Contenido

Introducción

Este documento describe cómo configurar el sensor del dispositivo, para poderlo utilizar para perfilar los propósitos en el ISE. El sensor del dispositivo es una característica de los dispositivos de acceso. Permite recoger la información sobre los puntos finales conectados. Sobre todo, la información recopilada por el sensor del dispositivo puede venir de los protocolos siguientes:

- Cisco Discovery Protocol (CDP)
- Discovery Protocol de la capa de link (LLDP)
- Dynamic Host Configuration Protocol (DHCP, Protocolo de configuración dinámica de hosts)

En algunas Plataformas es posible utilizar también el H323, el SORBO (Session Initiation Protocol), MDNS (resolución del dominio del Multicast) o los protocolos HTTP. Las posibilidades de configuración para las capacidades del sensor del dispositivo pueden variar del protocolo al protocolo. Como un ejemplo sobre está disponible en el Cisco Catalyst 3850 con el software 03.07.02.E.

Una vez que se recoge la información, puede ser encapsulada en las estadísticas del radio y enviar a un servidor de perfilado. En esta identidad del artículo mantenga el motor (ISE) se utiliza como servidor de perfilado.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Protocolo RADIUS
- CDP, LLDP y protocolos DHCP
- Motor del servicio de la identidad de Cisco
- Switch 2960 del Cisco Catalyst

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Corrección 3 de la versión 1.3 del motor del servicio de la identidad de Cisco
- Versión 15.2(2a)E1 del Switch 2960s del Cisco Catalyst
- SCCP 9-3-4-17 de la versión del Cisco IP Phone 8941

Configurar

Paso 1. Configuración AAA estándar

Para configurar la autenticación, la autorización y las estadísticas (AAA), siguen los pasos abajo:

1. Habilite el AAA usando el **comando aaa new-model** y habilite el 802.1x global en el Switch

2. Configure al servidor de RADIUS y habilite la autorización dinámica (cambio de la autorización - el CoA)

3. Habilite los protocolos CDP y LLDP

4. Agregue la configuración de autenticación del switchport

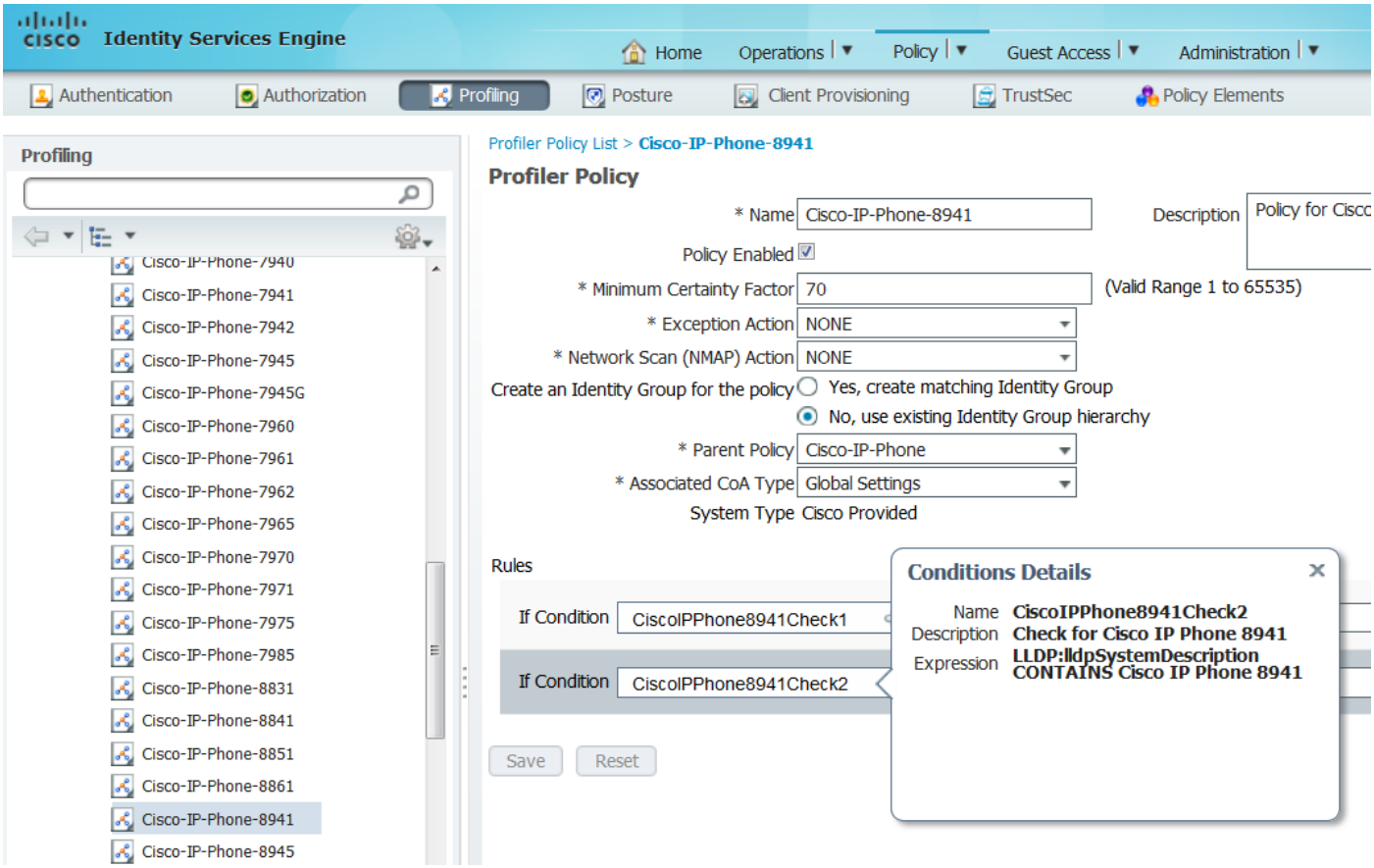
```
!
aaa new-model!aaa authentication dot1x default group radiusaaa authorization network default
group radiusaaa accounting update newinfoaaa accounting dot1x default start-stop group radius!
aaa server radius dynamic-author
 client 1.1.1.1 server-key xyz
!
dot1x system-auth-control
!lldp run
cdp run!interface 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 portfastend!radius-server host 1.1.1.1 auth-port 1812 acct-port 1813 key xyz
!
```

> En un más nuevo comando radius-server vsa send de la versión de software las **estadísticas** se habilitan por abandono. Si usted no puede ver los atributos enviar en las estadísticas, verifique si el comando en habilitado.

