# 瞭解ISE 3.3上適用於終端分類的Wifi分析

## 目錄



## 簡介

本檔案說明WiFi Analytics for Endpoint Classification的工作方式。本章還介紹了如何配置、驗證和排除故障。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 9800無線LAN控制器(WLC)配置
- 身份服務引擎(ISE)配置
- RADIUS 驗證.授權和記帳(AAA)封包流程和術語

本文檔假定已有一個正在工作的WLAN對使用ISE作為RADIUS伺服器的客戶端進行身份驗證。

此功能若要運作，至少必須具備：

- 9800 WLC Cisco IOS® XE都柏林17.10.1
- 辨識服務引擎v3.3。
- 802.11ac Wave2或802.11ax (Wi-Fi 6/6E)存取點

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 9800 WLC Cisco IOSXE v17.12.x
- 身分辨識服務引擎(ISE) v3.3
- Android 13裝置

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

透過WiFi裝置分析，Cisco 9800 WLC可以從連線到此裝置的一組終端瞭解屬性（例如型號和作業系統版本），並與ISE共用這些屬性。然後，ISE可以將此資訊用於終端分類（也稱為分析）。

目前，以下廠商支援WiFi分析：

- 蘋果
- Intel
- 三星

WLC使用RADIUS記帳資料包與ISE伺服器共用屬性資訊。


WiFi分析資料流

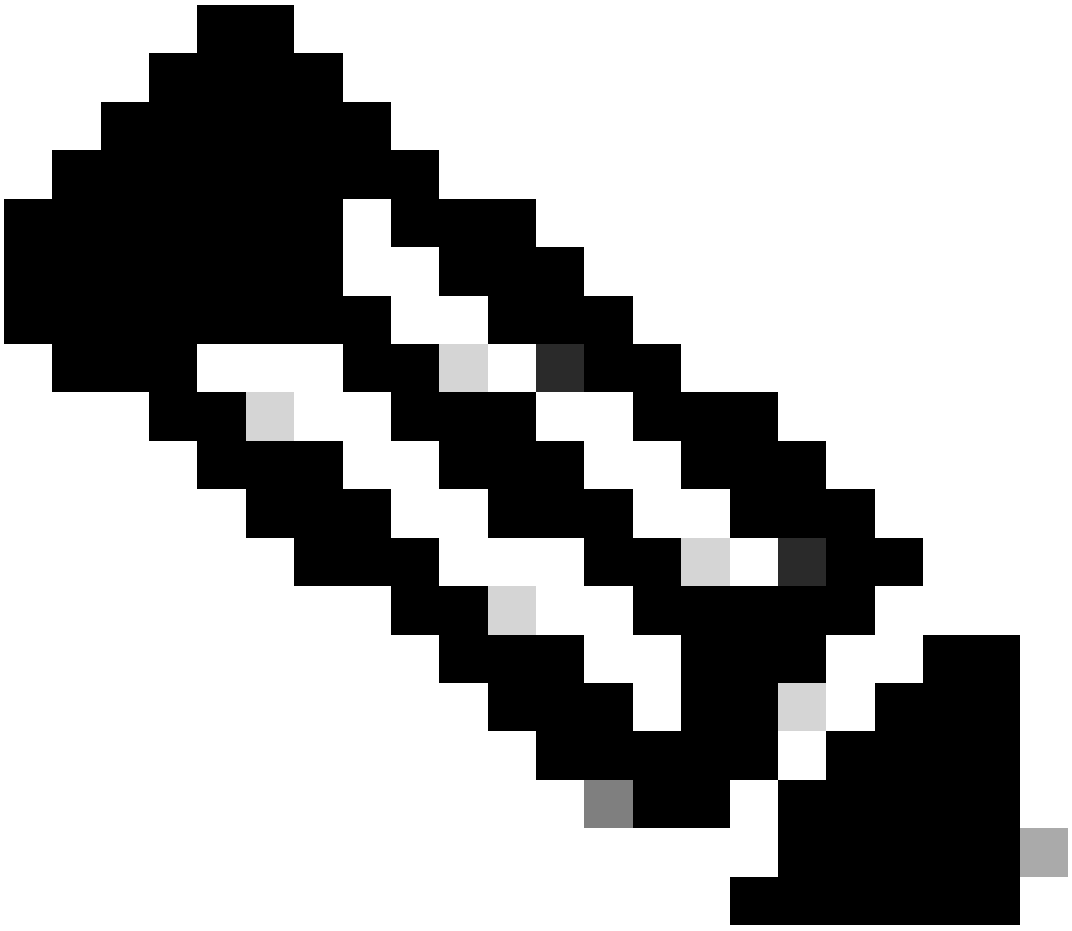
請務必記住，RADIUS AAA流上的RADIUS記帳資料包僅在RADIUS伺服器傳送RADIUS Access-Accept資料包作為對終端身份驗證嘗試的應答之後傳送。換句話說，只有在RADIUS伺服器(ISE)和

網路訪問裝置(WLC)之間建立了該終端的RADIUS會話後，WLC才會共用該終端屬性資訊。

以下是ISE可用於終端分類和授權的所有屬性：

- DEVICE_INFO_FIRMWARE_VERSION
- DEVICE_INFO_HW_MODEL
- 裝置_資訊_製造商_模型
- DEVICE_INFO_MODEL_NAME
- DEVICE_INFO_MODEL_NUM
- 裝置_資訊_作業系統_版本
- DEVICE_INFO_VENDOR_TYPE

