Wireless Device Overview

Wireless devices (commonly configured as access points) provide a secure, affordable, and easy-to-use wireless LAN solution that combines mobility and flexibility with the enterprise-class features required by networking professionals. When configured as an access point, the wireless device serves as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

With a management system based on Cisco IOS software, wireless devices are Wi-Fi CERTIFIED™, 802.11a-compliant, 802.11b-compliant, 802.11g-compliant, and 802.11n-compliant wireless LAN transceivers.

By adhering to the 802.11ac Wave 2 standard, the Cisco 1100 Series WLAN offers a data rate of up to 867 Mbps on the 5-GHz radio. This exceeds the data rates offered by access points that support the 802.11n standard. It also enables a total aggregate dual-radio data rate of up to 1 Gbps. This provides the necessary foundation for enterprise and service provider networks to stay ahead of the performance expectations and needs of their wireless users.

By leverage Cisco AP 1815i, the Cisco 1100 Series WLAN delivers industry-leading performance for highly secure and reliable wireless connections and provides a robust mobility end-user experience. For more detail specific information with Cisco Access point 1815i is available at: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1815-series-access-points/datasheet-c78-738243.html.

Wireless Connectivity for Cisco 1100 Series ISR

This module describes how to configure the WiFi card to the internal switch interface on the Cisco C1100 Integrated Services Routers (ISRs).

The WiFi card is connected to the internal switch interface, the *Wlan-GigabitEthernet* interface. The configuration of this interface is identical to the *GigabitEthernet 0/1/0* interface.

For Cisco 1111-8P Series of ISRs, it is always *Wlan-GigabitEthernet 0/1/8*; and for Cisco 1111-4P, 1116-4P, and 1117-4P Series of ISRs, is always *Wlan-GigabitEthernet 0/1/4*.

```
Router# show run int Wlan-GigabitEthernet 0/1/4
Building configuration...

Current configuration : 43 bytes
!
interface Wlan-GigabitEthernet0/1/4
end

Router#
```

Module Managment

The router configures, manages, and controls the supported interfaces and modules using the module management facility built in its architecture. This new centralized module management facility provides a common way to control and monitor all the modules in the system regardless of their type and application.

Slot and Subslots for WLAN

This section contains information on slots and subslots for WLAN. Slots specify the chassis slot number in your router and subslots specify the slot where the service modules are installed.

The table below describes the slot number for the Cisco 1100 Series ISR models.

Table 1: Slot Numbers for Cisco 1100 Series ISR Models

Cisco 1100 Series SKU	WiFi Slot
C1111-8PWB	0/2
C1111-8PLTEEAWB	0/3
C1113-8PWE	0/2
C1113-8PMWE	0/3
C1113-8PLTEEAWE	0/4
C1111-4PWE	0/2
C1116-4PLTEEAWE	0/4
C1116-4PWE	0/3
C1117-4PLTEEAWE	0/4
C1117-4PWE	0/3
C1117-4PMLTEEAWE	0/4

Cisco 1100 Series SKU	WiFi Slot
C1117-4PMWE	0/3

Note

- The WiFi slot is 0/2, if there is no 4G-LTE Advanced capability or no DSL configured.
- The WiFi slot is 0/3, if the model has either the 4G-LTE Advanced or VDSL/ADSL funtionalities.
- The WiFi slot is 0/4, if the model has both 4G-LTE Advanced or VDSL/ADSL funtionalities
- There will be no WiFi slot on the non-WiFi SKUs.

Supported WiFi Cards

The supported WiFi card Product IDs (PIDs) are as follows:

- ISR-AP1100AC-A
- ISR-AP1100AC-B
- ISR-AP1100AC-H
- ISR-AP1100AC-D
- ISR-AP1100AC-E
- ISR-AP1100AC-F
- ISR-AP1100AC-N
- ISR-AP1100AC-R
- ISR-AP1100AC-Q
- ISR-AP1100AC-Z

```
Router#show platform

Chassis type: C1111-8PLTELAWN

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         C1111-8PLTELAWN     ok                    00:04:56
 0/0      C1111-2x1GE         ok                    00:02:41
 0/1      C1111-ES-8          ok                    00:02:40
 0/2      C1111-LTE           ok                    00:02:41
 0/3      ISR-AP1100AC-N      ok                    00:02:41
R0        C1111-8PLTELAWN     ok, active            00:04:56
F0        C1111-8PLTELAWN     ok, active            00:04:56
P0        PWR-12V             ok                    00:04:30

Slot      CPLD Version        Firmware Version
--------- ------------------- ----------------------------------------
0         17100501            16.6(1r)RC3
R0        17100501            16.6(1r)RC3
F0        17100501            16.6(1r)RC3
```

```
Router#
```

Implementing Modules on Your Router

Accessing Your Module Through a Console Connection

Before you can access the modules, you must connect to the host router through the router console or through Telnet. After you are connected to the router, you must configure an IP address on the Gigabit Ethernet interface connected to your module. Open a session to your module using the **hw-module session** command in privileged EXEC mode on the router.

To establish a connection to the module, connect to the router console using Telnet or Secure Shell (SSH) and open a session to the switch using the **hw-module session** *slot/subslot* command in privileged EXEC mode on the router.

Use the following configuration examples to establish a connection:

- The following example shows how to open a session from the router using the **hw-module session** command:

```
Router# hw-module session slot/card
Router# hw-module session 0/2 endpoint 0

Establishing session connect to subslot 0/2
```

- The following example shows how to exit a session from the router, by pressing **Ctrl-A** followed by **Ctrl-Q** on your keyboard:

```
type ^a^q
picocom v1.7

port is        : /dev/ttyS3
flowcontrol    : none
baudrate is    : 9600
parity is      : none
databits are   : 8
escape is      : C-a
local echo is  : no
noinit is      : no
noreset is     : no
nolock is      : yes
send_cmd is    : sz -vv
receive_cmd is : rz -vv
imap is        :
omap is        :
emap is        : crcrlf,delbs,

Terminal ready
```

Deactivating a Module

A module can be removed from the router without first being deactivated. However, we recommend that you perform a graceful deactivation (or graceful power down) of the module before removing it. To perform a graceful deactivation, use the **hw-module subslot** *slot/subslot* **stop** command in EXEC mode.

Note When you are preparing for an OIR of a module, it is not necessary to independently shut down each of the interfaces before deactivating the module. The **hw-module subslot** *slot/subslot* **stop** command in EXEC mode automatically stops traffic on the interfaces and deactivates them along with the module in preparation for OIR. Similarly, you do not have to independently restart any of the interfaces on a module after OIR.

The following example shows how to use the **show facility-alarm status** command to verify if any critical alarm is generated when a module is removed from the system:

```
Device# show facility-alarm status
System Totals  Critical: 5  Major: 1  Minor: 0

Source                  Severity      Description [Index]
------                  --------      -------------------
Power Supply Bay 1      CRITICAL      Power Supply/FAN Module Missing [0]
GigabitEthernet0/0/0    CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/1    CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/2    CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/3    CRITICAL      Physical Port Link Down [1]
xcvr container 0/0/0    INFO          Transceiver Missing [0]
xcvr container 0/0/1    INFO          Transceiver Missing [0]
xcvr container 0/0/2    INFO          Transceiver Missing [0]
xcvr container 0/0/3    INFO          Transceiver Missing [0]
V: 1.0v PCH R0/18       MAJOR         Volt Above Normal [3]
```

Note A critical alarm (Active Card Removed OIR Alarm) is generated even if a module is removed after performing graceful deactivation.

Deactivating Modules and Interfaces in Different Command Modes

You can deactivate a module and its interfaces using the **hw-module subslot** command in one of the following modes:

- If you choose to deactivate your module and its interfaces by executing the **hw-module subslot** *slot/subslot* **shutdown unpowered** command in global configuration mode, you are able to change the configuration in such a way that no matter how many times the router is rebooted, the module does not boot. This command is useful when you need to shut down a module located in a remote location and ensure that it does not boot automatically when the router is rebooted.
- If you choose to use the **hw-module subslot** *slot/subslot* **stop** command in EXEC mode, you cause the module to gracefully shut down. The module is rebooted when the **hw-module subslot** *slot/subslot* **start** command is executed.

To deactivate a module and all of its interfaces before removing the module, use one of the following commands in global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	**hw-module subslot** *slot*/*subslot* **shutdown unpowered**	Deactivates the module located in the specified slot and subslot of the router, where:

	Command or Action	Purpose
	Example: `Router(config)# hw-module subslot 0/2 shutdown unpowered`	• *slot*—Specifies the chassis slot number where the module is installed. • *subslot*—Specifies the subslot number of the chassis where the module is installed. • **shutdown**—Shuts down the specified module. • **unpowered**—Removes all interfaces on the module from the running configuration and the module is powered off.
Step 2	**hw-module subslot** *slot/subslot* [**reload** | **stop** | **start**] **Example:** `Router# hw-module subslot 0/2 stop`	Deactivates the module in the specified slot and subslot, where: • *slot*—Specifies the chassis slot number where the module is installed. • *subslot*—Specifies the subslot number of the chassis where the module is installed. • **reload**—Stops and restarts the specified module. • **stop**—Removes all interfaces from the module and the module is powered off. • **start**—Powers on the module similar to a physically inserted module in the specified slot. The module firmware reboots and the entire module initialization sequence is executed in the IOSd and Input/Output Module daemon (IOMd) processes.

Reactivating a Module

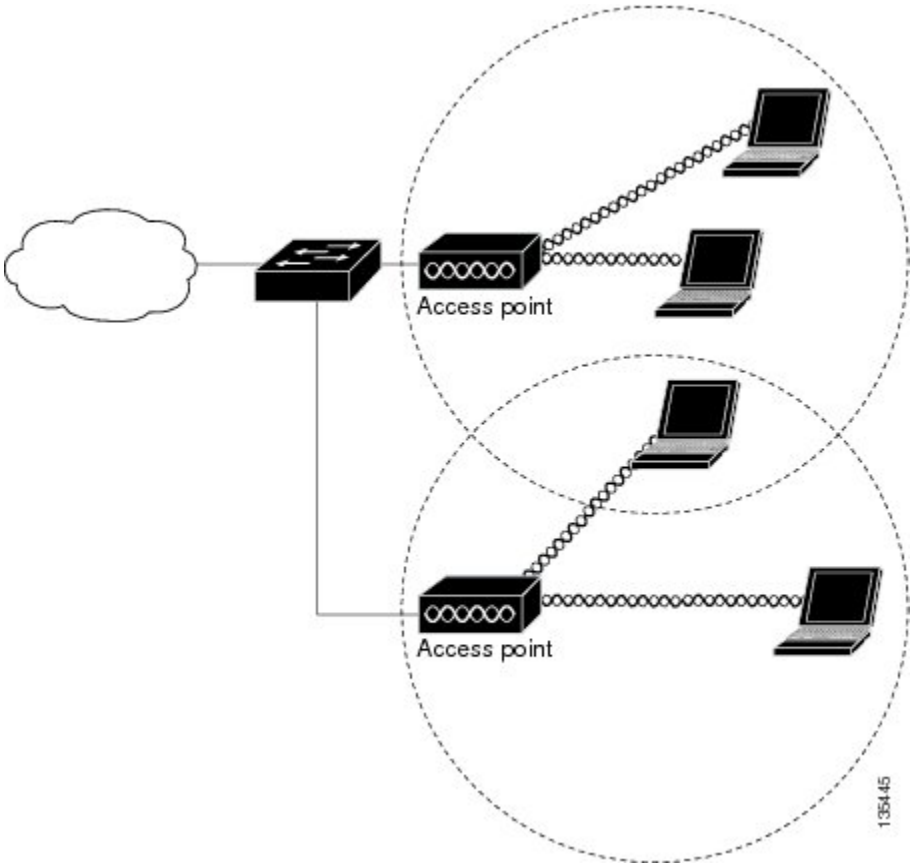
If, after deactivating a module using the **hw-module subslot** *slot/subslot* **stop** command, you want to reactivate it without performing an OIR, use one of the following commands (in privileged EXEC mode):

- **hw-module subslot** *slot/subslot* **start**
- **hw-module subslot** *slot/subslot* **reload**

Access Points

An access point connected directly to a wired LAN provides a connection point for wireless users. If more than one access point is connected to the LAN, users can roam from one area of a facility to another without losing their connection to the network. As users move out of range of one access point, they automatically connect to the network (associate) through another access point. The roaming process is seamless and transparent to the user. The figure below shows access points acting as root units on a wired LAN.

