



Cisco Mobility Express Deployment Guide

First Published: 2016-01-06

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2015 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface	vii
Audience	vii
Document Organization	vii
Command Syntax Conventions	viii
Related Documentation	ix
Obtaining Documentation and Submitting a Service Request	x

CHAPTER 1

Product Overview	1
Supported Cisco Aironet Access Points	2
Supported Features	3
Cisco Mobility Express CLI Commands	3
Licenses	3
Software Release Numbers	3
Interoperability	3

CHAPTER 2

Getting Started	5
Ports	5
Access Point Status LEDs	6
Interfaces	7
WLANs	7
Switch Configuration	7

CHAPTER 3

Deploying Mobility Express	9
Pre-requisites for Deploying Mobility Express	9
Connecting Mobility Express Capable Access Point	9
Configuring Mobility Express controller using Over-the-Air Setup Wizard	10

Configuring Mobility Express controller using Startup Wizard from CLI	17
Console Connection	17
Startup Wizard from CLI	17
Logging into Mobility Express	18

CHAPTER 4 **Monitoring Mobility Express Network** 21

Viewing Network Summary	21
Monitoring Dashboard	21
View Access Points Summary using GUI	23
View Access Points Summary using CLI	23
View Access Point Details using GUI	24
View Access Point Details using CLI	25
View Client Summary using GUI	26
View Client Summary using CLI	26
Viewing Wireless Dashboard	26
Viewing AP Performance	26
Viewing Client Performance	27
Best Practices	28

CHAPTER 5 **Managing Wireless Settings** 29

WLANs	29
Creating WLANs using GUI	29
Access Points	35
Managing Access Point using GUI	35
WLAN Users	39
Creating a WLAN User using GUI	40
Guest WLANs	40
Creating WLAN using GUI	40

CHAPTER 6 **Managing Mobility Express Network** 43

Management Access	43
Configuring Management Access using GUI	43
Configuring Management Access using CLI	44
Managing Administrator Accounts	45

Creating an Admin Account using GUI	45
Creating an Admin Account using CLI	47
Editing an Admin Account using GUI	47
Editing an Admin Account using CLI	48
Deleting Admin Account using GUI	48
Deleting Admin Account using CLI	49
Managing Time on Mobility Express Controller	49
Configuring NTP Server on Mobility Express Controller using GUI	49
Configuring NTP Server on Mobility Express Controller using CLI	50
Configuring Date and Time Manually on Mobility Express Controller using GUI (Method I)	51
Configuring Date and Time Manually on Mobility Express Controller using GUI (Method II)	52
Configuring Date and Time Manually on Mobility Express Controller using CLI	52
Updating Cisco Mobility Express Software	53
Updating Cisco Mobility Express network using GUI	54
Updating Cisco Mobility Express Network using CLI	57

CHAPTER 7**Using Advanced Settings 61**

SNMP	61
Managing SNMP using GUI	61
Managing SNMP using CLI	62
Logging	63
System Logging using GUI	63
System Logging using GUI using CLI	64
Reset to Factory Default	65
Mobility Express Network to Factory Default using GUI	65

CHAPTER 8**Adding an Access Point to Mobility Express Network 67**

Adding an Access Point to Mobility Express Network	67
--	----

CHAPTER 9**Primary AP Failover and Electing a New Primary 71**

Primary AP Failover	71
Primary Election	71

CHAPTER 10**Conversion 73**

Converting a CAWAP AP into a Mobility Express AP 74
 Converting a Mobility Express AP into a CAPWAP AP 76

CHAPTER 11 **Managing Mobility Express Deployments from Cisco Prime Infrastructure** 79

Adding Mobility Express to Prime 79

CHAPTER 12 **Mobility Express CLI Reference** 87

Application Visibility Commands 87
 ClearAir Commands 87
 Controller Image Upgrade Commands 88
 DNS Commands 88
 Flexconnect Commands 88
 Migration Commands 88
 NTP Commands 89
 Ports and Interface Commands 89
 RRM Commands 89
 Show Commands 89
 Config Commands 90
 Security Commands 93
 Show Commands 93
 Config Commands 94
 System Management Commands 95
 UX Regulatory Domain Commands 96
 VRRP Command 96
 WGB Commands 96
 WLAN Commands 97
 Config Commands 97
 Show Commands 99



Preface

- [Audience, on page vii](#)
- [Document Organization, on page vii](#)
- [Command Syntax Conventions, on page viii](#)
- [Related Documentation, on page ix](#)
- [Obtaining Documentation and Submitting a Service Request , on page x](#)

Audience

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

Document Organization

This document is organized into the following chapters:

Table 1: Document Organization

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

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

Command Syntax Conventions

This document uses the following conventions:

Table 2: Command Syntax Conventions

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

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

Reader Alert Conventions

This document uses the following conventions for reader alerts:



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



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



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



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

Related Documentation

- **User Guide**

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

- **Release Note**

<http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/crm83.html#pgfId-1515571>

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation, at:

<http://%20www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>

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



CHAPTER 1

Product Overview

This section provides an overview of Cisco Mobility Express.



Note In this document, Mobility Express refers to the Cisco 1800 series Access Point which supports the controller functionality. It is referred to as primary AP.

Cisco Mobility Express is a software-based controller function integrated on Cisco 1800 series Wave 2 Access Points. It is a simplified, low cost, feature rich WiFi architecture with enterprise level WLAN capability streamlined for small and mid-sized deployments.

In a Cisco Mobility Express network, Access Point (AP) running the wireless controller function is designated as the primary AP. The other Access Points which are managed by this primary AP are referred as Subordinate APs.

The primary AP has two roles:

1. It functions and operates as a wireless LAN controller to manage and control the Subordinate APs. The Subordinate APs operate as lightweight access points to serve clients.
2. Primary AP operates as an Access Point to serve clients.

For the list of supported primary and subordinate APs, see [Supported Cisco Aironet Access Points](#) , on page 2.



Note Cisco Mobility Express supports central authentication, and local switching.

- [Supported Cisco Aironet Access Points](#) , on page 2
- [Supported Features](#), on page 3
- [Cisco Mobility Express CLI Commands](#), on page 3
- [Licenses](#) , on page 3
- [Software Release Numbers](#), on page 3
- [Interoperability](#), on page 3

Supported Cisco Aironet Access Points

Access Points which support the Mobility Express controller function capability are listed in the following table:

Table 3: Access Points supporting Mobility Access (Primary APs)

Access Points supported as Primary AP	Supported Model Numbers
Cisco Aironet 1850 Series	<ul style="list-style-type: none"> • AIR-AP1852I-x-K9C • AIR-AP1852E-x-K9C
Cisco Aironet 1830 Series	<ul style="list-style-type: none"> • AIR-AP1832I-x-K9C



Note

The model numbers that contain -x- is a placeholder for the actual letter indicating the model's regulatory domain. For more information on regulatory domains, see [www.cisco.com go aironet compliance](http://www.cisco.com/go/aironet/compliance).

The Access Points which operate as subordinate APs are listed in the following table:

Table 4: Access Points supported as Subordinates

Access Points supported as Subordinate APs	Supported Model Numbers
Cisco Aironet 700i Series	<ul style="list-style-type: none"> • AIR-CAP702I- x-K9
Cisco Aironet 700w Series	<ul style="list-style-type: none"> • AIR-CAP702W- x-K9
Cisco Aironet 1600 Series	<ul style="list-style-type: none"> • AIR-CAP1602I-x-K9 • AIR-CAP1602E-x-K9
Cisco Aironet 1700 Series	<ul style="list-style-type: none"> • AIR-CAP1702I- x-K9
Cisco Aironet 1800 Series	<ul style="list-style-type: none"> • AIR-AP1832I-x-K9C • AIR-AP1852I-x-K9C • AIR-AP1852E-x-K9C
Cisco Aironet 2600 Series	<ul style="list-style-type: none"> • AIR-CAP2602I-x-K9 • AIR-CAP2602E-x-K9
Cisco Aironet 2700 Series	<ul style="list-style-type: none"> • AIR-CAP2702I-x-K9 • AIR-CAP2702E-x-K9

Access Points supported as Subordinate APs	Supported Model Numbers
Cisco Aironet 3600 Series	<ul style="list-style-type: none"> • AIR-CAP3602I-x-K9 • AIR-CAP3602E-x-K9
Cisco Aironet 3700 Series	<ul style="list-style-type: none"> • AIR-CAP3702I-x-K9 • AIR-CAP3702E-x-K9

Supported Features

See Supported features section in Release notes, <http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/crn81mr2.html#12966> .

Cisco Mobility Express CLI Commands

Cisco Mobility Express maintains CLI command parity for supported features with existing WLCs. New CLI commands specific to Mobility Express operation have been added and are documented in its respective sections. For more details on Mobility Express command reference for Release 8.2 see http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-2/cmd-ref/b_cr82/b_cr82_chapter_01101.html

Licenses

There is no license requirement for Mobility Express.

Software Release Numbers

Cisco Mobility Express is supported from 8.1.121.0 release. You can check the system information, using the command:

```
(cisco controller) >show sysinfo
Manufacturer's Name ..... Cisco systems Inc.
Product Name ..... Cisco controller
Product version ..... 8.1.121.0
```

Interoperability

Cisco Mobility Express can interoperate with the following:

Cisco Prime Infrastructure

- PI Release 3.0.1 and later

Connected Mobility Experiences (CMX)

- Presence is supported on CMX Release 10.2 and later

Cisco Identity Services Engine (ISE)

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



CHAPTER 2

Getting Started

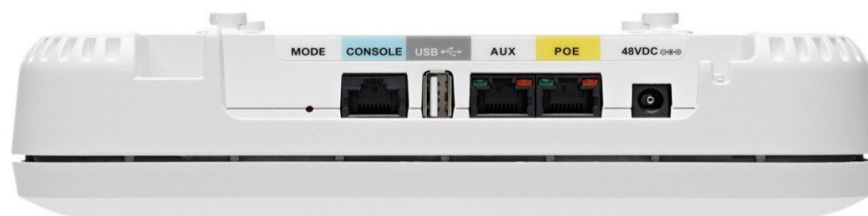
This chapter provides information about the Mobility Express ports, interfaces, WLANs, LED states and access switch configuration.

- [Ports, on page 5](#)
- [Access Point Status LEDs, on page 6](#)
- [Interfaces, on page 7](#)
- [WLANs, on page 7](#)
- [Switch Configuration, on page 7](#)

Ports

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

Figure 1: Ports of Cisco 1800 series Access Points



Mode

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

```

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

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

```

Console Port (RJ-45)

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

USB

This port is not currently supported.

Aux Port (RJ-45)

This port is not currently supported.

POE (Management Port) (RJ-45)

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

Access Point Status LEDs

The location of the access point status LED is shown in [Figure 1: Ports of Cisco 1800 series Access Points, on page 5](#).

**Note**

The LEDs may show small variations in color intensity and hue from unit to unit. This variation is within the normal range of the LED manufacturer's specifications and is not a defect.

The access point status LED indicates various conditions such as:

Table 5: LED Status Indications

Message Type	LED Type	Meaning of Message
Client Association status	Chirping Green	Normal operating condition, but no wireless client associated.
	Green	Normal operating condition, at least one wireless client association.
Boot loader status	Green	Executing boot loader
Boot loader error	Red	Boot loader signing verification failure.

Message Type	LED Type	Meaning of Message
Boot loader signing verification failure	Blinking Amber	AP priming to a new regulatory domain by Neighbor Discovery Protocol (NDP) is in progress.
	Cycling Red, Green and off	AP waiting to be primed.
	Chirping Red	AP primed to a wrong regulatory domain.
Operating status	Blinking amber	Software upgrade is in progress
	Cycling through green, red and amber	Discovery/join process is in progress
	Rapidly cycling through red, green, amber and off	Access point location command invoked from controller web interface.
Access point operating system	Cycling through red, green, amber, and off	General warning, insufficient inline power.

Interfaces

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

WLANs

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

Switch Configuration

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

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

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

interface Vlan10
 description >> Employee Network <<
 ip address 10.10.10.1 255.255.255.0
```

```
!  
interface Vlan20  
  description >> Guest Network <<  
  ip address 20.20.20.1 255.255.255.0  
!  
interface Vlan122  
  description >> Management, Master AP and Subordinate APs<<  
  ip address 172.20.229.2 255.255.255.0  
  
interface GigabitEthernet1/0/37  
  description >> Connected to Cisco 1850 Access Point <<  
  switchport trunk native vlan 122  
  switchport trunk allowed vlan 10,20,122
```



CHAPTER 3

Deploying Mobility Express

- [Pre-requisites for Deploying Mobility Express, on page 9](#)
- [Connecting Mobility Express Capable Access Point, on page 9](#)
- [Configuring Mobility Express controller using Over-the-Air Setup Wizard, on page 10](#)
- [Configuring Mobility Express controller using Startup Wizard from CLI, on page 17](#)
- [Logging into Mobility Express, on page 18](#)

Pre-requisites for Deploying Mobility Express

The pre-requisites for deploying Mobility Express network are as follows:

1. You must not have other Cisco wireless controllers, neither appliance nor virtual, in the same network, during set up or daily operation of a Cisco Mobility Express network.
2. Configure a DHCP server on the switch or externally so that Cisco 1800 series Access Point can obtain an IP address at boot up. The DHCP server also assigns IP address to other APs and wireless clients.
3. Configure a TFTP server which can be accessed from the Management interface of Mobility Express. Save the **AIR-<AP Type>-K9-<version>.tar** and **AIR-<AP Type>-K9-ME-<version>.zip** file (unzipped) on the TFTP server.
4. Decide on the first AP to set up. The first AP to setup must support Cisco Mobility Express controller functionality. You can also connect multiple Cisco 1800 series Access Points running Mobility Express to the switch.
5. If your network is using universal regulatory domain access points, then you need to prime the access point to the right regulatory domain, before the APs start serving clients. For more information, see *Cisco Aironet Universal AP Priming and Cisco Air Provision User Guide*, at this URL:
http://www.cisco.com/c/en/us/td/docs/wireless/access_point/ux-ap/guide/uxap-mobapp-g.html
6. A Wi-Fi-enabled laptop with G Band to connect to the pre-defined *CiscoAirProvision* SSID. The laptop needs to have a compatible browser. For a list of browsers compatible with the with the Cisco Mobility Express wireless LAN controller web interface and the initial configuration wizard, see .

Connecting Mobility Express Capable Access Point

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

Procedure

Step 1

Connect and power up the Mobility Express capable access point.

- a) The switch port to which Cisco 1800 Access Point is connected can be a trunk port or an access port. If multiple VLANs are being used for client traffic, the switch port should be configured to trunk the VLANs. Also, note that management traffic is untagged and if a VLAN is being used for management, it should be configured as a native VLAN on the switch port.

Example of the switch port is as follows:

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

Step 2

Observe the access point LED (for LED descriptions, see [Table 5: LED Status Indications](#)).

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

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

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

Procedure

Step 1

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

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

Note *CiscoAirProvision* SSID is broadcast at 2.4GHz.

Step 2

Open a browser and go to <http://192.168.1.1> which redirects to the initial configuration wizard.

The initial configuration wizard's admin account page appears.

Figure 2: Initial Configuration Wizard's Admin Account Page

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

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

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

- Enter the admin username. Maximum up to 24 ASCII characters.
- Enter the password. Maximum up to 24 ASCII characters.

When specifying a password, ensure that:

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

Step 4 Set up your controller by specifying the values.

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

Field Name	Description
System Name	Enter the system name for Mobility Express. Example: MobilityExpress-WLC
Country	Choose the country from the drop down list.

Field Name	Description
Date & Time	Choose the current date and time. Note The wizard attempts to import the clock information (date and time) from the computer using JavaScript. It is highly recommended that you confirm the clock settings before continuing. The access points depend on clock settings to join the WLC.
Time Zone	Choose the current time zone.
NTP Server	Enter the NTP server details.
Management IP Address	Enter the Management IP address.
Subnet Mask	Enter the subnet mask address.
Default Gateway	Enter the default gateway.

Figure 3: Set Up Your Controller Tab

The screenshot shows the 'Set Up Your Controller' tab in the Cisco Aironet 1850 Series Mobility Express configuration wizard. The form contains the following fields and values:

- System Name: MobilityExpress
- Country: United States (US)
- Date & Time: 08/31/2015, 14:00:37
- Timezone: Pacific Time (US and Canada)
- NTP Server: 10.10.10.5
- Management IP Address: 10.10.10.2
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.10.10.1

Buttons for 'Back' and 'Next' are located at the bottom of the form.

Step 5Click **Next**.**Step 6**

Create the wireless networks by specifying the following fields:

Field Name	Description
Network Name	Enter the network name.

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

Figure 4: Create Your Wireless Networks Tab Fields

Step 7

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

Field Name	Description
Network Name	Specify the SSID for your Guest network.
Security	Choose Web Consent or WPA2 Personal from the drop-down list.

Field Name	Description
Pass Phrase	If WPA2 Personal security is chosen, specify the Pre-Shared Key (PSK).
VLAN	Choose Employee VLAN or create a New VLAN (with VLAN ID 1 to 4096).
VLAN ID	Specify the VLAN ID of the new VLAN (with VLAN ID 1 to 4096).

Figure 5: Create Your Wireless Networks - Guest

Step 8

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

Figure 6: Advanced Settings Tab


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

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

Step 9 Select Traffic Type and click **Next** to continue.

A confirmation screen displays the summary of the configuration.

Step 10 Click **Apply**, if all the settings are correct

 Cisco Aironet 1850 Series Mobility Express

Please confirm settings and apply

1 Controller Settings

Username	admin
System Name	MobilityExpress
Country	United States (US)
Date & Time	08/31/2015 14:18:31
Timezone	Pacific Time (US and Canada)
NTP Server	10.10.10.5
Management IP Address	10.10.10.2
Management IP Subnet	255.255.255.0
Management IP Gateway	10.10.10.1

2 Wireless Network Settings

Employee Network

Network Name	Employee-PSK
Security	WPA2 Personal
Pass Phrase:	*****
Employee VLAN	Management VLAN
DHCP Server Address	-

Guest Network

Network Name	Guest
Security	Web Consent
VLAN ID	20
DHCP Server Address	-

3 Advanced Settings

RF Parameter Optimization

Client Density	Typical
Traffic Type	Data and Voice

A message appears with a prompt 'System will reboot...Do you want to apply these configuration?'

Step 11 Click **OK** to reboot.

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

Step 12 APs reboots and join the Mobility Express controller, if there are more than one 1800 series APs.

Configuring Mobility Express controller using Startup Wizard from CLI

Console Connection

Before you can configure the AP to Mobility Express Controller, connect to the port marked 'CONSOLE' using SecureCRT, Putty or similar applications. The default parameters for the console ports are 9600 baud, eight data bits, one stop bit, and no parity. The console ports do not support hardware flow control. Choose the serial baud rate of 9600.

Startup Wizard from CLI

After connecting to the 'CONSOLE' port on the AP, power up the AP. After a few minutes, the following Welcome message will be shown. To configure the Mobility Express controller, follow the steps as shown in the example below.

