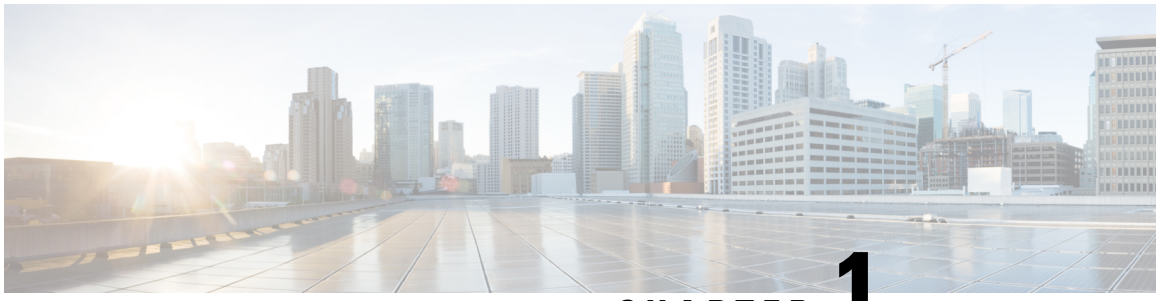
Cisco Mobility Express User Guide, Cisco Wireless Release 8.9

First Published: 2019-04-09

Last Modified: 2021-02-16

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

CONTENTS



CHAPTER 1

About Cisco Mobility Express

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Overview of Cisco Mobility Express

The Cisco Mobility Express wireless network solution comprises of at least one 802.11ac Wave 2 Cisco Aironet Series access point (AP) with an in-built software-based wireless controller (WLC) managing other APs in the network.

The AP acting as the WLC is referred to as the primary AP while the other APs in the Cisco Mobility Express network, which are managed by this primary AP, are referred to as subordinate APs.

In addition to acting as a WLC, the primary AP also operates as an AP to serve clients along with the subordinate APs.

Cisco Mobility Express provides most features of a Cisco WLC and has the capability to interface with the following:

- Cisco Prime Infrastructure—For simplified network management, including managing AP groups
- Cisco Identity Services Engine—For advanced policy enforcement
- Connected Mobile Experiences (CMX)—For providing presence analytics and guest access using Connect & Engage

Supported Cisco Access Points

The following Cisco Aironet Series APs are supported in the Cisco Mobility Express network:

Note

- APs listed under primary APs can also function as subordinate APs.
- The software on the APs listed under primary APs can be converted from Cisco Mobility Express to CAPWAP Lightweight AP software and vice versa. For ordering information, visit the Cisco Aironet Access Points Ordering Guide

Table 1: Cisco APs Supported in Cisco Mobility Express

Primary APs	Subordinate APs
Cisco Aironet 1560 Series	Cisco Aironet 700i Series
Cisco Aironet 1815i	Cisco Aironet 700w Series
Cisco Aironet 1815w	Cisco Aironet 1600 Series
Cisco Aironet 1830 Series	Cisco Aironet 1700 Series
Cisco Aironet 1850 Series	Cisco Aironet 1810W Series
Cisco Aironet 2800 Series	Cisco Aironet 2600 Series
Cisco Aironet 3800 Series	Cisco Aironet 2700 Series
	Cisco Aironet 3500 Series
	Cisco Aironet 3600 Series
	Cisco Aironet 3700 Series

Supported Software Images

AP models that are supported as primary can be ordered with either of the following as the default factory-shipped software:

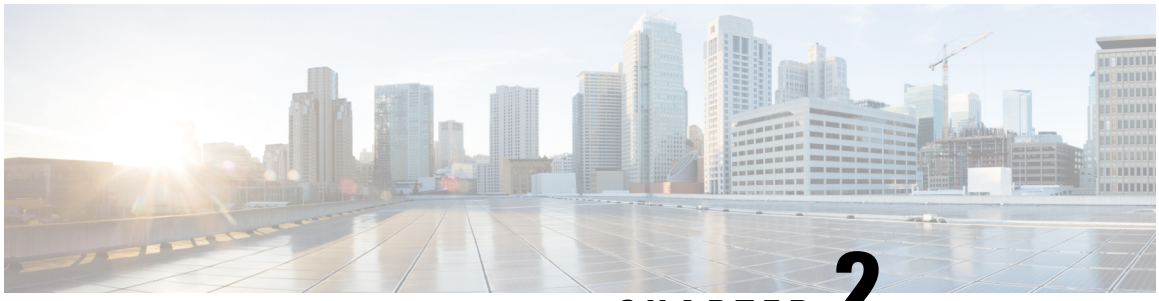
- A Cisco Mobility Express software image. These models have model numbers (or Product IDs) ending in *C*.
- A lightweight AP software image, based on the Control and Provisioning of Wireless Access Points (CAPWAP) protocol, for joining a wireless controller. You can manually convert these models on site to have a Cisco Mobility Express software image. For information about this conversion, see Converting from CAPWAP Lightweight AP to Cisco Mobility Express Software, on page 11.

AP models that are supported only as subordinates require a CAPWAP-based lightweight AP software image.

The Cisco Mobility Express software for your AP model can be downloaded from: https://software.cisco.com/download/navigator.html.

From the **Download Software** window, browse to your AP model and then select **Mobility Express Software** to view a list of currently available software, with the latest the top. The software releases are labeled as follows to help you determine which release to download:

- Early Deployment (ED)—These software releases provide new features, new hardware platform support, and bug fixes.
- Maintenance Deployment (MD)—These software releases provide bug fixes and ongoing software maintenance.
- Deferred (DF)—These software releases have been deferred. We recommend that you migrate to an upgraded release.



CHAPTER 2

Getting Started

Prerequisites for Setting Up and Accessing Cisco Mobility Express

- You must not have other Cisco wireless controllers, neither appliance nor virtual, in the same network, during setup or during daily operation of a Cisco Mobility Express network.

  The Cisco Mobility Express controller cannot interoperate or co-exist with other wireless controllers in the same network. Ensure that there no wireless controllers, other than the Cisco Mobility Express controller, in the network.

- Decide on the first access point (AP) to be set up. The first AP to be set up should be one that supports the Cisco Mobility Express wireless controller functionality. This is to ensure that this AP can act as the primary AP, and the other APs can then connect to it. This will ensure that the pre-defined *CiscoAirProvision* Service Set Identifier (SSID) is advertised only by the primary AP and not by other APs.

- Ensure that the AP is properly installed as per its *Hardware Installation Guide*.

- Cisco Mobility Express provides an internal DHCP server which can be optionally setup during the initial configuration wizard. However, if you want to use an external DHCP server instead, then ensure that a DHCP server is present and accessible in the network. The Mobility Express controller will use this DHCP server for IP address management of the access points and the wireless clients.

- The initial setup of the Cisco Mobility Express controller can be done only through the controller configuration wizard and over Wi-Fi.

  You require a Wi-Fi-enabled laptop to connect to the pre-defined *CiscoAirProvision* SSID advertised by the primary AP. You cannot access this SSID through a wired network.

- Your laptop should have a compatible browser. For a list of browsers compatible with the Cisco Mobility Express wireless controller web interface and the initial configuration wizard, see Supported Browsers, on page 99.

- If your network is using universal regulatory domain access points, then you will need prime the access point to the right regulatory domain, before the APs start serving clients. See the *Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide*, at this URL: http://www.cisco.com/c/en/us/td/docs/wireless/access_point/ux-ap/guide/uxap-mobapp-g.html.

After these prerequisites are met, proceed to Configuring the Switch Port, on page 6.

Note A CLI-based Initial Configuration Wizard is also available, but recommended only for advanced users. See Using the CLI Initial Configuration Wizard, on page 91.

Auto-provisioning the Primary AP via Cisco Plug and Play

Using the Cisco Network Plug and Play (PnP) solution, you can provision the primary AP automatically via a remote Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) server. PnP is activated only for the initial setup on Day 0 of the Cisco Mobility Express network deployment.

If there are multiple Cisco Mobility Express-capable APs on Day 0 in the Cisco Mobility Express network, they elect a primary AP among themselves through VRRP. This elected primary AP then receives its provisioning parameters from the APIC-EM server via PnP through one of the following ways:

- Via Cisco cloud redirect to APIC-EM
- Via DHCP option 43
- Via DNS discovery

For prerequisites and detailed instructions on automatically provisioning using Cisco PnP, see Cisco Network Plug and Play.

Configuring the Switch Port

Connect the access points to the switch and power them up. Ensure the following while configuring the switch port:

- All access points, including the primary AP, in a Mobility Express network should be in the same L2 broadcast domain. Management traffic must not be tagged.
- The switch port to which the primary AP is connected can be a trunk port or an access port and must be configured to trunk Native VLAN for management traffic. Data traffic must be trunked with appropriate VLANs for local switching as well.

The following is a sample switch port configuration.

```
Interface GigabitEthernet1/0/37
description » Connected to Master AP «
switchport trunk native vlan 122
switchport trunk allowed vlan 10,20,122
switchport mode trunk
```

Starting the Initial Configuration Wizard

Step 1 Boot the AP that has controller capability.

It will be a few minutes before the *CiscoAirProvision* SSID starts broadcasting after initially powering up the AP. Once the *CiscoAirProvision* SSID starts broadcasting, the AP's status LED start cycling through green, red, and amber.

Step 2 Connect the Wi-Fi-enabled laptop to the *CiscoAirProvision* SSID advertised by the AP, using Wi-Fi. The password is **password**.

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

Step 3 Open a supported web browser and enter the URL *mobilityexpress.cisco* to reach the initial configuration wizard. The wizard starts by asking you to create an admin account.

On Apple clients, after connecting to the *CiscoAirProvision* SSID, the captive portal window may automatically open with the initial configuration wizard. You can use this window itself complete the initial configuration without opening a web browser.

Note After connecting to the *CiscoAirProvision* SSID, upon opening a web browser you should be automatically redirected to *mobilityexpress.cisco*. If you are not automatically redirected, then you can manually enter the URL *mobilityexpress.cisco* or go to *http://192.168.1.1*, both of which redirect to the initial configuration wizard.

What to do next

If the initial configuration wizard's admin account window is displayed, then proceed to , else proceed to Checking if an AP has CAPWAP Lightweight AP Software or Cisco Mobility Express Software, on page 10.

Using the Initial Configuration Wizard

The initial configuration wizard helps you configure certain basic parameters on your Cisco Mobility Express wireless LAN controller, and thereby gets your Cisco Mobility Express network running.

Use the following sections as a reference for the data that you enter in the initial configuration wizard.

Initial Configuration Wizard Opening window

The banner on this window shows the name of the AP model on which the Cisco Mobility Express wireless controller is being configured, for example, Cisco Aironet 1830 Series Mobility Express.

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

- Enter an administrative username. You can enter up to 24 ASCII characters.

Note Change the username and password on factory-shipped Cisco Mobility Express-capable APs. If you use the default credentials `cisco` (not case sensitive), SSH will be disabled on these APs.

- Enter a password. You can enter up to 24 ASCII characters.

  When specifying a password, ensure the following:

  - The password must contain characters from at least three of the following classes, lowercase letters, uppercase letters, digits, and 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 or the username reversed.
  - The password must not be cisco, ocsic, or any variant obtained by changing the capitalization of the letters in the word Cisco. In addition, you cannot substitute 1, I, or ! for i, 0 for o, or $ for s.

Step 1—Set Up Your Controller

Specify the following basic parameters for setting up your controller:

- **System Name**—Enter the name that you want to assign to this controller.
- **Country**—Enter the country where this Cisco Mobility Express network is located.
- **Date and Time**—Specify the date. By default, your device's system time is applied here. You can manually edit the time, if required.
- **Timezone**—Select your time zone.
- **NTP Server**—To have the date and time set automatically using an Network Time Protocol (NTP) server, you can enter the IPv4 address or the FQDN name of the NTP server here.

  By default three NTP servers are automatically created. The default FQDN names of the NTP servers are:

  - 0.ciscome.pool.ntp.org, with NTP Index value 1.
  - 1.ciscome.pool.ntp.org, with NTP Index value 2.
  - 2.ciscome.pool.ntp.org, with NTP Index value 3.

  The IPv4 address or the FQDN name, which you specify here, will be applied to the server with NTP Index 1, thereby overwriting its default FQDN, *0.ciscome.pool.ntp.org* . For editing NTP server details, go to **Management** > **Time**.
- **Management IP Address**—Enter the IP address for managing the controller.
- **Subnet Mask**—Enter the subnet mask for the controller.
- **Default Gateway**—Enter the default gateway for the controller.

- **Enable DHCP Server (Management Network)**—This is optional. If you choose to enable the internal DHCP server, specify the following parameters:
  - **Network**
  - **Mask**
  - **Management VLAN ID**
  - **First IP**
  - **Last IP**
  - **Domain Name**
  - **Name Servers**

Step 2—Create Your Wireless Networks

You set up the following network here:

- **Employee Network**—A Wi-Fi network for employees and regular day-to-day users of the network. This provides more privileges than the guest network access.

In the **Employee Network** section, specify the following parameters:

- **Network Name**—Specify the SSID for your Employee network.
- **Security**—You can choose either **WPA2 Personal** that uses pre-shared key (PSK) authentication or **WPA2 Enterprise** (also called 802.1x), which requires a RADIUS server for authentication.
- **Pass Phrase**—If you have chosen WPA2 Personal security, specify the PSK here.
- **Authentication Server IP Address**—If you have chosen WPA2 Enterprise security, enter the IP address of the RADIUS server.
- **Shared Secret**—Enter the password for the RADIUS server.
- **VLAN**—Choose **Management VLAN** (VLAN 0) or create a **New VLAN** (with a VLAN ID ranging from 1 to 4094).
- **VLAN ID**—Specify the VLAN ID for the new VLAN here.
- **Enable DHCP Server (Employee Network)**—This is optional. If you choose to enable the internal DHCP server for assigning IP addresses on the **Employee Network**, specify the following parameters:
  - **Network**
  - **Mask**
  - **First IP**
  - **Last IP**
  - **Default Gateway**
  - **Domain Name**
  - **Name Servers**

- **Name Server IP1**
- **Name Server IP2**

Step 3—Advanced Settings

Optimize the network's radio frequency signal coverage and quality by indicating the expected client density and traffic type in your network. To know the values that are set when low, typical, or high client density type is selected, see RF Parameter Optimization Settings, on page 104.

Note If you do not enable RF Parameter Optimization during the initial configuration wizard, then client density is set to **Typical** (the default value), and RF traffic type is set to **Data** (the default value). To change this at a later time, see Optimizing RF Parameters, on page 83.

Once you apply these configuration settings, the access point reboots and the controller restarts. You can now proceed to Logging in to Cisco Mobility Express , on page 13.

Checking if an AP has CAPWAP Lightweight AP Software or Cisco Mobility Express Software

Both the Cisco 1850 Series and 1830 Series APs can be ordered with a factory-shipped CAPWAP lightweight AP software or a Cisco Mobility Express controller software. However, you can convert a CAPWAP AP to Cisco Mobility Express software, and vice-versa, on site. To determine if your AP has a Cisco Mobility Express image or CAPWAP Lightweight AP image, follow these steps:

Step 1 Connect to the console port of the AP.

Step 2 Log in to the AP using the username `Cisco` and password `Cisco`. Both are case-sensitive.

This is the default factory-shipped username and password on all Cisco Aironet APs.

Step 3 Enter the **sh version** command on the AP console.

Step 4 Check the command output for the **AP Image Type** and **AP Configuration** fields. There are three possible scenarios, as shown in the following table:

What to do next

Fields and Their Values in the Output	What to do Next
AP Image Type: `MOBILITY EXPRESS IMAGE` AP Configuration: `MOBILITY EXPRESS CAPABLE`	No conversion is required.

Fields and Their Values in the Output	What to do Next
AP Image Type: `MOBILITY EXPRESS IMAGE` AP Configuration: `NOT MOBILITY EXPRESS CAPABLE`	This means that the AP has the Cisco Mobility Express software, but is running as a CAPWAP lightweight AP. This AP is currently not configured to run as Mobility Express controller, does not take part in the primary AP election process either, and hence does not broadcast the the *CiscoAirProvision* SSID. This AP can, however, function as a subordinate AP in a Mobility Express network. To enable the Mobility Express controller functionality of this AP, run the command **ap-type mobility-express tftp** on the AP console. The AP will reboot, come back online, and take part in the primary AP election process. If and when it is elected as primary, it will broadcast the *CiscoAirProvision* SSID.
The **AP Image Type** and **AP Configuration** fields are not present in the output	This means that the AP has a CAPWAP lightweight AP software and not Cisco Mobility Express software. Proceed to Converting from CAPWAP Lightweight AP to Cisco Mobility Express Software, on page 11.

Converting from CAPWAP Lightweight AP to Cisco Mobility Express Software

Follow this procedure to convert the AP software to Cisco Mobility Express configuration-capable software.

note

Note The following procedure shows a conversion from the 8.1.122.0 Lightweight AP release on an 1850 series AP, and hence uses the corresponding software file. Ensure that you use the appropriate software file depending on the release you are converting from and the AP model.

Before you begin

- Your AP is either a Cisco 1850 Series or a 1830 Series AP with Lightweight AP software Release 15.3.3-JBB5, for Cisco Wireless Controller Software Release 8.1.122.0, or a newer software.
- A TFTP server and a DHCP server should be configured and accessible.
- Ensure that there are no Cisco WLCs, physical or virtual, in the network while you are performing this upgrade. The AP must not interface with any other wireless controller while you are performing this upgrade.
- Ensure that you remove the priming configuration in the AP by using the **capwap ap erase all** command.

Step 1 Download the *AIR-AP1850-K9-8.1.122.0.tar* software file from Cisco.com to the TFTP server.

On the Download Software page, for a given release, this .TAR file is labeled, *'Software to be used for conversion from Lightweight Access Points only'*.

Step 2 Connect to the console port of the AP.

Step 3 Log in to the AP using the username **Cisco** and password **Cisco**. Both are case-sensitive.

This is the default factory-shipped username and password on all Cisco Aironet APs.

Step 4 To convert the AP from CAPWAP lightweight AP software to Cisco Mobility Express software, use the **ap-type mobility-express tftp://***<tftp server ip-address>/<filename of TAR file with path from root on the TFTP server>* command.

The software file is downloaded to the AP, and is written to the AP's flash memory. The AP reboots with a Mobility Express-capable configuration and starts broadcasting the *CiscoAirProvison* SSID.

What to do next

For an alternative to the above conversion process, using the .ZIP file, see Alternative Method for CAPWAP to Mobility Express Conversion, on page 102.

To convert an AP from Mobility Express type to CAPWAP type, see Converting an AP from Mobility Express to CAPWAP Type, on page 103.

Preparing APs to Associate with the Primary AP

Follow this procedure to enable a new AP to associate itself with the Cisco Mobility Express wireless controller on the primary AP, and thereby enabling it to join the Cisco Mobility Express network.

Before you begin

- A primary AP with Cisco Mobility Express wireless controller should be up and running.
- If the AP that has to be prepared to associate with the primary AP is a universal regulatory domain AP, then it should be primed using the Cisco AirProvision mobile application. For more information, see the *Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide* at:

  http://www.cisco.com/c/en/us/td/docs/wireless/access_point/ux-ap/guide/uxap-mobapp-g.html

Step 1 Download the latest Cisco Mobility Express bundle from Cisco.com to the TFTP server. This pack is either in .zip format (for Windows) or .tar format (Linux or Mac OSX) and contains the software images for all the supported APs.

Step 2 Unzip the software pack to a folder on the TFTP server.

Step 3 Provide the path to the folder in the **Management > Software Update > File Path** field.

Step 4 Perform a software update. .

What to do next

Managing Associated Access Points, on page 37

Logging in to Cisco Mobility Express

Step 1 Open a browser and enter **https://<ip address>** in your browser's address bar to access the Cisco Mobility Express **Wireless LAN Controller** login page. This IP address is the one you have specified for managing the Cisco Mobility Wireless Express controller.

The Cisco Mobility Express controller uses a self-signed certificate for HTTPs. Therefore, all browsers will display a warning and ask you whether you wish to proceed with an exception or not when the certificate is presented to the browser. Accept the warning in order to access the Mobility Express **Wireless LAN Controller** login page.

Figure 1: Cisco Mobility Express Wireless LAN Controller Web Interface Login

Step 2 Click **Login**.

Step 3 Enter admin user credentials to log in.

