Configurazione di Device Sensor per la profilatura ISE

Sommario

Introduzione

In questo documento viene descritto come configurare Device Sensor in modo che possa essere usato a scopo di profiling su ISE.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Protocollo Radius
- Protocollo CDP (Cisco Discovery Protocol), LLDP (Link Layer Discovery Protocol) e DHCP (Dynamic Host Configuration Protocol)
- Cisco Identity Service Engine (ISE)

- Cisco Catalyst Switch 2960

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

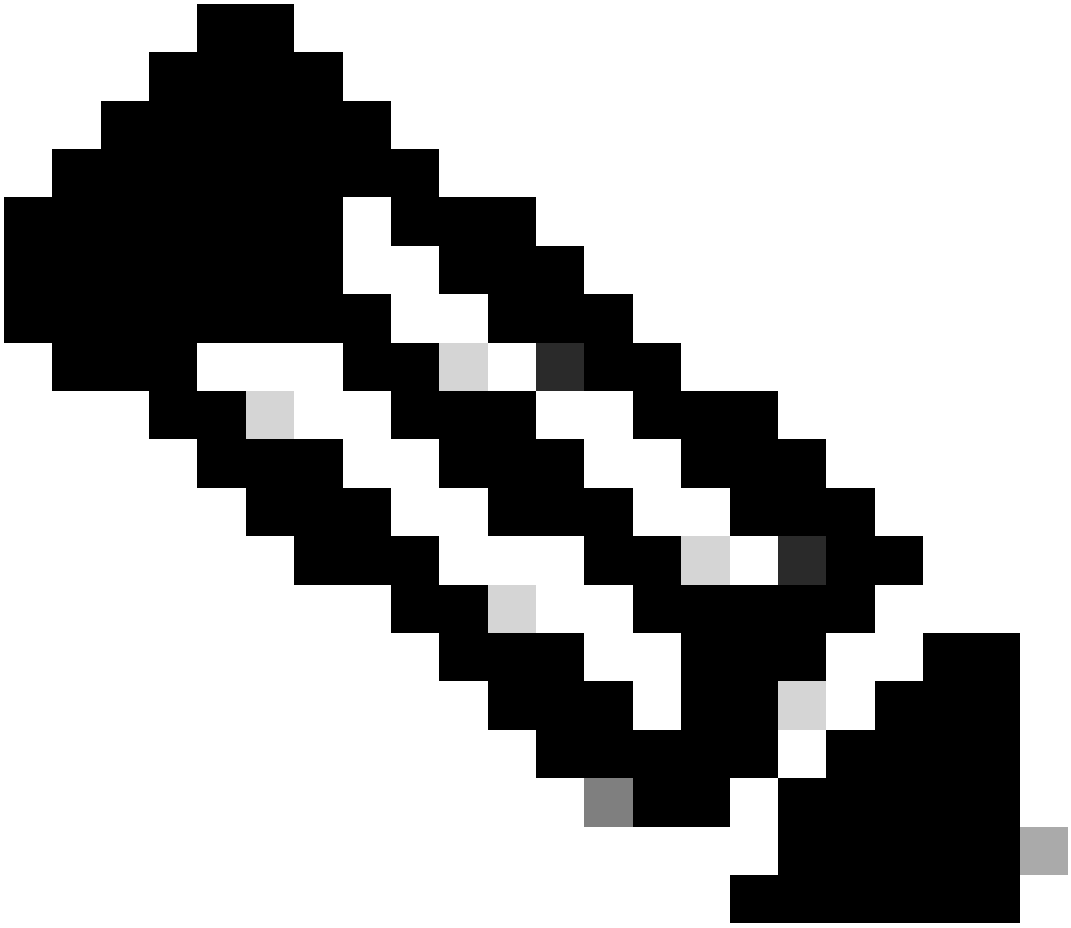
- Cisco ISE versione 1.3 patch 3
- Cisco Catalyst Switch 2960s versione 15.2(2a)E1
- Cisco IP Phone 8941 versione SCCP 9-3-4-17

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Un sensore dispositivo è una funzionalità delle periferiche di accesso. Consente di raccogliere informazioni sugli endpoint connessi. Nella maggior parte dei casi, le informazioni raccolte dal sensore dispositivo possono provenire dai seguenti protocolli:

- CDP
- LLDP
- DHCP



Nota: in alcune piattaforme è possibile utilizzare anche i protocolli H323, Session Initiation Protocol (SIP), Multicast Domain Resolution (MDNS) o HTTP. Le possibilità di configurazione delle funzionalità dei sensori dei dispositivi possono variare da protocollo a protocollo. Un esempio è disponibile su Cisco Catalyst 3850 con software 03.07.02.E.

Una volta raccolte, le informazioni possono essere incapsulate nell'accounting radius e inviate a un server di profiling. In questo articolo, ISE è usato come server di profiling.

Configurazione

Passaggio 1. Configurazione AAA standard

Per configurare l'autenticazione, l'autorizzazione e l'accounting (AAA), attenersi alla seguente procedura:

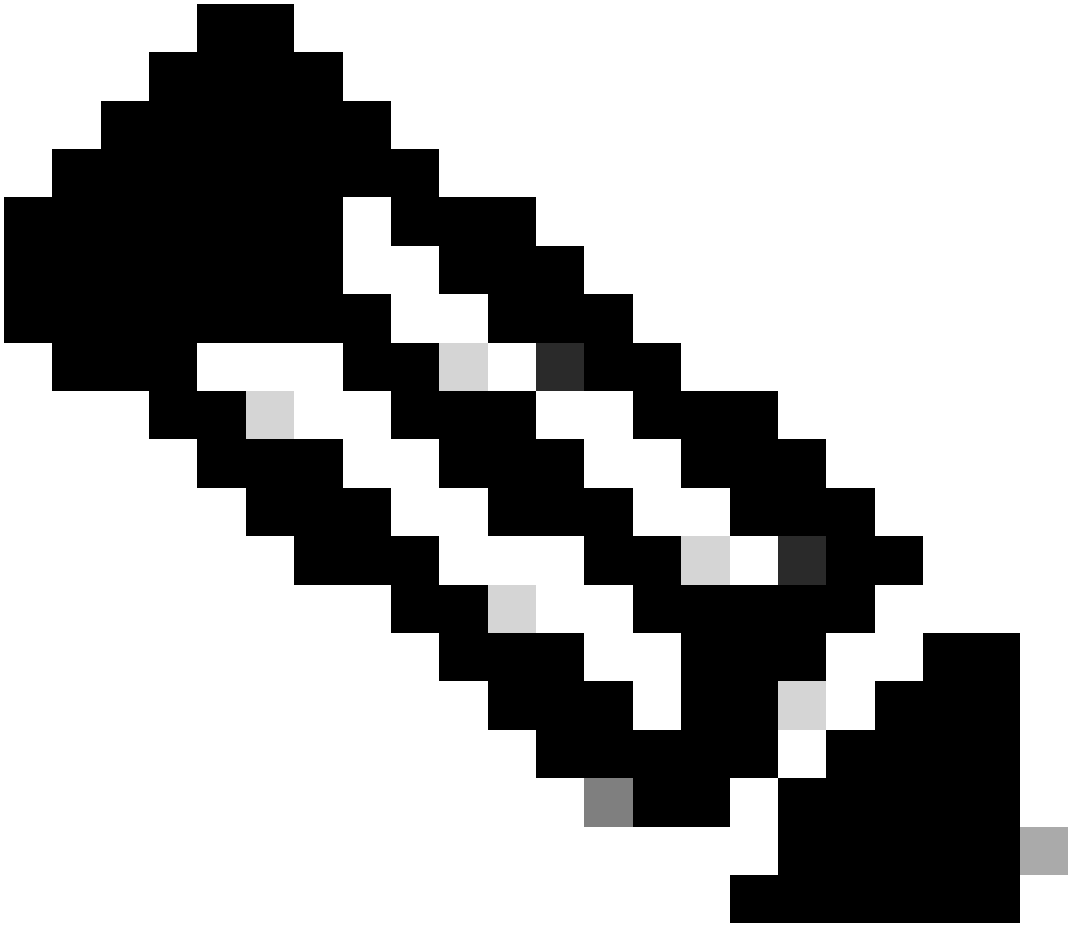
1. Abilitare il server AAA con `aaa new-model` il comando e abilitare 802.1X a livello globale sullo switch.

