Configuration du capteur de périphérique pour le profilage ISE

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Étape 1. Configuration AAA standard
  - Étape 2 : configuration du capteur de périphérique
- Vérifier
- Dépannage
  - Étape 1 : vérification des informations collectées par le protocole CDP/LLDP
  - Étape 2. Vérification du cache du capteur de périphérique
  - Étape 3. Vérifier si les attributs sont présents dans Radius Accounting
    - Débogage Radius
    - Capture de paquets
  - Étape 4. Vérification des débogages du profileur sur ISE
  - Étape 5. Reclassification du profil après réception de nouveaux attributs
- Informations connexes

Introduction

Ce document décrit comment configurer le capteur de périphérique afin qu'il puisse être utilisé à des fins de profilage sur ISE.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Protocole Radius

- Commutateur Cisco Catalyst 9300
- Cisco Identity Service Engine (ISE)
- CDP (Cisco Discovery Protocol) et LLDP (Link Layer Discovery Protocol)

Composants utilisés

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

- Cisco ISE version 3.4, correctif 3
- Téléphone IP Cisco 8811 version 12.8.1
- Commutateur Cisco Catalyst 9300-48P Version 17.12.4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Device Sensor est une fonctionnalité prise en charge sur les périphériques d'accès au réseau câblé, tels que les commutateurs Cisco Catalyst. Il peut collecter des informations sur les terminaux à l'aide de protocoles tels que CDP, LLDP et DHCP, et envoie les attributs collectés à ISE dans des paquets de comptabilité RADIUS. Dans les déploiements sans fil uniquement, le profilage ISE repose généralement sur les attributs reçus du contrôleur sans fil et les données de sonde DHCP plutôt que sur les données du capteur de périphérique de commutation. Les flux Profiler fournissent les politiques de profilage utilisées par ISE pour classer les terminaux.



Remarque : Device Sensor collecte des informations uniquement à partir des terminaux directement connectés au périphérique d'accès réseau (à un saut). ISE utilise les attributs collectés pour le profilage des terminaux.

Une fois les informations collectées, elles peuvent être encapsulées dans la comptabilité Radius et envoyées à un serveur de profilage. Dans cet article, ISE est utilisé comme serveur de profilage.

Configurer

Étape 1. Configuration AAA standard

Pour configurer l'authentification, l'autorisation et la comptabilité (AAA), reportez-vous aux étapes suivantes :

1. Activez AAA en exécutant la commande aaa new-model et activez 802.1X globalement sur le commutateur.
2. Configurer le serveur Radius et activer l'autorisation dynamique (Modification de l'autorisation - CoA.)
3. Activez les protocoles CDP et LLDP.
4. Ajoutez la configuration d'authentification switchport.

```
!
aaa new-model
!
!
aaa group server radius ISE-GROUP
 server name ise
!
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 <ISE_PSN_IP> server-key Krakow123
!
dot1x system-auth-control
!
lldp run
cdp run
!
interface GigabitEthernet1/0/1
 description IP_Phone
 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
!
radius server ise
 address ipv4 <ISE_PSN_IP> auth-port 1812 acct-port 1813
 key <shared_key>
```

!



Remarque : Vous devez configurer le commutateur pour qu'il envoie des attributs spécifiques au fournisseur Cisco (VSA) à ISE.

Ces attributs peuvent être envoyés à l'intérieur des paquets de comptabilité en configurant cette commande :

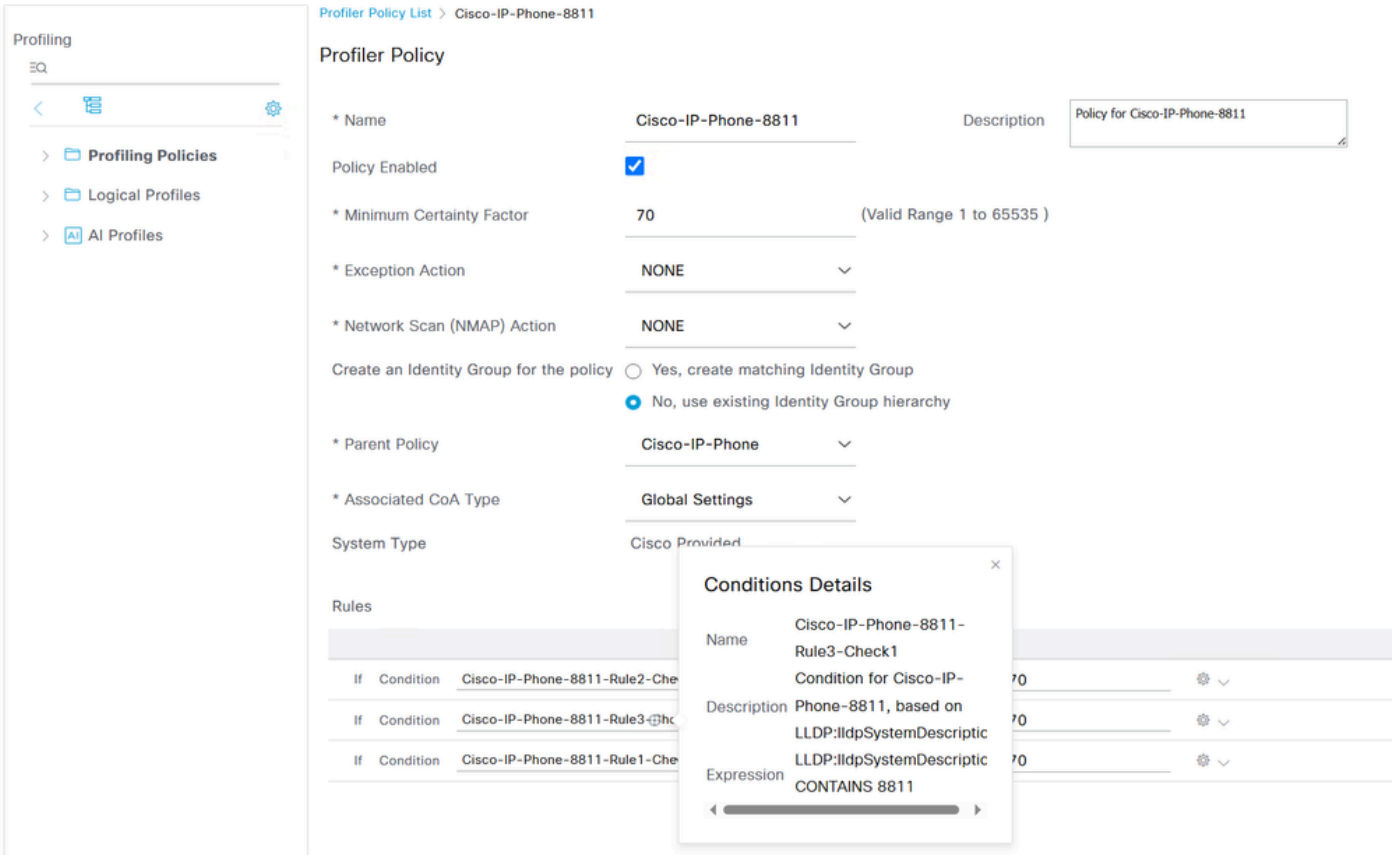
```
radius-server vsa send accounting
```

