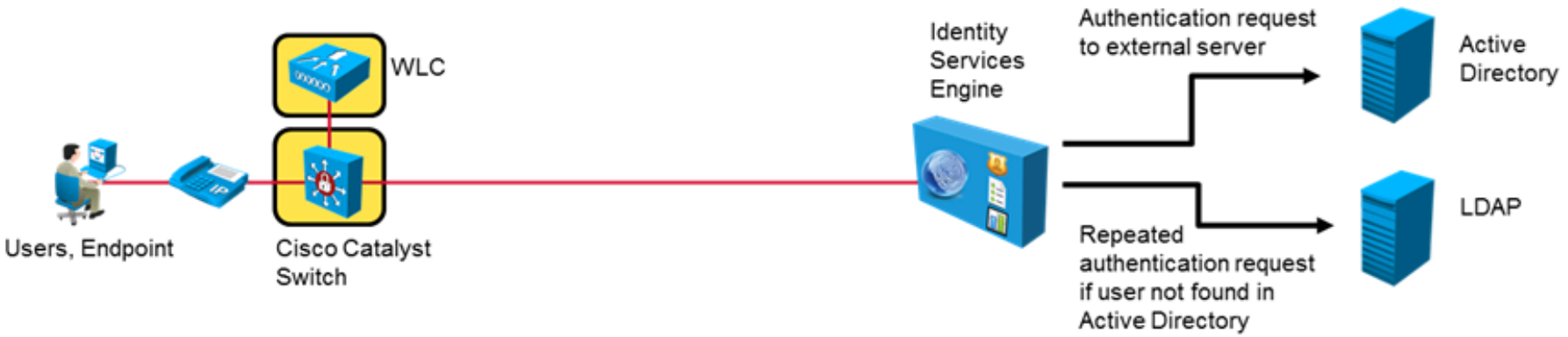
Cisco ISE External Authentication

Cisco ISE Fundamentals

Ahmed Sultan
Senior Network Security Engineer
ahmedsultan.me/about

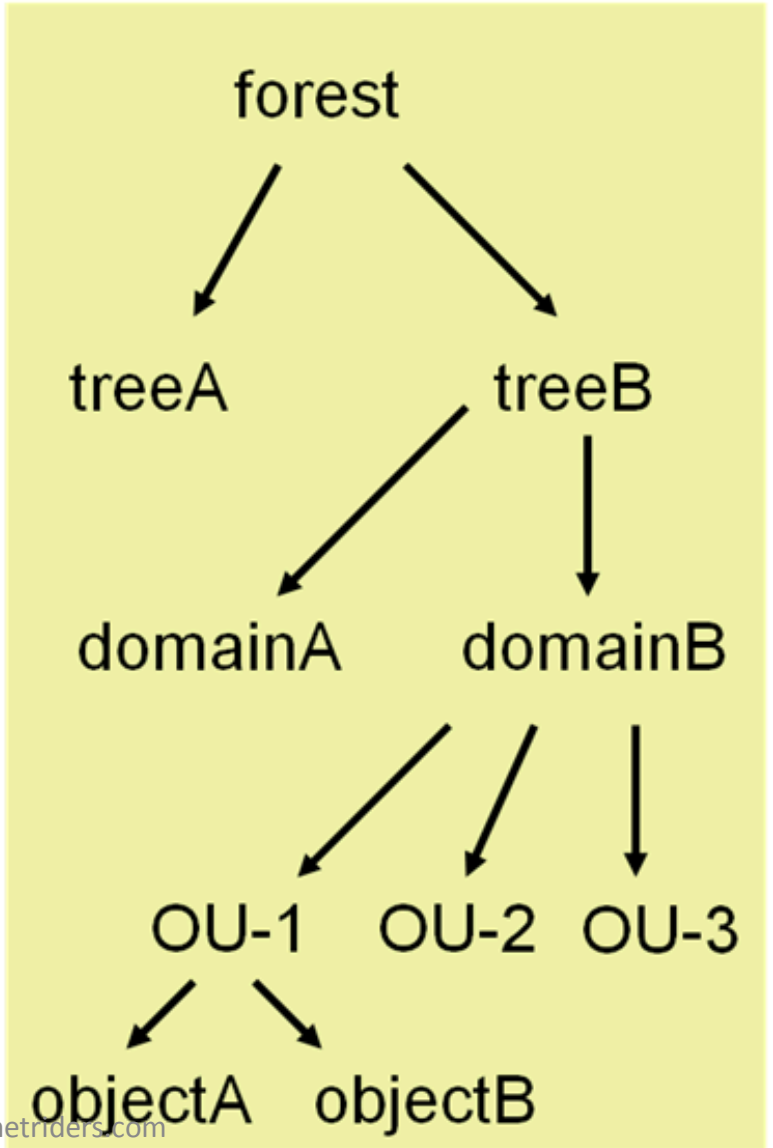
External Authentication

- 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



