IR Illuminator

User's Manual



V1.0.0

Foreword

General

This manual introduces the installation, functions and operations of the IR illuminator (hereinafter referred to as "the Illuminator"). Read carefully before using the device, and keep the manual safe for future reference.

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, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	April 2022

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates

might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.

- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of 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 company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, comply with the guidelines when using it, and keep the manual safe for future reference.

Transportation Requirements



- Pack the device with packaging provided by its manufacturer or packaging of the same quality before transporting it.
- Transport the device under allowed humidity and temperature conditions.

Storage Requirements



Store the device under allowed humidity and temperature conditions.

Installation Requirements



- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.
- When using a laser beam device, avoid exposing the surface of the device to laser beam radiation.
- Do not install the device in an environment that has a large amount of metal, advertising boards, walls or electromagnetic interference. Otherwise, the performance of the device might be affected.
- Do not install 2 devices with the same frequency in the same environment. Otherwise, the device might not work properly.



- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.

- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- An emergency disconnect device must be installed during installation and wiring at a readily accessible location for emergency power cut-off.
- Protect the line cord and wires from being walked on or squeezed particularly at plugs, power sockets, and the point where they exit from the device.
- Make sure that the device is installed horizontally, and that there are no items blocking the front of the device.

Operation Requirements



- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Use the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device without professional instruction.
- We recommend you use the device with a lightning protection device for stronger protection against lightning. For outdoor scenarios, strictly comply with the lightning protection regulations.
- Ground the function earthing portion of the device to improve its reliability. The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.

Maintenance Requirements



- Clean the device with a soft dry cloth or a clean soft cloth dipped in neutral detergent.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.

Table of Contents

Foreword I
Important Safeguards and Warnings III
1 Overview 1
1.1 Introduction 1
1.2 Features 1
2 Structure 2
2.1 Appearance 2
2.2 Dimensions 3
3 Installation 4
3.1 Installing the Illuminator 4
3.1.1 Installation without Bracket 4
3.1.2 Installation with Bracket 4
3.2 Cable Connection 6
3.2.1 Connecting the cables 6
3.2.2 Waterproof 6
3.3 Commissioning 7
4 FAQ 9
Appendix 1 Cybersecurity Recommendations 10
Appendix 2 Lightning and Surge Protection 13

1 Overview

1.1 Introduction

The DH-PFM522 series IR illuminator is a smart illuminator. You can control the on and off of the Illuminator according to different scenarios. The Illuminator uses an imported LED chip as the light source. With a precise optical design, the light intensity can be evenly and effectively distributed, and achieve the overall highlighting effect and provide professional supplementary light for video monitoring, vehicle and pedestrian detection and capture. The Illuminator can be widely used in scenarios including parking lot, toll station, entrance and exit, and security checkpoint.

1.2 Features

- IP 66 protection.
- Die cast aluminum cover.
- Explosion-proof design.
- One-piece lens and imported light source.
- Supports multiple installation methods including pole mount, wall mount and plane mount.

