ISE プロファイリング用のデバイス センサーの設定

目次

概要

このドキュメントでは、デバイス センサーを ISE でプロファイリング目的で使用できるように設定する方法を説明します。 デバイス センサーはアクセス デバイスの機能です。 これにより、接続エンドポイントに関する情報を収集できます。 ほとんどの場合、デバイス センサーは次のプロトコルからの情報を収集します。

- シスコ検出プロトコル（CDP）
- Link Layer Discovery Protocol（LLDP）
- Dynamic Host Configuration Protocol（DHCP）

一部のプラットフォームでは、H323、SIP（Session Initiation Protocol）、MDNS（Multicast Domain Resolution）、または HTTP プロトコルも使用できます。 デバイス センサー機能を設定できるかどうかは、プロトコルによって異なります。 例えば、ソフトウェア 03.07.02.E を実行している Cisco Catalyst 3850 では上記のプロトコルを使用できます。

収集された情報は、RADIUS アカウンティングでカプセル化してプロファイリング サーバに送信できます。 この記事では Identity Services Engine（ISE）がプロファイリング サーバとして使用されています。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- RADIUS プロトコル
- CDP、LLDP、および DHCP プロトコル
- Cisco Identity Service Engine
- Cisco Catalyst スイッチ 2960

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Identity Service Engine バージョン 1.3 パッチ 3
- Cisco Catalyst スイッチ 2960 バージョン 15.2(2a)E1
- Cisco IP Phone 8941 バージョン SCCP 9-3-4-17

