CONTENTS

CHAPTER 1 Cisco Mobility Express Overview 1
   Supported Cisco Aironet® Access Points 1
      Master Access Points 2
      Subordinate Access Points 3
      Cisco Mobility Express Scale Limits 4
      Cisco Mobility Express Supported Features 4
      Supported Software Release and Interoperability 4

CHAPTER 2 Deploying Cisco Mobility Express 7
   Pre-requisites for Deploying Mobility Express Solution 7
   Connecting Mobility Express capable Access Point to the network 7
   Determining image on the Access Point 9
   Conversion 11
      Converting Access Point from CAPWAP to Cisco Mobility Express 11
      Converting Access Point from Cisco Mobility Express to CAPWAP 13

CHAPTER 3 Configuring Cisco Mobility Express controller 15
   CLI Setup Wizard 15
   Over-the-Air Setup Wizard 16
   Network Plug and Play 18
      Introduction 18
      Pre-requisites 18
      APIC-EM discovery options 18
      Configuring APIC-EM / Network PnP server 19
         Site Pre-Provisioning Workflow 19
         Importing Cisco Mobility Express configuration file to Network PnP 19
         Creating a Project 20
Adding Cisco Mobility Express capable Access Point to the Project and associating the controller config 21
APIC-EM Network Plug and Play Deployment Options with Cisco Mobility Express 22
APIC-EM controller in Private Cloud 23
Cloud Plug and Play Connect redirect to APIC-EM controller 23
Cloud Plug and Play Device Redirect Provisioning Workflow 24
Obtain a Smart Account 24
Create APIC-EM Controller Profile 25
Adding Cisco Mobility Express capable Access Point to the Devices list 28

Connecting Cisco Mobility Access Points 31

CHAPTER 4
Using internal DHCP server on Cisco Mobility Express 33
Creating a DHCP Scope 33

CHAPTER 5
Configuring Cisco Mobility Express for Site Survey 37
Introduction 37
Pre-requisites 37
Configuring Mobility Express for Site Survey using CLI 38

CHAPTER 6
Creating Wireless Networks 41
WLANs 41
Creating Employee WLANs 42
Creating Employee WLAN with WPA2 Personal 42
Creating Employee WLAN using WPA2 Enterprise with External Radius Server 42
Creating Employee WLAN with WPA2 Enterprise and Authentication Server as AP 43
Creating Employee WLAN with WPA2 Enterprise/External RADIUS and MAC Filtering 43
Creating Guest WLANs 44
Creating Guest WLAN with Captive Portal on CMX Connect 44
Creating Guest WLAN with Internal Splash Page 45
Creating Guest WLAN with External Splash Page 46
Internal Splash Page for Web Authentication 47
Using default internal guest portal 47
Using customized internal guest portal 47
Managing WLAN Users 48
Adding MAC for Local MAC Filtering on WLANs 48

CHAPTER 7

Managing Services with Cisco Mobility Express 51
Application Visibility and Control 51
Enabling Application Visibility on WLAN 51
Enabling Application Control on WLAN 52
  Adding Application Control from Network Summary Page 52
  Adding Application Control from Applications Page 52
iOS Optimized WiFi connectivity and Fast Lane 52
  Configuring Optimized WiFi Connectivity 52
  Configuring Fast Lane 54
Cisco Mobility Express with CMX Cloud 55
  Cisco CMX Cloud 55
  Cisco CMX Cloud Solution Compatibility Matrix 55
Minimum requirements for Cisco CMX Cloud deployment 55
Enabling CMX Cloud Service on Mobility Express for Presence Analytics 56
  Configuring Site on CMX Cloud for Presence Analytics 56

CHAPTER 8

Managing the Cisco Mobility Express Deployment 57
Managing Access Points 57
Adding Access Points to Cisco Mobility Express Network 58
Configuring Management Access 59
Managing Admin Accounts 60
Managing TIME on Cisco Mobility Express 61
  Configuring NTP Server 61
Updating Cisco Mobility Express Software 62
  Software Update using cisco.com Transfer Mode 63
  Software Update using HTTP Transfer Mode 64
  Software Update using TFTP Transfer Mode 65
  Upgrading from WebUI 65
  Upgrading from CLI 66
Managing Advanced RF Parameters 67

CHAPTER 9

Master AP Failover and Electing a new Master 69
Master AP Failover 69
ELECTING A NEW MASTER ACCESS POINT  70

CHAPTER 10

MANAGING MOBILITY EXPRESS DEPLOYMENTS FROM CISCO PRIME INFRASTRUCTURE  73

ADDING MOBILITY EXPRESS TO PRIME  74
Cisco Mobility Express 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 Aironet® 1560, 1815W, 1815I, 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:

- Is ideal for small and medium-sized deployments of up to 100 access points.
- Provides an easy, over-the-air deployment in under 10 minutes. In addition, one can use Network Plug and Play to bring up a new site.
- Removes the need for a physical controller while supporting Cisco's advanced features.
- Is supported on Cisco Aironet® 1560, 1815W, 1815I, 1830, 1850, 2800 and 3800 Series 802.11ac Wave 2 Access Points.
- Can control other Aironet® access points, such as the 1700, 2700, and 3700 Series.
- Can be used to perform Site Survey.
- 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

Cisco Mobility Express solution consists of the following components:

- Supported Cisco Aironet® Access Points, page 1
• Master Access Point - Cisco Aironet® 1560, 1815W, 1815I, 1830, 1850, 2800 and 3800 Series 802.11ac Wave 2 Access Points running the virtual Wireless LAN Controller function.

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

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

---

**Master Access Points**

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

**Table 1: Cisco Aironet® Access Points capable of operating as Master Access Points**

<table>
<thead>
<tr>
<th>Master Access Points</th>
<th>Supported Model Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Aironet® 1560 Series</td>
<td>AIR-AP1562I-x-K9</td>
</tr>
<tr>
<td></td>
<td>AIR-AP1562E-x-K9</td>
</tr>
<tr>
<td></td>
<td>AIR-AP1562D-x-K9</td>
</tr>
<tr>
<td>Cisco Aironet® 1815I Series</td>
<td>AIR-AP18151-x-K9C</td>
</tr>
<tr>
<td>Cisco Aironet® 1815W Series</td>
<td>AIR-AP1815W-x-K9C</td>
</tr>
<tr>
<td>Cisco Aironet® 1830 Series</td>
<td>AIR-AP1832I-x-K9C</td>
</tr>
<tr>
<td>Cisco Aironet® 1850 Series</td>
<td>AIR-AP1852I-x-K9C</td>
</tr>
<tr>
<td></td>
<td>AIR-AP1852E-x-K9C</td>
</tr>
<tr>
<td>Cisco Aironet® 2800 Series</td>
<td>AIR-AP2802I-x-K9C</td>
</tr>
<tr>
<td></td>
<td>AIR-AP2802E-x-K9C</td>
</tr>
<tr>
<td>Cisco Aironet® 3800 Series</td>
<td>AIR-AP3802I-x-K9C</td>
</tr>
<tr>
<td></td>
<td>AIR-AP3802E-x-K9C</td>
</tr>
</tbody>
</table>

