Configure Device Sensor for ISE Profiling

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

- Step 1. Standard AAA Configuration
- Step 2. Configure Device Sensor

Verify

Troubleshoot

- Step 1. Verify Information Collected by CDP/LLDP
- Step 2. Check the Device Sensor Cache
- Step 3. Check if attributes are Present in Radius Accounting
  - Radius Debug
  - Packet Capture
- Step 4. Verify Profiler Debugs on ISE
- Step 5.Profile Reclassification After New Attributes Are Received

Related Information

Introduction

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

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Radius Protocol
- Cisco Catalyst Switch 9300
- Cisco Identity Service Engine (ISE)
- Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP)

Components Used

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

- Cisco ISE Version 3.4 Patch 3
- Cisco IP Phone 8811 Version 12.8.1
- Cisco Catalyst Switch 9300-48P Version 17.12.4

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

Device Sensor is a feature supported on wired network access devices, such as Cisco Catalyst switches. It can collect endpoint information using protocols such as CDP, LLDP, and DHCP, and sends the collected attributes to ISE in RADIUS accounting packets. In wireless-only deployments, ISE profiling generally relies on attributes received from the wireless controller and DHCP probe data rather than switch Device Sensor data. Profiler feeds provide the profiling policies that ISE uses to classify endpoints.



Note: Device Sensor collects information only from endpoints directly connected to the network access device (one hop away.) ISE uses the collected attributes for endpoint profiling.