2. Configurare il server Radius e abilitare l'autorizzazione dinamica (Cambia autorizzazione - CoA).

3. Abilitare i protocolli CDP e LLDP.

4. Aggiungere la configurazione di autenticazione 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
!
```



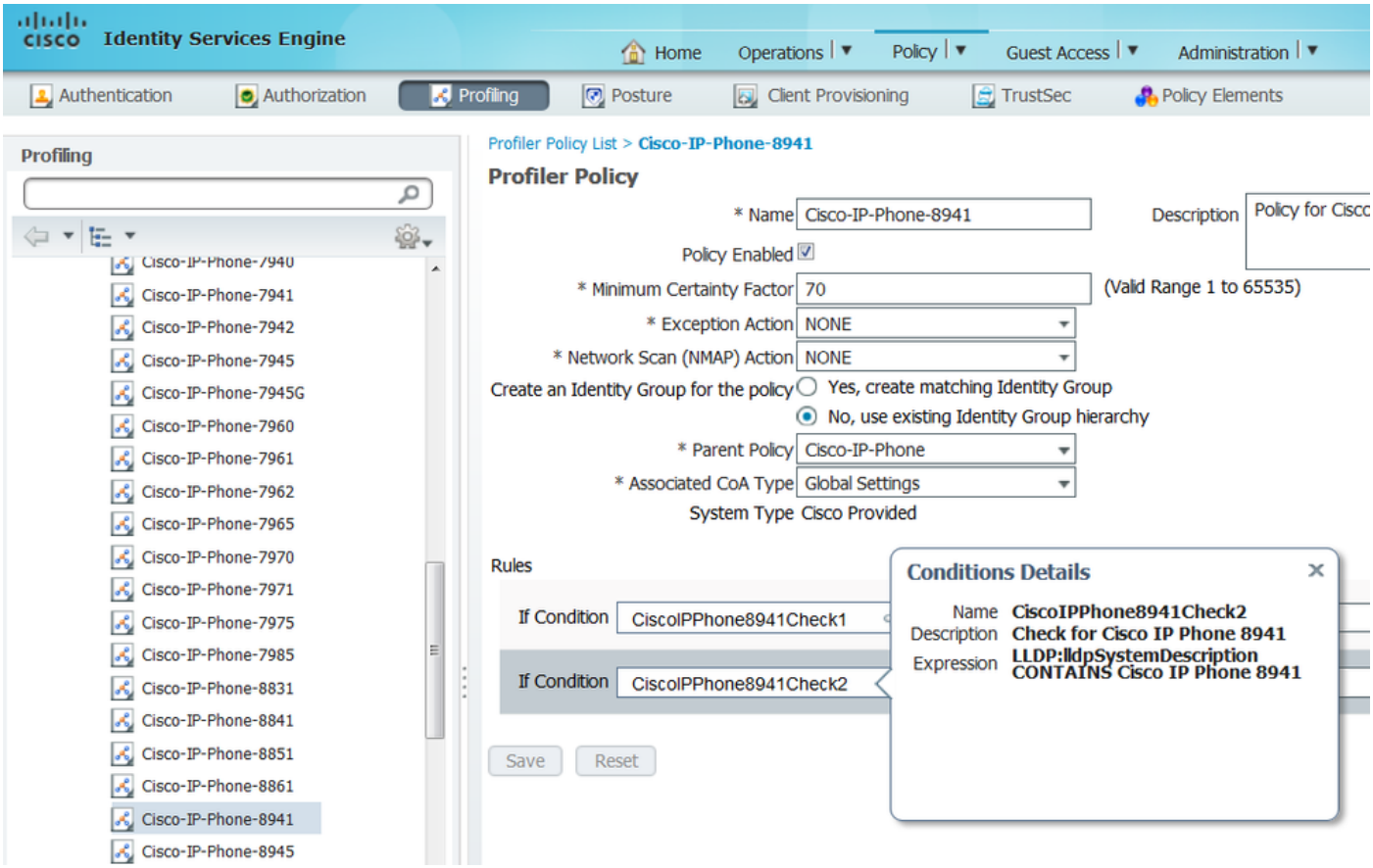
Nota: nella versione software più recente, il comando radius-server vsa send accounting è abilitato per impostazione predefinita. Se non è possibile visualizzare gli attributi inviati nell'accounting, verificare che il comando sia abilitato.

Passaggio 2. Configura sensore dispositivo

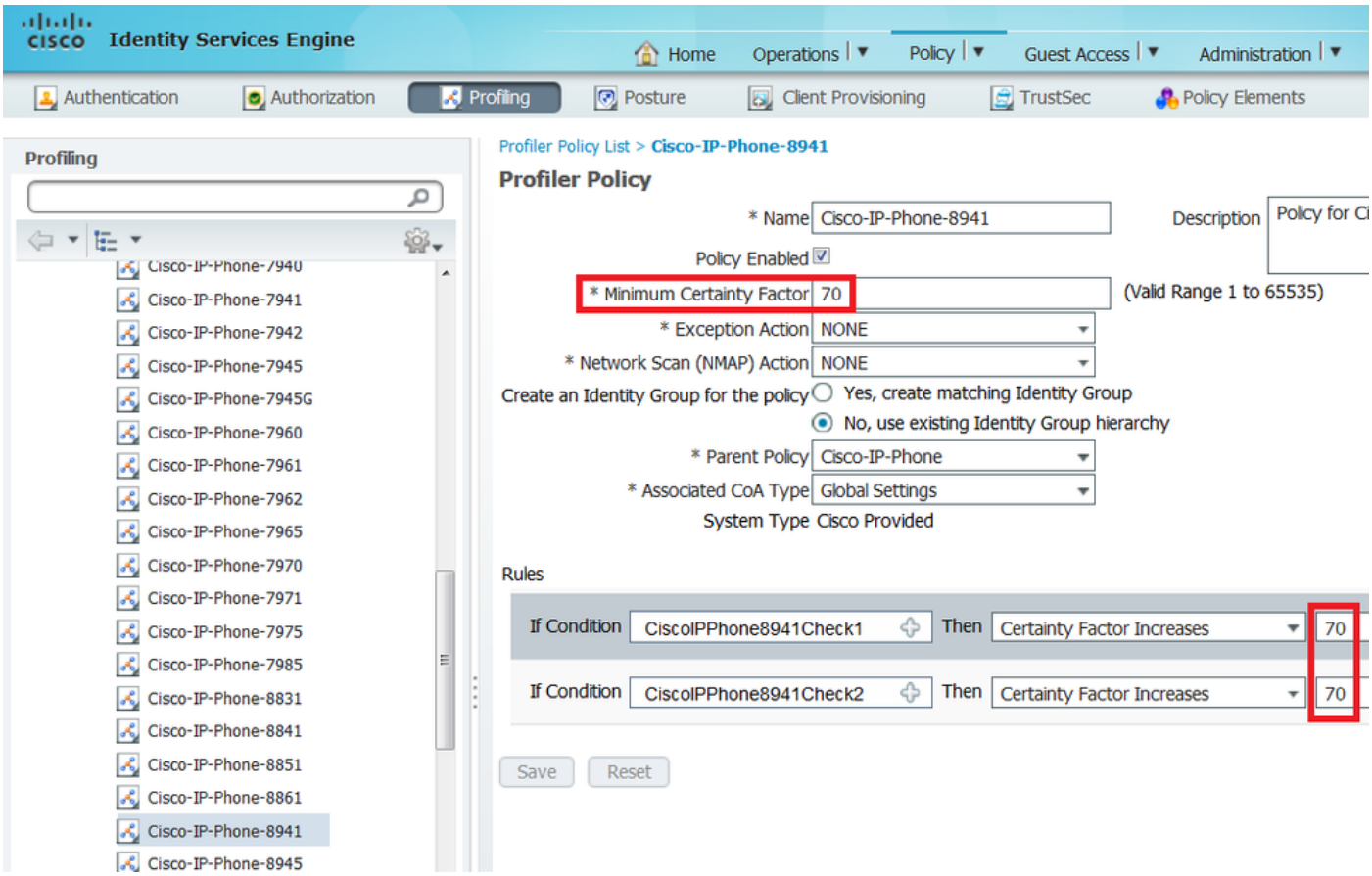
1. Determinare gli attributi CDP/LLDP necessari per la profilatura del dispositivo. Nel caso di Cisco IP Phone 8941, è possibile utilizzare quanto segue:

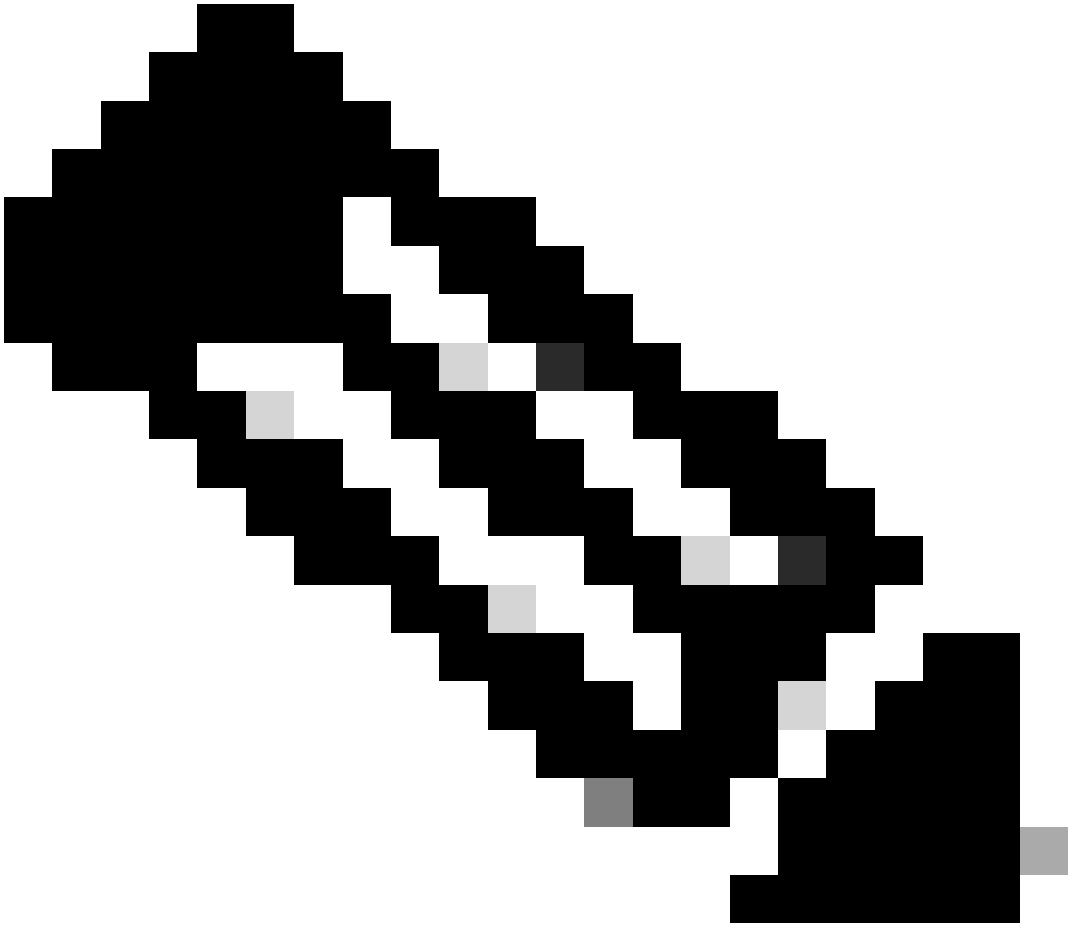
- Attributo LLDP SystemDescription

- Attributo CDP CachePlatform



Per il nostro scopo, è sufficiente ottenere solo uno di questi, in quanto entrambi forniscono un aumento di Fabbrica di Certezza di 70, e la Fabbrica di Certezza Minima richiesta per essere profilato come Cisco-IP-Phone-8941 è 70:


Identity Services Engine
Home
Operations
Policy
Guest Access
Administration
Authentication
Authorization
Profiling
Posture
Client Provisioning
TrustSec
Policy Elements
Profiling
Cisco-IP-Phone-7940
Cisco-IP-Phone-7941
Cisco-IP-Phone-7942
Cisco-IP-Phone-7945
Cisco-IP-Phone-7945G
Cisco-IP-Phone-7960
Cisco-IP-Phone-7961
Cisco-IP-Phone-7962
Cisco-IP-Phone-7965
Cisco-IP-Phone-7970
Cisco-IP-Phone-7971
Cisco-IP-Phone-7975
Cisco-IP-Phone-7985
Cisco-IP-Phone-8831
Cisco-IP-Phone-8841