**Note**
The -x- in the other model numbers is a placeholder for the actual letter indicating the model's regulatory domain. For information on regulatory domains, see [http://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html](http://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html)
Subordinate Access Points

Cisco Aironet® Access Points which operate as Subordinate Access Points and serve clients are listed in the table below:

Table 2: Cisco Aironet® Access Points capable of operating as Subordinate Access Points

<table>
<thead>
<tr>
<th>Master Access Points</th>
<th>Supported Model Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Aironet® 700i Series</td>
<td>AIR-CAP702I-x-K9</td>
</tr>
<tr>
<td>Cisco Aironet® 700w Series</td>
<td>AIR-CAP702W-x-K9</td>
</tr>
<tr>
<td>Cisco Aironet® 1560Series</td>
<td>AIR-AP1562I-x-K9, AIR-AP1562E-x-K9, AIR-AP1562D-x-K9</td>
</tr>
<tr>
<td>Cisco Aironet® 1600 Series</td>
<td>AIR-CAP1602I-x-K9, AIR-CAP1602E-x-K9</td>
</tr>
<tr>
<td>Cisco Aironet® 1700 Series</td>
<td>AIR-CAP1702I-x-K9</td>
</tr>
<tr>
<td>Cisco Aironet® 1810 Series</td>
<td>AIR-AP1810W-x-K9</td>
</tr>
<tr>
<td>Cisco Aironet® 1815I Series</td>
<td>AIR-AP1815I-x-K9C</td>
</tr>
<tr>
<td>Cisco Aironet® 1815W Series</td>
<td>AIR-AP1815W-x-K9C</td>
</tr>
<tr>
<td>Cisco Aironet® 1830 Series</td>
<td>AIR-AP1832I-x-K9C</td>
</tr>
<tr>
<td>Cisco Aironet® 1850 Series</td>
<td>AIR-AP1852I-x-K9C, AIR-AP1852E-x-K9C</td>
</tr>
<tr>
<td>Cisco Aironet® 2600 Series</td>
<td>AIR-CAP2602I-x-K9, AIR-CAP2602E-x-K9</td>
</tr>
<tr>
<td>Cisco Aironet® 2700 Series</td>
<td>AIR-CAP2702I-x-K9, AIR-CAP2702E-x-K9</td>
</tr>
<tr>
<td>Cisco Aironet® 2800 Series</td>
<td>AIR-AP2802I-x-K9C, AIR-AP2802E-x-K9C</td>
</tr>
<tr>
<td>Cisco Aironet® 3600 Series</td>
<td>AIR-CAP3602I-x-K9, AIR-CAP3602E-x-K9</td>
</tr>
<tr>
<td>Cisco Aironet® 3700 Series</td>
<td>AIR-CAP3702I-x-K9, AIR-CAP3702E-x-K9</td>
</tr>
</tbody>
</table>
Cisco Mobility Express Scale Limits

Cisco Mobility Express supports up to 100 Access Points and 2000 Clients in a single deployment. Given below are the scale limits per Master Access Point.

**Table 3: Cisco Mobility Express Scale Limits**

<table>
<thead>
<tr>
<th>Master Access Points</th>
<th># of Access Points Supported</th>
<th># of Clients Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Aironet® 1560 Series</td>
<td>100</td>
<td>2000</td>
</tr>
<tr>
<td>Cisco Aironet® 1815I Series</td>
<td>50</td>
<td>1000</td>
</tr>
<tr>
<td>Cisco Aironet® 1815W Series</td>
<td>50</td>
<td>1000</td>
</tr>
<tr>
<td>Cisco Aironet® 1830 Series</td>
<td>50</td>
<td>1000</td>
</tr>
<tr>
<td>Cisco Aironet® 1850 Series</td>
<td>50</td>
<td>1000</td>
</tr>
<tr>
<td>Cisco Aironet® 2800 Series</td>
<td>100</td>
<td>2000</td>
</tr>
<tr>
<td>Cisco Aironet® 3800 Series</td>
<td>100</td>
<td>2000</td>
</tr>
</tbody>
</table>

**Note**

If there are more than 50 Access Points in a Mobility Express network, the Master AP (running the Wireless LAN controller function) can service a maximum of 20 clients. This limit only applies to Master AP and not any other Access Point in the Mobility Express network.

Cisco Mobility Express Supported Features

See Supported features section in Release notes

**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.
Deploying Cisco Mobility Express

- Pre-requisites for Deploying Mobility Express Solution, page 7
- Connecting Mobility Express capable Access Point to the network, page 7
- Determining image on the Access Point, page 9
- Conversion, page 11

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 Master Access Point. This Access Point should be capable of supporting the Wireless LAN Controller function.

3. A DHCP server must be available on the network so that Access Points and clients can obtain an IP Address. Starting AireOS® Release 8.3.102.0 or later, one can configure a DHCP server on the Master Access Point as well but this is typically used for Site Survey.

Connecting Mobility Express capable Access Point to the network

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

If Access Points and WLANs are all on the same network, Mobility Express capable Access Points can connect to an access port on the switch as shown below.
On Mobility Express, management traffic is untagged. If Access Points and WLANs are all on different VLANs, Mobility Express capable Access Points will connect to a trunk port on the switch and traffic for individual WLANs will be switched locally on individual VLANs. Shown below is a deployment with Access Points and WLANs on different VLANs.
interface GigabitEthernet1/0/37
description » Connected to Master AP «
switchport trunk native vlan 40
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk

Determining image on the Access Point

The Cisco Aironet® 1560, 1815, 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 procedure 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.
If the `show version` displays `AP Image Type: MOBILITY EXPRESS IMAGE` and `AP Configuration: NOT MOBILITY EXPRESS CAPABLE`, it means that even though the Access Point has the Cisco Mobility Express image, it is configured to run as a CAPWAP Access Point. In this case Access Point will not run the controller function and will not participate in the Master Election process upon failure of the active Master AP.

For this AP to run the controller function, `AP Configuration` has to be changed to `MOBILITY EXPRESS CAPABLE`. To change the AP Configuration, execute the following command from the AP CLI. `AP#ap-type mobility-express tftp://`

Access Point will reboot and after it comes up, it will be capable of running the controller function. You can check the output of `show version` again to confirm that `AP Configuration` has changed to `MOBILITY EXPRESS CAPABLE`.

