

Demonstreren van clientprofielen op draadloze LAN-controller 9800

Inhoud

[Inleiding](#)

[Gebruikte componenten](#)

[Profileringsproces](#)

[MAC-adresprofielen](#)

[Lokaal beheerde MAC-adressen problemen](#)

[DHCP-profielen](#)

[HTTP-profielen](#)

[RADIUS-profilering](#)

[DHCP-RADIUS-profilering](#)

[HTTP-RADIUS-profilering](#)

[Profilering op 9800 WLC configureren](#)

[Lokale profielconfiguratie](#)

[Configuratie RADIUS-profielen](#)

[Gebruikscases profileren](#)

[Lokaal beleid toepassen op basis van lokale profielclassificatie](#)

[Radius-profilering voor geavanceerde beleidssets in Cisco ISE](#)

[Profilering in FlexConnect-implementaties](#)

[Centrale verificatie, lokale switching](#)

[Lokale verificatie en lokale switching](#)

[Probleemoplossing](#)

[Radioactieve sporen](#)

[PacketCapture](#)

Inleiding

Dit document beschrijft hoe apparaatclassificatie en profilering werken met Cisco Catalyst 9800 draadloze LAN-controllers.

Gebruikte componenten

- 9800 CL WLC met 17.2.1 afbeelding
- Aironet 1815i access point
- Draadloze Windows 10 Pro-client
- Cisco ISE-lijnkaart 2.7

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.

Profileringsproces

Dit artikel biedt een diepgaande analyse van de manier waarop apparaatclassificatie en profilering werkt met Cisco Catalyst 9800 draadloze LAN-controllers, beschrijft mogelijke gebruikscases, configuratievoorbeelden en stappen die nodig zijn om problemen op te lossen.

Apparaatprofilering is een functie die een manier biedt om aanvullende informatie te vinden over een draadloze client die zich heeft aangesloten bij de draadloze infrastructuur.

Zodra apparaat het profileren wordt uitgevoerd, kan het worden gebruikt om verschillend lokaal beleid toe te passen of specifieke RADIUS serverregels aan te passen.

Cisco 9800 WLC's zijn in staat om drie (3) typen apparaatprofilering uit te voeren:

1. MAC-adres OUI
2. DHCP
3. HTTP

MAC-adresprofielen

Het adres van MAC is een uniek herkenningsteken van elke draadloze (en getelegrafeerde) netwerkinterface. Het is een 48-bits getal dat gewoonlijk in hexadecimaal formaat MM:MM:MM:SS:SS wordt afgeschreven.

De eerste 24 bits (of 3 octetten) staan bekend als OUI (Organizationally Unique Identifier) en geven een unieke identificatie van een verkoper of fabrikant.

Zij worden gekocht van en door IEEE toegewezen. Eén leverancier of fabrikant kan meerdere OUI's aanschaffen.

Voorbeeld:

00:0D:4B - owned by Roku, LLC

90:78:B2 - owned by Xiaomi Communications Co Ltd

Zodra een draadloze client is gekoppeld aan het access point, voert de WLC de OUI lookup uit om de fabrikant te bepalen.

In Flexconnect lokale switching implementaties, de AP nog steeds relevante client informatie doorgeeft aan de WLC (zoals DHCP-pakketten en client mac-adres).

Profiling alleen op basis van OUI is uiterst beperkt en het is mogelijk om apparaat te classificeren als een specifiek merk, maar het is niet in staat om te onderscheiden tussen een laptop en smartphone.

Lokaal beheerde MAC-adressen problemen

Wegens privacyoverwegingen, begonnen vele fabrikanten mac randomiseringseigenschappen in hun apparaten uit te voeren.

Lokaal beheerde MAC-adressen worden willekeurig gegenereerd en hebben een op één na minst belangrijk bit van het eerste octet van het adres ingesteld op 1.

Dit bit fungeert als een vlag die aankondigt dat het mac-adres eigenlijk een willekeurig gegenereerde is.

Er zijn vier mogelijke formaten van lokaal beheerde MAC-adressen (x kan elke hex-waarde zijn):

```
x2-xx-xx-xx-xx-xx
x6-xx-xx-xx-xx-xx
xA-xx-xx-xx-xx-xx
xE-xx-xx-xx-xx-xx
```

Android 10 apparaten gebruikt standaard een willekeurig gegenereerd lokaal beheerd MAC-adres telkens wanneer ze verbinding maken met een nieuw SSID-netwerk.

Deze eigenschap verslaat volledig de op OUI gebaseerde apparatenclassificatie aangezien de controlemechanisme erkent dat het adres is willekeurig verdeeld en geen raadpleging uitvoert.

DHCP-profielen

DHCP-profilering wordt uitgevoerd door WLC door onderzoek van de draadloze client van DHCP-pakketten.

