Comprensión de Wifi Analytics for Endpoint Classification en ISE 3.3

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Antecedentes
- Configurar
  - Configuraciones en WLC
    - Paso 1. Activar globalmente la función de clasificación de dispositivos
    - Paso 2. Habilitación de TLV Caching y RADIUS Profiling
  - Configuraciones en ISE
    - Paso 1. Habilitar los servicios de definición de perfiles en los PSN en la implementación
    - Paso 2. Habilitar la sonda de perfiles RADIUS en ISE PSN
    - Paso 3. Establecer filtro de atributo de extremo y tipo de CoA
    - Paso 4. Configuración de políticas de autorización con atributos de datos de WiFi Analytics
- Verificación
- Troubleshoot
  - Paso 1. Los paquetes de contabilidad llegan a ISE
  - Paso 2. ISE analiza el paquete de cuentas con los atributos de terminal
  - Paso 3. Los atributos de terminal se actualizan y el terminal se clasifica
  - Paso 4. CoA y reautenticación
- Información Relacionada

Introducción

Este documento describe cómo funciona WiFi Analytics for Endpoint Classification. También se describe cómo configurarlo, verificarlo y solucionar problemas.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de controladores LAN inalámbricos (WLC) 9800
- Configuración de Identity Services Engine (ISE)
- Autenticación RADIUS. Flujo de paquetes de autorización y contabilidad (AAA) y terminología

Este documento asume que ya existe una WLAN que autentica a los clientes utilizando ISE como servidor RADIUS.

Para que esta función funcione, es necesario tener al menos:

- 9800 WLC Cisco IOS® XE Dublín 17.10.1
- Identificación de Services Engine v3.3.
- Puntos de acceso 802.11ac Wave2 u 802.11ax (Wi-Fi 6/6E)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

A través de WiFi Device Analytics, Cisco 9800 WLC puede aprender atributos, como el número de modelo y la versión del sistema operativo de un conjunto de terminales conectados a este dispositivo, y compartirlo con ISE. A continuación, ISE puede utilizar esta información para la clasificación de terminales, también conocida como definición de perfiles.

Actualmente, WiFi Analytics es compatible con los siguientes proveedores:

- Manzana
- Intel
- Samsung

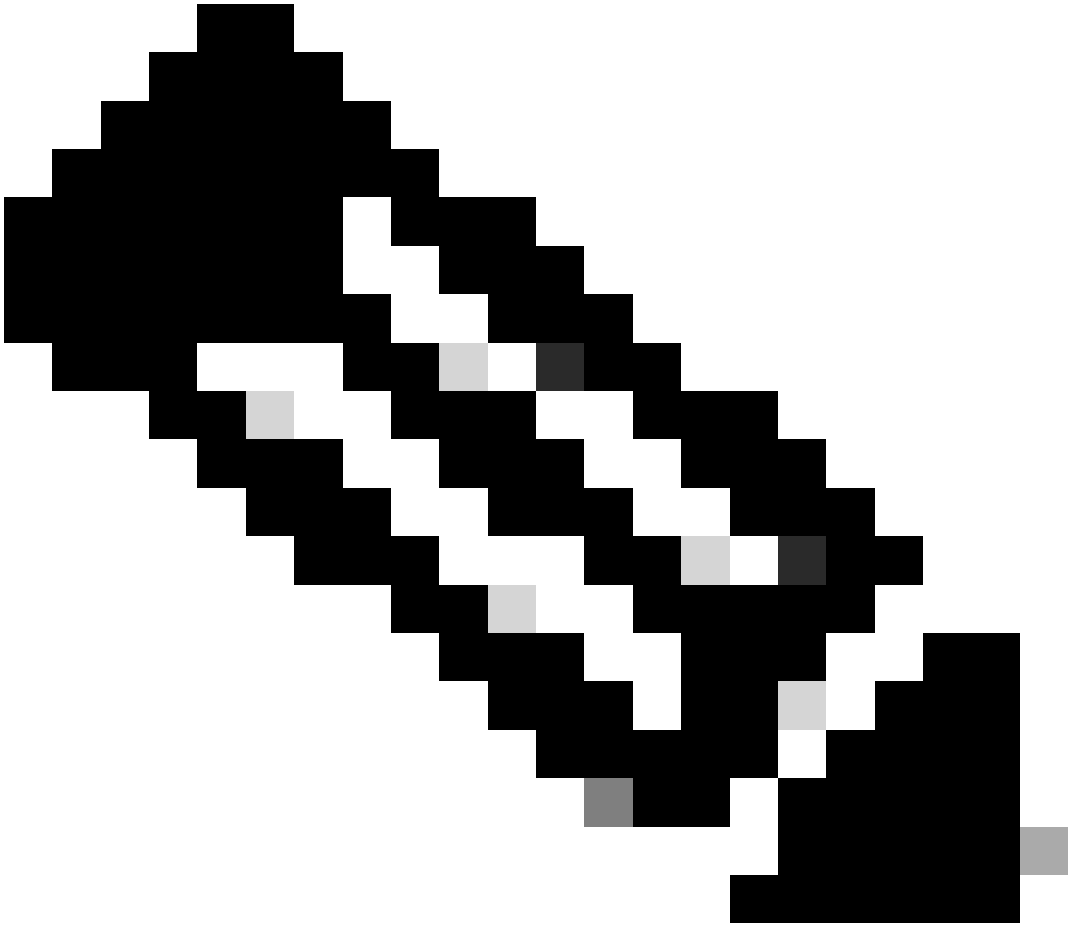
El WLC comparte la información de atributos con el servidor ISE mediante paquetes de contabilidad RADIUS.

WiFi Analytics Data Flow

Es importante recordar que los paquetes de RADIUS Accounting en un flujo RADIUS AAA se envían solamente después de que el servidor RADIUS envíe un paquete RADIUS Access-Accept como respuesta al intento de autenticación del punto final. En pocas palabras, el WLC comparte la información del atributo del extremo solamente después de que una sesión RADIUS para ese extremo se establece entre el servidor RADIUS (ISE) y el dispositivo de acceso a la red (WLC).

Estos son todos los atributos que ISE puede utilizar para la clasificación y autorización de terminales:

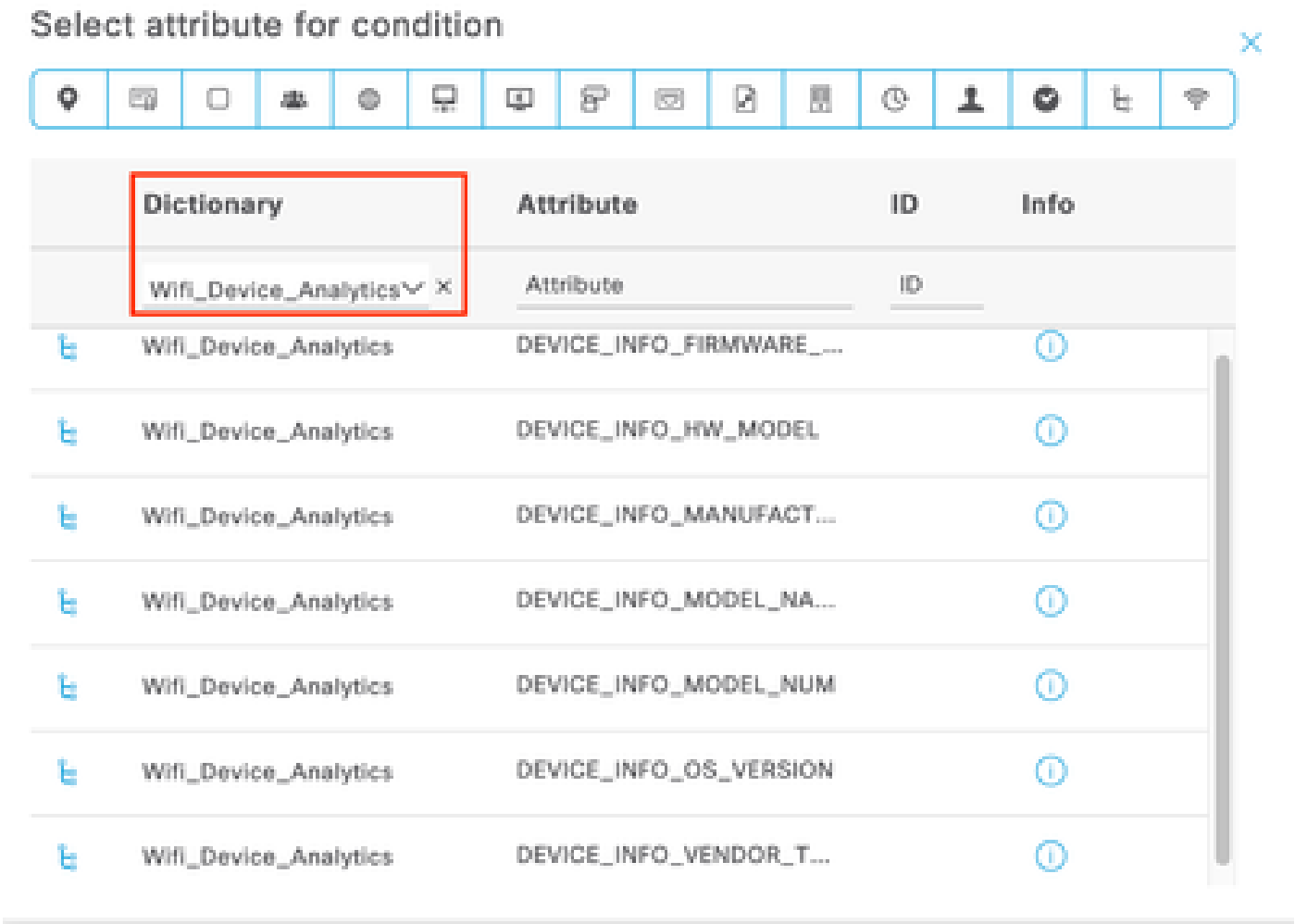
- DEVICE_INFO_FIRMWARE_VERSION
- DEVICE_INFO_HW_MODEL
- DEVICE_INFO_MANUFACTURER_MODEL
- DEVICE_INFO_MODEL_NAME
- DEVICE_INFO_MODEL_NUM
- DEVICE_INFO_OS_VERSION
- DEVICE_INFO_VENDOR_TYPE



Nota: el WLC puede enviar más atributos en función del tipo de terminal que se conecta, pero solo los enumerados se pueden utilizar para la creación de políticas de autorización en ISE.

Una vez que ISE recibe el paquete de cuentas, puede procesar y consumir estos datos de análisis en él y utilizarlo para reasignar un grupo de identidad o perfil de terminal.

Los atributos de WiFi Endpoint Analytics se enumeran en el diccionario WiFi_Device_Analytics. Los administradores de red pueden incluir estos atributos en las condiciones y políticas de autorización de terminales.



Diccionario de análisis de dispositivos WiFi

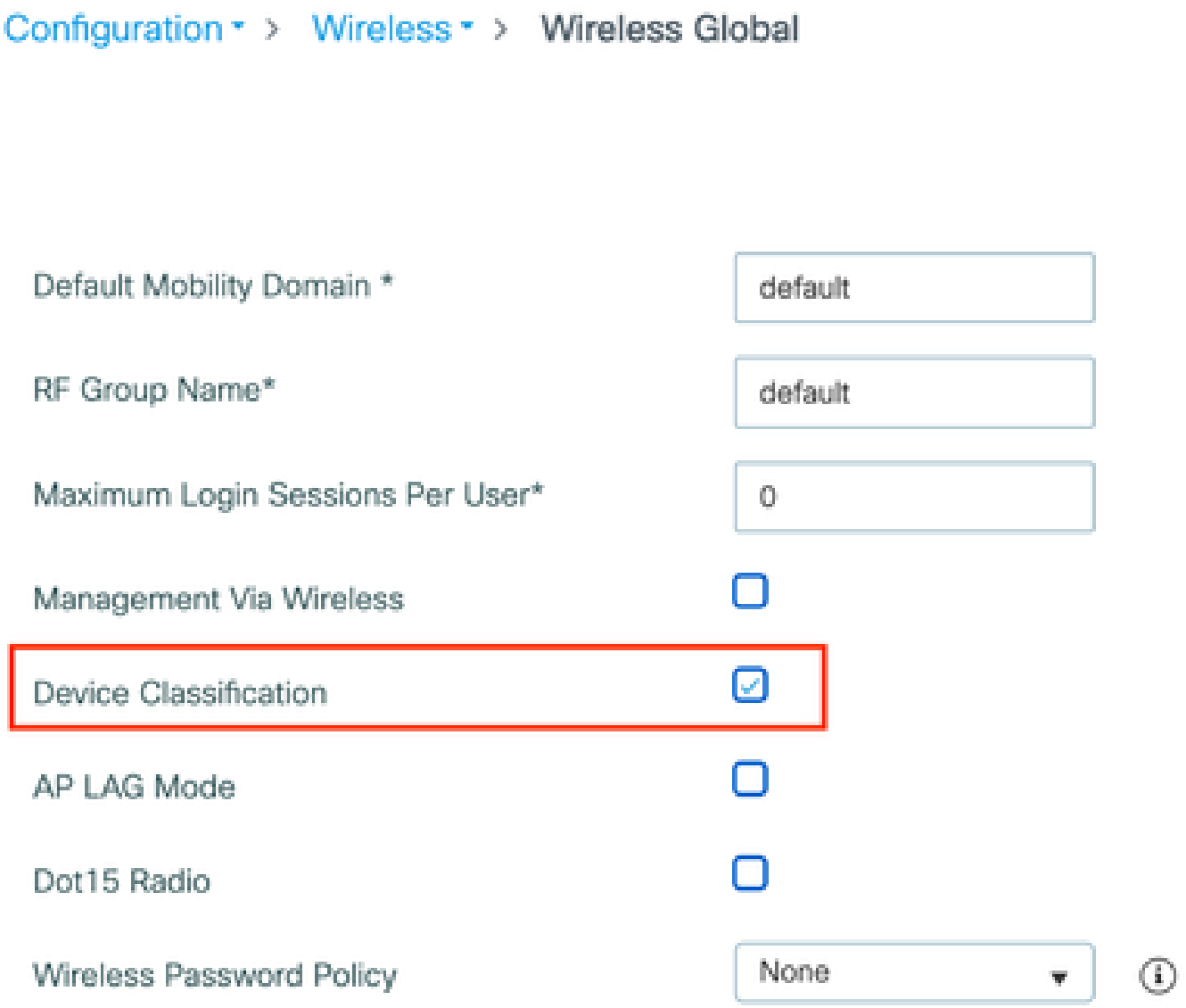
Si se produce algún cambio en los valores de atributo actuales que ISE almacena para el terminal, ISE inicia un cambio de autorización (CoA), lo que permite evaluar el terminal teniendo en cuenta los atributos actualizados.

