Universal AP Regulatory Domain Deployment Guide

System Requirements

**WLCs Supported with Code 8.0.MR and 8.1**
WLC2500, WLC5500, WiSM2, WLC7500, WLC8500

**Access Points Supported**
The following access points are supported with universal SKUs UXK9.
*The 11ac Module with –UX is also supported for AP3600.
All other AP models that are not listed above will NOT support Universal PIDs.

Universal Domain AP

The aim of introducing Universal SKU AP is to address the worldwide regulatory compliance requirement based on geo-location of the Cisco Wireless Access Points (APs). Solution will collapse all current regulatory domains into a single SKU APs. This will be applicable only to newer -UX PIDs introduced and will not affect the existing APs that are preconfigured with a specific regulatory configuration.

Universal AP can be configured to correct the regulatory domain in two phases:

- Manual Identification (*Through Cisco AirProvision App*)
- Automatic Identification (*Through NDP propagation*)
**Manual Identification**

The manual identification process involves the following tasks:

- Smart Phone based solution (Cisco Air Provision App) communicates with the Universal AP on a secure channel (2.4 GHz only).
- For new installations, the user needs to prime at least one AP in the RF neighborhood by manual identification method.
- APs primed at a different country/reg. domain rely on manual identification to automatically correct country configuration.
- Upon failure of automatic identification, the Universal AP retracts to manual identification.

**Automatic Identification**

The automatic identification process involves the following tasks:

- The process relies on Cisco Infrastructure to identify and apply reg. domain and country configurations.
- Cisco proprietary Neighbor Discovery mechanism identifies secure Cisco Universal APs in the RF neighborhood.
- Universal AP learns domain configurations from the adjacent neighbor’s 802.11 beacons frame and filters the invalid and malicious rogues.
- Adjacent Universal APs have NDP propagation flag set that will be used to propagate valid country and reg. domain to the rest of the APs.

**Associating Universal AP to WLC**

Universal AP does not require any particular configurations on Wireless LAN Controller (WLC) to allow Universal AP to associate. Connect the universal SKU AP to the WLC. Once the AP has joined the controller and downloaded the code, you can check the AP model and SKU by going to the **WIRELESS** tab from the WLC main menu bar.

<table>
<thead>
<tr>
<th>AP Name</th>
<th>IP Address (ipv4/ipv6)</th>
<th>AP Model</th>
<th>AP MAC</th>
<th>AP Up Time</th>
<th>Admin Status</th>
<th>Oper Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP1@10.10.10.110</td>
<td>10.10.10.113</td>
<td>AR521222X2XX2</td>
<td>56:08:00:00:02:21:80</td>
<td>0 d, 0 h 16 m 32 s</td>
<td>Enabled</td>
<td>RSQ</td>
</tr>
</tbody>
</table>

**Note**

You will see the APs LED blinking red and green even though the AP has obtained the IP address and joined the controller. This is because there is no regulatory domain set on the AP, and it has not been primed with the correct domain.

To check if the AP is not already primed for a specific country domain, click the AP Name, and under **Advanced** tab, the 'Regulatory Domains' shows –UX for both radios. Note that the 'Country Code' also shows 'UX' because the AP is not primed with the correct country domain.
You can configure multiple country domains on the WLC as well for AP join. As it is a universal SKU AP (-UXK9), it should join the WLC regardless of the country domain set on the WLC.

**Configuring the WLAN**

To configure a WLAN through which an administrator can prime the AP to a correct regulatory domain, perform the following steps:

1. Go to **WLAN > Advanced**.

2. Scroll down to the **Universal Admin Support** area, and check the **Universal Admin** check box to enable it.

3. Click **Apply**.
Note
Make sure that the WLAN has the security set to PSK or 802.1x as open authentication WLAN will not allow universal admin support.

Note
The universal admin enabled WLAN used for priming the AP should be able to reach the management IP of the controller. Similarly, for Autonomous AP, the universal admin enabled WLAN should be able to reach the Autonomous AP's management IP address.

