Cisco Mobility Express Deployment Guide–Release 8.3.102.0

First Published: 2016-08-01

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

Audience

This publication is for experienced network administrators who configure and maintain Cisco Mobility Express wireless network.

Document Organization

This document is organized into the following chapters:

Table 1: Document Organization

Chapter	Description
Product Overview	Provides details of supported Cisco Aironet access points, list of features, licenses, software release numbers, and supported software images.
Getting Started	Describes about Mobility Express ports, interfaces, WLANs, LED states and access switch configuration.
Deploying Cisco Mobility Express Solution	It describes the pre-requisites for deploying Mobility Express Solution, connecting Cisco Mobility Express Capable AP, determining the image on the Access Point, converting a CAWAP AP into a Mobility Express AP,converting a Mobility Express AP into a CAPWAP AP, configuring Mobility Express Controller using Over-the-Air Setup Wizard and Configuring Mobility Express Controller using Startup Wizard from CLI.

Chapter	Description
Creating DHCP Scopes for Wireless Networks	It briefs about creating DHCP scopes for Wireless networks
Creating Wireless Networks	It describes about the WLANs, creating networks and guest access.
Managing WLAN Users	It provides details of managing WLAN users.
Managing Access Points	It briefs about managing Access Points and adding an Access Point to Mobility Express Network.
Managing the Mobility Express Network	Briefs about adding an access point to the Mobility Express network.
Using Advanced Settings	It describes about SNMP, logging, RF Optimization, controller tools and the ways to collect export of logs, core and crash files.
Primary AP Failover and Electing a New Primary	It describes the Primary AP Failover and Primary Election.
Cisco Mobility Express with Cisco CMX Cloud	It describes Cisco CMX cloud, Cisco CMX cloud solution compatibility matrix,minimum requirements for CMX Cloud deploymen, CMX cloud trial sign-Up and sign-in and configuring Cisco Mobility Express to send data to CMX Cloud for presence analytics
Managing Mobility Express Deployments from Cisco Prime Infrastructure	It briefs about adding Mobility Express to Prime.

Command Syntax Conventions

This document uses the following conventions:

Table 2: Command Syntax Conventions

Convention	Description
bold font	Bold text indicates commands and keywords that you enter as shown
italic font	Italic text indicates arguments for which you supply value.
[x]	Square brackets enclose an optional keyword or argument.
…	An ellipsis (three consecutive non-bolded periods without spaces) after a syntax element indicates that the element can be repeated.

Convention	Description
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments
[x|y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice
{ x|y }	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y | z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

Reader Alert Conventions

This document uses the following conventions for reader alerts:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information will help you solve a problem.*

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning Means *reader beware*. In this situation, you might perform an action that could result in bodily injury.

Related Documentation

- **User Guide**

  http://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/83/user_guide/b_ME_User_Guide_83.html

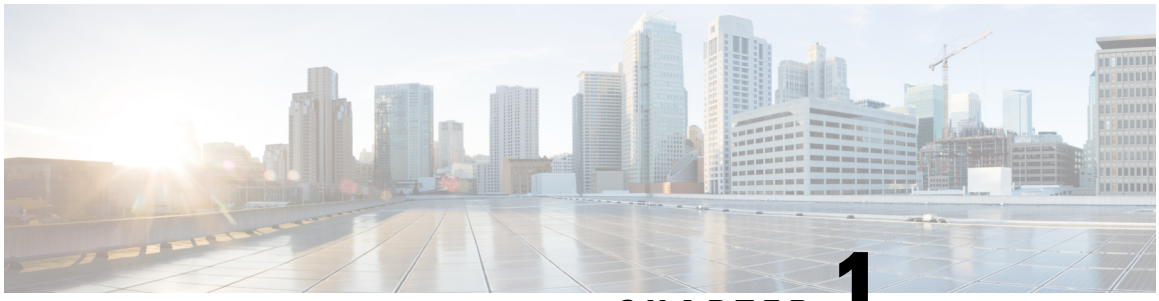
- **Release Note**

  http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/crn83.html#pgfId-1515571

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation, at: http://%20www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.



CHAPTER 1

Product Overview

With more devices attaching to the network and more bandwidth-intensive applications in use, mobile usage continues to rise. How do small and medium-sized businesses with little or no IT staff keep pace with unexpected growth?

The Cisco Mobility Express Solution is specifically designed to help small and medium-sized businesses easily and cost-effectively deliver enterprise-class wireless access to both employees and customers. It is a virtual Wireless LAN controller function embedded on Cisco 1830, 1850, 2800 and 3800 series 802.11ac Wave 2 Access Points. With the Cisco Mobility Express Solution, small and mid-sized networks can now enjoy the same quality user experiences as large enterprises.

Cisco Mobility Express Solution is an on-premise, managed Wi-Fi solution that:

- Provides an easy, over-the-air deployment in under 10 minutes
- Is ideal for small and medium-sized deployments of up to 25 access points
- Removes the need for a physical controller while supporting Cisco's advanced features
- Is supported on Cisco Aironet® 3800, 2800, 1850 and 1830 Series Access Points
- Can control other Aironet® access points, such as the 1700, 2700, and 3700 Series
- Is the Next Generation Autonomous. 802.11ac Wave 2 Access Point do not support the legacy autonomous mode.
- Industry-leading Cisco technology allows small and medium-sized networks to reduce the number of devices needed to enjoy enterprise-grade Wi-Fi. Advanced features such as Guest, BYOD and Cisco High Density Experience (HDX) are activated by default for compatible access points, making the deployment process even easier. CMX can be added to gain presence-based services and deep analytics.

- Supported Cisco Aironet® Access Points, on page 1
- Cisco Mobility Express Supported Features, on page 3
- Supported Software Release and Interoperability, on page 3

Supported Cisco Aironet® Access Points

Mobility Express solution consists of the following components:

- Primary Access Point–Cisco Aironet® Access Point 1800, 2800, 3800 series running the virtual Wireless LAN Controller function

- Subordinate Access Points–Cisco Aironet® Access Points which are managed by Primary Access Point similar to how a Wireless LAN Controller manages Access Points

Note Primary Access Point functions as Wireless LAN Controller, manages Subordinate Access Points and also serves clients at the same time.

Cisco Aironet® Access Points which support the Wireless LAN Controller function and operate as Primary Access points are listed in the table below:

Table 3: Cisco Aironet® Access Points capable of operating as Primary Access Points

Primary Access Points	Supported Model Numbers
Cisco Aironet® 1830 Series	AIR-AP1832I-x-K9C
Cisco Aironet® 1850 Series	AIR-AP1852I-x-K9C AIR-AP1852E-x-K9C
Cisco Aironet® 2800 Series	AIR-AP2802I-x-K9C AIR-AP2802E-x-K9C
Cisco Aironet® 3800 Series	AIR-AP3802I-x-K9C AIR-AP3802E-x-K9C

Cisco Aironet® Access Points which operate as Subordinate Access Points are listed in the table below.

Subordinate Access Points	Supported Model Numbers
Cisco Aironet® 700i Series	AIR-CAP702I-x-K9
Cisco Aironet® 700w Series	AIR-CAP702W-x-K9
Cisco Aironet® 1600 Series	AIR-CAP1602I-x-K9 AIR-CAP1602E-x-K9
Cisco Aironet® 1700 Series	AIR-CAP1702I-x-K9
Cisco Aironet® 1810 Series	AIR-AP1810W-x-K9
Cisco Aironet® 1830 Series	AIR-AP1832I-x-K9C
Cisco Aironet® 1850 Series	AIR-AP1852I-x-K9C AIR-AP1852E-x-K9C
Cisco Aironet® 2600 Series	AIR-CAP2602I-x-K9 AIR-CAP2602E-x-K9
Cisco Aironet® 2700 Series	AIR-CAP2702I-x-K9 AIR-CAP2702E-x-K9

Subordinate Access Points	Supported Model Numbers
Cisco Aironet® 2800 Series	AIR-AP2802I-x-K9C AIR-AP2802E-x-K9C
Cisco Aironet® 3600 Series	AIR-CAP3602I-x-K9 AIR-CAP3602E-x-K9
Cisco Aironet® 3700 Series	AIR-CAP3702I-x-K9 AIR-CAP3702E-x-K9
Cisco Aironet® 3800 Series	AIR-AP3802I-x-K9C AIR-AP3802E-x-K9C

Cisco Mobility Express Supported Features

See Supported features section in Release notes, http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/crn83.html#pgfId-1334529

Supported Software Release and Interoperability

AireOS® Release

- Cisco Mobility Express solution is supported from AireOS® Release 8.1.121.0 and later.

Cisco Prime Infrastructure

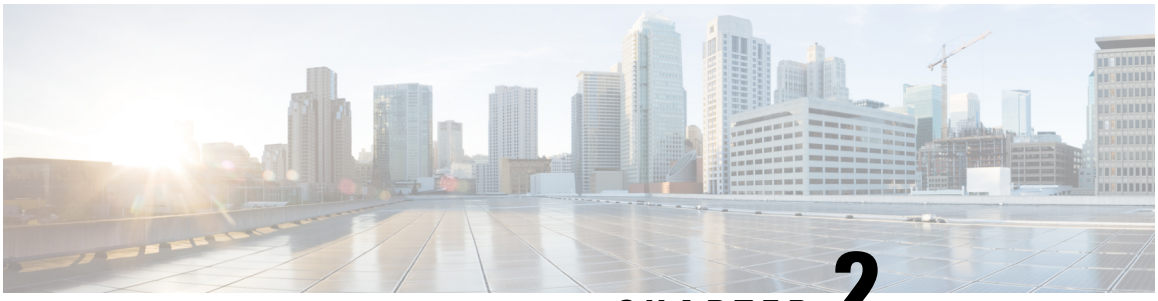
- PI Release 3.0.1 and later.

Connected Mobility Experiences (CMX)

- CMX Connect is supported starting AireOS® Release 8.3.100.0 for both On-Prem and CMX cloud deployments.
- CMX Presence Analytics is supported starting AireOS® Release 8.1.121.0 for On-Prem and CMX Release 10.2 and later. CMX Presence analytics in the cloud is supported starting AireOS® Release 8.3.102.0.

Cisco Identity Services Engine (ISE)

- ISE Release 1.4 and later. 802.1x authentication is supported.



CHAPTER 2

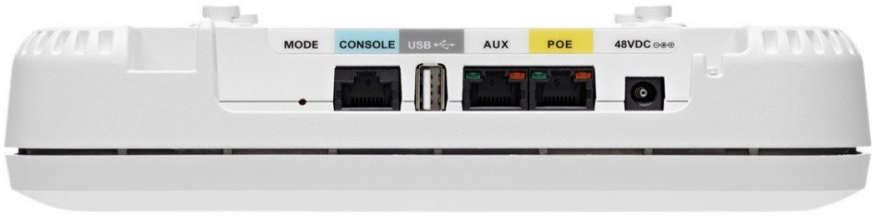
Getting Started

This chapter provides information about the Mobility Express ports, interfaces, WLANs, LED states and access switch configuration.

Ports

A port is a physical entity that is used to connect Cisco 1800 series access points to the network. The ports available on Cisco 1800 Access Points are as shown.

Figure 1: Ports of Cisco 1800 series Access Points



Mode

The Mode button is used to reset the Access Point to factory defaults. T o reset, depress the button and connect power to the AP. Hold the button depressed for 20s and then release it. When the button is released, the following message will be seen in the console. The AP will reboot and will be reset to factory defaults. If the AP has the Mobility Express controller image, after the reboot, it will broadcast the CiscoAirProvision SSID.

```
Button is pressed. Configuration reset activated..
Keep the button pressed for > 20 seconds for full reset

Wait for the button to be released ....
Button pressed for  22 seconds
```

Console Port (RJ-45)

The Cisco 1800 series has one console port. It provides console access to the Mobility Express controller CLI.

USB

This port is not currently supported.

Aux Port (RJ-45)

This port is not currently supported.

POE (Management Port) (RJ-45)

The Cisco 1800 series Access Points has a port marked as POE. This port is used to provide Management access to the Mobility Express Controller.

Interfaces

An interface is a logical entity on Mobility Express. The management interface must be configured and is used for in-band management: Web GUI, Telnet/SSH CLI, SNMP.

WLANs

A WLAN associates Service Set Identifier (SSID) to VLANs. It is configured with Security type, Quality of Service (QoS), radio policies, and other wireless network parameters. On Mobility Express network, up to 16 WLANs can be configured. The WLANs can be mapped to VLANs trunked on the switch port.

Switch Configuration

All Access Points including the Primary AP in a Mobility Express network should be in the same L2 broadcast domain. Management traffic must not be tagged.

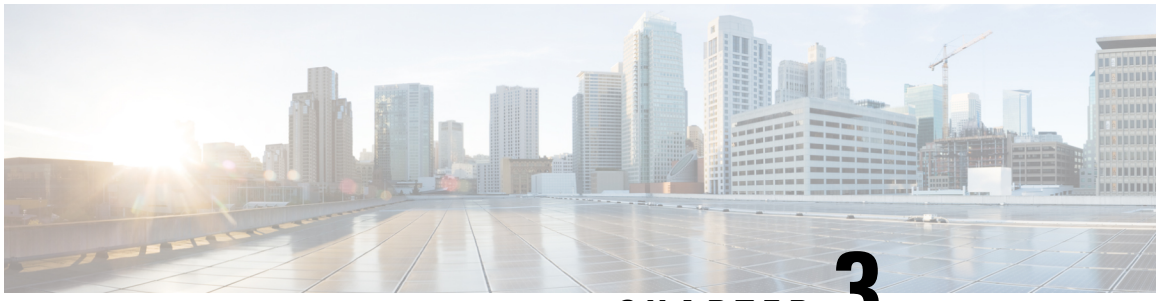
The switch to which the Access Points connects have configuration similar to the one shown below:

```
vlan 10
 name Employee
vlan 20
 name Guest
vlan 122
name Management

interface Vlan10
 description >> Employee Network <<
 ip address 10.10.10.1 255.255.255.0
!
interface Vlan20
 description >> Guest Network <<
 ip address 20.20.20.1 255.255.255.0
!
interface Vlan122
 description >> Management, Master AP and Subordinate APs<<
 ip address 172.20.229.2 255.255.255.0

interface GigabitEthernet1/0/37
 description >> Connected to Cisco 1850 Access Point <<
```

```
switchport trunk native vlan 122
switchport trunk allowed vlan 10,20,122
```



CHAPTER 3

Deploying Cisco Mobility Express Solution

Pre-requisites for Deploying Mobility Express Solution

1. You must not have 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. The Mobility Express controller cannot interoperate or co-exist with other Wireless LAN Controllers in the same 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. DHCP Server: A DHCP server must be configured so that Access Points and clients can obtain an IP Address and gateway assigned is reachable at all times.

Connecting Cisco Mobility Express Capable Access Point

To connect Cisco Mobility Express capable access point, perform the following steps:

Procedure

Step 1 Connect Cisco Mobility Express capable access point to a switch port and power it up.

Note All Access Points in a Mobility Express deployment should be in the same Layer 2 domain

Step 2 The switch port to which Access Point is connected can be a trunk port or an access port. If multiple VLANs are being utilized for client traffic, the switch port should be configured as a trunk interface. Also, note that

management traffic is untagged and if a VLAN is being used for management, it should be configured as a native VLAN on the switch port.

Example of the switch port configuration. In this example, vlan 40 is being used for Management.

```
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
```

Step 3 Observe the access point LED.

a) When you power up the access point—The access point starts a power-up sequence that you can verify by observing the access point LED. If the power-up sequence is successful, the discovery and join process starts. During this process, the LED blinks sequentially green, red, and OFF.
b) When the access point joins the Mobility Express controller—The LED chirps green if no clients are associated or turn green if one or more clients are associated.
c) If the LED is not ON—The access point does not receive power.
d) If the LED blinks sequentially for more than 10 minutes—This could be because the access point does not have the Mobility Express capable image.

Determining the image on the Access Point

The Cisco 1830, 1850, 2800 and 3800 series 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 steps below:

Procedure

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 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.

Note Access Point with CAPWAP image will not show the AP Image Type and AP Configuration parameters in the **AP#show version** output.

```
cisco AIR-AP1852E-UXK9 ARMv7 Processor rev 0 (v71) with 997184/525160K bytes of memory.
Processor board ID RFDP2BCR021
AP Running Image : 8.2.100.0
Primary Boot Image : 8.2.100.0
Backup Boot Image : 8.1.106.33
AP Image type : MOBILITY EXPRESS IMAGE
AP Configuration : MOBILITY EXPRESS CAPABLE
0 Gigabit Ethernet interfaces
0 802.11 Radios
```

```
Radio FW version . 1401b63d12113073a3C08aa67f0c039c0
NSS FW version : NSS.AK.1.0.c4-0Z026-E_cust C-1.24160
```

Step 3 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 only as a CAPWAP Access Point. Such an 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 AI R-AP1852E-UXK9 ARMv7 Processor rev 0 (v7I) with 997184/726252K bytes of memory.
Processor board ID RFDP2BCR021
AP Running Image : 8.2.101.0
Primary Boot Image : 8.2.100.0
Backup Boot Image : 8.1.106.33
AP Image type : MOBILITY EXPRESS IMAGE
AP Configuration : NOT MOBILITY EXPRESS CAPABLE
```

For this AP to run the controller function, execute the following command from the AP CLI.

```
AP#ap-type mobility-express tftp://
```

Conversion

Note On 1830 and 1850 Series Access points, conversion from CAPWAP to Mobility Express is supported from Release 8.1.122.0 and later but it is recommended to have CAPWAP version 8.2.100.0 on the Access Point prior to converting from CAPWAP to Mobility Express. If the CAPWAP image on the Access Point is prior to 8.2.121.0, Access Point MUST first join a WLC running 8.2.100.0 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.

Note On 2800 and 3800 series Access Points, Mobility Express is supported starting Release 8.3.102.0 so they must have 8.3.102.0 CAPWAP image before they can be converted to Mobility Express. If the CAPWAP image on the Access Point is prior to 8.3.102.0, Access Point MUST first join a WLC running 8.3.102.0 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.

The following conversions are supported:

1. Converting a CAWAP AP to Mobility Express–This conversion is required when you have an access point running CAPWAP image, and you want to use them to deploy a Mobility Express network. For this, you would convert the CAPWAP AP to a Primary AP (runs controller function in a Mobility Express network).
2. Converting a Mobility Express capable AP to CAPWAP AP - There are two reasons for this conversion:
   a. If you want to migrate the access points from a Mobility Express network to another controller (not Mobility Express) network.

b. If you do not want access points to participate in the Primary AP election process in a Mobility Express network.

Procedure

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 table lists the Cisco Mobility Express software for Cisco Wireless Release 8.3.102.0.

Access Points Supported As Primary	Software to be Used only for Conversion from Unified Wireless Network Lightweight AP Software To Cisco Mobility Express Software	AP Software Image Bundle, to be Used for Software Update, or Supported Access Point Images, or Both
1830	AIR-AP1830-K9-8-3-102-0.tar	AIR-AP1830-K9-ME-8-3-102-0.zip
1850	AIR-AP1850-K9-8-3-102-0.tar	AIR-AP1850-K9-ME-8-3-102-0.zip
2800	AIR-AP2800-K9-8-3-102-0.tar	AIR-AP2800-K9-ME-8-3-102-0.zip
3800	AIR-AP3800-K9-8-3-102-0.tar	AIR-AP3800-K9-ME-8-3-102-0.zip

Step 2 Login to the Access Point CLI using a console and type **AP#show version** and check the full output of showversion. The default login credentials are Username:cisco and Password:cisco

Converting a CAWAP AP into a Mobility Express AP

To convert an access point running CAPWAP image into a Mobility Express capable image, you have to download and install the Mobility Express image from a TFTP server. A single CLI command has been provided to download the Mobility Express image from a TFTP server and convert the **AP Configuration** to **MOBILITY EXPRESS CAPABLE**.

Pre-requisites for converting CAPWAP AP to Mobility Express:

1. A TFTP server with Mobility Express image. See Procedure below.
2. A DHCP server to assign an IP address to the Cisco access point.
3. The Cisco 1800 series access point must not join any existing controller in the network when you are trying to load Mobility Express image. If you have an existing controller on your network to which the AP can join, conversion is not successful.

To convert an AP running CAPWAP image to Mobility Express, perform the following steps:

Procedure

Step 1 Enter **enable** to go to privileged execution mode.

Step 2 Enter **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 process.

- Case 1: If the **AP Image type** is **MOBILITY EXPRESS IMAGE** and **AP configuration** is **NOT MOBILITY EXPRESS CAPABLE**, only conversion of AP Configuration is required. Go to 5.
- Case 2: In the `show version` output, if the **AP Image type** and **AP Configuration** are not available, download of the Mobility Express image and conversion of **AP Configuration** is required. Go to 6.

Step 3 Enter the command below to change the **AP Configuration** to **MOBILITY EXPRESS CAPABLE**.

```
AP#ap-type mobility-express tftp://<TFTP Server IP>/<path to tar file>
```

Since the Access Point has an **AP Image type: MOBILITY EXPRESS IMAGE**; a new image does not be downloaded. After the command is issued, the Access Point reboots and comes up as **AP Configuration MOBILITY EXPRESS CAPABLE** .

Step 4 If **AP Image Type** and **AP Configuration** is not available in show version, it means that the AP is running **CAPWAP image**. To do the conversion, execute the command below:

```
AP#ap-type mobility-express tftp://<TFTP Server IP>/<path to tar file>
```

Example:

```
AP#ap-type mobility-express tftp://10.18.22.34/AIR-AP1850-K9-8.1.120.0.tar

Starting the ME image download...
It may take few minutes to finish the download.
```

Note After the image download is complete, it writes to flash followed by a reboot.

```
Image downloaded, writing to flash...
do PREDOWNLOAD, part1 is active part
sh: CHECK_ME: unknown operand
Image start    0x40355008 size 0x01dae41a file size 0x01dae7ca
Key start      0x42103422 size 0x00000230
Sinature start 0x42103652 size 0x00000180
Verify returns 0
btldr rel is 16 vs 16, does not need update
part to upgrade is part2


activate part2, set BOOT to part2
AP primary version: 8.1.105.37
Archive done.
Oe as AP needs to boot up with ME image

The system is going down Now!
sent SIGTERM to all processes
sent SIGKILL to all processes
Requesting system reboot79]
[07/24/2015 18:19:43.0887] Restarting system.
[07/24/2015 18:19:43.1257] Going down for restart now
```

Step 5 After AP reboots, Mobility Express starts in Day 0 and ***CiscoAirProvison*** SSID is broadcast.

Converting a Mobility Express AP into a CAPWAP AP

When the AP type is CAPWAP, AP cannot run the controller function and cannot participate in the Primary AP election process.

After changing the AP Type, if this AP is migrated to another WLC network (non-Mobility Express network), it joins the controller in that network. If the image on the WLC is different than the one on the AP, a new CAPWAP image is requested from the WLC.

When the AP type is CAPWAP (as required for this conversion), the AP doesn't start its own controller function and when the AP joins the external controller, a new image is requested from the controller and the AP gets the CAPWAP image.

To convert the Mobility Express AP into the CAPWAP AP, perform the following steps:

Procedure

Step 1 Login to the Access Point CLI .

Step 2 Type **Enable** to go to privileged execution mode.

Step 3 Enter **ap#ap-type capwap** and confirm to switch to the CAPWAP type.

To convert multiple 1800 series access points running Mobility Express image to CAPWAP simultaneously from the Mobility Express controller CLI, execute the following command:

```
(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.
```

The above command converts all Cisco 1800 APs connected to the Mobility Express 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 in local mode.

Configuring Mobility Express Controller using Over-the-Air Setup Wizard

To configure the Mobility Express using Over-the-Air Setup wizard, perform the following steps:

Procedure

Step 1 When a LED chirps green, connect a WiFi enabled laptop, through Wi-Fi, to the *CiscoAirProvision* SSID. The default password is *password*.

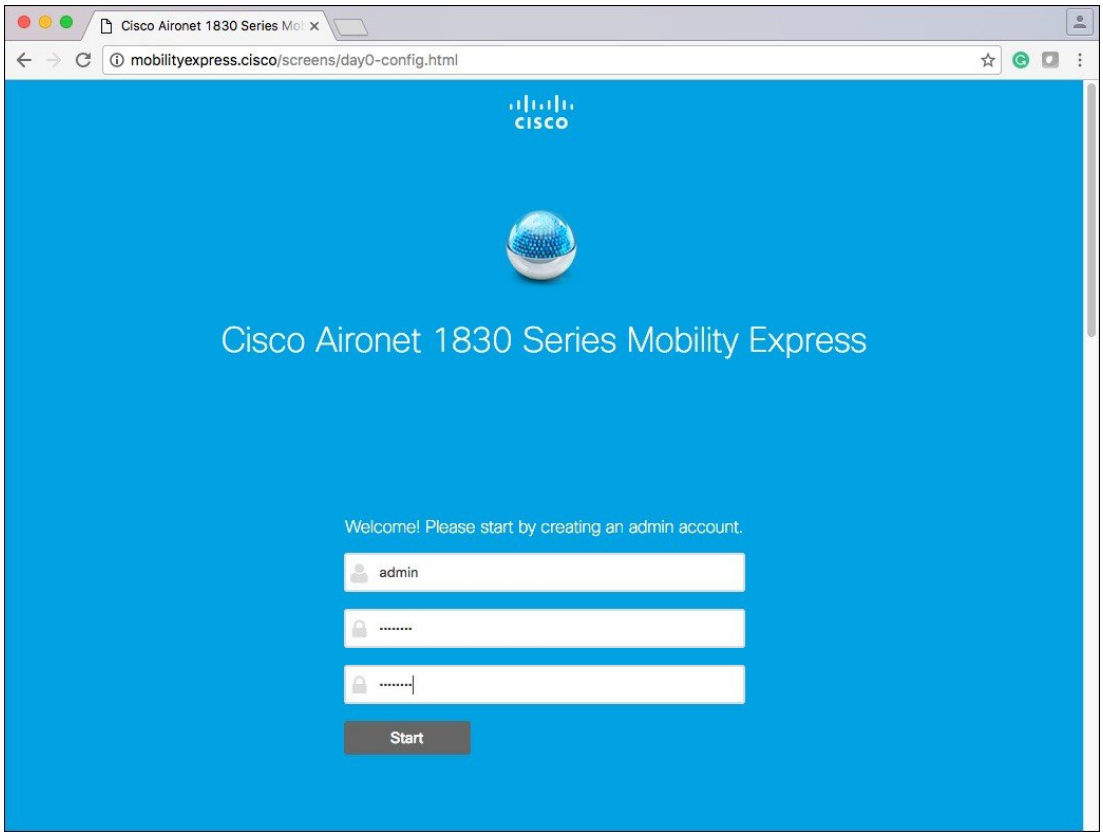
The laptop gets an IP address from subnet 192.168.1.0/24.

Note *CiscoAirProvision* SSID is broadcast at 2.4GHz.

Step 2 Open a browser and go to *http://192.168.1.1* which redirects to the initial configuration wizard.

The initial configuration wizard's admin account page appears.

Figure 2: Initial Configuration Wizard's Admin Account Page



The banner on the opening page shows the name of the AP model on which the Mobility Express wireless LAN controller is being configured. For example, '*Cisco Aironet 1850 Series Mobility Express*'.

Note Take the checklist that you have filled before and proceed with the following steps.

Step 3 Create an admin account on the controller by specifying the following parameters and then click **Start**.

- 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:

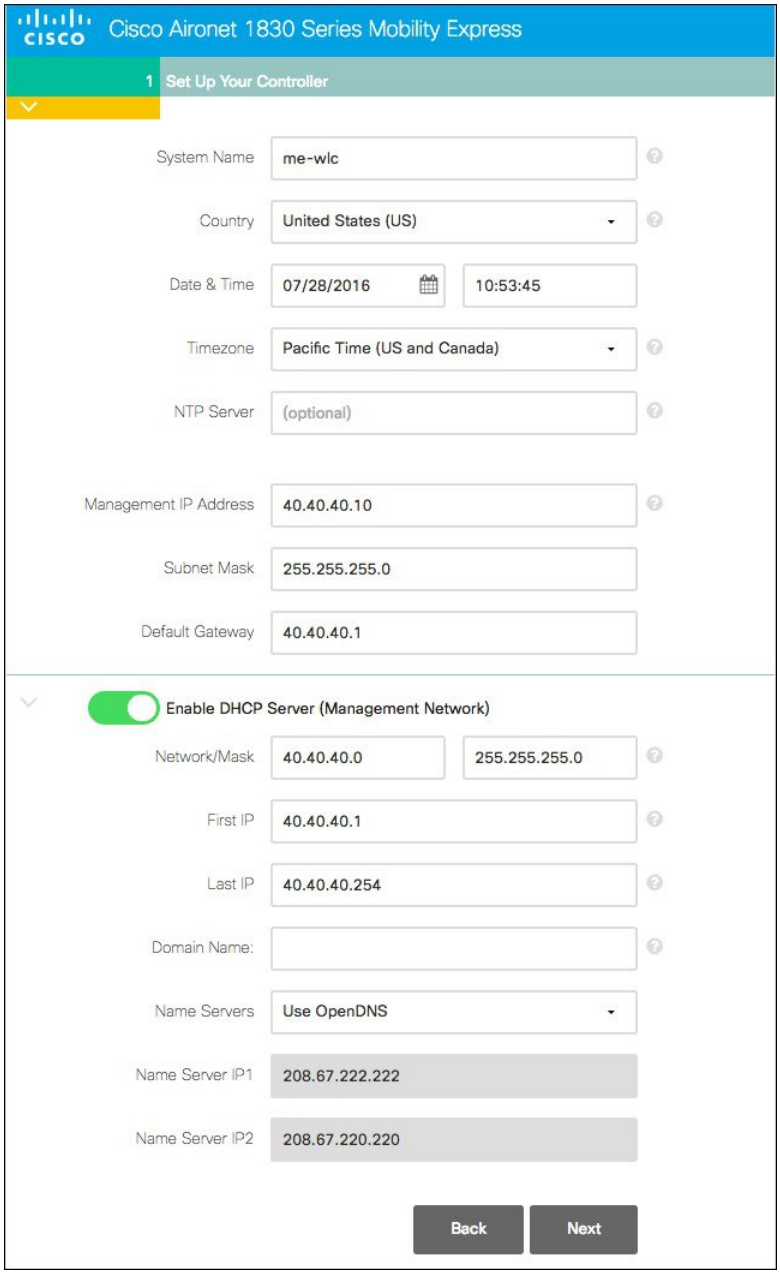
- The password must contain characters from at least three of the following classes – lowercase letters, uppercase letters, digits, special characters.
- No character in the password can be repeated more than three times consecutively.
- The new password must not be the same as the associated username 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 Set up your controller by specifying the values.

On the Set Up Your Controller screen, using the checklist, specify the following:

Field Name	Description
System Name	Enter the system name for Mobility Express. Example: me-wlc
Country	Choose the country from the drop down list.
Date & Time	Choose the current date and time. **Note** The wizard attempts to import the clock information (date and time) from the computer using JavaScript. It is highly recommended that you confirm the clock settings before continuing. The access points depend on clock settings to join the WLC.
Time Zone	Choose the current time zone.
NTP Server	Enter the NTP server details (Optional). If left blank, the following three NTP pools will be automatically configured:
Management IP Address	Enter the Management IP address.
Subnet Mask	Enter the subnet mask address.
Default Gateway	Enter the default gateway.
Enable DHCP Server (Management Network)	Internal DHCP server can be used to create scopes for Management & Access Points, Employee, and Guest Networks. Enabling of internal DHCP is optional but if you plan to use the internal DHCP server in your Mobility Express deployment, it is recommended to enable it and create a scope for Management in Day 0. In this configuration, we will enable internal DHCP server and create a scope for Management Network in Day 0. A DHCP scope for Employee and Guest Network will be configured in Day 1.
Network/Mask	Enter the Network and Mask for the Management Scope
First IP	Enter the first IP address of the Management Scope
First IP	Enter the last IP address of the Management Scope
Domain Name	Enter the Domain Name for the scope (Optional)
Name Servers	Enter the Name Server IP addresses or select Use Open DNS to configured Open DNS Name Server IP addresses

Figure 3: Set Up Your Controller Tab



Step 5 Click **Next**.

Step 6 Create the Employee wireless network by specifying the following fields:

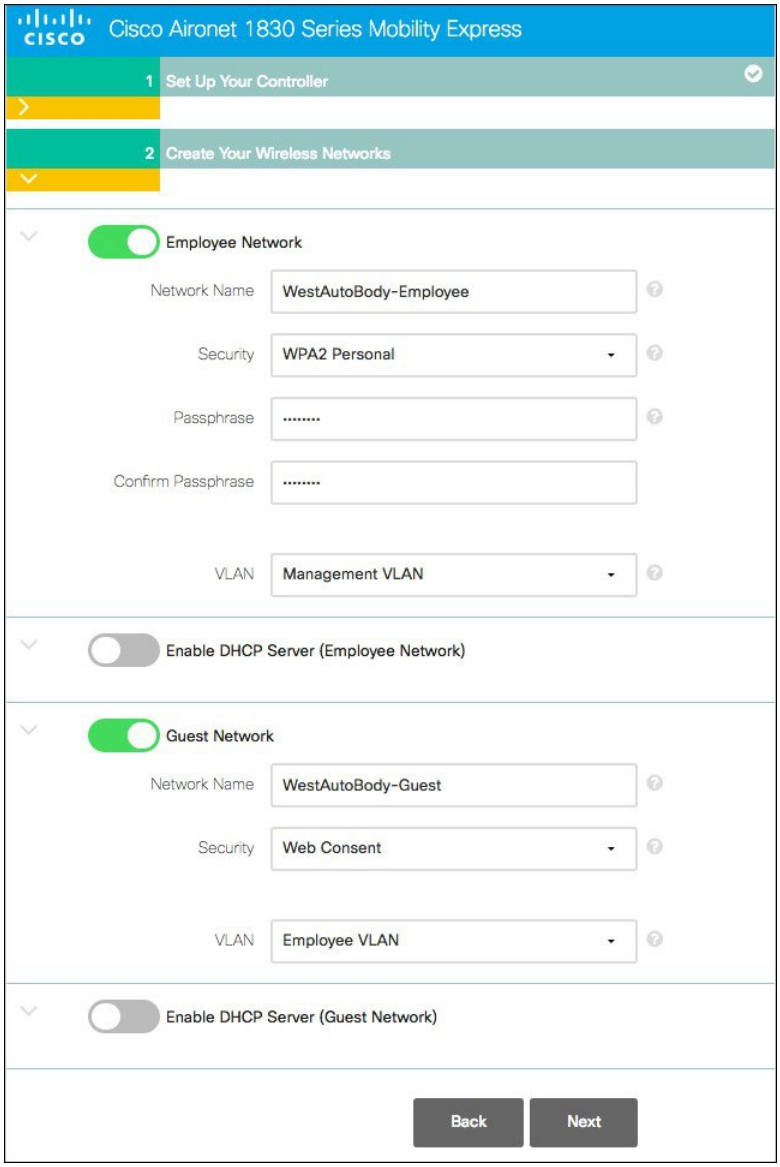
Field Name	Description
Network Name	Enter the network name.

Field Name	Description
Security	Choose the security type from the drop-down list. (Choose either **WPA2 Personal** which uses Pre-Shared Key (PSK) authentication or select **WPA2 Enterprise** (also called 802.1x) which requires a RADIUS server for authentication).
Pass Phrase	If you have chosen WPA2 Personal security, specify the Pre-Shared Key (PSK).
Confirm Pass Phrase	Re-enter and confirm the pass phrase.
Authentication Server IP Address	Enter the IP address of the Authentication Server
Shared Secret	If you have chosen WPA2 Enterprise, specify the shared secret for the RADIUS server.
VLAN	Choose Management VLAN or create a new VLAN.
VLAN ID	If you have created a new VLAN specify the VLAN ID. (VLAN ID from 1 to 4096).
Enable DHCP Server (Employee Network)	If internal DHCP server has to be used for Employee Network, Enable DHCP Server for Employee Network and specify the scope parameters.

Step 7 Enable the **Guest Network** slider and specify the following parameters:

Field Name	Description
Network Name	Specify the SSID for your Guest network.
Security	Choose **Web Consent** or **WPA2 Personal** from the drop-down list.
Pass Phrase	If WPA2 Personal security is chosen, specify the Pre-Shared Key (PSK).
VLAN	Choose **Employee VLAN** or create a New VLAN (with VLAN ID 1 to 4096).
VLAN ID	Specify the VLAN ID of the new VLAN (with VLAN ID 1 to 4096).
Enable DHCP Server (Guest Network)	If internal DHCP server has to be used for Guest Network, Enable DHCP Server for Guest Network and specify the scope parameters.

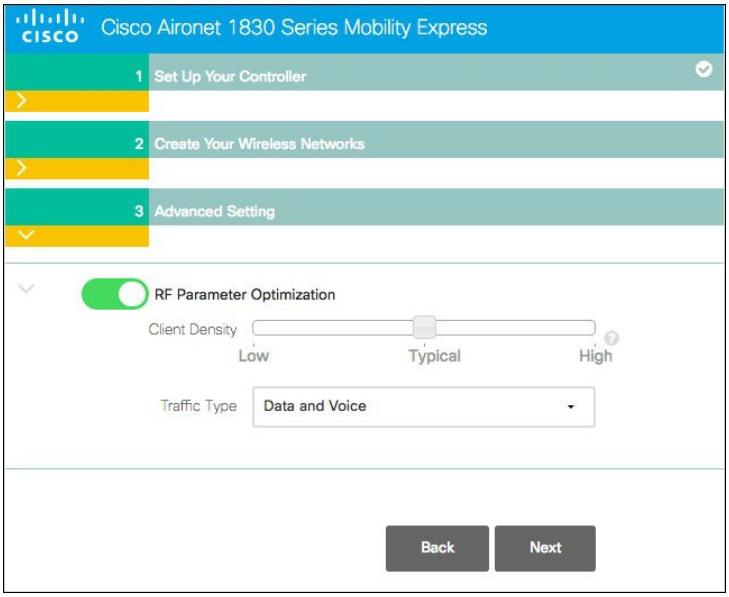
Figure 4: Create Your Wireless Networks - Guest



Step 8 Click **Next**.

Step 9 In the Advanced Settings tab, enable **RF Parameter Optimization** slider and optimize by indicating the expected client density and traffic type in your network.

Figure 5: Advanced Settings Tab



The following table depicts the default values when low, typical, or high deployment type is selected from RF parameters

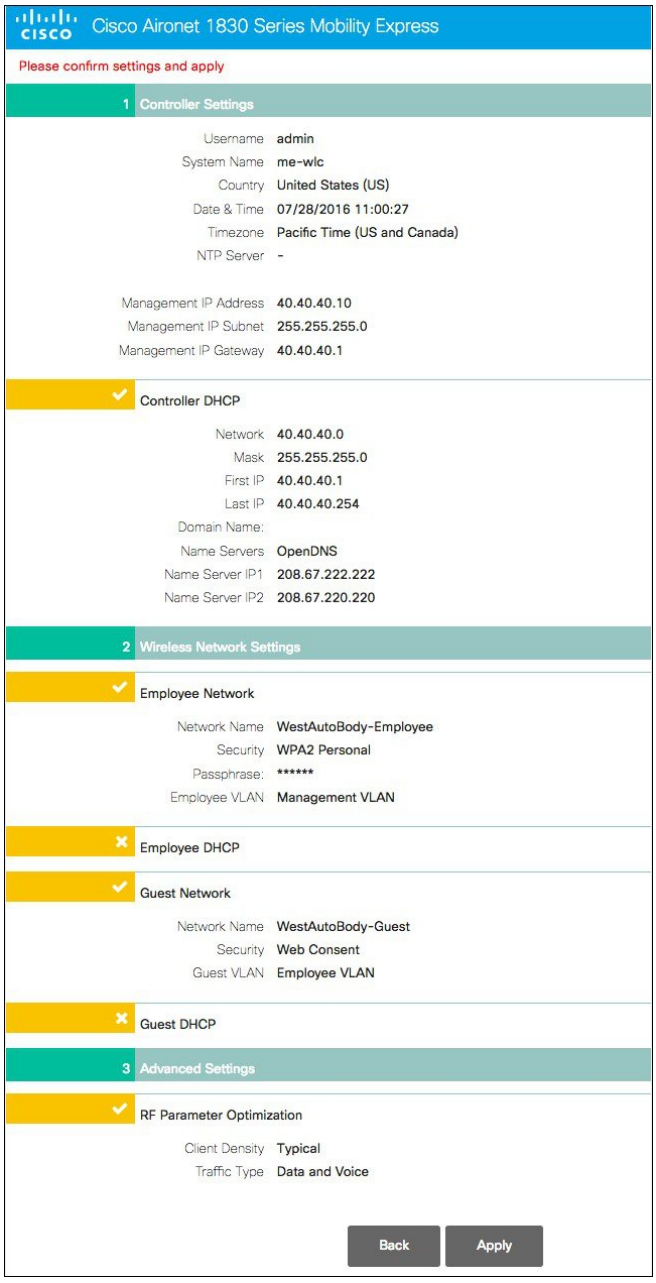
	dependency	Typical (Enterprise - default profile)	High Density (Throughput)	Low Density (Coverage Open Space)	Legacy (if disabled RF opt)
Tx Power (Following three items are equivalent to Tx Power) TPC threshold TPC min TPC max	Global per band Specific RF Profile per band	default TPC Min default (-10) TPC Max default (30)	Higher TPC threshold -65db 5G -70 for 2.4 TPC min +7dbm TPC max default (30)	Highest (1) threshold: 5G -60db 24G -65db TPC Min - Default(-10) TPC max - default (30)	default
Rx Sensitivity (rxsop)	Global per band (Advanced Rx Sop) RF profiles	default (auto)	medium (rxsop)	low	default
CCA Threshold	Global per band 802.11 a only (hidden) RF Profile	default (0)	default (0)	default(0)	default
Coverage RSSI Threshold	Global per band data and voice RSSI in (Coverage) RF Profile	default (Data : -80 Voice : -80)	default (Data : -80 Voice : -80)	Higher (Data : -90 Voice : -90)	default
Coverage Client Count	Global Per band (Coverage Exception) RF Profiles (Coverage Hole Detection)	default (3)	default (3)	Lower (2) (1-3)	default
Data Rates	Global per band (network) RF Profiles	12 Mbp mandatory 9 supported 1,2, 5.5, 6, 11 Mbp disable	12 Mbp mandatory 9 supported 1,2, 5.5, 6, 11 Mbp disable	CCK rates enable 1,2, 5.5, 6, 9,11,12 Mbp enable	default

Step 10 Select Traffic Type and click **Next** to continue.

A confirmation screen displays the summary of the configuration.

Step 11 Click **Apply**, if all the settings are correct

Note A message appears indicating that the System will reboot. Click OK on this window.



Step 12 Click **OK** to reboot.

Note After the Access Point reboots, it will start the Mobility Express controller function.

Configuring Mobility Express Controller using Startup Wizard from CLI

- Console Connection
- Startup Wizard from CLI

Console Connection

Before you can configure the AP to Mobility Express Controller, connect to the port marked '**CONSOLE**' using SecureCRT, Putty or similar applications. 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. Choose the serial baud rate of 9600.

Startup Wizard from CLI

After connecting to the 'CONSOLE' port on the AP, power up the AP. After a few minutes, the following Welcome message will be shown. 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: 40.40.40.10
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 40.40.40.1
Cleaning up Provisioning SSID
Create Management DHCP Scope? [yes][NO]: yes
DHCP Network : 40.40.40.0
DHCP Netmask : 255.255.255.0
Router IP: 40.40.40.1
Start DHCP IP address: 40.40.40.11
Stop DHCP IP address: 40.40.40.254
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
```

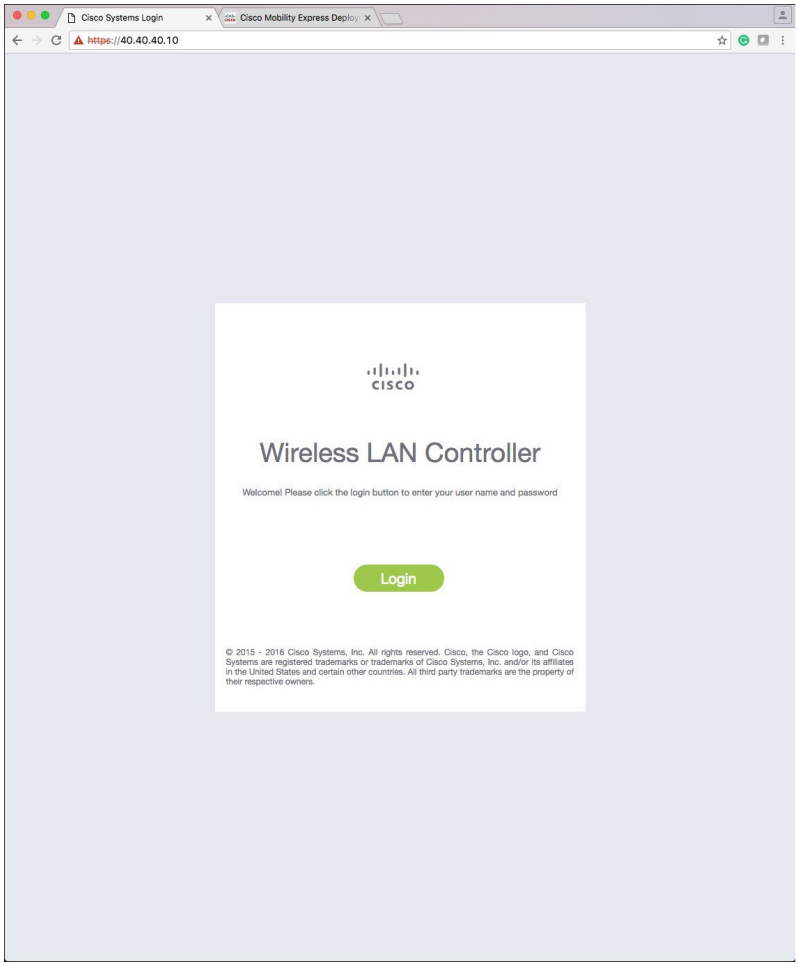
Note After the AP has finished rebooting, login to the Mobility Express controller WebUI using the Management IP address.

Logging into Mobility Express Controller

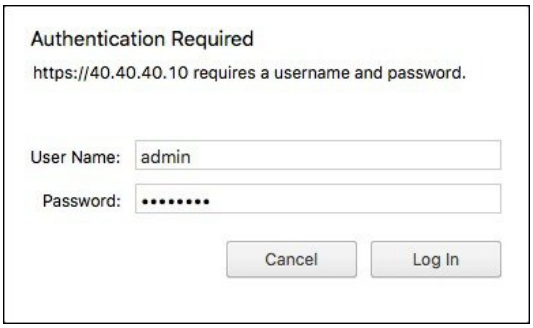
To log in to the Mobility Express, perform the following steps:

Procedure

Step 1 Enter the IP address of the Mobility Express management interface in the web browser. The **Cisco Wireless LAN Controller** window appears.



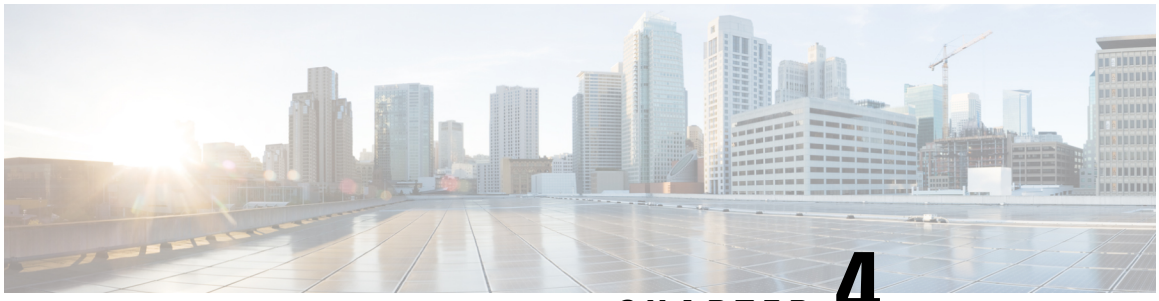
Step 2 Click **Login**.



Step 3 Enter the administrator user name and password.

Note The 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.

The Network Summary page appears.



CHAPTER 4

Creating DHCP Scopes for Wireless Networks

Starting Release 8.3.102.0, one can enable internal DHCP Server and create scopes for Access Points, Employee, and Guest Networks. A total of 17 DHCP scopes are supported on Mobility Express.

Note Using a mix of Internal DHCP server and External DHCP server at the same time in a Mobility Express Deployment is not supported at this time.

Creating DHCP Scopes for Wireless Networks

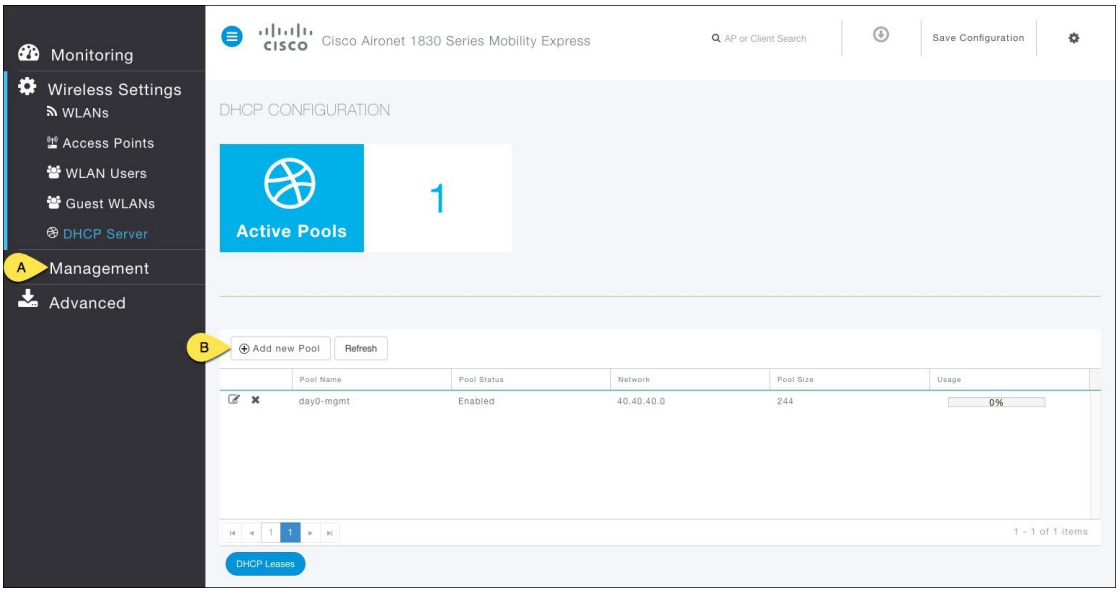
To create DHCP scopes, follow the steps below:

Note We enabled DHCP and created a pool for Management during the Day 0 Intial Setup Wizard. We also created Employee and Guest Networks. In this procedure, we will create and assign a DHCP pools for Employee and Guest networks which were created during Day 0.

Procedure

Step 1 Navigate to **Wireless Settings > DHCP Server > Add new Pool**.

Creating DHCP Scopes for Wireless Networks



Step 2 On the Add DHCP Pool window. Enter the following fields:

A. Enter the Pool Name for the Employee network

B. Enable the Pool Status

C. Enter the VLAN Id for the Employee Network

D. Enter the Lease Period for the clients. Defaul is 1 Day

E. Enter the Network address and Mask

F. Enter the Start IP for the DHCP Pool

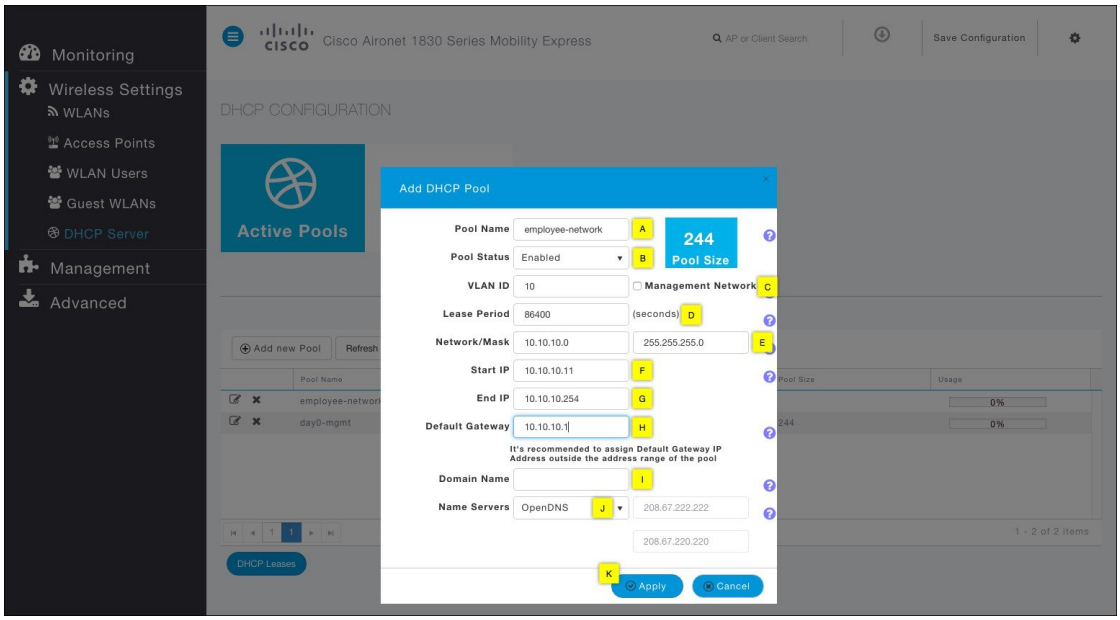
G. Enter the End IP for the DHCP Pool

H. Enter the Default Gateway

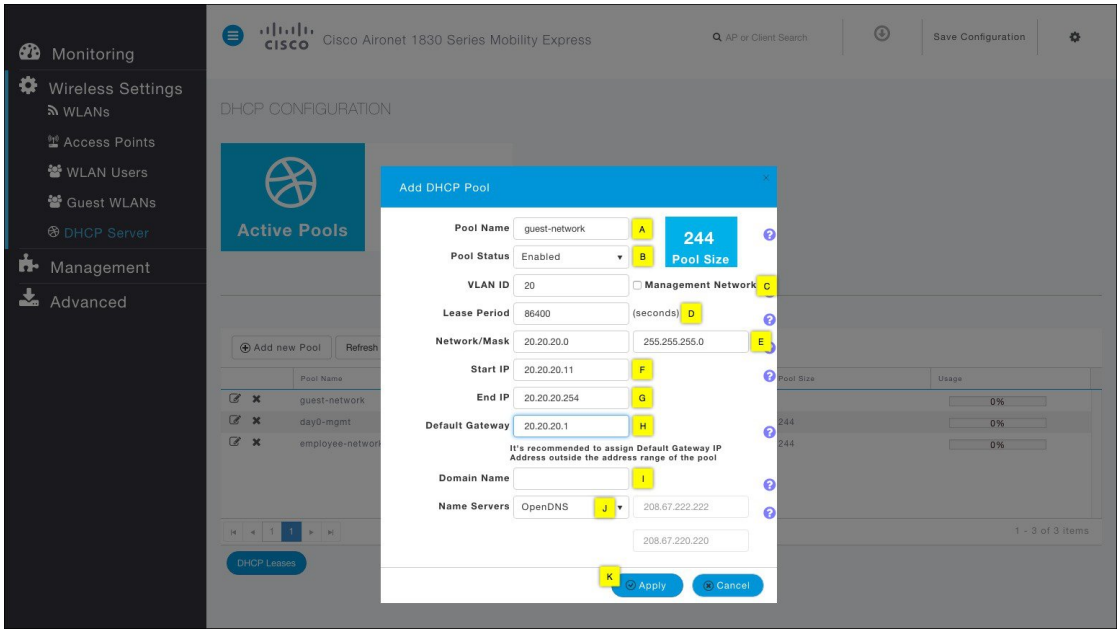
I. Enter the Domain Name (Optional)

J. 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

K. Click on Apply



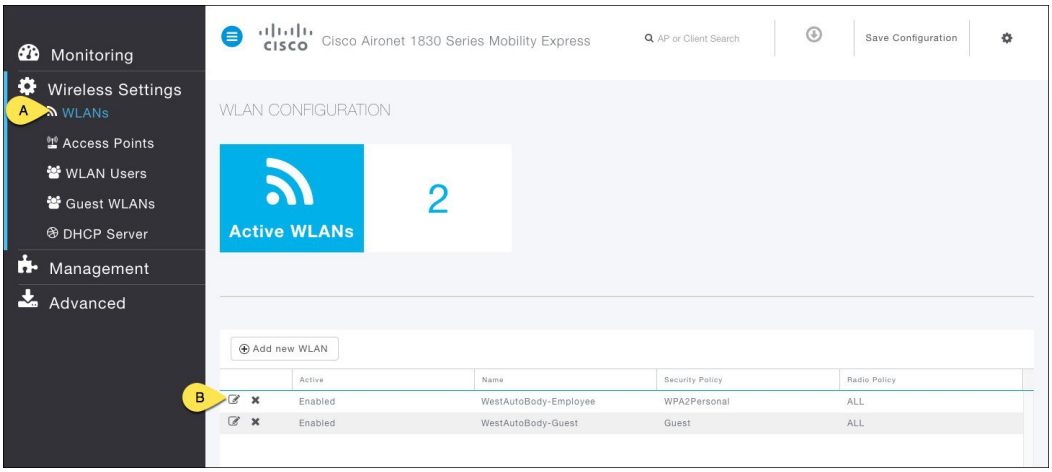
Step 3 Repeat Step 2 above for the Guest network.



Note After the DHCP Pools have been created for Employee and Guest networks, we should now assign them to the WLANs so that the clients get an IP address from their respective DHCP Pools.

Step 4 To assign the DHCP Pool to Employee Network, navigate to Wireless Settings > WLANs and then click on B to edit the Employee WLAN.

