Cisco live!

February 15 - 19, 2016 · Berlin, Germany

We’re ready. Are you?

BRKSEC-2132
What’s new in ISE Active Directory Connector

Christopher Murray

Technical Leader

Cisco live!

Agenda

- Introduction
- Deployment Tips
- New Features
- Q&A
- Wrap-up

Questions?

- Please ask questions as we go
- If very specific come see me after or book a MTE session

Feedback

- Your feedback is important
- Great opportunity to directly connect / influence
- If you have an AD issue or AD related feature request
  - I would love to hear about it
- Email chmurray@cisco.com
- Twitter @ChrisMurrayCSCO

Introduction

Warning!
Scotsman Ahead

Some History…

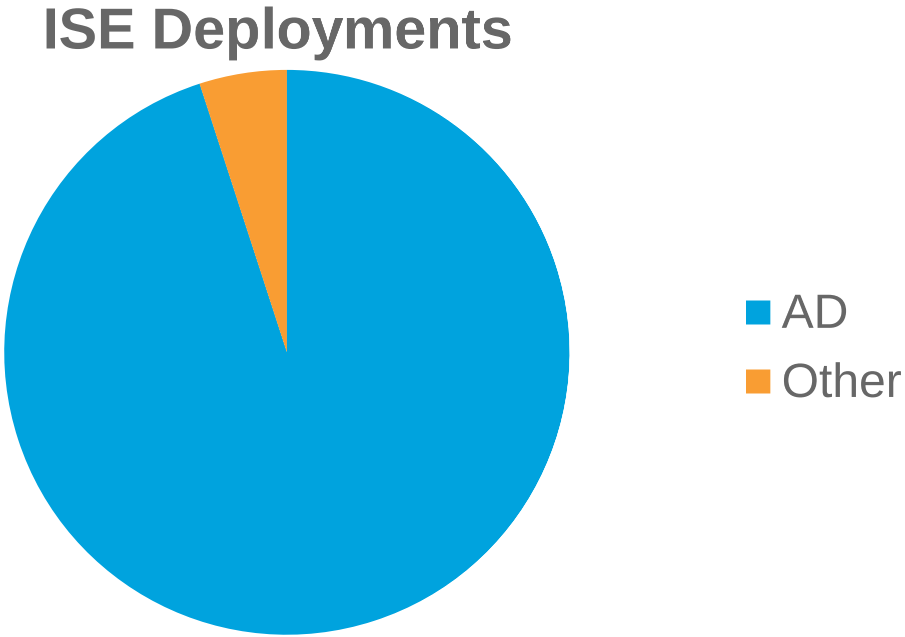
We replaced our AD connector in 1.3

Why?

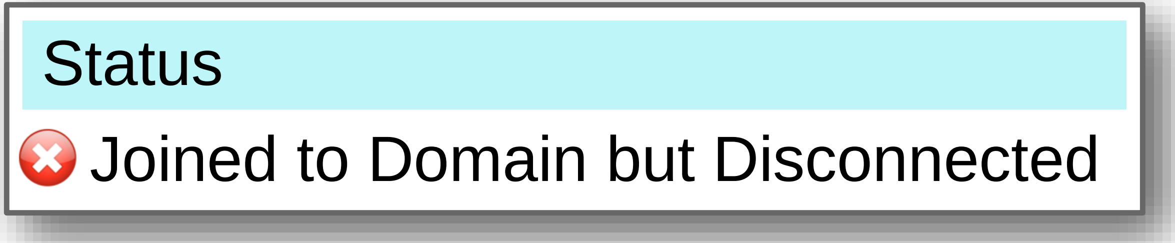
How many customers use AD with ISE?

?

Over 90%!



Seen this before?



Status
❌ Joined to Domain but Disconnected

Wondered where to look for more information?

You ask the AD and DNS guys if they did anything…

Your boss asks “who is in charge of this thing?”

Uh oh….

And then…

- You call Cisco TAC
- Various logs are exchanged
- Case gets escalated
- Various logs are exchanged
- Time passes… and probably more logs
- Meanwhile users are not getting service
- You know the rest...

- Maybe a simple environmental issue
- Why did it cause such mayhem?
- How can I avoid this in future?

Cisco live!

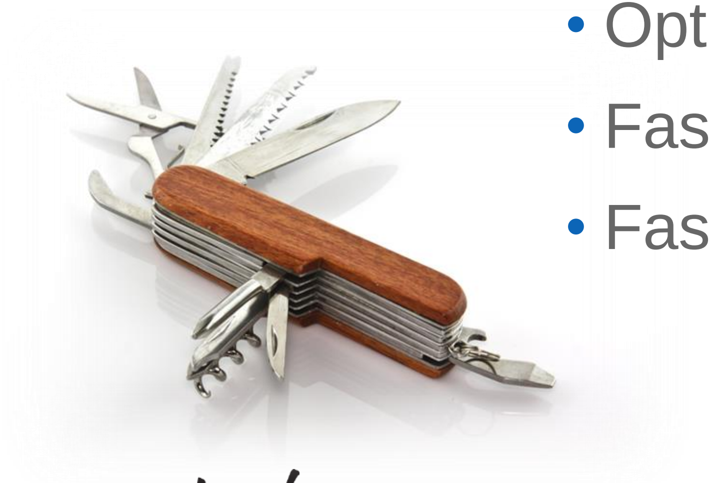
So we needed to do something

- 9/10 of you use AD with ISE
- Too many cases with slow resolution
- Old AD connector was vulnerable in some environments
- We were unable to make fixes and add features quickly
- And AD is a moving target

- We needed to OWN this problem to FIX this problem

OWN IT!

Introducing our new AD connector (since ISE 1.3)



- In-house dedicated team
- Optimized for our use cases
- Faster feature development
- Faster problem resolution

Take-aways for you today

3 ‘E’s

- Experience
  - Deployment Tips to minimize issues
  - Avoid some common mistakes
- Education
  - Deep dive on new AD connector features
  - Troubleshooting tips helping you to self-fix
  - And to ‘convince’ AD or DNS guys to step-in
- Engagement
  - Chat after
  - Book a slot with me in Meet The Engineer

Terminology

- DC
  - Domain Controller (also KDCs, GCs)
- Site
  - A subnet based AD logic grouping
- SID
  - Numeric representation of object in AD
- TGT
  - Ticket Granting Ticket (Kerberos)
- RODC
  - Read-only domain controller

- SAM name
  - Short form username, like “chris”
- UPN
  - Long form, like chris@cisco.com

New since ISE 1.3:

- Join Point
  - AD identity store instance
- Scope
  - Set of Join Points
  - Useful to limit identity search scope

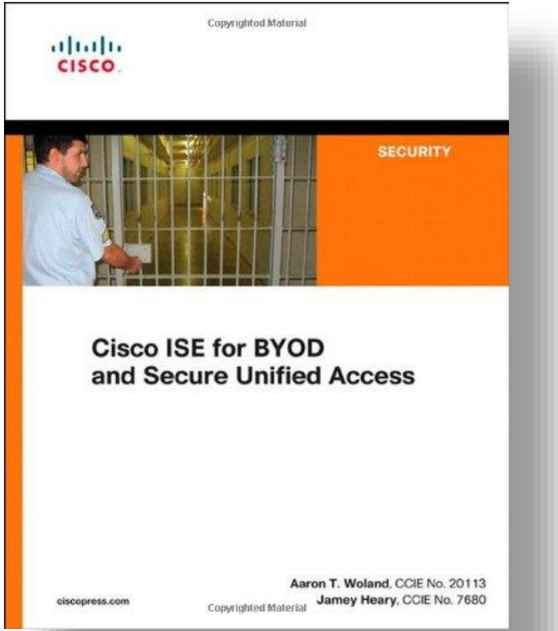
Deployment Tips

What would make your life easier?

- Having worked on 100s of cases
- Majority of AD ones were environment
- I was thinking what would be the best piece of advice?

- AD and its dependencies are complex with many variables…

Blatant plug



Copyrighted Material

SECURITY

Cisco ISE for BYOD and Secure Unified Access

ciscopress.com

Copyrighted Material

Aaron T. Woland, CCIE No. 20113
Jamey Heary, CCIE No. 7680

One of the first steps in the creation of any network access security policy (NASP) is the formation of the network access security policy ***committee****.”*

Cisco ISE for BYOD and Secure Unified Access
Aaron Woland, Jamey Hearey

Section III, Ch 6, Involving the Right People

- Security
- Networking
- Server
- Desktop support
- Company board member
- End-users

- Operations
- Security Incident Response Team
- Human resources
- Legal
- Audit
- Managers

Really?

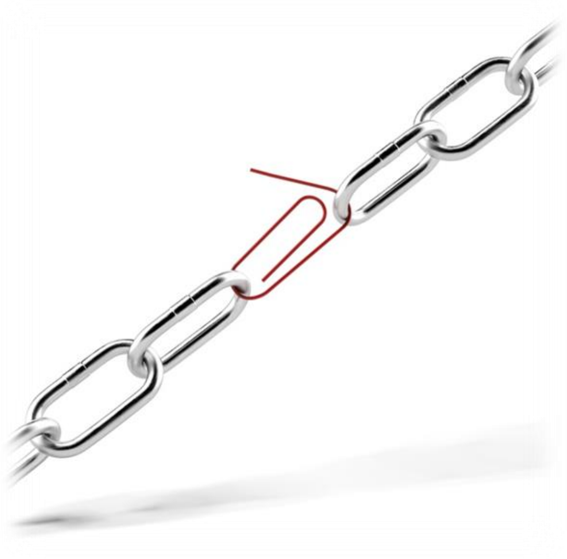
- Do customers really do that?
- Then I realized; that’s the point
- If they did, they would have less issues
- I’ve seen many configurations ranging from inefficient, ambiguous, right thru to wrong and actually insecure

Key point

Forming a **team** jointly responsible for a service and following some best practices will lead to a more stable service

The same is true for the AD connector

- When you join AD, you, the ISE admin, are no longer in full control of your network access service
- Even the new AD connector is only as good as the weakest link
- Network access is usually a critical service
- Therefore it should not be the sole responsibility of the ISE admin



Don’t go it alone

- Don’t join without engaging others
  - “Seems to work, I will roll with it”
  - You are throwing caution to the wind
  - Little sympathy from your AD / DNS guys when you need it most

- One little change in the environment
  - Shut down GC, retire a Site, remove a group, change permissions, delete machine account, block MS-RPC, install a hot fix, tweak DNS…

.. can render you in big trouble

Do it together

- Form a jointly responsible cross-functional team
- Communicate ISE’s needs from their services
- Optimize their services for ISE
- Factor in your future growth
- Get them working for you (monitor and scale)
- Communicate about outages, planned or not

And continual ownership, not just at roll-out

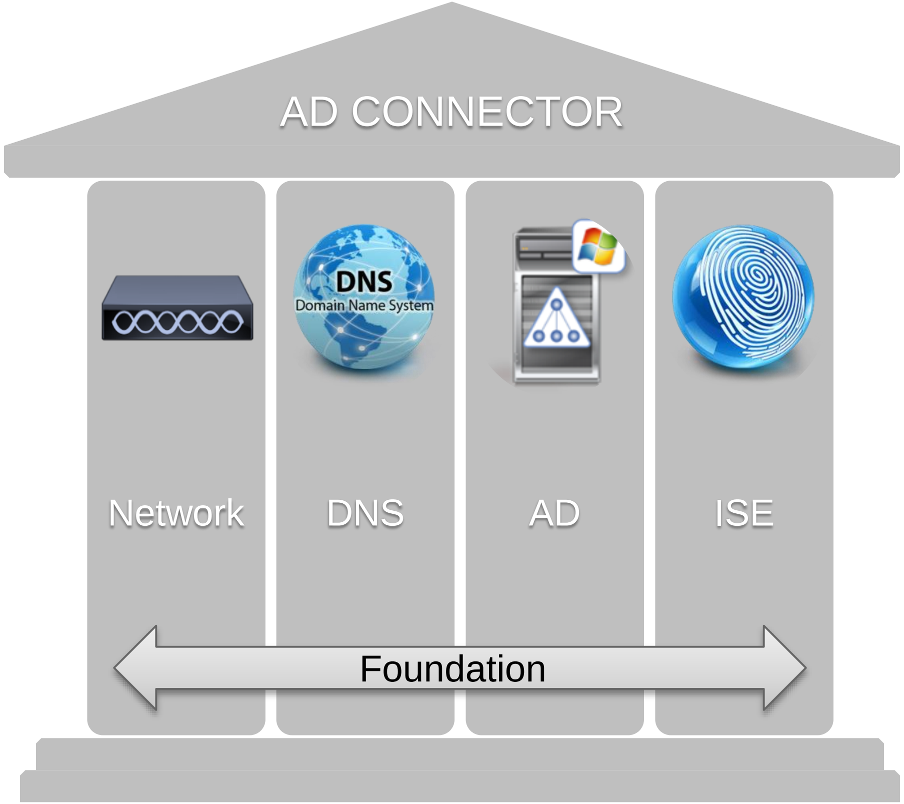
So which teams should be jointly responsible?

- At a minimum
  - DNS
  - Active Directory
  - Physical network

- Potentially also
  - Load balancing
  - Firewall
  - Hypervisor

i.e. anyone who can affect your service

Think of it like this



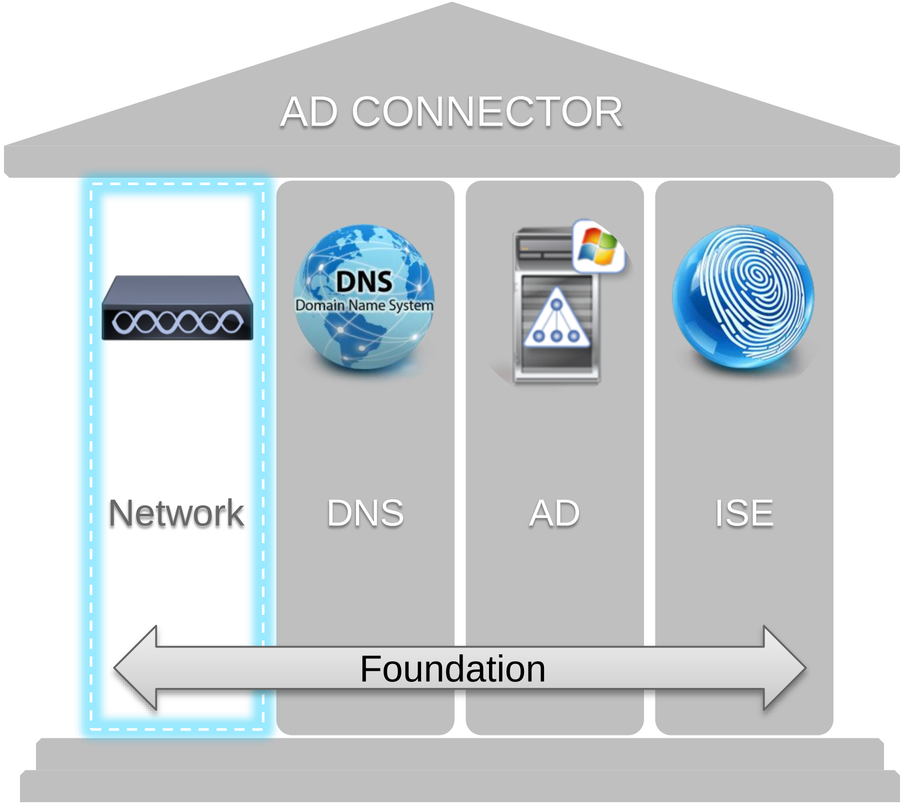
Key Point

Forming a **team** responsible for Network Access and following deployment tips will lead to a more stable service.

General guidelines for each dependency

- You are aiming for
  - Speed of retrieval
    - Their services need to be fast enough
  - Quality of information
    - Has optimized answers and not too much ‘noise’ or ‘fat’
  - Reliability of services
    - There should be no single point of failure
  - Scale
    - Scales per your requirements
    - Factor in future growth
- And
  - Proactively monitor

Network

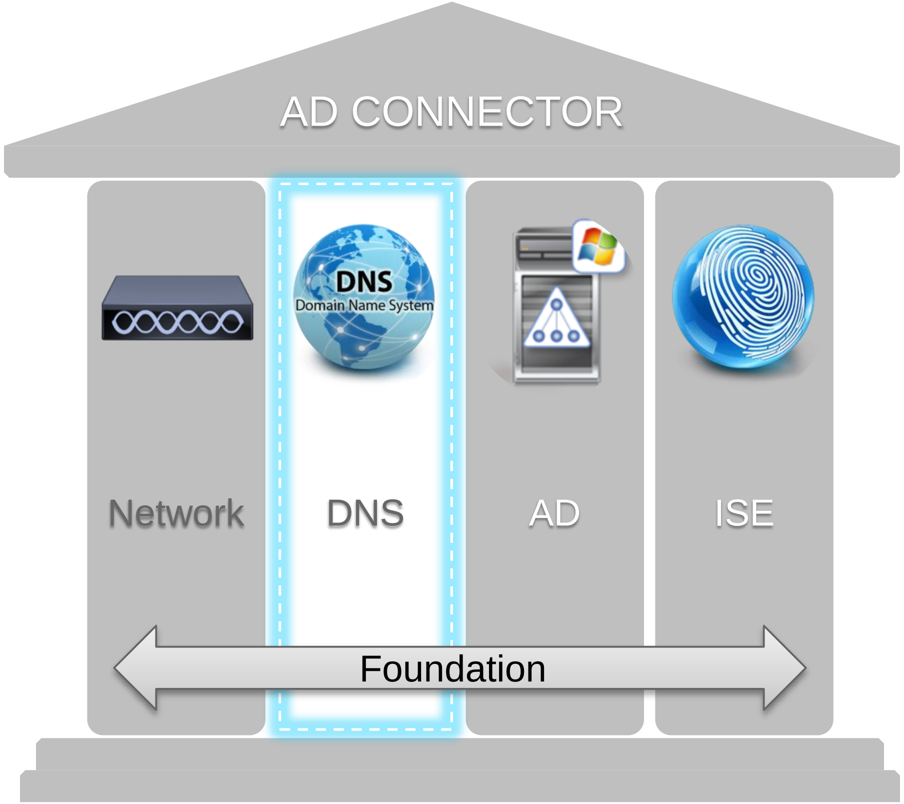

AD CONNECTOR
DNS
Domain Name System
Network
DNS
AD
ISE
Foundation

Network

- Sanity check
  - Eliminate packet issues
  - Got expected NIC speed or not?
- Bandwidth & Latency
  - Latency is your enemy
  - Check out Craig’s session
- Subnet/IP
  - Don’t just use arbitrary subnet/IP
  - You will need specific one for AD Site
- Geography
  - Are PSNs close to DCs / DNS?

- Reduce “sources of badness”
  - Scripts sending (bad) auths
  - Load balancer probes
  - Bad console/serial port noise
  - Misconfigured supplicants
- NADs
  - Beware short timeouts!
    - Supplicant race
    - WLC 3 second timeout
    - 10 sec minimum

DNS


AD CONNECTOR
DNS
Domain Name System
Network
DNS
AD
ISE
Foundation

DNS

- AD has tight integration with DNS
- Consequently, tight DEPENDENCE
- DNS is a big factor on stability

DNS

- DNS servers must know all records
  - You cannot split them across primary, secondary, tertiary…
- With multi-join this may need you to consolidate multiple DNS server information
  - Lots of ways to do that
    - Zone transfers, proxying, forwarding,..
- Do not use the same external DNS server you use for browsing etc
  - Insecure and slow

- Avoid using recursion or suffix substitution
  - Both slow things down without client knowledge and can lead to redundant queries
- Consider what happens when a bad domain name is received by ISE
  - You want this to fail FAST

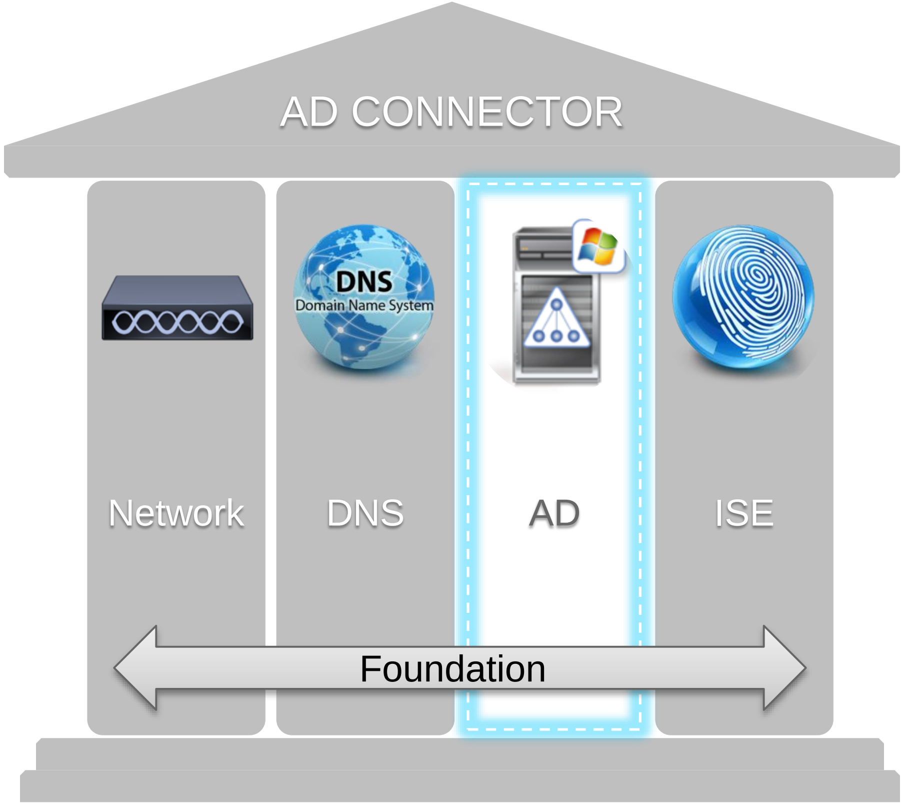
Example: customer case where ISE resolved domain over Internet…

DNS

- SRV records
  - Crucial for AD operation
  - Must be properly defined for GCs, DCs and KDCs, and for Sites
  - Admins should remove stale records
- PTRs
  - Should exist where possible
  - Kerberos insists on them sometimes
- Beware of replies over 4K
  - Can cause retry by TCP
  - Incurs performance hit
  - Use Sites!
  - Trim irrelevant additional records
- Not using Sites with a large number of DCs is recipe for disaster
- Optimize replies
  - Additional records contain IPs of relevant names in other records

Example: customer case where Site SRV reply has only 7 DCs but 100s of name server additional records, overflowing 4K

AD


AD CONNECTOR
DNS
Domain Name System
Network
DNS
AD
ISE
Foundation

AD

- Use SITES!

AD

- Use SITES!
- Use SITES!

AD – Key Point – Use Sites

- Use SITES!
- Use SITES!
- Use SITES!
- Tell your AD admin you want ISE machine accounts in correct AD Site geographically close to DCs
- Often a NEW Site exclusively for ISE is the BEST SOLUTION

AD – why use Sites?

- Make ISE use more predictable DCs
- Geographically efficient / near users
  - If defined correctly
- Site will contain list of DCs – usually much smaller list than all available
- Minimum 2 of each role (GC, DC, KDC) for HA
- Ideally no other services using these DCs except ISE
  - Why? Because NA is critical, right?

- Specific DNS records for your Site
- SRVs and additional records tuned
  - ‘A’ records (IPs) of hosts in additional records
  - Specific DCs used by ISE
- Helps keep
  - Number of records under control
  - Hence, DNS replies < 4K

AD – not using Site

- You are making it unpredictable which DC ISE uses
- Hard-coding DCs is not a good option
- AD guys usually don’t know you’ve done it
  - What happens if they alter or even retire a DC you are hardcoded to?
  - You will get no sympathy from them if they didn’t know

- How do you know if that DC is loaded or going down?
  - You are undermining lots of ‘smarts’ that AD provides
- AD Sites are the supported and best solution for many reasons
  - No DC coupling, faster/smaller responses
  - AD guys are aware your ISE machine accounts using the Site

One customer had over 1000 DCs, didn’t use Sites, reply was huge

AD

- Permissions (Key Point)
  - Explain the permissions ISE machine account requires
  - May require you to join specific OU
  - They can also move the ISE machine account after it is created (by ISE) – usually easier
  - Beware of AD hardening

  NOTE: 1.3 has new permission requirement: “Read tokenGroups”

- The machine account name is derived from appliance hostname
- Show them OS properties of ISE machine account (more later)
  - They should not edit this account without your permission
  - Nor alter its assigned permissions

AD

- Clean out old SIDs
- Clean out expired userCertificates
- Check/fix AD issues
  - Often I hear “our AD is fine, other apps are working”
  - That does not mean AD is OK

  - ISE has much heavier demands from AD and sometimes shows issues not apparent
  - Replication issues are common and not obvious until an AD admin looks..

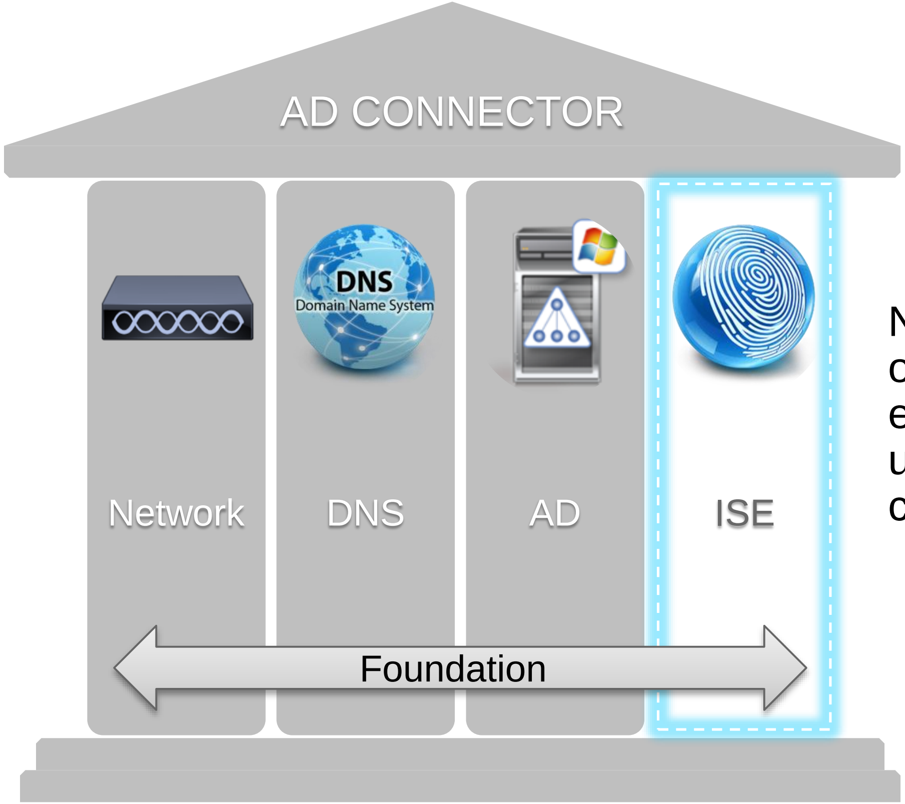
- Ask for heads-up when
  - Rebooting or patching servers in your Site
  - Ask them to validate any planned DC changes with ISE
    - Various Windows patches have broken ISE in the past

AD

- For NA machine accounts (not ISE)
  - These must have SPN attribute
    - servicePrincipalName
  - If not, they must create one
  - It is multi-valued and you should add an entry for short-form and FQDN
  - E.g.
    - HOST/laptop;HOST/laptop.domain.com

- Scripts exist to do that
- Basically look at dnsHostname attribute as start

ISE



Noticed that only one of the four foundation elements is typically under ISE admin control?

