# User Guide for Cisco Catalyst Wireless Mobile Application, Cisco Wireless Release 1.2

**First Published:** 2021-09-29

**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 NONINFRINGEMENT 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.

# CONTENTS

PREFACE

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

# Preface

This preface describes the conventions of this document and information on how to obtain other documentation. It also provides information on what's new in Cisco product documentation.

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

- Document Conventions , on page v
- Related Documentation, on page vii
- Obtaining Documentation and Submitting a Service Request, on page vii

# Document Conventions

This document uses the following conventions:

| Convention | Description |
|---|---|
| ^ or Ctrl | Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.) |
| **bold** font | Commands and keywords and user-entered text appear in **bold** font. |
| *Italic* font | Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font. |
| `Courier` font | Terminal sessions and information the system displays appear in `courier` font. |
| **`Bold Courier`** font | **`Bold Courier`** font indicates text that the user must enter. |
| [x] | Elements in square brackets are optional. |

| Convention | Description |
|---|---|
| ... | An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated. |
| \| | A vertical line, called a pipe, indicates a choice within a set of keywords or arguments. |
| [x \| y] | Optional alternative keywords are grouped in brackets and separated by vertical bars. |
| {x \| y} | Required alternative keywords are grouped in braces and separated by vertical bars. |
| [x {y \| z}] | Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element. |
| string | A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks. |
| < > | Nonprinting characters such as passwords are in angle brackets. |
| [ ] | Default responses to system prompts are in square brackets. |
| !, # | An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line. |

### Reader Alert Conventions

This document may use 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 do something that could result in equipment damage or loss of data.

**Timesaver** Means *the described action saves time.* You can save time by performing the action described in the paragraph.

**Warning** IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

# Related Documentation

**Note** Before installing or upgrading the CiscoEmbedded Wireless Controller, refer to the release notes.

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

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

# Overview of the Cisco Catalyst Wireless Mobile Application

## Information About the Cisco Catalyst Wireless Mobile Application

The Cisco Catalyst Wireless mobile application helps you to set up and deploy a Cisco Embedded Wireless Controller network easily and conveniently.

This mobile application provides the following key benefits:

- Provision Cisco Embedded Wireless Controller with best practices enabled
- Monitor real-time performance of the Cisco Embedded Wireless Controller network
- Manage the Cisco Embedded Wireless Controller network

For more information about the Cisco Embedded Wireless Controller, see the *Cisco Embedded Wireless Controller on Catalyst Access Points Configuration Guide*.

## Supported Operating Systems

The Cisco Catalyst Wireless mobile application is compatible with mobile devices that meet the following platform requirements:

- Android 8 +
- iOS 12 +

CHAPTER 2

# Download and Install the Cisco Catalyst Mobile Application

## Download and Installation

The Cisco Catalyst Wireless mobile application is available for download from the following locations:

- **Apple App Store:** For iOS devices
- **Google Play Store:** For Android devices

Depending on where you download the Cisco Catalyst Wireless mobile app from, follow the instructions given in the Apple App Store or the Google Play Store.

## Troubleshooting App Installation

The following are some common installation issues and workarounds:

**Issue**: The Cisco Catalyst Wireless mobile application repeatedly crashes or malfunctions.

**Solution**: Try restarting the app. If this does not resolve the app malfunction, write to catalyst-wireless-app-feedback@external.cisco.com.

CHAPTER 3

# Getting Started with the Cisco Catalyst Wireless Mobile Application

## Prerequisites for App Usage

To enable convenient usage and proper functioning of the Cisco Catalyst Wireless mobile app, ensure that the app is granted the following permissions on your mobile device:

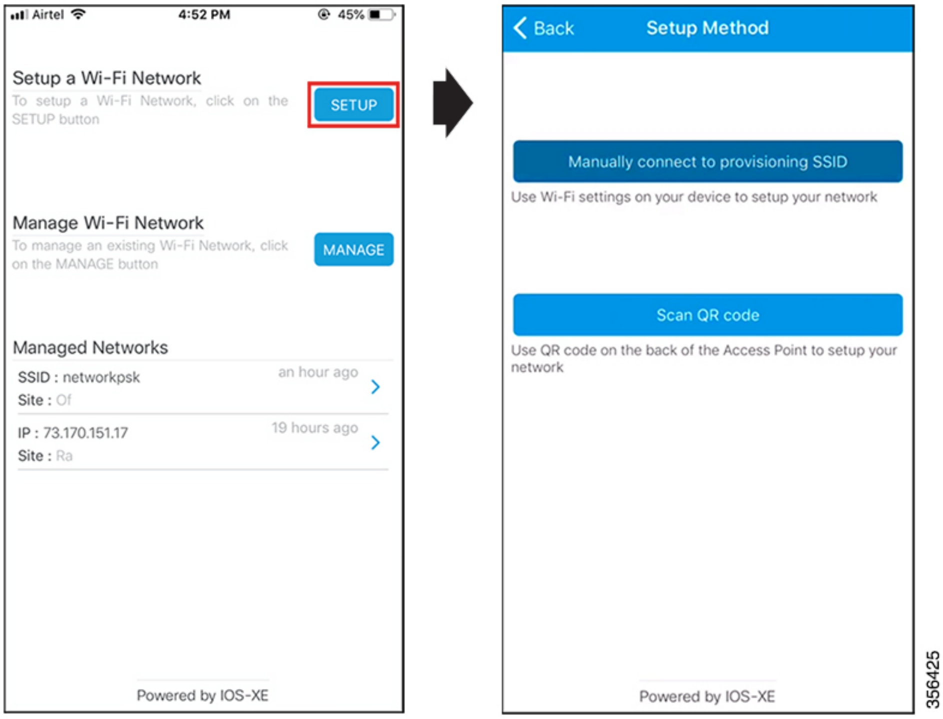
- Location permission on your mobile device (all Android devices and Apple devices with iOS Version 13 and later).
- Permission to access the mobile device camera to enable auto provisioning through QR code scanning.

## Setting Up a Wi-Fi Network

Use the Cisco Catalyst Wireless Mobile App to set up the Wi-Fi network for your Cisco Embedded Wireless Controller deployment by performing the procedures provided here, in the same order. The following sections also provide information about connecting to the provisioning SSID:

# Connecting to the Provisioning SSID

*Figure 1: Landing Screen and Provisioning Screen of the Cisco Catalyst Wireless Mobile App*



Setup a Wi-Fi Network

To setup a Wi-Fi Network, click on the SETUP button

Manage Wi-Fi Network

To manage an existing Wi-Fi Network, click on the MANAGE button

Managed Networks

SSID : networkpsk — an hour ago
Site : Of

IP : 73.170.151.17 — 19 hours ago
Site : Ra

Powered by IOS-XE

Use Wi-Fi settings on your device to setup your network

Use QR code on the back of the Access Point to setup your network

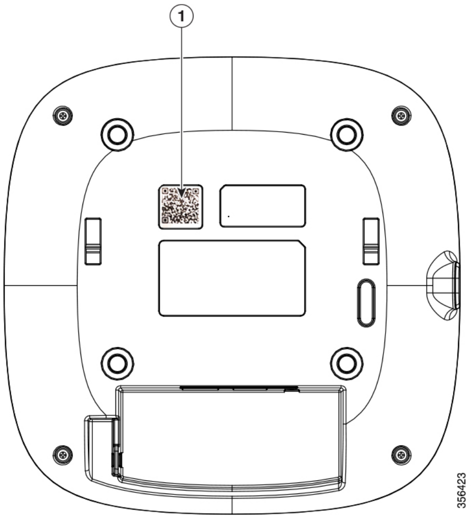
Powered by IOS-XE

To connect to the provisioning SSID, use either of the following methods.

## Scanning the QR code

1. You can locate the QR code at the back of your Cisco Catalyst Series access point.

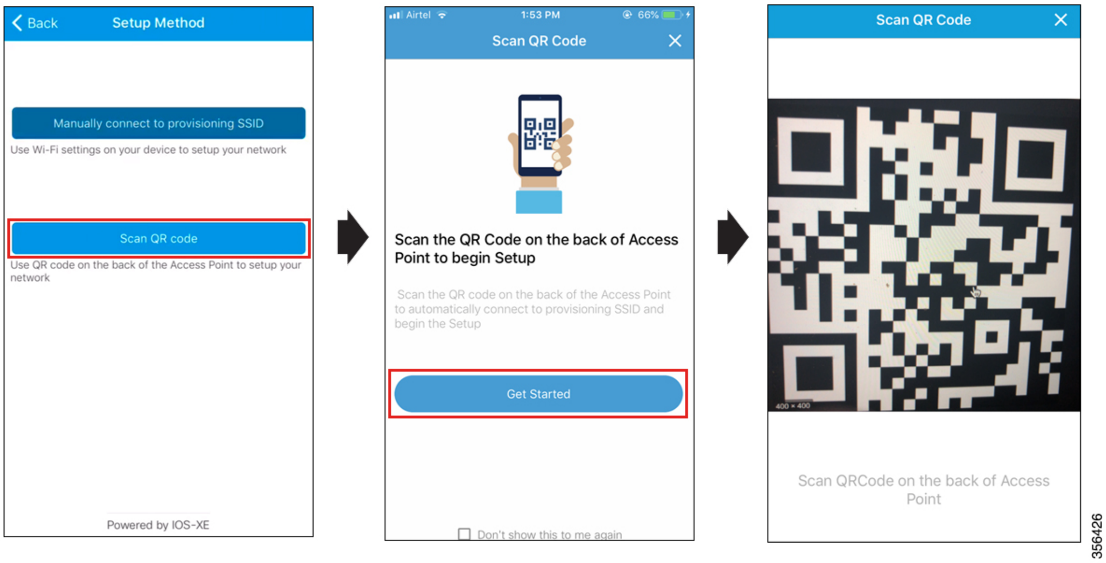
*Figure 2: Back view of Cisco Catalyst 9120AX Series AP*



| | |
|---|---|
| 1 | Location of the QR code at the back of the Cisco Catalyst 9120AX Series AP |

2. If the access point is capable of becoming a Cisco Embedded Wireless Controller, you can use the Cisco Catalyst Wireless mobile app to scan this QR code and automatically provision the AP to set up your Wi-Fi network.

