# **ISE Administrative Portal Access with AD Credentials Configuration Example**



Document ID: 116503

Contributed by Jatin Katyal, Cisco TAC Engineer.

Sep 30, 2013

### Contents

Introduction Prerequisites Componenets Used Configure Join ISE to AD Select Directory Groups Enable Administrative Access for AD Configure the Admin Group to AD Group Mapping Set RBAC Permissions for the Admin Group Access ISE with AD Credentials Verify Troubleshoot Related Information

## Introduction

This document describes a configuration example for the use of Microsoft Active Directory (AD) as an external identity store for administrative access to the Cisco Identity Services Engine (ISE) management GUI.

## Prerequisites

Cisco recommends that you have knowledge of these topics:

- Configuration of Cisco ISE Versions 1.1.x or Later
- Microsoft AD

#### **Componenets Used**

The information in this document is based on these software and hardware versions:

- Cisco ISE Version 1.1.x
- Windows Server 2008 Release 2

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. If your network is live, make sure that you understand the potential impact of any command.

# Configure

Use this section in order to configure for the use of Microsoft AD as an external identity store for administrative access to the Cisco ISE management GUI.

#### Join ISE to AD

- 1. Navigate to Administration > Identity Management > External Identity Sources > Active Directory.
- 2. Enter the AD Domain Name and Identity Store Name, and click Join.
- 3. Enter the credentials of the AD account that can add and make changes to computer objects, and click *Save Configuration*.

🛕 Hama Operations 🔻	Policy 🔻 Admir	etation 💌 👘 Task Navigali
🔆 System 🏾 👰 Identity M	anagement 🔛	Aetwork Resources 😹 Web Portal Management
Identifies Groups Exten	nal Identity Sources	Identity Source Sequences Settings
External Identity Sources	- 	Adve Directory > AD1 Connection Advanced Settings Groups Attributes
Certificate Authentication Profil de Active Directory	u 📀	* Domain Name Domian.local
LDAP	8	One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before a rejoin. Selections node for Test Connection
RSA SecuriD		요즘 Ion 요즘 Leave 요즘 Test Connection 후
		ISE Node ISE Node Connected to, windownin.local ISE Node Role ISE NODE

#### **Select Directory Groups**

- 1. Navigate to Administration > Identity Management > External Identity Sources > Active Directory > Groups > Add > Select groups form Directory.
- 2. Import at least one AD Group to which your administrator belongs.

Identity Management       Network Resources       Yeb Portal Management         Identities       Groups       External Identity Sources       Identity Source Sequences       Settings         External Identity Sources       Identity Source Sequences       Settings         Identities       Connection       Advanced Settings       Groups         Identity Sources       Identity Sources       Groups       Attributes         Identity Sources       Identity Sources       Groups       Attributes         Identity Sources       Identity Sources       Groups       Attributes         Identity Sources       Identity Sources       Identity Sources       Identity Sources         Identity Sources       Identity Sour	🛕 Home Operations 🔻 Policy 🔻	Administration 💌	😐 Task Navigator 👻 🧯
Identities Groups External Identity Sources     External Identity Sources     Image: Source Section Strate     Control C	🔆 System 🛛 👰 Identity Management	🖬 Network Resources 🛛 🖳 Web Portal Management	
External Identity Sources	Identities Groups External Identity Sc	urces Identity Source Sequences Settings	
Connection Advanced Settings Groups Attributes Connection Profile Connection Profile Connection Profile Connection Advanced Settings Groups Attributes Connection Advanced Settings Groups Attributes Connection Profile Connection Advanced Settings Groups Attributes Connection Profile Connection Profile Connection Advanced Settings Groups Attributes Connection Advanced Settings Groups Attributes Connection Advanced Settings Groups Attributes Connection Profile Connec	External Identity Sources	Addws Directory > AD1	
Certificate Authentication Profile  Active Directory  Active Directory  Active Directory  Name  Name  Domain.local /Users/Domain Admins  Active Structure  Domain.local /Users/Domain Admins	<b>↓-</b> = =	Connection Advanced Settings Groups Attributes	
Active Directory     Image: Same and the sam	Certificate Authentication Profile	Add - XDelete Group	
LDAP     Image: Construction of the second description of the second d	2 Active Directory	Name	
RADUS Token     ®       RSA Securitio     ®	CDAP	Domain local Alsers/Damain Admins	
SA SeartD ®	RADOUS Token	3	
	RSA SecurID	8	

