



Cisco Catalyst IW9167E Heavy Duty Access Point Hardware Installation Guide

First Published: 2022-12-08

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



CONTENTS

PREFACE

Preface **vii**

About this Guide **vii**

Conventions **vii**

Related Documentation **viii**

Communications, Services, and Additional Information **viii**

 Cisco Bug Search Tool **viii**

 Documentation Feedback **viii**

CHAPTER 1

About Cisco Catalyst IW9167E Heavy Duty Access Point **1**

Introduction to Cisco Catalyst IW9167E Heavy Duty Access Point **1**

Cisco Catalyst IW9167E Heavy Duty Access Point Features **1**

Connectors and Ports **2**

Power Sources **3**

 Power Adapters **3**

 Power Injectors **3**

 Ethernet (PoE) Ports **4**

Antennas and Radios **4**

 Supported External Antennas **4**

CHAPTER 2

Unpacking Your Access Point **9**

Package Contents **9**

Unpacking the Access Point **9**

Cisco Orderable Accessories **9**

CHAPTER 3

Installation Overview **13**

Performing a Preinstallation Configuration (Optional) **13**

Preinstallation Checks and Installation Guidelines	15
Mounting the Access Point	16
Mounting Hardware	16
Mounting Bracket Part Numbers	16
Using the Integrated Flange Mounts	16
Using the DIN Rail Mounting Bracket	18
Using the Pole Mounting Bracket	20
Using the Mounting Bracket AIR-ACCPMK3700=	20
Using the Mounting Bracket AIR-ACCPMK3700-2=	21
Attaching a Power Adapter	26
Attaching a Power Adapter Using the Mounting Bracket AIR-ACCPMK3700=	26
Attaching a Power Adapter Using the Mounting Bracket AIR-ACCPMK3700-2=	27
Installing a Lightning Arrestor	28
Lightning Arrestor Installation Notes	29
Grounding the Access Point	30
Powering the Access Point	31
Connecting a Power Injector	32
Connecting a DC Power Cable to the Access Point	32
Connecting Data Cables	33
Connecting an Ethernet Cable to the Access Point	34
Connecting a Fiber-optic Cable to the AP (AIR-SFP-KIT1=)	34

CHAPTER 4 **Configuring and Deploying the Access Point** 37

Controller Discovery Process	37
Deploying the Access Point in a Wireless Network	38
Checking the Access Point LEDs	38

CHAPTER 5 **Troubleshooting** 41

Using the Reset Button	41
Troubleshooting the Access Point to Controller Join Process	42
Important Information for Controller-based Deployments	42
Configuring DHCP Option 43	42

CHAPTER 6 **Safety Guidelines and Warnings** 45

FCC Safety Compliance Statement	45
Safety Precautions	45
Safety Precautions when Installing Antennas	46
Avoiding Damage to Radios in a Testing Environment	47
Performing Site Surveys	48

CHAPTER 7

Declarations of Conformity and Regulatory Information 49

Manufacturers Federal Communication Commission Declaration of Conformity Statement	49
Operation of Cisco Catalyst Access Points in México	50
VCCI Statement for Japan	50
Statement 191—Voluntary Control Council for Interference (VCCI) Class A Warning for Japan	50
ステートメント 191—日本向け VCCI クラス A に関する警告	51
Guidelines for Operating Cisco Catalyst Access Points in Japan	51
Compliance Statement for Canada	52
Industry Canada	52
European Community, Switzerland, Norway, Iceland, and Liechtenstein	53
Operation of Cisco Catalyst Access Points in Brazil	53
Declaration of Conformity for RF Exposure	54
Generic Discussion on RF Exposure	54
This Device Meets International Guidelines for Exposure to Radio Waves	55
This Device Meets FCC Guidelines for Exposure to Radio Waves	55
This Device Meets the Industry Canada Guidelines for Exposure to Radio Waves	56
Cet appareil est conforme aux directives internationales en matière d'exposition aux fréquences radioélectriques	56
Additional Information on RF Exposure	57
Declaration of Conformity Statements	57



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.

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 Catalyst IW9167E Heavy Duty access point is available at the following URL:

<https://www.cisco.com/c/en/us/support/wireless/catalyst-iw9167-series/series.html>

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

[Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Cupertino 17.9.x](#)

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 DevNet](#).
- 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 gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.



CHAPTER 1

About Cisco Catalyst IW9167E Heavy Duty Access Point

- [Introduction to Cisco Catalyst IW9167E Heavy Duty Access Point, on page 1](#)
- [Cisco Catalyst IW9167E Heavy Duty Access Point Features, on page 1](#)
- [Connectors and Ports, on page 2](#)
- [Power Sources, on page 3](#)
- [Antennas and Radios, on page 4](#)

Introduction to Cisco Catalyst IW9167E Heavy Duty Access Point

The Cisco Catalyst IW9167E Heavy Duty Access Point is a tri-band 802.11ax (Wi-Fi 6) AP that provides reliable wireless connectivity for mission-critical applications as organizations automate processes and operations. It can operate as Wi-Fi 6 or Cisco Ultra-Reliable Wireless Backhaul (Cisco URWB). Wi-Fi 6 technology brings higher density, higher throughput, more channels, power efficiency, and improved security in industrial or outdoor locations. Cisco URWB provides ultra-reliable wireless connectivity for moving assets or to extend the network where running fiber isn't feasible or is too costly.

The Cisco Catalyst IW9167E Heavy Duty Access Point comes with three 4x4 radios, in a heavy-duty design that is IP67 rated, and packed with advanced features.

A full listing of the AP's features and specifications is provided in the [Cisco Catalyst IW9167E Heavy Duty Access Point Data Sheet](#).

Cisco Catalyst IW9167E Heavy Duty Access Point Features

Cisco Catalyst IW9167E Heavy Duty Access Point is supported on Cisco Catalyst 9800 wireless controller-based products, and have the following features:

- 2 GB DDR4 memory, 1 GB NAND Flash
- Tri-radio, dual band support: 2.4 GHz Slot 0, 5 GHz Slot 1, and 5 GHz Slot 2
- 4 x 4 MIMO with up to 4 spatial streams
- 8 x N-type female connectors for Wi-Fi, 1x TNC female for GNSS, multi-protocol IoT radio, Aux radio, Barometer

- Bluetooth Low Energy (BLE) radio enables IoT use cases such as location tracking and wayfinding
- Client or AP mode – Cisco URWB, WGB, or AP
- 1 x multi-Gigabit (mGig) copper Ethernet port (supporting PoE, including IEEE 802.3at/bt, Cisco UPoE, 100 Mbps/1 Gbps/2.5 Gbps/5 Gbps)
- 1 x SFP interface – supports up to 10 Gbps



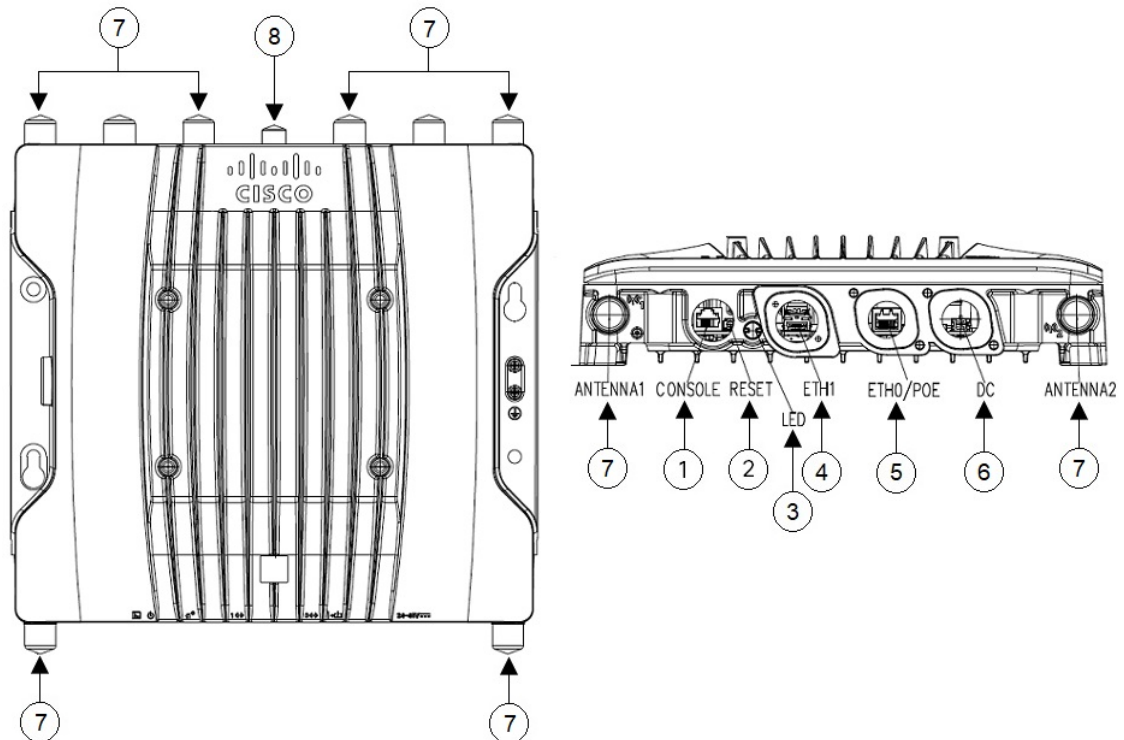
Note For 10G SFP fiber module, Cisco PID SFP-10G-LR10-I has guaranteed performance with IW9167EH access point.

- Optional M12 adapter for network and power interfaces
- Dual power input options – PoE-in and 24 - 48VDC
- Water and dust resistance – IP66/67
- Hardened for shock, vibration, and extreme temperatures

Connectors and Ports

The following figures show the available ports on the AP.

Figure 1: IW9167EH Connectors and Ports



1	Console port (RJ-45)	2	Reset button For information on how to use the Reset button, see Using the Reset Button, on page 41 .
3	Status LED	4	SFP (copper) 100M/1000M/10G Multigigabit Ethernet /M12 X-code or SFP (fiber) 1G/10G
5	100M/1000M/2.5G/5G Multigigabit Ethernet (RJ-45) / M12 X-code auto-sensing PoE+ in (802.3at/bt), UPOE-in	6	DC power input (micro-fit, or M12 4-pin A-code by using M12 adapter)
7	Antenna ports	8	GNSS port

Power Sources

The Cisco Catalyst IW9167E Heavy Duty Access Point is supported on these power sources:

- DC power: 24 to 48 VDC
- Power over Ethernet (PoE): 802.3at (PoE+), 802.3bt (PoE++), Cisco Universal PoE (Cisco UPOE). For more information, see [Powering the Access Point, on page 31](#).



Warning

Connect the unit only to DC power source that complies with the safety extra-low voltage (SELV) requirements in IEC 60950 based safety standards. Statement 1033

Power Adapters

The Cisco Catalyst IW9167E Heavy Duty Access Point supports the following DC power adapters::

- PID: IW-PWRADPT-MFIT4P=

Power Injectors

The Cisco Catalyst IW9167E Heavy Duty Access Point supports the following power injectors:

- IW-PWRINJ-60RGDMG=
- AIR-PWRINJ-60RGD1=
- AIR-PWRINJ-60RGD2=



Warning

To reduce the risk of fire, use only No. 24 AWG or larger telecommunications line cord. Statement 1023

**Caution**

When the AP is installed outdoors or in a wet or damp location, the AC branch circuit powering the AP should be provided with ground fault protection (GFCI), as required by Article 210 of the National Electrical Code (NEC).

