Overview

Cisco currently offers a rich set of features which provides device identification, onboarding, posture, and policy, through ISE. WLC has been enhanced with some of these capabilities. This document deals with basic configuration of device profiling and policy implementation through Cisco WLC.

This new feature (Profiling and Policy) on WLC does the profiling of devices based on protocols like HTTP and DHCP to identify the end devices on the network. Users can configure device based policies and enforce per user or per device policy on the network. The WLC will also display statistics based on per user or per device end points and policies applicable per device.

Wireless device profiling and policy classification engine enables simple BYOD deployments with visibility and user/wireless device policy integrated into the wireless controller.
### Scope, Objectives, and Expectations

Profiling and policy enforcement allows profiling of mobile devices and basic onboarding of the profiled devices to a specific VLAN assigns ACL and QoS, or configures session timeout. It can be configured as two separate components. The configuration on the WLC is based on defined parameters specific to clients joining the network. The policy attributes which are of interest are:

- **Role** – Defines the user type or the user group the user belongs to, for example, student or employee.
- **Device** – Defines the type of device, for example, Windows machine, Smart phone, Apple device such as iPad, iPhone and so on.
- **Location** – Defines where the end point is connected on the network. Location represents AP group. APs can be divided or grouped according to the location and policy can be applied per AP group.
- **Time of day** – Allows configuration to be defined at what time of the day end-points are allowed on the network.
- **EAP Type** - Checks what EAP method the client is getting connected to.

The above parameters are configurable as policy match attributes. Once WLC has a match corresponding to the above parameters per end-point, policy enforcement comes into picture. Policy enforcement allows basic device on-boarding of mobile devices based on session attributes such as:

- **VLAN Assignment**
- **ACL**
- **Session Timeout**
- **QoS**
The user can configure these policies and enforce end-points with specified policies. The wireless clients will be profiled based on MAC OUI, DHCP, HTTP user agent (valid Internet is required for successful HTTP profiling). The WLC uses these attributes and predefined classification profiles to identify devices.

### Profiling and Policy Configuration

In 7.5 release, only embedded or built-in profiles are available on the WLC through which it can identify devices.

In later releases, it should be possible to create user-defined profiles, which will take precedence over the embedded profiles. Currently there are 88 built-in profiles and can be viewed through WLC CLI prompt.

Go to WLC and run `show profiling policy summary`. For the purpose of this document we just displayed the first 6 profile.

![show profiling policy summary]

To configure device profiling on a WLAN through GUI, go to the WLAN (here we created WLAN Demo-Employee) and click **Advance**, then enable DHCP by checking the **Required** check box. After enabling the DHCP required option, scroll down and under **Local Client Profiling** enable **DHCP Profiling** and **HTTP Profiling** by checking the respective check boxes and click **Apply**.

---

**Terminology**

<table>
<thead>
<tr>
<th>Term</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>APM</td>
<td>AP Manager Interface</td>
</tr>
<tr>
<td>Dyn</td>
<td>Dynamic Interface</td>
</tr>
<tr>
<td>Mgmt</td>
<td>Management Interface</td>
</tr>
<tr>
<td>Port</td>
<td>Physical Gbps port</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>LAG</td>
<td>Link Aggregation</td>
</tr>
<tr>
<td>VSL</td>
<td>Virtual Switch Link</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual LAN</td>
</tr>
<tr>
<td>SSO</td>
<td>Stateful Switchover</td>
</tr>
<tr>
<td>WiSM-2</td>
<td>Wireless Service Module-2</td>
</tr>
</tbody>
</table>

---

**e.** Sleeping Client–Timeout duration for a specific sleeping client (in hours)
Wireless Device Profiling and Policy Classification Engine on WLC

To configure profiling through ISE use Radius Client Profiling.

Now, try associating a client to the WLAN on which profiling is enabled. In our setup we associated an Apple iPad, an Android device and a Windows machine.

From the WLC main menu bar, navigate to Monitor > Clients and under Device Type column, notice that there are three devices associated to the WLAN and all of them are being profiled. See the below figure – Windows PC as Microsoft-Workstation, iPad as an Apple-iPad and Motorola Zoom as an Android device.

The same can be viewed from CLI as well, run a command `show client summary devicetype` to see the clients being profiled.