Cisco-IP-Phone-8851
Cisco-IP-Phone-8861
Cisco-IP-Phone-8941
Cisco-IP-Phone-8945
Profiler Policy List > Cisco-IP-Phone-8941
Profiler Policy
* Name Cisco-IP-Phone-8941
Description Policy for Ci
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 Then Certainty Factor Increases 70
If Condition CiscoIPPhone8941Check2 Then Certainty Factor Increases 70
Save
Reset



Nota: per essere profilato come uno specifico Cisco IP Phone, è necessario soddisfare le condizioni minime per tutti i profili padre. Ciò significa che il profiler deve corrispondere a Cisco-Device (fattore di certezza minimo 10) e Cisco-IP-Phone (fattore di certezza minimo 20). Anche se il profiler corrisponde a questi due profili, deve comunque essere profilato come uno specifico Cisco IP Phone poiché ogni modello di telefono IP ha un fattore di certezza minimo di 70. Il dispositivo viene assegnato al profilo per il quale ha il fattore di certezza più alto.

2. Configurare due elenchi di filtri, uno per CDP e l'altro per LLDP. Indicano quali attributi devono essere inclusi nei messaggi di accounting Radius. Questo passaggio è facoltativo.

3. Creare due specifiche di filtro per CDP e LLDP. In filter-spec è possibile indicare l'elenco degli attributi che devono essere inclusi o esclusi dai messaggi di accounting. Nell'esempio sono inclusi i seguenti attributi:

- nome-dispositivo da CDP

- descrizione del sistema da LLDP

È possibile configurare altri attributi da trasmettere via Radius ad ISE, se necessario. Anche questo passaggio è facoltativo.

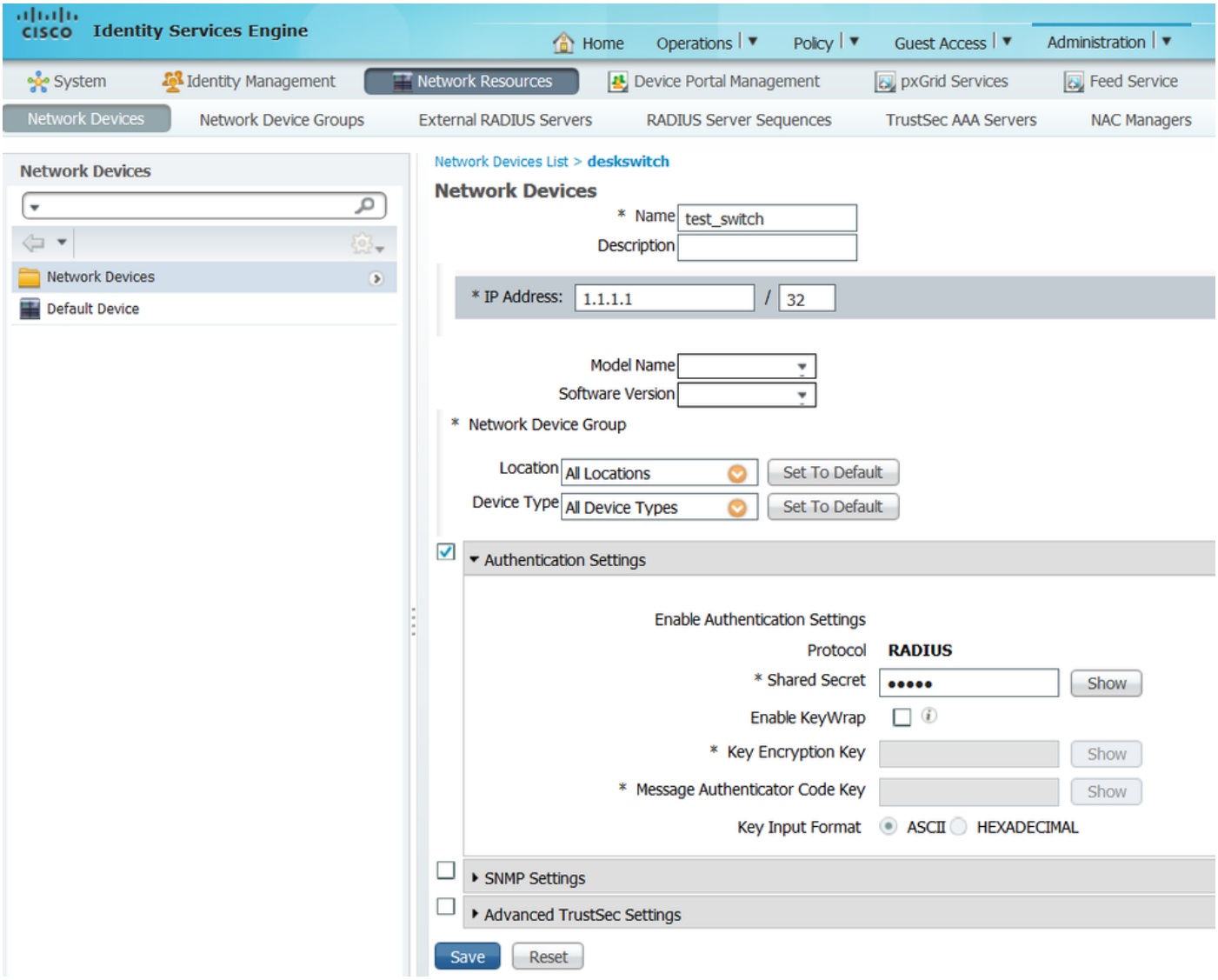
