ISE 프로파일링을 위한 장치 센서 구성

목차

소개

이 문서에서는 ISE에서 프로파일링 용도로 사용할 수 있도록 장치 센서를 구성하는 방법에 대해 설명합니다.장치 센서는 액세스 장치의 기능입니다.연결된 엔드포인트에 대한 정보를 수집할 수 있습니다.대부분 Device Sensor에서 수집한 정보는 다음 프로토콜에서 가져올 수 있습니다.

- CDP(Cisco Discovery Protocol)
- LLDP(Link Layer Discovery Protocol)
- DHCP(Dynamic Host Configuration Protocol)

일부 플랫폼에서는 H323, SIP(Session Initiation Protocol), MDNS(Multicast Domain Resolution) 또는 HTTP 프로토콜도 사용할 수 있습니다.장치 센서 기능의 구성 가능성은 프로토콜마다 다를 수 있습니다.위의 예와 같이 소프트웨어 03.07.02.E를 사용하는 Cisco Catalyst 3850에서 사용할 수 있습니다.

정보가 수집되면 radius 어카운팅에 캡슐화하여 프로파일링 서버로 보낼 수 있습니다.이 문서에서 ISE(Identity Service Engine)는 프로파일링 서버로 사용됩니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- RADIUS 프로토콜
- CDP, LLDP 및 DHCP 프로토콜
- Cisco Identity Service Engine
- Cisco Catalyst Switch 2960

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Identity Service Engine 버전 1.3 패치 3
- Cisco Catalyst Switch 2960s 버전 15.2(2a)E1
- Cisco IP Phone 8941 버전 SCCP 9-3-4-17

구성

1단계. 표준 AAA 컨피그레이션

AAA(Authentication, Authorization and Accounting)를 구성하려면 다음 단계를 수행합니다.

1. aaa **new-model** 명령을 사용하여 AAA를 활성화하고 스위치에서 802.1X를 전역적으로 활성화합니다.

2. RADIUS 서버를 구성하고 동적 권한 부여를 활성화합니다(권한 부여 변경 - CoA).

3. CDP 및 LLDP 프로토콜을 활성화합니다.

4. 스위치 포트 인증 구성 추가

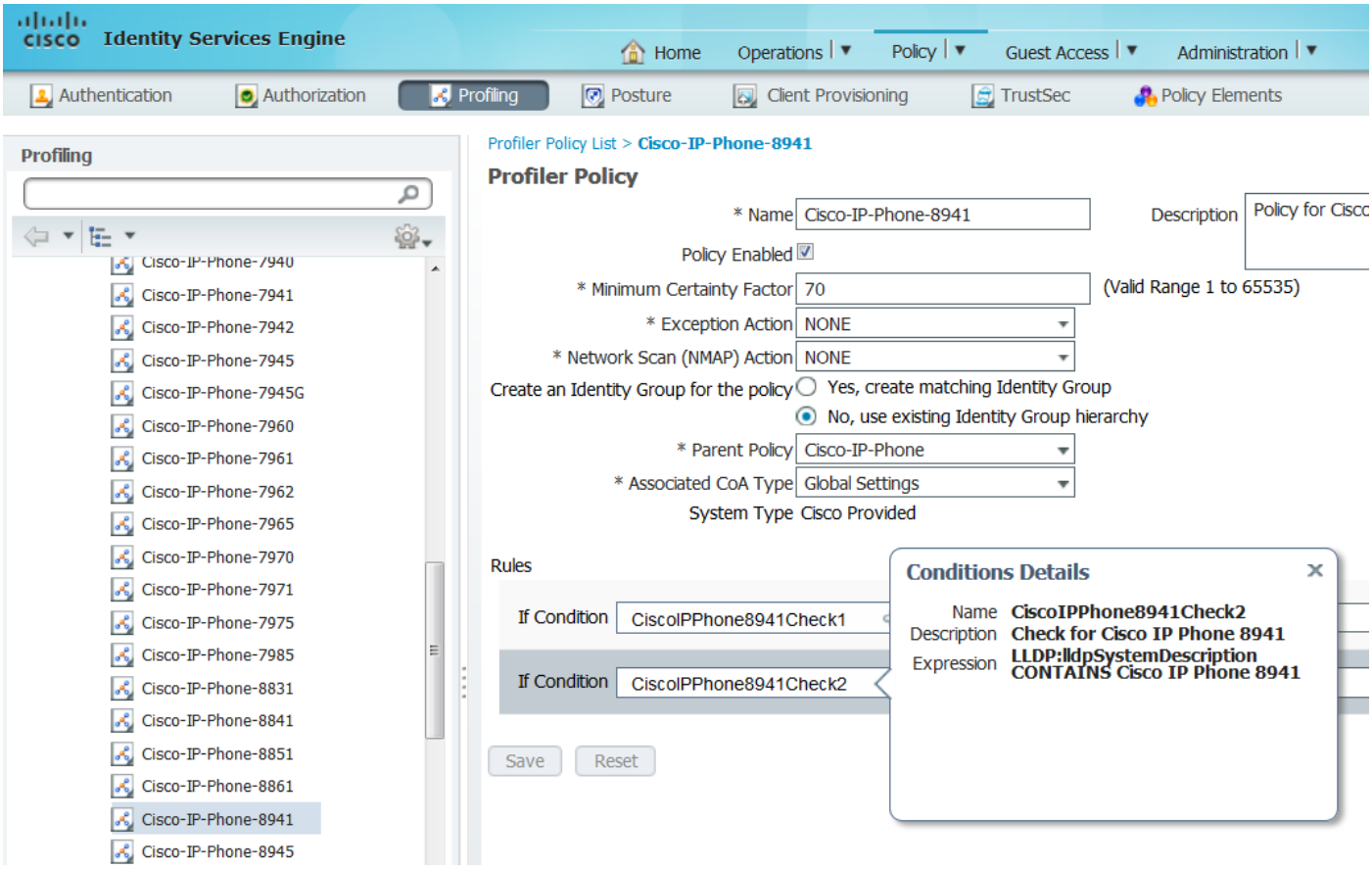
```
!
aaa new-model ! aaa authentication dot1x default group radius aaa authorization network default
group radius aaa accounting update newinfo aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
 client 1.1.1.1 server-key xyz
!
dot1x system-auth-control
! lldp run
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
!
```

