Entender a análise de WiFi para classificação de endpoint no ISE 3.3

Contents

Introdução

Este documento descreve como a análise de WiFi para classificação de endpoint funciona. Ele também descreve como configurá-lo, verificá-lo e solucionar seus problemas.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- 9800 Configuração de Wireless LAN Controllers (WLC)
- Configuração do Identity Services Engine (ISE)
- Autenticação RADIUS. Fluxo e terminologia de pacotes AAA (Authorization and Accounting)

Este documento pressupõe que já existe uma WLAN em funcionamento autenticando clientes

usando ISE como servidor RADIUS.

Para que esse recurso funcione, é necessário ter pelo menos:

- 9800 WLC Cisco IOS® XE Dublin 17.10.1
- Identifique o Services Engine v3.3.
- Access points 802.11ac Wave2 ou 802.11ax (Wi-Fi 6/6E)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

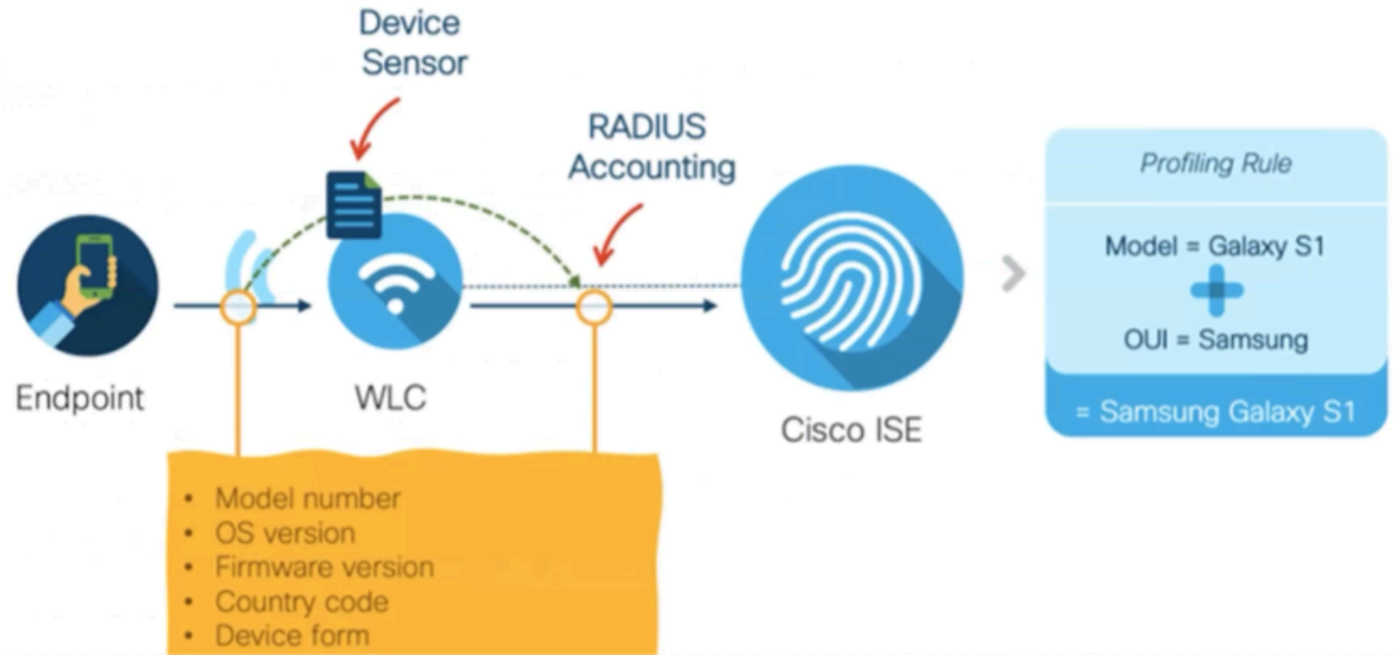
Por meio do WiFi Device Analytics, a WLC Cisco 9800 pode aprender atributos, como o número do modelo e a versão do SO, de um conjunto de endpoints conectados a esse dispositivo e compartilhá-lo com o ISE. O ISE pode usar essas informações para fins de classificação de endpoint, também conhecida como criação de perfil.

Atualmente, o WiFi Analytics é compatível com estes fornecedores:

- Maçã
- Intel
- Samsung

A WLC compartilha as informações de atributo com o servidor ISE usando pacotes de contabilização RADIUS.

