9800ワイヤレスLANコントローラでのクライアントプロファイリングのデモ

内容

概要

このドキュメントでは、Cisco Catalyst 9800ワイヤレスLANコントローラでのデバイス分類とプロファイリングの動作について説明します。

使用するコンポーネント

- 17.2.1イメージを実行する9800 CL WLC
- 1815iアクセスポイント
- Windows 10 Proワイヤレスクライアント
- Cisco ISE 2.7

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

プロファイルプロセス

この記事では、Cisco Catalyst 9800ワイヤレスLANコントローラでデバイスの分類とプロファイリングがどのように機能するかについて詳しく説明し、潜在的な使用例、設定例、およびトラブルシューティングに必要な手順について説明します。

デバイスプロファイリングは、ワイヤレスインフラストラクチャに参加したワイヤレスクライアントに関する追加情報を見つける方法を提供する機能です。

デバイスのプロファイリングが実行されると、そのプロファイルを使用してさまざまなローカルポリシーを適用したり、特定のRADIUSサーバルールに一致させることができます。

Cisco 9800 WLCは、次の3種類のデバイスプロファイリングを実行できます。

1. MACアドレスOUI
2. DHCP
3. HTTP

MACアドレスOUIプロファイリング

MACアドレスは、各ワイヤレス（および有線）ネットワークインターフェイスの一意の識別子です。通常は48ビットの数値で、16進数形式(MM:MM:MM:SS:SS:SS)で表記されます。

最初の24ビット（または3オクテット）はOUI(Organizational Unique Identifier)と呼ばれ、ベンダーまたは製造元を一意に識別します。

これらはIEEEから購入され、IEEEによって割り当てられます。1つのベンダーまたは製造業者が複数のOUIを購入できます。

例：

```
00:0D:4B - owned by Roku, LLC
90:78:B2 - owned by Xiaomi Communications Co Ltd
```

ワイヤレスクライアントがアクセスポイントに関連付けられると、WLCはOUIルックアップを実行して製造元を特定します。

Flexconnectローカルスイッチングの導入では、APは引き続き関連クライアント情報（DHCPパケットやクライアントMACアドレスなど）をWLCにリレーします。

OUIのみに基づくプロファイリングは非常に限られており、デバイスを特定のブランドとして分類することは可能ですが、ラップトップとスマートフォンを区別することはできません。

ローカルで管理されるMACアドレスの問題

プライバシーの問題が原因で、多くのメーカーがMACランダム化機能をデバイスに実装し始めました。

ローカルで管理されるMACアドレスはランダムに生成され、アドレスの最初のオクテットの2番目の最下位ビットが1に設定されます。

このビットは、MACアドレスが実際にはランダムに生成されたものであることを通知するフラグとして機能します。

ローカルで管理されるMACアドレスには、次の4つの形式があります（xは任意の16進数値です）。

```
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デバイスは、デフォルトで、新しいSSIDネットワークに接続するたびに、ランダムに生成されたローカル管理MACアドレスを使用します。

この機能は、アドレスがランダム化されたことをコントローラが認識し、ルックアップを実行しないため、OUIベースのデバイス分類を完全に無効にします。

DHCPプロファイリング

DHCPプロファイリングは、ワイヤレスクライアントが送信しているDHCPパケットを調査することによってWLCによって実行されます。

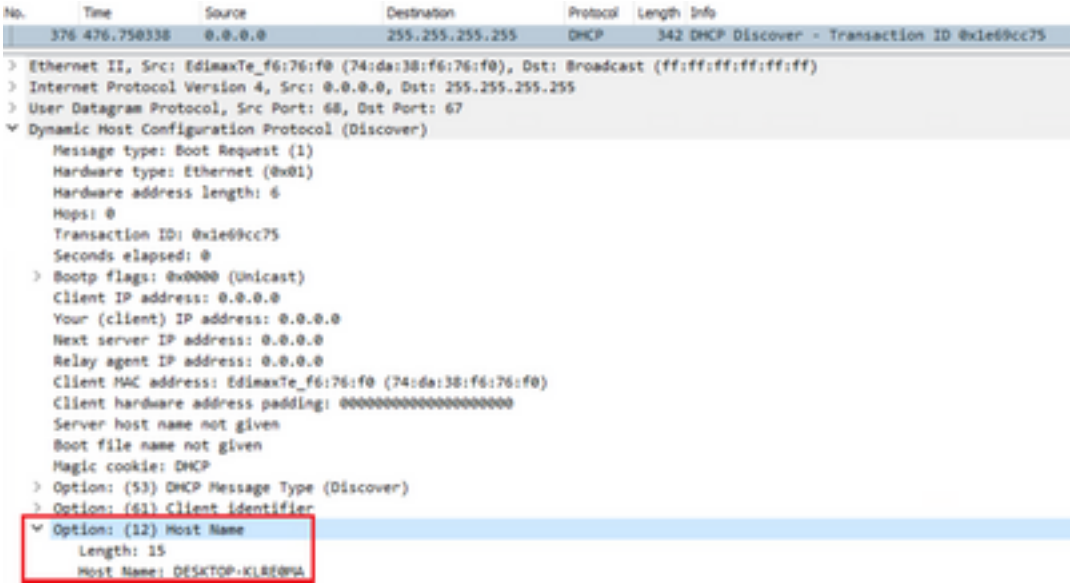
DHCPプロファイリングを使用してデバイスを分類した場合、**show wireless client mac-address [MAC_ADDR] detailed**コマンドの出力には次が含まれます。

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

WLCは、ワイヤレスクライアントから送信されるパケットの中のいくつかのDHCPオプションフィールドを検査します。

1.オプション12：ホスト名

このオプションはクライアントのホスト名を表し、DHCP DiscoverおよびDHCP Requestパケットで確認できます。



2.オプション60：ベンダークラスID

このオプションは、DHCP DiscoverおよびRequestパケットにも含まれています。

このオプションを使用すると、クライアントはDHCPサーバに対して自身を識別し、特定のベンダークラスIDを持つクライアントにのみ応答するようにサーバを設定できます。

このオプションは、ネットワーク内のアクセスポイントを特定し、それに対してオプション43でのみ応答するために最も一般的に使用されます。

ベンダークラスIDの例

- "MSFT 5.0" すべてのWindows 2000クライアント（以降）
- "MSFT 98" すべてのWindows 98およびMeクライアント用
- 「MSFT」 すべてのWindows 98、Me、および2000クライアント用

Apple MacBookデバイスは、デフォルトではオプション60を送信しません。

Windows 10クライアントからのパケットキャプチャ例：

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

3.オプション55：パラメータ要求リスト

[DHCPパラメータ要求リスト(DHCP Parameter Request List)]オプションには、DHCPクライアントがDHCPサーバに要求する設定パラメータ（オプションコード）が含まれています。カンマ区切り形式で記述された文字列です（例：1,15,43）。

生成されるデータはベンダーに依存し、複数のデバイスタイプで複製できるため、完全なソリューションではありません。

たとえば、Windows 10デバイスは常にデフォルトで特定のパラメータリストを要求します。AppleのiPhoneとiPadは、異なるパラメータセットを使用し、それらを分類することができます。

Windows 10クライアントからのキャプチャ例：

