

Configurez le capteur de périphérique pour le profilage ISE

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Étape 1. Configuration standard d'AAA](#)

[Étape 2. Configurez le capteur de périphérique](#)

[Étape 3. Configure profilant sur ISE](#)

[Vérifiez](#)

[Dépannez](#)

[Étape 1. Vérifiez les informations collectées par CDP/LLDP](#)

[Étape 2. Cache de capteur de périphérique de contrôle](#)

[Étape 3. Vérifiez si les attributs sont présents en comptabilité de Radius](#)

[Étape 4. Vérifiez le profileur met au point sur ISE](#)

[Informations connexes](#)

[Cisco relatif prennent en charge des discussions de la Communauté](#)

Introduction

Ce document décrit comment configurer le capteur de périphérique, de sorte qu'il puisse être utilisé pour profiler des buts sur ISE. Le capteur de périphérique est une caractéristique des périphériques d'accès. Il laisse collecter des informations sur des points finaux connectés. En grande partie, les informations collectées par le capteur de périphérique peuvent provenir les protocoles suivants :

- Cisco Discovery Protocol (CDP)
- Protocole LLDP (Link Layer Discovery Protocol)
- Protocole DHCP (DHCP)

Sur quelques Plateformes il est possible d'utiliser également le h323, le SIP (protocole SIP), les MDN (résolution de domaine de Multidiffusion) ou les protocoles HTTP. Les possibilités de configuration pour des capacités de capteur de périphérique peuvent varier du protocole au protocole. Comme exemple au-dessus de est disponible sur Cisco Catalyst 3850 avec le logiciel 03.07.02.E.

Une fois que les informations sont collectées, elles peuvent être encapsulées en comptabilité de rayon et envoyer à un serveur de profilage. Dans cette engine de gestion d'identité d'article (ISE) est utilisé en tant que serveur de profilage.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Protocole RADIUS
- Protocoles de CDP, de LLDP et DHCP
- Engine de gestion d'identité de Cisco
- Commutateur Cisco Catalyst 2960

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Correctif 3 de version 1.3 d'engine de gestion d'identité de Cisco
- Version 15.2(2a)E1 du commutateur Cisco Catalyst 2960s
- SCCP 9-3-4-17 de version du téléphone IP 8941 de Cisco

Configurez

Étape 1. Configuration standard d'AAA

Afin de configurer l'authentification, l'autorisation et la comptabilité (AAA), suivent les étapes ci-dessous :

1. Activez l'AAA utilisant la commande d'`aaa new-model` et activez le 802.1X globalement sur le commutateur
2. Configurez le serveur de Radius et activez l'autorisation dynamique (modification de l'autorisation - le CoA)
3. Protocoles de CDP et de LLDP d'enable
4. Ajoutez la configuration d'authentification de switchport

```
!  
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  
!
```

Dans un plus nouveau **radius-server vsa send** de commande de version de logiciel la **comptabilité** est activée par défaut. Si vous ne pouvez pas voir des attributs introduire la comptabilité, vérifiez si la commande dans activé.

Étape 2. Configurez le capteur de périphérique

1. Déterminez quels attributs de CDP/LLDP sont nécessaires pour profiler le périphérique. En cas de téléphone IP 8941 de Cisco vous pouvez utiliser ce qui suit :

- Attribut de SystemDescription de LLDP
- Attribut de CachePlatform de CDP

The screenshot shows the Cisco Identity Services Engine (ISE) Profiling configuration interface. The main area displays the configuration for a Profiler Policy named "Cisco-IP-Phone-8941".

Profiler Policy Configuration:

- 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 (for CiscoIPPhone8941Check2):

- Name: CiscoIPPhone8941Check2
- Description: Check for Cisco IP Phone 8941
- Expression: LLDP:lldpSystemDescription CONTAINS Cisco IP Phone 8941

The left sidebar shows a list of other profiler policies, with "Cisco-IP-Phone-8941" selected.

Pour notre but il serait assez pour obtenir juste un de ceux puisque chacun d'eux fournissent l'augmentation d'usine de certitude de 70 et l'usine minimum de certitude exigée pour être profilé comme Cisco-IP-Phone-8941 est 70 :

The screenshot shows the Cisco Identity Services Engine (ISE) Profiling configuration page for the policy **Cisco-IP-Phone-8941**. The interface includes a navigation menu at the top with options like Home, Operations, Policy, Guest Access, and Administration. Below the menu, there are tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, TrustSec, and Policy Elements. The main content area is divided into a left sidebar showing a list of policies (Cisco-IP-Phone-7940 to Cisco-IP-Phone-8945) and a right pane for the selected policy configuration.