Als DHCP-profilering is gebruikt om het apparaat te classificeren, bevat de output van **show wireless client mac-address [MAC_ADDR] gedetailleerde opdracht:**

```
Device Type      : Microsoft-Workstation
Device Name      : MSFT 5.0
Protocol Map     : 0x000009 (OUI, DHCP)
Protocol         : DHCP
```

WLC inspecteert verschillende DHCP Option velden in de pakketten verzonden door draadloze clients:

1. Optie 12 - Hostname

Deze optie vertegenwoordigt clients hostname en het kan worden gevonden in de DHCP Discover- en DHCP-verzoekpakketten:

No.	Time	Source	Destination	Protocol	Length	Info
376	476.750338	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID @x1e69cc75

```
> Ethernet II, Src: EdimaxTe_f6:76:f0 (74:da:38:f6:76:f0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: @x1e69cc75
  Seconds elapsed: 0
  > Bootp flags: @x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: EdimaxTe_f6:76:f0 (74:da:38:f6:76:f0)
  Client hardware address padding: @00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (61) Client identifier
  v Option: (12) Host Name
    Length: 15
    Host Name: DFSACTOP-KLR@0UA
```

2. Optie 60 - Identificatiecode van leveranciersklasse

Deze optie is ook te vinden in de DHCP Discover- en Aanvraagpakketten.

Met deze optie kunnen clients zich identificeren met de DHCP-server en kunnen de servers vervolgens worden geconfigureerd om alleen te reageren op de clients met een specifieke leveranciersidentificator.

Deze optie wordt het meest gebruikt om de toegangspunten in het netwerk te identificeren en er alleen op te reageren met optie 43.

Voorbeelden van leveranciersidentificatoren

- "MSFT 5,0" voor alle Windows 2000-clients (en hoger)
- "MSFT 98" voor alle Windows 98- en Me-clients
- "MSFT" voor alle Windows 98, ME en 2000 clients

Apple MacBook-apparaten sturen optie 60 standaard niet uit.

Voorbeeld pakketopname van Windows 10-client:

```
Option: (60) Vendor class identifier
Length: 8
Vendor class identifier: MSFT 5.0
```

3. Optie 55 - Aanvraaglijst voor parameters

De optie DHCP-parameterlijst bevat configuratieparameters (optiecodes) die de DHCP-client aanvraagt bij de DHCP-server. Het is een string geschreven in komma-gescheiden notatie (bijvoorbeeld 1,15,43).

Het is geen perfecte oplossing omdat de gegevens die het produceert afhankelijk zijn van de leverancier en kunnen worden gedupliceerd door meerdere apparaattypen.

Bijvoorbeeld, Windows 10 apparaten altijd standaard een bepaalde parameterlijst aanvragen. Apple iPhones en iPads gebruiken verschillende parameters waarop ze kunnen worden geclassificeerd.

Voorbeeld van opname van Windows 10-client:

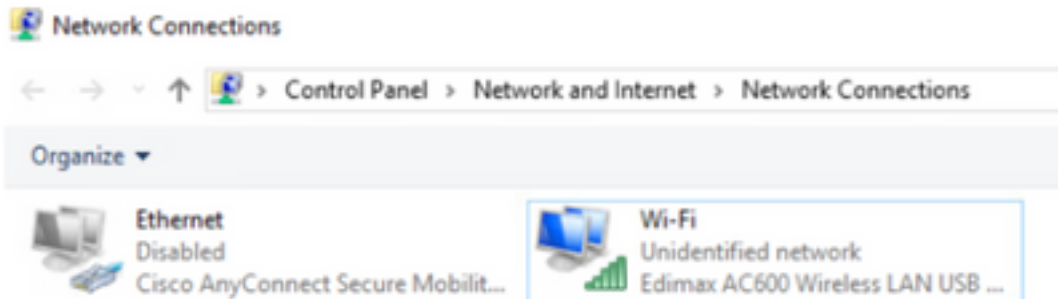
```
Option: (55) Parameter Request List
Length: 14
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (3) Router
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (31) Perform Router Discover
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (43) Vendor-Specific Information
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
Parameter Request List Item: (119) Domain Search
Parameter Request List Item: (121) Classless Static Route
Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
Parameter Request List Item: (252) Private/Proxy autodiscovery
```

4. Optie 77 - Gebruikersklasse

Gebruikersklasse is een optie die meestal niet standaard wordt gebruikt en waarvoor de client handmatig moet worden geconfigureerd. Deze optie kan bijvoorbeeld op een Windows-machine worden geconfigureerd met de opdracht:

```
ipconfig /setclassid "ADAPTER_NAME" "USER_CLASS_STRING"
```

De naam van de adapter kan worden gevonden in het Network & Sharing Center in het bedieningspaneel:



DHCP-optie 66 configureren voor Windows 10-client in CMD (vereist beheerdersrechten):

```
C:\Windows\system32>ipconfig /setclassid "Wi-Fi" "test_user_class"
Windows IP Configuration
Successfully set the DHCPv4 class id for adapter Wi-Fi.
```

Wegens de implementatie van Windows van optie 66, kan wireshark deze optie niet decoderen en een deel van het pakket dat na optie 66 komt verschijnt als misvormd:

```
  ▾ Option: (77) User Class Information
    Length: 15
    ▾ Instance of User Class: [0]
      User Class Length: 116
  ▾ [Malformed Packet: DHCP/BOOTP]
    ▾ [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
      [Malformed Packet (Exception occurred)]
      [Severity level: Error]
      [Group: Malformed]
```

HTTP-profielen

HTTP-profilering is de meest geavanceerde manier van profileren 9800 WLC-ondersteuning en biedt de meest gedetailleerde apparaatclassificatie.

Voor een client om HTTP geprofileerd te zijn, moet deze zich in een "Run"-status bevinden en een HTTP GET-verzoek uitvoeren.

WLC onderschept de aanvraag en kijkt naar het veld "User-Agent" in de HTTP-header van het pakket.

Dit veld bevat aanvullende informatie over de draadloze client die kan worden gebruikt voor de classificatie ervan.

Standaard hebben bijna alle fabrikanten een optie geïmplementeerd waarbij een draadloze client probeert de internetverbinding te controleren.

Deze controle wordt ook gebruikt voor automatische gast portal detectie. Als een apparaat een HTTP-respons met statuscode 200 (OK) ontvangt, betekent dit dat het WLAN niet is beveiligd met webauth.

Als dit zo is, voert de WLC interceptie uit die nodig is om de rest van de authenticatie uit te voeren. Deze eerste HTTP GET is niet de enige die WLC kan gebruiken om het apparaat te profileren.

Elk volgend HTTP verzoek wordt geïnspecteerd door de WLC en het resulteert mogelijk met nog meer gedetailleerde classificatie.

Windows 10-apparaten gebruiken het domein **msftconnecttest.com** om deze test uit te voeren. Apple-apparaten maken gebruik van **captive.apple.com**, terwijl Android-apparaten meestal **connectivitycheck.gatic.com** gebruiken.

Packet-opnamen van de Windows 10-client die deze controle uitvoert, zijn hieronder te vinden. Het veld User Agent is gevuld met **Microsoft NCSI**, waardoor client als **Microsoft-Workstation** wordt geprofileerd op de WLC:

```
No.    Time          Source                Destination           Protocol Length  Info
-----
32    11.238352     10.48.39.235         64.182.6.247         DNS      83      Standard query 0x66ed AAAA www.msftconnecttest.com
48    11.344857     64.182.6.247        10.48.39.235         DNS      249     Standard query response 0x6d26 A www.msftconnecttest.com CNAME v4nc
55    11.354877     10.48.39.235        13.187.4.52          HTTP     165     GET /connecttest.txt HTTP/1.1
70    11.370809     13.187.4.52         10.48.39.235         HTTP     624     HTTP/1.1 200 OK (text/plain)

> Frame 55: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface \Device\NPF_{95A000B2-0027-4F05-8918-96A8465839A8}, id 0
> Ethernet II, Src: EdimaxTe_f8:76:f0 (74:0d:38:f6:76:f0), Dst: Cisco_19:41:e1 (24:7e:12:19:41:e1)
> Internet Protocol Version 4, Src: 10.48.39.235, Dst: 13.187.4.52
> Transmission Control Protocol, Src Port: 56815, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
Hypertext Transfer Protocol
  GET /connecttest.txt HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /connecttest.txt HTTP/1.1\r\n]
  Request Method: GET
  Request URI: /connecttest.txt
  Request Version: HTTP/1.1
  Connection: Close\r\n
  User-Agent: Microsoft NCSI\r\n
  Host: www.msftconnecttest.com\r\n
  \r\n
  [Full request URI: http://www.msftconnecttest.com/connecttest.txt]
  [HTTP request 1/1]
  [Response in frame 70]
```

Voorbeeld uitvoer van **show wireless client mac-address [MAC_ADDR]** gedetailleerd voor een client die is geprofileerd via HTTP:

```
Device Type      : Microsoft-Workstation
Device Name      : MSFT 5.0
Protocol Map     : 0x000029 (OUI, DHCP, HTTP)
Device OS        : Windows NT 10.0; Win64; x64; rv:76.0
Protocol         : HTTP
```

RADIUS-profilering

Als het gaat om de methoden die worden gebruikt om het apparaat te classificeren, is er geen verschil tussen lokale en RADIUS-profilering.