---

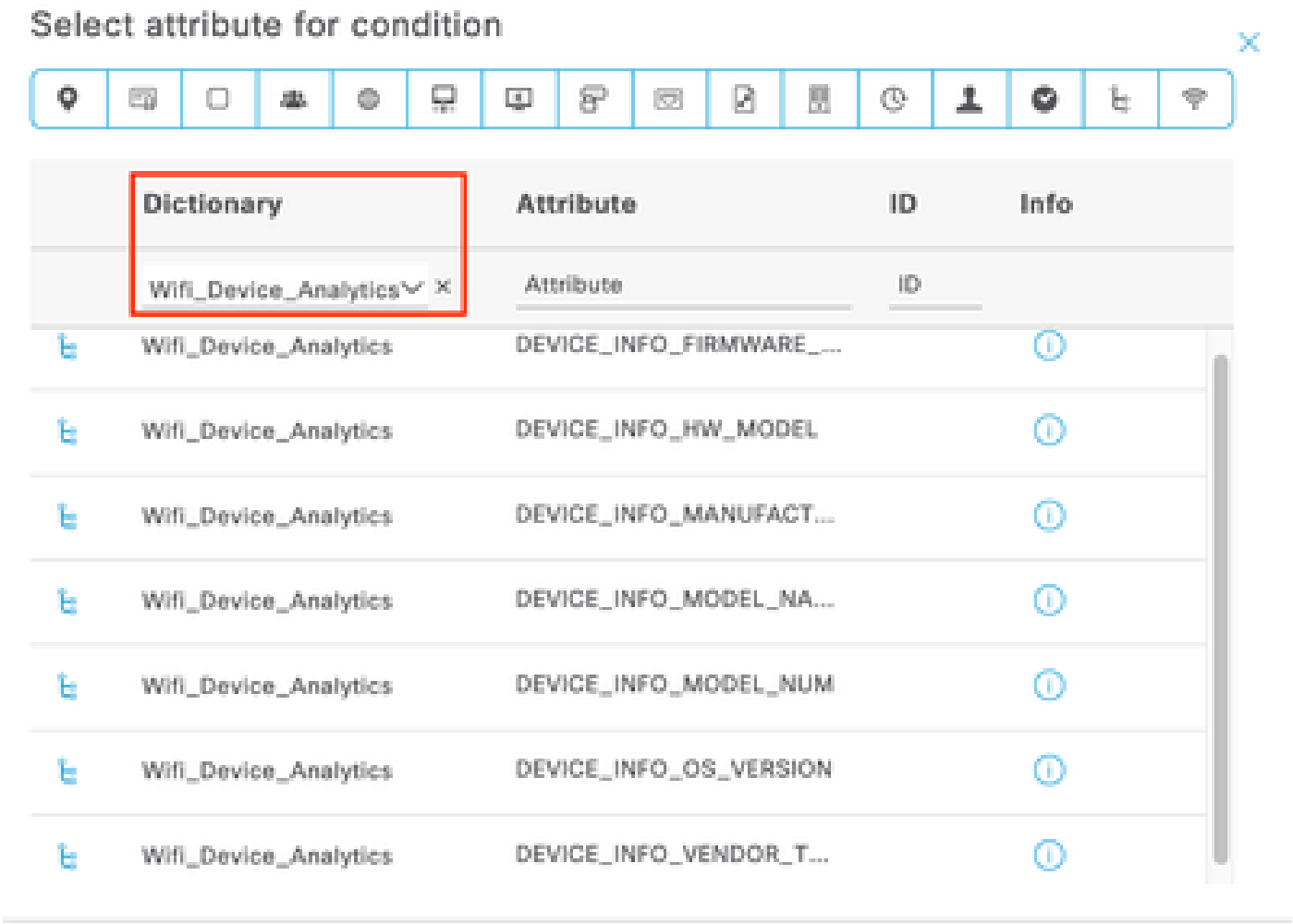


注意：WLC可以根據連線的終端型別傳送更多屬性，但只有列出的屬性可用於在ISE中建立授權策略。

---

一旦ISE收到記帳資料包，它可以在其中處理和使用此分析資料，並使用它來重新分配終端配置檔案/身份組。

WiFi Endpoint Analytics屬性列在WiFi_Device_Analytics詞典下。網路管理員可以在終端授權策略和條件中包含這些屬性。




WiFi裝置分析詞典

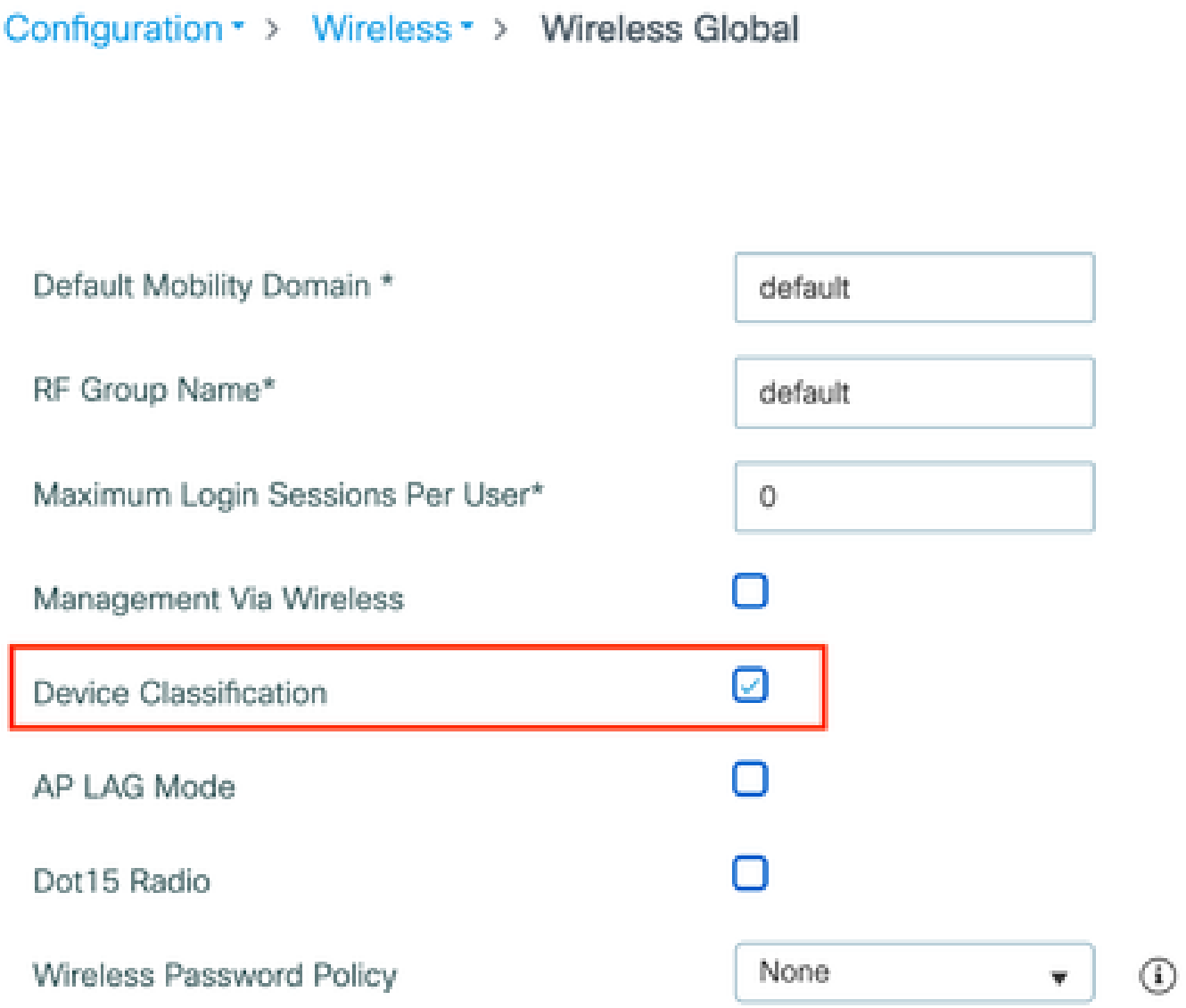
如果ISE為終端儲存的當前屬性值發生任何更改，則ISE會啟動授權更改(CoA)，允許對終端進行評估，計算更新的屬性。

# 設定

## WLC上的配置

步驟 1.全局啟用裝置分類功能

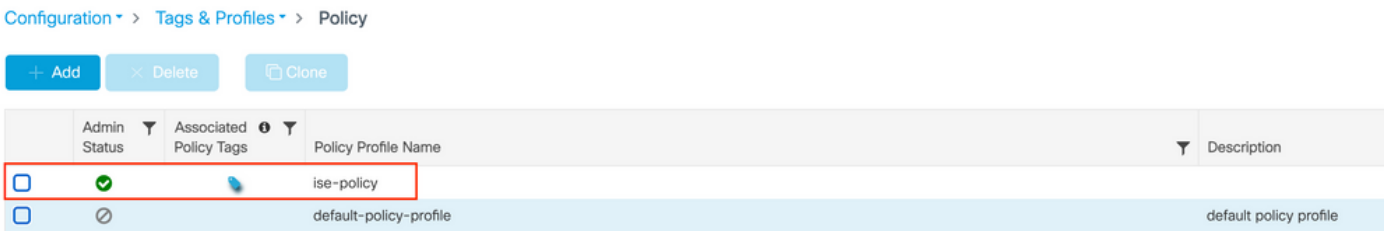
導航到Configuration > Wireless > Wireless Global，然後選中Device Classification覈取方塊。




