

Client-Profilerstellung für Wireless LAN-Controller 9800 demonstrieren

Inhalt

[Einleitung](#)

[Verwendete Komponenten](#)

[Profilstellungsprozess](#)

[OUI-Profilerstellung für MAC-Adresse](#)

[Lokal verwaltete MAC-Adressen behandeln Probleme](#)

[DHCP-Profilerstellung](#)

[HTTP-Profilerstellung](#)

[RADIUS-Profilerstellung](#)

[DHCP RADIUS-Profilerstellung](#)

[HTTP RADIUS-Profilerstellung](#)

[Konfigurieren der Profilerstellung auf dem 9800 WLC](#)

[Lokale Profilkonfiguration](#)

[Konfiguration der RADIUS-Profilerstellung](#)

[Profilerstellung - Anwendungsfälle](#)

[Anwenden lokaler Richtlinien auf Grundlage der lokalen Profilklassifizierung](#)

[Radius-Profilerstellung für erweiterte Policy Sets in der Cisco ISE](#)

[Profilierung in FlexConnect-Bereitstellungen](#)

[Zentrale Authentifizierung, lokales Switching](#)

[Lokale Authentifizierung, lokales Switching](#)

[Fehlerbehebung](#)

[Radioaktive Spuren](#)

[Paketerfassung](#)

Einleitung

In diesem Dokument wird die Funktionsweise der Klassifizierung und Profilerstellung für Geräte auf Cisco Catalyst Wireless LAN-Controllern der Serie 9800 beschrieben.

Verwendete Komponenten

- 9800 CL WLC mit 17.2.1 Image
- Access Point 1815i
- Windows 10 Pro Wireless-Client
- Cisco ISE 2.7

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Profilstellungsprozess

In diesem Artikel wird ausführlich erläutert, wie die Geräteklassifizierung und -profilierung auf Cisco Catalyst 9800 Wireless LAN-Controllern funktioniert. Darüber hinaus werden mögliche Anwendungsfälle, Konfigurationsbeispiele und die erforderlichen Schritte zur Fehlerbehebung beschrieben.

Die Erstellung von Geräteprofilen bietet eine Möglichkeit, zusätzliche Informationen zu einem Wireless-Client zu erhalten, der der Wireless-Infrastruktur beigetreten ist.

Sobald die Erstellung der Geräteprofile erfolgt ist, können mit dieser Funktion verschiedene lokale Richtlinien angewendet oder bestimmte RADIUS-Serverregeln abgeglichen werden.

Die Cisco WLCs der Serie 9800 können drei (3) Arten der Erstellung von Geräteprofilen durchführen:

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

OUI-Profilerstellung für MAC-Adresse

Die MAC-Adresse ist eine eindeutige Kennung für jede drahtlose (und kabelgebundene) Netzwerkschnittstelle. Es handelt sich um eine 48-Bit-Nummer, die in der Regel im Hexadezimalformat MM:MM:MM:SS:SS notiert ist.

Die ersten 24 Bit (oder 3 Achtbitzeichen) werden als OUI (Organizational Unique Identifier) bezeichnet und bezeichnen eindeutig einen Anbieter oder Hersteller.

Sie werden vom IEEE erworben und zugewiesen. Ein Anbieter oder Hersteller kann mehrere OUIs erwerben.

Beispiel:

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

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

Sobald ein Wireless-Client mit dem Access Point verbunden ist, führt der WLC eine OUI-Suche durch, um den Hersteller zu ermitteln.

In FlexConnect-Bereitstellungen für lokales Switching leitet der Access Point relevante Client-Informationen wie DHCP-Pakete und die MAC-Adresse des Clients weiter an den WLC weiter.

Eine Profilierung, die nur auf OUI basiert, ist äußerst begrenzt, und es ist möglich, ein Gerät als eine bestimmte Marke zu klassifizieren, es kann jedoch nicht zwischen einem Laptop und einem Smartphone unterscheiden.

Lokal verwaltete MAC-Adressen behandeln Probleme

Aus Datenschutzgründen begannen viele Hersteller, Mac-Randomisierungsfunktionen in ihre Geräte zu integrieren.

Lokal verwaltete MAC-Adressen werden nach dem Zufallsprinzip generiert und weisen ein

zweitgeringwertiges Bit des ersten Oktetts der Adresse auf 1 auf.

Dieses Bit fungiert als Flag, das ankündigt, dass die MAC-Adresse tatsächlich eine zufällig generierte ist.

