Wi-Fi analyses begrijpen voor endpointclassificatie op ISE 3.3

Inhoud

Inleiding

In dit document wordt beschreven hoe WiFi Analytics voor endpointclassificatie werkt. Het beschrijft ook hoe te te vormen, te verifiëren, en het problemen op te lossen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- 9800 draadloze LAN-controllers (WLC)
- Configuratie van Identity Services Engine (ISE)
- RADIUS-verificatie. Autorisatie en accounting (AAA), pakketstroom en terminologie

Dit document gaat ervan uit dat er al een werkende WLAN-verificatie-clients zijn die ISE als

RADIUS-server gebruiken.

Deze optie werkt alleen als minimaal het volgende is vereist:

- 980 WLC Cisco IOS® XE Dublin 17.10.1
- Identificeer Services Engine v3.3.
- 802.11ac Wave2- of 802.11ax (Wi-Fi 6/6E) access points

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- 980 WLC Cisco IOS XE v17.12.x
- Identity Services Engine (ISE) v3.3
- Android 13-apparaat

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Via WiFi-apparaatanalyse kan Cisco 9800 WLC kenmerken, zoals modelnummer en OS-versie, leren van een aantal eindpunten die met dit apparaat zijn verbonden en deze delen met ISE. ISE kan deze informatie gebruiken voor Endpoint Classification, ook bekend als Profiling, doeleinden.

Op dit moment wordt WiFi Analytics ondersteund door de volgende leveranciers:

- appel
- Intel
- Samsung

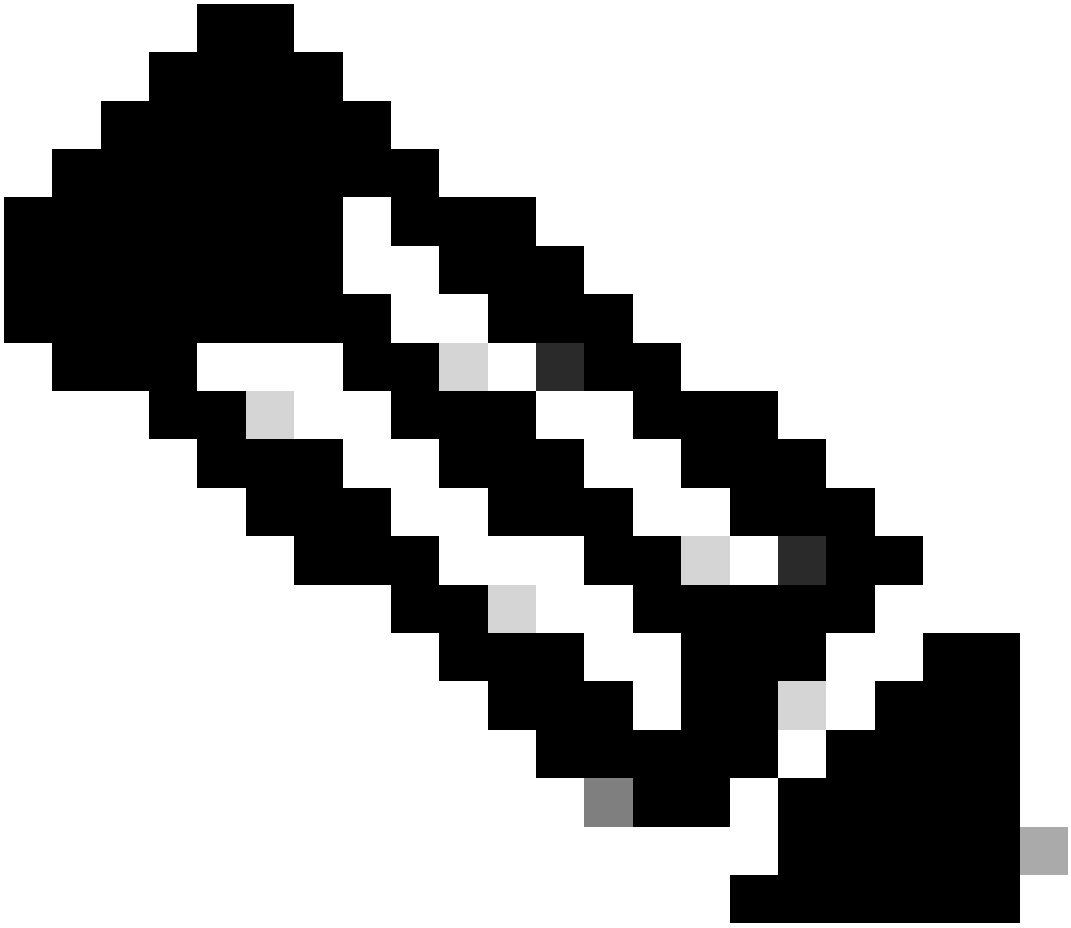
De WLC deelt de attribuutinformatie met ISE-server met behulp van RADIUS-accounting-pakketten.

WiFi Analytics Data Flow

Het is belangrijk om te onthouden dat RADIUS-accounting-pakketten op een RADIUS AAA-stroom alleen worden verzonden nadat de RADIUS-server een RADIUS-access-acceptabel pakket verstuurt als antwoord op de verificatiepoging voor endpoints. In volgorde van woorden deelt WLC de endpointattribuutinformatie alleen nadat een RADIUS-sessie voor dat eindpunt is ingesteld tussen de RADIUS-server (ISE) en Network Access Device (WLC).

Dit zijn alle eigenschappen waar ISE gebruik van kan maken voor Endpoint Classification en autorisatie:

