
First Published: June, 2014

Introduction

This document introduces Deployment Guide Release 3.6 for the Cisco Converged Access CT5760 and Cisco Catalyst 3850 products. This guide is designed to help you deploy and monitor new features introduced in the new release.
CT5760 Controller

The CT5760 Wireless LAN Controller (WLC) is an innovative UADP ASIC based wireless controller deployed as a centralized controller in the next generation unified wireless architecture. CT5760 controllers are specifically designed to function as unified model central wireless controllers. It also supports the newer mobility functionality with converged access switches in the wireless architecture.

CT5760 controllers are deployed behind a core switch or router. The core switch or router is the only gateway into the network for the controller. The uplink ports connected to the core switch can be configured as EtherChannel trunk to ensure port redundancy.

This new controller is an extensible and high performing wireless controller, which can scale up to 1000 access points (AP) and 12,000 clients. The controller has 6 - 10 Gbps data ports.

As a component of the Cisco Unified Wireless Network, the 5760 series works in conjunction with Cisco Aironet Access Points, the Cisco Prime infrastructure, and the Cisco Mobility Services Engine to support business-critical wireless data, voice, and video applications.

Catalyst 3850 Switch Controller

Unified Access Catalyst 3850 switches are innovative UADP ASIC hardware that can support multiple protocols and has many advantages over the current hardware platform. The Catalyst 3850 switch has an integrated hardware-based wireless support with CAPWAP and fragmentation. The Catalyst 3850 switch has 40 Gig of uplink bandwidth with all ports functioning at line rate.
Local Profiling

Cisco currently offers a rich set of features such as device identification, onboarding, posture, and policy management through ISE. However, large sets of customers do not deploy ISE but still require some of the above mentioned features. WLC is enhanced with some of these capabilities. This document deals with basic configuration of device profiling and policy implementation through Cisco WLC.

Cisco WLC performs profiling of devices based on protocols such as HTTP, DHCP, and MAC OUI to identify end devices in the network. You can configure the device-based policies and enforce per-user or per-device policy in the network. The WLC also displays statistics that are based on per-user or per-device end points and policies that are applicable per device.

When used with Bring your own device (BYOD), local profiling has an impact on understanding the different devices on the network. This also enables BYOD to be implemented on a small scale within the WLC itself.

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. User Role—User Role defines the user type or the user group the user belongs to, for example: student, employee and so on.

   Role is identified as a Cisco AV-pair from the AAA server and you can configure the role as per user on the AAA server by issuing the following command:
Cisco: cisco-av-pair = role = role-type

The following example displays the role type “student” configured on ISE.

Figure 3  Role AV-pair Configuration on ISE
Example of the similar role type configured on ACS:

**Figure 4 Role AV-Pair Configuration on ACS**

- **Device type**—Device type defines the type of device, for example: Windows machine, Smartphone, and Apple device such as iPad, iPhone and so on.
- **Username**—Username defines the login credentials entered by the user.
- **OUI**—Organizationally Unique Identifier of the device.
- **MAC**—MAC address of the device.

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

- **VLAN**
- **ACL**
- **Session Timeout**
- **Ingress QoS**
- **Egress QoS**

You can configure these policies and enforce end-points with specified policies. The wireless clients are profiled based on the MAC OUI, DHCP, and HTTP user-agent (valid Internet is required for successful HTTP profiling). The WLC uses these attributes and predefined classification profiles to identify the device in the network.

**Profiling Configuration**

In Cisco IOS XE Release 3.6, the WLC has embedded or built-in profiles available with which it identifies the devices in the network. In later releases, it should be possible to create user-defined profiles, which will take precedence over the embedded profiles. Currently, there are 287 default profiles and you can view these profiles through the WLC CLI prompt.
Open the WLC CLI prompt and run the `show device classifier profile type` command.