Figure 1: Access Points as Root Units on a Wired LAN



In an all-wireless network, an access point acts as a stand-alone root unit. The access point is not attached to a wired LAN; it functions as a hub linking all stations together. The access point serves as the focal point for communications, increasing the communication range of wireless users. Figure below shows an access point in an all-wireless network.

Configuring and Deploying the Access Point

This section describes how to connect the access point to a wireless LAN controller. The configuration process takes place on the controller. See the Cisco Wireless LAN Controller Configuration Guide for additional information.

The Controller Discovery Process

The access point uses standard Control and Provisioning of Wireless Access Points Protocol (CAPWAP) to communicate between the controller and other wireless access points on the network. CAPWAP is a standard, inter-operable protocol which enables an access controller to manage a collection of wireless termination points. The discovery process using CAPWAP is identical to the Lightweight Access Point Protocol (LWAPP) used with previous Cisco Aironet access points. LWAPP-enabled access points are compatible with CAPWAP, and conversion to a CAPWAP controller is seamless. Deployments can combine CAPWAP and LWAPP software on the controllers.

The functionality provided by the controller does not change except for customers who have Layer 2 deployments, which CAPWAP does not support.

In a CAPWAP environment, a wireless access point discovers a controller by using CAPWAP discovery mechanisms and then sends it a CAPWAP join request. The controller sends the access point a CAPWAP join response allowing the access point to join the controller. When the access point joins the controller, the controller manages its configuration, firmware, control transactions, and data transactions.

Note For additional information about the discovery process and CAPWAP, see the Cisco Wireless LAN Controller Software Configuration Guide. This document is available on Cisco.com.

Note CAPWAP support is provided in controller software release 8.5 or later. However, your controller must be running the release that supports Cisco 1100 Series access points.

Note You cannot edit or query any access point using the controller CLI if the name of the access point contains a space.

Note Make sure that the controller is set to the current time. If the controller is set to a time that has already passed, the access point might not join the controller because its certificate may not be valid for that time.

Access points must be discovered by a controller before they can become an active part of the network. The access point supports these controller discovery processes:

- Layer 3 CAPWAP discovery—Can occur on different subnets than the access point and uses IP addresses and UDP packets.
- Locally stored controller IP address discovery—If the access point was previously joined to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point's non-volatile memory. This process of storing controller IP addresses on an access point for later deployment is called priming the access point. For more information about priming, see the "Performing a Pre-Installation Configuration" section.
- DHCP server discovery—This feature uses DHCP option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability. For more information about DHCP option 43, see the "Configuring DHCP Option 43" section.
- DNS discovery—The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-CAPWAP-CONTROLLER.localdomain, where localdomain is the access point domain name. Configuring the CISCO-CAPWAP-CONTROLLER provides backwards compatibility in an existing customer deployment. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.localdomain. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.

Deploying the Access Point on the Wireless Network

Procedure

	Command or Action	Purpose
Step 1	Connect and power up the router.	
Step 2	Observe the wireless LAN LED (for LED descriptions, see “Checking the Access Point LED” section).	
Step 3	Reconfigure the Cisco wireless LAN controller so that it is not the primary controller.	**Note** A primary Cisco wireless LAN controller should be used only for configuring access points and not in a working network.

Checking the Wireless LAN LED

Note It is expected that there will be small variations in the LED color intensity and hue from unit to unit. This is within the normal range of the LED manufacturer’s specifications and is not a defect.

The wireless LAN status LED indicates various conditions which are described in Table.

Table 2: Wireless LAN LED

Message Type	LED State	Message Meanings
Boot loader status sequence	Blinking Green	DRAM memory test in progress
		DRAM memory test OK
		Board initialization in progress
		Initializing FLASH file system
		FLASH memory test OK
		Initializing Ethernet
		Ethernet OK
		Starting the Cisco AP-OS operating system of the AP
		Initialization successful

Message Type	LED State	Message Meanings
Association status	Chirping Green	Normal operating condition, but no wireless client associated
	Green	Normal operating condition with at least one wireless client association
Operating status	Blinking Amber	Software upgrade is in progress.
	Cycling through Green, Red, and Amber	Discovery/join process is in progress.
	Rapidly cycling through Red, Green, Amber, and off.	Access point location command invoked from controller web interface.
	Blinking Red	Ethernet link is not operational.
Boot loader warnings	Blinking Amber	Configuration recovery in progress (Mode button pushed for 2 to 3 seconds)
	Red	Ethernet failure or image recovery (Mode button pushed for 20 to 30 seconds)
	Blinking Green	Image recovery in progress (Mode button released)
Boot loader errors	Red	DRAM memory test failure
	Blinking Red and Amber	FLASH file system failure
	Blinking Red and off	One of the following: • Environment variable failure • Bad MAC address • Ethernet failure during image recovery • Boot environment failure • No Cisco image file • Boot failure

Miscellaneous Usage and Configuration Guidelines

Using the reset command you can reset the AP to the default factory-shipped configuration.

```
hw-module subslot x/y error-recovery password_reset
```

Note Since this is an IOS command, you must run this command on the Cisco 1100 router console, instead of the AP console.

The AP configuration files are cleared. This resets all configuration settings to factory defaults, including passwords, encryption keys, the IP address, and the SSID. However, the regulatory domain provisioning is not reset.

Note When you run the **hw-module subslot x/y error-recovery password_reset** command, the AP module automatically reloads to restore the configuration settings and enters the maintenance mode. In the maintenance mode, the AP module is on power on mode. When the module configuration reset is confirmed through the console or web UI, the **hw-module subslot x/x reload force** command reloads the AP and then quits the maintenance mode.

Important Information for Controller-Based Deployments

Keep these guidelines in mind when you use the Cisco 1100 series access points:

- The access point can only communicate with Cisco wireless LAN controllers.
- The access point does not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point joins it.
- CAPWAP does not support Layer 2. The access point must get an IP address and discover the controller using Layer 3, DHCP, DNS, or IP subnet broadcast.
- The access point console port is enabled for monitoring and debug purposes. All configuration commands are disabled when the access point is connected to a controller.

Deploying Cisco Mobility Express

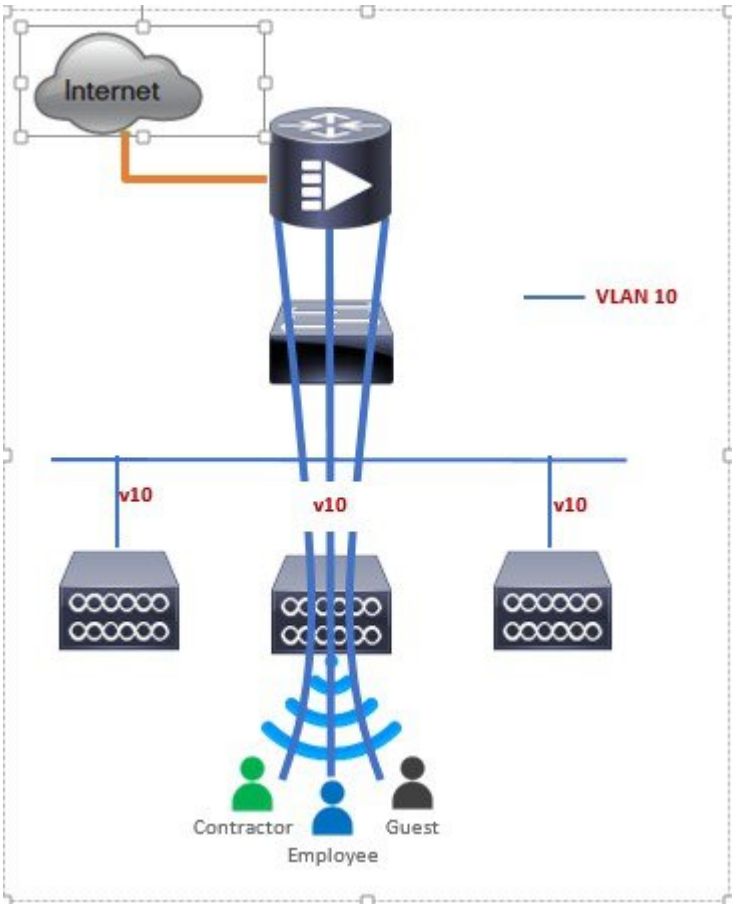
Pre-Requisites for Deploying Mobility Express Solution

1. It is recommended not to have any other Cisco Wireless LAN Controllers; neither appliance nor virtual in the same network during set up or during daily operation of a Cisco Mobility Express network.
2. Decide on the first Access Point to be configured as a primary Access Point. This Access Point should be capable of supporting the Wireless LAN Controller function.
3. A DHCP server must be available on the network so that Access Points and clients can obtain an IP Address. Starting AireOS® Release 8.4.100.0 or later, one can configure a DHCP server on the primary Access Point as well but this is typically used for Site Survey.

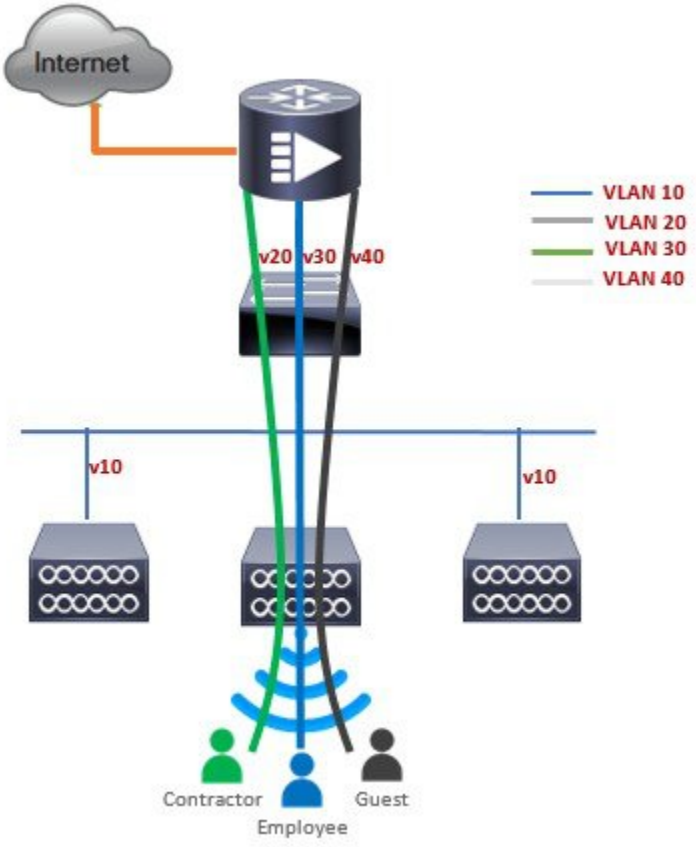
Connecting Mobility Express Capable Access Point to the Network

Depending on the deployment, Mobility Express capable Access Points can be connected to an access port or a trunk port on the switch.