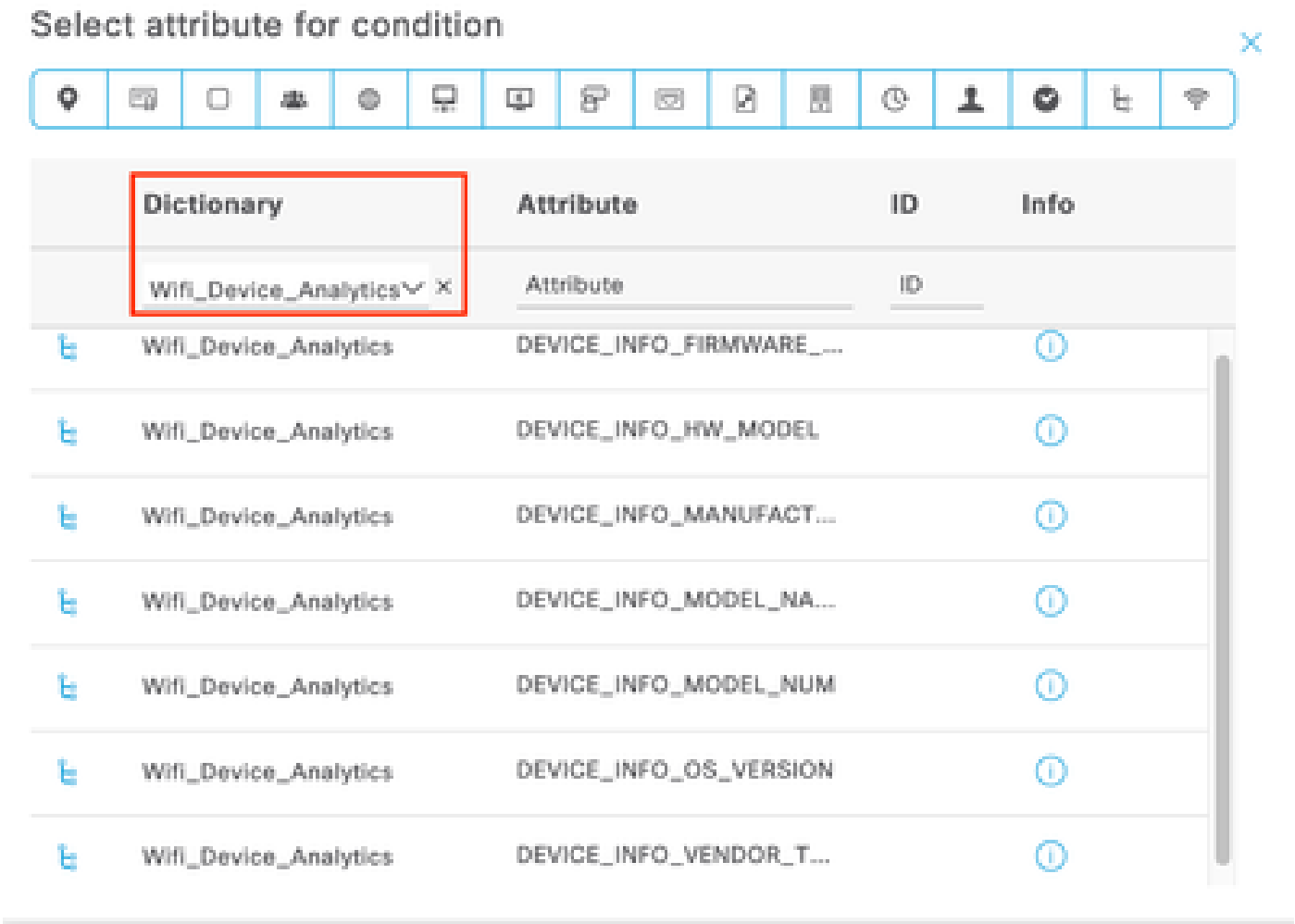
- APPARAAT_INFO_FIRMWARE_VERSIE
- APPARAAT_INFO_HW_MODEL
- APPARAAT_INFO_FABRIKANT_MODEL
- APPARAAT_INFO_MODEL_NAAM
- APPARAAT_INFO_MODEL_NUM
- APPARAAT_INFO_OS_VERSIE
- APPARAAT_INFO_LEVERANCIER_TYPE



> Opmerking: WLC kan meer attributen verzenden, afhankelijk van het endpointtype dat verbinding maakt, maar alleen de genoemde eigenschappen kunnen worden gebruikt voor de totstandkoming van Autorisatiebeleid in ISE.

Zodra ISE het Accounting pakket ontvangt, kan het deze analysegegevens verwerken en gebruiken binnen het pakket, en het gebruiken om een eindpuntprofiel/identiteitsgroep opnieuw toe te wijzen.

De eigenschappen van de WiFi Endpoint Analytics worden in het woordenboek WiFi_Device_Analytics vermeld. Netwerkbeheerders kunnen deze kenmerken opnemen in het beleid en de voorwaarden voor de endpointautorisatie.



Woordenboek voor WiFi-apparaatanalyse

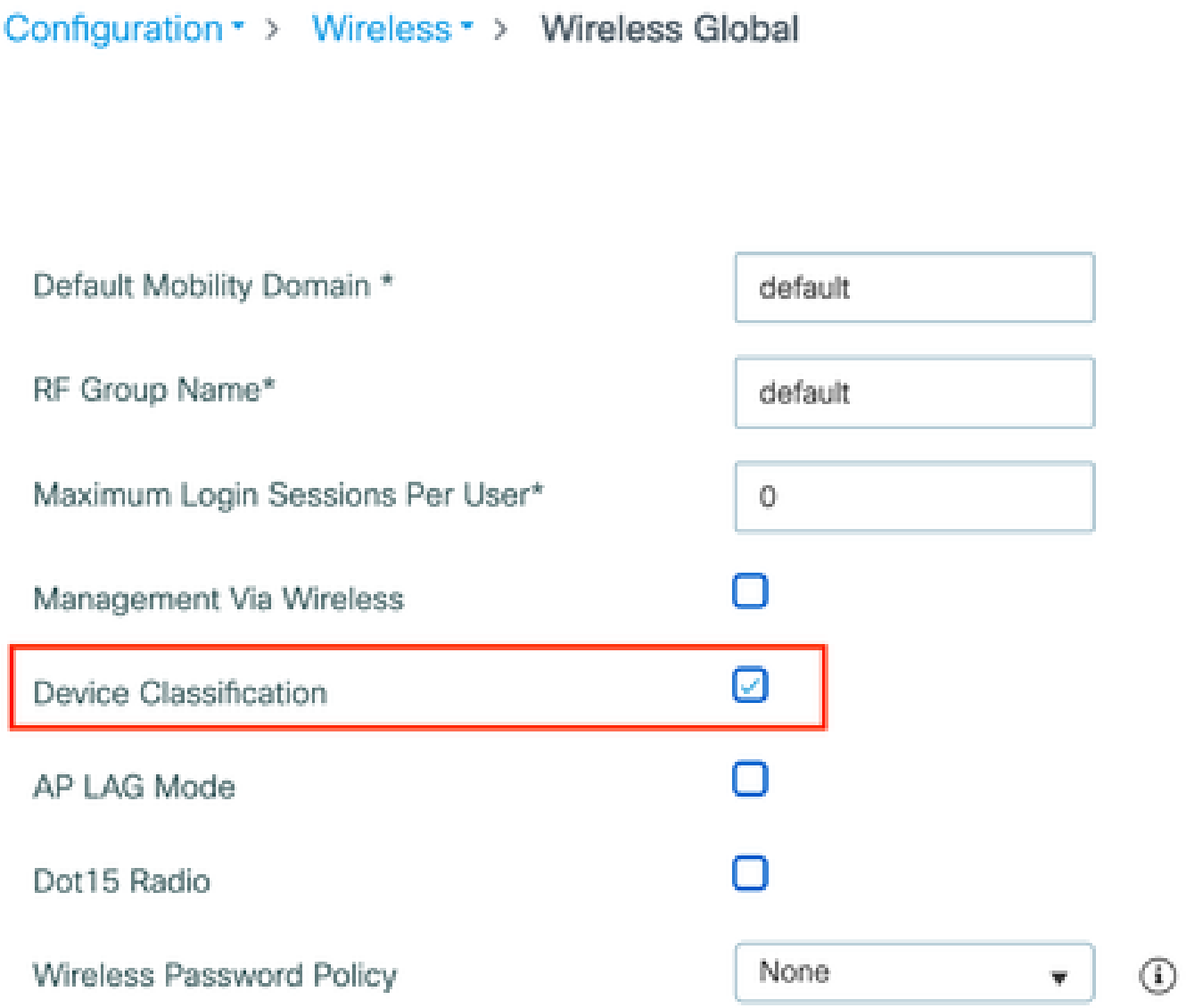
Als er veranderingen in de huidige attribuutwaarden plaatsvinden die ISE opslaat voor het eindpunt, start ISE vervolgens een Verandering van autorisatie (CoA), zodat het eindpunt kan worden geëvalueerd met inachtneming van de geactualiseerde eigenschappen.

