



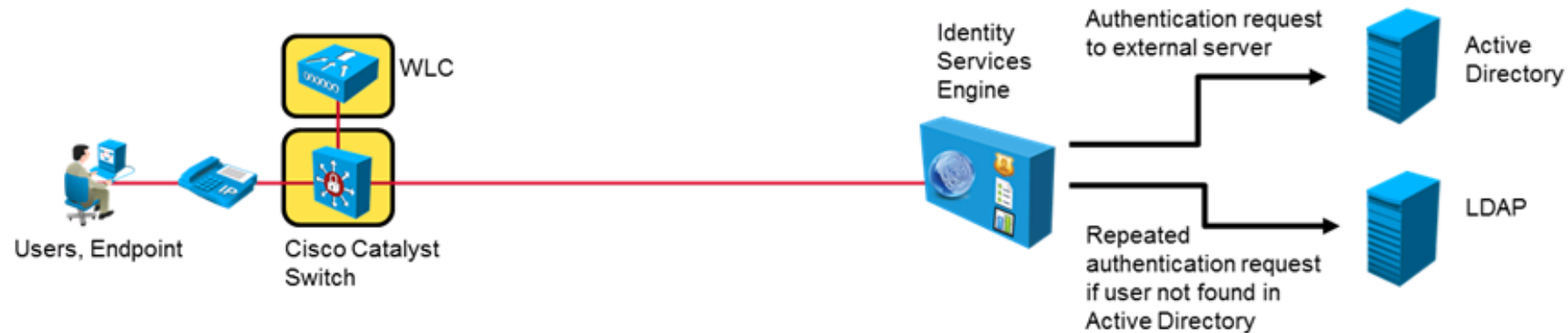
# Cisco ISE External Authentication

## Cisco ISE Fundamentals

Ahmed Sultan  
Senior Network Security Engineer  
[ahmedsultan.me/about](http://ahmedsultan.me/about)

