



Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points Hardware Installation Guide

First Published: 2022-05-23

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 following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

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

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

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

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

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

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

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

© 2022 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface vii

About this Guide vii

Conventions vii

Related Documentation viii

Communications, Services, and Additional Information viii

Cisco Bug Search Tool viii

CHAPTER 1

About Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points 1

Introduction to Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points 1

Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points Features 1

AP Model Numbers and Regulatory Domains 3

Antennas and Radios 3

Internal Antennas 3

CE Operating Frequency and Maximum Output Power 4

CHAPTER 2

Hardware Features 5

Access Point Views, Ports, and Connectors 5

Connectors and Ports on the AP 5

CW9164I (Internal Antenna) Radiation Patterns 5

CHAPTER 3

Unpacking Your Access Point 7

Package Contents 7

Unpacking the Access Point 7

Cisco Orderable Accessories 8

CHAPTER 4

Installation Overview 9

Performing a Pre-Installation Configuration (Optional) 9
 Preinstallation Checks and Installation Guidelines 11
 Mounting the Access Point 12
 Powering the Access Point 13

CHAPTER 5 **Configuring and Deploying the Access Point 15**

The Controller Discovery Process 15
 Deploying the Access Point on the Wireless Network 16
 Checking the Access Point LEDs 16

CHAPTER 6 **Troubleshooting 19**

Using the Mode Button 19
 Troubleshooting the Access Point to Cisco Controller Join Process 20
 Important Information for Controller-based Deployments 21
 Configuring DHCP Option 43 21

CHAPTER 7 **Safety Guidelines and Warnings 23**

Safety Instructions 23

CHAPTER 8 **Declarations of Conformity and Regulatory Information 25**

Manufacturers Federal Communication Commission Declaration of Conformity Statement 25
 VCCI Statement for Japan 26
 Guidelines for Operating Cisco Catalyst Access Points in Japan 27
 Canadian Compliance Statement 28
 Administrative Rules for Cisco Catalyst Access Points in Taiwan 30
 Operation of Cisco Catalyst Access Points in Brazil 31
 Declaration of Conformity for RF Exposure 32
 Generic Discussion on RF Exposure 32
 This Device Meets International Guidelines for Exposure to Radio Waves 32
 This Device Meets FCC Guidelines for Exposure to Radio Waves 32
 This Device Meets the Industry Canada Guidelines for Exposure to Radio Waves 33
 Additional Information on RF Exposure 34
 Declaration of Conformity Statements 34

APPENDIX A

About Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points 35

Transmit Power and Receive Sensitivity Values 35



Preface

This preface describes this guide and provides information about the conventions used in this guide, and related documentation.

It includes the following sections:

- [About this Guide, on page vii](#)
- [Conventions, on page vii](#)
- [Related Documentation, on page viii](#)
- [Communications, Services, and Additional Information, on page viii](#)

About this Guide

This guide provides instructions to install your Cisco Access Point and provides links to resources that can help you configure it. This guide also provides mounting instructions and troubleshooting information.

Note that the Cisco CW9164I access point is referred to as the access point or the AP in this document.

Conventions

This document uses the following conventions for notes, cautions, and safety warnings. Notes and cautions contain important information that you should know.



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



Caution Means *reader be careful*. Cautions contain information about something you might do that could result in equipment damage or loss of data.



Warning Safety warnings appear throughout this guide in procedures that, if performed incorrectly, can cause physical injuries. A warning symbol precedes each warning statement.

Related Documentation

All user documentation for the Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points is available at the following URL:

For detailed information and guidelines for configuring and deploying your access point in a wireless network, see the following documentation:

- Cisco 9800 Wireless Controller Configuration Guide at the following URL:

<https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-installation-and-configuration-guides-list.html>

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

About Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points

- [Introduction to Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points, on page 1](#)
- [Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points Features, on page 1](#)
- [AP Model Numbers and Regulatory Domains, on page 3](#)
- [Antennas and Radios, on page 3](#)

Introduction to Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points

The Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points is a low-power indoor (LPI) access point supporting tri-band (2.4-GHz, 5-GHz, 6-GHz), enterprise 802.11ax (Wi-Fi 6E) radios. The AP has one model with integrated antennas and is designed to use 2.4 GHz, 5 GHz, and 6 GHz, bands. The AP supports full interoperability with leading 802.11ax and 802.11ac clients and a hybrid deployment with other APs and controllers.

A full listing of the AP's features and specifications are provided in the Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points Data Sheet, at the following URL:

Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points Features

The CW9164I AP is a wireless controller-based product, and supports:

- Five radios:
 - a 4x4:4 6-GHz
 - a 4x4:4 5-GHz radio
 - a 2x2:2 2.4-GHz radio
 - a tri-band scanning radio
 - a 2.4-GHz IoT (802.15.4) radio

The Bluetooth Low Energy (BLE) uses the Omni IoT radio.

- Integrated internal antennas that are omni directional in azimuth, for 2.4-GHz, 5-GHz, and 6-GHz bands.
- Scanning radio utilizes two 2.4 GHz/5 GHz/6 GHz antennas.
- Multiuser Multiple-Input Multiple-Output (MU-MIMO) technology for uplink and downlink.
- Orthogonal Frequency Division Multiple Access (OFDMA)-based scheduling for both uplink and downlink.
- Multigigabit Ethernet (mGig)
- The following hardware external interfaces:
 - 1x100/1000/2500 Multigigabit Ethernet (RJ-45)
 - RS-232 Console Interface through RJ-45
 - Recovery push button (enables partial or full system configuration recovery)
 - USB 2.0 Port, type-A connector
 - DC power jack
 - One multi-color LED
- Integrated Bluetooth Low Energy (BLE) radio to enable IoT use cases such as location tracking and wayfinding.
- Intelligent Capture probes the network and provides Cisco DNA Center with deep analysis.
- Spatial Reuse (also known as Basic Service Set (BSS) coloring) which allows APs and their clients to differentiate between BSSs, thus permitting more simultaneous transmissions.
- Power savings mode called Target Wake Time (TWT) which allows the client to stay asleep and wake up only at pre-scheduled (target) times to exchange data with the AP. This provides significant energy savings for battery-operated devices.
- Cisco Digital Network Architecture (DNA) support enables Cisco DNA Spaces, Apple FastLane and Cisco Identity Services Engine.
- Optimized AP Roaming for ensuring that client devices associate with the AP in their coverage range that offers the fastest data rate available.
- Cisco CleanAir Pro technology enhanced with 160MHz channel support. CleanAir delivers proactive, high-speed spectrum intelligence across 20-, 40-, and 80-, and 160-MHz-wide channels to combat performance problems arising from wireless interference.