We clearly see that the client devices are classified under Device Type.
Creating Policies on WLAN from WLC GUI

Once the policy has been configured you can create policies and apply them on the WLAN. On WLC menu bar, go to Security > Local Policies which will navigate you to the Policy List.

In Policy List page, click New to create a Policy Name. In our set up we are using “Employee-iPad” as a policy-name but you can use any name to define your own policy.

Once the Policy Name is created, click that policy name to configure the rules.
Under **Policy Name**, you can create policies to match a Role, EAP Type and Device Type. You can also define what actions to take related to the Match criteria. In our setup we used Device Type for the Match Criteria but if required, you can use Role or EAP type as well.

To apply the policy based on a user device, go to **Device Type** and scroll down to select the device type from the drop down menu on which you want to enforce policy and then click **Add**.

Here we used Apple-iPad as a device type for **Match Criteria**.

The device type will appear under the **Device List** section.
There are 88 device profiles listed under Device Type, but you can add/list only 16 devices per policy.

Now to apply the appropriate action, choose from the parameters under the Action menu to enforce the Policy. There are five attributes ACL, VLAN ID, QoS Policy, Session Timeout and Sleeping Client Timeout. You can configure these attributes and enforce clients with specified policies. By default the Session timeout is 1800 seconds and Sleeping client timeout is 12 Hrs.

The Sleeping Client refers to the clients already in RUN state after successful web authentication and are allowed to sleep and wakeup without the need to re-authenticate through the login page. The sleep client’s duration for which client needs to be remembered for re-authentication is based on user configuration.

The Sleeping Client timeout configuration set in policy overrides the global sleeping client timeout configuration set on WLAN. These configurations and details are discussed later in this document, refer Appendix-A.

Active Hours menu allows configuration to be defined/set for what time of the day clients are allowed on the network.
For the purpose of ease and demonstration only device parameters and VLAN attributes are used to do profiling and policy enforcement in our setup.

Now Assign a VLAN ID and click Apply.

As discussed in previous sections, we created a separate interface on the WLC when enforcing policy through VLAN attributes. We have VLAN 20 for management and VLAN 22 for Employees iPads and Apple devices. Any iPad or Apple device connecting to a policy enforced WLAN will be redirected to a different VLAN. In the case of the given example, it is VLAN 22.

Mapping a Policy on WLAN

Go to WLANs from WLC menu and click the WLAN ID on which you want the policy to be implemented. As you can see in the WLAN> General tab, Interface/Interface Group is tied to management interface which is on VLAN 20.

From the WLAN edit menu choose the Policy-Mapping tab.
Set the **Priority index** to any value from 1-16. Then select the policy which you already created, from the **Local Policy** drop down menu. To Apply the policy on WLAN click **Add**. The policy will be mapped to WLAN and can be seen under Policy Name.

Now when an iPad associates to a policy enforced WLAN it is redirected to a VLAN tied to that policy. Scrolling down to Security Information will show you the local policy applied.
### Mapping a Policy on WLAN

#### Security Information

<table>
<thead>
<tr>
<th>Security Policy Completed</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Type</td>
<td>N/A</td>
</tr>
<tr>
<td>Auth Key Mgmt</td>
<td>N/A</td>
</tr>
<tr>
<td>Encryption Cipher</td>
<td>None</td>
</tr>
<tr>
<td>EAP Type</td>
<td>N/A</td>
</tr>
<tr>
<td>SNMP NAC State</td>
<td>Access</td>
</tr>
<tr>
<td>Radius NAC State</td>
<td>RUN</td>
</tr>
<tr>
<td>CTS Security Group Tag</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>AAA Override ACL Name</td>
<td>none</td>
</tr>
<tr>
<td>AAA Override ACL Applied Status</td>
<td>Unavailable</td>
</tr>
<tr>
<td>AAA Override Flex ACL</td>
<td>none</td>
</tr>
<tr>
<td>AAA Override Flex ACL Applied Status</td>
<td>Unavailable</td>
</tr>
<tr>
<td>Redirect URL</td>
<td>none</td>
</tr>
<tr>
<td>IPv4 ACL Name</td>
<td>none</td>
</tr>
<tr>
<td>IPv4 ACL Applied Status</td>
<td>Unavailable</td>
</tr>
<tr>
<td>IPv6 ACL Name</td>
<td>none</td>
</tr>
<tr>
<td>IPv6 ACL Applied Status</td>
<td>Unavailable</td>
</tr>
<tr>
<td>mDNS Profile Name</td>
<td>default-mdns-profile</td>
</tr>
<tr>
<td>mDNS Service Advertisement Count</td>
<td>0</td>
</tr>
<tr>
<td>AAA Role Type</td>
<td>none</td>
</tr>
<tr>
<td>Local Policy Applied</td>
<td>Employee-iPad</td>
</tr>
</tbody>
</table>
Mapping the Policy to an AP Group

Disable the WLAN on which you want to configure the policy.

