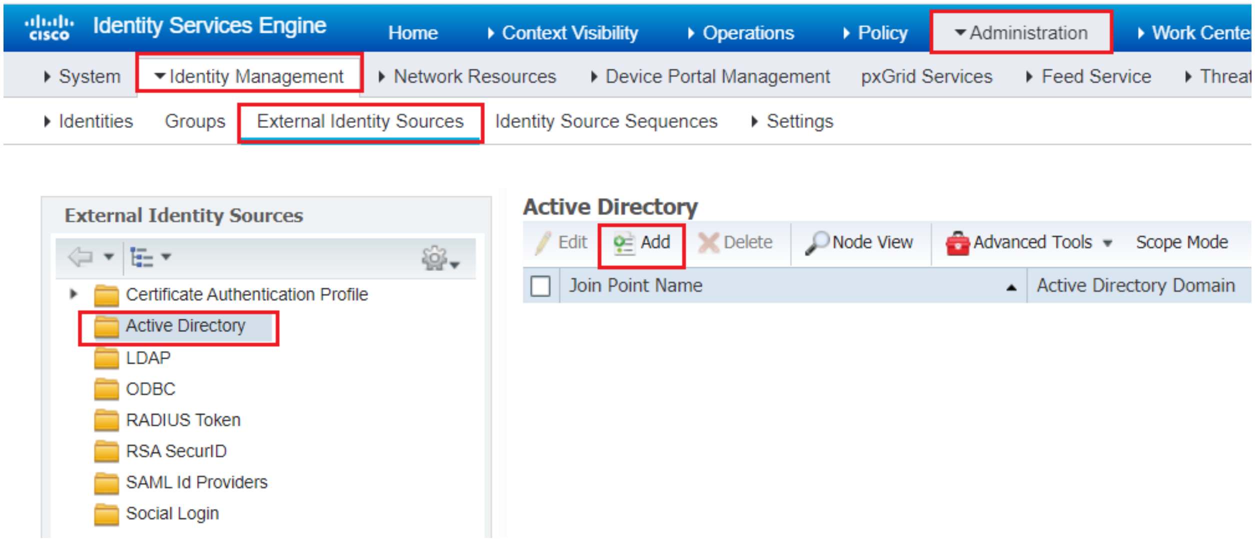
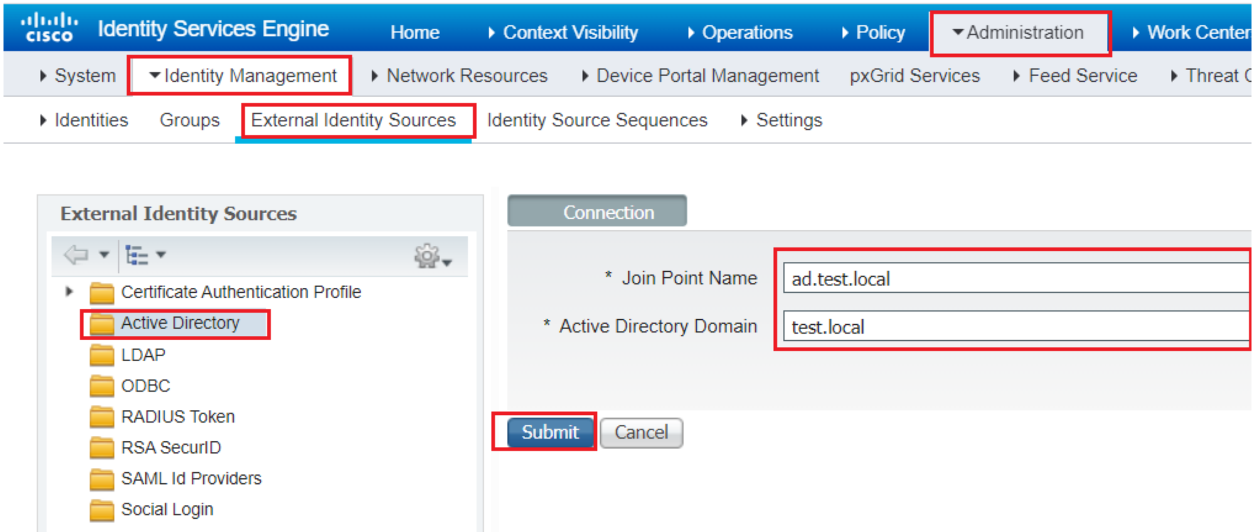
ISE Active Directory Integration:

Navigate to Administration >Identity Management> External Identity Sources > Active Directory and click on Add



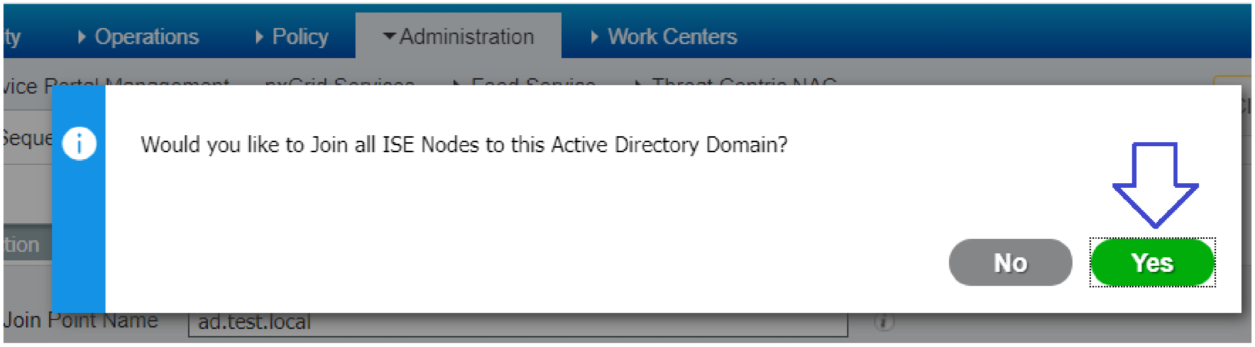
Enter domain name in Active Directory Domain boxes and Join Point Name anything you like click the Submit button.



* Join Point Name: ad.test.local

* Active Directory Domain: test.local

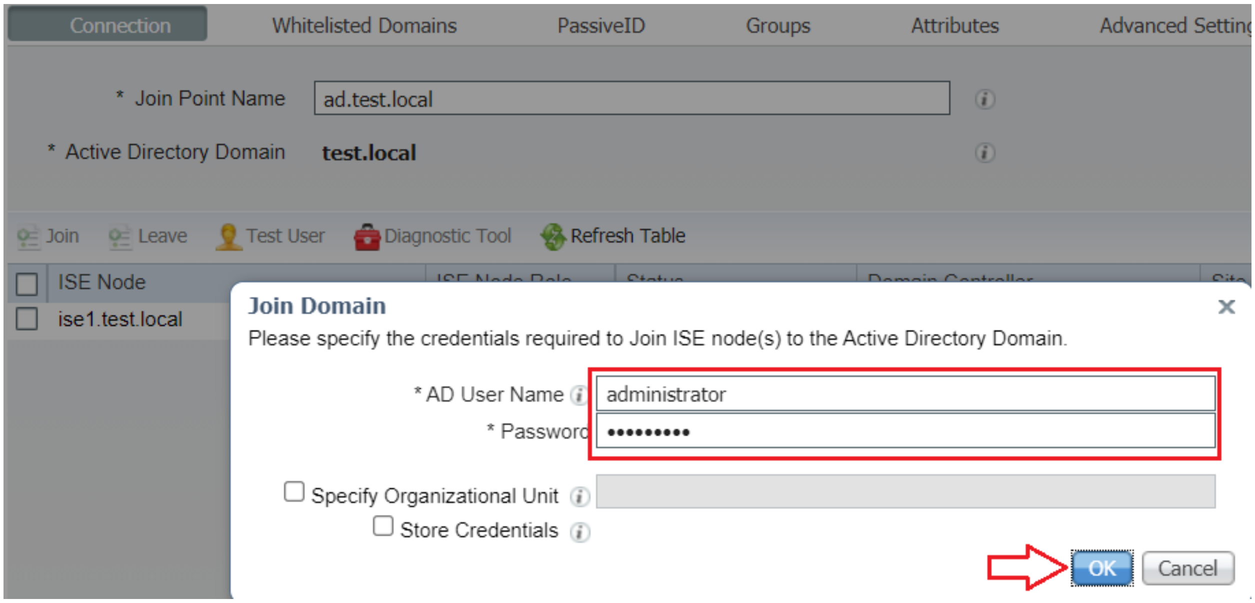
A pop-up appears asking if you want to join the newly created join point to the domain. Click Yes. If you want to join immediately. If you clicked No, then saving the configuration saves the Active Directory domain configuration globally, but none of the Cisco ISE nodes are joined to the domain yet.