If Access Points and WLANs are all on the same network, Mobility Express capable Access Points can connect to an access port on the switch as shown below.



On Mobility Express, management traffic is untagged. If Access Points and WLANs are all on different VLANs, Mobility Express capable Access Points will connect to a trunk port on the switch and traffic for individual WLANs will be switched locally on individual VLANs. Shown below is a deployment with Access Points and WLANs on different VLANs.




```
interface GigabitEthernet1/0/37
description » Connected to Master AP «
switchport trunk native vlan 40
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk
```

Determining image on the Access Point

The Cisco 1100 Series ISR access points can either have CAPWAP image or the Cisco Mobility Express image which is capable of running the virtual Wireless LAN controller function on the Access Point.

To determine the image and capability of an Access Point, follow the procedure below:

Procedure

	Command or Action	Purpose
Step 1	Login to the Access Point CLI using a console and type **AP#show version** and check the full output of show version. The default login credentials are Username:**Cisco** and Password:**Cisco**.	
Step 2	If **show version** output does not display AP Image Type and AP Configuration parameters	`cisco ISR-AP1100AC-B ARMv7 Processor rev 5 (v7l) with 1016284/594068K bytes of`

	Command or Action	Purpose
	as highlighted below, it means that AP is running the CAPWAP image and a conversion to Cisco Mobility Express is required if you want to run the controller function on the Access Point. To convert from a CAPWAP Access Point to Mobility Express, go to Conversion section.	memory. Processor board ID AP Running Image : 192.0.2.1 Primary Boot Image : 192.0.2.2 Backup Boot Image : 192.0.2.3 AP Image type : MOBILITY EXPRESS IMAGE AP Configuration : MOBILITY EXPRESS CAPABLE 1 Gigabit Ethernet interfaces 2 802.11 Radios Radio FW version : e1c63a0bb171f78c5800c1478007abc1 NSS FW version : not available If the show version displays AP Image Type: MOBILITY EXPRESS IMAGE and AP Configuration: NOT MOBILITY EXPRESS CAPABLE , it means that even though the Access Point has the Cisco Mobility Express image, it is configured to run as a CAPWAP Access Point. In this case Access Point will not run the controller function and will not participate in the primary Election process upon failure of the active primary AP. cisco ISR-AP1100AC-B ARMv7 Processor rev 5 (v7l) with 1016284/754820K bytes of memory. Processor board ID AP Running Image : 192.0.2.1 Primary Boot Image : 192.0.2.2 Backup Boot Image : 192.0.2.3 AP Image type : MOBILITY EXPRESS IMAGE AP Configuration : NOT MOBILITY EXPRESS CAPABLE 1 Gigabit Ethernet interfaces 2 802.11 Radios Radio FW version : e1c63a0bb171f78c5800c1478007abc1 NSS FW version : not available For this AP to run the controller function, AP Configuration has to be changed to MOBILITY EXPRESS CAPABLE . To change the AP Configuration, execute the following command from the AP CLI. AP#ap-type mobility-express tftp:// Access Point will reboot and after it comes up, it will be capable of running the controller function. You can check the output of show version again to confirm that AP Configuration has changed to MOBILITY EXPRESS CAPABLE . If the show version displays AP Image Type: MOBILITY EXPRESS IMAGE and AP Configuration: MOBILITY EXPRESS

	Command or Action	Purpose

		CAPABLE , it means that the Access Point has the Mobility Express image and is capable of running the controller function. For this scenario, the output of the show version is shown below:
		`cisco ISR-AP1100AC-B ARMv7 Processor rev 5 (v7l) with 1016284/594068K bytes of memory.`
		`Processor board ID`
		`AP Running Image : 192.0.2.1`
		`Primary Boot Image : 192.0.2.2`
		`Backup Boot Image : 192.0.2.3`
		`AP Image type : MOBILITY EXPRESS IMAGE`
		`AP Configuration : MOBILITY EXPRESS CAPABLE`
		`1 Gigabit Ethernet interfaces`
		`2 802.11 Radios`
		`Radio FW version : e1c63a0bb171f78c5800c1478007abc1`
		`NSS FW version : not available`

Converting Access Point from CAPWAP to Cisco Mobility Express

One can convert an Access Point running CAPWAP to Cisco Mobility Express and vice versa.

Cisco Mobility Express support on 11ac Wave 2 Access Points is introduced in different AireOS releases and it is important to note that before an Access Point can be converted to Mobility Express, it must have the minimum AireOS CAPWAP image which supported Cisco Mobility Express capability for that Access Point. Given below is the minimum OS release for an Access Point which will support conversion from CAPWAP to Cisco Mobility Express.

Access Point	Minimum AireOS Release with CAPWAP image
Cisco 1100 Series	Cisco IOS XE Everest 16.6.2 Release

Note If the CAPWAP image on the Access Point is older than the minimum AireOS release capable of supporting Cisco Mobility Express, Access Point MUST first join a WLC running the minimum AireOS release or higher to upgrade its CAPWAP image. After the CAPWAP image of the AP has been upgraded, conversion of AP from CAPWAP to Mobility Express can be performed.

To perform a conversion on an Access Point running CAPWAP to Mobility Express, follow the procedure below:

Procedure

	Command or Action	Purpose
Step 1	Download the conversion image for the Access Point from cisco.com to the TFTP server. It is a tar file. Do not untar the file. The following	

	Command or Action	Purpose
	table lists the Cisco Mobility Express software for Cisco Wireless Release 8.4.100.0.	
Step 2	Login to the Access Point	

Step 3	Execute AP#show version on the Access Point CLI. From the show version output, you can determine the AP Image type and AP Configuration and can then proceed with the conversion	Case 1: If the AP Image type is MOBILITY EXPRESS IMAGE and AP configuration is NOT MOBILITY EXPRESS CAPABLE, enter the command below to change the AP Configuration to MOBILITY EXPRESS CAPABLE .
		`AP#ap-type mobility-express`
		Example:
		`cisco ISR-AP1100AC-E ARMv7 Processor rev 5 (v7l) with 1016284/840700K bytes of memory.`
		`Processor board ID`
		`AP Running Image : 192.0.2.1`
		`Primary Boot Image : 192.0.2.2`
		`Backup Boot Image : 192.0.2.3`
		`1 Gigabit Ethernet interfaces`
		`2 802.11 Radios`
		`Radio FW version :`
		`e1c63a0bb171f78c5800c1478007abc1`
		`NSS FW version : not available`
		`Router#ap-type mobility-express`
		`Changing AP Type to Mobility Express`
		`Writing reload timestamp (Wed May 24 17:17:53 UTC 2017) to disk`
		`Router#[05/24/2017 17:17:54.4699] UBIFS: un-mount UBI device 0, volume 3`
		`[05/24/2017 17:17:54.5199] UBIFS: background thread "ubifs_bgt0_3" stops`
		`[05/24/2017 17:17:56.6099] reboot: Restart`
		Note Since the Access Point has AP Image type: MOBILITY EXPRESS IMAGE, a new image will not be downloaded. After the command is executed, the Access Point will reboot and after it comes up, the AP Configuration will be changed to MOBILITY EXPRESS CAPABLE.
		Case 2 : If the AP Image type and AP Configuration are not available, it means that the AP is running CAPWAP image. To do the conversion, execute the command below:

	Command or Action	Purpose

		`Router#ap-type mobility-express tftp://<TFTP Server IP>/<path to tar file>`
		Example:
		`Router#ap-type mobility-express tftp://10.74.5.99/8.4CCO/ap1g5`
		`Starting the ME image download...`
		`It may take a few minutes to finish download.`
		`If it is longer, please abort command, check network connection and try again`
		`##########################################################`
		`100.0%`
		`Image transfer complete.`
		`Image downloaded, writing to flash...`
		`do CHECK_ME, part1 is active part`
		`Image signing verify success.`
		`upgrade.sh: btldr rel is 33 vs 33, does not need update`
		`upgrade.sh: part to upgrade is part2`
		`upgrade.sh: activate part2, set BOOT to part2`
		`upgrade.sh: AP primary version: 8.4.100.0`
		`Archive done.`
		`[*10/11/2017 23:05:22.7599] AP Type changed: CAPWAP to ME. AP Mode changed to flexconnect. AP Rebooting...`
		`[*10/11/2017 23:05:22.7699] AP Rebooting: Reset Request from Controller(AP Type Changed from CAPWAP to ME)`
		`Writing reload timestamp (Wed Oct 11 23:05:22 UTC 2017) to disk`
		`M-P2B#[10/11/2017 23:05:23.9699] UBIFS: un-mount UBI device 0, volume 3`
		`[10/11/2017 23:05:24.0199] UBIFS: background thread "ubifs_bgt0_3" stops`
		`The system is going down NOW!`
		`Sent SIGKILL to all processes.1099]`
		`Requesting system reboot99]`
		`[10/11/2017 23:05:26.1099] reboot: Restarting`
		Note After the image download is complete, it will be written to the flash followed by a reboot. After the AP comes up, AP Image type will be MOBILITY EXPRESS IMAGE and AP Configuration will MOBILITY EXPRESS CAPABLE .

	Command or Action	Purpose
Step 4	If this is the first Access Point in the network, it will start the controller function and will broadcast the CiscoAirProvison SSID.	

Converting Access Point from Cisco Mobility Express to CAPWAP

There are typically two reasons why one would want to convert an Access Point running Mobility Express image to CAPWAP. There are as follows:

1. You want to keep the Access Point in a Mobility Express deployment but do not want the Access point to participate in the primary election process upon a failover of the primary AP.
2. You want to migrate one or more Access Points with Mobility Express to an appliance or vWLC based deployment.

1. If your reason to convert to CAPWAP is 1 above, follow the procedure below:
   a. Login to the Access Point CLI either through console or ssh and go to exec mode. If you are trying to convert the primary AP to CAPWAP, connecting a console will lead you to the controller CLI. To get to the AP CLI, type apciscochell at the controller prompt and login to the Access Point shell.
   b. Execute ap#ap-type capwap CLI. This will change the AP Configuration to NOT MOBILITY EXPRESS and the Access Point will no longer participate in the primary election process.

2. If your reason to convert to CAPWAP is 2 above, follow the procedure below:
   a. Login to the Access Point CLI either via console or ssh and go to exec mode.
   b. Execute the following CLI.

```
(Cisco Controller) >config ap unifiedmode <switch_name> <switch_ip_address>

<switch_name> and <switch_ip_address> is the name and IP address respectively of the
 WLC to which the APs need to be migrate.
```

Note The above command converts all connected Access Points with AP Configuration: MOBILITY EXPRESS CAPABLE to AP Configuration: NOT MOBILITY EXPRESS CAPABLE . When this command is issued, the APs are reloaded, and they come back up and look for the controller (switch_ip_address) to join.