```
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
```

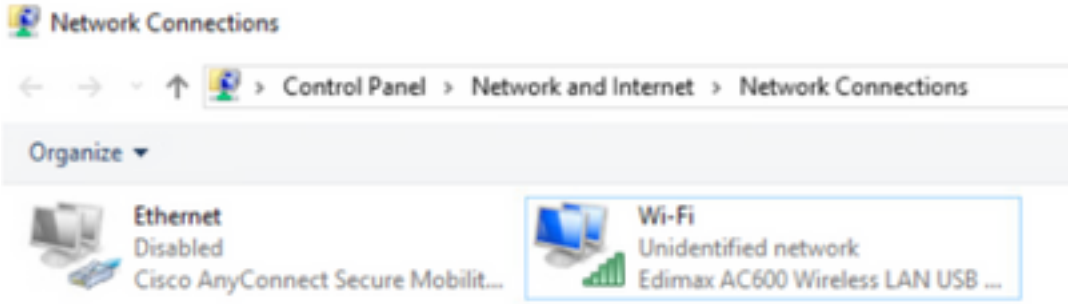
4.オプション77：ユーザクラス

ユーザクラスは、デフォルトでは最も一般的に使用されないオプションであり、クライアントを手動で設定する必要があります。たとえば、Windowsマシンでこのオプションを設定するには、

次のコマンドを使用します。

```
ipconfig /setclassid “ADAPTER_NAME” “USER_CLASS_STRING”
```

アダプタ名は、コントロールパネルの[ネットワークと共有センター]で確認できます。



CMDでWindows 10クライアント用のDHCPオプション66を設定します（管理者権限が必要）。

```
C:\Windows\system32>ipconfig /setclassid "Wi-Fi" "test_user_class"

Windows IP Configuration

Successfully set the DHCPv4 class id for adapter Wi-Fi.
```

Windowsのオプション66の実装により、Wiresharkはこのオプションをデコードできず、オプション66の後に来るパケットの一部が不正な形式として表示されます。

```
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プロファイリング

HTTPプロファイリングは、9800 WLCがサポートする最も高度なプロファイリング方法であり、最も詳細なデバイス分類を提供します。

クライアントをHTTPプロファイルするには、「Run」状態にしてHTTP GET要求を実行する必要があります。

WLCが要求を代行受信し、パケットのHTTPヘッダーの「User-Agent」フィールドを調べます。

このフィールドには、分類に使用できるワイヤレスクライアントに関する追加情報が含まれています。

デフォルトでは、ほぼすべてのメーカーが、ワイヤレスクライアントがインターネット接続チェックを実行する機能を実装しています。

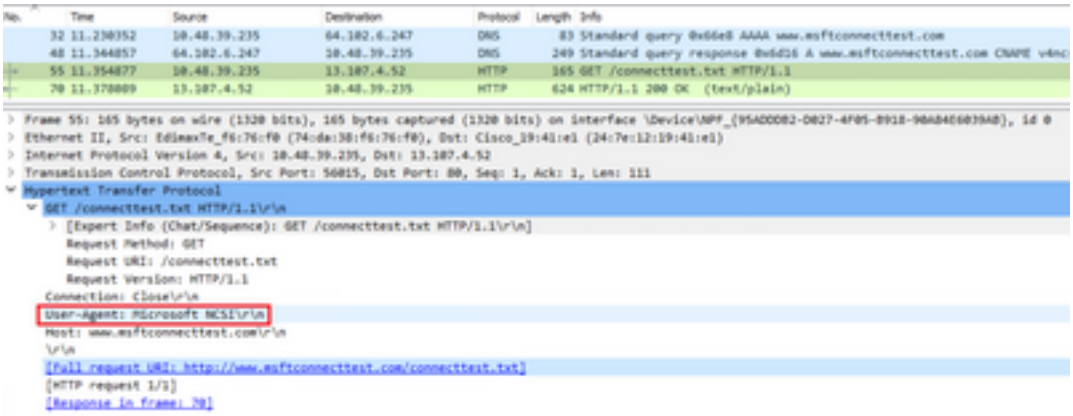
このチェックは、自動ゲストポータル検出にも使用されます。 デバイスがステータスコード200(OK)のHTTP応答を受信した場合は、WLANがwebauthで保護されていないことを意味します。

その場合、WLCは残りの認証を実行するために必要な代行受信を実行します。 この最初のHTTP GETは、WLCがデバイスのプロファイリングに使用できる唯一のHTTP GETではありません。

後続のHTTP要求はすべてWLCによって検査され、さらに詳細な分類が行われる可能性があります。

Windows 10デバイスは、ドメイン**msftconnecttest.com**を使用してこのテストを実行します。 Appleデバイスは**captive.apple.com**を使用しますが、Androidデバイスは通常**connectivitycheck.gstatic.com**を使用します。

このチェックを実行しているWindows 10クライアントのパケットキャプチャは次のとおりです。 [User Agent]フィールドに**Microsoft NCSI**が入力され、クライアントがWLC上で**Microsoft-Workstation**としてプロファイルされます。