If the `show version` displays `AP Image Type: MOBILITY EXPRESS IMAGE` and `AP Configuration: MOBILITY EXPRESS CAPABLE`, it means that the Access Point has the Mobility Express image and is capable of running the controller function. For this scenario, the output of the `show version` is shown below:
Conversion

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

Converting Access Point from CAPWAP to Cisco Mobility Express

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

Table 4: Minimum AireOS release supporting Cisco Mobility Express

<table>
<thead>
<tr>
<th>Access Point</th>
<th>Minimum AireOS Release with CAPWAP image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Aironet® 1560 Series</td>
<td>Release 8.3 MR1</td>
</tr>
<tr>
<td>Cisco Aironet® 1815I Series</td>
<td>Release 8.4 or later</td>
</tr>
<tr>
<td>Cisco Aironet® 1815W Series</td>
<td>Release 8.4 or later</td>
</tr>
<tr>
<td>Cisco Aironet® 1830 Series</td>
<td>Release 8.1 MR2 or later</td>
</tr>
<tr>
<td>Cisco Aironet® 1850 Series</td>
<td>Release 8.1 MR2 or later</td>
</tr>
<tr>
<td>Cisco Aironet® 2800 Series</td>
<td>Release 8.3 or later</td>
</tr>
<tr>
<td>Cisco Aironet® 3800 Series</td>
<td>Release 8.3 or later</td>
</tr>
</tbody>
</table>

Note

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

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

Procedure

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 8.4.100.0.
Table 5: Conversion tar file for Access Points

<table>
<thead>
<tr>
<th>Access Points supported as Master AP</th>
<th>Software to be used only for Conversion from Unified Wireless Network Lightweight AP Software to Cisco Mobility Express</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Aironet® 1560 Series</td>
<td>AIR-AP1560-K9-ME–8.4-100-0.tar</td>
</tr>
<tr>
<td>Cisco Aironet® 1815W Series</td>
<td>AIR-AP1815-K9-ME–8.4-100-0.tar</td>
</tr>
<tr>
<td>Cisco Aironet® 1830 Series</td>
<td>AIR-AP1830-K9-ME–8.4-100-0.tar</td>
</tr>
<tr>
<td>Cisco Aironet® 1850 Series</td>
<td>AIR-AP1850-K9-ME–8.4-100-0.tar</td>
</tr>
<tr>
<td>Cisco Aironet® 2800 Series</td>
<td>AIR-AP2800-K9-ME–8.4-100-0.tar</td>
</tr>
<tr>
<td>Cisco Aironet® 3800 Series</td>
<td>AIR-AP3800-K9-ME–8.4-100-0.tar</td>
</tr>
</tbody>
</table>

Step 2  Login to the Access Point.

Step 3  Execute `AP#show version` on the Access Point CLI. From the show version output, you can determine the **AP Image type** and **AP Configuration** and can then proceed with the conversion.

**Case 1:** If the **AP Image type** is **MOBILITY EXPRESS IMAGE** and **AP configuration** is **NOT MOBILITY EXPRESS CAPABLE**, enter the command below to change the **AP Configuration** to **MOBILITY EXPRESS CAPABLE**.

`AP#ap-type mobility-express`

Since the Access Point has **AP Image type**: **MOBILITY EXPRESS IMAGE**, a new image will not be downloaded. After the command is executed, the Access Point will reboot and after it comes up, the **AP Configuration** will be changed to **MOBILITY EXPRESS CAPABLE**.

**Case 2:** If the **AP Image type** and **AP Configuration** are not available, it means that the AP is running CAPWAP image. To do the conversion, execute the command below.

`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.
```

```
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
Signature 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 reboot
[07/24/2015 18:19:43.1257] Going down for restart now

Note After the image download is complete, it will be written to the flash followed by a reboot. After the AP comes up, AP Image type will be MOBILITY EXPRESS IMAGE and AP Configuration will MOBILITY EXPRESS CAPABLE.

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

Converting Access Point from Cisco Mobility Express to CAPWAP

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

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

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

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

(Cisco Controller) >config ap unifiedmode <switch_name> <switch_ip_address>
<switch_name> and <switch_ip_address> is the name and IP address respectively of the WLC to which the APs need to be migrate.

Note The above command converts all connected Access Points with AP Configuration: MOBILITY EXPRESS CAPABLE to AP Configuration: NOT MOBILITY EXPRESS CAPABLE. When this command is issued, the APs are reloaded, and they come back up and look for the controller (switch_ip_address) to join.
CHAPTER 3

Configuring Cisco Mobility Express controller

There are multiple ways one can configure a Cisco Mobility Express controller. They are as follows:

1. CLI Setup Wizard
2. Over-the-Air Setup Wizard
3. Network Plug and Play
   - CLI Setup Wizard, page 15
   - Over-the-Air Setup Wizard, page 16
   - Network Plug and Play, page 18
   - APIC-EM Network Plug and Play Deployment Options with Cisco Mobility Express, page 22
   - Connecting Cisco Mobility Access Points, page 31

CLI Setup Wizard

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

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

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

```
System Name [Cisco_2c:3a:40] (31 characters max): me-wlc
Enter Country Code list (enter 'help' for a list of countries) [US]:
Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: no

Note! Default NTP servers will be used

Management Interface IP Address: 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
```
Over-the-Air Setup Wizard

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

**Procedure**

**Step 1** When the LED on the Access Point chirps green, connect a WiFi enabled laptop to the **CiscoAirProvision** SSID. The default password is **password**. The laptop will get an IP address from subnet 192.168.1.0/24.

*Note* CiscoAirProvision SSID is broadcast at 2.4GHz.

**Step 2** Open a web browser and browse to **http://mobilityexpress.cisco**. This will redirect to configuration wizard and the admin account page will appear.

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

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

Step 4 In the **Set up Your Controller** section, configure the following:

- Enter the System Name
- Select the Country from the drop-down list
- Date and Time should be auto-filled but one can manually configure it as well
- Select the Timezone from the drop-down list
- Enter the IP address of NTP Server if there is one available. If left blank, NTP Pools will be automatically configured
- Enter the Management IP Address of the controller
- Enter the Subnet Mask
- Enter the Default Gateway

Step 5 Disable **Enable DHCP Server (Management Network)** if an external DHCP server is being used. If internal DHCP server on the Mobility Express controller has to be used, specify the DHCP server related information.

Step 6 Click **Next**.

Step 7 In the **Create Your Wireless Network**, under **Employee Network**, configure the following:

- Enter the Network Name
- Select Security as WPA2 Personal or WPA2 Enterprise from the drop-down list
- If WPA2 Personal is selected, enter the Passphrase

Step 8 One can also enable **RF Parameter Optimization** and configure the following:

- Move the **Client Density** slider as needed
- From the **Traffic Type**, select Data or Data and Voice

Step 9 Click **Next**.

Step 10 Confirm the settings on the page and click on the **Apply** button. The Access Point will reboot and after it comes up, it will run the controller.

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

Introduction

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

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

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

Pre-requisites

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

APIC-EM discovery options

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

   Note

   192.168.1.123 is the IP address of the APIC-EM Server

2. On-prem PnP server can be added to DNS using ‘pnpserver.yourlocal.domain’ If DHCP discovery fails to get the IP address of the APIC-EM controller, for example, because option 43 is not configured, the Cisco Plug and Play Agent falls back on a DNS lookup method. Based on the network domain name returned by the DHCP server, it constructs a fully qualified domain name (FQDN) for the APIC-EM controller, using the preset hostname pnpserver. For example, if the DHCP server returns the domain name "customer.com ", the Cisco Plug and Play IOS Agent constructs the FQDN "pnpserver.customer.com ". It then uses the local name server to resolve the IP address for this FQDN.
3. Cloud redirection service requires a connection to the internet, and a valid DNS server that can resolve 'devicehelper.cisco.com'. The cloud redirection service redirects Cisco Mobility Express Access Point to APIC-EM.

