CHAPTER 13

Cisco Mobility Express AireOS® Release 8.5

Solution Overview

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. 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 a virtual Wireless LAN controller function embedded on 802.11ac Wave 2 access points
- Is ideal for small and medium-sized deployments of up to 100 access points
- Is supported on Cisco Aironet® 1540, 1560, 1815W, 1815I, 1815M, 1830, 1850, 2800 and 3800 Series 802.11ac Wave 2 access points
- Can control other Aironet® access points, such as the 1810W, 1700, 2700, and 3700 etc.
- Provides simple over-the-air deployment in under 10 minutes. In addition, one can use Network Plug and Play to deploy the Wireless LAN controller and bring up a new site
- Can be used to perform Site Survey

Interoperability

- AireOS® Release - Recommended is AireOS® 8.4.100.0 or later.
- Cisco Prime Infrastructure - Prime Infrastructure Release 3.0.1 and later. Please deploy Prime Infrastructure version which is compatible with AireOS® Release running on Mobility Express.
- Connected Mobility Experiences (CMX) – CMX Connect and CMX Presence Analytics is supported for both On-Prem and CMX cloud deployments. For On-Prem, use CMX 10.3 or later. Please deploy CMX On-Prem version which is compatible with AireOS® Release running on Mobility Express.
- Cisco Identity Services Engine (ISE) - ISE Release 1.2 and later. 802.1x authentication is supported.

Mobility Express Access Points

Cisco Mobility Express solution consists of the following components:

- **Master Access Point**-Cisco Aironet® Access Point which runs the virtual Wireless LAN Controller function is called the Master AP. In addition to running the virtual Wireless LAN Controller function, it can also service clients at the same time.
- **Subordinate Access Point**-Cisco Aironet® Access Points which are managed by Master Access Point in a Mobility Express network and only service clients are called Subordinate Access Points. Subordinate Access Points do not actively run the Wireless LAN Controller function even though they may be capable of running the Wireless LAN Controller function.

There are two parameters which ensures an Access Points can run the Wireless LAN Controller function. These parameters are displayed in the **AP#show version** output of the access point. They are as follows:

- AP Image type
- AP Configuration

For an Access Point to run the Wireless LAN Controller function, the two parameters must have the following value:

- AP Image type: MOBILITY EXPRESS IMAGE
- AP Configuration: MOBILITY EXPRESS CAPABLE

Note On an Access Point with CAPWAP image, the two parameters are not displayed in the **AP#show version** output.

Master Access Points

Master AP running the virtual Wireless LAN controller function is the central point for management and control. Access Points capable of running the Wireless LAN Controller function are listed in the table below.

Table 13-1 Cisco Aironet® Access Points capable of operating as Master Access Points

Master Access Points	Supported Model Numbers
Cisco Aironet® 1540 Series	AIR-AP1540I-x-K9C AIR-AP1540D-x-K9C
Cisco Aironet® 1560 Series	AIR-AP1562I-x-K9C AIR-AP1562E-x-K9C AIR-AP1562D-x-K9C
Cisco Aironet® 1815I Series	AIR-AP1815I-x-K9C
Cisco Aironet® 1815M Series	AIR-AP1815M-x-K9C
Cisco Aironet® 1815W Series	AIR-AP1815W-x-K9C
Cisco Aironet® 1830 Series	AIR-AP1832I-x-K9C

Table 13-1 Cisco Aironet® Access Points capable of operating as Master Access Points

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

Note NOTE: The -x- in the other model numbers is a placeholder for the actual letter indicating the model's regulatory domain.

Subordinate Access Points

Subordinate AP(s) are managed by Master AP in a Mobility Express network and only service clients. There are two categories of Subordinate AP(s). The first category is the list of Subordinate AP(s) which are capable of running Wireless LAN controller function and second category is the list of Subordinate AP(s) which are not capable of running the Wireless LAN controller function. Access Points capable of operating as Subordinate AP(s) are listed in the table below.

Table 13-2 Subordinate Access Points and capability

Subordinate Access Points	Supported Model Numbers	Capability
Cisco Aironet® 700i Series	AIR-CAP702I-x-K9	Cannot run Mobility Express
Cisco Aironet® 700w Series	AIR-CAP702W-x-K9	Cannot run Mobility Express
Cisco Aironet® 1540 Series	AIR-AP1540I-x-K9 AIR-AP1540D-x-K9	Can run Mobility Express
Cisco Aironet® 1560 Series	AIR-AP1562I-x-K9 AIR-AP1562E-x-K9 AIR-AP1562D-x-K9	Can run Mobility Express
Cisco Aironet® 1600 Series	AIR-CAP1602I-x-K9 AIR-CAP1602E-x-K9	Cannot run Mobility Express
Cisco Aironet® 1700 Series	AIR-CAP1702I-x-K9	Cannot run Mobility Express

