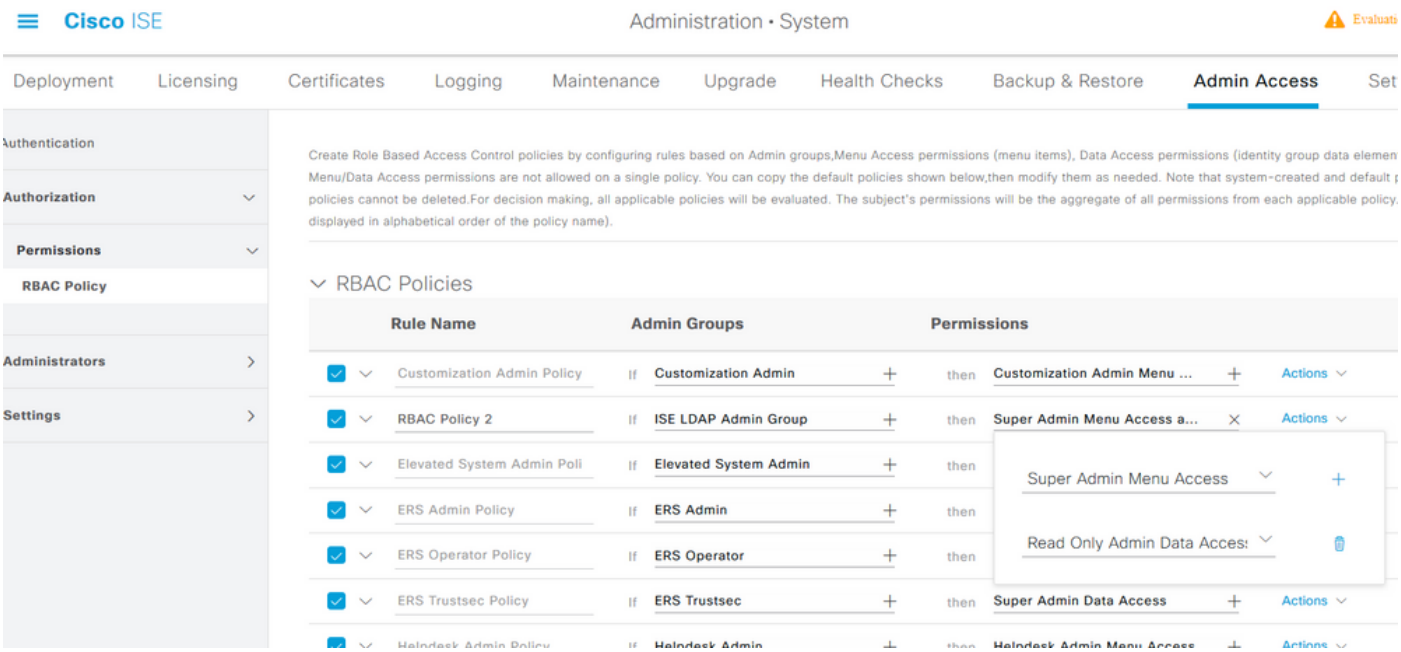
Auf diese Weise erhält der konfigurierte Benutzer Administratorzugriff, basierend auf der Autorisierung der RBAC-Richtlinien, die wiederum auf der LDAP-Gruppenmitgliedschaft des Benutzers basieren. Um eine Cisco ISE-Admin-Gruppe zu definieren und einer LDAP-Gruppe zuzuordnen, navigieren Sie zu **Administration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



