

Konfigurieren des Gerätesensors für ISE-Profilerstellung

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Schritt 1: Standard-AAA-Konfiguration](#)

[Schritt 2: Konfigurieren des Gerätesensors](#)

[Schritt 3: Konfigurieren von Profilen auf der ISE](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Schritt 1: Überprüfung der von CDP/LLDP erfassten Informationen](#)

[Schritt 2: Gerätesenscache überprüfen](#)

[Schritt 3: Überprüfen Sie, ob Attribute im Radius-Accounting vorhanden sind.](#)

[Schritt 4: Überprüfung des Profiler-Debug auf der ISE](#)

[Zugehörige Informationen](#)

[Ähnliche Diskussionen in der Cisco Support Community](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie den Gerätesensor so konfigurieren, dass er für die Profilerstellung auf der ISE verwendet werden kann. Der Gerätesensor ist eine Funktion von Zugriffsgeräten. Es ermöglicht das Sammeln von Informationen über verbundene Endpunkte. Die von Device Sensor erfassten Informationen können hauptsächlich von den folgenden Protokollen stammen:

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

Auf einigen Plattformen können auch H323-, SIP- (Session Initiation Protocol), MDNS- (Multicast Domain Resolution) oder HTTP-Protokolle verwendet werden. Die Konfigurationsmöglichkeiten für Gerätesensorfunktionen können von Protokoll zu Protokoll variieren. Ein Beispiel oben ist auf Cisco Catalyst 3850 mit Software 03.07.02.E verfügbar.

Nachdem die Informationen gesammelt wurden, können sie in die Radius-Accounting eingekapselt und an einen Profiling-Server gesendet werden. In diesem Artikel wird Identity Service Engine (ISE) als Profiling-Server verwendet.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Radius-Protokoll
- CDP-, LLDP- und DHCP-Protokolle
- Cisco Identity Service Engine
- Cisco Catalyst Switch 2960

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Identity Service Engine Version 1.3 Patch 3
- Cisco Catalyst Switch der Serie 2960, Version 15.2(2a)E1
- Cisco IP-Telefon 8941, Version SCCP 9-3-4-17

Konfigurieren

Schritt 1: Standard-AAA-Konfiguration

Führen Sie die folgenden Schritte aus, um Authentication, Authorization and Accounting (AAA) zu konfigurieren:

1. Aktivieren Sie AAA mithilfe **eines neuen** Befehls, und aktivieren Sie 802.1X global auf dem Switch.
2. Radius-Server konfigurieren und dynamische Autorisierung aktivieren (Autorisierungsänderung - CoA)
3. Aktivierung von CDP- und LLDP-Protokollen
4. SwitchPort-Authentifizierungskonfiguration hinzufügen

```
!  
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 neueren Softwareversionen ist der Befehl radius-server vsa send accounting standardmäßig aktiviert. Wenn Attribute nicht in Accounting gesendet werden, überprüfen Sie, ob der Befehl aktiviert ist.

Schritt 2: Konfigurieren des Gerätesensors

1. Bestimmen Sie, welche Attribute von CDP/LLDP für das Profiling des Geräts benötigt werden. Für das Cisco IP-Telefon 8941 können Sie Folgendes verwenden:

- LLDP SystemDescription-Attribut
- CDP CachePlatform-Attribut

The screenshot displays the Cisco Identity Services Engine (ISE) Profiling configuration interface. The main area shows 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

The 'Rules' section shows two conditions:

- If Condition:** CiscoIPPhone8941Check1
- If Condition:** CiscoIPPhone8941Check2

A 'Conditions Details' popup is open for CiscoIPPhone8941Check2, showing the following details:

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

Für unseren Zweck reicht es aus, nur eines davon zu erhalten, da beide einen Zuwachs von "Sicherer Betrieb" um 70 und eine Mindestsicherungs-Factory bieten, die als Cisco-IP-Telefon-8941 mit 70 eingestuft werden muss:

The screenshot shows the Cisco ISE Profiler Policy configuration interface. The main configuration area includes:

- 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 entries:

If Condition	Then	Value
CiscIPPhone8941Check1	Certainty Factor Increases	70