Priming UX AP Through AirProvision App (Manual Identification)

This method uses an AirProvision application on smartphone that runs on different flavors of mobile OS. Upon successful authentication, the smartphone communicates with the Universal AP on a secure 2.4 GHz channel. The smartphone then requests the AP configurations to differentiate Universal SKU AP from other access points. When the associated access point is identified as Universal AP, the smartphone pushes the regulatory configurations to the AP.

When a user wants to prime a universal AP, the user needs to access the AirProvision app with CCO credentials. Without proper authentication, the AirProvision app will not be able to configure the access point. After successful authentication, the smartphone associates to Universal AP over a secure 2.4 GHz channel as a client. Prior to the association with AP, the AirProvision app also gathers its location information from the inbuilt GPS and cell tower that advertise country information by extracting Mobile Country Code (MCC) Identifier from the Public LAN Mobile Network (PLMN). Once associated, Universal AP sends information about its AP type, Reg. Domain, and country configurations to distinguish from existing Cisco APs and to ensure that it has been primed already.

For an unprimed/out of box Universal AP, the AirProvision app configures the AP with correct reg. domain that will derive base on the AP information and country code details via GPS and MCC ID. The AirProvision app maintains a database that maps country configurations to regulatory domain for a specific AP model. This information is sent to Universal AP to migrate it into correct Reg. Domain and country configurations.

Modes of Availabilities
Manual Identification works only on the following modes of unified APs:

• Local
• FlexConnect
• Bridge*
• Autonomous APs

*Unified APs in Bridge mode require wired connection to WLAN Controller for initial AP deployment. In the absence of Universal Root AP (RAP), Universal Mesh AP will not allow domain conversion.

Following modes of Unified APs will NOT be able to leverage Manual Identification method:

• Monitor
• Sniffer
• Rogue-Detector
• SE Connect
The AirProvision app supports the following two modes of operations:

- **Configure Mode**—This is the default mode of operation for the AirProvision app to configure Universal SKU AP. Fresh out of box APs are configured via configure knob when associated AP is configured with Universal Attributes (Reg. Domain: -UX, Country: UX).

- **Audit Mode**—This special mode handles the misconfigured primed Universal APs, when the Universal APs are shipped via tier-2 distributors or were misconfigured due to change in location. In such cases, the reg. domain configurations are corrected via the AirProvision app in audit mode. The audit mode can overwrite the reg. domain configurations of an already primed Universal AP.

### Installing AirProvision Application

The AirProvision application, to migrate Universal AP into correct regulatory domain, is supported on following versions of SmartPhone Operating Systems:

- Android Jelly Bean 4.3 or higher
- Apple iOS 7.0 or higher
- Windows Mobile OS 8.0

Depending on your smartphone's platform, download and install the Cisco AirProvision application from iOS App Store, Google Play Store, or Windows Phone Store.

### Configuring Universal AP Through Airprovision App

To configure the Universal AP through AirProvision app, perform the following steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Connect the client (iPhone or Android phone) to the universal admin enabled SSID. (In this setup, it is POD6-PSK). Ensure that the client associates to the AP on 2.4 GHz radio.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Open the Airprovision app. Log in to the app using your CCO credentials. Also, enable location services for the app.</td>
</tr>
</tbody>
</table>
When the location service is enabled, the Universal AP login screen appears. The username and password appears as default in the login screen. (The default User name is ‘Cisco’ and Password is ‘Cisco’, and are case sensitive). If the admin has configured a specific username /password then enter admin configured username /password.

**Step 3**

Click Log In.

The AP configuration page appears, where you can see the **Configure** and **Audit** tabs. The status of the Universal AP can be seen by clicking these tabs. Currently, the AP is not provisioned, so it states the following under configure and Audit tabs:

- **AP Provision** = No
- **2.4 GHz** = -UX
- 5 GHz = -UX
- Configured Country = UX

Step 4  Click Configure.