Would you like to Join all ISE Nodes to this Active Directory Domain?

Join Point Name ad.test.local

Enter Active Directory username & password from Join Domain dialog box that opens. Click OK.



* Join Point Name ad.test.local

* Active Directory Domain **test.local**

□ ise1.test.local

Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

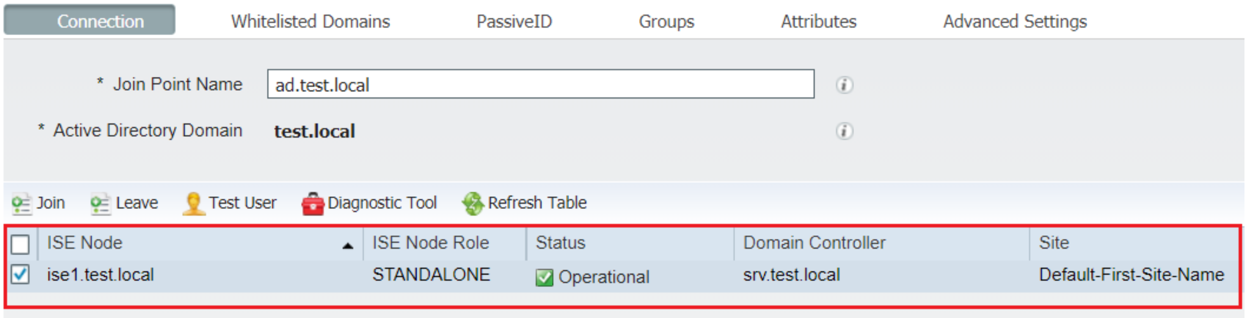
* AD User Name administrator

* Password ••••••••••

□ Specify Organizational Unit

□ Store Credentials

Now the status of Join Point change to Operational and list of Domain Controller.



