User Guide for Cisco Catalyst Wireless Mobile Application

First Published: 2020-01-19

Last Modified: 2020-03-16

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

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

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.
...	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.

Convention	Description
[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

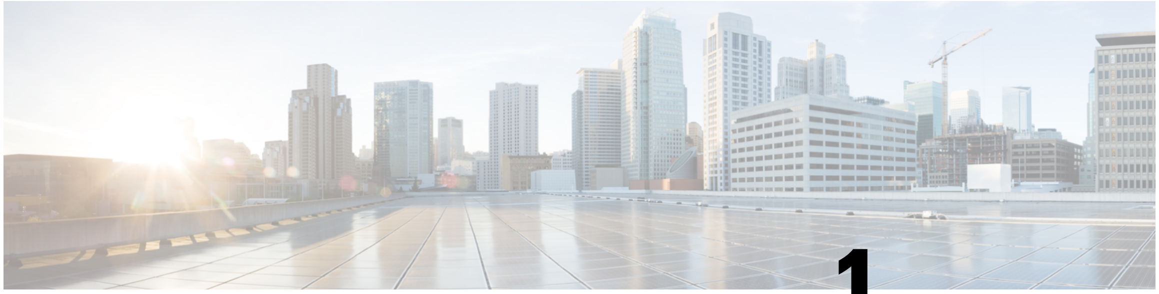
Note Before installing or upgrading the CiscoEmbedded Wireless Controller, refer to the release notes at https://www.cisco.com/c/en/us/support/wireless/embedded-wireless-controller-catalyst-access-points/products-release-notes-list.html.

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 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 detailed information about 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 meeting the below platform requirements:

- Android 6.0 (Marshmallow) to Android 9 (Pie)
- iOS 11.0 to iOS 13.2.3

CHAPTER 2

Download and Install the Mobile Application

Download and Installation

The Cisco Catalyst Wireless mobile application is available for download at 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, follow the instructions given in the Apple App Store or the Google Play Store.

Troubleshooting App Installation

Some common installation issues and workarounds are listed below:

Problem The Cisco Catalyst Wireless mobile application repeatedly crashes or malfunctions.

Solution Try restarting the app. If that does not resolve the app malfunction, contact Cisco Support.

CHAPTER 3

Getting Started

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

Overview of the Day 0 Wizard

The Day 0 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.

Setting Up a Wi-Fi Network

To set up the Wi-Fi network for your Cisco Embedded Wireless Controller deployment, use the Cisco Catalyst Wireless mobile app to first Connecting to the Provisioning SSID and then Provisioning the Network.

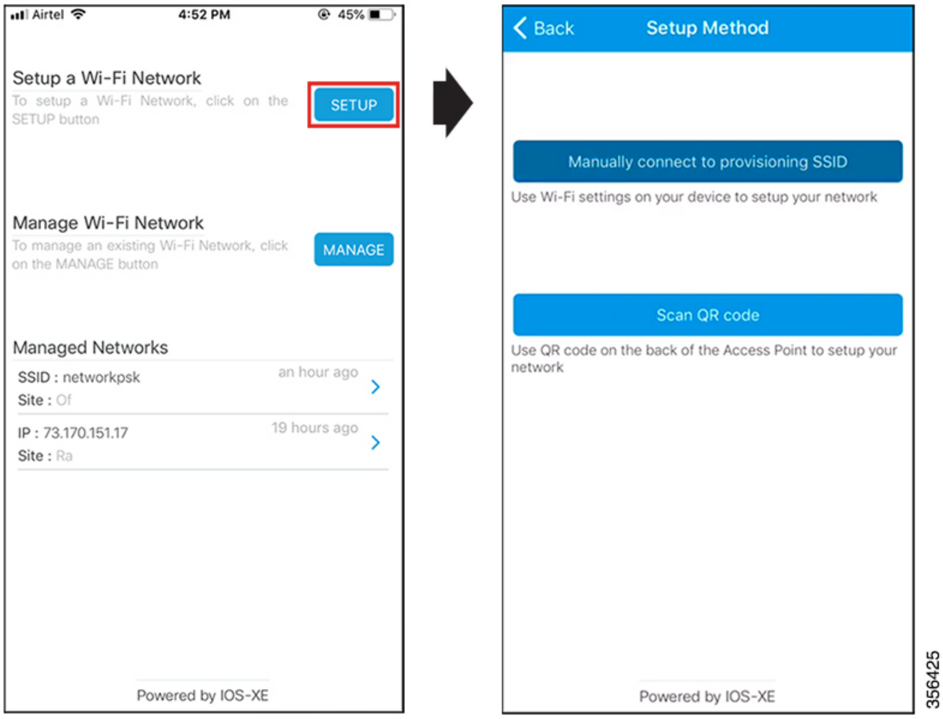
In the following sections you can find more information about connecting to the provisioning SSID:

Connecting to the Provisioning SSID

You can set up the Wi-Fi network for your Cisco Embedded Wireless Controller deployment through one of the following methods:

- Scanning the QR code, on page 6
- Manually Connecting to the Provisioning SSID, on page 7

Figure 1: Landing Page and Provisioning Page 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

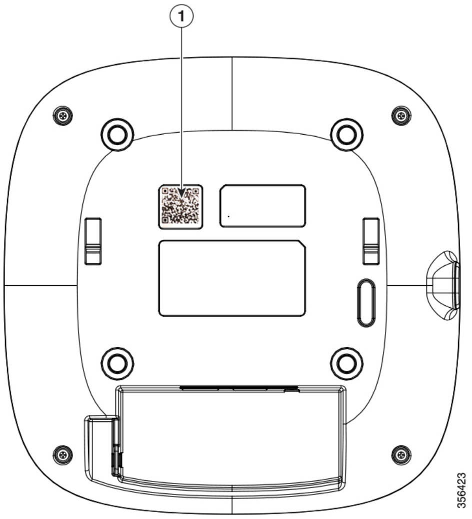
Powered by IOS-XE

Scanning the QR code

You can locate the QR code on the back of your Cisco Catalyst Series access point. 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 your Wi-Fi network up.