HTTP経由でプロファイルされたクライアントの**show wireless client mac-address [MAC_ADDR] detailed**の出力例を次に示します。

```
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プロファイリング

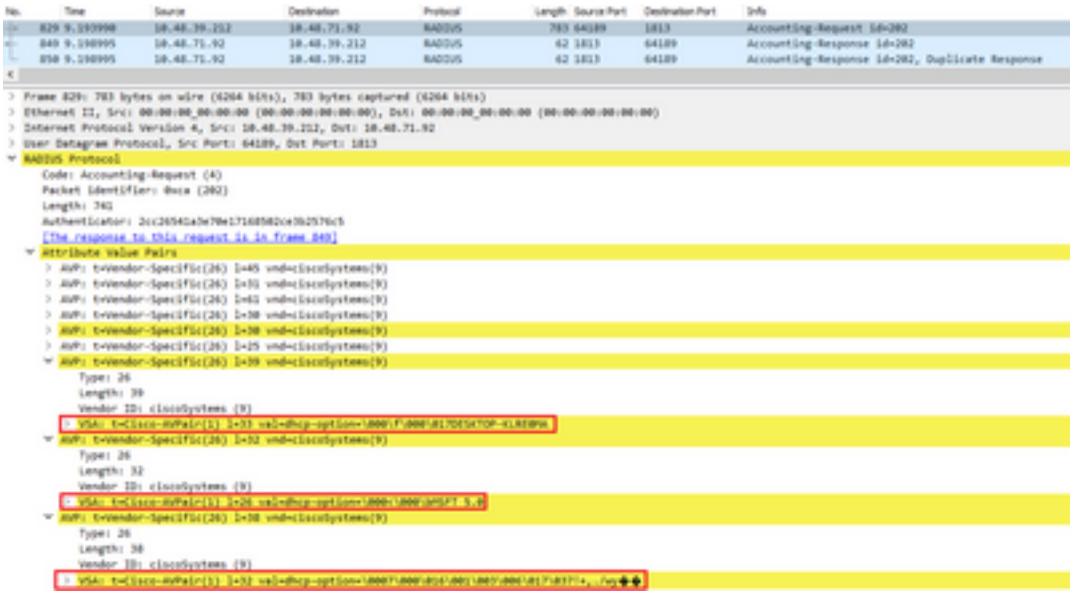
デバイスの分類に使用される方法に関しては、ローカルとRADIUSのプロファイリングに違いはありません。

Radiusプロファイリングが有効な場合、WLCはベンダー固有の特定のRADIUS属性セットを使用してデバイスについて学習した情報をRADIUSサーバに転送します。

DHCP RADIUSプロファイリング

DHCPプロファイリングによって取得された情報は、ベンダー固有のRADIUS AVPairとしてアカウンティング要求内のRADIUSサーバに送信されます **cisco-av-pair:dhcp-option=<DHCP option>**

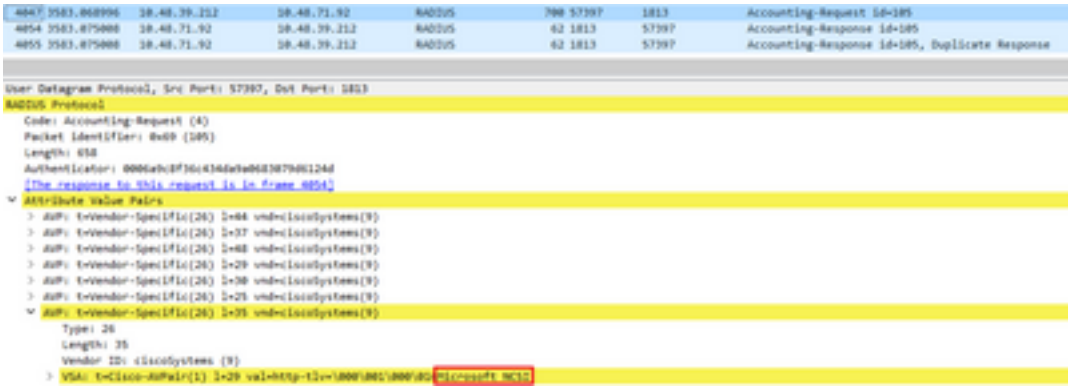
DHCPオプション12、60、および55のAVPairsを示すアカウンティング要求パケットの例。 WLCからRADIUSサーバにそれぞれ送信されます（Wiresharkのデコードにより、オプション55の値が破損している可能性があります）。



HTTP RADIUSプロファイリング

HTTPプロファイリング（HTTP GET要求のヘッダーのUser-Agentフィールド）によって取得された情報は、ベンダー固有のRADIUS AVPairとしてアカウンティング要求内のRADIUSサーバに送信されます **cisco-av-pair:http-tlv=User-Agent=<user-agent>**

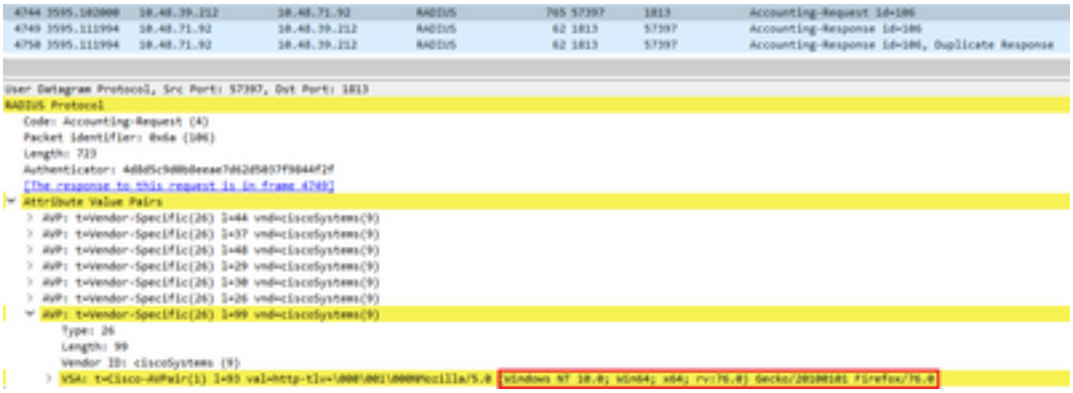
初期接続チェックHTTP GETパケットには、User-Agentフィールドに多くの情報が含まれず、「Microsoft NCSI」のみが含まれます。この単純な値をRADIUSサーバに転送するアカウンティングパケットの例を示します。



