Содержание

Введение

Этот документ описывает, как настроить Датчик Устройства, так, чтобы это могло использоваться в копировальных целях на ISE. Датчик устройства является функцией устройств доступа. Это позволяет собирать информацию о связанных оконечных точках. Главным образом собранные сведения Датчиком Устройства могут прибыть из следующих протоколов:

- Протокол CDP (Cisco Discovery Protocol)
- Протокол LLDP
- Протокол динамической настройки узлов (DHCP)

На некоторых платформах возможно использовать также H323, SIP (Протокол инициации сеанса), MDNS (Разрешение Домена Групповой адресации) или HTTP - протоколы. Возможности конфигурации для возможностей датчика устройства могут варьироваться от протокола до протокола. Поскольку приведенный выше пример доступен на Cisco Catalyst 3850 с программным обеспечением 07.03.02. E.

Как только информация собрана, она может инкапсулироваться в учете радиуса и передать к копировальному серверу. В этой статье Identity Service Engine (ISE) используется в качестве копировального сервера.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Протокол RADIUS
- CDP, LLDP и протоколы DHCP
- Идентификационный механизм сервиса Cisco
- Коммутатор Cisco Catalyst 2960

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Идентификационное исправление 3 версии 1.3 Механизма Сервиса Cisco
- Версия 15.2 (2a) E1 2960-x коммутатора Cisco Catalyst
- Cisco IP Phone 8941 SCCP версии 9-3-4-17

Настройка

Шаг 1. Стандартная конфигурация AAA

Для настройки Аутентификации, авторизации и учета (AAA) выполните действия ниже:

1. Включите AAA с помощью **команды aaa new-model** и включите 802.1X глобально на коммутаторе

2. Настройте сервер RADIUS и включите динамическую авторизацию (Изменение Авторизации - CoA)

3. Включите протоколы LLDP и CDP

4. Добавьте конфигурацию аутентификации порта коммутатора

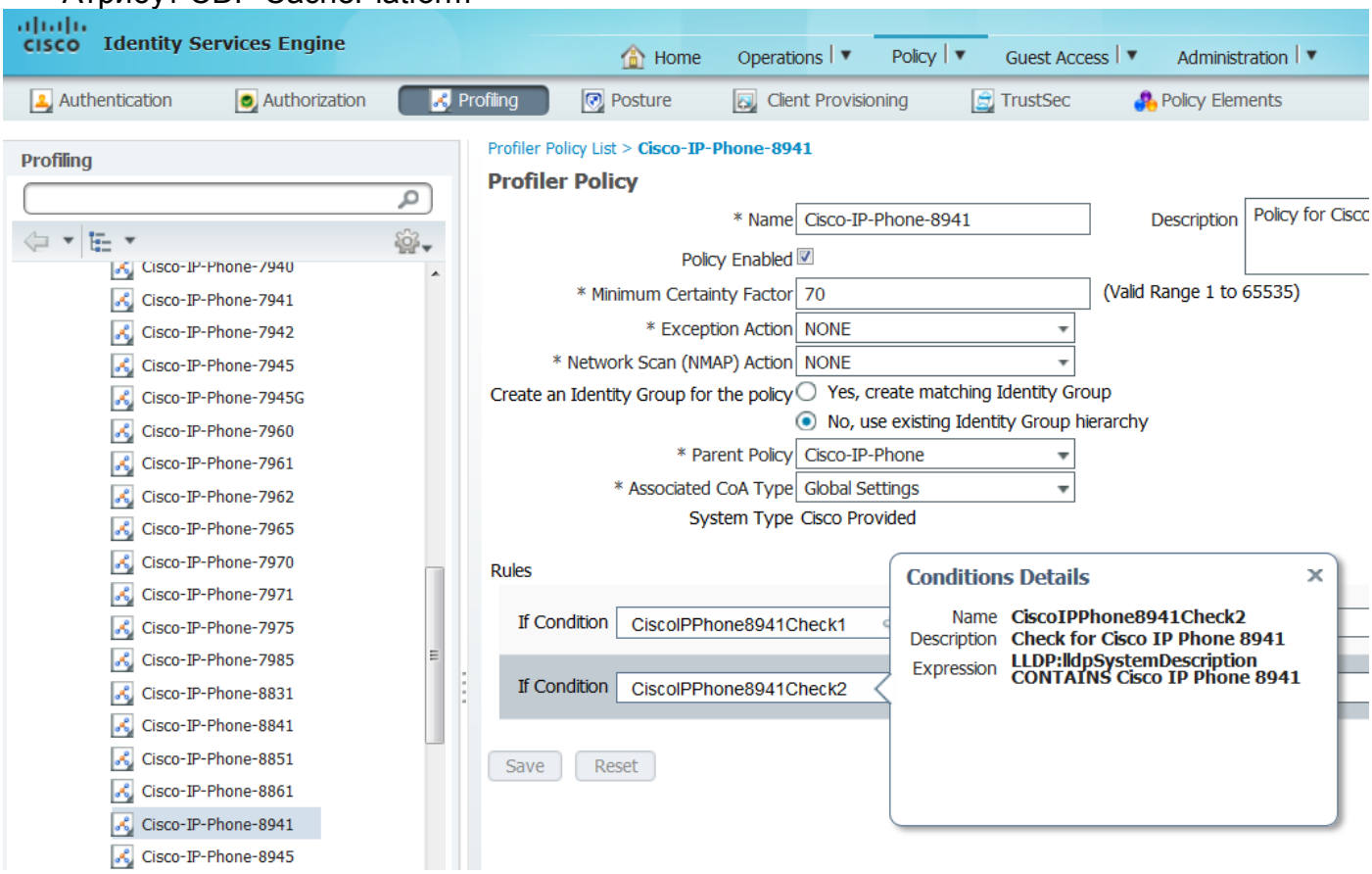
```
!




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
!
```

