

Apparaatsensor configureren voor ISE-profilering

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Stap 1. Standaard AAA-configuratie](#)

[Stap 2. Apparaatsensor configureren](#)

[Stap 3. Het maken van profielen op ISE configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Stap 1. Controleer de informatie die door CDP/LLDP wordt verzameld](#)

[Stap 2: Controleer het geheugen van de apparaatsensor](#)

[Stap 3: Controleer of de eigenschappen in RADIUS-accounting aanwezig zijn](#)

[Stap 4. Controleer de profielen op ISE](#)

[Gerelateerde informatie](#)

[Gerelateerde Cisco Support Community-discussies](#)

Inleiding

Dit document beschrijft hoe u de sensor van het apparaat moet configureren, zodat het gebruikt kan worden voor profielen op ISE. Apparaatsensor is een kenmerk van toegangsapparaten. Hiermee kan informatie worden verzameld over verbonden endpoints. Meestal kan de informatie die door Apparaatsensor wordt verzameld, afkomstig zijn van de volgende protocollen:

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

Op sommige platforms kan ook H323, SIP (Session Initiation Protocol), MDNS (Multicast Domain Solutions) of HTTP-protocollen worden gebruikt. De configuratiemogelijkheden voor de mogelijkheden van de sensor van het apparaat kunnen variëren van protocol tot protocol. Als een voorbeeld hierboven is beschikbaar op Cisco Catalyst 3850 met software 30.07.02.E.

Zodra de informatie wordt verzameld, kan deze in een Straalboekhouding worden ingekapseld en naar een profileringsserver worden verzonden. In dit artikel Identity Services Engine (ISE) wordt gebruikt als een profileringsserver.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Radius-protocol
- CDP-, LLDP- en DHCP-protocollen
- Cisco Identity Services Engine
- Cisco Catalyst switch 2960

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Identity Services Engine versie 1.3-pleister 3
- Cisco Catalyst switch 2960s versie 15.2(2a)E1
- Cisco IP-telefoon 8941 versie SCCP 9-3-4-17

Configureren

Stap 1. Standaard AAA-configuratie

Om verificatie, autorisatie en accounting (AAA) te configureren volgt u de onderstaande stappen:

1. AAA inschakelen met de opdracht **nieuw model** en 802.1X mondiaal inschakelen op de switch
2. Het configureren van een radiogateway en het inschakelen van dynamische autorisatie (wijziging van autorisatie - CoA)
3. Schakel CDP- en LLDP-protocollen in
4. Voeg configuratie van switchingverificatie toe

```
!  
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  
!
```

In nieuwere versie van de software is de opdracht `straal-server vsa` standaard ingeschakeld om accounting te verzenden. Als u geen eigenschappen kunt zien verzenden in accounting, controleer of de opdracht in ingeschakeld is.

Stap 2. Apparaatsensor configureren

1. Bepaal welke eigenschappen van CDP/LLDP nodig zijn om het apparaat te profileren. U kunt als volgt een Cisco IP-telefoon 8941 gebruiken:

- Eigenschappen LLDP-systeem
- CDP-cachepatriEFAARD

The screenshot shows the Cisco Identity Services Engine (ISE) Profiling configuration interface. The main window displays the configuration for a Profiler Policy named 'Cisco-IP-Phone-8941'. The configuration includes the following fields:

- 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

Below the configuration fields, there are two rules defined:

- Rule 1:** If Condition: CiscoIPPhone8941Check1
- Rule 2:** If Condition: CiscoIPPhone8941Check2

A 'Conditions Details' pop-up window is open, showing the details for 'CiscoIPPhone8941Check2':

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

The interface also includes a 'Profiling' sidebar on the left with a list of policies, and a 'Rules' section at the bottom with 'Save' and 'Reset' buttons.