To apply the policy on an AP group we assume that you already have AP Groups configured on the WLC. If AP Groups has already been configured in your setup, please skip Step1 to 3.

If not, create an AP Group by going to WLC menu.

---

**Step 1** Navigate to WLANs > Advanced> AP Groups and click Add Group.

Then type in the name to define your AP Group Name and click Add button.

**Step 2** Now click on the AP Group Name and then from the menu click WLANs and Add New.

**Step 3** From the drop down menu for WLAN SSID and Interface, select the required SSID and Interface respectively. Once selected click Add button to apply the selected WLAN on the AP Group.
Step 4 Hover your mouse over the blue drop-down arrow for the desired WLAN on which you want to configure the Policy. Then select Policy-Mapping from the drop-down menu.

Step 5 Set the Priority Index to any value from 1-16, and then select the policy which you already created from Local Policy drop down list. To apply the policy on AP Group click Add. The policy will be mapped to AP Group and can be seen under Policy Name.

Click Back to go to the AP Group menu.

Step 6 If the APs are not added to group go ahead and add them by selecting the AP and clicking the Add APs button. Here we added AP2600 to the AP Group.
Once the AP has joined the specific AP group then **Enable** the WLAN on which the policy is enforced. Test the policy enforcement by associating an iPad/Client to the WLAN. Once the device is associated and profiled, it gets redirected to the VLAN matching the policy.
Example of Policy Enforcement on Other Device Types

Example

Policies were created for different device types (Android, Macbook, and Windows) coming into our network to be redirected to particular VLANs once they get profiled and policies are being enforced.

For this, dynamic interfaces such as “android” mapped to VLAN 23, Interface “apple” mapped to VLAN 22 and interface “dynamic” mapped to VLAN 21 was created.

In the following example, we are demonstrating profiling and policy implementation for Android and MAC devices.

For Employee MacBooks we created a policy name Employee-Mac-Device and added the Profiles from the WLC predefined profile list from the Device Type drop down menu.

Once the profile is matched, the policy enforcement is based on VLAN attribute. Here, the device should be redirected to VLAN 22 if it is a MacBook and to VLAN 23 if it is an Android device.
Policy “Employee-Mac-Device”

<table>
<thead>
<tr>
<th>Device List</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS X Lion-Workstation</td>
</tr>
<tr>
<td>OS X Leopard-Workstation</td>
</tr>
<tr>
<td>OS X SnowLeopard-Workstation</td>
</tr>
<tr>
<td>OS X Tiger-Workstation</td>
</tr>
<tr>
<td>OS X-Workstation</td>
</tr>
<tr>
<td>Apple-MacBook</td>
</tr>
<tr>
<td>Apple-Device</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 ACL: none</td>
</tr>
<tr>
<td>VLAN ID: 22</td>
</tr>
<tr>
<td>Qos Policy: none</td>
</tr>
<tr>
<td>Session Timeout: 0</td>
</tr>
</tbody>
</table>

Policy “Employee-Android”

<table>
<thead>
<tr>
<th>Device List</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 ACL: none</td>
</tr>
<tr>
<td>VLAN ID: 23</td>
</tr>
<tr>
<td>Qos Policy: none</td>
</tr>
<tr>
<td>Session Timeout: 0</td>
</tr>
</tbody>
</table>
These policies are mapped to the WLAN “Demo-Employee”

In the above example, an Android device and a Macbook is associated to SSID Demo-Employee and both the device is being redirected to the VLAN 23 and VLAN 22 respectively.