Creating DHCP Scopes for Wireless Networks

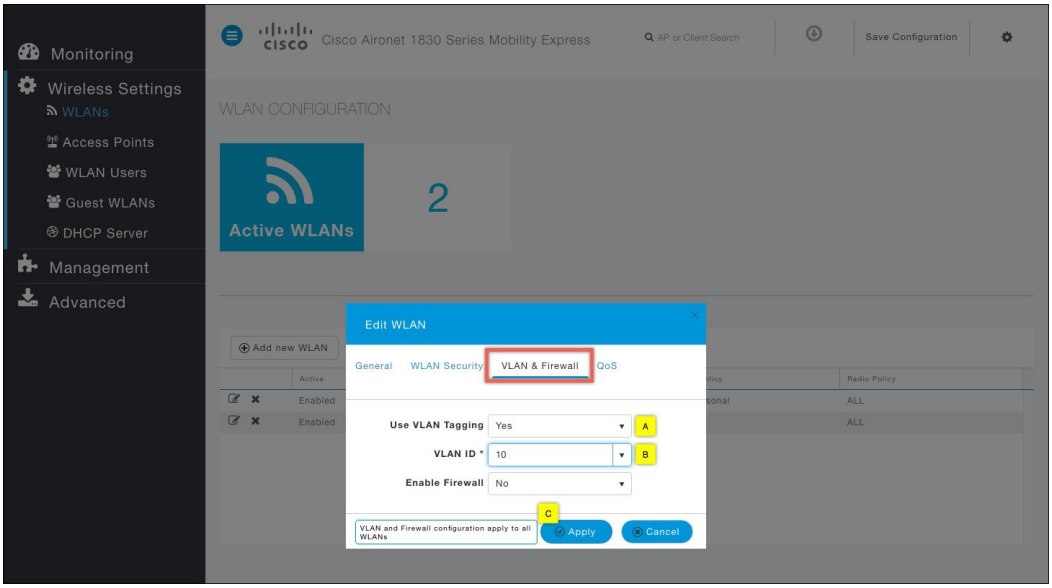


Step 5 In the Edit WLAN window, go to VLAN & Firewall, and configure the following:

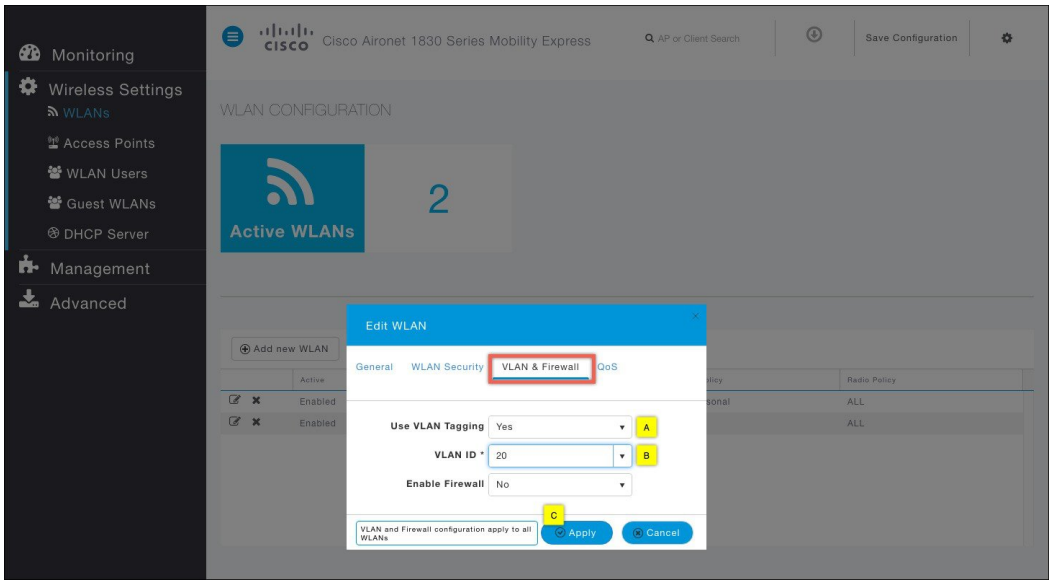
A. Select Yes from the VLAN Tagging

B. Enter the VLAN ID used for the Employee DHCP Pool

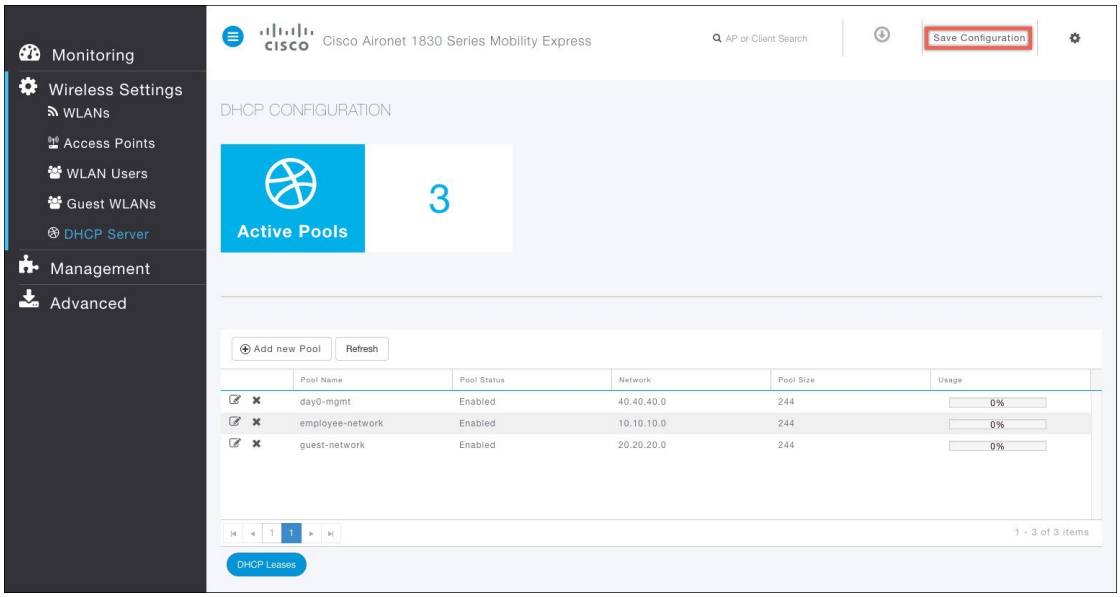
C. Click on the Apply Button



Step 6 Repeat the same for the Guest WLAN.

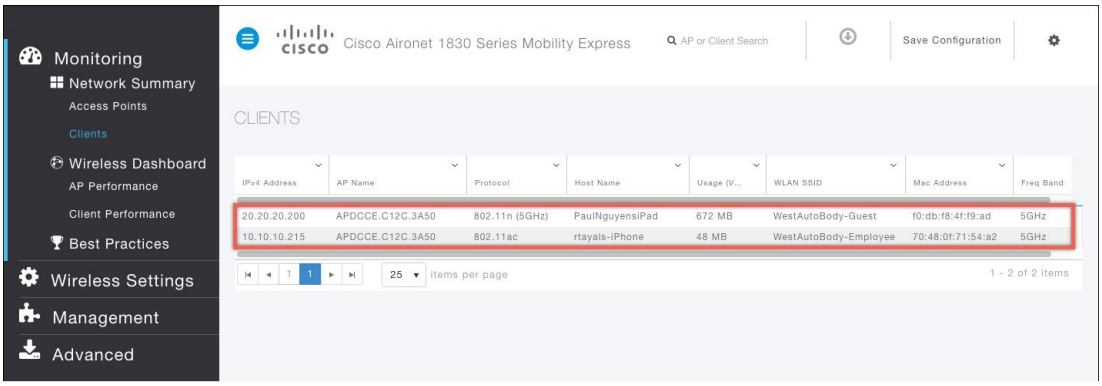


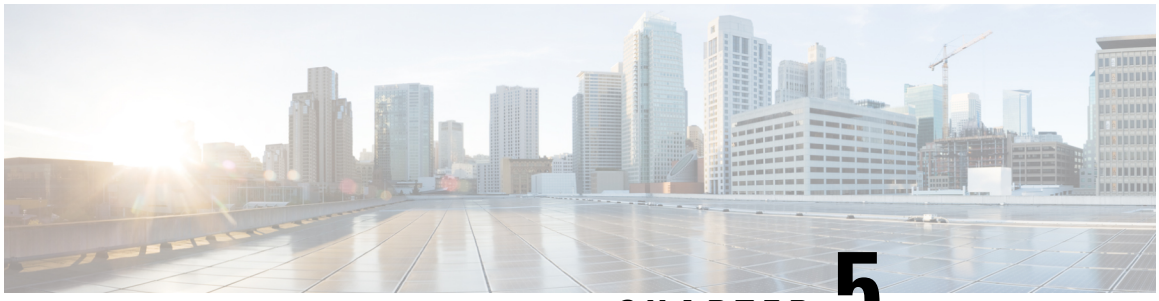
Step 7 Save the configuration.



Step 8 Connect the clients to Employee and Guest networks and verify their IP Addresses from their respective DHCP Pools.

Creating DHCP Scopes for Wireless Networks





CHAPTER 5

Configuring Mobility Express 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.

Pre-requisites

1. Access Points–Cisco 802.11ac Wave 2 access points running Cisco Mobility Express software. The following APs support site survey capability:

Access Point	Release
1830 Series	AireOS Release 8.3.111.0 and later
1850 Series	AireOS Release 8.3.111.0 and later
2800 Series	AireOS Release 8.3.111.0 and later
3800 Series	AireOS Release 8.3.111.0 and later
1560 Series	AireOS Release 8.3.111.0 and later

2. Power Source–Depending on the Access Point being used for Site Survey, one can use a power adapter or a battery pack capable of providing sufficient power to the Access Point.
3. Console Cable(Optional)–Cisco Mobility Express can be configure using the CLI or Over-the-air. For configuring Cisco Mobility Express via CLI, a console connect to the Access Point would be required.

Configuring Mobility Express for Site Survey using CLI

Procedure

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:

```
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 SHCP 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
DoaminName: mewlc.local
DNS Server:[OPENDNS][user DNS]OPENDNS
Create Employee Network?[YES][no]:yes
Employee Network Name(SSID)?:site_survey
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>
```

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 2800 and 3800 series 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. 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.

c. When the XOR (2.4 GHz) radio is configured to operate at 5GHz, 100MHz frequency separation is required from dedicated 5GHz radio.

d. 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.

To configure the XOR (2.4GHz) radio to operate at 5GHz on 2800 and 3800 Series Access Points, follow the steps below:

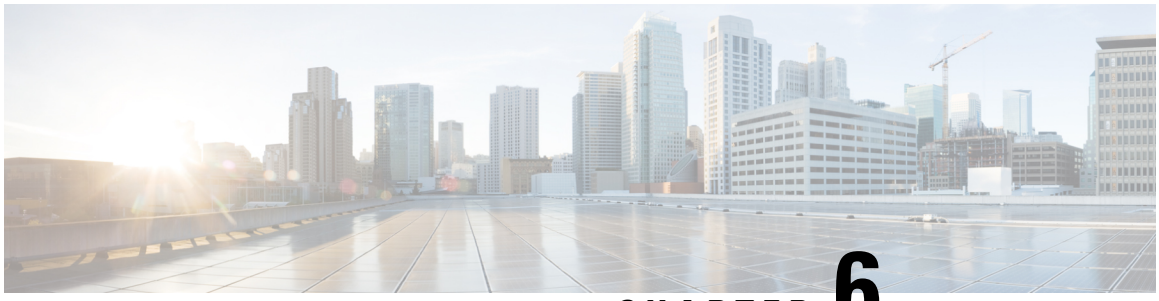
```
(Cisco Controller) >config 802.11-abgn disable ap
(Cisco Controller) >config 802.11-abgn role ap manual client-serving
(Cisco Controller) >config 802.11-abgn band ap ap 5GHz
(Cisco Controller) >config 802.11-abgn enable ap
```