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

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

1. Enable AAA running the **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 group server radius ISE-GROUP
 server name ise
!
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 <ISE_PSN_IP> server-key Krakow123
!
dot1x system-auth-control
!
lldp run
cdp run
!
interface GigabitEthernet1/0/1
 description IP_Phone
 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
!
radius server ise
 address ipv4 <ISE_PSN_IP> auth-port 1812 acct-port 1813
 key <shared_key>
!
```



Note: You must configure the switch to send Cisco vendor-specific attributes (VSAs) to ISE.

These attributes can be sent inside the accounting packets by configuring this command:

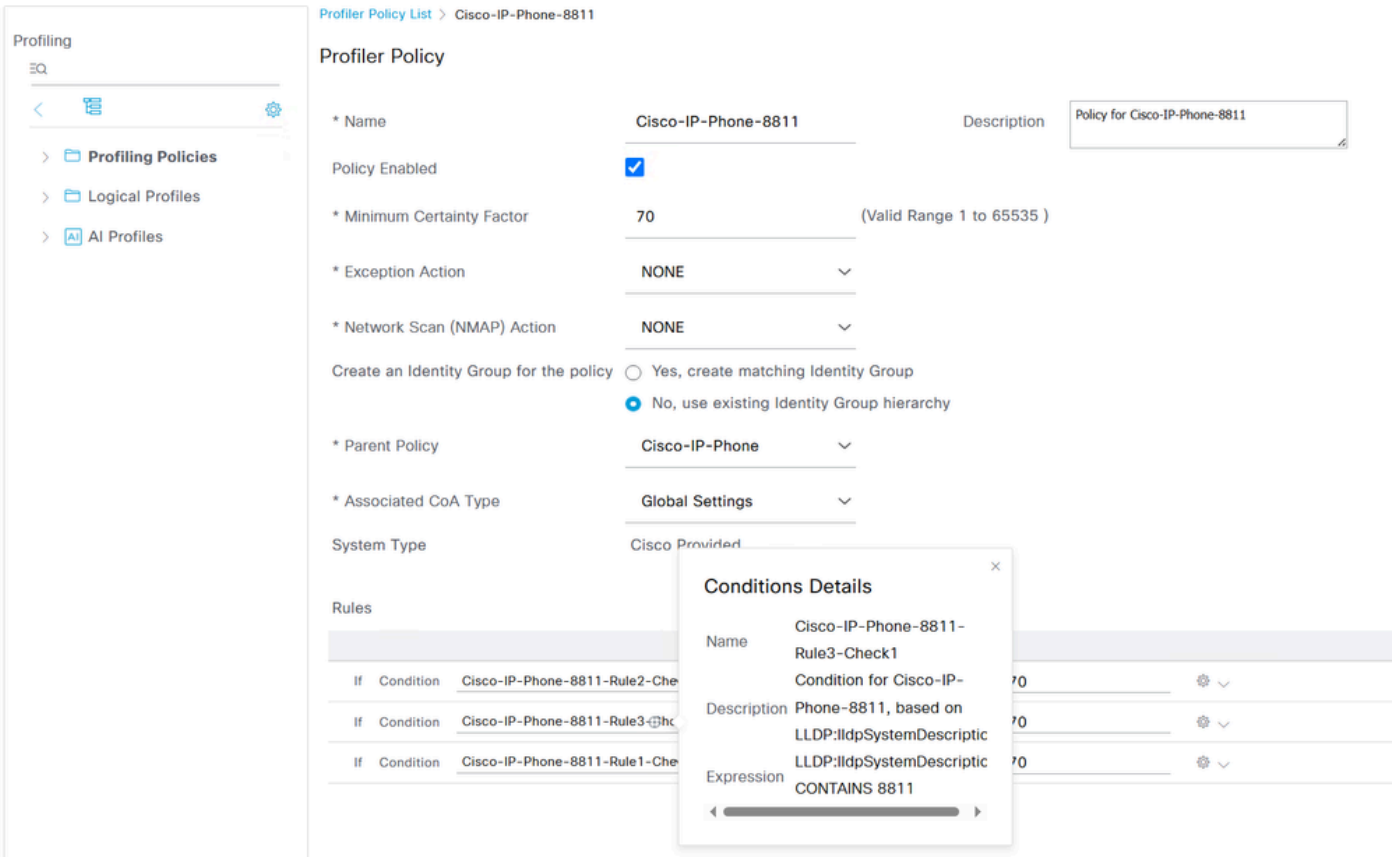
```
radius-server vsa send accounting
```

Step 2. Configure Device Sensor

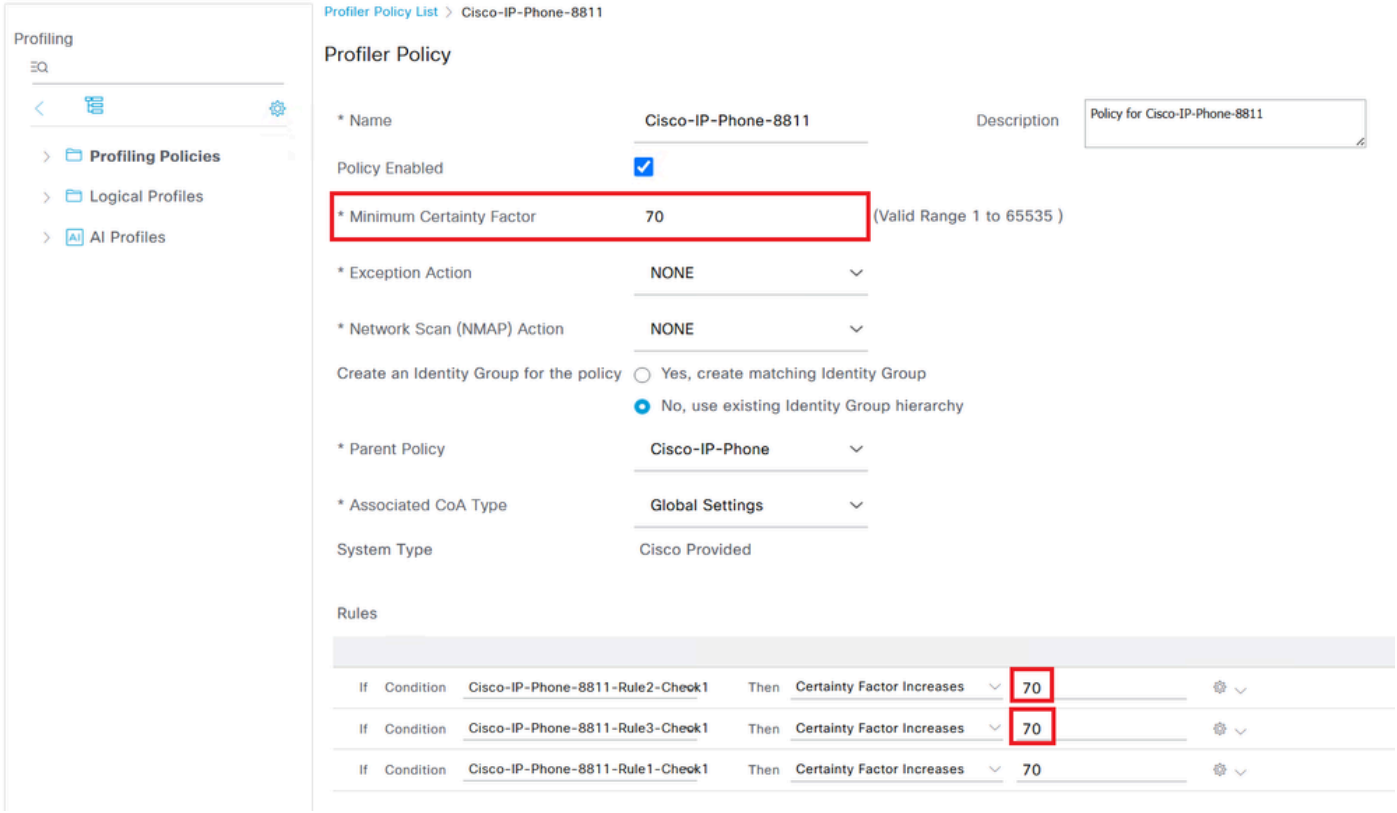
1. Determine which attributes from CDP/LLDP are needed in order to profile the device. In the case of Cisco IP Phone 8811 you can use these:

- LLDP SystemDescription attribute
- CDP CachePlatform attribute

You can validate which attributes are used to profile the device by checking the Profiler Policies. To do this, navigate to **Work Centers > Profiler > Profiling Policies** and select the profiling policy you want to match.



In the next screenshot, the Minimum Certainty Factor required for the endpoint to be profiled as Cisco-IP-Phone-8811 is 70. In this example, either attribute contributes a certainty factor of 70. However, the endpoint must also meet the required conditions for the applicable parent profiles before ISE assigns the final endpoint profile.