Configuring APIC-EM / Network PnP server

Site Pre-Provisioning Workflow

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

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

1. Importing Cisco Mobility Express controller configuration file to Network PnP
2. Creating a Project
3. Adding Cisco Mobility Express capable Access Point to the Project and associating the controller config.

Importing Cisco Mobility Express configuration file to Network PnP

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Login to APIC-EM controller and navigate to Network Plug and Play &gt; Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click on Upload to upload the controller configuration</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select a controller configuration file from your local machine</td>
</tr>
</tbody>
</table>
Creating a Project

Procedure

Step 1  Navigate to Network Plug and Play > Projects.

Step 2  Enter the name for the Project and click on the Add button.

Step 3  Click on the Create button to create the Project.
Adding Cisco Mobility Express capable Access Point to the Project and associating the controller config

Procedure

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

Step 4 Click on the Add button.
APIC-EM Network Plug and Play Deployment Options with Cisco Mobility Express

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

APIC-EM controller in Private Cloud

Cloud Plug and Play Connect redirect to APIC-EM controller
**APIC-EM controller in Private Cloud**

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

![Figure 1: APIC-EM controller in Private Cloud flow](image)

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

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

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

```
ip dhcp pool pnp_device_pool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
domain-name cisco.com
dns-server 172.20.229.8
```

**Cloud Plug and Play Connect redirect to APIC-EM controller**

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

**Figure 2: Cloud Plug and Play Device Redirect to APIC-EM controller flow**

Cloud Plug and Play Device Redirect Provisioning Workflow

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

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

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

**Obtain a Smart Account**

Procedure

- **Step 1** Go to http://software.cisco.com
- **Step 2** Request a Smart Account or Log In (existing Smart Account holders)
Create APIC-EM Controller Profile

Procedure

**Step 1** Go to http://software.cisco.com and login

**Step 2** Navigate to Provisioning > Plug and Play Connect
Step 3  Click on Controller Profiles. Select a Virtual Account. If you do have one, create a Virtual Account first.

Step 4  Click on the Add Profile to create a new controller profile.

Step 5  Select Controller Type as PNP Server from the drop-down list and click on Next.

Step 6  Enter the following and click Next.

1. Profile Name
2. Description
3. Select IPv4 or IPv6, HTTP or HTTPS and enter the IP address if the PNP Server

Note  If you select HTTPS, then you would have import a SSL certificate. Also, optionally one can enter information of the secondary controller.
Step 7  Review the entries and click on Submit button to add the Controller Profile and finally click Done.
Adding Cisco Mobility Express capable Access Point to the Devices list

Procedure

**Step 1** Navigate to Provisioning > Plug and Play Connect. Click on Devices.

**Step 2** Click on Devices. Select a Virtual Account. If you do have one, create a Virtual Account first.

**Step 3** Click on Add Devices button to add a new device (Mobility Express Access Point).

**Step 4** Import a csv file with the Device info or select Enter Device info manually. Click Next.
**Step 5**  Click on Identify Device button. The Identify Device window will pop up. Enter Serial Number, select Base PID, and Controller Profile(created earlier). Click on the Save button followed by Next button.
Step 6  Review the entries and click on Submit button to add the Device. Finally, click Done.

Step 7  Verify that the Device has been added and the status is Pending (Redirection).
Connecting Cisco Mobility Access Points

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

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

Starting Release 8.3.102.0, one can enable internal DHCP Server and create scopes for Access Points and WLANs. A total of 17 DHCP scopes are supported on Cisco Mobility Express. Using the internal DHCP server also enables Cisco Mobility Express to be used for performing Site Survey without the need of an external DHCP server.

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 a DHCP Scope, page 33

Creating a DHCP Scope

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

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

Procedure

Step 1 Navigate to Wireless Settings > DHCP Server > Add new Pool. The Add DHCP Pool window will pop up.

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

- Enter the Pool Name for the WLAN
- Enable the Pool Status
- Enter the VLAN ID for the WLAN
- Enter the Lease Period for the DHCP clients. Default is 1 Day
Creating a DHCP Scope

- Enter the **Network/Mask**
- Enter the **Start IP** for the DHCP pool
- Enter the End IP for the DHCP pool
- Enter the **Gateway IP** for the DHCP pool
- Enter the **Domain Name** (Optional) for the DHCP pool
- For **Name Servers**, select User Defined if one needs to enter IP addresses of Name Servers or select OpenDNS in which case OpenDNS Name Server IP addresses are automatically populated.

**Step 3** Click **Apply**.

**Step 4** After creating the scope, it is time to assign the VLAN mapped to the DHCP scope to the WLAN. To assign a VLAN to WLAN, navigate to **Wireless Settings > WLANs**.

**Step 5** If the WLAN does not exist, create a WLAN or if one does exist, edit the existing WLAN and click on the **VLAN and Firewall** tab.

**Step 6** On the **VLAN and Firewall** tab, configure the following:

- Select **Yes** for Use VLAN Tagging
- Enter the **Native VLAN ID**
- Select the **DHCP Scope** which was created previously for the WLAN. **VLAN ID** should be automatically populated after the DHCP scope is selected.
Step 7  Click Apply.
Configuring Cisco 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 Cisco Mobility Express:

<table>
<thead>
<tr>
<th>Access Point</th>
<th>Release supporting Site Survey capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1560 Series</td>
<td>AireOS Release 8.3.111.0 and later</td>
</tr>
<tr>
<td>1815I Series</td>
<td>AireOS Release 8.4 and later</td>
</tr>
<tr>
<td>1815W Series</td>
<td>AireOS Release 8.4 and later</td>
</tr>
<tr>
<td>1830 Series</td>
<td>AireOS Release 8.3.111.0 and later</td>
</tr>
<tr>
<td>1850 Series</td>
<td>AireOS Release 8.3.111.0 and later</td>
</tr>
<tr>
<td>2800 Series</td>
<td>AireOS Release 8.3.111.0 and later</td>
</tr>
<tr>
<td>3800 Series</td>
<td>AireOS Release 8.3.111.0 and later</td>
</tr>
</tbody>
</table>
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:

**Note** For Site Survey, a DHCP server is required and is supported on Cisco Mobility Express. DHCP Server configuration highlighted below is mandatory if you want to enable DHCP server on Cisco Mobility Express.

Would you like to terminate autoinstall? [yes]:yes
Enter Administrative User Name (24 characters max):admin
Enter Administrative Password (3 to 24 characters max):Cisco123
Re-enter Administrative Password: Cisco123
System Name:[Cisco_3a:d2:b4] {31 characters max}:me-wlc
Enter Country Code list (enter 'help' for a list of countries)[US]:US
Configure a NTP server now? [YES][no]:no
Configure the system time now? [YES][no]:yes
Enter the date in MM/DD/YY format:02/28/17
Enter the time in HH:MM:SS format:11:30:00
Enter timezone location index (enter 'help' for a list of timezones):5
Management Interface IP Address: 10.10.10.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1

Create Management DHCP Scope? [yes][NO]:yes
DHCP Network: 10.10.10.0
DHCP Netmask: 255.255.255.0
Router IP: 10.10.10.1
Start DHCP IP address: 10.10.10.10
Stop DHCP IP address: 10.10.10.250

DomainName: mewlc.local
DNS Server:[OPENDNS][user DNS]OPENDNS
Create Employee Network?[YES][no]:yes
Employee Network Name (SSID)?[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.