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
```



CHAPTER 6

Creating Wireless Networks

WLANs

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.

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 Networks

Creating WLAN using WPA2 Personal

Procedure

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:

a) Enter the **Profile Name**.
b) Enter the **SSID**.

Note Admin State is **Enabled** and Radio Policy is set to **ALL** by default. One can change this if needed.

Step 3 Click on the WLAN Security and configure the following:

a) Select **Security** as *WPA2 Personal*.
b) Enter the **Passphrase** and Confirm **PassPhrase**.

Step 4 Click the **Apply** Button.

Note If the WLAN users have to be put a specific vlan, click on **VLAN & Firewall** and configure the VLAN.

Creating Employee WLAN using WPA2 Enterprise with External Radius Server

Procedure

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:

a) Enter the **Profile Name**.
b) Enter the **SSID**.

Note Admin State is **Enabled** and Radio Policy is set to **ALL** by default. One can change this if needed.

Step 3 Click on the **WLAN Security** and configure the following:

a) Select **Security** as *WPA2 Personal*.
b) Select **Authentication Server** as *External Radius*.
c) Enter the Radius **IP Address**.
d) Enter the Radius **Port** number.

e) Enter the Shared Secret.

Step 4 Click on the Icon as pointed by the Red arrow to add the Radius server.

Note Optionally, a second Radius Server can be configured.

Step 5 Click the **Apply** Button.

Creating WLAN using WPA2 Enterprise with Local Authentication (AP)

Procedure

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:

a) Enter the **Profile Name**.

b) Enter the **SSID**.

Note Admin State is **Enabled** and Radio Policy is set to **ALL** by default. One can change this if needed.

Step 3 Click on the **WLAN Security** and configure the following:

a) Select **Security** as *WPA2 Personal*.

b) Select **Authentication Server** as *AP*.

Note For Authentication Server as AP, local user accounts have to created on the Primary AP.

Step 4 Click the **Apply** Button.

Creating Guest Network on Mobility Express

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, choose the Security as Guest. You can set the Guest Type by choosing one of the following options in the Guest Type drop-down list:

1. CMX Guest Connect
2. WPA2 Personal—This option stands for Wi-Fi Protected Access 2 with Pre-Shared Key (PSK). WPA2 Personal is a method of securing your network with the use of a PSK authentication. The PSK is configured separately both on the controller AP, under WLAN security policy, and on the client. WPA2 Personal does not rely on an authentication server on your network. This is used when you do not have an enterprise authentication server. If you choose this option, then specify the PSK in the Shared Key field.
3. Captive Portal (AP)
    - Require Username and Password—This is the default option. Choose this option to authenticate guests using the username and password which you can specify for guest users of this WLAN, under Wireless Settings > WLAN Users.

- Display Terms & Conditions—Choose this option to allow guest access to the WLAN upon acceptance of displayed terms and conditions. This option allows guest users to access the WLAN without entering a username and password.
- Require Email Address—Choose this option, if you want guest users to be prompted for their e-mail address when attempting to access the WLAN. Upon entering a valid email address, access it provided. This option allows guest users to access the WLAN without entering a username and password.

4. Captive Portal (External Web Server)

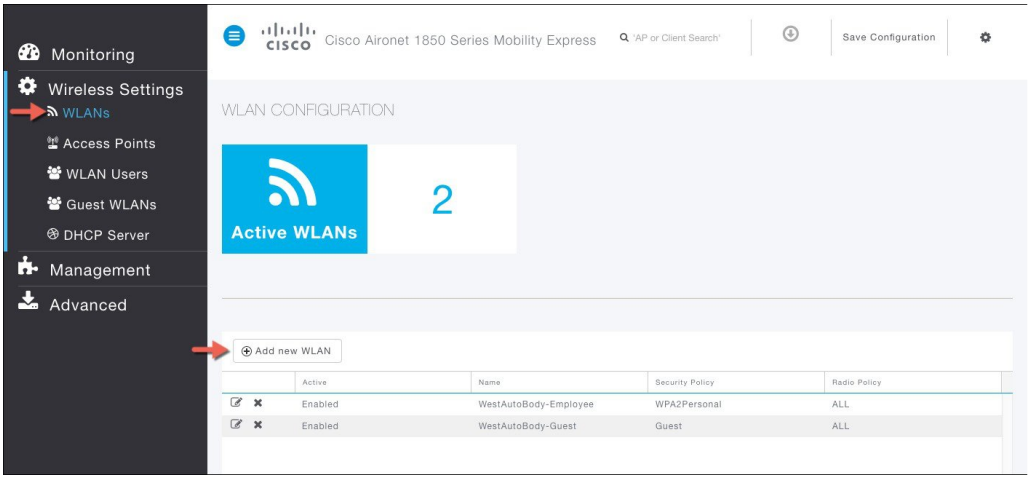
Guest Access using CMX Connect in the Cloud

Note In order to configure Guest Access using CMX Connect in the Cloud, you must have a CMX Cloud Account with subscription to the CMX Connect service. Also, Guest Portal have to be created in CMX Cloud so that when a client connects to the Guest WLAN which is configured for CMX Connect in the Cloud, the Guest Portal is presented to the client. To learn more about CMX Cloud, please refer to the chapter Cisco Mobility Express with Cisco CMX Cloud.

To configure a Guest WLAN with CMX Connect in the Cloud, follow the steps below:

Procedure

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

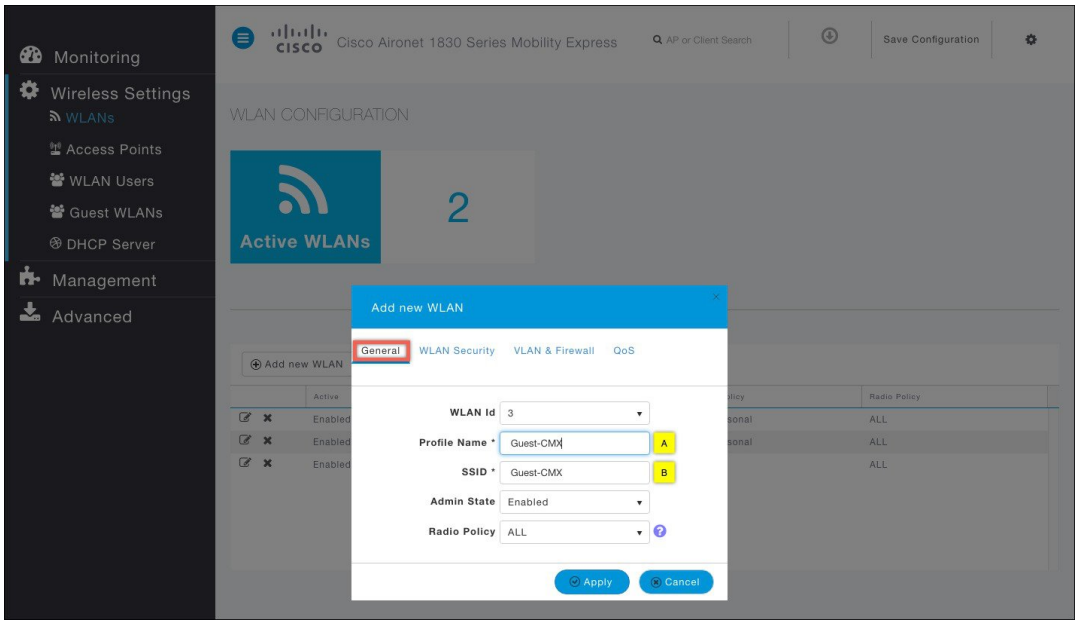


Step 2 In the **Add new WLAN** window, on the General page configure the following:

A. Enter the Profile Name

B. Enter the SSID

Note Admin State is **Enabled** and Radio Policy is set to **ALL** by default. One can change this if needed.



Step 3 Click on the WLAN Security and configure the following:

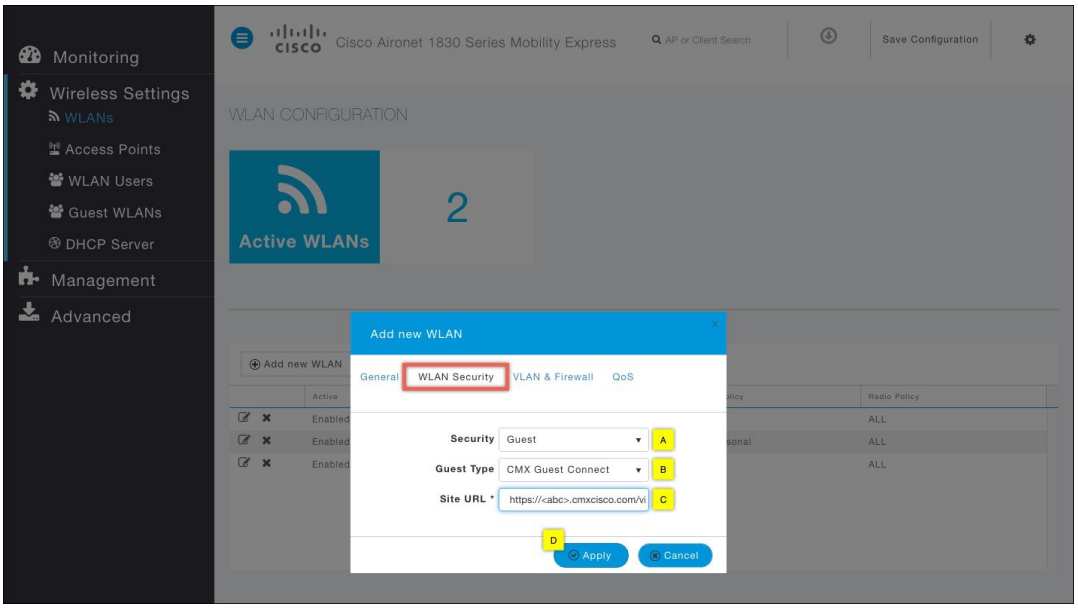
A. Select **Security** as *Guest*

B. Select **Guest Type** as *CMX Guest Connect*

C. Enter the **Site URL**. Site URL is the Guest Portal URL, which has been configured in CMX Connect in the cloud.

D. Click Apply button

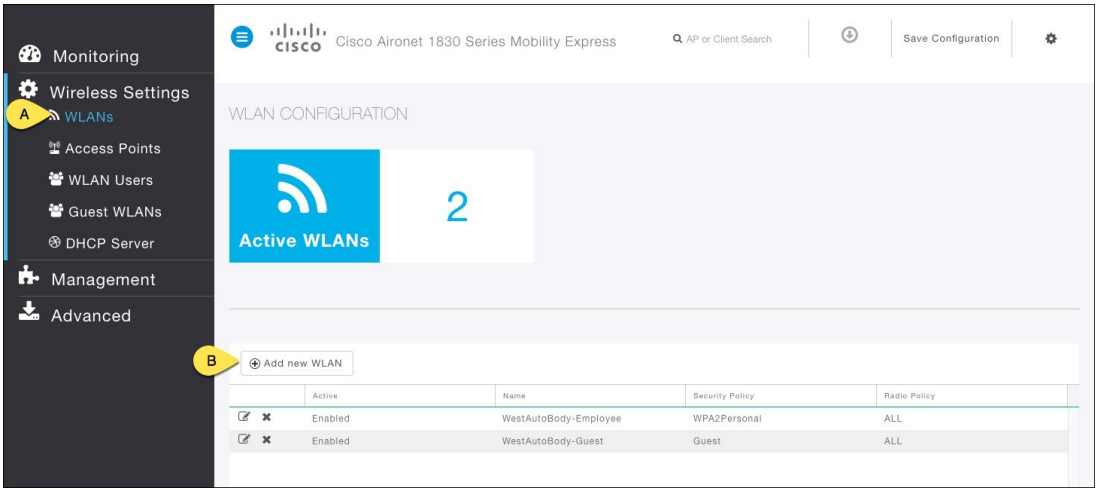
Note If the Guest users have to be put a specific vlan, click on **VLAN & Firewall** and configure the VLAN.



Guest Access using WPA2 Personal

Procedure

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

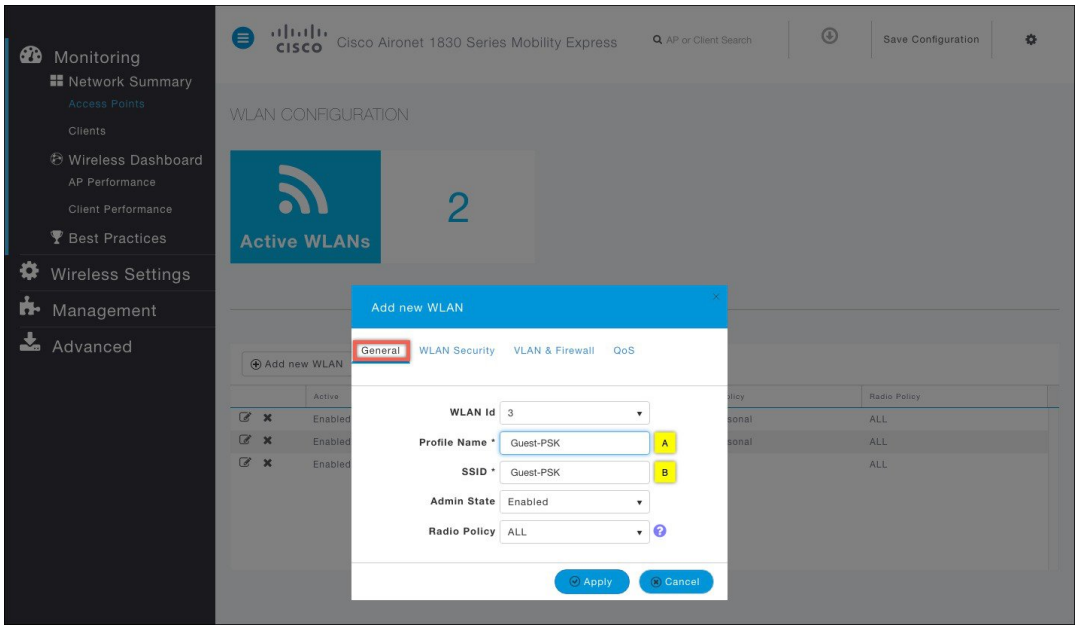


Step 2 In the **Add new WLAN** window, on the General page configure the following:

A. Enter the Profile Name

B. Enter the SSID

Note Admin State is **Enabled** and Radio Policy is set to **ALL** by default. One can change this if needed.



Step 3 Click on the WLAN Security and configure the following:

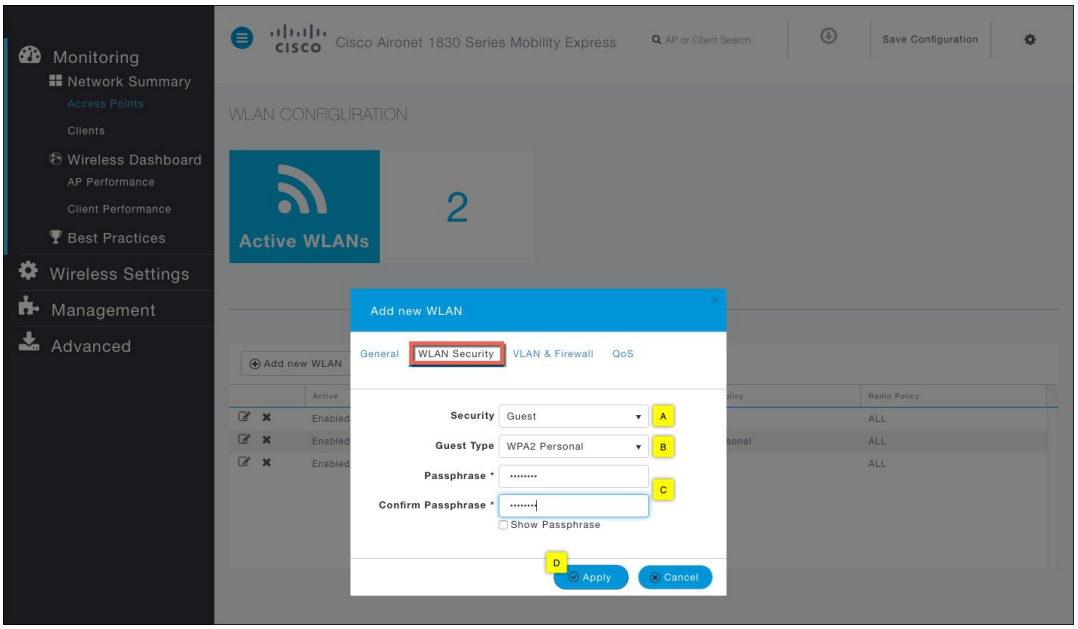
A. Select **Security** as *Guest*

B. Select **Guest Type** as *WPA2 Personal*

C. Enter the **Passphrase** and Confirm **PassPhrase**

D. Click Apply button

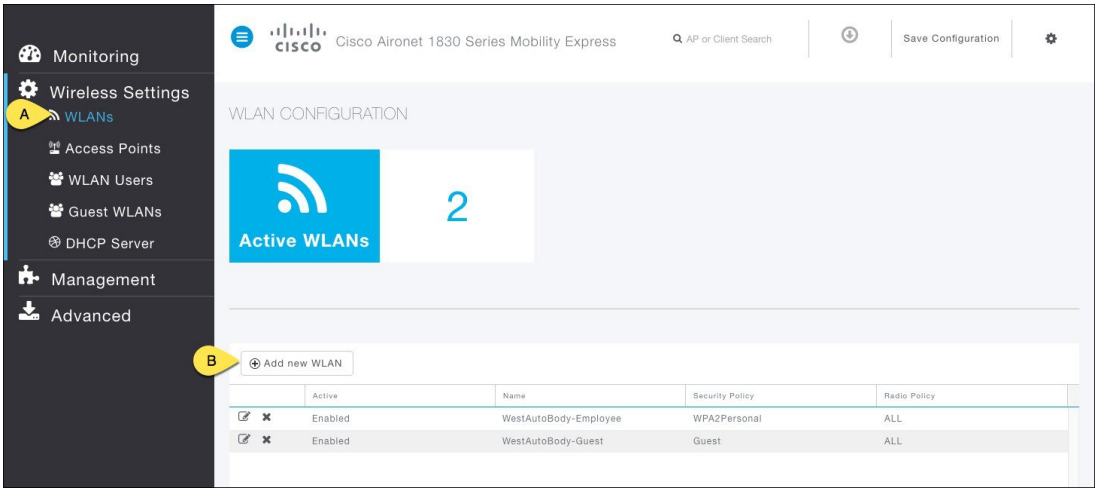
Note If the Guest users have to be put a specific vlan, click on **VLAN & Firewall** and configure the VLAN.



Guest Access using Captive Portal (AP)

Procedure

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

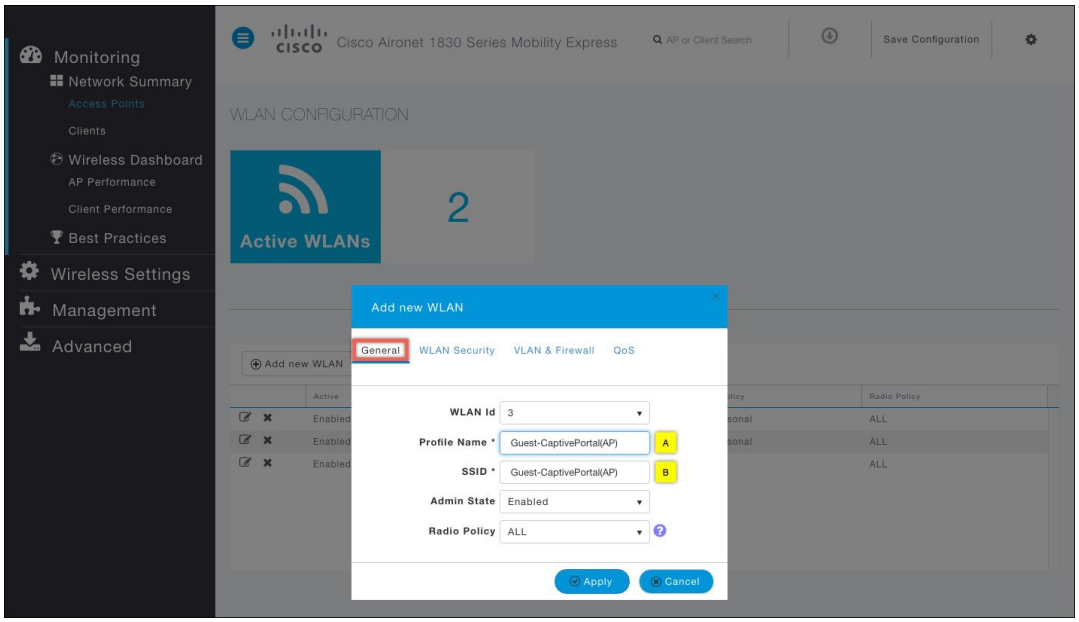


Step 2 In the **Add new WLAN** window, on the General page configure the following:

A. Enter the Profile Name

B. Enter the SSID

Note Admin State is **Enabled** and Radio Policy is set to **ALL** by default. One can change this if needed.



Step 3 Click on the WLAN Security and configure the following:

A. Select **Security** as *Guest*

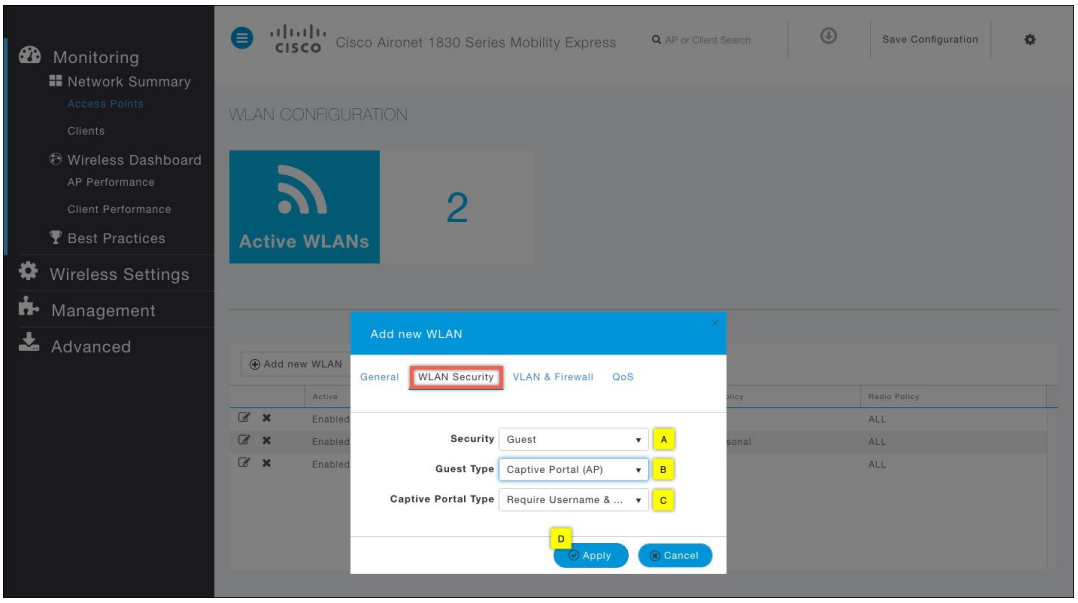
B. Select **Guest Type** as *Captive Portal (AP)*

C. Select **Captive Portal Type**. Options are:

- Require Username & Password (Note, local users would have to be created. To create local users, go to the WLAN Users section)
- Web Consent
- Require Email Address

D. Click Apply button

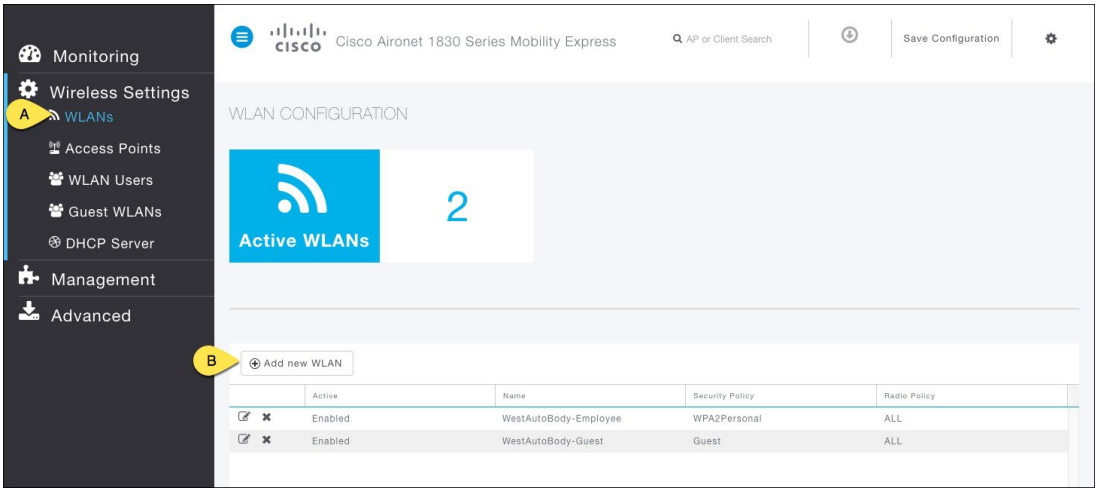
Note If the Guest users have to be put a specific vlan, click on **VLAN & Firewall** and configure the VLAN.



Guest Access using Captive Portal (External Web Server)

Procedure

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

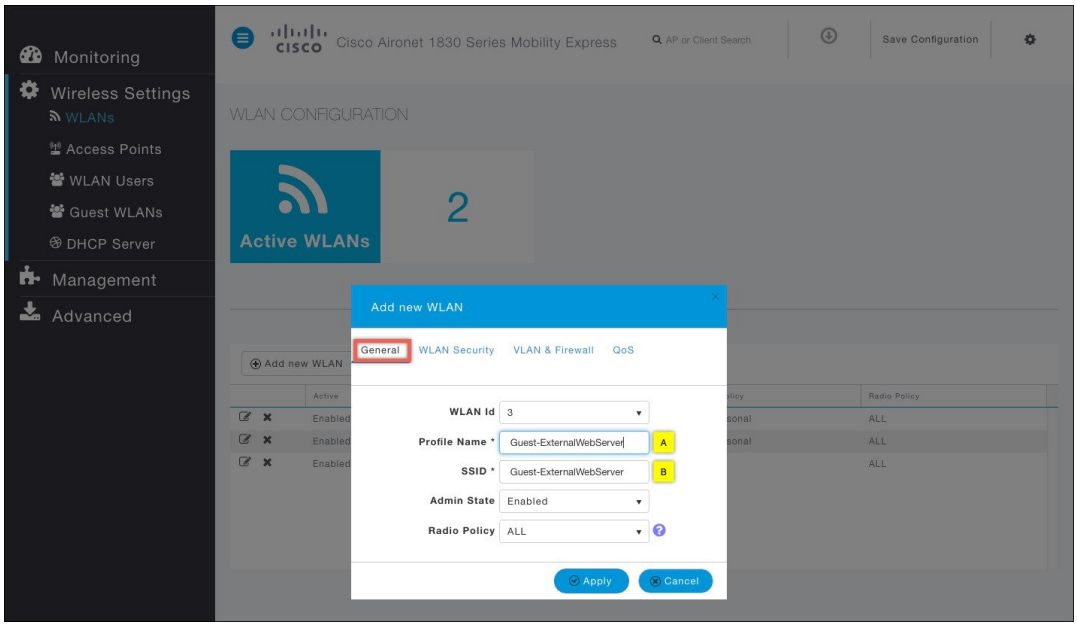


Step 2 In the **Add new WLAN** window, on the General page configure the following:

A. Enter the Profile Name

B. Enter the SSID

Note Admin State is **Enabled** and Radio Policy is set to **ALL** by default. One can change this if needed.



Step 3 Click on the WLAN Security and configure the following:

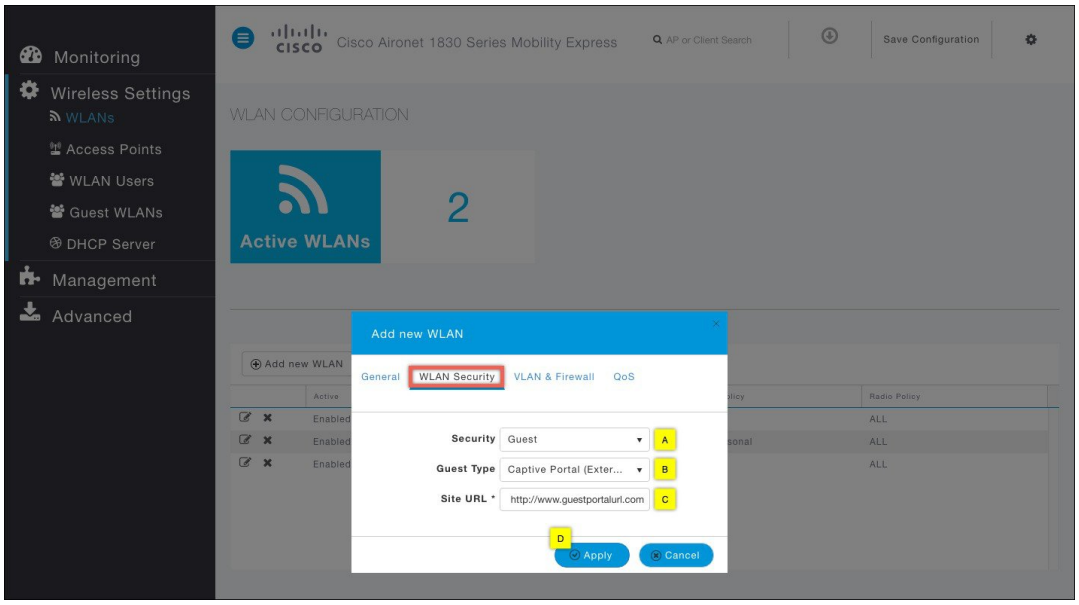
A. Select **Security** as *Guest*

B. Select **Guest Type** as *Captive Portal (External Web Server)*

C. Enter the **Site URL.** Site URL is the Guest Portal URL, which has been configured on the External Web Server

D. Click Apply button

Note If the Guest users have to be put a specific vlan, click on **VLAN & Firewall** and configure the VLAN.



Guest Portal Page for Internal WebAuth

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

Note The internal Guest Portal Page will be used for Guest WLANs with Guest Type as Captive Portal (AP) only.

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

Using Default Guest Portal Page

Procedure

Step 1 Navigate to **Wireless Settings > Guest WLANs.** The Guest WLAN page will be displayed showing the count of Guest WLANs configured on the Mobility Express controller.

Step 2 Configure the following:

A. **Page Type**—Select as *Internal (Default)*.

B. **Preview**—You can Preview the page by clicking on the **Preview** button.

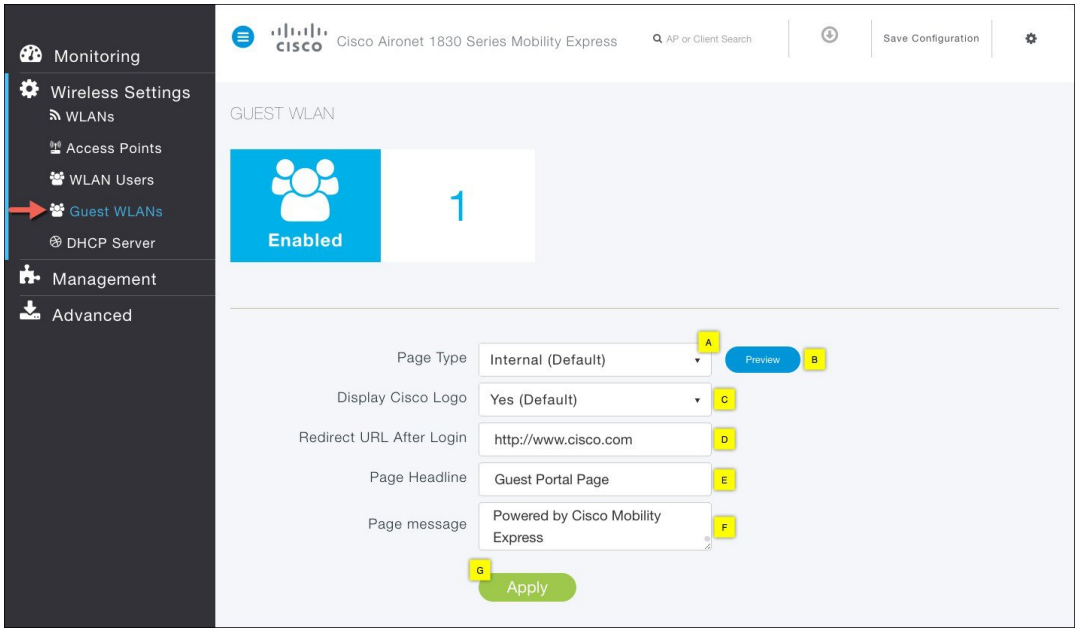
C. **Display Cisco Logo**—To hide the Cisco logo that appears in the top right corner of the default page, you can choose No. This field is set to Yes by default.

D. **Redirect URL After Login**—To have thee 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.

E. **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.

F. **Page Message**—To create your own message on the login page, enter the desired text in this text box. You can enter 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**.**

G. Click Apply button



Using Customized Guest Portal Page

If a customized Guest Portal page 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.

To download the sample bundle, navigate to

Once the page has been edited and ready to be uploaded to the Cisco Mobility Express controller, follow the steps below.

Procedure

Step 1 Navigate to **Wireless Settings > Guest WLANs.** The Guest WLAN page will be displayed showing the count of Guest WLANs configured on the Mobility Express controller.

Step 2 Configure the following:

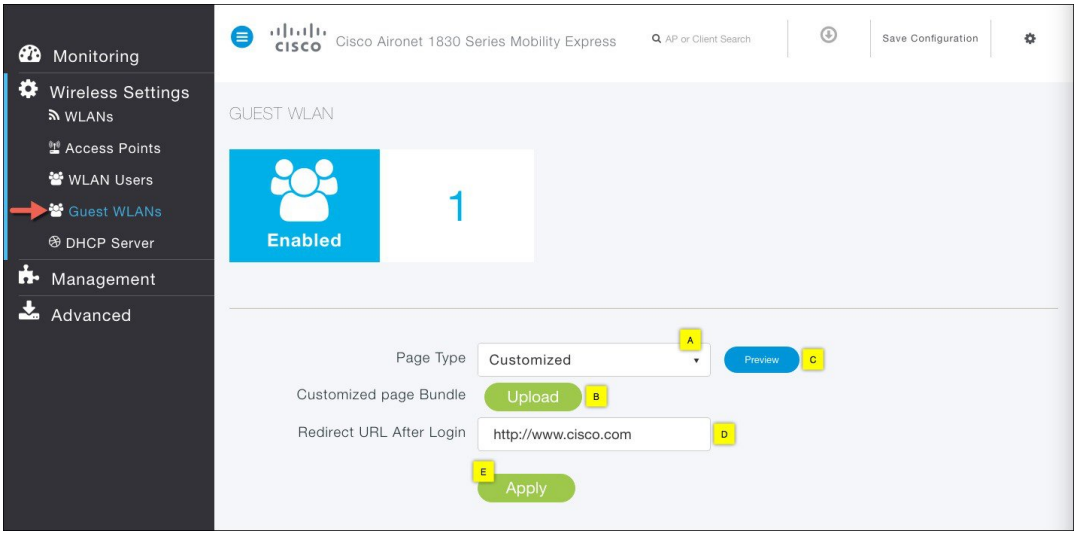
A. **Page Type**—Select as *Internal (Default).*

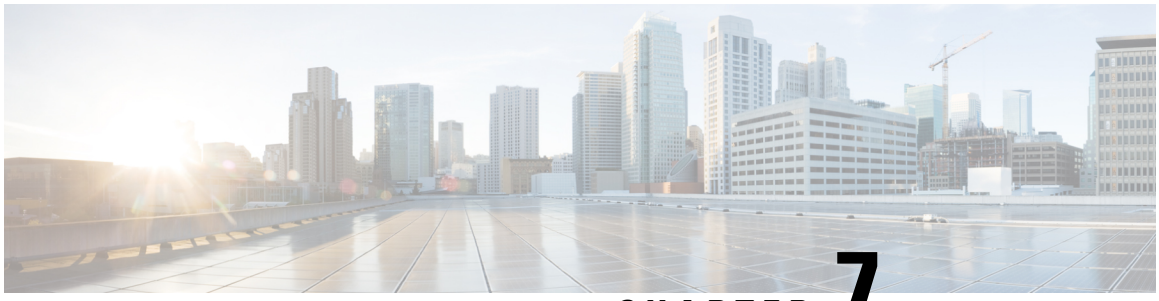
B. **Customized page Bundle**—Upload the customized page bundle to the Mobility Express controller.

C.**Preview**—You can Preview the page by clicking on the **Preview** button.

D. **Redirect URL After Login**—To have thee 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.

E. Click Apply button





CHAPTER 7

Managing WLAN Users

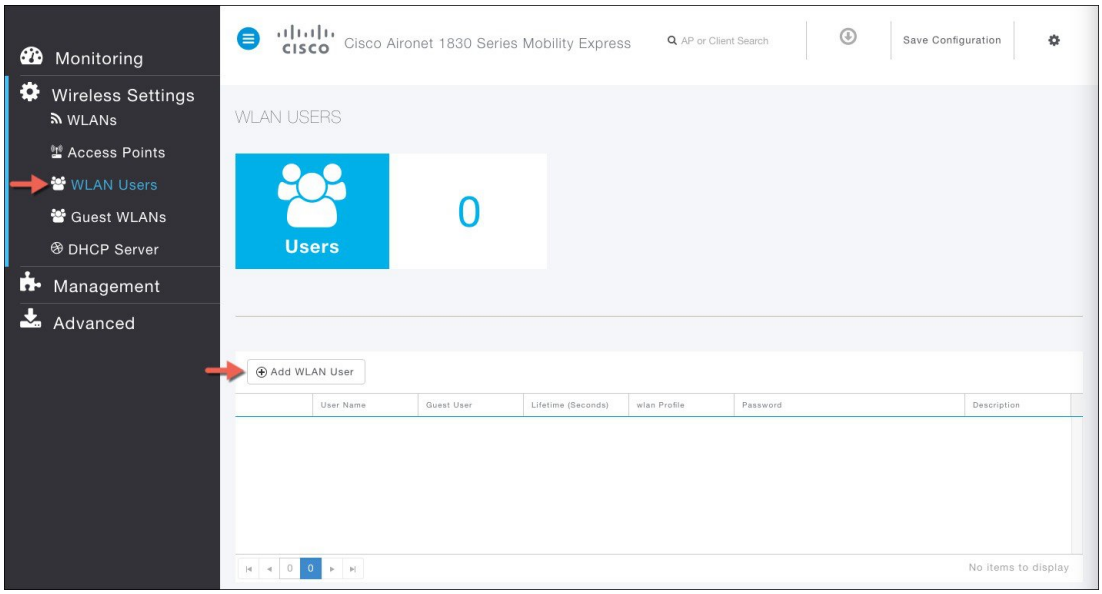
Cisco Mobility Express supports creation of local wireless users accounts. These wireless users can be authenticated for WLANs configured to use **Security** as *WPA2 Enterprise* with **Authentication Server** set to *AP* or Guest WLANs configured to use **Guest Type** as *Captive Portal (AP)* and **Captive Portal Type** set to *Require Username & Password*.

Managing WLAN Users

To create these users, follow the steps below:

Procedure

Step 1 Navigate to **Wireless Settings** > **WLAN Users** and click on the **Add WLAN user** button.



Step 2 Enter the following to configure the wireless user account.

Managing WLAN Users

A. **User Name**—Username of the wireless user

B. **Guest User**—For Guest wireless user, enable the checkbox

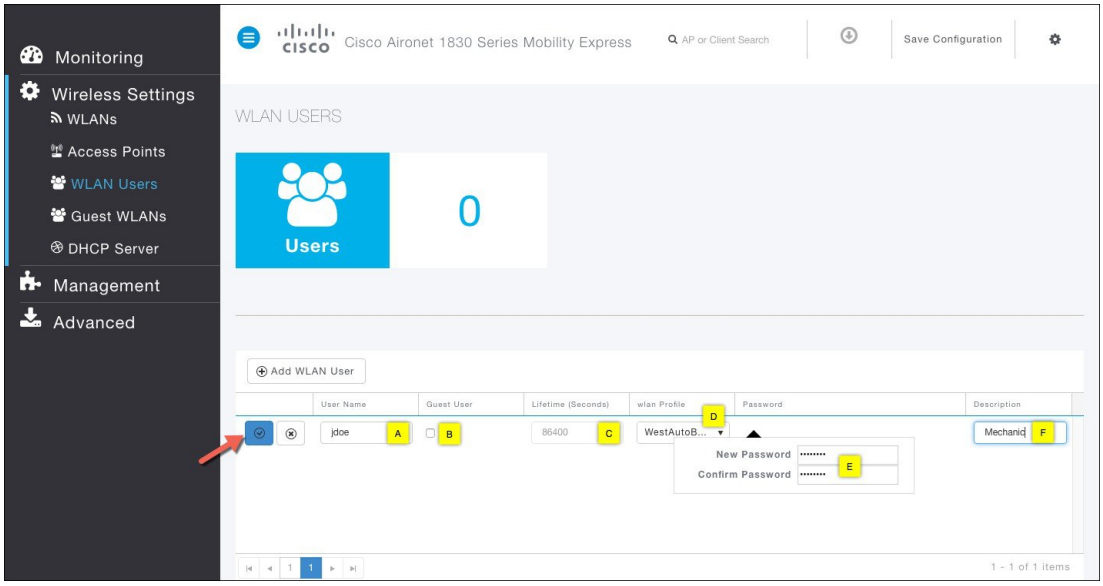
C. **Lifetime**—For Guest User, you can define the user account validity. Default is 86400 seconds (or, 24 hours) from the time of its creation

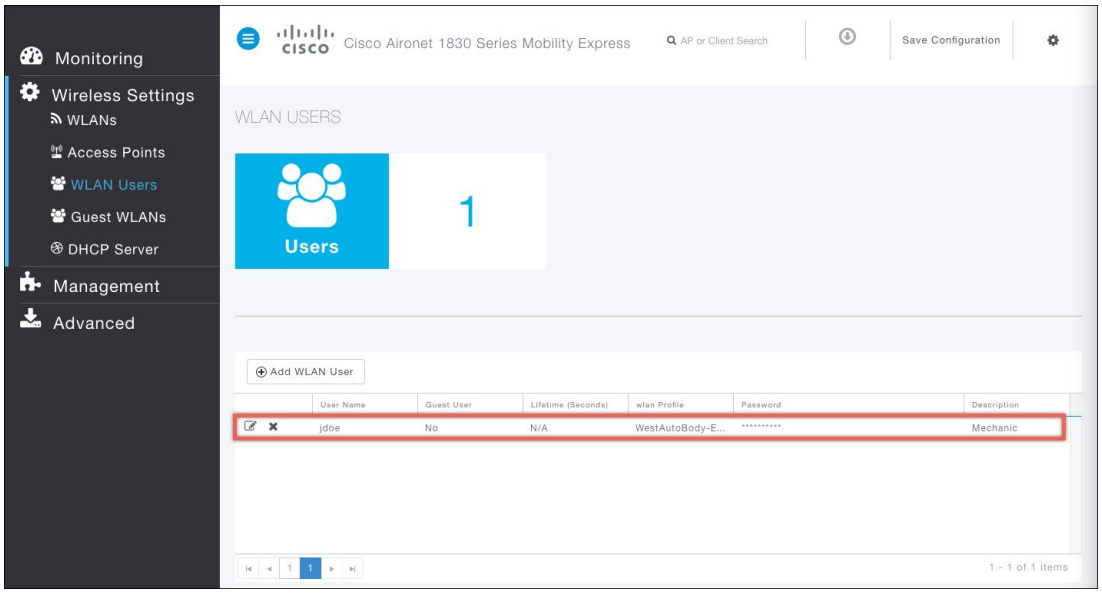
D. **WLAN Profile**—Select the WLAN that this user will connect

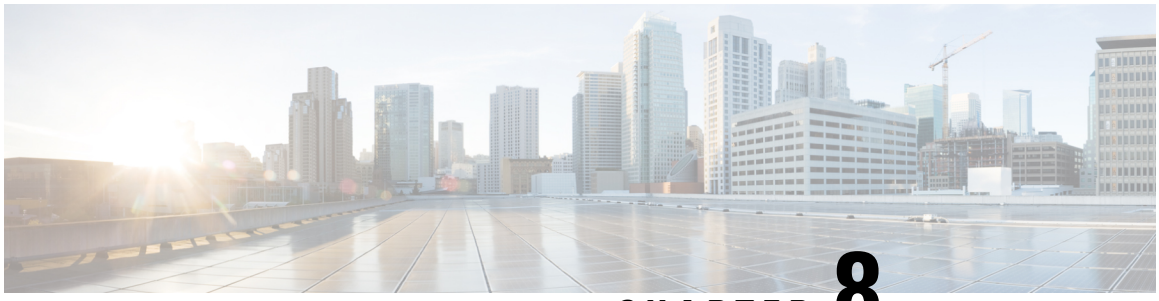
E. **Password**—Enter the password for the user account

F. **Description**—Additional details or comments on the user

G. Click on the icon pointed by the Red arrow to create the account







CHAPTER 8

Managing Access Points

Mobility Express supports a maximum of 25 Access points in a Mobility Express deployment.

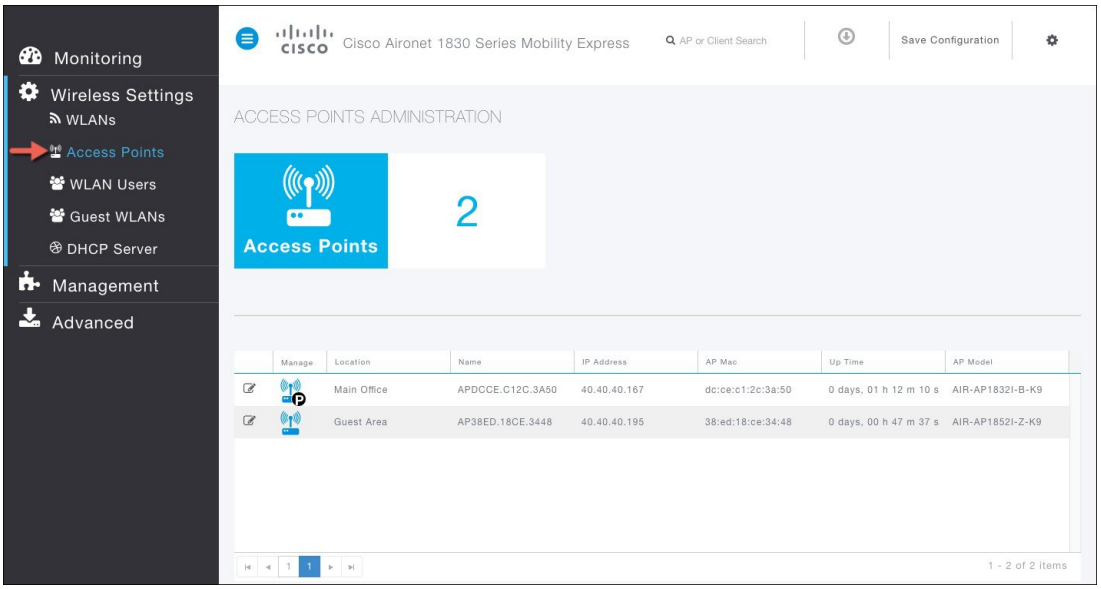
Managing Access Points

To view the list or modify Access Points associated with the Mobility Express controller, follow the steps below.

Procedure

Step 1 Navigate to **Wireless Settings** > **Access Points**.
The Access Point Administration page displays the count of access points and Access Point table with the associated APs.

Note The AP table will display 10 access points on the first page. If there are more than 10 access points, user has to go to the next page.



The first Access Point with the icon is the Primary AP and the rest of them are Subordinate APs. Please see figure below Primary AP and Subordinate AP.

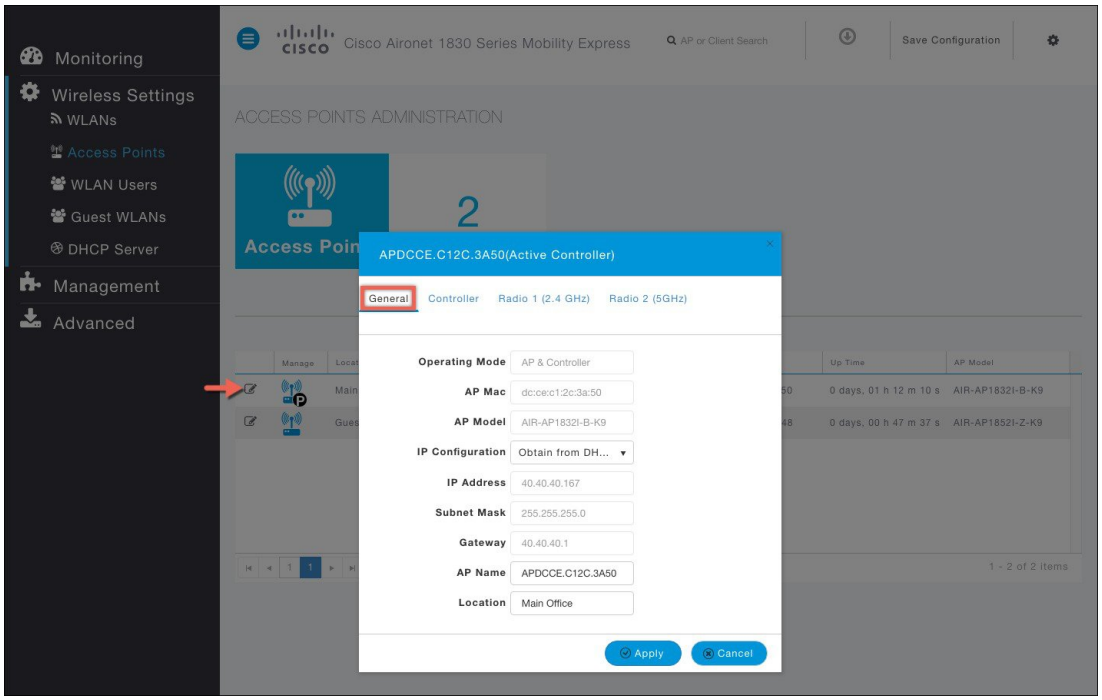
The Primary AP and Subordinate AP icons are as shown:

Figure 6: Primary AP Icon

Figure 7: Subordinate AP Icon

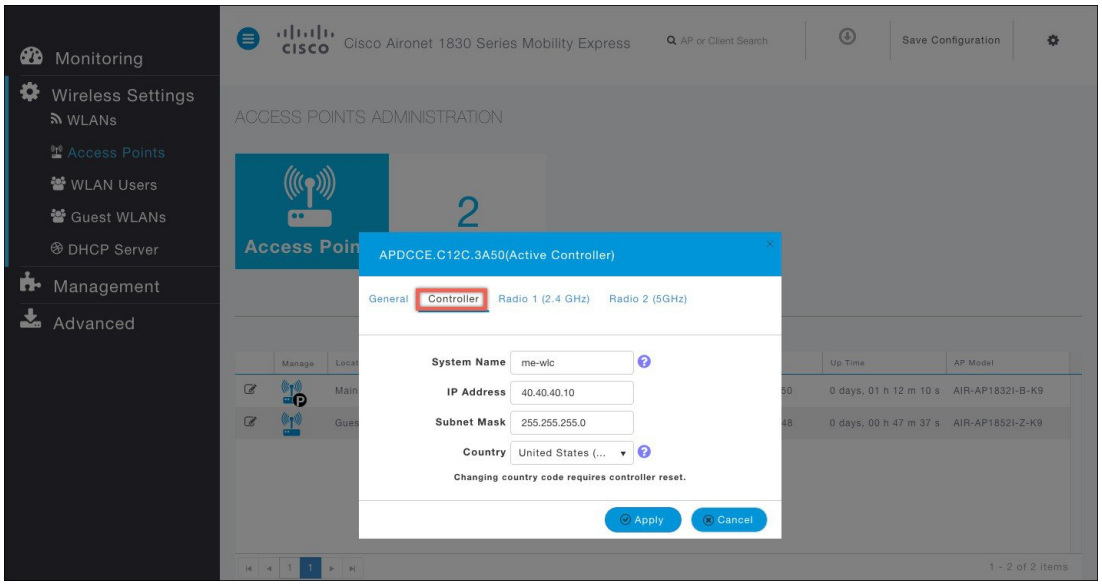
Step 2 To modify the parameters on an access point, click on the Edit button. The AP window will come up displaying the General parameters about the Access Point.

- **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 (Available only for Primary AP) tab, one can modify the following parameters:

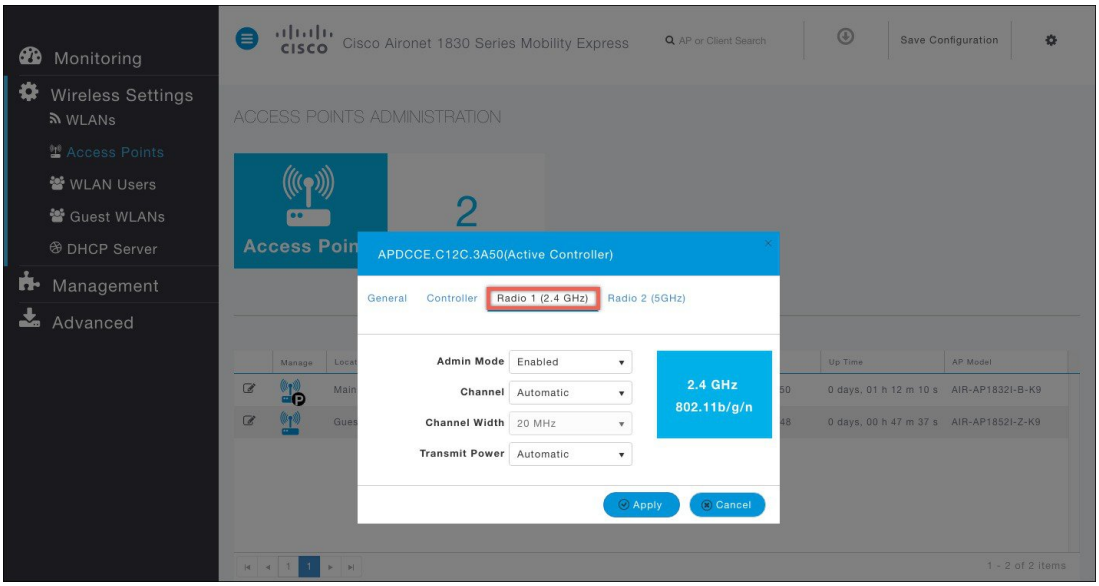
- **IP Address**—IP address decides the login URL to the controller's web interface. The URL is in *https://<ip address>* format. If you change this IP address, the login URL also changes.
- **Subnet Mask**
- **Country Code**



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** to save the changes.

Adding an Access Point to Mobility Express Network

When adding an access point to the Mobility Express network, the following have to be considered:

1. Software Version on the Access Point - If the software version of the access point, which is being added, is different than what is on the Primary AP, a software download of the code running on the Primary AP has to happen on the Access Point being added. For the new AP to download the code that is running on the Primary AP, one of the following has to be configured:
   - TFTP server and the AP file path information has to be configured on the Software Update page.
   - If the Primary AP has 8.3.102.0 or later code, one can configure the Cisco.com login credentials on the Software Update page and the code on the new AP will be automatically downloaded from cisco.com when an AP joins.

Note For Software download to take place directly from Cisco.com, the Primary AP should be the one with the SMARTNet Contract.

2. Is Access Point being added an 11ac Wave 2 or not?

   If the Access Point being added is an 11ac Wave 2 access point and is running Mobility Express image, it can be added to the Mobility Express network. If a software version is different, it will download the software version running on the Primary AP either from a configured TFTP server or directly from cisco.com. This AP will be capable of running the controller function if the Primary AP fails.

   If the Access Point being added is an 11ac Wave 2 Access point and is running CAPWAP image, it can be added to the Mobility Express network. If a software version is different, it will download the software version running on the Primary AP either from a configured TFTP server or directly from cisco.com. This AP will not be configured to run the controller function unless configured explicitly.