Étape 2 : configuration du capteur de périphérique

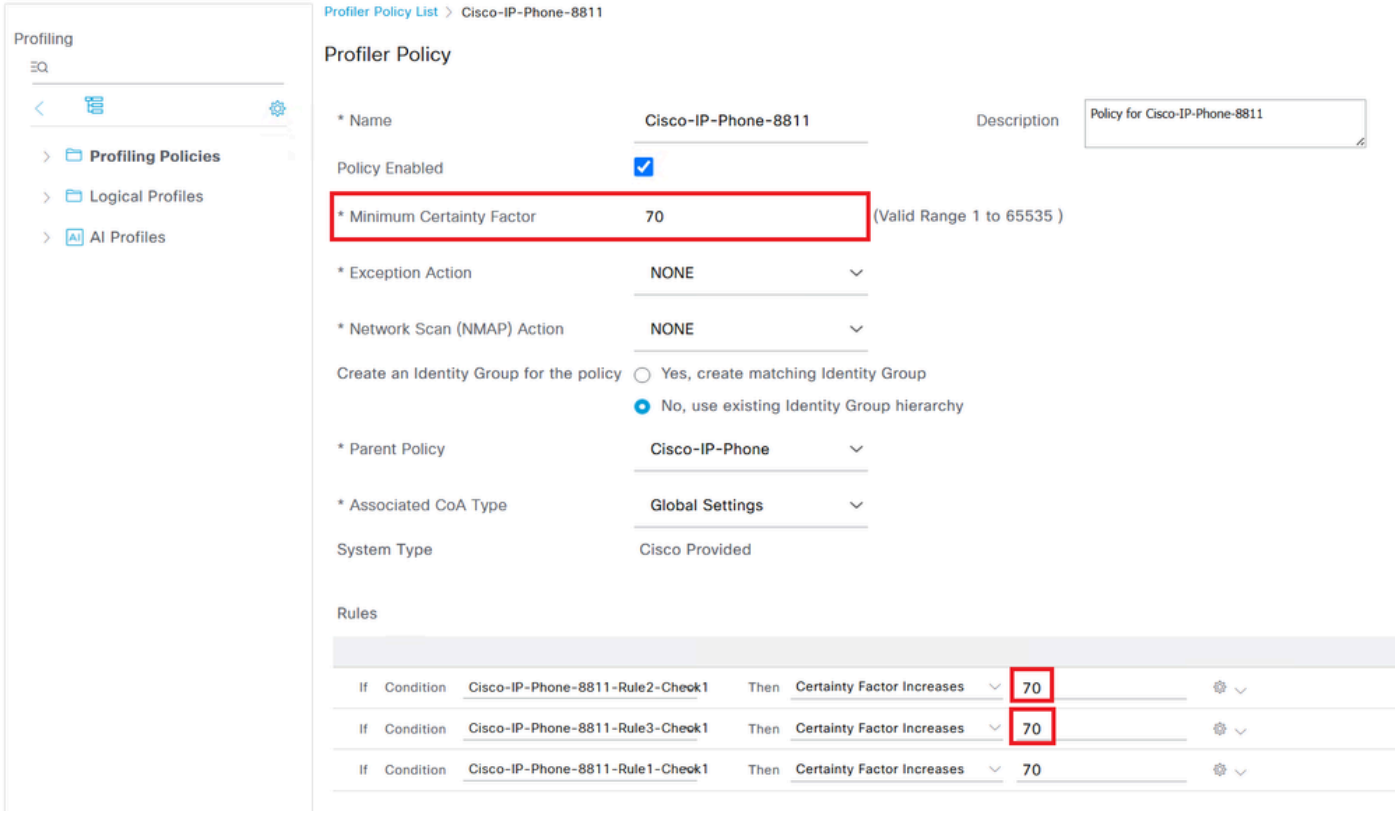
1. Déterminez quels attributs du protocole CDP/LLDP sont nécessaires pour profiler le périphérique. Dans le cas du téléphone IP Cisco 8811, vous pouvez utiliser les éléments suivants :

- Attribut LLDP SystemDescription
- Attribut CDP CachePlatform

Vous pouvez valider les attributs utilisés pour profiler le périphérique en vérifiant les stratégies du profileur. Pour ce faire, accédez à Work Centers > Profiler > Profiling Policies et sélectionnez la stratégie de profilage que vous souhaitez faire correspondre.



Dans la capture d'écran suivante, le facteur de certitude minimum requis pour que le point de terminaison soit profilé comme Cisco-IP-Phone-8811 est 70. Dans cet exemple, l'un des attributs contribue un facteur de certitude de 70. Cependant, le point de terminaison doit également remplir les conditions requises pour les profils parents applicables avant qu'ISE attribue le profil de point de terminaison final.



Remarque : Pour être profilé en tant que téléphone IP Cisco spécifique, vous devez remplir des conditions minimales pour tous les profils parents. Le profileur doit correspondre au Cisco-Device (facteur de sécurité minimum 10) et au Cisco-IP-Phone (facteur de sécurité minimum 20). Bien que le profileur corresponde aux deux profils, il doit toujours être profilé en tant que téléphone IP Cisco spécifique, car chaque modèle de téléphone IP a un facteur de certitude minimum de 70. Le périphérique est affecté au profil ayant le facteur de certitude le plus élevé.

---

2. Configurez deux listes de filtres, l'une pour CDP et l'autre pour LLDP. Ceux-ci indiquent les attributs qui doivent être inclus dans les messages de comptabilité Radius (cette étape est facultative).

3. Créez deux spécifications de filtre pour CDP et LLDP. Dans filter-spec, vous pouvez indiquer la liste des attributs qui doivent être inclus ou exclus des messages de comptabilité. Dans cet exemple, ces attributs sont inclus :

- nom-périphérique et type-plate-forme du protocole CDP
- system-description du protocole LLDP

Vous pouvez configurer des attributs supplémentaires à transmettre via Radius à ISE si nécessaire (cette étape est également facultative).

4. Ajoutez la commande device-sensor notify all-changes pour déclencher des mises à jour lorsque des TLV sont ajoutés, modifiés ou supprimés pour la session en cours.

5. Pour envoyer les informations collectées par le capteur de périphérique, configurez la commande device-sensor accounting.