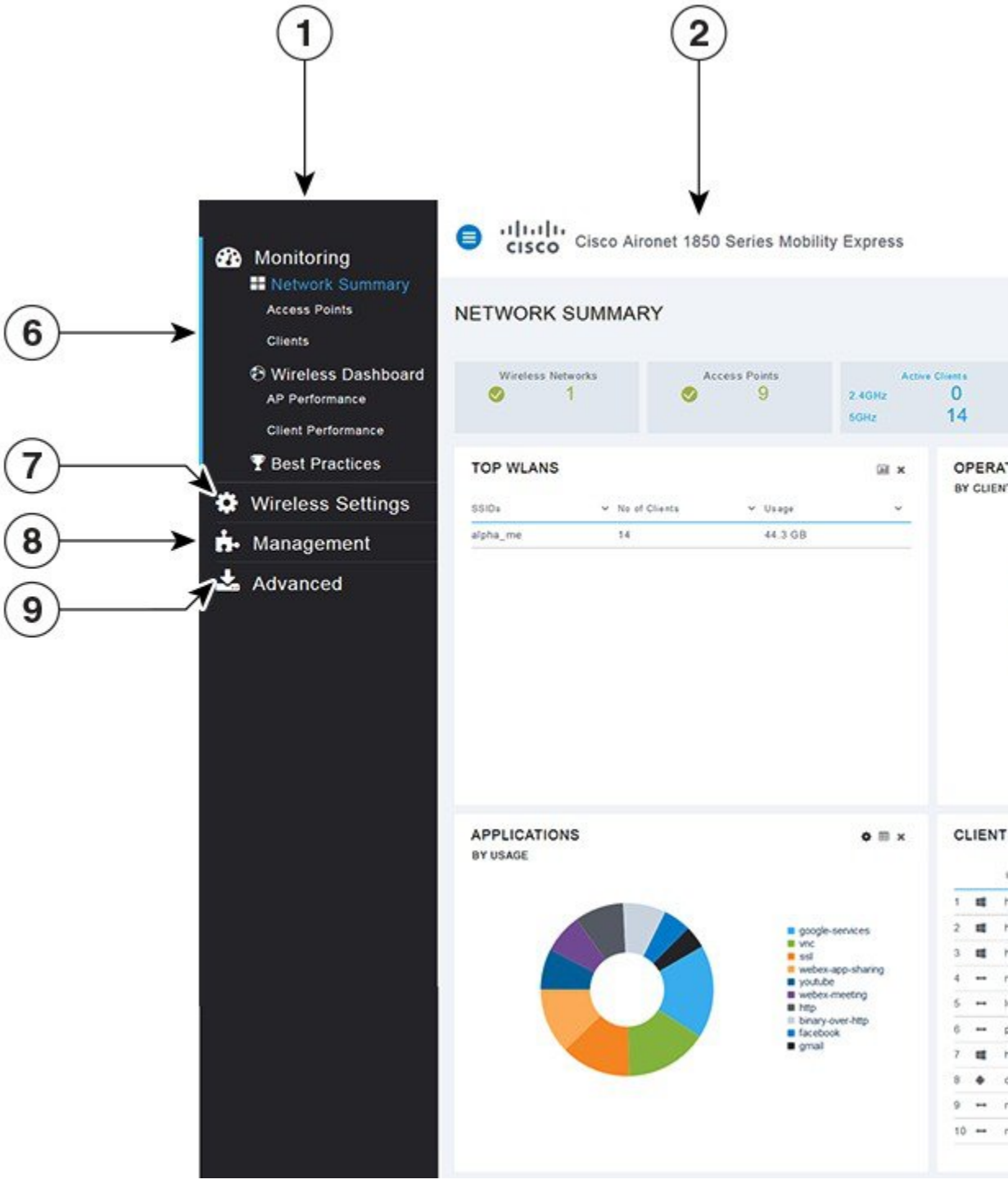
What to do next

After you log in, the default landing page is the **Network Summary** window. For more information, see About the Cisco Mobility Express Monitoring Service, on page 17.

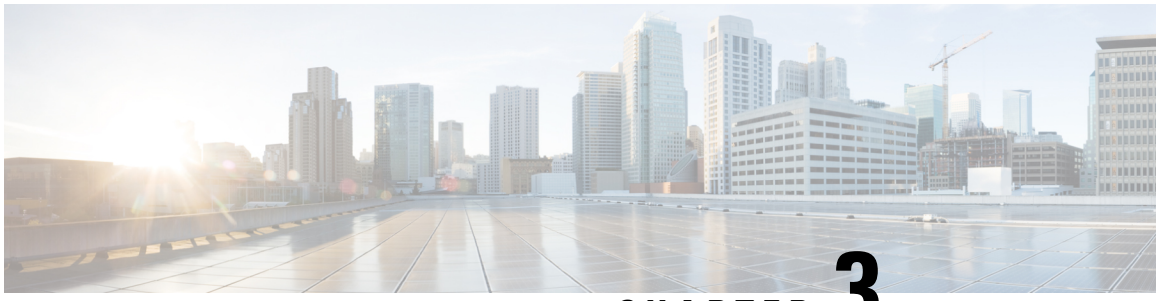
Understanding the Mobility Express Controller Web Interface

The following figure illustrates the opening page and the general layout of the Mobility Express controller web interface.

Figure 2: Mobility Express Controller Web Interface



No.	Web Interface Section or Feature
1	The side pane of the web interface. This is main navigational pane using which you can navigate to the various sub-sections in the web interface.
2	The title of the web interface. It indicates the AP model of the primary AP (on which the integrated controller functionality is currently operating)
3	Search for an AP or client using its MAC address.
4	Click to save the current controller configuration to the NVRAM. For more information, see Saving Controller Configuration, on page 86.
5	Click to view the current system information or to log off the controller web interface.
6	The Mobility Express Network Monitoring section. For more information, see About the Cisco Mobility Express Monitoring Service, on page 17.
7	The Wireless Settings section, where you can administer associated APs, manage WLANs, WLAN user accounts, and guest user accounts. For more information, see Specifying Wireless Settings, on page 31.
8	The Management section, where you can set management access parameters, manage admin accounts, network time, and perform software updates.
9	The Advanced section, where you can set SNMP settings, sys log settings, and perform a reset to factory default.



CHAPTER 3

Monitoring the Mobility Express Network

About the Cisco Mobility Express Monitoring Service

The Cisco Mobility Express Monitoring service enables the primary AP to monitor the WLANs and all the connected and unconnected devices on the network.

The **Monitoring** service offers the following capabilities through the **Network Summary** and **Wireless Dashboard** tabs:

- View details of configured WLANs.
- View list of top WLANs based on traffic and associated clients.
- View details of APs in the network.
- View details of clients operating actively at either 2.4 GHz or 5 GHz.
- View summary of client device-operating systems and applications running on these devices.
- View detailed listing of rogue clients and APs.
- View details of various interferers in the network on the 2.4GHz and 5 GHz radio frequencies.
- Monitor the performance of APs in the network.
- Monitor the performance of clients in the network.

Note

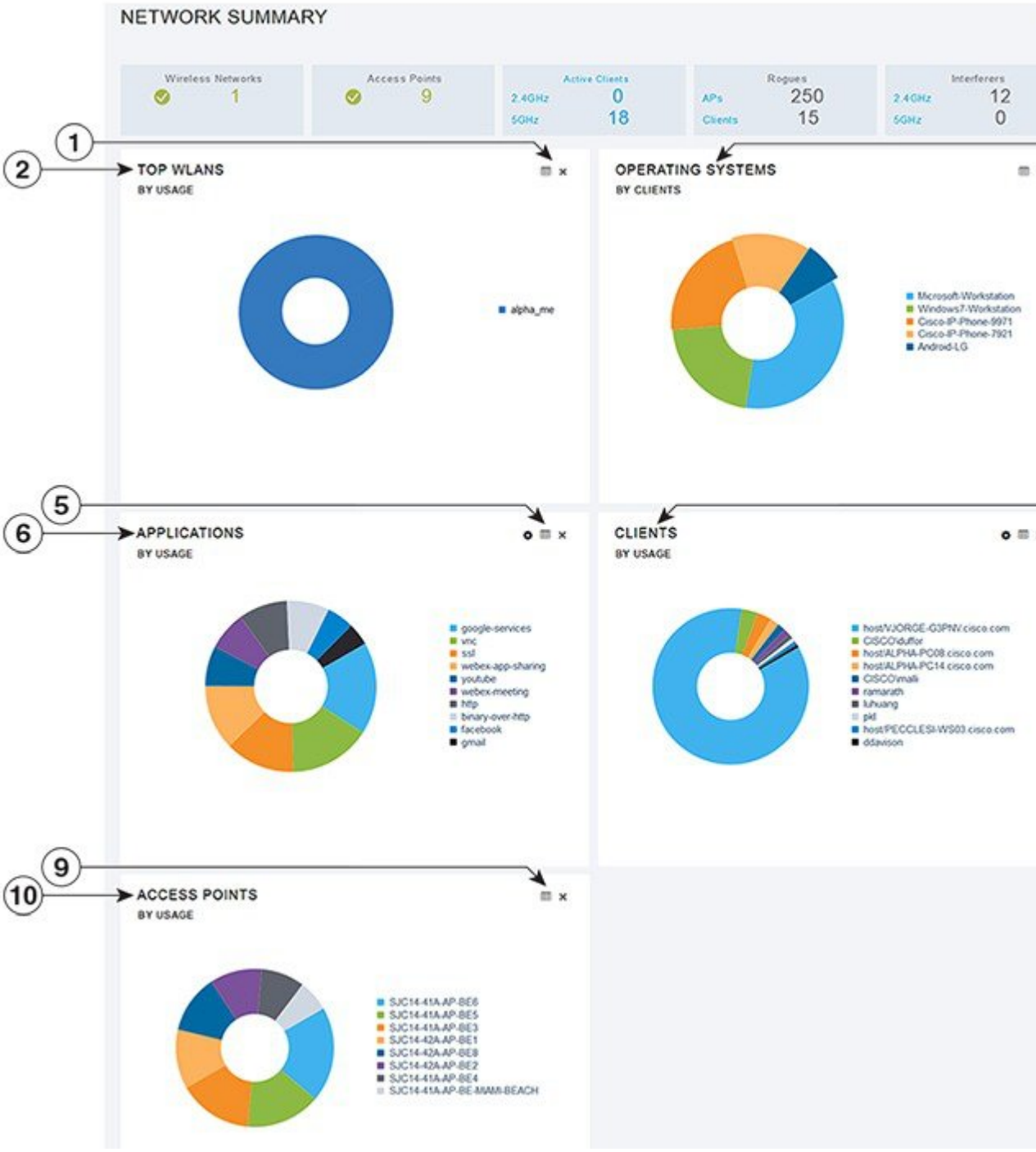
- All the parameters on the **Network Summary** window are read-only parameters.
- This page is automatically refreshed every 30 seconds.

Customizing the Network Summary View

You can customize the Network Summary view by adding or removing widgets. The data displayed in the various widgets can be viewed either in the doughnut format or in the tabular format by toggling the display icon on the top right corner of the individual widgets.

Figure 3: Network Summary Widgets - Tabular view

Figure 4: Network Summary Widgets - Doughnut view



Viewing and Managing WLAN Users

You can view and manage WLAN users only for WPA2 Enterprise with Local Server setup. To use your Cisco Mobility Express wireless network, a wireless client should connect to a WLAN in the network. To connect to a WLAN, the wireless client will have to use the user credentials set for that WLAN. If this WLAN uses WPA2-Personal as a Security Policy, then the user must provide the appropriate WPA2-PSK set for that WLAN on the Controller AP. If the Security Policy is set to WPA2-Enterprise, the user must provide a valid user identity and the corresponding password set in the RADIUS user database.

You can set up different users (and consequently, user credentials) for the different WLANs in the Cisco Mobility Express wireless network, in the **WLAN Users** window. These are local users authenticated by the primary AP using WPA2-PSK. Users authenticated by WPA2-Enterprise must have a valid record in the RADIUS database in order to be authenticated since they are not a part of the **WLAN Users** database.

Viewing WLANs

The **WLAN Configuration** window lists all the WLANs that are currently configured on the primary AP's controller, along with the following details for each WLAN:

- **Active**—Whether the WLAN is enabled or disabled.
- **Name**—Name of the WLAN
- **Security Policy**
- **Radio Policy**

Tip The total number of active WLANs is displayed at the top of the page. If the list of WLANs spans multiple pages, you can browse these pages by clicking the page number links or the forward and backward icons.

Viewing the Details of Configured WLANs

Step 1 Choose **Monitoring** > **Network Summary**.

A count of the configured WLANs is displayed in the **Wireless Networks** summary window.

Step 2 In the **Wireless Networks** summary window, click the status icon or count display icon to view high-level details of the corresponding WLAN, such as the **Active** status, **Name**, **Security Policy**, and **Radio Policy**.

Customizing Access Points Table View

Step 1 Click **Monitoring** > **Network Summary** > **Access Points**.
The **Access Points** view page appears.

Step 2 In the **Access Points** view page, toggle between the **2.4GHz** and **5GHz** tabs to view a tabular listing of the access points operating at the respective radio frequencies.

Step 3 (Optional) Click the downward facing arrow on the top right of the column header to select columns to be hidden or shown in the table view. hide or show desired or to filter the table view based on desired parameters.

Step 4 (Optional) Click the downward facing arrow on the top right of the column header to filter the table view based on desired parameters.

Viewing Details of Clients

Step 1 Click **Monitoring** > **Network Summary**.

A summary of all active clients is displayed in the Active Clients summary section. These clients are either 802.11 b/g/n clients operating at 2.4 GHz or 802.11 a/n/ac clients operating at 5 GHz.

Step 2 In the **Active Clients** summary section, click the count display icon to view high-level details of the client device.

The information shown includes:

- General details.
- Connectivity status graphic.
- Top applications on the client that are using the network connection.
- Mobility State graphic.
- Network, QoS, Security and Policy details.
- Client ping and packet capture tests.

Click the downward facing arrow on the top right of the column headers to customize the details displayed in the table either to hide or show desired columns or to filter the table view based on desired parameters.

Understanding the Mobility State Graphic

The Mobility State graphic for a client shows the following details:

- Name of the wireless LAN controller, with it's IP address and the model number of the AP on which it is running.
- Name of the AP through which the client is connected to the controller, along with the type of connection (for example, Flexconnect), the AP's IP address, and the AP's model number.
- Nature of connection between the AP and the client. For example, wireless 802.11n 5 GHz connection.
- Name of the client, type of client (for example, Microsoft Workstation), VLAN ID of the client, and the client's IP address.

Performing a Client Ping Test

You can perform a ping test on the client to determine the latency or delay between the controller and the client. This is an Internet Control Message Protocol (ICMP) based test. Using the ping test you can know the connectivity as well as the latency between the controller and the client.

To start the test, click **Start**. The latency in milliseconds is represented graphically.

Capturing Client Packets

Note This feature does not work on subordinate APs having Cisco AP-OS, namely the Cisco Aironet 1810W, 1830, 1850, 2800, and 3800 Series access points.

The Client Packet Capture feature allows network administrators to capture packets flowing to, through, and from an AP, while the AP continues to operate normally. The packets are captured and exported to an FTP server, where you can do an offline analysis by using a tool such as Wireshark. This feature facilitates troubleshooting by helping to gather information about the packet format, application analysis, and security.

Points to Note

- Packet capture can be enabled for only one client at a time.
- The packets are captured and dumped in the order of arrival or transmission of packets, except for beacons and probe responses. The packet capture contains information such as channel, RSSI, data rate, SNR, and timestamp. Each packet is appended with additional information from the AP.
- A file is created on the FTP server for each AP based on AP name, controller name and timestamp.
- If the FTP transfer time is slower than the packet rate, some of the packets may not appear in the capture file.
- If the buffer on the AP does not contain any packets, a dummy packet is dumped to keep the connection alive.
- If the FTP transfer fails or FTP connection is lost during packet capture, the AP stops capturing packets, notifies with an error message and SNMP trap, and a new FTP connection is established.
- Not all packets in the air are captured, but only those that reach the radio driver.
- Before you start ensure that you have an FTP server, that is reachable by the AP. The captured packets are dumped to this FTP server.

Performing the Packet Capture

1. Choose **Monitoring > Network Summary > Clients**.
2. On the **Client View** page, under **Client Test**, click the **Packet Capture** tab.
3. Under **Capture Point**, specify the following details:
    - **AP Name**—The name of the AP which will be the capture point. The capture point is a traffic transit point where the packets are captured. You can specify only an AP as the capture point

- **Time**—Specify the time period for packet capture. The range is from 1 to 60 minutes.

4. Under **Capture Filters**, specify the types of packets that need to be captured. You have the following types:
   - Control Packets
   - Data Packets
   - Dot1x
   - IAPP
   - Management Packets
   - ARP
   - Multicast frames
   - Broadcast frames
   - All IP
   - TCP with matching port number
   - UDP with matching port number
5. Under **FTP Details**, specify the following details of the FTP server to which the captured packets are dumped:
   - IP Address
   - Path of the folder on the FTP server where the packets are to be dumped
   - Username and Password for access to the FTP server
6. Click **Start**.

The **Client Status** icon is Green when a packet capture is in progress. It is Red otherwise.

Viewing Details of Rogue Devices (Clients and Access Points)

Step 1 Click **Monitoring** > **Network Summary**.

A summary of rogue APs and clients is displayed in the **Rogues** summary window.

Step 2 In the **Rogues** summary window, click the count display icon to view high-level details of the rogue devices (unmanaged neighboring APs or clients).

Viewing Details of Interferers

Step 1 Click **Monitoring** > **Network Summary**.

A summary of all non-WiFi interfering devices is displayed in the **Interferers** summary window. These interferers may either be operating at 2.4 GHz or at 5 GHz.

Step 2 In the **Interferers** summary window, click the count display icon to view high-level details of the interfering device.

Customizing the Access Point Performance View

You can customize the AP Performance view by adding or removing widgets.

Figure 5: Wireless Dashboard - AP Performance

Adding Widgets to Customize Access Point Performance View

Step 1 Choose **Monitoring** > **Wireless Dashboard** > **AP Performance**.

Step 2 Click the **Add Widget** icon on the top right hand side of the AP Performance window.

Step 3 Click to select the widgets that you want to add:

- Channel Utilization—Top APs
- Interference—Top APs
- Client Load—Top APs
- Coverage—Bottom APs

Step 4 Click **Close**.

The **AP Performance** window is refreshed with the new widgets.

Removing Widgets to Customize Access Point Performance View

Step 1 Choose **Monitoring** > **Wireless Dashboard** > **AP Performance**.

Step 2 Click the **Delete Widget** icon on the top right hand side of the widgets that you want to delete.

The **AP Performance** window does not display the deleted widgets.

Customizing the Client Performance View

You can customize the **Client Performance** view by adding or removing widgets.

Figure 6: Wireless Dashboard - Client Performance

Adding Widgets to Customize Client Performance View

Step 1 Choose **Monitoring** > **Wireless Dashboard** > **Client Performance**.

Step 2 Click the **Add Widget** icon on the top right hand side of the **Client Performance** window.

Step 3 Click to select the widgets that you want to add:

- **Signal Strength**
- **Signal Quality**
- **Connection Rate**

- **Client Connections**

Step 4 Click **Close**.

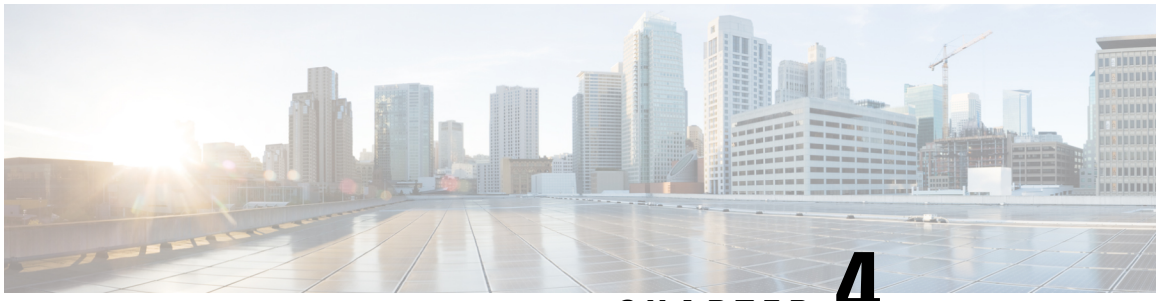
The **Client Performance** window is refreshed with the new widgets.

Removing Widgets to Customize Client Performance View

Step 1 Choose **Monitoring** > **Wireless Dashboard** > **Client Performance**.

Step 2 Click the **Delete Widget** icon on the top right hand side of the widgets that you want to delete.

The **Client Performance** window does not display the deleted widgets.



CHAPTER 4

Specifying Wireless Settings

Setting Up WLANs and WLAN Users

About WLANs in a Cisco Mobility Express Network

You can create and manage Wireless Local Area Networks (WLANs) through the **WLAN Configuration** window. Choose **Wireless Settings > WLANs**.

The total number of active WLANs is displayed at the top of the **WLAN Configuration** window along with a list of all the WLANs currently configured on the primary AP's controller. This list displays the following details for each WLAN:

- Whether the WLAN is enabled or disabled.
- Name of the WLAN.
- Security Policy on WLAN.
- Radio Policy on WLAN.

Guidelines and Limitations for Setting Up WLANs

- You can associate up to 16 WLANs with the Cisco Mobility Express controller. Cisco recommends a maximum of 4 WLANs. The controller assigns all the configured WLANs to all the connected APs.
- Each WLAN has a unique WLAN ID, a unique profile name, and an SSID.
- The WLAN name and SSID can have up to 32 characters.
- Each connected AP advertises only the WLANs that are in an **Enabled** state. The APs do not advertise disabled WLANs.
- The controller uses different attributes to differentiate between WLANs with the same SSID.