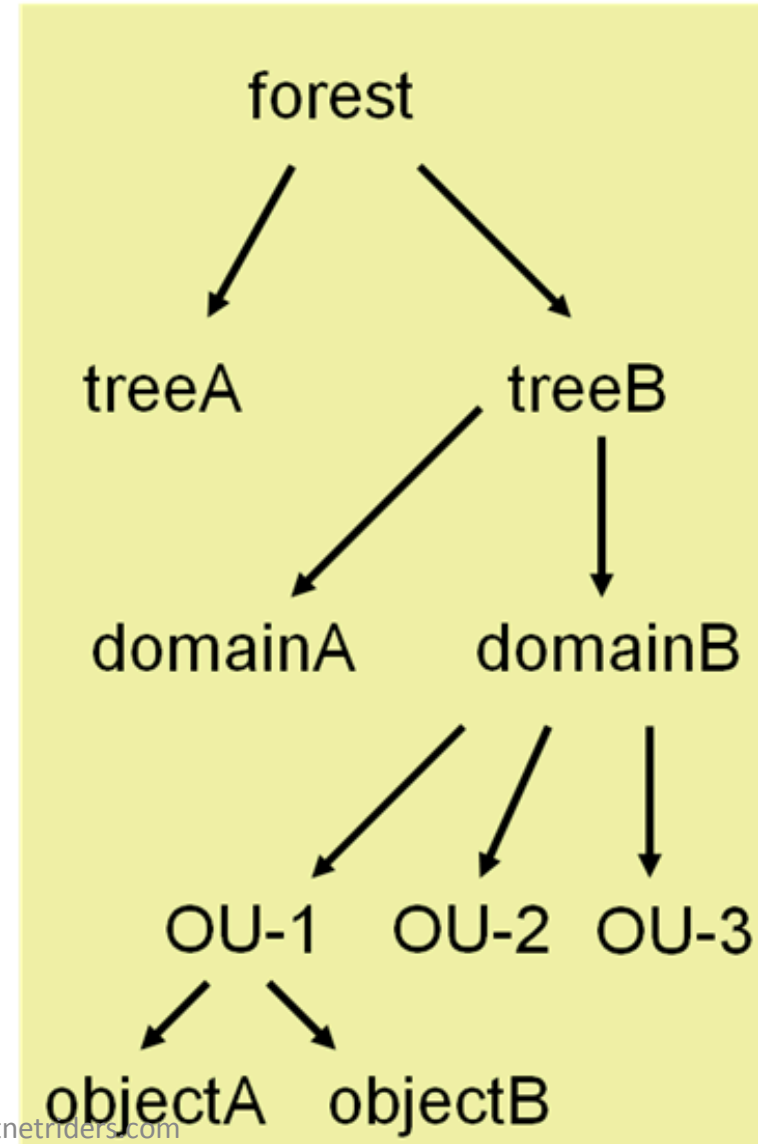
# External Authentication

- Cisco ISE can authenticate clients against the following:
  - A single authentication source
  - A sequence of authentication sources
- Supported external authentication sources include Active Directory, LDAP, RADIUS, and RSA servers



# Active Directory

- Widely deployed directory structure
  - Hierarchical format that allows logical grouping of users or devices
  - Can be used to assign permissions to users, network devices, and object groups
- Requires accurate time
  - Max 5 minutes difference between ISE and AD
- Firewalling constraints between Cisco ISE and Active Directory:
  - Certain ports need to be opened
  - No support for NAT



# Authentication Methods with Active Directory

- Most common authentication methods are supported in a Cisco ISE with Active Directory integration.
- EAP-TLS and PEAP-TLS use client-side certificates.
  - Active Directory records may include one or more certificates.
  - Cisco ISE can retrieve these certificates and use them to verify the identity of the user or machine.

PAP/ASCII

MS-CHAPv1

MS-CHAPv2

EAP-TLS

LEAP

PEAP

PEAP-TLS

EAP-FAST

EAP-GTC

# AD-Derived Group Membership

- Users belong to user groups
- Group membership improves manageability
  - Privileges assigned to user groups
- For domain users:
  - Group membership defined in AD
  - Groups downloaded from the AD
  - Group membership used in ISE policy decisions

## Select Directory Groups

This dialog is used to select groups from the Directory. Click **Retrieve Groups..** to read directory. Use \* for wildcard search (i.e. admin\*). Search filter applies to group name and not the fully qualified path.

Domain:

Filter:   Number of Groups Retrieved: 46 (Limit is 100)

<input type="checkbox"/> Name	Group Type
<input type="checkbox"/> secure-x.local/DomainGroups/Contractors	GLOBAL
<input type="checkbox"/> secure-x.local/DomainGroups/Employees	GLOBAL

# Active Directory Integration Procedure

1. Configure Active Directory domain name and store name in Cisco ISE
2. Test server connection (optional)
3. Join Cisco ISE nodes to the directory
4. Select groups from the directory (optional)

# Configure AD Domain and Store

- Enter domain name of the Active Directory server.
- Enter a friendly identity store name.
- Save the changes.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes links for Home, Operations, Policy, Administration, and Setup Assistant. The left sidebar shows the navigation menu with categories like System, Identity Management, Network Resources, Web Portal Management, and Feed Service. Under Identity Management, the 'External Identity Sources' tab is selected, showing a list of sources: Certificate Authentication Profile, Active Directory (selected), LDAP, RADIUS Token, and RSA SecurID.

The main content area is titled 'Active Directory > AD1' and has tabs for Connection, Advanced Settings, Groups, and Attributes. The 'Connection' tab is active, displaying instructions for configuring Active Directory:

- To configure Active Directory:
- First enter the required fields: the **Domain Name** to connect to and the **Identity Store Name** to refer to Active Directory in other pages, and click submit to commit the Active Directory configuration to all nodes in the ISE deployment.
- After the configuration has been submitted, then Join or Leave operations must be performed.

Below the instructions, there are two input fields:

- \* Domain Name:
- \* Identity Store Name:

A note states: '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. Select one node for Test Connection.'

At the bottom, there are two buttons: 'Save Configuration' and 'Delete Configuration'.