Table 13-2 Subordinate Access Points and capability

Subordinate Access Points	Supported Model Numbers	Capability
Cisco Aironet® 1810 Series	AIR-AP1810W-x-K9	Cannot run Mobility Express
Cisco Aironet® 1815I Series	AIR-AP1815I-x-K9	Can run Mobility Express
Cisco Aironet® 1815M Series	AIR-AP1815M-x-K9	Can run Mobility Express
Cisco Aironet® 1815W Series	AIR-AP1815W-x-K9	Can run Mobility Express
Cisco Aironet® 1830 Series	AIR-AP1832I-x-K9	Can run Mobility Express
Cisco Aironet® 1850 Series	AIR-AP1852I-x-K9 AIR-AP1852E-x-K9	Can run Mobility Express
Cisco Aironet® 2600 Series	AIR-CAP2602I-x-K9 AIR-CAP2602E-x-K9	Cannot run Mobility Express
Cisco Aironet® 2700 Series	AIR-CAP2702I-x-K9 AIR-CAP2702E-x-K9	Cannot run Mobility Express
Cisco Aironet® 2800 Series	AIR-AP2802I-x-K9 AIR-AP2802E-x-K9	Can run Mobility Express
Cisco Aironet® 3600 Series	AIR-CAP3602I-x-K9 AIR-CAP3602E-x-K	Cannot run Mobility Express
Cisco Aironet® 3700 Series	AIR-CAP3702I-x-K9 AIR-CAP3702E-x-K9	Cannot run Mobility Express
Cisco Aironet® 3800 Series	AIR-AP3802I-x-K9 AIR-AP3802E-x-K9	Can run Mobility Express

Note The -x- in the other model numbers is a placeholder for the actual letter indicating the model's regulatory domain.

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.

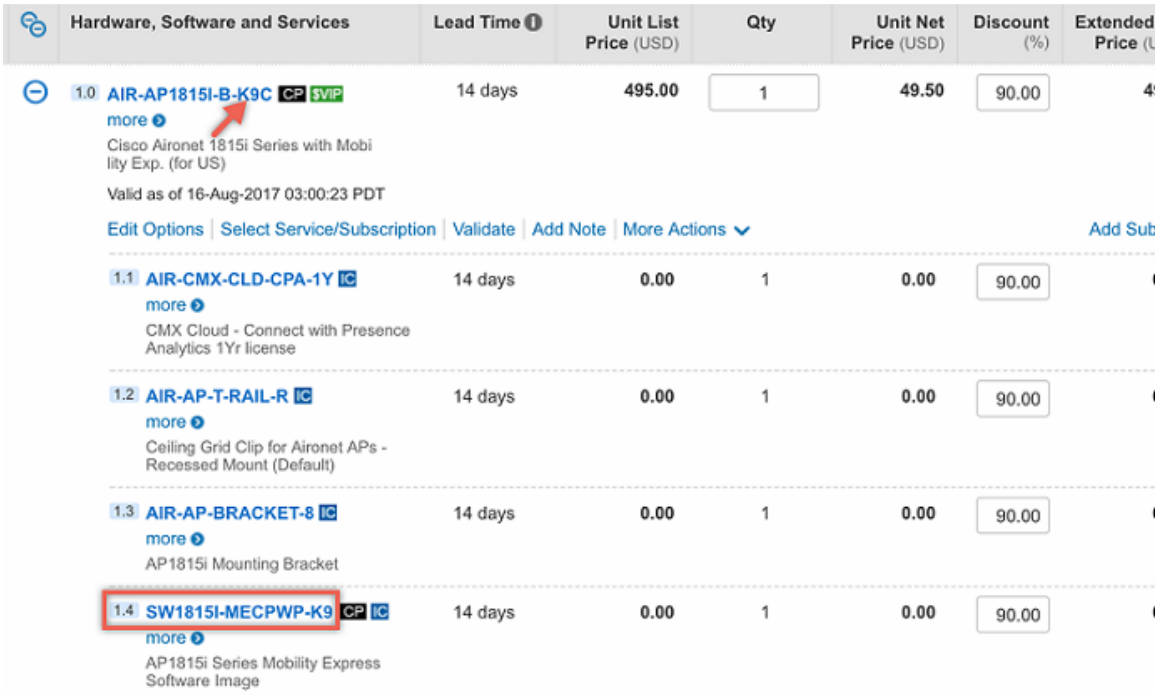
Table 13-3 Cisco Mobility Express Scale Limits

Master Access Points	No. of Access Points Supported	No. of Clients Supported
Cisco Aironet® 1540 Series	50	1000
Cisco Aironet® 1540 Series	100	2000
Cisco Aironet® 1815I Series	50	1000
Cisco Aironet® 1815M Series	50	1000
Cisco Aironet® 1815W Series	50	1000
Cisco Aironet® 1830 Series	50	1000
Cisco Aironet® 1850 Series	50	1000
Cisco Aironet® 2800 Series	100	2000
Cisco Aironet® 3800 Series	100	2000

Ordering Access Points with Cisco Mobility Express

Access Points capable of running Wireless LAN controller can be ordered with Cisco Mobility Express image pre-installed on the Access Points. To order such an Access Point, please select the Access Point SKU (Stock Keeping Unit) which ends with K9C when placing the order.

