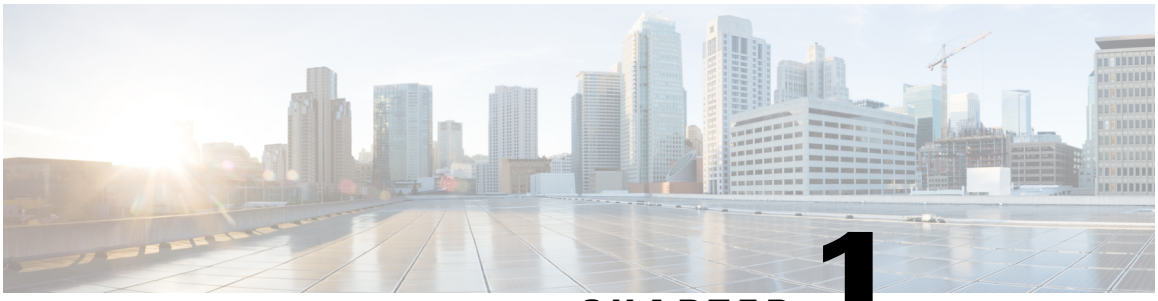
Cisco Mobility Express User Guide for Release 8.2

First Published: 2015-11-30

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

Overview of Cisco Mobility Express

The Cisco Mobility Express wireless network solution provides the virtual WLC functionality that is currently bundled into the Cisco Aironet 1830 and 1850 Series access points (APs). This functionality provides a simplified Wi-Fi architecture with enterprise-level WLAN capability to small and medium deployments.

In the Cisco Mobility Express wireless network solution, one AP, running the Cisco Mobility Express wireless controller, is designated as the master AP. Other APs, referred to as subordinate APs, associate themselves with this master AP.

The master AP operates as a WLC to manage and control the subordinate APs, besides operating as an AP to serve clients. The subordinate APs behave as normal lightweight APs to serve clients.

The Cisco Mobility Express solution provides most of the features of a 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.
- Cisco Mobility Services Engine—For providing presence-level data as well as an advanced spectrum solution.

Supported Cisco Aironet Access Points

In this Cisco Mobility Express Release , the following APs are supported.

APs Supported as Masters (support integrated WLC capability)	APs Supported as Subordinates [1]
• Cisco Aironet 1830 Series • Cisco Aironet 1850 Series	• Cisco Aironet 700i Series • Cisco Aironet 700w Series • Cisco Aironet 1600 Series • Cisco Aironet 1700 Series • Cisco Aironet 2600 Series • Cisco Aironet 2700 Series • Cisco Aironet 3500 Series • Cisco Aironet 3600 Series • Cisco Aironet 3700 Series

[1] **APs supported as master APs can function as subordinate APs also .**

Supported Software Images

AP models that are supported as masters 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 13.

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.

Cisco Mobility Express software for Cisco Wireless Release 8.2 is as follows:

Software Type and Purpose	Release	For AP 1850	For AP 1830
Mobility Express controller-capable AP software to be used for conversion from Lightweight Access Points only.	8.2.100.1	AIR-AP1850-K9-8.2.100.1.tar	AIR-AP1830-K9-8.2.100.1.tar
Access Point image bundle, to be used for updating ME controller software and images of supported access points.	8.2.100.1	AIR-AP1850-K9-ME-8-2-100-1.zip	AIR-AP1830-K9-ME-8-2-100-1.zip

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 master 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 master AP and not by other APs.
- Ensure that the AP is properly installed as per its *Hardware Installation Guide*.
- Ensure that a DHCP server is present and accessible in the network. The Mobility Express controller uses an external 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 master 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 65.

- 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 54.