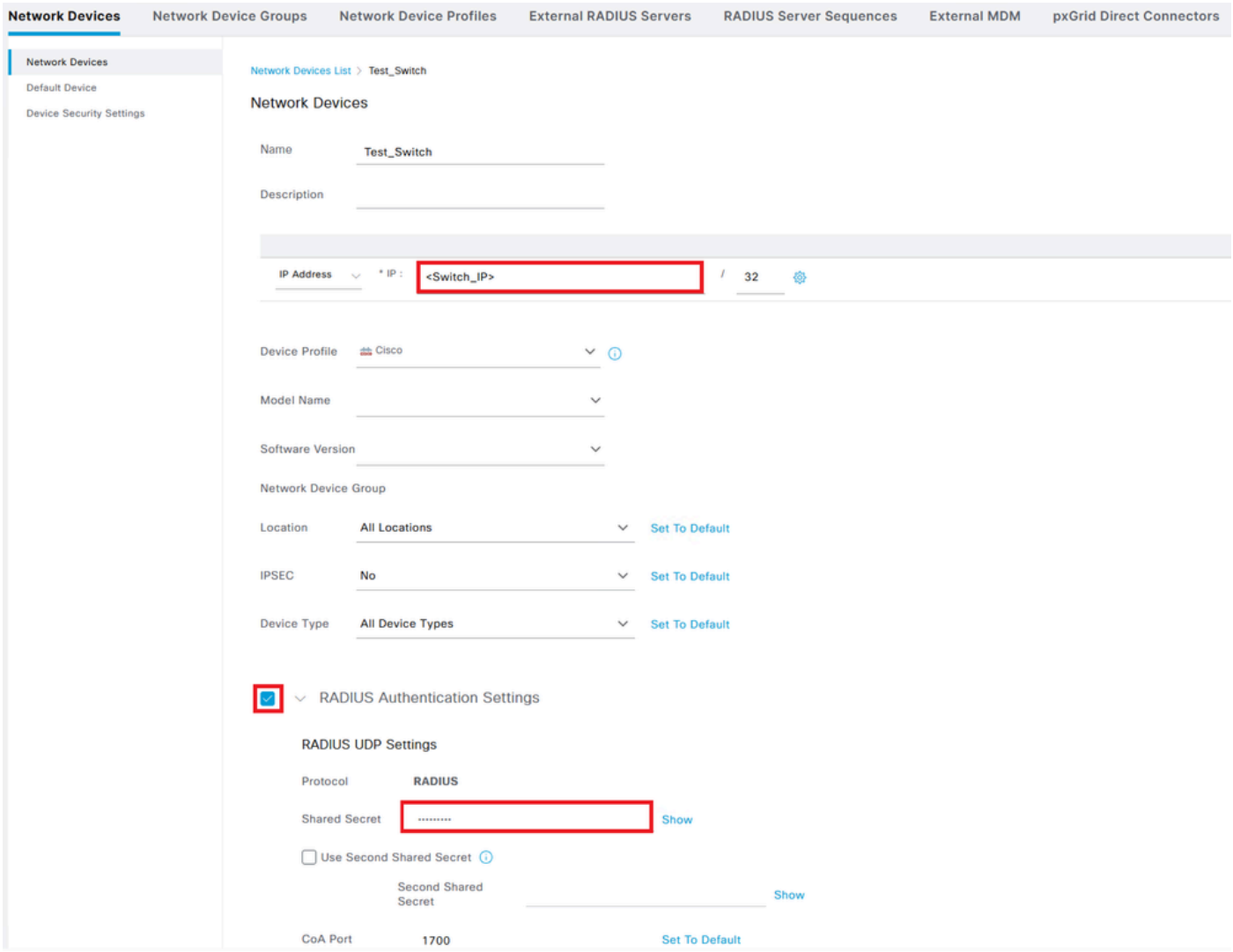
```
!
device-sensor filter-list cdp list cdp-list
 tlv name device-name
 tlv name platform-type
!
device-sensor filter-list lldp list lldp-list
 tlv name system-description
!
device-sensor filter-spec lldp include list lldp-list
device-sensor filter-spec cdp include list cdp-list
!
device-sensor accounting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



Remarque : Les commandes Device Sensor et les TLV pris en charge peuvent varier selon la plate-forme Catalyst et les versions IOS XE. Confirmer la prise en charge des commandes et les TLV disponibles dans le guide de configuration de la plate-forme de commutation utilisée ; Étape 3 : configuration du profilage sur ISE

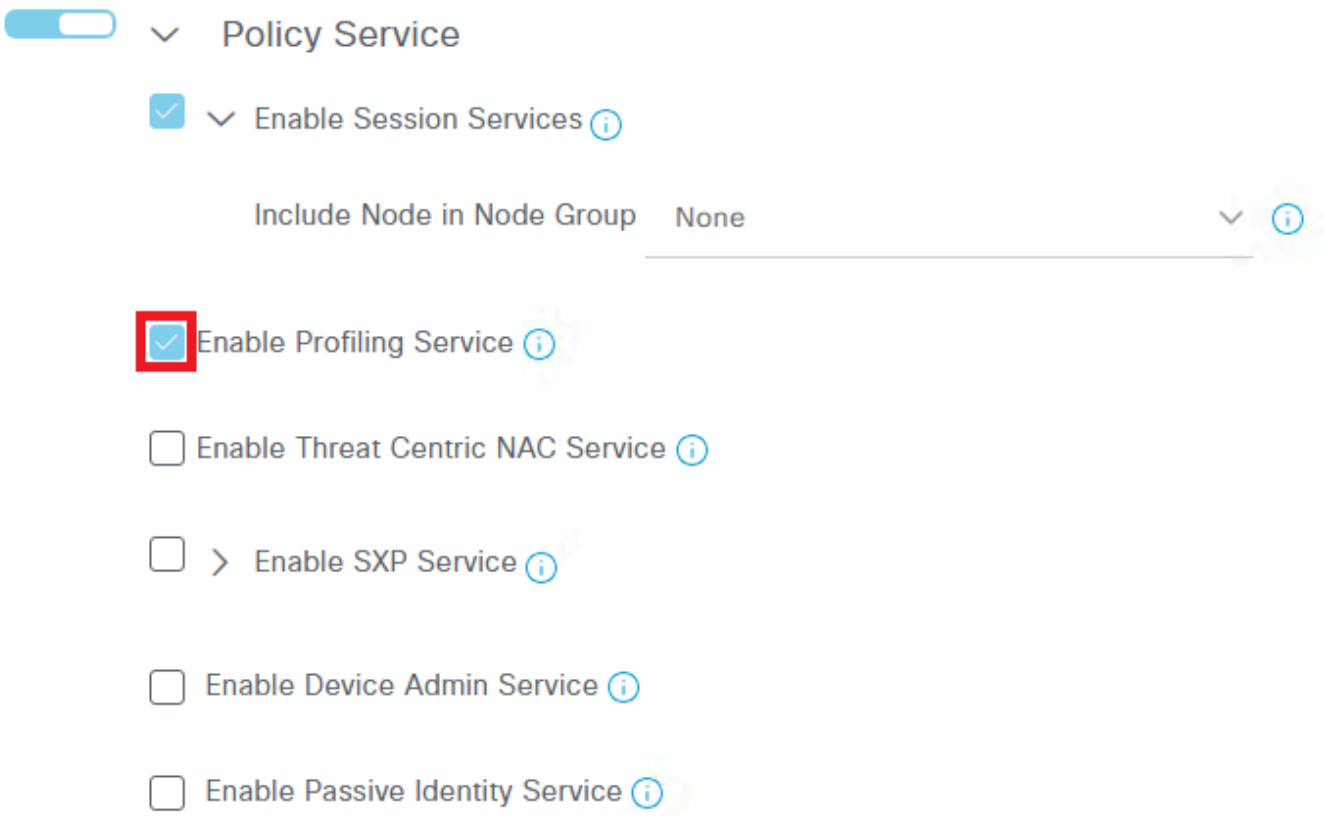
---

1. Ajoutez le commutateur en tant que périphérique réseau dans Administration > Network Resources > Network Devices. Utilisez la clé de serveur Radius du commutateur comme secret partagé dans les paramètres d'authentification :



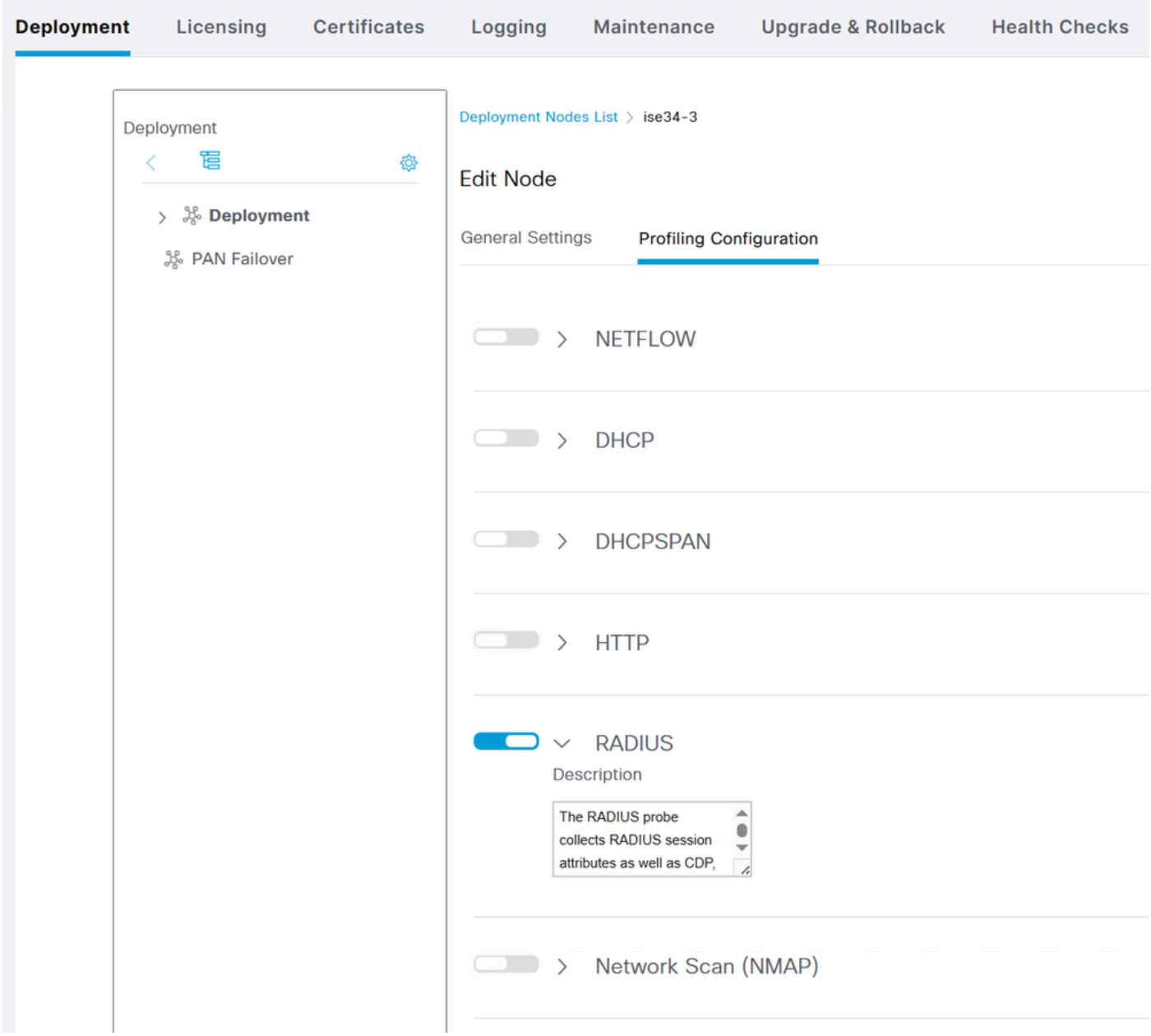
---

2. Activez le service de profilage sur le noeud ISE. Accédez à Administration > System > Deployment, choisissez le noeud ISE et, dans l'onglet Policy Service, activez l'option Profiling Service. Activez le service de profilage sur les noeuds PSN qui sont destinés à traiter les données de profilage. N'activez que les sondes requises pour le déploiement, car des sondes supplémentaires et des PSN activés pour le profilage peuvent augmenter l'utilisation des ressources système.



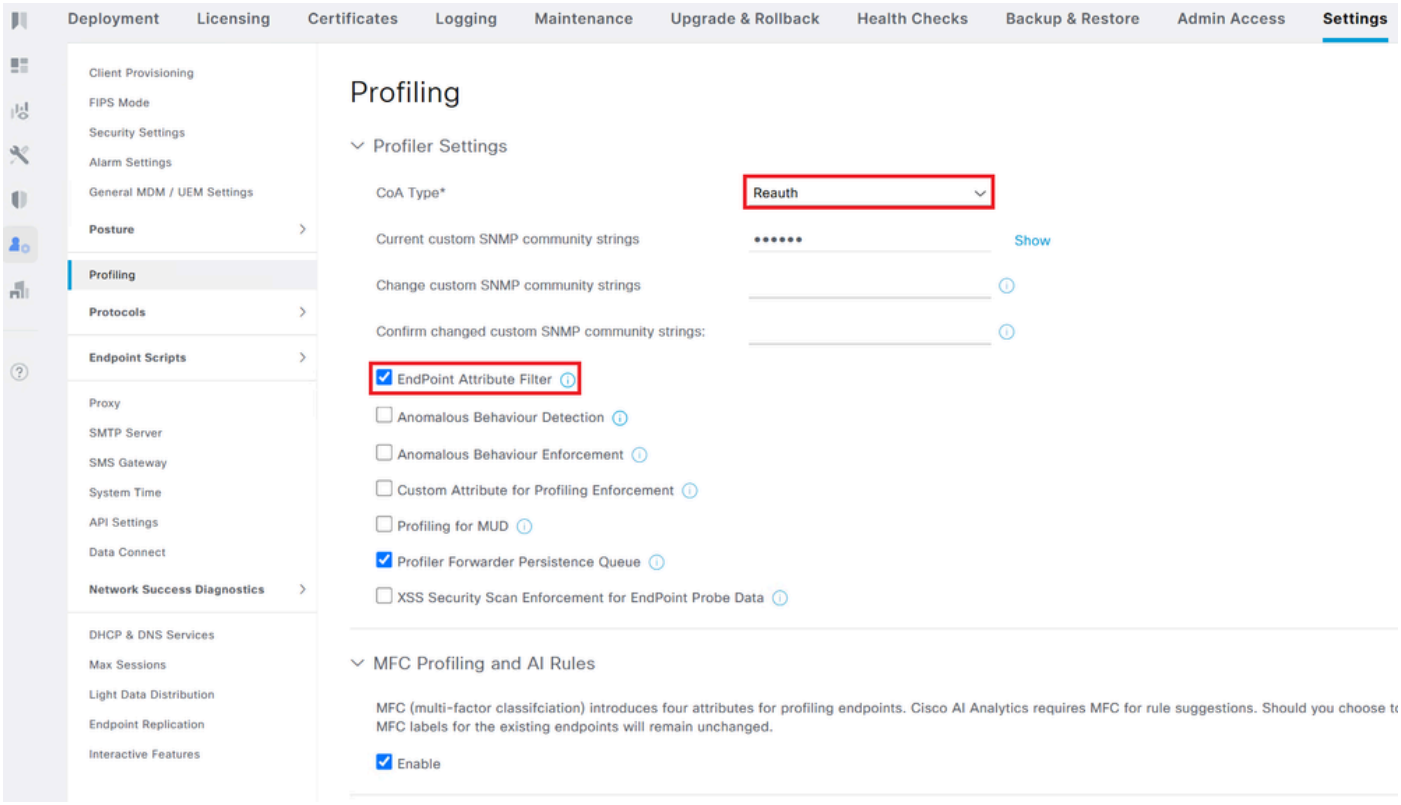
---

3. Activez la sonde Radius sur le noeud de profilage. Accédez à Administration > System > Deployment, choisissez le noeud ISE et cliquez sur l'onglet Profilage Configuration.



---