> **В более новой версии программного обеспечения `учет команды radius-server vsa send` включен по умолчанию. Если вы не видите, что атрибуты передают в учете, проверьте если команда во включенном.**

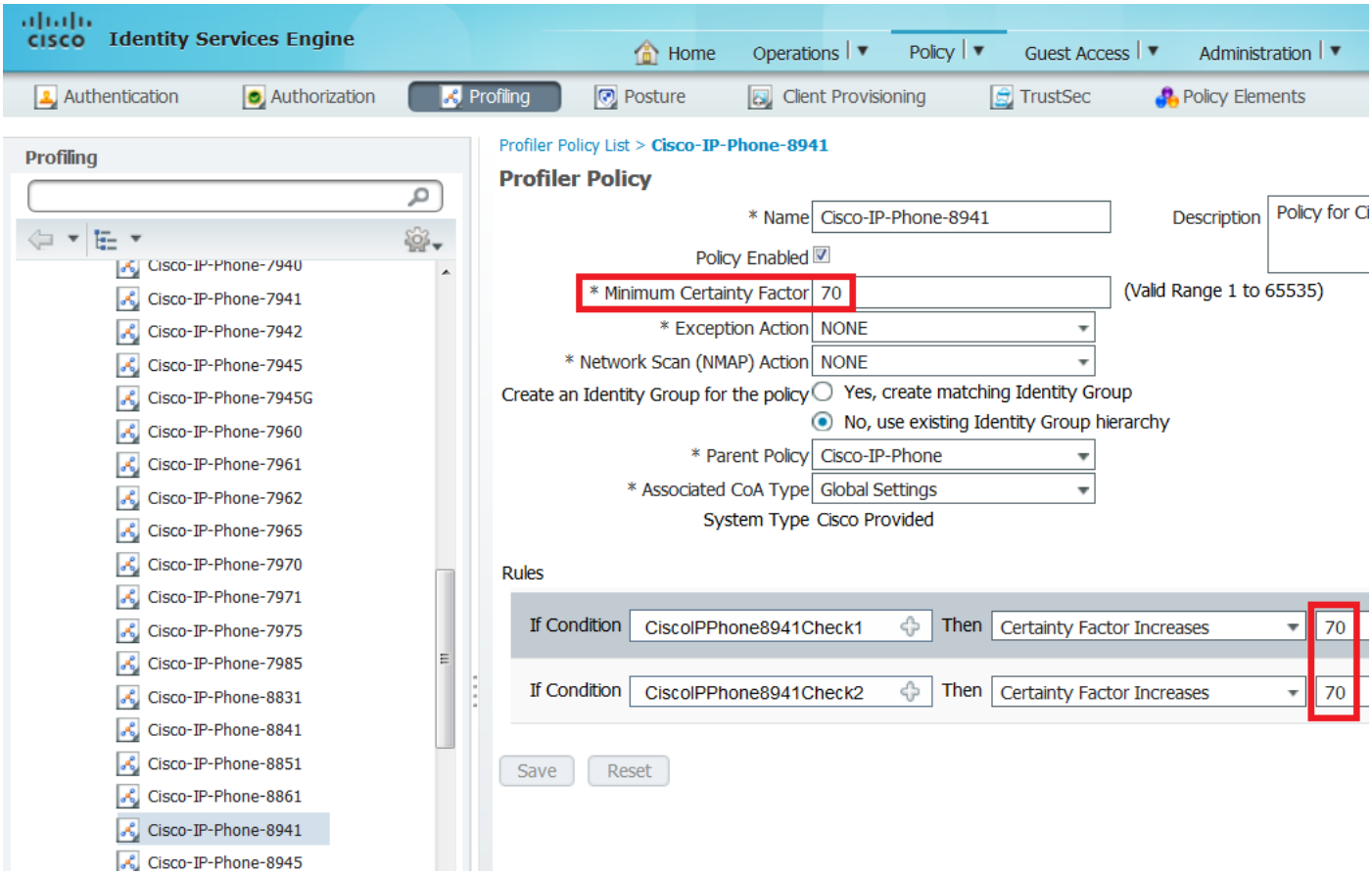
Шаг 2. Настройте датчик устройства

1. Определите, какие атрибуты от CDP/LLDP необходимы для профилирования устройства. В случае Cisco IP Phone 8941 можно использовать придерживающееся:

- Атрибут LLDP SystemDescription
- Атрибут CDP CachePlatform



Для нашей цели было бы достаточно получить только один из тех, так как они оба предоставляют увеличение Фабрики Уверенности 70 и Минимальная Фабрика Уверенности, требуемая быть представленной, поскольку Cisco-IP-Phone-8941 равняется 70:



Чтобы быть представленным как определенный Cisco IP Phone, youneed для удовлетворения минимальных условий для всех родительских профилей. Это означает потребности профилировщика совпасть с устройством Cisco (Фактор Уверенности min 10) и Cisco IP Phone (Фактор Уверенности min 20). Даже при том, что профилировщик совпадает с теми двумя профилями, это должно все еще быть представлено как определенный Cisco IP Phone, так как каждая Модель IP-телефона имеет Фактор Уверенности min 70. Устройство назначено на профиль, для которого оно имеет самый высокий Фактор Уверенности.