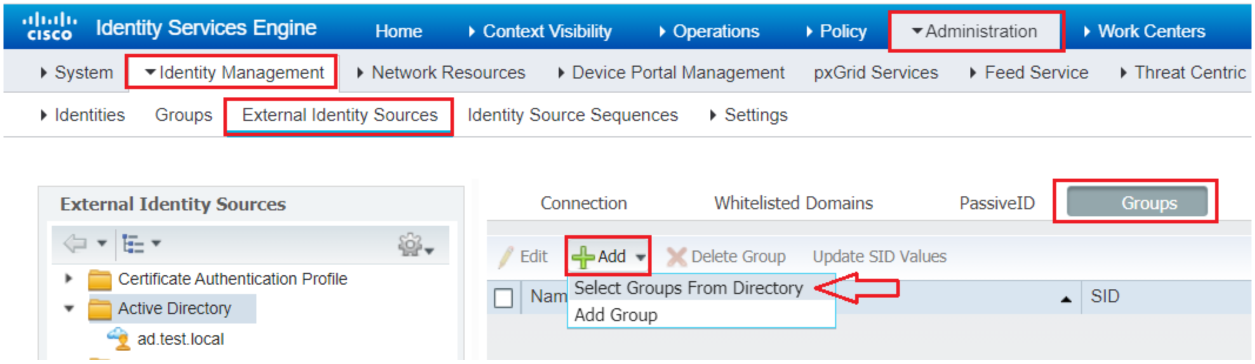
* Join Point Name ad.test.local

* Active Directory Domain **test.local**

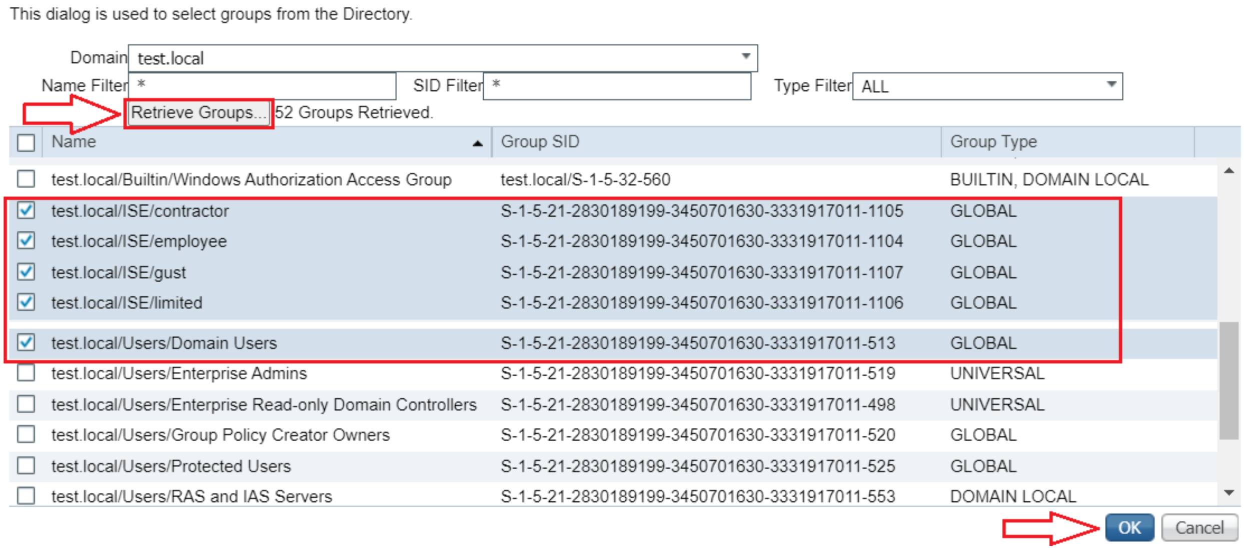
□	ISE Node	ISE Node Role	Status	Domain Controller	Site
☑	ise1.test.local	STANDALONE	✓ Operational	srv.test.local	Default-First-Site-Name

Add Groups:

Configure Active Directory user groups to be available for use in authorization policies. After ISE is joined to domain, Choose Administration > Identity Management > External Identity Sources > Active Directory. Click the Groups Tab. Click on Add and then Select Groups from Directory. This is where we add Active Directory groups to ISE for future use.



Used an asterisk to pull up all my AD groups: Check the check boxes next to the groups that you want to be available for use in authorization policies and click OK.

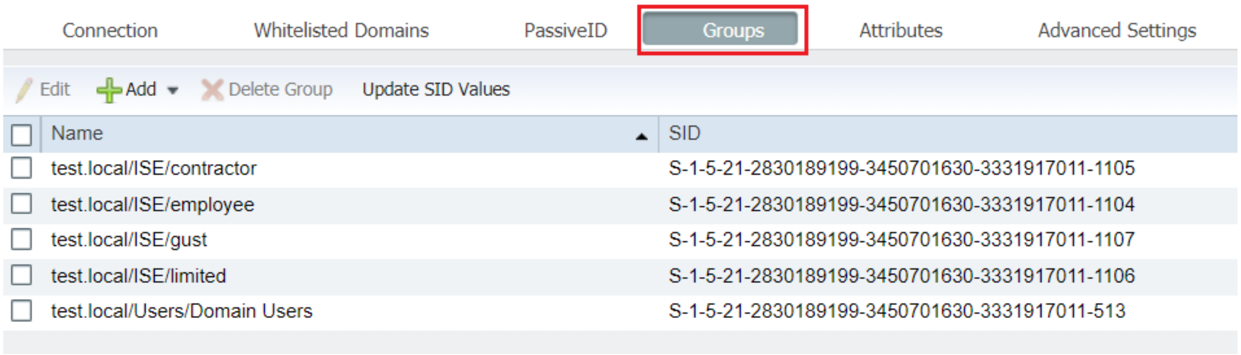

This dialog is used to select groups from the Directory.

Domain: test.local

Name Filter: *   SID Filter: *   Type Filter: ALL

Retrieve Groups... 52 Groups Retrieved.