4. Définissez le type CoA (Change of Authorization) sur Reauth pour appliquer la réauthentification du point de terminaison une fois profilé. En outre, assurez-vous que le filtre d'attribut de point de terminaison est coché. Accédez à Administration > System > Settings > Profilage.

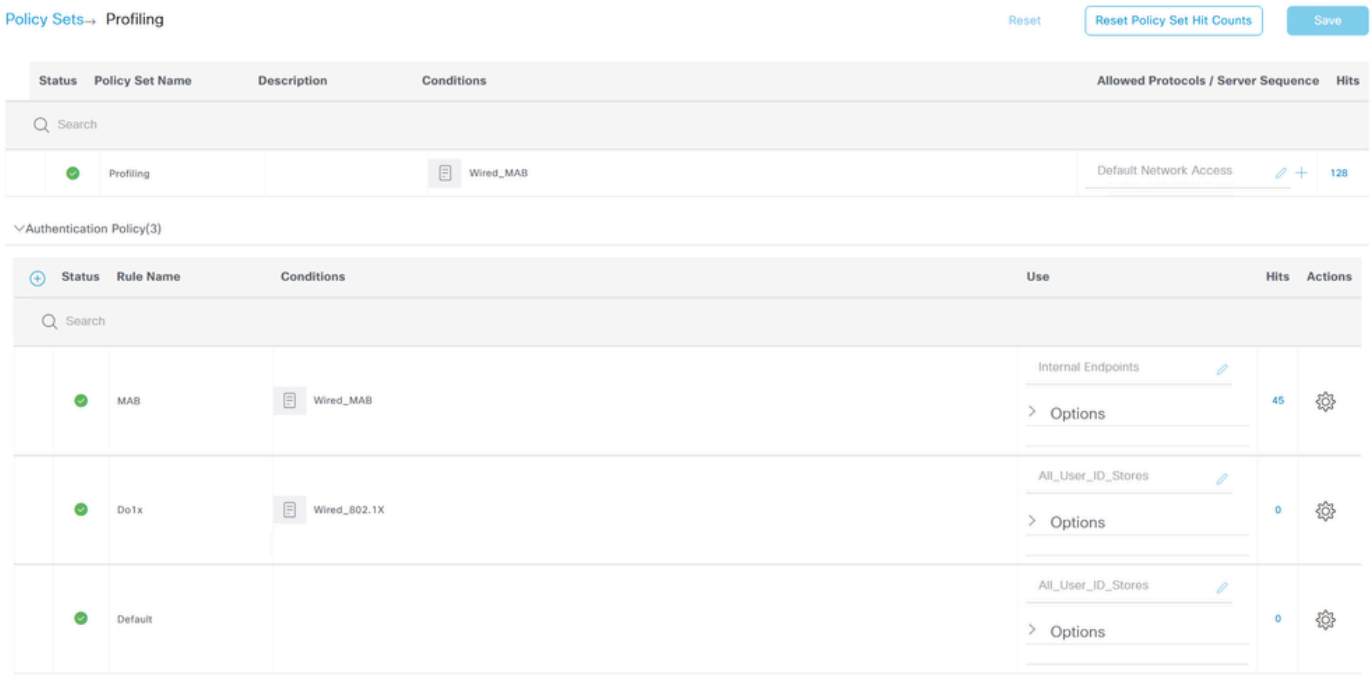


Remarque : Il est recommandé d'activer le filtre d'attribut de point de terminaison dans les déploiements de production afin d'éviter les problèmes de performances lorsque trop de données de profileur inutiles sont collectées.

Pour ajouter un attribut à la liste verte qui n'est pas présente actuellement, vous pouvez créer une condition et une stratégie de profileur qui utilise l'attribut. L'attribut peut être automatiquement ajouté à la liste verte des attributs stockés et répliqués. Si un point de terminaison reste classé comme Inconnu, vérifiez ses attributs collectés dans la Visibilité du contexte ou la Classification des points de terminaison et comparez-les avec les conditions et les facteurs de certitude configurés dans la stratégie de profilage prévue. Une concordance OUI seule n'est pas toujours suffisante pour répondre à un facteur de certitude minimum de profils spécifiques.

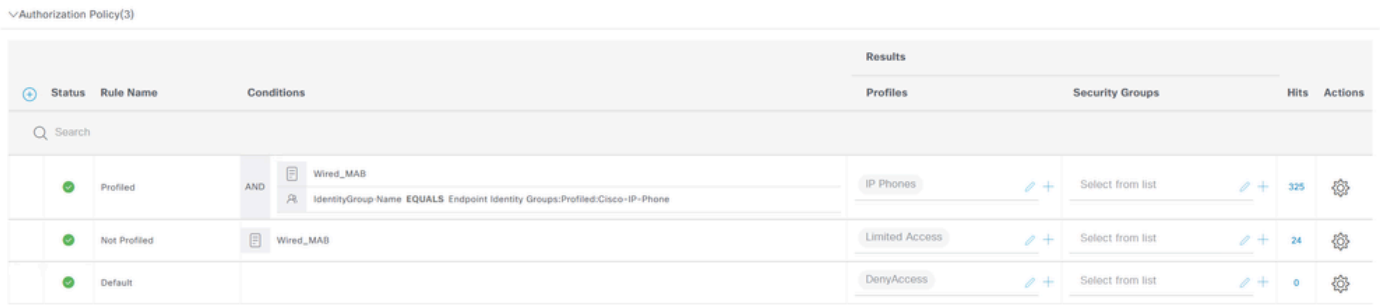
---

5. Configuration des règles d'authentification ISE :



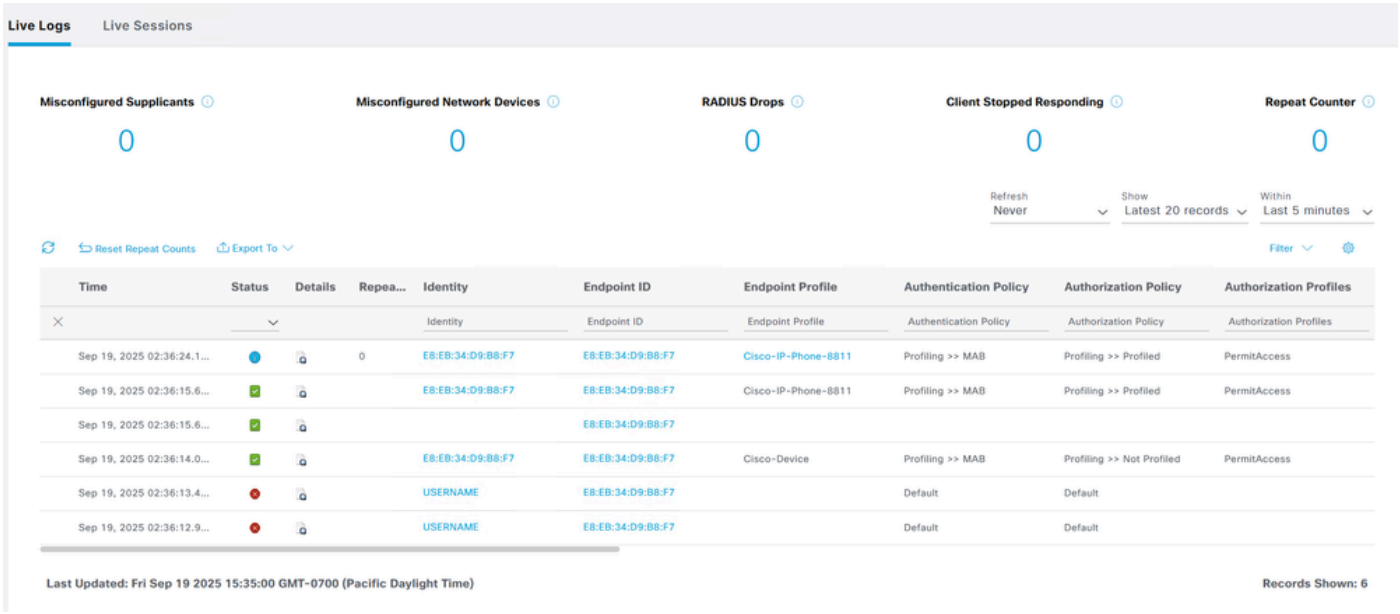
6. Configurez les règles d'autorisation ISE. La règle Téléphone IP Cisco profilé est utilisée, qui est préconfigurée sur ISE :

Vous pouvez configurer une stratégie d'autorisation qui peut agir comme une stratégie d'interception, ce qui permet aux points d'extrémité d'être autorisés sur le réseau (avec un accès limité) pour garantir que les attributs sont envoyés dans les paquets de comptabilité. En outre, créez une autre stratégie qui peut être mise en correspondance une fois que les périphériques sont profilés, en veillant à ce qu'ils puissent accéder aux ressources nécessaires sur le réseau.



Vérifier

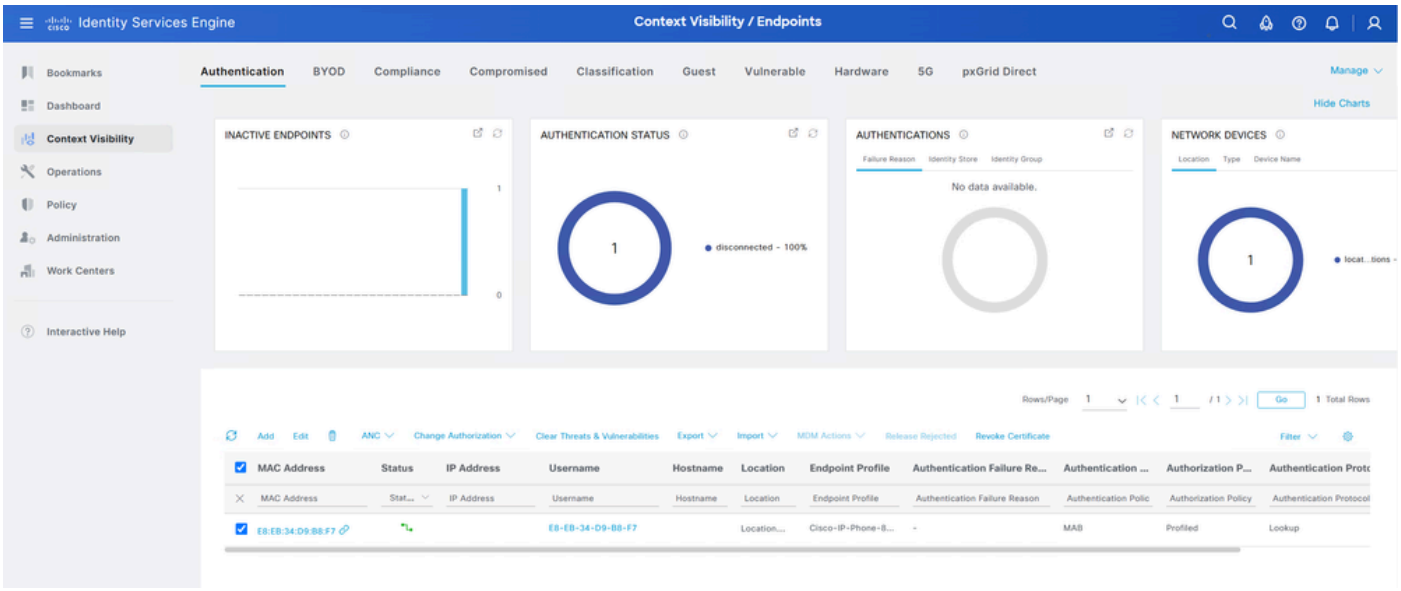