ユーザがインターネットの閲覧を開始し、追加のHTTP GET要求を作成すると、インターネットに関する詳細情報を取得できます。

WLCは、このクライアントの新しいユーザエージェント値を検出すると、追加のアカウンティングパケットをISEに送信します。

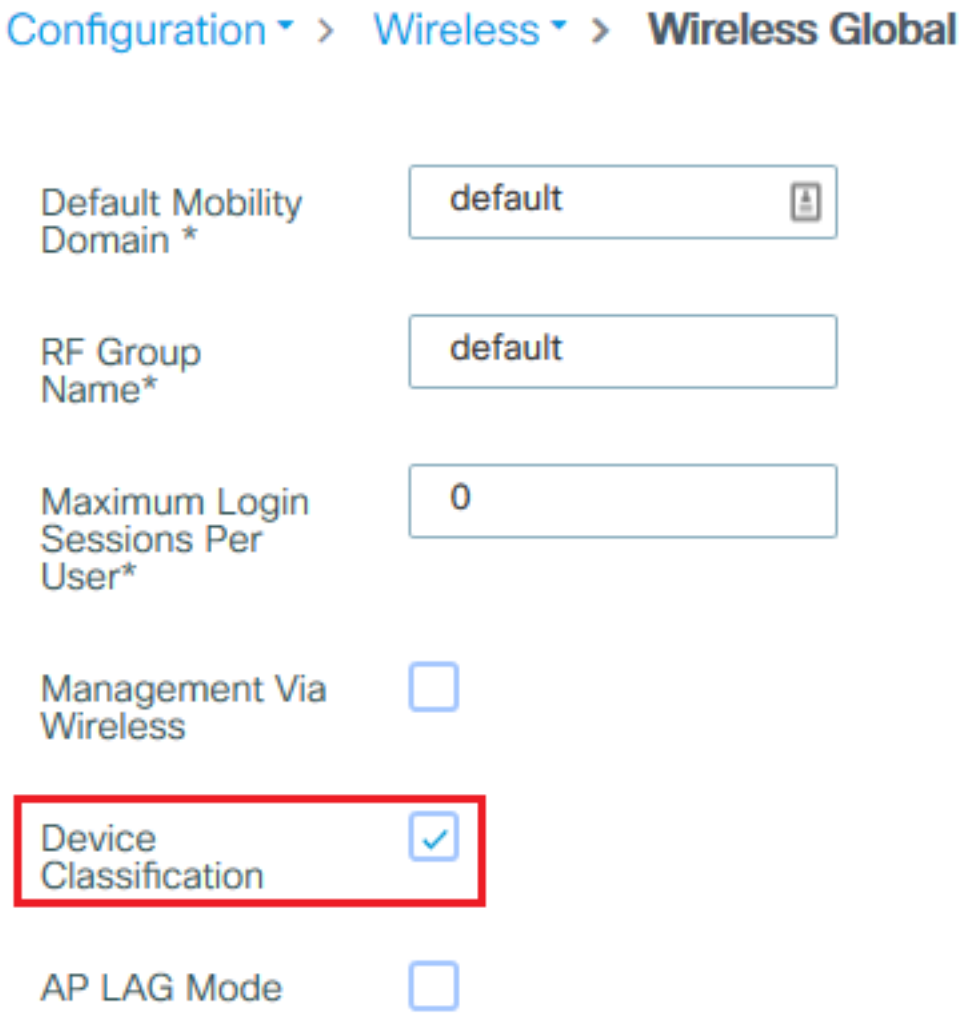
この例では、クライアントがWindows 10 64ビットとFirefox 76を使用していることを確認できます。



9800 WLCでのプロファイリングの設定

ローカルプロファイリング設定

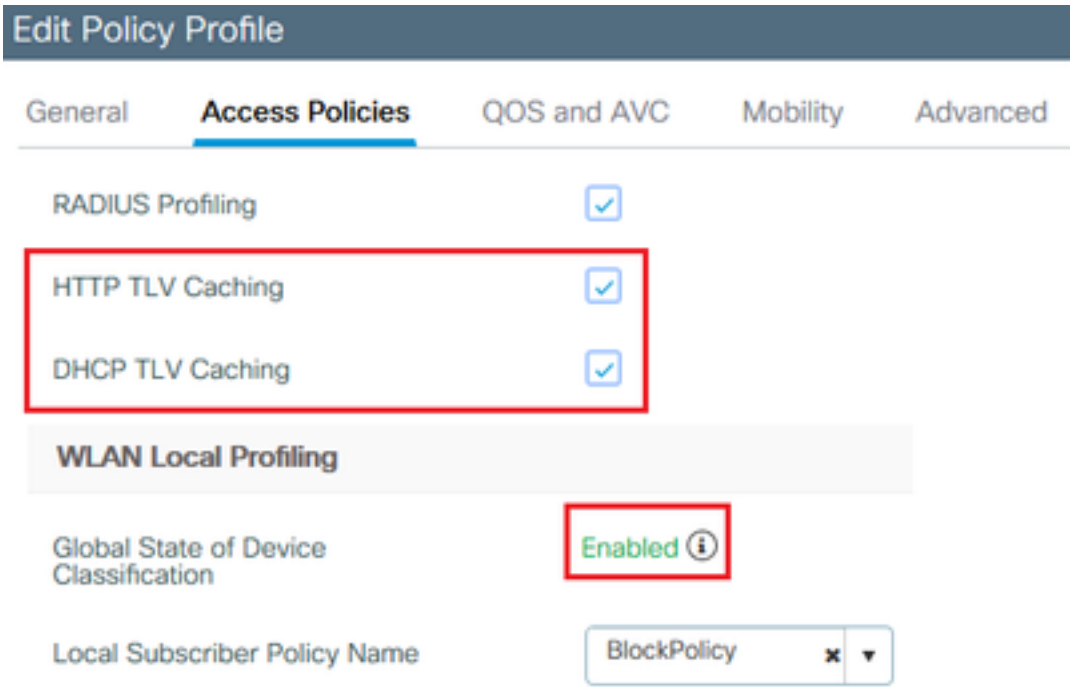
ローカルプロファイリングを機能させるには、[Configuration] > [Wireless] > [Wireless Global]で[Device Classification]を有効にします。このオプションは、MAC OUI、HTTP、およびDHCPプロファイリングを同時に有効にします。



また、[Policy configuration]で、[HTTP TLV Caching]と[DHCP TLV Caching]を有効にできます。WLCは、プロファイルがない場合でもプロファイリングを実行します。

これらのオプションを有効にすると、WLCはこのクライアントに関して以前に学習した情報をキ

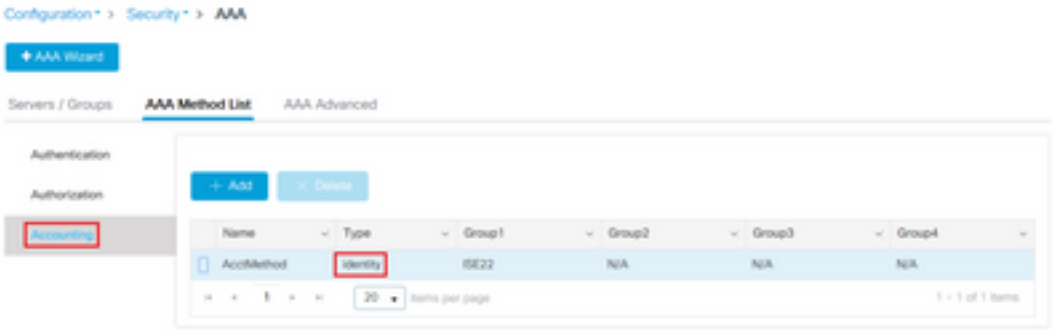
ャッシュし、このデバイスによって生成された追加のパケットを検査する必要がなくなります。



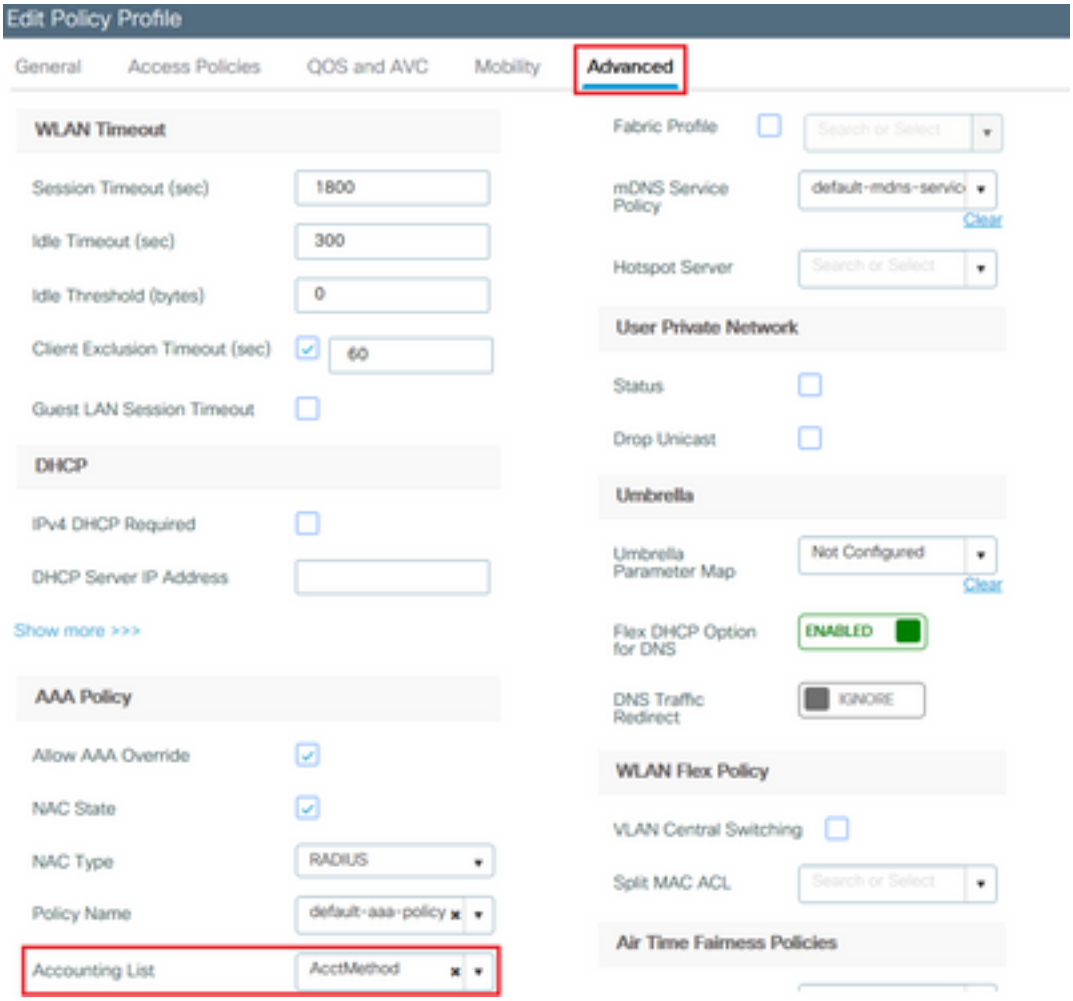
RADIUSプロファイリングの設定

RADIUSプロファイリングが機能するためには、（「ローカルプロファイリングの設定」で説明したように）デバイス分類をグローバルに有効にする以外に、次の作業が必要です。

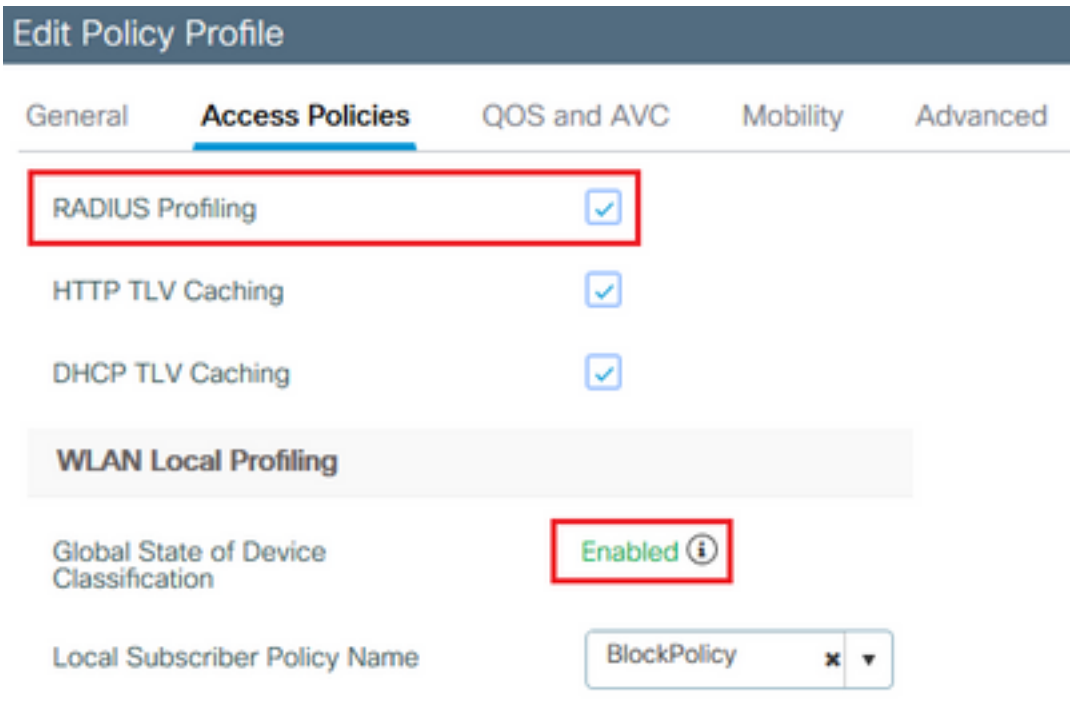
1. RADIUSサーバを指す「ID」タイプを使用して、AAAアカウンティング方式を設定します。