Es gibt vier mögliche Formate für lokal verwaltete MAC-Adressen (x kann ein beliebiger Hexadezimalwert sein):

```
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-Geräte verwenden standardmäßig eine zufällig generierte, lokal verwaltete MAC-Adresse, wenn sie sich mit einem neuen SSID-Netzwerk verbinden.

Diese Funktion verhindert vollständig die OUI-basierte Geräteklassifizierung, da der Controller erkennt, dass die Adresse randomisiert wurde und keine Suche durchführt.

DHCP-Profilerstellung

Die DHCP-Profilerstellung wird vom WLC durch Untersuchung der DHCP-Pakete durchgeführt, die der Wireless-Client sendet.

Wenn das Gerät mithilfe der DHCP-Profilerstellung klassifiziert wurde, enthält die Ausgabe des Befehls **show wireless client mac-address [MAC_ADDR]** Folgendes:

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

WLC überprüft mehrere DHCP-Optionsfelder in den von Wireless-Clients versendeten Paketen:

1. Option 12 - Hostname

Diese Option stellt den Hostnamen des Clients dar und ist in den Paketen "DHCP Discover" und "DHCP Request" zu finden:

No.	Time	Source	Destination	Protocol	Length	Info
376	476.750338	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x1e09cc75

```

> 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
Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x1e09cc75
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (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
  > Option: (12) Host Name
    Length: 15
    Host Name: DESKTOP-KLR8094
  
```

2. Option 60 - Anbieter-Klassenkennung

Diese Option finden Sie auch in den Paketen "DHCP Discover and Request" (DHCP erkennen und anfordern).

Mit dieser Option können sich die Clients gegenüber dem DHCP-Server identifizieren, und die Server können dann so konfiguriert werden, dass sie auf die Clients nur mit einer bestimmten Anbieterklassenkennung antworten.

Diese Option wird am häufigsten verwendet, um die Access Points im Netzwerk zu identifizieren und nur mit der Option 43 auf diese zu reagieren.

Beispiele für Anbieterklassen-IDs

- "MSFT 5.0" für alle Windows 2000-Clients (und höher)
- "MSFT 98" für alle Windows 98 und Me Clients
- "Microsoft" für alle Windows 98, Me und 2000 Clients

Apple MacBook-Geräte senden standardmäßig keine Option 60 aus.

Beispiel für die Paketerfassung vom Windows 10-Client:

```

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

3. Option 55 - Parameteranforderungsliste

Die DHCP Parameter Request List-Option enthält Konfigurationsparameter (Optionscodes), die der DHCP-Client vom DHCP-Server anfordert. Es handelt sich um eine Zeichenfolge in kommasetrennter Notation (z. B. 1,15,43).

Dies ist keine perfekte Lösung, da die generierten Daten herstellerabhängig sind und von verschiedenen Gerätetypen dupliziert werden können.

Beispielsweise fordern Windows 10-Geräte standardmäßig immer eine bestimmte Parameterliste an. Apple iPhones und iPads verwenden verschiedene Parameter, auf denen es möglich ist, sie

zu klassifizieren.

Beispielaufzeichnung vom Windows 10-Client:

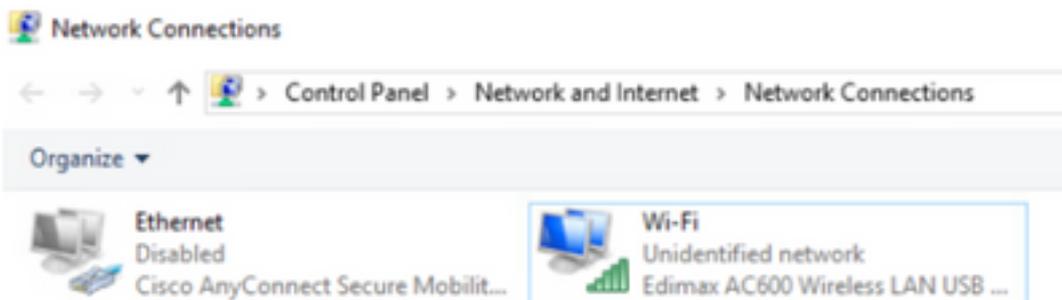
```
Option: (55) Parameter Request List
Length: 14
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (3) Router
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (31) Perform Router Discover
Parameter 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. Option 77 - Benutzerklasse

Benutzerklasse ist eine Option, die in der Regel nicht standardmäßig verwendet wird und die eine manuelle Konfiguration des Clients erfordert. Diese Option kann z. B. mithilfe des folgenden Befehls auf einem Windows-Computer konfiguriert werden:

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

Sie finden den Adapternamen im Netzwerk- und Freigabecenter in der Systemsteuerung:



Konfigurieren Sie die DHCP-Option 66 für den Windows 10-Client in CMD (erfordert Administratorrechte):

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

Aufgrund der Windows-Implementierung von Option 66 ist Wireshark nicht in der Lage, diese Option zu dekodieren, und ein Teil des Pakets, das nach Option 66 eingeht, wird als fehlerhaft angezeigt:

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

HTTP-Profilerstellung

Die HTTP-Profilerstellung ist die fortschrittlichste Methode zur Profilerstellung, die 9800 WLC unterstützt, und sie bietet die detaillierteste Geräteklassifizierung.

Damit ein Client ein HTTP-Profil erstellen kann, muss er den Status "Run" haben und eine HTTP GET-Anforderung ausführen.

WLC fängt die Anfrage ab und schaut in das Feld "User-Agent" im HTTP-Header des Pakets.

Dieses Feld enthält zusätzliche Informationen zum Wireless-Client, mit denen dieser klassifiziert werden kann.

Standardmäßig haben fast alle Hersteller eine Funktion implementiert, bei der ein Wireless-Client versucht, eine Prüfung der Internetverbindung durchzuführen.

Diese Prüfung wird auch für die automatische Erkennung von Gastportalen verwendet. Wenn ein Gerät eine HTTP-Antwort mit dem Statuscode 200 (OK) empfängt, bedeutet dies, dass das WLAN nicht durch Webauth gesichert ist.

Ist dies der Fall, führt der WLC das Abfangen durch, das für die restliche Authentifizierung erforderlich ist. Diese HTTP GET-Initialkonfiguration ist nicht die einzige, die der WLC für die Erstellung eines Geräteprofils verwenden kann.

Jede nachfolgende HTTP-Anfrage wird vom WLC geprüft und ergibt möglicherweise eine noch detailliertere Klassifizierung.

Windows 10-Geräte verwenden die Domäne **msftconnecttest.com**, um diesen Test durchzuführen. Apple-Geräte verwenden **captive.apple.com**, während Android-Geräte in der Regel **connectivitycheck.gstatic.com** verwenden.

Paketerfassungen des Windows 10-Clients, der diese Prüfung durchführt, finden Sie weiter unten. Das Feld "User Agent" wird mit **Microsoft NCSI** ausgefüllt, was dazu führt, dass der Client auf dem WLC als **Microsoft-Workstation** profiliert wird:

No.	Time	Source	Destination	Protocol	Length	Info
32	11.238752	10.48.39.235	64.182.6.247	DNS	83	Standard query 0x6d26 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 vnc
55	11.354877	10.48.39.235	13.187.4.52	HTTP	365	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: 365 bytes on wire (1320 bits), 365 bytes captured (1320 bits) on interface \Device\NPF_{95A000B2-0B27-4F05-B918-96A84E6839A8}, id 0
> Ethernet II, Src: EdimaxFe_f6:76: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: 50815, Dst Port: 80, Seq: 1, Ack: 1, Len: 333
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 NCS1\r\n
  Host: www.msftconnecttest.com\r\n
  \r\n
  [Full request URI: http://www.msftconnecttest.com/connecttest.txt]
  [HTTP request 1/3]
  [Response in frame 70]

```

Beispielausgabe von **show wireless client mac-address [MAC_ADDR]** detailliert für einen Client, der über HTTP profiliert wird:

```

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-Profilierstellung

Bei den Methoden zur Klassifizierung des Geräts gibt es keinen Unterschied zwischen der lokalen und der RADIUS-Profilierstellung.

Wenn die Radius-Profilierstellung aktiviert ist, leitet der WLC die vom Gerät erfassten Informationen über einen bestimmten Satz anbieterspezifischer RADIUS-Attribute an den RADIUS-Server weiter.

DHCP RADIUS-Profilierstellung

Die durch die DHCP-Profilierstellung erhaltenen Informationen werden als anbieterspezifische RADIUS AVPair-Nachricht an den RADIUS-Server innerhalb der Accounting-Anforderung gesendet. **cisco-av-pair: dhcp-option=<DHCP-Option>**

Beispiel eines Accounting-Anforderungspakets, das AVPairs für die DHCP-Option 12, 60 und 55 anzeigt und vom WLC an den RADIUS-Server gesendet wurde (Wert für Option 55 erscheint möglicherweise aufgrund der Wireshark-Dekodierung als beschädigt):

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
829	9.193990	10.40.39.212	10.40.71.92	RADIUS	783	64189	1813	Accounting-Request Id=282
830	9.198995	10.40.71.92	10.40.39.212	RADIUS	62	1813	64189	Accounting-Response Id=282
838	9.198995	10.40.71.92	10.40.39.212	RADIUS	62	1813	64189	Accounting-Response Id=282, Duplicate Response


