

# ISE and two way trust AD configuration

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Verify](#)

[Troubleshoot](#)

[Verify](#)

## Introduction

This document describes the definition of "two-way-trust" on ISE, and a simple configuration example : how to authenticate a user which is not present in the AD joined to ISE, but present in another AD.

## Prerequisites

### Requirements

Cisco recommends that you have basic knowledge of :

- ISE 2.x and Active Directory integration .
- External identity authentication on ISE.

### Components Used

- ISE 2.x .
- two Active Directories.

## Configure

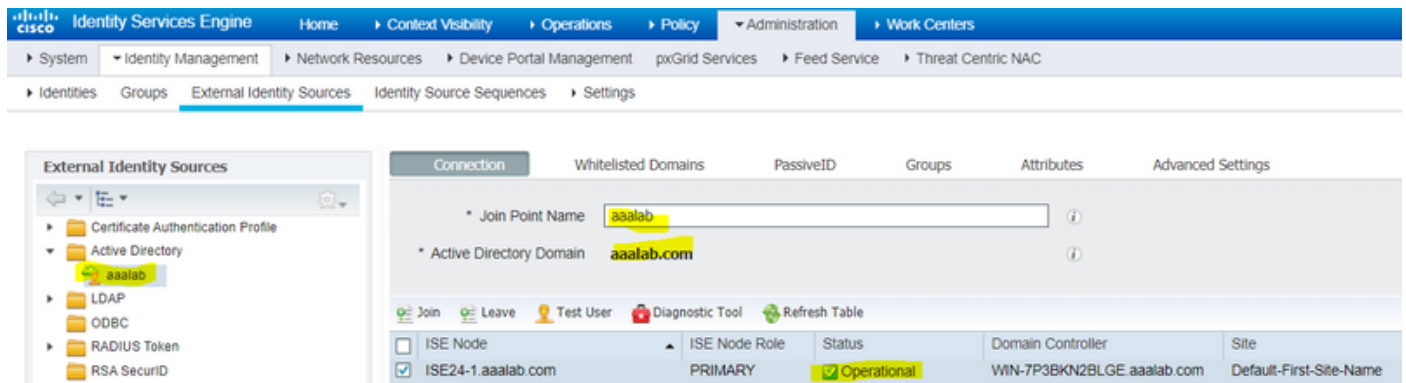
In order to expand your domain, and include other users in a different domain other than the one which is already joined to ISE, you have two ways to accomplish this :

1. you can add the domain manually and separately on ISE. by this, you would have two separate Active Directories.
2. Join one AD to ISE, then configure **two-way-trust** between this AD and the second AD, without adding it to ISE. This is mainly two way trust configuration, it is an option which is configured between two or more Active Directories. ISE will automatically detect these trusted domains using the AD-connector and add them to the "whitelisted domains" and treat them as separate ADs joined to ISE. This is how you can authenticate a user in the AD

"zatar.jo", which is not joined to ISE.

The following steps describe the configuration procedure on both ISE and AD:

**step 1.** make sure that ISE is joined to AD, in this example, you have the domain aaalab :

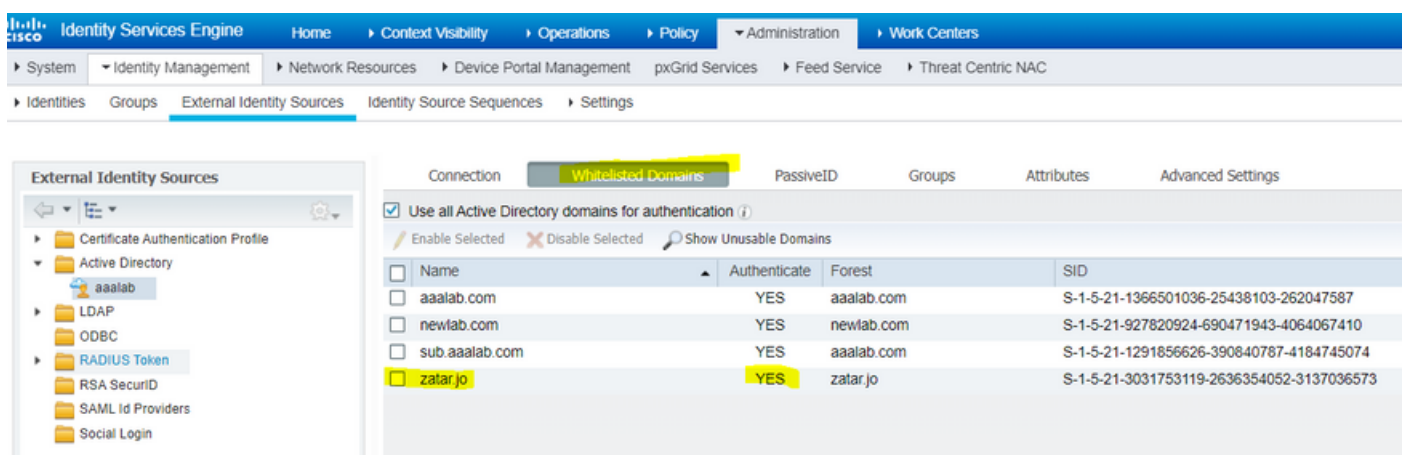


**step 2.** make sure that two-way trust is enabled between both Active Directories, as below :

1. Open the Active Directory Domains and Trusts snap-in.
2. In the left pane, right-click the domain you want to add a trust for, and select Properties.
3. Click on the Trusts tab.
4. Click the New Trust button.
5. After the New Trust Wizard opens, click Next.
6. Type the DNS name of the AD domain and click Next.
7. Assuming the AD domain was resolvable via DNS, the next screen will ask for the Direction of Trust. Select Two-way and click Next.
8. For the Outgoing Trust Properties, select all resources to be authenticated and click Next.
9. Enter and retype the trust password and click Next.
10. Click Next twice.

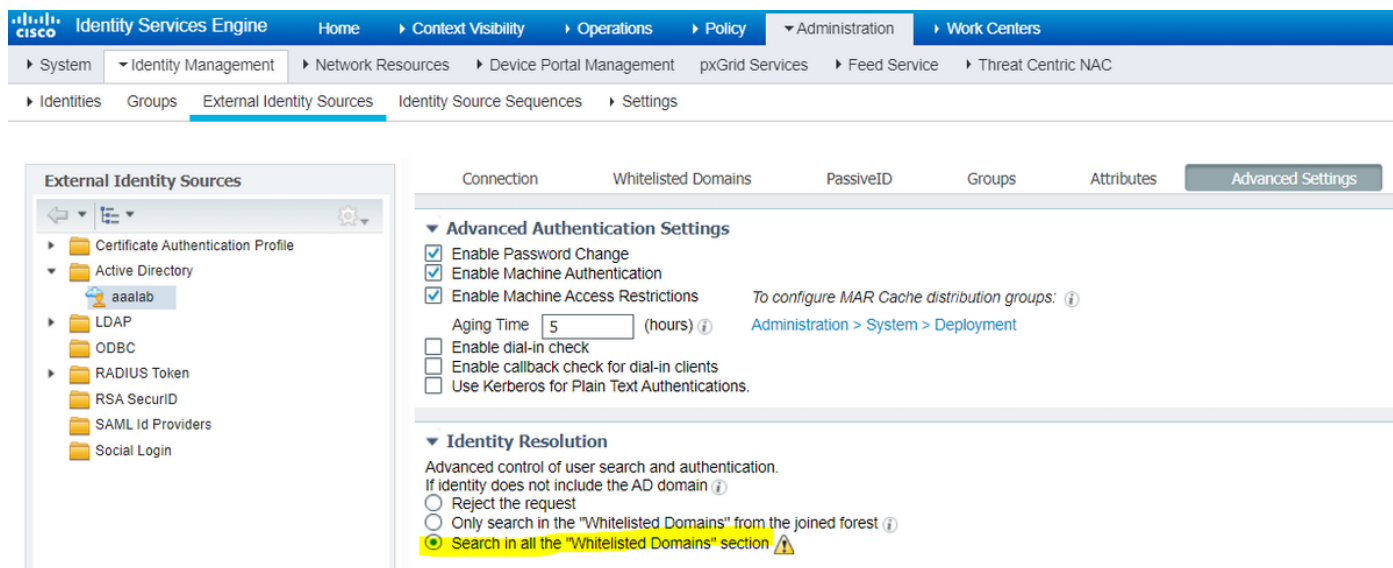
**Note:** AD configuration is out of Cisco support scope, Microsoft support can be engaged in case of any issues.

