

# Comprendre la classification Wifi Analytics for Endpoint sur ISE 3.3

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Configurations sur WLC](#)

[Étape 1. Activer globalement la fonctionnalité de classification des périphériques](#)

[Étape 2. Activer le cache TLV et le profilage RADIUS](#)

[Configurations sur ISE](#)

[Étape 1. Activer les services de profilage dans les PSN dans le déploiement](#)

[Étape 2. Activer la sonde de profilage RADIUS sur ISE PSN](#)

[Étape 3. Définir le type CoA et le filtre d'attribut de point final](#)

[Étape 4. Configurer les stratégies d'autorisation avec les attributs de données WiFi Analytics](#)

[Vérifier](#)

[Dépannage](#)

[Étape 1. Les paquets de comptabilisation atteignent ISE](#)

[Étape 2. ISE analyse le paquet de comptabilité avec les attributs de point de terminaison](#)

[Étape 3. Les attributs du point de terminaison sont mis à jour et le point de terminaison est classifié](#)

[Étape 4. CoA et réauthentification](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit le fonctionnement de WiFi Analytics for Endpoint Classification. Il décrit également comment le configurer, le vérifier et le dépanner.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration des contrôleurs LAN sans fil (WLC) du 9800
- Configuration ISE (Identity Services Engine)
- Authentification RADIUS. Flux de paquets et terminologie AAA (Authorization and Accounting)

Ce document suppose qu'il existe déjà un WLAN qui authentifie les clients utilisant ISE comme serveur RADIUS.

Pour que cette fonctionnalité fonctionne, il est nécessaire d'avoir au moins :

- 9800 WLC Cisco IOS® XE Dublin 17.10.1
- Identifiez le moteur de services v3.3.
- Points d'accès 802.11ac Wave2 ou 802.11ax (Wi-Fi 6/6E)

## Composants utilisés

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

- WLC 9800 Cisco IOSXE v17.12.x
- Identity Services Engine (ISE) v3.3
- Périphérique Android 13

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

Grâce au WiFi Device Analytics, le WLC Cisco 9800 peut apprendre des attributs, tels que le numéro de modèle et la version du système d'exploitation, à partir d'un ensemble de terminaux connectés à ce périphérique, et les partager avec ISE. ISE peut ensuite utiliser ces informations à des fins de classification des terminaux, également appelée profilage.

Actuellement, WiFi Analytics est pris en charge pour ces fournisseurs :

- Pomme
- Intel
- Samsung

Le WLC partage les informations d'attribut avec le serveur ISE à l'aide de paquets de comptabilité RADIUS.

