为ISE分析配置设备传感器

目录

简介

本文档介绍如何配置设备传感器，以便其可用于在ISE上进行分析。

先决条件

要求

Cisco 建议您了解以下主题：

- Radius协议
- 思科发现协议(CDP)、链路层发现协议(LLDP)和动态主机配置协议(DHCP)
- 思科身份服务引擎(ISE)
- Cisco Catalyst交换机2960

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1.3补丁3
- 思科Catalyst交换机2960s版本15.2(2a)E1
- Cisco IP Phone 8941版本SCCP 9-3-4-17

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

设备传感器是接入设备的功能。它允许收集有关已连接终端的信息。通常，设备传感器收集的信息可以来自以下协议：

- CDP
- LLDP
- DHCP

> 注意：在某些平台上，还可以使用H323、会话发起协议(SIP)、组播域解析(MDNS)或HTTP协议。设备传感器功能的配置可能因协议而异。示例在装有软件03.07.02.E的Cisco Catalyst 3850上提供。

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. 使用aaa new-model命令启用AAA，然后在交换机上全局启用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. 添加交换机端口身份验证配置

```
!
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
!
```

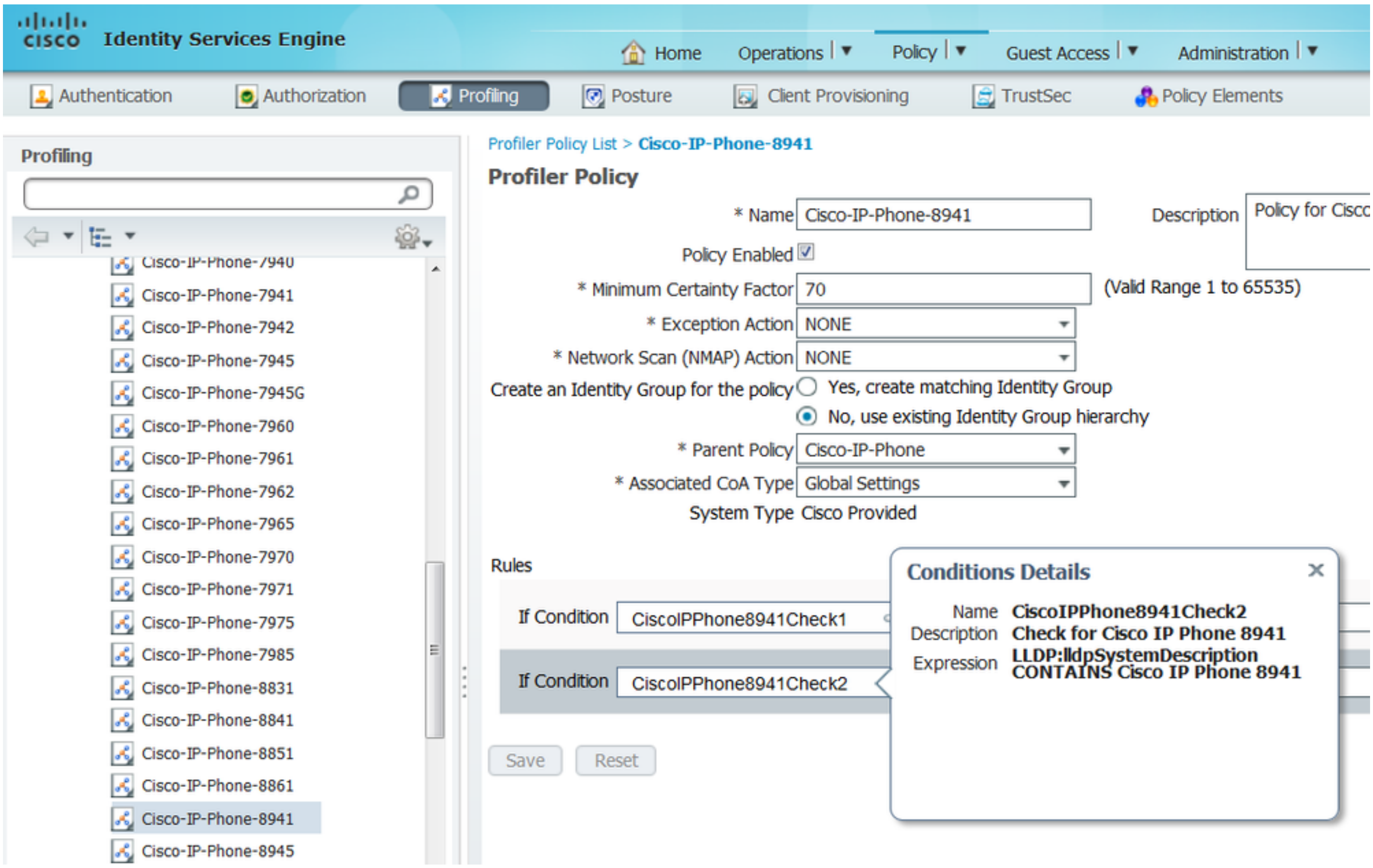
注意：在较新的软件版本中，默认情况下启用命令radius-server vsa send accounting。如果您在记账中看不到发送的属性，请验证是否已启用该命令。

第二步：配置设备传感器

1.