   If the Access Point being added is a non-11ac Wave 2 Access point, it can be added to the Mobility Express network as long as it is one of the supported AP for Mobility Express. If the software version is different, AP will download the software version running on the Primary AP either from a configured TFTP server or directly from cisco.com. This AP is not capable of running the controller function.

Note The Primary AP facilitates transfer of image from TFTP or Cisco.com to the new AP which is added.

Procedure

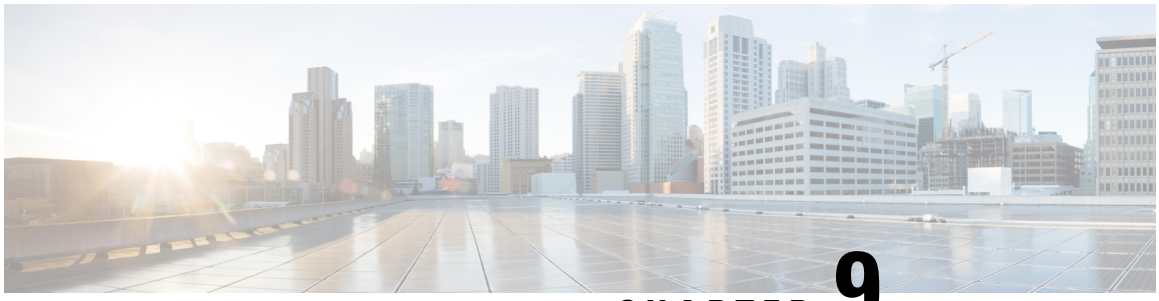
Step 1 Configure Cisco.com Login Credentials on the Primary AP, which has the SMARTNet Contract on **Software Update** (**Management > Software Update**) page.

OR

Download the **ap_bundle zip** file from cisco.com on a TFTP server. **The bundle version must be the same as the one running on the Master AP**. Unzip the file to extract the AP images. Configure TFTP Parameters on the **Software Update** (**Management > Software Update**) page.

Step 2 Connect the AP to the network. When the AP boots up, it obtains an IP address from the DHCP server. If the AP version matches the one on Primary AP, it joins. However, if the version on the AP being added is different than then one on the Primary AP, it starts to download the image from either the configured TFTP server or cisco.com. After the image download is complete, the AP will reboot and join the Primary AP.

Note During the image download there is no service interruption. After the image download is complete, the AP automatically re-boots and join the Primary AP.



CHAPTER 9

Managing the Mobility Express Network

Under the Management tab on the navigation pane, an admin users can do the following:

1. Configure access to the Mobility Express controller
2. Manage Admin Accounts
3. Configure Time
4. Perform a Software Update

Configuring Management Access

The Management Access Interface on the Mobility Express controller is the default interface for in-band management of the controller and connectivity to enterprise services. It is also used for communications between the controller and access points.

There are four types of Management Access supported on the Mobility Express controller.

1. HTTP Access-To enable HTTP access mode, which allows you to access the controller GUI using http://<ip-address> through a web browser, choose Enabled from the HTTP Access drop-down list. Otherwise, choose Disabled.

   The default value is Disabled. HTTP access mode is not a secure connection.

2. HTTPS Access-To enable HTTPS access mode, which allows you to access the controller GUI using http://ip-address through a web browser, choose Enabled from the HTTPS Access drop-down list. Otherwise, choose Disabled.

   The default value is Enabled. HTTPS access mode is a secure connection.

3. Telnet Access-To enable Telnet access mode, which allows remote access to the controller's CLI using your laptop's command prompt, choose Enabled from the Telnet Access drop-down list. Otherwise, choose Disabled.

   The default value is Disabled. The Telnet access mode is not a secure connection.

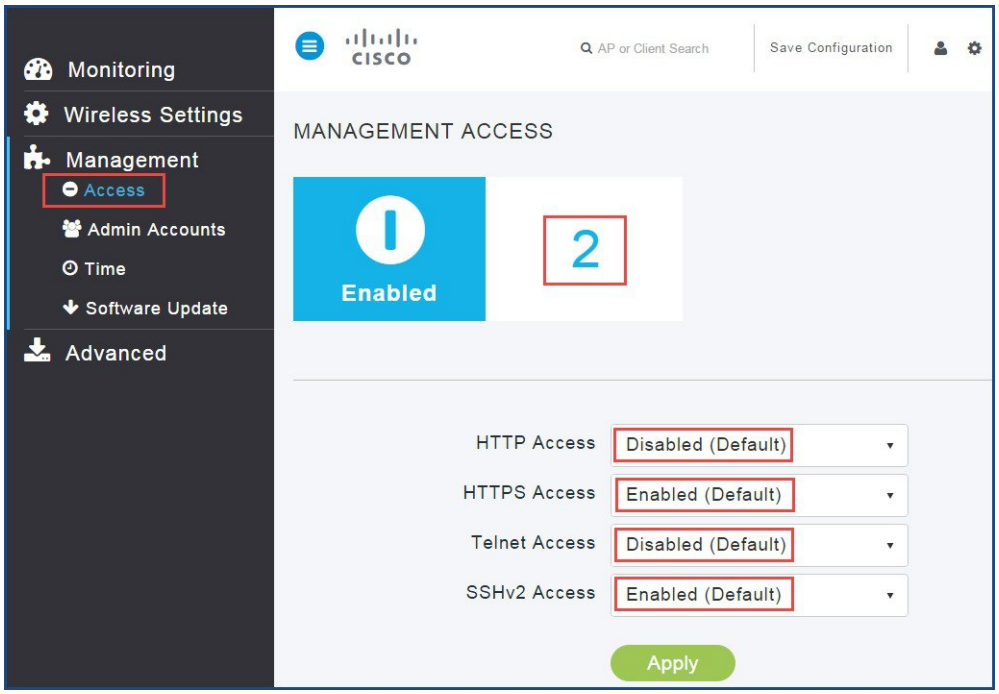
4. SSHv2 Access-To enable Secure Shell Version 2 (SSHv2) access mode, which is a more secure version of Telnet that uses data encryption and a secure channel for data transfer, choose Enabled from the SSHv2 Access drop-down list. Otherwise, choose Disabled.

   The default value is Enabled. The SSHv2 access mode is a secure connection.

To enable or disable the different types of management access to the controller, do the following:

Procedure

Step 1 Navigate to **Management** > **Access**. The Management Access page is shown displaying the count of the access type which are enabled.



Step 2 For the various Access Types, select either Enabled or Disabled.

Note There must be at least one access enabled else admin user will locked out of Mobility Express Controller and will have to use console to make changes to provide access again.

Step 3 Click the Apply button to submit the changes.

Managing Admin Accounts

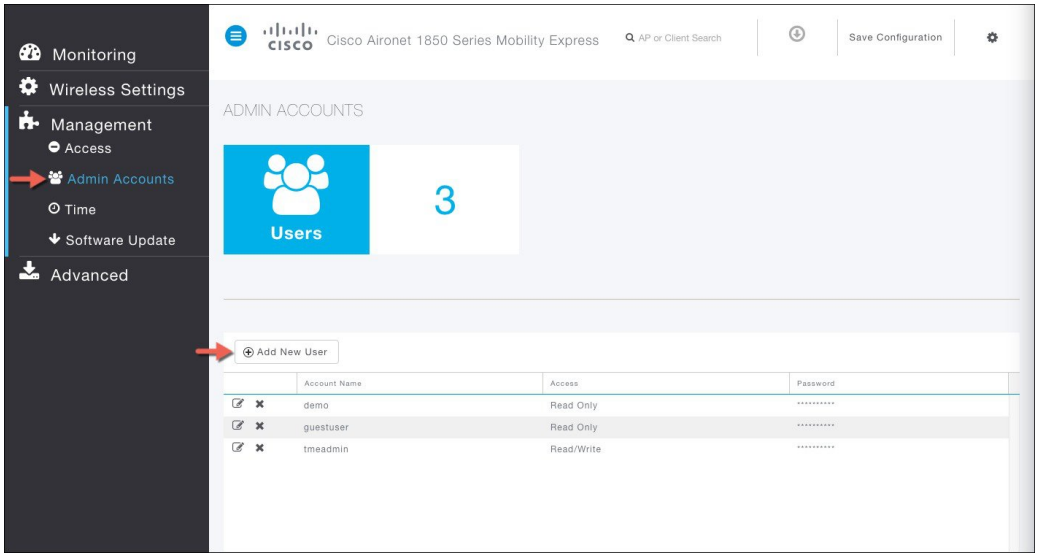
Cisco Mobility Express supports creation of admin usernames and passwords to prevent unauthorized users from reconfiguring the controller and viewing configuration information.

Admin user accounts are required for logging into Mobility Express controller to monitor and configure the wireless network. Admin accounts can be configured with Read/Write or Read only privileges.

To create these users, follow the steps below.

Procedure

Step 1 Navigate to **Management Admin Accounts** and click on the **Add New User** button.



Step 2 Enter the following to configure the admin user account.

a) **Account Name** - Enter the admin user name. Usernames are case-sensitive and can contain up to 24 ASCII characters. Usernames cannot contain spaces

Note Admin account name must be unique

b) **Access -** Select Read/Write or Read Only access for the admin account

- Read Only - This option creates an administrative account with read-only privileges. The admin user can only view the controller configuration but cannot make any changes to the configuration.
- Read/Write - This option creates an administrative account with read and writes privileges. The admin user can view and make changes to the controller configuration.

c) **New Password & Confirm Password** - Enter a password for the admin user account, in-keeping with the following rules:

- Passwords are case sensitive and cannot contain spaces
- The password should contain a minimum of 8 characters from ALL of the following classes:

  Lowercase letters

  Uppercase letters

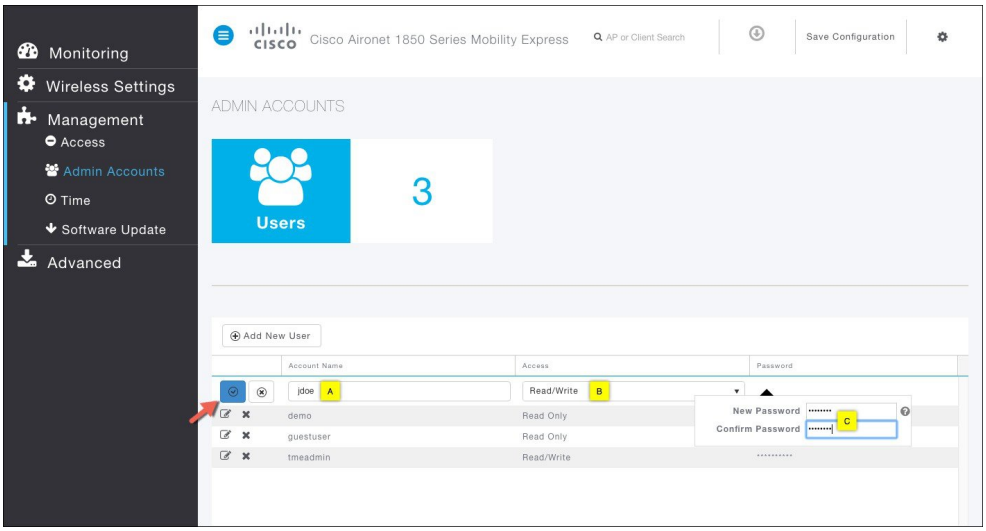
  Digits

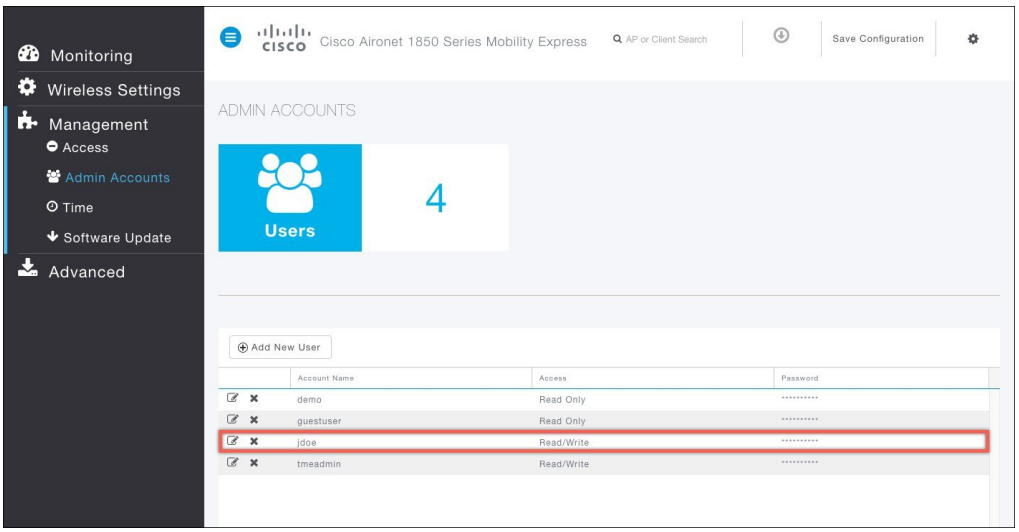
  Special characters

- No character in the password can be repeated more than three times consecutively.

- The password should not contain the word Cisco or a management username. The password should also not be any variant of these words, obtained by reversing the letters of these words, or by changing the capitalization of letters, or by substituting 1, |, or ! or substituting 0 for o or substituting $ for s.

d) Click on the icon pointed by the Red arrow to create the account.





Managing TIME on Mobility Express Controller

The system date and time on the Cisco Mobility Express controller is first configured when running the initial Wireless Express setup wizard.

A Network Time Protocol (NTP) server can be configured to sync date and time if one was not configured during the Wireless Express setup. Greenwich Mean Time (GMT) is used as the standard for setting the time zone on the controller.

Configuring NTP Server on Mobility Express Controller from GUI

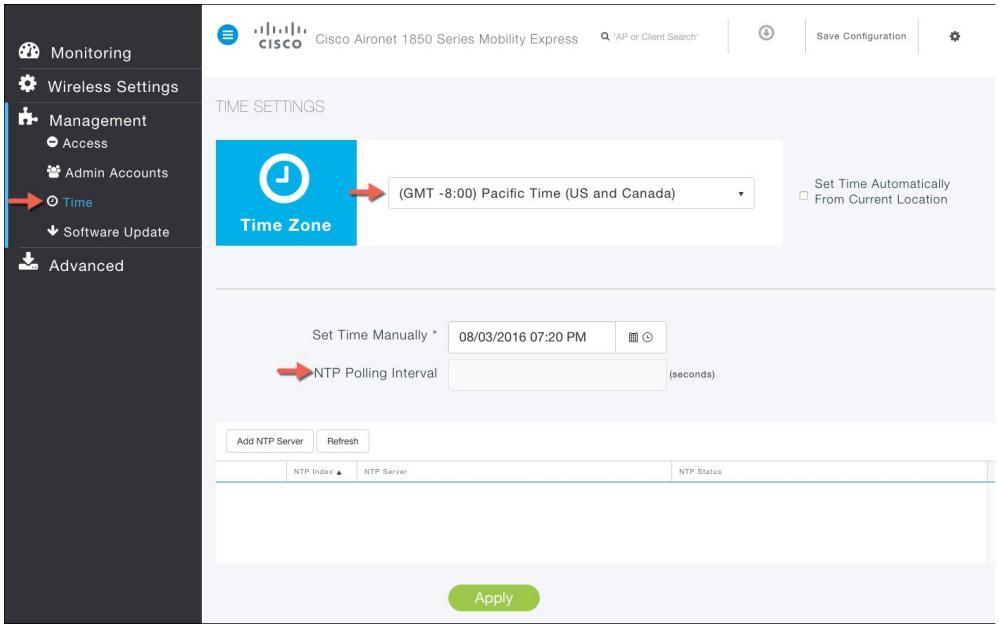
To configure an NTP server, perform the following steps:

Procedure

Step 1 Navigate to **Management** > **Time** from the left pane.

Step 2 Choose the desired **Time Zone** from the **Time Zone** drop down list.

Step 3 Enter the **NTP Polling Interval**. The polling interval ranges from 3600 to 604800 seconds.

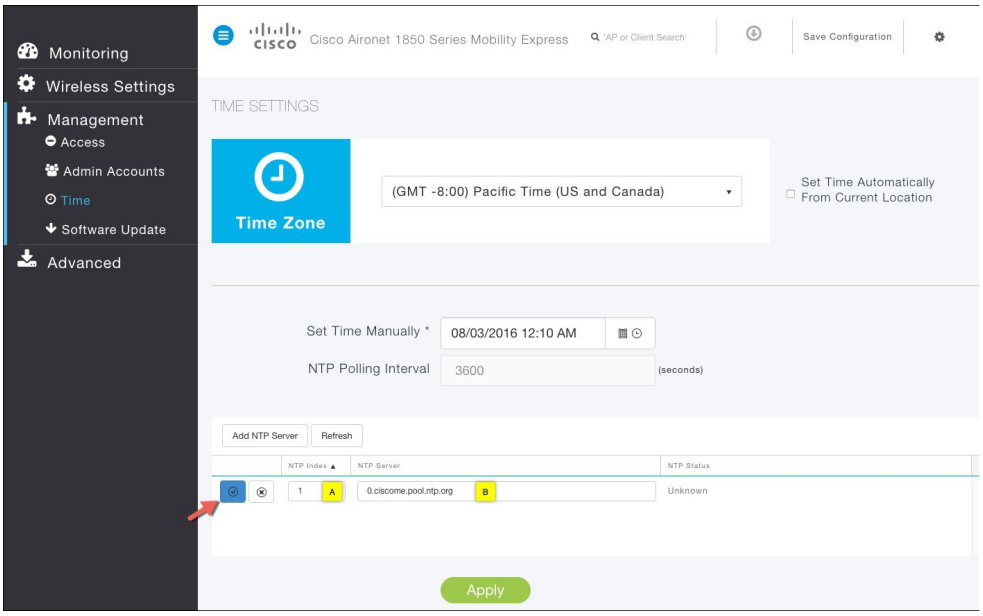


Step 4 To add an NTP server, click **Add NTP Server** button and configure the following:

- NTP Index
- NTP Server - This can be the NTP Server IP address, NTP Server Name or pool. A maximum of three NTP Servers are supported.

Step 5 Click on the icon pointed by the Red arrow to add the NTP Server.

Note Synchronization of the date and time with the NTP Server occurs each time the controller reboots and at each user-defined polling interval.



Step 6 Click on the **Apply** Button.

Configuring Date and Time manually on Mobility Express Controller from GUI

To configure Date and Time manually, follow the steps below.

Procedure

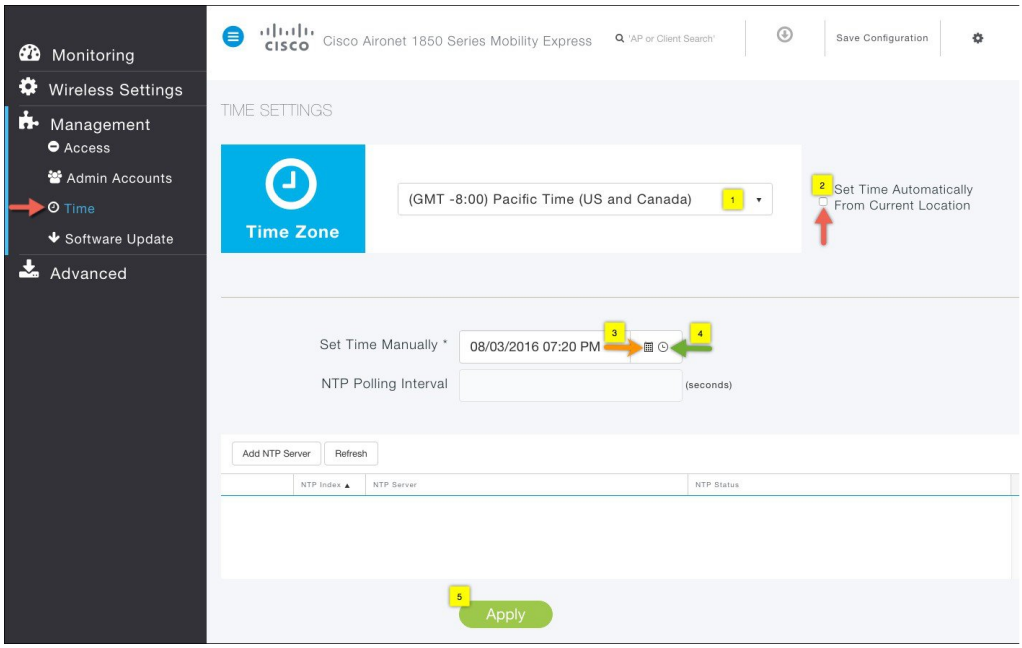
Step 1 Select the desired Time Zone from the drop down list.

Step 2 [Optional] Click the Set Time Automatically from Current Location check box, to adjust the time based on the Time Zone specified.

Step 3 Click on Date icon from Set Time Manually field and configure Date from the calendar.

Step 4 Click on Time icon from Set Time Manually field and configure time from the drop down list.

Step 5 Click the Apply button.



Updating Cisco Mobility Express Software

Cisco Mobility Express controller software update can be performed using the controller's web interface. Software update ensures that both the controller software and all the Access Points associated are updated. The Access Points that have older software are automatically upgraded to the Mobility Express software on joining the Primary AP. An AP joining the controller compares its software version with the Primary AP version and incase of mismatch, the new AP requests for a software upgrade. The Primary AP facilitates the transfer of the new software from the TFTP server to the new AP.

Software download on the Access Points is automatically sequenced to ensure that not more than 5 APs are downloading the software simultaneously and the queue refreshes till all the APs requiring upgrade have downloaded the new image.

Release 8.3.100.0 supports the following transfer modes for Software Update:

1. Cisco.com - Cisco.com transfer mode is introduced in 8.3.100.0. In this software update method, the software image can be directly streamed from cisco.com to the individual Access Points. Internet access required for this transfer mode and EULA and SMARTNet contract requirements have to be met for this transfer mode.
2. HTTP - HTTP transfer mode is supported if the Mobility Express Network has the same model of Access Points. Use HTTP as the transfer mode for Software Update using the AP file from a local machine.

Note If there is a mix of Access Points in the Mobility Express network, Software Update via cisco.com or TFTP must be used.

3. TFTP - TFTP transfer mode can be used to perform Software Update on a Mobility Express Network. Primary AP facilitates transfer of image from the TFTP server to the Subordinate APs. The AP images are stored and served from the TFTP server upon request.

Note

- There is no service interruption during pre-image download. After pre-image download is complete on all APs, a Manual or scheduled reboot of Mobility Express network can be triggered.
- After the pre-image download is initiated, no new AP that has a different version than the running controller will be able to join until it is fully upgraded and is running the new image.

Software Update via cisco.com

Software Update via Cisco.com works on all APs supported in a Cisco Mobility Express Deployment. Below requirements must be met to initiate a Software Update from cisco.com.

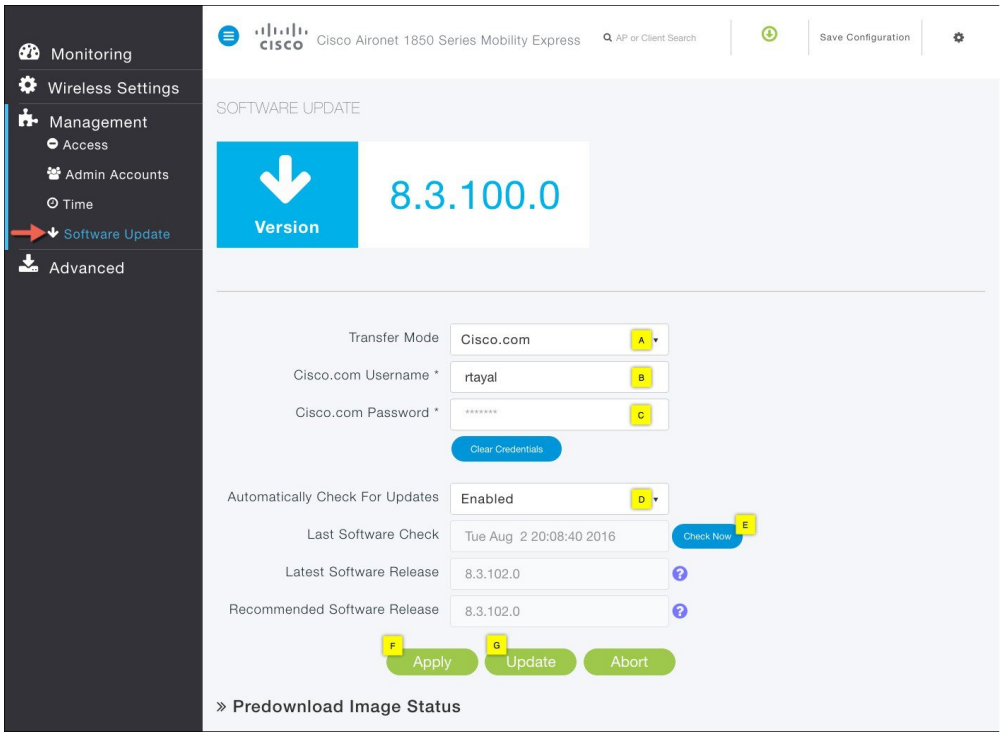
1. Internet access is required for software download from cisco.com to APs. However, no proxy is required.
2. A valid cisco.com (CCO) account with username & password required.
3. EULA Acceptance on a per user basis. Primary AP (not all APs in the network) must have SMARTNet contract else Software Update will not start.

Note Software Update from cisco.com is supported via GUI only.

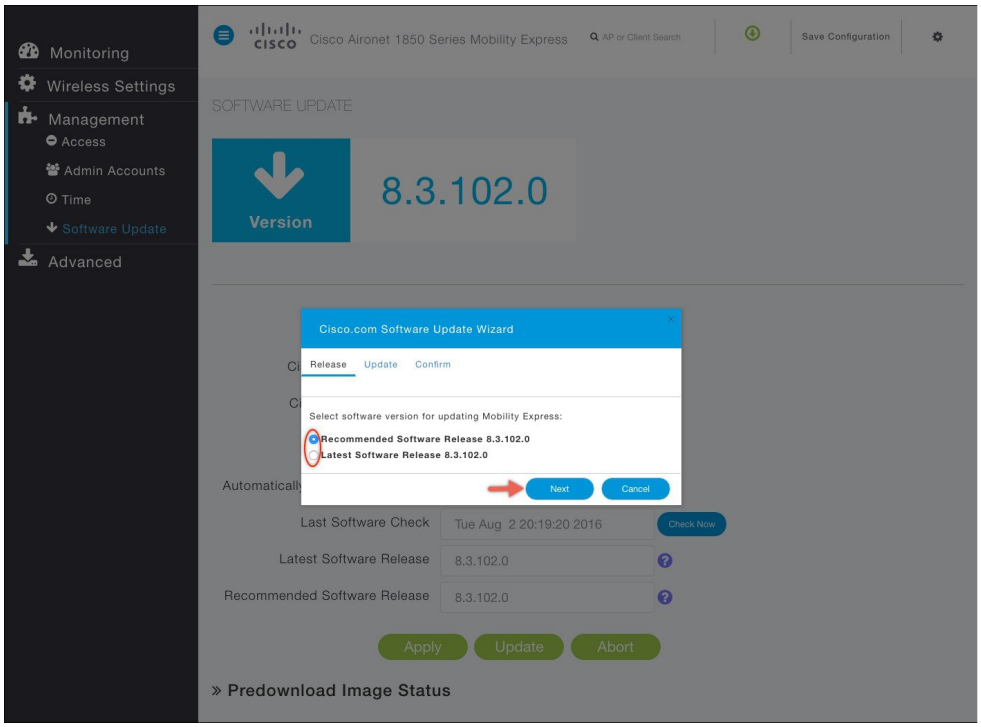
Procedure

Step 1 To perform Software Update via Cisco.com, navigate to **Management > Software Update** and perform the following:

a) For **Transfer Mode** select ***Cisco.com*** from the drop down list.
b) Enter Cisco.com Username.
c) Enter Cisco.com Password.
d) Enable **Automatically Check for Updates**. Check is done once in 30 days.
e) Click on the **Check Now** button to retrieve the Latest Software Release and the Recommended Software Release from Cisco.com.
f) Click on the **Apply** Button
g) Click on **Update** button to initiate software update

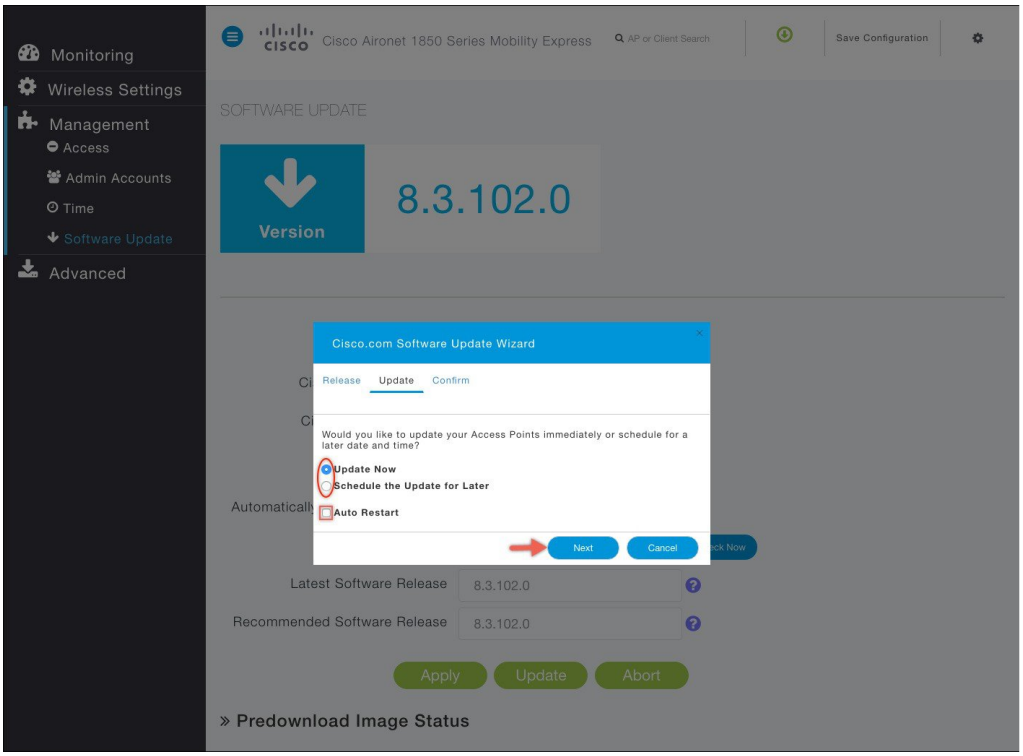


h) In the Software Update Wizard, select the Recommended Software Release or Latest Software Release. Click on the **Next** Button.

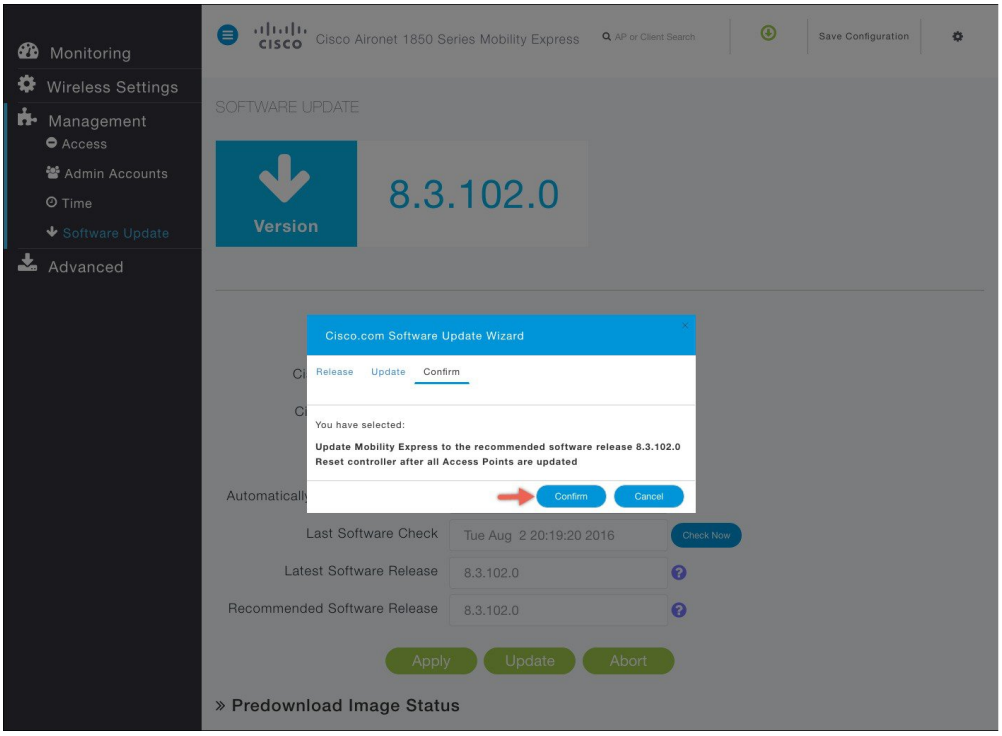


i) Select **Update Now** to initiate software update immediately or **Schedule the Update for Later**. If **Schedule the Update for Later** is selected, configure the **Set Update Time** field.

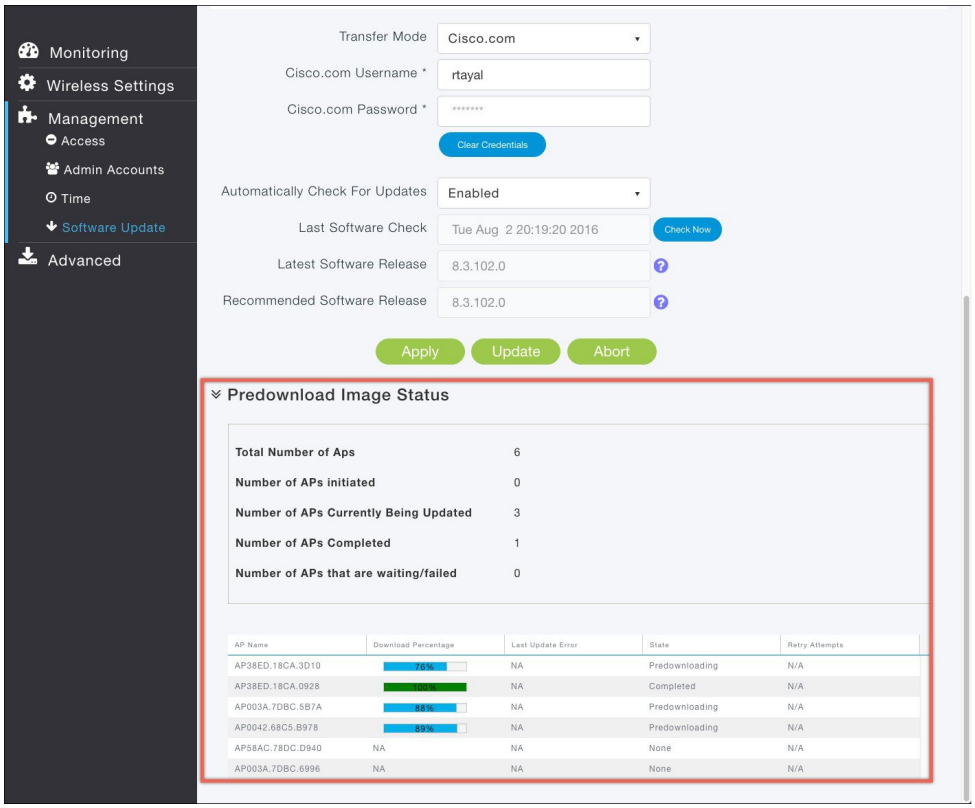
j) Click on the Auto Restart checkbox if automatic restart of all access points in the network is desired after the software update is finished. Click on the **Next** button.



k) Click on **Confirm** button to start the software update.



Step 2 To view the download status, expand the Predownload image status.



Software Update via HTTP

Procedure

Step 1 Download the AP Image bundle from cisco.com to the local machine.

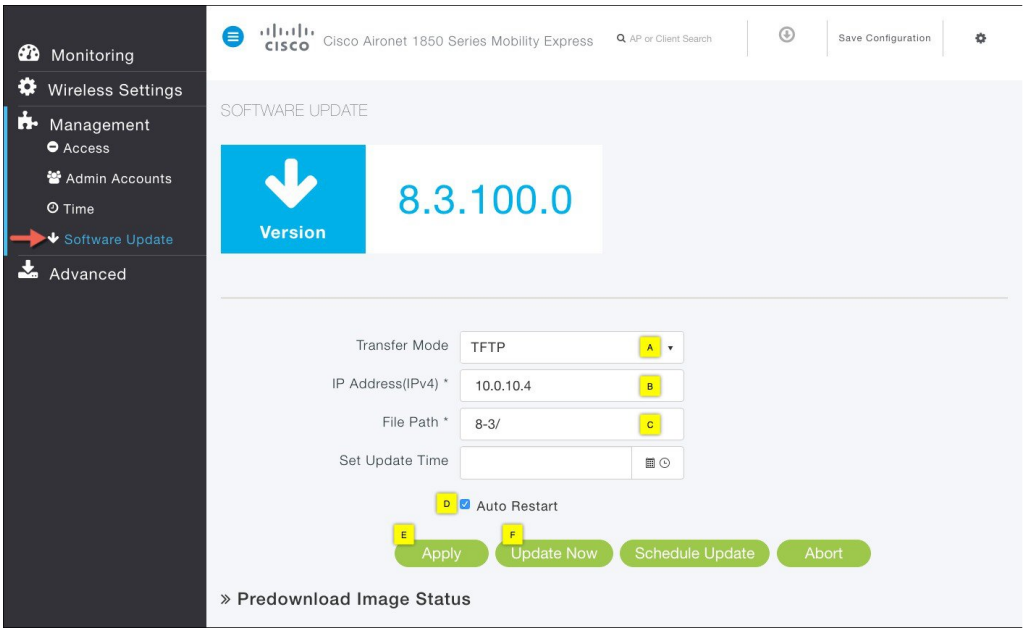
Step 2 Unzip the AP Image bundle to extract individual AP Images. Mapping of Access Points to their corresponding images is shown below.

AP Model	AP Image
AIR-AP1830	ap1g4
AIR-AP1850	ap1g4
AIR-AP2800	ap3g3
AIR-AP3800	ap3g3

Step 3 To perform Software Update via HTTP, navigate to **Management > Software Update** and perform the following:

a) For **Transfer Mode** select ***HTTP*** from the drop down list.

b) Browse to the local AP image, corresponding to the Access Point in your network.
c) Click on the Auto Restart checkbox if automatic restart of all access points in the network is desired after the software update is finished.
d) Click on the Apply Button.
e) Click on Update now to initiate software update.



Step 4 To view the download status, expand the Predownload image status.

Software Update via TFTP

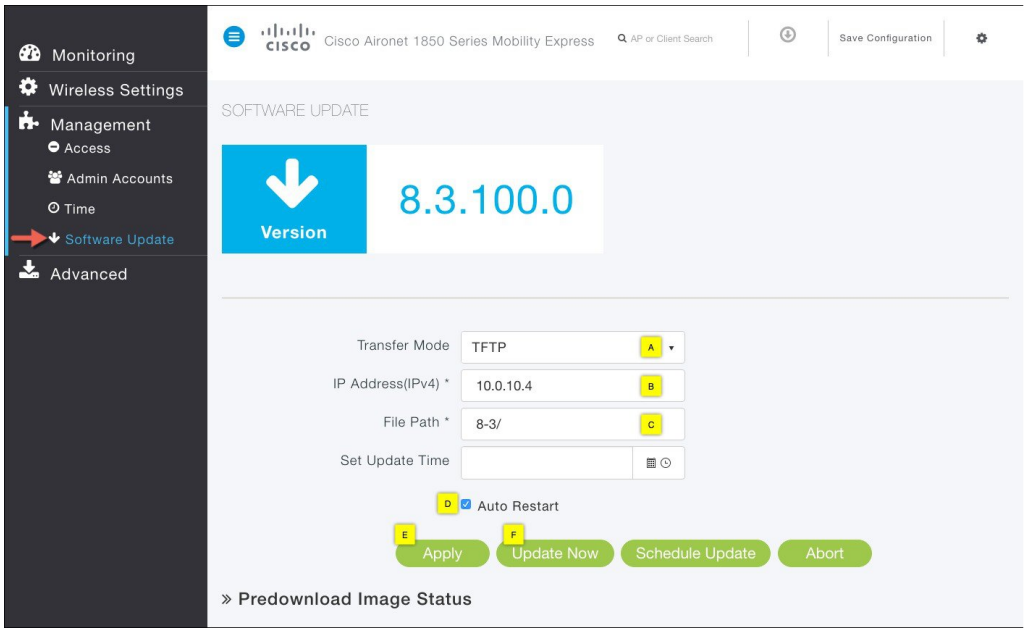
Procedure

Step 1 Download the AP Image bundle from cisco.com to the TFTP server.

Step 2 Unzip the AP Image bundle to extract individual AP Images.

Step 3 To perform Software Update via TFTP, navigate to **Management > Software Update** and perform the following:

a) For **Transfer Mode** select ***TFTP*** from the drop down list.
b) Enter the IPv4 address of the TFTP server in the **IP Address (IPv4)** field.
c) Enter the **File Path** to the unzipped AP images on the TFTP Server.
d) Click on the Auto Restart checkbox if automatic restart of all access points in the network is desired after the software update is finished.
e) Click on the Apply Button.
f) Click on **Update Now** to initiate software update. To Schedule Update at a later time, configure the **Set Update Time** and click on the **Schedule Update** button.



Note For schedule later, user must select a date and time in the future and then click on Schedule Later. Button. It is recommended that the Set Reboot Time should be at least 2 hours from the time pre-image download was initiated. This will ensure that pre-image download on all Access Points in the Mobility Express Network has completed.

Step 4 To view the download status, expand the Predownload image status.

Upgrading Cisco Mobility Express network via TFTP from the CLI

Procedure

Step 1 Login to AP running Mobility Express controller via Telnet or SSH.

Step 2 Specify the datatype.