Fluxo de dados de análise

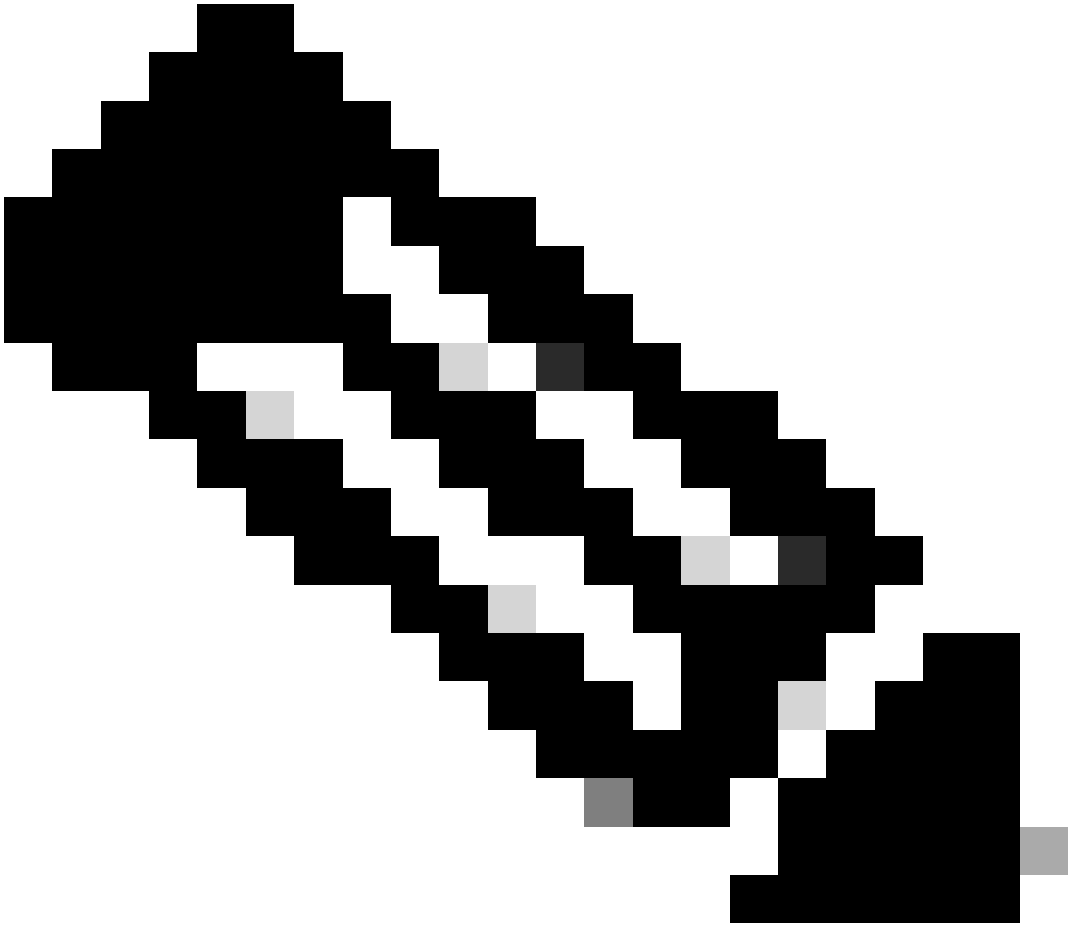


WiFi

É importante lembrar que os pacotes RADIUS Accounting em um fluxo AAA RADIUS são enviados somente depois que o servidor RADIUS envia um pacote RADIUS Access-Accept como resposta à tentativa de autenticação de ponto final. Em outras palavras, a WLC compartilha as informações de atributo do ponto final somente depois que uma sessão RADIUS para esse ponto final é estabelecida entre o servidor RADIUS (ISE) e o dispositivo de acesso à rede (WLC).

Estes são todos os atributos que o ISE pode usar para classificação e autorização de endpoints:

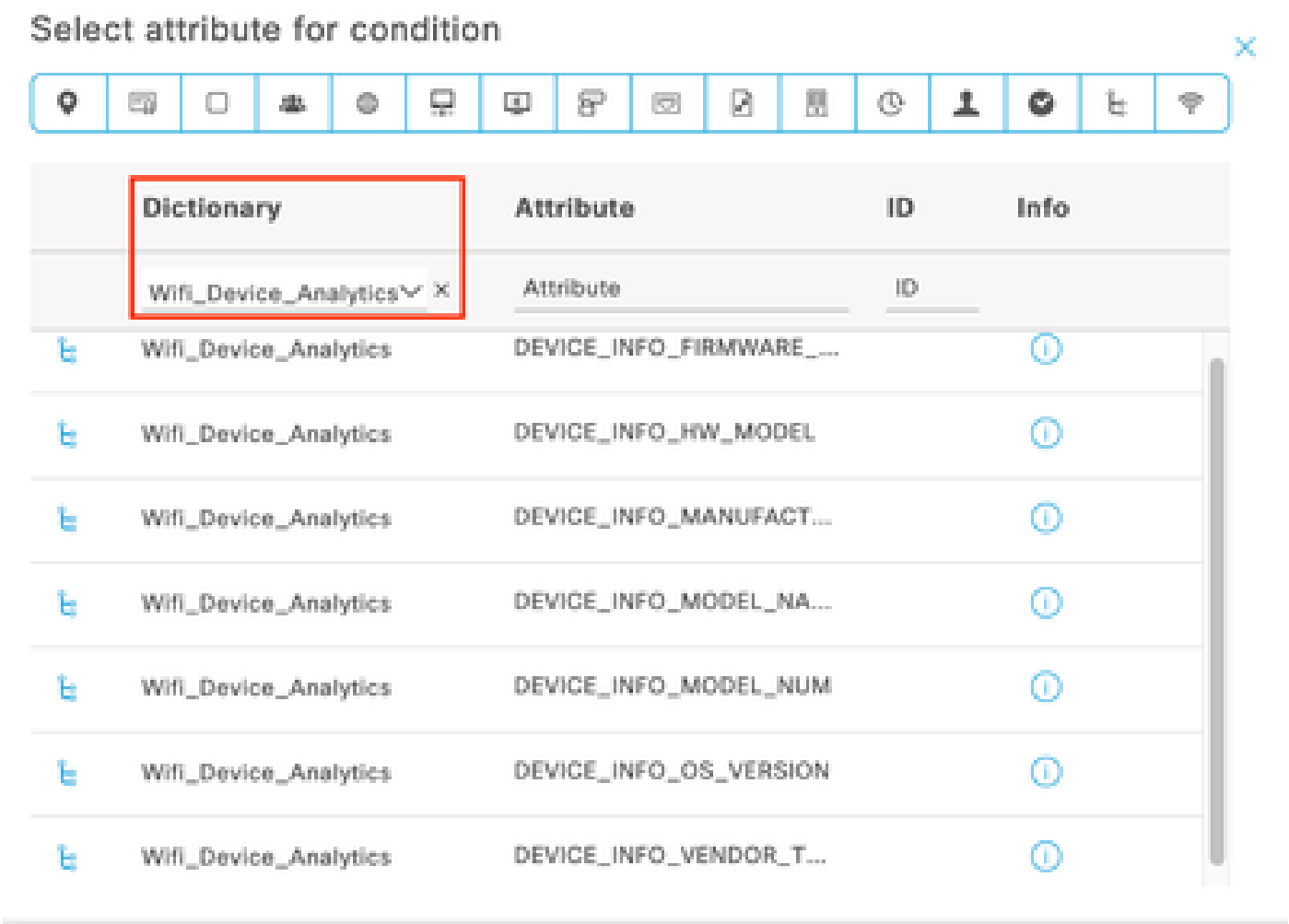
- DEVICE_INFO_FIRMWARE_VERSION
- DEVICE_INFO_HW_MODEL
- DEVICE_INFO_MANUFATURER_MODEL
- DEVICE_INFO_MODEL_NAME
- DEVICE_INFO_MODEL_NUM
- DEVICE_INFO_OS_VERSION
- DEVICE_INFO_VENDOR_TYPE



Observação: a WLC pode enviar mais atributos dependendo do tipo de ponto final que se conecta, mas somente os listados podem ser usados para a criação de Diretivas de Autorização no ISE.

Depois que o ISE recebe o pacote de contabilização, ele pode processar e consumir esses dados de análise dentro dele e usá-lo para reatribuir um perfil de endpoint/grupo de identidade.

Os atributos do WiFi Endpoint Analytics estão listados no dicionário WiFi_Device_Analytics. Os administradores de rede podem incluir esses atributos nas políticas e condições de autorização de endpoint.



