



Cisco Business Access Point Administration Guide, Version 10.8.1.0

First Published: 2020-06-10

Last Modified: 2022-09-15

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.

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.

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)

© 2022 Cisco Systems, Inc. All rights reserved.



The Java logo is a trademark or registered trademark of Sun Microsystems, Inc. in the U.S. or other countries.

© 2022 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1	Cisco Business Wireless Access Points Overview	1
	About Cisco Business Wireless Access Points	1
	Supported Cisco Access Points	1
	Supported Software Images	2
	Supported Browsers	2
	Related Documents	3

CHAPTER 2	Using Cisco Business Wireless Access Point GUI	5
	Using the Cisco Business Wireless Access Point GUI	5

CHAPTER 3	Getting Started	9
	Prerequisite for Setting up and Accessing Cisco Business Wireless AP	9
	AP Deployment Models	10
	Launching the Setup Wizard	12
	Using the Setup Wizard	13
	Logging into the Cisco Business Wireless AP	16
	Adding New Subordinate APs	16
	Adding Mesh Extenders	17

CHAPTER 4	Monitoring	19
	About the Cisco Business Wireless AP Monitoring Service	19
	Customizing the Network Summary View	20
	Customizing Access Points Table View	21
	Viewing Access Point Details	22
	Viewing Client Details	29
	Viewing Guest Client Details	32

Troubleshooting a Client	33
Performing a Client Ping Test	33
Performing a Connection Test	33
Generating an Event Log	33
Viewing Mesh Extender	34
Viewing Applications	35
Viewing Rogue Access Points	35
Configuring the Rogue AP States	36
Viewing Rogue Client Details	36
Viewing Interferer Details	37
Wireless Dashboard	37
Customizing the Access Point Performance View	39
Adding Widgets	39
Removing Widgets	40
Customizing the Client Performance View	40
Adding a Widget	40
Removing a Widget	41

CHAPTER 5
Wireless Settings 43

About WLANs and RLANs in CBW Access Point Network	43
Setting Up WLANs RLANs and WLAN Users	43
Viewing WLANs	44
Adding and Modifying a WLAN	45
Configuring General Details	45
Configuring WLAN Security	46
Configuring VLAN and Firewall	52
Configuring Traffic Shaping	53
Configuring Advanced Options	54
Configuring Scheduling	55
Enabling and Disabling WLANs RLANs	56
Configuring RLAN in AP	56
Editing and Deleting WLANs RLANs	57
Viewing and Managing WLAN Users	57
Blocking and Unblocking Clients	58

Social Login for Guest Users	59
Personal PSK for Clients	60
Managing Associated Access Points	61
Global AP Configuration	62
Administering Access Points	62
Access Point Groups	65
Setting a Login Page for WLAN Guest Users	66
Setting the Default Login Page	67
Setting a Customized Login Page	67
About Cisco Mesh	69
Convert Non-Mesh to Mesh Deployment	69
Mesh Network Components	70
Changing Mesh Parameters	72
Backhaul Client Access	72
Mesh Backhaul Radio Resource Management	73
Mesh Backhaul Slot	73
Modifying AP Port Configuration to Access/Trunk Mode	73
VLAN Transparent	74

CHAPTER 6
Management 75

About Management Access Interface	75
Setting Up Management Access Interface	75
Limitation of Web Based Management Sessions	76
Managing User Priority Order	77
Managing Admin Accounts	77
Adding an Admin Account	77
Editing an Admin Account	78
Deleting an Admin Account	79
Managing Guest Users using the Lobby Admin account	79
Creating a Guest User Account	79
Managing TACACS+ and RADIUS Servers	80
Adding TACACS+ Servers	80
Configuring RADIUS Servers	81
Adding RADIUS Servers	82

Viewing Auth Cached Users	83
Setting Date and Time	84
Using NTP Servers to Automatically Set the Date and Time	84
Adding and Editing NTP Servers	84
Refreshing NTP Server Status	85
Deleting and Disabling NTP Servers	85
Configuring Date and Time Manually	85
Updating the CBW AP Software	86
Updating the Software using HTTP	88
Upgrading the Software for First Mesh Extender using HTTP	89
Updating the Software using TFTP	90
Updating the Software using SFTP	91
Updating the Software through Cisco.com	92
Updating the Software through Cisco Business Dashboard	93

CHAPTER 7**Services 95**

Media Steam	95
About Multicast Domain Name System	98
Restrictions for Configuring Multicast DNS	100
Configuring Multicast DNS	100
Mapping mDNS Profile to WLAN	101
Configuring mDNS Policy	102
Cisco Umbrella Overview	103
Configuring Cisco Umbrella on Primary AP	104
Adding Policy to Umbrella Profile	104
Applying Cisco Umbrella Profile to WLAN	105

CHAPTER 8**Advanced 107**

Managing SNMP	107
Configuring SNMP Access	107
SNMP Trap Receivers	108
Add an SNMPv3 User	109
Delete SNMPv3 User	109
Setting Up System Message Logs	110

System Logs	111
Optimizing RF Parameters	111
Advanced RF Parameters	111
Optimized Roaming	111
Restrictions for Optimized Roaming	112
Configuring Optimized Roaming	112
RF Profiles	113
RF Parameter Optimization Settings	114
Troubleshooting in Primary AP	116
UI Indicator	116
Using Primary AP Tools	116
Restarting the Primary AP	116
Clearing the Primary AP Configuration and Resetting to Factory Defaults	116
Clearing Configurations for all APs and Resetting to Factory Defaults	117
Export and Import Primary AP Configuration	117
Saving the Primary AP Configuration	118
Troubleshooting Files	118
Troubleshooting Tools	118
Uploading Files	119
Certificates	121
Security Settings	121
Configuring Access Control Lists (ACL)	122
Applying the ACL to WLAN at Pre-Auth Level	124
Applying the ACL to WLAN at Post-Auth Level	124
Configuring AAA Override in WLAN	124
Cisco Business Dashboard Settings	124

APPENDIX A

Appendix - Supporting Topics	127
LAN port functionality for different models	127
LED Color Indicators for Cisco Business Wireless APs	128
LED Display Settings	130
Primary AP Failover and Election Process	131
Pre-downloading an Image to an Access Point	132
Creating a Guest Network	132

Resetting a Device to Factory Default 133
 SNMP Traps in CBW AP 135
 Deployment and Troubleshooting Guidelines 136

APPENDIX B

Appendix - Mounting and Grounding Access Points 141

About Mounting 141
 Preparing the AP for Installation 141
 Mounting CBW140AC/240AC 142
 Mounting CBW145AC 147
 Mounting CBW141AC 152
 Mounting CBW142AC 152
 Mounting CBW143AC 157
 Grounding an Access Point 159

APPENDIX C

Appendix - Glossary of Terms 161

Cisco Business Wireless - Glossary Of Terms 161

0-9 161

802.1Q-based VLAN 161

802.1X Supplicant 161

A 161

ACL 161

Allowlist 162

B 162

Band Steer 162

Bandwidth 162

Bandwidth Utilization 162

Blocklist 162

C 162

Captive Portal 162

CBD Probe 162

Central web authentication (CWA) 162

Channel Isolation 162

Channel Width 163

Client QoS 163

Connection Speed	163
D	163
DCA	163
E	163
EAPoL	163
Event Logging	163
F	164
Fast Roaming	164
H	164
HTTPS	164
I	164
IPv4	164
IPv6	164
ISE	164
L	164
LLDP	164
Load Balancing	165
Local Probe	165
M	165
Max Data Rate	165
Multiple SSIDs	165
N	165
Network Plug n Play	165
O	165
Operating Mode	165
P	165
PMKID	165
PoE-PD	166
PoE-PSE	166
Q	166
QoS	166
R	166
RADIUS Server	166
Radio Domains	166

Rogue AP Detection	166
S	166
Scheduler	166
Signal Quality	167
Signal Strength	167
Spatial Streams	167
Spectrum Intelligence	167
SSID	167
SSID Broadcast	167
V	167
VLAN	167
W	168
WDS	168
WPA/WPA2	168
WPA2 Enterprise	168
WPA3	168

APPENDIX D

Appendix - Cisco Online Support	169
Cisco Business Online Support	169



CHAPTER 1

Cisco Business Wireless Access Points Overview

This chapter contains the following sections:

- [About Cisco Business Wireless Access Points, on page 1](#)
- [Supported Cisco Access Points, on page 1](#)
- [Supported Software Images, on page 2](#)
- [Supported Browsers, on page 2](#)
- [Related Documents, on page 3](#)

About Cisco Business Wireless Access Points

The Cisco Business Wireless (CBW) network solution comprises of at least one 802.11ac Wave 2 Cisco Business Series Access Point with an in-built software that manages other access points in the network.

An Access Point (AP) that controls all the Access Points in the network is termed as the Primary AP and the access points controlled by the Primary AP is termed as the Subordinate AP in this guide.

The Primary AP has two roles: It controls all the Subordinate APs that join the network. It independently serves wireless clients like other Subordinate APs.

You may refer this administration guide for details on both the Primary APs and the Subordinate APs. It provides instructions on getting started with an access point and also explains various options available to monitor and manage the APs using the WebUI.



Note Cisco Business Wireless AP has the capability to interface with the Cisco Business Dashboard to monitor and manage your access points connected with the Primary AP. For more details, refer to [Cisco Business Dashboard Administration Guide](#).

Supported Cisco Access Points

The following Cisco Business Series APs are supported in the Cisco Business Wireless (CBW) AP network:



- Note**
- APs listed under Primary APs can also function as Subordinate APs.
 - This Administration Guide can be referred for both Primary APs and the Subordinate APs of all models in this series.

Table 1: Cisco APs supported in the CBW AP network

Primary APs	Subordinate APs
Cisco Business 140AC Access Point	Cisco Business 141AC Mesh Extender
Cisco Business 240AC Access Point	Cisco Business 142AC Mesh Extender
Cisco Business 145AC Access Point	Cisco Business 143AC Mesh Extender
Note While the Primary APs (140, 145 & 240) may be used as Subordinate APs, the Mesh Extenders (141, 142 & 143) cannot be used as a Primary AP.	Cisco Business 140AC Access Point
	Cisco Business 240AC Access Point
	Cisco Business 145AC Access Point

Supported Software Images

You can download the CBW AP software for your AP model by navigating to <https://software.cisco.com/download/navigator.html>

From the **Software Download** window, go to **Wireless > Access Points**. Based on your AP model, navigate to **Business 100 Series Access Points / Business 200 Series Access Points** and select a model from the list. You can view a list of currently available software with the latest version at the top. Choose the required version of the firmware image and proceed with the download to update the software.

Supported Browsers

Cisco Business Wireless Access Points are administered through a web user interface. To use this interface, your browser must be one of the following:

- Microsoft Internet Explorer 10 or above
- Apple Safari version 7 or above
- Mozilla Firefox version 33 or above
- Google Chrome version 38 or above

You can also use the Cisco Business App on your mobile phone to monitor and administer the Access Points. You will need one of the following Operating Systems:

- Android version 5.0 or above
- iOS version 8.0 or above

Related Documents

The documentation for Cisco Business Wireless Access Points is comprised of a number of separate guides.

These include the following:

Resources	Description
Administration Guide	This guide provides details on performing configuration for Cisco Business Wireless Access Points (APs) and also provides advanced options to manage and monitor APs in the Cisco Business Wireless AP network. Note This guide can be referred for both Primary APs and the Subordinate APs of all models in this CBW series.
Quick Start Guide	This guide provides details on performing the initial setup and configuration for Cisco Business Wireless Access Points (APs) using the most commonly selected options. For an overview of the basic tasks, refer the <i>Cisco Business Wireless Quick Start Guide</i> .
Release Notes	Summary of the features and caveats for Cisco Business Wireless Access Points (APs).
Open Source Documents (OSD)	This document contains the licenses and notices for open source software used in this product.
Cisco Regulatory Compliance and Safety Information (RCSI)	This document provides domestic and international regulatory compliance and safety information for the Cisco Business Wireless Access Points (APs).
Translated End-User Documents	The Translated Administration Guides for all APs supported by the Cisco Business Wireless Access Points (APs) are available in the <i>Cisco Business Wireless Access Points (APs)</i> product page on Cisco.com.



CHAPTER 2

Using Cisco Business Wireless Access Point GUI

This chapter contains the following sections:

- [Using the Cisco Business Wireless Access Point GUI, on page 5](#)

Using the Cisco Business Wireless Access Point GUI

Overview of the Cisco Business Wireless Access Point GUI with a description of the navigation pane links

Home window

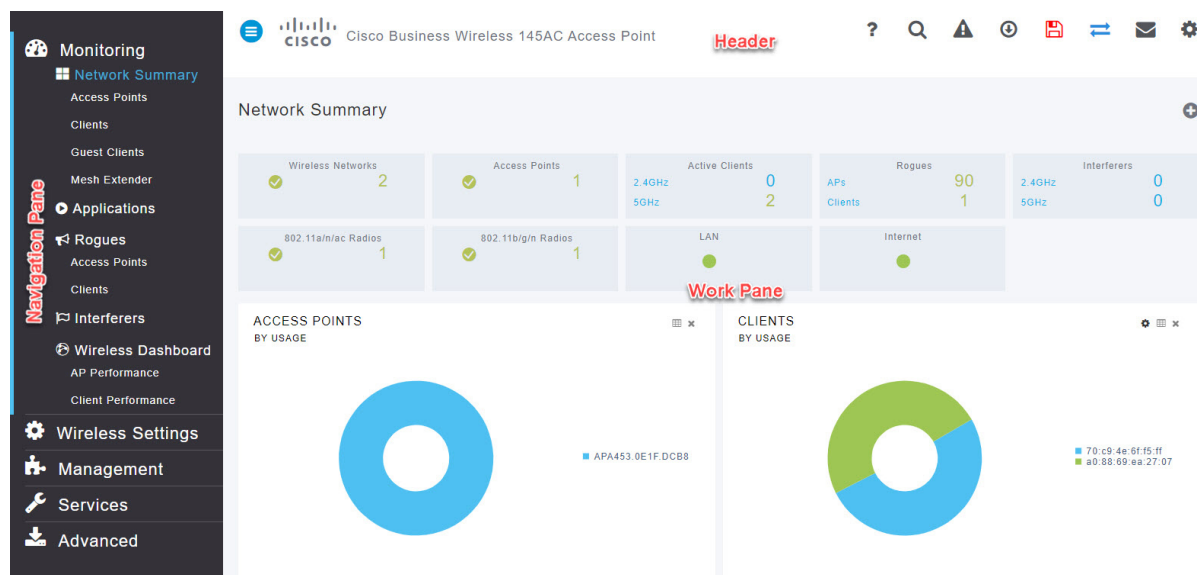





























Table 2: Cisco Business Wireless Access Point Home Page






Name	Description
Navigation pane	Provides access to the Cisco Business Wireless features. Each of these main feature tabs comprises of sub-level tabs. Click to expand and view the sub-level tabs.

Name	Description																				
Work pane	Area where the feature interface is displayed. When you click an option in the Navigation pane, its corresponding window opens in this area.																				
Header toolbar	<p>The header toolbar contains the following options:</p> <table border="1" data-bbox="513 470 1490 1757"> <tbody> <tr> <td data-bbox="513 470 711 611"></td> <td data-bbox="711 470 1490 611">A hamburger icon (toggle button) for expanding and collapsing the navigation pane.</td> </tr> <tr> <td data-bbox="513 611 711 730">Cisco Product Name</td> <td data-bbox="711 611 1490 730">Header title is the title of the web interface which indicates the AP model of the Primary AP (on which the integrated CBW AP functionality is currently operating).</td> </tr> <tr> <td data-bbox="513 730 711 871"></td> <td data-bbox="711 730 1490 871">Click the help icon (?) to view the Cisco Business Access Point Online Help document.</td> </tr> <tr> <td data-bbox="513 871 711 991"></td> <td data-bbox="711 871 1490 991">A search icon for searching an AP or client using its MAC address.</td> </tr> <tr> <td data-bbox="513 991 711 1131"></td> <td data-bbox="711 991 1490 1131">A notification icon that indicates if there was an incident of system crash or if a core dump is present.</td> </tr> <tr> <td data-bbox="513 1131 711 1272"></td> <td data-bbox="711 1131 1490 1272">A download icon that indicates if a new software update is available for your CBW APs on cisco.com. You may click this icon to redirect to the software update page in the UI and download the latest firmware.</td> </tr> <tr> <td data-bbox="513 1272 711 1371"></td> <td data-bbox="711 1272 1490 1371">A save icon to save the current CBW AP configuration to the NVRAM. For more details, see Saving the Primary AP Configuration, on page 118.</td> </tr> <tr> <td data-bbox="513 1371 711 1488"></td> <td data-bbox="711 1371 1490 1488">A bi-directional icon to switch to Expert View to access advanced user options. The default is set to standard view.</td> </tr> <tr> <td data-bbox="513 1488 711 1629"></td> <td data-bbox="711 1488 1490 1629">Click this mail icon to send your feedback or request for new features to Cisco Business Wireless Team. Note This is not intended for support questions.</td> </tr> <tr> <td data-bbox="513 1629 711 1757"></td> <td data-bbox="711 1629 1490 1757">A gear icon to view the current system information or to log off the Primary AP web interface. It also specifies the username of the user who has logged into the application.</td> </tr> </tbody> </table>		A hamburger icon (toggle button) for expanding and collapsing the navigation pane.	Cisco Product Name	Header title is the title of the web interface which indicates the AP model of the Primary AP (on which the integrated CBW AP functionality is currently operating).		Click the help icon (?) to view the Cisco Business Access Point Online Help document.		A search icon for searching an AP or client using its MAC address.		A notification icon that indicates if there was an incident of system crash or if a core dump is present.		A download icon that indicates if a new software update is available for your CBW APs on cisco.com. You may click this icon to redirect to the software update page in the UI and download the latest firmware.		A save icon to save the current CBW AP configuration to the NVRAM. For more details, see Saving the Primary AP Configuration, on page 118 .		A bi-directional icon to switch to Expert View to access advanced user options. The default is set to standard view.		Click this mail icon to send your feedback or request for new features to Cisco Business Wireless Team. Note This is not intended for support questions.		A gear icon to view the current system information or to log off the Primary AP web interface. It also specifies the username of the user who has logged into the application.
	A hamburger icon (toggle button) for expanding and collapsing the navigation pane.																				
Cisco Product Name	Header title is the title of the web interface which indicates the AP model of the Primary AP (on which the integrated CBW AP functionality is currently operating).																				
	Click the help icon (?) to view the Cisco Business Access Point Online Help document.																				
	A search icon for searching an AP or client using its MAC address.																				
	A notification icon that indicates if there was an incident of system crash or if a core dump is present.																				
	A download icon that indicates if a new software update is available for your CBW APs on cisco.com. You may click this icon to redirect to the software update page in the UI and download the latest firmware.																				
	A save icon to save the current CBW AP configuration to the NVRAM. For more details, see Saving the Primary AP Configuration, on page 118 .																				
	A bi-directional icon to switch to Expert View to access advanced user options. The default is set to standard view.																				
	Click this mail icon to send your feedback or request for new features to Cisco Business Wireless Team. Note This is not intended for support questions.																				
	A gear icon to view the current system information or to log off the Primary AP web interface. It also specifies the username of the user who has logged into the application.																				

Navigation Pane Options

The **Navigation** pane provides options to access the main Cisco Business Wireless Access Point features. Each of these options comprises several sub-options to perform various other tasks.

Table 3: Navigation Pane Options

Icon	Name	Description
	Monitoring	The Monitoring feature allows the Primary AP to monitor WLANs and all the connected devices on the network. It also helps to view the performance of your APs, clients and guest clients in the network. For more details, refer to About the Cisco Business Wireless AP Monitoring Service, on page 19 in this guide.
	Wireless Settings	The Wireless Settings page is used to administer associated APs, manage WLANs, WLAN user accounts, and guest user accounts. For more details, refer to About WLANs and RLANS in CBW Access Point Network, on page 43 in this guide.
	Management	The Management page allows you to set management access parameters, manage admin accounts, manage network time, and perform software updates. For more details, refer to Setting Up Management Access Interface, on page 75 in this guide.
	Services	The Services page provides the mDNS service discovery feature and the Cisco Umbrella network security feature. For more details, refer to About Multicast Domain Name System, on page 98 in this guide.
	Advanced	The Advanced page provides the capability to set SNMP, syslog, and log configuration settings and to perform a reset to factory default. For more details, refer to the Advanced, on page 107 section in this guide.



CHAPTER 3

Getting Started

This chapter contains the following sections:

- [Prerequisite for Setting up and Accessing Cisco Business Wireless AP, on page 9](#)
- [AP Deployment Models, on page 10](#)
- [Launching the Setup Wizard, on page 12](#)
- [Using the Setup Wizard, on page 13](#)
- [Logging into the Cisco Business Wireless AP, on page 16](#)
- [Adding New Subordinate APs, on page 16](#)
- [Adding Mesh Extenders, on page 17](#)

Prerequisite for Setting up and Accessing Cisco Business Wireless AP



Important

Ensure that there is no Primary AP running in the network other than the CBW AP during setup or daily operation of a CBW AP network. The Cisco Primary AP cannot inter-operate or co-exist with other Primary APs in the same network.



Important

Decide on the first access point (AP) to be set up. The first AP to be set up should be the one that supports the Primary AP functionality. This is to ensure that this AP can act as the Primary AP, and the other APs can then connect to it as Subordinate APs. This will ensure that the pre-defined *CiscoBusiness-Setup* Service Set Identifier (SSID) is broad-cast only by the Primary AP and not by other APs.

- Ensure that the AP is installed as per the instructions in the *Quick Start Guide*.
- The initial setup of the CBW AP can be performed using the following methods:
 - Through the Primary AP Setup Wizard and over Wi-Fi
 - Cisco Business Mobile App
 - Using *Network Plug n Play* via **Cisco Business Dashboard** application. For details, refer to the section, *Network Plug and Play* in the [Cisco Business Dashboard Administration Guide](#).

- If you are not using the Cisco Business Mobile App, you will need a Wi-Fi enabled laptop to connect to the pre-defined *CiscoBusiness-Setup* SSID broadcasted by the Primary AP. You cannot access this SSID through a wired network.



Note Only one client is allowed to connect to the *Ciscobusiness-Setup* SSID for security purposes. If connection is refused, another device may have joined automatically. In this case, you should reboot the AP.

- Your laptop should have a compatible browser. For a list of browsers compatible with the CBW AP web user interface (UI), see [Supported Browsers, on page 2](#).

AP Set Up Checklist

Before you set up and use your CBW network, follow the steps below for a successful deployment.

1. Decide on the AP Deployment model.
2. Use the setup wizard to configure the primary AP.
3. Configure the Wireless Networks on your primary AP.
4. If needed, add the subordinate APs.
5. Verify all your settings.

AP Deployment Models

The following deployment models are supported in the Cisco Business Wireless AP network:

- **Non-Mesh deployment (wired deployment only)**— All the APs in the CBW AP network have a Wired Uplink. The supported APs in the network are Primary capable. One among them will serve as a Primary AP and the other APs (referred to as Subordinate APs) in the CBW network will join the Primary AP. The APs will act in AP-only mode.

Supported APs (Primary APs)— CBW140AC, CBW145AC, CBW240AC.





Note Ensure that the switch is in turn connected to the router for internet access.

- **Mesh deployment (wireless deployment with single/multiple wired uplink APs)**— In this deployment model, the CBW AP network comprises of both Primary AP and Subordinate APs (wired APs and wireless Mesh Extenders). The APs that have a wired uplink (includes the Primary AP) acts as Root AP (RAP) to which the Mesh Extenders (MAP) joins wirelessly. Primary AP will act in Bridge mode. To setup this deployment, refer to the section, [About Cisco Mesh](#). For Associating the wireless Mesh Extenders to the network, add the Ethernet MAC address of the Extenders in the local MAC address table of the Primary AP. For details, refer to [Adding Mesh Extenders, on page 17](#). Wireless Mesh Extenders have the dynamic algorithm to select the best RAP based on the signal strength and join the same.



Note Ensure that you enable **Mesh** while configuring the **Initial Setup Wizard** for this deployment model.

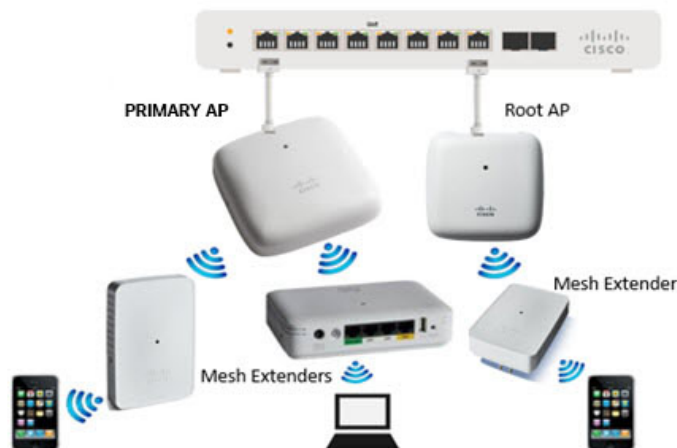


Note Only Mesh Extenders (such as CBW141AC, CBW142AC & CBW143AC) are required to be manually added to the auth-list. Where as, the Subordinate APs that are non-Mesh Extenders (such as CBW140AC, CBW145AC & CBW240AC) are connected via wired uplink and are automatically added to the auth-list.

You can obtain the MAC address by reading the QR code on the back of the device with a QR Reader app on a mobile phone. You can also find the MAC address at the bottom of the AP Device.

Supported APs in Mesh deployment:

- **Primary APs**— CBW140AC, CBW145AC, CBW240AC
- **Subordinate APs**— CBW141ACAM, CBW142ACM, CBW143ACM, CBW140AC, CBW145AC, CBW240AC.



Note APs listed under Primary APs can also function as Subordinate APs.

Launching the Setup Wizard



Note You may use the Cisco Business Mobile App instead of the Web UI to run the setup wizard.

Step 1 Boot the AP that has the Primary capability.

In a few minutes, the *CiscoBusiness-Setup* SSID starts broadcasting and the AP's status LED cycles through patterns from red, amber and green to blinking green.

Step 2 Connect the laptop to the *CiscoBusiness-Setup* SSID through Wi-Fi and enter the default password: **cisco123**.

Note The laptop obtains an IP address from the subnet of the Primary AP.

Step 3 Launch a supported web browser, such as Chrome, Firefox, Safari or Internet Explorer.

For the Apple clients, after connecting to the *CiscoBusiness-Setup* SSID, the captive portal window may automatically open with the Welcome page followed by the initial Setup Wizard.

Note After connecting to the *CiscoBusiness-Setup* SSID, upon opening a web browser, you should automatically be redirected to <http://ciscobusiness.cisco>. If not, go to the following step.

Step 4 In the address bar, type the URL: <http://ciscobusiness.cisco> and press **Enter**

Step 5 Click **Start** on the **Cisco Business Wireless Access Point** page to launch the Setup Wizard. You will be required to create an admin account.

- Note** Only one client can be connected to the CiscoBusiness-Setup SSID at a time.
- When connecting to CiscoBusiness-Setup SSID, if you see an invalid password error on your client, it indicates that another client has been connected to the SSID.
- You may confirm this by checking the LED status of the AP to be solid green. Turn off the client that is already connected and proceed with the Setup Wizard configuration of your AP.

For instructions on entering details on the Setup Wizard page, refer to [Using the Setup Wizard, on page 13](#).

Using the Setup Wizard

The Setup Wizard helps you configure certain basic parameters on your Cisco Business Wireless AP (CBW AP), and thereby get your AP network running.

Once you have completed the steps in [Launching the Setup Wizard, on page 12](#), use the following sections as a reference for the data that you enter and proceed with the configuration wizard pages.

Welcome Screen

Click the **Start** button in the **Welcome** screen. The **Cisco Business Wireless Access Point** page relevant to your AP model is displayed.

1. Create an admin user account on the Primary AP. You can enter up to 24 ASCII characters.



Note The username is case sensitive and cannot be cisco or its variant.

2. Enter a password. The password can contain 8-127 ASCII characters. When specifying a password, ensure the following:
 - The password must include lowercase letters, uppercase letters, digits, or special characters. The special characters can be ~, !, @, #, \$, %, ^, &, *.
 - No character in the password can be repeated more than three times consecutively.
 - The new password cannot be the same as the associated username or the username reversed.
 - The password cannot be cisco, ocsic, or any variant obtained by changing the capitalization of the letters in the word Cisco. In addition, you cannot substitute l, I, or ! for i, 0 for o, or \$ for s.
3. Confirm the password and click **Start**.

Set Up Your Primary AP

Specify the following basic parameters for setting up your Primary AP:

Field	Description
Primary AP Name	<p>Enter the name that you want to assign to the Primary AP.</p> <p>Note A max of 24 characters is allowed.</p> <p>The characters can be upper/lowercase letters, numbers, dot, and hyphen.</p> <p>The name should always start with an alphabet and should not end with '.' or '-'.</p>
Country	<p>Choose the country that matches the physical location of the CBW AP.</p> <p>Note The CBW AP will display only countries that are supported by the regulatory domain of the AP. You can choose your country from the drop-down list.</p> <p>There are strict regulatory rules to operate under the proper country code during the usage.</p>
Date and Time	<p>Specify the date. By default, your device's system time is applied. You can manually edit the date and time, if required.</p>
Timezone	<p>Select your time zone.</p>
Mesh	<p>To add Mesh Extenders to your AP network, enable the Mesh option. By default this option is disabled.</p>
Would you like Static IP for your Primary AP (Management Network)	<p>Enable this option, if you want to configure a static IP for the management interface. If not, the interface gets an IP address from your DHCP server (typically in your router). By default, this option is disabled.</p> <p>Note A management IP address should be within current subnet of your local VLAN and not in the client pool issued by your DHCP server.</p> <p>If you choose to configure the static IP, then you will be required to enter data in the following fields. If not, you can proceed to the next section.</p> <p>Note Even when a static IP address is selected for the Primary AP, a DHCP server is still required to provide IP addresses to the Access Points and Clients. If the device cannot find a DHCP server after completing the Day0 setup sequence and rebooting, it will not complete the bootup sequence and the LED will be blinking Red.</p>

Field	Description
Management IP Address	Enter the IP address for managing the Primary AP.
Subnet Mask	Enter the subnet mask for the Primary AP.
Default Gateway	Enter the default gateway or router IP address for the Primary AP.

Create your Wireless Networks

Specify the following parameters:

Field	Description
Network Name	Specify a SSID for your Wireless network. You can enter up to 31 characters in this field. Note Make a note of this SSID to connect a client and log into the CBW web user interface which is detailed in the later section of this chapter. For details, refer to Logging into the Cisco Business Wireless AP, on page 16 .
Security	By default, the SSID security is set to WPA2 Personal that uses pre-shared key (PSK) authentication. Choose SSID security for your Wireless network. It can be one of the following options: WPA2 Personal - This uses pre-shared key (PSK) handshake mechanism for authentication WPA2+WPA3 - Personal - This has both WPA2 and WPA3 enabled. WPA3 uses a reliable handshake mechanism called Simultaneous Authentication of Equals (SAE).
Passphrase	Specify the passphrase or the pre-shared key (PSK). The password should contain 8 - 63 ASCII characters. Note Make a note of this Passphrase to connect a client to the SSID and log into the CBW web user interface which is detailed in the later section of this chapter. For details, refer Logging into the Cisco Business Wireless AP, on page 16 .
Confirm Passphrase	Re-Enter the passphrase or the pre-shared key (PSK) here.
Show Passphrase	Enable in order to display the passphrase in clear text for visible confirmation.

Once you complete the configuration settings, click **Next** to proceed or **Back** to modify the data in the previous screens. Confirm the settings and click **Apply** to save the configuration.

The access point reboots. This may take up to 5 minutes. The booting process is complete when the LED is consistently blinking green, or solid green.



Note For a detailed explanation on the LED behavior, see, [LED Color Indicators for Cisco Business Wireless APs, on page 128](#).

You can now proceed to [Logging into the Cisco Business Wireless AP, on page 16](#).

Logging into the Cisco Business Wireless AP

Once you have completed the steps in [Using the Setup Wizard, on page 13](#), follow the subsequent instructions to log into the CBW AP web user interface (UI). You can monitor and manage the access point and associated devices using this web interface (UI).

-
- Step 1** Connect to the new SSID that you created using the **Setup Wizard ->Create Your Wireless Network** process.
- Step 2** Open a supported web browser. In the address bar, type `https://ciscobusiness.cisco` or `https://<ip address>` and press **Enter**. The **Cisco Business Wireless Access Point** login page is displayed.
- The CBW AP uses a self-signed certificate for HTTPS. Therefore, all browsers will display a warning and ask you whether you wish to proceed with an exception when the certificate is presented to the browser. Accept the warning in order to access the Primary AP login page.
- Note** If the Firefox browser doesn't throw an exception, navigate to **Options > Privacy & security > Certificates > view certificates> Servers > Add exception** and add an exception for `https://ciscobusiness.cisco`
- Step 3** Click **Login** and enter the user name and password you created during the initial Setup Wizard process to proceed with using the web UI options.
-

What to do next

After you log in, the default landing page is the **Network Summary** window. For more information, see [About the Cisco Business Wireless AP Monitoring Service, on page 19](#).

Adding New Subordinate APs

If you have a CBW network up and running, then adding new wired APs to the network is easy.

-
- Step 1** Plug the Wired uplink AP (CBW140AC, CBW145AC or CBW240AC) into the Ethernet LAN in which the current Primary AP is connected.
- Step 2** The new AP will boot up, update its firmware to match the Primary AP, copy the configuration information and then join the Wireless Network.

Now, you can manage the newly added AP through the Web UI by navigating to **Wireless Settings > Access Points** page.

Adding Mesh Extenders

You can add a Mesh Extender such as CBW141ACM, CBW142ACM, or CBW143ACM to the Wireless Network.

Ensure that you have enabled the **Mesh** option in the initial setup wizard. If not, then, go to **Wireless Settings > Mesh**, enable the **Mesh** toggle button and click **Apply**. For detailed information, refer to [About Cisco Mesh, on page 69](#).

Now, MAC address of the Mesh Extender should be added to the Local MAC Addresses table. You can add this using one of the following methods:

Using the Management Web UI

You must enter the MAC address of all Mesh Extenders that you want to use in the mesh network with the Primary AP. A Primary AP responds only to discovery requests from indoor radios that appear in its authorization list. To add the MAC Address in **Auth-List**, do the following:

1. Navigate to **Wireless Settings > WLAN Users > Local MAC Addresses**.
2. Click **Add MAC Address**.
3. Specify the MAC Addresses.
4. In the **Description** field, specify a description of the mesh access point. The text that you enter identifies the mesh access point on the Primary AP.



Note To make it easier you can include the last few digits of the MAC address, such as ap1522:62:39:10, the location, or the name.

5. You can now choose to join or block an Access Point using the following instructions:
 - Choose the **Type** as **Allowlist** to join the access points to the Primary AP.
 - Choose the **Type** as **Blocklist** to block a particular access point from joining the Primary AP.



Note Blocklisting a client or Mesh Extender that is currently joined to the network will not take effect until it attempts to rejoin the network (after disconnect or reboot).

6. Select the **Profile Name** from the drop-down list and click **Apply**. By default, the profile name is mapped to **Any WLAN/RLAN**.

You may now check to see if the MAC address you added has been listed in the AP network by navigating to **Wireless Settings > Access Points**. You will find the MAC address added in the column, **AP Mac** along with the AP name under the **AP Model** column of the table.

Using the Cisco Business Mobile App

1. Connect to the SSID setup for the Primary AP and log into the Primary AP admin account.
2. Select **Monitor my Network**, then choose **Add a device**.
3. Scan the MAC address of the Mesh Extender using the QR code reader.

To troubleshoot issues with Mesh Extender, refer to [Deployment and Troubleshooting Guidelines](#), on page 136.



CHAPTER 4

Monitoring

This chapter contains the following sections:

- [About the Cisco Business Wireless AP Monitoring Service, on page 19](#)
- [Customizing the Network Summary View, on page 20](#)
- [Customizing Access Points Table View, on page 21](#)
- [Viewing Access Point Details, on page 22](#)
- [Viewing Client Details, on page 29](#)
- [Viewing Guest Client Details, on page 32](#)
- [Troubleshooting a Client, on page 33](#)
- [Viewing Mesh Extender, on page 34](#)
- [Viewing Applications, on page 35](#)
- [Viewing Rogue Access Points, on page 35](#)
- [Viewing Interferer Details, on page 37](#)
- [Wireless Dashboard, on page 37](#)
- [Customizing the Access Point Performance View, on page 39](#)
- [Customizing the Client Performance View, on page 40](#)

About the Cisco Business Wireless AP Monitoring Service

The Cisco Business Wireless AP Monitoring service enables the Primary AP to monitor the WLANs and all the connected devices on the network.

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

- View details of configured WLANs.
- View list of top WLANs based on traffic and associated clients.
- View details of APs in the network.
- View details of clients operating actively at either 2.4 GHz or 5 GHz.
- View summary of client device, guest client device, operating systems and applications running on these devices.
- View a detailed list of rogue clients and APs.

- View details of various interferers in the network on the 2.4 GHz and 5 GHz radio frequencies.
- Monitor the performance of APs in the network.
- Monitor the performance of clients and guest clients in the network.

**Note**

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

Customizing the Network Summary View

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

**Note**

Each of the action icons available within the widget is discussed in the [Using the Widgets](#) section.