```
Cisco Aironet 1850 Series Mobility Express
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup

Would you like to terminate autoinstall? [yes]: yes
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (3 to 24 characters): *****
Re-enter Administrative Password          : *****

System Name [Cisco_ca:09:20] (31 characters max): Mobility Express
Enter Country Code list (enter 'help' for a list of countries) [US]: US
Configure a NTP server now? [YES][no]: Yes
Enter the NTP server's IP address: 10.10.10.77
Enter timezone location index (enter 'help' for a list of timezones): 5

Management Interface IP Address: 10.10.10.10
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Create Employee Network? [YES][no]: YES
Employee Network Name (SSID)? : Employee
Employee VLAN Identifier ?: 122
Employee Network Security? [PSK][enterprise]: PSK
Employee PSK Passphrase (8-38 characters)? : Cisco123
Re-enter Employee PSK Passphrase: Cisco123
Create Guest Network? [yes][NO]: NO
Enable RF Parameter Optimization? [YES][no]: YES
Client Density [TYPICAL][Low][High]: TYPICAL
Traffic with Voice [NO][Yes]: YES

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
```

```
Cleaning up Provisioning SSID  
  
Configuration saved!  
Resetting system with new configuration...
```



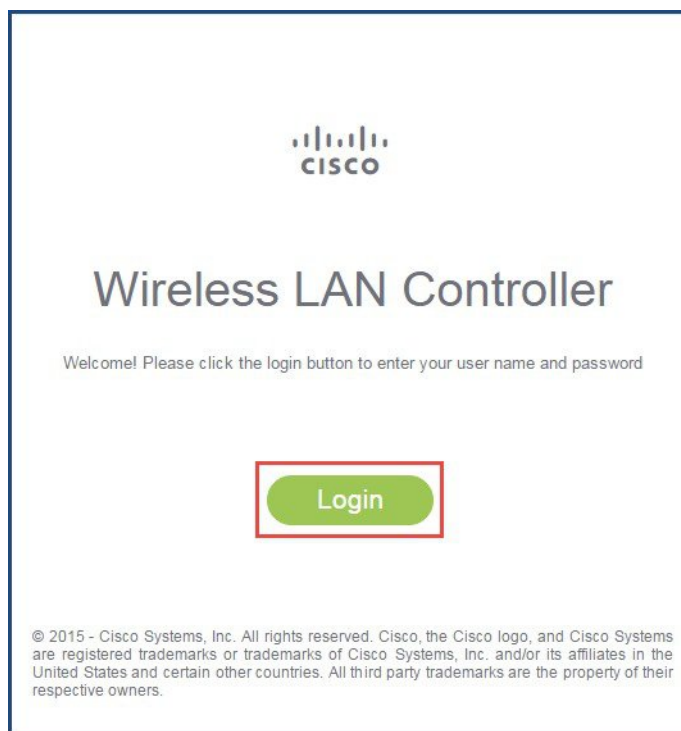
Note After the AP has finished rebooting, login to the Mobility Express controller WebUI using the Management IP address.

Logging into Mobility Express

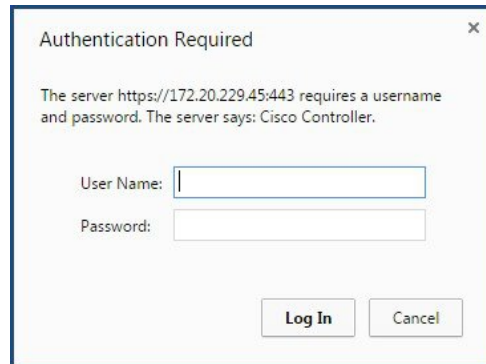
To log in to the Mobility Express, perform the following steps:

Procedure

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



Step 2 Click **Login**.



Authentication Required

The server https://172.20.229.45:443 requires a username and password. The server says: Cisco Controller.

User Name:

Password:

Step 3 Enter the administrator user name and password.

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

The Network Summary page appears.



CHAPTER 4

Monitoring Mobility Express Network

- [Viewing Network Summary](#) , on page 21
- [Viewing Wireless Dashboard](#), on page 26
- [Best Practices](#), on page 28

Viewing Network Summary

The Monitoring service enables the primary AP to monitor the Cisco Mobility Express network.

Monitoring Dashboard

The monitoring dashboard of the Network Summary page displays count of the following:

1. Wireless Networks
2. Access Points
3. Active Clients in 2.4 GHz and 5GHz
4. Rogues AP and Clients
5. Interferers



Note Rogues and interferers are not clickable link. Only the count is displayed.

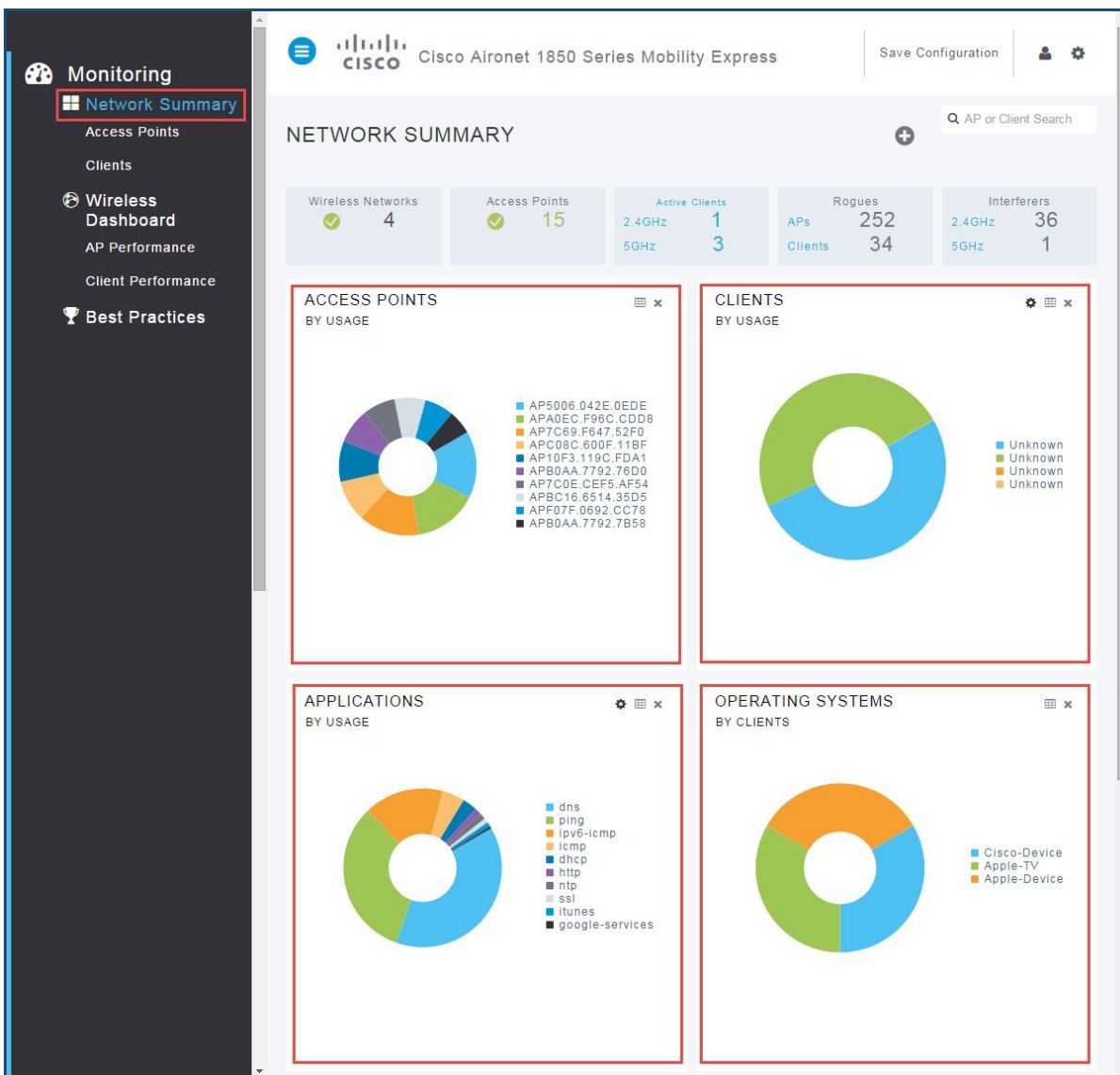
Wireless Networks		Access Points		Active Clients		Rogues		Interferers	
✓	4	✓	15	2.4GHz	1	APs	261	2.4GHz	33
				5GHz	2	Clients	29	5GHz	1

The Network Summary page has five customizable widgets representing data in both tabular and graphical formats for the following:

1. Access Points (by usage)
2. Clients (by usage)
3. Applications (by usage)
4. Operating System (by clients)
5. Top WLANs (by usage)



Note The widgets under Network Summary shows aggregate data for the wireless network.



View Access Points Summary using GUI

To view access points using GUI, perform the following steps:

Procedure

- Step 1** Click **Monitoring > Network Summary > Access Points**.
A table displays the list of Access Points.
- Step 2** Toggle between 2.4 GHz and 5 GHz tabs to view a list of the access points operating at respective radio frequencies.
- Step 3** (Optional) Click the down 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 fields or to filter the table view based on desired parameters.

The screenshot shows the Cisco GUI for monitoring access points. The left sidebar contains navigation options: Monitoring, Network Summary (with Access Points selected), Clients, Wireless Dashboard, AP Performance, Client Performance, and Best Practices. The main content area displays the 'ACCESS POINTS' table for a Cisco Aironet 1850 Series Mobility Express. The table has columns for AP Name, IP Address, Model, Clients, Usage, Throughput, and Channels. A dropdown menu is open over the 'Clients' column header, showing options for 'Sort Ascending', 'Sort Descending', 'Columns', and 'Filter'. The table lists 15 access points with their respective IP addresses, models, and usage statistics.

AP Name	IP Address	Model	Clients	Usage	Throughput	Channels
APB0AA.7792.7570	172.20.229.40	AIR-AP1852E-B-K9	0			(44,48)
AP10F3.119C.FDA1	172.20.229.23	AIR-CAP2602I-A-K9	0			(36,40)
AP5006.042E.0EDE	172.20.229.24	AIR-CAP702I-A-K9	0			(161,157)
APC08C.600F.11BF	172.20.229.56	AIR-CAP3602E-A-K9	0			(44,48)
APF07F.0692.CC78	172.20.229.55	AIR-CAP2702I-A-K9	0			(64,60)
AP7C0E.CEF5.AF54	172.20.229.54	AIR-CAP1702I-A-K9	0			(44,48)
APBC16.6514.35D5	172.20.229.53	AIR-CAP1602I-A-K9	1			(36,40)
AP7C69.F647.52F0	172.20.229.61	AIR-CAP702W-A-K9	0	12 GB	145 Kbps	(44,48)
APA0EC.F96C.CDD8	172.20.229.57	AIR-AP1852I-A-K9	0	12 GB	673 Kbps	(56,52)
APA0EC.F96C.D5E8	172.20.229.58	AIR-AP1852E-A-K9	0	1 GB	194 Kbps	(161,157)
APB0AA.7792.76D0	172.20.229.46	AIR-AP1852I-UXX9	0	5 GB	669 Kbps	(56,52)
APB0AA.7792.7828	172.20.229.50	AIR-AP1832I-B-K9	1	317 MB	48 Kbps	(149,153)
APB0AA.7792.7958	172.20.229.21	AIR-AP1832I-B-K9	0	3 GB	686 Kbps	(36,40)
APB0AA.7792.7B58	172.20.229.22	AIR-AP1832I-B-K9	0	3 GB	906 Kbps	(64,60)
APB0AA.7792.7838	172.20.229.28	AIR-AP1832I-B-K9	0	2 GB	767 Kbps	(161,157)

View Access Points Summary using CLI

To view access point summary using CLI, perform the following steps:

Procedure

Enter the following command to display a summary of all access points associated to the primary AP:

```
show ap summary
```

View Access Point Details using GUI

```
(Cisco Controller) >show ap summary
```

Number of Aps..... 15

Global AP User Name..... Not Configured

Global AP Dot1x User Name..... Not Configured

AP Name	Slots	AP Model	Ethernet MAC	Location	Country	IP Address	Clients	DSE Location
APB0AA.7792.7570	2	AIR-API1852E-B-K9	b0:aa:77:92:75:70	default location	US	172.20.229.40	0	[0,0,0]
AP10F3.119C.FDA1	2	AIR-CAP2602I-A-K9	10:f3:11:9c:fd:a1	CONF ROOM MARS	US	172.20.229.23	0	[0,0,0]
AP5006.042E.0EDE	2	AIR-CAP702I-A-K9	50:06:04:2e:0e:de	RESTROOM	US	172.20.229.24	0	[0,0,0]
APC08C.600F.11BF	2	AIR-CAP3602E-A-K9	c0:8c:60:0f:11:bf	CONF ROOM SATURN	US	172.20.229.56	1	[0,0,0]
APF07F.0692.CC78	2	AIR-CAP2702I-A-K9	f0:7f:06:92:cc:78	STORE ROOM	US	172.20.229.55	0	[0,0,0]
AP7C0E.CEF5.AF54	2	AIR-CAP1702I-A-K9	7c:0e:ce:f5:af:54	CONF ROOM PLUTO	US	172.20.229.54	0	[0,0,0]
APBC16.6514.35D5	2	AIR-CAP1602I-A-K9	bc:16:65:14:35:d5	LAB	US	172.20.229.53	2	[0,0,0]
AP7C69.F647.52F0	2	AIR-CAP702W-A-K9	7c:69:f6:47:52:f0	BREAK ROOM	US	172.20.229.61	0	[0,0,0]
APA0EC.F96C.CDD8	2	AIR-API1852I-A-K9	a0:ec:f9:6c:cd:d8	MAIN OFFICE	US	172.20.229.57	0	[0,0,0]
APA0EC.F96C.D5E8	2	AIR-API1852E-A-K9	a0:ec:f9:6c:d5:e8	MAIN OFFICE	US	172.20.229.58	0	[0,0,0]
APB0AA.7792.76D0	2	AIR-API1852I-UXK9	b0:aa:77:92:76:d0	CONF ROOM NEPTUN	US	172.20.229.46	0	[0,0,0]
APB0AA.7792.7828	2	AIR-API1832I-B-K9	b0:aa:77:92:78:28	default location	US	172.20.229.50	0	[0,0,0]
APB0AA.7792.7958	2	AIR-API1832I-B-K9	b0:aa:77:92:79:58	default location	US	172.20.229.21	1	[0,0,0]
APB0AA.7792.7B58	2	AIR-API1832I-B-K9	b0:aa:77:92:7b:58	default location	US	172.20.229.22	0	[0,0,0]

View Access Point Details using GUI

To view access point details using GUI, perform the following steps:

Procedure

Step 1

Click on any of the Access Points from the list to see detailed information about the AP. The default tab is the RF Troubleshoot tab, displays the following information:

- a. General AP Parameters
- b. Performance Summary of the two radios (2.4 GHz and 5 GHz)
- c. Neighbor and Rogue APs
- d. Clean Air Interferers
- e. Client Distribution by Usage
- f. Client Distribution by and Data Rates

The screenshot displays the Cisco Aironet 1850 Series Mobility Express web interface. The left sidebar contains navigation options: Monitoring, Network Summary, Access Points (highlighted), Clients, Wireless Dashboard, AP Performance, Client Performance, and Best Practices. The main content area is titled 'ACCESS POINT VIEW' and features a search bar for 'AP or Client Search'. The interface is divided into four main panels:

- GENERAL:** Displays AP Name (APF07F.0692.CC78), Location (STORE ROOM), MAC Address (f0.7f.06.92:cc:78), IP Address (172.20.229.55), CDP / LLDP, Model / Domain (AIR-CAP2702I-A-K9 / 802.11bg-A 802.11a-A), Serial Number (FTX1840R2XD), and Max Capabilities (802.11n 2.4GHz 5GHz, Spatial Streams: 3(2.4GHz), 3(5.0GHz), Max. Data Rate: 450Mbps(2.4GHz), 1300Mbps(5.0GHz)).
- PERFORMANCE SUMMARY:** Compares metrics for 2.4GHz (Ch 6) and 5GHz (Ch 60,64). Metrics include Number of clients (0), Configured Rate (Min: 9 Mbps, Max: 217 Mbps for 2.4GHz; Min: 6 Mbps, Max: 600 Mbps for 5GHz), Usage (11 GB vs 1 GB), Throughput (499 Kbps vs 15 Kbps), Transmit Power (1 dBm vs 11 dBm), Noise (-89 vs -94, -97), Channel Utilization (41% vs 10%), Interference (41% vs 10%), Traffic (0% vs 0%), Air Quality (97 vs 94, 99), and Admin Status (Enable).
- APF07F.0692.CC78 DETAILS:** Includes tabs for CLIENTS and RF TROUBLESHOOT. The RF TROUBLESHOOT tab has buttons for 2.4GHz and 5GHz. It contains two graphs: 'NEIGHBOR AND ROGUE APS' showing RSSI (dBm) vs Channel (1-11) for AP Channels, neighbor, and rogue; and 'CLEAN AIR INTERFERERS' showing Severity vs Channel (1-11) for AP Channels and interferer.
- TOOLS:** A section for performing actions on the AP.

Step 2 Click **Tools** to restart the AP or clear the AP configuration.

View Access Point Details using CLI

To view access points using CLI, perform the following steps:

Procedure

Step 1 Enter the following command to view the access points:

```
show ap <option>
```

Step 2 Enter the following command to restart the AP:

```
(Cisco Controller) >config ap reset <Cisco AP>
```

View Client Summary using GUI

To view client summary using GUI, perform the following steps:

Procedure

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

Step 2 (Optional) Click the down 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 fields or to filter the table view based on desired parameters.

View Client Summary using CLI

To view client summary using CLI, perform the following steps:

Procedure

Enter the following command to display a summary of all access points attached to the Mobility Express network:

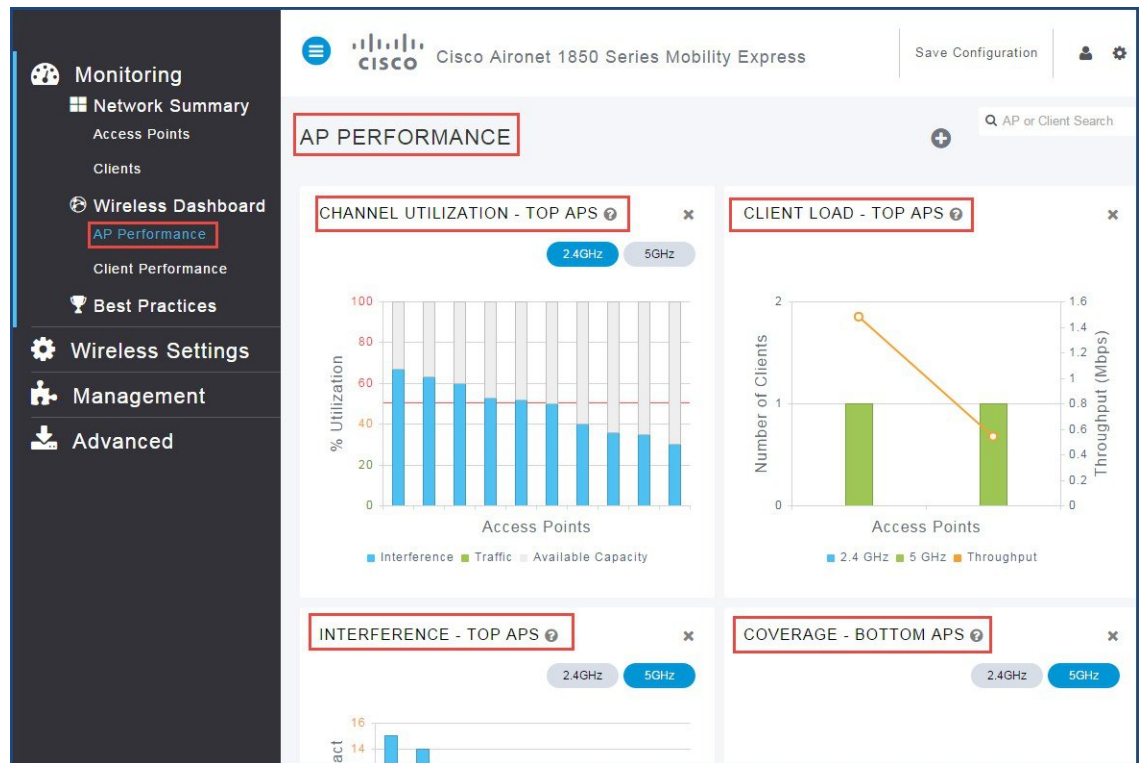
```
show client summary
```

Viewing Wireless Dashboard

The Wireless Dashboard provides details of AP and client performance.

Viewing AP Performance

The AP Performance dashboard helps the user to identify and troubleshoot the issues in the Mobility Express.



To access AP Performance dashboard, choose **Monitoring** > **AP Performance**.

The AP Performance dashboard displays the following charts:

- **Channel Utilization Top APs**—Level of traffic including data and interference over the channel that is assigned on the AP. Interference includes both Wi-Fi and non Wi-Fi signals. High utilization of channel, for example above 50%, suggests high level of interference including noise from nearby APs/clients/rogues on the same channel which results in poor client performance.
- **Client Load TOP APs**—Load indicator displays current number of connected clients on each access point. Higher load may impact performance, using client load balancing you can improve client distribution on the wireless network.
- **Interference Top APs**—RF interference involves unwanted, interference of RF signals that disrupt normal wireless operations, that creates potential network latency and poor client performance. Interfering RF signals includes both Wi-Fi and non Wi-Fi signals.
- **Coverage BOTTOM APs**—Coverage holes are areas where clients cannot receive a signal from the wireless network. A coverage hole is considered to have occurred when client SNRs falls below a predetermined level. A coverage hole event is when several clients are stuck in the same coverage hole.

Viewing Client Performance

The Client Performance dashboard helps the users to determine the cause of connection failure to the Mobility Express network and troubleshoot client related issues.

To access Client Performance dashboard, choose **Monitoring** > **Client Performance**.

The Client Performance dashboard displays the following charts:

- **Signal Strength**—Strong signal strength results in more reliable connections and higher speeds. Signal strength is represented in -dBm format, ranges from 0 to -100dBm. The closer the value to 0, the stronger the signal. Click to get a summary of clients.
- **Connection Rate**—Each client's throughput varies depending on the data rate used (802.11 a/b/n/ac) at any time, and this data rate may vary every second. Various factors such as RSSI values, RF interference, and so on, may affect a client device's instantaneous data rate.
- **Signal Quality**—Signal-to-noise ratio (SNR) is the power ratio between the signal strength and the noise level. This value is represented as a +dBm value. In general, you should have a minimum of +25dBm signal-to-noise ratio. Lower values than +25dBm result in poor performance and speed.
- **Client Connections**—Shows clients associated with the access points, of any connectivity types.

Best Practices

For more details on Best Practices, please refer: https://www-author.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/1/best_practices/b_ME_Best_Practices_Guide.html



CHAPTER 5

Managing Wireless Settings

The Wireless Settings tab helps you to manage WLANs, Access Points, WLAN Users and Guest WLANs.

- [WLANs, on page 29](#)
- [Access Points, on page 35](#)
- [WLAN Users, on page 39](#)
- [Guest WLANs, on page 40](#)

WLANs

The Cisco Mobility Express solution can control up to 16 WLANs for lightweight access points. Each WLAN has a WLAN ID (1 through 16), a Profile Name, a WLAN SSID, and can be assigned with unique security types.



Note Management traffic is untagged and we recommend you to assign one VLAN for Management and another set of VLANs for client.

Creating WLANs using GUI

To create a WLAN using GUI, perform the following steps:

Procedure

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

	Active	Name	Security Policy	Radio Policy
<input checked="" type="checkbox"/> ✕	Enabled	Employee-PSK	WPA2Personal	ALL
<input checked="" type="checkbox"/> ✕	Enabled	Guest-PSK	WPA2Personal	ALL
<input checked="" type="checkbox"/> ✕	Enabled	Guest-Email	Guest	ALL

The WLAN configuration page appears displaying the count of Active WLANs.

Step 2 Click **Add New WLAN**. The Add New WLAN window appears.

Step 3 In the **General** tab, perform the following:

- a) The **WLAN Id** is automatically selected but you can change it.
- b) Enter the **Profile Name** for the WLAN.
- c) Enter the **SSID**.
- d) Choose **Admin State** for the WLAN from the drop-down list. The default Admin State is Enabled.
- e) Choose **Radio Policy** from the drop-down list. The default Radio Policy is ALL.

Step 4 In the **WLAN Security** tab, perform the following:

Choose the **Security** type from the drop-down list. The supported security types for WLAN are:

The default **Security** is WPA2 Enterprise with **Authentication Server** as External Radius.

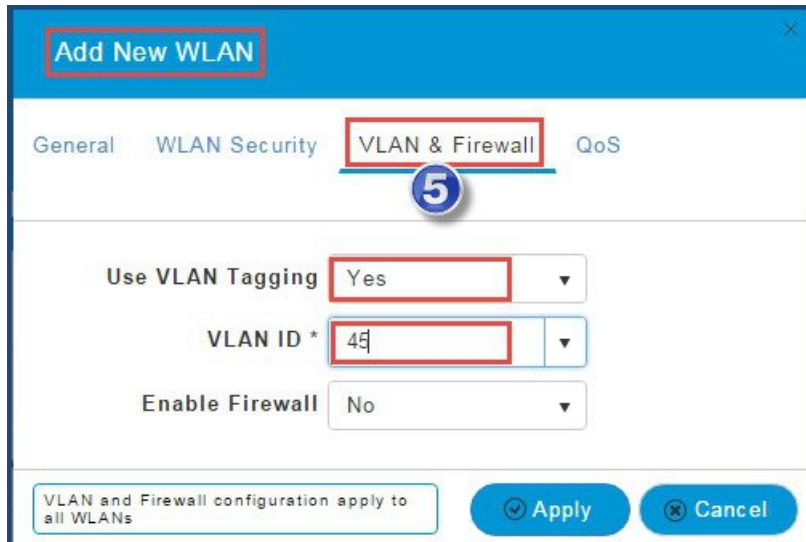
- **WPA2 Enterprise**—Means Wi-Fi Protected Access 2 with a with a local authentication server or RADIUS server.
 - a. **Local Authentication (AP)**—The default option is to have a local authentication method (choose AP in the Authentication Server drop-down list). This option is a Local EAP authentication method that allows users and wireless clients to authenticate locally. The Mobility Express controller serves as the authentication server using the local user database, thus removing dependence on an external authentication server.
 - b. To have a RADIUS server-based authentication method, choose **External Radius** in the Authentication Server drop-down list. Remote Authentication Dial-In User Service (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.

The screenshot shows the 'Add New WLAN' configuration window. The 'WLAN Security' tab is active. The 'Security' dropdown is set to 'WPA2 Enterprise' and the 'Authentication Server' dropdown is set to 'External Radius'. Below these, there is a table with columns for 'Radius IP', 'Radius Port', and 'Shared Secret'. A single row is visible with a checked checkbox in the first column, an empty 'Radius IP' field, '1812' in the 'Radius Port' field, and an empty 'Shared Secret' field. At the bottom, a message states 'External Radius configuration applies to all WLANs' and there are 'Apply' and 'Cancel' buttons.

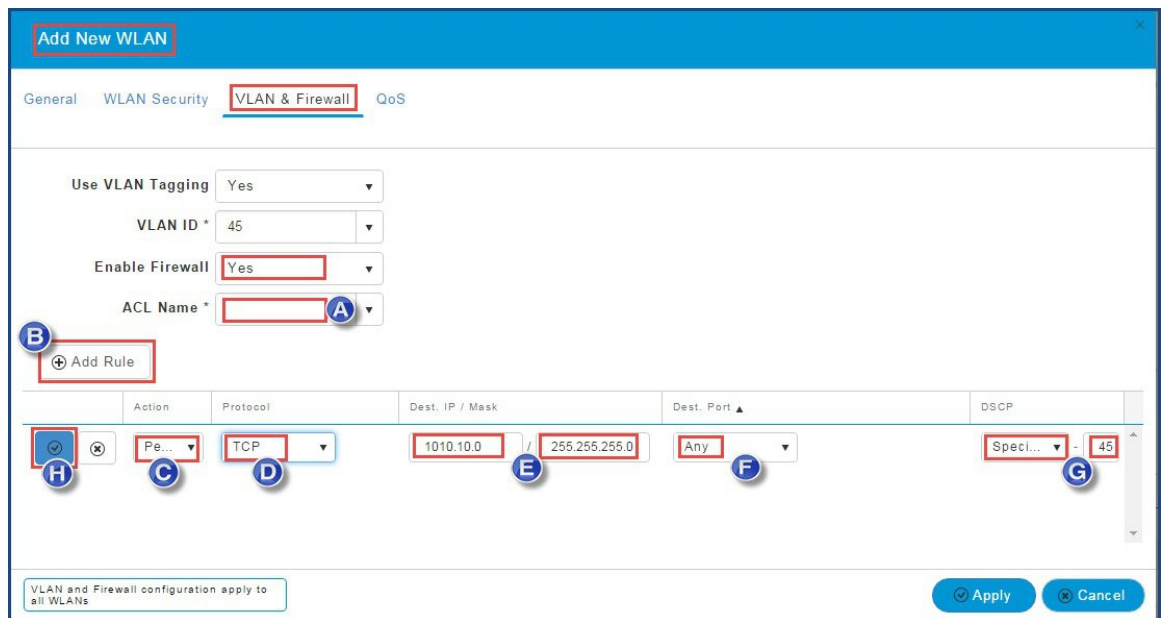
- **Guest**—The controller can provide guest user access on WLANs which are specifically designated for guest users. To set this WLAN exclusively for guest user access, choose the Security as Guest. You can set the authentication for guest users by choosing one of the following options in the Guest **Authentication** drop-down list:
 - a. **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**.
 - b. **Display Terms and Conditions**—Choose this option to allow guest access to the WLAN upon acceptance of displayed terms and conditions. This option allows guest users to access the WLAN without entering a username and password.
 - c. **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 is provided. This option allows guest users to access the WLAN without entering a username and password.
- **Open**—Open authentication allows any device to authenticate and then attempt to communicate with the access point. Using open authentication, any wireless device can authenticate with the access point.
- **WPA2 Personal**—This option stands for Wi-Fi Protected Access 2 with Pre-Shared Key (PSK). WPA2 Personal is a method of securing your network with the use of a PSK authentication. The PSK is configured separately both on the controller AP, under WLAN security policy, and on the client. WPA2 Personal does not rely on an authentication server on your network. This is used when you do not have an enterprise authentication server. If you choose this option, then specify the PSK in the Shared Key field.

Step 5 In the **VLAN & Firewall** tab, perform the following:

- a) **Use VLAN Tagging**—The default is **No**. If **Yes** is selected, enter the **VLAN ID**. By enabling VLAN Tagging, the chosen VLAN ID is inserted into a packet header in order to identify which VLAN 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.



b) **Enable Firewall**—The default is **No**. If **Yes** is selected, enter the following information:



	Field Name	Description
A	ACL Name	Enter the name for the new ACL. You can enter up to 32 alphanumeric characters. The ACL name must be unique.
B	Add Rule	To set rules for the ACL, click Add Rule . Note The ACL rules are applied to the VLAN. Multiple WLANs can use the same VLAN, hence inheriting ACL rules, if any.

	Field Name	Description
C	Action	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.
D	Protocol	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: <ul style="list-style-type: none"> • 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.
E	Dest. IP / Mask	In the Dest. IP / Mask field, enter the IP address and netmask of the specific destination.
F	Dest. Port	If you have chosen TCP or UDP, you need to 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.
G	DSCP	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. <ul style="list-style-type: none"> • Any—Any DSCP (this is the default value). • Specific—A specific DSCP, ranges from 0 to 63, which you can enter in the DSCP edit box.

Step 6 Click **Apply** to save ACL.

Step 7 In the **QoS** tab, perform the following:



- a) **QoS**—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, you can 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 and this is the default setting.
 - Bronze/Background—Provides the lowest bandwidth for guest services.
- b) **Application Visibility**—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. Application Visibility is enabled by default on WLANs. Protocol Pack version 13.0 and Engine version 16.0 is supported.

Step 8 Click **Apply**.

Access Points

Managing Access Point using GUI

To manage the access points that are associated with the Mobility Express controller using GUI, perform the following steps:

Procedure

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

The Access Point Administration page displays the count of access points and Access Point table with the associated APs.

Note The AP table displays the first 10 APs on first page and the other APs on the next page.

Manage	Location	Name	IP Address	AP Mac	Up Time	AP Model
	MAIN OFFICE	APA0EC.F96...	172.20.229.44	a0:ec:f9:6c:...	14 days, 07 ...	AIR-AP18521...
	default locat...	APB0AA.779...	172.20.229.49	b0:aa:77:92:...	8 days, 06 h...	AIR-AP18321...
	RESTROOM	AP5006.042...	172.20.228.45	50:06:04:2e:...	14 days, 05 ...	AIR-CAP702...
	MAIN OFFICE	APA0EC.F96...	172.20.229.37	a0:ec:f9:6c:...	9 days, 10 h...	AIR-AP1852...
	BREAK ROOM	AP7C69.F64...	172.20.229.47	7c:69:f6:47:...	14 days, 04 ...	AIR-CAP702...

The primary AP and Subordinate AP icons are as shown:

Figure 7: Primary AP Icon



Figure 8: Subordinate AP Icon



Step 2 Click Edit.

The Edit window displaying general parameters of access point appears.

The General tab displays the following AP parameters:

- **Operating Mode**(Read only field)—For a primary AP, this field displays *AP & Controller*. For other associated APs, this field displays *AP only*.
- **AP Mac**(Read only field)—Displays the MAC address of the Access Point.
- **AP Model**(Read only field)—Displays the model details of the Access Point.

- **IP Configuration**—Choose **Obtain from DHCP** to allow the IP address of the AP be assigned by a DHCP server on the network, or choose **Static IP** address. If you choose Static IP address, then you can edit the *IP Address*, *Subnet Mask*, and *Gateway* fields.
- **AP Name**—Edit the name of access point. This is a free text field.
- **Location**—Edit the location for the access point. This is a free text field.

The screenshot shows the 'Edit' configuration window for an access point. The 'General' tab is selected, and the 'Controller' option is active. The 'IP Configuration' dropdown is set to 'Obtain from DHCP'. The 'IP Address' field contains '172.20.229.57', 'Subnet Mask' is '255.255.255.192', and 'Gateway' is '172.20.229.2'. The 'AP Name' field contains 'APA0EC.F96C.CDD8' and 'Location' is 'MAIN OFFICE'. The 'Operating Mode' is 'AP & Controller', 'AP Mac' is 'a0:ec:f9:6c:cd:d8', and 'AP Model' is 'AIR-AP1852I-A-K9'. The 'Apply' and 'Cancel' buttons are at the bottom right.

Step 3 Click **Controller** to edit the following parameters for the Mobility Express controller:

Note The Controller option is available only for primary AP.

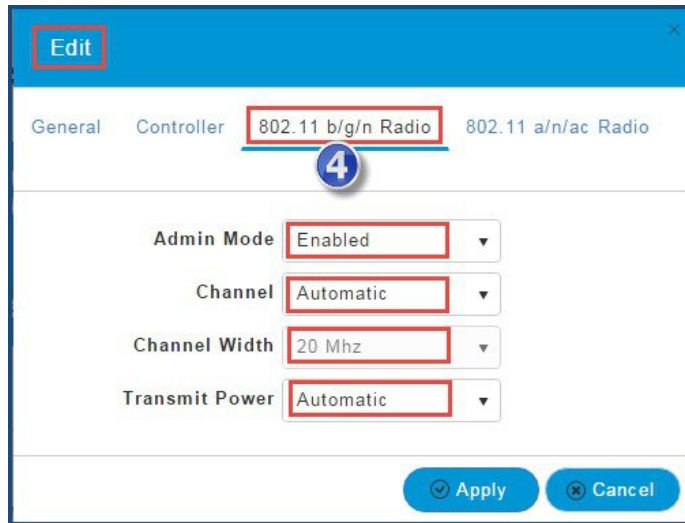
- **IP Address**—IP address decides the login URL to the controller's web interface. The URL is in *https://<ip address>* format. If you change this IP address, the login URL also changes.
- **Subnet Mask**
- **Country Code**

Step 4 Click **802.11 b/g/n Radio** and **802.11 a/n/ac Radio** to edit the following parameters:

- **Admin Mode**—Choose **Enabled** from the Admin drop-down list to enable the corresponding radio on the AP (2.4 GHz for 802.11 b/g/n or 5 GHz for 802.11 a/n/ac).
- **Channel**—**Automatic** is set as default channel. This enables dynamic channel assignment, such that the channels are dynamically assigned to each AP, under the control of the Mobility Express controller. This prevents neighboring APs from broadcasting over the same channel and hence prevents interference and other communication problems. For the 2.4 GHz radio, 11 channels are offered in the US, up to 14 in other parts of the world, but only 1-6-11 can be considered non-overlapping if they are used by neighboring APs. For the 5 GHz radio, up to 23 non-overlapping channels are offered. Assigning a specific value statically assigns a channel to that AP.
 - 802.11 b/g/n - 1 to 11
 - 802.11 a/n/ac - 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 165
- **Channel Width**—Set as 20 MHz for 2.4 GHz and 20, 40 and 80 MHz for 5 GHz.
- **Transmit Power**—1 to 8. The default value is **Automatic**.

This is a logarithmic scale of the transmit power, the transmission energy used by the AP, 1 being the highest, 2 being half of it, 3 being 1/4th and so on.

Selecting **Automatic** adjusts the radio transmitter output power based on the varying signal level at the receiver. This allows the transmitter to operate at less than maximum power for most of the time; when fading conditions occur, transmit power increases as needed until the maximum power is reached.



Step 5 Click **Apply** to save the changes.

WLAN Users

A wireless client needs to connect to a WLAN in the network. To connect to a WLAN, the wireless client enters the user credentials. If the WLAN uses WPA2-Personal as a security policy, then the user must provide the appropriate WPA2-PSK details for that WLAN. If the Security Policy is set to WPA2-Enterprise, then the user must provide a valid user identity and its corresponding password in the RADIUS user database. For local authentication, provide the valid user identity and its corresponding password in the RADIUS user database.

The WLAN Users page lists all WLAN users in the network. The WLAN Users page also displays the following information for each user:

Table 6: WLAN Users—Field and Description

Field	Description
User name	Specifies the name of the WLAN user.
Guest user	Specifies the type of WLAN user. Check this checkbox if the WLAN user is guest. Guest user account is limited with validity of 86400 seconds (or, 24 hours) from the time of its creation.
WLAN Profile	Specifies the WLANs to which the user can connect.
Password	Specifies the password of the WLAN user.
Description	Specifies the additional details or comments about the user.

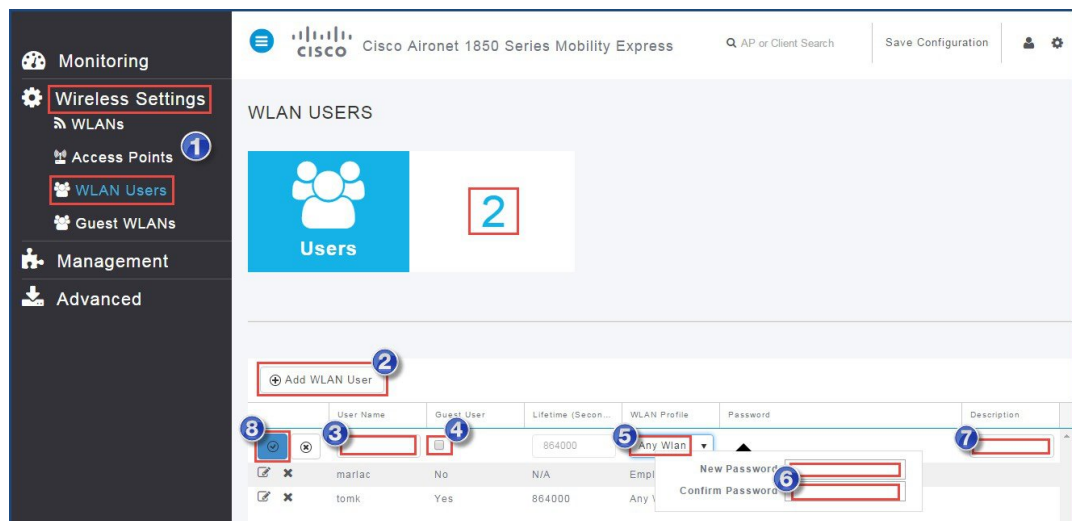
Creating a WLAN User using GUI

To add a local EAP user, perform the following steps:

Procedure

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

The WLAN Users page appears displaying the count of the users that are configured on the Mobility Express controller.



Step 2 Click **Add WLAN User** to create a WLAN user.

Step 3 Enter the **User Name** for the WLAN user.

Note User names are case-sensitive and can contain up to 24 ASCII characters. User names must not contain space.

Step 4 If the user is a Guest WLAN user, check the **Guest User** checkbox.

Step 5 From the drop down list, choose the **WLAN Profile** of the user.

Step 6 Enter a password and re-enter confirm password for the new WLAN User.

Step 7 Enter a description for the WLAN User.

Step 8 Click **Apply**.

Guest WLANs

Creating WLAN using GUI

To create a customized login page for guest WLANs, perform the following steps:



Note A Guest WLAN must be setup for Guest Users.

Procedure

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

The Guest WLAN page appears displaying the count of Guest WLANs that are configured on the Mobility Express controller.

The screenshot shows the Cisco Mobility Express GUI for configuring Guest WLANs. The left sidebar has a menu with 'Guest WLANs' highlighted. The main content area is titled 'GUEST WLAN' and shows a status of 'Enabled' with a count of '1'. Below this are four configuration fields, each with a red border: 'Display Cisco Logo' is a dropdown menu set to 'Yes (Default)'; 'Redirect URL After Login' is a text input field containing 'http://www.cisco.com'; 'Page Headline' is a text input field containing 'Welcome to Guest Portal'; and 'Page Message' is a text input field containing 'Powered by Cisco Mobility Express'. At the bottom of the form is a green 'Apply' button.

Step 2 From the **Display Cisco Logo** drop-down list, choose **Yes (Default)** to display Cisco logo.

You can choose **No**. However, you do not have an option to display any other logo of your choice. This field is set as Yes by default.

Step 3 Enter the desired URL in **Redirect URL After Login** field. The guest user is redirected to the specified URL (such as the URL of your company) after login.

You can enter up to 254 characters.

Step 4 Enter the headline that needs to be displayed when logged in **Page Headline** field.

You can enter up to 127 characters. The default headline is *Welcome to the Cisco Wireless Network*.

Step 5 Enter the message that needs to be displayed when logged in **Page Message** field.

You can enter up to 2047 characters. The default message is *Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.*

Step 6 Click **Apply**.



CHAPTER 6

Managing Mobility Express Network

Using the Management tab, the admin users can perform the following:

- Configure access to the Mobility Express controller
- Manage admin accounts
- Configure time
- Perform a software update
- [Management Access, on page 43](#)
- [Managing Administrator Accounts, on page 45](#)
- [Managing Time on Mobility Express Controller, on page 49](#)
- [Updating Cisco Mobility Express Software, on page 53](#)

Management Access

Configuring Management Access using GUI

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

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

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

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

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

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

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

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

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

To enable or disable the different types of management access on the controller, perform the following steps:

Procedure

Step 1

Click **Management > Access**.

The Management Access page appears displaying the count of the access type which are enabled.

Step 2

For the various Access Types, choose either as **Enabled** or **Disabled**.

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

Step 3

Click **Apply**.

Configuring Management Access using CLI

To configure the management access using CLI, enter the following commands:

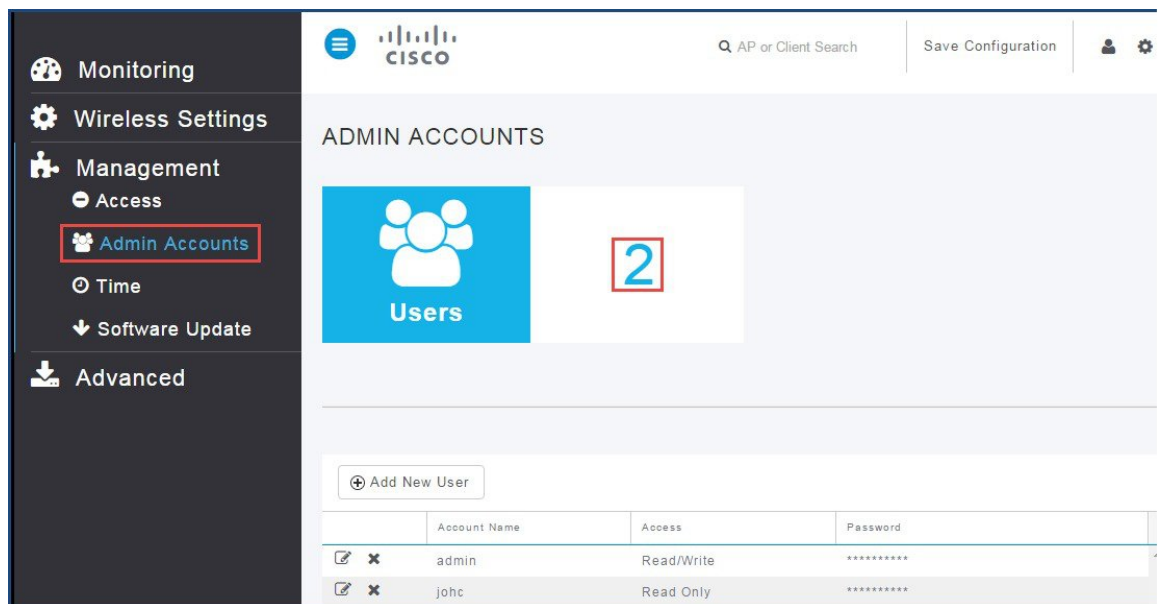
- (Cisco Controller) >config network webmode <enable | disable>
- (Cisco Controller) >config network secureweb <enable | disable>
- (Cisco Controller) >config network ssh <enable | disable>
- (Cisco Controller) >config network telnet <enable | disable>

Managing Administrator Accounts

You can configure admin usernames and passwords to prevent unauthorized users from reconfiguring the controller and viewing configuration information.

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

- Choose **Management > Admin Accounts**.
- The Admin Accounts page appears displaying the count of administrator accounts on the controller and list of all administrator accounts available on the Cisco Mobility Express controller.



The screenshot displays the Cisco Mobility Express GUI. On the left, a dark sidebar contains navigation options: Monitoring, Wireless Settings, Management (with sub-options Access, Admin Accounts, Time, Software Update), and Advanced. The 'Admin Accounts' option is highlighted with a red box. The main content area is titled 'ADMIN ACCOUNTS' and features a blue 'Users' icon with a red-bordered box containing the number '2'. Below this is an 'Add New User' button and a table of existing accounts.

	Account Name	Access	Password
<input checked="" type="checkbox"/> <input type="checkbox"/>	admin	Read/Write	*****
<input checked="" type="checkbox"/> <input type="checkbox"/>	johc	Read Only	*****

Creating an Admin Account using GUI

To create an admin account using GUI, perform the following steps:

	Account Name	Access	Password
<input checked="" type="checkbox"/>		Read/Write	
<input checked="" type="checkbox"/>	admin	Read/Write	
<input checked="" type="checkbox"/>	johc	Read Only	

New Password

Confirm Password

Procedure

Step 1 Click **Add New User**.

Step 2 Enter the admin user name in the **Account Name** field.

Note Admin account name must be unique. It is case-sensitive and can contain up to 24 ASCII characters without spaces.

Step 3 Choose **Read/Write** or **Read Only** from Access drop-down list.

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

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

Step 4 Enter the new password for admin user account in the **New Password** field.

- a. Passwords are case sensitive and cannot contain space.
- b. The password must contain a minimum of 8 characters from ALL of the following classes:
 1. Lowercase letters
 2. Uppercase letters
 3. Digits
 4. Special characters.
- c. No character in the password can be repeated more than three times consecutively.
- d. The password must not contain the word Cisco or a management username. The password must also not be any variant of these words, obtained by reversing the letters of these words, or by changing the capitalization of letters, or by substituting 1, |, or ! or substituting 0 for o or substituting \$ for s.

Step 5 Re-enter the password in the **Confirm Password** field.

Step 6 Click **Apply** to the save changes.

Creating an Admin Account using CLI

To create an admin account using CLI, perform the following steps:

Procedure

Step 1 Log in to the Mobility Express controller CLI.

Step 2 Create admin user using the following CLI commands:

```
(Cisco Controller) >config mgmtuser add <username> <password> <read-only | read-write>
```

To view the list of all the admin accounts, use the CLI below

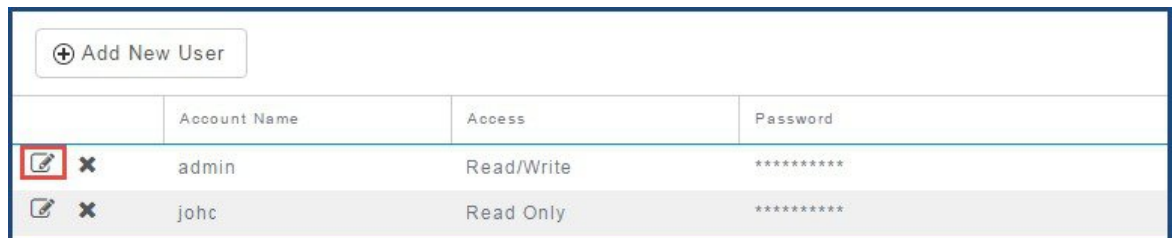
```
(Cisco Controller) >show mgmtuser
```





Editing an Admin Account using GUI

To edit an admin account using GUI, perform the following steps:

Procedure

Step 1 Click **Edit**.



	Account Name	Access	Password
 	admin	Read/Write	*****
 	johc	Read Only	*****

Step 2 Change password and click **Apply**.

Note Access cannot be changed for an admin account after creation, it can only be deleted and recreated.

+ Add New User			
	Account Name	Access	Password
	admin	Read/Write	*****
	johc	Read Only	*****

New Password

Confirm Password

Editing an Admin Account using CLI

To edit an admin account using CLI, perform the following steps:

Procedure

- Step 1** Log in to the Mobility Express controller CLI.
- Step 2** Edit an existing admin user account using the following command:
- ```
(Cisco Controller) >config mgmtuser password <username> <password>
```

**Note** Access cannot be changed for an admin account after creation, it can only be deleted and recreated.

## Deleting Admin Account using GUI

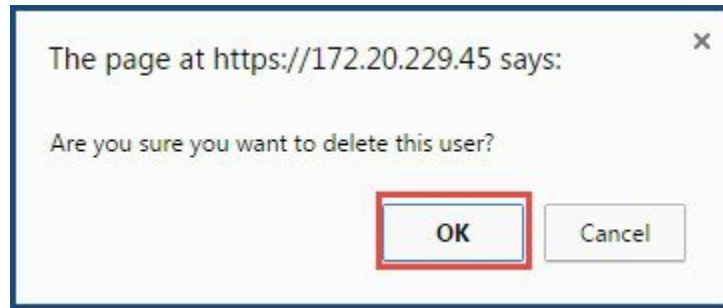
To delete an admin account using GUI, perform the following steps:

### Procedure

- Step 1** Click **Delete** in the GUI.

| + Add New User |              |            |          |
|----------------|--------------|------------|----------|
|                | Account Name | Access     | Password |
|                | admin        | Read/Write | *****    |
|                | johc         | Read Only  | *****    |

- Step 2** Click **OK** to confirm.



---

## Deleting Admin Account using CLI

To delete an admin account using CLI, perform the following steps:

### Procedure

---

- Step 1** Log in to the Mobility Express controller CLI.
- Step 2** Delete an existing admin user account using the following command:
- ```
(Cisco Controller) >config mgmtuser delete <username>
```
-

Managing Time on Mobility Express Controller

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

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

Configuring NTP Server on Mobility Express Controller using GUI

To configure an NTP server, perform the following steps:

Procedure

- Step 1** Choose **Management** > **Time** from the left pane.

The screenshot shows the 'TIME SETTINGS' configuration page for a Cisco Aironet 1850 Series Mobility Express controller. The left sidebar contains navigation options: Monitoring, Wireless Settings, Management (with sub-options Access, Admin Accounts, Time, and Software Update), and Advanced. The 'Time' option is highlighted. The main content area is titled 'TIME SETTINGS' and features a 'Time Zone' section with a clock icon and a dropdown menu currently set to '(GMT -8:00) Pacific Time (US and Canada)'. To the right of this dropdown is a checkbox labeled 'Set Time Automatically From Current Location'. Below the time zone section, there are several configuration fields: 'Set Time Manually *' with a date and time picker (09/05/2015 09:14 AM), 'NTP State' set to 'Enable', 'NTP Polling Interval' set to '3600' (seconds), and 'NTP Server' set to '10.10.10.50'. A green 'Apply' button is located at the bottom of the configuration area.

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

Note To change the Time zone; disable the NTP state, change the Time zone and enable the NTP state.

Step 3 Choose **Enable** from **NTP State** drop-down list.

Step 4 Enter the polling interval in seconds in the **NTP Polling Interval** field.

Note The polling interval ranges from 3600 to 604800 seconds.

Step 5 Enter the NTP server's IPv4 address in the **NTP Server** field

Step 6 Click Apply.

Note Synchronizing of the date and time with the NTP server occurs every moment when the controller reboots and at each user-defined polling interval.

Configuring NTP Server on Mobility Express Controller using CLI

To configure NTP server on Mobility Express Controller using CLI, perform the following steps:

Procedure

Step 1 Log in to the Mobility Express controller CLI.

Step 2 Configure an NTP server from CLI using the following commands:

```
(Cisco Controller) >config time ntp server <index> <NTP IP Address>
<index> 1 as only one NTP server is supported on Mobility Express controller

(Cisco Controller) >config time ntp interval <interval>
<interval> Enter NTP polling interval, between 3600 and 604800(in seconds).
```

Step 3 Configure the Time zone using anyone of the following commands:

```
(Cisco Controller) >config time timezone location <location_index>
```

```
(Cisco Controller) >config time timezone delta <delta_hours> <delta_min>  
<delta_hours> Enter the local hour difference from Universal Coordinated Time (UTC).  
<delta_mins> Enter the local minute difference from Universal Coordinated Time (UTC).
```

Step 4 View current date and time along with time setting using the following command:

```
(Cisco Controller) >show time
```

Configuring Date and Time Manually on Mobility Express Controller using GUI (Method I)

To configure date and time manually using GUI, perform the following steps:

Procedure

Step 1 Choose the desired Time Zone from the **Time Zone** drop down list.

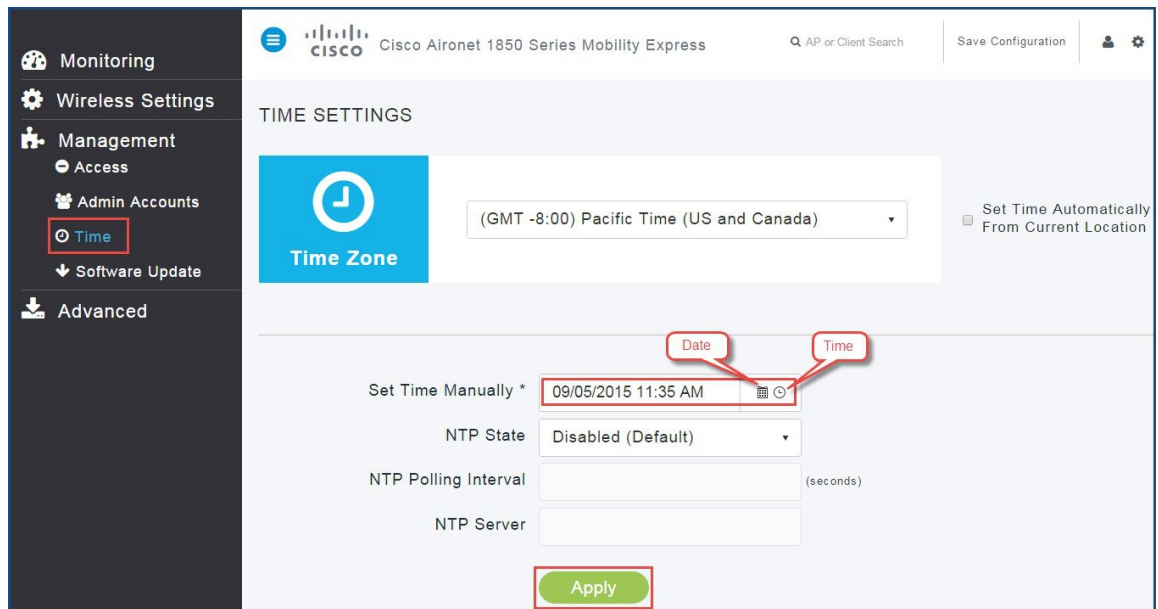
Step 2 Check the check box for **Set Time Automatically from Current Location** to set time based on the Time Zone.

The screenshot displays the Cisco Mobility Express GUI for a Cisco Aironet 1850 Series Mobility Express controller. The left sidebar shows the navigation menu with 'Time' highlighted. The main content area is titled 'TIME SETTINGS'. A blue 'Time Zone' section contains a dropdown menu set to '(GMT -8:00) Pacific Time (US and Canada)'. To the right of this dropdown is a checkbox labeled 'Set Time Automatically from Current Location', which is checked. Below this, the 'Set Time Manually' field is set to '09/17/2015 03:14 AM'. The 'NTP State' is set to 'Disabled (Default)'. The 'NTP Polling Interval' field is empty, with '(seconds)' indicated to its right. The 'NTP Server' field is also empty. A green 'Apply' button is located at the bottom of the configuration area.

Configuring Date and Time Manually on Mobility Express Controller using GUI (Method II)

Procedure

- Step 1** Click **Date** icon from **Set Time Manually** field and change the date.
- Step 2** Click **Time** icon from **Set Time Manual** and choose time from the drop down list.
- Step 3** Click **Apply**.



Configuring Date and Time Manually on Mobility Express Controller using CLI

To configure date and time manually using CLI, perform the following steps:

Procedure

- Step 1** Log in to the Mobility Express controller CLI.
- Step 2** Configure time manually using the following command:
- ```
(Cisco Controller) >config time manual <MM/DD/YY> <HH:MM:SS>
```
- Step 3** Configure the Time zone using one of the following commands:
- ```
(Cisco Controller) >config time timezone location <location_index>
(Cisco Controller) >config time timezone delta <delta_hours> <delta_min>
<delta_hours> Enter the local hour difference from Universal Coordinated Time (UTC).
<delta_mins> Enter the local minute difference from Universal Coordinated Time (UTC).
```

Step 4 View current date and time along with the time setting using the following command:

```
(Cisco Controller) >show time
```

Updating Cisco Mobility Express Software

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

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

Primary AP facilitates transfer of image from the TFTP server to the Subordinate APs. The AP images are stored and served from the TFTP server upon request.

Before you upgrade the Mobility Express network, ensure the following pre-requisites are met:

Pre-requisites for Software Update

1. A TFTP server is reachable from the management IP address of the Mobility Express controller.
2. The AP bundle with AP images downloaded from CCO is unzipped and copied into the TFTP server.

Software Update Sequence:

1. Download the **AIR-AP1850-K9-ME-<version>.zip** or **AIR-AP1830-K9-ME-<version>.zip** file from cisco.com on a device running TFTP server. Unzip the file to extract the AP images.
2. Configure TFTP parameters on the Software Update page.
3. Initiate image pre-download on Mobility Express network.
4. Reboot of or scheduled reboot of Mobility Express Controller and associated Access Points.



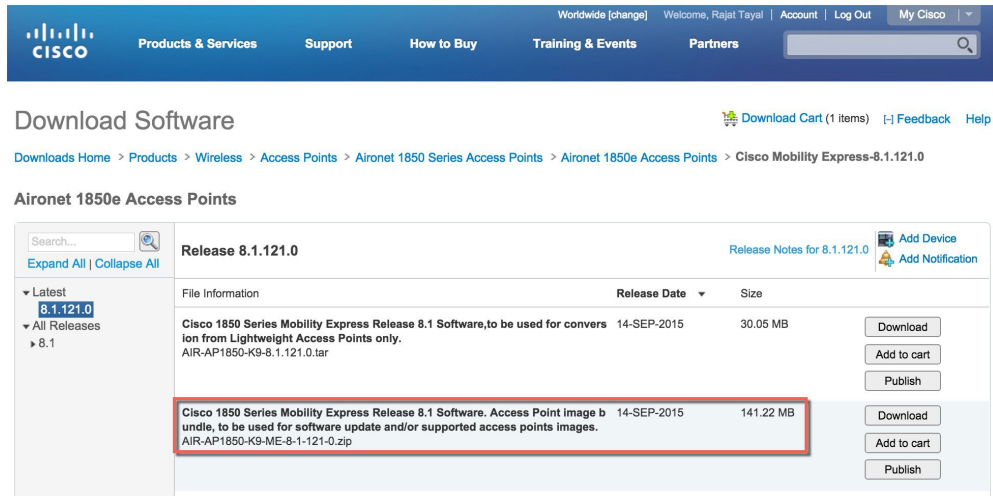
Note

- image pre-download on APs is automatically sequenced, such that not more than two APs are pre-download the image simultaneously.
- During the image pre-download there is no service interruption. After completion of the image pre-download on all APs, a manual or scheduled reboot of Mobility Express network must be triggered.

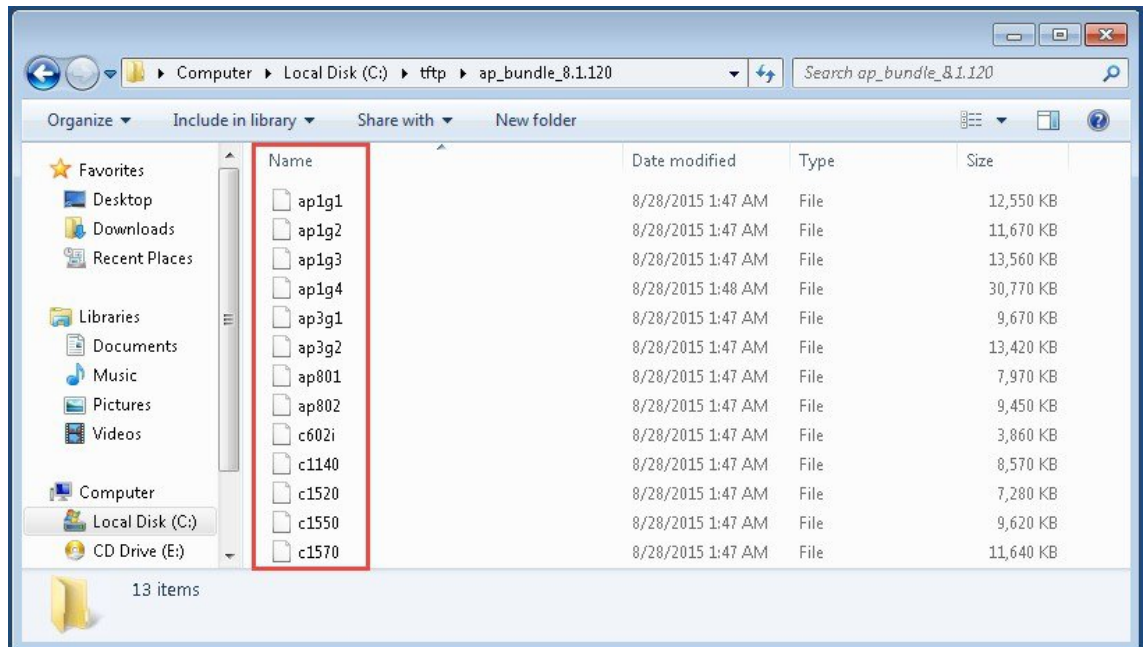
To begin Software Update, perform the following steps:

Procedure

Step 1 Download the **AIR-AP1850-K9-ME-<version>.zip** or **AIR-AP1830-K9-ME-<version>.zip** file from cisco.com to a machine running TFTP server.



Step 2 Unzip the AIR-AP1850-K9-ME-<version>.zip file to extract the AP images.

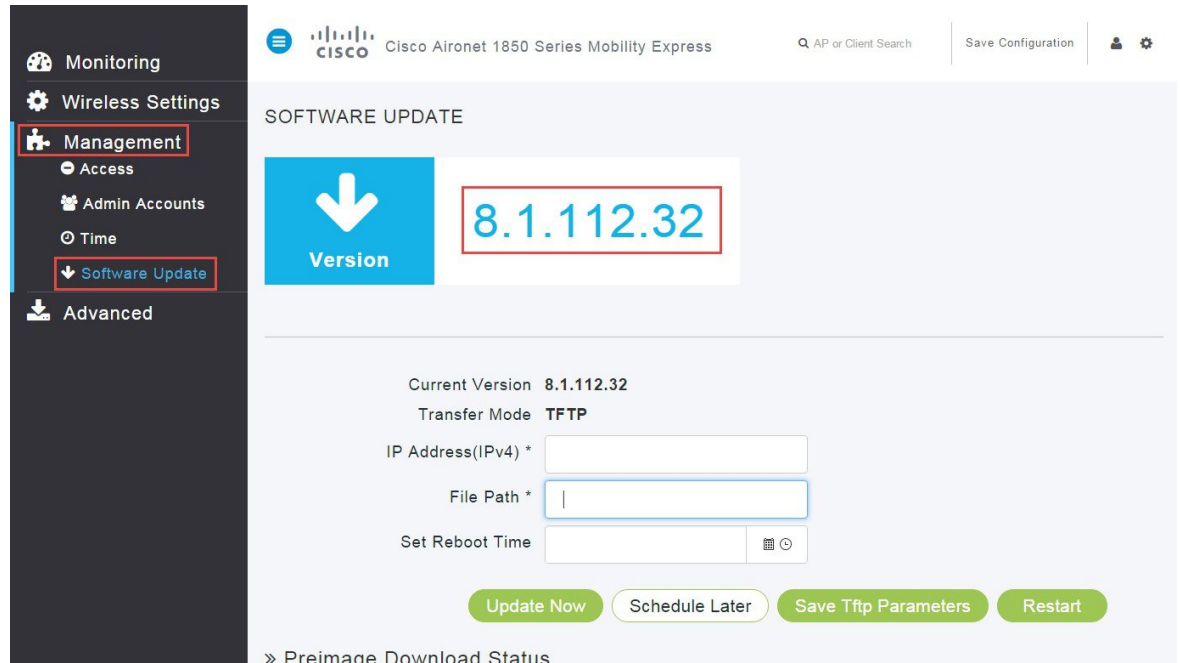


Updating Cisco Mobility Express network using GUI

To update the software using GUI, perform the following steps:

Procedure

Step 1 Log in to the Mobility Express user interface and choose **Management > Software Update**.



The system displays the current version of the Mobility Express.

Step 2 Enter the value in the **IP Address(IPv4)** field.

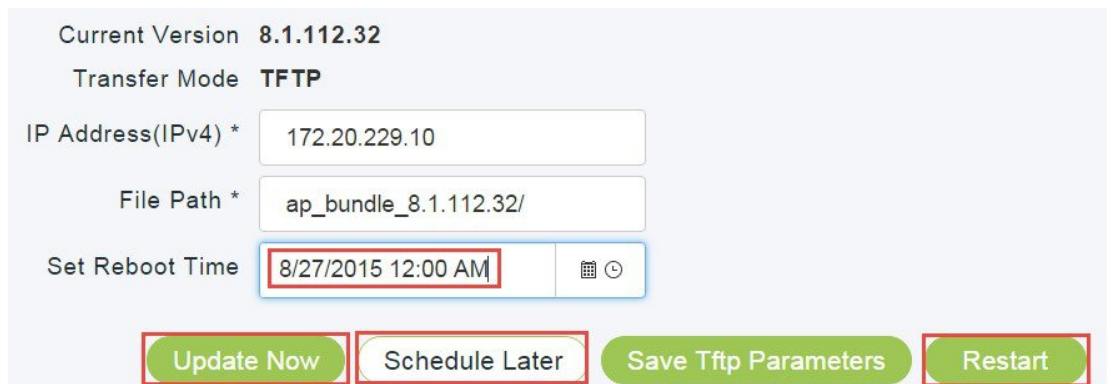
Note We recommend to have TFTP server in the same network as the management interface.

Step 3 Enter the **File Path** of the unzipped AP images.

Step 4 Click **Save Tftp Parameters**.

Step 5 To initiate the image pre-download, click **Update Now** or **Schedule Later**.

- **Update Now**—Initiates the image pre-download instantaneously. After image pre-download is complete on all APs, click **Restart** to manually reboot the APs. After the reboot, all APs will run the new image.
- **Schedule Later**—Initiates the image pre-download instantaneously. However, reboot of the APs happen at a scheduled time configured by the user in the **Set Reboot Time** field.



Step 6 Once the image pre-download starts, you can view the status by expanding **Preimage Download Status**.

Image pre-download involves different states, such as:

- a. **Predownloading**—The AP actively downloads an image on its flash during this state.
- b. **Initiated**—A image pre-download request is sent to the AP during this state.
- c. **BackedOff**—When image pre-download is initiated on two APs, the next two APs are identified and moved to Initiated state. After the image pre-download on the first two APs, APs which are in **Initiated** state are moved to **pre-downloading** state. If the **Initiated** state timer expires before the image pre-download is complete on the first set of the APs, the APs in **Initiated** state are moved to **BackedOff** state.

Note Each time the AP is BackedOff, the **Update Attempts** count increments.

- d. **Completed**—image pre-download is complete on the AP.

The screenshot displays the Cisco GUI for a Cisco Aironet 1850 Series Mobility Express. The left sidebar contains navigation options: Monitoring, Wireless Settings, Management (Access, Admin Accounts, Time, Software Update), and Advanced. The main content area is divided into two sections.

The top section, titled "Preimage Download Status", includes buttons for "Update Now", "Schedule Later", "Save Tftp Parameters", and "Restart". It shows a summary of AP update statistics:

Total Number of APs	10
Number of APs Currently Being Updated	1
Number of APs Completed	4
Number of APs that BackedOff	4

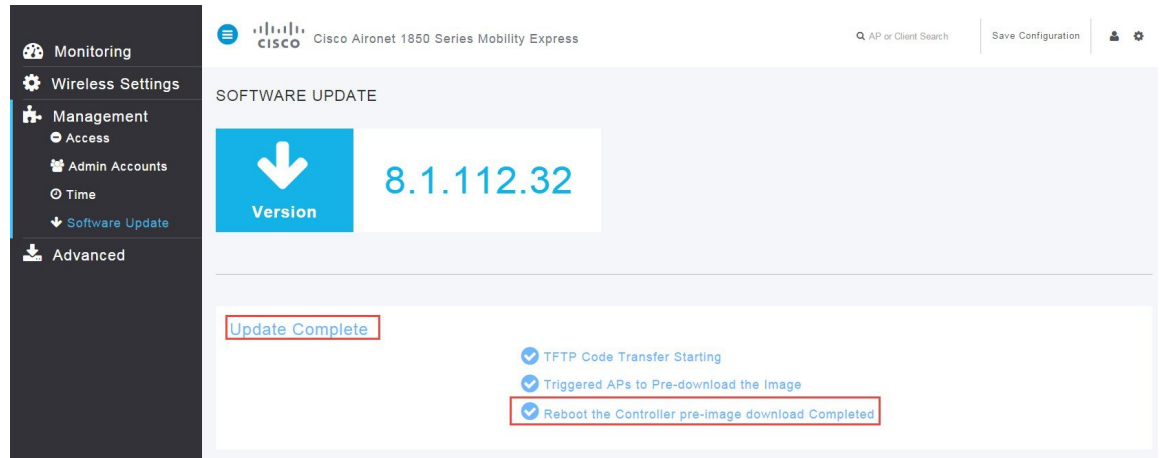
Below the summary is a table listing individual APs with their names, states, and update attempts:

AP Name	State	Update Attempts
APA0EC.F96C.CDD8	Completed	NA
APA0EC.F96C.D5E8	Initiated	2
AP7C0E.CEF5.AF54	Completed	NA
AP10F3.119C.FDA1	Predownloading	NA
AP7C69.F647.52F0	BackedOff	2
APF07F.0692.CC78	Completed	NA
AP5006.042E.0EDE	Completed	NA
APBC16.6514.35D5	BackedOff	2
APBC16.6509.3AC0	BackedOff	2
AP6C20.56E6.7725	BackedOff	2

The bottom section, titled "SOFTWARE UPDATE", shows the current version "8.1.112.32" and a "Version" button with a download icon. Below this, the "Update in Progress" section lists the following tasks:

- TFTP Code Transfer Starting
- Triggered APs to Pre-download the Image
- Reboot the Controller pre-image download Completed

After the image pre-download is complete, the status dashboard displays **Update Complete** and notifies the user to reboot the Mobility Express network.



Step 7 After image pre-download is complete, Mobility Express network needs to be re-booted to run the new software. If **Update Now** was selected for image pre-download, click **Restart** to reboot all the APs in the Mobility Express network.

Note If you chose **Schedule Later** for image pre-download and specified Set Reboot Time, do not **Restart** the APs, as the reboot happens at the scheduled time.



Step 8 After few minutes, log into Mobility Express and check the new version in the Software Update page.

Updating Cisco Mobility Express Network using CLI

To upgrade Cisco Mobility Express Network using CLI, perform the following steps:

Procedure

Step 1 Log in to Cisco 1850 AP running Mobility Express controller using Telnet or SSH.

Step 2 Specify the data type, using the following command:

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

Step 3 Specify the transfer mode, using the following command:

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

Step 4 Specify the IP address of the TFTP server, using the following command:

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

Step 5 Specify the path of the AP images on the TFTP server, using the following command:

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

Note For successful image pre-download, ensure that path to the AP images is correct.

Step 6 Pre-download the image on the APs, using the following command:

```
(Cisco Controller) >transfer download start
```

Output:

```
Mode..... TFTP
Data Type..... ap-image
TFTP Server IP..... 10.1.1.77
TFTP Packet Timeout..... 10
TFTP Max Retries..... 10
TFTP Path..... ap_bundle_8.1.112.30/
```

```
This may take some time.
Are you sure you want to start? (y/N) y
```

```
TFTP Code transfer starting.
```

```
Triggered APs to pre-download the image.
Reboot the controller once AP Image pre-download is complete.
```

Step 7 Check the pre-download status, using the following command:

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

Output:

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

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

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

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

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

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

Step 8 When pre-download is complete, reset the system using the following command:

```
(Cisco Controller) >reset system
```

Output:

```
The system has unsaved changes.
Would you like to save them now? (y/N) y
```

```
Configuration Saved!
System will now restart!
```

Cisco 1850 running Mobility Express re-boots followed by the rest of APs.

Step 9 Log in to the Mobility Express and check the version of primary image. The System displays the new version and the Backup Image displays the previous version.



CHAPTER 7

Using Advanced Settings

- [SNMP, on page 61](#)
- [Logging, on page 63](#)
- [Reset to Factory Default, on page 65](#)

SNMP

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

Managing SNMP using GUI

To manage SNMP using GUI, perform the following steps:

Procedure

- Step 1** Click **Advanced > SNMP**.
The SNMP Setup screen appears displaying the supported version details.

The screenshot shows the Cisco configuration interface for SNMP Setup. The left sidebar has a dark background with white text and icons. The main content area is light gray. At the top left of the main area is the Cisco logo and a search bar. Below the logo is the title 'SNMP SETUP'. A large blue button with a white arrow pointing down and the text 'Version' is on the left. To its right is a white box with a red border containing the text 'v2c'. Below these are five configuration fields, each with a red border around the input area: 'SNMPv2Access' (dropdown menu set to 'Enabled'), 'Read Only Community' (text input 'public'), 'Read-Write Community' (text input 'private'), 'SNMP Trap' (dropdown menu set to 'Enabled'), and 'SNMP Server IP' (text input '172.20.229.50'). At the bottom right is a green 'Apply' button.

- Step 2** From the **SNMPv2 Access** drop-down list, choose **Enabled**.
The default option is disabled.
- Step 3** Enter the community name in the **Read Only Community** field.
The default option is public.
- Step 4** Enter the community name in the **Read-Write Community** field.
The default option is private.
- Step 5** From the **SNMP Trap** drop-down list, choose **Enabled**.
The default option is Disabled. The SNMP Trap Receiver tool receives logs and displays the SNMP traps sent from the network.
- Step 6** Enter IP address of the server in the **SNMP Server IP** field.
- Step 7** Click **Apply**.

Managing SNMP using CLI

To manage SNMP using CLI, perform the following steps:

Procedure

- Step 1** Log in to the Mobility Express controller CLI.
- Step 2** Enter the following commands to enable and view the SNMP version:
- ```
(Cisco Controller) >config snmp version v2c enable
(Cisco Controller) >show snmpversion
```
- Step 3** Enter the following commands to configure and view the Read-Only Community:
- ```
(Cisco Controller) >config snmp community accessmode ro public
(Cisco Controller) >show snmpcommunity
```
- Step 4** Enter the following commands to configure and view the Read-Write Community:
- ```
(Cisco Controller) >config snmp community accessmode rw private
(Cisco Controller) >show snmpcommunity
```
- Step 5** Enter the following commands to configure and view the SNMP Trap Receive:
- ```
(Cisco Controller) >config snmp trapreceiver create 10.10.10.10
(Cisco Controller) >show snmptrap
```
- Step 6** Enter the following commands to send the SNMP traps:
- ```
(Cisco Controller) >config snmp trapreceiver mode enable
(Cisco Controller) >show snmptrap
```
- 

# 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 that contains the details of the event.

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

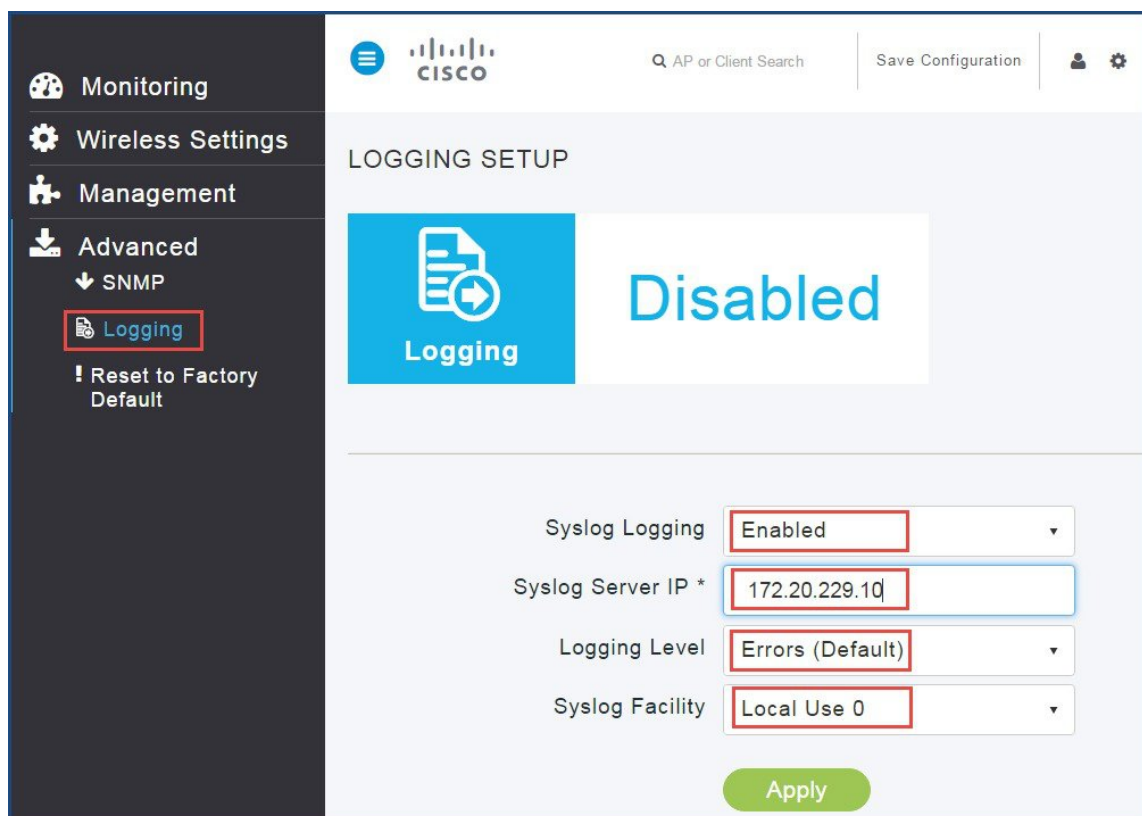
## System Logging using GUI

To perform system logging using GUI, follow these steps:

### Procedure

---

- Step 1** Click **Advanced > Logging**.  
The Logging Setup screen appears.
- Step 2** Choose **Enabled** from **Syslog Logging** drop-down list.  
The default option is disabled.



- Step 3** Enter the IPv4 address in the **Syslog Server IP** field.
- Step 4** From the **Logging level** drop-down list, choose syslog severity level.
- Step 5** From the **Syslog Facility** drop-down list, choose the syslog severity level.
- Step 6** Click **Apply**.

## System Logging using GUI using CLI

To perform system logging using CLI, follow these steps:

### Procedure

- Step 1** Enter the following commands to configure Syslog Server IP:

```
(Cisco Controller) >config logging syslog level <0-7>
<0-7> Set syslog message logging message severity level.
alerts Set syslog message logging severity to 'alerts' (severity 1).
critical Set syslog message logging severity to 'critical' (severity 2).
debugging Set syslog message logging severity to 'debugging' (severity 7).
emergencies Set syslog message logging severity to 'emergencies' (severity 0).
errors Set syslog message logging severity to 'errors' (severity 3).
informational Set syslog message logging severity to 'informational' (severity 6).
notifications Set syslog message logging severity to 'notifications' (severity 5).
warnings Set syslog message logging severity to 'warnings' (severity 4).
```

**Step 2** Enter the following commands to configure Syslog Logging Facility:

```
(Cisco Controller) >config logging syslog facility <facility>
auth-private Authorization system (private).
authorization Authorization system.
cron Cron/at facility.
daemon System daemons.
ftp FTP daemon.
kern Kernel.
local0 Local use.
local1 Local use.
local2 Local use.
local3 Local use.
local4 Local use.
local5 Local use.
local6 Local use.
local7 Local use.
lpr Line printer system.
mail Mail system.
news USENET news.
sys12 System use.
sys13 System use.
sys14 System use.
sys15 System use.
syslog Syslog itself.
user User process.
uucp Unix-to-Unix copy system.
```

## Reset to Factory Default

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

**Note**

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

## Mobility Express Network to Factory Default using GUI

To set Mobility Express network to factory default settings using GUI, perform the following steps:

**Procedure**

- Step 1** Click **Advanced > Reset to Factory Default**.  
The Reset Mobility Express Controller to Factory Default page appears.



- Step 2** Click **Continue**.  
A confirmation message box appears.



- Step 3** Click **Yes**.



## CHAPTER 8

# Adding an Access Point to Mobility Express Network

---

- [Adding an Access Point to Mobility Express Network, on page 67](#)

## Adding an Access Point to Mobility Express Network

Pre-requisites for Adding an Access Point:



---

**Note** The primary AP facilitates transfer of image from TFTP to the new AP which is added.

---

1. The AP bundle with AP images downloaded from cisco.com is unzipped and copied into the TFTP server.
2. A DHCP server on the same network, so that an Access Point being added and can obtain an IP.

### Sequence of Steps

1. Download the **AIR-AP1850-K9-ME-<version>.zip** file from cisco.com on a device running TFTP server. **The bundle version must be the same as the one running on the Master AP.** Unzip the file to extract the AP images.
2. Configure the TFTP parameters in the **Software Update (Management > Software Update)** page.
3. Connect the AP to the network.
4. When the AP reboots, it obtains an IP address from the DHCP server. If the AP version matches the one on primary AP, it joins. However, if the version on the AP being added is different than then one on the primary AP, it starts to download the image from the TFTP server. After the image download is complete, the AP will reboot and join the primary AP.



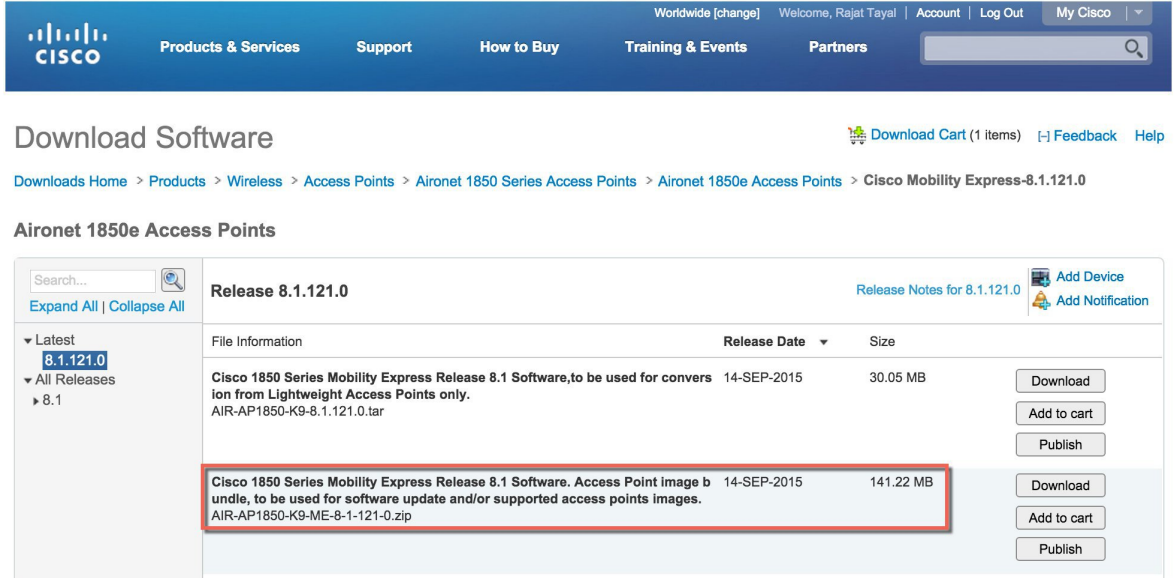
---

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

---

## Procedure

**Step 1** Download the `AIR-AP1850-K9-ME-<version>.zip` file from `cisco.com` to a machine running TFTP server.



Worldwide [change] | Welcome, Rajat Tayal | Account | Log Out | My Cisco

Products & Services | Support | How to Buy | Training & Events | Partners

### Download Software

Download Cart (1 items) | Feedback | Help

Downloads Home > Products > Wireless > Access Points > Aironet 1850 Series Access Points > Aironet 1850e Access Points > Cisco Mobility Express-8.1.121.0

#### Aironet 1850e Access Points

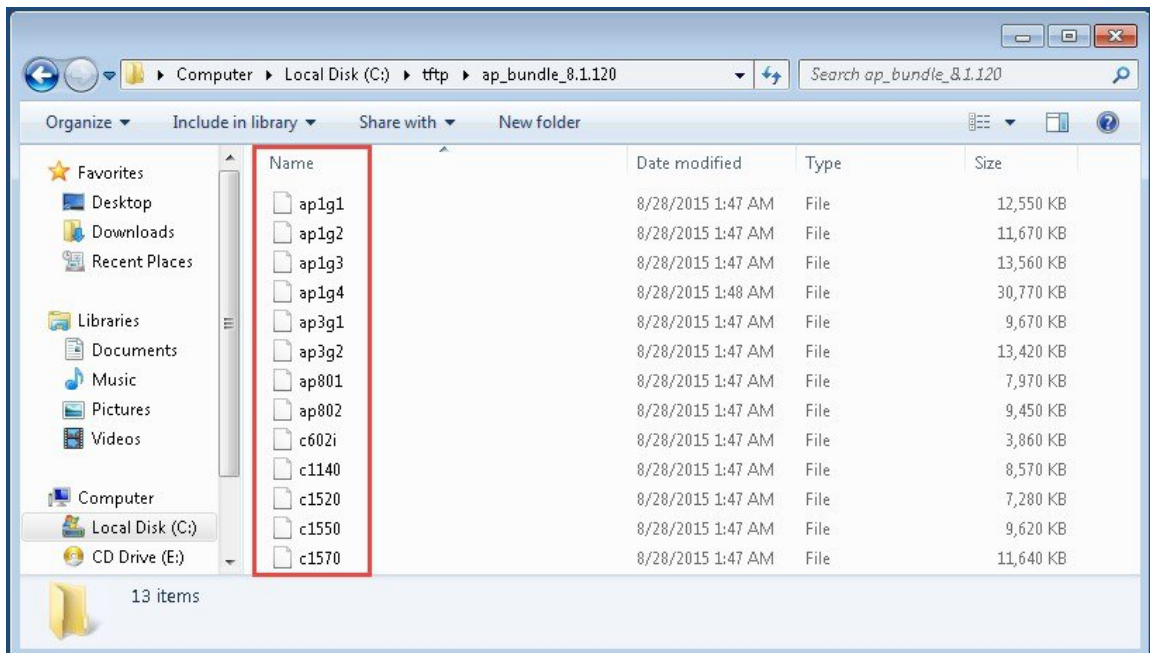
Search... | Expand All | Collapse All

Release 8.1.121.0 | Release Notes for 8.1.121.0 | Add Device | Add Notification

| File Information                                                                                                                                                                            | Release Date | Size      |                                    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------|------------------------------------|
| Cisco 1850 Series Mobility Express Release 8.1 Software, to be used for conversion from Lightweight Access Points only.<br>AIR-AP1850-K9-8.1.121.0.tar                                      | 14-SEP-2015  | 30.05 MB  | Download<br>Add to cart<br>Publish |
| Cisco 1850 Series Mobility Express Release 8.1 Software. Access Point image bundle, to be used for software update and/or supported access points images.<br>AIR-AP1850-K9-ME-8-1-121-0.zip | 14-SEP-2015  | 141.22 MB | Download<br>Add to cart<br>Publish |

**Step 2** Unzip the `AIR-AP1850-K9-ME-<version>.zip` file to extract the AP images.

**Note** Do not rename the AP images on the TFTP server.



Computer > Local Disk (C:) > tftp > ap\_bundle\_8.1.120

Search ap\_bundle\_8.1.120

| Name  | Date modified     | Type | Size      |
|-------|-------------------|------|-----------|
| ap1g1 | 8/28/2015 1:47 AM | File | 12,550 KB |
| ap1g2 | 8/28/2015 1:47 AM | File | 11,670 KB |
| ap1g3 | 8/28/2015 1:47 AM | File | 13,560 KB |
| ap1g4 | 8/28/2015 1:48 AM | File | 30,770 KB |
| ap3g1 | 8/28/2015 1:47 AM | File | 9,670 KB  |
| ap3g2 | 8/28/2015 1:47 AM | File | 13,420 KB |
| ap801 | 8/28/2015 1:47 AM | File | 7,970 KB  |
| ap802 | 8/28/2015 1:47 AM | File | 9,450 KB  |
| c602i | 8/28/2015 1:47 AM | File | 3,860 KB  |
| c1140 | 8/28/2015 1:47 AM | File | 8,570 KB  |
| c1520 | 8/28/2015 1:47 AM | File | 7,280 KB  |
| c1550 | 8/28/2015 1:47 AM | File | 9,620 KB  |
| c1570 | 8/28/2015 1:47 AM | File | 11,640 KB |

13 items

**Step 3** Log in to the Mobility Express user interface and choose **Management > Software Update**.

The Software Update page displays the current software version running on the Mobility Express controller.

The screenshot displays the 'SOFTWARE UPDATE' configuration page for a Cisco Aironet 1850 Series Mobility Express device. The left sidebar shows navigation options: Monitoring, Wireless Settings, Management (with sub-options: Access, Admin Accounts, Time, Software Update), and Advanced. The main content area shows the current version as 8.1.112.32. Below this, the configuration fields are: Transfer Mode (TFTP), IP Address (IPv4) (10.10.10.2), File Path (ap\_bundle\_8.1.112.32/), and Set Reboot Time. At the bottom, there are four buttons: Update Now, Schedule Later, Save Tftp Parameters (highlighted with a red box), and Restart. A link for 'Preimage Download Status' is also visible.

**Step 4** Enter the IPv4 address of the TFTP server in the **IP Address (IPv4)** field.

**Step 5** Enter **File Path** for the unzipped AP images.

**Step 6** Click **Save Tftp Parameters**.

**Step 7** Connect the AP to the Mobility Express network. After the image download is complete, the AP automatically reboots and joins the primary APs.







## CHAPTER 9

# Primary AP Failover and Electing a New Primary

Cisco Mobility Express is supported on Cisco 1800 Access Points and the primary AP election process determines which Cisco 1800 AP will be elected to run Mobility Express controller function in case of a Failover. VRRP is used to detect a failure of primary AP and to elect a new primary.



---

**Note** Mobility Express uses MAC 00-00-5E-00-01-VRID where VRID is 1 so if there are other instances of VRRP running in the environment, use VRID other than 1 for those instances.

---



---

**Note** Only Cisco 1800 series Access Points can be elected as primary APs.

---

- [Primary AP Failover, on page 71](#)
- [Primary Election, on page 71](#)

## Primary AP Failover

To have redundancy in the Mobility Express network, it must have two or more Cisco 1800 series Access Points. These Access Points should have AP Image type as **MOBILITY EXPRESS IMAGE** and **AP Configuration** as **MOBILITY EXPRESS CAPABLE**. In an event of a failure of primary AP, another Cisco 1800 series AP is elected as a primary automatically. The newly elected primary AP has the same IP and configuration as the original primary AP.



---

**Note** Cisco 1800 series Access points which have the Mobility Express Image but AP Configuration is NOT MOBILITY EXPRESS CAPABLE, they will not participate in the primary AP election process.

---

## Primary Election

The primary election process of Cisco 1800 series APs is based on a set of priorities. An AP with the highest priority is elected as the primary AP, running Mobility Express controller function.

The primary AP election priorities are as follows:

1. User Defined Primary— User can define a preferred primary AP to be elected incase of a failover. The following command can be entered on the controller CLI :

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

To view the preferred primary, use the following command:

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

To clear the user defined priority from an AP, use the following command:

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



---

**Note** We recommend user not to define the preferred primary AP unless it is required for debugging or serviceability reasons.

---

2. Least Client Load—Cisco 1800 series Access Point with least client load is elected as the primary AP.
3. Lowest MAC Address—If the User defined priority is not configured and everything else is the same, then Access Point with the lowest MAC gets elected as the primary AP.



## CHAPTER 10

# Conversion



**Note** Conversion from CAPWAP to Mobility Express is supported from 8.1.122.0. The AP must have 8.1.122.0 CAPWAP image or later (Recommend to use 8.2.100.0) on the 1800 series access point before you can convert them to MobilityExpress. If the 1800 series access point has an image older than 8.1.122.0, the AP must first join a WLC running 8.1.122.0 or higher to upgrade its CAWAP image. After the CAPWAP image on the AP has been upgraded, conversion of AP from CAPWAP to Mobility Express can be performed.

The Cisco 1800 series access point is capable of operating as a CAPWAP AP or a Mobility Express capable AP (runs controller function in a Mobility Express network) managing other access points as well as serving clients.

The following conversions are supported:

1. Converting a CAWAP AP to Mobility Express capable AP - This conversion is required when you have an 1800 series access point running CAPWAP image, and you want to use them to deploy a Mobility Express network. For this, you would convert the CAPWAP AP to a primary AP (runs controller function in a Mobility Express network).
2. Converting a Mobility Express capable AP to CAPWAP AP - There are two reasons for this conversion:
  - a. If you want to migrate the 1800 series access points from a Mobility Express network to another controller (not Mobility Express) network.
  - b. If you do not want 1800 series access points to participate in the primary AP election process in a Mobility Express network.

The Cisco 1800 series access points support two different images:

1. CAPWAP image - When a CAPWAP image is installed on an access point, it can only operate as a CAPWAP access point and does not support the controller function.
2. Mobility Express image - When a Mobility Express image is installed on an access point, it can operate in one of the modes:
  - a. Both as a controller and an access point
  - b. An access point alone

To determine the image and capability on the access point, you can do a show version on the AP CLI to determine the AP Image Type and AP Configuration:

If show version does not display AP Image Type and AP Configuration parameters, it means that AP is running the CAPWAP image.

If the show version CLI displays AP Image Type: MOBILITY EXPRESS IMAGE and AP Configuration: MOBILITY EXPRESS CAPABLE, it operates both as Controller and an Access Point. It participates in the Primary Election process in case of a failover.