Configureren

Configuraties op WLC

Stap 1. De functie voor apparaatclassificatie wereldwijd inschakelen

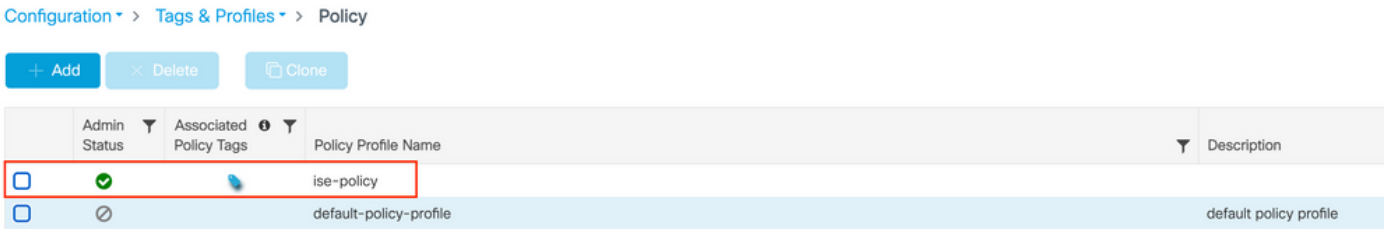
Navigeer naar Configuration > Wireless > Wireless Global en vink het aanvinkvakje Apparaatclassificatie aan.



Configuratie van apparaatclassificatie

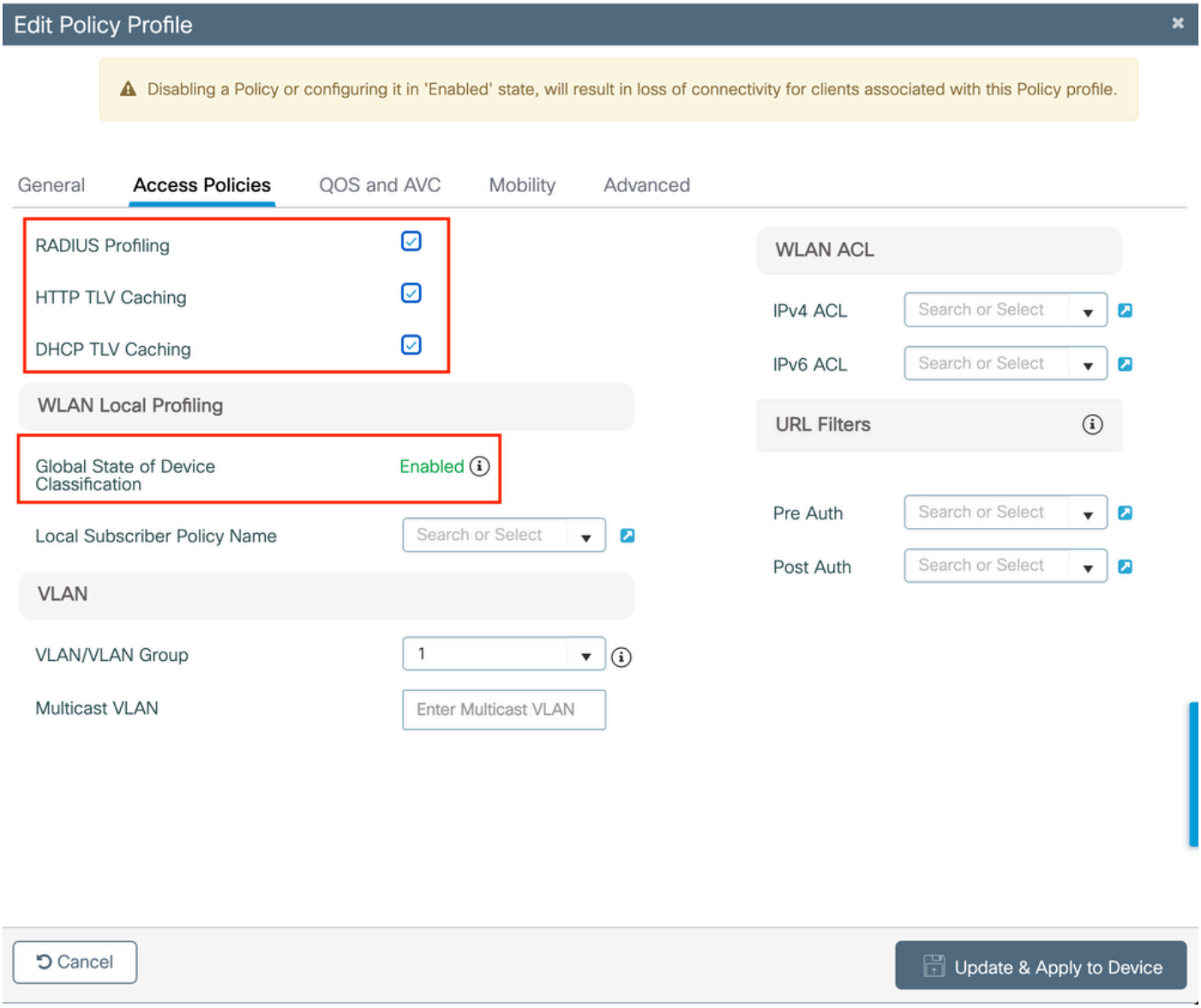
Stap 2. TLV-caching en RADIUS-profilering inschakelen

Navigeer naar Configuration > Tags en profielen > Policy en selecteer het beleidsprofiel dat wordt gebruikt door het WLAN waar de RADIUS-clients verbinding maken.