2 Structure

2.1 Appearance

Figure 2-1 Appearance

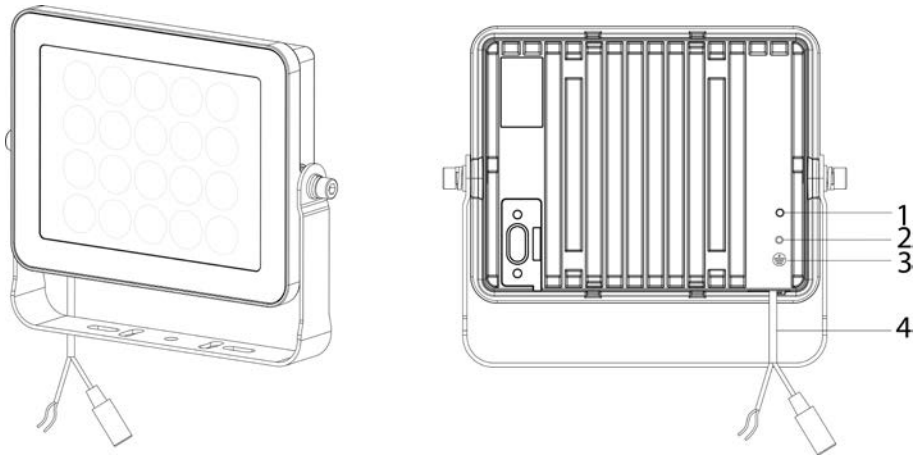
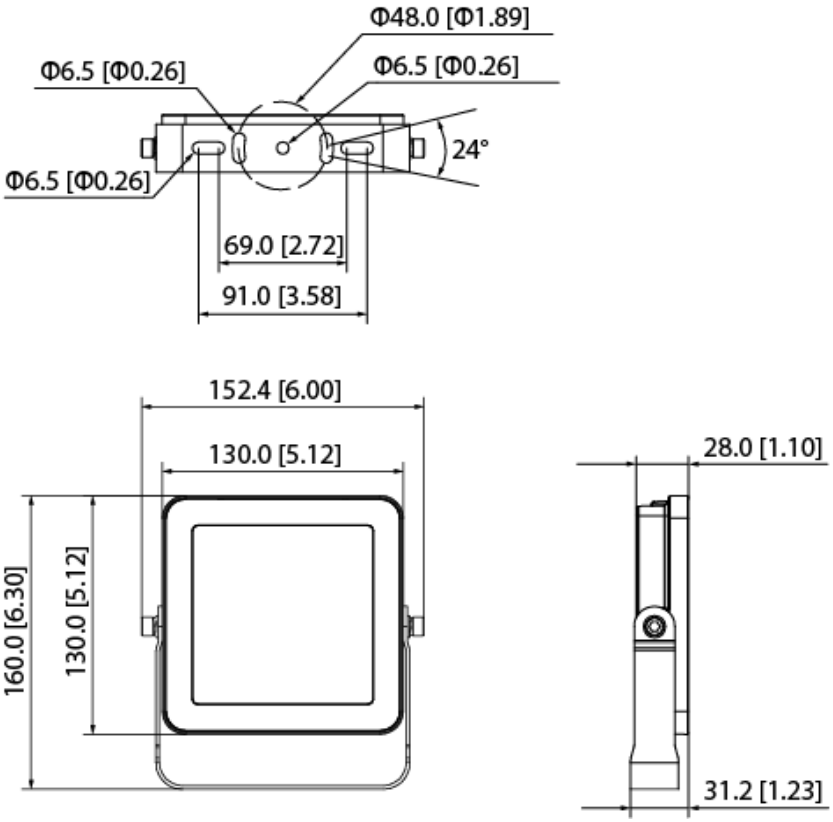


Table 2-1 Component description

No.	Port	Port description
1	Photosensitive tube	Decide whether to light up according to the scenarios.
2	Grounding hole	Ground through the grounding screw.
3	12 V input cable	Inputs 12 VDC.
4	RS–485 cable	Connects to cameras controlled by RS–485. Yellow: RS–485_A. Orange: RS–485_B.

2.2 Dimensions

Figure 2-2 Dimensions (unit: mm [inch])



3 Installation

WARNING

The Illuminator is classified as RG2 according to the *EN 62471-2006 Photobiological safety of lamps and lamp system*. Do not stare at the Illuminator. The Illuminator might cause blue-ray or heat damages to eyes.

- To protect the photosensitive components from being soaked by rain and affecting the normal operation, we recommend you face down the photosensitive components during installation, and avoid strong light towards the components. Otherwise the components might malfunction.
- To enhance the reliability, make sure to ground to the earth and make all port well waterproofed.

3.1 Installing the Illuminator

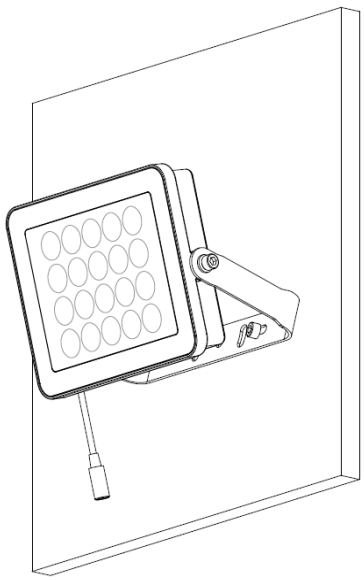
3.1.1 Installation without Bracket

Step 1 Drill two M6 mounting holes on the panel with the distance of 69 mm to 91 mm between the holes.