Dicionário de Análise de Dispositivo WiFi

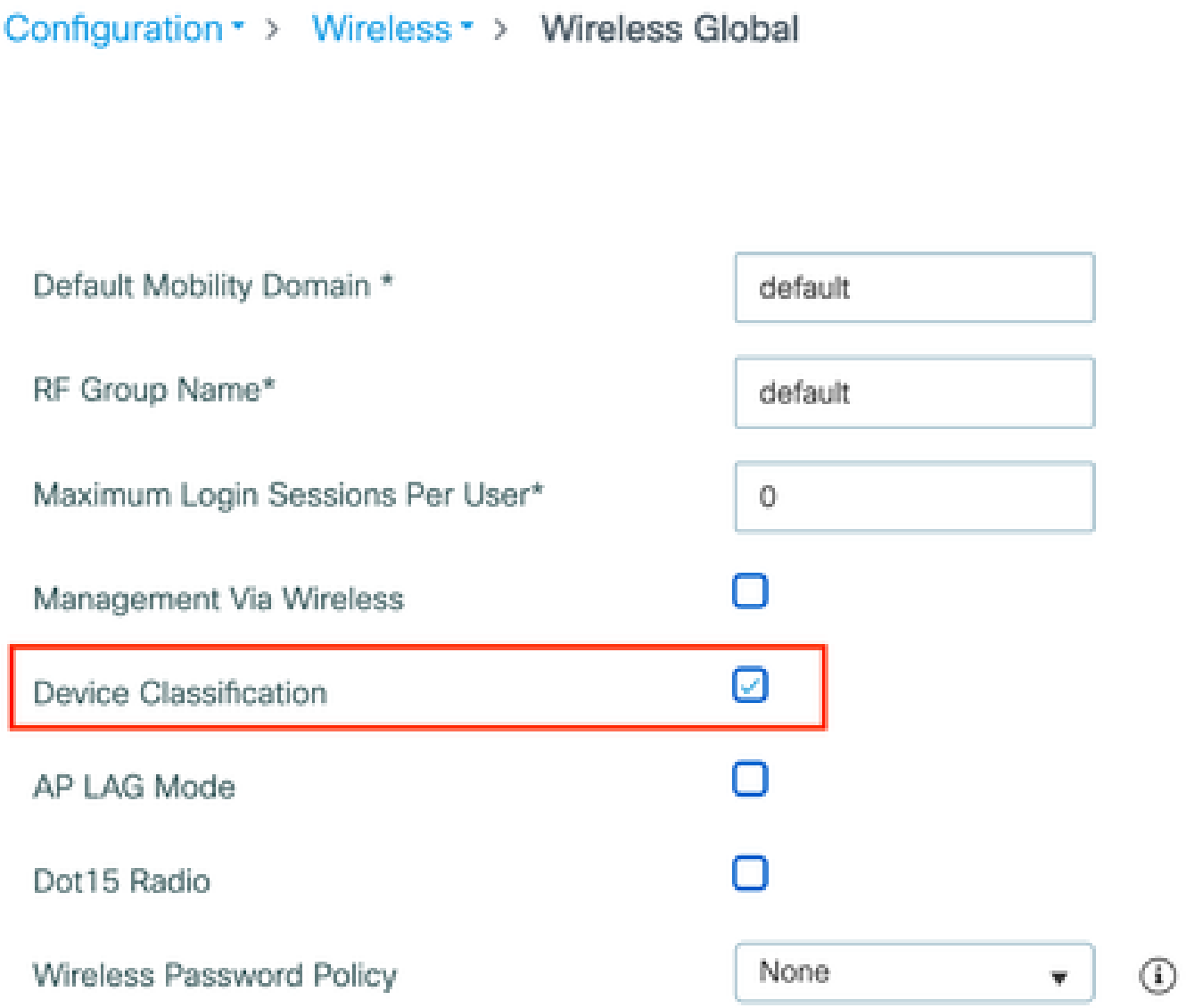
Se ocorrerem alterações nos valores de atributo atuais que o ISE armazena para o endpoint, o ISE iniciará uma Alteração de autorização (CoA), permitindo que o endpoint seja avaliado levando em consideração os atributos atualizados.

Configurar

Configurações no WLC

Etapa 1. Ativar globalmente o recurso de classificação de dispositivo

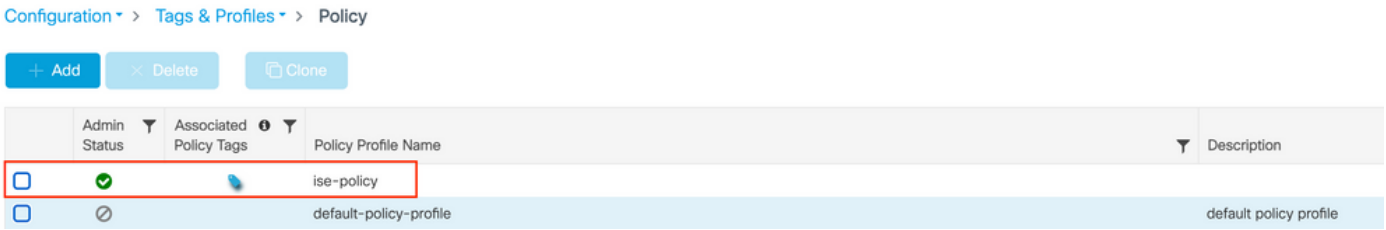
Navegue até Configuration > Wireless > Wireless Global e marque a caixa de seleção Device Classification.



Configuração da classificação do dispositivo

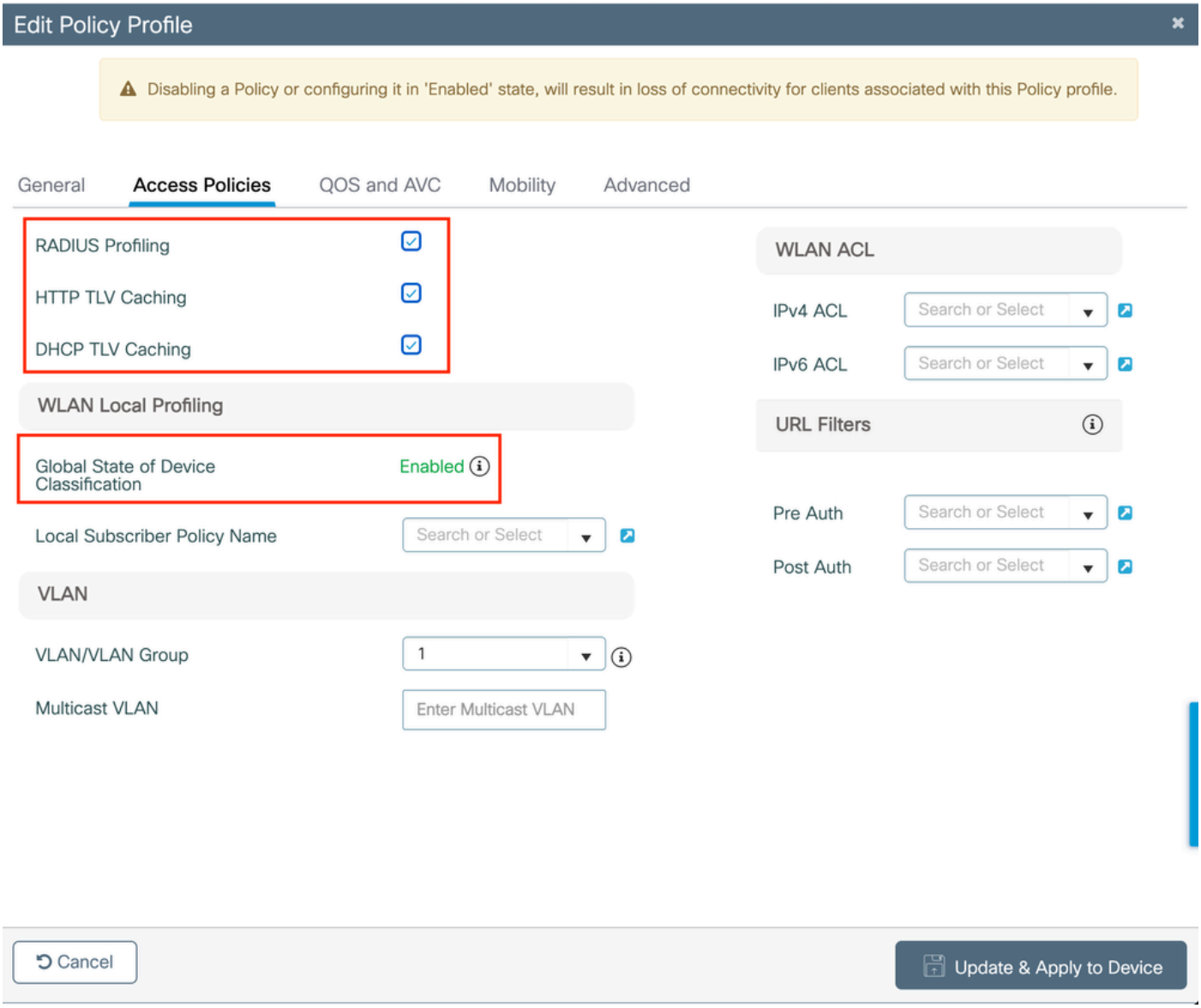
Etapa 2. Ativar cache TLV e criação de perfil RADIUS