ISE

- Site
  - Get appropriate Site from AD team
  - Check you’re in an appropriate AD site
  - If not, tell AD guys which account domains ISE needs to access and which data center it is in
    - They will arrange appropriate Site
    - This often means a specific subnet/IP for ISE appliance
- Distributed deployment
  - Usually entails different Sites

- IP and subnet mask
  - This should really come from the AD team once they decide your Site
- OU
  - Which OU should you join?
  - Ask AD guys after explaining permissions required
- Once joined
  - Use Test User feature to verify performance of authentication, groups and attributes

ISE

- DNS
  - Remember ISE appliance DNS servers must know ALL AD DNS records you care about
- NTP
  - Set correct time and timezone
  - Kerberos needs to be within 5 mins of the DCs you use
    - More than that = game over
    - That could be many DCs
    - Best use same clock sync source
    - Be careful of DST settings/changes

- Running under a hypervisor?
  - Don't skimp on VM resources
  - Dropping cores for example
    - Can impact our threading
    - EAP-TLS needs MHz
  - Beware of clock drift
  - Don't pause VM for too long
    - Typically 30 days will cause problems

ISE – Key Point - use indexed attributes

- Attributes
  - Strive to use GC indexed attributes
  - If not, consider making them indexed
  - If can’t, use another attribute or group
  - Using a non-indexed attribute can be a time bomb to slowness
  - It may work fast at first…

- Groups
  - Uses SIDs internally in 1.3
  - Fetching speed significantly faster
  - Resilient to renames externally
  - Resilient to unresolvable SIDs
  - BUILTINs now supported
  - Requires new AD permission though

Example: 90 seconds fetch time after one month

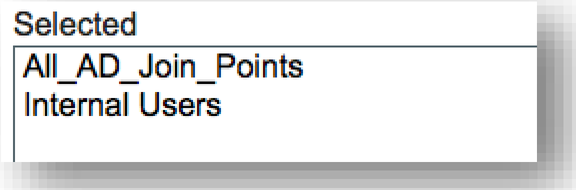
ISE - usernames

- Usernames
  - Encourage domain qualified
    - UPNs like chris@domain.com
    - FQDN like host/machine.domain.com
  - SAMs (e.g. “chris”)
    - Can be slower/ambiguous
    - And lead to account lockouts
    - Can be alleviated with authen policy
      - E.g. direct to specific Join Point by NDG
    - Or can be blocked altogether by ISE

- Reduce sources of bad usernames
  - Especially from scripts
  - Bad console/serial ports
  - Load balancer probes
  - Periodic monitoring
    - Configure new AD Alarms
- Filtering them from MNT help but is not as good

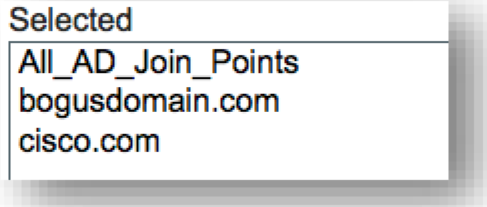
ISE – optimize identity sequences

- Optimize identity sequences
  - Do not check AD first, then internal
    - Check internal first
  - Don’t put > 1 join point in an identity sequence
    - Use a scope with specific join points
    - It evaluates more efficiently



Selected

All_AD_Join_Points
Internal Users



Selected

All_AD_Join_Points
bogusdomain.com
cisco.com

Customer who got it all wrong.. again

The customer who got it wrong

- Didn’t have SLA with other teams (AD, DNS)
- Didn’t grow infra as number of ISE endpoints and objects in AD increased
- Didn’t clean up or optimize DNS
- Didn’t remove old SIDs
- Didn’t remove old certs
- Had too small NAD timeouts (3 sec in some cases)

- Use Load Balancer which undermined some client aspects
- Used unindexed DN attribute
- Pointed ISE at loaded DC
  - Yes in a Site, but not just ISE using it
- Had AD before internal in idseq
- Had 9 second intermittently delay in DC and others in DNS

Things got quite heated…

Latency example

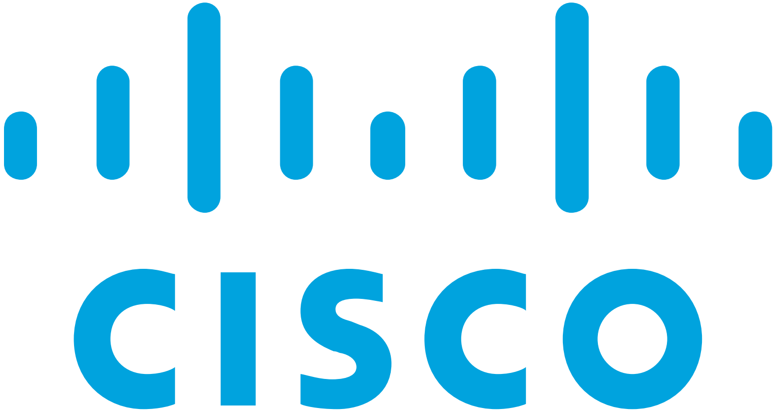
```
Dec  3 04:11:58 acs-bgl-1 adclient[6006]: DEBUG <fd:23
CAPIAuthValidatePlainTextUser > base.bind.cache ADCB::search base , filter
(&(objectClass=User)(|(objectCategory=Person)(objectCategory=Computer))(sAMA
ccountName=fred)), attrs 2 (cacheOps=7, GC=0)
```

```
Dec  3 04:12:32 acs-bgl-1 adclient[6006]: DIAG  <fd:23
CAPIAuthValidatePlainTextUser > base.bind.ldap 192.168.129.155:389 search
base="DC=cisco,DC=com" filter="(&(objectClass=U
```

… yes that’s 34 seconds to look something up in AD!

shouldn’t name names but…

it was..



And one year later..

It happened again.. Total WiFi outage

I believe that we have avoided this for too long, and after every P1 we come up with the same recommendation.

ISE IT Manager
Cisco

A memory leak on the AD PDC was provoked by 6 domain controllers that were missing a patch.

Directory admin
Cisco

> *This is a wakeup call as to how critical ISE and it’s dependent services are to the network.*

Directory admin
Cisco

Don’t be this guy

Learn from those mistakes

Forming a **team** responsible for Network Access and following deployment tips will lead to a more stable service.

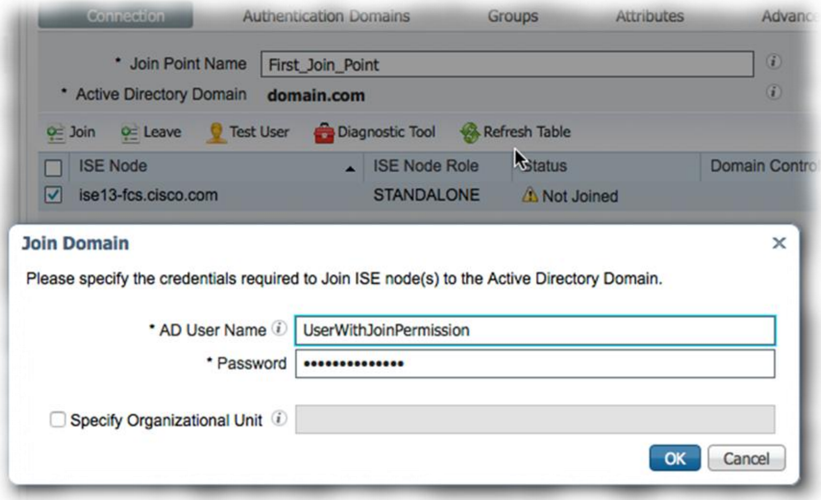
New Features

Summary of main ISE AD features (since 1.3)

- Up to 50 concurrent joins points
- New alarms and report
- Diagnostics built into ISE GUI
- Identity hunting / ambiguity resolution
- Scope mode
- Smarter certificate support
- Improved integration and failover

Join operation

- In 1.3, ISE machine account needs
  - “Read tokenGroups” permission
- Ask your AD admin to assign it
- Longer hostnames are supported
  - Up to 63 characters
  - Be wary of very long hostnames
    - The latter characters are hashed
    - Not predictable – do join, then look



* Join Point Name: First_Join_Point

* Active Directory Domain: domain.com

☐	ISE Node	ISE Node Role	Status	Domain Contro
☑	ise13-fcs.cisco.com	STANDALONE	⚠ Not Joined	

Join Domain ✕

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

* AD User Name: UserWithJoinPermission

* Password: •••••••••••••••

☐ Specify Organizational Unit

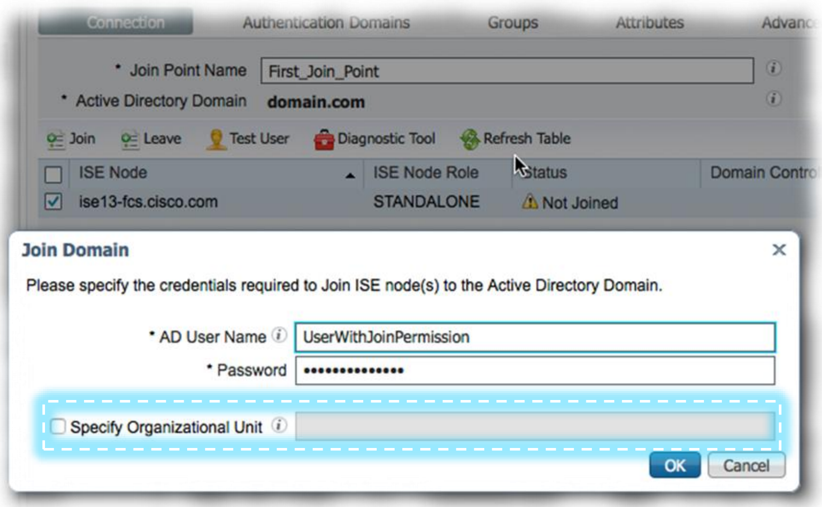
Join directly to OU

- You can now specify OU at join time
- You need to escape any special characters with a backslash

Example

```
OU=Cisco ISE\,US,OU=IT
Servers,OU=Servers\, and
Workstations,DC=someDomain,D
C=someTLD.
```

OU = Organizational Unit



* Join Point Name: First_Join_Point

* Active Directory Domain: domain.com

☐	ISE Node	ISE Node Role	Status	Domain Contro
☑	ise13-fcs.cisco.com	STANDALONE	Not Joined	

Join Domain

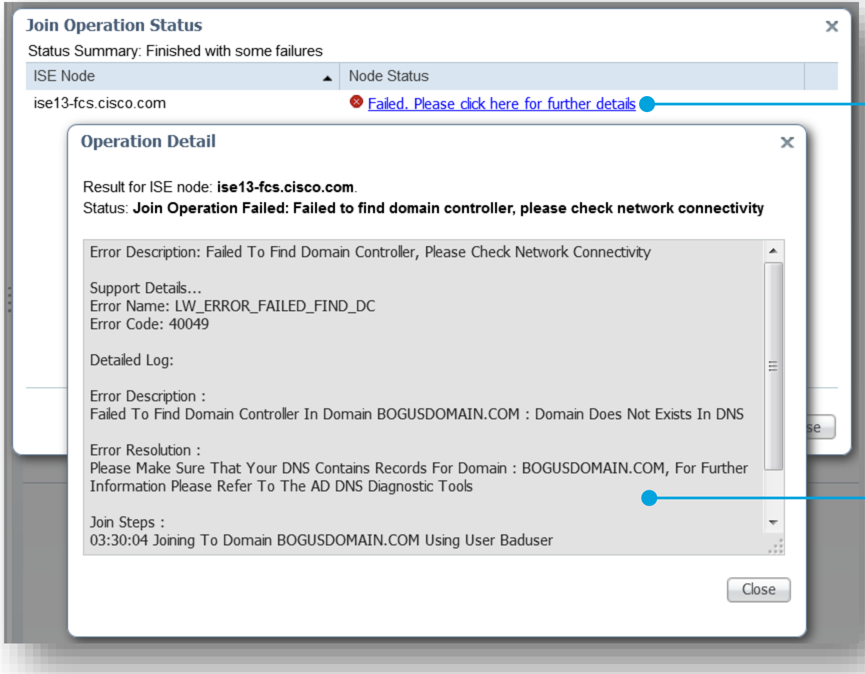
Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name: UserWithJoinPermission

* Password: •••••••••••••••

☐ Specify Organizational Unit

New detailed status if join fails



Join Operation Status
Status Summary: Finished with some failures
ISE Node
Node Status
ise13-fcs.cisco.com
Failed. Please click here for further details
Operation Detail
Close

Result for ISE node: **ise13-fcs.cisco.com**.

Status: **Join Operation Failed: Failed to find domain controller, please check network connectivity**

```
Error Description: Failed To Find Domain Controller, Please Check Network Connectivity

Support Details...
Error Name: LW_ERROR_FAILED_FIND_DC
Error Code: 40049

Detailed Log:

Error Description :
Failed To Find Domain Controller In Domain BOGUSDOMAIN.COM : Domain Does Not Exists In DNS

Error Resolution :
Please Make Sure That Your DNS Contains Records For Domain : BOGUSDOMAIN.COM, For Further
Information Please Refer To The AD DNS Diagnostic Tools

Join Steps :
03:30:04 Joining To Domain BOGUSDOMAIN.COM Using User Baduser
```

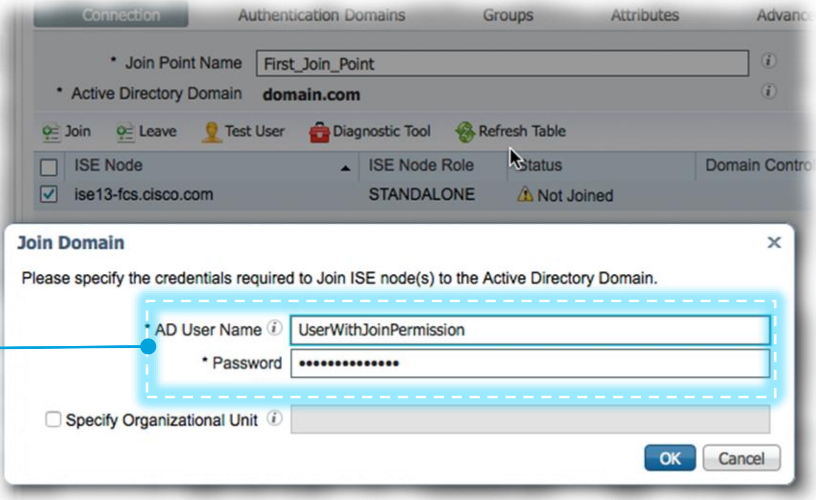
Click if join fails

Popup appears

Details on why join failed and resolution

Original join credentials are NOT stored

- The credentials used for a join are **not** stored permanently
- Only used to join ISE to AD and configure ISE’s machine account
- Tip: If you have problems joining, ask for elevated user like Domain Admin
  - Reassure the AD admin the password is not stored
  - They can disable or destroy it after



* Join Point Name: First_Join_Point

* Active Directory Domain: domain.com

☐	ISE Node	ISE Node Role	Status	Domain Contro
☑	ise13-fcs.cisco.com	STANDALONE	⚠ Not Joined	

Join Domain ✕

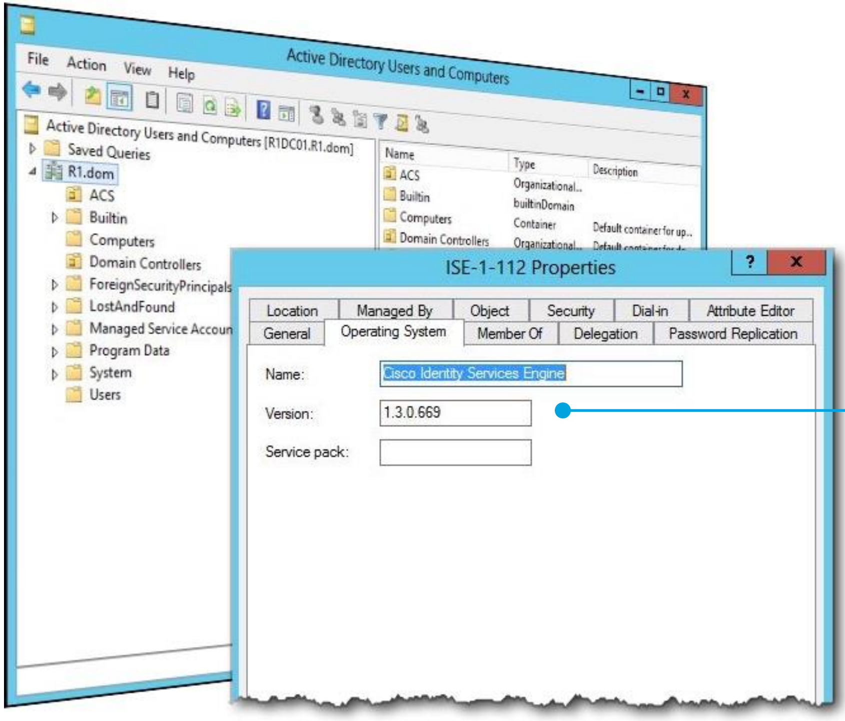
Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name: UserWithJoinPermission

* Password: •••••••••••••••

☐ Specify Organizational Unit

ISE machine account properties



Name: Cisco Identity Services Engine

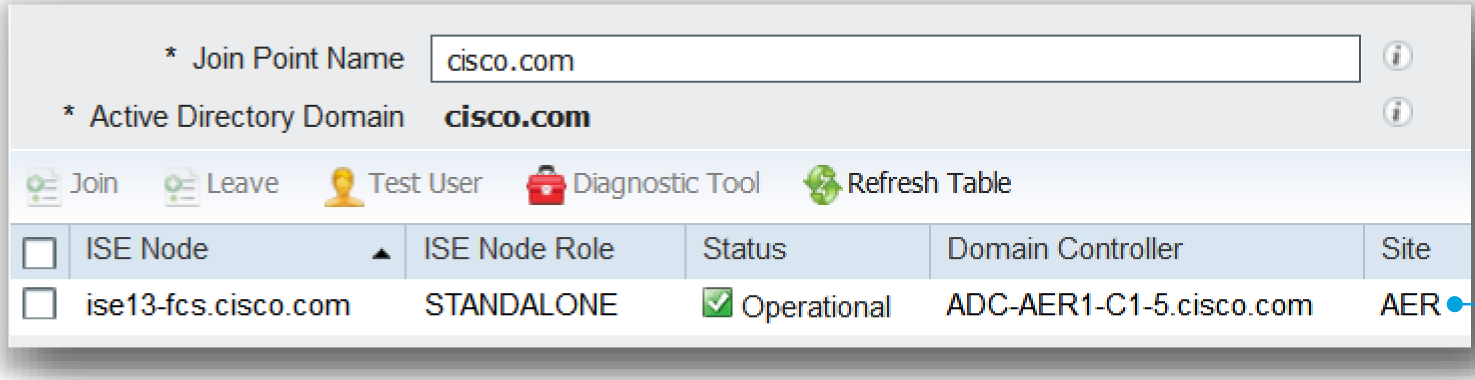
Version: 1.3.0.669

Service pack:

- When ISE does the Join (as opposed to doing it manually in AD)
  - Sets various attributes
  - Including the OS name and version
- This is useful for AD admins
  - Locating ISE machine accounts
  - Check its version of ISE
  - Helps deter unintentional changes when AD admin is unsure what the account is

Join – improved status display

- Verify the correct DC and Site have been negotiated
- Key point: be wary if Site says “Default-First-Site-Name” or “Not configured”
  - This means AD has not assigned this ISE machine to a specific Site
  - Not using a Site can lead to various problems and is not recommended



* Join Point Name: cisco.com

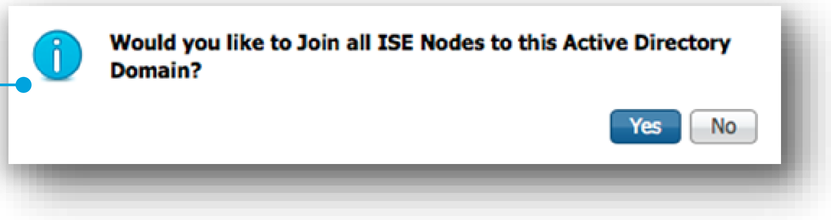
* Active Directory Domain: **cisco.com**

□	ISE Node ▲	ISE Node Role	Status	Domain Controller	Site
□	ise13-fcs.cisco.com	STANDALONE	✓ Operational	ADC-AER1-C1-5.cisco.com	AER

Check Site

Joining other PSNs

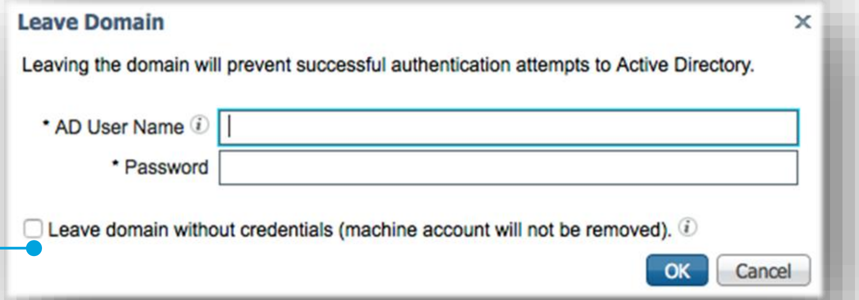
- You will be asked if other PSNs should join the same domain
  - Usually you say **Yes** here as it saves time joining other PSNs



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

Leave

- Leave has been enhanced to leave individual join points
- Force option
  - Removes join point from ISE but not the machine account from AD
- When to use force?
  - You don’t have credentials to do it
  - You don’t want to delete the account
    - e.g. you intend to rejoin and want it’s permissions kept intact
  - The domain or DCs are unavailable



Leave Domain

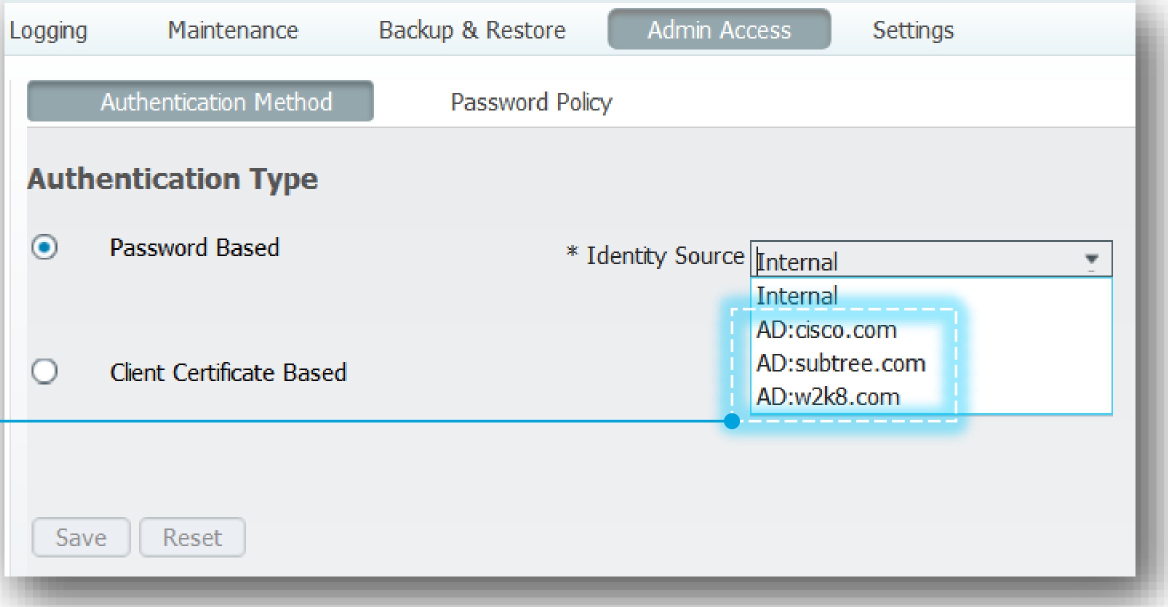
Leaving the domain will prevent successful authentication attempts to Active Directory.

* AD User Name:

* Password:

☐ Leave domain without credentials (machine account will not be removed).

ISE admins can log into ISE GUI with AD accounts



Authentication Type

● Password Based

○ Client Certificate Based

* Identity Source: Internal

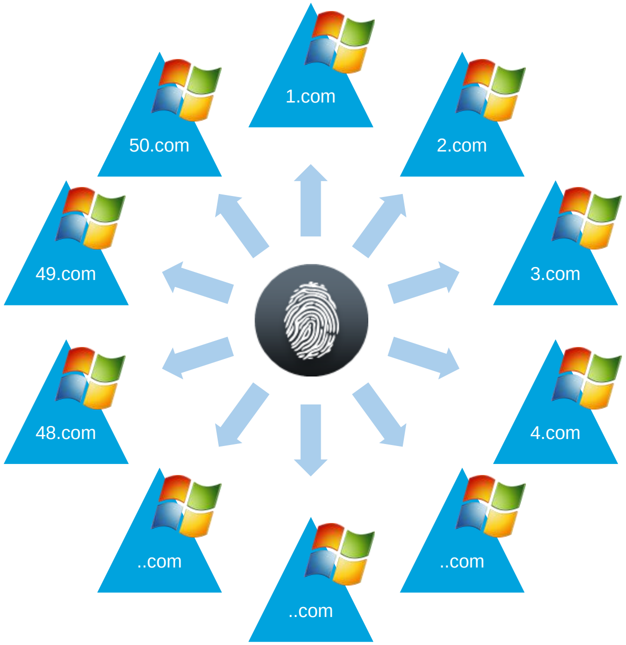
- Internal
- AD:cisco.com
- AD:subtree.com
- AD:w2k8.com

AD join points

Select one to log into ISE GUI with AD user

Multi join

- Now able to join up to 50 times
  - Either to different forests or different domains (in same forest)
- Use cases
  - Acquisitions
    - Use separate IT infrastructures
  - Untrusted sub-organizations
    - Don’t even know each other
  - Use existing separate ADs
    - Staff/students
    - Lab/production
  - Bypass permission issues (like 1-way)
    - Tip: join either side of trust



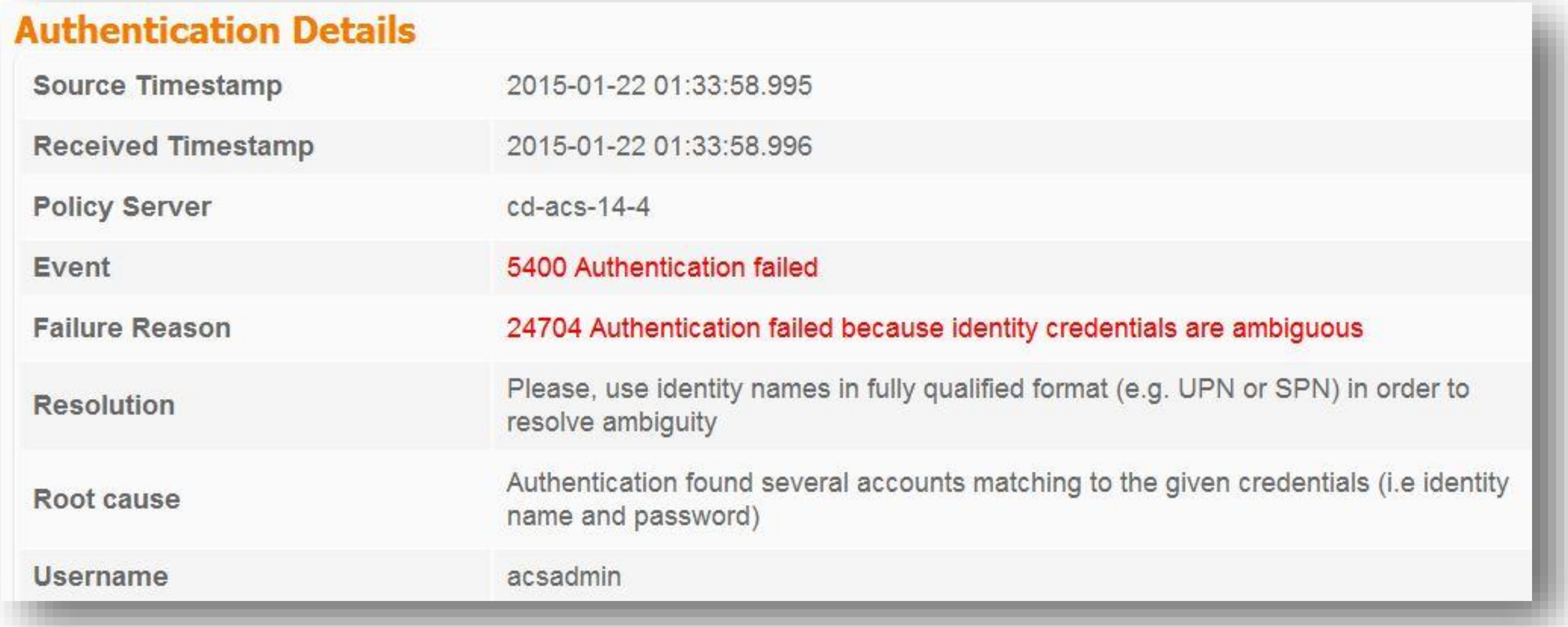
Multi join – brings new complications

- Recall that DNS server must know all records – for all join points
  - You may have to consolidate some external DNS server records
- Identity ambiguity
  - Usernames may not be unique
  - How can you even control that?
- Performance
  - Searching more places takes longer
- Security, information leakage
  - Sending credentials to wrong targets

Ambiguous identities

- Namespaces (usernames, domains) may not be unique especially with multi-join
  - You often have no control over these
- Authentication must fail if the identity cannot be resolved uniquely
- There is extra cost to hunt for ambiguous identities
  - Try to avoid by using qualified names
  - But if you can’t there are some options to control what happens

Ambiguous username - example



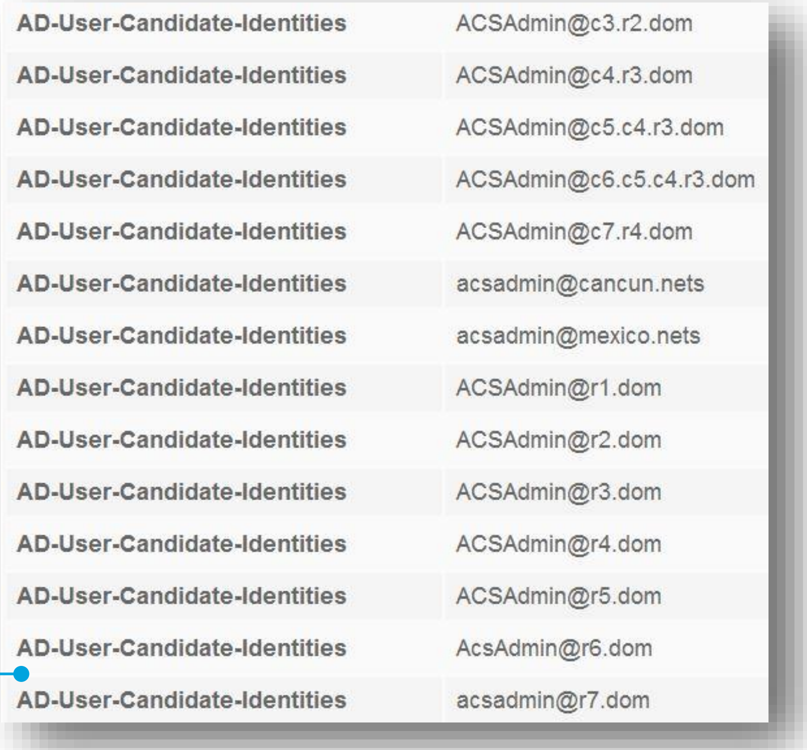
Authentication Details

Source Timestamp	2015-01-22 01:33:58.995
Received Timestamp	2015-01-22 01:33:58.996
Policy Server	cd-acs-14-4
Event	5400 Authentication failed
Failure Reason	24704 Authentication failed because identity credentials are ambiguous
Resolution	Please, use identity names in fully qualified format (e.g. UPN or SPN) in order to resolve ambiguity
Root cause	Authentication found several accounts matching to the given credentials (i.e identity name and password)
Username	acsadmin

Ambiguous username – useful attributes

- Authentication Details
  - Improved STEPS and Other Attributes to help locate ambiguity
- “Other Attributes”
  - To locate the conflict, look at
    - AD-User-Candidate-Identities
    - AD-Host-Candidate-Identities
  - These are the candidate identities

Quite a few acsadmin users!