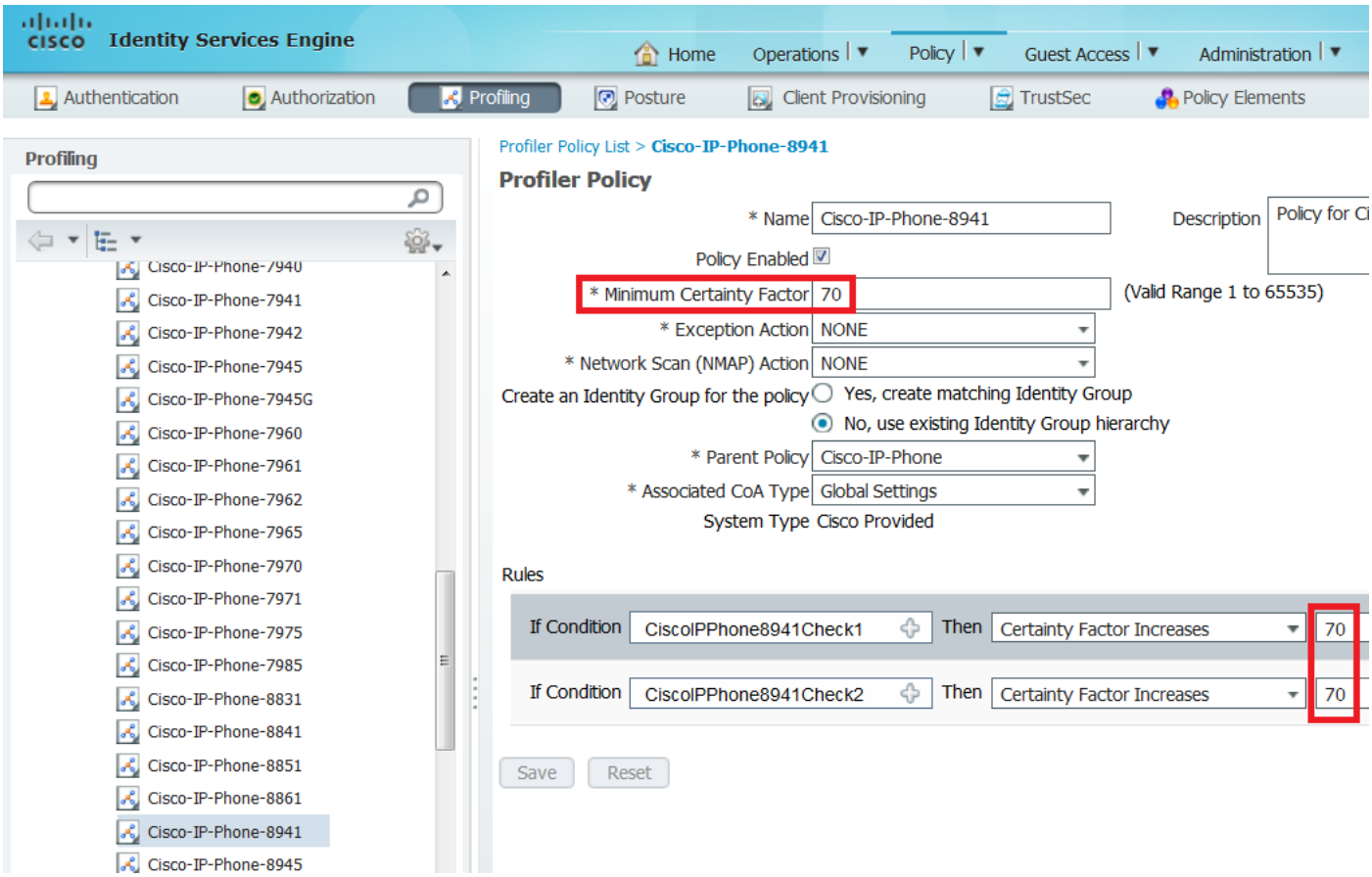
Paso 2. Sensor del dispositivo de la configuración

1. Determine que los atributos de CDP/LLDP son necesarios perfilar el dispositivo. En caso del Cisco IP Phone 8941 usted puede utilizar el siguiente:

- Atributo LLDP SystemDescription
- Atributo CDP CachePlatform



Para nuestro propósito sería bastante para obtener apenas uno de ésos puesto que ambos ellos proporcionan el aumento de la fábrica de la certeza de 70 y la fábrica mínima de la certeza requerida para ser perfilado como Cisco-IP-Phone-8941 es 70:



Para ser perfilado como Cisco IP Phone específico, youneed para satisfacer las condiciones mínimas para todos los perfiles del padre. Esto significa que el profiler necesita hacer juego el dispositivo de Cisco (factor mínimo de la certeza 10) y el Cisco IP Phone (factor mínimo 20 de la certeza). Aunque el profiler hace juego esos dos perfiles, debe todavía ser perfilado como Cisco IP Phone específico puesto que cada modelo del teléfono del IP tiene factor mínimo de la certeza de 70. El dispositivo se asigna al perfil para el cual tiene factor más alto de la certeza.