once this is configured, the example AD (aaalab) can communicate with the new AD (zatar.jo) and it should pop up in the "whitlested domains" tab, as below. if it is not displayed, then the two way trust configuraion is incorrect :



**step 3.** Make sure the option **search in all the "whitlested Domains" section** is enabled, as shown below. It will allow searching in all whitlested domains including two-way trusted domains.

if the option **Only search in the "Whitelisted Domains" from the joined forest** is enabled, it will only search in the "child" domains of the main domain. { child domain example: sub.aaalab.com in the screenshot above }.



Now, ISE can search for the user in aaalab.com and zatar.com.

## Verify

Verify that it works via "test user" option, use the user which is in "zatar.jo" domain (in this example, the user "demo" exist only in "zatar.jo" domain, and it is not in "aaalab.com", test result is below ) :

## Test User Authentication

\* Username

\* Password

Authentication Type

Authorization Data  Retrieve Groups  
 Retrieve Attributes

Authentication Result	Groups	Attributes
Test Username	: demo	
ISE NODE	: ISE24-1.aaalab.com	
Scope	: Default_Scope	
Instance	: aaalab	
Authentication Result	: SUCCESS	
Authentication Domain	: zatar.jo	
User Principal Name	: demo@zatar.jo	
User Distinguished Name	: CN=demo,CN=Users,DC=zatar,DC=jo	
Groups	: 2 found.	
Attributes	: 33 found.	
Authentication time	: 41 ms.	
Groups fetching time	: 3 ms.	
Attributes fetching time	: 1 ms.	

note that the users in aaalab.com, are also working, user kholoud is in aaalab.com :

## Test User Authentication

\* Username

\* Password

Authentication Type

Authorization Data  Retrieve Groups  
 Retrieve Attributes

Authentication Result	Groups	Attributes
Test Username	: kholoud	
ISE NODE	: ISE24-1.aaalab.com	
Scope	: Default_Scope	
Instance	: aaalab	
Authentication Result	: SUCCESS	
Authentication Domain	: aaalab.com	
User Principal Name	: kholoud@aaalab.com	
User Distinguished Name	: CN=kholoud,CN=Users,DC=aaalab,DC=com	
Groups	: 2 found.	
Attributes	: 32 found.	
Authentication time	: 33 ms.	
Groups fetching time	: 6 ms.	
Attributes fetching time	: 3 ms.	

## Troubleshoot

There are two main procedures to troubleshoot most AD/two-way-trust issues, even most External Identity authentications :

1. collecting ISE logs (support bundle) with debugs enabled. in specific folders in this support bundle, we can find all details of any authentication attempt on AD.
2. collecting packet captures between ISE and AD.

**step1.** collect ISE logs:

a. Enable the debugs, set the following debugs to "trace":

- Active Directory (ad\_agent.log)
- identity-store-AD (ad\_agent.log)
- runtime-AAA (prrt-server.log)

- nsf (ise-psc.log)
- nsf-session (ise-psc.log)

b. Reproduce the issue, connect with a problematic user.

c. Collect a support bundle.

### Working scenario "logs":

**Note:** Details of the authentication attempts will be found in the file ad\_agent.log

### from the file ad\_agent.log :

zatar two way trust connection verification:

```
2020-01-16 12:26:21,210 VERBOSE,140568698918656,LsaDmEnginepDiscoverTrustsForDomain: Adding
trust info zatar.jo (Other Forest, Two way) in forest
zatar.jo,LsaDmEnginepDiscoverTrustsForDomain(),lsass/server/auth-providers/ad-open-
provider/lsadmengine.c:472
2020-01-16 12:26:21,210 DEBUG ,140568698918656,New domain zatar.jo will be added to the trusted
domain list.,LsaDmAddTrustedDomain(),lsass/server/auth-providers/ad-open-provider/lsadm.c:1997
searching for the user "demo" in main domain aalab :
```

```
2020-01-16 12:29:08,579 DEBUG ,140568690480896,AdIdentityResolver::search: do
(&|(objectCategory=person)(objectCategory=computer))(sAMAccountName=demo)) search in forest
aalab.com,searchIdentity(),lsass/server/auth-providers/ad-open-
provider/ad_identity_resolver_impl.cpp:738
```