For example (refer to image below), to order an 1815I Access Point for the -B regulatory domain, select AIR-AP1815I-B-**K9C**. Under the options, verify that **SW1815I-MECPWP-K9** (Mobility Express Software Image) is also selected.



If you wish to order Access Points with CAPWAP image, do not select the Access Point SKU (Stock Keeping Unit) which ends with K9C when placing the order. If you wish to order Access Points with CAPWAP image, SKU (Stock Keeping Unit) ending with **K9** should be selected when placing the order.

Please note that an Access Point with CAPWAP image can also be converted to run Wireless LAN Controller function by installing the Mobility Express image. Conversely, Access Point with Mobility Express image can be converted to run as CAPWAP by migrating them to appliance or vWLC based deployment.

Deploying Cisco Mobility Express

After you have Access Points with Mobility Express image, configuring the Wireless LAN Controller on the Access Point is a simple process. There are multiple ways one can configure a Cisco Mobility Express controller. They are as follows:

1. CLI Setup Wizard
2. Over-the-Air Provisioning setup wizard
3. Network Plug and Play

In this chapter, we will configure the Wireless LAN Controller via Over-the-Air Provisioning setup wizard.

Pre-requisites

1. Decide on the Access Point to be configured as the Master AP which will run the Wireless LAN Controller function. After the Master AP is configured and operational, additional APs can be added to the Mobility Express network. Please note that additional APs must have the same software version as the Master AP for them to join.
2. Decide on DHCP server. Will you be using an external DHCP server (ex. on a switch or router) for access points and clients or will you be using internal DHCP server on Mobility Express.

Note Please note that mix of internal and external DHCP server is not supported.

If you plan to use an external DHCP server, configure that first before connecting the Master AP. If you want to use the internal DHCP server, you can configure it in Day 0 Setup Wizard. Please note that internal DHCP server is typically used for Site Survey so using an External DHCP server for Access Points and client is recommended unless there is a reason not to.

Configuring switch ports

In a Mobility Express deployment, all clients are centrally authenticated and data traffic is locally switched by the access point including Master AP which also service clients. The switch ports to which Access Points will connect can be an access port or a trunk port. It is recommended to use a trunk port because it enables management traffic and client data traffic to be segmented across separate VLANs. If you do not wish to segment management and client data traffic, configure the switch ports as access ports.

In this guide, we will use an external DHCP sever and different VLANs for management traffic and client data traffic. Given below is an example of a switch port configuration for access points.

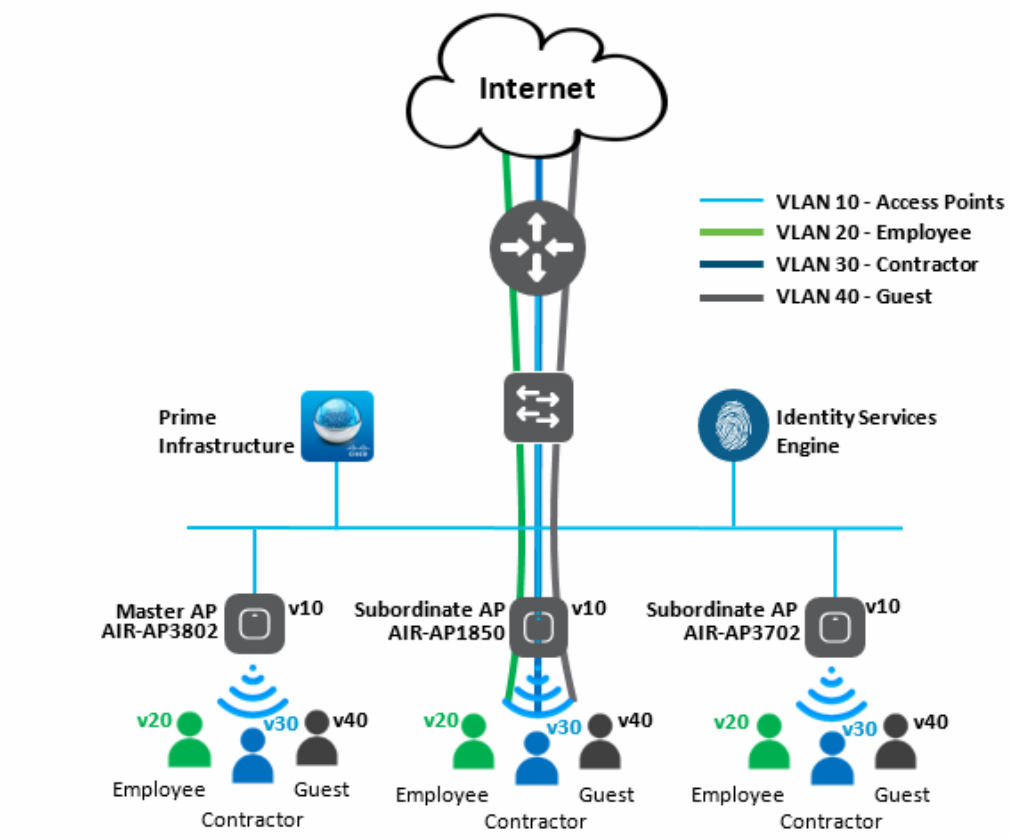
```
interface GigabitEthernet1/0/37
description » Connected to Master AP «
switchport trunk native vlan 10
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk

interface GigabitEthernet1/0/38
```

```
description » Connected to Subordinate AP-Lobby«
switchport trunk native vlan 10
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk
```