2. Configure dos listas de filtros - una para el CDP y otro para LLDP. Ésos indican que cuáles atribuyen debe ser incluido en los mensajes de las estadísticas del radio. Este paso es opcional

3. Cree dos filtro-SPEC para el CDP y LLDP. En espec. del fiter usted puede cualquiera indicar que la lista de atributos debe ser incluida o excluida de los mensajes de las estadísticas. En el ejemplo los atributos de siguiente son incluidos:

- Nombre del dispositivo del CDP
- Descripción del sistema de LLDP

Usted puede configurar los atributos adicionales que se transmited vía el radio al ISE si es necesario. Este paso es también opcional.

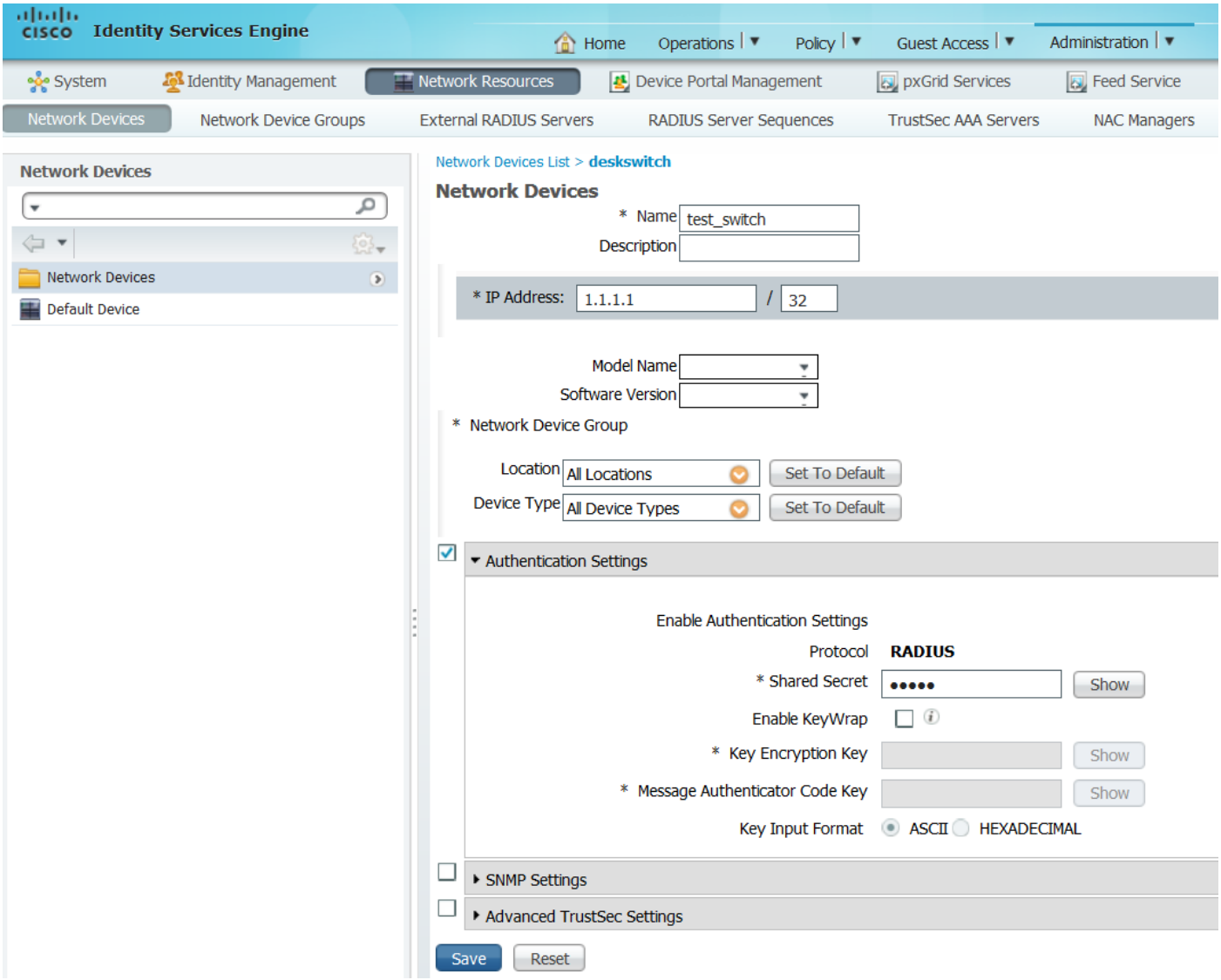
4. **El dispositivo-sensor del** comando Add **notifica los todo-cambios**. Acciona las actualizaciones siempre que los TLV se agreguen, se modifiquen o se quiten para la sesión en curso

5. Para enviar realmente la información recopilada vía la funcionalidad del sensor del dispositivo, usted necesita decir explícitamente el Switch hacer tan con las **estadísticas del dispositivo-sensor del** comando