2. Настройте два списка фильтров - один для CDP и другого для LLDP. Те указывают, какие атрибуты должны быть включены в сообщения учета Радиуса. Этот шаг не является обязательным

3. Создайте две спецификации фильтра для CDP и LLDP. В более подходящей спецификации можно или указать, что список атрибутов должен быть включен или исключен из учета сообщений. В примере после атрибутов включены:

- имя устройства от CDP
- описание системы от LLDP

Можно настроить дополнительные атрибуты, которые будут переданы через Радиус к ISE в случае необходимости. Этот шаг является также дополнительным.

4. **`Датчик устройства`** команды Add **`уведомляет все-изменения`**. Это инициирует обновления каждый раз, когда TLV добавляются, модифицируются или удаляются для текущего сеанса

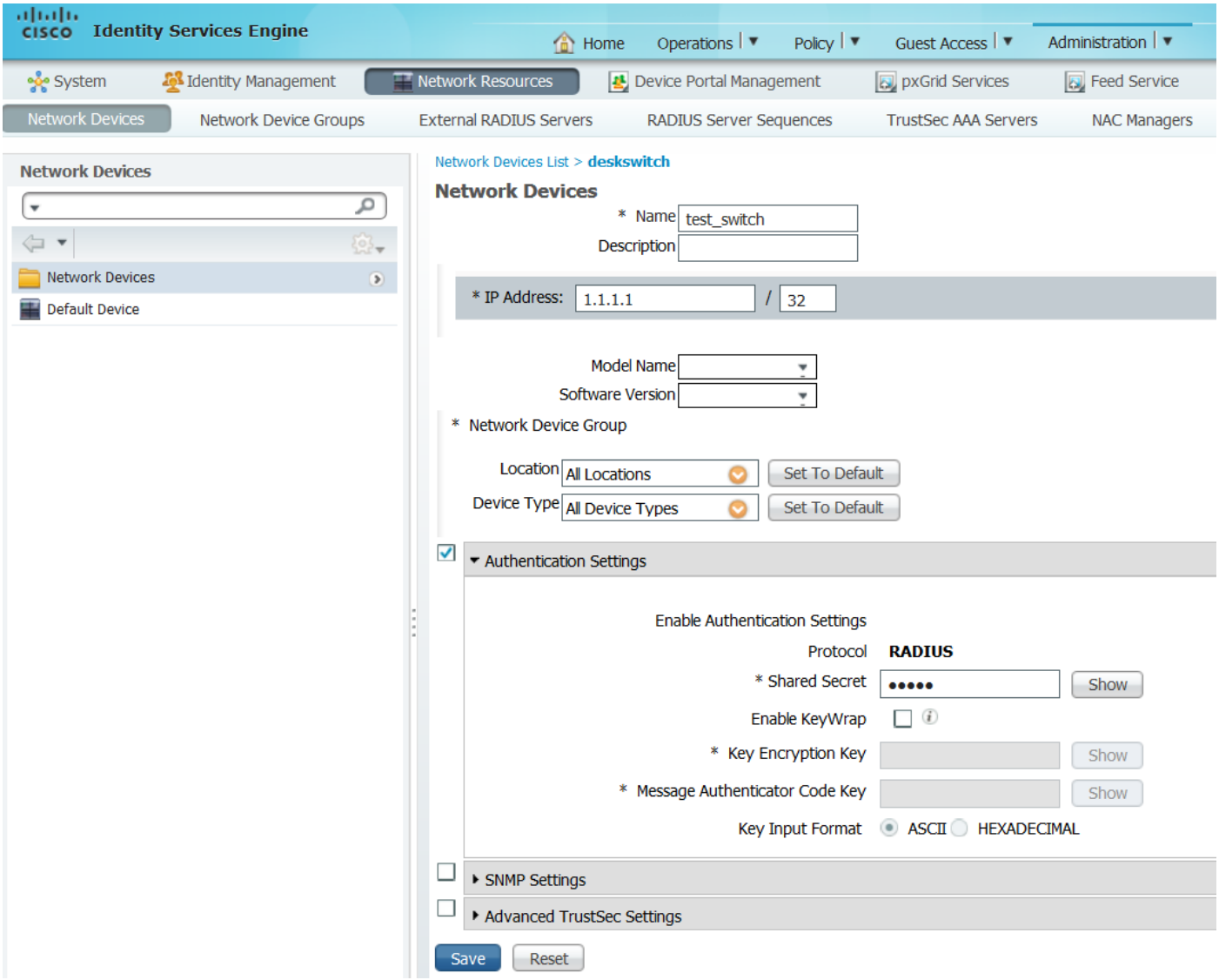
5. Для фактической передачи информации, собранной через Функцию sensor Устройства, необходимо явно сказать коммутатору делать так с **`учетом датчика устройства`**