4. Aggiungere il comando device-sensor notify all-changes. Attiva gli aggiornamenti ogni volta che i valori TLV vengono aggiunti, modificati o rimossi per la sessione corrente.

5. Per inviare effettivamente le informazioni raccolte tramite la funzionalità Device Sensor, è necessario dire esplicitamente allo switch di farlo con il comando device-sensor accounting.

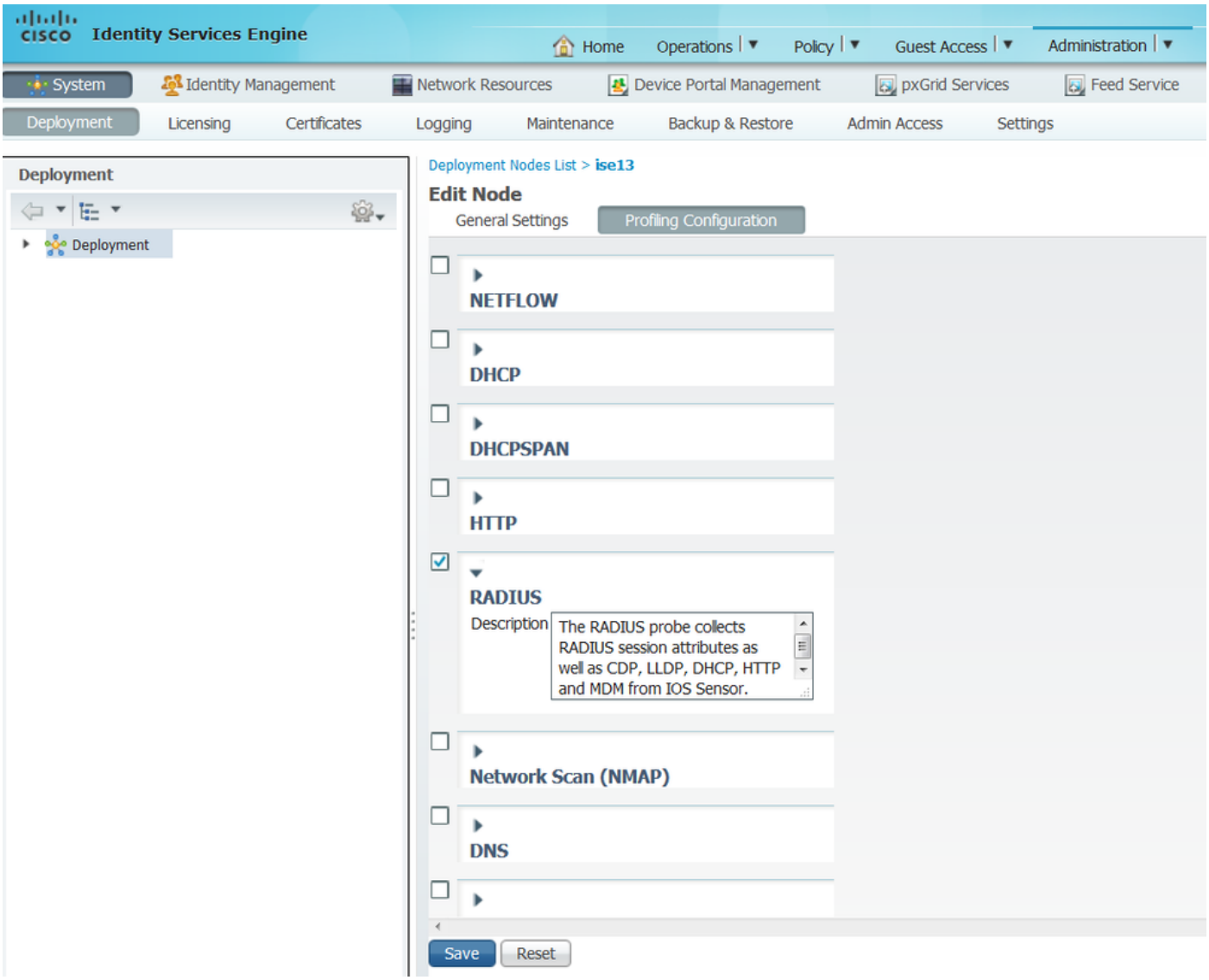
```
! device-sensor filter-list cdp list cdp-list tlv name device-name
 tlv name platform-type ! device-sensor filter-list lldp list lldp-list tlv name system-description ! device-sensor filter-spec lldp include list lldp-list device-se
```

Passaggio 3. Configurazione della profilatura su ISE

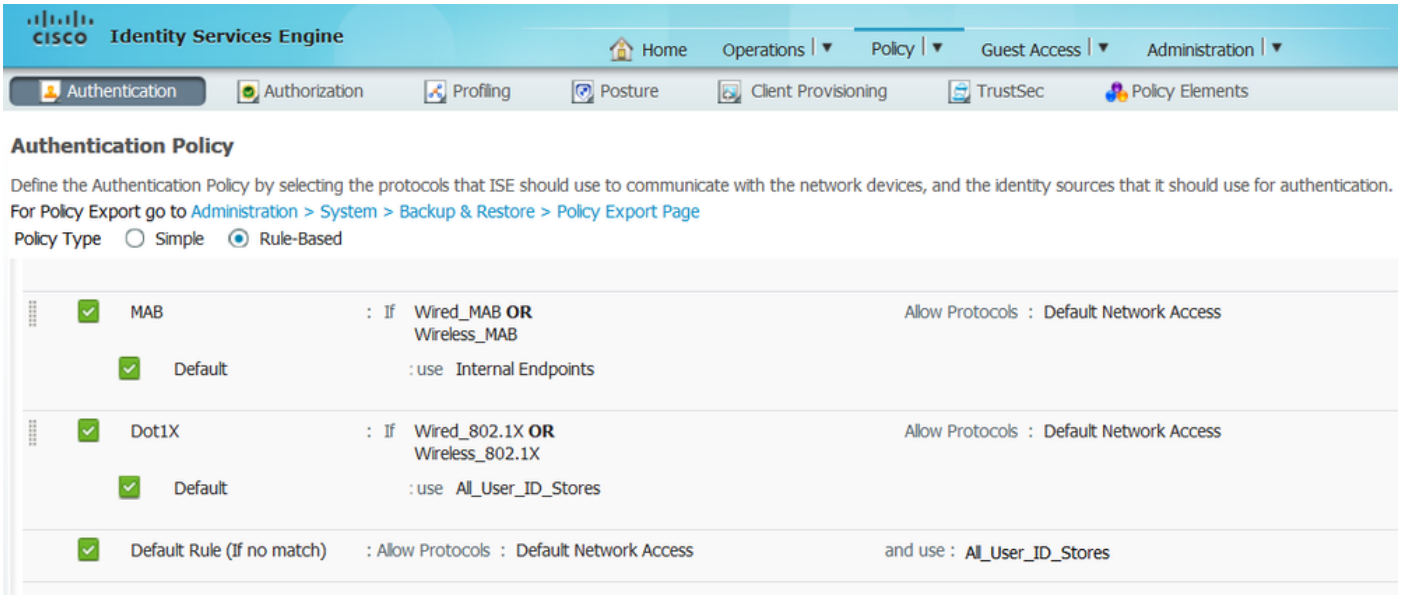
1. Aggiungere lo switch come dispositivo di rete in Administration > Network Resources > Network Devices. Utilizzare la chiave del server radius dello switch come segreto condiviso in Impostazioni di autenticazione:



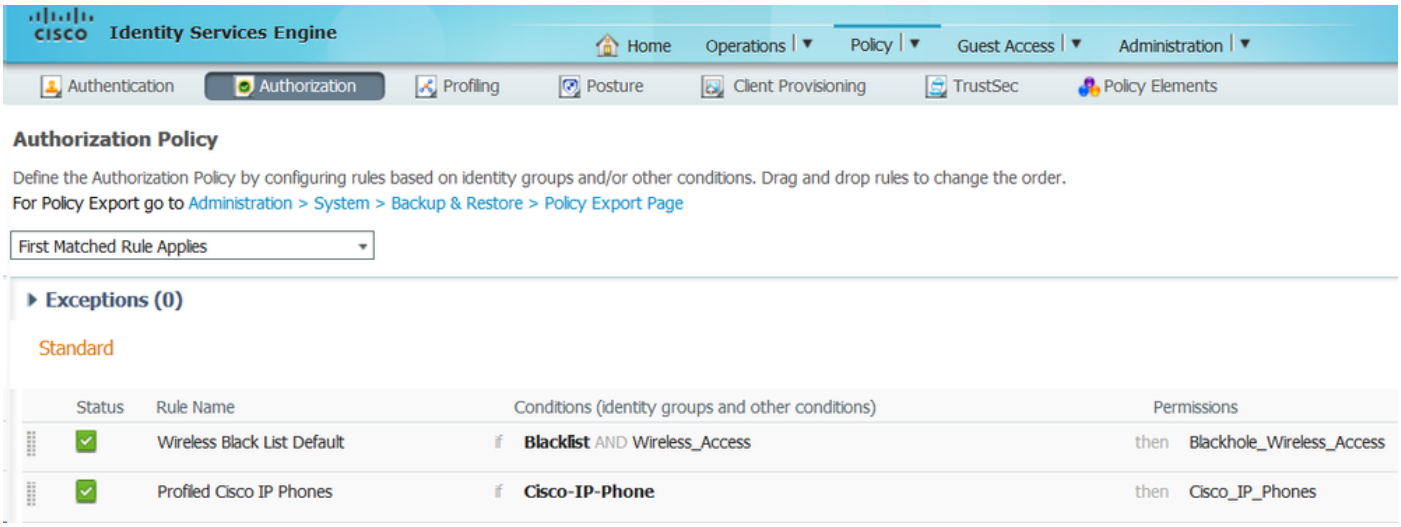
2. Abilitare la sonda Radius sul nodo di profilatura in Administration > System > Deployment > ISE node > Profiling Configuration. Se è necessario utilizzare tutti i nodi PSN per la profilatura, abilitare la sonda su tutti i nodi:



3. Configurare ISE Authentication Rules. Nell'esempio vengono usate le regole di autenticazione predefinite preconfigurate su ISE:

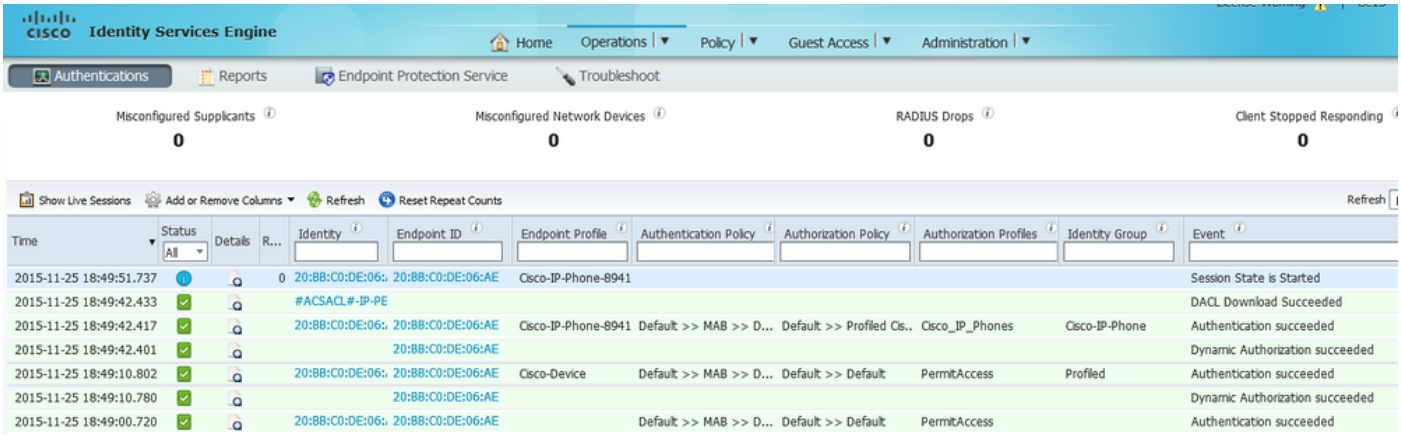


4. Configurare le regole di autorizzazione ISE. Si usa la regola 'Cisco IP Phone profilati', che è preconfigurata su ISE:

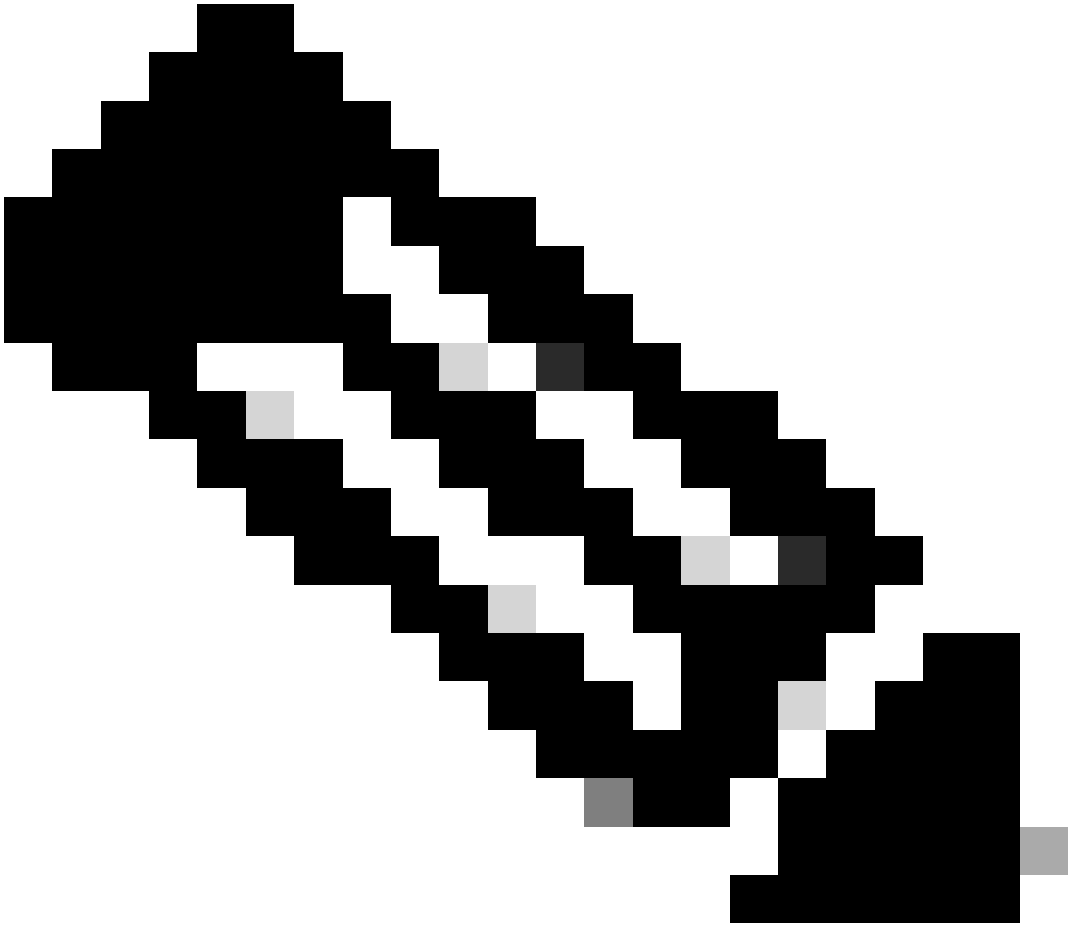


Verifica