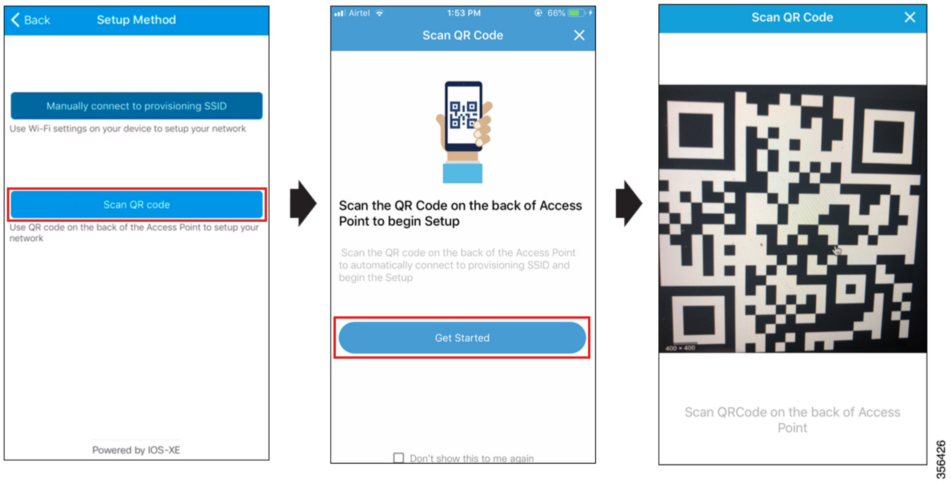
Note To initiate Day 0 configuration, follow the instructions in the Logging in to the Day 0 Wizard, on page 9 section, beginning at Step 3.

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



1	Location of the QR code on the back of the Cisco Catalyst 9120AX Series AP

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

Manually Connecting to the Provisioning SSID

Step 1 Under **Settings** in your mobile device, go to **Wi-Fi**.

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

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

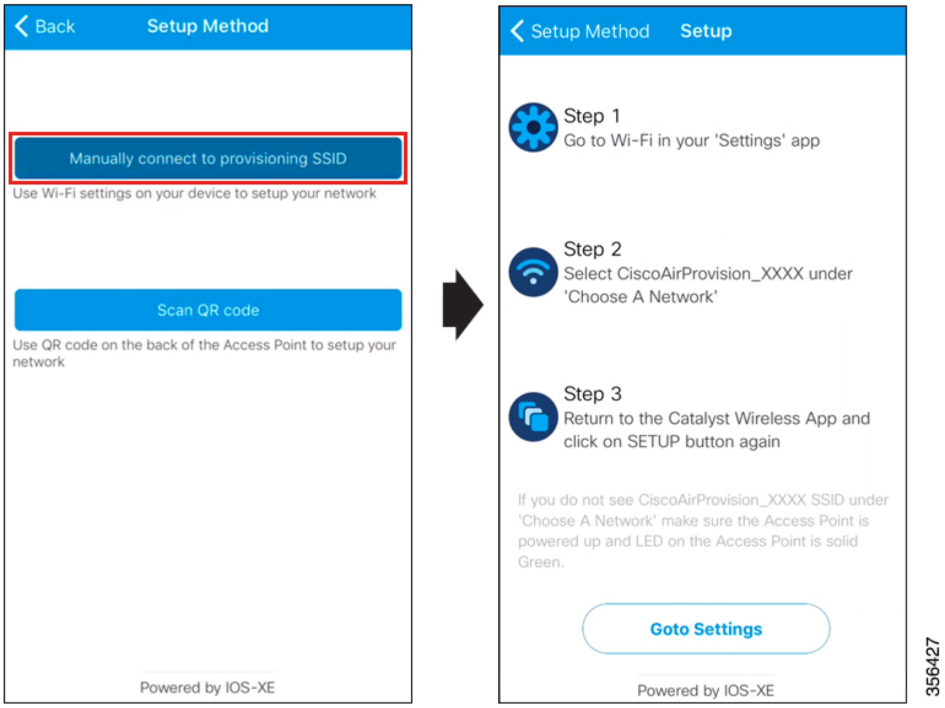
Step 4 Click **Join**.

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

What to do next

To initiate Day 0 configuration, return to the app **Landing Page** and follow the instructions provided in the Logging in to the Day 0 Wizard, on page 9 section.

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

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.

Troubleshooting 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 If your mobile device is connected to the desired SSID but the error message `Please check your Wi-Fi connection and try again.` appears. Note that this error might also appear during Day 1.