Voor ons doel zou het genoeg zijn om slechts één van deze te verkrijgen aangezien beiden de Verzekeringsfabriek van 70 en de Minimale Fabriek van de Veiligheid voorzien die vereist zijn om als Cisco-IP-telefoon 8941 70 is:

The screenshot shows the Cisco Identity Services Engine (ISE) Profiling configuration interface. On the left, a list of policies is shown, with 'Cisco-IP-Phone-8941' selected. The main configuration area is titled 'Profiler Policy' and includes the following fields:

- * 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

Under the 'Rules' section, two rules are defined:

If Condition	Then	Value
CiscolPPhone8941Check1	Certainty Factor Increases	70
CiscolPPhone8941Check2	Certainty Factor Increases	70

Buttons for 'Save' and 'Reset' are located at the bottom of the configuration area.

Wilt u als specifieke Cisco IP-telefoon worden weergegeven, dan hebt u eerst aan de minimumvoorwaarden voor alle parent-profielen voldaan. Dit betekent dat het profiel moet overeenkomen met het Cisco-apparaat (min. Beveiligingsfactor 10) en Cisco-IP-telefoon (min. Veiligheidsfactor 20). Zelfs al komt profiler die twee profielen aan, zou het nog steeds als specifieke Cisco IP telefoon moeten worden geprofileerd aangezien elk IP telefoonmodel min heeft. Veiligheidsfactor 70. Apparaat wordt toegewezen aan het profiel waarvoor het de hoogste veiligheidsfactor heeft.

2. Het configureren van twee filterlijsten - één voor CDP en één voor LLDP. Deze geven aan welke eigenschappen moeten worden opgenomen in Radius accounting boodschappen. Deze stap is optioneel

3. Maak twee filterspecificaties voor CDP en LLDP. In filter - specificaties kunt u aangeven dat de lijst van eigenschappen moet worden opgenomen of uitgesloten van de boekhoudkundige berichten. In het voorbeeld worden de volgende eigenschappen opgenomen:

- apparaatnaam van CDP
- systeembeschrijving van LLDP

U kunt indien nodig aanvullende eigenschappen configureren die via Straal naar ISE worden verzonden. Deze stap is ook optioneel.

4. **Waarschuwing** van de commando(**machine**). Er worden updates gestart als TLV's worden toegevoegd, aangepast of verwijderd voor de huidige sessie

5. Om de informatie die via de functionaliteit van de sensor is verzameld, daadwerkelijk te kunnen verzenden, moet u de schakelaar expliciet op de **rekenmachine** van de opdrachtgever **vermelden**