Navegue para Configuration > Tags and Profiles > Policy e selecione o Policy Profile usado pela WLAN onde os clientes RADIUS estão se conectando.



Seleção de política sem fio

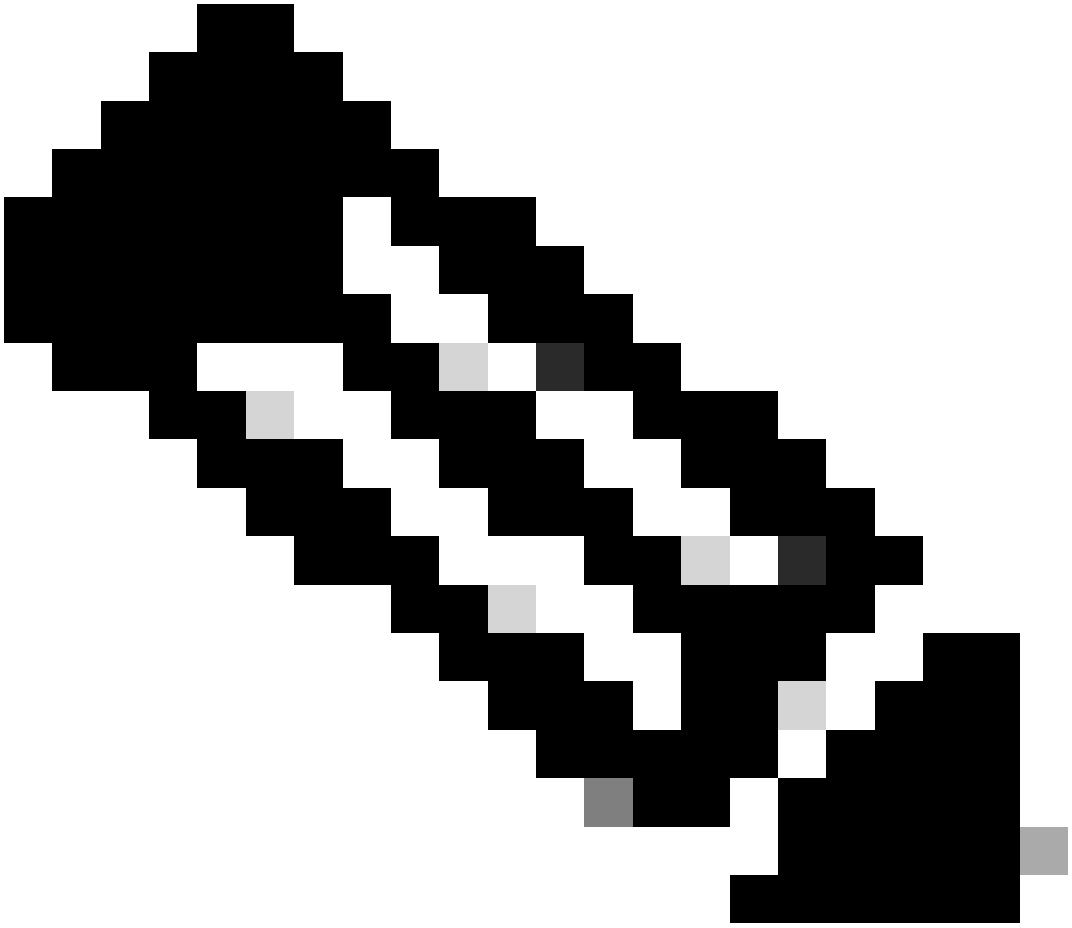
Clique em Access Policies e verifique as opções RADIUS Profiling, HTTP TLV Caching e DHCP TLV Caching. Devido à ação tomada na etapa anterior, o estado global da classificação do dispositivo agora aparece no status Ativado.



Configuração de criação de perfil e cache RADIUS

Faça login na CLI da WLC e habilite o dot11 TLV Accounting.

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

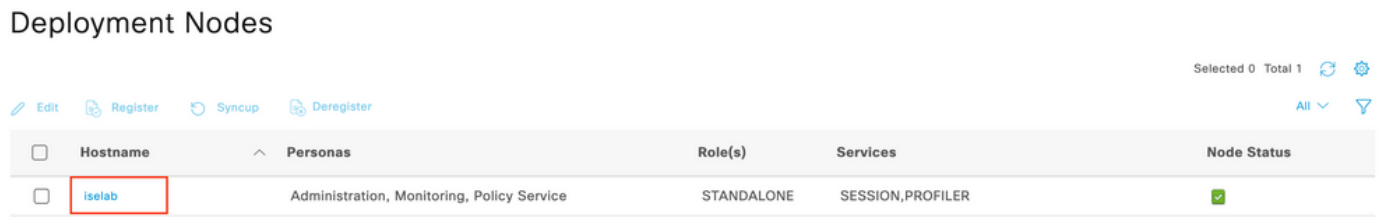


Observação: o perfil da diretiva sem fio deve ser desabilitado antes do uso deste comando. Esse comando está disponível apenas no Cisco IOS XE Dublin versão 17.10.1 e posterior.