*Figure 3: Scanning the QR code on the AP using the Cisco Catalyst Wireless mobile app*



Use Wi-Fi settings on your device to setup your network

Use QR code on the back of the Access Point to setup your network

Scan the QR Code on the back of Access Point to begin Setup

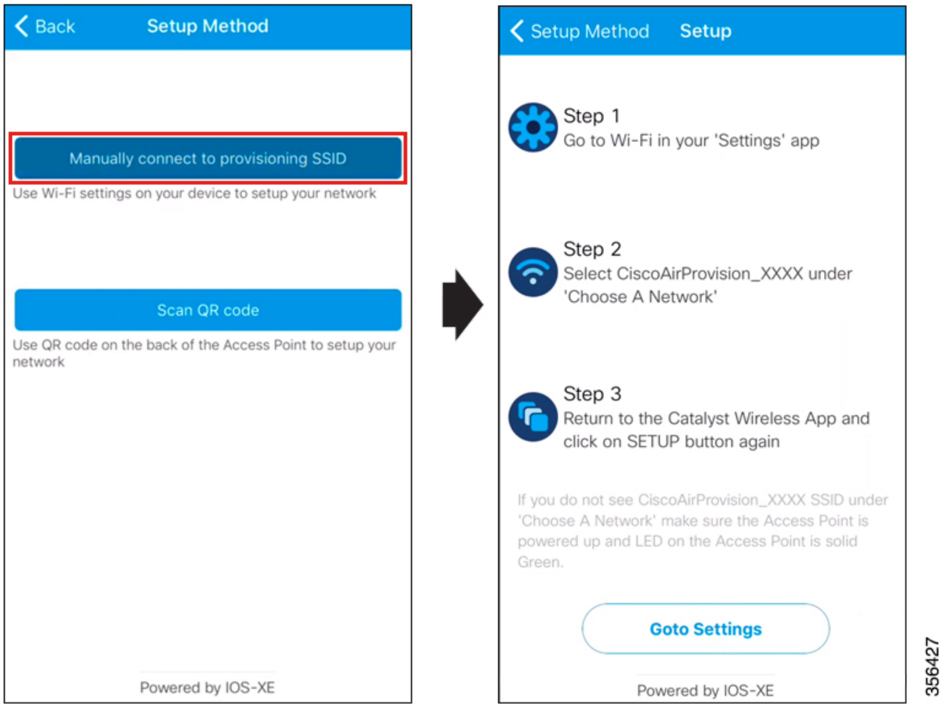
Scan the QR code on the back of the Access Point to automatically connect to provisioning SSID and begin the Setup

Scan QRCode on the back of Access Point

3. To initiate day zero configuration, follow the instructions in the Logging in to the Day 0 Wizard, on page 9 from Step 3.

# Manually Connecting to the Provisioning SSID

*Figure 4: Manually Connecting to the Provisioning SSID Using the Cisco Catalyst Wireless Mobile App*



Use Wi-Fi settings on your device to setup your network

Use QR code on the back of the Access Point to setup your network

Powered by IOS-XE

Step 1
Go to Wi-Fi in your 'Settings' app

Step 2
Select CiscoAirProvision_XXXX under 'Choose A Network'

Step 3
Return to the Catalyst Wireless App and click on SETUP button again

If you do not see CiscoAirProvision_XXXX SSID under 'Choose A Network' make sure the Access Point is powered up and LED on the Access Point is solid Green.

Powered by IOS-XE

**Step 1** In your mobile device, under **Settings**, go to **Wi-Fi**.

**Step 2** Under **Choose A Network**, tap CiscoAirProvision-xxxx from the list of available SSIDs.

**Step 3** In the **Password** field, enter the default password for the CiscoAirProvision-xxxx SSID.

**Step 4** Tap **Join**.

Your mobile device is now connected to the CiscoAirProvision-xxxx SSID.

### What to do next

To initiate day zero configuration, return to the Landing screen of the app, and follow the instructions provided in Logging in to the Day 0 Wizard, on page 9.

## Troubleshooting the Task of Connecting to the Provisioning SSID

**Problem** During SSID provisioning on your Android device, the login screen is repeatedly displayed in the mobile device browser.

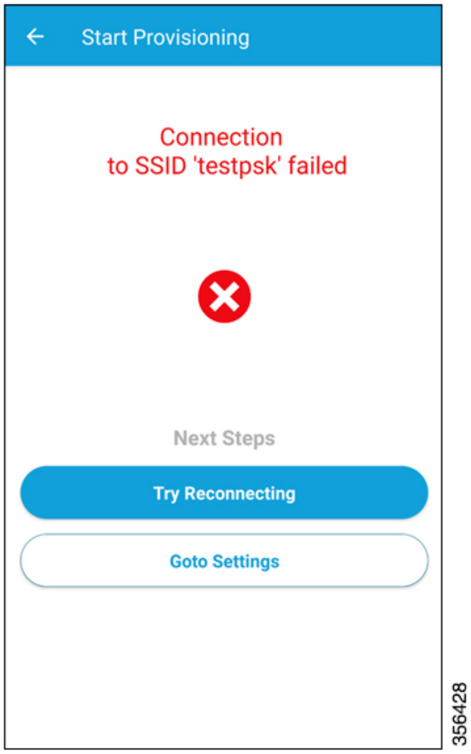
**Solution** Manually navigate to the Cisco Catalyst Wireless mobile app to continue using it.

**Problem** Your mobile device is connected to the corresponding SSID, but the error message "`Please check your Wi-Fi connection and try again`" is displayed. This error might also appear during the Day 1 setup.

**Solution** Switch off your mobile data and connect to the provisioning SSID.

**Problem** In Android 6.0 (Marshmallow) or later versions, you may see the error message "`Connection to SSID ssid-name failed`" even after repeated attempts to reconnect to the corresponding SSID. For more details, see https://developer.android.com/about/versions/marshmallow/android-6.0-changes#behavior-network. This error might also appear during Day 1 setup.

*Figure 5: Error Message in Android 6.0 and Later Versions While Connecting to the SSID*



Start Provisioning

Connection
to SSID 'testpsk' failed

Next Steps

**Solution** Navigate to **Settings** > **Wi-Fi** > **Choose A Network** and do one of the following:

- **Solution** Navigate to the corresponding SSID, and tap **Forget**. Wait for a couple of minutes and then return to the Cisco Catalyst Wireless mobile app to continue usage.
- **Solution** Manually connect to the corresponding SSID and return to the Cisco Catalyst Wireless mobile app.

# Provisioning the Network

The following sections provide information about the tasks involved in provisioning the network.

## Logging in to the Day 0 Wizard

### Before you begin

Your mobile device must be connected to the CiscoAirProvision-xxxx SSID.

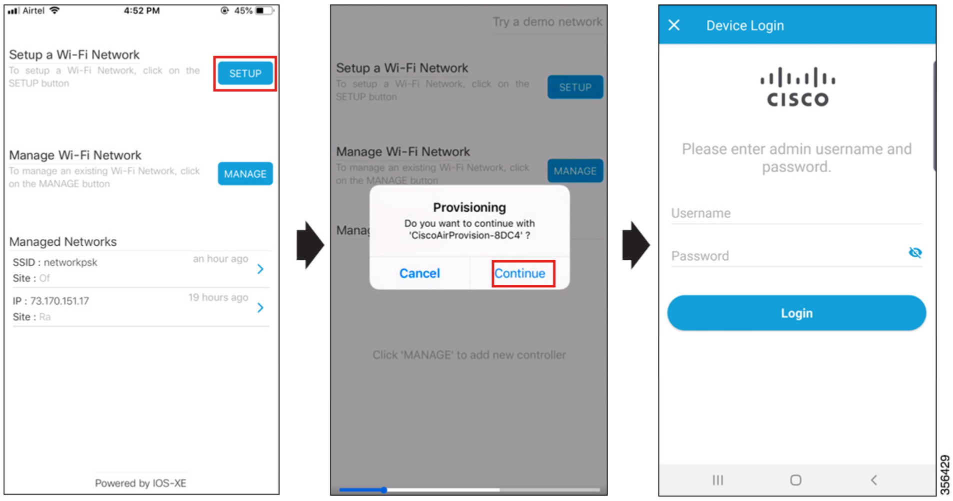
**Step 1** In your mobile device, under **Setup a Wi-Fi Network**, tap **Setup**.