Ethernet (PoE) Ports

The AP supports an Ethernet uplink port (also for PoE-In). The Ethernet uplink port on the AP uses an RJ-45 connector (with weatherproofing) to link the AP to the 100BASE-T, 1000BASE-T, 2.5G BASE-T, or 5G BASE-T network. The Ethernet cable is used to send and receive Ethernet data and optionally supply inline power from the power injector or a suitably powered switch port.

**Tip**

The AP senses the Ethernet and power signals, and automatically switch internal circuitry to match the cable connections.

**Danger**

To reduce the risk of fire, use only No. 24 AWG or larger telecommunication line cord. Statement 1023

The Ethernet cable must be a *shielded*, outdoor rated, Category 5e (CAT 5e) or better cable. The AP senses the Ethernet and power signals and automatically switches internal circuitry to match the cable connections.

Antennas and Radios

The Cisco Catalyst IW9167E Heavy Duty Access Point configuration is:

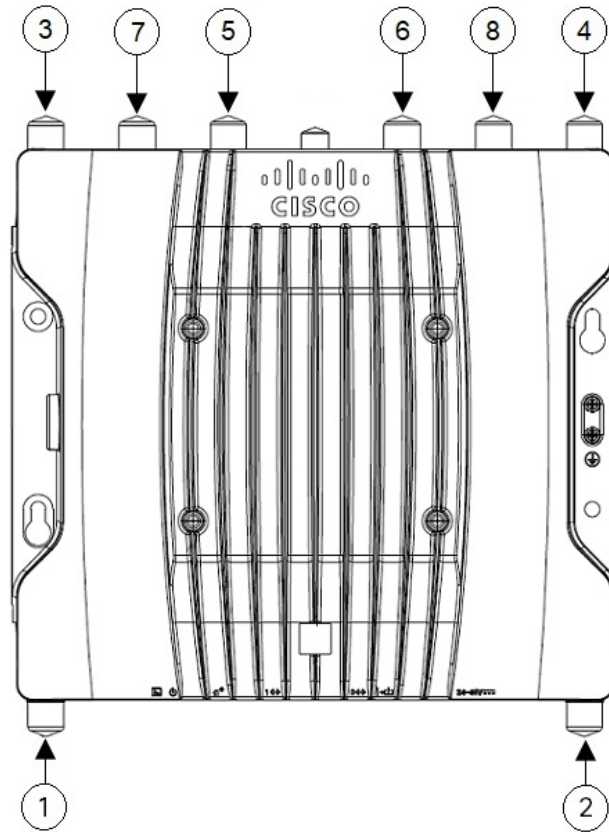
- IW9167EH-x

The IW9167EH access point has eight N-type female connectors to support multiple antenna options, such as the self-identifying antennas (SIA) on designated three SIA ports, dual-band antennas, and single-band antennas. To see the list of supported antennas and the radio bands they operate at, see [Supported External Antennas, on page 4](#).

Supported External Antennas

The following figure shows the antenna ports of the IW9167EH access point.

Figure 2: IW9167EH Access Point Antenna Ports



1	Port 1 Supports 2.4 GHz radio in 4x4, 2x2, or 1x1 mode. Supports 5 GHz radio in 4x4 mode. Supports SIA.	2	Port 2 Supports 2.4 GHz radio in 4x4, 2x2 mode. Supports 5 GHz radio in 4x4 mode.
3	Port 3 Supports 2.4 GHz radio in 4x4 mode. Supports 5 GHz radio in 4x4, 2x2 mode.	4	Port 4 Supports 2.4 GHz radio in 4x4 mode. Supports 5 GHz radio in 4x4, 2x2, or 1x1 mode. Supports Bluetooth Low Energy (BLE) radio. Supports SIA.
5	Port 5 Supports 5 GHz radio in 4x4, 2x2, 1x1 mode. Supports SIA.	6	Port 6 Supports 5 GHz radio in 4x4, 2x2 mode.
7	Port 7 Supports 5 GHz radio in 4x4 mode.	8	Port 8 Supports 5 GHz radio in 4x4 mode.

Supported Wi-Fi Antennas

The following table shows the external Wi-Fi antennas supported by the IW9167EH access point.

Table 1: Supported Wi-Fi Antennas

PID	Antenna Gain (dBi)			Connector	Antenna Name
	2.4 GHz	4.9 GHz	5 GHz		
IW-ANT-OMV-2567-N=	4	7	7	N male	2.4/5 GHz Tri-Band Omnidirectional Dipole Antenna, Vertically Polarized, Self-Identifying
IW-ANT-OMH-2567-N=	4	7	7	N male	2.4/5 GHz Tri-Band Omnidirectional Dipole Antenna, Horizontally Polarized, Self-Identifying
AIR-ANT2547V-N=	4	—	7	N male	Cisco Aironet Dual-Band Omnidirectional Dipole Antenna (White)
AIR-ANT2547VG-N=	4	—	7	N male	Cisco Aironet Dual-Band Omnidirectional Dipole Antenna (Gray)
AIR-ANT2547VG-NS=	4	—	7	N male	Cisco Aironet Dual-Band Omnidirectional Dipole Antenna (Gray), Self-Identifying
AIR-ANT2568VG-N=	6	—	8	N male	Cisco Aironet Dual-Band Omnidirectional Dipole Antenna (Gray)
AIR-ANT2568VG-NS=	6	—	8	N male	Cisco Aironet Dual-Band Omnidirectional Dipole Antenna (Gray), Self-Identifying
AIR-ANT2480V-N=	8	—	—	N male	Cisco Aironet 2.4 GHz 8 dBi Omnidirectional Dipole Antenna
AIR-ANT5180V-N=	—	7	8	N male	Cisco Aironet 5 GHz 8 dBi Omnidirectional Dipole Antenna
AIR-ANT2588P4M-NS=	9.1 (V), 7.1 (H)	—	9.6 (V), 7.8 (H)	N female (x4)	Cisco Aironet 2.4/5 GHz 8 dBi 4-Element Dual-Polarized Patch Antenna, Self-Identifying
AIR-ANT2413P2M-N=	13	—	—	N male (x2)	Cisco Aironet 2.4 GHz 13 dBi Dual-Port Dual-Polarized Directional Panel Antenna

PID	Antenna Gain (dBi)			Connector	Antenna Name
AIR-ANT5114P2M-N=	—	—	13	N male (x2)	Cisco Aironet 5 GHz 13 dBi Dual-Port Dual-Polarized Directional Panel Antenna
AIR-ANT2513P4M-N=	13	—	13	N female (x4)	Cisco Aironet Four-Port Dual-Band Polarization-Diverse Directional Panel Antenna
AIR-ANT2513P4M-NS=	13	—	13	N female (x4)	Cisco Aironet Four-Port Dual-Band Polarization-Diverse Directional Panel Antenna, Self-Identifying
IW-ANT-OMM-53-N=	—	3	3	N female	5 GHz Omnidirectional Multi-Polarized Antenna
IW-ANT-PNL-59-N=	—	—	9	N female (x2)	5 GHz Dual-Port Dual-Slant +/-45 Degree Polarized Directional Panel Antenna
IW-ANT-SKS-514-Q=	—	14	14	QMA female (x2)	5 GHz Directional Shark Antenna, Dual-Slant +/-45 Degree Polarized
IW-ANT-SKD-513-Q=	—	13	13	QMA female (x2)	5 GHz Bidirectional Shark Antenna, Dual-Slant +/-45 Degree Polarized
IW-ANT-H90-510-N=	—	—	10	N female (x2)	5 GHz Dual-Port Dual-Polarized Horn Antenna
FLMESH-HW-ANT-28	—	—	19.5	N female (x2)	5 GHz Dual-Port Dual-Slant Polarized Directional Panel Antenna

For installation instructions and detailed information on any of these antennas, refer to the antenna data sheet on Cisco.com, or see the antenna guides at:

- [Cisco Industrial Routers and Industrial Wireless Access Points Antenna Guide](#)
- <http://www.cisco.com/c/en/us/support/wireless/aironet-antennas-accessories/products-installation-guides-list.html>

Follow all safety precautions when installing the antennas. For information on safety, see [Safety Precautions when Installing Antennas, on page 46](#).

Supported GNSS Antenna

The following table shows the external GNSS antennas supported by the IW9167EH access point.

Table 2: Supported GNSS Antenna

PID	Frequencies Supported	Connector	Description
ANT-GNSS-OUT-TNC=	1560 - 1608 MHz	TNC male	Outdoor Active GNSS Antenna with 15-ft. integrated cable



CHAPTER 2

Unpacking Your Access Point

- [Package Contents](#), on page 9
- [Unpacking the Access Point](#), on page 9
- [Cisco Orderable Accessories](#), on page 9

Package Contents

Each AP package contains the following items:

Draft comment: Need to check default shipped items.

- One IW9167EH AP
- Ground lug kit
- Cisco product documentation and pointer card

Unpacking the Access Point

To unpack the AP, follow these steps:

-
- | | |
|---------------|---|
| Step 1 | Unpack and remove the access point and the selected mounting accessory kit from the shipping box. |
| Step 2 | Return the 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

Cisco PID	Description
AIR-ACCDMK3700=	DIN Rail Mounting Bracket
AIR-ACCPMK3700=	Pole Mounting Bracket (for 2”–3.2” diameter pole)
AIR-ACCPMK3700-2=	Pole Mounting Bracket (for 2”–16” diameter pole)

- Accessory kits

Cisco PID	Description
AIR-SFP-KIT1=	Gland kit for SFP port (Qty: 5)
IW-ACC-M12ETH=	Adapter, M12 X-code to RJ45 Ethernet connector
IW-ACC-M12PWR=	Adapter, M12 4 Pin A-Code to Micro-fit power connector
IW-ACC-M12SPCR1=	Spacer for M12 when using on SFP port (Qty: 5)

- RF Coaxial Adapters

Cisco PID	Description
AIR-ACC370-NF-NF=	N(f) to N(f) RF adapter DC-11 GHz

- RF Coaxial Cables

Cisco PID	Description
CAB-L400-5-N-N=	5 ft. LMR-400-DB, N(m)-STR to N(m)-R/A
CAB-L400-5-N-NS=	5 ft. LMR-400-DB, N(m)-STR to N(m)-STR
AIR-CAB010LL-N=	10 ft. LMR-400-DB, N(m)-STR to N(m)-STR
CAB-L400-20-N-N=	20 ft. LMR-400-DB, N(m)-STR to N(m)-RA
AIR-CAB025HZ-N=	25 ft. LMR-400-DB/FR/CMR, N(m)-STR to N(m)-RA
CAB-L600-30-N-N=	30 ft. LMR-600-DB, N(m)-STR to N(m)-RA
CAB-L240-10-Q-N=	10 ft. LMR-240-FR/CMR, N(m)-STR to QMA(m)-RA
CAB-L240-15-Q-N=	15 ft. LMR-240-FR/CMR, N(m)-STR to QMA(m)-RA
CAB-L240-20-Q-N=	20 ft. LMR-240-FR/CMR, N(m)-STR to QMA(m)-RA

- Lightning Arrestors

Lightning Arrestor	Description
CGR-LA-NF-NF=	Lightning Arrestor kit, N(f) connectors

Lightning Arrestor	Description
CGR-LA-NM-NF=	Lightning Arrestor kit, N(m) to N(f)
ACC-LA-G-TM-TF=	Lightning Arrestor kit, TNC(f) for GNSS

- Power adapter and power injectors when PoE is not available

Power Supply	Description
IW-PWRADPT-MFIT4P=	Power Adapter, AC-DC, Micro-Fit 4Pin connector
IW-PWRINJ-60RGDMG=	Power Injector, 60W, outdoor 5GE
AIR-PWRINJ-60RGD1=	60W outdoor rated power injector, with North America AC power plug. For more information, see the power injector data sheet .



