



# Cisco IW3702 Access Point Getting Started Guide

**First Published:** July 2015

**Last Updated:** August 2016

This guide documents the hardware features of the Cisco IW3702 access point. It describes the physical and performance characteristics of each access point, and explains how to install and configure an access point.

This publication is for the network technicians who install and configure access points. You must be familiar with network structures, terms, and concepts.

The Cisco IW3702 access point is referred to as *access point* in this document.

## Organization

This guide includes the following sections:

Section	Description
<a href="#">Conventions, page 1</a>	Describes text conventions used in this document.
<a href="#">Overview, page 2</a>	Describes the major components and features of the access point.
<a href="#">Installation, page 11</a>	Provides warnings, safety information, and installation information you need to install your access point.
<a href="#">Antennas, page 19</a>	Provides information about the antennas used by the access point and the antenna configurations deployed.
<a href="#">Configuration, page 30</a>	Describes the steps to configure the access point.
<a href="#">Technical Specifications, page 40</a>	Lists technical specifications for the access point.
<a href="#">Ports and Connectors, page 48</a>	Describes the port and connector pinouts for the access point.

## Conventions

This document uses the following conventions.

Convention	Indication
<b>bold font</b>	Commands and keywords and user-entered text appear in <b>bold font</b> .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[ ]	Elements in square brackets are optional.
{x   y   z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[ x   y   z ]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Convention	Indication
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

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

**Caution:** Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

**Warning:** **IMPORTANT SAFETY INSTRUCTIONS**

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**

**Regulatory:** Provided for additional information and to comply with regulatory and customer requirements.

## Overview

This document describes the Cisco IW3702 access point. The access point is an IEEE 802.11a/b/g/n/ac compliant, dual-band WiFi access point with external antennas.

The access point is IP67 rated, ruggedized, and certified for on-board rail and outdoor use-cases such as train and trackside, mining, intelligent transportation systems, and smart city applications. You can mount the access point on a DIN rail in an industrial enclosure. Its components are designed to withstand extremes in temperature, vibration, and shock common in industrial environments.

The access point features:

- IEEE 802.11a/b/g/n compliant operation
- IEEE 802.11ac Wave 1 support
- Dual-radio design for 2.4 GHz and/or 5 GHz bands
- 4x4 multiple-input multiple-output (MIMO) technology with three spatial streams
- Cisco CleanAir support for 20, 40, and 80 MHz channels
- DC input port (M12 connector)
- 2 Power over Ethernet (PoE) ports with M12 X-code connectors:
  - 1 x PoE-IN Gigabit Ethernet port compliant with IEEE 802.3at POE+ PD
  - 1 x PoE-OUT Gigabit Ethernet port compliant with IEEE 802.3af POE PSE
- RS232 console port with cover (RJ-45 connector)

## Overview

- 4 antenna ports (N connector-female)
- Rugged IP67 rated housing and -40 to 167°F (-40 to 75°C) operating temperature range (ambient–without solar loading or wind cooling)
- Compact size for space constrained environments

## Access Point Models

There are two access point models, based on antenna configuration. [Table 1 on page 3](#) lists the available IW3702 models.

**Table 1 Access Point Models**

Model	Description
Cisco IW3700 Series Access Points with Regulatory Domain Code <sup>1</sup>	
IW3702-2E-x-K9	Access point with four antenna connectors: 2 on the top and 2 on the bottom.
IW3702-4E-x-K9	Access point with four antenna connectors on top side.
Cisco IW3700 Series Universal Access Points	
IW3702-2E-UXX9	Access point with four antenna connectors: 2 on the top and 2 on the bottom.
IW3702-4E-UXX9	Access point with four antenna connectors on top side.

1. Regulatory Domains: (x=regulatory domains)  
Domain codes available for the IW3700 Series are x=A, B, D, E, M, R, and Z. Other regulatory domains are supported by the universal access points. Customers are responsible for verifying approval for use in their individual countries. To verify approval and to identify the regulatory domain that corresponds to a particular country, visit <http://www.cisco.com/go/aironet/compliance>.

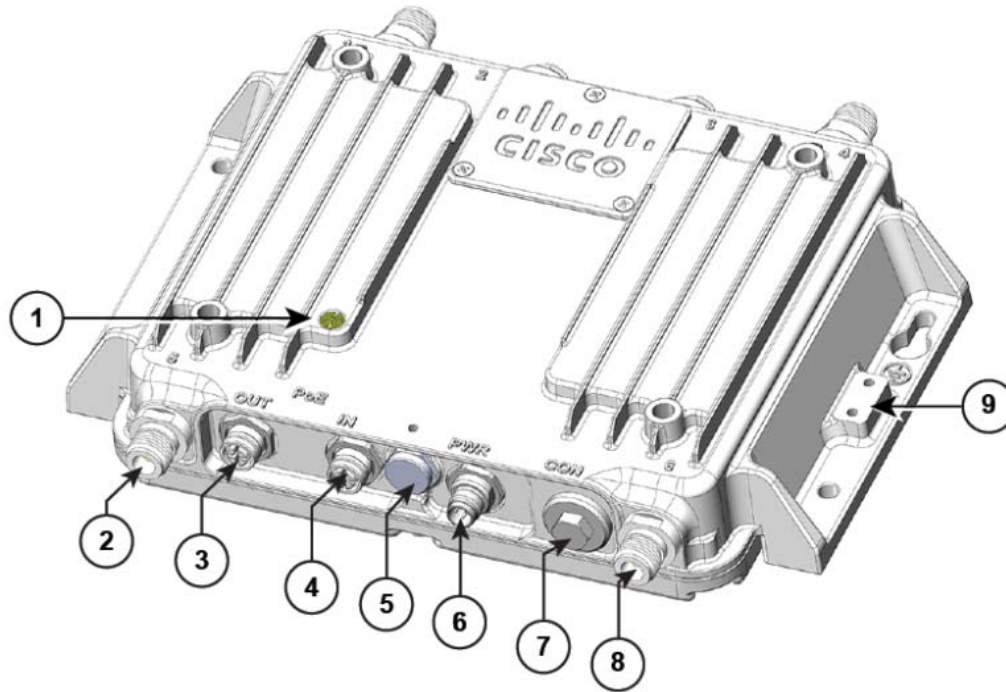
## Assembly Details

- [Bottom and Top Panel Views, page 3](#)
- [Bottom Panel Components, page 7](#)
- [Top Panel Components, page 10](#)

### Bottom and Top Panel Views

- [Cisco IW3702-2E-UXX9 / IW3702-2E-x-K9 Bottom Panel View, page 4](#)
- [Cisco IW3702-2E-UXX9 / IW3702-2E-x-K9 Top Panel View, page 5](#)
- [Cisco IW3702-4E-UXX9 / IW3702-4E-x-K9 Bottom Panel View, page 6](#)
- [Cisco IW3702-4E-UXX9 / IW3702-4E-x-K9 Top Panel View, page 7](#)

## Cisco IW3702-2E-UXK9 / IW3702-2E-x-K9 Bottom Panel View

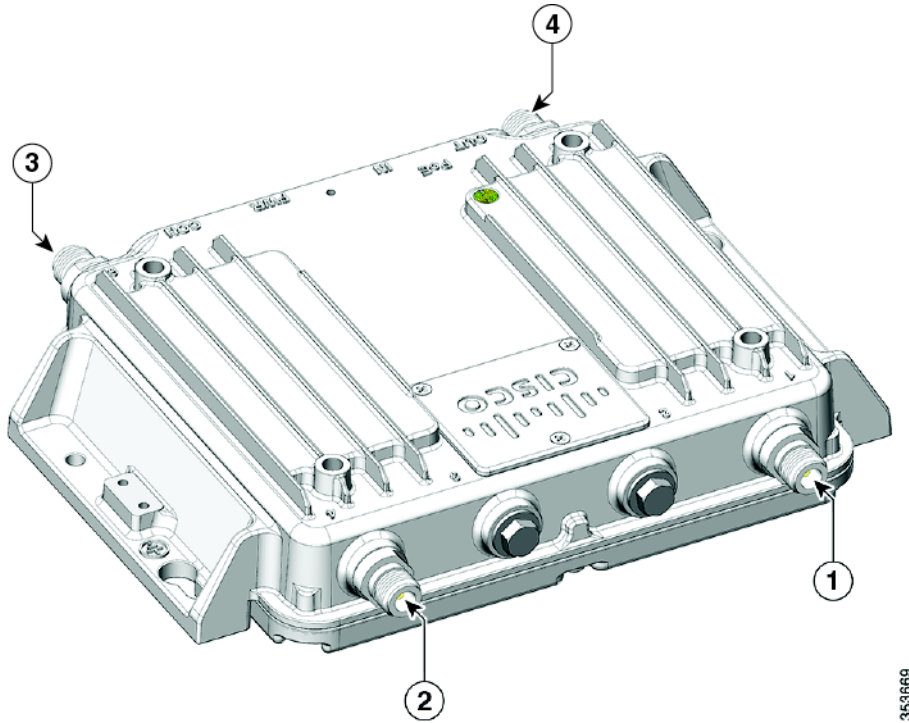
**Figure 1** Cisco IW3702-2E-UXK9 / IW3702-2E-x-K9 Bottom Panel View

1	Status LED	6	Power (PWR) connector
2	Antenna port B	7	Console (CON) port
3	PoE OUT port	8	Antenna port A
4	PoE IN port	9	Ground connection
5	Protective vent port / Reset button (covered)		

**Note:** There are four antenna ports on the Cisco IW3702-2E-UXK9 / IW3702-2E-x-K9 model: 2 on the top and 2 on the bottom.

Cisco IW3702-2E-UXX9 / IW3702-2E-x-K9 Top Panel View

Figure 2 Cisco IW3702-2E-UXX9 / IW3702-2E-x-K9 Top Panel View

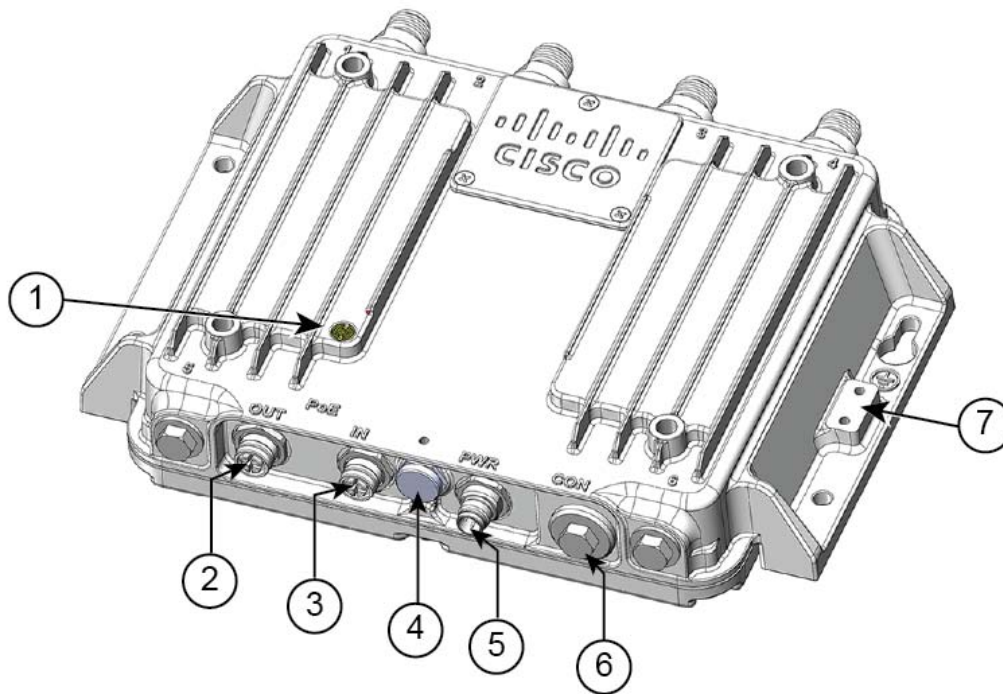


1	Antenna port C	3	Antenna port A
2	Antenna port D	4	Antenna port B

**Note:** There are four antenna ports on the Cisco IW3702-2E-UXX9 / IW3702-2E-x-K9 model: 2 on the top and 2 on the bottom.

