

Wireless Mount

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces the features, structure, and installation of the Wireless Mount (hereinafter referred to as "the Device").

Models

PFA15A

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 TIPS	Indicates dangerous high voltage. Take care to avoid coming into contact with electricity.
 NOTE	Indicates a laser radiation hazard. Take care to avoid exposure to a laser beam.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	November 2019

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product

updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.

- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

The manual helps you to use the product properly. To avoid danger and property damage, read the manual carefully before using the product, and keep it well for future reference.

Operating Requirements

- Do not expose the device directly to the sunlight, and keep it away from heat.
- Do not install the device in the damp environment, and avoid dust and soot.
- Make sure that the device is in horizontal installation, and install the device on solid and flat surface to avoid falling down.
- Avoid liquid spattering on the device. Do not place object full of liquid on the device to avoid liquid flowing into the device.
- Install the device in the well-ventilated environment. Do not block the air vent of the device.
- Use the device at rated input and output voltage.
- Do not disassemble the device without professional instruction.
- Transport, use, and store the device in allowed ranges of humidity and temperature.

Power Supply Requirements

- Use the battery properly to avoid fire, explosion, and other dangers.
- Replace the battery with battery of the same type.
- Use locally recommended power cord in the limit of rated specifications.
- Use the standard power adapter. We will assume no responsibility for any problems caused by nonstandard power adapter.
- The power supply shall meet the SELV requirement. Use the power supply that conforms to Limited Power Source, according to IEC60950-1. Refer to the device label.
- Adopt GND protection for I-type device.
- The coupler is the disconnecting apparatus. Keep it at the angle for easy operation.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Introduction	1
1.1 Overview	1
1.2 Functions.....	1
1.3 Unpack and Check.....	1
1.4 Dimensions	2
2 Installation	3
Appendix 1 Technical Specifications	8
Appendix 2 Cybersecurity Recommendations	9

1 Introduction

1.1 Overview

Wireless mount supports the installation of wireless devices whose weights are no more than 3 kg.

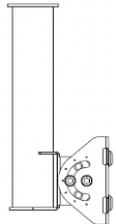
1.2 Features

- Material: Whole aluminum alloy material to ensure product strength.
- Load bearing: Applicable to the installation of wireless devices whose weights are no more than 3 kg. It is firm and reliable.
- Big clamp range: With a wide range of adaptability, supports pole diameters from 80 mm to 150 mm to fit most of the poles.
- Small clamp range: With a wide range of adaptability, supports pole diameters from 40 mm to 60 mm to meet the fixing requirements of wireless devices.

1.3 Out-of-Box Checking

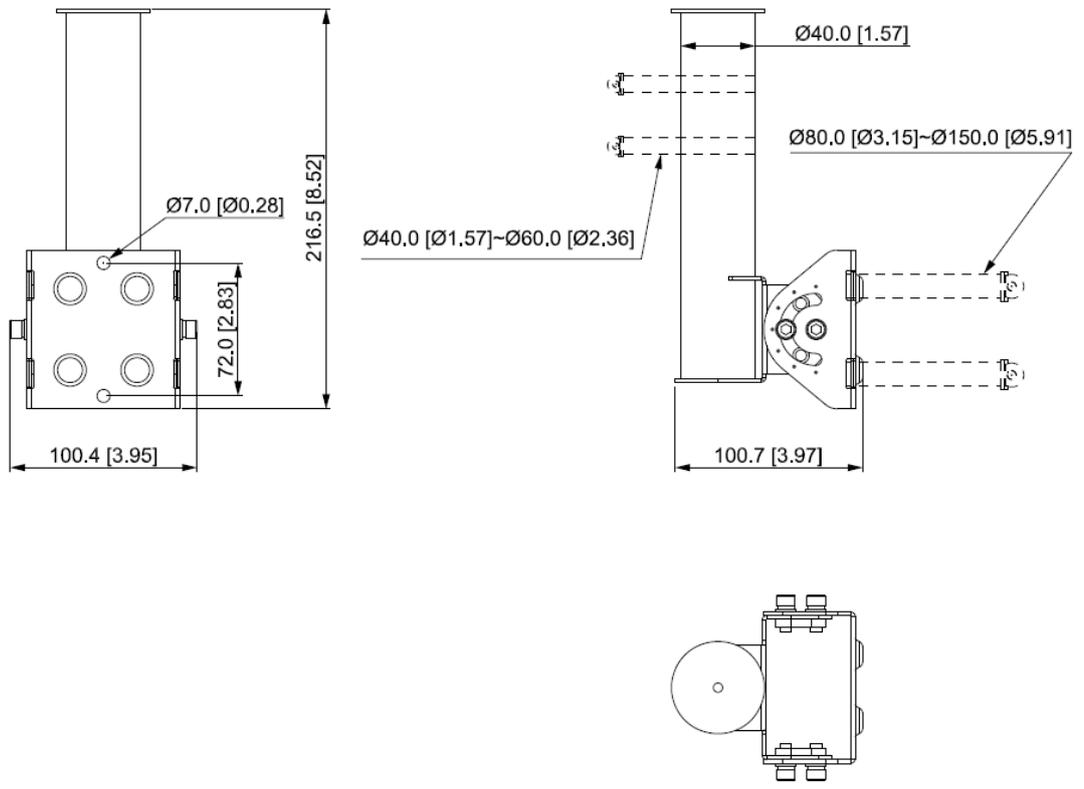
After unpacking the box, check if there is obvious damage to the appearance of the Device, and make sure that the components are complete against the packing list. See Table 1-1 for details.