Als Radius profiling is ingeschakeld, stuurt de WLC de informatie die het over het apparaat heeft geleerd door via een specifieke set leveranciersspecifieke RADIUS-kenmerken naar de RADIUS-server.

DHCP-RADIUS-profilering

Informatie die wordt verkregen door DHCP-profilering wordt als een leveranciersspecifieke RADIUS AVPair naar de RADIUS-server verzonden binnen het boekhoudverzoek **Cisco Av-paar: dhcp-option=<DHCP-optie>**


```

4744 1995,180880 18.48.39.112 18.48.71.92 AADIUS 765 57397 1813 Accounting-Request Id=186
4749 1995,111994 18.48.71.92 18.48.39.112 AADIUS 62 1813 57397 Accounting-Response Id=186
4758 1995,111994 18.48.71.92 18.48.39.112 AADIUS 62 1813 57397 Accounting-Response Id=186, Duplicate Response

```

```

User Datagram Protocol, Src Port: 57397, Dest Port: 1813
RADIUS Protocol
Code: Accounting-Request (4)
Packet Identifier: 866 (186)
Length: 723
Authenticator: 4885c9d9b8eeae7862d5837f9844f2f
[The response to this request is in frame 4763]
Attribute Value Pairs
  > AVP: t=Vendor-Specific(26) 1444 vnd=ciscoSystems(P)
  > AVP: t=Vendor-Specific(26) 1437 vnd=ciscoSystems(P)
  > AVP: t=Vendor-Specific(26) 1448 vnd=ciscoSystems(P)
  > AVP: t=Vendor-Specific(26) 1429 vnd=ciscoSystems(P)
  > AVP: t=Vendor-Specific(26) 1438 vnd=ciscoSystems(P)
  > AVP: t=Vendor-Specific(26) 1426 vnd=ciscoSystems(P)
  > AVP: t=Vendor-Specific(26) 1499 vnd=ciscoSystems(P)
    Type: 26
    Length: 99
    Vendor ID: ciscoSystems (9)
    > VS: t=Cisco-APPair(1) 1=93 val=http-tlv=000f00100000c111a/5.8 [Windows NT 10.0; x64; x64; rv:76.0] Gecko/20100101 Firefox/76.0


```

Profiling op 9800 WLC configureren

Lokale profielconfiguratie

Als u lokale profilering wilt laten werken, schakelt u Apparaatclassificatie in onder Configuratie > Draadloos > Draadloos wereldwijd. Met deze optie kunt u MAC OUI-, HTTP- en DHCP-profilering tegelijkertijd inschakelen:

Configuration > Wireless > Wireless Global

Default Mobility Domain *	default 
RF Group Name*	default
Maximum Login Sessions Per User*	0
Management Via Wireless	<input type="checkbox"/>
Device Classification	<input checked="" type="checkbox"/>
AP LAG Mode	<input type="checkbox"/>

Bovendien kunt u onder Policy Configuration HTTP TLV-caching en DHCP TLV-caching inschakelen. WLC doet aan profilering, zelfs als dit niet gebeurt.

Als deze opties zijn ingeschakeld, heeft de WLC eerst informatie over deze client in het

cachegeheugen opgeslagen en hoeft u geen extra pakketten te inspecteren die door dit apparaat zijn gegenereerd.

Edit Policy Profile

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification **Enabled** ⓘ

Local Subscriber Policy Name BlockPolicy ✕ ▼

Configuratie RADIUS-profielen

Om RADIUS-profilering te laten werken, is het naast het wereldwijd mogelijk maken van apparaatclassificatie (zoals vermeld in Local Profiling Configuration) noodzakelijk om:

1. De AAA-accounting methode configureren met het type "identiteit" dat naar de RADIUS-server wijst:

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

Name	Type	Group1	Group2	Group3	Group4
AccMethod	identity	ISE22	N/A	N/A	N/A

20 items per page 1 - 1 of 1 items

2. De boekhoudmethode moet worden toegevoegd onder Configuratie > Tags en profielen > Beleid > [Policy_Name] > Advanced:

Edit Policy Profile

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

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override

NAC State

NAC Type

Policy Name

Accounting List

Fabric Profile

mDNS Service Policy [Clear](#)

Hotspot Server

User Private Network

Status

Drop Unicast

Umbrella

Umbrella Parameter Map [Clear](#)

Flex DHCP Option for DNS **ENABLED**

DNS Traffic Redirect

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

3. Ten slotte moet het selectievakje RADIUS-profilering aangevinkt zijn onder Configuration > Tags & profielen > Policy Dit selectievakje maakt zowel HTTP- als DHCP RADIUS-profilering mogelijk (oude AireOS WLC's hadden 2 aparte selectievakjes):

Edit Policy Profile

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification **Enabled** ⓘ

Local Subscriber Policy Name

Gebruiscases profileren

Lokaal beleid toepassen op basis van lokale profielclassificatie

Deze voorbeeldconfiguratie toont de configuratie van Local Policy met QoS-profiel dat YouTube- en Facebook-toegang blokkeert die alleen wordt toegepast op apparaten die als Windows-Workstation zijn geprofileerd.

