You make **possible**

ISE under magnifying glass. How to troubleshoot ISE

Serhii Kucherenko, CX CSE, CCIE #35182
Eugene Korneychuk, CX TL, CCIE #43253

BRKSEC-3229

Barcelona | January 27-31, 2020

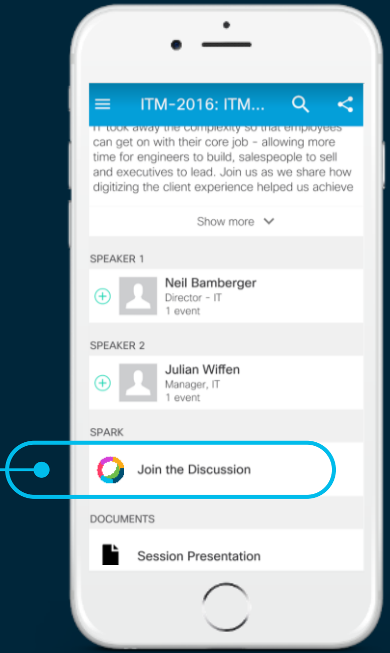
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat
with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



ITM-2016: ITM...

IT took away the complexity so that employees can get on with their core job - allowing more time for engineers to build, salespeople to sell and executives to lead. Join us as we share how digitizing the client experience helped us achieve

Show more

SPEAKER 1

Neil Bamberger
Director - IT
1 event

SPEAKER 2

Julian Wiffen
Manager, IT
1 event

SPARK

Join the Discussion

DOCUMENTS

Session Presentation

cs.co/ciscolivebot#BRKSEC-3229

Welcome to the mystery world of ISE troubleshooting

- Stay tuned for next 2 hours with CX AAA engineers from Krakow

Eugene Korneychuk
Technical Leader
AAA Team Krakow
8 years in TAC
14 years in Networking

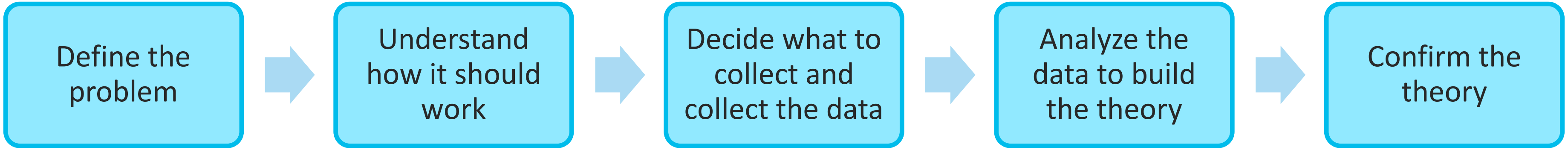
Serhii Kucherenko
Customer Support Engineer
AAA Team Krakow
5 years in TAC
13 years in Networking

Warning!
Slavic Accent Ahead

What do you imagine might be the most essential element in successful troubleshooting?

A structured approach, which is similar to a deductive method, is one of the key elements in successful troubleshooting

Troubleshooting Methodology



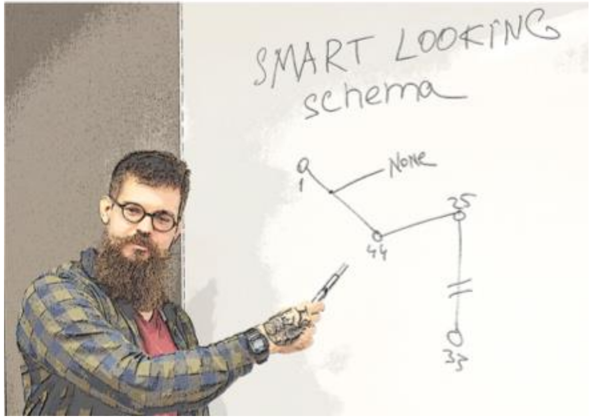
Define the problem

Understand how it should work

Decide what to collect and collect the data

Analyze the data to build the theory

Confirm the theory



Sessions Objectives

Session will cover:

- Theory on ISE and 802.1x operations
- Authentication, Profiling and Posture Troubleshooting
- Troubleshooting Methodology

Session will not cover:

- Marketing
- Roadmaps
- All possible ISE features

We want you to learn

And have fun

Icons Used Throughout the Presentation

For your reference

- For Your Reference – These items will usually NOT be covered in detail during the session

- Content enlarging – when something is not visible good enough we highlight and enlarge this area.

1

- GUI navigation assistant – This special type of highlighting is used to help you in navigation in the Graphical User Interface of a product.

- Hidden Content – slides which won't be presented during the session. Primarily those slides are here to give you more detailed information.

Agenda

- Introduction to DEMO
- Learn by example - Profiling and Authentication Troubleshooting
- Posture Overview
- 5 common ISE Posture misconceptions
- Learn by example - Posture Troubleshooting

Agenda

- Introduction to DEMO
- Learn by example - Profiling and Authentication Troubleshooting
- Posture Overview
- 5 common ISE Posture misconceptions
- Learn by example - Posture Troubleshooting

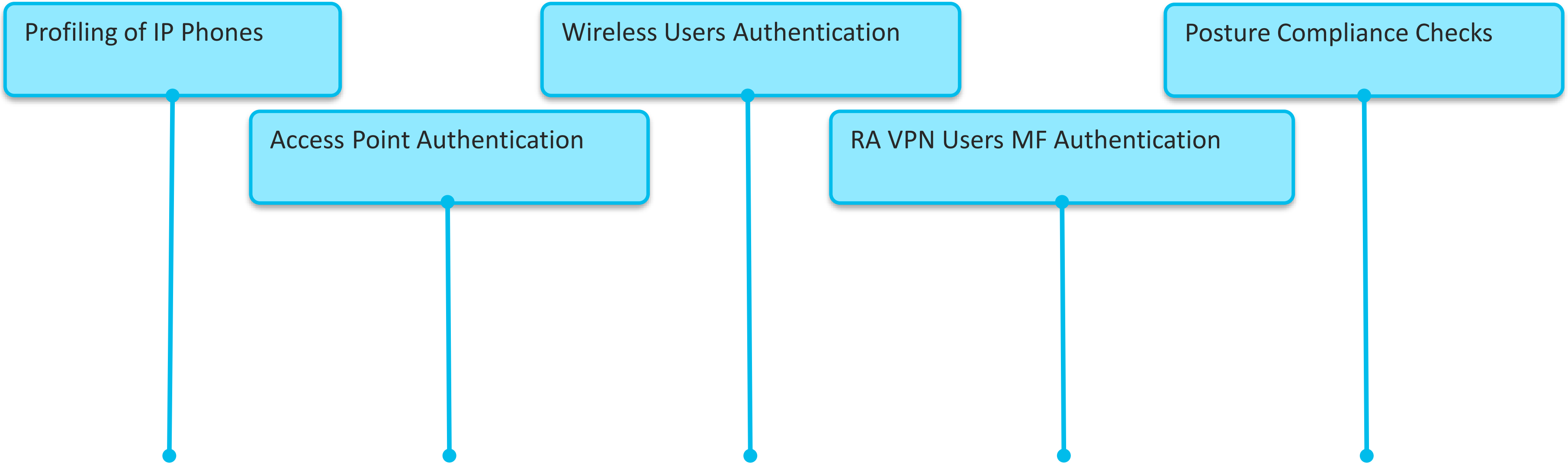
Based on a true story

Introduction to DEMO

- DEMO is a huge IT company with offices all around the globe and head office in Barcelona.
- Network security is one of the major concerns for DEMO top management.
- Identity networking is implemented based on Cisco ISE, DEMO started from ISE 1.2, currently deployment is on 2.4 Patch 9.

- ISE Distributed Deployment of 2 Nodes is deployed in Barcelona headquarters. Both nodes are having Administration, Monitoring and Policy Service Personas and back up each other for every function.

How ISE is used in DEMO



Profiling of IP Phones

Access Point Authentication

Wireless Users Authentication

RA VPN Users MF Authentication

Posture Compliance Checks

A Very Important Meeting

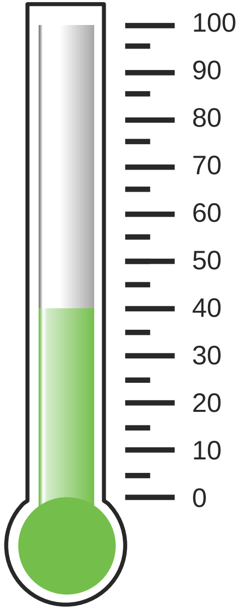
On Monday very important business meeting supposed to take place…

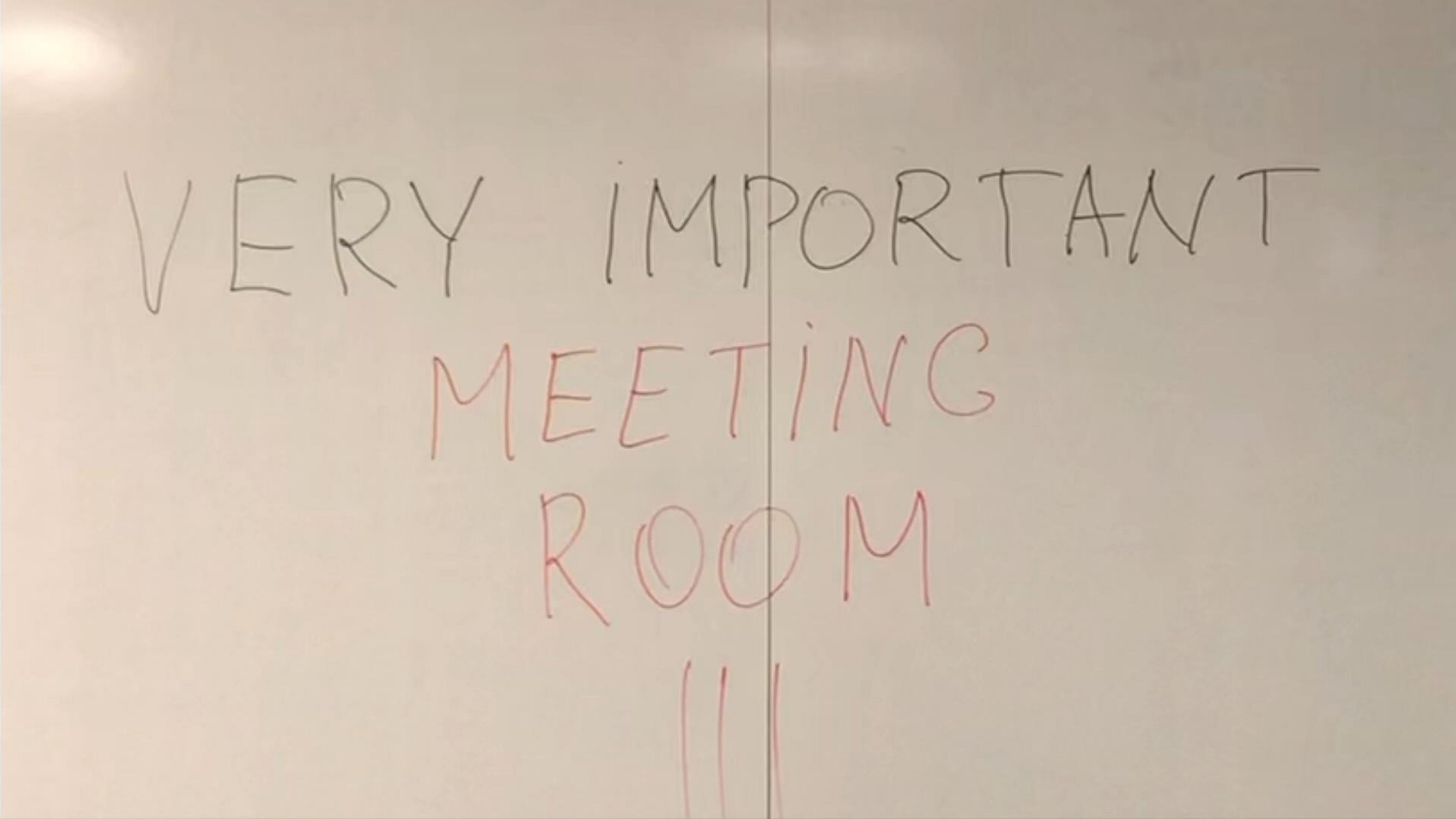
Agenda

- Introduction to DEMO
- Learn by example - Profiling and Authentication Troubleshooting
- Posture Overview
- 5 common ISE Posture misconceptions
- Learn by example - Posture Troubleshooting

Issue 1

Meeting's success scale





VERY IMPORTANT

MEETING

ROOM

!!!

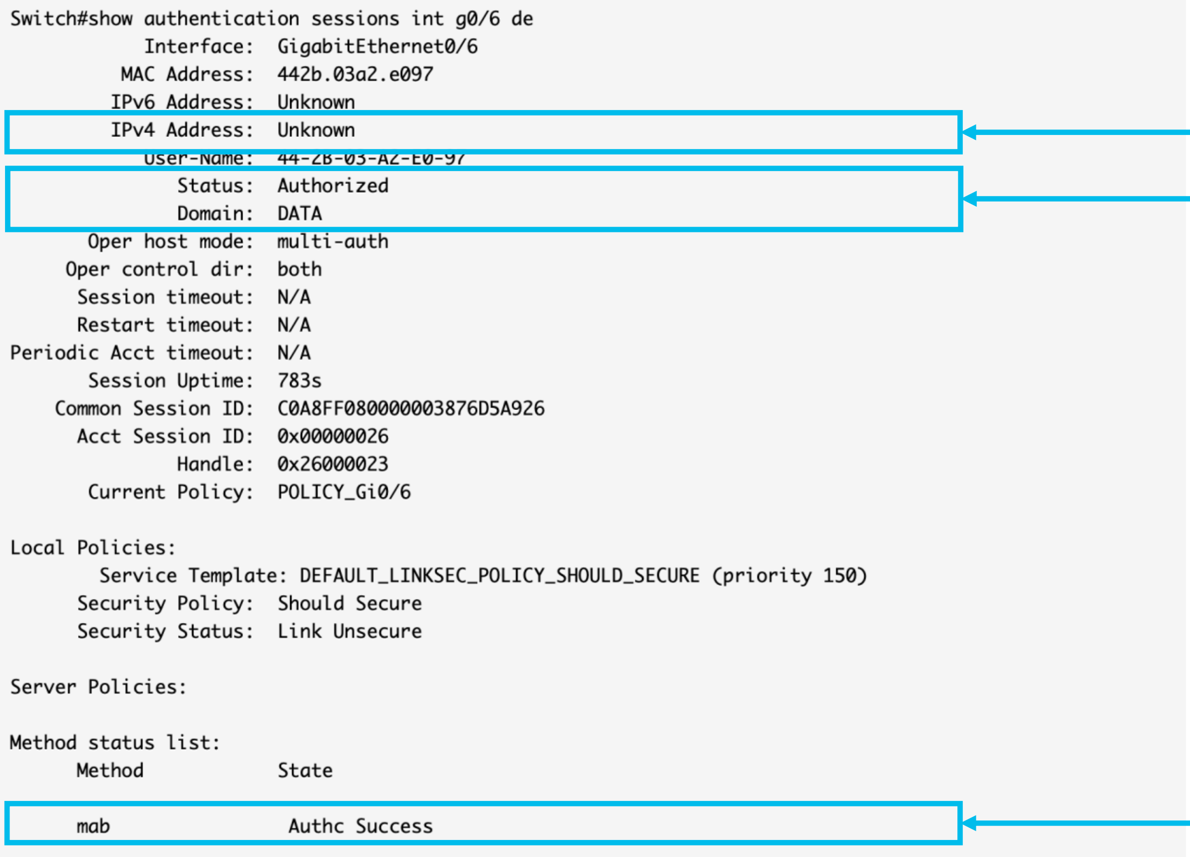
Define the problem – issue 1

IP Phone is stuck in “Phone not registered”

Supporting facts

- Only conference room phone is affected
- Problem is always reproducible
- Switching it off and on, disconnecting/connecting cables didn’t help
- No changes over the weekend

Switch > show authentication session



```
Switch#show authentication sessions int g0/6 de
            Interface:  GigabitEthernet0/6
          MAC Address:  442b.03a2.e097
         IPv6 Address:  Unknown
         IPv4 Address:  Unknown
            User-Name:  44-2B-03-A2-E0-97
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
Periodic Acct timeout:  N/A
       Session Uptime:  783s
    Common Session ID:  C0A8FF080000003876D5A926
      Acct Session ID:  0x00000026
               Handle:  0x26000023
       Current Policy:  POLICY_Gi0/6

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
      Security Policy:  Should Secure
      Security Status:  Link Unsecure

Server Policies:

Method status list:
      Method            State

      mab                Authc Success
```

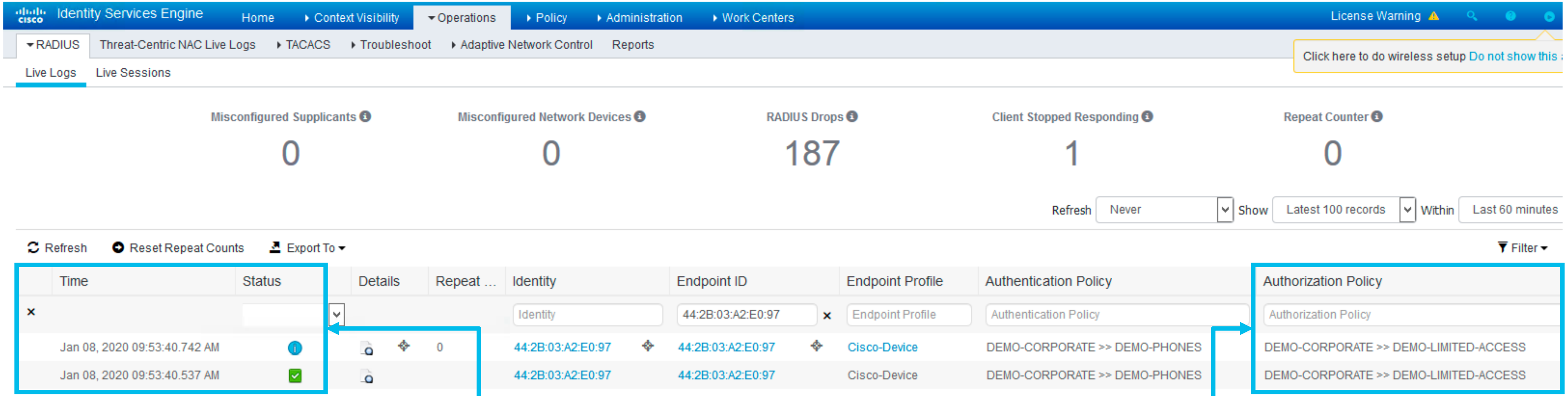
IPv4 Address is missing

Authorization is successful

Phone is stuck in the DATA domain

Authentication is successful

Operations > Radius > Live Logs



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	187	1	0

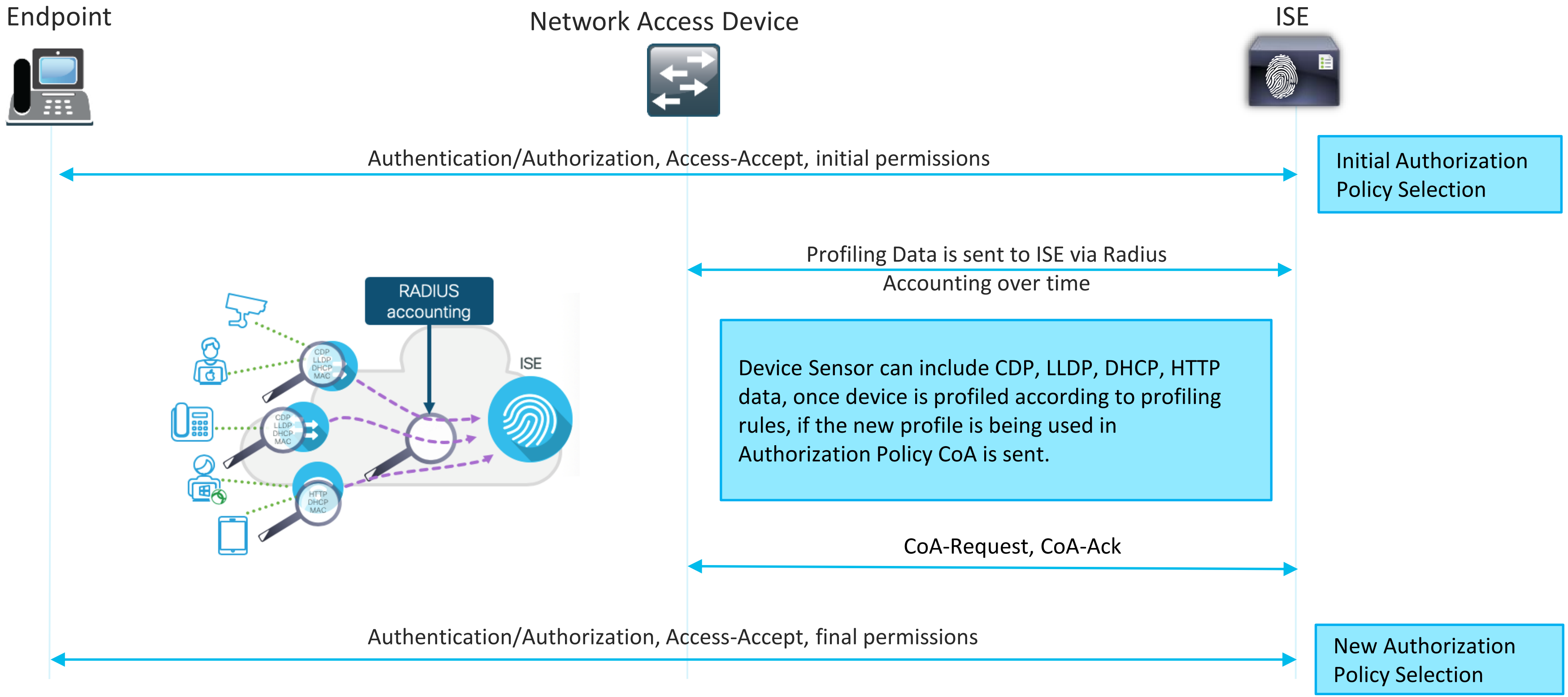
Refresh: Never Show: Latest 100 records Within: Last 60 minutes

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy
×				Identity	44:2B:03:A2:E0:97 ×	Endpoint Profile	Authentication Policy	Authorization Policy
Jan 08, 2020 09:53:40.742 AM	ℹ	🔍 ✥	0	44:2B:03:A2:E0:97 ✥	44:2B:03:A2:E0:97 ✥	Cisco-Device	DEMO-CORPORATE >> DEMO-PHONES	DEMO-CORPORATE >> DEMO-LIMITED-ACCESS
Jan 08, 2020 09:53:40.537 AM	✓	🔍		44:2B:03:A2:E0:97	44:2B:03:A2:E0:97	Cisco-Device	DEMO-CORPORATE >> DEMO-PHONES	DEMO-CORPORATE >> DEMO-LIMITED-ACCESS

Successfully processed Authentication and Authorization, Access-Accept is sent

DEMO-LIMITED-ACCESS Authorization policy is matched

Profiling high level overview with Device Sensor



Endpoint

Network Access Device

ISE

Authentication/Authorization, Access-Accept, initial permissions

Initial Authorization Policy Selection

Profiling Data is sent to ISE via Radius Accounting over time

Device Sensor can include CDP, LLDP, DHCP, HTTP data, once device is profiled according to profiling rules, if the new profile is being used in Authorization Policy CoA is sent.

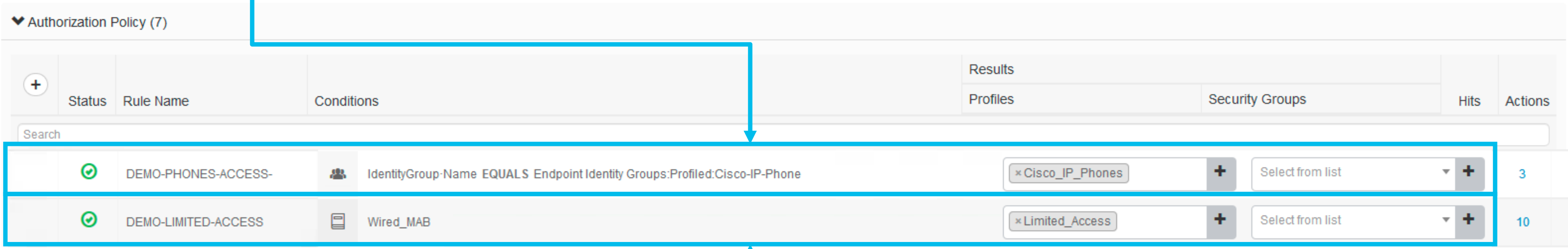
CoA-Request, CoA-Ack

Authentication/Authorization, Access-Accept, final permissions

New Authorization Policy Selection

How it should work. DEMO Profiling Flow

Final Policy DEMO-PHONES-ACCESS, once the device gets the right profile and placed in Cisco-IP-Phones Identity Group

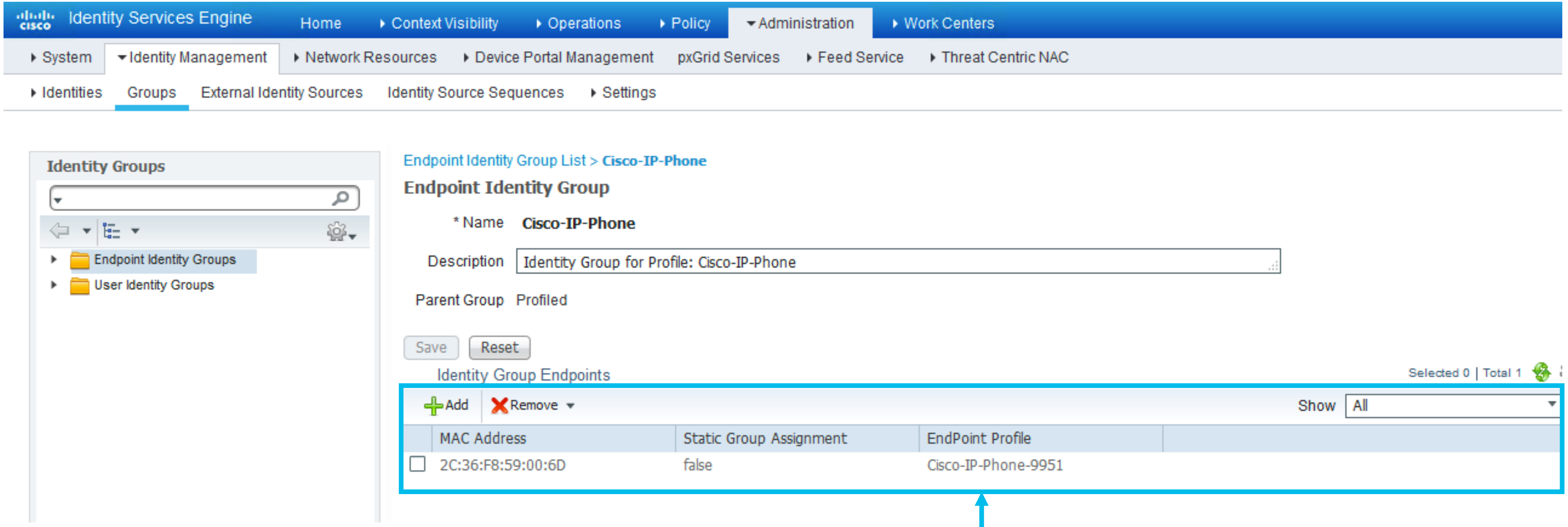


Authorization Policy (7)

+	Status	Rule Name	Conditions	Results Profiles	 Security Groups	Hits	Actions
	✓	DEMO-PHONES-ACCESS-	IdentityGroup·Name EQUALS Endpoint Identity Groups:Profiled:Cisco-IP-Phone	× Cisco_IP_Phones	Select from list	3	
	✓	DEMO-LIMITED-ACCESS	Wired_MAB	× Limited_Access	Select from list	10	

Original Policy DEMO-LIMITED-ACCESS, before the device gets profiled

Administration > Identity Management > Groups



Endpoint Identity Group List > **Cisco-IP-Phone**

Endpoint Identity Group

* Name **Cisco-IP-Phone**

Description Identity Group for Profile: Cisco-IP-Phone

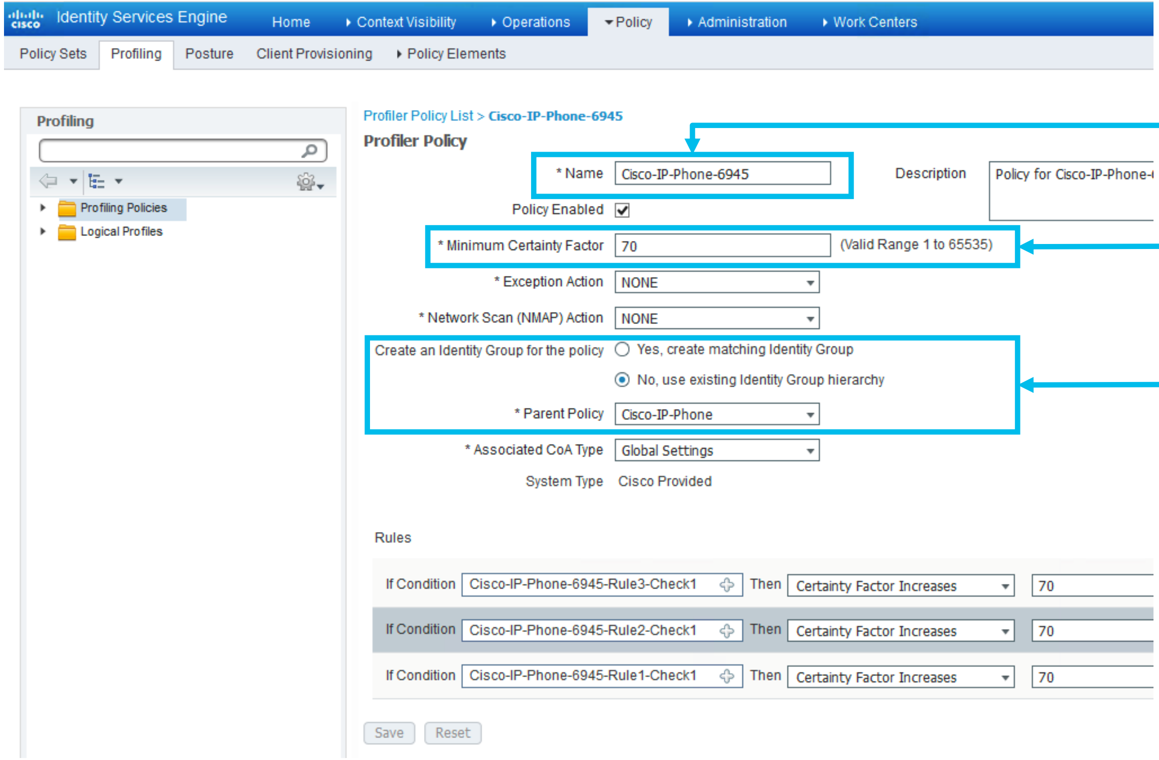
Parent Group Profiled

Identity Group Endpoints

	MAC Address	Static Group Assignment	EndPoint Profile
□	2C:36:F8:59:00:6D	false	Cisco-IP-Phone-9951

44:2B:03:A2:E0:97 is missing from the Cisco-IP-Phones Identity Group

Policy > Profiling



Profiler Policy List > **Cisco-IP-Phone-6945**

Profiler Policy

* Name	Cisco-IP-Phone-6945
Description	Policy for Cisco-IP-Phone-(
Policy Enabled	☑
* Minimum Certainty Factor	70 (Valid Range 1 to 65535)
* Exception Action	NONE
* Network Scan (NMAP) Action	NONE
Create an Identity Group for the policy	○ Yes, create matching Identity Group ● No, use existing Identity Group hierarchy
* Parent Policy	Cisco-IP-Phone
* Associated CoA Type	Global Settings
System Type	Cisco Provided

Rules

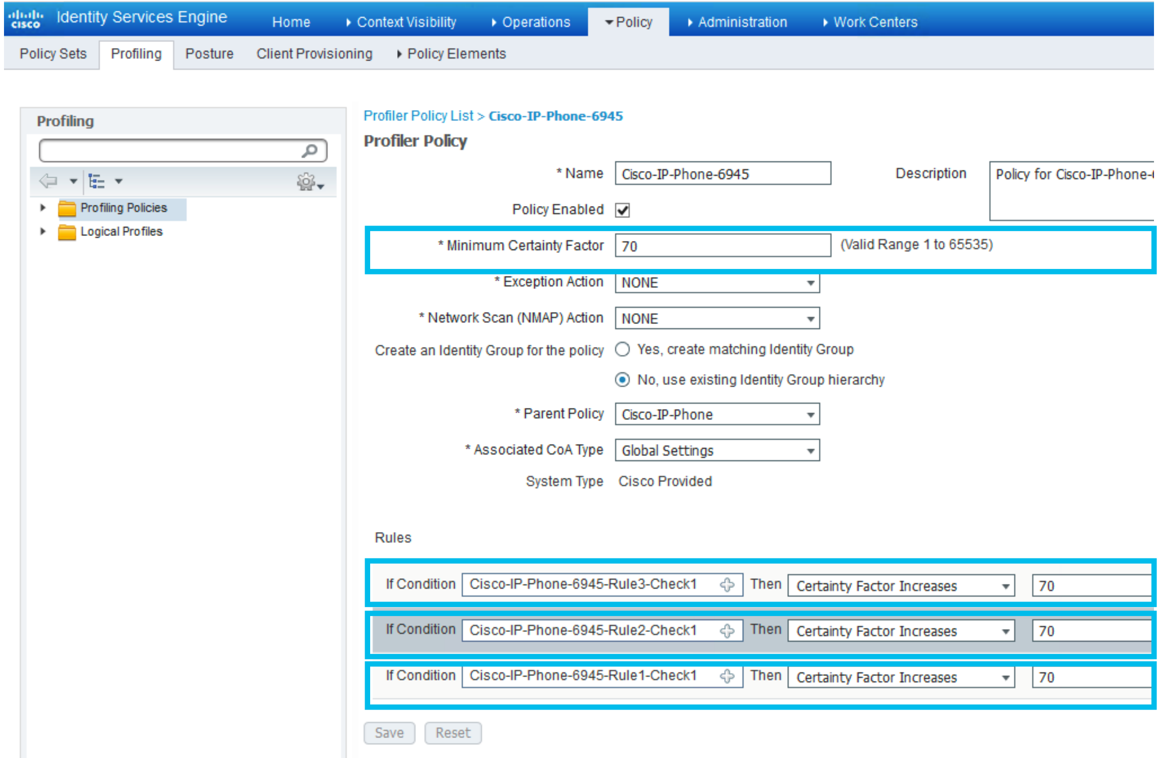
If Condition	Cisco-IP-Phone-6945-Rule3-Check1	Then	Certainty Factor Increases	70
If Condition	Cisco-IP-Phone-6945-Rule2-Check1	Then	Certainty Factor Increases	70
If Condition	Cisco-IP-Phone-6945-Rule1-Check1	Then	Certainty Factor Increases	70

Profile for Cisco-IP-Phones-6945

Minimum Certainty Factor instructs ISE when the device should be profiled

Identity Group will be reused from the Parent Policy - Cisco-IP-Phones

Policy > Profiling



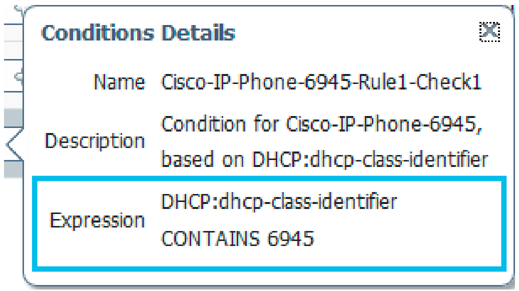
Profiler Policy List > **Cisco-IP-Phone-6945**

Profiler Policy

* Name	Cisco-IP-Phone-6945
Description	Policy for Cisco-IP-Phone-
Policy Enabled	☑
* Minimum Certainty Factor	70 (Valid Range 1 to 65535)
* Exception Action	NONE
* Network Scan (NMAP) Action	NONE
Create an Identity Group for the policy	○ Yes, create matching Identity Group ● No, use existing Identity Group hierarchy
* Parent Policy	Cisco-IP-Phone
* Associated CoA Type	Global Settings
System Type	Cisco Provided

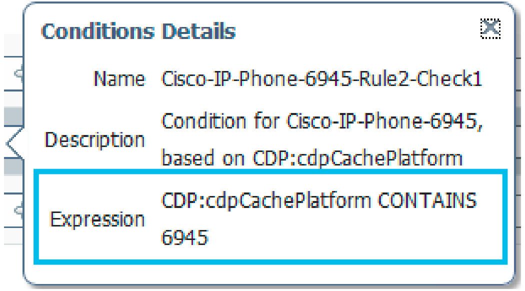
Rules

If Condition	Cisco-IP-Phone-6945-Rule3-Check1	Then	Certainty Factor Increases	70
If Condition	Cisco-IP-Phone-6945-Rule2-Check1	Then	Certainty Factor Increases	70
If Condition	Cisco-IP-Phone-6945-Rule1-Check1	Then	Certainty Factor Increases	70



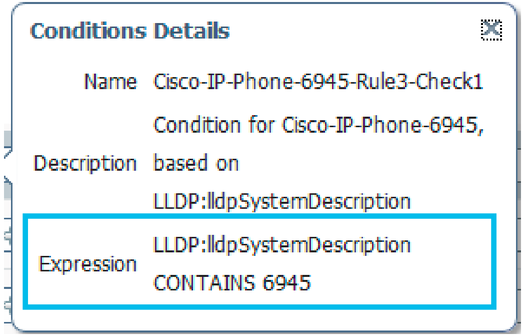
Conditions Details

Name	Cisco-IP-Phone-6945-Rule1-Check1
Description	Condition for Cisco-IP-Phone-6945, based on DHCP:dhcp-class-identifier
Expression	DHCP:dhcp-class-identifier CONTAINS 6945



Conditions Details

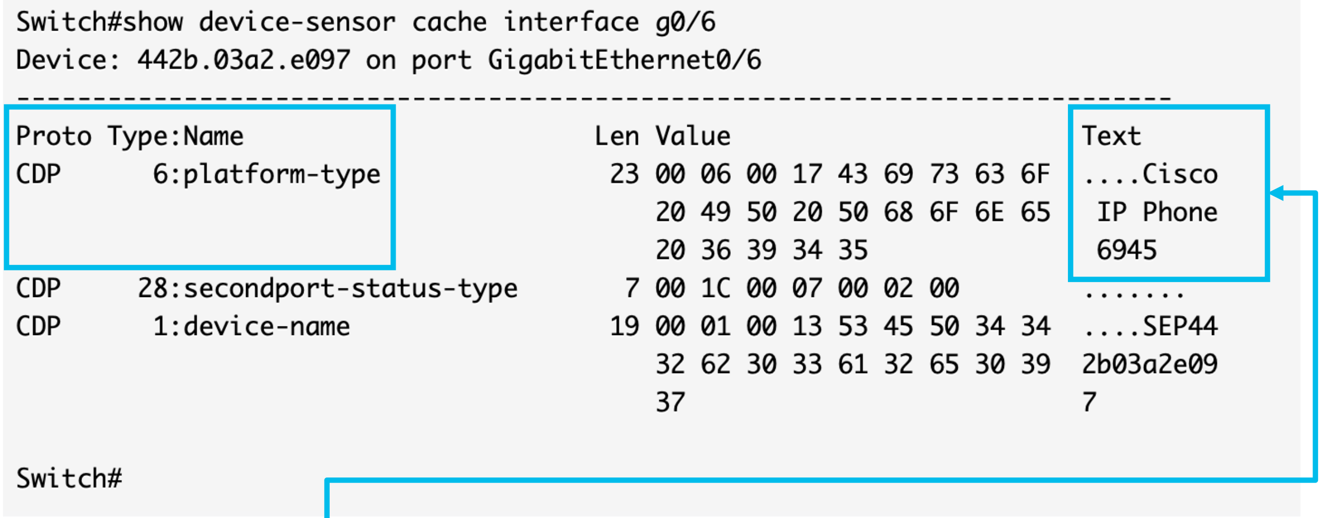
Name	Cisco-IP-Phone-6945-Rule2-Check1
Description	Condition for Cisco-IP-Phone-6945, based on CDP:cdpCachePlatform
Expression	CDP:cdpCachePlatform CONTAINS 6945



Conditions Details

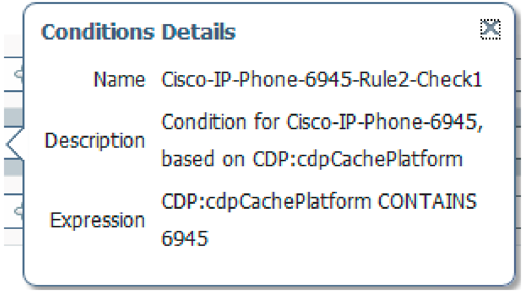
Name	Cisco-IP-Phone-6945-Rule3-Check1
Description	Condition for Cisco-IP-Phone-6945, based on LLDP:lldpSystemDescription
Expression	LLDP:lldpSystemDescription CONTAINS 6945

Device Sensor Cache verification on NAD



```
Switch#show device-sensor cache interface g0/6
Device: 442b.03a2.e097 on port GigabitEthernet0/6
----------------------------------------------------------------------------
Proto Type:Name                         Len Value                          Text
CDP       6:platform-type                23 00 06 00 17 43 69 73 63 6F     ....Cisco
                                            20 49 50 20 50 68 6F 6E 65      IP Phone
                                            20 36 39 34 35                  6945
CDP      28:secondport-status-type        7 00 1C 00 07 00 02 00           .......
CDP       1:device-name                  19 00 01 00 13 53 45 50 34 34     ....SEP44
                                            32 62 30 33 61 32 65 30 39     2b03a2e09
                                            37                             7

Switch#
```



Conditions Details

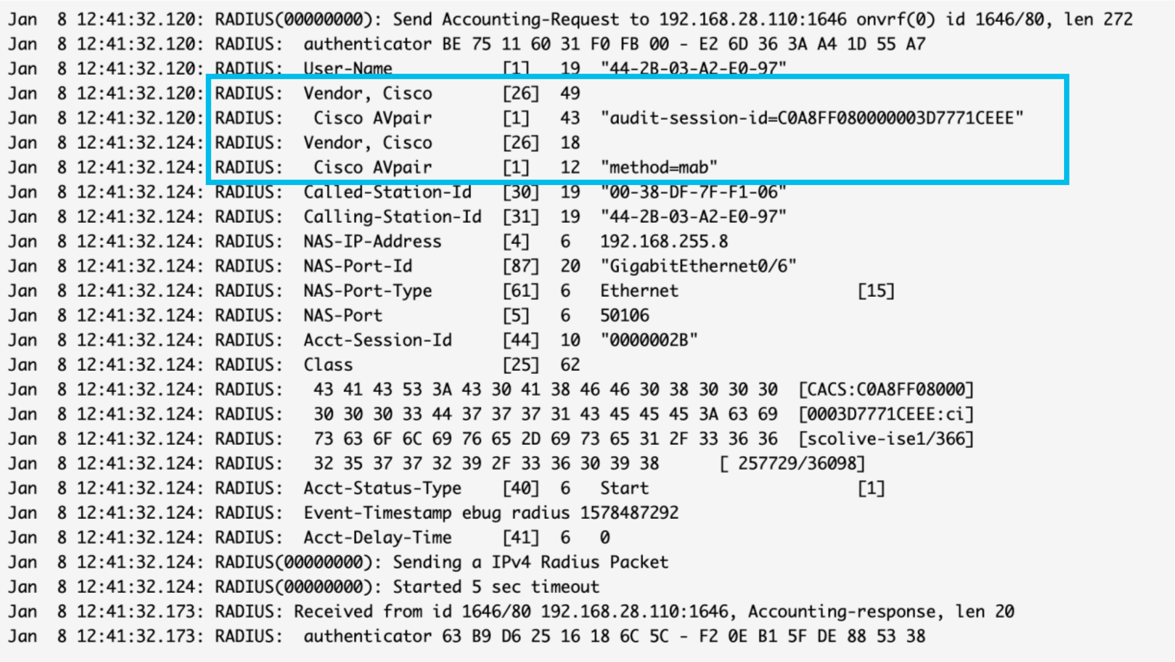
Name Cisco-IP-Phone-6945-Rule2-Check1

Description Condition for Cisco-IP-Phone-6945, based on CDP:cdpCachePlatform

Expression CDP:cdpCachePlatform CONTAINS 6945

CDP Platform Contains 6945 rule supposed to be matched

Verification of profiling data being sent. Switch



```
Jan  8 12:41:32.120: RADIUS(00000000): Send Accounting-Request to 192.168.28.110:1646 onvrf(0) id 1646/80, len 272
Jan  8 12:41:32.120: RADIUS:  authenticator BE 75 11 60 31 F0 FB 00 - E2 6D 36 3A A4 1D 55 A7
Jan  8 12:41:32.120: RADIUS:  User-Name           [1]   19  "44-2B-03-A2-E0-97"
Jan  8 12:41:32.120: RADIUS:  Vendor, Cisco       [26]  49
Jan  8 12:41:32.120: RADIUS:   Cisco AVpair       [1]   43  "audit-session-id=C0A8FF080000003D7771CEEE"
Jan  8 12:41:32.124: RADIUS:  Vendor, Cisco       [26]  18
Jan  8 12:41:32.124: RADIUS:   Cisco AVpair       [1]   12  "method=mab"
Jan  8 12:41:32.124: RADIUS:  Called-Station-Id   [30]  19  "00-38-DF-7F-F1-06"
Jan  8 12:41:32.124: RADIUS:  Calling-Station-Id  [31]  19  "44-2B-03-A2-E0-97"
Jan  8 12:41:32.124: RADIUS:  NAS-IP-Address      [4]   6   192.168.255.8
Jan  8 12:41:32.124: RADIUS:  NAS-Port-Id         [87]  20  "GigabitEthernet0/6"
Jan  8 12:41:32.124: RADIUS:  NAS-Port-Type       [61]  6   Ethernet                   [15]
Jan  8 12:41:32.124: RADIUS:  NAS-Port            [5]   6   50106
Jan  8 12:41:32.124: RADIUS:  Acct-Session-Id     [44]  10  "0000002B"
Jan  8 12:41:32.124: RADIUS:  Class               [25]  62
Jan  8 12:41:32.124: RADIUS:   43 41 43 53 3A 43 30 41 38 46 46 30 38 30 30 30  [CACS:C0A8FF08000]
Jan  8 12:41:32.124: RADIUS:   30 30 30 33 44 37 37 37 31 43 45 45 45 3A 63 69  [0003D7771CEEE:ci]
Jan  8 12:41:32.124: RADIUS:   73 63 6F 6C 69 76 65 2D 69 73 65 31 2F 33 36 36  [scolive-ise1/366]
Jan  8 12:41:32.124: RADIUS:   32 35 37 37 32 39 2F 33 36 30 39 38        [ 257729/36098]
Jan  8 12:41:32.124: RADIUS:  Acct-Status-Type    [40]  6   Start                      [1]
Jan  8 12:41:32.124: RADIUS:  Event-Timestamp ebug radius 1578487292
Jan  8 12:41:32.124: RADIUS:  Acct-Delay-Time     [41]  6   0
Jan  8 12:41:32.124: RADIUS(00000000): Sending a IPv4 Radius Packet
Jan  8 12:41:32.124: RADIUS(00000000): Started 5 sec timeout
Jan  8 12:41:32.173: RADIUS: Received from id 1646/80 192.168.28.110:1646, Accounting-response, len 20
Jan  8 12:41:32.173: RADIUS:  authenticator 63 B9 D6 25 16 18 6C 5C - F2 0E B1 5F DE 88 53 38
```