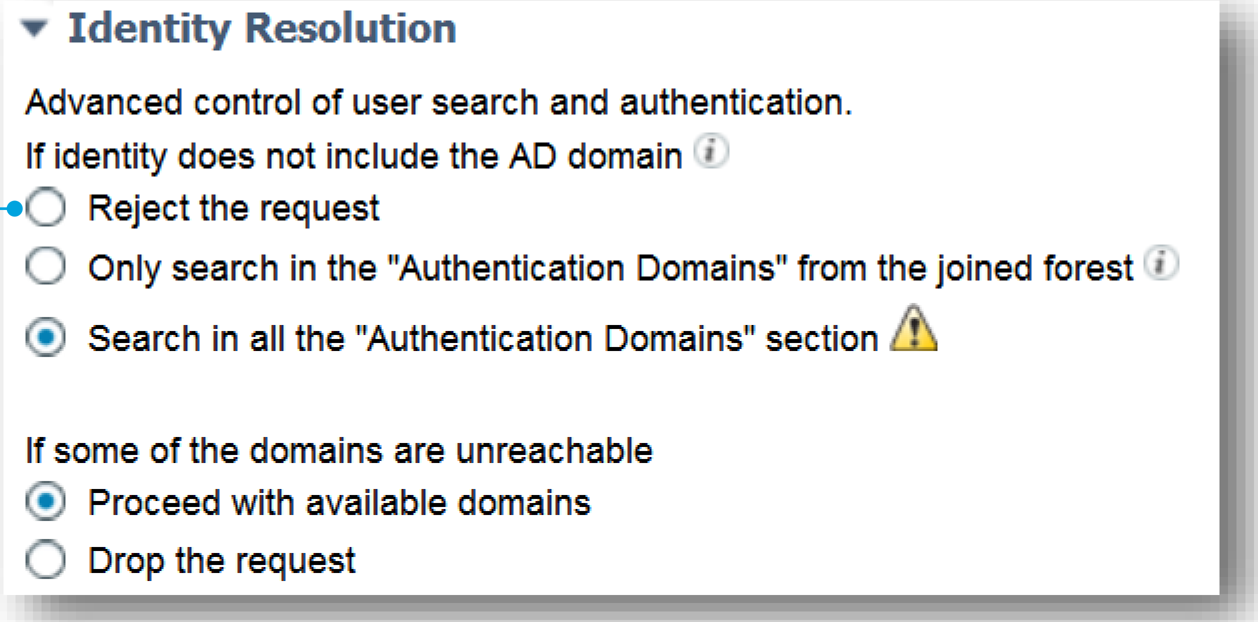


AD-User-Candidate-Identities	ACSAdmin@c3.r2.dom
AD-User-Candidate-Identities	ACSAdmin@c4.r3.dom
AD-User-Candidate-Identities	ACSAdmin@c5.c4.r3.dom
AD-User-Candidate-Identities	ACSAdmin@c6.c5.c4.r3.dom
AD-User-Candidate-Identities	ACSAdmin@c7.r4.dom
AD-User-Candidate-Identities	acsadmin@cancun.nets
AD-User-Candidate-Identities	acsadmin@mexico.nets
AD-User-Candidate-Identities	ACSAdmin@r1.dom
AD-User-Candidate-Identities	ACSAdmin@r2.dom
AD-User-Candidate-Identities	ACSAdmin@r3.dom
AD-User-Candidate-Identities	ACSAdmin@r4.dom
AD-User-Candidate-Identities	ACSAdmin@r5.dom
AD-User-Candidate-Identities	AcsAdmin@r6.dom
AD-User-Candidate-Identities	acsadmin@r7.dom

Identity resolution controls

Reject

SAM names not permitted at all



▾ Identity Resolution

Advanced control of user search and authentication.

If identity does not include the AD domain ⓘ

○ Reject the request

○ Only search in the "Authentication Domains" from the joined forest ⓘ

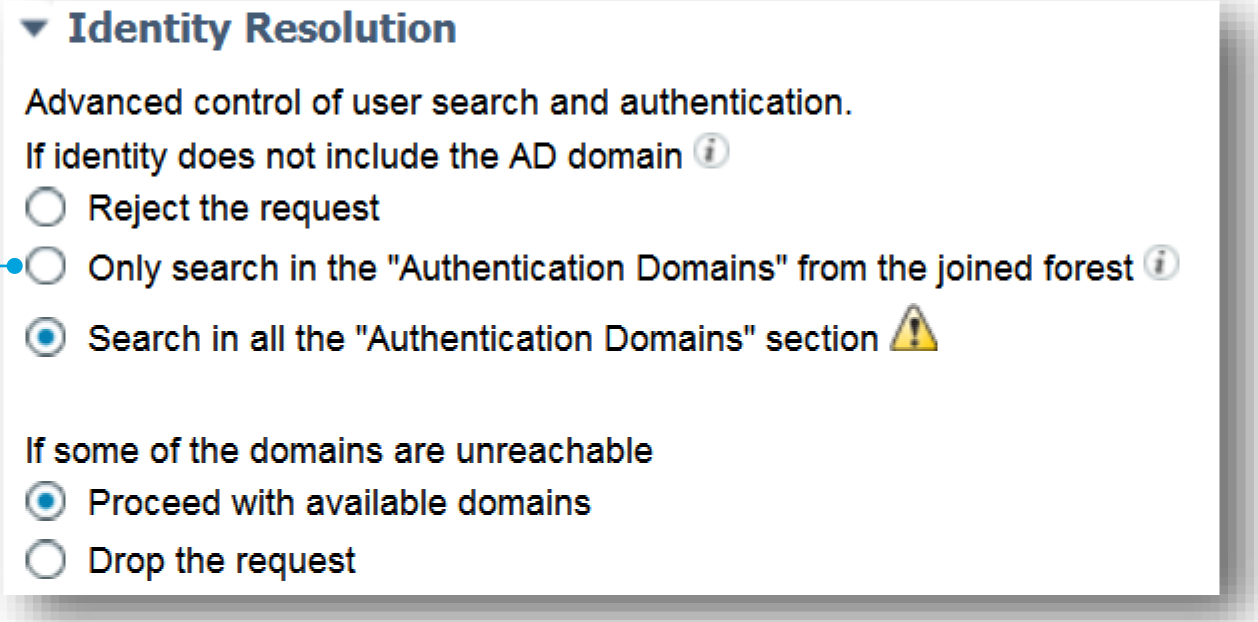
● Search in all the "Authentication Domains" section ⚠

If some of the domains are unreachable

● Proceed with available domains

○ Drop the request

Identity resolution controls



▾ **Identity Resolution**

Advanced control of user search and authentication.

If identity does not include the AD domain ⓘ

○ Reject the request

○ Only search in the "Authentication Domains" from the joined forest ⓘ

● Search in all the "Authentication Domains" section ⚠

If some of the domains are unreachable

● Proceed with available domains

○ Drop the request

Intra-forest

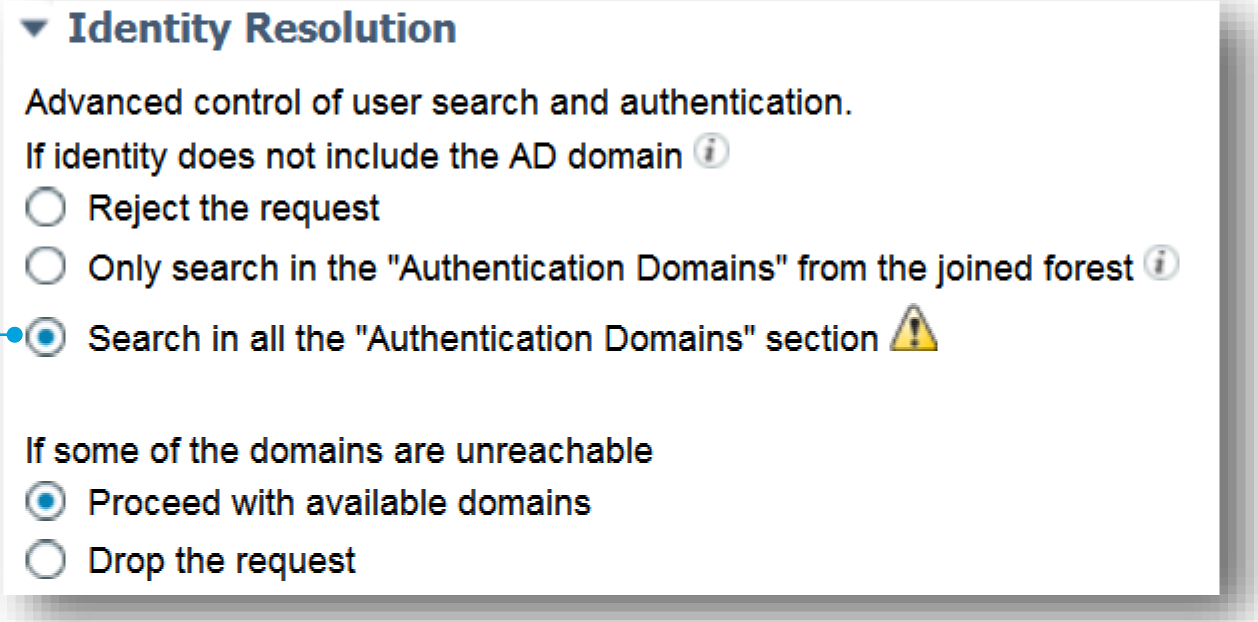
Only search in the join point's forest

This is similar to ISE 1.2 behavior

Identity resolution controls

Search everywhere

Subject to Auth Domains white list



Identity Resolution

Advanced control of user search and authentication.

If identity does not include the AD domain

○ Reject the request

○ Only search in the "Authentication Domains" from the joined forest

● Search in all the "Authentication Domains" section ⚠

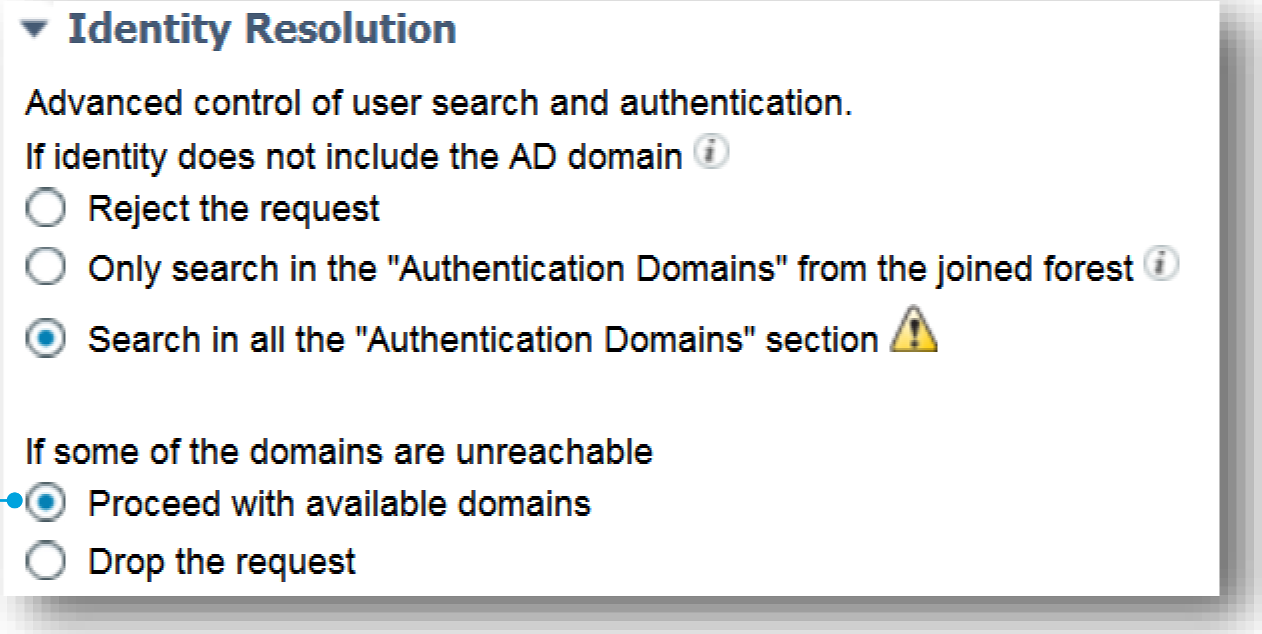
If some of the domains are unreachable

● Proceed with available domains

○ Drop the request

The recommended setting but ensure you optimize Authentication Domains

Identity resolution controls



▾ **Identity Resolution**

Advanced control of user search and authentication.

If identity does not include the AD domain ⓘ

○ Reject the request

○ Only search in the "Authentication Domains" from the joined forest ⓘ

● Search in all the "Authentication Domains" section ⚠

If some of the domains are unreachable

● Proceed with available domains

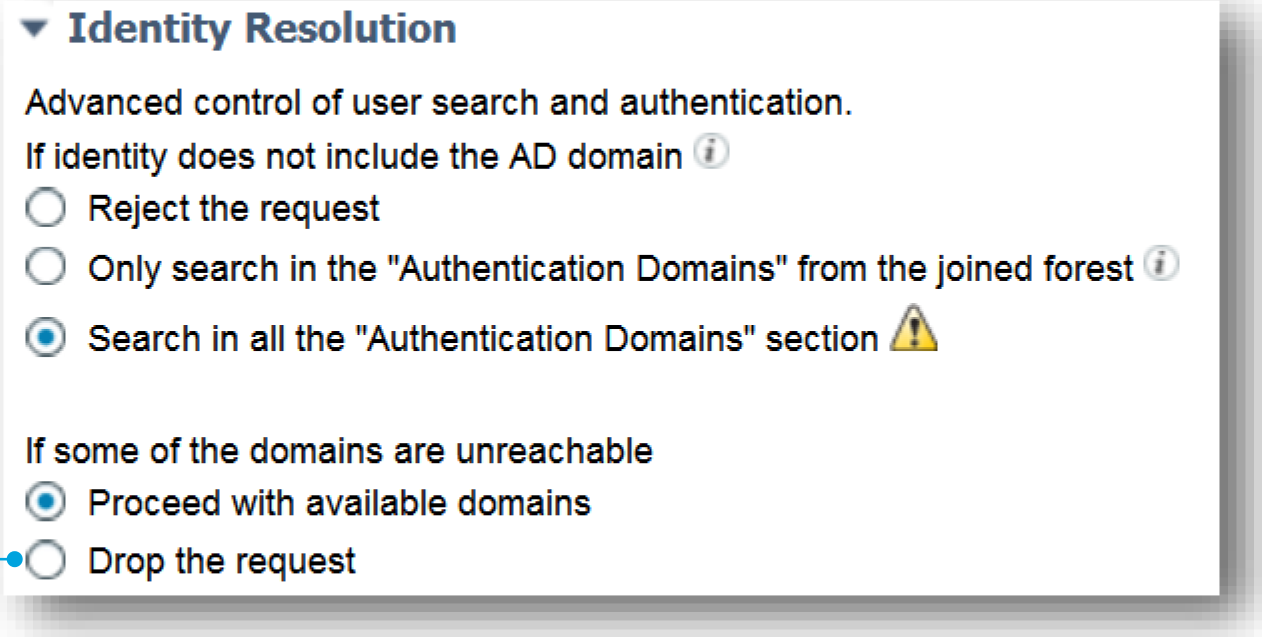
○ Drop the request

Skip bad domains

Other domains not affected

The recommended setting but doesn’t guarantee uniqueness if domain(s) offline

Identity resolution controls



Identity Resolution

Advanced control of user search and authentication.

If identity does not include the AD domain

○ Reject the request

○ Only search in the "Authentication Domains" from the joined forest

● Search in all the "Authentication Domains" section ⚠

If some of the domains are unreachable

● Proceed with available domains

○ Drop the request

Guarantees unique

But one unreachable domain impacts all

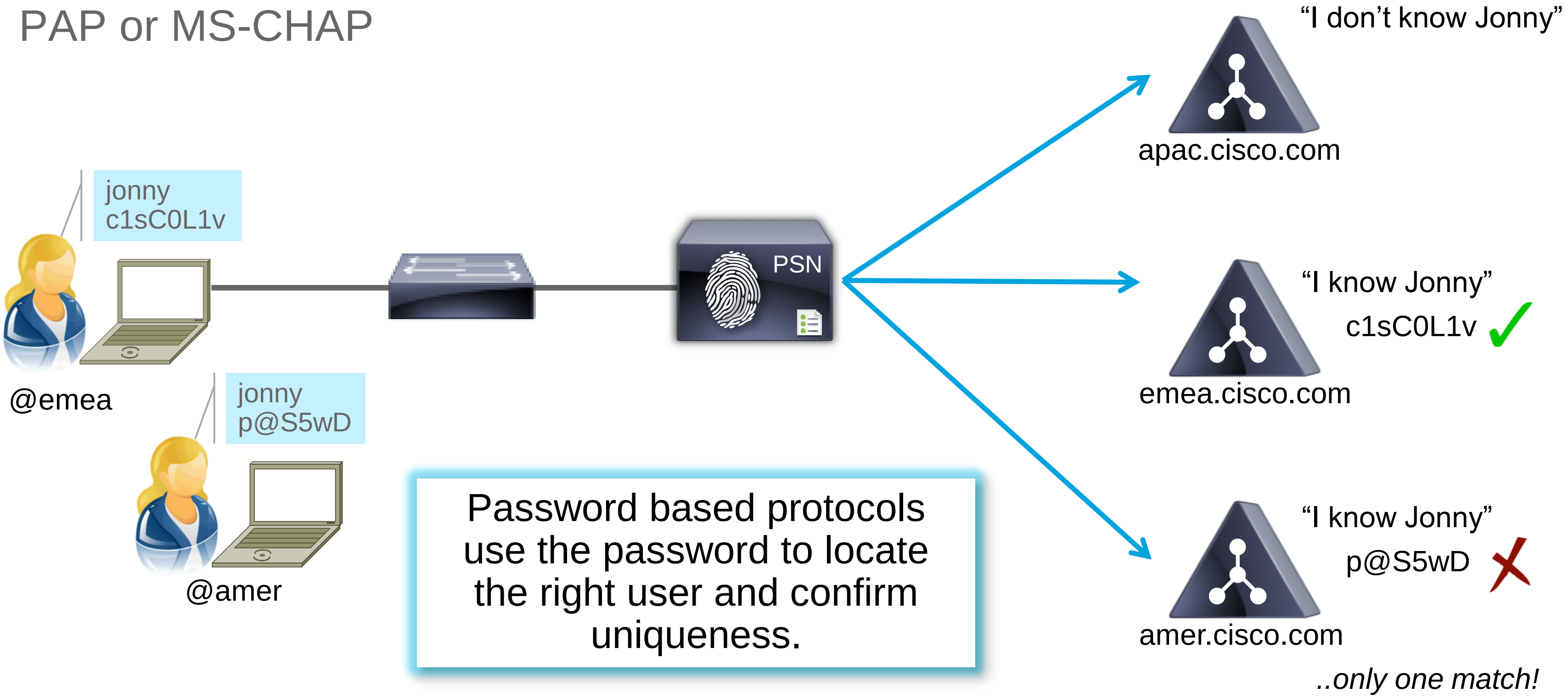
…most secure but one offline domain (in Auth Domains) will cause failures

Identity resolution algorithms – mailman analogy

- Imagine a mailman has a poorly addressed envelope to deliver
- He knows two recipients on his round called "Jonny"
- Return to sender?
- What if he peeked at the contents and verified it against each candidate?

Identity resolution

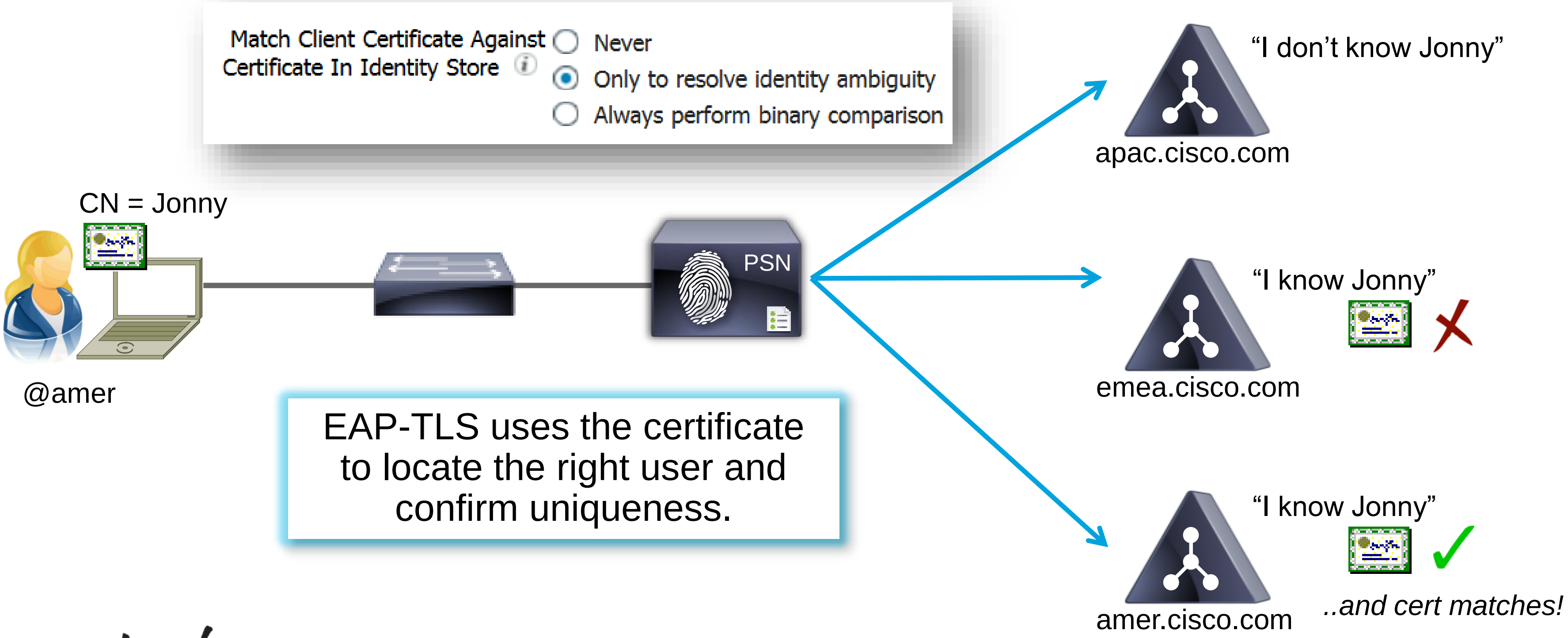
PAP or MS-CHAP



Password based protocols use the password to locate the right user and confirm uniqueness.

Identity resolution

EAP-TLS



Match Client Certificate Against Certificate In Identity Store ⓘ

○ Never

● Only to resolve identity ambiguity

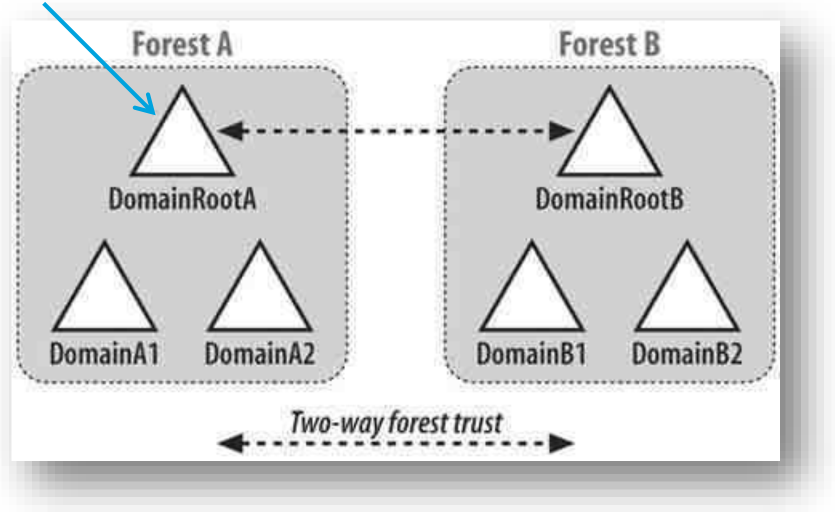
○ Always perform binary comparison

EAP-TLS uses the certificate to locate the right user and confirm uniqueness.

Authentication domains – default behavior

- By default ISE will discover all trusted domains from each join point
- Some of these could be child domains or domains in different forests
- If given an identity without domain markup, ISE will potentially search all of these
- **This default behavior is sub-optimal and can cause issues except in simple deployments**

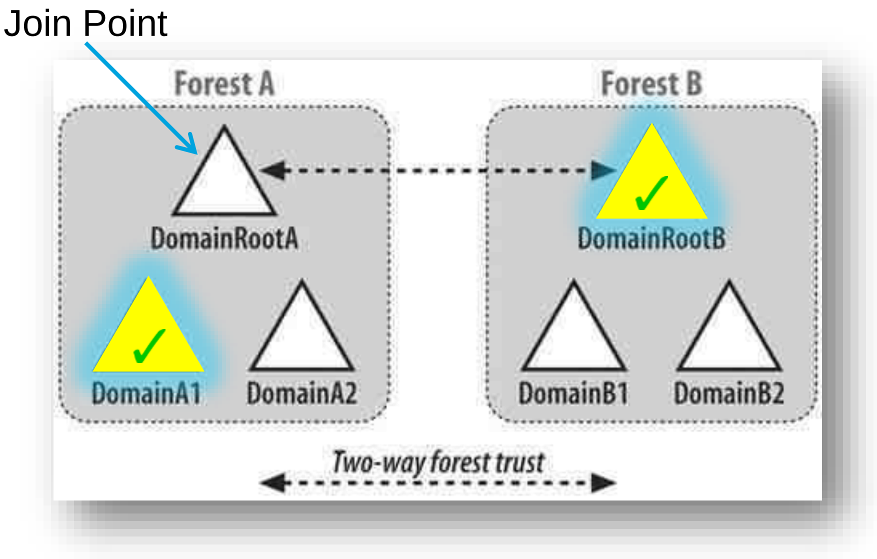
Join Point



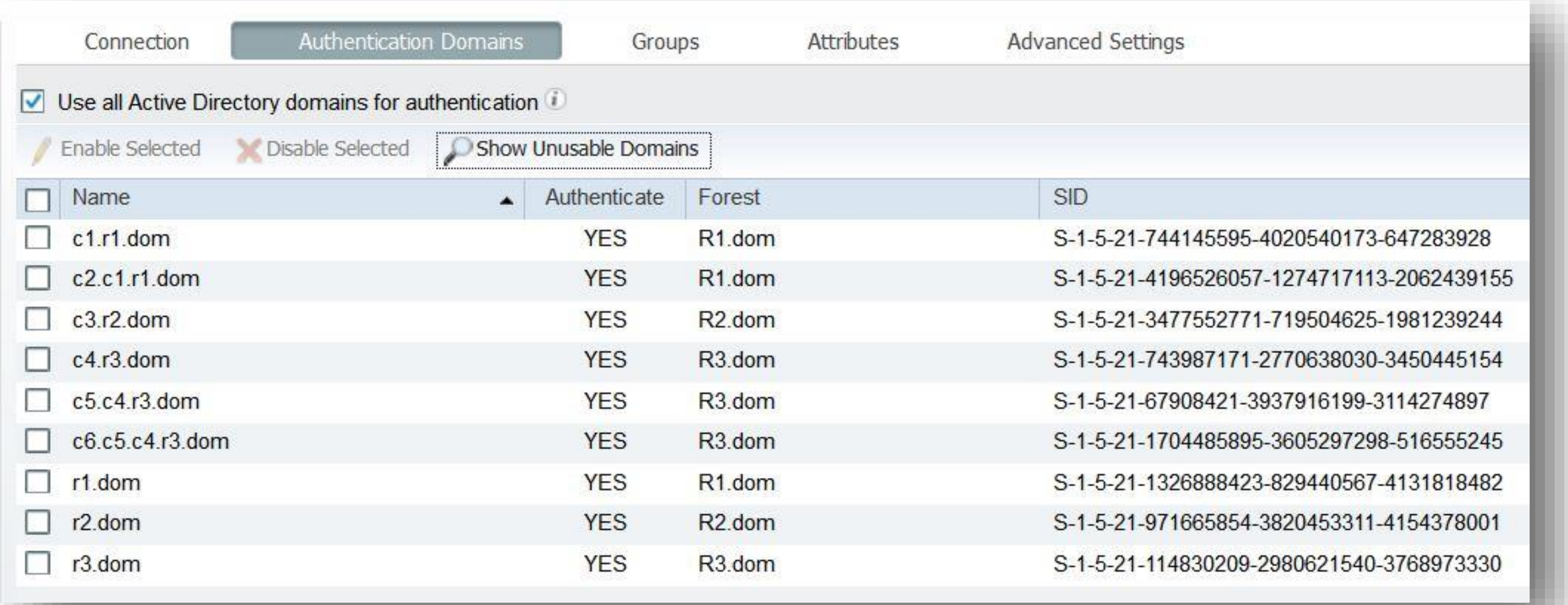
Authentication domains – how to optimize

We need to optimize this…

- Determine which domains you need
  - The ones with users and machine accounts you want ISE to authenticate
- We want to enable or ‘white list’ those
- And disable all others



Authentication domains – default interface

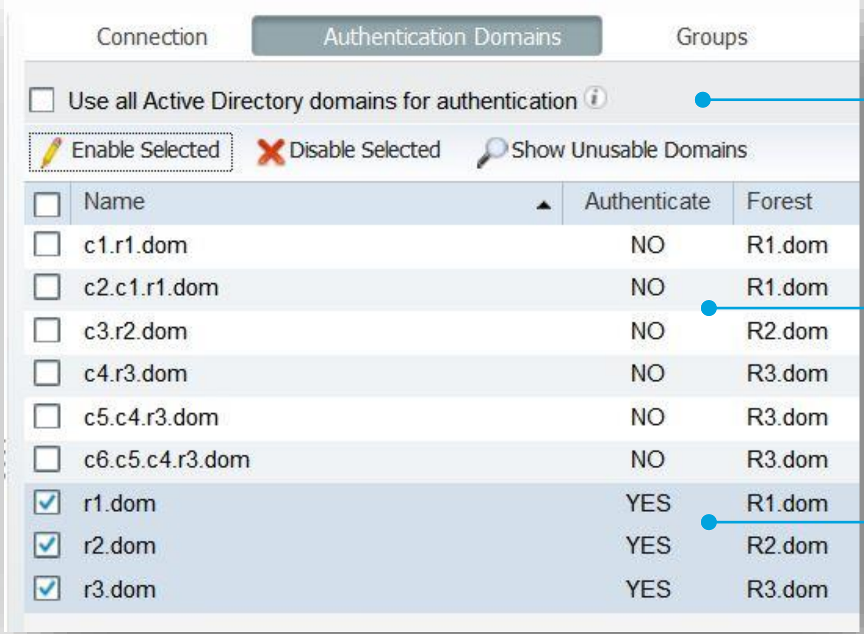


☑ Use all Active Directory domains for authentication

□	Name ▲	Authenticate	Forest	SID
□	c1.r1.dom	YES	R1.dom	S-1-5-21-744145595-4020540173-647283928
□	c2.c1.r1.dom	YES	R1.dom	S-1-5-21-4196526057-1274717113-2062439155
□	c3.r2.dom	YES	R2.dom	S-1-5-21-3477552771-719504625-1981239244
□	c4.r3.dom	YES	R3.dom	S-1-5-21-743987171-2770638030-3450445154
□	c5.c4.r3.dom	YES	R3.dom	S-1-5-21-67908421-3937916199-3114274897
□	c6.c5.c4.r3.dom	YES	R3.dom	S-1-5-21-1704485895-3605297298-516555245
□	r1.dom	YES	R1.dom	S-1-5-21-1326888423-829440567-4131818482
□	r2.dom	YES	R2.dom	S-1-5-21-971665854-3820453311-4154378001
□	r3.dom	YES	R3.dom	S-1-5-21-114830209-2980621540-3768973330