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 Master 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 Master 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
```

After the switch port configuration is done, proceed to Starting the Initial Configuration Wizard, on page 6.

Starting the Initial Configuration Wizard

Step 1 Boot the AP that has controller capability. This AP should either be a 1850 or a 1830 series AP.
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 Using a supported browser, go to *http://192.168.1.1*, which is redirected to the initial configuration wizard.
The initial configuration wizard's admin account window is displayed in your browser.

What to Do Next

If the initial configuration wizard's admin account window is displayed, then proceed to Using the Initial Configuration Wizard , on page 7, else proceed to Checking if an AP has CAPWAP Lightweight AP Software or Cisco Mobility Express Software, on page 12.

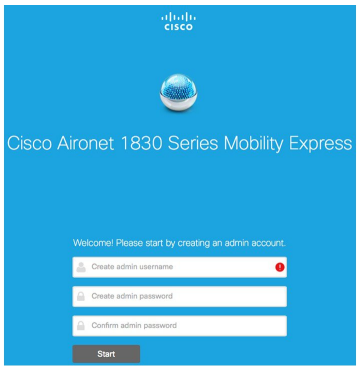
Using the Initial Configuration Wizard

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

Figure 1: Cisco Mobility Express 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.
- Enter a password. You can enter up to 24 ASCII characters.

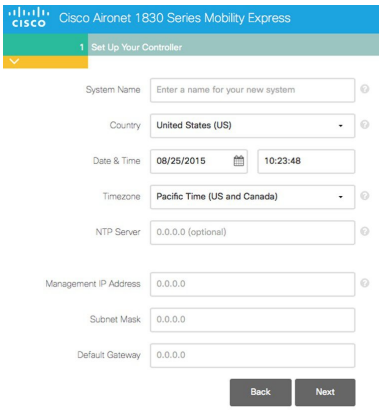
  When specifying a password, ensure the following:

  - 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

Figure 2: Setting 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.

Step 2—Create Your Wireless Networks

You set up the following two networks here:

- **Employee Network—**A Wi-Fi network for employees and regular day-to-day users of the network. This is not meant for guests.
- **Guest Network—**A Wi-Fi network for guest users.

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 4095).
- **VLAN ID—**Specify the VLAN ID for the new VLAN here.

- **DHCP Server Address—**This is optional.

Figure 3: Employee Network with WPA2 Enterprise Security Chosen

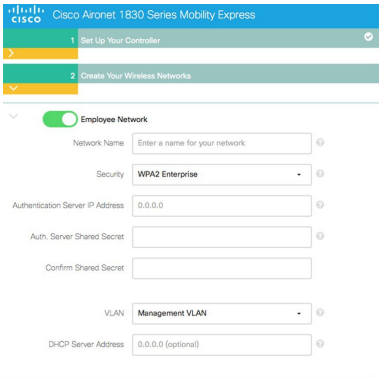
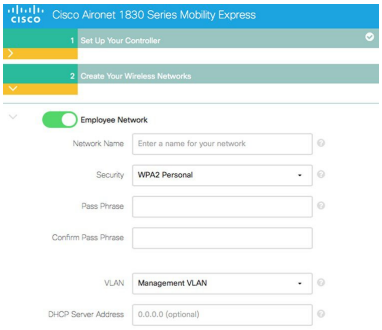


Figure 4: Employee Network with WPA2 Personal Security Chosen



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

- **Network Name—**Specify the SSID for your Guest network.
- **Security—**Choose **Web Consent**, which requires no authentication or **WPA2 Personal**, which uses PSK authentication.
- **Pass Phrase—**If you have chosen WPA2 Personal security, specify the PSK here.
- **VLAN—**Choose **Employee VLAN** to have the same VLAN as that defined for the Employee Network or create a **New VLAN** (with a VLAN ID ranging from 1 to 4095).
- **VLAN ID—**Specify the VLAN ID for the new VLAN.

- **DHCP Server Address—**This is optional.

Figure 5: Guest Network with Web Consent Security Chosen

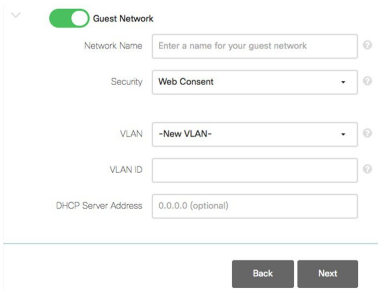
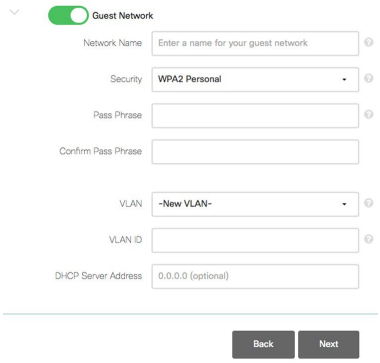


Figure 6: Guest Network with WPA2 Personal Security Chosen

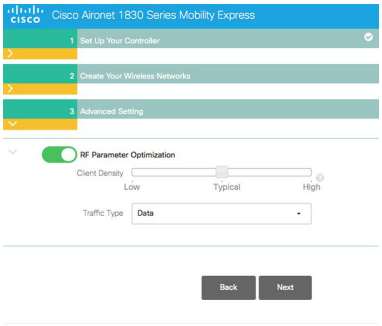


Step 3—Advanced Settings

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 69.

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).

Figure 7: RF Parameter Optimization



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 15.

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. Reboot the AP and proceed to Starting the Initial Configuration Wizard, on page 6.

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 master 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 master AP election process. If and when it is elected as master, 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 13.

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

Tip If you face issues with converting the AP software to a Cisco Mobility Express software, upgrade the AP CAPWAP software to the latest AP software version ap3g3-k9w8-tar.153-3.JD.tar. Now, you can convert the CAPWAP software to the Cisco Mobility Express software *AIR-AP2800-K9-ME-8-3-102-0.tar*.

This issue occurs in Mobility Express-capable APs shipped with default images or a version of the images prior to Cisco Wireless Release 8.3. This is due to insufficient space in the AP's memory or because the AP has been started in U-boot mode where the image is not found in flash.

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.

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

Proceed to Starting the Initial Configuration Wizard, on page 6.

For an alternative to the above conversion process, using the .ZIP file, see Alternative Method for CAPWAP to Mobility Express Conversion, on page 68.

To convert an AP from Mobility Express type to CAPWAP type, see Converting an AP from Mobility Express to CAPWAP Type, on page 68.

Preparing APs to Associate with the Master AP

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

Before You Begin

- A master AP with Cisco Mobility Express wireless controller should be up and running.
- If the AP that has to be prepared to associate with the master 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. .