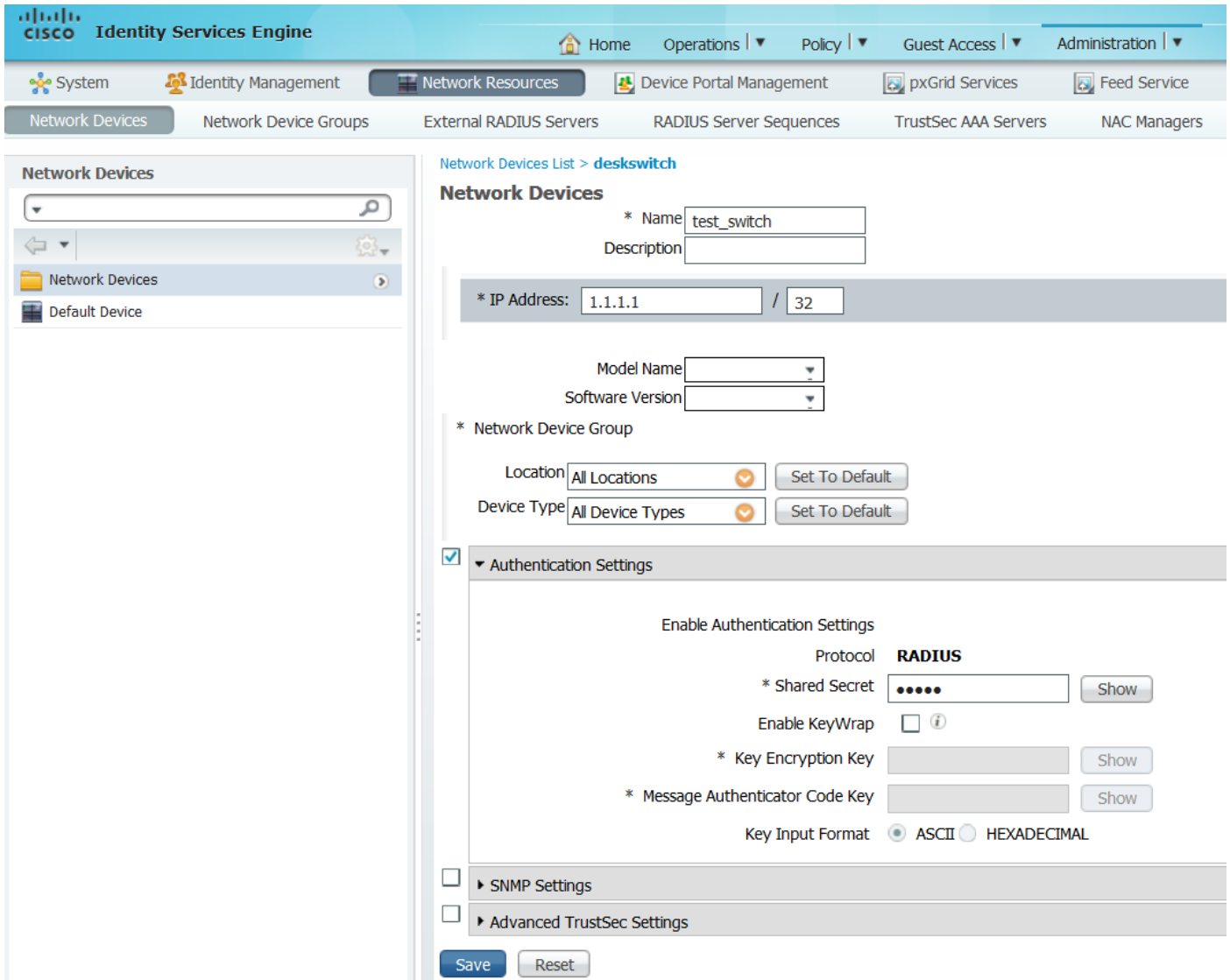
```

!
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