# Test AD Connection

- Click **Test Connection** and select **Basic** or **Detailed Test**
- Must have Super Admin or System Admin role

The screenshot shows the 'Active Directory > AD1' interface. The 'Connection' tab is active, displaying fields for 'Domain Name' (secure-x.local) and 'Identity Store Name' (AD1). Below these fields, a message states: '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. Select one node for Test Connection.' The 'Test Connection' button is highlighted, and a dropdown menu is open, showing 'Basic Test' and 'Detailed Test'. The 'Detailed Test' option is selected. Below the dropdown, a table lists nodes for testing. The first node, 'ise.secure-x.local', is selected with a checkmark. The 'ISE Node Role' is 'STANDALONE'. An arrow points from the 'Detailed Test' option to a separate window titled 'Detailed Test Connection Results'. This window displays the following information:

**Detailed Test Connection Results**

Result for ISE node: **ise.secure-x.local**  
Status: **SUCCESS**

adinfo (CentrifyDC 4.6.0-113)

**Host Diagnostics**  
uname: Linux ise 2.6.18-348.4.1.el5 #1 SMP Fri Mar 22 05:41:51 EDT 2013 x86\_64  
OS: Red Hat Enterprise Linux Server  
Version: 5.8 (Tikanga)  
Number of CPUs: 4

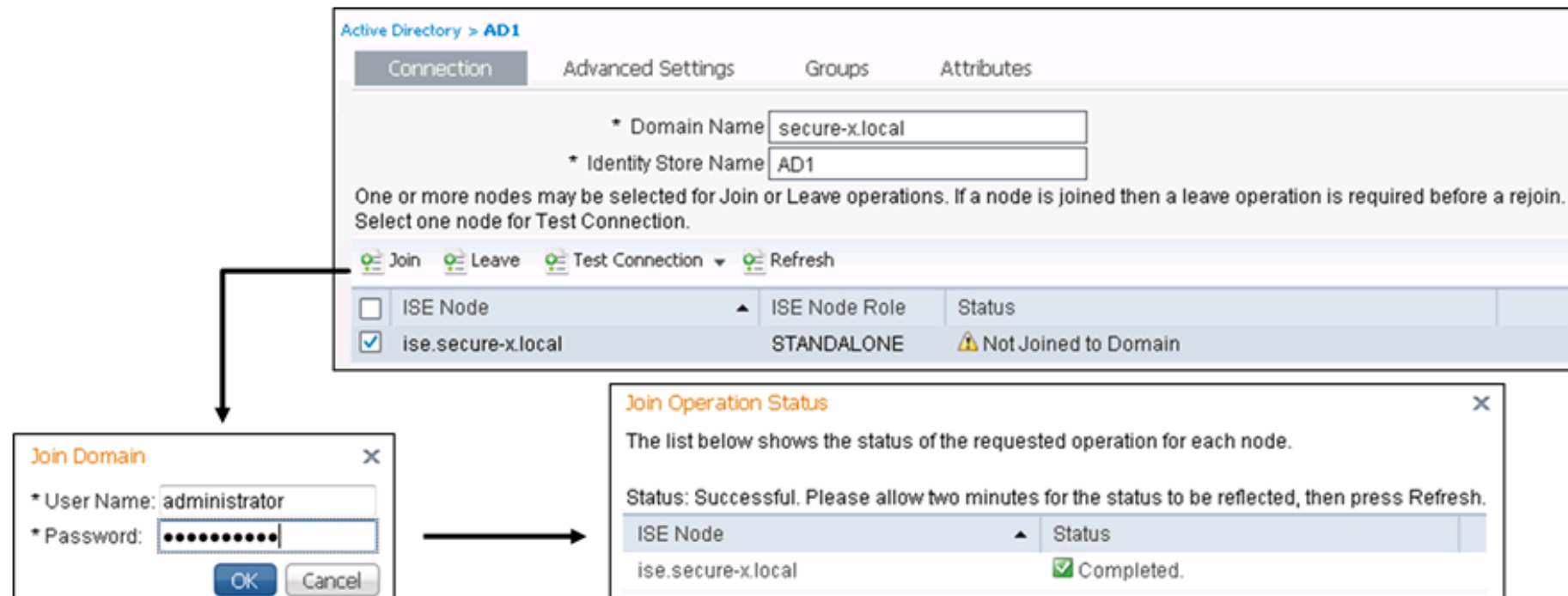
**IP Diagnostics**  
Local host name: ise  
Local IP Address: 10.10.2.20  
FQDN host name: hq-ise.secure-x.local

