Smart Plug

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

Foreword

This manual introduces the dimensions, structure and the operations of the smart plug. Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words 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.	May 2023

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, and comply with the guidelines when using it.

Operation Requirements

⚠

- Operate the device within the rated range of power input and output.
- Make sure your hands are dry when using the device to avoid being shocked.
- 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
- Change the device as soon as you can if it behaves abnormally.
- Do not disassemble the device or forcibly plug or unplug the external terminal. Otherwise, damage to the data port or communication anomaly might occur.
- Transport, use and store the device under allowed humidity and temperature conditions.

Installation Requirements

⚠ WARNING

- Make sure that the power is off when you connect the cables, install or uninstall the device.
- 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.

⚠

- Keep the device away from dampness, dust, and soot.
- Install the device on a stable surface to prevent it from falling.
- The device can only be installed indoors, or inside a waterproof electrical cabinet outdoors. Do not expose the device to rain or dampness.
- Operators need to have certificates or experience in installation and maintenance of low-voltage distribution systems and circuit breakers. They also need to have qualifications in related work, and the following knowledge and skills are required:
    - ◇ Basic knowledge and skills in installing low voltage distribution systems and their components.
    - ◇ Basic knowledge and skills in low-voltage wiring and in connecting low-voltage electronic circuits.
    - ◇ Basic knowledge of safety procedures and skills with low voltage distribution systems. They also have to have the ability to read the manual.

Maintenance Requirements

- Have the device regularly inspected when operating it.
- Cut off the power before cleaning the surface of the device. To clean the device, wipe its surface with a soft dry cloth or other replacements. Do not use liquid detergents on the device to avoid the risk of short circuits caused by water ingress and dampness.

- Immediately cut the power and disconnect the power cord if the device behaves abnormally, or if a strange noise or unpleasant odor comes from the device.
- Clean the device regularly to avoid a build-up of dust and verdigris, which can cause the temperature of the device to increase, shortening its lifespan.
- Do not use the device if it is behaving abnormally such as the temperature is too high, it is on fire, there is poor contact, or the cable tap is too tight or too loose.
- Contact your local dealer and provide details when the device is working abnormally. We will assume no responsibility for any problems caused by unauthorized modifications or repairs.

目录

1 Overview

1.1 Introduction

The smart plug uses the electronic switch and the built-in antenna to control the electricity. After you add and configure the smart plug on the DMSS app, you can remotely control the on/off status and configure the timing tasks for the plug. You can also configure alarms, switch on or switch off the arm and disarming linkage, and view the input voltage on the app.

1.2 Features

- RF two-way communication.
- Remote control and device control.
- LED light displays the status.
- Cloud update and recovery from update failure.
- Protection for overvoltage, overcurrent and high temperature.
- Detection for voltage, current, temperature and power.
- Energy consumption statistics. You can also reset the data.
- Mode switch between bistable mode and pulse mode.