```
cisco AI R-AP1852E-UXX9 ARMv7 Processor rev 0 (v71) with 997184/525160K bytes of memory.
Processor board ID RFDP2BCR021
AP Running Image : 8.1.121.0
Primary Boot Image : 8.1.121.0
Backup Boot Image : 8.1.106.33
AP Image type : MOBILITY EXPRESS IMAGE
AP Configuration : MOBILITY EXPRESS CAPABLE
0 Gigabit Ethernet interfaces
0 802.11 Radios
Radio FW version . 1401b63d12113073a3C08aa67f0c039c0
NSS FW version : NSS.AK.1.0.c4-0Z026-E_cust C-1.24160.1
```

If the show version CLI shows AP Image Type: MOBILITY EXPRESS IMAGE and AP Configuration: NOT MOBILITY EXPRESS CAPABLE, it operates only as access point and does not participate in the Primary Election process in case of a failover.

```
cisco AI R-AP1852E-UXX9 ARMv7 Processor rev 0 (v7I) with 997184/726252K bytes of memory.
Processor board ID RFDP2BCR021
AP Running Image : 8.1.121.0
Primary Boot Image : 8.1.121.0
Backup Boot Image : 8.1.106.33
AP Image type : MOBILITY EXPRESS IMAGE
AP Configuration : NOT MOBILITY EXPRESS CAPABLE
2 Gigabit Ethernet interfaces
2 802.11 Radios
Radio FW version : 1401b63d121b073a3008aa67f0c039d0
NSS FW version : NSS.AK.1.0.c4-00026-E_cust C-1. 24160.1
```

- [Converting a CAWAP AP into a Mobility Express AP, on page 74](#)
- [Converting a Mobility Express AP into a CAPWAP AP, on page 76](#)

## Converting a CAWAP AP into a Mobility Express AP

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

### Pre-requisites for converting CAPWAP AP to Mobility Express:

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

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

## Procedure

- Step 1** Download the AIR-AP1850-K9-<version>.tar or AIR-AP1830-K9-<version>.tar file from cisco.com to a machine running TFTP server. **Do not untar the file.**

The screenshot shows the Cisco Download Software page for Aironet 1850e Access Points. The page title is "Download Software" and the breadcrumb trail is "Downloads Home > Products > Wireless > Access Points > Aironet 1850 Series Access Points > Aironet 1850e Access Points > Cisco Mobility Express-8.1.121.0". The page displays a table of software releases for "Release 8.1.121.0". The table has columns for "File Information", "Release Date", and "Size". The first row is highlighted with a red border and contains the following information:

| File Information                                                                                                                                                                            | Release Date | Size      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------|
| Cisco 1850 Series Mobility Express Release 8.1 Software, to be used for conversion from Lightweight Access Points only.<br>AIR-AP1850-K9-8.1.121.0.tar                                      | 14-SEP-2015  | 30.05 MB  |
| Cisco 1850 Series Mobility Express Release 8.1 Software. Access Point image bundle, to be used for software update and/or supported access points images.<br>AIR-AP1850-K9-ME-8-1-121-0.zip | 14-SEP-2015  | 141.22 MB |

Each row has buttons for "Download", "Add to cart", and "Publish".

- Step 2** Connect and login to the Cisco 1800 series Access Point CLI.
- Step 3** Enter **enable** to go to privileged execution mode.
- Step 4** Enter **show version** on the Access Point CLI. From the **show version** output, you can determine the **AP Image type** and **AP Configuration** and can then proceed with the conversion process.
- Case 1: If the **AP Image type** is **MOBILITY EXPRESS IMAGE** and **AP configuration** is **NOT MOBILITY EXPRESS CAPABLE**, only conversion of AP Configuration is required. Go to [Step 5](#).
  - Case 2: In the `show version` output, if the **AP Image type** and **AP Configuration** are not available, download of the Mobility Express image and conversion of **AP Configuration** is required. Go to [Step 6](#).

- Step 5** Enter the command below to change the **AP Configuration** to **MOBILITY EXPRESS CAPABLE**.

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

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

- Step 6** If **AP Image Type** and **AP Configuration** is not available in `show version`, it means that the AP is running **CAPWAP image**. To do the conversion, execute the command below:

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

Example:

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

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

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

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

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

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

**Step 7** After AP reboots, Mobility Express starts in Day 0 and *CiscoAirProvision* SSID is broadcast.

## Converting a Mobility Express AP into a CAPWAP AP

When the AP type is CAPWAP, AP doesn't have the controller function and cannot participate in the primary AP election process.

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

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

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

### Procedure

- Step 1** Connect and login to the Cisco 1800 AP through CLI.
- Step 2** Type **Enable** to go to privileged execution mode.
- Step 3** Enter **ap#ap-type capwap** and confirm to switch to the CAPWAP type.

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

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

The above command converts all Cisco 1800 APs connected to the Mobility Express with **AP Configuration: MOBILITY EXPRESS CAPABLE** to **AP Configuration: NOT MOBILITY EXPRESS CAPABLE**. When this command is issued the APs are reloaded, and they come back up in local mode.

---



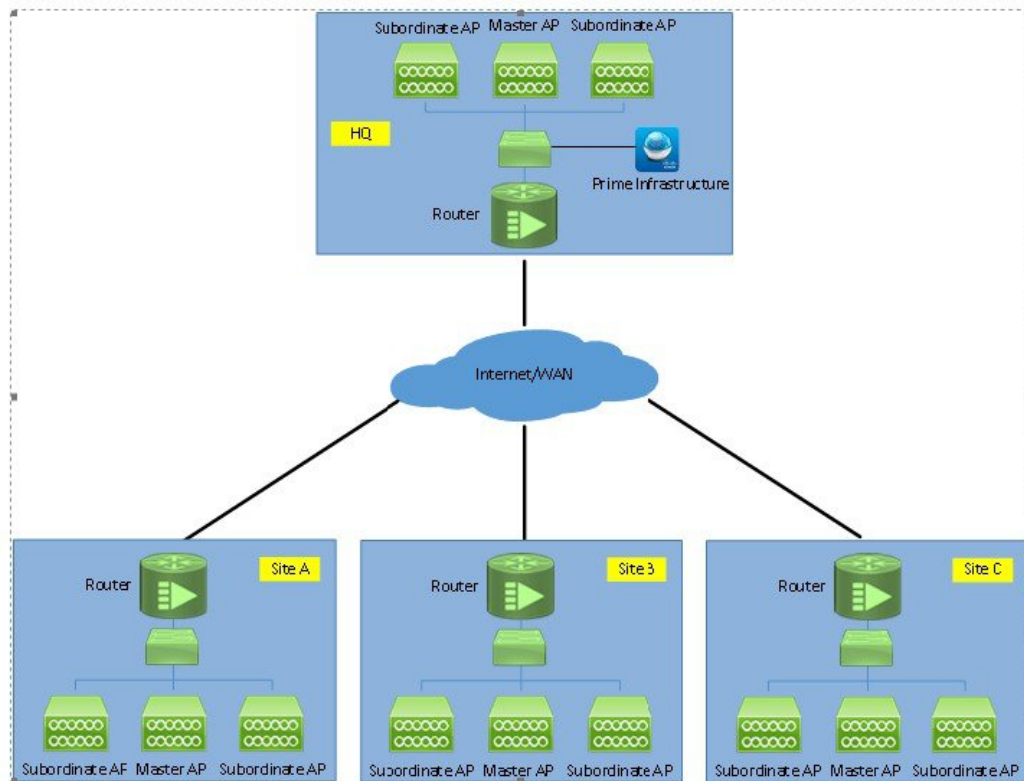




# CHAPTER 11

## Managing Mobility Express Deployments from Cisco Prime Infrastructure

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



- [Adding Mobility Express to Prime, on page 79](#)

## Adding Mobility Express to Prime

Perform the following steps to add the controllers:

## Procedure

### Step 1 Login to Cisco Prime

© 2009-2015 Cisco Systems, Inc., Cisco, Cisco Systems, and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. The copyrights to certain works contained in this software are owned by other third parties and used and distributed under license. Certain components of this software are licensed under the GNU GPL 2.0, GPL 3.0, LGPL 2.1, LGPL 3.0 and AGPL 3.0.

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

| Device Name          | Reachability         | IP Address           | DNS Name             | Device Type |
|----------------------|----------------------|----------------------|----------------------|-------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |             |

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

**Add Device**

\* General

\* SNMP

Telnet/SSH

HTTP/HTTPS

IPSec

\* General Parameters

IP Address

DNS Name

License Level: Full

Credential Profile: --Select--

Add Verify Credentials Cancel

**Step 4** Enter the SNMP Parameters and click Add.

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

**Add Device**

\* General ✓

\* SNMP

Telnet/SSH

HTTP/HTTPS

IPSec

\* SNMP Parameters

Version: v2c

\* SNMP Retries: 2

\* SNMP Timeout: 10 (secs)

\* SNMP Port: 161

\* Read Community:

\* Confirm Read Community:

Write Community:

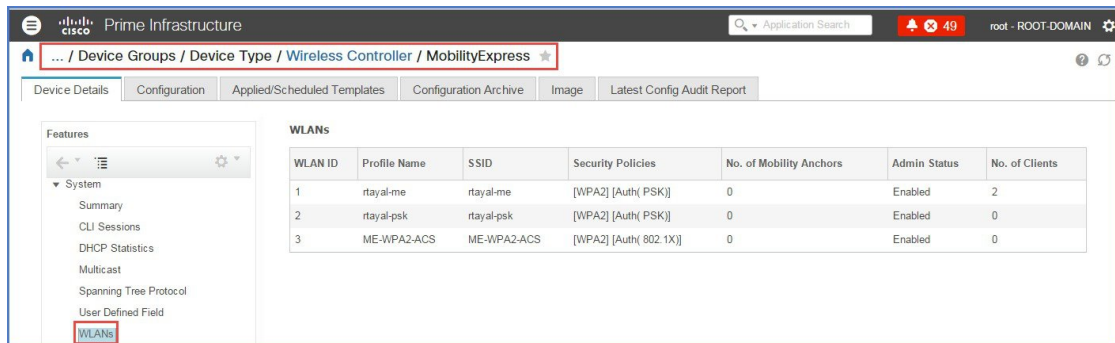
Confirm Write Community:

Add Verify Credentials Cancel

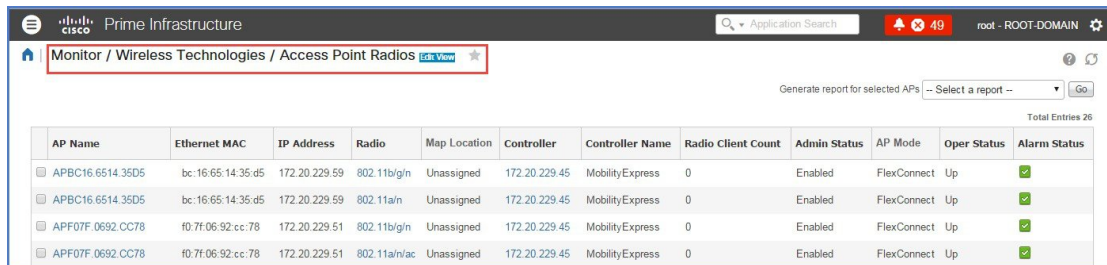
**Step 5** After the device is added, it shows up in the **All Devices** list.



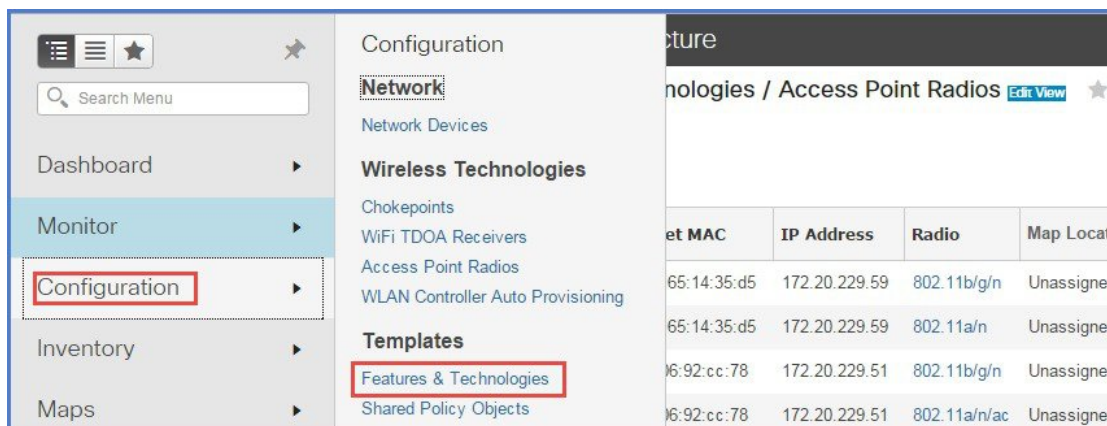
**Step 6** To view the list of WLANs, navigate to **Network Devices > Device Groups > Device Type > Wireless Controller** and select the Mobility Express controller you added in Step 4.



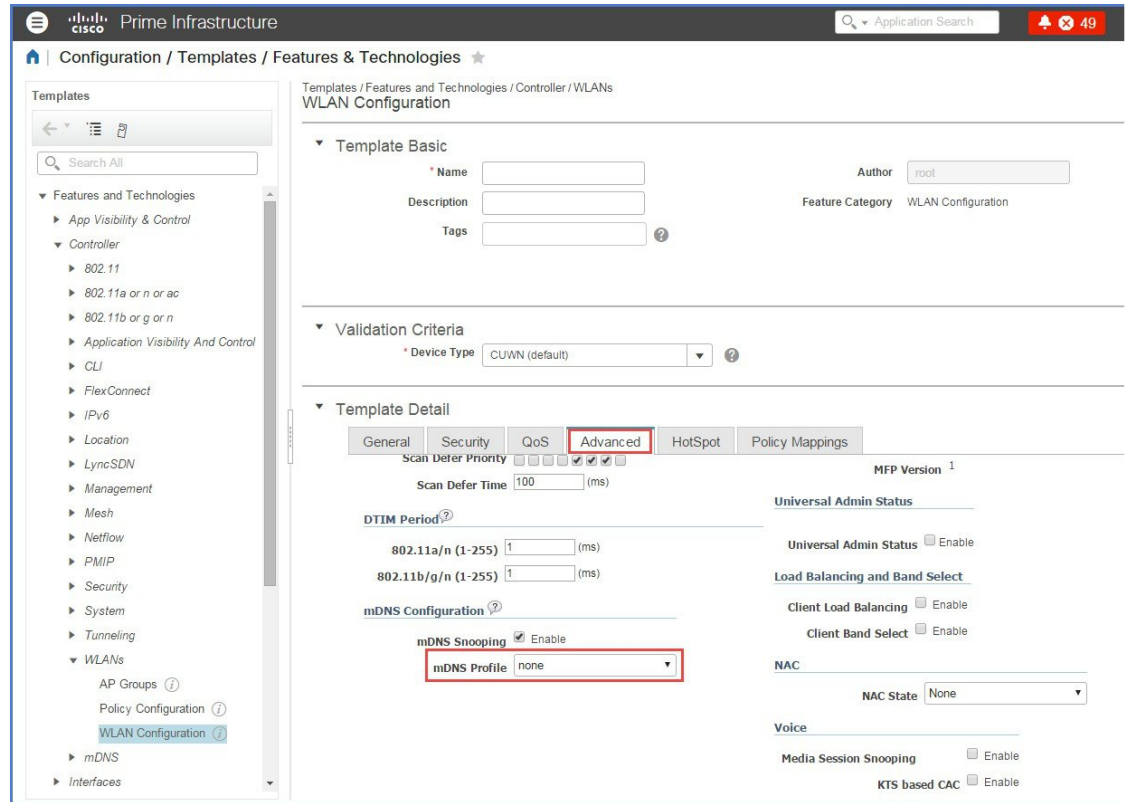
**Step 7** To view the list of AP, navigate to **Monitor > Wireless Technologies > Access Point Radios**



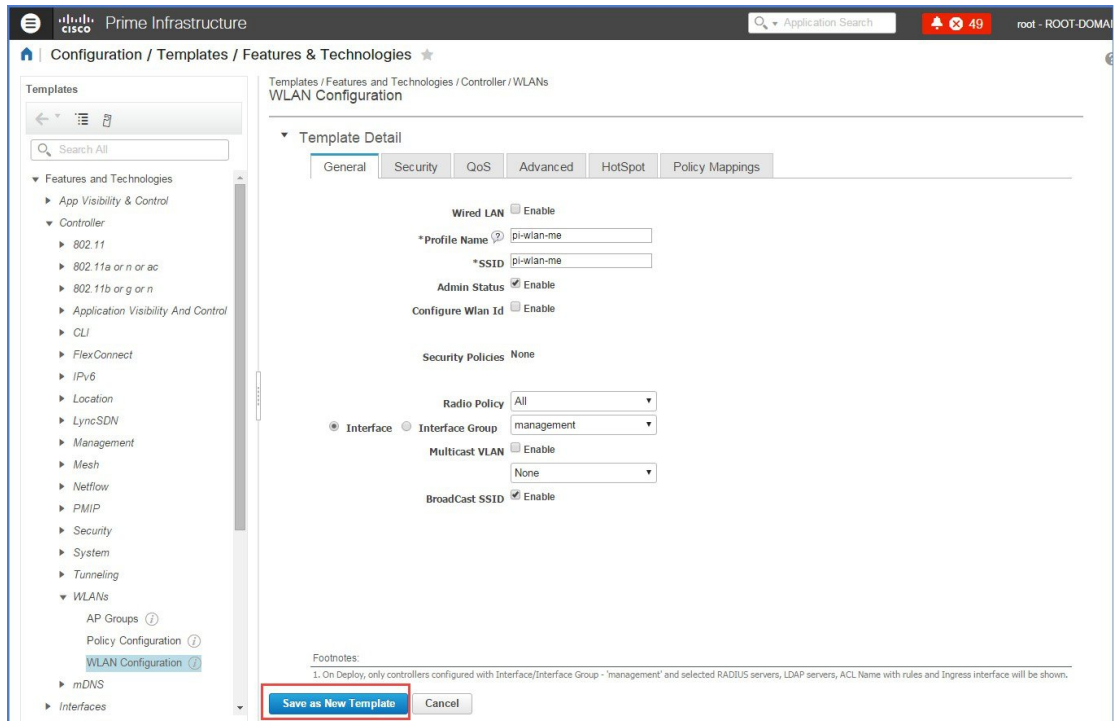
**Step 8** To configure WLANS from Prime on Mobility Express, navigate to **Configuration > Feature & Technologies** under **Template**.



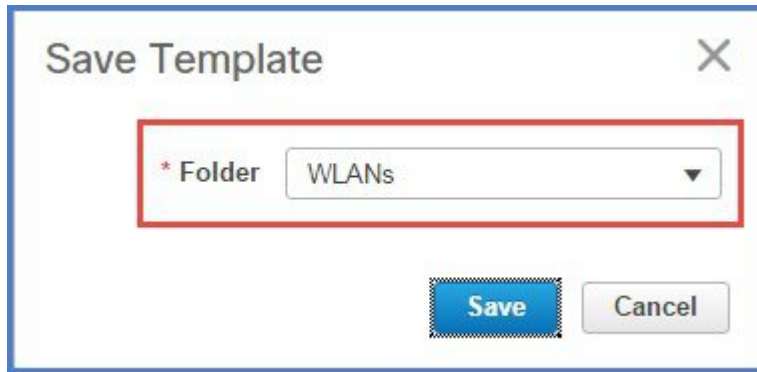
**Step 9** Navigate to **Controller > WLAN > WLAN Configuration**. Enter the Template name and the **Template Detail**.



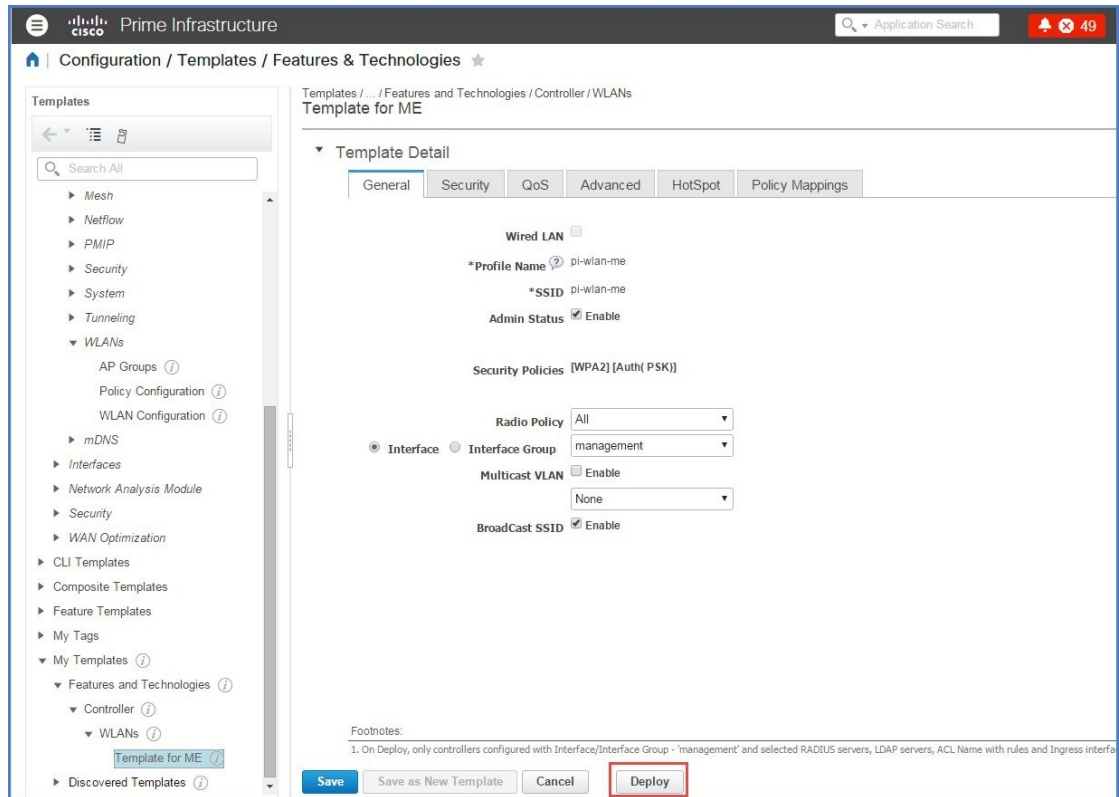
**Step 10** On the **Advanced Tab**, make sure mDNS profile is set to **none** as it is not supported on Mobility Express.



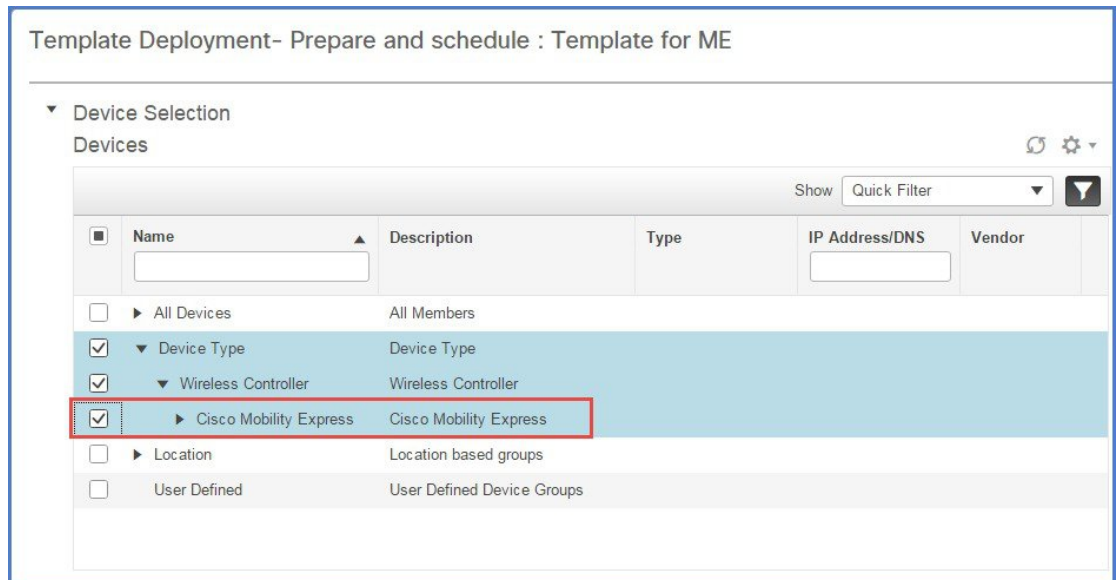
**Step 11** To save the Template, click on ‘Save as New Template’ and select the folder where the templates need to be saved.



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



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



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

Prime Infrastructure

Administration / Dashboards / Job Dashboard / Template for ME\_1

Recurrence None  
Description N/A

Showing latest 5 Job instances [Show All](#) Total 1

| Run ID  | Status  | Duration (hh:mm:ss) | Start Time       | Completion Time  |
|---------|---------|---------------------|------------------|------------------|
| 1637325 | Success | 00:00:02            | 2016-03-17 13:03 | 2016-03-17 13:03 |

Job summary Successful deployment on 1 device(s).

Job Results for Template for ME

| Device        | Status  | Transcript       |
|---------------|---------|------------------|
| 172.20.229.45 | Success | Deploy succeeded |





## CHAPTER 12

# Mobility Express CLI Reference

---

- [Application Visibility Commands](#) , on page 87
- [ClearAir Commands](#) , on page 87
- [Controller Image Upgrade Commands](#) , on page 88
- [DNS Commands](#) , on page 88
- [Flexconnect Commands](#), on page 88
- [Migration Commands](#) , on page 88
- [NTP Commands](#) , on page 89
- [Ports and Interface Commands](#) , on page 89
- [RRM Commands](#), on page 89
- [Security Commands](#), on page 93
- [System Management Commands](#), on page 95
- [UX Regulatory Domain Commands](#) , on page 96
- [VRRP Command](#) , on page 96
- [WGB Commands](#) , on page 96
- [WLAN Commands](#) , on page 97

## Application Visibility Commands

**config flexconnect group default-flexgroup avc 1 visibility { enable | disable }**— To enable or disable Application Visibility in a WLAN

**show flexconnect group detail default-flexgroup**— To display the status of Application Visibility in each WLAN

**show flexconnect avc statistics group default-flexgroup**— To view Application Visibility statistics based on the flex group

**show flexconnect avc statistics client *client\_MAC***—To view Application Visibility statistics based on each client

## ClearAir Commands

**config 802.11b cleanair enable *ap\_MAC***— To enable CleanAir on an associated AP. Not applicable to 1850 and 1830 series APs.

**show 802.11b cleanair device ap *ap\_MAC***—To list all the interference devices connected to the AP.

**show 802.11b cleanair device type jammer**—To jam a specific interference device

## Controller Image Upgrade Commands

**transfer download ap-images imagePath *image\_path***— To set the path of the software image on the TFTP server

**transfer download ap-images mode tftp**— To set the file transfer mode as TFTP

**transfer download ap-images serverIp *ipv4\_address***—To specify the IP address of the TFTP server/

**transfer download start**—To save the configuration and start the image download

**debug transfer all { enable | disable }**—To debug the transfer and download with all sub commands enabled

**debug transfer tftp { enable | disable }**—To debug transfer download tftp

**debug transfer trace { enable | disable }**—To debug transfer trace

## DNS Commands

**config network dns default**—To configure the default DNS servers.

**show network summary**—To view a network summary, with the default DNS servers listed, if they are enabled.

## Flexconnect Commands

**config flexconnect group default-flexgroup wlan-vlan wlan { WLAN id } add Vlan { VLAN ID}**—To configure VLAN to WLAN on FlexConnect group

**config flexconnect acl { apply | create | delete } acl\_name**—To apply access control lists that are configured on a FlexConnect access point, use the **config flexconnect acl** command

**config flexconnect aclrule { action rule\_name rule\_index { permit | deny } | add rule\_name rule\_index | change index rule\_name old\_index new\_index | delete rule\_name rule\_index | destination address rule\_name rule\_index ip\_address netmask | destination port range rule\_name rule\_index start\_port end\_port | direction rule\_name rule\_index { in | out | any } | dscp rule\_name rule\_index dscp | protocol rule\_name rule\_index protocol | source address rule\_name rule\_index ip\_address netmask | source port range rule\_name rule\_index start\_port end\_port | swap index rule\_name index\_1 index\_2 }**

**show flexconnect acl detailed acl-name**—To display a detailed summary of FlexConnect access control lists, use the **show flexconnect acl detailed** command

## Migration Commands

**ap-type capwap**—To convert ap-type from Mobility Express to CAPWAP

**ap-type mobilityexpress tftp:// tftp\_server / file\_name** —To convert ap-type from CAPWAP to MobilityExpress, when running an Mobility Express software image config ap unifiedmode *switch\_name switch\_IP\_address* - To convert all APs to type to CAPWAP simultaneously from the switch

## NTP Commands

**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

**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

## Ports and Interface Commands

**show interface summary**—To display summary details of the system interfaces, use the show interface summary command

**show interfacedetailed {management}**—To display details of the system interfaces, use the show interface command.