CiscIPPhone8941Check2	Certainty Factor Increases	70

Um als spezifisches Cisco IP-Telefon eingestuft zu werden, müssen Sie die Mindestanforderungen für alle übergeordneten Profile erfüllen. Das bedeutet, dass die Profilerstellung auf Cisco Geräte abgestimmt sein muss (min. Sicherheitsfaktor 10) und Cisco-IP-Telefon (mind. Sicherheitsfaktor 20). Obwohl die Profiler diesen beiden Profilen entsprechen, sollte sie dennoch als bestimmtes Cisco IP-Telefon eingestuft werden, da jedes IP-Telefonmodell über eine Mindestanzahl verfügt. Sicherheitsfaktor 70. Das Gerät wird dem Profil zugewiesen, für das es den höchsten Sicherheitsfaktor besitzt.

2. Konfigurieren Sie zwei Filterlisten: eine für CDP und eine weitere für LLDP. Diese geben an, welche Attribute in Radius-Accounting-Nachrichten enthalten sein sollen. Dieser Schritt ist optional.

3. Erstellen Sie zwei Filterspezifikationen für CDP und LLDP. In der Filter-Spezifikation können Sie entweder angeben, dass eine Liste von Attributen in die Accounting-Meldungen aufgenommen oder ausgeschlossen werden soll. Im Beispiel sind folgende Attribute enthalten:

- Gerätenamen von CDP
- Systembeschreibung aus LLDP

Sie können bei Bedarf weitere Attribute für die Übertragung über Radius an die ISE konfigurieren. Dieser Schritt ist ebenfalls optional.

4. Hinzufügen von Befehls-**Geräteerkennung benachrichtigt alle Änderungen**. Updates werden ausgelöst, wenn TLVs zur aktuellen Sitzung hinzugefügt, geändert oder entfernt werden.

5. Um die über die Funktion "Device Sensor" (Geräteerkennung) gesammelten Informationen tatsächlich zu senden, müssen Sie dem Switch dies explizit mithilfe der **Erfassung von Befehlsensoren** erklären.

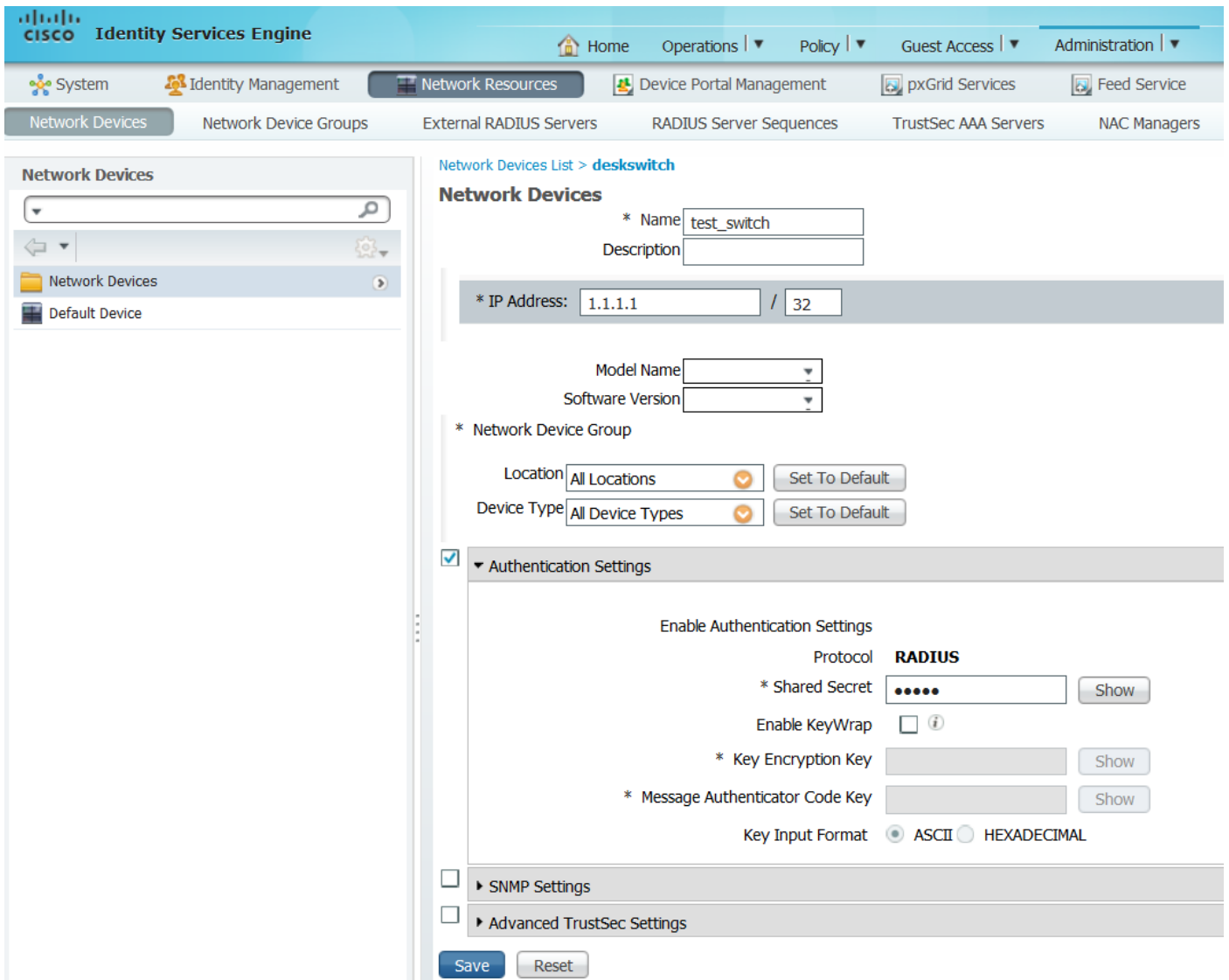
```