> **최신 소프트웨어 버전 명령에서 radius-server vsa send accounting은 기본적으로 활성화되어 있습니다.어카운팅에서 전송된 속성이 표시되지 않으면 이 명령이 활성화되었는지 확인합니다.**

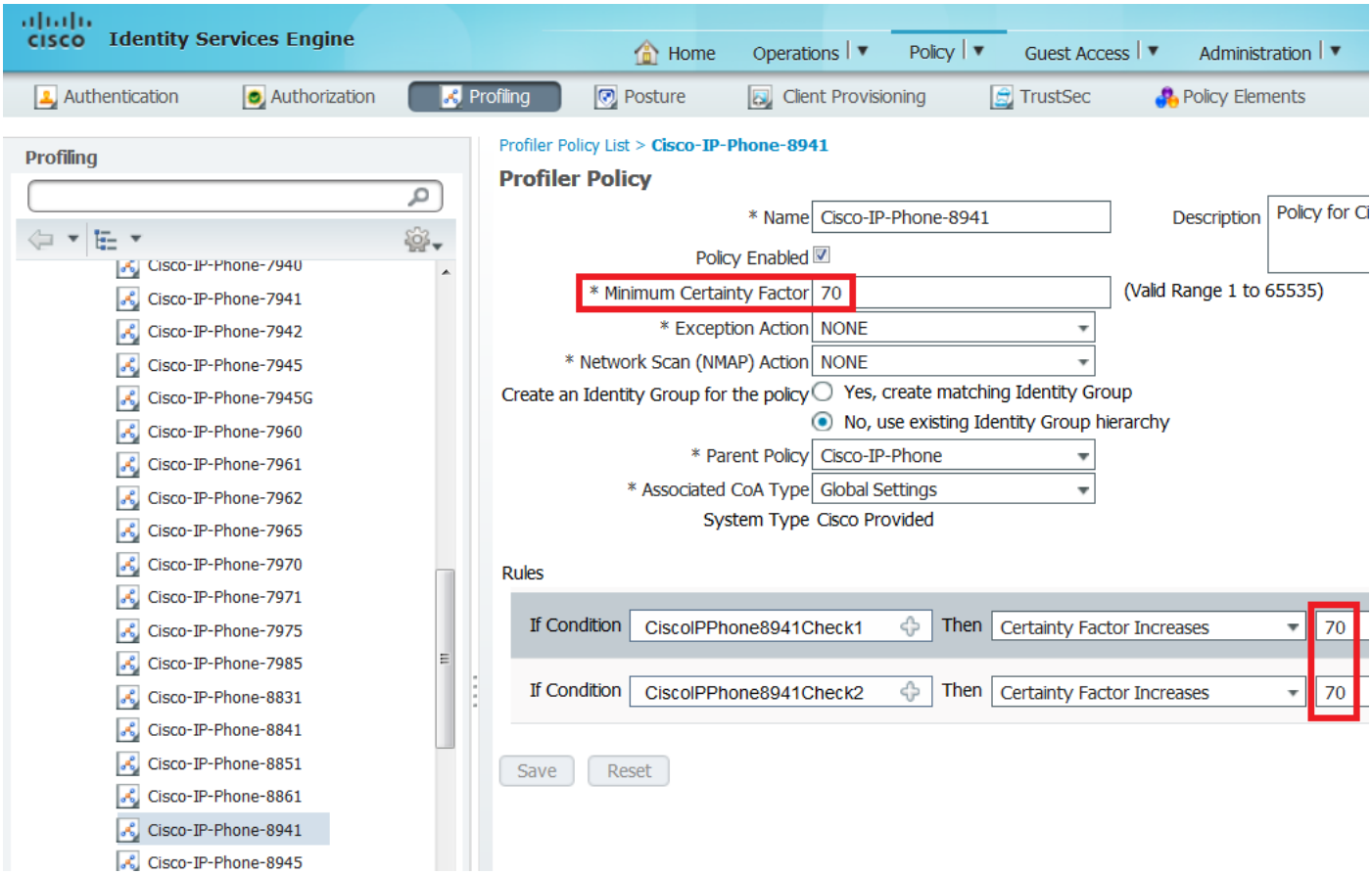
2단계. 장치 센서 구성

1. 디바이스를 프로파일링하는 데 필요한 CDP/LLDP의 특성을 확인합니다.Cisco IP Phone 8941의 경우 다음을 사용할 수 있습니다.

- LLDP SystemDescription 특성
- CDP CachePlatform 특성



Cisco-IP-Phone-8941로 프로파일링해야 하는 Certainty Factory가 70으로 증가되고 Minimum Certainty Factory가 70으로 증가되기 때문에 이 중 하나만 확보하면 됩니다.