The **Provisioning** screen is displayed.

**Step 2** Tap **Continue** to proceed with the configuration.

The **Device Login** screen for your Cisco Embedded Wireless Controller network is displayed.

***Figure 6: Logging in to the Day Zero Wizard***


Airtel
4:52 PM
45%
Setup a Wi-Fi Network
To setup a Wi-Fi Network, click on the SETUP button
SETUP
Manage Wi-Fi Network
To manage an existing Wi-Fi Network, click on the MANAGE button
MANAGE
Managed Networks
SSID : networkpsk
an hour ago
Site : Of
IP : 73.170.151.17
19 hours ago
Site : Ra
Powered by IOS-XE
Try a demo network
Setup a Wi-Fi Network
To setup a Wi-Fi Network, click on the SETUP button
SETUP
Manage Wi-Fi Network
To manage an existing Wi-Fi Network, click on the MANAGE button
MANAGE
Manag
Provisioning
Do you want to continue with 'CiscoAirProvision-8DC4' ?
Cancel
Continue
Click 'MANAGE' to add new controller
Device Login
CISCO
Please enter admin username and password.
Username
Password
Login
356429

**Step 3** In the **Device Login** screen, enter the default admin credentials. The default **Username** is **`webui`** and **Password** is **`cisco`**.

**Step 4** Tap **Login**.

## Overview of the Day Zero Wizard

The day zero wizard of the Cisco Catalyst Wireless mobile app helps in the initial setup of your Cisco Embedded Wireless Controller network. You can configure certain basic parameters on the controller and network parameters to get your Cisco Embedded Wireless Controller network running.

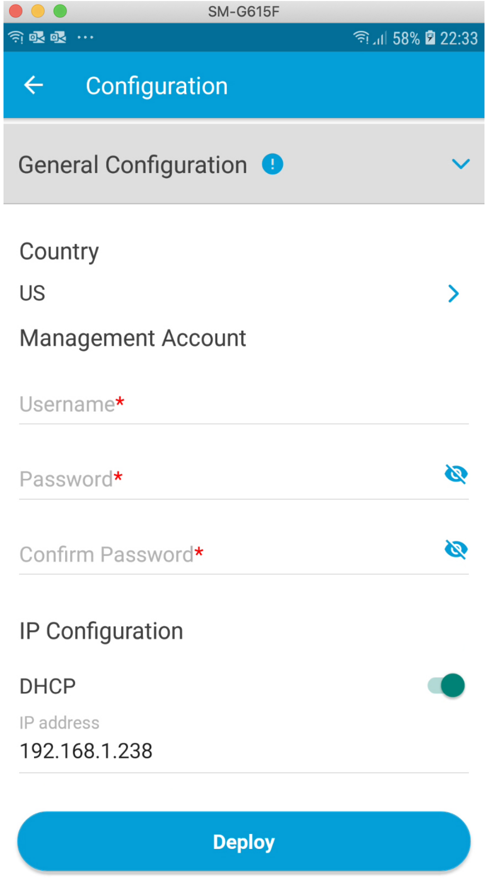
# Initial Network Configuration

After you log in to the day zero wizard of the Cisco Catalyst Wireless mobile application, perform the following steps to configure the basic settings for your Cisco Embedded Wireless Controller network:

**Step 1** In the **Configuration** screen, under **General Configuration**, tap the **Country** drop-down list and select a country.

**Step 2** Tap **Management Account** and enter the required management credentials.

*Figure 7: Day Zero Wizard - General Configuration*



General Configuration

Country

US

Management Account

Username*

Password*

Confirm Password*

IP Configuration

DHCP

IP address

192.168.1.238

**Step 3** Under **IP Configuration**, do one of the following:

- **DHCP**: Enable the DHCP option to get a dynamic management IP address.
- **IP Address**: Enter the static management IP address for the controller interface.

**Step 4** Under the **Configuration Mode**, do one of the following:

a) **Non Mesh**: Enable the nonmesh configuration mode.

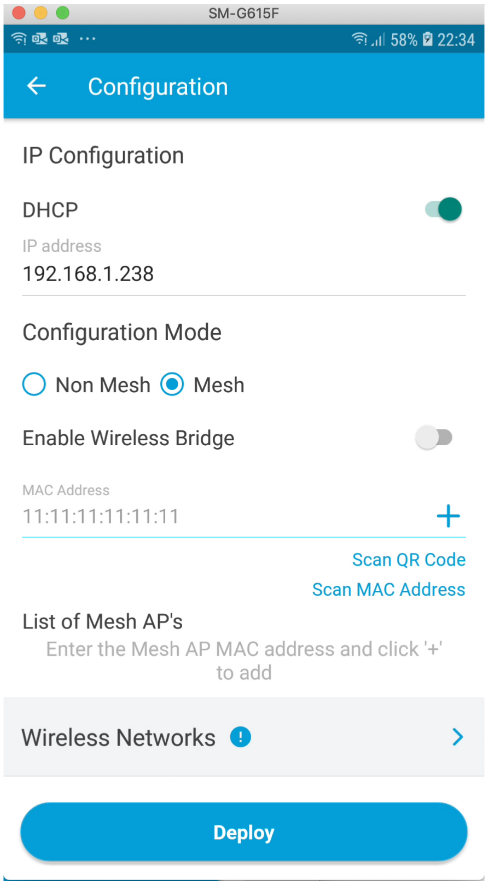
b) **Mesh**: Enable the mesh configuration mode and provide the following:

1. **Enable Wireless Bridge**: Slide the toggle button to enable or disable the wireless bridge.
2. **MAC Address**: Enter the MAC address of the mesh AP MAC address. Tap + to add a MAC address to the list of mesh AP MAC addresses.

   Additionally, you can enter MAC addresses by tapping the **Scan QR Code** link and scanning the MAC addresses, and by scanning the image to read the MAC addresses.

   **List of Mesh APs**: Tap the delete icon to clear the list of MAC addresses on the mesh APs.

*Figure 8: Day Zero Wizard - Configuration Mode*



IP Configuration

DHCP: on

IP address: 192.168.1.238

Configuration Mode

○ Non Mesh ● Mesh

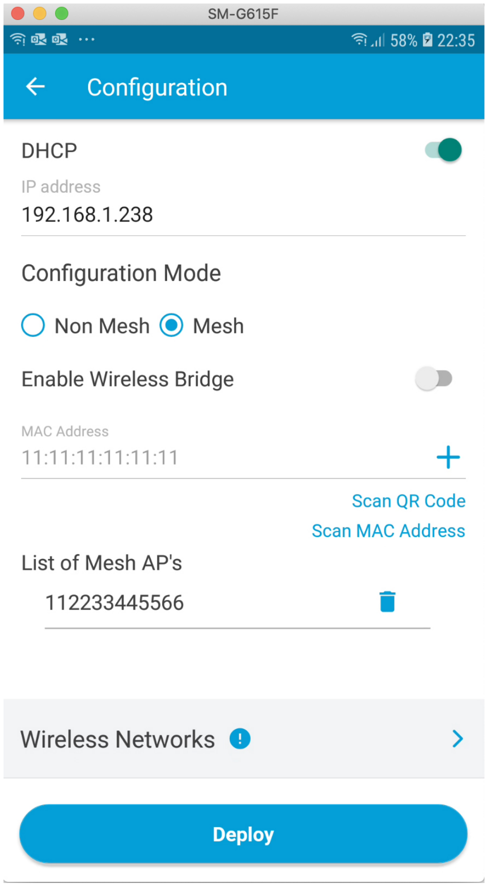
Enable Wireless Bridge: off

MAC Address: 11:11:11:11:11:11 +

List of Mesh AP's

Enter the Mesh AP MAC address and click '+' to add

*Figure 9: List of Mesh APs*


SM-G615F

58% 22:35

Configuration

DHCP ●

IP address
192.168.1.238

Configuration Mode

○ Non Mesh ● Mesh

Enable Wireless Bridge ○

MAC Address
11:11:11:11:11:11 +

Scan QR Code
Scan MAC Address

List of Mesh AP's

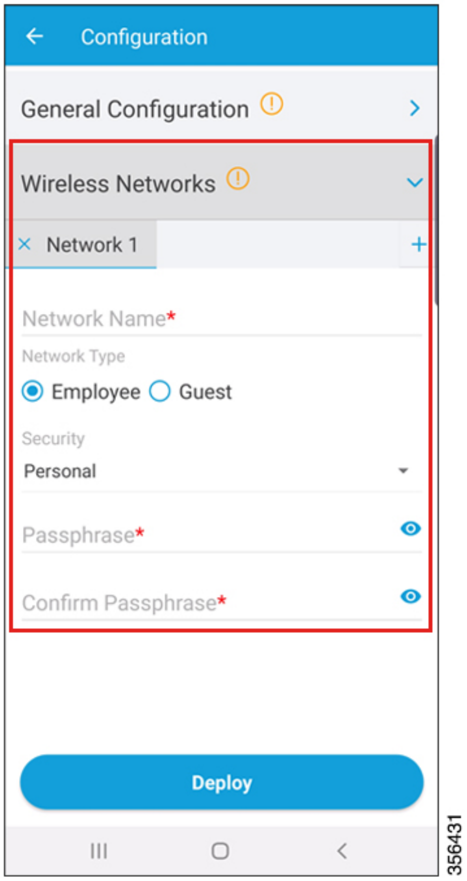
112233445566

Wireless Networks

Deploy

**Step 5** Under **Wireless Networks**, tap the + icon to add a network SSID.

*Figure 10: Day Zero Wizard – Wireless Network Configuration*



Network Name*

Network Type

● Employee ○ Guest

Security

Personal

Passphrase*

Confirm Passphrase*

**Step 6** In the **Network Name** field, enter a name.

**Step 7** Under the **Network Type**, tap either the **Employee** or the **Guest** radio button.

**Step 8** From the **Security** drop-down list, choose the required security type.

- If you selected **Employee** in the previous step, the available options are **Personal** or **Enterprise**.