Authentication domains – white list your domains

Best Practice: do this for every join point



□ Use all Active Directory domains for authentication

□	Name	Authenticate	Forest
□	c1.r1.dom	NO	R1.dom
□	c2.c1.r1.dom	NO	R1.dom
□	c3.r2.dom	NO	R2.dom
□	c4.r3.dom	NO	R3.dom
□	c5.c4.r3.dom	NO	R3.dom
□	c6.c5.c4.r3.dom	NO	R3.dom
☑	r1.dom	YES	R1.dom
☑	r2.dom	YES	R2.dom
☑	r3.dom	YES	R3.dom

Clear check box

Let’s you specify which domains to use

Disable domains you don’t need

NO = don’t use these

Enable domains you need

YES = use these

Authentication domains - benefits

- ✓ Speeds up all operations that need to search for identities
- ✓ Reduces chance of ambiguous identities
- ✓ Reduces 'information leakage' and traffic to irrelevant domains
- ✓ Increases tolerance – you don't care if irrelevant domains are unavailable
  - In strict mode, any domain that is offline will cause authentication failure

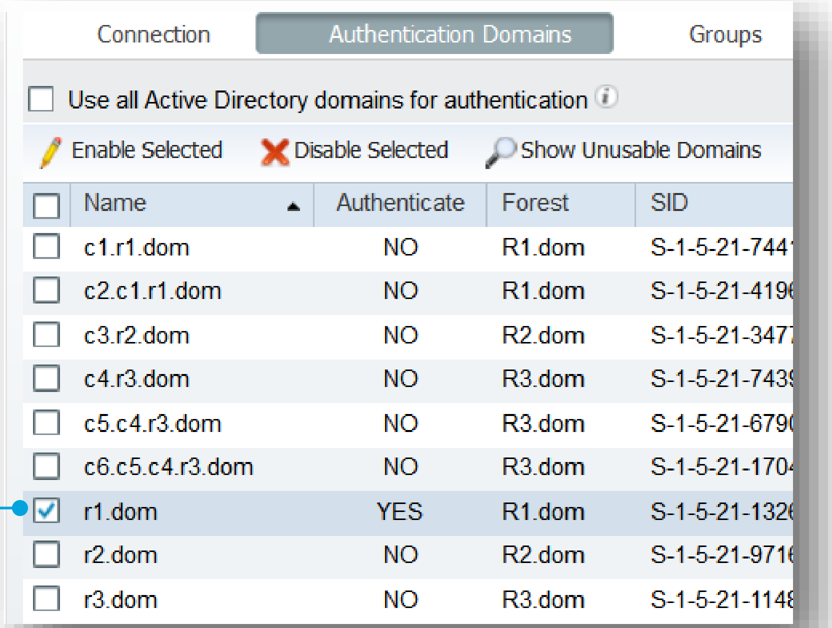
- The opposite is true
  - If you leave the default, you may have some or all of these issues
- Best Practices
  - Routinely configure Authentication Domains after you add a join point
  - Verify your identities work with the on-board Test User feature
  - Use minimum domains to maximize the benefits

Authentication domains - example

In this example, the join point can see many trusted domains but we only care about r1.dom

Enable r1.dom

And disable the rest



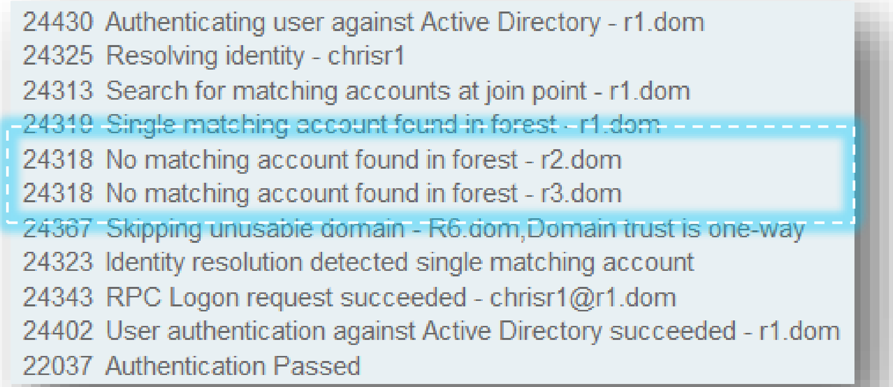
□ Use all Active Directory domains for authentication

□	Name	Authenticate	Forest	SID
□	c1.r1.dom	NO	R1.dom	S-1-5-21-744
□	c2.c1.r1.dom	NO	R1.dom	S-1-5-21-419
□	c3.r2.dom	NO	R2.dom	S-1-5-21-347
□	c4.r3.dom	NO	R3.dom	S-1-5-21-743
□	c5.c4.r3.dom	NO	R3.dom	S-1-5-21-679
□	c6.c5.c4.r3.dom	NO	R3.dom	S-1-5-21-170
☑	r1.dom	YES	R1.dom	S-1-5-21-132
□	r2.dom	NO	R2.dom	S-1-5-21-971
□	r3.dom	NO	R3.dom	S-1-5-21-114

Authentication domains – example benefit

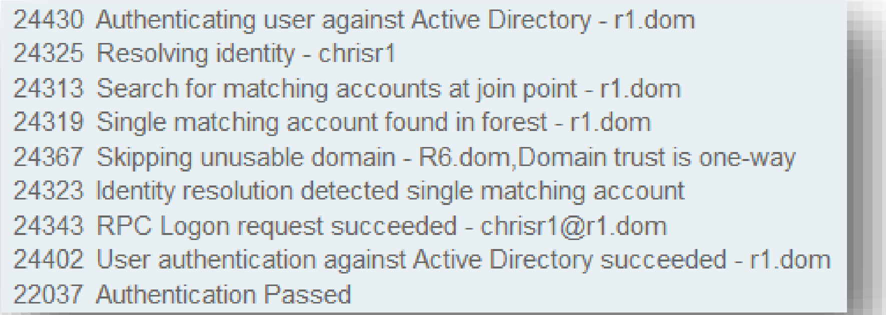
A search for a user without domain markup saved 2 forest searches:

Before



```
24430  Authenticating user against Active Directory - r1.dom
24325  Resolving identity - chrisr1
24313  Search for matching accounts at join point - r1.dom
24319  Single matching account found in forest - r1.dom
24318  No matching account found in forest - r2.dom
24318  No matching account found in forest - r3.dom
24367  Skipping unusable domain - R6.dom,Domain trust is one-way
24323  Identity resolution detected single matching account
24343  RPC Logon request succeeded - chrisr1@r1.dom
24402  User authentication against Active Directory succeeded - r1.dom
22037  Authentication Passed
```

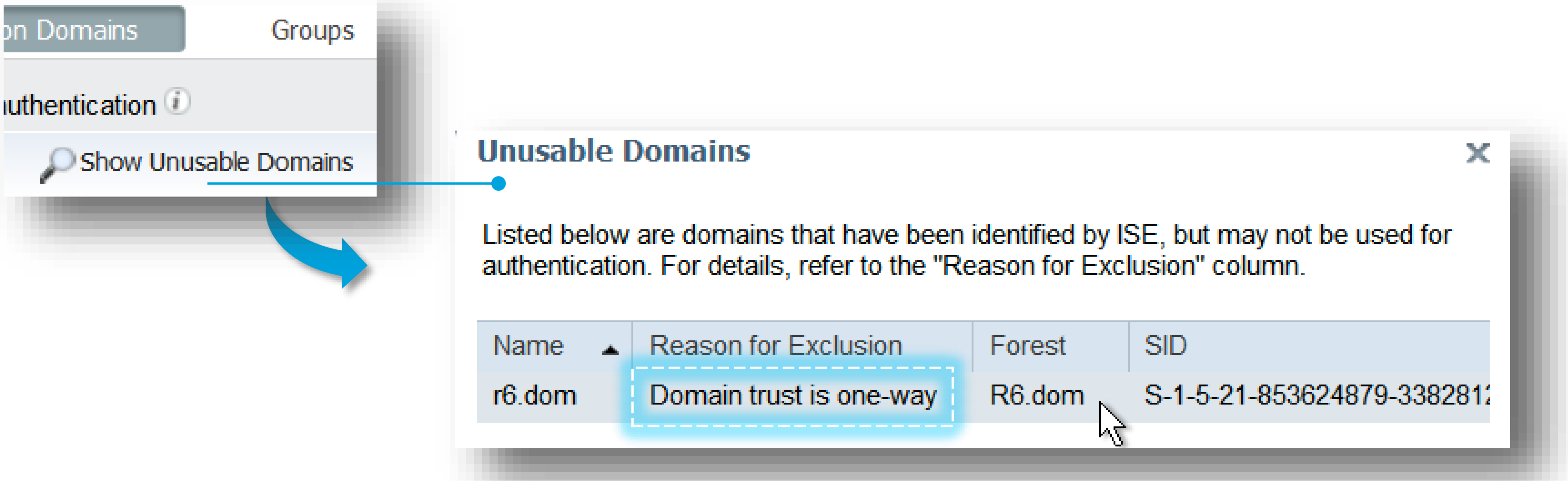
After



```
24430  Authenticating user against Active Directory - r1.dom
24325  Resolving identity - chrisr1
24313  Search for matching accounts at join point - r1.dom
24319  Single matching account found in forest - r1.dom
24367  Skipping unusable domain - R6.dom,Domain trust is one-way
24323  Identity resolution detected single matching account
24343  RPC Logon request succeeded - chrisr1@r1.dom
24402  User authentication against Active Directory succeeded - r1.dom
22037  Authentication Passed
```

Authentication domains – unusable domains

- Domains that are unusable, e.g. 1-way trusts, are hidden automatically
- There’s an option to reveal these and see the reason



Unusable Domains

Listed below are domains that have been identified by ISE, but may not be used for authentication. For details, refer to the "Reason for Exclusion" column.

Name	Reason for Exclusion	Forest	SID
r6.dom	Domain trust is one-way	R6.dom	S-1-5-21-853624879-338281

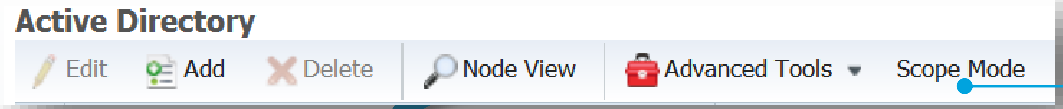
Scopes

- A scope is a set of join points
- They can be used in authentication policy and identity sequences
  - They are a configuration shortcut
  - They focus the search scope
  - They are efficient to evaluate
- There is already a pseudo-scope called “All_AD_Instances”

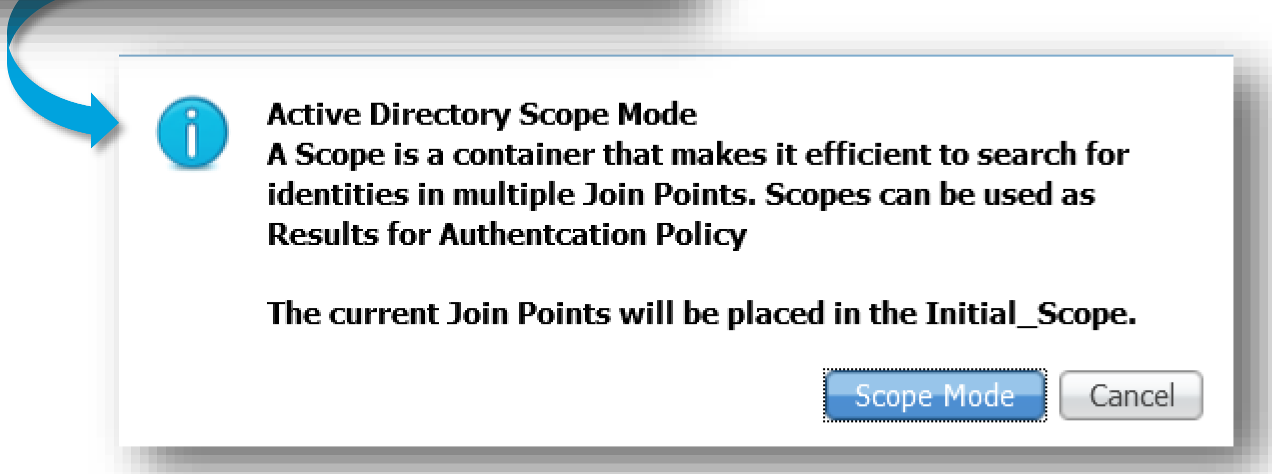
- When should you use them?
  - When you have multiple untrusted AD forests but you want to treat them as one entity

Enabling scopes

By default, scopes are not enabled, there is a button to enable it



Click here



Active Directory Scope Mode
A Scope is a container that makes it efficient to search for identities in multiple Join Points. Scopes can be used as Results for Authentcation Policy

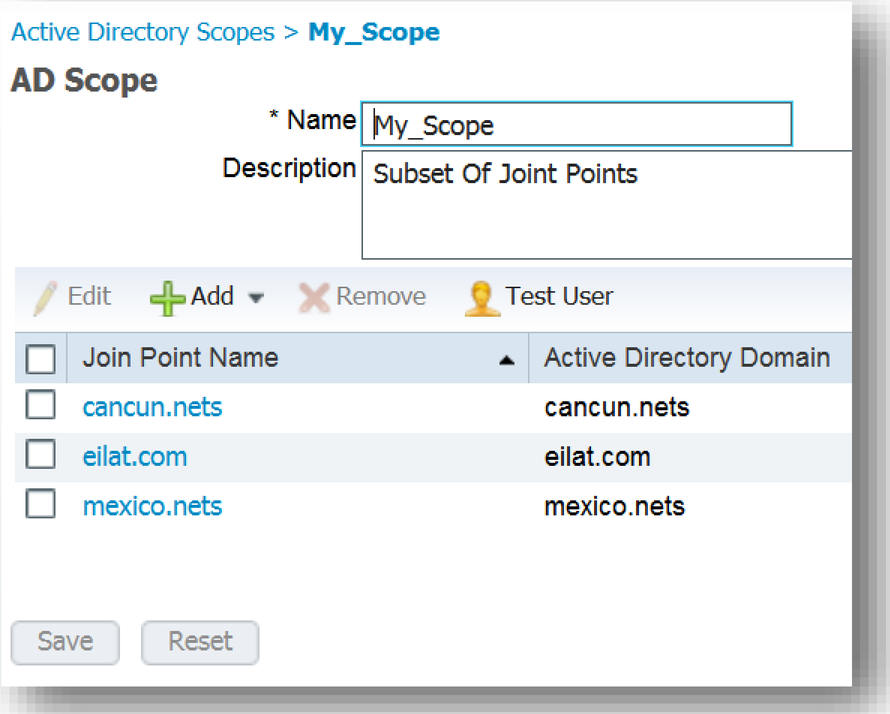
The current Join Points will be placed in the Initial_Scope.

A new scope will be created called “Initial_Scope” with your existing join points

Cisco live!

Creating a new scope

- You can then create new scopes
- Assign join points into it
- And use them in
  - Authentication Policy
  - Identity Sequences



Active Directory Scopes > **My_Scope**

AD Scope

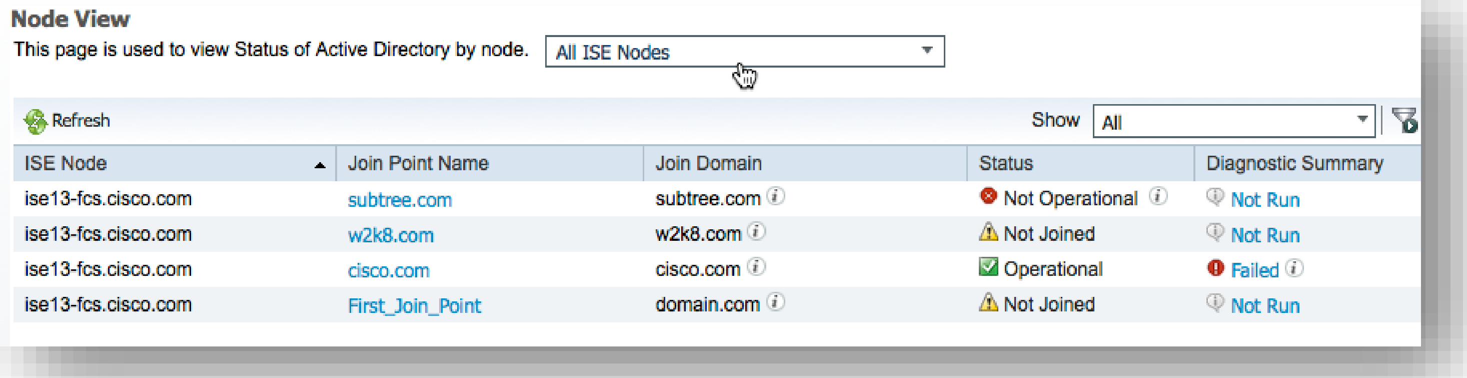
* Name: My_Scope

Description: Subset Of Joint Points

□	Join Point Name	Active Directory Domain
□	cancun.nets	cancun.nets
□	eilat.com	eilat.com
□	mexico.nets	mexico.nets

Quick word about Node View

- Shows all join points and their status on one page
- Useful for navigation, especially in Scope mode



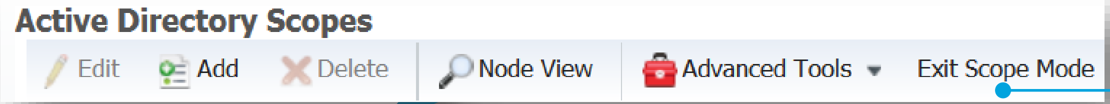
Node View

This page is used to view Status of Active Directory by node. All ISE Nodes

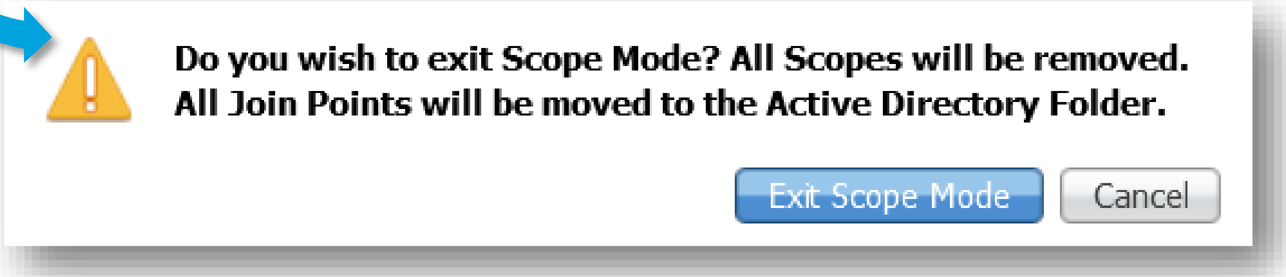
ISE Node	Join Point Name	Join Domain	Status	Diagnostic Summary
ise13-fcs.cisco.com	subtree.com	subtree.com	Not Operational	Not Run
ise13-fcs.cisco.com	w2k8.com	w2k8.com	Not Joined	Not Run
ise13-fcs.cisco.com	cisco.com	cisco.com	Operational	Failed
ise13-fcs.cisco.com	First_Join_Point	domain.com	Not Joined	Not Run

Leaving scope mode

If you prefer non-scope mode, you can go back



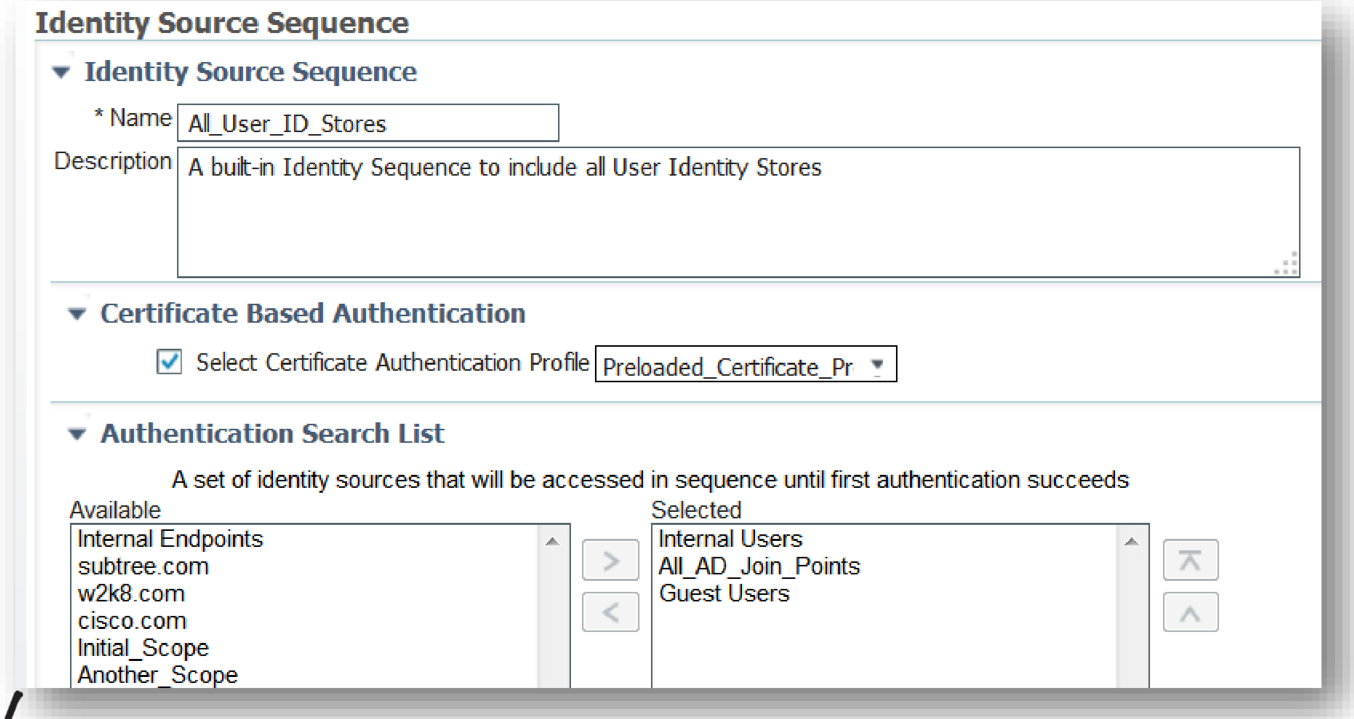
Click here



Do you wish to exit Scope Mode? All Scopes will be removed. All Join Points will be moved to the Active Directory Folder.

Identity source sequences

Now supports All_AD_Join_Points, join points and scopes



Identity Source Sequence

▼ Identity Source Sequence

* Name: All_User_ID_Stores

Description: A built-in Identity Sequence to include all User Identity Stores

▼ Certificate Based Authentication

☑ Select Certificate Authentication Profile: Preloaded_Certificate_Pr

▼ Authentication Search List

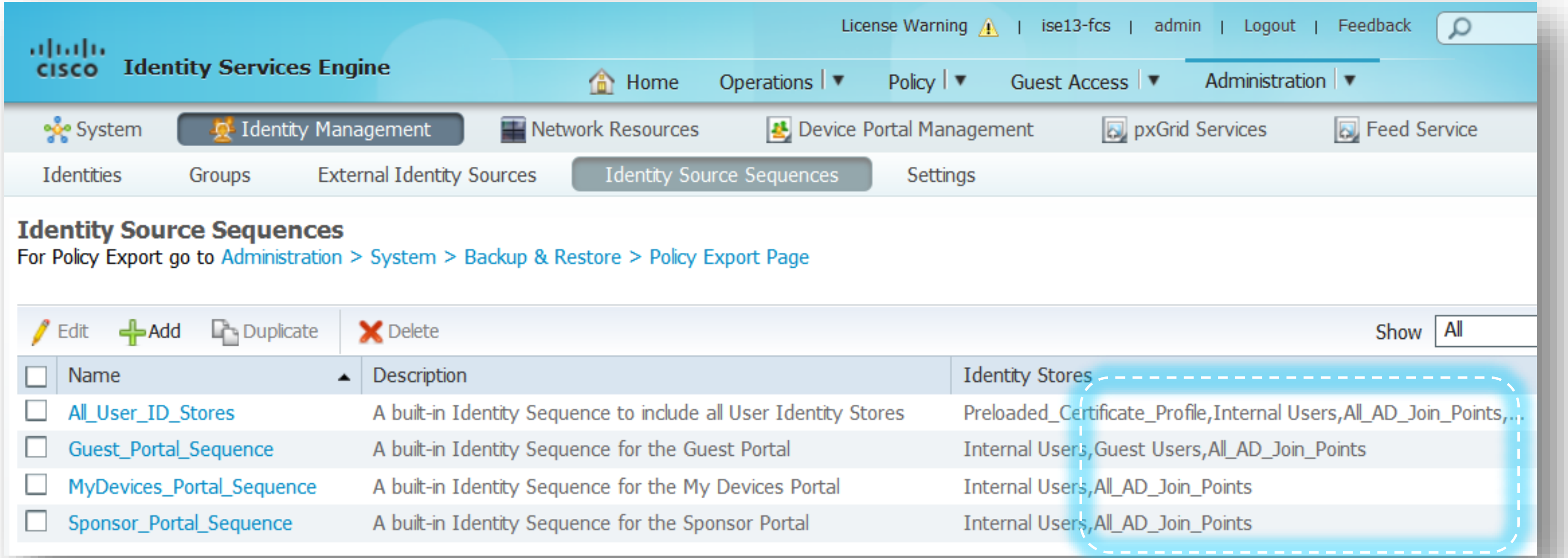
A set of identity sources that will be accessed in sequence until first authentication succeeds

Available:
Internal Endpoints
subtree.com
w2k8.com
cisco.com
Initial_Scope
Another_Scope

Selected:
Internal Users
All_AD_Join_Points
Guest Users

All_AD_Join_Points

Psuedo-scope meaning all join points available out-of-the-box



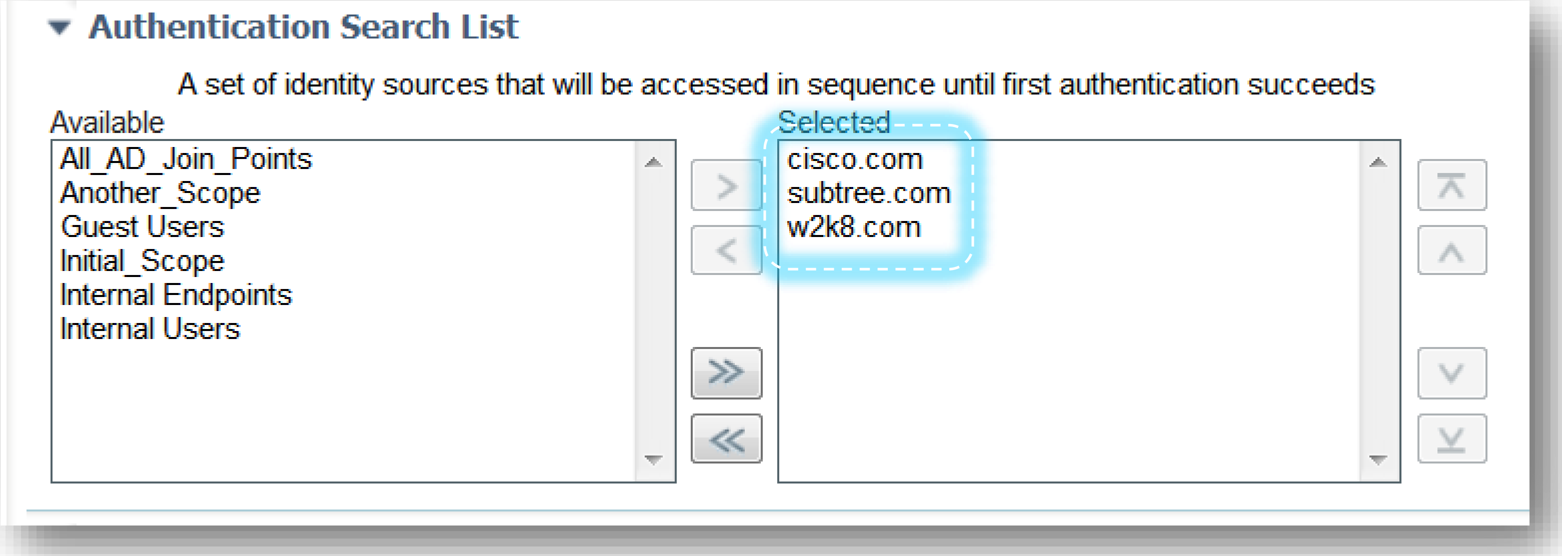
Identity Source Sequences

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

□	Name ▲	Description	Identity Stores
□	All_User_ID_Stores	A built-in Identity Sequence to include all User Identity Stores	Preloaded_Certificate_Profile,Internal Users,All_AD_Join_Points,...
□	Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users,Guest Users,All_AD_Join_Points
□	MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Portal	Internal Users,All_AD_Join_Points
□	Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users,All_AD_Join_Points