Configurações no ISE

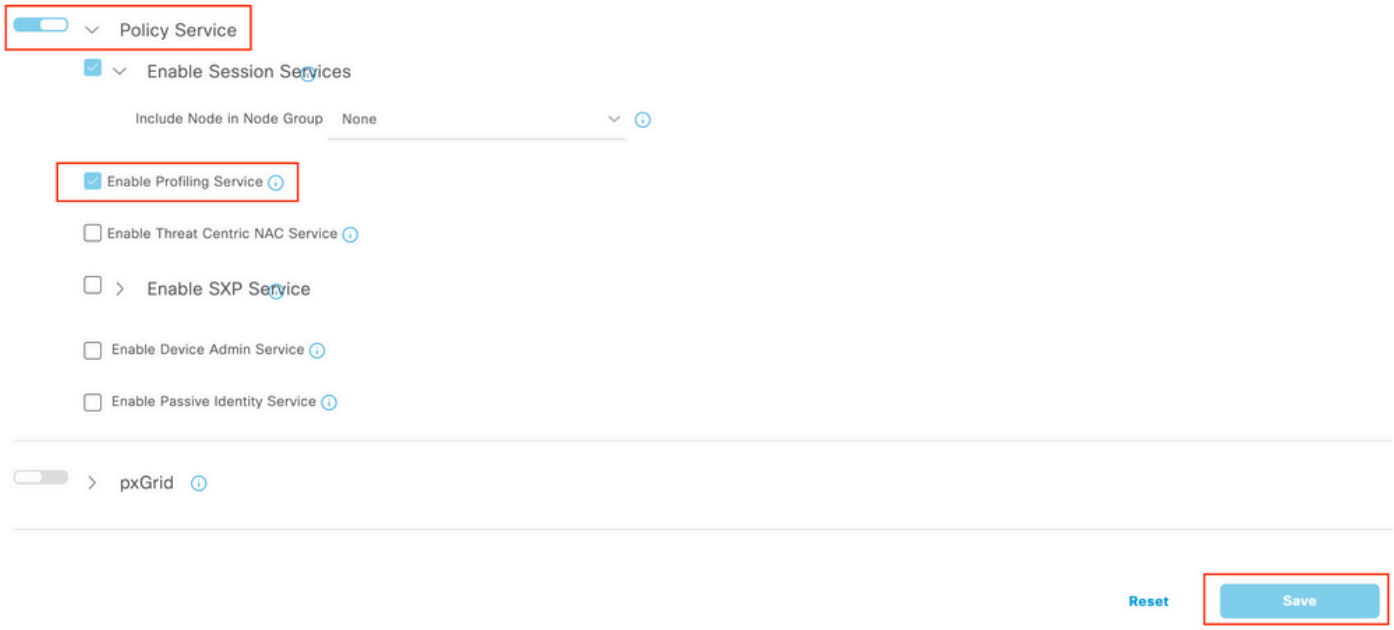
Etapa 1. Ative os serviços de criação de perfil nas PSNs na implantação

Navegue até **Administration > Deployment** e clique no nome do PSN.



Seleção de nó PSN do ISE

Role para baixo até a seção **Policy Service** e marque a caixa de seleção **Enable Profiling Service**. Clique no botão **Save**.



Configuração dos serviços do Profiler

Etapa 2. Ative a sonda de criação de perfil RADIUS na PSN do ISE

Role até a parte superior da página e clique na guia **Configuração de criação de perfil**. Isso exibe todas as sondas de criação de perfil disponíveis para uso no ISE. Habilite a **sonda RADIUS** e clique em **Salvar**.

Deployment Nodes List > iselab

Edit Node

General Settings | Profiling Configuration

> NETFLOW

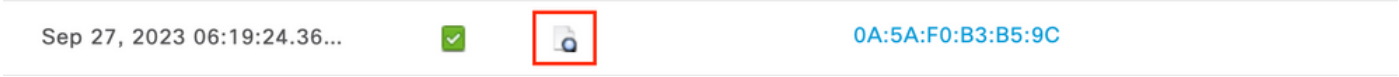
> DHCP

> DHCPSPAN

> HTTP

Observação: o pacote CoA sempre tem um campo de identidade vazio, mas o ID do ponto final é o mesmo do primeiro pacote de autenticação.

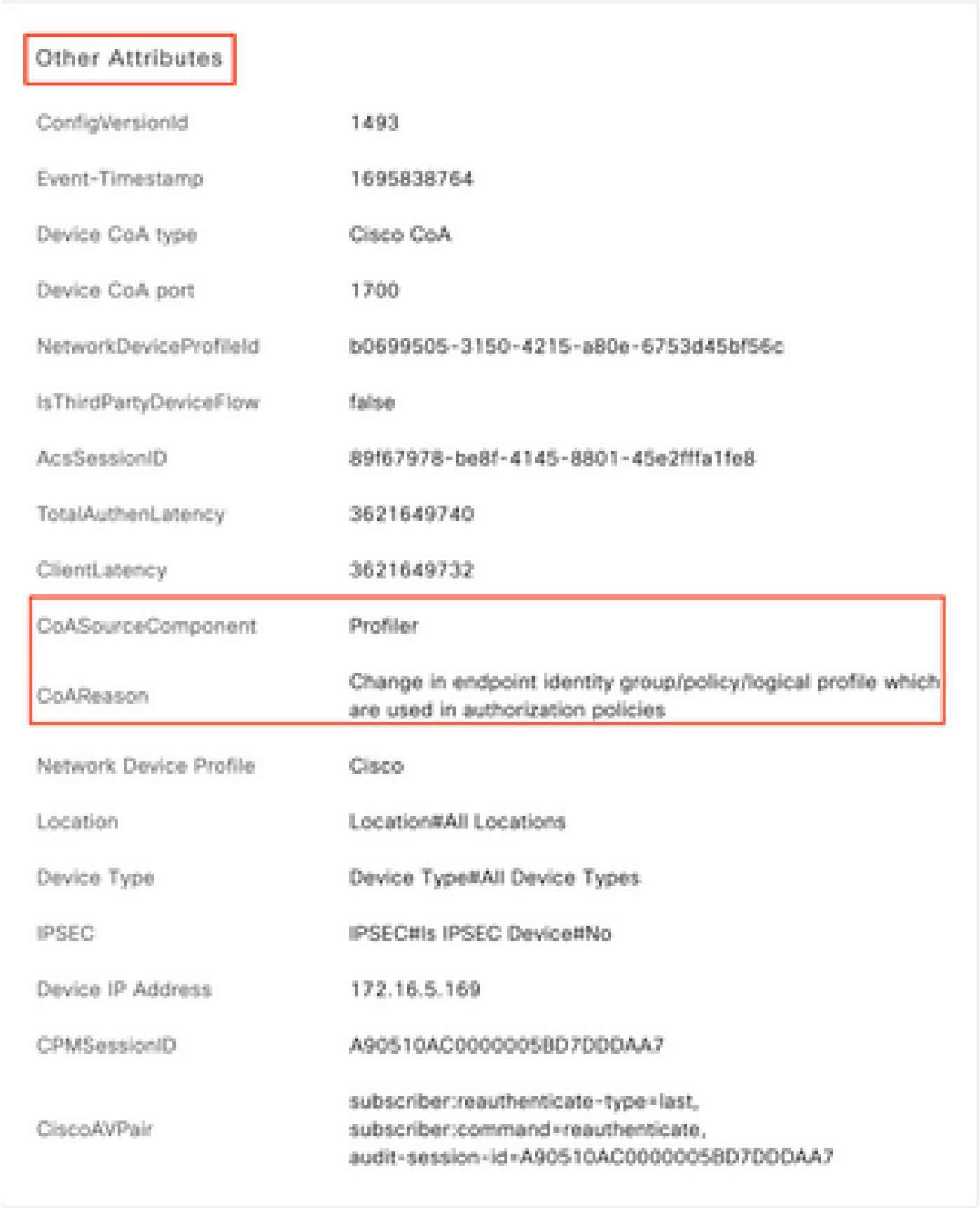
Clique no **ícone** localizado na coluna **Detalhes** no registro Alteração de autorização.



