ISE and two way trust AD configuration

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Configure](#)
[Verify](#)
[Troubleshoot](#)
[Verify](#)

Introduction

This document describes the defintition 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 reccomends 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

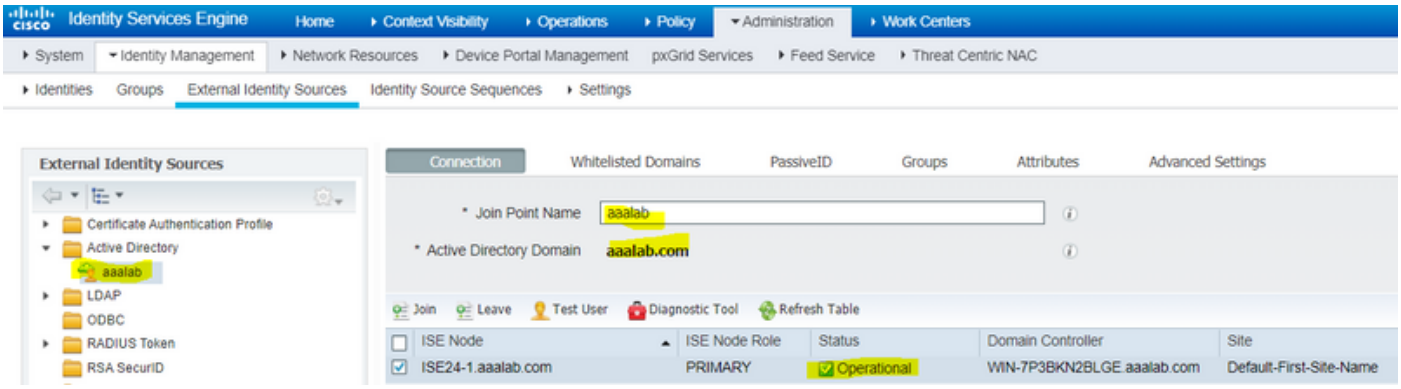
In order to expand your domain, and include other users in a different domain other than the one which is already joined to ISE, you have two ways to accomplish this :

1. you can add the domain manually and separetely on ISE. by this, you would have two seperate 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 :

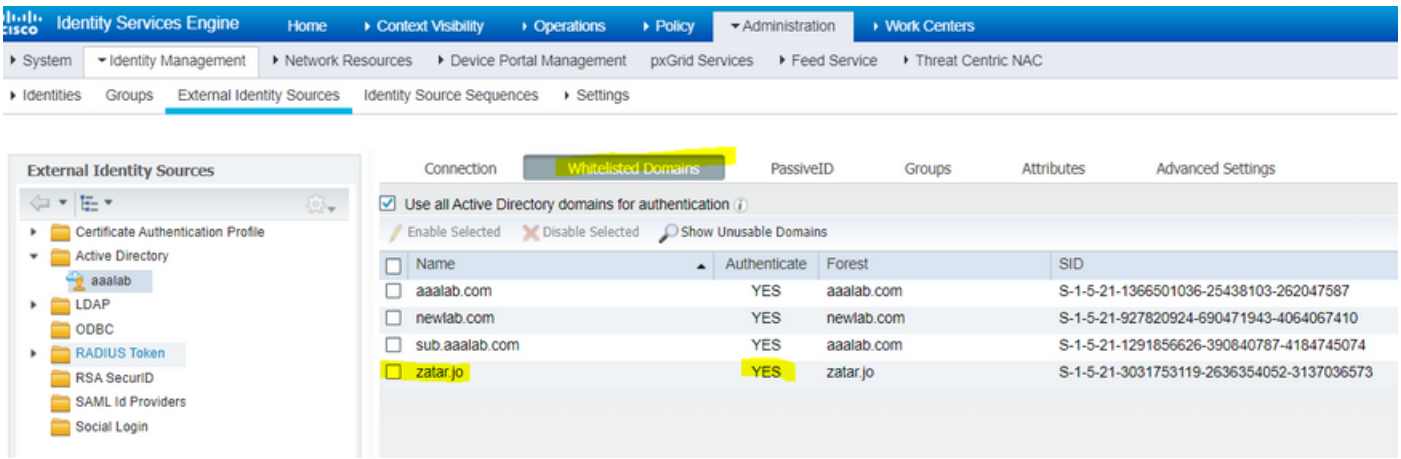


step 2. make sure that two-way trust is enabled between both Active Directories, as below :

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.