The AP supports lightweight deployments (using Cisco Wireless Controllers). The AP also supports the following operating modes:

- Local mode: This is the default mode for the Cisco AP. In this mode, the AP serves clients. In local mode, the AP creates two CAPWAP tunnels to the Cisco WLC, one for management and the other for data traffic. This is known as central switching because the data traffic is switched (bridged) from the AP to the controller where it is then routed.

- FlexConnect mode: In FlexConnect mode (previously known as HREAP), the data traffic is switched locally and is not sent to the controller. In this mode, the Cisco AP behaves like an autonomous AP, but is managed by the Cisco WLC. Here, the AP can continue to function even if connection to the controller is lost.
- Monitor mode: In this mode, specified Cisco APs can exclude themselves from handling data traffic between clients and the infrastructure. These APs act as dedicated sensors for location based services (LBS), rogue AP detection, and intrusion detection (IDS). When APs are in monitor mode, they actively monitor the airwaves and typically do not serve clients.
- Sniffer mode: In this mode, the AP starts sniffing the air on a given channel. It captures and forwards all the packets from the clients on that channel to a remote machine that runs Airopeek or Wireshark (packet analyzers for IEEE 802.11 wireless LANs). This includes information on the time stamp, signal strength, packet size, etc.
- Site Survey mode:



Note In the sniffer mode, the server to which the data is sent should be on the same VLAN as the wireless controller management VLAN otherwise an error will be displayed.

AP Model Numbers and Regulatory Domains

AP Type	Model Number	Details
Access Point for indoor environments, with internal antennas	CW9164I-x	Tri-band, controller-based 802.11ax

You need to verify whether the AP model you have is approved for use in your country. To verify approval and to identify the regulatory domain that corresponds to a particular country, visit <http://www.cisco.com/go/aironet/compliance> . Not all regulatory domains have been approved. As and when they are approved, this compliance list will be updated.



Note The 'x' in the model numbers represents the regulatory domain.

Antennas and Radios

The CW9164I access point configurations are:

- CW9164I-x

Internal Antennas

The Cisco Catalyst Wireless 9164I AP (C9164I-x) has the following list of internal antennas:

- Four internal dual-band antennas with a dedicated 2.4-GHz radio and a 5-GHz radio
- Four internal dual-band antennas with a dedicated 5-GHz radio and a 6-GHz radio
- Two tri-band antennas with a dedicated 2.4 GHz, 5-GHz and 6-GHz Aux radio
- One internal single-band antenna with a dedicated 2.4-GHz IoT radio

CE Operating Frequency and Maximum Output Power



CHAPTER 2

Hardware Features

This section describes the hardware features of Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points.

- [Access Point Views, Ports, and Connectors](#), on page 5
- [CW9164I \(Internal Antenna\) Radiation Patterns](#), on page 5

Access Point Views, Ports, and Connectors

Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points has multiple options that you can use to power the AP. For information about connectors and ports for the AP models, see [Connectors and Ports on the AP](#), on page 5.

Connectors and Ports on the AP

CW9164I (Internal Antenna) Radiation Patterns

The following illustrations show the CW9164I model with internal antenna radiation patterns:



CHAPTER 3

Unpacking Your Access Point

- [Package Contents, on page 7](#)
- [Unpacking the Access Point, on page 7](#)
- [Cisco Orderable Accessories, on page 8](#)

Package Contents

Each AP package contains the following items:

- One CW9164I AP
- Adjustable ceiling-rail clip (AIR-AP-T-RAIL-R or AIR-AP-T-RAIL-F—selected when you order the access point)
- (Optional) Mounting bracket (AIR-AP-BRACKET-1 (default) or AIR-AP-BRACKET-2, only if selected when you order the access point)
- Cisco product documentation and pointer card

Unpacking the Access Point

To unpack the access point, follow these steps:

Procedure

- Step 1** Unpack and remove the access point and the selected mounting accessory kit from the shipping box.
 - Step 2** Return any packing material to the shipping container and save it for future use.
 - Step 3** Verify that you have received all items ordered. If any item is missing or damaged, contact your Cisco representative or reseller for instructions.
-

Cisco Orderable Accessories

Order the following accessories separately from Cisco:

- AP-mounting brackets to mount the AP.

Mounting Brackets	Description
AIR-AP-BRACKET-1	For low profile installations
AIR-AP-BRACKET-2	For electrical or network boxes, above ceiling mounts
AIR-AP-T-RAIL-F	Flush ceiling grid clip
AIR-AP-T-RAIL-R	Recessed ceiling grid clip
AIR-CHNL-ADAPTER	T-RAIL channel adapter

- Power injectors when PoE is not available.

Power Supply	Description
AIR-PWRINJ7	Mid-span power injector AIR-PWRINJ7= when PoE is not available
AIR-PWRINJ6	A 802.3at power injector when PoE is not available
MA-INJ-6-x	Meraki 802.3bt PoE injector
MA-PWR-50WAC	DC Power Adapter



CHAPTER 4

Installation Overview

Installing an AP involves the following high-level tasks.