특정 Cisco IP Phone으로 프로파일링하려면 모든 상위 프로필에 대한 최소 조건을 충족해야 합니다.이는 프로파일러가 Cisco-Device(최소)와 일치해야 함을 의미합니다.확실성 요인 10) 및 Cisco-IP-Phone(최소확실성 요인 20). 프로파일러가 이 두 프로파일과 일치하더라도 각 IP Phone 모델에 최소값이 있으므로 특정 Cisco IP Phone으로 프로파일링해야 합니다.확실성 계수 70. 디바이스는 확실성 요소가 가장 높은 프로파일에 할당됩니다.

2. CDP용 필터 목록과 LLDP용 필터 목록 두 개를 구성합니다.이는 Radius 어카운팅 메시지에 포함해야 할 특성을 나타냅니다.이 단계는 선택 사항입니다.

3. CDP 및 LLDP에 대한 두 가지 필터 사양을 생성합니다.필터 사양에서 속성 목록을 어카운팅 메시지에 포함하거나 제외하도록 지정할 수 있습니다.이 예에서는 다음 속성이 포함됩니다.

- CDP의 디바이스 이름
- LLDP의 시스템 설명

필요한 경우 RADIUS를 통해 ISE로 전송할 추가 특성을 구성할 수 있습니다.이 단계도 선택 사항입니다.

4. 명령 **장치 센서가 모든 변경 사항을 알립니다**.현재 세션에 대해 TLV를 추가, 수정 또는 제거할 때마다 업데이트가 트리거됩니다.

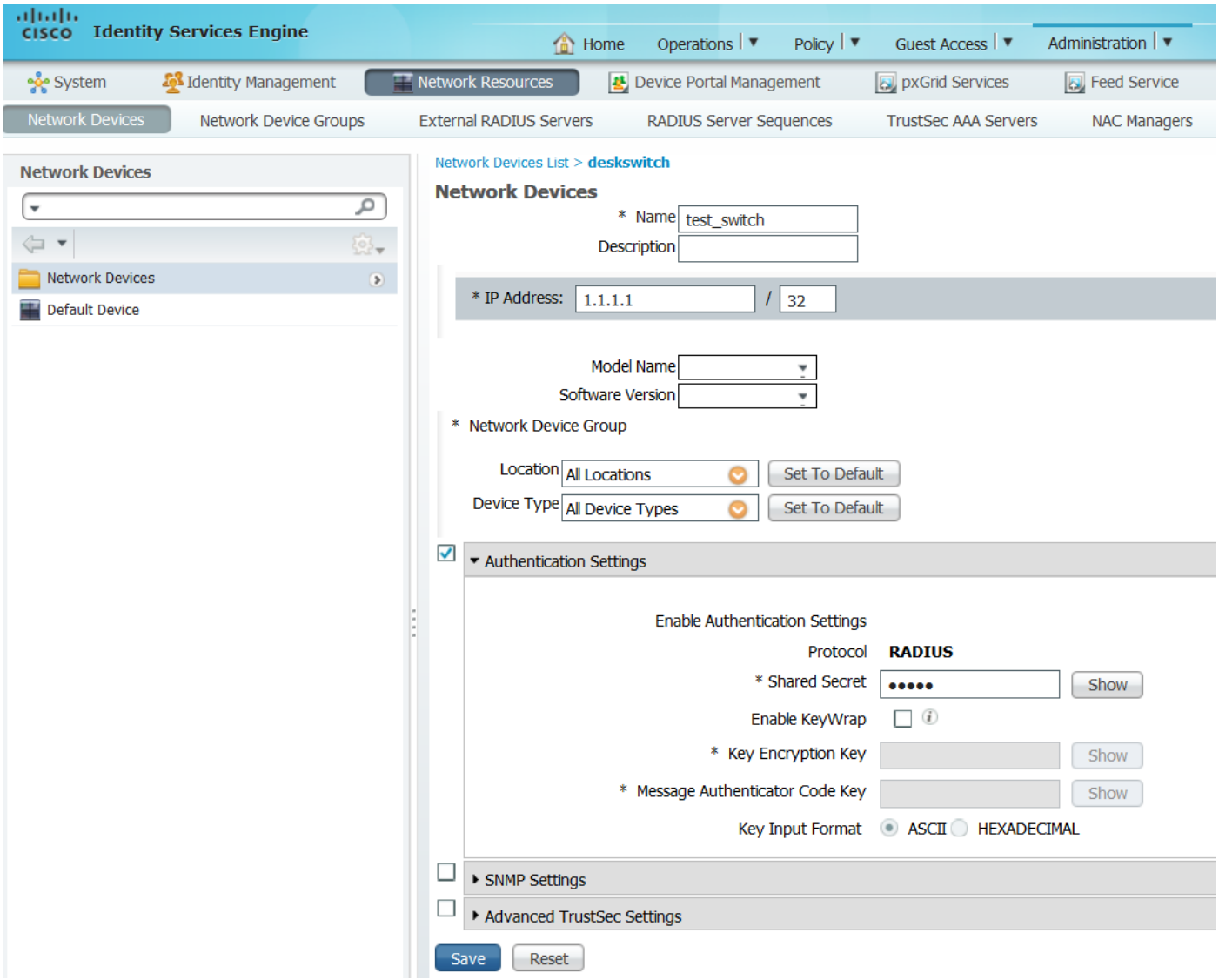
5. 장치 센서 기능을 통해 수집된 정보를 실제로 전송하려면 스위치에 명령 **장치 센서 계정 관리**를 사용하도록 명시적으로 알려야 합니다.

```
!
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-
```