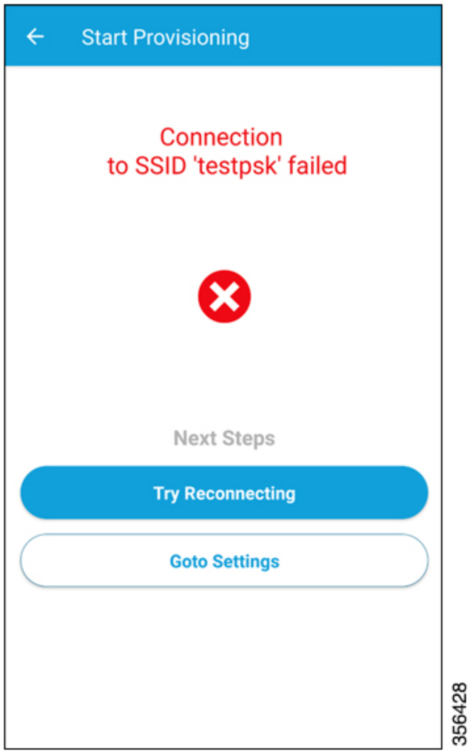
Solution Switch off your mobile data and connect to the provisioning SSID.

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

Solution Under **Settings** > **Wi-Fi** > **Choose A Network** in your mobile device, do either one of the following:

- **Solution** Navigate to the desired SSID, and click **Forget**. After waiting for some time, return to the Cisco Catalyst Wireless mobile app to continue usage.
- **Solution** Manually connect to the desired SSID and return to the Cisco Catalyst Wireless mobile app.

Figure 5: Error message in Android 6.0 and later versions while connecting to the SSID



Start Provisioning

Connection to SSID 'testpsk' failed

Provisioning the Network

Logging in to the Day 0 Wizard

Before you begin

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

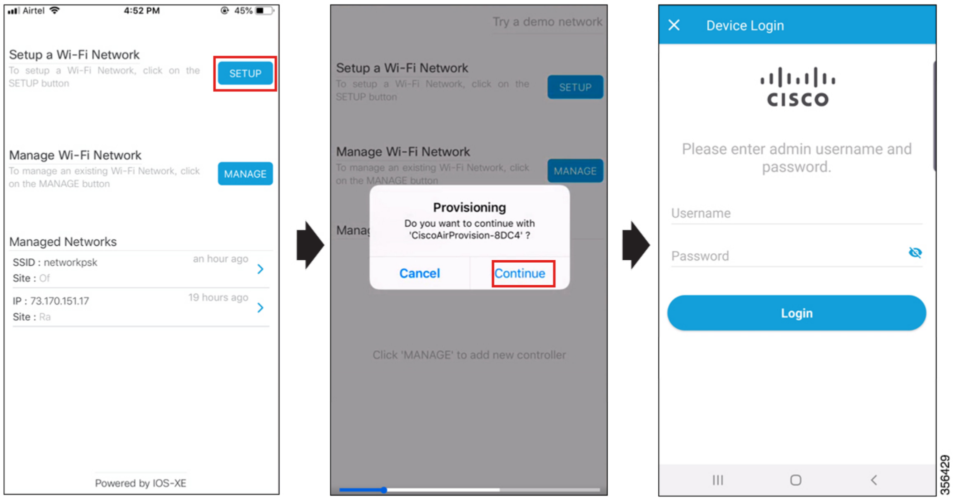
Step 1 Under **Setup a Wi-Fi Network**, click **Setup**.

The **Provisioning** dialog window appears.

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

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

Figure 6: Logging in to the Day 0 Wizard



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

Provisioning

Do you want to continue with 'CiscoAirProvision-8DC4' ?

Click 'MANAGE' to add new controller

Device Login

Please enter admin username and password.

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

Step 4 Click **Login**.

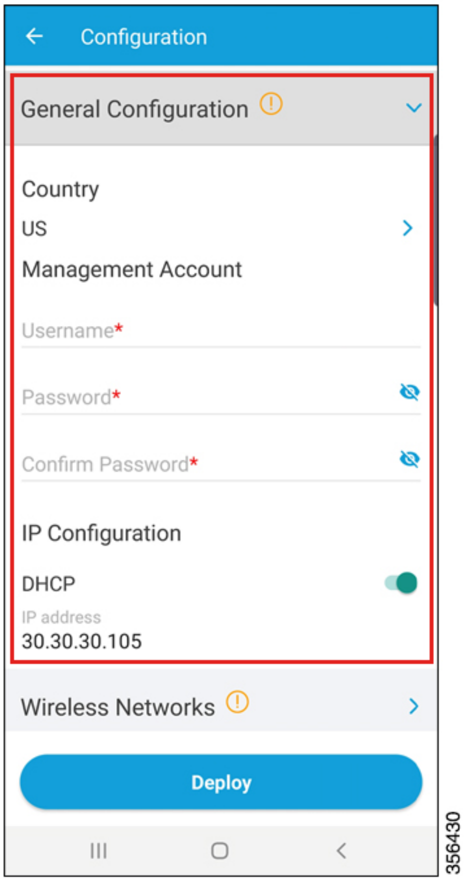
Initial Network Configuration

Once you are logged in to the Day 0 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 On the **Configuration** page, under **General Configuration**, select the desired country from the **Country** drop-down list.

Step 2 Under **Management Account**, enter the desired management credentials.