Configurar

Configuraciones en WLC

Paso 1. Activar globalmente la función de clasificación de dispositivos

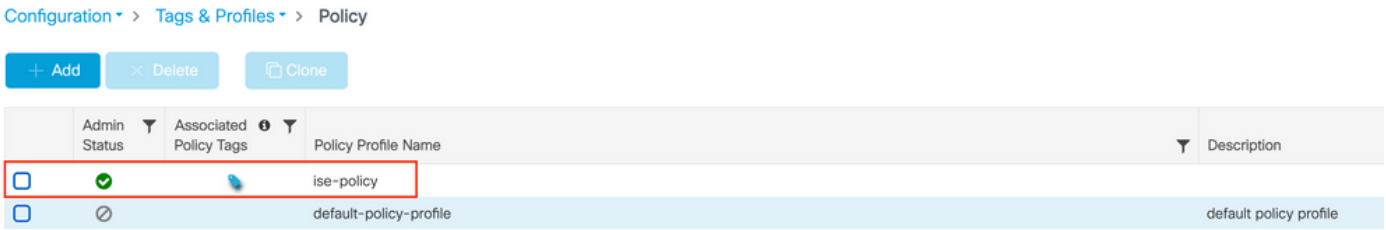
Navegue hasta Configuration > Wireless > Wireless Global y marque la casilla de verificación Device Classification.



Configuración de clasificación de dispositivos

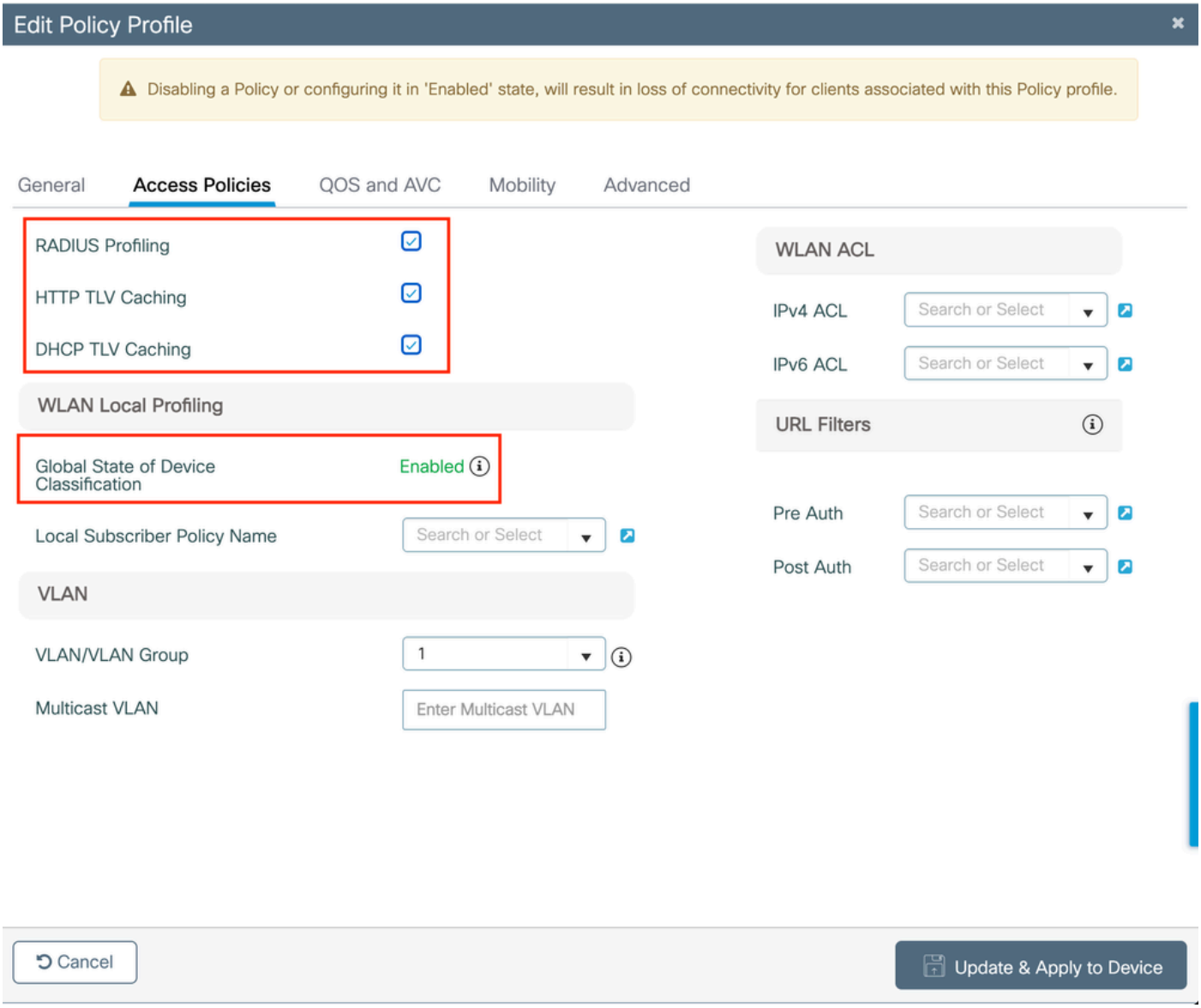
Paso 2. Habilitación de TLV Caching y RADIUS Profiling

Navegue hasta Configuration > Tags and Profiles > Policy y seleccione el Policy Profile utilizado por la WLAN donde se conectan los clientes RADIUS.