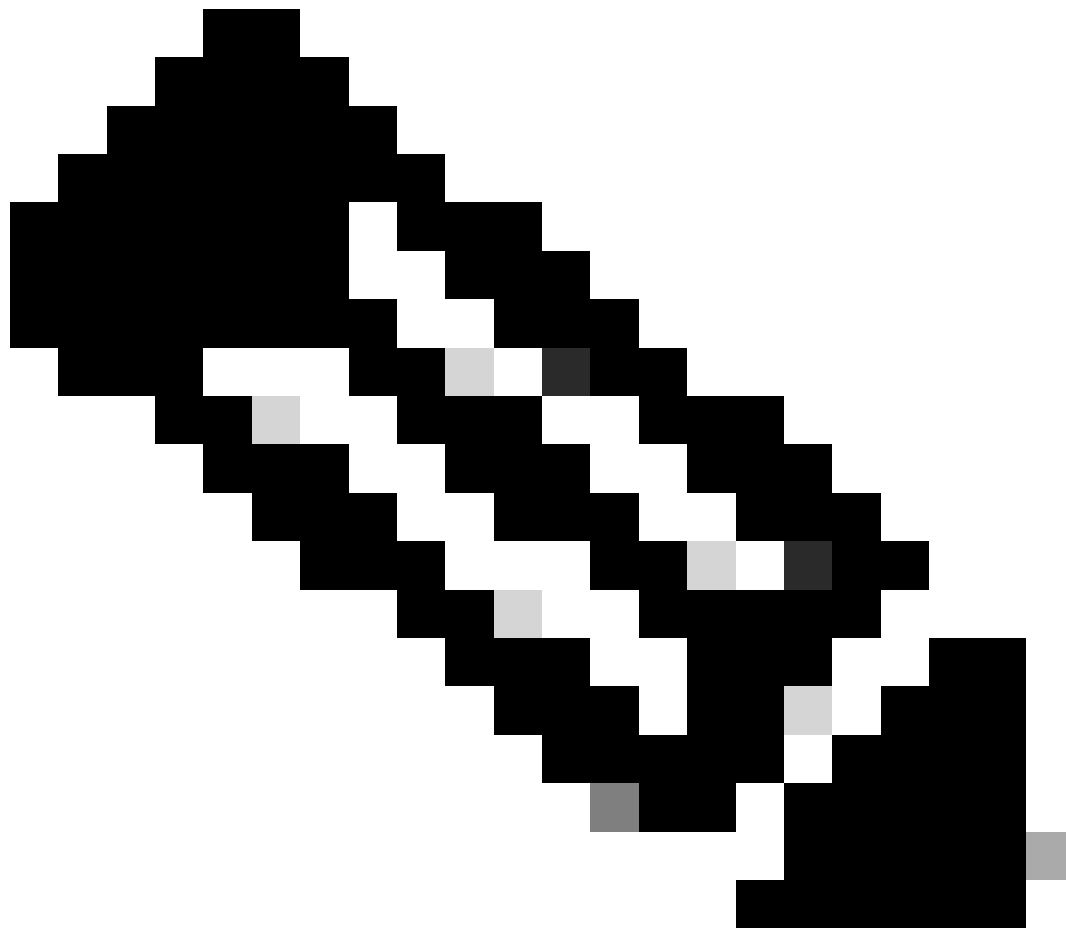


Flux de données WiFi Analytics

Il est important de se rappeler que les paquets de compte RADIUS sur un flux RADIUS AAA sont envoyés uniquement après que le serveur RADIUS ait envoyé un paquet d'acceptation d'accès RADIUS en réponse à la tentative d'authentification du point d'extrémité. En d'autres termes, le WLC partage les informations d'attribut de point d'extrémité seulement après qu'une session RADIUS pour ce point d'extrémité est établie entre le serveur RADIUS (ISE) et le périphérique d'accès réseau (WLC).

Voici tous les attributs qu'ISE peut utiliser pour la classification et l'autorisation des terminaux :

- INFO\_PÉRIPHÉRIQUE\_VERSION\_DU\_MICROPROGRAMME
- MODÈLE\_MATÉRIEL\_INFO\_PÉRIPHÉRIQUE
- INFO\_PÉRIPHÉRIQUE\_MODÈLE\_FABRICANT
- NOM\_MODÈLE\_INFO\_PÉRIPHÉRIQUE
- NUMÉRO\_MODÈLE\_INFO\_PÉRIPHÉRIQUE
- VERSION\_OS\_INFO\_PÉRIPHÉRIQUE
- TYPE\_FOURNISSEUR\_INFO\_PÉRIPHÉRIQUE



Remarque : le WLC peut envoyer plus d'attributs selon le type de point d'extrémité connecté, mais seuls ceux listés peuvent être utilisés pour la création de stratégies d'autorisation dans ISE.

---

Une fois qu'ISE a reçu le paquet Accounting, il peut traiter et utiliser ces données d'analyse et les utiliser pour réaffecter un profil/groupe d'identité de point d'extrémité.

Les attributs WiFi Endpoint Analytics sont répertoriés dans le dictionnaire WiFi\_Device\_Analytics. Les administrateurs réseau peuvent inclure ces attributs dans les politiques et conditions d'autorisation des terminaux.

## Select attribute for condition



|  | Dictionary                | Attribute                | ID | Info |
|--|---------------------------|--------------------------|----|------|
|  | Wifi_Device_Analytics ✓ X | Attribute                | ID |      |
|  | Wifi_Device_Analytics     | DEVICE_INFO_FIRMWARE_... |    | ⓘ    |
|  | Wifi_Device_Analytics     | DEVICE_INFO_HW_MODEL     |    | ⓘ    |
|  | Wifi_Device_Analytics     | DEVICE_INFO_MANUFACT...  |    | ⓘ    |
|  | Wifi_Device_Analytics     | DEVICE_INFO_MODEL_NA...  |    | ⓘ    |
|  | Wifi_Device_Analytics     | DEVICE_INFO_MODEL_NUM    |    | ⓘ    |
|  | Wifi_Device_Analytics     | DEVICE_INFO_OS_VERSION   |    | ⓘ    |
|  | Wifi_Device_Analytics     | DEVICE_INFO_VENDOR_T...  |    | ⓘ    |

Dictionnaire d'analyse des périphériques WiFi

Si des modifications sont apportées aux valeurs d'attribut actuelles qu'ISE stocke pour le point de terminaison, ISE initie alors une modification d'autorisation (CoA), ce qui permet d'évaluer le point de terminaison en tenant compte des attributs mis à jour.

## Configurer

### Configurations sur WLC

Étape 1. Activer globalement la fonctionnalité de classification des périphériques

Accédez à Configuration > Wireless > Wireless Global et cochez la case Device Classification.

|                                  |                                      |
|----------------------------------|--------------------------------------|
| Default Mobility Domain *        | <input type="text" value="default"/> |
| RF Group Name*                   | <input type="text" value="default"/> |
| Maximum Login Sessions Per User* | <input type="text" value="0"/>       |
| Management Via Wireless          | <input type="checkbox"/>             |
| <b>Device Classification</b>     | <input checked="" type="checkbox"/>  |
| AP LAG Mode                      | <input type="checkbox"/>             |
| Dot15 Radio                      | <input type="checkbox"/>             |
| Wireless Password Policy         | <input type="text" value="None"/> ⓘ  |

Configuration de la classification des périphériques

## Étape 2. Activer le cache TLV et le profilage RADIUS

Accédez à Configuration > Tags and Profiles > Policy et sélectionnez le Policy Profile utilisé par le WLAN auquel les clients RADIUS se connectent.

|                                     | Admin Status | Associated Policy Tags | Policy Profile Name    | Description            |
|-------------------------------------|--------------|------------------------|------------------------|------------------------|
| <input checked="" type="checkbox"/> | ✔            | 🔗                      | ise-policy             |                        |
| <input type="checkbox"/>            | ⊘            |                        | default-policy-profile | default policy profile |

Sélection de stratégie sans fil

Cliquez sur Access Policies et vérifiez les options RADIUS Profiling, HTTP TLV Caching et DHCP TLV Caching. En raison de l'action entreprise à l'étape précédente, l'état global de la classification des périphériques affiche désormais l'état Activé.

## Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General **Access Policies** QOS and AVC Mobility Advanced

RADIUS Profiling   
HTTP TLV Caching   
DHCP TLV Caching

### WLAN Local Profiling

Global State of Device Classification **Enabled** ⓘ

Local Subscriber Policy Name  ⓘ

### VLAN

VLAN/VLAN Group  ⓘ

Multicast VLAN

### WLAN ACL

IPv4 ACL  ⓘ

IPv6 ACL  ⓘ

### URL Filters ⓘ

Pre Auth  ⓘ

Post Auth  ⓘ

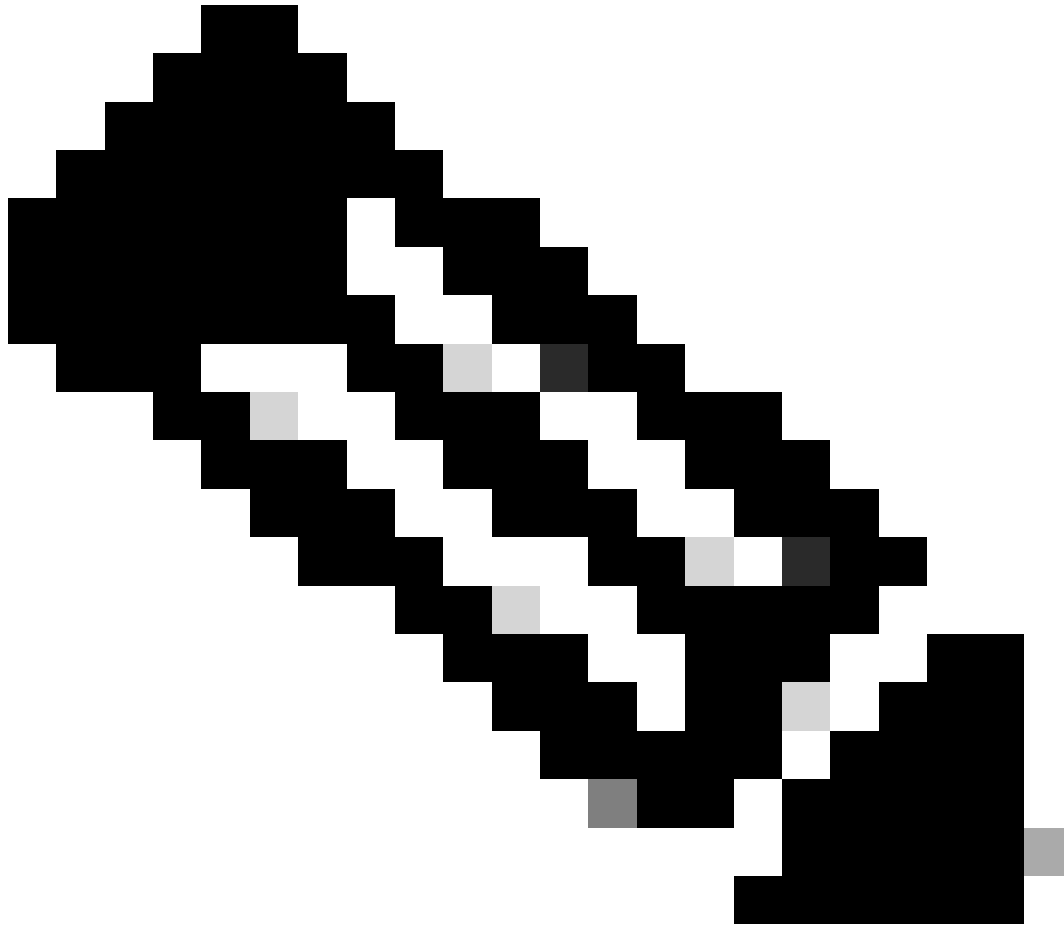
↶ Cancel

📄 Update & Apply to Device

Configuration du profilage et de la mise en cache RADIUS

Connectez-vous à l'interface de ligne de commande WLC et activez la comptabilité TLV dot11.

```
vimontes-wlc#configure terminal
vimontes-wlc(config)#wireless profile policy policy-profile-name
vimontes-wlc(config-wireless-policy)#dot11-tlv-accounting
```



**Remarque** : le profil de stratégie sans fil doit être désactivé avant d'utiliser cette commande. Cette commande n'est disponible que sur la version 17.10.1 de Cisco IOS XE Dublin et les versions ultérieures.

---



Configurations sur ISE







Étape 1. Activer les services de profilage dans les PSN dans le déploiement


Accédez à **Administration > Deployment** et cliquez sur le nom du PSN.