The following widgets are displayed in the Network Summary page.

- **OPERATING SYSTEMS** (By clients)—Displays the OS information of the Clients (such as Linux clients, Android clients and so on) that are connected to the WLAN. For this feature, the user has to enable Local Profiling in the WLAN.
- **GUESTS** (By usage)—Displays the Top 10 guest clients in the network based on the throughput and usage.
- **ACCESS POINTS** (By usage)—Displays the Top 10 access points in the network based on the number of clients connected, usage and throughput.
- **APPLICATIONS** (By usage)—Displays the Top 10 applications such as gmail, youtube, facebook and so on based on usage level of the clients connected in the network. For this feature, the user has to enable the Application Visibility Control (AVC) option in the WLAN.
- **TOP WLANS** (By usage)—Displays the Top 10 WLANs in the network by usage and number of clients connected.
- **CLIENTS** (By usage)—Displays the Top 10 clients in the network based on throughput and usage.

Using the Widgets

This section details the various icons/options available within the widget to customize and view data as required.

- Use the **x** icon within a widget to remove the widget from the **Monitoring** page.
- Use the **+** icon on the top right to add the widget in the **Monitoring** page.

- Use the clear data (gear) icon to clear the usage data and reset to zero.
- Use the tabular (graphical) toggle icon and the tabulated list toggle icon to change the display of data between tabular view or doughnut view.
- Use the Save icon within a widget to export the top 10 entries locally in Excel format.



Note All entries will be exported for Guests widget.

Customizing Access Points Table View

Step 1 Navigate to **Monitoring > Network Summary > Access Points**.

Note You can also obtain high level details of the Access point by clicking on the count link in the **Access Points** summary section under **Monitoring > Network Summary** page.

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

- AP Name**—Displays the name of the access point.
- Role**—Pictorial representation of the type of AP. A Primary AP is depicted with a (P) attached to the AP icon, a Mesh Extender is represented by an (E) attached to the AP icon and a Primary capable AP has no letter specified to the AP icon.
- Type**—Specifies if the AP is a Primary AP, Primary capable AP or a Mesh Extender.
- IP Address**—The IPv4 address of the device.
- Model**—Model of the CBW AP.
- Clients**—Number of client devices connected to the access point
- Usage**—The amount of data that has transferred between access point and the client device.
- Uptime**—Duration of how long the AP has been powered up.
- Admin Status**—Displays the configured status of 2.4GHz / 5GHz Radio is enabled or disabled.
- Operational Status**—Displays the running status of 2.4GHz / 5GHz Radio.
- Channel Utilization**—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. The values are represented in % format.
- Throughput(Avg)**—This represents the amount of data that can be transferred from the access point to the client device.
- Channel**—Channel number at which the access point's radio is broadcasting the signal.
- Transmit Power (Avg)**—The logarithmic power level at which the access point is broadcasting the signal. The values are displayed in decibel-milliwatt (dBm) units.
- Coverage Hole**—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 -80dBm of data RSSI.
- Interference(Avg)**—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. The values are represented in % format.

- q) **Noise**—Noise refers to any energy interference that degrades the quality of a wireless signal. Noise can affect everything from radio transmissions to network speeds. The values are displayed in decibel-milliwatt (dBm) units.
- r) **Rogues**—Any device that shares your channel and is not managed by your CBW network can be considered as a Rogue.
- s) **MAC Address**—The Unique physical address of the device.
- t) **Mode**—Displays if the device is in AP Only mode or Mesh mode.

Step 3 You can click the downward arrow on the top right of the column headers to customize the details displayed in the table. You may choose to hide, show or rearrange the desired columns, sort them in the order you wish or filter the table contents based on the desired parameters.

Viewing Access Point Details

Navigate to **Monitoring > Network Summary > Access Points**.

Click on one of the Access Point to display the **Access Point View** page. This page consists of the following AP parameter details:

GENERAL

- **AP Name**—Displays the name of the access point.
- **Location**—The physical location of the access point.
- **MAC Address**—The Unique physical address of the device.
- **Base Radio MAC**—The Hardware (HW) address of 2.4 and 5GHz radios. (The address is same for both the radios).
- **IP Address**—The IPv4 address is a 32-bit number that uniquely identifies an access point.
- **CDP / LLDP**—The name and the port of the switch to which the access point is connected.



Note This field is applicable only for Primary capable APs. (Wired uplink APs).

- **Ethernet Speed**—Link speed capability of the switch port.
- **Model / Domain**—Model number of the access point / Radio domains.
- **Power Status**— Indicates the power level and mode of power.
- **Parent MAC Address**—Displays the Parent MAC address (AP to which it is connected wirelessly) This option is available only for Mesh Extenders.
- **Nearest APs**—Displays the top 3 neighbor APs with high link SNR value. For more information see **Link SNR (dBm)** in [Viewing Mesh Extender, on page 34](#).

This field is helpful for determining best location APs and Mesh extenders during installation. It would also help to troubleshoot connectivity issues.



Note The nearest AP field also displays Wireless Mesh Extenders.

- **Serial Number**—The unique number provided at the time of manufacturing.
- **Max Capabilities**—The radio domains, Spatial streams and maximum data rates of the access point.

TECH SUPPORT

You can download the support bundle for individual Access Points, which provides the AP boot-up logs and specifies the configurations applied.

To generate and download the bundle, use **Start** and **Download** in the Primary AP UI.

- **Start**—Click **Start** to start the bundle generation. By default, this button is enabled.
- **Download**—Click **Download** to save the bundle locally. This button will be enabled only after the bundle is generated.



Note The Pop-up blocker should be disabled in your Browser settings to download the tech support bundle for the AP.

The status of the bundle generation can be tracked by using the **Tech Support Status**.



Note Tech Support bundle can be generated for only one AP at a time.

Tech Support Status—The support bundle generation status can be viewed in this field. The status values can be one of the following:

- **Not started**—The bundle generation has not been triggered. This is the default status.
- **In Progress**—Bundle generation is in progress.
- **Completed**—The bundle generation is complete and can be downloaded using **Download**.

PERFORMANCE SUMMARY

This table provides the following details specific to the radios:

- **Number of clients**—The number of client devices connected to a specific Access Point.
- **Channel**—Channel number at which the access point's radio is broadcasting the signal.



Note Number of channels will be 1, 2 and 4 for 20MHz, 40MHz and 80 MHz respectively.

- **Configured Rate**—The default minimum and maximum data rates of the access point.

- **Usage Traffic**—The amount of data that has transferred between access point and the client device.
- **Throughput**—This represents the amount of data that can be transferred from the access point to the client device.
- **Transmit Power**—The logarithmic power level at which the access point is broadcasting the signal.
- **Noise**—Noise refers to any energy interference that degrades the quality of a wireless signal. Noise can affect everything from radio transmissions to network speeds.
- **Channel Utilization**—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.
- **Interference**—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.
- **Traffic**—Shows the data traffic in 2.4GHz and 5GHz radio.
- **Admin Status**—Status of the Radios for 2.4 GHz and 5 GHz.
- **Interferer Detection**—Status of Interferer detection for 2.4GHz and 5GHz radios.

{AP Name} DETAILS

This table provides the following details specific to the Access Point:

- **CLIENTS**—This table shows the client details that are connected to it. For per field details, refer to [Viewing Client Details, on page 29](#).
- **RF TROUBLESHOOT**—Displays a visual graphical representation of parameters that can affect the radio performance of the access points, such as:
 - **NEIGHBOR AND ROGUE APs**—Displays the Neighbor and Rogue APs on the current and adjacent channels for a given radio and the signal strength they are heard at. This visualization allows you to quickly identify Neighbor and Rogue APs that are causing interference and reducing the overall RF performance for the cell.
 - **CLEAN AIR INTERFERERS**—Displays the sources of non Wi-Fi interferers and their severity on the current and adjacent channels for a given radio. This visualization allows you to quickly identify non Wi-Fi sources of interference that are reducing the overall RF performance for the cell.
 - **CLIENT DISTRIBUTION ON TOP NEIGHBOR APs**—Displays the top 5 neighbor AP with signal strength greater than -70 dBm on the APs current client serving channel (2.4 GHz and 5GHz). Tx power and number of clients associated to this AP and its neighbor APs are shown. Number of clients is not available for neighbor APs on different Primary AP.
 - **CLIENT DISTRIBUTION BY DATA RATES**—Each client's throughput varies depending on the data rate it is using (802.11 a/b/n/ac) at any given point in time, and this data rate may vary every second. Various factors such as RSSI values, RF interference, etc. may affect a client device's instantaneous data rate.
- **SPECTRUM INTELLIGENCE**



Note By default Spectrum Intelligence (SI) is disabled in order to reduce the CPU cycles and increase the performance.

You can enable the SI for the radio using the following instructions:

Ensure that you enable the **Interferer detection** globally under **Advanced > RF Optimization**(in Expert View).

Navigate to **Wireless Settings > Access Points** and select an AP. Click **Edit** and choose either 2.4GHz or 5GHz radio.

- **ACTIVE INTERFERERS**—Displays the Active Interferers for Access point for the selected radio. For further details of the table refer Viewing Details of Interferers under Viewing Interferers.
- **NON WI-FI CHANNEL UTILIZATION**—Displays the Non Wi-fi Channel Utilization for the Access point of the selected radio.
- **INTERFERENCE POWER**—Shows the Interference Power for the Access point on the selected radio.

• TOOLS

This section in the UI consists of options to configure the LED states of the access points and also provides details of the image in the description table:

- **AP LED DISABLE**—To configure LED, refer to the [LED Display Settings, on page 130](#).
- **BLINK AP LED**— The Blink AP LED function causes the LED to blink Red/Amber/Green for 60 seconds. This is used to identify the AP. To configure LED, refer to the [LED Display Settings, on page 130](#).
- **RESTART AP**—You can reload AP if needed. The AP which acts as a Primary AP does not have this option.
- **INTERCHANGE IMAGE**—You can swap the primary version and backup version of the image. This will take effect only after the AP reloads.
- **FACTORY DEFAULT**—You can reset the AP to factory default settings if required. The AP which acts as a Primary AP does not have this option. To reset Primary AP to factory defaults refer to [Clearing the Primary AP Configuration and Resetting to Factory Defaults, on page 116](#).
- **EXPORT CONFIG**—You can download the running configuration of the AP to .TXT file format. The configuration file is saved on the device in which the Primary AP UI is being viewed. By default the file is saved as AP<macaddress>_config.txt in your downloads folder. This option is available for the Primary AP and all the APs associated with the Primary AP.

The following mandatory configurations of an AP are exported, using which the AP can be restored even after a factory reset.

- **Information in AP Config File**

Table 4:

File Contents	Parameters
AP General Details	APModel, APLocation, APMODE, APRole, IPConfigMode (either DHCP or static), IsBridgeAP, NextPrimaryAP, IsPreferredPrimary
Radio Details	AdminStatus, ChannelWidth, Channel, TransmitPower, InterfererDetection
Mesh Mode detail	MeshRole (RAP or MAP), MeshBackhaulSlot, InstallMapping, BridgeType, BridgeGroupName, BackhaulInterface, StrictMatchBGN, PreferredParent, EthernetBridge, EthernetLinkStatus
Ethernet bridging VLANs	Name, Status, VlanTagging, NativeVlanId

Following is a sample of an AP Config file:

```

APModel: CBW240AC-H
APLocation: default location
APMode: 7
APRole: Root
IPConfigMode: 0
IsBridgeAP: 1
NextPrimaryAP: 00:00:00:00:00:00
IsPreferredPrimary 0
RogueDetectionStatus: 0
Radio0_AdminStatus: 1
Radio0_ChannelWidth: 20 MHz
Radio0_Channel: Automatic
Radio0_TransmitPower: Automatic
Radio0_InterfererDetection: 0
Radio1_AdminStatus: 1
Radio1_ChannelWidth: 80 MHz
Radio1_Channel: Automatic
Radio1_TransmitPower: Automatic
Radio1_InterfererDetection: 0
MeshRole: 1
MeshBackhaulSlot: 1
InstallMapping: 1
BridgeType: Indoor
BridgeGroupName: 00sasi
BackhaulInterface: 802.11a/n/ac
StrictMatchBGN: 0
EthernetBridge: 1
EthernetLinkStatus: UpDn
MeshInterfacel_Name: GigabitEthernet1
MeshInterfacel_Status: 0
MeshInterfacel_VlanTagging 1
MeshInterfacel_NativeVlanId 0

```

- **IMPORT CONFIG**—Using this option, you can upload the configuration file (in .TXT file format) of the AP. The configuration should match the AP model. This option is available for the Primary AP and all the APs associated with the Primary AP.

You can also track the status of the configuration file uploaded in the [TOOLS](#) section.



- Note**
1. Non Mesh Configuration file should not be imported to Mesh deployment APs.
 2. After uploading the configurations to the AP, it normally takes 1-2 minutes to take effect. You can also see the LED of the AP change from Solid/Blinking Green to Blinking Amber while applying the configurations and back to Blinking Green once the upload is complete.



Note The above **Export/Import Config** options added in the **Access Points** page is specific to a particular AP. If you want to change the configuration for the entire CBW network, refer to [Export and Import Primary AP Configuration, on page 117](#).

• Description Table Details

Description Item	Status Meaning
Primary AP Primary Image	The default active image version of the Primary AP.
Primary AP Backup Image	The backup image version of the Primary AP.
AP Primary Image	The active image version of the access point.
AP Backup image	The backup image version of the access point.
Predownload status	If the access point is going for an software update the corresponding predownload status is displayed.
Predownloaded version	Version of the predownloaded image during software upgrade process.

• PACKET CAPTURE

Using this option, you can capture the packets in the specified interface and for the specified protocol. Packet capture is supported on Wired Interfaces as well as the internal Primary AP interface responsible for communication between management functions and access points. Supported protocols are IP, TCP, and UDP. This option is available only in **Expert View**.

The following are the configurations required for starting the capture,

- **INTERFACE** – Choose whether the capture should be taken in Wired interface or Primary AP interface



Note Primary AP interface is available only for the AP acting as Primary AP.

- **WIRED INTERFACE** – Select the required Ethernet port. Based on the AP model, supported wired interfaces will be populated automatically.

CBW Model	No. of Ethernet Ports
CBW140AC	1
CBW240AC	2
CBW145AC	4
CBW141ACM	4
CBW142ACM	0
CBW143ACM	1

- **PROTOCOL** – Select the required protocol for starting the capture. Supported protocols are IP, UDP, and TCP.
- **START/STOP** – Button to Start/Stop the capture for the configured Interface and protocol.
- **DOWNLOAD** – Once the capture is stopped, the pcap file will be ready for download. By clicking on the Download button, the PCAP file will be saved to the local machine. By default, the PCAP file is saved as *AP<macaddress>_capture.pcap*.
You can also view the status of capture on top of the pane.



Note

- CBW142ACM does not support packet capture feature as it does not have Ethernet ports
 - The “Primary AP” capture will be visible only for AP which is currently acting as the Primary AP
 - The Wired0 interface of CBW141ACM is mapped to LAN4 Port
-

• Limitations:

- The maximum allowed pcap size is 5MB, after which the ongoing capture automatically stops and the pcap file can be downloaded locally by clicking on the Download button.
- Only one capture is allowed to run in single point of time. If the user is attempting to start the capture in one AP while the capture is in progress on other AP, a warning message will be displayed in CBW UI.

• SYSLOG

Using this option, you can collect per AP logs by configuring the Syslog server IP, and logging level for individual APs.

- **SYSLOG SERVER IP** – IP Address of the Syslog Server running in the network.
- **LOG SYSLOG LEVEL** – Sets the Logging level up to which the logs would be sent to the Syslog Server. By default, the log syslog level is set to **Notifications (5)**.

The available logging levels:

- **Emergencies (0)**
- **Alerts (1)**
- **Critical (2)**
- **Errors (3)**
- **Warnings (4)**
- **Notifications (5) (Default)**
- **Informational (6)**
- **Debugging (7)**

Messages with a severity equal to or less than the set level are sent to the syslog server.

- **LOGGING** – Option to Enable/disable the Logging for individual AP. By default, the logging is **Disabled**. If the logging is enabled, the syslog messages will be sent to the configured Syslog server else the messages will not be sent to the Syslog Server.



Note

- This configuration is available for all APs (Mesh Extenders, Primary AP, Primary Capable APs).
 - Syslog Server IP configured for each AP can be same/different.
 - By default, Syslog Server IP would be configured as broadcast (255.255.255.255). The Level will be set to Notifications.
 - To capture the Primary AP logs:
 - Configure the Syslog Server details under **Advanced > Logging > Add Syslog Server**.
 - Set the Logging level under **Advanced > Logging > Log Syslog Level**.
-

Viewing Client Details

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

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

Note You can also view this page by navigating via **Monitoring>Network SummaryClients**.

Step 2 In the **Active Clients** summary section, click the count display icon to view high-level details of the client device or navigate to **Monitoring>Network SummaryClients**. This section will give you an overview of the connected clients and its parameters as explained below:

In the **Clients** page, there are three upper blocks that list the following details:

- **Clients**—This tile displays the total number of clients connected.
- **Wireless**—This tile displays the number of clients specific to 2.4 GHz and 5 GHz radio.
- **Apple**—This tile is specific to the Apple Clients. Specifies the number of clients.
 - **Fastlane**—This tile displays the number of fastlane using clients. Fastlane allows iOS apps connected to CBW access points to be prioritized. This means your voice, video and real-time data gets to be first in line. To enable Fastlane go to **Wireless Settings>WLANs>Add/edit WLAN>Traffic Shaping>Fastlane**.
 - **Analytics**—This tile displays the number of Analytics capable clients.

Click on the required client from the list in the table displayed to view the per client details. The following details are displayed:

Client Details Table

You can click the downward arrow on the top right of the column headers to customize the details displayed in the table. You may choose to hide, show or rearrange the desired columns, sort them in the order you wish or filter the table contents based on the desired parameters.

- **User Name**—The user name of the client connected to the Primary AP (Default: Unknown).
- **IPv4 Address**— The IPv4 address is a 32-bit number that uniquely identifies the client device.
- **AP Name**—The configured AP name to which the client associated will be displayed in this column.
- **Protocol**—The WiFi standard through which the client is connected. It can be 802.11a/b/g/n/ac.
- **Hostname**—The MAC address of the client is displayed by default. Enable **Wireless Settings>Add/Edit WLAN>Local Profiling** to view the hostname of the clients supported.
- **Client Type**—The Capable Client's operating systems will be displayed in this column as Android, Apple-Device etc.
- **Connection Speed**—The maximum data rate strength of the client connected to the access point. The values are displayed in units of Mbps.
- **Status**—The active status of the client.
- **Signal Quality**—Signal quality is a value ranging from 0 to 100 dB. This includes, the noise generated by interference sources and the signal strength.
- **Signal Strength**—Signal strength is the wireless signal power level received by the wireless client. 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.
- **Usage**—The amount of data consumed by the client.
- **WLAN SSID**—Shows to which SSID the client has connected.
- **Uptime**—The duration of how long the client is connected to the access point.
- **Mac Address**—The MAC(Hardware) address of the client connected.
- **Frequency Bandwidth**—The radio on which the client is connected 2.4 GHz or 5 GHz.
- **WLAN Profile**—The profile name of the configured WLAN to which the client is connected.

- AP MAC—Radio MAC address of the corresponding access point to which the client is connected.
- AP Group—This column shows the access points groups to which it is configured.
- IPv6 Address—This is the IPv6 address of the client device.

Client View

Select a required client from the list displayed to view the following details:

• GENERAL

- User Name—The user name of the client connected to the Primary AP (Default: Unknown).
 - Hostname—The MAC address of the client is displayed by default. Enable **Wireless Settings > Add/Edit WLAN > Local Profiling** to view the hostname of the clients supported.
 - MAC Address—The MAC(Hardware) address of the client connected.
 - Deauthenticate—Click this option to disconnect the client.

Note Deauthenticating the client removes a client from the WLAN, but that client will be able to rejoin unless their MAC address is added to the Blocklist.

To block the client permanently, navigate to **Wireless Settings > WLAN Users > Local MAC Addresses**, click **Add MAC address**, select **Blocklist** as the type and hit **Apply & Save**.
 - Uptime—The duration of how long the client is connected to the access point.
 - SSID—Shows to which SSID the client has connected.
 - AP Name—The configured AP name to which the client is associated. The AP name along with the location can be configured by navigating to **Wireless Settings > Access Points**.
 - Nearest APs—List of AP names nearer to the client based on signal strength.
 - Device Type—The Capable Client's operating systems will be displayed in this column as Android, Apple-Device etc,
 - Performance—This shows the Signal Strength, Signal Quality, Connection Speed, Channel Width.
 - Capabilities—This gives information on which domain the client is associated to the AP and its Spatial Stream.
 - Cisco Compatible—Cisco Compatible state changes only when a Cisco client (which supports CCX extensions of the IEEE standards) get associated to your access point.
 - Client connection score—Connection score is the percentage based connection quality between client and the access point. It denotes the current client data transfer speed. Higher the percentage, the faster and higher the data transferred. This value is based on the Client Actual Rate divided by either the Client Max Capability or Max AP Configured (whichever is lower).
- CONNECTIVITY GRAPHIC—This line graph represents the stages and current status of the associated client as Start, Association, Authentication, DHCP, and Online.
 - TOP APPLICATIONS—The top applications that are being used by the client device is presented in a graphical or tabular format. To utilize this, the user must enable AVC in **Wireless Settings > WLANs > Add/Edit WLAN > Traffic Shaping > Application Visibility Control**.

Note Ensure that the Application Visibility Control (AVC) is active under WLAN settings to view this data.

- **MOBILITY STATE**—This shows the graphical flowchart of stages on how the client is connected to the Primary AP.
 - Name of the Primary AP, with its IP address and the model number of the AP on which it is running.
 - Name of the AP with which the client is connected to the Primary AP, the AP's IP address, and the AP's model number.
 - Nature of connection between the AP and the client. For example, wireless 802.11n 5 GHz connection.
 - Name of the client, type of client (such as Microsoft Workstation), VLAN ID of the client, and the client's IP address.
- **NETWORK & QOS** —This shows client capability of some IEEE standards and user configured parameters such as IP address, VLAN, Source Group Tag, Fastlan Client, Mobility Role, WMM, U-APSD and QoS Level.
- **SECURITY & POLICY**—This table shows the encryption type and security policies on which the client is associated to the access point such as Policy (WPA2 or WPA3), Cipher, Key Management, EAP Type, ACL, mDNS, and AAA Role.

Viewing Guest Client Details

The clients that are connected to the **Guest WLANs** are known as **Guest Clients**. To obtain Guest WLANs the Primary AP provides guest user access on WLANs which are specifically designated for use by guest users. The concept of creating Guest WLANs is discussed in the later chapters.

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

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

Step 2 In the **Guest Client** page, the summary blocks display the number of guest clients and recently connected clients to the Primary AP. Each guest client detail can be viewed by clicking the specific client record.

In the **Guest Clients** page, there are two upper blocks that list the following details:

- **Guest Clients / Recent Clients**—Specifies the total number of guest clients and recent clients connected.
- **Wireless**—Specifies the number of 802.11b/g/n guest clients connected and operating either at 2.4 GHz or 5 GHz.

Click on the required guest client from the list in the table displayed to view the per guest client details. For a description of the parameters displayed for a specific guest client, refer to [Viewing Client Details](#):

Step 3 You can click the downward arrow on the top right of the column headers to customize the details displayed in the table. You may choose to hide, show or rearrange the desired columns, sort them in the order you wish or filter the table contents based on the desired parameters.

- Note** The clients connected to Guest WLANs are considered to be Guest Clients.
- You can export details of all the guest clients connected to the CBW network and download in Excel format using the **save** icon in the **Guest Widget**.
-

Troubleshooting a Client

This section describes in detail how to perform a client ping test and a connection test. These help to effectively investigate and troubleshoot connection issues.

To troubleshoot wireless client joining issues, set the **Logging level** as **Notifications (5)** and check the logs in the Primary AP UI under **Management > Logging**.

Performing a Client Ping Test

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

Click **Start** to begin the test. The latency in milliseconds is represented graphically.

Performing a Connection Test

You may choose to perform a Connection test when the client fails to connect to a particular WLAN. This test takes about three minutes. Attempting to connect during the three minute test period will generate diagnostic information to aid in troubleshooting connection issues.

-
- Step 1** Go to **Monitoring > Network Summary > Clients**.
 - Step 2** Click on the client MAC address that you want to debug from the list of clients that are available.
 - Step 3** Scroll down to the **Client Test** and in the **Connection** tab click **Start**.
 - Step 4** Now disconnect the client from the WLAN and try re-connecting.
 - Step 5** The result at each stage of client connection establishment with the WLAN is displayed.
-

Generating an Event Log

The user may choose to perform a complete debug session by enabling the **Event Log** feature that is available in the per client view tab. The Event Log testing contains the time-stamp and message details that are exchanged between the client and the access point. The message type helps to analyze and conclude if a client is able to successfully join a WLAN or a reason for its failure in joining a particular WLAN.

-
- Step 1** Go to **Monitoring > Network Summary > Clients**.
 - Step 2** Click on the client MAC that you want to debug.

Step 3 Scroll down to the **Client Test** and in the **Event Log** tab, click on the **Start** option.

Step 4 Now, disconnect the client from the WLAN and try to re-connect it again.

Step 5 You can also save the results, by selecting the **Save to Disk** option in the Primary AP UI. Following is a sample output displayed when you generate an event log:

The screenshot shows the 'EVENT LOG' tab in a monitoring interface. At the top, there are buttons for 'Start', 'Stop', and 'Save To Disk'. Below is a table with columns: Time Stamp, Module, Severity, Message Type, Message Subtype, and Details. The table contains 18 rows of log entries.

Time Stamp	Module	Severity	Message Type	Message Subtype	Details
Mon Dec 09 201...	Dot11	INFO	ASSOC_REQ	MESSAGE_RECEIVED	None
Mon Dec 09 201...	Dot11	INFO	ASSOC_REQ	INVALID_RSN_IE	None
Mon Dec 09 201...	PEM	INFO	PEM_EVENT_MSG	WLAN_SUPPORTS_STATIC_DYNAMIC_W...	None
Mon Dec 09 201...	PEM	INFO	PEM_EVENT_MSG	IP_ACQUIRED_AND_AUTH_NOT_REG_O...	None
Mon Dec 09 201...	Dot11	INFO	ASSOC_REQ	CLIENT_MOVED_TO_ASSOCIATED_STATE	None
Mon Dec 09 201...	Dot11	ERROR	AUTH_DOT1X	WLAN_REQUIRES_802_1X_AUTH	None
Mon Dec 09 201...	PEM	INFO	PEM_EVENT_MSG	WEB_AUTH_MAX_RETRY_EXCEEDED	None
Mon Dec 09 201...	PEM	INFO	PEM_EVENT_MSG	WEB_AUTH_SUCCESS	None
Mon Dec 09 201...	Dot11	INFO	ASSOC_REQ	MESSAGE_RECEIVED	None
Mon Dec 09 201...	Dot11	INFO	ASSOC_REQ	INVALID_RSN_IE	None
Mon Dec 09 201...	PEM	INFO	PEM_EVENT_MSG	WLAN_SUPPORTS_STATIC_DYNAMIC_W...	None
Mon Dec 09 201...	PEM	INFO	PEM_EVENT_MSG	IP_ACQUIRED_AND_AUTH_NOT_REG_O...	None
Mon Dec 09 201...	Dot11	INFO	ASSOC_REQ	CLIENT_MOVED_TO_ASSOCIATED_STATE	None
Mon Dec 09 201...	Dot11	ERROR	AUTH_DOT1X	WLAN_REQUIRES_802_1X_AUTH	None
Mon Dec 09 201...	PEM	INFO	PEM_EVENT_MSG	WEB_AUTH_MAX_RETRY_EXCEEDED	None

Viewing Mesh Extender

Step 1 Navigate to **Monitoring > Network Summary > Mesh Extender**.

Step 2 In the **Mesh Extender** page, you can view the following details of the Mesh Extenders:

- **AP name**—Displays name of the Mesh Extender.
- **AP Model**—Displays the model of Mesh Extender.
- **Ethernet MAC**—Displays the Hardware MAC of the Mesh Extender.
- **Parent AP Name**—Displays the AP name to which the Mesh Extender has joined wirelessly.
- **Hop**—Displays the count of how far the Mesh Extender is operating from the Primary AP.
- **Link SNR (dBm)**— It's the signal to noise ratio calculated between the Mesh Extender and the Parent AP (to which the Mesh has joined).
- **Channel Utilization (%)**—Level of traffic including data and interference over the channel that is assigned on the AP. The values are represented in % format.
- **Channel**—Channel number at which the Mesh Extender's radio is operating.
- **Clients**—Total number of clients connected to this Mesh Extender.

Note Only devices operating in Mesh Extender Mode are displayed in the table.

Viewing Applications

Click the **Applications** menu to view the Top 10 application usage in the client traffic. This can be seen when you enable the Application Visibility Control (AVC) option in at least one WLAN. Navigate to **Wireless Settings > WLANs > Add/Edit WLAN > Traffic Shaping > Application visibility Control** to view.

Viewing Rogue Access Points

Any device that shares your channel and is not managed by you can be considered as a **Rogue**. This includes Rogue Access Points, Wireless Routers and Rogue clients. CBW APs have the in-built intelligence to detect rogue devices in both 2.4GHz and 5GHz radios.

The Rogue AP and Rogue Client Detection is **Disabled** on CBW APs by default. To enable Rogue Client Detection:

1. Navigate to **Wireless Settings > Access Points**.
2. Click the edit icon next to the AP you want change.
3. Click the **Rogue Detection** toggle button in the **General** tab.
4. Click **Apply** to save and exit.

After applying the changes, the Rogue detection will be enabled, and the Rogue APs will be reported to Primary AP.

You can view the following details of rogue devices which includes unmanaged neighboring Clients and Access Points.

- **MAC Address**—Rogue AP MAC address.
- **SSID**—The name of the SSID, which the Rogue AP is broadcasting.
- **Channels**—The channel in which the Rogue AP is operating.
- **Detecting AP Counts**—Displays the number of APs in which the Rogue AP is detected.
- **Clients**—Number of clients connected to the Rogue AP.
- **Class**—The class of the Rogue AP. By default, all the Rogue APs are unclassified. You can change the class of Rogue APs as **Friendly**, or **Malicious**.

Following are the classes that are supported by the CBW:

Class	Description
Unclassified	The CBW AP discovers all the Rogue APs and marks them under the Unclassified class by default. Also, the status of the Rogue AP remains as Alert since it remains unknown to the CBW network.

Class	Description
Friendly	<p>You can move the Rogue AP to a Friendly state if you know the Rogue APs MAC.</p> <p>Following are the options that are configurable:</p> <ul style="list-style-type: none"> • Internal—If the unknown access point is inside the network and poses no threat to WLAN security, you would manually configure it as Friendly, Internal. Example: An access point that exists within your premises. • External—If the unknown access point is outside the network and poses no threat to WLAN security, you would manually configure it as Friendly, External. Example: An access point that belongs to a neighboring coffee shop.
Malicious	<p>You can move the Rogue AP to Malicious class when you do not know the particulars of the AP. By default, the status remains as Alert since it remains unknown to the CBW network.</p>

- **State**—Displays the state of the Rogue AP. If the Rogue AP class is **friendly**, the state will be **Internal** or **External**, else the state will be **Alert**.

Configuring the Rogue AP States

-
- Step 1** Click **Monitoring > Network Summary**
 - Step 2** In the **Rogues** tab, click on the **Access Points**.
 - Step 3** Click on one of the available Rogue APs that is detected by the CBW.
 - Step 4** In the **Update class** drop-down list box, select the appropriate class.
 - Step 5** Select the class as **Friendly** to configure the status as **Internal** or **External**.
 - Step 6** If you specify the AP as **Malicious** class, then the status of the AP remains as **Alert**.
 - Step 7** You can also move an AP from one state (such as **Friendly**) to another (such as **Malicious**) by selecting the AP from the specific tabs.
 - Step 8** Click **Apply** to save the changes.
-

Viewing Rogue Client Details

-
- Step 1** Navigate to **Monitoring > Rogues > Clients** in **Expert View**.
 - Step 2** Clients that are associated to Rogue APs are displayed along with the following details:
 - **MAC address**—Rogue client's MAC address.
 - **AP MAC**—MAC address of the AP to which the Rogue client is connected.

- **SSID**—Displays to which SSID the client is connected.
 - **Detecting AP Counts**—Displays the number of APs in which the Rogue Client is detected.
 - **Last Seen**—Shows the time at which the Rogue client is detected.
 - **State**—Displays the state of the Rogue client.
 - **Wired**—Specifies if the detected Rogue client is Wired or Wireless.
-

Viewing Interferer Details

Interferers are non-Wi-Fi devices that cause disruption to your Wireless network. They may either be operating at 2.4 GHz or at 5 GHz. To view these devices, do the following:

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

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

Step 2 In the **Interferers** summary window, click the count display icon. The following details are displayed.

- **AP Name**—The name of the access point where the interference device is detected.
 - **Radio Slot**—Slot where the radio is installed.
 - **Interferer Type**—Type of the interferers such as Microwave Oven, Jammer, WiMax Mobile, and so on
 - **Affected Channel**—Channel that the device affects.
 - **Detected Time**—Time at which the interference was detected.
 - **Severity**—Severity index of the interfering device.
 - **Duty Cycle (%)**—Proportion of time during which the interfering device was active.
 - **RSSI**—Receive signal strength indicator (RSSI) of the access point.
 - **Dev ID**—Device identification number that uniquely identified the interfering device.
 - **Cluster ID**—Cluster identification number that is unique which identifies the type of the device.
-

Wireless Dashboard

This page displays the capabilities of AP and the Client for 2.4 GHz and 5 GHz. You can click the **Close Widget (X)** icon on the top right of the following widgets that you want to remove. You may add the closed widget again by clicking the + icon if you wish.

AP CAPABILITY

Displays the capability details for the APs managed by the Primary AP:

- **Max Configured Connection Rates:** Displays the graph and table for maximum configured connection rate in Mbps, mapped to different ranges, for each of the radios (2.4 GHz and 5GHz) for all the APs configured by the Primary AP.
- **AP Distribution by Channel Width:** Displays the graph and table for the maximum configured Channel Width for all the APs configured by the Primary AP.

CLIENT CAPABILITY

Displays the capability data for the clients managed by the Primary AP:

- **Client Capability by Spatial Stream:** Displays the graph and table for the number of clients capable of a particular spatial stream for all the clients connected to the Primary AP.
- **Client Capability by Max Protocol:** Displays the graph and table for the number of client based on the maximum data rate protocol supported for all the clients connected to the Primary AP.

AP PERFORMANCE-CHANNEL UTILISATION

Display the Performance details for the APs managed by the Primary AP:

- **Channel Utilization :** Displays the graph and table for the channel utilization as a percentage, mapped to different ranges, for each of the radios(2.4 GHz and 5GHz) for all the APs configured by the Primary AP.

CLIENT PERFORMANCE

Displays the connected characteristic for the clients managed by the Primary AP:

- **Client by Connection Score:** Displays the connection score percentages ranges for all the clients connected to the Primary AP. The Connection Score is calculated as a percentage value based on the Client Actual Rate divided by either Client Max Capability or Max AP Configured (whichever is lower). This ensures the Connection Score is always calculated based on the maximum possible rate based on each devices maximum rate capability.
- **Client by Connected Protocol:** Displays the graph and table for the number of client based on the connected protocol for all the clients connected to the Primary AP.

AP DISTRIBUTION

Displays the distribution of APs managed by the Primary AP:

- **AP distribution by Model:** Displays the graph and table for all APs configured by the Primary AP. Based on the Model name of the AP to the radios (2.4 GHz and 5GHz) the graph and table gets updated.
- **AP distribution by SpatialStream:** Displays the graph and table for all APs configured by Primary AP. Based on the SpatialStream to which it is connected for each of the radios (2.4 GHz and 5GHz) the graph and table get updated. The centre of the donut displays the maximum number of APs with the particular SpatialStream.

Customizing the Access Point Performance View

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

Table 5: Wireless Dashboard - AP Performance

Widgets	Description
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. Click to view the AP detail.
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. Click to view the AP detail.
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. Click to view the AP detail.
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.
AP Join Failure Status	This widget shows the number of APs that failed to join the Primary AP and the associated error types during a specific day, week or month. Click a specific join error to see the APs that have failed to join the Primary AP with the associated error type. Click the setting to clear the AP Join statistics.

You can view the above statistics in both 2.4GHz and 5 GHz type of radios by clicking on them respectively.

Adding Widgets

-
- Step 1** Choose **Monitoring > Wireless Dashboard > AP Performance**.
- Step 2** Click the + (plus) icon on the top right of the AP Performance window.
- Step 3** Select the widgets you want to add from the following:
- **Channel Utilization**—Top APs
 - **Interference**—Top APs
 - **Client Load**—Top APs
 - **Coverage**—Bottom APs

- **AP Join Failure Status**—Bottom APs

- Note**
- Top APs—AP with the maximum client load.
 - Bottom APs—AP with low SNR values for the client.

Step 4 Click **Close**. The **AP Performance** window is refreshed with the new widgets.

Removing Widgets

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

Step 2 Click the **Close Widget (X)** icon on the top right of the widgets that you want to remove. You may add the closed widget again by clicking the + icon if you wish.