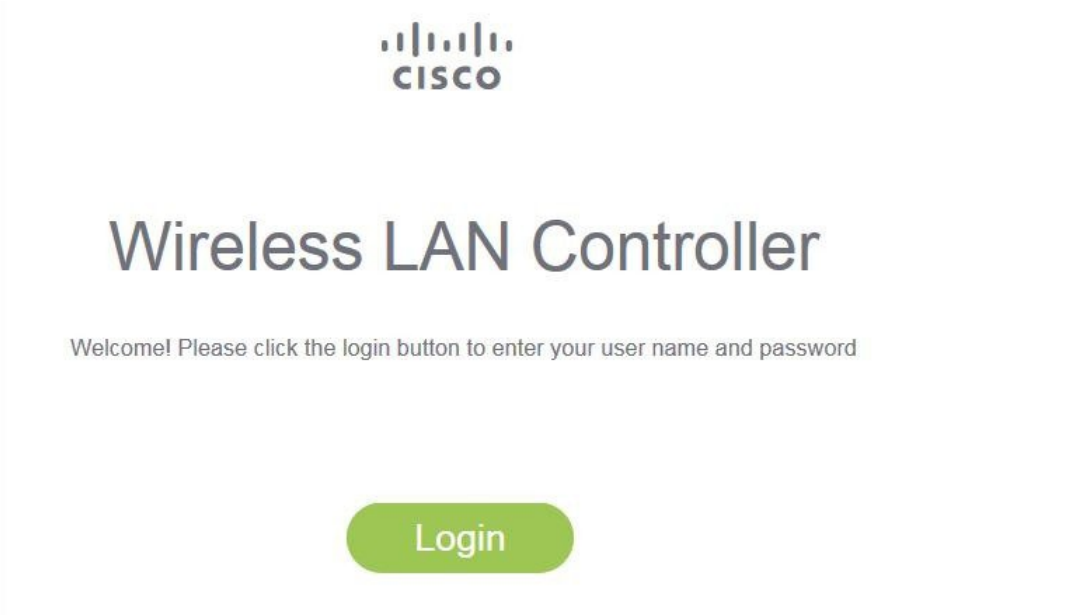
What to Do Next

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 8: Cisco Mobility Express Wireless LAN Controller Web Interface Login



Step 2 Click **Login**.

Step 3 Enter admin user credentials to log in.

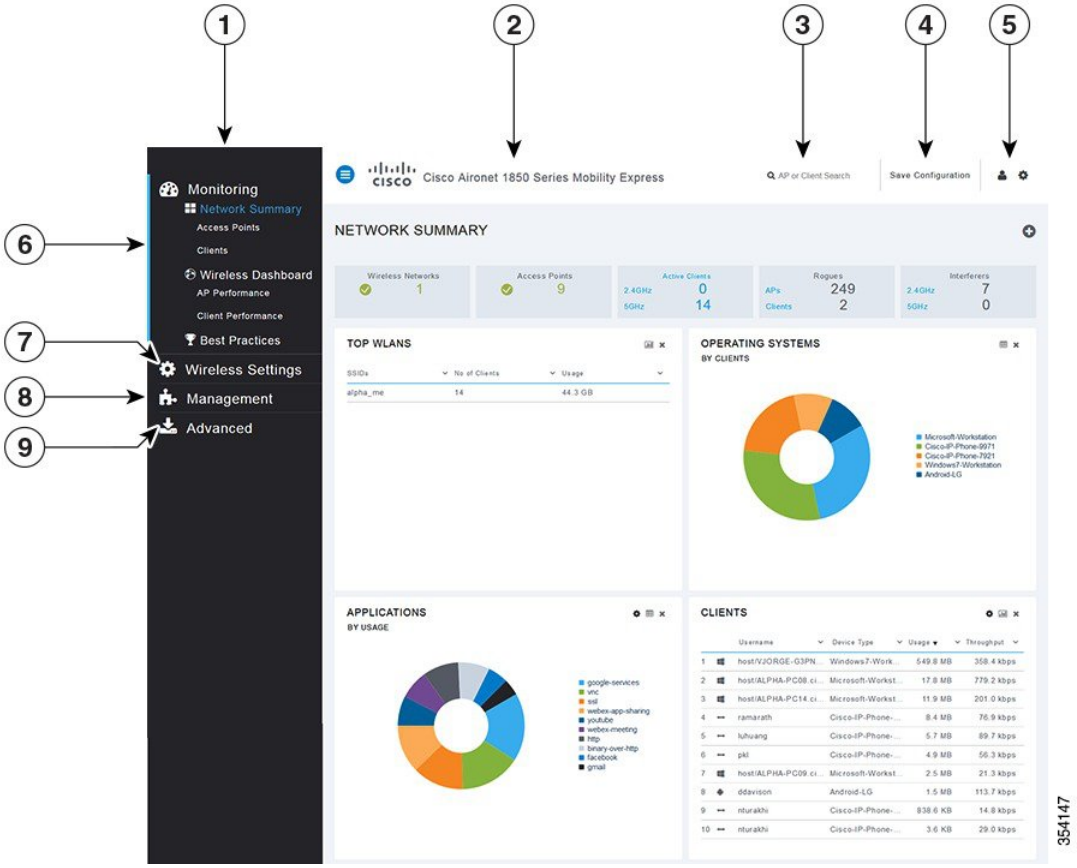
What to Do Next

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 19.

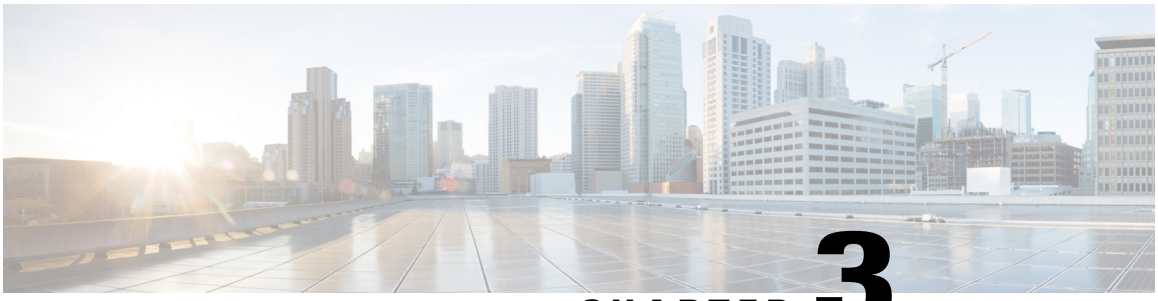
Understanding the Mobility Express Controller Web Interface

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

Figure 9: 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 master 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 52.
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 19.
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. For more information, see Managing the Network, on page 41.
9	The Advanced section, where you can set SNMP settings, sys log settings, and perform a reset to factory default. For more information, see Using Advanced Settings and Operations, on page 49.



CHAPTER 3

Monitoring the Mobility Express Network

About the Cisco Mobility Express Monitoring Service

The Cisco Mobility Express Monitoring service enables the master 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 10: Network Summary Widgets - Tabular view

Figure 11: 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 master 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 master 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**.
You can also add new WLANs from this page. For details, see Adding a WLAN, on page 32.

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 12: 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

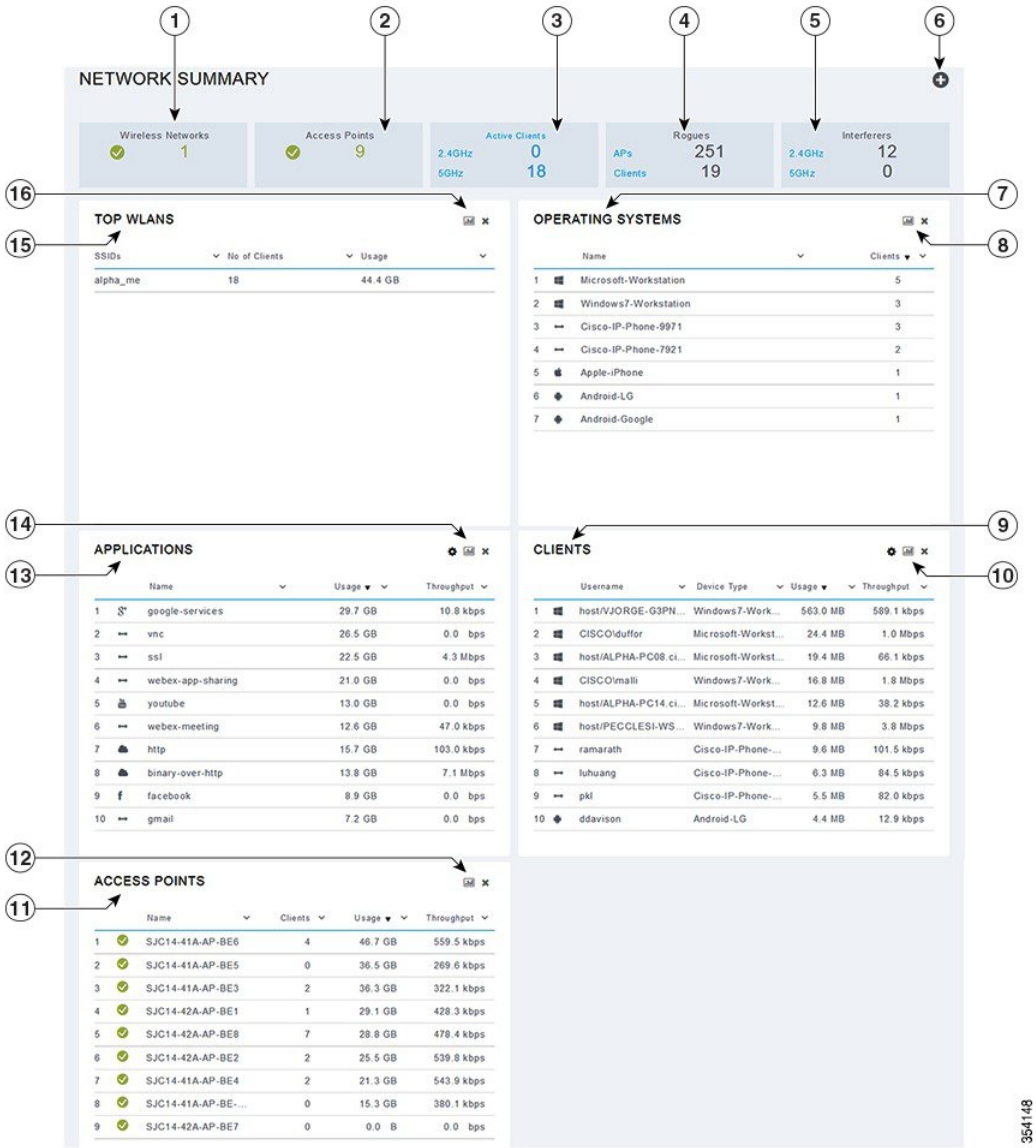
Step 1 Choose **Monitoring** > **Wireless Dashboard** > **AP Performance**.

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 13: 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:

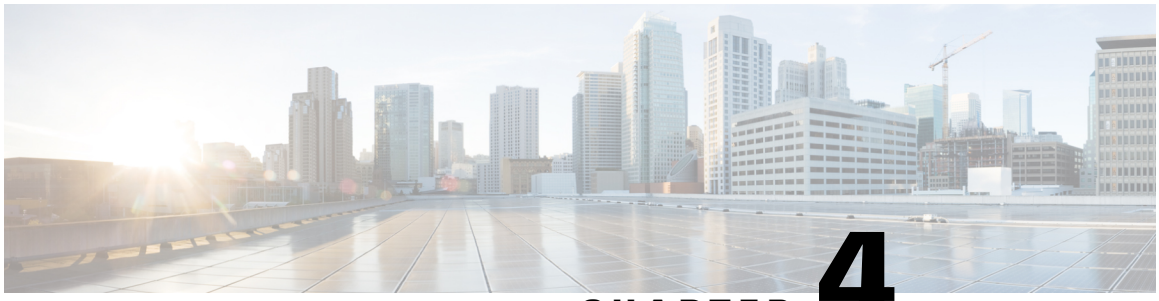
- **Signal Strength**
- **Signal Quality**
- **Connection Rate**
- **Client Connections**

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 > WLAN Users**.

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 master 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 To create a new WLAN, 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—**Enter up to 32 characters for the profile name to be assigned to this WLAN. The profile name must be unique.
- **SSID—**Enter up to 32 characters for the SSID to be assigned to this WLAN.
- **Admin State—**From the drop-down list, choose **Enabled** to enable this WLAN. Otherwise choose **Disabled**. The default is Enabled.
- **Radio Policy—**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 (the 802.11b or 802.11g modes) or on 5GHz (802.11a mode) or both.

  Set the RF profiles for APs that are associated with the controller. Choose one of the following from the **Radio Policy** drop-down list:

  - **All** (default)
  - **802.11a only**
  - **802.11a/g**
  - **802.11g only**
  - **802.11b/g**

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

- **Security—**Choose one of the following security authentication options from this drop-down list:
  - **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 Authentication** drop-down list:

- **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.
- **Display Terms & Conditions—**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.

- **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.
- **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 master 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.

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:

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

2 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.

3 Click Apply.

4 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:

1 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.

2 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.

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

4 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.

5 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

6 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 creating or editing user accounts for this WLAN. See Viewing and Managing WLAN Users, on page 36.

Enabling and Disabling WLANs

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 WLANs

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**.

  For information on adding WLANs, see Adding a WLAN, on page 32.
- 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 Master AP) or a subordinate AP.

Figure 14: Primary Controller (or Master AP) icon

Figure 15: 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.

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:

- **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:

- Operating Mode**—**For a master AP, this field shows *AP & Controller*. For other associated APs, this field shows **AP Only**.