## Deployment Nodes

Selected 0 Total 1  

 Edit  Register  Syncup  Deregister All  


| <input type="checkbox"/> | Hostname | Personas                                   | Role(s)    | Services         | Node Status   |
|--------------------------|----------|--|------------|------------------|---|
| <input type="checkbox"/> | iselab   | Administration, Monitoring, Policy Service | STANDALONE | SESSION,PROFILER |  |


Sélection du noeud ISE PSN


Faites défiler jusqu'à la section **Policy Service** et cochez la case **Enable Profiling Service**. Cliquez sur le bouton **Enregistrer**.

Policy Service


Enable Session Services


Include Node in Node Group  

Enable Profiling Service 


Enable Threat Centric NAC Service 

> Enable SXP Service

Enable Device Admin Service 

Enable Passive Identity Service 

---

> pxGrid 

---

[Reset](#)

Configuration des services de profilage

Étape 2. Activer la sonde de profilage RADIUS sur ISE PSN

Faites défiler la page jusqu'en haut et cliquez sur l'onglet **Configuration du profilage**. Cette option affiche toutes les sondes de profilage disponibles sur ISE. Activez la sonde **RADIUS** et cliquez sur **Save**.

## Edit Node

General Settings

**Profiling Configuration**

> NETFLOW

> DHCP

> DHCPSPAN

> HTTP

---

**Remarque** : le paquet CoA a toujours un champ d'identité vide, mais l'ID de point d'extrémité est le même que dans le premier paquet d'authentification.

---

Cliquez sur l'**icône** située dans la colonne **Détails** de l'enregistrement Modification de l'autorisation.

---

Sep 27, 2023 06:19:24.36...



0A:5A:F0:B3:B5:9C

*Accès aux détails des paquets CoA*

Les informations détaillées sur la CoA s'affichent dans un nouvel onglet du navigateur. Faites défiler jusqu'à la section **Autres attributs**.

Le composant source CoA s'affiche en tant que profileur. La raison CoA s'affiche sous la forme Modification du groupe d'identité/stratégie/profil logique du point de terminaison utilisé dans les stratégies d'autorisation.

## Other Attributes

|                        |   |
|------------------------|---|
| ConfigVersionId        | 1493  |
| Event-Timestamp        | 1695838764  |
| Device CoA type        | Cisco CoA   |
| Device CoA port        | 1700  |
| NetworkDeviceProfileId | b0699505-3150-4215-a80e-6753d45bf56c  |
| IsThirdPartyDeviceFlow | false   |
| AcsSessionID           | 89f67978-be8f-4145-8801-45e2fffa1fe8  |
| TotalAuthenLatency     | 3621649740  |
| ClientLatency          | 3621649732  |
| CoASourceComponent     | Profiler  |
| CoAReason              | Change in endpoint identity group/policy/logical profile which are used in authorization policies                       |
| Network Device Profile | Cisco   |
| Location               | Location#All Locations  |
| Device Type            | Device Type#All Device Types  |
| IPSEC                  | IPSEC#Is IPSEC Device#No  |
| Device IP Address      | 172.16.5.169  |
| CPMSessionID           | A90510AC00000058D7DD0AA7  |
| CiscoAVPair            | subscriber:reauthenticate-type=last,<br>subscriber:command=reauthenticate,<br>audit-session-id=A90510AC00000058D7DD0AA7 |

*Composant déclencheur CoA et raison*

Accédez à l'onglet **Context Visibility > Endpoints > Authentication**. Dans cet onglet, utilisez les filtres pour localiser le point de terminaison de test.

Cliquez sur l'**adresse MAC** du point de terminaison pour accéder aux **attributs** du **point de terminaison**.

| <input type="checkbox"/>            | MAC Address       | Status | IP Address | Username | Hostname     | Location    | Endpoint Profile | Authen...  | Authentication ...   | Authorization P...     |
|-------------------------------------|-------------------|--------|------------|----------|--------------|-------------|------------------|------------|----------------------|------------------------|
| <input checked="" type="checkbox"/> | 0A:5A:F0:B3:B5:9C | Status | IP Address | Username | Hostname     | Location    | Endpoint Profile | Authentic: | Authentication Polic | Authorization Policy   |
| <input type="checkbox"/>            | 0A:5A:F0:B3:B5:9C | ...    |            | bob      | Victor-s-S22 | Location... | Android          | -          | Default              | Wifi Endpoint Analy... |

Point de terminaison sur la visibilité contextuelle

Cette action affiche toutes les informations stockées par ISE sur ce terminal. Cliquez sur la section **Attributs**, puis sélectionnez **Autres attributs**.

MAC ADDRESS: 0A:5A:F0:B3:B5:9C

Username: bob  
Endpoint Profile: Android  
Current IP Address: -  
Location: Location → All Locations

MFC Endpoint Type: Phone  
MFC Hardware Manufacturer: Samsung Electronics Co.,Ltd  
MFC Hardware Model: Samsung Galaxy S22+  
MFC Operating System: Android 13

Applications: **Attributes** | Authentication | Threats | Vulnerabilities

General Attributes | Custom Attributes | **Other Attributes**

Sélection d'un autre attribut de point de terminaison sur la visibilité contextuelle

Faites défiler l'affichage jusqu'à ce que vous trouviez les attributs de **dictionnaire WiFi\_Device\_Analytics**. L'emplacement de ces attributs dans cette section signifie qu'ISE les a reçus avec succès via les paquets de comptabilité et peut être utilisé pour la classification des points de terminaison.