Acesso aos detalhes do pacote de CoA

As informações detalhadas do CoA são exibidas em uma nova guia do navegador. Role para baixo até a seção **Outros Atributos**.

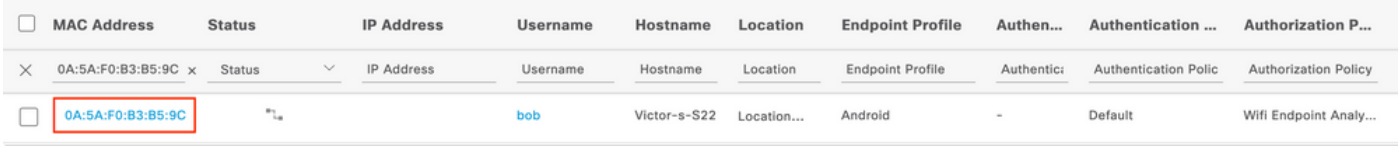
O componente de origem CoA é exibido como profiler. Razão da CoA é exibida como Alteração no grupo de identidade de ponto final/política/perfil lógico que são usados nas políticas de Autorização.



Componente de Disparo de CoA e Motivo

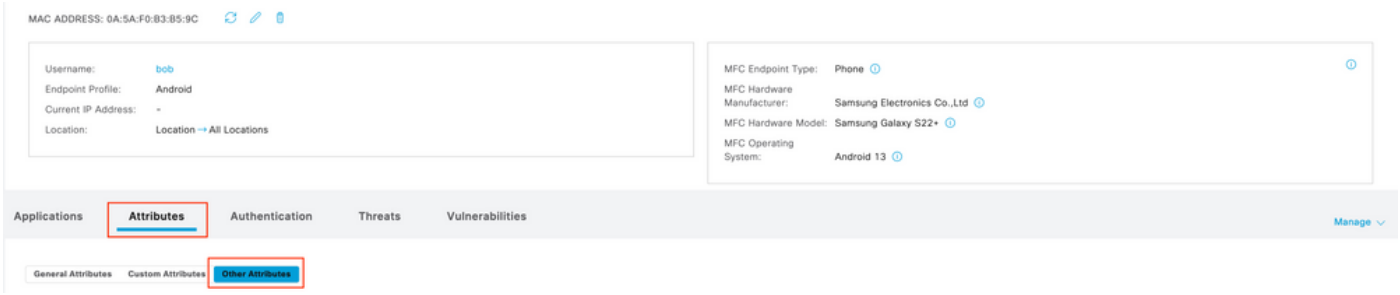
Navegue até a guia **Visibilidade de contexto > Pontos finais > Autenticação**. Nesta guia, use os filtros para localizar o ponto final de teste.

Clique no **Endereço MAC do ponto final** para acessar os **atributos do ponto final**.



Endpoint na visibilidade de contexto

Esta ação exibe todas as informações que o ISE está armazenando sobre este ponto final. Clique na seção **Atributos** e selecione **Outros Atributos**.



Seleção de Outros Atributos de Ponto Final na Visibilidade de Contexto

Role para baixo até encontrar os atributos do dicionário **WiFi_Device_Analytics**. Localizar esses atributos nesta seção significa que o ISE os recebeu com êxito através dos pacotes de contabilização e pode ser usado para classificação de endpoint.

Atributos do WiFi Analytics na visibilidade do contexto

Para sua referência, aqui estão exemplos de atributos do Windows 10 e do 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

Exemplo de

DEVICE_INFO_DEVICE_FORM	0
DEVICE_INFO_MODEL_NUM	IPHONE 11 PRO
DEVICE_INFO_OS_VERSION	IOS 16.4
DEVICE_INFO_VENDOR_TYPE	1

atributos de endpoint do Windows 10Exemplo de atributos de endpoint do iPhone

Troubleshooting

Etapa 1. Os pacotes de contabilização alcançam o ISE

Na CLI da WLC, certifique-se de que a **contabilidade de TLV DOT11, o cache de TLV DHCP** e o **cache de TLV HTTP** estejam habilitados nas configurações de perfil de política.