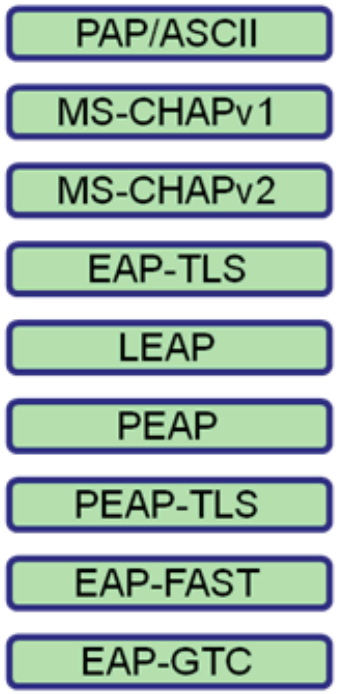
Active Directory

- 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



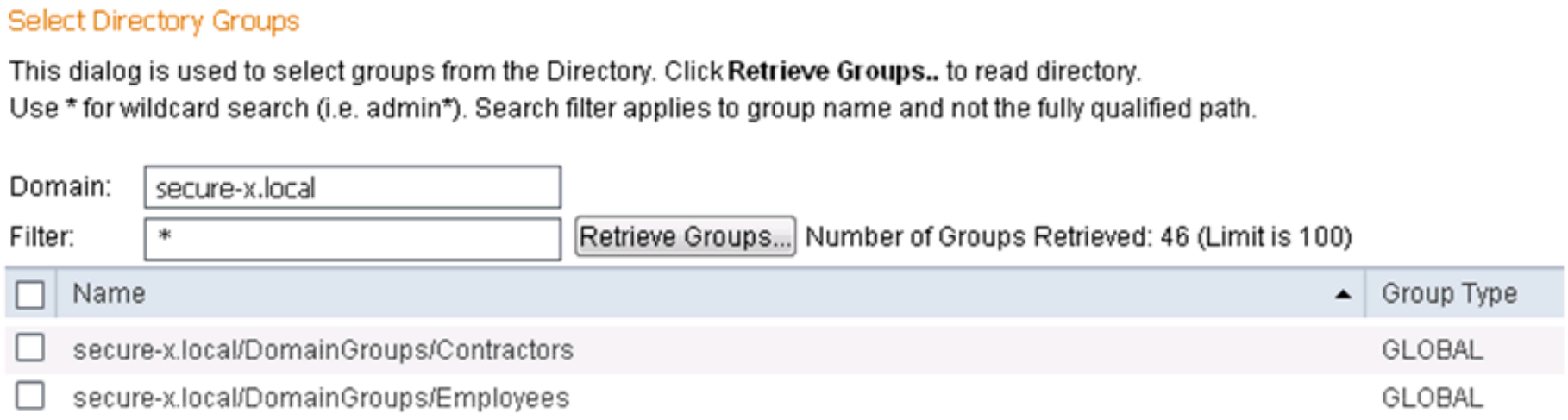
Authentication Methods with Active Directory

- 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.