确定分析设备时需要使用CDP/LLDP中的哪些属性。对于Cisco IP电话8941，您可以使用以下命令：

- LLDP SystemDescription属性
- CDP CachePlatform属性



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

Profiler Policy

* Name: Cisco-IP-Phone-8941

Description: Policy for Cisco

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

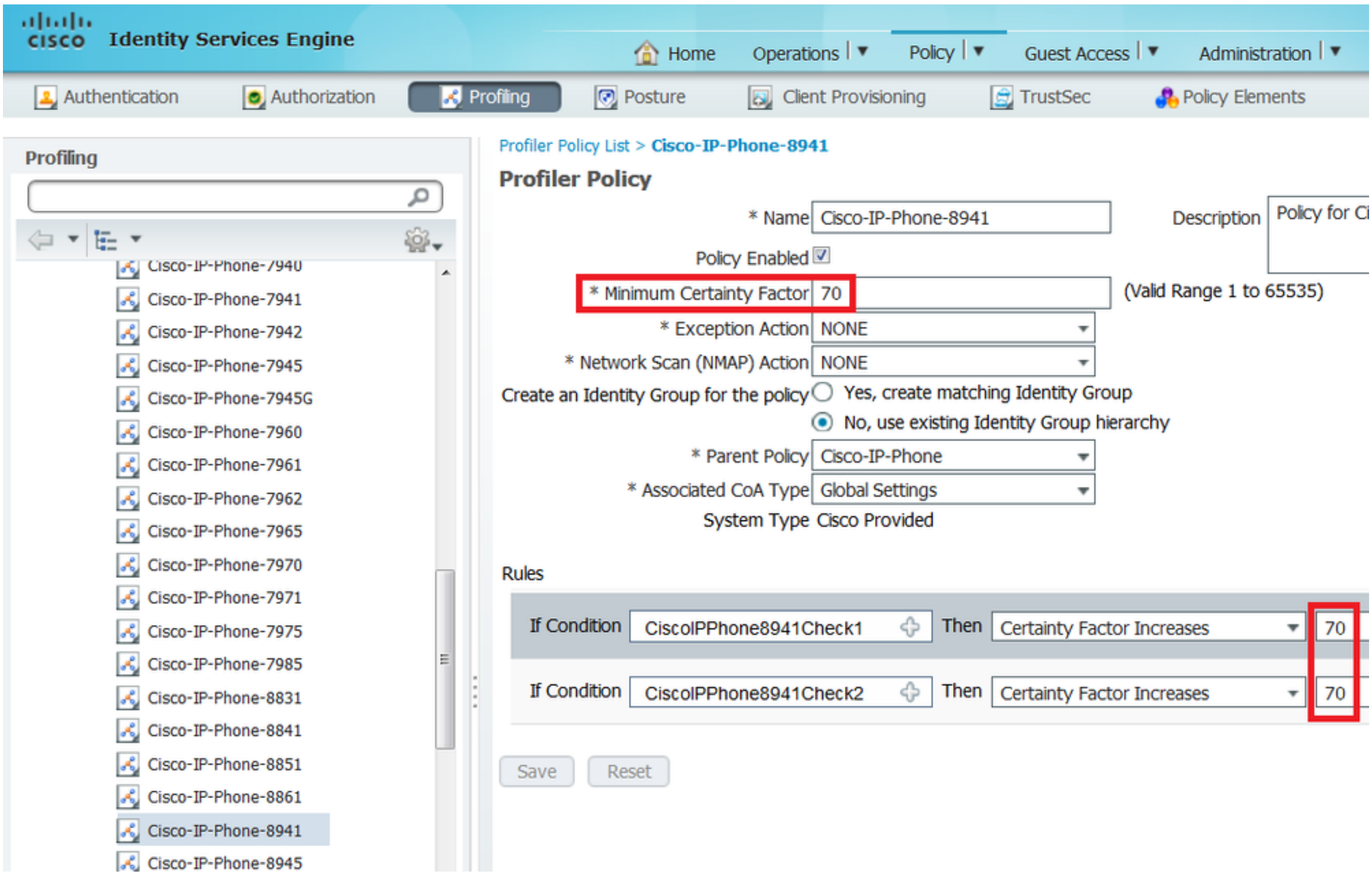
Conditions Details

Name: **CiscoIPPhone8941Check2**

Description: **Check for Cisco IP Phone 8941**

Expression: **LLDP:lldpSystemDescription CONTAINS Cisco IP Phone 8941**

出于我们的目的，仅获得其中一项就足够了，因为两者都提供70的确定性工厂增加，并且要求分析为Cisco-IP-Phone-8941的最低确定性工厂为70：



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

注意：要分析为特定思科IP电话，必须满足所有父配置文件的最低条件。这意味着分析器必须匹配Cisco-Device（最低确定系数10）和Cisco-IP-Phone（最低确定系数20）。即使分析器符合这两个配置文件，它仍必须分析为特定的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记账消息中。此步骤是可选的。