- Peer-to-peer blocking does not apply to multicast traffic.
- You cannot map a WLAN to VLAN0, and you cannot map VLANs 1002 to 1006.
- Dual-stack clients with static IPv4 addresses are not supported.
- When creating WLANs with the same SSID, create a unique profile name for each WLAN.

Adding a WLAN

Step 1 Choose **Wireless Settings** > **WLANs**.

The **WLAN Configuration** window is displayed.

Step 2 Click **Add New WLAN**.
The **Add New WLAN** window is displayed.

Step 3 Under the **General** tab, set the following parameters:

- **WLAN ID**—From the drop-down list, choose an ID number for this WLAN.
- **Profile Name**— The profile name must be unique and should not exceed 32 characters.
- **SSID**—The profile name also acts as the SSID. You can choose to specify an SSID that is different from the WLAN profile name. Like the profile name, the SSID can not exceed 32 characters and must be unique.
- **Admin State**—From the drop-down list, choose **Enabled** to enable this WLAN, else choose **Disabled**.

  The default is **Enabled**.
- **Radio Policy**—From the drop-down list, choose among the following options:
  - **All**—Configures the WLAN to support dual-band (2.4 GHz and 5 GHz) capable clients
  - **2.4 GHz only**—Configures the WLAN to support 802.11b/g/n capable clients only
  - **5 GHz only**—Configures the WLAN to support 802.11a/n/ac capable clients only

  The radio policy allows you to optimize the RF settings for all the APs associated with a WLAN. The selected radio policy applies to the 802.11 radios. Each radio policy specifies which part of the spectrum the WLAN is advertised on, whether it is on 2.4 GHz, 5 GHz, or both.
- **Broadcast SSID**—The default is **Enabled**. If you toggle it to make the SSID discoverable. Else, the SSID is hidden.
- **Local Profiling**

Step 4 Under the **WLAN Security** tab, set one of the following security authentication options from the **Security** drop-down list:

- **Open**—This option stands for Open authentication, which allows any device to authenticate and then attempt to communicate with an AP. Using open authentication, any wireless device can authenticate with the AP.
- **WPA2 Personal**—This option stands for Wi-Fi Protected Access 2 with pre-shared key (PSK). WPA2 Personal is a method used for securing your network with the use of a PSK authentication. The PSK is configured separately both on the controller AP, under the WLAN security policy, and on the client. WPA2 Personal does not rely on an authentication server on your network. This option is used when you do not have an enterprise authentication server.

If you choose this option, then specify the PSK in the **Shared Key** field, and confirm it by specifying it again in the **Confirm Shared Key** field. The PSK you enter is hidden under asterisks for security purposes. Check the **Show Shared Key** checkbox to reveal it.

- **WPA2 Enterprise**—This option stands for Wi-Fi Protected Access 2, with a local authentication server or a RADIUS server. This is the default option.

  To have a local authentication method, choose **AP** in the **Authentication Server** drop-down list. This option is a Local EAP authentication method that allows users and wireless clients to be authenticated locally. The controller in the primary AP serves as the authentication server and the local user database, which removes dependence on an external authentication server.

  To have a RADIUS server-based authentication method, choose **External Radius** in the **Authentication Server** drop-down list. RADIUS is a client/server protocol that enables communication with a central server to authenticate users and authorize their access to the WLAN. You can specify up to two RADIUS authentication servers. For each server you need to specify the following details:

  - **RADIUS IP**—IPv4 address of the RADIUS server.
  - **RADIUS Port**—Enter the communication port of the RADIUS server. The default value is 1812.
  - **Shared Secret**—Enter the secret key used by the RADIUS server, in ASCII format.

- **Guest**—The controller can provide guest user access on WLANs which are specifically designated for use by guest users. To set this WLAN exclusively for guest user access, choose the **Security** as **Guest**.

  You can set the authentication for guest users by choosing one of the following options in the **Guest Type** drop-down list:

  - **WPA2 Personal**—This option stands for Wi-Fi Protected Access 2 with pre-shared key (PSK). WPA2 Personal is a method used for securing your network with the use of a PSK authentication. The PSK is configured separately both on the controller AP, under the WLAN security policy, and on the client. WPA2 Personal does not rely on an authentication server on your network. This option is used when you do not have an enterprise authentication server.

    If you choose this option, then specify the PSK in the **Passphrase** field, and confirm it by specifying it again in the **Confirm Passphrase** field. The PSK you enter is hidden under asterisks for security purposes. Check the **Show Passphrase** checkbox to reveal it.

  - **Captive Portal (AP)**—Choose this option to set a captive portal which presents one of the following **Captive Portal Type**s to users:

    - **Require Username and Password**—This is the default option. Choose this option to authenticate guests using the username and password which you can specify for guest users of this WLAN, under **Wireless Settings > WLAN Users**. For more information, see Viewing and Managing WLAN Users, on page 36.
    - **Web Consent**—Choose this option to allow guests access to the WLAN upon acceptance of displayed terms and conditions. This option allows guest users to access the WLAN without entering a username and password.
    - **Require Email Address**—Choose this option, if you want guest users to be prompted for their e-mail address when attempting to access the WLAN. Upon entering a valid email address, access it provided. This option allows guest users to access the WLAN without entering a username and password.

  - **Captive Portal (External Web Server)**—Choose this option to have external captive portal authentication, using a web server outside your network. Also specify the URL of the server in the **Site URL** field.

- **CMX Guest Connect**—Choose this option to authenticate guests using the Cisco CMX Connect. Also, specify the URL of your CMX Cloud site in the **Site URL** field.

Step 5 Under the **VLAN & Firewall** tab, in the **Use VLAN Tagging** drop-down list, choose **Yes** to enable VLAN tagging of packets. Then, choose a **VLAN ID** from the drop-down list, to use for the tagging. By default VLAN Tagging is disabled.

By enabling VLAN Tagging, the chosen VLAN ID is inserted into a packet header in order to identify which VLAN (Virtual Local Area Network) the packet belongs to. This enables the controller to use the VLAN ID to determine which VLAN to send a broadcast packet to, thereby providing traffic separation between VLANs.

Step 6 If you have chosen to enable VLAN Tagging, then you have an option to enable a firewall for the WLAN based on Access Control Lists (ACLs). An ACL is a set of rules used to limit access to a particular WLAN to control data traffic to and from wireless clients or to the controller CPU to control all traffic destined for the CPU.

To enable an ACL-based firewall:

a. In the **Enable Firewall** drop-down list, choose **Yes**.

b. In the **ACL Name** field, enter a name for the new ACL. You can enter up to 32 alphanumeric characters. The ACL name must be unique.

c. Click Apply.

d. To set rules for the ACL, click **Add Rule**.

Note that ACL rules are applied to the VLAN. Multiple WLANs can use the same VLAN, hence inheriting ACL rules, if any.

Configure a rule for this ACL as follows:

a. From the **Action** drop-down list, choose **Deny** to cause this ACL to block packets or **Permit** to cause this ACL to allow packets. The default is Permit. The controller can permit or deny only IP packets in an ACL. Other types of packets (such as ARP packets) cannot be specified.

b. From the **Protocol** drop-down list, choose the protocol ID of the IP packets to be used for this ACL. These are the protocol options:

- **Any**—Any protocol (this is the default value)
- **TCP**—Transmission Control Protocol
- **UDP**—User Datagram Protocol
- **ICMP**—Internet Control Message Protocol

  ESP—IP Encapsulating Security Payload
- **AH**—Authentication Header
- **GRE**—Generic Routing Encapsulation
- **IP in IP**—Internet Protocol (IP) in IP (permits or denies IP-in-IP packets)
- **Eth Over IP**—Ethernet-over-Internet Protocol
- **OSPF**—Open Shortest Path First
- **Other**—Any other Internet Assigned Numbers Authority (IANA) protocol. If you choose Other, enter the number of the desired protocol in the Protocol text box. You can find the list of available protocols in the IANA website.

c. In the **Dest. IP/Mask** field, enter the IP address and netmask of the specific destination.

d. If you have chosen TCP or UDP, you will need specify a **Destination Port**. This destination port can be used by applications that send and receive data to and from the networking stack. Some ports are designated for certain applications such as Telnet, SSH, HTTP, and so on.

e. From the **DSCP** drop-down list, choose one of these options to specify the differentiated services code point (DSCP) value of this ACL. DSCP is an IP header text box that can be used to define the quality of service across the Internet. You can choose:

- Any—Any DSCP (this is the default value)
- Specific—A specific DSCP from 0 to 63, which you enter in the DSCP edit box

f. Click the **Apply** icon to commit your changes.

Step 7 Quality of service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies. The primary goal of QoS is to provide priority, including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics.

The Cisco Mobility Express controller supports the following four QoS levels. Under the **QoS** tab, from the **QoS** drop-down list, choose one of the following QoS levels:

- **Platinum (Voice)**—Ensures a high quality of service for voice over wireless.
- **Gold (Video)**—Supports high-quality video applications.
- **Silver (Best Effort)**—Supports normal bandwidth for clients.
- **Bronze (Background)**—Provides the lowest bandwidth for guest services.

Step 8 **Application Visibility** classifies applications using the Network-Based Application Recognition (NBAR2) engine, and provides application-level visibility in wireless networks. Application Visibility enables the controller to detect and recognize more than 1000 applications and perform real-time analysis, and monitor network congestion and network link usage. This feature contributes to the **Applications By Usage** statistic in the **Monitoring** > **Network Summary**.

To enable **Application Visibility**, choose **Enabled** (the default option) from the **Application Visibility** drop-down list. Otherwise, choose **Disabled**.

Step 9 Click **Apply**.

What to do next

You can proceed to create or edit user accounts for a WLAN. See Viewing and Managing WLAN Users, on page 36.

Enabling and Disabling a WLAN

Step 1 Choose **Wireless Settings** > **WLANs**.
The **WLAN Configuration** window is displayed.

Step 2 Click the **Edit** icon adjacent to the WLAN you want to enable or disable.
The **Edit WLAN** window is displayed.

Step 3 Choose **General** > **Admin State** and select **Enabled** or **Disabled**, as required.

Step 4 Click **Apply**.

Note Clicking **Apply** after creating a new WLAN or editing an existing one always enables the WLAN irrespective of whether it was previously enabled or disabled.

Editing and Deleting a WLAN

Choose **Wireless Settings** > **WLANs**. In the window that is displayed, perform one of the following actions:

- To edit a WLAN, click the **Edit** icon adjacent to it.
- To delete a WLAN, click the **Delete** icon adjacent to it.

Viewing and Managing WLAN Users

To view and manage WLAN users, choose **Wireless Settings** > **WLAN Users**.

The **WLAN Users** window is displayed, along with the total number of WLAN users configured on the controller. It also lists all the WLAN users in the network along with the following details for each:

- **User name**—Name of the WLAN user.
- **Guest user**—If this checkbox is selected, then this is a guest user account with a limited validity of only 86400 seconds (or 24 hours) from the time of its creation.
- **WLAN Profile**—The WLANs that this user can connect to.
- **Password**—The password to be used when connecting to a WLAN.
- **Description**—Additional details or comments about the user.

You can view and manage WLAN users only for the WPA2 Enterprise with Local Server setup. To use your Cisco Mobility Express wireless network, a wireless client should connect to a WLAN in the network. To connect to a WLAN, the wireless client will have to use the user credentials set for that WLAN. If this WLAN uses WPA2-Personal as a Security Policy, then the user must provide the appropriate WPA2-PSK set for that WLAN on the Controller AP. If the Security Policy is set to WPA2-Enterprise, the user must provide a valid user identity and the corresponding password set in the RADIUS user database.

Adding a WLAN User

To add a WLAN user, click **Add WLAN User**, and then fill in the following details:

- User name—Specify a name for WLAN user account.
- Guest user—Select this checkbox if this is meant to be a guest WLAN user account. You can also specify the validity of this account from the time of its creation, in seconds, the **Lifetime** field. The default value is 86400 seconds (that is, 24 hours). You can specify a lifetime value from 60 to 31536000 seconds (that is, 1 minute to 1 year).
- WLAN Profile—Select the WLAN that this user can connect to. From the drop-down list, choose a particular WLAN, or choose **Any WLAN** to apply this account for all WLANs set up on the controller.

This drop-down list is populated with the WLANs which have been configured under **Wireless Settings** > **WLANs**.

- Password—The password to be used when connecting to a WLAN.
- Description—Additional details or comments on the user.

Editing a WLAN User

To edit a WLAN user, click the **Edit** icon adjacent to the WLAN user whose details you want to edit and make the necessary changes.

Deleting a WLAN User

To delete a WLAN user, click the **Delete** icon adjacent to the WLAN user you want to delete. and then click **Ok** in the confirmation dialog box.

Managing Associated Access Points

Choose **Wireless Settings** > **Access Points**. The **Access Points Administration** window is displayed. The number of APs associated with the controller is displayed at the top of the window, along with the following details:

- **Manage**—The icons shown below indicate whether the AP is acting as Primary Controller (or Primary AP) or a subordinate AP.

Figure 7: Primary Controller (or Primary AP) icon

Figure 8: Subordinate AP icon

- **Location**—Location of the AP.
- **Name**—Name of the AP.
- **IP Address**—IP address of the AP.
- **AP MAC**—The MAC address of the AP.
- **Up Time**—Shows how long the AP has been associated to the controller.
- **AP Model**—The model number of the access point.

Note When an AP joins an AP group; or the RF profile of the AP group is changed, the CAPWAP process of the AP is restarted, to avoid rebooting of all the APs. A new CAPWAP restart payload is sent to the AP so that only the CAPWAP process is restarted. As a response, the AP will receive the new configuration specific to the new AP group or RF profile. The APs connection to the controller is lost and the AP reloads and re-joins the network.

Administering Access Points

Step 1 Choose **Wireless Settings** > **Access Points**.

The **Access Points Administration** window is displayed. You can only administer those APs that are associated to the controller.

Step 2 Click the **Edit** icon adjacent to the AP you want to manage.
The **Edit** window with the **General** tab is displayed.

Step 3 Under the **General** tab, you can edit the following AP parameters:

- **Operating Mode** and **Make me Controller**—For a primary AP, the **Operating Mode** field shows *AP & Controller*. For other associated APs, this field shows **AP Only**.

  The **Make me Controller** button is available only for subordinate APs that are capable of participating in the primary Election process. Click this button to make this AP the primary AP.

- **IP Configuration**—Choose **Obtain from DHCP** to let the IP address of the AP be assigned by a DHCP server on the network, or choose to have a **Static IP** address. If you choose to have a static IP address, then you can edit the IP Address, Subnet Mask, and Gateway fields.

- **AP Name**—Edit the name of the AP. This is a free text field.

- **Location**—Edit a location for the AP. This is a free text field.

The following non-editable AP parameters are also displayed under the **General** tab:

- AP MAC address
- AP Model number
- IP Address of the access point (non-editable only if **Obtain from DHCP** has been selected).
- Subnet mask (non-editable only if **Obtain from DHCP** has been selected).
- Gateway (non-editable only if **Obtain from DHCP** has been selected).

Step 4 (Only for the primary AP) Under the **Controller** tab, you can manually edit the following controller parameters for the integrated Mobility Express wireless LAN controller:

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

Step 5 Under the **Radio 1** and **Radio 2** tabs you can set the following parameters.

Note The **Radio 1** tab corresponds to the 2.4 GHz (802.11 b/g/n) radio on all APs, except the Cisco Aironet 3800 and 2800 series APs. On these APs, it can be set to either 2.4 GHz (802.11 b/g/n) or 5 GHz (802.11a/n/ac). The **Radio 2** tab corresponds to only the 5 GHz (802.11a/n/ac) radio on all APs.

The radio tab name also indicates the operational radio band within brackets.

Parameter	Description	
Admin Mode	Enable or Disable the corresponding radio on the AP.	
Band	Only present for Radio 1. It is set to 2.4 GHz by default. For 3800 and 2800 series APs you can change it to 5 GHz.	
Channel	For 2.4 GHz, you can set this to Automatic, or set a value from 1 to 11. Selecting **Automatic** enables Dynamic Channel Assignment. This means that channels are dynamically assigned to each AP, under the control of the primary AP. This prevents neighboring APs from broadcasting over the same channel and prevents interference and other communication problems. For the 2.4 GHz radio, 11 channels are offered in the U.S. and up to 14 in other parts of the world. However, only 1-6-11 can be considered non-overlapping if they are used by neighboring APs. Assigning a specific value statically assigns a channel to that AP.	For 5 GHz, you can set this to Automatic, 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, or 165. For the 5 GHz radio, up to 23 non-overlapping channels are offered. Assigning a specific value statically assigns a channel to that AP.
Channel Width	The channel width for 2.4 GHz can only be 20 MHz.	The channel width for 5 GHz can be set to Automatic, or to 20, 40, or 80 MHz, if channel bonding is used. Channel bonding groups the channels by 2 or 4 for a single radio stream. This increases the speed and the throughput. Because the number of channels is insufficient in 2.4 GHz, channel bonding cannot be used to enable multiple non-overlapping channels.

Parameter	Description
Transmit Power	You can set it to Automatic, or set a value from 1 to 8. This is a logarithmic scale of the transmit power, which is the transmission energy used by the AP, with 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 required until the maximum is reached.

Step 6 Click **Apply** to save your changes and exit.

Configuring External Antennas

Before you begin

Antenna configuration is done for the external antenna that have been configured for access points. Configuring antennas are important for receiving better signals. The Antenna Configuration tab is visible in the **AP Edit** window only when there an external antenna configured with the access point (AP).

Step 1 Choose **Wireless Settings** > **Access Points**.

The Access Points Administration window is displayed. The number of APs associated with the controller is displayed at the top of the window

Step 2 Click the **Edit** icon adjacent to the AP you want to configure the external antenna.

Note The Antenna Configuration tab is visible only when there is an external antenna configured with the AP.

The Edit window with the Antenna Configuration tab is displayed.

Step 3 Under the **Antenna Configuration** tab, set the following parameters:

a. Under **Radio 2 (5GHz)**, complete the following parameters:

1. **Diversity** - From the drop-down list select one of the following options:
   a. **Enable**: Select Enable to set the right and the left antennas to operate in the diversity mode. Both the right and left antennas will be enabled for sending and receiving signals.
   b. **Right**: Select the Right option to set the right antenna for receiving and transmitting signals.
   c. **Left**: Select the Left option to set the left antenna for receiving and transmitting signals.
2. Select the following antenna combinations for receiving and transmitting:
   a. **A**—Use antenna A
   b. **AB**—Use antennas A and B
   c. **ABC**—Use antennas A, B, and C

d. **ABCD**—Use antennas A, B, C, and D

Note If you select an invalid combination an error message is displayed.

3. **Antenna Gain** - Specify the resultant gain of the antenna attached to the device. Enter a value from –128 to 128 dB. If necessary, you can use a decimal in the value, such as 1.5.

b. Click **Apply** for the changes to take place.

Setting a Login Page for WLAN Guest Users

Before you begin, follow these steps to provide guest users with access to your network:

1. Set up a new WLAN or decide on an existing WLAN, to which you will provide access for guest users.

   You can also specifically set up a WLAN exclusively for guest access. This is done by setting the **WLAN Security** as **Guest** for that WLAN. For more information, see Adding a WLAN, on page 32.

2. Set up a guest user account. Go to **Wireless Settings** > **WLAN Users**, and set up an account with the **Guest User** check box selected. For more information, see Viewing and Managing WLAN Users, on page 36.

You can present the Guest users of your WLAN with either of the following login page options:

- A simple minimalist default login page with a few modification options. To configure this, see Setting the Default Login Page, on page 41.
- A customized login page uploaded into the controller. To configure this, see Setting a Customized Login Page, on page 42.

Setting the Default Login Page

Right out of the box, the default login page contains a Cisco logo and Cisco-specific text. You can choose to modify this default login page as described here.

Step 1 Choose **Wireless Settings** > **Guest WLAN**.

The Guest WLAN page is displayed. The number of Guest WLANs currently set up in the network is displayed at the top of the page.

Step 2 To use the default login page, in the **Page Type** drop-down list, choose **Internal**.

Step 3 Set the following parameters to modify the default internal login page:

- **Display Cisco Logo**—This field is set to **Yes** by default. To hide the Cisco logo that appears at the top-right corner of the default window, choose **No**. This field is set to **Yes** by default. However, you do not have an option to display any other logo.
- **Redirect URL After Login**— To have guest users redirected to a particular URL (such as the URL for your company) after login, enter the URL in this field. You can enter up to 254 characters.

- **Page Headline**—The default headline is *Welcome to the Cisco Wireless Network*. To create your own headline on the login page, enter the desired text in this field. You can enter up to 127 characters.
- **Page Message**— 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*. To create your own message on the login page, enter the desired text in this field, You can enter up to 2047 characters.