Note: To be profiled as a specific Cisco IP Phone, you must satisfy minimum conditions for all parent profiles. The profiler must match the Cisco-Device (minimum Certainty Factor 10) and the Cisco-IP-Phone (minimum Certainty Factor 20.) Even though the profiler matches the 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 with the highest Certainty Factor.

---

2. Configure two **filter lists**, one for CDP and another for LLDP. Those indicate which attributes must be included in the 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 this example, these attributes are included:

- **device-name** and **platform-type** 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** to trigger updates when TLVs are added, modified, or removed for the current session.

5. To send the information collected by the Device Sensor, configure the command **device-sensor accounting**.

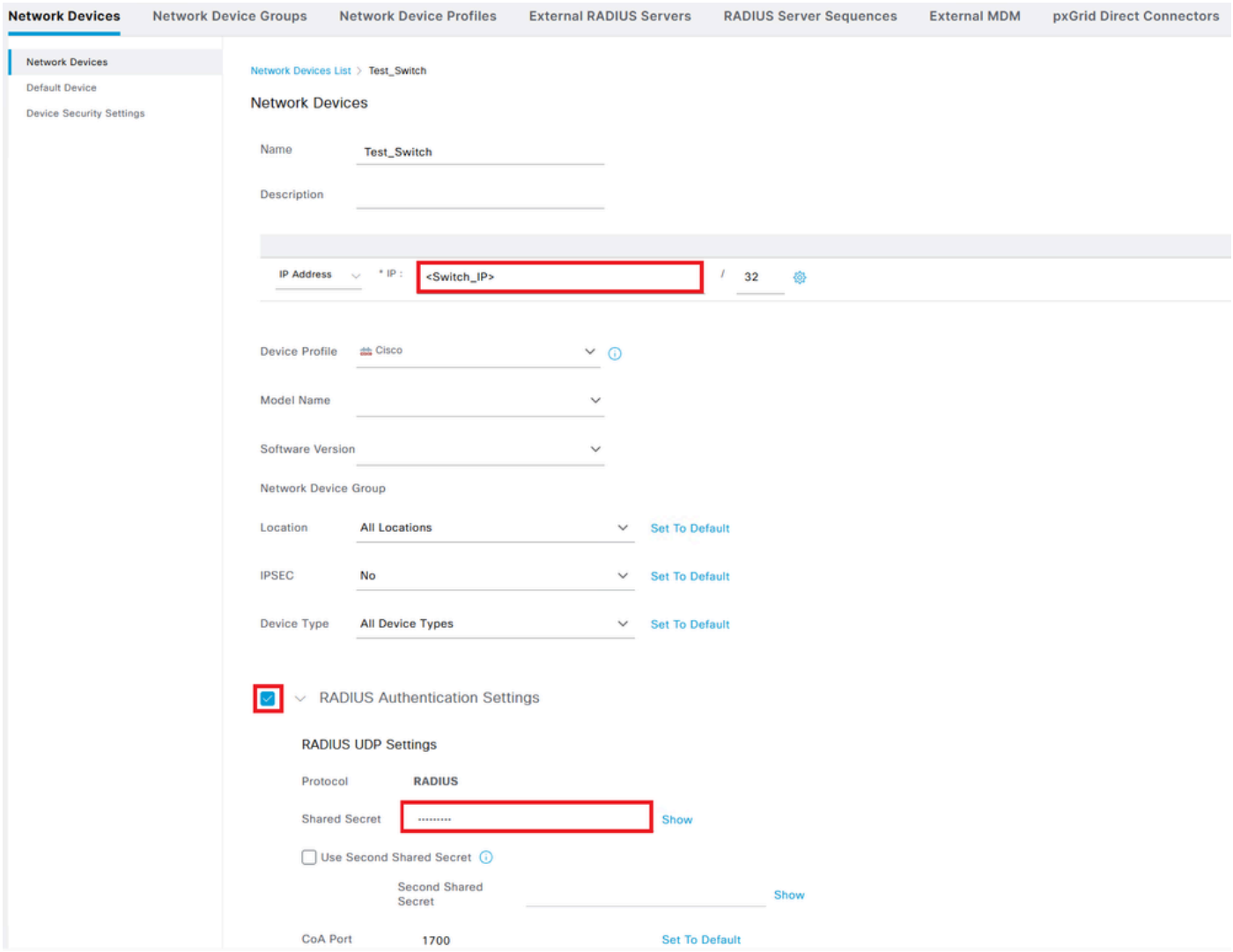
```
!
device-sensor filter-list cdp list cdp-list
 tlv name device-name
 tlv name platform-type
!
device-sensor filter-list lldp list lldp-list
 tlv name system-description
!
device-sensor filter-spec lldp include list lldp-list
device-sensor filter-spec cdp include list cdp-list
!
device-sensor accounting
device-sensor notify all-changes
!
```



Note: Device Sensor commands and supported TLVs can vary by Catalyst platform and IOS XE releases. Confirm command support and available TLVs in the configuration guide for the switch platform in use; Step 3. Configure Profiling on ISE.

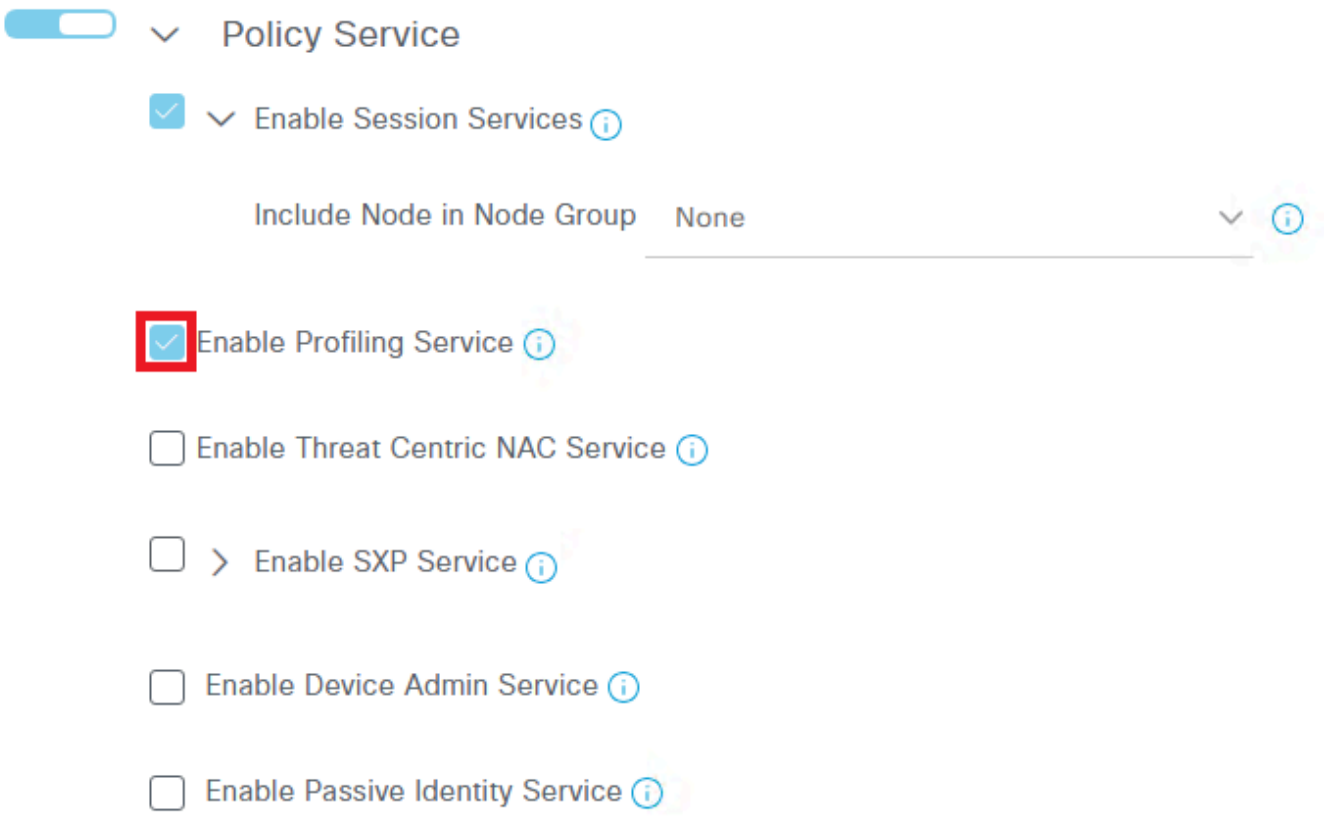
---

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 the Authentication Settings:



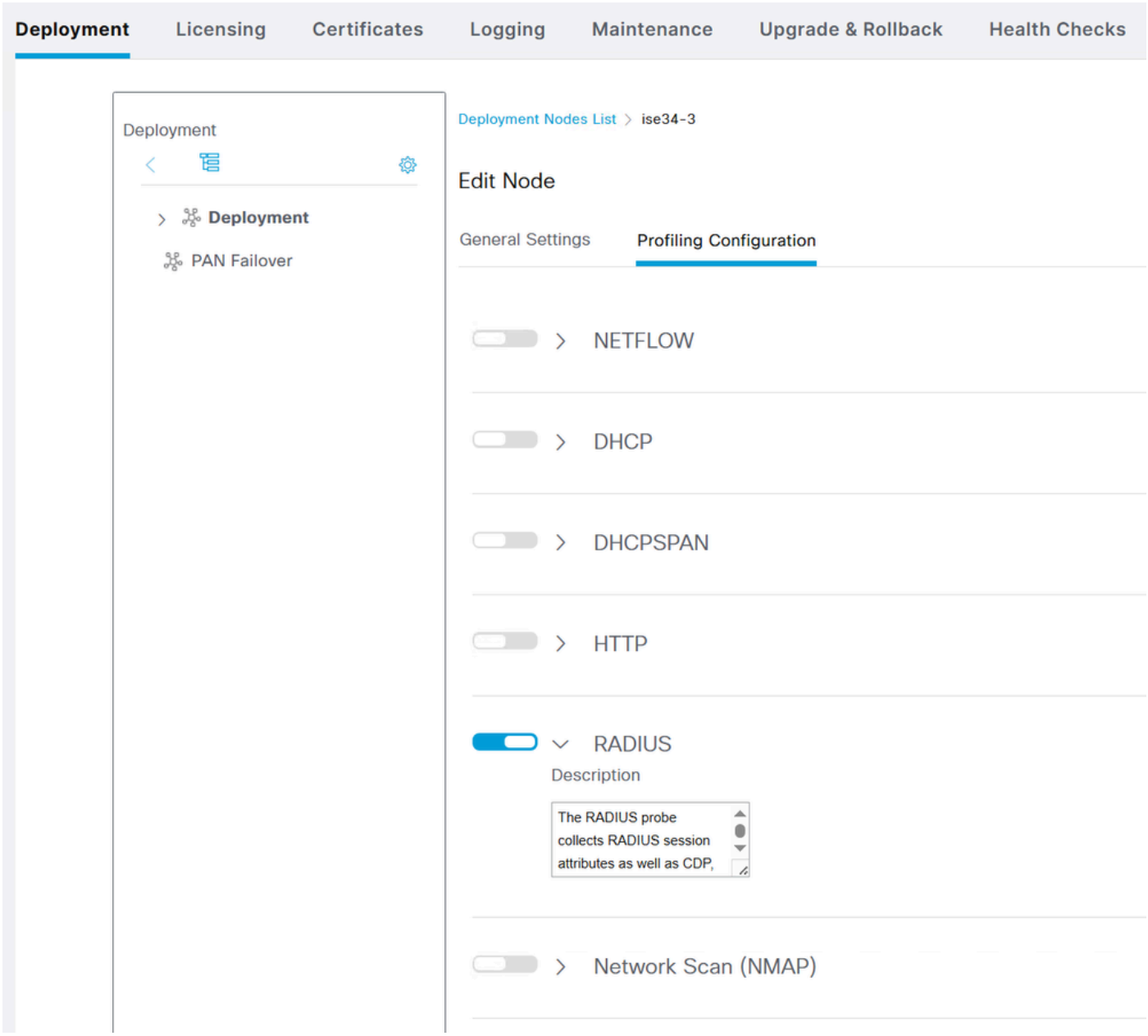
---

2. Enable the Profiling Service on the ISE node. Navigate to **Administration > System > Deployment**, choose the ISE node and on the Policy Service tab, enable the **Profiling Service** option. Enable the Profiling service on the PSN nodes that are intended to process profiling data. Enable only the probes required for the deployment, as additional probes and profiling-enabled PSNs can increase system resource utilization.