 !

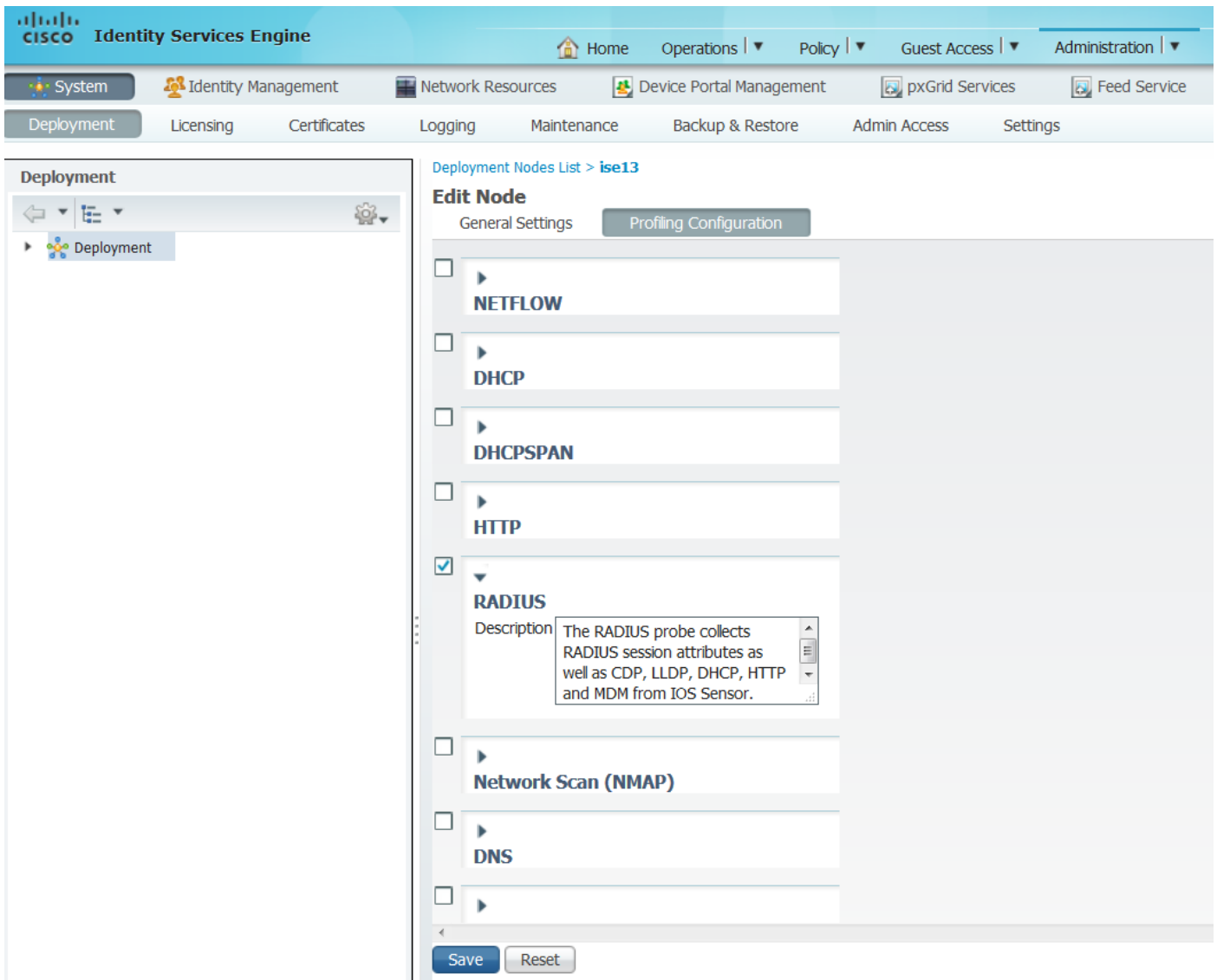
```