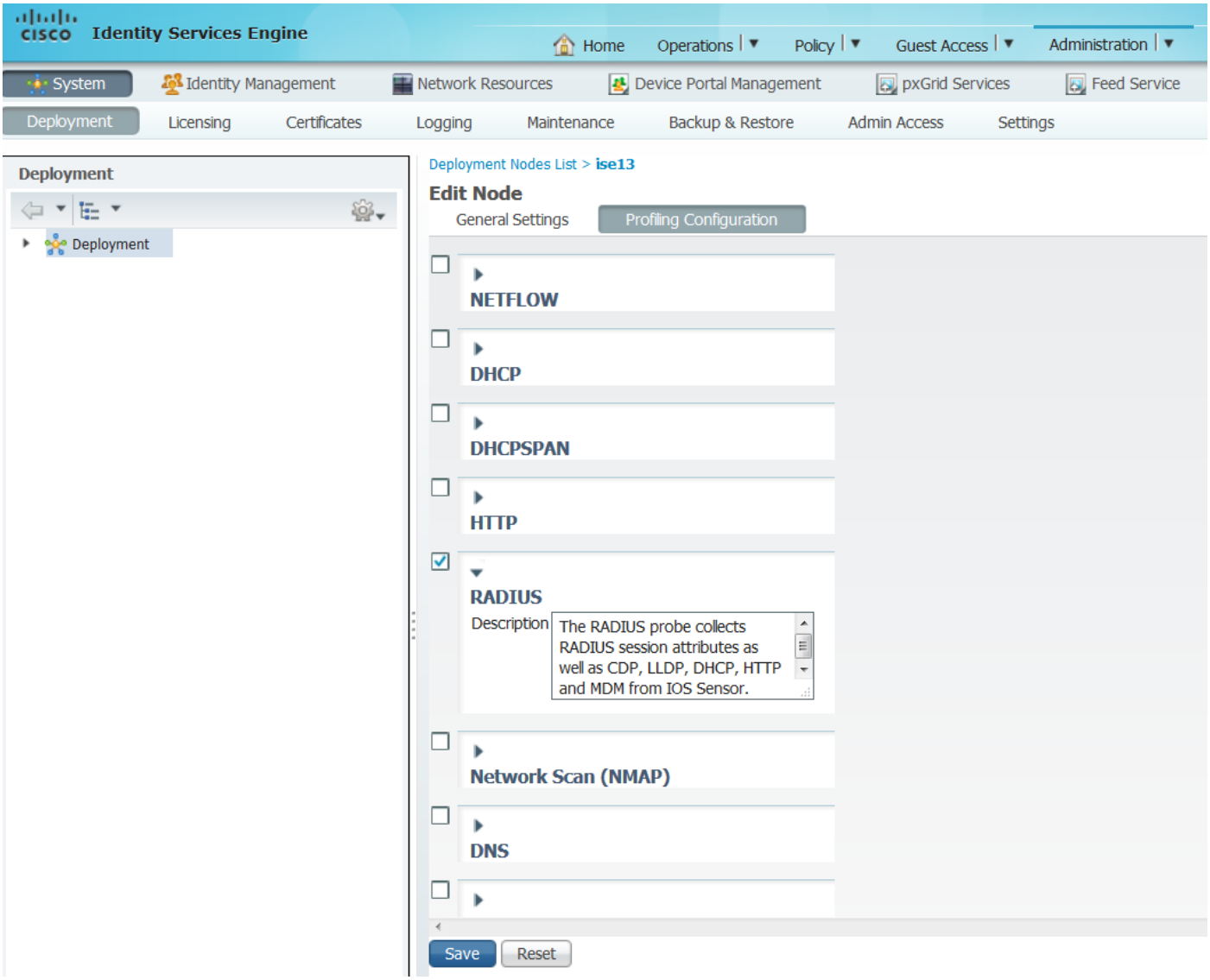
```
!device-sensor filter-list cdp list cdp-list tlv name device-name
 tlv name platform-type!device-sensor filter-list lldp list lldp-list tlv name system-
description!device-sensor filter-spec lldp include list lldp-listdevice-sensor filter-spec cdp
include list cdp-list!device-sensor accountingdevice-sensor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

Paso 3. Configuración que perfila en el ISE

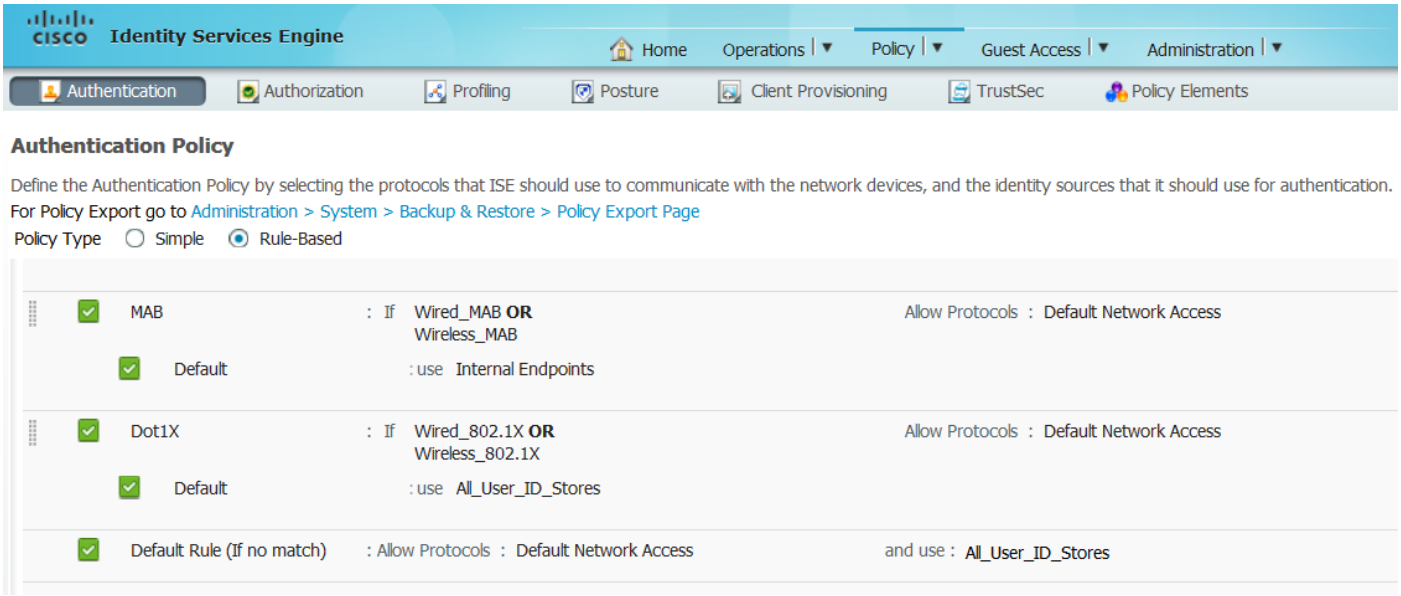
1. Agregue el Switch como dispositivo de red en los “dispositivos de Administration>Network Resources>Network”. Utilice la clave del servidor de RADIUS del Switch como secreto compartido en las configuraciones de la autenticación:



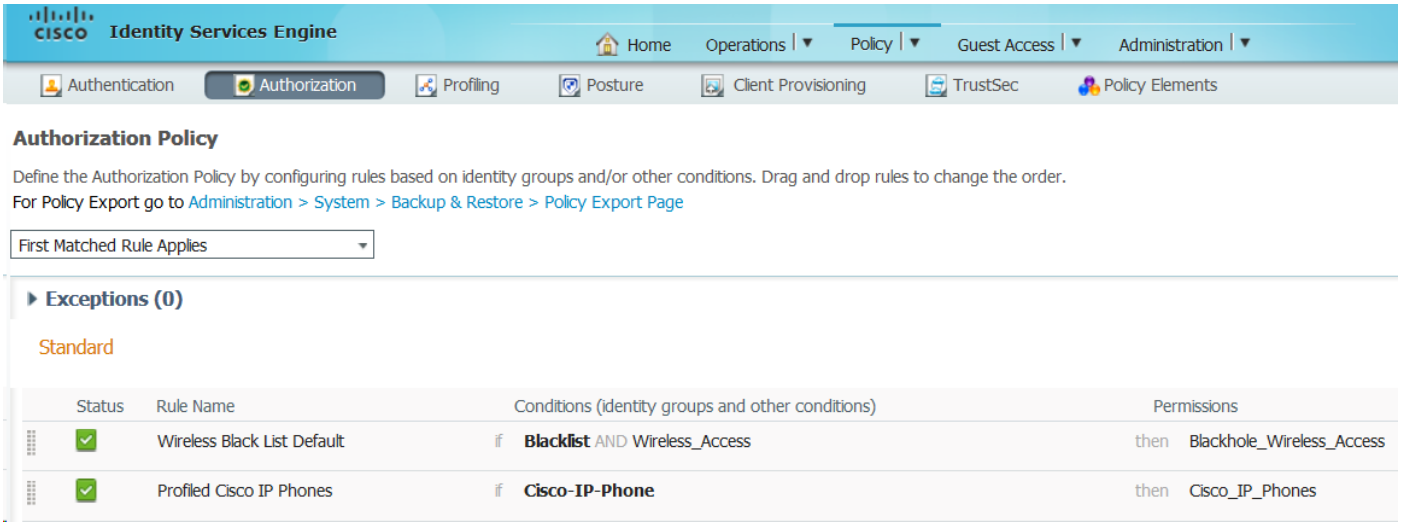
2. Habilite la sonda del radio en el nodo de perfilado en la “configuración node>Profiling de Administration>System>Deployment>ISE”. Si todos los Nodos PSN se utilizan para perfilar, habilite la sonda en todos:



3. Configure las reglas de la autenticación ISE. En el ejemplo las reglas de la autenticación predeterminada preconfiguradas en el ISE se utilizan:

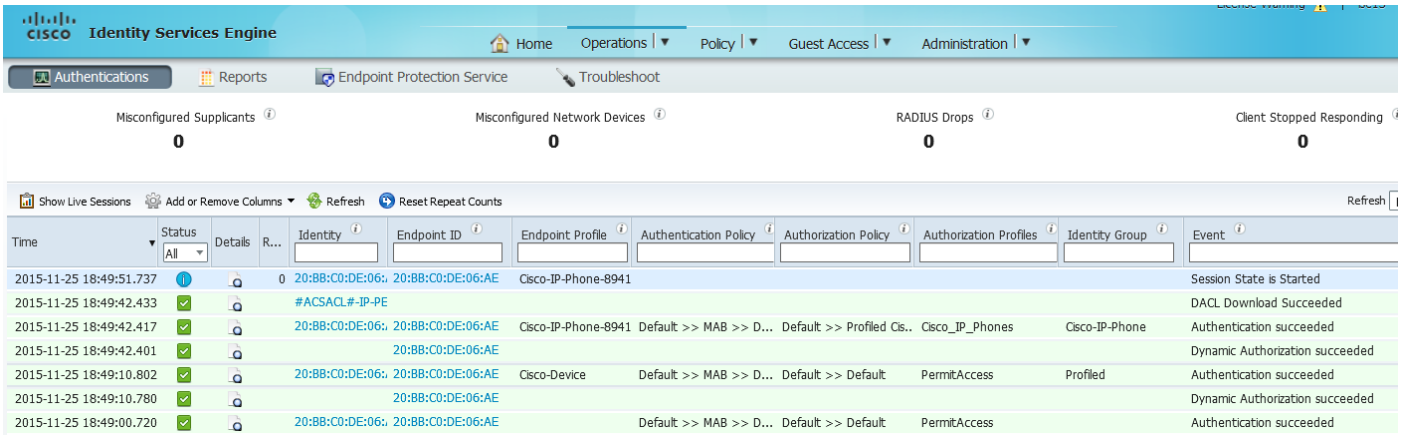


4. Reglas de la autorización de la configuración ISE. “Se utiliza la regla de los teléfonos del IP perfilados de Cisco, que se preconfigura en el ISE:



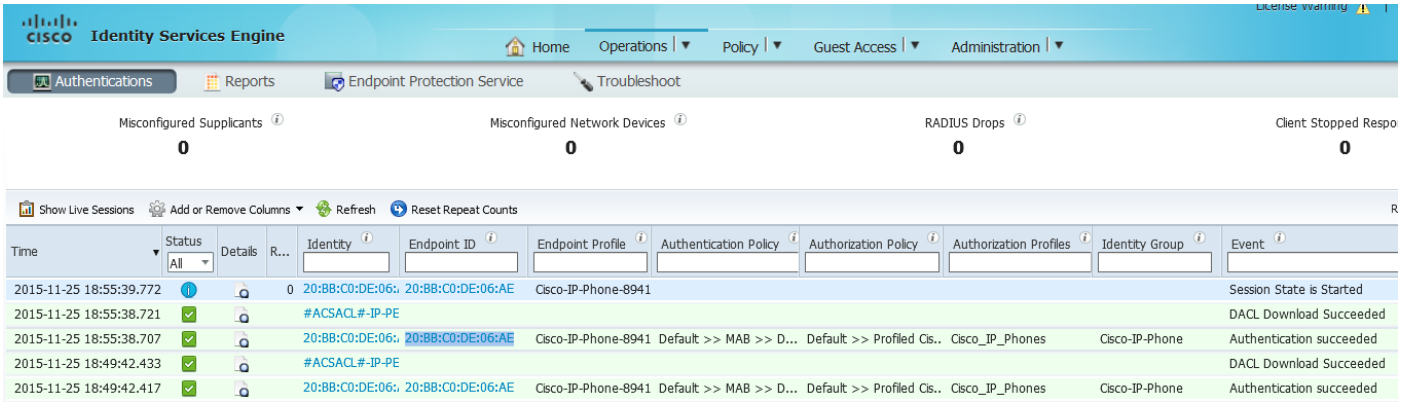
Verificación

Para verificar si el perfilado está trabajando correctamente, refiera por favor a "Operations>Authentications" en el ISE:

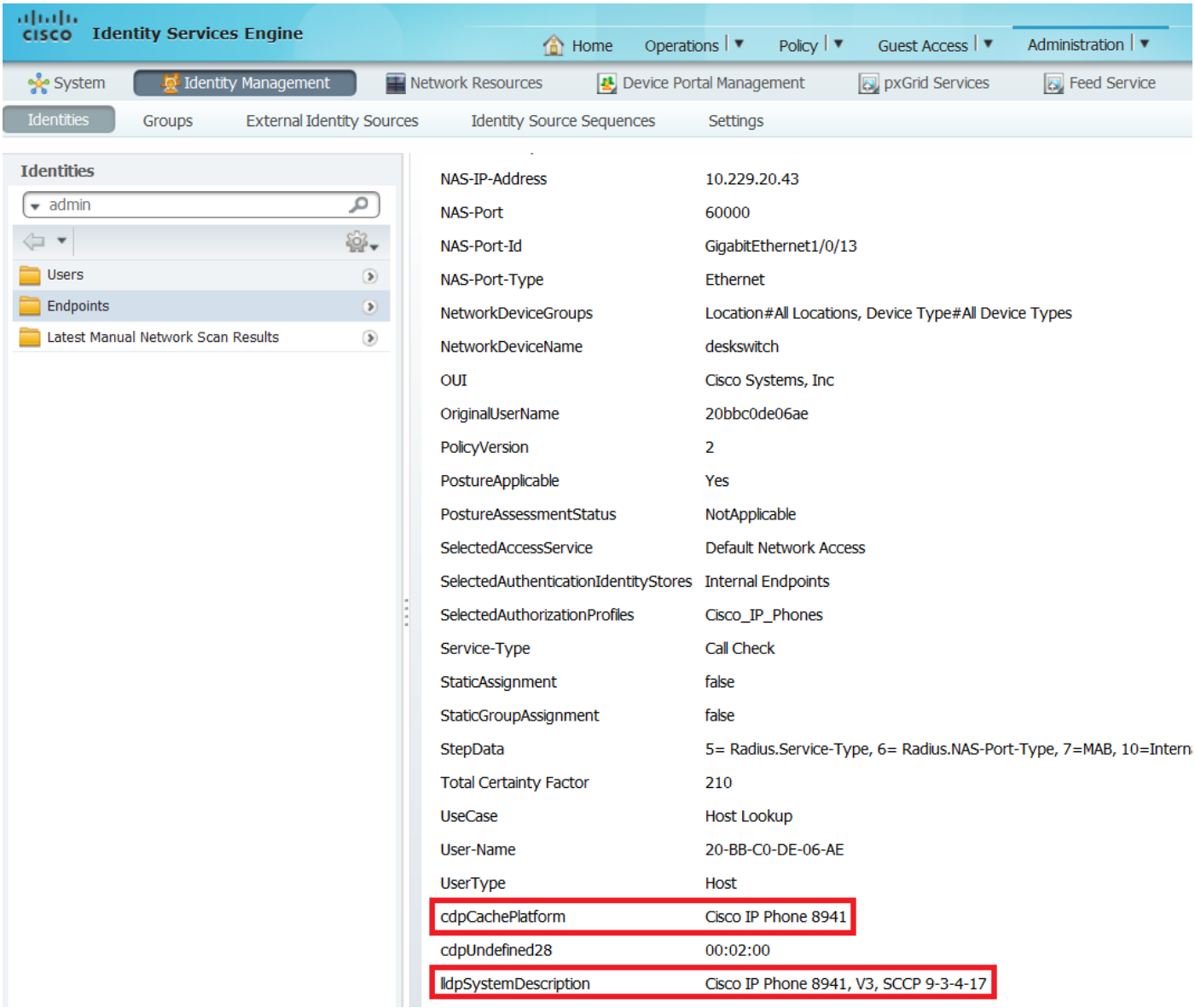


Primero el dispositivo fue autenticado usando MAB (18:49:00). Diez segundos después (18:49:10) reprofiled como dispositivo de Cisco y finalmente después de 42 segundos puesto que las primeras autenticaciones (18:49:42) él recibieron el perfil Cisco-IP-Phone-8941. Como consecuencia el ISE vuelve el específico del perfil de la autorización para los Teléfonos IP (Cisco_IP_Phones) y ACL descargable ese permite todo el tráfico (IP del permiso cualquier). Observe por favor que en este escenario el dispositivo desconocido tiene acceso básico a la red. Puede ser alcanzado agregando el MAC address a la base de datos interna del punto final ISE o permitiendo mismo el acceso de red básica para previamente los dispositivos desconocidos.

El perfilado inicial tardó alrededor 40 segundos en este ejemplo. En la autenticación siguiente ISE conoce el perfil y corrige ya los atributos (permiso para unirse al dominio de la Voz y DACL) se aplican inmediatamente, a menos que el ISE reciba los nuevos/actualizados atributos y necesita reprofile el dispositivo otra vez.



En el “punto final de Administration>Identity Management>Identities>Endpoints>tested” usted puede ver qué clase de atributos fueron recogidos por la sonda del radio y cuáles son sus valores:



Como usted puede observar el factor total de la certeza computado es 210 en este escenario. Viene fromt el hecho de que el punto final correspondió con también el perfil del dispositivo de Cisco (con el factor total de la certeza de 30) y el perfil del Cisco IP Phone (con el factor total de la certeza de 40). Puesto que el profiler correspondió con ambas condiciones en el perfil Cisco-IP-Phone-8941, el factor de la certeza para este perfil es 140 (70 para cada atributo según el perfilado de la directiva). Para resumir: 30+40+70+70=210.

Troubleshooting

Paso 1. Verifique la información recopilada por CDP/LLDP