1 Default operation state of XOR radio is 2.4GHz.

2 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.

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

4 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
Creating Wireless Networks

- WLANs, page 41
- Creating Employee WLANs, page 42
- Creating Guest WLANs, page 44
- Internal Splash Page for Web Authentication, page 47
- Managing WLAN Users, page 48
- Adding MAC for Local MAC Filtering on WLANs, page 48

**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 Employee WLANs

Creating Employee WLAN with 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.

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 Apply.

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.

Step 3 Click on the WLAN Security and configure the following:
   a) Select Security Type as WPA2 Enterprise.
   b) Select Authentication Server as External Radius.

Step 4 Add the Radius server and configure the following:
   • Enter the Radius IP
   • Enter the Radius Port
   • Enter the Shared Secret
   • Click on tick icon
Creating Employee WLAN with WPA2 Enterprise and Authentication Server as 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.

Step 3 Click on the WLAN Security and configure the following:
   a) Select Security as WPA2 Enterprise.
   b) Select Authentication Server as AP.
   Note AP is the Master AP running the controller function. In this use case, controller is the Authentication Server and therefore Local WLAN user account must exist to onboard the clients.

Step 4 Click the Apply.

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

Procedure

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

Step 2 In the Add new WLAN window, on the General tab, configure the following:
   • Enter the Profile Name
   • Enter the SSID

Step 3 Click on the WLAN Security tab and configure the following:
   • Enable MAC Filtering
   • Select Security Type as WPA2 Enterprise
   • Select Authentication Server as External RADIUS
   • Select RADIUS Compatibility from the drop-down list
Creating Guest WLANs

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

Creating Guest WLAN with Captive Portal on CMX Connect

Procedure

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

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

• Enter the Profile Name
• Enter the SSID

Step 3 Enable the Guest Network under the WLAN Security tab.

Step 4 Select Captive Portal as CMX Connect.

Step 5 Enter Captive Portal URL.

Note Captive Portal URL must have the following format: https://yya7lc.cmxcisco.com/visitor/login where yya7lc is your Account ID.

Step 6 Click Apply.

Note Additional steps are required on CMX Cloud to create the Captive Portal, Site with Access Points and associating Captive Portal to the Site.
Creating Guest WLAN with Internal Splash Page

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

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

1. Local User Account
2. Web Consent
3. Email Address
4. RADIUS
5. WPA2 Personal

Procedure

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

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

- Enter the Profile Name
- Enter the SSID

**Step 3** Enable the Guest Network under the WLAN Security tab.

**Step 4** Select Captive Portal as Internal Splash Page.

**Step 5** Select one of the following Access Type as needed:

1. Local User Account—Splash Page will present the user to enter username and password which must be authenticated by the controller before network access is granted. Local WLAN users must be created on the controller to onboard the Guest clients.

2. Web Consent—Splash Page will present the user to acknowledge before network access is granted.

3. Email Address—Splash Page will present the user to enter the email address before network access is granted.

4. RADIUS—Splash Page will present the user to enter username and password which must be authenticated by the RADIUS server before network access is granted. Select Access Type as RADIUS and enter the RADIUS server configuration.

5. WPA2 Personal—This is an example of L2 + L3 (Web Consent). Layer 2 PSK security authentication will happen first followed by Splash Page which will present the user to acknowledge before network access is granted. Select Access Type as WPA2 Personal and enter the Passphrase.

**Step 6** Click Apply.
Creating Guest WLAN with External Splash Page

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

1. Local User Account
2. Web Consent
3. Email Address
4. RADIUS
5. 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 tab, configure the following:
   - Enter the Profile Name
   - Enter the SSID

**Step 3** Enable the Guest Network under the WLAN Security tab.

**Step 4** Select Captive Portal as External Splash Page.

**Step 5** Select one of the following Access Type as needed:

1. Local User Account—Splash Page will present the user to enter username and password which must be authenticated by the controller before network access is granted. Local WLAN users must be created on the controller to onboard the Guest clients.

2. Web Consent—Splash Page will present the user to acknowledge before network access is granted.

3. Email Address—Splash Page will present the user to enter the email address before network access is granted.

4. RADIUS—Splash Page will present the user to enter username and password which must be authenticated by the RADIUS server before network access is granted. Select Access Type as RADIUS and enter the RADIUS server configuration.

5. WPA2 Personal—This is an example of L2 + L3 (Web Consent). Layer 2 PSK security authentication will happen first followed by Splash Page which will present the user to acknowledge before network access is granted. Select Access Type as WPA2 Personal and enter the Passphrase.

**Step 6** Click Apply.
Internal Splash Page for Web Authentication

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

Using default internal guest portal

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

**Procedure**

**Step 1** Navigate to Wireless Settings > Guest WLANs.

**Step 2** Configure the following on the Guest WLAN page:

- **Page Type**—Select as Internal (Default).
- **Preview**—You can Preview the page by clicking on the Preview button.
- **Display Cisco Logo**—To hide the Cisco logo that appears in the top right corner of the default page, you can choose No. This field is set to Yes by default.
- **Redirect URL After Login**—To have the guest users redirected to a particular URL (such as the URL for your company) after login, enter the desired URL in this text box. You can enter up to 254 characters.
- **Page Headline**—To create your own headline on the login page, enter the desired text in this text box. You can enter up to 127 characters. The default headline is Welcome to the Cisco Wireless Network.
- **Page Message**—To create your own message on the login page, enter the desired text in this text box. You can enter up to 2047 characters. The default message is Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.

**Step 3** Click Apply.

Using customized internal guest portal

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

**Procedure**

**Step 1** Navigate to Wireless Settings > Guest WLANs.

**Step 2** Configure the following on the Guest WLAN page:

- **Page Type**—Select as Customized.
Managing WLAN Users

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

To create local user accounts, follow the procedure below:

Procedure

Step 1 Navigate to Wireless Settings > WLAN Users and then click on Add WLAN User button.

Step 2 Configure the following for the WLAN user:

- **User Name**—Enter the username
- **Guest User**—For Guest user, enable the Guest User checkbox
- **Lifetime**—For Guest User, define the user account validity. Default is 86400 seconds (or, 24 hours) from the time of its creation.
- **WLAN Profile**—Select the WLAN to which the user will connect
- **Password**—Enter the password for the user account
- **Description**—Additional details or comments for the user account
- Click on tick icon.