Stap 3. Het maken van profielen op ISE configureren

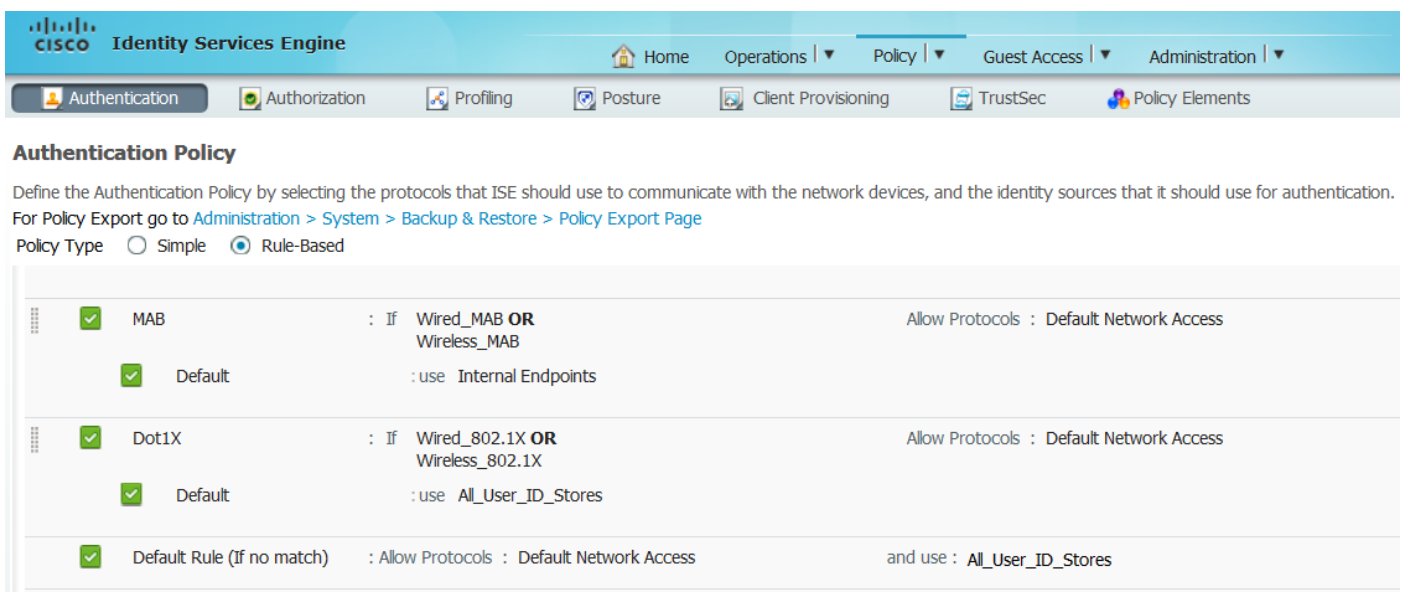
1. Voeg switch als een netwerkkapparaat toe in "Beheer>Netwerkbronnen>Netwerkkapparaten". Gebruik de Straalservoets van de schakelaar als gedeeld geheim in Verificatieinstellingen:



2. Schakel RADIUS-toets in op het profileringsknooppunt in "Beheer>Systeem>Implementatie>ISE-knooppunt>Configuratie profileren". Als alle PSN-knooppunten gebruikt zouden moeten worden voor het profileren, laat u de sonde op al deze toetsen in:



3. Configuratie van ISE-verificatieregels. In het voorbeeld worden de standaardverificatieregels gebruikt die vooraf op ISE zijn ingesteld:



4. Instellen van ISE-vergunningsregels. De regel "Gecombineerde Cisco IP-telefoons" wordt gebruikt, die op ISE is geconfigureerd:

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

Verifiëren

Om te controleren of het profiel correct werkt, raadpleeg "Operations>Authentications" op ISE:

Identity Services Engine

Home | Operations | Policy | Guest Access | Administration

Authentications | Reports | Endpoint Protection Service | Troubleshoot

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

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							DAACL 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 Cs..	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

Eerst werd het apparaat geauthentiseerd met MAB (18:49:00). Tien seconden later (18:49:10) werd het opnieuw gepropageerd als Cisco-apparaat en definitief na 42 seconden sinds eerste authenticaties (18:49:42) het Cisco-IP-telefoon-8941 profiel ontvangen. Als resultaat hiervan geeft ISE de specificiteit van het machtigingsprofiel voor IP telefoons (Cisco_IP_telefoons) en downloadbare ACL terugh die al verkeer toelaat (sta om het even welk toe). In dit scenario heeft het onbekende apparaat basistoegang tot het netwerk. Dit kan worden bereikt door het toevoegen van mac-adres aan ISE interne eindpuntdatabase of het toestaan van zeer basale netwerktoegang voor voorheen onbekende apparaten.

In dit voorbeeld duurde de eerste profilering ongeveer 40 seconden. Op de volgende authenticatie weet ISE reeds het profiel en de juiste eigenschappen (toestemming om zich aan te sluiten bij stemdomein en DAACL) worden onmiddellijk toegepast, tenzij ISE nieuwe/bijgewerkte eigenschappen ontvangt en het het apparaat opnieuw moet beschrijft.