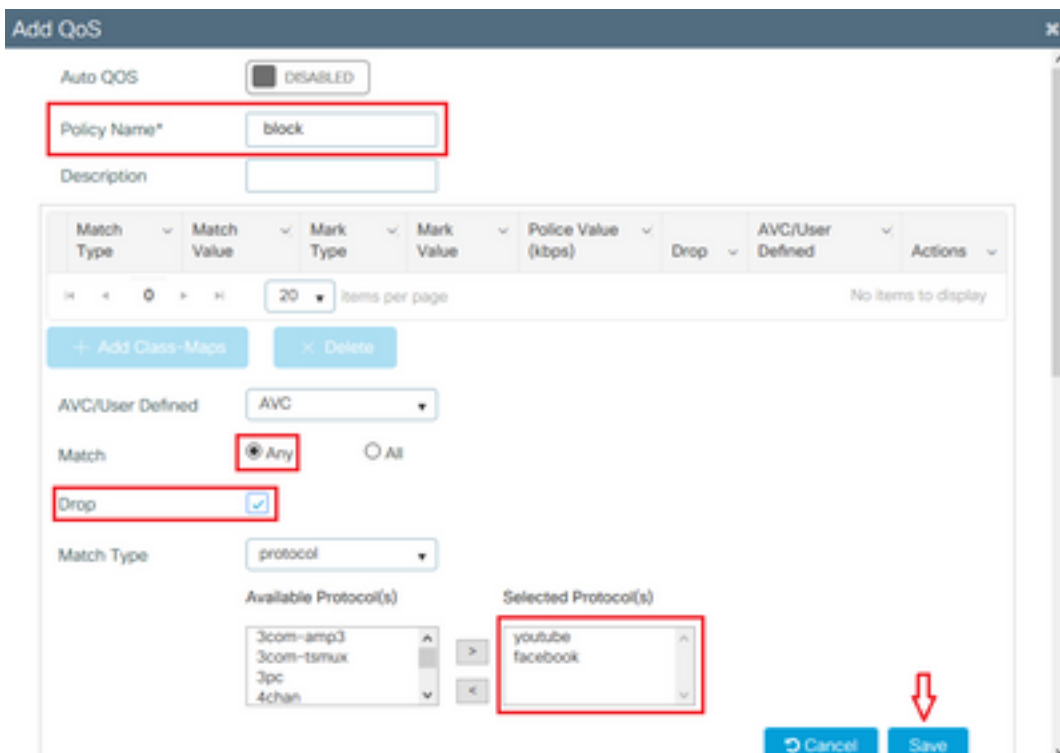
Met lichte veranderingen, kan deze configuratie worden aangepast aan, bijvoorbeeld, vastgestelde specifieke DSCP markering voor slechts draadloze telefoons.

Maak een QoS-profiel door te navigeren naar **Configuration > Services > QoS**. Klik op Add om een nieuw beleid te maken:



Specificeer de beleidsnaam en voeg een nieuwe klassenkaart toe. Selecteer uit de beschikbare protocollen de protocollen die moeten worden geblokkeerd, DSCP gemarkeerd of bandbreedte beperkt.

In dit voorbeeld zijn YouTube en facebook geblokkeerd. Zorg ervoor dat u dit QoS-profiel niet toepast op de beleidsprofielen onder in het QoS-venster:



Available (8) Selected (0)

Profiles

Profiles	Ingress	Egress
<ul style="list-style-type: none"> vasa 33nps webauth 11webauth 11mobility 11override 		

Cancel Apply to Device

Navigeer naar **Configuratie > Beveiliging > Lokaal beleid** en maak een nieuwe servicessjabloon:

Configuration > Security > Local Policy

Service Template Policy Map

Add Delete

Service Template Name	Source
<input type="checkbox"/> webauth-global-inactive	
<input type="checkbox"/> DEFAULT_CRITICAL_DATA_TEMPLATE	
<input type="checkbox"/> DEFAULT_CRITICAL_VOICE_TEMPLATE	
<input type="checkbox"/> DEFAULT_LINKSEC_POLICY_MUST_SECURE	
<input type="checkbox"/> DEFAULT_LINKSEC_POLICY_SHOULD_SECURE	

1 - 5 of 5 items

Specificeer profiel voor Ingress en uitgaande QoS dat in de vorige stap is gemaakt. Een toegangslijst kan ook in deze stap worden toegepast. Als er geen VLAN-wijziging nodig is, laat u het VLAN-veld leeg:

Create Service Template

Service Template Name* BlockTemplate

VLAN ID 1-4094

Session Timeout (secs) 1-65535


Access Control List None

Ingress QOS block

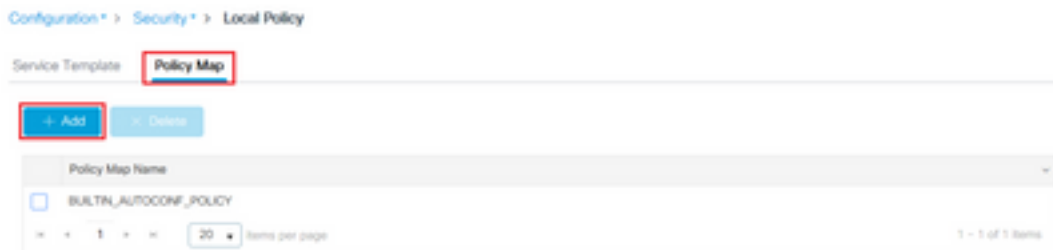
Egress QOS block

mDNS Service Policy Search or Select

Cancel Apply to Device



Navigeer naar het tabblad Policy Map en klik op Add:

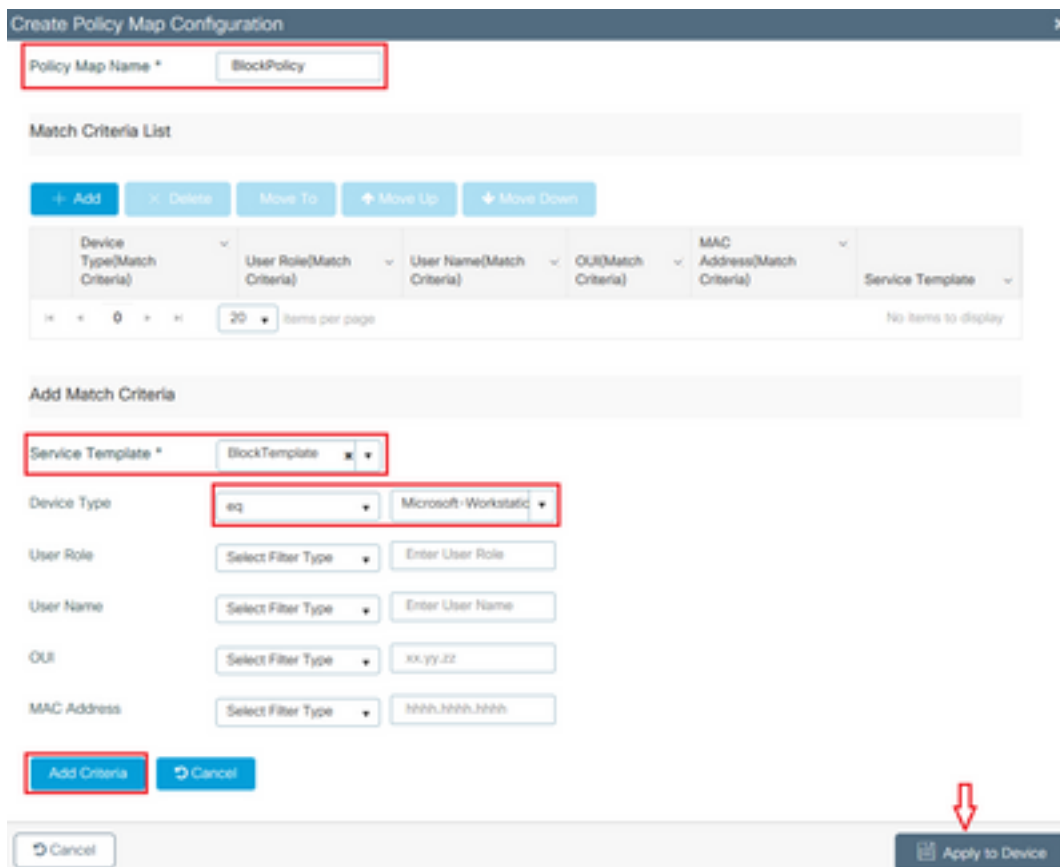


Stel een Policy Map-naam in en voeg nieuwe criteria toe. Specificeer de servicesjabloon die in de vorige stap is gemaakt en selecteer het apparaattype waarop deze sjabloon is toegepast.

In dit geval wordt Microsoft-Workstation gebruikt. Als er meerdere beleidsregels zijn gedefinieerd, wordt de eerste overeenkomst gebruikt.

Een andere veel voorkomende toepassing is het specificeren van op OUI gebaseerde matchcriteria. Als een plaatsing een groot aantal scanners of printers van het zelfde model heeft, hebben zij gewoonlijk zelfde MAC OUI.

