# Konfigurationsbeispiel für den Zugriff auf das ISE-Administrationsportal mit AD-Anmeldeinformationen

### Inhalt

Einführung Voraussetzungen Verwendete Komponenten Konfigurieren Werden Sie Teil der ISE Verzeichnisgruppen auswählen Administratorzugriff für AD aktivieren Konfigurieren der AD-Gruppenzuordnung für die Admin-Gruppe RBAC-Berechtigungen für die Admin-Gruppe festlegen Zugriff auf ISE mit AD-Anmeldeinformationen Überprüfen Fehlerbehebung Zugehörige Informationen

## Einführung

Dieses Dokument beschreibt ein Konfigurationsbeispiel für die Verwendung von Microsoft Active Directory (AD) als externem Identitätsspeicher für den administrativen Zugriff auf die Verwaltungs-GUI der Cisco Identity Services Engine (ISE).

### Voraussetzungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Konfiguration der Cisco ISE Version 1.1.x oder höher
- Microsoft AD

#### Verwendete Komponenten

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

Cisco ISE Version 1.1.x

Windows Server 2008 Version 2

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

In diesem Abschnitt können Sie die Verwendung von Microsoft AD als externer Identitätsspeicher für den Administratorzugriff auf die Cisco ISE-Management-GUI konfigurieren.

#### Werden Sie Teil der ISE

- 1. Navigieren Sie zu Administration > Identity Management > External Identity Sources > Active Directory.
- 2. Geben Sie den AD-Domänennamen und den Identitätsspeichernamen ein, und klicken Sie auf **Beitreten**.
- 3. Geben Sie die Anmeldeinformationen des AD-Kontos ein, das Computerobjekte hinzufügen und Änderungen daran vornehmen kann, und klicken Sie auf **Konfiguration speichern**.

🍐 Home Operations 🔹 Policy 🔹 Ad 🔆 System 🏾 👰 Identity Management	ministration 🔹	ee Task Navigator
Identities Groups External Identity Source	s Identity Source Sequences Settings	
External Identity Sources	Adve Directory > AD1 Connector Advanced Settings Groups Attributes	
LDAP     BTA Standard	One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before Selections node for Test Connection	e a rejoin.
	□ ISE Node         ISE Node Role         Status           ☑ ISE-JKATYAL         STANDALONE         ☑ Connected to windomain.local	

#### Verzeichnisgruppen auswählen

- 1. Navigieren Sie zu Administration > Identity Management > External Identity Sources > Active Directory > Groups > Add > Select groups from Directory.
- 2. Importieren Sie mindestens eine AD-Gruppe, der Ihr Administrator angehört.

🝐 Home Operations 🔻 Policy 🔻 Admini	Istadon 🔻 😐 🔤 Task N	lavigator + 😣
🔆 System 🛛 👰 Identity Management 🖉 🖬	Activoris, Resources 🛛 🙀 Web Portal Management	
Identities Groups External Identity Sources	Identity Source Sequences Settings	
External Identity Sources	Adve Directory > AD1 Connection Advanced Settings Groups Attributes	
ELDAP (8) RADUS Token (8)	Name     Domain.local /Users/Domain Admins	
RSA Securit		

#### Administratorzugriff für AD aktivieren

Gehen Sie wie folgt vor, um die kennwortbasierte Authentifizierung für AD zu aktivieren:

- 1. Navigieren Sie zu Administration > System > Admin Access > Authentication.
- 2. Wählen Sie auf der Registerkarte Authentication Method die Option Password Based aus.
- 3. Wählen Sie AD aus dem Dropdown-Menü Identity Source aus.
- 4. Klicken Sie auf Änderungen speichern.

🛕 Home Operations 🕶 Policy 💌 Admin	stration 🔻	👓 Task Navigator 👻 🕙
😵 System 🛛 🖉 Identity Management 🛛 📟	Network Resources 🛛 😹 Web Portal Management	
Deployment Licensing Certificates Loggin	ng Maintenance Admin Access Settings	
Admin Access	Authentication Method     Password Policy       Authentication Type:     • Menthy Source       Image: Password Based     • Menthy Source       Olient Certificate Based	

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

Definieren Sie eine Cisco ISE-Admin-Gruppe, und ordnen Sie sie einer AD-Gruppe zu. Dadurch kann der Administrator anhand der Gruppenmitgliedschaft in AD die Berechtigungen für die rollenbasierte Zugriffskontrolle (Role Based Access Control, RBAC) festlegen.

- 1. Navigieren Sie zu Administration > System > Admin Access > Administrator Groups.
- 2. Klicken Sie in der Tabellenkopfzeile auf **Hinzufügen**, um den neuen Konfigurationsbereich "Admin Group" anzuzeigen.
- 3. Geben Sie den Namen für die neue Admin-Gruppe ein.
- 4. Aktivieren Sie im Feld Typ das Kontrollkästchen Extern.
- 5. 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) definiert.
- 6. Klicken Sie auf Änderungen speichern.