裝置分類配置

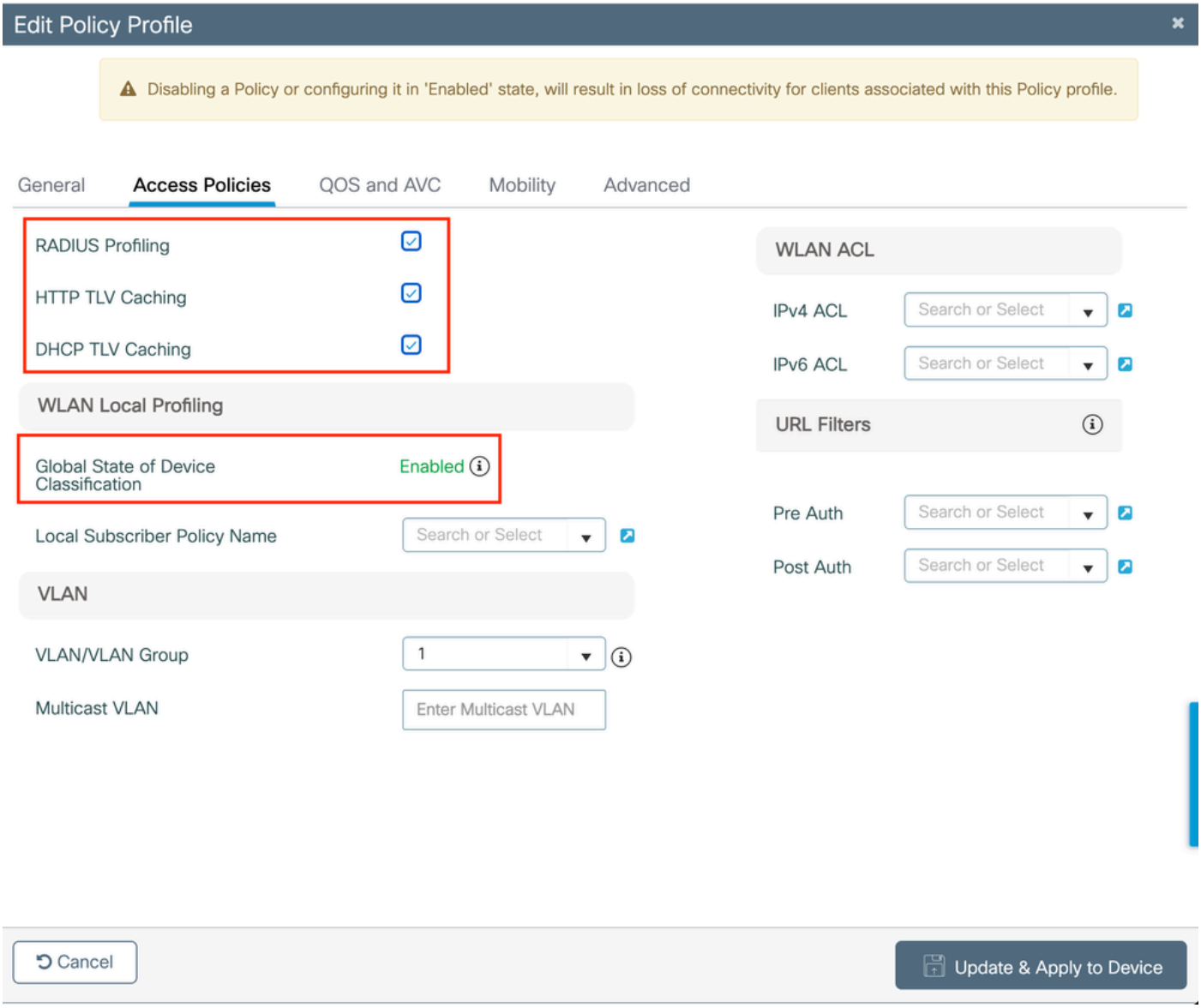
步驟 2.啟用TLV快取和RADIUS分析

導航到配置>標籤和配置檔案>策略，選擇RADIUS客戶端所連線的WLAN所使用的策略配置檔案。




無線策略選擇

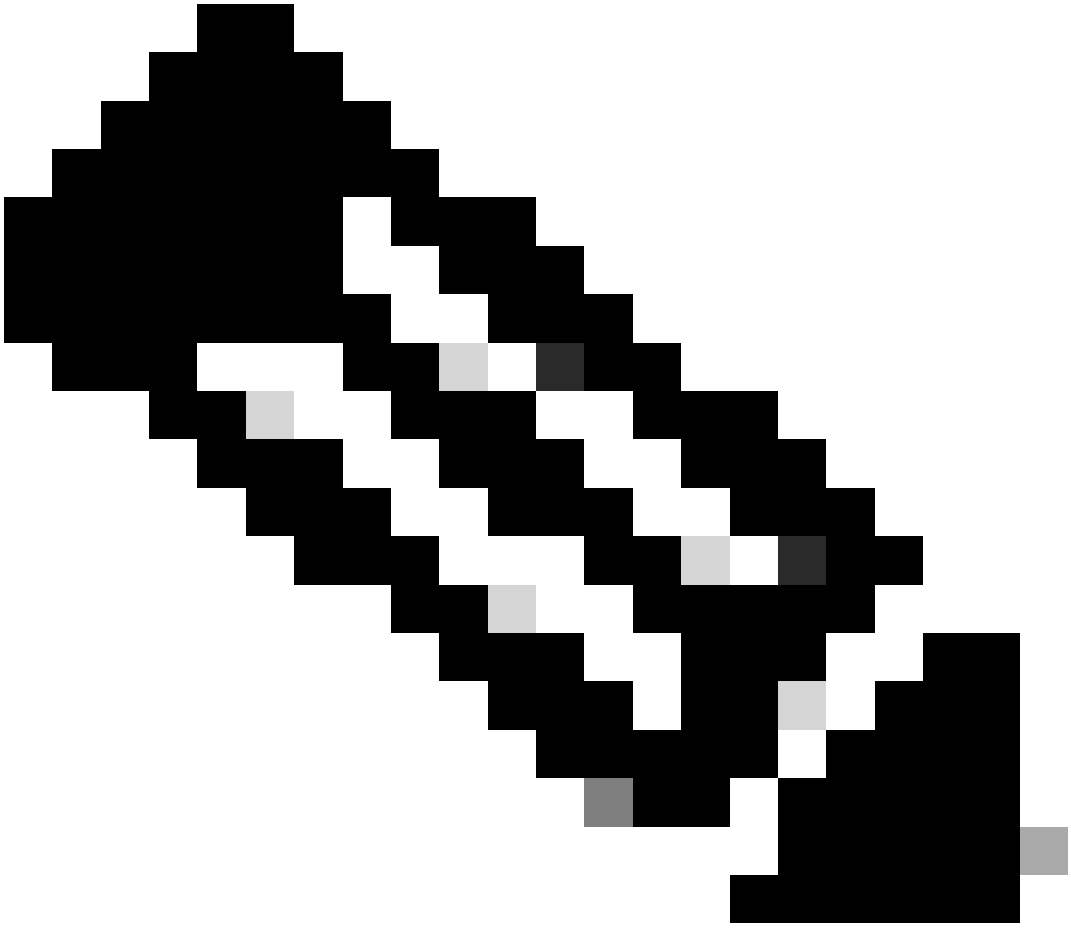
按一下Access Policies，然後選中RADIUS Profiling、HTTP TLV Caching 和DHCP TLV Caching 選項。由於在上一步中執行的操作，裝置分類全局狀態現在將顯示為「已啟用」狀態。