Customizing the Client Performance View

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

Table 6: Client Performance

Numbers & Labels	Description
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 quality is a value ranging from 0 to 100 dB. This includes the noise generated by interference sources and the signal strength.
Client Connections	Displays clients associated with the access points of any connectivity types.

Adding a Widget

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

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

Step 3 Select the widgets you want to add from the following:

- **Signal Strength**

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

Step 4 Click **Close**. The **Client Performance** window is refreshed with the new widgets.

Removing a Widget

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

Step 2 Click the **Close Widget(X)** icon on the top right of the widgets and select the ones you want to remove. You may add the closed widget again by clicking the + icon if you wish.



CHAPTER 5

Wireless Settings

This chapter contains the following sections:

- [About WLANs and RLANs in CBW Access Point Network, on page 43](#)
- [Setting Up WLANs RLANs and WLAN Users, on page 43](#)
- [Managing Associated Access Points, on page 61](#)
- [Setting a Login Page for WLAN Guest Users, on page 66](#)
- [About Cisco Mesh, on page 69](#)

About WLANs and RLANs in CBW Access Point Network

Wireless LAN (WLAN) is a network that allows devices to connect and communicate on wireless mode. Remote-LAN (RLAN) is similar to a WLAN. The only difference being that a WLAN is used for wireless connection, and a Remote-LAN is used for wired connection.

On connecting a wired client to the CBW240AC/CBW145AC ports in a non-mesh deployment, the client will be able to access the internet.



Note RLAN is not supported in Mesh deployments. To support wired devices in Mesh deployment, refer to [List item](#).

In a non-mesh deployment, when the Primary AP boots up, the **Default_RLAN** is automatically created.

You may also refer [LAN port functionality for different models, on page 127](#) to understand the LAN port functionality supported for different AP models.

You can create and manage Wireless Local Area Networks (WLANs) and Remote LANs (RLANs) using the **WLANs** screen. This is discussed in the following sections.

Setting Up WLANs RLANs and WLAN Users

Choose **Wireless Settings > WLANs**.

The total number of active WLANs and RLANs (in non-mesh deployments) is displayed at the top of the **WLANs/RLANs** window which includes a list of WLANs currently configured on the Primary AP. The following details are displayed for each WLAN/RLAN:

- Status of the WLAN. It can be enabled or disabled
- Displays if it is a WLAN or RLAN.
- Name of the WLAN
- Security Policy on WLAN
- Radio Policy on WLAN

Guidelines and Limitations for Setting Up WLANs

- You can associate up to 16 WLANs/RLANs (inclusive of DEFAULT_RLAN in non-mesh deployments) with the CBW Primary AP and create a total of 16 WLANs/RLANs. Cisco recommends a maximum of 4 WLANs. The Primary AP assigns all the configured WLANs to all the connected APs.
- Each WLAN has a unique WLAN ID, a unique profile name, and an SSID.
- The Profile name and SSID can have up to 31 characters.
- Each connected AP advertises only the WLANs that are in an **Enabled** state. The APs do not broadcast disabled WLANs.
- Peer-to-peer blocking does not apply to multicast traffic.
- You cannot map a WLAN to VLAN0, and you cannot map VLANs 1002 to 1006.
- Dual-stack clients with static IPv4 addresses are not supported.
- Profile name and security type must be unique for each WLAN.

Viewing WLANs

The **WLANs** window lists all the WLANs/RLANs that are currently configured on the Primary AP, along with the following details for each WLAN/RLAN:

- **Action**—Provides option to **Edit** or **Delete** the WLAN.
- **Active**—Status of the WLAN. It can be enabled or disabled.
- **Type**—Displays the type as WLAN or RLAN
- **Name**—Profile Name of the WLAN. Several WLANs can be configured with the same SSID name but with unique policy name and security mechanisms.
- **SSID**—SSID name of the WLAN.
- **Security Policy**—Denotes the Security Type of the WLAN. It can be an Open network, WPA2 Personal, WPA2+WPA3(Personal), WPA3 Personal, WPA2 Enterprise, Central Web Auth (CWA) or guest network.
- **MAC filtering**—This option is displayed when you configure a Security Type with MAC Filtering enabled in the previous field. For example, when you configure a Open WLAN with the MAC Filtering enabled, then it displays Open+Macfilter.
- **Radio Policy**—Displays the Radio in which the WLAN is broadcasting. By default, it is **All**.



Note See [About WLANs and RLANs in CBW Access Point Network, on page 43](#) section for a brief explanation on WLANs.



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

To view details of configured WLANs, go to **Wireless Settings > WLANs**.

Adding and Modifying a WLAN

To add a WLAN, do the following:

1. Choose **Wireless Settings > WLANs**.
2. In the **WLANs** window, click **Add new WLAN/RLAN**. The **Add new WLAN/RLAN** window is displayed.

To edit a WLAN/RLAN, do the following:

Click the **Edit** icon adjacent to the WLAN/RLAN you want to modify.



Note Editing the WLAN/RLAN will disrupt the network momentarily.

For example, to change the Security Type for a WLAN that has been created, do the following:

- a. Click the **Edit** icon.
- b. Click **Yes** in the pop-up message.
- c. Go to **WLAN security** tab and select the required security type from the drop down-list.
- d. Click **Apply** to save the configurations or **Cancel** to discard the changes.

Each of the tabs in this window is explained in the following sections.

To delete a WLAN/RLAN, click the **Delete** icon adjacent to the WLAN/RLAN you want to delete and follow the instructions.

Configuring General Details

Navigate to **Wireless Settings > WLANs > Add new WLAN/RLAN > General**.

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

1. **WLAN ID**—From the drop-down list, choose an ID number for the WLAN.
2. **Type**—Indicates if the type of network is WLAN or RLAN. Choose WLAN option.
3. **Profile Name**— The profile name must be unique and should not exceed 31 characters.

4. **SSID**—The profile name also acts as the SSID. You can choose to specify an SSID that is different from the WLAN profile name. The SSID must be unique and should not exceed 31 characters.
5. **Enable**—Click this tab to enable/disable the WLAN.
6. **Radio Policy**—Click the drop-down list and choose from the following options:
 - a. **All**—Configures the WLAN to support dual-band (2.4 GHz and 5 GHz) capable clients
 - b. **2.4 GHz only**—Configures the WLAN to support 802.11b/g/n capable clients only
 - c. **5 GHz only**—Configures the WLAN to support 802.11a/n/ac capable clients only
7. **Broadcast SSID**—The default is **Enabled** for the SSID to be discovered. Use the toggle button to hide the SSID.
8. **Local Profiling**—By default, this option is **disabled**. Enable this option to view the Operating System that is running on the Client or to see the User name.

Configuring WLAN Security

Navigate to **Wireless Settings > WLANs > Add new WLAN/RLAN > WLAN Security**.

Under the **WLAN Security** tab, set the following parameters.

- **Guest Network**—Guest user access can be provided on WLANs which are specifically designated for use by guest users. If the Guest Network is enabled, then the WLAN is considered as Guest WLAN. By default, this field is disabled.

The following fields are displayed when you **Enable** the **Guest Network** option. These are applicable for WLANs and Guest WLANs.

For details on creating a Guest Network, refer to [Creating a Guest Network, on page 132](#).

- **Captive Network Assistant**—This feature detects the presence of a captive portal by sending a web request on connecting to a wireless network. This request is directed to a URL for iPhone models and if a response is received, then the internet access is assumed available and no further interaction is required. If no response is received, then the Internet access is assumed to be blocked by the captive portal and Apple's Captive Network Assistant (CNA) auto-launches the pseudo-browser to request portal login in a controlled window.
- **MAC Filtering**— You can also restrict or permit a particular client joining your network by enabling the MAC Filtering feature. For details, refer to [Blocking and Unblocking Clients, on page 58](#).



Note When MAC Filtering is enabled on the WLAN, the client MAC address must be added to the Local MAC Addresses list by navigating to **Wireless Settings > WLAN Users > Local MAC Addresses** with the **Type** as **Allowlist** for enabling the client to join the network via that SSID.

- **Captive Portal**—This field is visible only when the **Guest Network** option is enabled. This is used to specify the type of web portal that can be used for authentication purposes. Following are the types of web portals that you can choose.
 - **Internal Splash Page**—Choose this option to have a default Cisco web portal based authentication.

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



Note Ensure to add this URL rule in the configuring ACL name under **Advanced > Security Settings** page.

- **Access Type**—This field is visible only when the **Guest Network** option is enabled.
 - **Local User Account**—This is the default option. Choose this option to authenticate guests using the username and password which you can specify for guest users of this WLAN, under **Wireless Settings > WLAN Users**. For more information, see [Viewing and Managing WLAN Users, on page 57](#)
 - **Web Consent**—Choose this option to allow guests access to the WLAN upon acceptance of displayed terms and conditions. This option allows guest users to access the WLAN without entering a username and password.
 - **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, the access to the internet is provided. This option allows guest users to access the WLAN without entering a username and password.



Note You can also collect the email address information by configuring **Accounting Radius Server** under **Management > Admin Accounts > Radius** in **Expert View**. By default, the email address will be sent to the first Radius server configured.

- **RADIUS**—Refer to details on RADIUS in the [Security Type-WPA2 Enterprise](#) section.
- **WPA2 Personal**—Refer to [Security Type Personal, on page 49](#) in the following section.
- **Social Login**—Choose this option to allow guest access to WLAN upon authentication by Google/Facebook using their personal credentials. Once the user connects to this guest WLAN they will be redirected to the default login page where they can find the login buttons for Google or Facebook, or both depending on which toggle buttons are enabled. Log in using the respective account, and get the specific Internet access.

If **Social Login** Access type is selected, the two toggle options will be displayed:

- **Facebook** —Turn on this option when you want to allow a guest user access only using Facebook accounts.
- **Google**—Turn on this option when you want to allow a guest user access only using Google accounts.

By default both toggles are enabled, so guest users can use Facebook or Google accounts for authentication.



Note Apple devices will not be able to sign-in via Google, if **Captive Network Assistant** (CNA) is enabled with **Social Login** as **Access Type**. You will need to disable CNA and sign-in via Google for Guest access.

- **ACL Name(IPv4)**—This field is visible only when the **Guest Network** option is enabled.



Note For a detailed explanation on this feature refer to [Configuring Access Control Lists \(ACL\), on page 122](#). This description is applicable for WLAN and Guest WLAN.

Any ACL created through **Advanced > Security Settings > Add new ACL** is also displayed here.

- **None**— No ACL is applied
- **Enable Facebook Login**— The user can map to this when required to configure a Guest WLAN with Social Login as **Access type** and the Facebook toggle is enabled.
- **Enable Google Login**— The user can map to this when required to configure a Guest WLAN with Social Login as **Access type** and the Google toggle is enabled.
- **Enable Social Login**— This is a default setting. The user can map this when required to configure a Guest WLAN with Social Login as Access type.
- **ACL Name(IPv6)**—This field is visible only when the **Guest Network** option is enabled.



Note For a detailed explanation on this feature refer to [Configuring Access Control Lists \(ACL\), on page 122](#). This description is applicable for WLAN and Guest WLAN.

Any ACL created through **Advanced > Security Settings > Add new ACL** is also displayed here.

- **Security Type**—For details on this option, refer to the following section:



Note Security Type is only displayed when Guest Network option is disabled.

Each of the options available in the **Security Type** drop-down is explained in detail below:

Security Type-Open

This option stands for Open authentication, which allows any device to authenticate and then attempt to communicate with an AP. Using open authentication, any wireless device can authenticate with the AP.

Security Type Personal

- **WPA2**—This option stands for Wi-Fi Protected Access 2 with Pre-Shared Key (PSK). WPA2 Personal is a method used for securing your network with the use of a PSK authentication. The PSK is configured separately both on the Primary AP, under the WLAN security policy, and on the client. WPA2 Personal does not rely on an authentication server on your network. By default, it is **enabled**.
- **WPA3**—This option stands for Wi-Fi Protected Access 3 (WPA3), the latest version of Wi-Fi Protected Access (WPA), which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks. WPA3 leverages Simultaneous Authentication of Equals (SAE) to provide stronger protections for users against password guessing attempts by third parties. When the client connects to the Access Point, they perform an SAE exchange. If successful, they will each create a cryptographically strong key, from which the session key will be derived. Typically, a client and Access Point goes into phases of commit and then confirm. Once there is a commitment, the client and Access Point can then go into the confirm states each time there is a session key to be generated.

For advanced security, enable WPA3 in addition to WPA2. By default, the value is disabled.



Note You can also enable WPA3 individually, provided the client is WPA3 compatible.

- **Passphrase Format**—Choose **ASCII** or **HEX** (hexadecimal range) from the PSK Format drop-down list and then enter a pre-shared key in the text box. WPA pre-shared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.
- **Passphrase**—Specify the password.



Note The PSK you enter is hidden under dots for security purposes.

- **Confirm Passphrase**—Confirm the password.
- **Show Passphrase**—Check the checkbox, if you would like to display the password that was entered for verification.
- **Password Expiry**—This option helps to enable password expiry for WLANs with WPA-PSK. By default, the password expiry is **disabled**.
- **Expiry (Days)**—Set Value for expiry in days. Range: 1 - 180 days. By default, 180 days will be set as expiry value. This field is displayed when you enable the **Password Expiry** toggle switch.



Note Once the expiry value is exceeded, the WLAN will be disabled. If required, re-enable the WLAN and set the expiry value.

Security Type-WPA2 Enterprise

This option stands for Wi-Fi Protected Access 2, with a local authentication server or a RADIUS server. When you choose this option, you will see the following fields:

- **Authentication Server**—You can choose **External Radius** or **AP**. The default option is **External Radius**.

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



Note You will see note specifying whether the Radius Server is configured for Authentication and Accounting. Radius Server can be configured by navigating to **Admin Accounts > RADIUS** in Expert view.

- To have a RADIUS server-based authentication method, choose **External Radius** in the **Authentication Server** drop-down list. RADIUS is a client/server protocol that enables communication with a central server to authenticate users and authorize their access to the WLAN.
- **Radius Profiling**—The Primary AP acts as the collector of the information and sends the RADIUS server with the required data in an optimal form. Clients on the WLANS will be profiled as soon as profiling is enabled.

Profiling can be based on the following:

- Role defining the user type or the user group to which the user belongs.
 - Device type, such as Windows machine, Smart Phone, iPad, iPhone and Android.
 - Username / password.
 - Location, based on the AP group to which the client is connected.
 - Time of the day based on what time of the day the client is allowed on the network.
- **BYOD**—This is a **Bring Your Own Device (BYOD)** solution architecture, combining elements across the network for a unified approach to secure device access. It is enabled when a user wants to connect their personal devices in a more secure manner.

Security Type-Central Web Auth

It is a method of authentication in which the host's Web browser is redirected to a RADIUS server. The RADIUS server provides a web portal where the user can enter a username and password. If these credentials are validated by the RADIUS server, the user is authenticated and is allowed access to the network. When you choose this option, you will see the following fields:

Radius Profiling—Refer to [Radius Profiling](#) in the earlier section.

RADIUS Server

RADIUS is a client/server protocol that enables communication with a central server to authenticate users and authorize their access to the WLAN/RLAN. To have a RADIUS server-based authentication method, choose **External Radius** in the **Authentication Server** drop-down list.



Note This section appears in UI, when you do the following:

- Set the WLAN security to **WPA2 Enterprise with Authentication Server** and choose **External Radius**.
 - Set the WLAN security to **Central Web Auth**.
 - Set the WLAN security to **WPA2/WPA3 Personal**, and enable the **MAC filtering** toggle button.
-

The following fields are visible for the Security Types: **WPA2 Enterprise**, **Central Web Auth**, and **WPA2 Personal** with the MAC filter option turned on.

- **Radius Server**—Provided for external authentication when you connect to a WLAN.
- **Authentication Caching**—This feature helps store the client information essential for authentication locally in the cache on the CBW. This happens when the authentication with the RADIUS Server is successful. If the connectivity to the RADIUS server is lost, the information stored in the cache is used for authenticating the clients. You can also configure cache when the RADIUS Server is up and running. If the client details are not available locally, the request for authentication is sent through the RADIUS Server disabled.



Note This field is not visible for the security type **Central Web Auth**.

When you enable this option, the following fields are displayed.

- **User Cache Timeout**—Specifies the time period at which the authenticated credential in the cache expires.
If the client's cache that expires is associated to the controller, then it would get deauthenticated,



Note Any change in cache timeout value on the WLAN will affect only new client associations and the existing clients won't get impacted.

- **User Cache Reuse**—Use the credentials cache information before cache timeout. By default this is disabled.



Note Local cache client entries are deleted in the following scenarios:

- The CBW Primary AP reboots
 - The cache time expires
 - The security of the WLAN changes
 - A WLAN is deleted
 - Authentication Caching is disabled on the WLAN
-

- **Add RADIUS Authentication Server**—Click this tab to add the following RADIUS Authentication Server details:
 - **Server IP Address**—Select the IP address of the RADIUS server from the drop down list.
 - **State**—Shows the state of the RADIUS server.
 - **Port Number**—Provided for communication with the RADIUS server. By default, it is 1812.



Note To map RADIUS server to WLAN, first configure the RADIUS server details under **Management > Admin Accounts > RADIUS** in Expert View.

- **Add RADIUS Accounting Sever**—Click this tab to add the following RADIUS Accounting Server details:
 - **Server IP Address**—Select the IP address of the RADIUS server from the drop down list.
 - **State**—Displays if the accounting server is in an enabled or disabled state.
 - **Port Number**—It is used for communication with the RADIUS server. By default, the value is 1813.



Note You can only add/delete the Radius server entries.

To map RADIUS server to WLAN, first configure the RADIUS server details under **Management > Admin Accounts > RADIUS** in Expert View.

Configuring VLAN and Firewall

Navigate to **Wireless Settings > WLANs > Add new WLAN/RLAN > VLAN & Firewall**.

Specify the following parameters:

1. **Client IP Management**—To assign an IP address to the client through external DHCP server.
2. **Peer to Peer Block**—It disables communication between clients that are connected in the same WLAN. By default this is **disabled**.

For example, when you connect two clients (say A and B) on the same WLAN with Peer to Peer Blocking enabled, then the client (A) will not be able to reach client (B) and vice versa.

3. **Use VLAN Tagging**—From the drop-down list, choose **Yes** to enable VLAN tagging of packets. By default this field is set to **No**.

If you choose to enable **VLAN Tagging**, choose the VLAN ID in the **VLAN ID** field. By default, the Native VLAN ID set to **1** will be mapped.

You can configure Native VLAN ID, under **Wireless Settings > Access Points > Global AP configuration > VLAN Tagging**.

4. **Enable Firewall**—To enable a firewall for the WLAN based on Access Control Lists (ACLs), choose **Yes** from the drop-down list. By default, this field is set to **No**. To create an ACL, refer to [Configuring](#)

[Access Control Lists \(ACL\)](#), on page 122 later in this section. When you enable the **Enable Firewall** option, the following fields are displayed:

- a. In the **WLAN Post-auth ACL** section, choose **IPv4/IPv6 ACLs** in the **ACL Name(IPv4) / ACL Name(IPv6)** fields. These ACL rules are applied to the clients connected to the WLAN after successful authentication.
- b. In the **VLAN ACL** section, choose **IPv4/IPv6 ACLs** in the **ACL Name(IPv4)** and specify the **ACL Direction**. The ingress (inbound) and egress (outbound) ACL specifies the types of network traffic that are allowed in or out of the device in the network. Choose **Both** to allow ingress and egress traffic.

Configuring Traffic Shaping

Navigate to **Wireless Settings > WLANs > Add new WLAN/RLAN > Traffic Shaping**. Configure the following parameters:

- **Quality of service (QoS)**—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 CBW Primary AP supports the following four QoS levels. Under the **QoS** tab, from the **QoS** drop-down list, choose one of the following QoS levels:

- **Platinum (Voice)**—Ensures a high quality of service for voice over wireless.
 - **Gold (Video)**—Supports high-quality video applications.
 - **Silver (Best Effort)**—Supports normal bandwidth for clients.
 - **Bronze (Background)**—Provides the lowest bandwidth for guest services.
- Specify the **Rate limits per client** and **Rate limits per BSSID** (in Kbps) using the following criteria:
 - **Average downstream bandwidth limit**—Define the average data rate for downstream TCP traffic by entering the rate in Kbps in the Average Data Rate text boxes.
 - **Average real-time downstream bandwidth limit**—Define the average real-time rate for downstream UDP traffic by entering the rate in Kbps in the Average Real-Time Rate text boxes.
 - **Average upstream bandwidth limit**—Define the average data rate for upstream TCP traffic by entering the rate in Kbps in the Average Data Rate text boxes.
 - **Average real-time upstream bandwidth limit**—Define the average real-time rate for upstream UDP traffic by entering the rate in Kbps in the Average Real-Time Rate text boxes.



Note

Average Data Rate is used to measure TCP traffic while Average Real-time rate is used for UDP traffic. They are measured in kbps for all the entries. The values for Average Data Rate and Average Real-time rate can be different because they are applied to different upper layer protocols such as TCP and UDP. These different values for the rates do not impact the bandwidth.

- **Fastlane**—Wireless application traffic in real-time environments often needs to be prioritized by its type. For example, due to real time application constraints, voice over Wi-Fi traffic needs a higher priority than Safari web traffic.

Various standards exist to help network devices agree on how different types of traffic are marked to make sure they are prioritized. QoS Fastlane greatly simplifies this agreement process so that network congestion is minimized and time sensitive traffic (like voice or video) is delivered on time.

On enabling the fastlane, the QoS is set to platinum such that voice traffic has higher priority than any other traffic.

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

To enable **Application Visibility Control**, choose **Enabled** from the **Application Visibility** drop-down list. Otherwise, choose **Disabled** which is the default option.

- **AVC Profile**—Displays the WLAN name.
- **Add Rule**—To allow/deny specific applications when the clients get connected to the specific WLAN.
 - **Application**—List the applications that can be allowed/denied.
 - **Action**— Choose **Mark** to allow the application process with priority, **Drop** to deny the application and **Rate limit** to limit the rate (includes the Average Rate and Burst Rate) at which the application runs.

Configuring Advanced Options

Switch to Expert View in the CBW Web-UI by clicking the bi-directional arrows toggle button on the top-right.

Navigate to **Wireless Settings > WLANs > Add new WLAN/RLAN > Advanced**:

- **Allow AAA Override**—AAA Override option of a WLAN enables you to configure the WLAN for identity networking. It enables you to apply VLAN, Access Control Lists (ACLs) and Quality of Service (QoS) to individual WLANs on the returned RADIUS attributes from the AAA server.
- **802.11r**—802.11r enabled WLAN provides faster roaming for wireless client devices. It is desired that 11r capable devices will be able to join a WLAN with 11r enabled for better roaming experience. However, if 11r is enabled on a WLAN, the legacy devices (i.e. is non-11r clients) will not be able to join the WLAN.

This feature help clients roam better by telling them when to roam and providing them with information about neighboring APs so that no time is wasted scanning when roaming is needed.

This option is available only for WPA2/WPA3 Personal WLAN with the WPA2 toggle button alone enabled, or WPA2 Enterprise enabled WLANs. By default, this option is **Disabled**.



Note The 802.11r and WPA3 are not compatible with each other.

- **Over The DS**—Use **Over The DS** (Distributed System) button to enable or disable the fast roaming facility. By default, this is **Disabled**.
- **Reassociation Timeout(secs)**—Enter the number of seconds after which the re-association attempt of a client to an AP should time out. The valid range is 1 to 100 seconds. Default is 20 seconds.
- **DTIM Period 802.11a/n(beacon intervals)**—Depending on the timing set for your AP, it “buffers” broadcast and multicast data and let your mobile devices or clients know when to “wake up” to receive those data.
- **DTIM Period 802.11b/g/n(beacon intervals)**—Depending on the timing set for your AP, it “buffers” broadcast and multicast data and let your mobile devices or clients know when to “wake up” to receive those data.
- **Client Band Select**—Band selection enables client radios that are capable of dual-band (2.4 and 5 GHz) operation to move to a less congested band.
- **Client Load Balancing**— This feature can be used in order to load-balance clients across access points. Enabling this will improve client distribution on the wireless network.



Note You cannot configure the number of clients per AP.

- **Umbrella Profile, Umbrella Mode, Umbrella DHCP Override**—For details on these options, refer to [Configuring Cisco Umbrella on Primary AP, on page 104](#)
- **mDNS, mDNS Profile**—For details on these options, refer to [Mapping mDNS Profile to WLAN, on page 101](#)
- **Multicast IP**— Enter the Multicast IP group address. By default, the field will be null.
- **Multicast Direct** — Enable the Multicast Direct toggle button to enhance the video streaming for wireless clients by converting multicast packets to unicast at CBW AP. By default, this is **Disabled**.

To enable this toggle, change the **QoS** value under the **Traffic Shaping** section to **Gold** or **Platinum**.

For details, see [Media Steam, on page 95](#).

Configuring Scheduling

CBW supports an option to schedule availability for every WLAN. By default, all WLANs are available 24/7 when they are initially created. To schedule the WLAN availability, do the following:

1. Navigate to **Wireless Settings > WLANs > Add new WLAN/RLAN > Scheduling**.
2. **Schedule WLAN**—You may choose one of the following options from the drop-down.
 - **Enable**—This enables scheduling for a chosen WLAN.
 - **Disable**—This disables scheduling for all the WLANs except the WLAN that is enabled.
 - **No Schedule**—Scheduling is not applied to the WLAN.



Note You can also schedule the day/time for the WLAN to be broadcasted by enabling the corresponding Day and mention the start and end time using the slider.

Enable the option **Apply to all Weekdays** to make changes for all the weekdays. By default, it is **disabled**.

3. Click **Apply** to save the changes.

Enabling and Disabling WLANs RLANs

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

Step 2 In the **WLANs** window, click the **Edit** icon adjacent to the WLAN you want to enable or disable.

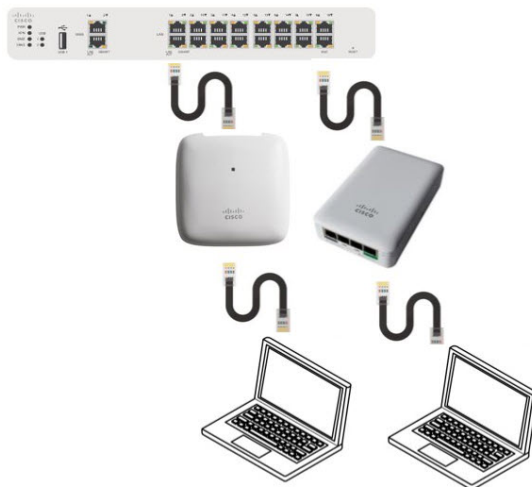
Step 3 In the **Edit WLAN/RLAN** window, under **General**, select **Enabled** or **Disabled** to enable/disable WLAN/RLAN.

Step 4 Click **Apply**.

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

Configuring RLAN in AP

In order to configure RLAN in Primary capable APs (CBW140AC, CBW240AC and CBW145AC), execute the following steps to map the RLAN to your AP ports:



1. Create RLANs with 802.1x Authentication or Open access type
2. Create AP Groups, associate RLAN to AP Group, add APs to AP Group and finally associate Wired Ports to RLANs.

To create RLAN, follow the procedure below:

-
- Step 1** Navigate to **Wireless Settings > WLANs** and click **Add new WLAN/RLAN**.
- Step 2** Under the **General** tab, select **RLAN** from the **Type** drop-down list box.
- Step 3** Enter the Profile name.
- Step 4** Under the RLAN Security, select **802.1x** or **Open** for authentication type.
- Step 5** When you enable the **802.1x**, the following options are displayed:
- MAB (MAC Authentication Bypass)—MAB enables port-based access control using the MAC address of the client. A MAB-enabled port can be dynamically enabled or disabled based on the MAC address of the device that connects to it. Add the client MAC in the Local MAC Address table. Refer to [Blocking and Unblocking Clients, on page 58](#) clients. By default, it is **enabled**.
 - Authentication Server—Please refer to [Security Type - WPA2 Enterprise](#).
- Step 6** Use the parameters available on the **General**, **RLAN Security**, and **Advanced** tabs for configuring the remote LAN.
- Note** For descriptions of parameters available under **RLAN Security**, **VLAN & Firewall**, **Traffic Shaping** and **Advanced** tabs, refer to [Configuring WLAN Security, on page 46](#).
- Step 7** Click **Apply** to save the changes.
- You can monitor the number of clients connected to the network by navigating to **Monitoring > Network Summary** and view the wired clients in the **Wired Networks** block.
-

Editing and Deleting WLANs RLANs

- Step 1** Choose **Wireless Settings > WLANs/RLANs**.
- Step 2** In the table of WLANs listed, perform one of the following actions as required:
- To edit a WLAN/RLAN, click the **Edit** icon adjacent to the WLAN/RLAN you want to modify.
 - To delete a WLAN/RLAN, click the **Delete** icon adjacent to the WLAN/RLAN you want to delete.
-

Viewing and Managing WLAN Users

You can view and manage WLAN users only for WPA2 Enterprise and Guest WLAN with Local User Accounts as access types. To use your Cisco Business Wireless network, a wireless client should connect to a WLAN in the network. To connect to a WLAN, the wireless client will have to use the user credentials set for that WLAN. If this WLAN uses WPA2-Personal as a Security Policy, then the user must provide the appropriate WPA2-PSK set for that WLAN on the Primary AP. If the Security Policy is set to WPA2-Enterprise/Local User Account, the user must provide a valid user identity and the corresponding password

In the **WLAN Users** window, you can set up different users and their respective user credentials for the different WLANs in the CBW AP wireless network. These are local users authenticated by the Primary AP using WPA2-PSK.

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

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

- **User name**—Name of the WLAN user.
- **Guest user**—Indicates a guest user account if the toggle button is enabled. This user account is provided with a limited validity of 86400 seconds (or 24 hours) from the time of its creation.
- **WLAN Profile**—The WLANs that the user can connect to.
- **Password**—The password to connect to a WLAN.
- **Description**—Additional details or comments about the user.

Adding a WLAN User

To add a WLAN user, click **Add WLAN User** and specify the following details:

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

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

For information on adding WLANs, see [Adding and Modifying a WLAN, on page 45](#).

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

Editing a WLAN User

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

Deleting a WLAN User

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

Blocking and Unblocking Clients

-
- Step 1** Go to **Wireless Settings > WLAN Users > Local MAC Address**.
- Step 2** Click **Add MAC Address** and add the client MAC address.

Step 3 You can choose to **Allowlist/Blocklist** the client by selecting it from the **Type** option and then click **Apply**.

Choose the type as **Blocklist** to deny the client joining your network.

Note Blocklisting a client or Mesh Extender that is currently joined to the network will not take effect until it attempts to rejoin the network after a disconnect or reboot.

Choose the type **Allowlist** to add the client to your network. The **MAC Filtering** should be enabled on the WLAN to add your client MAC to the Local MAC address with Type as **Allowlist**. This helps the client to join the network.

You can also import/export the Local MAC address list.

The status of Import is displayed under **Local MAC Address** section. Select **Click Here** to see the list of MAC IDs which failed to be imported.

Social Login for Guest Users

This feature provides social login privileges for guest users that are connected using Google or Facebook accounts. To enable this option, execute the following on the Primary AP:

Step 1 On the left navigation pane, choose **Wireless Settings > WLANs > Add new WLAN/RLAN**

Step 2 Under the **General tab**, fill in the basic information for your WLAN. For details, see [Adding and Modifying a WLAN, on page 45](#).

Step 3 Click the **WLAN Security** tab. Specify the following details:

- a) Enable the **Guest Network** toggle button.
- b) Under **Access Type** drop down list, select **Social Login**.
- c) Enable **Facebook** or **Google**, or both.
 - If the **Facebook** toggle alone is enabled, guest users are authenticated using Facebook accounts.
 - If the **Google** toggle alone is enabled, guest users are authenticated using Google accounts.
 - If **both** toggles are enabled, guest users are authenticated using Facebook or Google accounts.
- d) Click **Apply** to save the configuration.
- e) Once the WLAN is created with the **Social Login** access type, the respective **Pre-auth ACL** is automatically mapped to the WLAN.

Note Note You can also add and edit your URLs by navigating to Enable_Social_Login in **Advanced > Security settings**.

The Guest WLAN with an enabled Social login access type will be created. Once you connect to this guest WLAN you will be redirected to the default login page where you will find the login buttons for Google, or Facebook, or both depending on the toggle buttons enabled. Log in using the respective account and obtain the Internet access.

Personal PSK for Clients

This feature provides the flexibility of configuring a different PSK passphrase for clients connecting to the same WPA2 Personal WLAN with WPA2 policy enabled. CBW AP uses an AAA server to authenticate the client.



Note This feature is not supported for WPA3 enabled WLANs.

To enable this feature, switch to Expert View and configure the following on the Primary AP:

- Step 1** Navigate to **Wireless Settings > WLANs > Add new WLAN/RLAN**.
- Step 2** Under the **General** tab, fill in the basic information for your WLAN. For more information see [Adding and Modifying a WLAN, on page 45](#).
- Step 3** Click the **WLAN Security** tab and specify the following details:
- Enable **MAC Filtering** toggle button.
 - Under the **Security Type** drop-down list, select **WPA2/WPA3 Personal**.
 - Click the **WPA2** toggle button to turn it on.
 - Select the **Passphrase Format** as either HEX or ASCII.
 - Enter the **Passphrase**.
 - Confirm the **Passphrase**. For more information see [Adding and Modifying a WLAN, on page 45](#).
- Step 4** Under the **Radius Server** tab, map the radius server detail using the following steps.
- Click **Add RADIUS Authentication Server**.
 - Click **Add RADIUS Accounting Server**.
 - Select the Radius Server IP address from the drop-down list.
 - Click **Apply**.
- After a successful MAC authentication, RADIUS Server will display the following Cisco AVPair attributes:
- **psk-mode** – This contains the format of the Passphrase, it could be either ASCII, HEX, asciiEnc, or hexEnc.
 - **psk** – This contains the Passphrase configured for the client on the RADIUS Server
- Note** The psk value could be a simple ASCII or HEX value or encrypted bytes in case of asciiEnc or hexEnc. The algorithm used for encryption or decryption is as per RFC2865 (user-password section – 16 bytes authenticator followed by encrypted key).
- To configure radius server, navigate to **Management > Admin Accounts > Radius (Expert View)**. For details, refer to [Managing TACACS+ and RADIUS Servers, on page 80](#)
- Step 5** Click the **Authentication Caching** toggle button.
- Enter the **User Cache Timeout** in minutes
 - Enter the **User Cache Reuse** if required.
- By default, the **User Cache Reuse** is disabled. For more information see [RADIUS Server, on page 50](#)

If **Authentication caching** is enabled, the PSK key is stored in the local cache along with the MAC Address and is used for subsequent authentications. The CBW AP first checks if any local DB is available for authenticating the client otherwise the request will be sent to Radius server for Authentication.

View the Auth cached clients at **Management > Admin Accounts > Auth Cached Users (Expert View)**. For more information see [Viewing Auth Cached Users, on page 83](#)

Step 6 Under the **Advanced** tab, click the **AAA Override** toggle button.

Step 7 Click **Apply** to save the WLAN updates.

- Note**
- Devices with MAC addresses configured on Radius server will be able to connect to WLAN only with PSK passphrase configured on Radius server.
 - Devices with MAC addresses configured on Radius server will not be able to connect to WLAN with PSK configured on WLAN.
 - Devices with no MAC addresses configured on Radius server will be able to connect to WLAN with PSK configured on WLAN only. Navigate to **Wireless Settings > WLAN Users > Local MAC Addresses** and add the Client MAC in the **Allowlist** field. For more information see [Blocking and Unblocking Clients, on page 58](#).

Managing Associated Access Points

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

Step 2 In the **Access Points Administration** window, the number of APs associated with the CBW is displayed at the top of the window, along with the following details:

- **Manage**—The following icons indicate whether the AP is acting as a Primary AP or Primary capable AP or Mesh Extender.

Figure 1: Primary AP icon



Figure 2: Mesh Extender icon



Figure 3: Subordinate AP icon



- **Type**—Specifies if the AP is Primary capable or a Mesh Extender.
- **Location**—Location of the AP.

- **AP Role**—Operating role of the AP. It can be either Root or Mesh. The AP Role is only accessible on APs and only when in Expert mode.
- **Name**—Name of the AP.
- **IP Address**—IP address of the AP.
- **AP MAC**—The MAC address of the AP.
- **Up Time**—Duration of how long the AP has been powered up.
- **AP Model**—The model number of the access point.

Note When an AP joins an AP group; or the RF profile of the AP group is changed, the AP rejoins the Primary AP. The AP will receive new configuration specific to the new AP group or RF profile.

Global AP Configuration

This allows you to configure a Native VLAN ID.

-
- Step 1** Navigate to **Wireless Settings > Access Points**.
 - Step 2** Click **Global AP Configuration** and configure the **Native VLAN ID** under the **VLAN Tagging** tab.
 - Step 3** Click **Apply**.
-

Administering Access Points

-
- Step 1** Choose **Wireless Settings > Access Points**.
 - Step 2** In the **Access Points** window, click the **Edit** icon adjacent to the AP you want to manage.

Note You can only administer those APs that are associated to the Primary AP.