```

Frame 829: 783 bytes on wire (6264 bits), 783 bytes captured (6264 bits)
Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 10.40.39.212, Dst: 10.40.71.92
User Datagram Protocol, Src Port: 64189, Dst Port: 1813
RADIUS Protocol
Code: Accounting-Request (4)
Packet Identifier: 0x0 (282)
Length: 783
Authenticator: 31c265454b70e17169582ce362576c5
[The response to this request is in frame 830]
Attribute Value Pairs
AVP: t=Vendor-Specific(26) l=45 vnd=ciscoSystems(9)
AVP: t=Vendor-Specific(26) l=30 vnd=ciscoSystems(9)
AVP: t=Vendor-Specific(26) l=60 vnd=ciscoSystems(9)
AVP: t=Vendor-Specific(26) l=38 vnd=ciscoSystems(9)
AVP: t=Vendor-Specific(26) l=38 vnd=ciscoSystems(9)
AVP: t=Vendor-Specific(26) l=25 vnd=ciscoSystems(9)
AVP: t=Vendor-Specific(26) l=39 vnd=ciscoSystems(9)
Type: 26
Length: 39
Vendor ID: ciscoSystems(9)
VSA: t=Cisco-APPair(1) l=33 val=http-protocol=HTTP-Frame-81705xTOP-CLASS000
AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)
Type: 26
Length: 32
Vendor ID: ciscoSystems(9)
VSA: t=Cisco-APPair(1) l=32 val=http-protocol=HTTP-Frame-81707xTOP-3x
AVP: t=Vendor-Specific(26) l=38 vnd=ciscoSystems(9)
Type: 26
Length: 38
Vendor ID: ciscoSystems(9)
VSA: t=Cisco-APPair(1) l=32 val=http-protocol=HTTP-Frame-81709xTOP-81709x11x...

```

HTTP RADIUS-Profilerstellung

Die durch die HTTP-Profilerstellung (User-Agent-Feld aus dem Header der HTTP GET-Anforderung) erhaltenen Informationen werden als anbieterspezifische RADIUS AVPair an den RADIUS-Server innerhalb der Accounting-Anforderung gesendet. **cisco-av-pair: http-tlv=User-Agent=<Benutzer-Agent>**

Die erste Verbindungsprüfung für das HTTP GET-Paket enthält nur "Microsoft NCSI", da im Feld "User-Agent" nur wenige Informationen enthalten sind. Beispiel für ein Accounting-Paket, das diesen einfachen Wert an den RADIUS-Server weiterleitet:

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
4047	3583.068996	10.40.39.212	10.40.71.92	RADIUS	798	57397	1813	Accounting-Request Id=185
4054	3583.075988	10.40.71.92	10.40.39.212	RADIUS	62	1813	57397	Accounting-Response Id=185
4055	3583.075988	10.40.71.92	10.40.39.212	RADIUS	62	1813	57397	Accounting-Response Id=185, Duplicate Response