- 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 master AP) Under the **Controller** tab, you can manually edit the following controller parameters for the integrated Mobility Express wireless LAN controller:

- **System Name—**Edit the name that you have assigned to this controller. You can enter up to 31 ASCII characters. The system name is first specified during the initial configuration wizard.
- **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—**You can set the country code for the controller and all associated APs using this drop-down list. Once you apply your changes, the country codes on all subordinate APs are automatically changed, the APs reboot and come back online with the new country code, and rejoin the controller. However the change will not be applied on the controller and the master AP until the master AP is manually rebooted.

Step 5 Under the **802.11 b/g/n** tab, you can set the following parameters:

- **Admin Mode—**Enabled or Disabled. This enables or disables the corresponding radio on the AP (2.4 GHz for 802.11 b/g/n)
- **Channel—**Automatic, 1 to 11.

  Selecting **Automatic** enables Dynamic Channel Assignment. This means that channels are dynamically assigned to each AP, under the control of the master 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.
- **Channel Width—**20 MHz

  The channel width for 2.4 GHz can only be 20 MHz.

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.

- **Transmit Power—**Automatic, 1 to 8.

  This is a logarithmic scale of the transmit power, that 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 Under the **802.11 a/n/ac** tab, you can set the following parameters:

- **Admin Mode—**Enabled or Disabled. This enables or disables the corresponding radio on the AP (5 GHz for 802.11a/n/ac).
- **Channel—**Automatic, 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 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—**20, 40, 80 MHz

  The channel width for 5 GHz can be set to 20, 40, or 80 MHz, if channel bonding is used.
- **Transmit Power—**1 to 8.

  This is a logarithmic scale of the transmit power, that 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 7 Click **Apply** to save your changes and exit.

Creating a Customized Login Page for Guest WLAN Users

Before You Begin

To allow a guest user the 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.

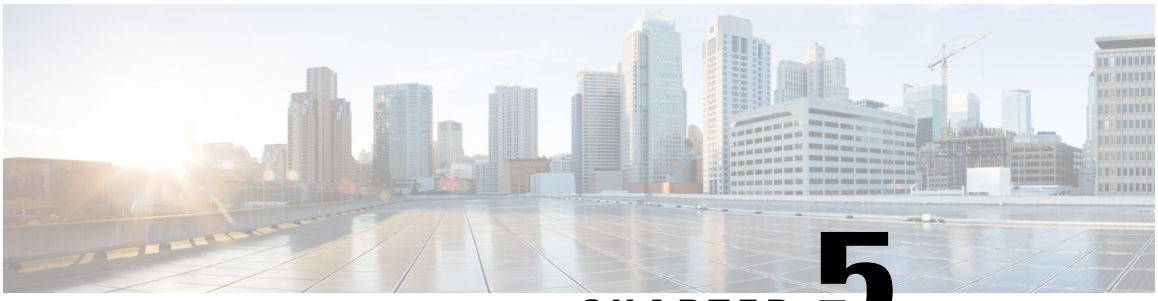
2 Set up a guest user account. Go to **Wireless Settings > WLAN Users**, and set up an account with the **Guest User** check box selected. For more information, see Viewing and Managing WLAN Users, on page 36.

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 In the window that is displayed, set the following parameters:

- **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 3 Click **Apply**.



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 Administrator Accounts

You require administrative (or admin) user accounts for logging in to the controller user interface, for configuring the controller, and for viewing configuration information. This prevents unauthorized users from accessing or configuring the controller.

Adding an Admin Account

Step 1 Choose **Management** > **Admin Accounts**.
The **Admin Accounts** window is displayed, and lists 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 window.

Step 2 Click **Add New User** to add a new admin user.

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—**This option creates an administrative account with read-only privileges. The admin user can view the controller configuration but cannot make any changes to the configuration.

- **Read-Write—**This option creates an administrative account with read and write privileges. The admin user can view and make changes to the controller configuration.

- **Password—**Enter a password for the administrative user account, based on the following rules:
  - Passwords are case sensitive.
  - The password should contain a minimum of eight 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 password should not contain the word Cisco or a management username. The password should not be any variant of these words, obtained by reversing the letters of these words, or by changing the capitalization of letters, or by substituting 1, |, or ! or substituting 0 for o or substituting $ for s.

Step 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 42.

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.

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:

- **NTP Index—**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.
- **NTP Server—**Specify the IPv4 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**.

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. This will prevent the current configurations on the Cisco Mobility Express controller from being deleted.

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 master 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 master AP and if a mismatch is detected, the new AP requests for a software upgrade. The master AP facilitates the transfer of the new software from the TFTP server or the HTTP path, to the new AP.