Client details for Android Device:

Client details for Apple MacBook:
Role Based Policy

Role is identified as a Cisco AV-pair from the AAA server and a user needs to configure the role as per user on the AAA server as:

```
cisco:cisco-av-pair= role= <role-type>
```
The following example shows the role type “student” configured on ISE.
Example of similar role type configured on ACS:

Now, to apply the role based policy on WLC, navigate to Policy > Edit page and under Match Criteria define the Match Role String that the user created earlier on the AAA server. In the example, the Match Role String is configured as student. Once the policy is created, the user can tie the policy to a specific WLAN (with L2 Security set to 802.1x).
The following table explains the Policy application support matrix for FlexConnect mode.

<table>
<thead>
<tr>
<th>Flex Operation</th>
<th>Feature Support</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Switched</td>
<td>Yes</td>
<td>The policy application will work for central switching as per design.</td>
</tr>
<tr>
<td>Local Switched</td>
<td>Partial support</td>
<td>Only VLAN override is supported.</td>
</tr>
<tr>
<td>Central Authentication</td>
<td>Yes</td>
<td>The policy application will work as per design.</td>
</tr>
<tr>
<td>Local Authentication</td>
<td>No</td>
<td>No local authentication support.</td>
</tr>
<tr>
<td>Standalone mode</td>
<td>No</td>
<td>When in standalone mode the clients will be out of policy. The clients need to be centrally authenticated to get the policies applied again. Same would apply for external web-authenticated clients.</td>
</tr>
</tbody>
</table>

**Limitations**

- When local profiling is enabled, radius profiling is not allowed on a particular WLAN, both configurations are mutually exclusive.
- If AAA override is enabled and you get any AAA attributes from AAA server other than role type, the configured policy action is not applied. The AAA override attributes will have higher precedence.
• Wired clients behind the WGB won’t be profiled and policy action will not be done.
• Only the first Policy rule which matches will be given precedence. Each policy profile will have an associated policy rule which will be used for matching the policies.
• Only sixteen policies per WLAN can be configured and globally sixty four policies will be allowed.
• Policy action will be done after L2 authentication is complete or after L3 authentication or when device sends http traffic and gets the device profiled. Due to which certain scenarios profiling and policy actions will happen more than once per client.
• This release will support only IPv4 clients to be profiled.
• No support for WGB wired clients for profiling as http profiling is not supported on WGB wired clients.

Summary

• By default profiling is disabled on all WLANs.
• Each WLAN can have mapped profiling policies configured.
• Each Policy can have matching Role Type, Device Type, EAP type configured and an associated policy index mapped.
• The policy index signifies which policy needs to be matched first.
• The corresponding policy name will be deduced from the policy Index.
• The policy matching will exit at the first policy match and the corresponding policy action attributes will be set per client.
• The order of applying the policies per client will be based on security type.
• If a device is profiled once, the client is stored and the corresponding policy actions is applied.

Note
See Cisco Wireless Device Profiling and Policy video for more information on setup and configuration.

Show Commands

```
show user <username> devices
show client wlan <WLAN Id>
show client wlan <WLAN Id> device-type <ipad | ipod | macbook ..>
show wlan <wlan-id>
```

Debug Commands

```
debug policy [events|errors] <enable|disables>
```

Debugs for profiler will be enabled by the existing "debug profiling <enable | disable>" CLI
Commands to Configure Profiling through CLI

```plaintext
config wlan disable <wlan-id>
config wlan profiling <radius/local> <all/dhcp/http> enable <wlan-id>
config wlan enable <wlan-id>
```

Commands to Configure Policy through CLI

```plaintext
config policy <policy-name> create
config policy <policy-name> match device-type add <device name>
config policy <policy-name> action vlan <enable|disable> <vlan #>
config wlan policy add <policy index number> <policy-name> <WLAN Id>
```

To configure the policy and match it to a corresponding AP group, we need the policy Index also, which signifies which policies need to be matched first. The CLI command will be:

```plaintext
config wlan apgroup policy add <policy index number> <policy-name> <apgroup name> <WLAN Id>
```

To configure the policy and match it with time of day, the CLI command will be:

```plaintext
config policy <policy-name> active add hours <08:00 – 17:00> days <Mon | Tue | Wed | Thurs | Fri | Daily | Weekdays >
```

To configure the policy match with EAP type, the CLI command will be:

```plaintext
config policy <policy-name> match eap-type add <peap | leap | eap-fast | eap-tls>
```