|                              |                     |
|------------------------------|---------------------|
| DEVICE_INFO_COUNTRY_CODE     | Unknown             |
| DEVICE_INFO_DEVICE_FORM      | PHONE               |
| DEVICE_INFO_FIRMWARE_VERSION | WH6                 |
| DEVICE_INFO_MODEL_NUM        | Samsung Galaxy S22+ |
| DEVICE_INFO_OS_VERSION       | Android 13          |
| DEVICE_INFO_SALES_CODE       | MXO                 |
| DEVICE_INFO_VENDOR_TYPE      | SAMSUNG             |

Attributs WiFi Analytics sur la visibilité du contexte

Pour référence, voici des exemples d'attributs Windows 10 et iPhone :

|                               |              |
|-------------------------------|--------------|
| DEVICE_INFO_DEVICE_FORM       | 0            |
| DEVICE_INFO_FIRMWARE_VERSION  | 22.180.02.01 |
| DEVICE_INFO_HW_MODEL          | AX201/AX1650 |
| 160MHZ                        |              |
| DEVICE_INFO_MANUFACTURER_NAME | LENOVO       |
| DEVICE_INFO_MODEL_NAME        | 20RAS0C000   |
| DEVICE_INFO_MODEL_NUM         | LENOVO       |
| 20RAS0C000                    |              |
| DEVICE_INFO_OS_VERSION        | WINDOWS 10   |
| DEVICE_INFO_POWER_TYPE        | AC POWERED   |
| DEVICE_INFO_VENDOR_TYPE       | 3            |

*Exemple d'attributs de point de terminaison Windows 10*

|                         |          |
|-------------------------|----------|
| DEVICE_INFO_DEVICE_FORM | 0        |
| DEVICE_INFO_MODEL_NUM   | IPHONE   |
| 11 PRO                  |          |
| DEVICE_INFO_OS_VERSION  | IOS 16.4 |
| DEVICE_INFO_VENDOR_TYPE | 1        |

*Exemple d'attributs de point de terminaison iPhone*

Étape 1. Les paquets de comptabilisation atteignent ISE

Sur l'interface de ligne de commande WLC, assurez-vous que la **comptabilité TLV DOT11**, la **mise en cache TLV DHCP** et la **mise en cache TLV HTTP** sont activées sur les configurations de profil de stratégie.

```
<#root>
```

```
vimontes-wlc#show running-config | section wireless profile policy policy-profile-name
wireless profile policy policy-profile-name
aaa-override
accounting-list AAA-LIST
```

```
dhcp-tlv-caching
```

```
dot11-tlv-accounting
```

```
http-tlv-caching
```

```
radius-profiling
```

```
no shutdown
```

Collecter les **captures de paquets** sur les extrémités WLC ou ISE lors de la connexion d'un terminal. Vous pouvez utiliser n'importe quel outil d'analyse de paquets bien connu, tel que Wireshark, pour analyser les fichiers collectés.

Filtrer par paquets de comptabilité RADIUS et par ID de station appelante (test de l'adresse MAC du point d'extrémité). Par exemple, ce filtre peut être utilisé :

```
radius.code == 4 && radius.Calling_Station_Id == "xx-xx-xx-xx-xx-xx"
```

Une fois localisé, développez les champs **Cisco-AVPair** pour localiser les **données d'analyse WiFi** dans le paquet Accounting.

```

No. | Time | Source | Destination | Protocol | Length | Info
---|---|---|---|---|---|---
104 2023-09-27 12:19:23.584661 172.16.5.169 172.16.5.112 RADIUS 976 Accounting-Request id=39

> AVP: t=Vendor-Specific(26) l=28 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=36 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=39 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=36 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
  Type: 26
  Length: 49
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=43 val=dot11-device-info=\000\000\000\023Samsung Galaxy S22+
> AVP: t=Vendor-Specific(26) l=33 vnd=ciscoSystems(9)
  Type: 26
  Length: 33
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=27 val=dot11-device-info=\000\001\000\003WH6
> AVP: t=Vendor-Specific(26) l=33 vnd=ciscoSystems(9)
  Type: 26
  Length: 33
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=27 val=dot11-device-info=\000\002\000\003MX0
> AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
  Type: 26
  Length: 31
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=25 val=dot11-device-info=\000\003\000\0011
> AVP: t=Vendor-Specific(26) l=40 vnd=ciscoSystems(9)
  Type: 26
  Length: 40
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=34 val=dot11-device-info=\000\004\000\Android 13
> AVP: t=Vendor-Specific(26) l=37 vnd=ciscoSystems(9)
  Type: 26
  Length: 37
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=31 val=dot11-device-info=\000\005\000\Unknown
> AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
  Type: 26
  Length: 31
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=25 val=dot11-device-info=\000\n\000\0012
> AVP: t=Framed-IP-Address(8) l=6 val=172.16.5.76

```

Attributs TLV de point de terminaison dans un paquet de comptabilisation

Étape 2. ISE analyse le paquet de comptabilité avec les attributs de point de terminaison