Selección de política inalámbrica

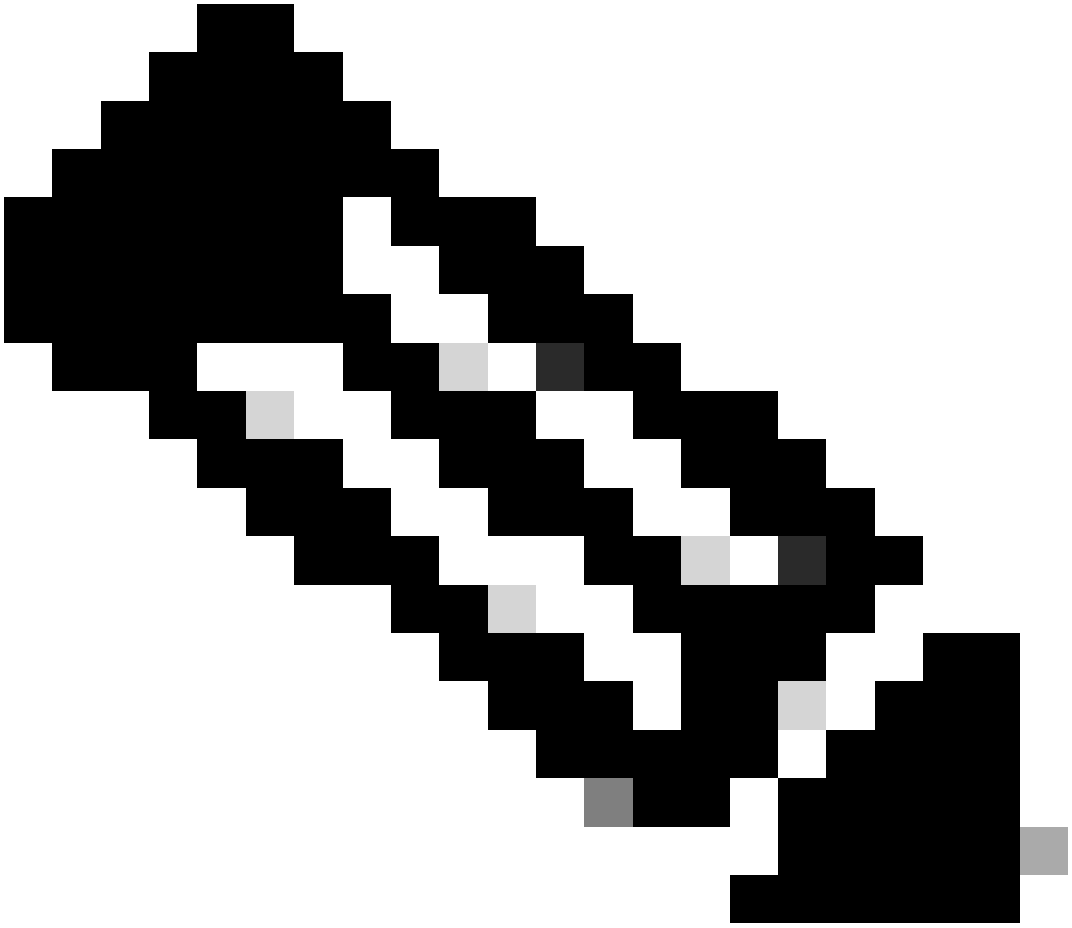
Haga clic en Access Policies y verifique las opciones RADIUS Profiling, HTTP TLV Caching y DHCP TLV Caching. Debido a la acción realizada en el paso anterior, la clasificación del estado global de los dispositivos ahora aparece en el estado Activado.



Configuración de RADIUS Profiling y Caching

Inicie sesión en WLC CLI y habilite dot11 TLV Accounting.

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

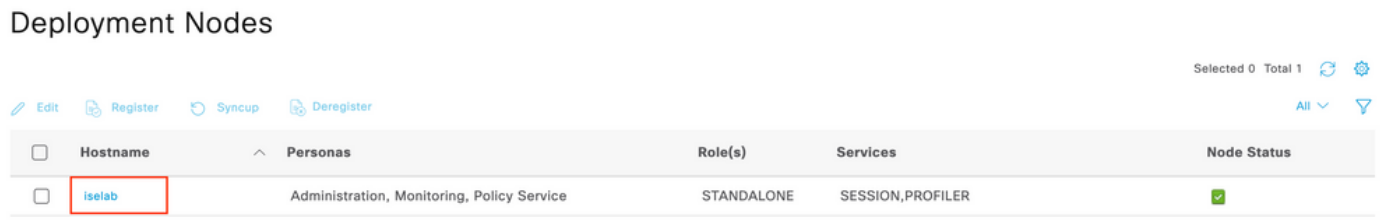


Nota: El perfil de política inalámbrica debe desactivarse antes de utilizar este comando. Este comando sólo está disponible en Cisco IOS XE Dublin 17.10.1 versión y posteriores.

Configuraciones en ISE

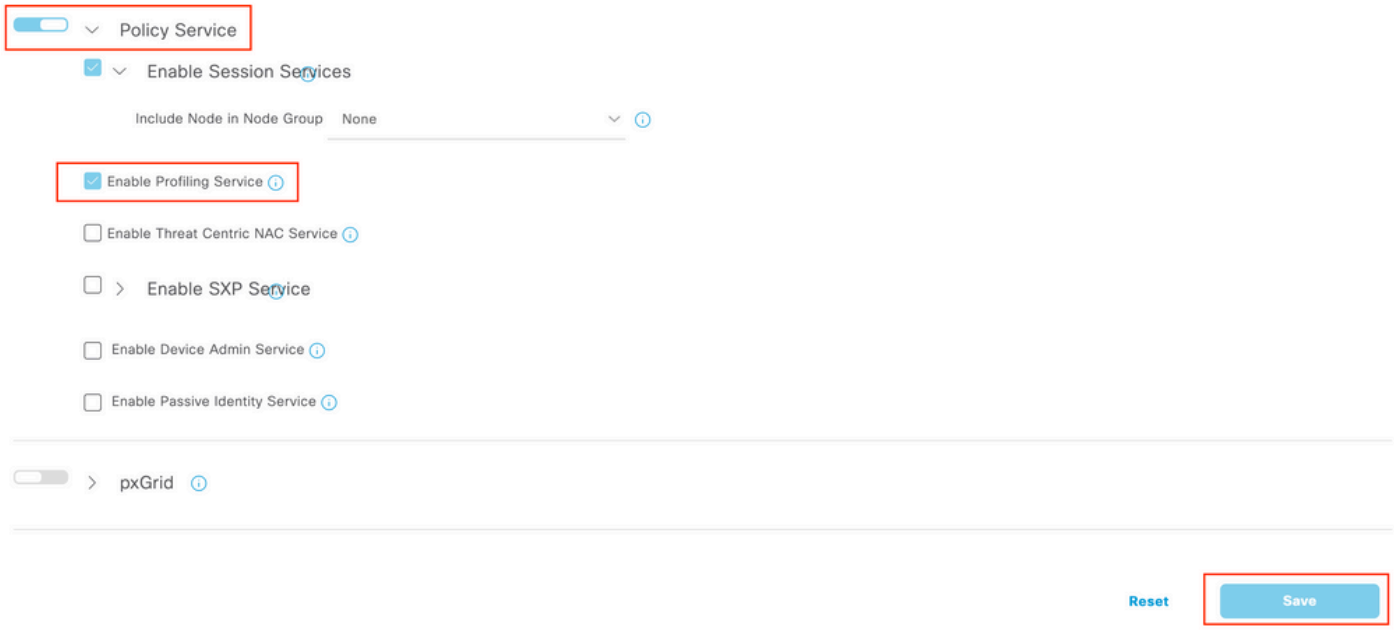
Paso 1. Habilitar los servicios de definición de perfiles en los PSN en la implementación

Vaya a **Administration > Deployment** y haga clic en el nombre de PSN.