#### **Enable Administrative Access for AD**

Complete these steps in order to enable password-based authentication for AD:

- 1. Navigate to *Administration > System > Admin Access > Authentication*.
- 2. From the Authentication Method tab, select the Password Based option.
- 3. Select AD from the Identity Source drop-down menu.
- 4. Click Save Changes.

🛕 Home Operations 🔻 Policy 🔻 Admin	straton 🔻	👓 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         ····································	

#### Configure the Admin Group to AD Group Mapping

Define a Cisco ISE Admin Group and map it to an AD group. This allows authorization to determine the Role Based Access Control (RBAC) permissions for the administrator based on group membership in AD.

- 1. Navigate to *Administration > System > Admin Access > Administrators > Admin Groups*.
- 2. Click *Add* in the table header in order to view the new Admin Group configuration pane.
- 3. Enter the name for the new Admin group.
- 4. In the Type field, check the *External* check box.
- 5. From the *External Groups* drop–down menu, select the AD group to which you want this Admin Group to map, as defined in the Select Directory Groups section.
- 6. Click Save Changes.

🛕 Home Operations 🔻 Policy 💌 Adr	ninstration 🔹	👓 Task Navigator 👻 🙆
🔆 System 🦉 Identity Management 🕴	🖬 Network Resources 🛛 😨 Web Portal Management	
Deployment Licensing Certificates Log	iging Maintenance Admin Access Settings	
Admin Access	Admin Group > ISE-Administration_AD1  Admin Group	
High     High       High     Authoritation       High     Authoritation       High     Authoritation       High     Authoritation       High     Authoritation       High     Authoritation	Description	
<ul> <li>Admin Groups</li> <li>Helpslack Admin</li> <li>Lidentity Admin</li> <li>Ste-Administration_AD1</li> <li>Not Admin</li> </ul>	▼ External Groups     * ∰ [Domain.local/Users/Domain Admon] 4	
Le Network Device Admin Le Poley Admin Le REAC Admin	Save Reset	
System Admin		

#### Set RBAC Permissions for the Admin Group

Complete these steps in order to assign RBAC permissions to the Admin Groups created in the previous section:

- 1. Navigate to Administration > System > Admin Access > Authorization > Policy.
- 2. From the *Actions* drop-down menu on the right, select *Insert New Policy Below* in order to add a new policy.
- 3. Create a new rule called *ISE\_administration\_AD*, map it with the Admin Group defined in the Enable Administrative Access for AD section, and assign it permissions.

*Note*: In this example, the Admin Group called *Super Admin* is assigned, which is equivalent to the standard admin account.

4. Click *Save Changes*, and confirmation of the changes saved are displayed in the lower-right corner of the GUI.



#### Access ISE with AD Credentials

Complete these steps in order to access ISE with AD credentials:

- 1. Log out of the administrative GUI.
- 2. Select *AD1* from the *Identity Source* drop–down menu.
- 3. Enter the username and password from the AD database, and log in.

	Identity Se	ervices Engine	
	Username	iseadmin	
	Password	•••••	_
	Identity Source	AD1 Login Remember username	
		Problem logging in?	
0 1013 Carp Statement Into Carp Carp Statement and Carp Statement		adamatics of Case 5 stress las	

*Note*: ISE defaults to the internal user store in the event that AD is unreachable, or the account credentials used do not exist in AD. This facilitates quick log in if you use the internal store while AD is configured for administrative access.

# Verify

In order to confirm that your configuration works properly, verify the authenticated username at the top-right corner of the ISE GUI.



### Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

### **Related Information**

- Cisco Identity Services Engine User Guide, Release 1.1 Managing Indentities and Admin Access
- Technical Support & Documentation Cisco Systems

Updated: Sep 30, 2013

Document ID: 116503