```
(Cisco Controller) >transfer download datatype ap-image
```

Step 3 Specify the transfer mode.

```
(Cisco Controller) >transfer download ap-images mode tftp
```

Step 4 Specify the IP address of the TFTP server.

```
(Cisco Controller) >transfer download ap-images serverIp <IP addr>
```

Step 5 Specify the path of the AP images on the TFTP server.

```
(Cisco Controller) >transfer download ap-images imagePath <path to AP images>
```

Note For pre-image download to be successful make sure path to the AP images is correct

Step 6 Start pre-downloading of the image on the APs.

```
(Cisco Controller) > transfer download start
Mode..................................... TFTP
Data Type................................ ap-image
TFTP Server IP........................... 10.1.1.77
TFTP Packet Timeout...................... 10
TFTP Max Retries......................... 10
TFTP Path................................ ap_bundle_8.1.112.30/
This may take some time.
Are you sure you want to start? (y/n) y
TFTP Code transfer starting.
Triggered APs to pre-download the image.
Reboot the controller once AP Image pre-download is complete
```

Step 7 Check the pre-download status by executing the CLI below.

```
(Cisco Controller) >show ap image all

Total number of APs.............. 3
Number of APs
       Initiated.......................1
       Predownloading..................2
       Completed predownloading..........0
       Not Supported.....................0
       Failed/BackedOff to Predownload...0

                    Primary    Backup  Predownload Predownload Next Retry  Retry Failure
AP Name               Image     Image     Status      Version    Time      Count Reason
--------------   ----------  ---------  --------    ---------   -------   ----  -----
AP6412.256e.0e78 8.1.112.21  8.1.112.21 Predownloading   --       NA       NA
APAOEC.F96C.D640 8.1.112.21  8.1.112.21 Predownloading   --       NA       NA
3600-gemini   8.1.112.21  8.1.112.21 Predownloading   --          NA
```

Step 8 Wait for the pre-image download to complete on the APs.

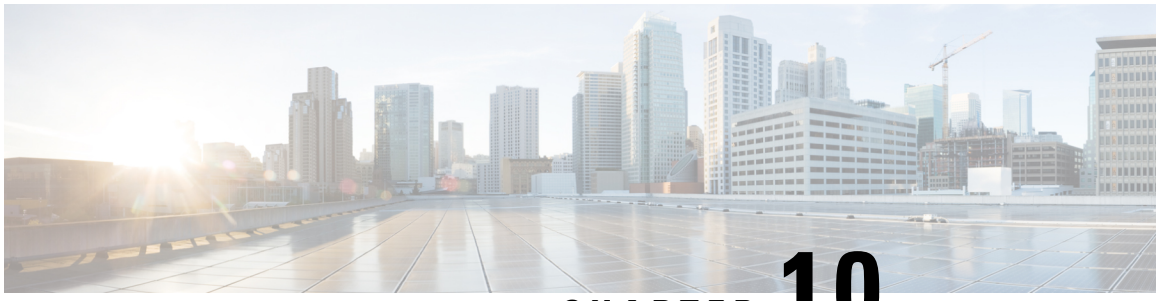
```
(Cisco Controller) >show ap image all
Total number of APs.............. 3
Number of APs
       Initiated.......................1
       Predownloading..................2
       Completed predownloading..........0
       Not Supported.....................0
       Failed/BackedOff to Predownload...0

                     Primary    Backup  Predownload Predownload Next Retry Retry Failure
AP Name               Image     Image     Status      Version    Time      Count Reason
 --------------   ----------  ---------  --------    ---------   -------   ----  -----
AP6412.256e.0e78 8.1.112.21  8.1.112.21 Complete     --          NA        NA
APAOEC.F96C.D640 8.1.112.21  8.1.112.21 Complete     --          NA        NA
3600-gemini   8.1.112.21  8.1.112.21 Complete   --              NA
```

Step 9 After the pre-download is complete, issue a reset system as shown below. This will cause a reboot of the Cisco 1850 running Mobility Express followed by rest of the APs.