Figure 7: Day 0 Wizard - General Configuration



Configuration

General Configuration

Country

US

Management Account

Username*

Password*

Confirm Password*

IP Configuration

DHCP

IP address

30.30.30.105

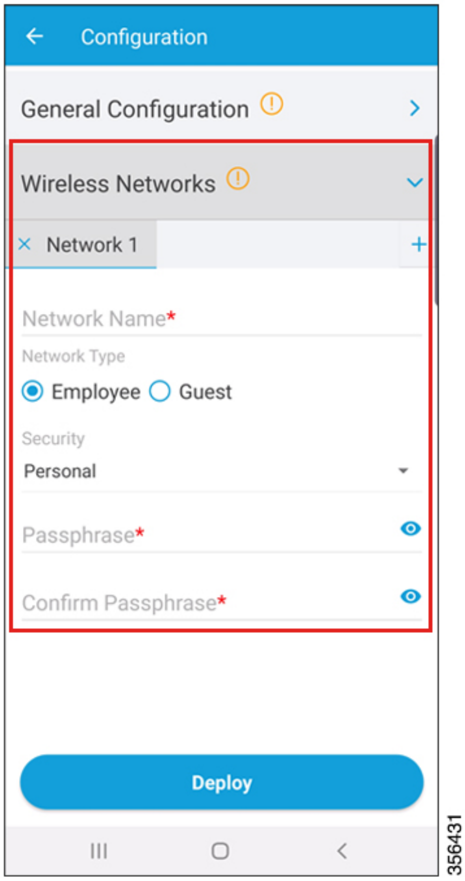
Wireless Networks

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 **Wireless Networks**, click + to add a network SSID.

Figure 8: Day 0 Wizard – Wireless Networks Configuration



Network Name*

Network Type
● Employee ○ Guest

Security
Personal

Passphrase*

Confirm Passphrase*

Step 5 In the **Network Name** field, enter the desired name.

Step 6 Click the **Network Type** radio button to choose between **Employee** or **Guest**.

Step 7 From the **Security** drop-down list, choose the desired security type.

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

  The default security type is **Personal**. To know more about configuring **Enterprise** security, refer to 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.

Step 8 In the **Passphrase** field, enter a passcode.

Step 9 In the **Confirm Passphrase** field, enter the same passcode entered in the previous step.

Step 10 Click **Deploy**.

A confirmation message is displayed.

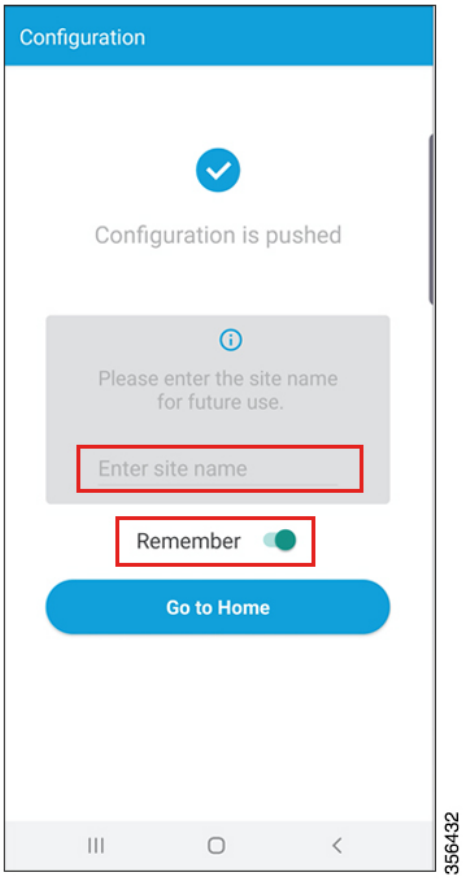
Step 11 (Optional) Click **Review** to review the configured network settings.

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

Step 12 Click **Deploy**.

A confirmation page appears where you can enter the site name and choose to **Remember** the configured site.

Figure 9: Day 0 Wizard – Confirmation Page



Configuration

Configuration is pushed

Please enter the site name for future use.

Enter site name

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 will find options to add, modify, or delete a previously configured Employee or Guest network. You can also modify the AP details using this wizard.

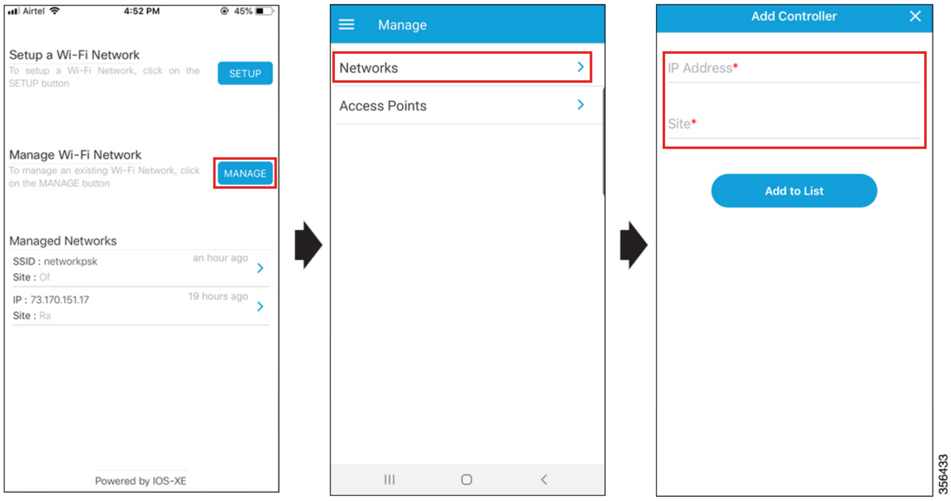
Under **Managed Networks**, you can find your list of configured embedded wireless controllers that are being managed by the Cisco Catalyst Wireless mobile app.