3. 为CDP和LLDP创建两个过滤器规格。在filter-spec中，您可以指示必须包括在记帐消息中或从中排除的属性的列表。本示例包括以下属性：

- 来自CDP的设备名称
-

来自LLDP的系统说明

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

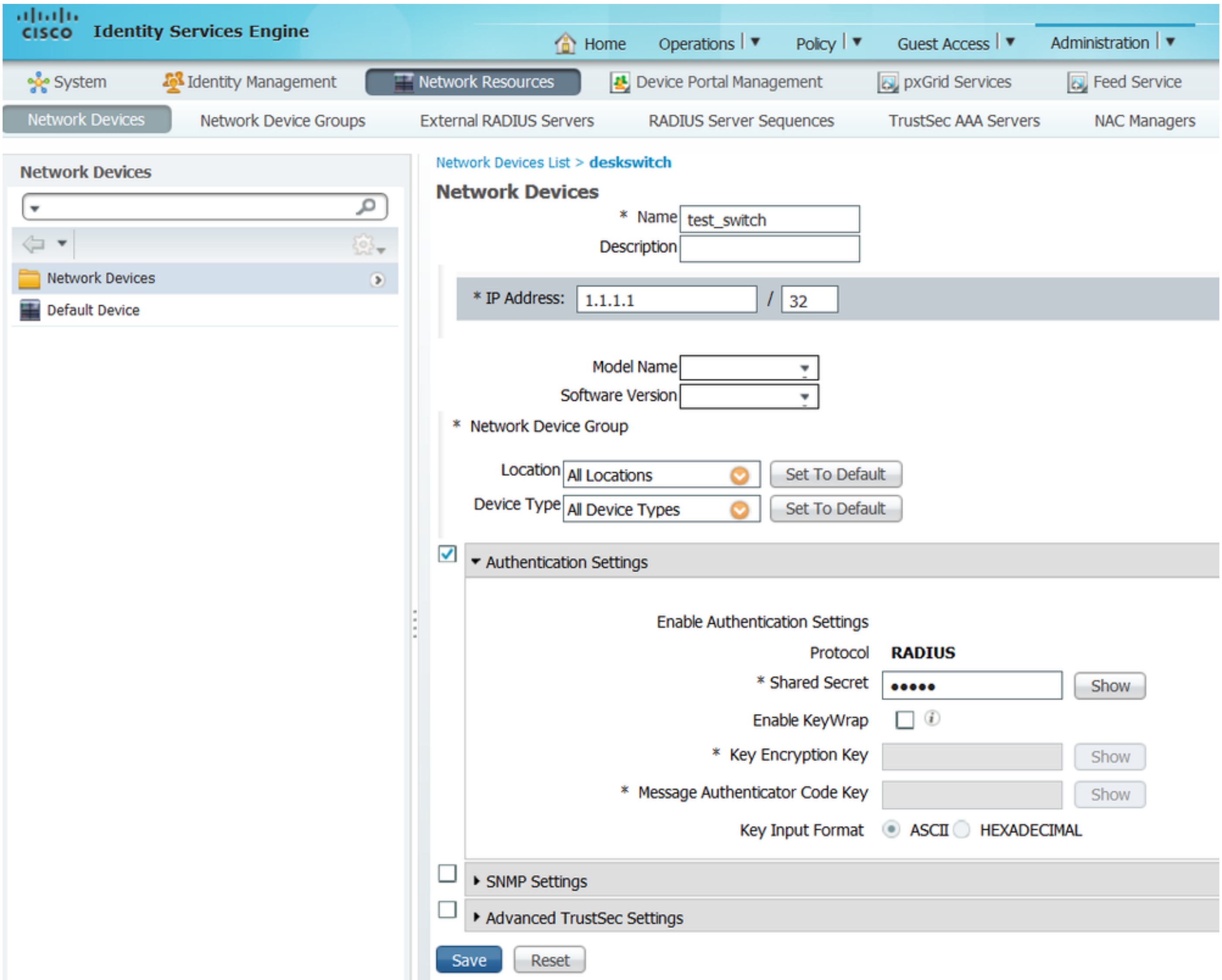
4. 添加命令device-sensor notify all-changes。每当为当前会话添加、修改或删除TLV时，它都会触发更新。

5. 要实际发送通过设备传感器功能收集的信息，必须使用device-sensor accounting命令明确通知交换机完成此操作。

```
! 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-se
```

第三步：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。在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:

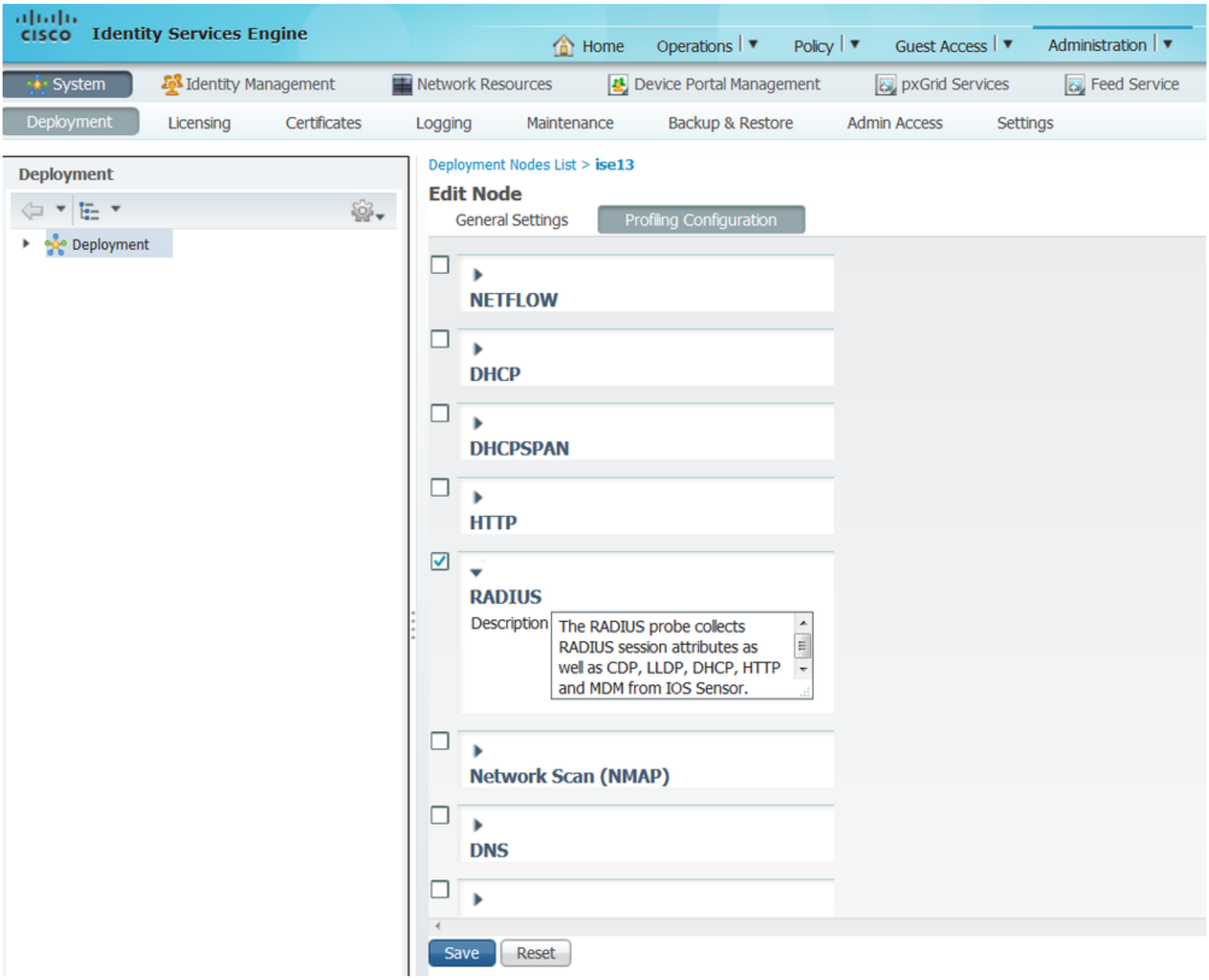
* Message Authenticator Code Key:

Key Input Format: ● ASCII ○ HEXADECIMAL

□ SNMP Settings

□ Advanced TrustSec Settings

2. 在Administration > System > Deployment > ISE node > Profiling Configuration中的分析节点上启用RADIUS探测器。如果必须使用所有PSN节点进行分析，请在所有PSN节点上启用探测：