!
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 !

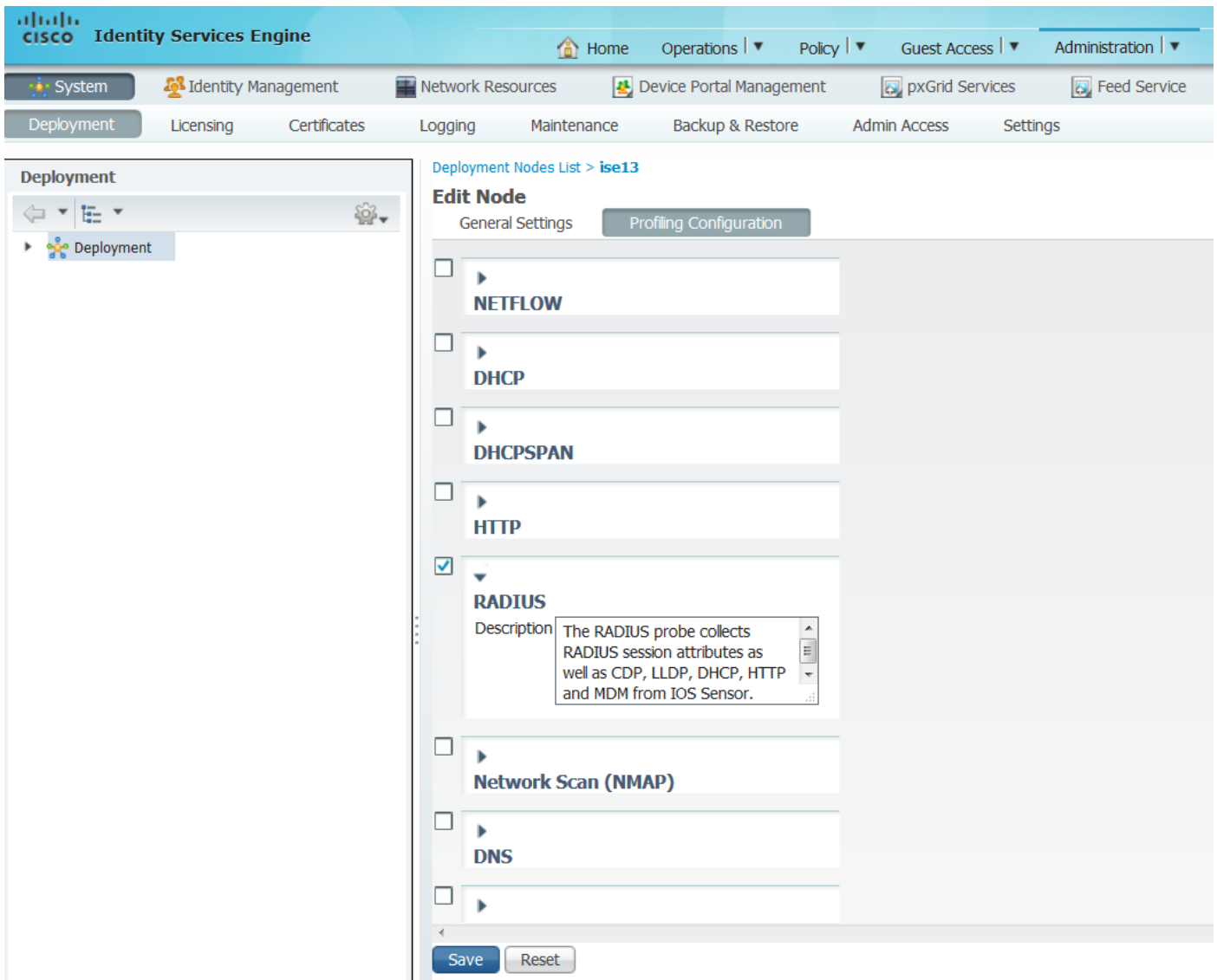
```

Schritt 3: Konfigurieren von Profilen auf der ISE

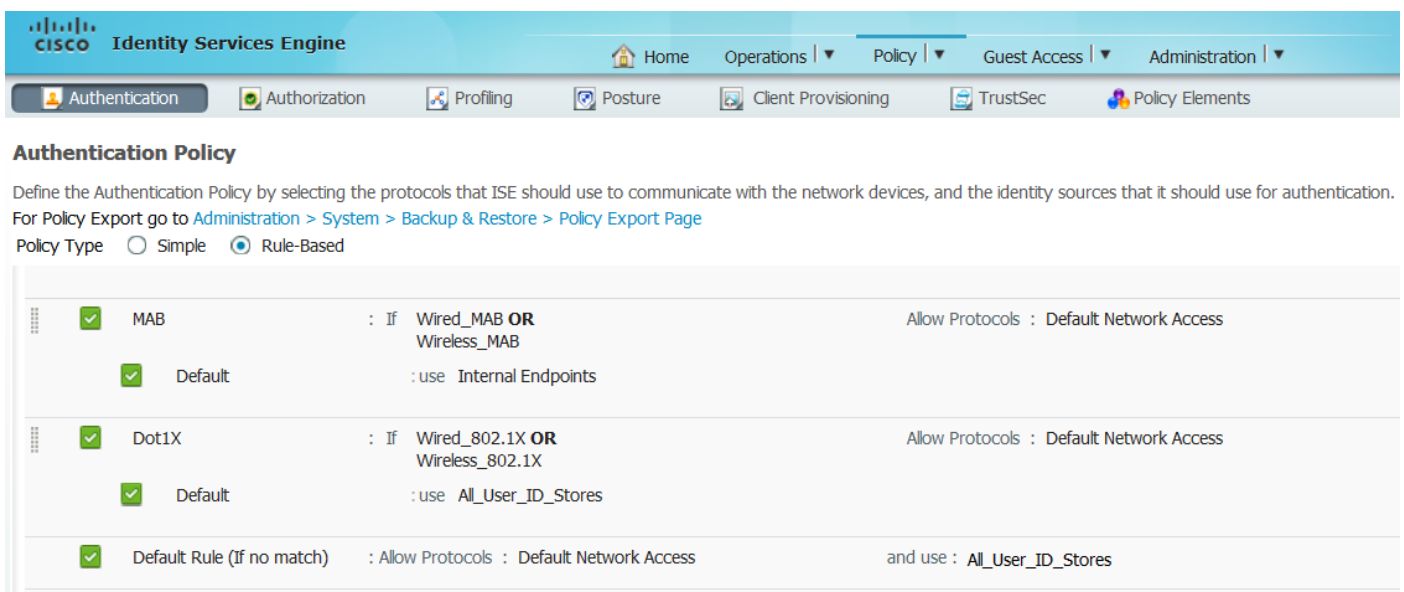
1. Fügen Sie als Netzwerkgerät Switch unter "Administration>Network Resources>Network Devices" hinzu. Verwenden Sie den Radius-Serverschlüssel vom Switch in den Authentifizierungseinstellungen als gemeinsam genutzter geheimer Schlüssel:



2. Aktivieren Sie RadiusSonde auf dem Profilierungsknoten unter "Administration>System>Deployment>ISE node>Profiling Configuration". Wenn alle PSN-Knoten für die Profilerstellung verwendet werden sollen, aktivieren Sie die Funktion für alle:



3. Konfigurieren Sie die ISE-Authentifizierungsregeln. Im Beispiel werden die auf der ISE vorkonfigurierten Standardauthentifizierungsregeln verwendet:



4. Konfigurieren der ISE-Autorisierungsregeln Die auf der ISE vorkonfigurierte Regel "Profiled Cisco IP Phones" wird verwendet:

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

Überprüfen

Um zu überprüfen, ob die Profilerstellung ordnungsgemäß funktioniert, lesen Sie "Operations>Authentications" (Vorgänge > Authentifizierungen) zur 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

Zuerst wurde das Gerät mit MAB authentifiziert (18:49:00). Zehn Sekunden später (18:49:10) wurde es als Cisco-Gerät neu eingestuft und nach 42 Sekunden seit der ersten Authentifizierung (18:49:42) erhielt es das Profil Cisco-IP-Phone-8941. Infolgedessen gibt die ISE ein für IP-Telefone spezifisches Autorisierungsprofil (Cisco_IP_Phones) und eine herunterladbare ACL zurück, die den gesamten Datenverkehr zulässt (IP-Adressen aller Art zulassen). Bitte beachten Sie, dass in diesem Szenario das unbekannte Gerät über einen Basiszugriff auf das Netzwerk verfügt. Dies kann durch das Hinzufügen einer MAC-Adresse zur internen ISE-Endpunktdatenbank oder das Zulassen eines sehr einfachen Netzwerkzugriffs für zuvor unbekannte Geräte erreicht werden.