Step 2 Hammer two SX8 × 40 anchor bolts into the mounting holes.

Step 3 Fix the Illuminator onto the panel with two M6 × 20 combination screws.

Figure 3-1 Installation without bracket

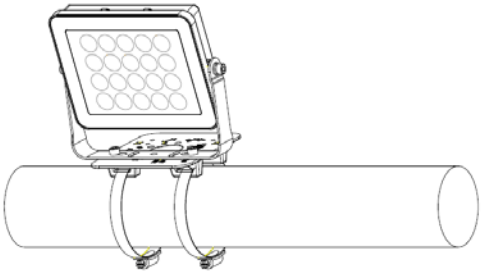
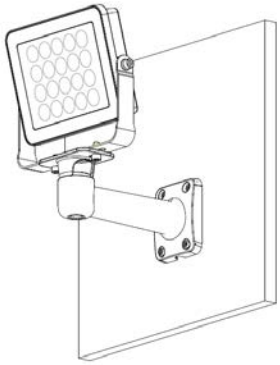
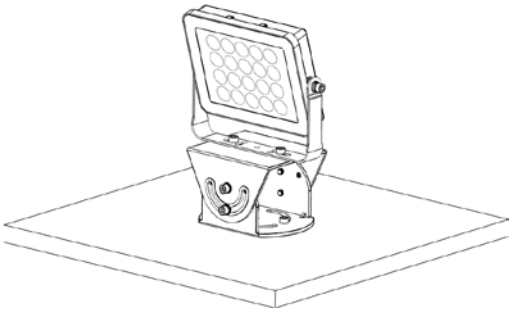


3.1.2 Installation with Bracket

Fix the Illuminator onto the bracket with two M6 × 12 combination screws and M6 hexagonal nuts, and then adjust the bracket to the specific position.

The bracket does not come with the delivery. Buy it if it is necessary.

Table 3-1 Bracket diagram

Bracket model	Diagram
Pole mount	
Wall mount	
Plane mount	

3.2 Cable Connection

3.2.1 Connecting the cables

For details on lightning and surge protection, see "Appendix 2 Lightning and Surge Protection".

Figure 3-2 Cable connection

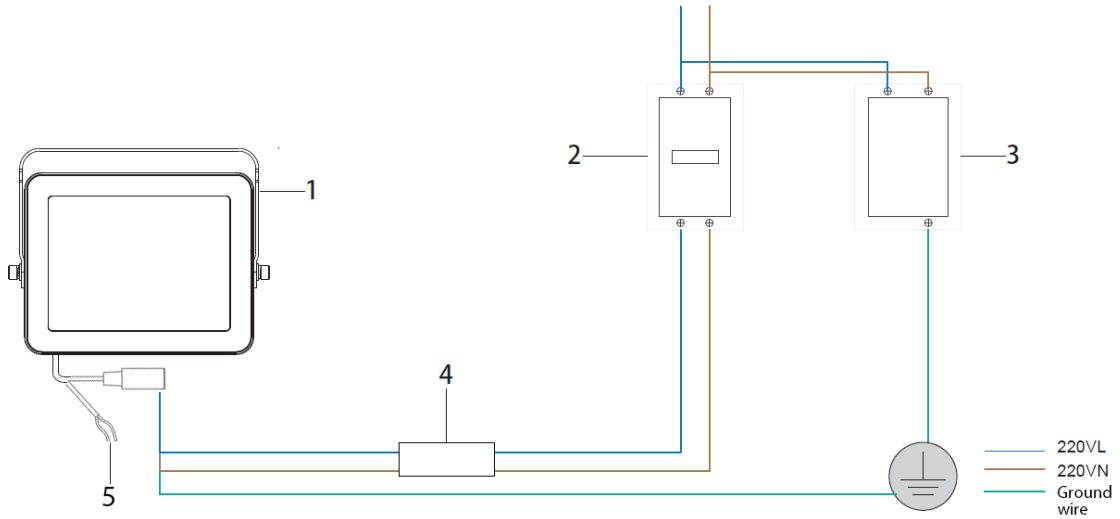


Table 3-2 Component description

No.	Component
1	Illuminator
2	Air circuit breaker
3	Lightning protector
4 (Optional)	Check if the adapter is needed: ● If the power input is main electricity, connect the adapter directly. ● If the power input is not main electricity, connect the corresponding adapter.
5	RS–485 cable