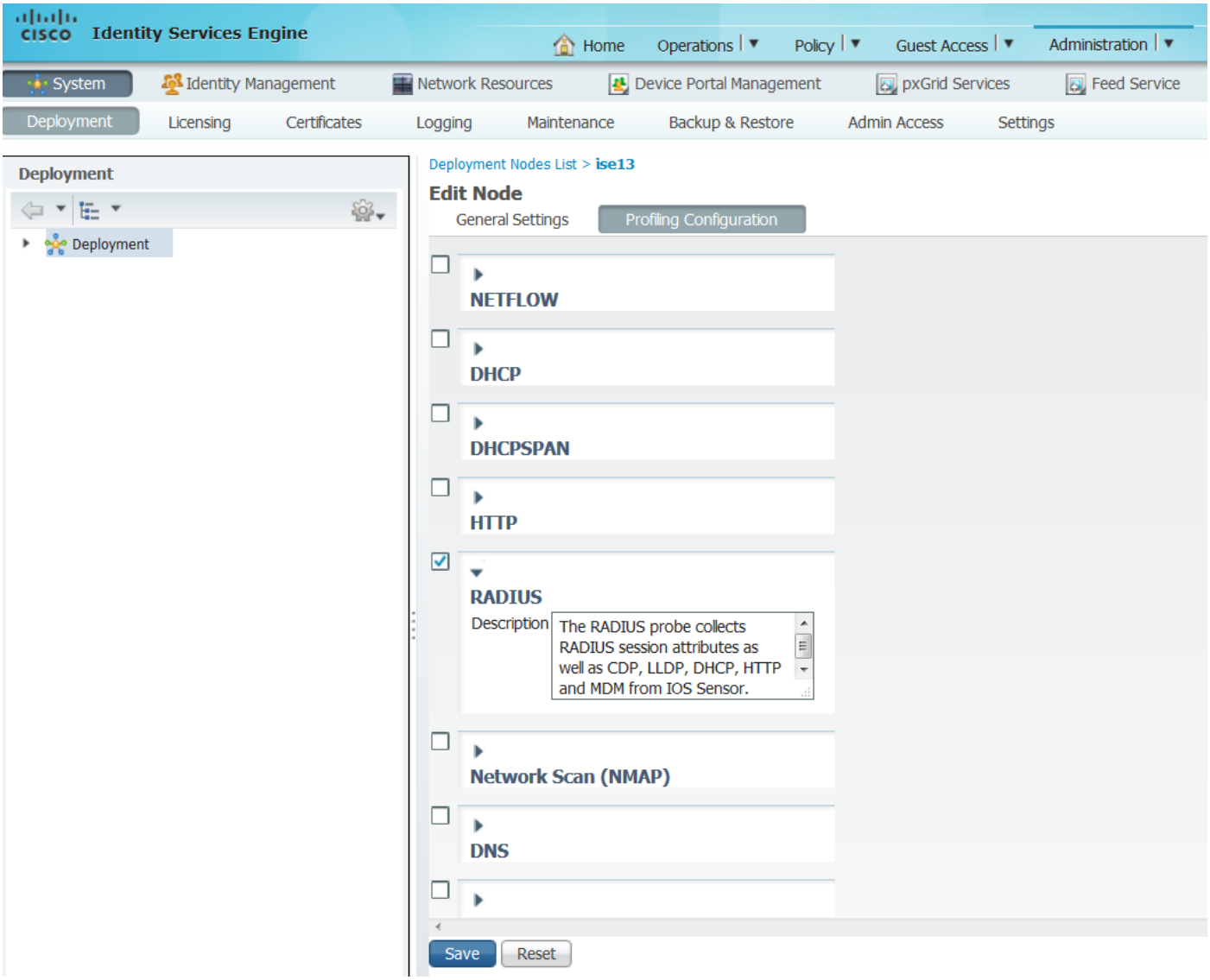
```
description ! device-sensor filter-spec lldp include list lldp-list device-sensor filter-spec
cdp include list cdp-list ! device-sensor accounting device-sensor notify all-changes !
```

3단계. ISE에서 프로파일링 구성

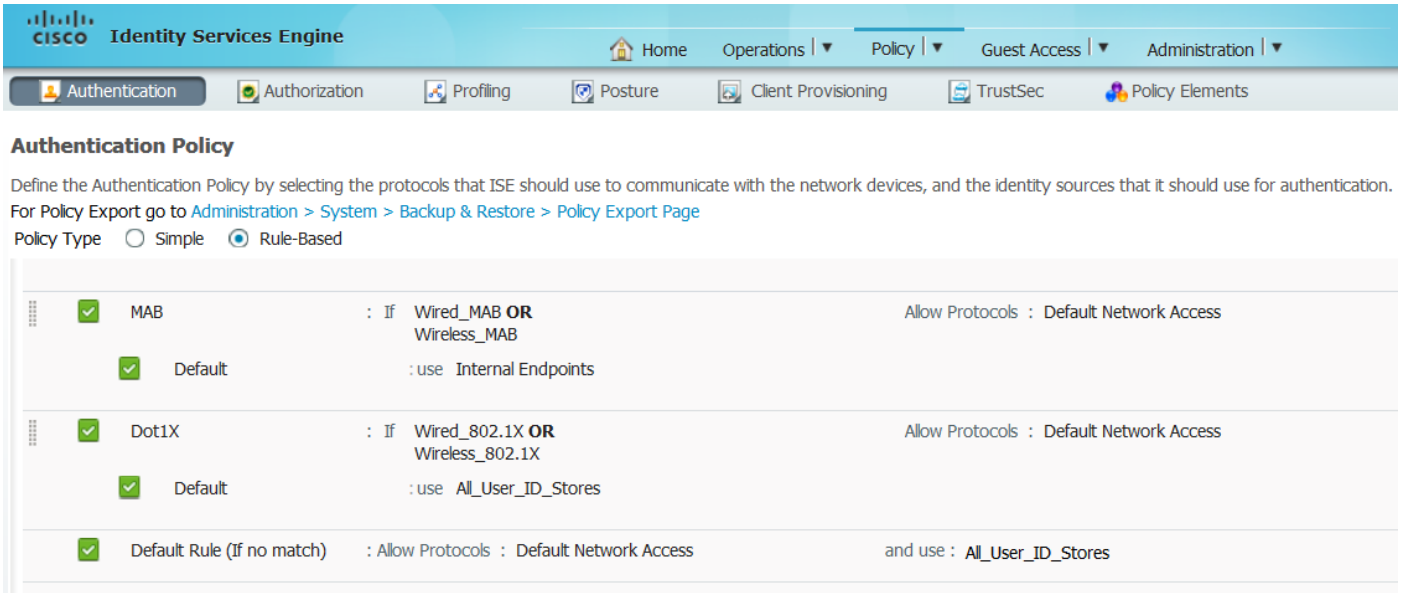
1. "관리>네트워크 리소스>네트워크 장치"에서 스위치를 네트워크 장치로 추가합니다. Authentication Settings(인증 설정)에서 스위치의 radius 서버 키를 공유 암호로 사용합니다.