RADIUS分析和快取配置

登入到WLC CLI並啟用dot11 TLV Accounting。

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



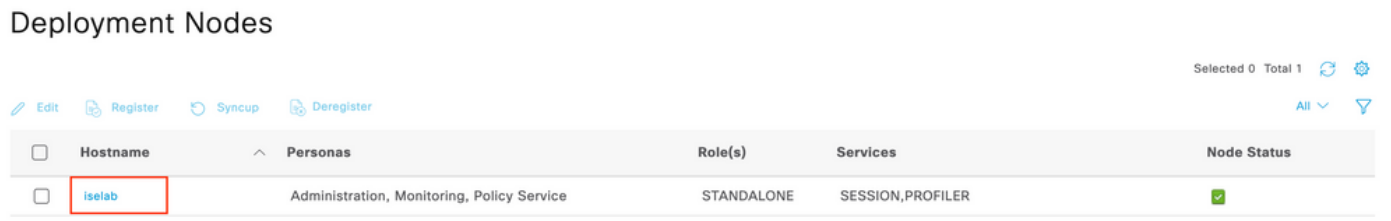
**注意**：使用此命令之前，必須停用無線策略配置檔案。此命令僅適用於Cisco IOS XE Dublin 17.10.1版及更高版本。

---

ISE上的配置

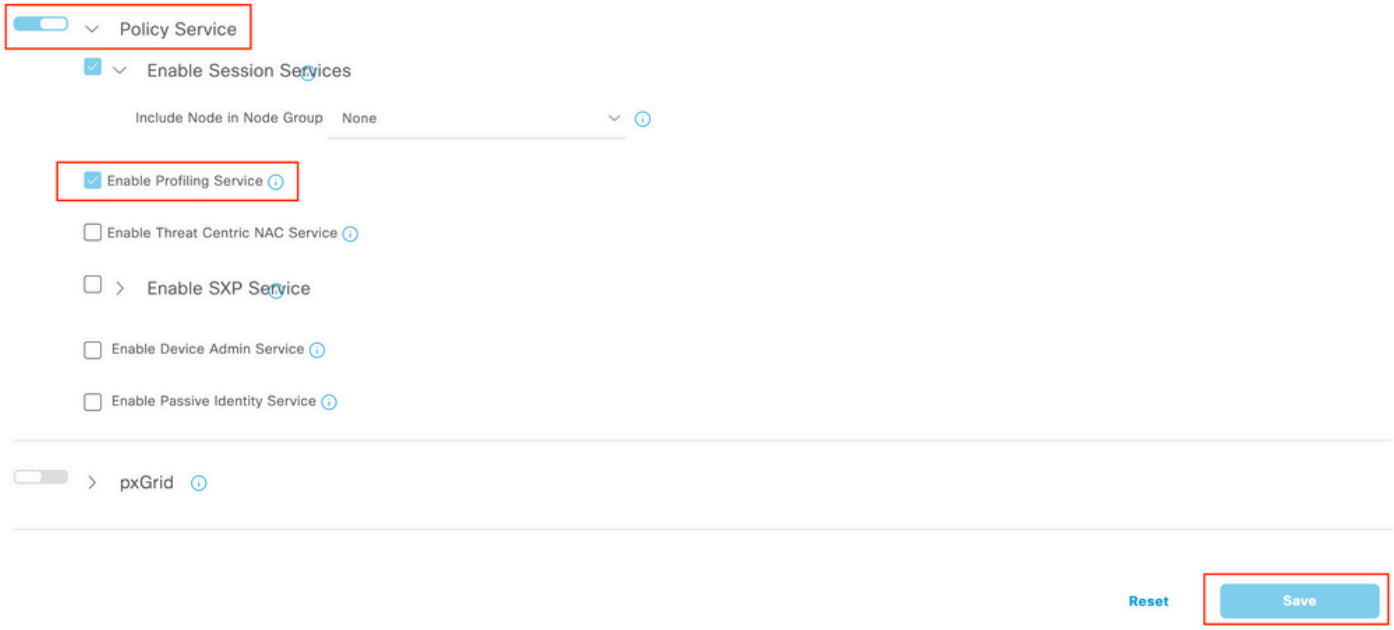
步驟 1.在部署中的PSN中啟用分析服務

導航到**管理>部署**，然後點選PSN的名稱。




*ISE PSN節點選擇*

向下滾動到**Policy Service**部分並標籤**Enable Profiling Service**覈取方塊。按一下**Save**按鈕。




效能分析工具服務組態

步驟 2.在ISE PSN上啟用RADIUS分析探測

向上滾動到頁面頂部，然後按一下**Profiling Configuration**頁籤。這會顯示可在ISE上使用的所有分析探測。啟用**RADIUS探測**，然後按一下**儲存**。

Deployment Nodes List > iselab

# Edit Node

General Settings | Profiling Configuration

> NETFLOW

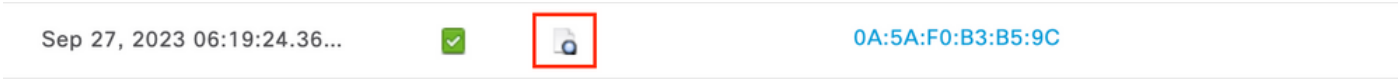
> DHCP

> DHCPSPAN

> HTTP

**注意**：CoA資料包的標識欄位始終為空，但終端ID與第一個身份驗證資料包中的終端ID相同。

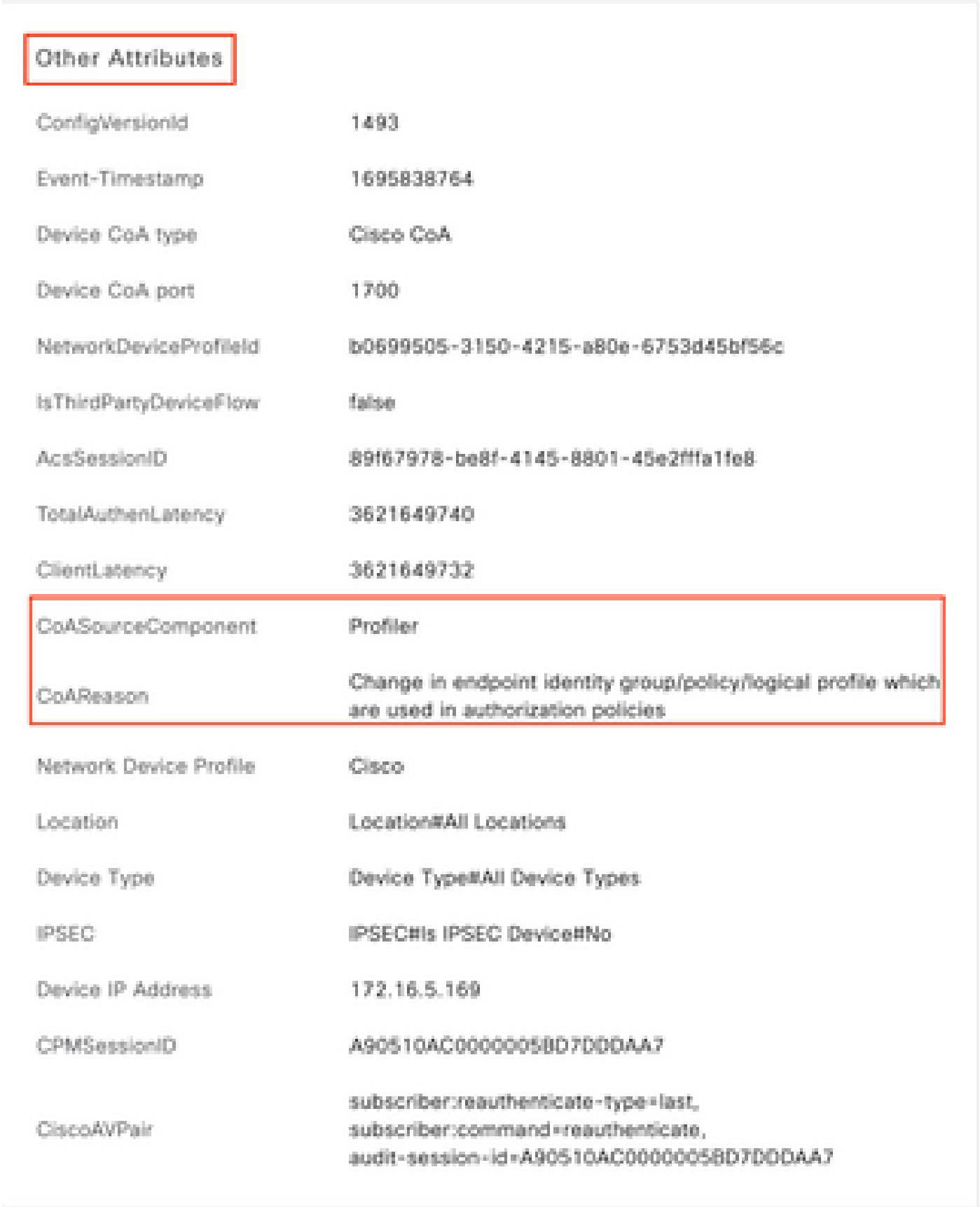
按一下位於「Change of Authorization」記錄上的**Details**列中的**圖示**。