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

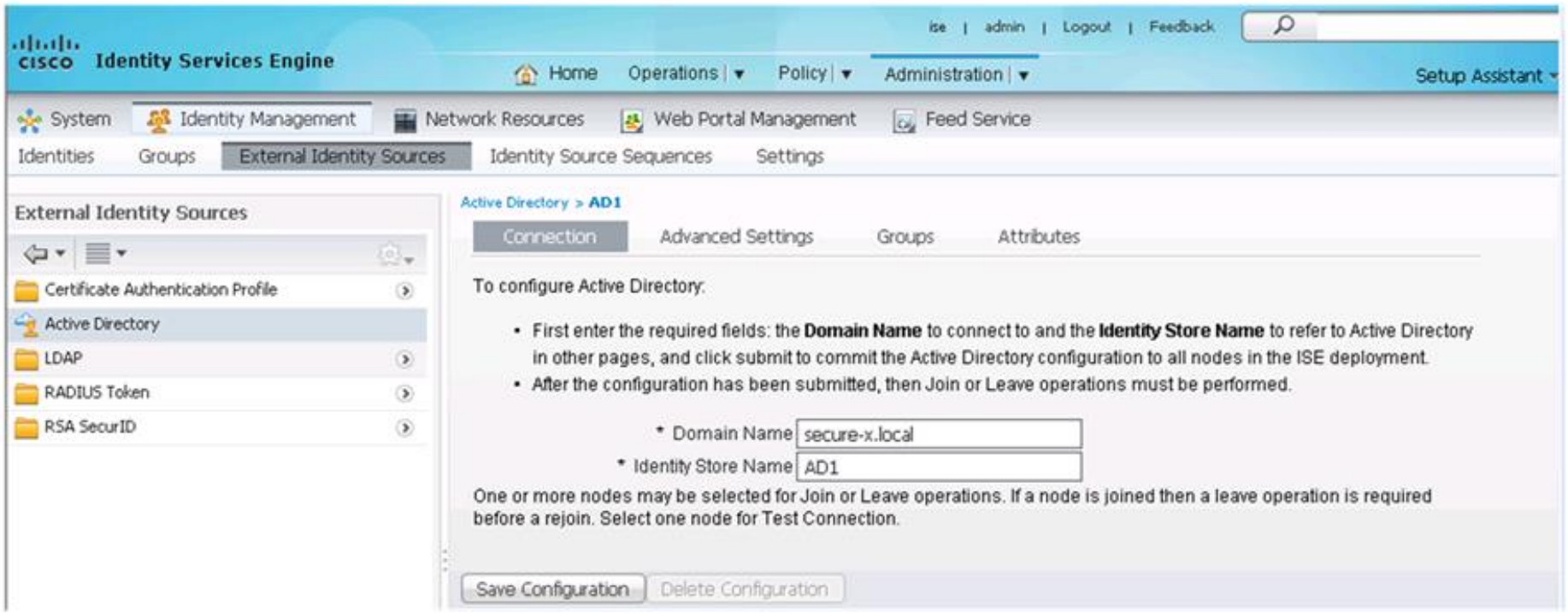


Active Directory Integration Procedure

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)