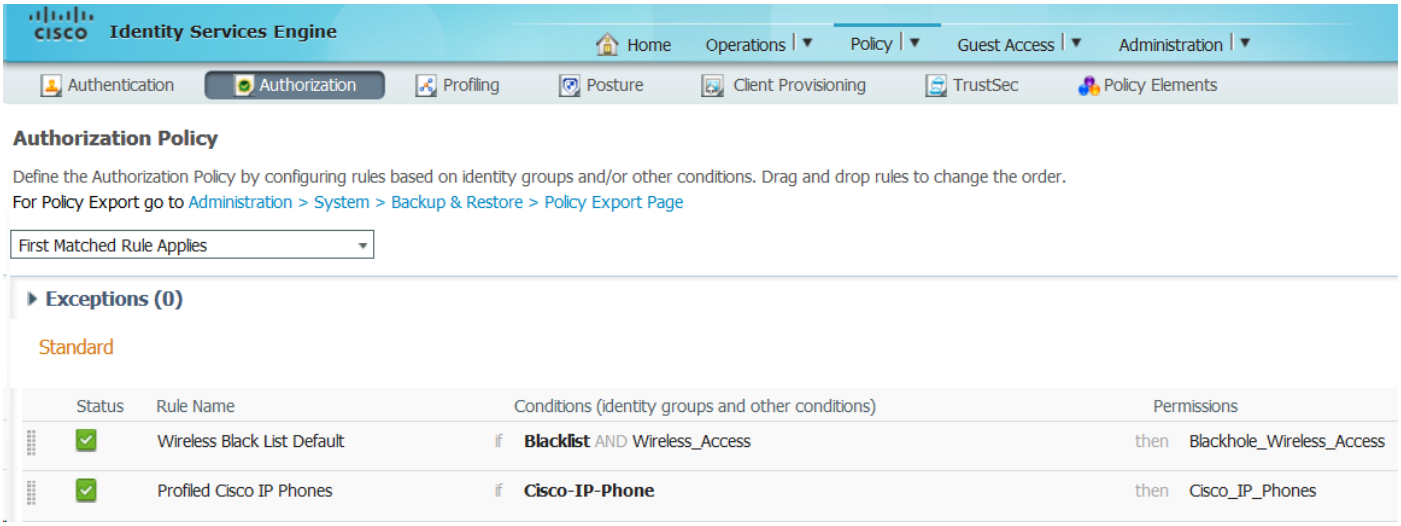
2. "Administration(관리)>System(시스템)>Deployment(구축)>ISE 노드>Profiling Configuration(프로파일링 컨피그레이션)"에서 프로파일링 노드에서 Radius 프로브를 활성화합니다. 모든 PSN 노드를 프로파일링에 사용해야 하는 경우 모든 노드에서 프로브를 활성화합니다.