Also, when you choose **Remember** on the **Confirmation Page** of the Day 0 wizard (Figure 9: Day 0 Wizard – Confirmation Page), the controller gets added to the **Managed Networks** list.

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

- SSID
- IP Address

Figure 10: Adding an Embedded Wireless Controller Using the Cisco Catalyst Wireless Mobile Application



Airtel 4:52 PM 45%

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

Manage

Networks

Access Points

Add Controller

IP Address*

Site*

- License, on page 26
- Logout, on page 26

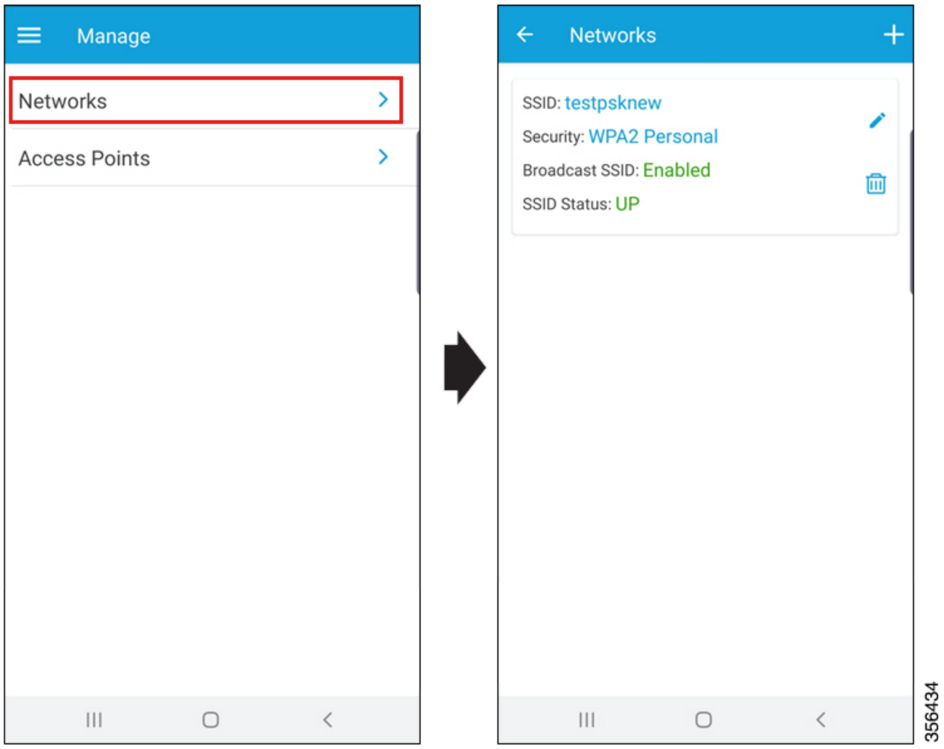
Manage

Using the Cisco Catalyst Wi-Fi mobile application, you can manage the controller and AP in a Cisco Embedded Wireless Controller network. You can create, modify or delete the various configurations by following the desired procedure listed below.

Manage the Network

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

Figure 11: 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 here:

- SSID
- Security
- Broadcast SSID
- SSID Status

Create a WLAN

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

- Employee Network
- Guest Network

Adding an Employee Network

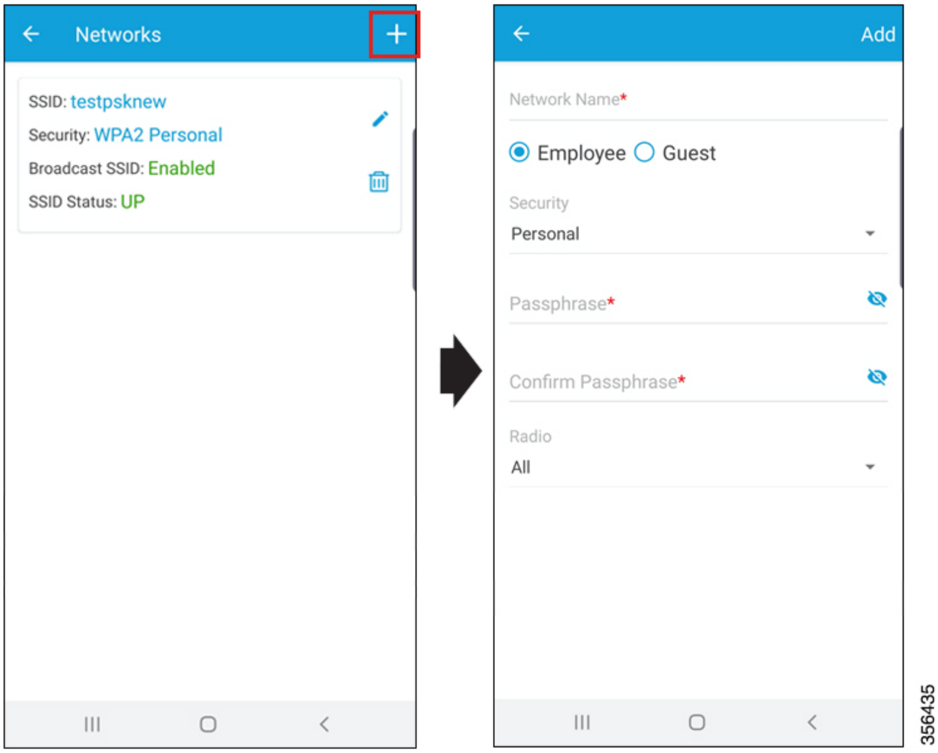
Step 1 Click **Manage** > **Networks**.