Adding MAC for Local MAC Filtering on WLANs

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Navigate to <strong>Wireless Settings</strong> &gt; <strong>WLAN Users</strong> and click on <strong>Local MAC Addresses</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click <strong>Add MAC Address</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Add MAC Address</strong> window, configure the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>MAC Address</strong>—Enter the MAC Address of the device</td>
</tr>
<tr>
<td></td>
<td>• <strong>Description</strong>—Enter the description</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>—Select whether this MAC has to be WhitleList or BlackList</td>
</tr>
<tr>
<td></td>
<td>• <strong>Profile Name</strong>—Select the WLAN to which the user will connect</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>
Managing Services with Cisco Mobility Express

There are a number of services supported in a Cisco Mobility Express deployment. In this section, the following Services will be covered.

- Application Visibility and Control, page 51
- iOS Optimized WiFi connectivity and Fast Lane, page 52
- Cisco Mobility Express with CMX Cloud, page 55

Application Visibility and Control

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

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

Enabling Application Visibility on WLAN

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

Procedure

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

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

Adding Application Control from Network Summary Page

Procedure

Step 1 Add the Applications widget on the Network Summary Page. To add the Applications widget, click on the + icon on the right of the Network Summary banner. Select the Applications widget. The Applications widget will display the top 10 applications being browsed by the clients in the Mobility Express network.

Step 2 Click on the application you wish to add control. The Add AVC Rule window will pop up. Select the Action. Action can be Mark, Drop or Rate Limit. For Mark, one can select DSCP as Platinum, Gold, Silver, Bronze or Custom. If custom is selected, one has to specify the DSCP value. For Rate Limit, one can specify the Average Rate and Burst Rate for the application.

Step 3 Select one or more AVC Profile/SSID combinations.

Step 4 Click Apply.

Adding Application Control from Applications Page

Procedure

Step 1 Navigate to Monitoring > Applications Page.

Step 2 Click on the application you wish to add control. The Add AVC Rule window will pop up. Select the Action. Action can be Mark, Drop or Rate Limit. For Mark, one can select DSCP as Platinum, Gold, Silver, Bronze or Custom. If custom is selected, one has to specify the DSCP value. For Rate Limit, one can specify the Average Rate and Burst Rate for the application.

Step 3 Select one or more AVC Profile/SSID combinations.

Step 4 Click Apply.

iOS Optimized WiFi connectivity and Fast Lane

Configuring Optimized WiFi Connectivity

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

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

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

**Procedure**

**Step 1** Enable **Expert View** on Cisco Mobility Express. **Expert View** is available on the top banner of the Cisco Mobility Express WebUI as shown below and enabled various configurable parameters which are not available in Standard view.

![Expert View](image)

**Step 2** Navigate to **Wireless Settings > WLANs**. On the **Add new WLAN** or **Edit WLAN** window, click on the **Advanced** tab. Configure 802.11k, r, v as needed on this page.
Configuring Fast Lane

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

• Your WLC QoS configuration is optimized globally to better support real-time applications
• iOS 10 devices can send upstream voice traffic without the requirement to perform WMM TSPEC/TCLAS negotiation. The infrastructure will honor the voice marking for these devices.
• You can apply a QoS profile to your iOS 10 devices, and decide which applications should receive QoS marking upstream, and which applications should be sent as best effort or background.

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

**Step 1**  
Login to the controller CLI.

**Step 2**  
Enable Fast Lane using the CLI below:

(Cisco Controller) > config qos fastlane enable 1

Warning: This command will temporarily disable all WLANs and Networks. Active WLANs and networks will be re-enabled automatically after the configuration completes.

This command will also override the file named AUTOQOS-AVC-PROFILE, if it exists, and will apply it to the WLAN, if Application Visibility is enabled.

Are you sure that you want to continue? (y/N) y

---

**Cisco Mobility Express with CMX Cloud**

**Cisco CMX Cloud**

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

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

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

**Cisco CMX Cloud Solution Compatibility Matrix**

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

**Minimum requirements for Cisco CMX Cloud deployment**

Below are the minimum requirements for CMX Cloud deployment:

2. Recommended browser is Chrome 45 or later.
3. Signup at https://cmxcisco.com for 60 day trial or go to Cisco Commerce Workspace (CCW) and purchase license for your choice of CMX Cloud service
Enabling CMX Cloud Service on Mobility Express for Presence Analytics

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

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>On Cisco Mobility Express WebUI, navigate to Advanced &gt; CMX.</td>
</tr>
<tr>
<td>2</td>
<td>Enter the CMX Server URL (Site URL).</td>
</tr>
<tr>
<td>3</td>
<td>Enter the CMX Server Token (Account Token).</td>
</tr>
</tbody>
</table>
| 4    | Click Apply.  
**Tip**  
Click the Test Link button to verify connectivity from Master AP to CMX Cloud Site using the configured information. |

Configuring Site on CMX Cloud for Presence Analytics

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

**Procedure**

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

- Managing Access Points, page 57
- Adding Access Points to Cisco Mobility Express Network, page 58
- Configuring Management Access, page 59
- Managing Admin Accounts, page 60
- Managing TIME on Cisco Mobility Express, page 61
- Updating Cisco Mobility Express Software, page 62

Managing Access Points

Starting Release 8.4, Cisco Mobility Express supports up to 100 Access Points. To view the list or modify parameters on an Access Points, follow the procedure below:

Procedure

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

*Note*  The first Access Point with the *P* icon is the Master AP and the rest of them are Subordinate Access Points.

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

- Operating Mode(Read only field)-For a master AP, this field displays AP & Controller. For other associated APs, this field displays AP only.
- AP Mac(Read only field)--Displays the MAC address of the Access Point.
- AP Model(Read only field)-Displays the model details of the Access Point.
• IP Configuration—Choose Obtain from DHCP to allow the IP address of the AP be assigned by a DHCP server on the network, or choose Static IP address. If you choose Static IP address, then you can edit the IP Address, Subnet Mask, and Gateway fields.

• AP Name—Edit the name of access point. This is a free text field.

• Location—Edit the location for the access point. This is a free text field.

**Step 3** Under the Controller tab (Available only for Master AP), one can modify the following parameters:

- System Name—Enter the System Name for Mobility Express
- IP Address—IP address decides the login URL to the controller's web interface. The URL is in https://<ip address> format. If you change this IP address, the login URL also changes.
- Subnet Mask—Enter the Subnet Mask.

**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.

- 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.

---

**Adding Access Points to Cisco Mobility Express Network**

When adding Access Points to Cisco Mobility Express network, the following have to be considered:
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 Master AP, a software download of the code running on the Master Access Point has to happen on the Access Point being added. For the new Access Point to download the code that is running on the Master Access Point, one of the following has to be configured:

- TFTP server details and the Access Point images path information has to be configured on the Software Update page.
- If the Master 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 Access Point will be automatically downloaded from cisco.com when an Access Point joins.

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

Procedure

Step 1 Download the Access Point image 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 individual Access Point images.

Step 2 Navigate to Management > Software Update. Select TFTP for Transfer Mode and configure the TFTP Parameters.

(OR)

Step 3 Navigate to Management > Software Update. Select Cisco.com as the Transfer Mode and configure parameters related to the Cisco.com user account.

Step 4 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 Master AP, it joins. However, if the version on the AP being added is different than then one on the Master 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 Master 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 Master AP.