```
(Cisco Controller) > reset system
  The system has unsaved changes.
  Would you like to save them now? (y/n)y
  Configuration Saved!
  System will now restart!
```

Step 10 Log back in the Mobility Express and check the version under Primary Image. It will show the new version and the Backup Image will show the previous version.



CHAPTER 10

Using Advanced Settings

SNMP

Simple Network Management Protocol is a protocol for network management. It is used for collecting information from, and configuring, managing all the devices in the network.

Cisco Mobility Express supports SNMP Version 2 and SNMP Version 3. Both SNMP v2c and v3 are enabled by default. SNMP Version 1 is also supported on Mobility Express but enabling and disabling on SNMP Version 1 is available in CLI only.

Managing SNMP Version 2c

Procedure

Step 1 Navigate to **Advanced>SNMP**. The SNMP Setup screen will be displayed supported version.

Step 2 SNMPv2 Access - To enable, choose Enabled from the drop-down list. The default is Disabled.

Step 3 Read-Only Community - To configure the SNMP community with read-only privileges, in the Read -Only Community field enter a name for the community. The default is *public*.

Step 4 Read-Write Community - To configure an SNMP community with read-write privileges, in the Read -Write Community field enter a name for the community. The default is *private*.

Step 5 SNMP Trap - To enable the SNMP Trap Receiver tool, which receives, logs, and displays SNMP traps sent from network, choose Enabled from the SNMP Trap drop-down list. The default is *Disabled*

Step 6 SNMP Server IP - To connect to an SNMP server, enter the IP address of the server in the SNMP Server IP field.

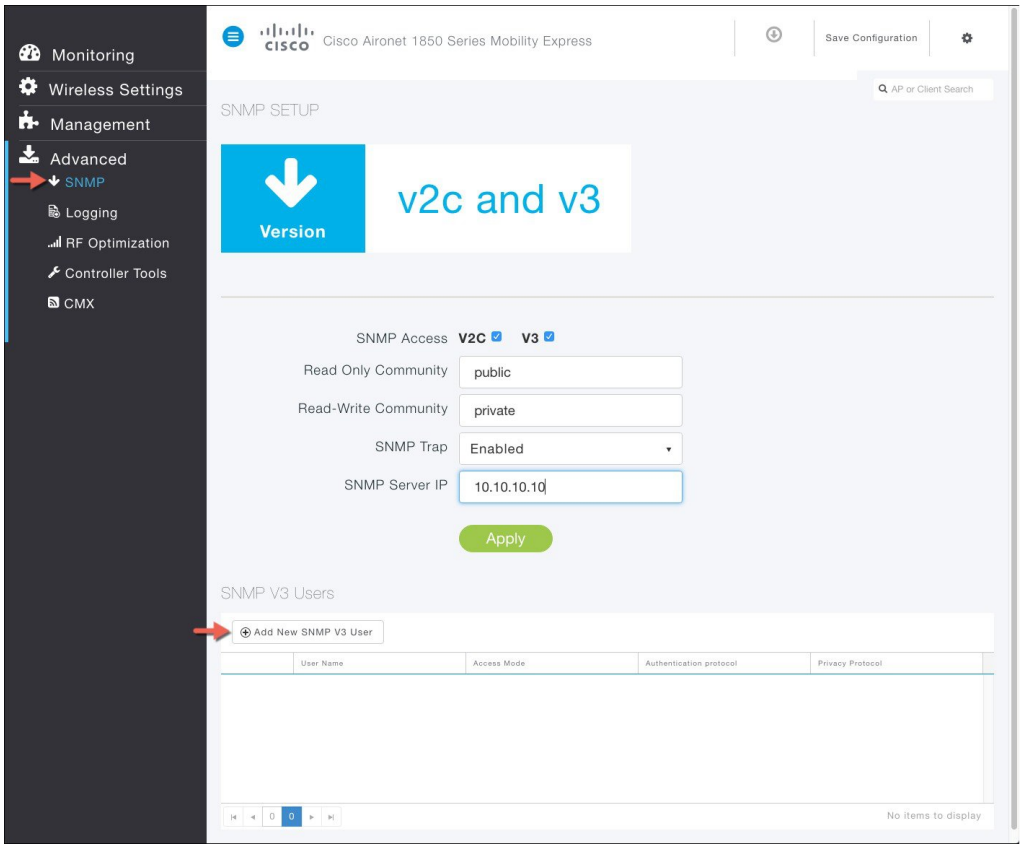
Step 7 Click the **Apply** button to submit the changes.

Managing SNMP Version 3 users

Procedure

Step 1 Navigate to **Advanced>SNMP**. The SNMP Setup screen will be displayed supported version.

Step 2 Click on **Add New SNMP V3 User** button.



Step 3 Enter the following parameters for the user:

A. Username

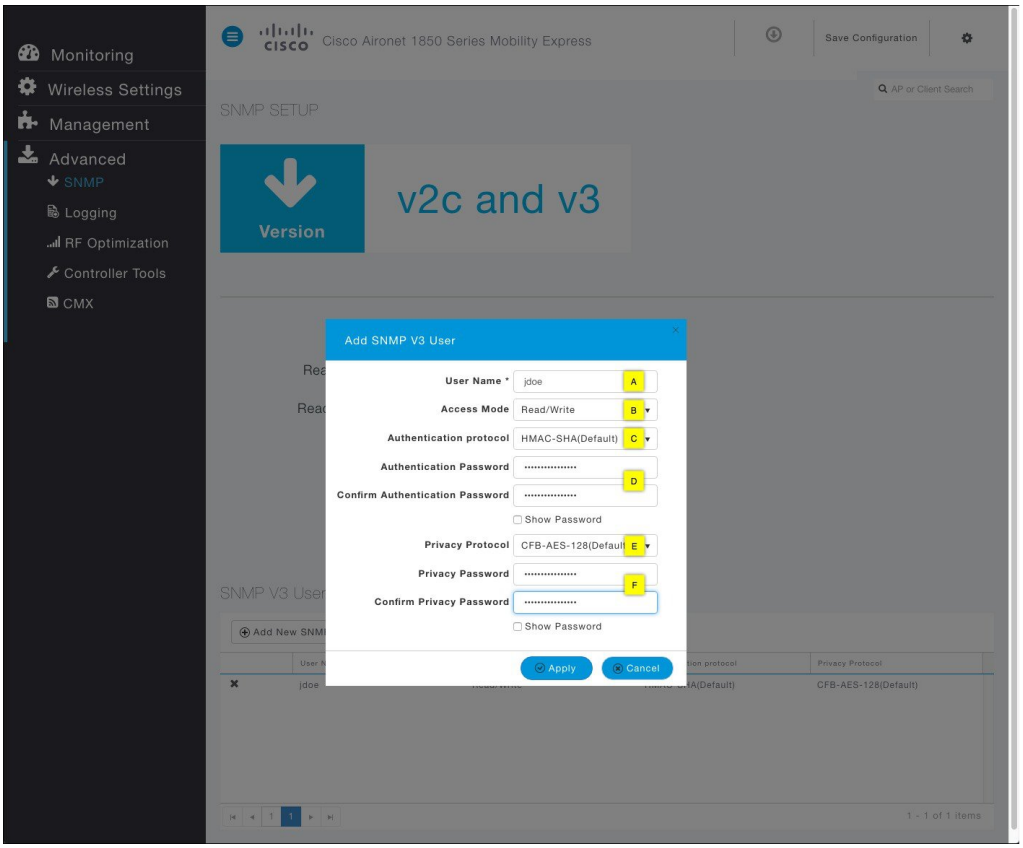
B. Access Mode

C. Authentication Protocol

D. Authentication Password and Confirm Authentication Password

E. Privacy Protocol

F. Privacy Password and Confirm Privacy Password



Step 4 Click on the Apply button and save the configuration.

Logging

The System Message logging feature logs the system events to a remote server, called a Syslog server. Each system event triggers a Syslog message containing the details of that event.

If the System Message logging feature is enabled, the controller sends a syslog message to the syslog server configured on the controller.

To configure Logging on Cisco Mobility Express, follow the procedure below.

Procedure

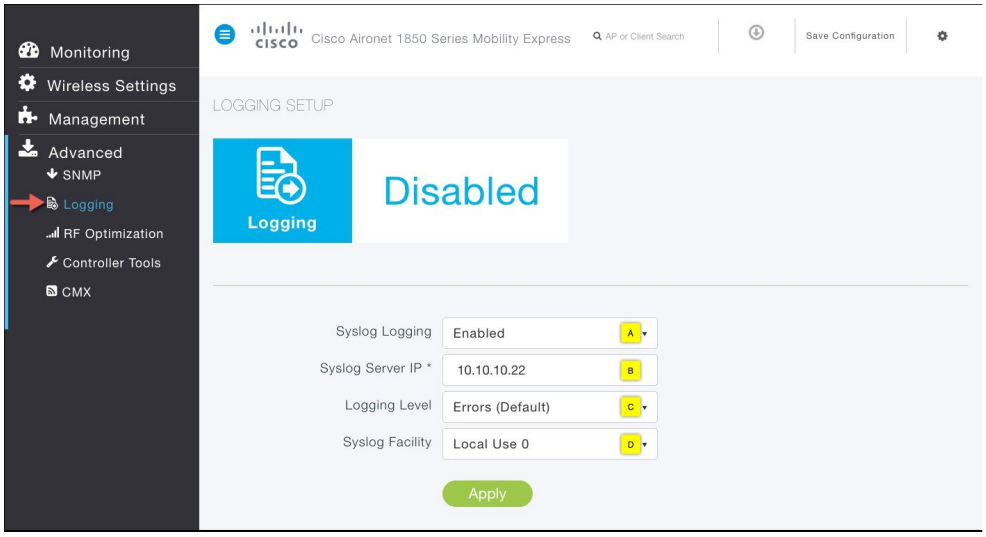
Step 1 Navigate to Advanced > Logging. The Logging Setup screen will be displayed. Configure the following Logging Parameters.

A. Syslog Logging - To enable Syslog Logging, choose Enabled from the Syslog Logging drop down list. The default is Disabled.

B. Syslog Server IP - In the Syslog Server IP field, enter the IPv4 address of the syslog server

C. Logging Level - In the Logging Level drop-down list, select the syslog severity level

D. Syslog Facility - In the Syslog Facility drop-down list, select the syslog severity level



Step 2 Click the Apply button to submit the changes.

RF Optimization

RF Optimization has control knobs for Client Density and Traffic Type in the Mobility Express deployment. Typically, RF Optimization is enabled and Client Density and Traffic Type is configured during the initial Setup Wizard when deploying Cisco Mobility Express. However, it can modified by following the steps below.

Procedure

Step 1 To modify RF Optimization Parameters, navigate to **Advanced > RF Optimization**.

Step 2 Move the slider as per the Client Density in your deployment.

Step 3 Make the Traffic Type selection from the drop down list as per your deployment.

Step 4 Click on the Apply button and the save the configuration.

Controller Tools

The Controller Tools enables admin users to Restart the controller, clear the controller configuration and set the Mobility Express network to Factory Default, and Export and Import Controller configuration files.

Restart Controller

Procedure

Step 1 To Restart the Controller, navigate to **Advanced > Controller Tools**.

Step 2 Click on the Restart Controller button.

Step 3 Click Yes on the Restart Controller window.

Note Since you chose to reset the active Primary AP which is running the controller function, upon reset, a new Primary AP will be elected as a Primary. During the reset, AP will fall back to Standalone mode and will continue to service clients. No new clients can be on-boarded until a new Primary AP is elected and the Standalone APs go back to Connected Mode.

Clear Controller Configuration

You can change the Mobility Express network to its default configuration by clearing the controller configuration and performing Reset to Factory Default.

Note

- This operation must be performed by an Admin user. You cannot restore the previous configurations.
- Performing Reset to Factory Default using GUI deletes the controller configuration from all the Mobility Express capable Access Points which is followed by a reboot of the Primary AP. After the reboot, all Mobility Express capable Access Points will broadcast the ***CiscoAirProvsion*** SSID.

Procedure

Step 1 Navigate to Advanced > Controller Tools.

Step 2 Click on Clear Controller Configuration.

Step 3 Click Yes on the Clear Controller Configuration window.

Export and Import of Controller Configuration File

One can export or import Mobility Express controller configuration file. To export the active controller configuration file, follow the steps below:

Exporting Controller Configuration File

Procedure

Step 1 Navigate to Advanced > Controller Tools.

Step 2 Click on the Export Configuration Button.

Step 3 Click Yes on the Export Configuration window.

Note It may take up to a minute to generate the configuration file before you see it being saved to your local device.

Importing Controller Configuration File

Procedure

Step 1 Navigate to Advanced > Controller Tools.

Step 2 Click on the Import Configuration Button.

Step 3 In the Import Configuration window, click on the Choose File button and browse to the configuration file on your local device.

Step 4 Click the Yes button to initiate the HTTP upload of the configuration file. You will see import status messages being displayed on top of the window.

Note After the configuration file is imported, System will be reset.

Export of Logs, core and crash files

Cisco Mobility Express provides a simplified way to collect and bundle all the necessary files for TAC. This bundle can then be transferred to a TFTP or FTP server.

The following files are collected from the Controller:

- ap-crash-data—Upload the ap-crash files.
- config—Upload the system's configuration file.
- coredump—Upload the system's Core Dump.
- crashfile—Upload the system's crash file.
- debug-file—Upload the system's debug log file
- run-config—Upload the controller's running configuration
- systemtrace—Upload the system's trace file.
- traplog—Upload the system's msglog and traplog collected before previous system reset.
- errorlog—Upload the system's error log.
- radio-core-dump—Upload the ap-radio core dump files

The following files are collected from an Access Point:

- show tech-support
- /var/log/messages
- /var/log/messages.0
- /var/log/crash_log
- /storage/base_capwap_cfg_info
- /storage/config.*
- /proc/meminfo
- /proc/*/status

To generate the bundle with the files, follow the steps below:

Procedure

Step 1 Set the data-type to support-bundle.

(Cisco Controller) >transfer upload datatype support-bundle

Step 2 Set the transfer upload mode to tftp or ftp.

(Cisco Controller) >transfer upload mode tftp

Step 3 Set the Set the TFTP ***server ip*** .

(Cisco Controller) >transfer upload serverip <server ip>

Step 4 Set the ***path*** on TFTP server.

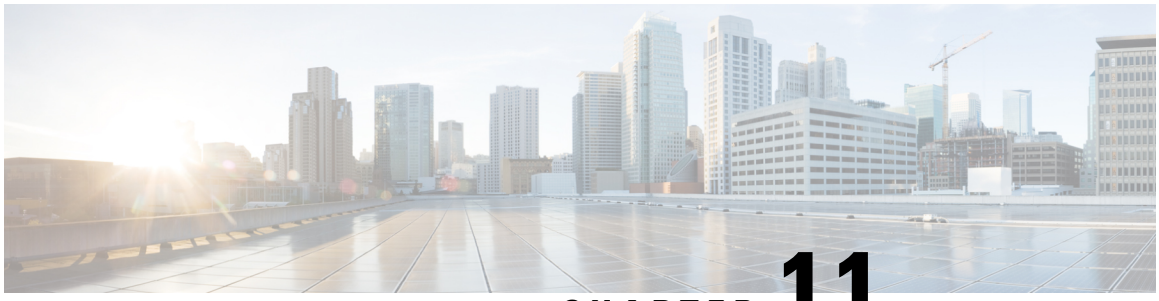
(Cisco Controller) >transfer upload path <tftp path>

Step 5 Set the ***file name***.

(Cisco Controller) >transfer upload filename <file name>

Step 6 Initiate the transfer.

(Cisco Controller) >transfer upload start



CHAPTER 11

Primary AP Failover and Electing a New Primary

Cisco Mobility Express is supported on Cisco 1830, 1850, 2800 and 3800 series Access Points and the Primary AP election process determines which Cisco of the supported Access Point will be elected to run Mobility Express controller function in case of a Failover. VRRP is used to detect a failure of Primary AP and to elect 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 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.

Primary Election

The Primary election process is based on a set of priorities. An AP with the highest priority is elected as the Primary AP, running Mobility Express controller function.

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.

The Primary AP election priorities are as follows:

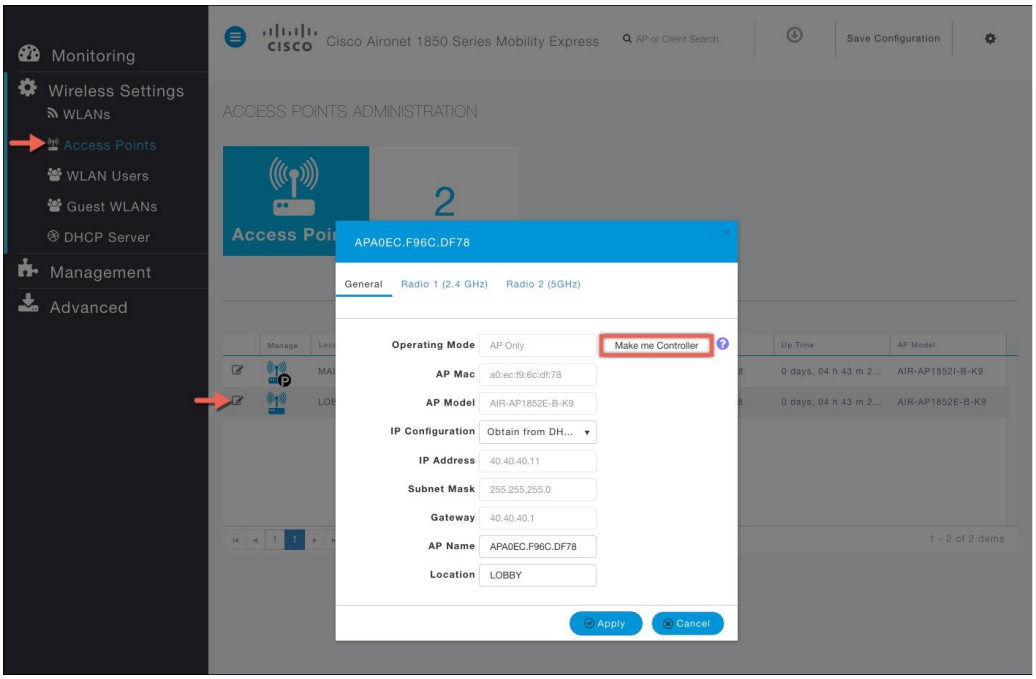
1. **User Defined Primary**—User can select an Access Point to be the Primary Access Point. If such a selection is made, no new Primary will be elected in case of a reboot of the Primary Access Point. After five minutes, if the current Primary is still not active, it will be assumed dead and Primary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

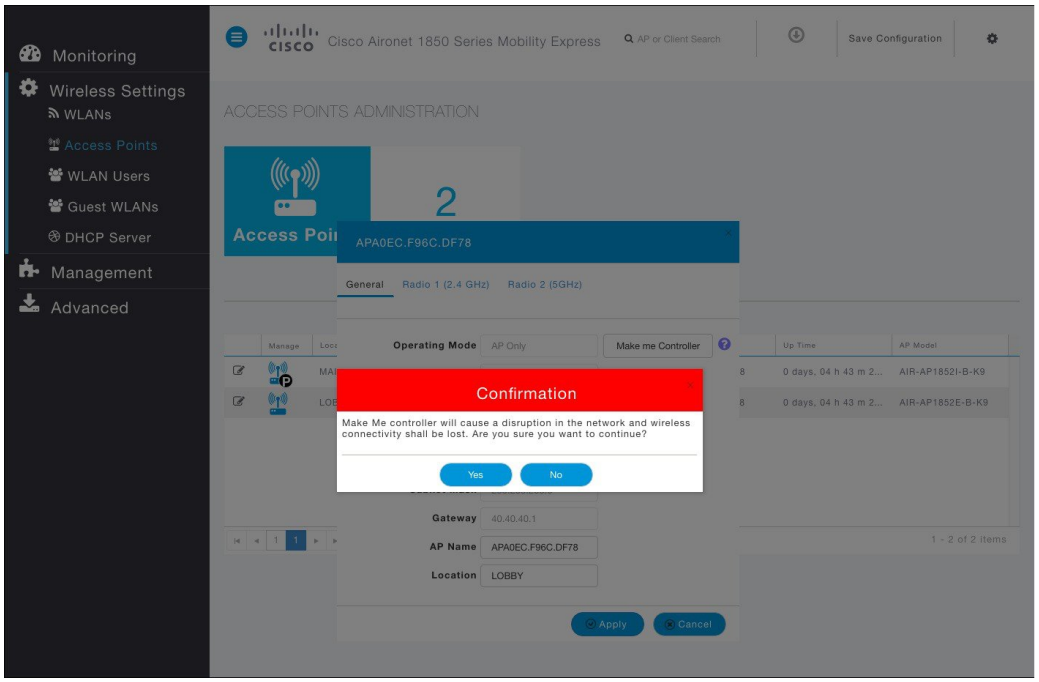
   Step 1: Navigate to **Wireless Settings > Access Points**.

   Step 2: From the list of Access Points, click **Edit** icon of the Access Point which you would like to define as the Primary AP.

   Step 3: Under the General tab, click **Make me Controller** button.

   Step 4: Click Yes on the Confirmation window.





Note

To clear the user defined priority, login to the Controller CLI and execute the following command:

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

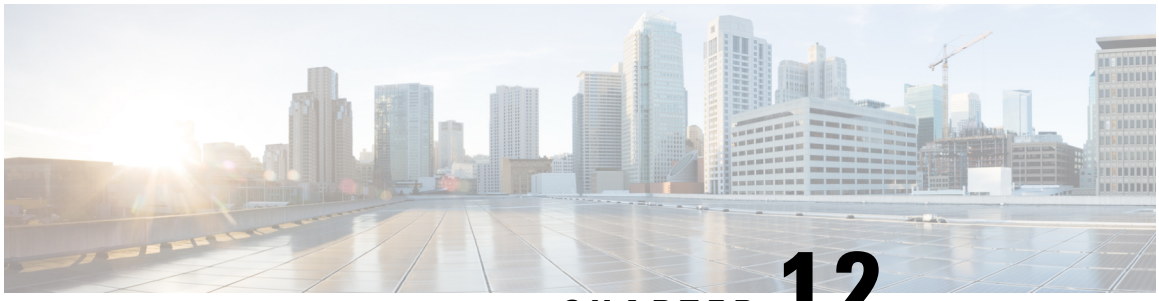
If a preferred Primary AP has to be elected incase of a failover, the following command can be entered on the controller CLI to define the preferred Primary.

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

To view the preferred Primary, use the following command:

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

2. Most capable Access Point - If the user priority is not set, Primary AP Election algorithm will select the new Primary based on capability of the Access Point. For example, 3800 is the most capable followed by 2800 and then 1850 and finally 1830.
3. Least Client Load— If there are multiple Access Points with the same capability i.e. multiple 3800 Access points, the one with least client load is elected as the Primary AP.
4. Lowest MAC Address—If the User defined priority is not configured and everything else is the same, then Access Point with the lowest MAC gets elected as the Primary AP.



CHAPTER 12

Cisco Mobility Express with Cisco 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
- All Cisco Mobility Express supported Access Points

Minimum requirements for 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 to https://cmxcisco.com for 60 day trial or go to Cisco Commerce Workspace (CCW) and purchase license for your choice of CMX Cloud service. Refer to CMX Cloud Ordering information.

   After sign-up, start using Connect or Connect and Presence Analytics.

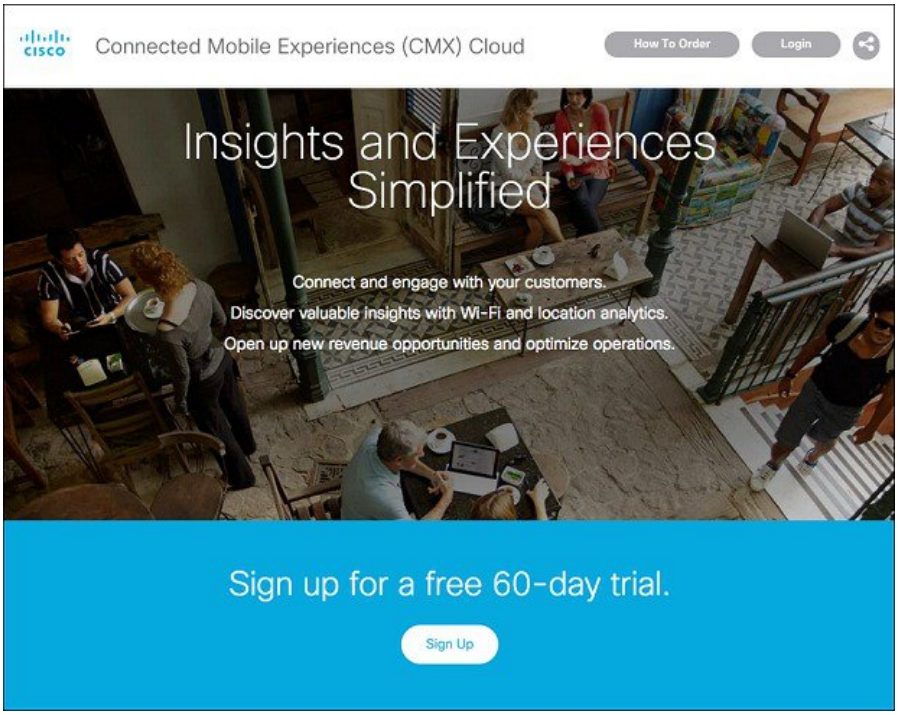
CMX Cloud Trial Sign-Up and Sign-In

Sign-Up

To sign-up for a trial account, perform the following steps:

Procedure

Step 1 Browse to https://cmxcisco.com and sign-up for a 60-Day trial.



Step 2 Enter the following details:

a. Full Name

b. E-mail address

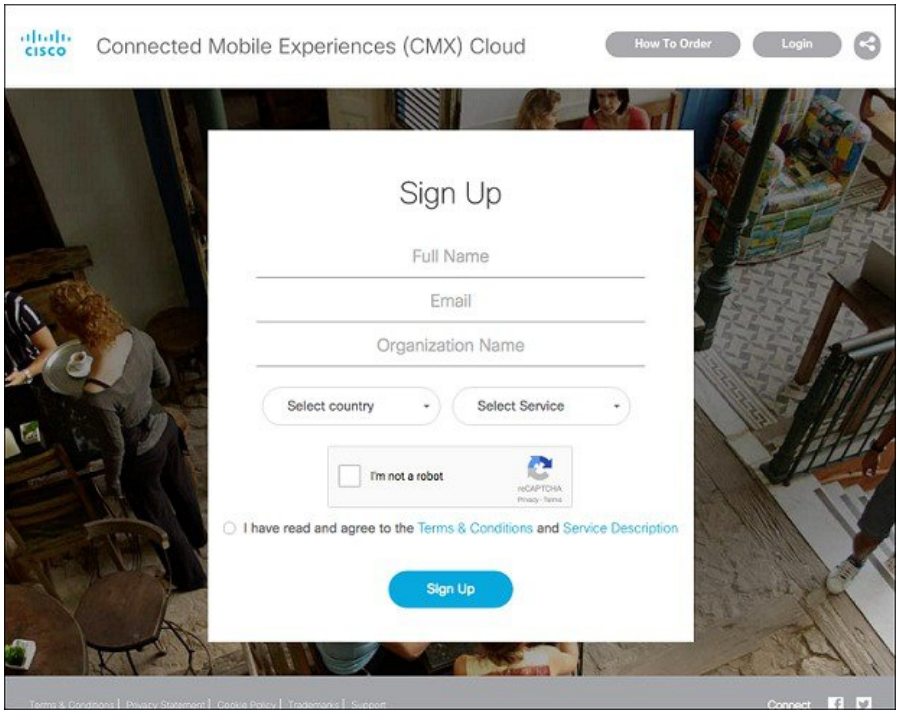
c. Organization name

d. Select Country

e. Select Service (Connect or Connect with Presence Analytics) from drop down list

f. Check “I have read and agree to the Terms and Conditions”

g. Click Sign Up



After your account is created and Site is provisioned, an email will be sent to you with the following:

a. Account Login Password

b. Site URL

c. Token

Sign In

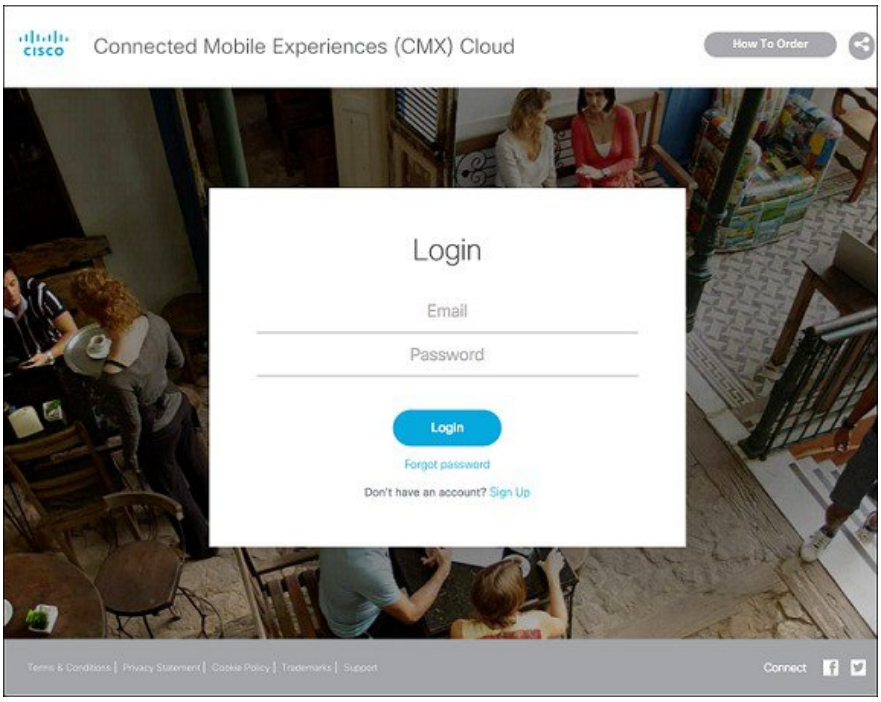
To sign-in, perform the following steps:

Procedure

Step 1 Browse to https://cmxcisco.com

Step 2 Click Login on the top right and enter the email address which was used to create the account and password.

Step 3 Click Login to get redirected to you CMX Cloud site.



Configuring Cisco Mobility Express to send data to CMX Cloud for Presence Analytics

Enabling CMX Cloud Service on Primary Access Point

After CMX Cloud Account is created and CMX Site provisioned, 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.

Note Primary Access Point should be able to talk to the CMX Cloud.

To configure, perform the following steps:

Procedure

Step 1 On Cisco Mobility Express WebUI, navigate to **Advanced > CMX**.

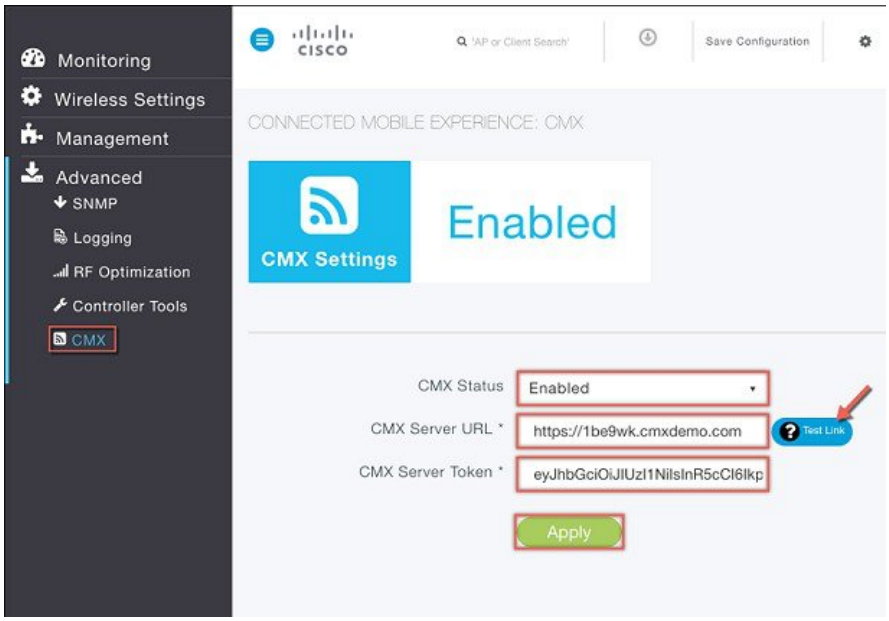
Step 2 On Cisco Mobility Express WebUI, navigate to **Advanced > CMX**.

Step 3 Enter the **CMX Server URL** (Site URL).

Step 4 Enter the **CMX Server Token**.

Step 5 Click **Apply**.

Tip Click the **Test Link** button to verify connectivity from Primary AP to CMX Cloud Site using the configured information.



Collecting Base MAC Address of Access Points to add them to the Site in CMX Cloud

In AireOS release 8.3, Access Points, which are part of the Cisco Mobility Express deployment, are not discovered automatically in the CMX Cloud when the CMX Could Service is started on the Primary Access Point. Access Points have to be manually added to the site in CMX Cloud. To obtain the Base MAC address, execute the following command in the Controller CLI.

```
(Cisco Controller) >show ap join stats summary all

Number of APs.......................................... 3

Base Mac            AP EthernetMac      AP Name               IP Address        Status
38:ed:18:ca:8b:00   38:ed:18:ca:09:28   AP38ED.18CA.0928      172.20.229.60     Joined

38:ed:18:cb:60:60   38:ed:18:ca:3d:10   AP38ED.18CA.3D10      172.20.229.21     Joined