```

User Datagram Protocol, Src Port: 57397, Dst Port: 1813
RADIUS Protocol
Code: Accounting-Request (4)
Packet Identifier: 0x0 (185)
Length: 798
Authenticator: 00064b0f36c4344a968387946124d
[The response to this request is in frame 4054]
Attribute Value Pairs
AVP: t=Vendor-Specific(26) l=44 vnd=ciscoSystems(9)
AVP: t=Vendor-Specific(26) l=37 vnd=ciscoSystems(9)
AVP: t=Vendor-Specific(26) l=40 vnd=ciscoSystems(9)
AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)
AVP: t=Vendor-Specific(26) l=30 vnd=ciscoSystems(9)
AVP: t=Vendor-Specific(26) l=25 vnd=ciscoSystems(9)
AVP: t=Vendor-Specific(26) l=35 vnd=ciscoSystems(9)
Type: 26
Length: 35
Vendor ID: ciscoSystems(9)
VSA: t=Cisco-APPair(1) l=29 val=http-tlv=HTTP-12=1000:00:000000 Microsoft NCSI

```

Sobald der Benutzer mit dem Surfen im Internet beginnt und einige zusätzliche HTTP GET-Anforderungen erstellt, können weitere Informationen dazu abgerufen werden.

WLC sendet ein zusätzliches Accounting-Paket an die ISE, wenn neue User-Agent-Werte für diesen Client erkannt werden.

In diesem Beispiel können Sie sehen, dass der Client Windows 10 64 Bit und Firefox 76 verwendet:

4744	1995.180880	10.48.39.112	10.48.71.92	RADIUS	765	57397	1813	Accounting-Request Id=186
4749	1995.111994	10.48.71.92	10.48.39.112	RADIUS	62	1813	57397	Accounting-Response Id=186
4758	1995.111994	10.48.71.92	10.48.39.112	RADIUS	62	1813	57397	Accounting-Response Id=186, Duplicate Response

User Datagram Protocol, Src Port: 57397, Dst Port: 1813

RADIUS Protocol

Code: Accounting-Request (4)
Packet Identifier: 866 (186)
Length: 723
Authenticator: 4885c9d9b8ee7662f5837f9844f2f
[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)
 - > VSA: t=Cisco-APPair(1) 1=93 val=http-tlv=000f00100000c111a/5.8 [Windows NT 10.0; x64; rv:76.0] Gecko/20100101 Firefox/76.0

Konfigurieren der Profilerstellung auf dem 9800 WLC

Lokale Profilkonfiguration

Damit die lokale Profilerstellung funktioniert, aktivieren Sie einfach die Geräteklassifizierung unter Konfiguration > Wireless > Wireless Global. Diese Option aktiviert die MAC OUI-, HTTP- und DHCP-Profilerstellung gleichzeitig:

Configuration > Wireless > Wireless Global

Default Mobility Domain *

RF Group Name*

Maximum Login Sessions Per User*

Management Via Wireless

Device Classification

AP LAG Mode

Darüber hinaus können Sie unter "Policy configuration" das HTTP TLV-Caching und das DHCP TLV-Caching aktivieren. WLC führt Profilerstellung durch, selbst wenn diese nicht erforderlich ist.