In the above example, all Access Points will get an IP address in native VLAN 10. Management IP address of Wireless LAN Controller will also be in VLAN 10 which must be configured during Day 0. Client Data traffic will be in VLAN 20, 30 and 40.

Note In a Mobility Express deployment, all access points must be in the same VLAN.



Connecting Access Points to switch ports

Connect your designated Master AP to the switch port. If the switch port supports PoE+, access point can be powered via the switch port else use the applicable power supply or a power injector for the Access Points.

During boot up, access point will obtain an IP address via DHCP. After it has obtained an IP address, it will start the Wireless LAN Controller function in Day 0.

If multiple access points capable of running the Wireless LAN Controller function are connected to the switch ports simultaneously, one of them would be elected as a designated Master AP and it will start the Wireless LAN Controller function in Day 0.

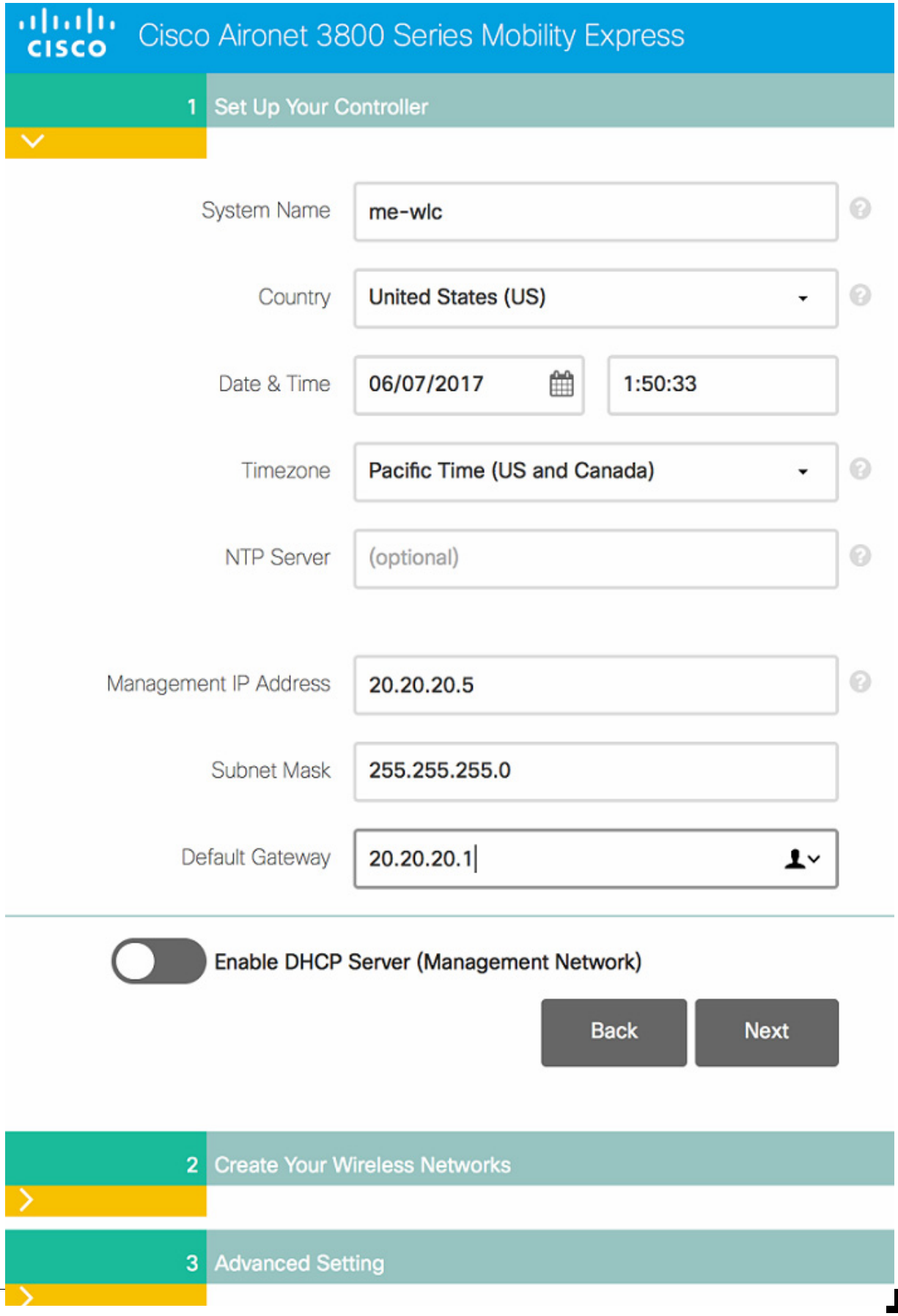
After the Wireless LAN Controller function has started in Day 0, it will broadcast the **CiscoAirProvision** SSID.