CDP attributes are missing in the Accounting-Request

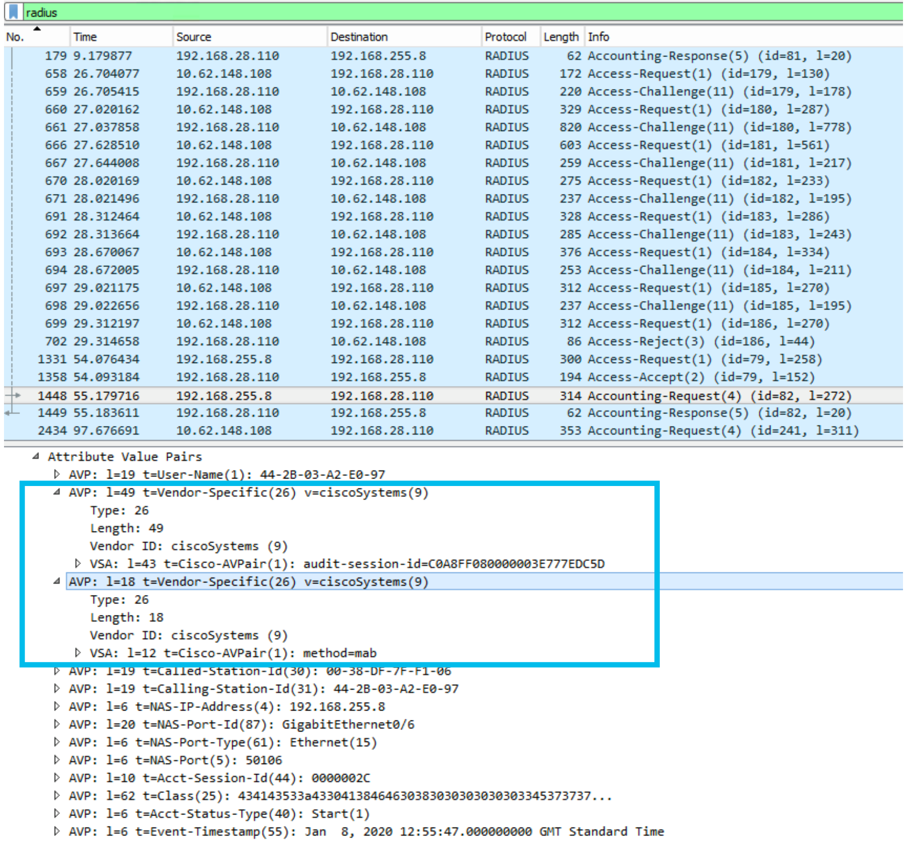
Pre 16.x

debug radius
--- followed by ---
show logging

Post 16.11

debug radius
--- followed by ---
show logging process smd internal

Verification of profiling data being sent. Network

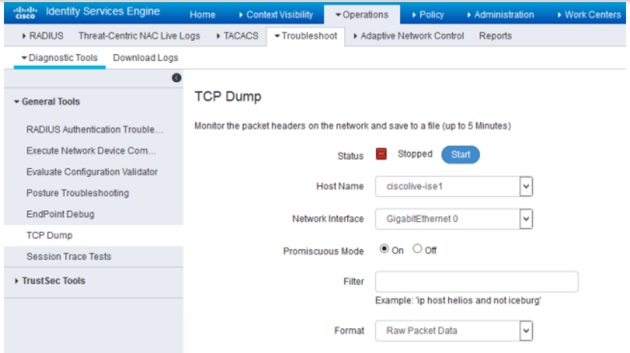


```
radius
No.     Time        Source           Destination      Protocol Length Info
   179 9.179877    192.168.28.110   192.168.255.8    RADIUS     62 Accounting-Response(5) (id=81, l=20)
   658 26.704077   10.62.148.108    192.168.28.110   RADIUS    172 Access-Request(1) (id=179, l=130)
   659 26.705415   192.168.28.110   10.62.148.108    RADIUS    220 Access-Challenge(11) (id=179, l=178)
   660 27.020162   10.62.148.108    192.168.28.110   RADIUS    329 Access-Request(1) (id=180, l=287)
   661 27.037858   192.168.28.110   10.62.148.108    RADIUS    820 Access-Challenge(11) (id=180, l=778)
   666 27.628510   10.62.148.108    192.168.28.110   RADIUS    603 Access-Request(1) (id=181, l=561)
   667 27.644008   192.168.28.110   10.62.148.108    RADIUS    259 Access-Challenge(11) (id=181, l=217)
   670 28.020169   10.62.148.108    192.168.28.110   RADIUS    275 Access-Request(1) (id=182, l=233)
   671 28.021496   192.168.28.110   10.62.148.108    RADIUS    237 Access-Challenge(11) (id=182, l=195)
   691 28.312464   10.62.148.108    192.168.28.110   RADIUS    328 Access-Request(1) (id=183, l=286)
   692 28.313664   192.168.28.110   10.62.148.108    RADIUS    285 Access-Challenge(11) (id=183, l=243)
   693 28.670067   10.62.148.108    192.168.28.110   RADIUS    376 Access-Request(1) (id=184, l=334)
   694 28.672005   192.168.28.110   10.62.148.108    RADIUS    253 Access-Challenge(11) (id=184, l=211)
   697 29.021175   10.62.148.108    192.168.28.110   RADIUS    312 Access-Request(1) (id=185, l=270)
   698 29.022656   192.168.28.110   10.62.148.108    RADIUS    237 Access-Challenge(11) (id=185, l=195)
   699 29.312197   10.62.148.108    192.168.28.110   RADIUS    312 Access-Request(1) (id=186, l=270)
   702 29.314658   192.168.28.110   10.62.148.108    RADIUS     86 Access-Reject(3) (id=186, l=44)
  1331 54.076434   192.168.255.8    192.168.28.110   RADIUS    300 Access-Request(1) (id=79, l=258)
  1358 54.093184   192.168.28.110   192.168.255.8    RADIUS    194 Access-Accept(2) (id=79, l=152)
  1448 55.179716   192.168.255.8    192.168.28.110   RADIUS    314 Accounting-Request(4) (id=82, l=272)
  1449 55.183611   192.168.28.110   192.168.255.8    RADIUS     62 Accounting-Response(5) (id=82, l=20)
  2434 97.676691   10.62.148.108    192.168.28.110   RADIUS    353 Accounting-Request(4) (id=241, l=311)
```

```
◢ Attribute Value Pairs
   ▷ AVP: l=19 t=User-Name(1): 44-2B-03-A2-E0-97
   ◢ AVP: l=49 t=Vendor-Specific(26) v=ciscoSystems(9)
        Type: 26
        Length: 49
        Vendor ID: ciscoSystems (9)
      ▷ VSA: l=43 t=Cisco-AVPair(1): audit-session-id=C0A8FF080000003E777EDC5D
   ◢ AVP: l=18 t=Vendor-Specific(26) v=ciscoSystems(9)
        Type: 26
        Length: 18
        Vendor ID: ciscoSystems (9)
      ▷ VSA: l=12 t=Cisco-AVPair(1): method=mab
   ▷ AVP: l=19 t=Called-Station-Id(30): 00-38-DF-7F-F1-06
   ▷ AVP: l=19 t=Calling-Station-Id(31): 44-2B-03-A2-E0-97
   ▷ AVP: l=6 t=NAS-IP-Address(4): 192.168.255.8
   ▷ AVP: l=20 t=NAS-Port-Id(87): GigabitEthernet0/6
   ▷ AVP: l=6 t=NAS-Port-Type(61): Ethernet(15)
   ▷ AVP: l=6 t=NAS-Port(5): 50106
   ▷ AVP: l=10 t=Acct-Session-Id(44): 0000002C
   ▷ AVP: l=62 t=Class(25): 434143533a4330413846463038303030303030303345373737...
   ▷ AVP: l=6 t=Acct-Status-Type(40): Start(1)
   ▷ AVP: l=6 t=Event-Timestamp(55): Jan  8, 2020 12:55:47.000000000 GMT Standard Time
```

CDP attributes are missing in the Accounting-Request, AVP pairs containing CDP data are not there

Operations > Troubleshoot > Diagnostic Tools



TCP Dump

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

Status: Stopped

Host Name: ciscolive-ise1

Network Interface: GigabitEthernet 0

Promiscuous Mode: ● On ○ Off

Filter:

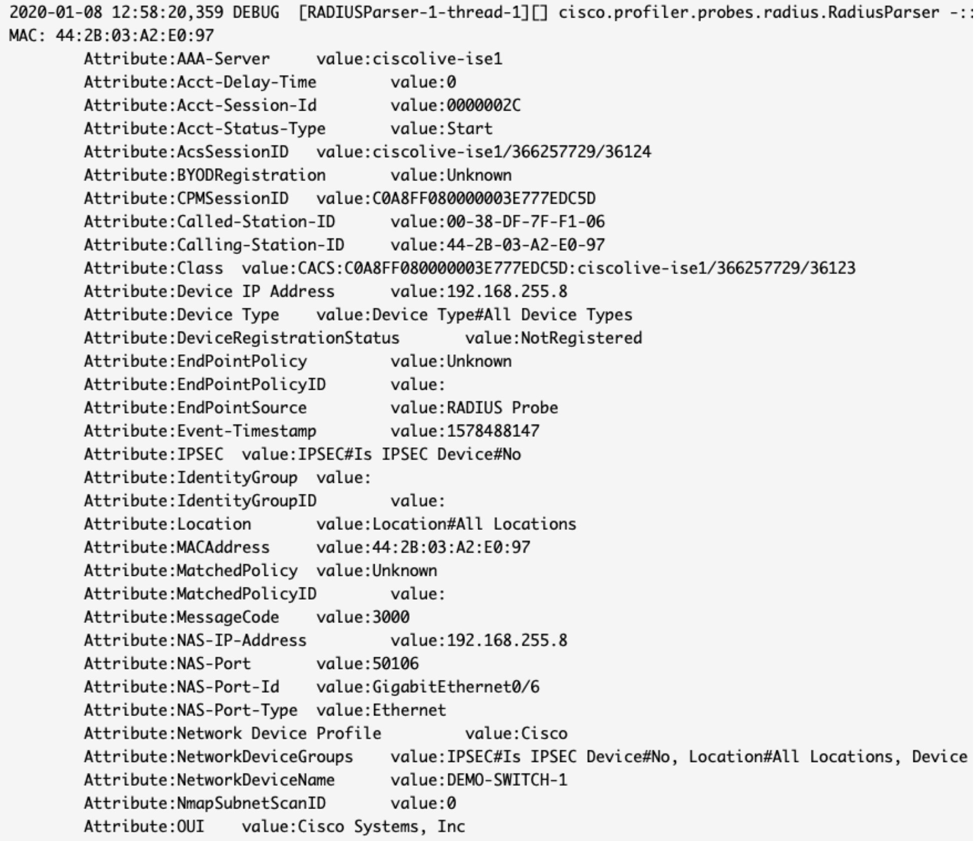
Example: 'ip host helios and not iceburg'

Format: Raw Packet Data

SPAN, EPC (Embedded Packet Capture)

cisco Live!

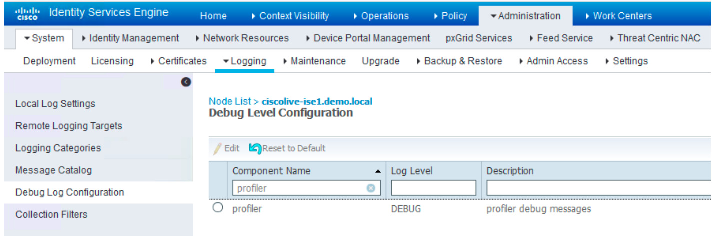
Verification of profiling data being sent. ISE



```
2020-01-08 12:58:20,359 DEBUG  [RADIUSParser-1-thread-1][] cisco.profiler.probes.radius.RadiusParser -::
MAC: 44:2B:03:A2:E0:97
        Attribute:AAA-Server     value:ciscolive-ise1
        Attribute:Acct-Delay-Time        value:0
        Attribute:Acct-Session-Id        value:0000002C
        Attribute:Acct-Status-Type       value:Start
        Attribute:AcsSessionID   value:ciscolive-ise1/366257729/36124
        Attribute:BYODRegistration       value:Unknown
        Attribute:CPMSessionID   value:C0A8FF080000003E777EDC5D
        Attribute:Called-Station-ID      value:00-38-DF-7F-F1-06
        Attribute:Calling-Station-ID     value:44-2B-03-A2-E0-97
        Attribute:Class  value:CACS:C0A8FF080000003E777EDC5D:ciscolive-ise1/366257729/36123
        Attribute:Device IP Address      value:192.168.255.8
        Attribute:Device Type    value:Device Type#All Device Types
        Attribute:DeviceRegistrationStatus       value:NotRegistered
        Attribute:EndPointPolicy         value:Unknown
        Attribute:EndPointPolicyID       value:
        Attribute:EndPointSource         value:RADIUS Probe
        Attribute:Event-Timestamp        value:1578488147
        Attribute:IPSEC  value:IPSEC#Is IPSEC Device#No
        Attribute:IdentityGroup  value:
        Attribute:IdentityGroupID        value:
        Attribute:Location       value:Location#All Locations
        Attribute:MACAddress     value:44:2B:03:A2:E0:97
        Attribute:MatchedPolicy  value:Unknown
        Attribute:MatchedPolicyID        value:
        Attribute:MessageCode    value:3000
        Attribute:NAS-IP-Address         value:192.168.255.8
        Attribute:NAS-Port       value:50106
        Attribute:NAS-Port-Id    value:GigabitEthernet0/6
        Attribute:NAS-Port-Type  value:Ethernet
        Attribute:Network Device Profile         value:Cisco
        Attribute:NetworkDeviceGroups    value:IPSEC#Is IPSEC Device#No, Location#All Locations, Device
        Attribute:NetworkDeviceName      value:DEMO-SWITCH-1
        Attribute:NmapSubnetScanID       value:0
        Attribute:OUI    value:Cisco Systems, Inc
```

CDP attributes are missing in parsed Accounting Start

Administration > System > Logging > Debug Log Configuration



Node List > ciscolive-ise1.demo.local

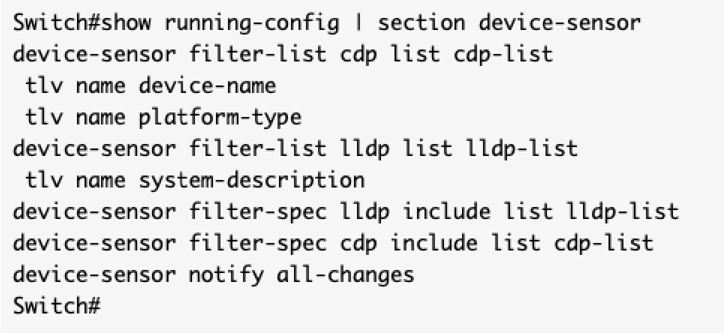
Debug Level Configuration

	Component Name	Log Level	Description
	profiler		
○	profiler	DEBUG	profiler debug messages

--- followed by ---

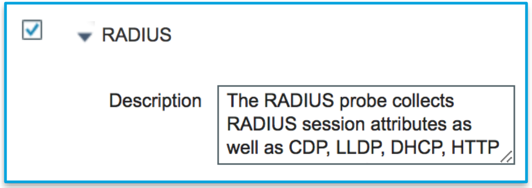
show logging application profiler.log tail

Confirming the theory – issue 1



```
Switch#show running-config | section device-sensor
device-sensor filter-list cdp list cdp-list
 tlv name device-name
 tlv name platform-type
device-sensor filter-list lldp list lldp-list
 tlv name system-description
device-sensor filter-spec lldp include list lldp-list
device-sensor filter-spec cdp include list cdp-list
device-sensor notify all-changes
Switch#
```

Issue 1: “device-sensor accounting” command is missing, causing switch not to send device-sensor cache data to ISE. Switches was replaced few weeks ago
Solution 1: configure “device-sensor accounting” on the switch



☑ ▾ RADIUS

Description: The RADIUS probe collects RADIUS session attributes as well as CDP, LLDP, DHCP, HTTP

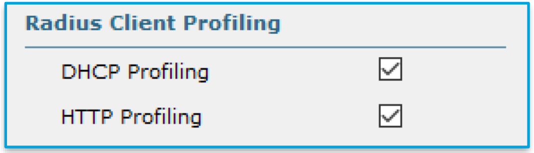
From 15.0(2)SE

```
device-sensor accounting
device-sensor notify all-changes
```

But Wait

Issue 1a: Due to **CSCvq58785 Static group information is lost from EP in some scenarios** Phones lost identity group assignment, and due to Issue 1, never got re-profiled.
Solution 1a: Upgrade to fixed release 2.4 patch 11

From AireOS 7.2



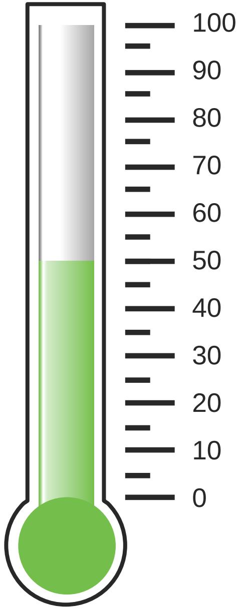
Radius Client Profiling

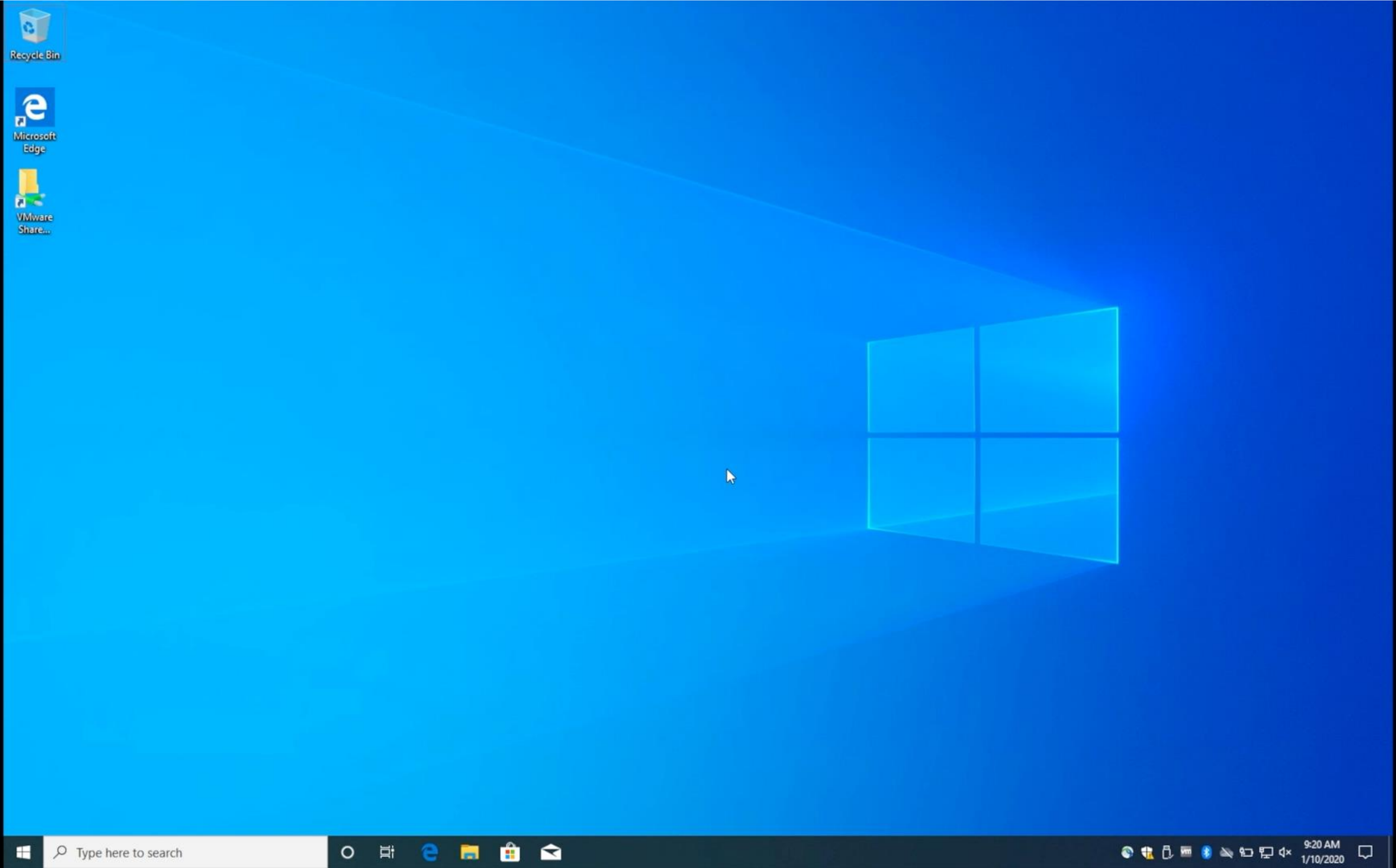
DHCP Profiling	☑
HTTP Profiling	☑

WLANs > (SSID) > Advanced

Issue 2

Meeting's success scale




Recycle Bin
Microsoft Edge
VMware Share...
Type here to search
9:20 AM
1/10/2020

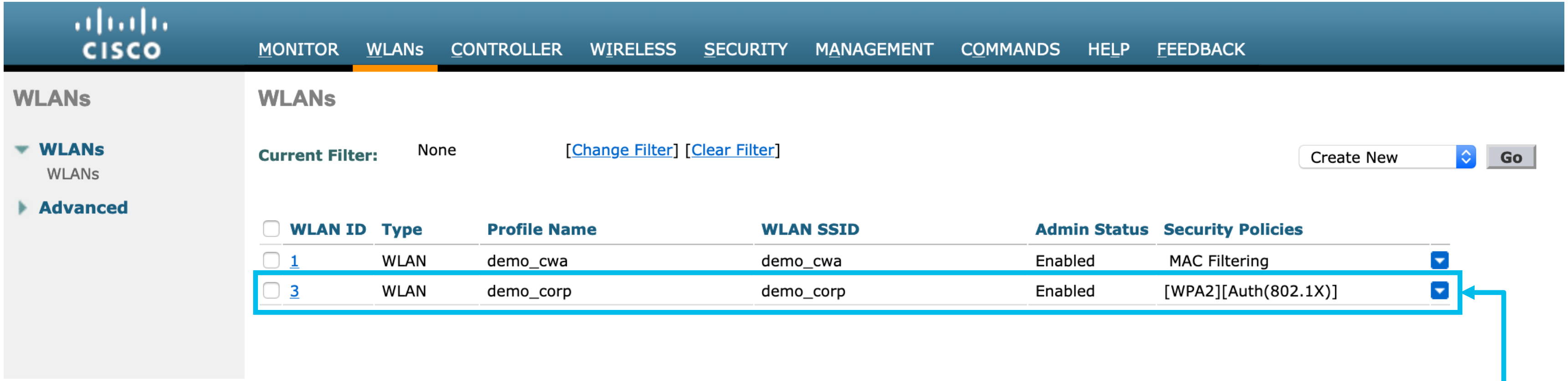
Define the problem – issue 2

Users can’t connect to the wireless network, “demo_corp” SSID is not broadcasted

Supporting facts

- Demo_corp is company wide corporate SSID, network is seen in some of the other locations

WLC > WLANs

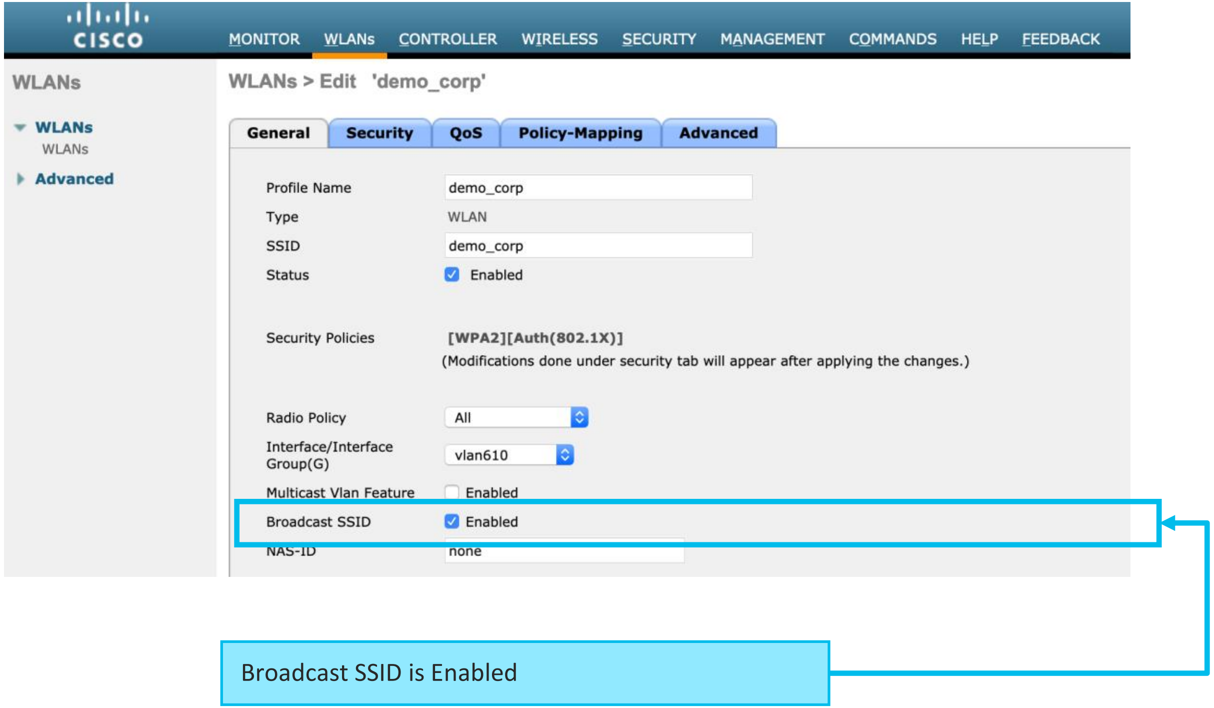


Current Filter: None [Change Filter] [Clear Filter]

□ WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
□ 1	WLAN	demo_cwa	demo_cwa	Enabled	MAC Filtering
□ 3	WLAN	demo_corp	demo_corp	Enabled	[WPA2][Auth(802.1X)]

WLAN demo_corp is configured and Enabled

WLC > WLANs

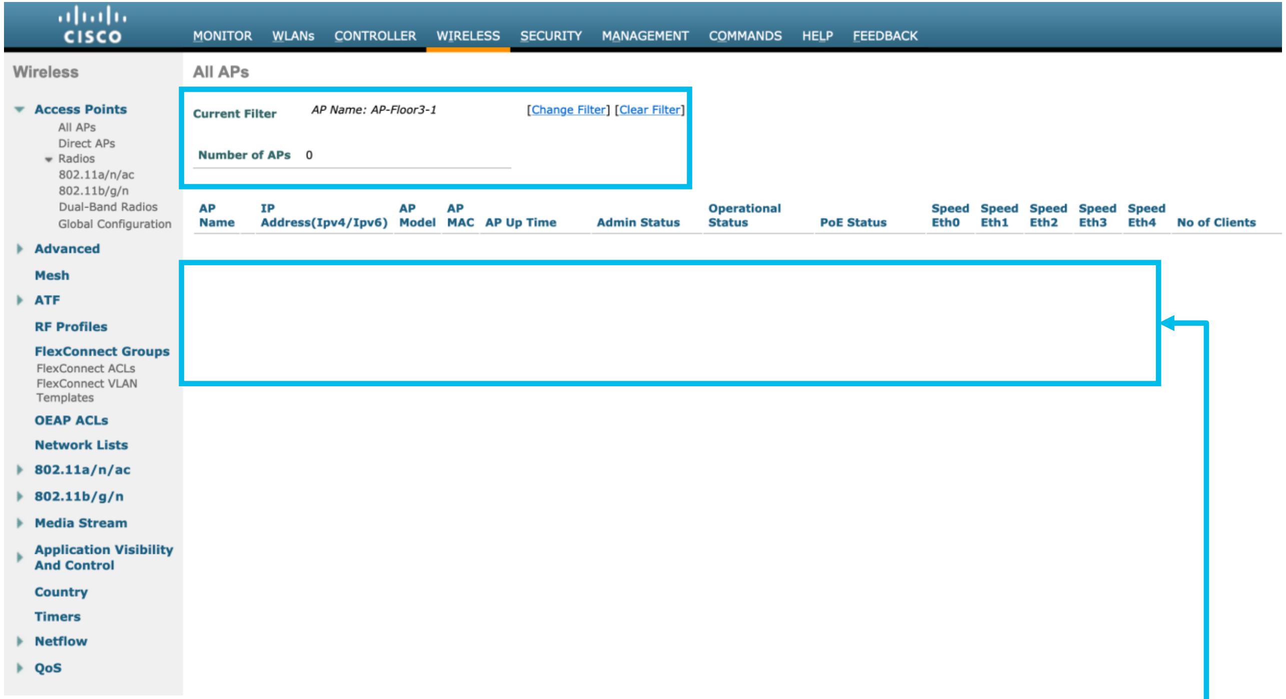


WLANs > Edit 'demo_corp'

Profile Name	demo_corp
Type	WLAN
SSID	demo_corp
Status	☑ Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	vlan610
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	none

Broadcast SSID is Enabled

WLC > WLANs



All APs

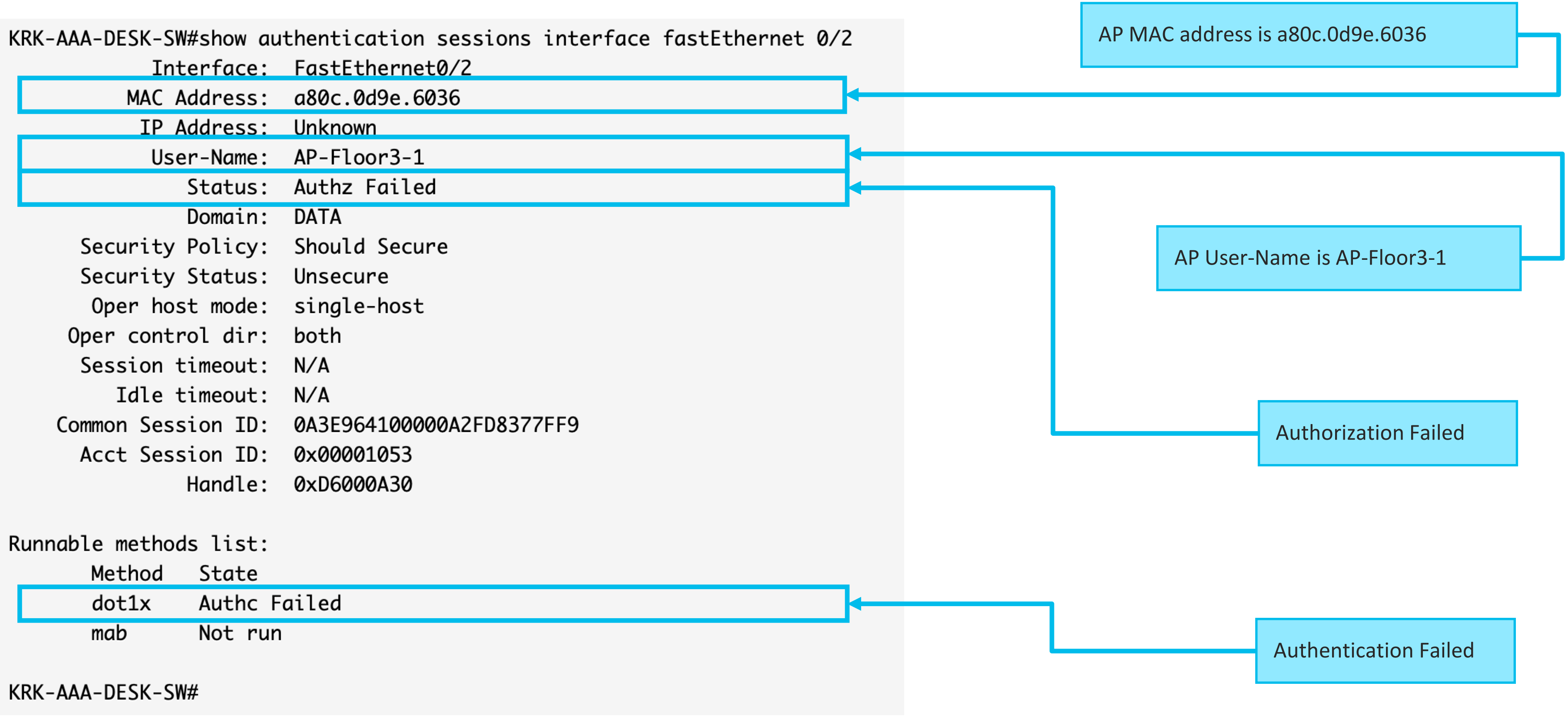
Current Filter *AP Name: AP-Floor3-1* [Change Filter] [Clear Filter]

Number of APs 0

AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	PoE Status	Speed Eth0	Speed Eth1	Speed Eth2	Speed Eth3	Speed Eth4	No of Clients

AP-Floor3-1 AP is not registered on WLC

Switch > show authentication session



```
KRK-AAA-DESK-SW#show authentication sessions interface fastEthernet 0/2
            Interface:  FastEthernet0/2
          MAC Address:  a80c.0d9e.6036
           IP Address:  Unknown
            User-Name:  AP-Floor3-1
               Status:  Authz Failed
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3E964100000A2FD8377FF9
      Acct Session ID:  0x00001053
               Handle:  0xD6000A30

Runnable methods list:
       Method   State
       dot1x    Authc Failed
       mab      Not run

KRK-AAA-DESK-SW#
```

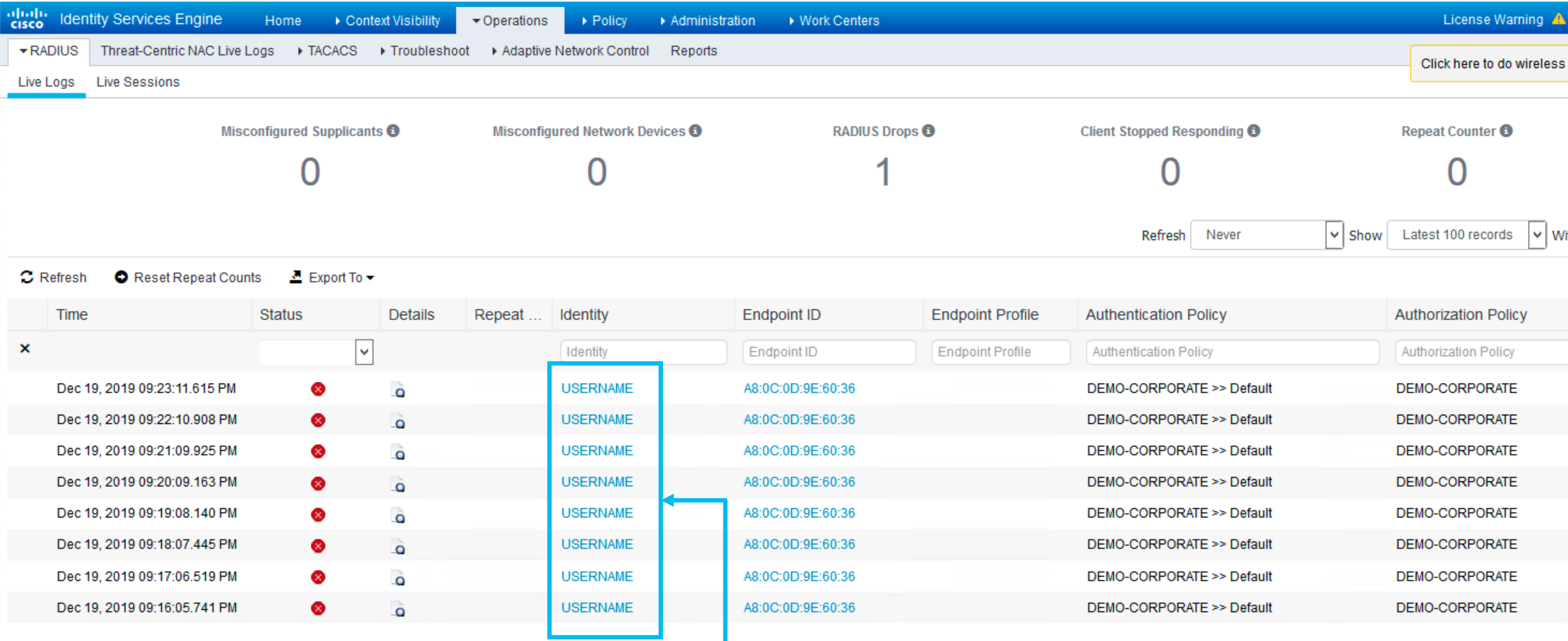
AP MAC address is a80c.0d9e.6036

AP User-Name is AP-Floor3-1

Authorization Failed

Authentication Failed

Operations > Radius > Live Logs



Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning ⚠

RADIUS | Threat-Centric NAC Live Logs | TACACS | Troubleshoot | Adaptive Network Control | Reports

Click here to do wireless

Live Logs | Live Sessions

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	1	0	0

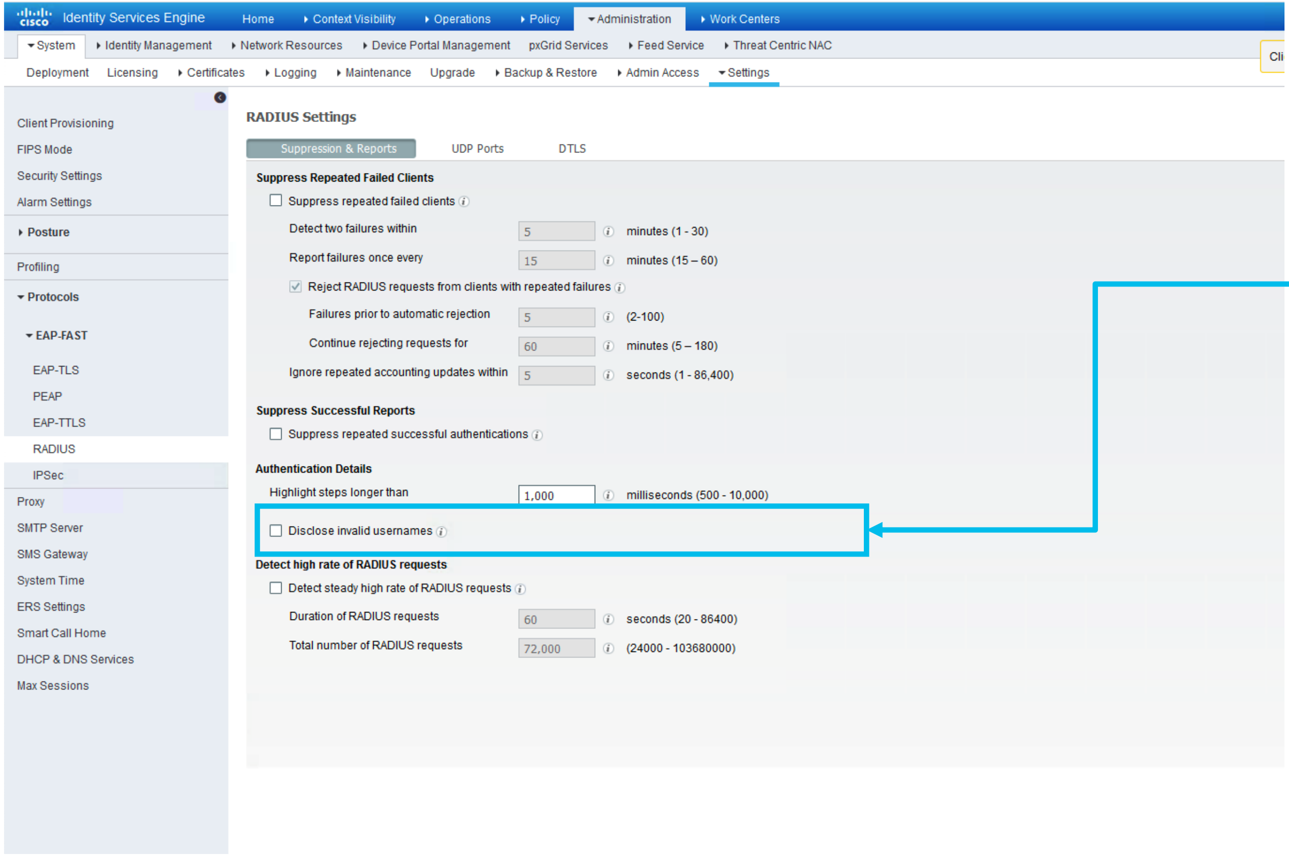
Refresh: Never | Show: Latest 100 records | Wi

Refresh | Reset Repeat Counts | Export To

	Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy
×					Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy
	Dec 19, 2019 09:23:11.615 PM	✖	🔍		USERNAME	A8:0C:0D:9E:60:36		DEMO-CORPORATE >> Default	DEMO-CORPORATE
	Dec 19, 2019 09:22:10.908 PM	✖	🔍		USERNAME	A8:0C:0D:9E:60:36		DEMO-CORPORATE >> Default	DEMO-CORPORATE
	Dec 19, 2019 09:21:09.925 PM	✖	🔍		USERNAME	A8:0C:0D:9E:60:36		DEMO-CORPORATE >> Default	DEMO-CORPORATE
	Dec 19, 2019 09:20:09.163 PM	✖	🔍		USERNAME	A8:0C:0D:9E:60:36		DEMO-CORPORATE >> Default	DEMO-CORPORATE
	Dec 19, 2019 09:19:08.140 PM	✖	🔍		USERNAME	A8:0C:0D:9E:60:36		DEMO-CORPORATE >> Default	DEMO-CORPORATE
	Dec 19, 2019 09:18:07.445 PM	✖	🔍		USERNAME	A8:0C:0D:9E:60:36		DEMO-CORPORATE >> Default	DEMO-CORPORATE
	Dec 19, 2019 09:17:06.519 PM	✖	🔍		USERNAME	A8:0C:0D:9E:60:36		DEMO-CORPORATE >> Default	DEMO-CORPORATE
	Dec 19, 2019 09:16:05.741 PM	✖	🔍		USERNAME	A8:0C:0D:9E:60:36		DEMO-CORPORATE >> Default	DEMO-CORPORATE

Why Username is ”USERNAME” and not AP-Floor3-1 like on switch?