U kunt deze optie gebruiken om specifieke QoS DSCP-markering of een ACL toe te passen:



Om WLC in staat te stellen het youtube- en facebook-verkeer te herkennen, moet de zichtbaarheid van toepassingen worden ingeschakeld.

Navigeren naar **Configuratie > Services > Toepassingszichtbaarheid** eZichtbaarheid voor het beleidsprofiel van uw WLAN inschakelen:

Drag and Drop, double click or click on the button from Selected Profiles to add/remove Profiles

Available (11)

Profiles

- 11webauth
- 11mobility
- 11profiling
- 33nps
- Capwap1
- default-policy-profile

Enabled (1)

Profiles	Visibility	Collector Address
11override	<input checked="" type="checkbox"/>	Local <input checked="" type="checkbox"/> External <input type="checkbox"/>

Enable All Disable All

Legend: up - down - administratively down

Controleer dat onder het beleidsprofiel de HTTP TLV-caching, DHCP TLV-caching en Global Device Classification zijn ingeschakeld en dat Local Subscriber Policy verwijst naar de Local Policy map die in een van de vorige stappen is gemaakt:

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification Enabled ⓘ

Local Subscriber Policy Name BlockPolicy

VLAN

VLAN/VLAN Group VLAN0039

Multicast VLAN Enter Multicast VLAN

WLAN ACL

IPv4 ACL Search or Select

IPv6 ACL Search or Select

URL Filters

Pre Auth Search or Select

Post Auth Search or Select

Nadat de klant verbinding heeft gemaakt, is het mogelijk om te controleren of het lokale beleid is toegepast en te testen of YouTube en Facebook daadwerkelijk worden geblokkeerd.

Uitvoer van de show draadloze client mac-adres [MAC_ADDR] gedetailleerd bevat:

```

Input Policy Name : block
Input Policy State : Installed
Input Policy Source : Native Profile Policy
Output Policy Name : block
Output Policy State : Installed
Output Policy Source : Native Profile Policy

```

Local Policies:

```

Service Template : BlockTemplate (priority 150)
Input QOS : block

```

Output QOS : **block**
Service Template : wlan_svc_11override_local (priority 254)
VLAN : VLAN0039
Absolute-Timer : 1800

Device Type : **Microsoft-Workstation**
Device Name : **MSFT 5.0**
Protocol Map : 0x000029 (OUI, DHCP, HTTP)
Protocol : **HTTP**

Radius-profilering voor geavanceerde beleidssets in Cisco ISE

Als RADIUS-profilering is ingeschakeld, stuurt de WLC profileringsinformatie door naar de ISE. Gebaseerd op deze info, is het mogelijk om geavanceerde authenticatie en autorisatieregels te creëren.

Dit artikel is niet van toepassing op ISE-configuraties. Raadpleeg de [ontwerpgids voor Cisco ISE-profielen](#) voor meer informatie.

Deze werkstroom vereist meestal het gebruik van CoA, dus zorg ervoor dat het is ingeschakeld op de 9800 WLC.

Profiling in FlexConnect-implementaties

Centrale verificatie, lokale switching

In deze installatie blijven zowel lokale als RADIUS-profilering werken zoals in eerdere hoofdstukken is beschreven. Als AP in standalone modus gaat (AP verliest verbinding met WLC), stopt het apparaat profileren met werken en geen nieuwe cliënten kunnen verbinden.

Lokale verificatie en lokale switching

Als AP in de verbonden modus is (AP is aangesloten bij de WLC), blijft profileren werken (AP stuurt een kopie van client-DHCP-pakketten naar de WLC om het profileringsproces uit te voeren).

Ondanks het profileren van het werken, aangezien de authenticatie plaatselijk op AP wordt uitgevoerd, kan het profileren van informatie niet voor om het even welke Lokale configuratie van het Beleid of het profileren van RADIUS regels worden gebruikt.

Probleemoplossing

Radioactieve sporen

De gemakkelijkste manier om client profiling op de WLC problemen op te lossen is via radioactieve sporen. Navigeer naar **Problemen oplossen > Radioactive Trace**, voer het MAC-adres van de draadloze clientadapter in en klik op Start:

Conditional Debug Global State: **Started**

MAC/IP Address	Trace file	
<input type="checkbox"/> 74da.38f6.76f0	debugTrace_74da.38f6.76f0.txt	<input type="button" value="▶ Generate"/>

items per page
 1 - 1 of 1 items

Sluit de client aan op het netwerk en wacht tot de uitvoerstatus is bereikt. Stop de sporen en klik op **Generate**. Zorg ervoor dat de interne logbestanden zijn ingeschakeld (deze optie bestaat alleen bij 17.1.1-releases en hoger):