Die erste Profilerstellung dauerte in diesem Beispiel etwa 40 Sekunden. Bei der nächsten Authentifizierung kennt die ISE bereits das Profil, und die richtigen Attribute (Berechtigung zum Beitritt zur Sprachdomäne und zur DACL) werden sofort angewendet, es sei denn, die ISE erhält neue/aktualisierte Attribute und sie muss das Gerät erneut einem Profil zuordnen.

Cisco 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 Respo: 0

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

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

Unter "Administration>Identity Management>Identities>Endpoints>Getestete Endpunkte" können Sie sehen, welche Attribute von RadiusSonde gesammelt wurden und welche Werte sie haben:

Cisco Identity Services Engine

Home | Operations | Policy | Guest Access | Administration

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Identities

admin

- Users
- Endpoints
- Latest Manual Network Scan Results

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

Wie Sie sehen können, ist der berechnete Gesamtfaktor für Sicherheit in diesem Szenario 210. Es liegt daran, dass das Endgerät dem Cisco-Device-Profil (mit einem Gesamtsicherheitsfaktor von 30) und dem Cisco-IP-Telefon-Profil (mit einem Gesamtsicherheitsfaktor von 40) entspricht. Da der Profiler beide Bedingungen im Profil Cisco-IP-Phone-8941 erfüllte, beträgt der Sicherheitsfaktor für dieses Profil 140 (70 für jedes Attribut gemäß Profilerstellungsrichtlinie). Zusammenfassung: 30+40+70+70=210.

Fehlerbehebung

Schritt 1: Überprüfung der von CDP/LLDP erfassten Informationen