設定

ステップ 1：標準 AAA 設定

認証、許可、およびアカウンティング（AAA）を設定するには、次の手順を実行します。

1. **aaa new-model** コマンドを使用して AAA を有効にし、スイッチで 802.1X をグローバルに有効にします。

2. RADIUS サーバを設定し、動的認可（認可変更 - CoA）を有効にします。

3. CDP および LLDP プロトコルを有効にします。

4. スイッチ ポート認証設定を追加します。

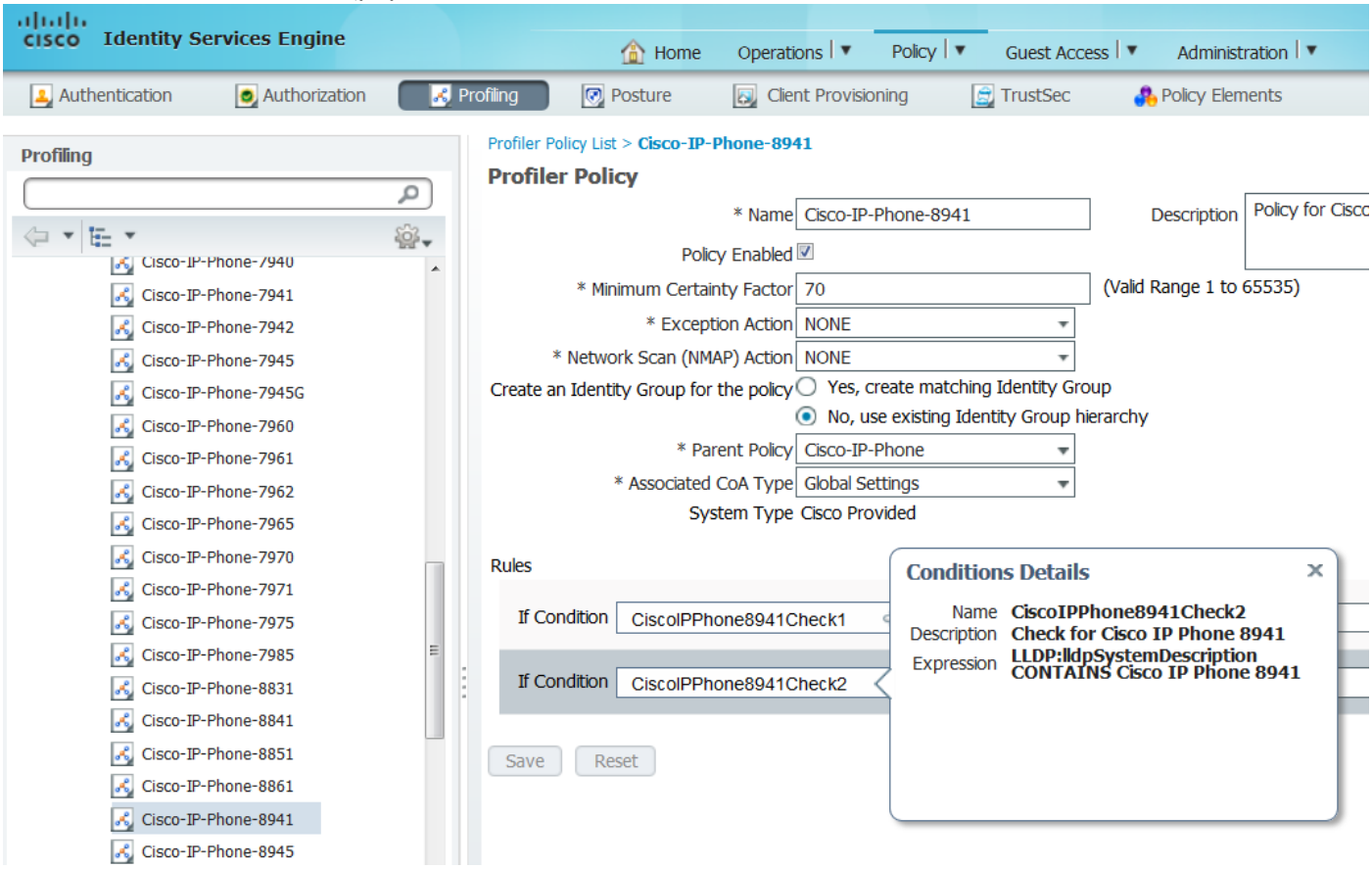
```
!
aaa new-model ! aaa authentication dot1x default group radius aaa authorization network default
group radius aaa accounting update newinfo aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
 client 1.1.1.1 server-key xyz
!
dot1x system-auth-control
! lldp run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

新しいソフトウェア バージョン コマンド radius-server vsa send accounting は、デフォルトで有効になっています。 アカウンティングで属性の送信が確認できない場合は、コマンドが有効であるかどうかを確認します。

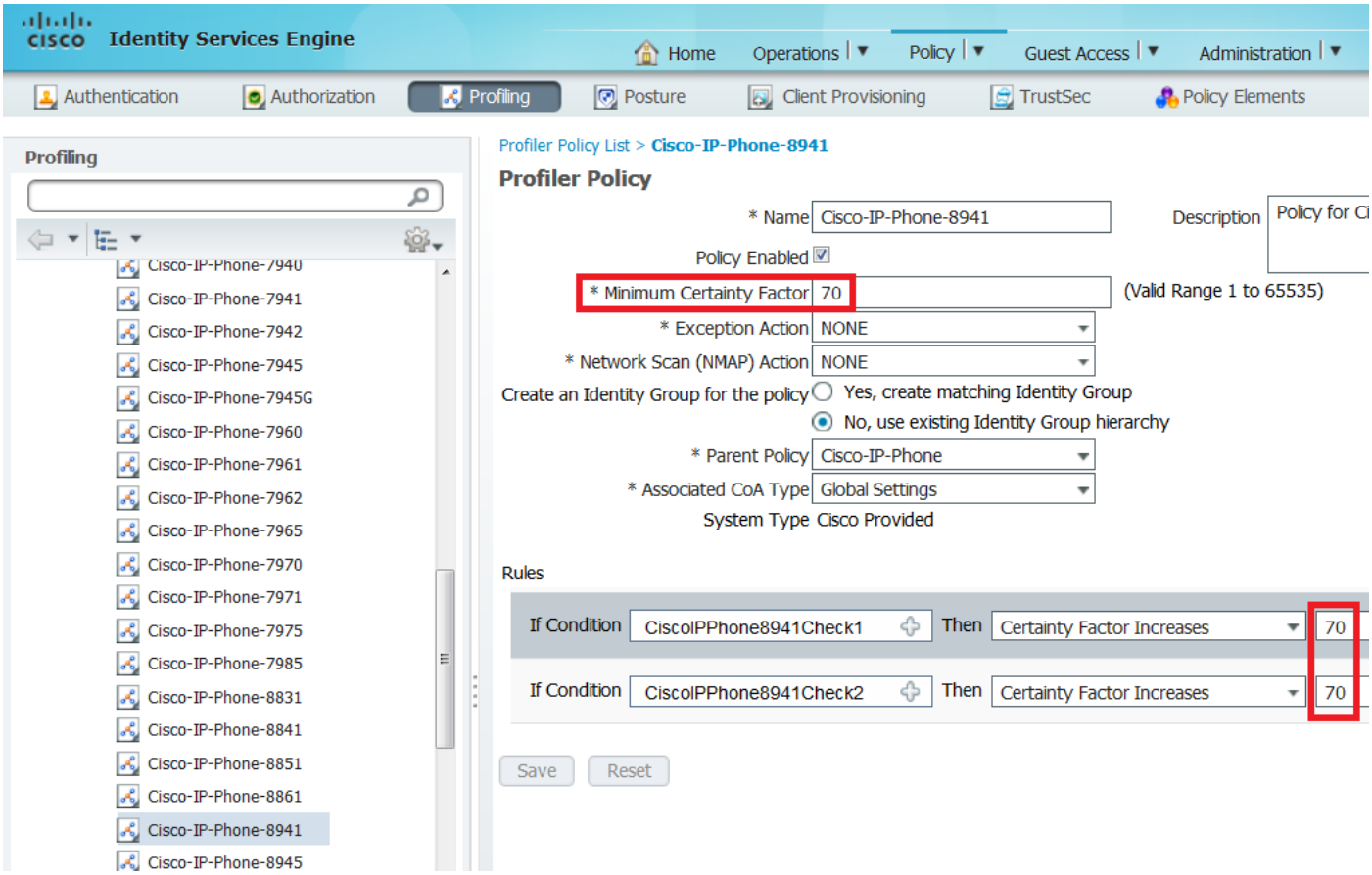
ステップ 2：デバイス センサーの設定

1. デバイスのプロファイリングに必要な CDP/LLDP の属性を判断します。 Cisco IP Phone 8941 の場合は次の属性を使用できます。

- LLDP SystemDescription 属性
- CDP CachePlatform 属性