<#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

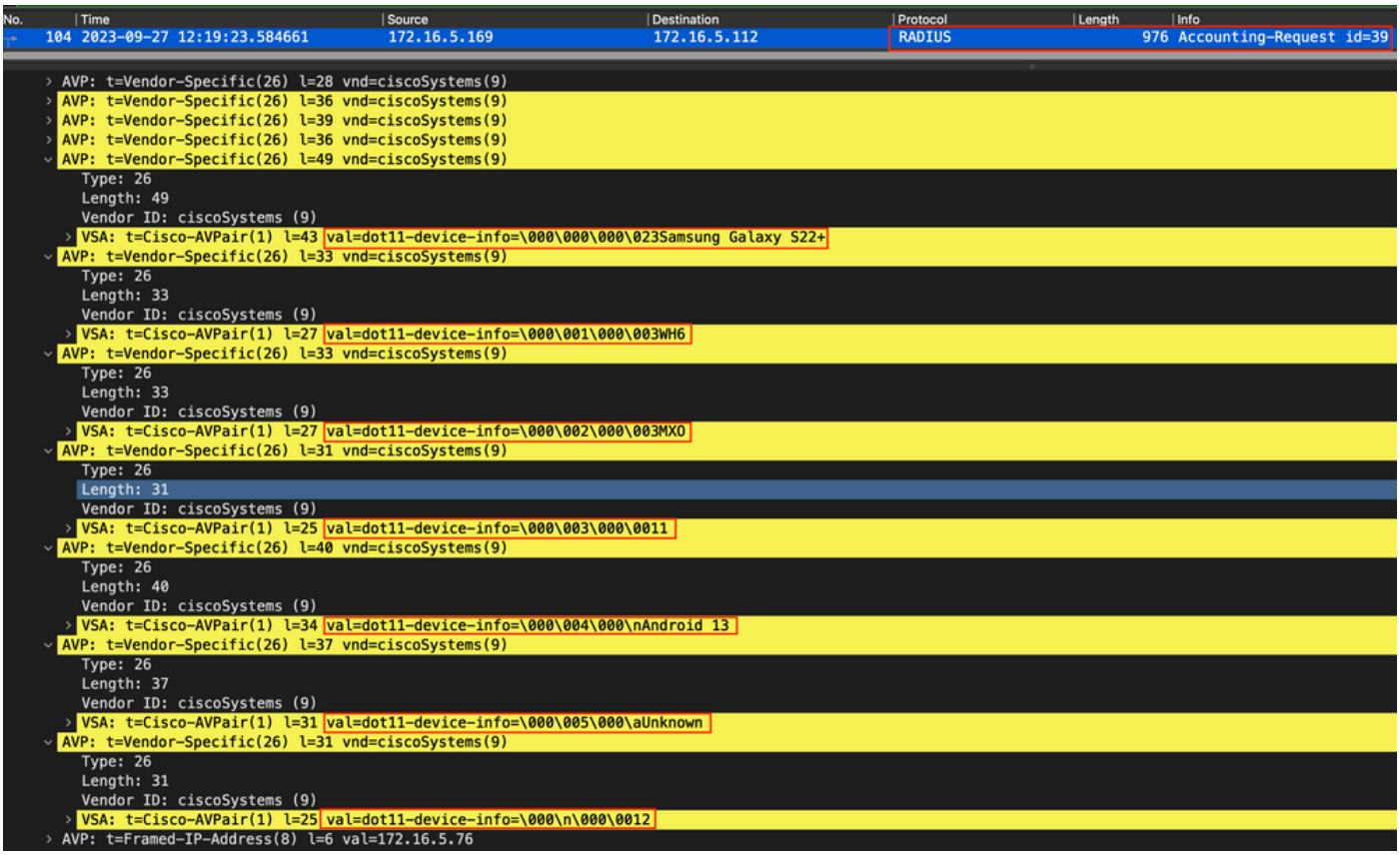
no shutdown

Colete **capturas de pacotes** nas extremidades da WLC ou do ISE ao conectar um endpoint. Você pode usar qualquer ferramenta de análise de pacotes conhecida, como o Wireshark, para analisar os arquivos coletados.

Filtrar por pacotes de contabilização RADIUS e por ID de estação de chamada (testando o endereço MAC do ponto final). Por exemplo, este filtro pode ser usado:

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

Depois de localizado, expanda os campos **Cisco-AVPair** para localizar os **Dados do WiFi Analytics** no pacote Accounting.



Atributos TLV de Ponto Final em um Pacote de Contabilização

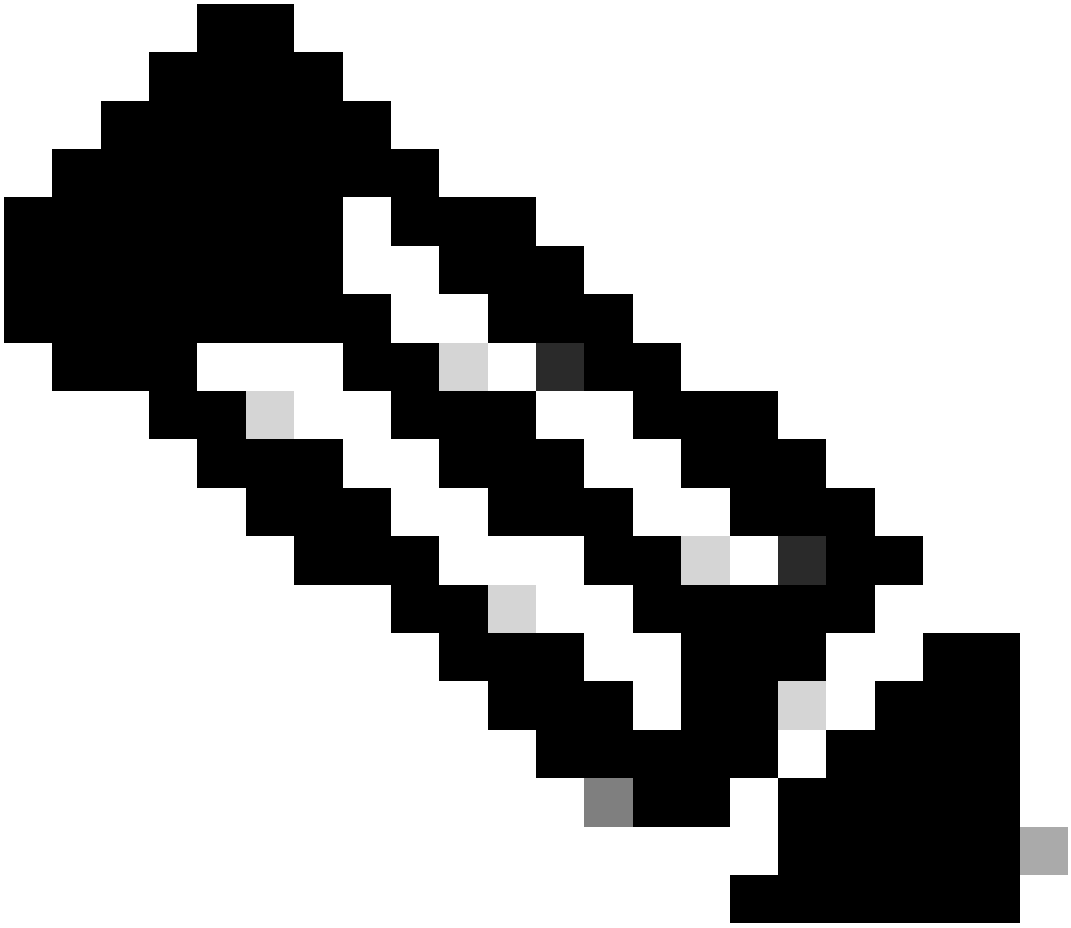
Etapa 2. O ISE analisa o pacote de contabilização com os atributos do ponto final

Na extremidade ISE, esses componentes podem ser definidos no nível DEBUG para garantir que os pacotes de contabilização RADIUS enviados pela WLC cheguem ao ISE e sejam processados corretamente.

Você pode coletar o **pacote de suporte do ISE** para reunir os arquivos de log. Para obter mais informações sobre como coletar o pacote de suporte, consulte a seção **Informações relacionadas**.

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 a serem depurados para solução de problemas



Observação: os componentes são ativados para o nível DEBUG somente no PSN que autentica os pontos finais.

Em iseLocalStore.log, a mensagem Accounting-Start é registrada sem a necessidade de habilitar qualquer componente para o nível DEBUG. Aqui, o ISE deve ver o pacote de relatório de entrada que contém os atributos do 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,

Em prt-server.log, o ISE analisa a mensagem de syslog do pacote de contabilização recebido, incluindo os atributos do WiFi Analytics. Use os campos **CallingStationID** e **CPMSessionID** para garantir que a sessão e o ponto de extremidade corretos sejam rastreados.