**Domain Diagnostics**  
Domain: secure-x.local



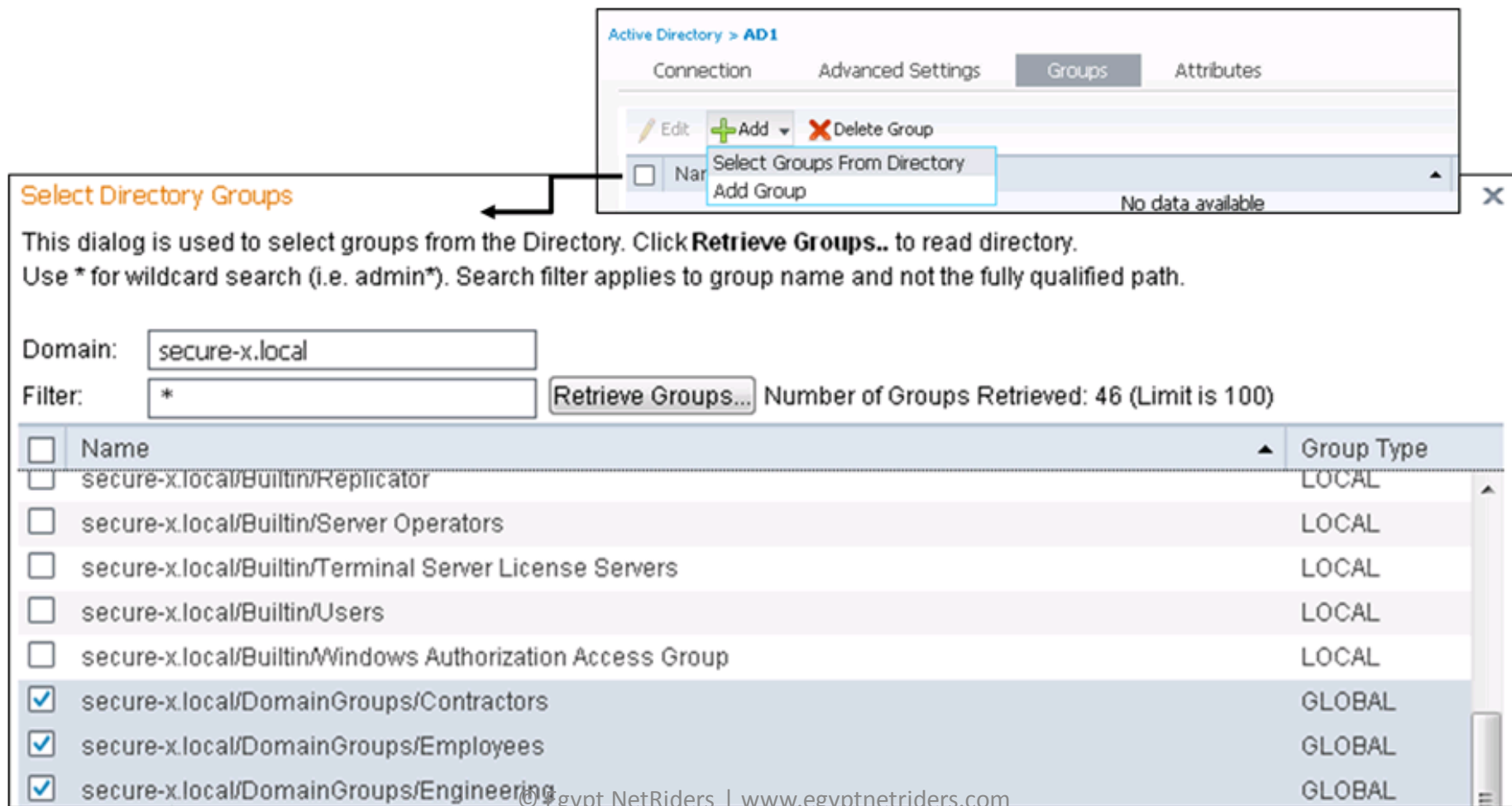
# Join Active Directory

- Creating the connection does not automatically join the AD
- Join one or multiple nodes in a single step
- Click **Join** and provide the Active Directory username and password