- Step 3** In the **Edit**, under the **General** tab, you can edit the following AP parameters:
 - The **Make me Primary AP** button is available only for subordinate APs that are capable of participating in the Primary Election process. Click this button, to make the AP, the Primary AP.
 - **IP Configuration**—Choose **Obtain from DHCP** to let the IP address of the AP be assigned by a DHCP server on the network, or choose to have a **Static IP** address. If you choose to have a static IP address, then you can edit the IP Address, Subnet Mask, and Gateway fields.
 - **AP Name**—Edit the name of the AP. This is a free text field.
 - **Location**—Edit a location for the AP. This is a free text field.
 - **Set as Preferred Primary**—Enable this to make the AP as the preferred Primary.

Note Setting as Preferred Primary will not change the current network status. In other words, it will not force the AP to take over as Primary, but it will take effect next time the network reboots.

- **Rogue Detection**— Enable this option to make the AP detect Rogue AP and client on both 2.4GHz and 5GHz radios.

Note

- Imported AP configuration would take precedence. Refer to the *Tools* section in [Viewing Access Point Details, on page 22](#).
- When upgrading from earlier versions (where rogue detection was enabled), even after upgrade rogue detection would remain enabled.
- If rogue detection is disabled, no new rogues would be detected. Rogues that are already detected, would be removed after 5 minutes, based on the default expiry time of rogue APs and clients.

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

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

Step 4 For the Primary AP, under the **Primary** tab, you can manually edit the following Primary AP parameters:

- **Primary AP Name**—You can edit the Primary AP Name set during Initial configuration using Setup Wizard.
- **IP configuration**—You can configure either Static IP or obtain from DHCP.
- **IP Address**—This IP address can be used in the Login URL to access the Primary AP's web interface. The URL is in the format `http://<ip addr>` or `https://<ip addr>`. If you change this IP address, the login URL also changes.
- **Subnet Mask**—Subnet mask of the network.

Note **IP Address**, **Subnet Mask** and **Gateway** fields are editable only if **Static IP Address** is selected.

- **VRID**—Virtual Router Identifier, is a unique number used to identify a virtual router. By default, the value of VRID is 1 and the configurable range is between 1-255. This option is available only in **Expert View**.

Note Change the VRID only if a VRID conflict is detected in the network. To check if there are any VRID conflicts, go to **Advanced > Logging**. In the **Logs** window, the following message will be logged in **Errors (3) level**: `%CNFGR-3-VRRP_CONFLICT_DETECTED: cnfgr.c:4856 VRRP group conflict detected with VRID <vrid number>! Configure new VRID value under Wireless Settings > Access Points > Edit AP > Primary AP in Expert View"`

- **Country Code**—Select the country for your Primary AP. It is not advisable to change the country code unless you have not configured the correct country in the initial setup wizard.

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

Note The **Radio 1** tab corresponds to the 2.4 GHz (802.11 b/g/n) radio on all APs. The **Radio 2** tab corresponds to only the 5 GHz (802.11a/n/ac) radio on all APs.

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

Parameter	Description
Status	Enable or Disable the corresponding radio on the AP.
Channel	<p>For 2.4 GHz, you can set this to Automatic, or set a value from 1 to 11.</p> <p>Selecting Automatic enables Dynamic Channel Assignment. This means that channels are dynamically assigned to each AP, under the control of the Primary AP. This prevents neighboring APs from broadcasting over the same channel and prevents interference and other communication problems. For the 2.4 GHz radio, 11 channels are offered in the U.S. and up to 14 in other parts of the world. However, only 1-6-11 can be considered non-overlapping if they are used by neighboring APs.</p> <p>Assigning a specific value statically assigns a channel to that AP.</p> <p>For 5 GHz, you can set this to Automatic,36,40,44,48,52 (DFS),56 (DFS),60 (DFS),64 (DFS),100 (DFS),104 (DFS),108 (DFS),112 (DFS),116 (DFS),120 (DFS),124 (DFS),128 (DFS),132 (DFS),136 (DFS),140 (DFS),144 (DFS),149,153,157,161 or 165.</p> <p>For the 5 GHz radio, up to 23 non-overlapping channels are offered.</p> <p>Assigning a specific value statically assigns a channel to that AP.</p> <p>Note The channels in both the radios will change according to the country configured in the Primary AP.</p> <p>For Mesh backhaul Radio, the Automatic option is not supported in Mesh mode.</p>
Channel Width	<p>The channel width for 2.4 GHz can only be 20 MHz.</p> <p>The channel width for 5 GHz can be set to Automatic, or to 20, 40, or 80 MHz, if channel bonding is used. By default, it is set to 80 MHz.</p> <p>Channel bonding groups the channels by 2 or 4 for a single radio stream. This increases the speed and the throughput. Because the number of channels is insufficient in 2.4 GHz, channel bonding cannot be used to enable multiple non-overlapping channels.</p>

Parameter	Description
Transmit Power	<p>You can set it to Automatic, or provide a value ranging from 100, 75, 50, 25, 12 (in terms of percentages).</p> <p>By default, it is set to 100% (maximum power).</p> <p>Selecting Automatic adjusts the radio transmitter output power based on the varying signal level at the receiver. This allows the transmitter to operate at less than maximum power for most of the time; when fading conditions occur, transmit power will be increased as required until the maximum is reached.</p> <p>For Mesh backhaul Radio, the Automatic option is not supported in Mesh mode.</p> <p><i>Nations apply their own RF emission regulations to the allowable channels, allowed users and maximum power levels within these frequency ranges. As per the regulatory rules, the DFS channels (52 – 144) have low TX power levels compared to non-DFS channels (36-48, 149-165).</i></p> <p>Please choose the non DFS channel for maximizing the coverage.</p> <p>In Mesh Mode navigate to: Wireless Settings > Access Points and click the edit icon at the left end of the row, then select Radio 2 and Channel.</p> <p>In Non-mesh mode: (in Expert view) navigate to: Advanced > RF Optimization > Select DCA channels > 5Ghz then unselect the DFS channel numbers.</p>
Interferer Detection	<p>Enable this option to identify the non Wi-Fi devices.</p> <p>Note Ensure that you enable the Interferer detection globally under Advanced > RF Optimization (in Expert View).</p>

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

Note For details on the **Mesh** tab, refer to [Mesh Network Components, on page 70](#).

Access Point Groups

By creating Access Point Groups you can control which SSIDs or RLANs can be pushed to each AP group. Each access point advertises the enabled WLANs/RLANs that belong to its access point group. The access point does not advertise disabled WLANs/RLANs in its access point group or WLANs/RLANs that belong to another group.

By default, there is a AP Group called **default-group** created on your Primary AP and all the WLANs/RLANs are mapped to this default group. All the access points are also mapped to this default-group. This means, WLAN/RLAN (ID 1-16) will be available in any of the APs belonging to the default group.



Note Any AP or Mesh extender added to the network is mapped to the **default-group**. If required, you can create your own AP group and map the AP to the same.

For Mesh deployments, ensure both the Root AP and Mesh AP are mapped to the same Access Point Group.

To configure this, do the following:

1. Switch to **Expert View** by clicking the bi-directional icon on the top right of the Primary AP UI.
2. Go to **Wireless Settings > Access Points Groups > Add New Group**.
3. In the **General** tab, provide an AP Group Name and a description for your reference.
4. In the **WLANs** tab, select the WLAN or RLAN that you want to push to the group.
5. In the **Access Points** tab, push the access point to the group that you created such that the WLANs/RLANs is advertised in only those particular APs.



Note RLANs are supported in non-mesh deployment only.

6. Select the **RF profile** in 2.4 GHz and 5 GHz, if needed. Else, you can create a custom RF Profile. For details, refer to [RF Profiles, on page 113](#).
7. In the **Ports** tab, enable the LAN ports to which you want to map the RLAN. Thereby, select a particular RLAN from the Remote LAN drop-down list box. This is applicable only in non-mesh deployments.

By default, LAN1 and PoE is enabled.



Note Power over Ethernet- PoE enables Power and Data to be combined onto a single Ethernet cable. For example, IP cameras can be powered up through this port.

8. Click **Apply**.

Setting a Login Page for WLAN Guest Users

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

-
- Step 1** Set up a new WLAN or decide on an existing WLAN, to which you will provide access for guest users. You can also specifically set up a WLAN exclusively for guest access. This is done by setting the **WLAN Security** as **Guest** for that WLAN. For more information, see [Adding and Modifying a WLAN, on page 45](#).
- Step 2** Set up a guest user account. Go to **Wireless Settings > WLAN Users**, and set up an account with the **Guest User** check box selected. For more information, see [Viewing and Managing WLAN Users, on page 57](#).

You can provide the Guest Users of your WLAN with one of the following login page options:

- A simple minimalist default login page with a few modification options. To configure this, see [Setting the Default Login Page, on page 67](#).
 - A customized login page uploaded into the Primary AP. To configure this, see [Setting a Customized Login Page, on page 67](#).
-

Setting the Default Login Page

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

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

Step 2 In the **Guest WLANs** page, the number of Guest WLANs currently set up in the network is displayed at the top of the page.

Step 3 Choose the **Internal (Default)** login page in the **Page Type** drop-down list.

Step 4 Set the following parameters to modify the default internal login page:

- **Display Cisco Logo**—This field is set to **Yes** by default. To hide the Cisco logo that appears at the top-right corner of the default window, choose **No**. However, you do not have an option to display any other logo.

Note You can preview the changes by clicking **Apply** > **Preview**.

- **Redirect URL After Login**— To have guest users redirected to a particular URL (such as the URL for your company) after login, enter the URL in this field. You can enter up to 254 characters.
- **Page Headline**—The default headline is *Welcome to the Cisco Business Wireless*. To create your own headline on the login page, enter the desired text in this field. You can enter up to 127 characters.
- **Page Message**— The default message is displayed: *Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.* To create your own message on the login page, enter the desired text in this field. You can enter up to 2047 characters.

Step 5 Click **Apply**.

Setting a Customized Login Page

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



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



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

Before you begin

Create a custom login page on a computer while ensuring the following:

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

Compress the page and image files into a .TAR file. The maximum allowed size of the files in their uncompressed state is 1 MB.

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

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



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

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

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

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

Step 3 Click **Upload** and browse to upload the .TAR file of the customized web authentication bundle. While uploading the .TAR file, the status of file upload is displayed on the same page.

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

Step 5 Click **Apply**.

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

About Cisco Mesh

Cisco Mesh introduces a new paradigm of wireless internet access by providing high data rate service and reliability. It is also a solution to reduce the complexity of wiring between each devices in a network. For a stable network establishment, there must be a wireless interacting medium between each APs.

CBW indoor mesh brings these values to you:

- Not having to run Ethernet wiring to each AP.
- Network connectivity where wires cannot provide connectivity.
- Easy to deploy and provide flexibility in deployment.

This chapter summarizes the design details for deploying a Cisco Mesh Extender for indoor environments. The indoor wireless access takes advantage of the growing popularity of inexpensive Wi-Fi clients, enabling new service opportunities and applications that improve user productivity and responsiveness.

Adding a Mesh Extender

For details refer to [Adding Mesh Extenders, on page 17](#).

Convert Non-Mesh to Mesh Deployment

For maintaining, the mesh state between the AP's there must be a communication establishment between them and this takes place through the backhaul radio (2.4GHz or 5GHz – user configurable). To configure the mesh mode in the Primary AP, do the following:

Step 1 Go to **Wireless Settings>Mesh**.

Step 2 Enable the **Mesh** toggle button and click **Apply**.

Step 3 The entire network will operate in the **Mesh** mode after the Primary AP reboots.

Step 4 Add the MAC address of the Mesh Extenders in the auth-list that you wish to join the network.

Note For details refer, [Adding Mesh Extenders, on page 17](#).

For the wired access points (CBW140AC, CBW240AC, CBW145AC) the MAC address will be added automatically in the Local MAC Address table, provided they exist in the same network.

Step 5 The automatic entry of the physical address of the wired AP can be verified by knowing its last few digits in the MAC address.

For example, when a CBW140AC has joined the Primary AP, its MAC address will be displayed in the Local MAC Address table with its corresponding description as (CBW140AC-f898). Here, **f898** is the ending digits of its MAC address *A4:53:39:0E:F8:98*.

Step 6 Wait for few minutes and navigate to **Wireless Settings>Access Points**.

Step 7 Check if the access point has joined the Primary AP.

Mesh Network Components

Navigate to **Wireless Settings > Access Points**. Click **Edit Access point**. The following options are available under the **Mesh** tab.

- **AP Role**—By default, the Primary/Primary Capable AP role is set to **Root** and the mesh extenders role is set to **Mesh**. You can configure the AP Role for Primary Capable APs from Root/Mesh to Mesh/Root. This option is configurable in **Expert View**. After changing the AP Role, the Primary Capable AP will reload and join the Primary AP.

To check the AP role and type, navigate to **Wireless Settings > Access Points**.

If the Primary Capable AP role is changed from **Root** to **Mesh**, the type will be displayed as **Mesh Extender**. The AP will join as a **Wired Mesh Extender** if a wired uplink is present. If not present, the AP will join as **Wireless Mesh Extender**. In either case, the functionality of Mesh Extender remains the same.

If the Primary Capable AP role is changed from **Mesh** to **Root**, the Type will be displayed as **Primary Capable**.



Note

- Only Primary Capable APs (CBW140AC, CBW145AC, CBW240AC) are allowed to change the AP role.
- Primary Capable APs that are operating with AP Role as **Mesh**, will not be considered for Primary AP selection.

- **Bridge Type**—By default, it is set as **indoor**
- **Bridge Group Name**—Bridge group names (BGNs) control the association of mesh access points. BGNs can logically group radios to avoid two networks on the same channel from communicating with each other. The setting is also useful if you have more than one Primary capable AP in your network in the same sector (area). Default BGN is set with first 10 characters of the configured SSID during initial setup wizard. This option is available in **Expert View**.



Caution

Exercise caution when you configure a BGN on a live network. Always start a BGN assignment from the farthest-most node (last node, bottom of mesh tree) and move up toward the RAP to ensure that no mesh access points are dropped due to old and new BGNs mixed within the same network.

- **Strict Matching BGN**—When Strict Match BGN is enabled on the mesh AP, it will scan ten times to find the matched BGN parent. After ten scans, if the AP does not find the parent with matched BGN, it will connect to the non-matched BGN and maintain the connection for 15 minutes. After 15 minutes, the AP will again scan ten times and this cycle continues. The default BGN functionalities remain the same when Strict Match BGN is enabled. By default, it is **disabled**. This option is available in **Expert View**.
- **Preferred Parent**—This has to be computed from the Radio MAC of the Primary capable AP which you would like to set as preferred parent your Mesh AP. We need to add 11 in hex to last two bytes of the Preferred Parent's radio MAC. To obtain the Radio MAC of the Primary capable AP, go to **Monitoring > Access Points**, and view the AP details by selecting the AP you want. Note down the Radio MAC

(xx:xx:xx:xx:xx:yy) and compute the value to be set in **Preferred Parent** field. Refer the table for sample computation.



Note This field is present only in Mesh Extender's **Mesh** tab.

Before (yy)	After adding (+11) (yy')
20	31
40	51
60	71
80	91
A0	B1
C0	D1
E0	F1

- **Backhaul Interface**—This displays the type of interface. It can be either 802.11a/n/ac if Mesh Backhaul Slot is 5GHz and 802.11b/g, if Mesh Backhaul Slot is 2.4GHz.
- **Install Mapping on Radio Backhaul**—This option helps to broadcast the SSIDs in backhaul radio such that the client can join the AP using the backhaul radio. By default it is **Enabled**. If you experience Mesh performance or stability issues, you can disable this option to avoid wireless clients joining the backhaul radio.
- **Mesh Backhaul Slot**—The communication between each APs are carried over a particular radio and you can configure it in either 5GHz or 2.4GHz. By default, it is in **5GHz** mode.



Note The Backhaul interface configuration done under **Wireless Settings > Mesh > Mesh Backhaul Slot** is the global configuration. If you want to override it for selected Access Points, you can change the Backhaul interface configuration by navigating to **Wireless Settings > Access Points (Edit) > Mesh > Mesh Backhaul Slot**.

- **Ethernet Bridging**—By using this feature, you can access internet by connecting a wired client to the LAN ports of the APs in the Mesh network. By default, it is **Enabled**.

Primary APs (**CBW240AC**, **CBW145AC**) and Mesh Extender (**CBW141AC** or **CBW143AC with PoE adapter module**) support the Ethernet Bridging functionality.

Refer [LAN port functionality for different models, on page 127](#) to know the LAN port functionalities for different model APs.

Ethernet bridging is **enabled** by default in Mesh mode.

1. Connect a client to the **Ethernet port of CBW240AC or CBW145AC or CBW141ACM or CBW143ACM**.



Note The wired client connected to the LAN port of the AP will obtain the IP address in the AP's VLAN network.

2. Check if you are able to access the internet.



Note The Primary AP Web UI can be accessed only through the Management IP and not through the URL: *https://ciscobusiness.cisco*.

3. In the **Mesh** mode, the wired client connected to LAN ports will not be displayed in the Primary AP UI.

4. On connecting a client to the Ethernet port, the **Operational Status** changes to **UP**. You can change the VLAN and mode of that LAN port using the following steps. (By Default the Mode is **Access**).

To configure VLANs, enable VLAN Transparency in **Mesh** Tab under **Wireless Settings > Mesh > VLAN Transparent**. Click on the **Edit** icon to change the configuration of the particular port. The **VLAN Mapping** window is displayed:

- a. Set the **Mode** to **Access** or **Trunk**.
- b. When you select the mode as **Access**, the VLAN Id is 0 by default. This enables the Wired client to obtain the IP in AP's VLAN.
- c. When you select the mode as **Trunk**, you can configure the Native VLAN on that port and other allowable VLANs for incoming or outgoing traffic.



Note You can configure the Native VLAN under **Wireless Settings > Access Points > Global AP Configuration > VLAN Tagging**.

Changing Mesh Parameters

Following are the several mesh configurations that are available in the Primary AP UI under **Wireless Settings > Mesh**.

Backhaul Client Access

When Backhaul Client Access is enabled, it allows wireless client association over the backhaul radio. The backhaul radio is a 5-GHz radio for most of the Cisco Access Points. This means that a backhaul radio can carry both backhaul traffic and client traffic.

When Backhaul Client Access is disabled, only backhaul traffic is sent over the backhaul radio and client association is over the second radio(s). By default, this option is **Enabled**.

Mesh Backhaul Radio Resource Management

The Radio Resource Management (RRM) software embedded in the Primary AP acts as a built-in RF engineer to consistently provide real-time RF management of your wireless network. RRM enables the Primary AP to continually monitor their associated lightweight access points for information on traffic load, interference, noise, coverage and other nearby APs.

The RRM measurement in the mesh AP backhaul is enabled, if the wired Root AP has Ethernet uplink and there is no Mesh Extender joined to it.

Mesh Backhaul Slot



Note The Backhaul interface configuration done under **Wireless Settings > Mesh > Mesh Backhaul Slot** is the global configuration. If you want to override it for selected Access Points, you can change the Backhaul interface configuration by navigating to **Wireless Settings > Access Points > (Edit) > Mesh > Mesh Backhaul Slot**.

In certain countries, Mesh Network with 5 GHz backhaul network is not allowed to use. Even in countries which is permitted with 5 GHz, customers may prefer to use 2.4 GHz radio frequencies to achieve much larger Mesh or Bridge distances.

When a Primary AP downlink backhaul is changed from 5 to 2.4 GHz or from 2.4GHz to 5 GHz, that selection gets propagated from Primary AP to all the Subordinate APs and they will disconnect from the previously configured channel to get reconnected to another channel. To do this, follow the instructions below:

Step 1 Go to **Wireless Settings>Mesh>Mesh Backhaul Slot**.

Step 2 Select the **backhaul radio** (either 5 GHz or 2.4GHz) in the Primary AP such that the configuration gets pushed to its subordinate APs to have a better mesh coverage.

Note Only Primary capable APs are configured with the backhaul frequency of 5 or 2.4GHz. Once the AP is configured, the same frequency selection will propagate down the branch to all the Subordinate APs.

Modifying AP Port Configuration to Access/Trunk Mode



Note AP port configuration is applicable only to CBW240AC, CBW145AC, and CBW143ACM APs.

Step 1 Go to **Wireless Settings > Access Points**.

Step 2 Click **Edit AP**.

Step 3 In the **Mesh** tab, ensure that the **Ethernet Bridging** is enabled.

Step 4 Click **Edit** in the Port table. This is available when **Ethernet Bridging** is enabled.

Step 5 In the **Mode** tab, select **Access** or **Trunk**.

Step 6 In the **VLAN Id**, specify the VLAN.

The Operational Status changes to UP when an ethernet port is connected to a client.

VLAN Transparent

This feature determines how a mesh access point handles VLAN tags for Ethernet bridged traffic. If **VLAN Transparent** is enabled, then VLAN tags are not handled and packets are bridged as untagged packets. To configure, go to **Wireless Settings > Mesh > Ethernet Bridging**.



Note No configuration of Ethernet ports is required when VLAN transparent is enabled. The Ethernet port passes both tagged and untagged frames without interpreting the frames.

If **VLAN Transparent** is disabled, then all packets are handled according to the VLAN configuration on the port (trunk, access mode). For details, see [Modifying AP Port Configuration to Access/Trunk Mode, on page 73](#).



Note

- If the Ethernet port is set to Trunk mode, then Ethernet VLAN tagging must be configured.
- To use VLAN tagging, you must uncheck the VLAN Transparent check box. By default, it is enabled.

To enable the VLAN Transparent, do the following:

-
- Step 1** Navigate to **Wireless Settings>Mesh>Ethernet bridging**.
- Step 2** Enable **VLAN Transparent**.
-



CHAPTER 6

Management

This chapter describes how to manage the network and upgrade the software. It contains the following topics:

- [About Management Access Interface, on page 75](#)
- [Setting Up Management Access Interface, on page 75](#)
- [Limitation of Web Based Management Sessions, on page 76](#)
- [Managing User Priority Order, on page 77](#)
- [Managing Admin Accounts, on page 77](#)
- [Managing Guest Users using the Lobby Admin account, on page 79](#)
- [Managing TACACS+ and RADIUS Servers, on page 80](#)
- [Viewing Auth Cached Users, on page 83](#)
- [Setting Date and Time, on page 84](#)
- [Configuring Date and Time Manually, on page 85](#)
- [Updating the CBW AP Software, on page 86](#)
- [Updating the Software using HTTP, on page 88](#)
- [Updating the Software using TFTP, on page 90](#)
- [Updating the Software using SFTP, on page 91](#)
- [Updating the Software through Cisco.com, on page 92](#)
- [Updating the Software through Cisco Business Dashboard, on page 93](#)

About Management Access Interface

The Management Access Interface is the default interface for in-band management of the Primary AP and connectivity to enterprise services. It is also used for communication between the Primary AP and connected access points (APs). You can access the web interface of the Primary AP by entering the management interface IP address of the Primary AP or using <https://ciscobusiness.cisco> in your browser's address bar.

A single AP manager interface is used to control all Primary AP to Access point (both AP and ME) communications, regardless of the number of APs and MEs.

Setting Up Management Access Interface

To enable or disable the different types of management access to the Primary AP, do the following:

Step 1 Choose **Management > Access**.

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

Step 2 You can enable or disable the following types of management access to the Primary AP, by toggling the switch buttons.

- **HTTP Access**—This enables the HTTP access mode, which allows you to access the Primary AP GUI using `http://<ip-address>` or `http://ciscobusiness.cisco` through a web browser. By default, this is **Enabled**.

Note HTTP access mode is not a secure connection.

- **HTTPS Access**—A secure access for Primary AP UI, using `https://<ip-address>` or `https://ciscobusiness.cisco`. By default, this is **Enabled**.
- **HTTP-HTTPS Maximum Session**—To set the maximum number of web sessions (HTTP/HTTPS). It can range between 1-15. By default, you can support up to 15 sessions.

Step 3 **WebAuth SecureWeb**—Enable web based authentication for Guest WLAN in order to access or visit the Guest authentication page over HTTPS.

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

Note You can access the CBW AP UI via HTTP or HTTPS connection. By default, HTTP connection will be redirected to HTTPS connection. It means, if you enter `ciscobusiness.cisco`, you will be redirected to `https://ciscobusiness.cisco` which is a secured connection.

HTTP Access	HTTPS Access	UI Accessibility
On	On	HTTP->HTTPS Redirect
Off	On	HTTPS only
On	Off	HTTP only
Off	Off	UI does not load

Limitation of Web Based Management Sessions

This feature helps to provision the number of sessions supported for the Primary AP UI. It is implemented by limiting the number of UI management sessions based on the number of HTTP/HTTPS sessions configured by the user.

- Choose **Management > Access**. Under **HTTP-HTTPS Maximum Sessions** field set the number of allowed sessions. Configurable value is from 1-15.
- Click **Apply** to save the changes. On configuring try to access the web sessions from the client using management IP.
- If the number of users exceeds the configured value, the session access is restricted and prompts for a reload of session.

Managing User Priority Order

When multiple databases are configured, it is important to configure the admin account user priority. To configure the priority, do the following:

-
- Step 1** Enable **Expert View** on the Primary AP UI. To switch to expert view, click the bidirectional arrow icon on the top right of the home screen.
 - Step 2** Navigate to **Management > Admin Accounts** and click on the **Management User Priority Order**. By default, the local database is always queried first. If the username is not found, the Primary AP switches to the RADIUS server if configured for RADIUS or to the TACACS+ server if configured for TACACS+. The default priority setting is in the order of Local Admin Accounts and then RADIUS.
 - Step 3** To change the priority, between TACACS+ and RADIUS, click on the drag icon and move UP or DOWN.
Local Admin Accounts cannot be moved to Priority 3. It can be in the order of either 1 or 2 only.
 - Step 4** Click **Apply** to save the changes.
-

Managing Admin Accounts

You can manage the Cisco Business Wireless AP network through the Primary AP UI based on the privileges assigned to your user account. This prevents unauthorized users from accessing or configuring the Primary Ap.

You can log in to the Primary AP UI using an admin account having one of the following access types:

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

For information about creating guest user accounts, see [Creating a Guest User Account, on page 79](#).

Adding an Admin Account

-
- Step 1** Choose **Management > Admin Accounts**.
The total count of admin accounts on the Primary AP is displayed at the top of this window while the table provides a detailed listing of all the available admin accounts.
 - Step 2** In the **Admin Accounts** window, click **Add New User** to add a new admin user.
 - Step 3** In the **Add/Edit Local admin account** window, set the following parameters as required:

- **Username**—The login user name used by the administrative user. User name must be unique. You can enter up to 24 ASCII characters.

Note User names are case sensitive.

- **Access**—Set one of the following access privileges for the administrator:

- **Read Only**
- **Read/Write**
- **Lobby Ambassador**

- **Password**—The password is case sensitive and can contain 8-127 ASCII characters. When specifying a password, ensure the following:

- The password must include a combination of lowercase letters, uppercase letters, digits, and special characters. The special characters can be ~, !, @, #, \$, %, ^, &, *.
- No character in the password can be repeated more than three times consecutively.
- The new password cannot be the same as the associated username or the username reversed.
- The password cannot be cisco, ocsic, or any variant obtained by changing the capitalization of the letters in the word Cisco. In addition, you cannot substitute l, I, or ! for i, 0 for o, or \$ for s.

Step 4 Re-enter the same password in **Confirm Password**.

Step 5 Enable **Show Password** to view the password entered.

Step 6 **Password Expiry**—This option facilitates to expire password for admin accounts. By default, the password expiry is **disabled** and the expiry value is set to 0 (The Admin Account will remain constant until deleted). If the password expiry is enabled, then the value is set to 180 days by default. You can set the value ranging from 1 - 180 days.

Note If the Primary AP UI is logged in with an admin account that has the password expiry enabled, a reminder message will pop-up when you log in. This message will start popping up only when there are 7 days left for password expiry.

Once the expiry value is exceeded, the admin account will be deleted.

Step 7 Click **Update** to save your changes.

Editing an Admin Account

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

The **Admin Accounts** page is displayed, along with the list of all the admin accounts present on the Primary AP. The total count of admin accounts on the Primary AP is displayed at the top of the page.

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

Step 3 Modify the admin account parameters, as required. For descriptions of these parameters, see [Adding an Admin Account, on page 77](#).

Step 4 Click **Update** to modify the parameters.

Deleting an Admin Account

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

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

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

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

Managing Guest Users using the Lobby Admin account

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

You can create and manage guest user accounts using the lobby ambassador admin account. To know more about lobby ambassador accounts, see [Managing Admin Accounts, on page 77](#).

Creating a Guest User Account

Before you begin

You will need at least one lobby ambassador user account and one Guest WLAN with **Local User Account** or **RADIUS Access Type**, before you create a guest user account. For information about creating a lobby ambassador account, see [Adding an Admin Account, on page 77](#).

Step 1 In your browser, navigate to the Primary AP UI.

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

Step 3 In the **Lobby Ambassador Guest Management** window, click **Add Guest User**.

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

- **User Name**—Specify a user name for the guest user account.
- **Wireless Network**—Select the desired guest WLANs that have already been configured for guest access to the network.

Note To know more about creating a guest WLAN, see [Creating a Guest Network, on page 132](#).

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

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

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

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

- **Password**—Specify a password for the guest user account.
- **Confirm Password**—Ensure that this entry matches what you have typed in the **Password** field.
- **Description**—This field is optional. The user can specify a suitable description for the guest user account.

Step 5 Click **Update**.

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

Note Username and password are case sensitive.

You can also modify or delete the Guest User account by using the **Edit/Delete** icons.

Managing TACACS+ and RADIUS Servers

Primary AP supports up to Six RADIUS and Three TACACS Servers. To configure RADIUS and TACACS+ Servers, enable **Expert View** on the Primary AP UI by clicking the bidirectional arrow icon on the top right of the home screen.

Adding TACACS+ Servers

Step 1 Navigate to **Management > Admin Accounts**.

Step 2 To add TACACS+ servers, click **TACACS+** tab.

Step 3 Click **Add TACACS+ Authentication Server** button and enter the following:

Note For adding TACACS+ Accounting Server, choose **Add TACACS+ Accounting Server** and proceed with the following instructions

- **Server Index**—Select 1 through 3
- **State**—Enable the state. By default this is **Enabled**
- **Server IP Address**—Enter the IPv4 address of the TACACS+ server
- **Shared Secret**—Enter the shared secret
- **Port Number**—Enter the port number being used for communicating with the TACACS+ server. By default, the port number is 49.
- **Server Timeout**—Enter the server timeout. By default, the timeout is 5 seconds.

The Table displays the configured TACACS+ (authenticating, authorizing, accounting) servers.

You can also modify or delete TACACS+ servers by using the **Edit/Delete** icons.

Configuring RADIUS Servers

Step 1 Navigate to **Management > Admin Accounts**.

Step 2 To add the RADIUS servers, click **RADIUS** and enter data as specified in the following steps:

Step 3 **Authentication Call Station ID Type**—From the drop-down list, choose the option that is sent to the RADIUS server in the Access-Request message. One of the following format types can be chosen as the Authentication Call Station ID Type that is sent to the RADIUS server:

- IP Address
- Primary AP MAC Address
- AP MAC Address
- AP MAC Address:SSID
- AP Name:SSID
- AP Name
- AP Group
- Flex Group
- AP Location
- VLAN ID
- AP Ethernet MAC Address
- AP Ethernet MAC Address: SSID
- AP Label Address
- AP Label Address: SSID
- AP MAC:SSID AP Group
- AP Eth MAC:SSID AP Group

Step 4 **Authentication MAC Delimiter**—From the drop-down list, choose the option that is sent to the RADIUS server in the Access-Request message. The delimiters can be one of the following:

- Colon
- Hyphen
- Single-hyphen
- No Delimiter

Step 5 **Accounting Call Station ID Type**—From the drop-down list, choose the option that is sent to the RADIUS server in the Access-Request message. One of the following format types can be chosen as the Accounting Call Station ID Type that is sent to the RADIUS server:

- IP Address
- Primary AP MAC Address
- AP MAC Address
- AP MAC Address:SSID
- AP Name:SSID
- AP Name
- AP Group

- Flex Group
- AP Location
- VLAN ID
- AP Ethernet MAC Address
- AP Ethernet MAC Address: SSID
- AP Label Address
- AP Label Address: SSID
- AP MAC:SSID AP Group
- AP Eth MAC:SSID AP Group

Step 6 **Accounting MAC Delimiter**—From the drop-down list, choose the option that is sent to the RADIUS server in the Access-Request message. The delimiters can be one of the following:

- Colon
- Hyphen
- Single-hyphen
- No Delimiter

Step 7 **Fallback Mode**—Specify the RADIUS server fallback behavior from the drop-down list. It can be one of the following:

- Off—Disables RADIUS server fallback.
- Passive—Causes the Primary AP to revert to a server with a lower priority from the available backup servers without using extraneous probe messages. The Primary AP ignores all inactive servers for a time period and retries later when a RADIUS message needs to be sent.
- Active—Causes the Primary AP to revert to a server with a lower priority from the available backup servers by using RADIUS probe messages to proactively determine whether a server that has been marked inactive is back online. The Primary AP ignores all inactive servers for all active RADIUS requests. Once the primary server receives a response from the recovered ACS server, the active fallback RADIUS server no longer sends probe messages to the server requesting the active probe authentication.

Step 8 **Username**—If you enabled Active fallback mode, enter the name to be sent in the inactive server probes in the Username field. You can enter up to 16 alphanumeric characters. The default value is **cisco-probe**.

Step 9 **Interval**—If you enabled Active fallback mode, enter the probe interval value (in seconds) in the Interval text box. The interval serves as inactive time in passive mode and probe interval in active mode. The valid range is 180 to 3600 seconds, and the default value is 300 seconds.

Step 10 **AP Events Accounting**—Enable this toggle button to activate sending of accounting requests to RADIUS server. During network issues, the APs join/disjoin from the Primary AP. Enabling this option ensures that these events are monitored and the accounting requests are sent to the RADIUS server to help you detect the network issues.

Step 11 Click **Apply** to save the changes.

Adding RADIUS Servers

Step 1 Navigate to **Management > Admin Accounts**.

Step 2 To add the RADIUS servers, click **RADIUS**.

This page lists any RADIUS servers that have already been added. Choose to add one of the following:

- **Add RADIUS Authentication Server**

- **Add RADIUS Accounting Server**

Note The pages used to add authentication and accounting servers contain similar fields. The following instructions are detailed for **Add RADIUS Authentication Server** pages. You would follow the same steps for **Add RADIUS Accounting Server** page.

- You can also modify or delete the Radius servers by using the **Edit/Delete** icons.

Step 3 Click **Add RADIUS Authentication Server** and enter the following:

- **Server Index**—Select 1 through 6
- **State**—Enable the state. By default this is **Enabled**.
- **Server IP Address**—Enter the IPv4 address of the RADIUS server
- **Shared Secret**—Enter the shared secret
- **Port Number**—Enter the port number used for communicating with the RADIUS server. By default, the port number of Authentication server is 1812, and the Accounting server is 1813.
- **Server Timeout**—Enter the server timeout. By default, the timeout is 5 seconds.

Viewing Auth Cached Users

Before you begin

To view the client entries which are connected to WLANs with **Authentication Caching** enabled follow the steps below.

Step 1 Switch to **Expert View** and navigate to **Management > Admin Accounts**.

Step 2 In the **Admin Accounts** page, choose the **Auth Cached Users** tab.

Step 3 The client entries stored in the local cache of Primary AP are displayed in the table with the following details:

- **MAC Address**—Displays the MAC address of the client.
- **Username**—Displays the username of the client. The MAC address is shown by default.
- **SSID**—Displays the WLAN in use by the client.
- **Timeout (Minutes)**—Displays the **User Cache Timeout Value** configured in the WLAN under **Authentication Caching**. By default, the timeout interval is 1440 minutes.
- **Remaining Time (Minutes)**—Displays the amount of time the local cache client entry is valid.

Step 4 Double-click the listed auth cached user to view the details.

You can also delete the client entry from CBW Primary AP local cache by selecting the client and click **Delete Selected**. If the client entry is removed from local cache, the authentication of the client will be done by Radius Server. For more details see [Authentication Caching](#)

Setting Date and Time

The date and time on the Cisco Business Wireless Primary AP is first set when running the initial configuration setup wizard. You can enter the date and time manually or you can specify a Network Time Protocol (NTP) server that sets the time and date.

Using NTP Servers to Automatically Set the Date and Time

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

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

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

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

Adding and Editing NTP Servers

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

Step 1 Choose **Management > Time**.

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

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

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

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

- a) **NTP Index**—Specify an NTP Index value to set the priority of the NTP server. NTP Index values can be set from 1 to 3, in the order of decreasing priority. The Primary AP will try and sync with the NTP server with the highest priority first, until the specified polling interval time runs out. If the sync is successful, the Primary AP does not continue trying to sync with any of the remaining NTP servers. If the sync is unsuccessful, then the Primary AP will try to sync with the next NTP server.
- b) **NTP Server**—Specify the IPv4 address or the fully qualified domain name (FQDN) for the NTP server. When you specify an FQDN, a DNS lookup is done. If the lookup fails, an error will be logged in the Syslog server. The Primary

AP will continue to resolve this FQDN and errors will be logged until you change the NTP configuration or specify a valid FQDN.

Step 5 Click **Apply**.

Refreshing NTP Server Status

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

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

The NTP status is automatically updated every minute.

Deleting and Disabling NTP Servers

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

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

Configuring Date and Time Manually

Step 1 Choose **Management > Time**.