For policy action as ACL, the CLI command will be:

```plaintext
config policy <policy-name> action acl <acl-name> <enable|disable>
```

For policy action as QoS, the CLI command will be:

```plaintext
config policy <policy-name> action qos <bronze | gold | platinum | silver> <enable|disable>
```

For policy action as Session-Timeout, the CLI command will be:

```plaintext
config policy <policy-name> action session-timeout <timeout in sec> <enable|disable>
```

For policy action as Sleeping Client Timeout, the CLI command will be:

```plaintext
config policy <policy-name> action sleeping-client-timeout <enable|disable><timeout in hours>
```

Appendix-A

Sleeping Client Support

Currently in 7.4 release, guest client devices connected to the WLC on web-auth enabled WLANs have to enter login credentials every time the client goes to sleep and wakes up.

From 7.5 release, clients already in RUN state after successful web authentication are allowed to sleep and wakeup without the need to re-authenticate through the login page. The sleep client duration for which client needs to be remembered for re-authentication is based on the configuration.

Other salient features are as follows:
Wireless Device Profiling and Policy Classification Engine on WLC

Appendix-A

- Feature is configurable per wlan.
- Supported only for L3 security enabled WLANs. Not applicable to Guest LAN or Remote LAN.
- Sleep client duration is configurable for 1hrs to 30days (720 Hrs) with a default value set to 12 hours. This duration is configurable on WLAN as well as on the policy mapped to the WLAN. The policy mapped configuration takes precedence over WLAN configuration.
- The maximum number of sleeping clients supported is based on the platform.
  - WiSM/5508 – 1000
  - 7500/8500 – 9000
  - 2500 – 500
- Flex connect AP Support – Sleep client support feature works with flexconnect mode AP’s in local switching case for both internal and external web-auth.
- High Availability– Only configuration sync is supported. Sleep cache entries are not synchronized across active and standby.

WLAN Configuration for Sleeping Client

As sleeping client is only supported for L3 security WLANs, navigate to the particular WLAN on which you want to enable the sleeping client feature. Navigate to Security > Layer 3 and select Web Policy from the Layer 3 Security drop-down list.

Select the radio button Authentication and enable Sleeping Client by checking the box as shown in the image below.

Navigate to Advanced tab and make sure that the session timeout is greater than the client idle timeout, otherwise the sleeping client entry would not be created.
Now connect a client to the WLAN on which sleeping client feature is enabled. Then navigate to Monitor > Clients, the status of the client shows that it is in **Associated** state but Not Authenticated as username/password required for web-auth.
Under **Client Properties** menu, it is seen that the client is in Web-auth required state.

After entering the appropriate login credentials for web-auth, the client get authenticated and moves to RUN state.
After successful web-auth, the user is successfully authenticated.

Now if the client configured is idle for 300 seconds (default idle timeout value) or disconnects from the WLAN it is connected to, then the client will move to sleeping clients. Click **Sleeping Clients** option to check if the client entry exists.
Once the client is moved to the Sleeping Clients, the timeout session starts and the remaining time before the client entry is deleted/cleared is displayed.

If the client wakes up or joins back to the same WLAN, it doesn’t require re-authentication.

**Sleeping Client CLI commands**

To enable the sleeping-client feature on wlan:

```
(controller) >config wlan custom-web sleep-client enable/disable <wlan-id>
```

To configure sleeping-client interval on wlan:

```
(controller) > config wlan custom-web sleep-client timeout <1- 720hours> <wlan-id>
```

To check sleep client configuration on wlan:

```
(controller) > show wlan <wlan-id>
```

To delete any unwanted sleeping-client entries:

```
(controller) > config custom-web sleep-client delete <mac-addr>
```

To show summary of all the sleeping-client entries:

```
(controller) > show custom-web sleep-client summary
```

To show the details of sleeping-client entry based on mac address:

```
(controller) > show custom-web sleep-client detail <mac-addr>
```
Native Profiling and Policy in CUWN Release 8.0

In release 8.0, two major enhancements were introduced related to Native Profiling and Policy classification feature on WLC:

- New attributes added to Local Policy
- Dynamic MAC OUI and Device Profile updates

AVC/mDNS Profiles Attached to Local Policies

Prior to release 8.0, all clients associated with a WLAN/SSID pick the same AVC/mDNS profile mapped to the WLAN and allow the services configured for the profile. In release 8.0, an AVC/mDNS profile can be mapped to a local policy for a client with a particular device type. This ensures that each Local policy can be configured with a different AVC/mDNS profile name based on AAA override, to restrict the policy from being able to use the services not allowed by the profile on the same WLAN.

