为ISE分析配置设备传感器

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 步骤1.标准AAA配置
- 步骤2.配置设备传感器

验证

故障排除

- 步骤1.检验CDP/LLDP收集的信息
- 步骤2.检查设备传感器缓存
- 步骤3.检查Radius记账中是否存在属性
  - Radius调试
  - 数据包捕获
- 步骤4.检验ISE上的分析器调试
- 步骤5.接收新属性后的配置文件重新分类

相关信息

简介

本文档介绍如何配置设备传感器，以便其在ISE上用于分析目的。

先决条件

要求

Cisco 建议您了解以下主题：

- Radius协议
- 思科Catalyst交换机9300
- 思科身份服务引擎(ISE)
- 思科发现协议(CDP)和链路层发现协议(LLDP)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ISE版本3.4补丁3
- 思科IP电话8811版本12.8.1
- 思科Catalyst交换机9300-48P版本17.12.4

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

设备传感器是有线网络接入设备（例如Cisco Catalyst交换机）支持的功能。它可以使用CDP、LLDP和DHCP等协议收集终端信息，并将收集的属性发送到RADIUS记帐数据包中的ISE。在仅无线部署中，ISE分析通常依赖于从无线控制器和DHCP探测数据接收的属性，而不是交换机设备传感器数据。分析器源提供ISE用于分类终端的分析策略。



注意：设备传感器仅从直接连接到网络接入设备的终端（一跳远）收集信息。 ISE使用收集的属性进行终端分析。

收集信息后，可以将其封装在Radius记账中，并发送到分析服务器。在本文中，ISE用作分析服务器。

配置

步骤1.标准AAA配置

要配置身份验证、授权和记帐(AAA)，请参阅以下步骤：

1. 在交换机上启用运行aaa new-model命令的AAA并全局启用802.1X。
2. 配置Radius服务器并启用动态授权（授权更改 — CoA。）
3. 启用CDP和LLDP协议。
4. 添加switchport身份验证配置。

```
!
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



          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



           auth-port 1812 acct-port 1813
 key




!
```

注意：您必须配置交换机以将思科供应商特定属性(VSA)发送到ISE。

可通过配置以下命令在记帐数据包内部发送以下属性：

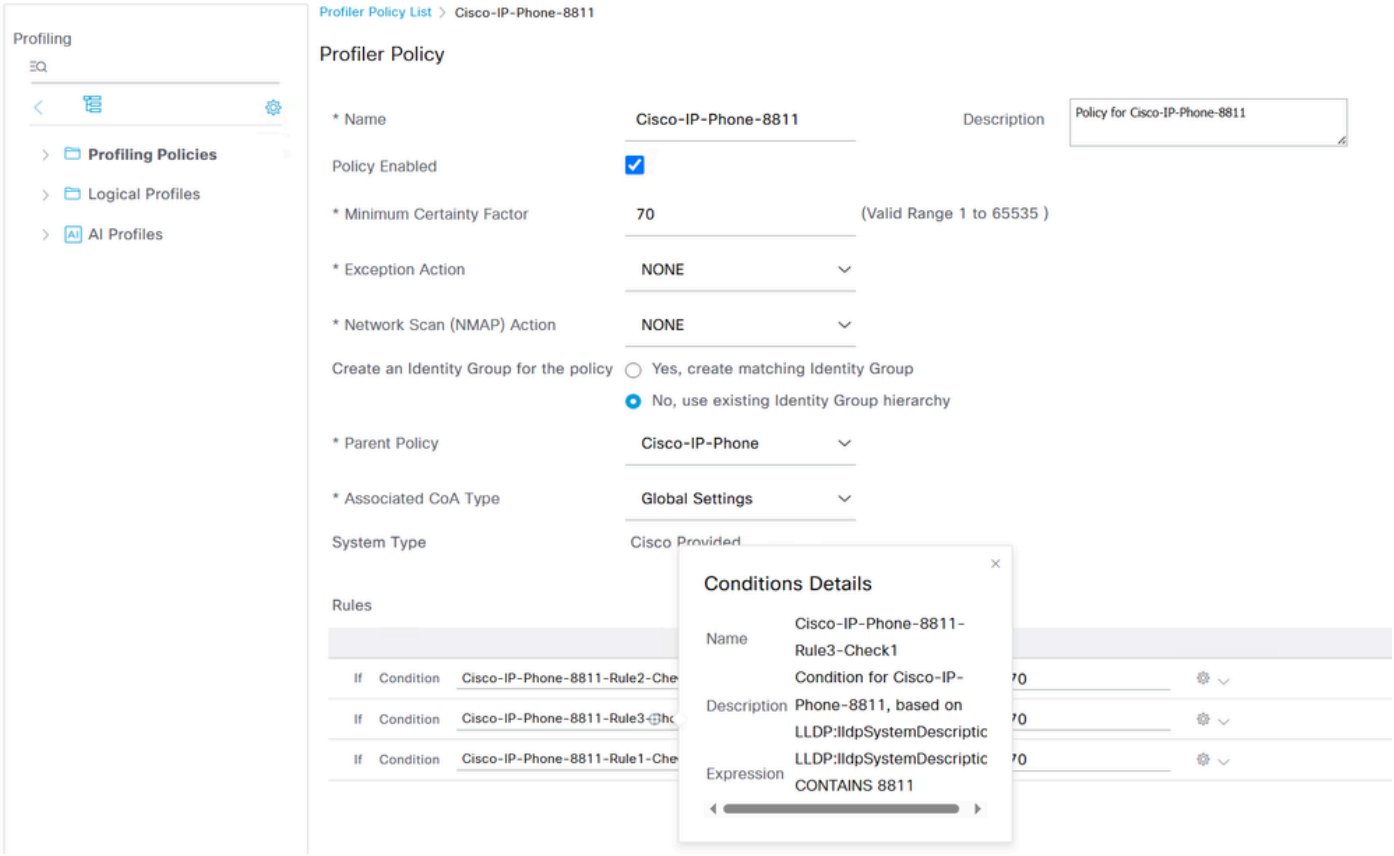
```
radius-server vsa send accounting
```