```
switch#sh cdp neighbors gl/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 gl/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

Wenn keine der gesammelten Daten angezeigt wird, überprüfen Sie Folgendes:

- Überprüfen Sie den Status der Authentifizierungssitzung auf dem Switch (sollte erfolgreich sein):

```
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
```

- Überprüfen Sie, ob CDP- und LLDP-Protokolle aktiviert sind. Überprüfen Sie, ob nicht standardmäßige Befehle für CDP/LLDP/etc. vorhanden sind. und wie diese den Attributabruf vom Endpunkt beeinflussen können

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

- Überprüfen Sie im Konfigurationsleitfaden für Ihr Endgerät, ob CDP/LLDP/etc. unterstützt wird.

Schritt 2: Gerätesenscache überprüfen

```

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

```

Wenn Sie keine Daten in diesem Feld sehen oder Informationen nicht vollständig sind, überprüfen Sie die Befehle 'Device-Sensor', insbesondere Filterlisten und Filterspezifikationen.

Schritt 3: Überprüfen Sie, ob Attribute im Radius-Accounting vorhanden sind.

Sie können überprüfen, ob der Befehl 'debug radius' auf dem Switch oder die Paketerfassung zwischen Switch und ISE verwendet wird.

Radius-Debuggen:

```

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

```

Paketerfassung:

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
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						

Schritt 4: Überprüfung des Profiler-Debug auf der ISE

Wenn die Attribute vom Switch gesendet wurden, kann überprüft werden, ob sie auf der ISE empfangen wurden. Um dies zu überprüfen, aktivieren Sie bitte die Profiler-Debug für den richtigen PSN-Knoten (Administration>System>Logging>Debug Log Configuration>PSN>Profiler>debug) und führen Sie die Authentifizierung des Endpunkts noch einmal durch.

Suchen Sie nach folgenden Informationen:

- Debug, der angibt, dass die RADIUS-Sonde Attribute empfangen hat:

```
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, ]
```

- Debuggen, das angibt, dass Attribute erfolgreich analysiert wurden:

```
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, der angibt, dass Attribute von Forwarder verarbeitet werden:

```
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
```

Ein Forwarder speichert Endpunkte zusammen mit ihren Attributdaten in der Cisco ISE-Datenbank und benachrichtigt den Analyzer dann über neue Endpunkte, die in Ihrem Netzwerk erkannt wurden. Der Analyzer klassifiziert Endpunkte in die Endpunkt-Identitätsgruppen und speichert Endpunkte mit den entsprechenden Profilen in der Datenbank.

Schritt 5: Wenn der vorhandenen Auflistung für ein bestimmtes Gerät neue Attribute hinzugefügt werden, wird dieses Gerät/Endgerät in der Profilerstellungswarteschlange hinzugefügt, um zu überprüfen, ob dem Gerät je nach neuen Attributen ein anderes Profil zugewiesen werden muss:

```
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

Zugehörige Informationen

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