The **Profiler Policy** configuration for **Cisco-IP-Phone-8941** includes the following settings:

- Name:** Cisco-IP-Phone-8941
- Description:** Policy for C
- 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

The **Rules** section contains two rules:

If Condition	Then	Value
CiscoIPPhone8941Check1	Certainty Factor Increases	70
CiscoIPPhone8941Check2	Certainty Factor Increases	70

Buttons for **Save** and **Reset** are located at the bottom of the configuration pane.

Afin d'être profilé en tant que téléphone IP spécifique de Cisco, you need pour remplir des conditions minimum pour tous les profils de parent. Ceci signifie que le profileur doit apparier le Cisco-périphérique (facteur minimal de certitude 10) et le Cisco-IP-téléphone (facteur minimal 20 de certitude). Quoique le profileur apparie ces deux profils, il devrait encore être profilé en tant que téléphone IP spécifique de Cisco puisque chaque modèle de téléphone IP a le facteur minimal de certitude de 70. Le périphérique est assigné au profil pour lequel il a le facteur de certitude le plus élevé.

2. Configurez deux listes de filtre - une pour le CDP et un autre pour le LLDP. Ceux indiquent que ce qui attribue devrait être incluse dans les messages la comptabilité de Radius. Cette étape est facultative

3. Créez deux filtre-spécifications pour le CDP et le LLDP. Dans la spécification de filter vous pouvez l'un ou l'autre indiquer que la liste d'attributs devrait être incluse ou exclue des messages de comptabilité. Dans l'exemple les attributs suivants sont inclus :

- nom du périphérique de CDP
- système-description de LLDP

Vous pouvez configurer des attributs supplémentaires à transmiter par l'intermédiaire de Radius à ISE si nécessaire. Cette étape est également facultative.

4. Ajoutez le périphérique-captteur de commande **informent des tout-modifications**. Il déclenche des mises à jour toutes les fois que TLVs sont ajoutés, modifiés ou retirés pour la session en cours

5. Afin d'envoyer réellement les informations a recueilli par l'intermédiaire de la fonctionnalité de capteur de périphérique, vous doit dire explicitement le commutateur de faire ainsi avec la **comptabilité de périphérique-captteur de commande**

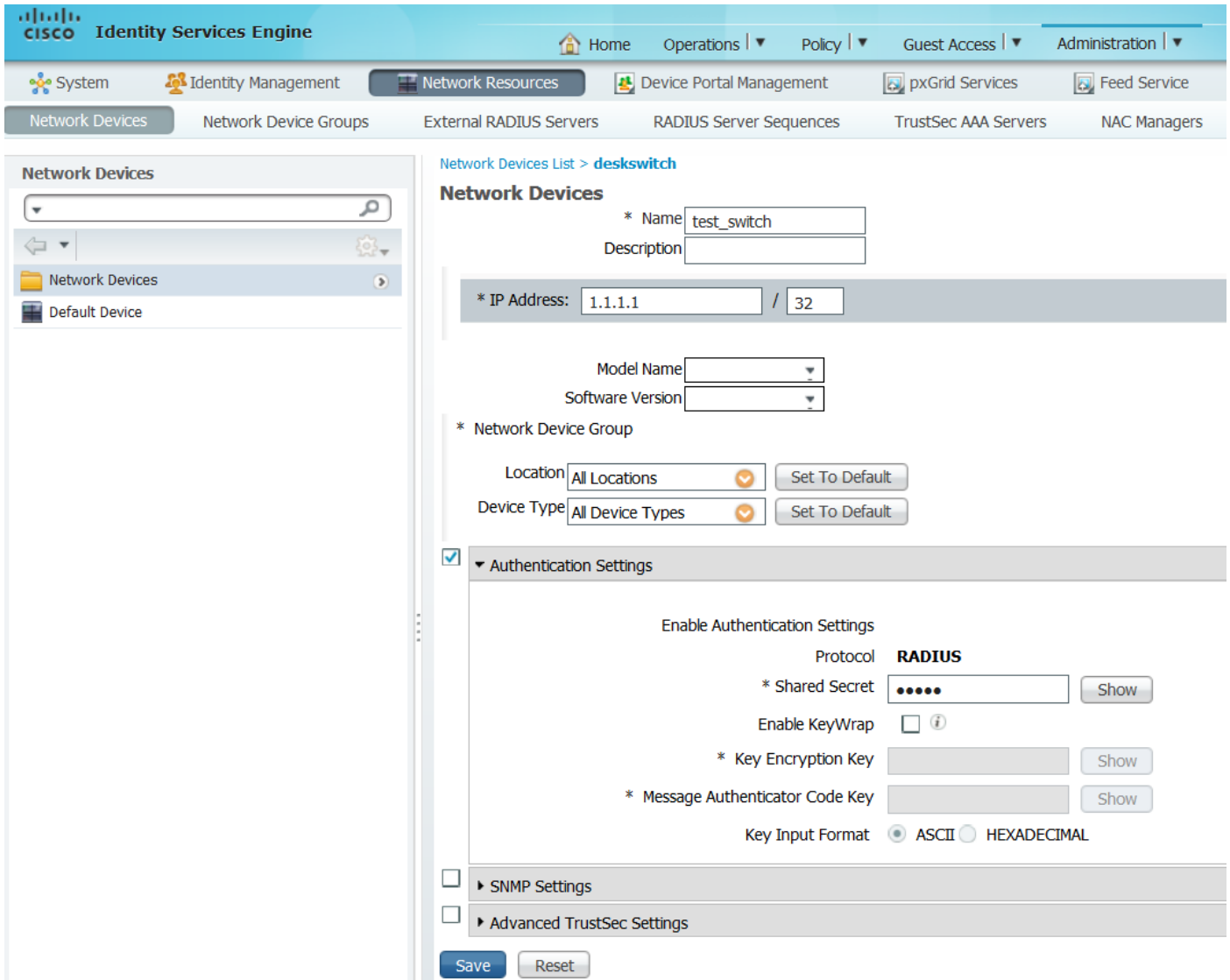
```

!
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 !