步骤2.配置设备传感器

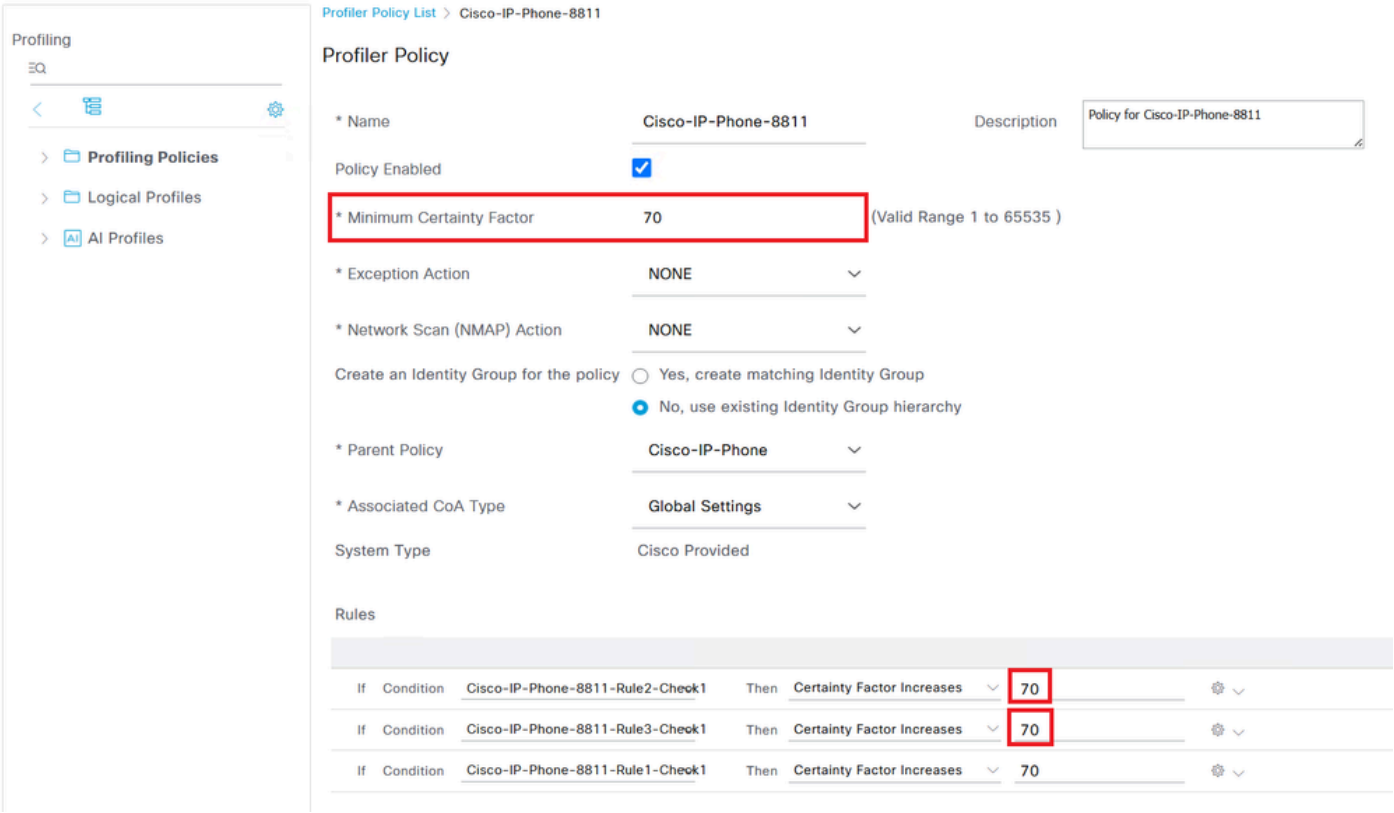
1.确定需要从CDP/LLDP获取哪些属性才能分析设备。对于Cisco IP电话8811，您可以使用以下命令：

- LLDP SystemDescription属性
- CDP CachePlatform属性

您可以通过检查分析器策略来验证用于分析设备的属性。为此，请导航到Work Centers > Profiler > Profiling Policies，然后选择要匹配的分析策略。



在下一个屏幕截图中，要分析为Cisco-IP-Phone-8811的终端所需的最小确定性因子为70。在本示例中，任一属性提供的确定性因子为70。但是，在ISE分配最终终端配置文件之前，终端还必须满足适用父配置文件的所需条件。



注意：要分析为特定的Cisco IP电话，必须满足所有父配置文件的最低条件。分析器必须匹配思科设备（最小确定系数10）和思科IP电话（最小确定系数20）。 即使分析器匹配这两个配置文件，也必须将其分析为特定的Cisco IP电话，因为每个IP电话型号的最小可信度因子为70。设备将分配给具有最高可信度的配置文件。

2.配置两个过滤器列表，一个用于CDP，另一个用于LLDP。这些指示哪些属性必须包含在Radius记帐消息中（此步骤是可选的）。

3.为CDP和LLDP创建两个过滤规格。在filter-spec中，您可以指示必须包括在记帐消息中或排除的属性列表。在本示例中，包括以下属性：

- 来自CDP的设备名称和平台类型
- 来自LLDP的系统说明

如果需要，您可以配置通过Radius传输到ISE的其他属性（此步骤也是可选的）。

4.添加device-sensor notify all-changes命令，以在为当前会话添加、修改或删除TLV时触发更新。

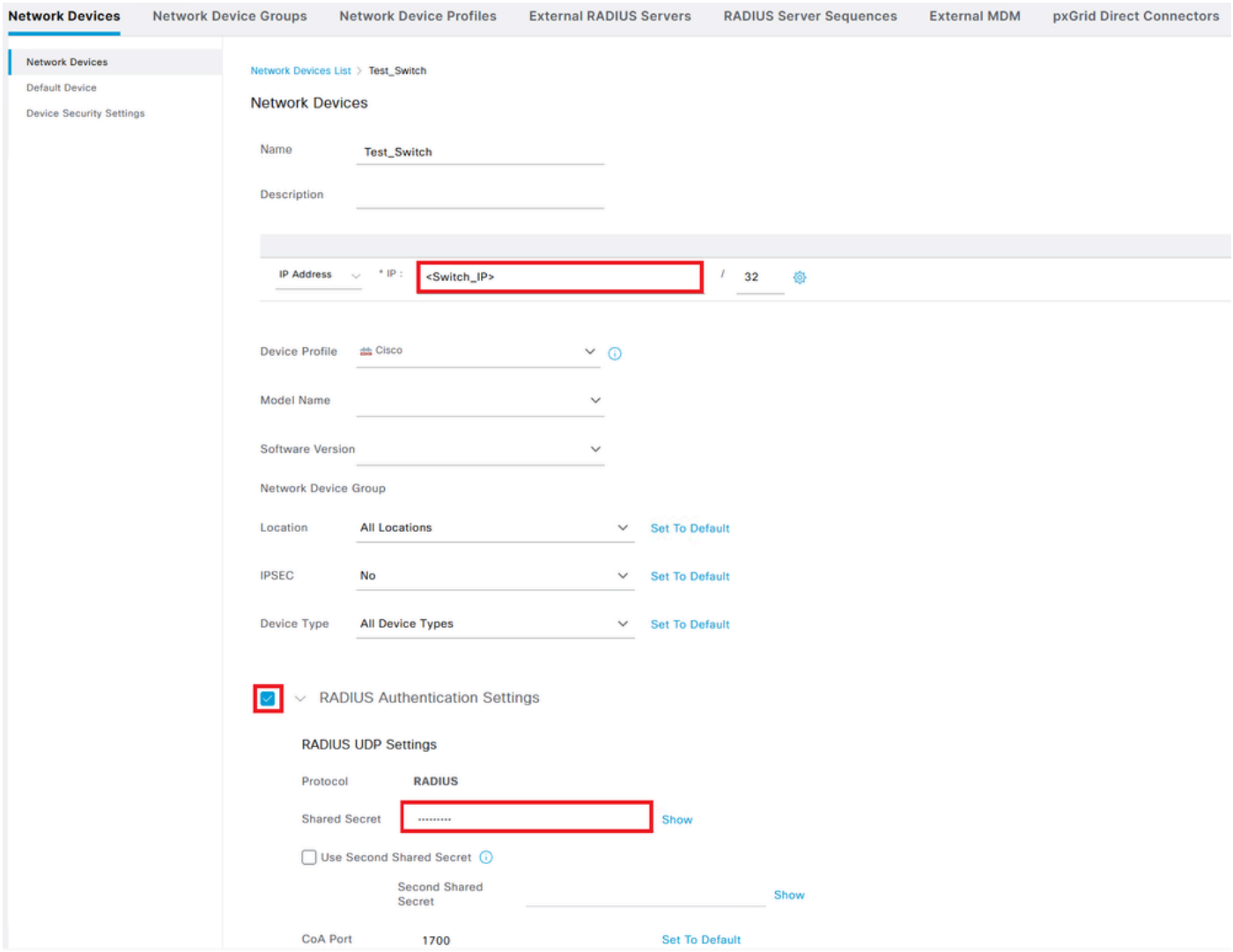
5.要发送设备传感器收集的信息，请配置device-sensor accounting命令。

```
!
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
!
```