Draadloos beleid selecteren

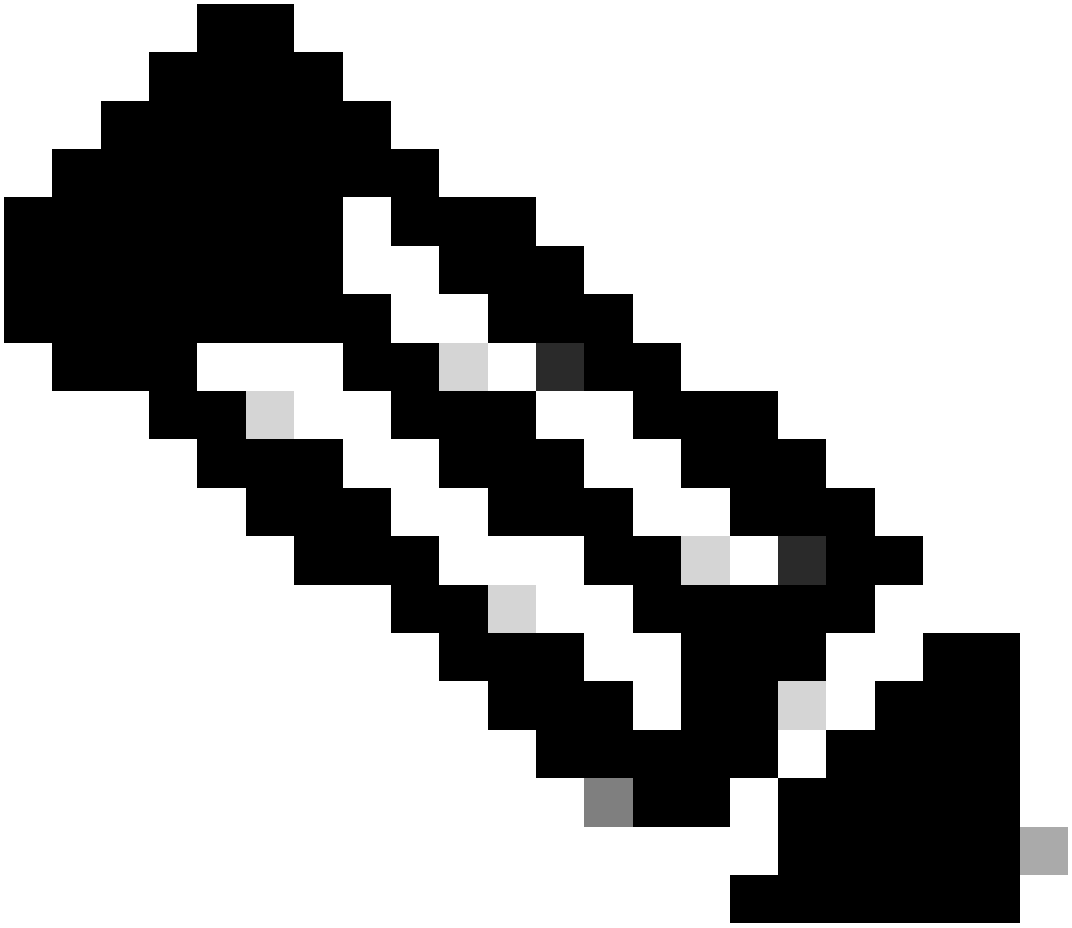
Klik op Toegangsbeleid en controleer de opties RADIUS-profielen, HTTP TLV-caching en DHCP TLV-caching. Vanwege de actie die is ondernomen in de vorige stap, wordt nu de status Ingeschakeld weergegeven in de Global State of Device Classification.



Configuratie van RADIUS-profielen en -caching

Log in op WLC CLI en schakel dot11 TLV-accounting in.

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

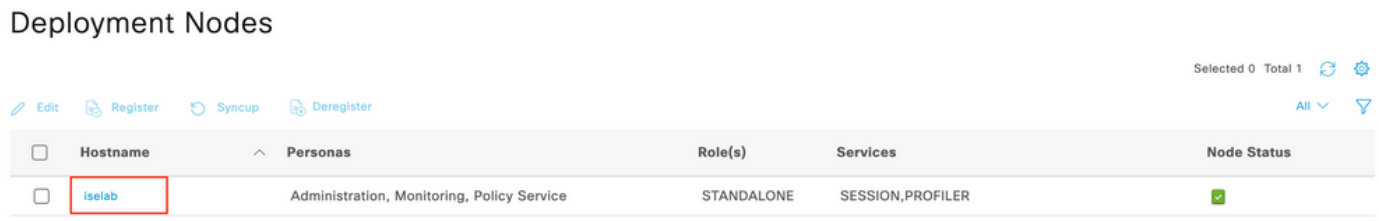


Opmerking: het draadloze beleidsprofiel moet worden uitgeschakeld voordat u deze opdracht gebruikt. Deze opdracht is alleen beschikbaar op Cisco IOS XE Dublin 17.10.1 versie en hoger.

Configuraties op ISE

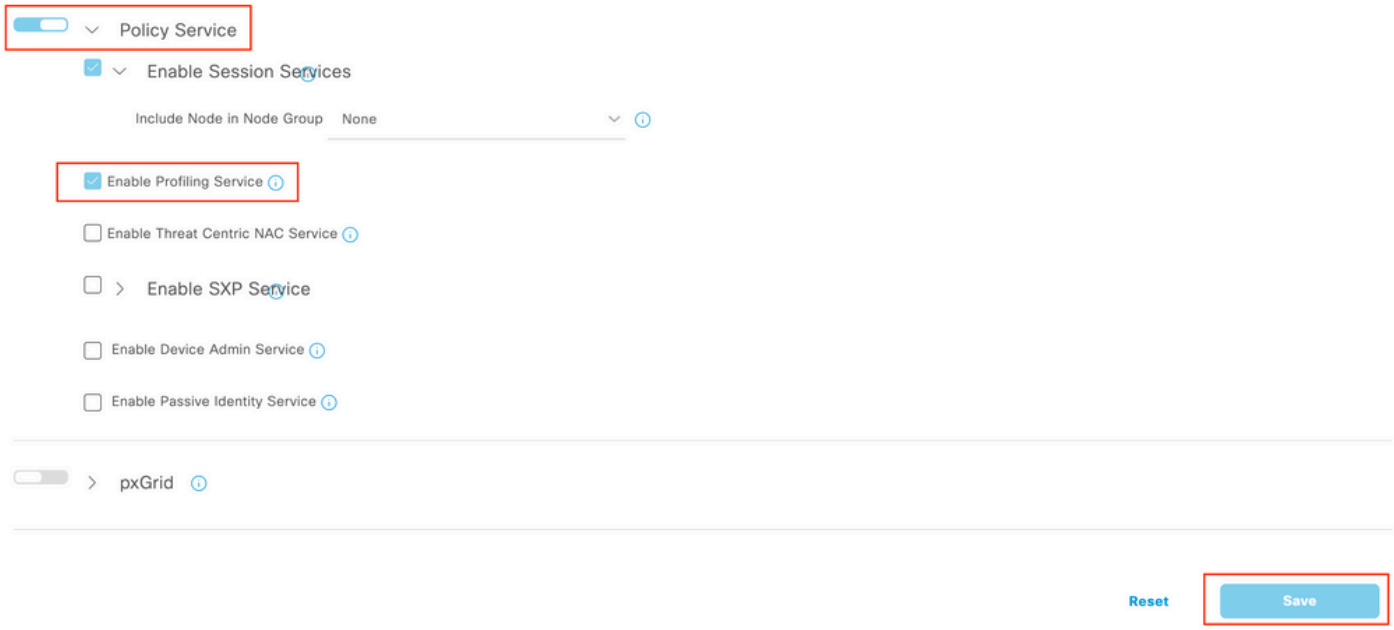
Stap 1. Profilingservices inschakelen in de PSN's bij de implementatie

Navigeer naar **Beheer > implementatie** en klik op de naam van de PSN.