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, follow the procedure below:

**Procedure**

**Step 1** Navigate to Management > Access.

**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 Apply to submit changes.

---

**Managing Admin Accounts**

Cisco Mobility Express supports creation of admin accounts to prevent unauthorized users from reconfiguring the controller and viewing configuration. It supports the following three access levels for Admin user accounts:

1 Read/Write—Accounts with read and write privilege have full provisioning and monitoring capability
2 Read only—Accounts with Read only privilege only have monitoring capability and can browse all screens
3 Lobby Ambassador—A Lobby Ambassador can create and manage guest user accounts on the Cisco Mobility Express. The lobby ambassador has limited configuration privileges and can access only the web pages used to manage the guest accounts.

**Note** The local user database is limited to a maximum of 2048 entries, which is also the default value. This database is shared by local management users (including lobby ambassadors), local network users (including guest users), MAC filter entries, exclusion list entries. Together they cannot exceed the maximum value.

To create admin users, follow the procedure 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.

- **Account Name**—Enter the admin user name. Username is case-sensitive and can contain up to 24 ASCII characters. Username cannot contain spaces and must be unique.
• **Access** - Select Read/Write, Read Only or Lobby Ambassador access for the admin account.

• **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.

**Step 3** Click tick icon.

---

**Managing TIME on Cisco Mobility Express**

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

**Configuring NTP Server**

Up to three Network Time Protocol (NTP) servers can be configured to sync date and time if one was not configured during the Wireless Express setup. Time Zone can be configured to offset the clock.

To configure Time Zone and NTP servers, follow the procedure below:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Navigate to Management &gt; Time.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose the desired Time Zone.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the NTP Polling Interval. The polling interval ranges from 3600 to 604800 seconds.</td>
</tr>
<tr>
<td>Step 4</td>
<td>To add an NTP server, click Add NTP Server button and configure the following:</td>
</tr>
</tbody>
</table>
  - **NTP Index** – It can be 1, 2 or 3. |
  - **NTP Server** - This can be the NTP Server IP address, NTP Server Name or pool. A maximum of three NTP Servers are supported. |
• Click **tick** icon.

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

---

**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.

An AP joining the controller compares its software version with the Master AP version and in case of mismatch, the new AP requests for a software update. For software update, one must configure the **Transfer Mode** and corresponding details on the Software Update page.

**Note**  
Master AP does not have AP images. It facilitates the transfer of new software from the configured **Transfer Mode** to the Access Points requesting for Software Update.

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 Access Points requiring upgrade have downloaded the new image.

Starting Release 8.3.100.0, Cisco Mobility Express supports the following **Transfer Mode** for Software Update:

- **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.

- **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 Transfer Method** should be used.

TFTP–TFTP transfer mode can be used to perform Software Update on a Mobility Express Network. Master AP facilitates transfer of image from the TFTP server to the individual Access Points. 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.
Software Update using cisco.com Transfer Mode

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

- Internet access is required for software download from cisco.com to APs. However, no proxy is required.
- A valid cisco.com (CCO) account with username & password required.
- EULA acceptance on a per user basis. Only Master 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.

In order to perform Software Update using cisco.com Transfer Mode, follow the procedure below:

Procedure

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

- Select Cisco.com for Transfer Mode.
- Enter Cisco.com Username.
- Enter Cisco.com Password.
- Enable Automatically Check for Updates. Check is done once in 30 days.
- Click on the Check Now button to retrieve the Latest Software Release and the Recommended Software Release from Cisco.com.

Step 2
Click Apply.

Step 3
Click Update to initiate software update wizard.

Step 4
In the Software Update Wizard, select the Recommended Software Release or Latest Software Release. Click Next.

Step 5
Select Update Now to initiate software update immediately or Schedule the Update for Later. 
Note: If Schedule the Update for Later is selected, configure the Set Update Time field.

Step 6
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 Next.

Step 7
Click Confirm to start the software update. 
To monitor the download progress on individual Access Points, expand the Predownload image status.
Software Update using HTTP Transfer Mode

If you have the same model of Access Points in the Mobility Express deployment, HTTP Transfer mode can be used to perform Software Update. For HTTP Transfer mode, one can simply upload the Access Point upgrade image from the local machine. To perform Software Update using HTTP Transfer Mode, follow the procedure below:

Procedure

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

**Step 2**

<table>
<thead>
<tr>
<th>Access Point</th>
<th>Access Point image bundle. Contains individual AP images to be used for Software Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Aironet® 1560 Series</td>
<td>AIR-AP1560-K9-ME-8-4-100-0.zip</td>
</tr>
<tr>
<td>Cisco Aironet® 1815I Series</td>
<td>AIR-AP1815-K9-ME-8-4-100-0.zip</td>
</tr>
<tr>
<td>Cisco Aironet® 1815W Series</td>
<td>AIR-AP1815-K9-ME-8-4-100-0.zip</td>
</tr>
<tr>
<td>Cisco Aironet® 1830 Series</td>
<td>AIR-AP1830-K9-ME-8-4-100-0.zip</td>
</tr>
<tr>
<td>Cisco Aironet® 1850 Series</td>
<td>AIR-AP1850-K9-ME-8-4-100-0.zip</td>
</tr>
<tr>
<td>Cisco Aironet® 2800 Series</td>
<td>AIR-AP2800-K9-ME-8-4-100-0.zip</td>
</tr>
<tr>
<td>Cisco Aironet® 3800 Series</td>
<td>AIR-AP3800-K9-ME-8-4-100-0.zip</td>
</tr>
</tbody>
</table>

**Note** The above images are for AireOS Release 8.4.100.0. The image bundle would be different for different releases.

**Step 3**
Unzip the AP Image bundle to extract individual AP Images. Mapping of Access Points to their corresponding images is shown below:

<table>
<thead>
<tr>
<th>Access Point</th>
<th>Access Point Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Aironet® 1560 Series</td>
<td>ap3g3</td>
</tr>
<tr>
<td>Cisco Aironet® 1815I Series</td>
<td>ap1g5</td>
</tr>
<tr>
<td>Cisco Aironet® 1815W Series</td>
<td>ap1g5</td>
</tr>
<tr>
<td>Cisco Aironet® 1830 Series</td>
<td>ap1g4</td>
</tr>
<tr>
<td>Cisco Aironet® 1850 Series</td>
<td>ap1g4</td>
</tr>
<tr>
<td>Cisco Aironet® 2800 Series</td>
<td>ap3g3</td>
</tr>
<tr>
<td>Cisco Aironet® 3800 Series</td>
<td>ap3g3</td>
</tr>
</tbody>
</table>

**Step 4**
To perform Software Update via HTTP Transfer Mode, navigate to Management > Software Update and configure the following:

- Select HTTP for Transfer Mode
Software Update using TFTP Transfer Mode

Software Update via TFTP Transfer Mode works for all Access Points supported in a Cisco Mobility Express Deployment. You would need a TFTP server which can communicate with the Master Access Point to use this upgrade method. This update method is supported from controller WebUI as well as CLI.