Don’t add multiple join points to sequences

It causes multiple searches



Authentication Search List

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

Available

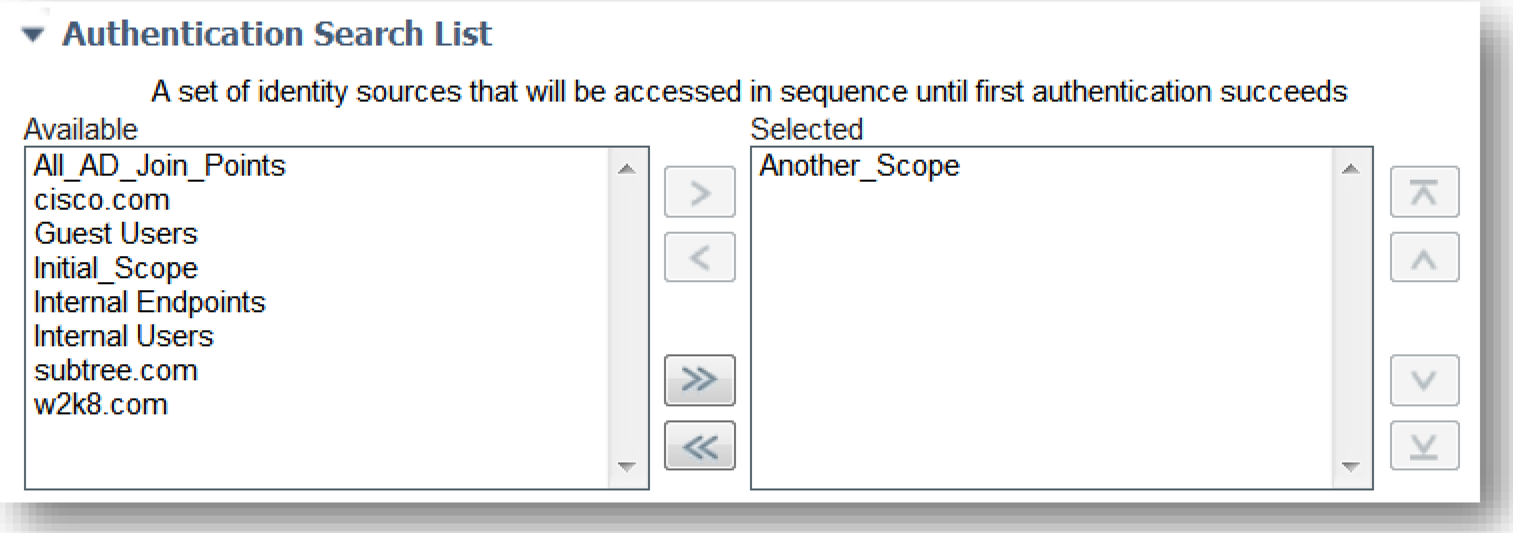
- All_AD_Join_Points
- Another_Scope
- Guest Users
- Initial_Scope
- Internal Endpoints
- Internal Users

Selected

- cisco.com
- subtree.com
- w2k8.com

Use a new scope instead = more efficient

This will do an optimized search



Authentication Search List

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

Available

- All_AD_Join_Points
- cisco.com
- Guest Users
- Initial_Scope
- Internal Endpoints
- Internal Users
- subtree.com
- w2k8.com

Selected

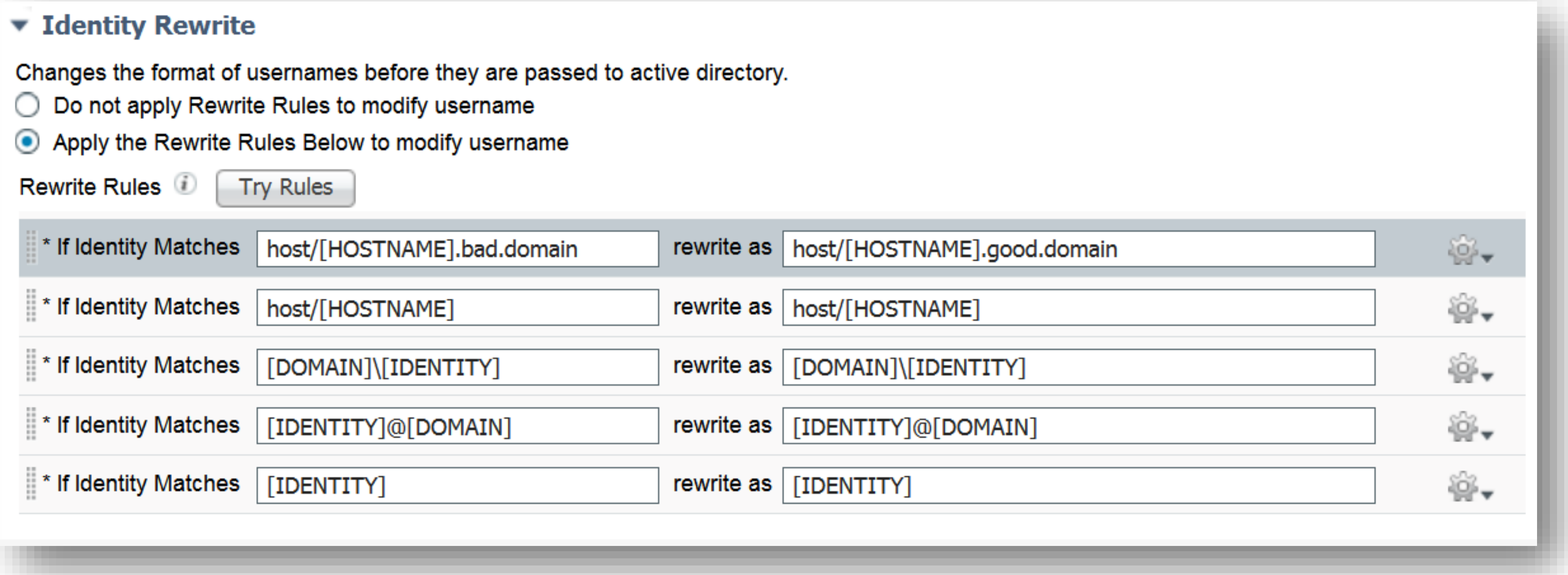
- Another_Scope

Identity rewrite

- Each join point can define some rules to rewrite an identity
- Even any identity from any of the certificate fields
- Uses
  - Fix bad certificate identities
  - Add domains to usernames
  - Strip prefixes or suffixes
- It is located in the join point’s Advanced Settings

Identity rewrite rules

A default set of rules is supplied which matches common identity formats



▾ **Identity Rewrite**

Changes the format of usernames before they are passed to active directory.

○ Do not apply Rewrite Rules to modify username

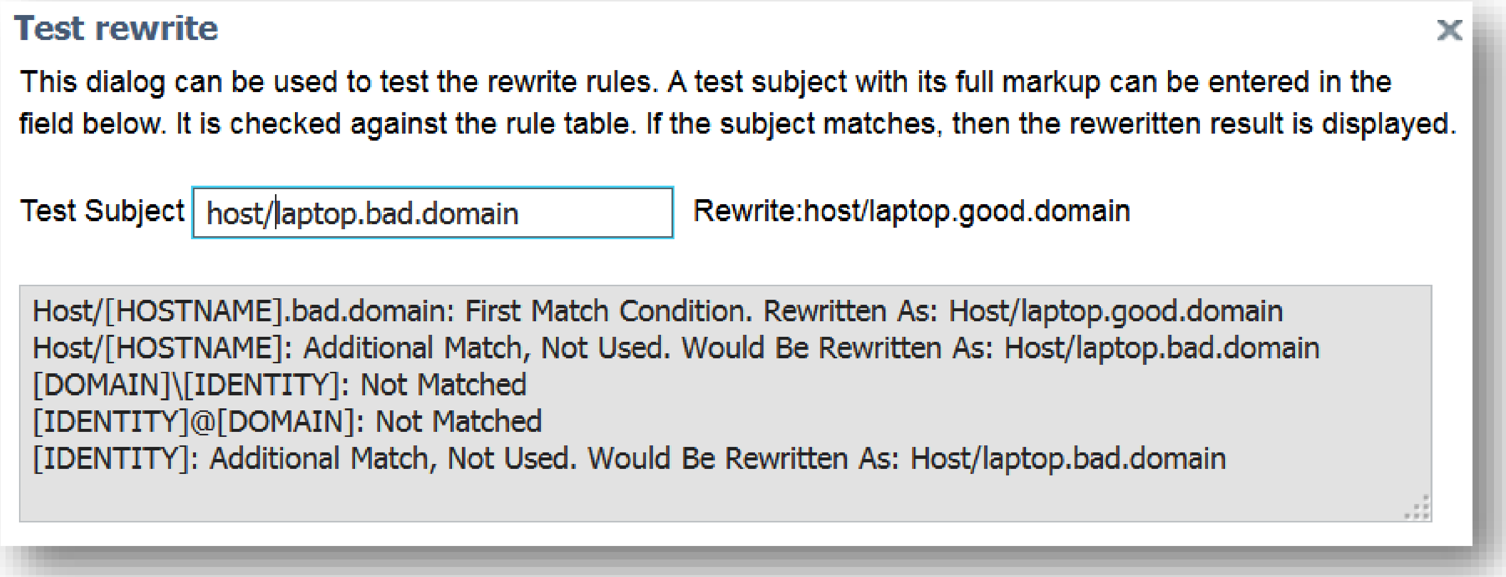
● Apply the Rewrite Rules Below to modify username

Rewrite Rules

* If Identity Matches	host/[HOSTNAME].bad.domain	rewrite as	host/[HOSTNAME].good.domain
* If Identity Matches	host/[HOSTNAME]	rewrite as	host/[HOSTNAME]
* If Identity Matches	[DOMAIN]\[IDENTITY]	rewrite as	[DOMAIN]\[IDENTITY]
* If Identity Matches	[IDENTITY]@[DOMAIN]	rewrite as	[IDENTITY]@[DOMAIN]
* If Identity Matches	[IDENTITY]	rewrite as	[IDENTITY]

Testing identity rewrite rules

The Try Rules button allows you to test your rules with different input



This dialog can be used to test the rewrite rules. A test subject with its full markup can be entered in the field below. It is checked against the rule table. If the subject matches, then the reweritten result is displayed.

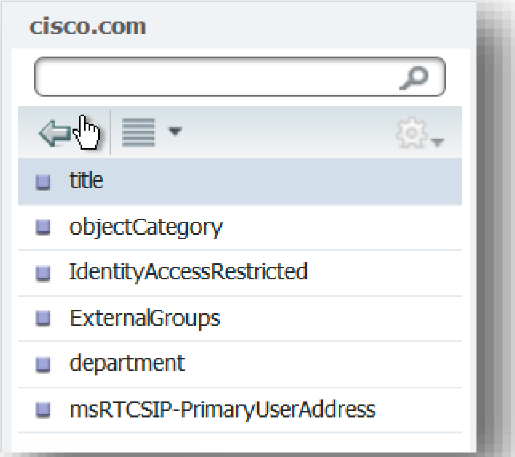
Test Subject: host/laptop.bad.domain

Rewrite:host/laptop.good.domain

```
Host/[HOSTNAME].bad.domain: First Match Condition. Rewritten As: Host/laptop.good.domain
Host/[HOSTNAME]: Additional Match, Not Used. Would Be Rewritten As: Host/laptop.bad.domain
[DOMAIN]\[IDENTITY]: Not Matched
[IDENTITY]@[DOMAIN]: Not Matched
[IDENTITY]: Additional Match, Not Used. Would Be Rewritten As: Host/laptop.bad.domain
```

Attributes

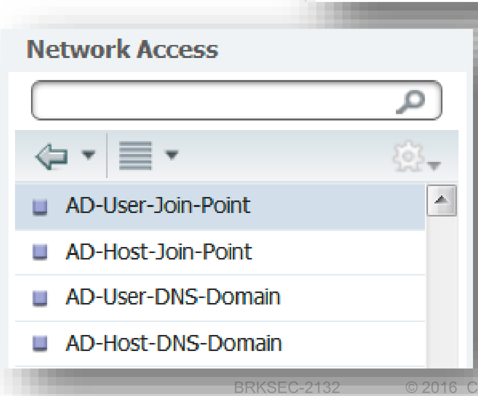
- Similar to before except attributes are selected from a join point dictionary (instead of "AD1")



cisco.com

- title
- objectCategory
- IdentityAccessRestricted
- ExternalGroups
- department
- msRTCSIP-PrimaryUserAddress

- The Network Access dictionary provides some new AD related attributes useful in policy rules



Network Access

- AD-User-Join-Point
- AD-Host-Join-Point
- AD-User-DNS-Domain
- AD-Host-DNS-Domain

Group evaluation uses SIDs now

SIDs = Security Identifiers

Prior to 1.3

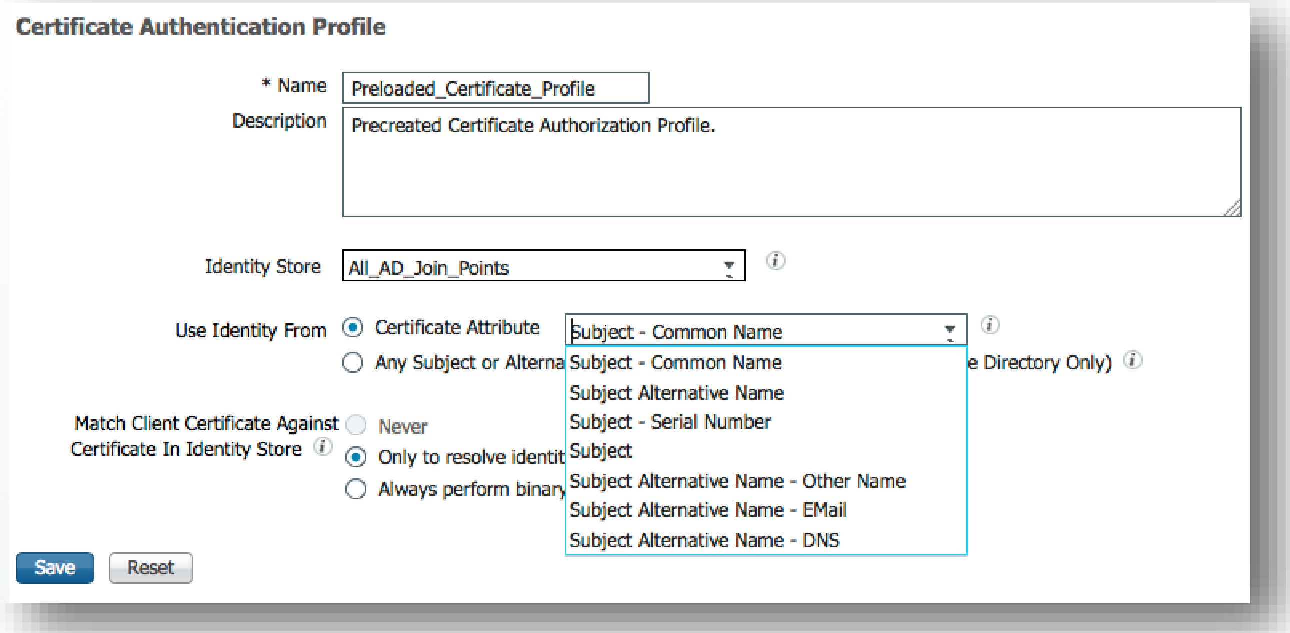
- Groups were resolved to text for evaluation
- What if no DC was available or SID was stale?
- Caused serious delays even if group wasn’t used in policy conditions

ISE 1.3

- Runtime evaluates groups using binary SIDs
  - This avoids the need to resolve them to text
  - ISE policy rules don’t break if groups are renamed in AD
  - Helps deal with ambiguity

Certificate Authentication Profile

Out-of-the-box profile, useful for deploying EAP-TLS



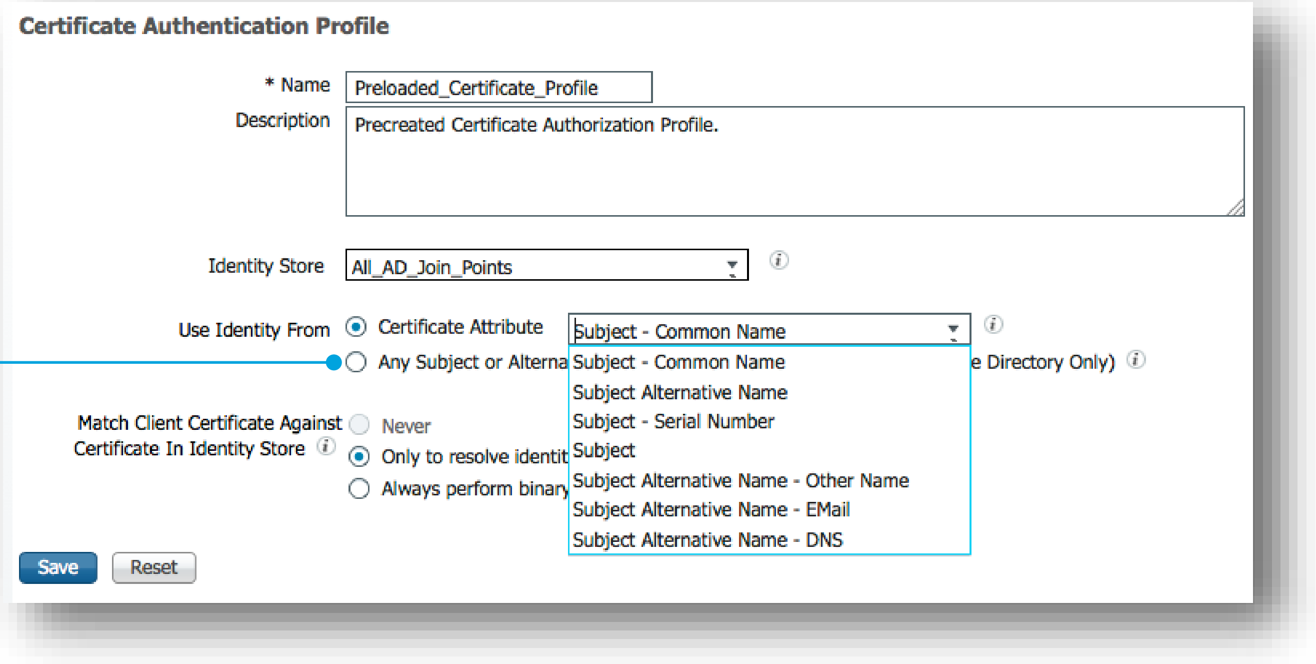
Certificate Authentication Profile

* Name	Preloaded_Certificate_Profile
Description	Precreated Certificate Authorization Profile.
Identity Store	All_AD_Join_Points
Use Identity From	● Certificate Attribute: Subject - Common Name ○ Any Subject or Alterna… e Directory Only)
Match Client Certificate Against Certificate In Identity Store	○ Never ● Only to resolve identit… ○ Always perform binary…

Subject - Common Name
Subject Alternative Name
Subject - Serial Number
Subject
Subject Alternative Name - Other Name
Subject Alternative Name - EMail
Subject Alternative Name - DNS
Save
Reset

Certificate Authentication Profile – smart search

When you upgrade, smart search is not enabled by default



Certificate Authentication Profile

* Name: Preloaded_Certificate_Profile

Description: Precreated Certificate Authorization Profile.

Identity Store: All_AD_Join_Points

Use Identity From:
- ● Certificate Attribute: Subject - Common Name
- ○ Any Subject or Alterna… e Directory Only)

Subject - Common Name
Subject Alternative Name
Subject - Serial Number
Subject
Subject Alternative Name - Other Name
Subject Alternative Name - EMail
Subject Alternative Name - DNS

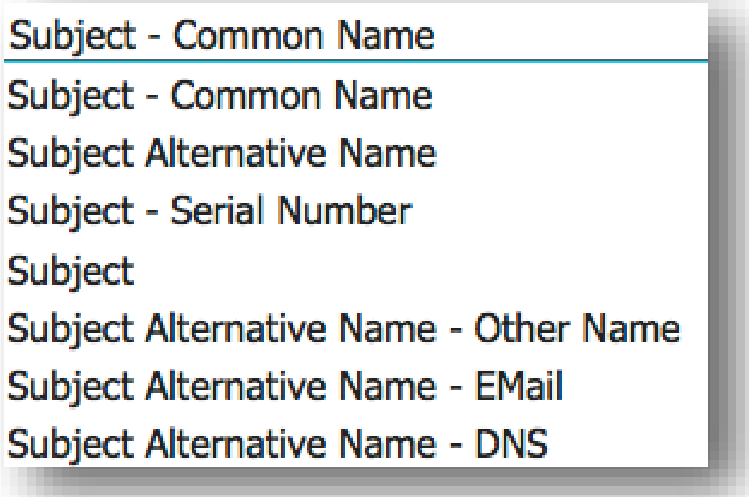
Match Client Certificate Against Certificate In Identity Store:
- ○ Never
- ● Only to resolve identit…
- ○ Always perform binary…

Smart search

Use this 2nd option

What is smart search?

- Legacy mode only uses one attribute from the certificate
- Smart search inspects all certificate attributes for potential identities
- All candidates are passed to the AD identity store
- Rewrite may be performed
- The AD connector will construct one search filter to search for the object



Subject - Common Name

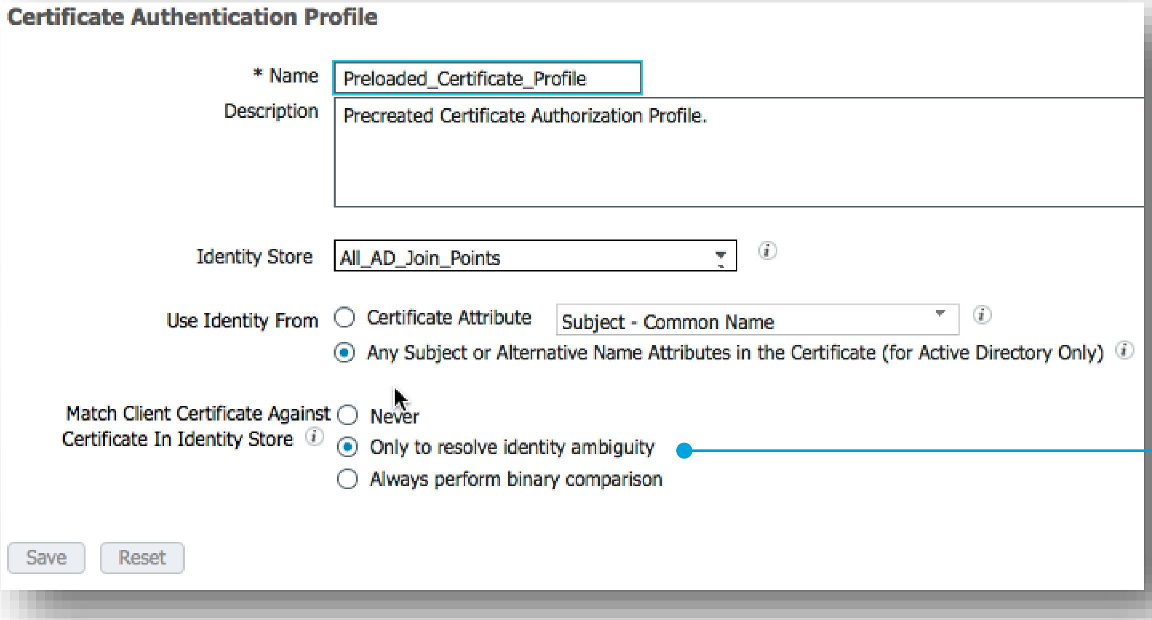
Subject - Common Name
Subject Alternative Name
Subject - Serial Number
Subject
Subject Alternative Name - Other Name
Subject Alternative Name - EMail
Subject Alternative Name - DNS

Why do I need smart search?

- In 1.2, it was not possible to have more than one CAP
  - Certs with identities in different fields could not be used
  - This could be costly to rectify
- Smart search allows you to mix certs and ‘not care’ which attribute they use

- Combined with rewrite, it allows you to actually use mis-generated certs
  - Example: customer with 30,000 Verisign certs with email address instead of UPN
- Why not multi-CAPs?
  - Less efficient processing – requires multiple AD searches

Certificate Authentication Profile - ambiguity



Certificate Authentication Profile

* Name	Preloaded_Certificate_Profile
Description	Precreated Certificate Authorization Profile.
Identity Store	All_AD_Join_Points
Use Identity From	○ Certificate Attribute — Subject - Common Name ● Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)
Match Client Certificate Against Certificate In Identity Store	○ Never ● Only to resolve identity ambiguity ○ Always perform binary comparison

Smart resolve

Uses AD certs to resolve any ambiguity

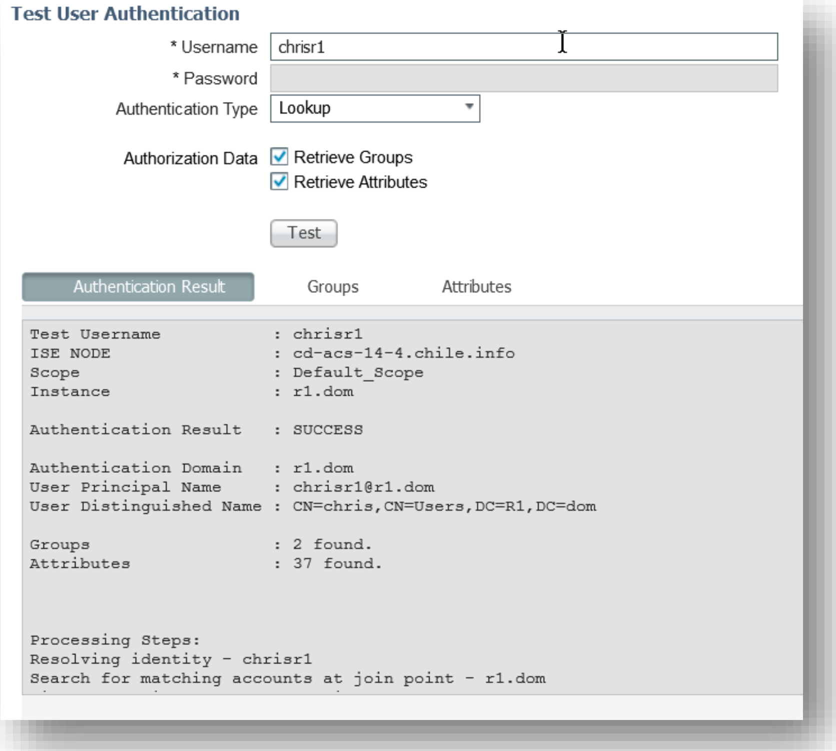
EAP-TLS and AD

- Want to lock out an EAP-TLS user without revoking their certificate?
  - ISE does some additional checks to make this easy for you
  - If their AD account is disabled or locked-out, the authentication fails
  - ✓ This gives you a quick way to disable them from AD

- Which identity to log when using smart search?
  - The **implicit** UPN will be used, i.e. sam@user-account-domain.com
  - Don’t be concerned if this does not match the certificate identity

Test user authentication

- **Very** useful!
- Test authentications from GUI
  - Choice of protocol
  - Can fetch attributes and/or groups
  - Detailed result
- Can be launched on
  - All join points, specific join point, or on specific ISE node



Test User Authentication

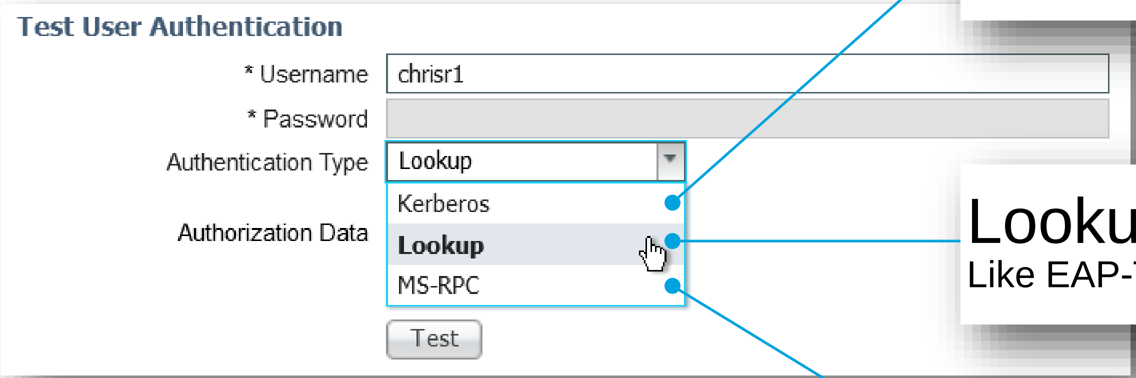
* Username	chrisr1
* Password	
Authentication Type	Lookup
Authorization Data	☑ Retrieve Groups ☑ Retrieve Attributes

```
Test Username            : chrisr1
ISE NODE                 : cd-acs-14-4.chile.info
Scope                    : Default_Scope
Instance                 : r1.dom

Authentication Result    : SUCCESS

Authentication Domain    : r1.dom
User Principal Name      : chrisr1@r1.dom
User Distinguished Name  : CN=chris,CN=Users,DC=R1,DC=dom

Groups                   : 2 found.
Attributes               : 37 found.



Processing Steps:
Resolving identity - chrisr1
Search for matching accounts at join point - r1.dom
```

Test user authentication

- Can take various identity formats
  - Users: chris, DOMAIN\chris, chris@domain.com
  - Machines: laptop$, DOMAIN\laptop$, host/laptop.domain.com
  - Even distinguished names: CN=chris,CN=Users,DC=R1,DC=dom
- Check authentications – environment OK?
- Check AD connector configuration – efficient?
- Check authorization policy working as expected
- Verify groups, attributes
- Troubleshoot different users / protocols