1. [Performing a Pre-Installation Configuration \(Optional\), on page 9](#)
2. [Preinstallation Checks and Installation Guidelines, on page 11](#)
3. [Mounting the Access Point, on page 12](#)
4. [Powering the Access Point, on page 13](#)
 - [Performing a Pre-Installation Configuration \(Optional\), on page 9](#)
 - [Preinstallation Checks and Installation Guidelines, on page 11](#)
 - [Mounting the Access Point, on page 12](#)
 - [Powering the Access Point, on page 13](#)

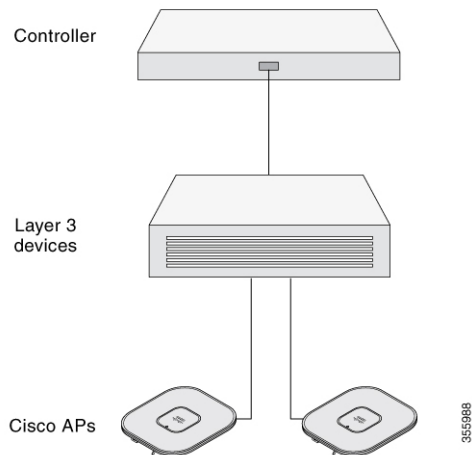
Performing a Pre-Installation Configuration (Optional)

The following procedures ensure that your access point installation and initial operation go as expected. This procedure is optional.



Note Performing a pre-installation configuration is an optional procedure. If your network controller is properly configured, you can install your access point in its final location and connect it to the network from there. For more information, see [Deploying the Access Point on the Wireless Network, on page 16](#).

The pre-installation configuration setup is illustrated in the following illustration:



To perform pre-installation configuration, perform the following steps:

Procedure

Step 1

Ensure that the Cisco Controller Distribution System port is connected to the network. Use the procedure for CLI or web-browser interface as described in the release appropriate [Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide](#).

- a) Ensure that the access points have Layer 3 connectivity to the Cisco Controller Management and AP-Manager Interface.
- b) Configure the switch to which your access point is to attach. See the [Cisco Wireless Controller Configuration Guide](#) for the release you are using, for additional information.
- c) Set the Cisco controller as the master so that new access points always join with it.
- d) Ensure DHCP is enabled on the network. The access point must receive its IP address through DHCP.

Note An 802.11ax Cisco AP will be assigned an IP address from the DHCP server only if a default router (gateway) is configured on the DHCP server (enabling the AP to receive its gateway IP address) and the gateway ARP is resolved.

- e) CAPWAP UDP ports must not be blocked in the network.
- f) The access point must be able to find the IP address of the controller. This can be accomplished using DHCP, DNS, or IP subnet broadcast. This guide describes the DHCP method to convey the controller IP address. For other methods, refer to the product documentation. See also the [Configuring DHCP Option 43, on page 21](#) for more information.

Note The access point requires a multi-gigabit Ethernet (5Gbps) link to prevent the Ethernet port from becoming a bottleneck for traffic.

Step 2

Apply power to the access point. See [Powering the Access Point, on page 13](#).

- a) As the access point attempts to connect to the controller, the LED cycles through a green, red, and off sequence, which can take up to 5 minutes.

Note If the access point remains in this mode for more than five minutes, the access point is unable to find the Master Cisco Wireless Controller. Check the connection between the access point and the Cisco Wireless Controller and be sure that they are on the same subnet.

- b) If the access point shuts down, check the power source.
- c) After the access point finds the Cisco Wireless Controller, it attempts to download the new operating system code if the access point code version differs from the Cisco Wireless Controller code version. While this is happening, the Status LED blinks blue.
- d) If the operating system download is successful, the access point reboots.

Step 3 Configure the access point if required. Use the controller CLI, controller GUI, or Cisco DNA Spaces to customize the access-point-specific 802.11ax network settings.

Step 4 If the pre-installation configuration is successful, the Status LED is green indicating normal operation. Disconnect the access point and mount it at the location at which you intend to deploy it on the wireless network.

Step 5 If your AP does not indicate normal operation, turn it off and repeat the pre-installation configuration.

Note When you are installing a Layer 3 access point on a different subnet than the Cisco controller, be sure that a DHCP server is reachable from the subnet on which you will be installing the access point, and that the subnet has a route back to the Cisco controller. Also be sure that the route back to the Cisco controller has destination UDP ports 5246 and 5247 open for CAPWAP communications. Ensure that the route back to the primary, secondary, and tertiary controller allows IP packet fragments. Finally, be sure that if address translation is used, that the access point and the Cisco controller have a static 1-to-1 NAT to an outside address. (Port Address Translation is not supported.)

Preinstallation Checks and Installation Guidelines

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: below a suspended ceiling, on a flat horizontal surface, or on a desk top



Note You can mount the access point above a suspended ceiling but you must purchase additional mounting hardware: For more information, see [Mounting the Access Point, on page 12](#).

- Access point power options: You may use either of the following two options to power the AP.
 - Cisco approved power injector
 - Power over Ethernet (PoE) with a supporting switch



Note The UL approved Listed Power Adapter must meet the following minimum specifications: Rated output of 42.5-57 Vdc, min. 1.11A, Tma is 50°C minimum, Altitude is 3048m minimum.



Note If 802.3af is used, all radios get switched off. Ethernet gets downgraded to 1 GbE. The USB port will also be off.

- Operating temperature:
 - CW9164I: 32°-122°F (0°-50°C)



Note When installing the AP in an environment where the ambient temperature is in the range of 104°-122°F (>40°-50°C), the access point configuration will change from 4x4 on the 5 GHz radios and the uplink Ethernet will downgrade to 1GbE. However, the USB port will remain enabled.