Selectie van ISE-PSN-knooppunt

Blader naar beneden naar **de** sectie **Beleidsservice** en vink het aanvinkvakje **Enable Profiling Service aan**. Klik op de knop **Opslaan**.



Configuratie van profielservices

Stap 2. De RADIUS-profileringssonde inschakelen op ISE-PSN

Blader naar boven op de pagina en klik op het tabblad **Configuratie profielen**. Dit toont alle het profileren sondes beschikbaar aan gebruik op ISE. Schakel de **RADIUS-sonde in** en klik op **Opslaan**.

Deployment Nodes List > iselab

Edit Node

General Settings | Profiling Configuration

> NETFLOW

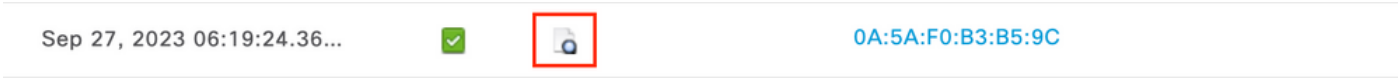
> DHCP

> DHCPSPAN

> HTTP

Opmerking: CoA-pakket heeft altijd een leeg identiteitsveld, maar endpoint-id is hetzelfde als in het eerste verificatiepakket.

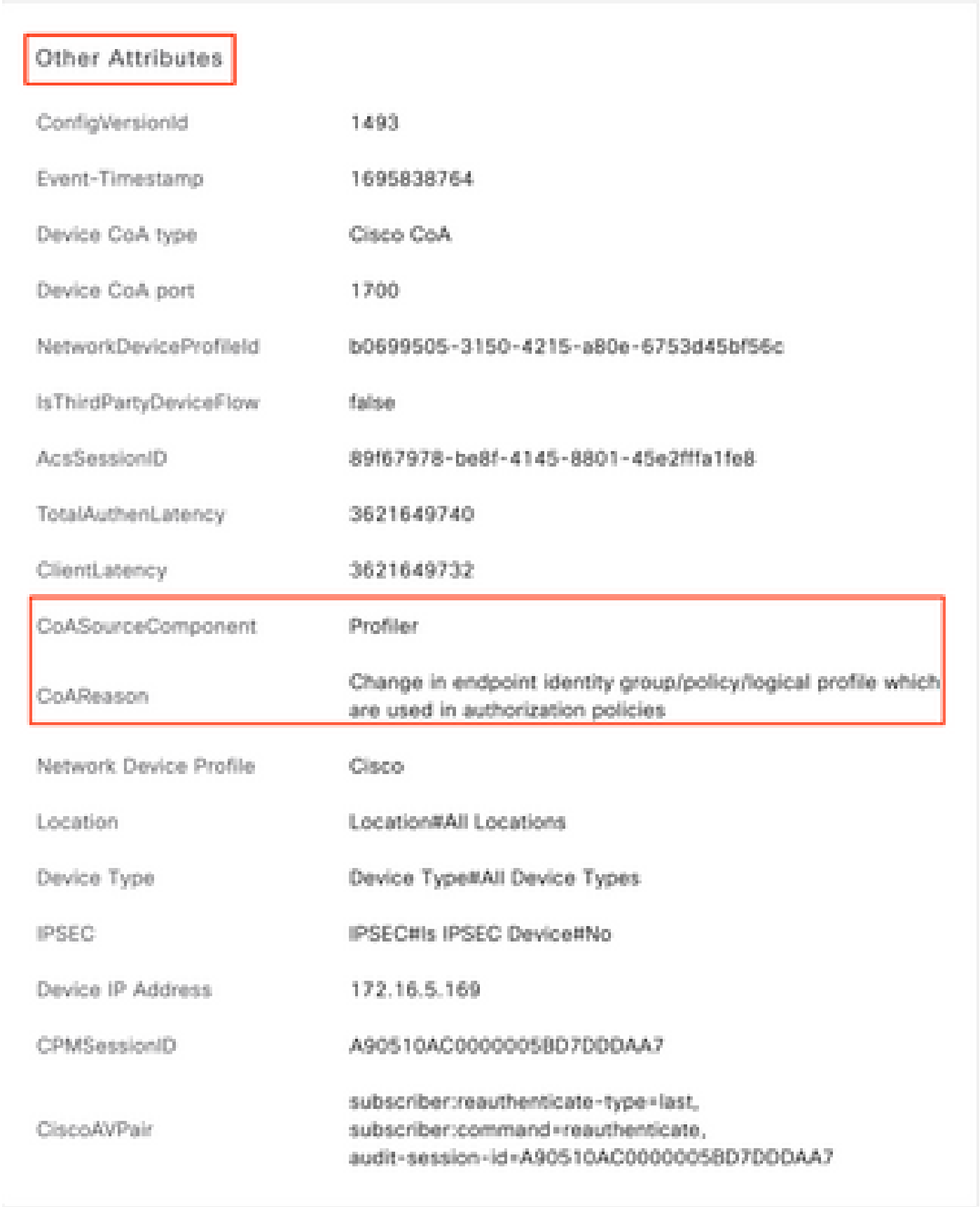
Klik op het **pictogram** in de kolom **Details** in het veld Wijzigen van autorisatie.



Toegang tot CoA-pakketgegevens

De CoA gedetailleerde informatie wordt weergegeven in een nieuwe browser tabblad. Blader naar beneden naar de sectie **Andere kenmerken**.

CoA-broncomponent wordt weergegeven als profiler. CoA Reason wordt weergegeven als wijziging in endpointidentiteitsgroep/beleid/logisch profiel die worden gebruikt in het autorisatiebeleid.