Test user authentication – protocol choice



Test User Authentication

* Username	chrisr1
* Password	
Authentication Type	Lookup
Authorization Data	

Kerberos
Forces Kerberos protocol

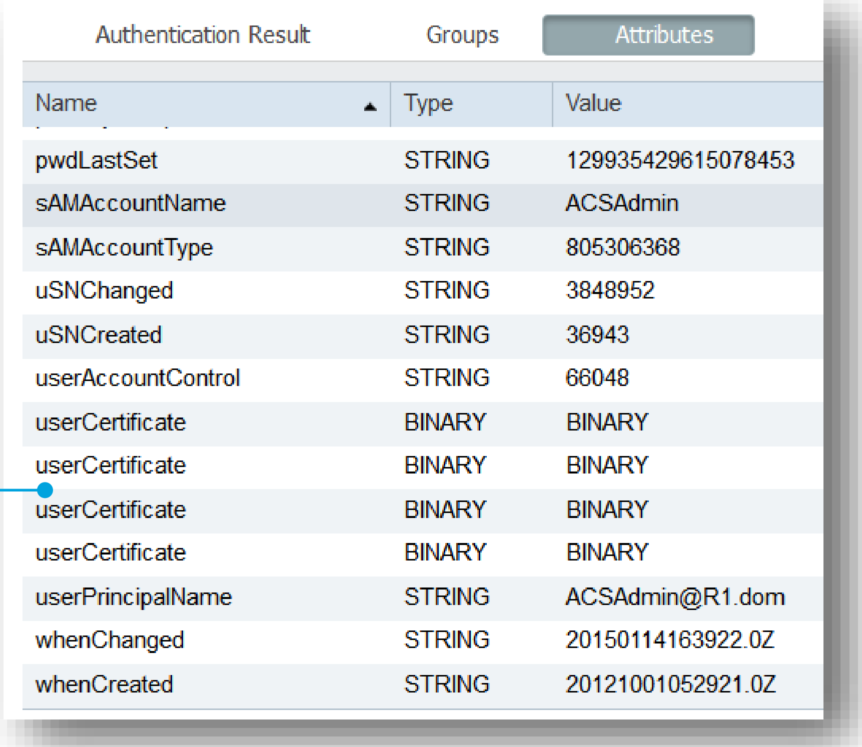
Lookup
Like EAP-TLS, no password

MS-RPC
Normal protocol ISE uses for password based authentication

Test user authentication – attributes

- Browse attributes a user has
- Check what can be used in policy

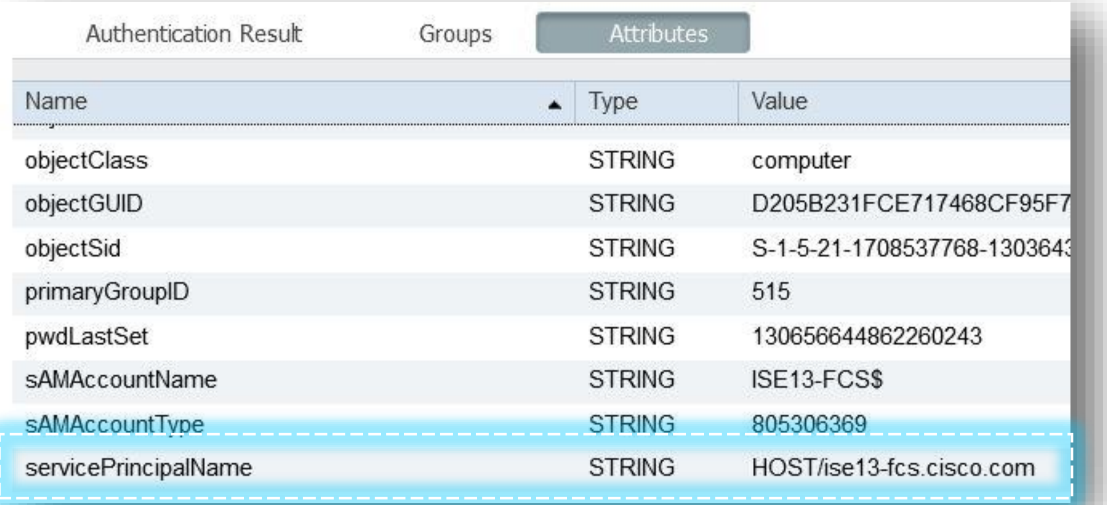
- Multi-valued attributes will appear multiple times
  - Note the userCertificate attribute
  - Usually suggest expired certificates



Name	Type	Value
pwdLastSet	STRING	129935429615078453
sAMAccountName	STRING	ACSAdmin
sAMAccountType	STRING	805306368
uSNChanged	STRING	3848952
uSNCreated	STRING	36943
userAccountControl	STRING	66048
userCertificate	BINARY	BINARY
userCertificate	BINARY	BINARY
userCertificate	BINARY	BINARY
userCertificate	BINARY	BINARY
userPrincipalName	STRING	ACSAdmin@R1.dom
whenChanged	STRING	20150114163922.0Z
whenCreated	STRING	20121001052921.0Z

Test user authentication – verify machine SPN

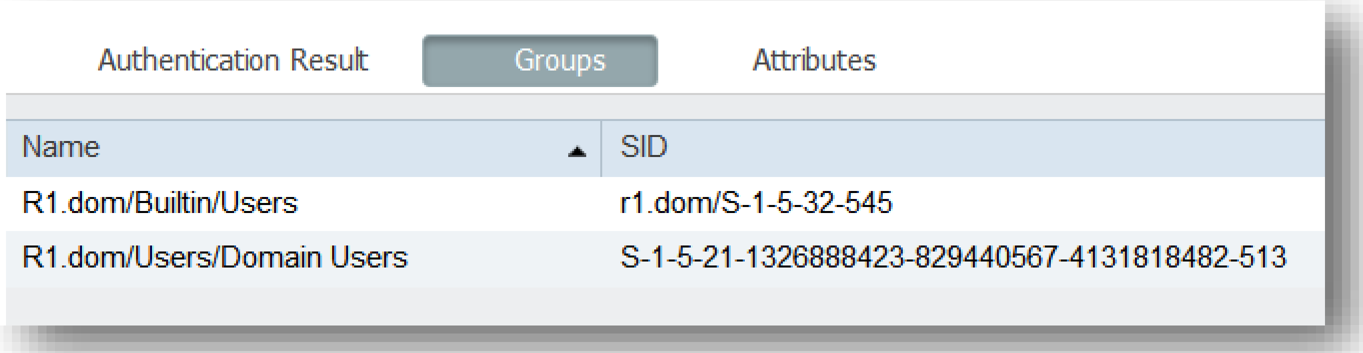
- If a machine is failing with “No such user” use Test Authentication (Lookup) and verify it has servicePrincipalName attribute – if not, one needs created



Name	Type	Value
objectClass	STRING	computer
objectGUID	STRING	D205B231FCE717468CF95F7
objectSid	STRING	S-1-5-21-1708537768-130364
primaryGroupID	STRING	515
pwdLastSet	STRING	130656644862260243
sAMAccountName	STRING	ISE13-FCS$
sAMAccountType	STRING	805306369
servicePrincipalName	STRING	HOST/ise13-fcs.cisco.com

Test user authentication - groups

- Browse a user’s group membership

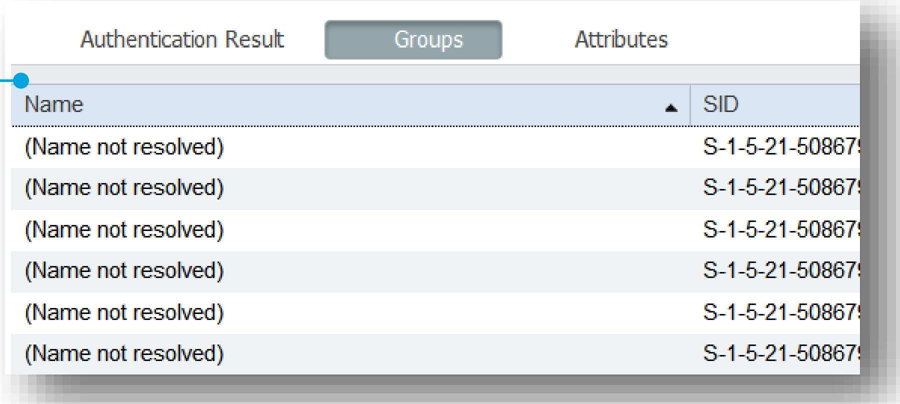


Name	SID
R1.dom/Builtin/Users	r1.dom/S-1-5-32-545
R1.dom/Users/Domain Users	S-1-5-21-1326888423-829440567-4131818482-513

- The SID helps confirm the real group in AD
  - Use the Refresh SIDs option if these appear out of date
  - BuiltIn groups are prefixed with domain name to make them unique in policy conditions

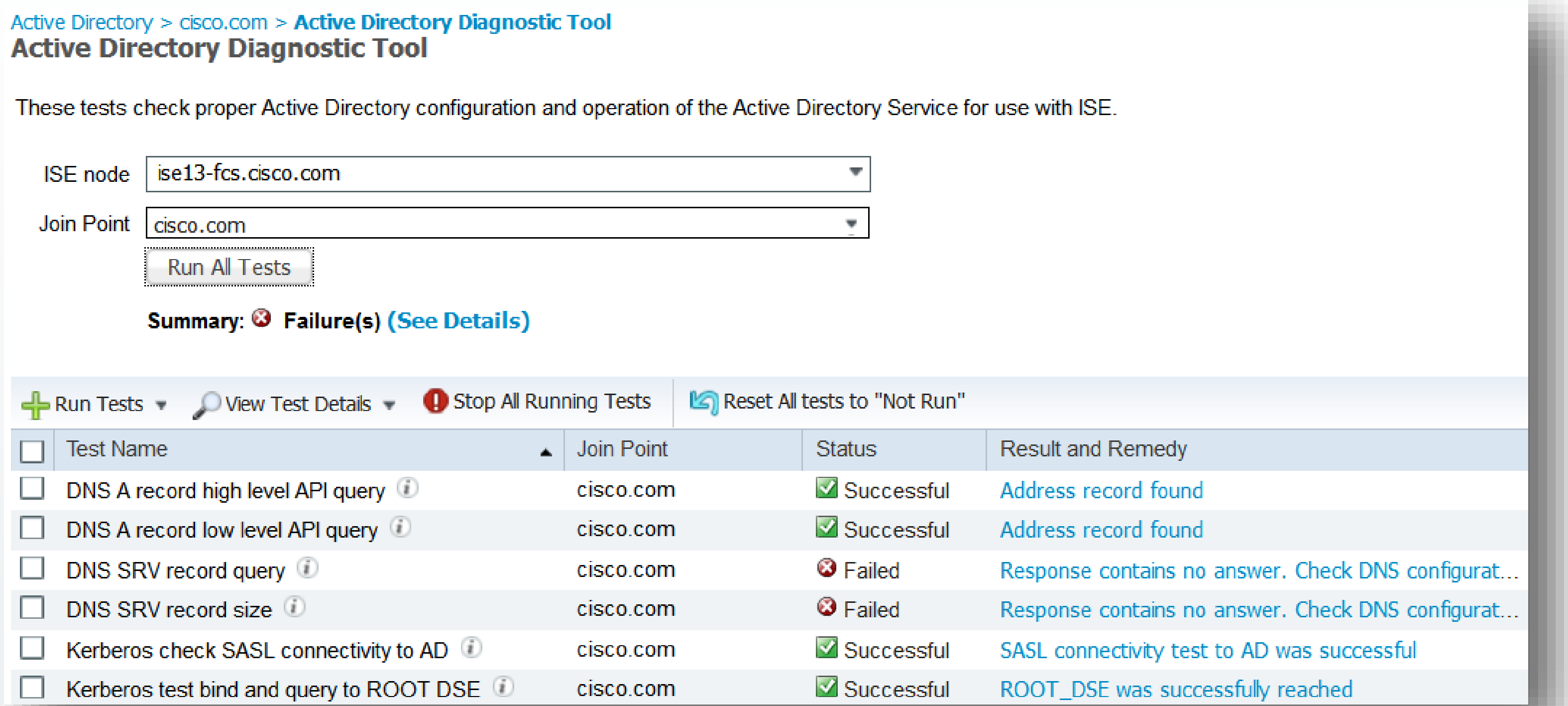
Test user authentication – stale groups

- If you see “(Name not resolved)”, user’s have “stale” groups
- Typically, from a domain that no longer exists
- In 1.2, these could cause significant delays fetching groups
- In 1.3, they do not but it is still good practice to clean these from AD
  - If you see them, mention it to your AD admin



Name	SID
(Name not resolved)	S-1-5-21-50867
(Name not resolved)	S-1-5-21-50867
(Name not resolved)	S-1-5-21-50867
(Name not resolved)	S-1-5-21-50867
(Name not resolved)	S-1-5-21-50867
(Name not resolved)	S-1-5-21-50867

Diagnostic Tool - interface



Active Directory > cisco.com > **Active Directory Diagnostic Tool**

Active Directory Diagnostic Tool

These tests check proper Active Directory configuration and operation of the Active Directory Service for use with ISE.

ISE node: ise13-fcs.cisco.com

Join Point: cisco.com

Summary: ☒ **Failure(s)** **(See Details)**

□	Test Name	Join Point	Status	Result and Remedy
□	DNS A record high level API query	cisco.com	☑ Successful	Address record found
□	DNS A record low level API query	cisco.com	☑ Successful	Address record found
□	DNS SRV record query	cisco.com	☒ Failed	Response contains no answer. Check DNS configurat...
□	DNS SRV record size	cisco.com	☒ Failed	Response contains no answer. Check DNS configurat...
□	Kerberos check SASL connectivity to AD	cisco.com	☑ Successful	SASL connectivity test to AD was successful
□	Kerberos test bind and query to ROOT DSE	cisco.com	☑ Successful	ROOT_DSE was successfully reached

Diagnostic Tool

- Best practice to run this after adding a new join point
- Also when you have an issue and suspect something environmental
- Detailed report on test results
- Runs in background – no need to wait

- Extensive environment tests including
  - AD, DNS, LDAP, NTP, Kerberos…
  - Warns if things slow
  - Warns if low availability
  - Warns if not in AD Site
  - Warns if DNS replies too big

Advanced Tuning

- Allows tweaks in the field via GUI
  - Usually under guidance by TAC
- Maintains a history of tweaks
- Has ‘reset parameter to default’
- Can restart AD connector
- **Very important for**
  - Disable AD encryption temporarily
  - Forcing specific DCs or GCs

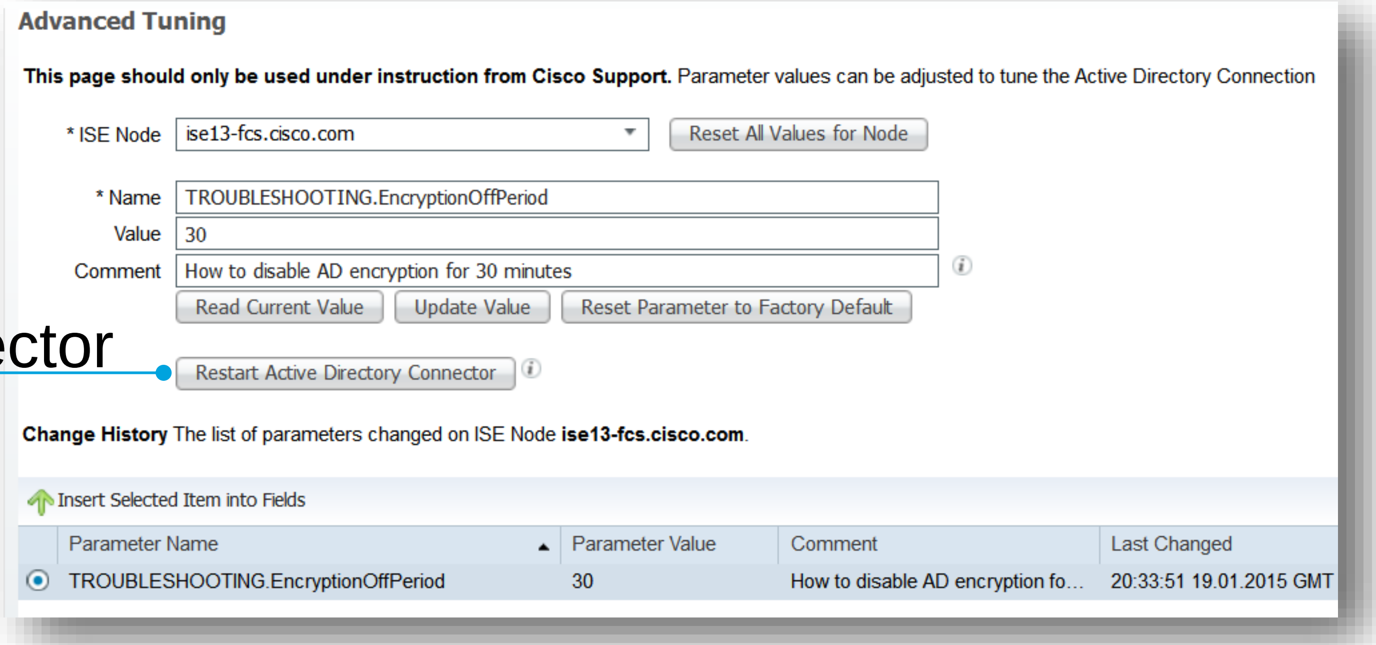
- During normal operation LDAP and MS-RPC traffic is encrypted
- When diagnosing an issue, it can be useful to disable this encryption prior to taking a packet capture
- Sniffer traces can then be decoded better which may help determine root cause

https://techzone.cisco.com/t5/Identity-Services-Engine-ISE/ISE-1-3-Active-Directory-Advanced-Tuning/ta-p/831737

Advanced Tuning - interface

Restarts connector

Can be used on its own



Advanced Tuning

This page should only be used under instruction from Cisco Support. Parameter values can be adjusted to tune the Active Directory Connection

* ISE Node: ise13-fcs.cisco.com

Reset All Values for Node

* Name: TROUBLESHOOTING.EncryptionOffPeriod

Value: 30

Comment: How to disable AD encryption for 30 minutes

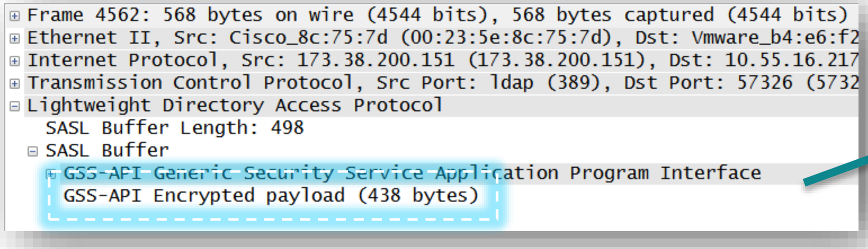
Read Current Value
Update Value
Reset Parameter to Factory Default
Restart Active Directory Connector

Change History The list of parameters changed on ISE Node **ise13-fcs.cisco.com**.

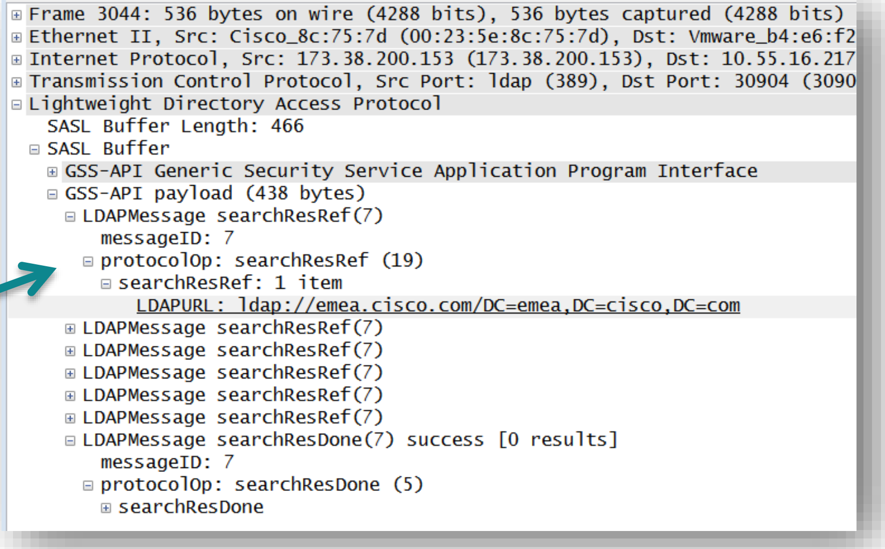
	Parameter Name	Parameter Value	Comment	Last Changed
●	TROUBLESHOOTING.EncryptionOffPeriod	30	How to disable AD encryption fo...	20:33:51 19.01.2015 GMT

Advanced Tuning – disabled encryption

Disabling encryption renders packet captures of AD traffic much more useful.



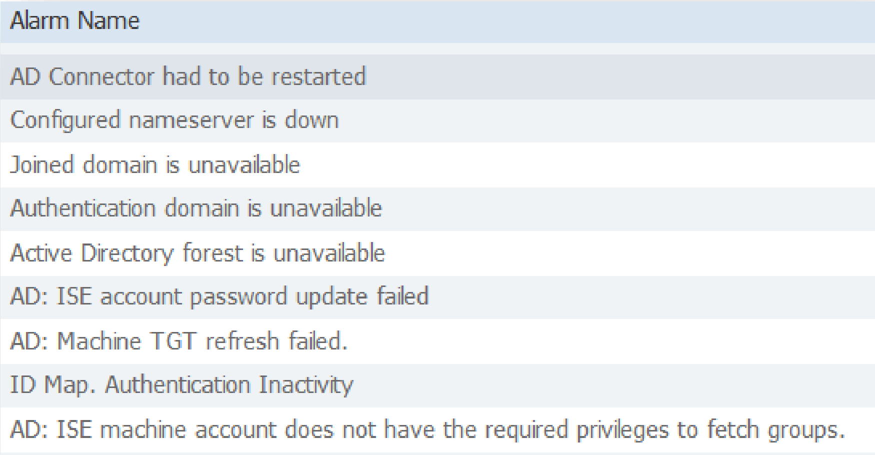
```
⊞ Frame 4562: 568 bytes on wire (4544 bits), 568 bytes captured (4544 bits)
⊞ Ethernet II, Src: Cisco_8c:75:7d (00:23:5e:8c:75:7d), Dst: Vmware_b4:e6:f2
⊞ Internet Protocol, Src: 173.38.200.151 (173.38.200.151), Dst: 10.55.16.217
⊞ Transmission Control Protocol, Src Port: ldap (389), Dst Port: 57326 (5732
⊟ Lightweight Directory Access Protocol
    SASL Buffer Length: 498
  ⊟ SASL Buffer
    ⊞ GSS-API Generic Security Service Application Program Interface
      GSS-API Encrypted payload (438 bytes)
```



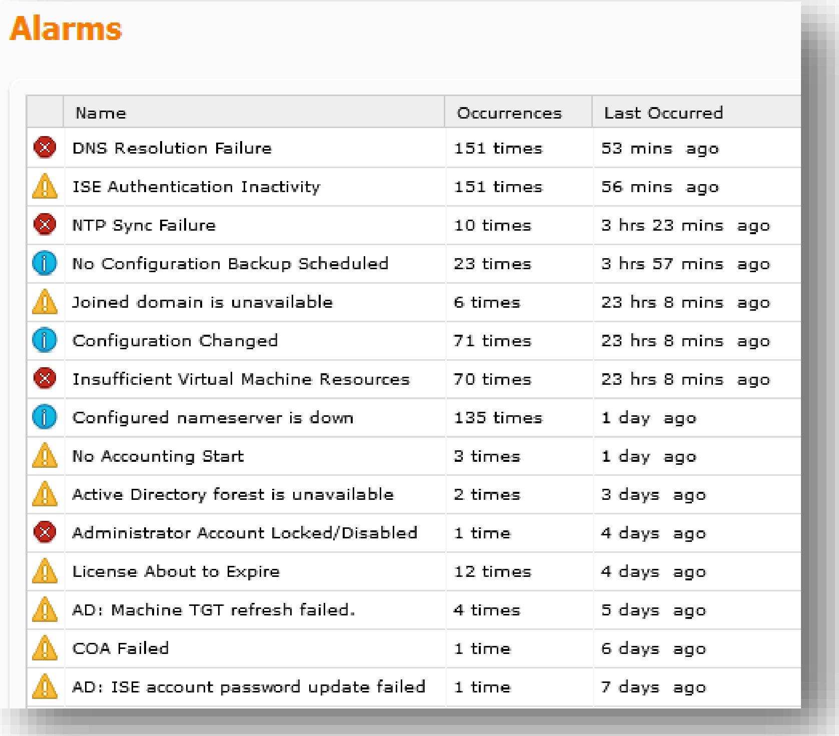
```
⊞ Frame 3044: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits)
⊞ Ethernet II, Src: Cisco_8c:75:7d (00:23:5e:8c:75:7d), Dst: Vmware_b4:e6:f2
⊞ Internet Protocol, Src: 173.38.200.153 (173.38.200.153), Dst: 10.55.16.217
⊞ Transmission Control Protocol, Src Port: ldap (389), Dst Port: 30904 (3090
⊟ Lightweight Directory Access Protocol
    SASL Buffer Length: 466
  ⊟ SASL Buffer
    ⊞ GSS-API Generic Security Service Application Program Interface
    ⊟ GSS-API payload (438 bytes)
      ⊟ LDAPMessage searchResRef(7)
          messageID: 7
        ⊟ protocolOp: searchResRef (19)
          ⊟ searchResRef: 1 item
              LDAPURL: ldap://emea.cisco.com/DC=emea,DC=cisco,DC=com
      ⊞ LDAPMessage searchResRef(7)
      ⊞ LDAPMessage searchResRef(7)
      ⊞ LDAPMessage searchResRef(7)
      ⊞ LDAPMessage searchResRef(7)
      ⊞ LDAPMessage searchResRef(7)
      ⊟ LDAPMessage searchResDone(7) success [0 results]
          messageID: 7
        ⊟ protocolOp: searchResDone (5)
          ⊞ searchResDone
```

Alarms for AD connector issues

- Finally, there are alarms for AD
- Use them to get early alerts



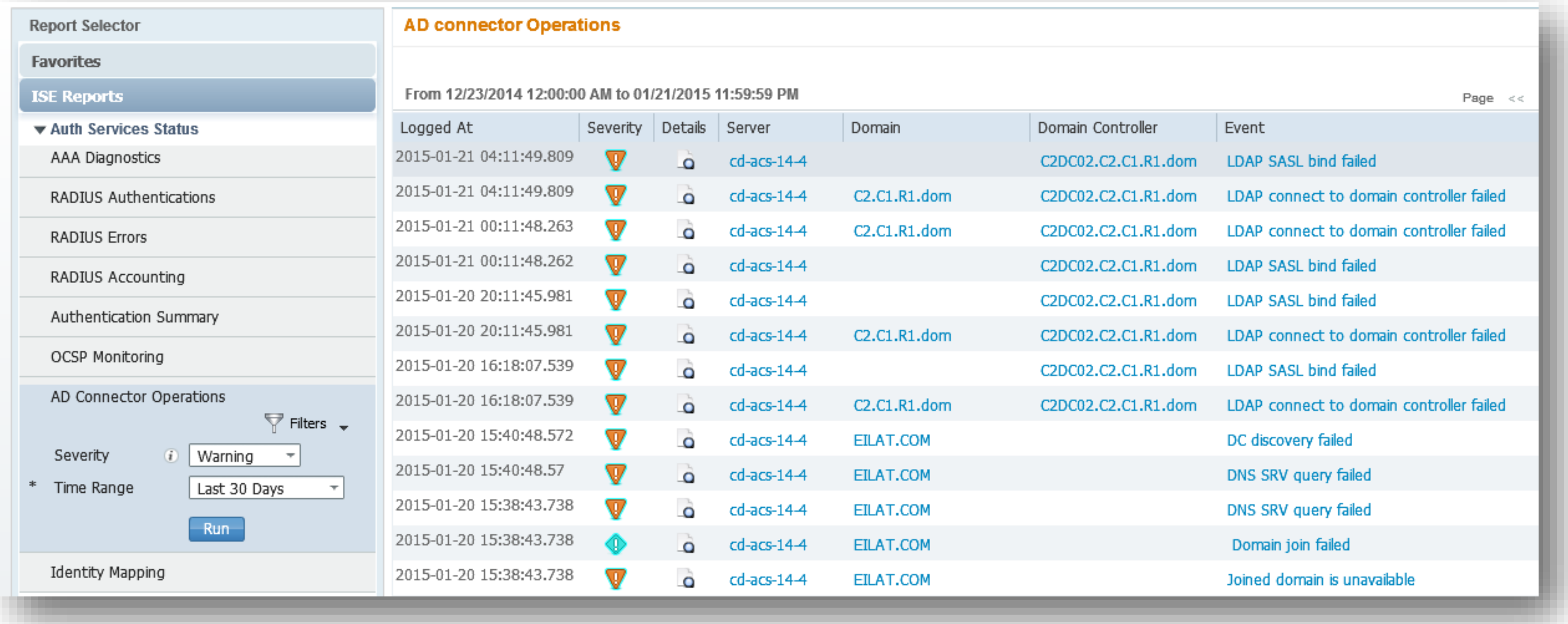
Alarm Name
AD Connector had to be restarted
Configured nameserver is down
Joined domain is unavailable
Authentication domain is unavailable
Active Directory forest is unavailable
AD: ISE account password update failed
AD: Machine TGT refresh failed.
ID Map. Authentication Inactivity
AD: ISE machine account does not have the required privileges to fetch groups.