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 the Access Point

Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points can be mounted in several configurations:

- Suspended ceiling
- Hard ceiling
- Wall
- Electrical or network box
- Above a suspended ceiling
- Desk mount

For access point mounting instructions, go to the following URL:

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/mounting/guide/apmount.html

The standard mounting hardware supported by the AP is listed in .

Table 1: Brackets and Clips for Mounting the AP

Mounting Type	Part Number	Description
Brackets ¹²³	AIR-AP-BRACKET-1	Low-profile bracket—Used for ceiling mount installations(This is the default option.)
	AIR-AP-BRACKET-2	Universal bracket—Used for wall or electrical box installations.

Mounting Type	Part Number	Description
Clips	AIR-AP-T-RAIL-R	Ceiling Grid Clip (Recessed mounting)(This is the default option)
	AIR-AP-T-RAIL-F	Ceiling Grid Clip (Flush mounting)
	AIR-CHNL-ADAPTER	Optional adapter for channel-rail ceiling grid profile.
Desk mount		Desk mount rubber feet using screw size 8-32x.28"

- ¹ Mount the AP using no less than four screw holes on a bracket.
- ² AIR-AP-BRACKET-3 is not compatible for use with Cisco Catalyst Wireless 9164I access points.
- ³ You can also use “in-tile” mounting options available from third parties. For more information, visit the access point data sheet available on Cisco.com at <https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/nb-06-cat-9130-ser-ap-ds-cte-en.html>

When mounting the AP in areas where there is a possibility of the AP being knocked off the mounting bracket, use the lock hasp on the back of the AP to lock it to the bracket.

Powering the Access Point



Caution Ensure that the AP is powered using a UL-compliant PoE power source. You must connect the unit only to PoE network without routing to the outside plant.

The AP can be powered only through Power-over-Ethernet (PoE) using the following:

- 802.3bt: Any 802.3bt compliant switch port or Cisco Power Injector AIR-PWRINJ7=
- Cisco Universal PoE (Cisco UPOE)
- 802.3at (PoE+): Any 802.3at (30.0 W) compliant switch port
- 802.3af: Any 802.3af (15.4 W) compliant switch port



Note If 802.3af is used, all radios get switched off. Ethernet port gets downgraded to 1 GbE and the USB port is shutoff.



CHAPTER 5

Configuring and Deploying the Access Point

This section describes how to connect the AP to a controller. For instructions on how to configure the AP, see the relevant release's *Cisco Wireless Controller Configuration Guide*.

- [The Controller Discovery Process, on page 15](#)
- [Deploying the Access Point on the Wireless Network, on page 16](#)
- [Checking the Access Point LEDs, on page 16](#)

The Controller Discovery Process

To support CW9164I AP, the controller must be running release IOS-XE 17.9.1 or later. For more information, visit the access point data sheet available on Cisco.com at

Guidelines and Limitations

- You cannot edit or query any access point using the controller CLI if the name of the access point contains a space.
- Make sure that the controller is set to the current time. If the controller is set to a time that has already occurred, the access point might not join the controller because its certificate may not be valid for that time.

The controller must discover AP before it can become an active part of the network. The AP supports the following controller discovery processes:

- Locally stored controller IP address discovery—If the access point was previously joined to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point non-volatile memory. This process of storing controller IP addresses on an access point for later deployment is called priming the access point. For more information about priming, see the [Performing a Pre-Installation Configuration \(Optional\), on page 9](#).
- DHCP server discovery—This feature uses DHCP option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability. For more information about DHCP option 43, see the [Configuring DHCP Option 43, on page 21](#).
- DNS discovery—The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-CAPWAP-CONTROLLER.localdomain, where localdomain is the access point domain name. Configuring the CISCO-CAPWAP-CONTROLLER provides backwards compatibility in an existing

customer deployment. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.localdomain. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.

Deploying the Access Point on the Wireless Network

After you have mounted the access point, follow these steps to deploy it on the wireless network:

Procedure

Step 1 Connect and power up the access point.

Step 2 Observe the access point LED.

For LED status descriptions, see [Checking the Access Point LEDs, on page 16](#).

- a) When you power up the access point, it begins a power-up sequence that you can verify by observing the access point LED. If the power-up sequence is successful, the discovery and join process begins. During this process, the LED blinks sequentially green, red, and off. When the access point has joined a controller, the LED is green if no clients are associated or blue if one or more clients are associated.
- b) If the LED is not on, the access point is most likely not receiving power.
- c) If the LED blinks sequentially for more than 5 minutes, the access point is unable to find its primary, secondary, and tertiary Cisco Wireless Controller. Check the connection between the access point and the Cisco Wireless Controller, and be sure the access point and the Cisco Wireless Controller are either on the same subnet or that the access point has a route back to its primary, secondary, and tertiary Cisco Wireless Controller. Also, if the access point is not on the same subnet as the Cisco Wireless Controller, be sure that there is a properly configured DHCP server on the same subnet as the access point.

For additional information, see [Configuring DHCP Option 43, on page 21](#).

Step 3 Reconfigure the Cisco Wireless Controller so that it is not the master.

Note A master Cisco Wireless Controller should be used only for configuring access points and not in a working network.

Checking the Access Point LEDs

The location of the access point status LED is shown in [#unique_17 unique_17_Connect_42_ap_face_view](#).



Note Regarding LED status colors, it is expected that there will be small variations in color intensity and hue from unit to unit. This is within the normal range of the LED manufacturer's specifications and is not a defect. However, the intensity of the LED can be changed through the controller.

The access point status LED indicates various conditions and are described in [Table 2: LED Status Indications, on page 17](#).