Configuring Cisco Mobility Express controller

CLI Setup Wizard

To use the Setup Wizard from CLI, you must connect to the console port of the Access Point. The default parameters for the console ports are 9600 baud, eight data bits, one stop bit, and no parity. The console ports do not support hardware flow control.

After connecting to the console port on the Access Point, power up the Access Point. After a few minutes, Access Point will start the Controller.

To configure the Mobility Express controller, follow the steps as shown in the example below:

```
System Name [Cisco_2c:3a:40] (31 characters max): me-wlc
Enter Country Code list (enter 'help' for a list of countries) [US]:

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: no

Note! Default NTP servers will be used

Management Interface IP Address: 192.0.2.1
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 192.0.2.2
Cleaning up Provisioning SSID
Create Management DHCP Scope? [yes][NO]: yes
DHCP Network : 192.0.2.1
DHCP Netmask : 255.255.255.0
Router IP: 40.40.40.1
Start DHCP IP address: 192.0.2.3
Stop DHCP IP address: 192.0.2.4
DomainName :
DNS Server : [OPENDNS][user DNS]
Create Employee Network? [YES][no]: YES
Employee Network Name (SSID)?: WestAutoBody-Employee
Employee VLAN Identifier? [MGMT][1-4095]: MGMT
Employee Network Security? [PSK][enterprise]: PSK
Employee PSK Passphrase (8-38 characters)?: Cisco123
Re-enter Employee PSK Passphrase: Cisco123
Create Guest Network? [yes][NO]: YES
Guest Network Name (SSID)?: WestAutoBody-Guest
Guest VLAN Identifier? [EMPLOYEE][1-4095]: EMPLOYEE
Guest Network Security? [WEB-CONSENT][psk]: WEB-CONSENT
Create Guest DHCP Scope? [yes][NO]: NO
Enable RF Parameter Optimization? [YES][no]: YES
Client Density [TYPICAL][Low][High]: TYPICAL
Traffic with Voice [NO][Yes]: Yes

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
Cleaning up Provisioning SSID
```

Note The Access Point will reboot and after it comes back up, login to the Mobility Express controller WebUI from the browser using https://<mangement_ip_address> Cisco Mobility Express controller uses a self-signed certificate for HTTPS. Therefore, all browsers display a warning message and asks whether you wish to proceed with an exception or not when the certificate is presented to the browser. Accept the risk and proceed to access the Mobility Express Wireless LAN Controller login page.

Over-the-Air Setup Wizard

Over-the-air is a simple and easy way to configure Mobility Express out of the box. Over-the-Air provisioning can be done using a WiFi enabled device or the Cisco Wireless app which can be downloaded from App Store for iOS devices and Play Store for Android Devices. The Cisco Wireless app provides a minimum set of configurable options to deploy Mobility Express in just a few minutes.

Procedure

	Command or Action	Purpose
Step 1	When the LED on the Access Point chirps green, connect a WiFi enabled laptop to the CiscoAirProvision SSID. The default password is password. The laptop will get an IP address from subnet 192.168.1.0/24.	**Note** CiscoAirProvision SSID is broadcast at 2.4GHz.
Step 2	Open a web browser and browse to http://mobilityexpress.cisco. This will redirect to configuration wizard and the admin account page will appear.	

Step 3	Create an admin account on the controller by specifying the following parameters and then click on the Start button.	• Enter the admin username. Maximum up to 24 ASCII characters.
		• Enter the password. Maximum up to 24 ASCII characters. When specifying a password, ensure that:
		  • The password must contain characters from at least three of the following classes – lowercase letters, uppercase letters, digits, special characters.
		  • No character in the password can be repeated more than three times consecutively.
		  • The new password must not be the same as the associated username and the username reversed.
		  • The password must not be cisco, ocsic, or any variants obtained by changing the capitalization of letters of the word Cisco. In addition, you cannot substitute 1, I, or ! for i, 0 for o, or $ for s.

Step 4	In the Set up Your Controller section, configure the following:	• Enter the System Name • Select the Country from the drop-down list • Date and Time should be auto-filled but one can manually configure it as well • Select the Timezone from the drop-down list

	Command or Action	Purpose
		• Enter the IP address of NTP Server if there is one available. If left blank, NTP Pools will be automatically configured • Enter the Management IP Address of the controller • Enter the Subnet Mask • Enter the Default Gateway
Step 5	Disable Enable DHCP Server(Management Network) if an external DHCP server is being used. If internal DHCP server on the Mobility Express controller has to be used, specify the DHCP server related information.	
Step 6	Click Next.	
Step 7	In the Create Your Wireless Network, under Employee Network, configure the following:	• Enter the Network Name • Select Security as WPA2 Personal or WPA2 Enterprise from the drop-down list • If WPA2 Personal is selected, enter the Passphrase
Step 8	One can also enable RF Parameter Optimization and configure the following:	• Move the Client Density slider as needed • From the Traffic Type, select Data or Data and Voice
Step 9	Click Next.	
Step 10	Confirm the settings on the page and click on the Apply button. The Access Point will reboot and after it comes up, it will run the controller.	**Note** The Access Point will reboot and after it comes back up, login to the Mobility Express controller WebUI from the browser using https:<management_ip_address>. Cisco Mobility Express controller uses a self-signed certificate for HTTPS. Therefore, all browsers display a warning message and asks whether you wish to proceed with an exception or not when the certificate is presented to the browser. Accept the risk and proceed to access the Mobility Express Wireless LAN Controller login page.

Network Plug and Play

Introduction

The Cisco Network Plug and Play solution provides a simple, secure, unified, and integrated offering for enterprise network customers to ease new site rollouts for provisioning Cisco Mobility Express. The solution allows use of Cloud Redirection service, on-prem, or combination which provide a unified approach to provision enterprise networks comprised of Cisco Mobility Express, Cisco routers, switches, with a near zero touch deployment experience.

You can use the Cisco Network Plug and Play application to pre-provision the site and add Cisco Mobility Express capable access points to the site. This includes entering access point information and uploading a controller configuration file for virtual controller which will run on Mobility Express capable access points.

When an installer installs and powers up the Cisco Mobility Express capable access points, it auto-discovers the Cisco APIC-EM controller by using the DHCP, DNS or cloud redirection service. After the auto-discovery process is complete, the AP downloads the controller configuration file from local PnP server, or communicates with the cloud redirection service for direction to target PnP server.

Pre-Requisites

- APIC-EM Release 1.4 with Cisco Network Plug and Play, virtually hosted in a Cisco UCS or equivalent server.
- Access Points–Cisco 802.11ac Wave 2 access points running Cisco Mobility Express software.
- Controller Configuration–Cisco Mobility Express controller configuration file to be uploaded on Network PnP.

APIC-EM Discovery Options

1. DHCP server configured with option 43 to allow Cisco Mobility Express capable access points to auto-discover the APIC-EM controller (option 43 is not required if only testing cloud redirection). DHCP option 43 consists of a string value that is a configured DHCP server: option 43 ascii "5A1N;B2;K4;I192.168.1.123;J80"

Note 192.168.1.123 is the IP address of the APCI-EM Server

2. On–prem PnP server can be added to DNS using ‘pnpserver.yourlocal.domain’ If DHCP discovery fails to get the IP address of the APIC-EM controller, for example, because option 43 is not configured, the Cisco Plug and Play Agent falls back on a DNS lookup method. Based on the network domain name returned by the DHCP server, it constructs a fully qualified domain name (FQDN) for the APIC-EM controller, using the preset hostname pnpserver. For example, if the DHCP server returns the domain name " customer.com ", the Cisco Plug and Play IOS Agent constructs the FQDN "pnpserver.customer.com ". It then uses the local name server to resolve the IP address for this FQDN

Cloud redirection service requires a connection to the internet, and valid DNS server that can resolve ‘devicehelper.cisco.com’. The cloud redirection service redirect Cisco Mobility Express Access Point to APIC-EM.

Configuring APIC-EM / Network PnP Server

Site Pre-Provisioning Workflow

Cisco Network Plug and Play allows you to pre-provision and plan for new sites. When you create a new site, Cisco Network Plug and Play enables you to pre-provision Cisco Mobility Express access point(s) controller, configuration file, product ID, and product serial # for selected Access Points. This simplifies and accelerates the time that it takes to get a site fully functional.

To pre-provision a site on your network, perform these steps:

Procedure

	Command or Action	Purpose
Step 1	Importing Cisco Mobility Express controller configuratio	
Step 2	Creating a Project	
Step 3	Adding Cisco Mobility Express capable Access Point to the Project and associating the controller config.	

Importing Cisco Mobility Express Configuration File to Network PnP

Procedure

	Command or Action	Purpose
Step 1	Login to APIC-EM controller and navigate to Network Plug and Play > Configurations	
Step 2	Click on Upload to upload the controller configuration.	
Step 3	Select a controller configuration file from your local machine.	

Creating a Project

Procedure

	Command or Action	Purpose
Step 1	Navigate to Network Plug and Play > Projects.	
Step 2	Enter the name for the Project and click on the Add button.	
Step 3	Click on the Create button to create the Project.	
Step 4		

Adding Cisco Mobility Express Capable Access Point to the Project and Associating the Controller Configuration

Procedure

	Command or Action	Purpose
Step 1	Navigate to Network Plug and Play > Projects.	
Step 2	Click on Add button under Project Devices.	
Step 3	In the Add Device window, enter the following:	• Device Name–Enter the device name; unique for each site • Product ID–Select the Access Point device ID from the drop-down list • Serial Number–Enter the Serial Number of the Mobility Express Access Point • Config–You can either upload a new configuration or select the configuration file which was added earlier
Step 4	Click the Add button.	

APIC-EM Network Plug and Play Deployment Options with Cisco Mobility Express

There are two deployment options supported for deploying Cisco Mobility Express with Network Plug and Play.

APIC-EM controller in Private Cloud

In this deployment option, there will be an On-Prem APIC-EM controller which can be discovered by Cisco Mobility Express Access Points using option 43 or DNS discovery.

Figure 2: APIC-EM controller in Private Cloud flow

Option 43 points to APIC-EM controller IP address. To configure DHCP scope with Option 43, it is important follow the format as shown below. In the example below, 192.168.1.123 is the IP address of APIC-EM controller .

```
ip dhcp pool pnp_device_pool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
option 43 ascii "5A1N;B2;K4;I192.168.1.123;J80"
```

To discover APIC-EM controller using the DNS discovery options, configure the DNS server and domain name on the DHCP scope.

```
ip dhcp pool pnp_device_pool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
```

```
domain-name cisco.com
dns-server 172.20.229.8
```

Cloud Plug and Play Connect Redirect to APIC-EM Controller

Cloud re-direction service uses Cisco public hosted cloud to re-direct Cisco Mobility Express capable access points to APIC-EM controller. The minimal requirement is that the Mobility Express Access Points network have DHCP and DNS, and connectivity reachable to Cisco public cloud. There is no need to configure Option 43 on DHCP scope with this deployment option. A simple test would be to obtain DHCP address and ping 'devicehelper.cisco.com' from where the Mobility Express AP will be deployed.