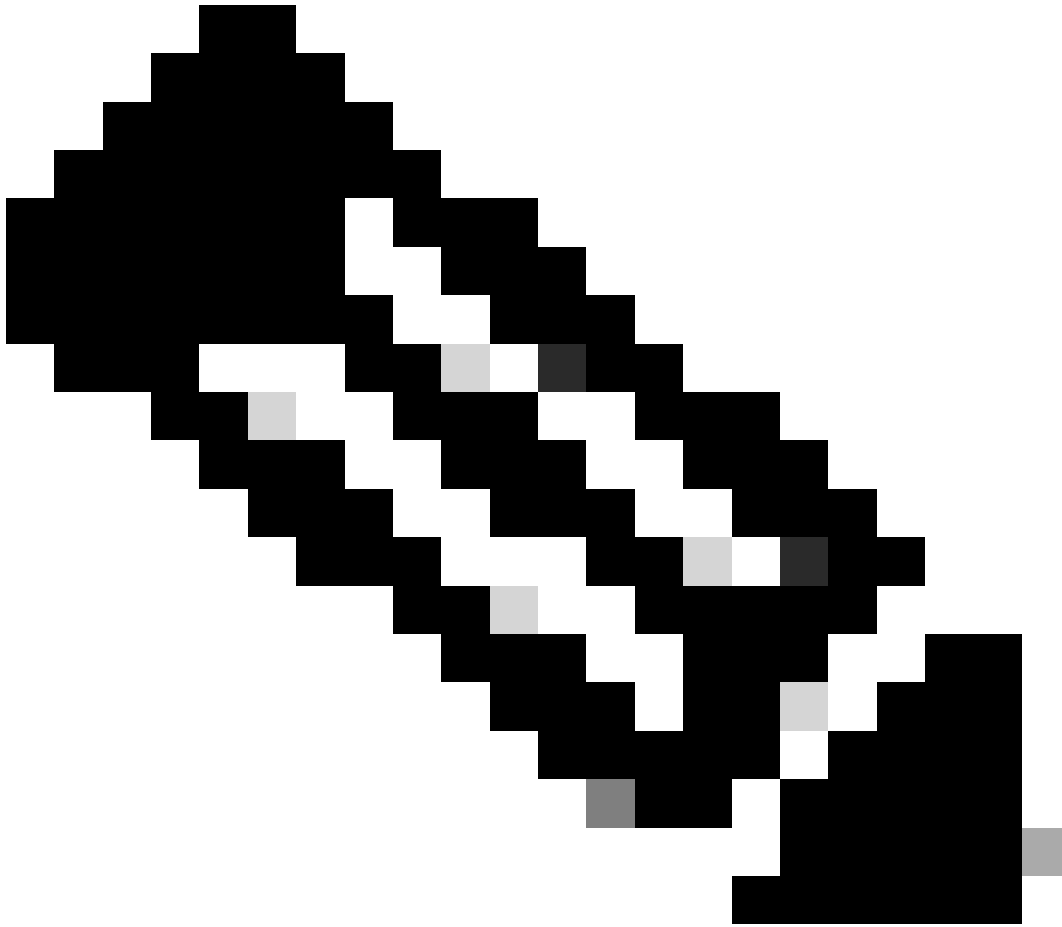
Du côté ISE, ces composants peuvent être définis au niveau DEBUG pour s'assurer que les paquets de comptabilité RADIUS envoyés par le WLC atteignent ISE et sont correctement traités.

Vous pouvez ensuite collecter l'offre groupée de support ISE pour collecter les fichiers journaux. Pour plus d'informations sur la collecte du bundle d'assistance, consultez la section **Informations connexes**.

| Component Name   | Log Level | Description                 | Log file Name   |
|------------------|-----------|-----------------------------|-----------------|
| × Component Name | DEBUG     | × Description               | Log file Name   |
| nsf              | DEB... ▾  | NSF related messages        | ise-psc.log     |
| nsf-session      | DEB... ▾  | Session cache messages      | ise-psc.log     |
| profiler         | DEB... ▾  | profiler debug messages     | profiler.log    |
| runtime-AAA      | DEB... ▾  | AAA runtime messages (prrt) | prrt-server.log |

Composants à déboguer pour le dépannage





**Remarque** : les composants sont activés au niveau DEBUG uniquement sur le PSN qui authentifie les terminaux.

---

Sur iseLocalStore.log, le message Accounting-Start est consigné sans qu'il soit nécessaire d'activer un composant au niveau DEBUG. Dans ce cas, ISE doit voir le paquet Accounting entrant contenant les attributs WiFi Analytics.

<#root>

2023-09-27 18:19:23.600 +00:00 0000035538 3000

**NOTICE Radius-Accounting: RADIUS Accounting start request,**

ConfigVersionId=1493,  
Device IP Address=172.16.5.169,





cisco-av-pair=dhcp-option=host-name=Victor-s-S22, cisco-av-pair=dhcp-option=dhcp-class-identifier=andro  
cisco-av-pair=dot11-device-info=DEVICE\_INFO\_MODEL\_NUM=Samsung Galaxy S22+, cisco-av-pair=dot11-device-in  
  
cisco-av-pair=dot11-device-info=DEVICE\_INFO\_DEVICE\_FORM=1, cisco-av-pair=dot11-device-info=DEVICE\_INFO\_C  
  
cisco-av-pair=dot11-device-info=DEVICE\_INFO\_VENDOR\_TYPE=2, cisco-av-pair=audit-session-id=A90510AC000000  
, cisco-av-pair=vlan-id=2606, cisco-av-pair=method=dot1x, cisco-av-pair=cisco-wlan-ssid=VIcSSID,  
cisco-av-pair=wlan-profile-name=ISE-AAA, Airespace-Wlan-Id=1, AcsSessionID=iselab/484624451/304,

Les informations sur les attributs des terminaux sont mises à jour.

