Configure Device Sensor for ISE Profiling

Contents

Introduction

This document describes how to configure the Device Sensor so that it can be used for profiling purposes on ISE.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Radius protocol
- Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), and Dynamic Host Configuration Protocol (DHCP)
- Cisco Identity Service Engine (ISE)
- Cisco Catalyst Switch 2960

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ISE version 1.3 patch 3
- Cisco Catalyst Switch 2960s version 15.2(2a)E1
- Cisco IP Phone 8941 version SCCP 9-3-4-17

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

A Device Sensor is a feature of access devices. It allows to collect information about connected endpoints. Mostly, information collected by the Device Sensor can come from these protocols:

- CDP
- LLDP
- DHCP

Note: On some platforms, it is possible to also use H323, Session Initiation Protocol (SIP), Multicast Domain Resolution (MDNS), or HTTP protocols. Configuration possibilities for device sensor capabilities can vary from protocol to protocol. An example is available on Cisco Catalyst 3850 with software 03.07.02.E.

Once the information is collected, it can be encapsulated in radius accounting and sent to a profiling server.

In this article, ISE is used as a profiling server.

Configure

Step 1. Standard AAA Configuration

In order to configure Authentication, Authorization, and Accounting (AAA), refer to these steps:

1. Enable AAA using aaa new-model command and enable 802.1X globally on the switch.

2. Configure the Radius server and enable dynamic authorization (Change of Authorization - CoA).

3. Enable CDP and LLDP protocols.

4. Add switchport authentication configuration

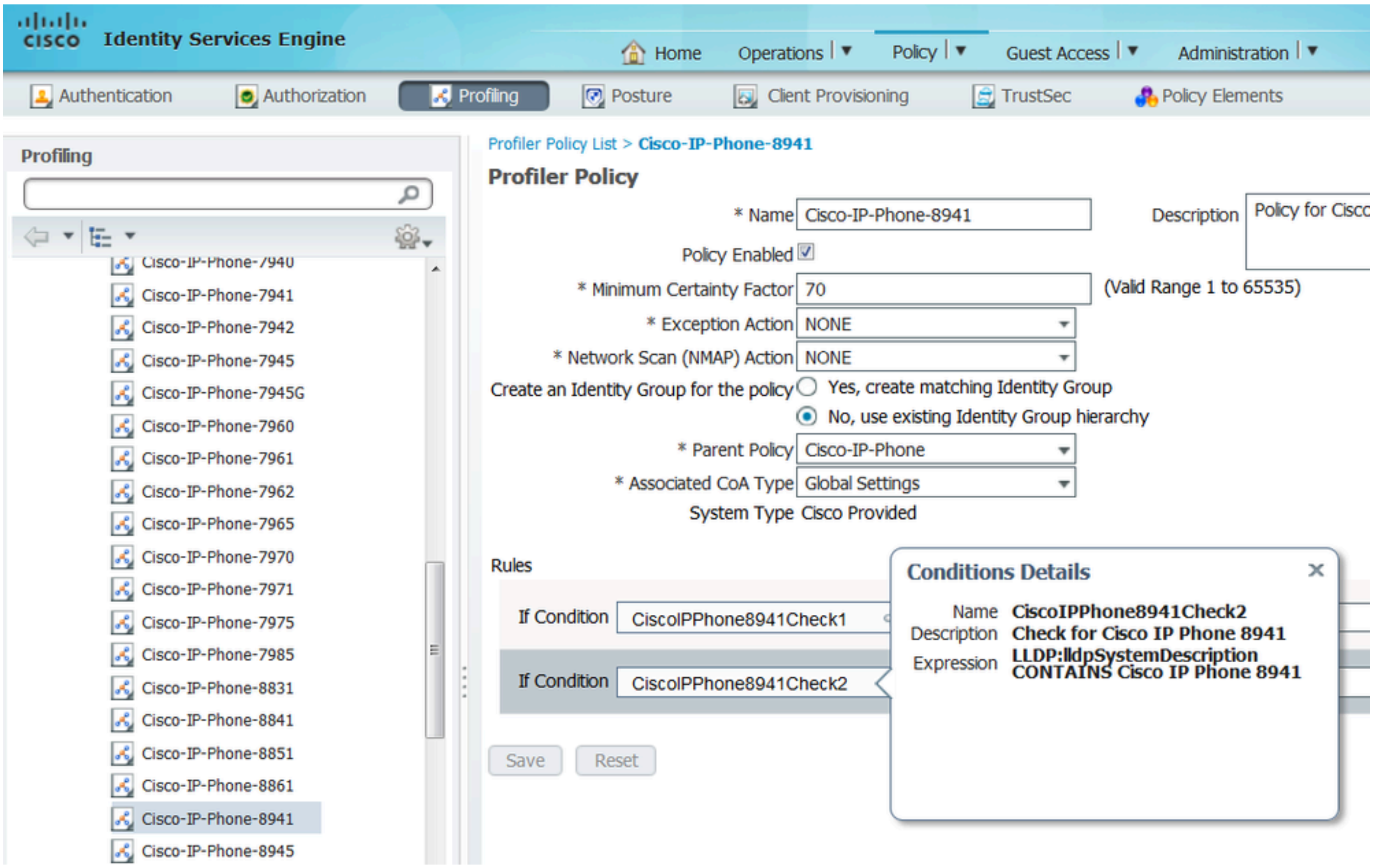
```
!
aaa new-model
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting update newinfo
aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
 client 1.1.1.1 server-key xyz
!
dot1x system-auth-control
!
lldp run
cdp run
!
interface GigabitEthernet1/0/13
 description IP_Phone_8941_connected
 switchport mode access
 switchport voice vlan 101
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 2
 spanning-tree portfast
end
!
radius-server host 1.1.1.1 auth-port 1812 acct-port 1813 key xyz
!
```

Note: In the newer software version, the command `radius-server vsa send accounting` is enabled by default. If you cannot see attributes sent in accounting, verify if the command is enabled.

Step 2. Configure Device Sensor

1. Determine which attributes from CDP/LLDP are needed in order to profile the device. In the case of Cisco IP Phone 8941 you can use these:

- LLDP SystemDescription attribute
- CDP CachePlatform attribute



Cisco-IP-Phone-7940
Cisco-IP-Phone-7941
Cisco-IP-Phone-7942
Cisco-IP-Phone-7945
Cisco-IP-Phone-7945G
Cisco-IP-Phone-7960
Cisco-IP-Phone-7961
Cisco-IP-Phone-7962
Cisco-IP-Phone-7965
Cisco-IP-Phone-7970
Cisco-IP-Phone-7971
Cisco-IP-Phone-7975
Cisco-IP-Phone-7985
Cisco-IP-Phone-8831
Cisco-IP-Phone-8841
Cisco-IP-Phone-8851
Cisco-IP-Phone-8861
Cisco-IP-Phone-8941
Cisco-IP-Phone-8945