## Overview

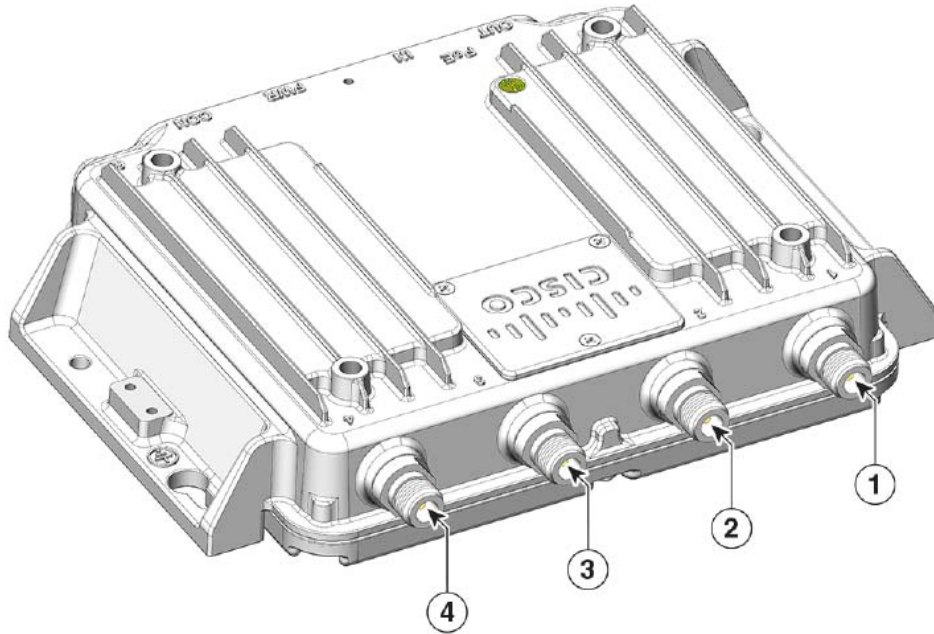
## Cisco IW3702-4E-UXK9 / IW3702-4E-x-K9 Bottom Panel View

**Figure 3 Cisco IW3702-4E-UXK9 / IW3702-4E-x-K9 Bottom Panel View**

1	Status LED	5	Power (PWR) connector
2	PoE OUT port	6	Console (CON) port
3	PoE IN port	7	Ground connection
4	Protective vent port / Reset button (covered)		

## Overview

## Cisco IW3702-4E-UXX9 / IW3702-4E-x-K9 Top Panel View

**Figure 4 Cisco IW3702-4E-UXX9 / IW3702-4E-x-K9 Top Panel View**

1	Antenna port C	3	Antenna port B
2	Antenna port A	4	Antenna port D

## Bottom Panel Components

This section describes the bottom panel components shown in [Figure 1 on page 4](#) and [Figure 3 on page 6](#):

- [Status LED, page 7](#)
- [PWR Connectors, page 9](#)
- [Console Port, page 10](#)
- [PoE IN Port, page 9](#)
- [PoE OUT Port, page 9](#)
- [Ground Stud, page 10](#)
- [Protective Vent Port, page 9](#)

## Status LED

The Status LEDs provide information on access point status, activity, and performance. [Table 2 on page 8](#) describes Status LED states.

**Table 2** Status LED

Message Type	LED Color	System State
Boot loader status	Blinking pink	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 Cisco IOS.
Client association status	Green	Normal operating condition but no wireless client association.
	Blue	Normal operating condition with at least one wireless client association.
Operational status	Blinking blue	Software upgrade in progress.
	Cycling green-red-off	Discovery/join process in progress.
	Rapidly cycling blue-green-red	Access point location command invoked.
	Blinking red	Ethernet link not operational.
Boot loader warnings	Blinking blue	Configuration recovery in progress (MODE button pushed for 2 to 3 seconds).
	Red	Ethernet failure or image recovery (MODE button pushed for 20 to 30 seconds).
	Blinking pink	Image recovery in progress (MODE button released).
Boot loader errors	Red	DRAM memory test failure.
	Blinking red-blue	FLASH file system failure.
	Blinking red-off	Environment variable failure.
		Bad MAC address.
		Ethernet failure during image recovery.
		Boot environment failure.
		No Cisco image file.
Boot failure.		
Cisco IOS errors	Red	Software failure. Disconnect and reconnect unit power.
	Cycling blue-green-red-off	General warning. Insufficient inline power.
AP status when provisioned by Cisco AirProvision	Cycling red-green-off	AP waiting to be primed.
	Blinking white	AP priming via Cisco NDP in progress.
	Blinking teal (for 15 seconds)	AP upon successful connection to Cisco AirProvision.
	Blinking blue	AP priming via Cisco AirProvision in progress.
	Chirping red	AP primed to wrong regulatory domain.



## Overview

## PWR Connectors

There are two options for powering the access point:

- DC input over the PWR connector.
- PoE inline power over the PoE IN port.

**Notes:** ■ **When powering the access point:**

- **Power can be supplied via DC input (PWR connector) or PoE inline (PoE IN port), but not both.**
- We recommend that you not use two power options concurrently, but no harm results if both are present.
- If using both power inputs, DC input (PWR connector) power takes precedence and PoE inline power is not used.
- Power supply redundancy is not supported.

The access point requires a DC power supply. To power the access point with a DC power supply, you connect the DC power to the PWR connector on the bottom panel (see [Figure 1 on page 4](#) and [Figure 4 on page 7](#)). The DC input voltage range is +12 to +48 VDC (-20%, +25%).

The PWR connector is an M12 A-code, 4-pin (male) connector. See [Power Port, page 49](#) and [DC Input and PoE IN Specifications, page 41](#).

## PoE OUT Port

**Note:** The PoE OUT port is only supported when the access point is powered over the PWR port. When powered over the PoE IN port, PoE OUT functionality is not supported.

The PoE OUT port is a 10/100/1000 BASE-T port with an M12 X-code connector. The PoE OUT port supplies PoE inline DC power to power external devices. The PoE OUT port pin-out conforms to Alternative A-MDIX mode.

**Note:** PoE inline power supports IEEE 802.3af compliant devices and delivers up to 15.4 W of PoE.

For more information about the PoE OUT, PoE IN, and DC input, see [DC Input and PoE IN Specifications, page 41](#).

## PoE IN Port

The PoE IN port is a 10/100/1000 BASE-T port with an M12 X-code connector. The port has auto-sensing and auto-MDIX capabilities.

- Notes:**
- The PoE IN port is an alternate power input to DC input over the PWR port.
  - Power the access point over the PWR port to enable the PoE OUT port.
  - When powered over the PoE IN port, PoE OUT functionality is not supported.

For more information, see [DC Input and PoE IN Specifications, page 41](#).

## Protective Vent Port

The protective vent port relieves pressure inside the access point chassis possibly caused by changing temperatures in the installation environment. The vent prevents pressure from building up and damaging enclosure seals and potentially exposing sensitive components to water. The vent also protects the access point interior from dust, dirt, water, and other environmental elements.

## Overview

**Note:** If the vent is removed or damaged, the access point is subject to moisture damage.

### Reset Button

You use the reset button to reset the access point or reload the software. The reset button is under the protective vent port. To access the reset button:

1. Use a 5/8" socket to remove the protective vent.
2. Press the reset button.
  - Press the reset button for 3 seconds to reset the access point to its factory settings.
  - Press the reset button for 20 seconds to reload the access point software.
3. Replace the protective vent using 5/8" socket.
4. Torque the protective vent to 5-7 inch-lbs.

### Console Port

You can connect the access point to a PC or laptop through the RJ45 CON port. The RJ45 CON port uses the Cisco console port RJ45-to-DB9 cable (Cisco PN 72-3383-01).

A cable port seal covers the CON port. This liquid-tight plug protects the access point from environmental elements. Ensure that the plug is installed during normal operation or when unit is unattended. You can remove and install the port plug with a 1/2" (13 mm) socket. Torque it to 6-7 ft-lbs

For more information, see [Console Port, page 51](#).

### Ground Stud

The ground stud is the access point ground. You use screws to attach the wired grounding lug to the ground stud ([Figure 7 on page 16](#)). Connect the other end of the ground wire to an earth ground such as a grounding rod or appropriate ground point on a grounded pole.

## Top Panel Components

This section describes the top panel components shown in [Figure 5 on page 11](#).

### Antenna Port

The antenna connector is a type N female coaxial connector.

### Hard Points

The hard points are alternate mounting or attachment points for additional equipment such as directional antennas or covers.

**Note:** Do not attach third-party radios using these hard points.

**Figure 5 Cisco IW3702 Series Access Point Hard Points**

353679

1	Hard points 1/4-20UNC-2B, .45" deep
---	-------------------------------------

## Management Options

You can manage the access point using the following options:

- Web browser Interface—Contains management pages to change the wireless device settings, upgrade firmware, and monitor and configure other wireless devices on the network.
- Cisco IOS command-line interface (CLI)—Configures the access point. You can access the CLI by directly connecting a PC to the console port, or you can access the CLI using a Telnet session from a remote management station.

## Installation

You can install the access point on a wall, ceiling or pole, in a cabinet or rack, under a seat, or in a plenum airspace. You can direct mount, DIN rail mount, or attach the access point on a pole mounting bracket.

Perform the installation procedures in this order:

1. [Preparing for Installation, page 12](#)
2. [Unpacking the Components, page 14](#)
3. [Mounting the Access Point, page 15](#)
4. [Connecting the Protective Ground and Power, page 15](#)
5. [Connecting the Antennas, page 18](#)
6. [Connecting to Access Point Ports, page 18](#)

## Preparing for Installation

The following topics prepare you for installing the unit:

- [Warnings, page 12](#)
- [EMC Environmental Conditions for Products Installed in the European Union, page 13](#)
- [National Restrictions within the European Union, page 13](#)
- [Tools and Hardware Required, page 13](#)
- [Installation Guidelines, page 13](#)
- [Site Surveys, page 14](#)

## Warnings

These warnings are translated into several languages in the *Regulatory Compliance and Safety Information for the Cisco IW3702 Access Point* on Cisco.com.

**Warning: Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

**Warning: In order to comply with FCC radio frequency (RF) exposure limits, antennas for this product should be located a minimum of 7.9 in. (20 cm) or more from the body of all persons.** Statement 332

**Warning: Read the installation instructions before you connect the system to its power source.** Statement 1004

**Warning: This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

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

**Warning: To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 70° C** Statement 1047

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

**Warning: This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 15 A.** Statement 1005

**Warning: Do not operate your wireless network device near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.** Statement 245B

**Caution:** The fasteners you use to mount an access point on a ceiling must be capable of maintaining a minimum pullout force of 20 lbs (9 kg) and must use all 4 indented holes on the mounting bracket.

**Note:** The access point is suitable for use in environmental air space 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, C22.1. You should not install the power supply or power injector in air handling spaces.

**Note:** Use only with listed ITE equipment.

## EMC Environmental Conditions for Products Installed in the European Union

This section applies to products installed in the European Union. The equipment is intended to operate under the following environmental conditions with respect to EMC:

- A separate defined location under the user's control.
- Earthing and bonding meets the requirements of ETSI EN 300 253 or ITU-T K.27.
- AC-power distribution shall be one of the following types, where applicable: TN-S and TN-C as defined in IEC 60364-3.