どちらの属性でも、確信度が 70 増加し、Cisco-IP-Phone-8941 としてプロファイリングする必要がある最小確信度が 70 であるため、いずれか 1 つの属性を取得するだけで十分です。



特定の Cisco IP Phone としてプロファイリングするには、すべての親プロファイルの最小条件を満たしている必要があります。 つまり、プロファイラが Cisco-Device (最小確信度 10) と Cisco-IP-Phone (最小確信度 20) に一致している必要があります。 プロファイラがこの 2 つのプロファイルに一致しても、各 IP フォン モデルの最小確信度は 70 であるため、特定の Cisco IP Phone としてプロファイリングする必要があります。 デバイスは、確信度が最も大きいプロファイルに割り当てられます。

2. 2 つのフィルタ リスト (CDP のリストと LLDP のリスト) を設定します。 これらのリストは、RADIUS アカウンティング メッセージに組み込む必要がある属性を示しています。 この手順はオプションです。

3. CDP と LLDP の 2 つのフィルタ仕様を作成します。 フィルタ仕様では、属性リストをアカウンティング メッセージに含めるかまたは除外するかを指定できます。 この例では、次の属性が含まれます。

- device-name (CDP)
- system-description (LLDP)

必要に応じて、追加属性を RADIUS 経由で ISE に送信することを設定できます。 この手順もオプションです。

4. **device-sensor notify all-changes** コマンドを追加します。 これにより、現行セッションで TLV の追加、変更、または削除が行われるたびに更新がトリガーされます。

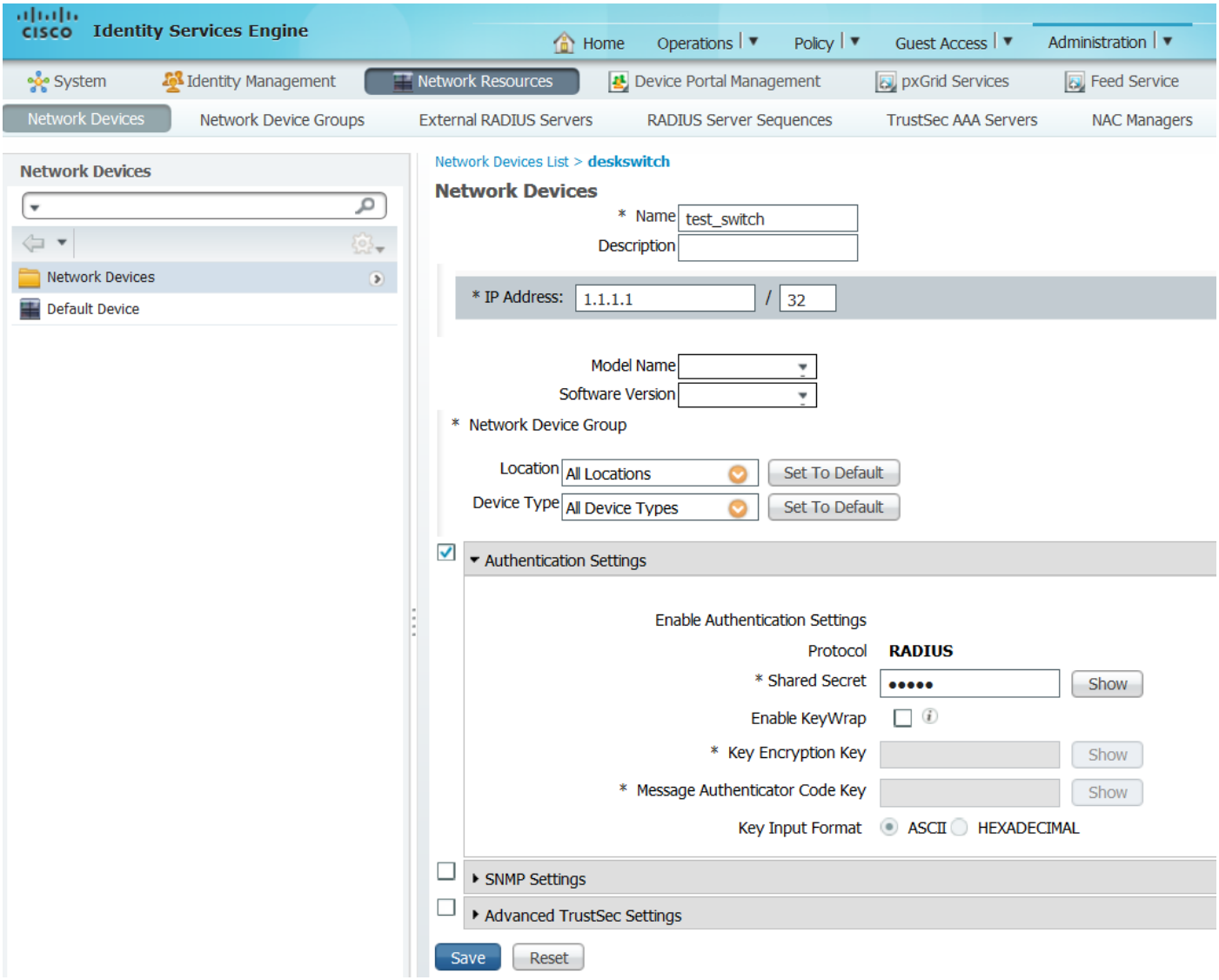
5. デバイス センサー機能により収集した情報を実際に送信するには、**device-sensor accounting** コマンドを使用してスイッチに対しこの操作を実行するように明示的に指示します。