3. ISE 인증 규칙을 구성합니다.이 예에서는 ISE에 미리 구성된 기본 인증 규칙이 사용됩니다.

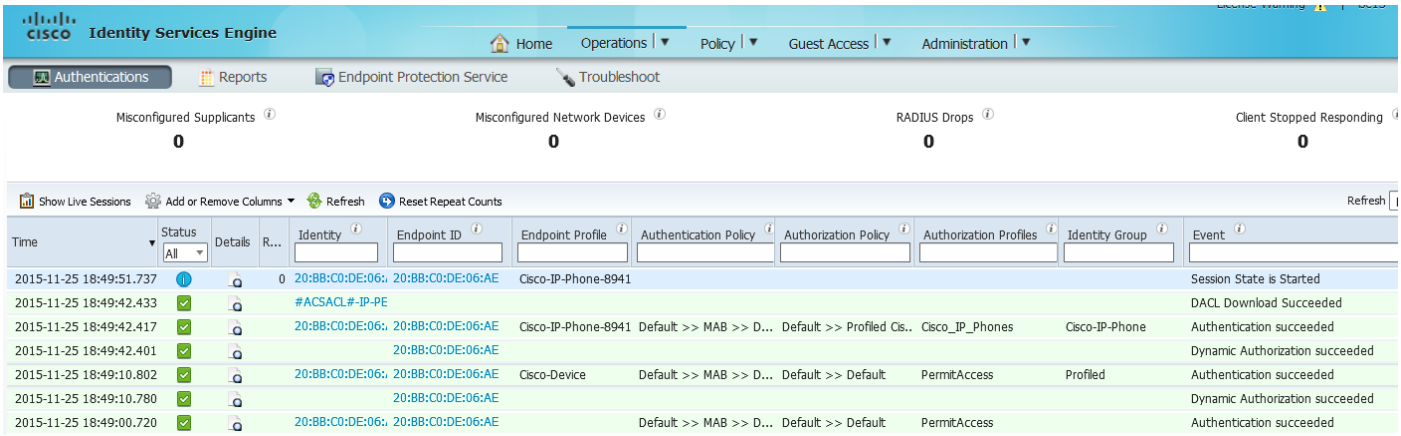


4. ISE 권한 부여 규칙을 구성합니다.'프로파일링된 Cisco IP Phones' 규칙이 사용되며 ISE에서 미리 구성됩니다.



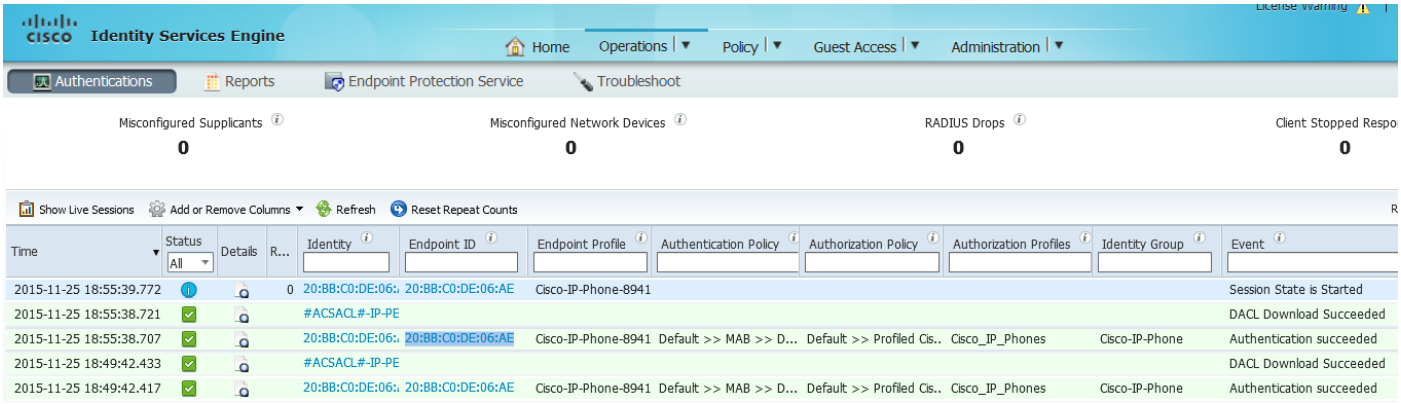
다음을 확인합니다.

프로파일링이 올바르게 작동하는지 확인하려면 ISE에서 "Operations>Authentications"를 참조하십시오.