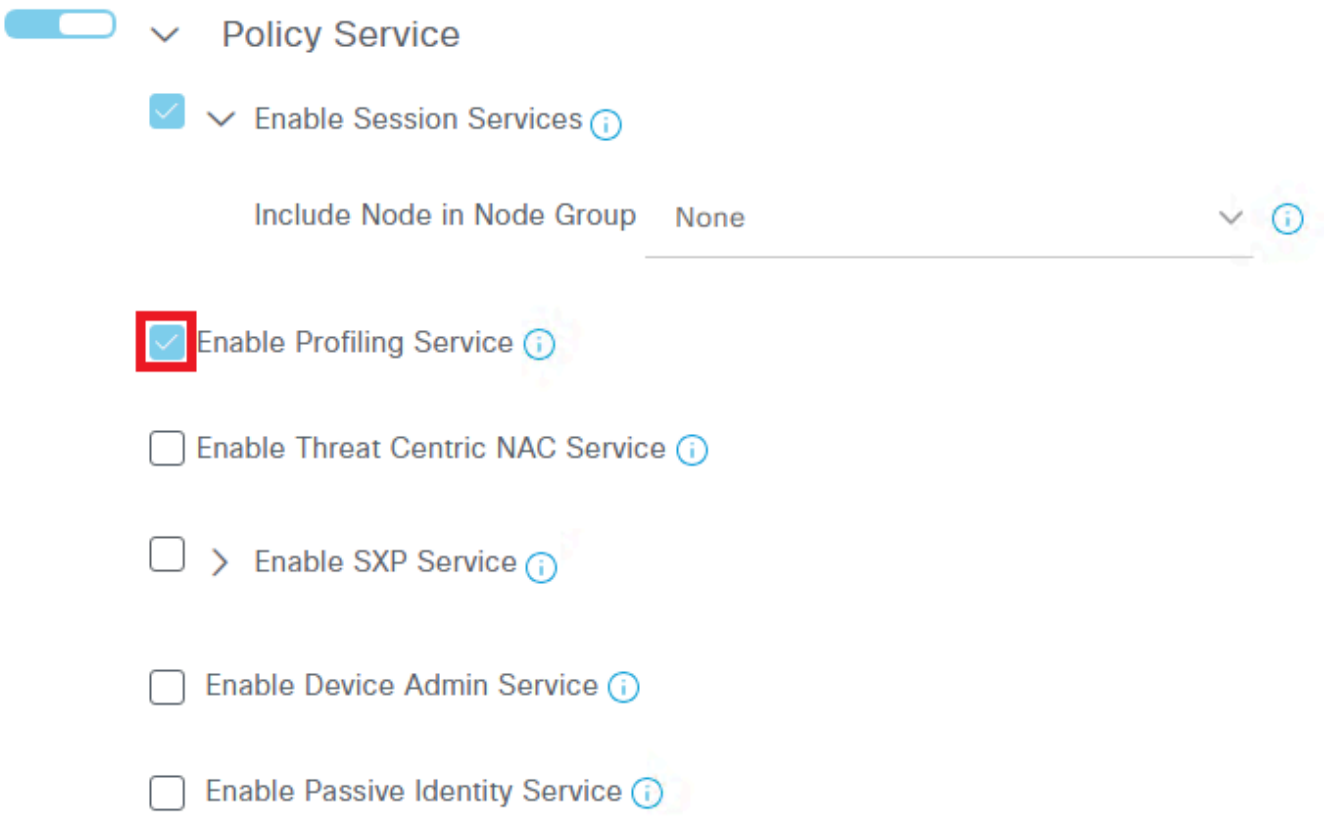


注意：设备传感器命令和支持的TLV可能因Catalyst平台和IOS XE版本而异。确认正在使用的交换机平台的配置指南中的命令支持和可用的TLV;步骤3.在ISE上配置分析。

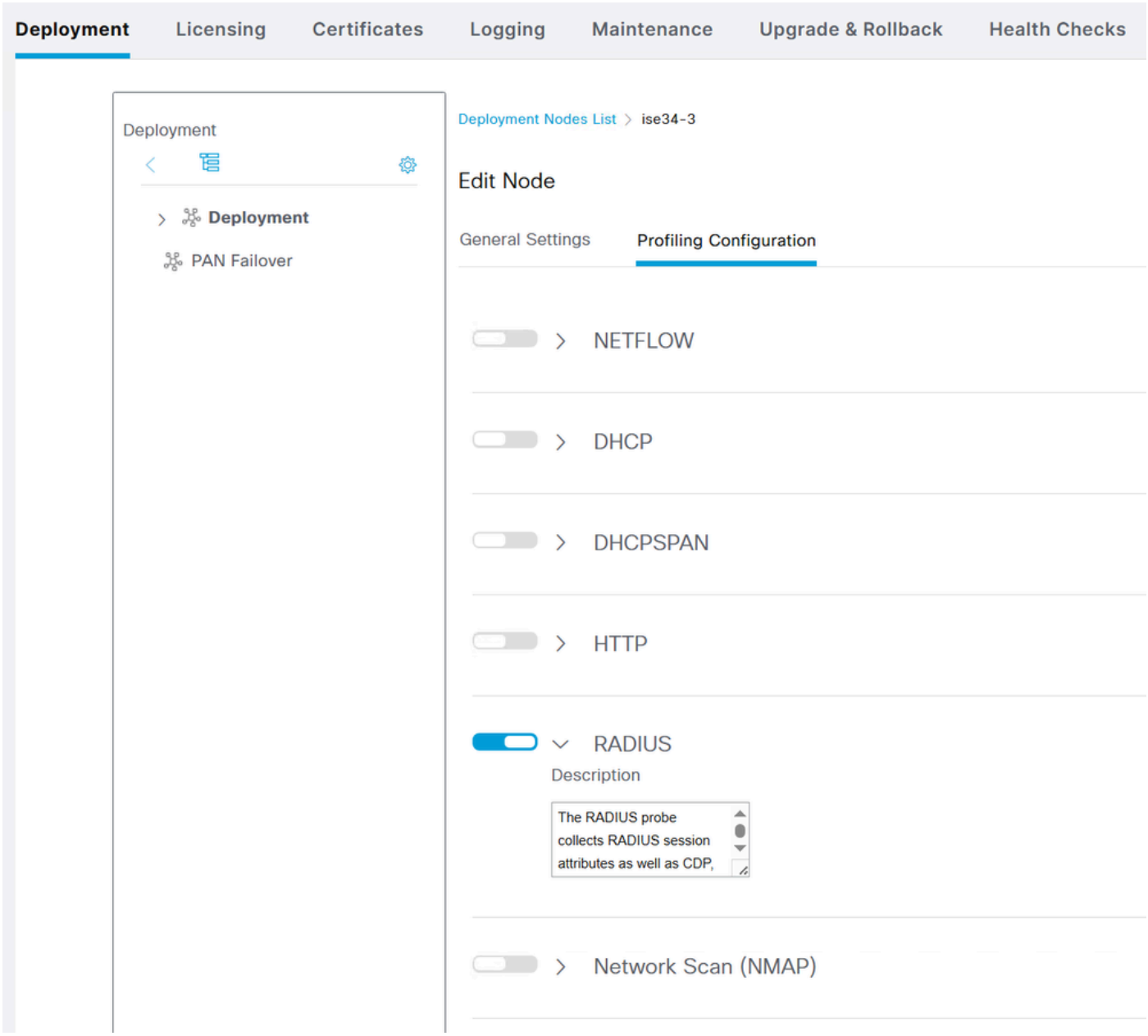
1.在Administration > Network Resources > Network Devices中将交换机添加为网络设备。使用交换机的Radius服务器密钥作为Authentication Settings:



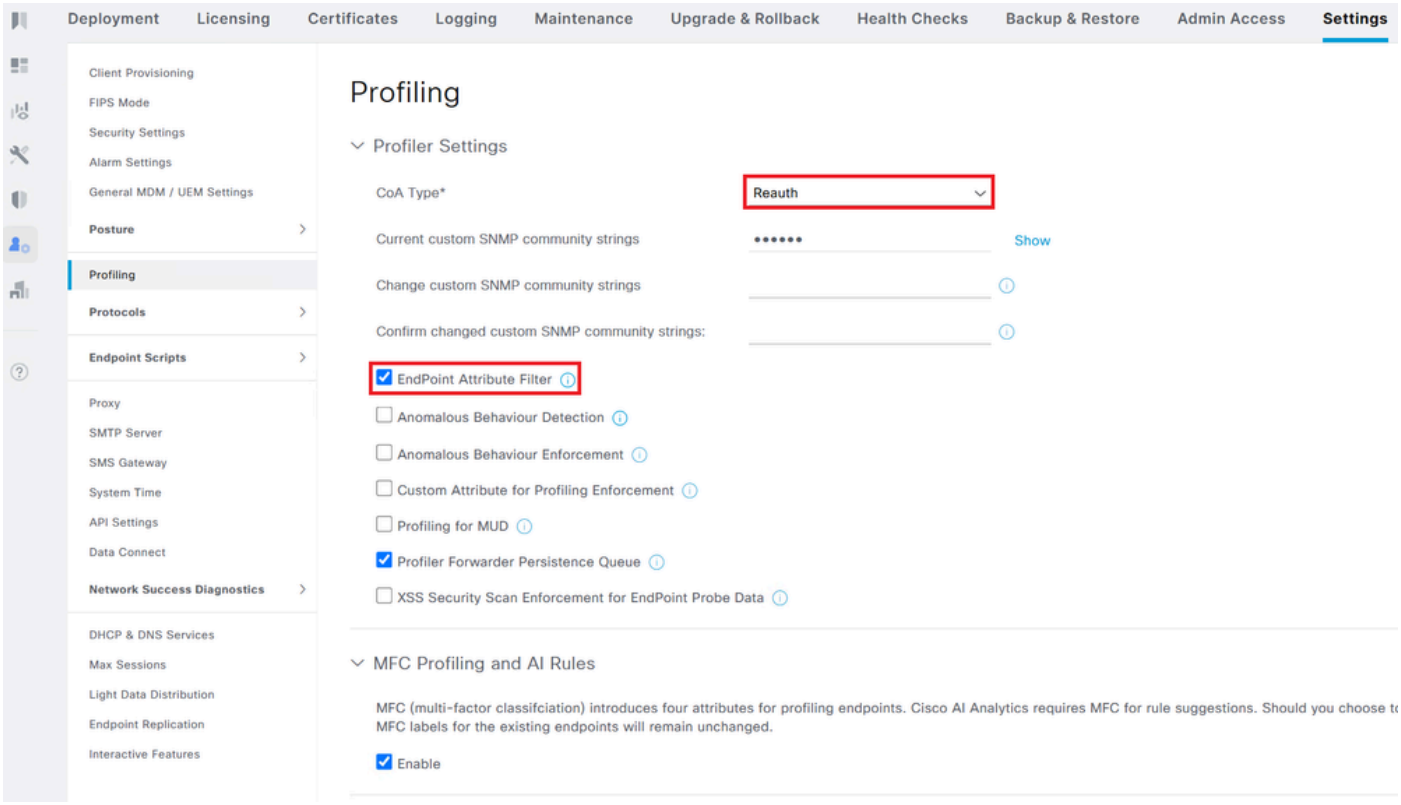
2.在ISE节点上启用分析服务。导航到管理>系统>部署，选择ISE节点，并在“策略服务”选项卡上启用分析服务选项。在要处理分析数据的PSN节点上启用分析服务。仅启用部署所需的探测，因为其他探测和启用分析的PSN可以提高系统资源利用率。



3.在分析节点上启用Radius探测。导航到Administration > System > Deployment，选择ISE节点，然后点击Profiling Configuration选项卡。