Enter time interval ×

Enable Internal Logs

Generate logs for last
 10 minutes
 30 minutes
 1 hour
 since last boot

Relevante fragmenten van het radioactieve spoor zijn hieronder te vinden:

Cliënt die door WLC als Microsoft-Workstation wordt geprofileerd:

```

2020/06/18 10:46:41.052366 {wncd_x_R0-0}{1}: [auth-mgr] [21168]: (info):
[74da.38f6.76f0:capwap_90000004] Device type for the session is detected as Microsoft-Workstation and old device-type not classified earlier &Device name for the session is detected as MSFT 5.0 and old device-name not classified earlier & Old protocol map 0 and new is 41
2020/06/18 10:46:41.052367 {wncd_x_R0-0}{1}: [auth-mgr] [21168]: (debug):
[74da.38f6.76f0:capwap_90000004] updating device type Microsoft-Workstation, device name MSFT 5.0
    
```


WLC caching de apparatenclassificatie:

```
(debug): [74da.38f6.76f0:unknown] Updating cache for mac [74da.38f6.76f0] device_type:
Microsoft-Workstation, device_name: MSFT 5.0 user_role: NULL protocol_map: 41
```

WLC die de apparatenclassificatie binnen het geheime voorgeheugen vindt:

```
(info): [74da.38f6.76f0:capwap_90000004] Device type found in cache Microsoft-Workstation
```

WLC past lokaal beleid toe gebaseerd op classificatie:

```
(info): device-type filter: Microsoft-Workstation required, Microsoft-Workstation set - match
for 74da.38f6.76f0 / 0x9700001A
```

```
(info): device-type Filter evaluation succeeded
```

```
(debug): match device-type eq "Microsoft-Workstation" :success
```

WLC-verzendingspakketten met DHCP- en HTTP-profileringskenmerk:

```
[caaa-acct] [21168]: (debug): [CAAA:ACCT:c9000021] Accounting session created
```

```
[auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap_90000004] Getting active filter list
```

```
[auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap_90000004] Found http
```

```
[auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap_90000004] Found dhcp
```

```
[aaa-attr-inf] [21168]: (debug): Filter list http-tlv 0
```

```
[aaa-attr-inf] [21168]: (debug): Filter list dhcp-option 0
```

```
[aaa-attr-inf] [21168]: (debug): Get acct attrs dc-profile-name 0 "Microsoft-Workstation"
```

```
[aaa-attr-inf] [21168]: (debug): Get acct attrs dc-device-name 0 "MSFT 5.0"
```

```
[aaa-attr-inf] [21168]: (debug): Get acct attrs dc-device-class-tag 0 "Workstation:Microsoft-
Workstation"
```

```
[aaa-attr-inf] [21168]: (debug): Get acct attrs dc-certainty-metric 0 10 (0xa)
```

```
[aaa-attr-inf] [21168]: (debug): Get acct attrs dhcp-option 0 00 0c 00 0f 44 45 53 4b 54 4f 50
2d 4b 4c 52 45 30 4d 41
```

```
[aaa-attr-inf] [21168]: (debug): Get acct attrs dhcp-option 0 00 3c 00 08 4d 53 46 54 20 35 2e
30
```

```
[aaa-attr-inf] [21168]: (debug): Get acct attrs dhcp-option 0 00 37 00 0e 01 03 06 0f 1f 21 2b
2c 2e 2f 77 79 f9 fc
```

```
### http profiling sent in a separate accounting packet
```

```
[aaa-attr-inf] [21168]: (debug): Get acct attrs http-tlv 0 00 01 00 0e 4d 69 63 72 6f 73 6f 66
74 20 4e 43 53 49
```

PacketCapture

In een centraal switched implementatie kunnen pakketopnamen op de WLC zelf worden uitgevoerd. Navigeer naar **Problemen oplossen > Packet Capture** en maak een nieuw opnamepunt op een van de interfaces die in gebruik zijn bij deze client.

Het is vereist om SVI op het VLAN te hebben om opname op het uit te voeren, anders neem de opname op de fysieke poort zelf

Troubleshooting > Packet Capture

+ Add - Delete

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
0							

20 items per page No items to display

Create Packet Capture

Capture Name* capture

Filter* any

Monitor Control Plane

Buffer Size (MB)* 10

Limit by* Duration 3600 secs == 1.00 hour

Available (4) Selected (1)

<input checked="" type="checkbox"/> GgabitEthernet1	→
<input checked="" type="checkbox"/> GgabitEthernet2	→
<input checked="" type="checkbox"/> GgabitEthernet3	→
<input checked="" type="checkbox"/> Vlan1	→

<input checked="" type="checkbox"/> Vlan39	←
--	---

Cancel Apply to Device

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.