```
switch#sh cdp neighbors g1/0/13 detail------------------------Device ID: SEP20BBC0DE06AEEntry
address(es):Platform: Cisco IP Phone 8941 ,  Capabilities: Host Phone Two-port Mac
RelayInterface: GigabitEthernet1/0/13,  Port ID (outgoing port): Port 1Holdtime : 178 secSecond
Port Status: DownVersion :SCCP 9-3-4-17advertisement version: 2Duplex: fullPower drawn: 3.840
WattsPower request id: 57010, Power management id: 3Power request levels are:3840 0 0 0 0Total
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
```

Si usted no puede ver ningunos datos recogidos para verificar el siguiente:

- Marque el estado de la sesión de la autenticación sobre el Switch (debe ser acertado):

```
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_Gi1/0/13Local Policies:        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
(priority 150)Server Policies:Method status list:       Method           State       dot1x
Stopped       mab             Authc Success
```

- Marque si se habilitan los protocolos CDP y LLDP. Marque si hay algunos comandos no valor por defecto con respecto a CDP/LLDP/etc. y cómo ésos pueden afectar a la extracción del atributo del punto final

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

- Verifique en la guía de configuración para su punto final si soporta CDP/LLDP/etc

Paso 2. Caché del sensor del dispositivo del control

```
switch#show device-sensor cache interface g1/0/13Device: 20bb.c0de.06ae on port
GigabitEthernet1/0/13-------------------------------------------------Proto Type:Name
Len ValueLLDP     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 37CDP      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 20CDP
28:secondport-status-type       7 00 1C 00 07 00 02 00
```

Si usted no ve ningunos datos en este campo o información no son completos verifican los comandos del “dispositivo-sensor”, particularmente las listas de filtros y los filtro-SPEC.

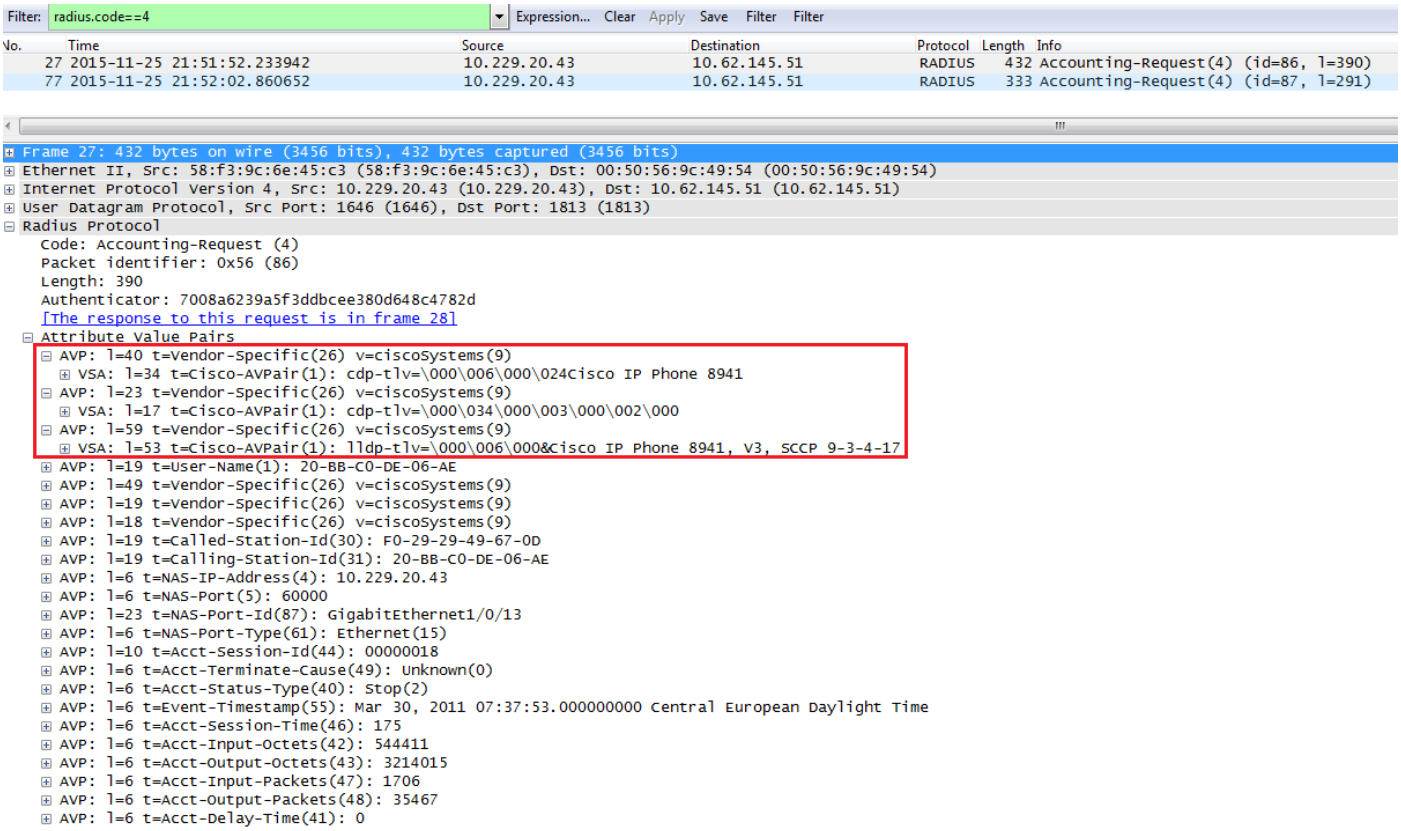
Paso 3. Marque si los atributos están presentes en las estadísticas del radio

Usted puede verificar eso usando “el comando del radio del debug” en el Switch o captura de paquetes de la ejecución entre el Switch y el ISE.

Debug del radio:

```
Mar 30 05:34:58.716: RADIUS(00000000): Send Accounting-Request to 1.1.1.1:1813 id 1646/85, len
378Mar 30 05:34:58.716: RADIUS:  authenticator 17 DA 12 8B 17 96 E2 0F - 5D 3D EC 79 3C ED 69
20Mar 30 05:34:58.716: RADIUS:  Vendor, Cisco       [26]  40Mar 30 05:34:58.716: RADIUS:   Cisco
AVpair       [1]   34   "cdp-tlv= "Mar 30 05:34:58.716: RADIUS: Vendor, Cisco [26] 23Mar 30
05:34:58.716: RADIUS: Cisco AVpair [1] 17 "cdp-tlv= "Mar 30 05:34:58.721: RADIUS: Vendor, Cisco
[26] 59Mar 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] 49Mar 30
05:34:58.721: RADIUS: Cisco AVpair [1] 43 "audit-session-id=0AE518200000022800E2481C"Mar 30
05:34:58.721: RADIUS: Vendor, Cisco [26] 19Mar 30 05:34:58.721: RADIUS: Cisco AVpair [1] 13
"vlan-id=101"Mar 30 05:34:58.721: RADIUS: Vendor, Cisco [26] 18Mar 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 10.229.20.43Mar 30 05:34:58.721: RADIUS: NAS-Port [5]
6 60000Mar 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 1301463298Mar 30 05:34:58.721: RADIUS:
Acct-Input-Octets [42] 6 538044Mar 30 05:34:58.721: RADIUS: Acct-Output-Octets [43] 6 3201914Mar
30 05:34:58.721: RADIUS: Acct-Input-Packets [47] 6 1686Mar 30 05:34:58.721: RADIUS: Acct-Output-
Packets [48] 6 35354Mar 30 05:34:58.721: RADIUS: Acct-Delay-Time [41] 6 0Mar 30 05:34:58.721:
RADIUS(00000000): Sending a IPv4 Radius PacketMar 30 05:34:58.721: RADIUS(00000000): Started 5
sec timeoutMar 30 05:34:58.737: RADIUS: Received from id 1646/85 10.62.145.51:1813, Accounting-
response, len 20
```

Captura de paquetes:



Paso 4. Verifique los debugs del profiler en el ISE

Si los atributos fueron enviados del Switch, es posible marcar si fueron recibidos en el ISE. Para marcar esto, habilite por favor los debugs del profiler para el nodo correcto PSN (registro Configuration>PSN>profiler>debug de Administration>System>Logging>Debug) y realice la autenticación del punto final una vez más.

Busque la siguiente información:

- Haga el debug de la indicación de que la sonda del radio recibida atribuye:

```
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=0AE518200000020040099C216, 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=0AE518200000020040099C216,
AllowedProtocolMatchedRule=MAB, Location=Location#All Locations, Device Type=Device Type#All
Device Types, ]
```

- Haga el debug de la indicación de que los atributos fueron analizados con éxito:
  ```
  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
  ```
- Haga el debug de la indicación de que los atributos son procesados por el promotor:
  ```
  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:nullName:nullMAC: 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
  ```

  Un promotor salva los puntos finales en la base de datos de Cisco ISE junto con sus datos de los atributos, y después notifica el analizador de los nuevos puntos finales detectados en su red. El analizador clasifica los puntos finales a la identidad del punto final agrupa y salva los puntos finales con los perfiles correspondidos con en la base de datos.

Paso 5. Típicamente después de que los nuevos atributos se agreguen a la colección existente para el dispositivo específico, este dispositivo/punto final se agrega a perfilar la cola para marcar si él tiene que ser asignado diverso perfil basado en los nuevos atributos:

```
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
```

Información Relacionada

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