Table 1-1 Product list

Illustration	Accessory	Quantity
	Mounting bracket	1
	M6 x 14 mm screw	4
	Small clamp	2
	Big clamp	2
	S6.0 wrench	1

1.4 Dimensions

Figure 1-1 Dimensions (Unit: mm [inch])



2 Installation



- During installation, avoid objects like the equipment, components or tools falling off; otherwise people, animals, other objects or the equipment might be damaged.
- Make sure that the pole can sustain 8 times the weight of the device and the bracket.

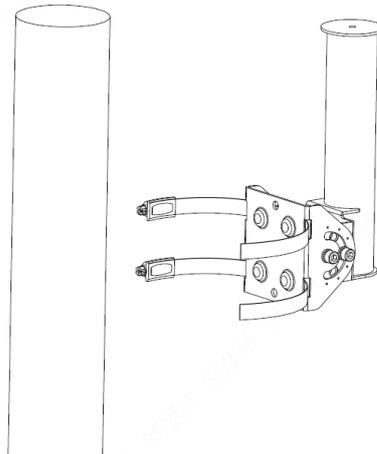
Step 1 Install the mounting bracket on the pole with the big clamp. See Figure 2-1.

- 1) The two big clamps need to pass through the holes on the front side of the mounting bracket. And make sure that the mounting bracket faces upwards.
- 2) Put the big clamp around the pole.



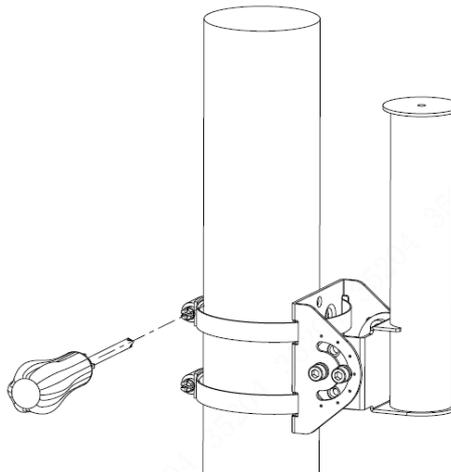
The big clamp must cling to the pole.

Figure 2-1 Installation (1)



Step 2 Lock the big clamp with a screwdriver to fix the bracket on the pole. See Figure 2-2.