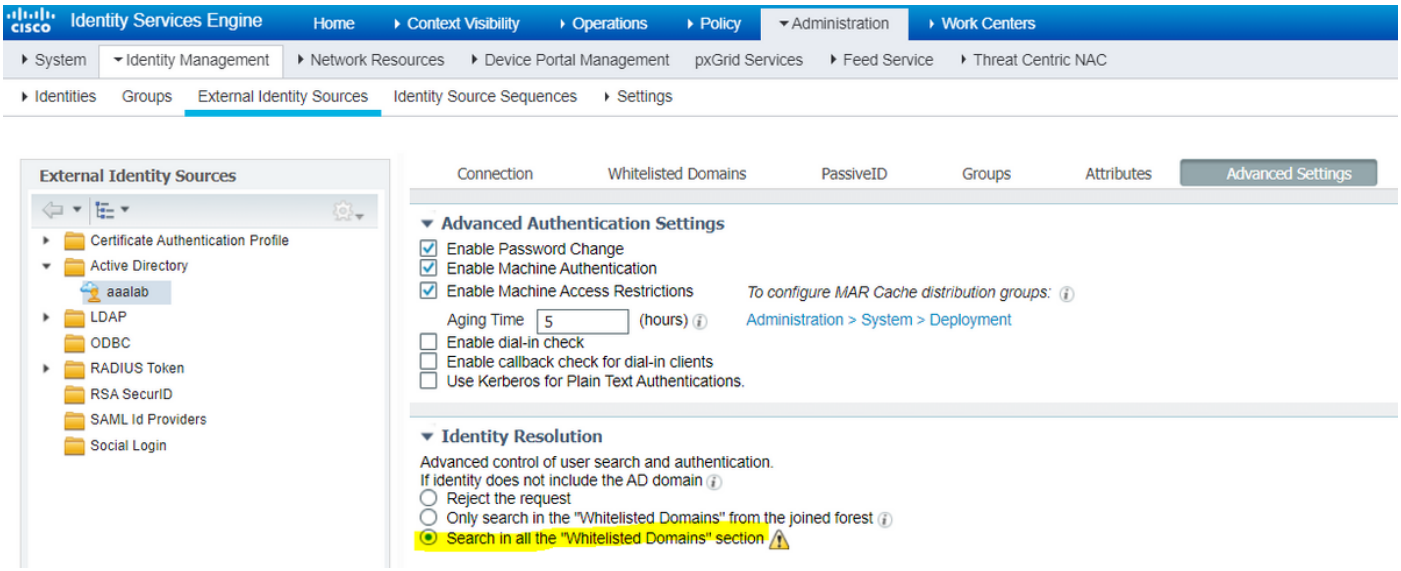
Note: AD configuration is out of Cisco support scope, Microsoft support can be engaged in case of any issues.

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 whiltlested domains including two-way trusted domains.