Configuring the Master AP

Follow the steps below to configure Wireless LAN controller on the designated Master AP.

1. Power up the Master AP by connecting it to the PoE enabled switch port or using an external power source.
2. After the AP had finished rebooting, it will broadcast the **CiscoAirProvision** SSID.Depending on the AP, this can take upto 10 min.
3. Connect your WiFi enabled laptop to the **CiscoAirProvision** SSID. When prompted for password enter **password**.
4. Open a web browser and access mobilityexpress.cisco to navigate to the Setup Wizard.

5. Configure the admin account for the Wireless LAN Controller by entering the username and password. Enter password again to confirm it and click on the **Start** button.
6. In the **Set up your controller** section, enter **System Name** and **Country**. **Date & Time** will be automatically filled from your browser or one can optionally enter the NTP server. If NTP server is left blank, three NTP pools will automatically be configured. Enable the **IP Management** and enter the **Management IP address, Subnet Mask and Default Gateway** of the Wireless LAN Controller. **Do not** enable the DHCP Server. This is because we are using an External DHCP server in this example. Click on the **Next** button.


Cisco Aironet 3800 Series Mobility Express
1 Set Up Your Controller
System Name
me-wlc
Country
United States (US)
Date & Time
06/07/2017
1:50:33
Timezone
Pacific Time (US and Canada)
NTP Server
(optional)
Management IP Address
20.20.20.5
Subnet Mask
255.255.255.0
Default Gateway
20.20.20.1
Enable DHCP Server (Management Network)
Back
Next
2 Create Your Wireless Networks
3 Advanced Setting

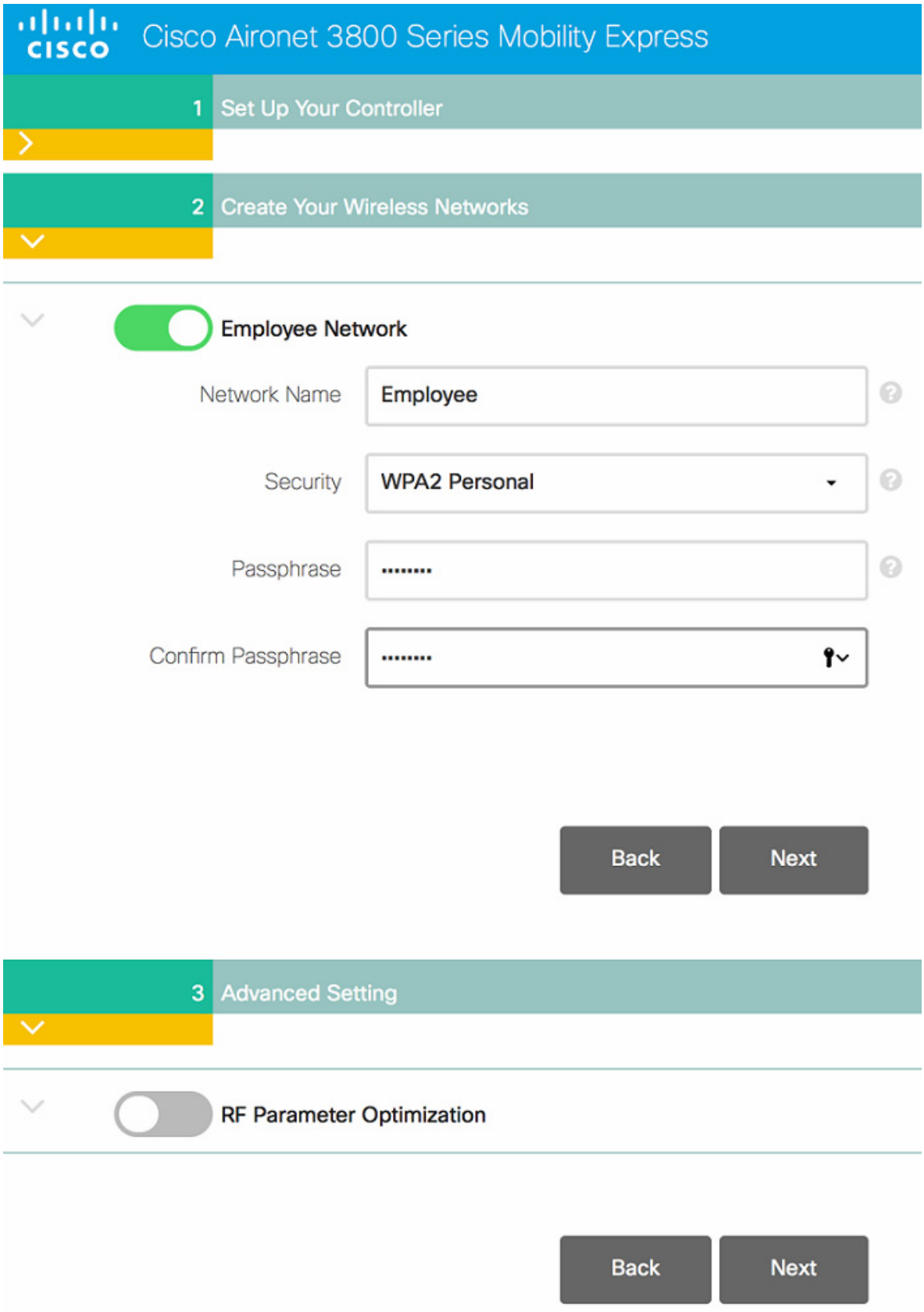
7. Create an Employee Network by entering the Network Name and selecting the **Security Type**. For **WPA2 Personal**, enter the Passphrase twice. For **WPA2 Enterprise**, enter the RADIUS Server IP address and shared Secret.