2. [Configuration] > [**Tags & Profiles] > [Policy] > [Policy_Name] > [Advanced]でアカウンティング方式を追加する必要があります。**



3.最後に、[Configuration] > [Tags & Profiles] > [Policy]で[RADIUS Profiling]チェックボックスをオンにする必要があります。このチェックボックスは、HTTPとDHCPの両方のRADIUSプロファイリングを有効にします（古いAireOS WLCには2つの個別のチェックボックスがありました）。



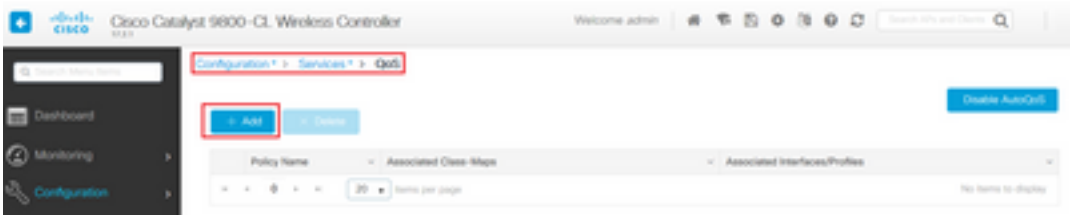
プロファイリングの使用例

ローカルプロファイリング分類に基づくローカルポリシーの適用

この設定例では、Windows-Workstationとしてプロファイリングされたデバイスだけに適用される、YouTubeおよびFacebookアクセスをブロックするを使用したローカルポリシーの設定を示します。

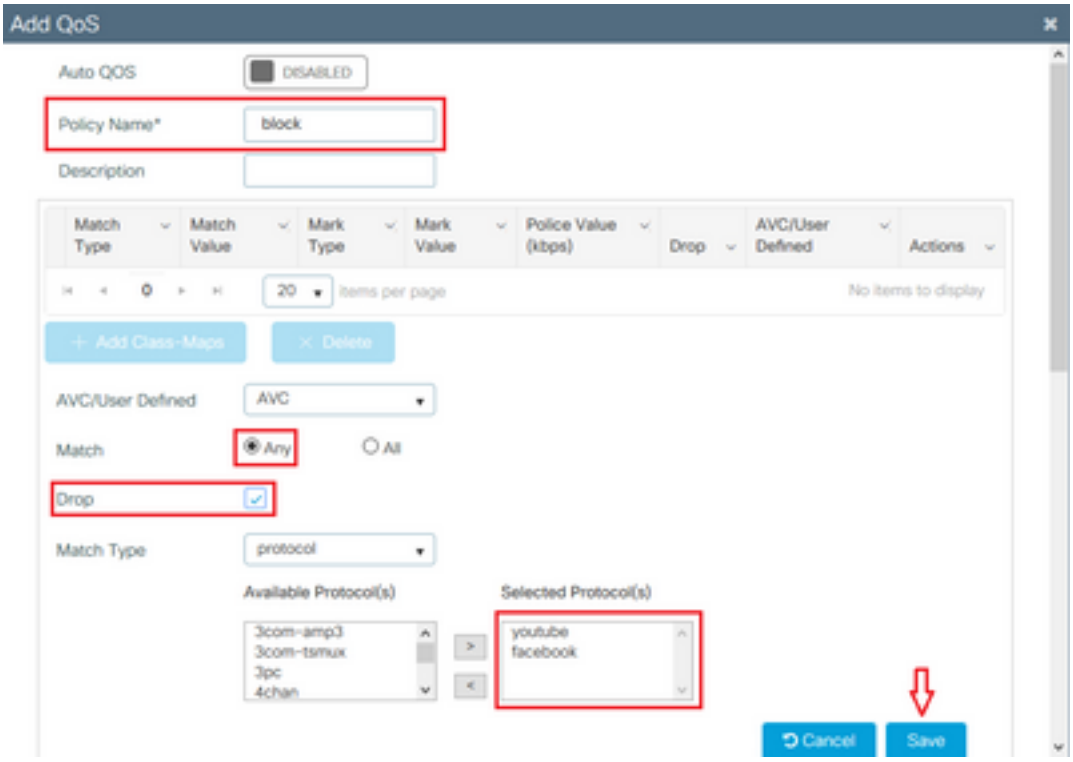
わずかな変更を加えると、この設定を変更して、たとえばワイヤレス電話だけに特定のDSCPマーキングを設定できます。

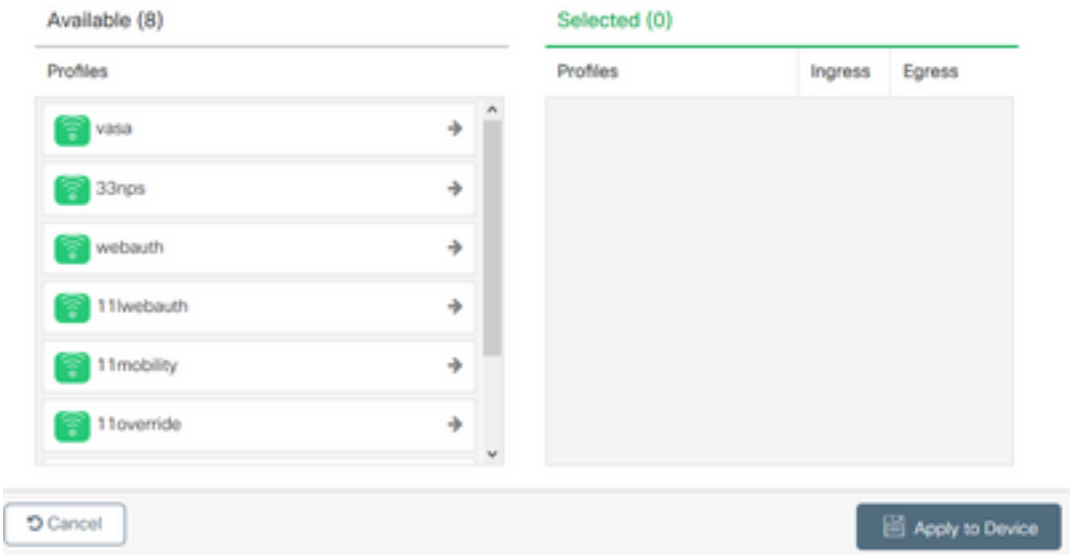
[Configuration] > [Services] > [QoS] に移動して、QoSプロファイルを作成します。[add]をクリックして新しいポリシーを作成します。



ポリシー名を指定し、新しいクラスマップを追加します。使用可能なプロトコルから、ブロックする必要があるプロトコル、DSCPがマークされているプロトコル、または帯域幅が制限されているプロトコルを選択します。

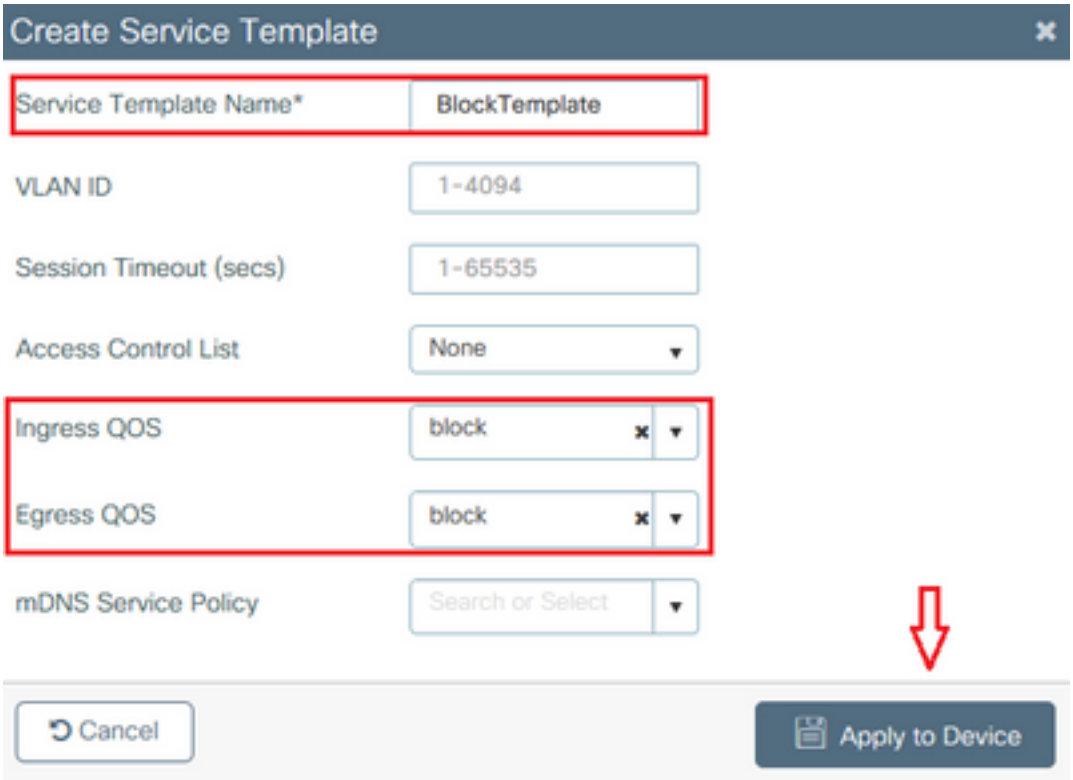
この例では、YouTubeとFacebookがブロックされています。QoSウィンドウの下部にあるPolicy Profilesには、このQoSプロファイルが適用されないことを確認してください。





[Configuration] > [Security] > [Local Policy] に移動し、新しいサービステンプレートを作成します。