команды

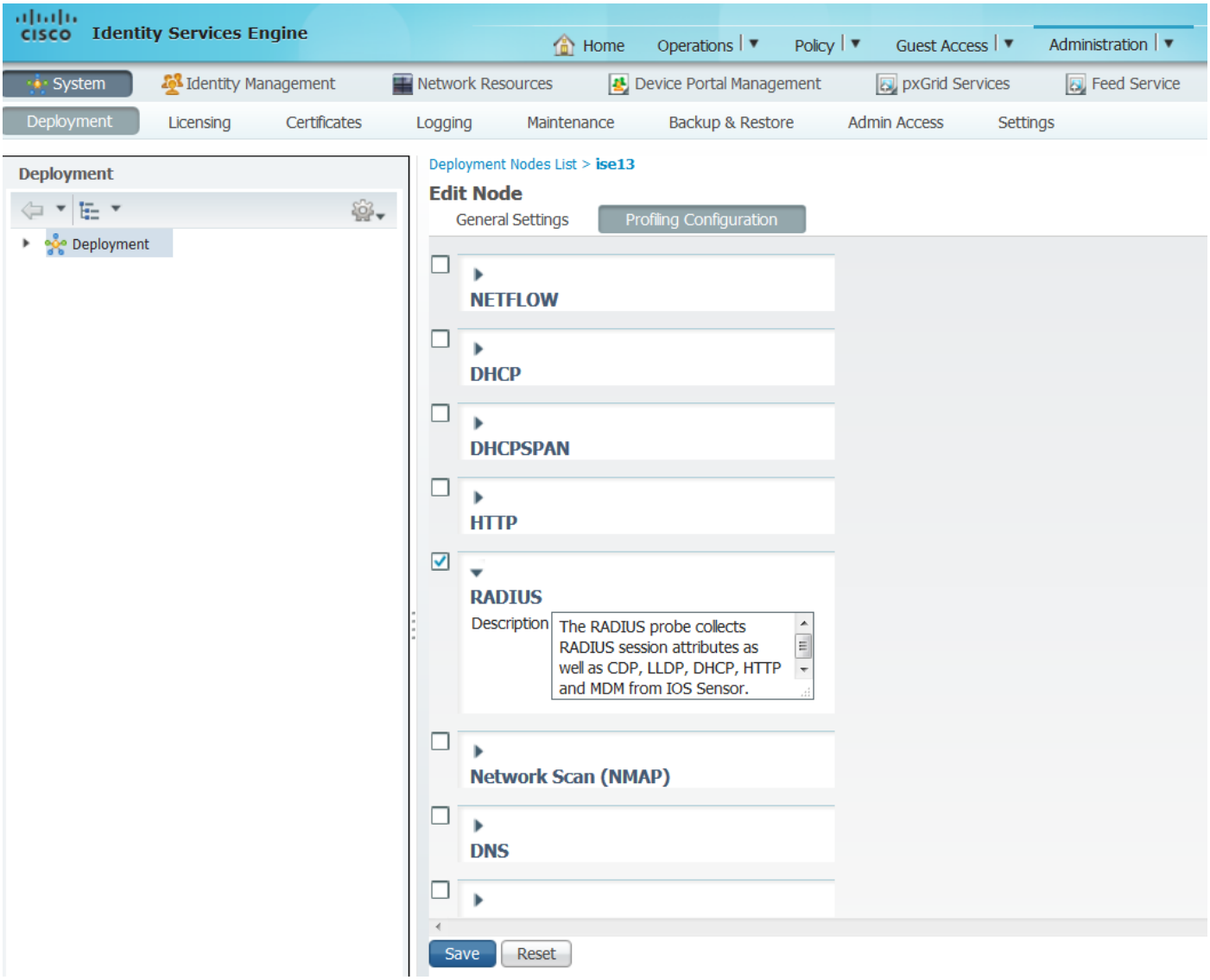
```
!device-sensor filter-list cdp list cdp-list tlv name device-name
 tlv name platform-type!device-sensor filter-list lldp list lldp-list tlv name system-
description!device-sensor filter-spec lldp include list lldp-listdevice-sensor filter-spec cdp
include list cdp-list!device-sensor accountingdevice-sensor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

Шаг 3. Настройте профилирование на ISE

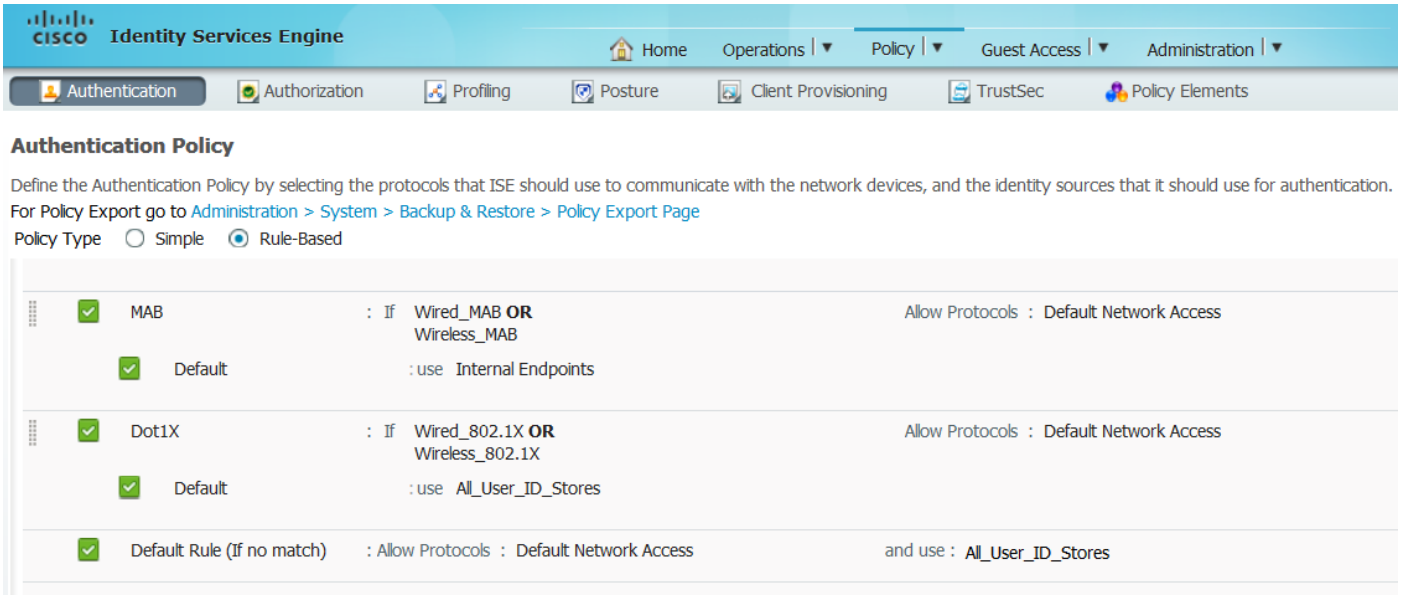
1. Добавьте коммутатор как сетевое устройство в "администрировании> Сетевые ресурсы> Сетевые устройства". Используйте ключ сервера RADIUS от коммутатора как общий секретный ключ в параметрах аутентификации:



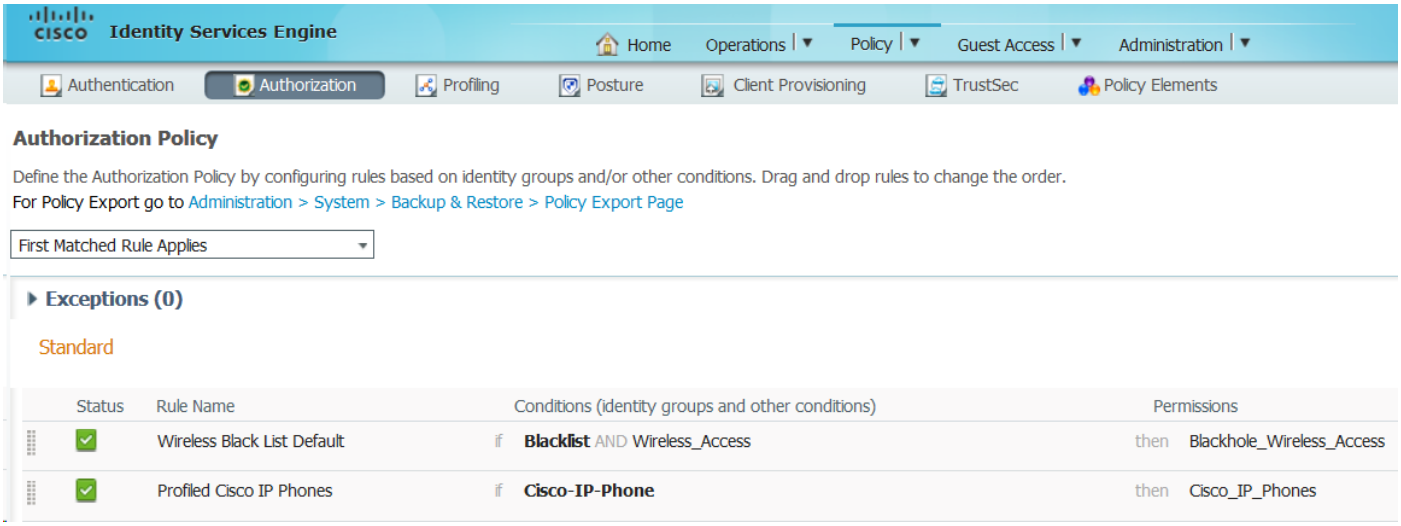