Invalid Username Disclosure



RADIUS Settings

Suppress Repeated Failed Clients

☐ Suppress repeated failed clients

Detect two failures within 5 minutes (1 - 30)

Report failures once every 15 minutes (15 – 60)

☑ Reject RADIUS requests from clients with repeated failures

Failures prior to automatic rejection 5 (2-100)

Continue rejecting requests for 60 minutes (5 – 180)

Ignore repeated accounting updates within 5 seconds (1 - 86,400)

Suppress Successful Reports

☐ Suppress repeated successful authentications

Authentication Details

Highlight steps longer than 1,000 milliseconds (500 - 10,000)

☐ Disclose invalid usernames

Detect high rate of RADIUS requests

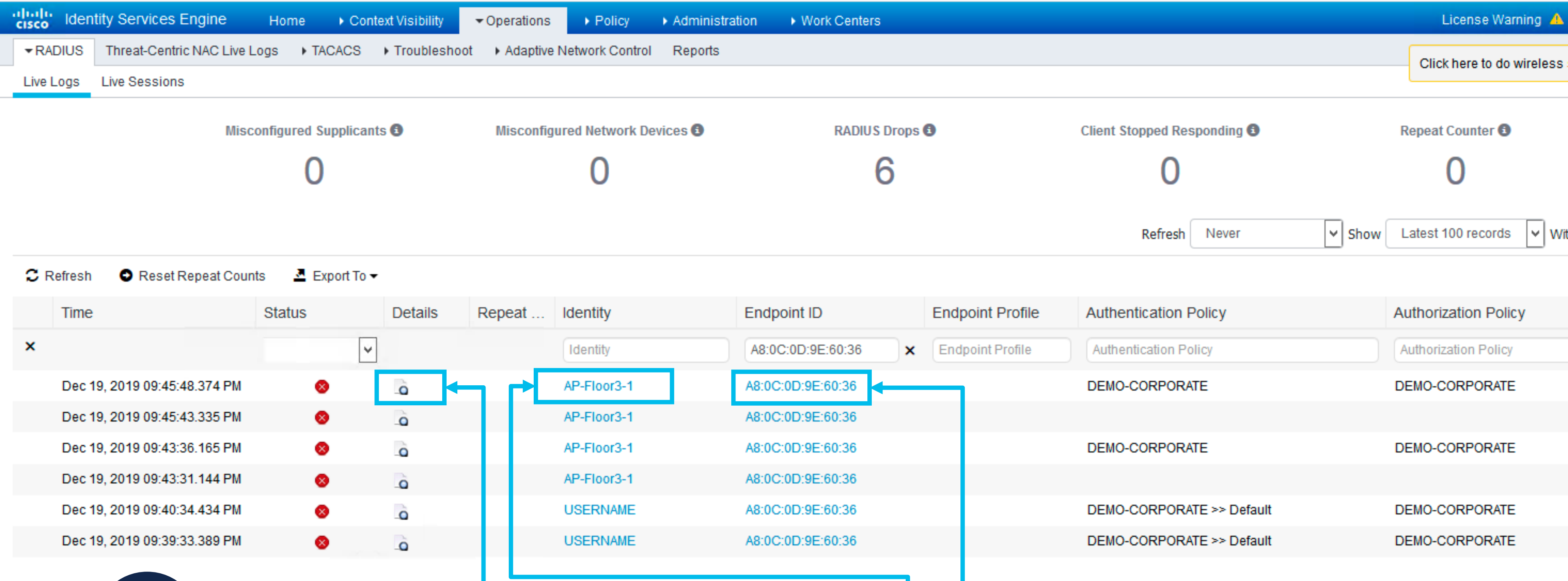
☐ Detect steady high rate of RADIUS requests

Duration of RADIUS requests 60 seconds (20 - 86400)

Total number of RADIUS requests 72,000 (24000 - 103680000)

Check this checkbox to disclose the usernames labelled as 'USERNAME' or 'INVALID' in the Radius Live Logs. You can then view the logged in username in the Radius Live Logs as well as in the Authentication Summary Report.

Operations > Radius > Live Logs



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	6	0	0

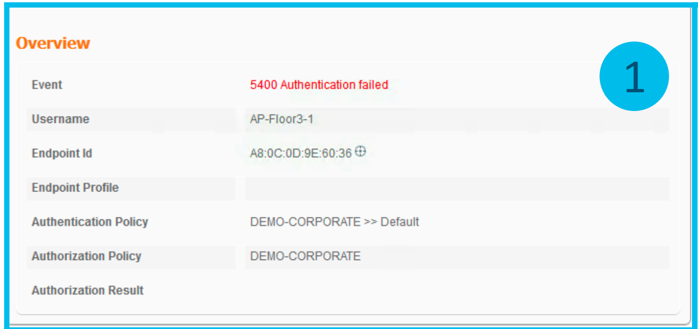
Refresh: Never Show: Latest 100 records

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy
✕				Identity	A8:0C:0D:9E:60:36 ✕	Endpoint Profile	Authentication Policy	Authorization Policy
Dec 19, 2019 09:45:48.374 PM	✖	🔍		AP-Floor3-1	A8:0C:0D:9E:60:36		DEMO-CORPORATE	DEMO-CORPORATE
Dec 19, 2019 09:45:43.335 PM	✖	🔍		AP-Floor3-1	A8:0C:0D:9E:60:36			
Dec 19, 2019 09:43:36.165 PM	✖	🔍		AP-Floor3-1	A8:0C:0D:9E:60:36		DEMO-CORPORATE	DEMO-CORPORATE
Dec 19, 2019 09:43:31.144 PM	✖	🔍		AP-Floor3-1	A8:0C:0D:9E:60:36			
Dec 19, 2019 09:40:34.434 PM	✖	🔍		USERNAME	A8:0C:0D:9E:60:36		DEMO-CORPORATE >> Default	DEMO-CORPORATE
Dec 19, 2019 09:39:33.389 PM	✖	🔍		USERNAME	A8:0C:0D:9E:60:36		DEMO-CORPORATE >> Default	DEMO-CORPORATE

Username of Access Point to confirm correct log message

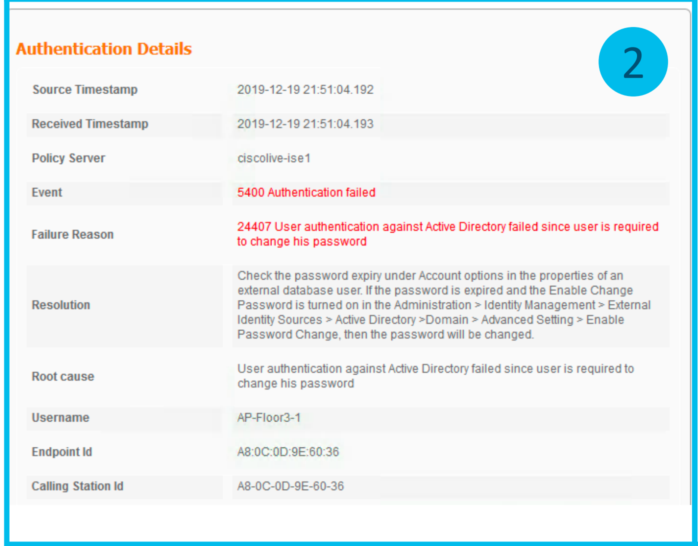
MAC address of the Access Point to confirm correct log message

How about Detailed Authentication Report?



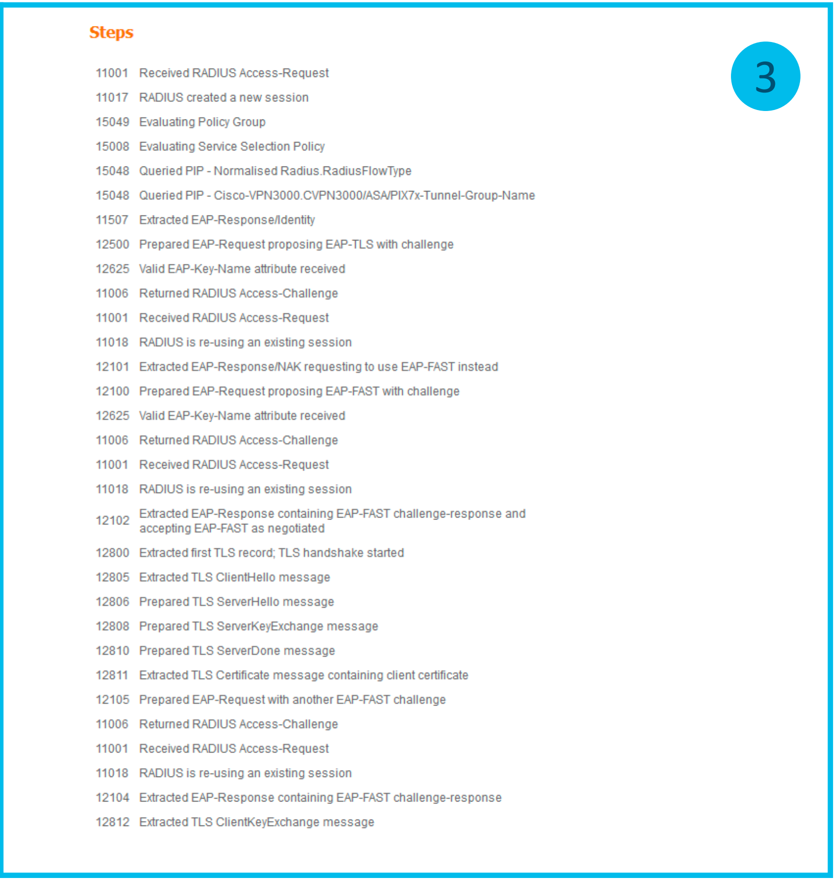
Overview

Event	5400 Authentication failed
Username	AP-Floor3-1
Endpoint Id	A8:0C:0D:9E:60:36 ⊕
Endpoint Profile	
Authentication Policy	DEMO-CORPORATE >> Default
Authorization Policy	DEMO-CORPORATE
Authorization Result	



Authentication Details

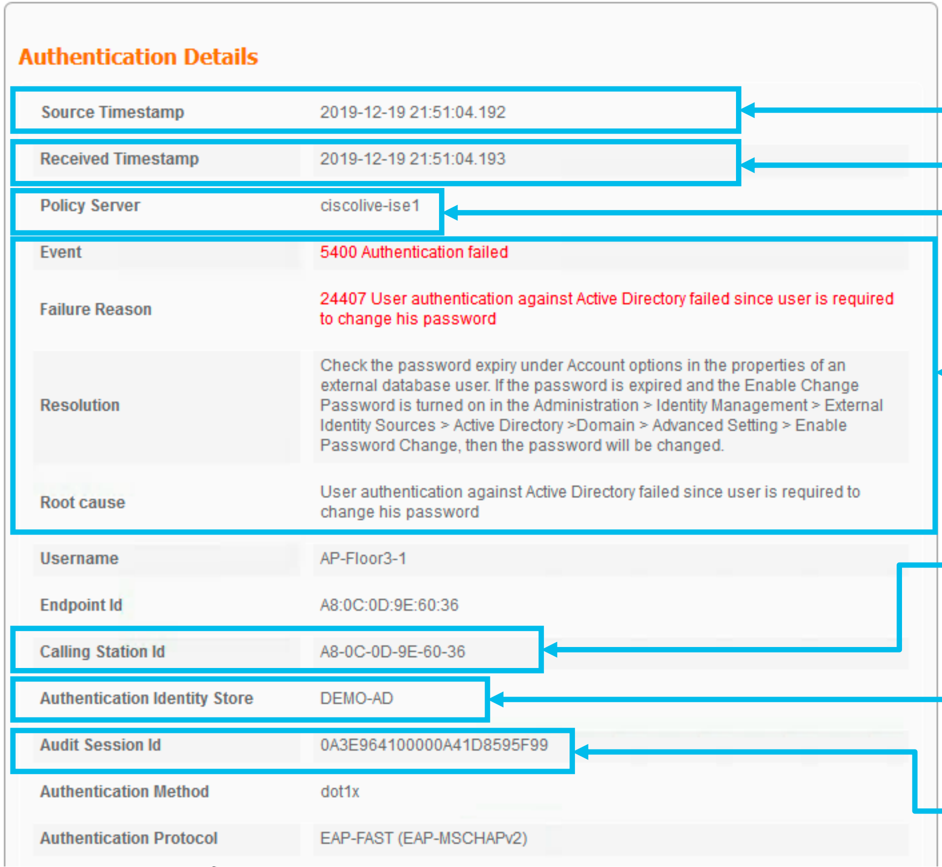
Source Timestamp	2019-12-19 21:51:04.192
Received Timestamp	2019-12-19 21:51:04.193
Policy Server	ciscolive-ise1
Event	5400 Authentication failed
Failure Reason	24407 User authentication against Active Directory failed since user is required to change his password
Resolution	Check the password expiry under Account options in the properties of an external database user. If the password is expired and the Enable Change Password is turned on in the Administration > Identity Management > External Identity Sources > Active Directory >Domain > Advanced Setting > Enable Password Change, then the password will be changed.
Root cause	User authentication against Active Directory failed since user is required to change his password
Username	AP-Floor3-1
Endpoint Id	A8:0C:0D:9E:60:36
Calling Station Id	A8-0C-0D-9E-60-36



Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - Normalised Radius.RadiusFlowType
15048	Queried PIP - Cisco-VPN3000.CVPN3000/ASA/PIX7x-Tunnel-Group-Name
11507	Extracted EAP-Response/Identity
12500	Prepared EAP-Request proposing EAP-TLS with challenge
12625	Valid EAP-Key-Name attribute received
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12101	Extracted EAP-Response/NAK requesting to use EAP-FAST instead
12100	Prepared EAP-Request proposing EAP-FAST with challenge
12625	Valid EAP-Key-Name attribute received
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12102	Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated
12800	Extracted first TLS record; TLS handshake started
12805	Extracted TLS ClientHello message
12806	Prepared TLS ServerHello message
12808	Prepared TLS ServerKeyExchange message
12810	Prepared TLS ServerDone message
12811	Extracted TLS Certificate message containing client certificate
12105	Prepared EAP-Request with another EAP-FAST challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12104	Extracted EAP-Response containing EAP-FAST challenge-response
12812	Extracted TLS ClientKeyExchange message

Live Logs > Detailed authentication report



Authentication Details

Source Timestamp	2019-12-19 21:51:04.192
Received Timestamp	2019-12-19 21:51:04.193
Policy Server	ciscolive-ise1
Event	5400 Authentication failed
Failure Reason	24407 User authentication against Active Directory failed since user is required to change his password
Resolution	Check the password expiry under Account options in the properties of an external database user. If the password is expired and the Enable Change Password is turned on in the Administration > Identity Management > External Identity Sources > Active Directory >Domain > Advanced Setting > Enable Password Change, then the password will be changed.
Root cause	User authentication against Active Directory failed since user is required to change his password
Username	AP-Floor3-1
Endpoint Id	A8:0C:0D:9E:60:36
Calling Station Id	A8-0C-0D-9E-60-36
Authentication Identity Store	DEMO-AD
Audit Session Id	0A3E964100000A41D8595F99
Authentication Method	dot1x
Authentication Protocol	EAP-FAST (EAP-MSCHAPv2)

Timestamp from the Radius

Timestamp from ISE

PSN, where authentication took place

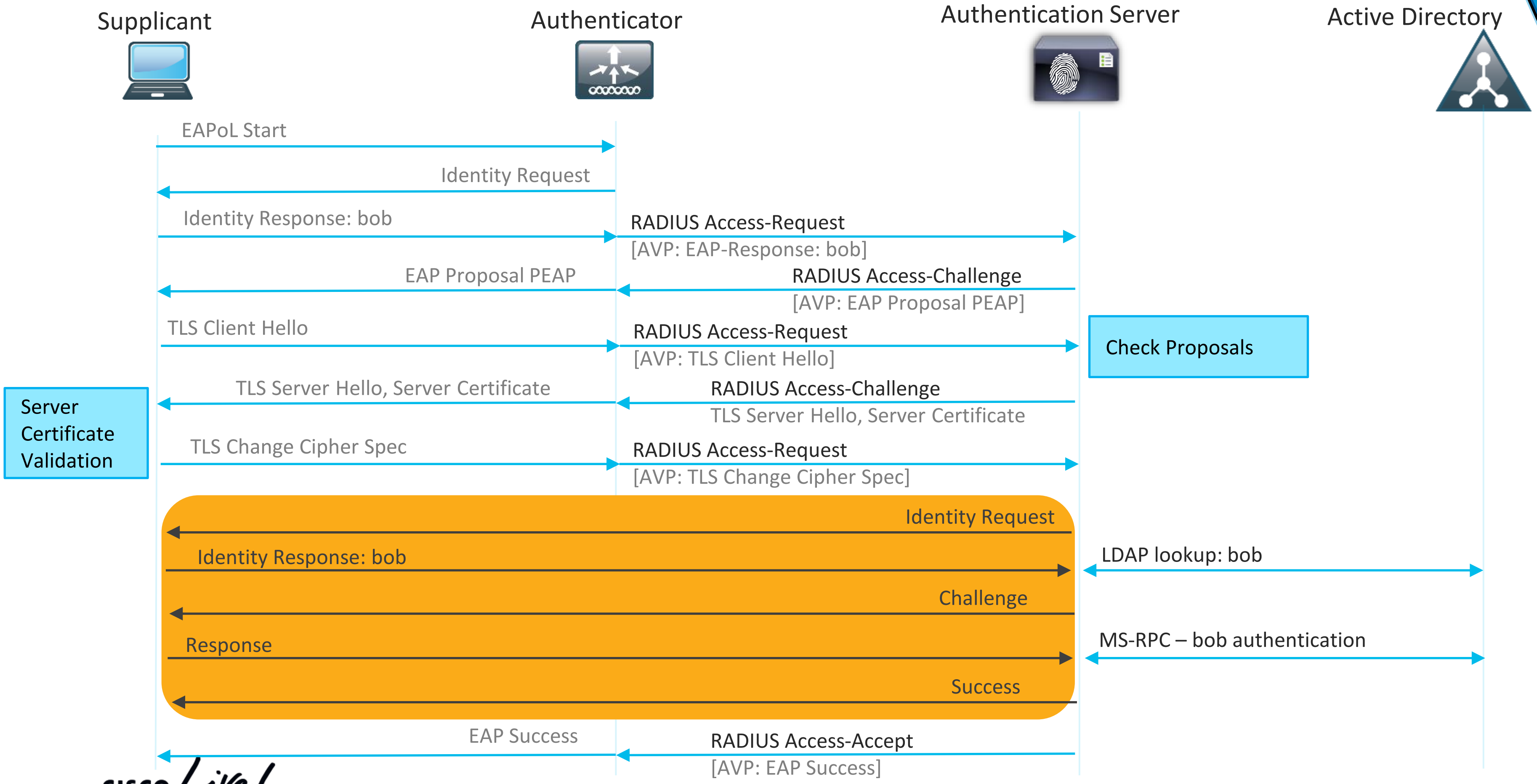
Troubleshooting section, very useful information, which contains the reason for the failure, root cause of it, and potential resolution. The first thing to look into if you are facing the authentication issues.

Radius attribute which should show client's mac address, ip address in vpn usecase.

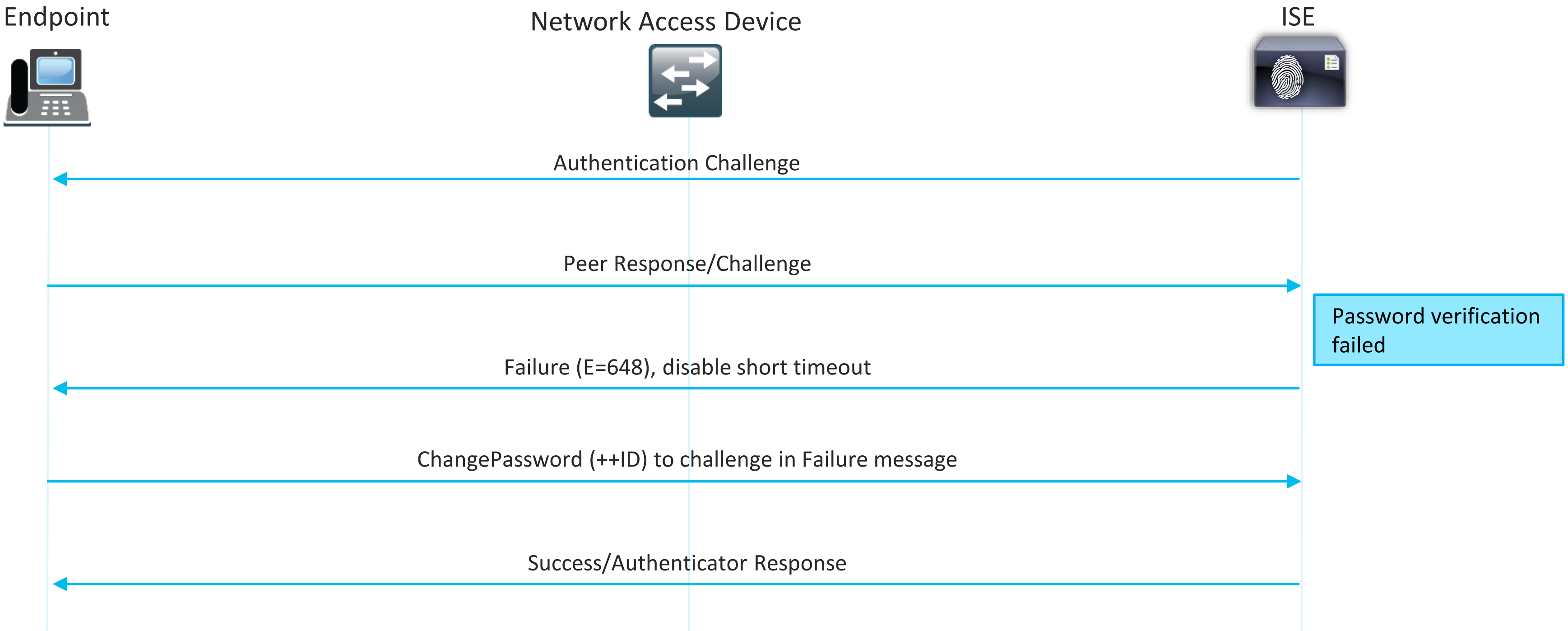
Identity Store used for authentication

Audit Session Id, can be used for any session related issues troubleshooting

PEAP with MSCHAPv2 flow high level overview



Successful Authentication with password change



Endpoint

Network Access Device

ISE

Authentication Challenge

Peer Response/Challenge

Password verification failed

Failure (E=648), disable short timeout

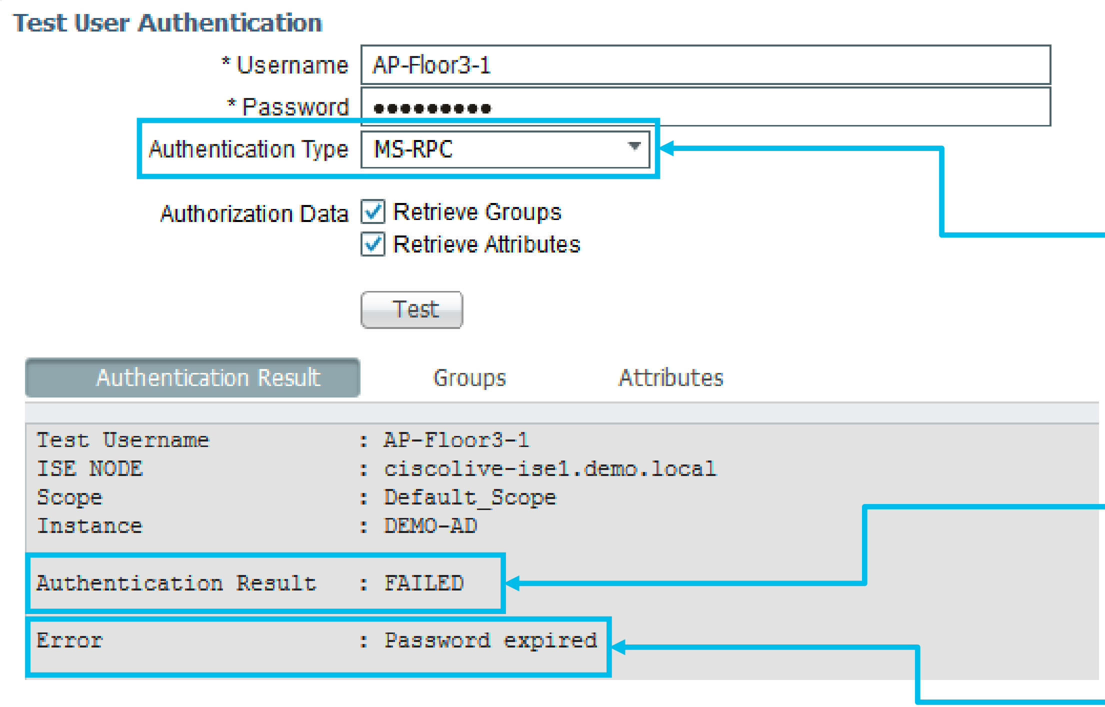
ChangePassword (++ID) to challenge in Failure message

Success/Authenticator Response

RFC 2759, Change-Password Packet The Change-Password packet appears in MS-CHAP-V2. It allows the peer to change the password on the account specified in the preceding Response packet. The Change-Password packet should be sent only if the authenticator reports ERROR_PASSWD_EXPIRED (E=648) in the Message field of the Failure packet.

Alternative Troubleshooting - ISE

Test User Authentication Tool



Test User Authentication

* Username	AP-Floor3-1
* Password	●●●●●●●●●●
Authentication Type	MS-RPC
Authorization Data	☑ Retrieve Groups ☑ Retrieve Attributes

```
Test Username              : AP-Floor3-1
ISE NODE                   : ciscolive-ise1.demo.local
Scope                      : Default_Scope
Instance                   : DEMO-AD

Authentication Result      : FAILED

Error                      : Password expired
```

Use **MS-RPC** for password based authentications

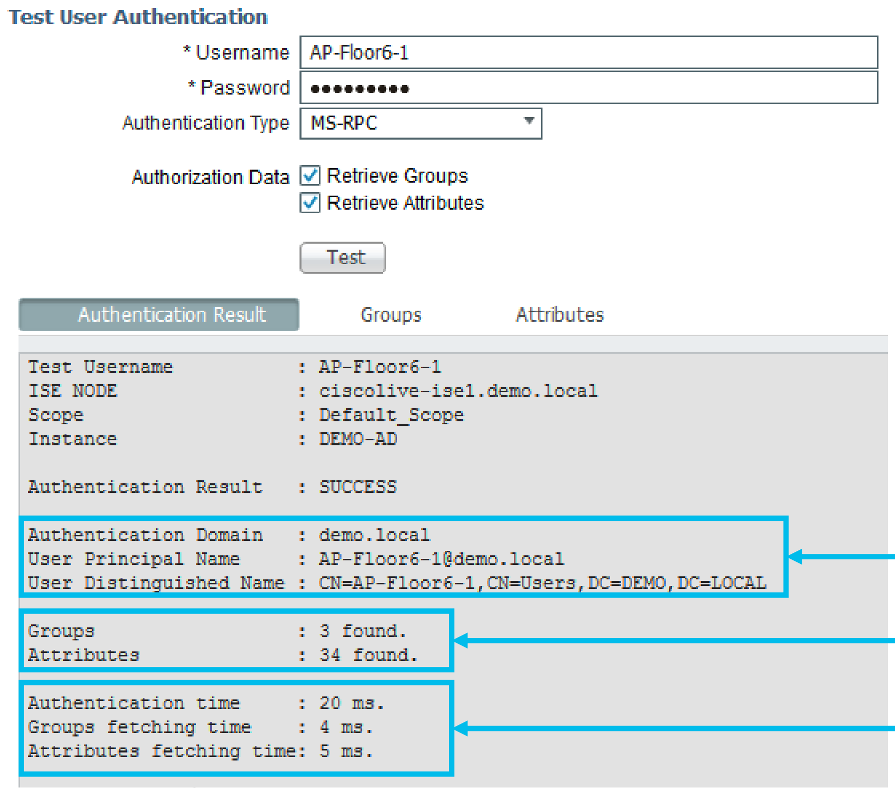
Use **Lookup** for authentications without password, like EAP-TLS

Authentication Result can be **SUCCESS** or **FAILED**

Error message – Password Expired

Alternative Troubleshooting - ISE

Test User Authentication Tool



Test User Authentication

* Username	AP-Floor6-1
* Password	●●●●●●●●●●
Authentication Type	MS-RPC
Authorization Data	☑ Retrieve Groups ☑ Retrieve Attributes

```
Test Username          : AP-Floor6-1
ISE NODE               : ciscolive-ise1.demo.local
Scope                  : Default_Scope
Instance               : DEMO-AD

Authentication Result  : SUCCESS

Authentication Domain  : demo.local
User Principal Name    : AP-Floor6-1@demo.local
User Distinguished Name : CN=AP-Floor6-1,CN=Users,DC=DEMO,DC=LOCAL

Groups                 : 3 found.
Attributes             : 34 found.

Authentication time    : 20 ms.
Groups fetching time   : 4 ms.
Attributes fetching time: 5 ms.
```

- Domain, which authenticated the client.
- UPN and DN of the client.

Total number for Groups/Attributes retrieved for the client

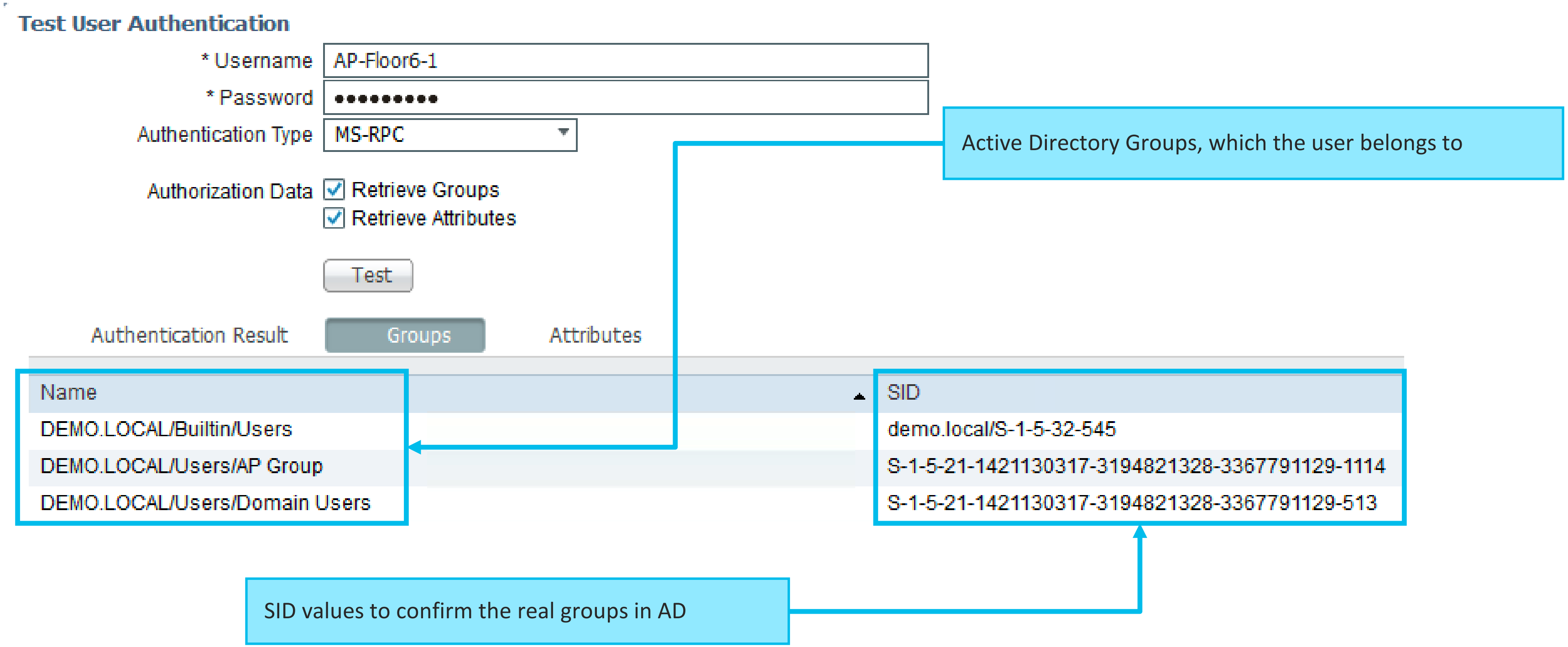
Time it took to:

- Perform authentication.
- Fetch Groups/Attributes.

Useful when troubleshooting latency

Alternative Troubleshooting - ISE

Test User Authentication Tool



Test User Authentication

* Username	AP-Floor6-1
* Password	••••••••••
Authentication Type	MS-RPC
Authorization Data	☑ Retrieve Groups ☑ Retrieve Attributes

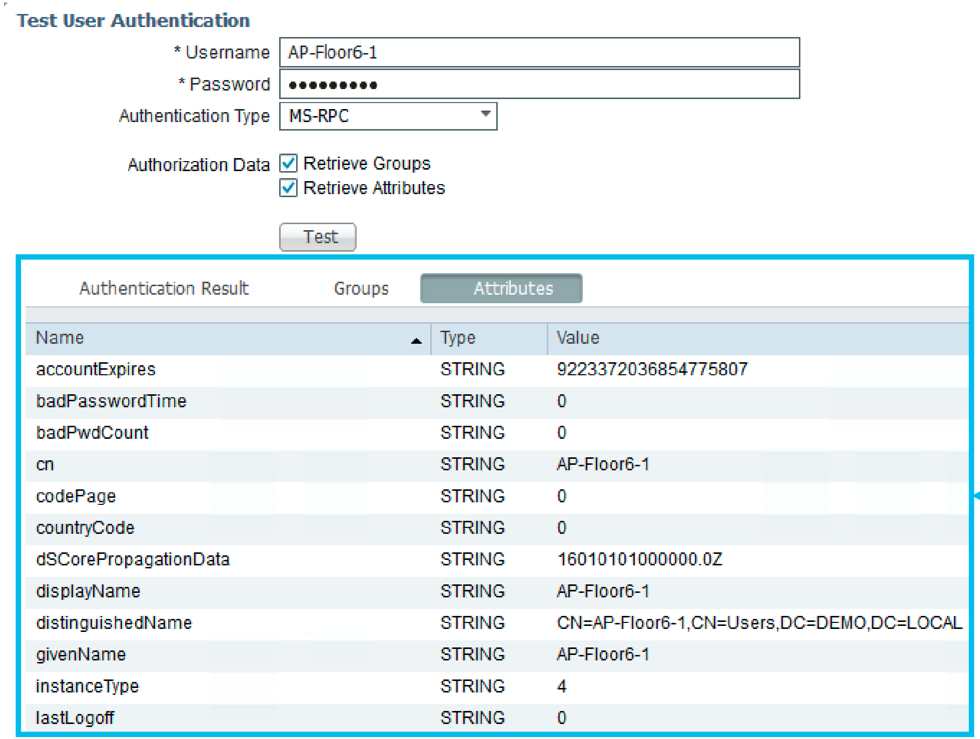
Name	SID
DEMO.LOCAL/Builtin/Users	demo.local/S-1-5-32-545
DEMO.LOCAL/Users/AP Group	S-1-5-21-1421130317-3194821328-3367791129-1114
DEMO.LOCAL/Users/Domain Users	S-1-5-21-1421130317-3194821328-3367791129-513

Active Directory Groups, which the user belongs to

SID values to confirm the real groups in AD

Alternative Troubleshooting - ISE

Test User Authentication Tool



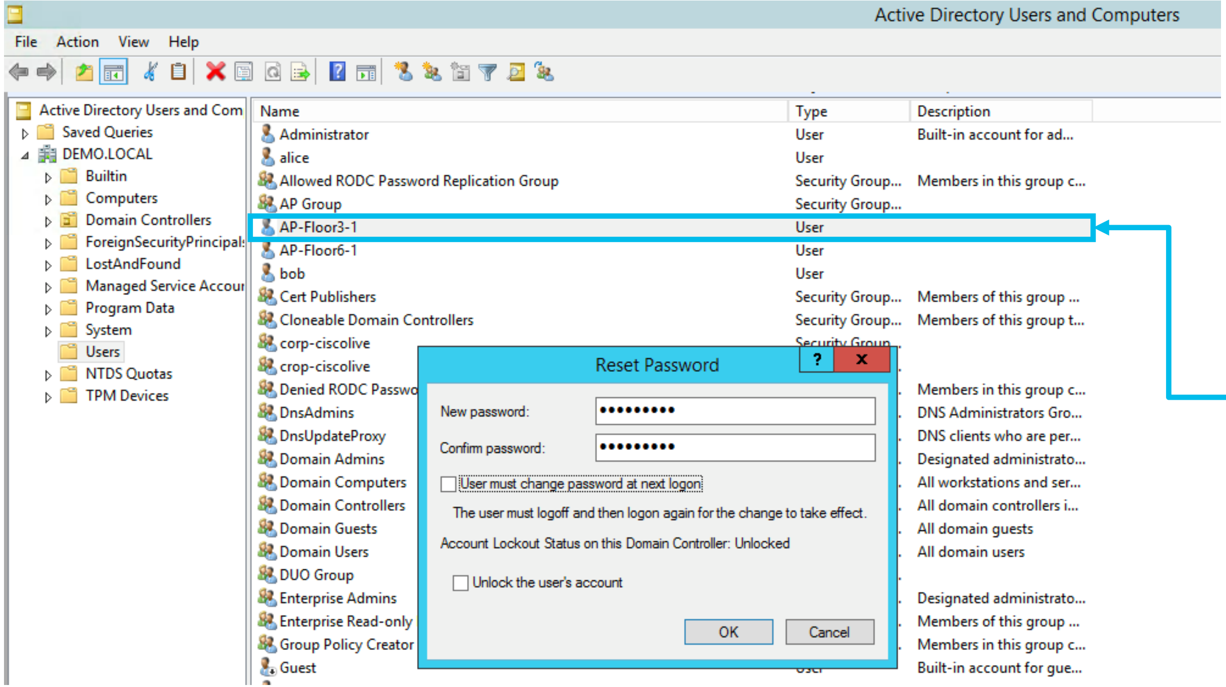
Test User Authentication

* Username	AP-Floor6-1
* Password	●●●●●●●●●●
Authentication Type	MS-RPC
Authorization Data	☑ Retrieve Groups ☑ Retrieve Attributes

Name	Type	Value
accountExpires	STRING	9223372036854775807
badPasswordTime	STRING	0
badPwdCount	STRING	0
cn	STRING	AP-Floor6-1
codePage	STRING	0
countryCode	STRING	0
dSCorePropagationData	STRING	16010101000000.0Z
displayName	STRING	AP-Floor6-1
distinguishedName	STRING	CN=AP-Floor6-1,CN=Users,DC=DEMO,DC=LOCAL
givenName	STRING	AP-Floor6-1
instanceType	STRING	4
lastLogoff	STRING	0

- Full list of User Attributes.
- Attributes can be used in Authorization Policies.

Confirming the theory – issue 2



- Active Directory Users and Com
  - Saved Queries
  - DEMO.LOCAL
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipal:
    - LostAndFound
    - Managed Service Accour
    - Program Data
    - System
    - Users
    - NTDS Quotas
    - TPM Devices

Name	Type	Description
Administrator	User	Built-in account for ad...
alice	User	
Allowed RODC Password Replication Group	Security Group...	Members in this group c...
AP Group	Security Group...	
AP-Floor3-1	User	
AP-Floor6-1	User	
bob	User	
Cert Publishers	Security Group...	Members of this group ...
Cloneable Domain Controllers	Security Group...	Members of this group t...
corp-ciscolive	Security Group...	
crop-ciscolive		
Denied RODC Passwo		Members in this group c...
DnsAdmins		DNS Administrators Gro...
DnsUpdateProxy		DNS clients who are per...
Domain Admins		Designated administrato...
Domain Computers		All workstations and ser...
Domain Controllers		All domain controllers i...
Domain Guests		All domain guests
Domain Users		All domain users
DUO Group		
Enterprise Admins		Designated administrato...
Enterprise Read-only		Members of this group ...
Group Policy Creator		Members in this group c...
Guest	User	Built-in account for gue...

Reset Password

New password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

□ User must change password at next logon

The user must logoff and then logon again for the change to take effect.