訪問*CoA*資料包詳細資訊

CoA詳細資訊顯示在新的瀏覽器頁籤中。向下滾動到**Other Attributes**部分。

CoA源元件顯示為效能分析器。CoA Reason在用於授權策略的終端身份組/策略/邏輯配置檔案中顯示為更改。

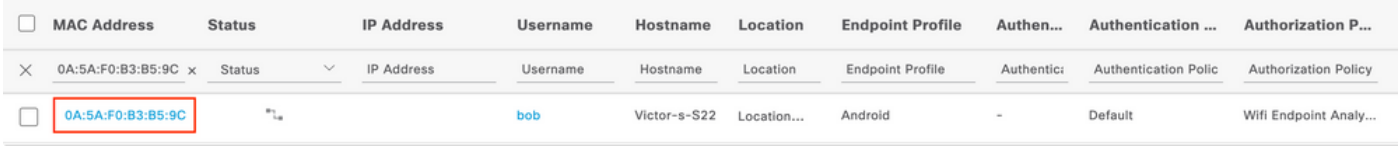


| Other Attributes | |
|---|---|
| ConfigVersionId | 1493 |
| Event-Timestamp | 1695838764 |
| Device CoA type | Cisco CoA |
| Device CoA port | 1700 |
| NetworkDeviceProfileId | b0699505-3150-4215-a80e-6753d45bf56c |
| IsThirdPartyDeviceFlow | false |
| AcsSessionID | 89f67978-be8f-4145-8801-45e2fffa1fe8 |
| 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 | A90510AC0000005BD7DDDAA7 |
| CiscoAVPair | subscriber:reauthenticate-type=last, subscriber:command=reauthenticate, audit-session-id=A90510AC0000005BD7DDDAA7 |

*CoA*觸發元件和原因

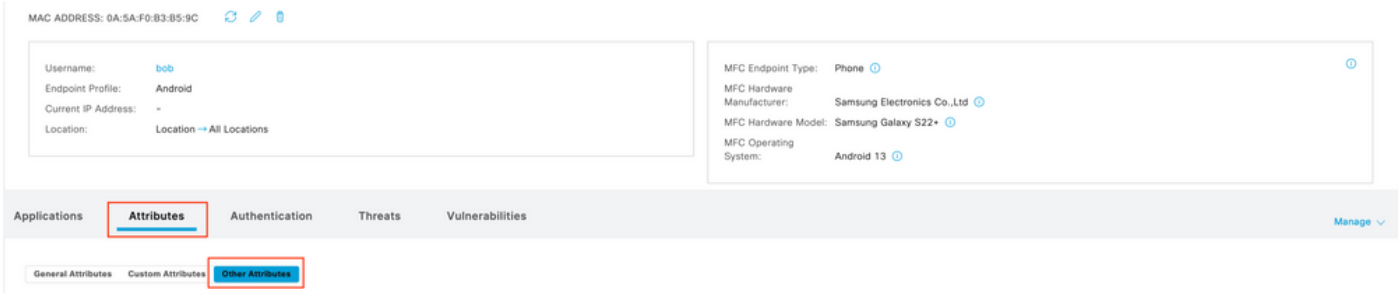
**導航到情景可視性>端點>身份驗證**頁籤。在此頁籤上，使用過濾器查詢測試端點。