**config interface address {management IP\_address netmask gateway}**—To configure address information for an interface, use the **config interface address** command

## RRM Commands

### Show Commands

**show 802.11 {a | b} extended**—To display access point radio extended configurations, use the **show 802.11 extended** command

**show advanced 802.11{a | b} channel**—To display the automatic channel assignment configuration and statistics, use the **show advanced 802.11 channel** command

**show advanced 802.11{a | b} coverage** —To display the configuration and statistics for coverage hole detection, use the **show advanced 802.11 coverage** command

**show advanced 802.11{a | b} l2roam {rf-param | statistics} mac\_address}**—To display 802.11a or 802.11b/g Layer 2 client roaming information, use the **show advanced 802.11 l2roam** command

**show advanced 802.11{a | b} logging**—To display 802.11a or 802.11b RF event and performance logging, use the **show advanced 802.11 logging** command

**show advanced 802.11{a | b} monitor** —To display the 802.11a or 802.11b default Cisco radio monitoring, use the **show advanced 802.11 monitor** command

**show advanced 802.11{a | b} profile {global | cisco\_ap}** —To display the 802.11a or 802.11b lightweight access point performance profiles, use the **show advanced 802.11 profile** command

**show advanced 802.11{a | b} receiver**—To display the configuration and statistics of the 802.11a or 802.11b receiver, use the **show advanced 802.11receiver** command

**show advanced 802.11{a | b} summary**—To display the 802.11a or 802.11b Cisco lightweight access point name, channel, and transmit level summary, use the **show advanced 802.11 summary** command

**show advanced 802.11{a | b} txpower**—To display the 802.11a or 802.11b automatic transmit power assignment, use the **show advanced 802.11txpower** command

## Config Commands

**config {802.11-a49 | 802.11-a58} {enable | disable} cisco\_ap**—To enable or disable the 4.9-GHz and 5.8-GHz public safety channels on an access point, use the **config 802.11-a** command

**config {802.11-a49 | 802.11-a58} antenna extAntGain ant\_gain cisco\_ap {global | channel\_no}**—To configure the external antenna gain for the 4.9-GHz and 5.8-GHz public safety channels on an access point, use the **config 802.11-a antenna extAntGain** commands

**config {802.11-a49 | 802.11-a58} channel ap cisco\_ap {global | channel\_no}**—To configure the channel properties for the 4.9-GHz and 5.8-GHz public safety channels on an access point, use the **config 802.11-a channel ap** command

**config {802.11-a49 | 802.11-a58} txpower ap cisco\_ap {global | power\_level}**—To configure the transmission power properties for the 4.9-GHz and 5.8-GHz public safety channels on an access point, use the **config 802.11-a txpower ap** command

**config 802.11a 11acsupport {enable | disable | mcs tx mcs\_index ss spatial\_stream {enable | disable}}**—To configure 802.11ac 5-GHz parameters, use the **config 802.11a 11acsupport** command

**config 802.11b 11gSupport {enable | disable}**—To enable or disable the Cisco wireless LAN solution 802.11g network, use the **config 802.11b 11gSupport** command

**config 802.11b preamble {long | short}**—To change the 802.11b preamble as defined in subclause 18.2.2.2 to long (slower, but more reliable) or short (faster, but less reliable), use the **config 802.11b preamble** command

**config 802.11h channelswitch {enable {loud | quiet} | disable}**—To configure an 802.11h channel switch announcement, use the **config 802.11h channelswitch** command

**config 802.11h powerconstraint value**—To configure the 802.11h power constraint value, use the **config 802.11h powerconstraint** command

**config 802.11h setchannel cisco\_ap**—To configure a new channel using 802.11h channel announcement, use the **config 802.11h setchannel** command

**config 802.11{a | b} 11nsupport {enable | disable}**—To enable 802.11n support on the network, use the **config 802.11 11nsupport** command

**config 802.11{a | b} 11nsupport antenna cisco\_ap {A | B | C | D} {enable | disable}**—To configure an access point to use a specific antenna, use the **config 802.11 11nsupport antenna** command

**config 802.11 {a | b} 11nsupport guard-interval {any | long}**—To configure the guard interval, use the **config 802.11 11nsupport guard-interval** command

**config 802.11{a | b} 11nsupport mcs tx {0-15} {enable | disable}**—To specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client, use the **config 802.11 11nsupport mcs tx** command

**config 802.11{a | b} 11nsupport mcs tx {0-15} {enable | disable}**—To configure the Reduced Interframe Space (RIFS) between data frames and its acknowledgment, use the **config 802.11 11nsupport rifs** command

**config 802.11{a | b} antenna diversity {enable | sideA | sideB} cisco\_ap**—To configure the diversity option for 802.11 antennas, use the **config 802.11 antenna diversity** command

**config 802.11{a | b} antenna extAntGain antenna\_gain cisco\_ap**—To configure external antenna gain for an 802.11 network, use the **config 802.11 antenna extAntGain** command

**config 802.11{a | b} antenna mode {omni | sectorA | sectorB} cisco\_ap**—To configure the Cisco lightweight access point to use one internal antenna for an 802.11 sectorized 180-degree coverage pattern or both internal antennas for an 802.11 360-degree omnidirectional pattern, use the **config 802.11 antenna mode** command

**config 802.11{a | b} antenna selection {internal | external} cisco\_ap**—To select the internal or external antenna selection for a Cisco lightweight access point on an 802.11 network, use the **config 802.11 antenna selection** command

**config 802.11{a | b} channel {global [auto | once | off | restart]} | ap {ap\_name [global | channel]}**—To configure an 802.11 network or a single access point for automatic or manual channel selection, use the **config 802.11 channel** command

**config 802.11{a | b} channel ap cisco\_ap {global | channel\_no}**—To set the operating radio channel for an access point, use the **config 802.11 channel ap** command

**config 802.11{a | b} chan\_width cisco\_ap {20 | 40 | 80}**—To configure the channel width for a particular access point, use the **config 802.11 chan\_width** command

**config 802.11{a | b} txPower {global {power\_level | auto | max | min | once } | ap cisco\_ap}**—To configure the transmit power level for all access points or a single access point in an 802.11 network, use the **config 802.11 txPower** command

**config advanced 802.11{a | b} channel add channel\_number**—To add channel to the 802.11 networks auto RF channel list, use the **config advanced 802.11 channel add** command

**config advanced 802.11{a | b} channel cleanair-event {enable | disable | sensitivity [low | medium | high] | custom threshold threshold\_value}**—To configure CleanAir event driven Radio Resource Management (RRM) parameters for all 802.11 Cisco lightweight access points, use the **config advanced 802.11 channel cleanair-event** command.

**config advanced 802.11{a | b} channel dca anchor-time value**—To specify the time of day when the Dynamic Channel Assignment (DCA) algorithm is to start, use the **config advanced 802.11 channel dca anchor-time** command.

**config advanced 802.11{a | b} channel dca chan-width-11n {20 | 40 | 80}**—To configure the Dynamic Channel Assignment (DCA) channel width for all 802.11n radios in the 5-GHz band, use the **config advanced 802.11 channel dca chan-width-11n** command.

**config advanced 802.11{a | b} channel dca interval value**—To specify how often the Dynamic Channel Assignment (DCA) is allowed to run, use the **config advanced 802.11 channel dca interval** command

**config advanced 802.11{a | b} channel dca RSSI\_value**—To configure the 5-GHz minimum RSSI energy metric for DCA, use the **config advanced 802.11 channel dca min-metric** command

**config advanced 802.11{a | b} channel dca sensitivity {low | medium | high}**—To specify how sensitive the Dynamic Channel Assignment (DCA) algorithm is to environmental changes (for example, signal, load, noise, and interference) when determining whether or not to change channels, use the **config advanced 802.11 channel dca sensitivity** command

**config advanced 802.11{a | b} channel foreign {enable | disable}**—To have Radio Resource Management (RRM) consider or ignore foreign 802.11a interference avoidance in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel foreign** command

**config advanced 802.11{a | b} channel load {enable | disable}**—To have Radio Resource Management (RRM) consider or ignore the traffic load in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel load** command

**config advanced 802.11{a | b} channel noise {enable | disable}**—To have Radio Resource Management (RRM) consider or ignore non-802.11a noise in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel noise** command.

**config advanced 802.11{a | b} channel update**—To have Radio Resource Management (RRM) initiate a channel selection update for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel update** command

**config advanced 802.11{a | b} coverage {enable | disable}**—To enable or disable coverage hole detection, use the **config advanced 802.11 coverage** command

**config advanced 802.11{a | b} coverage exception global percent**—To specify the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point, use the **config advanced 802.11 coverage exception global** command

**config advanced 802.11{a | b} coverage {data | voice} fail-rate percent**—To specify the failure rate threshold for uplink data or voice packets, use the **config advanced 802.11 coverage fail-rate** command

**config advanced 802.11{a | b} coverage level global clients**—To specify the minimum number of clients on an access point with an received signal strength indication(RSSI) value at or below the data or voice RSSI threshold, use the **config advanced 802.11 coverage level global** command

**config advanced 802.11{a | b} coverage {data | voice} packet-count packets**—To specify the minimum failure count threshold for uplink data or voice packets, use the **config advanced 802.11 coverage packet-count** command

**config advanced 802.11{a | b} coverage {data | voice} rssi-threshold rssi**—To specify the minimum receive signal strength indication (RSSI) value for packets that are received by an access point, use the **config advanced 802.11 coverage rssi-threshold** command

**config advanced 802.11{a | b} factory**—To reset 802.11a advanced settings back to the factory defaults, use the **config advanced 802.11 factory** command

**config advanced 802.11{a | b} group-member {add | remove} controller controller-ip-address**—To configure members in 802.11 static RF group, use the **config advanced 802.11 group-member** command

**config advanced 802.11{a | b} group-mode {auto | leader | off | restart}**—To set the 802.11a automatic RF group selection mode on or off, use the **config advanced 802.11 group-mode** command

**config advanced 802.11{a | b} logging channel {on | off}**—To turn the channel change logging mode on or off, use the **config advanced 802.11 logging channel** command

**config advanced 802.11{a | b} logging coverage {on | off}**—To turn the coverage profile logging mode on or off, use the **config advanced 802.11 logging coverage** command

**config advanced 802.11{a | b} logging foreign {on | off}**—To turn the foreign interference profile logging mode on or off, use the **config advanced 802.11 logging foreign** command

**config advanced 802.11{a | b} logging load {on | off}**—To turn the 802.11a load profile logging mode on or off, use the **config advanced 802.11 logging load** command

**config advanced 802.11{a | b} logging noise {on | off}**—To turn the 802.11a noise profile logging mode on or off, use the **config advanced 802.11 logging noise** command

**config advanced 802.11{a | b} logging performance {on | off}**—To turn the 802.11a performance profile logging mode on or off, use the **config advanced 802.11 logging performance** command

**config advanced 802.11{a | b} logging txpower {on | off}**—To turn the 802.11a transmit power change logging mode on or off, use the **config advanced 802.11 logging txpower** command

**config advanced 802.11{a | b} profile noise {global | cisco\_ap} dBm**—To set the 802.11a foreign noise threshold between -127 and 0 dBm, use the **config advanced 802.11 profile noise** command

**config advanced 802.11{a | b} profile throughput {global | cisco\_ap} value**—To set the Cisco lightweight access point data-rate throughput threshold between 1000 and 10000000 bytes per second, use the **config advanced 802.11 profile throughput** command

**config advanced 802.11{a | b} profile utilization {global | cisco\_ap} percent**—To set the RF utilization threshold between 0 and 100 percent, use the **config advanced 802.11 profile utilization** command. The operating system generates a trap when this threshold is exceeded

**config advanced 802.11{a | b} receiver {default | rxstart jumpThreshold value}**—To set the advanced receiver configuration settings, use the **config advanced 802.11 receiver** command

**config advanced 802.11{a | b} tpc-version {1 | 2}**—To configure the Transmit Power Control (TPC) version for a radio, use the **config advanced 802.11 tpc-version** command

**config advanced 802.11{a | b} tpcv1-thresh threshold**—To configure the threshold for Transmit Power Control (TPC) version 1 of a radio, use the **config advanced 802.11 tpcv1-thresh** command

**config advanced 802.11{a | b} tpcv2-intense intensity**—To configure the computational intensity for Transmit Power Control (TPC) version 2 of a radio, use the **config advanced 802.11 tpcv2-intense** command

**config advanced 802.11{a | b} tpcv2-per-chan {enable | disable}**—To configure the Transmit Power Control Version 2 on a per-channel basis, use the **config advanced 802.11 tpcv2-per-chan** command

**config advanced 802.11{a | b} tpcv2-thresh threshold**—To configure the threshold for Transmit Power Control (TPC) version 2 of a radio, use the **config advanced 802.11 tpcv2-thresh** command

**config advanced 802.11{a | b} txpower-update**—To initiate updates of the 802.11a transmit power for every Cisco lightweight access point, use the **config advanced 802.11 txpower-update** command

**config network rf-network-name name**—To set the RF-Network name, use the **config network rf-network-name** command

## Security Commands

### Show Commands

**show 802.11 { a | b | h }**—To display basic 802.11a, 802.11b/g, or 802.11h network settings, use the **show 802.11** command

**show aaa auth**— To display the configuration settings for the AAA authentication server database, use the **show aaa auth** command

**show database summary**—To display the maximum number of entries in the database, use the **show database summary** command

**show local-auth certificates**—To display local authentication certificate information, use the **show local-auth certificates** command

**show local-auth config**— To display local authentication configuration information, use the **show local-auth config** command.

**show local-auth statistics**—To display local Extensible Authentication Protocol (EAP) authentication statistics, use the **show local-auth statistics** command

**show netuser { detail *user\_name* | guest-roles | summary }**—To display the configuration of a particular user in the local user database, use the **show netuser** command

**show network summary**—To display the network configuration of the Cisco wireless LAN controller, use the **show network summary** command

**show radius acct detailed *radius\_index*** — To display RADIUS accounting server information, use the **show radius acct detailed** command

**show radius acct statistics** —To display the RADIUS accounting server statistics for the Cisco wireless LAN controller, use the **show radius acct statistics** command

**show radius auth detailed *radius\_index*** —To display RADIUS authentication server information, use the **show radius auth detailed** command.

**show radius summary**—To display the RADIUS authentication and accounting server summary, use the **show radius summary** command

**show radius auth statistics**—To display the RADIUS authentication server statistics for the Cisco wireless LAN controller, use the **show radius auth statistics** command

## Config Commands

**config aaa auth mgmt [ radius | tacacs ]**—To configure the order of authentication when multiple databases are configured, use the **config aaa auth mgmt** command