Deployment Nodes List > ise13

Edit Node

General Settings | Profiling Configuration

□ NETFLOW

□ DHCP

□ DHCPSPAN

□ HTTP

☑ RADIUS

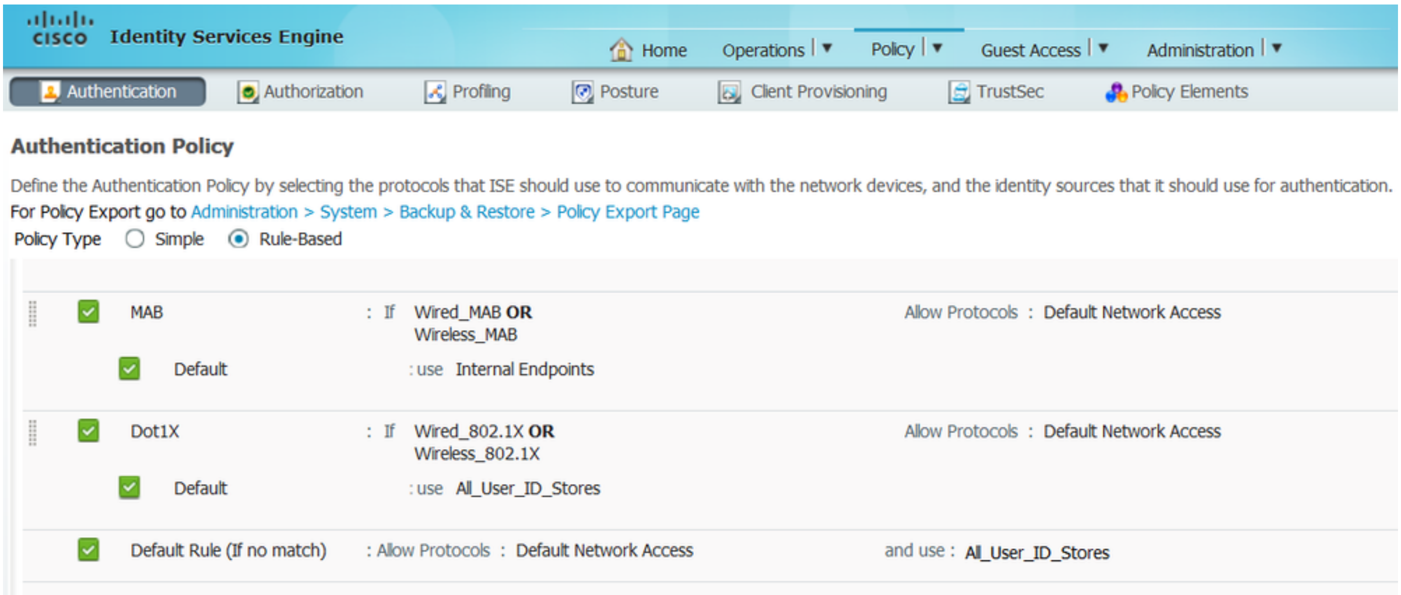
Description: The RADIUS probe collects RADIUS session attributes as well as CDP, LLDP, DHCP, HTTP and MDM from IOS Sensor.

□ Network Scan (NMAP)

□ DNS

□

3. 配置ISE身份验证规则。在本例中，使用ISE上预配置的默认身份验证规则：



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

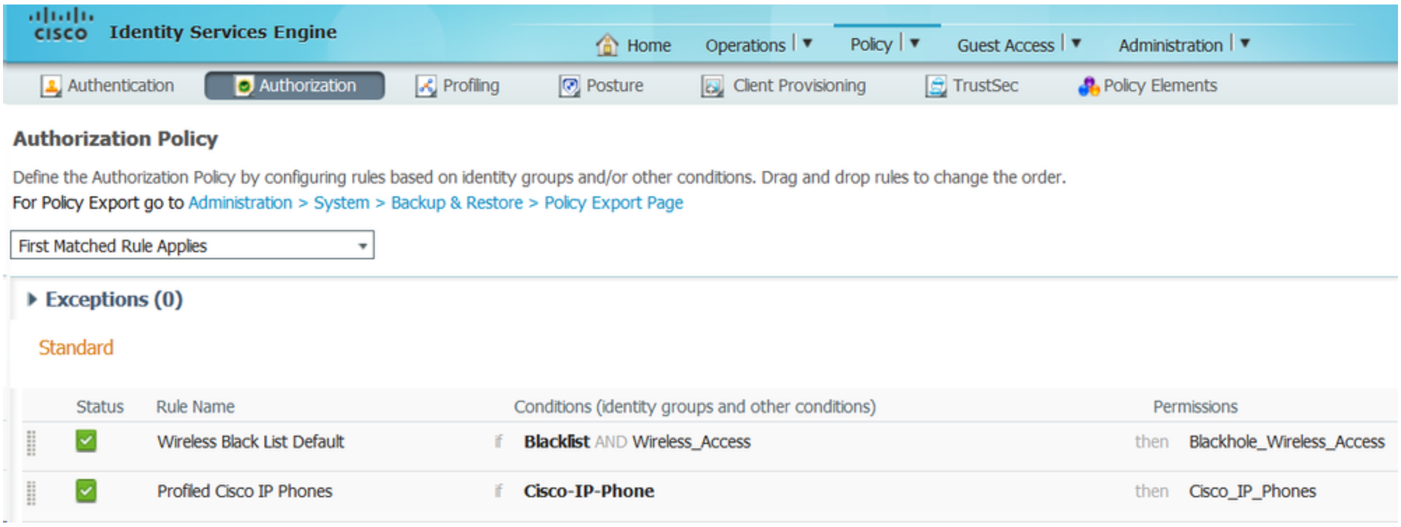
Policy Type ○ Simple ● Rule-Based

☑ 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. 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上已预配置：