  The default security type is **Personal**. For more information about configuring **Enterprise** security, see the Configuring the AAA Server section.

- If you selected **Guest** in the previous step, the security type is fixed as **Consent**. Go to Step 11.

- If you selected **Employee** in the previous step, then continue from Step 9.

**Step 9** In the **Passphrase** field, enter a passcode.

**Step 10** In the **Confirm Passphrase** field, re-enter the passcode.

**Step 11** Tap **Deploy**.

A confirmation message is displayed.

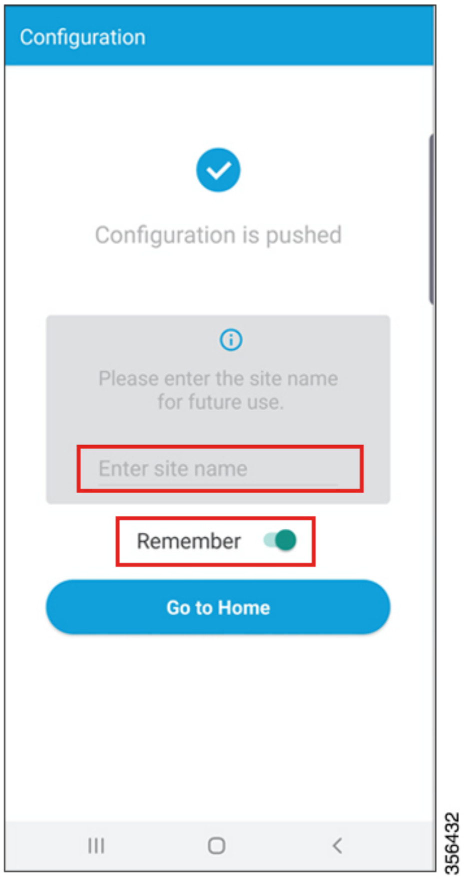
**Step 12** (Optional) Tap **Review** to review the configured network settings.

The **Summary** screen is displayed. Here, you can view and edit the **General Configuration** and **Wireless Network** settings.

**Step 13** Tap **Deploy**.

A confirmation screen is displayed. Here, you can enter the site name and opt to **Remember** the configured site.

*Figure 11: Day Zero Wizard – Confirmation Screen*



Configuration is pushed

Please enter the site name for future use.

# Feedback and Support

To submit feedback or to receive support for the Cisco Catalyst Wireless mobile application, write to catalyst-wireless-app-feedback@external.cisco.com.

CHAPTER 4

# Managing the Wi-Fi Network

Under **Manage Wi-Fi Network** > **Manage**, you can add, modify, or delete a previously configured employee or guest network. You can also modify AP details.

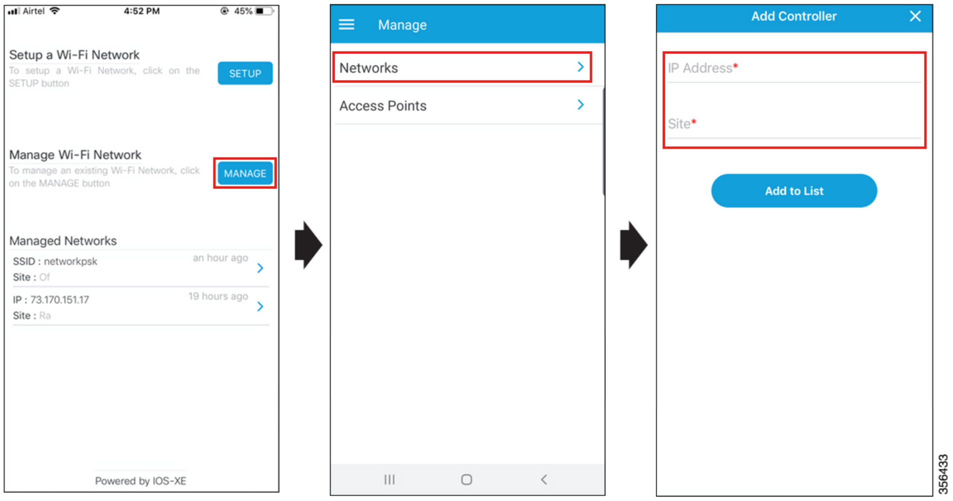
Under **Managed Networks**, you can find your list of configured embedded wireless controllers that are being managed by the Cisco Catalyst Wireless mobile app.

Also, if you enable the **Remember** toggle button in the **Confirmation Screen** of the Day Zero wizard (Figure 11: Day Zero Wizard – Confirmation Screen), the corresponding controller is added to the **Managed Networks** list.

You can add a new embedded wireless controller to be managed by the Cisco Catalyst Wireless mobile app using one of the the following options. These controllers are listed under **Managed Networks**.

- IP Address
- SSID

*Figure 12: Add an Embedded Wireless Controller Using the Cisco Catalyst Wireless Mobile Application*



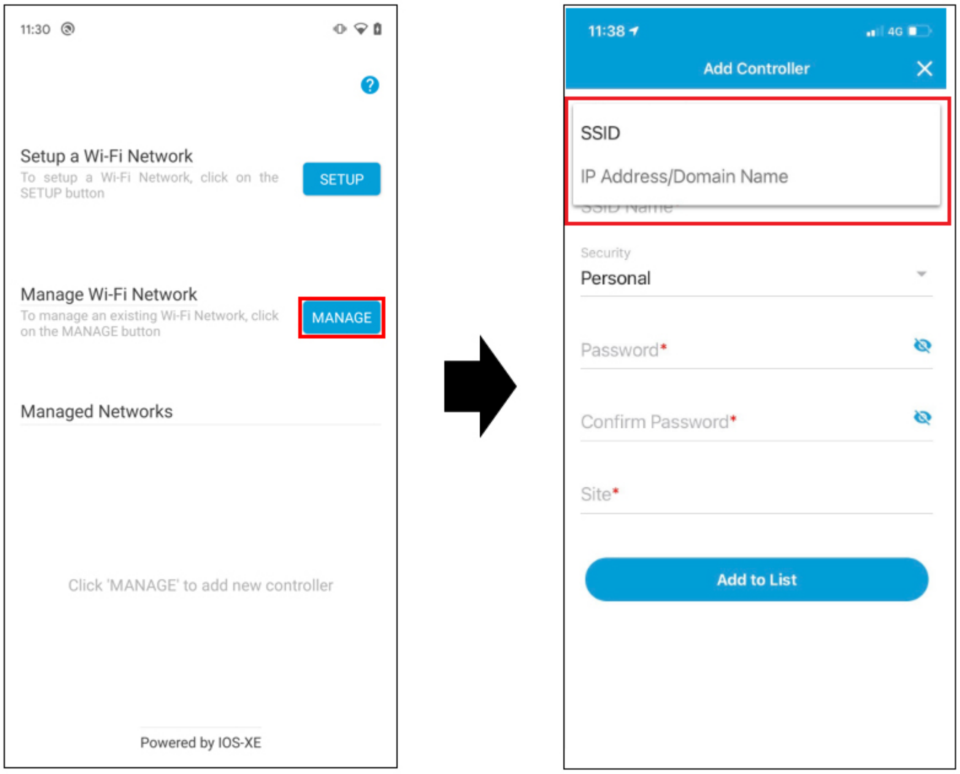
To setup a Wi-Fi Network, click on the SETUP button

To manage an existing Wi-Fi Network, click on the MANAGE button

SSID : networkpsk an hour ago
Site : Of

IP : 73.170.151.17 19 hours ago
Site : Ra

*Figure 13: Add an Embedded Wireless Controller Using the Cisco Catalyst Wireless Mobile Application*



To setup a Wi-Fi Network, click on the SETUP button

To manage an existing Wi-Fi Network, click on the MANAGE button

Click 'MANAGE' to add new controller

The following sections provide details about managing your Embedded Wireless Controller network and associated devices:

- Manage, on page 18
- Controller Details, on page 23
- Monitoring, on page 25
- Mesh, on page 27
- Security, on page 30
- Administration, on page 31
- License, on page 32
- Logout, on page 32