# Select Groups from Directory

- Import groups for use in policy conditions and rules
- Later changes in AD are not automatically reflected in ISE



**Select Directory Groups**

This dialog is used to select groups from the Directory. Click **Retrieve Groups..** to read directory.  
Use \* for wildcard search (i.e. admin\*). Search filter applies to group name and not the fully qualified path.

Domain:

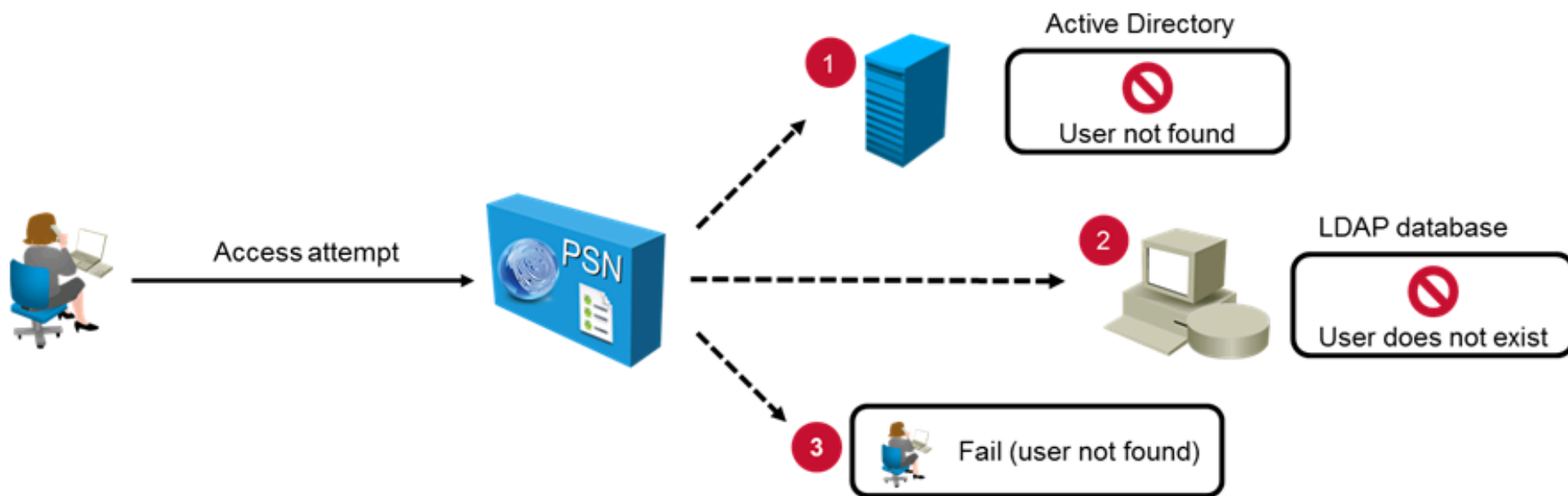
Filter:   Number of Groups Retrieved: 46 (Limit is 100)

<input type="checkbox"/>	Name	Group Type
<input type="checkbox"/>	secure-x.local/Builtin/Replicator	LOCAL
<input type="checkbox"/>	secure-x.local/Builtin/Server Operators	LOCAL
<input type="checkbox"/>	secure-x.local/Builtin/Terminal Server License Servers	LOCAL
<input type="checkbox"/>	secure-x.local/Builtin/Users	LOCAL
<input type="checkbox"/>	secure-x.local/Builtin/Windows Authorization Access Group	LOCAL
<input checked="" type="checkbox"/>	secure-x.local/DomainGroups/Contractors	GLOBAL
<input checked="" type="checkbox"/>	secure-x.local/DomainGroups/Employees	GLOBAL
<input checked="" type="checkbox"/>	secure-x.local/DomainGroups/Engineering	GLOBAL