(note that demo user is in zatar domain, however ise will check it in aalab domain first, then other domains in the "whitelisted" domains tab such as newlab.com. to avoid cheking in the main domain, and to check in zatar.jo directly, you have to use the UPN suffix so that ISE will know where to search, so the user should login by this format : demo.zatar.jo).

searching for the user "demo" in zatar.jo.

```
2020-01-16 12:29:08,604 DEBUG ,140568690480896,AdIdentityResolver::search: do
(&|(objectCategory=person)(objectCategory=computer))(sAMAccountName=demo)) search in forest
zatar.jo,searchIdentity(),lsass/server/auth-providers/ad-open-
provider/ad_identity_resolver_impl.cpp:738
2020-01-16 12:29:08,604 DEBUG ,140568690480896,LsaDmpLdapOpen: gc=1,
domain=zatar.jo,LsaDmpLdapOpen(),lsass/server/auth-providers/ad-open-provider/lsadm.c:4102
2020-01-16 12:29:08,604 DEBUG ,140568690480896,LsaDmpIsDomainOffline: checking status of domain
zatar.jo,LsaDmpIsDomainOffline(),lsass/server/auth-providers/ad-open-provider/lsadm.c:3158
```

user "demo" found in zatar domain :

```
18037: pszResolvedIdentity = "demo@zatar.jo"
Line 18039: pszResolvedDN = "CN=demo,CN=Users,DC=zatar,DC=jo"
Line 18044: pszResolvedSAM = "demo"
Line 18045: pszResolvedExplicitUPN = "demo@zatar.jo"
Line 18056: "1579177748579 24325 "demo" AD-Log-Id=1579177581/40,
Line 18095: pszBase = "CN=demo,CN=Users,DC=zatar,DC=jo"
```

**step2.** Collect captures:

a. The packets exchanged between ISE and AD/LDAP, are encrypted so they would not be readable if we collect the captures without decrypting them first.

To decrypt packets between ISE and AD (this step needs to be applied before collecting the captures and applying the attempt):

1. On ISE, navigate to the tab : External-ID-Stores -> Active Directory -> Advanced Tools -> Advanced Tuning
2. Choose your ISE node.
3. The 'Name' field gets a specific TROUBLESHOOTING string :  
TROUBLESHOOTING.EncryptionOffPeriod.
4. The 'Value' field gets the number of minutes you would like to troubleshoot for  
<Positive integer in minutes>

Example for half an hour:

30

5. Type any description. Required before next step.
6. Click 'Update Value' button
7. Click 'Restart Active Directory Connector.
8. wait for 10 mins for the decrypt to take affect .

b. start the captures on ISE.

c. reproduce the issue.