CHAPTER 3

Installation Overview

- [Performing a Preinstallation Configuration \(Optional\), on page 13](#)
- [Preinstallation Checks and Installation Guidelines, on page 15](#)
- [Mounting the Access Point, on page 16](#)
- [Attaching a Power Adapter, on page 26](#)
- [Installing a Lightning Arrestor, on page 28](#)
- [Grounding the Access Point, on page 30](#)
- [Powering the Access Point, on page 31](#)
- [Connecting Data Cables, on page 33](#)

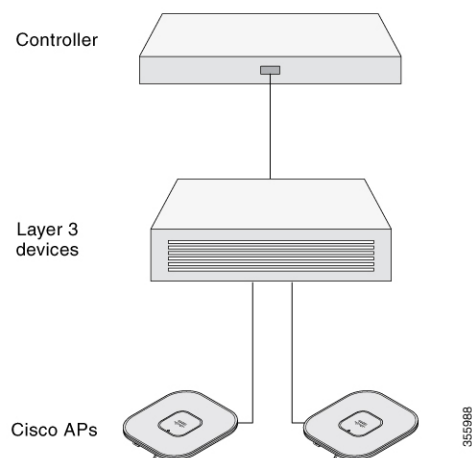
Performing a Preinstallation Configuration (Optional)

The following procedures describe the processes to ensure that your AP installation and initial operation go as expected.



Note Performing a preinstallation configuration is an optional procedure. If your network controller is properly configured, you can install your AP in its final location and connect it to the network from there.

The following illustration shows the preinstallation configuration setup:



Perform the following steps:

Before you begin

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

- Enable Layer 3 connectivity between APs, Cisco Controller Management, and AP-Manager interface.
- Configure the switch to which your AP has to attach. See the [Cisco Wireless Controller Configuration Guide](#) for the release you are using, for additional information.
- Configure the Cisco Catalyst 9800 Series Wireless Controller as the primary so that new APs always join it.
- Ensure that the DHCP is enabled on the network. The AP must receive its IP address through DHCP.



Note An 802.11ax AP is 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.

- CAPWAP UDP ports must not be blocked in the network.
- The AP 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, see the product documentation.



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

Step 1 Power the AP using supported power source.

- As the AP attempts to connect to the controller, the LED cycles through a green, red, and off sequence, which can take up to five minutes.

Note If the AP remains in this mode for more than five minutes, the AP cannot find the primary Cisco Catalyst 9800 Series Wireless Controller. Check the connection between the AP and the Cisco Catalyst 9800 Series Wireless Controller and be sure that they are on the same subnet.

- If the AP shuts down, check the power source.
- After the AP finds the Cisco Catalyst 9800 Series Wireless Controller, it attempts to download the new operating system code if the AP code version differs from the Cisco Catalyst 9800 Series Wireless Controller code version. While this is happening, the Status LED blinks blue.

If the operating system download is successful, the AP reboots.

Step 2 (Optional) Configure the AP. Use the controller CLI, GUI, or Cisco DNA Center to customize the access point-specific 802.11ax network settings.

- Step 3** If the preinstallation configuration is successful, the Status LED is green, indicating normal operation. Disconnect the AP and mount it at the location at which you intend to deploy it on the wireless network.
- Step 4** If your AP does not indicate normal operation, turn it off and repeat the preinstallation configuration.
- Note** When you are installing a Layer 3 access point on a subnet that is different from the Cisco Catalyst 9800 Series Wireless Controller, ensure the following setup is configured:
- A DHCP server is reachable from the subnet on which you plan to install the AP.
 - The subnet has a route back to the controller.
 - This route has destination UDP ports 5246 and 5247 open for CAPWAP communications.
 - The route back to the primary, secondary, and tertiary controller allows IP packet fragments.
 - If address translation is used, the access point and the 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: To a vertical or horizontal wall or a pole
- Access point power options: Use either of the following options to power the AP:
 - DC power input
 - Cisco-approved power injector
 - 802.3at (PoE+), 802.3bt, and Cisco Universal PoE (Cisco UPOE)
- Operating temperature: -40° to +158°F (-40° to +70°C) with solar load and still air.
Extended operating temperature (DC powered): -58° to +167°F (-50° to +75°C) without solar loading, still air, and cold start limited to -40°C
- Console access using the console port

We recommend that you use a console cable that is one meter or less in length.



Note The AP may face issues while booting if you use an unterminated console cable (not plugged into any device or terminal) or a console cable that is more than one meter in length.

We recommend 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

Mounting Hardware

The IW9167EH access point has built-in mounting flanges. You can also use the following mounting hardware:

- DIN rail mounting bracket
- Pole mounting bracket

Required mounting hardware depends on the mounting location:

- For ceilings or hard ceilings or walls, directly mount the access point using the built-in mounting flanges.

The mounting flanges are on the sides of the access point that are without ports.

- For electrical cabinets or network boxes, directly mount the access point using the mounting flanges or use the DIN rail mounting bracket.
- For pole mounting, use the pole mounting bracket.

Mounting Bracket Part Numbers



Note These brackets do not ship with the access point, but you can order them separately.

Table 3: Mounting Bracket Part Numbers

Mounting Bracket	Cisco Part Number
DIN Rail Mounting Bracket	AIR-ACCDMK3700=
Pole Mounting Bracket (for 2"–3.2" diameter pole)	AIR-ACCPMK3700=
Pole Mounting Bracket (for 2"–16" diameter pole)	AIR-ACCPMK3700-2=

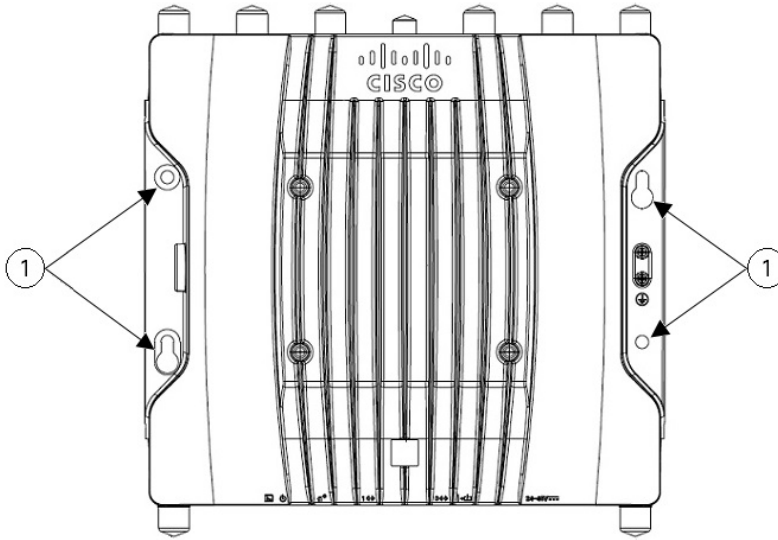
Using the Integrated Flange Mounts

Direct mounting using the integrated flange mounts is typically for confined spaces or deployments that experience severe shock and vibration.

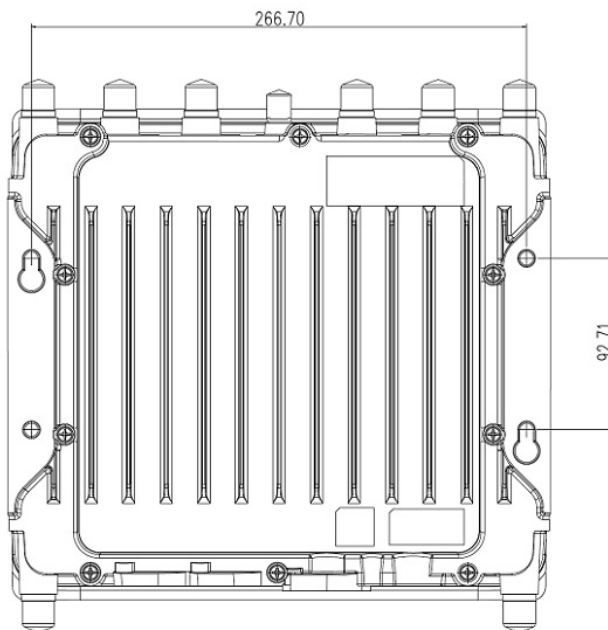
To mount the access point using the integrated flange mounts:

Step 1 Choose the access point location that can safely support the weight of the access point.

Step 2 Use the access point mounting holes as a template, and mark them at the mounting location.



1	mounting holes
---	----------------



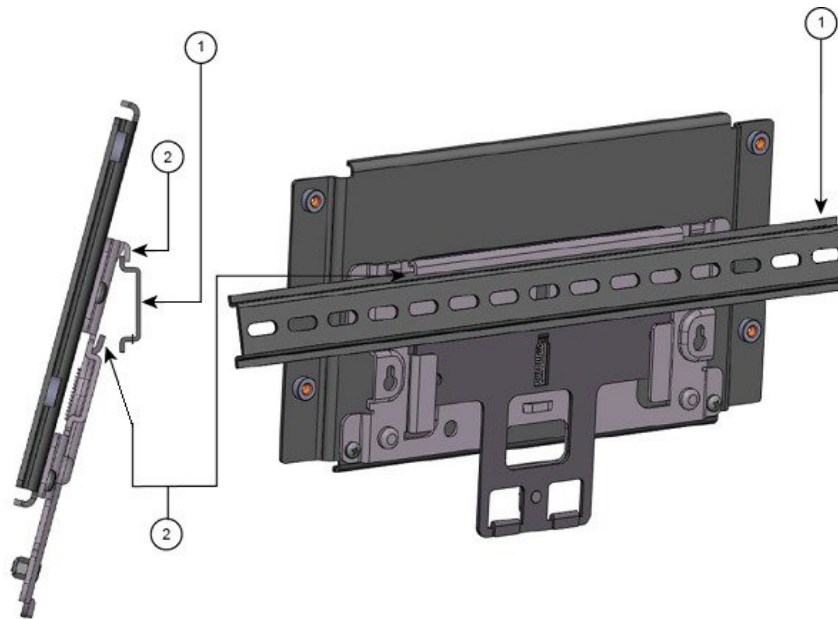
- Step 3** Drill holes on the mounting surface for plastic wall anchors to suit 1/4-20 or M6 bolts, and add the appropriate anchors.
- Step 4** Align the access point mounting holes with the suspended ceiling mounting holes.
- Step 5** Insert a mounting screw in each of the four mounting holes and tighten.
- Step 6** You can use the keyholes for “hands-free” installation.

Note Ensure that the access point is firmly secured.

Using the DIN Rail Mounting Bracket

You can use DIN rail mounting in network or electrical closets or cabinets, or in wiring rooms that have low-levels of shock and vibration. [Figure 3: DIN Rail Mounting Assembly, on page 18](#) shows the DIN rail and DIN rail mounting assembly.