Figure 2-2 Installation (2)

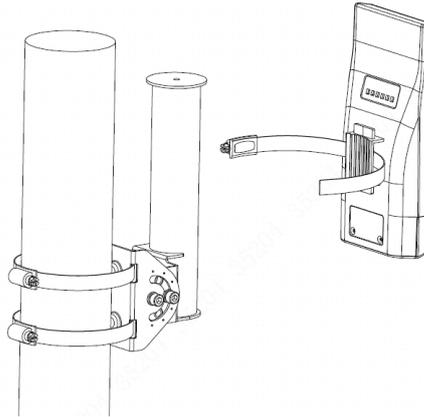


Step 3 The small clamp goes through a small hole of the wireless device. See Figure 2-3.



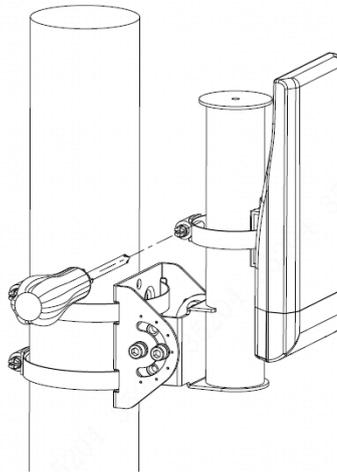
Take installation of PFM881-L as an example.

Figure 2-3 Installation (3)



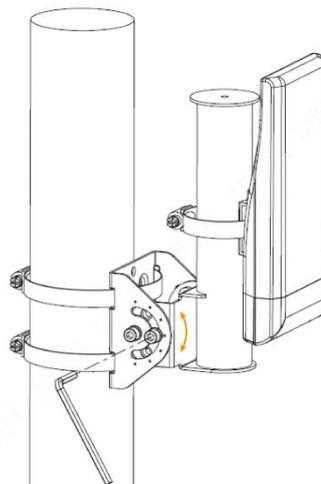
Step 4 Wrap the small clamp around the bracket pole and fix it with a screwdriver. See Figure 2-4.

Figure 2-4 Installation (4)



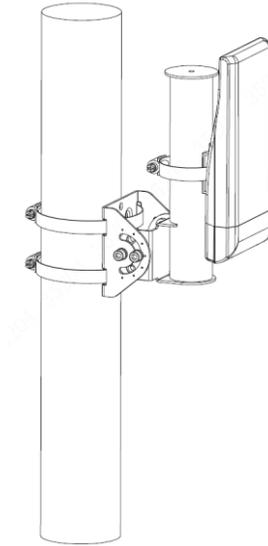
Step 5 Loosen the M6 screw with the S6.0 wrench, and adjust the pitch angle of the wireless device (up to 90°). Fasten M6 screw after adjustment. See Figure 2-5.

Figure 2-5 Installation (5)



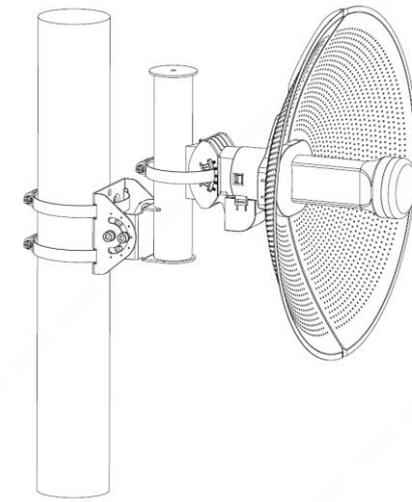
- For the completed installation of PFM881-L, see Figure 2-6.