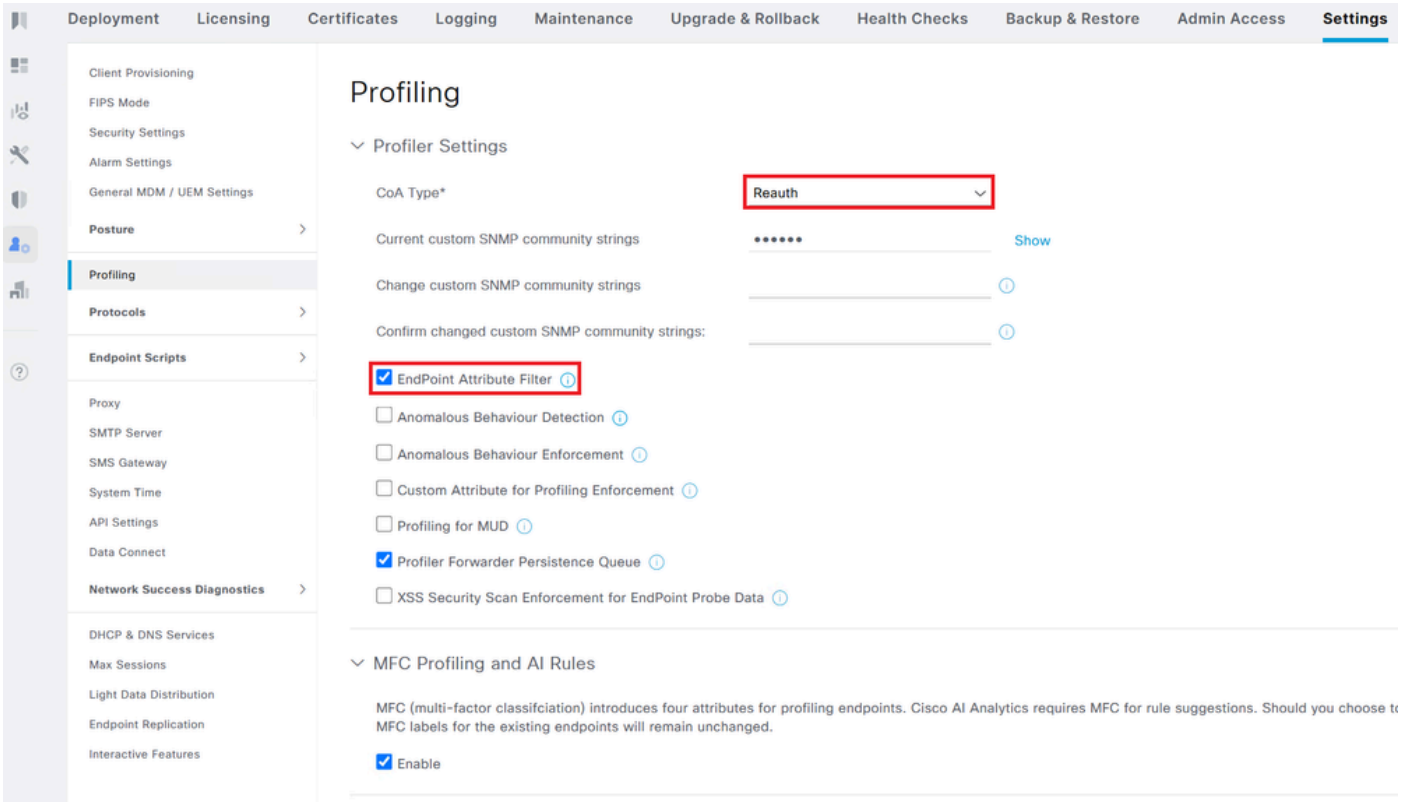
---

3. Enable the Radius probe on the profiling node. Navigate to **Administration > System > Deployment**, choose the ISE node, and click the **Profiling Configuration** tab.



---

4. Set the CoA (Change of Authorization) type to **Reauth** to enforce reauthentication of the endpoint once profiled. In addition, ensure the **Endpoint Attribute Filter** is checked. Navigate to **Administration > System > Settings > Profiling**.

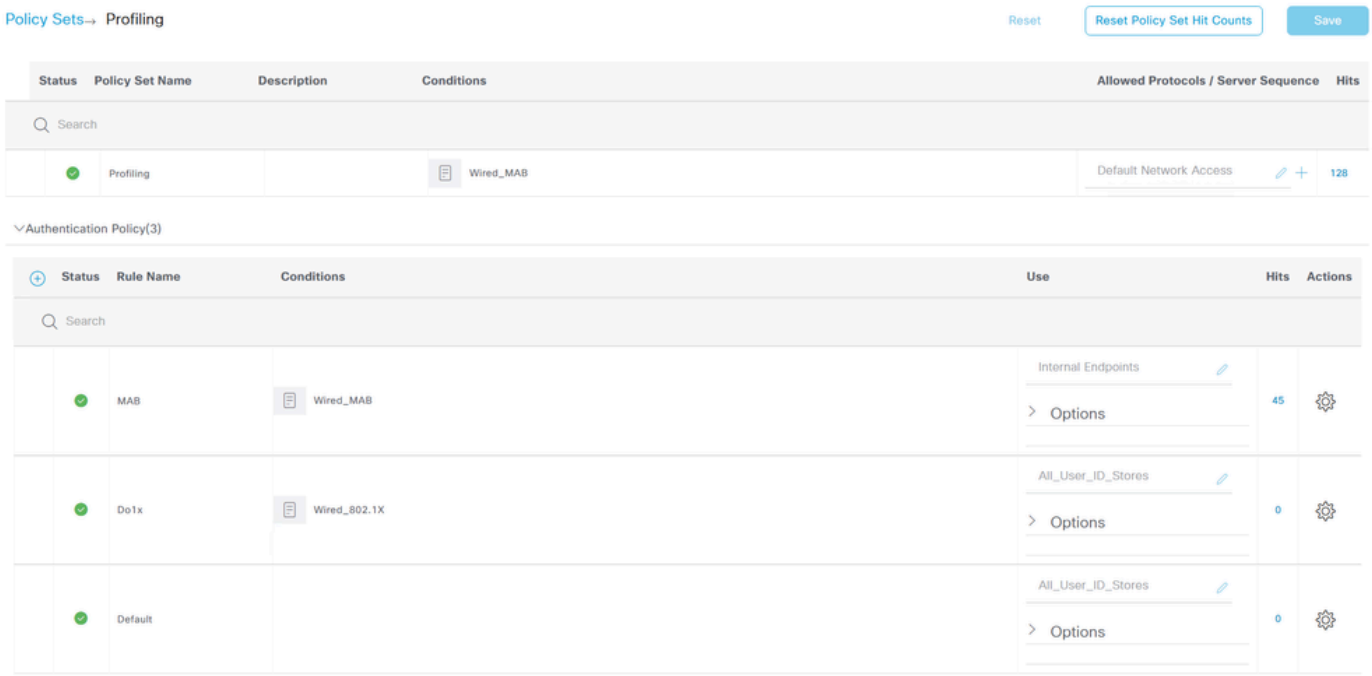


Note: It is a best practice to enable the Endpoint Attribute Filter in production deployments to avoid performance issues when too much unnecessary profiler data is gathered.

To add an attribute to the allow list that is currently not present, you can create a new Profiler Condition and Policy that uses the attribute. The attribute can automatically be added to the allow list of stored and replicated attributes. If an endpoint remains classified as Unknown, review its collected attributes in the Context Visibility or Endpoint Classification and compare them with the conditions and certainty factors configured in the intended profiling policy. An OUI match alone is not always sufficient enough to meet a specific profiles minimum certainty factor.

---

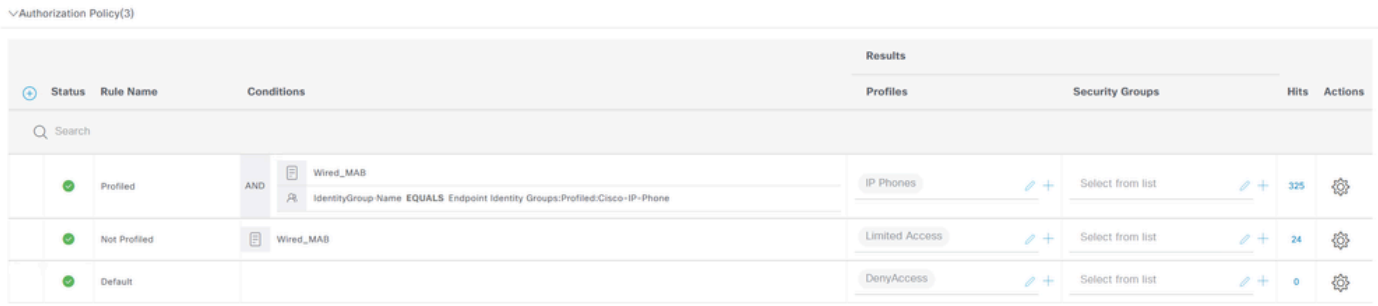
5. Configure ISE Authentication Rules:



---

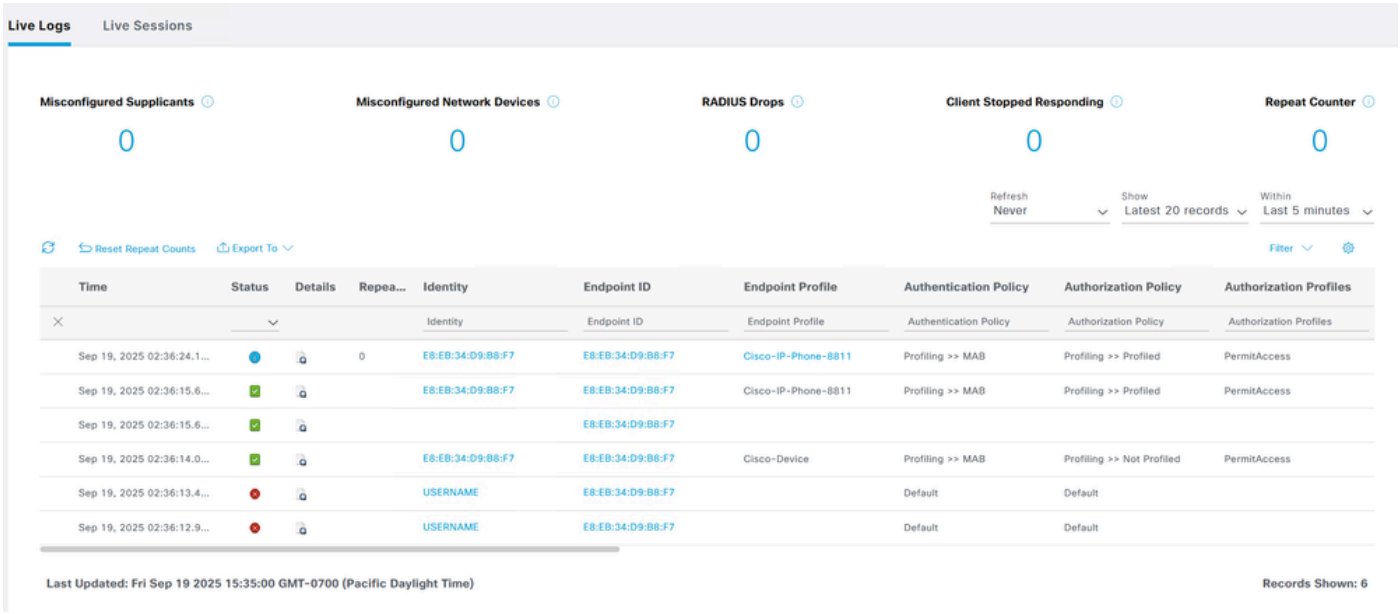
6. Configure ISE Authorization Rules. The Profiled Cisco IP Phone rule is used, which is preconfigured on ISE:

You can configure an Authorization Policy that can act as a catch policy, which allows the endpoints to be authorized into the network (with limited access) to ensure the attributes are sent in the accounting packets. In addition, create another policy that can be matched once the devices are profiled, ensuring they can access the necessary resources in the network.