Account Lockout Status on this Domain Controller: Unlocked

□ Unlock the user's account

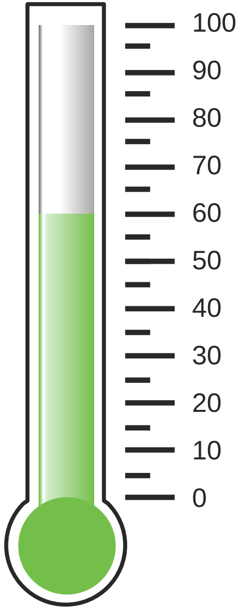
OK Cancel

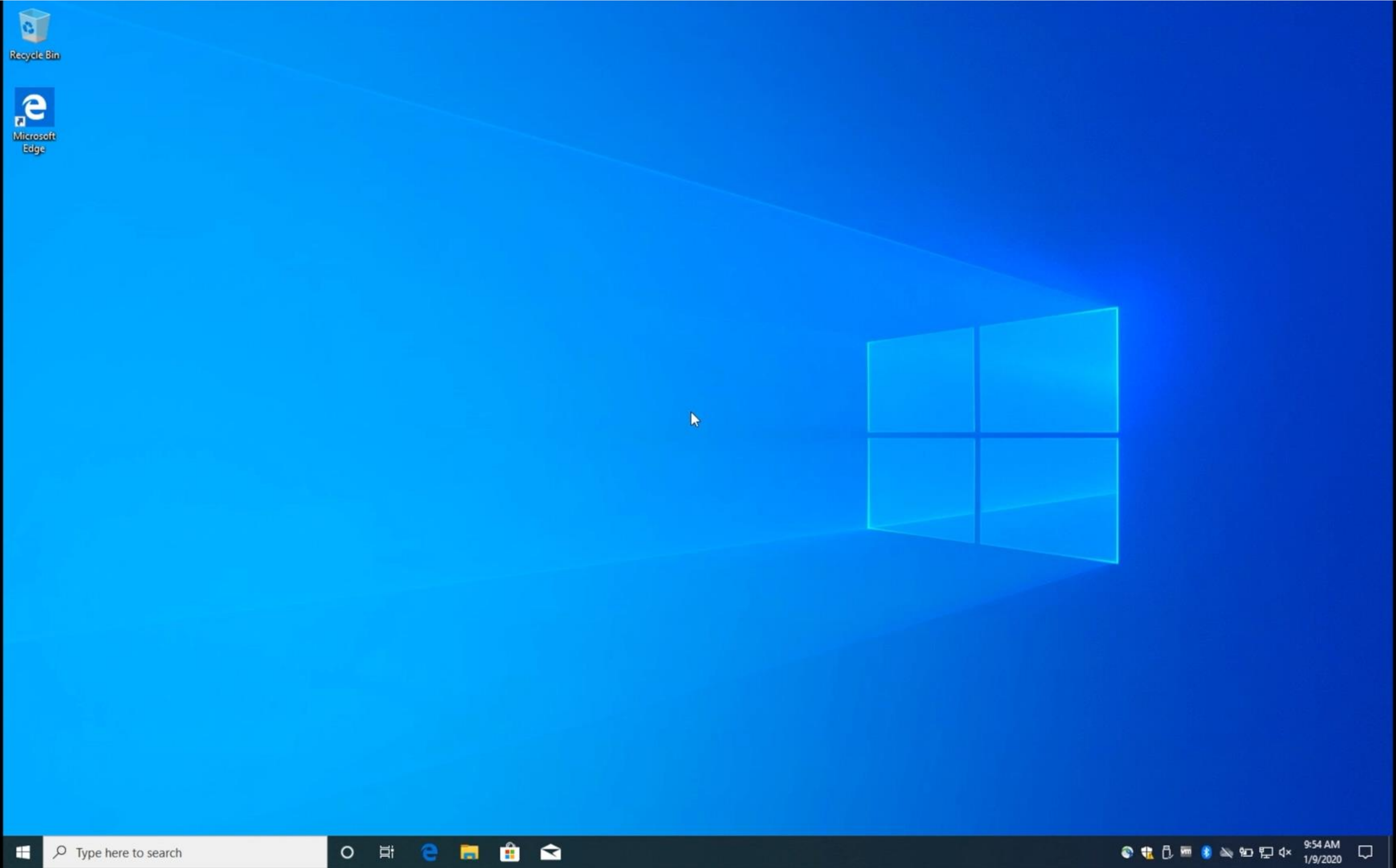
Password Reset for the user AP-Floor3-1

Issue 2: Password for the user AP-Floor3-1 got expired. AP Username was created with Password Expiration Policy
Solution 2: Reset the password for the user AP-Floor3-1 on Active Directory, disable Password Expiration Policy for AP Group

Issue 3

Meeting's success scale



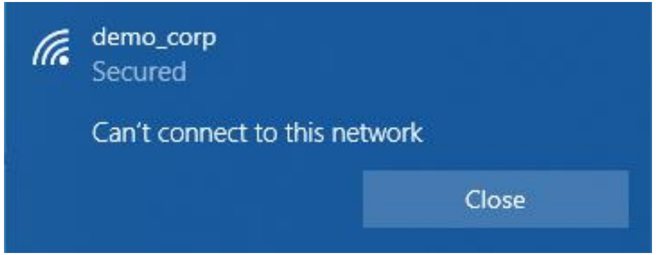

Recycle Bin
Microsoft Edge
Type here to search
9:54 AM
1/9/2020

Define the problem – issue 3

Users can’t connect to the wireless network, “demo_corp” connection is failing with the error message “Can’t connect to this network”

Supporting facts

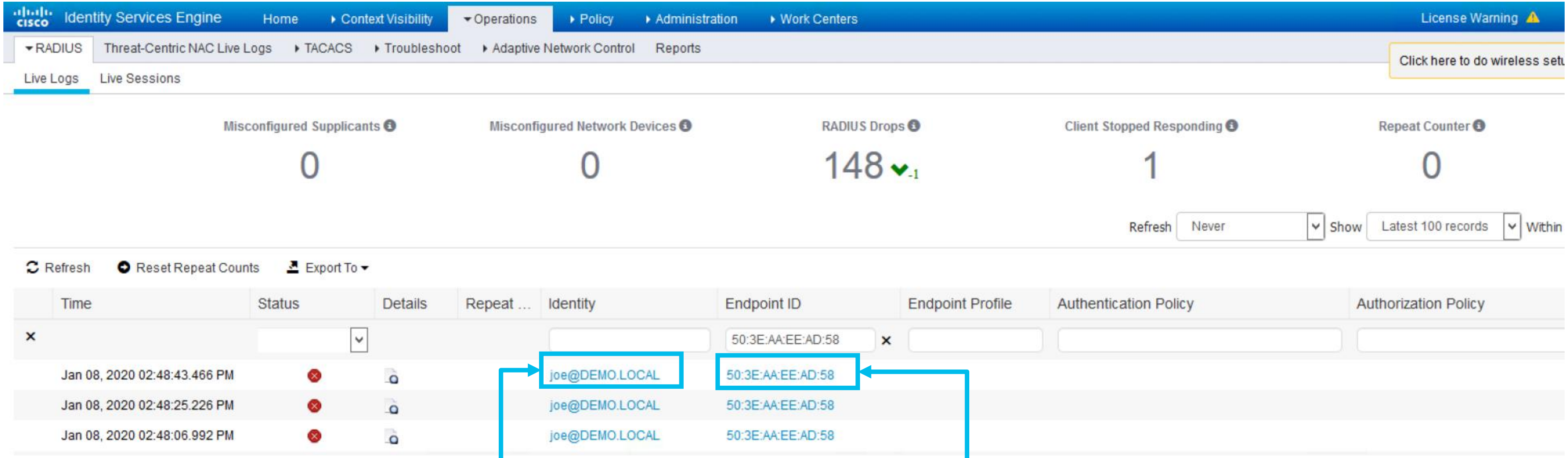
- Demo_corp is company wide corporate SSID
- Few other users reported the same issue after the weekend



demo_corp
Secured

Can’t connect to this network

Operations > Radius > Live Logs



Misconfigured Supplicants: 0

Misconfigured Network Devices: 0

RADIUS Drops: 148 ✓-1

Client Stopped Responding: 1

Repeat Counter: 0

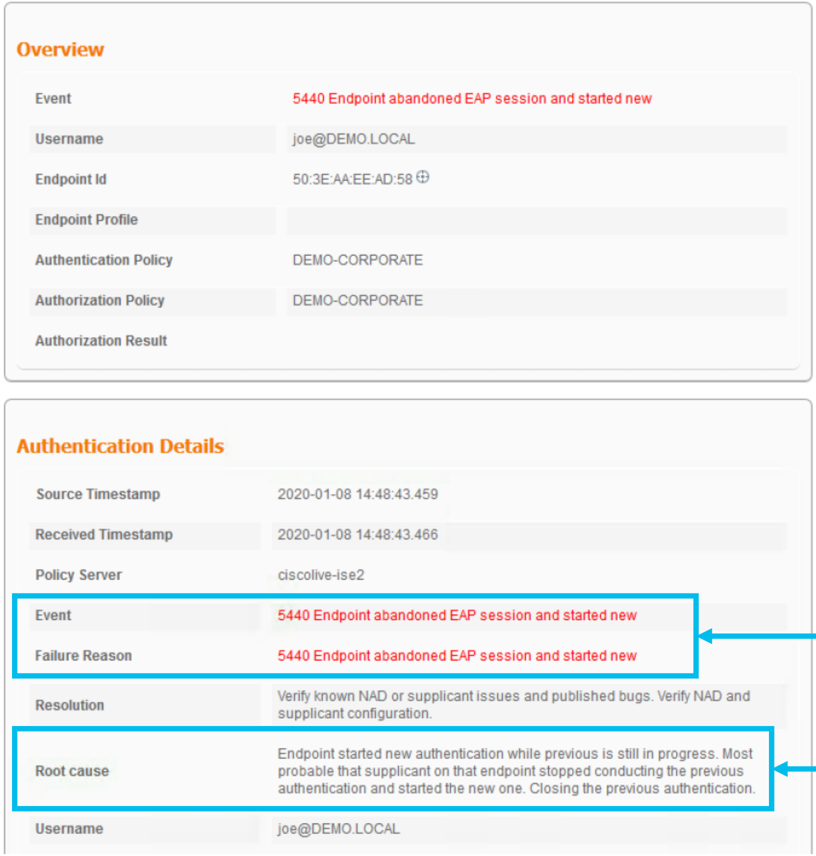
Refresh: Never
Show: Latest 100 records
Within

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy
×					50:3E:AA:EE:AD:58 ×			
Jan 08, 2020 02:48:43.466 PM	✖	🔍		joe@DEMO.LOCAL	50:3E:AA:EE:AD:58			
Jan 08, 2020 02:48:25.226 PM	✖	🔍		joe@DEMO.LOCAL	50:3E:AA:EE:AD:58			
Jan 08, 2020 02:48:06.992 PM	✖	🔍		joe@DEMO.LOCAL	50:3E:AA:EE:AD:58			

Identity of the user which is trying to connect

MAC address of the user to confirm correct log message

Live Logs > Detailed authentication report



Overview

Event	5440 Endpoint abandoned EAP session and started new
Username	joe@DEMO.LOCAL
Endpoint Id	50:3E:AA:EE:AD:58 ⊕
Endpoint Profile	
Authentication Policy	DEMO-CORPORATE
Authorization Policy	DEMO-CORPORATE
Authorization Result	

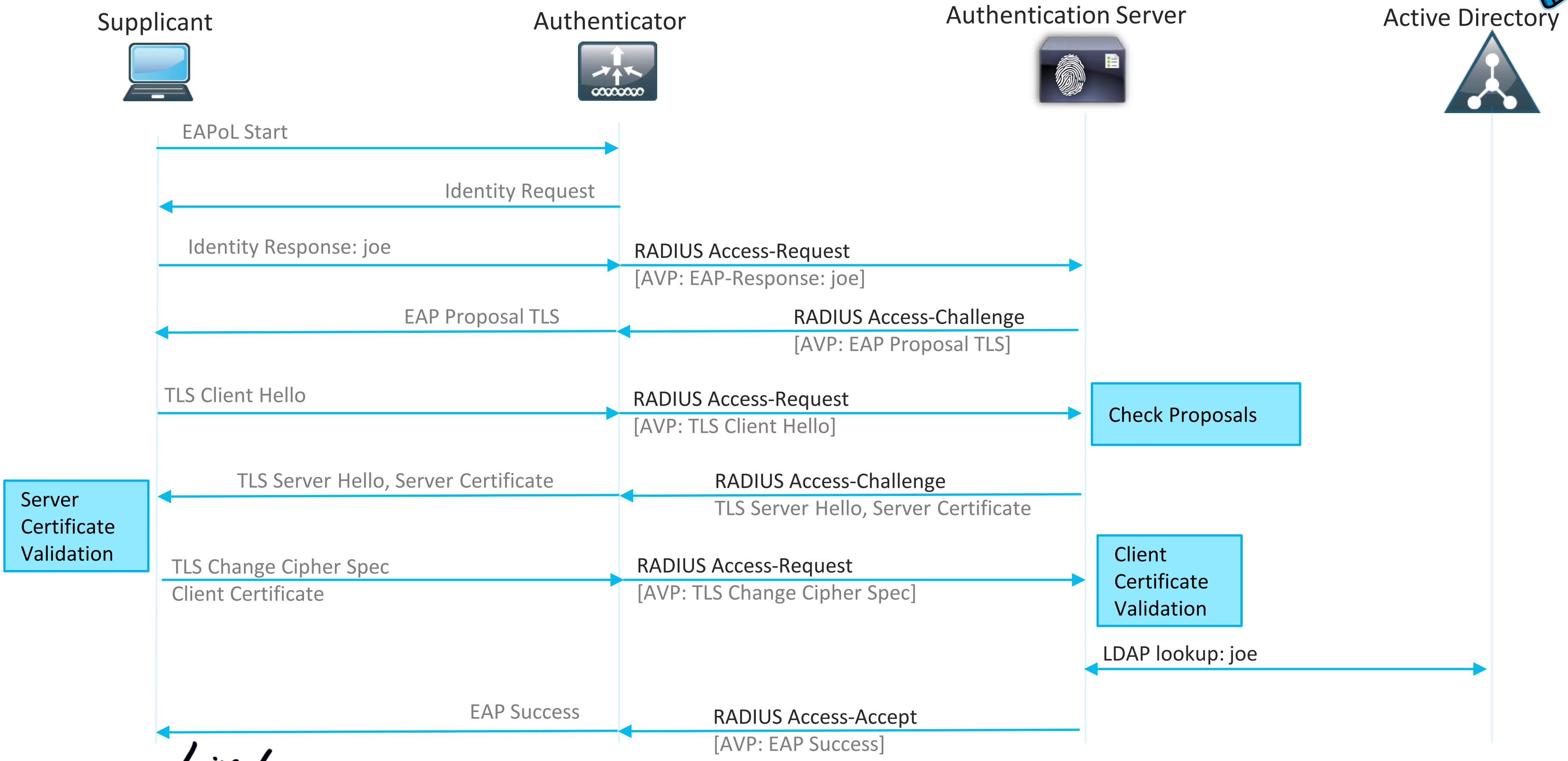
Authentication Details

Source Timestamp	2020-01-08 14:48:43.459
Received Timestamp	2020-01-08 14:48:43.466
Policy Server	ciscolive-ise2
Event	5440 Endpoint abandoned EAP session and started new
Failure Reason	5440 Endpoint abandoned EAP session and started new
Resolution	Verify known NAD or supplicant issues and published bugs. Verify NAD and supplicant configuration.
Root cause	Endpoint started new authentication while previous is still in progress. Most probable that supplicant on that endpoint stopped conducting the previous authentication and started the new one. Closing the previous authentication.
Username	joe@DEMO.LOCAL

Endpoint abandoned EAP session and started new

Most probable that supplicant on that endpoint stopped conducting the previous authentication and started the new one

EAP-TLS flow high level overview



Supplicant

Authenticator

Authentication Server

Active Directory

EAPoL Start

Identity Request

Identity Response: joe

RADIUS Access-Request
[AVP: EAP-Response: joe]

EAP Proposal TLS

RADIUS Access-Challenge
[AVP: EAP Proposal TLS]

TLS Client Hello

RADIUS Access-Request
[AVP: TLS Client Hello]

Check Proposals

TLS Server Hello, Server Certificate

RADIUS Access-Challenge
TLS Server Hello, Server Certificate

Server Certificate Validation

TLS Change Cipher Spec
Client Certificate

RADIUS Access-Request
[AVP: TLS Change Cipher Spec]

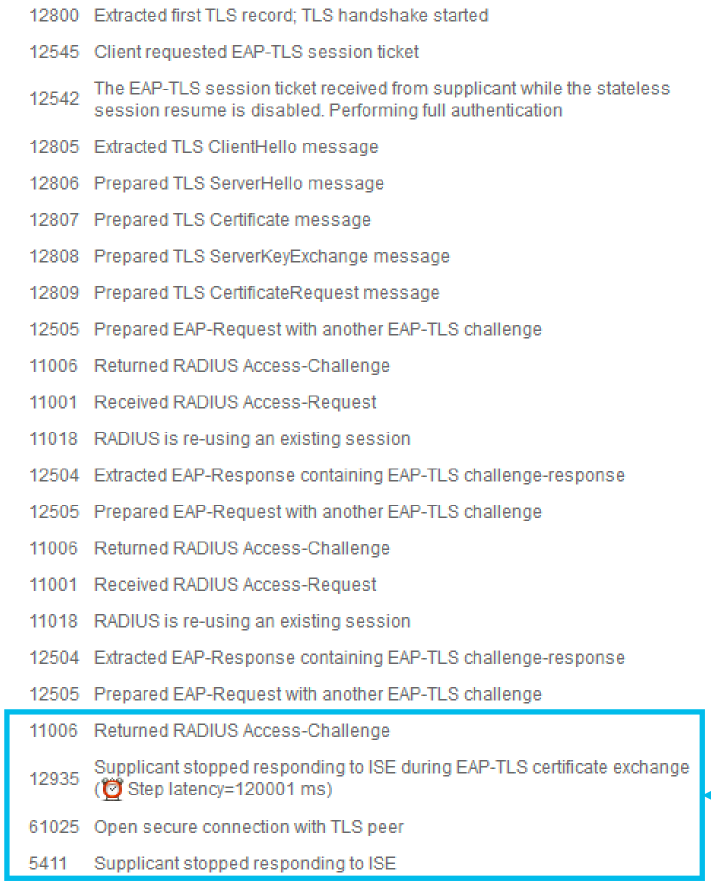
Client Certificate Validation

LDAP lookup: joe

EAP Success

RADIUS Access-Accept
[AVP: EAP Success]

Live Logs > Detailed authentication report

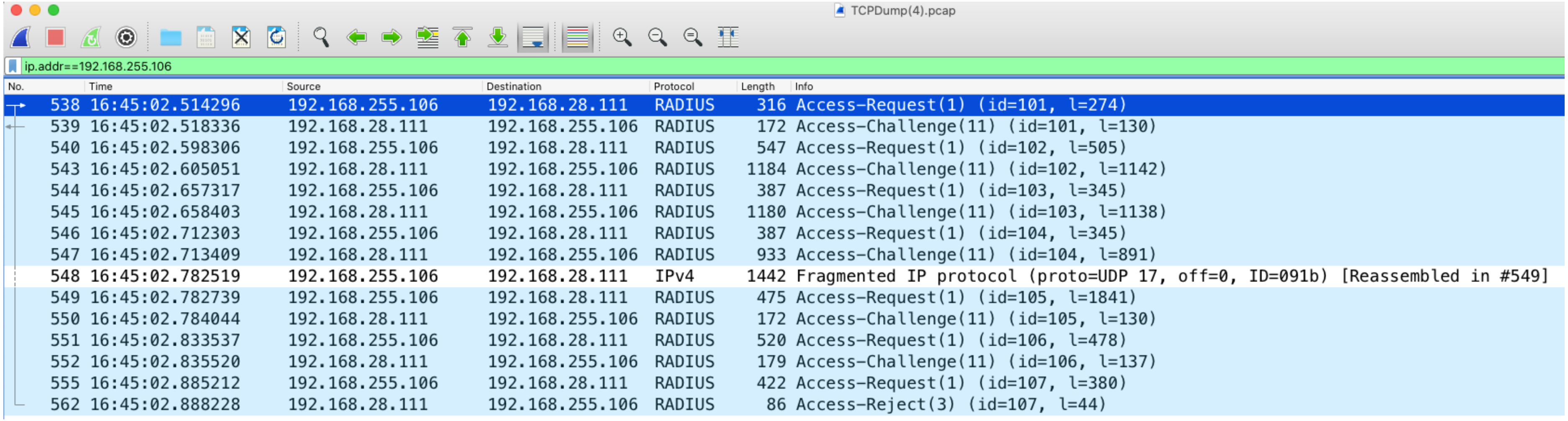


```
12800   Extracted first TLS record; TLS handshake started
12545   Client requested EAP-TLS session ticket
12542   The EAP-TLS session ticket received from supplicant while the stateless
        session resume is disabled. Performing full authentication
12805   Extracted TLS ClientHello message
12806   Prepared TLS ServerHello message
12807   Prepared TLS Certificate message
12808   Prepared TLS ServerKeyExchange message
12809   Prepared TLS CertificateRequest message
12505   Prepared EAP-Request with another EAP-TLS challenge
11006   Returned RADIUS Access-Challenge
11001   Received RADIUS Access-Request
11018   RADIUS is re-using an existing session
12504   Extracted EAP-Response containing EAP-TLS challenge-response
12505   Prepared EAP-Request with another EAP-TLS challenge
11006   Returned RADIUS Access-Challenge
11001   Received RADIUS Access-Request
11018   RADIUS is re-using an existing session
12504   Extracted EAP-Response containing EAP-TLS challenge-response
12505   Prepared EAP-Request with another EAP-TLS challenge
11006   Returned RADIUS Access-Challenge
12935   Supplicant stopped responding to ISE during EAP-TLS certificate exchange
        (⏰ Step latency=120001 ms)
61025   Open secure connection with TLS peer
5411    Supplicant stopped responding to ISE
```

Access-Challenge is sent with no Reply

Comparing Packet captures

Upstream Switch

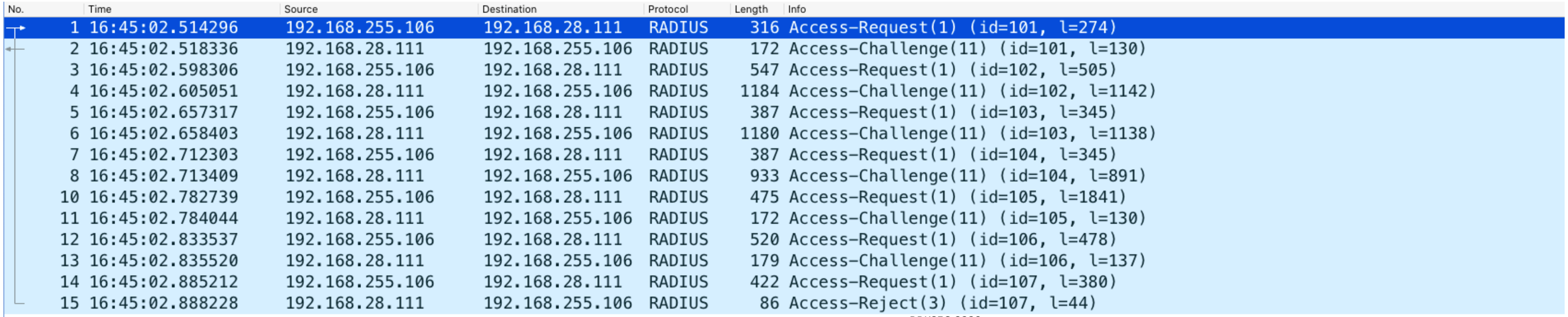


TCPDump(4).pcap

ip.addr==192.168.255.106

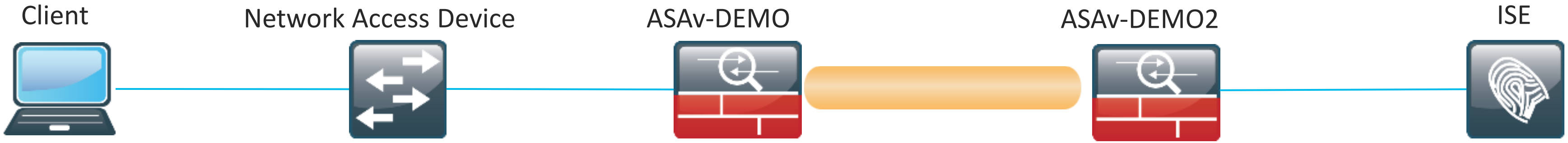
```
No.  Time             Source           Destination      Protocol  Length Info
538 16:45:02.514296  192.168.255.106  192.168.28.111   RADIUS     316 Access-Request(1) (id=101, l=274)
539 16:45:02.518336  192.168.28.111   192.168.255.106  RADIUS     172 Access-Challenge(11) (id=101, l=130)
540 16:45:02.598306  192.168.255.106  192.168.28.111   RADIUS     547 Access-Request(1) (id=102, l=505)
543 16:45:02.605051  192.168.28.111   192.168.255.106  RADIUS    1184 Access-Challenge(11) (id=102, l=1142)
544 16:45:02.657317  192.168.255.106  192.168.28.111   RADIUS     387 Access-Request(1) (id=103, l=345)
545 16:45:02.658403  192.168.28.111   192.168.255.106  RADIUS    1180 Access-Challenge(11) (id=103, l=1138)
546 16:45:02.712303  192.168.255.106  192.168.28.111   RADIUS     387 Access-Request(1) (id=104, l=345)
547 16:45:02.713409  192.168.28.111   192.168.255.106  RADIUS     933 Access-Challenge(11) (id=104, l=891)
548 16:45:02.782519  192.168.255.106  192.168.28.111   IPv4      1442 Fragmented IP protocol (proto=UDP 17, off=0, ID=091b) [Reassembled in #549]
549 16:45:02.782739  192.168.255.106  192.168.28.111   RADIUS     475 Access-Request(1) (id=105, l=1841)
550 16:45:02.784044  192.168.28.111   192.168.255.106  RADIUS     172 Access-Challenge(11) (id=105, l=130)
551 16:45:02.833537  192.168.255.106  192.168.28.111   RADIUS     520 Access-Request(1) (id=106, l=478)
552 16:45:02.835520  192.168.28.111   192.168.255.106  RADIUS     179 Access-Challenge(11) (id=106, l=137)
555 16:45:02.885212  192.168.255.106  192.168.28.111   RADIUS     422 Access-Request(1) (id=107, l=380)
562 16:45:02.888228  192.168.28.111   192.168.255.106  RADIUS      86 Access-Reject(3) (id=107, l=44)
```

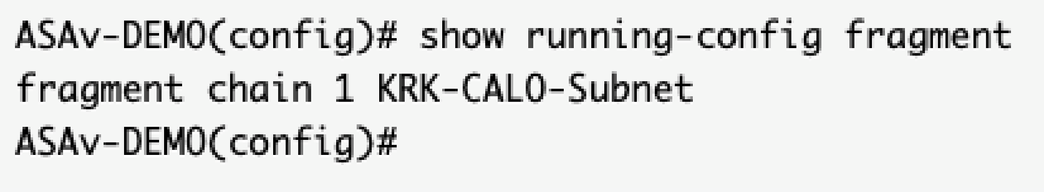
ISE



```
No.  Time             Source           Destination      Protocol  Length Info
  1 16:45:02.514296  192.168.255.106  192.168.28.111   RADIUS     316 Access-Request(1) (id=101, l=274)
  2 16:45:02.518336  192.168.28.111   192.168.255.106  RADIUS     172 Access-Challenge(11) (id=101, l=130)
  3 16:45:02.598306  192.168.255.106  192.168.28.111   RADIUS     547 Access-Request(1) (id=102, l=505)
  4 16:45:02.605051  192.168.28.111   192.168.255.106  RADIUS    1184 Access-Challenge(11) (id=102, l=1142)
  5 16:45:02.657317  192.168.255.106  192.168.28.111   RADIUS     387 Access-Request(1) (id=103, l=345)
  6 16:45:02.658403  192.168.28.111   192.168.255.106  RADIUS    1180 Access-Challenge(11) (id=103, l=1138)
  7 16:45:02.712303  192.168.255.106  192.168.28.111   RADIUS     387 Access-Request(1) (id=104, l=345)
  8 16:45:02.713409  192.168.28.111   192.168.255.106  RADIUS     933 Access-Challenge(11) (id=104, l=891)
 10 16:45:02.782739  192.168.255.106  192.168.28.111   RADIUS     475 Access-Request(1) (id=105, l=1841)
 11 16:45:02.784044  192.168.28.111   192.168.255.106  RADIUS     172 Access-Challenge(11) (id=105, l=130)
 12 16:45:02.833537  192.168.255.106  192.168.28.111   RADIUS     520 Access-Request(1) (id=106, l=478)
 13 16:45:02.835520  192.168.28.111   192.168.255.106  RADIUS     179 Access-Challenge(11) (id=106, l=137)
 14 16:45:02.885212  192.168.255.106  192.168.28.111   RADIUS     422 Access-Request(1) (id=107, l=380)
 15 16:45:02.888228  192.168.28.111   192.168.255.106  RADIUS      86 Access-Reject(3) (id=107, l=44)
```

Confirming the theory – issue 3



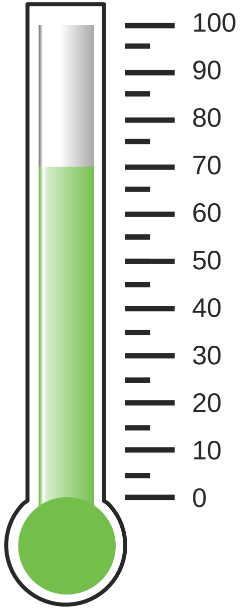


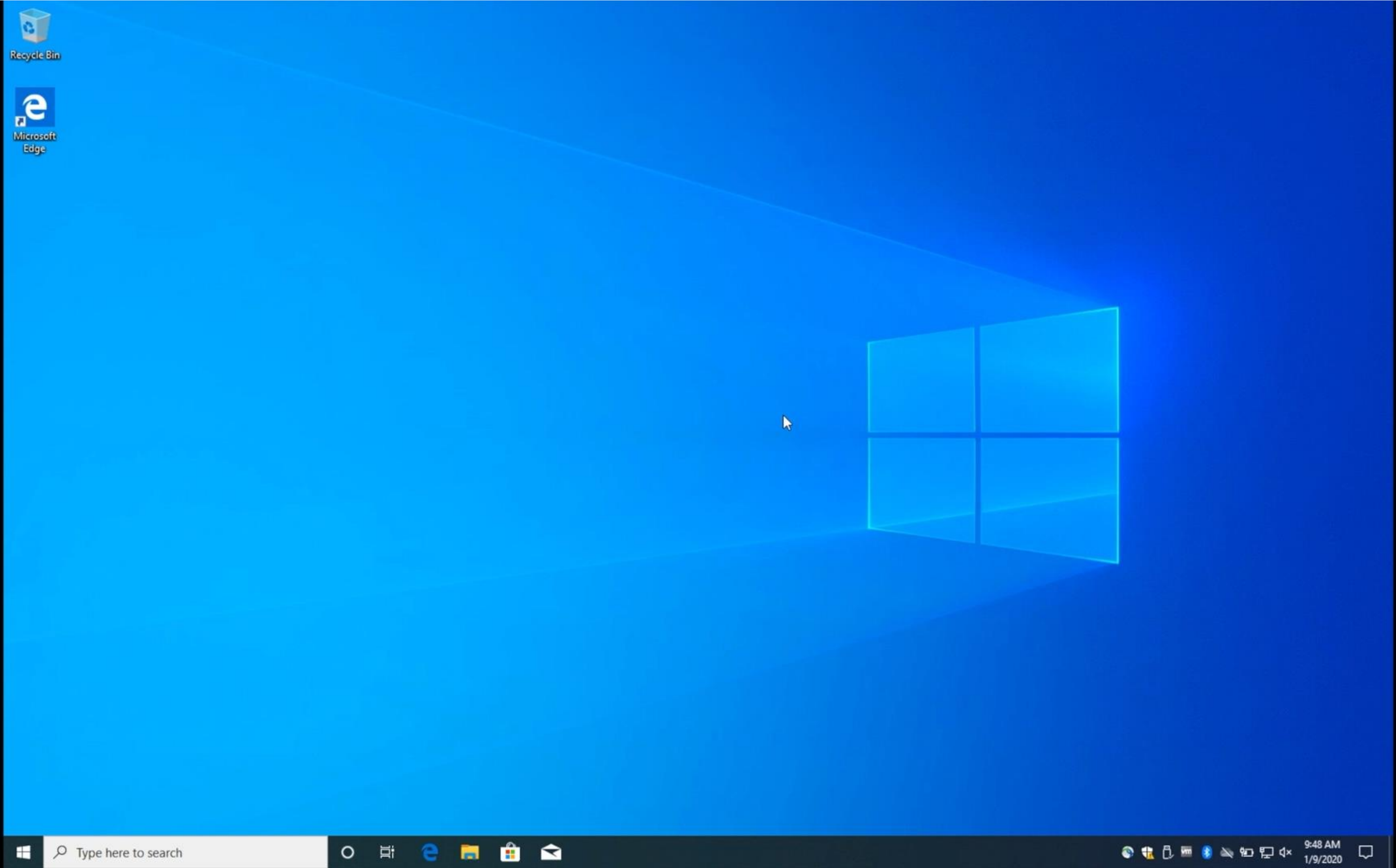
```
ASAv-DEMO(config)# show running-config fragment
fragment chain 1 KRK-CALO-Subnet
ASAv-DEMO(config)#
```

Issue 2: Security Team implemented fragmentation attack protection by disabling fragments to pass the firewalls, this caused ip fragments of Radius packets to be dropped
Solution 2: Allow fragmentation on the interfaces within NAD <> ISE path

Issue 4

Meeting’s success scale



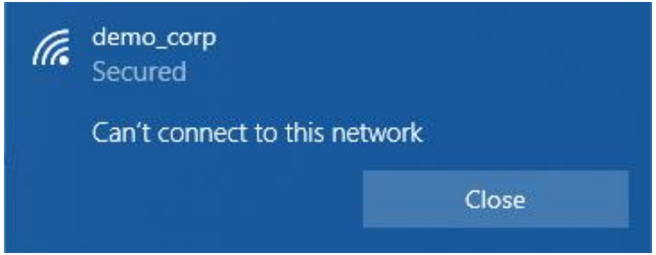

Recycle Bin
Microsoft Edge
Type here to search
9:48 AM
1/9/2020

Define the problem – issue 4

Users can’t connect to the wireless network, “demo_corp” connection is failing with the error message “Can’t connect to this network”

Supporting facts

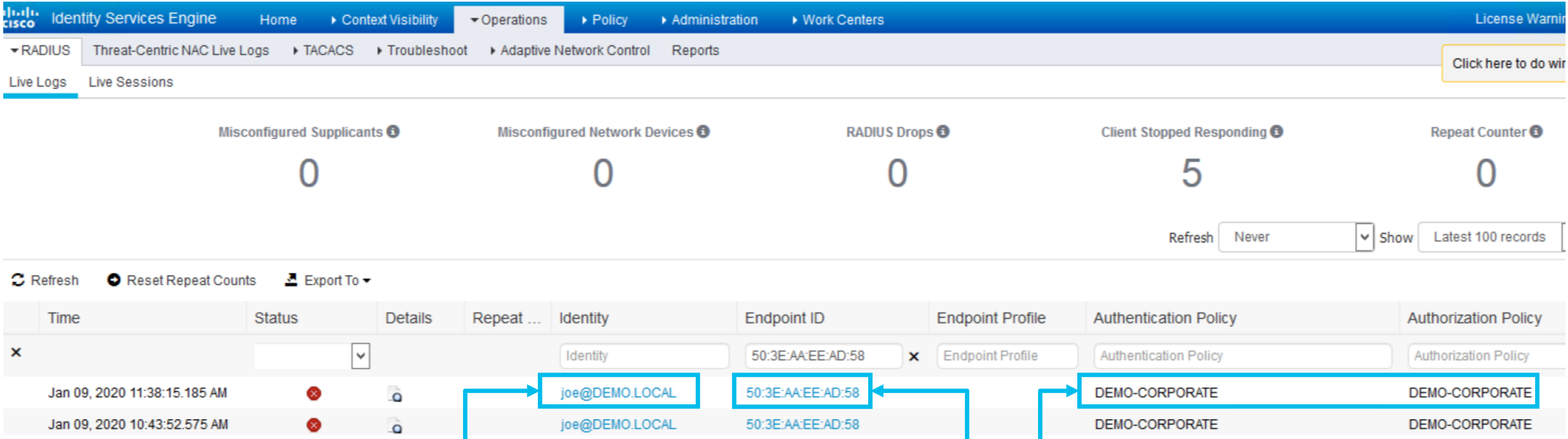
- Demo_corp is company wide corporate SSID
- Few other users reported the same issue after the weekend



demo_corp
Secured

Can’t connect to this network

Operations > Radius > Live Logs



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	5	0

Refresh: Never Show: Latest 100 records

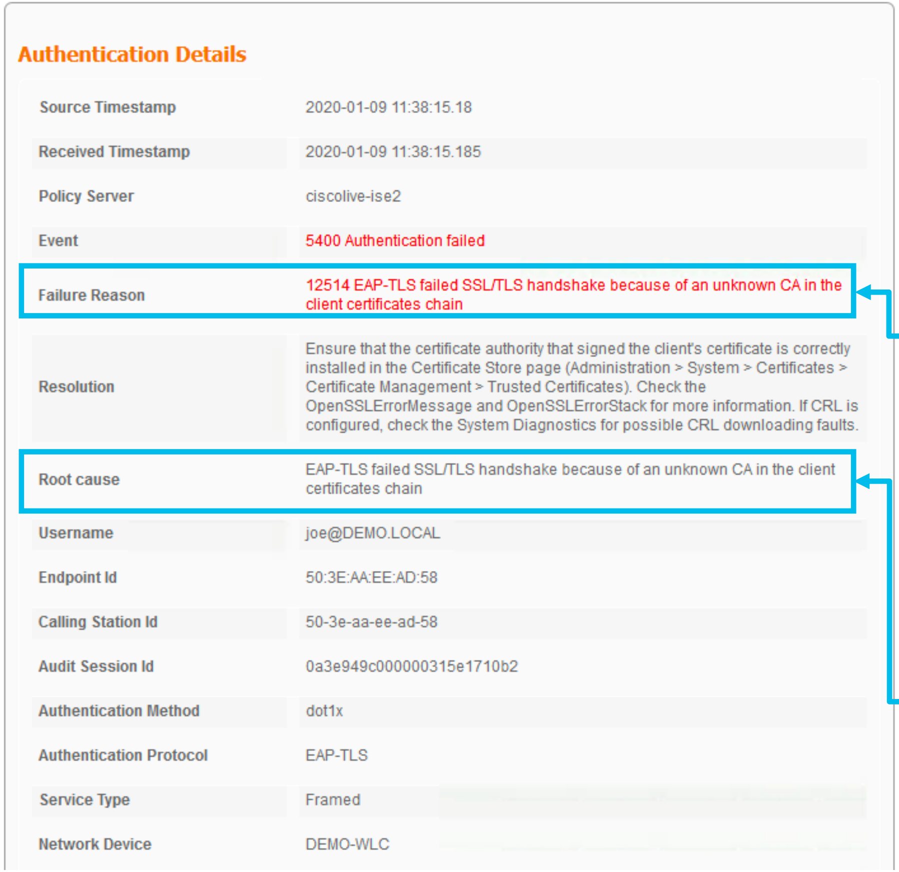
Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy
				Identity	50:3E:AA:EE:AD:58	Endpoint Profile	Authentication Policy	Authorization Policy
Jan 09, 2020 11:38:15.185 AM	⊗			joe@DEMO.LOCAL	50:3E:AA:EE:AD:58		DEMO-CORPORATE	DEMO-CORPORATE
Jan 09, 2020 10:43:52.575 AM	⊗			joe@DEMO.LOCAL	50:3E:AA:EE:AD:58		DEMO-CORPORATE	DEMO-CORPORATE

Identity of the user which is trying to connect

MAC address of the user to confirm correct log message

Selected Authentication and Authorization Policy indicate rules which were matched

Live Logs > Detailed authentication report



Authentication Details

Source Timestamp	2020-01-09 11:38:15.18
Received Timestamp	2020-01-09 11:38:15.185
Policy Server	ciscolive-ise2
Event	5400 Authentication failed
Failure Reason	12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain
Resolution	Ensure that the certificate authority that signed the client's certificate is correctly installed in the Certificate Store page (Administration > System > Certificates > Certificate Management > Trusted Certificates). Check the OpenSSLErrorMessage and OpenSSLErrorStack for more information. If CRL is configured, check the System Diagnostics for possible CRL downloading faults.
Root cause	EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain
Username	joe@DEMO.LOCAL
Endpoint Id	50:3E:AA:EE:AD:58
Calling Station Id	50-3e-aa-ee-ad-58
Audit Session Id	0a3e949c000000315e1710b2
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	DEMO-WLC

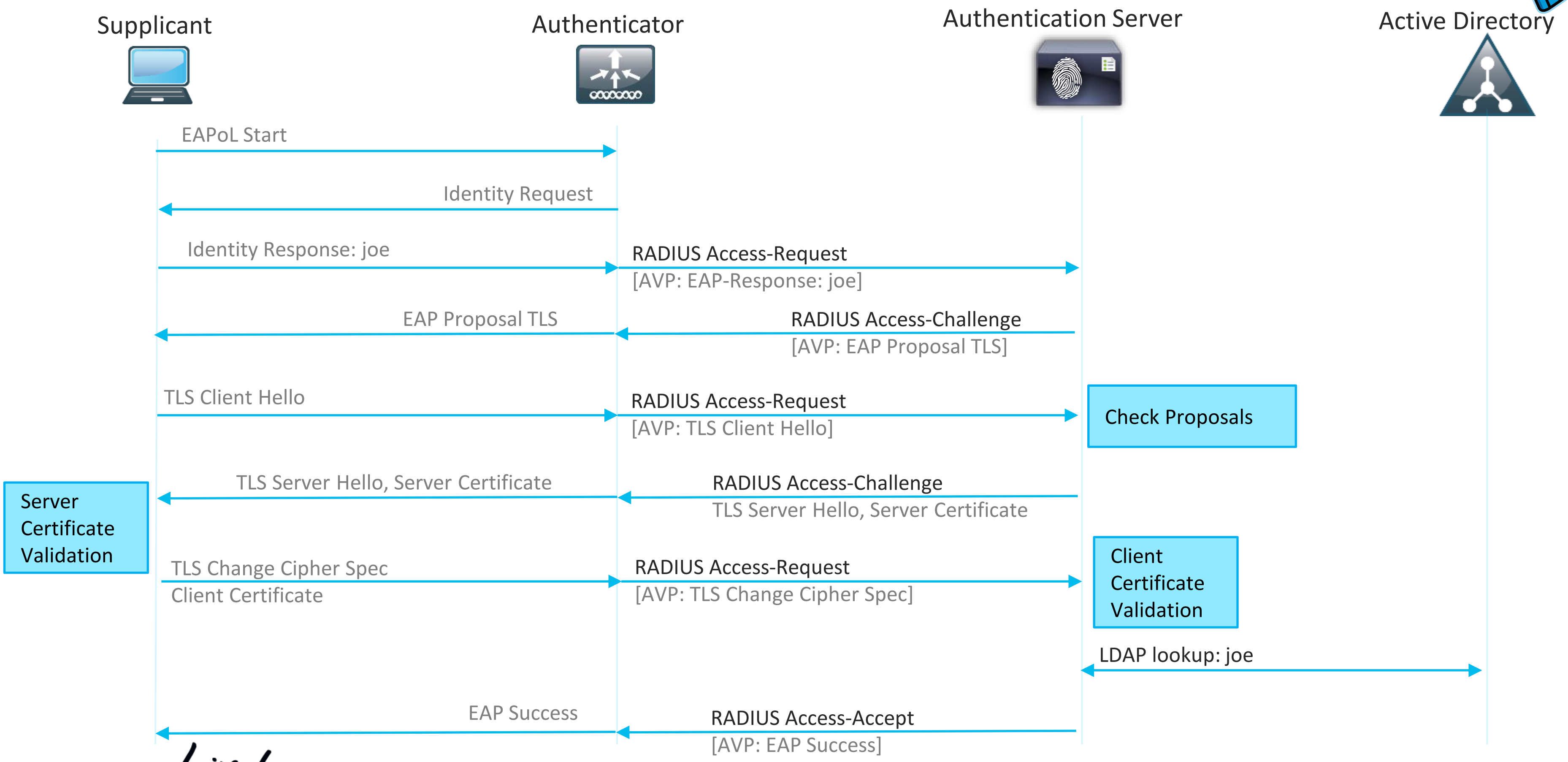
12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain

Server doesn’t trust client certificates in the chain

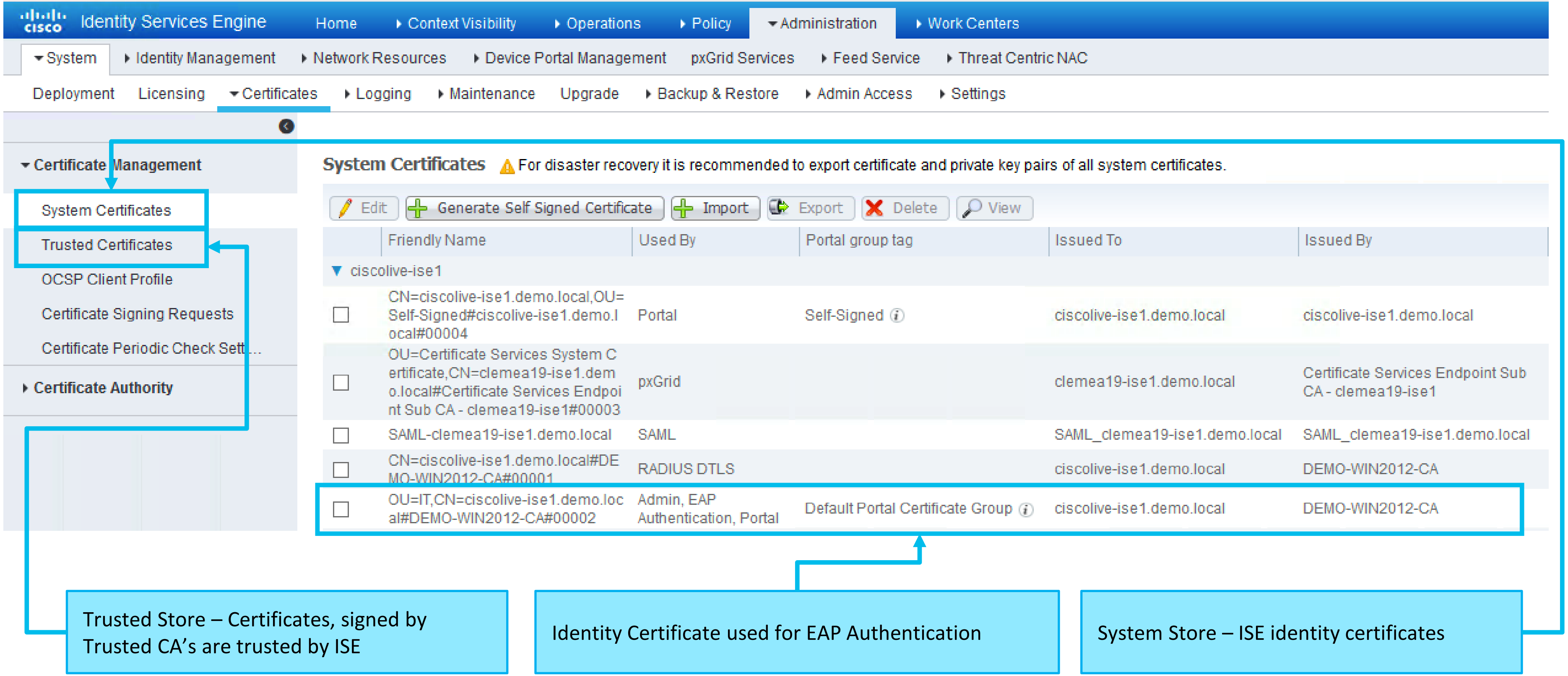
Ensure that the certificate authority that signed the client's certificate is correctly installed in the Certificate Store page (Administration > System > Certificates > Certificate Management > Trusted Certificates). Check the OpenSSLErrorMessage and OpenSSLErrorStack for more information. If CRL is configured, check the System Diagnostics for possible CRL downloading faults.