前の手順で作成した入力および出力QoSプロファイルを指定します。この手順では、アクセスリストも適用できます。VLANを変更する必要がない場合は、vlanフィールドを空のままにします。



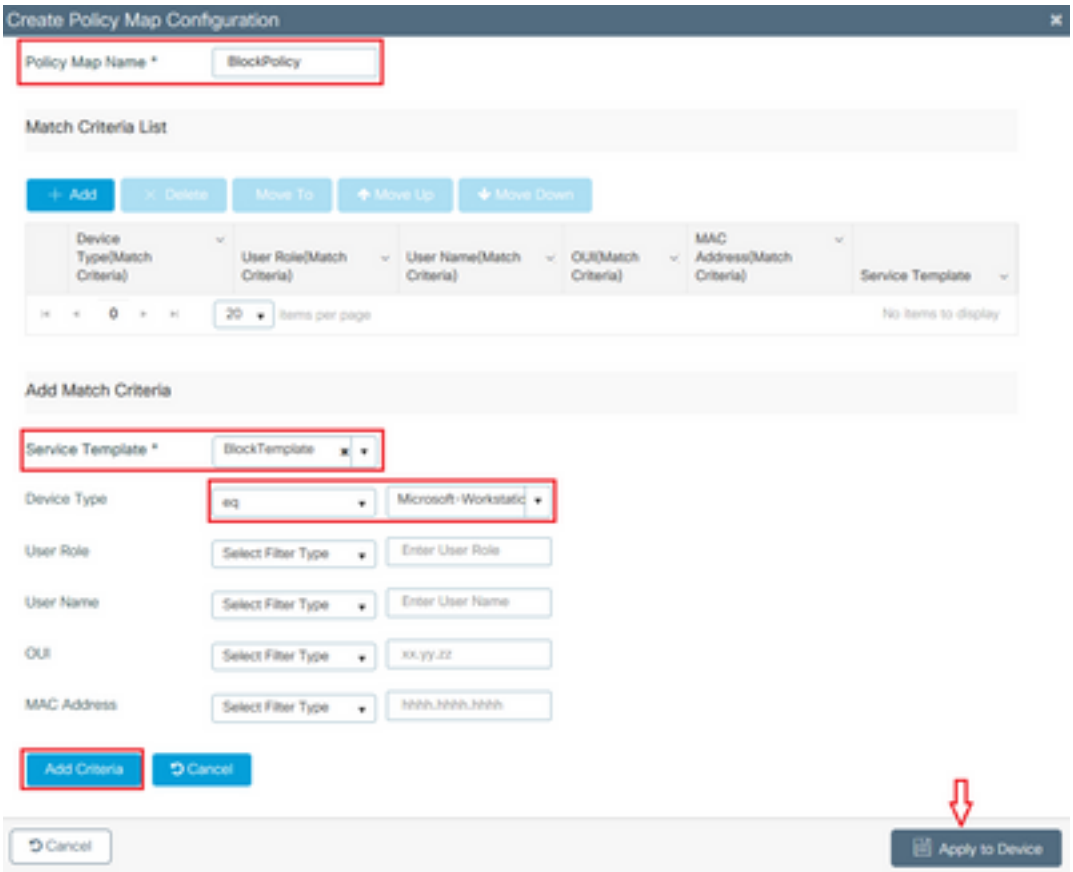
[Policy Map]タブに移動し、[add]をクリックします。

ポリシーマップ名を設定し、新しい基準を追加します。前の手順で作成したサービステンプレートを指定し、このテンプレートを適用するデバイスタイプを選択します。

この場合、Microsoft-Workstationが使用されます。複数のポリシーが定義されている場合は、最初の一致が使用されます。

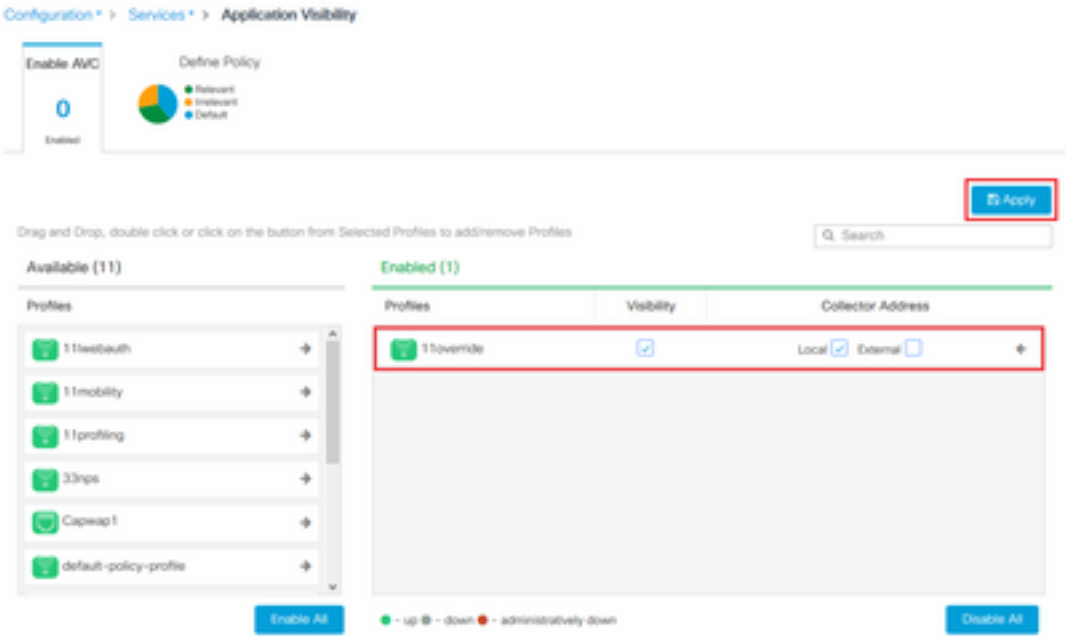
もう1つの一般的な使用例は、OUIベースの一致基準を指定することです。導入環境に同じモデルのスキャナまたはプリンタが多数存在する場合、通常は同じMAC OUIを使用します。

これは、特定のQoS DSCPマーキングまたはACLを適用するために使用できます。

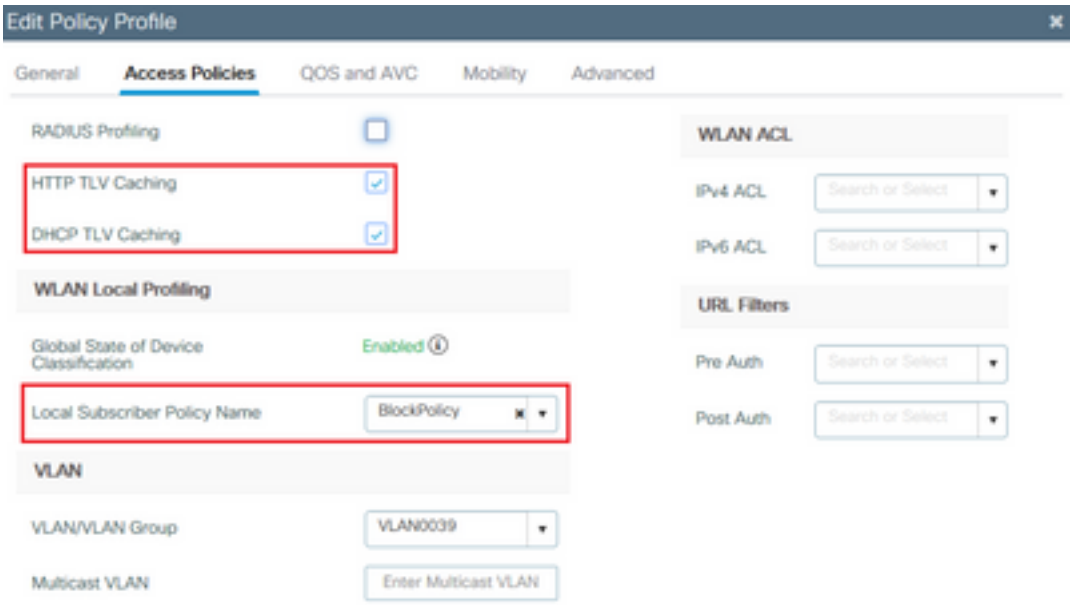


WLCがYouTubeおよびFacebookトラフィックを認識できるようにするには、アプリケーションの可視性をオンにする必要があります。

[Configuration] > [Services] > [Application Visibility] に移動します。wlanのポリシープロファイルの可視性を有効にします。



ポリシープロファイルで[HTTP TLV Caching]、[DHCP TLV Caching]、[Global device Classification]が有効になっており、ローカルサブスクライバポリシーが、前のいずれかの手順で作成されたローカルポリシーマップを指していることを確認します。



クライアントが接続すると、ローカルポリシーが適用されているかどうかを確認し、YouTubeとFacebookが実際にブロックされているかどうかをテストできます。

show wireless client mac-address [MAC_ADDR] detailedの出力には、次が含まれます。