**點選終端MAC地址**以訪問**終端屬性**。



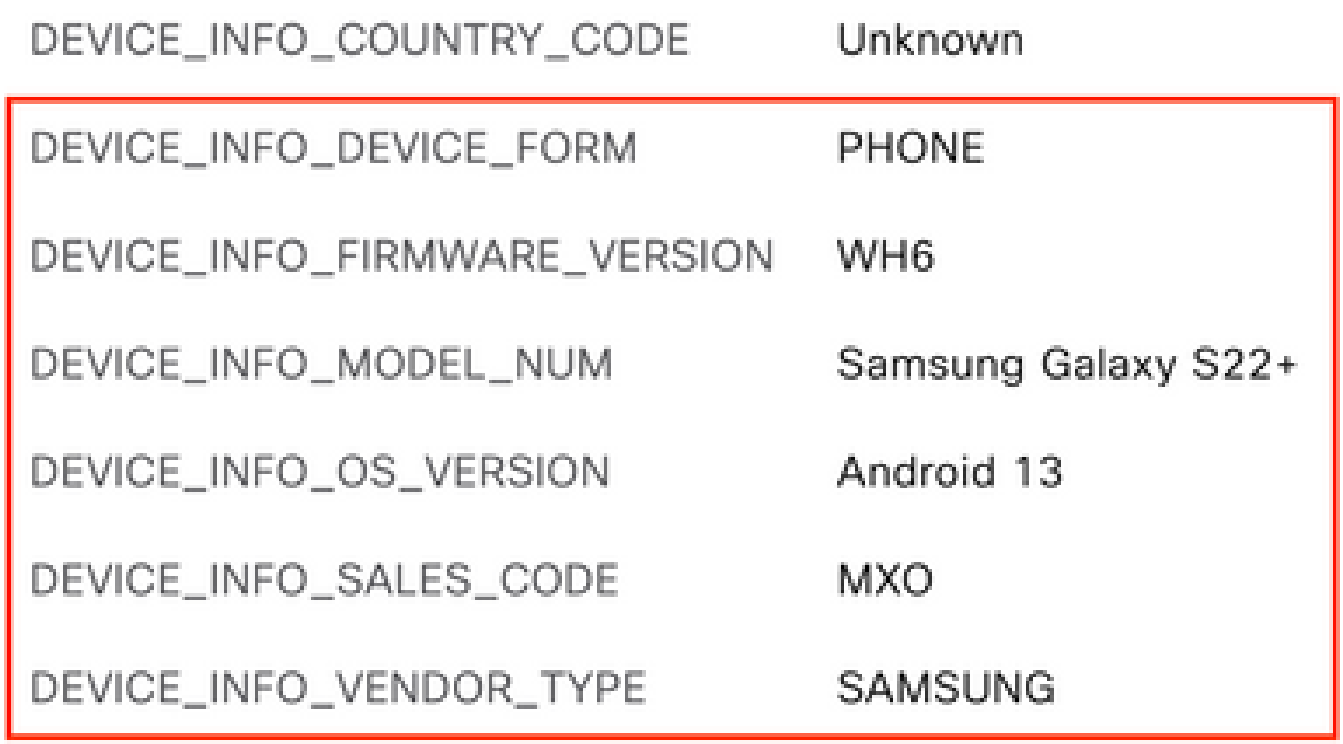

情景可視性上的端點

此操作顯示ISE儲存的有關此終端的所有資訊。點選**屬性**部分，然後選擇**其他屬性**。




在情景可視性上選擇終結點其他屬性

向下滾動，直到找到**WiFi_Device_Analytics詞典**屬性。在此部分找到這些屬性意味著ISE透過記帳資料包成功接收這些屬性，可用於終端分類。




*WiFi*分析屬性與情景可視性

以下是Windows 10和iPhone屬性的示例，供您參考：

| | |
|---|---|
| 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 |

*Windows 10*終端

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

屬

性示例*iPhone*終端屬性示例

**疑難排解**

步驟 1.會計資料包到達ISE

在WLC CLI上，確保在策略配置檔案配置中啟用**DOT11 TLV記帳、DHCP TLV快取**和**HTTP TLV快取**。

<#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**

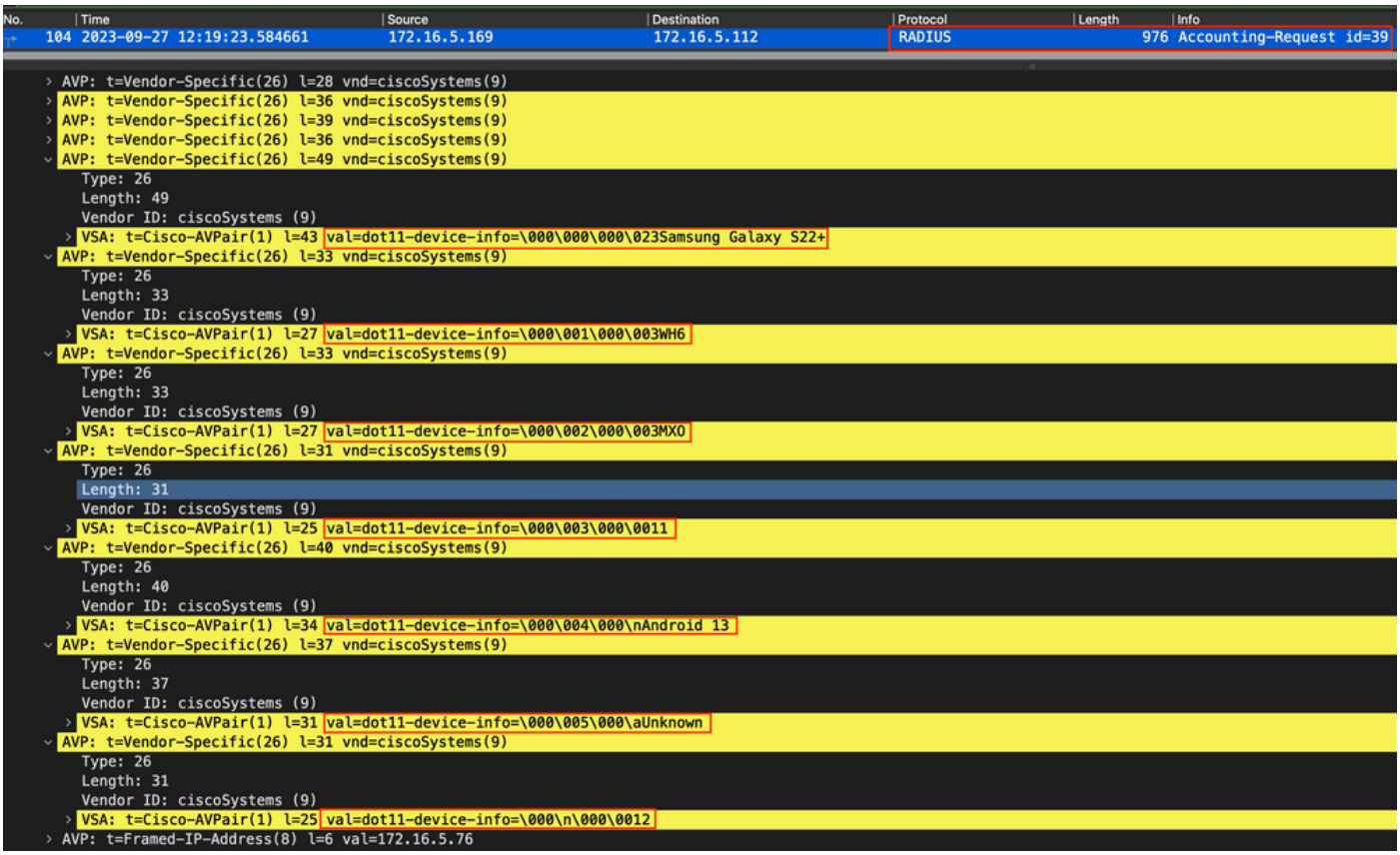
 no shutdown

連線終端時，在WLC或ISE端上收集**資料包捕獲**。您可以使用任何已知的資料包分析工具（如Wireshark）來分析收集的檔案。

按RADIUS記帳資料包和呼叫站ID（測試終端MAC地址）進行過濾。例如，可以使用以下過濾器：

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

找到後，展開**Cisco-AVPair**欄位以查詢Accounting資料包中的**WiFi Analytics Data**。




記賬資料包中的終端*TLV*屬性

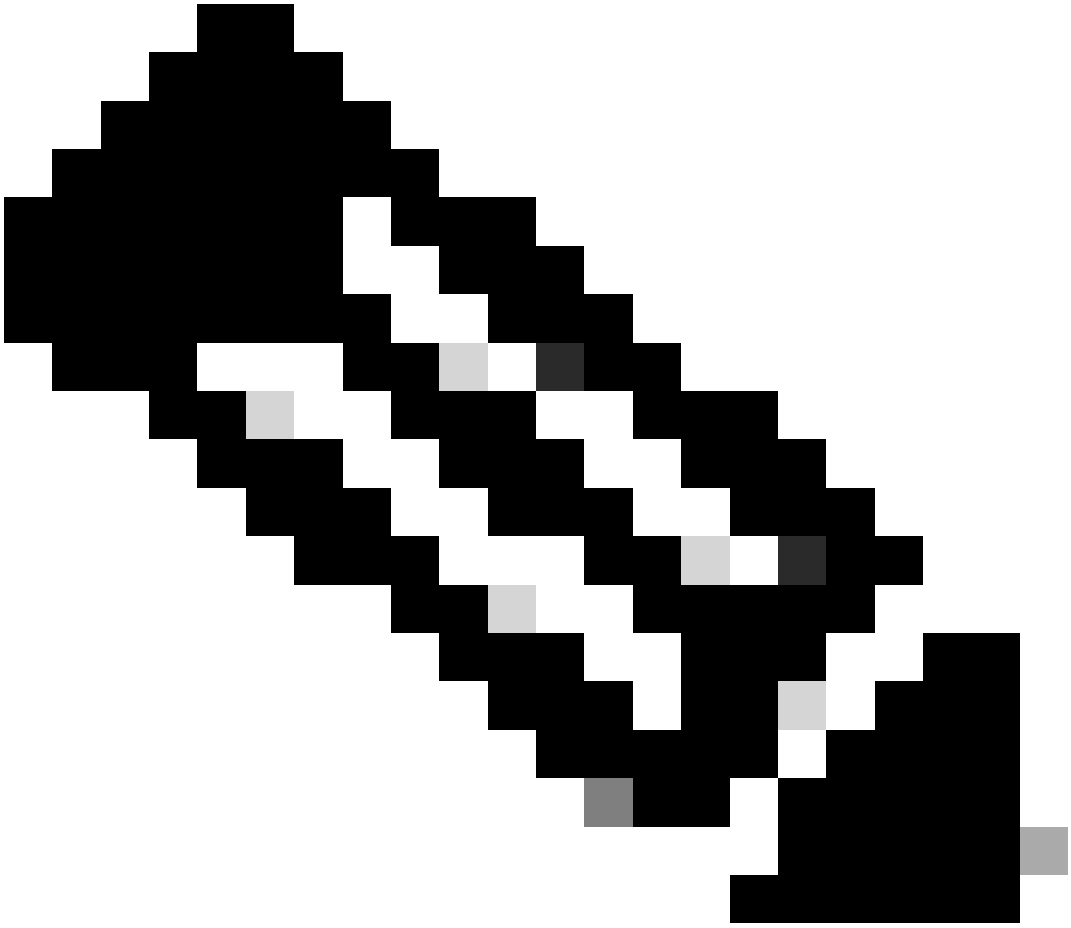
步驟 2.ISE使用終端屬性解析記帳資料包

在ISE端，可以將這些元件設定為調試級別，以確保所傳送的RADIUS記帳資料包到達ISE並正確處理。

然後，您可以收集**ISE支援捆綁包**以收集日誌檔案。有關如何收集支援捆綁的詳細資訊，請參閱**相關資訊**部分。

| 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 |

要調試以進行故障排除的元件



**註**：僅在驗證終端的PSN上啟用元件到DEBUG級別。

---

在iseLocalStore.log上，記帳-Start消息無需啟用任何元件到調試級別。在這裡，ISE必須看到包含WiFi分析屬性的傳入記帳資料包。

<#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,

**UserName=bob**

, NetworkDeviceName=lab-wlc, User-Name=bob, NAS-IP-Address=172.16.5.169, NAS-Port=260613,
Framed-IP-Address=172.16.5.76, Class=CACS:A90510AC0000005BD7DDDAA7:iselab/484624451/303, Called-Station

**Calling-Station-ID=0a-5a-f0-b3-b5-9c**

, NAS-Identifier=vimontes-wlc, Acct-Status-Type=Start, Acct-Delay-Time=0, Acct-Session-Id=00000018,
Acct-Authentic=Remote, Event-Timestamp=1695838756, NAS-Port-Type=Wireless - IEEE 802.11, cisco-av-pair=
cisco-av-pair=dc-device-name=Victor-s-S22, cisco-av-pair=dc-device-class-tag=Samsung Galaxy S22+, cisco
cisco-av-pair=64:63:2d:6f:70:61:71:75:65:3d:01:00:00:00:00:00:00:00:00:00:00:00, cisco-av-pair=dc-proto
cisco-av-pair=dhcp-option=dhcp-class-identifier=android-dhcp-13, cisco-av-pair=dhcp-option=dhcp-paramet

**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_SALES_CODE=MXO, cisco-av-pair=dot11-device-info=DEVICE_INFO_**

**cisco-av-pair=dot11-device-info=DEVICE_INFO_OS_VERSION=Android 13, cisco-av-pair=dot11-device-info=DEVIC**

**cisco-av-pair=dot11-device-info=DEVICE_INFO_VENDOR_TYPE=2,**

cisco-av-pair=audit-session-id=A90510AC0000005BD7DDDAA7, cisco-av-pair=vlan-id=2606, cisco-av-pair=met
cisco-av-pair=cisco-wlan-ssid=VIcSSID, cisco-av-pair=wlan-profile-name=ISE-AAA, Airespace-Wlan-Id=1, Ac