RBAC-Berechtigungen für die Admin-Gruppe festlegen

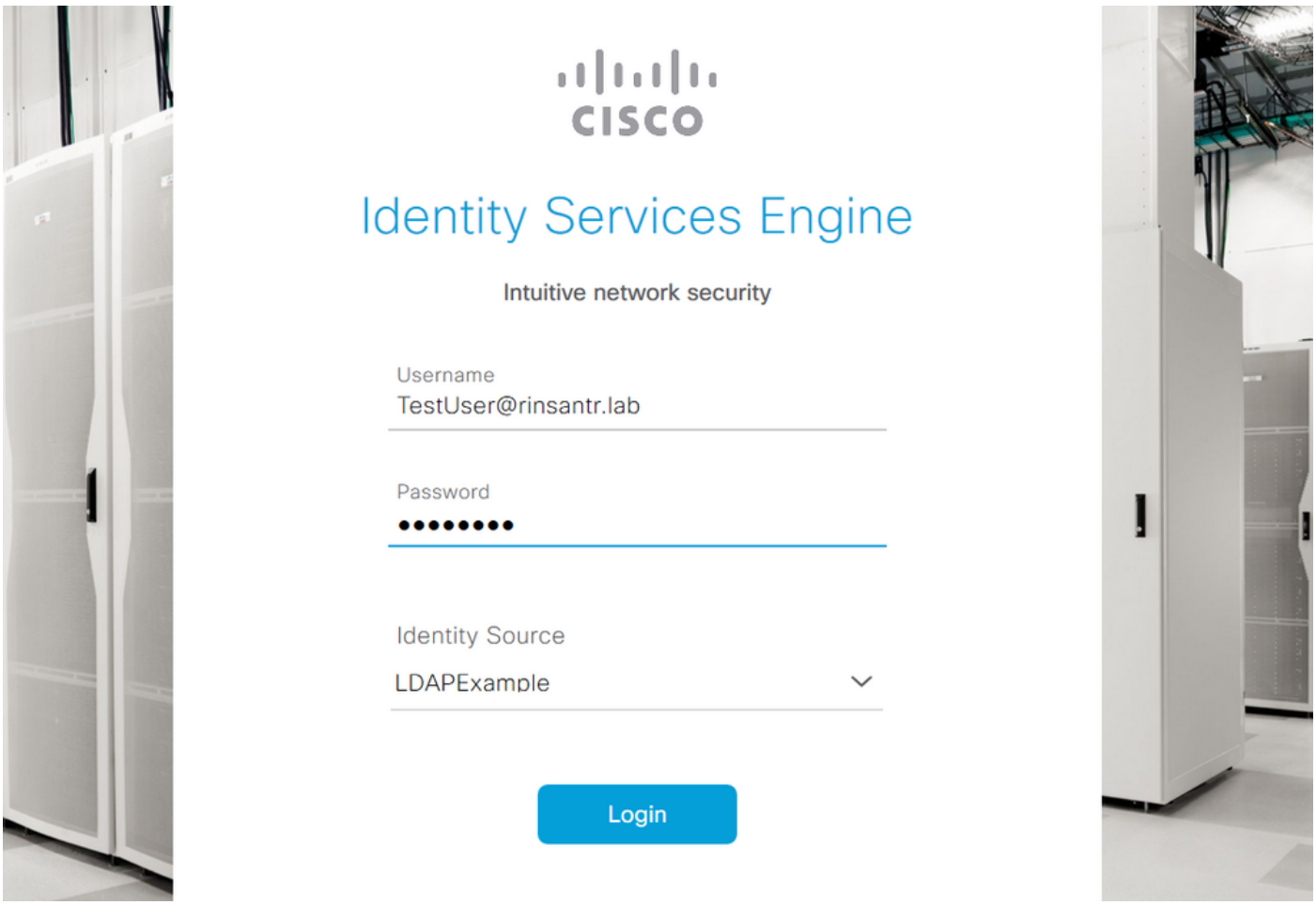
Um der im vorherigen Abschnitt erstellten Admin Group RBAC-Berechtigungen zuzuweisen, navigieren Sie zu **Administration > System > Admin Access > Authorization > RBAC Policy**. Wählen Sie im Dropdown-Menü **Aktionen** rechts die Option **Neue Richtlinie einfügen aus**. Erstellen Sie eine neue Regel,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

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



Zugriff auf ISE mit LDAP-Anmeldeinformationen und Überprüfen

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



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