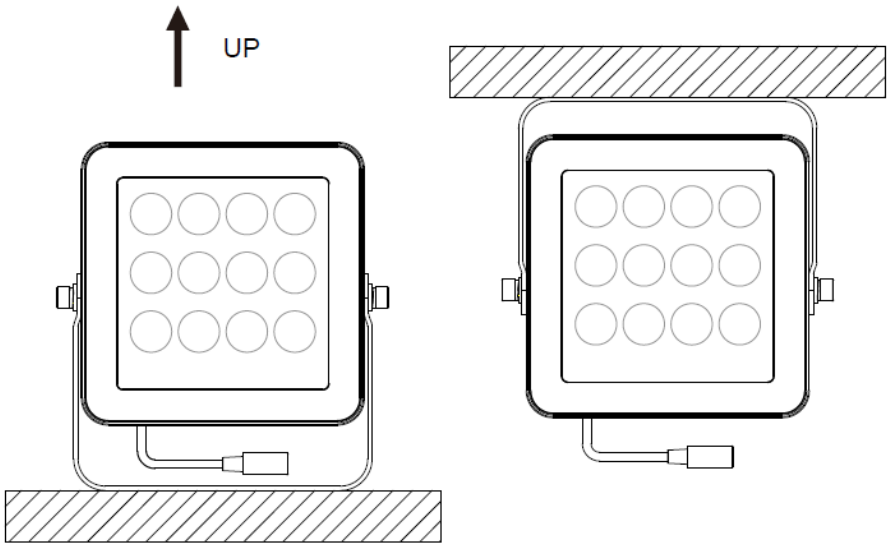
3.2.2 Waterproof

Make sure to waterproof all the connectors to enhance the reliability of the Illuminator.

You need to waterproof the connector even if there is no RS–485 cable connection.

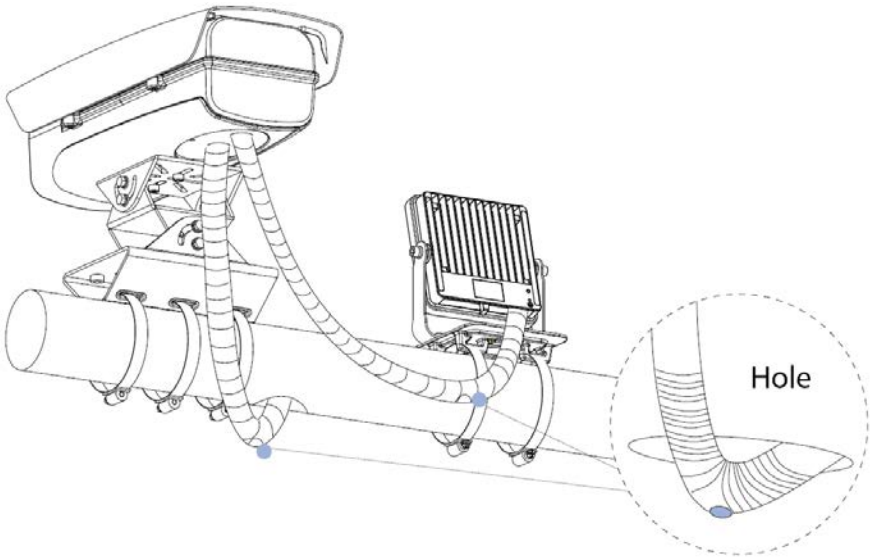
- Upright installation.
  Make sure to install the Illuminator upright and place the connection part downward.

Figure 3-3 Upright installation



- Drilling a hole under the waterproof pipe.
  Put the cables in the waterproof pipe, and drill a hole under the pipe to prevent water from accumulating.