RequestLatency=15, Step=11004, Step=11017, Step=15049, Step=15008, Step=22083, Step=11005, NetworkDevic
NetworkDeviceGroups=Device Type#All Device Types,

**CPMSessionID=A90510AC0000005BD7DDDAA7**

, TotalAuthenLatency=15, ClientLatency=0, Network Device Profile=Cisco, Location=Location#All Locations
Device Type=Device Type#All Device Types, IPSEC=IPSEC#Is IPSEC Device#No,

在prrt-server.log上，ISE解析收到的記帳資料包系統日誌消息，包括WiFi Analytics屬性。使用**CallingStationID**和**CPMSessionID**欄位確保跟蹤正確的會話和終端。

<#root>

Radius,2023-09-27 18:19:23,586,

**DEBUG,0x7f50a2b67700,**

cntx=0000192474,sesn=iselab/484624451/304,

**CPMSessionID=A90510AC0000005BD7DDDAA7**

,

**CallingStationID=0a-5a-f0-b3-b5-9c**

,FramedIPAddress=172.16.5.76,

**RADIUS PACKET::**

**Code=4(AccountingRequest)**

Identifier=39 Length=934

**[1] User-Name - value: [bob]**

[4] NAS-IP-Address - value: [172.16.5.169] [5] NAS-Port - value: [260613] [8] Framed-IP-Address - valu

**26] cisco-av-pair - value: [dot11-device-info=<00><00><00><13>Samsung Galaxy S22+] [26] cisco-av-pair -**

[26] cisco-av-pair - value: [audit-session-id=A90510AC0000005BD7DDDAA7] [26] cisco-av-pair - value: [v

步驟 3.終端屬性已更新且終端已分類

然後，此系統日誌消息將與Profiler元件共用。Profiler.log接收經過解析的系統日誌消息並提取終端屬性。

<#root>

2023-09-27 1

**8:19:23,601 DEBUG [SyslogListenerThread]**

[[]] cisco.profiler.probes.radius.SyslogMonitor -::::::-

**Radius Packet Received 1266**

2023-09-27

**18:19:23,601 DEBUG [SyslogListenerThread]**

[[]] cisco.profiler.probes.radius.SyslogDefragmenter -::::::- parseHeader inBuffer=<181>Sep 27 18:19:23

**CISE_RADIUS_Accounting 0000000297**

3 0 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,

**UserName=bob**

, NetworkDeviceName=lab-wlc, User-Name=bob, NAS-IP-Address=172.16.5.169, NAS-Port=260613, Framed-IP-Add
Called-Station-ID=00-1e-f6-5c-16-ff,

**Calling-Station-ID=0a-5a-f0-b3-b5-9c**

, NAS-Identifier=vimontes-wlc, Acct-Status-Type=Start, Acct-Delay-Time=0, Acct-Session-Id=00000018, Acc
Event-Timestamp=1695838756, NAS-Port-Type=Wireless - IEEE 802.11, cisco-av-pair=dc-profile-name=Samsung
cisco-av-pair=dc-device-class-tag=Samsung Galaxy S22+, cisco-av-pair=dc-certainty-metric=40,
cisco-av-pair=64:63:2d:6f:70:61:71:75:65:3d:01:00:00:00:00:00:00:00:00:00:00:00, cisco-av-pair=dc-proto

**18:19:23,601 DEBUG**

[SyslogListenerThread][[]] cisco.profiler.probes.radius.SyslogMonitor -::::::-

**Radius Packet Received 1267**

2023-09-27

**18:19:23,601 DEBUG**

[SyslogListenerThread][[]] cisco.profiler.probes.radius.SyslogDefragmenter -::::::- parseHeader inBuffe