Step 4 Click **Apply**.

Setting a Customized Login Page

You can create a custom login page on a computer, compress the page and image files into a .TAR file, and then upload it to the controller. The upload is done via HTTP.

Note When you save the controller's configuration, it does not include extra files or components, such as the web authentication bundle, that you download and store on your controller. Hence, manually save external backup copies of such files.

Note Cisco TAC is not responsible for creating a custom web authentication bundle.

Before you begin

- Create a custom login page on a computer while ensuring the following:
  - Name the login page **`login.html`**. The controller prepares the web authentication URL based on this name. If the server does not find this file after the web authentication bundle has been untarred, the bundle is discarded, and an error message appears.
  - The page should not contain more than 5 elements (including HTML, CSS, and Images). This is because the internal controller web server implements a DoS protection mechanism that limits each client to open a maximum of 5 (five) concurrent TCP connections depending on the load. Some browsers may try to open more than 5 TCP sessions at the same time if the page contains more elements and this may result in the page loading slowly depending on how the browser handles the DoS protection.
  - Include input text boxes for the username and the password.
  - Extract and set the action URL in the page from the original URL.
  - Include scripts to decode the return status code.
  - All paths used in the main page (to refer to images, for example) are of relative type.
  - No filenames within the bundle are longer than 30 characters.
- Compress the page and image files into a ,TAR file. The maximum allowed size of the files in their uncompressed state is 1 MB.

Cisco recommends that you use an application that complies with GNUstandards to compress the .TAR file (also referred to as the web authentication bundle.). If you load a web authentication bundle with a .TAR compression application that is not GNU compliant, the controller will not be able to extract the files in the bundle.

The .TAR file enters the controller's file system as an untarred file.

Note If you have a complex customized web authentication bundle which does not comply with the aforementioned prerequisites, then Cisco recommends that you host it on an external web server. See (..)

Step 1 Choose **Wireless Settings** > **Guest WLAN**.

The **Guest WLAN** page is displayed. The number of Guest WLANs currently set up in the network is displayed at the top of the page.

Step 2 To upload a customized login page into the controller, in the **Page Type** drop-down list, choose **Customized**.

Step 3 Click **Upload**, to browse to and upload the .TAR file of the customized web authentication bundle.

Step 4 If you want the user to be directed to a particular URL (such as the URL for your company) after login, enter that URL in the **Redirect URL After Login** text box. You can enter up to 254 characters.

Step 5 Click **Apply**.

Click **Preview** to view your customized web authentication login page.

Managing the Internal DHCP Server

The Cisco Mobility Express controller contains an internal DHCP server which manages the DHCP addresses assigned to network devices associated with it. The IP addresses assigned to client devices are not preserved across reboots. This enables reuse of IP addresses across multiple client devices. To resolve IP address conflicts, client devices need to release their existing IP address and request for a new one.

Starting Cisco Wireless Release 8.3, you can configure the internal DHCP server using the Cisco Mobility Express web interface.

Add DHCP Pool

Step 1 Choose **Wireless Settings** > **DHCP Server**.

The **DHCP Configuration** window appears.

Step 2 Click **Add New Pool**.

The **Add DHCP Pool** window appears.

Step 3 In the **Pool Name** field, enter the desired name.

The DHCP pool name must meet the following conditions:

Step 4 From the **Active** drop-down list, select either **Enabled** or **Disabled**.

The default setting is **Disabled**.

Step 5 In the **VLAN ID** field, specify the VLAN ID for the DHCP Pool.

Note Select the **Management Network** checkbox to set the management interface IP address of the Cisco Mobility Express controller as the DHCP server IP address.

Step 6 In the **Network/Mask** fields, specify the IP address of the network and the subnet mask.

Step 7 In the **Start IP** field, specify the starting IP address for the network.

Step 8 In the **End IP** field, specify the ending IP address for the network.

Step 9 In the **Default Gateway** field, specify the IP address for the default gateway to the network.

Note The default gateway, starting IP address, and the ending IP address must be in the same subnet.

Step 10 In the **Domain Name** field, enter the desired name.

The domain name must meet the following conditions:

Step 11 From the **Name Servers** drop-down list, select either **OpenDNS** or **User Defined**.

The default setting is **OpenDNS**.

Step 12 Enter the IP address for the name servers in the provided fields.

Edit DHCP Pool

Step 1 Choose **Wireless Settings** > **DHCP Server**.

The **DHCP Configuration** window appears.

Step 2 Click the <edit_icon.gif> icon in the row containing the DHCP Pool whose details you wish to modify.

The desired row in the DHCP Pool table becomes editable (or the **Edit DHCP Pool** window appears.)

Step 3 In the DHCP Pool table, make the desired modifications inline (or in the **Edit DHCP Pool** window).

Step 4 Click **Apply**.

The DHCP Pool table is refreshed and the updated entry appears in this table.

Delete DHCP Pool

Step 1 Choose **Wireless Settings** > **DHCP Server**.

The **DHCP Configuration** window appears.

Step 2 Click the **X** icon in the row containing the DHCP pool you wish to delete.

A warning message appears.

Step 3 Click **Yes** in the pop-up window.

The DHCP pool table is refreshed and the deleted entry is removed from this table.

View DHCP Lease Details

Step 1 Choose **Wireless Settings** > **DHCP Server**.

The **DHCP Configuration** window appears.

Step 2 Under the DHCP pool table, click **DHCP Leases**.

The **DHCP Pool Information** window appears where you can view details such as the host name, its MAC address, assigned IP address, and lease expiry details.

Note You can release a specific IP address by removing the lease to the host in the corresponding entry of the **DHCP Pool Information** table.

Export Details of Leased IP Addresses

Step 1 Choose **Wireless Settings** > **DHCP Server**.

The **DHCP Configuration** window appears.

Step 2 Under the DHCP pool table, click **DHCP Leases**.

The **DHCP Pool Information** window appears.

Step 3 Below the **DHCP Pool Information** table, click **Export**.

Step 4 Choose the format in which you wish to export the details of the leased IP addresses and the corresponding hosts.

Release Leased IP Address

Step 1 Choose **Wireless Settings** > **DHCP Server**.

The **DHCP Configuration** window appears.

Step 2 Under the DHCP pool table, click **DHCP Leases**.

The **DHCP Pool Information** window appears.

Step 3 In the row containing the the host assigned the leased IP address you wish to delete, click the <release_icon.gif> icon.

A warning message appears.

Step 4 You can release a specific IP address by removing the lease to in the corresponding entry of the **DHCP Pool Information** table.

Step 5 Click **Yes** in the pop-up window.

The **DHCP Pool Information** table is refreshed and the deleted entry is removed from this table.

Information about Authentication Caching

With the Authentication Caching feature, client information essential for authentication is stored locally in the cache on the Controller, when the authentication with the RADIUS Server is successful. When the connectivity to the RADIUS server is lost, the information stored in the cache is used for the authentication of clients.

You can also configure cache when the RADIUS Server is up and running. If the client details are not available locally, the the request for authentication is sent through the RADIUS Server.

The following security types are supported:

- MAC Filtering using RADIUS Server
- WPA/WPA2-Dot1x Authentication
- Web-Auth on MAC Filtering Failure
- Identity PSK (iPSK)

Configuring WPA/WPA2 Dot1x Authentication

Follow the procedure given below to configure WPA/WPA2 Dot1x Authentication:

Step 1 Choose **Wireless Settings** > **WLANs**.
The **WLAN/RLAN Configuration** page is displayed.

Step 2 Click **Add new WLAN/RLAN**.
The Add new WLAN/RLAN window is displayed.

Step 3 Under the **General** tab, set the following parameters:

a) **Profile Name**— The profile name must be unique and should not exceed 32 characters.

b) **SSID**—The profile name also acts as the SSID. You can choose to specify an SSID that is different from the WLAN profile name. Like the profile name, the SSID can not exceed 32 characters and must be unique.

Step 4 Under the **WLAN Security** tab, set one of the following security authentication options from the **Security** drop-down list:

a) **WPA2 Enterprise**—This option stands for Wi-Fi Protected Access 2, with a local authentication server or a RADIUS server.

b) In the **Radius Server** section, enable **Authentication Caching**, enter the **User Cache Timeout** in minutes, and enable **User Cache Reuse**, if required. By default, **User Cache Reuse** is disabled.

c) Click **Add RADIUS Authentication Server**. Enter the server details and click **Apply**.

Note The following are the AV Pairs configured on the RADIUS Server:

- **AC-Supported=yes** - It is sent through ACCESS-REQUEST only to indicate authentication cache support is enabled.
- **AC-User-Name** - Username of the dot1x use is sent as part of ACCESS-ACCEPT.
- **AC-Credential-Hash** - User password hashed using RFC2865 is sent as part of ACCESS-ACCEPT.

Step 5 Choose the **Advanced** tab.

Step 6 Use the **Allow AAA Override** toggle button to enable AAA override.

Step 7 Click **Apply**.

Configuring MAC Filtering on RADIUS Server

Follow the procedure given below to configure MAC Filtering and to enable the On MAC Filter Failure on the RADIUS Server:

Step 1 Choose **Wireless Settings** > **WLANs**.
The **WLAN/RLAN Configuration** page is displayed.

Step 2 Click **Add new WLAN/RLAN**.
The Add new WLAN/RLAN window is displayed.

Step 3 Under the **General** tab, set the following parameters:

a) **Profile Name**— The profile name must be unique and should not exceed 32 characters.
b) **SSID**—The profile name also acts as the SSID. You can choose to specify an SSID that is different from the WLAN profile name. Like the profile name, the SSID can not exceed 32 characters and must be unique.

Step 4 Under the **WLAN Security** tab, set the following parameters:

a) Enable **Guest Network**.
b) Enable **MAC Filtering**.
c) Select **Captive Portal** as **`External Splash Page`**.
d) In the **Captive Portal URL** field, enter the Web Server URL.
e) Select the **Access Type** as **`RADIUS`**.
f) Enable **On MAC Filter Failure**.
g) Click **Add RADIUS Authentication Server**. Enter the server details and click **Apply**.

Step 5 Choose the **Advanced** tab.

Step 6 Use the **Allow AAA Override** toggle button to enable AAA override.

Step 7 Click **Apply**.

Configuring Identity PSK

Follow the procedure given below to configure Identity PSK:

Step 1 Choose **Wireless Settings** > **WLANs**.
The **WLAN/RLAN Configuration** page is displayed.

Step 2 Click **Add new WLAN/RLAN**.
The Add new WLAN/RLAN window is displayed.

Step 3 Under the **General** tab, set the following parameters:

a) **Profile Name**— The profile name must be unique and should not exceed 32 characters.

b) **SSID**—The profile name also acts as the SSID. You can choose to specify an SSID that is different from the WLAN profile name. Like the profile name, the SSID can not exceed 32 characters and must be unique.

Step 4 Under the **WLAN Security** tab:

a) Enable **MAC Filtering**.

b) Set the following security authentication option from the **Security Type** drop-down list:**WPA2 Personal**—This option stands for Wi-Fi Protected Access 2 with pre-shared key (PSK). WPA2 Personal is a method used for securing your network with the use of a PSK authentication.

c) Select the **Passphrase Format** as either **`HEX`** or **`ASCII`**.

d) Enter the **Passphrase** and **Confirm Passphrase**.

e) In the **Radius Server** section, enable **Authentication Caching**, enter the **User Cache Timeout** in minutes, and enable **User Cache Reuse**, if required. By default, **User Cache Reuse** is disabled.

f) Click **Add RADIUS Authentication Server**. Enter the server details and click **Apply**.

After a successful MAC authentication, RADIUS Server returns the following Cisco AVPair attributes:

- **psk-mode** - Value could be either **`ASCII`**, **`HEX`**, **`asciiEnc`**, or **`hexEnc`**.
- **psk**

Note The key is stored in the local cache along with the MAC Address, and is used for subsequent authentications.

Note The psk value could be a simple **`ASCII`** or **`HEX`** value or encrypted bytes in case of **`asciiEnc`** or**`hexEnc`**. The algorithm used for encryption or decryption is as perRFC2865 (user-password section – 16 bytes authenticator followed by encrypted key).

Step 5 Choose the **Advanced** tab.

Step 6 Use the **Allow AAA Override** toggle button to enable AAA override.

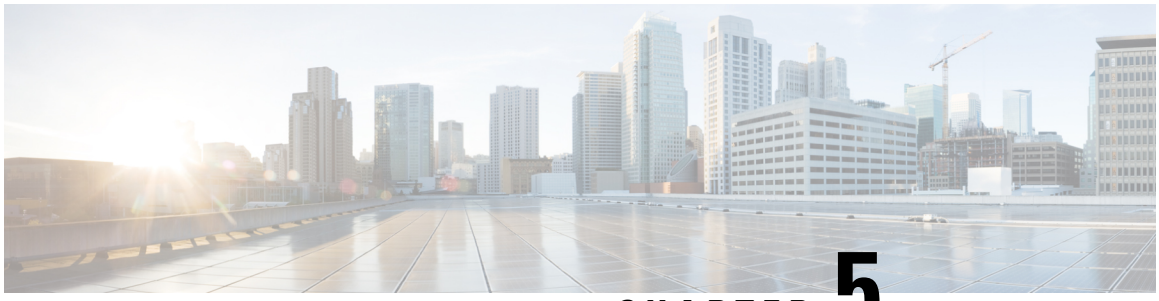
Step 7 Click **Apply**.

Verifying Authentication Cached Users

Step 1 To verify the authenticated cached users, choose **Management** > **Admin Accounts**.
The Admin Accounts page is displayed.

Step 2 In the **Admin Accounts** page, choose the **Auth Cached Users** tab.
The auth cached user summary is displayed with details such as, MacAddress, Username, SSID, Timeout, and Remaining Time.

Step 3 Double-click the listed auth cached user to view the cache details.



CHAPTER 5

Managing the Network

Setting the Management Access Interface

The Management Access Interface is the default interface for in-band management of the controller and connectivity to enterprise services. It is also used for communication between the controller and access points (APs). The management interface has the only consistently pingable in-band interface IP address on the controller. You can access the web interface of the controller by entering the management interface IP address of the controller in your browser's address bar.

For APs, the controller requires one management interface to control all inter-controller communications and one AP manager interface to control all controller-to-access point communications, regardless of the number of ports.

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

Step 1 Choose **Management** > **Access**.

The **Management Access** window is displayed. The number of enabled management types are displayed at the top of the window.

Step 2 You can enable or disable the following types of management access to the controller, by choosing the appropriate option from the drop-down list:

- **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**.

  Note HTTP access mode is not a secure connection.

- **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**.

  Note HTTPs access mode is a secure connection.

- **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**.

  Note Telnet access mode is not a secure connection.

- **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**.

  Note The SSHv2 access mode is a secure connection.

Step 3 Click **Apply** to save your changes.

Managing Admin Accounts

You can manage the Cisco Mobility Express network through the Cisco Mobility Express controller GUI based on the privileges assigned to your user account. This prevents unauthorized users from accessing or configuring the controller.

You can log in to the Cisco Mobility Express GUI using an admin account having one of the following access types:

- **Read/Write**—This administrative account has complete access to view and modify the controller configuration.
- **Read Only**—This limited access administrative account allows the user to only view the controller configuration. This user is restricted from making any changes to the configuration.
- **Lobby Ambassador**—This restricted administrative account allows the user to only create and manage guest user accounts. The lobby ambassador can also print or email the guest user account credentials.

  For information about creating guest user accounts, see Creating a Guest User Account.

Adding an Admin Account

Step 1 Choose **Management** > **Admin Accounts**.

The total count of admin accounts on the Cisco Mobility Express controller is displayed at the top of this window while the table provides a detailed listing of all the available admin accounts.

The **Admin Accounts** window is displayed.

Step 2 Click **Add New User** to add a new admin user.
A new editable row entry appears in the table.

Step 3 Set the following parameters as required:

- **Account name**—The login user name used by the administrative user. Admin account names must be unique.
- **Access**—Set one of the following access privileges for the administrator:
  - **Read Only**
  - **Read/Write**
  - **Lobby Ambassador**
- **Password**—The password is case sensitive and should be created based on the following guidelines:
  - It should have at least eight characters using a combination of numbers, special characters, as well as upper and lower case letters.
  - It should neither contain the word Cisco or a management username nor be a variant of these words obtained by:
    - Reversing the letters of these words
    - Changing the capitalization of the letters
    - Substituting the following:
      - 1, |, or ! for i
      - 0 for o
      - $ for s
  - No character can be repeated more than three times consecutively in the password.

Step 4 Click **Apply** to save your changes.

Editing an Admin Account

Step 1 Choose **Management** > **Admin Accounts**.

The **Admin Accounts** page is displayed, along with the list of all the admin accounts present on the Cisco Mobility Express controller. The total count of admin accounts on the controller is displayed at the top of the page.

Step 2 Click the **Edit** icon adjacent to the account you want to edit.

Step 3 Modify the admin account parameters, as required. For descriptions of these parameters, see Adding an Admin Account, on page 52.

Step 4 Click **Apply**.

Deleting an Admin Account

Step 1 Choose **Management** > **Admin Accounts**.

The **Admin Accounts** window is displayed, along with the list of all the admin accounts present on the Cisco Mobility Express controller. The total count of admin accounts on the controller is displayed at the top of the page.

Step 2 Click the Delete icon adjacent to the account you want to delete.

Step 3 Click **Ok** in the confirmation dialog box.

Managing Guest Users using the Lobby Admin account

Guest user accounts are created to allow temporary access to the network. This network access is granted after successful authentication of the guest account credentials.

You can create and manage guest user accounts using the lobby ambassador admin account. To know more about lobby ambassador accounts, see Managing Admin Accounts, on page 52.

Creating a Guest User Account

Before you begin

You need to have at least one lobby ambassador user account before you can create a guest user account. For information about creating a lobby ambassador account, see Adding an Admin Account, on page 52.

Step 1 In your browser, navigate to the Cisco Mobility Express GUI.

Step 2 Login using valid **Lobby Ambassador** credentials.

The **Lobby Ambassador Guest Management** window appears.

Step 3 Click **Add Guest User**.

The **Add Guest User** dialog box appears.

Step 4 Enter the following details for the guest user account:

- **User Name**
- **Wireless Network**—Select the desired guest WLANs that have already been configured for guest access to the network. If no guest WLANs have been cofigured or no guest WLAN is selected, then **All Guest WLANs** is selected by default.

  Note To know more about creating a guest WLAN, see Adding a WLAN, on page 32.

- **Permanent User**—Select this check box to allow this guest user account access to the network without any time restriction.
- **Expiry Date & Time**—Specify the date and time by clicking the calendar and clock icons respectively. The guest user account gets disabled at the specified date and time preventing access to the guest network.

Note If the **Permanent User** check box is selected, then this field disappears from the dialog box.

- **Generate Password**—Click this radio button to automatically generate a password for the guest user account being created.

  If you prefer to manually specify a password for the guest user account, enter it in the **Password** and **Confirm Password** fields.

- **Password**

  Note If you have clicked the **Generate Password** radio button, then this field disappears from the dialog box.

- **Confirm Password**—Ensure that this entry matches what you have typed in the **Password** field.
- **Description**

Step 5 Click **Update**.

You can choose to share the account credentials with the guest user either via email or by printing it out.

The **Guest User Credentials** pop-up appears while the **Guest Users List** table refreshes to include this new guest user account entry.

Setting Date and Time

The date and time on the Cisco Mobility Express controller is first set when running the initial configuration setup wizard of the controller. You can either enter the date and time manually or you can specify a Network Time Protocol (NTP) server that sets the time and date.

Using NTP Servers to Automatically Set the Date and Time

You can have up to three Network Time Protocol (NTP) servers, to which the controller can automatically sync to set the date and time.

By default three NTP servers are automatically created. The default fully qualified domain names (FQDN) of the NTP servers are:

- 0.ciscome.pool.ntp.org, with NTP Index value 1.
- 1.ciscome.pool.ntp.org, with NTP Index value 2.
- 2.ciscome.pool.ntp.org, with NTP Index value 3.

You can specify the IPv4 address or the FQDN name of an NTP server during the initial configuration wizard. This will be applied to the server having NTP Index 1, thereby overwriting its default FQDN, *0.ciscome.pool.ntp.org* .

For adding and editing NTP server details, go to **Management > Time**. This opens the Time Settings page.

Adding and Editing NTP Servers

You can have up to three Network Time Protocol (NTP) servers, using which the controller can automatically set the date and time.

Step 1 Choose **Management** > **Time**.

The **Time Settings** window is displayed, with the set time zone shown at the top of the page. The current date and time are displayed in the **Set Time Manually** field. Existing NTP servers, if any, are listed in the order of their **NTP Index** values.

Step 2 In the **NTP Polling Interval** field, specify the polling interval, in seconds.

Step 3 To edit an existing NTP server, click its adjacent **Edit** icon. To add a new NTP server, click **Add NTP Server**.