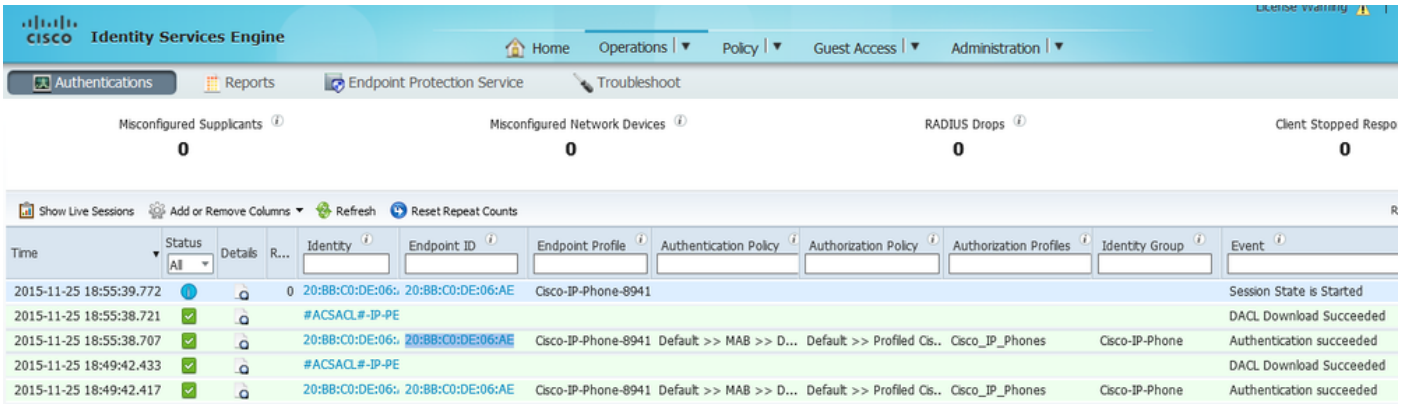
Per verificare se la profilatura funziona correttamente, consultare il documento sullOperations > Authentications'ISE:



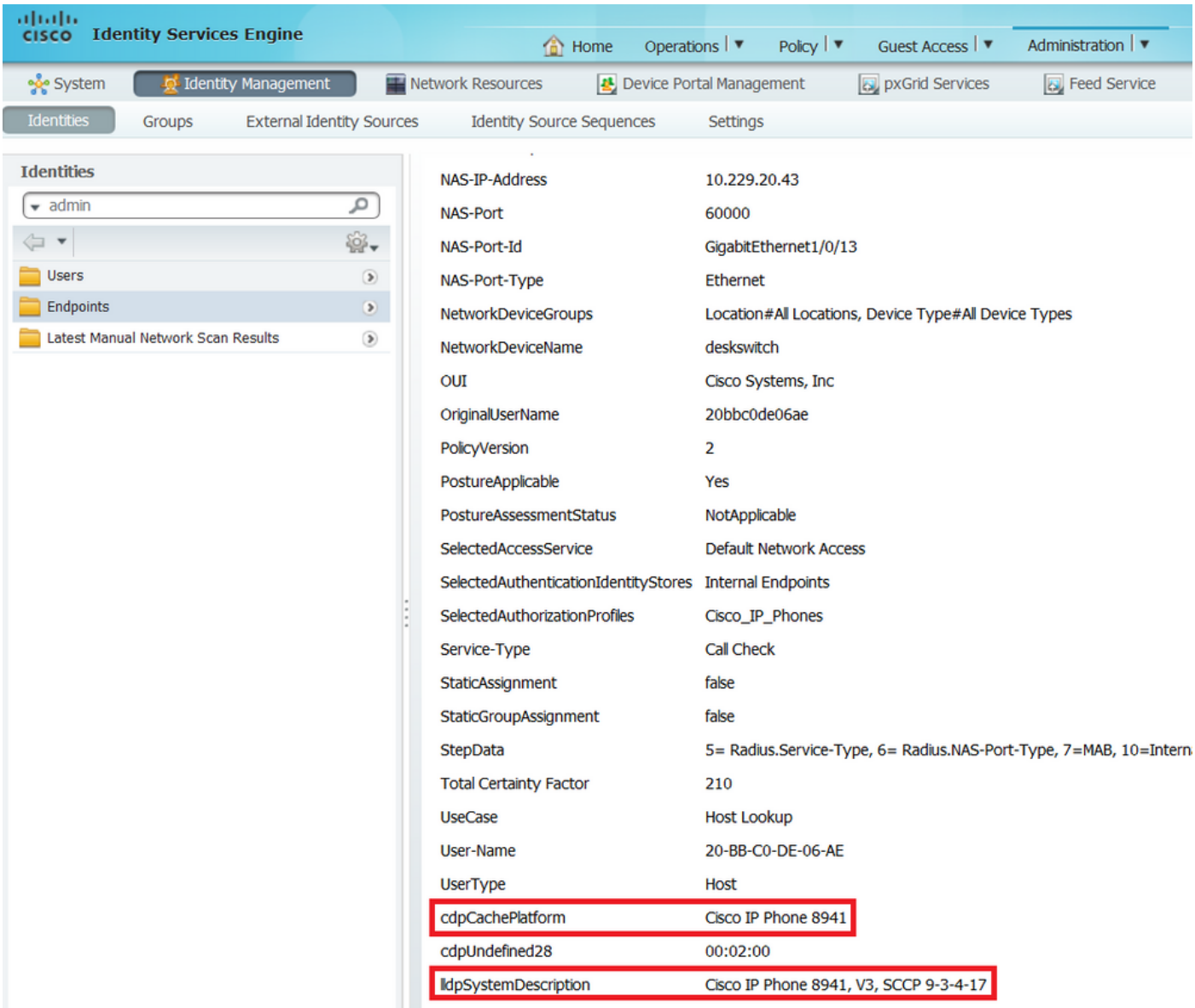
Il dispositivo è stato autenticato tramite MAB (18:49:00). Dieci secondi dopo (18:49:10) è stato riprofilato come Cisco-Device, e finalmente dopo 42 secondi dalle prime autenticazioni (18:49:42), ha ricevuto il profilo Cisco-IP-Phone-8941. Di conseguenza, ISE restituisce un profilo di autorizzazione specifico per i telefoni IP (Cisco_IP_Phones) e un ACL scaricabile che autorizza tutto il traffico (allow ip any). Notare che in questo scenario la periferica sconosciuta ha accesso di base alla rete. A tale scopo, è possibile aggiungere un indirizzo Mac al database interno degli endpoint ISE o consentire l'accesso alla rete molto semplice a dispositivi sconosciuti in precedenza.



Nota: in questo esempio, la creazione del profilo iniziale ha richiesto circa 40 secondi. Alla prossima autenticazione, ISE conosce già il profilo e gli attributi corretti (autorizzazione ad unirsi a voice domain e DACL) vengono applicati istantaneamente a meno che ISE non riceva attributi nuovi/aggiornati e debba ricreare il profilo del dispositivo.



In Administration > Identity Management > Identities > Endpoints > tested endpoint è possibile visualizzare il tipo di attributi raccolti dalla sonda Raggio e i relativi valori:



Come si può osservare, in questo scenario il fattore di certezza totale calcolato è 210. Viene dal fatto che l'endpoint ha abbinato anche il profilo Cisco-Device (con un fattore di certezza totale di 30) e il profilo Cisco-IP-Phone (con un fattore di certezza totale di 40). Poiché il profiler soddisfa entrambe le condizioni nel profilo Cisco-IP-Phone-8941, il fattore di certezza per questo profilo è 140 (70 per ogni attributo in base ai criteri di profilatura). Per riassumere: 30+40+70+70=210.

Risoluzione dei problemi

Passaggio 1. Verifica delle informazioni raccolte da CDP/LLDP

switch#sh cdp neighbors g1/0/13 detail ---------- Device ID: SEP20BBC0DE06AE Entry address(es): Platform: Cisco IP Phone 8941 , Capabil

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

Se non è possibile visualizzare i dati raccolti, verificare quanto segue:

- Verificare lo stato della sessione di autenticazione sullo switch (l'operazione deve avere esito positivo):

piborowi#show authentication sessions int g1/0/13 details Interface: GigabitEthernet1/0/13 MAC Address: 20bb.c0de.06ae IPv6 Address: Unknown IPv4 A

- Verificare se i protocolli CDP e LLDP sono abilitati. Verificare se sono presenti comandi non predefiniti relativi a CDP/LLDP/e così via e come possono influire sul recupero degli attributi dall'endpoint

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

- Verificare nella guida alla configurazione dell'endpoint se supporta CDP, LLDP e così via.

Passaggio 2. Controllare la cache dei sensori del dispositivo

switch#show device-sensor cache interface g1/0/13 Device: 20bb.c0de.06ae on port GigabitEthernet1/0/13 ---------- Proto

Se in questo campo non vengono visualizzati dati o se le informazioni non sono complete, verificare i comandi 'device-sensor', in particolare gli elenchi dei filtri e le specifiche dei filtri.