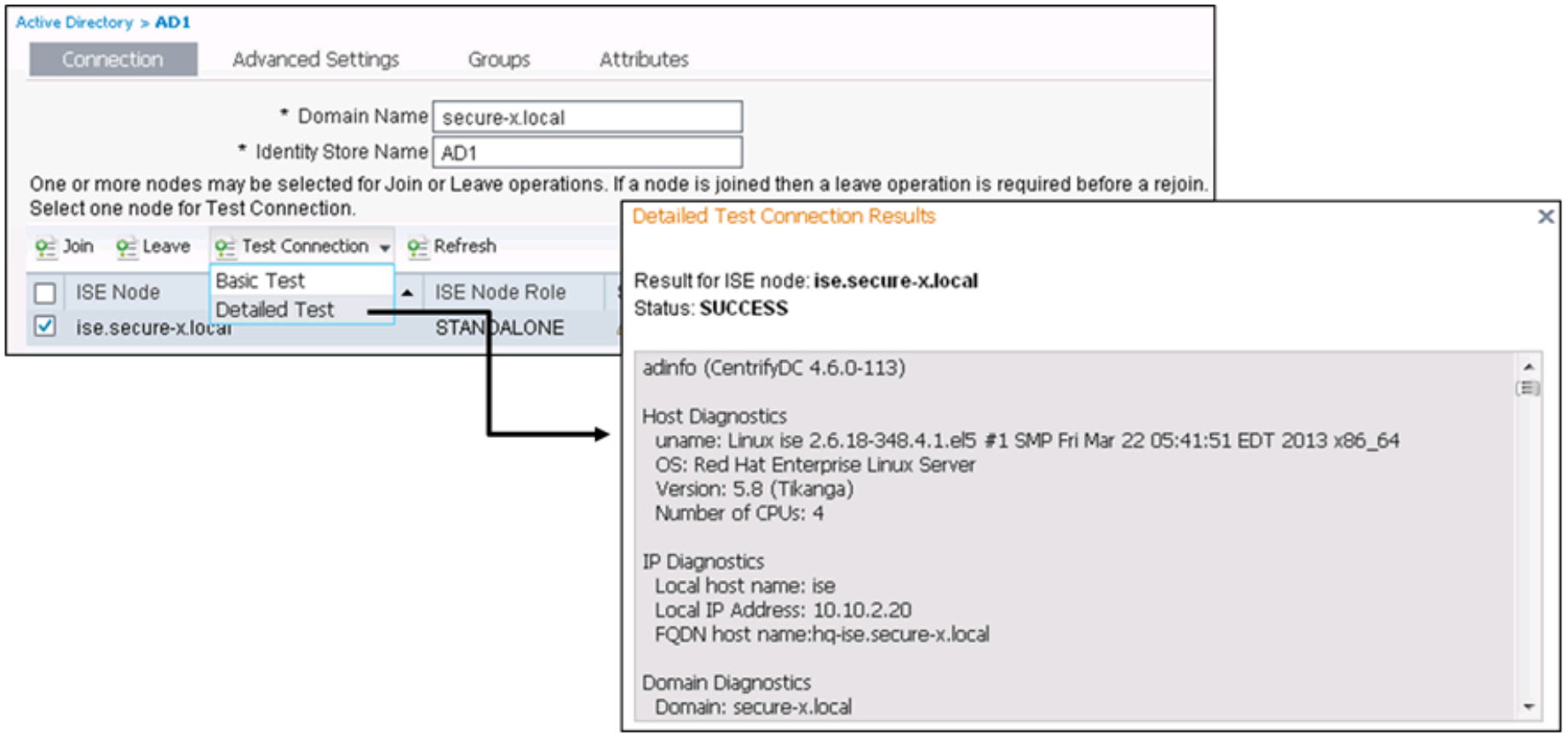
Configure AD Domain and Store

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



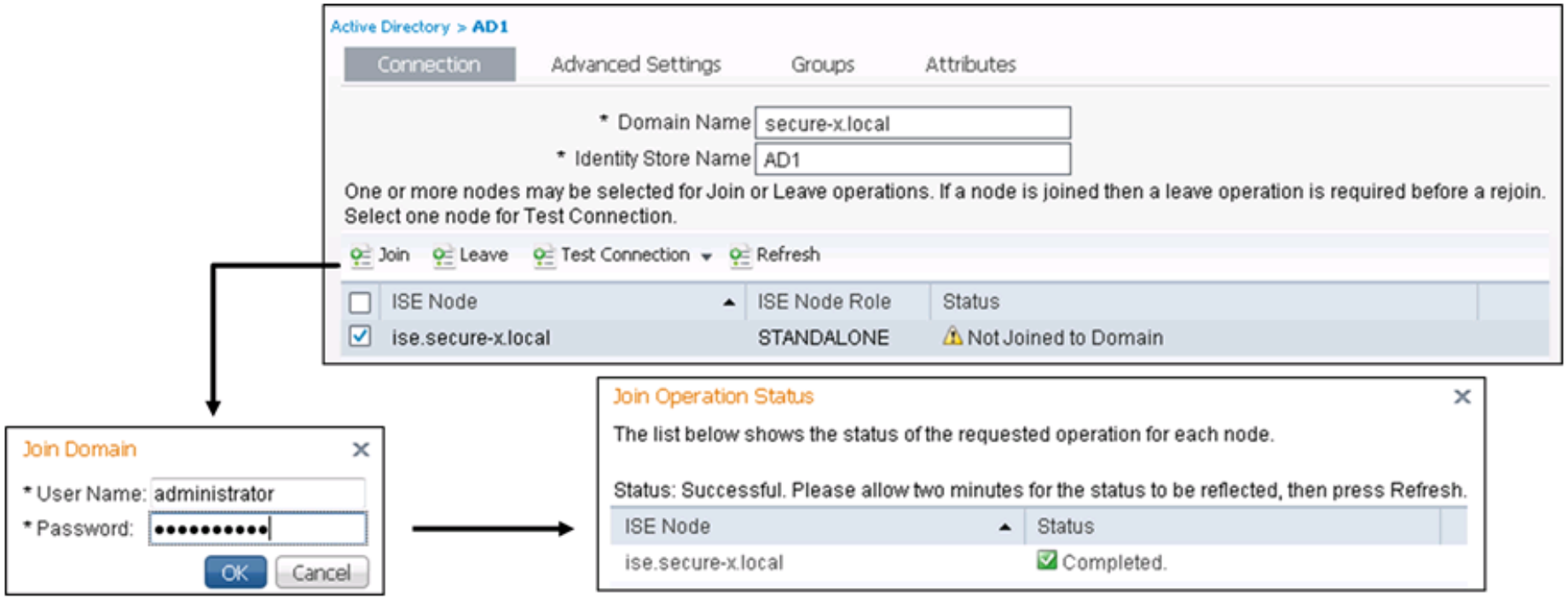