**Figure 5  Device Profiling List**

<table>
<thead>
<tr>
<th>Valid</th>
<th>Type</th>
<th>Profile Name</th>
<th>min</th>
<th>Conf</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Android</td>
<td>30</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Apple-Device</td>
<td>10</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Intel-Device</td>
<td>5</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Apple-MacBook</td>
<td>20</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Apple-iPad</td>
<td>20</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Apple-iPhone</td>
<td>20</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Apple-iPod</td>
<td>20</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Aruba-Device</td>
<td>10</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Avaya-Device</td>
<td>10</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Avaya-IP-Phone</td>
<td>20</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>BlackBerry</td>
<td>20</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Brother-Device</td>
<td>10</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Brother-HL-3040CM-series</td>
<td>30</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Brother-HL-5370DW-series</td>
<td>30</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Brother-MFC-890DW</td>
<td>30</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Brother-MFC-9018CH</td>
<td>30</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Canon-Device</td>
<td>10</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Canon-MF4690</td>
<td>30</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Cisco-Device</td>
<td>10</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Cisco-Router</td>
<td>10</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>Valid</td>
<td>Default</td>
<td>Cisco-Switch</td>
<td>20</td>
<td>20</td>
<td></td>
</tr>
</tbody>
</table>
Complete the following steps:

**Step 1**
Enable Device Classification under **Configuration > Controller > System > General**. Click **Apply**. This step turns on the MAC OUI and DHCP profiling on the controller.

*Figure 6*  **Enable Device Classification Globally**
Step 2  Enable Device classification per WLAN under Configuration > WLAN > Edit > Policy Mapping. Click Apply.

Figure 7  Enable Device Classification per WLAN
**Step 3**

To configure HTTP device profiling on a WLAN through GUI, navigate to the WLAN > Policy Mapping page. Check the Local HTTP Profiling check box and click **Apply**.

*Figure 8*  **Enable Local HTTP Profiling—GUI**

The same can be turned on from the CLI by executing the command `profiling local http` under the WLAN sub-mode.

*Figure 9*  **Enable Local HTTP Profiling - CLI**

Note: You can use radius client profiling to configure profiling through ISE.

**Step 4**

Associate a client to the WLAN and access a web page from the browser of the device in order to trigger HTTP profiling. In this example, an iPad and a MacBookPro are associated to the SSID. You can also use other devices to verify the profiling functionality.

**Step 5**

Verify that the client is put into the default VLAN mapped on the WLAN.

**Step 6**

From the WLC main menu, navigate to the **Monitor > Clients** page. The device type can be seen under the column **Device Type**.
You can view the Device profiling information in a visual pie-chart under Monitor > Controller > Local Profiling > Profiling. This page displays the global count and percentage of devices based on the profiling information obtained.

Client profiling information can be viewed from the CLI by executing the command `show device classifier attached detail`
Policy Configuration and Enforcement

Once profiling is setup, you can create policies and apply them on the WLAN. This is a three-step process:

1. Creation of Service-template.
2. Creation of Policy-Map.
3. Association of Service Policy to WLAN.

Creating Service Templates

Complete the steps:

- **Step 1** From the WLC menu, navigate to Configuration > Security > Service Template > New.
- **Step 2** Enter the Service Template name, VLAN ID, and Session timeout in seconds. Click **Apply**.
Creating Policy Maps

Complete the steps:

**Step 1**  
Once the Service Template is configured, create the Policy Map. From the WLC menu, navigate to **Configuration > Security > Policy Map > New.**

**Step 2**  
Enter the Policy Map name and click **Add** under **Match Criteria Lists** to create Policy rules.

**Step 3**  
Under **Match Criteria**, you can create policies to match a Role and Device Type from the GUI. You can also define what actions to take related to the Match criteria by selecting an appropriate service template.
Device Type match type can be one of the three values:
- `eq` (equal to)
- `not-eq` (Not equal to)
- `regex` (regular expression)

As an example, create a match criteria with Device Type as **Apple-iPad** and Service Template as **POD1-ServiceTemplate** and click **Add**. Once the Match Criteria Lists section is populated, click **Apply**.

**Figure 14** Match Criteria Configuration

### Associating Service Policies to WLAN/Interface

Complete the steps:

**Step 1** Under the **WLAN > Policy Mapping** page, click **Local Subscriber Policy**. Choose the policy created in the previous section from the drop-down list and click **OK**.