# Manage

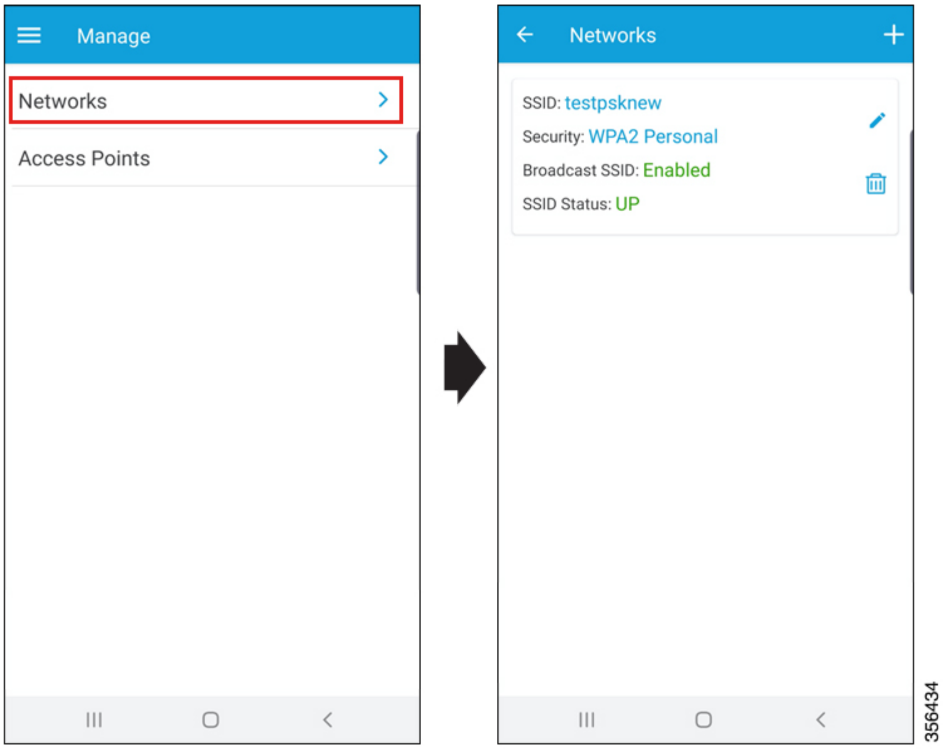
Using the Cisco Catalyst Wi-Fi mobile application, you can:

- Manage the controller and AP in an Cisco Embedded Wireless Controller network.
- Create, modify, or delete the configurations by following the instructions provided in the following sections.

# Manage the Network

Under **Manage** > **Networks**, you can create, edit, or delete a network in a Cisco Embedded Wireless Controller deployment.

*Figure 14: Manage Networks Using the Cisco Catalyst Wireless Mobile Application*



SSID: testpsknew
Security: WPA2 Personal
Broadcast SSID: Enabled
SSID Status: UP

The following details of each available network can also be viewed in the **Networks** screen:

- SSID
- Security
- Broadcast SSID
- SSID Status

## Create a WLAN

You can create and manage the following types of network in a Cisco Embedded Wireless Controller deployment:

- Employee Network
- Guest Network

## Adding an Employee Network

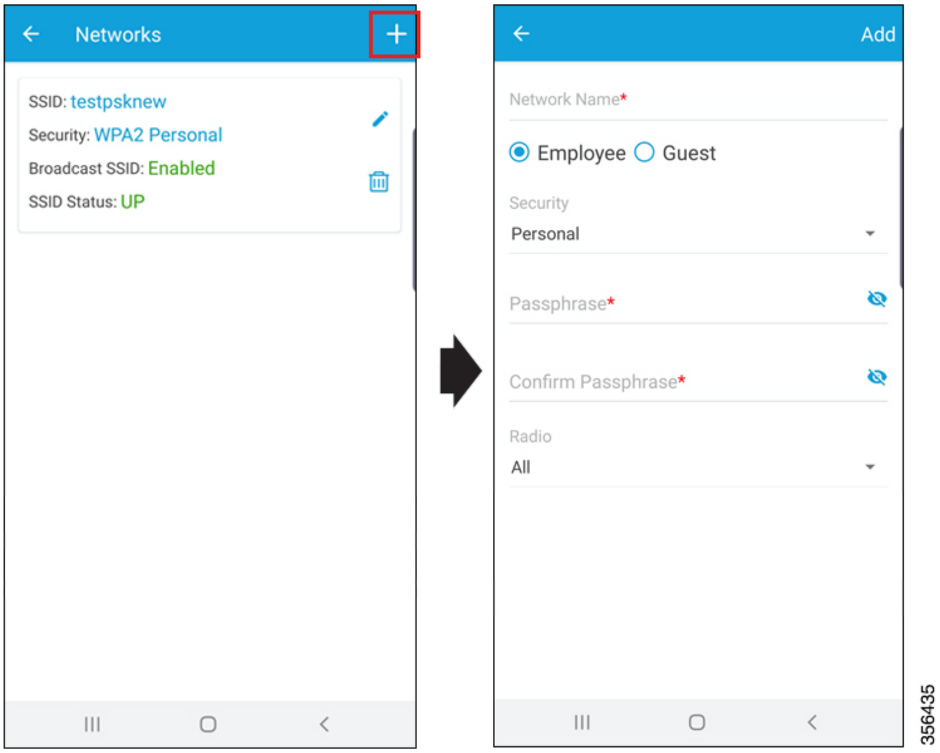
**Step 1** Navigate to **Manage** > **Networks**.

The **Networks** screen is displayed.

**Step 2** Tap the + icon to add a new user.

**Step 3** In the **Network Name** field, enter a name for the network.

*Figure 15: Add a New Network*



SSID: testpsknew
Security: WPA2 Personal
Broadcast SSID: Enabled
SSID Status: UP

Network Name*
● Employee ○ Guest
Security: Personal
Passphrase*
Confirm Passphrase*
Radio: All

**Step 4** Tap the **Employee** radio button.

**Step 5** From the **Security** drop-down list, choose the security level-**Personal** or **Enterprise**.

**Step 6** In the **Passphrase** field, enter a passcode.

**Step 7** In the **Confirm Passphrase** field, re-enter the passcode.

**Step 8** From the **Radio** drop-down list, choose a radio.

**Step 9** Slide the **Status** toggle button to enable the network.

**Step 10** Slide the **Broadcast** toggle button to broadcast the name of the network.

After successful completion of the task, the newly added employee network is listed under **Manage** > **Network**, from where you can view the status. You can also modify (using the pencil icon) or delete (using the trash icon) the employee network from this screen.

*Configuring the AAA Server*

**Step 1** In the **Network Name** field (Figure 15: Add a New Network, on page 20), enter a name for the network.

**Step 2** Tap either the **Employee** or **Guest** radio button.

**Step 3** From the **Security** drop-down list, choose the security level, as **Enterprise**.

The **Radius** screen is displayed.

**Step 4** Under the **Primary Radius** section, in the **IP Address** field, enter the IP address of the primary RADIUS server.

**Step 5** In the **Port Number** field, enter the port number.

**Step 6** In the **Secret** field, enter a password.

Configuring the secondary RADIUS server is optional. To configure the secondary RADIUS server, go to the **Secondary Radius** section.

**Step 7** (Optional) In the **IP Address** field, enter the IP address of the secondary RADIUS.

**Step 8** In the **Port Number** field, enter the port number.

**Step 9** Tap **Save**.

A confirmation message is displayed indicating that the AAA server is configured.

### Adding a Guest Network

**Step 1** Navigate to **Manage** > **Networks** (Figure 14: Manage Networks Using the Cisco Catalyst Wireless Mobile Application, on page 19).

The **Networks** screen is displayed.

**Step 2** Click the + icon to add a new user (Figure 15: Add a New Network, on page 20).

**Step 3** In the **Network Name** field, enter a name for the network.

**Step 4** Click the **Guest** radio button.

**Note** The security protocol for the guest network is **Consent**. After successful completion of the task, the newly added guest network is listed under **Manage** > **Network**, from where you can view the status. You can also modify (using the pencil icon) or delete (using the trash icon) the guest network from this screen.