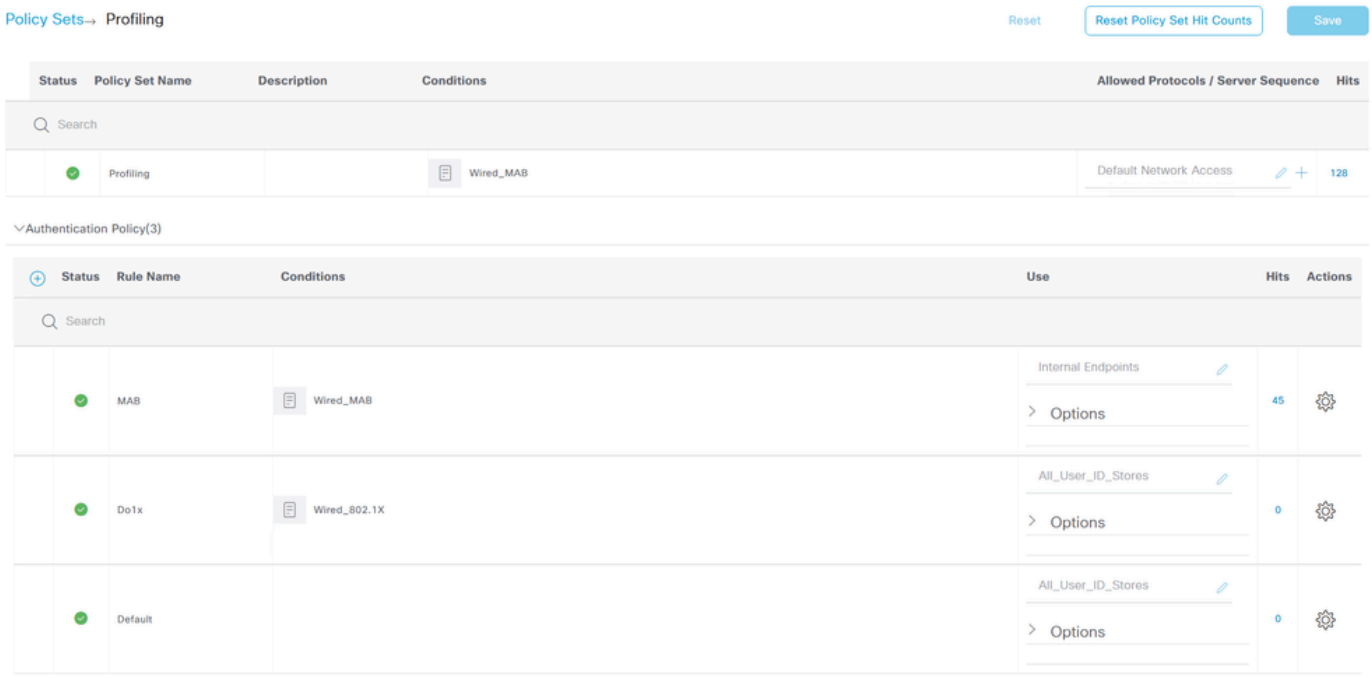
4.将CoA（授权更改）类型设置为Reauth，以便在分析后对终端执行重新身份验证。此外，请确保选中Endpoint Attribute Filter。导航到Administration > System > Settings > Profiling。



注意：最佳实践是在生产部署中启用终端属性过滤器，以避免收集过多不必要的分析器数据时出现性能问题。

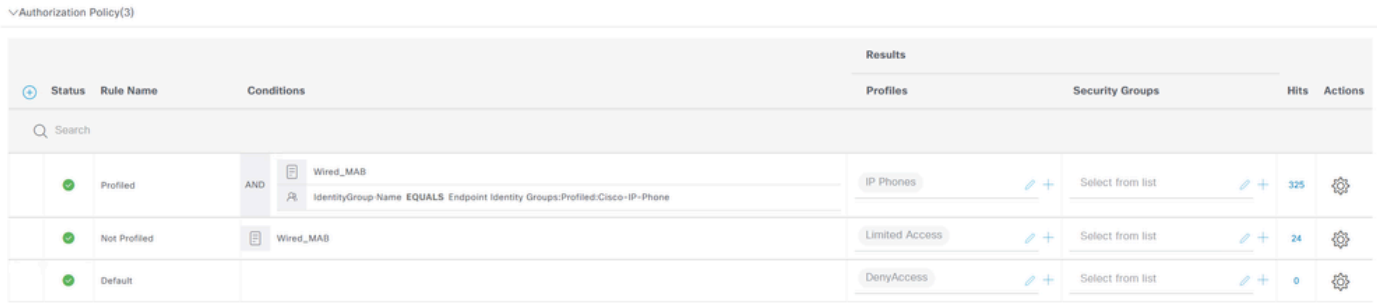
要向当前不存在的允许列表添加属性，您可以创建使用该属性的新Profiler条件和策略。可以将此属性自动添加到已存储和已复制属性的允许列表。如果某个终端仍被分类为“未知”，请在上下文可视性或终端分类中查看其收集的属性，并将其与目标分析策略中配置的条件和确定性因素进行比较。仅仅OUI匹配并不总是足以满足特定配置文件的最小确定性因素。

5.配置ISE身份验证规则：



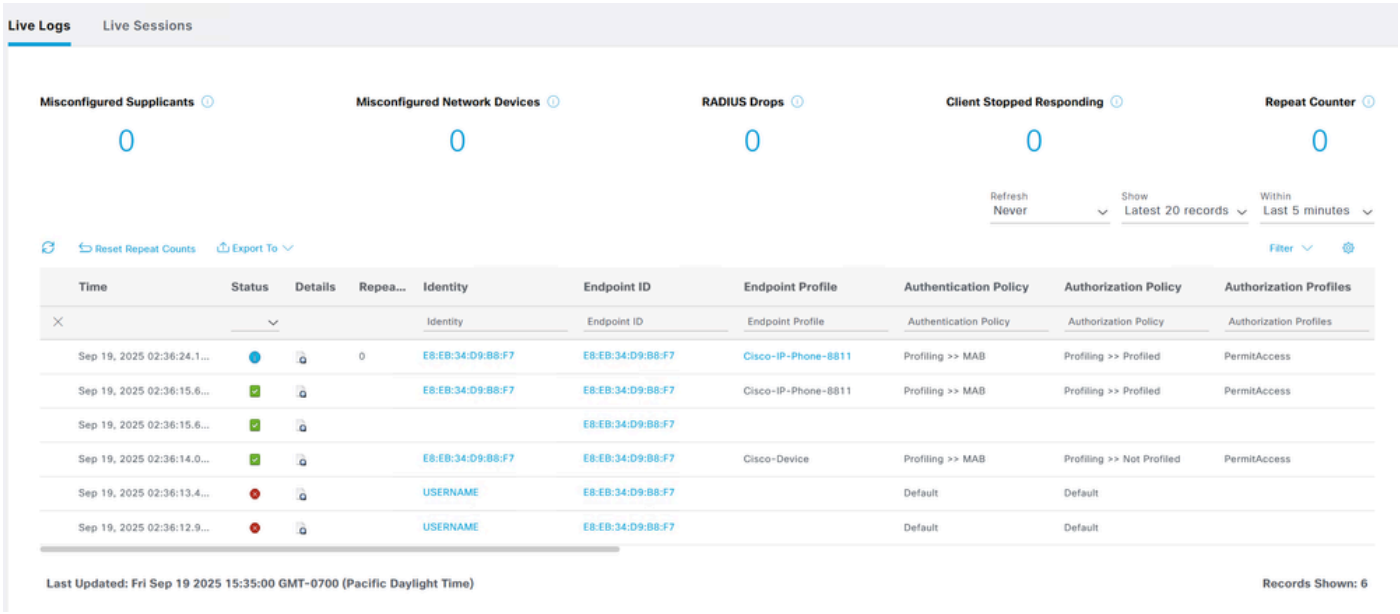
6.配置ISE授权规则。使用已分析的思科IP电话规则，该规则在ISE上预配置：

您可以配置可充当catch策略的授权策略，允许终端获得网络授权（有限访问），以确保属性在记帐数据包中发送。此外，创建另一个在设备分析后可以匹配的策略，确保设备可以访问网络中的必要资源。