```
!
device-sensor filter-list cdp list cdp-list
```

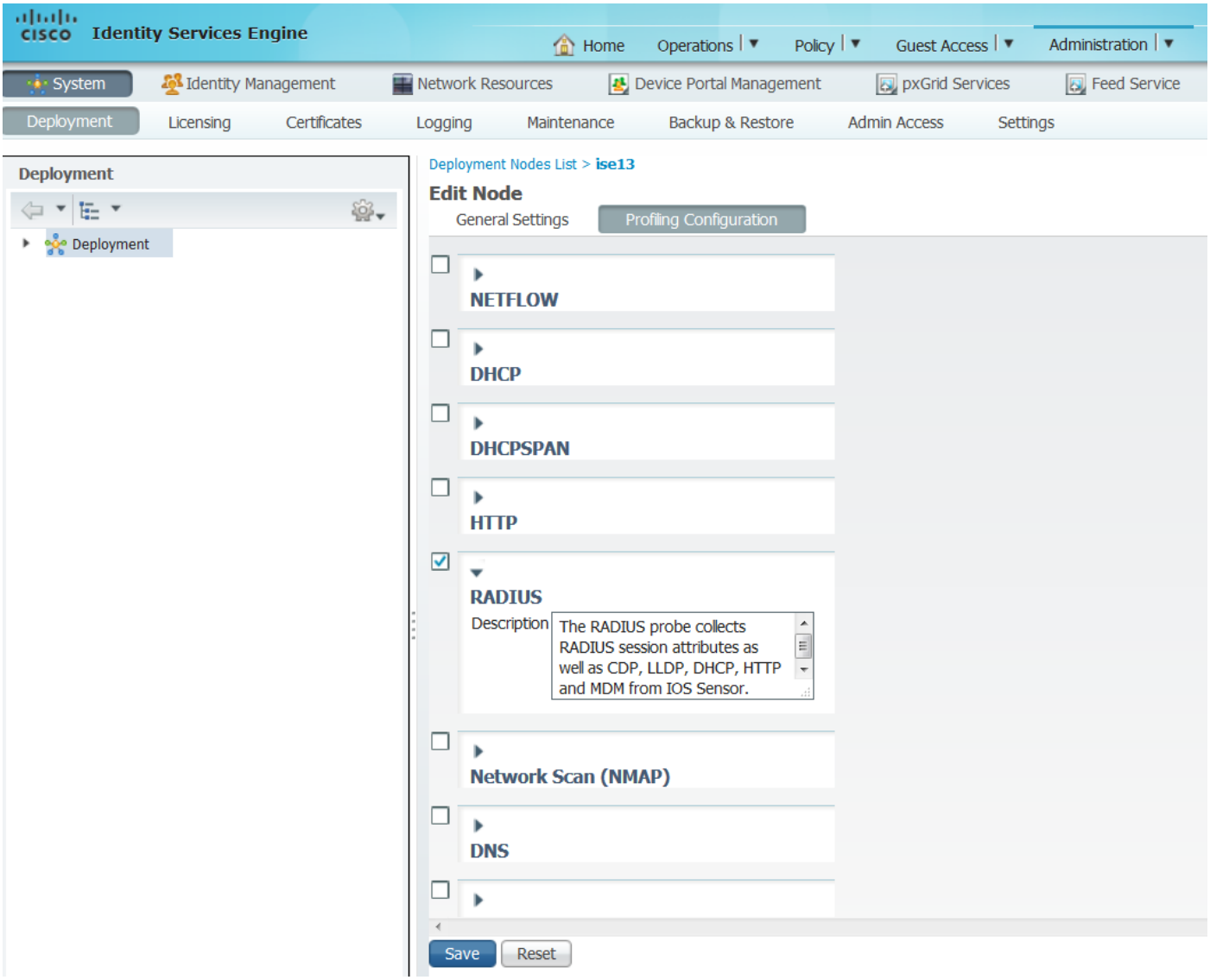
```
 tlv name device-name
 tlv name platform-type ! device-sensor filter-list lldp list lldp-list tlv name system-
description ! device-sensor filter-spec lldp include list lldp-list device-sensor filter-spec
cdp include list cdp-list ! device-sensor accounting device-sensor notify all-changes !
```

ステップ 3：ISE でのプロファイリングの設定

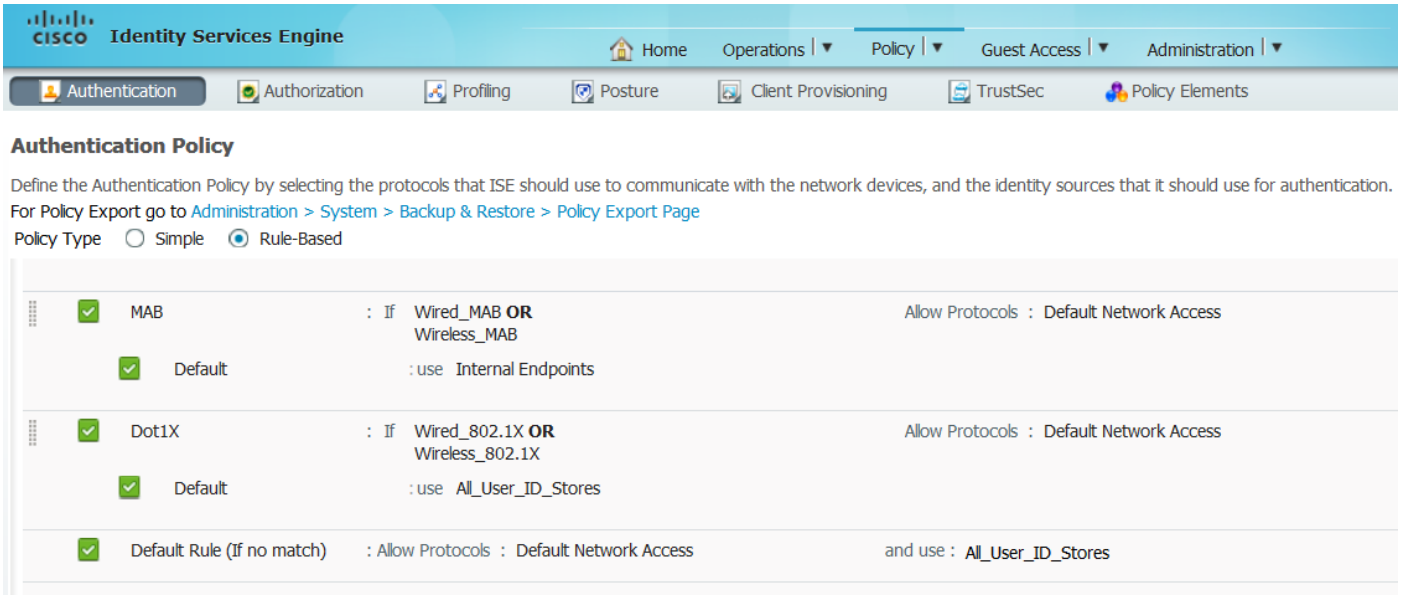
1. [Administration] > [Network Resources] > [Network Devices] でスイッチをネットワーク デバイスとして追加します。 [Authentication Settings] でスイッチの RADIUS サーバ キーを共有秘密として使用します。