## Manage the AP

You can add, modify, or view the AP details by completing the following steps:

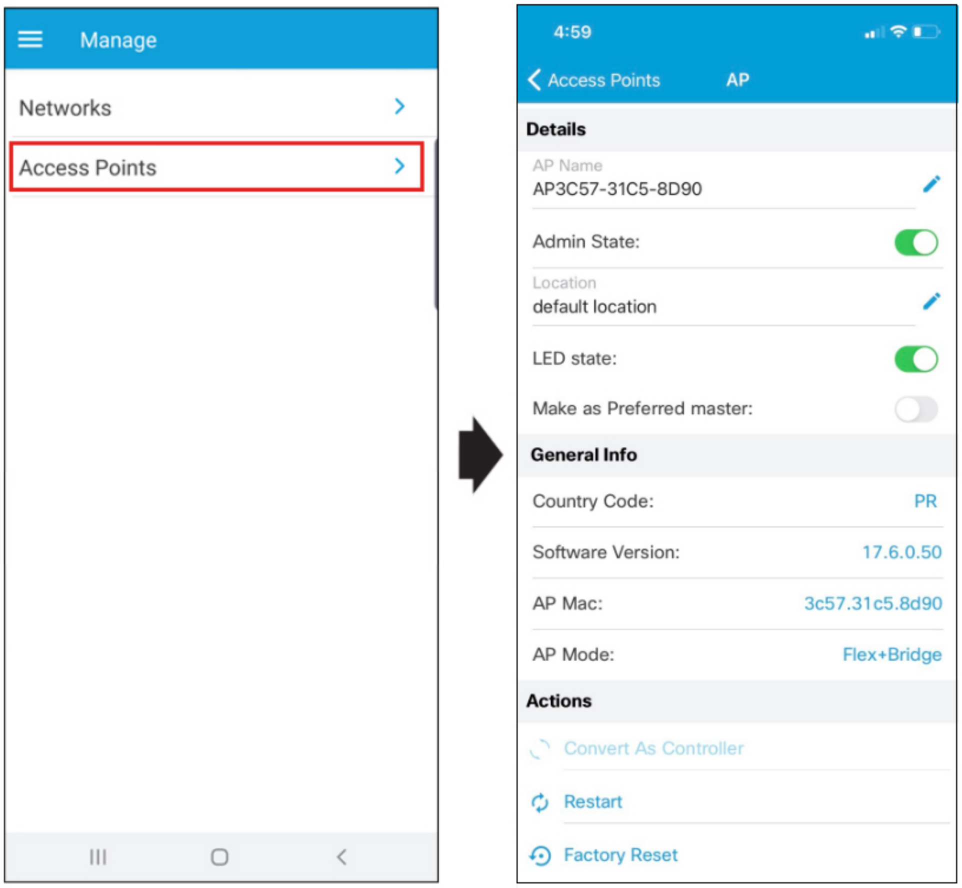
**Step 1** Navigate to **Manage** > **Access Points**.

All the available access points in the network are listed on the screen.

**Step 2** Click an access point to view its details.

**Step 3** Tap the pencil icon adjacent to the **AP Name** field, to edit the AP name.

*Figure 16: Edit Access Point Details*



AP Name
AP3C57-31C5-8D90

Admin State:

Location
default location

LED state:

Make as Preferred master:

Country Code: PR

Software Version: 17.6.0.50

AP Mac: 3c57.31c5.8d90

AP Mode: Flex+Bridge

**Step 4** Slide the **Admin State** toggle button to switch the status of the admin.

**Step 5** Tap the pencil icon adjacent to the **Location** field, to edit the location.

By default, your current country is selected as the location.

**Step 6** Slide the **LED State** toggle button to switch the status of the LED.

**Step 7** Slide the **Make as Preferred Master** toggle button to switch the status of the preferred primary AP.

Additionally, you can view the general information of the AP, such as **Country Code**, **Software Version**, and **AP MAC address**.

**Step 8** Perform the following AP management tasks:

a) **Convert As Controller**: Makes the Cisco Catalyst AP Series function as a controller.

This option is available only if the AP is capable of becoming a master AP in a Cisco Embedded Wireless Controller network.

b) **Restart**: Restarts the AP.

If the selected AP is the master AP in a Cisco Embedded Wireless Controller network, then there is a network outage and clients are not served.

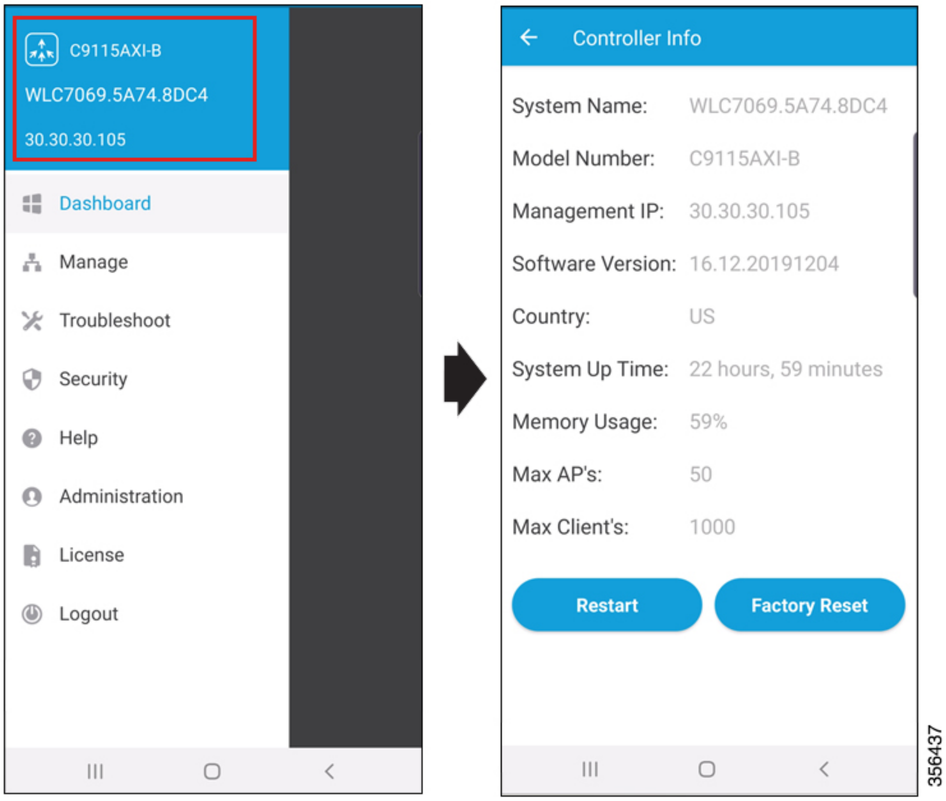
c) **Factory Reset**: Removes all the configuration from the AP.

# Controller Details

In the collapsible side pane, click the name of the Primary AP to view the following details of your Cisco Embedded Wireless Controller:

- **System Name**
- **Model Number**
- **Management IP**
- **Software Version**
- **Country**
- **System Up Time**
- **Memory Usage**
- **Maximum APs**
- **Maximum Clients**

*Figure 17: Controller Details Page*



System Name: WLC7069.5A74.8DC4

Model Number: C9115AXI-B

Management IP: 30.30.30.105

Software Version: 16.12.20191204

Country: US

System Up Time: 22 hours, 59 minutes

Memory Usage: 59%

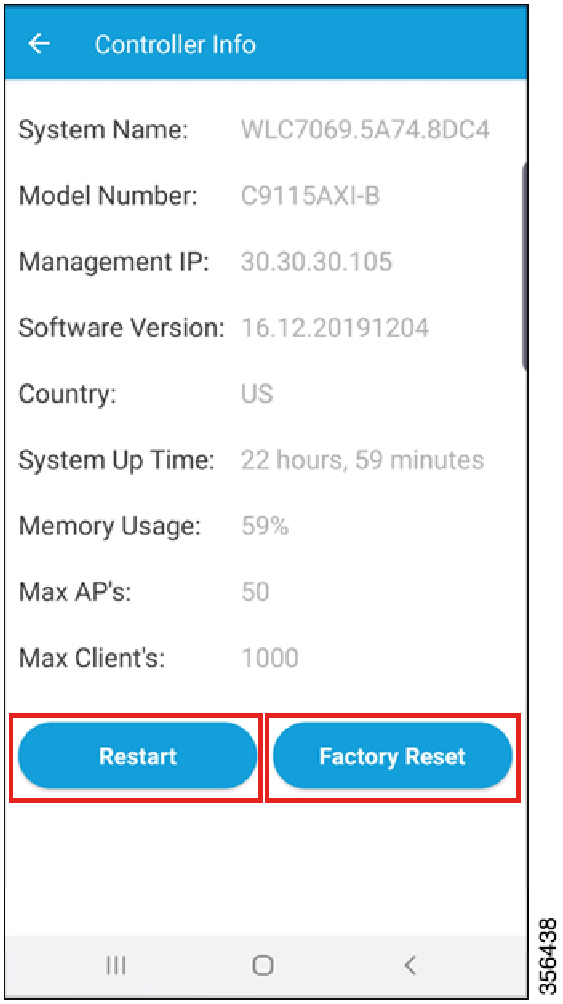
Max AP's: 50

Max Client's: 1000

You can also perform the following tasks:

- Restart
- Factory Reset

*Figure 18: Controller Restart and Reset on the Controller Details Page*



Controller Info

System Name: WLC7069.5A74.8DC4

Model Number: C9115AXI-B

Management IP: 30.30.30.105

Software Version: 16.12.20191204

Country: US

System Up Time: 22 hours, 59 minutes

Memory Usage: 59%

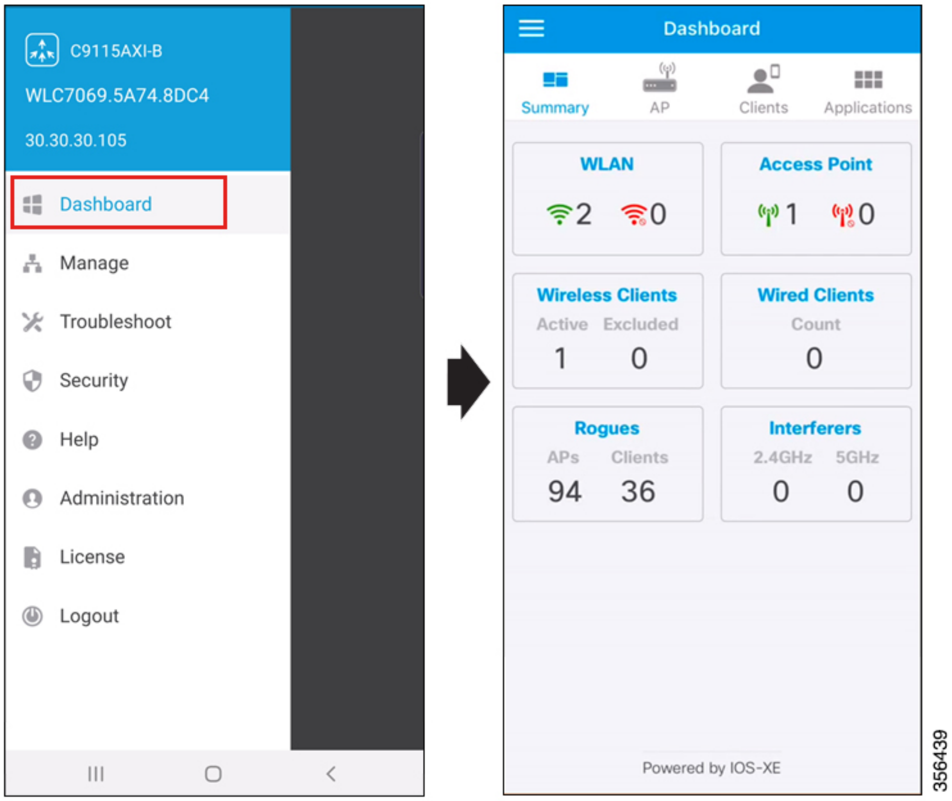
Max AP's: 50

Max Client's: 1000

# Monitoring

You can monitor your Cisco Embedded Wireless Controller network, by navigating to the **Dashboard** screen in the side pane of the Cisco Catalyst Wireless mobile app GUI.

*Figure 19: Cisco Catalyst Wireless Mobile Application Dashboard*



Here, you can view the following details:

- **Summary**
- **APs**
- **Clients**
- **Applications**

# Summary

Navigate to **Dashboard** > **Summary**, to view the count and status of the following elements in your Cisco Embedded Wireless Controller network:

- **WLAN**
- **Access Point**
- **Wireless Clients**
- **Wired Clients**
- **Rogues**
- **Interferers**

## APs

The top 10 access points in your Cisco Embedded Wireless Controller network are listed under **Dashboard** > **AP**. Here you can also view the following details for each AP:

- **MAC address**
- **AP model**
- **IP Address**
- **Channels**
- **Mode**
- **UP Time**

## Top Clients

Navigate to **Dashboard** > **Clients**, to view the list of the **Top 10 Clients by Usage**. You can also view the following details for each client:

- **Client Identity**
- **SSID**
- **Device Type**
- **Usage**

## Top Applications

Navigate to **Dashboard** > **Applications**, to view a list of the various applications running on a specific WLAN. Choose a WLAN from the **WLAN** drop-down list.

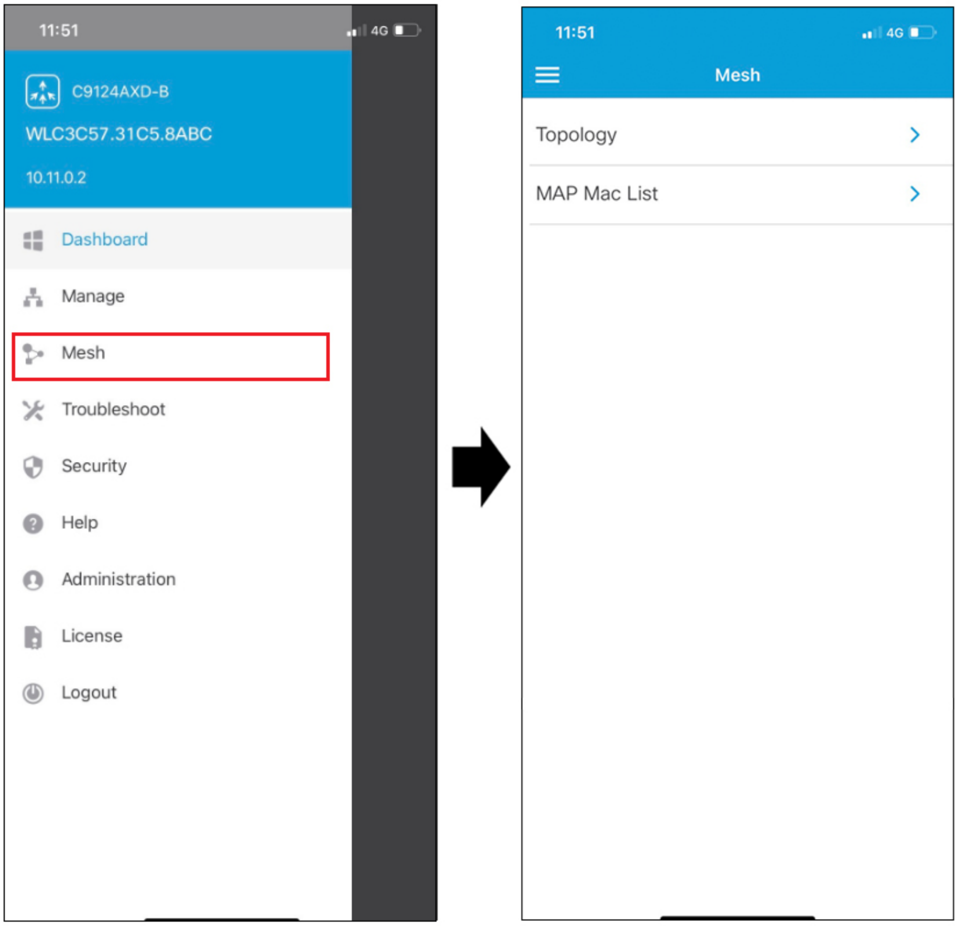
You can also view the following details for the various applications:

- **Application name**
- **Usage %**
- **Bytes**

# Mesh

In the **Mesh** screen of the Cisco Catalyst Wireless mobile app, you can view the **Mesh Topology** and the **MAP MAC List**.

*Figure 20: Cisco Catalyst Wireless Mobile Application Mesh*



The following sections describe the **Mesh Topology** and the **MAP MAC List** details.

# Mesh Topology

The Mesh Topology screen displays the mesh AP tree, the number of bridge APs, number of root APs, and the number of mesh access points (MAP) in the network.

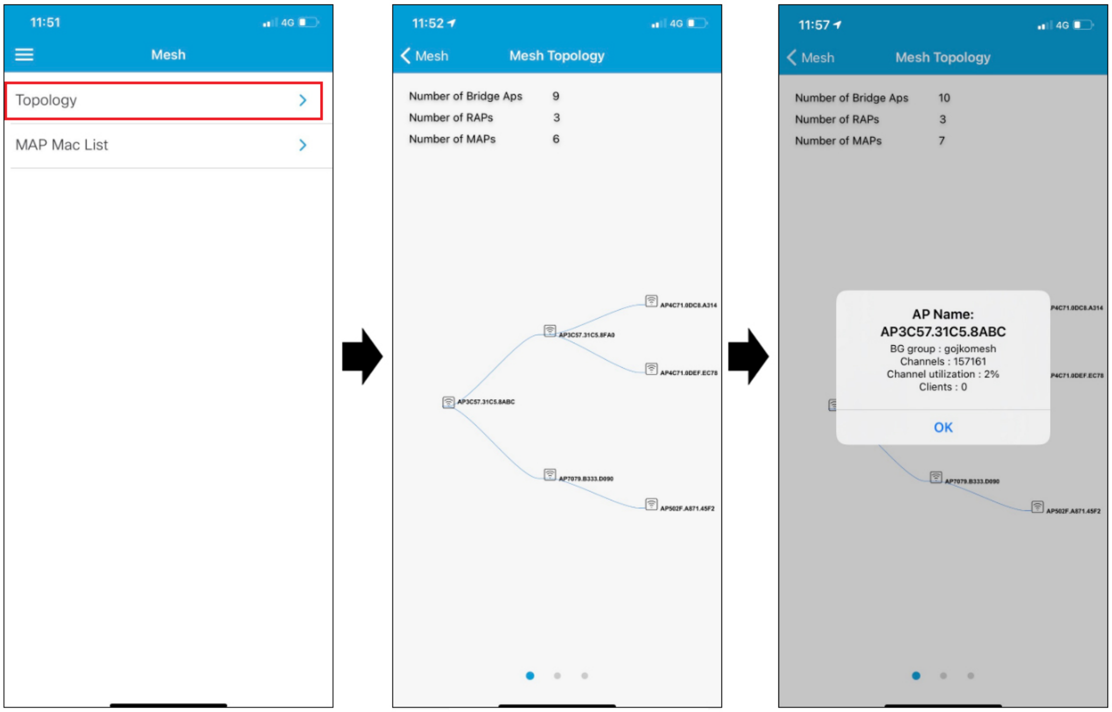
To view the mesh topology, follow these steps:

**Step 1** Navigate to **Mesh** > **Mesh Topology**.

The mesh AP tree, the number of bridge APs, number of root APs, and the number of MAPs in the network, are displayed on the screen.