Step 4 You can add or edit the following values for an NTP server:

a) In the **NTP Index** box, specify an NTP Index value to set the priority of the NTP server. NTP Index values can be set from 1 to 3, in the order of decreasing priority. The controller will try and sync with the NTP server with the highest priority first, until the specified polling interval time runs out. If the sync is successful, the controller does not continue trying to sync with any remaining NTP servers. If the sync is unsuccessful, then the controller will try to sync with the next NTP server.

b) In the **NTP Server** box, specify the IP address or the fully qualified domain name (FQDN) for the NTP server. When you specify an FQDN, a DNS lookup is done. If the lookup fails, an error will be logged in the Syslog server. The controller will continue to resolve this FQDN and errors will be logged until you change the NTP configuration or specify a valid FQDN.

Step 5 Click **Apply**.

Refreshing NTP Server Status

The NTP server table on the **Time Settings** page, displays the status of the connection to each NTP server in the **NTP Status** column. The status maybe one of the following:

- **Not Tried**—A sync has not been attempted yet.
- **In Sync**—The controller time is in sync with the NTP server.
- **Not Synched**—The controller time is not in sync with the NTP server.
- **In Progress**—A sync is being attempted.

Click **Refresh** at any time to see the updated NTP statuses.

Deleting and Disabling NTP Servers

To delete an NTP server, choose **Management > Time**. In the **Time Settings** page that is displayed, click the **Delete** icon adjacent the NTP server you want to delete. Click **OK** in the confirmation dialog, and then click **Apply**.

To disable setting the date and time using NTP servers, you will need to delete all configured NTP servers by following the above process.

Configuring Date and Time Manually

Step 1 Choose **Management** > **Time**.

The **Time Settings** window is displayed, with the set time zone shown at the top of the page. The current date and time are displayed in the **Set Time Manually** field.

Note These fields cannot be edited if the **NTP State** is set to **Enable**.

Step 2 From the **NTP State** drop-down list, choose **Disable**.

Step 3 From the **Time Zone** drop-down list, choose your local time zone.

When you choose a time zone that uses Daylight Saving Time (DST), the controller automatically sets its system clock to reflect the time change when DST occurs. In the U.S., DST starts on the second Sunday in March and ends on the first Sunday in November.

Step 4 Select the **Set Time Automatically from Current Location** check box to set the time based on the time zone specified.

Step 5 In the **Set Time Manually** field:

- Click the calendar icon and choose the month, day, and year.
- Click the clock icon and specify the time, in hour and minutes.

Step 6 Click **Apply**.

Updating the Cisco Mobility Express Software

To view the current software version of your Cisco Mobility Express controller:

- Click the gear icon at the top-right corner of the web interface, and then click **System Information**.
- Choose **Management** > **Software Update**.

  This displays the **Software Update** window, with the current software version number displayed at the top.

You can update the Cisco Mobility Express controller software using the controller's web interface. Current configurations on the Cisco Mobility Express controller will not be deleted.

The following table shows the software update methods available.

Method	Link to Method
Updating the software using HTTP **Note** This method is possible only if your network consists of only Cisco Aironet 1830, 1850, 2800, and 3800 access points (which support ap1g4 and ap3g3 images).	See Updating the Software using HTTP, on page 59.
Updating the software using TFTP	See Updating the Software using TFTP, on page 60.
Updating the software using SFTP	See Updating the Software using SFTP, on page 62
Updating the software directly from Cisco.com	See Updating the Software Directly from Cisco.com, on page 63.

A software update ensures that both the internal controller software and the AP software on all the associated APs are updated. APs that have older Cisco Mobility Express AP software, on joining the primary AP after the software upgrade are automatically upgraded to the latest Cisco Mobility Express AP software. This is because, during the software update process, the latest Cisco Mobility Express software for all Cisco Mobility Express-supported APs that are associated with the controller is also downloaded. An AP joining the controller compares its Cisco Mobility Express software version with that on the primary AP and if a mismatch is detected, the new AP requests for a software upgrade. The primary AP facilitates the transfer of the new software from the TFTP server or the HTTP path, to the new AP.

The software download happens in the background, without impacting the network. The upgrades are automatically sequenced to ensure that the network performance is not impacted by software update.

Note The software of up to five access points can be concurrently updated.

Efficient AP Join for Heterogeneous Network

In the Efficient AP Join feature, when a new AP joins the network, the AP downloads the image from the image primary AP instead of downloading from the network file server. When the new AP joins the network, and another AP of the same image type is already present in the network, the new AP downloads the image from the existing AP (image primary). Therefore, the traffic on the WAN network is reduced.

The sequence of the efficient AP join image download, is as follows:

- When a new AP (subordinate AP) joins the Mobility Express (ME) network, ME first checks if the Efficient AP Join feature is enabled, if the AP type is Cisco Wave 2 AP, and if image version is 8.8 or later versions.
- ME sends the primary and subordinate configuration messages to the selected primary. Trigger messages are sent to the subordinate as a response to the join message.
- Thereafter, the subordinate AP contacts the image primary AP to download the image via TFTP. If there is no response from the image primary AP, the subordinate AP continuously sends TFTP requests to the image primary AP and goes back to the discovery mode if the retry count is exceeded.
- If the subordinate AP downloads the image from the image primary successfully, the subordinate AP reboots and joins the ME with the new image.

Note If the system does not have sufficient memory, the fallback is to stream image from external server down to new AP join.

This fallback is not supported if you have configured the transfer mode as HTTP.

Configuring Efficient AP Join

Before you begin

The Cisco Wireless Release version should be 8.8 or later versions, to support the Efficient AP Join feature.

Step 1 Navigate to **Management** > **Software Update**.

Step 2 Enable the Efficient Join option and click the Apply button.

To enable or disable the efficient join feature, use the command given below. By default, the feature is enabled.

```
(Cisco Controller) > config flexconnect group default-flexgroup efficient-join {enable | disable}
```

Verifying the Status of Efficient AP Join

To verify the status of the efficient AP join feature on ME, use the following **show** command:

```
(Cisco Controller) > show flexconnect group detail default-flexgroup
```

To verify the progress of the download, use the following **show** commands:

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

```
(Cisco Controller) > show flexconnect efficient-upgrade aps
```

Updating the Software using HTTP

Before you begin

You can perform the software update via HTTP only if your network consists of only Cisco Aironet 1830, 1850, 2800, and 3800 access points (which support ap1g4 and ap3g3 images). If you have other supported AP models in your network, then use TFTP or update directly from Cisco.com.

Step 1 Get the controller software image by following these steps:

a) Using a computer, browse to the Cisco Download Software page at: http://www.cisco.com/cisco/software/navigator.html.

b) Browse to your AP model and click **Mobility Express Software** to view the list of currently available software, with the latest release at the top.

c) Choose a software release number.

d) Click **Download** corresponding to the ZIP file.

e) Read Cisco's End User Software License Agreement and then click **Agree**.

f) Save the ZIP file to your computer's hard drive, and then extract the contents to a directory on your computer.

Step 2 From the Cisco Mobility Express controller web interface, choose **Management > Software Update**.

The **Software Update** window, with the current software version number, is displayed.

Step 3 In the **Transfer Mode** drop-down list, choose **HTTP**.

Step 4 Click the **Browse** button adjacent the **File** field, browse to the folder having the unpacked ZIP file contents, and choose the software file as indicated in the following table.

Cisco AP Series of the Mobility Express Controller	Software File to be Chosen
1830, 1850	ap1g4
2800, 3800	ap3g3

Note The file explorer that opens here is an operating system-specific explorer depending on the OS of your computer.

Step 5 To set the controller to automatically reboot after the image pre-download is complete, check the **Auto Restart** check box.

You can also manually reboot the controller, after the upgrade, by choosing **Advanced > Controller Tools**, and clicking **Restart Controller**.

Step 6 Click **Apply** to save the parameters that you have specified.

These parameters will remain saved unless you specifically change them in future. You do not have to enter these parameters afresh for the next software update.

Step 7 Click **Update Now**, and then click **Ok** in the confirmation dialog.

The top section of the page indicates the status of the download. Do not manually power down or reset the controller or any AP during this process; otherwise, you might corrupt the software image.

The Image Pre-Download Status section of the page shows the status of the pre-image download to the APs in the network.

You can cancel a software update that is in progress, at anytime before the controller completes rebooting, by clicking **Abort**.

Step 8 After the image pre-download is complete, the controller must restart (or reboot) to complete the software upgrade. If you have not checked the **Auto Restart** check box, you can manually reboot the controller, after the upgrade, by choosing **Advanced > Controller Tools**, and clicking **Restart Controller**.

For more information on the image pre-download feature, see Predownloading an Image to an Access Point, on page 101.

You can cancel a software update that is in progress, at anytime before the controller completes rebooting, by clicking **Abort**.

Step 9 Log in to the controller and verify the controller software version in the **Software Update** window.

Updating the Software using TFTP

Before you begin

- Prepare a TFTP server, following these guidelines, for hosting the Cisco Mobility Express software file:
  - Ensure that the TFTP server supports extended TFTP for file sizes greater than 32 MB. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within the Cisco Prime Infrastructure.
  - If you attempt to download the controller software and your TFTP server does not support files of this size, this error message appears: `TFTP failure while storing in flash`
  - If you are upgrading through the distribution system network port, the TFTP server can be on the same subnet or a different subnet because the distribution system port is routable.
- A computer that can access Cisco.com and the TFTP server, should be available.

Note Ensure that the TFTP server always has the same Cisco Mobility Express software bundle as that on the Cisco Mobility Express controller, or the latest software bundle.

Step 1 Get the controller software image by following these steps:

a) Using a computer, browse to the Cisco Download Software page at: http://www.cisco.com/cisco/software/navigator.html.
b) Browse to your AP model and click **Mobility Express Software** to view the list of currently available software, with the latest release at the top.
c) Choose a software release number.
d) Click the filename.
e) Click **Download** corresponding to the ZIP file.
f) Read Cisco's End User Software License Agreement and then click **Agree**.
g) Save the file to your computer's hard drive.
h) Copy the file from your computer's hard drive, and then unzip and extract the entire contents to the default directory on your TFTP server.

Step 2 From the Cisco Mobility Express controller web interface, choose **Management > Software Update**.

The **Software Update** window, with the current software version number, is displayed.

Step 3 In the **Transfer Mode** drop-down list, choose **TFTP**.

Step 4 In the **IP Address (IPv4)** field, enter the IP address of the TFTP server.

Step 5 In the **File Path** field, enter the TFTP server directory path of the software file, along with the name of the file.

Step 6 To set the controller to automatically reboot after the image pre-download is complete, check the **Auto Restart** check box.

You can also manually reboot the controller, after the upgrade, by choosing **Advanced > Controller Tools**, and clicking **Restart Controller**.

Step 7 Click **Apply** to save the parameters that you have specified.

These parameters will remain saved unless you specifically change them in future. You do not have to enter these parameters afresh for the next software update.

Step 8 You can perform the update right away or schedule it for a later time.

- To proceed with the update right away, click **Update Now**, and then click **Ok** in the confirmation dialog.
- To perform the update at a later time, up to a maximum of 5 days from the current date, specify the later date and time in the **Set Update Time** field, and then click **Schedule Update**.

The top section of the page indicates the status of the download. Do not manually power down or reset the controller or any AP during this process; otherwise, you might corrupt the software image.

The Image Pre-Download Status section of the page shows the status of the pre-image download to the APs in the network.

You can cancel a software update that is in progress, at anytime before the controller completes rebooting, by clicking **Abort**.

Step 9 After the image pre-download is complete, the controller must restart (or reboot) to complete the software upgrade. If you have not checked the **Auto Restart** check box, you can manually reboot the controller, after the upgrade, by choosing **Advanced > Controller Tools**, and clicking **Restart Controller**.

For more information on the image pre-download feature, see Predownloading an Image to an Access Point, on page 101.

You can cancel a software update that is in progress, at anytime before the controller completes rebooting, by clicking **Abort**.

Step 10 Log in to the controller and verify the controller software version in the **Software Update** window.

Updating the Software using SFTP

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

Step 1 Get the controller software image by following these steps:

a) Using a computer, browse to the Cisco Download Software page.
b) Navigate to the desired AP model and click **Mobility Express Software** to view the list of currently available software, with the latest release at the top.
c) Choose the desired software release number.
d) Click the filename.
e) Click **Download** corresponding to the ZIP file.
f) Read Cisco's End User Software License Agreement and then click **Agree**.
g) Save the file to your computer's hard drive.
h) Copy the file from your computer's hard drive, and then unzip and extract the entire contents to the default directory on your SFTP server.

Step 2 From the Cisco Mobility Express controller web interface, choose **Management > Software Update**.

The **Software Update** window, with the current software version number, is displayed.

Step 3 In the **Transfer Mode** drop-down list, choose **SFTP**.

Step 4 In the **IP Address (IPv4)/Name** field, enter the IP address or the domain name of the SFTP server.

Step 5 In the **Port Number** field, enter the port number. The default is 22.

Step 6 In the **File Path** field, enter the SFTP server directory path of the software file.

Step 7 Enter the username and password to log in to the SFTP server.

Step 8 You can perform the update right away or schedule it for a later time.

- To proceed with the update right away, click **Update**, and then click **Ok** in the confirmation dialog.
- To perform the update at a later time, up to a maximum of 5 days from the current date, click the **Schedule Update** toggle button and specify the later date and time in the **Set Update Time** field.

Step 9 To set the controller to automatically reboot after the image pre-download is complete, check the **Auto Restart** check box.

You can also manually reboot the controller, after the upgrade, by choosing **Advanced > Controller Tools**, and clicking **Restart Controller**.

Step 10 Click **Apply** to save the parameters that you have specified.

`

These parameters will remain saved unless you specifically change them in future. You do not have to enter these parameters afresh for the next software update.

Step 11 After the image pre-download is complete, the controller must restart (or reboot) to complete the software upgrade. If you have not checked the **Auto Restart** check box, you can manually reboot the controller, after the upgrade, by choosing **Advanced > Controller Tools**, and clicking **Restart Controller**.

For more information on the image pre-download feature, see Predownloading an Image to an Access Point, on page 101.

You can cancel a software update that is in progress, at anytime before the controller completes rebooting, by clicking **Abort**.

Step 12 Log in to the controller and verify the controller software version in the **Software Update** window.

Updating the Software Directly from Cisco.com

Before you begin

- The primary AP's serial number must be present in the service contract. This cannot be done through the Cisco.com site. You need to contact Cisco customer service to have the serial number added to your service contract.

  However, if you have done a Return to Manufacturer Authorization (RMA), the serial number gets added to the service contract by the team that replaces the device. Certain Cisco partners having access to the Cisco Services Contract Center database can also get the serial number added in the service contract.
- You should have valid Cisco.com user credentials.
- The Mobility Express controller should be able to reach Cisco.com.

Step 1 From the **Software Update Mode** drop-down list, choose **Cisco.com**.

Step 2 Enter the Cisco.com username and password of your Cisco.com account.

To clear any existing and previously used credentials, click **Clear Credentials**, before entering new credentials .

Step 3 To set the controller to automatically check for software updates, choose **Enabled** in the **Automatically Check for Updates** drop-down list. This is enabled by default.

When a software check is done and if a newer latest or recommended software update is available on Cisco.com, then:

- the Software Update Alert icon at the top right corner of the GUI will be Green in color (Grey otherwise). Clicking the icon will bring you to the **Software Update** page.
- the **Update** button at the bottom of the **Software Update** page is enabled.

Step 4 Click **Apply**.

This saves the entries or changes you have made in the Software Update Mode, Cisco.com credentials, and Automatically Check For Updates fields.

The controller runs the automatic check every 30 days to check for the latest software and the recommended software versions that are available for download on Cisco.com. This information is then displayed in the **Latest Software Release** and **Recommended Software Release** fields. You can view the release notes of displayed releases by clicking the "**?**" icon next to it.

The **Last Software Check** field displays the time stamp of the last automatic or manual software check.

If your Cisco.com username, password, or both, are not valid, then the software check will fail and you will not be able to a perform the software update.

Step 5 Manually run a software check by clicking **Check Now**.

You can manually run a software check at any time by clicking **Check Now**.

Step 6 To proceed with the software update, click **Update**.

The **Software Update Wizard** appears. The wizard takes you through the following three tabs in sequence:

- **Release** tab—Specify whether you want to update to the recommended software release or the latest software release
- **Update** tab—Specify when the APs should be reset. You can opt to have it done right away or schedule it for a later time.

  To set the controller to automatically reboot after the image pre-download is complete, check the **Auto Restart** check box.
- **Confirm** tab—Confirm your selections.

Follow the instructions in the wizard. You can go back to any tab at anytime before you click **Confirm**. After you click **Confirm**, the **Cisco Software EULA** is displayed.

Step 7 Click **Agree** to accept the EULA and start the update. The update will cancel displaying an error if you do not accept the EULA.

You can cancel a software update that is in progress, at anytime before the controller completes rebooting, by clicking **Abort**.

What to do next

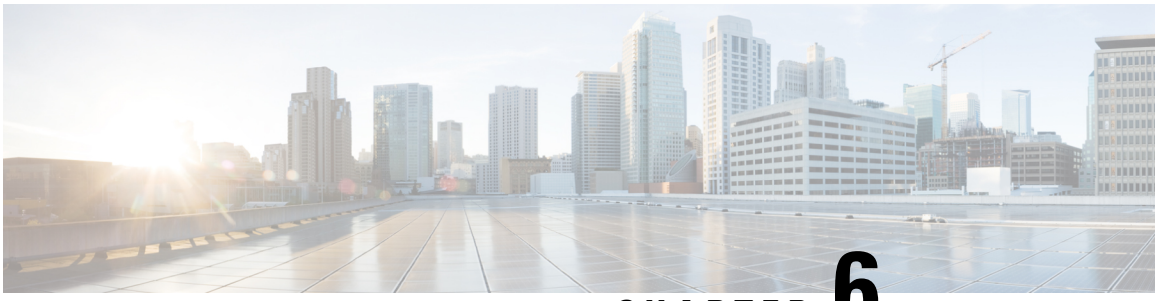
You can monitor the status and progress of the update on the **Software Update** page. The following data is displayed as the update progresses:

- Total number of APs in the network.
- Number of APs that:
  - Are currently being updated.
  - Are waiting to be updated.
  - Are being rebooted.
  - Failed to update.

Additionally for each AP, the progress of the update is also shown using the following data:

- AP Name
- State - Waiting to be updated, Pre-downloading software, Rebooting, or Failed
- Download Percentage with color
- Update Attempts
- Last Update Error

You can cancel a software update that is in progress, at anytime before the controller completes rebooting, by clicking **Abort**.



CHAPTER 6

Using Services

mDNS

Information about Multicast Domain Name System

Multicast Domain Name System (mDNS) service discovery provides a way to announce and discover the services on the local network. The mDNS service discovery enables wireless clients to access Apple services such as Apple Printer and Apple TV advertised in a different Layer 3 network. mDNS performs DNS queries over IP multicast. mDNS supports zero-configuration IP networking. As a standard, mDNS uses multicast IP address 224.0.0.251 as the destination address and 5353 as the UDP destination port.

Location Specific Services

The processing of mDNS service advertisements and mDNS query packets support Location Specific Services (LSS). All the valid mDNS service advertisements that are received by the controller are tagged with the MAC address of the AP that is associated with the service advertisement from the service provider while inserting the new entry into the service provider database. The response formulation to the client query filters the wireless entries in the SP-DB using the MAC address of the AP associated with the querying client. The wireless service provider database entries are filtered based on the AP-NEIGHBOR-LIST if LSS is enabled for the service. If LSS is disabled for any service, the wireless service provider database entries are not filtered when they respond to any query from a wireless client for the service.

LSS applies only to wireless service provider database entries. There is no location awareness for wired service provider devices.

The status of LSS cannot be enabled for services with the ORIGIN set to wired and vice versa.

mDNS Policy

This section explains how you can define a policy to access a specific service provider. The access policy explains the client attributes, the constructs, and the rule components that make up the policy; and how rules and policies are evaluated. This helps in deciding whether the given service provider should be included in the mDNS response for the client (that made the mDNS query).

When LSS is enabled, it provides the information only about nearby service providers. But, MDNS Policy enables you to define a policy that is even more granular.

mDNS policies can be framed based on:

- User
- Role
- AP Name
- AP Location
- AP Group

mDNS Policy Limitations

The limitations of the mDNS policy are as follows:

- LSS cannot be applied in conjunction with the mDNS policy.
- Role and User info is provided from the ISE server.
- If the keyword **Any** is used as a rule parameter value, then that check is bypassed.
- Since the rule is applied based on Service Provider MAC, the rule is evaluated for all the services advertised by the service provider.
- mDNS Policy is applied based on Service Provider MAC and not based on the mDNS Service.
- mDNS Policy will be active only when mDNS Snooping is enabled.
- The maximum number of policies that can be configured per MAC address is limited to five policies.

Client Attributes in an mDNS Policy

Any client initiating an mDNS query is associated with a set of attributes that describe the context of the client. The list of attributes can be Role, User-Id, associated AP Name, associated AP Location, and associated AP Group. Only these enumerated attributes are used to articulate an access policy rule.