Wenn diese Optionen aktiviert sind, speichert der WLC zuvor erfasste Informationen zu diesem

Client im Cache-Modus ab, sodass keine zusätzlichen Pakete geprüft werden müssen, die von diesem Gerät generiert wurden.

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 x ▾

Konfiguration der RADIUS-Profilerstellung

Damit die RADIUS-Profilerstellung funktioniert, muss neben der globalen Geräteklassifizierung (wie in der Konfiguration für lokale Profilerstellung erwähnt) Folgendes ausgeführt werden:

1. Konfigurieren Sie die AAA-Abrechnungsmethode mit dem Typ "identity", der auf den RADIUS-Server verweist:

Configuration > Security > AAA

+ AAA Wizard

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

Authentication

Authorization

Accounting

+ Add - Details

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. Die Buchungsmethode muss unter Konfiguration > Tags & Profile > Policy > [Policy_Name] > Advanced hinzugefügt werden:

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. Schließlich muss das Kontrollkästchen RADIUS Profiling unter Configuration > Tags & Profiles > Policy aktiviert werden. Dieses Kontrollkästchen aktiviert sowohl HTTP als auch DHCP RADIUS Profiling (die alten AireOS WLCs hatten zwei separate Kontrollkästchen):

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

Profilerstellung - Anwendungsfälle

Anwenden lokaler Richtlinien auf Grundlage der lokalen Profilklassifizierung

Diese Beispielkonfiguration zeigt die Konfiguration der lokalen Richtlinie mit einem QoS-Profil, das den Zugriff auf YouTube und Facebook blockiert und nur auf Geräte angewendet wird, die als Windows-Workstation eingestuft sind.

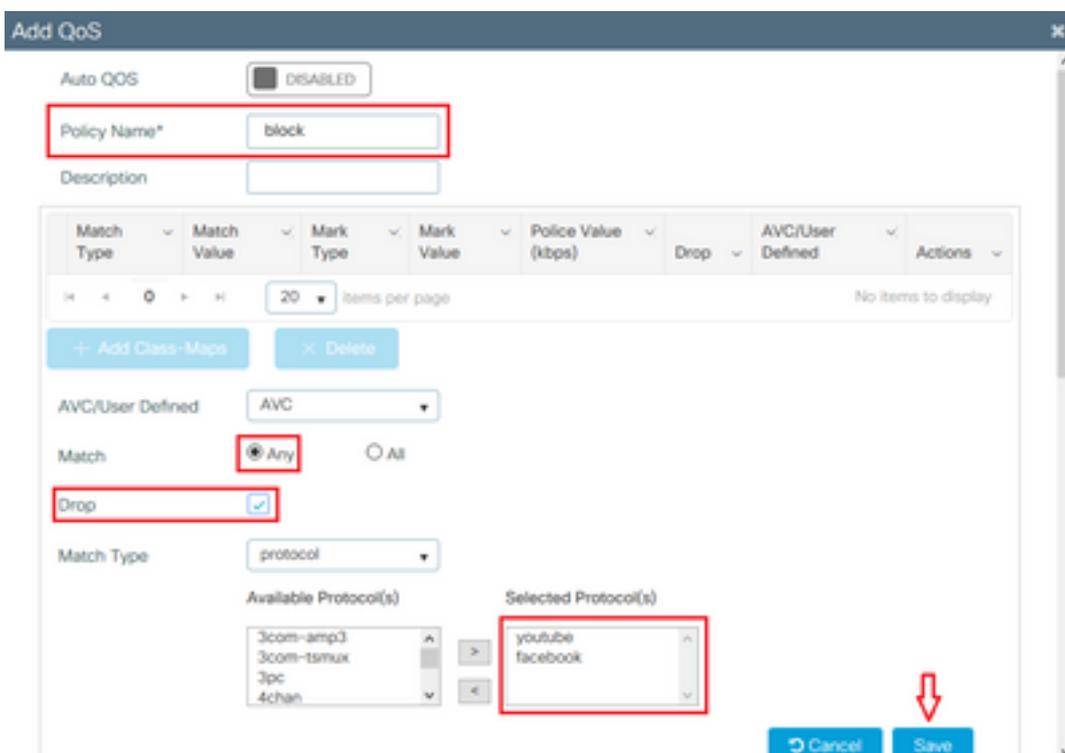
Bei geringfügigen Änderungen kann diese Konfiguration geändert werden, um z. B. eine bestimmte DSCP-Markierung nur für Wireless-Telefone festzulegen.

Erstellen Sie ein QoS-Profil, indem Sie zu **Configuration > Services > QoS** navigieren. Klicken Sie auf Hinzufügen, um eine neue Richtlinie zu erstellen:



Geben Sie den Richtliniennamen an, und fügen Sie eine neue Klassenzuordnung hinzu. Wählen Sie aus den verfügbaren Protokollen die Protokolle aus, die blockiert, DSCP markiert oder auf eine bestimmte Bandbreite beschränkt werden sollen.

In diesem Beispiel werden YouTube und Facebook blockiert. Achten Sie darauf, dieses QoS-Profil nicht auf eines der Richtlinienprofile unten im QoS-Fenster anzuwenden:



Available (8) Selected (0)

Profiles