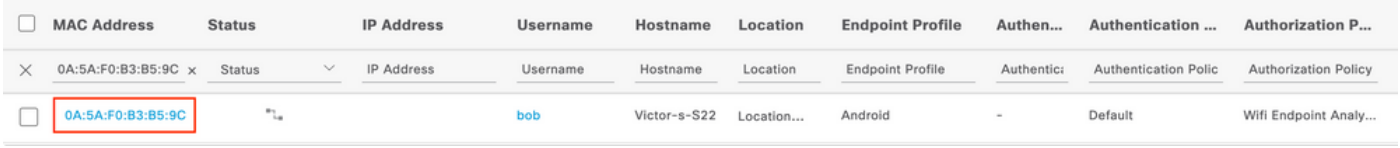


Other Attributes	
ConfigVersionId	1493
Event-Timestamp	1695838764
Device CoA type	Cisco CoA
Device CoA port	1700
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	89f67978-be8f-4145-8801-45e2fffa1fe8
TotalAuthenLatency	3621649740
ClientLatency	3621649732
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-triggercomponent en reden

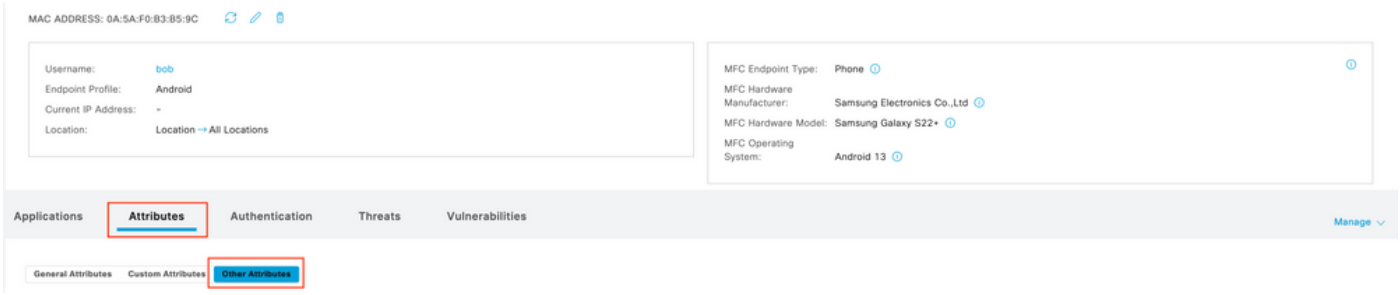
Navigeer naar **Context Visibility > Endpoints > Verificatie** tabblad. Gebruik in dit tabblad de filters om het testendpoint te vinden.

Klik op het **MAC-adres** van het **eindpunt** om toegang te krijgen tot de **endpointkenmerken**.



Endpoint op zichtbaarheid context

Deze actie geeft alle informatie weer die ISE over dit eindpunt opslaat. Klik op **de** sectie **Kenmerken** en selecteer vervolgens **Andere kenmerken**.



Endpoint andere selectie van kenmerken op zichtbaarheid context

Scroll naar beneden tot je de attributen van het **woordenboek WiFi_Device_Analytics** vindt. De plaatsbepaling van deze eigenschappen op deze sectie betekent dat ISE hen met succes door de pakketten van de Boekhouding ontving en voor Endpoint Classificatie kan worden gebruikt.

WiFi-analysekenmerken op contextzichtbaarheid

Hier zijn voorbeelden van Windows 10- en iPhone-kenmerken:

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

Voorbeeld van Windows 10 Endpoint

DEVICE_INFO_DEVICE_FORM	0
DEVICE_INFO_MODEL_NUM	IPHONE 11 PRO
DEVICE_INFO_OS_VERSION	IOS 16.4
DEVICE_INFO_VENDOR_TYPE	1

AttributesVoorbeeld van iPhone Endpoint Attributes

Problemen oplossen

Stap 1. Boekhoudpakketten bereiken ISE

Zorg er bij WLC CLI voor dat **DOT11 TLV-accounting, DHCP TLV-caching** en **HTTP TLV-caching** zijn ingeschakeld op de configuraties van beleidsprofielen.