2. Включите зонд Радиуса на копировальном узле в "администрировании> Система> Развертывания> узел ISE> Профилирование Конфигурации". Если все узлы PSN должны использоваться для профилирования, включите зонд на всех них:



3. Настройте Правила Аутентификации ISE. В примере используются правила проверки подлинности по умолчанию, предварительно сконфигурированные на ISE:

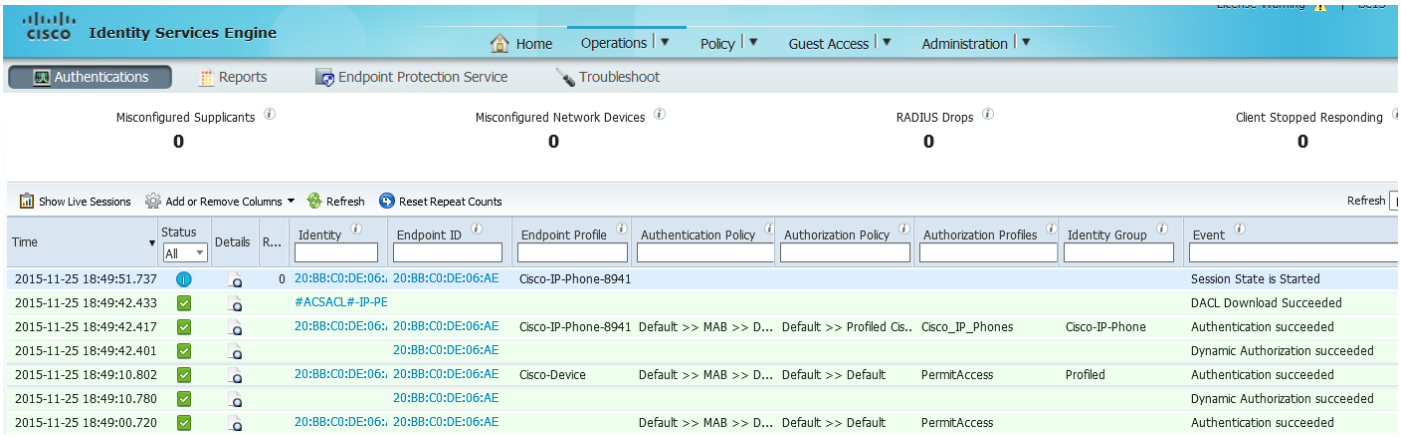


4. Настройте Правила авторизации ISE. 'Представленные Cisco IP Phone' правило используются, который предварительно сконфигурирован на ISE:



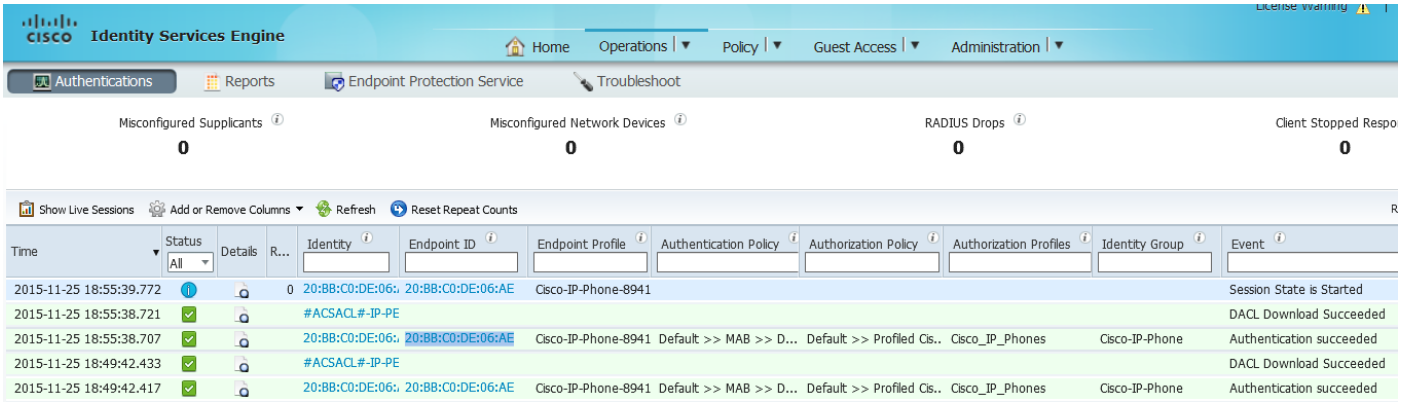
Проверка

Чтобы проверить, работает ли профилирование правильно см. "Операции> Аутентификации" на ISE:

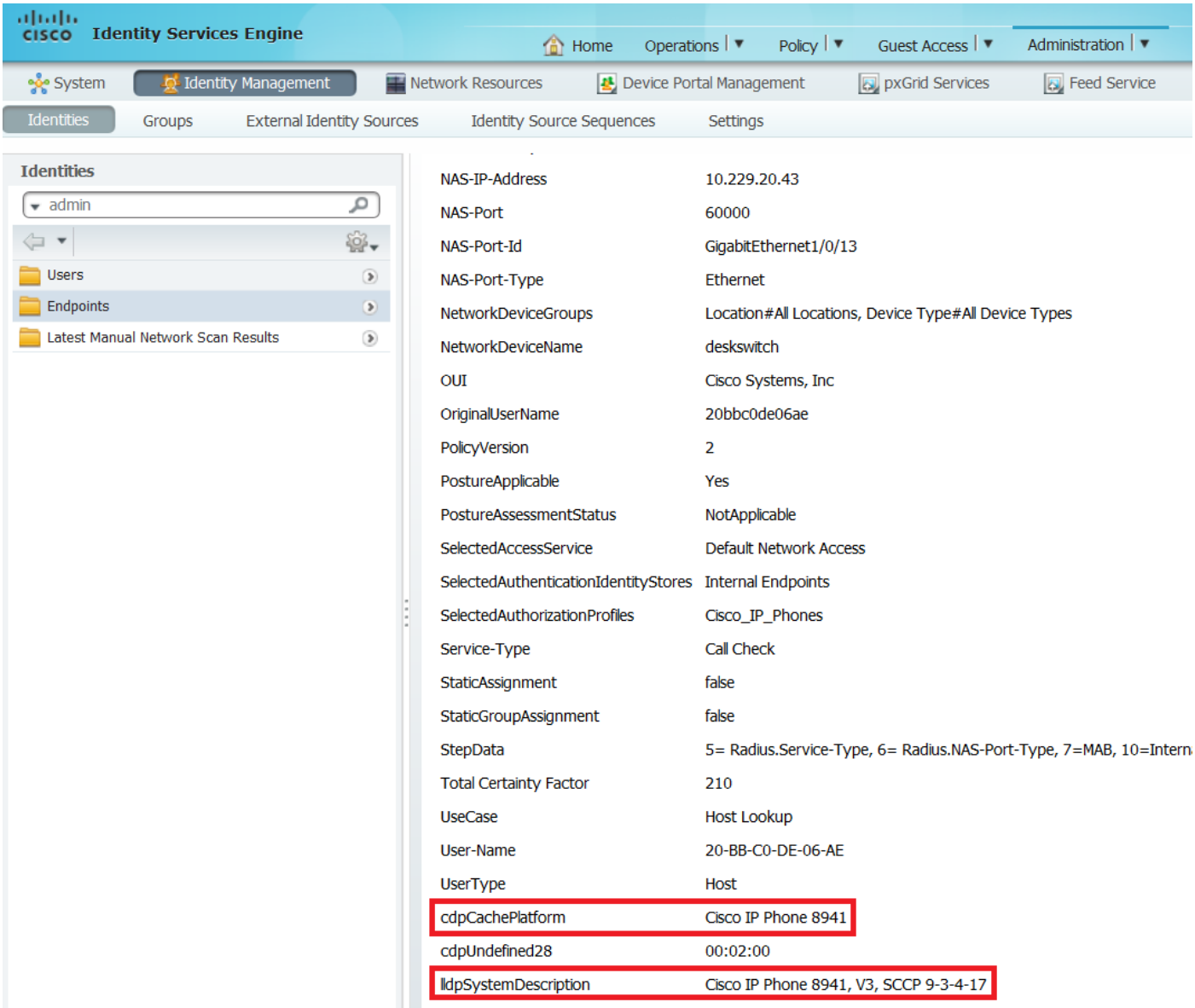


Сначала устройство аутентифицировалось с помощью MAB (18:49:00). Десять секунд спустя (18:49:10), это было повторно представлено как устройство Cisco и наконец после 42 секунд начиная