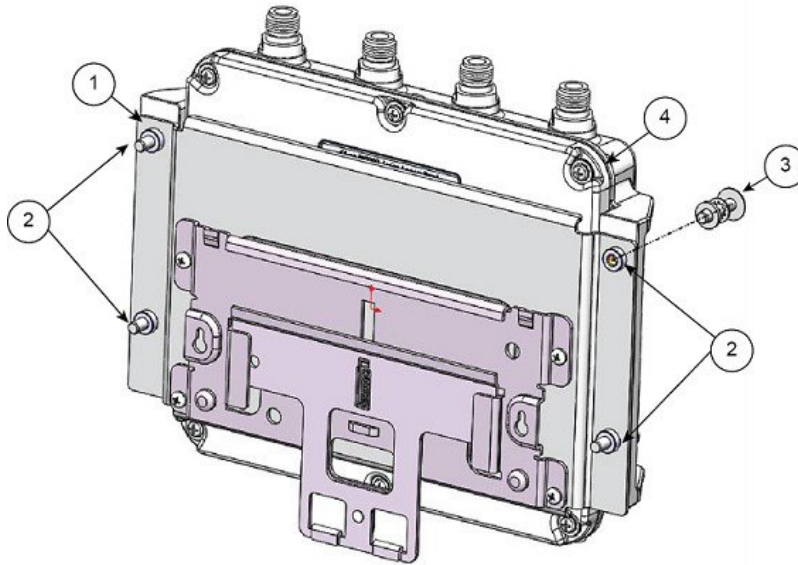
Figure 3: DIN Rail Mounting Assembly



1	35 mm DIN rail (not supplied by Cisco)	2	DIN rail mounting bracket clip
---	--	---	--------------------------------

To DIN rail mount the access point:

Step 1 Assemble the access point and DIN rail mounting bracket using the M6 hardware supplied as shown in the following figure.



1	Steel DIN mounting bracket	3	M6 screw (Torque 6–7 ft-lbs)
2	M6 insert	4	Access Point

Step 2 Position the access point assembly directly in front of the DIN rail.

Step 3 Insert the DIN rail mounting bracket under the spring-loaded upper mounting clips.



Note Ensure that the DIN rail seats into the anti-slip clips.

Step 4 Pull down the retention handles until the lower lip of the DIN rail mounting bracket seats in the lower mounting bracket clip.

Step 5 Release the retention handles.

Using the Pole Mounting Bracket

You can choose one of the following pole mounting brackets in the following table, according to the size of the pole that you are going to mount your access point on.

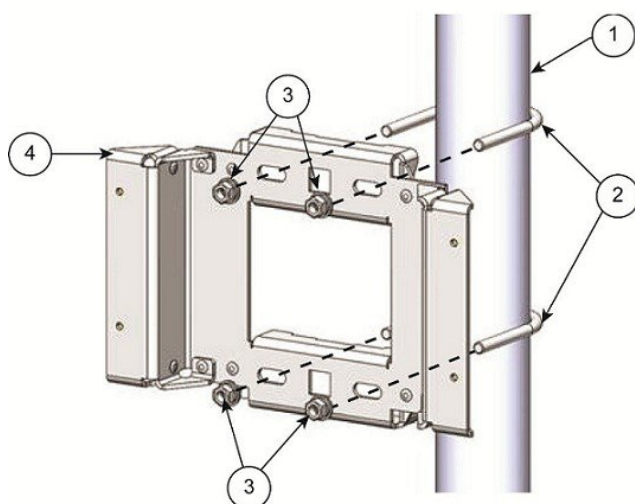
Table 4: Pole Mounting Brackets

Mounting Bracket	Cisco Part Number	Applicable Pole Diameter
Pole Mounting Bracket	AIR-ACCPMK3700=	2–3.2 inches
Pole Mounting Bracket 2	AIR-ACCPMK3700-2=	2–16 inches

Using the Mounting Bracket AIR-ACCPMK3700=

To mount the access point on a pole using the mounting bracket AIR-ACCPMK3700=:

Step 1 Use the supplied U bolts, washers, and nuts to attach the mounting bracket to the pole.

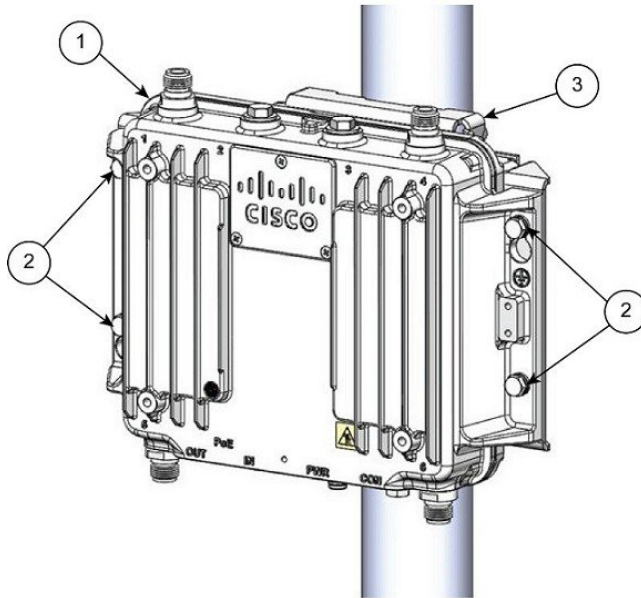


1	2"– 3.2" (5–8 cm) diameter pole	3	M8 x 1.25 nuts and washers
2	M8 x 1.25 U-bolt	4	Pole mounting bracket

Step 2 Use the included bolts, washers, and nuts to attach the access point to the mounting plate.

Note Ensure that you symmetrically tighten the nuts on the U-bolts. If you over tighten one side, the U-bolt will skew.

Step 3 Torque the nuts to 6 to 7 foot-pounds.



Draft comment: Need to replace with AP IW9167

1	Access point	3	Pole mounting bracket
2	M6 bolts and washers	4	

Note Ensure that the access point is firmly secured to the mounting bracket.

You can use the keyholes for “hands-free” installation. Ensure that you torque the nuts to 6 to 7 ft-lbs.

Caution Never leave the access point unattended if the mounting hardware is not torqued to full value.

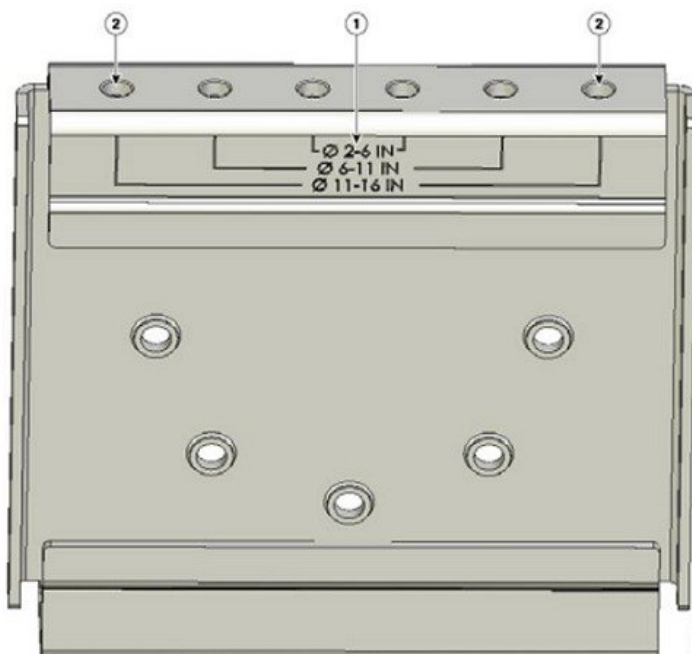
Using the Mounting Bracket AIR-ACCPMK3700-2=

The mounting bracket AIR-ACCPMK3700-2= supports poles from 2 to 16 inches in diameter. To mount the access point on a pole using this mounting bracket:

Step 1

Assemble two strap brackets on the pole clamp bracket that are positioned for the pole diameter you are using to mount the access point. The following image illustrates the pole diameter indicators and bolt holes on the pole clamp bracket.

Figure 4: Pole Clamp Bracket Adjustment Hole Locations

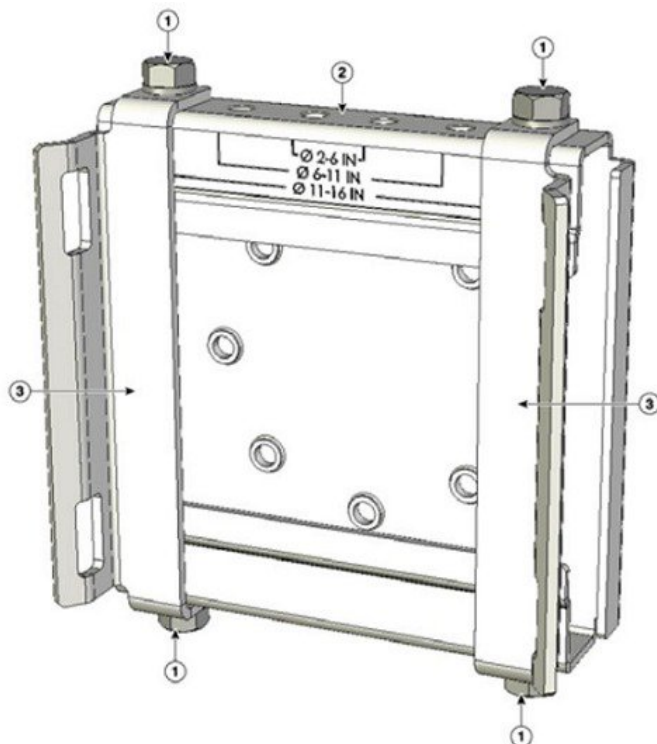


1	Pole size indicators <ul style="list-style-type: none"> • 2 to 6 in. • 6 to 11 in. • 11 to 16 in.
2	Bolt holes for pole diameters (11 to 16 inches indicated)

Step 2

Position the strap brackets on the pole clamp bracket for the pole diameter you are using and secure each strap bracket with two M8 x16 bolts (with lock washers), as the following image shows. Tighten the bolts to 13 to 15 ft lbs (17.6 to 20.3 N-m).

Figure 5: Assembled Pole Clamp Bracket and Strap Brackets



1	M8 x1.25x16 bolts (with lock washers)	3	Strap bracket (shown positioned for 11 to 16 inch diameter pole)
2	Pole clamp bracket		

Step 3

Screw the M8 nut onto the pole clamp bracket support bolt, and tighten just enough to prevent the bolt from falling off.

Step 4

To mount your access point on a vertical pole, you need to install two metal bands around the pole to support the access point. This process requires extra tools and material not provided in the pole mount kit (see the following table for details).

Table 5: Material Needed to Mount Access Point on a Pole

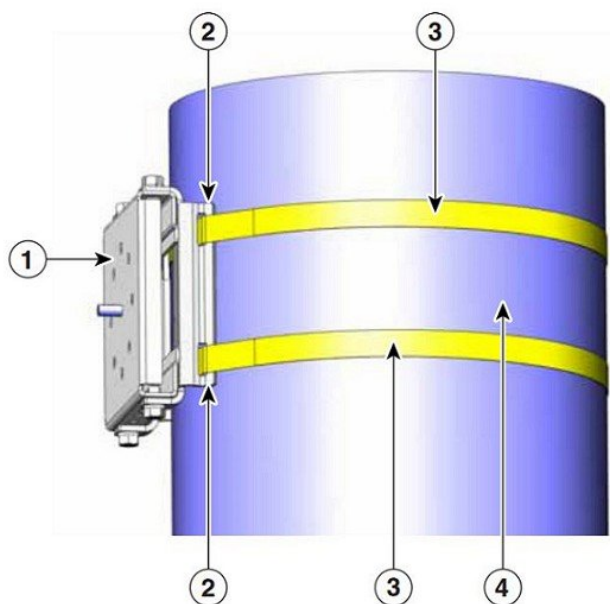
Mounting Method	Materials Required	In Kit
Vertical pole	• Two 0.75-in (1.9 cm) stainless steel bands	Yes
	• Banding strap tool (BAND IT) (Cisco AIR-BAND-INST-TL=)	No
	• Ground lug (provided with access point)	Yes
	• Crimping tool for ground lug, Panduit CT-720 with CD-720-1 die (http://onlinecatalog.panduit.com)	No
	• #6 AWG ground wire	No

Step 5 Select a mounting location on the pole to mount the access point. You can attach the access point to any pole from 2 to 16 inch (5.1 to 40.6 cm) in diameter.