<#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

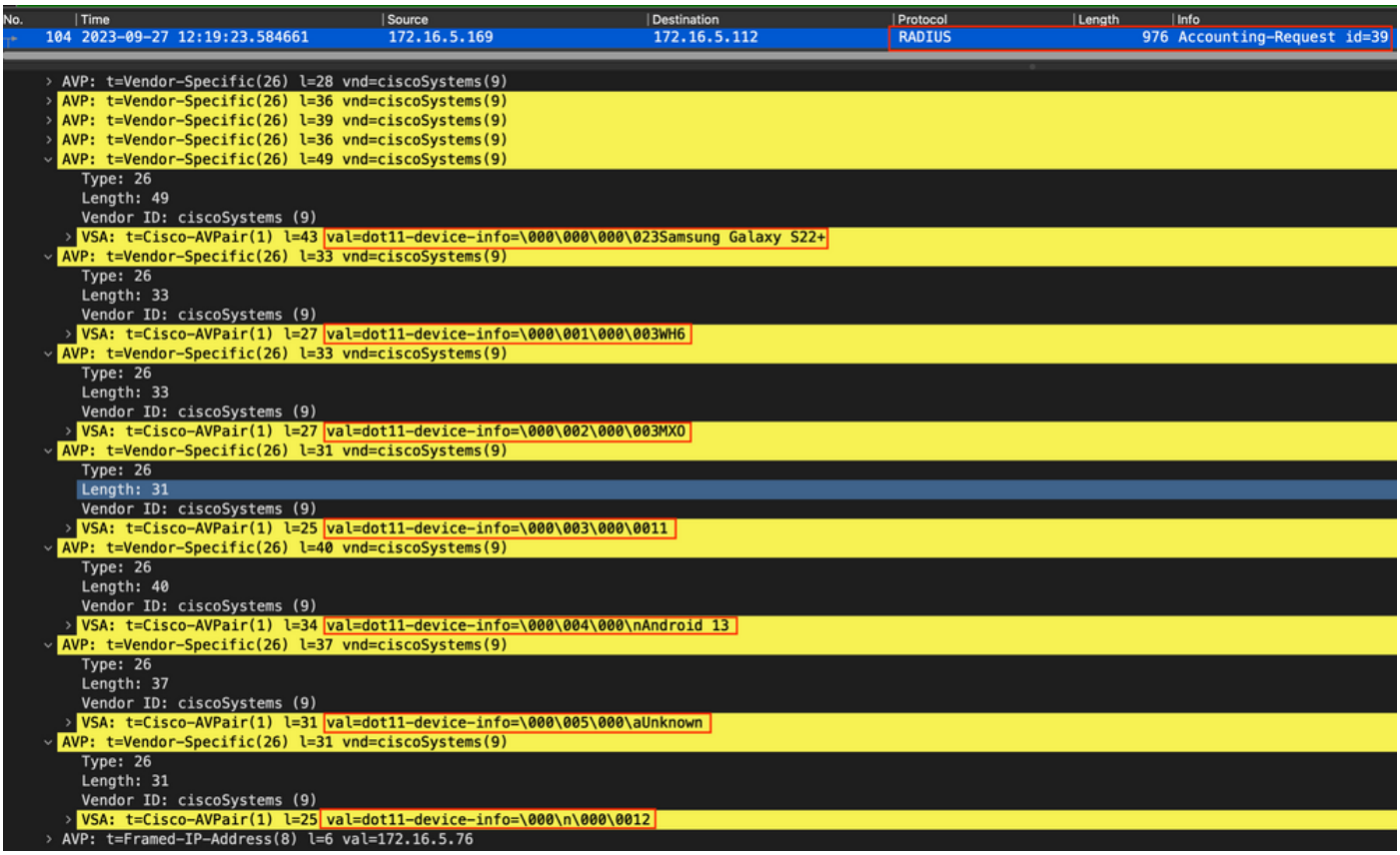
 no shutdown

Verzamel **pakketopnamen** op WLC- of ISE-eindpunten terwijl u een eindpunt aansluit. U kunt elk bekend pakketanalyseprogramma gebruiken, zoals Wireshark, om de verzamelde bestanden te analyseren.

Filter op RADIUS-accounting pakketten en door Calling Station ID (testend endpoint MAC Address). Dit filter kan bijvoorbeeld worden gebruikt:

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

Nadat u de locatie hebt bepaald, vouwt u de velden **Cisco-AVPair uit** om de **WiFi-analysegegevens** in het accounting pakket te vinden.



Endpoint TLV-kenmerken in een accounting pakket

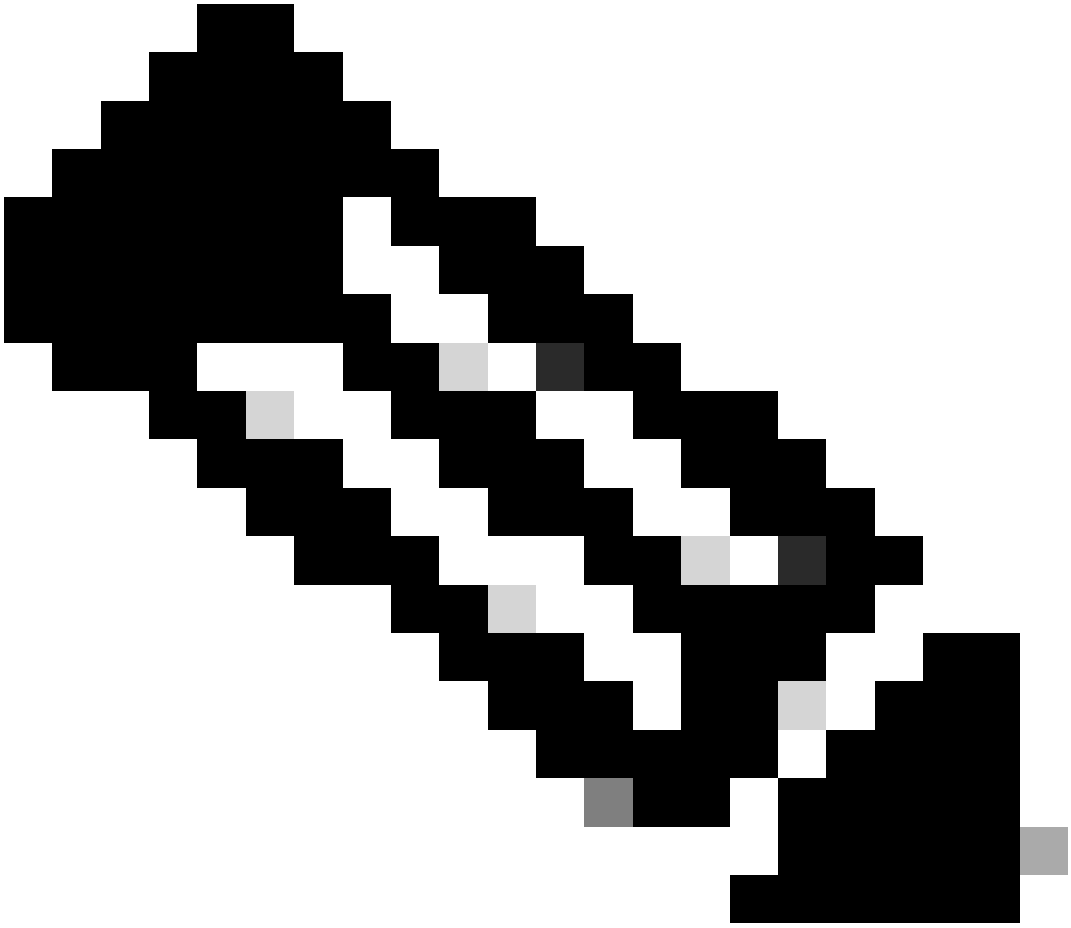
Stap 2. ISE Parseert het accounting pakket met de endpointkenmerken

Op ISE-end kunnen deze componenten op DEBUG-niveau worden ingesteld om ervoor te zorgen dat RADIUS-accounting pakketten die tegen dan WLC worden verzonden, ISE bereiken en correct worden verwerkt.

U kunt vervolgens **ISE-ondersteuningsbundel** verzamelen om de logbestanden te verzamelen. Raadpleeg het gedeelte **Verwante informatie** voor meer informatie over het verzamelen van ondersteuningsbundels.

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

Te debuggen componenten voor probleemoplossing



Opmerking: componenten zijn alleen ingeschakeld om het DEBUG-niveau te bereiken op het PSN dat de eindpunten verifieert.

Op iseLocalStore.log wordt het bericht Accounting-Start geregistreerd zonder dat een component op DEBUG-niveau moet worden ingeschakeld. Hier moet ISE het inkomende accounting pakket zien dat de WiFi Analytics kenmerken bevat.

<#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,

Op prt-server.log parseert ISE het ontvangen pakketanalysebericht, inclusief de WiFi Analytics-kenmerken. Gebruik de velden **CallingStationID** en **CPMSessionID** om ervoor te zorgen dat de juiste sessie en het juiste eindpunt worden bijgehouden.

<#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

Stap 3. Endpoint Attributes worden bijgewerkt en Endpoint wordt geclassificeerd

Dit syslog bericht wordt dan gedeeld met de profiler component. Profiler.log ontvangt het geparste syslog bericht en haalt de endpointkenmerken uit.

<#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,

De informatie over endpointkenmerken wordt bijgewerkt.

<#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

De attributenupdate leidt tot een nieuwe endpoint profiling gebeurtenis. Profileringsbeleid wordt opnieuw geëvalueerd en er wordt een nieuw profiel toegewezen.