Test AD Connection

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



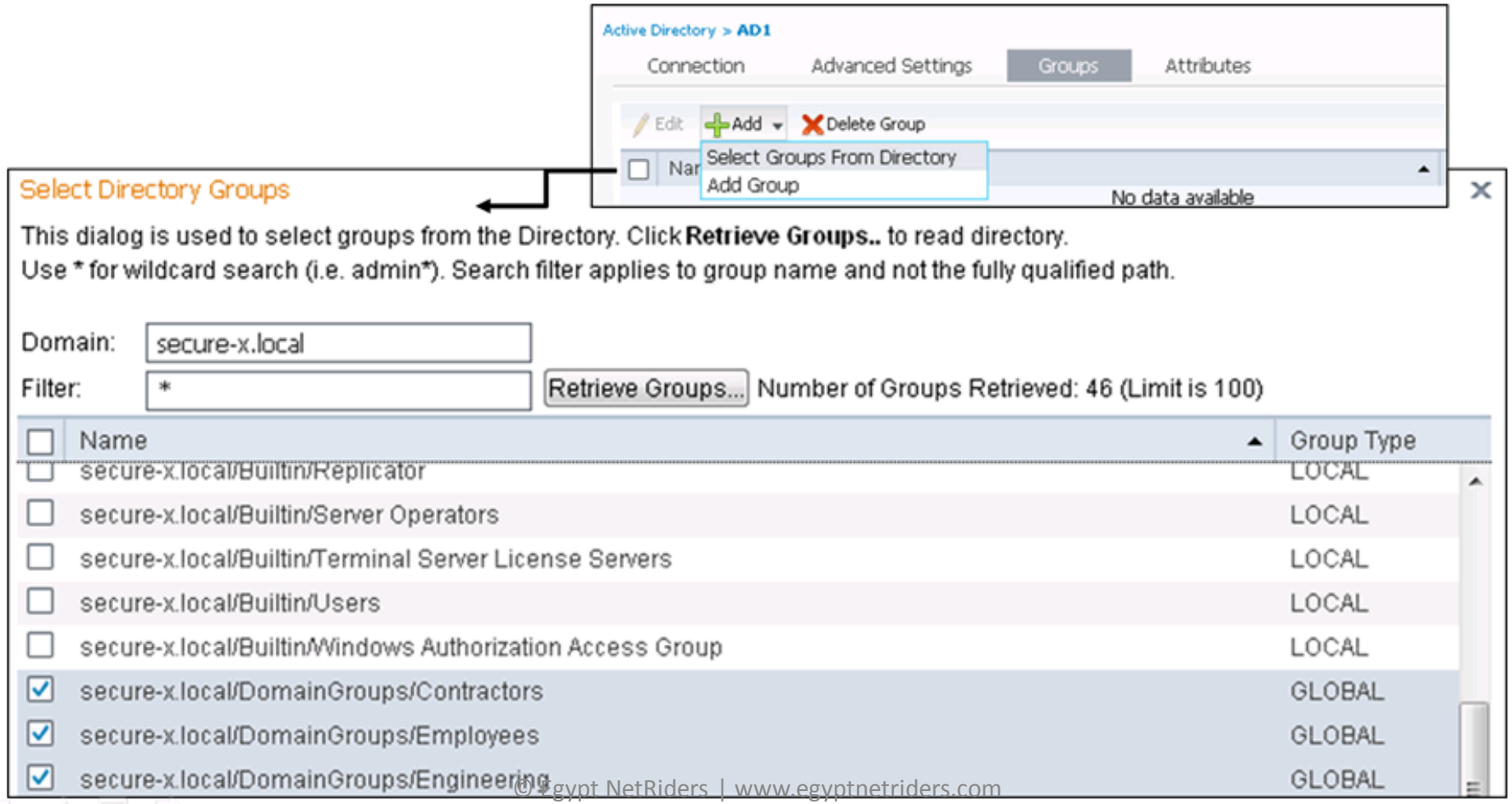
Join Active Directory

- 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