с первых аутентификаций (18:49:42), это получило профиль Cisco-IP-Phone-8941. В результате ISE возвращает Профиль Авторизации, определенный для IP-телефонов (Cisco_IP_Phones) и Загружаемый список ACL, который разрешает весь трафик (permit ip any any). Обратите внимание на то, что в этом сценарии неизвестное устройство имеет базовый доступ к сети. Это может быть достигнуто путем добавления мак адреса к ISE внутренняя база данных оконечной точки или разрешения очень простого доступа к сети для ранее неизвестных устройств.

> **Начальное профилирование заняло приблизительно 40 секунд в данном примере. На следующем опознавательном ISE уже знает профиль, и корректные атрибуты (разрешения для присоединения к речевому домену и DACL) применены немедленно, пока ISE не получает новые/обновленные атрибуты, и это должно повторно представить устройство снова.**



В "администрировании> Управление идентификацией> Личности> Оконечные точки> протестировали оконечную точку", вы видите, какие атрибуты были собраны зондом Радиуса и каковы их значения:



Поскольку можно заметить, что общий вычисленный Фактор Уверенности 210 в этом сценарии. Это прибывает передняя сторона факт, что оконечная точка совпала также с профилем устройства Cisco (с общим фактором уверенности 30) и профилем Cisco IP Phone (с общим фактором уверенности 40). Так как профилировщик совпал с обоими условиями в профиле Cisco-IP-Phone-8941, фактор уверенности для этого профиля равняется 140 (70 для каждого атрибута согласно копировальной политике). Подвести итог: 30+40+70+70=210.

Устранение неполадок

Шаг 1. Проверьте собранные сведения 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
```