Figure 3-4 Drill hole under the pipe



3.3 Commissioning

After connecting the power supply, if the RS–485 signal is not connected or the signal is not sent, the Illuminator enters the photosensitive mode by default and starts the environmental monitoring mode, and then the Illuminator will turn on or off according to the outdoor environment in one minute. If the RS–485 signal is connected and the signal is sent, the Illuminator answers to the corresponding signals.

Table 3-3 Mode description

Mode	Description
RS–485 mode	Connects to RS–485 signals according to label description to control the on-off and brightness of the Illuminator. You can operate through the Camera web page.
Photosensitive mode	Turns on and off according to the outdoor environment. • Make sure that the photosensitive tube is not blocked after installation, otherwise the normal operation might be affected. If there is block, you can adjust the photosensitive tube to a proper position and avoid the solid-on of the Illuminator. • The photosensitive mode is set with switch delay to avoid abnormal switches caused by sudden changes of ambient light.

Mode switch:

- From photosensitive mode to RS–485 mode: Connecting to signal cables and sending signals.
- From RS–485 mode to photosensitive mode: No sending signals or not connecting to signal cables for at least one minute.

To avoid sudden accidents such as dizziness caused by strong light, after the power supply is connected, the Illuminator is set with delay. After one minute, the Illuminator enters the working mode, and the Illuminator remains off before entering the working mode.

There are two working modes of the Illuminator:

Table 3-4 Working mode description

Mode	Description
RS–485 control mode	After connecting the Illuminator to the RS–485 signals, the switch and power of the Illuminator can be controlled by RS–485 command. The photosensitive control mode is unavailable. After the RS–485 signals are off for one minute, the Illuminator switches photosensitive control mode.
Photosensitive control mode	Powering on is photosensitive controlled by default, and the Illuminator turns on and off according to the outdoor environment.

Make sure that the photosensitive tube is not blocked after installation, otherwise the normal operation might be affected. If there is block, you can adjust the photosensitive tube to a proper position and avoid the solid-on of the Illuminator.

4 FAQ

This section introduces the frequently occurred problems and solutions during the installation and use.

Table 4-1 Problems and solutions

Problem	Reason	Solution
After connecting to the power supply, the Illuminator is off.	• Power input parameters are wrong. • Power cord is poorly connected. • The Illuminator is broken. • The brightness is great and the Illuminator does not need to turn on. • The Illuminator is in environment monitoring and needs one minute until it turns on. • The Illuminator connects to RS–485 signal, and the signal command is off.	• Check if the input power and power cord are correct, if not, replace them. • Contact customer service if the Illuminator is broken.
The Illuminator is on during daylight when the ambient light is bright.	• The photosensitive tube is blocked (directly blocked or hidden by other objects). • The photosensitive tube is broken. • The Illuminator connects to RS–485 signal, and the signal command is on.	• Check if the photosensitive tube is blocked, remove the blocks. • Contact customer service if the photosensitive tube is broken. • The Illuminator turns on and off according to the on-site environment. The Illuminator turns on in dark environment and there is a delay when it turns on.
After working for a while, the Illuminator flickers and turns off.	• There are devices with large power in the area where the Illuminator works. The controlling chip of the Illuminator is broken caused by overvoltage. • The Illuminator is installed outdoors and is not lightning protected, and the controlling chip is broken.	Contact customer service.

Appendix 1 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.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.

Appendix 2 Lightning and Surge Protection

The Illuminator adopts TVS lightning protection technology. It can effectively prevent damage from various pulse signals, such as a sudden lightning and surge. However, you still need to take necessary precaution measures in accordance with your local electrical safety code when installing the Camera in outdoor environment.

- For vast land, use sealing steel tube under the land to implement cable layout and make sure that both ends of the tube are equipotentially grounded. Open floor cable layout is forbidden.
- In area of strong thunderstorm or near high sensitive voltage (such as near high-voltage transformer substation), install additional high-power thunder protection device or lightning rod.
- The system shall adopt equal-potential wiring. The grounding devices shall meet anti-jamming requirements and at the same time conforms to your local electrical safety code.
- The grounding devices shall not be connected to N (neutral) line of high voltage power grid or mixed with other wires. When you connect the system to the ground alone, the grounding resistance shall not be more than 4 Ω and the cross-sectional area of grounding cable shall be no less than 25 mm^2.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883