验证

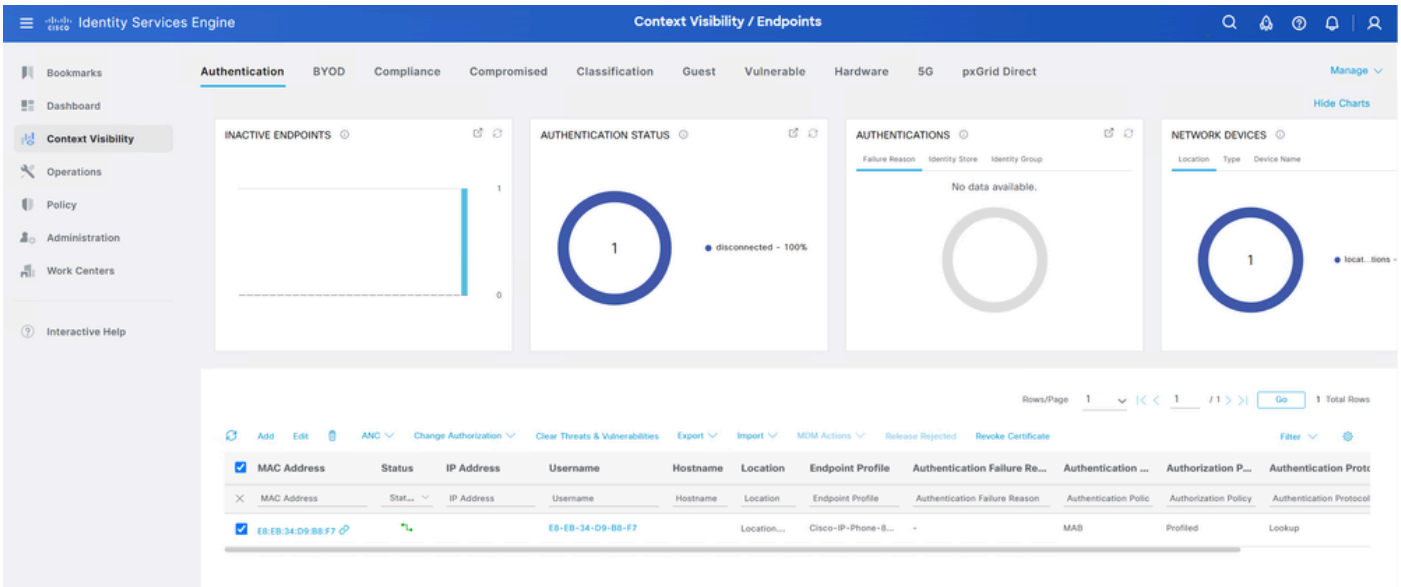
要验证分析是否正常工作，请参阅操作> Radius > Live Logs on ISE:

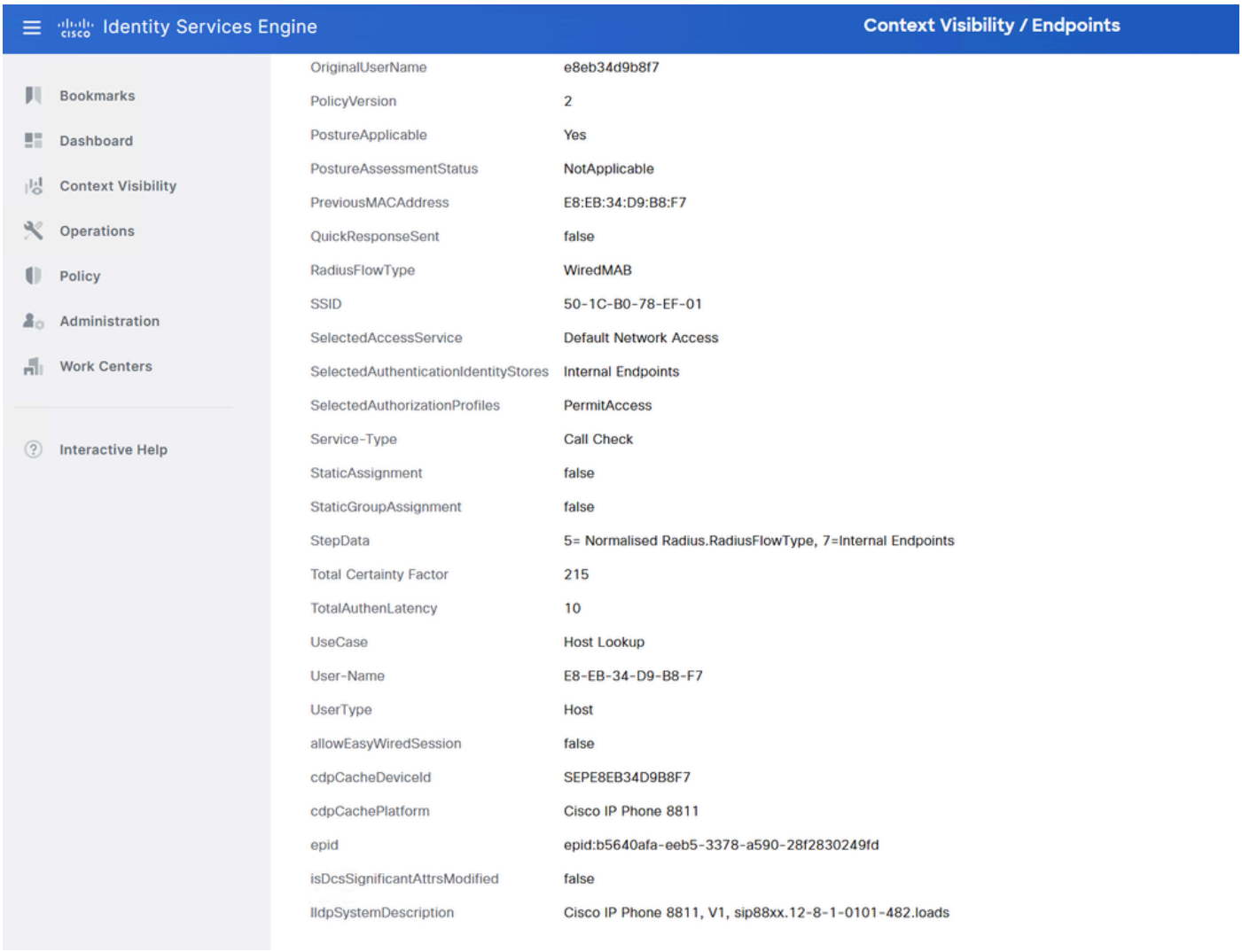


在此IP电话示例中，802.1X不进行身份验证，因此交换机根据配置的方法顺序回退到MAB。对于不使用802.1X的终端，此行为是预期行为。

MAB身份验证在下午02:36:14成功。在实时日志中，设备最初被分析为思科设备，因为MAC地址OUI与思科关联，与预定义的思科设备分析策略匹配。一旦设备收到网络访问，交换机就会在Radius Accounting数据包中发送CDP和LLDP属性。下午2:36:15,ISE分析终端并发送CoA以强制重新身份验证。在CoA成功后，终端重新验证并匹配思科IP电话的授权策略。