Note NOTE: At this time, WLAN clients will be in the same network as Access Points. To configure WLAN clients on a different VLAN, go to the WLAN section.

Click **Next**.

Under **Advanced Settings**, enable **RF Parameter Optimization**. Select the **Client Density** and **Traffic Type** for the deployment.

Click **Next**.

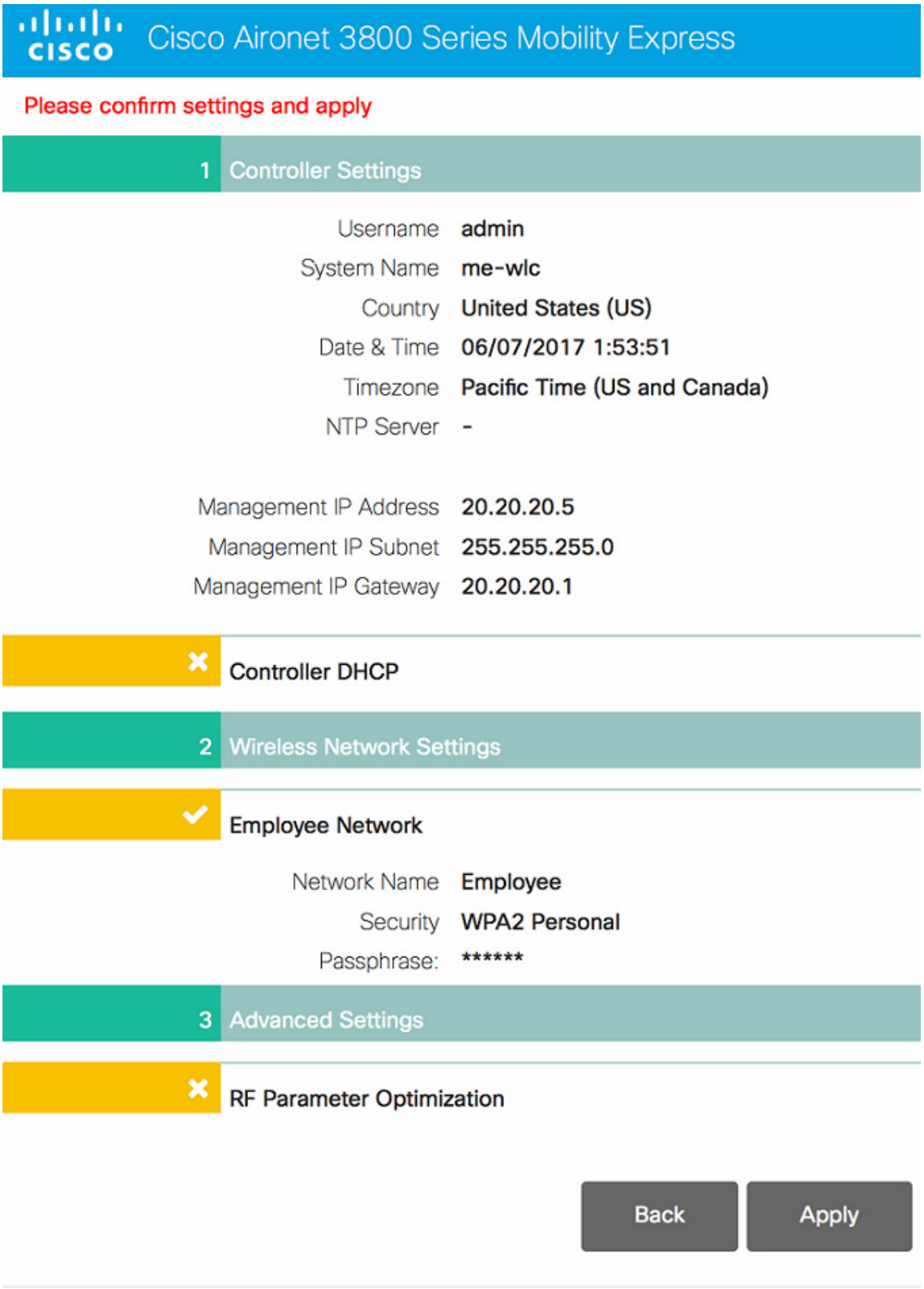

Cisco Aironet 3800 Series Mobility Express
1 Set Up Your Controller
2 Create Your Wireless Networks
Employee Network
Network Name
Employee
Security
WPA2 Personal
Passphrase
Confirm Passphrase
Back
Next
3 Advanced Setting
RF Parameter Optimization
Back
Next