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

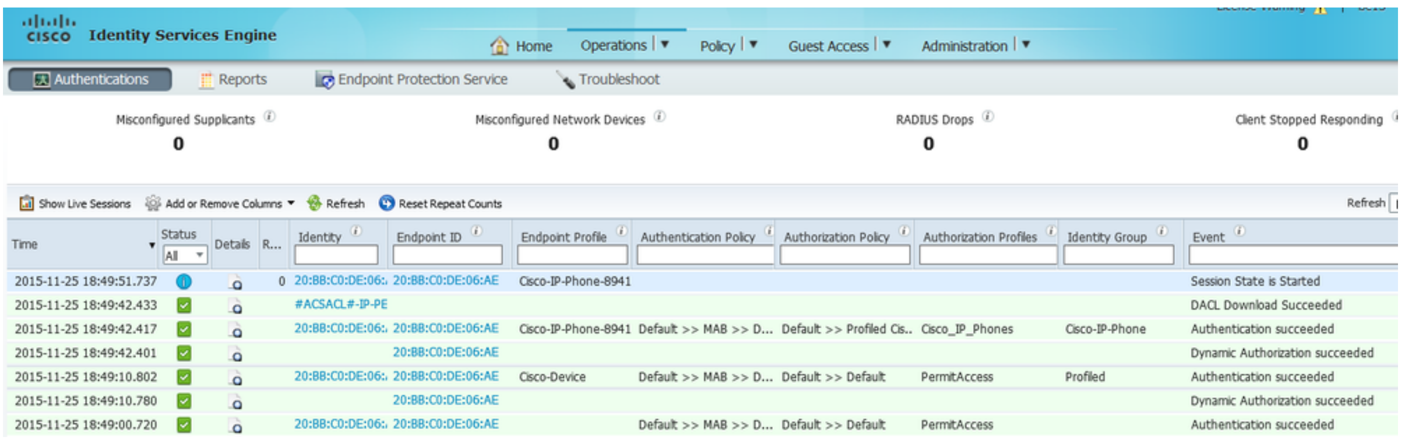
Exceptions (0)

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

验证

要验证分析是否正常工作，请参阅ISE上的Operations > Authentications：

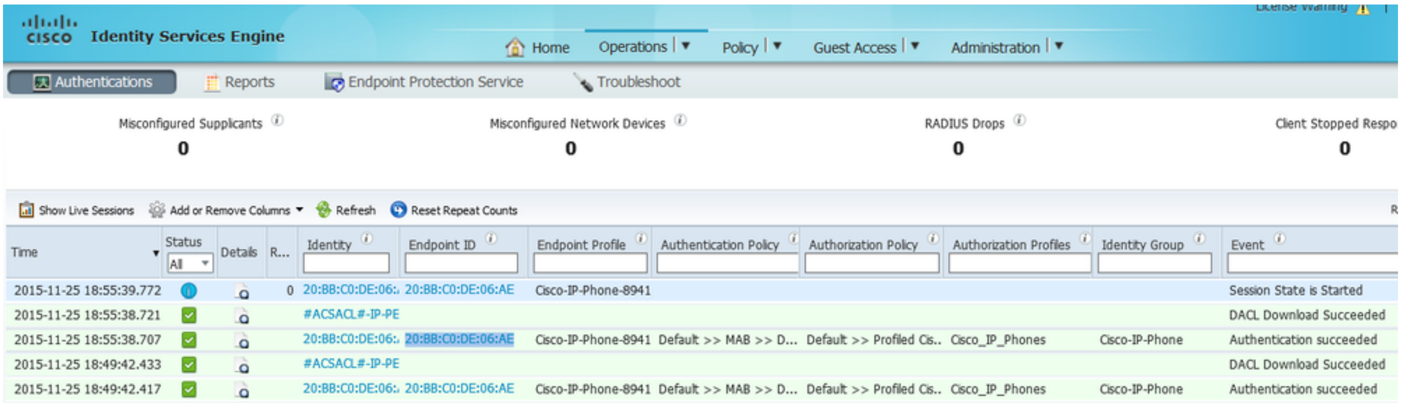


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding
0	0	0	0

Time	Status	Details	R...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Identity Group	Event
	All										
2015-11-25 18:49:51.737	ⓘ		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

首先，使用MAB (18:49:00)对设备进行身份验证。十秒后(18:49:10)，它被重新归档为Cisco-Device，在第一次身份验证(18:49:42)后的42秒后，它收到了Cisco-IP-Phone-8941配置文件。因此，ISE会返回特定于IP电话(Cisco_IP_Phones)的授权配置文件和允许所有流量(permit ip any)的可下载ACL。请注意，在这种情况下，未知设备具有基本的网络访问权限。这可以通过向ISE内部终端数据库添加Mac地址或允许对之前未知设备进行非常基本的网络访问来实现。