Verify

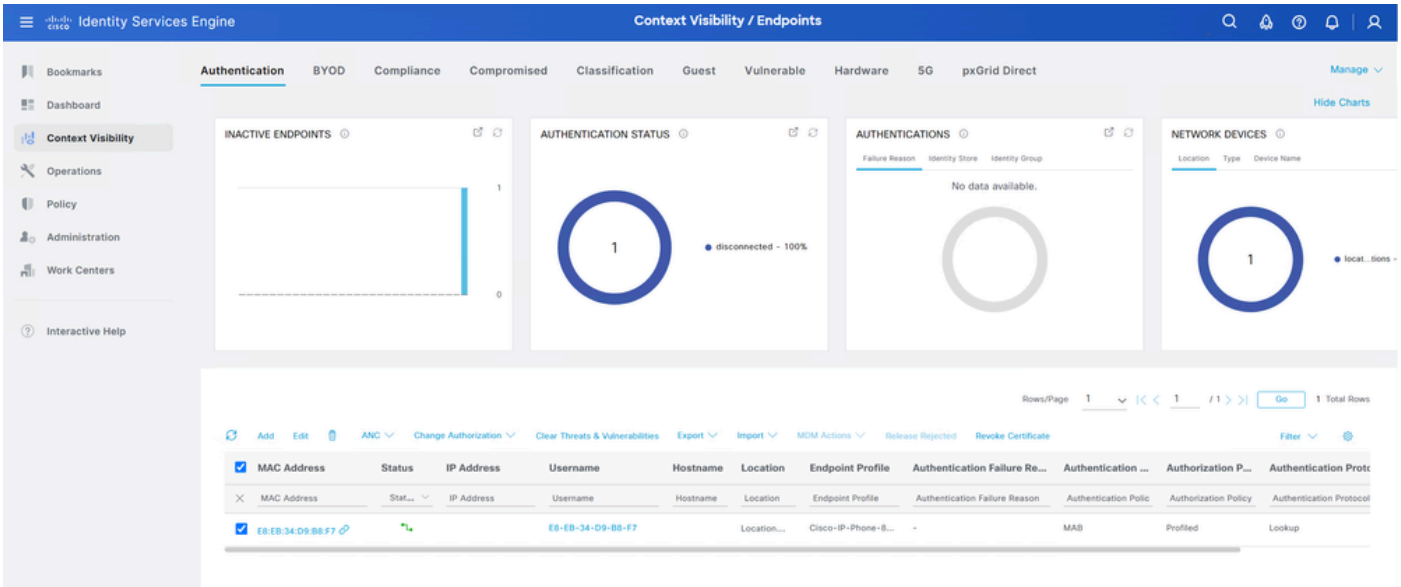
To verify if profiling is working properly, refer to **Operations > Radius > Live Logs** on ISE:

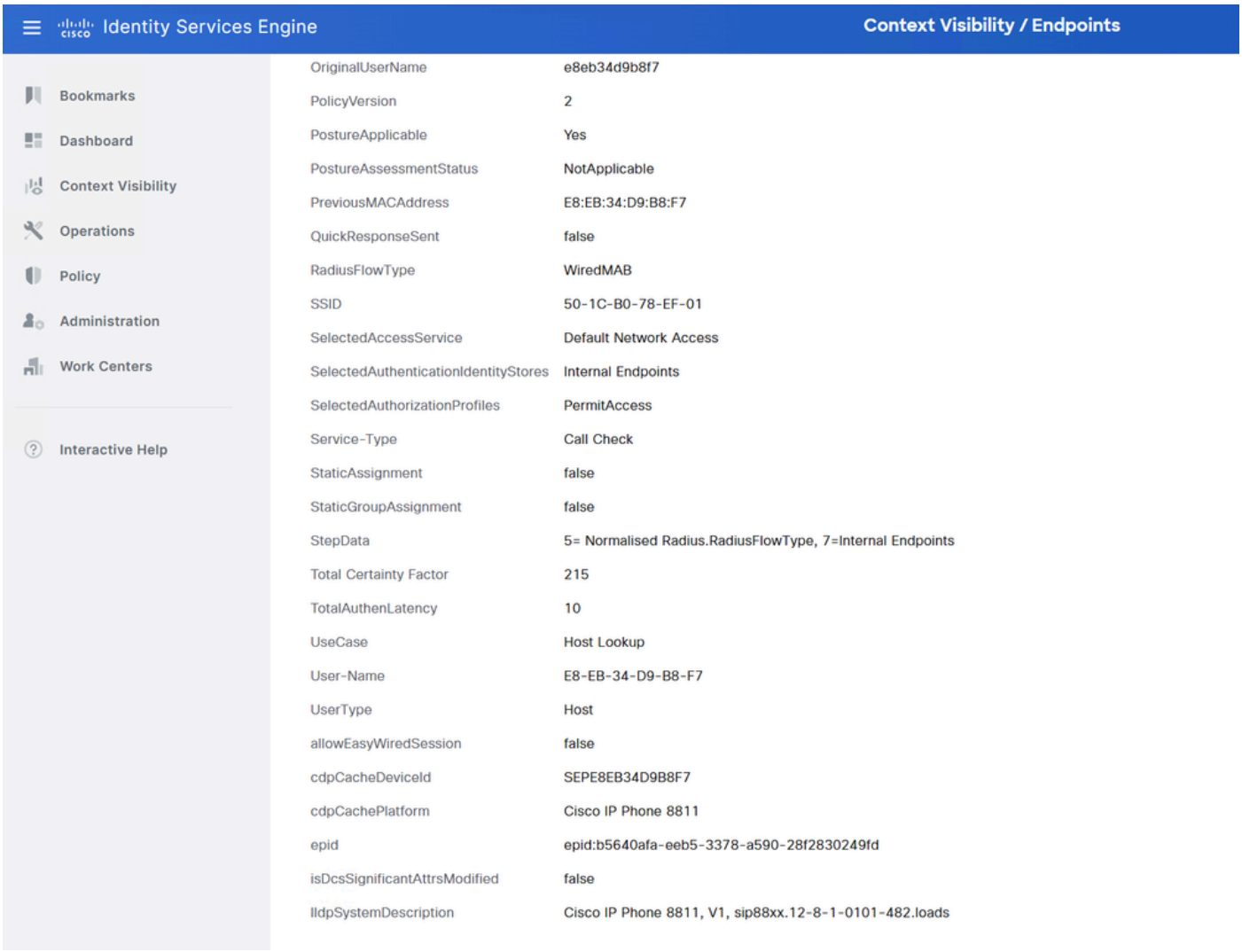


In this IP phone example, 802.1X does not authenticate, so the switch falls back to MAB based on the configured method order. This behavior is expected for endpoints that do not use 802.1X.

MAB authentication is successful at 02:36:14 PM. In the live log, the device is initially profiled as a Cisco device as the MAC address OUI is associated with Cisco, matching the predefined Cisco-Device profiling policy. Once the device receives network access, the switch sends the CDP and LLDP attributes in Radius Accounting packets. At 02:36:15 PM, ISE profiles the endpoint and sends a CoA to force reauthentication. After the CoA succeeds, the endpoint reauthenticates and matches the authorization policy for Cisco IP Phones.

In **Administration > Identity Management > Identities > Endpoints**, you can filter by the tested endpoint MAC address and see the types of attributes collected by the Radius probe and their values:





As you can observe, the total Certainty Factor computed is 215 in this scenario. It comes from the fact the endpoint also matches the Cisco-Device profile (with a total certainty factor of 30) and the Cisco-IP-Phone profile (with a total certainty factor of 45.) Moreover, the profiler also matches both conditions in the profile for the Cisco-IP-Phone-8811, the certainty factor for this profile is 140 (70 for each attribute according to profiling policy.) To sum up: 30 + 45 + 70 + 70 = 215.

Troubleshoot

Step 1. Verify Information Collected by CDP/LLDP