Profiler Policy List > **Cisco-IP-Phone-8941**

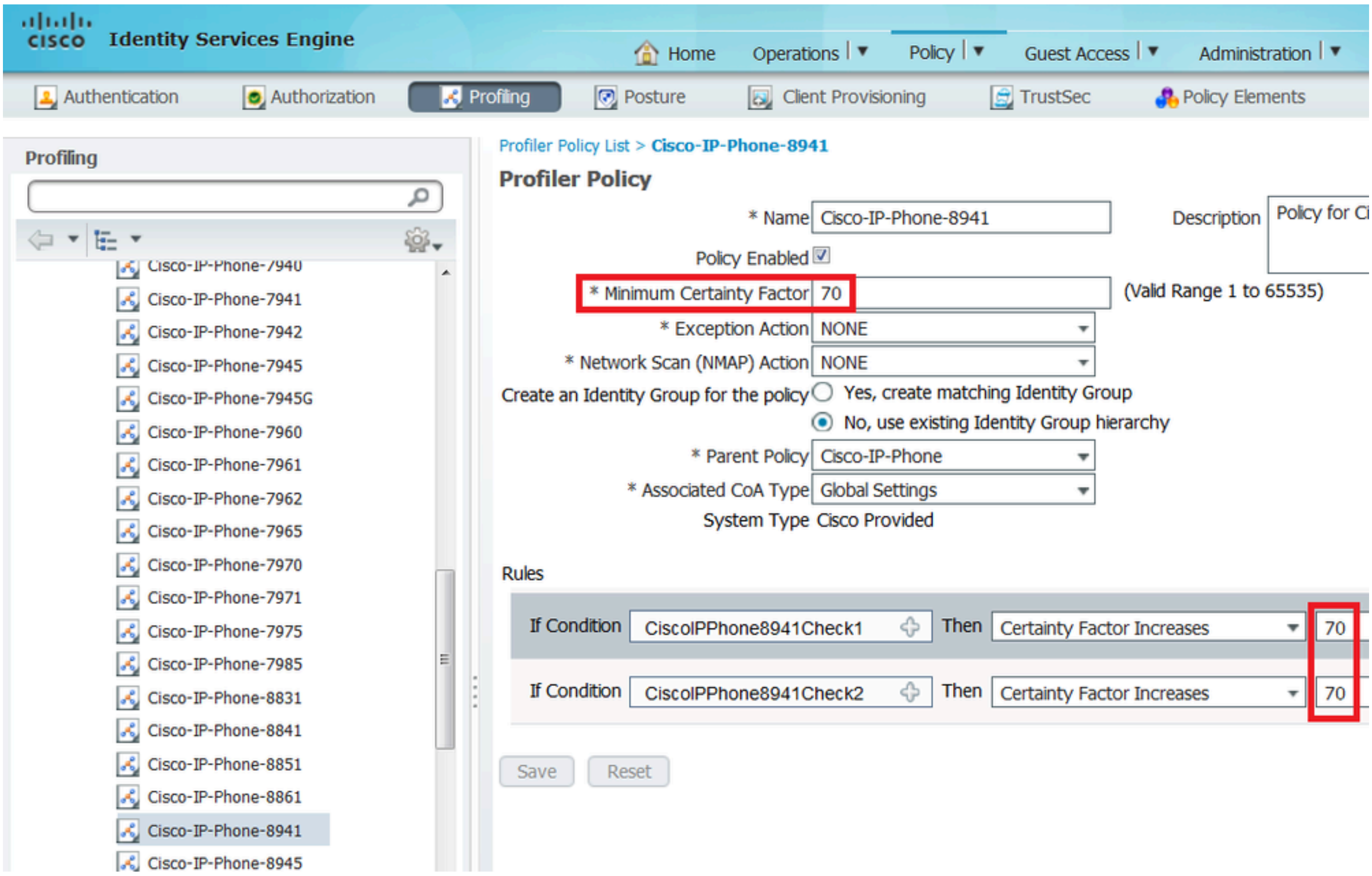
Profiler Policy

* Name Cisco-IP-Phone-8941
Description Policy for Cisc
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 CiscoIPPhone8941Check1
If Condition CiscoIPPhone8941Check2

Conditions Details
Name **CiscoIPPhone8941Check2**
Description **Check for Cisco IP Phone 8941**
Expression **LLDP:lldpSystemDescription CONTAINS Cisco IP Phone 8941**

For our purpose, it is enough to obtain just one of those since both of them provide a Certainty Factory increase of 70, and the Minimum Certainty Factory required to be profiled as Cisco-IP-Phone-8941 is 70:



Cisco-IP-Phone-7940
Cisco-IP-Phone-7941
Cisco-IP-Phone-7942
Cisco-IP-Phone-7945
Cisco-IP-Phone-7945G
Cisco-IP-Phone-7960
Cisco-IP-Phone-7961
Cisco-IP-Phone-7962
Cisco-IP-Phone-7965
Cisco-IP-Phone-7970
Cisco-IP-Phone-7971
Cisco-IP-Phone-7975
Cisco-IP-Phone-7985
Cisco-IP-Phone-8831
Cisco-IP-Phone-8841
Cisco-IP-Phone-8851
Cisco-IP-Phone-8861
Cisco-IP-Phone-8941
Cisco-IP-Phone-8945

Profiler Policy List > **Cisco-IP-Phone-8941**

Profiler Policy

* Name Cisco-IP-Phone-8941
Description Policy for Ci
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 CiscoIPPhone8941Check1 Then Certainty Factor Increases 70
If Condition CiscoIPPhone8941Check2 Then Certainty Factor Increases 70

Note: In order to be profiled as a specific Cisco IP Phone, you must satisfy minimum conditions for all parent profiles. This means the profiler must match Cisco-Device (minimum Certainty Factor 10) and Cisco-IP-Phone (minimum Certainty Factor 20). Even though the profiler matches those two profiles, it must still be profiled as a specific Cisco IP Phone since each IP Phone model has a minimum Certainty Factor of 70. The device is assigned to the profile for which it has the highest Certainty Factor.

2. Configure two filter lists - one for CDP and another one for LLDP. Those indicate which attributes must be included in Radius accounting messages. This step is optional.

3. Create two filter-specs for CDP and LLDP. In the filter-spec, you can indicate the list of attributes that must be included or excluded from accounting messages. In the example, these attributes are included:

- device-name from CDP
- system-description from LLDP

You can configure additional attributes to be transmitted via Radius to ISE if needed. This step is also optional.

4. Add the command `device-sensor notify all-changes`. It triggers updates whenever TLVs are added, modified, or

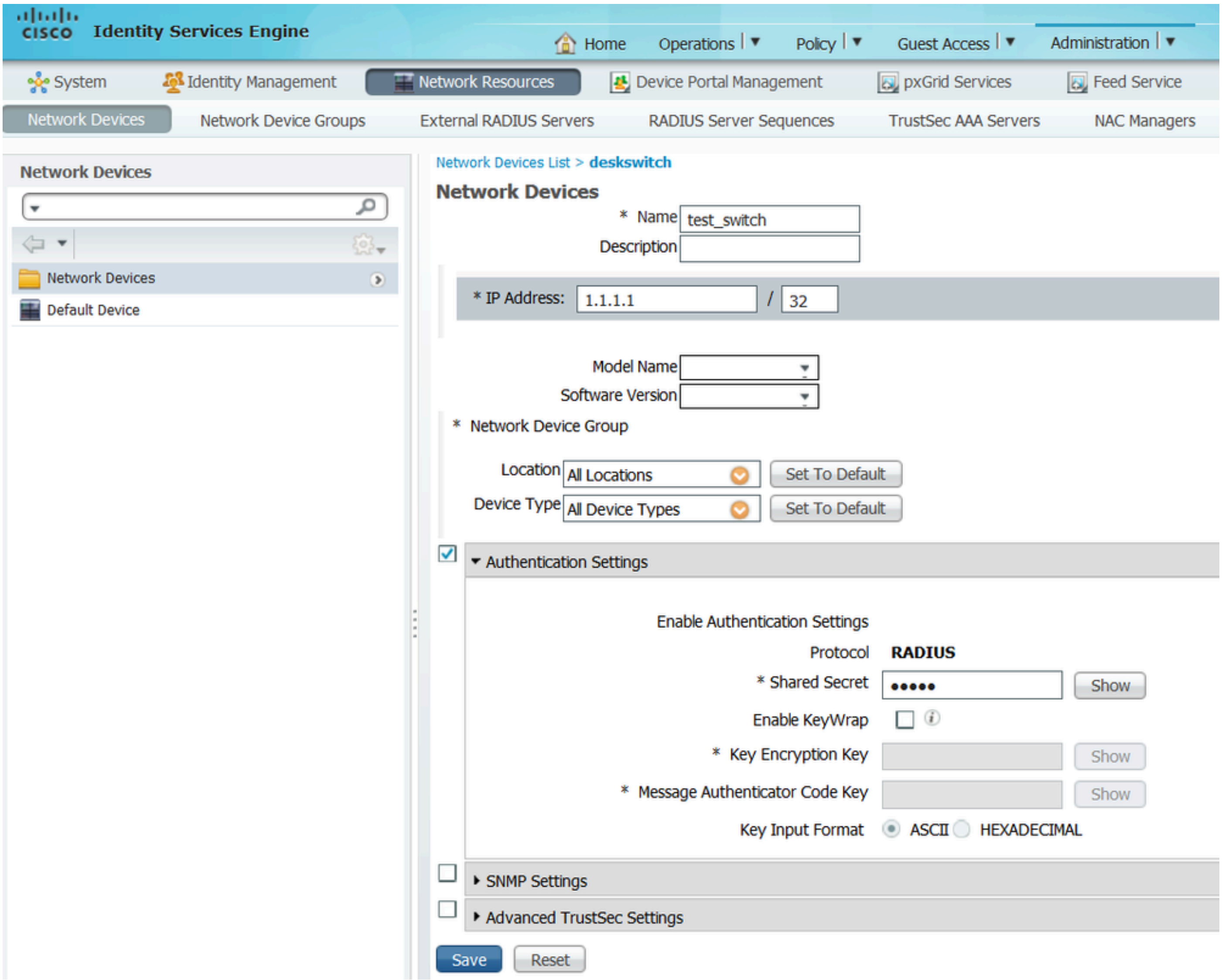
removed for the current session.