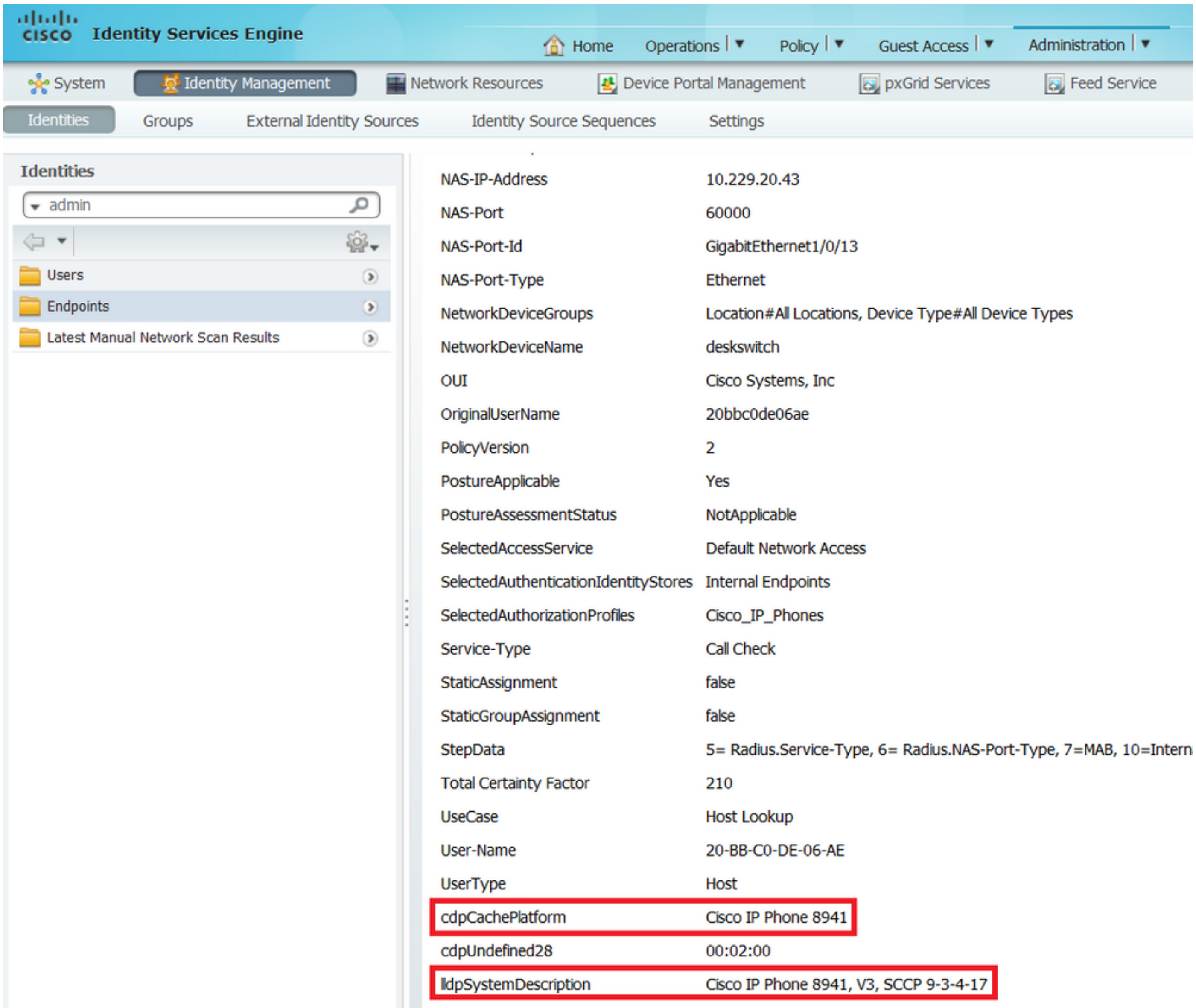
注意：在本示例中，初始分析大约需要40秒。在下一次身份验证中，ISE已经知道配置文件，并且会立即应用正确的属性（加入语音域和DACL的权限），除非ISE收到新的/更新的属性，并且必须重新分析设备。



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
	All										
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

在Administration > Identity Management > Identities > Endpoints > tested endpoint中，您可以查看RADIUS探测功能收集了什么类型的属性以及它们的值：



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

正如您看到的，在此场景中计算的总夺取系数为210。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40）。由于分析器匹配配置文件Cisco-IP-Phone-8941中的两个条件，因此此配置文件的确定系数为140（根据分析策略，每个属性为70）。总和：30+40+70+70=210。

故障排除

步骤1:验证CDP/LLDP收集的信息

```
switch#sh cdp neighbors g1/0/13 detail ------------------------- Device ID: SEP20BBC0DE06AE Entry address(es): Platform: Cisco IP Phone 8941 , Capabil

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: PUC17140FBO
    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
```

如果看不到收集的任何数据，请验证以下事项：

- 检查交换机上身份验证会话的状态（必须成功）：

```
piborowi#show authentication sessions int g1/0/13 details Interface: GigabitEthernet1/0/13 MAC Address: 20bb.c0de.06ae IPv6 Address: Unknown IPv4 A
```

- 检查CDP和LLDP协议是否已启用。检查是否存在任何有关CDP/LLDP/等的非默认命令，以及这些命令如何影响从终端进行属性检索

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

- 验证您的终端的配置指南中是否支持CDP/LLDP/等。

第二步：检查设备传感器缓存

```
switch#show device-sensor cache interface g1/0/13 Device: 20bb.c0de.06ae on port GigabitEthernet1/0/13 -------------------------------------------------- Proto
```