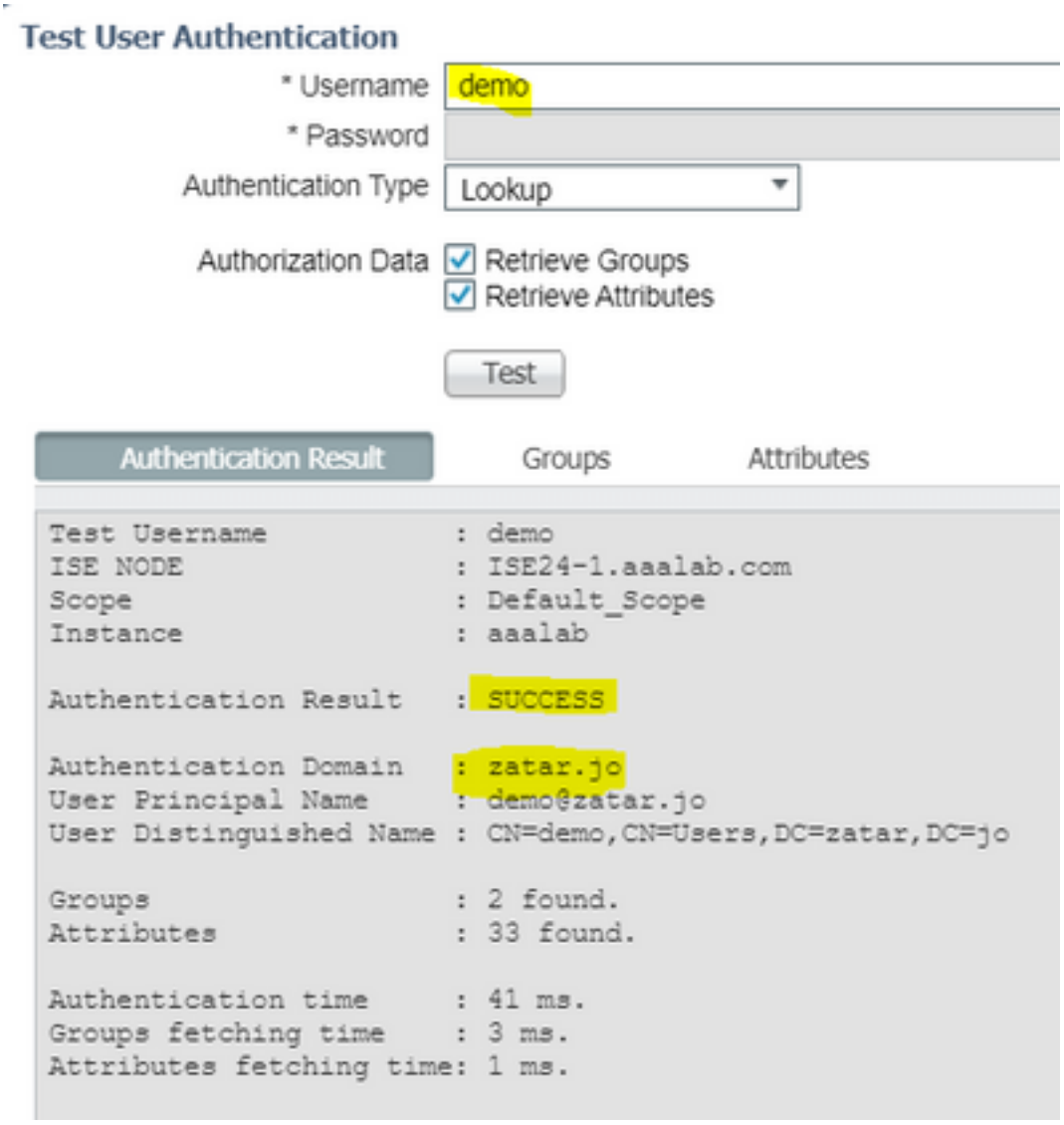
if the option **Only search in the "Whitelisted Domains" from the joined forest** is enabled, it will only search in the "child" domains of the main domain. { child domain example: sub.aaalab.com in the screenshot above }.