<#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

Stap 4. CoA en opnieuw authenticeren

ISE moet een CoA verzenden voor de endpointsessie omdat er een wijziging is opgetreden in de eigenschappen van de WiFi-apparaatanalyse.

<#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-

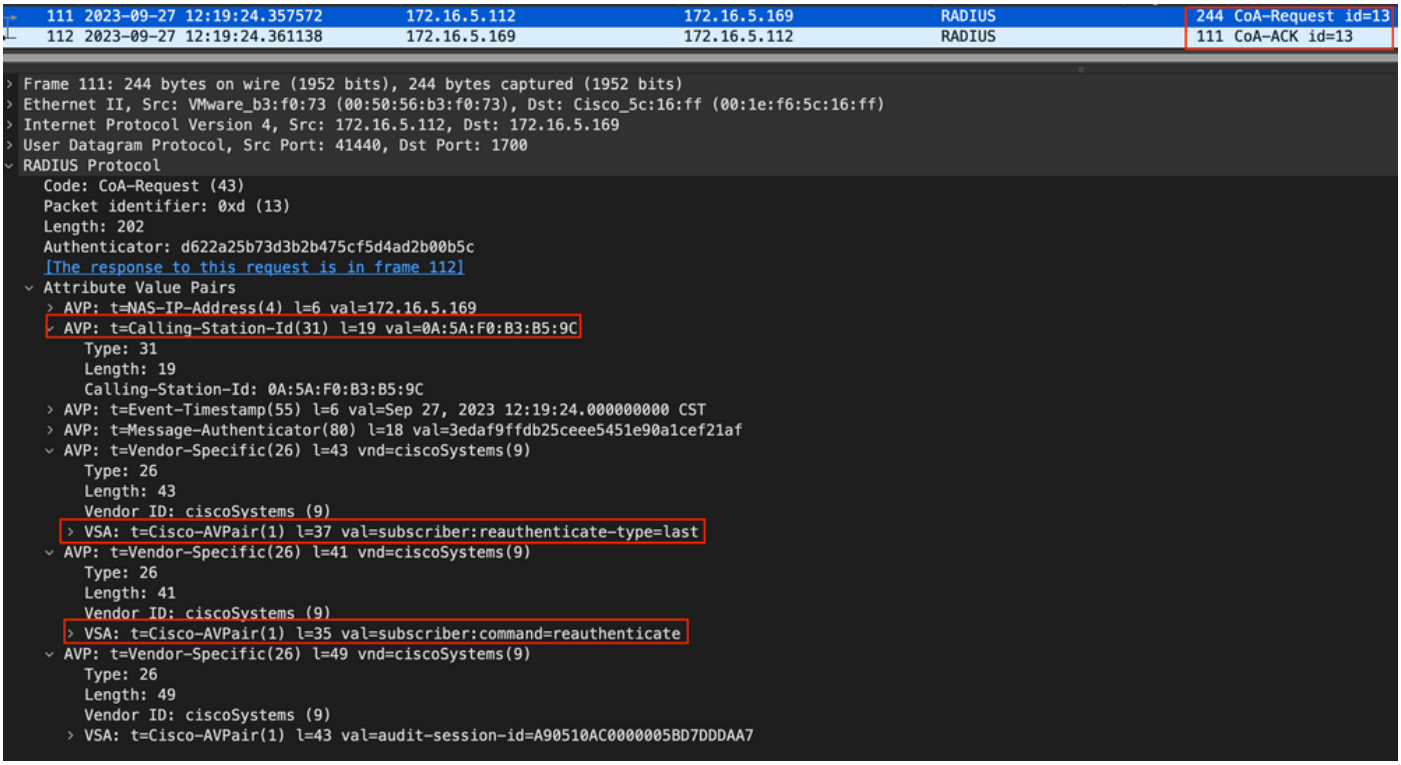
ConditionalCoAEvent with Endpoint Details : EndPoint[id=62caa550-5d62-11ee-bf1f-b6bb1580ab0d,name=] MAC:

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

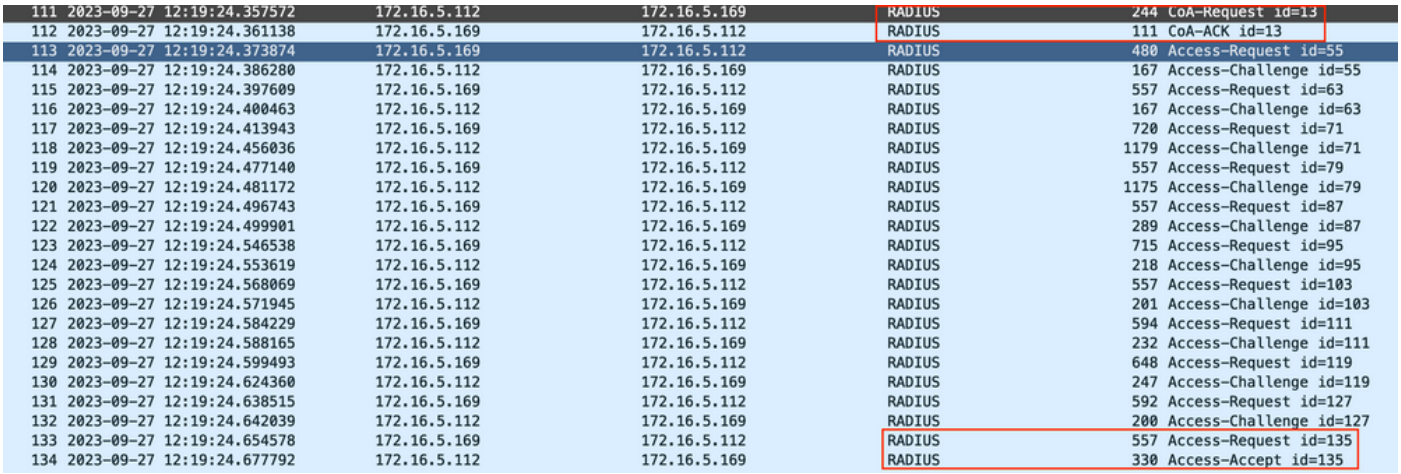
Attribute:DEVICE_INFO_COUNTRY_CODE value:Unknown Attribute:DEVICE_INFO_DEVICE_FORM value:PHONE Attribute

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

Packet Capture helpt ervoor te zorgen dat ISE de CoA naar de WLC stuurt. Het toont ook aan dat een nieuw access-request pakket wordt ontvangen na verwerking van de CoA.



Radius CoA-pakket na endpointprofilering



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 en nieuwe access-aanvraag na endpointprofilering

Gerelateerde informatie

- Beheerdershandleiding voor Cisco Identity Services Engine, release 3.3
- Releaseopmerkingen voor Cisco Identity Services Engine, release 3.3
- Verzamel ondersteuningsbundel op de Identity Services Engine

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.