Pour vérifier si le profilage fonctionne correctement, référez-vous à Opérations > Radius > Journaux actifs sur ISE :

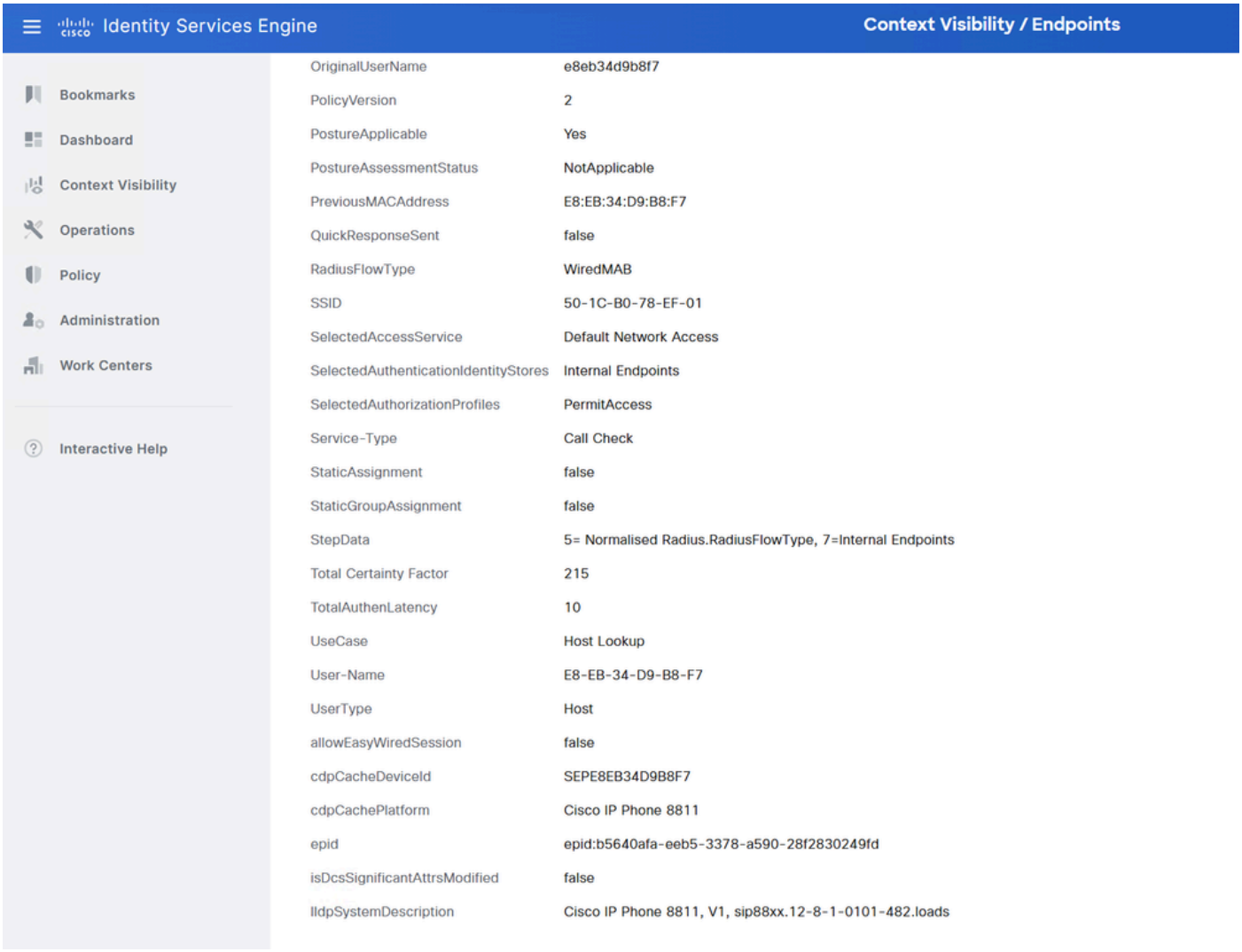


Dans cet exemple de téléphone IP, 802.1X ne s'authentifie pas, de sorte que le commutateur revient à MAB en fonction de l'ordre de méthode configuré. Ce comportement est attendu pour les terminaux qui n'utilisent pas la norme 802.1X.

L'authentification MAB a réussi à 14 h 36 14. Dans le journal en direct, le périphérique est initialement profilé en tant que périphérique Cisco, car l'adresse MAC OUI est associée à Cisco, ce qui correspond à la politique de profilage prédéfinie de Cisco-Device. Une fois que le périphérique reçoit l'accès réseau, le commutateur envoie les attributs CDP et LLDP dans les paquets de comptabilité Radius. À 14 h 36 min 15 s, ISE crée le profil du terminal et envoie une CoA pour forcer la réauthentification. Une fois que la CoA a réussi, le terminal se réauthentifie et correspond à la stratégie d'autorisation pour les téléphones IP Cisco.

Dans Administration > Identity Management > Identities > Endpoints, vous pouvez filtrer par l'adresse MAC du terminal testé et voir les types d'attributs collectés par la sonde Radius et leurs valeurs :





Comme vous pouvez l'observer, le facteur de certitude total calculé est de 215 dans ce scénario. Elle provient du fait que le terminal correspond également au profil Cisco-Device (avec un facteur

de certitude total de 30) et au profil Cisco-IP-Phone (avec un facteur de certitude total de 45). En outre, le profileur correspond également aux deux conditions du profil du téléphone IP Cisco 8811, le facteur de certitude de ce profil étant de 140 (70 pour chaque attribut conformément à la politique de profilage). Pour résumer : 30 + 45 + 70 + 70 = 215.

Dépannage

Étape 1 : vérification des informations collectées par le protocole CDP/LLDP