5. In order to actually send the information gathered via Device Sensor functionality, you must explicitly tell the switch to accomplish so with the command device-sensor accounting.

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

Step 3. Configure Profiling on ISE

1. Add the switch as a network device in Administration > Network Resources > Network Devices. Use the radius server key from the switch as a shared secret in Authentication Settings:



Network Devices

* Name test_switch

Description

* IP Address: 1.1.1.1 / 32

Model Name

Software Version

* Network Device Group

Location All Locations

Device Type All Device Types

☑ Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret •••••

Enable KeyWrap □

* Key Encryption Key

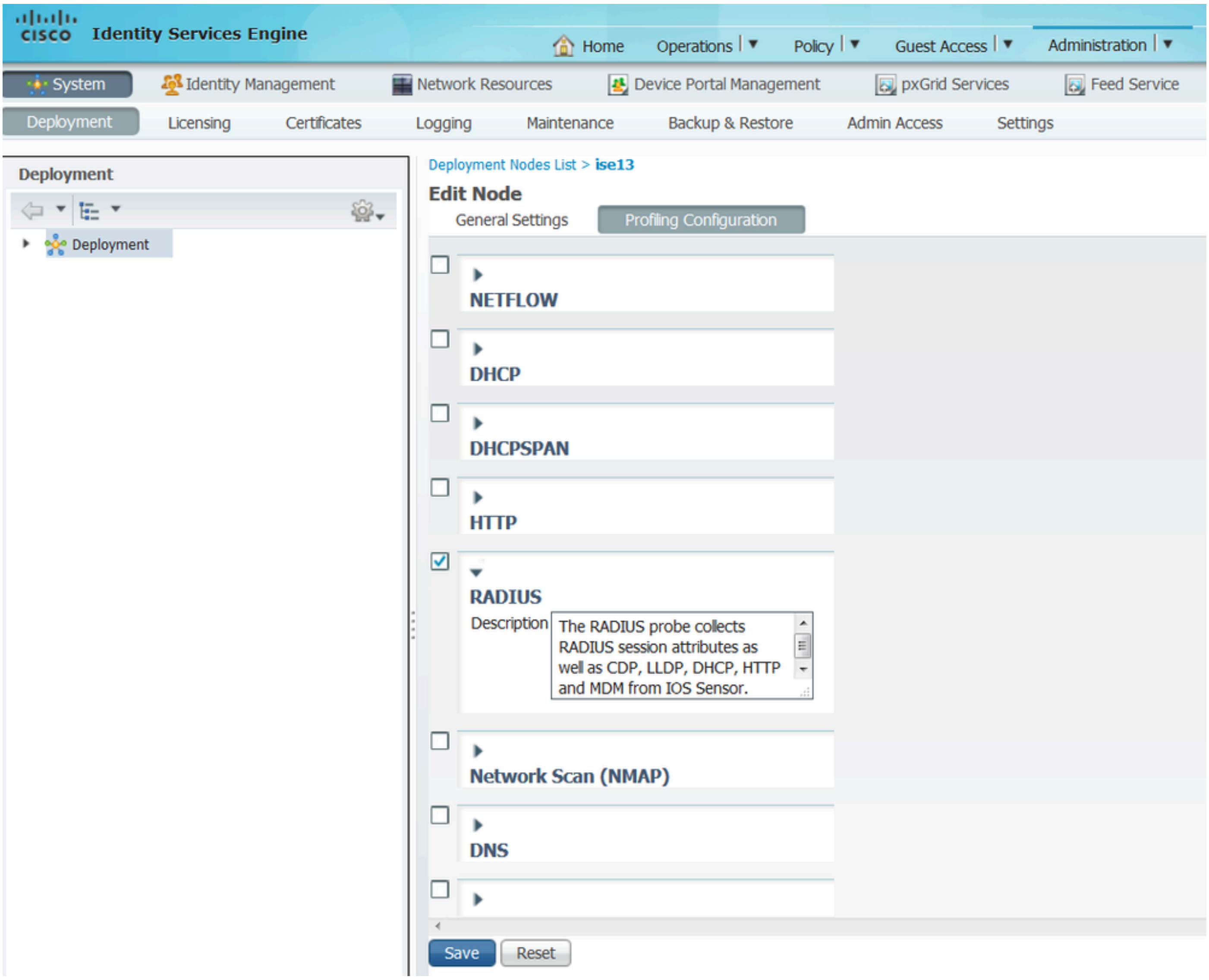
* Message Authenticator Code Key

Key Input Format ● ASCII ○ HEXADECIMAL

□ SNMP Settings

□ Advanced TrustSec Settings

2. Enable the Radius probe on the profiling node in Administration > System > Deployment > ISE node > Profiling Configuration. If all PSN nodes must be used for profiling, enable the probe on all of them:



Deployment Nodes List > ise13

Edit Node

General Settings | Profiling Configuration

□ NETFLOW

□ DHCP

□ DHCPSPAN

□ HTTP

☑ RADIUS

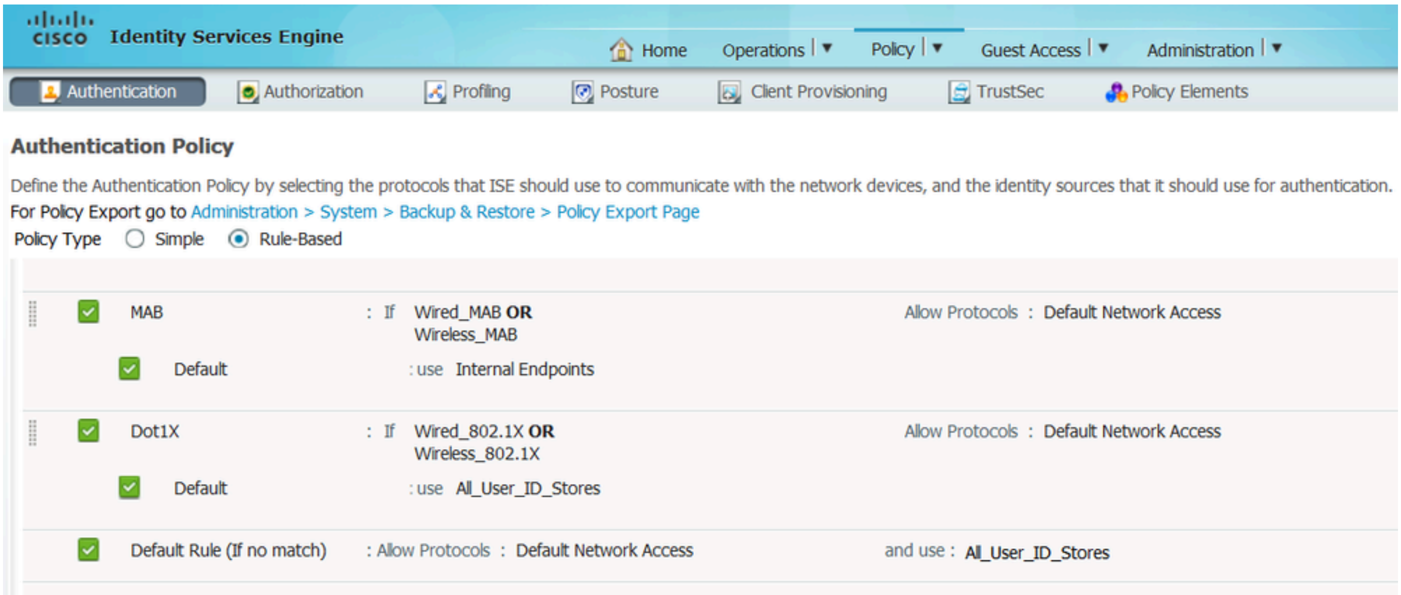
Description: The RADIUS probe collects RADIUS session attributes as well as CDP, LLDP, DHCP, HTTP and MDM from IOS Sensor.