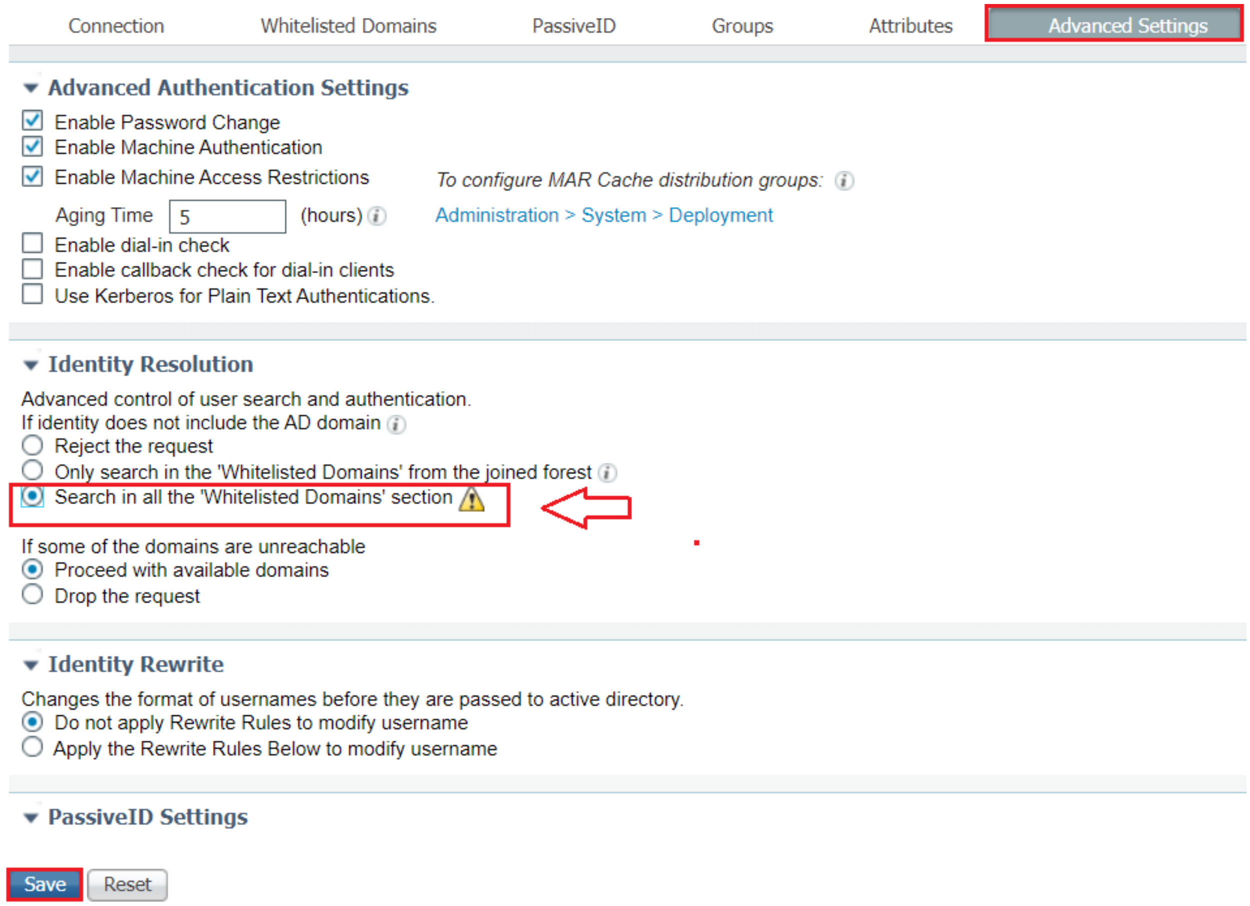
□	Name	Group SID	Group Type
□	test.local/Builtin/Windows Authorization Access Group	test.local/S-1-5-32-560	BUILTIN, DOMAIN LOCAL
☑	test.local/ISE/contractor	S-1-5-21-2830189199-3450701630-3331917011-1105	GLOBAL
☑	test.local/ISE/employee	S-1-5-21-2830189199-3450701630-3331917011-1104	GLOBAL
☑	test.local/ISE/gust	S-1-5-21-2830189199-3450701630-3331917011-1107	GLOBAL
☑	test.local/ISE/limited	S-1-5-21-2830189199-3450701630-3331917011-1106	GLOBAL
☑	test.local/Users/Domain Users	S-1-5-21-2830189199-3450701630-3331917011-513	GLOBAL
□	test.local/Users/Enterprise Admins	S-1-5-21-2830189199-3450701630-3331917011-519	UNIVERSAL
□	test.local/Users/Enterprise Read-only Domain Controllers	S-1-5-21-2830189199-3450701630-3331917011-498	UNIVERSAL
□	test.local/Users/Group Policy Creator Owners	S-1-5-21-2830189199-3450701630-3331917011-520	GLOBAL
□	test.local/Users/Protected Users	S-1-5-21-2830189199-3450701630-3331917011-525	GLOBAL
□	test.local/Users/RAS and IAS Servers	S-1-5-21-2830189199-3450701630-3331917011-553	DOMAIN LOCAL