```
Switch#show cdp neighbors GigabitEthernet1/0/1 details
-------------------------
Device ID: SEPE8EB34D9B8F7
Entry address(es):
Platform: Cisco IP Phone 8811,  Capabilities: Host Phone Two-port Mac Relay
Interface: GigabitEthernet1/0/1,  Port ID (outgoing port): Port 1
Holdtime : 151 sec
Second Port Status: Down

Version :
sip88xx.12-8-1-0101-482.loads

advertisement version: 2
Peer Source MAC: e8eb.34d9.b8f7
Duplex: full
Power drawn: 6.086 Watts
Power request id: 63418, Power management id: 4
Power request levels are:6086 0 0 0 0


Switch#show lldp neighbors GigabitEthernet1/0/1 details
------------------------------------------------
Local Intf: Gi1/0/1
Local Intf service instance: -
Chassis id: 0.0.0.0
Port id: E8EB34D9B8F7:P1
Port Description: SW PORT
System Name: SEPE8EB34D9B8F7

System Description:
Cisco IP Phone 8811, V1, sip88xx.12-8-1-0101-482.loads

Time remaining: 175 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: 30
```

```
Vlan ID: - not advertised
Peer Source MAC: e8eb.34d9.b8f7

MED Information:

    MED Codes:
          (NP) Network Policy, (LI) Location Identification
          (PS) Power Source Entity, (PD) Power Device
          (IN) Inventory

    H/W revision: 1
    F/W revision: sb2388xx.BE-01-027.sbn size=-1

    S/W revision: sip88xx.12-8-1-0101-482.loads
    Serial number: FCH25023CZN
    Manufacturer: Cisco Systems, Inc.
    Model: CP-8811
    Capabilities: NP, PD, IN
    Device type: Endpoint Class III
    Network Policy(Voice): VLAN 101, tagged, Layer-2 priority: 5, DSCP: 46
    Network Policy(Voice Signal): VLAN 101, tagged, Layer-2 priority: 4, DSCP: 32
    PD device, Power source: PSE, Power Priority: Unknown, Wattage: 5.9
    Location - not advertised


Total entries displayed: 1
```

Si vous ne voyez aucune donnée collectée, vérifiez et vérifiez l'état de la session d'authentification sur le commutateur (elle doit aboutir) :

```
OCEAN#sh access-session int gig1/0/1 det
            Interface:  GigabitEthernet1/0/1
               IIF-ID:  0x172041DB
          MAC Address:  e8eb.34d9.b8f7
         IPv6 Address:  Unknown
         IPv4 Address:  Unknown
            User-Name:  E8-EB-34-D9-B8-F7
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-domain
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  F24D300A0000001B9A787BED
      Acct Session ID:  0x0000012b
               Handle:  0x79000011
       Current Policy:  POLICY_Gi1/0/1


Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
      Security Policy:  Should Secure
      Security Status:  Link Unsecured

Server Policies:
```

```
Method status list:
       Method           State
        dot1x           Stopped
          mab           Authc Success
```

Vérifiez si les protocoles CDP et LLDP sont activés. Vérifiez s'il existe des commandes autres que celles par défaut concernant CDP/LLDP et comment elles peuvent affecter la récupération des attributs à partir du point d'extrémité.

```
Switch#show running-config all | include cdp run
cdp run
Switch#show running-config all | include lldp run
lldp run
```

Vérifiez dans le guide de configuration de votre terminal s'il prend en charge CDP/LLDP, etc.

Étape 2. Vérification du cache du capteur de périphérique

```
Switch#show device-sensor cache interface GigabitEthernet1/0/1
Device: e8eb.34d9.b8f7 on port GigabitEthernet1/0/1
-------------------------------------------------------------------------------
Proto Type:Name                       Len Value                       Text
LLDP     6:system-description          56 0C 36 43 69 73 63 6F 20 49  .6Cisco I
                                          50 20 50 68 6F 6E 65 20 38  P Phone 8
                                          38 31 31 2C 20 56 31 2C 20  811, V1,
                                          73 69 70 38 38 78 78 2E 31  sip88xx.1
                                          32 2D 38 2D 31 2D 30 31 30  2-8-1-010
                                          31 2D 34 38 32 2E 6C 6F 61  1-482.loa
                                          64 73                       ds
CDP      6:platform-type               23 00 06 00 17 43 69 73 63 6F  ....Cisco
                                          20 49 50 20 50 68 6F 6E 65   IP Phone
                                          20 38 38 31 31               8811
CDP      1:device-name                 19 00 01 00 13 53 45 50 45 38  ....SEPE8
                                          45 42 33 34 44 39 42 38 46  EB34D9B8F
                                          37                          7
```

Si vous ne voyez aucune donnée dans ce champ ou si les informations ne sont pas complètes, vérifiez et exécutez les commandes device-sensor ; en particulier, filter-lists et filter-specs.

Étape 3. Vérifier si les attributs sont présents dans Radius Accounting

Vous pouvez vérifier l'exécution de la commande debug radius sur le commutateur ou l'exécution de la capture de paquets entre le commutateur et ISE.

Débogage Radius

```
Switch#debug radius
Switch#set platform software trace smd switch active R0 dot1x-all verbose
Switch#show platform software trace level smd switch active R0 | inc dot1x
dot1x Notice
dot1x-all Verbose
dot1x-redun Notice
```

Pour désactiver les débogages, vous pouvez exécuter cette commande :