```

Étape 3. Configure profilant sur ISE

1. Ajoutez le commutateur comme périphérique de réseau dans des « périphériques d'Administration>Network Resources>Network ». Utilisez la clé de serveur de rayon du commutateur en tant que secret partagé dans des configurations d'authentification :



2. Sonde de Radius d'enable sur le noeud de profilage dans « la configuration node>Profiling d'Administration>System>Deployment>ISE ». Si tous les Noeuds RPC sont utilisés pour le profilage, activez la sonde sur tous :

Deployment

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
-

Save | Reset

3. Configurez les règles d'authentification ISE. Dans l'exemple les règles d'authentification par défaut préconfigurées sur ISE sont utilisées :

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

<input checked="" type="checkbox"/>	MAB	: If Wired_MAB OR Wireless_MAB	Allow Protocols : Default Network Access
<input checked="" type="checkbox"/>	Default	: use Internal Endpoints	
<input checked="" type="checkbox"/>	Dot1X	: If Wired_802.1X OR Wireless_802.1X	Allow Protocols : Default Network Access
<input checked="" type="checkbox"/>	Default	: use All_User_ID_Stores	
<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Network Access and use : All_User_ID_Stores	

4. Configurez les règles d'autorisation ISE. « La règle des téléphones IP profilés de Cisco est utilisée, qui est préconfigurée sur ISE :

Identity Services Engine

Home | Operations | Policy | Guest Access | Administration

Authentication | **Authorization** | Profiling | Posture | Client Provisioning | TrustSec | Policy Elements

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

Vérifiez

Afin de vérifier si le profilage fonctionne correctement, référez-vous s'il vous plaît à « Operations>Authentications » sur ISE :

Identity Services Engine

Home | Operations | Policy | Guest Access | Administration

Authentications | Reports | Endpoint Protection Service | Troubleshoot

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

Show Live Sessions | Add or Remove Columns | Refresh | Reset Repeat Counts | Refresh

Time	Status	Details	R...	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Identity Group	Event
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

D'abord le périphérique a été authentifié utilisant le MAB (18:49:00). Dix secondes plus tard (18:49:10) il reprofiled comme Cisco-périphérique et finalement après 42 secondes puisque les premières authentications (18:49:42) il ont reçu le profil Cisco-IP-Phone-8941. En conséquence ISE renvoie la particularité de profil d'autorisation pour des Téléphones IP (Cisco_IP_Phones) et l'ACL téléchargeable qui permet tout le trafic (IP d'autorisation tout). Veuillez noter que dans ce scénario le périphérique inconnu a accès de base au réseau. Il peut être réalisé en ajoutant le MAC address à la base de données interne de point final ISE ou en permettant l'accès au réseau très de base pour les périphériques précédemment inconnus.

Le profilage initial a pris environ 40 secondes dans cet exemple. Sur la prochaine authentification ISE déjà connaît le profil et corrige des attributs (autorisation de joindre le domaine de Voix et le DAcl) est appliqué immédiatement, à moins qu'ISE reçoive nouveaux/mis à jour attributs et il a besoin reprofile du périphérique de nouveau.