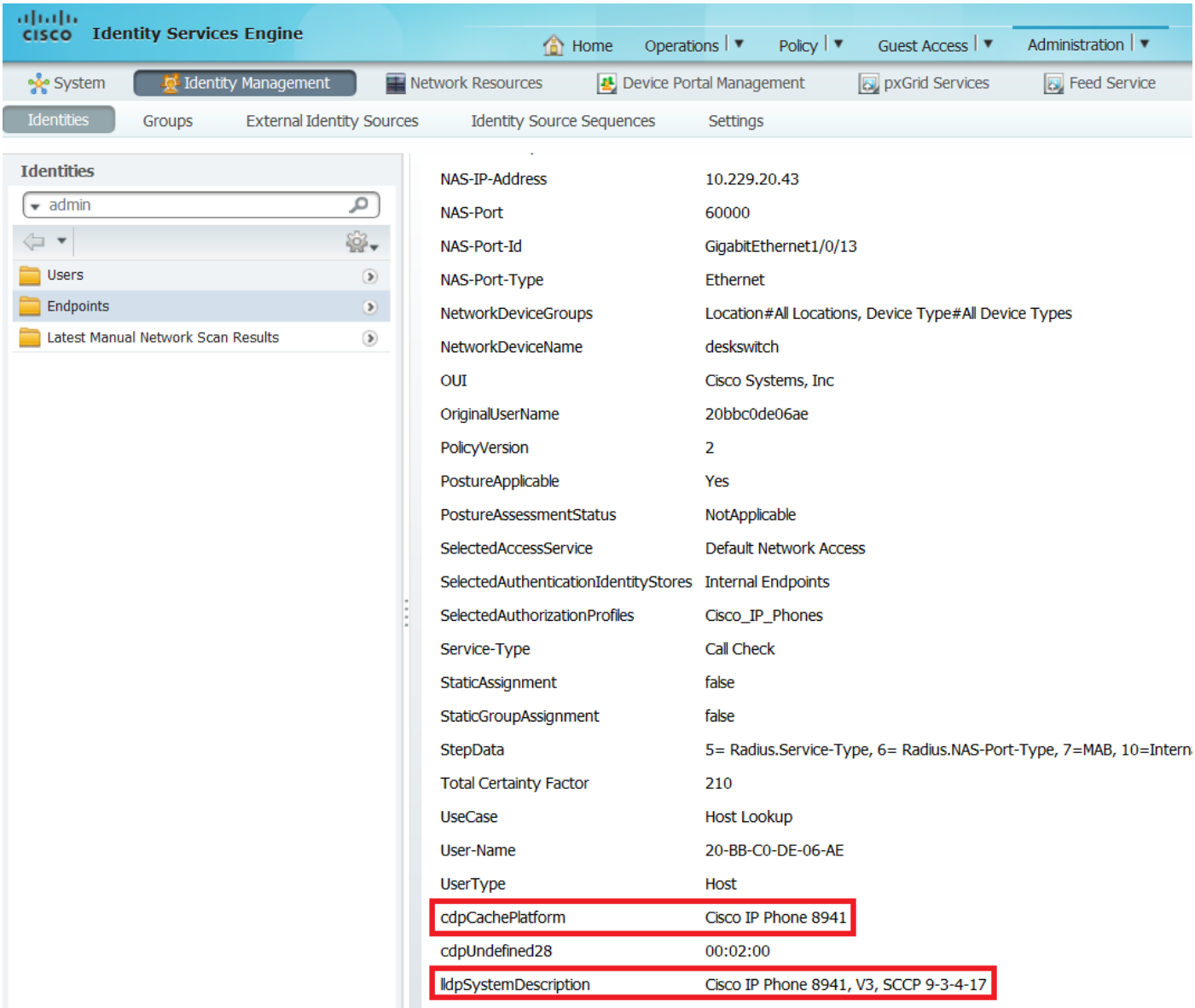


먼저 디바이스가 MAB(18:49:00)를 사용하여 인증되었습니다. 10초 후(18:49:10)는 Cisco-Device로 보고되었으며 첫 인증(18:49:42)이 Cisco-IP-Phone-8941 프로파일을 수신한 후 42초 후에 마지막으로 보고되었습니다.그 결과 ISE는 모든 트래픽을 허용하는 IP Phone(Cisco_IP_Phones) 및 다운로드 가능한 ACL에 대한 권한 부여 프로파일을 반환합니다(IP any 허용). 이 시나리오에서는 알 수 없는 디바이스가 네트워크에 대한 기본 액세스 권한을 갖습니다.ISE 내부 엔드포인트 데이터베이스에 MAC 주소를 추가하거나 이전에 알려지지 않은 디바이스에 대한 매우 기본적인 네트워크 액세스를 허용하여 이를 실현할 수 있습니다.

이 예에서는 초기 프로파일링이 약 40초 걸렸습니다.다음 인증 ISE에서는 ISE가 새/업데이트된 특성을 수신하고 디바이스를 다시 프로파일링해야 하는 경우를 제외하고, 프로파일 및 올바른 특성(음성 도메인 및 DACL에 조인할 수 있는 권한)이 즉시 적용된다는 사실을 이미 알고 있습니다.



"Administration(관리)>Identity Management(ID 관리)>Identities(ID)>Endpoints(엔드포인트)tested endpoint(테스트된 엔드포인트)"에서 Radius 프로브에 의해 수집되는 특성의 종류 및 해당 값이 무엇인지 확인할 수 있습니다.



이 시나리오에서 계산된 총 확실성 계수는 210입니다.엔드포인트가 Cisco-Device 프로필(총 확실성 요인 30 포함) 및 Cisco-IP-Phone 프로필(총 확실성 요인 40 포함)과 일치한다는 점을 알 수 있습니다. 프로파일러가 프로파일 Cisco-IP-Phone-8941의 두 조건을 일치하므로 이 프로파일의 확실성 요인은 140(프로파일링 정책에 따라 각 속성에 대해 70)입니다. 요약하려면30+40+70+70=210입니다.

문제 해결

1단계. CDP/LLDP에서 수집한 정보 확인

```
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: 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
```

수집된 데이터가 표시되지 않으면 다음을 확인하십시오.

- 스위치에서 인증 세션의 상태를 확인합니다(성공해야 함).

```
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:  0AE518200000020400 99C216
      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
```

- CDP 및 LLDP 프로토콜이 활성화되었는지 확인합니다.CDP/LLDP/등과 관련하여 기본이 아닌 명령이 있는지 확인합니다.엔드포인트에서 특성 검색에 미치는 영향

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

- CDP/LLDP/등을 지원하는 엔드포인트의 컨피그레이션 가이드에서 확인

2단계. 장치 센서 캐시 확인

```
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
```

이 필드에 데이터가 표시되지 않거나 정보가 완전하지 않은 경우, 특정 필터 목록 및 필터 사양에서 'device-sensor' 명령을 확인하십시오.