Passaggio 3. Verifica se gli attributi sono presenti in Contabilità Radius

È possibile verificare questa condizione usando il comando sullodebug radius switch o eseguendo l'acquisizione dei pacchetti tra lo switch e ISE.

Debug Radius:

<#root>

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 1

cdp-tlv

= " Mar 30 05:34:58.716: RADIUS: Vendor, Cisco [26] 23 Mar 30 05:34:58.716: RADIUS: Cisco AVpair [1] 17

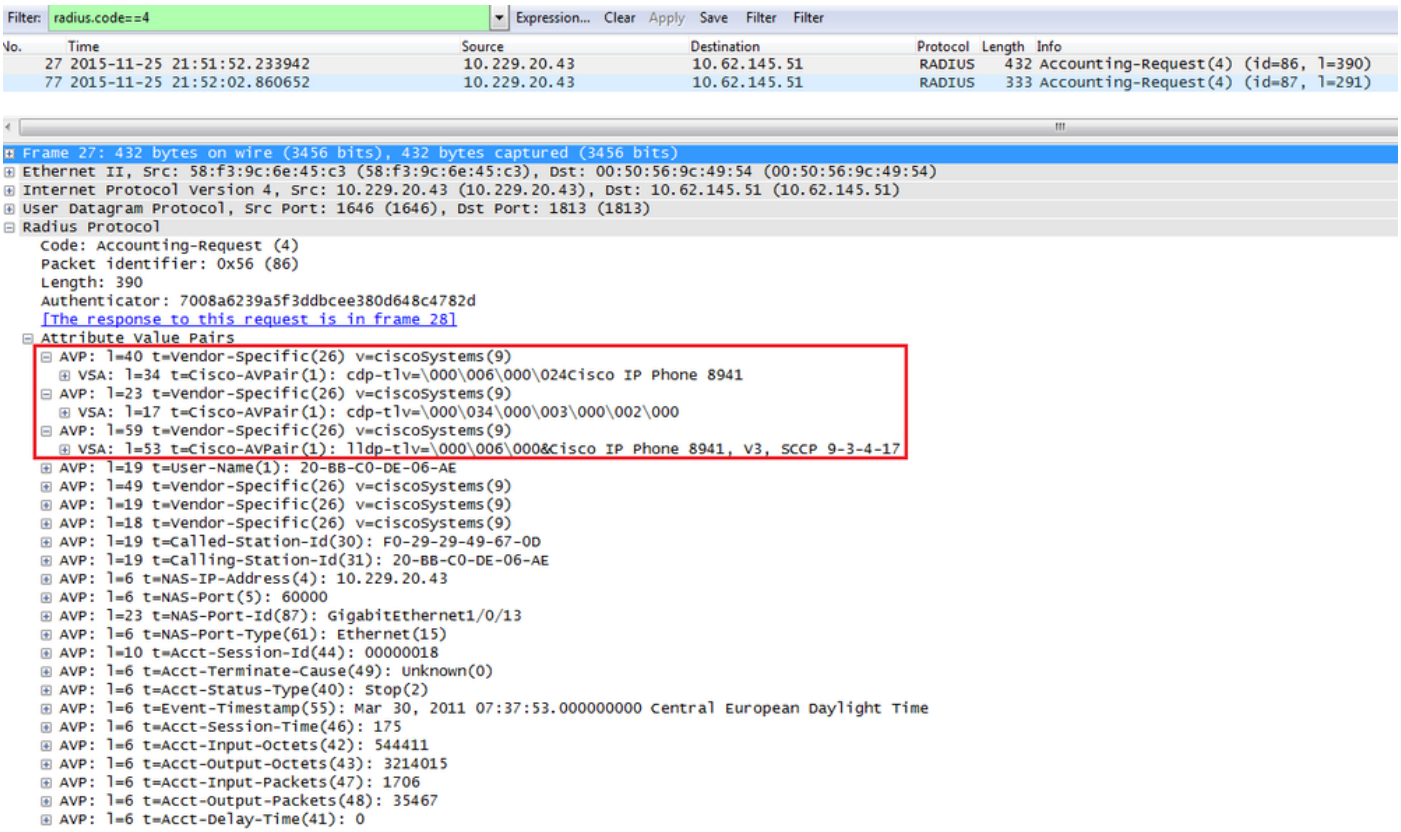
cdp-tlv

= " 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: Vend

Acquisizione pacchetti:



Passaggio 4. Verifica dei debug del profiler sull'ISE

Se gli attributi sono stati inviati dallo switch, è possibile verificare se sono stati ricevuti con ISE. Per verificare questa condizione, abilitare i debug del profiler per il nodo PSN corretto (Administration > System > Logging > Debug Log Configuration > PSN > profiler > debug) ed eseguire di nuovo l'autenticazione dell'endpoint.

Cercare le informazioni seguenti:

- Debug che indica che la sonda radius ha ricevuto gli attributi:

<#root>

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=0AE5182000000020040099C216, cisco-av-pair=vlan-id=101,
cisco-av-pair=method=mab, AcsSessionID=ise13/235487054/2511, SelectedAccessService=Default Network Acces
Step=11004, Step=11017, Step=15049, Step=15008, Step=15004, Step=11005, NetworkDeviceGroups=Location#Al
NetworkDeviceGroups=Device Type#All Device Types, Service-Type=Call Check, CPMSessionID=0AE518200000020