Step 6 For poles larger than 3.5 inch (8.9 cm), mount the pole clamp bracket assembly to a pole (see the following image) using two metal straps. Following the instructions provided with the banding strap tool (BAND IT) (AIR-BAND-INST-TL=), loop each metal strap twice through the slots on the strap bracket.

Caution Do not place the metal straps in the large open area between the pole clamp bracket and the strap brackets, because this does not properly secure the access point.

Figure 6: Clamp Bracket Assembly Mounted on Poles Larger than 3.5 inch (8.9 cm)



1	Pole clamp bracket	3	Metal mounting strap
2	Strap slot in strap bracket	4	Pole

Step 7 For pole diameters of 3.5 inch (8.9 cm) or less, mount the pole clamp bracket assembly to a pole using two metal straps looped through the space between the pole clamp bracket and the strap brackets to provide maximum holding strength for extreme environments. Following the instructions provided with the banding strap tool (BAND IT) (AIR-BAND-INST-TL=), loop each metal strap twice.

Caution Do not place the metal straps in the large open area between the pole clamp bracket and the strap brackets because this does not properly secure the access point.

Step 8 Position the pole clamp bracket on the pole as needed before tightening the metal bands.

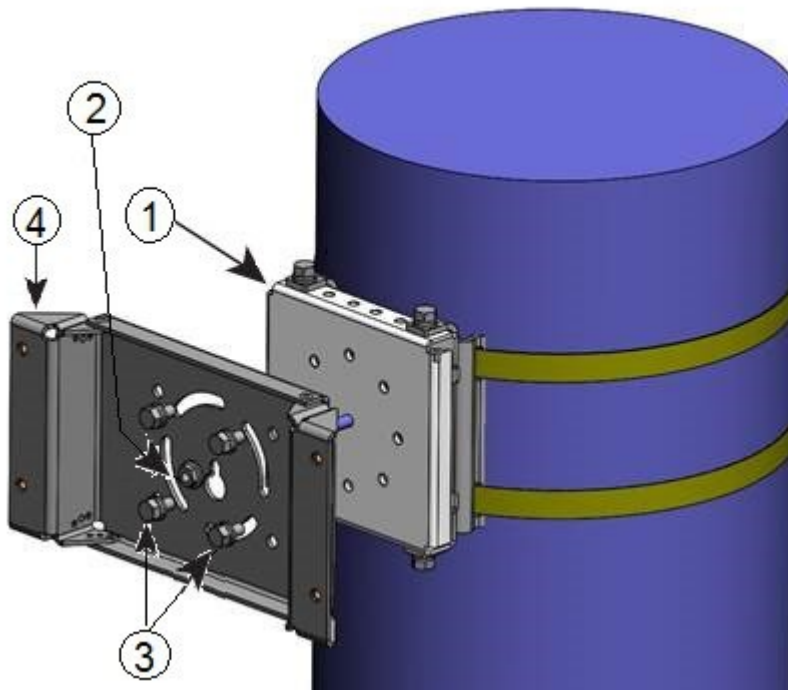
Note When the metal bands are tightened to the full tension, the pole clamp bracket cannot be adjusted unless the metal bands are cut or disassembled.

Step 9 Tighten the metal bands using the banding strap tool (BAND IT) (Cisco AIR-BAND-INST-TL=) by following the operating instructions in the box with the tool. Ensure that the metal bands are as tight as possible.

Step 10 Place the mounting bracket onto the pole clamp bracket support bolt.

Step 11 Install four M8 x16 bolts (with flat and lock washers) into the bolt holes.

Figure 7: Mounting Bracket and Pole Clamp Bracket Assembly



1	Pole clamp bracket assembly	3	Bolt holes
2	Access point support bolt	4	Mounting bracket

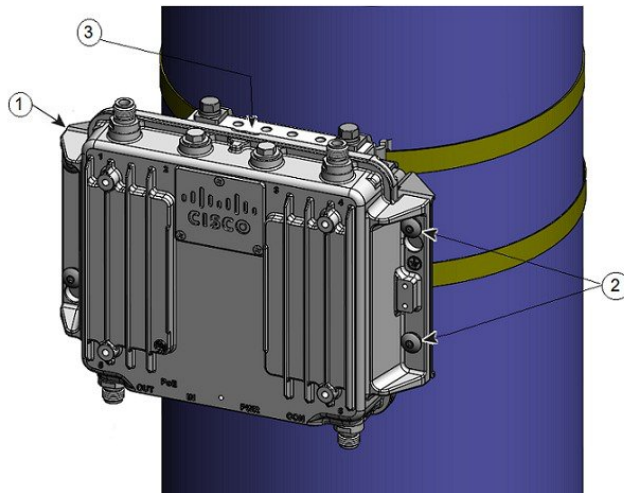
Step 12 Hand-tighten the bolts and the nut (do not overtighten).

Step 13 Adjust the top edge of the mounting bracket until it is horizontal and tighten the bolts and the flange nut to 13 to 15 ft-lbs (17.6 to 20.3 N-m).

Step 14 Use the included bolts, washers, and nuts to attach the access point to the mounting plate.

Step 15 Torque the nuts to 6 to 7 ft-lbs.

Figure 8: Access Point Installed in the Mounting Bracket



Draft comment: Need to replace with AP9167

1	Access point	3	Pole mounting bracket
2	M6 bolts and washers		

Note Ensure that the access point is firmly secured to the mounting bracket.

Caution Never leave the access point unattended if the mounting hardware is not torqued to full value.

Attaching a Power Adapter

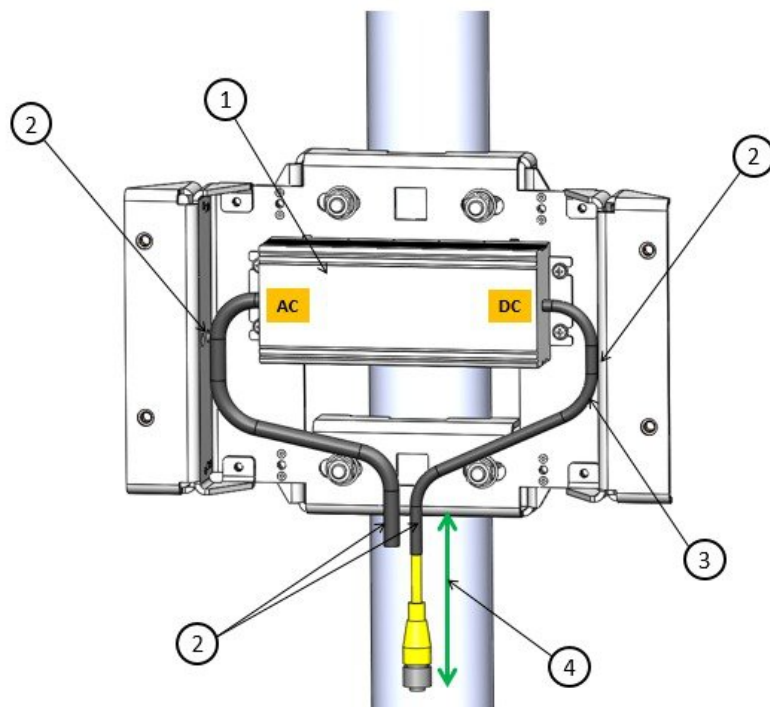
If you want to attach a power adapter (IW-PWRADPT-MFIT4P=) to the access point on a pole using the mounting bracket AIR-ACCPMK3700= or AIR-ACCPMK3700-2=, use the procedures in the following sections.

Attaching a Power Adapter Using the Mounting Bracket AIR-ACCPMK3700=

To attach a power adapter (IW-PWRADPT-MFIT4P=) to the access point on a pole using the mounting bracket AIR-ACCPMK3700=, use the following procedures:

- Step 1** Ensure you have the mounting bracket set up as described in Step 1 of [Using the Mounting Bracket AIR-ACCPMK3700=](#), on page 20.
- Step 2** Attach the power supply using 4x 6-32 screws and torque the screws to 8.3-11 in-lbs, as shown in the following figure.

Figure 9: Power Adapter Installed Using Mounting Bracket AIR-ACCPMK3700=



1	Power Adapter	3	DC Output Cable
2	Tie Wraps	4	10 inches Minimum Length

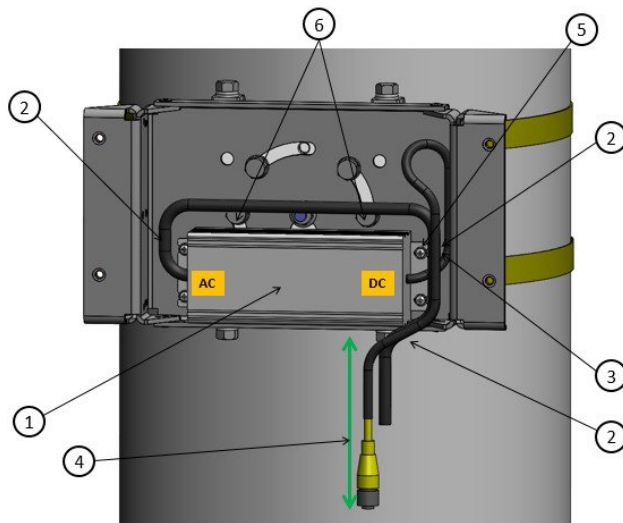
- Step 3** Ensure that the excess cable is bundled and tie wrapped to the mounting bracket. Route the cable as shown in the figure in Step 2.
- Step 4** Ensure that there is 10 inches minimum length from the bottom edge of the power supply to the end of the connector as shown in the figure in Step 2.
- Step 5** Attach the access point to the mounting plate as described in Step 2 and Step 3 of [Using the Mounting Bracket AIR-ACCPMK3700=](#), on page 20.

Attaching a Power Adapter Using the Mounting Bracket AIR-ACCPMK3700-2=

To attach a power adapter (IW-PWRADPT-MFIT4P=) to the access point on a pole using the mounting bracket AIR-ACCPMK3700-2=, use the following procedures:

- Step 1** Ensure you have the mounting bracket set up as described in Step 1 through Step 13 of [Using the Mounting Bracket AIR-ACCPMK3700-2=](#), on page 21. But for step 11, the 2 lower bolts need to be repositioned to the locations indicated as No. 6 in the following figure.
- Step 2** Attach the power supply using 4x 6-32 screws and torque the screws to 8.3-11 in-lbs, as shown in the following figure.