1.3 Structure

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

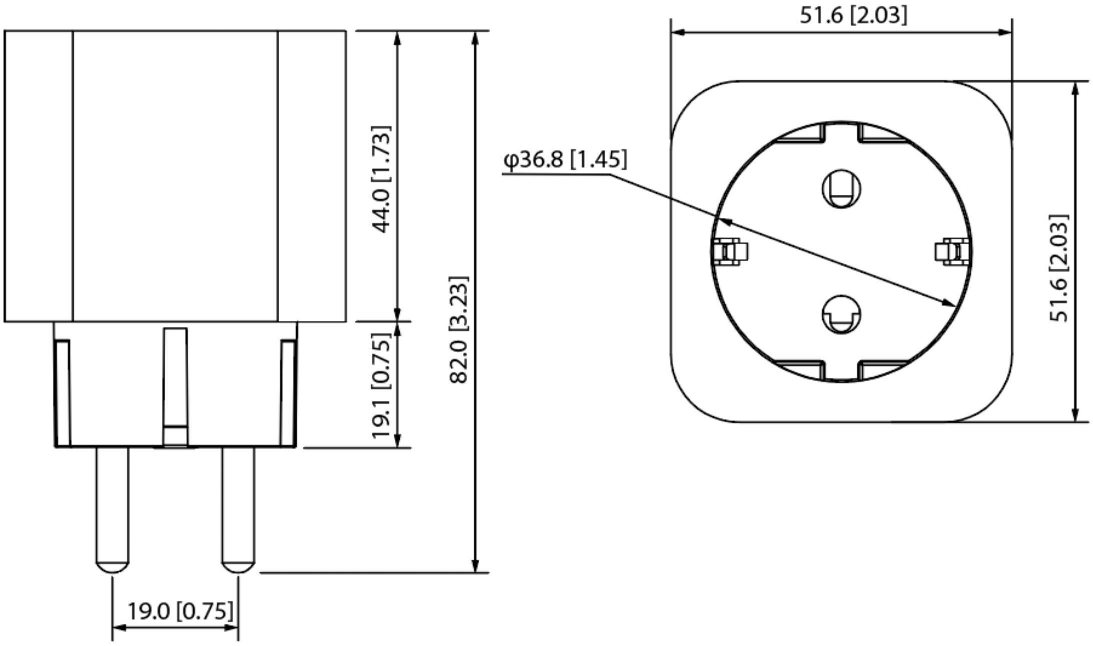


Figure 1-2 Structure

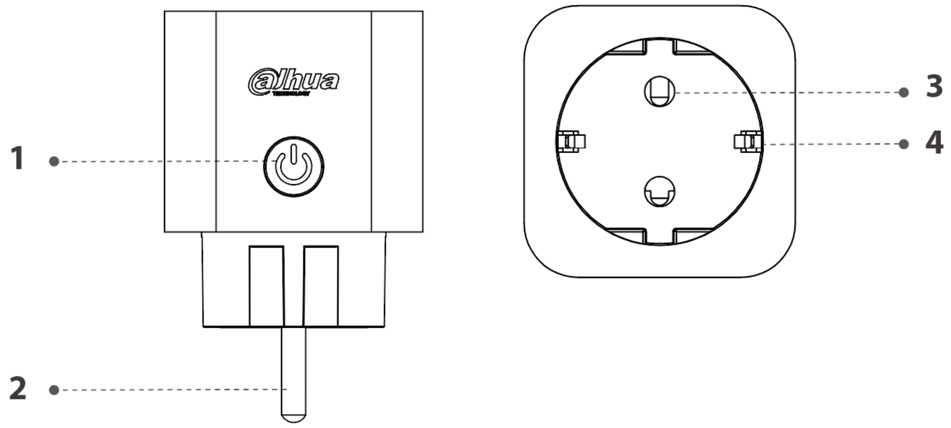


Table 1-1 Structure

No.	Name
1	Power button
2	Round prong
3	Prong receptacle
4	Earthing pin

Indicator light description

- Flashing green quickly for 30 seconds after solid green for 2 seconds: The device is connecting to the alarm hub.
- Flashing green quickly (low brightness): Attenuation mode.
- Flashing green slowly (low brightness): Signal test mode.
- Solid green (high brightness): The device closes the circuit.
- Indicator light off: The device opens the circuit or is powered off.

Button description

- Press the button, and the device opens/closes the circuit.
- Press the button for 4 seconds, and the device starts connecting to the alarm hub.
- Press the button for 8 seconds, and the device restores to factory default.