□ Network Scan (NMAP)

□ DNS

□

3. Configure ISE Authentication Rules. In the example, the default authentication rules preconfigured on ISE are used:



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB **OR** Wireless_MAB Allow Protocols : Default Network Access

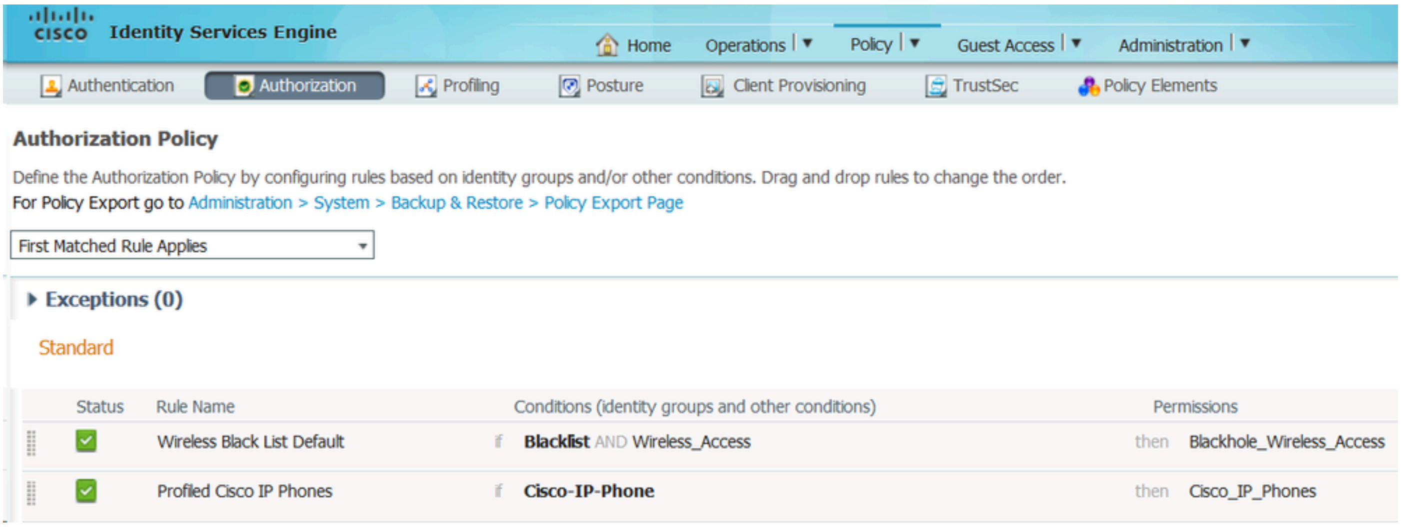
☑ Default : use Internal Endpoints

☑ Dot1X : If Wired_802.1X **OR** Wireless_802.1X Allow Protocols : Default Network Access

☑ Default : use All_User_ID_Stores

☑ Default Rule (If no match) : Allow Protocols : Default Network Access and use : All_User_ID_Stores

4. Configure ISE Authorization Rules. The Profiled Cisco IP Phones rule is used, which is preconfigured on ISE:



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

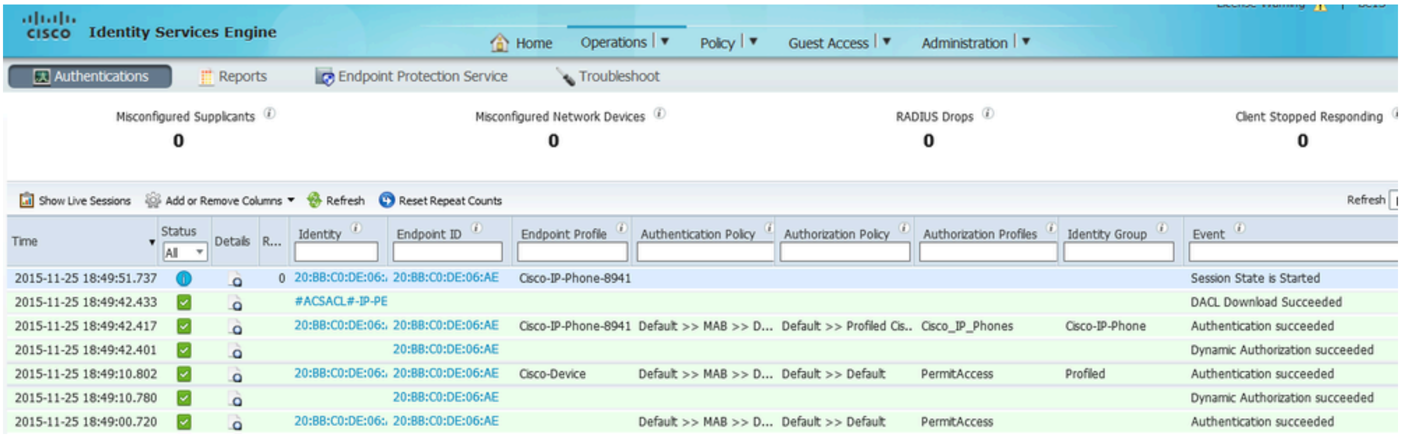
Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones

Verify

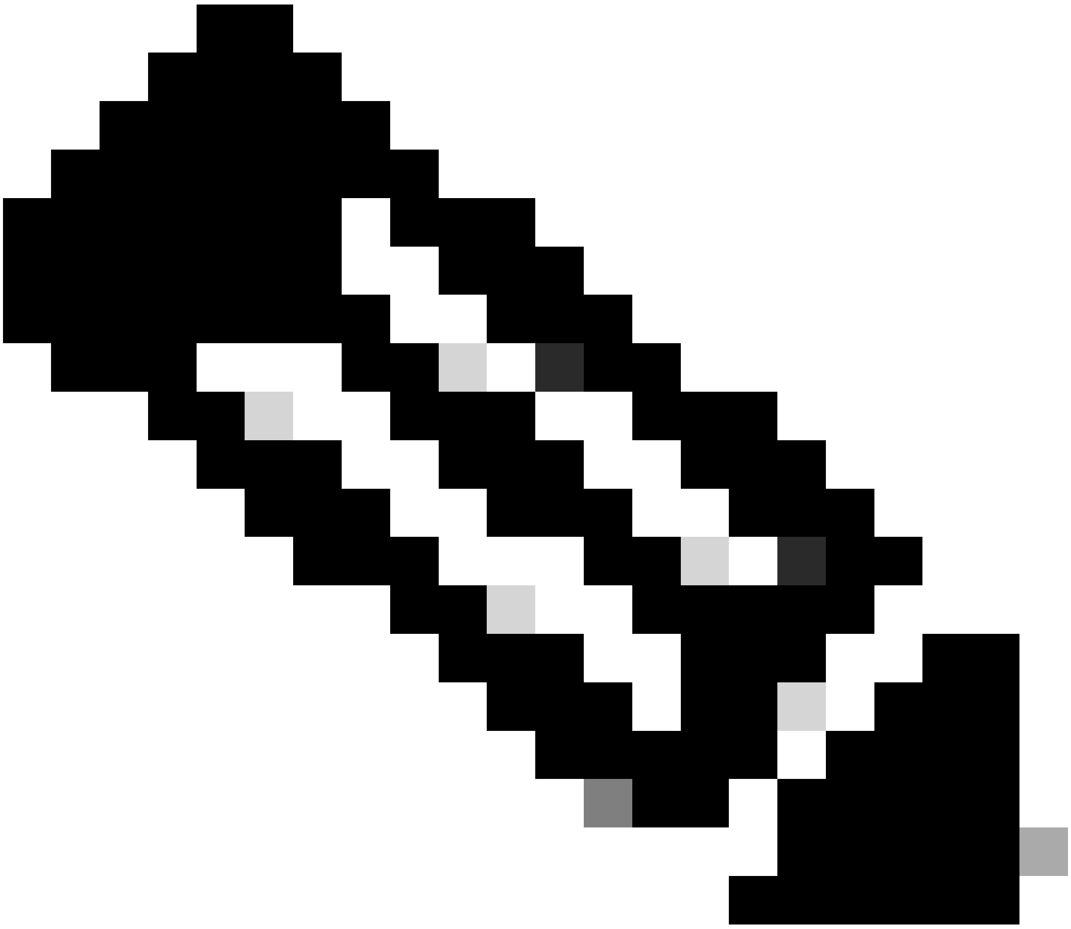
In order to verify if profiling is working correctly, refer to Operations > Authentications on ISE:



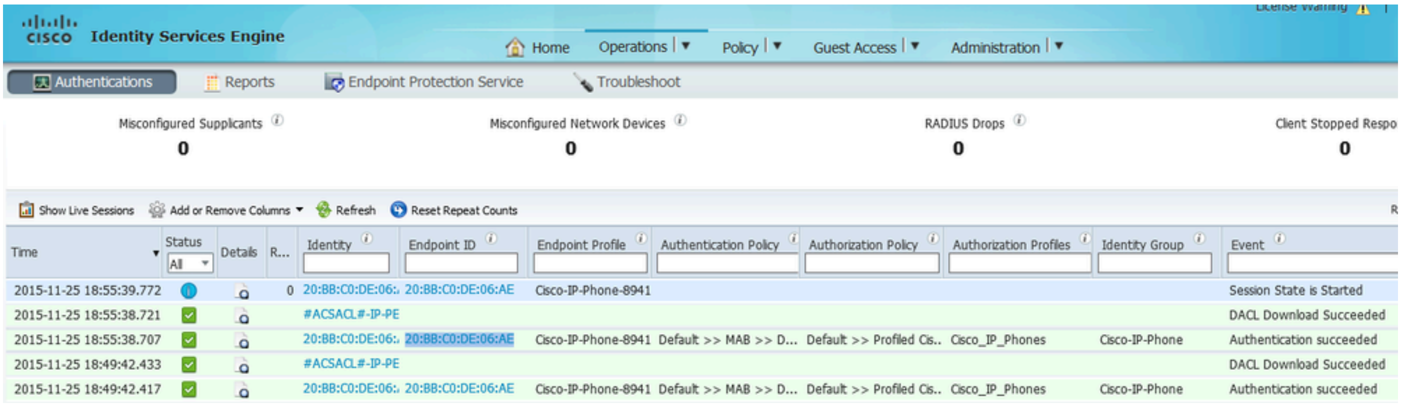
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding
0	0	0	0

Time	Status	Details	R...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Identity Group	Event
2015-11-25 18:49:51.737	i		0	20:BB:C0:DE:06:.	20:BB:C0:DE:06:AE	Cisco-IP-Phone-8941					Session State is Started
2015-11-25 18:49:42.433	✓			#ACSACL#-IP-PE							DACL Download Succeeded
2015-11-25 18:49:42.417	✓			20:BB:C0:DE:06:.	20:BB:C0:DE:06:AE	Cisco-IP-Phone-8941	Default >> MAB >> D...	Default >> Profiled Cis..	Cisco_IP_Phones	Cisco-IP-Phone	Authentication succeeded
2015-11-25 18:49:42.401	✓				20:BB:C0:DE:06:AE						Dynamic Authorization succeeded
2015-11-25 18:49:10.802	✓			20:BB:C0:DE:06:.	20:BB:C0:DE:06:AE	Cisco-Device	Default >> MAB >> D...	Default >> Default	PermitAccess	Profiled	Authentication succeeded
2015-11-25 18:49:10.780	✓				20:BB:C0:DE:06:AE						Dynamic Authorization succeeded
2015-11-25 18:49:00.720	✓			20:BB:C0:DE:06:.	20:BB:C0:DE:06:AE		Default >> MAB >> D...	Default >> Default	PermitAccess		Authentication succeeded

First, the device was authenticated using MAB (18:49:00). Ten seconds later (18:49:10) it was reprofiled as a Cisco-Device, and finally after 42 seconds since the first authentications (18:49:42), it received Cisco-IP-Phone-8941 profile. As a result, ISE returns Authorization Profile specific for IP Phones (Cisco_IP_Phones) and Downloadable ACL that permits all traffic (permit ip any). Note that in this scenario the unknown device has basic access to the network. It can be achieved by adding a Mac address to ISE internal endpoint database or allowing very basic network access for previously unknown devices.



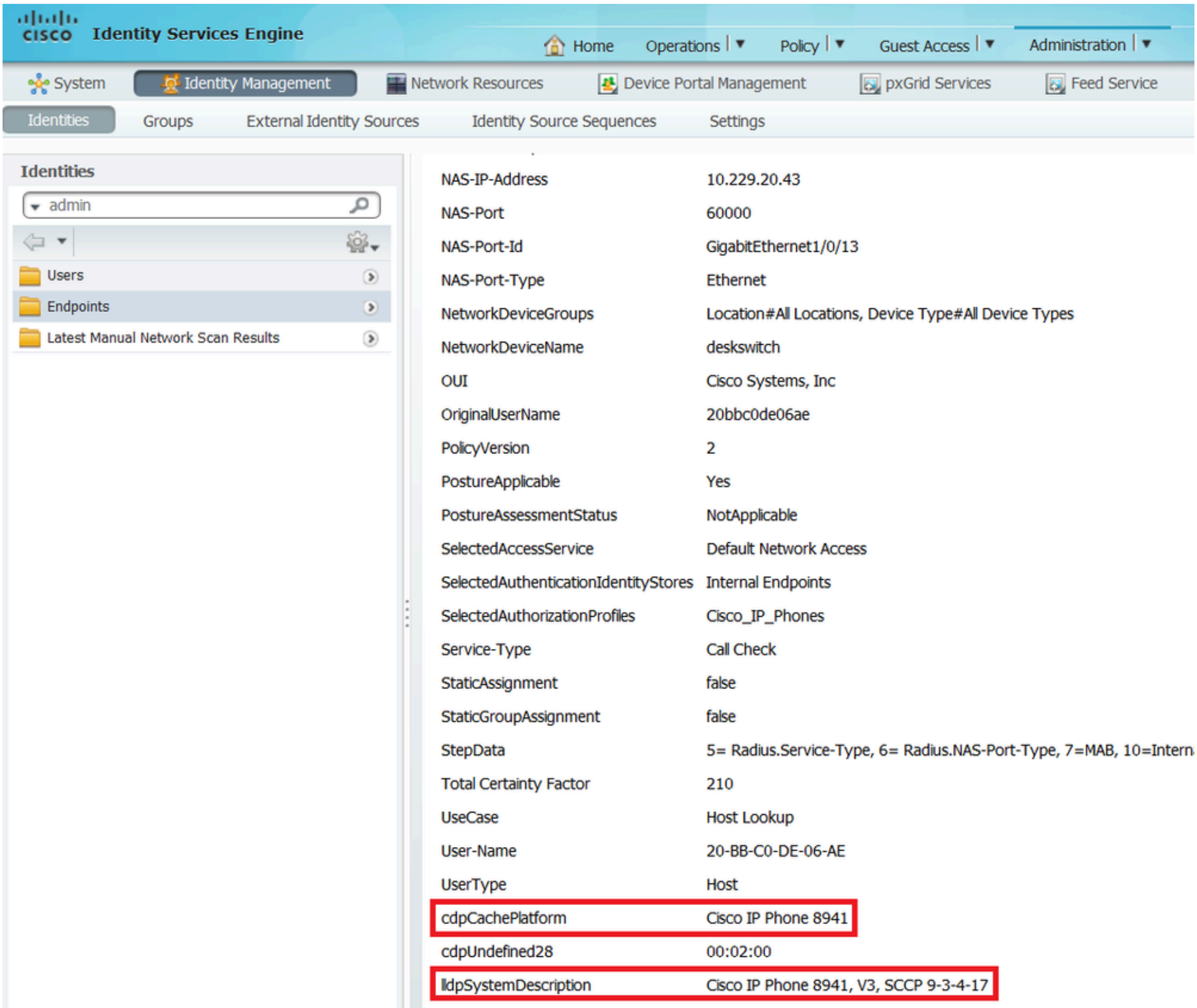
Note: Initial profiling took around 40 seconds in this example. On the next authentication, ISE already knows the profile, and correct attributes (permission to join voice domain and DACL) are applied instantly unless ISE receives new/updated attributes and it must reprofile the device again.