<#root>

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE\_INFO\_FIRMWARE\_VERSION=[WH6]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE\_INFO\_SALES\_CODE=[MXO]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE\_INFO\_DEVICE\_FORM=[1]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE\_INFO\_OS\_VERSION=[Android 13]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE\_INFO\_COUNTRY\_CODE=[Unknown]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE\_INFO\_VENDOR\_TYPE=[2]

<#root>

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7:::- Endpoint: EndPoint[id=,name=

MAC: 0A:5A:F0:B3:B5:9C

Attribute:AAA-Server value:iselab Attribute:Acct-Authentic value:Remote Attribute:Acct-Delay-Time valu

Attribute:DEVICE\_INFO\_COUNTRY\_CODE value:Unknown Attribute:DEVICE\_INFO\_DEVICE\_FORM value:PHONE Attribute

Attribute:Device IP Address value:172.16.5.169 Attribute:Device Type value:Device Type#All Device Type

La mise à jour des attributs déclenche un nouvel événement de profilage de point de terminaison. Les stratégies de profilage sont évaluées à nouveau et un nouveau profil est attribué.

<#root>

2023-09-27 18:19:24,098

DEBUG [pool-533-thread-35]

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC0000005BD7DDDA7:::62cc7a10-5d62-

Policy Android matched 0A:5A:F0:B3:B5:9C (certainty 30)

2023-09-27 18:19:24,098

DEBUG [pool-533-thread-35]

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC0000005BD7DDDA7:::62cc7a10-5d62-

DEBUG [pool-533-thread-35]

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC0000005BD7DDDA7:::62cc7a10-5d62-

Policy Android matched 0A:5A:F0:B3:B5:9C (certainty 30)

com.cisco.profiler.infrastructure.profiling.ProfilerManager\$MatchingPolicyInternal@14ec7800

Étape 4. CoA et réauthentification

ISE doit envoyer une CoA pour la session de point d'extrémité lorsqu'une modification des attributs WiFi Device Analytics a eu lieu.

<#root>

2023-09-27 18:19:24,103

DEBUG [pool-533-thread-35]

```

[[]] cisco.profiler.infrastructure.profilng.ProfilerManager -:A90510AC000005BD7DDDA7::62cc7a10-5d62-
Endpoint 0A:5A:F0:B3:B5:9C IdentityGroup / Logical Profile Changed/ WiFi device analytics attribute char
2023-09-27 18:19:24,103

```

```

DEBUG [pool-533-thread-35]

```

```

[[]] cisco.profiler.infrastructure.profilng.ProfilerManager -:A90510AC000005BD7DDDA7::62cc7a10-5d62-
ConditionalCoAEvent with Endpoint Details : EndPoint[id=62caa550-5d62-11ee-bf1f-b6bb1580ab0d,name=] MAC:
Attribute:AAA-Server value:iselab Attribute:Airespace-Wlan-Id value:1 Attribute:AllowedProtocolMatched
Attribute:DEVICE_INFO_COUNTRY_CODE value:Unknown Attribute:DEVICE_INFO_DEVICE_FORM value:PHONE Attribute
Attribute:DTLSSupport value:Unknown Attribute:DestinationIPAddress value:172.16.5.112 Attribute:Destin

```

La capture de paquets permet de s'assurer que l'ISE envoie la CoA au WLC. Il indique également qu'un nouveau paquet de demande d'accès est reçu après le traitement de la CoA.

|     |                            |              |              |        |                       |
|-----|----------------------------|--------------|--------------|--------|-----------------------|
| 111 | 2023-09-27 12:19:24.357572 | 172.16.5.112 | 172.16.5.169 | RADIUS | 244 CoA-Request id=13 |
| 112 | 2023-09-27 12:19:24.361138 | 172.16.5.169 | 172.16.5.112 | RADIUS | 111 CoA-ACK id=13     |

```

> Frame 111: 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits)
> Ethernet II, Src: VMware_b3:f0:73 (00:50:56:b3:f0:73), Dst: Cisco_5c:16:ff (00:1e:f6:5c:16:ff)
> Internet Protocol Version 4, Src: 172.16.5.112, Dst: 172.16.5.169
> User Datagram Protocol, Src Port: 41440, Dst Port: 1700
< RADIUS Protocol
  Code: CoA-Request (43)
  Packet identifier: 0xd (13)
  Length: 202
  Authenticator: d622a25b73d3b2b475cf5d4ad2b00b5c
  [The response to this request is in frame 112]
< Attribute Value Pairs
  > AVP: t=NAS-IP-Address(4) l=6 val=172.16.5.169
  > AVP: t=Calling-Station-Id(31) l=19 val=0A:5A:F0:B3:B5:9C
    Type: 31
    Length: 19
    Calling-Station-Id: 0A:5A:F0:B3:B5:9C
  > AVP: t=Event-Timestamp(55) l=6 val=Sep 27, 2023 12:19:24.000000000 CST
  > AVP: t=Message-Authenticator(80) l=18 val=3edaf9ffdb25ceee5451e90a1cef21af
  < AVP: t=Vendor-Specific(26) l=43 vnd=ciscoSystems(9)
    Type: 26
    Length: 43
    Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=37 val=subscriber:reauthenticate-type=last
  < AVP: t=Vendor-Specific(26) l=41 vnd=ciscoSystems(9)
    Type: 26
    Length: 41
    Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=35 val=subscriber:command=reauthenticate
  < AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
    Type: 26
    Length: 49
    Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=43 val=audit-session-id=A90510AC000005BD7DDDA7