```
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
```

Cisco ISEの高度なポリシーセットのRADIUSプロファイリング

RADIUSプロファイリングを有効にすると、WLCはプロファイリング情報をISEに転送します。この情報に基づいて、高度な認証および許可ルールを作成できます。

この記事では、ISEの設定については説明しません。詳細については、『Cisco ISEプロファイリング設計ガイド』を参照してください。

このワークフローでは通常、CoAを使用する必要があるため、9800 WLCでCoAが有効になっていることを確認してください。

FlexConnectの導入におけるプロファイリング

中央認証、ローカル スイッチング

この設定では、ローカルとRADIUSの両方のプロファイリングが、前の章で説明したとおりに動作し続けます。APがスタンドアロンモードになると（APがWLCへの接続を失うと）、デバイスのプロファイリングは機能しなくなり、新しいクライアントは接続できなくなります。

ローカル認証、ローカル スイッチング

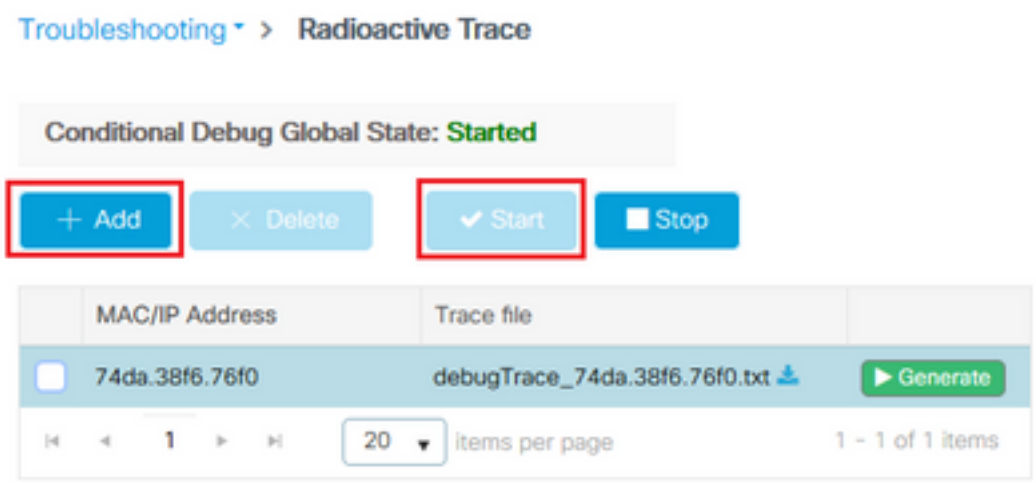
APが接続モード（APがWLCに加入）の場合、プロファイリングは引き続き動作します（APはクライアントDHCPパケットのコピーをWLCに送信して、プロファイリングプロセスを実行します）。

プロファイリングが機能しても、認証はAP上でローカルに実行されるため、プロファイリング情報をローカルポリシー設定やRADIUSプロファイリングルールに使用することはできません。

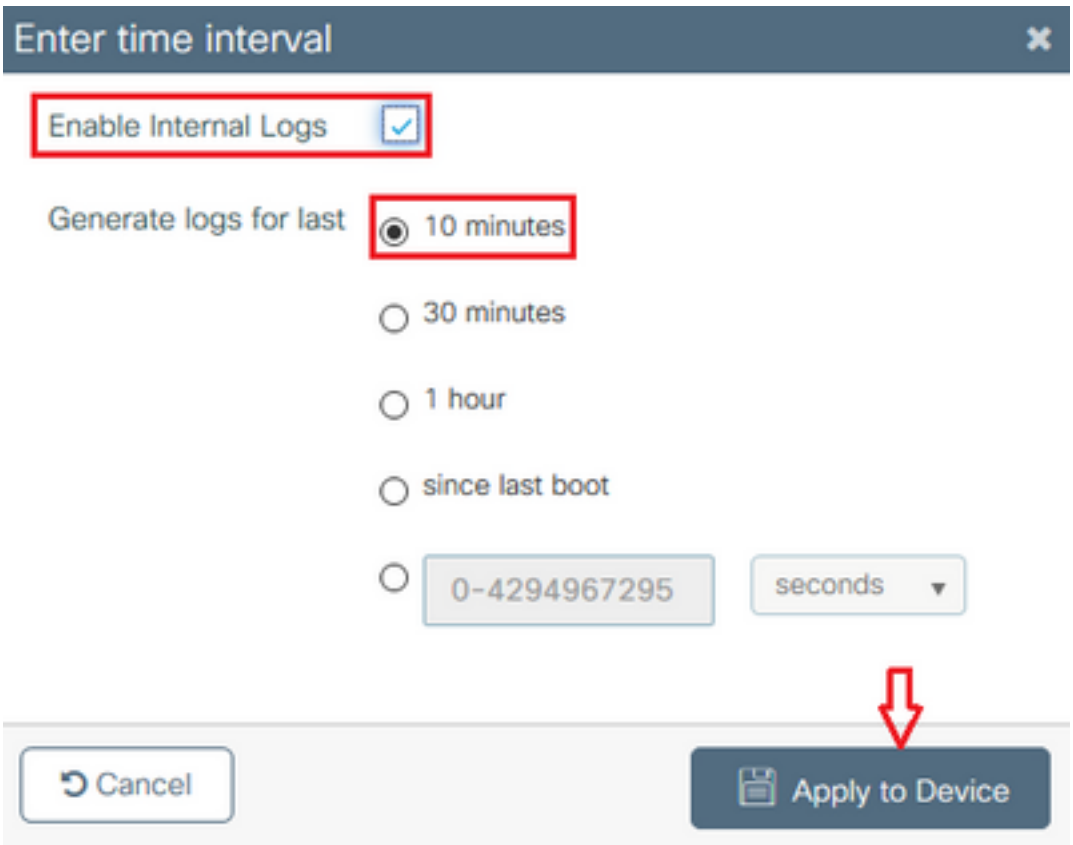
トラブルシューティング

放射能痕跡

WLCでクライアントプロファイリングをトラブルシューティングする最も簡単な方法は、放射性トレースを使用することです。[Troubleshooting] > [Radioactive Trace] に移動し、クライアントワイヤレスアダプタのMACアドレスを入力して、[Start] をクリックします。



クライアントをネットワークに接続し、実行状態になるまで待ちます。トレースを停止し、**Generate**をクリックします。[Internal Logs]が有効になっていることを確認します（このオプションは17.1.1リリース以降にのみ存在します）。



以下に、放射性物質の痕跡から得られた関連する断片を示す：

WLCによってMicrosoft-Workstationとしてプロファイルされるクライアント：