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Respo
0	0	0	0

Time	Status	Details	R...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Identity Group	Event
2015-11-25 18:55:39.772	●		0	20:BB:C0:DE:06:.	20:BB:C0:DE:06:AE	Cisco-IP-Phone-8941					Session State is Started
2015-11-25 18:55:38.721	✓			#ACSACL#-IP-PE							DACL Download Succeeded
2015-11-25 18:55:38.707	✓			20:BB:C0:DE:06:.	20:BB:C0:DE:06:AE	Cisco-IP-Phone-8941	Default >> MAB >> D...	Default >> Profiled Cis..	Cisco_IP_Phones	Cisco-IP-Phone	Authentication succeeded
2015-11-25 18:49:42.433	✓			#ACSACL#-IP-PE							DACL Download Succeeded
2015-11-25 18:49:42.417	✓			20:BB:C0:DE:06:.	20:BB:C0:DE:06:AE	Cisco-IP-Phone-8941	Default >> MAB >> D...	Default >> Profiled Cis..	Cisco_IP_Phones	Cisco-IP-Phone	Authentication succeeded

In Administration > Identity Management > Identities > Endpoints > tested endpoint you can see what kind of attributes were collected by the Radius probe and what their values are:



NAS-IP-Address	10.229.20.43
NAS-Port	60000
NAS-Port-Id	GigabitEthernet1/0/13
NAS-Port-Type	Ethernet
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	deskswitch
OUI	Cisco Systems, Inc
OriginalUserName	20bbc0de06ae
PolicyVersion	2
PostureApplicable	Yes
PostureAssessmentStatus	NotApplicable
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	Internal Endpoints
SelectedAuthorizationProfiles	Cisco_IP_Phones
Service-Type	Call Check
StaticAssignment	false
StaticGroupAssignment	false
StepData	5= Radius.Service-Type, 6= Radius.NAS-Port-Type, 7=MAB, 10=Intern
Total Certainty Factor	210
UseCase	Host Lookup
User-Name	20-BB-C0-DE-06-AE
UserType	Host
cdpCachePlatform	Cisco IP Phone 8941
cdpUndefined28	00:02:00
lldpSystemDescription	Cisco IP Phone 8941, V3, SCCP 9-3-4-17

As you can observe, the total Certainty Factor computed is 210 in this scenario. It comes from the fact that the endpoint also matched the Cisco-Device profile (with a total certainty factor of 30) and the Cisco-IP-Phone profile (with a total certainty factor of 40). Since the profiler matched both conditions in profile Cisco-IP-Phone-8941, the certainty factor for this profile is 140 (70 for each attribute according to profiling policy). To sum up: 30+40+70+70=210.

Troubleshoot

Step 1. Verify Information Collected by CDP/LLDP

```
switch#sh cdp neighbors g1/0/13 detail
-------------------------
Device ID: SEP20BBC0DE06AE
Entry address(es):
Platform: Cisco IP Phone 8941 ,  Capabilities: Host Phone Two-port Mac Relay
Interface: GigabitEthernet1/0/13,  Port ID (outgoing port): Port 1
Holdtime : 178 sec
Second Port Status: Down

Version :
```

```
SCCP 9-3-4-17

advertisement version: 2
Duplex: full
Power drawn: 3.840 Watts
Power request id: 57010, Power management id: 3
Power request levels are:3840 0 0 0 0


Total cdp entries displayed : 1

switch#
switch#sh lldp neighbors g1/0/13 detail
------------------------------------------------
Chassis id: 0.0.0.0
Port id: 20BBC0DE06AE:P1
Port Description: SW Port
System Name: SEP20BBC0DE06AE.

System Description:
Cisco IP Phone 8941, V3, SCCP 9-3-4-17

Time remaining: 164 seconds
System Capabilities: B,T
Enabled Capabilities: B,T
Management Addresses - not advertised
Auto Negotiation - supported, enabled
Physical media capabilities:
    1000baseT(FD)
    100base-TX(FD)
    100base-TX(HD)
    10base-T(FD)
    10base-T(HD)
Media Attachment Unit type: 16
Vlan ID: - not advertised

MED Information:

    MED Codes:
          (NP) Network Policy, (LI) Location Identification
          (PS) Power Source Entity, (PD) Power Device
          (IN) Inventory

    H/W revision: 3
    F/W revision: 0.0.1.0
    S/W revision: SCCP 9-3-4-17
    Serial number: PUC17140FB0
    Manufacturer: Cisco Systems , Inc.
    Model: CP-8941
    Capabilities: NP, PD, IN
    Device type: Endpoint Class III
    Network Policy(Voice): VLAN 101, tagged, Layer-2 priority: 0, DSCP: 0
    Network Policy(Voice Signal): VLAN 101, tagged, Layer-2 priority: 3, DSCP: 24
    PD device, Power source: Unknown, Power Priority: Unknown, Wattage: 3.8
    Location - not advertised


Total entries displayed: 1
```

If you cannot see any data collected, verify this:

- Check the state of the authentication session on the switch (it must be successful):

```
piborowi#show authentication sessions int g1/0/13 details
            Interface:  GigabitEthernet1/0/13
          MAC Address:  20bb.c0de.06ae
         IPv6 Address:  Unknown
         IPv4 Address:  Unknown
            User-Name:  20-BB-C0-DE-06-AE
               Status:  Authorized
               Domain:  VOICE
       Oper host mode:  multi-domain
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  0AE51820000002040099C216
      Acct Session ID:  0x00000016
               Handle:  0xAC0001F6
       Current Policy:  POLICY_Gi1/0/13

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:

Method status list:
       Method           State
       dot1x            Stopped

       mab              Authc Success
```

- Check if CDP and LLDP protocols are enabled. Check if there are any non-default commands regarding CDP/LLDP/ and how those can affect attribute retrieval from the endpoint

```
switch#sh running-config all | in cdp run
cdp run
switch#sh running-config all | in lldp run
lldp run
```

- Verify in the configuration guide for your endpoint if it supports CDP/LLDP/and so on.

Step 2. Check the Device Sensor Cache

```
switch#show device-sensor cache interface g1/0/13
Device: 20bb.c0de.06ae on port GigabitEthernet1/0/13
--------------------------------------------------
Proto Type:Name                          Len Value
LLDP     6:system-description             40 0C 26 43 69 73 63 6F 20 49 50 20 50 68 6F 6E 65
                                             20 38 39 34 31 2C 20 56 33 2C 20 53 43 43 50 20
                                             39 2D 33 2D 34 2D 31 37
CDP      6:platform-type                  24 00 06 00 18 43 69 73 63 6F 20 49 50 20 50 68 6F
                                             6E 65 20 38 39 34 31 20
```

```
CDP     28:secondport-status-type       7 00 1C 00 07 00 02 00
```

If you do not see any data in this field or information is not complete, verify **device-sensor** commands; in particular, filter-lists and filter-specs.