The attribute Location, for example, dynamically changes when the client move to a different location. You can formulate a rule by combining these attributes with logical OR operations and attach the rule to the policy.

A service group can have one or more rules.

mDNS AP

The mDNS AP feature allows the controller to have visibility of the wired service providers that are on VLAN. You must configure VLANs on all APs. VLAN visibility on the controller is achieved by the APs that forward the mDNS advertisements to the controller.

Use the configurable knob that is provided on the controller to start or stop mDNS packet forwarding, through the internal AP. You can also use this configuration to specify the VLANs from which the AP should snoop the mDNS advertisements from the wired side. The maximum number of VLANs that an AP can snoop is 10.

Note By default, the mDNS AP does not snoop on any VLAN, you must specify the Management VLAN to snoop on the mDNS packets.

The mDNS AP configuration is retained on those mDNS APs even if global mDNs snooping is disabled.

Priority MAC Support

You can configure up to 50 MAC addresses per service; these MAC addresses are the service provider MAC addresses that require priority. This guarantees that any service advertisements originating from these MAC addresses for the configured services are learned even if the service provider database is full by deleting the last nonpriority service provider from the service that has the highest number of service providers. When you configure the priority MAC address for a service, there is an optional parameter called **ap-group**, which is applicable only to wired service providers to associate a sense of location to the wired service provider devices. When a client mDNS query originates from this **ap-group**, the wired entries with priority MAC and **ap-group** are looked up and the wired entries are listed first in the aggregated response.

Origin-Based Service Discovery

You can configure a service to filter inbound traffic that is based on its origin, that is either wired or wireless. All the services that are learned from an mDNS AP are treated as wired. When the learn origin is wired, the LSS cannot be enabled for the service because LSS applies only to wireless services.

A service that has its origin set to wireless cannot be changed to wired if the LSS status is enabled for the service because LSS is applicable only to wireless service provider database. If you change the origin between wired and wireless, the service provider database entries with the prior origin type are cleared.

Restrictions for Configuring Multicast DNS

- mDNS over IPv6 is not supported.
- mDNS is not supported on remote LANs.
- Third-party mDNS servers or applications are not supported on the controller using the mDNS feature. Devices that are advertised by the third-party servers or applications are not populated on the mDNS service or device table correctly on the controller.
- In a Layer2 network, if Apple servers and clients are in the same subnet, mDNS snooping is not required on the controller. However, this relies on the switching network to work. If you use switches that do not work as expected with mDNS snooping, you must enable mDNS on the controller.
- Video is not supported on Apple iOS 6 with WMM in enabled state.
- mDNS APs cannot duplicate the same traffic for the same service or VLAN.
- LSS filtering is restricted to only wireless services.
- The LSS, mDNS AP, Priority MAC address, and origin-based discovery features cannot be configured using the controller GUI.
- mDNS-AP feature is not supported in CAPWAP V6.
- mDNS user profile mobility is not supported in guest anchors.

- Apple devices such as iPads and iPhones can discover Apple TV through Bluetooth. This might result in Apple TVs being visible to end users.

Configuring Multicast DNS

Step 1 Configure the global mDNS parameters and the Master Services Database by following these steps:

a) Click the **Switch to Expert View** icon. A message is displayed, confirming if you want to switch to the expert view. Click Yes.

b) Choose **Services** > **mDNS**.

c) Use the **mDNS Global Snooping** toggle button to enable or disable snooping of mDNS packets, respectively.

d) Enter the mDNS query interval in minutes. The query interval is the frequency at which the controller queries for a service. Default is 15 minutes.

e) Click the Add VLAN Id button to add a list of VLANs for internal AP snooping.

Note
- VLANs added from the ME GUI will be configured on all the APs (Internal and External). Individual AP VLANs can be configured only by running the **config mdns ap vlan add vlan-id ap-name** command.
- The 'mDNS VLAN Mapping' table on the GUI only lists the VLANs that are set on the internal AP. Since you can configure VLAN specifically on the external APs only by running the **config mdns ap vlan add vlan-id ap-name** command, you can view the VLANs added on all the APs (both internal and external) only by running the **show ap summary** command. GUI does not show the VLANs, if any, set on the external APs.

f) Complete the details in the following tabs:

1. **Master Services Database** – to view the services listed in the primary database. The controller snoops and learns about the mDNS service advertisements only if the service is available in the Master Services Database. The controller can snoop and learn a maximum of 64 services.
   - Click the **Add Service** button to add a new service in the primary database.
   - In the **Add/Edit mDNS Service** window, specify the **Service Name**, **Service String**, **Query Status**, **Location Services**, and **Origin**.
   - Click **Update**.
2. **mDNS Profiles** – to view the list of mDNS profiles.
   - Click the **Add Profile** button to add a new profile.
   - In the **Add/Edit mDNS** window, enter the profile name that can be later mapped to the WLAN.
3. **Domain Names** – to view domain names and add domain names from the discovered list.
4. **mDNS Browser** – to view the number of mDNS services running.

g) Click **Apply**.

Step 2 Map an mDNS profile to a WLAN by following these steps:

a) Choose **Wireless Settings** > **WLANs**.

b) Click **Add new WLAN**. The Add new WLAN window is displayed.
c) In the Add new WLAN window, select the **Advanced** tab.
d) Use the **mDNS** toggle button to enable or disable mDNS.
e) From the **mDNS Profile** drop-down list, choose a profile.
f) Use the **Passive Client** toggle button to enable the passive client. Ensure that you enable Global Multicast in Services > Media Stream, as Passive Client will not work when Global Multicast is disabled.
g) Enter the **Multicast IP** address.
h) Use the **Multicast Direct** toggle to enable multicast direct.
i) Click **Apply**.

Note The wireless controller advertises the services from the wired devices (such as Apple TVs) learned over VLANs, when:

- mDNS snooping is enabled in the WLAN Advanced options.
- mDNS profile is enabled either at the interface or WLAN.

Configuring mDNS Policy

Configure the mDNS policy by following these steps:

a) Click the **Switch to Expert View** icon. A message is displayed, confirming if you want to switch to the expert view. Click Yes.
b) Choose **Services** > **mDNS**.
c) Use the **mDNS Global Snooping** toggle button to enable or disable snooping of mDNS packets, respectively.
d) Use the **mDNS Policy** toggle button to enable or disable mDNS policy, respectively.
e) Enter the mDNS query interval in minutes. The query interval is the frequency at which the controller queries for a service. Default is 15 minutes.
f) Click the **mDNS Policy** tab.
The number of mDNS policies are displayed.
g) Click the **Add mDNS Policy** button.
In the Add mDNS Policy window, you must first add the mDNS Service Group.

1. Enter the **mDNS Service Group Name** and the **Description**.
2. Click the **Add Service Instance** button. The Add Service Instance window is displayed. Complete the following details to add a service instance:
   - **Mac Address**
   - **Name**
   - **Location Type** - Choose the Location Type by AP Group, AP Name, or AP Location.
   - **Location** - Based on the Location Type selected.
3. Click **Apply**.

The service instance created is displayed in the mDNS Policy window.

h) Enter the **Policy/Rule** and click **Apply**.

Cisco Umbrella

Overview of Cisco Umbrella on Cisco Mobility Express

The Cisco Umbrella platform is a cloud-delivered network security solution. At the Domain Name System (DNS) level, it provides real-time insights that help protect devices from malware and breach. As of Cisco Mobility Express Release 8.8, Cisco Umbrella mapping is supported only at the WLAN level.

Cisco Umbrella works in the following manner in Cisco Mobiliry Express:

- Wireless clients join a wireless controller and send DNS queries when they initiate traffic to the Internet. Cisco Umbrella transparently intercepts the DNS traffic and redirects the DNS queries to the Cisco Umbrella cloud servers.
- Security policies based on fully qualified domain names (FQDN) in a DNS query are defined in the Cisco Umbrella cloud servers.
- Based on the FQDN in a DNS query, Cisco Umbrella returns one of the following responses:
  - Malicious FQDN: Returns Cisco Umbrella-blocked page IP to the corresponding client.
  - Safe FQDN: Returns Destination IP address.

Cisco Umbrella Support in Cisco Mobility Express

- Up to 10 different Cisco Umbrella profiles are supported, each with a unique device ID.
- In the context of mapping Cisco Umbrella profiles or device IDs to wireless entities, only WLAN level mapping is supported.
- In the context of provisioning device IDs to APs, AP snoops the DNS packets and applies EDNS tags.
- Forced or Ignore Open modes are supported.
- The new DHCP-6 override option is supported at the WLAN level.

Limitations

This feature does not work with the following:

- This feature does not work with the following:
  - Cisco IOS APs
  - Local-auth
  - IPv6 addresses
-
- If an application or host uses an IP address directly, instead of using DNS to query domain names.

- If a client is connected to a web proxy and does not send a DNS query to resolve the server address.
- Wired guests and clients behind Workgroup Bridges (WGB).
- Virtual Wireless LAN Controller (WLC).
- The application of wireless Cisco Umbrella profiles on wireless entities, like WLAN, through configuration, is dependent on the success of the registration of the device.
- The Cisco Umbrella Cloud provides two IPv4 addresses. WLC/AP uses the first server address that is configured. It does not load balance across servers.

Configuring Cisco Umbrella on Cisco Mobility Express (GUI)

Configure Cisco Umbrella on Cisco Mobility Express by doing these steps:

Before you begin

- You should have an account with Cisco Umbrella.
- You should have an API token from Cisco Umbrella.

Step 1 Click the **Switch to Expert View** icon.

A message is displayed, confirming if you want to switch to the expert view. Click **Ok**.

Step 2 Choose **Services** > **Umbrella**.

Step 3 Use the **Umbrella Global Status** toggle button to enable or disable the Umbrella status, respectively.

Step 4 Enter the **Umbrella API Token** that you obtained from Cisco Umbrella.

Step 5 Click **Apply** to enable Cisco Umbrella.

Step 6 Click **Add Profile** to create a new profile.

The Add Profile Name window is displayed.

Step 7 Enter the **Profile Name** and click **Apply**.

A new profile is created.

Step 8 Map a Cisco Umbrella profile to WLAN by following these steps:

a) Choose **Wireless Settings** > **WLANs**.
b) Click **Add new WLAN/RLAN.** The Add new WLAN/RLAN window is displayed.
c) In the Add new WLAN window, select the **Advanced** tab.
d) From the **Umbrella Profile** drop-down list, choose a profile.
e) From the **Umbrella Mode** drop-down list, choose either **Ignore** or **Forced**.
f) Use the **Umbrella DHCP Override** toggle button to enable the Cisco Umbrella DHCP override.
g) Click **Apply**.

What to do next

1. From Cisco Umbrella Dashboard, verify that your Cisco WLC shows up under **Device Name**, along with their identities
2. Create classification rules for the user roles, for example, rules for employees and nonemployees.
3. Configure policies on the Cisco Umbrella server.

Configuring Cisco Umbrella on Cisco Mobility Express (CLI)

This section describes the procedure to configure Cisco Umbrella on Cisco Mobility Express:

Before you begin

- You should have an account with Cisco Umbrella.
- You should have an API token from Cisco Umbrella.

Step 1 To enable or disable Cisco Umbrella, use the **config opendns** {**enable** | **disable**}

Example:

```
(Cisco Controller) > config opendns enable
```

Enables or disables the Cisco Umbrella global configuration.

Step 2 **config opendns api-token** *api-token*

Example:

```
(Cisco Controller) > config opendns api-token D0986C18DC334FB2E3AA46148D600A4001E5997
```

Registers the Cisco Umbrella API token on the network.

Step 3 **config opendns profile** {**create** | **delete** | **refresh**} *profilename*

Example:

```
(Cisco Controller) > config opendns profile create profile1
```

Creates, deletes, or refreshes a Cisco Umbrella profile that can be applied over a WLAN.

Step 4 **config wlan opendns-profile** *wlan-id profile-name* {**enable** | **disable**}

Example:

```
(Cisco Controller) > config wlan opendns-profile 1 profile-name enable
```

Maps the Cisco Umbrella profile identity to a WLAN.

Step 5 **config wlan opendns-dhcp-opt6** *wlan-id* {**enable** | **disable**}

Example:

```
(Cisco Controller) >config wlan opendns-dhcp-opt6 1 enable
```

Enables or disables DHCP option 6 per WLAN.

Step 6 **config wlan opendns-mode** *wlan-id* {**ignore** | **forced**}

Example:

```
(Cisco Controller) >config wlan opendns-mode 1 forced
```

Ignores or Forces the Cisco Umbrella mode on the WLAN.

TLS

TLS Secure Tunnel

Transport Layer Security (TLS) provides secure and reliable signaling and data transfer between two systems or devices, by using secure ports and certificate exchange. To overcome the challenge of multi-site deployment Cisco Mobility Express uses TLS Secure Tunnel to establish a secure connection from Cisco Mobility Express to the central data center. Inbound traffic includes SSH, SNMP, Ping, HTTP, HTTPS, and TFTP; and outbound traffic includes SNMP, RADIUS, and TFTP

TLS Tunnel has two components:

- TLS Client: TLS Client has been embedded in the Cisco Mobility Express code and will run on the primary AP.
- TLS Gateway: This is a Virtual Machine which is deployed at the central site to establish the TLS Tunnel. TLS Gateway has two network interfaces – Public Network and Private Network.

Following are the features of the TLS Client:

- Zero Touch Provisioning support with PnP
- FQDN support for TLS Gateway
- PSK-based authentication
- Dead Peer Detection (DPD)
- Implicit and Explicit configuration for traffic tunneling
- NAT and Firewall traversal support
- Support System information for device parameters - serial number, MAC address, and system name

Following are the features of TLS-Gateway:

- VMware based Virtual Security Solution
- Dynamic IP allocation to TLS client - Static Pool based IP allocation with TLS-GW internal DHCP server.
- Dead Peer Detection (DPD) and Periodic Re-keying - Configuring DPD and Rekey intervals, DPD – in sync with NAT timeout.
- PSK Authentication - Pre-Shared Key (PSK) based authentication, multiple PSK configurations, and encrypted storage of PSK on the Gateway.
- Internal DNS Server - Configurable DNS server for the TLS client for DNS resolution.

- Connection Rate Limiting - Connection Rate limit of 50 connections per second.
- Scale Characteristic - Scale limit of 10000 tunnels per instance.
- IP Event Notification - Notify events when the TLS client tunnel is connected, disconnected, and reconnected (rekey); to Notify Server [syslog server] Netconf/Restconf.
- Serviceability - Configuration CLIs, Debug Stats (Gateway level and Device Level), and Logging supported.
- SSH login control - Support for enabling and disabling SSH login to TLS Gateway VM (only on private interface).

The Cisco Mobility Express Secure Tunnel supports:

- Outbound - SNMP Traps, RADIUS (Authentication/Accounting)
- Inbound - SNMP, SSH, Ping, HTTPS, and HTTP
- TLS Gateway FQDN
- PSK based authentication
- Inbound traffic - TFTP, SFTP, and FTP
- Rekey Mechanism
- Implicit and Explicit ways of configuration for tunneling the traffic. Implicit Tunneling enables the application for tunneling. For example, SNMP Traps or RADIUS. Explicit Tunneling adds the host or network for tunneling. For example, SSH and PI/SNMP, and Cisco DNA Center.

Following is the sequence of steps given below when configuring the TLS Secure Tunnel for Cisco Mobility Express:

1. Deploying the TLS Gateway - Follow the steps listed here to deploy the TLS Gateway at the central site.
2. CLI Configuration - For more information, refer to the Mobility Express Controller Commands section.
3. Configuring TLS (GUI) - For more information, refer to Configuring TLS Tunnel.

Configuring TLS Tunnel

Follow the procedure given below to configure TLS Tunnel:

Step 1 Click the **Switch to Expert View** icon.
A message is displayed, confirming if you want to switch to the expert view. Click **Yes**.

Step 2 Choose **Services** > **TLS**.
The TLS Tunnel Settings page is displayed.

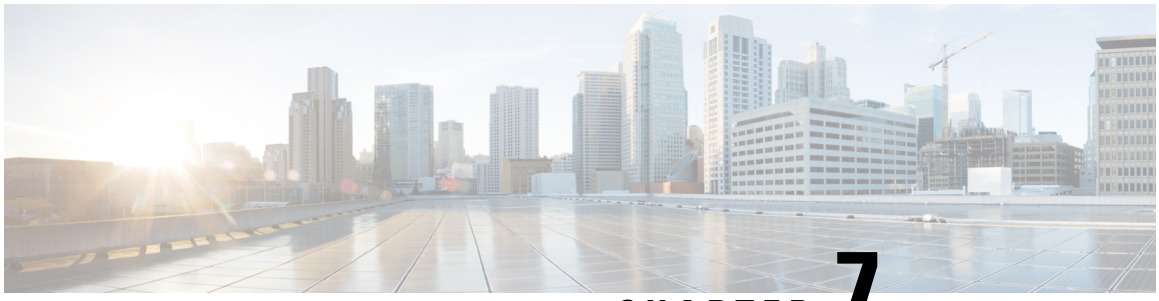
Step 3 Use the **TLS Tunnel** toggle button to enable or disable TLS Tunnel.

Step 4 On the TLS Tunnel Settings page, configure the following parameters:

- Enter the **TLS Gateway URL/IP Address**
- Enter the PSK ID

- Enter the PSK Key
- Enable RADIUS and SNMP

Step 5 Click Apply.



CHAPTER 7

Using Advanced Settings and Operations

Managing SNMP

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

Starting Cisco Wireless Release 8.3, you can configure both SNMPv2c and SNMPv3 using the Cisco Mobility Express web interface.

Configuring SNMP Access

You can configure the following SNMP access modes for the Cisco Mobility Express primary AP:

- SNMPv2c only
- SNMPv3 only
- Both SNMPv2c and SNMPv3
- Neither SNMPv2c nor SNMPv3

Note You can configure SNMPv1, SNMPv2c, and SNMPv3 using the Cisco Mobility Express CLI too.

Step 1 Choose **Advanced** > **SNMP**.

The **SNMP Setup** window appears.

Step 2 Next to **SNMP Access**, select the appropriate check box to enable the desired SNMP mode.

The default mode is v2c (or by default both or neither SNMP access mode is selected).

The selected SNMP access mode is enabled.

Note For information about configuring SNMPv3 users using Cisco Mobility Express, see the Configuring SNMPv3 users section.

Step 3 In the **Read Only Community** field, enter the desired community name.

The default name is *public*.

Step 4 In the **Read-Write Community** field, enter the desired community name.

The default name is *private*.

Step 5 From the **SNMP Trap** drop-down list, choose **Enabled** or **Disabled** to configure the SNMP Trap Receiver. This tool receives, logs, and displays SNMP traps sent from network devices.

The default setting is **Disabled**.

Step 6 In the **SNMP Server IP** field, specify the IP address of the server you wish to connect to.

Add an SNMPv3 User

Step 1 Choose **Advanced** > **SNMP**.

The **SNMP Setup** window appears.

Step 2 In the **SNMP v3 Users** section, click the **Add New SNMP v3 User** button.

The **Add SNMP v3 User** window appears.

Step 3 In the **User Name** field, enter the desired username for the new SNMPv3 user.

The username must meet the following conditions:

-
-

Step 4 From the **Access Mode** drop-down list, choose the desired mode among **Read Only** and **Read/Write**.

The default is **Read Only**.

Step 5 From the **Authentication Protocol** drop-down list, select one of **HMAC-MD5**, **HMAC-SHA**, or **None**.

The default authentication protocol is **HMAC-SHA**.

Step 6 In the **Authentication Password** and **Confirm Authentication Password** fields, enter the desired authentication password as per the following password policy:

Note You can select the **Show Password** checkbox to display the entries in the **Authentication Password** and the **Confirm Authentication Password** fields and verify that they match.

Step 7 In the **Privacy Protocol** drop-down list, select one of **CBC-DES**, **CFB-AES-128**, or **None**.

The default privacy protocol is **CFB-AES-128**.

Step 8 In the **Privacy Password** and **Confirm Privacy Password** fields, enter the desired privacy password as per the following password policy:

Note You can select the **Show Password** checkbox to display the entries in the **Privacy Password** and the **Confirm Privacy Password** fields and verify that they match.

Step 9 Click **Apply** to create a new SNMPv3 user.

The newly added SNMP v3 User appears in the **SNMP v3 Users** table on the **SNMP Setup** window.

Note You can add up to a maximum of 7 SNMPv3 users.

Edit SNMPv3 User

Step 1 Choose **Advanced** > **SNMP**.

The **SNMP Setup** window appears.

Step 2 Click the <edit_icon.gif> icon in the row containing the SNMPv3 user whose details you wish to modify.

The desired row in the **SNMPv3 Users** table becomes editable (or the **Edit SNMPv3 User** window appears.)

Step 3 In the **SNMPv3 Users** table, make the desired modifications inline (or in the **Edit SNMPv3 User** window).

Step 4 Click **Apply**.