The **Networks** screen is displayed.

Step 2 Click on the + icon to add a new user.

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

Figure 12: Add a New Network



Networks

SSID: testpsknew

Security: WPA2 Personal

Broadcast SSID: Enabled

SSID Status: UP

Add

Network Name*

● Employee ○ Guest

Security: Personal

Passphrase*

Confirm Passphrase*

Radio: All

Step 4 Use the radio button to choose **Employee**.

Step 5 Use the **Security** drop-down list to select the security level, either as **Personal** or **Enterprise**.

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

Step 7 In the **Confirm Passphrase** field, enter the same passcode entered in the previous step.

Step 8 Use the **Radio** drop-down list to select the radio.

Step 9 Move the slider in the **Status** field to enable the network.

Step 10 Move the slider in the **Broadcast** field 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 (pencil icon) or delete (trash icon) the employee network from this screen.

Configuring the AAA Server

Step 1 In the **Network Name** field, enter a name for the network.

Step 2 Use the radio buttons to select the network type either as **Employee** or **Guest**.

Step 3 Use the **Security** drop-down list to select 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 Click **Save**.

A confirmation message is displayed. The AAA server is configured.

Adding a Guest Network

Step 1 Click **Manage > Networks**.

The **Networks** screen is displayed.

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

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

Step 4 Use the radio button to select **Guest**.

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 (pencil icon) or delete (trash icon) the guest network from this screen.

Manage the AP

You can add, modify or view the AP details by performing the following tasks:

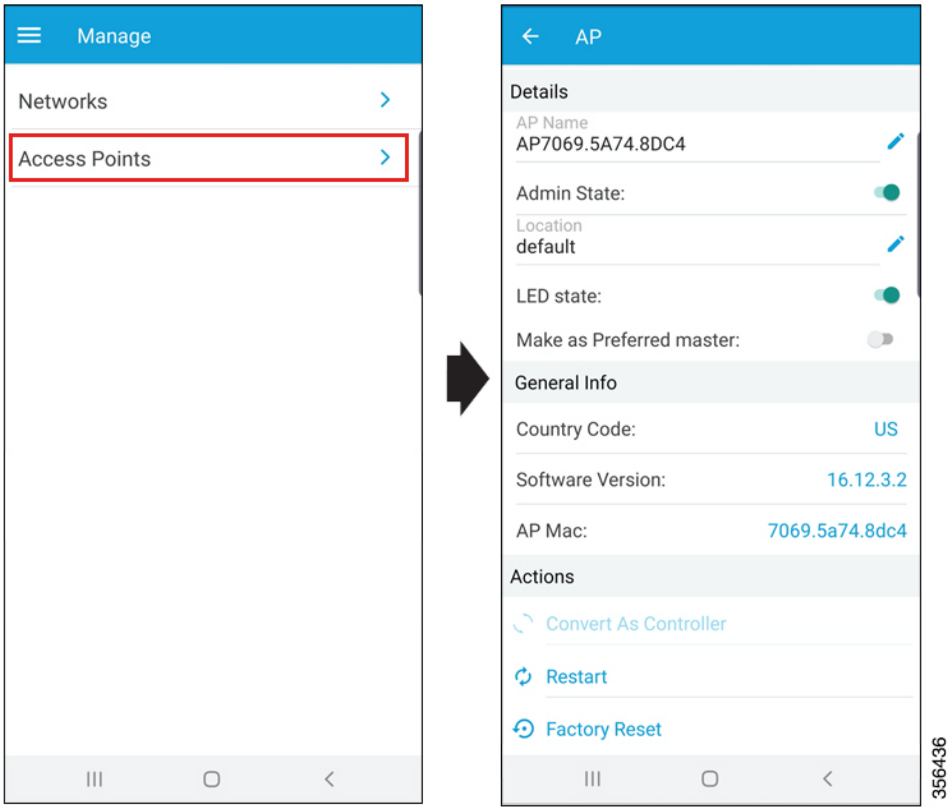
Step 1 Click **Manage** > **Access Points**.

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

Step 2 Select an access point to view its details.

Step 3 In the **AP Name** field, click on the pencil icon to edit the AP's name.

Figure 13: Edit Access Point Details



Details

AP Name: AP7069.5A74.8DC4

Admin State: ●

Location: default

LED state: ●

Make as Preferred master: ○

General Info

Country Code: US

Software Version: 16.12.3.2

AP Mac: 7069.5a74.8dc4

Actions

Step 4 In the **Admin State** field, use the toggle button to switch the status.

Step 5 In the **Location** field, click on the pencil icon to edit the location.

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

Step 6 In the **LED State** field, use the toggle button to switch the status.

Step 7 In the **Make as Preferred Master** field, use the toggle button to switch the status.

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

Step 8 You can also perform the following AP management tasks:

a) **Convert As Controller**: Makes the Catalyst Series AP 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.