Ensure that clients CA is Trusted (installed in the trusted store) and valid to be used for EAP authentication

EAP-TLS flow high level overview



Certificate Based Authentication. ISE System Store



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

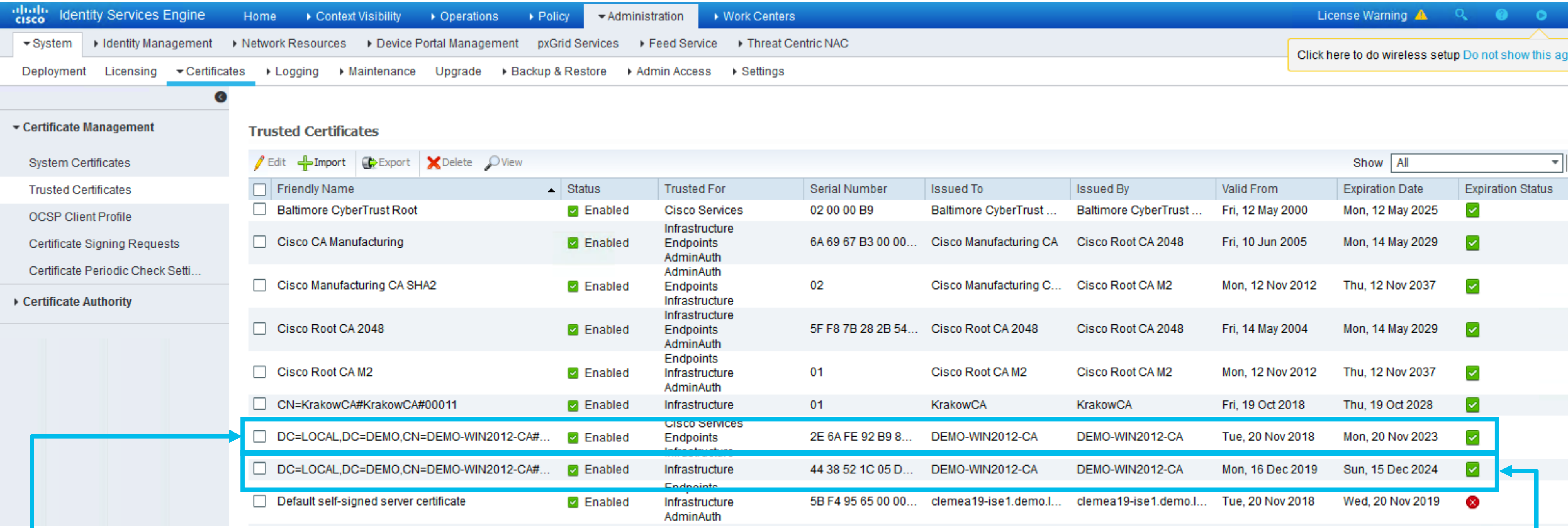
	Friendly Name	Used By	Portal group tag	Issued To	Issued By
▼ ciscolive-ise1					
□	CN=ciscolive-ise1.demo.local,OU=Self-Signed#ciscolive-ise1.demo.local#00004	Portal	Self-Signed ⓘ	ciscolive-ise1.demo.local	ciscolive-ise1.demo.local
□	OU=Certificate Services System Certificate,CN=clemea19-ise1.demo.local#Certificate Services Endpoint Sub CA - clemea19-ise1#00003	pxGrid		clemea19-ise1.demo.local	Certificate Services Endpoint Sub CA - clemea19-ise1
□	SAML-clemea19-ise1.demo.local	SAML		SAML_clemea19-ise1.demo.local	SAML_clemea19-ise1.demo.local
□	CN=ciscolive-ise1.demo.local#DEMO-WIN2012-CA#00001	RADIUS DTLS		ciscolive-ise1.demo.local	DEMO-WIN2012-CA
□	OU=IT,CN=ciscolive-ise1.demo.local#DEMO-WIN2012-CA#00002	Admin, EAP Authentication, Portal	Default Portal Certificate Group ⓘ	ciscolive-ise1.demo.local	DEMO-WIN2012-CA

Trusted Store – Certificates, signed by Trusted CA's are trusted by ISE

Identity Certificate used for EAP Authentication

System Store – ISE identity certificates

Certificate Based Authentication. ISE Trusted Store



Trusted Certificates

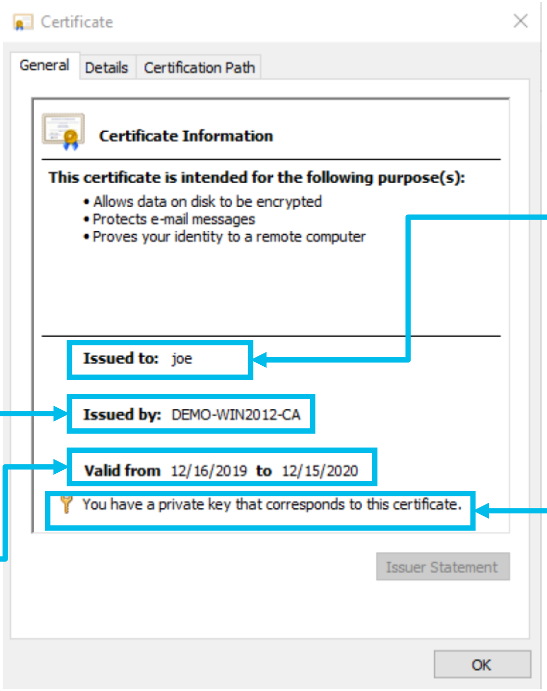
□	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
□	Baltimore CyberTrust Root	✓ Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust ...	Baltimore CyberTrust ...	Fri, 12 May 2000	Mon, 12 May 2025	✓
□	Cisco CA Manufacturing	✓ Enabled	Infrastructure Endpoints AdminAuth	6A 69 67 B3 00 00...	Cisco Manufacturing CA	Cisco Root CA 2048	Fri, 10 Jun 2005	Mon, 14 May 2029	✓
□	Cisco Manufacturing CA SHA2	✓ Enabled	AdminAuth Endpoints Infrastructure	02	Cisco Manufacturing C...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	✓
□	Cisco Root CA 2048	✓ Enabled	Infrastructure Endpoints AdminAuth	5F F8 7B 28 2B 54...	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 2029	✓
□	Cisco Root CA M2	✓ Enabled	Endpoints Infrastructure AdminAuth	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	✓
□	CN=KrakowCA#KrakowCA#00011	✓ Enabled	Infrastructure	01	KrakowCA	KrakowCA	Fri, 19 Oct 2018	Thu, 19 Oct 2028	✓
□	DC=LOCAL,DC=DEMO,CN=DEMO-WIN2012-CA#...	✓ Enabled	Cisco Services Endpoints Infrastructure	2E 6A FE 92 B9 8...	DEMO-WIN2012-CA	DEMO-WIN2012-CA	Tue, 20 Nov 2018	Mon, 20 Nov 2023	✓
□	DC=LOCAL,DC=DEMO,CN=DEMO-WIN2012-CA#...	✓ Enabled	Infrastructure	44 38 52 1C 05 D...	DEMO-WIN2012-CA	DEMO-WIN2012-CA	Mon, 16 Dec 2019	Sun, 15 Dec 2024	✓
□	Default self-signed server certificate	✓ Enabled	Endpoints Infrastructure AdminAuth	5B F4 95 65 00 00...	clemea19-ise1.demo.l...	clemea19-ise1.demo.l...	Tue, 20 Nov 2018	Wed, 20 Nov 2019	✗

DEMO CA is installed in the ISE Trusted Store

CSCvj31598 Import two CA certs with same subject name (Available 2.4 patch 8 +)

Another DEMO CA is installed in the ISE Trusted Store

Certificate Based Authentication. Endpoint



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Allows data on disk to be encrypted
- Protects e-mail messages
- Proves your identity to a remote computer

Issued to: joe

Issued by: DEMO-WIN2012-CA

Valid from 12/16/2019 **to** 12/15/2020

You have a private key that corresponds to this certificate.

Issuer Statement

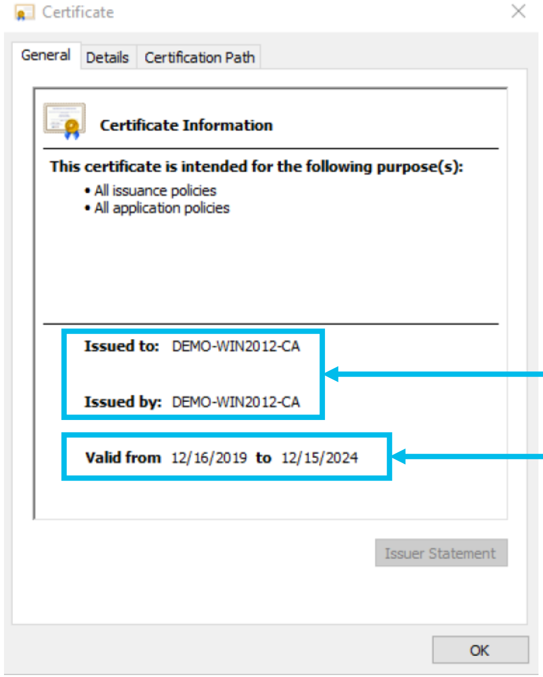
OK

Whom the certificate is issued to

Who issued the certificate

Certificate Validity

Confirmation on private key existence, which allows this certificate to be used to present the identity



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: DEMO-WIN2012-CA

Issued by: DEMO-WIN2012-CA

Valid from 12/16/2019 **to** 12/15/2024

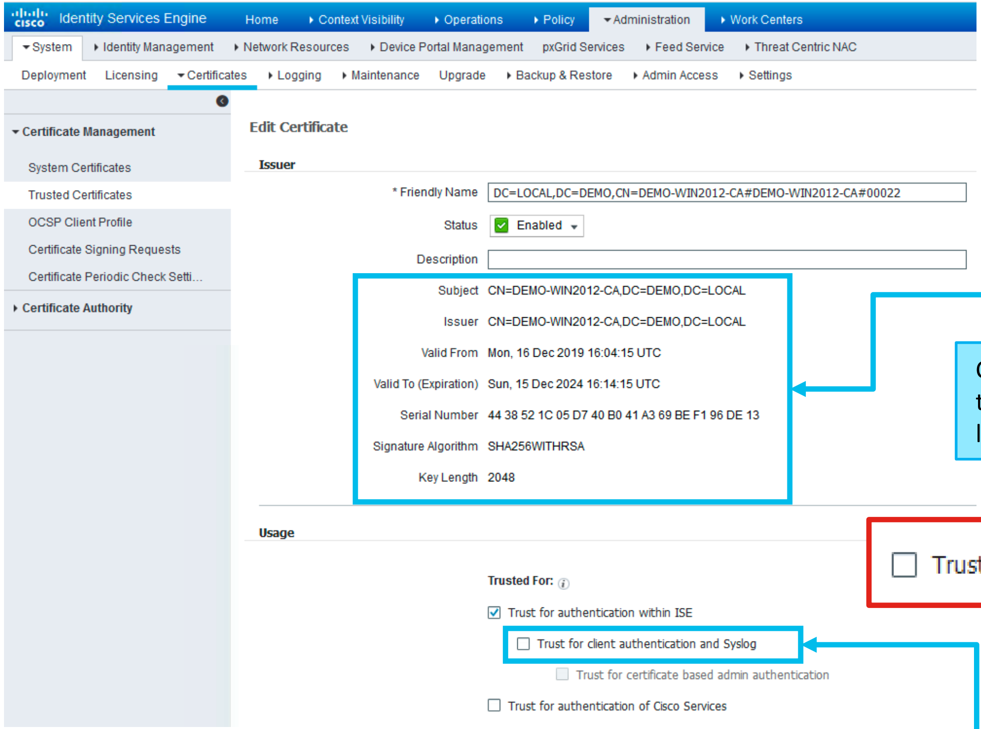
Issuer Statement

OK

CA Certificate

Validity of CA Certificate

Confirming the theory – issue 4



Edit Certificate

Issuer

* Friendly Name: DC=LOCAL,DC=DEMO,CN=DEMO-WIN2012-CA#DEMO-WIN2012-CA#00022

Status: ☑ Enabled

Description:

Subject: CN=DEMO-WIN2012-CA,DC=DEMO,DC=LOCAL

Issuer: CN=DEMO-WIN2012-CA,DC=DEMO,DC=LOCAL

Valid From: Mon, 16 Dec 2019 16:04:15 UTC

Valid To (Expiration): Sun, 15 Dec 2024 16:14:15 UTC

Serial Number: 44 38 52 1C 05 D7 40 B0 41 A3 69 BE F1 96 DE 13

Signature Algorithm: SHA256WITHRSA

Key Length: 2048

Usage

Trusted For:

☑ Trust for authentication within ISE

☐ Trust for client authentication and Syslog

☐ Trust for certificate based admin authentication

☐ Trust for authentication of Cisco Services

Certificate Fields to confirm that the right certificate is being looked at

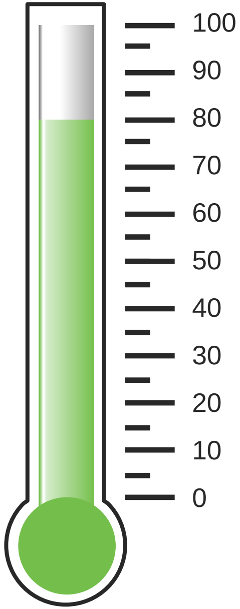
☐ Trust for client authentication and Syslog

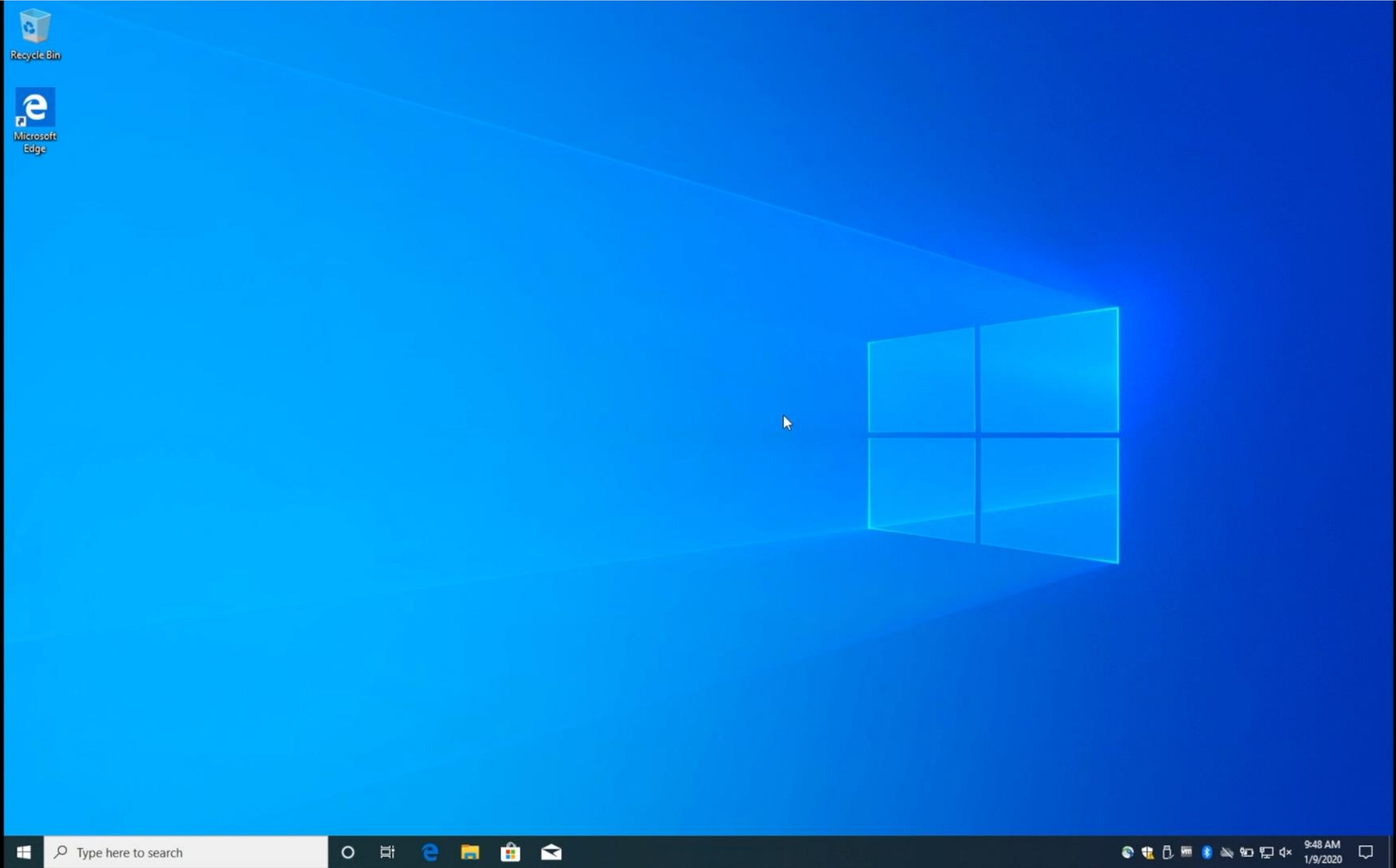
Issue 4: Enterprise CA was renewed. Some of the clients got new Certificates . New CA certificate was imported on ISE but not enabled for client authentication

Solution 4: Mark the checkbox “Trust for client authentication and Syslog” and Save

Issue 5

Meeting’s success scale



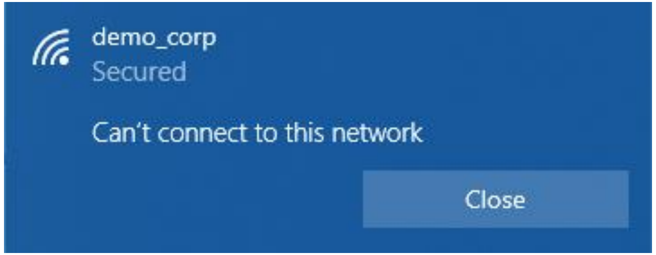

Recycle Bin
Microsoft Edge
Type here to search
9:48 AM
1/9/2020

Define the problem – issue 5

Users can’t connect to the wireless network, “demo_corp” connection is failing with the error message “Can’t connect to this network”

Supporting facts

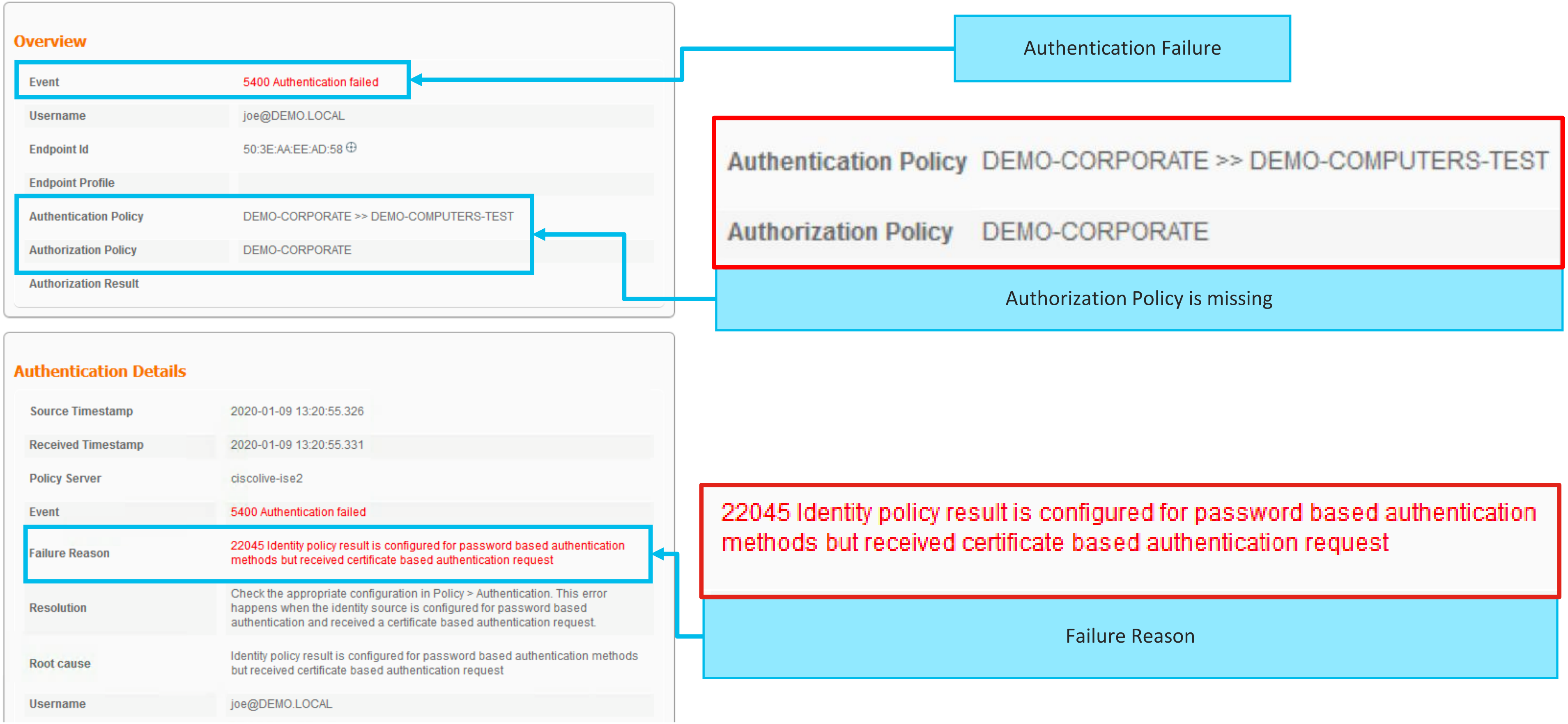
- Demo_corp is company wide corporate SSID



demo_corp
Secured

Can’t connect to this network

Live Logs - Detailed Authentication Report



Overview

Event	5400 Authentication failed
Username	joe@DEMO.LOCAL
Endpoint Id	50:3E:AA:EE:AD:58
Endpoint Profile	
Authentication Policy	DEMO-CORPORATE >> DEMO-COMPUTERS-TEST
Authorization Policy	DEMO-CORPORATE
Authorization Result	

Authentication Details

Source Timestamp	2020-01-09 13:20:55.326
Received Timestamp	2020-01-09 13:20:55.331
Policy Server	ciscolive-ise2
Event	5400 Authentication failed
Failure Reason	22045 Identity policy result is configured for password based authentication methods but received certificate based authentication request
Resolution	Check the appropriate configuration in Policy > Authentication. This error happens when the identity source is configured for password based authentication and received a certificate based authentication request.
Root cause	Identity policy result is configured for password based authentication methods but received certificate based authentication request
Username	joe@DEMO.LOCAL

Authentication Failure

Authentication Policy DEMO-CORPORATE >> DEMO-COMPUTERS-TEST

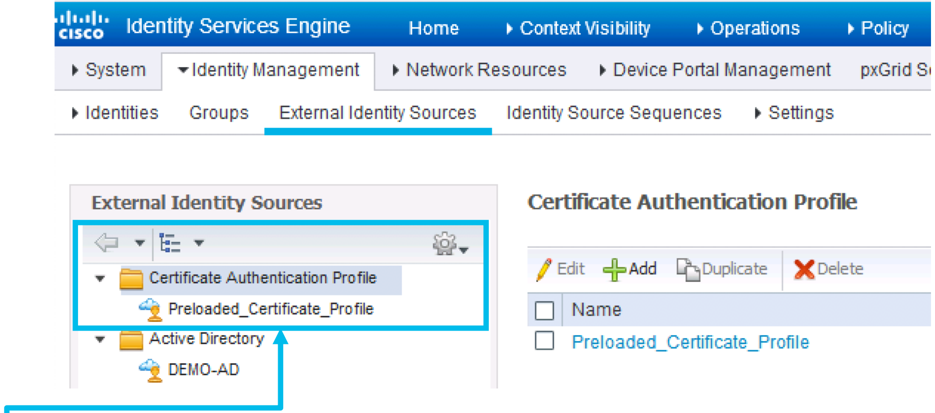
Authorization Policy DEMO-CORPORATE

Authorization Policy is missing

22045 Identity policy result is configured for password based authentication methods but received certificate based authentication request

Failure Reason

Certificate Based Authentication and Identity Sources

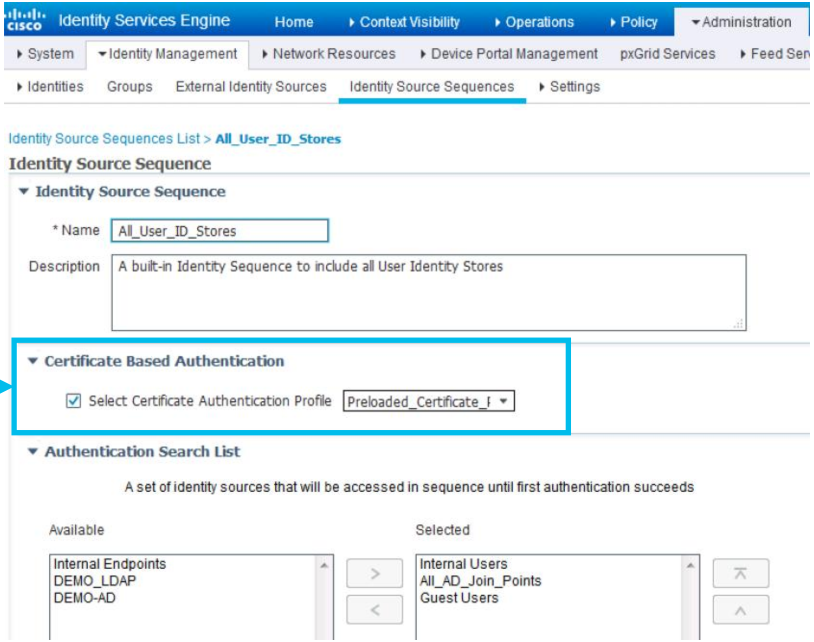


External Identity Sources

- Certificate Authentication Profile
  - Preloaded_Certificate_Profile
- Active Directory
  - DEMO-AD

Certificate Authentication Profile

□	Name
□	Preloaded_Certificate_Profile



Identity Source Sequences List > **All_User_ID_Stores**

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_I

Authentication Search List

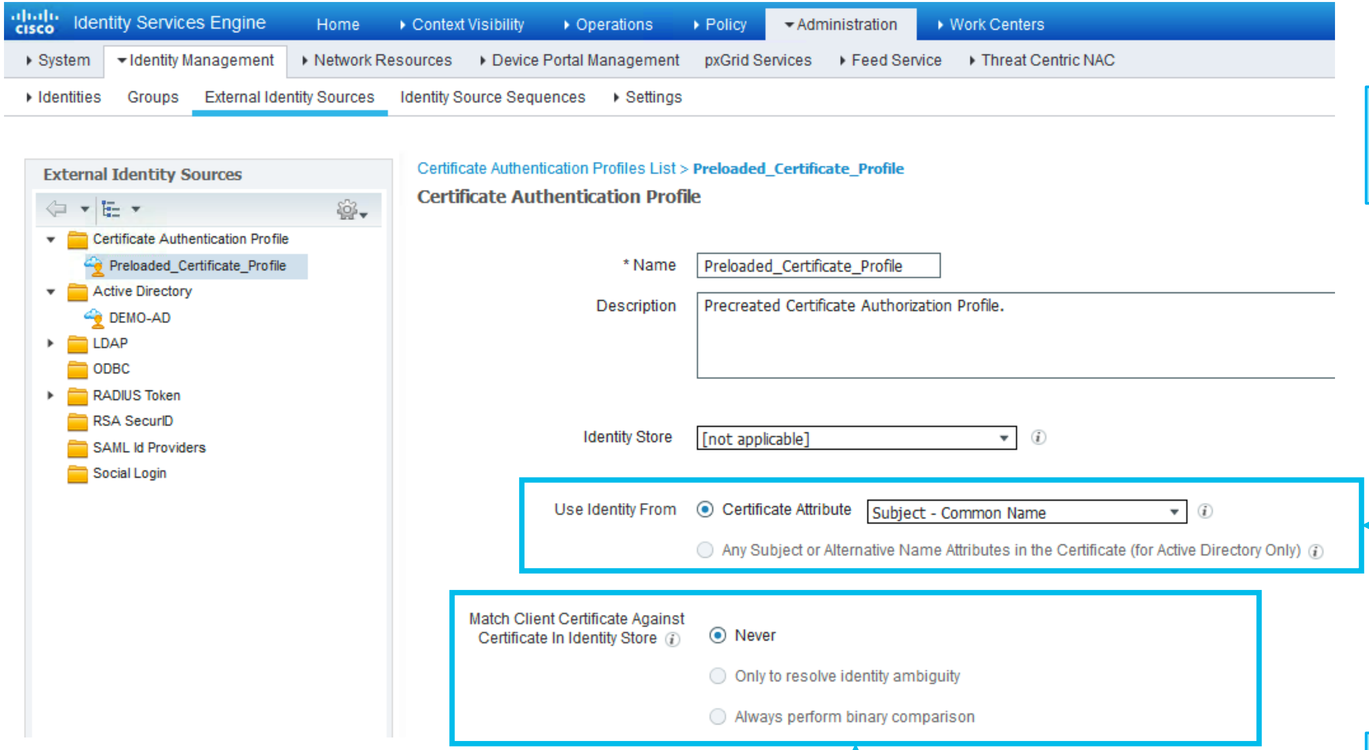
A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints DEMO_LDAP DEMO-AD	Internal Users All_AD_Join_Points Guest Users

Certificate Authentication Profile is "Identity Source" for EAP-TLS authentication

Certificate Authentication Profile needs to be referenced in Identity Source Sequence, if the Sequence is used for multiple Authentication methods

Certificate Based Authentication and Identity Sources



Certificate Authentication Profiles List > **Preloaded_Certificate_Profile**

Certificate Authentication Profile

* Name: Preloaded_Certificate_Profile

Description: Precreated Certificate Authorization Profile.

Identity Store: [not applicable]

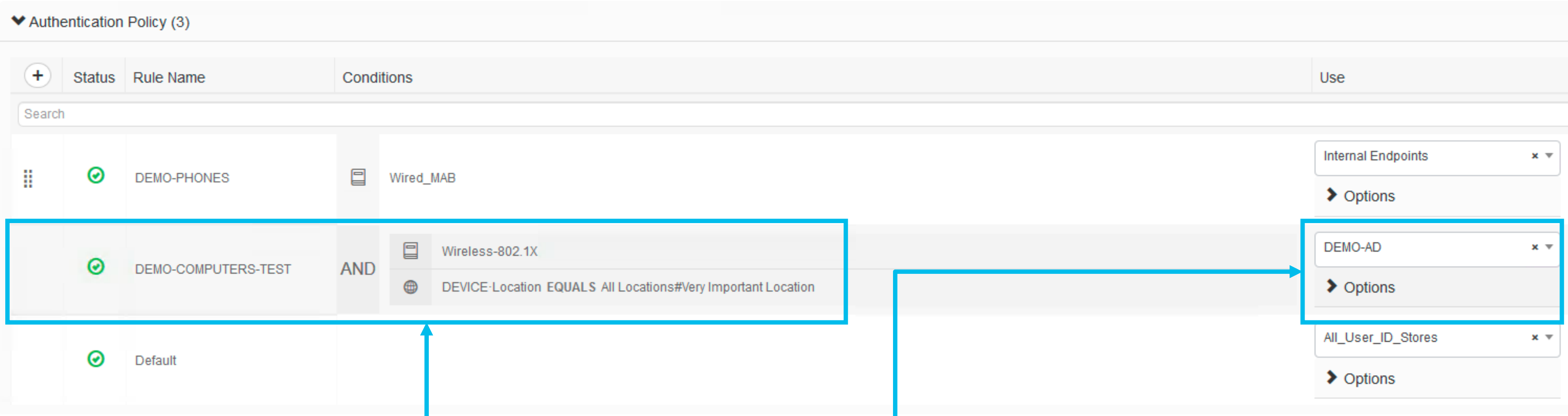
Use Identity From:
- ● Certificate Attribute: Subject - Common Name
- ○ Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate In Identity Store:
- ● Never
- ○ Only to resolve identity ambiguity
- ○ Always perform binary comparison

Use Identity From option instructs ISE which certificate attribute to be used as User Identity

Binary Certificate Comparison can be used to resolve ambiguity, certificate should exist as an attribute on Active Directory

Confirming the theory – issue 5



Authentication Policy (3)

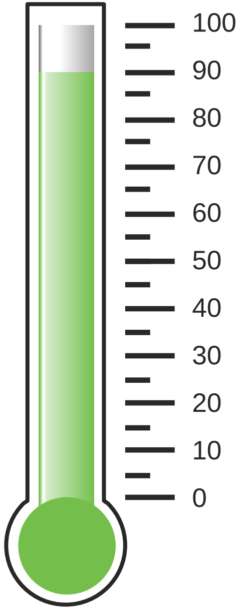
Status	Rule Name	Conditions	Use
✓	DEMO-PHONES	Wired_MAB	Internal Endpoints Options
✓	DEMO-COMPUTERS-TEST	AND Wireless-802.1X DEVICE·Location EQUALS All Locations#Very Important Location	DEMO-AD Options
✓	Default		All_User_ID_Stores Options

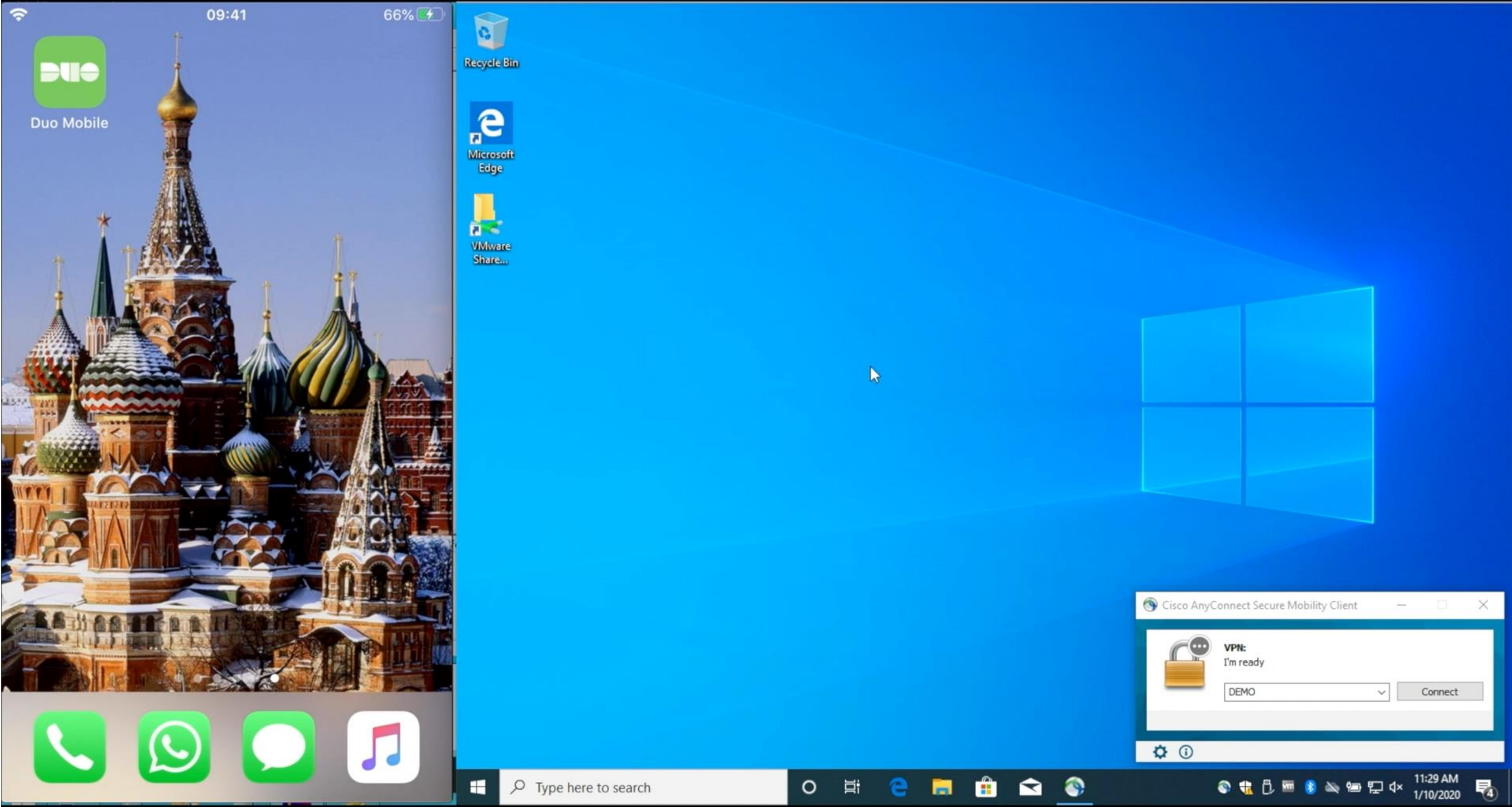
Authentication Policy DEMO-COMPUTERS-TEST was created with Active Directory as an Identity Store

Issue 5: EAP-TLS authentication expects Certificate Profile itself or Identity Source Sequence with Certificate Profile as an Identity Source, instead Active Directory was configured
Solution 5: Remove the TEST rule, so default All_User_ID_Store will take over

Issue 6

Meeting’s success scale





Cisco AnyConnect Secure Mobility Client

VPN:
I'm ready

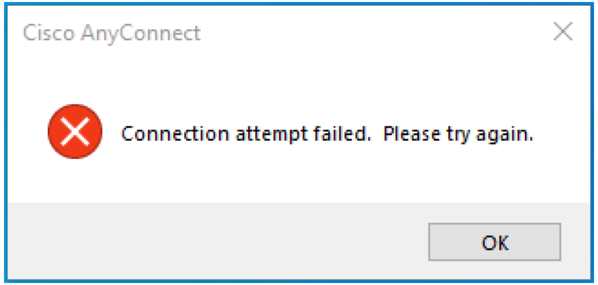
DEMO

Define the problem – issue 6

Users can’t connect to the VPN network, connection is failing with the error message “Connection attempt failed. Please try again”

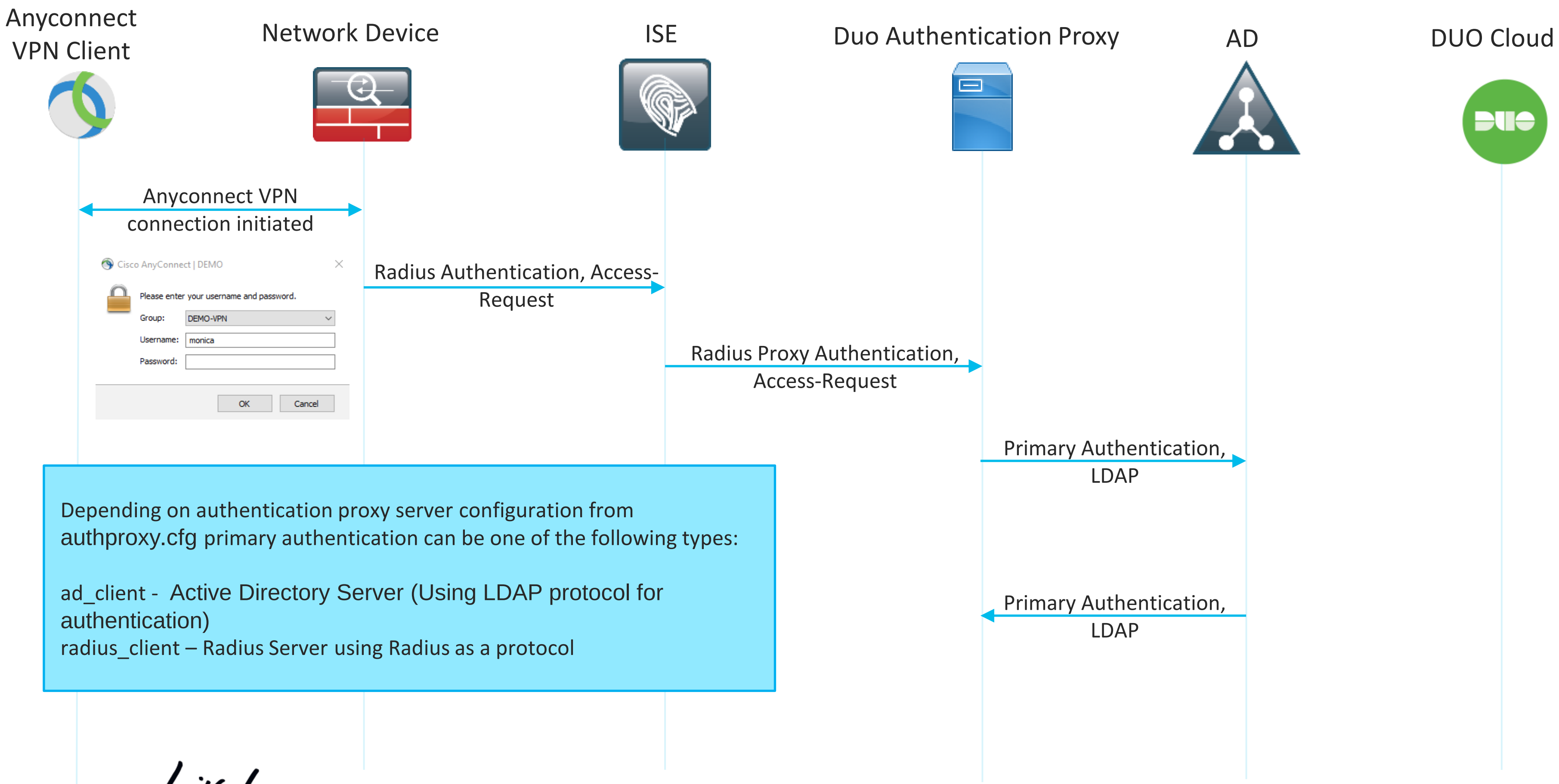
Supporting facts

- Issue is seen intermittently


Cisco AnyConnect

Connection attempt failed. Please try again.

Anyconnect MFA with DUO


Anyconnect VPN Client
Network Device
ISE
Duo Authentication Proxy
AD
DUO Cloud
Anyconnect VPN connection initiated
Radius Authentication, Access-Request
Radius Proxy Authentication, Access-Request
Primary Authentication, LDAP
Primary Authentication, LDAP

Cisco AnyConnect | DEMO

Please enter your username and password.

Group: DEMO-VPN

Username: monica

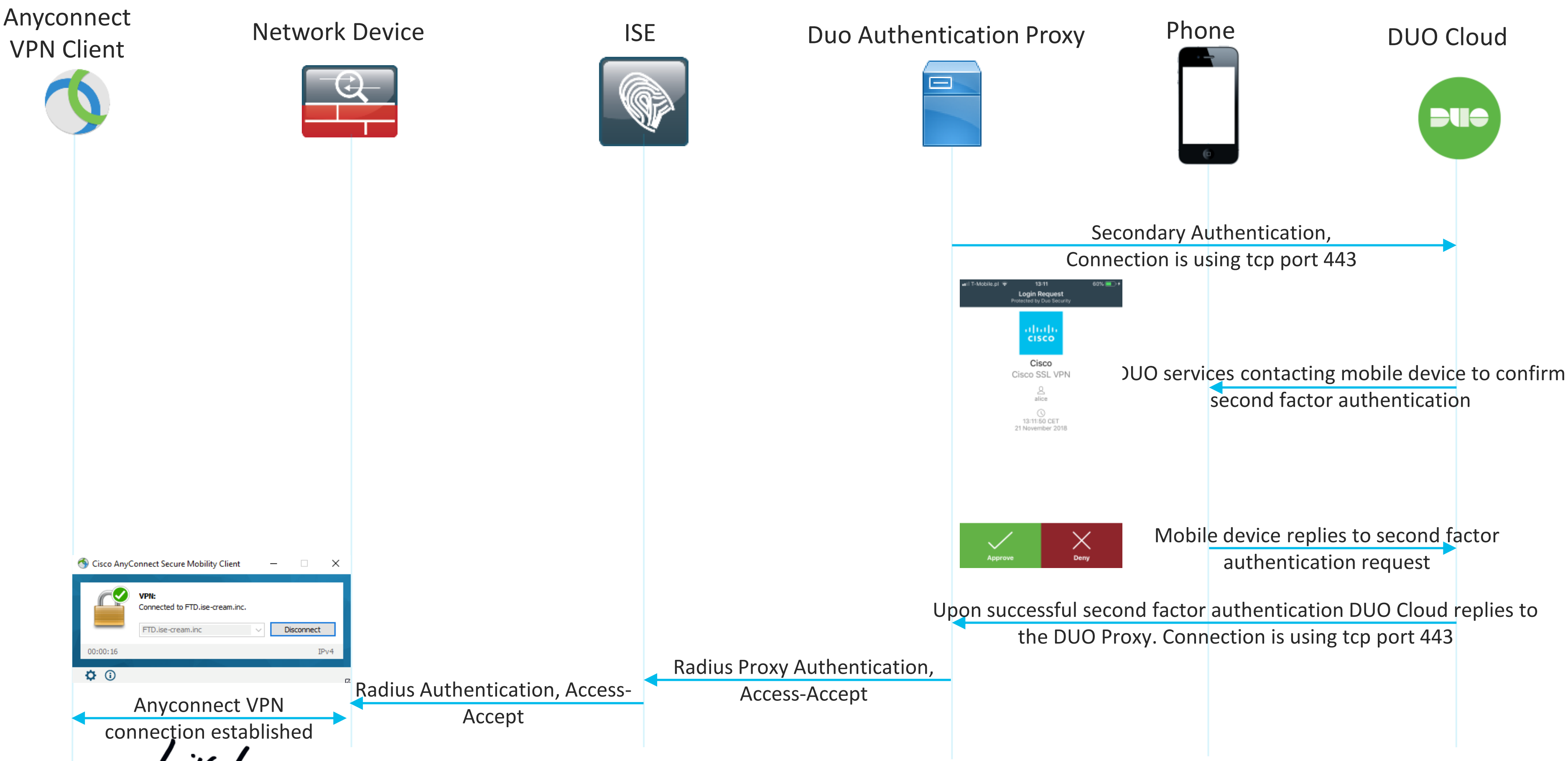
Password:

OK Cancel

Depending on authentication proxy server configuration from authproxy.cfg primary authentication can be one of the following types:

ad_client - Active Directory Server (Using LDAP protocol for authentication)
radius_client – Radius Server using Radius as a protocol

Anyconnect MFA with DUO



Anyconnect VPN Client

Network Device

ISE

Duo Authentication Proxy

Phone

DUO Cloud

Secondary Authentication,
Connection is using tcp port 443

T-Mobile.pl 13:11 60%
Login Request
Protected by Duo Security
Cisco
Cisco SSL VPN
alice
13:11:50 CET
21 November 2018

DUO services contacting mobile device to confirm second factor authentication

Approve
Deny

Mobile device replies to second factor authentication request

Upon successful second factor authentication DUO Cloud replies to the DUO Proxy. Connection is using tcp port 443

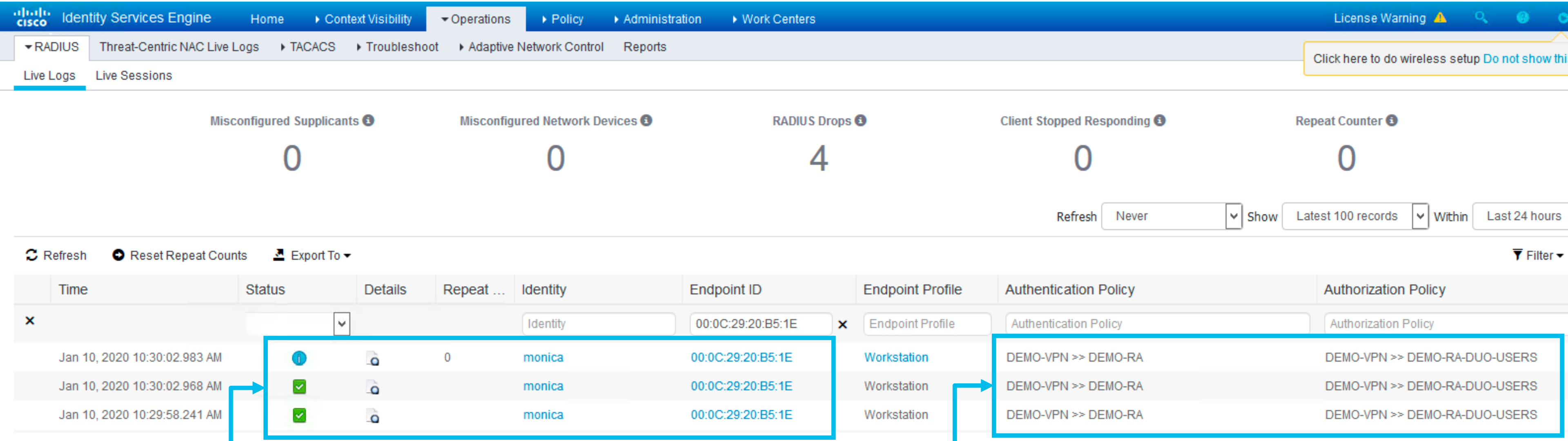
Radius Proxy Authentication, Access-Accept

Radius Authentication, Access-Accept

Cisco AnyConnect Secure Mobility Client
VPN:
Connected to FTD.ise-cream.inc.
FTD.ise-cream.inc
Disconnect
00:00:16
IPv4