Selección de nodo de ISE PSN

Desplácese hasta la sección **Servicio de políticas** y marque la casilla de verificación **Habilitar servicio de perfiles**. Haga clic en el botón **Save**.



Configuración de Profiler Services

Paso 2. Habilitar la sonda de perfiles RADIUS en ISE PSN

Desplácese hasta la parte superior de la página y haga clic en la ficha **Profiling Configuration**. Muestra todos los sondeos de perfiles disponibles para su uso en ISE. Active la **sonda RADIUS** y haga clic en **Save**.

Deployment Nodes List > iselab

Edit Node

General Settings | Profiling Configuration

> NETFLOW

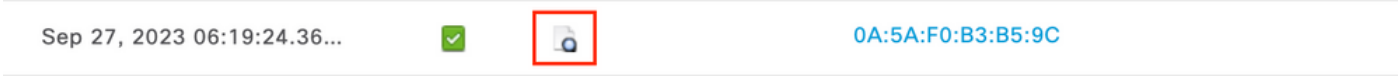
> DHCP

> DHCPSPAN

> HTTP

Nota: El paquete CoA siempre tiene un campo de identidad vacío, pero el ID de terminal es el mismo que en el primer paquete de autenticación.

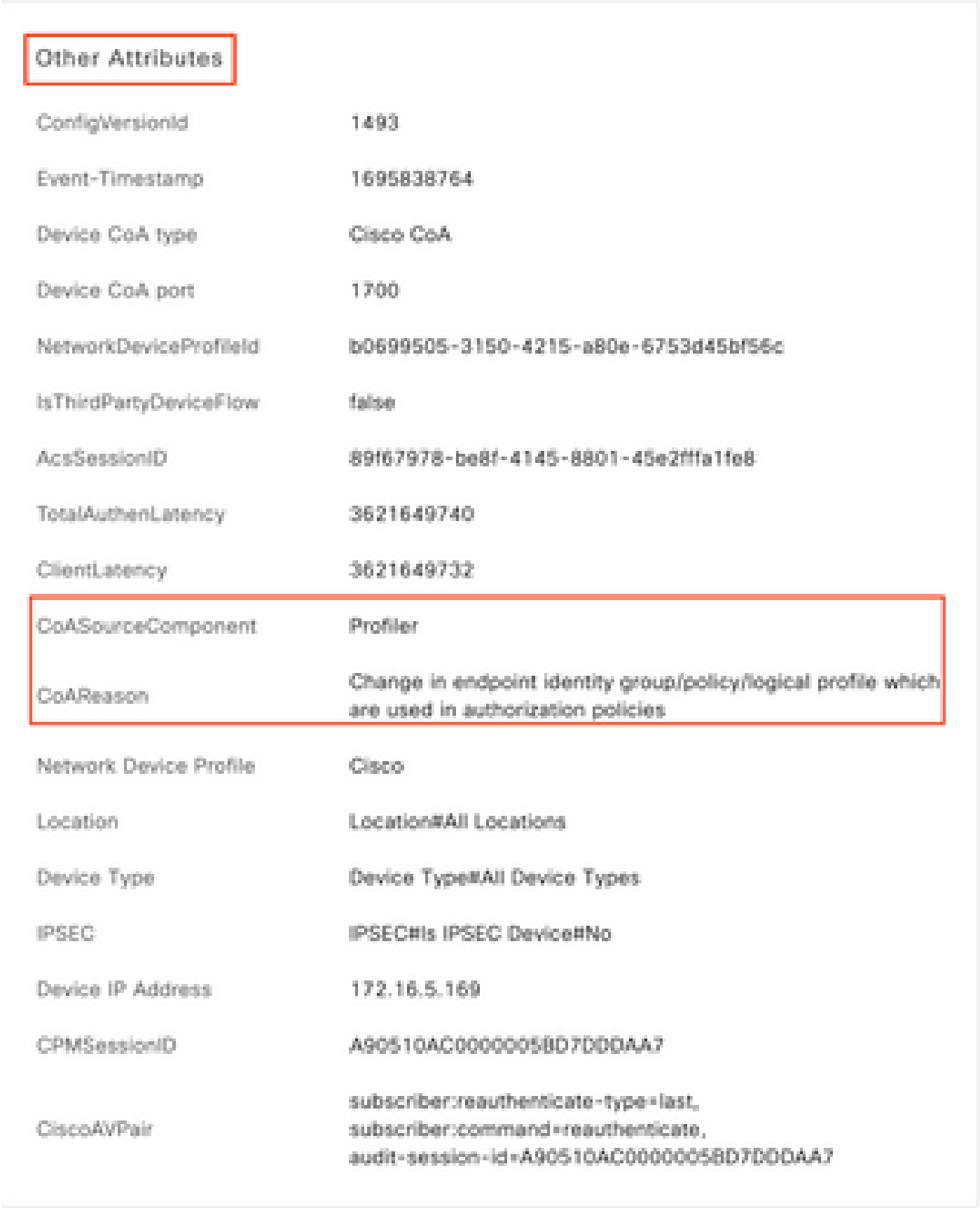
Haga clic en el **icono** situado en la columna **Detalles** del registro de cambio de autorización.



Acceso a los detalles del paquete CoA

La información detallada de CoA se muestra en una nueva pestaña del navegador. Desplácese hacia abajo hasta la sección **Otros atributos**.

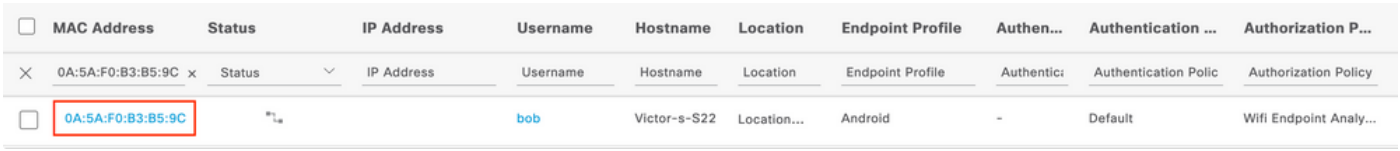
El componente de origen CoA se muestra como generador de perfiles. El motivo de CoA se muestra como Cambio en el grupo de identidades de terminales/política/perfil lógico que se utilizan en las políticas de autorización.



Componente y motivo del desencadenado de CoA

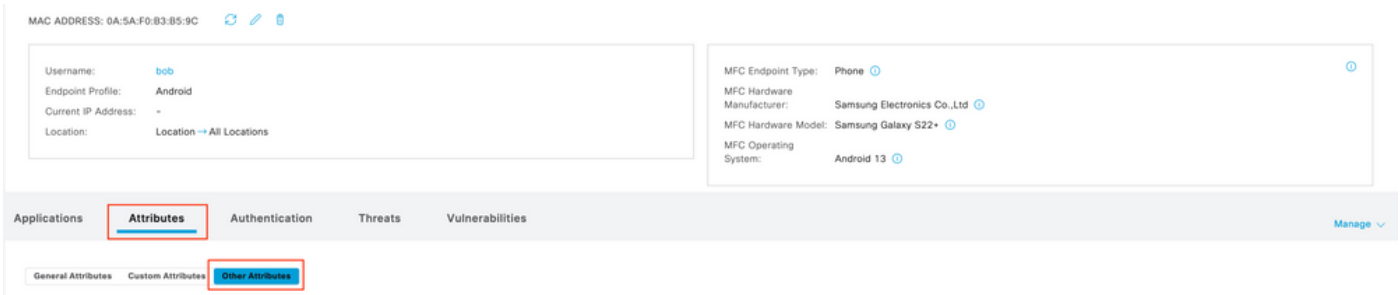
Navegue hasta **Visibilidad de contexto > Terminales > Autenticación**. En esta ficha, utilice los filtros para localizar el extremo de prueba.