In addition, if equipment is operated in a domestic environment, interference could occur.

## National Restrictions within the European Union

Within the European Union as well as within the majority of the other European Countries, the 2.4 and 5 GHz bands are available for use by wireless LANs.

[Table 3 on page 13](#) provides an overview of the regulatory requirements that are generally applicable for 2.4 and 5 GHz bands.

The requirements for any country might evolve. We recommend that you check with your local authorities for the current status of regulations for 2.4 and 5 GHz wireless LANs within your country.

**Table 3 Overview of Regulatory Requirements for Wireless LANs**

Frequency Band (MHz)	Maximum Power Level Effective Isotropic Radiated Power (EIRP) mW	Indoor only	Indoor and Outdoor
2400–2483.5	100	–	x
5150–5350	200	x	–
5470–5725	1000	–	x

## Tools and Hardware Required

These tools and hardware are required for access point installation:

- Crimping tool (such as Thomas & Bett part number WT2000, ERG-2001, or equivalent)
- 6-gauge copper ground wire
- Wire-stripping tools for stripping 6-gauge wire
- Number 2 Phillips screwdriver
- 1/2" (13 mm) socket for port plug
- 5/8" (16 mm) socket for protective vent
- 5/32" (4 mm) hex key for mounting screws
- Torque wrench (both inch-lbs and ft-lbs)

## Installation Guidelines

Because the access point is a radio device, it is susceptible to common causes of interference that can reduce throughput and range. Follow these guidelines to ensure the best possible performance:

## Installation

- For information on planning and initially configuring your Cisco Mesh network, refer to the [Cisco Wireless Mesh Access Points, Design and Deployment Guide](#).
- Review the *FCC Guidelines for Installation and Operation of Outdoor Wireless LAN Devices (U-NII devices) Operating in the 5470-5725 MHz Band Data Sheet* at: [http://www.cisco.com/c/en/us/products/collateral/routers/3200-series-rugged-integrated-services-routers-isr/data\\_sheet\\_c78-647116.html](http://www.cisco.com/c/en/us/products/collateral/routers/3200-series-rugged-integrated-services-routers-isr/data_sheet_c78-647116.html)  
  
The above document provides guidelines to mitigate interference to Federal Aviation Administration (FAA) Terminal Doppler Weather Radar (TDWR) as well as details on registering your access point with the Wireless Internet Service Providers Association (WISPA).
- Perform a site survey before beginning the installation.
- Install the access point in an area where structures, trees, or hills do not obstruct radio signals to and from the devices.
- For information on priming a Cisco universal access point, see the *Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide* at: [http://www.cisco.com/c/en/us/td/docs/wireless/access\\_point/ux-ap/guide/uxap-mobapp-g.html](http://www.cisco.com/c/en/us/td/docs/wireless/access_point/ux-ap/guide/uxap-mobapp-g.html)

## Site Surveys

Every network application is a unique installation. Before installing an access point, perform a site survey to determine the optimum use of networking components and maximize range, coverage, and network performance.

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

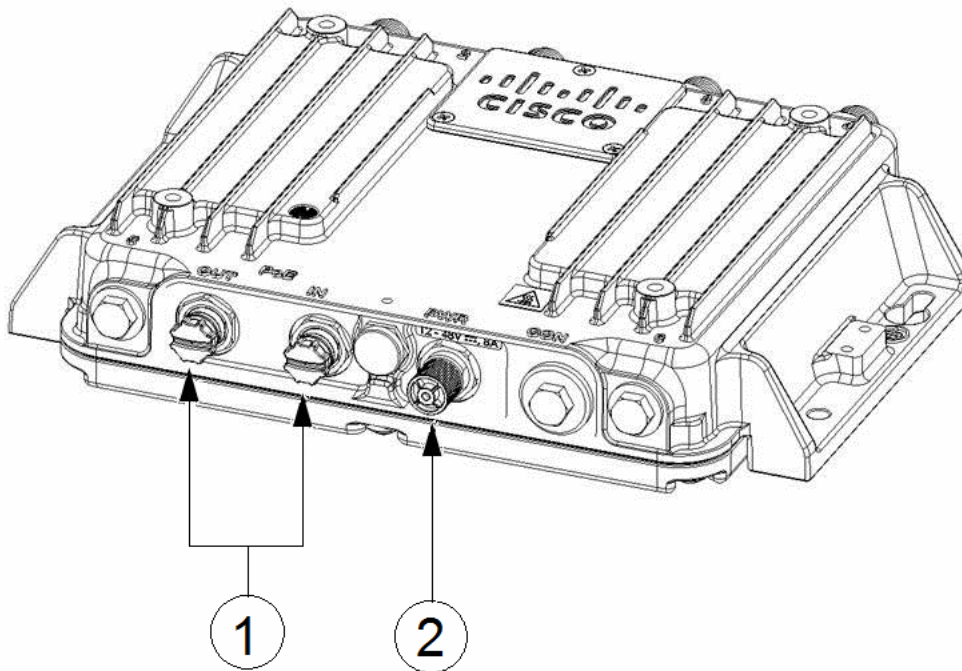
- Data rates—Sensitivity and range are inversely proportional to data bit rates. The maximum radio range is achieved at the lowest workable data rate. A decrease in receiver sensitivity occurs as the radio data increases.
- Antenna type and placement—Proper antenna configuration is a critical factor 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 extra height 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 performance of wireless devices. Avoid locating the devices in a location where an obstruction exists between the sending and receiving antennas.

## Unpacking the Components

The typical access point package contains the following items:

- Access point
- Cisco product documentation and translated safety warnings
- Ground lug (Panduit PLCD6-10A-L), screws, and oxide inhibitor (contained in a tube)
- Console cable
- CoaxSeal—Coaxial cable/connector seal tape for N connectors
- Two M12 Ethernet connector caps (installed on the PoE OUT and PoE IN ports)
- One M12 power connector cap (installed on the PWR port)

**Note:** The M12 connector caps are installed on the ports for protection when the AP is shipped. Remove the caps before using the ports. See [Figure 6 on page 15](#) for the locations of each port with M12 cap.

**Figure 6 PoE and PWR Connectors With Caps**

1	PoE ports with caps	2	PWR connector with cap
---	---------------------	---	------------------------

To unpack the access point:

1. Open the shipping container and carefully remove the contents.
2. Return all packing materials to the shipping container, and save it.
3. Ensure that all the access point package items are included in the shipment.

**Note:** If any item is damaged or missing, notify your sales representative.

## Mounting the Access Point

For instructions about mounting the access point, see the [Cisco IW3702 Access Point Mounting Guide](#)

## Connecting the Protective Ground and Power

Perform the following steps in order when connecting the access point to power and ground.

1. [Grounding the Access Point, page 16](#)
2. [Wiring the Access Point DC Power, page 17](#)

## Grounding the Access Point

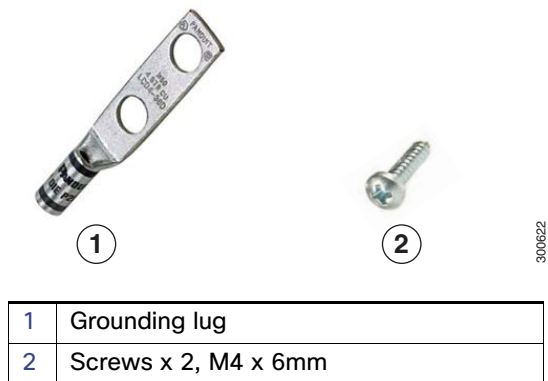
In all installations, after mounting the access point, you must properly ground the unit before connecting power cables.

**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.

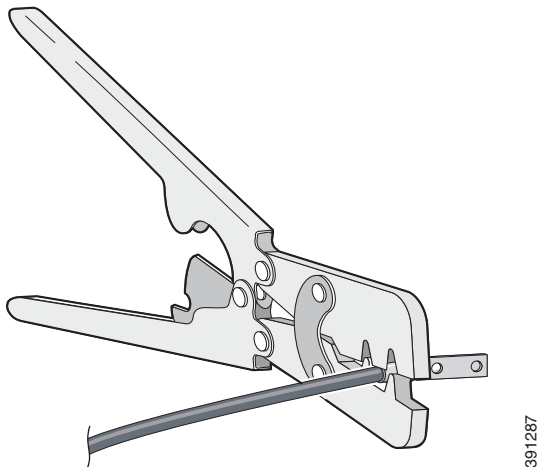
**Figure 7 Access Point Grounding Kit Contents**



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

To ground the access point:

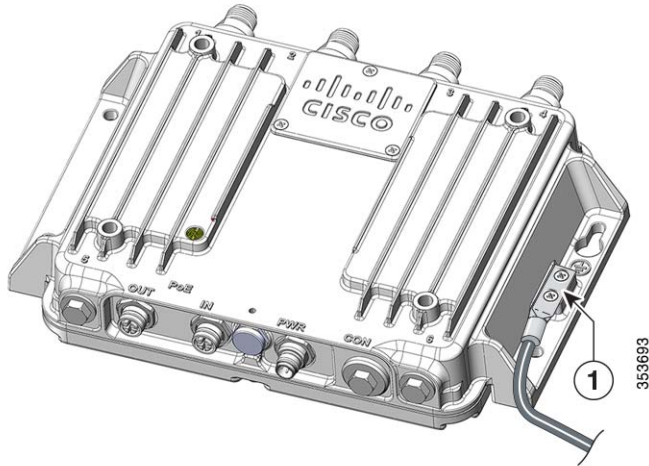
1. Use a crimping tool to crimp a 6-AWG ground wire (not included in the grounding kit) to the ground lug.



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



Installation



1	Ground connection
---	-------------------

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.

### Wiring the Access Point DC Power

To wire the access point to a DC power source:

1. Verify that the access point is grounded (see [Grounding the Access Point, page 16](#)).
2. Connect the power lead to the PWR connector by turning the cable clockwise, as shown in the following figure.



1	Power cable and PWR connector
---	-------------------------------

3. Connect the other end of the power cable to the DC power source using the power source wiring instructions.

The PWR connector pinout descriptions are in [Power Port](#), page 49.

## Connecting the Antennas

Connect each antenna based on:

- Antenna arrangement, cabling, lightning arrestor, and adapter information in [Antenna Configurations](#), page 20.
- Installation information in [Antenna Types](#), page 19.

## Connecting to Access Point Ports

This section describes connecting the access point to PoE.

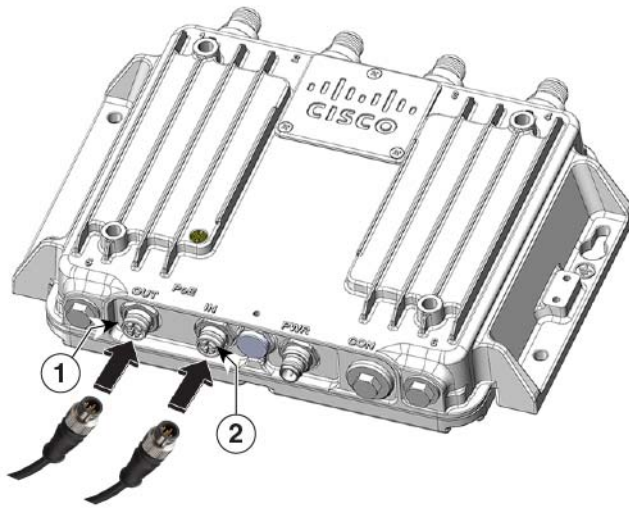
**Warning:** For connections outside the building where the equipment is installed, the following ports must be connected through an approved network termination unit with integral circuit protection.  
**10/100/1000 Ethernet Statement 1044**

### Connecting to the PoE IN or PoE OUT Port

1. Use shielded cables with a M12 X-Code plug to connect to the PoE IN or PoE OUT ports.

**Note:** Ethernet cables must have an internal shield around the signal wires. There must be a contiguous ground between the connector shell that interfaces with the IW3702 and the connector shell on the far end of the cable. Maximum cable length should not exceed 100 meters.