Figure 2-6 Installation of PFM881-L



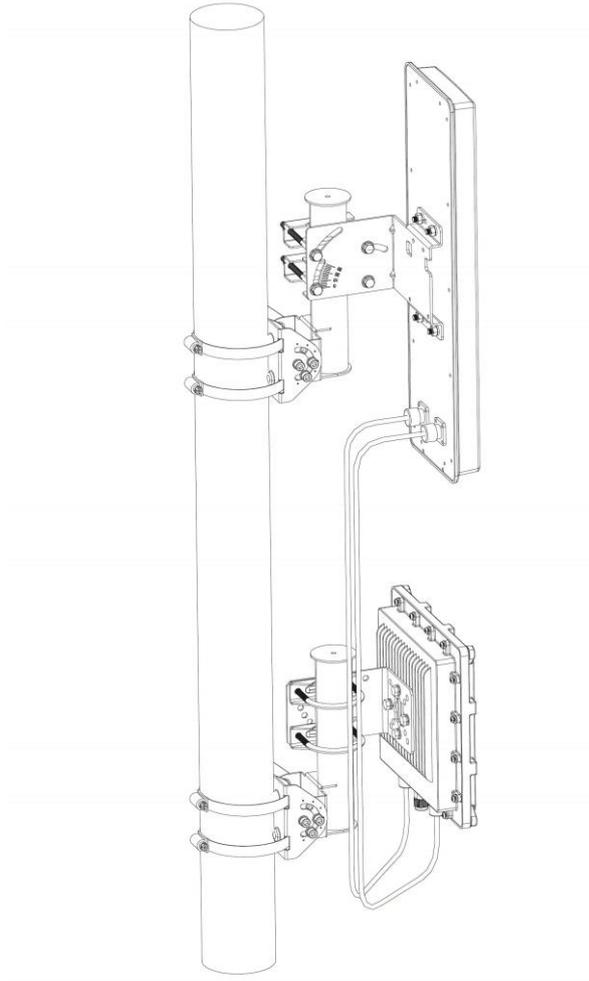
- For the completed installation of PFM886-15, see Figure 2-7.

Figure 2-7 Installation of PFM886-15



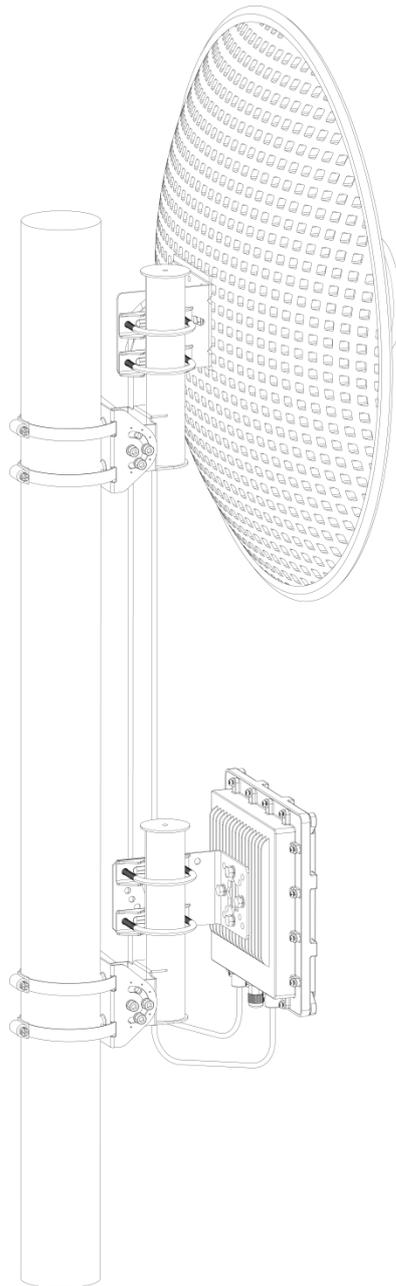
- For the completed installation of PFM880E, see Figure 2-8.

Figure 2-8 Installation of PFM880E



- For the completed installation of PFM886-20, see Figure 2-9.

Figure 2-9 Installation of PFM886-20



For installation of the specific wireless devices, refer to the corresponding user's manual.

Appendix 1 Technical Specification

Appendix table 1-1 Specification

Item	Description
Model	PFA15A
Dimensions (L x W x H)	218.0 mm x 100.0 mm x 64.0 mm (8.58" x 3.94" x 2.52")
Material	Aluminum alloy
Bearing weight	<= 3 kg (6.61 lb)
Pole diameter	Ø 80 mm–Ø 150 mm (3.15" x 5.91")
Mounting mode	Pole mount and wall mount

Appendix 2 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use overlapped characters, such as 111, aaa, etc.;

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. Physical Protection

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. Enable Whitelist

We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

8. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

9. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

10. Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

11. Audio and Video Encrypted Transmission

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

12. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

13. Network Log

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

14. Construct a Safe Network Environment

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.

- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.