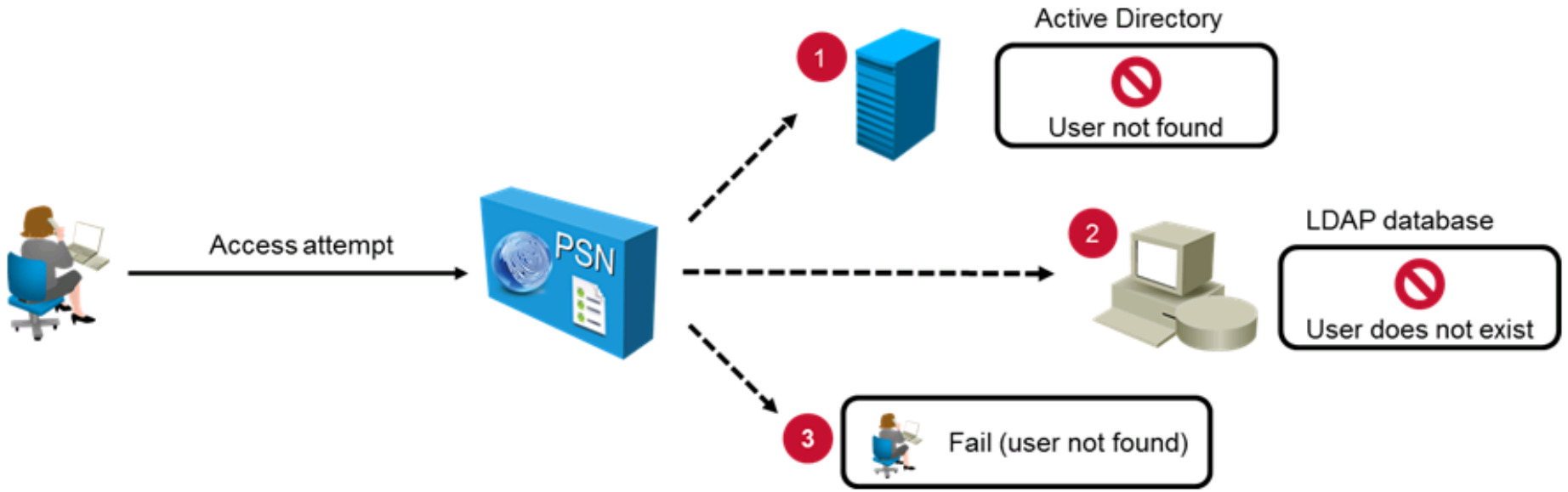
Select Groups from Directory

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

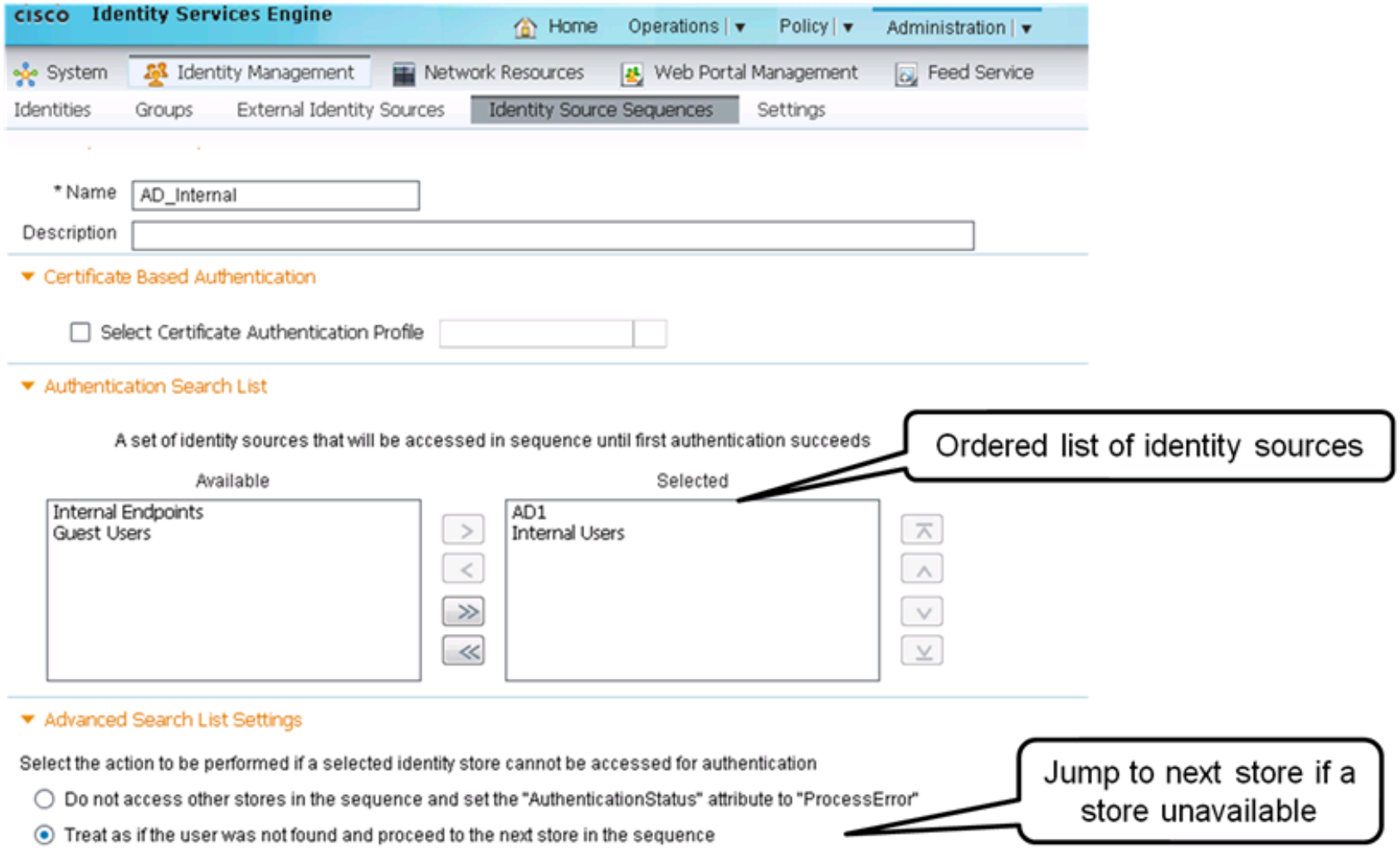