👌 Heme Operations 🔻 Policy 💌 Admi	nistration •	👓 Task Navigator 👻 🙆
🔆 System 🧏 Identity Management	Network Resources 😨 Web Portal Management	
Deployment Licensing Certificates Logg	ing Maintenance Admin Access Settings	
Admin Access	Admin Groups > ISE-Administration_AD1	
Authentication     Authentication     Authorization     Administration     Gadnin Users	Trama SE-Administration_ADI     Description     Type □ Internal ☑ External     External Identity Source     Name AD1	
<ul> <li>Admin Groups</li> <li>Religitusk Admin</li> <li>Edentityk Admin</li> <li>Stendministration_AD1</li> <li>Mini Admin</li> </ul>	External Groups     [Comain.local/Users/Domain Adn] 4	
Rebuck Device Admin	Save Reset	
System Admin     Settings		

#### RBAC-Berechtigungen für die Admin-Gruppe festlegen

Gehen Sie wie folgt vor, um den im vorherigen Abschnitt erstellten Administratorgruppen RBAC-Berechtigungen zuzuweisen:

- 1. Navigieren Sie zu Administration > System > Admin Access > Authorization > Policy.
- 2. Wählen Sie im Dropdown-Menü **Aktionen** rechts die Option **Neue Richtlinie einfügen**, um eine neue Richtlinie hinzuzufügen.
- 3. Erstellen Sie eine neue Regel mit dem Namen ISE\_Administration\_AD, ordnen Sie sie der im Abschnitt Enable Administrative Access for AD definierten Admin-Gruppe zu, und weisen Sie ihr Berechtigungen zu.Hinweis: In diesem Beispiel wird die Admin-Gruppe Super Admin genannt, die dem Standard-Admin-Konto entspricht.
- 4. Klicken Sie auf **Save Changes**, und die Bestätigung der gespeicherten Änderungen wird in der rechten unteren Ecke der GUI angezeigt.

💧 Home Operations 🔹 Policy 🔻	Adminis	stration 🔻				🕫 Task Navigator + 🧯
🔆 System 🛛 👙 Identity Management	i 💼 1	Network Resources 🛛 🛃 Web Po	rtal Management			
Deployment Licensing Certificates	Logging	g Maintenance Admin Acces	s Settings			
Admin Access	<u>م</u>	Create Role Dased Access Control points elements) and other conditions. Note that modify them as meeded. Note that syste will be evaluated. The subject's permissio alphabetical order of the policy name).	s by configuring rules t multiple Menu,Data n-created and defau ns will be the apgreg	s based on Admin groups, Men a Access permissions are not a ift policies cannot be updated, gate of all permissions from ea-	u Access permissions (nenu items), Data Ac lowed on a single policy. You can copy the o and default policies cannot be deleted. For h applicable policy. Permit overrides Deny.	coess permissions (identity group data default policies shown below, then decision making, all applicable policies (The policies are displayed in
Authentication		▼ RBAC Policies				
T Authoricalitari		Rule Name	/	Admin Groups	Permissions	
<ul> <li>Vernissians</li> </ul>		Helpdesk Admin Po	icy If	Helpdesk/Admin	<j> then</j>	容 Actions *
Policy     Administrators		Helpdesk Admin Menu Access	$\Leftrightarrow$			
Admin Liaans		Identity Admin Pol	cy If	Identity Admin	then	🔆 Actions +
* 🤮 Admin Groups		Identity Admin Menu Access	÷			
A Helpdesk Admin						-14
🥵 Identity Admin		<ul> <li>ISE administration_</li> </ul>	AD 1†	ISE-Administration_AD1	<i>⊲&gt; then</i>	督 Actions *
35 ISE-Administration_AD1		Super Admin Menu Access	0			

#### Zugriff auf ISE mit AD-Anmeldeinformationen

Gehen Sie wie folgt vor, um mit AD-Anmeldeinformationen auf die ISE zuzugreifen:

1. Melden Sie sich von der Verwaltungs-GUI ab.

- 2. Wählen Sie AD1 aus dem Dropdown-Menü Identity Source aus.
- 3. Geben Sie den Benutzernamen und das Kennwort aus der AD-Datenbank ein, und melden Sie sich an.



**Hinweis**: Die ISE verwendet standardmäßig den internen Benutzerspeicher, wenn AD nicht erreichbar ist oder die verwendeten Kontoanmeldeinformationen in AD nicht vorhanden sind. Dies erleichtert die schnelle Anmeldung, wenn Sie den internen Speicher verwenden, während AD für den Administratorzugriff konfiguriert ist.

### Überprüfen

Um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert, überprüfen Sie den authentifizierten Benutzernamen in der rechten oberen Ecke der ISE-GUI.



### Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

### Zugehörige Informationen

- <u>Cisco Identity Services Engine-Benutzerhandbuch, Version 1.1 Verwalten von Identitäten</u> <u>und Administratorzugriff</u>
- Technischer Support und Dokumentation Cisco Systems