Anyconnect VPN connection established

Operations > Live Logs



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	4	0	0

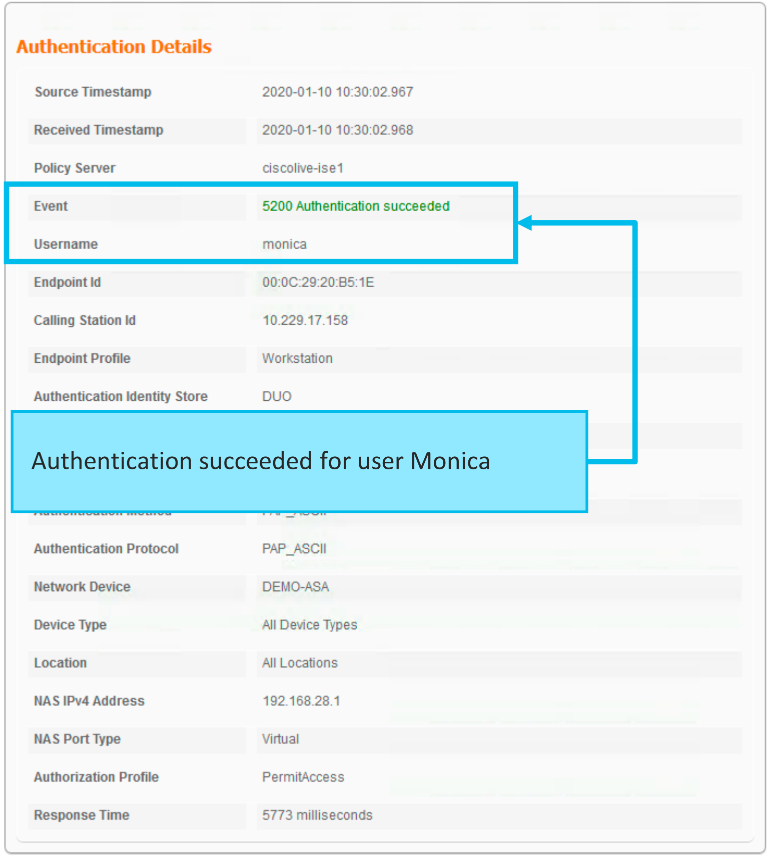
Refresh: Never   Show: Latest 100 records   Within: Last 24 hours

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy
✕				Identity	00:0C:29:20:B5:1E ✕	Endpoint Profile	Authentication Policy	Authorization Policy
Jan 10, 2020 10:30:02.983 AM	ℹ	🔍	0	monica	00:0C:29:20:B5:1E	Workstation	DEMO-VPN >> DEMO-RA	DEMO-VPN >> DEMO-RA-DUO-USERS
Jan 10, 2020 10:30:02.968 AM	☑	🔍		monica	00:0C:29:20:B5:1E	Workstation	DEMO-VPN >> DEMO-RA	DEMO-VPN >> DEMO-RA-DUO-USERS
Jan 10, 2020 10:29:58.241 AM	☑	🔍		monica	00:0C:29:20:B5:1E	Workstation	DEMO-VPN >> DEMO-RA	DEMO-VPN >> DEMO-RA-DUO-USERS

Successful Authentications for user Monica, correct mac address confirms the right authentication

Correct Authentication and Authorization Policies are matched

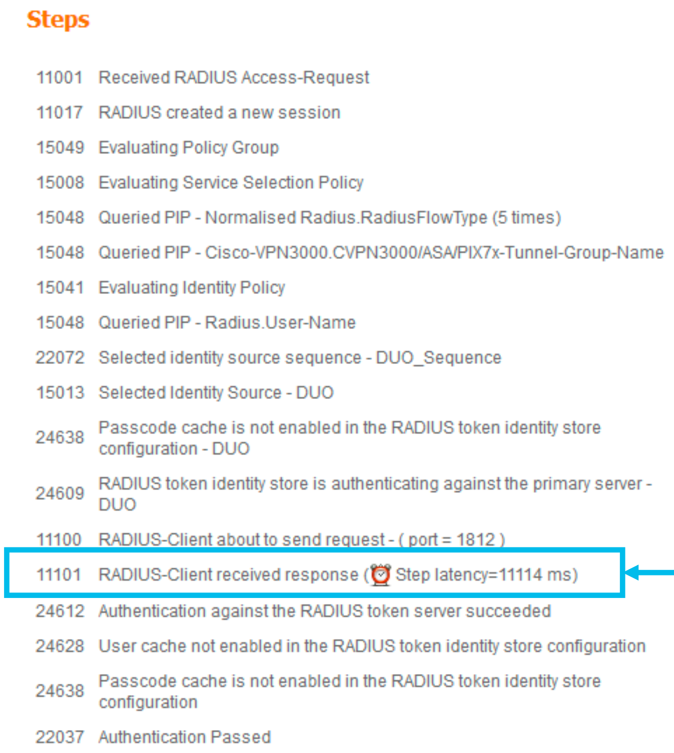
Live Logs > Detailed authentication report



Authentication Details

Source Timestamp	2020-01-10 10:30:02.967
Received Timestamp	2020-01-10 10:30:02.968
Policy Server	ciscolive-ise1
Event	5200 Authentication succeeded
Username	monica
Endpoint Id	00:0C:29:20:B5:1E
Calling Station Id	10.229.17.158
Endpoint Profile	Workstation
Authentication Identity Store	DUO
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII
Network Device	DEMO-ASA
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.168.28.1
NAS Port Type	Virtual
Authorization Profile	PermitAccess
Response Time	5773 milliseconds

Authentication succeeded for user Monica

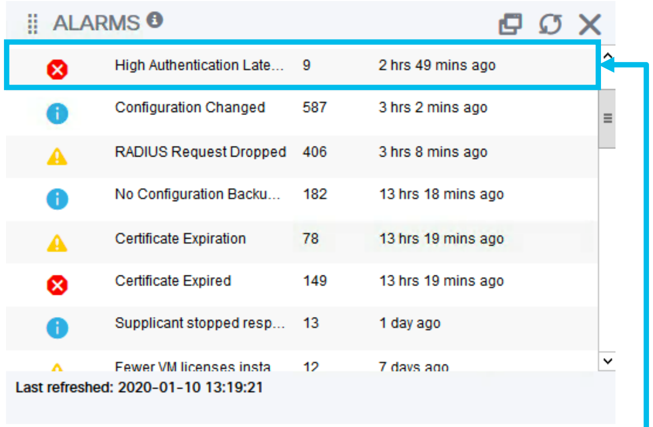


Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - Normalised Radius.RadiusFlowType (5 times)
15048	Queried PIP - Cisco-VPN3000.CVPN3000/ASA/PIX7x-Tunnel-Group-Name
15041	Evaluating Identity Policy
15048	Queried PIP - Radius.User-Name
22072	Selected identity source sequence - DUO_Sequence
15013	Selected Identity Source - DUO
24638	Passcode cache is not enabled in the RADIUS token identity store configuration - DUO
24609	RADIUS token identity store is authenticating against the primary server - DUO
11100	RADIUS-Client about to send request - (port = 1812)
11101	RADIUS-Client received response (⏰ Step latency=11114 ms)
24612	Authentication against the RADIUS token server succeeded
24628	User cache not enabled in the RADIUS token identity store configuration
24638	Passcode cache is not enabled in the RADIUS token identity store configuration
22037	Authentication Passed

11 seconds latency for the DUO Proxy to reply to ISE Server

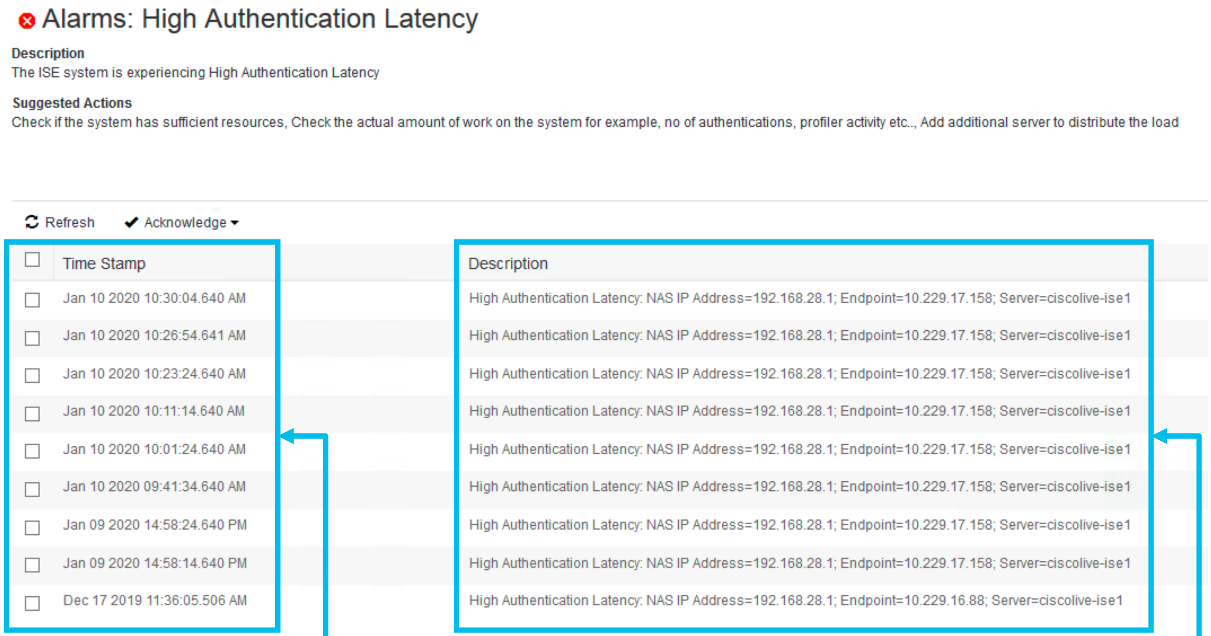
Alarms: High Authentication Latency



ALARMS

✖	High Authentication Late...	9	2 hrs 49 mins ago
ℹ	Configuration Changed	587	3 hrs 2 mins ago
⚠	RADIUS Request Dropped	406	3 hrs 8 mins ago
ℹ	No Configuration Backu...	182	13 hrs 18 mins ago
⚠	Certificate Expiration	78	13 hrs 19 mins ago
✖	Certificate Expired	149	13 hrs 19 mins ago
ℹ	Supplicant stopped resp...	13	1 day ago
⚠	Fewer VM licenses insta	12	7 days ago

Last refreshed: 2020-01-10 13:19:21



✖ Alarms: High Authentication Latency

Description
The ISE system is experiencing High Authentication Latency

Suggested Actions
Check if the system has sufficient resources, Check the actual amount of work on the system for example, no of authentications, profiler activity etc.., Add additional server to distribute the load

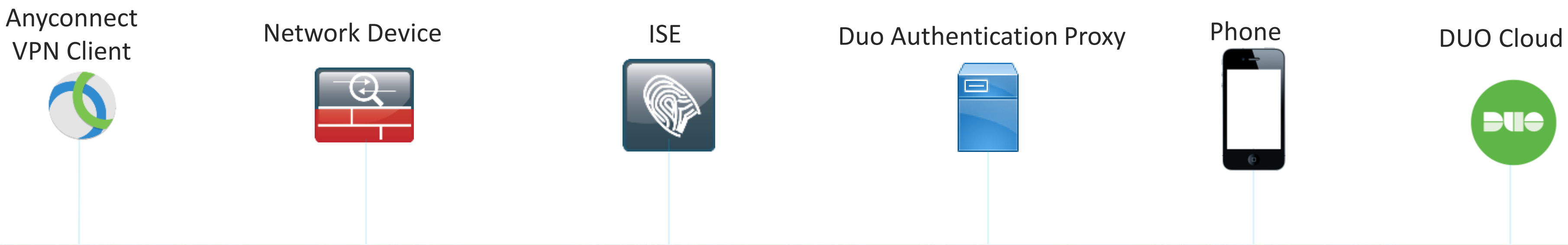
□	Time Stamp	Description
□	Jan 10 2020 10:30:04.640 AM	High Authentication Latency: NAS IP Address=192.168.28.1; Endpoint=10.229.17.158; Server=ciscolive-ise1
□	Jan 10 2020 10:26:54.641 AM	High Authentication Latency: NAS IP Address=192.168.28.1; Endpoint=10.229.17.158; Server=ciscolive-ise1
□	Jan 10 2020 10:23:24.640 AM	High Authentication Latency: NAS IP Address=192.168.28.1; Endpoint=10.229.17.158; Server=ciscolive-ise1
□	Jan 10 2020 10:11:14.640 AM	High Authentication Latency: NAS IP Address=192.168.28.1; Endpoint=10.229.17.158; Server=ciscolive-ise1
□	Jan 10 2020 10:01:24.640 AM	High Authentication Latency: NAS IP Address=192.168.28.1; Endpoint=10.229.17.158; Server=ciscolive-ise1
□	Jan 10 2020 09:41:34.640 AM	High Authentication Latency: NAS IP Address=192.168.28.1; Endpoint=10.229.17.158; Server=ciscolive-ise1
□	Jan 09 2020 14:58:24.640 PM	High Authentication Latency: NAS IP Address=192.168.28.1; Endpoint=10.229.17.158; Server=ciscolive-ise1
□	Jan 09 2020 14:58:14.640 PM	High Authentication Latency: NAS IP Address=192.168.28.1; Endpoint=10.229.17.158; Server=ciscolive-ise1
□	Dec 17 2019 11:36:05.506 AM	High Authentication Latency: NAS IP Address=192.168.28.1; Endpoint=10.229.16.88; Server=ciscolive-ise1

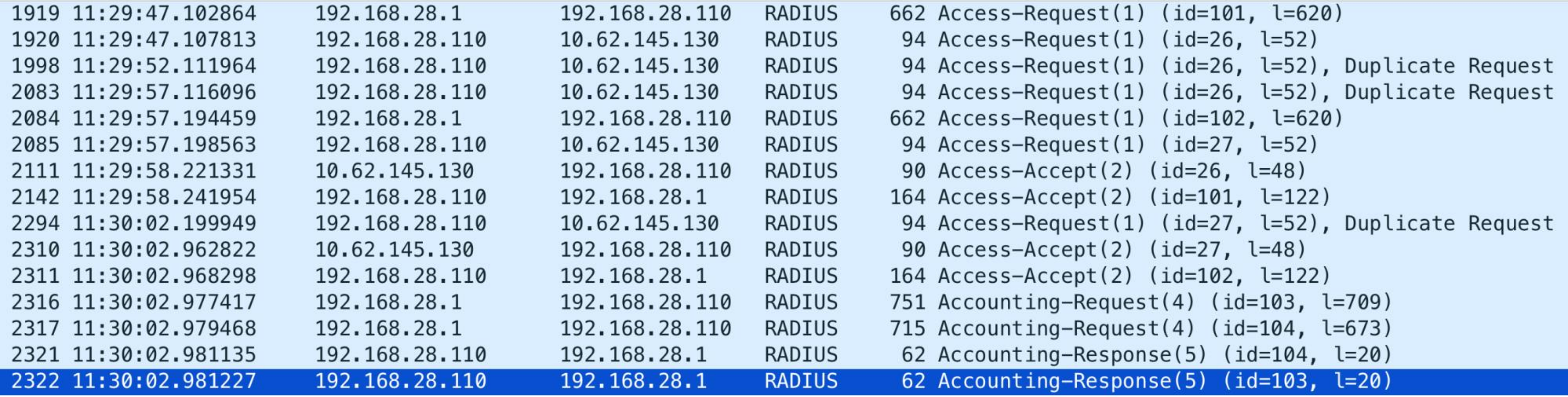
High Authentication Latency Alarms

Timestamp of the Alarm

NAD IP Address, Endpoint, PSN

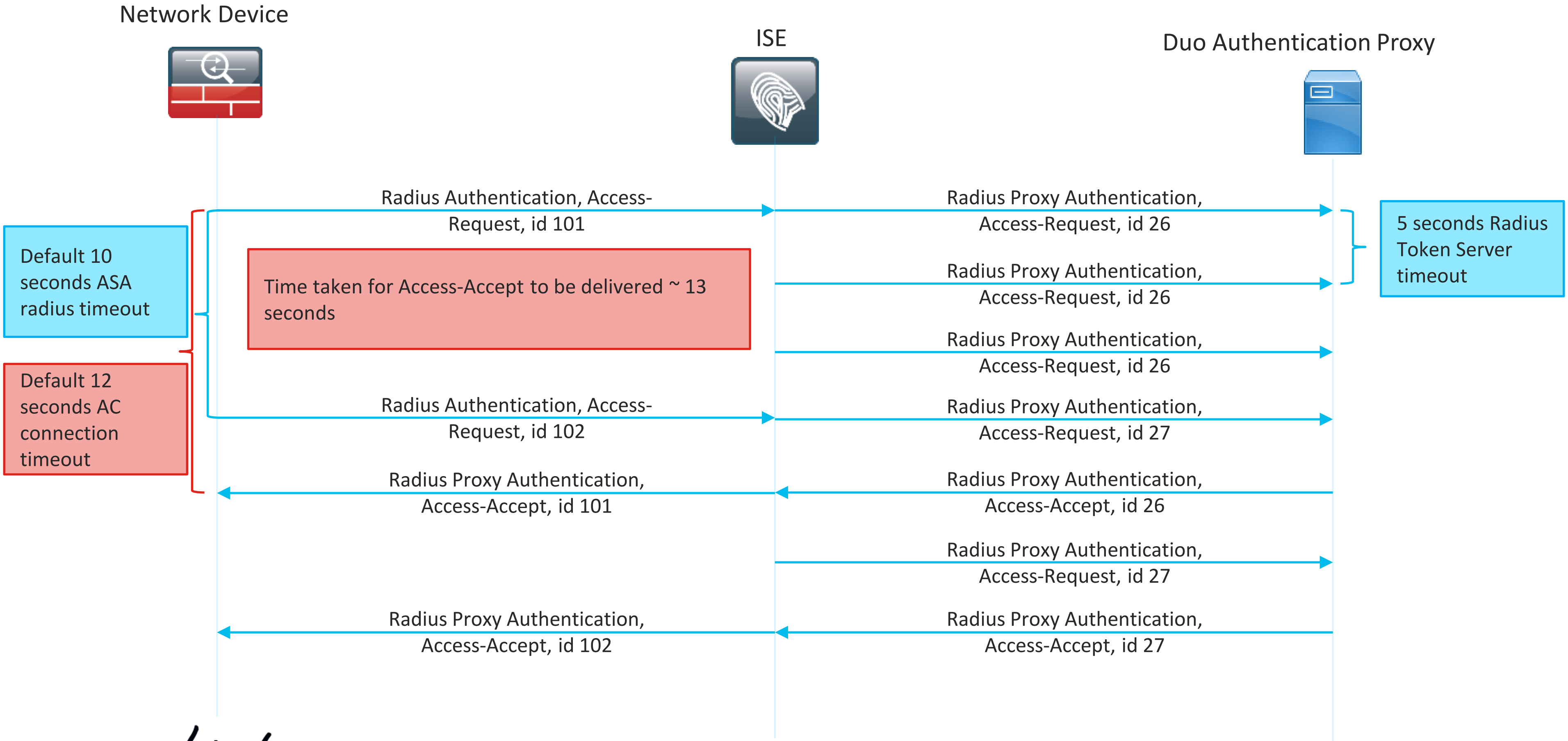
What next?





```
1919 11:29:47.102864    192.168.28.1      192.168.28.110   RADIUS    662 Access-Request(1) (id=101, l=620)
1920 11:29:47.107813    192.168.28.110    10.62.145.130    RADIUS     94 Access-Request(1) (id=26, l=52)
1998 11:29:52.111964    192.168.28.110    10.62.145.130    RADIUS     94 Access-Request(1) (id=26, l=52), Duplicate Request
2083 11:29:57.116096    192.168.28.110    10.62.145.130    RADIUS     94 Access-Request(1) (id=26, l=52), Duplicate Request
2084 11:29:57.194459    192.168.28.1      192.168.28.110   RADIUS    662 Access-Request(1) (id=102, l=620)
2085 11:29:57.198563    192.168.28.110    10.62.145.130    RADIUS     94 Access-Request(1) (id=27, l=52)
2111 11:29:58.221331    10.62.145.130     192.168.28.110   RADIUS     90 Access-Accept(2) (id=26, l=48)
2142 11:29:58.241954    192.168.28.110    192.168.28.1     RADIUS    164 Access-Accept(2) (id=101, l=122)
2294 11:30:02.199949    192.168.28.110    10.62.145.130    RADIUS     94 Access-Request(1) (id=27, l=52), Duplicate Request
2310 11:30:02.962822    10.62.145.130     192.168.28.110   RADIUS     90 Access-Accept(2) (id=27, l=48)
2311 11:30:02.968298    192.168.28.110    192.168.28.1     RADIUS    164 Access-Accept(2) (id=102, l=122)
2316 11:30:02.977417    192.168.28.1      192.168.28.110   RADIUS    751 Accounting-Request(4) (id=103, l=709)
2317 11:30:02.979468    192.168.28.1      192.168.28.110   RADIUS    715 Accounting-Request(4) (id=104, l=673)
2321 11:30:02.981135    192.168.28.110    192.168.28.1     RADIUS     62 Accounting-Response(5) (id=104, l=20)
2322 11:30:02.981227    192.168.28.110    192.168.28.1     RADIUS     62 Accounting-Response(5) (id=103, l=20)
```

Anyconnect MFA with DUO



Network Device

ISE

Duo Authentication Proxy

Radius Authentication, Access-Request, id 101

Radius Proxy Authentication, Access-Request, id 26

Default 10 seconds ASA radius timeout

Time taken for Access-Accept to be delivered ~ 13 seconds

Radius Proxy Authentication, Access-Request, id 26

5 seconds Radius Token Server timeout

Radius Proxy Authentication, Access-Request, id 26

Default 12 seconds AC connection timeout

Radius Authentication, Access-Request, id 102

Radius Proxy Authentication, Access-Request, id 27

Radius Proxy Authentication, Access-Accept, id 101

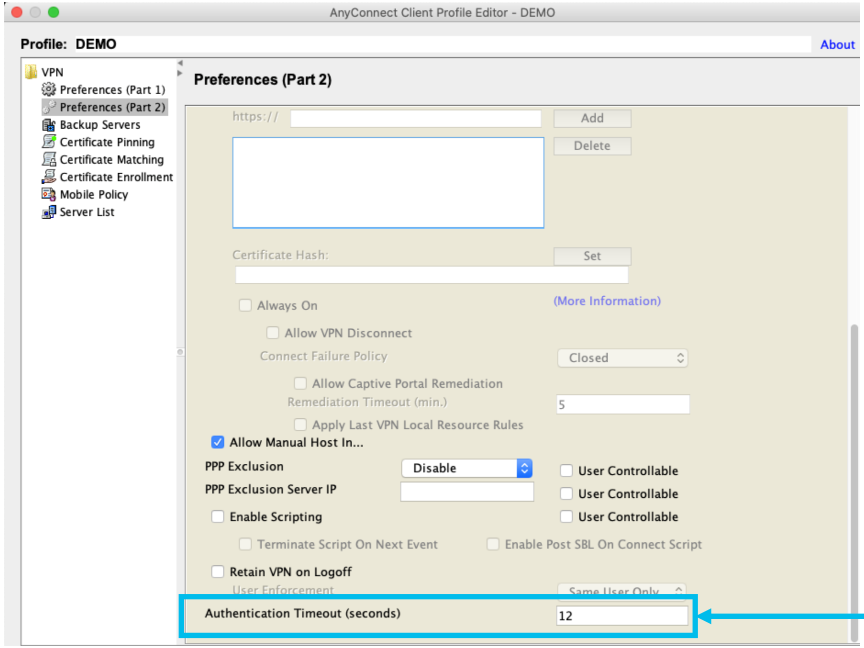
Radius Proxy Authentication, Access-Accept, id 26

Radius Proxy Authentication, Access-Request, id 27

Radius Proxy Authentication, Access-Accept, id 102

Radius Proxy Authentication, Access-Accept, id 27

Confirming the theory – issue 6



AnyConnect Client Profile Editor - DEMO

Profile: DEMO

Preferences (Part 2)

https://

Certificate Hash:

□ Always On

□ Allow VPN Disconnect

Connect Failure Policy: Closed

□ Allow Captive Portal Remediation

Remediation Timeout (min.): 5

□ Apply Last VPN Local Resource Rules

☑ Allow Manual Host In...

PPP Exclusion: Disable □ User Controllable

PPP Exclusion Server IP □ User Controllable

□ Enable Scripting □ User Controllable

□ Terminate Script On Next Event □ Enable Post SBL On Connect Script

□ Retain VPN on Logoff

User Enforcement: Same User Only

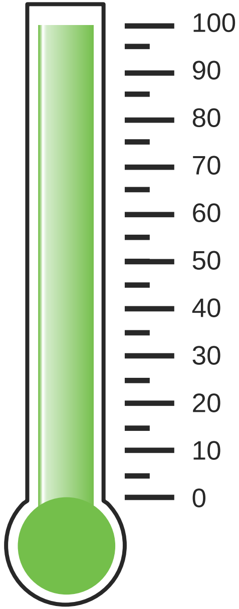
Authentication Timeout (seconds): 12

Authentication Timeout is set to default 12 seconds

Issue 6: AnyConnect Authentication was timing out before Access-Accept was arriving at the ASA.
Solution 6: Increase Authentication timeout to give users time to accept the push notification

Issue 6a: New Push notifications are coming before the user accepted the original
Solution 6a: Increase Radius timeout on ASA, to give users time to accept original push notification

Meeting’s success scale



- Everyone is connected.
- Time for Very Important Break in the Very Important meeting

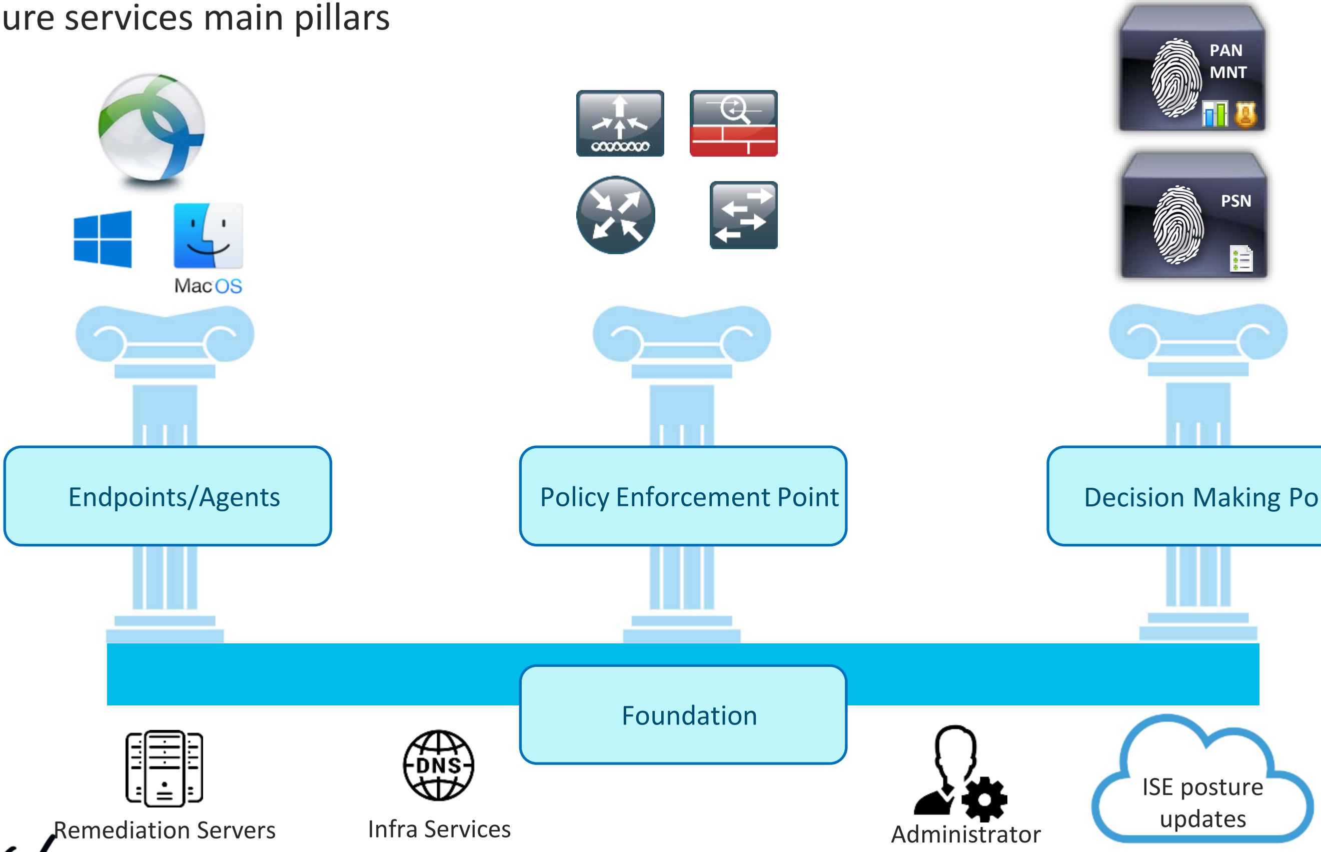
Agenda

- Introduction to DEMO
- Learn by example - Profiling and Authentication Troubleshooting
- Posture Overview
- 5 common ISE Posture misconceptions
- Learn by example – Posture Troubleshooting

Posture overview

What are the components?

- ISE posture services main pillars



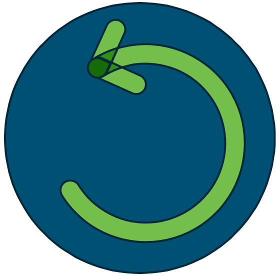
Posture life Cycle in a nutshell

Step 0	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Manual installation	Initial authentication	Client Provisioning	Actual posture	Remediation	CoA	Final Authentication

Posture flow types

There are two types of posture flows:

Redirect based posture flow:



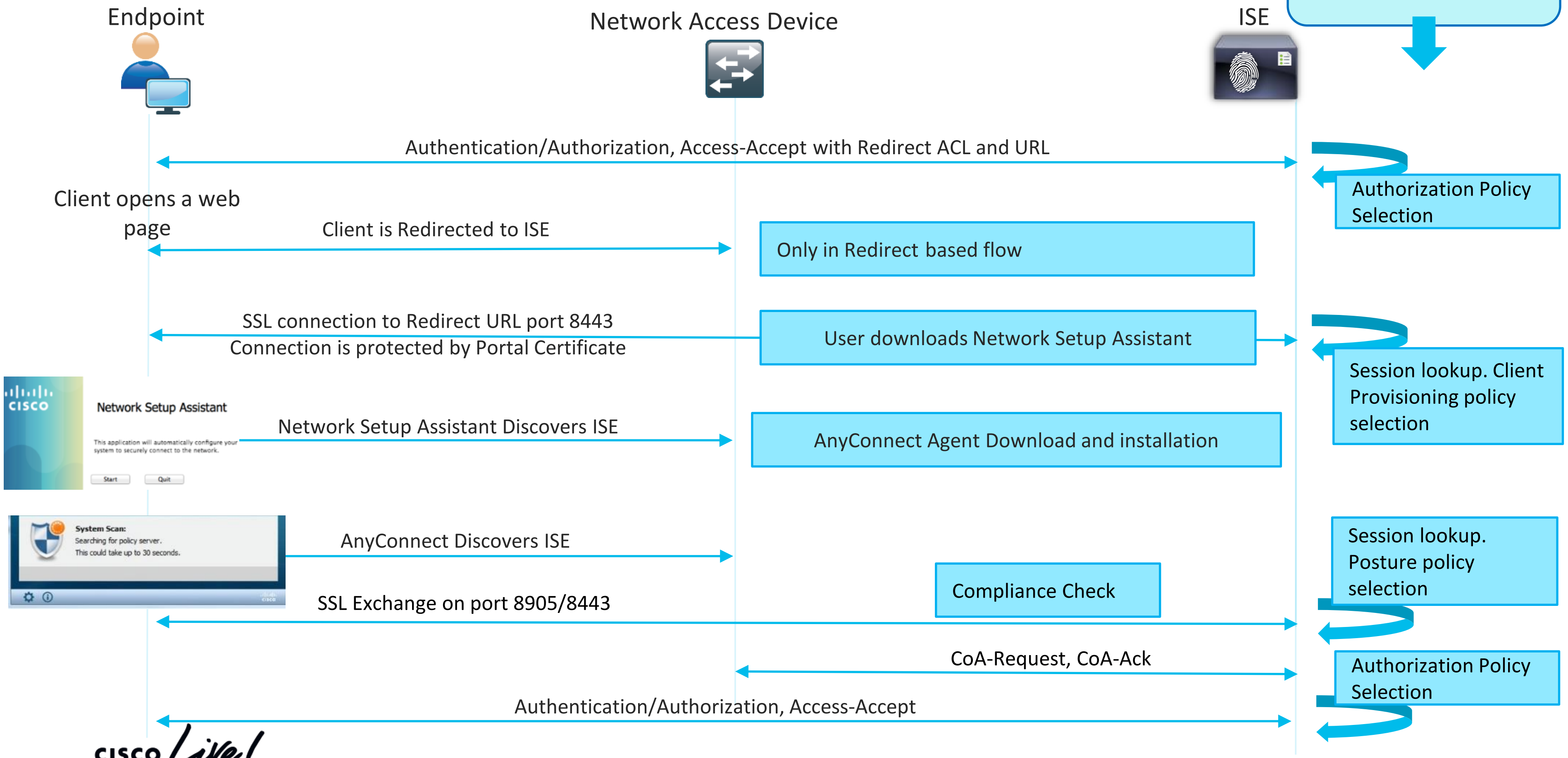
Original approach that is available on all supported ISE versions

Non-redirect based posture flow:

Next generation approach that is supported from ISE 2.2+

Posture Lifecycle - Let's visualize

Understand how it should work


Endpoint
Network Access Device
ISE
Authentication/Authorization, Access-Accept with Redirect ACL and URL
Authorization Policy Selection
Client opens a web page
Client is Redirected to ISE
Only in Redirect based flow
SSL connection to Redirect URL port 8443
Connection is protected by Portal Certificate
User downloads Network Setup Assistant
Session lookup. Client Provisioning policy selection
cisco
Start
Quit
Network Setup Assistant Discovers ISE
AnyConnect Agent Download and installation
AnyConnect Discovers ISE
Session lookup. Posture policy selection
Compliance Check
SSL Exchange on port 8905/8443
CoA-Request, CoA-Ack
Authorization Policy Selection
Authentication/Authorization, Access-Accept

Network Setup Assistant

This application will automatically configure your system to securely connect to the network.

System Scan:
Searching for policy server.
This could take up to 30 seconds.

Agenda

- Introduction to DEMO
- Learn by example - Profiling and Authentication Troubleshooting
- Posture Overview
- 5 common ISE Posture misconceptions
- Learn by example – Posture Troubleshooting

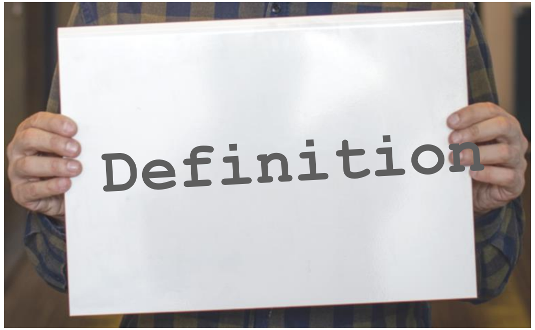
Misconception 1 – posture and session management

1. Unneeded sessions are removed

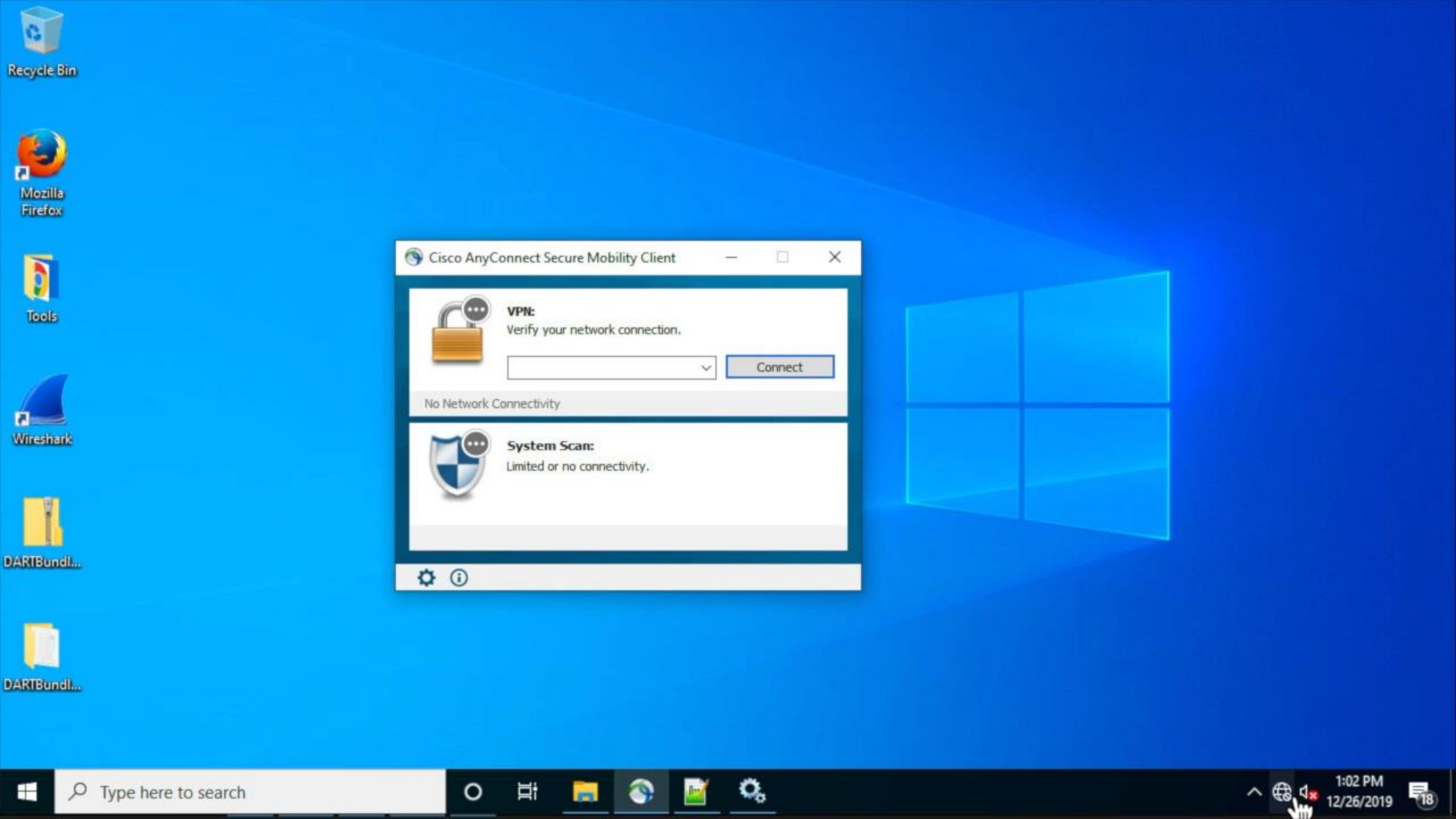
Misconception definition –

”As soon as endpoint got disconnected from the network session context is removed from ISE”

Let's have a look on standard problematic scenario -



Demo – Misconception 1



Cisco AnyConnect Secure Mobility Client

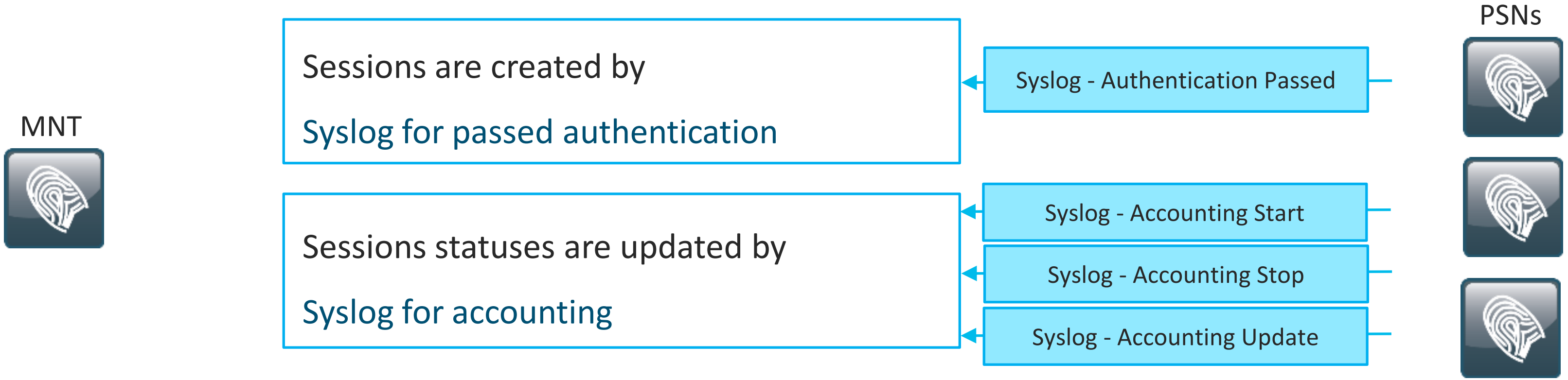
VPN:
Verify your network connection.

No Network Connectivity

System Scan:
Limited or no connectivity.

Session management - theory walkthrough

Who is responsible for session management in ISE deployment?



MNT

Sessions are created by

Syslog for passed authentication

Sessions statuses are updated by

Syslog for accounting

Syslog - Authentication Passed

Syslog - Accounting Start

Syslog - Accounting Stop

Syslog - Accounting Update

PSNs

Rules for sessions removal

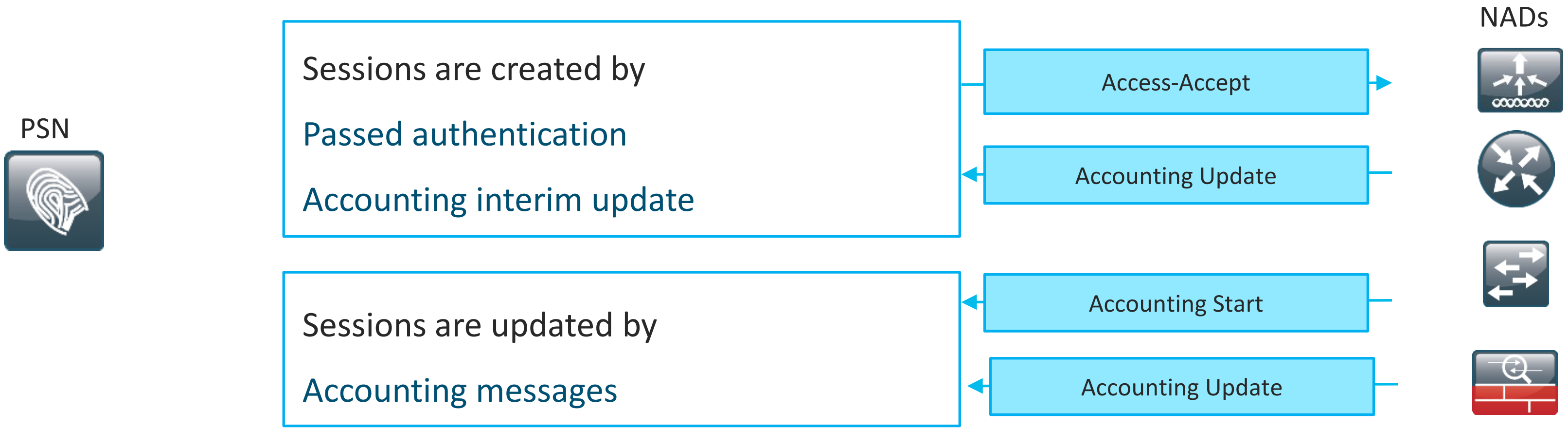
a. Sessions without accounting start (Authenticated) removed after 60 minutes,

b. Sessions with accounting stop (Terminated) removed after 15 minutes

c. Sessions in ‘Started’ state (MNT got accounting start) removed after 120 hours without Interim update.

Session management - theory walkthrough

Who is responsible for session management in ISE deployment?