<#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

Etapa 3. Os atributos de endpoint são atualizados e o endpoint é classificado

Essa mensagem de syslog é compartilhada com o componente profiler. Profiler.log recebe a mensagem de syslog analisada e extrai os atributos de ponto 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,

As informações de atributo do ponto de extremidade são atualizadas.

<#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

A atualização de atributo aciona um novo evento de criação de perfil de ponto de extremidade. As políticas de criação de perfil são avaliadas novamente e um novo perfil é atribuído.

<#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

Etapa 4. CoA e reautenticação

O ISE deve enviar um CoA para a sessão de endpoint quando ocorre uma alteração nos atributos do WiFi Device Analytics.

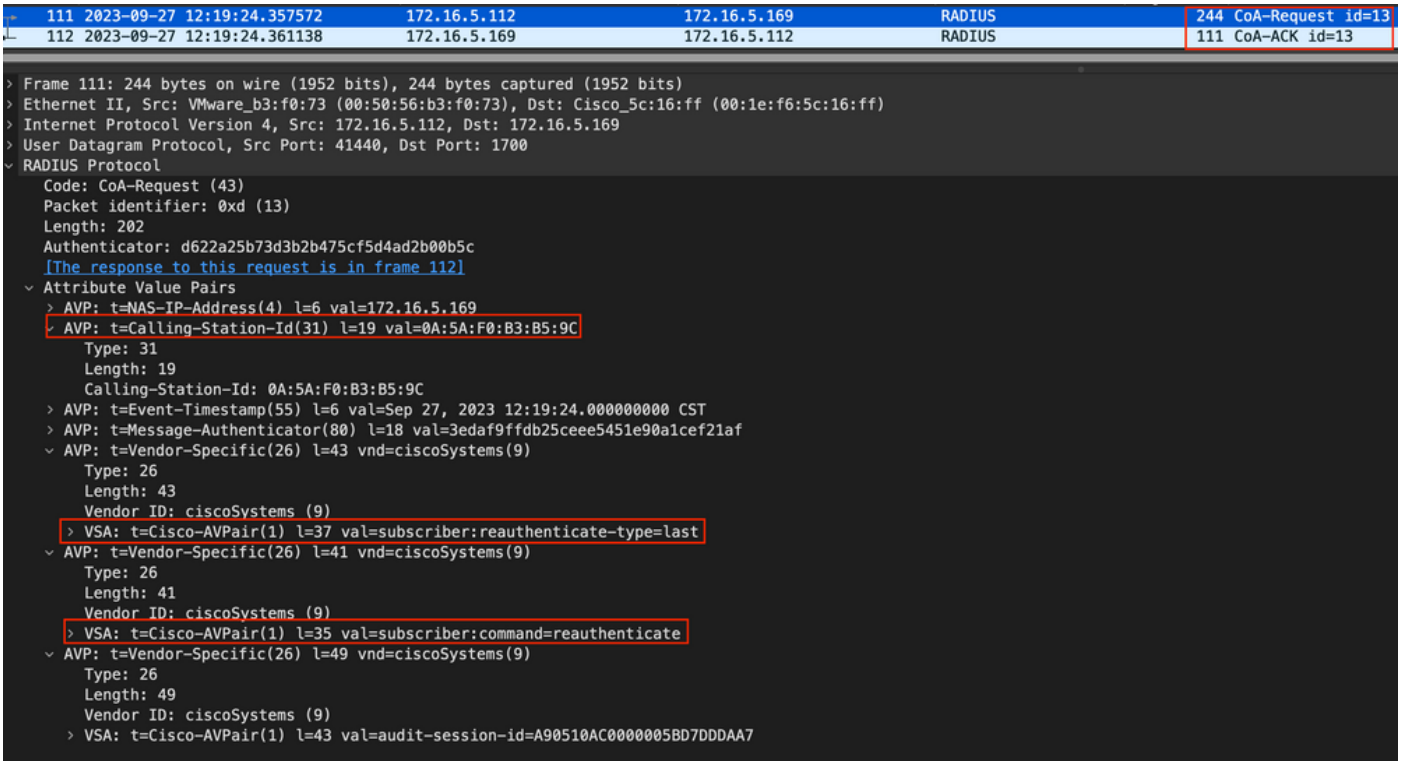
<#root>

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

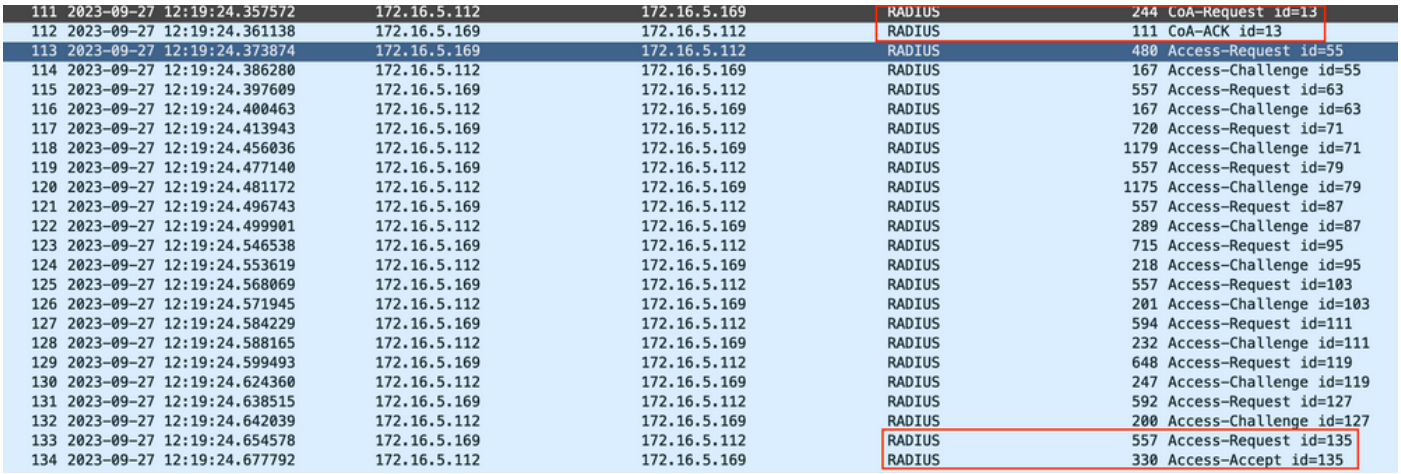
DEBUG [pool-533-thread-35]

```
[[]] 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
```

A captura de pacotes ajuda a garantir que o ISE envie o CoA para a WLC. Ele também mostra que um novo pacote de solicitação de acesso é recebido após o processamento do CoA.



Pacote CoA Radius após criação de perfil de endpoint



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 e nova solicitação de acesso após criação de perfil de endpoint

Informações Relacionadas

- Guia do Administrador do Cisco Identity Services Engine, Versão 3.3
- Notas de versão do Cisco Identity Services Engine, versão 3.3
- Coletar pacote de suporte no Identity Services Engine

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.