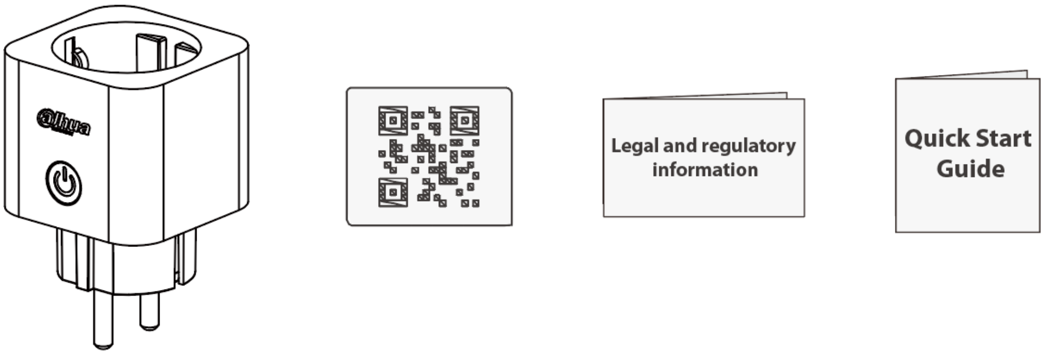
1.4 Checklist

Table 1-2 Checklist

Item Name	Quantity
Smart Plug	1
Quick Start Guide	1
Legal and Regulatory Information	1

Item Name	Quantity
QR Code	1

Figure 1-3 Checklist



1.5 Basic Parameters

Table 1-3 Basic parameters description

Parameter	Description
Power Input	100 VAC–240 VAC, 50/60 Hz
Power Output	100 VAC–240 VAC, Max 16 A
Operating Environment	–10 °C to +55 °C/+14 °F to +131 °F (Indoor scenario)
Operating Humidity	10%–90% (RH)

2 Configuration

2.1 Configuration Procedure

Connect the plug to the alarm hub.

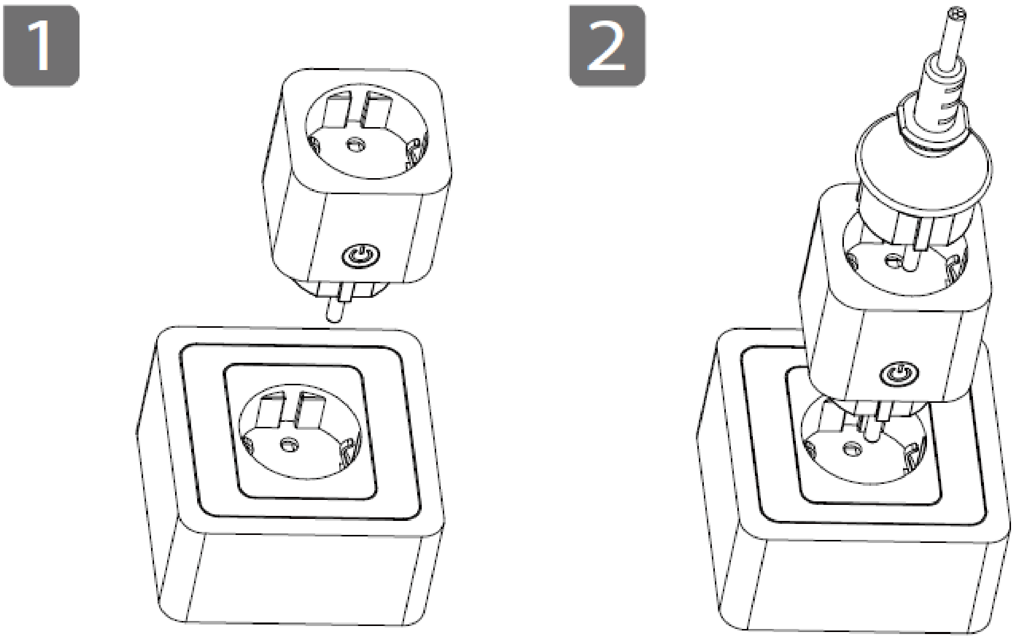
Prerequisites

- Make sure the alarm hub is powered on and is successfully connected to the DMSS app.
- Make sure the alarm hub works normally and enters the connection mode by pressing the on/off button for 2 times.
- The connection will be success when both the plug and the alarm hub are in the connection mode.

Procedure

Step 1 Plug the round prongs into the wall socket or the power strip, and then connect the electrical load to the prong receptacle.

Figure 2-1 Installation



Step 2 Connect the plug to the alarm hub.