Downloading a newer version of the Cisco Mobility Express software image from the TFTP server to the Cisco Mobility Express network that has to be upgraded can take around 5 minutes per 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.

Guidelines for Preparing a TFTP Server

Follow these guidelines while preparing the TFTP server 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, the following 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.

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.

Performing the Software Update

Before You Begin

- Decide whether you are using TFTP or HTTP for the software update.

  If your network consists of only 1850, 1830, or both models of access points (which support ap1g4 images), then you can perform the update via TFTP or HTTP. If you have other supported AP models in your network, then you can use only TFTP for the update.

- If you are using a TFTP server for the software update, then the TFTP server should be configured and accessible. See Guidelines for Preparing a TFTP Server, on page 46.

- A computer that can access Cisco.com and the TFTP server should be available.

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 file to your computer's hard drive.
g) 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 or HTTP as required.

Step 4 If you have chosen **TFTP** as the transfer mode then:

a) In the **IP Address (IPv4)** field, enter the IP address of the TFTP server.
b) In the **File Path** field, enter the TFTP server directory path of the software file, along with the name of the file.

Step 5 If you have chosen **HTTP** as the transfer mode, then click the **Browse** button adjacent the **File Path** field, and then browse to and choose the software file.
The file name of the software file appears in the **File Path** field

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 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.

  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.

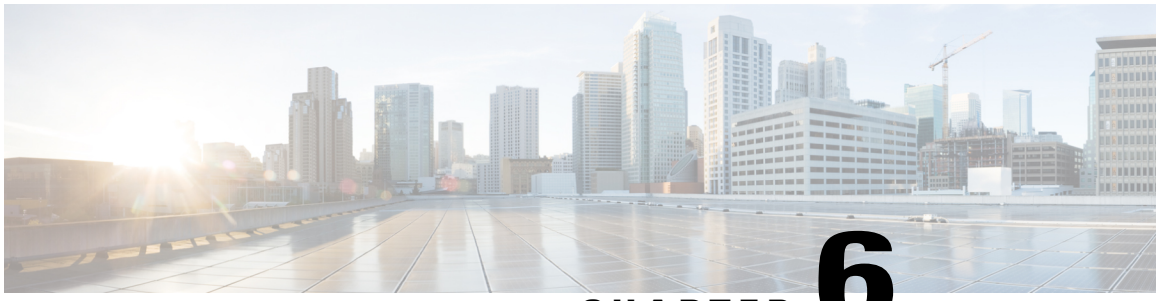
The Preimage Download Status section of the page shows the status of the pre-image download to the APs in the network.

After the pre-image download is complete, click **Reboot** to reboot the controller.

- 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 Reboot Time** field, and then click **Schedule Later**. After the preimage download is complete, the controller automatically reboots.

For more information on the Preimage Download feature, see Predownloading an Image to an Access Point, on page 67.

Step 8 Log in to the controller and verify the controller software version in the **Software Update** window.



CHAPTER 6

Using Advanced Settings and Operations

Managing SNMP

Simple Network Management Protocol Version 2 (SNMPv2) is a protocol for network management. It is used for collecting information from, and configuring and managing all the devices in the network.

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

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

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

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

To connect to an SNMP server, specify the IP address of the server in the **SNMP Server IP** field.

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**.

Resetting the Mobility Express Controller

This operation can be performed only by Admin users.

To reset your Cisco Mobility Express wireless LAN controller to its default factory-shipped parameters:

1. Choose **Advanced > Reset to Factory Default**.
   This opens the **RESET MOBILITY EXPRESS CONTROLLER TO FACTORY DEFAULT** window.
2. Click **Continue** to:
   - Erase the Cisco Mobility Express controller configuration parameters to their factory default values and reboot the Cisco Mobility Express wireless LAN controller.
   - Reset and reboot the master AP to it's default factory-shipped configuration.

After the Mobility Express Controller reboots, proceed to Starting the Initial Configuration Wizard, on page 6.

Rebooting the Mobility Express Controller

At any time, you can reboot the controller by choosing **Management > Software Update**, and then clicking **Restart**.

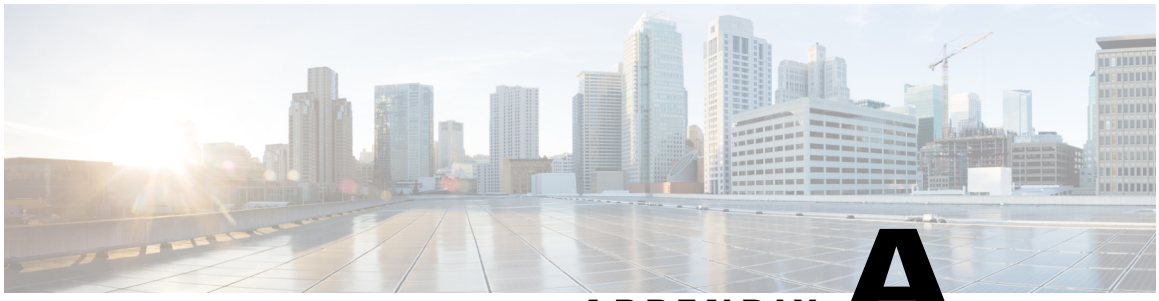
Saving Controller Configuration

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 master 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 master 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.



APPENDIX A

Controller CLI Commands

About Supported CLI Commands

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

The Cisco Wireless Controller Command Reference guides, for Cisco Unified Wireless Network Software Releases, are listed at the following URL: 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 the Employee Network, enter **YES**. Otherwise enter **no**.
If you have entered **YES**, then enter the following:

1. Employee Network Name (SSID)
2. Employee VLAN Identifier (0 = untagged)
3. Employee Network Security. You can enter **PSK** or **enterprise**.
4. 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).
5. 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 11 To enable the Guest Network, enter **YES**. Otherwise enter **no**.
If you have entered **YES**, then enter the following:

1. Guest Network Name (SSID).
2. Guest VLAN Identifier (0 = untagged).
3. Guest Network Security. You can enter **WEB_CONSENT** or **psk**.
4. 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 12 To enable RF Parameter Optimization, enter **YES**. Otherwise, enter **no**.

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

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

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

Step 13 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.

Application Visibility Commands

The following commands are used to configure Application Visibility on the Mobility Express controller.

Command	Description	Added in Release
config flexconnect group default-flexgroup avc 1 visibility { enable | disable }	To enable or disable Application Visibility in a WLAN	8.1.122.0
show flexconnect group detail default-flexgroup	To display the status of Application Visibility in each WLAN	8.1.122.0
show flexconnect avc statistics group default-flexgroup	To view Application Visibility statistics based on the flex group	8.1.122.0
how flexconnect avc statistics client *client_MAC*	To view Application Visibility statistics based on each client	8.1.122.0

Commands for Collecting Log, Core, and Crash Files

Command	Description	Added in Release
1 transfer upload datatype support-bundle **2** transfer upload mode { tftp | ftp } **3** transfer upload username *username* password *password* This command is only for an FTP transfer. **4** transfer upload filename *filename* **5** transfer upload path *file_path* **6** transfer upload serverip *server_ip_address* **7** transfer upload start	Use these commands in sequence to collect log, core and crash files. The files of the following data types are collected, bundled into a .TAR file, and the uploaded to a configured TFTP or FTP server: • run-config • systemtrace • traplog • debug-file • crashfile • coredump • ap-crash-data	8.3.102.0
debug transfer all enable	To debug the code-flow, use this command before the **transfer upload start** command.	8.3.102.0
debug disable-all	To disable debugging of the code-flow.	8.3.102.0

Commands for Software Download from Cisco.com

Step	Command	Description	Added in Release
1	transfer download ap-images mode cco	To set the mode of download of software images to be from Cisco.com.	8.3.102.0
2	transfer download ap-images cco-username *username* cco-password *password*	To specify the Cisco.com credentials to be used.	8.3.102.0

Step	Command	Description	Added in Release
3	transfer download ap-images version { suggested | latest }	To specify whether the suggested or the latest software version images are to be downloaded.	8.3.102.0
4	transfer download ap-images cco-auto-check { enable | disable }	To set the controller to automatically check for software image updates from Cisco.com.	8.3.102.0
5	transfer download start	To start the download.	8.3.102.0

CleanAir Commands

Command	Description	Added in Release
config 802.11b cleanair enable *ap_MAC*	To enable CleanAir on an associated AP. Not applicable to 1850 and 1830 series APs.	8.1.122.0
show 802.11b cleanair device ap *ap_MAC*	To list all the interference devices connected to the AP.	8.1.122.0
show 802.11b cleanair device type jammer	To jam a specific interference device.	8.1.122.0

CMX Cloud Commands

Command	Description	Added in Release
config cloud-services server id-token *CMX_token*	To specify a valid CMX server token.	8.3.102.0
config cloud-services server url *url*	To specify a valid CMX server URL.	8.3.102.0
config cloud-services cmx enable	To enable CMX analytics.	8.3.102.0
show cloud-services cmx summary	To view details of the configured CMX cloud services.	8.3.102.0

Controller Image Upgrade Commands

The following commands are used when performing a Mobility Express controller software image upgrade.

Command	Description	Added in Release
transfer download ap-images imagePath *image_path*	To set the path of the software image on the TFTP server	8.1.122.0
transfer download ap-images mode tftp	To set the file transfer mode as TFTP	8.1.122.0
transfer download ap-images serverIp *ipv4_address*	To specify the IP address of the TFTP server	8.1.122.0
transfer download start	To save the configuration and start the image download	8.1.122.0
transfer download stop	To stop the ongoing image download	8.3.102.0
debug transfer all { enable | disable }	To debug the transfer and download with all sub commands enabled	8.1.122.0
debug transfer tftp { enable | disable }	To debug transfer download of TFTP	8.1.122.0
debug transfer trace { enable | disable }	To debug transfer trace	8.1.122.0