2. Connect the PoE IN cable to the PoE IN port, or the PoE OUT cable to the PoE OUT port by turning the cable clockwise, as shown in [Figure 8 on page 19](#).

**Figure 8** Connecting to the PoE IN or PoE OUT Ports

410333

1	PoE OUT cable
2	PoE IN cable

**Note:** When powered over the PoE IN port, PoE OUT functionality is not supported.

## Antennas

This section describes antennas and their configuration for the access point.

- [Antenna Types, page 19](#)
- [Antenna Configurations, page 20](#)

Cisco recommends using a coax seal (such as CoaxSeal) for outdoor connections, to prevent moisture and other weathering elements from affecting performance. For more information on using coax seal on the N connector to cable or antenna interface, see the instructions on your antenna documents.

## Antenna Types

The antennas used in these configurations are:

- Cisco Aironet Dual-Band Omnidirectional Antenna (White model—Cisco PID AIR-ANT2547V-N)

These are the related models:

- White model (Cisco PID AIR-ANT2547V-N=)

## Antennas

- Grey Model (Cisco PID AIR-ANT2547VG-N=)
- Cisco Aironet Dual-Band Omnidirectional Antenna (Cisco PID AIR-ANT2547VG-N)
- Cisco Aironet Four-Port Dual-Band Polarization-Diverse Array Antenna (Cisco PID AIR-ANT2513P4M-N)
- Cisco Aironet Four-Element, MIMO, Dual-Band Ceiling Mount Omnidirectional Antenna (Cisco PID AIR-ANT2524V4C-R)
- Cisco Aironet Dual-Band MIMO Wall-Mounted Omnidirectional Antenna (Cisco PID AIR-ANT2544V4M-R)
- Cisco Aironet 2.4 GHz/5 GHz MIMO 4-Element Patch Antenna (Cisco PID AIR-ANT2566P4W-R)
- Cisco Aironet Dual-band Dipole Antenna (Cisco PID AIR-ANT2524DB-R, AIR-ANT2524DG-R, and AIR-ANT2524DW-R)
- Cisco Aironet 2.4-GHz 13-dBi Directional Antenna (Cisco PID AIR-ANT2413P2M-N)
- Cisco Aironet 5-GHz 14-dBi Directional Antenna (Cisco PID AIR-ANT5114P2M-N)

## Antenna Configurations

The section describes antenna configurations.

- [Indoor or Outdoor Cisco Aironet Dual-Band Omnidirectional Antenna and Access Point, page 21](#)
- [Outdoor Cisco Aironet Dual-Band Omnidirectional Antenna and Access Point for Indoor Use Scenario, page 22](#)
- [Indoor Cisco Aironet Dual-Band Omnidirectional Antenna Directly and Cable Connected to Access Point, page 22](#)
- [Outdoor Cisco Aironet Four-Port Dual-Band Polarization-Diverse Array Antenna and Access Point, page 24](#)
- [Outdoor Cisco Aironet Four-Port Dual-Band Polarization-Diverse Array Antenna and Access Point for Indoor Use Scenario, page 25](#)
- [Indoor Cisco Aironet Four-Element MIMO Dual-Band Ceiling Mount Omnidirectional Antenna and Access Point, page 26](#)
- [Indoor or Outdoor Cisco Aironet Dual-Band MIMO Wall-Mounted Omnidirectional Antenna and Access Point, page 27](#)
- [Outdoor Cisco Aironet Dual-Band MIMO Wall-Mounted Omnidirectional Antenna and Access Point for Indoor Use Scenario, page 28](#)
- [Indoor or Outdoor Cisco Aironet Dual-Band MIMO 4-Element Patch Antenna and Access Point, page 29](#)
- [Outdoor Cisco Aironet Dual-Band MIMO 4-Element Patch Antenna and Access Point for Indoor Use Scenario, page 30](#)

## Indoor or Outdoor Cisco Aironet Dual-Band Omnidirectional Antenna and Access Point

**Table 4 Indoor or Outdoor Dual-Band Omnidirectional Antenna and Access Point**

Item	Description
Antenna Arrangement	4 x Cisco Aironet dual-band omnidirectional antennas directly connected to access point antenna connectors.
Access Point	IW3702-2E-UXX9 only.  <b>Note:</b> Do not use this configuration with the IW3702-4E-UXX9 model. All four antenna ports are on one side, and too close for optimal MIMO IEEE 802.11ac operation.
Internal Cable	–
Adapter and/or Lightning Arrestor	–
External Cable	–
Antenna	<p>4 x Cisco Aironet dual-band omnidirectional antennas are required.</p> <p>The antenna specification is:</p> <ul style="list-style-type: none"> <li>■ 2400-2484MHz, 5150-5875MHz, dual-band, WiFi, operating frequency range</li> <li>■ 4 dBi (2.4 GHz), 7 dBi (5 GHz) gain</li> <li>■ 11 in. (27.94 cm) stick antennas for indoor or outdoor use with a type N(m) connector</li> <li>■ IP67 rated, -40 to 185°F (-40° C to 85° C) operating temperature range</li> </ul> <p>Select from:</p> <ul style="list-style-type: none"> <li>■ White model, Cisco PID<sup>1</sup> AIR-ANT2547V-N</li> <li>■ Grey Model, Cisco PID AIR-ANT2547VG-N</li> </ul>

1. PID = Product identifier code.

## Antennas

## Outdoor Cisco Aironet Dual-Band Omnidirectional Antenna and Access Point for Indoor Use Scenario

**Table 5 Outdoor Dual-Band Omnidirectional Antenna and Access Point for Indoor Use Scenario**

Item	Description
Antenna Arrangement	4 x Cisco Aironet dual-band omnidirectional antennas mounted remotely outdoors, with the access point indoors or enclosed.
Access Point	IW3702-4E-UXX9 or IW3702-2E-UXX9
Adapter and/or Lightning Arrestor	You need: <ul style="list-style-type: none"> <li>4 x DC pass, N(f)-N(f) lightning arrestors. Cisco PID CGR-LA-NF-NF, Cisco PN 07-1158-02.</li> <li>4 x N(f) to N(f) RF-adapters. Cisco PID AIR-ACC370-NF-NF, Cisco PN 29-100818-01.</li> </ul>
Internal Cable	–
External Cable	Select from: <ul style="list-style-type: none"> <li>4 x RA-N(m) to N(m), LMR-400-DB, 20 ft. cables. Cisco PID CAB-L400-20-N-N, Cisco PN 37-1392-01</li> <li>4 x RA-N(m) to N(m), LMR-600-DB, 30 ft. cables. Cisco PID CAB-L600-30-N-N, Cisco PN 37-1396-01</li> </ul>
Antenna	4 x Cisco Aironet dual-band omnidirectional antennas are required. The antenna specification is: <ul style="list-style-type: none"> <li>2400-2484MHz, 5150-5875MHz, dual-band, WiFi, operating frequency range</li> <li>4 dBi (2.4 GHz), 7 dBi (5 GHz) gain</li> <li>11 in. (27.94 cm) stick antennas for indoor or outdoor use with a type N(m) connector</li> <li>IP67 rated, -40 to 185° F (-40° C to 85° C) operating temperature range</li> </ul> Select from: <ul style="list-style-type: none"> <li>White model, Cisco PID AIR-ANT2547V-N=</li> <li>Grey Model, Cisco PID AIR-ANT2547VG-N=</li> </ul> <p><b>Note:</b> To mast-mount the antenna, you must purchase a mast-mount U-bolt bracket from a third party.</p>

## Indoor Cisco Aironet Dual-Band Omnidirectional Antenna Directly and Cable Connected to Access Point

**Table 6 Indoor Dual-Band Omnidirectional Antenna Directly and Cable Connected to Access Point**

Item	Description
Antenna Arrangement	4 x indoor Cisco Aironet dual-band omnidirectional antennas connected to the IW3702-2E-UXX9 model: <ul style="list-style-type: none"> <li>2 x antennas directly mounted on top panel side.</li> <li>2 x antennas connected via internal cables on the bottom side.</li> </ul>
Access Point	IW3702-2E-UXX9 only
Adapter and/or Lightning Arrestor	You need: <ul style="list-style-type: none"> <li>2 x N(f) to N(f) RF adapters. Cisco PID AIR-ACC370-NF-NF, Cisco PN 29-100818-01.</li> </ul> <p><b>Note:</b> No lightning arrestors are required.</p>

**Table 6 Indoor Dual-Band Omnidirectional Antenna Directly and Cable Connected to Access Point (continued)**

Item	Description
Internal Cable	–
External Cable	–
Antenna	<p>4 x Cisco Aironet dual-band omnidirectional antennas are required. The antenna specification is:</p> <ul style="list-style-type: none"> <li>■ 2400-2484MHz, 5150-5875MHz, dual-band, WiFi, operating frequency range</li> <li>■ 4 dBi (2.4 GHz), 7 dBi (5 GHz) gain</li> <li>■ 11 in. (27.94 cm) stick antennas for indoor or outdoor use with a type N(m) connector</li> <li>■ IP67 rated, -40 to 185°F (-40° C to 85° C) operating temperature range</li> </ul> <p>Select from:</p> <ul style="list-style-type: none"> <li>■ White model, Cisco PID AIR-ANT2547V-N</li> <li>■ Grey Model, Cisco PID AIR-ANT2547VG-N</li> </ul>

## Outdoor Cisco Aironet Four-Port Dual-Band Polarization-Diverse Array Antenna and Access Point

**Table 7 Outdoor Four-Port Dual-Band Polarization-Diverse Array Antenna and Access Point**

Item	Description
Antenna Arrangement	4 x Cisco Aironet four-port dual-band polarization-diverse array antennas located outdoors, connected by external cable to the access point antenna connectors.
Access Point	IW3702-4E-U XK9 or IW3702-2E-U XK9
Adapter and/or Lightning Arrestor	4 x DC pass, N(m)-N(f) lightning arrestors. Cisco PID CGR-LA-NM-NF, Cisco PN 07-1091-02.
Internal Cable	–
External Cable	Select from: <ul style="list-style-type: none"> <li>■ 4 x N(m)-R/A to N(m)-STR, RF-cable, 37-1436-01, CAB-L400-5-N-N</li> <li>■ 4 x RA-N(m) to N(m), LMR-400-DB, 20', 37-1392-01, CAB-L400-20-N-N</li> <li>■ 4 x RA-N(m)-N(m), LMR-600-DB, 30', 37-1396-01, CAB-L600-30-N-N</li> </ul>
Antenna	4 x Cisco Aironet four-port dual-band polarization-diverse array antennas are required. The antenna specification is: <ul style="list-style-type: none"> <li>■ 2.4–2.5 GHz, 5.15–5.925 GHz dual-band WiFi operating frequency ranges</li> <li>■ 13 dBi peak gain</li> <li>■ Type N(f) connector</li> <li>■ IP67 rated, -40 to 185° F (-40° C to 85° C) operating temperature range</li> <li>■ Cisco PID AIR-ANT2513P4M-N</li> </ul>