d. then stop and download the capture

**Working scenario "logs":**

no.	Time	Source	Destination	Protocol	Length	Info
1588	2020-01-16 12:29:08...	10.48.60.101	10.48.60.241	KRBS	1488	TGS-REP
1589	2020-01-16 12:29:08...	10.48.60.241	10.48.60.101	TCP	74	46537 → 3268 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=785544300 TSecr=
1590	2020-01-16 12:29:08...	10.48.60.101	10.48.60.241	TCP	74	3268 → 46537 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=
1591	2020-01-16 12:29:08...	10.48.60.241	10.48.60.101	TCP	66	46537 → 3268 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=785544300 TSecr=260534689
1592	2020-01-16 12:29:08...	10.48.60.241	10.48.60.101	LDAP	1505	bindRequest(1) "<ROOT>" sasl
1593	2020-01-16 12:29:08...	10.48.60.101	10.48.60.241	LDAP	278	bindResponse(1) success
1594	2020-01-16 12:29:08...	10.48.60.241	10.48.60.101	TCP	66	46537 → 3268 [ACK] Seq=1440 Ack=213 Win=30336 Len=0 TSval=785544303 TSecr=260534689
1595	2020-01-16 12:29:08...	10.48.60.241	10.48.60.101	LDAP	370	SASL GSS-API Integrity: searchRequest(2) "dc=aaalab,dc=com" wholeSubtree
1596	2020-01-16 12:29:08...	10.48.60.101	10.48.60.241	LDAP	120	SASL GSS-API Integrity: searchResDone(2) success [0 results]
1604	2020-01-16 12:29:08...	10.48.60.241	10.48.60.101	KRBS	1476	TGS-REQ

```

krb5_sgn_cksum: 60093f3168802bc1276063af
  GSS-API payload (272 bytes)
    LDAPMessage searchRequest(2) "dc=aaalab,dc=com" wholeSubtree
      messageID: 2
        protocolOp: searchRequest (3)
          searchRequest
            baseObject: dc=aaalab,dc=com
            scope: wholeSubtree (2)
            derefAliases: neverDerefAliases (0)
            sizeLimit: 0
            timeLimit: 0
            typesOnly: False
            Filter: (&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=demo))
              filter: and (0)
                and: (&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=demo))
                  and: 2 items
                    Filter: (|(objectCategory=person)(objectCategory=computer))
                      and item: or (1)
                        or: (|(objectCategory=person)(objectCategory=computer))
                    Filter: (sAMAccountName=demo)
                      and item: equalityMatch (3)
                        equalityMatch
                          attributeDesc: sAMAccountName
                          assertionValue: demo

```

## Verify

Here are a couple of examples of working and non working situations you might encounter and the logs they produce.

### 1. Authentication based on AD "zatar.jo" groups:

If the group not retrieved from the group tab you will get this logs message:

```

2020-01-22 10:41:01,526 DEBUG ,140390418061056,Do not know about domain for object SID 'S-1-5-21-3031753119-2636354052-3137036573-513',LsaDmpMustFindDomainByObjectSid(),lsass/server/auth-providers/ad-open-provider/lsadm.c:1574

```

We need to retrieve the groups in zatar.jo from the Groups tab.

Verifying AD group retrievals from AD tab:



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

\* Join Point Name:  ⓘ

\* Active Directory Domain: **aaalab.com** ⓘ

Join | Leave | Test User | Diagnostic Tool | Refresh Table

ISE Node	ISE Node Role	Status	Domain Controller	Site
<input checked="" type="checkbox"/> isefire.wall.com	STANDALONE	<input checked="" type="checkbox"/> Operational	WIN-7P3BKN2BLGE.aaalab.com	Default-First-Site-Name

**Test User Authentication**

\* Username:

\* Password:

Authentication Type: MS-RPC

Authorization Data:  Retrieve Groups,  Retrieve Attributes

**Authentication Result** | Groups | Attributes

```

Test Username      : amman
ISE NODE          : isefire.wall.com
Scope            : Default_Scope
Instance         : aaalab

Authentication Result : SUCCESS

Authentication Domain : zatar.jo
User Principal Name  : amman@zatar.jo
User Distinguished Name : CN=amman,CN=Users,DC=zatar,DC=jo

Groups           : 2 found.
Attributes       : 33 found.

Authentication time      : 83 ms.
Groups fetching time    : 5 ms.
Attributes fetching time: 6 ms.
          
```

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

\* Join Point Name:  ⓘ

\* Active Directory Domain: **aaalab.com** ⓘ

Join | Leave | Test User | Diagnostic Tool | Refresh Table

ISE Node	ISE Node Role	Status	Domain Controller	Site
<input checked="" type="checkbox"/> isefire.wall.com	STANDALONE	<input checked="" type="checkbox"/> Operational	WIN-7P3BKN2BLGE.aaalab.com	Default-First-Site-Name

**Test User Authentication**

\* Username:

\* Password:

Authentication Type: MS-RPC

Authorization Data:  Retrieve Groups,  Retrieve Attributes

**Authentication Result** | Groups | Attributes

Name	SID
zatar.jo/Builtin/Users	zatar.jo/S-1-5-32-545
zatar.jo/Users/Domain Users	S-1-5-21-3031753119-2636354052-3137036573-513