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

Step 2 From the **Time Zone** drop-down list, choose your local time zone.

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

Step 3 Select the **Set Time Automatically from Current Location** check box to set the time based on the time zone specified.

Step 4 In the **Set Time Manually** field:

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

Step 5 Click **Apply**.

Updating the CBW AP Software



Note Refer to [Image Update Prerequisite](#) for updating a device later in this section.

To view the current software version of your Primary AP, you can choose the one of the following methods:

- Click the gear icon at the top-right corner of the web interface, and then click **Primary AP Information**.
- Choose **Management > Software Update**. The **Software Update** window is displayed with the current software version number listed on the top.

You can update the CBW AP software using the Primary AP's web interface. Current configurations on the Primary AP will not be deleted.

The following are the software update methods:

- [Updating the Software using HTTP](#)
- [Updating the Software using TFTP](#)
- [Updating the Software using SFTP](#)
- [Updating the Software through Cisco.com](#)
- [Updating the Software through Cisco Business Dashboard, on page 93](#)

A software update ensures that both the Primary AP software and the software on all the associated Subordinate APs are updated. Newly joining APs will be upgraded to the current version of the software running on the Primary AP.

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



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

Image Update Prerequisite

Before updating the CBW APs, you are required to obtain the Primary AP firmware image and the Mesh Extender (if your network has any Mesh Extenders) firmware image using the following steps:

- Navigate to the **Cisco Download Software** page: <http://software.cisco.com/download/navigator.html>
- From the **Download Software** window, browse to **Wireless > Access Points**. Navigate to **Business 100 Series Access Points / Business 200 Series Access Points**. Choose the model (140AC/145AC/240AC), to view a list of currently available software, with the latest displayed on the top.
- Choose a software release number.
- Click **Download** corresponding to the **CBW-Bundle-10-x-1-0.zip** file.

- Read the **Cisco's End User Software License Agreement** and then click **Agree** to proceed.
- Save the ZIP file to your computer's hard drive, and then extract the contents to a directory on your computer.

CBW AP Series	Software File to be Chosen	Image Size
CBW140AC, CBW145AC, CBW240AC (Primary capable APs)	ap1g5	~60MB
CBW141ACM, CBW142ACM, CBW143ACM (Mesh Extenders)	ap1g5-capwap	~35MB

Pre-download Image Status

You can monitor the status and progress of the update via HTTP/TFTP/SFTP/cisco.com on the Software Update page. The following data is displayed as the update progresses:

- Total number of APs in the network.
- Number of APs that are currently being updated, waiting to be updated, being rebooted and those that failed to update.

In addition to the summary above, each AP update progress is also shown with the following data:

- **AP Name**—The AP name.
- **AP Type** —Displays if the AP is a Primary AP or Primary Capable AP or Mesh Extender.
- **AP Role**— The operating role of the AP. It can be **Root** or **Mesh**. This field is available only in Mesh deployments.
- **AP Location**—The AP location.
- **Download Percentage**— By default, it displays as **NA**. While pre-downloading the software, the percentage of download is displayed.
- **Last Update Error**—In case of any error, during pre-download, the error is displayed here.
- **State**—Status of the pre-image download to the Mesh Extenders in the network. It can be one of the following:
 - **None**
 - **Initiated**
 - **Pre-downloading**
 - **Completed**
- **Retry Attempts**—Number of Attempts re-tried.

Updating the Software using HTTP

- Step 1** Obtain the ZIP file and extract the Primary AP software image and Mesh Extender (if your network has any Mesh Extenders) firmware image.
- Step 2** From the Primary AP web interface, choose **Management > Software Update**.
The **Software Update** window with the current software version number is displayed.
- Step 3** In the **Transfer Mode** drop-down list, choose **HTTP**.
- Note** For Mesh deployments, you must upgrade the Mesh Extender image prior to the Primary AP image upgrade.
- Important** Proceed with Step 4-7 if you have Mesh Extenders in the CBW AP network.
- Step 4** Enable **Mesh Extender Image** option to load the Mesh Extender image (ap1g5-capwap). By default, this option will be **disabled**.
- Step 5** Click the **Browse** button adjacent to the **Mesh Image File** field, navigate to the folder having the unpacked ZIP file contents, and choose **ap1g5-capwap** software file.
- Note** The file explorer that opens here is an operating system-specific explorer depending on the OS of your computer.
- Step 6** Click **Update**, and then click **Ok** in the confirmation dialog.
- Caution** The top section of the page indicates the status of the download. Do not manually power down or reset the Primary AP or any AP during this process.
- The **Pre-Download Image Status** section displays the status of the pre-image download to the Mesh Extenders in the network.
- You can abort a software update that is in progress, at any time before the Primary AP completes rebooting, by clicking **Abort**.
- Step 7** One Mesh Extender in the network obtains the image first and then shares the image to other Mesh Extenders. Once all the Mesh Extenders in the network are pre-downloaded or moved to **Complete** status, **Disable** the **Mesh Extender Image** option.
- Step 8** Now, update the Primary AP and other Primary capable APs in the network. To do so, click **Browse** adjacent to the **File** field. Navigate to the folder having the unpacked ZIP file contents, and choose the **ap1g5** software file.
- Step 9** Check the **Auto Restart** check box for the Primary AP and Mesh Extender to reboot automatically after the image pre-download is complete for all the APs. By default, this option is **Enabled**.
- Step 10** Click **Update** and then click **Ok** in the confirmation dialog.
The status of the download is displayed on top of the page.
- Step 11** One Primary AP in the network obtains the image and shares the image to all other Primary capable APs.
- Step 12** After all the APs' state is moved to **Complete**, the Primary AP restarts (or reboots) to complete the software upgrade. If you have not checked the **Auto Restart** check box, you can manually reboot the Primary AP, after the upgrade, by choosing **Advanced > Primary AP Tools**, and clicking **Restart Primary AP**.
- Step 13** Log in to the Primary AP UI (after clearing the cache) and verify the Primary AP software version in the **Software Update** window.

- Note**
- While adding the Mesh Extender to the existing Mesh deployment, the new Mesh Extender will obtain the image from the existing connected Mesh Extender. This ensures efficient upgrade.
 - The newly joining Mesh Extender can obtain the image from Cisco.com, TFTP/SFTP server, or via CBD. Configure the **Transfer Type** accordingly to enable the new Mesh Extender obtain the image and join the CBW network. You can also upgrade software through HTTP. For details, refer to [Upgrading the Software for First Mesh Extender using HTTP, on page 89](#).

Upgrading the Software for First Mesh Extender using HTTP

You will be required to upgrade the software of first Mesh Extender that joins the CBW Primary AP. To add a new Mesh Extender to the Primary AP, refer to [Adding Mesh Extenders, on page 17](#).

Once you have added the Mac Address of the Mesh Extender in **Local Mac Addresses** list, check the predownload status of the Mesh Extender by navigating to **Network Summary > Management > Software Update** page.

If the Mesh Extender has not joined, the predownload status shows as `ImageReq to AP failed`. This requires that you upgrade the software of the Mesh Extender to enable it join the network. Do the following to upgrade the software using HTTP:

-
- Step 1** Obtain the ZIP file and extract the Primary AP software image and Mesh Extender firmware image.
- Step 2** From the Primary AP web interface, choose **Management > Software Update**. The **Software Update** window with the current software version number is displayed.
- Step 3** In the **Transfer Mode** drop-down list, choose **HTTP**.
- Step 4** Enable the **Mesh Extender Image** option to load the Mesh Extender image **ap1g5-capwap**. By default, this option will be **Disabled**.
- Step 5** Click **Browse** adjacent to the **Mesh Image File** field, navigate to the folder containing the unpacked ZIP file contents, and choose **ap1g5-capwap** software file.

Caution The top section of the page indicates the status of the image upload to Primary AP. Do not manually power down or reset the Primary AP or any AP during this process.

Note The uploaded **ap1g5-capwap** image will be stored in temporary location of the Primary AP. So do not upgrade or reload the Primary AP until the first Mesh Extender joins the network.

- Step 6** Click **Update**, and then click **Ok** in the confirmation dialog.
- Step 7** When the first Mesh Extenders attempts to joins the network, the Primary AP shares the **ap1g5-capwap** image to the Mesh Extender.

The **Pre-Download Image Status** section displays the status of the image download to the Mesh Extenders in the network.

Once the image is transferred, the Mesh Extender reloads and joins the CBW network.

Updating the Software using TFTP

Before you begin

- Prepare a TFTP server to host the CBW AP software file using the following guidelines:
 - Ensure that the TFTP server supports extended TFTP for file sizes greater than 32 MB. Some TFTP servers that support files of this size are tftpd32.
 - If you attempt to download the Primary AP software and your TFTP server does not support the file size, an error message is displayed: `TFTP failure while storing in flash`
- A computer that can access Cisco.com and the TFTP server will be required.



Note Ensure that the TFTP server has the latest software bundle on Cisco.com

- Step 1** Obtain the ZIP file and extract the Primary AP software image and Mesh Extender (if your network has any Mesh Extenders) firmware image. Copy the folder to the default directory on your TFTP server.
- Step 2** From the Primary AP UI, choose **Management > Software Update**.
The **Software Update** window with the current software version number is displayed.
- Step 3** In the **Transfer Mode** drop-down list, choose **TFTP**.
- Step 4** In the **IP Address (IPv4)** field, enter the IP address of the TFTP server.
- Step 5** In the **File Path** field, enter the TFTP server directory path of the software file.
- Step 6** To set the Primary AP to automatically reboot after the image pre-download is complete, check the **Auto Restart** check box. By default, this option is **Enabled**.
You can also manually reboot the Primary AP after the upgrade. Choose **Advanced > Primary AP Tools** and click **Restart Primary AP**.
- Step 7** Click **Save** to save the parameters that you have specified.
These parameters (IP address and File Path of the TFTP server) will remain saved unless you specifically change them in future. You do not have to re-enter these parameters during the next software update.
- Step 8** You can perform the update right away or schedule it for a later time.
- To proceed with the update right away, click **Update**, and then click **Ok** in the confirmation dialog.
 - To perform the update later, up to a maximum of 5 days from the current date, enable **Schedule Update** and specify the later date & time in the **Set Update Time** field.

The top section of the page indicates the status of the download. Do not manually power down or reset the Primary AP or any AP during this process.

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

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

- Step 9** After you click **Update**, one Primary capable AP and one Mesh Extender will obtain the image from the configured TFTP server and share the images to other Primary capable APs and Mesh Extenders correspondingly.
- Step 10** After the image pre-download is **Complete**, the Primary AP must restarts (or reboots) to complete the software upgrade. If you have not checked the **Auto Restart** check box, you can manually reboot the Primary AP, after the upgrade, by choosing **Advanced > Primary AP Tools**, and clicking **Restart Primary AP**.
- Step 11** Clear cache and log in to the Primary AP UI and verify the Primary AP software version in the **Software Update** window.

Updating the Software using SFTP

Software Update through SFTP Transfer Mode works for all Access Points supported in a CBW AP Deployment. You would need a SFTP server which can communicate with the Primary Access Point to use this upgrade method.

-
- Step 1** Obtain the ZIP file and extract the Primary AP software image and Mesh Extender (if your network has any Mesh Extenders) firmware image. Copy the folder to the default directory on your SFTP server.
- Step 2** From the Primary AP web interface, choose **Management > Software Update**.
The **Software Update** window with the current software version number is displayed.
- Step 3** In the **Transfer Mode** drop-down list, choose **SFTP**.
- Step 4** In the **IP Address (IPv4)/Name** field, enter the IP address or the domain name of the SFTP server.
- Step 5** In the **Port Number** field, enter the port number. The default is 22.
- Step 6** In the **File Path** field, enter the SFTP server directory path of the software file.
- Step 7** Enter the **username** and **password** to log in to the SFTP server.
- Step 8** To set the Primary AP to automatically reboot after the image pre-download is complete, check the **Auto Restart** check box. By default, this option is **Enabled**. You can also manually reboot the Primary AP, after the upgrade, by choosing **Advanced > Primary AP Tools**, and clicking **Restart Primary AP**.
- Step 9** Click **Save** to save the parameters (IP address, file path, port number, username and password) that you have specified. These parameters will remain saved unless you specifically change them in future. You do not have to re-enter these parameters for the next software update.
- Step 10** You can perform the update right away or schedule it for a later time.
- To proceed with the update right away, click **Update**, and then click **Ok** in the confirmation dialog.
 - To perform the update at a later time, up to a maximum of 5 days from the current date, click the **Schedule Update** and specify the later date & time in the **Set Update Time** field.

Note The top of the page indicates the status of the download. Do not manually power down or reset the Primary AP or any AP during this process.

The **Predownload Image Status** section of the page shows the status of image predownloaded to the APs in the network.

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

- Step 11** After you click **Update**, one Primary capable AP and one Mesh Extender will obtain the image from the configured SFTP server and share the images to other Primary capable APs and Mesh Extenders correspondingly.
- Step 12** After all the APs' state are moved to **Complete** state, the Primary AP restarts (or reboots) to complete the software upgrade. If you have not checked the **Auto Restart** check box, you can manually reboot the Primary AP, after the upgrade, by choosing **Advanced > Primary AP Tools**, and clicking **Restart Primary AP**.
- Step 13** Clear the cache and log in to the Primary AP. Verify the Primary AP software version in the **Software Update** window.

Updating the Software through Cisco.com

Before you begin

- Ensure that the Primary AP can access and reach Cisco.com.
- To check the accessibility, go to **Advanced > Primary AP Tools > Troubleshooting**. In the DNS servers, enter **Cisco.com** and click **Start**. If the access is successful, then a green tick mark is displayed indicating that the Primary AP can access *Cisco.com*

Step 1 From the Primary AP UI, choose **Management > SoftwareUpdate**. The **Software Update** window, with the current software version number is displayed.

Step 2 From the **Transfer Mode** drop-down list, choose **Cisco.com**.

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

By default, **Cisco.com** is set to **Transfer Mode**. The Primary AP runs the automatic check every 7 days to check for the latest software and recommends software versions that are available for download on *Cisco.com*. If a new version is available, then:

- The **Software Update Alert icon** at the top right corner of the UI will be Green in color (Grey, otherwise). Clicking the icon will lead you to the **Software Update** page.
- The **Update** button at the bottom of the **Software Update** page is enabled.
- The version information is displayed in the **Latest Software Release** and **Recommended Software Release** fields. You can view the release notes of displayed releases by clicking the "?" icon next to it. If the running software version is the latest, then these fields shows as **Up-to-date** and **Update** button will remain **Disabled**.
- The **Last Software Check** field displays the time stamp of the last automatic or manual software check.

Step 4 Click **Save**. This saves the entries or changes you have made in the **Software Update Transfer Mode**, and **Automatically Check For Updates** fields.

Step 5 Apart from the automatic check, you can also manually run a software check at any time by clicking **Check Now**.

Step 6 Enter the **Latest Software Release** and **Recommended Software Release** fields. Proceed with the software update, by clicking **Update**.

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

- **Release**—Specify if you want to update the recommended software release or the latest software release.

- **Update**—Specify a time for the APs to restart (or reload). You can opt to have it done right away or schedule it for a later time.

To set the Primary AP to automatically reboot after the image pre-download is complete, check the **Auto Restart** check box. By default, this option is **Enabled**.

- **Confirm**—Confirm your choices.

Follow the instructions in the wizard. You can revert to any tab at any given point of instance before you click **Confirm**.

Step 7 After you click **Confirm**, one Primary capable APs and one Mesh Extenders will obtain the image from *Cisco.com* server and share their images to all the Primary capable APs and Mesh Extenders correspondingly.

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

The **Predownload Image Status** section of the page displays the status of image pre-downloaded to the APs in the network.

Step 8 After all the APs' have moved to **complete** state, the Primary AP must restart (or reboot) to complete the software upgrade. If you have not checked the **Auto Restart** in Software Update Wizard, you can manually reboot the Primary AP, after the upgrade, by choosing **Advanced > Primary AP Tools**, and clicking **Restart Primary AP**.

Step 9 Clear the cache and log in to the Primary AP UI to verify the Primary AP software version in the **Software Update** window.

Updating the Software through Cisco Business Dashboard

When you add a Mesh Extender(S) to your Access Point network for the first time, you may choose to upgrade the firmware for the Mesh AP(s) through the Cisco Business Dashboard (CBD).

Updating the Software through Cisco Business Dashboard is possible, only if CBW is currently managed by CBD.

Before you start the image upgrade for the Mesh AP in Cisco Business Dashboard, configure the **Transfer Mode** in CBW interface.



- Note**
1. When the CBW is connected to CBD through direct management, then you can check the **Connection Status** in CBW GUI under **Advanced > CBD Settings** and confirm if the connection is up/down.
 2. If the CBW is managed by CBD Probe, then check the status of the device online/offline in CBD inventory using the device's serial number. Device serial number can be found in CBW GUI under **Monitoring > Access Points**. Click on the AP name to view the information.
-

Step 1 From the Primary AP UI, navigate to **Management > Software Update**.

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

Step 2 From the **Transfer Mode** drop-down list, choose **CBD-HTTPS** to update the software through CBD.

Step 3 Click **Save**.

- Step 4** Refer to *Performing Device Actions*, in the [Cisco Business Dashboard Administration Guide](#) and follow the instructions to update the software.
- Step 5** Click the **Predownload Image Status** arrows to display the status of the software update.
-



CHAPTER 7

Services

Cisco Business Wireless Access Points provides the following services:

- **Media Stream** – The Media Stream (formerly VideoStream) feature makes the IP multicast stream delivery reliable over the air, by converting the multicast frame to a unicast frame over the air. Each Media Stream client acknowledges receiving a video IP multicast stream.
- **mDNS** – Multicast Domain Name System (mDNS) service discovery provides a way to announce and discover the Apple services to the Wireless clients connected to the CBW AP.
- **Cisco Umbrella** – The Cisco Umbrella is a cloud-delivered network security solution. It provides real-time insights that help protect devices from malware and breach.

This chapter contains the following sections:

- [Media Steam, on page 95](#)
- [About Multicast Domain Name System, on page 98](#)
- [Cisco Umbrella Overview, on page 103](#)

Media Steam

The IEEE 802.11 wireless multicast delivery mechanism does not provide a reliable way to acknowledge lost or corrupted packets. As a result, if any multicast packet is lost in the air, it is not sent again which may lead to poor quality of IP multicast stream.

The Media Stream (formerly Video Stream) feature makes the IP multicast stream delivery to the wireless clients more reliable over the air and facilitates better usage of wireless bandwidth, by converting the multicast frame to a unicast frame over the air. Each Media Stream client acknowledges receiving a video IP multicast stream.

Configure Media Stream Parameters

Configure the global multicast parameters by the following steps:

1. Switch to **Expert View** by clicking the bidirectional arrow icon on the top right of the home screen in the Web UI of the Primary AP.
A message is displayed to confirm if you want to switch to the expert view.
2. Click **OK**.
3. Navigate to **Services >Media Stream**.

The **Media Stream** page will be displayed.

4. Enable **Global Multicast** to support multicast traffic on Primary AP. The default value is **Disabled**.



Note Global multicast cannot be enabled without configuring IPv4 multicast address in WLAN page.

5. Enable **Multicast Direct** to enhance the video streaming for wireless clients. The default value is **Disabled**.



Note Enabling the multicast direct feature does not automatically reset the existing client state. The wireless clients must re-join the multicast stream after enabling the multicast direct feature on the controller.

6. **IGMP Query Interval** - Configure the interval of how often querier sends IGMP host-query messages from an interface. By default, 20 seconds is set. The configurable range is 15-2400 secs.

This option is available only if both Global Multicast and Multicast Direct are enabled.

7. Select **Session Announcement State** toggle button to enable the session announcement mechanism. If the session announcement state is enabled, clients are informed each time a controller is not able to serve the multicast direct data to the client. The following parameters needs to be filled only if Session Announcement State is enabled.
 - a. **Session Announcement URL**— Enter the URL where the client can find more information when an error occurs during the multicast media stream transmission.
 - b. **Session Announcement E-mail**— Enter the e-mail address of the person who can be contacted.
 - c. **Session Announcement Phone**— Enter the phone number of the person who can be contacted.
 - d. **Session Announcement Note**— Enter a reason as to why a particular client cannot be served with a multicast media.

8. Click **Apply**.

Configuring a New Media Stream

To add a new Media stream switch to **Expert View** and navigate to **Services>Media Stream**.

1. Click **Add New Stream** to configure a new media stream. The **Add New Media Stream** page is displayed.
2. Enter the media stream name in the **Stream Name** text box. The stream name can be up to 64 characters.
3. Enter the starting IPv4 address of the multicast media stream in the **Multicast Start IP Address** text box.
4. Enter the ending IPv4 address of the multicast media stream in the **Multicast End IP Address** text box.
5. Enter the maximum expected bandwidth that you want to assign to the media stream into the **Maximum Expected Bandwidth (Kbps)** text box. The range is 1 to 35000 kbps.



Note We recommend that you use a template to add a media stream to the Primary AP.

6. From the **Select from Predefined Templates** drop-down list under **Resource Reservation Control (RRC) Parameters**, choose one of the following options to specify the details about the resource reservation control:

- Very Coarse (below 300 kbps)
- Coarse (below 500 kbps)
- Ordinary (below 750 kbps)
- Low (below 1 Mbps)
- Medium (below 3 Mbps)
- High (below 5 Mbps)



Note When you select a predefined template from the drop-down list, the following text boxes under the **Resource Reservation Control (RRC) Parameters** list their default values that are assigned with the template.

7. Specify the average packet size in the **Average Packet Size** field. The value can be in the range of 100 to 1500 bytes. The default value is 1200.
8. Enable the RRC (Resource Reservation Control Check) Periodic update in the **RRC Periodic update** field. By default, this option is enabled.
- RRC periodically updates the admission decision on the admitted stream according to the correct channel load. As a result, it may deny certain low priority admitted stream requests.
9. Specify the priority bit set in the media stream in the **RRC Priority** field. The priority can be any number between 1 and 8.
- The larger the value means the priority is higher. For example, a priority of 1 is the lowest value and a value of 8 is the highest value. The default priority is 4. The low priority stream may be denied in the RRC periodic update.
10. Specify the action to perform in case of a violation after a re-RRC in the **Traffic Profile Violation** field. Choose an action from the drop-down list. The possible values are as follows:
- **Best Effort**— Specifies that a stream is set to Best Effort class on periodic reevaluation. This is the default value.
 - **Drop**— Specifies that a stream is dropped on periodic reevaluation.
11. Click **Apply**.
- The newly created Media stream is displayed in the table along with details of Stream Name, Start and End IP Address, and Operation Status.

Viewing Media Stream Clients

Media stream clients will be displayed under this section with the following details:

- **Client MAC**—Displays the MAC address of the client.
- **Stream Name**—Shows the Media stream name. The Stream Name will be Null for clients that are connected to WLAN with the **Multicast Direct** toggle disabled.
- **Multicast IP**—Displays the Multicast Group Address configured in the WLAN page.
- **AP Name**—Displays the AP Name connected to the client.
- **VLAN**—Displays the Client VLAN.
- **Type**—Displays **Multicast Only** or **Multicast Direct** based on the **Multicast Direct** toggle configured in the WLAN.

About Multicast Domain Name System

Multicast Domain Name System (mDNS)

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

Bonjour Advertisements for CBW device discovery

CBW AP sends Bonjour Advertisements to the local network to support CBW device discovery in CBD probe. Using these advertisements, CBD probe obtains details of individual AP and the Primary AP.



Note During the initial setup phase, if there is more than one primary capable AP in the network, only one AP will get DHCP IP, and sends VRRP and Bonjour Advertisements. The rest of the APs will wait for the AP to be configured and then join the Primary AP.

Location Specific Services

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

LSS applies only to wireless service provider entries. There is no location awareness for wired service provider devices. The status of LSS cannot be enabled for services with the ORIGIN set to wired and vice versa.

mDNS Policy

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

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

mDNS policies can be framed based on:

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

mDNS Policy Limitations

The limitations of the mDNS policy are as follows:

- LSS cannot be applied in conjunction with the mDNS policy.
- If the keyword **Any** is used as a role parameter value, then that check is bypassed.
- mDNS Policy will be active only when mDNS Snooping is enabled.
- The maximum number of policies that can be configured per MAC address is limited to five policies.

Client Attributes in an mDNS Policy

Any client initiating an mDNS query is associated with a set of attributes that describe the context of the client. The list of attributes can be based on Role, User-Id, associated AP Name, associated AP Location, and associated AP Group.

mDNS AP

The mDNS AP feature allows the Primary AP to have visibility of the wired service providers. This is in-built in the Primary AP.

Priority MAC Support

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

Origin-Based Service Discovery

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

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

Restrictions for Configuring Multicast DNS

- mDNS is not supported on access points in **AP Only** mode within a locally switched WLAN and mesh access points.
- mDNS is not supported on remote LANs.
- Third-party mDNS servers or applications are not supported on the Primary AP using the mDNS feature. Devices that are advertised by the third-party servers or applications are not populated on the mDNS service or device table correctly on the Primary AP.
- In a Layer2 network, if Apple servers and clients are in the same subnet, mDNS snooping is not required on the Primary AP. However, this relies on the function of switching network. If you use switches that do not work as expected with mDNS snooping, you must enable mDNS on the Primary AP.
- Video is not supported on Apple iOS 6 with WMM in enabled state.
- mDNS APs cannot duplicate the same traffic for the same service or VLAN.
- LSS filtering is restricted to only wireless services.
- The mDNS AP, Priority MAC address, and origin-based discovery features cannot be configured using the Primary AP web-UI.
- mDNS user profile mobility is not supported in guest anchors.
- Apple devices such as iPads and iPhones can discover Apple TV through Bluetooth. This might result in Apple TVs being visible to end users.

Configuring Multicast DNS

Configure the global mDNS parameters and the Primary Services Database by following these steps:

-
- Step 1** Switch to **Expert View** by clicking the bidirectional arrow icon on the top right of the home screen in the Web-UI of the Primary AP. A message is displayed to confirm if you want to switch to the expert view. Click **Ok**.
 - Step 2** Choose **Services > mDNS**.
 - Step 3** Use the **mDNS Global Snooping** toggle button to enable or disable snooping of mDNS packets, respectively.
 - Step 4** Use **Bonjour Advertisements** toggle button to enable or disable sending of Bonjour advertisement packets to the local network. By default it is **enabled** and advertisements will be sent every minute.

- Note**
- By enabling this option, CBD probe can discover CBW APs in the network.
 - CBW AP sends Bonjour packets only in Native VLAN.
 - CBW AP sends **Goodbye Bonjour** message to CBD probe
 - If the **Bonjour Advertisements** toggle button is disabled.
 - If the name of the AP joined to Primary AP is changed, or the Primary AP name is changed, a **Goodbye Bonjour** message is sent for the old name. A new name will be updated in Bonjour Advertisements at the next interval. A **Goodbye Bonjour** message on AP name change will be sent only if the **Bonjour Advertisement** is enabled.

Step 5 Use the **mDNS Policy** toggle button to enable or disable mDNS policy mapping.

Step 6 Enter the mDNS query interval in minutes. The query interval is the frequency at which the Primary AP queries for a service. Default is 15 minutes.

Step 7 Click **Add VLAN Id** to add a list of VLANs for internal AP snooping.

Step 8 Complete the details in the following tabs:

- Primary Services Database** —To view the services listed in the Primary database. The Primary AP looks and learns about the mDNS service advertisements only if the service is available in the Primary Services Database. The Primary AP can check and learn a maximum of 64 services.
 - Click the **Add Service** button to add a new service in the Primary database.
 - In the **Add/Edit mDNS Service** window, specify the **Service Name**, **Service String**, **Query Status**, **Location Services**, and **Origin**.
 - Click **Update**.
- mDNS Profiles** —To view the list of mDNS profiles. By default, one mDNS profile will be available.
 - Click the **Add Profile** button to add a new profile.
 - In the **Add/Edit mDNS profile** window, enter the profile name that can be later mapped to the WLAN.
- mDNS policy**—To view the mDNS policies. By default, one mDNS policy will be available.
 - Click **Add mDNS policy** to add a new policy.
 - In the **Edit mDNS policy** window, enter the role name and user name.
- Domain Names** —To view domain names and add domain names from the discovered list.
- mDNS Browser** —To view the number of mDNS services running.
- Click **Apply**.

Mapping mDNS Profile to WLAN

Switch to **Expert View** by clicking the bidirectional arrow icon on the top right of the home screen in the Web-UI of Primary AP.

-
- Step 1** Choose **Wireless Settings > WLANs**.
- Step 2** Click **Add new WLAN/RLAN** to create a new WLAN.
- Step 3** In the **Add new WLAN/RLAN** window, select **Advanced** to configure the mDNS.
- Step 4** Use the **mDNS** toggle button to add the mDNS services to the WLAN.
- Step 5** From the **mDNS Profile** drop-down list, choose a profile to map the required policy to the WLAN.
- Step 6** Click **Apply** to save your changes.
- Note** The wireless Primary AP broadcasts the services from the wired devices such as Apple TVs learned over VLANs, when:
- mDNS snooping is enabled in the WLAN Advanced options.
 - mDNS profile is enabled either at the interface or WLAN.
-

Configuring mDNS Policy

Switch to **Expert View** by clicking the bidirectional arrow icon on the top right of the home screen in the Web-UI of the Primary AP. A message is displayed to confirm if you want to switch to the expert view. Click **Ok**.

To configure the mDNS policy, do the following:

- Step 1** Choose **Services > mDNS**.
- Step 2** Use the **mDNS Global Snooping** toggle button to enable or disable snooping of mDNS packets, respectively.
- Step 3** Use the **mDNS Policy** toggle button to enable or disable mDNS policy, respectively.
- Step 4** Enter the mDNS query interval in minutes. The query interval is the frequency at which the Primary AP queries for a service. Default is 15 minutes.
- Step 5** Click **mDNS Policy**. The number of mDNS policies are displayed.
- Step 6** In the **Add mDNS Policy** window, you must add the mDNS Service Group
- a. Enter the **mDNS Service Group Name** and the **Description**.
 - b. Click the **Add Service Instance** button. The Add Service Instance window is displayed. Complete the following details to add a service instance:
 - **Mac Address**—MAC address of the service provider such as Apple TV.
 - **Name**—Add a name for the device.
 - **Location Type**—Choose the Location Type by AP Group, AP Name, or AP Location.
 - **Location**—Based on the Location Type selected.
 - c. Click **Apply**.

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

Step 7 Enter the **Policy/Rule** and click **Apply**.

Cisco Umbrella Overview

Cisco Umbrella is a cloud based security platform that provides the first line of defense against threats on the internet wherever users go. It acts as a gateway between the internet and your systems and data to block malware, botnets and phishing over any port, protocol or app.

At the Domain Name System (DNS) level, it provides real-time insights that help protect devices from malware and breach.

The following points summarizes the way in which Cisco Umbrella works in the Primary AP:

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

Cisco Umbrella Support for the Primary AP

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

Limitations

This feature does not work with the following:

- Local-auth
- IPv6 addresses
- If an application or host uses an IP address directly, instead of using DNS to query domain names.
- If a client is connected to a web proxy and does not send a DNS query to resolve the server address.
- The application of wireless Cisco Umbrella profiles on wireless entities, like WLAN, through configuration, is dependent on the success of the registration of the device.
- The Cisco Umbrella Cloud provides two IPv4 addresses. The AP uses the first server address that is configured. It does not load balance across servers.

Configuring Cisco Umbrella on Primary AP

To configure Cisco Umbrella on the Primary AP, ensure the following:

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

To generate the API token, do the following:

1. Login into your Cisco Umbrella Account
2. In the Umbrella dashboard, navigate to **Admin > API Keys** and click **Create**.
3. Select **Legacy Network Devices** and click **Create**.
4. Expand **Legacy Network Devices** and copy the API token **Your Key**. The API token is a lengthy string of alphanumeric characters.

To configure Cisco Umbrella on the Primary AP, do the following:

-
- Step 1** Switch to **Expert View** by clicking the bidirectional arrow icon on the top right of the home screen in the Web-UI of the Primary AP.
A message is displayed to confirm if you want to switch to the expert view. Click **Ok**.
- Step 2** Choose **Services > Umbrella**.
- Step 3** Click the **Umbrella Global Status** toggle button to enable Umbrella status.
- Step 4** Enter or paste the **Umbrella API Token** that you copied.
- Step 5** Click **Apply** to enable Cisco Umbrella.
- Step 6** Click **Add Profile** to create a new profile.
- Step 7** In the **Add Profile** window, enter the **Profile Name** and click **Apply**.
A new profile is created.
- Step 8** Verify that the State changes from *Registration in Progress* to *Profile Registered*. This may take a few seconds, and may require you to refresh your browser window.
- Step 9** In the Umbrella dashboard, navigate to **Deployments > Core Identities > Network Devices**. You can check if your device is listed in this window.
-

Adding Policy to Umbrella Profile

-
- Step 1** Browse to the Cisco Umbrella UI using your Cisco credentials. Add your device details to protect from breach and malware.
- Step 2** Navigate to **Policies > All Policies** to create rules and map this to your network device.
- Step 3** Click **Add** to create new rules.
- Step 4** Select **Network Devices** from the list of Identities and click **Next**. This helps to add your APs such that the whole network is monitored by the umbrella.

- Step 5** You can configure the required **Security Settings and Limit Content Access**. These are user configurable and you can select the type of attacks that you want to block such as phishing attack, malware, potentially harmful domains, web page contents such as games, gambling, drugs etc.
- Step 6** In the **Application** tab, select the applications that need to be blocked. You can limit access to certain applications like youtube, facebook, google-services etc., if you wish.
- Step 7** Specify the **Destination**, **File Analysis** and **Block Pages** in the network.
- Destination List** shows the global allowable list and global block list that you configure in the umbrella and **Block pages** define the appearance and bypass options for your block pages.
- These all are user configurable.
- Step 8** You may now go to **Deployments > Core Identities > Network Devices** and verify if the Policy has been applied to your network device.
-

Applying Cisco Umbrella Profile to WLAN

- Step 1** Switch to **Expert View** by clicking the bidirectional arrow icon on the top right of the home screen in the Web-UI of the Primary AP.
- Step 2** Choose **Wireless Settings > WLANs**.
- Step 3** Click **Add new WLAN/RLAN**. The Add new WLAN/RLAN window is displayed.
- Step 4** In the **Add new WLAN** window, select **Advanced**.
- Step 5** From the **Umbrella Profile** drop-down list, choose a profile that was created for the WLAN.
- Step 6** From the **Umbrella Mode** drop-down list, choose either **Ignore** or **Forced**.
- When a client obtains DNS IPs, users can manually change them on the client device, thus bypassing Umbrella policy enforcement. To prevent this security compromise, configure Umbrella Mode to Forced. This ensures that Umbrella policy enforcement cannot be overridden on the client device.
- Step 7** Optionally, use the **Umbrella DHCP Override** toggle button to enable the Cisco Umbrella DHCP override.
- The DNS IP addresses that a client obtains when connecting to the SSID are configured on the DHCP server. For Umbrella enforcement to work, clients must send out DNS requests to Umbrella IP addresses (208.67.222.222, 208.67.220.220). **Umbrella DHCP Override** ignores the DNS IPs configured via DHCP and forces the Umbrella DNS IPs on the client device. If you set Umbrella Mode to **Forced**, you do not need to enable **Umbrella DHCP Override**.
- Step 8** Click **Apply** and **Save** your configuration.
-



CHAPTER 8

Advanced

This chapter contains the following sections:

- [Managing SNMP, on page 107](#)
- [Setting Up System Message Logs, on page 110](#)
- [System Logs, on page 111](#)
- [Optimizing RF Parameters, on page 111](#)
- [Troubleshooting in Primary AP, on page 116](#)
- [Using Primary AP Tools, on page 116](#)
- [Saving the Primary AP Configuration, on page 118](#)
- [Troubleshooting Files, on page 118](#)
- [Configuring Access Control Lists \(ACL\), on page 122](#)
- [Cisco Business Dashboard Settings, on page 124](#)

Managing SNMP

Simple Network Management Protocol (SNMP) is a popular network management protocol used for collecting information from all the devices in the network and configuring and managing these devices. You can configure both SNMPv2c and SNMPv3 access modes using the Primary AP web interface.

Configuring SNMP Access

You can configure the following SNMP access modes for the Primary AP:

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

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

Step 2 In the SNMP window, enable **SNMP service** option for querying the configuration using MIB browser. By default, the SNMP service is **disabled**.

Step 3 Select the appropriate check box next to the **SNMP Access** to enable the desired SNMP mode. The SNMP access mode is **disabled** by default.

The selected SNMP access mode is enabled.

Note For information about configuring SNMPv3 users using CBW AP, see topics on SNMPv3 later in this chapter.

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

Step 5 In the **Read-Write Community** field, enter the desired community name.

Step 6 Click **Apply** to save the SNMP access configurations.

Note A community name should be between 8-32 characters and be a combination of lowercase letters, uppercase letters, digits, and special characters.

SNMP Trap Receivers

A Simple Network Management Protocol (SNMP) Trap receiver captures, displays and logs SNMP Traps. Traps are notices of events that are sent immediately to the SNMP client's trap receiver from Primary AP instead of waiting for a poll – a request – to the device by the SNMP client.

To add a SNMP Trap Receiver, do the following:

Step 1 Click **Add New SNMP Trap Receiver**, under **Advanced > SNMP**.