Figure 3: Cloud Plug and Play Device Redirect to APIC-EM controller flow

Cloud Plug and Play Device Redirect Provisioning Workflow

This section describes the steps to redirect Cisco Mobility Express Access Points to APIC-EM controller using Cloud Plug and Play Connect service.

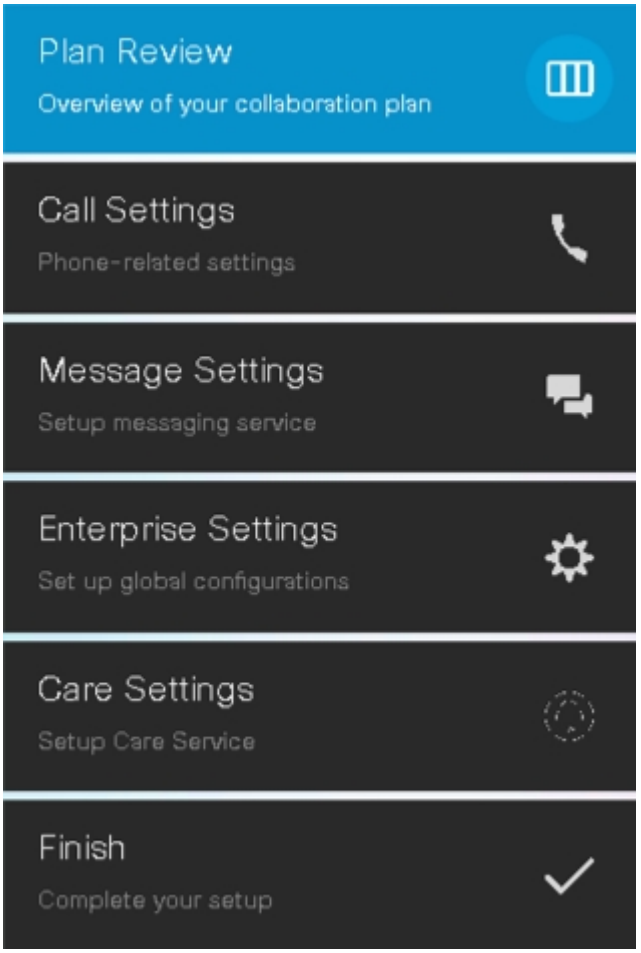
To configure cloud Plug and Play connect redirect service, perform the following steps:

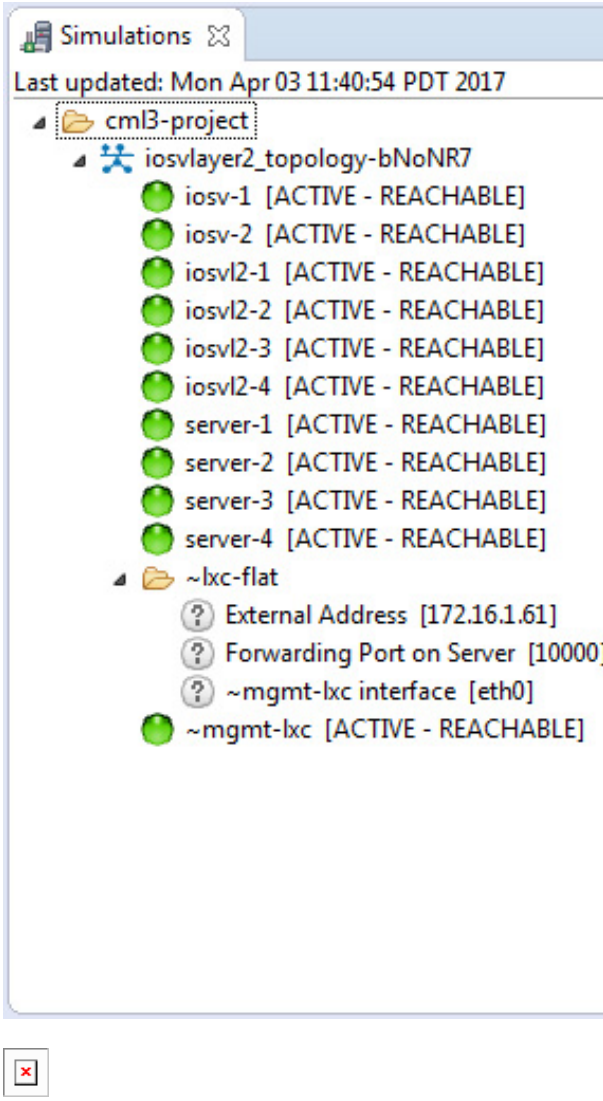
1. Obtain a Smart Account
2. Create APIC-EM Controller Profile
3. Adding Mobility Express capable Access Point to the Devices list
4. Associate Mobility Express capable Access Point to APIC-EM Controller profile

Obtain a Smart Account

Procedure

	Command or Action	Purpose
Step 1	Go to http://software.cisco.com	
Step 2	Request a Smart Account or Log In (existing Smart Account holders).	
Step 3	Click on Controller Profiles. Select a Virtual Account. If you do have one, create a Virtual Account first.	
Step 4	Click on the Add Profile to create a new controller profile.	
Step 5	Select Controller Type as PNP Server from the drop-down list and click on Next.	
Step 6	Enter the following and click Next.	• Profile Name • Description • Select IPv4 or IPv6, HTTP or HTTPS and enter the IP address if the PNP Server

	Command or Action	Purpose
		Note If you select HTTPS, then you would have import a SSL certificate. Also, optionally one can enter information of the secondary controller. 

	Command or Action	Purpose
Step 7	Review the entries and click on Submit button to add the Controller Profile and finally click Done.	

Create APIC-EM Controller Profile

Procedure

	Command or Action	Purpose
Step 1	Go to http://software.cisco.com and login	
Step 2	Navigate to Provisioning > Plug and Play Connect	
Step 3	Click on Controller Profiles. Select a Virtual Account. If you do have one, create a Virtual Account first.	

	Command or Action	Purpose
Step 4	Click the Add Profile to create a new controller profile.	
Step 5	Select Controller Type as PNP Server from the drop-down list and click on Next. .	
Step 6	Enter the following and click Next.	• Profile Name • Description • Select IPv4 or IPv6, HTTP or HTTPS and enter the IP address if the PNP Server **Note** If you select HTTPS, then you would have import a SSL certificate. Also, optionally one can enter information of the secondary controller.
Step 7	Review the entries and click on Submit button to add the Controller Profile and finally click Done.	

Adding Cisco Mobility Express capable Access Point to the Devices List

Procedure

	Command or Action	Purpose
Step 1	Navigate to Provisioning > Plug and Play Connect. Click on Devices.	
Step 2	Click on Devices. Select a Virtual Account. If you do have one, create a Virtual Account first.	
Step 3	Click on Add Devices button to add a new device (Mobility Express Access Point).	
Step 4	Import a csv file with the Device info or select Enter Device info manually. Click Next.	
Step 5	Click on Identify Device button. The Identify Device window will pop up. Enter Serial Number, select Base PID, and Controller Profile(created earlier). Click on the Save button followed by Next button.	
Step 6	Review the entries and click on Submit button to add the Device. Finally, click Done.	
Step 7	Verify that the Device has been added and the status is Pending (Redirection).	

Connecting Cisco Mobility Access Points

To bring up a new Mobility Express site, make sure that Plug and Play service has been configured with Mobility Express Access Points with related controller configuration. If APIC-EM controller in Private Cloud deployment option is used, Option 43 or DNS discovery on DHCP scope must be configured. If Cloud Plug and Play Connect redirect to APIC-EM controller deployment option is used, make sure all the related configuration on Cloud Plug and Play Connect has also been done for successful redirect to APIC-EM controller.

Now, it is time to connect the Mobility Express Access Points at the site. One may connect one or more Access Points at a site. It is important to note that if multiple Mobility Express Access Points are connected at a site, primary Election will happen first and only after primary Access Point has been elected, it will initiate communication with the Network Plug and Play service and download the controller configuration file regardless of the deployment option. The other Access Points will not initiate communicate with the Network Plug and Play service. After the controller configuration file has been downloaded on the Access Point, it will reboot and after it comes up, it will run the controller. The rest of the Access Points at the site will join this primary Access Point as Subordinate Access Points.

Using internal DHCP server on Cisco Mobility Express

Creating a DHCP Scope

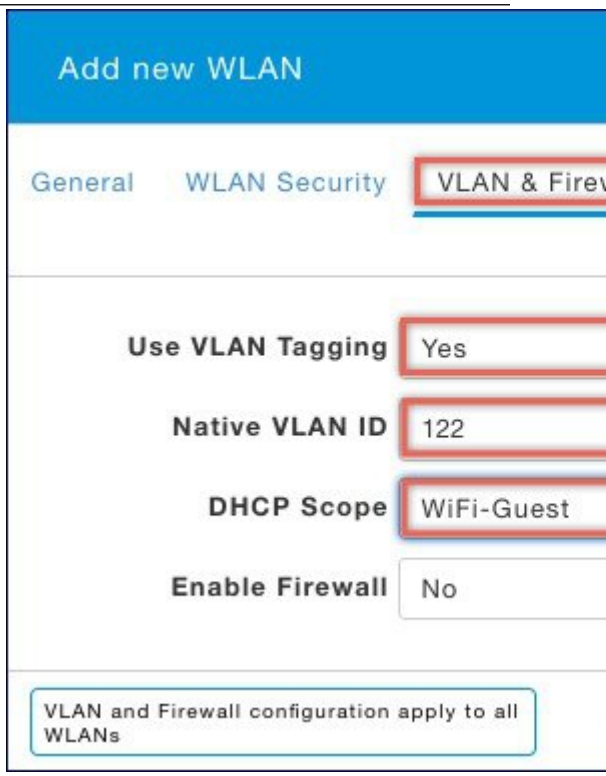
Internal DHCP server can be enabled and DHCP scope created during Day 0 from Setup Wizard as well as in Day 1 using the controller WebUI. Typically, one would create DHCP scopes in Day 1 if they want to associate the scopes with WLANs.

To create a scope and associate it to a WLAN using the controller WebUI, follow the procedure below:

Procedure

	Command or Action	Purpose
Step 1	Navigate to Wireless Settings > DHCP Server > Add new Pool . The Add DHCP Pool window will pop up.	
Step 2	On the Add DHCP Pool window. Enter the following fields:	• Enter the Pool Name for the WLAN • Enable the Pool Status • Enter the VLAN ID for the WLAN • Enter the Lease Period for the DHCP clients. Default is 1 Day • Enter the Network/Mask • Enter the Start IP for the DHCP pool • Enter the End IP for the DHCP pool • Enter the Gateway IP for the DHCP pool

	Command or Action	Purpose
		• Enter the Domain Name (Optional) for the DHCP pool • For Name Servers, select User Defined if one needs to enter IP addresses of Name Servers or select OpenDNS in which case OpenDNS Name Server IP addresses are automatically populated
Step 3	Click Apply.	
Step 4	After creating the scope, it is time to assign the VLAN mapped to the DHCP scope to the WLAN. To assign a VLAN to WLAN, navigate to Wireless Settings > WLANs .	
Step 5	If the WLAN does not exist, create a WLAN or if one does exist, edit the existing WLAN and click on the VLAN and Firewall tab.	
Step 6	On the VLAN and Firewall tab, configure the following:	• Select Yes for Use VLAN Tagging • Enter the Native VLAN ID • Select the DHCP Scope which was created previously for the WLAN. VLAN ID should be automatically populated after the DHCP scope is selected

	Command or Action	Purpose
		
Step 7	Click Apply.	