**working scenario From the logs AD\_agent.log:**

```

2020-01-22 10:41:01,516 DEBUG ,140390418061056,AD_GetTokenGroups: SID selected: [zatar.jo/S-1-5-32-545],AD_GetTokenGroups() ,lsass/server/auth-providers/ad-open-provider/provider-main.c:9669
2020-01-22 10:41:01,516 DEBUG ,140390418061056,AD_GetTokenGroups: SID selected: [S-1-5-21-
  
```

```
3031753119-2636354052-3137036573-513],AD_GetTokenGroups(),lsass/server/auth-providers/ad-open-provider/provider-main.c:9669
```

```
pTokenGroupsList =  
{  
dwStringsCount = 2  
ppszStrings =  
{  
"zatar.jo/S-1-5-32-545"  
"S-1-5-21-3031753119-2636354052-3137036573-513"  
}  
}
```

## 2. If the advance option "Only search in the "Whitelisted Domains" from the joined forest" checked:

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  (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.

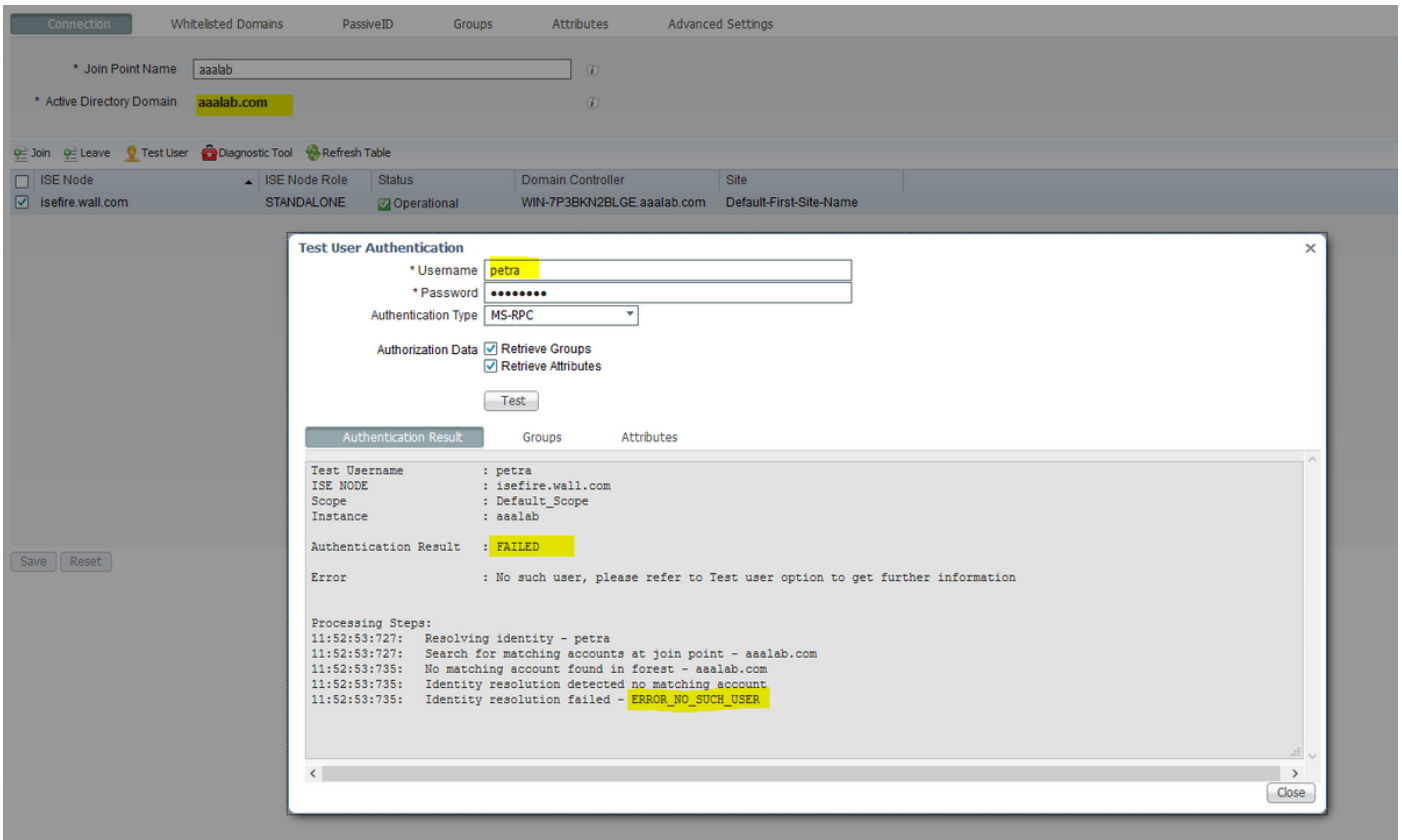
- Do not apply Rewrite Rules to modify username
- Apply the Rewrite Rules Below to modify username