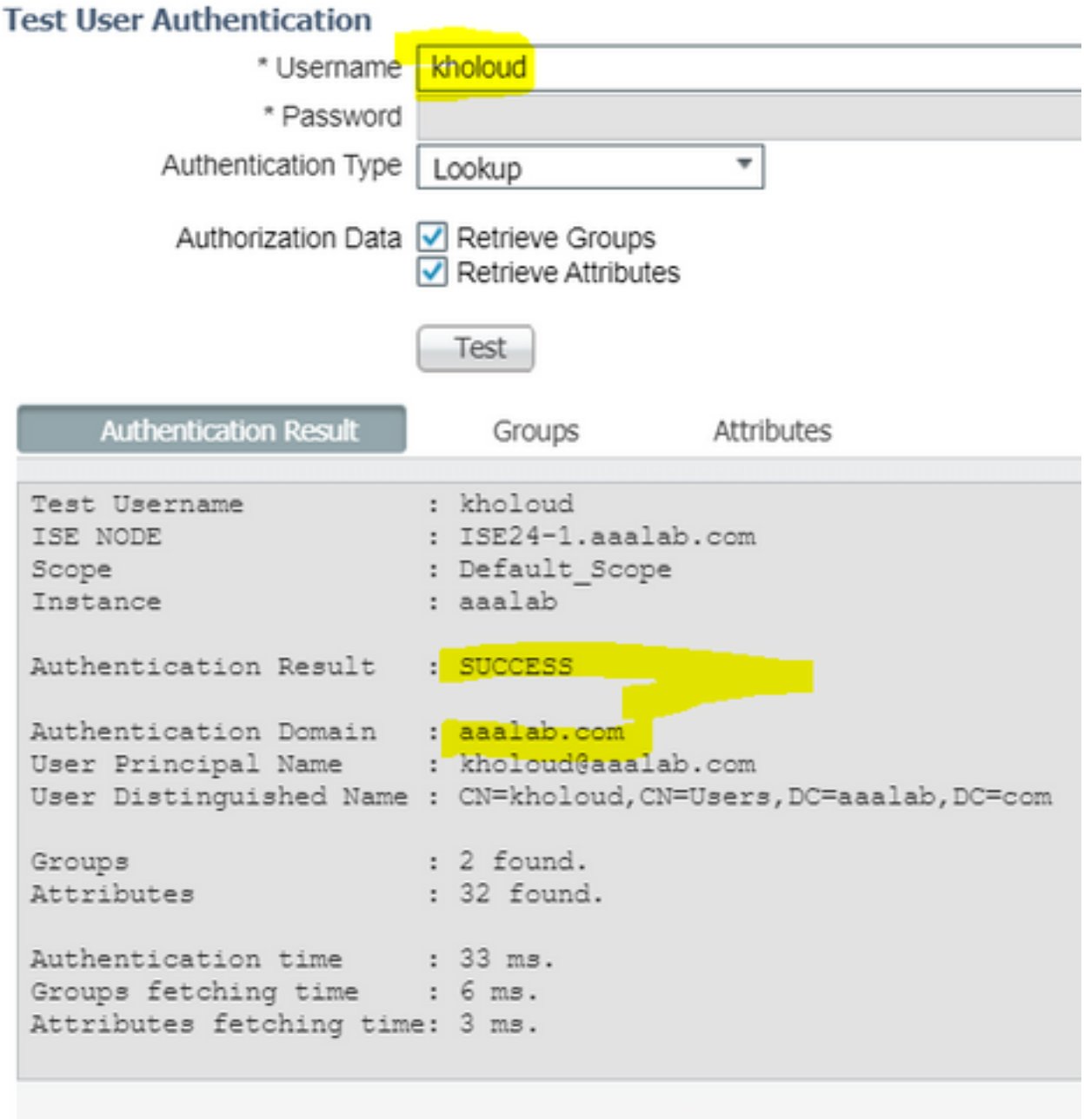
Now, ISE can search for the user in aaalab.com and zatar.com.

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) :