Haga clic en la **dirección MAC del terminal** para acceder a los **atributos** del **terminal**.



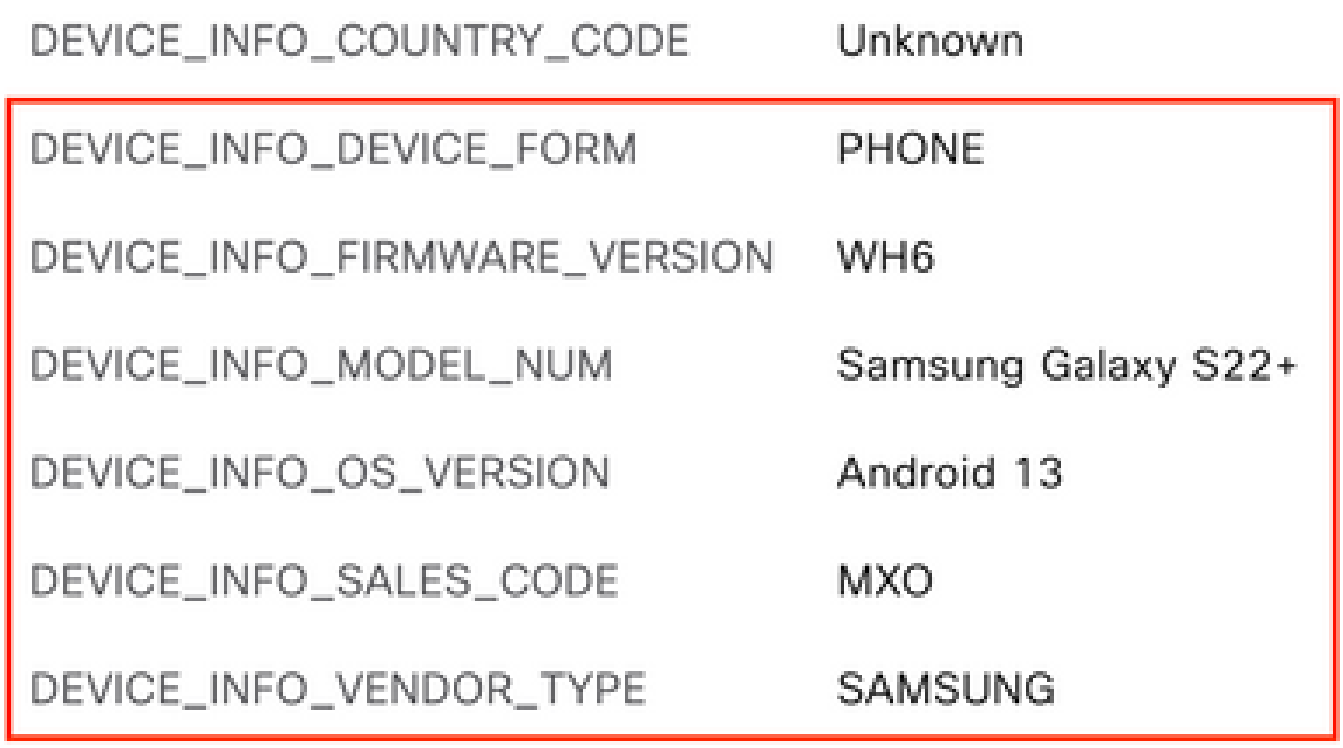
Terminal en visibilidad de contexto

Esta acción muestra toda la información que ISE almacena sobre este terminal. Haga clic en la sección **Atributos** y, a continuación, seleccione **Otros atributos**.



Selección de otro atributo de terminal en la visibilidad del contexto

Desplácese hacia abajo hasta que encuentre los atributos del **diccionario WiFi_Device_Analytics**. La ubicación de estos atributos en esta sección significa que ISE los recibió correctamente a través de los paquetes de contabilidad y se puede utilizar para la clasificación de terminales.



Atributos de WiFi Analytics en la visibilidad del contexto

A modo de referencia, a continuación se muestran ejemplos de atributos de Windows 10 y 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

Ejemplo de atributos de extremo de 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

Ejemplo de atributos de extremo de iPhone

Troubleshoot

Paso 1. Los paquetes de contabilidad llegan a ISE

En WLC CLI, asegúrese de que la **contabilización DOT11 TLV, el almacenamiento en caché DHCP TLV** y el **almacenamiento en caché HTTP TLV** estén habilitados en las configuraciones de perfiles de políticas.