Step 3. Check if attributes are Present in Radius Accounting

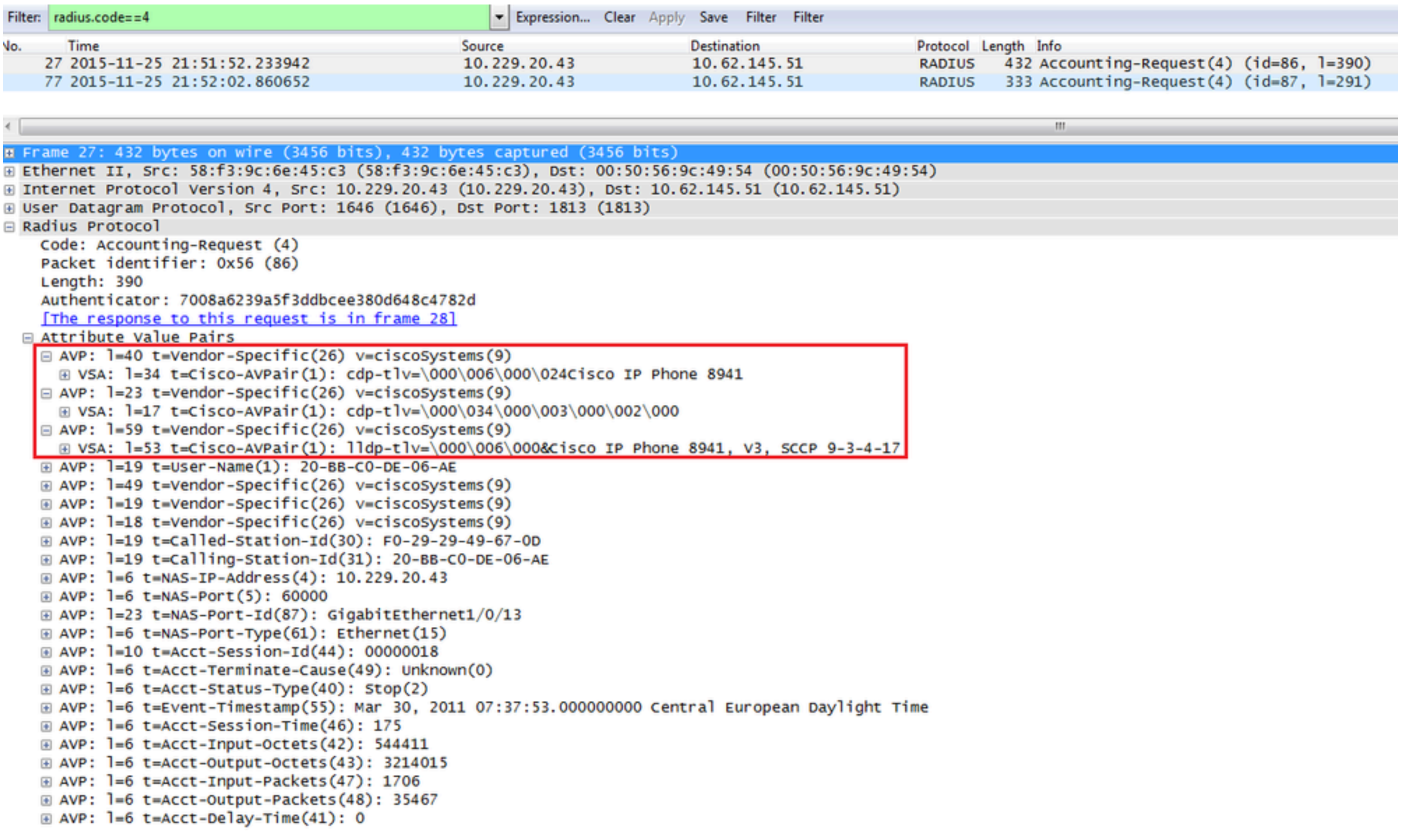
You can verify that using the `debug radius` command on the switch or performing packet capture between the switch and ISE.

Radius debug:

<#root>

```
Mar 30 05:34:58.716: RADIUS(00000000): Send Accounting-Request to 1.1.1.1:1813 id 1646/85, len 378
Mar 30 05:34:58.716: RADIUS:  authenticator 17 DA 12 8B 17 96 E2 0F - 5D 3D EC 79 3C ED 69 20
Mar 30 05:34:58.716: RADIUS:  Vendor, Cisco       [26]  40
Mar 30 05:34:58.716: RADIUS:   Cisco AVpair       [1]   34  "

cdp-tlv

=                        "
Mar 30 05:34:58.716: RADIUS:  Vendor, Cisco       [26]  23
Mar 30 05:34:58.716: RADIUS:   Cisco AVpair       [1]   17  "

cdp-tlv

=       "
Mar 30 05:34:58.721: RADIUS:  Vendor, Cisco       [26]  59
Mar 30 05:34:58.721: RADIUS:   Cisco AVpair       [1]   53  "

lldp-tlv

=                                         "
Mar 30 05:34:58.721: RADIUS:  User-Name           [1]   19  "20-BB-C0-DE-06-AE"
Mar 30 05:34:58.721: RADIUS:  Vendor, Cisco       [26]  49
Mar 30 05:34:58.721: RADIUS:   Cisco AVpair       [1]   43  "audit-session-id=0AE518200000022800E2481C"
Mar 30 05:34:58.721: RADIUS:  Vendor, Cisco       [26]  19
Mar 30 05:34:58.721: RADIUS:   Cisco AVpair       [1]   13  "vlan-id=101"
Mar 30 05:34:58.721: RADIUS:  Vendor, Cisco       [26]  18
Mar 30 05:34:58.721: RADIUS:   Cisco AVpair       [1]   12  "method=mab"
Mar 30 05:34:58.721: RADIUS:  Called-Station-Id   [30]  19  "F0-29-29-49-67-0D"
Mar 30 05:34:58.721: RADIUS:  Calling-Station-Id  [31]  19  "20-BB-C0-DE-06-AE"
Mar 30 05:34:58.721: RADIUS:  NAS-IP-Address      [4]   6   10.229.20.43
Mar 30 05:34:58.721: RADIUS:  NAS-Port            [5]   6   60000
Mar 30 05:34:58.721: RADIUS:  NAS-Port-Id         [87]  23  "GigabitEthernet1/0/13"
Mar 30 05:34:58.721: RADIUS:  NAS-Port-Type       [61]  6   Ethernet                  [15]
Mar 30 05:34:58.721: RADIUS:  Acct-Session-Id     [44]  10  "00000018"
Mar 30 05:34:58.721: RADIUS:  Acct-Status-Type    [40]  6   Watchdog                  [3]
Mar 30 05:34:58.721: RADIUS:  Event-Timestamp     [55]  6   1301463298
Mar 30 05:34:58.721: RADIUS:  Acct-Input-Octets   [42]  6   538044
Mar 30 05:34:58.721: RADIUS:  Acct-Output-Octets  [43]  6   3201914
Mar 30 05:34:58.721: RADIUS:  Acct-Input-Packets  [47]  6   1686
Mar 30 05:34:58.721: RADIUS:  Acct-Output-Packets [48]  6   35354
Mar 30 05:34:58.721: RADIUS:  Acct-Delay-Time     [41]  6   0
Mar 30 05:34:58.721: RADIUS(00000000): Sending a IPv4 Radius Packet
Mar 30 05:34:58.721: RADIUS(00000000): Started 5 sec timeout
Mar 30 05:34:58.737: RADIUS: Received from id 1646/85 10.62.145.51:1813, Accounting-response, len 20
```

Packet capture:



Filter: radius.code==4 Expression... Clear Apply Save Filter Filter

```
No.   Time                        Source         Destination    Protocol  Length  Info
   27 2015-11-25 21:51:52.233942  10.229.20.43   10.62.145.51   RADIUS       432  Accounting-Request(4) (id=86, l=390)
   77 2015-11-25 21:52:02.860652  10.229.20.43   10.62.145.51   RADIUS       333  Accounting-Request(4) (id=87, l=291)
```

```
⊞ Frame 27: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits)
⊞ Ethernet II, Src: 58:f3:9c:6e:45:c3 (58:f3:9c:6e:45:c3), Dst: 00:50:56:9c:49:54 (00:50:56:9c:49:54)
⊞ Internet Protocol Version 4, Src: 10.229.20.43 (10.229.20.43), Dst: 10.62.145.51 (10.62.145.51)
⊞ User Datagram Protocol, Src Port: 1646 (1646), Dst Port: 1813 (1813)
⊟ Radius Protocol
    Code: Accounting-Request (4)
    Packet identifier: 0x56 (86)
    Length: 390
    Authenticator: 7008a6239a5f3ddbcee380d648c4782d
    [The response to this request is in frame 28]
  ⊟ Attribute Value Pairs
    ⊟ AVP: l=40 t=Vendor-Specific(26) v=ciscoSystems(9)
      ⊞ VSA: l=34 t=Cisco-AVPair(1): cdp-tlv=\000\006\000\024Cisco IP Phone 8941
    ⊟ AVP: l=23 t=Vendor-Specific(26) v=ciscoSystems(9)
      ⊞ VSA: l=17 t=Cisco-AVPair(1): cdp-tlv=\000\034\000\003\000\002\000
    ⊟ AVP: l=59 t=Vendor-Specific(26) v=ciscoSystems(9)
      ⊞ VSA: l=53 t=Cisco-AVPair(1): lldp-tlv=\000\006\000&Cisco IP Phone 8941, V3, SCCP 9-3-4-17
    ⊞ AVP: l=19 t=User-Name(1): 20-BB-C0-DE-06-AE
    ⊞ AVP: l=49 t=Vendor-Specific(26) v=ciscoSystems(9)
    ⊞ AVP: l=19 t=Vendor-Specific(26) v=ciscoSystems(9)
    ⊞ AVP: l=18 t=Vendor-Specific(26) v=ciscoSystems(9)
    ⊞ AVP: l=19 t=Called-Station-Id(30): F0-29-29-49-67-0D
    ⊞ AVP: l=19 t=Calling-Station-Id(31): 20-BB-C0-DE-06-AE
    ⊞ AVP: l=6 t=NAS-IP-Address(4): 10.229.20.43
    ⊞ AVP: l=6 t=NAS-Port(5): 60000
    ⊞ AVP: l=23 t=NAS-Port-Id(87): GigabitEthernet1/0/13
    ⊞ AVP: l=6 t=NAS-Port-Type(61): Ethernet(15)
    ⊞ AVP: l=10 t=Acct-Session-Id(44): 00000018
    ⊞ AVP: l=6 t=Acct-Terminate-Cause(49): Unknown(0)
    ⊞ AVP: l=6 t=Acct-Status-Type(40): Stop(2)
    ⊞ AVP: l=6 t=Event-Timestamp(55): Mar 30, 2011 07:37:53.000000000 Central European Daylight Time
    ⊞ AVP: l=6 t=Acct-Session-Time(46): 175
    ⊞ AVP: l=6 t=Acct-Input-Octets(42): 544411
    ⊞ AVP: l=6 t=Acct-Output-Octets(43): 3214015
    ⊞ AVP: l=6 t=Acct-Input-Packets(47): 1706
    ⊞ AVP: l=6 t=Acct-Output-Packets(48): 35467
    ⊞ AVP: l=6 t=Acct-Delay-Time(41): 0
```

Step 4. Verify Profiler Debugs on ISE

If the attributes were sent from the switch, it is possible to check if they were received on ISE. In order to check this, enable profiler debugs for the correct PSN node (Administration > System > Logging > Debug Log Configuration > PSN > profiler > debug) and perform authentication of the endpoint one more time.

Look for this information:

- Debug indicating that radius probe received attributes:

<#root>

```
2015-11-25 19:29:53,641 DEBUG  [RADIUSParser-1-thread-1][]
cisco.profiler.probes.radius.RadiusParser -:::-
MSG_CODE=[3002], VALID=[true], PRRT_TIMESTAMP=[2015-11-25 19:29:53.637 +00:00],
ATTRS=[Device IP Address=10.229.20.43, RequestLatency=7,
NetworkDeviceName=deskswitch, User-Name=20-BB-C0-DE-06-AE,
NAS-IP-Address=10.229.20.43, NAS-Port=60000, Called-Station-ID=F0-29-29-49-67-0D,
Calling-Station-ID=20-BB-C0-DE-06-AE, Acct-Status-Type=Interim-Update,
Acct-Delay-Time=0, Acct-Input-Octets=362529, Acct-Output-Octets=2871426,
Acct-Session-Id=00000016, Acct-Input-Packets=1138, Acct-Output-Packets=32272,
Event-Timestamp=1301458555, NAS-Port-Type=Ethernet, NAS-Port-Id=GigabitEthernet1/0/13,
```

```
cisco-av-pair=cdp-tlv=cdpCachePlatform=Cisco IP Phone 8941
```

 ,

```
cisco-av-pair=cdp-tlv=cdpUndefined28=00:02:00,
```

```
cisco-av-pair=lldp-tlv=lldpSystemDescription=Cisco IP Phone 8941\, V3\, SCCP 9-3-4-17,
cisco-av-pair=audit-session-id=0AE51820000002040099C216, cisco-av-pair=vlan-id=101,
cisco-av-pair=method=mab, AcsSessionID=ise13/235487054/2511, SelectedAccessService=Default Network Acce
Step=11004, Step=11017, Step=15049, Step=15008, Step=15004, Step=11005, NetworkDeviceGroups=Location#Al
NetworkDeviceGroups=Device Type#All Device Types, Service-Type=Call Check, CPMSessionID=0AE5182000000020
AllowedProtocolMatchedRule=MAB, Location=Location#All Locations, Device Type=Device Type#All Device Typ
```

- Debug indicating that attributes were successfully parsed:

```
2015-11-25 19:29:53,642 DEBUG  [RADIUSParser-1-thread-1][] cisco.profiler.probes.radius.RadiusParser -:
2015-11-25 19:29:53,642 DEBUG  [RADIUSParser-1-thread-1][] cisco.profiler.probes.radius.RadiusParser -:
2015-11-25 19:29:53,642 DEBUG  [RADIUSParser-1-thread-1][] cisco.profiler.probes.radius.RadiusParser -:
```

- Debug indicating that attributes are processed by the forwarder:

<#root>

```
2015-11-25 19:29:53,643 DEBUG  [forwarder-6][] cisco.profiler.infrastructure.probemgr.Forwarder -:20:BB
ID:null
Name:null
MAC: 20:BB:C0:DE:06:AE
        Attribute:AAA-Server     value:ise13
        (... more attributes ...)
        Attribute:User-Name      value:20-BB-C0-DE-06-AE


Attribute:cdpCachePlatform       value:Cisco IP Phone 8941
        Attribute:cdpUndefined28         value:00:02:00
        Attribute:lldpSystemDescription  value:Cisco IP Phone 8941, V3, SCCP 9-3-4-17

        Attribute:SkipProfiling  value:false
```

Note: A forwarder stores endpoints in the Cisco ISE database along with their attributes data, and then notifies the analyzer of new endpoints detected on your network. The analyzer classifies endpoints to the endpoint identity groups and stores endpoints with the matched profiles in the database.

Step 5. Profiling New Attributes and Device Assignment

Typically after new attributes are added to the existing collection for a specific device, this device/endpoint is added to the profiling queue in order to check if it has to be assigned a different profile based on new attributes:

```
<#root>

2015-11-25 19:29:53,646 DEBUG  [EndpointHandlerWorker-6-31-thread-1][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:20:BB:C0:DE:06:AE:Profiling:-

Classify hierarchy 20:BB:C0:DE:06:AE


2015-11-25 19:29:53,656 DEBUG  [EndpointHandlerWorker-6-31-thread-1][]
```

```
cisco.profiler.infrastructure.profiling.ProfilerManager -:20:BB:C0:DE:06:AE:Profiling:-

Policy Cisco-Device matched 20:BB:C0:DE:06:AE (certainty 30)


2015-11-25 19:29:53,659 DEBUG  [EndpointHandlerWorker-6-31-thread-1][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:20:BB:C0:DE:06:AE:Profiling:-

Policy Cisco-IP-Phone matched 20:BB:C0:DE:06:AE (certainty 40)


2015-11-25 19:29:53,663 DEBUG  [EndpointHandlerWorker-6-31-thread-1][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:20:BB:C0:DE:06:AE:Profiling:-

Policy Cisco-IP-Phone-8941 matched 20:BB:C0:DE:06:AE (certainty 140)


2015-11-25 19:29:53,663 DEBUG  [EndpointHandlerWorker-6-31-thread-1][]
cisco.profiler.infrastructure.profiling.ProfilerManager -:20:BB:C0:DE:06:AE:Profiling:-

After analyzing policy hierarchy: Endpoint: 20:BB:C0:DE:06:AE EndpointPolicy:Cisco-IP-Phone-8941 for:210
```

Related Information

- https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html
- https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html
- Cisco Technical Support & Downloads