Configuring Cisco Mobility Express for Site Survey

Cisco 802.11ac Wave 2 access points are capable of running Cisco Mobility Express which a virtual wireless controller function embedded on an Access Point.

Cisco Mobility Express access point running the wireless controller function will also provide wireless connectivity to the clients. It also supports internal DHCP server which enables Access Point to be used for Site Survey.

Introduction

Cisco 802.11ac Wave 2 access points are capable of running Cisco Mobility Express which a virtual wireless controller function embedded on an Access Point.

Cisco Mobility Express access point running the wireless controller function will also provide wireless connectivity to the clients. It also supports internal DHCP server which enables Access Point to be used for Site Survey.

Configuring Mobility Express for Site Survey Using CLI

Procedure

	Command or Action	Purpose
Step 1	Connect to the console of the Access Point.	
Step 2	Power up the Access Point using a power adapter or battery pack.	
Step 3	Wait for the Access Point to boot up completely such that it is running the Wireless Controller and is waiting to be configured.	

Step 4	Configure the Wireless Controller using the CLI Setup Wizard:	**Note** For Site Survey, a DHCP server is required and is supported on Cisco Mobility Express. DHCP Server configuration highlighted below is mandatory if you want to enable DHCP server on Cisco Mobility Express.
		
		`Would you like to terminate autoinstall? [yes]:yes`
		`Enter Administrative User Name (24 characters max):admin`
		`Enter Administrative Password (3 to 24 characters max):Cisco123`
		`Re-enter Administrative Password: Cisco123`
		`System Name:[Cisco_3a:d2:b4] (31 characters max):me-wlc`
		`Enter Country Code list(enter 'help' for a list of countries)[US]:US`
		`Configure a NTP server now?[YES][no]:no`
		`Configure the system time now?[YES][no]:yes`
		`Enter the date in MM/DD/YY format:02/28/17`
		`Enter the time in HH:MM:SS format:11:30:00`
		`Enter timezone location index(enter 'help' for a list of timezones):5`
		`Management Interface IP Address: 10.10.10.2`
		`Management Interface Netmask: 255.255.255.0`
		`Management Interface Default Router: 10.10.10.1`
		`Create Management DHCP Scope?[yes][NO]:yes`
		`DHCP Network: 10.10.10.0`
		`DHCP Netmask: 255.255.255.0`
		`Router IP: 10.10.10.1`
		`Start DHCP IP address: 10.10.10.10`
		`Stop DHCP IP address: 10.10.10.250`
		`DomainName: mewlc.local`
		`DNS Server:[OPENDNS][user DNS]OPENDNS`
		`Create Employee Network?[YES][no]:yes`
		`Employee Network Name(SSID)?:site_survey`

	Command or Action	Purpose
		Employee VLAN Identifier?[MGMT][1-4095]:MGMT Employee Network Security?[PSK][enterprise]:PSK Employee PSK Passphrase (8-38 characters)?: Cisco123 Re-enter Employee PSK Passphrase: Cisco123 Re-enter Employee PSK Passphrase: Cisco123 Create Guest Network? [yes][NO]:NO Enable RF Parameter Optimization?[YES][no]:no Configuration correct? If yes, system will save it and reset.[yes][NO]:yes
Step 5	Wait for the Access Point to boot up completely. After the Wireless controller has started, log back in to the controller using administrative username or password configured during the initial setup wizard.	
Step 6	(Optional): During the CLI setup wizard, Employee Network Security was configured to PSK. This can be disabled for easy association of clients and also disable SSID broadcast to avoid unwanted clients from joining the SSID. To disable PSK and SSID broadcast, enter the following commands in the Controller CLI.	(Cisco Controller)>config wlan disable 1 (Cisco Controller)>config wlan security wpa disable 1 (Cisco Controller)>config wlan broadcast-ssid disable wlan 1 (Cisco Controller)>config wlan enable 1 (Cisco Controller)>save config
Step 7	To configure channel, TX power, and channel bandwidth for the radios, disable the radio first, make the changes and then re-enable it.	To change the 2.4GHz radio to channel 6, follow the steps below: (Cisco Controller)>config 802.11b disable <ap name> (Cisco Controller)>config 802.11b channel <ap name> <ap name> 6 (Cisco Controller)>config 802.11b enable <ap name> To change the 2.4GHz radio Transmit Power to power level 3, follow the steps below: (Cisco Controller)>config 802.11b disable <ap name> (Cisco Controller)>config 802.11b txPower <ap name> <ap name> 3 (Cisco Controller)>config 802.11b enable <ap name> To change the 5 GHz radio to channel 44, follow the steps below: (Cisco Controller)>config 802.11a disable <ap name> (Cisco Controller)>config 802.11a channel <ap name> <ap name> 44 (Cisco Controller)>config 802.11a enable <ap name>

	Command or Action	Purpose

		To change the 5 GHz radio Transmit Power to level 5, follow the steps below:
		`(Cisco Controller)>config 802.11a disable <ap name>`
		`(Cisco Controller)>config 802.11a txPower <ap name> <ap name> 5`
		`(Cisco Controller)>config 802.11a enable <ap name>`
		To change the 5 GHz radio channel width to 40MHz, follow the steps below:
		`(Cisco Controller)>config 802.11a disable <ap name>`
		`(Cisco Controller)>config 802.11a chan_width <ap name> 40`
		`(Cisco Controller)>config 802.11a enable <ap name>`
		If access points are being used for Site Survey, please note the following with respect to the XOR radio.
		a. Default operation state of XOR radio is 2.4GHz.
		b. When the XOR (2.4 GHz) radio is configured to operate at 5GHz, 100MHz frequency separation is required from dedicated 5GHz radio.
		c. When the XOR radio is configured to operate in 5GHz mode on an internal (I) Access Points, the Transmit power (tx) power will be fixed and cannot be modified.
		d. One can configure the XOR radio on internal (I) Access Points from 2.4GHz to 5 and vice versa. On an external (E) Access Point, one must have an external antenna plugged into the DART connector prior to changing any configuration on the XOR radio.
		e. To configure the XOR (2.4GHz) radio to operate at 5GHz on Access Points, follow the steps below:
		`(Cisco Controller) >config 802.11-abgn disable ap`
		`(Cisco Controller) >config 802.11-abgn role ap manual client-serving`
		`(Cisco Controller) >config 802.11-abgn band ap ap 5GHz`
		`(Cisco Controller) >config 802.11-abgn enable ap`

	Command or Action	Purpose

		To configure the XOR radio operating at 5 GHz to channel 40, follow the steps below:
		`(Cisco Controller) >config 802.11-abgn disable ap`
		`(Cisco Controller) >config 802.11-abgn channel ap ap 40`
		`(Cisco Controller) >config 802.11-abgn enable ap`
		To configure the XOR radio operating at 5 GHz channel width to 40MHz, follow the steps below:
		`(Cisco Controller) >config 802.11-abgn disable ap`
		`(Cisco Controller) >config 802.11-abgn chan_width ap 40`
		`(Cisco Controller) >config 802.11-abgn enable ap`

Creating Wireless Networks

Cisco Mobility Express solution supports a maximum of 16 WLANs. Each WLAN has a unique WLAN ID (1 through 16), a unique Profile Name, SSID, and can be assigned different security policies.

Access Points broadcast all active WLAN SSIDs and enforce the policies that you define for each WLAN.

You can configure WLANs with different service set identifiers (SSIDs) or with the same SSID. An SSID identifies the specific wireless network that you want the controller to access. Creating WLANs with the same SSID enables you to assign different Layer 2 security policies within the same wireless LAN. To distinguish among WLANs with the same SSID, you must create a unique profile name for each WLAN. WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on information advertised in beacon and probe responses.

A number of WLAN Security options are supported on Cisco Mobility Express solution and are outlined below:

1. Open
2. WPA2 Personal
3. WPA2 Enterprise (External RADIUS, AP)

For Guest WLAN, a number of capabilities are supported:

1. CMX Guest Connect
2. WPA2 Personal
3. Captive Portal (AP)
4. Captive Portal (External Web Server)

Creating Employee WLANs

Creating Employee WLAN with WPA2 Personal

Procedure

	Command or Action	Purpose
Step 1	Navigate to Wireless Settings > WLANs and then click on Add new WLAN button. The Add new WLAN Window will pop up.	
Step 2	In the Add new WLAN window, on the General page, configure the following:	
Step 3	Click on the WLAN Security and configure the following:	
Step 4	Click Apply.	

Creating Employee WLAN using WPA2 Enterprise with External Radius Server

Procedure

	Command or Action	Purpose
Step 1	Navigate to Wireless Settings > WLANs and then click on Add new WLAN button. The Add new WLAN Window will pop up.	
Step 2	In the Add new WLAN window, on the General page configure the following:	
Step 3	Click on the WLAN Security and configure the following:	
Step 4	Add the Radius server and configure the following:	
Step 5	Click Apply.	

Creating Employee WLAN with WPA2 Enterprise and Authentication Server as AP

Procedure

	Command or Action	Purpose
Step 1	Navigate to Wireless Settings > WLANs and then click on Add new WLAN button. The Add new WLAN Window will pop up.	

	Command or Action	Purpose
Step 2	In the Add new WLAN window, on the General page configure the following:	• Enter the Profile Name. • Enter the SSID.
Step 3	Click on the WLAN Security and configure the following:	• Select Security as WPA2 Enterprise. • Select Authentication Server as AP. **Note** AP is the primary AP running the controller function. In this use case, controller is the Authentication Server and therefore Local WLAN user account must exist to onboard the clients.
Step 4	Click the Apply.	

Creating Employee WLAN with WPA2 Enterprise/External RADIUS and MAC Filtering

Procedure

	Command or Action	Purpose
Step 1	Navigate to Wireless Settings > WLANs and then click on Add new WLAN. The Add new WLAN Window will pop up.	
Step 2	In the Add new WLAN window, on the General tab, configure the following:	• Enter the Profile Name • Enter the SSID
Step 3	Click on the WLAN Security tab and configure the following:	• Enable MAC Filtering • Select Security Type as WPA2 Enterprise • Select Authentication Server as External RADIUS • Select RADIUS Compatibility from the drop-down list • Select MAC Delimiter from the drop-down list
Step 4	Add the Radius server and configure the following:	• Enter the Radius IP • Enter the Radius Port • Enter the Shared Secret • Click on tick icon

	Command or Action	Purpose
Step 5	Click Apply.	

Creating Guest WLANs

Mobility Express controller can provide guest user access on WLANs which are specifically designated for use by guest users. To set this WLAN exclusively for guest user access, enable the Guest Network under the WLAN Security tab.