Sessions are created by

Passed authentication

Accounting interim update

Sessions are updated by

Accounting messages

Rules for sessions removal

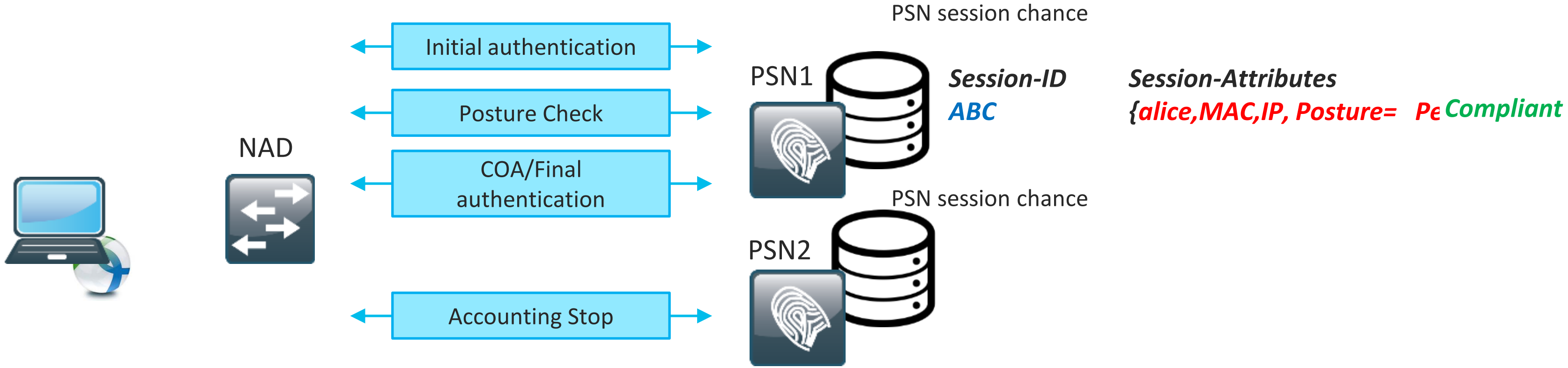
a. Sessions are removed upon processing Accounting stop,

b. Least recently used sessions are removed after reaching platform limit

c. Session cache is cleared upon PSN reload or Application Server restart

Session management - What it brings

Stale session - a scenario when accounting stop was processed by the wrong PSN



PSN session chance

Initial authentication

Posture Check

COA/Final authentication

Accounting Stop

NAD

PSN1

Session-ID

ABC

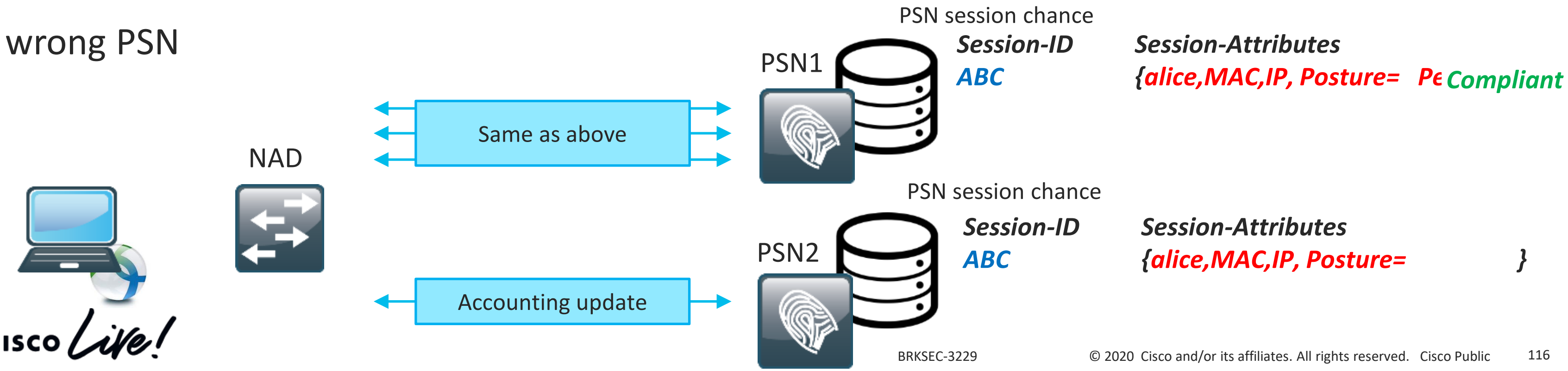
Session-Attributes

{alice,MAC,IP, Posture= *Pe* *Compliant*

PSN session chance

PSN2

Phantom session - scenario when one of the accounting interim update packets was processed by the wrong PSN



PSN session chance

Same as above

Accounting update

NAD

PSN1

Session-ID

ABC

Session-Attributes

{alice,MAC,IP, Posture= *Pe* *Compliant*

PSN session chance

PSN2

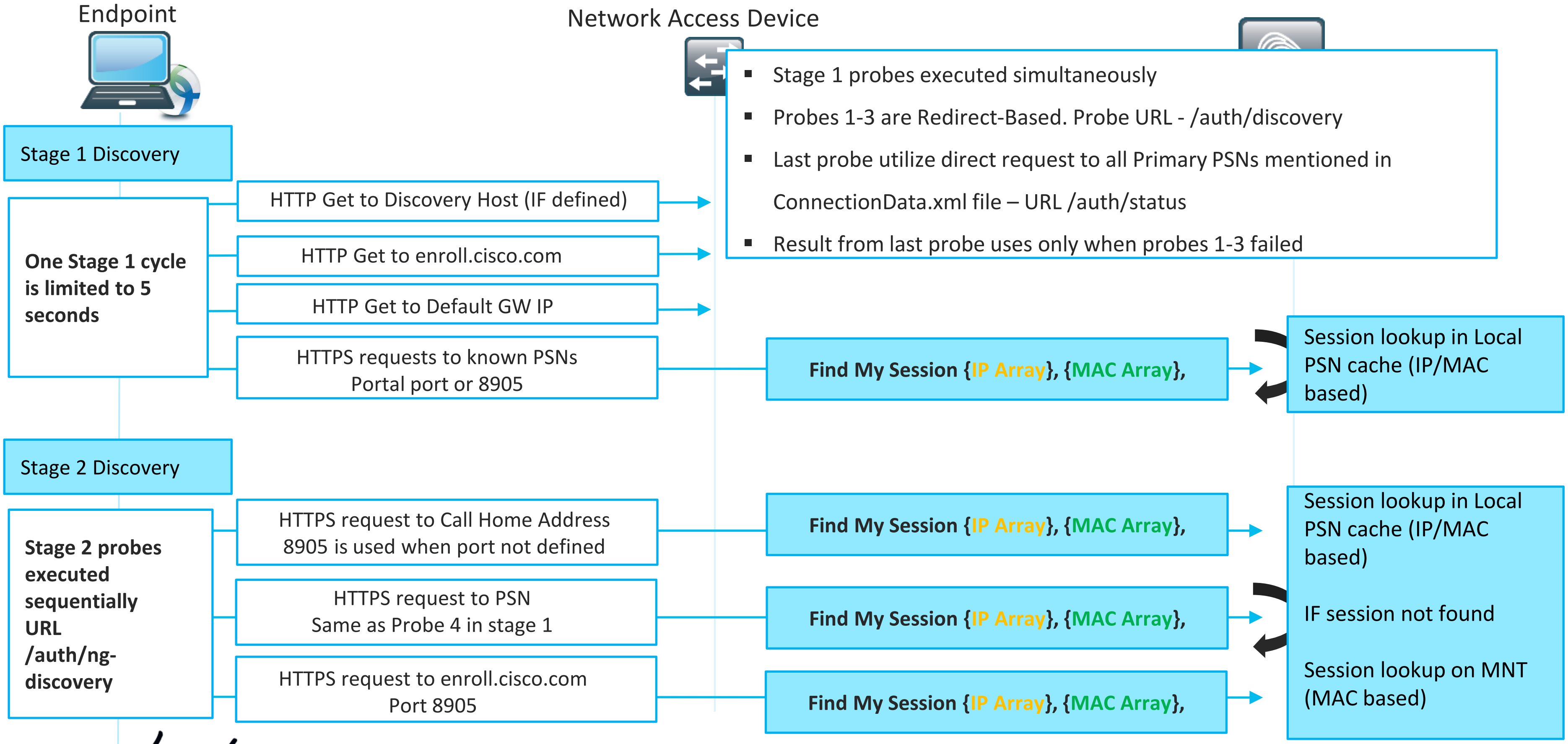
Session-ID

ABC

Session-Attributes

{alice,MAC,IP, Posture= *}*

Session management –Where is the threat



Endpoint

Network Access Device

- Stage 1 probes executed simultaneously
- Probes 1-3 are Redirect-Based. Probe URL - /auth/discovery
- Last probe utilize direct request to all Primary PSNs mentioned in ConnectionData.xml file – URL /auth/status
- Result from last probe uses only when probes 1-3 failed

Stage 1 Discovery

One Stage 1 cycle is limited to 5 seconds

HTTP Get to Discovery Host (IF defined)

HTTP Get to enroll.cisco.com

HTTP Get to Default GW IP

HTTPS requests to known PSNs
Portal port or 8905

Find My Session {IP Array}, {MAC Array},

Session lookup in Local PSN cache (IP/MAC based)

Stage 2 Discovery

Stage 2 probes executed sequentially URL /auth/ng-discovery

HTTPS request to Call Home Address
8905 is used when port not defined

Find My Session {IP Array}, {MAC Array},

HTTPS request to PSN
Same as Probe 4 in stage 1

Find My Session {IP Array}, {MAC Array},

HTTPS request to enroll.cisco.com
Port 8905

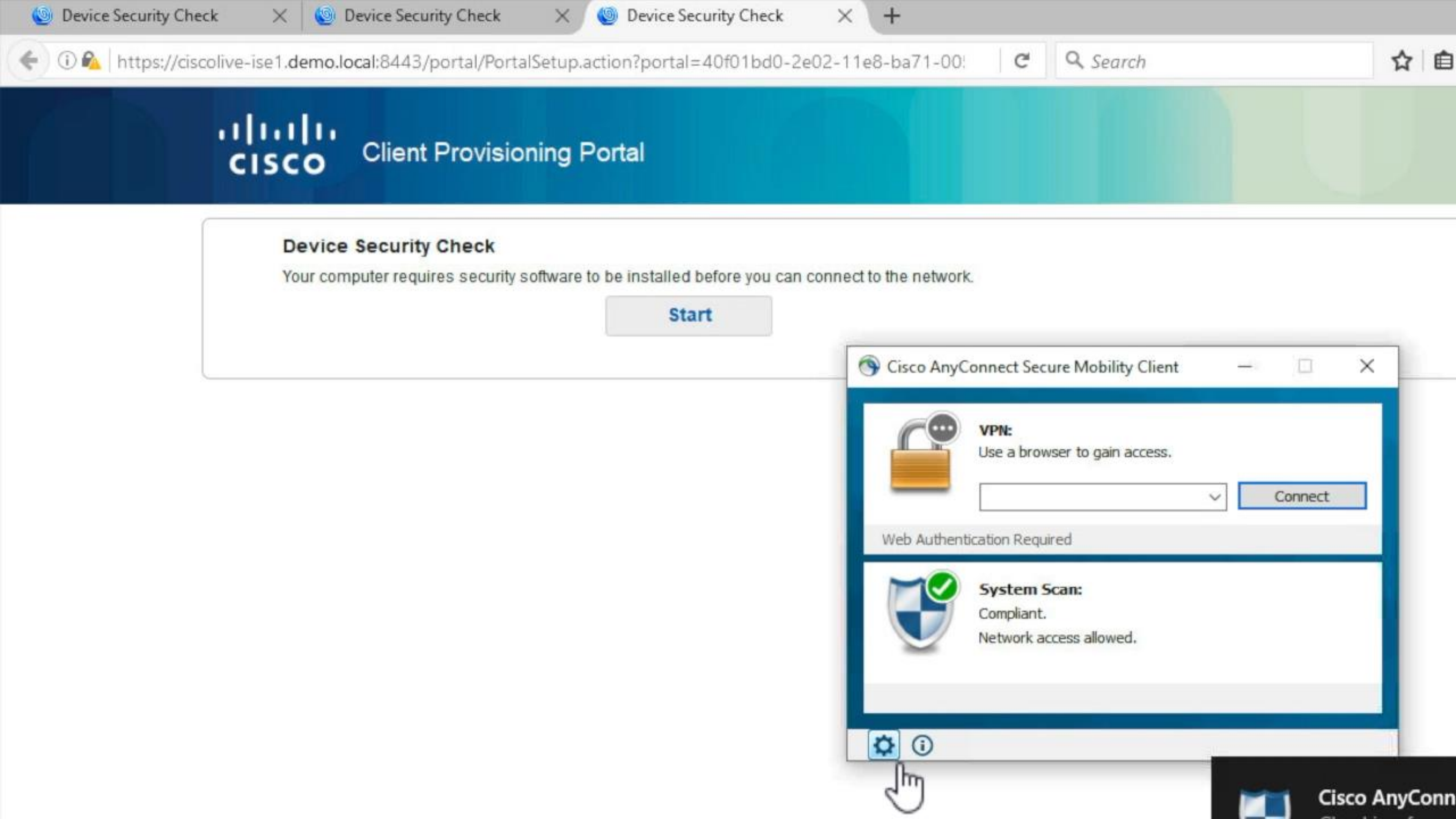
Find My Session {IP Array}, {MAC Array},

Session lookup in Local PSN cache (IP/MAC based)

IF session not found

Session lookup on MNT (MAC based)

Demo – Misconception 1, quick identification


Device Security Check
Device Security Check
Device Security Check
https://ciscolive-ise1.demo.local:8443/portal/PortalSetup.action?portal=40f01bd0-2e02-11e8-ba71-00
Search
cisco
Client Provisioning Portal

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Start
Cisco AnyConnect Secure Mobility Client

VPN:
Use a browser to gain access.

Web Authentication Required

System Scan:
Compliant.
Network access allowed.

Misconception 1 – How to avoid?

- USE REDIRECTION when it’s supported by NAD

counterargument

ISE posture module is pre-installed in our environment. Redirection and captive portal detection pop-ups are confusing for end-users.

argument

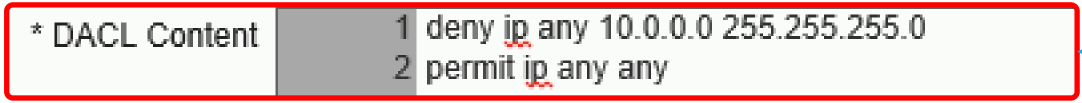
Redirection can be configured in the way when only certain probes are redirected

```
ip access-list extended REDIRECT-DH-ENROLL
permit tcp any host 1.1.1.1 eq www
permit tcp any host 72.163.1.80
deny   ip any any
```

Redirect for Discovery Host IP

Redirect for enroll.cisco.com IP

Bypass redirection for everything else

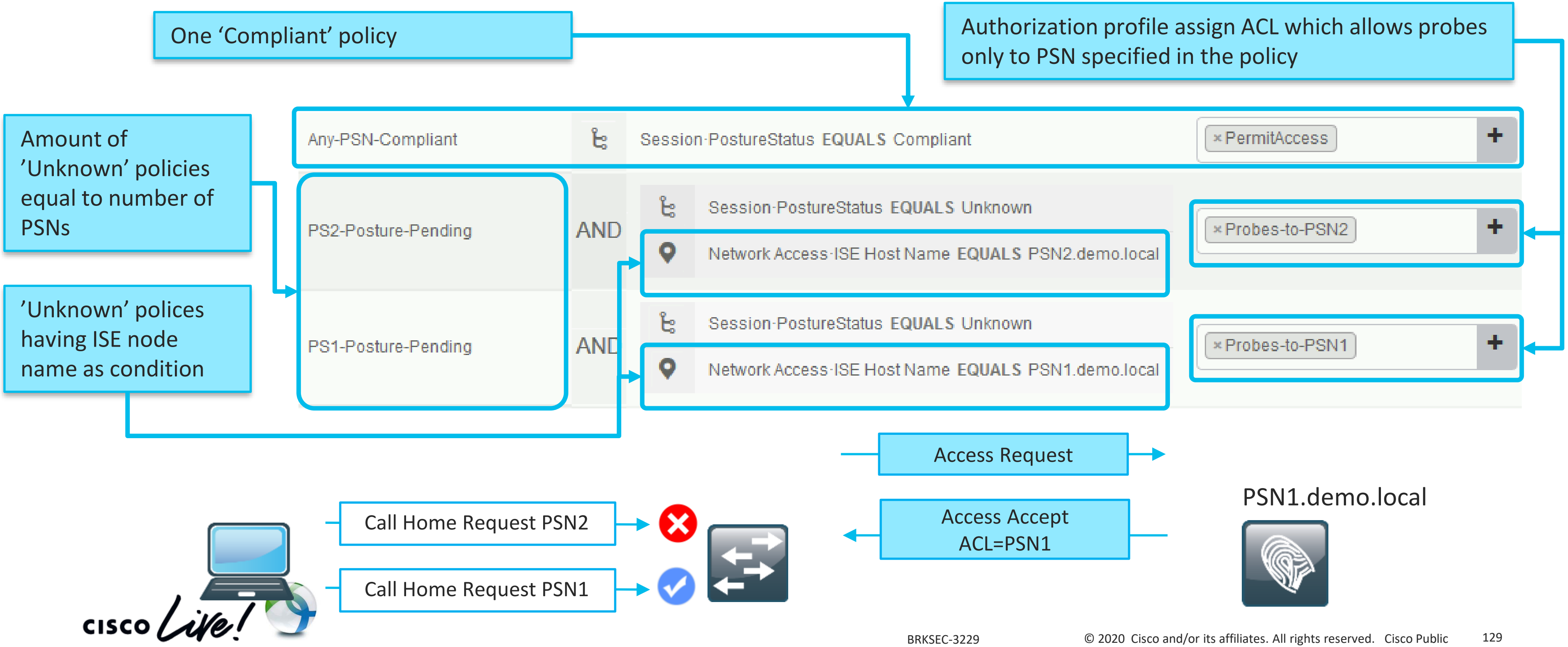


```
* DACL Content    1 deny ip any 10.0.0.0 255.255.255.0
                  2 permit ip any any
```

Access to corporate resources is restricted while everything else allowed

Misconception 1 – How to avoid? (continue)

- For NADs without redirect capabilities we can artificially ensure that Probes are hitting only PSN which handled authentication.



One 'Compliant' policy

Authorization profile assign ACL which allows probes only to PSN specified in the policy

Amount of 'Unknown' policies equal to number of PSNs

'Unknown' polices having ISE node name as condition

Any-PSN-Compliant	Session·PostureStatus EQUALS Compliant	PermitAccess
PS2-Posture-Pending	AND Session·PostureStatus EQUALS Unknown Network Access·ISE Host Name EQUALS PSN2.demo.local	Probes-to-PSN2
PS1-Posture-Pending	AND Session·PostureStatus EQUALS Unknown Network Access·ISE Host Name EQUALS PSN1.demo.local	Probes-to-PSN1

Misconception 1 – How to avoid? (continue)

- Enabled stickiness on LB for authentication and accounting with Calling-Station-ID as a stickiness key. More details

- Use stickiness timer a bit higher than average working day (e.g. 10 hours).

- Set reauthentication timer from ISE with value a bit lower than stickiness timer (e.g. 8 hours).

- On VPN set higher accounting interim-update interval than 'vpn-session-timeout', To avoid accounting flapping between PSNs on a long living sessions.

See hidden slides for more details

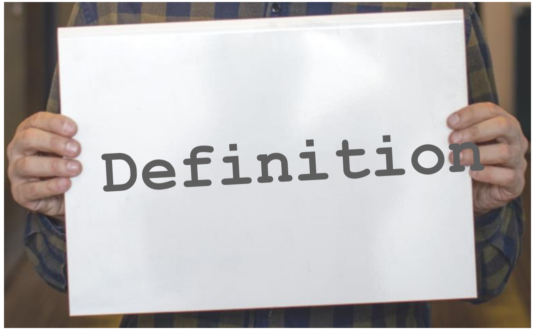
Misconception 2 – session sharing

2. There is a session sharing in ISE

Misconception definition –

”Session context is shared within ISE deployment so PSN can run posture even when authentication hit another node”

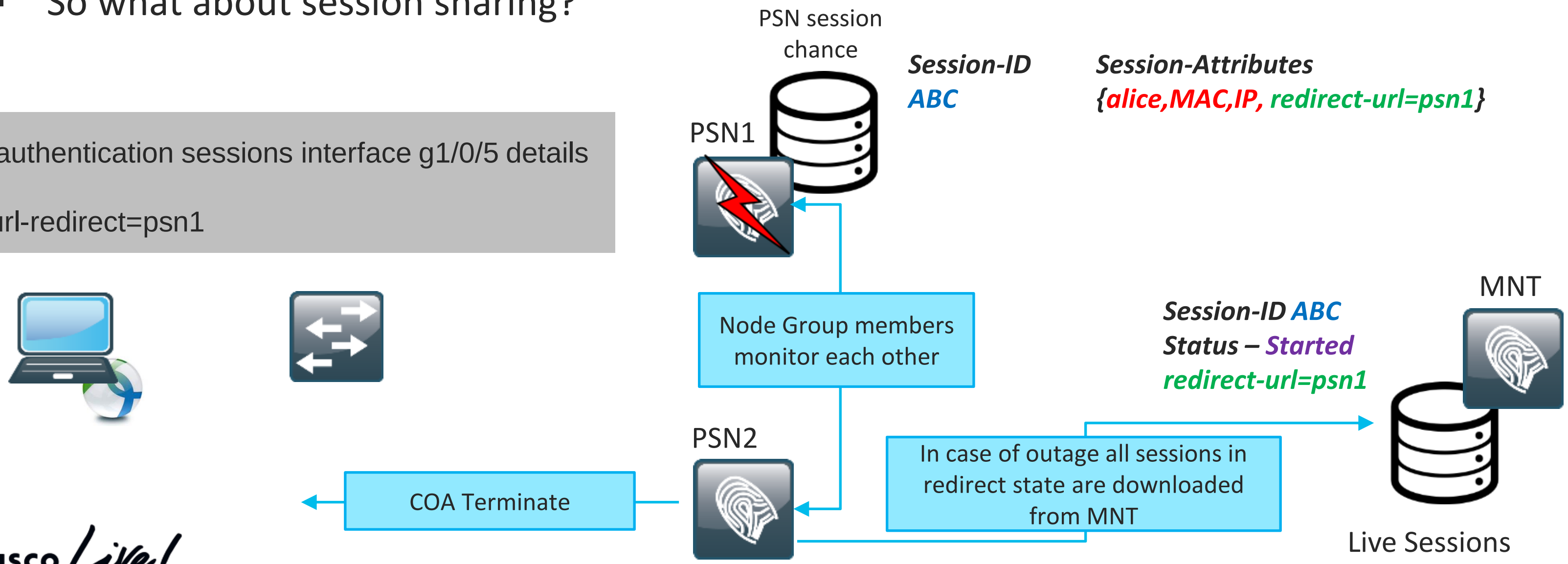
- Old myth – Node Groups
- New myth - Light Session Directory (LSD)



Node Groups and session sharing

- Node groups came into picture in ISE 1.2 together with full redesign of deployment replication
- Main idea behind is to minimize amount of global replication events (keep whatever possible inside the group)
- So what about session sharing?

```
SW#sh authentication sessions interface g1/0/5 details
…
          url-redirect=psn1
```



PSN session chance

Session-ID
ABC

Session-Attributes
{alice,MAC,IP, redirect-url=psn1}

Node Group members monitor each other

Session-ID ABC
Status – Started
redirect-url=psn1

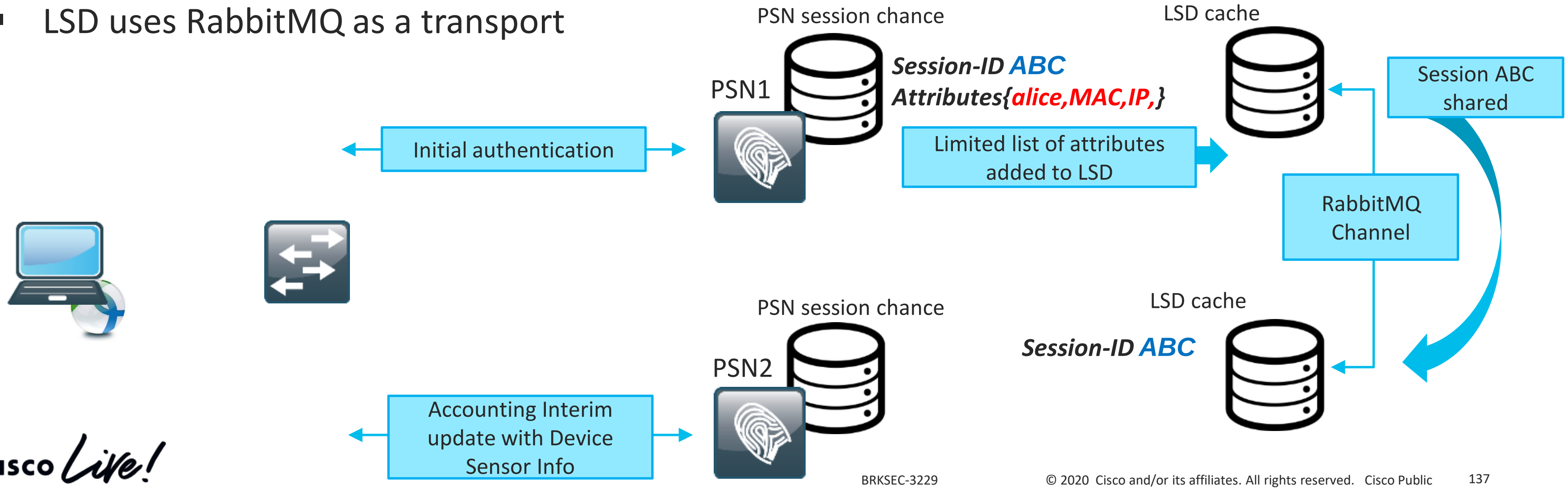
In case of outage all sessions in redirect state are downloaded from MNT

COA Terminate

Light Session Directory and session sharing

- LSD is a new feature introduced in ISE 2.6
- LSD allows to share limited information about session context across all the nodes in the ISE deployment
- Information shared limited to attributes required to execute COA
- LSD uses RabbitMQ as a transport

See hidden slides for more details



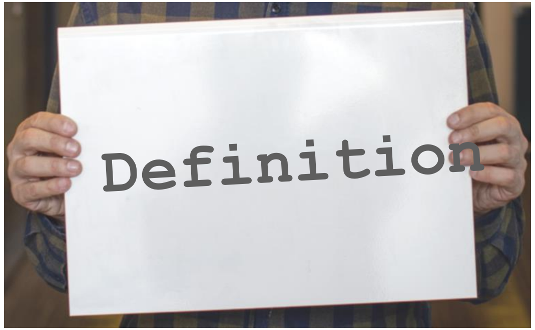
Misconception 3 – posture discovery and authentication

3. Authentications triggers Discovery process

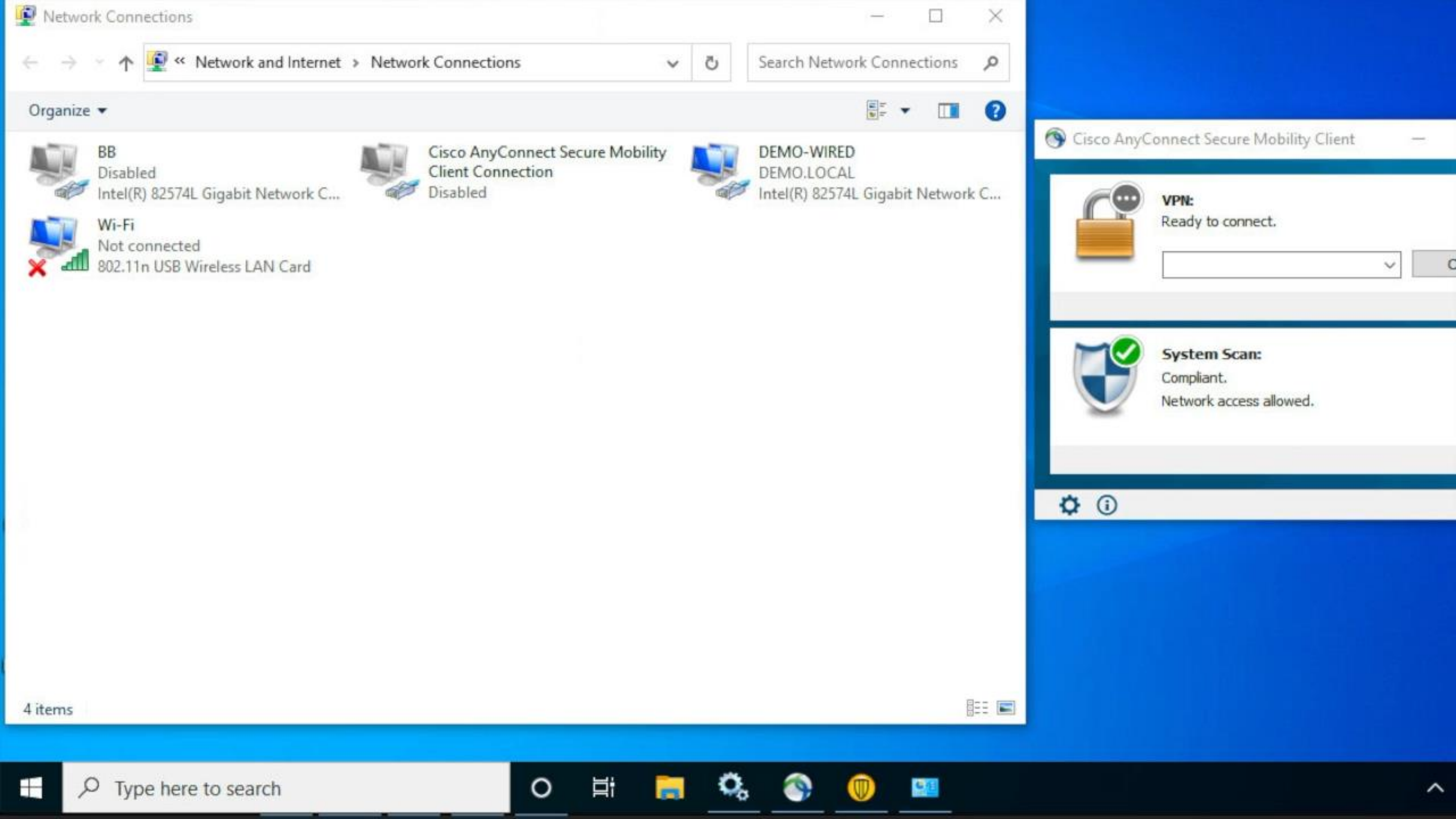
Misconception definition –

”Every time when dot1x authentication happens Discovery process is restarted by the ISE posture module”

Let's have a look on standard problematic scenario -



Demo – Misconception 3


Network Connections
« Network and Internet › Network Connections
Search Network Connections
Organize ▾
Cisco AnyConnect Secure Mobility Client
4 items
Type here to search

BB
Disabled
Intel(R) 82574L Gigabit Network C...

Cisco AnyConnect Secure Mobility Client Connection
Disabled

DEMO-WIRED
DEMO.LOCAL
Intel(R) 82574L Gigabit Network C...

Wi-Fi
Not connected
802.11n USB Wireless LAN Card

VPN:
Ready to connect.

System Scan:
Compliant.
Network access allowed.

Discovery process triggers

ISE posture module monitors following events to restart discovery process

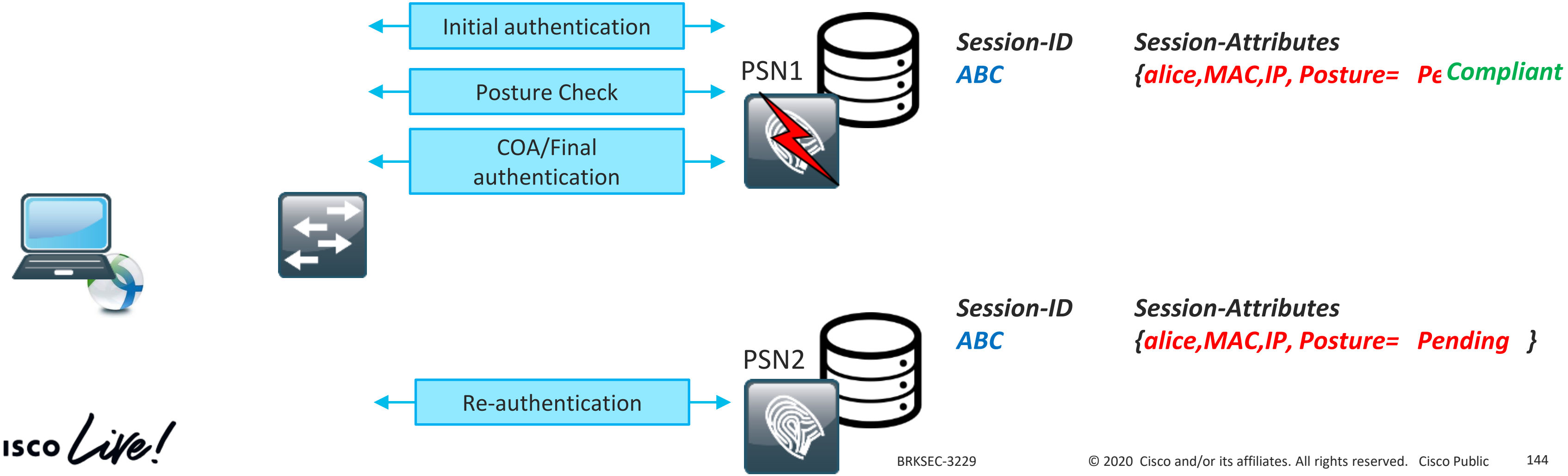
- Initial ISE posture module installation
- Posture Reassessment (PRA) failure, added as a fix for CSCvo69557
- User login
- Power events
- Interface status change
- OS resume after sleep
- Default Gateway (DG) change

Note: dot1x authentication, PC unlock, IP address change are not triggering discovery process

Common problematic scenarios

This issue may happen in bunch of different scenarios, but all of them can be divided into two main groups:

- Re-authentication hits different PSN (either due to LB decision or issues with original PSN)
- NAD generates new session-id on reauthentication



Initial authentication

Posture Check

COA/Final authentication

PSN1

Session-ID

ABC

Session-Attributes

{alice,MAC,IP, Posture= Pe Compliant

Re-authentication

PSN2

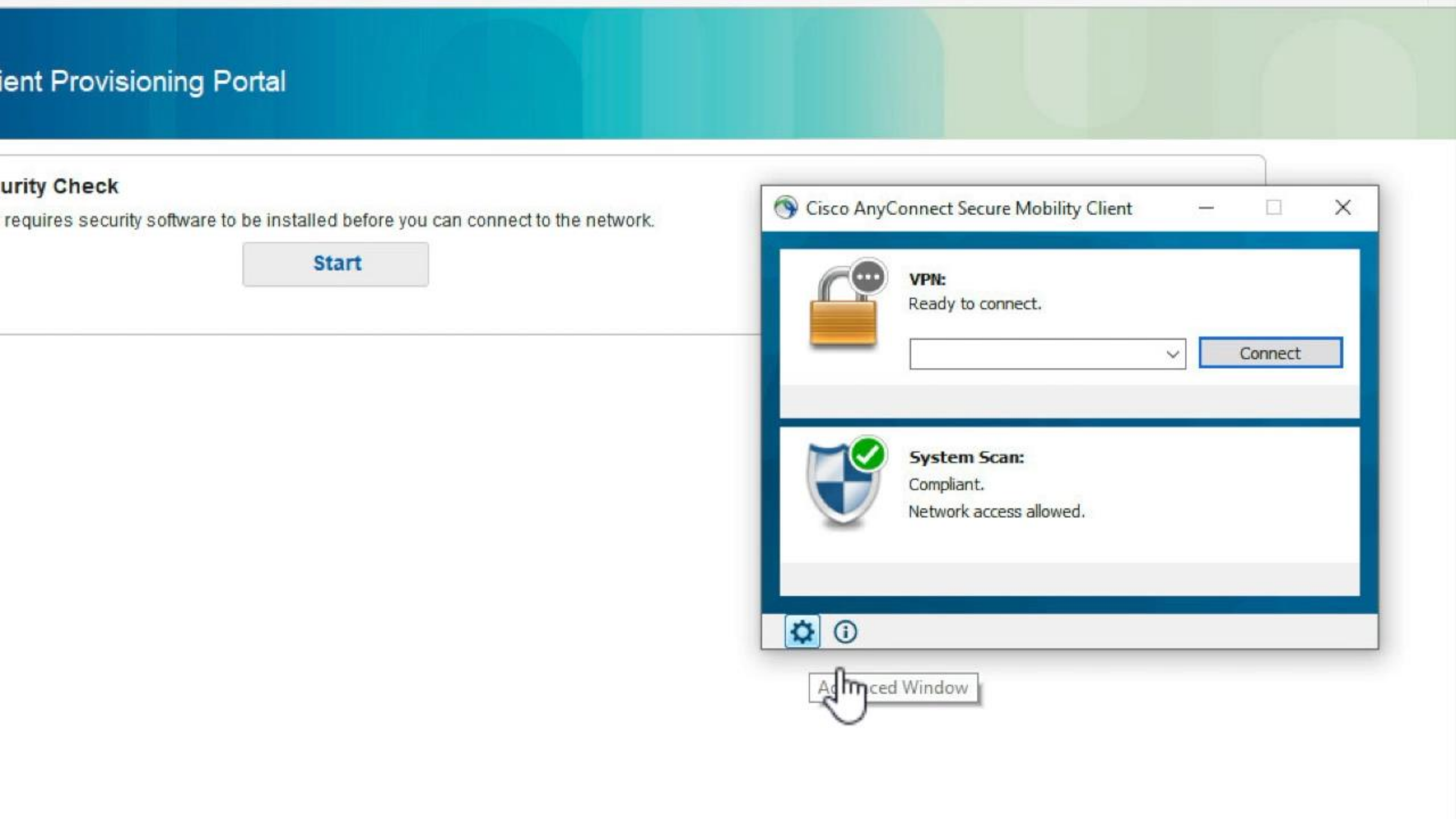
Session-ID

ABC

Session-Attributes

{alice,MAC,IP, Posture= Pending }

Demo – Misconception 3, quick identification



ient Provisioning Portal

urity Check

requires security software to be installed before you can connect to the network.

Cisco AnyConnect Secure Mobility Client

VPN:
Ready to connect.

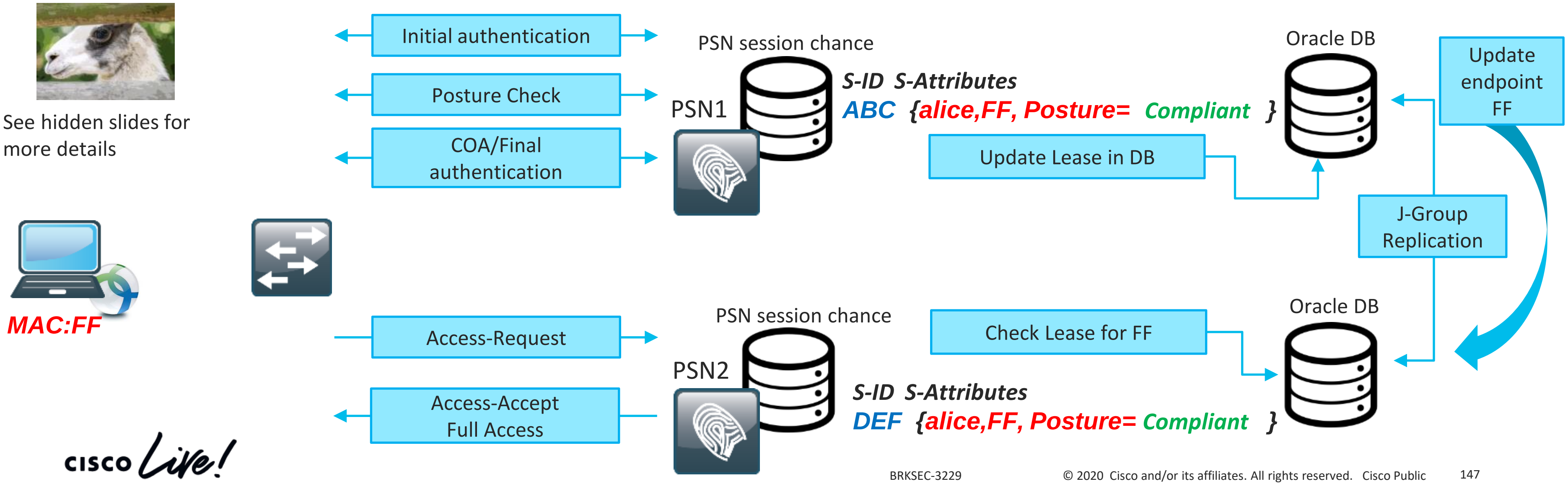
System Scan:
Compliant.
Network access allowed.

Misconception 3 – How to avoid?

- Use ‘Posture lease’ when possible. Posture lease allows ISE to mark endpoint as compliant for defined time period (1-365 days).

When endpoint has a valid lease posture status of session is always ‘Compliant’

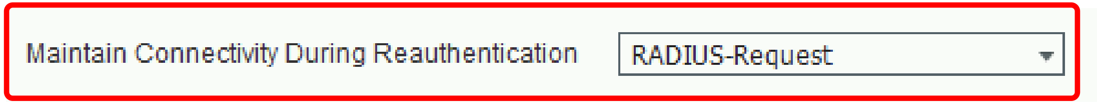
Since posture lease is an endpoint attribute this value is known to all nodes



See hidden slides for more details

Misconception 3 – How to avoid? (continue)

- If re-authentication timer is needed send it from ISE, with –



Maintain Connectivity During Reauthentication: RADIUS-Request

- Apply same LB best practices as in Misconception 1 to ensure that re-authentication hits the same PSN when possible

- Use different L3 subnets when possible for ‘Restricted’ and ’Full Access’ states to trigger discovery by DG change

- Enable PRA with re-assessment timer equal to re-authentication timer. This can help to trigger discovery by re-assessment failure when DG change is impossible by design

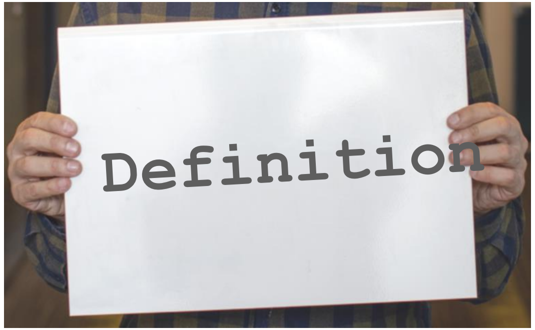
See hidden slides for more details

Misconception 4 – packets on the wire

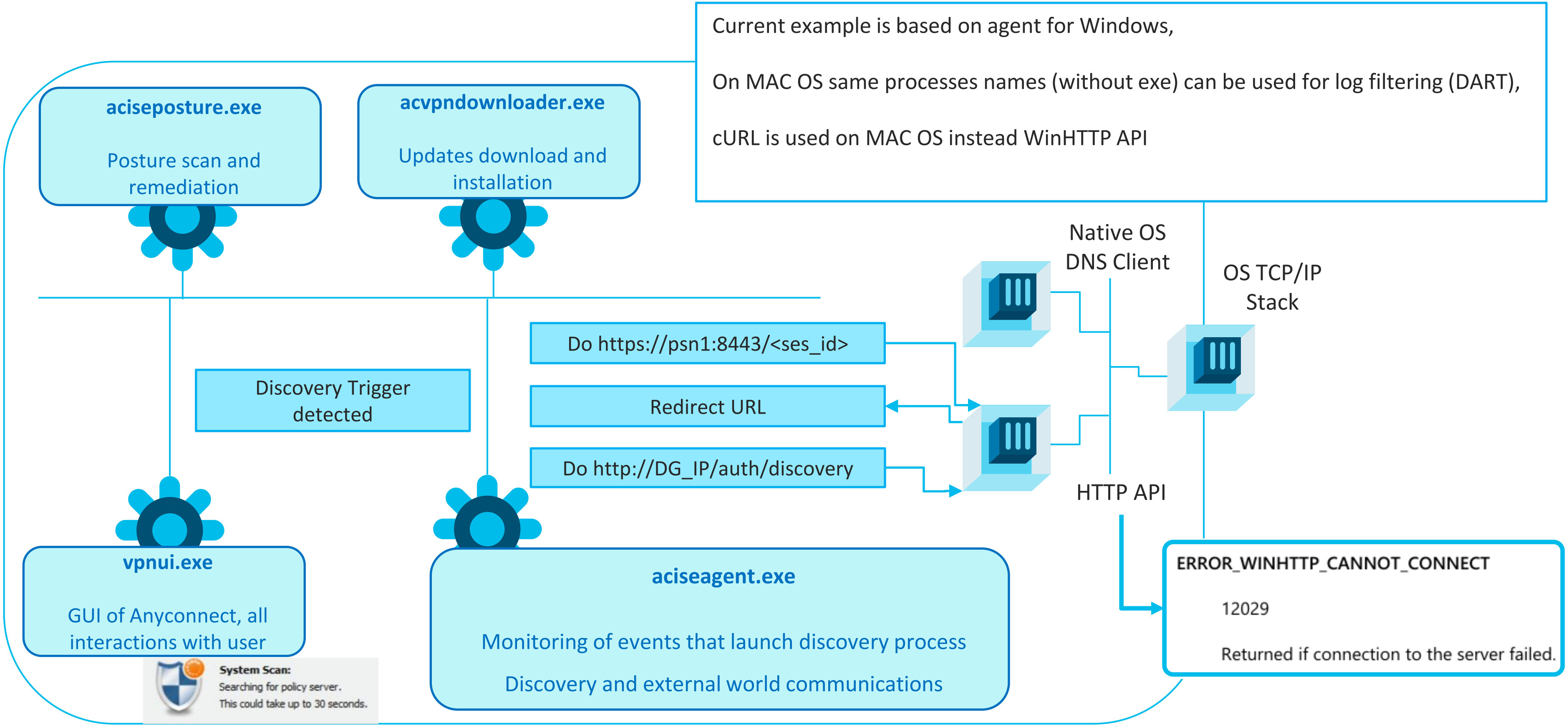
4. ISE Posture module manages packet flow

Misconception definition –

”ISE posture module has ultimate responsibility on all packets needed to be generated during discovery and posture process”



ISE Posture module architecture



Current example is based on agent for Windows,

On MAC OS same processes names (without exe) can be used for log filtering (DART),

cURL is used on MAC OS instead WinHTTP API

acisеposture.exe

Posture scan and remediation

acvpndownloader.exe

Updates download and installation

Discovery Trigger detected

Do https://psn1:8443/<ses_id>

Redirect URL

Do http://DG_IP/auth/discovery

Native OS DNS Client

OS TCP/IP Stack

HTTP API

vpnui.exe

GUI of Anyconnect, all interactions with user

System Scan:
Searching for policy server.
This could take up to 30 seconds.

aciseagent.exe

Monitoring of events that launch discovery process

Discovery and external world communications

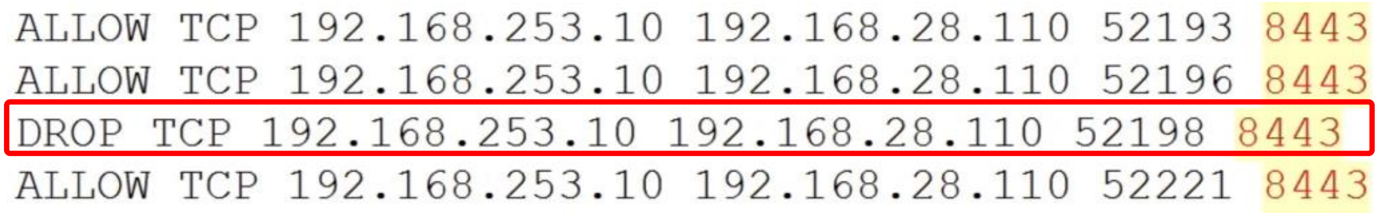
ERROR_WINHTTP_CANNOT_CONNECT

12029

Returned if connection to the server failed.