如果在此字段中看不到任何数据或信息不完整，请验证“device-sensor”命令，特别是filter-lists和filter-specs。

第三步：检查Radius记账中是否存在属性

您可以在交换机上使用debug radius命令验证是否在交换机和ISE之间执行数据包捕获。

Radius调试：

<#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 1
```

cdp-tlv

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

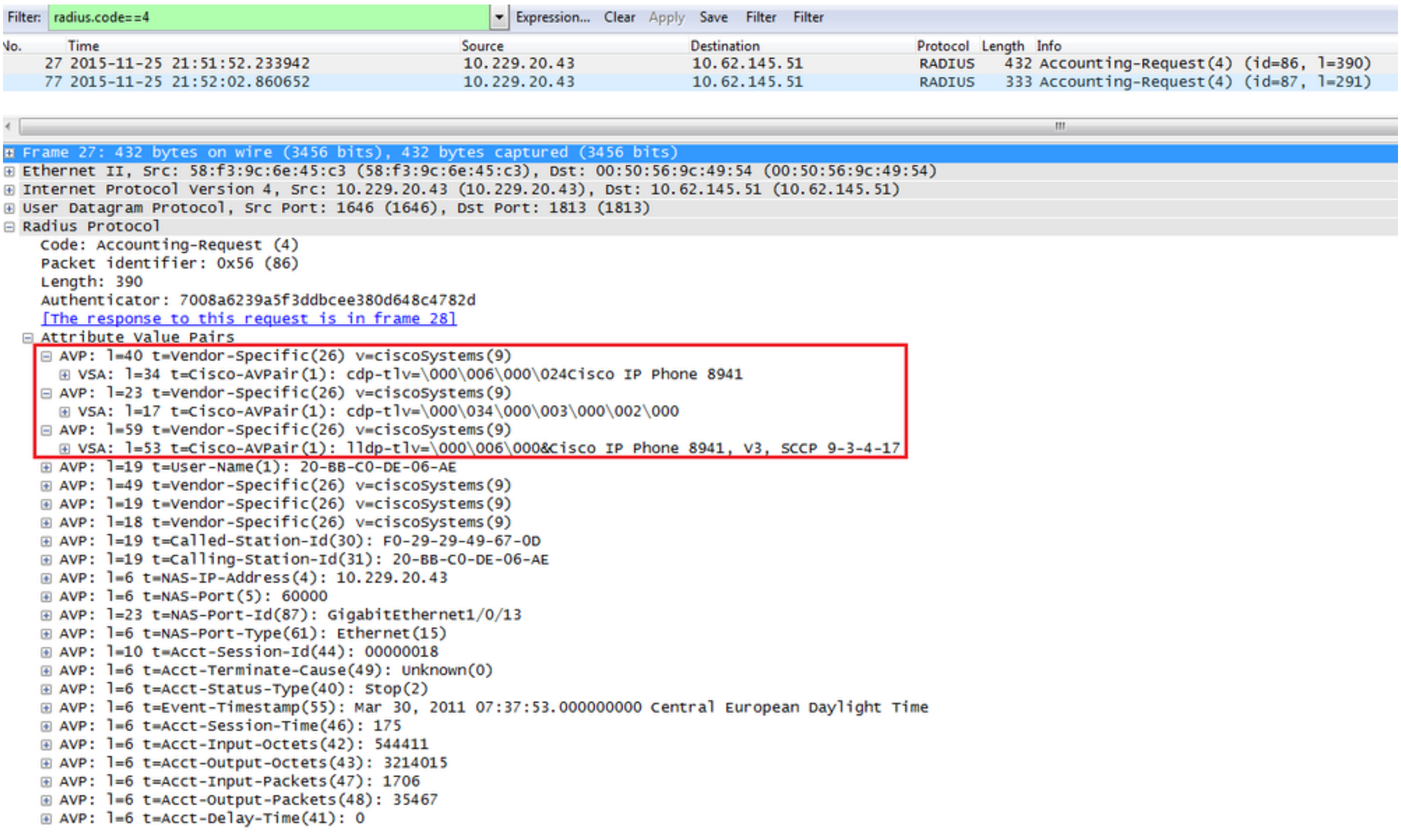
cdp-tlv

```
= " 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: Vend
```

数据包捕获:



```
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
```

第四步：验证ISE上的分析器调试

如果属性是从交换机发送的，可以检查ISE上是否收到这些属性。要检查此配置，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。

请查找以下信息：

- 调试指示radius探测功能已接收属性：

<#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=0AE518200000020
AllowedProtocolMatchedRule=MAB, Location=Location#All Locations, Device Type=Device Type#All Device Typ
```

- 调试指示已成功分析属性：

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

- 调试指示由转发器处理属性：

```
<#root>

2015-11-25 19:29:53,643 DEBUG [forwarder-6][] cisco.profiler.infrastructure.probemgr.Forwarder -:20:BB:C0:DE:06:AE:ProfilerCollection:- Endpoint A

Attribute:cdpCachePlatform value:Cisco IP Phone 8941 Attribute:cdpUndefined28 value:00:02:00 Attribute:l

 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，然后通知分析器您的网络中检测到的新终端。分析器将终端分类到终端身份组，并将具有匹配配置文件的终端存储在数据库中。

第五步： 分析新属性和设备分配

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

<#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
```

相关信息

- 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
- 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）。