Upgrading from WebUI

To perform Software Update using TFTP Transfer mode from WebUI, follow the procedure below:

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 Transfer Mode, navigate to Management > Software Update and configure the following:

- Select TFTP for Transfer Mode.
- Enter the IP Address of the TFTP server in the IP Address (IPv4) field.
- Enter the File Path to the unzipped AP images on the TFTP Server.

Note The most common mistake made is entering this path correctly. It is important that this path be entered correctly before going to the next step. Do not point to individual AP image. You need to only point to the directory which contains the AP images.

Step 4 Click Apply.
Step 5 Click Update Now to initiate software update.

Note To Schedule Update at a later time, user must select a date and time in Set Update Time field and then click on the 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.
Upgrading from CLI

Procedure

**Step 1** Login to AP running Mobility Express controller via SSH or Telnet(if it is enabled).

**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* The most common mistake made is entering this path correctly. It is important that this path be entered correctly before going to the next step. Do not point to individual AP image. You need to only point to the directory which contains the AP images.

**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

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Primary Image</th>
<th>Backup Image</th>
<th>Predownload Status</th>
<th>Predownload Version</th>
<th>Next Retry</th>
<th>Retry Count</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP6412.256e.0e78</td>
<td>8.1.112.21</td>
<td>8.1.112.21</td>
<td>Predownloading</td>
<td>8.1.112.21</td>
<td>NA</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>APAOEC.F96C.D640</td>
<td>8.1.112.21</td>
<td>8.1.112.21</td>
<td>Predownloading</td>
<td>8.1.112.21</td>
<td>NA</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>3600-gemini</td>
<td>8.1.112.21</td>
<td>8.1.112.21</td>
<td>Predownloading</td>
<td>8.1.112.21</td>
<td>NA</td>
<td>NA</td>
<td></td>
</tr>
</tbody>
</table>
Step 8  Wait for the pre-image download to complete on the Access Points.

(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

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Primary</th>
<th>Backup</th>
<th>Predownload</th>
<th>Predownload</th>
<th>Next Retry</th>
<th>Retry Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP6412.256e.0e78</td>
<td>8.1.112.21</td>
<td>8.1.112.21</td>
<td>Complete</td>
<td>—</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>APAOEC.F96C.D640</td>
<td>8.1.112.21</td>
<td>8.1.112.21</td>
<td>Complete</td>
<td>—</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>3600-gemini</td>
<td>8.1.112.21</td>
<td>8.1.112.21</td>
<td>Complete</td>
<td>—</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

Step 9  After the pre-download is complete, issue a reset system as shown below.

(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!

Managing Advanced RF Parameters

Cisco Mobility supports a number RF Parameters which can be configured the administrator to optimize their network deployment. To manage advanced RF Parameters, follow the procedure below:

Procedure

Step 1  Enable Expert View on Cisco Mobility Express. Expert View is available on the top banner of the Cisco Mobility Express WebUI as shown below and enabled various configurable parameters which are not available in Standard view.

Step 2  Under Advanced RF Parameters, the following parameters are available:

- **2.4 GHz Band** - This is a global setting and can be enabled or disabled.
- **5.0 GHz Band** - This is a global setting and can be enabled or disabled.
- **Automatic Flexible Radio Assignment** - If there are 2800 and 3800 series access points in the Cisco Mobility Express deployment which supports Flexible Radio Assignment, one can choose to enable or disable it.
- **Optimized Roaming** - This is a global setting and can be enabled or disabled.
• **Event Driven RRM**—This is a global setting and can be enabled or disabled.

• **CleanAir Detection**—CleanAir is supported on 2800 and 3800 series access points and one can choose to enable or disable it.

• **5.0 GHz Channel Width**—Global setting is configured to best but one can select 20, 40, 80 or 160 MHz for channel width.

• **2.4 GHz Data Rates**—Move the slider to disable/enable data rates in the 2.4 GHz band

• **5.0 GHz Data Rates**—Move the slider to disable/enable data rates in the 5.0 GHz band

• **Select DCA Channels**—One can select (click on individual channels) the channels to be included in DCA for both 2.4 GHz and 5.0 GHz band

**Note** Green with an underline below the channel indicates that it is selected.

**Step 3** Click **Apply**.
Master AP Failover and Electing a new Master

Cisco Mobility Express is supported on Cisco 1560, 1815I, 1815M, 1815W, 1830, 1850, 2800 and 3800 series Access Points. If you have a mix of these Access Points in a Cisco Mobility Express deployment, the Master AP election process determines which of the supported Access Point will be elected to run Mobility Express controller function in case of a Failover of the Active Master AP. VRRP is used to detect the failure of Master AP which initiates the election of a new Master.

**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.

- Master AP Failover, page 69
- Electing a new Master Access Point, page 70

Master 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 Master AP, another Mobility Express capable AP is elected as a Master automatically. The newly elected Master AP has the same IP and configuration as the original Master AP.

**Note**

Given Access Point models support different scale limits in terms of the number of Access Points supported, it is highly recommended to have at least two or more Access Points which support the same scale limits. For example, if you need to support scale of 100 Access Points, you should have at least two or more of either 3800, 2800 or a combination of both.

**Note**

Access Points, which have the Mobility Express Image but AP Configuration, is NOT MOBILITY EXPRESS CAPABLE, will not participate in the Master AP election process.
Electing a new Master Access Point

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

Note
During the Master Election process, even though the Master 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 Master is elected, the Standalone Access points will move to connected mode.

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

Procedure

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

a) Navigate to Wireless Settings > Access Points.

b) From the list of Access Points, click Edit icon of the Access Point which you would like to select as the Master AP.

c) Under the General tab, click on Make me Controller button.

d) Click Yes on the Confirmation window.

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

Step 2 Next Preferred Master - Admin can configure the Next Preferred Master from CLI. When this is configured and the active Master AP fails, the one configured as the Next Preferred Master will be elected as a Master.

To configure the Next Preferred Master, follow the procedure below:

a) Login to the CLI of the controller.

b) Execute the following CLI:

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

(Cisco Controller) >config ap next-preferred-master <Cisco AP>

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

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

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

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

Step 3 Most Capable Access Point– If the first two priorities are not configured, Master AP election algorithm will select the new Master based on the capability of the Access Point. For example, 3800 is the most capable followed by 2800, 1850, 1830 and finally the 1815 Series.

Note All 1815 Series Access Points have the same capability.
Step 4  **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 Master Access Point.

Step 5  **Lowest MAC Address**– If all of the Access Points are the same and have the same client load, then Access Point with the lowest MAC will be elected as a Master.
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, page 74
Adding Mobility Express to Prime

Perform the following steps to add the controllers:

**Procedure**

**Step 1** Login to Cisco Prime

![Cisco Prime Infrastructure login screen]

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

![Add Device screen]

**Step 3** Enter the IP address of the Mobility Express controller.
**Step 4** Enter the SNMP Parameters and click Add.
You must configure the SNMP community strings on the Mobility Express controller prior to adding the device in Prime.

**Note**

**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 templates need to be saved.

![Save Template dialog](image)

**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
Adding Mobility Express to Prime