Profiling and Policy Engine on WLC

In this section, you will configure and implement Profiling and Policy on a Cisco WLC running AireOS 8.0 code.

The profiling and policy enforcement are configured as two separate components. The configuration on the WLC is based on defined parameters specific to clients joining the network. The policy attributes which are of interest are:

a. Role—Defines the user type or the user group the user belongs to, for example, student or employee.
b. Device—Device defines the type of device, for example, Windows machine, Smart phone, Apple devices such as iPad, iPhone, and so on.
c. Time of day—Allows configuration to be defined at what time of the day, the end-points are allowed on the network.
d. EAP Type—Checks what EAP method the client is getting connected to.

The above parameters are configurable as policy match attributes. Once WLC has a match corresponding to the above parameters per end-point, policy enforcement comes into picture. Policy enforcement is based on session attributes such as:

- VLAN
- IPv4 ACL
- Session Timeout
- QoS
- Sleeping Client Timeout
- Flexconnect ACL
- AVC Profile (added in release8.0)
- mDNS Profile (added in release 8.0)
- Avg.Data Rate (added in release 8.0)
- Avg. Real Time Data Rate (added in release 8.0)
• Burst Data Rate (added in release 8.0)

You can configure these policies and enforce end-points with specified policies. The wireless clients will be profiled based on the MAC OUI, DHCP, HTTP user agent (valid Internet required for successful HTTP profiling). The WLC uses these attributes and predefined classification profiles to identify devices.
Profiling and Policy Configuration

Complete these steps:

**Step 1** To configure device profiling on a WLAN, go to the specific WLAN (with 802.1x security configured) on which you want to implement Native profiling and policy and click the *Advanced* tab. In the *Allow AAA Override* field, uncheck the *Enabled* check box if it is checked. In the *DHCP* area, in the *DHCP Addr. Assignment* field, check the *Required* check box.

**Step 2** In the *Local Client Profiling* area, check the check boxes corresponding to DHCP Profiling and HTTP Profiling if they are not checked and click *Apply*.

Now, associate a client to the WLAN on which profiling is enabled.
From the WLC main menu, go to *Monitor > Clients*. The profiled devices are listed under the *Device Type* column.
Notice that there are three devices associated to the WLAN, and all of them are being profiled in the following example.
Also, the Local Profiling option under the Monitor page provides the administrator a better understanding of the kind of devices that exists in the network. The local profiling option, which was introduced in CUWN 7.6 release, enables viewing the basic device statuses.

Creating Policies on WLAN from the WLC GUI

**Step 3** Once profiling is configured, you can create Local policies and apply them on the WLAN. From the WLC main menu, go to Security > Local Policies.
Step 4 When in the Local Policy List, click New to create a Policy Name. In this example, teacher-LP is used as a policy name, but you can use any name to define your own policy.

Once Policy Name is configured, you can create policies to match a Role, EAP Type, and Device Type. Also, you can define the required actions related to the Match criteria. In this example, we use User Role and Device Type to Match Criteria, but you can use any other type if required.

Note Ensure that the Match Role string is the same as AAA defined role name. In this example, it is configured as teacher.

Step 5 In the Match Role String text box, enter a user role, for example, teacher. From the Match EAP Type drop-down list, choose the EAP type that you want to match the clients to, else, leave as is and click Apply.
**Step 6**  
To apply the policy based on a user device, in the **Device List** area, from the **Device Type** drop-down list, choose the device type on which you want to enforce the policy and then click **Add**. In this example, Apple-iPad is used as a device type for Match Criteria. You can add other devices as well from the Device Type drop-down list.

**Note**  
If you do not want to match any device type, then do not configure the **Device Type** option. There are 156 default device profiles that the users can choose from the **Device Type** drop-down list, but only 16 can be applied per policy.

**Step 7**  
To apply the appropriate action, choose from the parameters under the **Action** area to enforce the policy. In the following example, only the **AVC Profile** attribute is selected, but you can select other attributes as well according to your network requirement and then click **Apply**.