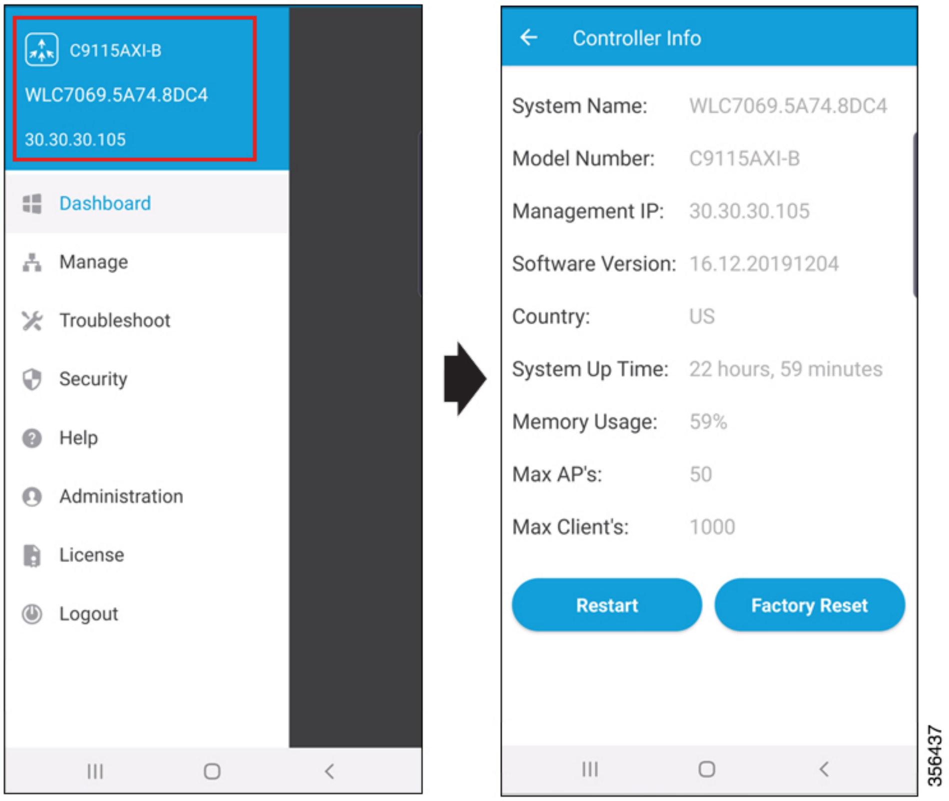
c) **Factory Reset**: Removes all the configuration from the AP.

Controller Details

In the collapsible menu sidebar, click the name of the master AP to view the following details for your Cisco Embedded Wireless Controller:

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

Figure 14: 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%

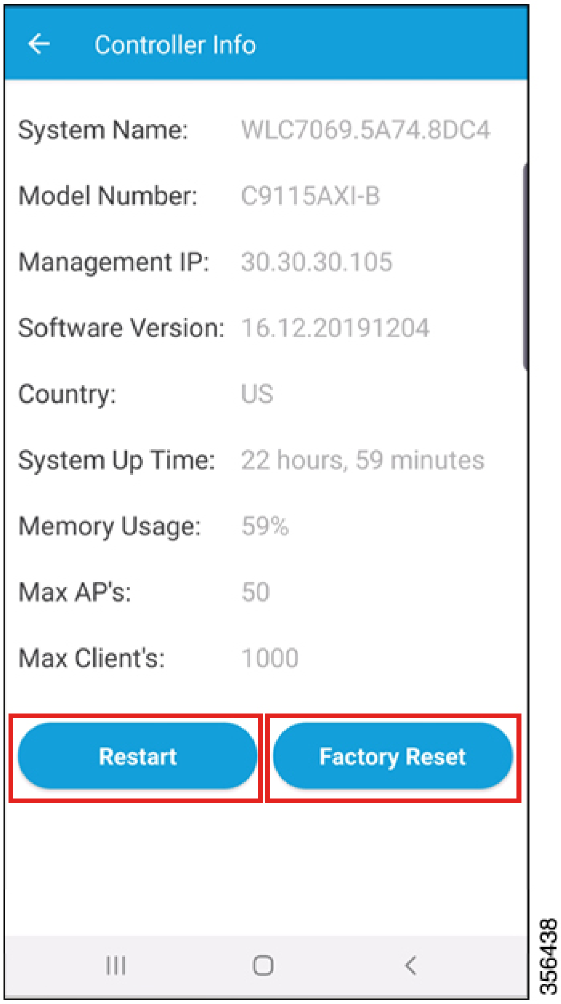
Max AP's: 50

Max Client's: 1000

You can also perform the following tasks:

- Restart
- Factory Reset

Figure 15: 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%

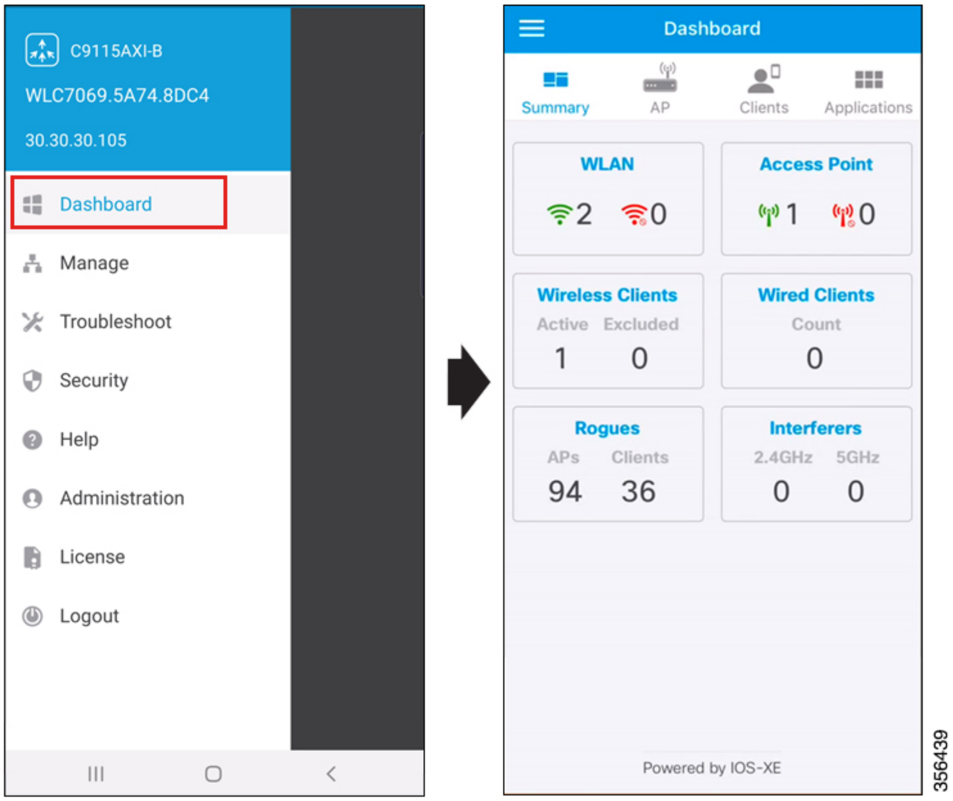
Max AP's: 50

Max Client's: 1000

Monitoring

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

Figure 16: Cisco Catalyst Wireless Mobile Application Dashboard



Here you can view the following details:

- Summary
- APs
- Clients
- Applications

Summary

Under **Dashboard** > **Summary**, you can 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

Under **Dashboard** > **Clients**, you can find a listing of the **Top 10 Clients by Usage**. Here you can also view the following details for each client:

- Client Identity
- SSID
- Device Type
- Usage

Top Applications

Under **Dashboard** > **Applications**, you can find a listing of the various applications running on a specific WLAN. Choose the desired WLAN from the **WLAN** drop-down list.

Here you can also view the following details for the various applications:

- Application name
- Usage %
- Bytes

Security

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

Here you can view the following details of your AAA server:

- Name
- IP Address

- Accounting Port
- Authorization Port
- Status

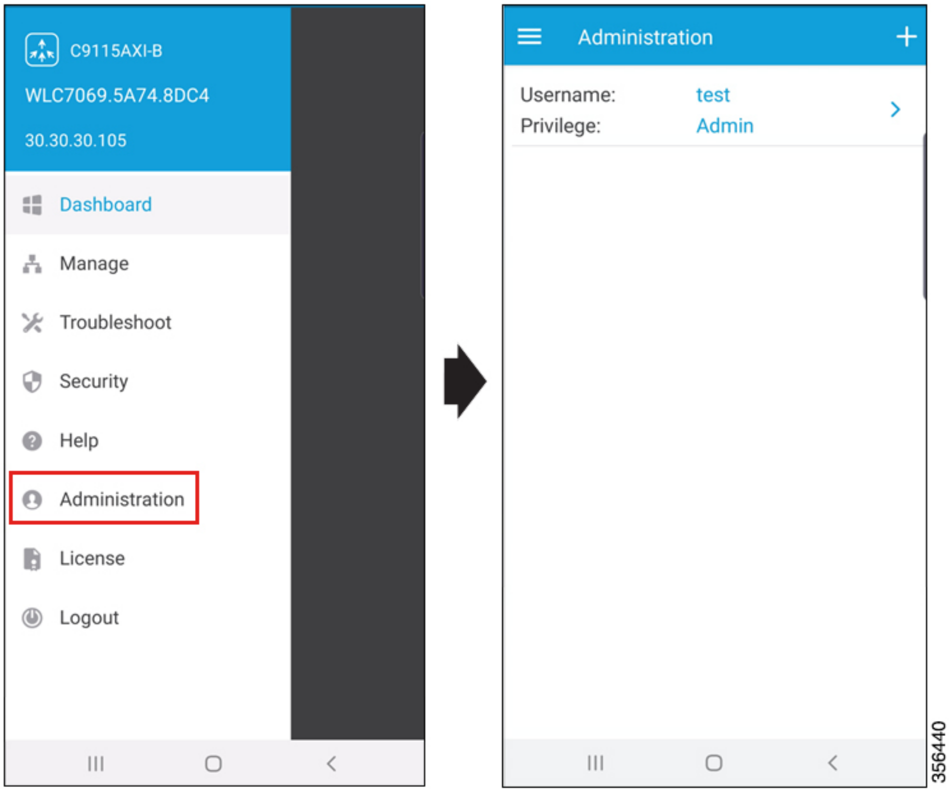
Administration

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 by performing the tasks listed below:

Step 1 Under **Administration**, click on the + icon to add a new user.

Figure 17: Cisco Catalyst Wireless Mobile ApplicationAdministration Page



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, enter the same password entered in the previous step.

Step 5 From the **Privilege** drop-down list, select the privilege, as 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 and switch to another session by logging in to desired controller.