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



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 follwoing 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 aaalab :

```
2020-01-16 12:29:08,579 DEBUG ,140568690480896,AdIdentityResolver::search: do
(&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=demo)) search in forest
aaalab.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 aaalab domain first, then other domains in the "whitlested" 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, naigate 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

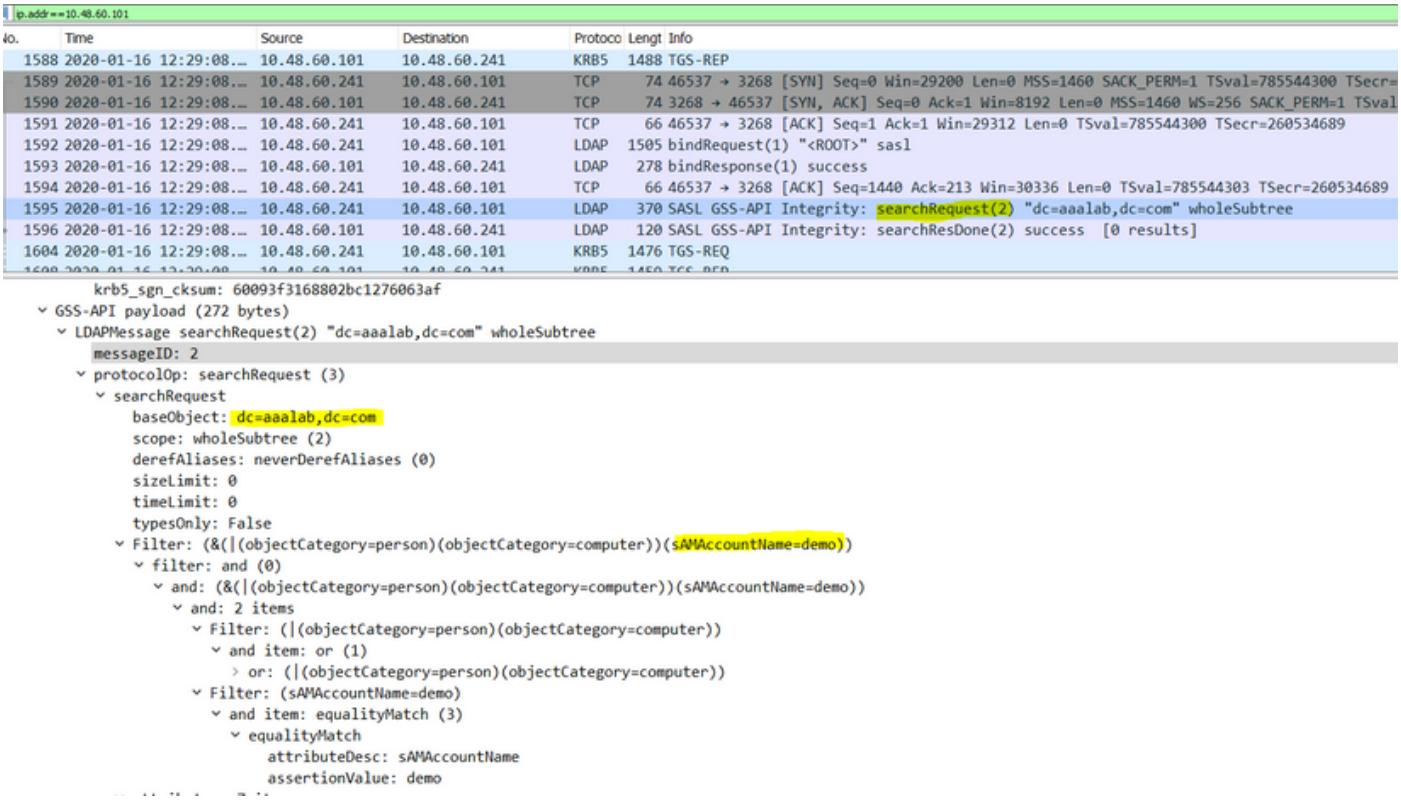
5. Type any description. Required before next step.
6. Click 'Update Value' button
7. Click 'Restart Active Directory Connector.
8. wait for 10 mins for the decrypt to take affect .

b. start the captures on ISE.

c. reproduce the issue.

d. then stop and download the capture

Working scenario "logs":



Verify

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

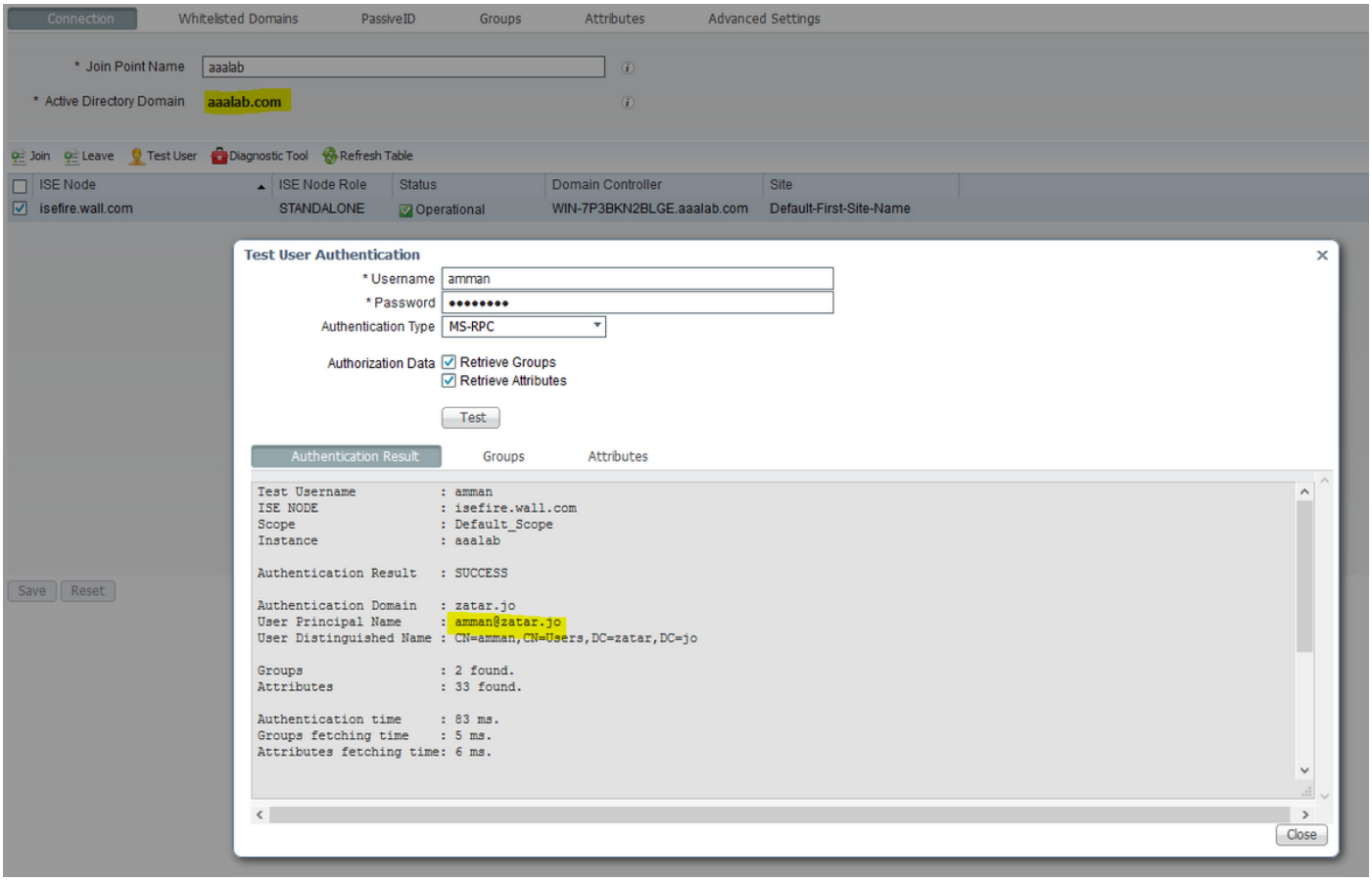
1. Authentication based on AD "zatar.jo" groups:

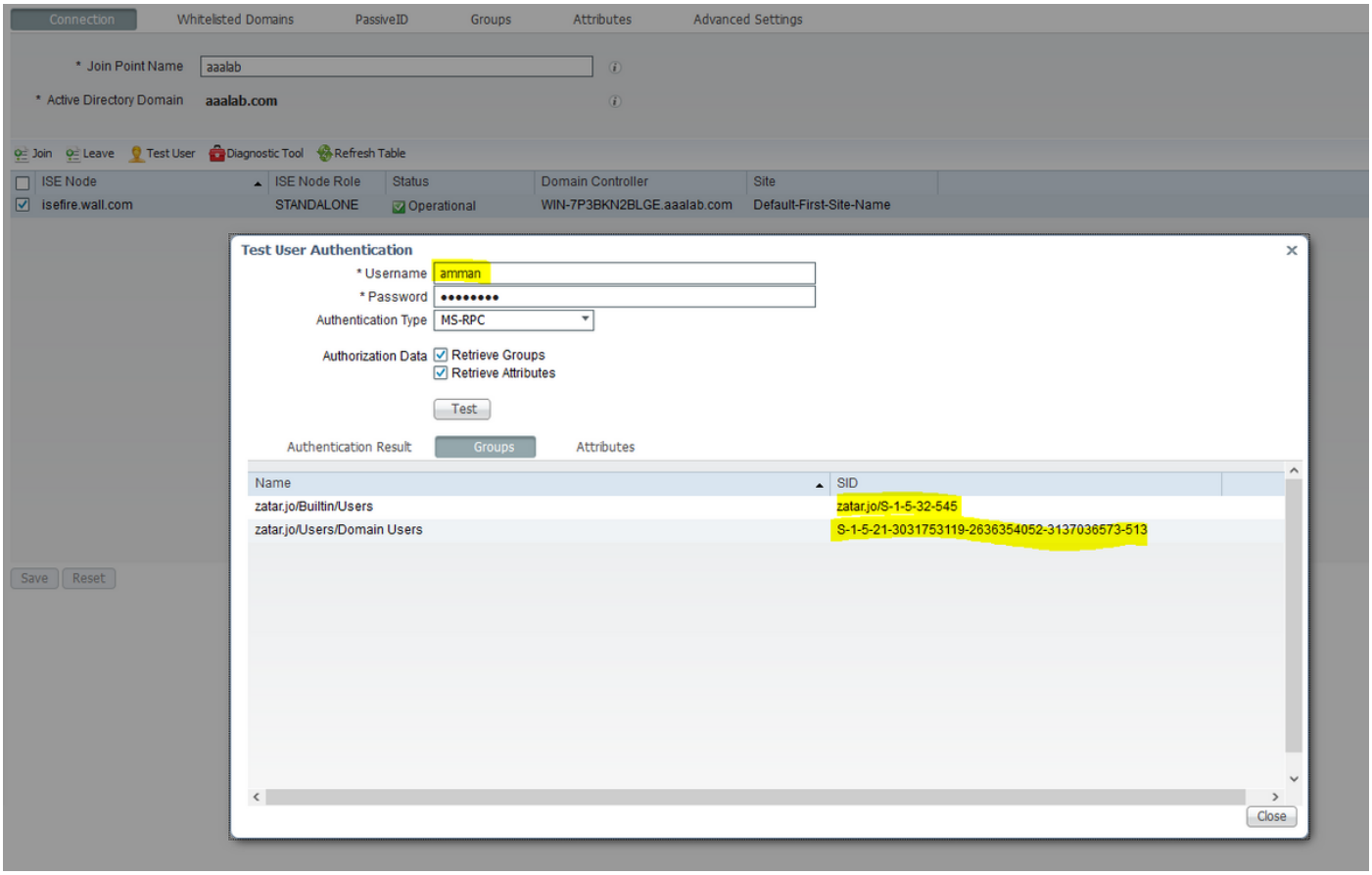
If the group not retreived from the group tab you will get this logs message:

```
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:





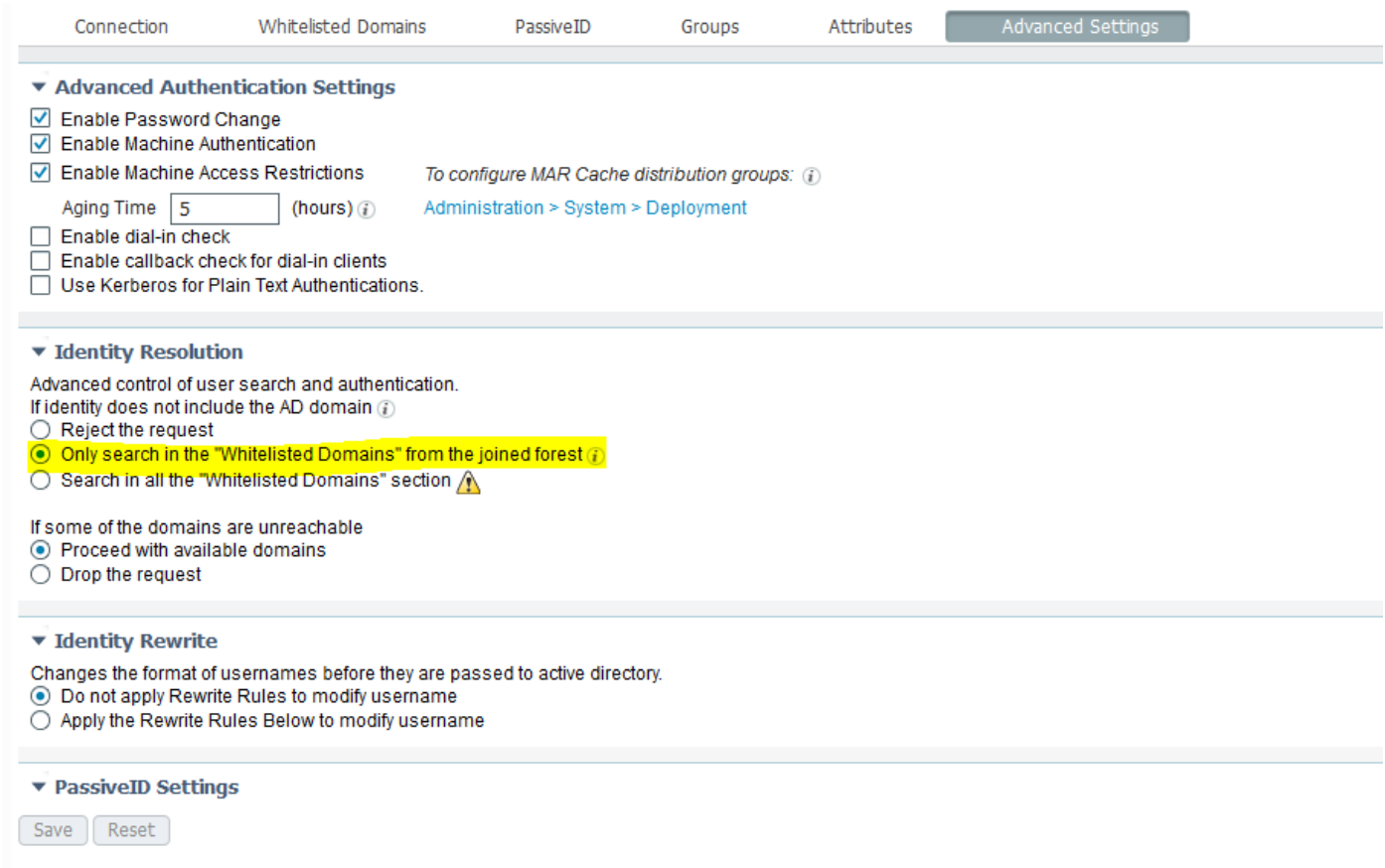
working scenario From the logs AD_agent.log:

```
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"
}
}
```