Table 2: LED Status Indications

Message Type	LED State	Message Meaning
Association status	Green	Normal operating condition, but no wireless client associated
	Blue	Normal operating condition, at least one wireless client association
Boot loader status	Green	Executing boot loader
Boot loader error	Blinking Green	Boot loader signing verification failure
Operating status	Blinking Blue	Software upgrade in progress
	Alternating between Green and Red	Discovery/join process in progress
Access point operating system errors	Cycling through Red-Off-Green-Off-Blue-Off	General warning; insufficient inline power



CHAPTER 6

Troubleshooting

- [Using the Mode Button, on page 19](#)
- [Troubleshooting the Access Point to Cisco Controller Join Process, on page 20](#)
- [Important Information for Controller-based Deployments, on page 21](#)
- [Configuring DHCP Option 43, on page 21](#)

Using the Mode Button

Using the Mode button (see [#unique_17 unique_17_Connect_42_ap_top_connectors](#)) you can:

- Reset the AP to the default factory-shipped configuration.
- Clear the AP internal storage, including all configuration files.

To use the mode button, press, and keep pressed, the mode button on the access point during the AP boot cycle. Wait until the AP console shows a seconds counter. Once the counter indicates the number of seconds the mode button is pressed, the AP status LED changes to blinking red. Then:

- To reset the AP to the default factory-shipped configuration, keep the mode button pressed for less than 20 seconds. The AP configuration files are cleared.

This resets all configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID.

- To clear the AP internal storage, including all configuration files, keep the mode button pressed for more than 20 seconds, but less than 60 seconds.



Note If the mode button is pressed for more than 30 seconds but less than 60 seconds, the FIPS mode flag is also cleared during the full factory reset of the AP. The FIPS flag when set disables console access.

The AP status LED changes from Blue to Red, and all the files in the AP storage directory are cleared.

If you keep the mode button pressed for more than 60 seconds, the mode button is assumed faulty and no changes are made.

Troubleshooting the Access Point to Cisco Controller Join Process



Note As specified in the Cisco Wireless Solutions Software Compatibility Matrix, ensure that your controller is running controller software release IOS-XE 17.9.1 or later to support Cisco CW9164I AP.

Access points can fail to join a controller for many reasons: a RADIUS authorization is pending; self-signed certificates are not enabled on the controller; the access point and the controller regulatory domains do not match, and so on.

Controller software enables you to configure the access points to send all CAPWAP-related errors to a syslog server. You do not need to enable any debug commands on the controller because all of the CAPWAP error messages can be viewed from the syslog server itself.

The state of the access point is not maintained on the controller until it receives a CAPWAP join request from the access point. Therefore, it can be difficult to determine why the CAPWAP discovery request from a certain access point was rejected. In order to troubleshoot such joining problems without enabling CAPWAP debug commands on the controller, the controller collects information for all access points that send a discovery message to it and maintains information for any access points that have successfully joined it.

The controller collects all join-related information for each access point that sends a CAPWAP discovery request to the controller. Collection begins with the first discovery message received from the access point and ends with the last configuration payload sent from the controller to the access point.

When the controller is maintaining join-related information for the maximum number of access points, it does not collect information for any more access points.

An access point sends all syslog messages to IP address 255.255.255.255 by default.

You can also configure a DHCP server to return a syslog server IP address to the access point using option 7 on the server. The access point then starts sending all syslog messages to this IP address.

When the access point joins a controller for the first time, the controller sends the global syslog server IP address (the default is 255.255.255.255) to the access point. After that, the access point sends all syslog messages to this IP address until it is overridden by one of the following scenarios:

- The access point is still connected to the same controller, and the global syslog server IP address configuration on the controller has been changed using the `config ap syslog host global syslog_server_IP_address` command. In this case, the controller sends the new global syslog server IP address to the access point.
- The access point is still connected to the same controller, and a specific syslog server IP address has been configured for the access point on the controller using the `config ap syslog host specific Cisco_AP syslog_server_IP_address` command. In this case, the controller sends the new specific syslog server IP address to the access point.
- The access point is disconnected from the controller and joins another controller. In this case, the new controller sends its global syslog server IP address to the access point.
- Whenever a new syslog server IP address overrides the existing syslog server IP address, the old address is erased from persistent storage, and the new address is stored in its place. The access point also starts

sending all syslog messages to the new IP address provided the access point can reach the syslog server IP address.

You can configure the syslog server for access points and view the access point join information only from the controller CLI.

Important Information for Controller-based Deployments

Keep these guidelines in mind when you use Cisco CW9164I Series AP:

- The access point can only communicate with Cisco wireless controllers.
- The access point does not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point joins it.
- CAPWAP does not support Layer 2. The access point must get an IP address and discover the controller using Layer 3, DHCP, DNS, or IP subnet broadcast.
- The access point console port is enabled for monitoring and debug purposes. All configuration commands are disabled when the access point is connected to a controller.

Configuring DHCP Option 43

You can use DHCP Option 43 to provide a list of controller IP addresses to the access points, enabling them to find and join a controller.

The following is a DHCP Option 43 configuration example on a Windows 2003 Enterprise DHCP server for use with Cisco Catalyst lightweight access points. For other DHCP server implementations, consult product documentation for configuring DHCP Option 43. In Option 43, you should use the IP address of the controller management interface.



Note DHCP Option 43 is limited to one access point type per DHCP pool. You must configure a separate DHCP pool for each access point type.