Alarms

	Name	Occurrences	Last Occurred
✖	DNS Resolution Failure	151 times	53 mins ago
⚠	ISE Authentication Inactivity	151 times	56 mins ago
✖	NTP Sync Failure	10 times	3 hrs 23 mins ago
ℹ	No Configuration Backup Scheduled	23 times	3 hrs 57 mins ago
⚠	Joined domain is unavailable	6 times	23 hrs 8 mins ago
ℹ	Configuration Changed	71 times	23 hrs 8 mins ago
✖	Insufficient Virtual Machine Resources	70 times	23 hrs 8 mins ago
ℹ	Configured nameserver is down	135 times	1 day ago
⚠	No Accounting Start	3 times	1 day ago
⚠	Active Directory forest is unavailable	2 times	3 days ago
✖	Administrator Account Locked/Disabled	1 time	4 days ago
⚠	License About to Expire	12 times	4 days ago
⚠	AD: Machine TGT refresh failed.	4 times	5 days ago
⚠	COA Failed	1 time	6 days ago
⚠	AD: ISE account password update failed	1 time	7 days ago

AD connector operations report



Report Selector

Favorites

ISE Reports

▼ Auth Services Status

- AAA Diagnostics
- RADIUS Authentications
- RADIUS Errors
- RADIUS Accounting
- Authentication Summary
- OCSP Monitoring
- AD Connector Operations

Filters

Severity: Warning

* Time Range: Last 30 Days

Run

- Identity Mapping

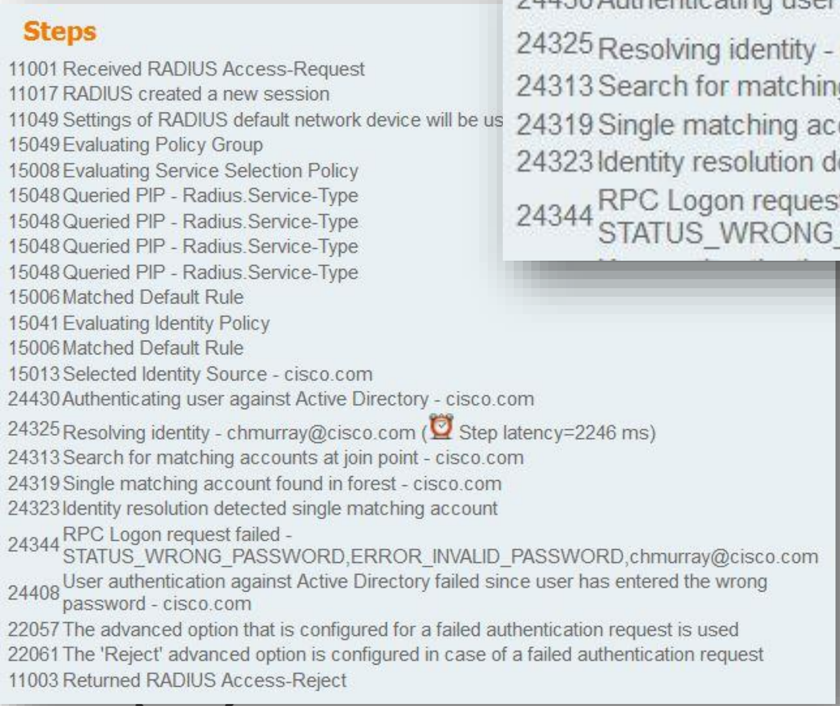
AD connector Operations

From 12/23/2014 12:00:00 AM to 01/21/2015 11:59:59 PM

Page <<

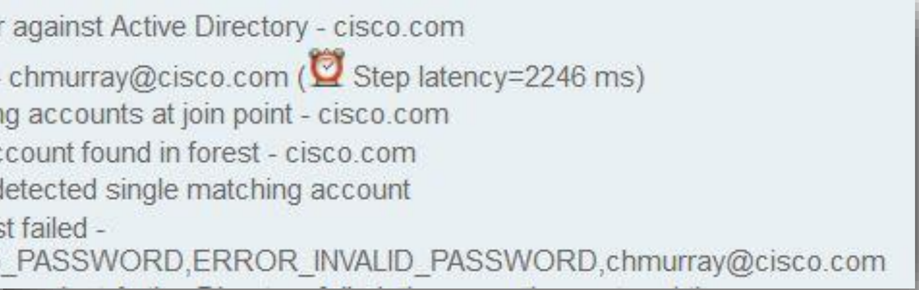
Logged At	Severity	Details	Server	Domain	Domain Controller	Event
2015-01-21 04:11:49.809	⚠	🔍	cd-acs-14-4		C2DC02.C2.C1.R1.dom	LDAP SASL bind failed
2015-01-21 04:11:49.809	⚠	🔍	cd-acs-14-4	C2.C1.R1.dom	C2DC02.C2.C1.R1.dom	LDAP connect to domain controller failed
2015-01-21 00:11:48.263	⚠	🔍	cd-acs-14-4	C2.C1.R1.dom	C2DC02.C2.C1.R1.dom	LDAP connect to domain controller failed
2015-01-21 00:11:48.262	⚠	🔍	cd-acs-14-4		C2DC02.C2.C1.R1.dom	LDAP SASL bind failed
2015-01-20 20:11:45.981	⚠	🔍	cd-acs-14-4		C2DC02.C2.C1.R1.dom	LDAP SASL bind failed
2015-01-20 20:11:45.981	⚠	🔍	cd-acs-14-4	C2.C1.R1.dom	C2DC02.C2.C1.R1.dom	LDAP connect to domain controller failed
2015-01-20 16:18:07.539	⚠	🔍	cd-acs-14-4		C2DC02.C2.C1.R1.dom	LDAP SASL bind failed
2015-01-20 16:18:07.539	⚠	🔍	cd-acs-14-4	C2.C1.R1.dom	C2DC02.C2.C1.R1.dom	LDAP connect to domain controller failed
2015-01-20 15:40:48.572	⚠	🔍	cd-acs-14-4	EILAT.COM		DC discovery failed
2015-01-20 15:40:48.57	⚠	🔍	cd-acs-14-4	EILAT.COM		DNS SRV query failed
2015-01-20 15:38:43.738	⚠	🔍	cd-acs-14-4	EILAT.COM		DNS SRV query failed
2015-01-20 15:38:43.738	◆	🔍	cd-acs-14-4	EILAT.COM		Domain join failed
2015-01-20 15:38:43.738	⚠	🔍	cd-acs-14-4	EILAT.COM		Joined domain is unavailable

Improved authentication details



Steps

```
11001 Received RADIUS Access-Request
11017 RADIUS created a new session
11049 Settings of RADIUS default network device will be us
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - Radius.Service-Type
15048 Queried PIP - Radius.Service-Type
15048 Queried PIP - Radius.Service-Type
15048 Queried PIP - Radius.Service-Type
15006 Matched Default Rule
15041 Evaluating Identity Policy
15006 Matched Default Rule
15013 Selected Identity Source - cisco.com
24430 Authenticating user against Active Directory - cisco.com
24325 Resolving identity - chmurray@cisco.com (⏰ Step latency=2246 ms)
24313 Search for matching accounts at join point - cisco.com
24319 Single matching account found in forest - cisco.com
24323 Identity resolution detected single matching account
24344 RPC Logon request failed -
      STATUS_WRONG_PASSWORD,ERROR_INVALID_PASSWORD,chmurray@cisco.com
24408 User authentication against Active Directory failed since user has entered the wrong
      password - cisco.com
22057 The advanced option that is configured for a failed authentication request is used
22061 The 'Reject' advanced option is configured in case of a failed authentication request
11003 Returned RADIUS Access-Reject
```



```
24430 Authenticating user against Active Directory - cisco.com
24325 Resolving identity - chmurray@cisco.com (⏰ Step latency=2246 ms)
24313 Search for matching accounts at join point - cisco.com
24319 Single matching account found in forest - cisco.com
24323 Identity resolution detected single matching account
24344 RPC Logon request failed -
      STATUS_WRONG_PASSWORD,ERROR_INVALID_PASSWORD,chmurray@cisco.com
```

There is a lot of new output from the AD connector on what it is doing that can help identify issues.

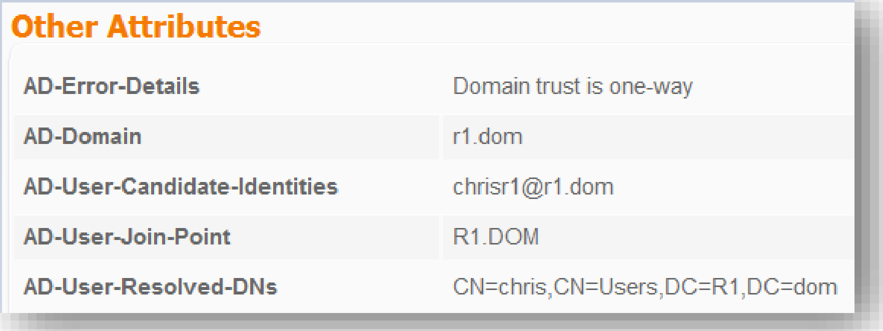
Watch for latency icons; they help you locate where a delay is.

Improved authentication details

- There are also some new AD attributes available to authorization

- AD-Error-Details
  - Description of last error encountered
- AD-Domain
  - DNS domain where user was located
- AD-User-Candidate-Identities
  - Potential accounts that matched

- AD-User-Join-Point
  – Which join point identity was found via
- AD-User-Resolved-DNs
  – Distinguished name of user



Other Attributes

AD-Error-Details	Domain trust is one-way
AD-Domain	r1.dom
AD-User-Candidate-Identities	chrisr1@r1.dom
AD-User-Join-Point	R1.DOM
AD-User-Resolved-DNs	CN=chris,CN=Users,DC=R1,DC=dom

Upgrading from ISE 1.2?

- **1.3 machine accounts require a new permission**
  - “Read tokenGroups” attribute
  - Check with your AD administrator
- You will need to rejoin to AD
  - Old credentials cannot be used with new connector
- Complaint about group SIDs not resolving?
  - Check those groups still exist in AD
- Customized centrifydc.conf or resolv.conf?
  - Such customizations no longer apply
- Hard-coded DC?
  - Use AD Sites

ISE 1.2

Upgrade checklist

1. Get AD admin to grant “Read tokenGroups” permission
2. Rejoin ISE to Active Directory
3. Verify the right Site and DC are being used
4. Configure Authentication Domains
5. Configure Identity Resolution options
6. If using EAP-TLS, configure CAP smart search
7. Use Test User to verify configuration

ISE 1.2

Upgrading to 2.0 from 1.3/1.4

- Be aware there is known issue that loses AD configuration
  - CSCux04189

- Take a backup, restore and rejoin to AD

Recent enhancements

- Support for Boolean attributes
- Support for msRadiusFramedIPAddress
  - Microsoft IP Address attribute in AD
  - Can be used in authorisation result
  - E.g. Framed-IP-Address

Some under the hood improvements

- Enhanced DC locator
  - Closer to Windows implementation
  - Can cope with large responses and rendezvous quicker
- Periodic information discovery
  - Domains, forests, trusts, UPNs
- Faster failover for Kerberos, LDAP, MS-RPC
- Performance on par (sometimes better) than 1.2 for one join point
- Hostname length up to 63 characters
  - Appliance names like ise-some-prefix-10.1.1.2 are usable now

Some known issues

- RPC/Policy errors and SMB connection resets?
  - Load related usually – check DC load and MaxConcurrentApi Registry setting
  - http://blogs.technet.com/b/get-exchangehelp/archive/2013/01/31/the-curious-case-of-maxconcurrentapi.aspx
  - 2003, 2008 default to 2 connections
  - Scripts exist to help diagnose if you have a problem
- 1.3 memory leak fix
  - Patch your 1.3 if you experience memory leak
- Check **PDC** performance (see separate slide)

Primary Domain Controller (Role) dependency

- Bad passwords can cause serious delays
- WHY?
  - When there is an invalid password, the DC passes the authentication back to the PDC Emulator because it's going to have a copy of the latest password. If the PDC Emulator authenticates him successfully then the logon is processed. This happens behind the scenes and does not increment the bad password count attribute.
- If the PDC is busy and bad passwords keep coming this can cause big latency
- Try to minimise your sources of bad passwords, monitor PDC performance
- Advise AD guys install correct patches to maintain PDC health
- Beware load balancers that do RADIUS test probes with invalid passwords

Q&A

Some questions for you

- Who requires support for RODC
  - Discuss the change-password implications
- Soon-to-be-released Server 2016
  - SMB 3.11 (security improvements, new ciphers)
  - Don’t set to ‘only 3.11’ for now
- Passive identity mapping configuration (WMI)

Wrap-Up

Remember…

Forming a **team** responsible for Network Access and following deployment tips will lead to a more stable service.

Takeaways

- Treat NA as a joint responsibility
- Follow our deployment tips
- Use new alarms and diagnostics
- And don’t worry if you hit an issue
  - We are in a better place now

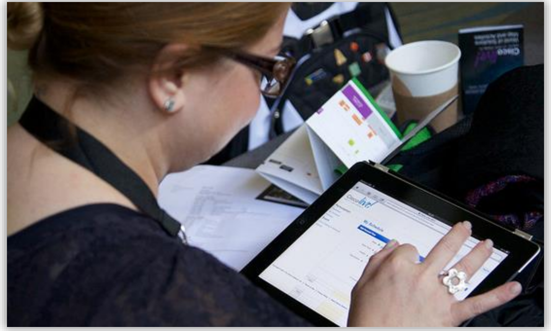
Call to Action

- Attend the following related sessions
  - Tue 14.15 BRKSEC-3699 – Craig’s session on ISE scale and HA
    - Well that was yesterday! Watch the video if you missed it
  - Thu 09.00 BRKSEC-3697 – Aaron’s Advanced ISE session
  - Thu 11.30 BRKSEC-2060 – Doug’s session on TACACS+
- Visit the World of Solutions for
  - Cisco Campus – find us in the Security section – look for **RED**
- Meet the Engineer
  - I am available Thursday

Complete Your **Online Session Evaluation**

- Please complete your online session evaluations after each session. Complete 4 session evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt.

- All surveys can be completed via the Cisco Live Mobile App or the Communication Stations



Thank you

CISCO

We’re ready. Are you?

Additional Material - Troubleshooting

Old AD connector was hard to diagnose

- One of biggest problems with old AD connector was it was hard to troubleshoot
- Troubleshooting was often invasive and slow
- Sometimes required installing root patch to change settings

Objectives

- Make it easier to understand root cause directly from ISE GUI
- Make it obvious
  - Use Alarms
  - New Report
  - Increased details in authentication STEPS
- Built-in tools
  - Test user authentication on-board
  - Diagnose Environment on-board
  - Tweaking on-board
  - Ability to decrypt AD traffic temporarily

Top issues

- Permissions of ISE machine account
    - Ask AD admin to check your ISE machine accounts have sufficient permissions
- Clocks of DCs and ISE are not within 5 minutes of each other
    - Check the clocks – run the Diagnostic Tool
- Not using Authentication Domains when you should
- DNS or DCs are not responding fast enough
    - Look at the STEPS detail / use sniffers – TRUST THE LATENCY ALARMS
- Not using AD Sites
    - Causes various issues, slowness, 4K DNS problem, …
- Review the Deployment Tips and check everything is still sound

Permissions

- Required for Join
  - Search AD
  - Create machine account
  - Set attributes on it
- Caveat:
  - You can create it manually
  - If name matches, it should sync up

- Permissions required by ISE machine account
  - Ability to change its own password
  - Read machine/user objects
  - Search AD – both DC and GC
  - Query some parts of AD schema to learn about domains and UPNs
  - Ability to Read tokenGroups

Permissions

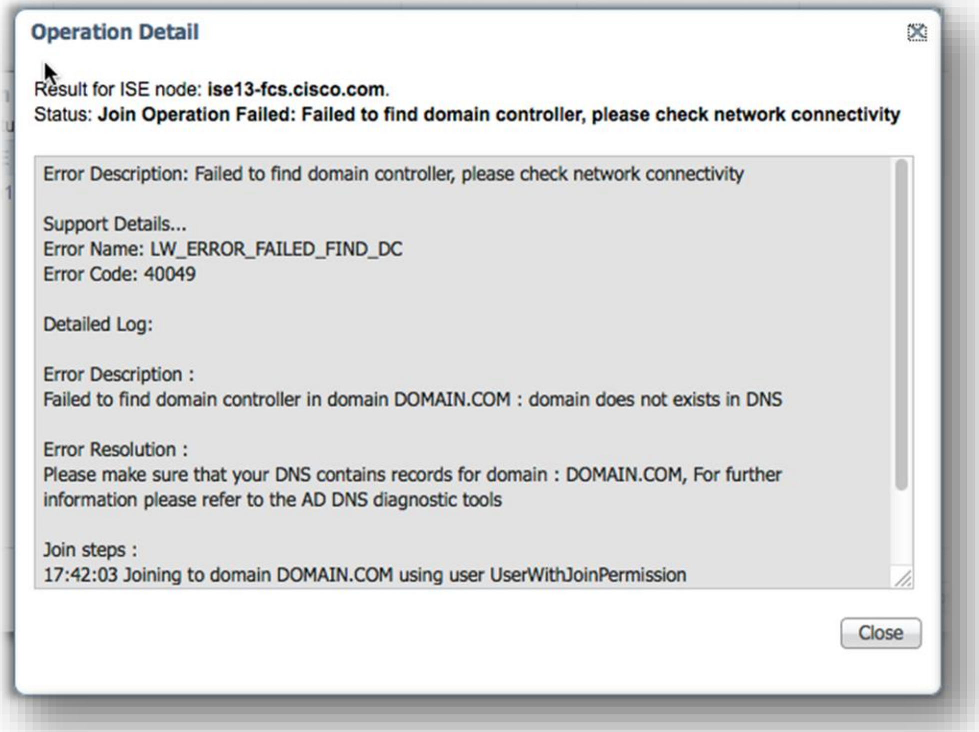
- Has someone moved the ISE machine account(s) or edited its AD permissions?
- Or even deleted it? (does happen)
- Has it failed to change its password?
- Note in 1.3 ISE machine accounts request “Read tokenGroups”
  - That is NOT granted automatically by “Read all objects” permission
  - It needs added explicitly

- Quick hack (to grant tokenGroups)
  - **dsacls "OU=No-O365,OU=External,OU=Users,OU=EG,DC=yourdomain,DC=com" /I:T /G “ISE_MACHINE_NAME$":rp;tokenGroups**
- If that works, AD admin should correct the permissions properly
- OU can impact you – try moving machine account to less restrictive OU (even just as a test)

Join Error?

- Check clock difference – it MUST be less than 5 minutes difference with DC
- Check permissions
  - Of the credentials being used to attempt the join
  - Where (Organizational Unit) the ISE machine account is being created
    - Try another OU
    - Ask AD admin to determine which permissions objects in that OU inherit
    - There are tools to do that – compare it to the list of required permissions
- Get a weird ‘quota exceeded’ error?
  - This means the user has exceeded their join quota, typically 10 times for a user who is not a Domain Administrator
- Node not joined – bogus error, means DC blocked – check permissions

Join Errors – Check Detailed Report

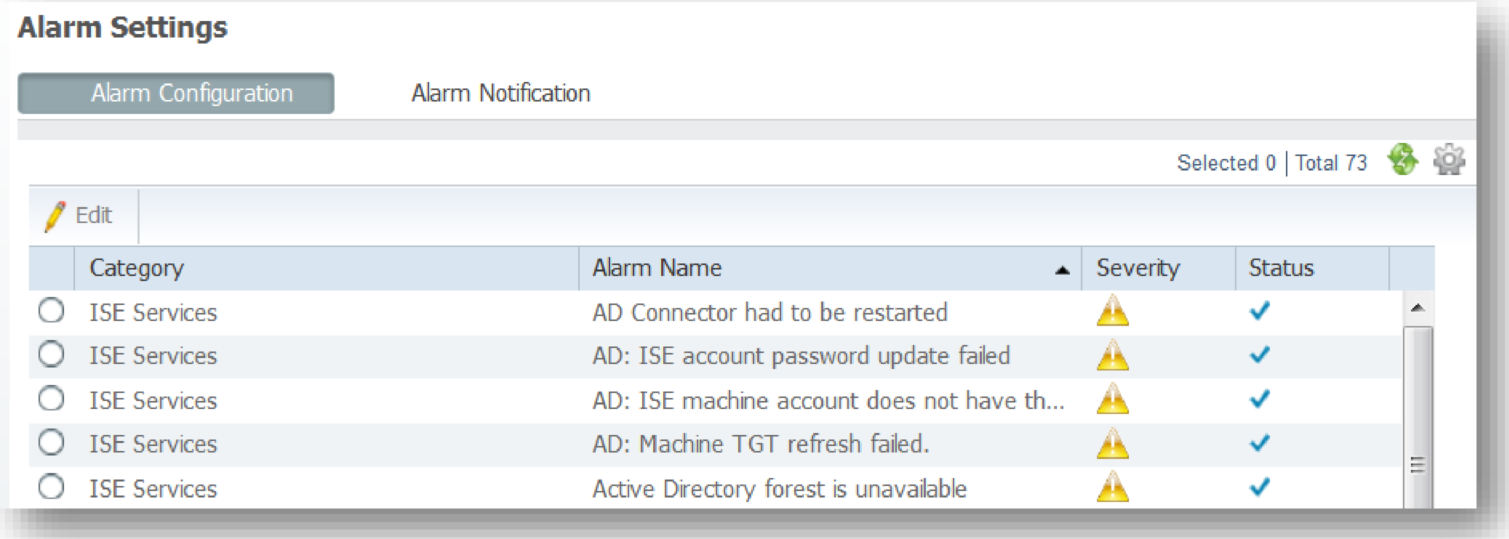


Result for ISE node: **ise13-fcs.cisco.com**.
Status: **Join Operation Failed: Failed to find domain controller, please check network connectivity**

```
Error Description: Failed to find domain controller, please check network connectivity

Support Details...
Error Name: LW_ERROR_FAILED_FIND_DC
Error Code: 40049

Detailed Log:

Error Description :
Failed to find domain controller in domain DOMAIN.COM : domain does not exists in DNS

Error Resolution :
Please make sure that your DNS contains records for domain : DOMAIN.COM, For further
information please refer to the AD DNS diagnostic tools

Join steps :
17:42:03 Joining to domain DOMAIN.COM using user UserWithJoinPermission
```

Check for AD Alarms

Recommend you get alerts about anything above Warning level

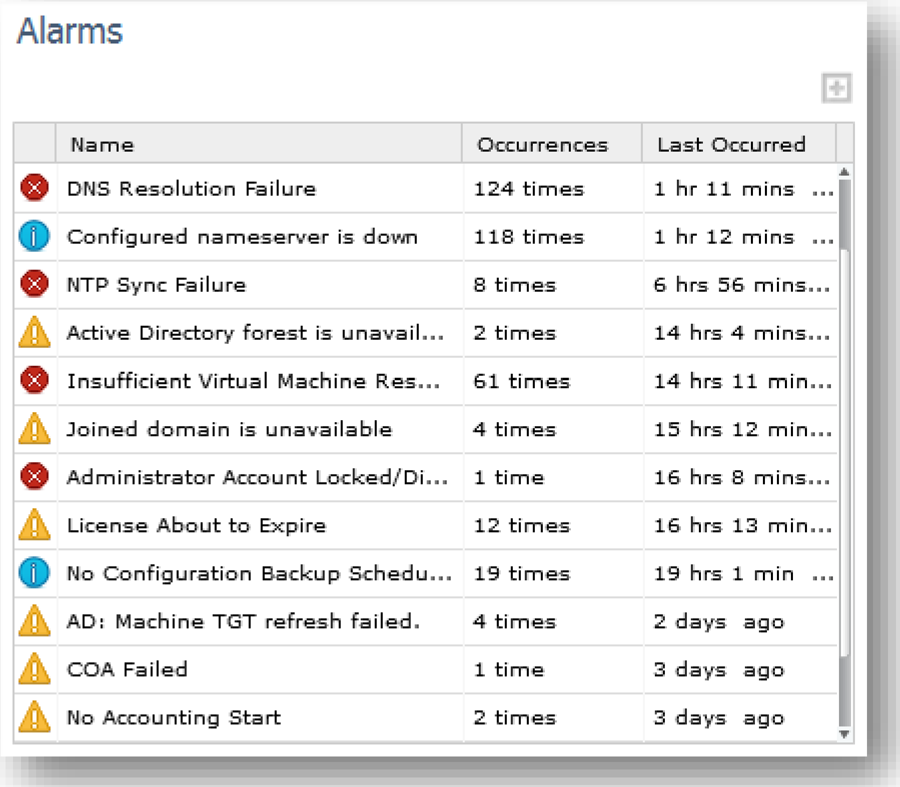


Alarm Settings

	Category	Alarm Name	Severity	Status
○	ISE Services	AD Connector had to be restarted	⚠	✓
○	ISE Services	AD: ISE account password update failed	⚠	✓
○	ISE Services	AD: ISE machine account does not have th...	⚠	✓
○	ISE Services	AD: Machine TGT refresh failed.	⚠	✓
○	ISE Services	Active Directory forest is unavailable	⚠	✓

Example Alarms

- TGT failures are serious
  - Often due to clock sync issue
- DNS – speak to DNS guys
- NTP – time bomb – rectify ASAP

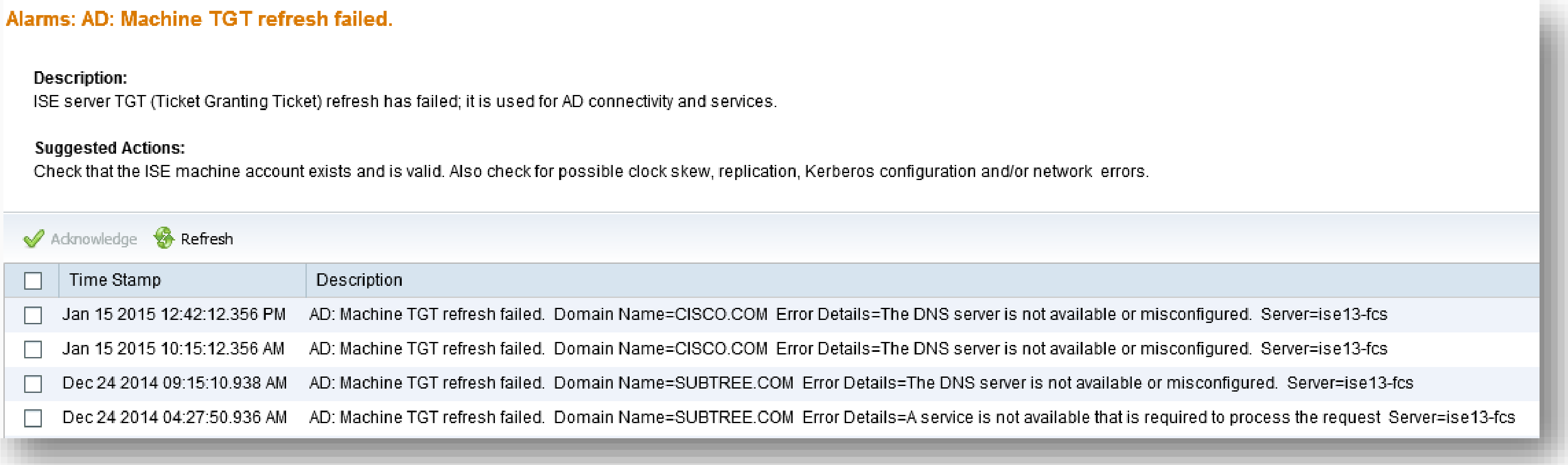


Alarms

	Name	Occurrences	Last Occurred
✖	DNS Resolution Failure	124 times	1 hr 11 mins ...
ⓘ	Configured nameserver is down	118 times	1 hr 12 mins ...
✖	NTP Sync Failure	8 times	6 hrs 56 mins...
⚠	Active Directory forest is unavail...	2 times	14 hrs 4 mins...
✖	Insufficient Virtual Machine Res...	61 times	14 hrs 11 min...
⚠	Joined domain is unavailable	4 times	15 hrs 12 min...
✖	Administrator Account Locked/Di...	1 time	16 hrs 8 mins...
⚠	License About to Expire	12 times	16 hrs 13 min...
ⓘ	No Configuration Backup Schedu...	19 times	19 hrs 1 min ...
⚠	AD: Machine TGT refresh failed.	4 times	2 days ago
⚠	COA Failed	1 time	3 days ago
⚠	No Accounting Start	2 times	3 days ago

Example Alarm

A TGT refresh failure is serious – you have a few hours until everything fails



Alarms: AD: Machine TGT refresh failed.

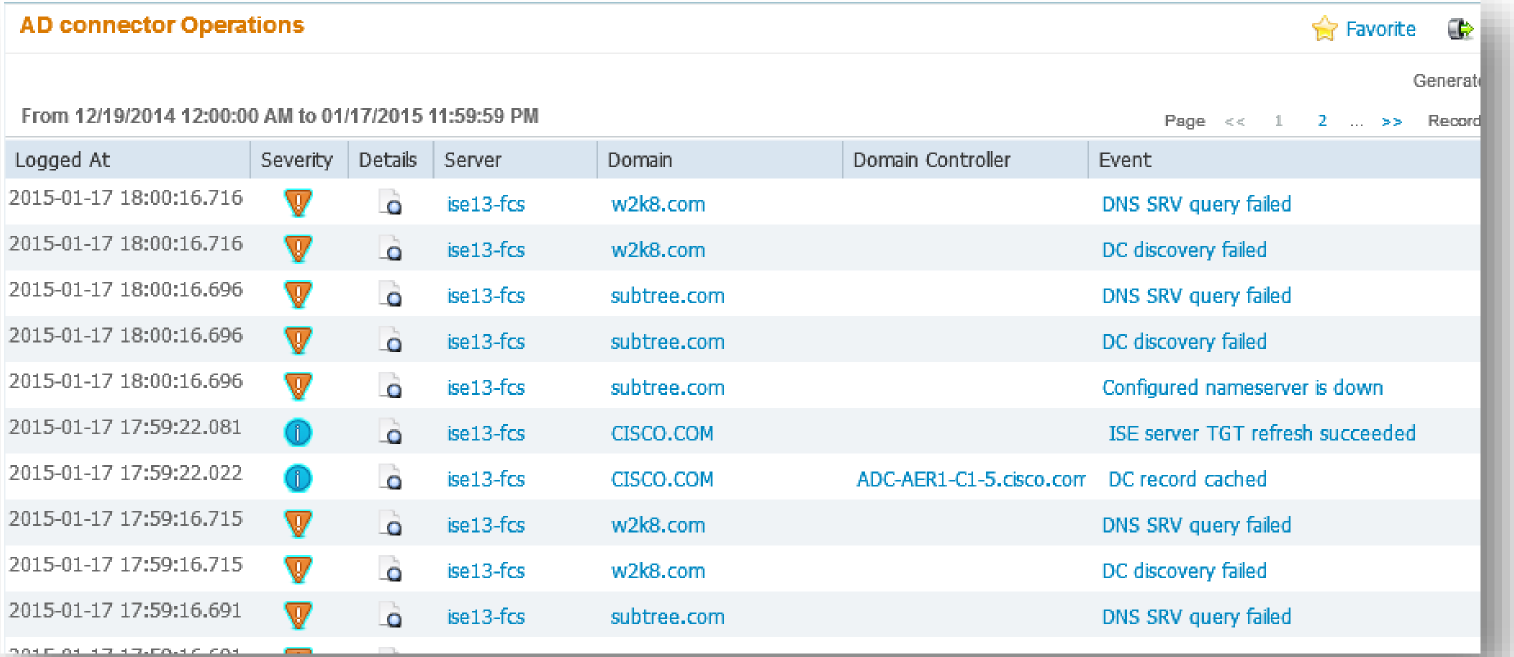
Description:
ISE server TGT (Ticket Granting Ticket) refresh has failed; it is used for AD connectivity and services.

Suggested Actions:
Check that the ISE machine account exists and is valid. Also check for possible clock skew, replication, Kerberos configuration and/or network errors.