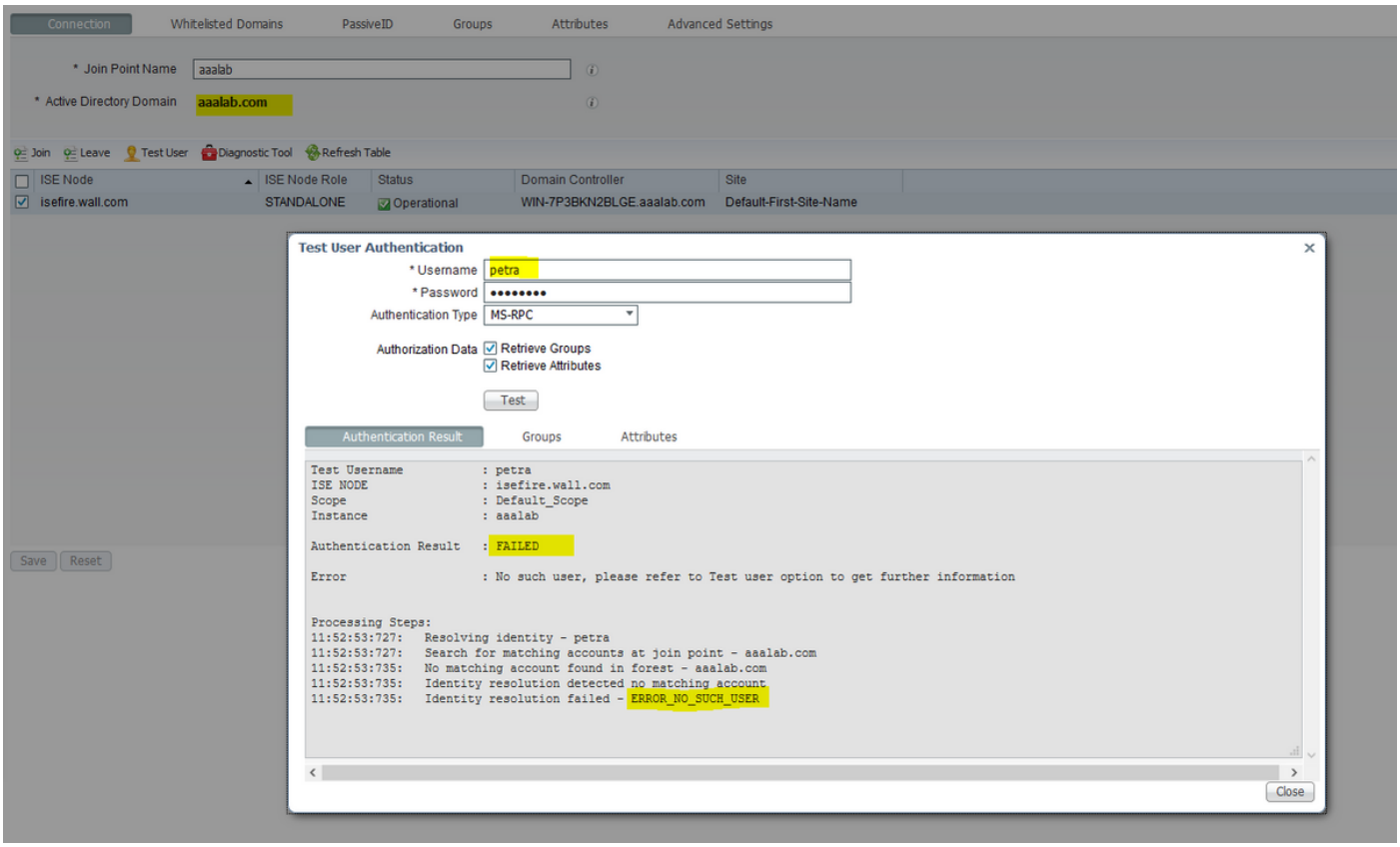
2. If the advance option "Only search in the "Whitelisted Domains" from the joined forest" checked:



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
```