The Cisco CW9164I Series access point uses the type-length-value (TLV) format for DHCP Option 43. DHCP servers must be programmed to return the option based on the access point DHCP Vendor Class Identifier (VCI) string (DHCP Option 43). The VCI string for the Cisco CW9164I access point is:

Cisco AP CW9164I

The format of the TLV block is listed below:

- Type—0xf1 (decimal 241)
- Length—Number of controller IP addresses * 4
- Value—IP addresses of the WLC management interfaces listed sequentially in hex

To configure DHCP Option 43 in the embedded Cisco IOS DHCP server, follow these steps:

Procedure

- Step 1** Enter configuration mode at the Cisco IOS CLI.
- Step 2** Create the DHCP pool, including the necessary parameters such as default router and name server. A DHCP scope example is as follows:

Example:

```
ip dhcp pool <pool name>
network <IP Network> <Netmask>
default-router <Default router>
dns-server <DNS Server>
```

Where:

Example:

<pool name> is the name of the DHCP pool, such as AP916xI
<IP Network> is the network IP address where the controller resides, such as 10.0.15.1
<Netmask> is the subnet mask, such as 255.255.255.0
<Default router> is the IP address of the default router, such as 10.0.0.1
<DNS Server> is the IP address of the DNS server, such as 10.0.10.2

- Step 3** Add the option 43 line using the following syntax:

Example:

```
option 43 hex <hex string>
```

The hex string is assembled by concatenating the TLV values shown below:

Type + Length + Value

For example, suppose that there are two controllers with management interface IP addresses, 10.126.126.2 and 10.127.127.2. The type is f1(hex). The length is $2 * 4 = 8 = 08$ (hex). The IP addresses translate to 0a7e7e02 and 0a7f7f02. Assembling the string then yields f1080a7e7e020a7f7f02. The resulting Cisco IOS command added to the DHCP scope is option 43 hex f1080a7e7e020a7f7f02.



CHAPTER 7

Safety Guidelines and Warnings

- [Safety Instructions, on page 23](#)

Safety Instructions

Translated versions of the following safety warnings are provided in the translated safety warnings document that is shipped with your access point. The translated warnings are also in the Translated Safety Warnings for Cisco Catalyst Access Points, which is available on Cisco.com.



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



Danger **Read the installation instructions before using, installing or connecting the system to the power source.** Statement 1004



Danger **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than 20A.** Statement 1005



Danger **Installation of the equipment must comply with local and national electrical codes.** Statement 1074



Danger **In order to comply with FCC radio frequency (RF) exposure limits, antennas should be located at a minimum of 16.14 inches (41 cm) or more from the body of all persons.** Statement 332



Danger Ultimate disposal of this product should be handled according to all national laws and regulations. Statement 1040



Danger This equipment is suitable for use in environment air spaces (plenums) in accordance with Section 300.22 (C) of the National Electrical Code, and Sections 2-128, 12-010(3) and 12-100 of the Canadian Electrical Code, Part 1, CSA C22.2. External power supply, power adapter and/or power injector, if provided, are not suitable for installation in air spaces. Statement 440



Caution Ensure to connect the power cord of the power adapter to a socket outlet with an earthing connection.



CHAPTER 8

Declarations of Conformity and Regulatory Information

This section provides declarations of conformity and regulatory information for the Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points. You can find additional information at this URL: <http://www.cisco.com/go/aironet/compliance>.

- [Manufacturers Federal Communication Commission Declaration of Conformity Statement, on page 25](#)
- [VCCI Statement for Japan, on page 26](#)
- [Canadian Compliance Statement, on page 28](#)
- [Administrative Rules for Cisco Catalyst Access Points in Taiwan, on page 30](#)
- [Operation of Cisco Catalyst Access Points in Brazil, on page 31](#)
- [Declaration of Conformity for RF Exposure, on page 32](#)
- [Declaration of Conformity Statements, on page 34](#)

ManufacturersFederalCommunicationCommissionDeclaration of Conformity Statement



Access Point Models	Certification Number
Cisco CW9164I-B	LDK-9160S2578

Manufacturer:

Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA

This device complies with Part 15 rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits of a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, uses, and radiates radiofrequency energy, and if not installed and used according to the instructions, it may cause harmful interference. Hence, professional installation is recommended. However, there is no guarantee that interference will not occur. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna
- Increase separation between the equipment and receiver
- Connect the equipment to an outlet on a circuit different from which the receiver is connected
- Consult the dealer or an experienced radio/TV technician


Caution

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter. For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible. FCC regulations restrict the operation of this device to indoor use only. The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet. Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

VCCI Statement for Japan

	<p>Warning This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.</p>
<p>警告</p>	<p>Warning この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。</p> <p style="text-align: right;">VCCI-B</p>

Access Point Models:

CW9164I-Q

Guidelines for Operating Cisco Catalyst Access Points in Japan

This section provides guidelines for avoiding interference when operating Cisco Catalyst access points in Japan. These guidelines are provided in both Japanese and English.

この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。

- 1 この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。
- 2 万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先にご連絡頂き、混信回避のための処置等(例えば、パーティションの設置など)についてご相談して下さい。
- 3 その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。

連絡先 : 03-6434-6500

208697

English Translation

This equipment operates in the same frequency bandwidth as industrial, scientific, and medical devices such as microwave ovens and mobile object identification (RF-ID) systems (licensed premises radio stations and unlicensed specified low-power radio stations) used in factory production lines.

1. Before using this equipment, make sure that no premises radio stations or specified low-power radio stations of RF-ID are used in the vicinity.
2. If this equipment causes RF interference to a premises radio station of RF-ID, promptly change the frequency or stop using the device; contact the number below and ask for recommendations on avoiding radio interference, such as setting partitions.
3. If this equipment causes RF interference to a specified low-power radio station of RF-ID, contact the number below.

Contact Number: **03-6434-6500**

Statement 371—Power Cable and AC Adapter

接続ケーブル、電源コード、ACアダプタ、バッテリーなどの部品は、必ず添付品または指定品をご使用ください。添付品・指定品以外の部品をご使用になると故障や動作不良、火災の原因となります。また、電気用品安全法により、当該法の認定（PSEとコードに表記）でなくUL認定（ULまたはCSAマークがコードに表記）の電源ケーブルは弊社が指定する製品以外の電気機器には使用できないためご注意ください。

English Translation

When installing the product, please use the provided or designated connection cables/power cables/AC adapters. Using any other cables/adapters could cause a malfunction or a fire. Electrical Appliance and Material

Safety Law prohibits the use of UL-certified cables (that have the “UL” shown on the code) for any other electrical devices than products designated by CISCO. The use of cables that are certified by Electrical Appliance and Material Safety Law (that have “PSE” shown on the code) is not limited to CISCO-designated products.