**CISE_RADIUS_Accounting 0000000297 3 1**

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=A90510AC000006**

, 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,

終端屬性資訊已更新。

<#root>

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

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

cisco.profiler.probes.radius.RadiusParser -:*A90510AC0000005BD7DDDAA7*::::-

**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 -:A90510AC0000005BD7DDDAA7::::-

**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 -:A90510AC0000005BD7DDDAA7::::-

**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 -:A90510AC0000005BD7DDDAA7::::-

**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 -:A90510AC0000005BD7DDDAA7::::-

**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 -:A90510AC0000005BD7DDDAA7::::-

**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 -:A90510AC0000005BD7DDDAA7::::- 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

屬性更新會觸發新的端點分析事件。再次評估分析策略，並分配新的配置檔案。

<#root>

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

**DEBUG [pool-533-thread-35]**

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC0000005BD7DDDAA7::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 -:A90510AC0000005BD7DDDAA7::62cc7a10-5d62-

**DEBUG [pool-533-thread-35]**

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC0000005BD7DDDAA7::62cc7a10-5d62-

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

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

步驟 4.CoA和重新認證

當WiFi裝置分析屬性發生更改時，ISE必須為終端會話傳送CoA。

<#root>

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

**DEBUG [pool-533-thread-35]**

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC0000005BD7DDDAA7::62cc7a10-5d62-

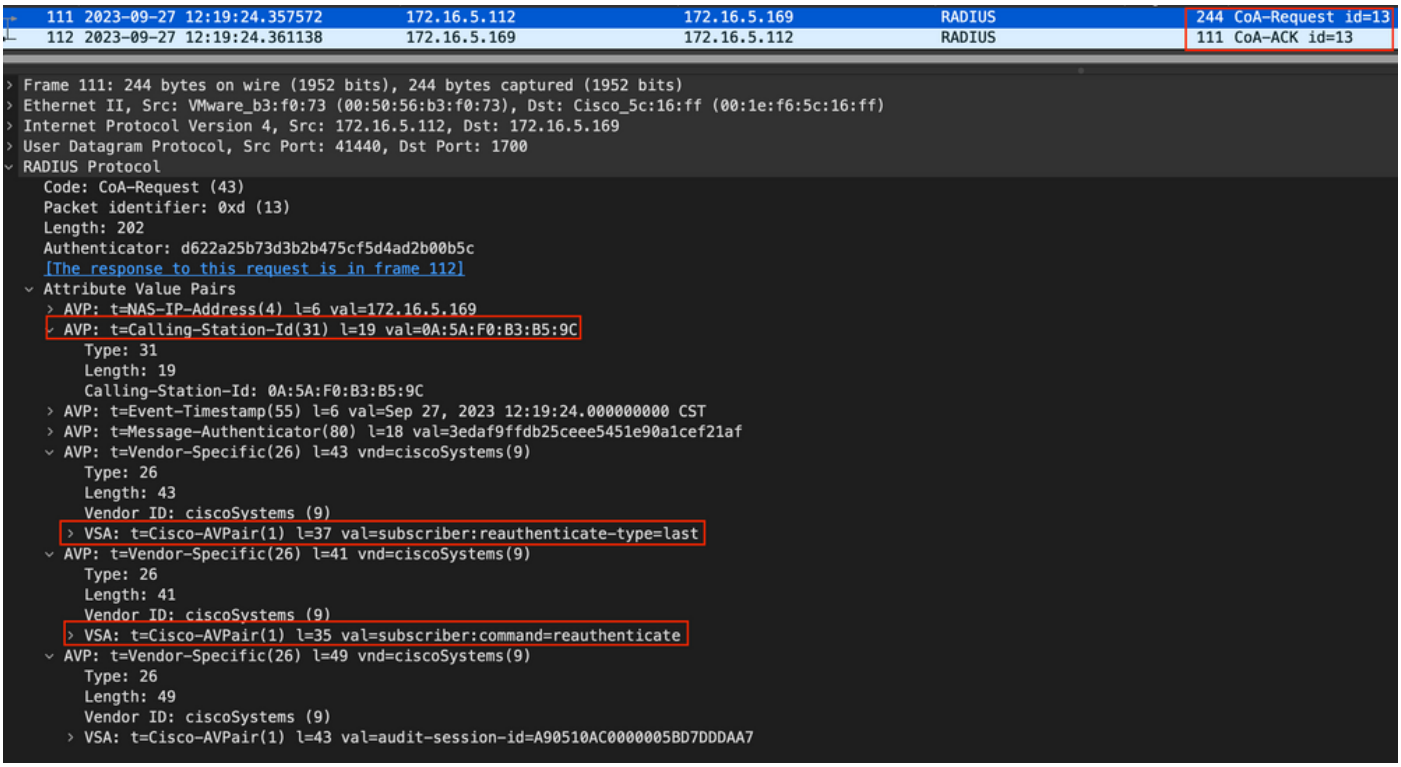
**Endpoint 0A:5A:F0:B3:B5:9C IdentityGroup / Logical Profile Changed/ WiFi device analytics attribute char**

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

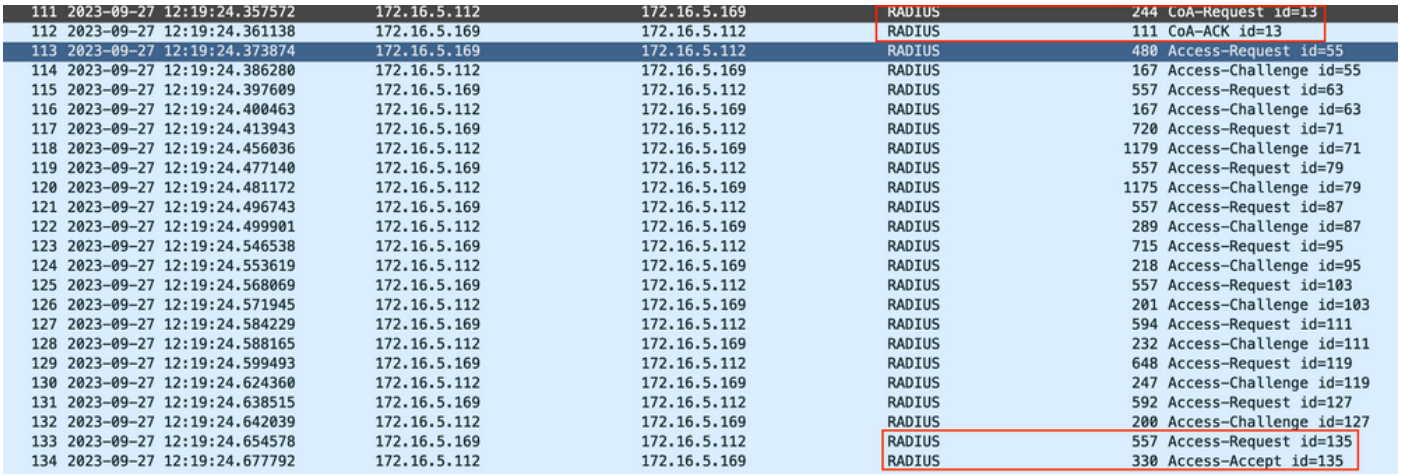
**DEBUG [pool-533-thread-35]**

```
[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC0000005BD7DDDAA7::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
```

資料包捕獲有助於確保ISE將CoA傳送到WLC。它還顯示在處理CoA之後收到新的訪問請求資料包。




終端分析後的*RADIUS CoA*資料包




終端分析後的*Radius CoA*和新的訪問請求

**相關資訊**

- 思科身份服務引擎管理員指南3.3版
- 思科身份服務引擎發行版本註釋，版本3.3
- 收集身份服務引擎上的支援捆綁包

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。