Step 2 In the **Add SNMP Trap Receiver** window, configure the following fields:

- a) **Receiver Name**—Enter the desired username for the new Trap Receiver.
- b) **IP Address**—Specify the IP address of the Trap Receiver to which you wish to connect.
- c) **Status**—Enable/Disable the Trap Receiver. By default, it is **enabled**.
- d) **SNMPv3**—If you have configured SNMP v3 access and have SNMPv3 User, then enable this option. By default, it is **disabled**.
- e) **SNMPv3 User**—Map the SNMPv3 User details for the Trap receiver entry, if SNMPv3 toggle is enabled.

The **SNMP Trap Receiver** table shows the list of SNMP Trap Receivers configured in the network.

Step 3 Click **Apply**.

To Edit/Delete the SNMP Trap Receivers, click the **Edit/Delete** icon in the row containing the SNMP Trap Receiver whose details you wish to modify or delete.

The **SNMP Trap Receivers** table is refreshed and the updated entry appears in the table.

Note Few traps are enabled by default. For a complete list of available traps, refer to [SNMP Traps in CBW AP, on page 135](#).

Add an SNMPv3 User

- Step 1** Choose **Advanced > SNMP**.
- Step 2** In the **SNMP** window, under the **SNMP v3 Users** section, click the **Add New SNMP v3 User** button.
- Step 3** In the **Add SNMP v3 User** window, enter the following details:

Field	Description
User Name	Enter the desired username for the new SNMPv3 user.
Access Mode	From the drop-down list, choose one of the desired modes: Read Only or Read/Write . The default is Read Only .
Authentication protocol	From the Authentication Protocol drop-down list, choose one of the options: HMAC-MD5 , HMAC-SHA , or None . The default authentication protocol is HMAC-SHA .
Authentication Password	Enter the desired authentication password. Use a minimum password length of 12 -31 characters.
Confirm Authentication Password	Confirm the authentication password specified above. You can select the Show Password checkbox to display the entries in the Authentication Password and the Confirm Authentication Password fields and verify if the characters match.
Privacy Protocol	From the drop-down list, select one of the options: CBC-DES , CFB-AES-128 , or None . The default privacy protocol is CFB-AES-128 .
Privacy Password	Enter the desired privacy password. Use a minimum password length of 12 -31 characters.
Confirm Privacy Password	Confirm the privacy password specified above. You can select the Show Password checkbox to display the entries in the Privacy Password and the Confirm Privacy Password fields and verify if the characters match.

- Step 4** Click **Apply** to create a new SNMPv3 user.
- The newly added SNMP v3 User appears in the **SNMP v3 Users** table on the **SNMP** window. You can add up to a maximum of 7 SNMPv3 users.

Delete SNMPv3 User

- Step 1** Choose **Advanced > SNMP**.
- Step 2** In the **SNMP Setup**, click the **X** icon in the row containing the SNMPv3 user you wish to delete.
- A warning message appears to confirm the action.

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

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

Setting Up System Message Logs

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

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

Before you begin

Set up a Syslog server in your network before you start the following procedure.

Step 1 Choose **Advanced > Logging**.

The **Logging** window appears.

Step 2 Click **Add Server** to add a new **Syslog Server**.

The System Message Log feature is enabled.

Step 3 In the **Syslog Server IP** field, enter the IPv4 address of the server to which the syslog messages are sent and click **Apply**. The table displays the list of Syslog server configured in the network. You can choose to delete the Syslog server if you wish.

Step 4 Set the severity level for filtering the syslog messages that are sent to the syslog server. From the **Log Syslog Level** drop-down list, you may choose the severity level. It can be one of the following (given in the order of severity):

- **Emergencies (0) (Highest severity)**
- **Alerts (1)**
- **Critical (2)**
- **Errors (3)**
- **Warnings (4)**
- **Notifications (5) (Default)**
- **Informational (6)**
- **Debugging (7) (Lowest severity)**

Messages with a severity equal to or less than the set level are sent to the syslog server.

Step 5 Click **Apply**.

System Logs

This feature is used to analyze the system logs depending upon the log level that the user sets. To view the logs in Primary AP UI, do the following configurations.

-
- Step 1** Navigate to **Advanced > Logging**. The Logging window is displayed.
- Step 2** From the **Log Buffer level** drop-down list, choose the required log level for the system logs to be redirected to the logging buffer.
- Step 3** The System logs will be displayed in the **Logs** section of the same page.
- Note** The wireless client events such as Assoc, Auth, Success or failure logs will be logged in the Notification level (5)
- Step 4** Click **Clear** to clear the logs displayed in the Primary AP UI.
-

Optimizing RF Parameters

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

-
- Step 1** Navigate to **Advanced > RF Optimization**.
- Step 2** **Enable** the **RF Optimization** option to enhance your Wi-Fi performance by adjusting the APs' radio parameters. By default, **Medium client density** based RF settings is applied.
- Step 3** Select the **Client Density** by moving the slider and choose the **Traffic Type**.
To know the values that are set when low, typical, or high client density type is selected, see [RF Parameter Optimization Settings, on page 114](#).
- Step 4** Click **Apply** to save the changes.
-

Advanced RF Parameters

In addition to changing the client density and traffic type, you can also use the advanced parameters to maximize your network's Wi-Fi performance. The following sections in this chapter, provides details for the same.

Optimized Roaming

Optimized roaming resolves the problem of sticky clients that remain associated to access points that are far away and outbound clients that attempt to connect to a Wi-Fi network without having a stable connection. Optimized roaming allows clients to disassociate based on the RSSI of the client data packets and data rate.

The client is disassociated if the RSSI alarm condition is met and the current data rate of the client is lower than the optimized roaming data rate threshold.

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

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

Optimized Roaming is useful in the following scenarios:

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

Restrictions for Optimized Roaming

When BSS transition is sent to 802.11v capable clients before the disconnect timer expires, the client is disconnected forcefully. BSS transition is enabled by default for 802.11v capable clients.

Configuring Optimized Roaming

Before you begin

- Ensure you have switched to **Expert View** to be able to configure optimized roaming via Primary AP UI.

-
- Step 1** Choose **Advanced > RF Optimization**. The **RF Optimization** page allows you to configure Optimized Roaming parameters, Data Rates, Channels, Global Interferer detection.
- Step 2** In the **RF Optimization** page, enable the **2.4 GHz/5 GHz Optimized Roaming** toggle button to set interval and threshold values.
- If **2.4 GHz/5 GHz Optimized Roaming** is enabled, the following parameters are displayed.
- 2.4 GHz/ 5 GHz Interval
 - 2.4 GHz/ 5 GHz Threshold
- Step 3** In the **2.4 GHz Interval** and **5.0 GHz Interval** text boxes, specify the values for the interval at which an access point reports the client coverage statistics to the Primary AP.
- **2.4 GHz/5 GHz Interval**—Configures the client coverage reporting interval for 2.4 GHz and 5 GHz networks. The interval ranges from 5 seconds to 90 seconds (default). If you configure a low reporting interval, the network can get overloaded with coverage report messages. The client coverage statistics includes data packet RSSIs, Coverage Hole Detection and Mitigation (CHDM) pre-alarm failures, retransmission requests, and current data rates.
- Note**
- By default, the AP sends client statistics to the Primary AP every 90 seconds.
 - If the Interval is set to a value other than the 90 second default, the client statistics will be sent only during failure cases.

- **2.4 GHz / 5 GHz Threshold**—Configures the threshold data rates for 2.4 GHz and 5 GHz. The Threshold values are **disabled** by default.

For 2.4 GHz threshold value that can be configured are 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps.

Optimized roaming disassociates clients based on the RSSI of the client data packet and data rate. The client is disassociated if the current data rate of the client is lower than the Optimized Roaming Data Rate Threshold. For 5 GHz threshold value that can be configured are 6, 9, 12, 18, 24, 36, 48, 54 Mbps.

- **Event Driven RRM**—The toggle allows an AP in distress to bypass normal RRM intervals and immediately change channels. This is a global setting and can be enabled or disabled.
- **Interferer detection**—This is global setting which enables the Primary AP to detect the non Wi-Fi sources. By default, it is disabled.
- **5.0 GHz Channel Width**—The dropdown option basically controls how broad the signal is for transferring data as 20MHz/40MHz/80MHz/Best. By increasing the channel width, we can increase the speed and throughput of a wireless broadcast. This Global setting is set to **Best** by default.

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

The following data rates are available:

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

Step 5 Select DCA Channels—One can select or click individual channels to be included in DCA for 2.4 GHz and 5.0 GHz band.

Note A green underline below the channel number indicates that it is selected. Click to unselect the same.

RF Profiles

RF Profiles allows you to tune groups of APs that share a common coverage zone together and selectively change how RRM will operate the APs within that coverage zone. For example, a university might deploy a high density of APs in an area where a high number of users will congregate or meet. This situation requires that you manipulate both data rates and power to address the cell density while managing the co-channel interference. In adjacent areas, normal coverage is provided and such manipulation would result in a loss of coverage. Using RF profiles and AP groups allows you to optimize the RF settings for AP groups that operate in different environments or coverage zones. RF profiles are created for the 802.11 radios. RF profiles are applied to all APs that belong to an AP group, where all APs in that group will have the same profile settings. The RF profile gives you the control over the data rates and power (TPC) values. One can either associate a built in RF Profile with AP Groups or create a new RF Profile and then associate that with the AP Group.

To configure this, do the following:

Step 1 Switch to Expert View in the CBW Web-UI by clicking the bi-directional arrows toggle button on the top-right.

Step 2 Navigate to **Advanced > RF Profiles**.

Step 3 Click **Add New RF Profile**.

Step 4 Under the **General** tab, configure the following:

- a) **RF Profile Name**—Provide a RF Profile name.
- b) **RF Profile description**—Provide an one-line reference for it.
- c) **Band**—Select the band 2.4GHz or 5 GHz.
- d) **Maximum Clients per radio**—Select the maximum clients per radio. By default, it is 200. The maximum value that is configurable is 200.
- e) **Rx SOP Threshold**—Receiver Start of Packet Detection Threshold (RxSOP) determines the Wi-Fi signal level in dBm at which an access point's radio demodulates and decodes a packet. The default value is **Auto**.

As the Wi-Fi level increases, the radio sensitivity decreases and the receiver cell size becomes smaller. Reduction of the cell size affects the distribution of clients in the network. RxSOP is used to address clients with weak RF links, sticky clients, and client load balancing across access points. RxSOP helps to optimize the network performance at high-density deployments (i.e larger number of clients) where access points need to optimize the nearest and strongest clients.

- f) **Multicast data rate**—Use the Data rates option to specify the rate at which the multicast traffic can be transmitted between the access points and the client. The default value is **Auto**.

Step 5 In the **802.11** tab, set the data rates and MCS for the RF profile.

- a) **Data Rates**—Use the Data rates option to specify the rate at which the data can be transmitted between the access points and the client. The default rate is 11 Mbps.
- b) **MCS Settings**—The MCS settings determine the number of spatial streams, the modulation, the coding rate, and the data rate values that are used. Ensure that all of the 0 to 31 MCS data rate indices are enabled (which is the default setting).

Step 6 In the **RRM** tab, set the following parameters:

- a) **Channel Width**—By default, 20 MHz and cannot be changed.
- b) **Select DCA Channels**—The DCA dynamically manages channel assignment for an AP group. It also evaluates the assignments on a per AP radio basis. The DCA makes decisions during an RSSI based cost metric function which evaluates performance based on interference for each available channel.

It dynamically adjusts the channel plan to maintain performance of individual radios.

Step 7 In the **Client Distribution** tab, set the following parameters:

- a) **Window**—In the Window size text box, enter a value between 0 and 20. The default size is 5. The window size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

The access point with the lowest number of clients has the lightest load. The window size and the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.

- b) **Denial**—In the Denial Count text box, enter a value between 1 and 10. The denial count sets the maximum number of association denials during load balancing. The default size is 3.

Step 8 Click **Apply**.

RF Parameter Optimization Settings

Use this feature to select the appropriate RF Parameter Optimization settings for your deployment. The following table shows the default values when low, typical, or high client density type is selected.



Note If you do not enable RF Parameter Optimization during the initial configuration wizard, then client density is set to **Typical** (the default value), and RF traffic type is set to **Data** (the default value).

TPC (Tx Power Control) algorithm to determine whether the power of an AP needs to be adjusted down. Reducing the power of an AP helps mitigate co-channel interference with another AP on same channel in close proximity.

Table 7: RF Optimization Table

Parameter	Dependency	Typical (Default Profile)	High Density (Where throughput is most important)	Low Density (For coverage in open spaces)
TX Power	Global per band	Default	Higher	Highest
TPC Threshold, TPC Min, and TPC max (These parameters are equivalent to TX Power)	Specific RF profile per band	TPC Threshold: <ul style="list-style-type: none"> • -70 dBm for 5 GHz • -70 dBm for 2.4 GHz TPC Min: Default at -10dBm TPC Max: Default at 30 dBm	TPC Threshold: <ul style="list-style-type: none"> • -65 dB for 5GHz • -70 dB for 2.4 GHz TPC Min: +7 dBm for 2.4 GHz and -10 dBm for 5GHz. TPC Max: Default at 30 dB	TPC Threshold: <ul style="list-style-type: none"> • -60 dBm for 5GHz • -65 dBm for 2.4 GHz TPC Min: -10 dBm TPC Max: Default at 30 dBm
RX Sensitivity	Global per band (Advanced RX-SOP) RF profiles	Default (Automatic)	Medium (RX-SOP)	Low
CCA Threshold	Global per band 802.11a only (hidden) RF Profiles	Default (0)	Default (0)	Default (0)
Coverage RSSI Threshold	Global per band Data and Voice RSSI RF Profiles	Default (Data: -80dBm, Voice: -80dBm)	Default (Data: -80dBm, Voice: -80dBm)	Default (Data: -90dBm, Voice: -80dBm)
Coverage Client Count	Global per band (Coverage Exception) RF Profiles (Coverage Hole Detection)	Default (3 clients)	Default (3 clients)	Lower (2 clients)

Parameter	Dependency	Typical (Default Profile)	High Density (Where throughput is most important)	Low Density (For coverage in open spaces)
Data Rates	Global per band (network) RF Profiles	12 Mbp mandatory 9Mbp supported 1, 2, 5.5, 6, 11 Mbp disabled	12 Mbp mandatory 9Mbp supported 1, 2, 5.5, 6, 11 Mbp disabled	CCK rates enabled 1, 2, 5.5, 6, 9, 11, 12 Mbp enabled

Troubleshooting in Primary AP

To troubleshoot in the Primary AP, there are features that allow you to check the connectivity, internet access, radio admin state and to analyze the logs depending upon the log level setting. The following sections describe these features.

UI Indicator

Once you login into the Primary AP GUI, navigate to **Monitoring > Network Summary**. Check the following indicators:

- **LAN Indicator**—Checks if the default gateway IP of management interface is reachable.
- **Internet Indicator**—Checks if the public DNS (8.8.8.8) is reachable.
- **Wireless Indicator**—Checks the wireless connectivity by looping through all the APs present in Primary AP for both the global networks provided both networks (A and B) are enabled. If any of the network is down in any of the APs, the wireless status is considered to be down. Otherwise, the wireless indicator is operational

Using Primary AP Tools



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

You use the **Primary AP Tools** page to manage the following operations:

Restarting the Primary AP

You can reboot (or restart) the Primary AP. Navigate to **Advanced > Primary AP Tools**, and then click **Restart Primary AP**.

Clearing the Primary AP Configuration and Resetting to Factory Defaults

This procedure resets your Primary AP to its factory-default configuration.

Step 1 Choose **Advanced > Primary AP Tools**.

Step 2 In the **Primary AP Tools** page, click **Factory Default Primary AP**.

This erases the current Primary AP configuration, resets the configuration to the factory-default values, and reboots the Primary AP.

What to do next

After the Primary AP reboots, proceed to [Launching the Setup Wizard, on page 12](#).

Clearing Configurations for all APs and Resetting to Factory Defaults

This procedure resets all the CBW APs (including Primary AP) to factory-default configuration.

Step 1 Choose **Advanced > Primary AP Tools**.

Step 2 In the **Primary AP Tools** page, click **Factory Default All APs**.

This erases the current configuration in all the APs simultaneously, resets the configuration to the factory-default values, and reboots all the APs.

Note Primary AP will be rebooted at last.

What to do next

After the Primary AP reboots, proceed to [Launching the Setup Wizard, on page 12](#).

Export and Import Primary AP Configuration

Exporting / Saving Primary AP Configuration

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

To export the current configuration, choose **Advanced > Primary AP Tools**, and then under **Configuration management**, click **Export Configuration**. Set the direction as **download** and Transfer Mode as **HTTP**.

The configuration file is saved on the device in which the Primary UI is being viewed. By default the file is saved as *config.txt* in your downloads folder.

Importing / Restoring Primary AP Configuration

You can import configuration from a previously saved configuration file, which is in .TXT file format. Choose **Advanced > Primary AP Tools**. Under **Configuration management**, select direction as **Upload**, and choose the **Transfer mode** as HTTP/TFTP/SFTP/FTP.

If HTTP is selected as Transfer mode, then browse the file and click **Apply**.

If FTP/SFTP/TFTP is selected as Transfer mode, configure the IP address, File path, File name, and other mandatory parameters and click **Apply**.



Note You can also do regular import of configuration file, by selecting FTP/SFTP/TFTP transfer mode and by enabling **Scheduled Update** and configuring the Frequency, Time, window.

By default, the option is **disabled**.

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

For more information about the Primary AP Election Process, see [Primary AP Failover and Election Process, on page 131](#).

Saving the Primary AP Configuration

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

You can save the Primary AP's configuration from the RAM to the NVRAM of the Primary AP. This ensures that in the event of a reboot, the Primary AP can restart with the last saved configuration.

To save the Primary AP's current configuration from the RAM to the NVRAM, click **Save Configuration** at the top-right of the Primary AP web interface, and then click **Ok**.

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

Troubleshooting Files

This section helps you to download the Support Bundle which includes configuration, logs and crash files for trouble shooting.



Note The Pop-up blocker should be disabled in Browser settings to upload or download the configuration file.

Click **Download Support Bundle** for downloading support bundle to local machine.

The support bundle can also be downloaded via FTP Server if configured. Specify the **IP address**, **File path**, **Username**, **password**, **server port** and select **Apply settings and Export**.

Cisco Business Wireless will attempt to export troubleshooting files as soon as they are generated. If export of troubleshooting files to FTP server is successful, the files are deleted from Cisco Business Wireless.

Troubleshooting Tools

The following tools can be used for troubleshooting:

SSHv2 Access

1. Switch to the Expert View, if you are currently in the Standard View.
2. Enable Secure Shell Version 2 (SSHv2) access mode for Primary AP console, that uses data encryption and a secure channel for data transfer. By default, this is **Disabled**.



Note By default, SSH is disabled for all APs that are connected to the CBW network. SSH can be enabled only by TAC for debugging purposes.

DNS Servers

- Choose **Umbrella** to use Public Open DNS Services
- Choose **User Defined DNS** to configure custom defined DNS Services.

Ping Test

This is similar to the client ping test. You can use this test to check if a particular IP (IP received by sub-ordinate APs or client or open DNS IP) is reachable.

Example: Ping 8.8.8.8

DNS

This feature is used to verify if a particular DNS entered is valid.

Example: Ping google.com

Radius Response

This operates like a simulation tool to verify if the Primary AP is able to reach the RADIUS server. For this, you should have at least one WLAN with WPA2 Enterprise as the access type. It is also used to verify if the username and password details exist in the RADIUS server.

By clicking **Start** all tests will run all the above test.

Uploading Files

This section details the process to upload files to the Primary AP from WebUI using the local file upload such as (HTTP), FTP or TFTP.

To upload a file, do the following:

Step 1 Navigate to **Advanced > Primary AP Tools > Upload File**.

Step 2 Select the **File Type** to upload. It can be one of the following:

- **OUI file**—OUI file contains list of device MAC-IDs and specific owner for the device MAC-ID. The latest file can be downloaded from <http://standards-oui.ieee.org/oui.txt>. Only a **.txt** file format is allowed.

- **EAP Device Certificate**—Certificates that are needed for Extensible Authentication Protocol (EAP) based authentication of the device.

Note Once the certificate is uploaded successfully, the Primary AP has to be reloaded to apply the new certificate.

- **EAP CA Certificate**—Certificate Authority (CA) Certificates that are needed for Extensible Authentication Protocol (EAP) based authentication. Only a **.pem**, **.crt** file format are allowed.

- **CCO Root CA Certificate**—CloudCenter Orchestrator (CCO) Root CA based certificate for authentication of the device. Only a **.crt** file format is allowed.

Note A CCO Root CA is a Certificate Authority that owns one or more trusted roots. That means that they have roots in the trust stores of the major browsers.

- **CBD Serv CA Certificate**—The CA certs is used to establish a secure communication from CBW to CBD. If the CBD has updated the self-signed certificate then that certificate file should be uploaded in the CBW.

If connection between CBW and CBD is based on CBD probe or if the CBD uses certificate signed by a trusted certificate authority, CBD Server CA Certificate upload is not required. The allowed certificate file formats are **.pem**, **.crt**, and **.cert**.

- **WEBAUTH Certificate**—This certificate is used for Captive portal. By default, CBW AP uses self-signed certificate for guest users. You can also upload custom certificate for captive portal using this option. Only **.pem** file format is allowed.

- **WEBADMIN Certificate**—This certificate used for CBW Primary AP UI Access. By default, CBW AP uses self-signed certificate for management access page. You can also upload custom certificate for management access using this option. Only **.pem** file format is allowed. Please ensure that **CommonName** and **SubjectAltName** in the custom certificate is **ciscobusiness.cisco**.

Note For both Web Auth or Web Admin certificate upload:

- When the certificate is uploaded successfully, the Primary AP has to be reloaded to apply the new certificate.
- The root CA certificate has to be installed in the client browser.

Step 3 Select **HTTP**, **FTP** or **TFTP** for the **Transfer Mode** and provide relevant details.

Step 4 If the **Transfer Mode** is **HTTP (Local Machine)**, click **Browse** and upload the file. If the **Transfer Mode** is **FTP/TFTP**, then please enter the server IP, filename, file path and upload the file.

Step 5 Enter the Certificate password.

This field is available only for EAP Device Certificate or Webauth Certificate or Webadmin Certificate File Type.

The fields **Certificate name** and **Valid up to** show the certificate name and the validity of the certificated that is used by the CBW AP.

Step 6 Click **Apply settings** and **Import** to upload the new certificate.

The status of certificate upload can be viewed in the same page. Once the certificate upload is successful, the **Certificate Name** and **Valid up to** fields will be updated.

Certificates

This section displays the list of all certificates that are installed on CBW Primary AP. For each certificate, the following details will be displayed.

- **Name** - The name of the certificate
- **Common Name** - The fully qualified domain name (FQDN) of the certificate
- **Start Date/End Date** - Displays the start and end date of the certificate during which the certificate would be valid.
- **Status** - Displays whether the certificate is **Active** or **Expired** based on the validity period of the certificate.

Security Settings

This section details on controlling the client traffic using Primary AP UI. You have an option to create ACL rules and apply the rules at per WLAN level. The following topic briefs about the creation of an ACL

Access Control Lists

The Access Control Lists (ACLs) is a set of rules that is usually used to filter network traffic. ACLs contains a list of conditions that categorize packets and help you determine when to allow or deny network traffic.

The Access Control Lists (ACLs) on Cisco Business Wireless APs, supports both IP based and domain based filtering. The ACL rules can be applied either before authentication (pre-Auth ACLs) or after authentication (post-Auth ACLs).

You can selectively allow URLs of your choice without authorizations. With this feature, more than one IP can be learnt for the FQDN configured in the URL rule, for both pre-auth and post-auth.

CBW AP supports the following:

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



Note The features that are listed above are also applicable to post-auth.

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

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

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

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

Configuring Access Control Lists (ACL)

To configure Access Control Lists (ACLs) for pre-auth, do the following:



Note

- Enabling the policy ACL, will make the ACL to be added to default-flex-group and pushed down to APs.
- You can create a maximum of 32 IPv4 and IPv6 ACLs.
- You can also configure both IP and URL rules for the same ACL name.
- ACL rules are applied to the VLAN. Multiple WLANs can use the same VLAN and inherit ACL rules, if any.

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

Step 2 In the **Security Settings**, click **Add new ACL**. The **Add ACL Rule** window is displayed.

Step 3 Do the following to add new ACL rules:

- Choose the **ACL Type**. It can be either **IPv4** or **IPv6**.
- Enter the **ACL Name**.
- Use the **Policy ACL** toggle button, to enable or disable the ACL policy.

The device that supports policy-based ACLs allows you to apply access control policies across object groups. An object group is a group of IP addresses or a group of TCP or UDP ports. When you create a rule, you specify the object groups rather than specifying IP addresses or ports.

- Click the **Add IP Rule** button.
- In the **Add/Edit IP ACLs** window, enter the following details and click **Apply**:
 - **Action**—From the **Action** drop-down list, choose **Deny** for the ACL to **Block** packets or **Permit** for the ACL to allow packets. The default is set to **Deny**. The AP can permit or deny only IP packets in an ACL. Other types of packets, such as ARP packets cannot be specified.
 - **Protocol**—Specify the type of protocol. From the **Protocol** drop-down list, choose the protocol ID of the IP packets to be used for this ACL. It can be one of the following or other layer 3 protocols.
 - **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 a list of available protocols in the IANA website.

Note When you specify **Others** as the protocol, you must specify the protocol number in the text box that appears.

- **Source IP/Mask**—You can specify the starting range (here source IP) for applying the IP ACL.
- **Mask**—Masks are used with IP addresses in IP ACLs to specify what should be permitted and denied. Example: 255.255.255.0
- **Source Port**—You can choose a single TCP/UDP source port to which packets are matched.
- **Dest. IP Address/Mask**—You can specify the ending range (destination IP) for applying the IP ACL.
- **Dest. Port**—If you have chosen TCP or UDP, you will 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.
- **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. You can choose:
 - **Any**—Any DSCP (this is the default value).
 - **Specific**—A specific DSCP ranging from 0 to 63, which you can specify in the DSCP edit box.

After configuring all the above details, click **Apply** to configure IP ACL.

- Click **Add URL Rules**.
- In the **Add/Edit URL ACLs** window, enter the **URL** and specify to permit or deny in the **Action** field.

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

- Click **Apply**.

On the **Security Settings** page, the ACL Type, ACL Name, and the Policy Name are listed. You can also view if the policy names are mapped.

Applying the ACL to WLAN at Pre-Auth Level

- Step 1** Choose **Wireless Settings > WLANs**.
 - Step 2** In the **WLANs** window, click the **Edit** icon adjacent to the Guest WLAN for which you want to add the ACL name.
 - Step 3** In the **Edit WLAN** window, under the **WLAN Security** tab, from the **ACL Name (IPv4)** and **ACL Name (IPv6)** drop-down lists, choose a value.
 - Step 4** Click **Apply**.
-

Applying the ACL to WLAN at Post-Auth Level

- Step 1** Choose **Wireless Settings > WLANs**.
 - Step 2** In the **WLANs** window, click the **Edit** icon adjacent to the WLAN for which you want to add ACL rules. The **Edit WLAN** window is displayed.
 - Step 3** Under the **VLAN & Firewall** tab, in the **Enable Firewall** field, choose **Yes** to enable the firewall.
 - Step 4** In the **WLAN Post-auth ACL** section, select either **ACL Name(IPv4)** or **ACL Name(IPv6)**, or both.
 - Step 5** Click **Apply**.
-

Configuring AAA Override in WLAN

The Allow AAA Override option of a WLAN allows you to configure the WLAN for identity networking. It allows you to apply VLAN tagging, QoS, and ACLs to individual clients based on the returned RADIUS attributes from the AAA server.

- Step 1** Switch to the **Expert View**, if you are currently in the Standard View.
 - Step 2** Choose **Wireless Settings > WLANs**.
 - Step 3** In the **WLANs** window, click the **Edit** icon adjacent to the WLAN you select.
 - Step 4** In the **Edit WLAN** window, choose the **Advanced** tab and enable the **Allow the AAA Override** toggle button.
 - Step 5** Click **Apply**.
-

Cisco Business Dashboard Settings

Cisco Business Dashboard Overview

Cisco Business Dashboard (CBD) is a network management tool for deploying and maintaining Cisco Business Switches, Routers, and Wireless Access Points.

Configuring Cisco Business Dashboard Settings

You can connect CBW Access Points to Cisco Business Dashboard (CBD) by configuring the following parameters under CBD Settings in the Primary AP UI.



Note The below configuration is not applicable if you are using a CBD probe to manage CBW. When CBW is managed by CBD probe, you are required to configure the SNMP settings on the Primary AP. Refer to [Managing SNMP, on page 107](#) for more details.

1. Navigate to **Advanced > CBD settings**. The **Cisco Business Dashboard** window is displayed with the following parameters:
 - **Connection Status**—Indicates if the connectivity status between the CBW and CBD is up or down.
 - **Agent Version**—Specifies the CBD agent version. For example, version 2.4.1



Note To troubleshoot issues with CBD connection, refer to [Resolving connection issues between CBW and CBD](#).

2. In the **CBD settings** page, configure the following fields.



Note Ensure that the data you provide on this page matches with the data configured in the CBD application. To login and verify the details as configured in the CBD application, refer to [Cisco Business Dashboard Administration Guide](#).

- **Dashboard Connection Enabled**—To enable/disable the CBW connection with CBD application.



Note To update the CBD parameters disable the **Dashboard Connection Enabled** toggle, and then re-enable the toggle to establish the connection with CBD.

- **Dashboard Name or IP**—Specify the IP address or dashboard name to which you wish to connect.



Note The name or IP address specified in this field must be listed in the Subject-Alternative-Name field of the certificate on Cisco Business Dashboard. Refer to the *Managing Certificates* in the [Cisco Business Dashboard Administration Guide](#) for more information on configuring the certificate.

- **Dashboard Port**—The default HTTPS port is 443.
- **Organization Name**—Enter the organization name created in the CBD application.
- **Network Name**—Enter the organization name created in the CBD application.
- **Access Key ID**—Enter the access key id created in the CBD application.

- **Access Key Secret**—Enter the access key secret created in the CBD application.

3. Click **Save** to establish a connection between the CBW and CBD.



Note If the CBD is using a self-signed certificate, then download a copy of that certificate from the CBD application. Follow the instructions below to download:

1. In the CBD page, navigate to **System > Certificate** and select the **Current Certificate** tab.
2. Click **Download** at the bottom of the page. The certificate will be downloaded in PEM format by your browser.

To upload the certificate, refer to [Uploading Files, on page 119](#).



APPENDIX **A**

Appendix - Supporting Topics

This appendix contains the following sections:

- [LAN port functionality for different models, on page 127](#)
- [LED Color Indicators for Cisco Business Wireless APs, on page 128](#)
- [Primary AP Failover and Election Process, on page 131](#)
- [Pre-downloading an Image to an Access Point, on page 132](#)
- [Creating a Guest Network, on page 132](#)
- [Resetting a Device to Factory Default, on page 133](#)
- [SNMP Traps in CBW AP, on page 135](#)
- [Deployment and Troubleshooting Guidelines, on page 136](#)

LAN port functionality for different models

Cisco Business AP Model	Type	Wired Ethernet Ports	AP Mode	Mesh Mode
CBW140AC	Primary AP Capable	1 (Uplink POE-PD)	NA	NA
CBW145AC	Primary AP Capable	2 ports on the back of the device (1 Uplink POE-PD, 1 passthrough) 4 ports on the bottom of the device (1 POE-PSE LAN, 2 LAN, and 1 passthrough)	RLAN	Ethernet Bridging
CBW240AC	Primary AP Capable	2 (1 Uplink POE-PD, 1 LAN)	RLAN	Ethernet Bridging
CBW141AC	Mesh Extender	4 (1 POE-PSE LAN, 3 LAN)	NA	Ethernet Bridging
CBW142AC	Mesh Extender	NONE	NA	NA
CBW143AC	Mesh Extender	1 (1 POE-PD LAN)	NA	Ethernet Bridging

LED Color Indicators for Cisco Business Wireless APs

This chapter provides information on the LED behavior for Primary APs and Mesh Extenders. It also details the LED states during TFTP and HTTP upgrades.

LED behavior for Primary Capable Access Points

The Cisco access point has an LED indicator on the face of the unit for CBW140AC, CBW240AC, CBW141AC, CBW142AC and CBW143AC AP models. For the CBW145AC model, the LED is located on its lateral side. You can check the device activity based on the LED pattern.

After you have mounted the access point, connect and power up the access point. Observe the LED state to determine the device operation. The following table provides description for different states of the LED and their patterns on the AP device.

For normal Reload of Primary Capable APs, the LED states are as follows:

Table 8: LED behavior for Primary Capable Access Points

Stages of LED States	CBW240AC	CBW140AC	CBW145AC
Stage — 1 POE cable plug in	Red LED (1sec) Blinking Green (3-4 secs)		Blinking Green (3-4 secs)
Stage — 2 Mode button pressed	Blinking Green and Amber (below 20 secs) Blinking Green (after 20 secs when keep it pressed)	Blinking Green and Amber (below 20 secs) Blinking Green (after 20 secs when keep it pressed)	Blinking Red and Amber (below 20 secs) Blinking Green (after 20 secs when keep it pressed)
Stage — 3 Mode button released / Pressed for more than 60 seconds (Logs: Starting Image...)	Blinking Green	Blinking Green	Blinking Green
Note	The Mode Button functionality described in Stage 1, 2 and 3 above are applicable for both Mesh Extenders and Primary Capable Access Points.		
Stage — 4 Sequence of Boot up (Logs: Linux Version...)	Solid Green	Solid Green	Solid Green
Stage — 5 Sequence of Boot up (Logs: 5g radio Domain...)	Blinking Green	Blinking Green	Blinking Green

Stages of LED States	CBW240AC	CBW140AC	CBW145AC
Stage — 6 Radio Init Stage and waiting for Uplink IP config	Blinking Red	Blinking Red	Blinking Red
Stage — 7 IP assigned and Capwap Init (If a Primary AP exists in network moves to stage 8 else switchdriver process starts)	Cyclic change of Red , Amber , Green	Cyclic change of Red , Amber , Green	Cyclic change of Red , Amber , Green
Stage — 8 Capwap discovery to join state and image data response followed by image upgrade if version mismatch and reload (LED stages1-7)	Blinking Amber	Blinking Amber	Blinking Amber
Stage — 9 Capwap setup, configure and run without clients connected (skip stage-8 if the image version is same)	Blinking Green	Blinking Green	Blinking Green
Stage — 10 At least one client connected	Solid Green	Solid Green	Solid Green

LED behavior for Mesh Extenders

The Stage 1-6 in the following table is similar for both the Primary capable APs and Mesh extenders. The different stages for mesh joining process is as follows:

Table 9: LED behavior for Mesh Extenders

Process	Mesh Extenders— CBW 141AC / CBW142AC / CBW143AC
Mesh Stage —1 Starting mesh through searching for parent	Blinking Red

Process	Mesh Extenders— CBW 141AC / CBW142AC / CBW143AC
Mesh Stage — 2 Mesh AP image data Note If Mesh AP image version doesn't match the Primary AP version, the Mesh AP will begin upgrade, then reload. Reload will cycle through Primary Capable Stages 1-6, then Mesh stages 1 & 2.	Cyclic change of Red, Amber, Green
Mesh Stage — 3 Mesh AP image data Note If the mesh image version doesn't match the primary AP version, and the mesh AP has started to upgrade the image version, then the LED will repeat stages 1-6 and mesh stages 1 & 2.	Blinking Amber
Mesh Stage — 4 Mesh AP joined Primary AP	Blinking Green
Stage — 5 At least one client connected	Solid Green

LED behavior during TFTP / HTTP Upgrade

When the AP or Mesh Extender starts to pre-download (TFTP or HTTP) the LED will begin Blinking Amber.

LED Display Settings

To enable, disable or set the LED display to blink an access point, do the following using the web UI:

-
- Step 1** Navigate to **Monitoring>Network Summary>Access Points**.
 - Step 2** Click on any one of the access point available from the list for which you want to enable/disable the LED.
 - Step 3** Click **Tools** from the list of menu available.
 - Step 4** Click **AP LED disable** to turn off the LED display. By default the LED is in the ON state.
 - Step 5** To identify a particular access point from a group of access points placed together, click **Blink AP LED**.
-

Primary AP Failover and Election Process

Primary AP Redundancy for Failover

In a Cisco Business Wireless network, not all APs have the capability to work as a Primary AP. See [Supported Cisco Access Points, on page 1](#) to know which AP models are capable of working as a Primary AP.

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



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

Primary AP Forced Failover

You can manually force any AP, that has the capability to work as a Primary AP, to become the Primary AP. This forced failover of the Primary AP to another Primary-capable AP of your choice can be performed using the Primary AP UI.

To perform a forced failover using the Primary AP UI:

1. Choose **Wireless Settings > Access Points**.
2. In the **Access Points** window, click the **Edit** icon adjacent to the AP you want to set as Primary.
The **Edit** window with the **General** tab is displayed.
3. Under the **General** tab, next to the **Operating Mode field**, click **Make Me Primary AP**.



Note The **Make Me Primary** button is available only for the subordinate APs that are capable of participating in the Primary election process.