Canadian Compliance Statement

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada’s license-exempt RSS(s). Operation is subject to the following two conditions:

- This device may not cause interference.
- This device must accept any interference, including interference that may cause undesired operation of the device.

L’émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d’Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence.

L’exploitation est autorisée aux deux conditions suivantes:

- L’appareil ne doit pas produire de brouillage.
- L’appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d’en compromettre le fonctionnement.

Wi-Fi 6E Device

- Operation shall be limited to indoor use only.
- Operation on oil platforms, cars, trains, boats and aircraft shall be prohibited except for on large aircraft flying above 10,000 ft.

appareil Wi-Fi 6E

- Utilisation limitée à l’intérieur seulement.
- Utilisation interdite à bord de plateformes de forage pétrolier, de voitures, de trains, de bateaux et d’aéronefs, sauf à bord d’un gros aéronef volant à plus de 10 000 pieds d’altitude.

Table 3: List of Internal Antennas Supported on Cisco CW9164I AP

Antenna Type	Antenna Gain	Antenna Impedance
Single-Port Dual-Band Omni-Directional (Vertical Polarization)	2.4 GHz—3dBi 5 GHz—5dBi	50 ohms
Single-Port Dual-Band Omni-Directional (Vertical Polarization)	2.4 GHz—3dBi 5 GHz—5dBi	50 ohms
Single-Port Single-Band Omni-Directional (Vertical Polarization)	5 GHz—5dBi	50 ohms

Antenna Type	Antenna Gain	Antenna Impedance
Single-Port Single-Band Omni-Directional (Vertical Polarization)	5 GHz—5dBi	50 ohms
Single-Port Single-Band Omni-Directional (Horizontal Polarization)	6 GHz—4dBi	50 ohms
Single-Port Single-Band Omni-Directional (Horizontal Polarization)	6 GHz—4dBi	50 ohms
Single-Port Single-Band Omni-Directional (Horizontal Polarization)	6 GHz—4dBi	50 ohms
Single-Port Single-Band Omni-Directional (Horizontal Polarization)	6 GHz—4dBi	50 ohms
Single-Port Tri-Band Omni-Directional (Linear Polarization, Auxiliary)	2.4 GHz—3dBi 5 GHz—4dBi 6 GHz—5dBi	50 ohms
Single-Port Tri-Band Omni-Directional (Linear Polarization, Auxiliary)	2.4 GHz—3dBi 5 GHz—4dBi 6 GHz—5dBi	50 ohms
Single-Port Single-Band Omni-Directional (Linear Polarization, BLE)	3dBi	50 ohms

The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

The transmitter module may not be co-located with any other transmitter or antenna.

Le module émetteur peut ne pas être coimplanté avec un autre émetteur ou antenne.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.

Industry Canada**Access Point Models:**

CW9164I-A

Access Point Model	Certification Number
CW9164I-A	2461N-9160S2578

European Union

The product carries the CE Mark:



The device is restricted to indoor use only when operating between 5945 MHz and 6425 MHz frequency range.

This equipment complies with EU radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.



Note This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. For more details, contact Cisco Corporate Compliance.

Access Point Models:

CW9164I-E

Importer:

Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA

United Kingdom

The device is restricted to indoor use only when operating between 5925 MHz and 6425 MHz frequency range.

Access Point Models:

CW9164I-ROW

Importer:

Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA

Administrative Rules for Cisco Catalyst Access Points in Taiwan

This section provides administrative rules for operating Cisco Catalyst access points in Taiwan. The rules for all access points are provided in both Simplified Chinese and English.

Simplified Chinese Translation

【低功率射頻器材技術規範】取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫用電波輻射性電機設備之干擾。應避免影響附近雷達系統之操作。

English Translation

Without permission granted by the NCC, any company, enterprise, or user is not allowed to change frequency, enhance transmitting power or alter original characteristic as well as performance to a approved low power radio-frequency devices. The low power radio-frequency devices shall not influence aircraft security and interfere legal communications; If found, the user shall cease operating immediately until no interference is achieved. The said legal communications means radio communications is operated in compliance with the Telecommunications Management Act. The low power radio-frequency devices must be susceptible with the interference from legal communications or ISM radio wave radiated devices.

The operations near the radar system shall not be influenced.

This section contains special information for operation of Cisco Catalyst access points in Taiwan.

Access Point Models	Certification Number
CW9164I-ROW	XXXXX-XX-XXXXX

Operation of Cisco Catalyst Access Points in Brazil

Figure 1: Brazil Regulatory Information



Portuguese Translation

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados.

English Translation

This equipment is not entitled to the protection from harmful interference and may not cause interference with duly authorized systems.

This section contains special information for operation of Cisco Catalyst access points in Brazil.

Access Point Models	Certification Number
CW9164I-ROW	XXXXX-XX-XXXXX

Declaration of Conformity for RF Exposure

This section contains information on compliance with guidelines related to RF exposure.

Generic Discussion on RF Exposure

The Cisco products are designed to comply with the following national and international standards on Human Exposure to Radio Frequencies:

- US 47 Code of Federal Regulations Part 2 Subpart J
- American National Standards Institute (ANSI) / Institute of Electrical and Electronic Engineers / IEEE C 95.1 (99)
- International Commission on Non Ionizing Radiation Protection (ICNIRP) 98
- Ministry of Health (Canada) Safety Code 6. Limits on Human Exposure to Radio Frequency Fields in the range from 3kHz to 300 GHz
- Australia Radiation Protection Standard

To ensure compliance with various national and international Electromagnetic Field (EMF) standards, the system should only be operated with Cisco approved antennas and accessories.