8. Verify the selections and click Apply. Click Ok on the confirm window.

The Master AP will reboot and when it comes back up, it will run the Wireless Controller function.

Using a web browser, access the controller WebUI at https://<management IP address>. Please note that Management IP address was configured in Step 6 above.

To login into the controller WebUI interface, click Login and enter the username and password configured in Step 5 above


Cisco Aironet 3800 Series Mobility Express
Please confirm settings and apply
1 Controller Settings
Username admin
System Name me-wlc
Country United States (US)
Date & Time 06/07/2017 1:53:51
Timezone Pacific Time (US and Canada)
NTP Server -
Management IP Address 20.20.20.5
Management IP Subnet 255.255.255.0
Management IP Gateway 20.20.20.1
Controller DHCP
2 Wireless Network Settings
Employee Network
Network Name Employee
Security WPA2 Personal
Passphrase: ******
3 Advanced Settings
RF Parameter Optimization
Back
Apply

Configuring 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 in a Mobility Express Deployment is supported in the Centralized NAT use case.

Configuring Cisco Mobility Express for Site Survey

Cisco 802.11ac Wave 2 access points are capable of running Cisco Mobility Express which a virtual wireless controller function embedded on the Access Point. It also supports internal DHCP server which enables Access Point to be used for Site Survey.

Pre-requisite

1. Access Points - Cisco 802.11ac Wave 2 access points running Cisco Mobility Express software.
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

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 and run the Wireless Controller function.

Step 4 Configure the Wireless Controller using the CLI Setup Wizard.

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

```
Would you like to terminate autoinstall? [yes]:yes
Enter Administrative User Name (24 characters max):admin
Enter Administrative Password (3 to 24 characters max):Cisco123
Re-enter Administrative Password: Cisco123
System Name:[Cisco_3a:d2:b4] (31 characters max):me-wlc
Enter Country Code list(enter 'help' for a list of countries)[US]:US
```

```
Configure a NTP server now?[YES][no]:no
Configure the system time now?[YES][no]:yes
Enter the date in MM/DD/YY format:02/28/17
Enter the time in HH:MM:SS format:11:30:00
Enter timezone location index(enter 'help' for a list of timezones):5
Management Interface IP Address: 10.10.10.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Create Management DHCP Scope?[yes][NO]:yes
DHCP Network: 10.10.10.0
DHCP Netmask: 255.255.255.0
Router IP: 10.10.10.1
Start DHCP IP address: 10.10.10.10
Stop DHCP IP address: 10.10.10.250
DomainName: mewlc.local
DNS Server:[OPENDNS][user DNS]OPENDNS
Create Employee Network?[YES][no]:yes
Employee Network Name(SSID)?:site_survey
Employee VLAN Identifier?[MGMT][1-4095]:MGMT
Employee Network Security?[PSK][enterprise]:PSK
Employee PSK Passphrase (8-38 characters)?: Cisco123
Re-enter Employee PSK Passphrase: Cisco123
Re-enter Employee PSK Passphrase: Cisco123
Create Guest Network? [yes][NO]:NO
Enable RF Parameter Optimization?[YES][no]:no
Configuration correct? If yes, system will save it and reset.[yes][NO]:yes
```

Step 5 Wait for the Access Point to boot up completely. After the Wireless controller has started, log back in to the controller using administrative username or password configured during the initial setup wizard.

Step 6 (Optional): During the CLI setup wizard, Employee Network Security was configured to PSK. This can be disabled for easy association of clients and also disable SSID broadcast to avoid unwanted clients from joining the SSID. To disable PSK and SSID broadcast, enter the following commands in the Controller CLI.

```
(Cisco Controller)>config wlan disable 1
(Cisco Controller)>config wlan security wpa disable 1
(Cisco Controller)>config wlan broadcast-ssid disable wlan 1
(Cisco Controller)>config wlan enable 1
(Cisco Controller)>save config
```

Step 7 To configure channel, TX power, and channel bandwidth for the radios, disable the radio first, make the changes and then re-enable it.