When you force the failover of the Primary to an AP of your choice, using the UI, the current Primary AP reboots while the new AP takes over as the Primary AP, with the IP address and configuration as the previous Primary. The previous Primary, after rebooting, comes back online and joins the new Primary AP as a subordinate AP.



Note Like any failover, the forced failover causes downtime in the Cisco Business Wireless network. During this downtime, clients associated to wired uplink APs will not face any disruption in service and no new clients can be connected.

Primary AP Election Process

In a Cisco Business Wireless network, when the Primary AP shuts down, one of the other Primary-capable APs in this deployment is automatically designated as the Primary AP. The automatic selection of the Primary

AP among the Primary-capable APs is as per an internal automatic Primary election process. This process is used to both detect the failure of the Primary AP and to designate the new Primary AP among the eligible APs. This process is based on Virtual Router Redundancy Protocol (VRRP) that algorithmically determines the next Primary AP, based on the following parameters listed in the order of descending precedence:

- The AP configured as next-preferred Primary.
- The AP with the least load in terms of the number of associated clients.
- Among APs with a similar client load, the AP with the lowest MAC address.

Pre-downloading an Image to an Access Point

To minimize network outages, an upgrade software image is downloaded to the access point from the Primary AP without resetting the access point or losing network connectivity. This means that, first the upgrade image to the Primary AP is downloaded and then the image is downloaded to all the Primary capable APs and Mesh Extenders while the network is still up. When the Primary AP reboots, the access points are disassociated and reboot. The Primary AP comes up first, followed by the access points, all with their upgraded images. Once the Primary AP responds to the discovery request sent by an access point with its discovery response packet, the access point sends a join request.

Creating a Guest Network

Login to the Primary AP Web UI, and navigate to **Wireless Settings > WLANs**.

-
- Step 1** Click **Add new WLAN/RLAN**.
- Step 2** Set **Profile name** and **SSID** under the **General** tab.
- Step 3** Under **WLAN Security** tab, enable **Guest Network** using the slider toggle button.
- Step 4** Choose the type of web portal in the **Captive Portal** option. It can be either **Internal Splash Page** or **External Splash Page**.
- Step 5** Choose one of the **Access Type** for Authentication.
- For example, if you want your guests to use their Google/Facebook accounts for authenticating, then use **Social Login** as the Access Type for your Guest WLAN.
- Step 6** Choose the **ACL Name** if you want the guest to access or block few sites / IP.
- Step 7** Click **Apply** to create the Guest WLAN.

Once the Guest connects to your Guest WLAN, it pop ups an **Authentication** page, and the network access is provided if successfully authenticated.

- Note**
- You can also export Guest information by navigating to **Monitoring > Network Summary > Guests** option.
 - The login page of the Guest WLAN can be configured in Web UI under **Wireless Settings > Guest WLAN** page. Refer to the section [Setting a Login Page for WLAN Guest Users](#), on page 66.
-

Resetting a Device to Factory Default



Note

- To reset to factory default using the Mobile App: Select the ... **More** icon on the bottom right of the screen, then select **Reset to Factory Default**.
- To clear the Primary AP configuration and reset the entire network, see [Clearing the Primary AP Configuration and Resetting to Factory Defaults, on page 116](#).
- To factory default a single AP, refer to the **Factory Default** section, under **Tools** in the [Viewing Access Point Details, on page 22](#).

To reset the AP or Mesh extender to factory default using the **Mode button**, do the following:

1. Remove or unplug the Power to device.
2. Press and hold the **Mode button** while re-applying power to the device.
3. Once the LED pattern changes to Green/off, release the Mode button and allow the device to continue booting up.

The location of the Mode button on various CBW models is described in the following table:

Table 10: Mode button Location on the CBW Models

Device Model	Mode Button Location
CBW140AC & CBW141ACM	Located near the Ethernet ports and labeled Mode .
CBW142ACM & CBW143ACM	Located near to the Kensington lock as displayed in the following Mode Button and Kensington Lock figure.
CBW145AC	Located on the rear of the device and labeled Mode .
CBW240AC	A small hole located next to the USB port.

The following figure displays the location of the mode button on the CBW142ACM and CBW143ACM devices:

Figure 4: Mode Button and Kensington Lock

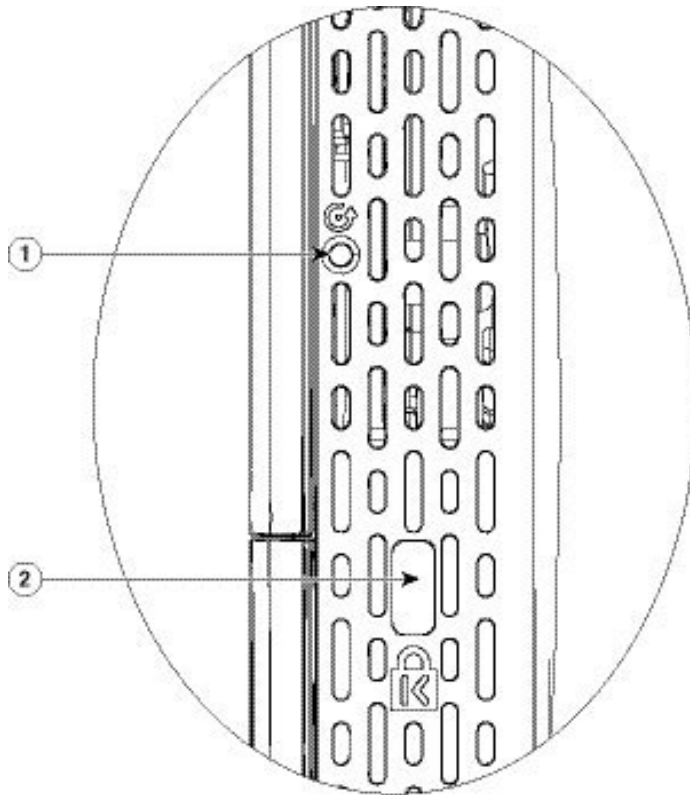


Image Number	Description
1	Mode button, on the right side of the AP
2	Kensington security lock slot



Note If the Mode button is pressed for over 60 seconds, factory defaults reset will be ignored or if it is pressed after the device boots up, it is ignored.

After a few seconds, the device LED will begin blinking alternating Green/Amber for 20 seconds, then switch to Green/off.



Note In the CBW145, the LED blinks Red/Amber during the 20 second countdown while the Mode button is pressed.

SNMP Traps in CBW AP

You can configure the SNMP trap receiver in CBW UI and receive the SNMP traps. The SNMP Trap receiver can be configured using the Web UI by navigating to **Advanced > SNMP**. The following table lists the set of SNMP traps available in CBW AP and the instance at which these traps are triggered:

Table 11: SNMP Traps in CBW AP

Category	Trap Name	Purpose
System/Primary AP	Authentication Flag	Sending traps with invalid SNMP access
	Multiple Users Flag	Sending of traps when multiple logins of Primary AP are active
	configsave	Sending of traps when Primary AP save config called by UI/CLI
	strong-pwd check	Sending of traps when Primary AP user credential's password policy is changed
802.11 client	Excluded	Wireless client exclusion trap; If any client excluded by Primary AP, triggers this trap
	Max Client Wrning Threshold	Triggers the trap when the system reaches 90% of max client associated with this Primary AP
	Nac-Alert Traps	Sending of traps when the client joined on NAC enabled WLAN
	WebAuthUserLogin	Guest user login on Guest WLAN
	WebAuthUserLogout	Guest user logged out/client delete from Primary AP
Cisco AP	AuthFailure	Access point authentication failure trap while Access point joining to the Primary AP it checks the mac filter. It is applicable in Mesh mode.
	Register	Access point join/disjoin from the Primary AP
	InterfaceUp	Access point radio interface up/down trap
	modeChange	Any operational mode change
802.11 Security	WEP/WPA Decrypt Error	Sending traps if any wep/wpa decrypt error detected on any of the APs
	IDS Signature attack detected	Sending traps if any IDS signature attack (Assoc, deauth flood) is detected by the Access point

Category	Trap Name	Purpose
AAA	auth	Sending when an AAA authentication failure occurs for management user, net user, or MAC filter.
	servers	sending when no RADIUS servers are responding
Rogue	Rogueap	Sending trap when detects the Rogue AP
Auto-RF Profiles(RRM)	Client/Channels Load,Noise, interference, coverage hole	Sending trap when failure or max threshold reached for the RRM measurements
	Txpower	Send trap when Access points radio's tx power level changed
	Channel	Send trap when Access points radio's channel changed
Mesh	auth failure	Send trap when Mesh Extender's authentication is failed
	child excluded parent	Sending trap if Mesh Extender excludes the parent node
	parent change	Send trap if mesh extender changes the parent
	child moved	Send trap if mesh extender moved from this parent
	excessive parent change	Send trap if mesh extender change parent rapidly
	onsetSnr	Send trap if parent SNR is poor (less than 12)
	abate SNR	Send trap if parent SNR is high (more than 60)
	excessive association	Send trap if mesh extender attempted too many association (10 count without success)
	excessive children	Send trap if any node has more than 20 mesh extenders (this will not hit for SMB customers)

Deployment and Troubleshooting Guidelines

This section provides details on deployment and troubleshooting issues.

Placing an AP/ Mesh Extender

- Consider to place the Mesh extenders in the line of sight of the Primary/Primary Capable AP or another Mesh Extender. Walls and other objects between the Mesh Extender and the Primary/Primary Capable AP or other Mesh Extender may interfere or reduce connectivity.
- Check the SSID signal strength of the Primary AP and place the Mesh Extender in a location that has enough signal strength.

- The following table captures the recommended maximum distance between the CBW APs (considering the cell overlap as well). These values (approx.) are computed in the open space. We recommend the distance range to avoid interference by other APs and Mesh disconnection issues.

AP	Meters	Foot
CBW140AC	15 to 18	50 to 60
CBW145AC	15 to 18	50 to 60
CBW240AC	18 to 21	60 to 70
CBW141ACM	15 to 18	50 to 60
CBW142ACM	10 to 13	32 to 42
CBW143ACM	10 to 13	32 to 42

- Avoid placing the Mesh Extenders very close to each other and other Primary Capable APs.
- Locate the Mesh Extenders where the Signal to Noise Ratio (SNR) value is good (more than 30). To check the SNR value, navigate to **Monitoring > Network Summary > Mesh Extender**.

You can also identify the Nearest APs for each Mesh Extender by checking on **Nearest APs** field under **Monitoring > Access Points**. Select the Mesh Extender and then refer to the **General** section in the **Access Point** View page.

Setting Up Channel of Primary/Primary capable APs

The Radio channel settings for Access Points and Mesh extenders default to Automatic. The channel settings for an Access Point or Mesh Extender can be changed in the Web UI by navigating to **Wireless Settings > Access Points**, and selecting the **Edit AP** action from the table. A pop-up window will have a tab for Radio 1 (2.4 GHz) and Radio 2 (5 GHz). For Mesh extenders, the backhaul radio channel is controlled by the Primary AP (by default 5 GHz) and cannot be changed in the Mesh Extender window.

Following are some of the instances in which you would need to change the channel of Primary/Primary capable APs for better performance.

By default, the APs in mesh deployment are configured with the mesh backhaul radio configured for channel number 36 and channel width as 80MHz in 5GHz radio.

- If additional Primary Capable APs are deployed to primarily provide additional capacity, then they should be deployed on a different channel than its neighboring Primary/ Primary Capable APs to minimize the co-channel interference.
- If many Rogue APs are present in the AP's current channel, then change the channel of the Primary capable APs. To view the Rogue APs, navigate to **Monitoring > Rogues > Access Points**.
- If Channel Utilization is high (greater than 75) and Interference is high in the serving channel, then change the channel in the AP. You can view the following error logs by navigating to **Advanced > Logging > Logs**.

Following is an example of a log displayed in the **Logs** window:

```
*RRM-DCLNT-5_0: Dec 25 16:51:34.543: %RRM-3-HIGHCHANNEL_UTIL: rrmLrad.c:7678
Interference is high on AP: APA453.0E1F.E480 [Level: 85] on Radio:
```

5Ghz (Radio2) .Change Channel (Wireless->Access Points->Edit AP->Radio->Channel) to get better/stable performance.

- Choose non-DFS channels (36-48, 149-165) for maximizing the coverage, as DFS channels (channel 52 - 144) will have low power level. To change the channel for the AP:

1. Navigate to **Wireless Settings > Access Points**.
2. Select the AP to edit the channel.
3. Change the Channel under **Radio 2** in Mesh deployments.

In Non-Mesh deployment:

1. switch to Expert view
2. Navigate to **Advanced > RF optimization > Select DCA channels > 5Ghz**.
3. Deselect the DFS channel numbers.



Note Nations apply their own RF emission regulations to the allowable channels, allowed users and maximum power levels within the frequency ranges.

Recommendation on Mesh Hop Count

- Data Traffic: Maximum of 4 hops
- Voice Traffic: Maximum of 2 hops

Grouping Mesh Extenders using BGN name

You can also deploy more than one Primary capable AP in your network in the same sector (area), and can logically group the Mesh Extenders by configuring BGN string under **Wireless Settings > Access Points > Edit Access point > Mesh tab**. By default, the BGN value is set with first 10 characters of the configured SSID during initial setup. If BGN is configured, then Mesh Extenders will select the same BGN configured Parent and if there are no matched BGN configured parent, then it will select any parent in the network and periodically disconnect and check for matched BGN parent.



Note This option is available in **Expert View** only.

Best practices for HTTP Image Upgrade

- Prefer wired client to do the image upgrade or wireless client with good connection score.
- Place the wireless client near the Primary AP and ensure it is connected to a Primary AP while trying to upgrade image through HTTP image transfer method.
- Ensure your wireless client has high signal strength (greater than -65 dBm) and a good connection score (higher than 75%) to avoid any image download failures.
- If the image upgrade constantly fails, then use **Cisco.com** mode for Image upgrade.

- When uploading the images using HTTP method, if you see a **Transfer fail** error on the Chrome browser, then the self-signed certificate of Primary AP should be added in the **Trusted Root Authority**. Following are the steps to add the certificate:

Adding Self-Signed certificate of Primary AP in Windows:

1. Navigate to the Primary AP UI using *https://ciscobusiness.cisco* or *https://<managementip>*, and click through the usual warnings for untrusted certificates.
2. In the address bar, right click on the red warning triangle that reads, **Not Secure**. From the resulting menu, select **Certificate** to display the certificate.
3. In the pop-up window, select the **Details** tab, and click **Copy to File** at the bottom right of the tab.
4. This launches the **Certificate Export Wizard**. Click **Next** at the bottom.
5. In the radio-button dialogue, select the format. Leave the default **DER encoded binary X.509 (.CER)** and click **Next**.
6. Use **Browse** to select a folder path to download the exported cert. Click **Next** to export the certificate and then click **Finish**.
7. You should see another pop-up window confirming the export was successful. Click **OK**.
8. In the original **Certificate** pop-up window, click **OK** again.
9. Next, open the Chrome **Settings** page and click **Privacy and security** tab on the left navigation pane. Click the **more** arrow to expand this section. Choose the **Manage certificates** area.
10. In the pop-up **Certificates** window, select the **Trusted Root Certification Authorities** tab, and click on the **Import** button; this will launch the **Certificate Import Wizard**.
11. Click **Next**. Select **Browse** and use the explorer window to locate the certificate you exported in the earlier step.
12. Click **Next** and then **Finish**. In the **Security Warning** pop-up, click on **Yes**; you should see yet another pop-up letting you know that the import was successful.
13. Restart Chrome, and navigate to the Primary AP UI using *https://<managementip>*. You should see a closed padlock and **Secure** annotation to the left of the URL.

Adding Self-signed certificate of Primary AP in macOS:

Navigate to the Primary AP UI using *https://ciscobusiness.cisco* or *https://<managementip>*. Do the following in Chrome:

1. Navigate to **Developer Tools > Security tab**.
2. Click **View Certificate** to see the certificate.
3. Click and drag the image to your desktop.
4. Open the **Keychain Access** utility in OS X.
5. Select the **System** option on the left.
6. Click the **lock** icon on the upper-left to enable changes.
7. In the lower left, select the **Certificates** option.

8. Drag the certificate you copied to the desktop into the list of certificates.
9. After the certificate is added to the **System** keychain, double-click to open.
10. Expand the **Trust** section. For the first option, pick **Always Trust**.
11. Quit Chrome and all other browsers and navigate to the Primary AP UI using `https://<managementip>`. You should see the closed padlock and **Secure** annotation to the left of the URL.



Note Use `https://<managementip>` to access the Primary AP UI, if the self-signed certificate is added to your machine.

Resolving connection issues between CBW and CBD

- If the connection is based on a CBD probe, please ensure that the SNMP configuration in CBD and CBW are the same. To configure the SNMP details of the device on CBD, refer to *Managing Device Credentials* in the [Cisco Business Dashboard Administration Guide](#).
- If the connection between CBD and CBW is a direct management connection, ensure the following:
 - Verify if the credentials specified in **CBD Settings** page, is the same as created in CBD.
 - Verify if the correct certificate file is uploaded in CBW (in case CBD uses self-signed certificate).
 - Verify that the name or IP address configured for the Dashboard in CBW is listed in the Subject-Alternative-Name field of the dashboard's certificate
 - Check the system logs in the **logging** page.



APPENDIX **B**

Appendix - Mounting and Grounding Access Points

This appendix contains the following sections:

- [About Mounting, on page 141](#)
- [Preparing the AP for Installation, on page 141](#)
- [Mounting CBW140AC/240AC, on page 142](#)
- [Mounting CBW145AC, on page 147](#)
- [Mounting CBW141AC, on page 152](#)
- [Mounting CBW142AC, on page 152](#)
- [Mounting CBW143AC, on page 157](#)
- [Grounding an Access Point, on page 159](#)

About Mounting

These mounting instructions describe the steps for mounting supported Cisco Business Wireless series access points in several configurations, including on a suspended ceiling, on a hard ceiling or wall, on an electrical or network box, and above a suspended ceiling.

Preparing the AP for Installation

Before you mount and deploy your access point, we recommend that you perform a site survey (or use the site planning tool) to determine the best location to install your access point.

You should have the following information about your wireless network available:

- Access point locations.
- Access point mounting options: on a wall or a ceiling only.



Note You can mount the access point above a suspended ceiling but you must purchase additional mounting hardware. For additional information, see mounting and grounding sections for individual access point models in the later sections.

Access points mounted in a building's environmental airspace must be powered using PoE to comply with safety regulations.

The CBW140AC, CBW240AC, CBW145AC access point models are powered through PoE and the CBW142ACM model is directly plugged into an AC source.

Cisco recommends that you make a site map showing access point locations so that you can record the device MAC addresses from each location and return them to the person who is planning or managing your wireless network.

Mounting CBW140AC/240AC

Cisco Business Wireless 140AC/240AC access points can be mounted in several configurations; on a suspended ceiling, on a hard ceiling or wall, or in the plenum air space above a suspended ceiling. You can mount the AP on an electrical or network box.



Note When mounting the AP in the plenum air space or above a suspended ceiling, it should be mounted on a vertical wall or with the face of the AP (having the status LED) directed downwards.

Mounting the Hardware

Mounting hardware for access points consists of brackets, which connect to the bottom of the access point, and ceiling grid clips, which connect the bracket to a suspended ceiling. The bracket that you need depends on the mounting location for the access point. The ceiling grid clip that you need depends on the type of suspended ceiling where you need to install the access point. You don't need ceiling grid clips if you are mounting the access point to a hard-surface ceiling or a wall.

Mounting Brackets

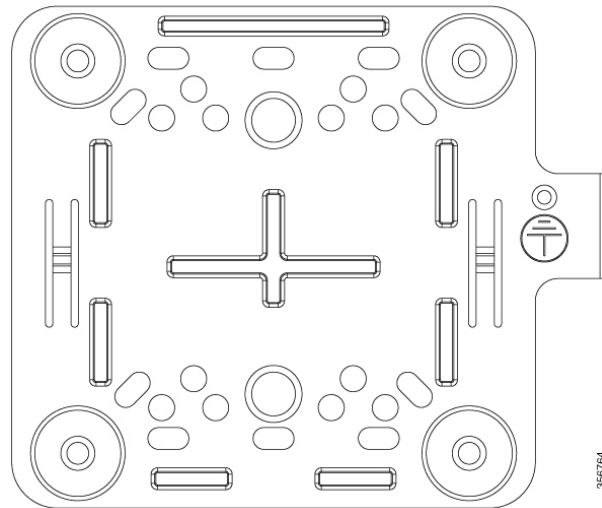
The standard mounting hardware supported by the AP is listed in the following table:

Table 12: Bracket for Mounting the Access Points

Parts	Part Number	Description
Bracket It has 4 expansion screws. You can fasten the bracket to the wall or ceiling using these expansion screws.	74-123953-01	Mounting bracket for ceiling and wall. It also includes the Ceiling Grid Clip.

The following figure shows the low-profile bracket installed on an access point.

Figure 5: Low-Profile Mounting Bracket



Ceiling Grid Clip

You use a ceiling grid clip (included) to mount an access point on a suspended ceiling.

Figure 6: Ceiling Grid Clip

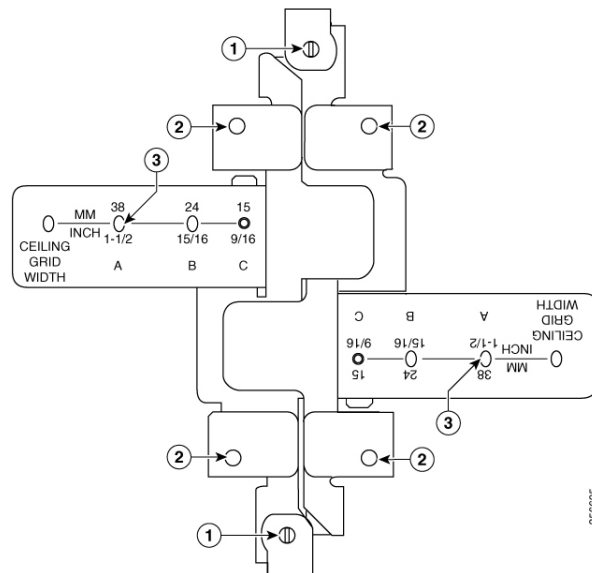


Image Number	Description
1	Locking screws
2	Bracket screw holes
3	T-rail width detents (A, B, or C)

Mounting an Access Point Below a Suspended Ceiling

Follow these steps to mount the access point below a standard or recessed suspended ceiling. The following figure shows an access point mounted on a T-rail ceiling rail using a ceiling grid clip.

Figure 7: Suspended Ceiling Mounting Details

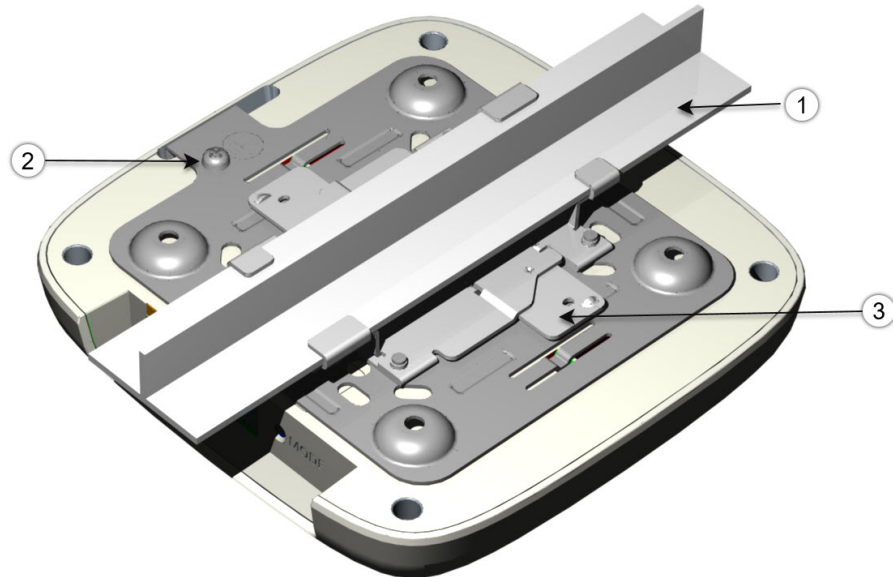


Image Number	Description
1	Ceiling T-rail
2	Grounding point
3	Ceiling grid clip

To mount the access point below a suspended ceiling, do the following:

1. Decide where you want to mount the access point on your suspended ceiling.
2. Open the ceiling grid clip completely.
3. Place the ceiling grid clip over the T-rail and close it to the appropriate detent (A, B, or C).
4. Use a screwdriver to tighten the two ceiling grid clip locking screws to prevent the clip from sliding along the T-rail.
5. Observe the ceiling grid clip width detent letter (A, B, or C) that corresponds to the T-rail width.
6. Align the corresponding holes (A, B, or C) on the mounting bracket over the mounting holes on the ceiling grid clip.
7. Hold the mounting bracket and insert a 6-32 x 1/4 in. screw into each of the four corresponding holes (A, B, or C) and tighten.

8. If necessary, drill or cut a cable access hole in the ceiling tile large enough for the Ethernet cable.
9. (Optional) Use the ground screw to ground the access point to a suitable building ground. See [Grounding an Access Point, on page 159](#) for general grounding instructions.
10. Connect the Ethernet cable to the access point.
11. Align the bracket feet over the keyhole mounting slots on the access point.
12. Gently slide the access point onto the mounting bracket until it clicks into place.
13. Fasten the AP to the bracket using the M2 x 5.5mm Torx security screw. Cover it with the mylar label.

Mounting an Access Point on a Hard Ceiling or a Wall

This procedure describes the steps required to mount the access point on a ceiling constructed of 3/4-in (19.05-mm) or thicker plywood using #8 fasteners using the mounting bracket.



Note Access points with integrated antennas perform best when the access point is mounted on horizontal surfaces such as a table top or ceiling. For advanced features such as voice, location, and rogue access point detection, ceiling mounting is strongly recommended. However, for smaller areas such as conference rooms, kiosks, transportation environments, or hot-spot usage where data coverage is the primary concern, the unit may be wall mounted using wall anchors or screws.

To mount the access point on a solid ceiling or wall, do the following:

1. Use the mounting bracket as a template to mark the locations of the mounting holes on the bracket.



Caution Be sure to mark all four locations. To ensure a safe and secure installation, make sure you are using adequate fasteners and mount the access point using no less than four fasteners.

Do not use plastic wall anchors or the keyhole slots on the mounting bracket for ceiling installations. When mounting the access point on a hard ceiling, use four fasteners capable of maintaining a minimum pullout force of 20 lbs (9 kgs).

2. Use a #29 drill (0.1360-in. [3.4772 mm]) bit to drill a pilot hole at the mounting hole locations you marked.



Note The pilot hole size varies according to the material and thickness you are fastening. Cisco recommends that you test the material to determine the ideal hole size for your mounting application.

3. (Optional) Drill or cut a cable access hole large enough for the Ethernet cable and the building ground wire.
4. (Optional) Use the ground screw to attach the building ground wire to the mounting bracket. See [Grounding an Access Point, on page 159](#) for general grounding instructions.
5. Position the mounting bracket mounting holes (with indents down) over the pilot holes.
6. Insert a fastener into each mounting hole and tighten.

7. Connect the Ethernet cable to the access point.
8. Align the bracket feet over the keyhole mounting slots on the access point.
9. Gently slide the access point onto the mounting bracket keyhole slots until it clicks into place.
10. Fasten the AP to the bracket using the M2 x 5.5mm Torx security screw. Cover it with the mylar label.

Mounting an Access Point to a Network or Electrical Box

To mount an access point to a network box or an electrical box, do the following:

1. Position the universal mounting bracket over the existing network or electrical box and align the bracket mounting holes with the box holes.
2. Hold the mounting bracket in place and insert a 6 x 32 x 1/4-in pan head screw into each of the mounting holes and tighten.
3. (Optional) Use the ground screw to attach the building ground wire to the mounting bracket. See [Grounding an Access Point, on page 159](#) for general grounding instructions.
4. Connect the Ethernet cable to the access point.
5. Align the bracket feet over the keyhole mounting slots on the access point.
6. Slide the access point onto the optional mounting bracket until it clicks into place.
7. Fasten the AP to the bracket using the M2 x 5.5mm Torx security screw. Cover it with the mylar label.

Mounting an Access Point Above a Suspended Ceiling

Using third-party accessories (not offered by Cisco) you can mount an access point above a suspended ceiling.



Note Install access points above ceiling tiles only when mounting below the ceiling is not an option. Mounting access points above the ceiling can interfere with advanced wireless LAN features that depend on uniform coverage, such as voice and location.

Figure 8: T-Bar Grid Mounting Bracket Parts

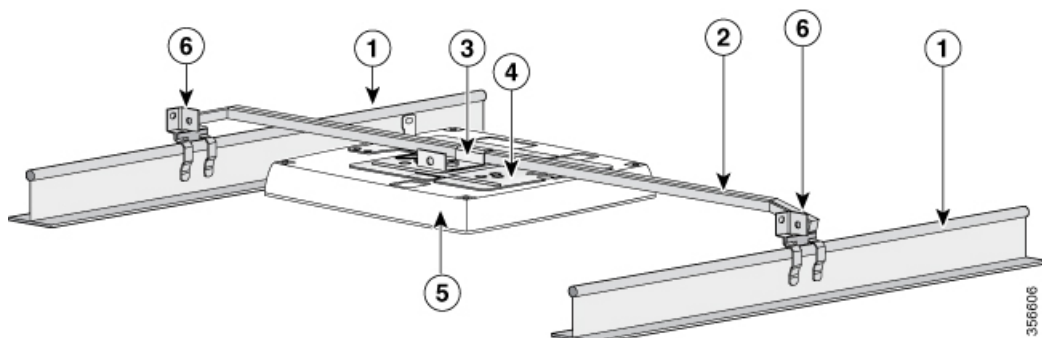


Image Number	Description
1	Suspended ceiling T-rail
2	Box hanger
3	Box hanger clip
4	Mounting bracket
5	Access point
6	T-rail clip

To mount the access point above a suspended ceiling, do the following:

1. Remove a ceiling tile adjacent to the mounting location.
2. Fasten the access point mounting bracket to the box hanger using the clip or screws provided with the box hanger kit.
3. Connect the Ethernet cable to the access point.
4. Align the bracket feet over the keyhole mounting slots on the access point.
5. Slide the access point onto the mounting bracket until it clicks into place.
6. Attach the T-rail clips on each end of the T-bar box hanger to the ceiling rails. Make sure the clips are securely attached to the T-rails.
7. Fasten the AP to the bracket using the M2 x 5.5mm Torx security screw. Cover it with the mylar label.
8. Replace the ceiling tile.

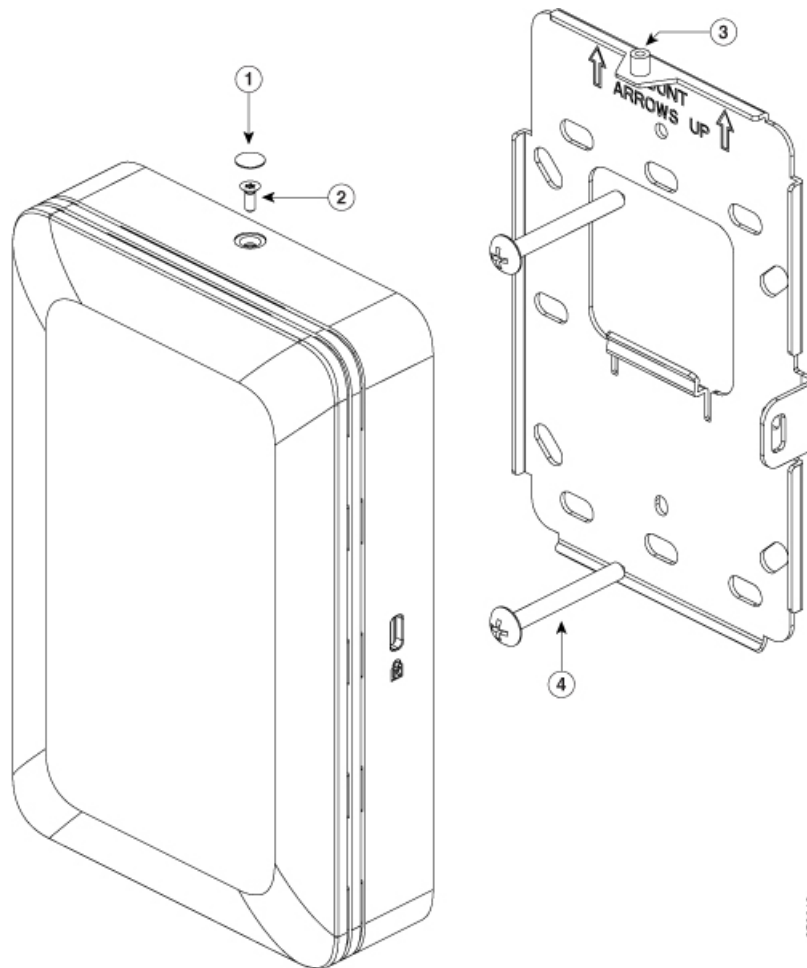
Mounting CBW145AC

The Cisco Business Wireless 145AC access points can be mounted in several configurations—on a suspended ceiling, on a hard ceiling or wall, or in the plenum air space above a suspended ceiling and on a electrical junction box using the spacer.

Table 13: Access Point Mounting Options

Parts	Part Number	Description
Bracket	74-112728-01 (Included)	Mounting the AP directly on a Wall
		Mounting the AP on an Electrical Junction Box
		Mounting the AP on a Wall using the Spacer
	AIR-AP1815W-KIT= (Optional, not included)	Spacer Kit: Includes spacer and RJ-45 jumper cable.

Figure 9: Mounting AP on a Wall



356613

Mounting the AP on 74-112728-01 and Electrical Junction Box

To mount the CBW145AC-B on the junction box, do the following:

1. Fasten the wall-mount bracket (74-112728-01) to the wall, using two M3.5X32mm screws. Ensure that the side having the **Mount Arrows Up** label is facing outwards, and the bracket is oriented vertically as indicated by the arrows.
2. Connect the PoE cable from the junction box to the PoE port on the rear of the device. If there is a second Ethernet cable in the junction box, it can be connected to the Pass-Through port on the rear of the device and accessed using the Pass-Through port on the bottom of the device.



Note If you are unable to connect a PoE cable to the port on the back of the AP, then:

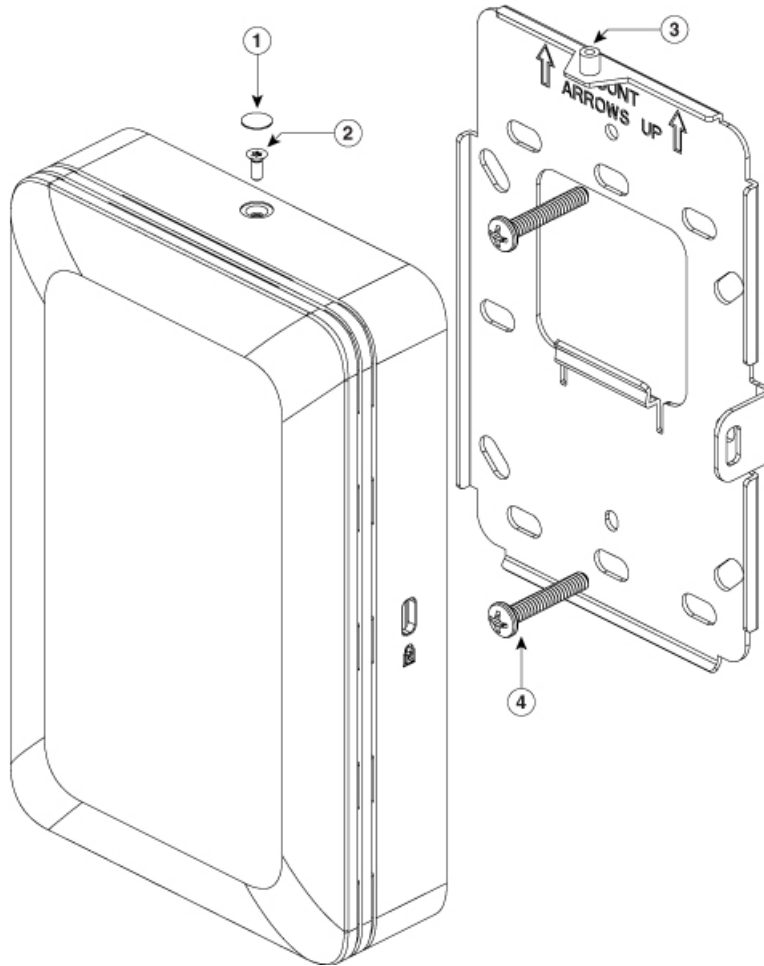
- a. On the back of the AP, use an RJ45 jumper cable to connect the PoE port to the Pass-Through port. This jumper cable is available as part of the spacer kit AIR-AP1815W-KIT=.
- b. Connect the PoE supply cable to the Pass-Through port on the base of the AP.

This connection sends power internally from the Pass-Through port on the base, to the Pass-Through port on the back, and then through the jumper cable into the PoE port on the back.

3. Mount the AP onto the wall-mount bracket. For this, align the AP with the bracket and then offset the AP around ¼ inch above the bracket.
4. Fasten the AP to the bracket using the M2 x 5.5mm Torx security screw. Cover it with the mylar label.