在Administration > Identity Management > Identities > Endpoints中，您可以按测试的终端MAC地址进行过滤，并查看Radius探测功能收集的属性类型及其值：





如您所观察，在此场景中计算的总确定系数为215。这是因为终端还匹配思科设备配置文件（总确定系数为30）和思科IP电话配置文件（总确定系数为45）。 此外，分析器还匹配Cisco-IP-Phone-8811的配置文件中的两个条件，此配置文件的确定系数为140（根据分析策略，每个属性为70）。综上所述：30 + 45 + 70 + 70 = 215。

故障排除

步骤1.检验CDP/LLDP收集的信息

```
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
```

如果您看不到收集的任何数据，请验证并检查交换机上的身份验证会话的状态（必须成功）：

```
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
```

检查是否启用了CDP和LLDP协议。检查是否存在任何有关CDP/LLDP的非默认命令，以及这些命令如何影响从终端检索属性。

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

在终端配置指南中验证该终端是否支持CDP/LLDP等。

步骤2.检查设备传感器缓存

```
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
```

如果在此字段中看不到任何数据或信息不完整，请验证并运行device-sensor命令；特别是过滤器列表和过滤器规格。

步骤3.检查Radius记账中是否存在属性

您可以检验在交换机上运行debug radius命令或在交换机和ISE之间执行数据包捕获。

Radius调试

```
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
```

要禁用调试，可以运行此命令：

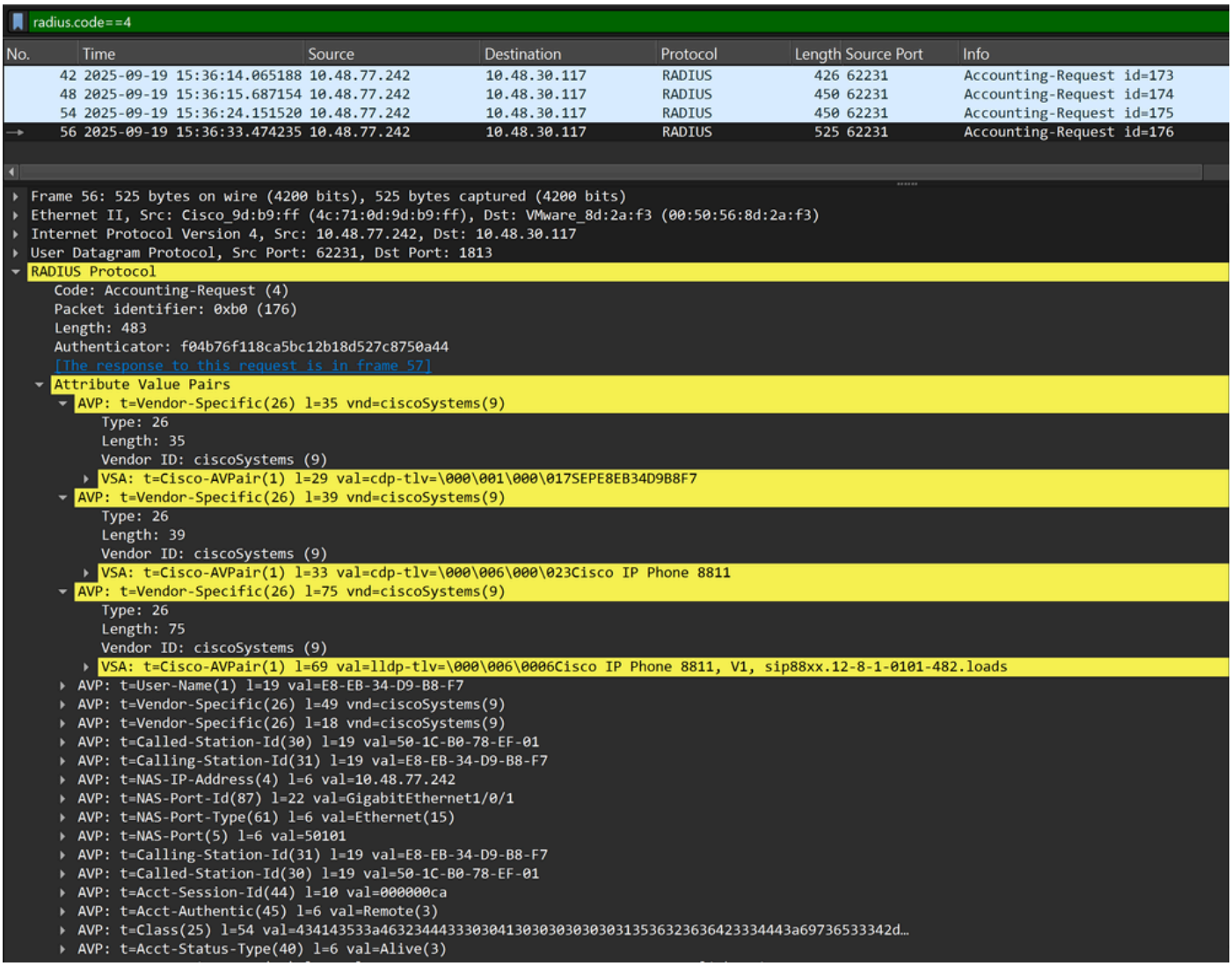
```
Switch#set platform software trace all notice
```