The **SNMP v3 Users** table is refreshed and the updated entry appears in this table.

Delete SNMPv3 User

Step 1 Choose **Advanced** > **SNMP**.

The **SNMP Setup** window appears.

Step 2 Click the **X** icon in the row containing the SNMPv3 user you wish to delete.

A warning message appears.

Step 3 Click **Yes** in the pop-up window.

The **SNMP v3 Users** table is refreshed and the deleted entry is removed from this table.

Setting Up System Message Logging

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

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

Before you begin

Set up a Syslog server in your network before starting with the following procedure.

Step 1 Choose **Advanced** > **Logging**.

The **Logging Setup** window appears.

Step 2 From the **Syslog Logging** drop-down list, choose **Enabled**. The default is Disabled.

The System Message Logging feature is enabled.

Step 3 In the **Syslog Server IP** field, enter the IPv4 address of the server to which the syslog messages are to be sent.

Step 4 Set the severity level for filtering syslog messages to the syslog server. From the **Logging Level** drop-down list, set the severity level by choosing one of the following (given in the order of severity):

- **Emergencies (Highest severity)**
- **Alerts**
- **Critical**
- **Errors (Default)**
- **Warnings**
- **Notifications**
- **Informational**
- **Debugging (Lowest severity)**

After a syslog level is set, only messages with a severity equal to or more than the set level are sent to the syslog server.

Step 5 To set the facility for outgoing syslog messages to the syslog servers, choose one of the following options from the **Syslog Facility** drop-down list:

- Kernel = Facility level 0
- User Process = Facility level 1
- Mail = Facility level 2
- System Daemons = Facility level 3
- Authorization System = Facility level 4
- Syslog = Facility level 5 (default value)
- Line Printer = Facility level 6
- USENET = Facility level 7
- Unix-to-Unix Copy = Facility level 8
- Cron = Facility level 9
- FTP Daemon = Facility level 11
- System Use 12 = Facility level 12

- System Use 13 = Facility level 13
- System Use 14 = Facility level 14
- System Use 15 = Facility level 15
- Local Use 0 = Facility level 16
- Local Use 1 = Facility level 17
- Local Use 2 = Facility level 18
- Local Use 3 = Facility level 19
- Local Use 4 = Facility level 20
- Local Use 5 = Facility level 21
- Local Use 6 = Facility level 22
- Local Use 7 = Facility level 23
- Authorization System (Private) = Facility level 24

Step 6 Click **Apply**.

Optimizing RF Parameters

To maximize your network's Wi-Fi performance, you can optimize the radio frequency signals' coverage and quality.

Step 1 Choose **Enabled** from the **RF Optimization** drop-down list.

Step 2 Indicate the expected **Client Density** and **Traffic Type** in your network.

To know the values that are set when low, typical, or high client density type is selected, see RF Parameter Optimization Settings, on page 104.

Step 3 Click **Apply**.

Optimized Roaming

Information About Optimized Roaming

Optimized roaming resolves the problem of sticky clients that remain associated to access points that are far away and outbound clients that attempt to connect to a Wi-Fi network without having a stable connection. Optimized roaming allows clients to disassociate based on the RSSI of the client data packets and data rate. The client is disassociated if the RSSI alarm condition is met and the current data rate of the client is lower than the optimized roaming data rate threshold. You can disable the data rate option so that only RSSI is used for disassociating clients.

Optimized roaming also prevents client association when the client's RSSI is low by checking the RSSI of the incoming client against the RSSI threshold. This check prevents the clients from connecting to a Wi-Fi network unless the client has a viable connection. In many scenarios, even though clients can hear beacons and connect to a Wi-Fi network, the signal might not be strong enough to support a stable connection.

You can also configure the client coverage reporting interval for a radio by using optimized roaming.

Optimized Roaming is useful in the following scenarios:

- To address the sticky client challenge by proactively disconnecting clients.
- To actively monitor data RSSI packets.
- To disassociate a client when the RSSI is lower than the set threshold.

Restrictions for Optimized Roaming

- You cannot configure the optimized roaming interval until you disable the 802.11a/b network.
- When BSS transition is sent 802.11v capable clients and if the clients are not transitioned to other BSS before the disconnect timer expires, the client is disconnected forcefully. BSS transition is enabled by default for 802.11v capable clients.

Configuring Optimized Roaming

Before you begin

- Ensure you have switched to **Expert View** to be able to configure optimized roaming via GUI.
- You cannot configure the optimized roaming interval until you disable the 802.11a/b network.

Step 1 Choose **Advanced** > **RF Optimization**.

The **RF Optimization** page is displayed.

Step 2 Enable the **Optimized Roaming** knob.

You are presented with various options to configure for optimized roaming. data rate checks and default RSSI threshold values taken from Coverage Hole Detection and Mitigation (CHDM).

Step 3 In the **2.4 GHz Interval** and **5.0 GHz Interval** text boxes, specify the values for the interval at which an access point reports the client coverage statistics to the primary AP.

The interval ranges from 5 seconds to 90 seconds (default). If you configure a low reporting interval, the network can get overloaded with coverage report messages.

The client coverage statistics includes data packet RSSIs, Coverage Hole Detection and Mitigation (CHDM) pre-alarm failures, retransmission requests, and current data rates.

Note The access point sends client statistics to the primary AP based on the following conditions:

- When the interval is set to 90 seconds by default.
- When the interval is configured (for instance to 10 secs) only during optimized roaming failure due to Coverage Hole Detection (CHD) RED ALARM.

Step 4 Set the threshold data rates of the client by manipulating the **2.4 GHz Data Rates** and **5.0 GHz Data Rates** sliders.

The following data rates are available:

- 2.4 GHz—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54

• 5 GHz—6, 9, 12, 18, 24, 36, 48, 54

Information About RSSI Low Check

The Received Signal Strength Indicator (RSSI) low check feature causes the controller to deny a client's association if the signal from the client is below the configured RSSI threshold. In most deployments, this feature is not required and may lead to client connectivity issues

Restrictions for RSSI Low Check

• This feature is not supported if you have enabled optimized roaming.

Using Controller Tools

Note This feature is available only for administrative user accounts with read and write privileges.

The **Controller Tools** page provides the following operations on the controller:

• Restarting the controller.

See Restarting the Controller, on page 85.

• Clearing controller configuration and resetting the controller to factory-defaults. See Clearing Controller Configuration and Resetting the Controller, on page 85.

• Exporting and importing controller configuration. See Exporting and Importing the Controller Configuration, on page 86.

Restarting the Controller

At any time, you can restart (or reboot) the controller by choosing **Advanced** > **Controller Tools**, and then clicking **Restart Controller**.

Clearing Controller Configuration and Resetting the Controller

This procedure resets your Cisco Mobility Express wireless LAN controller to its factory-default configuration.

Step 1 Choose **Advanced** > **Controller Tools**.

This opens the **Controller Tools** page.

Step 2 Click **Clear Controller Configuration**.

This erases the current Cisco Mobility Express controller configuration , resets the configuration to the factory-default values, and reboots the Cisco Mobility Express wireless LAN controller.

What to do next

After the Cisco Mobility Express Controller reboots, proceed to Starting the Initial Configuration Wizard, on page 7.

Exporting and Importing the Controller Configuration

Exporting Controller Configuration

At any time, you can export the current controller configuration to a .TXT file format.

To export the current configuration, choose **Advanced > Controller Tools**, and then under **Configuration File**, click **Export Configuration**.

The configuration file is saved, though HTTPS, onto the device on which the Mobility Express UI is being viewed. By default the file is saved as *configuration.txt* in your downloads folder.

Importing Controller Configuration

You can import configuration from a previously saved configuration file, which is in .TXT file format. For this, choose **Advanced > Controller Tools**, and then under **Configuration File**, click **Import Configuration**, and then browse to and choose the required file.

The import causes all controller-capable APs in the network to reboot. When the APs come back online, the primary AP Election process happens and a primary AP comes online with the new imported controller configuration.

For more information about the primary AP Election Process, see Cisco Mobility Express Controller Failover and Primary AP Election Process, on page 100.

Saving Controller Configuration

Access points have two kinds of memory, the active, but volatile, RAM, and the nonvolatile RAM (NVRAM). During normal operation, the current configuration of the Cisco Mobility Express controller resides on the RAM of the primary AP. During a reboot, the volatile RAM is completely erased, but the data on the NVRAM is retained.

At any time, you can save the Cisco Mobility Express controller's configuration from the RAM to the NVRAM of the primary AP. This ensures that in the event of a reboot, the controller can restart with the last saved configuration.

To save the controller's current configuration from the RAM to the NVRAM, click **Save Configuration** at the top-right corner of the Cisco Mobility Express web interface, and then click **Ok**.

Upon successful saving of the configuration, a message conveying the same is displayed.

Using CMX Cloud Presence Analytics

Cisco Connected Mobile Experiences Cloud (Cisco CMX Cloud) is a Software-as-a-Service (SaaS) product that provides in-venue analytics. You can configure the Cisco CMX Cloud solution using the Cisco Mobility Express web interface.

The Cisco CMX Cloud solution integrated with Cisco Mobility Express provides the following capabilities:

- Enables configuration of secure guest-access solutions for visitors through a custom portal.

  Note CMX Connect configuration is done at the WLAN level for guest access.

- Facilitates detection of all Wi-Fi devices.
- Provides analytics on the Wi-Fi device's presence, such as dwell times, new vs. repeat visitors, and peak times.
- Engages visitors directly on the guest portal page or mobile app with location-based content.

Prerequisites for CMX Presence Analytics

- You should have a valid CMX server URL and the corresponding CMX server token. To register for a CMX Cloud account, go to www.cmxcisco.com. For more information, see http://support.cmxcisco.com/hc/en-us.

  Note In the server URL field, ensure that the URL is appended with /visitor/login.

- A WLAN is created for CMX Cloud. For more information, see the **Adding a WLAN** section in the **Specifying Wireless Settings** chapter.

Enabling CMX Presence Analytics

Before you begin

You will need a valid CMX server URL and a corresponding token.

Step 1 Choose **Advanced** > **CMX**.

The **CMX** window appears.

Step 2 In the **CMX Status** drop-down box, select **Enabled**.

Step 3 In the **CMX Server URL** field, enter a valid CMX server URL.

Step 4 In the **CMX Server Token** field, enter a valid CMX server token.

Step 5 Click **Apply**.

DNS Access Control Lists

The DNS Access Control Lists (ACLs) feature is now supported on Cisco Mobility Express, which allows domain based filtering for Flex Mode. Now, you can selectively allow URLs of your choice without authorizations. With this feature, more than one IPs can be learnt for the FQDN configured in the URL rule, for both pre-auth and post-auth.

This feature supports:

- IPv4 and IPv6
- Wildcard match - Out of the 32 URL rules, a maximum of 20 characters can be wildcard matches.
- Allow/Deny Rules for any post-auth use.
- Configuration of ACL using the FQDN.
- 32 URL rules that can be configured per ACL name.

Note With this enhancement, the features that are listed above are applicable to post-auth also.

The controller is configured with the ACL name as per the WLAN, or an AP group, or an AP, or that what is returned by the AAA server. The data path of the AP, monitors the DNS requests or responses and learns the IP address of the configured DNS names; and allows traffic for these IP addresses learnt.

If the ACL action is **Allow** DNS response, the IP address will be added to the snooped list. For post-auth ACL, if the URL action is **Deny**, AP modifies the DNS response and sends the 0.0.0.0 IP address to the client.

The two types of DNS ACL supported on Wave 2 APs are:

- Pre-Auth or Web-Auth DNS ACL: These ACLs have URLs set to **Allow** before the client authentication phase. If the client has the URL rule set to **Allow**, then the client data is switched locally. If the URLs do not match any rule, then all the packets are forwarded to the controller. By default, if the client data does not match any of the configured rules on the AP, the AP sends such traffic to the controller for L3 authorization.
- Post-Auth DNS ACL: These ACLs are applied when the client is running. Post-Auth ACL name can be configured on the WLAN and it can be overridden by the ACL name configured on the AAA server for a given client. If the ACL rule action is set to **Deny** for any URL, these URLs do not get any IP addresses in the DNS response. The APs over-write the DNS response with 0.0.0.0 and sends it to the client.

Configuring DNS Access Control Lists (ACL)

The steps to configure DNS ACLs for pre-auth have been modified. Follow the procedure given below to configure DNS ACLs:

Step 1 Choose **Advanced** > **Security Settings**.

The **Security Settings** page is displayed.

Step 2 Click **Add new ACL**.
The Add ACL Rule window is displayed.

Step 3 Follow the procedure given below to add new ACL rules:

a) Choose the **ACL Type**, either **IPv4** or **IPv6**.
b) Enter the **ACL Name**.
c) Use the **Policy ACL** toggle button, to enable or disable policy ACL.
d) Click the **Add IP Rule** button.
The **Add/Edit IP ACLs** window is displayed.
e) In the Add/Edit IP ACLs window, enter details such as **Action**, **Protocol**, **Source IP/Mask**, **Source Port**, **Dest. IP Address/Mask**, **Dest. Port**, **DSCP**, and click **Apply**.
f) Click the **Add URL Rules** button.
The **Add/Edit URL ACLs** window is displayed.
g) In the Add/Edit URL ACLs window, enter the **URL** and **Action**.

Note You cannot add the same URL in IPv4 and IPv6.

h) Click **Apply**.

On the Security Settings page, the ACL Type, ACL Name, and Policy Name are listed. You can also view if the policy names are mapped or not.

Applying the ACL to WLAN at Pre-Auth Level

Step 1 Choose **Wireless Settings** > **WLANs**.
The **WLAN Configuration** window is displayed.

Step 2 Click the **Edit** icon adjacent to the WLAN you want to enable or disable.
The **Edit WLAN** window is displayed.

Step 3 Under the **WLAN Security** tab, enable **Guest Network**.

Step 4 From the **Rule Name(IPv4)** and **Rule Name (IPv6)** drop-down lists choose a value.

Step 5 Click **Apply**.

Applying the ACL to WLAN at Post-Auth Level

Step 1 Choose **Wireless Settings** > **WLANs**.
The **WLAN Configuration** window is displayed.

Step 2 Click the **Edit** icon adjacent to the WLAN you want to enable or disable.
The **Edit WLAN** window is displayed.

Step 3 Under the **VLAN & Firewall** tab, in the **Enable Firewall** field, choose **Yes** to enable the firewall.

Step 4 In the **WLAN Post-auth ACL** section, select either **ACL Name(IPv4)** or **ACL Name(IPv6)**, or both.

Step 5 Click **Apply**.

Configuring AAA Override in WLAN

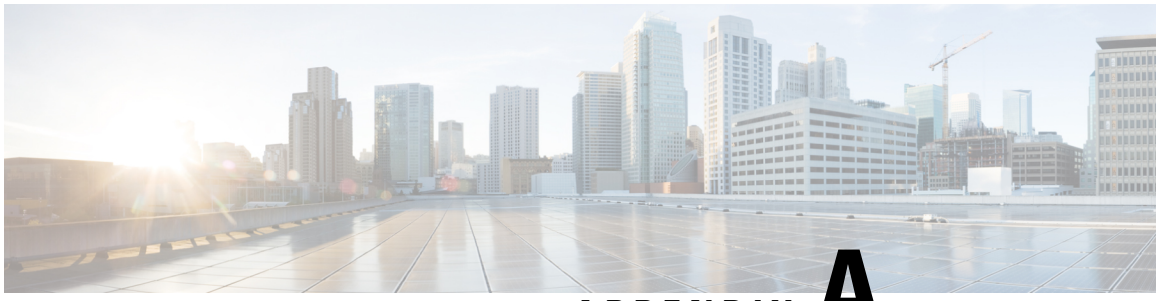
Step 1 Switch to the **Expert View**, if you are currently in the Standard View.

Step 2 Choose **Wireless Settings** > **WLANs**.
The **WLAN Configuration** window is displayed.

Step 3 Click the **Edit** icon adjacent to the WLAN you want to enable or disable.
The **Edit WLAN** window is displayed.

Step 4 Choose the **Advanced** tab and enable the **Allow the AAA Override** toggle button.

Step 5 Click **Apply**.



APPENDIX A

Controller CLI Commands

Cisco Mobility Express CLI

For features supported in a specific Cisco Mobility Express software release, the Cisco Mobility Express controller software supports most commands that are supported by the Cisco WLC in the same Cisco Unified Wireless Network Software Release version. However, there are several commands and procedures which are specific to, or behave differently on, the Cisco Mobility Express controller. These procedures are given in the following sections.

For a complete listing of the commands supported on the Cisco Mobility Express controller CLI, refer to the Cisco Mobility Express Command Reference for the specific release listed at https://www.cisco.com/c/en/us/support/wireless/mobility-express/products-command-reference-list.html. Cisco Mobility Express only supports the AireOS commands mentioned in this document.

For information on the commands available on the WLC CLI, refer to the Cisco Wireless Controller Command Reference guides for Cisco Unified Wireless Network Software Releases listed at http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-command-reference-list.html

Using the CLI Initial Configuration Wizard

Before you begin

- Connect to the console port of the access point to perform the following procedure.
- The available options appear in brackets after each configuration parameter. The default value appears in all uppercase letters.
- If you enter an incorrect response, the controller provides you with an appropriate error message, such as “Invalid Response,” and returns you to the wizard prompt.
- Press the **hyphen** key if you ever need to return to the previous command line.

Step 1 When prompted to terminate the autoinstall process (the CLI Initial Configuration Wizard), wait for 30 seconds. The CLI Initial Configuration Wizard begins after 30 seconds.

To terminate and exit the process, enter **yes**.

The wizard downloads a configuration file from a TFTP server and then loads the configuration onto the controller automatically.

Step 2 Enter the **Administrative Username** and **Administrative password** to be assigned to this controller. You can enter up to 24 ASCII characters for each.

The following is the password policy:

- 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 must be repeated more than three times consecutively.
- The new password must not be the same as the associated username and not be the username reversed.
- The password must not be cisco, ocsic, or any variant 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 3 Enter the **System Name**, which is the name that you want to assign to the controller. You can enter up to 31 ASCII characters.

Step 4 Enter the code for the country in which the Mobility Express network is located.

Note Enter **help** to view the list of available country codes.

Step 5 If you want the controller to receive its time setting from an external Network Time Protocol (NTP) server when it powers up, enter **YES** to configure an NTP server. Otherwise, enter **no**.

If you entered **YES**, then enter the NTP server's IP address.

If you entered **no**, then enter the following to manually set the time and date:

- Enter the date in MM/DD/YY format.
- Enter the time in HH:MM:SS format.

Step 6 Enter the timezone location index to set the timezone. Enter **help** for a list of timezones listed by their indexes.

Step 7 Enter the IP address of the management interface.

Note The management interface is the default interface for in-band management of the controller and connectivity to enterprise services.

Step 8 Enter the IP address and subnet mask of the management interface.

Step 9 Enter the IP address of the default gateway router.

Step 10 To enable and configure a management DHCP scope, enter **yes**. Otherwise enter **NO**.

If you have entered **YES**, you will need to enter the following:

a. DHCP Network IP address.

b. DHCP Netmask.

c. Router IP address.

d. Start DHCP IP address and Stop DHCP IP address, for the IP address range.

e. Domain Name.

f. Specify whether you want OpenDNS or user DNS.

Step 11 To enable the Employee Network, enter **YES**. Otherwise enter **no**.

If you have entered **YES**, then enter the following:

a. Employee Network Name (SSID)

b. Employee VLAN Identifier (0 = untagged)

c. Employee Network Security. You can enter **PSK** or **enterprise**.

d. If you have entered Employee Network Security as **enterprise**, specify the following:

- RADIUS Server's Address.
- RADIUS Server's Port.
- RADIUS Server's Secret (password).

e. If you have entered Employee Network Security as **PSK**, specify the following:

- Enter PSK Pass phrase (8 to 38 characters).
- Re-Enter PSK Pass phrase (8 to 38 characters).

Step 12 To enable and configure an employee DHCP scope, enter **yes**. Otherwise enter **NO**.

If you have entered **YES**, you will need to enter the following:

a. DHCP Network IP address.

b. DHCP Netmask.

c. Router IP address.

d. Start DHCP IP address and Stop DHCP IP address, for the IP address range.

e. Domain Name.

f. Specify whether you want OpenDNS or user DNS.

Step 13 To enable the Guest Network, enter **YES**. Otherwise enter **no**.

If you have entered **YES**, then enter the following:

a. Guest Network Name (SSID).

b. Guest VLAN Identifier (0 = untagged).

c. Guest Network Security. You can enter **WEB_CONSENT** or **psk**.

d. If you have entered Guest Network Security as **PSK**, specify the following:

- Enter Guest Pass phrase (8 to 38 characters).
- Re-Enter Guest Pass phrase (8 to 38 characters).

Step 14 To enable RF Parameter Optimization, enter **YES**. Otherwise, enter **no**.

If you have entered **YES**, then enter the following:

a. Client Density. You can enter **TYPICAL**, **Low**, or **High**, as per your requirement.

b. Traffic with Voice. You can enter **NO** or **yes**, as per your requirement.