Step 5  The AP reboots and joins back with the regulatory domain it received through the GPS/Location services. You can check this by navigating to the WIRELESS > AP Name > Advanced tabs. The Regulatory Domains is changed from –UX to –A, which is the correct regulatory domain. The country code also shows US. As the AP is primed through the app, the Universal Prime status shows as Web App.
Once the AP is primed, all the radios are configured to the correct domain. This holds true for 11ac module as well.

Also, you can insure this by connecting the client (iPhone or Android phone) to the universal admin enabled SSID (POD6-PSK in this setup). Then, log in to the AirProvision app to see that the Universal AP is configured correctly as follow:

- AP Provision = Yes
- 2.4 GHz = -A
- 5 GHz = -A
- Configured Country = US

In an Android phone, the AirProvision app behaves little different. That is, once you open the Airprovision app, it asks for CCO credentials to connect to the universal admin enabled SSID from the list of discovered SSIDs. Once you connect to the SSID, the procedure is same as iPhone.
Once the AP is primed with the correct domain, the NDP will be used to propagate valid country and reg. domain to the rest of the Universal domain APs on the network in the same RF neighborhood. This process is also known as Automatic Identification.

**Note**

Automatic Identification method solely relies on Cisco’s RF intelligence to propagate the new reg. domain and country configurations to the local RF neighborhood. Cisco proprietary Neighbor Discovery Protocol (NDP) frames are leveraged to discover secure Cisco
Universal APs in the network and propagate reg. domain attributes to the localized RF neighborhood. The following UX-AP is primed to correct regulatory domain through automatic identification.

![Image](image.png)

**Note** Automatic identification through NDP is only valid among the –UX PIDs APs.

Automatic Identification method is the default method used by Cisco Universal APs. While manual identification helps to migrate Universal AP into correct reg. domain, automatic identification propagates reg. domain configuration to the localized RF neighborhood quickly and efficiently. The automatic identification method requires dependencies on presence of existing Cisco Universal APs in the network. Therefore, for initial seed AP or when APs are installed in disjoint RF neighborhood, the user needs to prime at least one Universal AP in the network. The automatic identification method also helps to autocorrect already primed Universal AP; this will be addressed by special notification via NDP that can override other Universal APs configurations.

**Limited Support on Autonomous APs**

Current framework is designed to work on both Unified and Autonomous APs.

However, Phase 1 of this project does not include Automatic Identification (through NDP) support for Autonomous APs. It will be deferred to future 8.x SW release.

**Automatic Identification on a Mesh Network**

Access points operating in Bridge mode can be provisioned over the air using the Automatic Identification process. Both Bridge mode Root Access Points (RAPs) and Mesh Access Points (MAPs) use over the air 2.4 GHz NDP packets to determine the local regulatory domain. The list of supported 5 GHz channels differ based on regulatory domain, so no packets are transmitted across the 5 GHz radios until the access point is provisioned.
RAP sends NDP messages on all 2.4 GHz channels to adjacent MAPs. All MAPs that can hear the message will be provisioned to match the same regulatory domain as the RAP. Once provisioned, the Bridge mode access points will re-join the RAP and form a mesh tree.

**Summary**

To summarize, this deployment guide covers the following:

- Combines intelligence from trusted Cisco Neighbor Discovery Messages along with Smart Phone based audit scheme (App).
- Solution works for customers with no Cisco APs in prior deployments.
- Expedites domain identification process from existing RF neighbors to bring faster network convergence.
- Reliable solution for worldwide distributors where APs are shipped to one location and then get distributed to end customers.
- Covers boundary conditions when APs are primed in a different regulatory domain/country.
- Encompasses safety net for deployments where initial seed or majority of existing APs are configured with incorrect country / reg. domain configurations.
<table>
<thead>
<tr>
<th>Americas Headquarters</th>
<th>Asia Pacific Headquarters</th>
<th>Europe Headquarters</th>
</tr>
</thead>
<tbody>
<tr>
<td>San Jose, CA 95134-1706 USA</td>
<td>Singapore</td>
<td>Amsterdam, The Netherlands</td>
</tr>
</tbody>
</table>

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.