Figure 10: Power Adapter Installed Using Mounting Bracket AIR-ACCPMK3700-2=



1	Power Adapter	4	10 inches Minimum Length
2	Tie Wraps	5	4x 6-32 Screws
3	10 inches Minimum Length	6	Reposition the bolts

- Step 3** Ensure that the excess cable is bundled and tie wrapped to the mounting bracket. Route the cable as shown in the figure in Step 2.
- Step 4** Ensure that there is 10 inches minimum length from the bottom edge of the power supply to the end of the connector as shown in the figure in Step 2.
- Step 5** Attach the access point to the mounting plate as described in step 14 and step 15 of [Using the Mounting Bracket AIR-ACCPMK3700-2=](#), on page 21.

Installing a Lightning Arrestor

Overvoltage transients can be created through lightning static discharges, switch processes, direct contact with power lines, or through earth currents. The Lightning Arrestor limits the amplitude and duration of disturbing interference voltages and improves the over voltage resistance of in-line equipment, systems, and components. A lightning arrestor installed according to these mounting instructions balances the voltage potential, thus preventing inductive interference to parallel signal lines within the protected system.

Installation Considerations

Cisco recommends that you bulkhead mount the lightning arrestor so it can be installed as a wall-feed through on the wall of the protected space.

The importance of obtaining a good ground and bonding connection cannot be overstressed. Consider these points when grounding the lightning arrestor:

- Connect the lightning arrestor components directly to the grounding point.
- The contact points of the ground connection must be clean and free of dust and moisture.
- Tighten threaded contacts to the torque specified by the manufacturer.

Lightning Arrestor Installation Notes

This lightning arrestor is designed to be installed between the antenna cable that is attached to an outdoor antenna and the Cisco wireless device. You can install the lightning arrestor either indoors or outdoors. It can be connected directly to a wireless device having an external N connector. It can also be mounted inline or as a feed-through. Feed-through installations require 5/8 in. (16 mm) hole to accommodate the lightning arrestor.

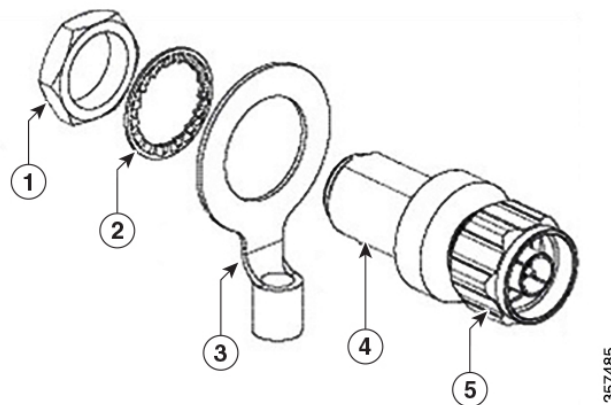


Note

- This lightning arrestor is part of a lightning arrestor kit. The kit contains a lightning arrestor and a grounding lug.
- When you install the lightning arrestor, follow the regulations or best practices applicable to lightning protection installation in your local area.

Installing the Lightning Arrestor Outdoors

If you install the lightning arrestor outdoors, use the supplied ground lug and a heavy wire (#6 solid copper) to connect it to a good earth ground, such as a ground rod. The connection should be as short as possible.



1	Nut	4	Unprotected Side (to antenna)
2	Lockwasher	5	Protected side (to wireless device)
3	Ground lug		

Cable for the Lightning Arrestor

Coaxial cable loses efficiency as the frequency increases, resulting in signal loss. The cable should be kept as short as possible because cable length also determines the amount of signal loss (the longer the run, the greater the loss).

Cisco recommends a high-quality, low-loss cable for use with the lightning arrestor.

Grounding the Access Point

In all installations, after mounting the access point, you must properly ground the unit before connecting power cables.

⚡

Warning

This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available. Statement 1024

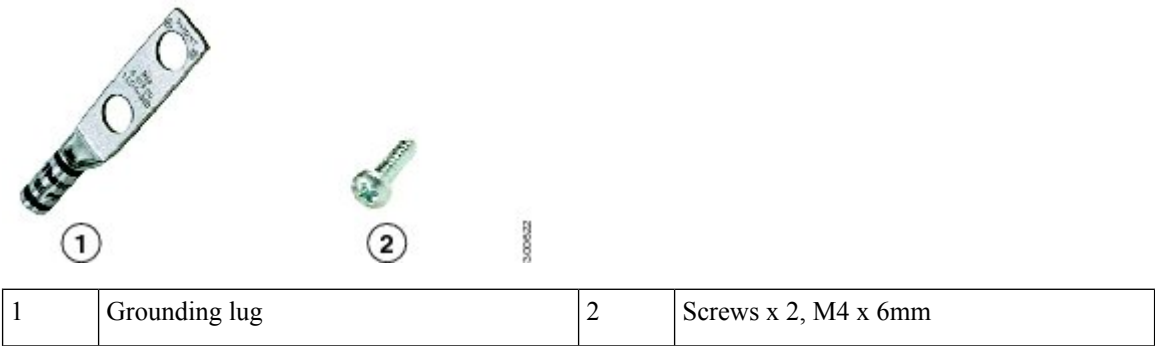
⚡

Warning

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

The access point is shipped with a grounding kit.

Figure 11: Access Point Grounding Kit Contents



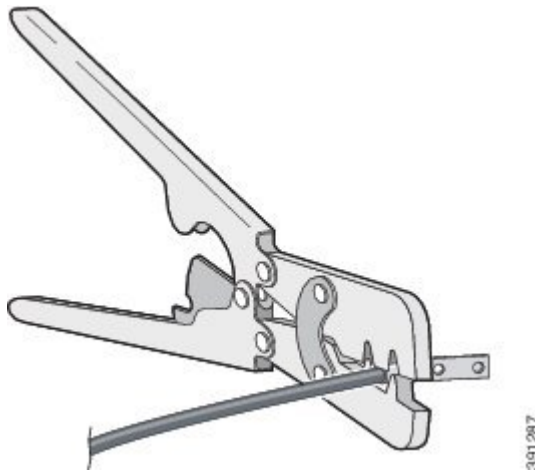
✎

Note

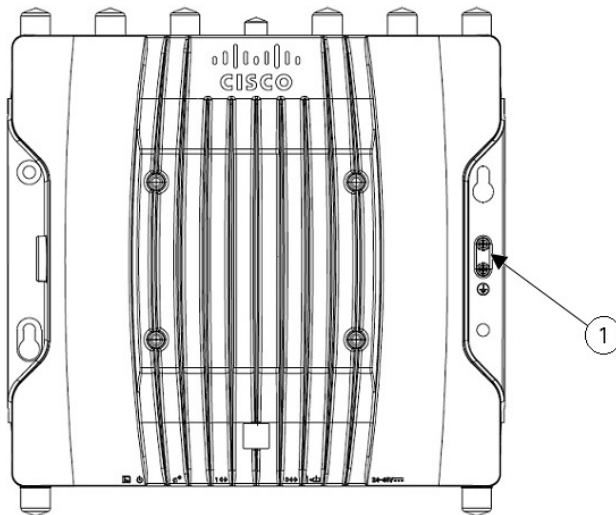
The grounding kit also includes the oxide inhibitor, which is contained in a tube.

To ground the access point:

Step 1 Use a crimping tool to crimp a 6-AWG ground wire (not included in the grounding kit) to the ground lug.



- Step 2** Connect the supplied ground lug to the access point ground connection point using the supplied screws. Apply supplied oxide inhibitor between the ground lug and the access point ground connection.



1	AP ground connection point
---	----------------------------

- Step 3** Tighten the screws to 20-25 inch-lbs of torque.

- Step 4** If necessary, strip the other end of the ground wire and connect it to a reliable earth ground such as a grounding rod or appropriate ground point on a grounded pole. Length of the ground cable should not exceed 1 meter, and 0.5 meter is preferred. Use supplied oxide inhibitor on the grounded interface.

Powering the Access Point

The AP supports these power sources:

- DC power – 24–48 VDC

- Power-over-Ethernet (PoE)

The AP can be powered via the PoE input from an inline power injector or a suitably powered switch port. Depending on the configuration and regulatory domain, the required power for full operation is 802.3bt or UPOE.

Connecting a Power Injector

The AP supports the following power injectors:

Table 6: Supporting Power Injectors

Power Source	Description
AIR-PWRINJ-60RGD1=	60W rated outdoor power injector, with North America AC plug
AIR-PWRINJ-60RGD2=	60W rated outdoor power injector, global version without AC plug
IW-PWRINJ-60RGDMG=	60W rated outdoor power injector, 5GE

The power injector provides DC voltage to the AP over the Ethernet cable and supports a total end-to-end Ethernet cable length of 100 m (328 ft) from the switch to the AP.

When an optional power injector powers your AP, follow these steps to complete the installation:

-
- Step 1** Before applying PoE to the AP, ensure that the AP is grounded (see [Grounding the Access Point, on page 30](#)).
- Step 2** Connect a CAT5e or better Ethernet cable from your wired LAN network to the power injector.
- Warning** To reduce the risk of fire, use only No. 24 AWG or larger telecommunication line cord. Statement 1023
- Note** The installer is responsible for ensuring that powering the AP from this type of power injector is allowed by local and/or national safety and telecommunications equipment standards.
- Step 3** Ensure that the antennas are connected, and that ground is attached to the AP before you apply power to the AP.
- Step 4** Connect a shielded outdoor-rated Ethernet (CAT5e or better) cable between the power injector and the AP's PoE-in connector.
- Step 5** Connect the Ethernet cable to the AP PoE-In port.
-

Connecting a DC Power Cable to the Access Point

When powering the AP with DC power, you must ensure that DC power can be conveniently removed from the unit. The power should not be removed by disconnecting the DC power connector on the unit.



Warning

Connect the unit only to a DC power source that complies with the safety extra-low voltage (SELV) requirements in IEC 60950 based safety standards. Statement 1033

To connect a DC power cable, you need to supply these tools and material:

- Shielded outdoor-rated DC power cable (18 AWG) with outside cable diameter of 0.20 to 0.35 inch (0.51 to 0.89 cm)
- Adjustable or open-end wrench
- Hex crimp tool: 0.10 inch (2.54-mm)

Draft comment:

Need a section for M12 adapter installation and use.

Need a section for DC micro-fit pin out and connection.

To connect the DC power cable to the AP, follow these steps:

-
- Step 1** Before connecting DC power to the AP, ensure that the ground is connected to the AP (see [Grounding the Access Point, on page 30](#)).
- Step 2** Turn off all power sources to the AP, including the DC power source.
- Warning** **This unit might have more than one power supply connection. All connections must be removed to de-energize the unit.** Statement 1028
- Caution** When installing DC power to the AP, always connect the AP end of the cable FIRST. When removing the DC power connector, always disconnect the AP end of the cable LAST.
- Step 3** Remove the cap from the DC connector located on the side of the AP. Do not discard the cap unless you are sure the port will never need to be sealed in the future.
- Step 4** Connect the other end of the power cable to the DC power source using the power source wiring instructions.
-

Connecting Data Cables

This AP supports data connections through the Ethernet port and the Small Form-factor Pluggable (SFP) port. However, both the Ethernet port and the SFP port cannot be used for data simultaneously.

If you are using the SFP port to deliver data through a fiber-optic cable, the AP must be powered by DC power, power adapter, PoE+ power source (?), or a power injector.

Draft comment: Is SFP port supported on all above power source?

For details on installing Ethernet cable, see [Connecting an Ethernet Cable to the Access Point, on page 34](#).

For details on installing a fiber-optic cable, see [Connecting a Fiber-optic Cable to the AP \(AIR-SFP-KIT1=\), on page 34](#).