## Outdoor Cisco Aironet Four-Port Dual-Band Polarization-Diverse Array Antenna and Access Point for Indoor Use Scenario

**Table 8 Outdoor Four-Port Dual-Band Polarization-Diverse Array Antenna and Access Point for Indoor Use Scenario**

Item	Description
Antenna Arrangement	4 x Cisco Aironet four-port dual-band polarization-diverse array antennas mounted remotely outdoors, with access point indoors or enclosed.
Access Point	IW3702-4E-UXX9 or IW3702-2E-UXX9
Adapter and/or Lightning Arrestor	4 x DC pass, N(f)-N(f) lightning arrestors. Cisco PID CGR-LA-NF-NF, Cisco PN 07-1158-02.
Internal Cable	–
External Cable	Select from: <ul style="list-style-type: none"> <li>■ 4 x RA-N(m) to N(m), LMR-400-DB, 20 ft. cable, Cisco PID CAB-L400-20-N-N, Cisco PN 37-1392-01</li> <li>■ 4 x RA-N(m)-N(m), LMR-600-DB, 30 ft. cable, Cisco PID CAB-L600-30-N-N, Cisco PN 37-1396-01</li> </ul>
Antenna	4 x Cisco Aironet four-port dual-band polarization-diverse array antennas are required. The antenna specification is: <ul style="list-style-type: none"> <li>■ 2.4–2.5 GHz, 5.15–5.925 GHz dual-band WiFi operating frequency ranges</li> <li>■ 13 dBi peak gain</li> <li>■ Type N(f) connector</li> <li>■ IP67 rated, –40 to 185°F (–40° C to 85° C) operating temperature range</li> <li>■ Cisco PID AIR-ANT2513P4M-N</li> </ul>

## Indoor Cisco Aironet Four-Element MIMO Dual-Band Ceiling Mount Omnidirectional Antenna and Access Point

**Table 9 Indoor Four-Element MIMO Dual-Band Ceiling Mount Omnidirectional Antenna and Access Point**

Item	Description
Antenna Arrangement	4 x Cisco Aironet indoor four-element MIMO dual-band ceiling mount omnidirectional antennas directly connected to the access point. Antennas are indoor only.
Access Point	IW3702-4E-UXX9 or IW3702-2E-UXX9
Adapter and/or Lightning Arrestor	<p>You need:</p> <ul style="list-style-type: none"> <li>■ 4 x N(m) to RP-TNC (jack), RF coax adapters. Cisco PID AIR-ACC370-NM-RF, Cisco PN 29-100817-01.</li> </ul> <p><b>Note:</b> No lightning arrestors are required.</p>
Internal Cable	–
External Cable	–
Antenna	<p>4 x Cisco Aironet indoor four-element, MIMO, dual-band ceiling mount omnidirectional antennas are required. The antenna specification is:</p> <ul style="list-style-type: none"> <li>■ 2400–2500 MHz, 5150–5850 MHz dual-band WiFi operating frequency range</li> <li>■ MIMO operation</li> <li>■ 2 dBi (2.4 GHz), 4 dBi (5.8 GHz) gain</li> <li>■ RP-TNC (plug) connector</li> <li>■ Indoor operation, 32 to 133°F (0 to 56°C) operating temperature range</li> <li>■ Cisco PID AIR-ANT2524V4C-R=</li> </ul>

## Indoor or Outdoor Cisco Aironet Dual-Band MIMO Wall-Mounted Omnidirectional Antenna and Access Point

**Table 10 Indoor or Outdoor Dual-Band MIMO Wall-Mounted Omnidirectional Antenna and Access Point**

Item	Description
Antenna Arrangement	4 x Cisco Aironet dual-band MIMO wall-mounted omnidirectional antennas directly connected to the access point antenna connectors.
Access Point	IW3702-4E-UXX9 or IW3702-2E-UXX9
Adapter and/or Lightning Arrestor	<p>You need:</p> <ul style="list-style-type: none"> <li>■ 4 x N(m) to RP-TNC (jack), RF coax adapters. Cisco PID AIR-ACC370-NM-RF, Cisco PN 29-100817-01</li> </ul> <p><b>Note:</b> No lightning arrestors are required.</p>
Internal Cable	–
External Cable	–
Antenna	<p>4 x Cisco Aironet dual-band MIMO wall-mounted omnidirectional antennas are required. The antenna specification is:</p> <ul style="list-style-type: none"> <li>■ 2400-2484 MHz, 5150-5850MHz dual-ban WiFi operating frequency range <ul style="list-style-type: none"> <li>– Bands 5150-5350MHz are not supported for outdoor installations within Regulatory Domain E</li> </ul> </li> <li>■ MIMO, omnidirectional operation</li> <li>■ 4 dBi (2.4 GHz), 4 dBi (5.8 GHz) gain</li> <li>■ Indoor or outdoor operation, -40 to 158° F (-40 to +70° C) operating temperature range</li> <li>■ RP-TNC (plug) connector</li> <li>■ Cisco PID AIR-ANT2544V4M-R</li> </ul>

## Outdoor Cisco Aironet Dual-Band MIMO Wall-Mounted Omnidirectional Antenna and Access Point for Indoor Use Scenario

**Table 11 Outdoor Dual-Band MIMO Wall-Mounted Omnidirectional Antenna and Access Point for Indoor Use Scenario**

Item	Description
Antenna Arrangement	4 x Cisco Aironet dual-band MIMO wall-mounted omnidirectional antennas mounted remotely outdoors.
Access Point	IW3702-4E-U XK9 or IW3702-2E-U XK9
Adapter and/or Lightning Arrestor	4 x DC pass, N(f)-N(f) lightning arrestors, Cisco PID CGR-LA-NF-NF, Cisco PN 07-1158-02.
Internal Cable	–
External Cable	Select from: <ul style="list-style-type: none"> <li>■ 4 x RA-N(m) to RP-TNC (jack), LMR-240-DB, 10 ft. cables. Cisco PID CAB-L240-10-N-R, Cisco PN 37-100814-01</li> <li>■ 4 x RA-N(m) to RP-TNC (jack), LMR-400-DB, 20 ft. cables. Cisco PID CAB-L400-20-N-R, Cisco PN 37-100815-01</li> </ul>
Antenna	4 x Cisco Aironet dual-band MIMO wall-mounted omnidirectional antennas are required. The antenna specification is: <ul style="list-style-type: none"> <li>■ 2400-2484 MHz, 5150-5850MHz dual-ban WiFi operating frequency range</li> <li>■ MIMO, omnidirectional operation</li> <li>■ 4 dBi (2.4 GHz), 4 dBi (5.8 GHz) gain</li> <li>■ Indoor or outdoor operation, -40 to 158° F (-40 to +70° C) operating temperature range</li> <li>■ RP-TNC (plug) connector</li> <li>■ Cisco PID AIR-ANT2544V4M-R</li> </ul>

## Indoor or Outdoor Cisco Aironet Dual-Band MIMO 4-Element Patch Antenna and Access Point

**Table 12 Indoor or Outdoor Dual-Band MIMO 4-Element Patch Antenna and Access Point**

Item	Description
Antenna Arrangement	4 x Cisco Aironet dual-band WiFi MIMO 4-element patch antennas directly connected to the access point.
Access Point	IW3702-4E-UXX9 or IW3702-2E-UXX9
Adapter and/or Lightning Arrestor	<p>You need:</p> <ul style="list-style-type: none"> <li>■ 4 x N(m) to RP-TNC (jack), RF coax adapters. Cisco PID AIR-ACC370-NM-RF. Cisco PN 29-100817-01.</li> </ul> <p><b>Note:</b> No lightning arrestors are required.</p>
Internal Cable	–
External Cable	–
Antenna	<p>4 x Cisco Aironet dual-band WiFi MIMO 4-element patch antennas are required. The antenna specifications is:</p> <ul style="list-style-type: none"> <li>■ 2400-2484 MHz, 5150-5850 MHz operating frequency range</li> <li>■ WiFi, MIMO operation</li> <li>■ 6dBi (2.4 GHz), 6 dBi (5.8 GHz) gain</li> <li>■ IP54 rated, indoor or outdoor operation, -40 to 158°F (-40 to +70°C) operating temperature range</li> <li>■ RP-TNC (plug) connector</li> <li>■ Cisco PID AIR-ANT2566P4W-R</li> </ul>

## Outdoor Cisco Aironet Dual-Band MIMO 4-Element Patch Antenna and Access Point for Indoor Use Scenario

**Table 13 Outdoor Dual-Band MIMO 4-Element Patch Antenna and Access Point for Indoor Use Scenario**

Item	Description
Antenna Arrangement	4 x Cisco Aironet dual-band WiFi MIMO 4-element patch antennas mounted remotely outdoors, access point is indoors.
Access Point	IW3702-4E-U XK9 or IW3702-2E-U XK9
Adapter and/or Lightning Arrestor	4 x DC pass, N(f)-N(f), lightning arrestors. Cisco PID CGR-LA-NF-NF, Cisco PN 07-1158-02.
Internal Cable	–
External Cable	Select from: <ul style="list-style-type: none"> <li>■ 4 x RA-N(m) to RP-TNC (jack), LMR-240-DB, 10 ft. cables. Cisco PID CAB-L240-10-N-R, Cisco PN 37-100814-01</li> <li>■ 4 x RA-N(m) to RP-TNC (jack), LMR-400-DB, 20 ft. cables. Cisco PID CAB-L400-20-N-R, Cisco PN 37-100815-01</li> </ul>
Antenna	4 x Cisco Aironet dual-band WiFi MIMO 4-element patch antennas are required. The antenna specifications is: <ul style="list-style-type: none"> <li>■ 2400-2484 MHz, 5150-5850 MHz operating frequency range</li> <li>■ WiFi, MIMO operation</li> <li>■ 6dBi (2.4 GHz), 6 dBi (5.8 GHz) gain</li> <li>■ IP54 rated, indoor or outdoor operation, -40 to 158° F (-40 to +70° C) operating temperature range</li> <li>■ RP-TNC (plug) connector</li> <li>■ Cisco PID AIR-ANT2566P4W-R</li> </ul>

## Configuration

This section contains the following topics:

- [Management Options, page 30](#)
- [Configuring the Access Point, page 31](#)

## Management Options

You can manage the access point using the following options:

- [Using the Command Line Interface, page 30](#)
- [Using the Web Browser Interface, page 31](#)

## Using the Command Line Interface

Use either of the following methods to access the CLI:

## Configuration

- Telnet—This protocol allows TCP/IP connections to a host. Telnet allows a user at one site to establish a TCP connection to a login server at another site, and then pass the keystrokes from one device to the other. Telnet can accept either an IP address or domain name as the remote device address.
- Secure Shell (SSH)—This protocol provides a secure, remote connection to networking devices. The SSH software package provides secure login sessions by encrypting the entire session. SSH features strong cryptographic authentication, strong encryption, and integrity protection.

For more information about using the CLI, see the “Using the Command-Line Interface” chapter of the [Cisco IOS Configuration Guide for Autonomous Aironet Access Points](#).

## Using the Web Browser Interface

The web browser interface contains management pages you can use to change the wireless device settings, upgrade firmware, and monitor and configure other wireless devices on the network.

You use the wireless device IP address of the access point to access the web browser interface. Prior to using the web browser interface for the first time, you must assign an IP address to the access point (see [Configuring the Access Point, page 31](#)).

To use the web browser interface:

1. Open your browser and enter the IP address of the access point in the address field.

The login screen appears.

2. Enter the user name *Cisco* and password *Cisco*.

The username and password are case-sensitive.

**Note:** We recommend that you change your user name and password after first-time log in.

3. Use the system management pages to define the access point configuration settings.

For more information about using the web browser interface, see the “Using the Web Browser Interface” chapter of the [Cisco IOS Configuration Guide for Autonomous Aironet Access Points](#).

## Configuring the Access Point

- [Obtaining an IP Address, page 31](#)
- [Setting Access Point Settings, page 34](#)
- [Connecting the Access Point to a Wireless LAN Controller, page 34](#)

**Note:** Refer to [Installation Guidelines, page 13](#) for details on registering your access point with the Wireless Internet Service Providers Association (WISPA) database.