Creating Guest WLAN with Captive Portal on CMX Connect

Procedure

	Command or Action	Purpose
Step 1	Navigate to Wireless Settings > WLANs and then click on Add new WLAN button. The Add new WLAN Window will pop up.	
Step 2	In the Add new WLAN window, on the General tab, configure the following:	• Enter the Profile Name • Enter the SSID
Step 3	Enable the Guest Network under the WLAN Security tab.	
Step 4	Select Captive Portal as CMX Connect.	
Step 5	Enter Captive Portal URL.	**Note** Captive Portal URL must have the following format: https://yya7lc.cmxcisco.com/visitor/login where yya7lc is your Account ID.
Step 6	Click Apply.	**Note** Additional steps are required on CMX Cloud to create the Captive Portal, Site with Access Points and associating Captive Portal to the Site.

Creating Guest WLAN with Internal Splash Page

There is an internal splash page built into the Mobility Express controller which can be used to onboard the clients connecting to Guest WLANs. This internal splash page can also be customized by uploading a customized bundle. To upload a customized internal splash page, navigate to Wireless Settings > Guest WLANs. Select Page Type as Customized and click on the Upload button to upload a customized page bundle.

For internal splash page, Cisco Mobility Express supports multiple options for Access Type. They are as follows:

1. Local User Account
2. Web Consent

3. Email Address
4. RADIUS
5. WPA2 Personal

Procedure

	Command or Action	Purpose
Step 1	Navigate to Wireless Settings > WLANs and then click on Add new WLAN button. The Add new WLAN Window will pop up.	
Step 2	In the Add new WLAN window, on the General tab, configure the following:	• Enter the Profile Name • Enter the SSID
Step 3	Enable the Guest Network under the WLAN Security tab.	
Step 4	Select Captive Portal as Internal Splash Page.	
Step 5	Select one of the following Access Type as needed:	• Local User Account–Splash Page will present the user to enter username and password which must be authenticated by the controller before network access is granted. Local WLAN users must be created on the controller to onboard the Guest clients. • Web Consent–Splash Page will present the user to acknowledge before network access is granted. • Email Address–Splash Page will present the user to enter the email address before network access is granted. • RADIUS–Splash Page will present the user to enter username and password which must be authenticated by the RADIUS server before network access is granted. Select Access Type as RADIUS and enter the RADIUS server configuration. • WPA2 Personal–This is an example of L2 + L3 (Web Consent). Layer 2 PSK security authentication will happen first followed by Splash Page which will present the user to acknowledge before network access is granted. Select Access Type as WPA2 Personal and enter the Passphrase.
Step 6	Click Apply.	

Creating Guest WLAN with External Splash Page

An external splash page is one which resides on an external Web Server. Similar to the internal splash page, Cisco Mobility Express supports multiple options for Access Type with external splash page. They are as follows:

- Local User Account
- Web Consent
- Email Address
- RADIUS
- WPA2 Personal

Procedure

	Command or Action	Purpose
Step 1	Navigate to Wireless Settings > WLANs and then click on Add new WLAN button. The Add new WLAN Window will pop up.	
Step 2	In the Add new WLAN window, on the General tab, configure the following:	• Enter the Profile Name • Enter the SSID
Step 3	Enable the Guest Network under the WLAN Security tab.	
Step 4	Select Captive Portal as External Splash Page.	
Step 5	Select one of the following Access Type as needed:	• Local User Account–Splash Page will present the user to enter username and password which must be authenticated by the controller before network access is granted. Local WLAN users must be created on the controller to onboard the Guest clients. • Web Consent–Splash Page will present the user to acknowledge before network access is granted. • Email Address–Splash Page will present the user to enter the email address before network access is granted. • RADIUS–Splash Page will present the user to enter username and password which must be authenticated by the RADIUS server before network access is granted. Select Access Type as RADIUS and enter the RADIUS server configuration.

	Command or Action	Purpose
		• WPA2 Personal–This is an example of L2 + L3 (Web Consent). Layer 2 PSK security authentication will happen first followed by Splash Page which will present the user to acknowledge before network access is granted. Select Access Type as WPA2 Personal and enter the Passphrase.
Step 6	Click Apply	

Internal Splash Page for Web Authentication

Cisco Mobility Express supports a default internal guest portal that comes built-in and also a customized page, which can be imported by the user.

Using Default Internal Guest Portal

To use the default Guest Portal Page or import a customized Guest Portal page, follow the procedure below:

Procedure

	Command or Action	Purpose
Step 1	Navigate to Wireless Settings > Guest WLANs.	
Step 2	Configure the following on the Guest WLAN page:	• Page Type–Select as Internal (Default). • Preview–You can Preview the page by clicking on the Preview button. • Display Cisco Logo–To hide the Cisco logo that appears in the top right corner of the default page, you can choose No. This field is set to Yes by default. • Redirect URL After Login–To have the guest users redirected to a particular URL (such as the URL for your company) after login, enter the desired URL in this text box. You can enter up to 254 characters. • Page Headline–To create your own headline on the login page, enter the desired text in this text box. You can enter up to 127 characters. The default headline is Welcome to the Cisco Wireless Network. • Page Message–To create your own message on the login page, enter the desired text in this text box. You can enter

	Command or Action	Purpose
		up to 2047 characters. The default message is Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.
Step 3	Click Apply.	

Using Customized Internal Guest Portal

If a customized guest portal has to be presented to guest users, a sample page can be downloaded from cisco.com which can then be edited and imported to the Cisco Mobility Express controller. After the page has been edited and ready to be uploaded to the Cisco Mobility Express controller, follow the steps below.

Procedure

	Command or Action	Purpose
Step 1	Navigate to Wireless Settings > Guest WLANs.	
Step 2	Configure the following on the Guest WLAN page:	• Page Type–Select as Customized. • Customized page Bundle–Click on the Upload button to upload the he customized page bundle to the Mobility Express controller. • Preview–You can Preview the Guest portal by clicking on the Preview button. • Redirect URL After Login–To have the guest users redirected to a particular URL (such as the URL for your company) after login, enter the desired URL in this text box. You can enter up to 254 characters.
Step 3	Click Apply.	

Managing WLAN Users

Cisco Mobility Express supports creation of local user accounts. These users can be authenticated for WLANs configured to use Security as WPA2 Enterprise with Authentication Server set to AP or Guest WLANs configured to use internal or external splash page with Access Type as Local User Account.

To create local user accounts, follow the procedure below:

Procedure

	Command or Action	Purpose
Step 1	Navigate to Wireless Settings > WLAN Users and then click on Add WLAN User button.	
Step 2	Navigate to Wireless Settings > WLAN Users and then click on Add WLAN User button.	• User Name–Enter the username • Guest User–For Guest user, enable the Guest User checkbox • Lifetime–For Guest User, define the user account validity. Default is 86400 seconds (or, 24 hours) from the time of its creation. • WLAN Profile–Select the WLAN to which the user will connect • Password–Enter the password for the user account • Description–Additional details or comments for the user account • Click on tickicon.

Adding MAC for Local MAC Filtering on WLANs

Cisco Mobility Express supports MAC Filtering on WLANs on controller as well as with external RADIUS. MAC addresses can be added to the controller and be either allowed or blocked. To add MAC addresses to the controller, follow the procedure below:

Procedure

	Command or Action	Purpose
Step 1	Navigate to Wireless Settings > WLAN Users and click on Local MAC Addresses.	
Step 2	Click Add MAC Address.	
Step 3	In the Add MAC Address window, configure the following:	• MAC Address–Enter the MAC Address of the device • Description–Enter the description • Type–Select whether this MAC has to be allowed or blocked • Profile Name–Select the WLAN to which the user will connect
Step 4	Click Apply.	

Managing Services with Cisco Mobility Express

Application Visibility and Control

Network Based Application Recognition (NBAR) provides application-aware control on a wireless network and enhances manageability and productivity. It also extends Cisco's Application Visibility and Control (AVC) as an end-to-end solution, which gives a complete visibility of applications in the network and allows the administrator to take some action on the same.

NBAR is a deep-packet inspection technology, which supports stateful L4 - L7 classification. The key use cases for NBAR are capacity planning, network usage base lining and better understanding of what applications are consuming bandwidth. Trending of application usage helps network admin improve quality of experience by protecting key applications from bandwidth-hungry applications when there is congestion on the network, capability to prioritize or de-prioritize, and drop certain application traffic. The AVC/NBAR2 engine interoperates with QoS settings on the specific WLAN.

Enabling Application Visibility on WLAN

To configure Application Visibility on a WLAN, follow the procedure below:

Procedure

To enable Application Visibility on WLAN, navigate to Wireless Settings > WLANs. On the Add new WLAN or Edit WLAN window, click on the Traffic Shaping tab. To enable Application Visibility on this WLAN, select Enabled for Application Visibility Control.

Enabling Application Control on WLAN

After Application Visibility has been enabled on the WLAN, one can add control for various applications. There are two way to add control for applications. One can either add control directly from the Applications widget on the Network Summary page or one can navigate to Monitoring > Applications and add control for applications as needed.

Adding Application Control from Network Summary Page

Procedure

	Command or Action	Purpose
Step 1	Add the Applications widget on the Network Summary Page. To add the Applications widget, click on the + icon on the right of the Network Summary banner. Select the Applications widget. The Applications widget will display the top 10 applications being browsed by the clients in the Mobility Express network.	
Step 2	Click on the application you wish to add control. The Add AVC Rule window will pop up. Select the Action. Action can be Mark, Drop or Rate Limit. For Mark, one can select DSCP	

	Command or Action	Purpose
	as Platinum, Gold, Silver, Bronze or Custom. If custom is selected, one has to specific he DSCP value. For Rate Limit, one can specify the Average Rate and Burst Rate for the application.	
Step 3	Select one or more AVC Profile/SSID combinations.	
Step 4	Click Apply.	

Adding Application Control from Applications Page

Procedure

	Command or Action	Purpose
Step 1	Navigate to Monitoring > Applications Page.	
Step 2	Click on the application you wish to add control. The Add AVC Rule window will pop up. Select the Action. Action can be Mark, Drop or Rate Limit. For Mark, one can select DSCP as Platinum, Gold, Silver, Bronze or Custom. If custom is selected, one has to specific he DSCP value. For Rate Limit, one can specify the Average Rate and Burst Rate for the application.	
Step 3	Select one or more AVC Profile/SSID combinations.	
Step 4	Click Apply.	

iOS Optimized WiFi Connectivity and Fast Lane

Configuring Optimized WiFi Connectivity

802.11r enabled WLAN provides faster roaming for wireless client devices. It is desired that iOS devices running iOS 10 will be able to join a WLAN with 11r enabled for better roaming experience. However, if 11r is enabled on a WLAN, the legacy devices that do not recognize the FT AKM's beacons and probe responses will not be able to join the WLAN. We need a way to identify the Client device capability and allow 11r capable device to join on the WLAN as an FT enabled device and at the same time to allow legacy device to join as an 11i/WPA2 device.

Cisco Mobility Express Release 8.4 will enable 802.11r on an 802.11i-enabled WLAN selectively for iOS devices. The capable iOS devices will identify this functionality and perform an FT Association on the WLAN. The Cisco Wireless infrastructure will allow FT association on the WLAN from devices that can negotiate FT association on a non-FT WLAN. In addition, with Mobility Express running AireOS 8.4, 802.11k and 11v features are enabled by default on an SSID. These features help clients roam better by telling them when to roam and providing them with information about neighboring APs so that no time is wasted scanning when

roaming is needed. Since iOS devices support dual band, the 802.11k neighbor list is updated on dual-band, adaptively for iOS devices.