Draft comment:

Need a section to cover M12 adapter installation and use.

Connecting an Ethernet Cable to the Access Point

Draft comment:

Steps of using PG13.5 glands to be added.

Connecting a Fiber-optic Cable to the AP (AIR-SFP-KIT1=)

The optional Cisco accessory fiber-optic kit enables the AP to support fiber-optic network connections.

You can connect the fiber-optic networking cable to the SFP port. The small form-factor pluggable (SFP) transceiver module connects the cable to the SFP port.

Before you begin

You require the following materials for connecting the fiber-optic cable to the AP:

- Cisco Small form-factor pluggable (SFP) adapter kit
- SFP transceiver module
- Duplex LC fiber-optic cables. The fiber optic cable's outer diameter should be 0.24 to 0.50 inch (6 to 12.7 mm). The cable gland cannot hold a cable with a diameter more than 0.50" (12.7 mm)
- 12-mm wrench or large flat blade or Philips screwdriver
- Adjustable wrench

Step 1 Disconnect all power sources from the AP.

Step 2 Remove the plug from the SFP port by following the guidelines given in this step.

Do not discard the plug unless you are sure the SFP port will never need to be sealed in the future.

- Place the AP on its back (resting on the heat fins) on a stable but padded surface to avoid scratching the paint.
- Using a 12-mm wrench or large flat blade, or Philips screwdriver, turn the SFP port plug counterclockwise and remove it.

Step 3 Insert the SFP module into the SFP port and ensure that it latches properly.

Step 4 Loosen and dis-assemble the SFP adapter gland components.

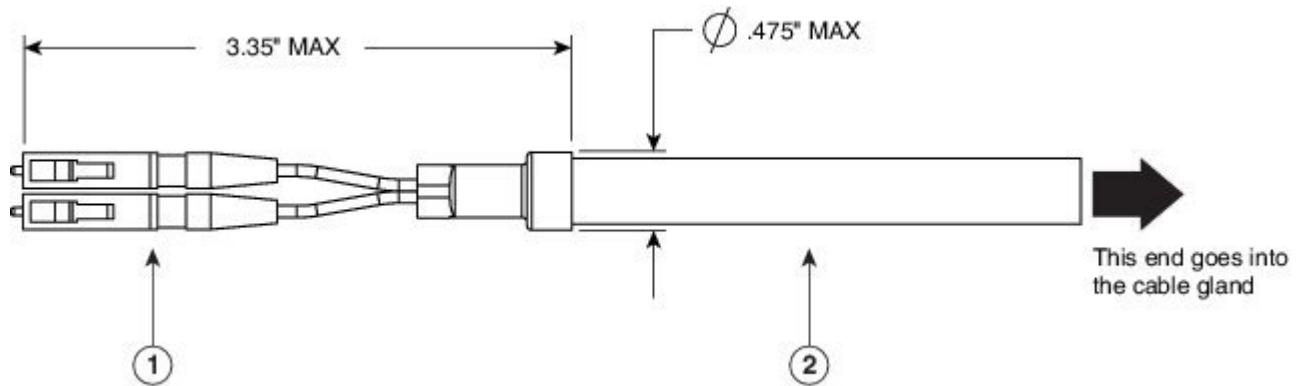
Figure 12: Exploded view of Fiber-Optic cable and Gland assembly

Draft comment: Need both exploded view and installed views

1	SFP Transceiver Module	5	Gland Compression Ferrule
2	Duplex LC Fiber-optic cable	6	Large Cable Rubber Gland 0.30 to 0.50 inch (7.6 to 12.7 mm) diameter
3	SFP Gland Adapter body	7	Small Cable Rubber Gland 0.24 to 0.30 inch (6.0 to 7.6 mm) diameter
4	Body O-ring	8	Gland nut

Step 5 Terminate the fiber optic cable.

Figure 13: Duplex LC Fiber Optic Cable



1	Duplex LC optic fiber connector	2	Optic fiber cable
---	---------------------------------	---	-------------------

Step 6 Using caution not to damage the fiber connector end, pass the fiber connector through the adapter gland components. Ensure components are ordered and orientated, as shown in [Figure 13: Duplex LC Fiber Optic Cable, on page 35](#).

Note Ensure you use the proper rubber gland combination. If the fiber cable outside diameter (OD) is 0.30 to 0.50 inches (7.6 to 12.7 mm), then the small rubber gland can be discarded. If the cable OD is 0.24 to 0.30 inches (6.0 to 7.6 mm), then the small rubber gland is inserted into the large rubber gland.

Step 7 Verify the O-ring is correctly seated on the gland adapter body. Re-assemble the components of the adapter gland. Do not tighten the gland nut on the rubber inserts. Leave it loose so the gland can easily slide on the fiber cable. If you tightened the cable in this step, you might damage the cable.

Step 8 Insert the optic fiber connector-end of the cable into the SFP transceiver module and ensure it latches into place.

Step 9 Thread the adapter body into the SFP port on the AP. Tighten the adapter body by hand until it is fully seated. Inspect that the body is seated correctly. Using an adjustable wrench, tighten the body snugly to the AP body to approximately 13 to 17 lb-in (15 to 20 kgf-cm) of torque.

Step 10 To seal the rubber gland to the fiber cable, hand tighten the gland nut. Using an adjustable wrench, tighten the nut ¼ revolution to make a water-tight seal on the cable to approximately 15 to 22 lbf-in (17 to 25 kgf-cm) torque.

Caution When removing this SFP assembly, you must proceed in the reverse order of this installation. Start by loosening the cable gland's nut.



CHAPTER 4

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](#).

- [Controller Discovery Process, on page 37](#)
- [Deploying the Access Point in a Wireless Network, on page 38](#)
- [Checking the Access Point LEDs, on page 38](#)

Controller Discovery Process

The Cisco AP must join a controller to function as an AP and start serving clients. Cisco uses a process called controller discovery process to join a controller. The devices use Lightweight Access Point Protocol (LWAPP) to communicate with each other. The AP can be plugged associated to a controller regardless of the physical location or logical location in the network. A new AP, out of the box, can be plugged in anywhere regardless of the subnet. After it is plugged in, it locates the controller, receives the controller version of the software image and configuration. After this is sent to the AP, it can start serving clients.

Guidelines and Limitations

- You cannot edit or query any AP using the controller CLI if the AP's name 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 AP might not join the controller because its certificate might 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 AP was previously joined to a controller, the primary, secondary, and tertiary controllers' IP addresses are stored in the AP's non-volatile memory. This process of storing controller IP addresses on an AP for later deployment is called priming the AP. For more information about priming, see [Performing a Preinstallation Configuration \(Optional\), on page 13](#).
- DHCP server discovery: This feature uses DHCP option 43 to provide controller IP address to the AP. Cisco switches support a DHCP server option that is typically used for this capability. For more information about DHCP option 43, see [Configuring DHCP Option 43, on page 42](#).
- DNS discovery: The AP can discover controllers through your domain name server (DNS). For the AP to do so, you must configure your DNS to return controller IP addresses in response to CISCO-CAPWAP-CONTROLLER.localdomain, where localdomain is the AP domain name. Configuring

the CISCO-CAPWAP-CONTROLLER provides backward compatibility in an existing customer deployment. When an AP 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 AP sends discovery requests to the controllers.

Deploying the Access Point in a Wireless Network

After you have mounted the AP, follow these steps to deploy it in a wireless network:

Step 1 Connect the power supply and power up the AP.

Step 2 Observe the AP's LED.

For LED descriptions, see the *Cisco Catalyst IW9167E Heavy Duty Access Point Hardware Installation Guide*.

- a) When you power up the AP, it begins a power-up sequence that you can verify by observing the AP's 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 AP has joined a controller, and there are no clients associated, the LED is green or blue when clients are associated with it.
- b) If the LED is not on, the AP is most likely not receiving power.
- c) If the LED blinks sequentially for more than five minutes, the AP could not find its primary, secondary, and tertiary controller. Check the connection between the AP and the controller, and be sure the AP and the controller are either on the same subnet or that the AP has a route back to its primary, secondary, and tertiary controller. If the AP is not on the same subnet as the controller, be sure that there is a properly configured DHCP server on the same subnet as the AP. See [Configuring DHCP Option 43, on page 42](#) for additional information.

Step 3 Reconfigure the controller so that it is not the primary controller.

Note Use the primary controller to configure the AP only. Avoid using this controller in a working network.

Checking the Access Point LEDs

The location of the AP status LED is shown in [Connectors and Ports, on page 2](#).



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 AP status LED indicates various conditions and are described in the following table.

Table 7: AP LED Signals

LED Message Type	Color	Meaning
Boot loader status sequence	Blinking Green	Boot loader status sequence: <ul style="list-style-type: none"> • DRAM memory test in progress • DRAM memory test OK • Board initialization in progress • Initializing FLASH file system • FLASH memory test OK • Initializing Ethernet • Ethernet OK • Starting AP OS • Initialization successful
Boot loader warnings	Blinking Red	Configuration recovery is in progress (the Reset button has been pushed for 2 to 3 seconds)
	Solid Red	There is an Ethernet failure or an image recovery (the Reset button has been pushed for 20-30 seconds)
	Blinking Green	Image recovery is in progress (the Reset button has been released)
Catalyst OS		
Association status	Chirping (short blips) Green	This status indicates a normal operating condition. The unit is joined to a controller, but no wireless client is associated with it.
	Solid Green	Normal operating condition with at least one wireless client associated with the unit.
Operating Status	Blinking Amber	A software upgrade is in progress.
	Cycling through Green, Red, and Amber	Discovery or join process is in progress.
	Rapidly cycling through Red, Green, Amber, and Off	This status indicates that the AP location command has been invoked.
	Blinking Red	This status indicates that an Ethernet link is not operational.
	Cycling through Red, Green, and Amber	This is a general warning of insufficient inline power.
CURWB OS		

LED Message Type	Color	Meaning
Link Quality/SNR Indicator	Blinking Green	SNR Excellent (≥ 25)
	Fade-in Green	SNR Good ($15 \leq x < 25$)
	Fade-in Amber	SNR Poor ($10 \leq x < 15$)
	Fade-in Red	SNR Unbearable (< 10)
Operating Status	Cycling through Red, Green, and Amber	This is a general warning of insufficient inline power.
Limbo (Provisioning) mode: Fallback	Chirping (short blips) Amber	In the state of requesting IP address from DHCP server.
Limbo (Provisioning) mode: DHCP	Amber	This status indicates that the IP address is retrieved from DHCP server.



CHAPTER 5

Troubleshooting

- [Using the Reset Button, on page 41](#)
- [Troubleshooting the Access Point to Controller Join Process, on page 42](#)
- [Important Information for Controller-based Deployments, on page 42](#)
- [Configuring DHCP Option 43, on page 42](#)

Using the Reset Button

Using the **Reset** button (see [Connectors and Ports, on page 2](#)), you can reset the AP to factory default or clear the AP's internal storage.



Note Using the **Reset** button does not change the booting OS (CAPWAP or URWB).