This Device Meets International Guidelines for Exposure to Radio Waves

The Cisco CW9164I series device includes a radio transmitter and receiver. It is designed not to exceed the limits for exposure to radio waves (radio frequency electromagnetic fields) recommended by international guidelines. The guidelines were developed by an independent scientific organization (ICNIRP) and include a substantial safety margin designed to ensure the safety of all persons, regardless of age and health.

As such the systems are designed to be operated as to avoid contact with the antennas by the end user. It is recommended to set the system in a location where the antennas can remain at least a minimum distance as specified from the user in accordance to the regulatory guidelines which are designed to reduce the overall exposure of the user or operator.

Separation Distance
20 cm (7.87 inches)

The World Health Organization has stated that present scientific information does not indicate the need for any special precautions for the use of wireless devices. They recommend that if you are interested in further reducing your exposure then you can easily do so by reorienting antennas away from the user or placing he antennas at a greater separation distance then recommended.

This Device Meets FCC Guidelines for Exposure to Radio Waves

The Cisco CW9164I series device includes a radio transmitter and receiver. It is designed not to exceed the limits for exposure to radio waves (radio frequency electromagnetic fields) as referenced in FCC Part 1.1310. The guidelines are based on IEEE ANSI C 95.1 (92) and include a substantial safety margin designed to ensure the safety of all persons, regardless of age and health.

As such the systems are designed to be operated as to avoid contact with the antennas by the end user. It is recommended to set the system in a location where the antennas can remain at least a minimum distance as specified from the user in accordance to the regulatory guidelines which are designed to reduce the overall exposure of the user or operator.

The device has been tested and found compliant with the applicable regulations as part of the radio certification process.

Separation Distance
41 cm (16.14 inches)

The US Food and Drug Administration has stated that present scientific information does not indicate the need for any special precautions for the use of wireless devices. The FCC recommends that if you are interested in further reducing your exposure then you can easily do so by reorienting antennas away from the user or placing the antennas at a greater separation distance than recommended or lowering the transmitter power output.

This Device Meets the Industry Canada Guidelines for Exposure to Radio Waves

The Cisco CW9164I series device includes a radio transmitter and receiver. It is designed not to exceed the limits for exposure to radio waves (radio frequency electromagnetic fields) as referenced in Health Canada Safety Code 6. The guidelines include a substantial safety margin designed into the limit to ensure the safety of all persons, regardless of age and health.

As such the systems are designed to be operated as to avoid contact with the antennas by the end user. It is recommended to set the system in a location where the antennas can remain at least a minimum distance as specified from the user in accordance to the regulatory guidelines which are designed to reduce the overall exposure of the user or operator.

Table 4: Separation Distance

Frequency	Distance
2.4-GHz	20 cm (7.87 inches)
5-GHz	
6-GHz	

Health Canada states that present scientific information does not indicate the need for any special precautions for the use of wireless devices. They recommend that if you are interested in further reducing your exposure you can easily do so by reorienting antennas away from the user, placing the antennas at a greater separation distance than recommended, or lowering the transmitter power output.

Cet appareil est conforme aux directives internationales en matière d'exposition aux fréquences radioélectriques

Cet appareil de la gamme Cisco CW9164I comprend un émetteur-récepteur radio. Il a été conçu de manière à respecter les limites en matière d'exposition aux fréquences radioélectriques (champs électromagnétiques de fréquence radio), recommandées dans le code de sécurité 6 de Santé Canada. Ces directives intègrent une marge de sécurité importante destinée à assurer la sécurité de tous, indépendamment de l'âge et de la santé.

Par conséquent, les systèmes sont conçus pour être exploités en évitant que l'utilisateur n'entre en contact avec les antennes. Il est recommandé de poser le système là où les antennes sont à une distance minimale telle que précisée par l'utilisateur conformément aux directives réglementaires qui sont conçues pour réduire l'exposition générale de l'utilisateur ou de l'opérateur.

Table 5: Distance d'éloignement

Fréquence	Distance
2.4-GHz	20 cm (7.87 inches)
5-GHz	
6-GHz	

Santé Canada affirme que la littérature scientifique actuelle n'indique pas qu'il faille prendre des précautions particulières lors de l'utilisation d'un appareil sans fil. Si vous voulez réduire votre exposition encore davantage, selon l'agence, vous pouvez facilement le faire en réorientant les antennes afin qu'elles soient dirigées à l'écart de l'utilisateur, en les plaçant à une distance d'éloignement supérieure à celle recommandée ou en réduisant la puissance de sortie de l'émetteur.

Additional Information on RF Exposure

You can find additional information on the subject at the following links:

- Cisco Systems Spread Spectrum Radios and RF Safety white paper at this URL:
http://www.cisco.com/warp/public/cc/pd/witc/ao340ap/prodlit/rfhr_wi.htm
- FCC Bulletin 56: Questions and Answers about Biological Effects and Potential Hazards of Radio Frequency Electromagnetic Fields
- FCC Bulletin 65: Evaluating Compliance with the FCC guidelines for Human Exposure to Radio Frequency Electromagnetic Fields

You can obtain additional information from the following organizations:

- World Health Organization Internal Commission on Non-Ionizing Radiation Protection
- United Kingdom, National Radiological Protection Board
- Cellular Telecommunications Association at this URL:
<https://www.ctia.org>
- The Mobile & Wireless Forum at this URL:
<https://www.mwfai.org>

Declaration of Conformity Statements

All the Declaration of Conformity statements related to this product can be found at the following location:

<https://pas.cisco.com/pdenc/#/>



APPENDIX **A**

About Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points

- [Transmit Power and Receive Sensitivity Values, on page 35](#)

Transmit Power and Receive Sensitivity Values