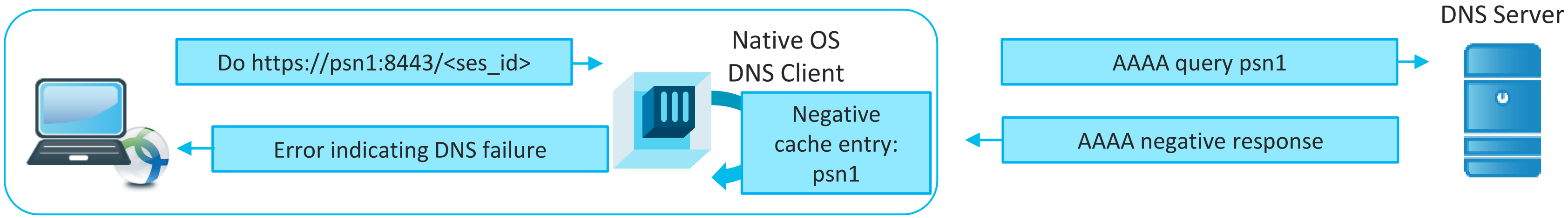
Common problematic scenarios

- Other 3rd party security application may consider posture module activities as malicious



```
ALLOW TCP 192.168.253.10 192.168.28.110 52193 8443
ALLOW TCP 192.168.253.10 192.168.28.110 52196 8443
DROP TCP 192.168.253.10 192.168.28.110 52198 8443
ALLOW TCP 192.168.253.10 192.168.28.110 52221 8443
```

- In dual stack environment MS negative DNS caching feature may impact agent communication with ISE


Do https://psn1:8443/<ses_id>
Native OS DNS Client
Negative cache entry: psn1
Error indicating DNS failure
AAAA query psn1
AAAA negative response
DNS Server

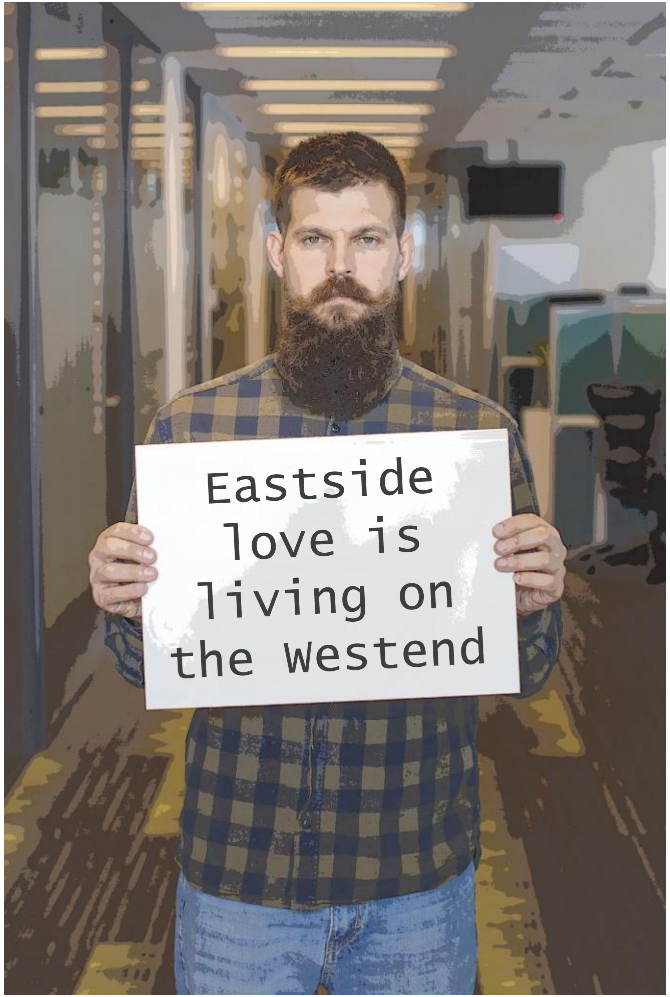
Misconception 4 – How to avoid?

- AnyConnect folders must be whitelisted in all 3rd party security application

Windows	MAC OS
C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\ C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\	/opt/cisco/anyconnect/

- In case when issue with Negative DNS caching suspected we can disable this feature on few PCs for testing. More details here

Misconception 5 – network multi-homing

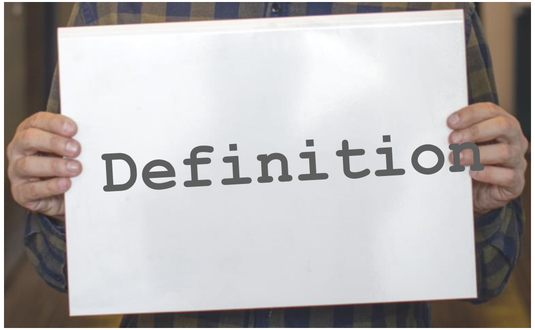


5. Multi-homing is fine

Misconception definition –

”Posture should not encounter any problems on Windows when both Wired and Wireless connections are active at the same time”

Let's have a look on standard problematic scenario -



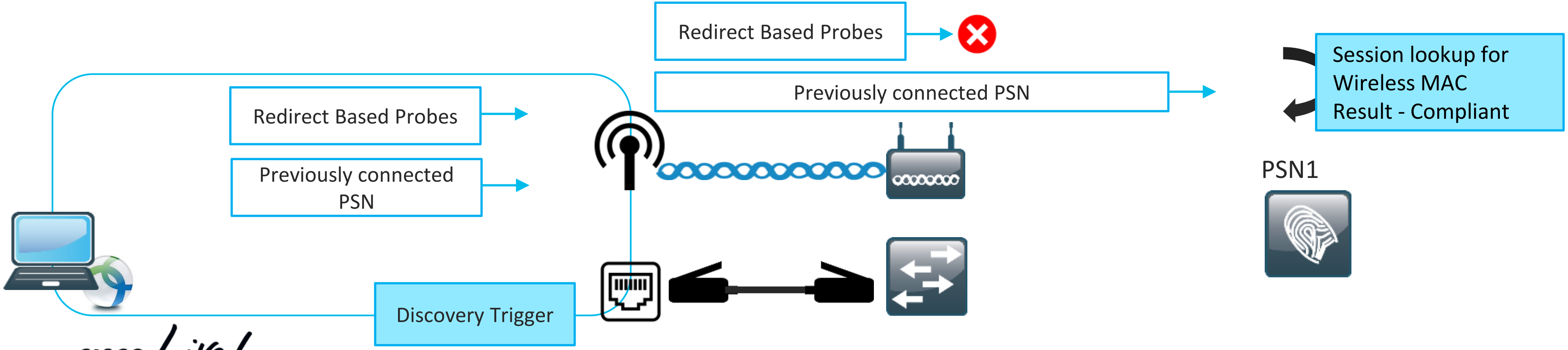
Common problematic scenario

1. User came at the morning and agent did posture over Wired connection,

2. User went to the meeting room and agent did posture on Wireless connection,

3. User returned to the desk and connected laptop back to wire – At this point Posture module detects DG change on wired connection and starts discovery but OS may not be ready yet to forward packets over wire.

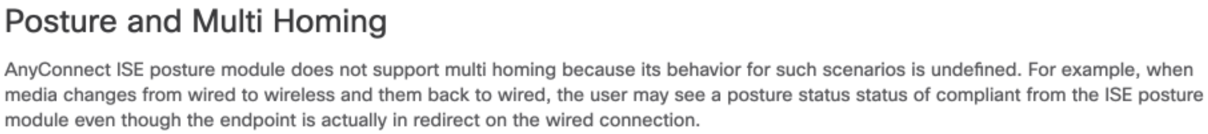
4. Posture happens again for Wireless MAC and this leaves session in redirect state on the switch



Misconception 5 – How to avoid?

In general Dual-homing is not supported by posture agent

AC 4.8 admin guide



Posture and Multi Homing

AnyConnect ISE posture module does not support multi homing because its behavior for such scenarios is undefined. For example, when media changes from wired to wireless and them back to wired, the user may see a posture status status of compliant from the ISE posture module even though the endpoint is actually in redirect on the wired connection.

The only supported solution is to use AnyConnect NAM as a supplicant as NAM allows only one connection at single point in time

If NAM cannot be used below mentioned workarounds can minimize impact:

- Use posture lease – in such case when user returns to wired connection endpoint is already compliant,
- Deny access to ISE PSNs in the 'Full Access' authorization profile with DACL/Airespace ACL. This solution will break a Posture Reassessment*

* - PRA is not supported with Multi-homing CSCve55308

Agenda

- Introduction to DEMO
- Learn by example - Profiling and Authentication Troubleshooting
- Posture Overview
- 5 common ISE Posture misconceptions
- Learn by example – Posture Troubleshooting

Learn on example – Posture troubleshooting

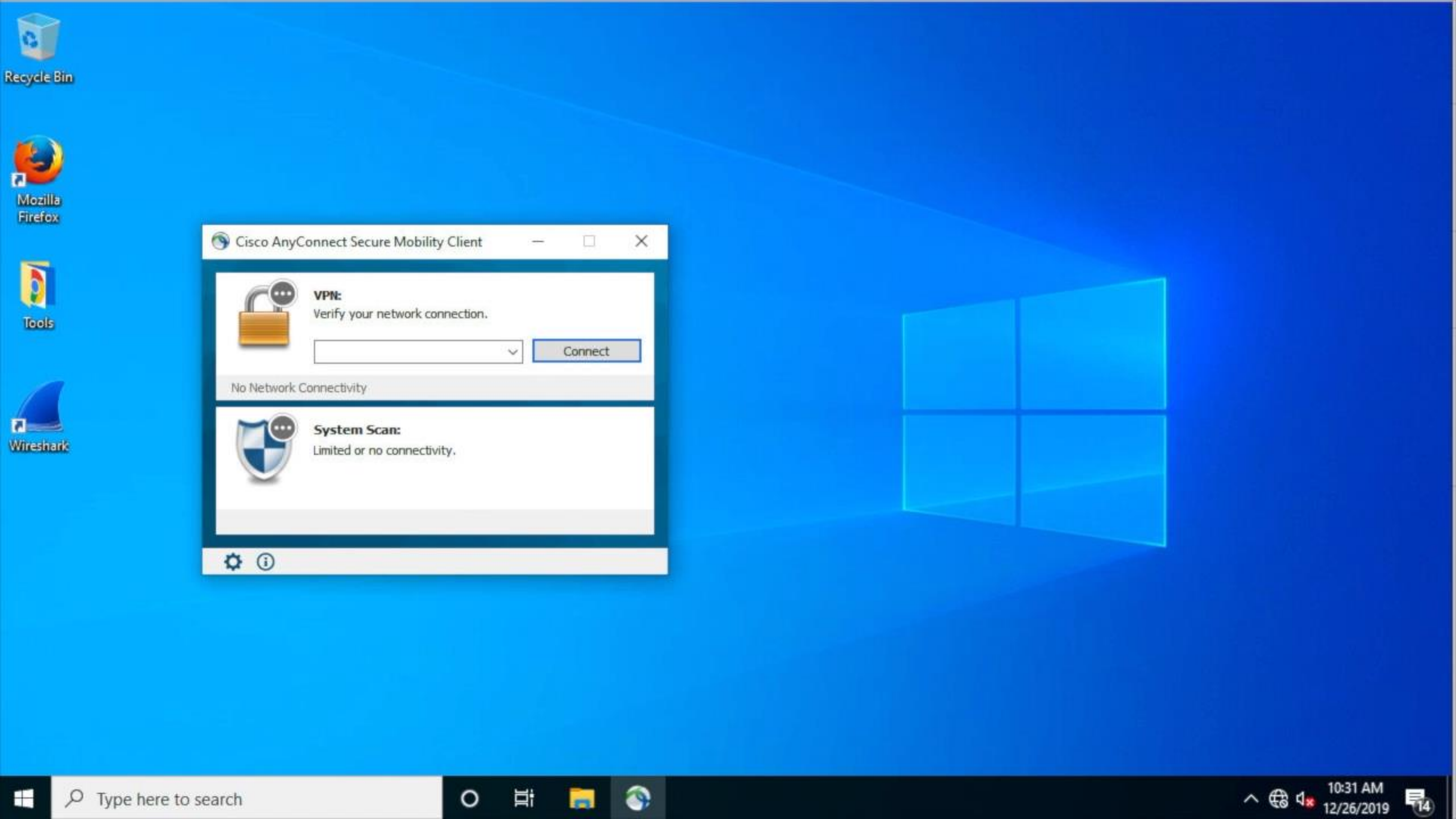
Posture got stuck on 10%

After long and exhausting troubleshooting it was decided to have a short break in Very Important Meeting …

But after meeting was resumed strange things started to happen with posture

Demo – got stuck on 10%

user experience



VPN:
Verify your network connection.

No Network Connectivity

System Scan:
Limited or no connectivity.

Define the problem

Define the problem

- **Problem Description –**

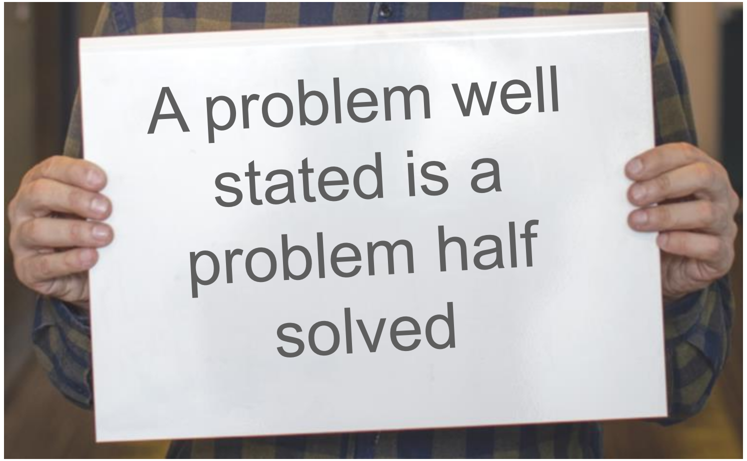
ISE posture agent gets stuck on 10% every time when endpoint connected to the network. After some time agent fails back to 'Searching Policy Server’

- **Supporting facts –**

Redirection seems to be working,

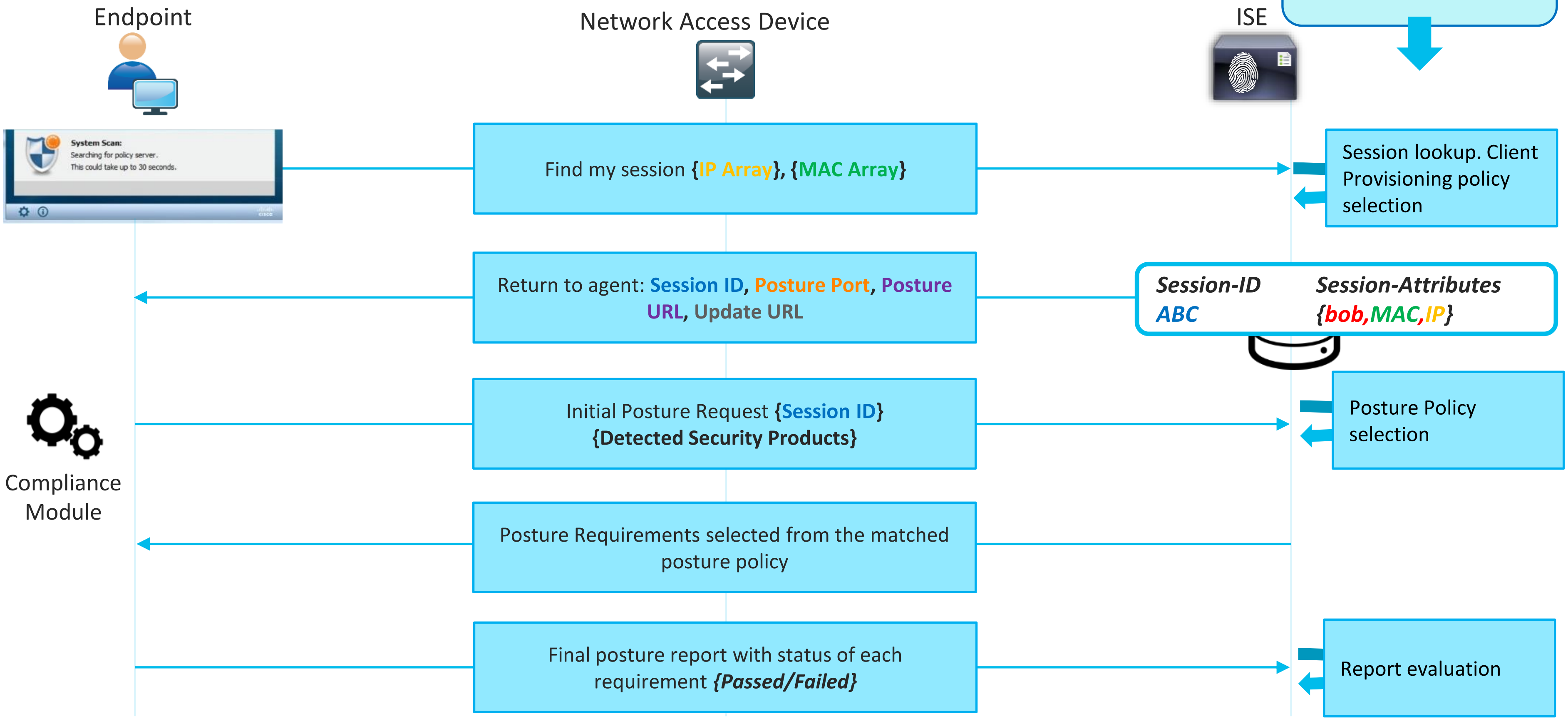
Problem is always reproducible,

Like snowball issue affects more and more users.



Posture process - Closer look

Understand how it should work



Endpoint

Network Access Device

ISE

System Scan:
Searching for policy server.
This could take up to 30 seconds.

Find my session {IP Array}, {MAC Array}

Session lookup. Client Provisioning policy selection

Return to agent: Session ID, Posture Port, Posture URL, Update URL

Session-ID	*Session-Attributes*
ABC	*{bob,MAC,IP}*

Compliance Module

Initial Posture Request {Session ID} **{Detected Security Products}**

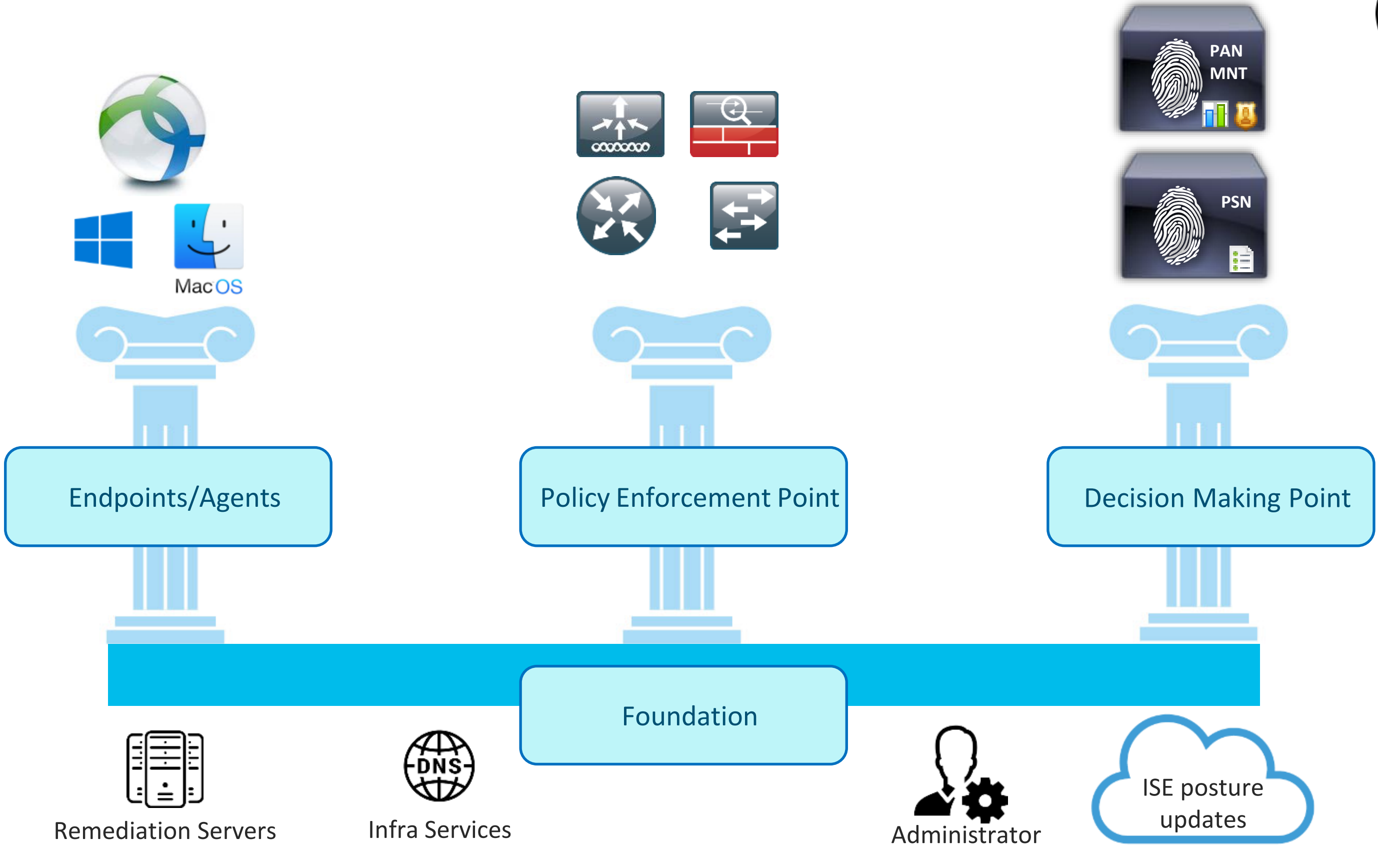
Posture Policy selection

Posture Requirements selected from the matched posture policy

Final posture report with status of each requirement ***{Passed/Failed}***

Report evaluation

What pillar can be faulty?



Endpoints/Agents

Policy Enforcement Point

Decision Making Point

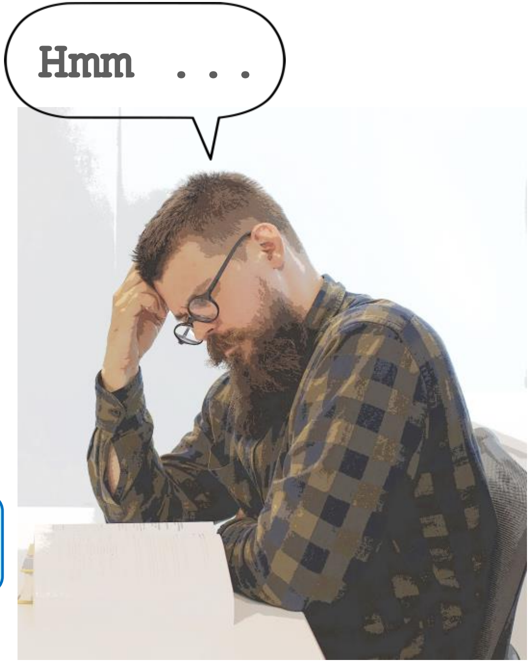
Foundation

Remediation Servers

Infra Services

Administrator

ISE posture updates



Investigation on Endpoint side

Data collection - Endpoint

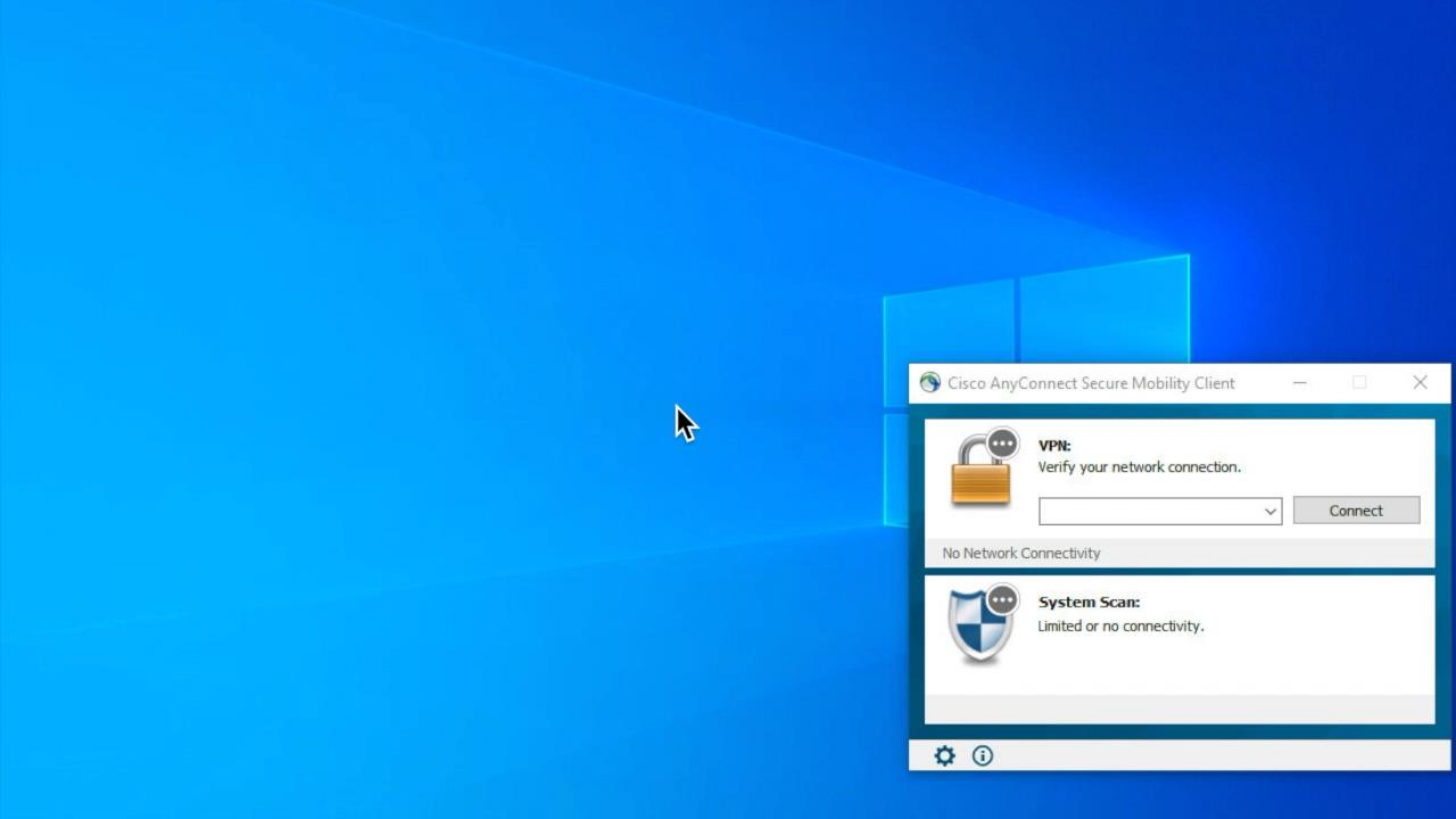
Decide what to collect and collect the data

What to check-

- DART bundle to track Discovery and Posture events in AnyConnect_ISEPosture.txt
- Packet capture – filtered by Discovery probes and ports used during the posture

Demo –

DART bundle analysis



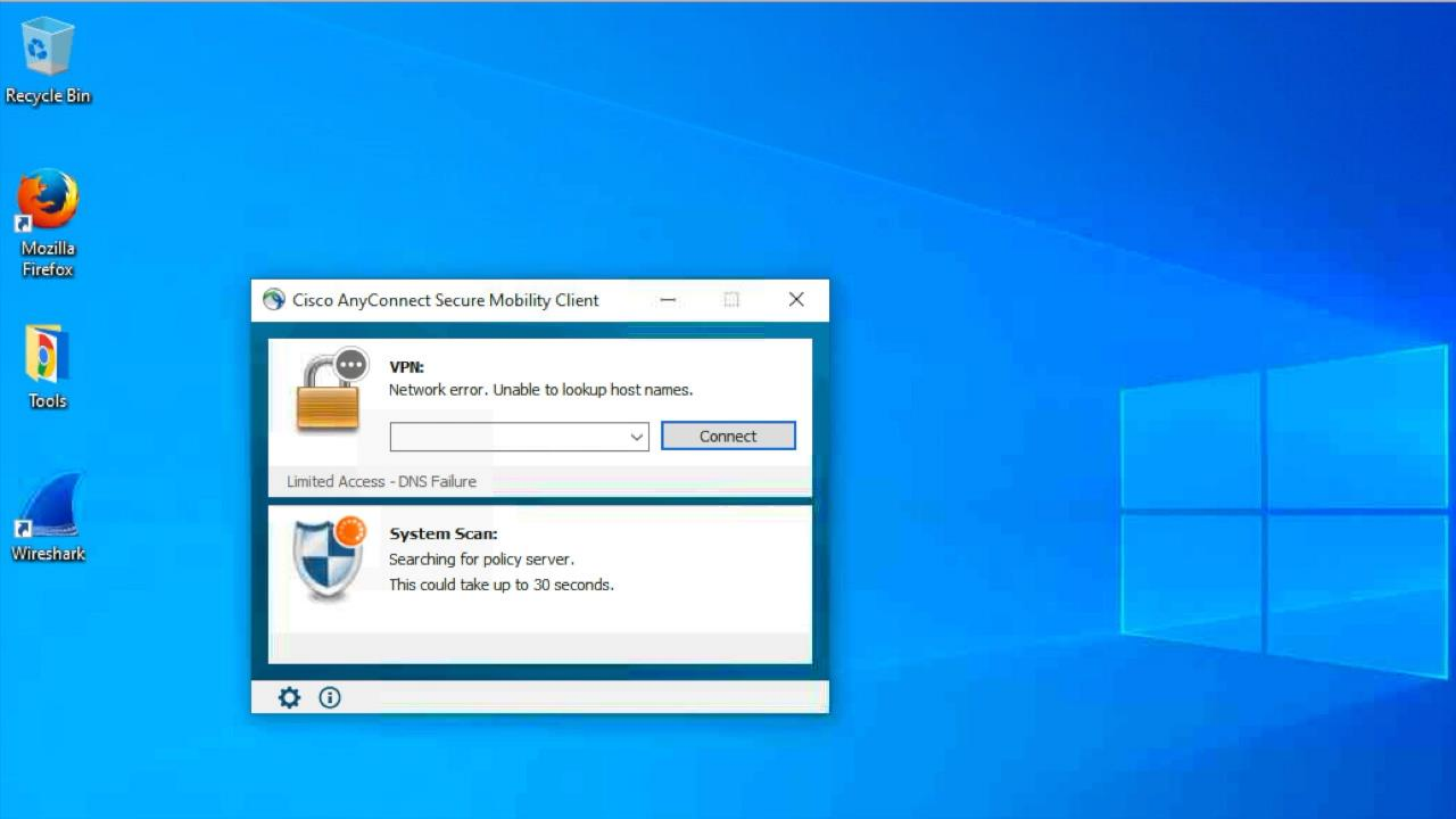
VPN:
Verify your network connection.

No Network Connectivity

System Scan:
Limited or no connectivity.

Demo –

Packet capture analysis



VPN:
Network error. Unable to lookup host names.

Limited Access - DNS Failure

System Scan:
Searching for policy server.
This could take up to 30 seconds.

Investigation on NAD side

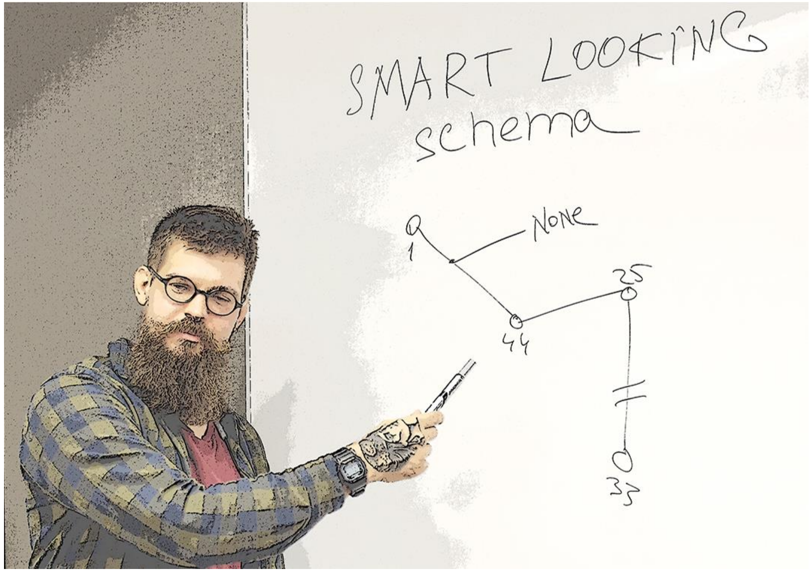
Investigation on ISE side

ISE what to collect

Decide what to collect and collect the data

Generally on ISE all posture related troubleshooting can be divided into the following areas:

- Configuration analysis – ensure that you rules, and policies are configured according to the recommendations,
- Report analysis – Detailed authentication report, Posture Assessment by Endpoint, Client Provisioning,
- Log analysis - first we need to know what debugs we need and in which files those debugs are stored.



ISE posture related debugs

For your reference

ise-psc.log

- Processing of initial and final posture report
- Posture policy selection
- PRA operations

Debug to enable

posture

Search Keys

One from list (order defines priority):

- *Session ID, EP MAC, EP IP,*

Combined with

- *cisco.cpm.posture.runtime*

guest.log

- Session lookup process when Discovery probe has reached PSN without redirect
- Client provisioning policy selection

Debug to enable

provisioning

guestaccess

client-webapp

Search Keys

One from list (order defines priority):

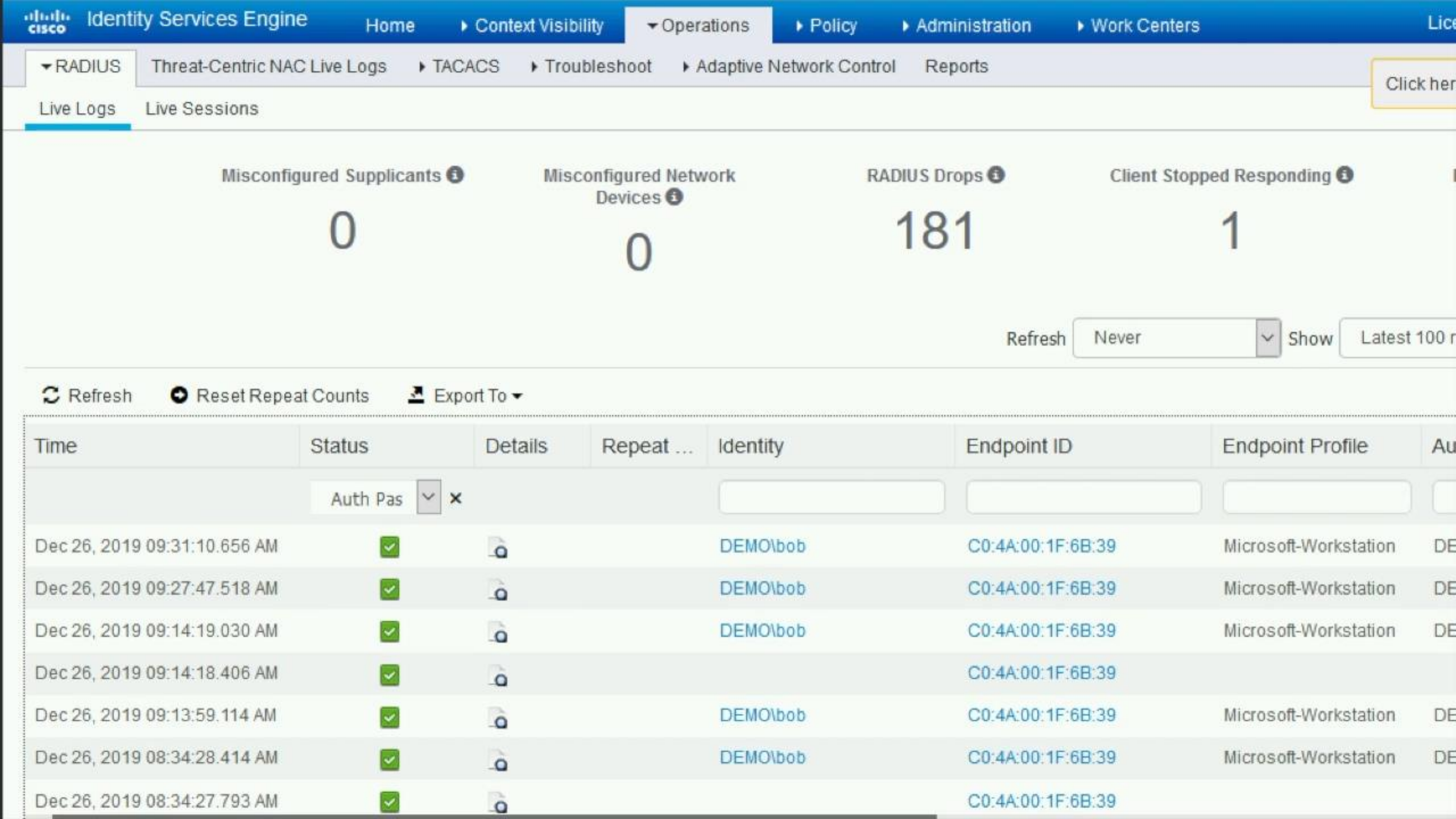
- *EP MAC, Endpoint IP, username*

Combined with

- *cisco.cpm.client.posture*

Demo –

Investigation on ISE side



Misconfigured Supplicants: 0

Misconfigured Network Devices: 0

RADIUS Drops: 181

Client Stopped Responding: 1

Refresh: Never   Show: Latest 100 r

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Au
	Auth Pas ×						
Dec 26, 2019 09:31:10.656 AM	✓	🔍		DEMO\bob	C0:4A:00:1F:6B:39	Microsoft-Workstation	DE
Dec 26, 2019 09:27:47.518 AM	✓	🔍		DEMO\bob	C0:4A:00:1F:6B:39	Microsoft-Workstation	DE
Dec 26, 2019 09:14:19.030 AM	✓	🔍		DEMO\bob	C0:4A:00:1F:6B:39	Microsoft-Workstation	DE
Dec 26, 2019 09:14:18.406 AM	✓	🔍			C0:4A:00:1F:6B:39		
Dec 26, 2019 09:13:59.114 AM	✓	🔍		DEMO\bob	C0:4A:00:1F:6B:39	Microsoft-Workstation	DE
Dec 26, 2019 08:34:28.414 AM	✓	🔍		DEMO\bob	C0:4A:00:1F:6B:39	Microsoft-Workstation	DE
Dec 26, 2019 08:34:27.793 AM	✓	🔍			C0:4A:00:1F:6B:39		

So where are we with troubleshooting?

- Capture shows communication over port 8443
- Packets are crossing WLC
- No posture report received by ISE
- In DART we fail with - unable to send request: 12002

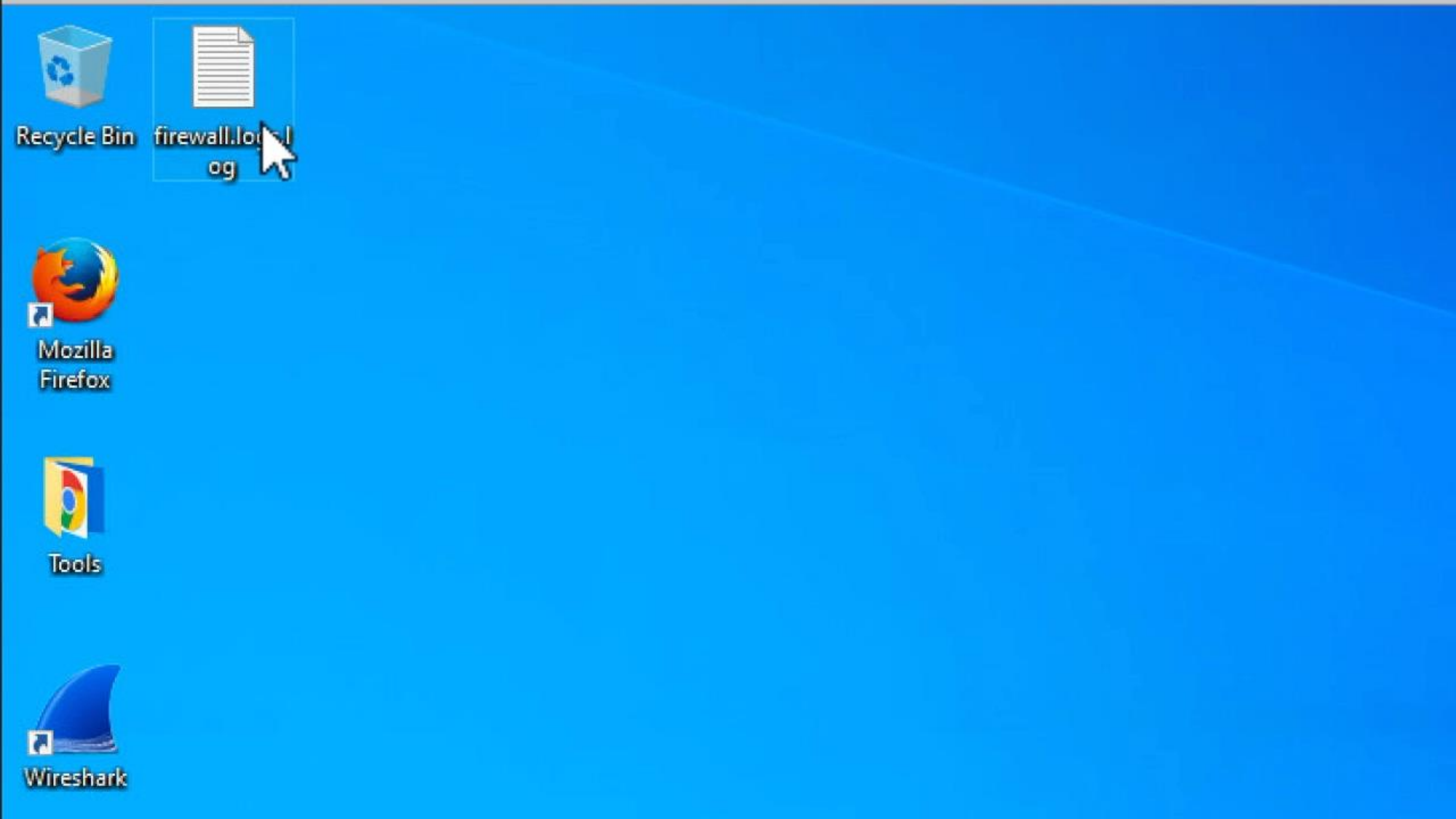
Posture got stuck on 10%– Build a Theory

Analyze the data to build the theory

All date collected so far points to some issue on the endpoint itself

As a next step we need to investigate logs from 3rd party Security Software to understand what may break communication over port 8443

Demo – 3rd party log investigation, confirm the theory

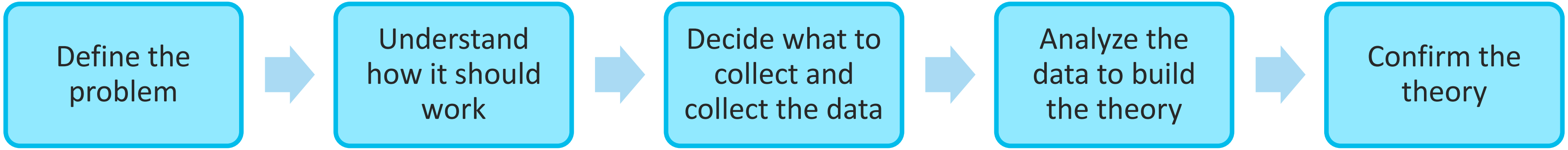

Recycle Bin
firewall.log.log
Mozilla Firefox
Tools
Wireshark

Issue recap

- Monday morning desktop security team discovered new Windows vulnerability
- Due to absence of fix from vendor more strict rules were enforced on endpoint firewalls
- Endpoints started to encounter problems after firewall changes were distributed on next posture attempt

Key Takeaways

It's better to avoid some problems instead of troubleshooting them



Define the problem

Understand how it should work

Decide what to collect and collect the data

Analyze the data to build the theory

Confirm the theory

Full version of slide deck and all demos are available for download

BRKSEC-3229

In case of access problem please contact
skuchere@cisco.com or ekorneyc@cisco.com

Complete your online survey to help us make this session better

Thank you

You make **possible**