▼ **PassiveID Settings**

When you choose the option "Only search in the "Whitelisted Domains" from the joined forest" the ISE marked them offline:

```
2020-01-22 13:53:31,000 DEBUG ,140629434660608,LsaDmpFilterOfflineCallback: examine domain  
newlab.com,LsaDmpFilterOfflineCallback(),lsass/server/auth-providers/ad-open-  
provider/lsadm.c:3423  
2020-01-22 13:53:31,001 DEBUG ,140629434660608,LsaDmpFilterOfflineCallback: domain newlab.com is  
usable and is marked offline (DC or GC).,LsaDmpFilterOfflineCallback(),lsass/server/auth-  
providers/ad-open-provider/lsadm.c:3498  
2020-01-22 13:53:31,001 DEBUG ,140629434660608,LsaDmpFilterOfflineCallback: examine domain  
zatar.jo,LsaDmpFilterOfflineCallback(),lsass/server/auth-providers/ad-open-provider/lsadm.c:3423  
2020-01-22 13:53:31,001 DEBUG ,140629434660608,LsaDmpFilterOfflineCallback: domain zatar.jo is  
not marked offline (DC or GC).,LsaDmpFilterOfflineCallback(),lsass/server/auth-providers/ad-  
open-provider/lsadm.c:3454
```

The user "petra" is in zatar.jo and will fail the authentication, as the below screenshot:



In the logs:

ISE was not able to reach other domains, due to advanced option "Only search in the "Whitelisted Domains" from the joined forest":

```
2020-01-22 13:52:53,735 DEBUG ,140629511296768,AdIdentityResolver::search: already did (&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=petra)) search in forest aaalab.com,searchIdentity(),lsass/server/auth-providers/ad-open-provider/ad_identity_resolver_impl.cpp:735
2020-01-22 13:52:53,735 VERBOSE,140629511296768,AdIdentityResolver::examineDomains: newlab.com,examineDomains(),lsass/server/auth-providers/ad-open-provider/ad_identity_resolver_impl.cpp:601
2020-01-22 13:52:53,735 VERBOSE,140629511296768,AdIdentityResolver::examineDomains: zatar.jo,examineDomains(),lsass/server/auth-providers/ad-open-provider/ad_identity_resolver_impl.cpp:601
2020-01-22 13:52:53,735 VERBOSE,140629511296768,AdIdentityResolver::finalizeResult: result: 40008 (symbol: LW_ERROR_NO_SUCH_USER),finalizeResult(),lsass/server/auth-providers/ad-open-provider/ad_identity_resolver_impl.cpp:491
2020-01-22 13:52:53,735 VERBOSE,140629511296768,AD_ResolveIdentity: identity=[petra], flags=0, dwError=40008,AD_ResolveIdentity(),lsass/server/auth-providers/ad-open-provider/ad_identity_resolver.cpp:131
2020-01-22 13:52:53,735 VERBOSE,140629511296768,LsaSrvResolveIdentity: identity=[petra], flags=0, dwError=40008,LsaSrvResolveIdentity(),lsass/server/api/api2.c:2877
2020-01-22 13:52:53,735 VERBOSE,140629511296768,Error code: 40008 (symbol: LW_ERROR_NO_SUCH_USER),LsaSrvResolveIdentity(),lsass/server/api/api2.c:2890
2020-01-22 13:52:53,735 VERBOSE,140629511296768,LsaSrvResolveIdentity: identity=[petra], flags=0, dwError=40008, resolved identity list returned = NO,LsaSrvIpcResolveIdentity(),lsass/server/api/ipc_dispatch.c:2738
```