```
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
```

デバイス分類をキャッシュするWLC:

```
(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
```

キャッシュ内のデバイス分類を検出するWLC:

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

分類に基づいてローカルポリシーを適用するWLC:

```
(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
```

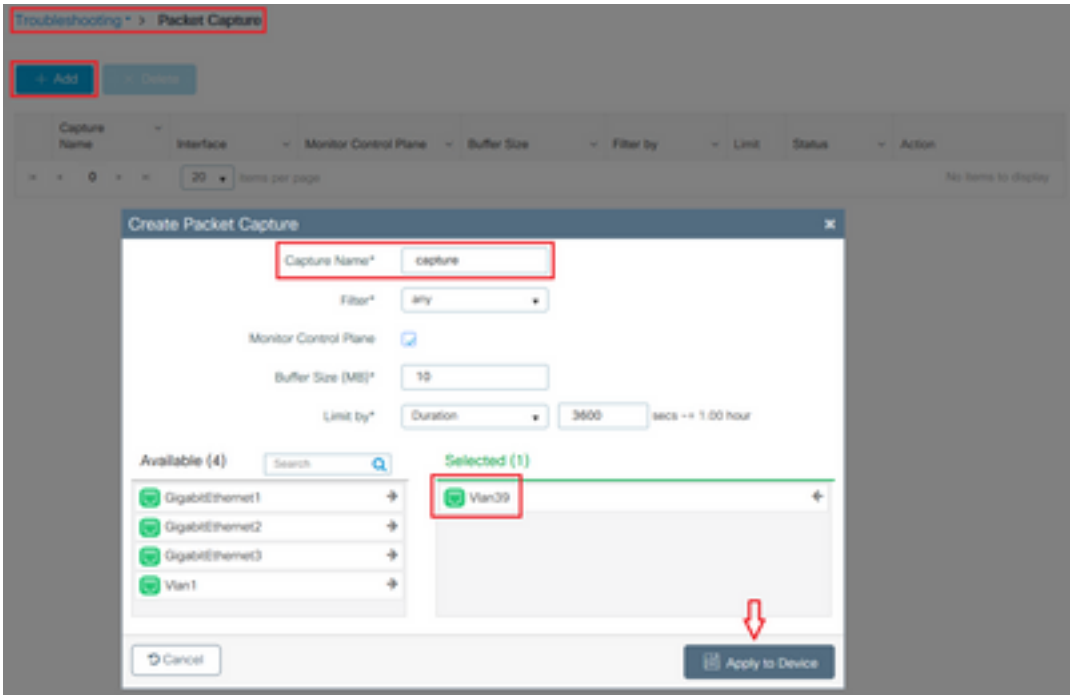
DHCPおよびHTTPプロファイリング属性を含むアカウンティングパケットを送信するWLC:

```
[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
```

パケット キャプチャ

中央でスイッチされる展開では、パケットキャプチャはWLC自体で実行できます。[Troubleshooting] > [Packet Capture] に移動し、このクライアントが使用しているインターフェイスの1つに新しいキャプチャポイントを作成します。

VLANでキャプチャを実行するには、VLAN上にSVIが必要です。SVIが存在しない場合は、物理ポート自体でキャプチャを実行します


Troubleshooting
Packet Capture
Add
Delete
Capture Name
Interface
Monitor Control Plane
Buffer Size
Filter by
Limit
Status
Action
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)
Search
GigabitEthernet1
GigabitEthernet2
GigabitEthernet3
Vlan1
Selected (1)
Vlan39
Cancel
Apply to Device

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。