DNS Commands

Command	Description	Added in Release
config network dns default	To configure the default DNS servers.	8.2.100.1
show network summary	To view a network summary, with the default DNS servers listed, if they are enabled.	8.2.100.1

Migration Commands

The following commands are used for converting an AP from Mobility Express software image to Lightweight CAPWAP AP software image, and vice-versa.

Command	Description	Added in Release
ap-type capwap	To convert ap-type from Mobility Express to CAPWAP	8.1.122.0
ap-type mobilityexpress tftp://*tftp_server*/*file_name*	To convert ap-type from CAPWAP to Mobility Express, when running an Mobility Express software image	8.1.122.0
config ap unifiedmode *switch_name switch_IP_address*	To convert all APs to type CAPWAP simultaneously from the switch	8.1.122.0

NTP Commands

Command	Description	Added in Release
config time ntp server 1 *FQDN_of_server*	To configure the fully qualified domain name of the NTP server having, for example here, NTP index 1.	8.2.100.1
config time ntp server 2 *NTP_Server_IP_address*	To configure the IP address of the NTP server having, for example here, NTP index 2.	8.2.100.1

Next Preferred Master AP and Forced Failover

Command	Description	Added in Release
config ap next-preferred-master *cisco_ap_name*	To set the next preferred master AP.	8.3.102.0

Command	Description	Added in Release
config ap next-preferred-master *cisco_ap_name* forced-failover	To set the next preferred master AP and to manually trigger a failover to that AP.	8.3.102.0

UX Regulatory Domain Commands

Command	Description	Added in Release
config wlan disable 1	To disable WLAN 1	8.1.122.0
config wlan universal-ap-admin enable 1	To enable as universal-ap-admin for wlan 1	8.1.122.0
config wlan enable 1	To enable WLAN 1	8.1.122.0
show ap summary	To show the present country configured (US, IN, etc) if not UX.	8.1.122.0

VRRP Commands

The following Virtual Router Redundancy Protocol (VRRP) commands are used during the Mobility Express controller failover and for the master AP.

Command	Description	Added in Release
config ap next-preferred-master	To configure the master AP that has been elected to take over as the new master AP	8.1.122.0
show ap next-preferred-master	To display the status of the master AP	8.1.122.0
clear ap next-preferred-master	To clear the configuration of the master AP	8.1.122.0

WGB Commands

The following show commands can be used to view details of workgroup bridges (WGBs).

Command	Description	Added in Release
show wgb summary	To display the summary of workgroup bridges	8.1.122.0
show wgb detail *WGB_MAC*	To display the details of a specific workgroup bridge	8.1.122.0

WLAN Security Commands

Command	Description	Added in Release
config wlan security wpa akm cckm {enable | disable} wlan_id	To enable or disable CCKM	8.2.100.1

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.

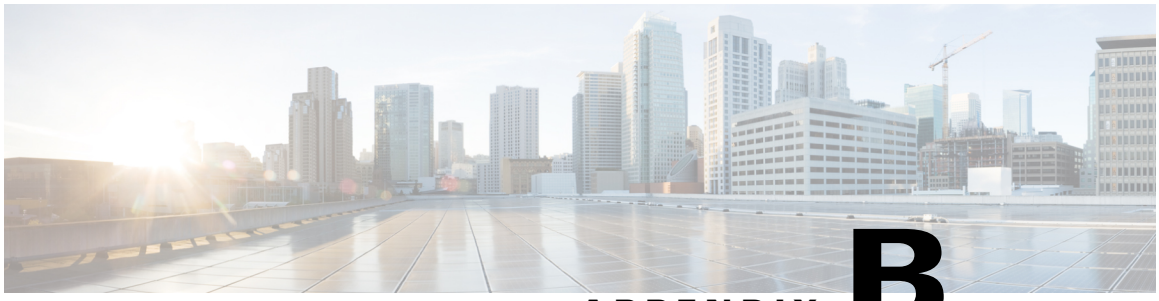
Step 6 To enable or disable the authentication key management for fast transition over a distributed system, use the **config wlan security wpa akm ft over-the-ds** {**enable** | **disable**} *wlan-id* command.
By default, the authentication key management for fast transition over a distributed system 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.



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 Master AP Election Process

Mobility Express Controller Redundancy for Failover

In a Cisco Mobility Express network, not all the APs may have the capability to work as a master AP. See the Supported Cisco Aironet Access Points, on page 1 to know which AP models are capable of working as a master AP.

In order to have Cisco Mobility Express controller redundancy to enable a failover, your network must have two or more active APs with master AP capability. In the event of a failover, one of these other APs will automatically be elected as a master. The newly elected Master will have the same IP and configuration as the original Master. From an administrator perspective, there will be no difference between the original Master and the newly elected Master in case of a failover.

Note Clients that connect to the master AP will lose connectivity during a failover.

Mobility Express Controller Forced Failover

In a Cisco Mobility Express network, not all the APs may have the capability to work as a master AP. See the Supported Cisco Aironet Access Points, on page 1 to know which AP models are capable of working as a master AP.

You can manually force any AP, that has the capability to work as a master AP, to become the master AP. This forced failover of the master AP to another master-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 master.

   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 master 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 Master 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 master to an AP of your choice, using the GUI or CLI methods, the current master AP reboots while the new AP takesover as the controller, with the IP address and configuration as the