Cisco ISE Identity Source Sequence

- 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

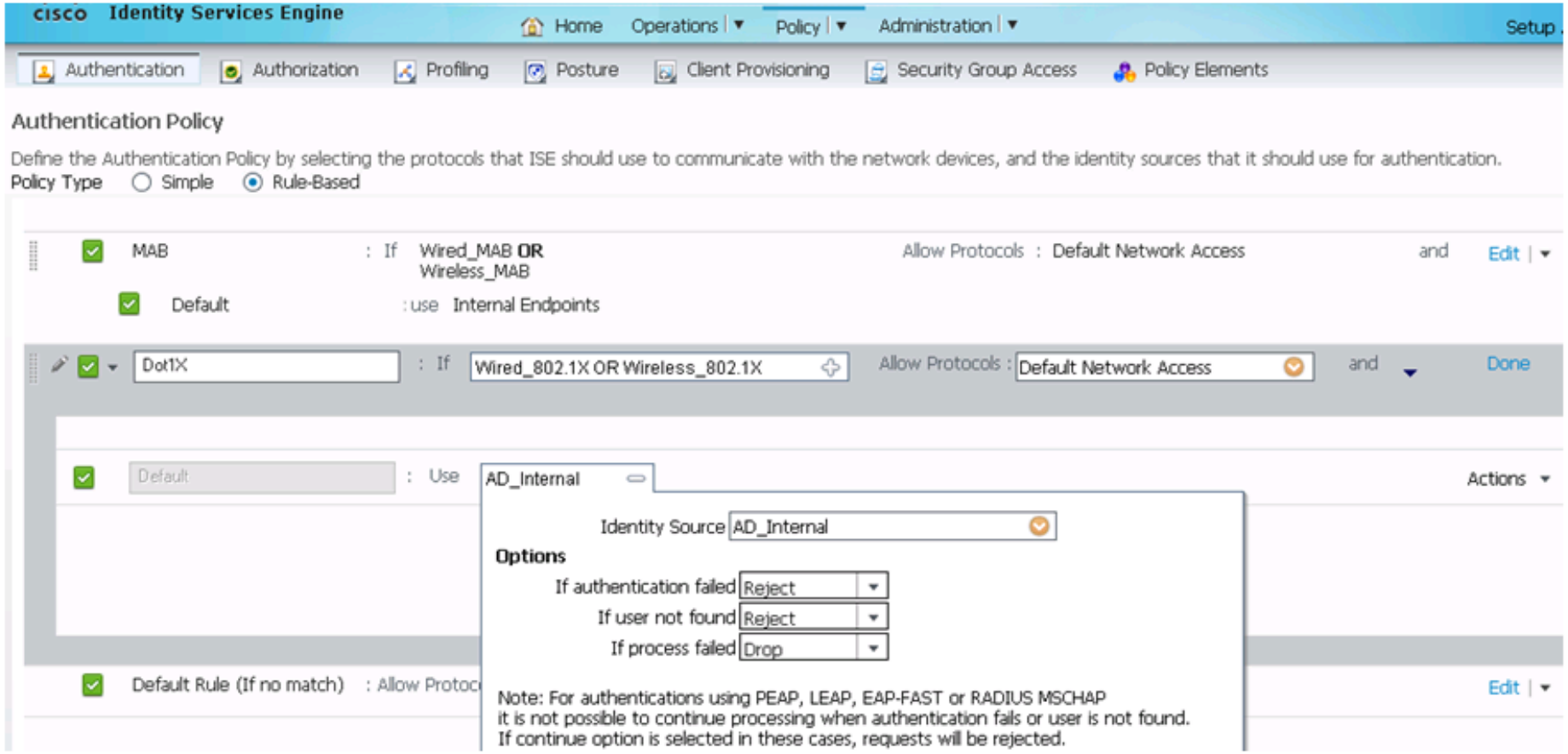


Configure Identity Source Sequence (Cont.)