<#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

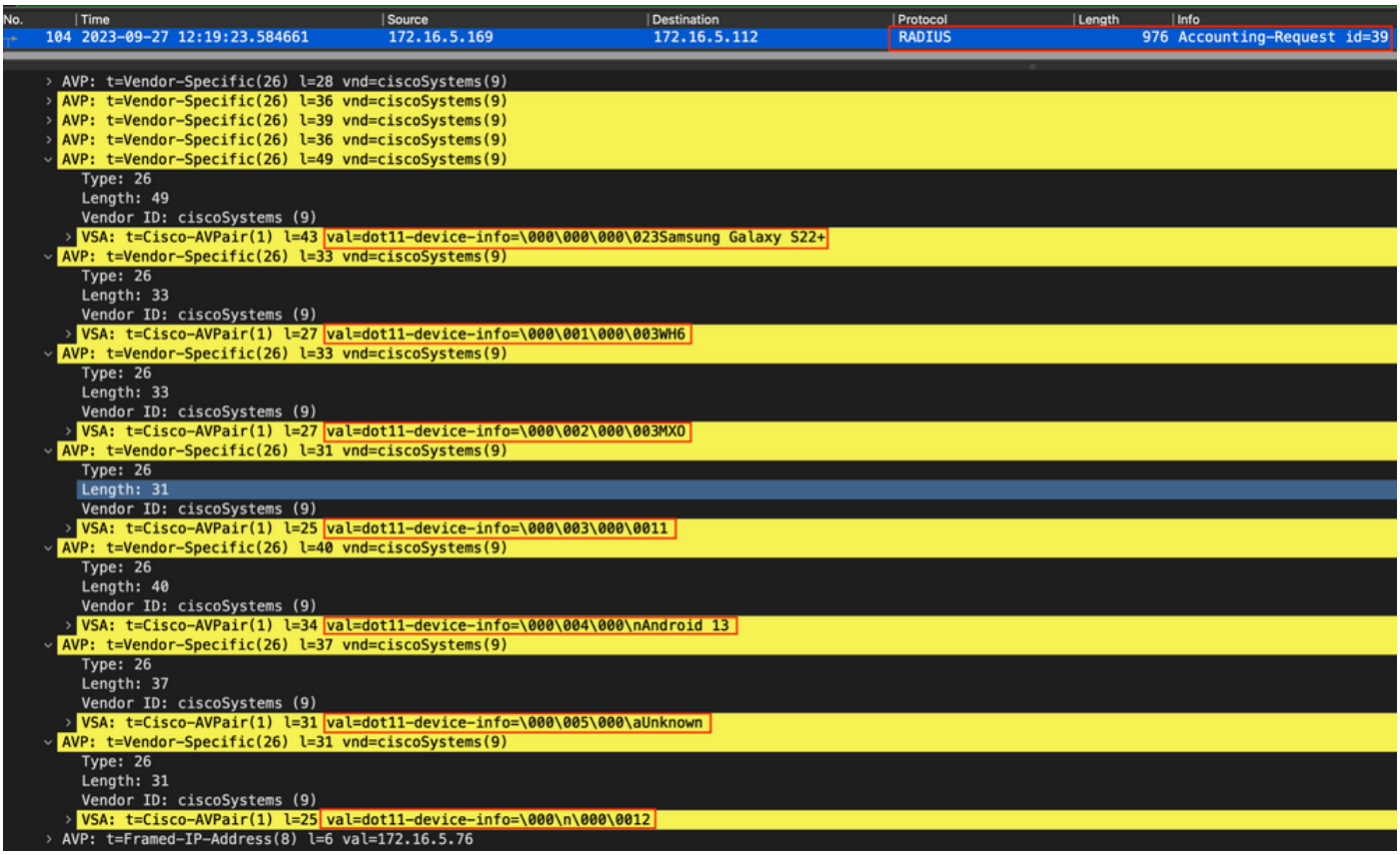
 no shutdown

Recopile **capturas de paquetes** en los extremos de WLC o ISE mientras conecta un terminal. Puede utilizar cualquier herramienta de análisis de paquetes conocida, como Wireshark, para analizar los archivos recopilados.

Filtre por paquetes de cuentas RADIUS y por ID de estación de llamada (dirección MAC del terminal de prueba). Por ejemplo, este filtro se puede utilizar:

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

Una vez localizados, expanda los campos **Cisco-AVPair** para localizar los **datos de análisis WiFi** dentro del paquete de contabilidad.



Atributos TLV de Extremo dentro de un Paquete de Contabilización

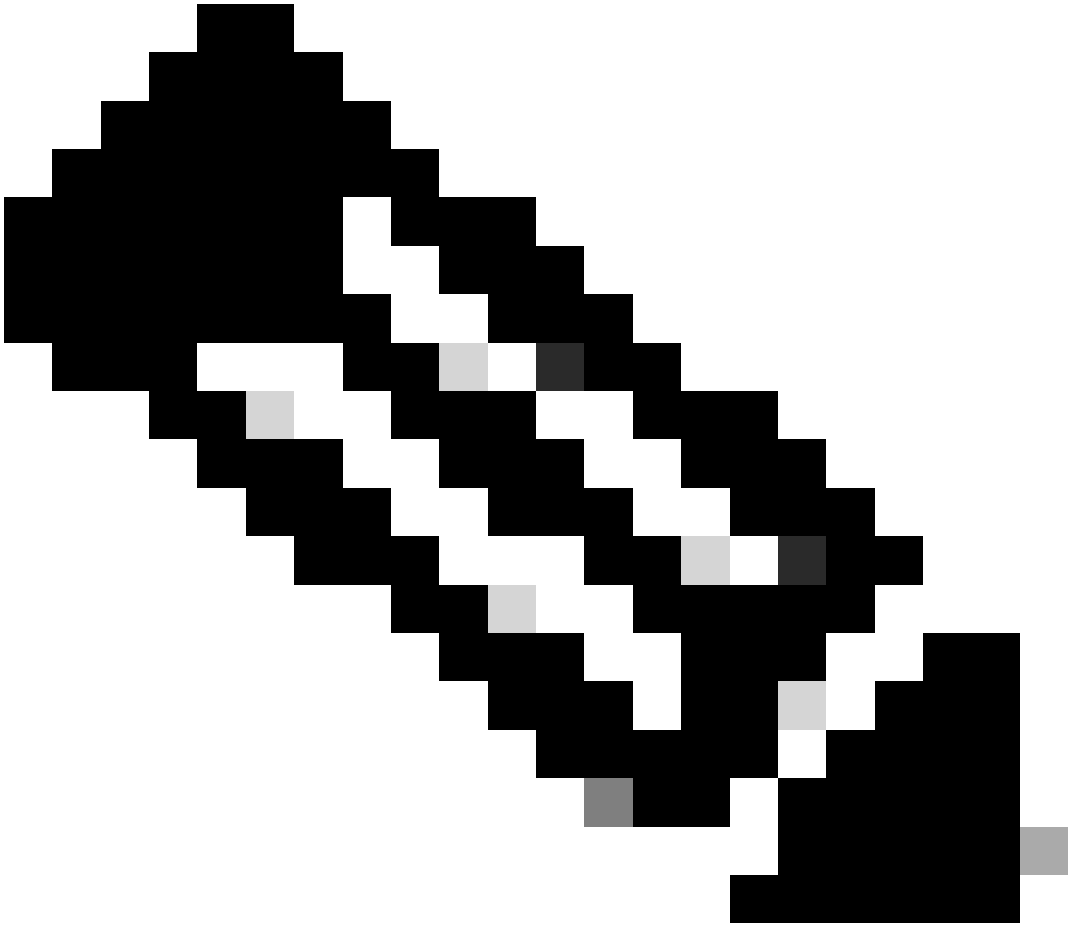
Paso 2. ISE analiza el paquete de cuentas con los atributos de terminal

Al final de ISE, estos componentes se pueden configurar en el nivel DEBUG para garantizar que los paquetes de contabilidad RADIUS enviados por el WLC alcanzan ISE y se procesan correctamente.

A continuación, puede recopilar **ISE Support Bundle** para recopilar los archivos de registro. Para obtener más información sobre cómo recopilar el paquete de soporte, consulte la sección **Información Relacionada**.

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

Componentes que se depurarán para solucionar problemas



Nota: Los componentes están habilitados al nivel DEBUG solamente en el PSN que autentica los extremos.

En iseLocalStore.log, se registra el mensaje de inicio de cuentas sin necesidad de habilitar ningún componente en el nivel DEBUG. Aquí, ISE debe ver el paquete de cuentas entrante que contiene los atributos de 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,

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,

En prrt-server.log, ISE analiza el mensaje syslog del paquete de contabilidad recibido, incluidos los atributos de WiFi Analytics. Utilice los campos **CallingStationID** y **CPMSessionID** para asegurarse de que se realiza un seguimiento de la sesión y el punto final correctos.

<#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

Paso 3. Los atributos de terminal se actualizan y el terminal se clasifica

Este mensaje de syslog se comparte con el componente del analizador. Profiler.log recibe el mensaje syslog analizado y extrae los atributos de punto final.

<#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=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,

Se actualiza la información de atributos del terminal.