```
Switch#show cdp neighbors GigabitEthernet1/0/1 details
-------------------------
Device ID: SEPE8EB34D9B8F7
Entry address(es):
Platform: Cisco IP Phone 8811,  Capabilities: Host Phone Two-port Mac Relay
Interface: GigabitEthernet1/0/1,  Port ID (outgoing port): Port 1
Holdtime : 151 sec
Second Port Status: Down
```

```
Version :
sip88xx.12-8-1-0101-482.loads

advertisement version: 2
Peer Source MAC: e8eb.34d9.b8f7
Duplex: full
Power drawn: 6.086 Watts
Power request id: 63418, Power management id: 4
Power request levels are:6086 0 0 0 0


Switch#show lldp neighbors GigabitEthernet1/0/1 details
------------------------------------------------
Local Intf: Gi1/0/1
Local Intf service instance: -
Chassis id: 0.0.0.0
Port id: E8EB34D9B8F7:P1
Port Description: SW PORT
System Name: SEPE8EB34D9B8F7

System Description:
Cisco IP Phone 8811, V1, sip88xx.12-8-1-0101-482.loads

Time remaining: 175 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: 30
Vlan ID: - not advertised
Peer Source MAC: e8eb.34d9.b8f7

MED Information:

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

    H/W revision: 1
    F/W revision: sb2388xx.BE-01-027.sbn size=-1

    S/W revision: sip88xx.12-8-1-0101-482.loads
    Serial number: FCH25023CZN
    Manufacturer: Cisco Systems, Inc.
    Model: CP-8811
    Capabilities: NP, PD, IN
    Device type: Endpoint Class III
    Network Policy(Voice): VLAN 101, tagged, Layer-2 priority: 5, DSCP: 46
    Network Policy(Voice Signal): VLAN 101, tagged, Layer-2 priority: 4, DSCP: 32
    PD device, Power source: PSE, Power Priority: Unknown, Wattage: 5.9
    Location - not advertised


Total entries displayed: 1
```

If you cannot see any data collected, verify and check the state of the authentication session on the switch (it must be successful):

```
OCEAN#sh access-session int gig1/0/1 det
            Interface:  GigabitEthernet1/0/1
               IIF-ID:  0x172041DB
          MAC Address:  e8eb.34d9.b8f7
         IPv6 Address:  Unknown
         IPv4 Address:  Unknown
            User-Name:  E8-EB-34-D9-B8-F7
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-domain
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  F24D300A0000001B9A787BED
      Acct Session ID:  0x0000012b
               Handle:  0x79000011
       Current Policy:  POLICY_Gi1/0/1


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

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#show running-config all | include cdp run
cdp run
Switch#show running-config all | include lldp run
lldp run
```

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

Step 2. Check the Device Sensor Cache

```
Switch#show device-sensor cache interface GigabitEthernet1/0/1
Device: e8eb.34d9.b8f7 on port GigabitEthernet1/0/1
-------------------------------------------------------------------------------
Proto Type:Name                       Len Value                       Text
LLDP     6:system-description          56 0C 36 43 69 73 63 6F 20 49  .6Cisco I
                                          50 20 50 68 6F 6E 65 20 38  P Phone 8
                                          38 31 31 2C 20 56 31 2C 20  811, V1,
                                          73 69 70 38 38 78 78 2E 31  sip88xx.1
                                          32 2D 38 2D 31 2D 30 31 30  2-8-1-010
                                          31 2D 34 38 32 2E 6C 6F 61  1-482.loa
                                          64 73                       ds
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 38 38 31 31               8811
CDP      1:device-name                 19 00 01 00 13 53 45 50 45 38  ....SEPE8
                                          45 42 33 34 44 39 42 38 46  EB34D9B8F
                                          37                          7
```

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

Step 3. Check if attributes are Present in Radius Accounting

You can verify running the **debug radius** command on the switch or performing packet capture between the switch and ISE.

Radius Debug