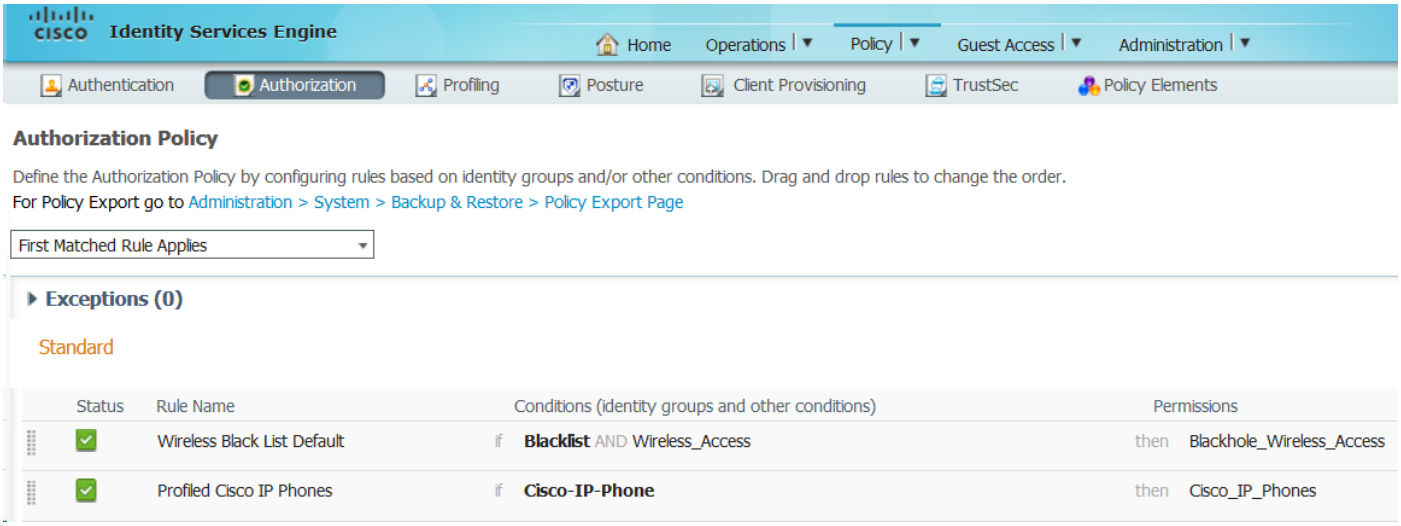
2. [Administration] > [System] > [Deployment] > [ISE node] > [Profiling Configuration] でプロファイリング ノードの RADIUS プローブを有効にします。 すべての PSN ノードをプロファイリングに使用する場合は、すべてのノードでプローブを有効にします。



3. ISE 認証ルールを設定します。 次の例では、ISE で事前に設定されているデフォルトの認証ルールが使用されます。

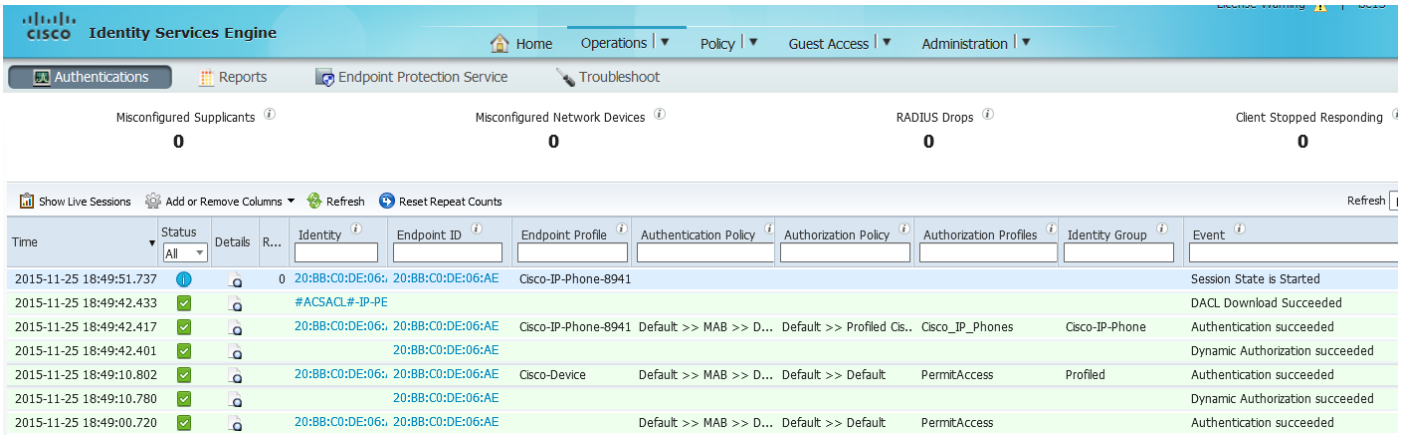


4. ISE 認可ルールを設定します。 ISE で事前に設定された「Profiled Cisco IP Phone」ルールを使用します。



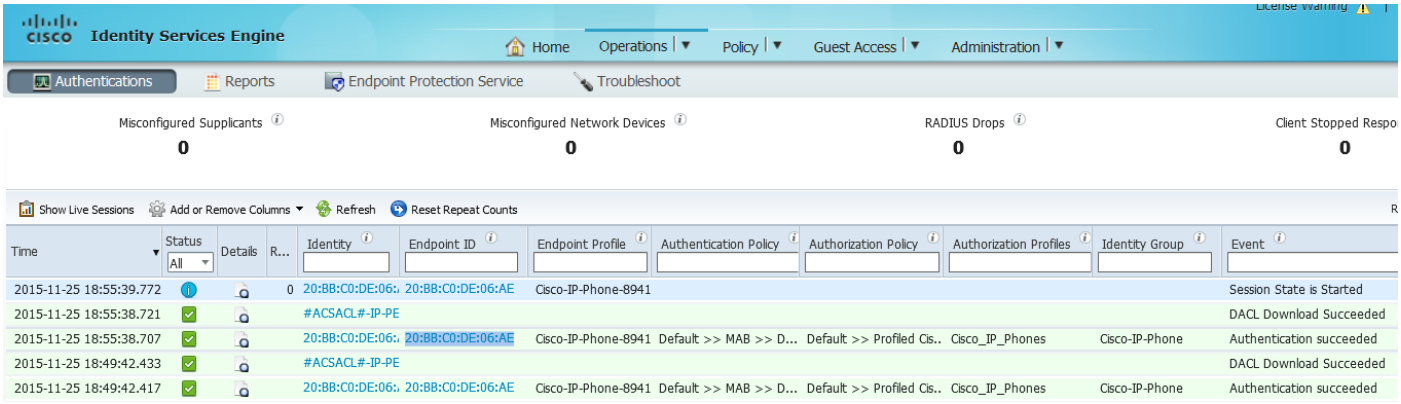
確認