## Obtaining an IP Address

Your access point requires an IP address to operate. The access point is not shipped with a default IP address. It obtains an IP address from the DHCP server in your network when you make the connection. If your network does not have a DHCP server, the access point continues to request an IP address until you assign it one. You must configure the IP address by opening the CLI from a terminal session established through the console port on the access point.

You must know the IP address assigned to the access before you can use the browser-based management GUI. If your access point obtained its IP address the network DHCP server, you or your network administrator can obtain it by querying the DHCP server using the MAC address of the access point.

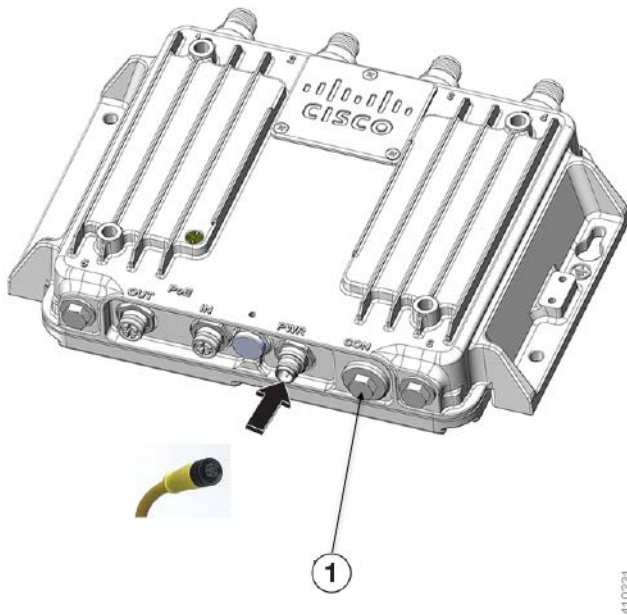
For more information, see the “Obtaining and Assigning an IP Address” section of the “Configuring the Access Point for the First Time” chapter of the [Cisco IOS Configuration Guide for Autonomous Aironet Access Points](#).

## Connecting to the Access Point Console Port

You can connect to the console port and open the CLI from a terminal session to begin configuring the device.

To connect to the access point:

1. Use a 0.5 in. (13 mm) socket wrench to remove the console (CON) port cover by turning it counterclockwise.

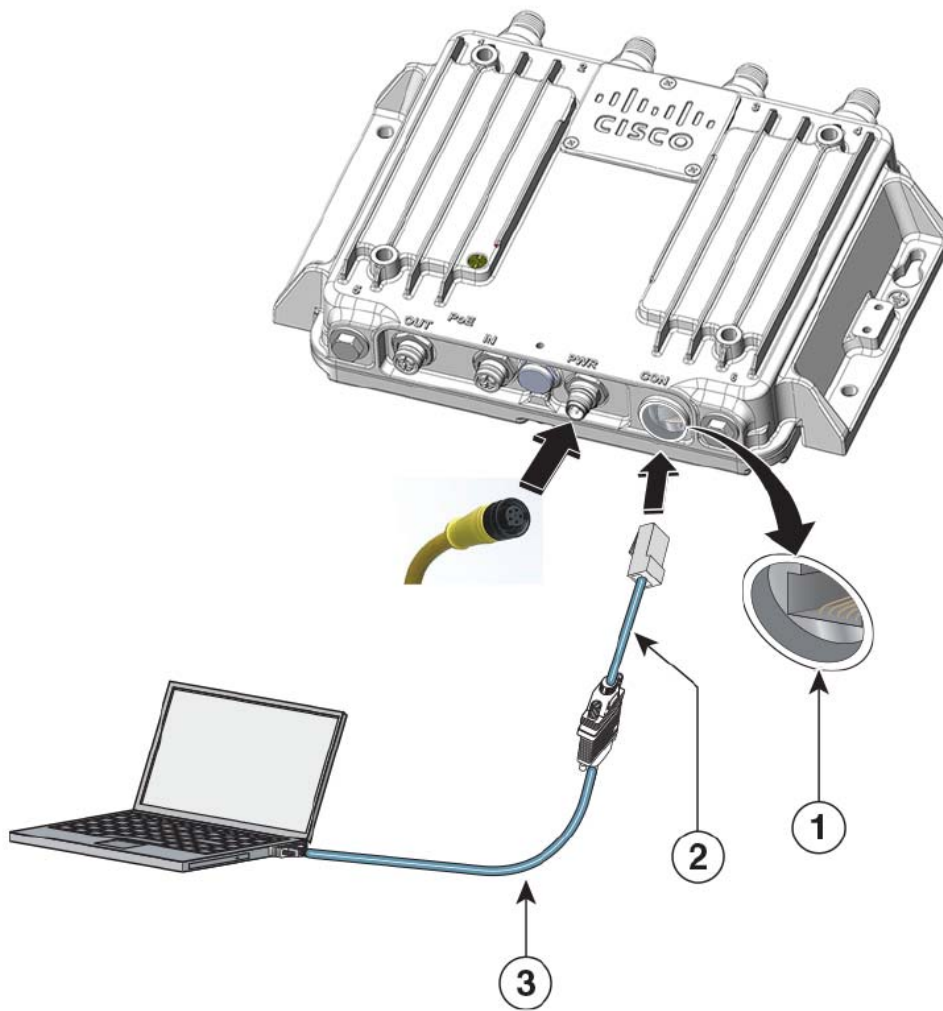


1	Console port cover
---	--------------------

2. Connect the RJ-45-to-DB-9 adapter cable to the 9-pin serial port on the PC.
3. Connect the other end of the cable to the access point console port.



Configuration



353683

1	Console port
2	RJ-45-to-DB-9 adapter cable
3	USB-to-DB-9 adapter cable

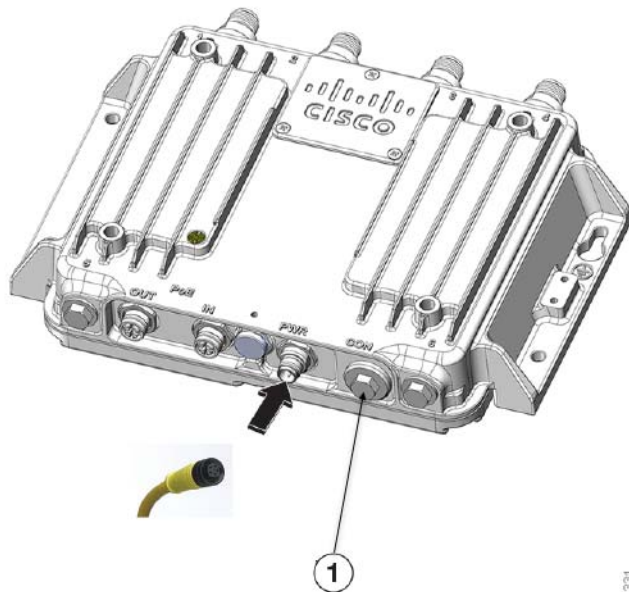
4. Set up a terminal emulator (for example, puTTY or SSH) on your PC to communicate with the access point, using the following connection settings:
  - 9600 baud
  - 8 data bits
  - No parity
  - 1 stop bit
  - No flow control
5. When connected, press enter or type *en* to access the command prompt.

## Configuration

Entering *en* prompts you for a password, and then enters privileged exec mode. The default password is *Cisco* and is case-sensitive.

When you finish configuring the access point:

6. Use a small flat-blade screwdriver to depress the tab on the RJ45 connector and disconnect the cable from the CON port.
7. Replace the CON port cover.
8. Use a 0.5 in. (13 mm) socket wrench to torque the CON port cover to 6-7 ft-lbs (8.13-9.49 N-m).



1	Console port cover
---	--------------------

## Setting Access Point Settings

Use the system management pages in the web browser interface to set the access point settings. For information on how to access the web browser interface, see [Configuring the Access Point for Autonomous Operation, page 34](#).

Use the system management pages to define configuration settings. A navigation bar appears on the left side of the page; the configuration action buttons appear at the bottom. Use the navigation bar to access the various management pages. Use the configuration action buttons to save or cancel setting changes.

## Configuring the Access Point for Autonomous Operation

For information about configuring the access point for autonomous operation, see the [Cisco IOS Configuration Guide for Autonomous Aironet Access Points](#).

## Connecting the Access Point to a Wireless LAN Controller

This section describes how to connect the access point to a wireless LAN controller. Because the configuration process occurs on the controller, see the [Cisco Wireless LAN Controller Configuration Guide](#) for additional information.

## The Controller Discovery Process

The access point uses standard Control and Provisioning of Wireless Access Points Protocol (CAPWAP) to communicate between the controller and other wireless access points on the network. CAPWAP is a standard, interoperable protocol that allows an access controller to manage a collection of wireless termination points. The discovery process using CAPWAP is identical to the Lightweight Access Point Protocol (LWAPP) used with Cisco IW3702 access points. LWAPP-enabled access points are compatible with CAPWAP, and conversion to a CAPWAP controller is seamless. Deployments can combine CAPWAP and LWAPP software on the controllers.

The functionality provided by the controller does not change, except for customers who have Layer 2 deployments, which CAPWAP does not support.

In a CAPWAP environment, the wireless access point discovers a controller by using CAPWAP discovery mechanisms and then sends it a CAPWAP join request. The controller sends the access point a CAPWAP join response to allow the access point to join the controller. When the access point joins the controller, the controller manages its configuration, firmware, control transactions, and data transactions.

For additional information about the discovery process and CAPWAP, see the [Cisco Wireless LAN Controller Software Configuration Guide](#).

- Notes:**
- Refer to the *Release Notes* for the Cisco IW3702 access points for the minimum required Cisco Wireless LAN Controller software release.
  - You cannot edit or query any access point using the controller CLI if the name of the access point contains a space.
  - Ensure 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 yet be valid.

Access points must be discovered by a controller before they can become active in the network. The access point supports these controller discovery processes:

- Layer 3 CAPWAP discovery—Can occur on different subnets than the access point and uses IP addresses and UDP packets rather than MAC addresses used by Layer 2 discovery.
- 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's non-volatile memory. This process of storing controller IP addresses on an access point for later deployment is called *priming the access point*. See [Performing a Pre-Installation Configuration, page 35](#).
- DHCP server discovery—This feature uses DHCP option 43 to provide controller IP addresses to access points. Cisco switches support a DHCP server option that is typically used for this capability. See [Configuring DHCP Option 43 and DHCP Option 60, page 38](#).
- DNS discovery—The access point can discover controllers through your domain name server (DNS). To use this discovery method, you must configure the 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 backward compatibility in an existing deployment. When an access point receives the 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.

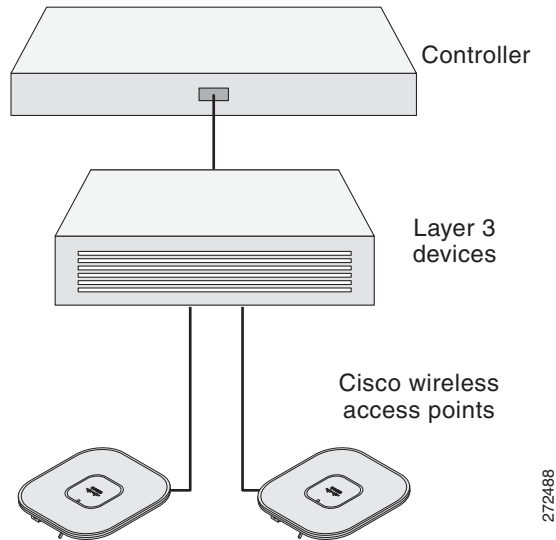
## Performing a Pre-Installation Configuration

The following procedures ensure a successful access point installation and initial operational setup. Pre-installation configuration – priming the access point – is optional.