```
config radius acct { {add index IP addr port {ascii | hex} secret} | delete index | disable
 index | enable index | ipsec {authentication {hmac-md5 index | hmac-sha1 index }
 | disable index | enable index | encryption {256-aes | 3des | aes | des} index | ike {auth-mode
 {pre-shared-key index type shared_secret_key | certificate index }
 | dh-group { 2048bit-group-14 | group-1 | group-2 | group-5} index | lifetime seconds index
 | phasel {aggressive | main} index } } | {mac-delimiter {colon
 | hyphen | none | single-hyphen}} | {network index {disable | enable}} | {region {group |
 none | provincial}}
```

| retransmit-timeout index seconds | realm {add | delete} index realm-string}  
To configure settings for a RADIUS accounting server for the Cisco wireless LAN controller, use the **config radius acct** command

```
config radius auth {add index IP addr portascii/hexsecret} | {callStationIdType
 {ap-ethmac-only | ap-ethmac-ssid | ap-group-name | ap-label-address | ap-label-address-ssid
 | ap-location | ap-macaddr-only | ap-macaddr-ssid | ap-name | ap-name-ssid | flex-group-name
 | ipaddr | macaddr | vlan-id}} | delete index | disable index | enable index |
 { ipsec {authentication {hmac-md5 index | hmac-sha1 index } | disable index | enable index
 | encryption {256-aes | 3des | aes | des} index
 | ike {auth-mode {pre-shared-key index ascii/hex shared_secret | certificate index }
 | dh-group { 2048bit-group-14 | group-1 | group-2 | group-5} index
 | lifetime seconds index | phasel {aggressive | main} index } } | { {keywrap {add ascii/hex
 kek mack index } | delete index | disable | enable} }
 | {mac-delimiter {colon | hyphen | none | single-hyphen}} | {(management index {enable
 | disable}} | { mgmt-retransmit-timeout index Retransmit Timeout }
 | { network index {enable | disable}} | {realm {add | delete} radius-index realm-string} }
 | {region {group | none | provincial}} | {retransmit-timeout index RetransmitTimeout}
 | { rfc3576 {enable | disable} index } - To configure settings for a RADIUS authentication
 server for the Cisco wireless LAN controller, use the config radius auth command.
```

**config radius acct network index {enable | disable}** —To configure a default RADIUS server for network users, use the **config radius acct network** command

**config radius auth network index {enable | disable}** —To configure a default RADIUS server for network users, use the **config radius auth network** command



**config netuser add username password {wlan wlan\_id | guestlan guestlan\_id} userType guest lifetime lifetime description description**—To add a guest user on a WLAN or wired guest LAN to the local user database on the controller, use the **config netuser add** command.

**config netuser delete { username username | wlan-id wlan-id}**—To delete an existing user from the local network, use the **config netuser delete** command

**config netuser description username description**—To add a description to an existing net user, use the **config netuser description** command.

**config radius acct{ [add index IP addr port {ascii | hex} secret] | delete index | disable index | enable index | ipsec {authentication {hmac-md5 index | hmac-sha1 index } | disable index | enable index | encryption{256-aes| 3des| aes|des} index | ike {auth-mode {pre-shared-key index type shared\_secret\_key | certificate index } | dh-group { 2048bit-group-14 | group-1 | group-2 | group-5} index | lifetime seconds index | phase1 {aggressive | main} index } } | {mac-delimiter {colon | hyphen | none | single-hyphen}} | {network index {disable | enable}} | {region {group | none | provincial}} | retransmit-timeout index seconds | realm {add | delete} index realm-string}**

**config local-auth eap-profile { [ add | delete ] profile\_name | cert-issuer { cisco | vendor } | method method local-cert { enable | disable } profile\_name | method method client-cert { enable | disable } profile\_name | method method peer-verify ca-issuer { enable | disable } | method method peer-verify cn-verify { enable | disable } | method method peer-verify date-valid { enable | disable } }** — To configure local Extensible Authentication Protocol (EAP) authentication profiles, use the **config local-auth eap-profile** command

## System Management Commands

**show snmpcommunity**—To display Simple Network Management Protocol (SNMP) community entries, use the **show snmpcommunity** command

**show snmptrap**— To display Cisco wireless LAN controller Simple Network Management Protocol (SNMP) trap receivers and their status, use the **show snmptrap** command

**show snmpv3user**—To display Simple Network Management Protocol (SNMP) version 3 configuration, use the **show snmpv3user** command

**show snmpversion**—To display which versions of Simple Network Management Protocol (SNMP) are enabled or disabled on your controller, use the **show snmpversion** command

**config snmp community accessmode { ro | rw } name**—To modify the access mode (read only or read/write) of an SNMP community, use the **config snmp community accessmode** command

**config snmp community create name**—To create a new SNMP community, use the **config snmp community create** command

**config snmp community delete name**—To delete an SNMP community, use the **config snmp community delete** command

**config snmp community mode { enable | disable } name**— To enable or disable an SNMP community, use the **config snmp community mode** command

**config snmp trapreceiver create name IP addr**—To configure a server to receive SNMP traps, use the **config snmp trapreceiver create** command

**config snmp trapreceiver delete name**—To delete a server from the trap receiver list, use the **config snmp trapreceiver delete** command

**config snmp trapreceiver mode** { **enable** | **disable** } *name*— To send or disable sending traps to a selected server, use the **config snmp trapreceiver mode** command

**config snmp v3user create** *username* { **ro** | **rw** } { **none** | **hmacmd5** | **hmacsha** } { **none** | **des** | **aescfb128** } [ *auth\_key* ] [ *encrypt\_key* ]— To create a version 3 SNMP user, use the **config snmp v3user create** command

**config snmp v3user delete** *username*— To delete a version 3 SNMP user, use the **config snmp v3user delete** command

**config snmp version** { **v1** | **v2** | **v3** } { **enable** | **disable** }— To enable or disable selected SNMP versions, use the **config snmp version** command

**show sysinfo**—To display high-level Cisco wireless LAN controller information, use the **show sysinfo** command.

**show time** —To display the Cisco wireless LAN controller time and date, use the **show time** command

**show band-select** —To display band selection information, use the **show band-select** command

**transfer download datatype** { **eapdevcert** | **eapcert** }—To set the download file type, use the **transfer download datatype** command

## UX Regulatory Domain Commands

**config wlan disable 1** —To disable WLAN 1

**config wlan universal-ap-admin enable 1** —To enable as universal-ap-admin for wlan 1

**config wlan enable 1**—To enable WLAN 1

**config wlan enable 1**—To enable WLAN 1

## VRRP Command

**config ap next-preferred-master**—To configure the primary AP that has been elected to take over as the new primary AP

**show ap next-preferred-master**—To display the status of the primary AP

**clear ap next-preferred-master**—To clear the configuration of the primary AP

## WGB Commands

**show wgb summary**—To display the summary of workgroup bridges

**show wgb detail *WGB\_MAC***—To display the details of a specific workgroup bridge

# WLAN Commands

## Config Commands

**config wlan security wpa wpa2 enable** *wlan\_id*—To enable WPA2, use the **config wlan security wpa wpa2 enable** command

**config wlan security wpa wpa2 disable** *wlan\_id*—To disable WPA2, use the **config wlan security wpa wpa2 disable** command

**config wlan security wpa wpa2 ciphers** {**aes** | **tkip**} {**enable** | **disable**} *wlan\_id*—To configure WPA2 ciphers and enable or disable Advanced Encryption Standard (AES) or Temporal Key Integrity Protocol (TKIP) data encryption for WPA2, use the **config wlan security wpa wpa2 ciphers** command

**config wlan security wpa akm 802.1x** {**enable** | **disable**} *wlan\_id*—To configure authentication key-management (AKM) using 802.1X, use the **config wlan security wpa akm 802.1x** command

**config wlan radio** *wlan\_id* {**all** | **802.11a** | **802.11bg** | **802.11g** | **802.11ag**}—To set the Cisco radio policy on a wireless LAN, use the **config wlan radio** command

**config wlan** {**enable** | **disable** | **create** | **delete**} *wlan\_id* [*name* | **all** ]—To create, delete, enable, or disable a wireless LAN, use the **config wlan** command

**config wlan band-select allow** {**enable** | **disable**} *wlan\_id*—To configure band selection on a WLAN, use the **config wlan band-select allow** command

**config wlan broadcast-ssid** {**enable** | **disable**} *wlan\_id*—To configure an Service Set Identifier (SSID) broadcast on a wireless LAN, use the **config wlan broadcast-ssid** command

**config wlan qos** *wlan\_id* {**bronze** | **silver** | **gold** | **platinum**}—To change the quality of service (QoS) for a wireless LAN, use the **config wlan qos** command

**config wlan radius\_server acct** {**enable** | **disable**} *wlan\_id* | **add** *wlan\_id server\_id* | **delete** *wlan\_id* {**all** | *server\_id* } | **framed-ipv6** {**address** | **both** | **prefix**} *wlan\_id* }—To configure RADIUS accounting servers of a WLAN, use the **config wlan radius\_server acct** command

**config wlan radius\_server auth** {**enable** *wlan\_id* | **disable** *wlan\_id* } {**add** *wlan\_id server\_id* | **delete** *wlan\_id* {**all** | *server\_id* } } - To configure RADIUS authentication servers of a WLAN, use the **config wlan radius\_server auth** command

**config wlan security 802.1X** {**enable** { *wlan\_id* } | **disable** { *wlan\_id* } | } }—To change the state of 802.1X security on the wireless LAN Cisco radios, use the **config wlan security 802.1X** command

**config wlan security wpa akm cckm** {**enable** *wlan\_id* | **disable** *wlan\_id* | *timestamp-tolerance* }—To configure authentication key-management using Cisco Centralized Key Management (CCKM), use the **config wlan security wpa akm cckm** command

**config wlan security wpa akm psk** {**enable** | **disable** | **set-key** *key-format key* } *wlan\_id*—To configure the Wi-Fi protected access (WPA) preshared key mode, use the **config wlan security wpa akm psk** command

**config wlan security wpa wpa2** {**enable** | **disable**} *wlan\_id*—To enable/disable WPA2, use the **config wlan security wpa wpa2 enable/disable** command

**config wlan ssid** *wlan\_id ssid*—To edit an SSID associated to a WLAN, use the **config wlan ssid** command

**config wlan security wpa akm ft** [ **over-the-air** | **over-the-ds** | **psk** | [ **reassociation-timeout** *seconds* ] ] { **enable** | **disable** } *wlan\_id* —To configure authentication key-management using 802.11r fast transition 802.1X, use the **config wlan security wpa akm ft** command

**config wlan security ft** { **enable** | **disable** | **reassociation-timeout** *timeout-in-seconds* } *wlan\_id* — To configure 802.11r fast transition parameters, use the **config wlan security ft** command

**config wlan security ft** { **enable** | **disable** | **reassociation-timeout** *timeout-in-seconds* } *wlan\_id* — To configure 802.11r fast transition parameters, use the **config wlan security ft** command

**config wlan security wpa akm cckm** { **enable** *wlan\_id* | **disable** *wlan\_id* | **timestamp-tolerance** }— To configure authentication key-management using Cisco Centralized Key Management (CCKM), use the **config wlan security wpa akm cckm** command

**config 802.11** { **a** | **b** } **cac voice acm** { **enable** | **disable** }— To enable or disable bandwidth-based voice Call Admission Control (CAC) for the 802.11a or 802.11b/g network, use the **config 802.11 cac voice acm** command

**config 802.11** { **a** | **b** } **cac voice tspec-inactivity-timeout** { **enable** | **ignore** }— To process or ignore the Wi-Fi Multimedia (WMM) traffic specifications (TSPEC) inactivity timeout received from an access point, use the **config 802.11 cac voice tspec-inactivity-timeout** command

**config 802.11** { **a** | **b** } **cac voice stream-size** *stream\_size number* **mean\_datarate max-streams mean\_datarate** — To configure the number of aggregated voice Wi-Fi Multimedia (WMM) traffic specification (TSPEC) streams at a specified data rate for the 802.11a or 802.11b/g network, use the **config 802.11 cac voice stream-size** command

**config 802.11** { **a** | **b** } **cac voice max-bandwidth** *bandwidth* — To set the percentage of the maximum bandwidth allocated to clients for voice applications on the 802.11a or 802.11b/g network, use the **config 802.11 cac voice max-bandwidth** command

**config 802.11** { **a** | **b** } **cac voice roam-bandwidth** *bandwidth* — To configure the percentage of the Call Admission Control (CAC) maximum allocated bandwidth reserved for roaming voice clients on the 802.11a or 802.11b/g network, use the **config 802.11 cac voice roam-bandwidth** command

**config 802.11** { **a** | **b** } **cac voice load-based** { **enable** | **disable** }— To enable or disable load-based Call Admission Control (CAC) for the 802.11a or 802.11b/g network, use the **config 802.11 cac voice load-based** command

**config 802.11** { **a** | **b** } **cac voice max-calls** *number* — To configure the maximum number of voice call supported by the radio, use the **config 802.11 cac voicemax-calls** command



**Note** Do not use the **config 802.11 cac voice max-calls** command if the SIP call snooping feature is disabled and if the SIP based Call Admission Control (CAC) requirements are not met

**config 802.11** { **a** | **b** } **cac voice sip bandwidth** *bw\_kbps sample-interval number\_msecs* —To configure the bandwidth that is required per call for the 802.11a or 802.11b/g network, use the **config 802.11 cac voice sip bandwidth** command



**Note** SIP bandwidth and sample intervals are used to compute per call bandwidth for the SIP-based Call Admission Control (CAC).

**config 802.11 { a | b } cac voice sip codec { g711 | g729 } sample-interval *number\_msecs*** — To configure the Call Admission Control (CAC) codec name and sample interval as parameters and to calculate the required bandwidth per call for the 802.11a or 802.11b/g network, use the **config 802.11 cac voice sip codec** command

**config 802.11 { a | b } cac voice stream-size *stream\_size number mean\_datarate max-streams mean\_datarate*** — To configure the number of aggregated voice Wi-Fi Multimedia (WMM) traffic specification (TSPEC) streams at a specified data rate for the 802.11a or 802.11b/g network, use the **config 802.11 cac voice stream-size** command

## Show Commands

**show wlan { apgroups | summary | *wlan\_id* }**—To display configuration information for a specified wireless LAN or a foreign access point, or to display wireless LAN summary information, use the **show wlan** command

**show client wlan *wlan\_id* [ devicetype *device* ]**—To display the summary of clients associated with a WLAN, use the **show client wlan** command.

**show client summary [ *ssid / ip / username / devicetype* ]**—To display a summary of clients associated with a Cisco lightweight access point, use the **show client summary** command

**show client detail *mac\_address*** —To display detailed information for a client on a Cisco lightweight access point, use the **show client detail** command