**Step 2** Once the Local Subscriber Policy is populated, click **Apply**.
Verifying Policy Enforcement

Re-associate the iPad to the WLAN, open a web page in the browser and verify that the iPad is in the VLAN assigned in the Service Template created earlier.
Profiling and Policy Classification Facts

- If you enable AAA override and there are AAA attributes other than the role type from the AAA server, the configured policy action is not applied. The AAA override attributes have higher precedence.
- Wired clients behind the WGB are not profiled and the policy action is not applied.
- Each policy profile has an associated policy rule, which is used to match the policies, in a match-first fashion.
- There are 255 match-criteria per parameter-map and 255 parameter maps per policy map supported. A WLAN or interface can only be associated with one Policy Map at any given time.
- Policy action is taken after L2 authentication or L3 authentication is complete, or when the device sends HTTP traffic and gets the device profiled. Therefore, profiling and policy actions occur more than once per client.
- Only VLAN, ACL, Session Timeout, and QoS are supported as policy action attributes.
- Local profiling is not supported for Guest Anchor scenarios.

![Image of CLI output showing access session details and policy map](image-url)
Local Profiling CLI Configuration (Optional)

Configuration of Service Templates using CLI

Service templates can be configured from CLI using the command `service-template name` under config sub mode. Note that only certain fields are relevant for the WLC.

Figure 16 Service Template Configuration - CLI

```
5760(config)#service-template ST1
5760(config-service-template)#?

service-template configuration commands:
  absolute-timer    Absolute timeout value in seconds
  access-group      Access list to be applied
  description       Enter a description
  exit              Exit identity policy configuration submode
  inactivity-timer  Inactivity timeout value in seconds
  interface-template Configure interface template to be applied
  linkssec          Configure link security parameters
  no                Negate a command or set its defaults
  redirect          Redirect clients to a particular location
  service-policy    Configure service policy
  tag               tag name
  tunnel            tunnel for wired client access
  vlan              Vlan to be applied
  voice             Voice Feature

<cr>
```

To see Service templates from the CLI, execute the command:

```
show template service user all
```

Figure 17 Service Template Configuration
Configuration of Policy Maps from CLI

Creation of Policy Maps from the CLI is a set of steps:

1. Creation of Parameter-map.
2. Creation of Policy-map.
3. Associating Parameter-map to Policy-map.

Creation of Parameter-map

Match Criteria Lists are equivalent to parameter maps on the CLI. Parameter maps are configured from the CLI using the command:

```command
parameter-map type subscriber attribute-to-service name
```

**Figure 18 Parameter-map Configuration**

```
5760(config)#ap type subscriber attribute-to-service PolicyMapDemo-param
5760(config-parameter-map-filter)# map ?
  device-type specify device-type
  mac-address specify mac-address
  oui specify oui
  user-role specify user-role
  username specify username

5760(config-parameter-map-filter)# map device-type eq Apple-iPhone
5760(config-parameter-map-filter-submode)# service-template ?
  WORD service-template

5760(config-parameter-map-filter-submode)# service-template ST1
```

Multiple match criteria can be added in a “match-all” fashion with the `<number> map` CLI command.

**Note**

For the purpose of ease and demonstration, only device parameters and VLAN attributes are used for profiling and policy enforcement in this example.

To view the parameter-maps configuration, use CLI command:

```
show parameter-type type subscriber attribute-to-service [name <>|all]
```

**Figure 19 Parameter-map Configuration**

```
5760#ster-map type subscriber attribute-to-service name PolicyMapDemo-param
Parameter-map name: PolicyMapDemo-param
Map: 1 map device-type eq "Apple-iPhone"
  Action(s):
  1 service-template ST1
```

5760#
Creation of Policy-map

Policy-map is configured using the CLI command:

```
policy-map type control subscriber Policy Map Name
```

Association of Parameter-map to Policy-map

Once the policy-map is created, associate the parameter-map under the policy-map.

Figure 20  Policy Map Configuration

![Policy Map Configuration](image)

Association of Service-policy from CLI

Associate the policy map either to the WLAN or to the interface as shown below.

Figure 21  Service Policy Association

![Service Policy Association](image)

Associating under an interface:

```
5760(config-if)#service-policy type control subscriber Policy Map name
```
Verification of Policy Enforcement

To verify the policy enforcement, use the command:

```
show access-session mac mac-address details
```

**Figure 22 Verifying Policy Enforcement**