To configure 11k, r, v on a WLAN, follow the procedure below:

Procedure

	Command or Action	Purpose
Step 1	Enable Expert View on Cisco Mobility Express. Expert View is available on the top banner of the Cisco Mobility Express WebUI as shown below and enabled various configurable parameters which are not available in Standard view.	
Step 2	Navigate to Wireless Settings > WLANs. On the Add new WLAN or Edit WLAN window, click on the Advanced tab. Configure 802.11k, r, v as needed on this page.	
Step 3	Click Apply.	

Configuring Fast Lane

Apple iOS device mark QoS as per IETF recommendations. With Mobility Express running AireOS 8.4, one can enable the Fastlane feature from CLI, which enables several beneficial functions:

Your WLC QoS configuration is optimized globally to better support real-time applications

iOS 10 devices can send upstream voice traffic without the requirement to perform WMM TSPEC/TCLAS negotiation. The infrastructure will honor the voice marking for these devices.

You can apply a QoS profile to your iOS 10 devices, and decide which applications should receive QoS marking upstream, and which applications should be sent as best effort or background.

To configure Fast Lane on a WLAN from CLI, follow the procedure below:

Procedure

	Command or Action	Purpose
Step 1	Login to the controller CLI.	

Step 2	Enable Fast Lane using the CLI below:	`(Cisco Controller) >config qos fastlane enable 1`
		
		`Warning: This command will temporarily disable all WLANs and Networks. Active WLANs and networks will be re-enabled automatically after the configuration completes. This command will also override the file named AUTOQOS-AVC-PROFILE, if it exists, and will apply it to the WLAN, if Application Visibility is enabled. Are you sure that you want to continue? (y/N)y`

Cisco Mobility Express with CMX Cloud

Cisco CMX Cloud

Cisco Connected Mobile Experiences Cloud (Cisco CMX Cloud) is an simple and scalable offering which enables delivery of wireless guest access and in-venue analytics, integrating seamlessly with Cisco wireless infrastructure.

This cloud-delivered Software-as-a-Service (SaaS) offering is quick to deploy and intuitive to use. It is based on CMX 10.x code and is compatible with Cisco Mobility Express Release 8.3. It offers the following services:

- Connect for Guest Access-Providing an easy-to-use guest-access solution for visitors through a custom portal using various authentication methods including social, self-registration, and Short Message Service (SMS).
- Presence Analytics-Detecting all Wi-Fi devices (the "devices") in the venue and providing analytics on their presence, including dwell times, new vs. repeat visitors, and peak time.

Cisco CMX Cloud Solution Compatibility Matrix

- Cisco Mobility Express running AireOS Release 8.3 and later.
- All Cisco Mobility Express supported Access Points.

Minimum Requirements for Cisco CMX Cloud Deployment

Below are the minimum requirements for CMX Cloud deployment:

1. Verify Cisco CMX Cloud Solution Compatibility Matrix above.
2. Recommended browser is Chrome 45 or later.
3. Signup at https://cmxcisco.com for 60 day trial or go to Cisco Commerce Workspace (CCW) and purchase license for your choice of CMX Cloud service.

Enabling CMX Cloud Service on Mobility Express for Presence Analytics

After CMX Cloud Account has been created, next step is to configure and enable the CMX Cloud Service on primary Access Point so that it can send data to the CMX Cloud. To configure, follow the procedure below:

Procedure

	Command or Action	Purpose
Step 1	On Cisco Mobility Express WebUI, navigate to Advanced > CMX.	
Step 2	Enter the CMX Server URL (Site URL).	
Step 3	Enter the CMX Server Token (Account Token).	

	Command or Action	Purpose
Step 4	Click Apply.	**Note** Click the Test Link button to verify connectivity from primary AP to CMX Cloud Site using the configured information.

Configuring Site on CMX Cloud for Presence Analytics

To create a site and add Access Points to the site in CMX Cloud for Presence Analytics, follow the procedure below:

Procedure

	Command or Action	Purpose
Step 1	Login to CMX Cloud account at https://cmscisco.com/	
Step 2	Navigate to Manage > Cloud Enabled WLC and verify that the IP address of the WLC shows up on the list.	
Step 3	Navigate to PRESENCE ANALYTICS > Manage. You should be in the Sites pane. Click on the Add Site button to create a site.	
Step 4	In the NEW SITE window, configure the following details:	• Enter the Name for the site • Enter the Address for the site • Select Timezone from the drop-down list • Select the Signal Strength Threshold for Ignore, Passerby, and Visitors • Enter the Minimum Dwell Time for Visitor (minutes)
Step 5	Click Save to create the Site.	
Step 6	After the Site is created, click on Access Points under PRESENCE ANALYTICS > Manage.	
Step 7	Select the Access Points and add them to the Site by clicking on Add to Site button and selecting the Site from the drop-down list.	
Step 8	Finally, navigate to Presence Analytics dashboard. Select the Site you created. Within a few minutes, you should begin to see Presence data get populated.	

Managing the Cisco Mobility Express Deployment

Managing Access Points

Starting Release 8.4, Cisco Mobility Express supports up to 50 Access Points. To view the list or modify parameters on an Access Points, follow the procedure below:

Procedure

	Command or Action	Purpose
Step 1	Navigate to **Wireless Settings > Access Points**.	**Note** The first Access Point with the P icon is the primary AP and the rest of them are Subordinate Access Points.
Step 2	To modify the parameters on an access point, click on the Edit button. The Access Point window will come up displaying the General parameters about the Access Point.	• Operating Mode(Read only field)-For a primary AP, this field displays AP & Controller. For other associated APs, this field displays AP only. • AP Mac(Read only field)–Displays the MAC address of the Access Point. • AP Model(Read only field)-Displays the model details of the Access Point. • IP Configuration–Choose Obtain from DHCP to allow the IP address of the AP be assigned by a DHCP server on the network, or choose Static IP address. If you choose Static IP address, then you can edit the IP Address, Subnet Mask, and Gateway fields. • AP Name–Edit the name of access point. This is a free text field. • Location–Edit the location for the access point. This is a free text field.
Step 3	Under the Controller tab (Available only for primary AP), one can modify the following parameters:	• System Name–Enter the System Name for Mobility Express • IP Address–IP address decides the login URL to the controller's web interface. The URL is in https://<ip address> format. If you change this IP address, the login URL also changes. • Subnet Mask–Enter the Subnet Mask.

	Command or Action	Purpose
		• Country Code–Enter the Country Code.
Step 4	Under Radio 1 (2.4 GHz) and Radio 2 (5 GHz), one can edit the following parameters:	• Admin Mode–Enabled/Disabled. This enables or disables the corresponding radio on the AP (2.4 GHz for 802.11 b/g/n or 5 Ghz for 802.11 a/n/ac). • Channel–Default is Automatic. Automatic enables Dynamic Channel Assignment. This means that channels are dynamically assigned to each AP, under the control of the Mobility Express controller. This prevents neighboring APs from broadcasting over the same channel and hence prevents interference and other communication problems. For the 2.4GHz radio, 11 channels are offered in the US, up to 14 in other parts of the world, but only 1-6-11 can be considered non-overlapping if they are used by neighboring APs. For the 5GHz radio, up to 23 non-overlapping channels are offered. Assigning a specific value statically assigns a channel to that AP. • 802.11 b/g/n–1 to 11. • 802.11 a/n/ac –40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 165. • Channel Width - 20 MHz for 2.4GHz and for 20, 40 and 80 for 5 GHz. • Transmit Power - 1 to 8. The default value is Automatic. This is a logarithmic scale of the transmit power, that is the transmission energy used by the AP, 1 being the highest,2 being half of it, 3 being 1/4th and so on. Selecting Automatic adjusts the radio transmitter output power based on the varying signal level at the receiver. This allows the transmitter to operate at less than maximum power for most of the time; when fading conditions occur, transmit power will be increased as needed until the maximum is reached.
Step 5	Click Apply.	

Primary AP Failover and Electing a New Primary

Cisco Mobility Express is supported on Cisco 1100 series Access Points. If you have a mix of these Access Points in a Cisco Mobility Express deployment, the primary AP election process determines which of the supported Access Point will be elected to run Mobility Express controller function in case of a Failover of the Active primary AP. VRRP is used to detect the failure of primary AP which initiates the election of a new primary.

Note Mobility Express uses MAC 00-00-5E-00-01-VRID where VRID is 1 so if there are other instances of VRRP running in the environment, use VRID other than 1 for those instances.

Primary AP Failover

To have redundancy in the Mobility Express network, it must have two or more Mobility Express capable Access Points. These Access Points should have AP Image type as MOBILITY EXPRESS IMAGE and AP Configuration as MOBILITY EXPRESS CAPABLE. In an event of a failure of primary AP, another Mobility Express capable AP is elected as a primary automatically. The newly elected primary AP has the same IP and configuration as the original primary AP.

Note Given Access Point models support different scale limits in terms of the number of Access Points supported, it is highly recommended to have at least two or more Access Points which support the same scale limits.

Note Access Points, which have the Mobility Express Image but AP Configuration, is NOT MOBILITY EXPRESS CAPABLE, will not participate in the primary AP election process.

Electing a new Primary Access Point

As mentioned above, primary Access Point election is based on a set of priorities. The priorities are as follows:

Before you begin

Primary election process is based on a set of priorities. When an active primary Access Point fails, the election process gets initiated and it elects the Access Point with the highest priority as the primary AP.

Note During the primary Election process, even though the primary AP running the controller function is down, the remaining Access Points will fall into Standalone mode and will continue to service connected clients and switch data traffic locally. After the new primary is elected, the Standalone Access points will move to connected mode.

Procedure

Step 1 User Defined Primary–User can select an Access Point to be the primary Access Point. If such a selection is made, no new primary will be elected in case of a failure of the active primary. After five minutes, if the current primary is still not active, it will be assumed dead and primary Election will begin to elect a new primary. To manually define a primary, follow the procedure below:

a) Navigate to Wireless Settings > Access Points.
b) From the list of Access Points, click Edit icon of the Access Point which you would like to select as the primary AP.
c) Under the General tab, click on Make me Controller button.
d) Click Yes on the Confirmation window.

Note The previous primary will reboot and the selected Access Point will immediately launch the controller and become the active primary.

Step 2 Next Preferred Primary - Admin can configure the Next Preferred Primary from CLI. When this is configured and the active primary AP fails, the one configured as the Next Preferred Primary will be elected as a primary. To configure the Next Preferred Primary, follow the procedure below:

a) Login to the CLI of the controller.
b) Execute the following CLI:

To configure the Next Preferred Primary, execute the following CLI:

```
(Cisco Controller) >config ap next-preferred-master <Cisco AP>
<Cisco AP> Enter the name of the Cisco AP
```

To see the Next Preferred Primary, execute the following CLI:

```
(Cisco Controller) >show ap next-preferred-master
```

To clear the Next Preferred Primary, execute the following CLI:

```
Cisco Controller) >clear ap next-preferred-master
```

Step 3 Most Capable Access Point– If the first two priorities are not configured, primary AP election algorithm will select the new primary based on the capability of the Access Point.

Step 4 Least Client Load– If here are multiple Access Points with the same capability, the one with least client load is elected as the primary Access Point.

Step 5 Lowest MAC Address–If all of the Access Points are the same and have the same client load, then Access Point with the lowest MAC will be elected as a primary.