**Note:** If your network controller already properly configured, you can skip priming and simply install your access point in its final location and connect it to the network. See [Deploying in a Wireless Network, page 39](#).

Figure 9 on page 36 shows the pre-installation configuration setup.

**Figure 9 Pre-Installation Configuration Setup**



To prime the access point:

1. Ensure that the Cisco Wireless LAN Controller Management DS Port is connected to the network.

Use the CLI, browser-based interface, or Cisco WCS procedures described in the appropriate Cisco Wireless LAN Controller guide to perform the following:

- a. Ensure that the access points have Layer 3 connectivity to the Cisco Wireless LAN Controller Management and AP-Manager Interface.
- b. Configure the switch to which your access point is to attach. See the appropriate Cisco Wireless LAN Controller guide.
- c. Set the Cisco Wireless LAN Controller as the **master** so that new access points always join with it.
- d. Ensure that DHCP is enabled on the network.

**Note:** The access point must receive its IP address through DHCP.

- e. Ensure that no CAPWAP UDP ports are blocked in the network.
- f. Use a DHCP, DNS, or IP subnet broadcast to ensure that the access point finds the IP address of the controller.

This guide describes the DHCP method to convey the controller IP address. For other methods, refer to product documentation. See also [Using DHCP Option 43, page 37](#).

2. Apply power to the access point:

The access point is IEEE 802.3at (30 W) compliant and can be powered by a third-party DC power supply that you provide. The Cisco power injector option is AIR-PWRINJ1500-2=.

## Configuration

- Notes:**
- The access point downgrades to 3x3 when connected to a 15.4W power supply. For maximum operating efficiency, use an IEEE 802.3at compliant PoE switch or AIR-PWRINJ1500-2= power injector.
  - To prevent Ethernet port bottlenecks due to wireless traffic speeds exceeding 10/100 Ethernet port transmit speeds, the Cisco IW3702 access point requires a Gigabit Ethernet link.

As the access point attempts to connect to the controller, the LEDs cycle through a green-red-amber sequence, which can take up to 5 minutes.

- Notes:**
- If this connection takes longer than five minutes, the access point cannot find the **master** Cisco Wireless LAN Controller. Check the connection, and ensure that both are on the same subnet.
  - To prevent Ethernet port bottlenecks due to wireless traffic speeds exceeding 10/100 Ethernet port transmit speeds, the Cisco IW3702 access point requires a Gigabit Ethernet link.
  - If the access point shuts down, check the power source.

After a successful connection, the access point compares operating system code versions with the Cisco Wireless LAN Controller. If versions differ, it downloads the newest version. The Status LED blinks dark blue during this process. On a successful download, the access point reboots.

### 3. (Optional) Configure the access point.

Use the controller CLI, controller GUI, or Cisco Prime Infrastructure to customize access-point-specific IEEE 802.11ac network settings.

On successful access point priming, the Status LED is green indicating normal operation.

### 4. Disconnect the access point and mount it in location.

- Notes:**
- If the access point LEDs do not indicate normal operation, turn it off and repeat the access point priming procedure (see [Performing a Pre-Installation Configuration, page 35](#)).
  - When installing a Layer 3 access point on a different subnet than the Cisco Wireless LAN Controller, ensure that:
    - a DHCP server is reachable from the subnet on which you are installing the access point and that subnet has a return route to the Cisco Wireless LAN Controller.
    - the return route to the Cisco Wireless LAN Controller has destination UDP ports 5246 and 5247 open for CAPWAP communications.
    - the return route to the primary, secondary, and tertiary Cisco Wireless LAN Controllers allows IP packet fragments.
    - if using address translation, the access point and the Cisco Wireless LAN Controller have a static 1-to-1 NAT to an outside address. (Port address translation is not supported.)

## Using 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. For additional information, refer to [Configuring DHCP Option 43 and DHCP Option 60, page 38](#).

## Configuring DHCP Option 43 and DHCP Option 60

This section contains a DHCP Option 43 configuration example on a Windows 2003 Enterprise DHCP server for use with Cisco wireless access points. For other DHCP server implementations, consult the product documentation for configuring DHCP Option 43.

With DHCP Option 43, use the IP address of the controller management interface.

- Notes:**
- 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.
  - DHCP servers must be programmed to return the option based on the DHCP Vendor Class Identifier (VCI) string of the access point (DHCP Option 60). The VCI string for the access point is:

```
Cisco AP iw370s
```

If you ordered an access point with the Service Provider Option (AIR-OPT60-DHCP) selected in the ordering tool, the VCI string for the access point contains **-ServiceProvider**. For example, an access point with this option returns this VCI string:

```
Cisco AP iw3702-ServiceProvider
```

The Cisco IW3702 access point uses the type-length-value (TLV) format for DHCP Option 43. The TLV block format is:

- Type: 0xf1 (decimal 241)
- Length: Number of controller IP addresses \* 4
- Value: List of Cisco Wireless LAN Controller management interfaces

To configure DHCP Option 43 in the embedded Cisco IOS DHCP server:

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.

### Example DHCP scope commands:

```
ip dhcp pool pool_name
network IP_network netmask
default-router default_router
dns-server DNS_Server
```

where,

- *pool\_name* is the name of the DHCP pool (for example, AP3702).
- *IP\_network* is the network IP address where the controller resides (for example, 10.0.15.1).
- *netmask* is the subnet mask (for example, 255.255.255.0).
- *default\_router* is the IP address of the default router (for example, 10.0.0.1).
- *DNS\_Server* is the IP address of the DNS server (for example, 10.0.10.2).

3. Add the option 60 line using the following syntax:

```
option 60 ascii VCI_string
```

where,

- *VCI\_string* = "Cisco AP iw3702"

## Configuration

**Note:** You must include the quotation marks.

4. Add the option 43 line using the following syntax:

```
option 43 hex <hex_string>
```

The hex string is assembled by concatenating the TLV values: *Type* + *Length* + *Value*

where,

- *Type* is always f1(hex).
- *Length* is the number of controller management IP addresses times 4 in hex.
- *Value* is the IP address of the controller listed sequentially in hex.

#### TLV Example

For two controllers with management interface IP addresses 10.126.126.2 and 10.127.127.2

- *Type* is f1(hex)
- *Length* is  $2 * 4 = 8 = 08$  (hex)

The resultant IP addresses translate to 0a7e7e02 and 0a7f7f02. Assembling the string yields f1080a7e7e020a7f7f02.

The resulting Cisco IOS command added to the DHCP scope is option 43 hex f1080a7e7e020a7f7f02.

### Deploying in a Wireless Network

To deploy the access point in a wireless network:

1. Connect and power up the access point.
2. Observe the Status LED (see [“Status LED” on page 7](#)).

On successful power-up, the discovery and join process begins. During this process, the Status LED blinks green-red-off.

On a successful join, the Status LED is green when no clients are associated, or blue when one or more clients are associated.

- Notes:**
- If the Status LED is not on, the access point may not have power.
  - If the Status LED blinks green-red-off longer than 5 minutes, it cannot find its primary, secondary, and tertiary Cisco Wireless LAN Controller. Check the connection, and ensure that both are on the same subnet or that the access point has a return route to its primary, secondary, and tertiary Cisco Wireless LAN Controller.
  - If the access point is not on the same subnet as the Cisco Wireless LAN Controller, ensure that there is a properly configured DHCP server on the same subnet. See [Configuring DHCP Option 43 and DHCP Option 60, page 38](#).

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

## Technical Specifications

This section provides the following technical specifications for the access point:

- [Environmental and Operational Specifications, page 40](#)
- [Power Specifications, page 40](#)
- [Mechanical Specifications, page 42](#)
- [Regulatory Compliance and Safety Information, page 42](#)
- [Declaration of Conformity for RF Exposure, page 42](#)
- [Declaration of Conformity Statements, page 48](#)

## Environmental and Operational Specifications

**Table 14 Environmental and Operating Specifications for the Access Point**

Description	Specification
Operating temperature	-40 to 158°F (-40 to +70°C) with solar load and still air
Altitude	15,000 ft. (4.5 m)
Humidity	5 to 95% (non-condensing)
Extended operating temperature (DC power)	-58 to 167°F (-50 to +75°C) without solar loading, still air, and cold start limited to -40°C
Operating type test	185°F (85°C) for 16 hours
Storage temperature	-40 to 185°F (-40 to +85°C)
Vibration	Per IEEE 1613, IEC 61850, EN50155, and AREMA
Shock	Per IEEE 1613, IEC 61850, EN50155, and AREMA
Seismic	Per IEC 61850-3 Class 2

## Power Specifications

- [Power Requirements, page 41](#)
- [DC Input and PoE IN Specifications, page 41](#)



## Power Requirements

**Table 15 Power Requirements for the Access Point**

Description	Specification
DC input voltage	<ul style="list-style-type: none"> <li>■ 12V to 48V DC (-20%, +25%)</li> <li>■ Nominal: 12, 24, or 48 VDC<sup>1</sup></li> </ul>
Maximum input current rating	<ul style="list-style-type: none"> <li>■ 2 A @ 48 VDC</li> <li>■ 4 A @ 24 VDC</li> <li>■ 8 A @ 12 VDC</li> </ul>

1. Voltage rating is measured at the input pins of the load (IW3702) and not at the power source.

### DC Input and PoE IN Specifications

The access point supports two power options:

- DC input from the PWR connector.
- PoE inline power from the PoE IN port.

**Notes:** ■ The PoE OUT port is enabled only when the access point is powered over the PWR port. When powered over the PoE IN port, PoE OUT functionality is not supported.

In relation to powering the access point:

- Power can be supplied by the DC input (PWR port connection) or the PoE inline power (PoE IN port), but not both.
- We recommend not using the two power options at the same time, but no harm results if both are present.
- If both power inputs are present, the DC input (PWR port connection) takes precedence and PoE IN becomes idle and unused.
- Power supply redundancy is not supported.

Table 16 on page 42 lists specifications for the available power inputs.

**Table 16 Power Connections Specifications**

Power INPUT	WiFi 4 x 4 MIMO	GE-POE-OUT (POE PSE)	GE-POE-OUT (10/100/1000)	Operating Temperature Range	Wire Thickness, Min Rating	Length (Max)
DC Input at +12V	Yes	Yes, 802.3af	Yes	-58 to 167° F (-50 to 75° C) <sup>2</sup>	16 AWG, 8 A	20'/6.1m <sup>1</sup>
DC Input at +24V	Yes	Yes, 802.3af	Yes	-58 to 167° F (-50 to 75° C) <sup>2</sup>	20 AWG, 4 A	30'/9.1m <sup>1</sup>
DC Input at +48V	Yes	Yes, 802.3af	Yes	-58 to 167° F (-50 to 75° C) <sup>2</sup>	20 AWG, 2 A	60'/18.3m <sup>1</sup>
POE-IN, 802.3at (POE+, 25W)	Yes	No	Yes	-40 to 167° F (-40 to 75° C)	CAT5e(24AWG , 0.6 A, shielded	100m
POE-IN, 802.3af (POE, 13W)	No (3x3 only)	No	No	-4 to 167° F (-20 to 75° C)	CAT5e(24AWG , 0.6 A, shielded	100m

- When you use a thicker cable, the maximum length can be increased. When the unit is installed in the environment where the temperature is always higher than -20°C, the maximum length can be double of the value in the table for DC inputs. Furthermore, if the GE-POE-OUT port is not used as POE-PSE (power source), the maximum length can be increased by 10 feet.
- Refer to [Table 14 on page 40](#) for the restrictions on the temperature limits.