プロファイリングが正しく機能するかどうかを確認するには、ISE で [Operations] > [Authentications] を参照してください。

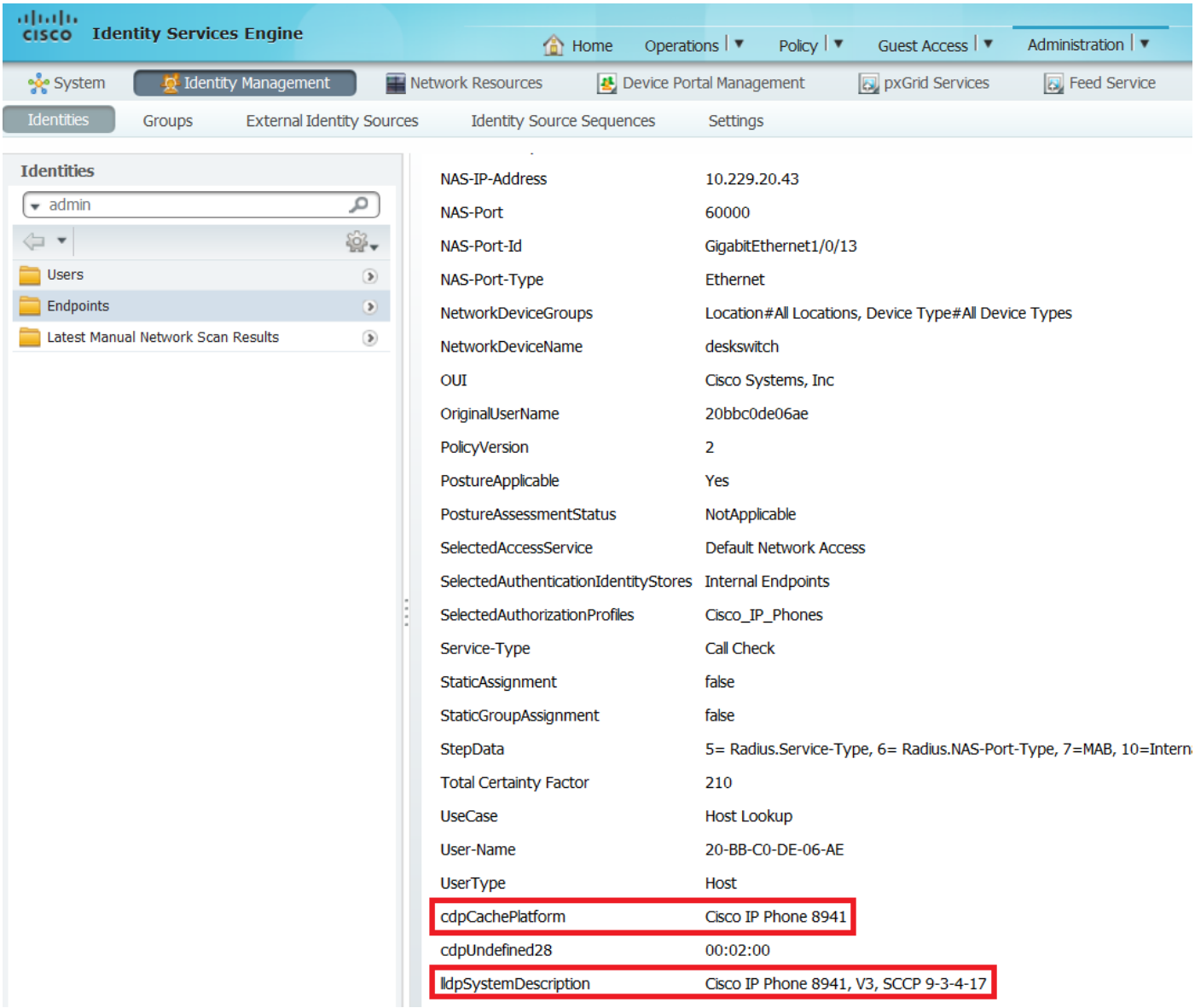


最初にデバイスは MAB を使用して認証されます（18:49:00）。 10 秒後（18:49:10）に Cisco-Device として報告され、最初の認証から 42 秒後（18:49:42）に Cisco-IP-Phone-8941 プロファイルを受信しています。 その結果、ISE は IP フォンに固有の認証プロファイル（Cisco_IP_Phones）とダウンロード可能な ACL を返します。この ACL では、すべてのトラフィックが許可されます（permit ip any any）。 このシナリオでは、不明なデバイスに、ネットワークへの基本アクセス権限があることに注意してください。 これは、MAC アドレスを ISE 内部エンドポイント データベースに追加するか、または以前に不明だったデバイスに対して非常に基本的なネットワーク アクセス権限を付与することで実現できます。

この例では、初回プロファイリングに約 40 秒かかりました。 ISE が新しい属性/更新された属性を受け取り、デバイスを再プロファイリングする必要がある場合を除き、次回の認証ではすでにプロファイルと正しい属性（音声ドメインへの参加権限と DACL）が即時に適用されることを ISE が認識しています。



[Administration] > [Identity Management] > [Identities] > [Endpoints] > [tested endpoint] で、RADIUS プローブにより収集された属性の種類とその値を確認できます。



このシナリオでは、計算された確信度の合計が 210 であることがわかります。 これは、エンドポイントが Cisco-Device プロファイル（合計確信度 30）と Cisco-IP-Phone プロファイル（合計確信度 40）にも一致することに基づいています。 プロファイラがプロファイル Cisco-IP-Phone-8941 の両方の条件に一致するため、このプロファイルの確信度は 140 です（プロファイリングポリシーに基づき属性ごとに 70）。 まとめると、次のようになります。 30+40+70+70=210

トラブルシューティング

ステップ 1：CDP/LLDP により収集される情報の検証