© Egypt NetRiders | www.egyptnetriders.com

# Cisco ISE Identity Source Sequence

- A sequence of identity databases that is used for authentication
- Always proceed to next store if user not found
- Optionally proceed to next store if current source failed
  - Fallback behavior defined in the Advanced Search List settings
  - Example illustrates a case with “Proceed to the next store in sequence” option if the store cannot be accessed for authentication



# Configure Identity Source Sequence

**CISCO Identity Services Engine**

Home Operations Policy Administration

System Identity Management Network Resources Web Portal Management Feed Service

Identities Groups External Identity Sources **Identity Source Sequences** Settings

\* Name

Description

## ▼ Certificate Based Authentication

☐ Select Certificate Authentication Profile

## ▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available		Selected
Internal Endpoints Guest Users	<div>&gt; &lt; &gt;&gt; &lt;&lt;</div>	AD1 Internal Users <div>⬆ ⬆ ⬇ ⬇</div>

Ordered list of identity sources

## ▼ Advanced Search List Settings

Select the action to be performed if a selected identity store cannot be accessed for authentication

- ☐ Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- ☒ Treat as if the user was not found and proceed to the next store in the sequence

Jump to next store if a store unavailable

## Configure Identity Source Sequence (Cont.)

- By default, processing stops after the identity source cannot be accessed.
  - Do not access other stores in the sequence
  - Sets the Authentication Status to Process Error
- To enable rollover:
  - Choose 2nd radio box
  - Treat as if the user was not found and proceed to the next store in the sequence

# Apply Identity Source Sequence

- Identity source sequence referenced by authentication rules
- Options independent from chaining behavior within the sequence

**Authentication Policy**

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ☐ Simple ☒ Rule-Based

**Rules:**

- ☒ MAB : If Wired\_MAB OR Wireless\_MAB Allow Protocols : Default Network Access and [Edit](#)
- ☒ Default : use Internal Endpoints
- ☒ Dot1X : If Wired\_802.1X OR Wireless\_802.1X Allow Protocols : Default Network Access and [Done](#)
- ☒ Default : Use **AD\_Internal** [Actions](#)
- ☒ Default Rule (If no match) : Allow Protocols [Edit](#)

**AD\_Internal Options:**

- Identity Source: AD\_Internal
- If authentication failed: Reject
- If user not found: Reject
- If process failed: Drop

Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected.



# Verify External Authentication

- Details in the authentication pages show the actual source.

The screenshot displays the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Operations', and 'Policy'. The 'Operations' tab is active, showing 'Authentications', 'Reports', 'Endpoint Protection Service', and 'Troubleshoot'. Below this, there are three status indicators: 'Misconfigured Suppliants' (0), 'Misconfigured Network Devices' (0), and 'RADIUS' (0). The main content area shows a table of authentication sessions. The table has columns for Time, Status, Details, Repeat Count, Identity, Device Port, Event, Auth Method, and Authentication Protocol. The table shows two sessions: one at 2013-11-25 21:19:18.299 with a status of 'i' and another at 2013-11-25 21:19:17.550 with a status of '✓'. The second session is highlighted in green and has an arrow pointing to its details. The details panel on the right, titled 'Authentication Details', shows the following information:

Authentication Details	
Source Timestamp	2013-11-25 21:19:17.549
Received Timestamp	2013-11-25 21:19:17.55
Policy Server	ise
Event	5200 Authentication succeeded
Failure Reason	
Resolution	
Root cause	
Username	sales1
User Type	
Endpoint Id	A0:36:9F:1A:3B:B1
Endpoint Profile	
IP Address	10.10.9.11
Identity Store	AD1
Identity Group	
Audit Session Id	0A0A01020000172113E2B5E5



# Summary

- Cisco ISE can authenticate the users against the local or an external database.
- Active Directory is a widely used external user database.
- Cisco ISE joins the Active Directory to authenticate the domain users and computers.
- Identity source sequence defines an authentication chain.
- Identity source sequence can be referenced by the authentication policy rules.