□	Name	SID
□	test.local/ISE/contractor	S-1-5-21-2830189199-3450701630-3331917011-1105
□	test.local/ISE/employee	S-1-5-21-2830189199-3450701630-3331917011-1104
□	test.local/ISE/gust	S-1-5-21-2830189199-3450701630-3331917011-1107
□	test.local/ISE/limited	S-1-5-21-2830189199-3450701630-3331917011-1106
□	test.local/Users/Domain Users	S-1-5-21-2830189199-3450701630-3331917011-513

Option Settings:

In the same window click the Advanced Settings tab and select the Search in all the Whitelisted Domains section radio button. This is optional but you will be able to log into your networking devices without having to specify the entire FQDN. Click Save button.



Connection | Whitelisted Domains | PassiveID | Groups | Attributes | Advanced Settings

Advanced Authentication Settings

☑ Enable Password Change
☑ Enable Machine Authentication
☑ Enable Machine Access Restrictions

To configure MAR Cache distribution groups:

Aging Time 5 (hours)

Administration > System > Deployment

□ Enable dial-in check
□ Enable callback check for dial-in clients
□ Use Kerberos for Plain Text Authentications.

Identity Resolution

Advanced control of user search and authentication.
If identity does not include the AD domain
○ Reject the request
○ Only search in the 'Whitelisted Domains' from the joined forest
● Search in all the 'Whitelisted Domains' section ⚠

If some of the domains are unreachable
● Proceed with available domains
○ Drop the request

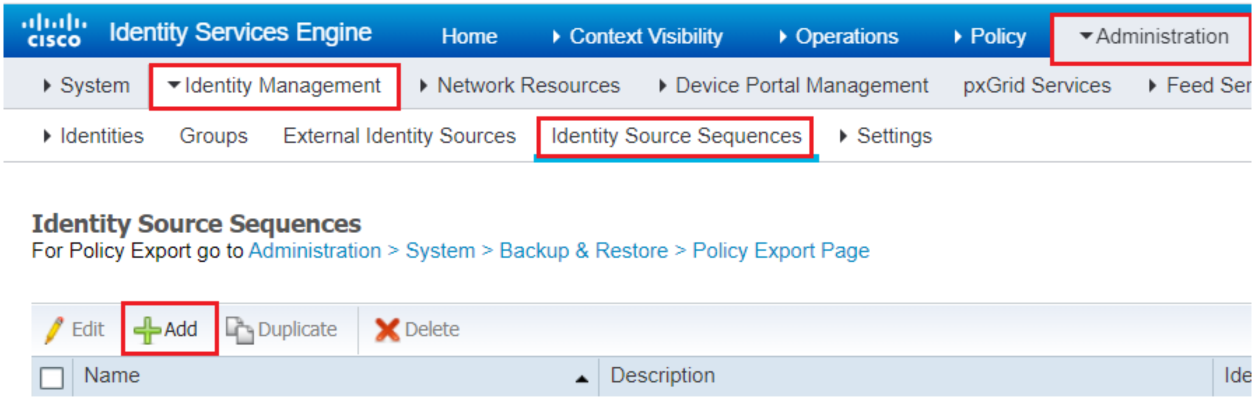
Identity Rewrite

Changes the format of usernames before they are passed to active directory.
● Do not apply Rewrite Rules to modify username
○ Apply the Rewrite Rules Below to modify username

PassiveID Settings

Create Identity Source Sequence:

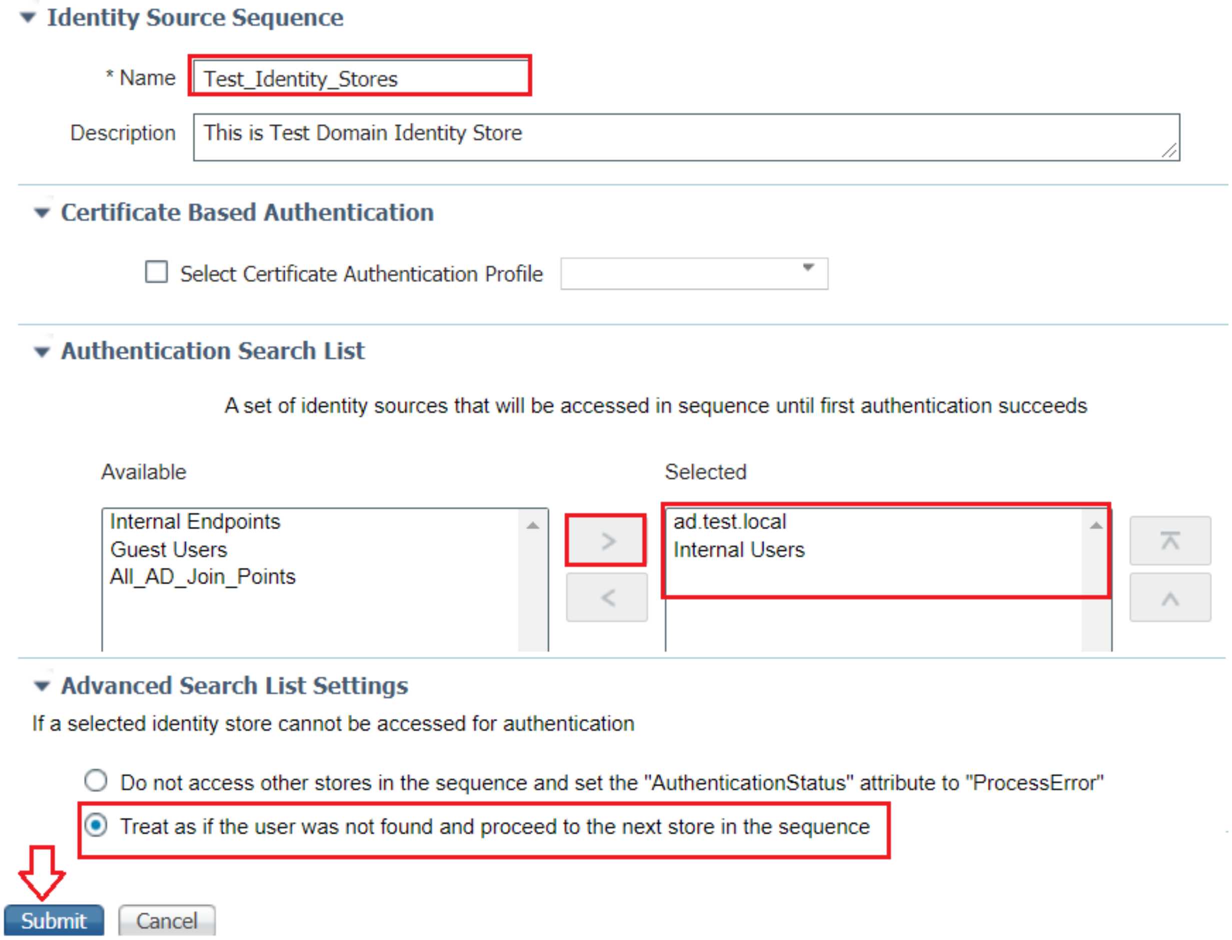
The next step is to create & Identity Source Sequence. This will tell ISE what order of databases to search for a user account when authenticating to a device. Navigate to Administration -> Identity Management -> Identity Source Sequences -> Add.



Identity Source Sequences

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Give Identity Source Sequence a Name. Move your domain and the Internal Users group over to Selected from Available. Select the "Treat as if the user was not found" radio button.



▾ Identity Source Sequence

* Name: Test_Identity_Stores

Description: This is Test Domain Identity Store

▾ 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: Internal Endpoints, Guest Users, All_AD_Join_Points

Selected: ad.test.local, Internal Users

▾ Advanced Search List Settings

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