To change the 2.4GHz radio to channel 6, follow the steps below:

```
(Cisco Controller)>config 802.11b disable <ap name>
(Cisco Controller)>config 802.11b channel <ap name> <ap name> 6
(Cisco Controller)>config 802.11b enable <ap name>
```

To change the 2.4GHz radio Transmit Power to power level 3, follow the steps below:

```
(Cisco Controller)>config 802.11b disable <ap name>
(Cisco Controller)>config 802.11b txPower <ap name> <ap name> 3
(Cisco Controller)>config 802.11b enable <ap name>
```

To change the 5 GHz radio to channel 44, follow the steps below:

```
(Cisco Controller)>config 802.11a disable <ap name>
(Cisco Controller)>config 802.11a channel <ap name> <ap name> 44
(Cisco Controller)>config 802.11a enable <ap name>
```

To change the 5 GHz radio Transmit Power to level 5, follow the steps below:

```
(Cisco Controller)>config 802.11a disable <ap name>
(Cisco Controller)>config 802.11a txPower <ap name> <ap name> 5
(Cisco Controller)>config 802.11a enable <ap name>
```

To change the 5 GHz radio channel width to 40MHz, follow the steps below:

```
(Cisco Controller)>config 802.11a disable <ap name>
(Cisco Controller)>config 802.11a chan_width <ap name> 40
(Cisco Controller)>config 802.11a enable <ap name>
```

If 2800 and 3800 series access points are being used for Site Survey, please note the following with respect to the XOR radio:

- Default operation state of XOR radio is 2.4GHz.
- 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.
- When the XOR (2.4 GHz) radio is configured to operate at 5GHz, 100MHz frequency separation is required from dedicated 5GHz radio
- 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 DHCP scope in Day 1

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. 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 and click on Add new Pool** button.

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

- Enter the Pool Name for the WLAN
- Enable the Pool Status
- Enter the VLAN ID for the WLAN
- Enter the Lease Period for the DHCP clients. Default is 1 Day
- Enter the Network/Mask
- Enter the Start IP for the DHCP pool
- Enter the End IP for the DHCP pool
- Enter the Default Gateway for the DHCP pool

Note If the scope is for client devices connecting to the Centralized NAT, one must select Mobility Express Controller for Default Gateway

- 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 & Firewall tab.

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

- Select Network(Default) for Client IP Management or Mobility Express Controller if this scope is for
- Centralized NAT'ed WLAN
- 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**.

Creating Wireless Networks

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

Access Points broadcast all active WLAN SSIDs and enforce the policies that you define for each WLAN. SSID broadcast can be disabled for individual WLAN if desired. QoS, Application Visibility and Control along with Local profiling is supported on WLAN. In addition, 802.11k, 802.11r, 802.11v and Fastlane are supported as well.

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)

Note AP indicates Master AP and the authentication is done by the Controller.

For Guest WLAN, a number of capabilities are supported:

1. CMX Guest Connect
2. Internal Splash Page

3. External Splash Page

For Internal and External Splash Page, a number of Access Types are supported. They are as follows:

a. Local User Account
b. Web Consent
c. Email Address
d. RADIUS
e. WPA2 Personal

Note MAC Filtering using RADIUS or local WLC database is also supported.

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 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 Click on the WLAN Security tab and configure the following:

- Select Security Type as WPA2 Enterprise
- Select Authentication Server as External RADIUS
- Select RADIUS Compatibility from the drop-down list
- Select MAC Delimiter from the drop-down list

Step 4 Add the Radius server and configure the following:

- Enter the Radius IP
- Enter the Radius Port
- Enter the Shared Secret
- Click on Tic icon

Step 5 Click Apply.

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 If Guest Clients have to be on a separate VLAN, click on the VLAN & Firewall tab and select **Yes** for Use VLAN Tagging and enter the following:

- Enter the native VLAN. This is the VLAN for your APs
- In the VLAN ID field, enter the VLAN for the Guest clients

Note Guest VLAN must be configured on the switch port.

Step 7 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 Wireless Networks

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 incase 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.

Cisco Mobility Express supports the following Transfer Mode for Software Update:

1. Cisco.com -. In this software update method, the software image can be directly streamed from cisco.com to the individual Access Points. Internet access is required for this transfer mode and EULA and SMARTNet contract requirements have to be met before software download can be initiated.
2. HTTP - HTTP transfer mode is supported if the Mobility Express Network has the same model of Access Points and one can use 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.

3. 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 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
- 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.

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 on Update button 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 on Confirm button to start the software update.

To monitor the download progress on individual Access Points, expand the Predownload image status.

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:

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:

- 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.
- 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.

Failover and Resiliency

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.

Electing a new Master

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.

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:

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:

Procedure

Step 1 Navigate to Wireless Settings > Access Points.

Step 2 From the list of Access Points, click Edit icon of the Access Point which you would like to select as the Master AP.

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

Step 4 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.

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:

Procedure

Step 1 Login to the CLI of the controller.

Step 2 Execute the following CLI-

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

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

To see the Next Preferred 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
```

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.

4. Least Client Load – If here 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.
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.

Mobility Express supports variety of features as they supported on the UWNC controllers. For complete listing of the supported features per specific release please see the link below:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-5/b_Mobility_Express_FlexConnect_Feature_Matrix.html