previous master. The previous master, after rebooting, comes back online and joins the new master AP as a subordinate AP.

Note Like any failover, this forced failover causes some downtime in the 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.

Master AP Election Process

In a Cisco Mobility Express AP network, when the master AP shuts down, one of the other master-capable APs in this deployment is automatically designated as the master AP. The automatic selection of the master AP among the Cisco Mobility Express-enabled APs is as per an internal automatic master election process. This process is used to both detect the failure of the master AP and to designate the new master AP among the eligible APs. This process is based on Virtual Router Redundancy Protocol (VRRP) and algorithmically determines the next master AP, based on the following parameters listed in the order of descending precedence:

- The AP configured as VRRP master, 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.

How an Access Point is Added to the Cisco Mobility Express Network

When a supported AP that is running a CAPWAP lightweight AP software is added to the Cisco Mobility Express network, it will start with the CAPWAP State: Discover advertisements on boot up. The Cisco Mobility Express controller running on Master AP will respond to the advertisement and the new AP will go through the process of joining the Cisco Mobility Express controller. If the AP being added is running the same version, it will straightaway join the Cisco Mobility Express network. However, if the AP is running an image older than the one running on the Cisco Mobility Express, the controller will download the corresponding Cisco Mobility Express-capable AP image from the TFTP server.

For information on performing a software update, see Updating the Cisco Mobility Express Software, on page 45 .

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 13. 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.

Tip If you face issues with converting the AP software to a Cisco Mobility Express software, upgrade the AP CAPWAP software to the latest AP software version ap3g3-k9w8-tar.153-3.JD.tar. Now, you can convert the CAPWAP software to the Cisco Mobility Express software *AIR-AP2800-K9-ME-8-3-102-0.tar*.

This issue occurs in Mobility Express-capable APs shipped with default images or a version of the images prior to Cisco Wireless Release 8.3. This is due to insufficient space in the AP's memory or because the AP has been started in U-boot mode where the image is not found in flash.

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.

What to Do Next

Proceed to Starting the Initial Configuration Wizard, on page 6.

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 master 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.

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

	Dependency	Typical (For enterprise deployments. Default profile.)	High Density (Where throughput is most important)	Low Density (For coverage in open spaces)
RX Sensitivity	Global per band (Advanced RX-SOP) RF profiles	Default (Automatic)	Medium (RX-SOP)	Low
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

Related Documents

Cisco Mobility Express Release Notes, 8.2 Release

http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/crn82.html#pgfId-1349826

Cisco Wireless Controller Command Reference, Release 8.2

http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-2/cmd-ref/b_cr82.html

Cisco Aironet 1850 Series Access Points Hardware Guide

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1850/hardware/guide/ap1850hwguide.html

Cisco Aironet 1830 Series Access Points Hardware Guide

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1830/quick/guide/ap1830getstart.html

Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide

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

FAQs

Which access points can host the Mobility Express wireless LAN controller function and which access points can be managed by it?

See Supported Cisco Aironet Access Points, on page 1.

What controller-based modes does the Mobility Express wireless LAN controller function support?

Access points managed by the 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 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 Access Points 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 68.

If my deployment needs to downsize to 25 access points or less, can they convert from existing controller-based deployment to Mobility Express?

Yes. You can convert your wireless controller-based deployment to Mobility Express, as long as your deployment has access points capable of hosting the Mobility Express controller functionality, such as Cisco Aironet 1850 or 1830 series access points.

Where can I get more information on the Cisco Mobility Express solution?

Go to http://www.cisco.com/go/mobilityexpress.