Image Number	Description
1	Mylar label for covering Torx security screw slot
2	M2 x 5.5mm Torx security screw
3	Screw hole on the wall-mount bracket for the security screw
4	Two M3.5 x 32mm screws for fastening the bracket to the wall

Figure 10: Mounting the AP on an Electrical Junction Box



Mounting the AP on a Wall using the Spacer box

To mount the AP on a wall, using a spacer box, do the following:

1. Fasten the spacer box (AIR-AP1815W-KIT=) to the wall, using four M3.5 x 32mm screws. Ensure that the side having the **Mount Arrows Up** label is facing outwards, and the box is oriented vertically as indicated by the arrows.
2. Fasten the wall-mount bracket (74-112728-01) to the spacer box, using two M3X8mm tapping screws. Ensure that the side having the **Mount Arrows Up** label is facing outwards, and the bracket is oriented vertically as indicated by the arrows.
3. Connect the power and network cables to the AP.

If you are unable to connect a PoE cable to the port on the back of the AP, then do the following:

- a. On the back of the AP, use an RJ45 jumper cable to connect the PoE port to the Pass-Through port. This jumper cable is available as part of the spacer kit AIR-AP1815W-KIT=spacer kit.
- b. Connect the PoE supply cable to the Pass-Through port on the base of the AP.



Note The punch-out holes on the spacer box (AIR-AP1815W-KIT) can be used for routing cables. However, an RJ45 connector will not fit through these holes. If this is required, you must first route a cable through the hole and then crimp an RJ45 connector on to the cable.

This connection sends power internally from the Pass-Through port on the base, to the Pass-Through port on the back, and then through the jumper cable into the PoE port on the back.

4. Mount the AP onto the wall-mount bracket. For this, align the AP with the bracket and then offset the AP around $\frac{1}{4}$ inch above the bracket.
5. Fasten the AP to the bracket using the M2 x 5.5mm Torx security screw. Cover it with the mylar label

Figure 11: Mounting the AP on a Wall using the Spacer

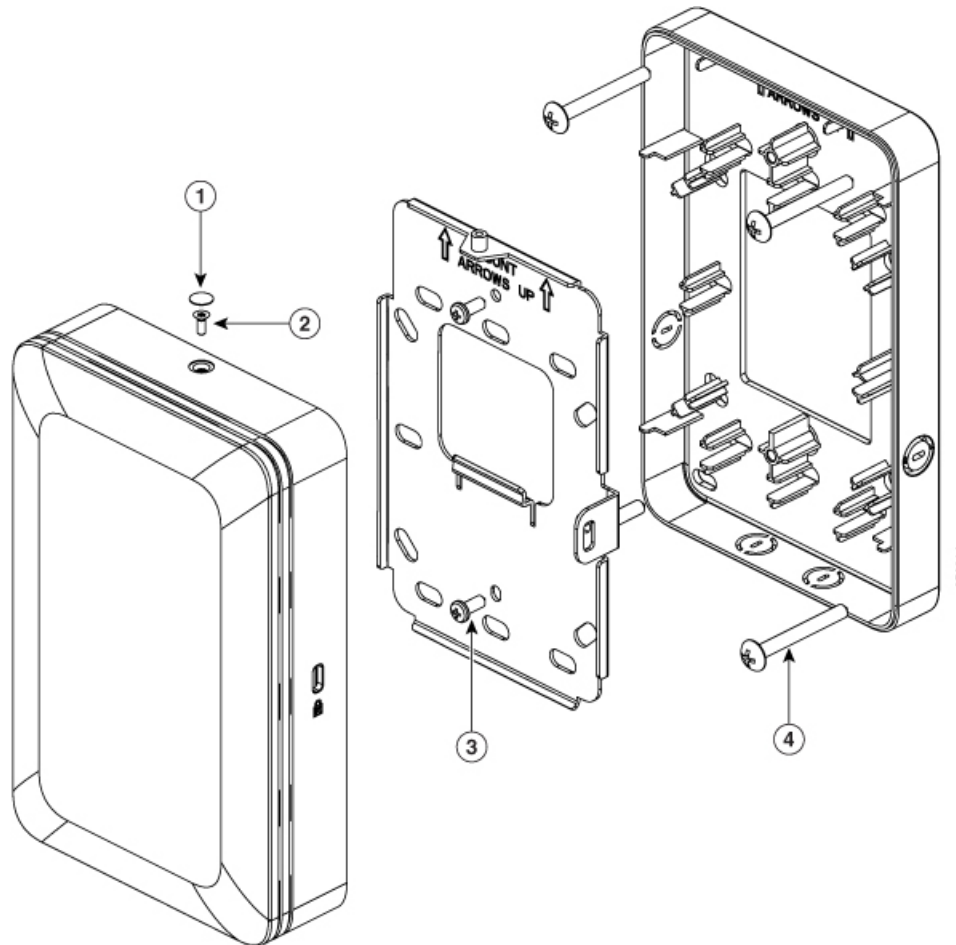


Image Number	Description
1	Mylar label for covering Torx security screw slot.
2	M2 x 5.5mm Torx security screw.

Image Number	Description
3	M3X8mm tapping screws for fastening the wall-mount bracket to the spacer.
4	M3.5 x 32mm screws for fastening the spacer to the wall.

Mounting CBW141AC

The access point can be placed/mounted in a horizontal position, on a horizontal surface such as a table.

To ensure the best RF coverage for your access point, place your access point in an area as close to the wireless clients as possible and practical to do so. If the Internet source or gateway router is in a remote area, position your access point away from metal obstructions.

Areas to avoid or places that may result in reduced range or performance are as follows.

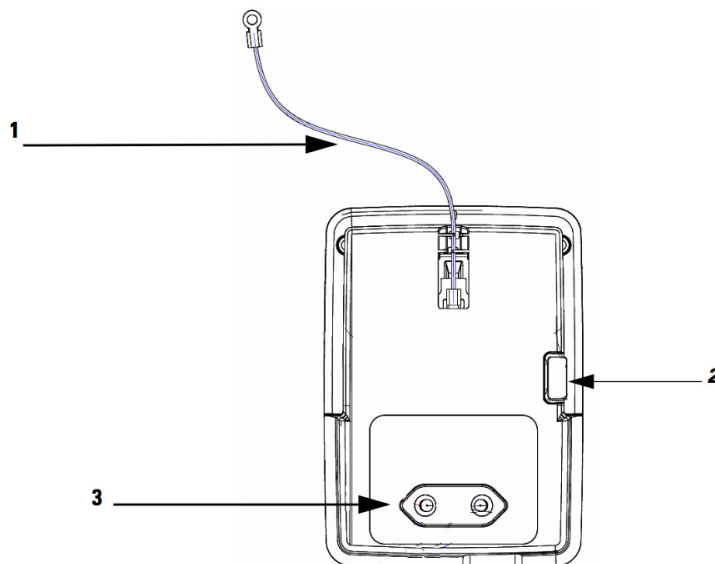
- In a basement of a multi-story home, as the signals must penetrate many walls.
- Near large obstructions that can block the radio signals. Avoid areas like metal cabinets or refrigerators.
- On the floor under a metal desk or other dense or conductive objects.

The AP is powered using 44 to 57 VDC power via the VDC port, using Cisco Power Adapter. The PoE-Out port provides 802.3af Class 0 (15.4W) power.

Mounting CBW142AC

You can additionally secure the AP by fastening the security wire to the wall or desk.

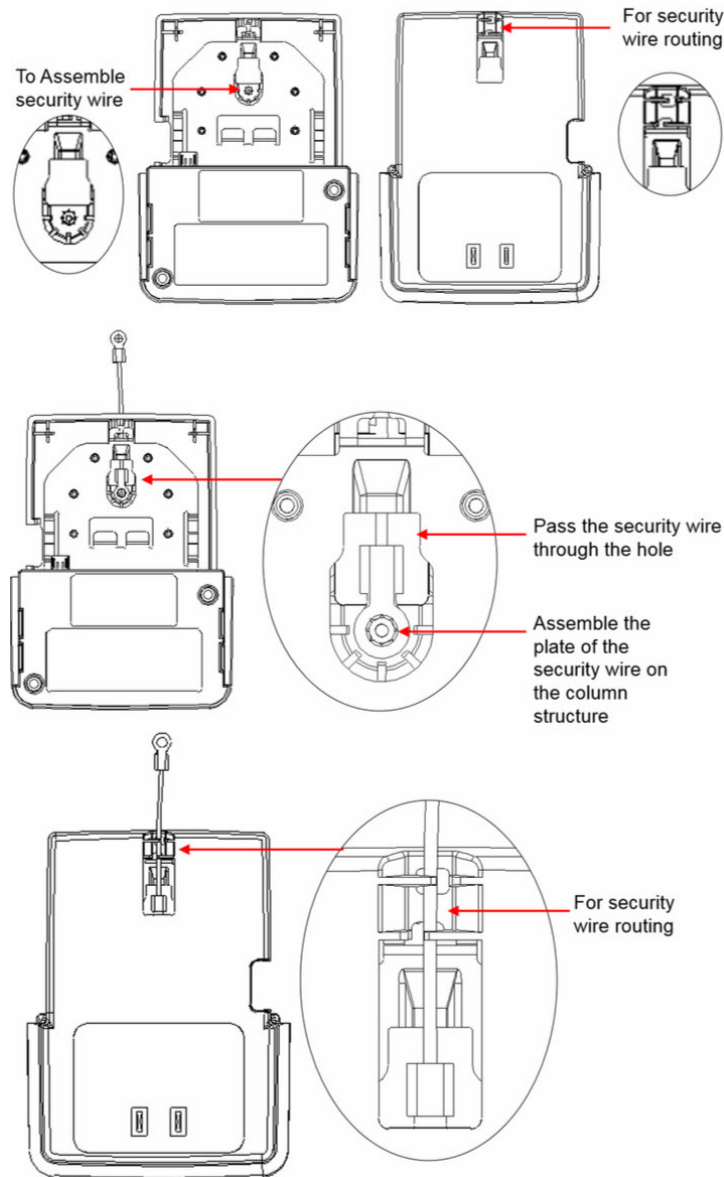
Figure 12: Back of the AP – With AC Adapter Module



The assembling of front and rear views are shown below:

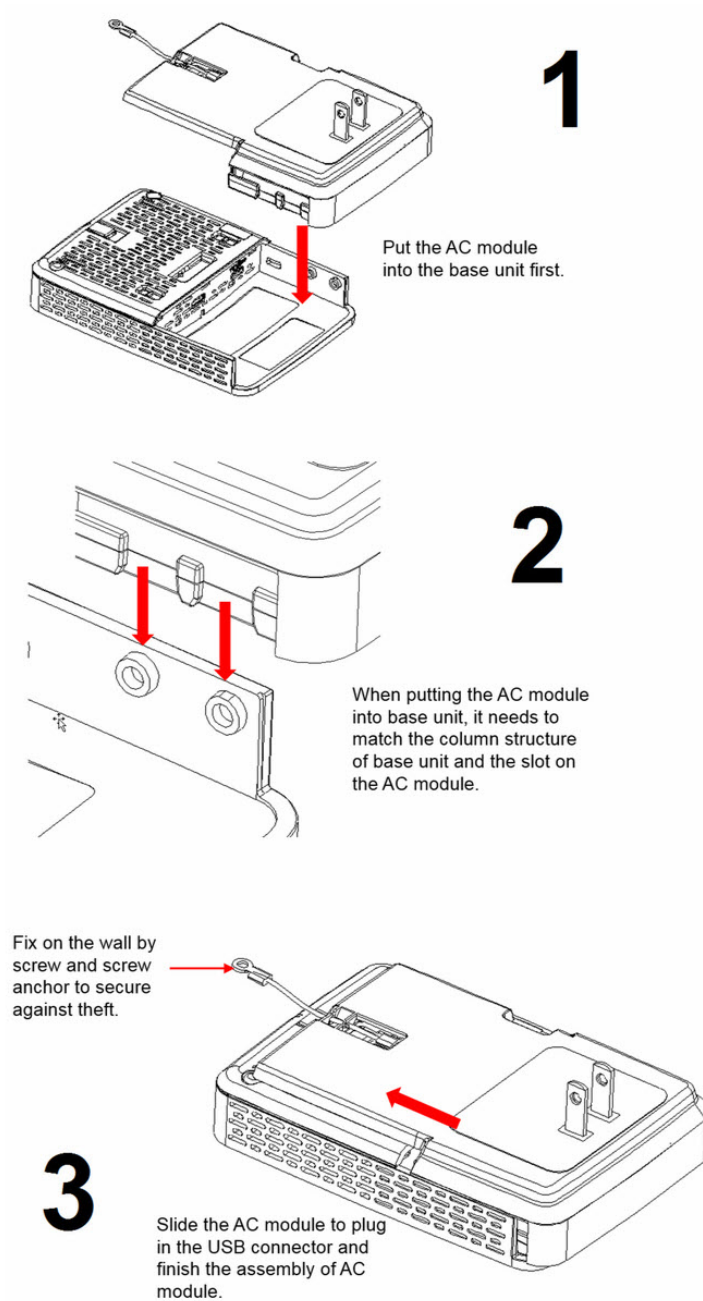
Image Number	Description
1	Security wire which can be used to secure the AP by fastening it to the wall.
3	EU-specification AC adapter module CBW142 The AC adapter module/cradle provided differs in design according to regional power supply standards.

Figure 13: Assembling and Routing the Security Wire – Front and Rear Views



The assembling of AC unit with base module is shown below:

Figure 14: Assembling AC module with Base Unit



The various assembling models for CBW142AC is as follows:

Assembling model for AU Region**Assembling model for CN Region**

Assembling model for EU Region**Assembling model for SA Region**

Assembling model for UK Region



CBW142AC: AC power from a wall socket power outlet, through the AC Adapter module, providing 120~240VAC, 50~60Hz power.

The AC adapter module also functions as a mounting cradle, thereby mounting the sensor on a wall socket power outlet mounted with the help of a stabilizer.

Mounting CBW143AC

The CBW143AC series access points can be mounted, in a vertical orientation, on a wall or desk. The mounting is done using the wall-mount bracket 74-123954-01.

Item	Part Number	Description
Bracket	74-123954-01 (Included)	Mounting the AP directly on a Wall

To mount the AP on a wall:

1. Identify the location for mounting the AP.
2. Use the wall-mount bracket 74-123954-01, as a template to mark the screw-hole locations for fastening the bracket to the wall.
3. At the marked locations, drill a hole into the wall.
4. Fasten the 74-123954-01 to the wall using two 18mm expansion screws.
5. Hold the back of the AP against the wall, above the bracket, and then slide the AP down onto the bracket, till it clicks into place. The hooks on the bracket will click into the recesses on the back of the AP.
6. Proceed with connecting the data and power cables.

The AP can be powered using the following power sources and devices only:

- AC power, using the AC-USB adapter, supplying 5V DC, 1.5A power.

The USB ports are located on the base of the AP.

The CBW143AC can also be powered using PoE (802.3af) supplied through the Ethernet port from a power injector.



Note Cisco recommends that you use only the Cisco supplied AC-USB adapter, for powering the AP through the USB port. Other power supply devices which do not meet the specifications of the Cisco supplied device, can cause silent reboots or crashes.

Figure 15: Wall and Desk Mounting Bracket 74-123954-01

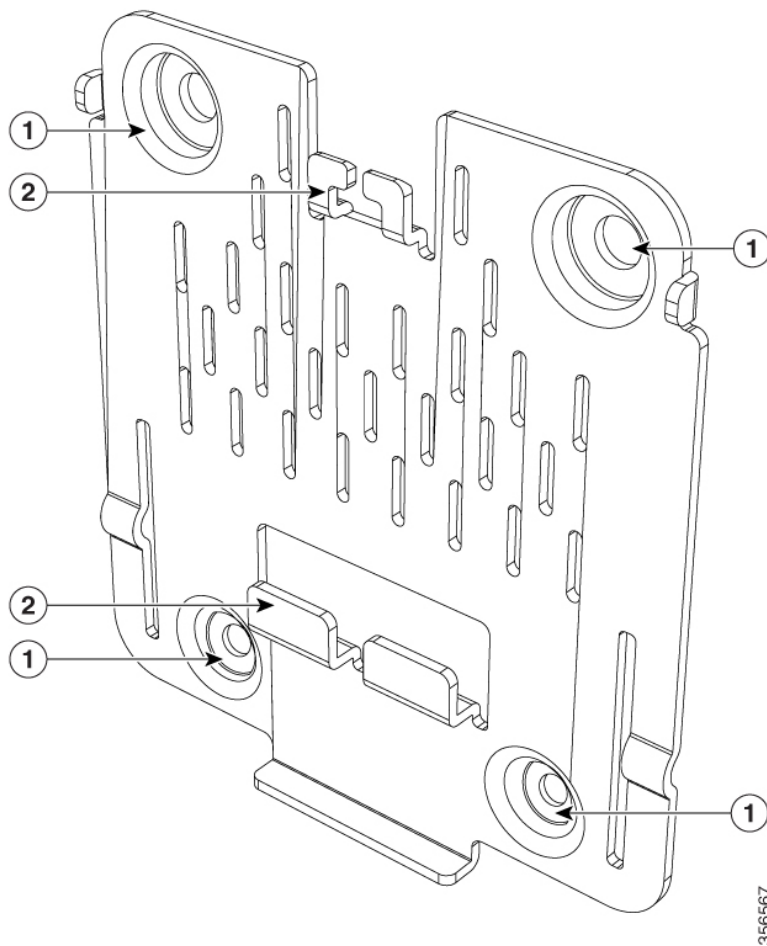


Image Number	Description
1	Screw holes for fastening the bracket to the wall
2	Hooks which click into the recesses on the back of the AP for mounting the AP on the bracket

Figure 16: Back of the AP

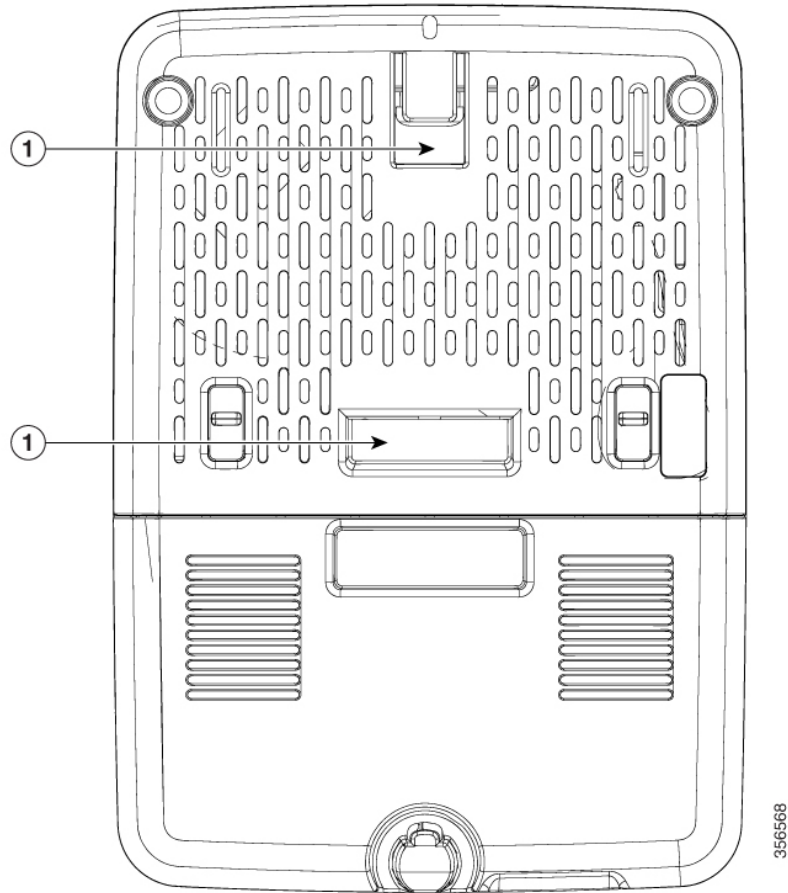


Image Number	Description
1	Recesses on the back of the AP into which the hooks on the wall-mount bracket slide and click into place.

The CBW145AC, CBW141ACM, CBW142ACM, and CBW143ACM devices support a Kensington-style lock.

The location of the Kensington lock slot is shown in the Quick Start guides provided with the device.

Grounding an Access Point

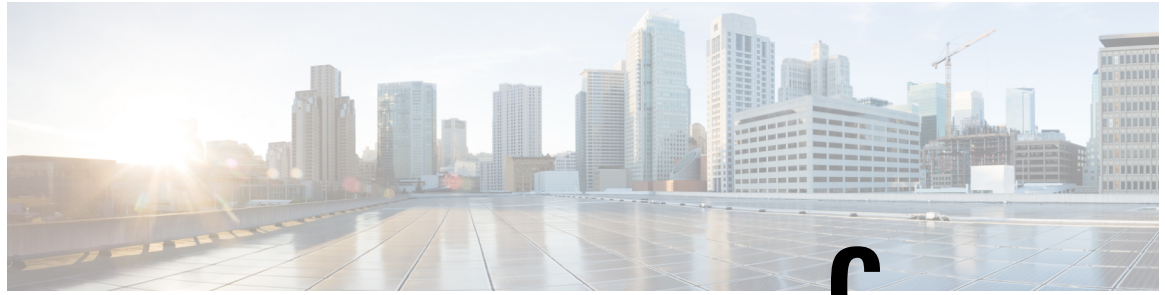
Grounding is not always required for indoor installations because Cisco Business Access Points are classified as low-voltage devices and do not contain internal power supplies. We recommend that you check your local and national electrical codes to see if grounding is a requirement.

Although grounding is not mandatory for indoor access points, it is required in certain scenarios. It has been observed that an ungrounded indoor access point that is mounted too close to an electromagnetic source of interference (such as a fluorescent light that is on) may reboot suddenly or suffer hardware damage. This

occurs even if the indoor AP is in close proximity to the electromagnetic source of interference, and not touching the source. Grounding the corresponding access point or the mounting bracket helps prevent this issue from occurring. We recommend that a certified electrical technician verify whether your installation requires grounding.

If grounding is required in your area or you wish to ground your access point, do the following:

-
- Step 1** Find a suitable building grounding point as close to the access point as possible.
 - Step 2** Connect a user-supplied ground wire to the building grounding point. The wire should be a minimum of #14AWG assuming a circuit length of 25 ft (30.5 cm). Consult your local electrical codes for additional information.
 - Step 3** Route the ground wire to the access point.
 - Step 4** Attach the wire to a suitable grounding O-ring lug.
To locate the grounding point on the device, refer this [Figure 7: Suspended Ceiling Mounting Details](#).
 - Step 5** Crimp or solder the wire to the lug.
 - Step 6** Insert the grounding post screw into the O-ring lug and install it on the mounting bracket as shown in the figure above.
 - Step 7** Use a Phillips screwdriver to tighten the ground screw.
-



APPENDIX **C**

Appendix - Glossary of Terms

This appendix contains the following sections:

- [Cisco Business Wireless - Glossary Of Terms, on page 161](#)

Cisco Business Wireless - Glossary Of Terms

0-9

802.1Q-based VLAN

The IEEE 802.1Q specification establishes a standard method for tagging Ethernet frames with VLAN membership information, and defines the operation of VLAN bridges that permit the definition, operation, and administration of VLAN topologies within a bridged LAN infrastructure. The 802.1Q standard is intended to address the problem of how to divide large networks into smaller parts so broadcast and multicast traffic does not use more bandwidth than necessary. The standard also helps provide a higher level of security between segments of internal networks

802.1X Supplicant

Supplicant is one of the three roles in the 802.1X IEEE Standard. The 802.1X was developed to provide security in Layer 2 of the OSI Model. It is composed of the following components: Supplicant, Authenticator, and Authentication Server. A Supplicant is the client or software that connects to a network so that it can access resources on that network. It needs to provide credentials or certificates to obtain an IP address and be part of that particular network. A Supplicant cannot have access to the network's resources until it has been authenticated.

A

ACL

An Access Control List (ACL) is a list of network traffic filters and correlated actions used to improve security. It blocks or allows users to access specific resources. An ACL contains the hosts that are permitted or denied access to the network device. ACLs can be defined in one of two ways: by IPv4 address or by IPv6 address.

Allowlist

Allowlist is a list of Client/Mesh Extender MAC addresses that are allowed to join the network.

B

Band Steer

Advanced load balancing, better known as band steering, is a feature that detects devices capable of transmitting at 5 GHz band. The 2.4 GHz band is often congested and experiences interference from different devices such as Bluetooth, and even microwave ovens. This feature allows your access point to steer and direct devices to a more optimal radio frequency, thus, improving network performance.

Bandwidth

Bandwidth is the measurement of the ability of a device to send and receive information.

Bandwidth Utilization

Bandwidth utilization allows you to place a threshold on the average successful data transfer through a communication path. Some of the techniques used to improve this are bandwidth shaping, management, capping, and allocation.

Blocklist

A **Blocklist** is a list of Client/Mesh Extender MAC addresses that are denied to join the network.

C

Captive Portal

Captive Portal method forces LAN users or hosts on the network to see a special web page before they can access the public network normally. Captive Portal turns a web browser into an authentication device. The web page requires user interaction or authentication before the access is allowed to use the network.

CBD Probe

Cisco Business Dashboard Probe is installed at each site in the network and associated with the Dashboard. The probe performs network discovery and communicates directly with each managed device.

Central web authentication (CWA)

CWA offers the possibility to have a central device that acts as a web portal. Once the user logs into the portal, it is possible to re-authenticate the client so that a new Layer 2 MAC filtering occurs using the Change of Authorization (CoA). This way, the ISE remembers that it was a webauth user and pushes the necessary authorization attributes to the Primary AP for accessing the network.

Channel Isolation

A device with channel management enabled, automatically assigns wireless radio channels to the other A2 devices in the cluster. The automatic channel assignment reduces interference with other access points outside of its cluster and maximizes Wi-Fi bandwidth to help maintain the efficiency of communication over the wireless network. Automatic channel assignments are supported in non-mesh deployments.

Channel Width

Channel width controls how broad the signal is for transferring data. Think of it like a highway. The wider the road, the more traffic (data) can pass through. On the other hand, the more cars (routers) you have on the road, the more congested the traffic becomes. By increasing the channel width, we can increase the speed and throughput of a wireless broadcast. By default, the 2.4 GHz frequency uses a 20 MHz channel width. A 20MHz channel width is wide enough to span one channel.

A 40 MHz channel width bonds two 20 MHz channels together, forming a 40 MHz channel width; therefore, it allows for greater speed and faster transfer rates.

Client QoS

The Client Quality of Service (QoS) Association is a section that provides additional options for customization of a wireless client's QoS. These options include the bandwidth allowed to send, receive, or guaranteed. Client QoS Association can further be manipulated with the use of Access Control Lists (ACL).

Connection Speed

Connection speed is the speed that data is transferred between your client and the internet.

D

DCA

Dynamic Channel Assignment (DCA) can dynamically determine best bandwidth for each AP connected to the Primary AP. DCA algorithm manages, evaluates the channel assignments on AP on per radio basis. It automatically adjusts the channel to maintain performance of individual radios.

E

EAPoL

Extensible Authentication Protocol (EAP) over LAN (EAPoL) is a network port authentication protocol used in IEEE 802.1X (Port Based Network Access Control) developed to give a generic network sign-on to access network resources.

EAPoL, is a simple encapsulation that can run over any LAN. The following are the three main components defined in EAP and EAPoL to accomplish the authentication conversation:

- Supplicant—Port Authentication Entity (PAE) seeking access to network resources
- Authenticator—PAE that controls network access
- Authentication Server—RADIUS/AAA server

Event Logging

System events are activities in the system that may require attention and necessary actions to be taken in order to run the system smoothly and prevent failures. These events are recorded as logs. System Logs enable the administrator to keep track of particular events that take place on the device. Event logs are useful for network troubleshooting, debugging packet flow, and monitoring events.

F

Fast Roaming

Fast roaming between wireless access points permits a fast, secure, and uninterrupted wireless connectivity to achieve seamless mobile experience for real-time applications such as FaceTime, Skype, and Cisco Jabber.

H

HTTPS

Hyper Text Transfer Protocol Secure (HTTPS) is a transfer protocol that is more secure than HTTP. The access point can be managed through both HTTP and HTTPS connections when the HTTP/HTTPS servers are configured. Some web browsers use HTTP while others use HTTPS. An access point must have a valid Secure Socket Layer (SSL) certificate to use HTTPS service.

I

IPv4

IPv4 is a 32-bit addressing system used to identify a device in a network. It is the addressing system used in most computer networks, including the Internet.

IPv6

IPv6 is a 128-bit addressing system used to identify a device in a network. It is the successor to IPv4 and the most recent version of the addressing system used in computer networks. IPv6 is currently being rolled out around the world. An IPv6 address is represented in eight fields of hexadecimal numbers, each field containing 16 bits. An IPv6 address is divided into two parts, each part composed of 64 bits. The first part being the Network Address, and the second part the Host Address.

ISE

Identity Services Engine (ISE) is a network administration product that enables the creation and enforcement of security and access policies for endpoint devices connected to the company's routers and switches. The purpose is to simplify identity management across diverse devices and applications.

L

LLDP

Link Layer Discovery Protocol (LLDP) is a discovery protocol that is defined in the IEEE 802.1AB standard. LLDP allows network devices to advertise information about themselves to other devices on the network. LLDP uses the Logical Link Control (LLC) services to transmit and receive information to and from other LLDP agents. LLC provides a Link Service Access Point (LSAP) for access to LLDP. Each LLDP frame is transmitted as a single MAC service request. Each incoming LLDP frame is received at the MAC Service Access Point (MSAP) by the LLC entity as a MAC service indication.

Load Balancing

Load balancing is a network terminology which is used to distribute the workload across multiple computers, network links, and various other resources to achieve proper resource utilization, maximize throughput, response time, and mainly avoid the overload.

Local Probe

Local probe is the same as **Cisco Business Dashboard Probe**. This may be installed on the same host as Cisco Business Dashboard in order to manage devices on the network that is local to the Dashboard.

M

Max Data Rate

Maximum Data rate is the max speed at which data is transferred between two devices, measured in mega bits per second (Mbps or mbps)

Multiple SSIDs

You can configure several Service Set Identifiers (SSIDs) or Virtual Access Points (VAPs) on your access point and assign different configuration settings to each SSID. All the SSIDs may be active at the same time. Client devices can associate to the access point using any of the SSIDs.

N

Network Plug n Play

Network Plug and Play is a service that works in conjunction with Network Plug and Play enabled devices to allow firmware and configuration to be managed centrally, and to allow zero-touch deployment of new network devices. Devices may be deployed directly using the Network Plug and Play protocol, or indirectly if discovered by a probe that is associated with the Dashboard.

O

Operating Mode

The A2 Access points, CBW140, CBW240, CBW145 are Primary Capable and they can serve as Primary AP. CBW141, CBW142, CBW143 are Mesh Extenders. The Primary capable AP can serve as Mesh Extenders wirelessly, in addition to connecting the clients. The A2 Access Points acting as Mesh Extenders helps in extending the network coverage.

P

PMKID

Pairwise Primary Key Identifier (PMKID) is the unique key identifier used by the Access Point to keep track of the PMK being used for the client.

PoE-PD

Power Over Ethernet Powered Device. An Ethernet port that can receive power to provide network connectivity.

PoE-PSE

Power Over Ethernet Power Sourcing Equipment. An Ethernet port that can supply power and provide network connectivity.

Q

QoS

Quality of Service (QoS) allows you to prioritize traffic for different applications, users or data flows. It can also be used to guarantee performance to a specified level, thus, affecting the quality of service of the client. QoS is generally affected by the following factors: jitter, latency, and packet loss.

R

RADIUS Server

Remote Authentication Dial-In User Service (RADIUS) is an authentication mechanism for devices to connect and use a network service. It is used for centralized authentication, authorization, and accounting purposes. A RADIUS server regulates access to the network by verifying the identity of the users through the login credentials entered. For example, a public Wi-Fi network is installed in a university campus. Only those students who have the password can access these networks. The RADIUS server checks the passwords entered by the users and grants or denies access as appropriate.

Radio Domains

Based on the regulatory domain of the AP, the carrier set values will be set for both 2.4 GHz and 5GHz. For example, the radio domains for US regulatory domain is –A for 2.4GHz and –B for 5GHz.

Rogue AP Detection

A rogue Access Point (AP) is an access point that has been installed on a network without explicit authorization from a system administrator. Rogue access points pose a security threat because anyone with access to the area can knowingly or unknowingly install a wireless access point that can allow unauthorized parties to access the network. The Rogue AP Detection feature on your access point allows it to see these rogue access points that are within the range and it displays their information in the web-based utility. You can add any authorized access points to the Trusted AP List

S

Scheduler

The wireless scheduler helps to schedule a time interval for a Virtual Access Point (VAP) or radio to be operational, which helps to save power and increase security. You can associate up to 16 profiles to different VAPs or radio interfaces, but each interface is allowed only one profile. Each profile can have a certain number of time rules that control the uptime of the associated VAP or WLAN.

Signal Quality

Signal quality is a value ranging from 0 to 100, which considers, the noise generated by interference sources, along with signal strength.

Signal Strength

The signal strength is the wireless signal power level received by the wireless client. Strong signal strength results in more reliable connections and higher speeds. Signal strength is represented in -dBm format (0 to -100). This is the power ratio in decibels (dB) of the measured power referenced to one milliwatt. The closer the value is to 0, the stronger the signal. For example, -41dBm is better signal strength than -61dBm.

Spatial Streams

Wi-Fi Spatial streaming or multiplexing is a transmission technique used in multiple-input-multiple-output (MIMO) wireless communication to transmit/receive independent and separately coded data signals (which are called as streams), from each of the multiple transmit antennas.

In other words, wireless signals that are transmitted or received by the various antennae are multiplexed by using different spaces within the same spectral channel. These spaces is known as spatial streams.

Spectrum Intelligence

Spectrum intelligence scans for non-Wi-Fi radio interference on 2.4-GHz and 5-GHz bands, and provides basic functions to detect interferences of three types, namely microwave, continuous wave (like video bridge and baby monitor), Wi-Fi and frequency hopping (Bluetooth and frequency-hopping spread spectrum (FHSS) cordless phone).

SSID

The Service Set Identifier (SSID) is a unique identifier that wireless clients can connect to or share among all devices in a wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters. This is also called Wireless Network Name.

SSID Broadcast

When a wireless device searches the area for wireless networks that it can connect to, it will detect the wireless networks within its range through their network names or SSIDs. The broadcast of the SSID is enabled by default. However, you may also choose to disable it.

V

VLAN

A Virtual Local Area Network (VLAN) is a switched network that is logically segmented by function, area, or application, without regard to the physical locations of the users. VLANs are a group of hosts or ports that can be located anywhere in a network but communicate as if they are on the same physical segment. VLANs help to simplify network management by letting you move a device to a new VLAN without changing any physical connections

W

WDS

Wireless Distribution System (WDS) is a feature which enables the wireless interconnection of access points in a network. It enables the user to expand the network with multiple access points wirelessly. WDS also preserves the MAC addresses of client frames across links between access points. This capability is critical because it provides a seamless experience for roaming clients and allows management of multiple wireless networks.

WPA/WPA2

Wi-Fi Protected Access (WPA and WPA2) are security protocols used for wireless networks to protect privacy by encrypting the transmitted data over the wireless network. This uses AES type of encryption. The encryption keys that are used for each client on the network are unique and specific to that client. WPA and WPA2 are both forward compatible with IEEE 802.11e and 802.11i. WPA and WPA2 have improved authentication and encryption features compared to the Wired.

WPA2 Enterprise

This mode of security will use EAP-FAST for authenticating the Wireless clients and AES for encryption. Cisco Secure ACS server will be used as the external RADIUS server for authenticating the wireless clients.

In Enterprise mode of operation there is a mutual authentication between a client and an authentication server (Internal or External). In addition, it removes the administrative burden and security issues surrounding static encryption keys.

WPA3

Wi-Fi Protected Access 3 (WPA3) is the third iteration of a security standard or protocol developed by the Wi-Fi Alliance. WPA3 was designed to replace the WPA2 security standard, adding several security enhancements and tackling security vulnerabilities of the WPA2 to better secure personal and enterprise wireless networks. WPA3 uses a more powerful and robust encryption by AES with the GCMP (Galois/Counter Mode Protocol) and uses more reliable handshake mechanism called Simultaneous Authentication of Equals (SAE).



APPENDIX **D**

Appendix - Cisco Online Support

This appendix contains the following sections:

- [Cisco Business Online Support, on page 169](#)

Cisco Business Online Support

For current support information, visit the following URLs:

Cisco Business	
Cisco Business Home	http://www.cisco.com/go/ciscobusiness
Support	
Cisco Business Support Community	http://www.cisco.com/go/cbcommunity
Cisco Business Support and Resources	http://www.cisco.com/go/smallbizhelp
Cisco Business Phone Support	http://www.cisco.com/go/cbphone
Cisco Business Chat Support	http://www.cisco.com/go/cbchat
Cisco Business Firmware Downloads	http://www.cisco.com/go/smallbizfirmware Select a link to download the firmware for your Cisco product. No account required.
Cisco Business Open Source Requests	If you wish to receive a copy of the source code to which you are entitled under the applicable free/open source license(s) (such as the GNU Lesser General Public License), please send your request to: external-opensource-requests@cisco.com In your request, please include the Cisco product name, version, and part number (for example: 7XEEX17D99-3X49X08 1) found in the open source documentation.