```

Paquet Radius CoA après profilage des points de terminaison

|     |            |                 |              |              |        |      |                         |
|-----|------------|-----------------|--------------|--------------|--------|------|-------------------------|
| 111 | 2023-09-27 | 12:19:24.357572 | 172.16.5.112 | 172.16.5.169 | RADIUS | 244  | CoA-Request id=13       |
| 112 | 2023-09-27 | 12:19:24.361138 | 172.16.5.169 | 172.16.5.112 | RADIUS | 111  | CoA-ACK id=13           |
| 113 | 2023-09-27 | 12:19:24.373874 | 172.16.5.169 | 172.16.5.112 | RADIUS | 480  | Access-Request id=55    |
| 114 | 2023-09-27 | 12:19:24.386280 | 172.16.5.112 | 172.16.5.169 | RADIUS | 167  | Access-Challenge id=55  |
| 115 | 2023-09-27 | 12:19:24.397609 | 172.16.5.169 | 172.16.5.112 | RADIUS | 557  | Access-Request id=63    |
| 116 | 2023-09-27 | 12:19:24.400463 | 172.16.5.112 | 172.16.5.169 | RADIUS | 167  | Access-Challenge id=63  |
| 117 | 2023-09-27 | 12:19:24.413943 | 172.16.5.169 | 172.16.5.112 | RADIUS | 720  | Access-Request id=71    |
| 118 | 2023-09-27 | 12:19:24.456036 | 172.16.5.112 | 172.16.5.169 | RADIUS | 1179 | Access-Challenge id=71  |
| 119 | 2023-09-27 | 12:19:24.477140 | 172.16.5.169 | 172.16.5.112 | RADIUS | 557  | Access-Request id=79    |
| 120 | 2023-09-27 | 12:19:24.481172 | 172.16.5.112 | 172.16.5.169 | RADIUS | 1175 | Access-Challenge id=79  |
| 121 | 2023-09-27 | 12:19:24.496743 | 172.16.5.169 | 172.16.5.112 | RADIUS | 557  | Access-Request id=87    |
| 122 | 2023-09-27 | 12:19:24.499901 | 172.16.5.112 | 172.16.5.169 | RADIUS | 289  | Access-Challenge id=87  |
| 123 | 2023-09-27 | 12:19:24.546538 | 172.16.5.169 | 172.16.5.112 | RADIUS | 715  | Access-Request id=95    |
| 124 | 2023-09-27 | 12:19:24.553619 | 172.16.5.112 | 172.16.5.169 | RADIUS | 218  | Access-Challenge id=95  |
| 125 | 2023-09-27 | 12:19:24.568069 | 172.16.5.169 | 172.16.5.112 | RADIUS | 557  | Access-Request id=103   |
| 126 | 2023-09-27 | 12:19:24.571945 | 172.16.5.112 | 172.16.5.169 | RADIUS | 201  | Access-Challenge id=103 |
| 127 | 2023-09-27 | 12:19:24.584229 | 172.16.5.169 | 172.16.5.112 | RADIUS | 594  | Access-Request id=111   |
| 128 | 2023-09-27 | 12:19:24.588165 | 172.16.5.112 | 172.16.5.169 | RADIUS | 232  | Access-Challenge id=111 |
| 129 | 2023-09-27 | 12:19:24.599493 | 172.16.5.169 | 172.16.5.112 | RADIUS | 648  | Access-Request id=119   |
| 130 | 2023-09-27 | 12:19:24.624360 | 172.16.5.112 | 172.16.5.169 | RADIUS | 247  | Access-Challenge id=119 |
| 131 | 2023-09-27 | 12:19:24.638515 | 172.16.5.169 | 172.16.5.112 | RADIUS | 592  | Access-Request id=127   |
| 132 | 2023-09-27 | 12:19:24.642039 | 172.16.5.112 | 172.16.5.169 | RADIUS | 200  | Access-Challenge id=127 |
| 133 | 2023-09-27 | 12:19:24.654578 | 172.16.5.169 | 172.16.5.112 | RADIUS | 557  | Access-Request id=135   |
| 134 | 2023-09-27 | 12:19:24.677792 | 172.16.5.112 | 172.16.5.169 | RADIUS | 330  | Access-Accept id=135    |

*Radius CoA et nouvelle demande d'accès après profilage des terminaux*

#### Informations connexes

- [Guide de l'administrateur de Cisco Identity Services Engine, version 3.3](#)
- [Notes de version de Cisco Identity Services Engine, version 3.3](#)
- [Collecter l'offre groupée d'assistance sur Identity Services Engine](#)

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.