**Step 2** Press an AP icon on the mesh tree to view the AP details.

*Figure 21: Cisco Catalyst Wireless Mobile Application Mesh Topology*



Number of Bridge Aps 9
Number of RAPs 3
Number of MAPs 6

Number of Bridge Aps 10
Number of RAPs 3
Number of MAPs 7

AP Name:
AP3C57.31C5.8ABC
BG group : gojkomesh
Channels : 157161
Channel utilization : 2%
Clients : 0

# Mesh Access Points MAC List

The MAP MAC list displays the MAC addresses of the mesh APs.

To add a MAC address, follow these steps:

**Step 1** Navigate to **Mesh** > **MAP MAC List**.

All the available MAC addresses of the mesh APs are displayed on the screen.

**Step 2** Press a MAC address to view its details.

**Step 3** To add a new MAC address, press the + icon.
The **Add Mac Address** screen is displayed.

**Step 4** To add a new MAC address, you can do one of the following:

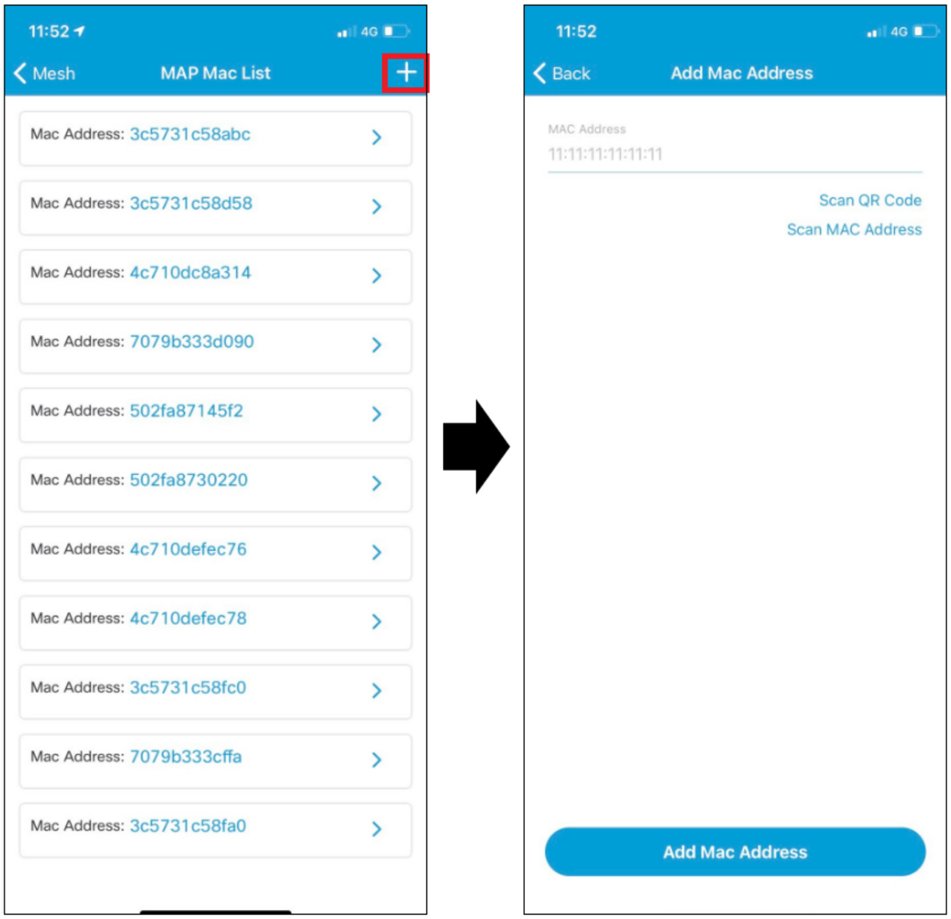
a) Enter the MAC address in the **Address** field.

b) Tap the **Scan QR Code** link to capture the MAC address.

c) Tap the **Scan MAC Address** link to scan and add the MAC address.

**Step 5** Tap **Add Mac Address**.

*Figure 22: Cisco Catalyst Wireless Mobile Application MAP MAC List Screen*



11:52

Mesh — MAP Mac List — +

Mac Address: 3c5731c58abc

Mac Address: 3c5731c58d58

Mac Address: 4c710dc8a314

Mac Address: 7079b333d090

Mac Address: 502fa87145f2

Mac Address: 502fa8730220

Mac Address: 4c710defec76

Mac Address: 4c710defec78

Mac Address: 3c5731c58fc0

Mac Address: 7079b333cffa

Mac Address: 3c5731c58fa0

11:52

Back — Add Mac Address

MAC Address: 11:11:11:11:11:11

Scan QR Code

Scan MAC Address

Add Mac Address

# Security

In the **Security** screen of the Cisco Catalyst Wireless mobile app, you can view the available 802.1x configurations of the primary and secondary RADIUS servers in your Cisco Embedded Wireless Controller network.

You can view the following details of the AAA server:

- **Name**
- **IP Address**
- **Accounting Port**
- **Authorization Port**
- **Status**

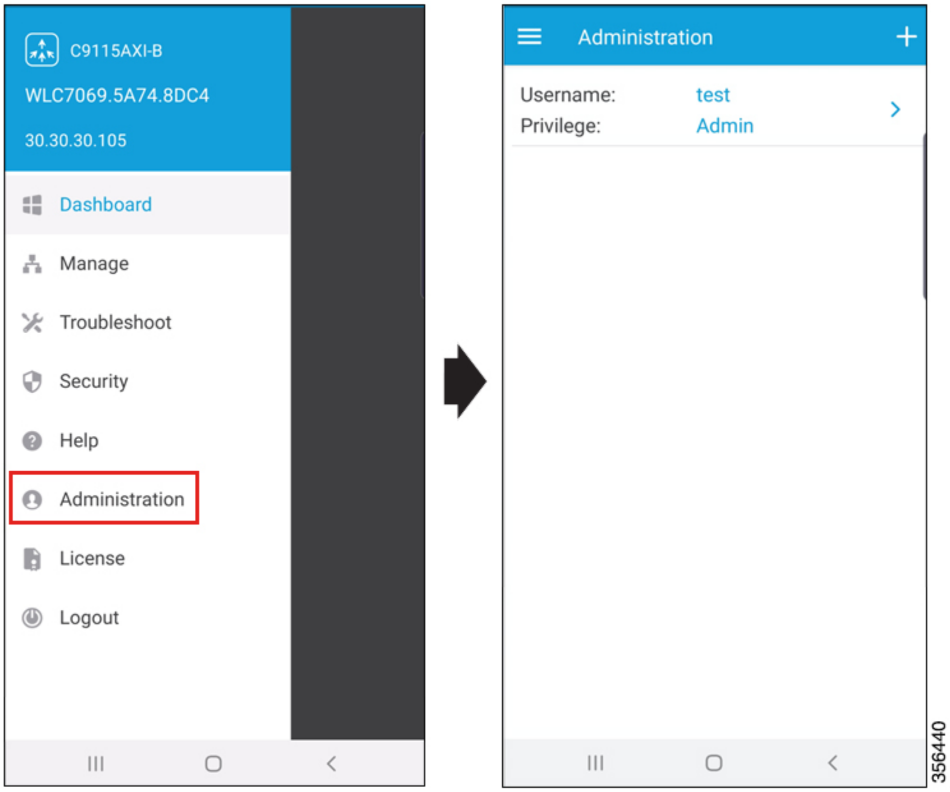
# Administration

Under **Dashboard** > **Administration**, you can find a listing of the various user accounts with associated privilege (admin or user) configured for your Cisco Embedded Wireless Controller network. You can also add new users or delete existing users here.

To add a new user, follow this procedure:

**Step 1** Tap **Administration**, and then the **+** icon to add a new user.

*Figure 23: Cisco Catalyst Wireless Mobile Application Administration Screen*



Username: test
Privilege: Admin

**Step 2** In the **Username** field, enter the username.

**Step 3** In the **Password** field, enter a password.

**Step 4** In the **Confirm Passphrase** field, re-enter the password.

**Step 5** From the **Privilege** drop-down list, choose either **User** or **Admin**.

A confirmation message is displayed. Click **Okay** to dismiss the message.

# License

Under **License**, you can find the following licensing details for your Cisco Embedded Wireless Controller network.

- Under **General Information**, the following information is displayed:
  - **Smart License Status**
  - **Authorization Status**
  - **Registration Status**
  - **Evaluation Period Remaining**
  - **Unique Device Identifier (UDI)**
- Under **Used Licenses**, the following information is displayed:
  - **License**
  - **Count**
  - **Status**

# Logout

Click **Logout** to end the current controller session. Switch to another session by logging in to corresponding controller.