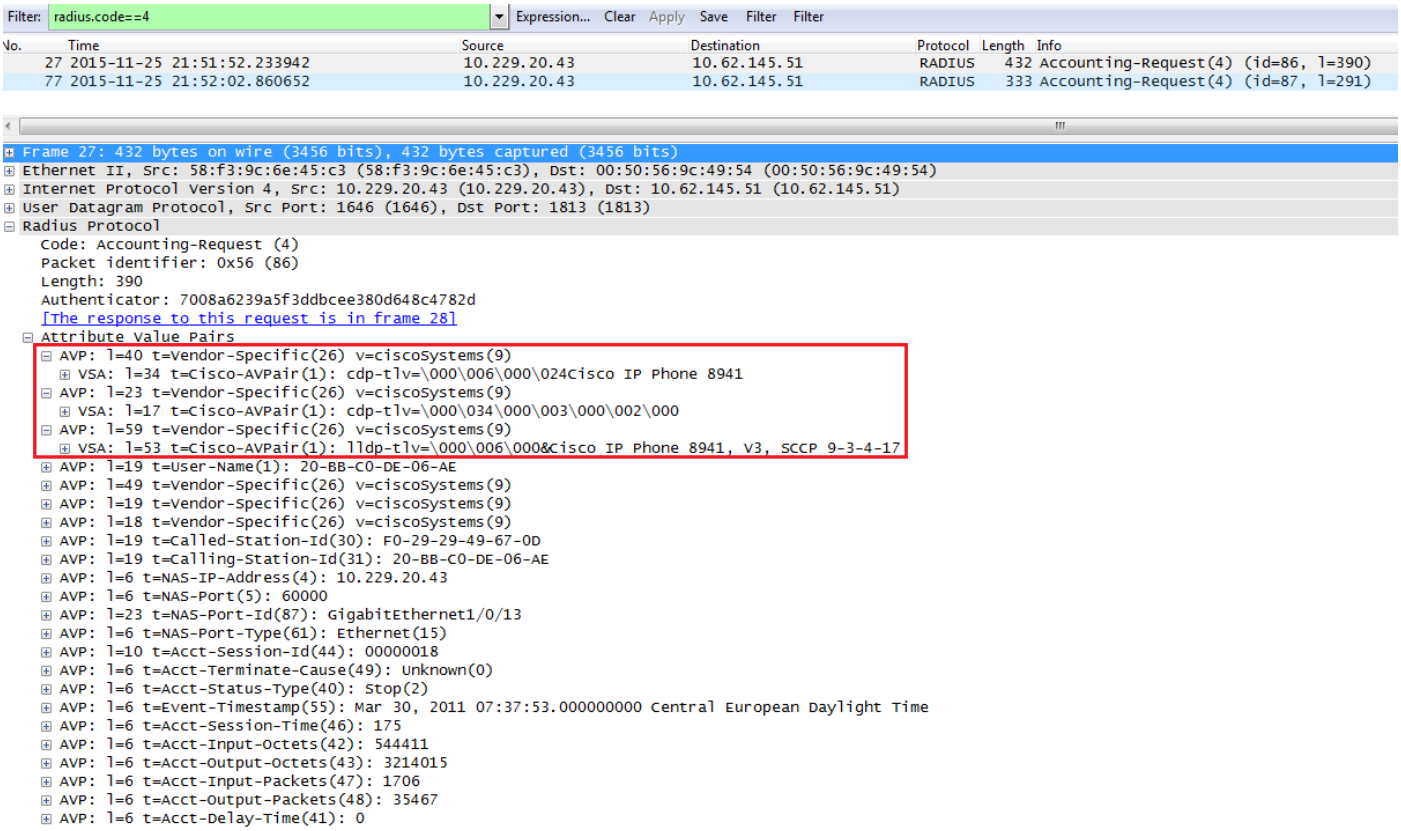
3단계. Radius 어카운팅에 특성이 있는지 확인

스위치에서 'debug radius' 명령을 사용하거나 스위치와 ISE 간에 패킷 캡처를 수행하는지 확인할 수 있습니다.

Radius 디버그:

```
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
```

패킷 캡처:



4단계. ISE에서 프로파일러 디버깅 확인

스위치에서 특성이 전송된 경우 ISE에서 수신되었는지 확인할 수 있습니다.이를 확인하려면 올바른 PSN 노드(Administration>System>Logging>Debug Log Configuration>PSN>profiler>debug)에 대해 프로파일러 디버그를 활성화하고 엔드포인트 인증을 한 번 더 수행합니다.

다음 정보를 찾습니다.

- RADIUS 프로브가 특성을 받았음을 나타내는 디버그:

```
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=0AE5182000000020400099C216, cisco-av-pair=vlan-id=101,
cisco-av-pair=method=mab, AcsSessionID=ise13/235487054/2511, SelectedAccessService=Default
Network Access,
Step=11004, Step=11017, Step=15049, Step=15008, Step=15004, Step=11005,
NetworkDeviceGroups=Location#All Locations,
NetworkDeviceGroups=Device Type#All Device Types, Service-Type=Call Check,
CPMSessionID=0AE5182000000020400099C216,
AllowedProtocolMatchedRule=MAB, Location=Location#All Locations, Device Type=Device Type#All
Device Types, ]
```

- 특성을 성공적으로 구문 분석했음을 나타내는 디버그:

```
2015-11-25 19:29:53,642 DEBUG  [RADIUSParser-1-thread-1][]
cisco.profiler.probes.radius.RadiusParser -:::- Parsed IOS Sensor 1: cdpCachePlatform=[Cisco
IP Phone 8941]
2015-11-25 19:29:53,642 DEBUG  [RADIUSParser-1-thread-1][]
cisco.profiler.probes.radius.RadiusParser -:::- Parsed IOS Sensor 2:
cdpUndefined28=[00:02:00]
2015-11-25 19:29:53,642 DEBUG  [RADIUSParser-1-thread-1][]
cisco.profiler.probes.radius.RadiusParser -:::- Parsed IOS Sensor 3:
lldpSystemDescription=[Cisco IP Phone 8941, V3, SCCP
```

- 전달자가 특성을 처리함을 나타내는 디버그:

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

전달자는 Cisco ISE 데이터베이스에 해당 특성 데이터와 함께 엔드포인트를 저장하고 네트워크에서 탐지된 새 엔드포인트를 분석기에 알립니다.분석기는 엔드포인트를 엔드포인트 ID 그룹에 분류하고 데이터베이스에 일치하는 프로파일이 있는 엔드포인트를 저장합니다.

5단계. 일반적으로 특정 장치에 대한 기존 컬렉션에 새 특성을 추가한 후 이 장치/끝점이 새 특성에 따라 다른 프로필을 할당해야 하는지 확인하기 위해 프로파일링 큐에 추가됩니다.

```
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 ExceptionRuleMatched:false
```

관련 정보

1.http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/howto_30_ise_profiling.pdf

2 .http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html