## Mechanical Specifications

**Table 17 Mechanical Specifications for the Access Point**

Description	Specification
Enclosure type	IP67 Type 4X
Dimensions (h x w x d)	<ul style="list-style-type: none"> <li>■ IW3702-2E-U XK9: 2.34 x 11.30 x 8.00 in. (5.94 x 28.7 x 20.32 cm)</li> <li>■ IW3702-4E-U XK9: 2.34 x 11.30 x 8.00 in. (5.94 x 28.7 x 20.32 cm)</li> </ul>
Weight	6.7 lbs. (3.0 kg)

## Regulatory Compliance and Safety Information

For information about the international regulatory compliance and safety information for the Cisco IW3702 access point, see the *Regulatory Compliance and Safety Information for Cisco IW3702 Access Point* on Cisco.com.

## Declaration of Conformity for RF Exposure

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

- [Generic Discussion on RF Exposure, page 43](#)
- [Declaration of Conformity for RF Exposure \(ANSI\), page 43](#)
- [This Device Meets International Guidelines for Exposure to Radio Waves \(ICNIRP\), page 43](#)
- [This Device Meets FCC Guidelines for Exposure to Radio Waves, page 44](#)

## Technical Specifications

- [This Device Meets the Industry Canada Guidelines for Exposure to Radio Waves, page 44](#)
- [Additional Information on RF Exposure, page 44](#)
- [Guidelines for Operating Cisco IW3702 Access Points in Japan, page 45](#)
- [Administrative Rules for Cisco IW3702 Access Points in Taiwan, page 46](#)
- [Operation of Cisco IW3702 Access Points in Brazil, page 48](#)

## 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.

## Declaration of Conformity for RF Exposure (ANSI)

- [United States, page 43](#)
- [Canada, page 43](#)

### United States

This system has been evaluated for RF exposure for humans in reference to ANSI C 95.1 (American National Standards Institute) limits. The evaluation was based on ANSI C 95.1 and FCC OET Bulletin 65C rev 01.01. The minimum separation distance from the antenna to general bystanders is 9 inches (23 cm) to maintain compliance.

### Canada

This system has been evaluated for RF exposure for humans in reference to ANSI C 95.1 (American National Standards Institute) limits. The evaluation was based on RSS-102 Rev 2. The minimum separation distance from the antenna to general bystanders is 9 inches (23cm) to maintain compliance.

## This Device Meets International Guidelines for Exposure to Radio Waves (ICNIRP)

The Cisco IW3702 access point 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 to avoid contact with the antennas by the end user.

It is recommended to place the system in a location where the antennas can remain the minimum distance from the user specified in the regulatory guidelines, which are designed to reduce the overall exposure of the user or operator.

## Technical Specifications

Separation Distance		
MPE	Distance	Limit
0.63 mW/cm <sup>2</sup>	7.87 in. (20 cm)	1.00 mW/cm <sup>2</sup>

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, you can easily orient antennas away from users or place the antennas at a greater separation distance than recommended.

### This Device Meets FCC Guidelines for Exposure to Radio Waves

The Cisco IW3702 access point 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 to avoid contact with the antennas by the end user. We recommend that you place the system in a location where antennas remain a minimum distance 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		
MPE	Distance	Limit
0.63 mW/cm <sup>2</sup>	20 cm (7.87 inches)	1.00 mW/cm <sup>2</sup>

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, you can easily orient antennas away from the user or place the antennas at a greater separation distance than recommended, or lower the transmitter power output.

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

The Cisco IW3702 access point 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 to avoid contact with the antennas by the end user. We recommend that you place the system in a location where antennas remain a minimum distance from the user in accordance to the regulatory guidelines, which are designed to reduce the overall exposure of the user or operator.

Separation Distance		
MPE	Distance	Limit
0.63 mW/cm <sup>2</sup>	20 cm (7.87 inches)	1.00 mW/cm <sup>2</sup>

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 orient antennas away from the user or place the antennas at a greater separation distance than recommended, or lower the transmitter power output.

### Additional Information on RF Exposure

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

## Technical Specifications

- 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](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
- FCC Bulletin 65C (01-01): Evaluating Compliance with the FCC guidelines for Human Exposure to Radio Frequency Electromagnetic Fields: Additional Information for Evaluating Compliance for Mobile and Portable Devices with FCC limits for Human Exposure to Radio Frequency Emission

You can obtain additional information from the following organizations:

- World Health Organization Internal Commission on Non-Ionizing Radiation Protection at this URL: [www.who.int/emf](http://www.who.int/emf)
- United Kingdom, National Radiological Protection Board at this URL: [www.nrpb.org.uk](http://www.nrpb.org.uk)
- Cellular Telecommunications Association at this URL: [www.wow-com.com](http://www.wow-com.com)
- The Mobile Manufacturers Forum at this URL: [www.mmfa.org](http://www.mmfa.org)

## Guidelines for Operating Cisco IW3702 Access Points in Japan

This section provides guidelines for avoiding interference when operating Cisco IW3702 access points in Japan. These guidelines are provided in both Japanese and English:

- [Japanese, page 45](#)
- [English, page 46](#)

### Japanese

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

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, ensure that no premises radio stations or specified low-power radio stations of RF-ID are 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; call 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, call the number below.  
Contact Number: 03-6434-6500

## Administrative Rules for Cisco IW3702 Access Points in Taiwan

This section provides administrative rules for operating Cisco IW3702 access points in Taiwan. The rules for all access points are provided in both Chinese and English:

- [Chinese Translation—Part 1, page 46](#)
- [English Translation—Part 1, page 47](#)
- [Chinese Translation—Part 2, page 47](#)
- [English Translation—Part 2, page 47](#)

## Chinese Translation—Part 1

## 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，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。

第十四條 低功率射頻電機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。

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

127048

## English Translation—Part 1

## Administrative Rules for Low-power Radio-Frequency Devices

Article 12: For those low-power radio-frequency devices that have already received a type-approval, companies, business units or users should not change its frequencies, increase its power or change its original features and functions.

Article 14: The operation of the low-power radio-frequency devices is subject to the conditions that no harmful interference is caused to aviation safety and authorized radio station; and if interference is caused, the user must stop operating the device immediately and can't re-operate it until the harmful interference is clear.

The authorized radio station means a radio-communication service operating in accordance with the Communication Act.

The operation of the low-power radio-frequency devices is subject to the interference caused by the operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator.

## Chinese Translation—Part 2

低功率射頻電機技術規範

## 4.7 無線資訊傳輸設備

4.7.5 在 5.25-5.35 兆赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

4.7.6 無線資訊傳輸設備須忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。

4.7.7 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中。

202591

## English Translation—Part 2

## Low-power Radio-frequency Devices Technical Specifications:

4.7	Unlicensed National Information Infrastructure
4.7.5	Within the 5.25-5.35 GHz band, U-NII devices will be restricted to indoor operations to reduce any potential for harmful interference to co-channel MSS operations.
4.7.6	The U-NII devices shall accept any interference from legal communications and shall not interfere the legal communications. If interference is caused, the user must stop operating the device immediately and can't re-operate it until the harmful interference is clear.
4.7.7	Manufacturers of U-NII devices are responsible for ensuring frequency stability such that an emission is maintained within the band of operation under all conditions of normal operation as specified in the user manual.

## Operation of Cisco IW3702 Access Points in Brazil

This section contains information for operating Cisco IW3702 access points in Brazil:

- [Regulatory Information, page 48](#)
- [Declaration of Conformity Statements, page 48](#)
- [Portuguese Translation, page 48](#)
- [English Translation, page 48](#)

## Regulatory Information

### Portuguese Translation

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

### English Translation

This equipment operates on a secondary basis and consequently must accept harmful interference, including interference from stations of the same kind. This equipment may not cause harmful interference to systems operating on a primary basis.

## Declaration of Conformity Statements

All the Declaration of Conformity statements related to this product can be found at the following location:  
<http://www.ciscofax.com>

## Ports and Connectors

The port pinouts and connector details are described in this section:

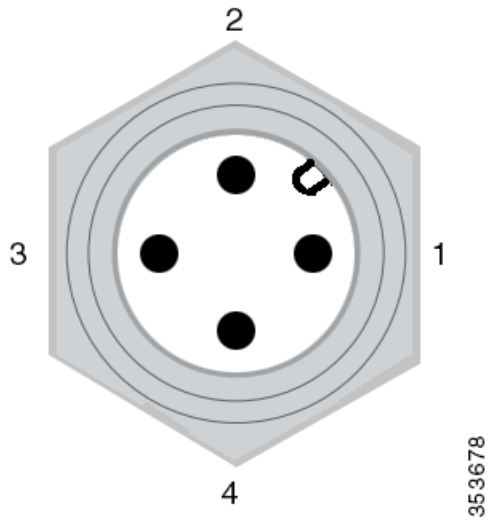
- [Power Port, page 49](#)
- [PoE OUT Port, page 50](#)
- [PoE IN Port, page 51](#)
- [Console Port, page 51](#)



## Power Port

The power port is a 4-pin M12 A-code male connector.

**Figure 10 Power Port Connector Pinouts**

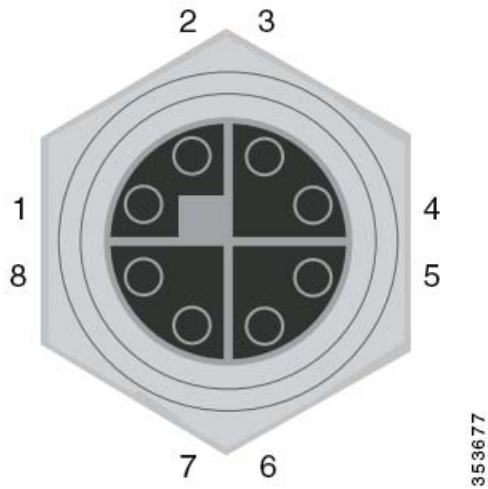


1	Positive DC power connection	3	Negative DC power connection
2	Positive DC power connection	4	Negative DC power connection

## PoE OUT Port

The PoE OUT port is an 8-pin M12 X-code female connector.

**Figure 11 PoE OUT Port Pinouts**

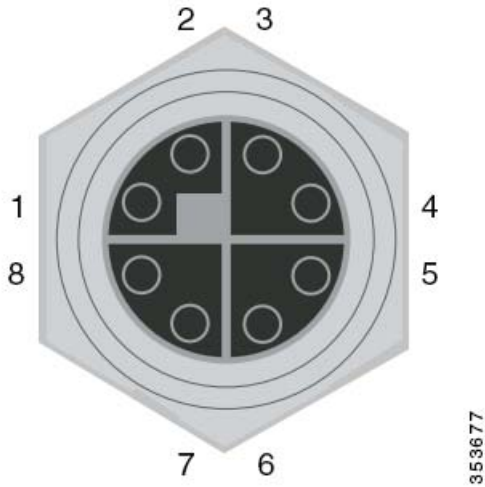


1	0_P signal	5	3_P
2	0_N signal	6	3_N
3	1_P signal	7	2_N
4	1_N signal	8	2_P

## PoE IN Port

The PoE IN port is a 8-pin M12 X-code female connector.

**Figure 12 PoE IN Port Pinouts**



1	0_P signal	5	3_P
2	0_N signal	6	3_N
3	1_P signal	7	2_N
4	1_N signal	8	2_P

## Console Port

The console port is an RJ-45 connector.

**Table 18 Console Port Pinouts**

Pin	Signal
1	RTS output
2	DTR input
3	TxD output
4	GND
5	GND
6	RxD input
7	DSR output
8	CTS input

## Related Documentation

The following are other documents in the IW3700 Industrial Wireless Access Point Series:

- [Cisco IW3702 Access Point Mounting Guide](#)
- [Cisco Wireless LAN Controller Software Release Notes](#)

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). The RSS feeds are a free service.

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 NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

No combinations are authorized or intended under this document.

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.

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: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). 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. (1110R)

© 2015-2016 Cisco Systems, Inc. All rights reserved.

Related Documentation