- 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

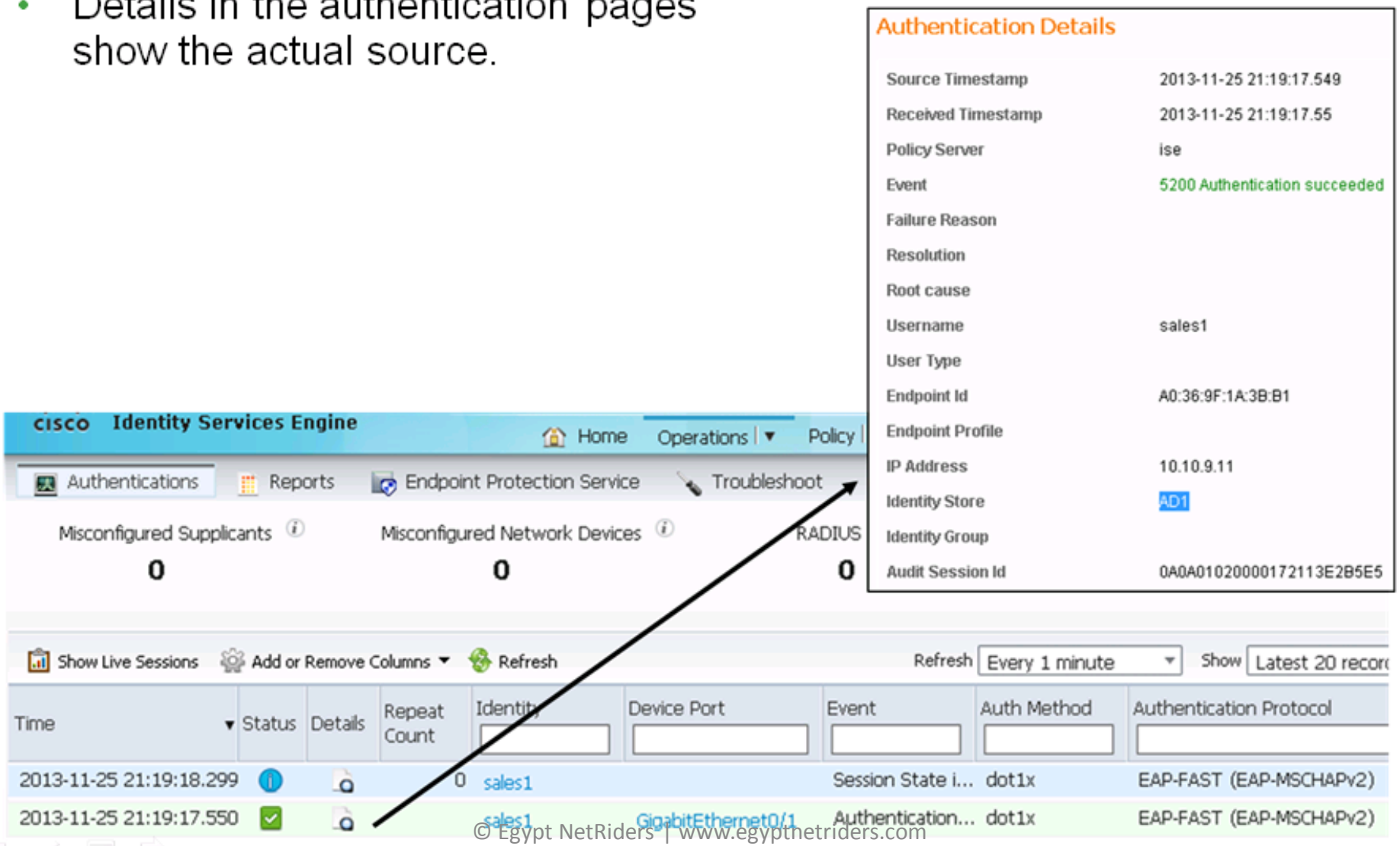
Apply Identity Source Sequence

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



Verify External Authentication

- Details in the authentication pages show the actual source.



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.