Profiles	Ingress	Egress
vasa		
33nps		
webauth		
11webauth		
11mobility		
11override		

Cancel Apply to Device

Navigieren Sie zu **Configuration > Security > Local Policy**, und erstellen Sie eine neue Servicemaske:

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

Geben Sie das Eingangs- und Ausgangs-QoS-Profil an, das im vorherigen Schritt erstellt wurde. In diesem Schritt kann auch eine Zugriffsliste angewendet werden. Wenn keine VLAN-Änderung erforderlich ist, lassen Sie das VLAN-Feld leer:

Create Service Template

Service Template Name* BlockTemplate

VLAN ID 1-4094

Session Timeout (secs) 1-65535

Access Control List None

Ingress QOS block x

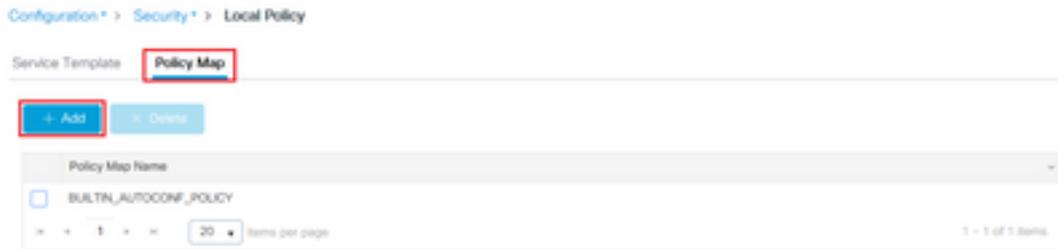
Egress QOS block x

mDNS Service Policy Search or Select

Cancel Apply to Device



Navigieren Sie zur Registerkarte Policy Map, und klicken Sie auf Hinzufügen:

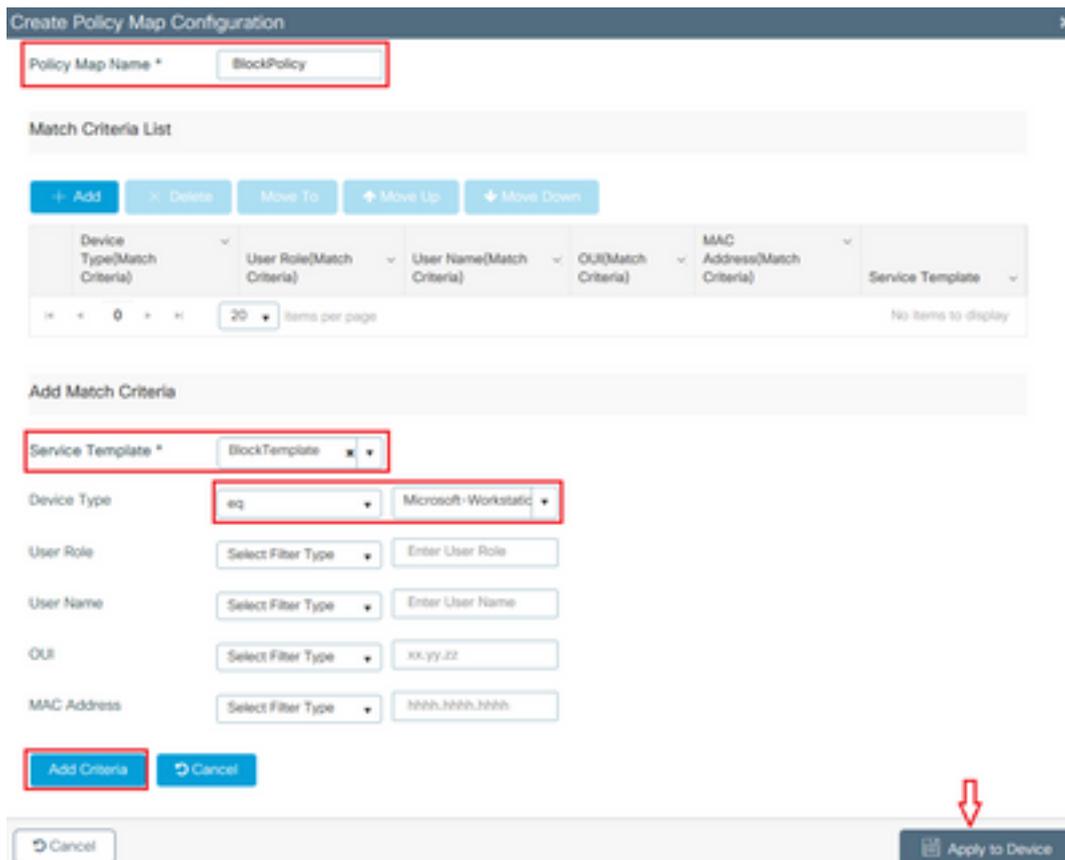


Legen Sie den Namen der Richtlinienzuordnung fest, und fügen Sie neue Kriterien hinzu. Geben Sie die im vorherigen Schritt erstellte Dienstvorlage an, und wählen Sie den Gerätetyp aus, auf den diese Vorlage angewendet wird.

In diesem Fall wird Microsoft-Workstation verwendet. Wenn mehrere Richtlinien definiert sind, wird die erste Übereinstimmung verwendet.

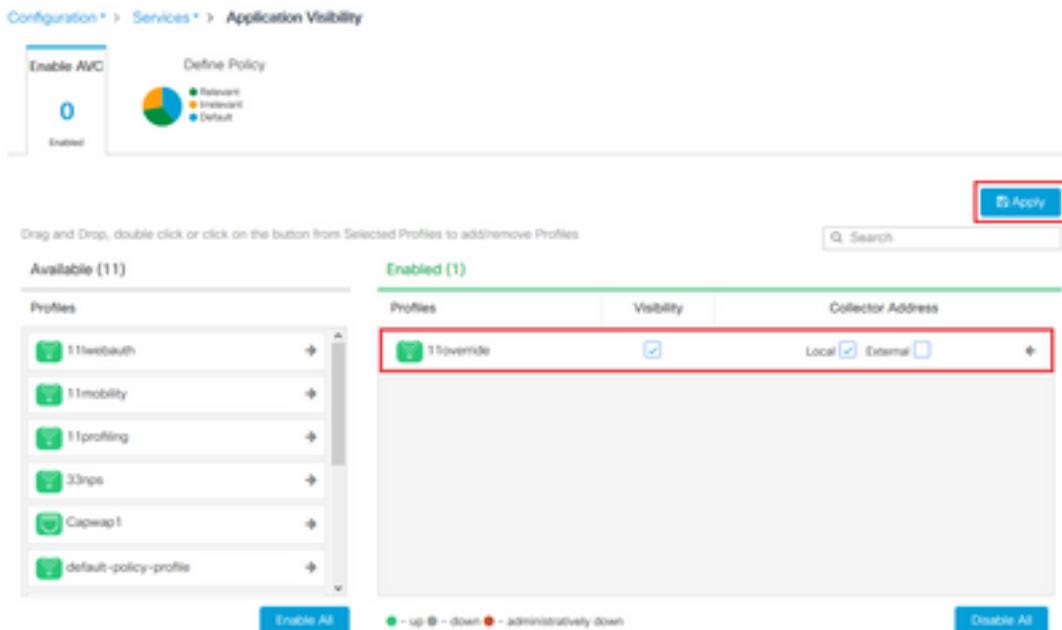
Ein weiterer gängiger Anwendungsfall wäre die Angabe von OUI-basierten Abgleichskriterien. Wenn eine Bereitstellung über eine große Anzahl von Scannern oder Druckern desselben Modells verfügt, verfügen diese in der Regel über dieselbe MAC-OUI.

Hiermit kann eine bestimmte QoS DSCP-Markierung oder eine ACL angewendet werden:

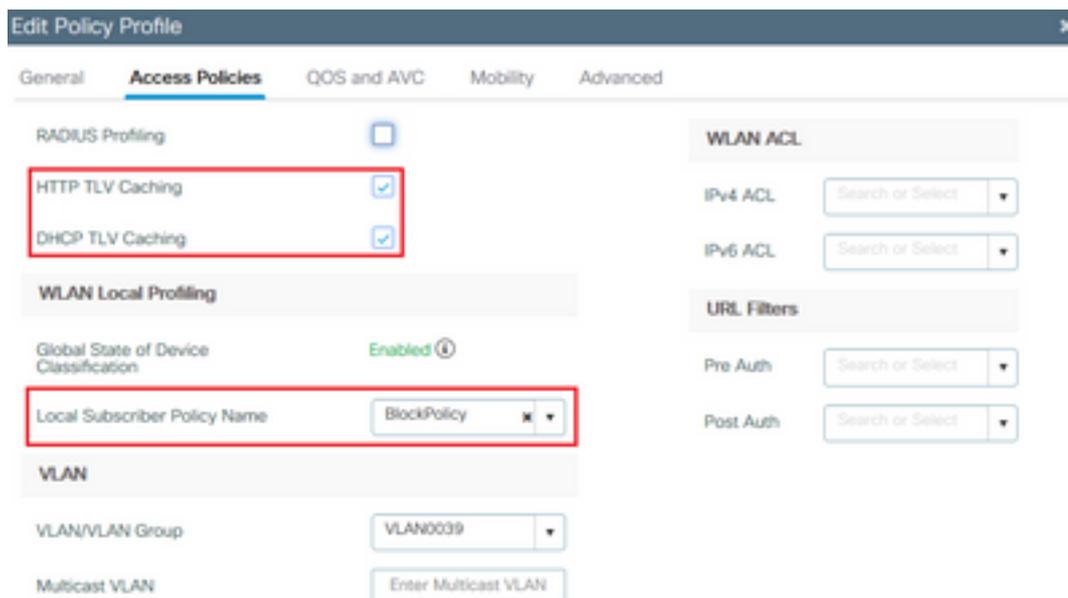


Damit der WLC den Datenverkehr auf YouTube und Facebook erkennen kann, muss die Anwendungstransparenz aktiviert sein.

Navigieren Sie zu **Konfiguration > Services > Anwendungstransparenz** eErmöglichen Sie Transparenz für das Richtlinienprofil Ihres WLAN:



Überprüfen Sie, ob unter dem Richtlinienprofil die HTTP TLV-Caching-, DHCP TLV-Caching- und globale Geräteklassifizierung aktiviert sind und ob die lokale Teilnehmerrichtlinie auf die lokale Richtlinienzuordnung verweist, die in einem der vorherigen Schritte erstellt wurde:



Nachdem der Client eine Verbindung hergestellt hat, kann überprüft werden, ob die lokale Richtlinie angewendet wurde, und getestet werden, ob YouTube und Facebook tatsächlich blockiert sind.

Die Ausgabe der MAC-Adresse [MAC_ADDR] des Show Wireless-Clients enthält:

```

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_1loVERRIDE_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-Profilerstellung für erweiterte Policy Sets in der Cisco ISE

Bei aktivierter RADIUS-Profilerstellung leitet der WLC Profilerstellungsinformationen an die ISE weiter. Basierend auf diesen Informationen können erweiterte Authentifizierungs- und Autorisierungsregeln erstellt werden.

Dieser Artikel behandelt nicht die ISE-Konfiguration. Weitere Informationen finden Sie im [Cisco ISE Profiling Design Guide](#).

Für diesen Workflow muss in der Regel CoA verwendet werden. Stellen Sie deshalb sicher, dass er auf dem 9800 WLC aktiviert ist.

Profilierung in FlexConnect-Bereitstellungen

Zentrale Authentifizierung, lokales Switching

In dieser Konfiguration funktionieren sowohl die lokale als auch die RADIUS-Profilerstellung weiterhin genau wie in den vorherigen Kapiteln beschrieben. Wenn der AP in den Standalone-Modus wechselt (die Verbindung des AP mit dem WLC wird unterbrochen), funktioniert die Erstellung der Geräteprofile nicht mehr, und es können keine neuen Clients eine Verbindung herstellen.

Lokale Authentifizierung, lokales Switching

Wenn sich der AP im verbundenen Modus befindet (der AP ist mit dem WLC verbunden), wird die Profilerstellung fortgesetzt (der AP sendet eine Kopie der Client-DHCP-Pakete an den WLC, um den Profilerstellungsprozess durchzuführen).

Obwohl die Profilerstellung funktioniert, können Profilerstellungsinformationen nicht für lokale Richtlinienkonfigurationen oder RADIUS-Profilerstellungsregeln verwendet werden, da die Authentifizierung lokal auf dem Access Point ausgeführt wird.

Fehlerbehebung

Radioaktive Spuren

Die einfachste Methode zur Fehlerbehebung bei der Client-Profilerstellung auf dem WLC sind radioaktive Spuren. Navigieren Sie zu **Troubleshooting > Radioactive Trace**, geben Sie die MAC-Adresse des Client-Wireless-Adapters ein, und klicken Sie auf 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

Verbinden Sie den Client mit dem Netzwerk, und warten Sie, bis der Ausführungsstatus erreicht ist. Stoppen Sie die Ablaufverfolgungen, und klicken Sie auf **Generate (Generieren)**. Stellen Sie sicher, dass interne Protokolle aktiviert sind (diese Option existiert nur in Versionen 17.1.1 und höher):

Enter time interval ×

Enable Internal Logs

Generate logs for last 10 minutes

30 minutes

1 hour

since last boot

Relevante Schnipsel aus der radioaktiven Spur finden Sie unten:

Client, der von WLC als Microsoft-Workstation profiliert wird:

```

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 der Geräteklassifizierung:

```
(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-Suche nach der Geräteklassifizierung im Cache:

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

WLC wendet lokale Richtlinie basierend auf Klassifizierung an:

```
(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 sendet Abrechnungspakete, die das DHCP- und das HTTP-Profiling-Attribut enthalten:

```
[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
```

Paketerfassung

In einer zentral gesteuerten Bereitstellung kann die Paketerfassung auf dem WLC selbst durchgeführt werden. Navigieren Sie zu **Troubleshooting > Packet Capture**, und erstellen Sie einen neuen Erfassungspunkt auf einer der Schnittstellen, die von diesem Client verwendet werden.

Für die Erfassung auf dem VLAN ist eine SVI erforderlich. Andernfalls wird die Erfassung auf dem physischen Port selbst durchgeführt.

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	←
--	---

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.