Если вы не видите, что любые собранные данные проверяют придерживающееся:

- Проверьте состояние сеанса аутентификации на коммутаторе (это должно быть успешно):
```
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
```
- Проверьте, включены ли CDP и протоколы LLDP. Проверьте, существуют ли какие-либо команды ня по умолчанию относительно CDP/lldp/и т.д. и как те могут влиять на извлечение атрибута от оконечной точки
```
switch#sh running-config all | in cdp runcdp runswitch#sh running-config all | in lldp
runlldp run
```
- Проверьте в руководстве по конфигурации для вашей оконечной точки, если это поддерживает CDP/lldp/и т.д.

Шаг 2. Проверьте кэш Датчика Устройства

```
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
```
Если вы не видите данных в этом поле, или информация не завершена, проверяют команды 'датчика устройства', в особенности filter-list и спецификации фильтра.

Шаг 3. Проверьте, присутствуют ли атрибуты в Учете Радиуса

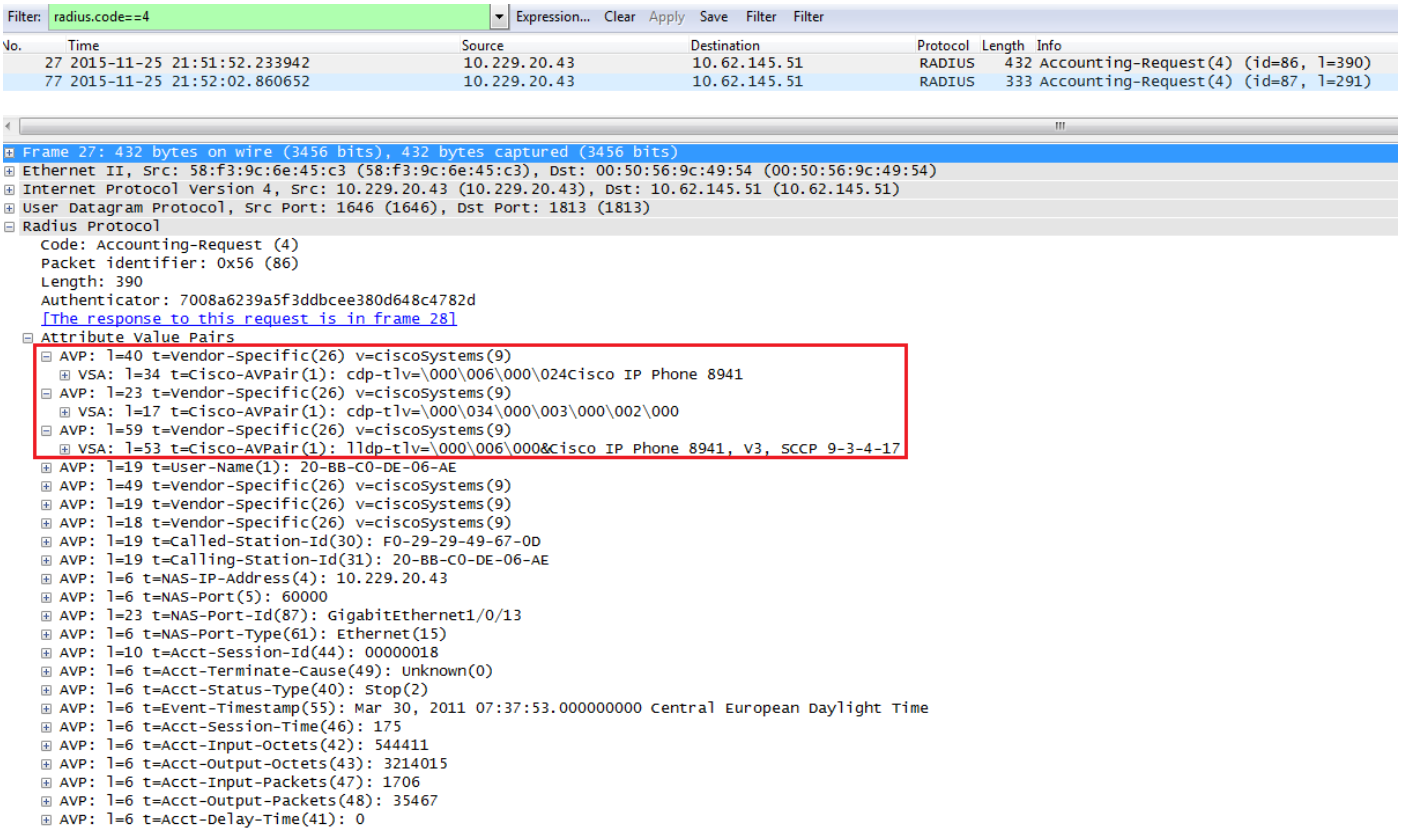
Можно проверить что с помощью команды 'debug radius' на коммутаторе или выполнив захват пакета между коммутатором и ISE.

Отладка радиуса:

```
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
```

Захват пакета:



Шаг 4. Проверьте отладки профилировщика на ISE

Если атрибуты передавались от коммутатора, возможно проверить, были ли они получены на ISE. Для проверки этого включите отладки профилировщика для корректного узла PSN (администрирование> Система> Регистрация> Конфигурация Журнала Отладки> PSN> профилировщик> отладка) и выполните аутентификацию оконечной точки еще раз.

Ищите следующую информацию:

- Отладка, указывающая, что зонд радиуса получил атрибуты:

```
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=0AE518200000020400 99C216, 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=0AE518200000020400 99C216,
AllowedProtocolMatchedRule=MAB, Location=Location#All Locations, Device Type=Device Type#All
Device Types, ]
```

- Отладка, указывающая, что были успешно проанализированы атрибуты:

```
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
```

- Отладка, указывающая, что атрибуты обработаны средством передачи:

```
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
```

Средство передачи хранит оконечные точки в базу данных Cisco ISE наряду с их данными атрибутов, и затем уведомляет анализатор новых оконечных точек, обнаруженных в вашей сети. Анализатор классифицирует оконечные точки идентификационным группам оконечной точки и хранит оконечные точки профилями, с которыми совпадают, в базе данных.

Шаг 5. Как правило, после того, как новые атрибуты добавлены к существующему набору для определенного устройства, это устройство/оконечная точка добавлено к копировальной очереди, чтобы проверить, нужно ли этому назначить другой профиль на основе новых атрибутов:

```
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
```

Дополнительные сведения

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