□	Time Stamp	Description
□	Jan 15 2015 12:42:12.356 PM	AD: Machine TGT refresh failed. Domain Name=CISCO.COM Error Details=The DNS server is not available or misconfigured. Server=ise13-fcs
□	Jan 15 2015 10:15:12.356 AM	AD: Machine TGT refresh failed. Domain Name=CISCO.COM Error Details=The DNS server is not available or misconfigured. Server=ise13-fcs
□	Dec 24 2014 09:15:10.938 AM	AD: Machine TGT refresh failed. Domain Name=SUBTREE.COM Error Details=The DNS server is not available or misconfigured. Server=ise13-fcs
□	Dec 24 2014 04:27:50.936 AM	AD: Machine TGT refresh failed. Domain Name=SUBTREE.COM Error Details=A service is not available that is required to process the request Server=ise13-fcs

Check new AD Connector Report

Look for warnings – there SHOULD be NONE



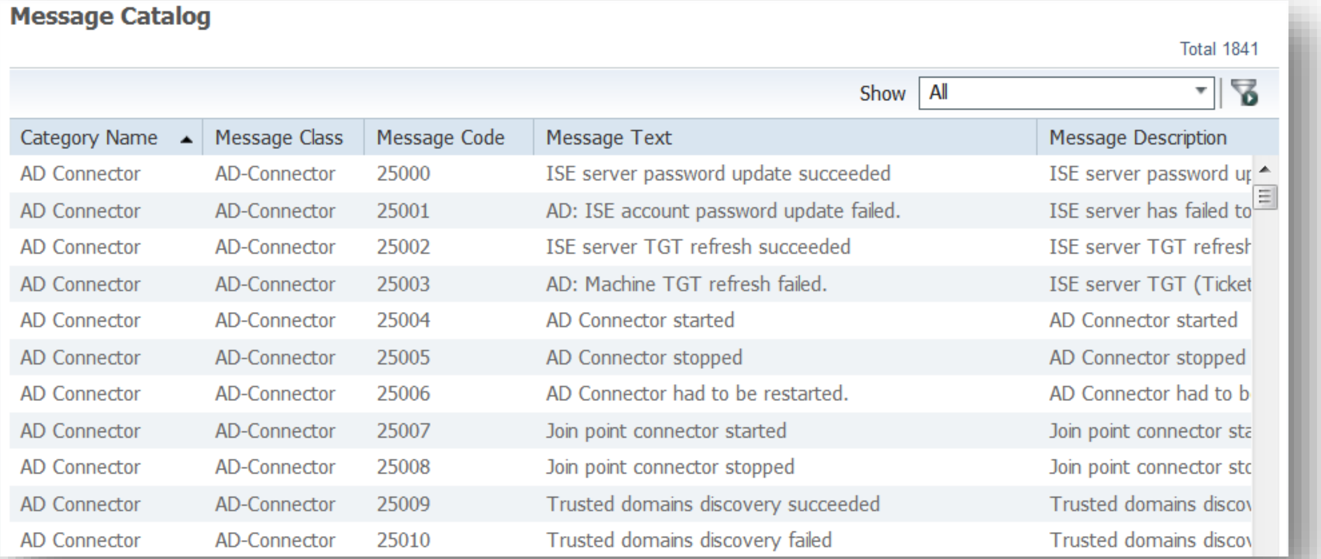
AD connector Operations

From 12/19/2014 12:00:00 AM to 01/17/2015 11:59:59 PM

Logged At	Severity	Details	Server	Domain	Domain Controller	Event
2015-01-17 18:00:16.716	⚠	🔍	ise13-fcs	w2k8.com		DNS SRV query failed
2015-01-17 18:00:16.716	⚠	🔍	ise13-fcs	w2k8.com		DC discovery failed
2015-01-17 18:00:16.696	⚠	🔍	ise13-fcs	subtree.com		DNS SRV query failed
2015-01-17 18:00:16.696	⚠	🔍	ise13-fcs	subtree.com		DC discovery failed
2015-01-17 18:00:16.696	⚠	🔍	ise13-fcs	subtree.com		Configured nameserver is down
2015-01-17 17:59:22.081	ⓘ	🔍	ise13-fcs	CISCO.COM		ISE server TGT refresh succeeded
2015-01-17 17:59:22.022	ⓘ	🔍	ise13-fcs	CISCO.COM	ADC-AER1-C1-5.cisco.com	DC record cached
2015-01-17 17:59:16.715	⚠	🔍	ise13-fcs	w2k8.com		DNS SRV query failed
2015-01-17 17:59:16.715	⚠	🔍	ise13-fcs	w2k8.com		DC discovery failed
2015-01-17 17:59:16.691	⚠	🔍	ise13-fcs	subtree.com		DNS SRV query failed

New possible AD messages to watch for

System > Logging > Message Catalog



Message Catalog

Total 1841

Show: All

Category Name	Message Class	Message Code	Message Text	Message Description
AD Connector	AD-Connector	25000	ISE server password update succeeded	ISE server password up
AD Connector	AD-Connector	25001	AD: ISE account password update failed.	ISE server has failed to
AD Connector	AD-Connector	25002	ISE server TGT refresh succeeded	ISE server TGT refresh
AD Connector	AD-Connector	25003	AD: Machine TGT refresh failed.	ISE server TGT (Ticket
AD Connector	AD-Connector	25004	AD Connector started	AD Connector started
AD Connector	AD-Connector	25005	AD Connector stopped	AD Connector stopped
AD Connector	AD-Connector	25006	AD Connector had to be restarted.	AD Connector had to b
AD Connector	AD-Connector	25007	Join point connector started	Join point connector sta
AD Connector	AD-Connector	25008	Join point connector stopped	Join point connector stc
AD Connector	AD-Connector	25009	Trusted domains discovery succeeded	Trusted domains discov
AD Connector	AD-Connector	25010	Trusted domains discovery failed	Trusted domains discov

Failed Authentications?

- Check STEPS in failed authentication
  - Look for latency warnings/icons – they should indicate what ISE is doing
  - E.g. authentication, fetching attribute, groups, …
- Use Test Authentication tool to get detailed information
- See if certain users work and not others
- Kerberos OK but not MSRPC? Firewalled
- Specific domain? Are DC’s up?
- Corresponding alarms or errors in AD report?
- Run environment diagnostic

Test user authentication

- Can authenticate but not retrieve attributes?
  - Indicates ISE machine account needs more AD permissions
  - If groups are not working this is usually lack of “Read tokenGroups”
    - Note that’s an attribute, not a group
- Can authenticate but not if retrieve groups?
  - Also indicates ISE machine account needs more AD permissions
- Do you see SID = “(Name not resolved)”
  - Indicates stale SIDs in user object or no DC available for the domain
- Does one of MS-RPC and Kerberos work but not the other?
  - Suspect environment configuration or blocking ports

No such object.. Yes there is!

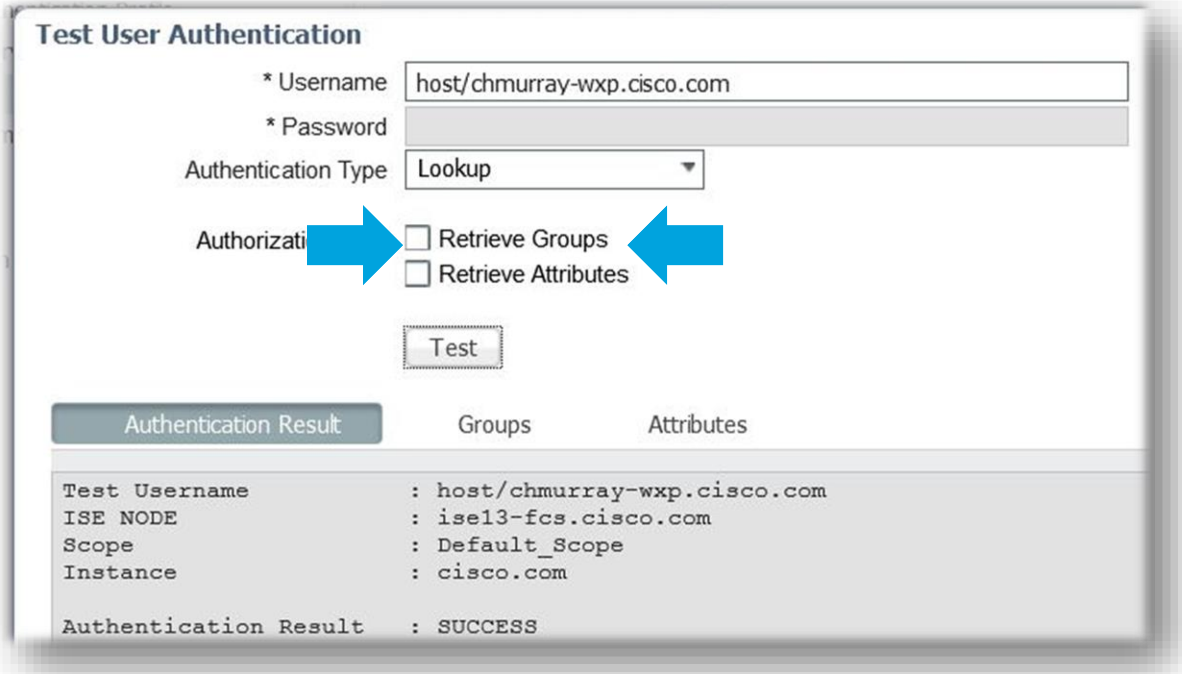
- Are you seeing ‘object not found’ or ‘no such object’ errors
  - Usually when looking up a group SID
- CAN mean domain no longer exists or no DCs left for that domain
- BUT can also mean you don’t have sufficient permissions to read it
  - LDAP replies the same – no such object, even if it exists and you just don;’t have permission to read it
- So double-check permissions (of ISE machine account) if you know the SID is resolvable

Are users getting a Workstation restriction?

- Key point
  - To AD, the origin of authentications and other traffic is the ISE machine account
    - **NOT** the user’s workstation or device
  - This is why “Logon to Workstation” does not work as expected
- So user authentication appears to come from the ISE machine accounts
- Therefore, users must be granted **Logon to ISE machine accounts**, not their end devices
- If you are getting Workstation restriction error, discuss the above with AD admin

Using Test Tool to check machine SPN

These are needed for ISE to authenticate machine accounts

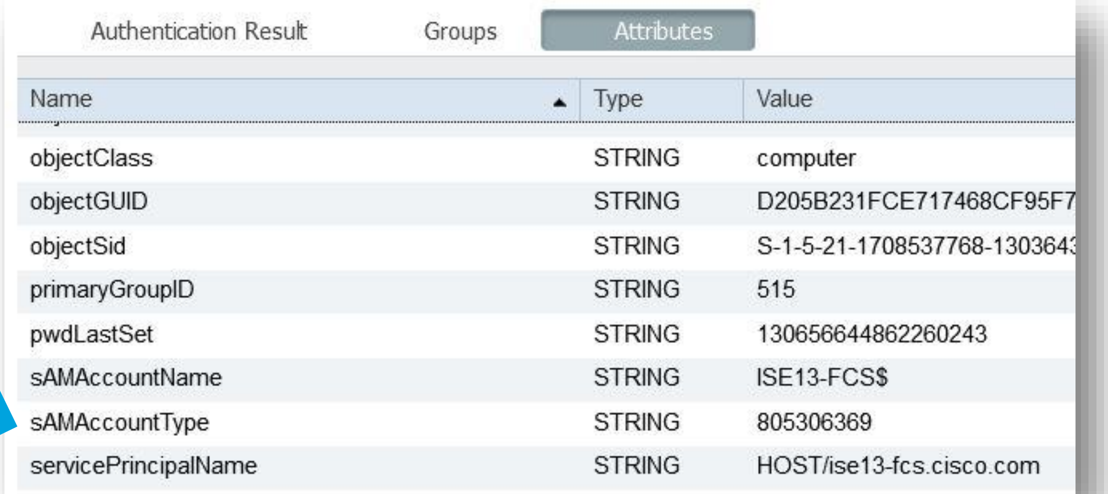


* Username	host/chmurray-wxp.cisco.com
* Password	
Authentication Type	Lookup
Authorizati	□ Retrieve Groups □ Retrieve Attributes

```
Test Username            : host/chmurray-wxp.cisco.com
ISE NODE                 : ise13-fcs.cisco.com
Scope                    : Default_Scope
Instance                 : cisco.com

Authentication Result    : SUCCESS
```

Using Test Tool to check machine SPN

This attribute must be added if it is missing

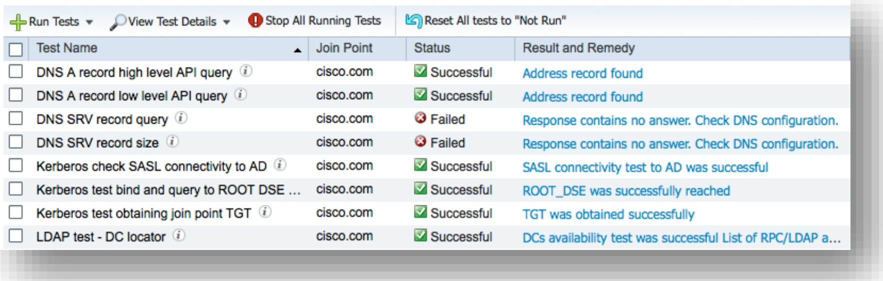


Name	Type	Value
objectClass	STRING	computer
objectGUID	STRING	D205B231FCE717468CF95F7
objectSid	STRING	S-1-5-21-1708537768-130364
primaryGroupID	STRING	515
pwdLastSet	STRING	130656644862260243
sAMAccountName	STRING	ISE13-FCS$
sAMAccountType	STRING	805306369
servicePrincipalName	STRING	HOST/ise13-fcs.cisco.com

If that attribute is missing, you need to add it!

Diagnostic Tool

Run this periodically or when the issue is not obvious

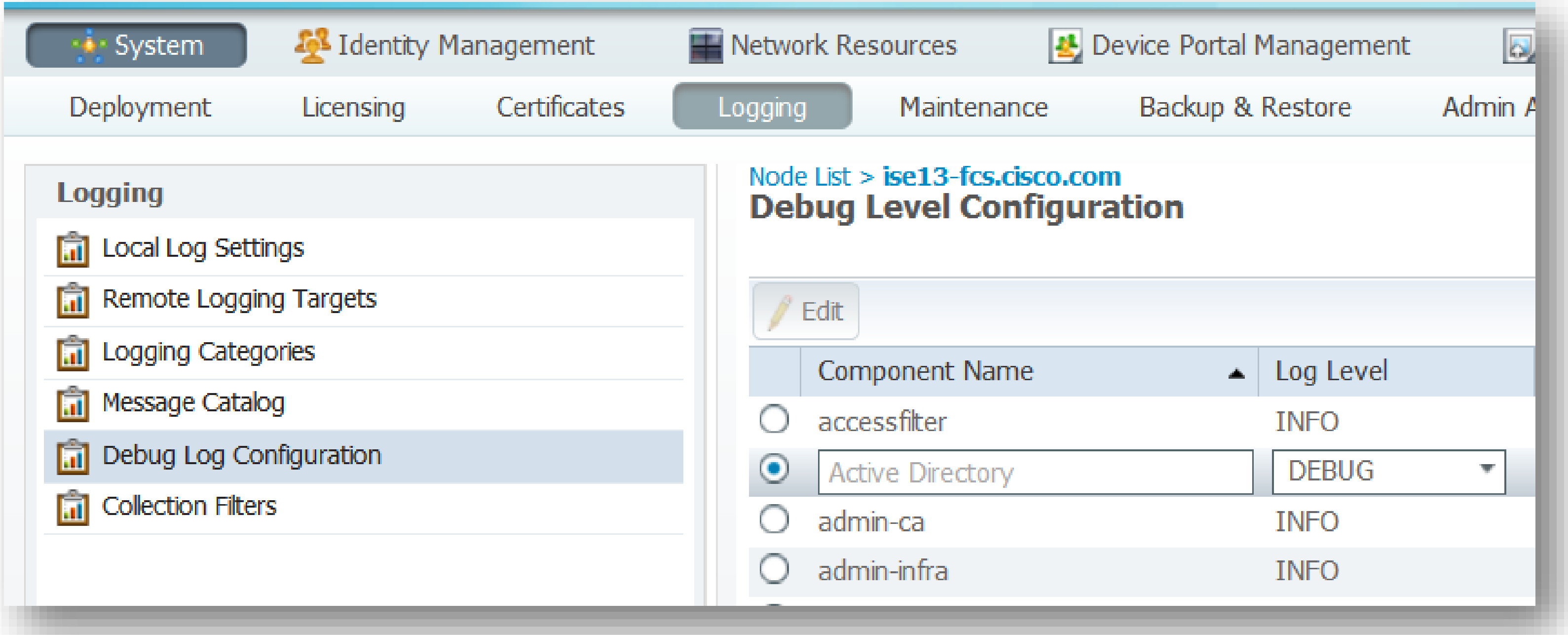


□	Test Name	Join Point	Status	Result and Remedy
□	DNS A record high level API query	cisco.com	✓ Successful	Address record found
□	DNS A record low level API query	cisco.com	✓ Successful	Address record found
□	DNS SRV record query	cisco.com	☒ Failed	Response contains no answer. Check DNS configuration.
□	DNS SRV record size	cisco.com	☒ Failed	Response contains no answer. Check DNS configuration.
□	Kerberos check SASL connectivity to AD	cisco.com	✓ Successful	SASL connectivity test to AD was successful
□	Kerberos test bind and query to ROOT DSE ...	cisco.com	✓ Successful	ROOT_DSE was successfully reached
□	Kerberos test obtaining join point TGT	cisco.com	✓ Successful	TGT was obtained successfully
□	LDAP test - DC locator	cisco.com	✓ Successful	DCs availability test was successful List of RPC/LDAP a...

- The DNS SRV errors can actually mean something else
- The response was too big
- And retried with TCP
- A sniffer can confirm
- Sites or DNS configuration changes are required to get that optimized

Debug Log

Elevate to DEBUG log level (TRACE is overkill)



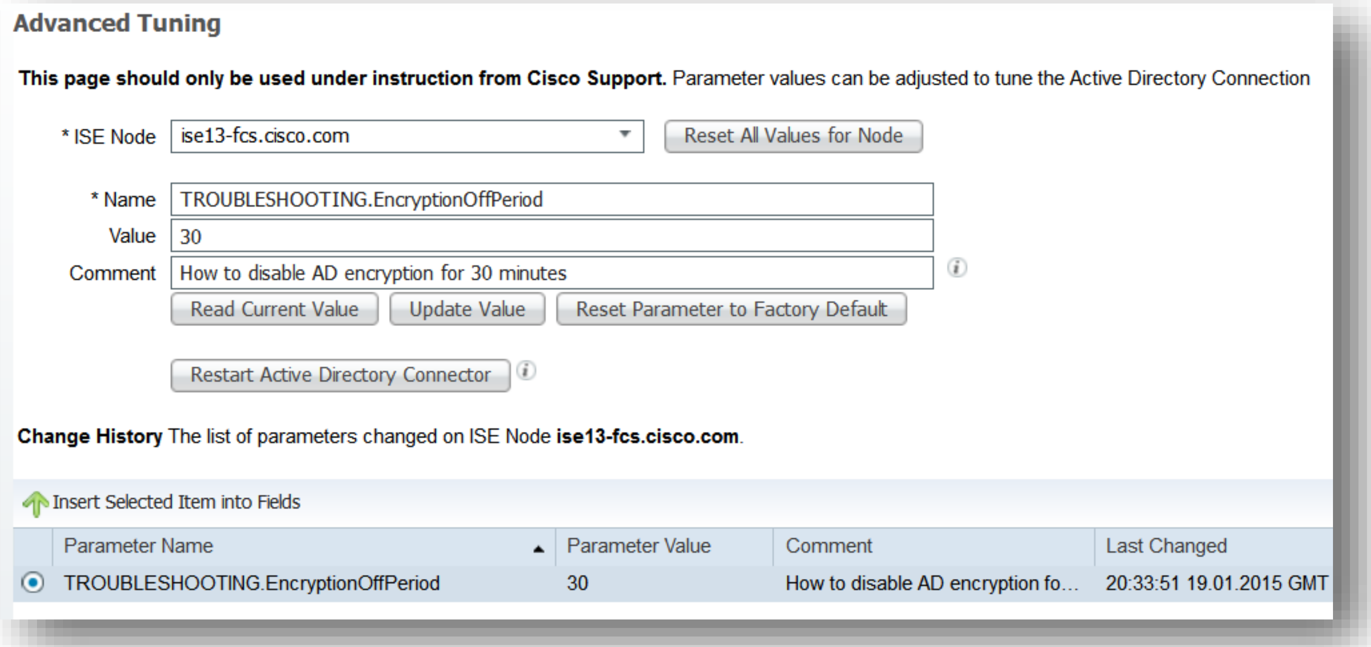
Node List > ise13-fcs.cisco.com

Debug Level Configuration

	Component Name	Log Level
○	accessfilter	INFO
●	Active Directory	DEBUG
○	admin-ca	INFO
○	admin-infra	INFO

Getting captures – use Advanced Tuning

This will disable AD encryption temporarily



Reset All Values for Node
Read Current Value
Update Value
Reset Parameter to Factory Default
Restart Active Directory Connector
Insert Selected Item into Fields

Advanced Tuning

This page should only be used under instruction from Cisco Support. Parameter values can be adjusted to tune the Active Directory Connection

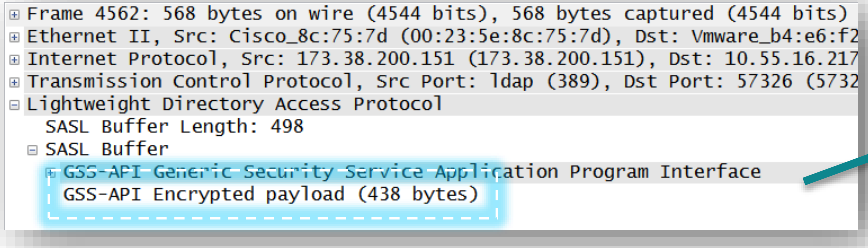
* ISE Node	ise13-fcs.cisco.com
* Name	TROUBLESHOOTING.EncryptionOffPeriod
Value	30
Comment	How to disable AD encryption for 30 minutes

Change History The list of parameters changed on ISE Node **ise13-fcs.cisco.com**.

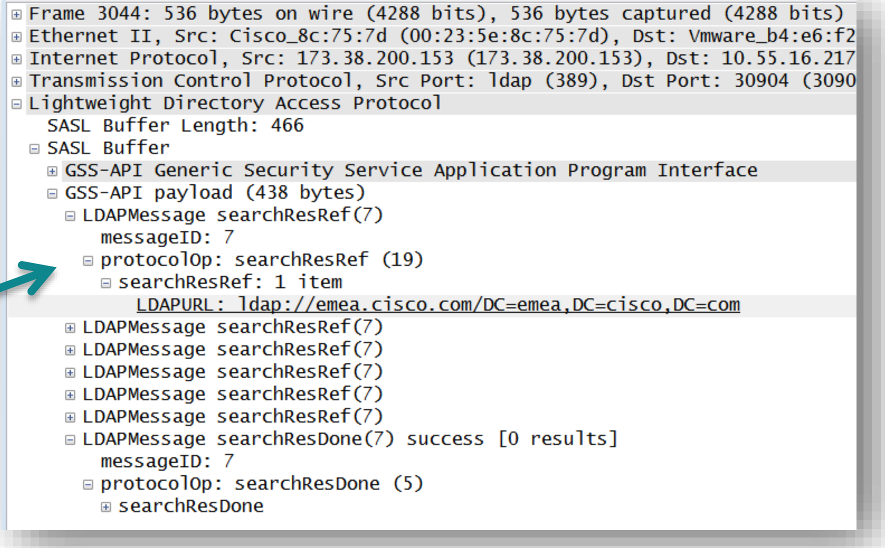
	Parameter Name	Parameter Value	Comment	Last Changed
●	TROUBLESHOOTING.EncryptionOffPeriod	30	How to disable AD encryption fo...	20:33:51 19.01.2015 GMT

Example of disabled encryption

Disabling encryption renders packet captures of AD traffic much more useful.



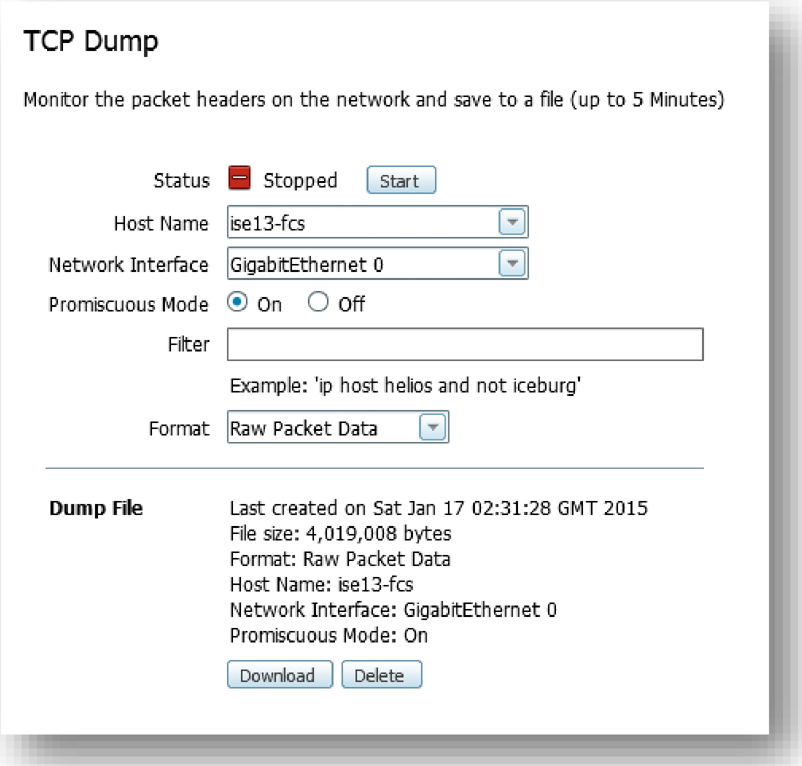
```
⊞ Frame 4562: 568 bytes on wire (4544 bits), 568 bytes captured (4544 bits)
⊞ Ethernet II, Src: Cisco_8c:75:7d (00:23:5e:8c:75:7d), Dst: Vmware_b4:e6:f2
⊞ Internet Protocol, Src: 173.38.200.151 (173.38.200.151), Dst: 10.55.16.217
⊞ Transmission Control Protocol, Src Port: ldap (389), Dst Port: 57326 (5732
⊟ Lightweight Directory Access Protocol
    SASL Buffer Length: 498
  ⊟ SASL Buffer
    ⊞ GSS-API Generic Security Service Application Program Interface
      GSS-API Encrypted payload (438 bytes)
```



```
⊞ Frame 3044: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits)
⊞ Ethernet II, Src: Cisco_8c:75:7d (00:23:5e:8c:75:7d), Dst: Vmware_b4:e6:f2
⊞ Internet Protocol, Src: 173.38.200.153 (173.38.200.153), Dst: 10.55.16.217
⊞ Transmission Control Protocol, Src Port: ldap (389), Dst Port: 30904 (3090
⊟ Lightweight Directory Access Protocol
    SASL Buffer Length: 466
  ⊟ SASL Buffer
    ⊞ GSS-API Generic Security Service Application Program Interface
    ⊟ GSS-API payload (438 bytes)
      ⊟ LDAPMessage searchResRef(7)
          messageID: 7
        ⊟ protocolOp: searchResRef (19)
          ⊟ searchResRef: 1 item
              LDAPURL: ldap://emea.cisco.com/DC=emea,DC=cisco,DC=com
      ⊞ LDAPMessage searchResRef(7)
      ⊞ LDAPMessage searchResRef(7)
      ⊞ LDAPMessage searchResRef(7)
      ⊞ LDAPMessage searchResRef(7)
      ⊞ LDAPMessage searchResRef(7)
      ⊟ LDAPMessage searchResDone(7) success [0 results]
          messageID: 7
        ⊟ protocolOp: searchResDone (5)
          ⊞ searchResDone
```

You can then use ISE TCP Dump

- Filters
  - IP of DC/ISE
- Important protocols
  - LDAP, CLDAP
  - Kerberos
  - MS-RPC
  - DNS



TCP Dump

Monitor the packet headers on the network and save to a file (up to 5 Minutes)

Status	🟥 Stopped Start
Host Name	ise13-fcs
Network Interface	GigabitEthernet 0
Promiscuous Mode	● On ○ Off
Filter	
	Example: 'ip host helios and not iceburg'
Format	Raw Packet Data

Dump File

Last created on Sat Jan 17 02:31:28 GMT 2015
File size: 4,019,008 bytes
Format: Raw Packet Data
Host Name: ise13-fcs
Network Interface: GigabitEthernet 0
Promiscuous Mode: On

Look for big DNS and LDAP time deltas

- Wireshark can show these by adding a column called dns.time and ldap.time
- You can do filters like “dns.time > 0.5” (seconds) to home in on slow packets
- Can really speed up finding slow DNS or LDAP responses

Beware ‘hardening’

- AD ‘SMB hardening’
- AD ‘Extended Protection’
- Disabling SMB / MSCHAP
- Firewalling MS-RPC
- Security patches
- These can block some features required by the connector

- These ports must be open
  - DNS TCP/UDP 53
  - MSRPC 445
  - Kerberos TCP/UDP 88
  - LDAP TCP/UDP 389
  - LDAP TCP/UDP 3268 (GC)
  - NTP 123

Beware Hypervisors

- Don’t pause VMs for long
  - Clock and replication problems
- Careful with your cloning
- Watch their clocks
- And other resources

Attribute indexing

- How to check an attribute is indexed
  - http://msdn.microsoft.com/en-us/library/ms675095%28v=vs.85%29.aspx
- Consider indexing them if that attribute must be used
  - http://technet.microsoft.com/en-gb/library/aa995762%28v=exchg.65%29.aspx

Verify your SRV records

- To use Nslookup to verify the SRV records, follow these steps: On your DNS, click **Start**, and then click **Run**.
  - In the **Open** box, type cmd.
  - Type nslookup, and then press ENTER.
  - Type set type=all, and then press ENTER.
  - Type _ldap._tcp.dc._msdcs.Domain_Name, where Domain_Name is the name of your domain, and then press ENTER.
- This will show DCs for your domain. You can also query for gc and kdc.
- Note if ISE is in a Site (and it should be) the query should be changed to query for your Site's records
  - Syntax: _ldap._tcp.***Site_Name***._sites.dc._msdcs.Domain_Name

nslookup SRV example output

```
C:\nslookup
Default Server: dc1.example.microsoft.com
Address: 10.0.0.14
set type=srv
_ldap._tcp.dc._msdcs.example.microsoft.com
Server: dc1.example.microsoft.com
Address: 10.0.0.14
_ldap._tcp.dc._msdcs.example.microsoft.com SRV service location: priority = 0
weight = 0 port = 389 svr hostname = dc1.example.microsoft.com
_ldap._tcp.dc._msdcs.example.microsoft.com SRV service location: priority = 0
weight = 0 port = 389 svr hostname = dc2.example.microsoft.com
dc1.example.microsoft.com internet address = 10.0.0.14
dc2.example.microsoft.com internet address = 10.0.0.15
```

Thank you