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

In "Administration>Identity Management>Identities>Endpoints>testeindpunt" kunt u zien welke eigenschappen door een RADIUS-test zijn verzameld en wat de waarden ervan zijn:

Identities	
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
ldpSystemDescription	Cisco IP Phone 8941, V3, SCCP 9-3-4-17

Zoals je kunt zien is de totale berekende zekerheidsfactor 210 in dit scenario. Het komt uit het feit dat het eindpunt ook profiel van Cisco-apparaat (met totale helderheidsfactor 30) en het profiel van Cisco-IP-telefoon (met totale zekerheidsfactor 40) overeenkwam. Aangezien profiler aan beide voorwaarden in profiel voldeed, is Cisco-IP-telefoon-8941, is de betrouwbaarheidsfactor voor dit profiel 140 (70 voor elke eigenschap volgens het profileringsbeleid). Samenvattend: 30+40+70+70=210.

Problemen oplossen

Stap 1. Controleer de informatie die door CDP/LLDP wordt verzameld

```
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

Indien u geen verzamelde gegevens kunt zien, verifieert u het volgende:

- Controleer de status van de authenticatiesessie op de schakelaar (dit moet een succes zijn):

```
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
```

- Controleer of CDP- en LLDP-protocollen zijn ingeschakeld. Controleer of er geen standaardopdrachten zijn voor CDP/LLDP/enzovoort. en hoe die het ophalen van eigenschap vanuit het eindpunt kunnen beïnvloeden

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

- Controleer in de configuratiehandleiding voor uw eindpunt of deze CDP/LLDP/enz. ondersteunt

Stap 2: Controleer het geheugen van de apparaatsensor

```
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

```

Als u geen gegevens in dit veld ziet of als de informatie niet compleet is, controleert u de opdrachten 'apparaatsensor', met name de filterlijsten en de filterspecificaties.

Stap 3: Controleer of de eigenschappen in RADIUS-accounting aanwezig zijn

U kunt controleren of het gebruik van de opdracht 'debug Straal' op de schakelaar of het uitvoeren van pakketvastlegging tussen schakelaar en ISE.

Straal debug:

```

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

```

PacketCapture:

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

Stap 4. Controleer de profielen op ISE

Als de eigenschappen vanuit de schakelaar werden verzonden, is het mogelijk om te controleren of ze op ISE werden ontvangen. Om dit te controleren, schakelt u profilerdefecten in voor de juiste PSN-knooppunten (Administratie>Systeem>Vastlegging>Meld loggen>Logconfiguratie>PSN>Profiler>debug) en voert u de verificatie van het eindpunt nog een keer uit.

Bekijk de volgende informatie:

- Debug die aangeeft dat de Straalonde eigenschappen heeft ontvangen:

```
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=0AE5182000002040099C216, 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=0AE5182000002040099C216,
AllowedProtocolMatchedRule=MAB, Location=Location#All Locations, Device Type=Device Type#All
```

Device Types,]

- Debug die aangeeft dat eigenschappen succesvol zijn geparkeerd:

```
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
```

- Debug die aangeeft dat eigenschappen door expediteur worden verwerkt:

```
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
```

Een expediteur slaat endpoints in de Cisco ISE-database op samen met hun eigenschappen gegevens, en stelt de analyzer vervolgens in kennis van nieuwe endpoints die op uw netwerk zijn gedetecteerd. De analyzer classificeert eindpunten aan de identiteitsgroepen van endpoints en slaat eindpunten op met de aangepaste profielen in de database.

Stap 5. Meestal nadat nieuwe eigenschappen aan de bestaande verzameling voor specifieke apparatuur zijn toegevoegd, wordt dit apparaat/eindpunt toegevoegd aan de profileringsrij om te controleren of het verschillende profiel moet worden toegewezen op basis van nieuwe eigenschappen:

```
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
```

Gerelateerde informatie

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