38:ed:18:cd:31:80   38:ed:18:cc:32:c0   AP38ED.18CC.32C0      172.20.229.61     Joined
```

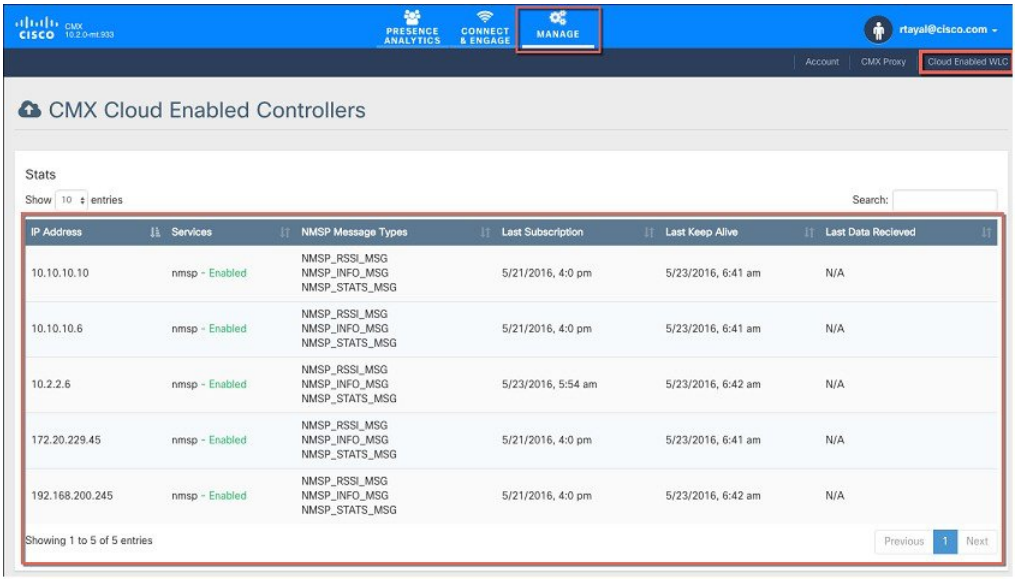
Creating a Site and Adding Access Points to Site in CMX Cloud for Presence Analytics

To create a site and add Access Points to the site in CMX Cloud for Presence Analytics, perform the following steps:

Procedure

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.** Click **Add Site** to create a Site and add Access points to the Site.

Step 4 In the New Site window, enter the following dertails:

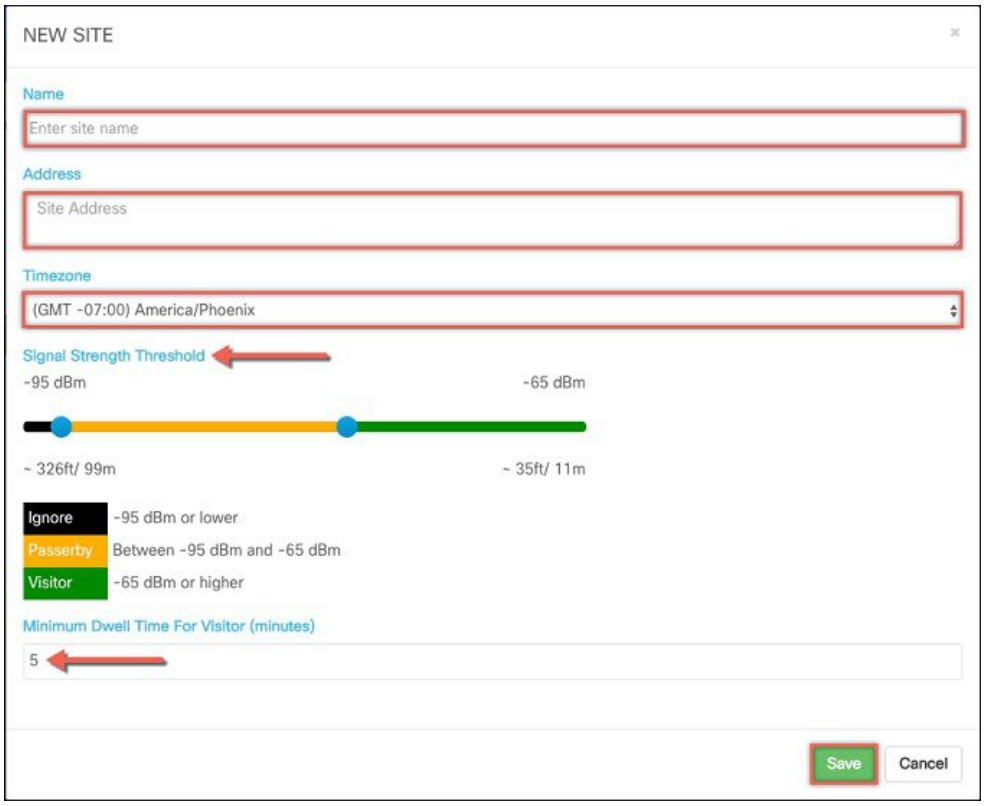
a. Site Name

b. Site Address

c. Timezone from the drop down list

d. Signal Strength Threshold for Ignore, Passerby, and Visitors

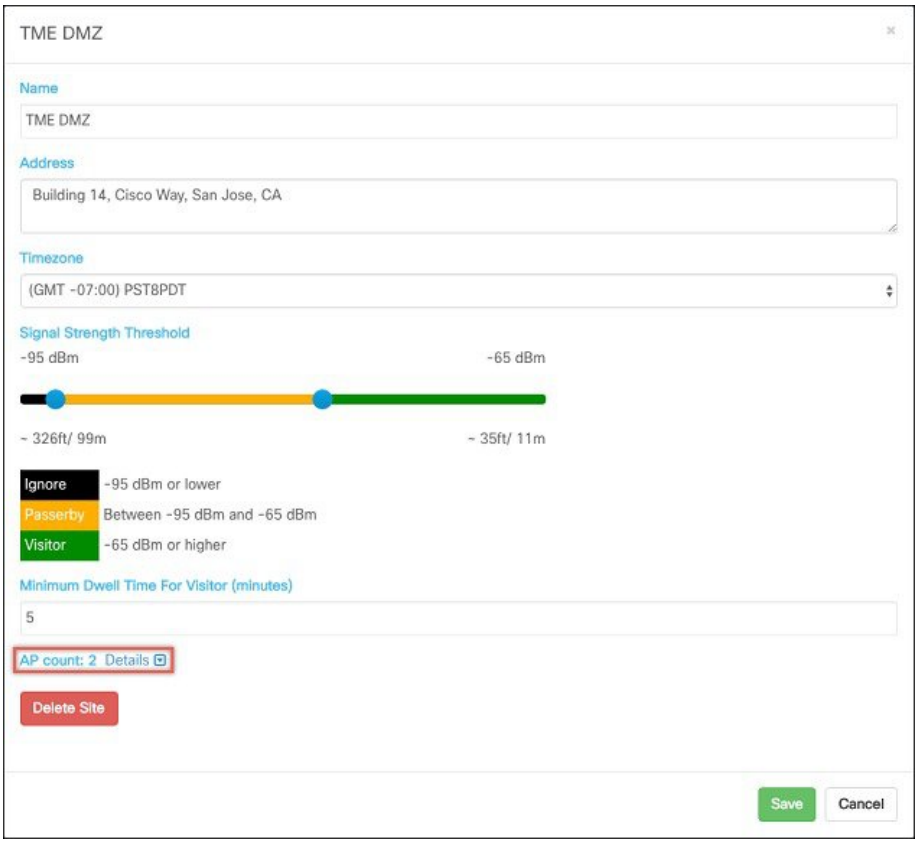
e. Minimum Dwell Time for Visitor



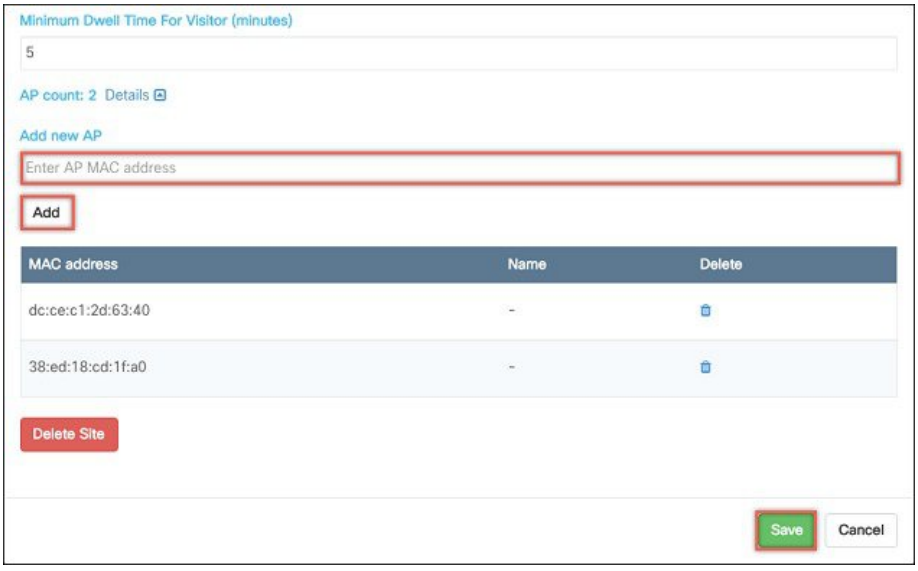
Step 5 Click **Save** to create the Site.

The site gets created.

Step 6 Click Site Name and then click the Details link next to the AP Count as shown in the Site window.

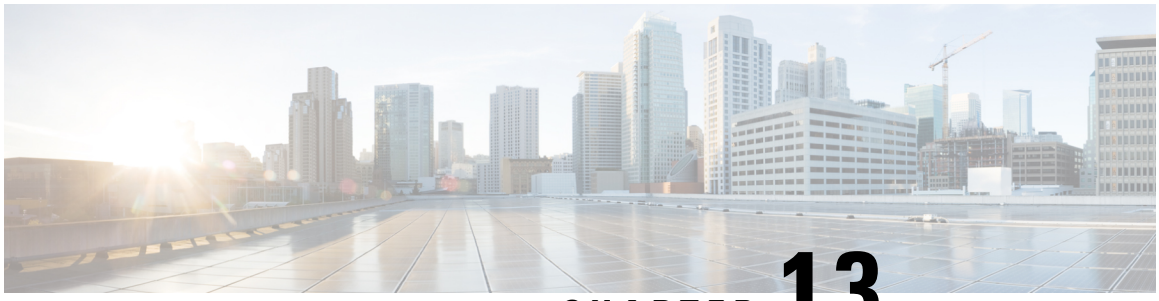


Step 7 The window will expand and **Add new AP** field will be displayed. Enter the Base MAC Address of the Access point and click **Add**. When finished with adding Base MAC of AP to the sites, click on the **Save**.



Understanding Data on the CMX Cloud for Presence Analytics Dashboard

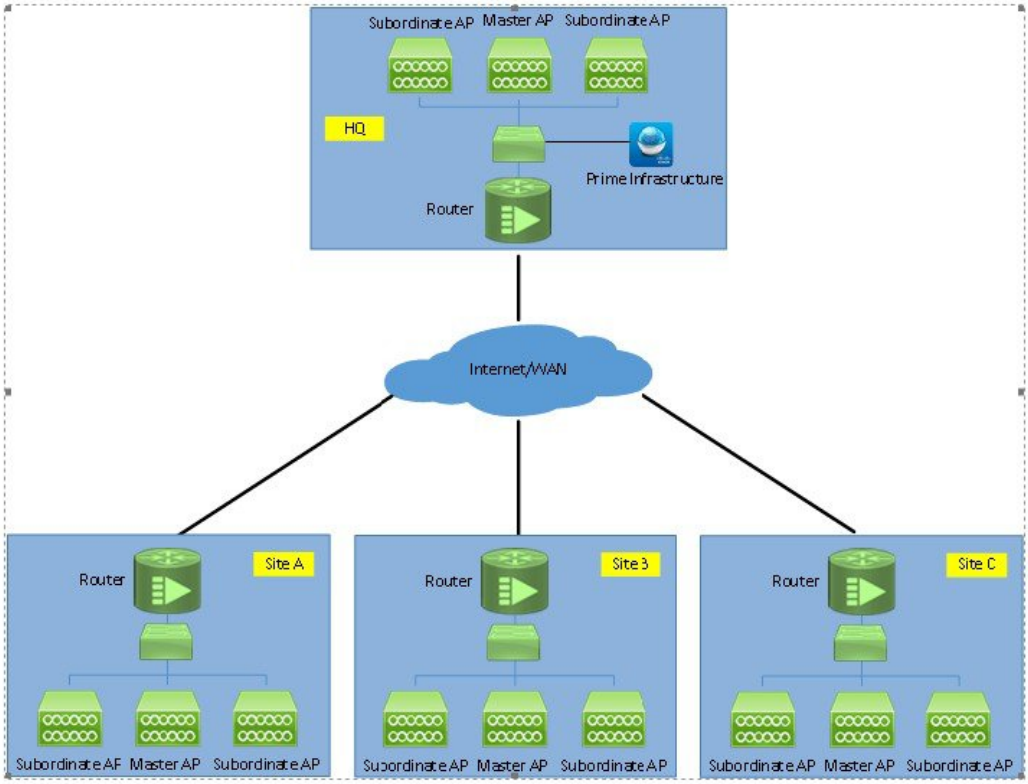
After the Sites have been created and Access Points have been added to the sites, data will begin to appear on the Presence Analytics dashboard. To understand the Data represented on this dashboard, please visit the following site:



CHAPTER 13

Managing Mobility Express Deployments from Cisco Prime Infrastructure

Cisco Prime Infrastructure 3.01 or later can be utilized to monitor multiple instances of Cisco Mobility Express deployment.



• Adding Mobility Express to Prime, on page 95

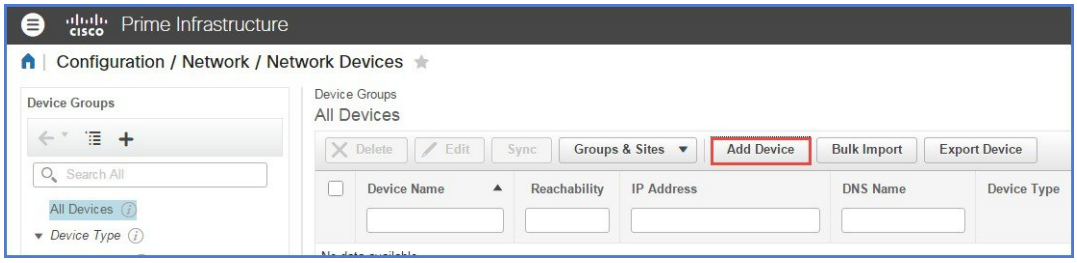
Adding Mobility Express to Prime

Perform the following steps to add the controllers:

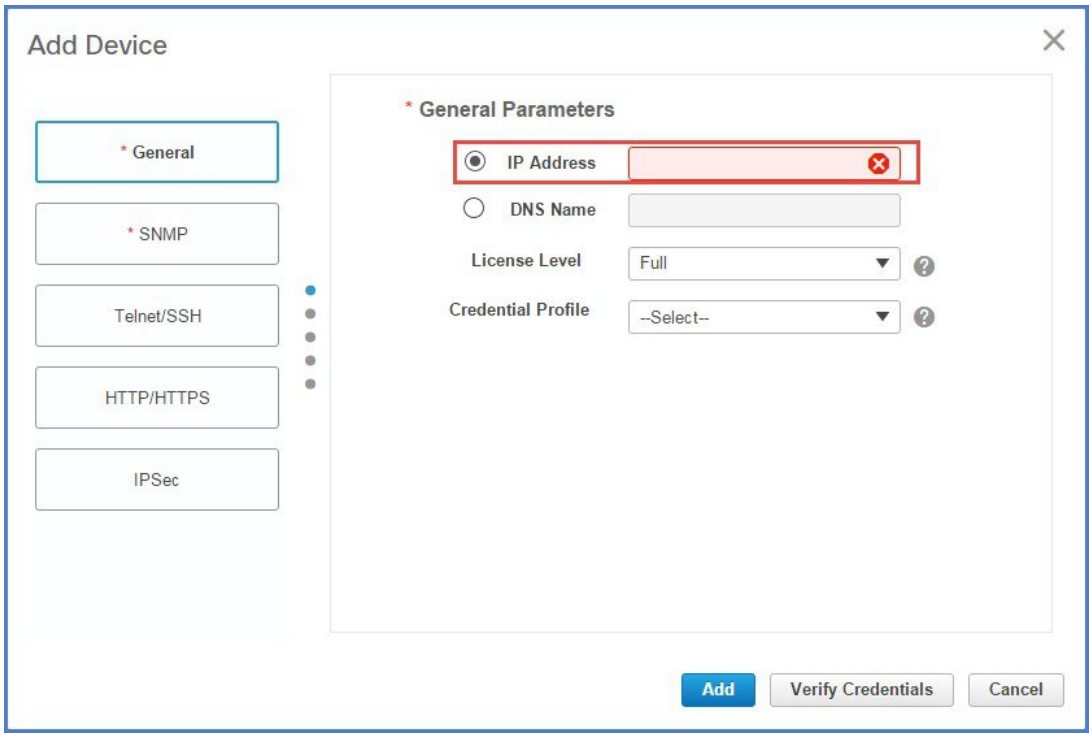
Procedure

Step 1 Login to Cisco Prime

Step 2 Navigate to Configuration / Network / Network Devices, click on **Add Device**.

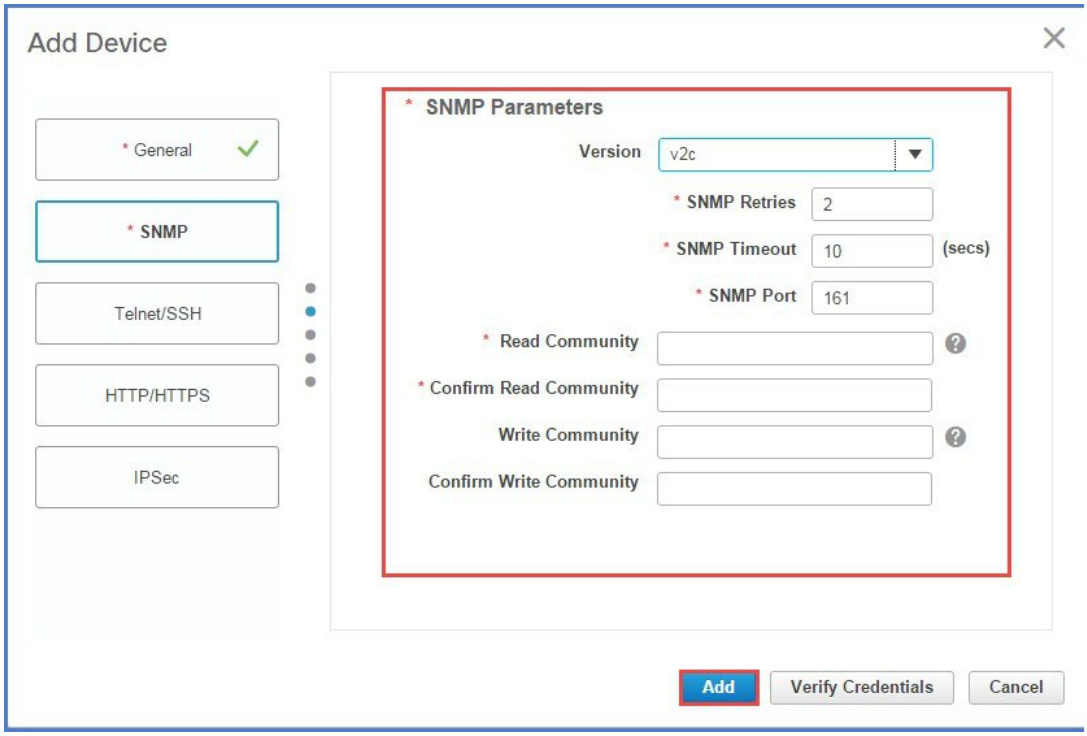


Step 3 Enter the IP address of the Mobility Express controller.

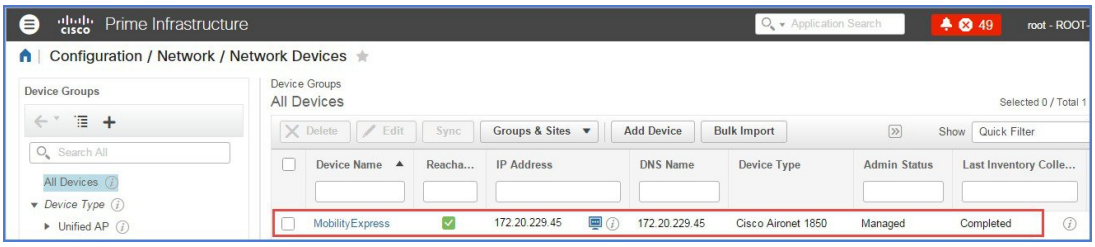


Step 4 Enter the SNMP Parameters and click Add.

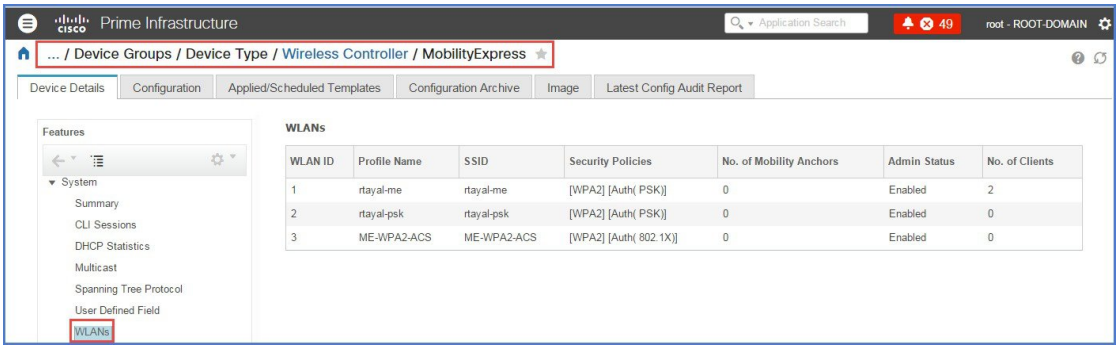
Note You must configure the SNMP community strings on the Mobility Express controller prior to adding the device in Prime.



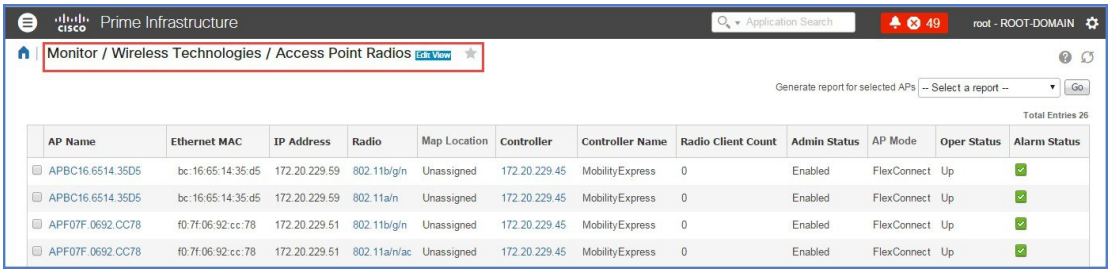
Step 5 After the device is added, it shows up in the **All Devices** list.



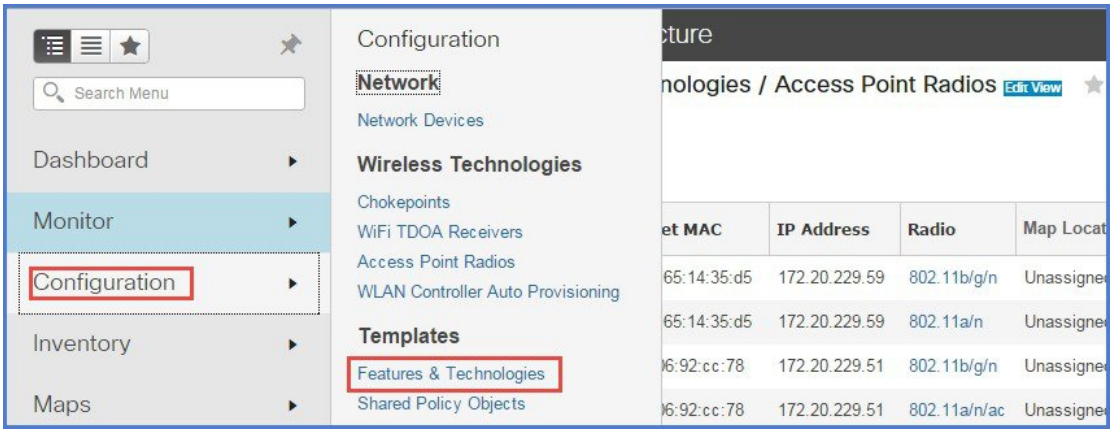
Step 6 To view the list of WLANs, navigate to **Network Devices > Device Groups > Device Type > Wireless Controller** and select the Mobility Express controller you added in Step 4.



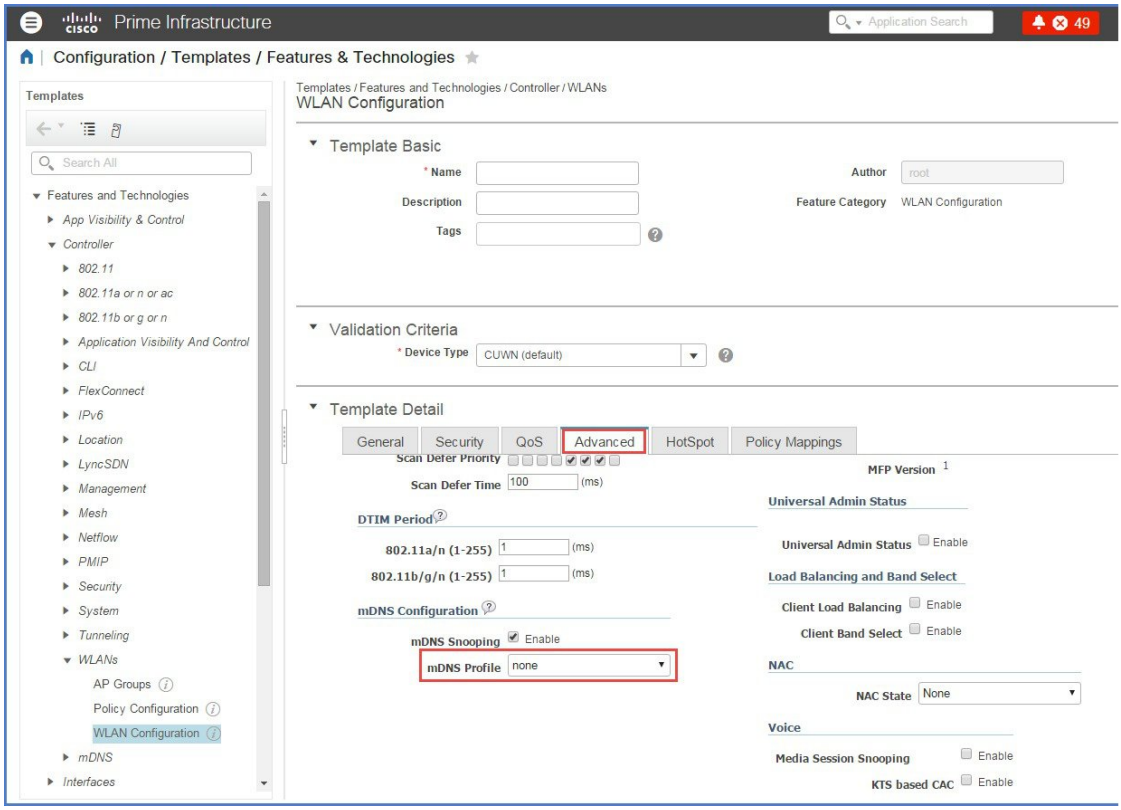
Step 7 To view the list of AP, navigate to **Monitor > Wireless Technologies > Access Point Radios**



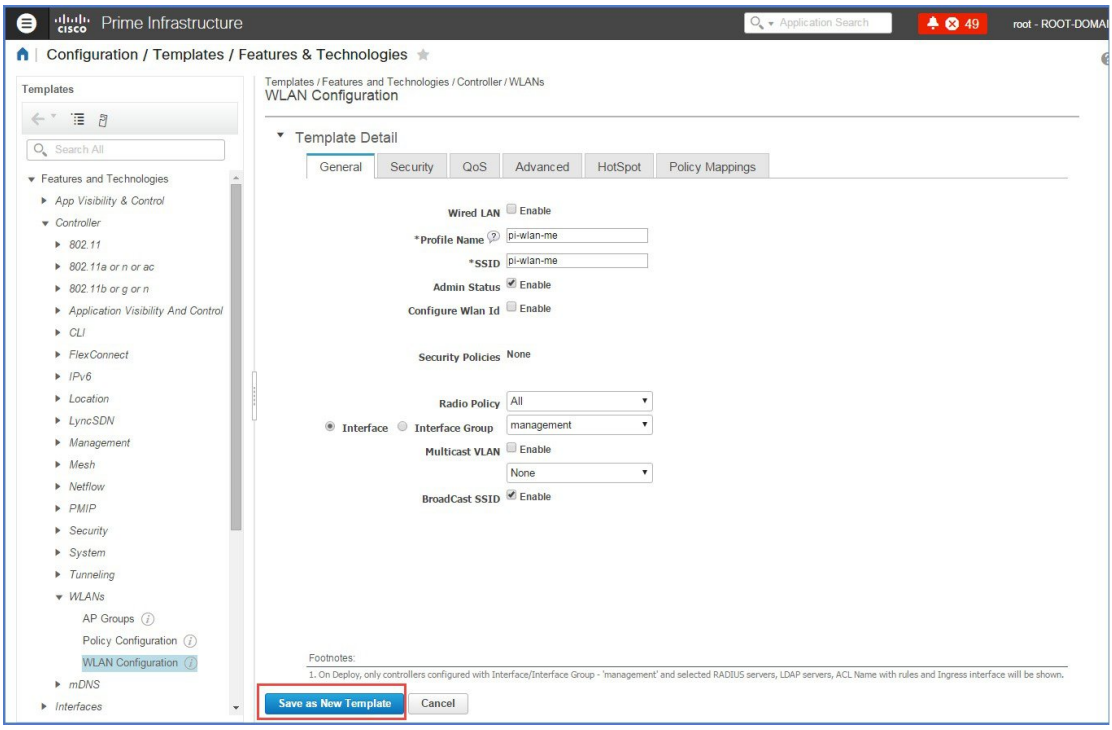
Step 8 To configure WLANS from Prime on Mobility Express, navigate to **Configuration > Feature & Technologies** under **Template**.



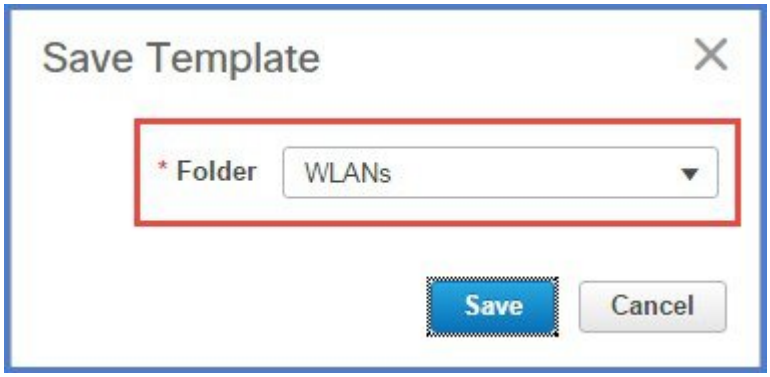
Step 9 Navigate to **Controller > WLAN > WLAN Configuration**. Enter the Template name and the **Template Detail**.



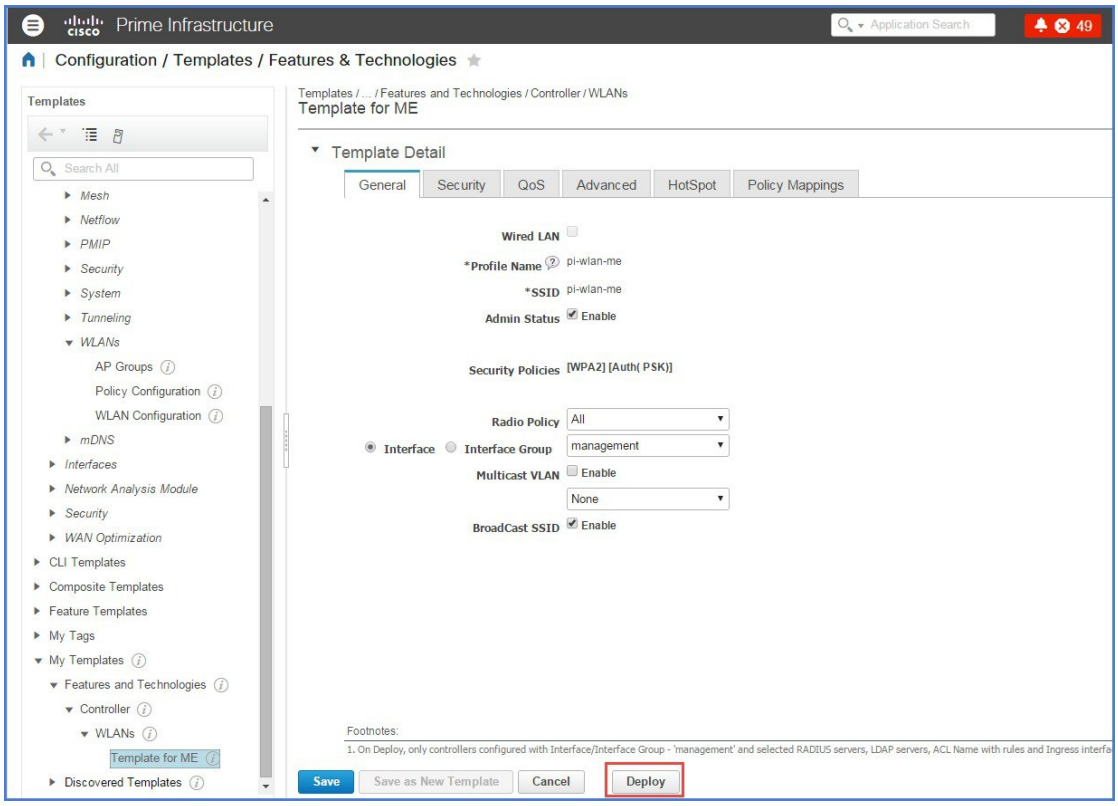
Step 10 On the **Advanced Tab**, make sure mDNS profile is set to **none** as it is not supported on Mobility Express.



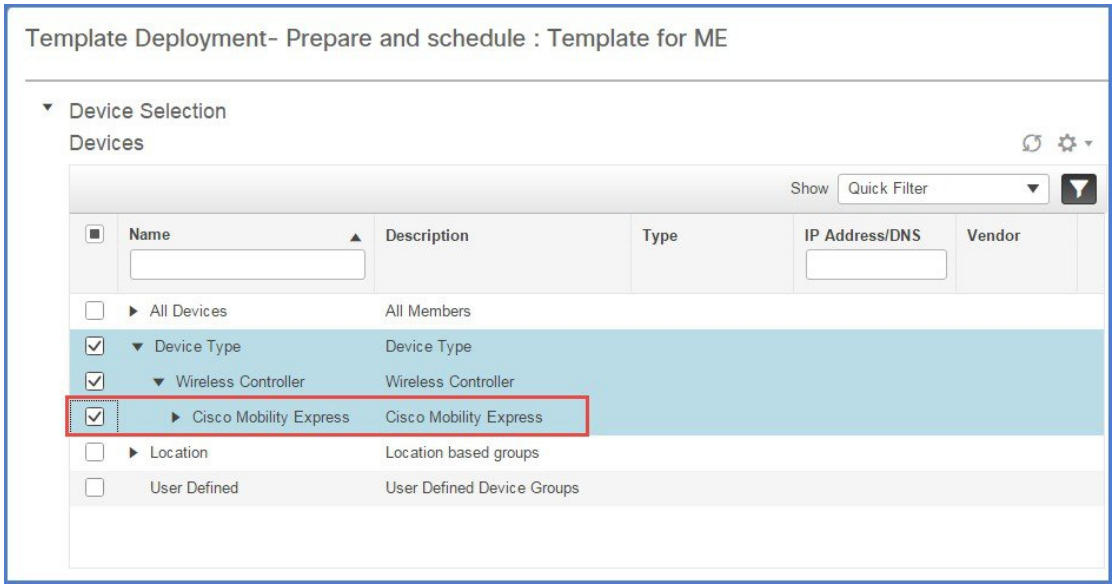
Step 11 To save the Template, click on ‘Save as New Template’ and select the folder where the teamplates need to be saved.



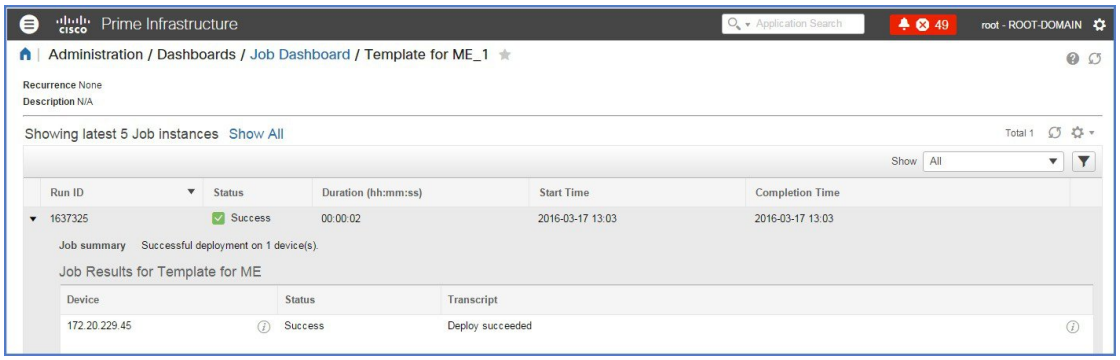
Step 12 To deploy the template to Mobility Express, click **Deploy**.



Step 13 Select the **Cisco Mobility Express** controller and click OK.



Step 14 Navigate to **Job Dashboard** to view the Job Status


Prime Infrastructure
Application Search
49
root - ROOT-DOMAIN
Administration / Dashboards / Job Dashboard / Template for ME_1
Recurrence None
Description N/A
Showing latest 5 Job instances Show All
Total 1
Show All
Run ID
Status
Duration (hh:mm:ss)
Start Time
Completion Time
1637325
Success
00:00:02
2016-03-17 13:03
2016-03-17 13:03
Job summary Successful deployment on 1 device(s).
Job Results for Template for ME
Device
Status
Transcript
172.20.229.45
Success
Deploy succeeded