要显示日志：

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

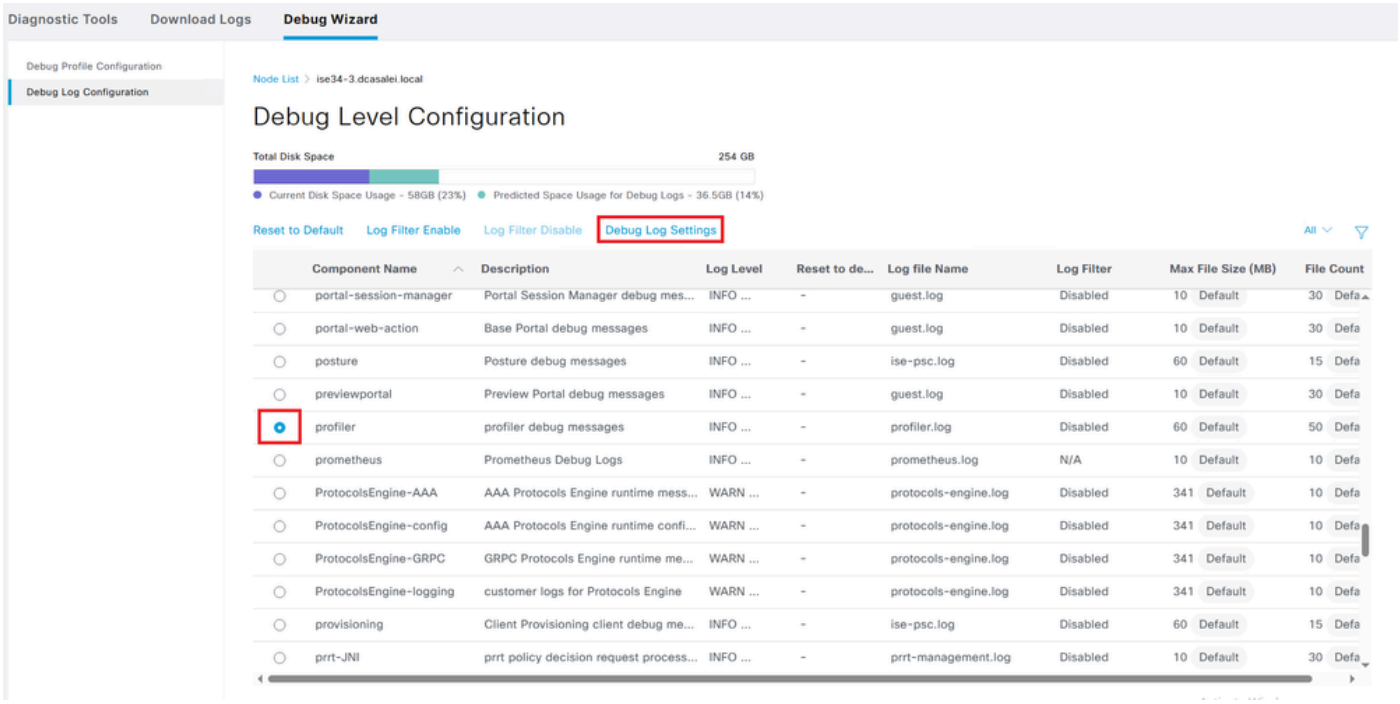
2025/09/19 14:36:25.431793040 {smd_RO-0}{1}: [radius] [23554]: (info): RADIUS: Send Accounting-Request
2025/09/19 14:36:25.431800182 {smd_RO-0}{1}: [radius] [23554]: (info): RADIUS:  authenticator 37 19 72
2025/09/19 14:36:25.431804371 {smd_RO-0}{1}: [radius] [23554]: (info): RADIUS:  Vendor, Cisco 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

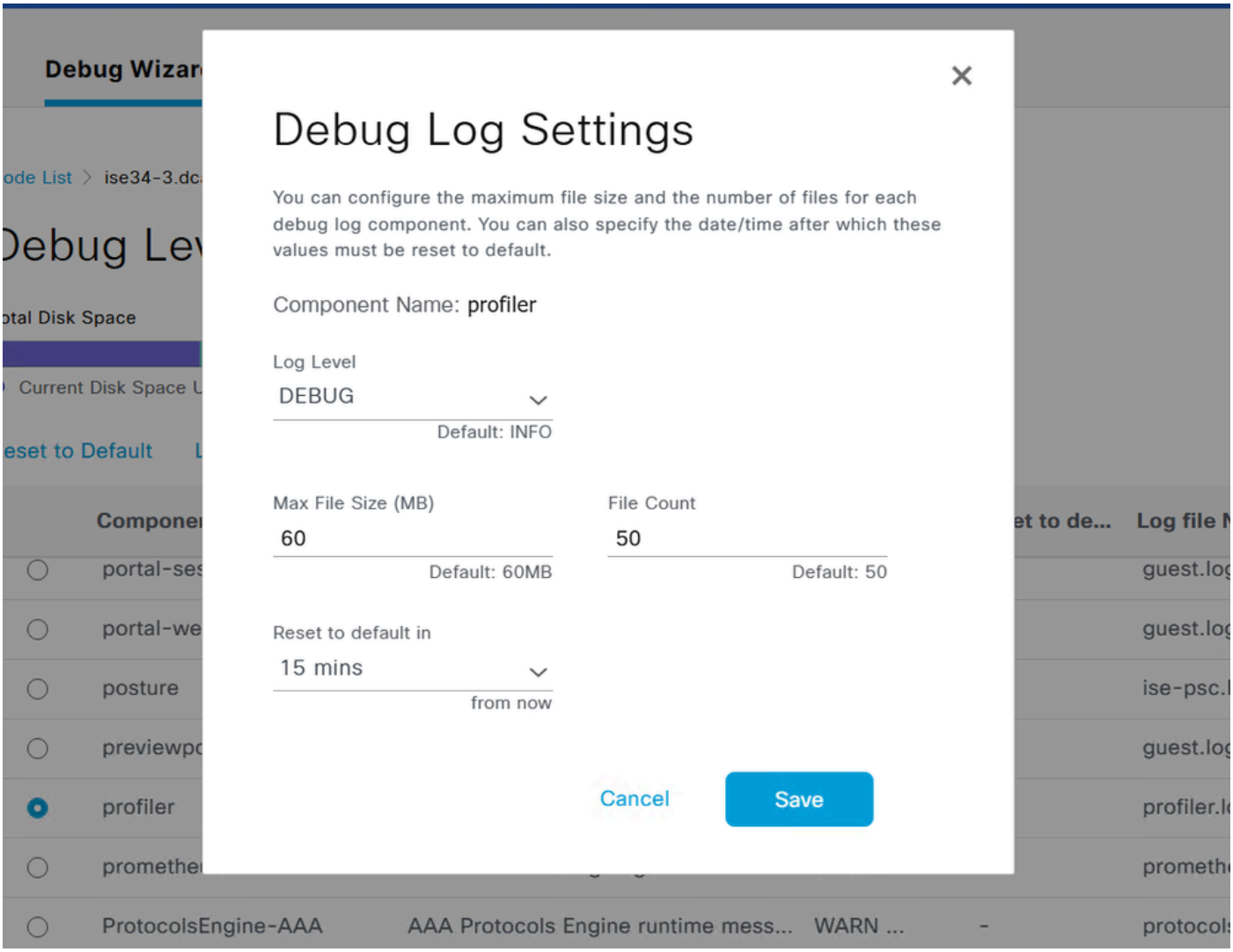
数据包捕获



步骤4.检验ISE上的分析器调试

如果属性是从交换机发送的，则可以检查是否在ISE上收到它们。要检查这一点，请为正确的PSN节点Administration > System > Logging > Debug Log Configuration > PSN > Profiler > Debug启用分析器调试，并再次执行终端身份验证。


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

查找以下信息：

- 调试表明Radius探测功能收到了以下属性：

```
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
```

- 调试指示已成功分析属性：

```
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
```

- 调试指示转发器已处理属性：

```
2025-09-21 07:14:08,709 DEBUG  [pool-55-thread-8][[]] cisco.profiler.infrastructure.probemgr.Forwa



       ,name=



        ]
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
```

注意：转发器将终端与其属性数据一起存储在Cisco ISE数据库中，然后通知分析器在网络上检测到的新终端。分析器将终端分类到终端身份组，并在数据库中存储具有匹配配置文件的终端。

步骤5.在收到新属性后重新分类配置文件

通常，在将新属性添加到特定设备的现有集合后，设备或终端会添加到分析队列，以检查是否必须根据新属性为其分配不同的配置文件：

```
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
```

相关信息

- 设计区园区和分支机构
- 配置分析器策略
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。