AllowedProtocolMatchedRule=MAB, Location=Location#All Locations, Device Type=Device Type#All Device Typ

- Debug che indica che gli attributi sono stati analizzati correttamente:

2015-11-25 19:29:53,642 DEBUG [RADIUSParser-1-thread-1][] cisco.profiler.probes.radius.RadiusParser -:::- Parsed IOS Sensor 1: cdpCachePlatform=[

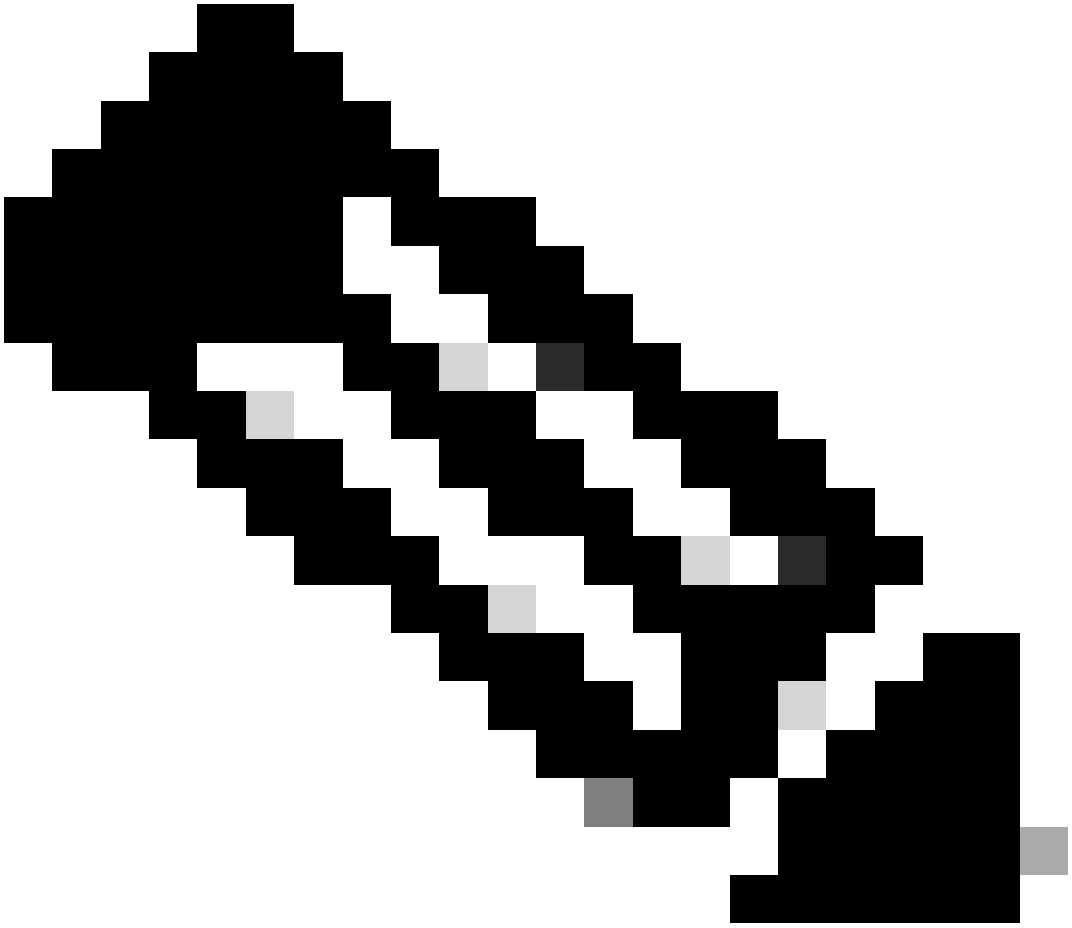
- Debug che indica che gli attributi vengono elaborati dal server di inoltro:

<#root>

2015-11-25 19:29:53,643 DEBUG [forwarder-6][] cisco.profiler.infrastructure.probemgr.Forwarder -:20:BB:C0:DE:06:AE:ProfilerCollection:- Endpoint A

Attribute:cdpCachePlatform value:Cisco IP Phone 8941 Attribute:cdpUndefined28 value:00:02:00 Attribute:

Attribute:SkipProfiling value:false



Nota: un server d'inoltro memorizza gli endpoint nel database Cisco ISE insieme ai dati dei relativi attributi, quindi notifica all'analizzatore i nuovi endpoint rilevati sulla rete. L'analizzatore classifica gli endpoint nei gruppi di identità degli endpoint e archivia gli endpoint con i profili corrispondenti nel database.

Passaggio 5. Creazione profilo nuovi attributi e assegnazione dispositivo

In genere, dopo l'aggiunta di nuovi attributi alla raccolta esistente per un dispositivo specifico, questo dispositivo/endpoint viene aggiunto alla coda di profilatura per verificare se è necessario assegnare un profilo diverso in base ai nuovi attributi:

<#root>

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

Informazioni correlate

- https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html
- https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).