```
Switch#set platform software trace all notice
```

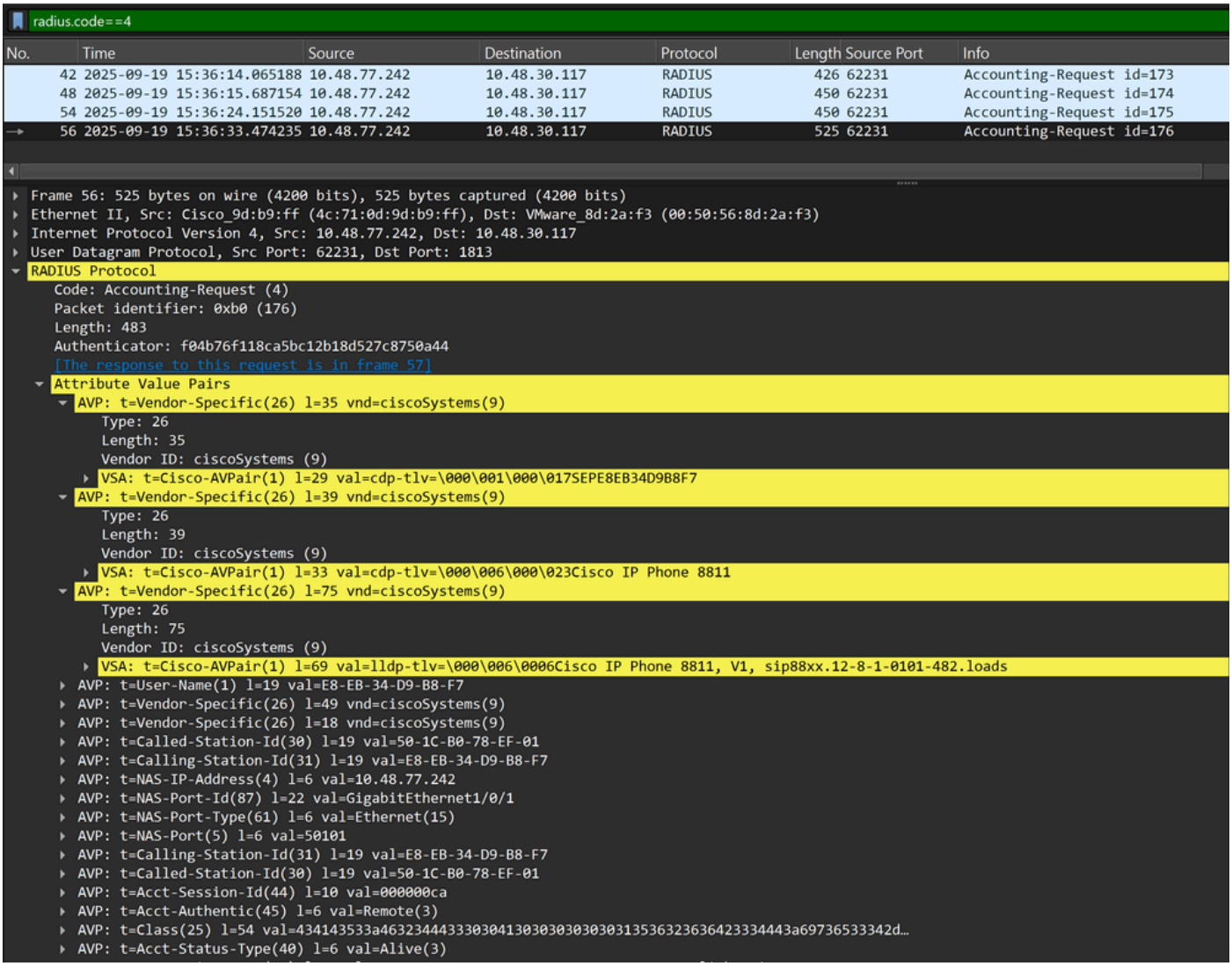
Pour afficher les journaux :

```
Switch#show logging process smd | include RADIUS

2025/09/19 14:36:25.431793040 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS: Send Accounting-Request
2025/09/19 14:36:25.431800182 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  authenticator 37 19 72
2025/09/19 14:36:25.431804371 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Vendor, Cisco       [26]
2025/09/19 14:36:25.431808600 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:   Cisco AVpair       [1]
2025/09/19 14:36:25.431811616 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Vendor, Cisco       [26]
2025/09/19 14:36:25.431815180 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:   Cisco AVpair       [1]
2025/09/19 14:36:25.431817947 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Vendor, Cisco       [26]
2025/09/19 14:36:25.431822305 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:   Cisco AVpair       [1]
2025/09/19 14:36:25.431826085 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  User-Name           [1]
2025/09/19 14:36:25.431828885 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Vendor, Cisco       [26]
2025/09/19 14:36:25.431832691 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:   Cisco AVpair       [1]
2025/09/19 14:36:25.431835418 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Vendor, Cisco       [26]
2025/09/19 14:36:25.431839009 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:   Cisco AVpair       [1]
2025/09/19 14:36:25.431842591 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Called-Station-Id   [30]
2025/09/19 14:36:25.431846145 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Calling-Station-Id  [31]
2025/09/19 14:36:25.431851298 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  NAS-IP-Address      [4]
2025/09/19 14:36:25.431854702 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  NAS-Port-Id         [87]
2025/09/19 14:36:25.431859269 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  NAS-Port-Type       [61]
2025/09/19 14:36:25.431863238 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  NAS-Port            [5]
2025/09/19 14:36:25.431866514 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Calling-Station-Id  [31]
2025/09/19 14:36:25.431870007 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Called-Station-Id   [30]
2025/09/19 14:36:25.431873587 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Acct-Session-Id     [44]
2025/09/19 14:36:25.431882560 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Acct-Authentic      [45]
2025/09/19 14:36:25.431885338 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Class               [25]
2025/09/19 14:36:25.431933331 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Acct-Status-Type    [40]
2025/09/19 14:36:25.431937105 {smd_R0-0}{1}: [radius] [23554]: (info): RADIUS:  Event-Timestamp     [55]
```

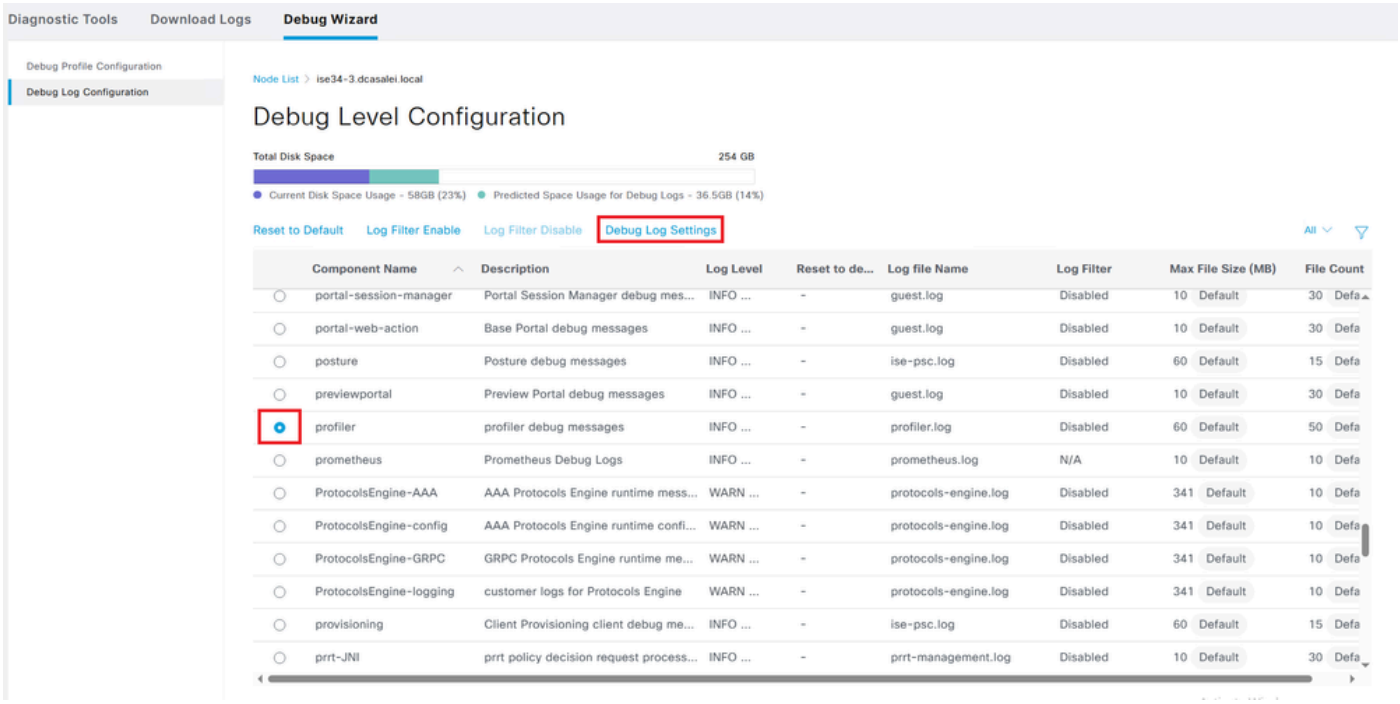
```
2025/09/19 14:36:25.431940547 {smd_RO-0}{1}: [radius] [23554]: (info): RADIUS:  Acct-Delay-Time     [41
2025/09/19 14:36:25.431973200 {smd_RO-0}{1}: [radius] [23554]: (info): RADIUS: Started 5 sec timeout
```

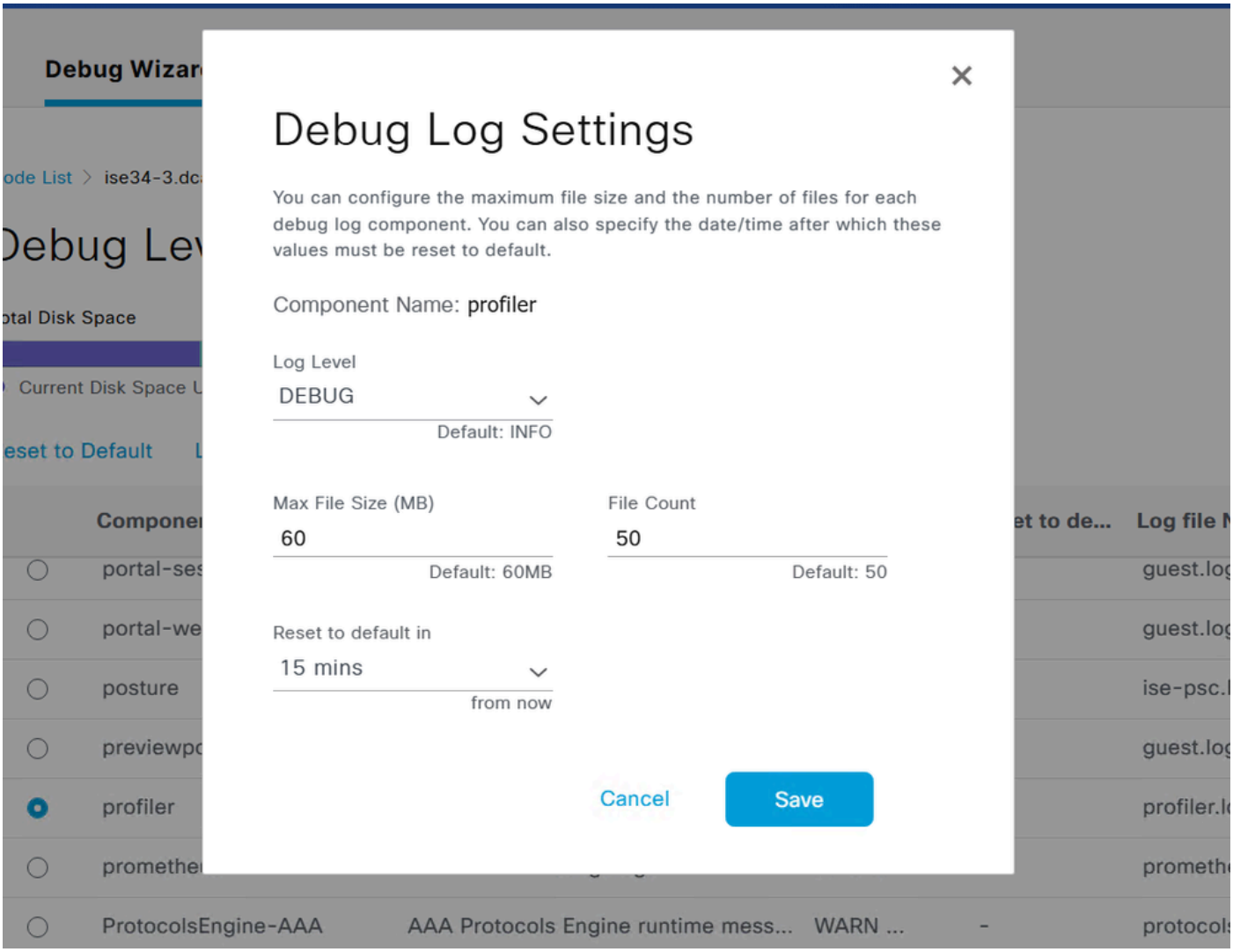
Capture de paquets



Étape 4. Vérification des débogages du profileur sur ISE

Si les attributs ont été envoyés à partir du commutateur, il est possible de vérifier s'ils ont été reçus sur ISE. Pour vérifier cela, activez les débogages du profileur pour le noeud PSN correct Administration > System > Logging > Debug Log Configuration > PSN > Profiler > Debug et effectuez une nouvelle fois l'authentification du point de terminaison.


Diagnostic Tools
Download Logs
Debug Wizard
Debug Profile Configuration
Debug Log Configuration
Node List > ise34-3.dcasalei.local
Debug Level Configuration
Total Disk Space
254 GB
Current Disk Space Usage - 58GB (23%)
Predicted Space Usage for Debug Logs - 36.5GB (14%)
Reset to Default
Log Filter Enable
Log Filter Disable
Debug Log Settings
Component Name
Description
Log Level
Reset to de...
Log file Name
Log Filter
Max File Size (MB)
File Count
portal-session-manager
Portal Session Manager debug mes...
guest.log
Disabled
portal-web-action
Base Portal debug messages
guest.log
Disabled
posture
Posture debug messages
ise-psc.log
Disabled
previewportal
Preview Portal debug messages
guest.log
Disabled
profiler
profiler debug messages
profiler.log
Disabled
prometheus
Prometheus Debug Logs
prometheus.log
N/A
ProtocolsEngine-AAA
AAA Protocols Engine runtime mess...
protocols-engine.log
Disabled
ProtocolsEngine-config
AAA Protocols Engine runtime confi...
protocols-engine.log
Disabled
ProtocolsEngine-GRPC
GRPC Protocols Engine runtime me...
protocols-engine.log
Disabled
ProtocolsEngine-logging
customer logs for Protocols Engine
protocols-engine.log
Disabled
provisioning
Client Provisioning client debug me...
ise-psc.log
Disabled
prrt-JNI
prrt policy decision request process...
prrt-management.log
Disabled


Debug Log Settings
You can configure the maximum file size and the number of files for each debug log component. You can also specify the date/time after which these values must be reset to default.
Component Name: profiler
Log Level
DEBUG
Default: INFO
Max File Size (MB)
60
Default: 60MB
File Count
50
Default: 50
Reset to default in
15 mins
from now
Cancel
Save

Recherchez les informations suivantes :

- Débogage indiquant que la sonde Radius a reçu des attributs :