```
Switch#debug radius
Switch#set platform software trace smd switch active R0 dot1x-all verbose
Switch#show platform software trace level smd switch active R0 | inc dot1x
dot1x Notice
dot1x-all Verbose
dot1x-redun Notice
```

To disable debugs, you can run this command:

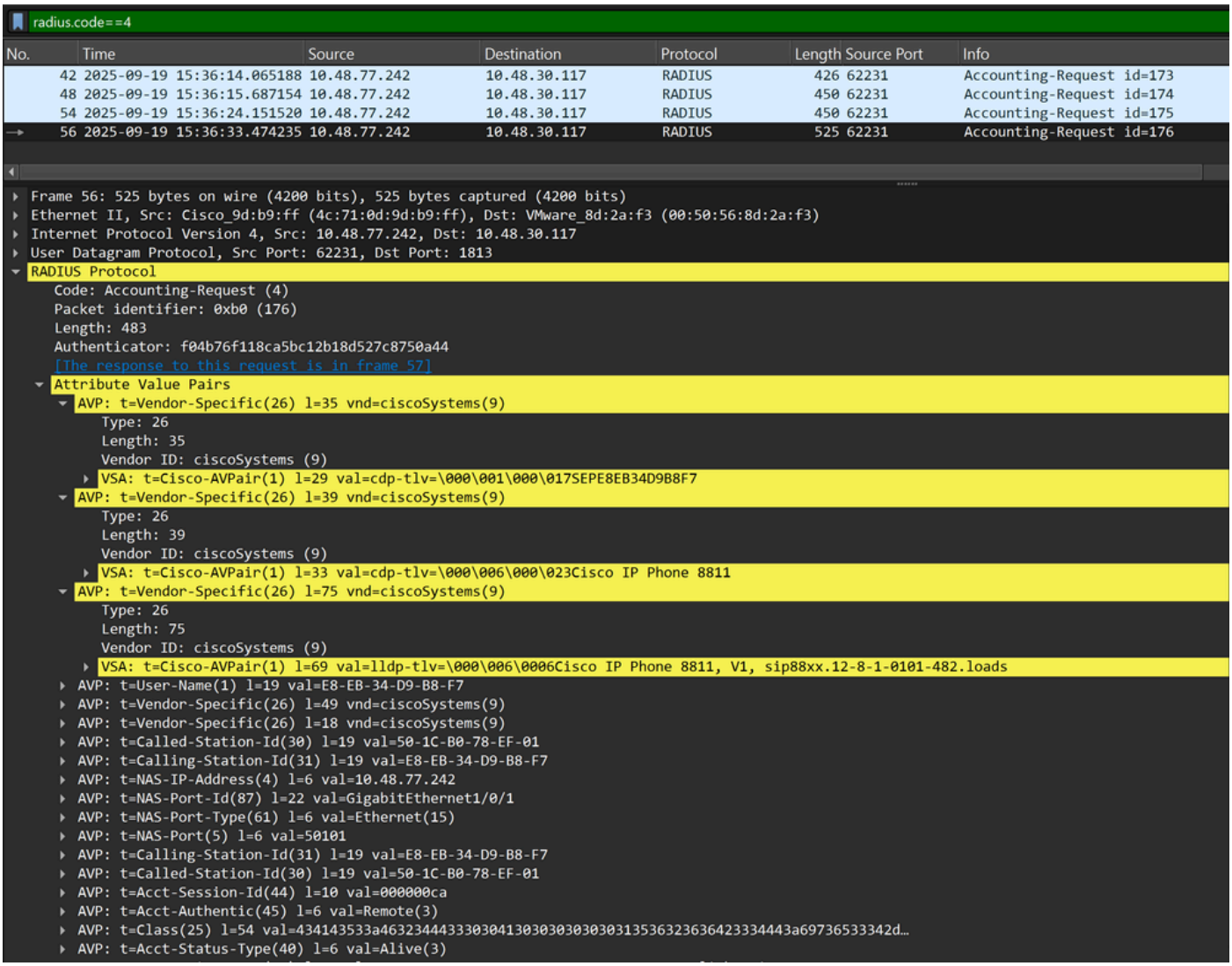
```
Switch#set platform software trace all notice
```

To show the logs:

```
Switch#show logging process smd | include RADIUS

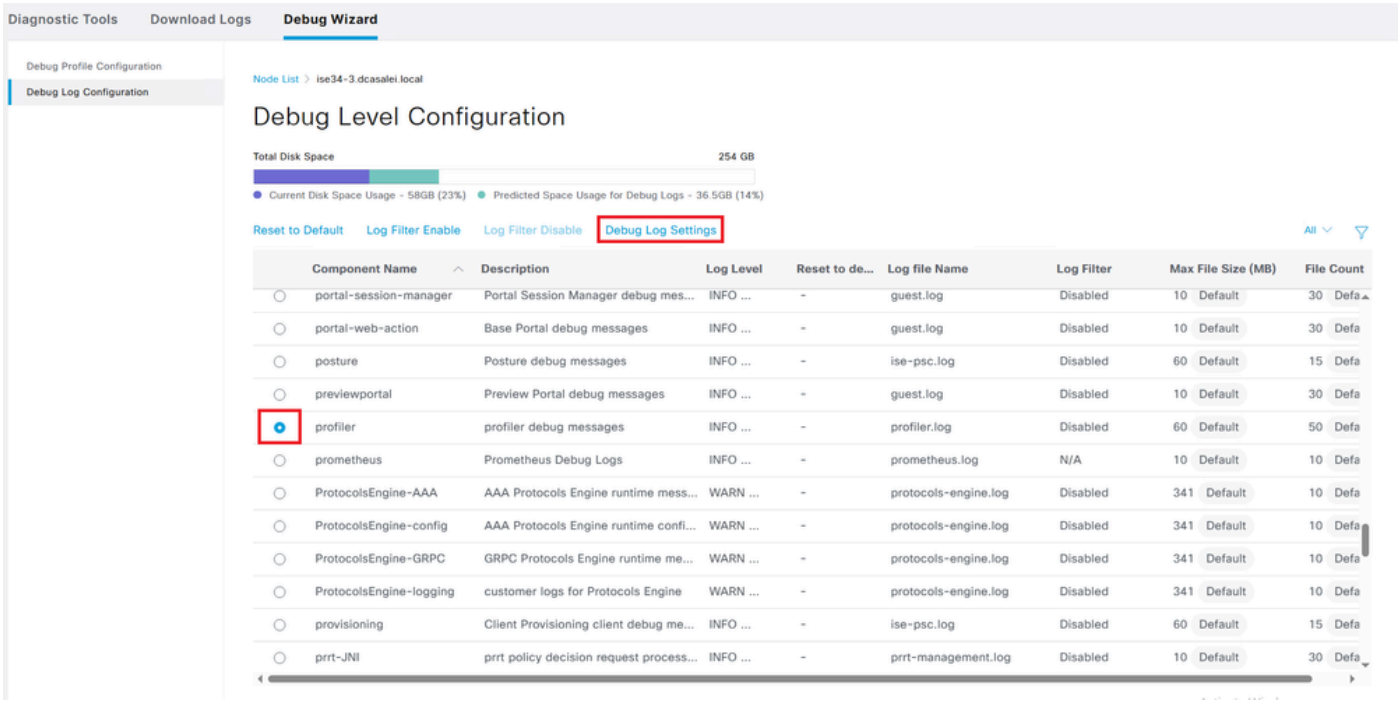
2025/09/19 14:36:25.431793040 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS: Send Accounting-Request
2025/09/19 14:36:25.431800182 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  authenticator 37 19 72
2025/09/19 14:36:25.431804371 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Vendor, Cisco       [26]
2025/09/19 14:36:25.431808600 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:   Cisco AVpair       [1]
2025/09/19 14:36:25.431811616 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Vendor, Cisco       [26]
2025/09/19 14:36:25.431815180 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:   Cisco AVpair       [1]
2025/09/19 14:36:25.431817947 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Vendor, Cisco       [26]
2025/09/19 14:36:25.431822305 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:   Cisco AVpair       [1]
2025/09/19 14:36:25.431826085 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  User-Name           [1]
2025/09/19 14:36:25.431828885 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Vendor, Cisco       [26]
2025/09/19 14:36:25.431832691 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:   Cisco AVpair       [1]
2025/09/19 14:36:25.431835418 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Vendor, Cisco       [26]
2025/09/19 14:36:25.431839009 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:   Cisco AVpair       [1]
2025/09/19 14:36:25.431842591 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Called-Station-Id   [30]
2025/09/19 14:36:25.431846145 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Calling-Station-Id  [31]
2025/09/19 14:36:25.431851298 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  NAS-IP-Address      [4]
2025/09/19 14:36:25.431854702 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  NAS-Port-Id         [87]
2025/09/19 14:36:25.431859269 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  NAS-Port-Type       [61]
2025/09/19 14:36:25.431863238 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  NAS-Port            [5]
2025/09/19 14:36:25.431866514 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Calling-Station-Id  [31]
2025/09/19 14:36:25.431870007 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Called-Station-Id   [30]
2025/09/19 14:36:25.431873587 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Acct-Session-Id     [44]
2025/09/19 14:36:25.431882560 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Acct-Authentic      [45]
2025/09/19 14:36:25.431885338 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Class               [25]
2025/09/19 14:36:25.431933331 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Acct-Status-Type    [40]
2025/09/19 14:36:25.431937105 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Event-Timestamp     [55]
2025/09/19 14:36:25.431940547 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Acct-Delay-Time     [41]
2025/09/19 14:36:25.431973200 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS: Started 5 sec timeout
```

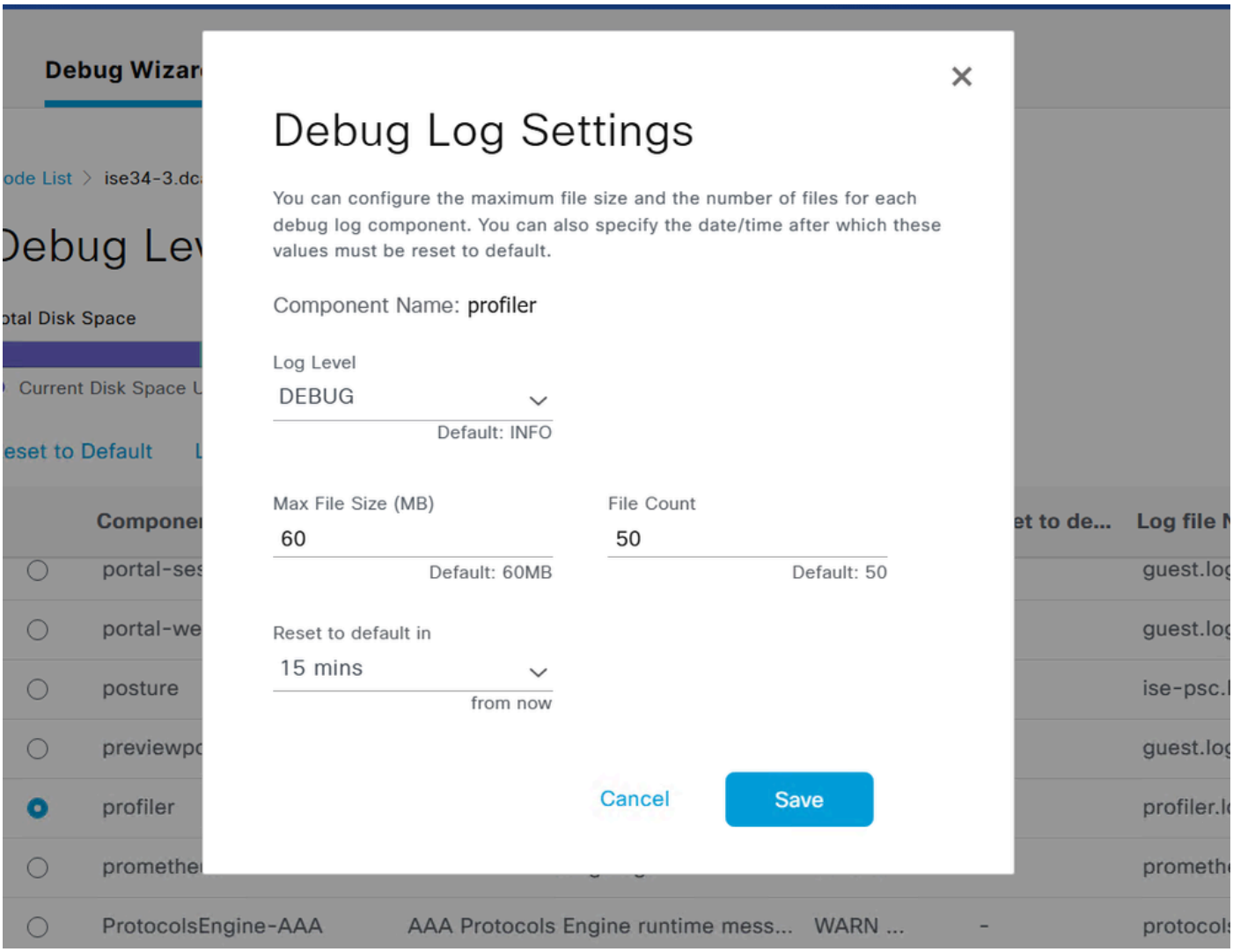
Packet Capture



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. 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.


Diagnostic Tools
Download Logs
Debug Wizard
Debug Profile Configuration
Debug Log Configuration
Node List > ise34-3.dcasalei.local
Debug Level Configuration
Total Disk Space
254 GB
Current Disk Space Usage - 58GB (23%)
Predicted Space Usage for Debug Logs - 36.5GB (14%)
Reset to Default
Log Filter Enable
Log Filter Disable
Debug Log Settings
Component Name
Description
Log Level
Reset to de...
Log file Name
Log Filter
Max File Size (MB)
File Count
portal-session-manager
Portal Session Manager debug mes...
guest.log
Disabled
portal-web-action
Base Portal debug messages
guest.log
Disabled
posture
Posture debug messages
ise-psc.log
Disabled
previewportal
Preview Portal debug messages
guest.log
Disabled
profiler
profiler debug messages
profiler.log
Disabled
prometheus
Prometheus Debug Logs
prometheus.log
N/A
ProtocolsEngine-AAA
AAA Protocols Engine runtime mess...
protocols-engine.log
Disabled
ProtocolsEngine-config
AAA Protocols Engine runtime confi...
protocols-engine.log
Disabled
ProtocolsEngine-GRPC
GRPC Protocols Engine runtime me...
protocols-engine.log
Disabled
ProtocolsEngine-logging
customer logs for Protocols Engine
protocols-engine.log
Disabled
provisioning
Client Provisioning client debug me...
ise-psc.log
Disabled
prrt-JNI
prrt policy decision request process...
prrt-management.log
Disabled


Debug Log Settings
You can configure the maximum file size and the number of files for each debug log component. You can also specify the date/time after which these values must be reset to default.
Component Name: profiler
Log Level
DEBUG
Default: INFO
Max File Size (MB)
60
Default: 60MB
File Count
50
Default: 50
Reset to default in
15 mins
from now
Cancel
Save

Look for this information:

- Debug indicating that the Radius probe received attributes:

```
2025-09-21 07:14:07,574 INFO   [RADIUSParser-1-thread-2][[]] cisco.profiler.probes.radius.RadiusPa
2025-09-21 07:14:07,574 DEBUG  [RADIUSParser-1-thread-2][[]] cisco.profiler.probes.radius.RadiusPa
```

- Debug indicating the attributes were successfully parsed:

```
2025-09-21 07:14:07,574 DEBUG  [RADIUSParser-1-thread-2][[]] cisco.profiler.probes.radius.RadiusPa
2025-09-21 07:14:07,574 DEBUG  [RADIUSParser-1-thread-2][[]] cisco.profiler.probes.radius.RadiusPa
2025-09-21 07:14:07,574 DEBUG  [RADIUSParser-1-thread-2][[]] cisco.profiler.probes.radius.RadiusPa
```

- Debug indicating the attributes were processed by the forwarder:

```
2025-09-21 07:14:08,709 DEBUG  [pool-55-thread-8][[]] cisco.profiler.infrastructure.probemgr.Forwa
MAC: E8:EB:34:D9:B8:F7
    Attribute:AAA-Server     value:ise34-3
        (... more attributes ...)
         Attribute:User-Name     value:CP-8811-SEPE8EB34D9B8F7
        Attribute:cdpCacheDeviceId     value:SEPE8EB34D9B8F7
        Attribute:cdpCachePlatform     value:Cisco IP Phone 8811
        Attribute:lldpSystemDescription     value:Cisco IP Phone 8811, V1, sip88xx.12-8-1-0101-482
        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. Profile Reclassification After New Attributes Are Received

Typically after new attributes are added to an existing collection for a specific device, the device or endpoint is added to the profiling queue to check if it must be assigned a different profile based on the new attributes:

```
2025-09-21 07:14:08,714 INFO   [pool-3352-thread-8][[]] cisco.profiler.infrastructure.profiling.Profile

2025-09-21 07:14:08,724 DEBUG  [pool-3352-thread-8][[]] cisco.profiler.infrastructure.profiling.Profile
```

```
2025-09-21 07:14:08,727 DEBUG  [pool-3352-thread-8][[]] cisco.profiler.infrastructure.profiling.Profile

2025-09-21 07:14:08,729 DEBUG  [pool-3352-thread-8][[]] cisco.profiler.infrastructure.profiling.Profile

2025-09-21 07:14:08,729 DEBUG  [pool-3352-thread-8][[]] cisco.profiler.infrastructure.profiling.Profile
```

Related Information

- Design Zone Campus and Branch
- Configuring Profiler Policies
- Cisco Technical Support & Downloads