<#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

La actualización de atributos desencadena un nuevo evento de definición de perfiles de terminales. Las directivas de perfiles se evalúan de nuevo y se asigna un nuevo perfil.

<#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

Paso 4. CoA y reautenticación

ISE debe enviar una CoA para la sesión de terminal cuando se produzca un cambio en los atributos de WiFi Device Analytics.

<#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-

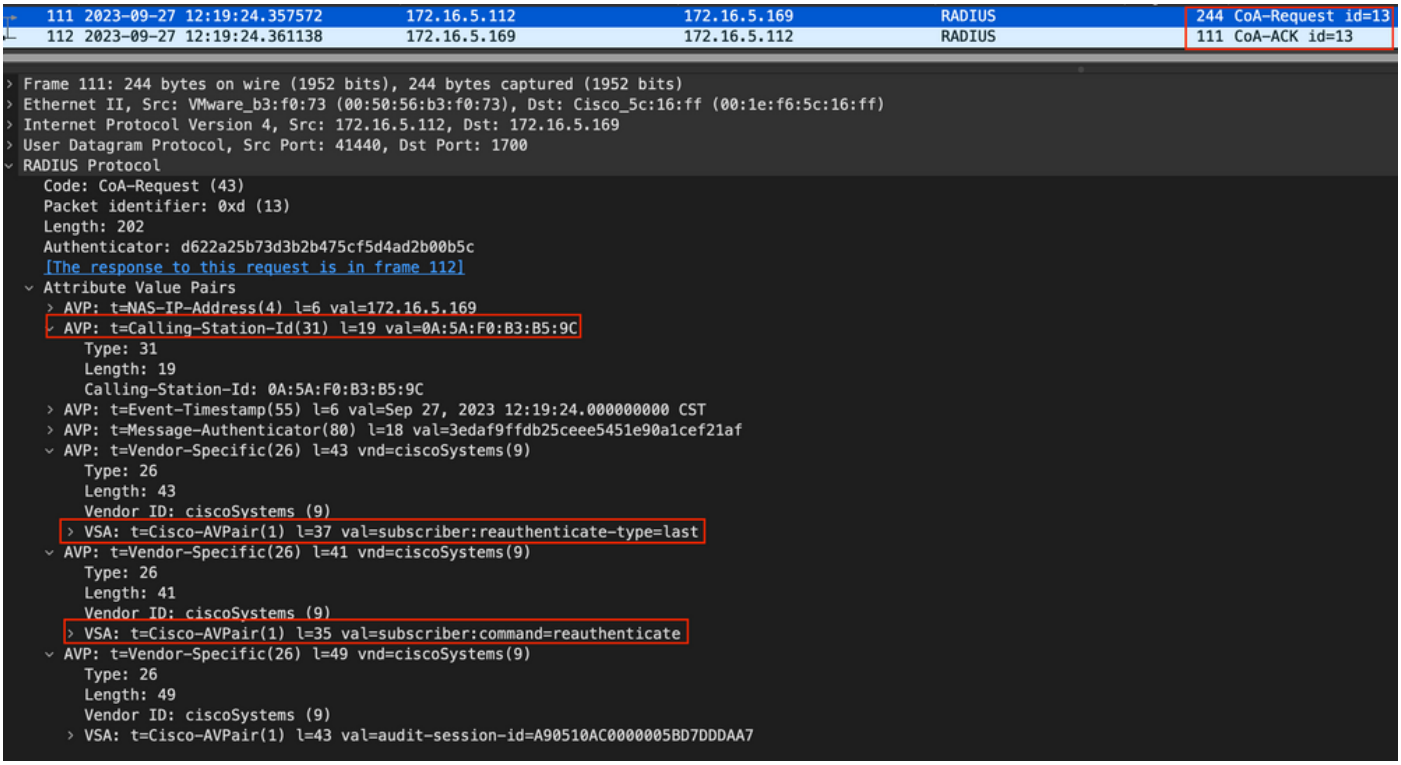
ConditionalCoAEvent with Endpoint Details : EndPoint[id=62caa550-5d62-11ee-bf1f-b6bb1580ab0d,name=] MAC:

Attribute:AAA-Server value:iselab Attribute:Airespace-Wlan-Id value:1 Attribute:AllowedProtocolMatched

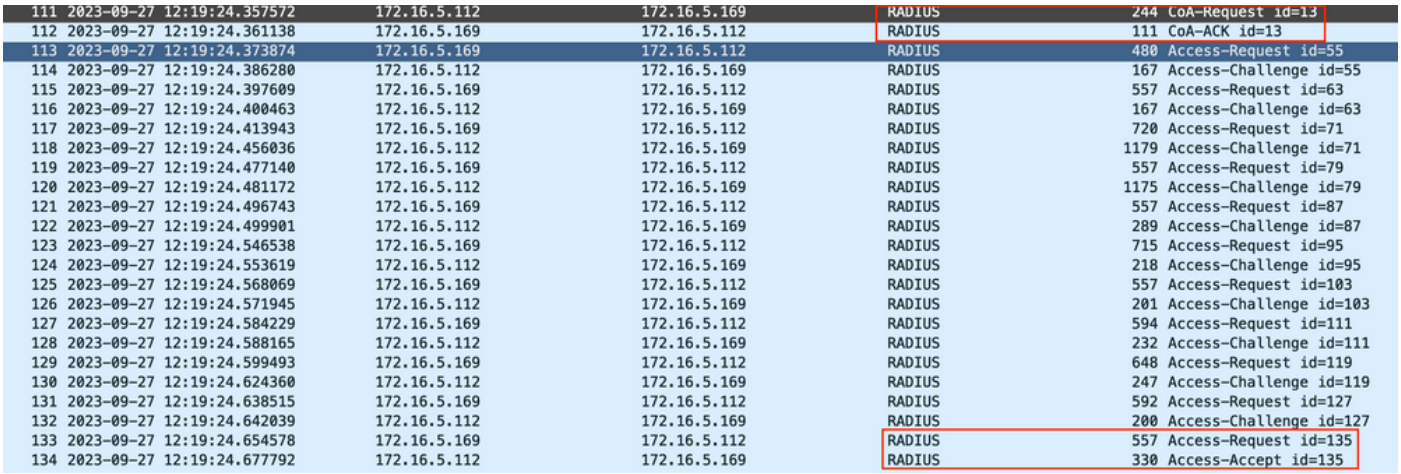
Attribute:DEVICE_INFO_COUNTRY_CODE value:Unknown Attribute:DEVICE_INFO_DEVICE_FORM value:PHONE Attribute

Attribute:DTLSSupport value:Unknown Attribute:DestinationIPAddress value:172.16.5.112 Attribute:Destin

La captura de paquetes ayuda a garantizar que ISE envíe el CoA al WLC. También muestra que se recibe un nuevo paquete Access-Request después de procesar el CoA.



Perfiles de paquetes CoA de RADIUS después del terminal



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 y New Access-Request after Endpoint Profiling

Información Relacionada

- Guía del administrador de Cisco Identity Services Engine, versión 3.3
- Notas de la versión de Cisco Identity Services Engine, versión 3.3
- Recopile el paquete de asistencia en Identity Services Engine

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).