```
2025-09-21 07:14:07,574 INFO   [RADIUSParser-1-thread-2][[]] cisco.profiler.probes.radius.RadiusPa
2025-09-21 07:14:07,574 DEBUG  [RADIUSParser-1-thread-2][[]] cisco.profiler.probes.radius.RadiusPa
```

- Débogage indiquant que les attributs ont été analysés avec succès :

```
2025-09-21 07:14:07,574 DEBUG  [RADIUSParser-1-thread-2][[]] cisco.profiler.probes.radius.RadiusPa
2025-09-21 07:14:07,574 DEBUG  [RADIUSParser-1-thread-2][[]] cisco.profiler.probes.radius.RadiusPa
2025-09-21 07:14:07,574 DEBUG  [RADIUSParser-1-thread-2][[]] cisco.profiler.probes.radius.RadiusPa
```

- Débogage indiquant que les attributs ont été traités par le redirecteur :

```
2025-09-21 07:14:08,709 DEBUG  [pool-55-thread-8][[]] cisco.profiler.infrastructure.probemgr.Forwa
MAC: E8:EB:34:D9:B8:F7
    Attribute:AAA-Server     value:ise34-3
        (... more attributes ...)
         Attribute:User-Name     value:CP-8811-SEPE8EB34D9B8F7
        Attribute:cdpCacheDeviceId     value:SEPE8EB34D9B8F7
        Attribute:cdpCachePlatform     value:Cisco IP Phone 8811
        Attribute:lldpSystemDescription     value:Cisco IP Phone 8811, V1, sip88xx.12-8-1-0101-482
        Attribute:SkipProfiling     value:false
```



Remarque : Un redirecteur stocke les terminaux dans la base de données Cisco ISE avec les données de leurs attributs, puis informe l'analyseur des nouveaux terminaux détectés sur votre réseau. L'analyseur classe les points d'extrémité en groupes d'identité de points d'extrémité et stocke les points d'extrémité avec les profils correspondants dans la base de données.

Étape 5. Reclassification Du Profil Après Réception De Nouveaux Attributs

Généralement, après l'ajout de nouveaux attributs à une collection existante pour un périphérique spécifique, le périphérique ou le point de terminaison est ajouté à la file d'attente de profilage pour vérifier s'il doit être affecté à un profil différent en fonction des nouveaux attributs :

```
2025-09-21 07:14:08,714 INFO   [pool-3352-thread-8][[]] cisco.profiler.infrastructure.profiling.Profile
2025-09-21 07:14:08,724 DEBUG  [pool-3352-thread-8][[]] cisco.profiler.infrastructure.profiling.Profile
2025-09-21 07:14:08,727 DEBUG  [pool-3352-thread-8][[]] cisco.profiler.infrastructure.profiling.Profile
2025-09-21 07:14:08,729 DEBUG  [pool-3352-thread-8][[]] cisco.profiler.infrastructure.profiling.Profile
2025-09-21 07:14:08,729 DEBUG  [pool-3352-thread-8][[]] cisco.profiler.infrastructure.profiling.Profile
```

Informations connexes

- Zone de conception Campus et filiales
- Configuration des stratégies de profileur
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.