The screenshot shows the Cisco Identity Services Engine (ISE) dashboard. At the top, there are navigation tabs for Home, Operations, Policy, Guest Access, and Administration. Below these are sub-tabs for Authentications, Reports, Endpoint Protection Service, and Troubleshoot. A summary row displays four metrics: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (0), and Client Stopped Responses (0). Below this is a table of authentication events.

Time	Status	Details	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Identity Group	Event
2015-11-25 18:55:39.772	Info		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	Success		#ACSACL#-IP-PE							DACL Download Succeeded
2015-11-25 18:55:38.707	Success		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	Success		#ACSACL#-IP-PE							DACL Download Succeeded
2015-11-25 18:49:42.417	Success		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

Dans le « point final d'Administration>Identity Management>Identities>Endpoints>tested » vous pouvez voir que ce qui attribue un peu ont été collectés par la sonde de Radius et ce que sont leurs valeurs :

The screenshot shows the Cisco Identity Services Engine (ISE) interface for the 'Identities' section. The left sidebar shows a search bar with 'admin' and a list of categories: Users, Endpoints, and Latest Manual Network Scan Results. The main area displays a list of attributes for an endpoint.

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

Comme vous pouvez observer tout le facteur de certitude calculé est 210 dans ce scénario. Il est livré le front le fait que le point final a apparié également le profil de Cisco-périphérique (avec le facteur total de certitude de 30) et le profil de Cisco-IP-téléphone (avec le facteur total de certitude de 40). Puisque le profileur a apparié les deux conditions dans le profil Cisco-IP-Phone-8941, le facteur de certitude pour ce profil est 140 (70 pour chaque attribut selon profiler la stratégie). Pour résumer : $30+40+70+70=210$.

Dépannez

Étape 1. Vérifiez les informations collectées par CDP/LLDP

```
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:
```

```
  100baseT(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 vous ne pouvez voir aucune données collectées pour vérifier ce qui suit :

- Vérifiez l'état de session d'authentification sur le commutateur (il devrait être réussi) :

```
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: 0AE51820000002040099C216
      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
```

- Vérifiez si des protocoles de CDP et de LLDP sont activés. Vérifiez s'il y a des commandes de non-par défaut concernant CDP/LLDP/etc. et comment ceux peuvent affecter la récupération d'attribut du point final

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

- Vérifiez dans le guide de configuration pour votre point final s'il prend en charge CDP/LLDP/etc

Étape 2. Cache de capteur de périphérique de contrôle

```
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

```

Si vous ne voyez pas aucune donnée dans ce domaine ou les informations n'est complète vérifiez des commandes de « périphérique-captteur », en particulier des filters-list et des filtre-spécifications.

Étape 3. Vérifiez si les attributs sont présents en comptabilité de Radius

Vous pouvez vérifier cela utilisant la « commande des debugs radius sur le commutateur ou exécuter la capture de paquet entre le commutateur et l'ISE.

Radius mettent au point :

```

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

```

Capture de paquet :

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)

Filter	Expression...	Clear	Apply	Save	Filter	Filter
radius.code==4						

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

Étape 4. Vérifiez le profileur met au point sur ISE

Si les attributs étaient envoyés du commutateur, il est possible de vérifier s'ils étaient reçus sur ISE. Afin de vérifier ceci, activez s'il vous plaît le profileur met au point pour le noeud correct RPC (log Configuration>PSN>profilier>debug d'Administration>System>Logging>Debug) et exécute l'authentification du point final une fois de plus.

Look for après les informations :

- Debug indiquant que la sonde de rayon reçue attribue :

```
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 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=0AE51820000002040099C216,
AllowedProtocolMatchedRule=MAB, Location=Location#All Locations, Device Type=Device Type#All
Device Types, ]
```

- Debug indiquant que des attributs ont été avec succès analysés :

```
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 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=0AE51820000002040099C216,
AllowedProtocolMatchedRule=MAB, Location=Location#All Locations, Device Type=Device Type#All
Device Types, ]
```

- Débuggez indiquer que des attributs sont traités par l'expéditeur :

```
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
```

Un expéditeur enregistre des points finaux dans la base de données de Cisco ISE avec leurs données d'attributs, et puis informe l'analyseur de nouveaux points finaux détectés sur votre réseau. L'analyseur classe des points finaux à l'identité de point final groupe et enregistre des points finaux avec les profils appariés dans la base de données.

Étape 5. Typiquement après que de nouveaux attributs soient ajoutés à la collection existante pour l'appareil spécifique, ces périphérique/point final est ajouté à profiler la file d'attente afin de vérifier si elle doit être assignée le profil différent basé sur de nouveaux attributs :

```
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
```

[Informations connexes](#)

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