Step 15 When prompted to verify that the configuration is correct, enter **yes** or **NO**.

The controller saves your configuration when you enter **yes**, reboots, and prompts you to log on.

CLI Procedures

Changing the SNMPv3 User Default Values

The controller uses a default value of "default" for the username, authentication password, and privacy password for SNMPv3 users. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values.

Before you begin

SNMPv3 is time sensitive. Ensure that you configure the correct time and time zone on your controller.

Step 1 See the current list of SNMPv3 users for this controller by entering this command:

show snmpv3user

Step 2 If "default" appears in the SNMPv3 User Name column, enter this command to delete this user:

config snmp v3user delete *username*

The *username* parameter is the SNMPv3 username (in this case, "default").

Step 3 Create a new SNMPv3 user by entering this command:

config snmp v3user create *username* {**ro** | **rw**} {**none** | **hmacmd5** | **hmacsha**} {**none** | **des** | **aescfb128**} *auth_key encrypt_key*

where

- *username* is the SNMPv3 username.

- **ro** is read-only mode and **rw** is read-write mode.
- **none**, **hmacmd5**, and **hmacsha** are the authentication protocol options.
- **none**, **des**, and **aescfb128** are the privacy protocol options.
- *auth_key is the authentication shared secret key.*
- *encrypt_key is the encryption shared secret key.*

  Do not enter "default" for the *username*, *auth_key*, and *encrypt_key* parameters.

Step 4 Enter the **save config** command.

Step 5 Reboot the controller so that the SNMPv3 user that you added takes effect by entering **reset system** command.

Configuring 802.11r Fast Transition

Step 1 To enable or disable 802.11r fast transition parameters, use the **config wlan security ft** {**enable** | **disable**} *wlan-id* command.

By default, the fast transition is disabled.

Step 2 To enable or disable 802.11r fast transition parameters over a distributed system, use the **config wlan security ft over-the-ds** {**enable** | **disable**} *wlan-id* command.

By default, the fast transition over a distributed system is disabled.

Step 3 To enable or disable the authentication key management for fast transition using preshared keys (PSK), use the **config wlan security wpa akm ft-psk** {**enable** | **disable**} *wlan-id* command.

By default, the authentication key management using PSK is disabled.

Step 4 To enable or disable the authentication key management for fast transition using 802.1X, use the **config wlan security wpa akm ft-802.1X** {**enable** | **disable**} *wlan-id* command.

By default, the authentication key management using 802.1X is disabled.

Step 5 To enable or disable 802.11r fast transition reassociation timeout, use the **config wlan security ft reassociation-timeout** *timeout-in-seconds wlan-id* command.

The valid range is 1 to 100 seconds. The default value of reassociation timeout is 20 seconds.

Step 6 To enable or disable the authentication key management for fast transition over a distributed system, use the **config wlan security wpa akm ft over-the-ds** {**enable** | **disable**} *wlan-id* command.

By default, the authentication key management for fast transition over a distributed system is enabled.

Step 7 To view the fast transition configuration on a client, use the **show client detailed** *client-mac* command.

Step 8 To view the fast transition configuration on a WLAN, use the **show wlan** *wlan-id* command.

Step 9 To enable or disable debugging of fast transition events, use the **debug ft events** {**enable** | **disable**} command.

Step 10 To enable or disable debugging of key generation for fast transition, use the **debug ft keys** {**enable** | **disable**} command.

Configuring CDP Timer

Note You cannot set the CDP hold time by configuring it from the controller console on the primary AP. The controller's hold time configuration is ignored since both the controller and internal AP on the Cisco Mobility Express primary AP share the same interface on the switch.

Configuring Cisco Umbrella on Cisco Mobility Express (CLI)

This section describes the procedure to configure Cisco Umbrella on Cisco Mobility Express:

Before you begin

- You should have an account with Cisco Umbrella.
- You should have an API token from Cisco Umbrella.

Step 1 To enable or disable Cisco Umbrella, use the **config opendns** {**enable** | **disable**}

Example:

```
(Cisco Controller) > config opendns enable
```

Enables or disables the Cisco Umbrella global configuration.

Step 2 **config opendns api-token** *api-token*

Example:

```
(Cisco Controller) > config opendns api-token D0986C18DC334FB2E3AA46148D600A4001E5997
```

Registers the Cisco Umbrella API token on the network.

Step 3 **config opendns profile** {**create** | **delete** | **refresh**} *profilename*

Example:

```
(Cisco Controller) > config opendns profile create profile1
```

Creates, deletes, or refreshes a Cisco Umbrella profile that can be applied over a WLAN.

Step 4 **config wlan opendns-profile** *wlan-id profile-name* {**enable** | **disable**}

Example:

```
(Cisco Controller) > config wlan opendns-profile 1 profile-name enable
```

Maps the Cisco Umbrella profile identity to a WLAN.

Step 5 **config wlan opendns-dhcp-opt6** *wlan-id* {**enable** | **disable**}

Example:

```
(Cisco Controller) >config wlan opendns-dhcp-opt6 1 enable
```

Enables or disables DHCP option 6 per WLAN.

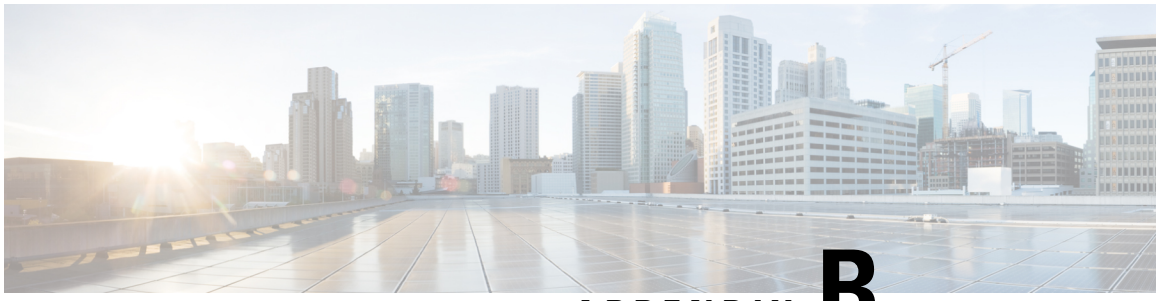
Step 6 **config wlan opendns-mode** *wlan-id* {**ignore** | **forced**}

Example:

```
(Cisco Controller) >config wlan opendns-mode 1 forced
```

Ignores or Forces the Cisco Umbrella mode on the WLAN.

Controller CLI Commands



APPENDIX B

Concepts, FAQs, and Information for Advanced Users

Supported Browsers

Operating System	Supported Browsers and Versions
Microsoft Windows	• Internet Explorer 10 and later • Mozilla Firefox 33 and later • Google Chrome 38 and later
Apple Mac OS	• Safari 7 and later • Mozilla Firefox 33 and later • Google Chrome 38 and later

Cisco Mobility Express Controller Failover and Primary AP Election Process

Mobility Express Controller Redundancy for Failover

In a Cisco Mobility Express network, not all APs have the capability to work as a primary AP. See Supported Cisco Access Points, on page 2 to know which AP models are capable of working as a primary AP.

In order to have Cisco Mobility Express controller redundancy to enable a failover, your network must have two or more active APs with primary AP capability. In the event of a failover, one of these other APs will automatically be elected as a primary. The newly elected primary will have the same IP and configuration as the original primary. From an administrator perspective, there will be no difference between the original primary and the newly elected primary in case of a failover.

Note Clients that connect to the primary AP will lose connectivity during a failover.

Mobility Express Controller Forced Failover

In a Cisco Mobility Express network, not all APs have the capability to work as a primary AP. See Supported Cisco Access Points, on page 2 to know which AP models are capable of working as a primary AP.

You can manually force any AP, that has the capability to work as a primary AP, to become the primary AP. This forced failover of the primary AP to another primary-capable AP of your choice can be performed both using the GUI and the CLI.

To perform a forced failover using the GUI:

1. Choose **Wireless Settings** > **Access Points**.

   The **Access Points Administration** window is displayed.

2. Click the **Edit** icon adjacent to the AP you want to set as primary.

   The **Edit** window with the **General** tab is displayed.

3. Under the **General** tab, next to the **Operating Mode field**, click **Make me Controller**.

Note For a primary AP, the **Operating Mode** field shows *AP & Controller*. For other associated APs, this field shows *AP Only*. The **Make Me Controller** button is available only for subordinate APs that are capable of participating in the primary election process.

To perform a forced failover using CLI, use the following command:

```
config ap next-preferred-master cisco-ap-name forced-failover
```

When you force the failover of the primary to an AP of your choice, using the GUI or CLI methods, the current primary AP reboots while the new AP takesover as the controller, with the IP address and configuration as the previous primary. The previous primary, after rebooting, comes back online and joins the new primary AP as a subordinate AP.

Note Like any failover, this forced failover causes some downtime in the Cisco Mobility Express network. During this downtime, clients associated to APs that have the standalone feature enabled will not face any disruption in service. Clients of APs that do not have the standalone functionality enabled will be affected.

Primary AP Election Process

In a Cisco Mobility Express network, when the primary AP shuts down, one of the other primary-capable APs in this deployment is automatically designated as the primary AP. The automatic selection of the primary AP among the Cisco Mobility Express-capable APs is as per an internal automatic primary election process. This process is used to both detect the failure of the primary AP and to designate the new primary AP among the eligible APs. This process is based on Virtual Router Redundancy Protocol (VRRP) that algorithmically determines the next primary AP, based on the following parameters listed in the order of descending precedence:

- The AP with highest controller up-time compared to other Cisco Mobility Express-capable APs
- The AP configured as VRRP primary, using the VRRP command **config ap next-preferred-master** on the controller's CLI.
- The AP with the least load in terms of the number of associated clients associated.
- Among APs with a similar client load, the AP with the lowest MAC address.

Configuring VRID

Virtual router identifier (VRID) is used to identify the virtual router. Prior to Cisco Wireless Release 8.8, the VRID of Cisco Mobility Express was fixed as **01** which resulted in a fixed VRRP MAC based on 00:00:5e:00:01:*VRID*. This caused VRRP MAC conflict issues on Cisco Mobility Express networks if they used the same VRID. Beginning Cisco Wireless Release 8.8, when a VRRP MAC conflict is detected, you can change the VRID on the primary AP. This new VRRP MAC is then sent to the subordinate AP via a VRRP message. The following commands are available to configure the VRID or display the VRID or VRRP MAC.

Step 1 Configure or change the VRID by using the **config mob-exp vrid** *new_vrid* command.

The range for **new_vrid** is 1 to 255 where the default is 1.

Step 2 To display the VRID, use the **show mob-exp vrrp vrid** command.

Step 3 To display the VRRP MAC, use the **show mob-exp vrrp mac** command.

What to do next

Predownloading an Image to an Access Point

To minimize network outages, an upgrade software image is downloaded to the access point from the controller without resetting the access point or losing network connectivity. This means that, first the upgrade image to

the controller is downloaded and then the image is downloaded to the access point while the network is still up. When the controller reboots, the access points are disassociated and reboot. The controller comes up first, followed by the access points, all with their upgraded images. Once the controller responds to the discovery request sent by an access point with its discovery response packet, the access point sends a join request.

Alternative Method for CAPWAP to Mobility Express Conversion

Note

- The recommended method is Converting from CAPWAP Lightweight AP to Cisco Mobility Express Software, on page 11. The following is an alternative only in case the recommended method does not work.
- The following procedure shows a conversion from the 8.1.122.0 Lightweight AP release on an 1850 series AP, and hence uses the corresponding software file. Ensure that you use the appropriate software file depending on the release you are converting from and the AP model.

Step 1 Download the *AIR-AP1850-K9-ME-8-1-122-0.zip* software file from Cisco.com to the TFTP server.

On the Download Software page, for a given release, this .ZIP file is labeled, *"Access point image bundle, to be used for software update and/or supported access points images"*.

Step 2 Unzip the contents of the ZIP file to a directory on the TFTP server.

Step 3 Connect to the console port of the AP.

Step 4 Log in to the AP using the username `Cisco` and password `Cisco`. Both are case-sensitive.

This is the default factory-shipped username and password on all Cisco Aironet APs.

Step 5 Use the command **ap-type mobility-express tftp://***<tftp server ip-address>/<filename of ap1g4 TAR file with path from root on the TFTP server>* command.

The AP reboots, comes back online, and tries to join a controller for about 5 minutes. After this, the AP continues to boot into Mobility Express mode and starts broadcasting the *CiscoAirProvison* SSID.

CAPWAP Image Conversion

The CAPWAP Image Conversion feature is enhanced to allow the AP to download the image from Mobility Express (ME), and flash the ME image on the AP, to make it ME capable even though build version is the same.

Note

- If the image type of the AP is CAPWAP, which is the same as that of the primary AP, then the new ME image is downloaded.
- If the image type of the AP is a different CAPWAP image, regardless of the image type mismatch, the new ME image is downloaded.
- The SFTP support mode of software download is newly added to convert CAPWAP COS AP to Mobility Express AP.
- The new ME image is downloaded from the Image primary. If there is no Image primary, then the new image is downloaded to the AP via the TFTP or SFTP server.

Converting an AP from Mobility Express to CAPWAP Type

To convert a Mobility Express AP into a CAPWAP AP, you must change its ap-type from mobility-express to capwap, though the CLI, as given in this procedure:

1. Connect to the Console Port, Telnet or SSH to the AP.
2. Login to the Mobility Express controller console.
3. In the Mobility Express controller console, use the command **apciscoshell** to connect to the AP console.
4. Login to the AP console using the username *Cisco* and password *Cisco*. Both are case-sensitive.
5. Enter **enable**.
6. Enter the command **ap-type capwap**, and confirm .

   Once the AP type is CAPWAP, the AP will not start its Mobility Express controller functionality and does not participate in the Mobility Express primary AP election process. This AP can then be deployed in a physical wireless controller-based network (i.e. in a non-Mobility Express network). There the AP will join that controller, and as the image on the controller will be different, the AP will request a CAPWAP image from the controller, reboot, and rejoin the controller as a CAPWAP AP.

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

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

The arguments <switch_name> and <switch_ip_address> are the name and IP address, respectively, of the WLC to which the APs need to be migrated to.

The above command converts all APs to *AP Configuration: NOT MOBILITY EXPRESS CAPABLE*. The APs are then reloaded, and they come back up in local mode.

Mobility Express AP Conversion to CAPWAP via DHCP Option

This feature allows the ME APs to convert to CAPWAP mode from ME mode using DHCP option 43. To achieve this, you must first configure specific values in the DHCP server for DHCP option 43. Once the AP receives the DHCP values for this option, the AP type is changed from ME to CAPWAP.

DHCP Option 43

DHCP option 43 is an option used for providing Wireless LAN Controller IP addresses to the AP. The DHCP option 43 is used to notify the AP to convert into CAPWAP AP.

```
ip dhcp pool vlan177
network <wlc IP>
option 43 hex f205.0907.b10a.01
```

When an AP reloads and gets the IP details from the DHCP server, it receives the option 43 value that consists of a hex value of F205 along with ME-WLC IP, which then converts the AP to CAPWAP mode so that the AP can join AireOS WLC.

RF Parameter Optimization Settings

When making the RF Parameter Optimization settings, use the information in the following table to select the right settings for your deployment. The following table shows the default values when low, typical, or high client density type is selected.

Note If you do not enable RF Parameter Optimization during the initial configuration wizard, then client density is set to **Typical** (the default value), and RF traffic type is set to **Data** (the default value).

	Dependency	**Typical** (For enterprise deployments. Default profile.)	**High Density** (Where throughput is most important)	**Low Density** (For coverage in open spaces)
TX Power	Global per band	Default	Higher	Highest
TPC Threshold, TPC Min, and TPC max (These parameters are equivalent to TX Power)	Specific RF profile per band	TPC Min: Default at -10 dB TPC Max: Default at 30 dB	TPC Threshold: • -65 dB for 5 GHz • -70 dB for 2.4 GHz TPC Min: +7 dB TPC Max: Default at 30 dB	TPC Threshold: • -60 dB for 5 GHz • -65 dB for 2.4 GHz TPC Min: -10 dB TPC Max: Default at 30 dB
RX Sensitivity	Global per band (Advanced RX-SOP) RF profiles	Default (Automatic)	Medium (RX-SOP)	Low

	Dependency	Typical (For enterprise deployments. Default profile.)	High Density (Where throughput is most important)	Low Density (For coverage in open spaces)
CCA Threshold	Global per band 802.11 a only (hidden) RF Profiles	Default (0)	Default (0)	Default (0)
Coverage RSSI Threshold	Global per band Data and voice RSSI RF Profiles	Default (Data: -80 Voice: -80)	Default (Data: -80 Voice: -80)	Higher (Data: -90 Voice:-90)
Coverage Client Count	Global per band (Coverage Exception) RF Profiles (Coverage Hole Detection)	Default (3)	Default (3)	Lower (2) Lower (1 to 3)
Data Rates	Global per band (network) RF Profiles	12 Mbp mandatory 9 Mbp supported 1,2, 5.5, 6, 11 Mbp disabled	12 Mbp mandatory 9 Mbp supported 1,2, 5.5, 6, 11 Mbp disabled	CCK rates enabled 1,2, 5.5, 6, 9, 11, 12 Mbp enabled

RFID Tracking on Access Points

Beginning with Cisco Wireless Release 8.8, Cisco Mobility Express supports tracking of assets that have been appropriately tagged with RFIDs. With Cisco Aironet 4800, 3800, and 2800 Series APs, you can track up to 2000 active RFIDs. With all the other applicable Cisco APs, you can track up to 1000 active RFIDs.

When an active RFID is in range, the primary AP adds the RFID-related information to its own database. RFID tracking can be configured on all APs, primary or subordinate, in the Cisco Mobility Express network. You can configure RFID tracking on any AP in the Cisco Mobility Express network only through the primary AP's CLI.

Configuring RFID Tracking

Step 1 Configure RFID parameters like custom CCX multicast addresses, message rate limit or timeout by using the **config rfid {ccx | rate-limit | timeout}** command.

Step 2 To enable or disable RFID tag data collection, use the **config rfid status {enable | disable}** command.

Step 3 To display the default RFID configuration, use the **show rfid config** command.

Step 4 To display a summary of RFID tags and closest APs, use the **show rfid summary** command.

Step 5 To display RFID tag details, use the **show rfid detail** *mac-id* command.

Step 6 To display RFID statistics, use the **show rfid stats** command.

Related Documents

- Cisco Mobility Express Release Notes
- Cisco Mobility Express Command References
- Cisco Aironet Access Points Ordering Guide
- Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide
- Cisco Aironet AP Hardware Guides
  - Cisco Aironet 1560 Access Point Hardware Guide
  - Cisco Aironet 1815i Access Point Hardware Guide
  - Cisco Aironet 1815w Access Point Hardware Guide
  - Cisco Aironet 1830 Series Access Points Hardware Guide
  - Cisco Aironet 1850 Series Access Points Hardware Guide
  - Cisco Aironet 2800 Series Access Points Hardware Guide
  - Cisco Aironet 3800 Series Access Points Hardware Guide

FAQs

Which access points can host the Cisco Mobility Express wireless LAN controller function and which access points can be managed by it?

See Supported Cisco Access Points, on page 2#unique_145.

What controller-based modes does the Cisco Mobility Express wireless LAN controller function support?

Access points managed by the Cisco Mobility Express solution will operate with Centralized Control Plane and Distributed Data Plane, similar to the AireOS FlexConnect mode.

What are the licensing requirements for Cisco Mobility Express?

The Cisco Mobility Express solution does not require any licenses for access points.

Can I expand the scale of access points and convert to a wireless controller deployment?

Yes, you can simply point the APs to the WLAN controller IP address as the primary controller. This is independent of modes. The WLAN controller will push the right AP image and respective configuration. For detailed information, see Converting an AP from Mobility Express to CAPWAP Type, on page 103.

If my deployment needs to downsize to 25 access points or less, can they convert from existing controller-based deployment to Cisco Mobility Express?

Yes. You can convert your wireless controller-based deployment to Cisco Mobility Express, as long as your deployment has APs capable of hosting the Cisco Mobility Express controller functionality (listed as primary APs in Supported Cisco Access Points, on page 2#unique_145).

If the number of APs connected to the primary AP is less than or equal to 25, the maximum clients for the internal AP is limited to 20. What is the workaround for more efficiency and reducing traffic congestion?

The workaround is to move Cisco Mobility Express to some other AP that has lower loads. Complete the following steps to move Cisco Mobility Express to other APs:

1. Enter the **show ap summary** command. The list of APs are listed.
2. Identify the APs with the least number of clients.
3. Enter the **config ap next-preferred-master <new_ap_name> forced-failover** command. This command will move the Cisco Mobility Express controller to the new AP and the current AP will serve the clients.

Where can I get more information on the Cisco Mobility Express solution?

Go to http://www.cisco.com/go/mobilityexpress.

Concepts, FAQs, and Information for Advanced Users