```
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
```

収集データが表示されない場合は、次の点を確認します。

- スイッチの認証セッションの状態を確認します（正常に完了しているはずです）。

```
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 プロトコルと LLDP プロトコルが有効になっているかどうかを確認します。 CDP/LLDP などに関連するデフォルト以外のコマンドがあるかどうかを確認します。また、エンドポイントからの属性の取得にこれらが影響するかどうかも確認します。

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

- エンドポイントが CDP/LLDP などをサポートしているかどうかについては、エンドポイントの設定ガイドで確認してください。

呼び出します。 デバイス センサー キャッシュの確認

```
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
```

このフィールドにデータが表示されない場合、または情報が完全ではない場合は、「device-

sensor」コマンド、特に filter-list と filter-spec を確認します。

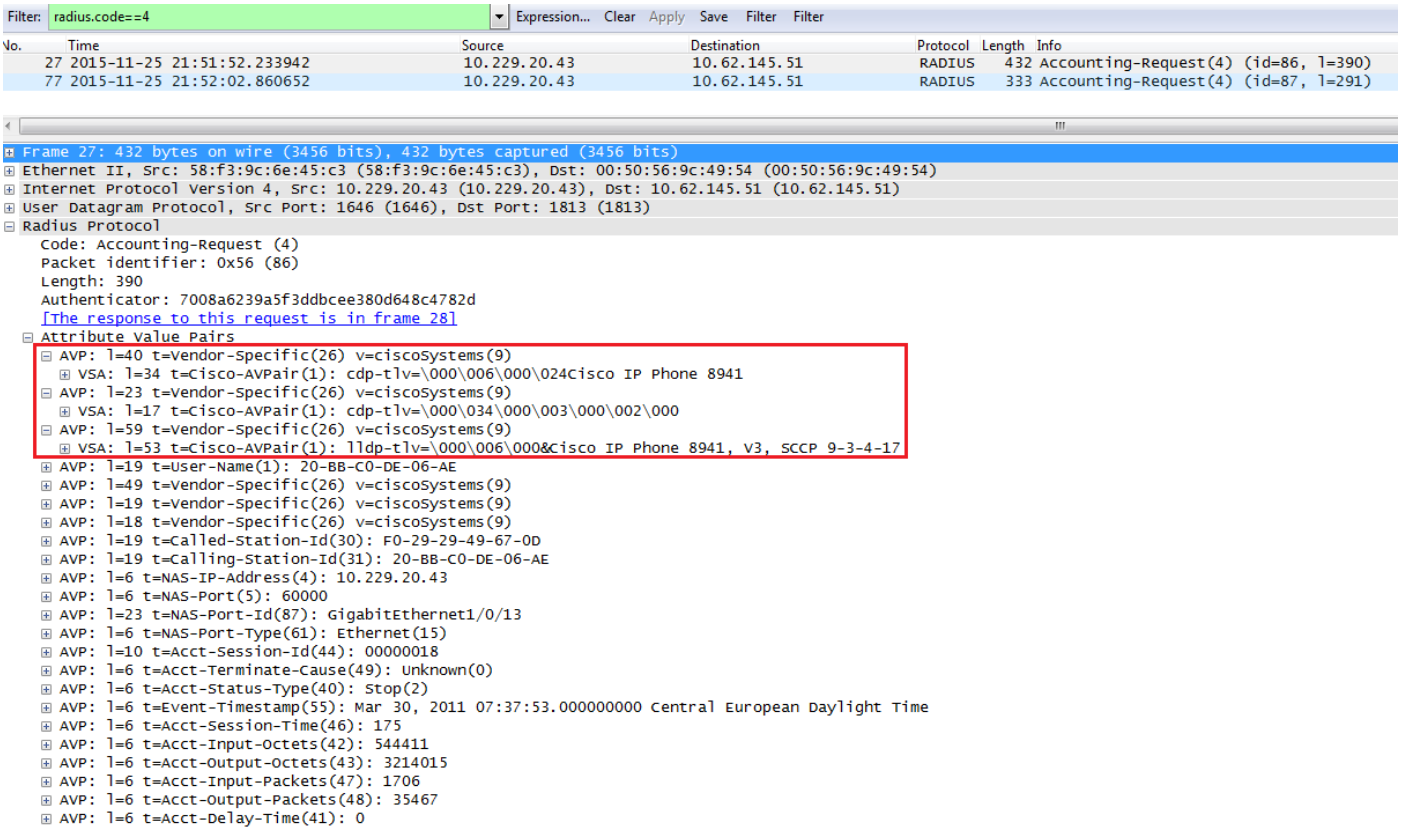
ステップ 3 RADIUS アカウンティングに属性があるかどうかの確認

スイッチで「debug radius」コマンドを使用するか、スイッチと ISE の間でパケット キャプチャを実行することでこれを確認できます。

RADIUS デバッグ：

```
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
```

パケット キャプチャ：



ステップ 4：ISE でのプロファイラ デバッグの確認

スイッチから属性が送信された場合は、ISE で属性が受信されたかどうかを確認できます。 これを確認するには、正しい PSN ノードのプロファイラ デバッグを有効にし（[Administration] > [System] > [Logging] > [Debug Log Configuration] > [PSN] > [profiler] > [debug]）、エンドポイントの認証をもう一度実行します。

次の情報を探します。

- RADIUS プローブが属性を受信したことを示すデバッグ：

```
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, ]
```

- 属性が正常に解析されたことを示すデバッグ：

```
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, ]
```

- 属性がフォワーダにより処理されたことを示すデバッグ：

```
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
```

フォワーダは、エンドポイントをその属性データとともに Cisco ISE データベースに保存し、ネットワークで検出された新しいエンドポイントをアナライザに通知します。 アナライザは、エンドポイントをエンドポイント ID グループに分類し、一致プロファイルとともにエンドポイントをデータベースに保存します。

ステップ 5 通常、特定デバイスの既存のコレクションに新しい属性を追加すると、このデバイス/エンドポイントに、新しい属性に基づいて異なるプロファイルを割り当てる必要があるかどうかを確認するため、デバイス/エンドポイントがプロファイリング キューに追加されます。

```
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
```

関連情報

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