To reset the AP to the default factory-shipped configuration, perform the following steps:

-
- Step 1** Press, and continue to press the **Reset** button on the access point during the AP boot cycle.
- Step 2** Press until the AP status LED changes to blinking red. It indicates that the Reset signal has been caught by u-boot.
- Step 3**
- Press the **Reset** button for less than 20 seconds to reset the AP to the default factory-shipped configuration. The AP configuration files are cleared.
 - Press the **Reset** button for more than 20 seconds, but less than 60 seconds to clear the AP internal storage, including all the configuration files.
- Note**
- If the **Reset** 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. If the FIPS flag is set, the console access is disabled.
 - The AP status LED changes to solid red, and all the files in the AP storage directory are cleared.
 - If you keep the **Reset** button pressed for more than 60 seconds, the button is assumed as being faulty and no changes are made.
-

Troubleshooting the Access Point to Controller Join Process

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

Controller software enables you to configure the AP to send all CAPWAP-related errors to a syslog server. You do not have to enable any debug commands on the controller. View all the of the CAPWAP error messages from the syslog server itself.

The AP is not maintained on the controller until it receives a CAPWAP join request from the AP. Therefore, it can be challenging to determine why the CAPWAP discovery request from a particular AP was rejected. To troubleshoot such joining problems without enabling CAPWAP debug commands on the controller, the controller collects information for all APs that send a discovery message and maintains information for any AP that has successfully joined it.

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

When the controller maintains join-related information for the maximum number of APs, it does not collect information for any more APs.

An AP 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 AP using option 7 on the server. The AP then starts sending all syslog messages to this IP address.

You can configure the syslog server for APs and view the AP join information only from the controller CLI interface.

Important Information for Controller-based Deployments

Keep these guidelines in mind when you use the AP:

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

The following is a DHCP Option 43 configuration example on a Microsoft Windows 2003 Enterprise DHCP server for Cisco Catalyst lightweight APs. For other DHCP server implementations, consult the product

documentation to configure DHCP Option 43. In Option 43, use the IP address of the controller management interface.



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

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

Cisco AP IW9167EH

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 controller management interfaces listed sequentially in hexadecimal format.

SUMMARY STEPS

1. Enter configuration mode at the Cisco IOS CLI.
2. Create the DHCP pool, including the necessary parameters such as default router and name server. A DHCP scope example is as follows:
3. Add the option 43 line using the following syntax:

DETAILED STEPS

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 IW9167EH
<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 6

Safety Guidelines and Warnings

- [FCC Safety Compliance Statement, on page 45](#)
- [Safety Precautions, on page 45](#)
- [Safety Precautions when Installing Antennas, on page 46](#)
- [Avoiding Damage to Radios in a Testing Environment, on page 47](#)
- [Performing Site Surveys, on page 48](#)

FCC Safety Compliance Statement

The FCC, with its action in ET Docket 96-8, has adopted a safety standard for human exposure to RF electromagnetic energy emitted by FCC-certified equipment. When used with approved Cisco antennas, Cisco Catalyst products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio device according to the instructions in this publication results in user exposure substantially below the FCC recommended limits.

Safety Precautions

For safety and to achieve a good installation, please read and follow these safety precautions:

- Select your installation site with safety as well as performance in mind. Remember: electric power lines and phone lines look alike. For safety, assume that any overhead line can kill.
- Call your electric power company. Tell them your plans, and ask them to come to look at your proposed installation
- Plan your installation carefully and thoroughly before you begin. Successful raising of a mast or tower is mostly a matter of coordination. Each person should be assigned to a specific task and know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.
- When installing the AP or its antennas, remember:
 - Do not use a metal ladder.
 - Do not work on a wet or windy day.
 - Do dress properly—shoes with rubber soles and heels, rubber gloves, long-sleeved shirt or jacket.

- Use a rope to lift the AP. If the assembly starts to drop, get away from it and let it fall.
- If any part of the antenna system comes in contact with a power line, do not touch it or remove it yourself. Call your local power company. They will remove it safely.

If an accident should occur, call for qualified emergency help immediately.

Safety Precautions when Installing Antennas



Danger

Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.: NFPA 70, National Electrical Code, Article 810, Canada: Canadian Electrical Code, Section 54). Statement 280

- Before you install an antenna, contact your Cisco account representative to explain which mounting method to use for the size and type of antenna that you are about to install
- Select your installation site with safety, as well as performance, in mind. Remember that electric power lines and phone lines look alike. For your safety, assume that any overhead line can kill you.
- Contact your electric power company. Tell them your plans and ask them to come look at your proposed installation.
- Plan your installation carefully and completely before you begin. Each person involved in an installation should be assigned to a specific task and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.
- When installing your antenna, follow these guidelines:
 - Do not use a metal ladder
 - Do not work on a wet or windy day
 - Do dress properly—wear shoes with rubber soles and heels, rubber gloves, and a long-sleeved shirt or jacket
- If the assembly starts to drop, move away from it and let it fall. Because the antenna, mast, cable, and metal guy wires are all excellent conductors of electrical current, even the slightest touch of any of these parts to a power line completes an electrical path through the antenna and the installer.
- If any part of the antenna system should come in contact with a power line, do not touch it or try to remove it yourself. Call your local power company to have it removed safely.
- If an accident should occur with the power lines, call for qualified emergency help immediately.

Avoiding Damage to Radios in a Testing Environment

The radios on outdoor units (bridges) have higher transmit power levels than radios on indoor units (APs). When you test high-power radios in a link, you must avoid exceeding the receiver's maximum receive input level. At levels above the normal operating range, packet error rate (PER) performance is degraded. At even higher levels, the receiver can be permanently damaged. To avoid receiver damage and PER degradation, you can use one of the following techniques:

- Separate the omnidirectional antennas by at least 2 ft (0.6 m) to avoid receiver damage or by at least 25 ft (7.6 m) to avoid PER degradation.



Note These distances assume free space path loss and are conservative estimates. Required separation distances for damage and performance degradation levels in actual deployments are less if conditions are not non-line-of-sight.

- Reduce the configured transmit power to the minimum level.
- Use directional antennas, and keep them away from each other.
- Cable the radios together using a combination of attenuators, combiners, or splitters to achieve a total attenuation of at least 60 dB.

For a radiated testbed, the following equation describes the relationships among transmit power, antenna gain, attenuation, and receiver sensitivity:

$$\text{txpwr} + \text{tx gain} + \text{rx gain} - [\text{attenuation due to antenna spacing}] < \text{max rx input level}$$

Where:

txpwr = Radio transmit power level

tx gain = transmitter antenna gain

rx gain = receiver antenna gain

For a conducted test bed, the following equation describes the relationships among transmit power, antenna gain, and receiver sensitivity:

$$\text{txpwr} - [\text{attenuation due to coaxial components}] < \text{max rx input level}$$


Caution Under no circumstances should you connect the antenna port from one AP to the antenna port of another AP without using an RF attenuator. If you connect antenna ports, you must not exceed the maximum survivable receive level of 0 dBm. Never exceed 0 dBm, or damage to the AP can occur. Using attenuators, combiners, and splitters having a total of at least 60 dB of attenuation ensures that the receiver is not damaged and that PER performance is not degraded.

Performing Site Surveys

Every network application is a unique installation. Before installing multiple APs, you should perform a site survey to determine the optimum use of networking components and maximize range, coverage, and network performance.

Site surveys reveal problems that can be resolved before the network is operational. Because 802.11a/b/g/n/ac/ax operates in an unlicensed spectrum, there may be sources of interference from other 802.11a wireless devices (especially in multi-tenant buildings) that could degrade your 802.11 signals. A site survey can determine if such interference exists at the time of deployment.

Consider the following operating and environmental conditions when performing a site survey:

- **Data rates:** Sensitivity and range are inversely proportional to data bit rates. The maximum radio range is achieved at the lowest workable data rate. A decrease in receiver sensitivity occurs as the radio data increases.
- **Antenna type and placement:** Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, range increases in proportion to antenna height. However, do not place the antenna higher than necessary because the extra height also increases potential interference from other unlicensed radio systems and decreases the wireless coverage from the ground.
- **Physical environment:** Clear or open areas provide better radio range than closed or filled areas.
- **Obstructions:** Physical obstructions such as buildings, trees, or hills can hinder the performance of wireless devices. Avoid locating the devices in a location where there is an obstruction between the sending and receiving antennas.
- How far is your wireless link?
- Has a previous site survey been conducted?
- Do you have a clear Fresnel zone between the APs or radio line of sight?
- What is the minimum acceptable data rate within the link?
- Do you have the correct antenna (if more than one antenna is being offered?)
- Do you have the proper permits, if required?
- Are you following the proper safety procedures and practices?
- Have you configured the APs before you go onsite? It is always easier to resolve configurations or device problems first.
- Do you have the proper tools and equipment to complete your survey?



CHAPTER 7

Declarations of Conformity and Regulatory Information

- [Manufacturers Federal Communication Commission Declaration of Conformity Statement, on page 49](#)
- [Operation of Cisco Catalyst Access Points in México, on page 50](#)
- [VCCI Statement for Japan, on page 50](#)
- [Compliance Statement for Canada, on page 52](#)
- [European Community, Switzerland, Norway, Iceland, and Liechtenstein, on page 53](#)
- [Operation of Cisco Catalyst Access Points in Brazil, on page 53](#)
- [Declaration of Conformity for RF Exposure, on page 54](#)
- [Declaration of Conformity Statements, on page 57](#)

Manufacturers Federal Communication Commission Declaration of Conformity Statement



Access Point Models	Certification Number
IW9167EH-B	LDKIW9167EH

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.

Federal Communication Commission Interference Statement

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 the user will be required to correct the interference at his own expense.



Caution

The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using the integrated antennas. Any changes or modification to the product not expressly approved by Cisco could void the user's authority to operate this device.

Operation of Cisco Catalyst Access Points in México

Declaración para México

La operación de este equipo está sujeta a las siguientes dos condiciones: (1) es posible que este equipo o dispositivo no cause interferencia perjudicial y (2) este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.

VCCI Statement for Japan

Statement 191—Voluntary Control Council for Interference (VCCI) Class A Warning for Japan



Warning

This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case, you may be required to take corrective actions.

ステートメント 191—日本向け VCCI クラス A に関する警告



警告 この装置は、クラス A 機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

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

208637

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**

Compliance Statement for Canada

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device. Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication. Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This radio transmitter has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device. Le présent émetteur radio a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

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. La bande 5 150-5 250 MHz est réservée uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Users are advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices. Les utilisateurs êtes avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5 250-5 350 MHz et 5 650-5 850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Industry Canada

Access Point Models	Certification Number
IW9167EH-A	IC:2461A-IW9167EH

European Community, Switzerland, Norway, Iceland, and Liechtenstein

Access Point Models:

IW9167EH-E

This equipment complies with EU radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm (7.87 inches) 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.

The product carries the CE Mark:



Operation of Cisco Catalyst Access Points in Brazil

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

Access Point Models	Certification Number
IW9167EH-ROW	Draft comment: TBD

Figure 14: 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.

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 IW9167EH 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.

Table 8: Separation Distance

MPE	Distance
	20 cm

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 the antennas at a greater separation distance than recommended.

This Device Meets FCC Guidelines for Exposure to Radio Waves

The IW9167EH 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.

Table 9: Separation Distance

MPE	Distance
	100 cm

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 IW9167EH 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 10: Separation Distance

Frequency	Distance
	43 cm

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 IW9167EH 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 11: Distance d'éloignement

Fréquence	Distance
	43 cm

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 International Commission on Non-Ionizing Radiation Protection at this URL: www.who.int/emf
- United Kingdom, National Radiological Protection Board at this URL: www.nrpb.org.uk
- Cellular Telecommunications Association at this URL: www.wow-com.com
- The Mobile Manufacturers Forum at this URL: www.mmfa.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/pdtncc/#/>