**AVC Configuration**  
In this example, two AVC profiles (teacher-AVC and student-AVC) are created. The **teacher-AVC** profile is configured to just mark some applications, while the **student-AVC** profile is configured to drop applications such as YouTube, BitTorrent and so on.

If there are no AVC profiles configured on the WLC, go ahead and create them.

See the Application Visibility and Control Feature Deployment Guide for AVC configuration.
Step 8 You can have multiple policies with different role types and different AVC Profiles set on the same WLAN. In this example, we created one more local policy for student role as student-LP.

**Note** Ensure that the Match Role string is the same with Radius Server defined role name (student).

To apply the policy based on a user device, in the Device List area, from the Device Type drop-down list, choose the device type (Apple-iPad) on which you want to enforce the policy and then click Add.

To apply the appropriate action, choose from the parameters under the Action area to enforce the policy. Select an AVC profile from the AVC Profile drop-down list. In this example, the AVC profile (student-AVC) is already created. Click Apply.
Step 9  Create a default local policy for any other device.

- If no other ACL is applied in the Local policy, then any other device, other than Apple-iPad, will be able to access the applications because the final filter function of all policies is **Allow all**. In order to block all applications on all devices except Apple-iPad, create a **deny all** ACL and apply it on the Local Policy and then apply that policy on the WLAN as the last resort. See the configuration examples in the following screenshots.

- On the WLC, create an ACL to deny all IPv4 flow.
Create a Local Policy Block-all and apply the deny all ACL to it, do not choose any device roles or profiles.

Mapping Policy on WLAN

Complete these steps:

**Step 1** Go to WLANs from the WLC menu and click the WLAN ID on which you want the policy to be implemented. From the WLAN edit menu, click the Policy-Mapping tab.
Set the Priority index to any value from 1-16. From the **Local Policy** drop-down list, choose the policy which you have already created. To apply the policy on the WLAN, click **Add**. The policy is mapped to the WLAN and can be seen under Policy Name.

**Step 2** Add the appropriate policies to Policy-Mapping under WLAN.

**Step 3** In the **Advanced** tab, in the **Allow AAA Override** field, uncheck the **enabled** check box if it is checked.
**Step 4** Check if the AAA role is configured properly, and applied on the Radius Server (in this example, it is Cisco ISE). The AAA role name on the ISE must match the role string defined in the local policy. See the ISE settings below.

Once the client associates to SSID with teacher credentials through Apple iPad, it should be able to access the Internet and different applications per its AVC profile (teacher-AVC) configuration. If the user tries to connect from any device other than Apple iPad, then it will not be able to access the Internet.

To verify if the policy (teacher-LP) is applied, from the WLC GUI, go to Monitor > Clients, and then click the Client MAC address. In the Security Information area, you should see the policy in the Local Policy Applied text box.
To verify if the policy is applied, from WLC CLI prompt, run the following command—
show client detail <mac_address> and then scroll down to the end to see the applied profile.

AAA Role Type: teacher
Local Policy Applied: teacher-LP
IPv4 ACL Name: none
IPv4 ACL Applied Status: Unavailable
IPv6 ACL Name: none
IPv6 ACL Applied Status: Unavailable
Layer2 ACL Name: none
Layer2 ACL Applied Status: Unavailable
Client Type: SimpleIP
mDNS Status: Enabled
mDNS Profile Name: default-mdns-profile
No. of mDNS Services Advertised: 0
Policy Type: WPA2
Authentication Key Management: 802.1x
Encryption Cipher: CCMP (AES)
Protected Management Frame: No
Management Frame Protection: No
EAP Type: PEAP
Interface: management

To verify if the policy is applied from the WLC:

AVC Profile Name: teacher-AVC
Similarly, try to connect to the same WLAN/SSID using student credentials with the user role **student**, you should see another policy applied (student-AVC).

To verify if the policy (student-LP) is applied, from WLC GUI, go to **Monitor > Clients** and then click the Client MAC address. In the **Security Information** area, you should see the policy in the **Local Policy Applied** text box.

To verify if the policy is applied, from WLC CLI prompt, run the following command—**show client detail <mac_address>** and then scroll down to the end to see the applied profile.
Dynamic MAC OUI and Device Profile Update

In CUWN release 8.0, the WLC administrator can update the MAC OUIs and device profiles on the WLC. The IEEE file containing the OUIs must be downloaded and saved as a .txt file from the following location: http://standards.ieee.org/develop/regauth/oui/oui.txt. Download the .txt file to the WLC, using tftp/ftp.

Apart from the OUI update, the WLC also has a mechanism to update the device profiles. Device profiles refers to the different types of devices that the WLC can profile. In release 8.0, the WLC supports profiling 156 types of devices, by default. When a new device profile is updated by the ISE team, the WLC must integrate the new profile to be on par with the ISE. This feature is implemented to take care of both the OUI updates as well as the device profile updates.
Downloading MAC-OUI Through the WLC GUI

Complete these steps:

**Step 1**  From WLC main menu, go to **Commands > Download File**.
**Step 2**  From the **File Type** drop-down list, choose **OUI Update**.
**Step 3**  From the **Transfer Mode** drop-down list, choose **TFTP** or **FTP**.
**Step 4**  Provide the appropriate information under **Server Details** and click **Download**.

**Note**  The WLC is not required to reboot after the download. This is a cosmetic error which will be corrected in the next update. The bug ID is **CSCup84476**.
Downloading MAC-OUI Through the WLC CLI

The following CLI command downloads the IEEE oui.txt file to the WLC:

```
<WLC> transfer download datatype oui-update
```

Updating Device Profile Through the GUI

Complete these steps:

- **Step 1** From the WLC main menu, go to Commands > Download File.
- **Step 2** From the File Type drop-down list, choose Device Profile.
- **Step 3** From the Transfer Mode drop-down list, choose TFTP or FTP.
- **Step 4** Provide the appropriate information under Server Details and then click Download.

**Note** The Profile update file is an XML file containing the device profiles. A new GUI option is added to enable you to download the device profiles file to the WLC.
The WLC is not required to reboot after the download. This is a cosmetic error which will be corrected in the next update. The bug ID is CSCup84476.

### Updating Device Profile Through the CLI

The following CLI command is used to enable downloading device profiles to the WLC:

```
<WLC> transfer download datatype device-profile
```

```
<POD2-WLC> transfer download datatype device-profile
<POD2-WLC> transfer download filename profiler_policies.xml
<POD2-WLC> transfer download mode tftp
<POD2-WLC> transfer download serverip 10.10.105.112
<POD2-WLC> transfer download start
```

```
Mode: TFTP
DataType: Device Profile
TFTP Server IP: 10.10.105.112
TFTP Packet Timeout: 6
TFTP Max Retries: 10
TFTP Path: /profiler_policies.xml
Starting transfer of Device profiles
This may take some time.
Are you sure you want to start? [y/N] y
TFTP Device Profile transfer starting.
TFTP receive complete... Loading Device profiles.
Device Profiles installed.
```

Both the OUI file and device profiles file are independent of each other, and even if one of them needs to be updated, the other will still work.
For example, if the customers want to update only the OUIs, they must download only the OUI file to the WLC. The existing device profiles will remain as it is, and only the OUIs will get updated.

The new CLI command—`show profiling oui-string summary`, can be executed to check the updated MAC OUIs, if any.

The existing CLI command—`show profiling policy summary`, can be executed to check the updated profiles, if any.

**Limitations**

- Wired clients behind the WGB will not be profiled and policy action will not be done.
- Only 16 policies per WLAN can be configured, and globally 64 policies will be allowed.
- Only 16 device profiles (device types) can be added per policy.
- Policy action will be done after L2 authentication or L3 authentication is complete or when the device sends HTTP traffic and gets the device profiled. Thus, certain scenarios such as profiling and policy actions will happen more than once per client.
- This release will support only IPv4 clients to be profiled.
- No support for WGB wired clients for profiling because HTTP profiling is not supported on WGB wired clients.

**Summary**

- By default, profiling is disabled on all WLANs.
- Each WLAN can have mapped profiling policies configured.
- Each Policy can have matching Role Type, Device Type, and EAP type configured and an associated policy index mapped.
- The policy index signifies which policy needs to be matched first.
• The corresponding policy name will be deduced from the policy Index.
• The policy matching will exit at the first policy match and the corresponding policy action attributes will be set per client.
• The order of applying the policies per client will be based on the security type.