- Automatic connection: Power on the plug. The plug automatically enters the connection mode and the indicator light flashes green (high brightness) quickly for 30 seconds.
- Manual connection: Press the button on the plug for 4 seconds to enter the connection mode.
- Connection through the app: Scan the QR code on the plug through DMSS app and connect the plug with the alarm hub according to the prompts.

Results

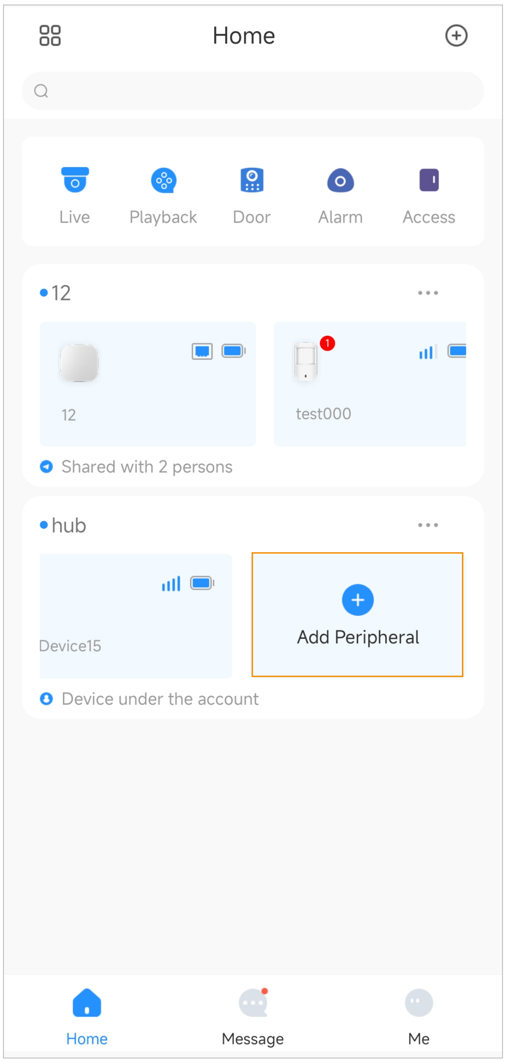
- Successful connection: The indicator light turns solid green for 2 seconds and turns off. The plug opens the circuit. Press the button to close the circuit. The indicator light turns solid green.
- Failed to connect: The indicator light flashes for 3 times and turns off. Press the button, and the indicator light does not change. Press the button for 4 seconds to enter the connection mode again.

2.2 Operations on DMSS

Adding the plug

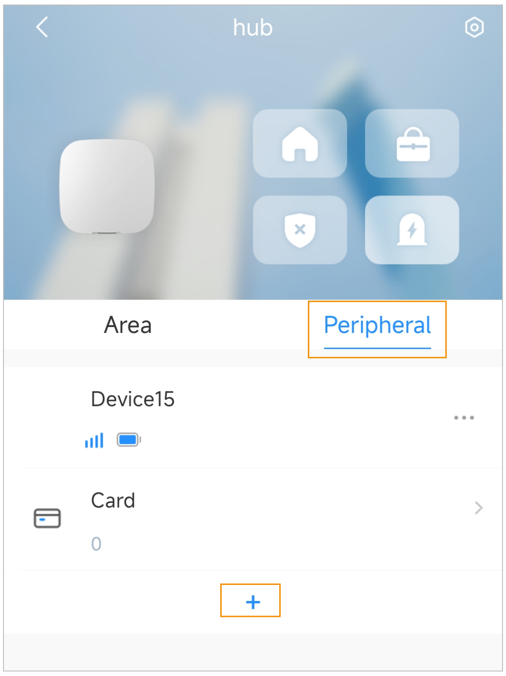
- On the home screen, tap **Add Peripheral**. Scan the QR code of the plug.

Figure 2-2 Adding the device (1)



- On the home screen, tap the hub device, and then tap **Peripheral** > **+** . Scan the QR code of the plug.

Figure 2-3 Adding the device (2)

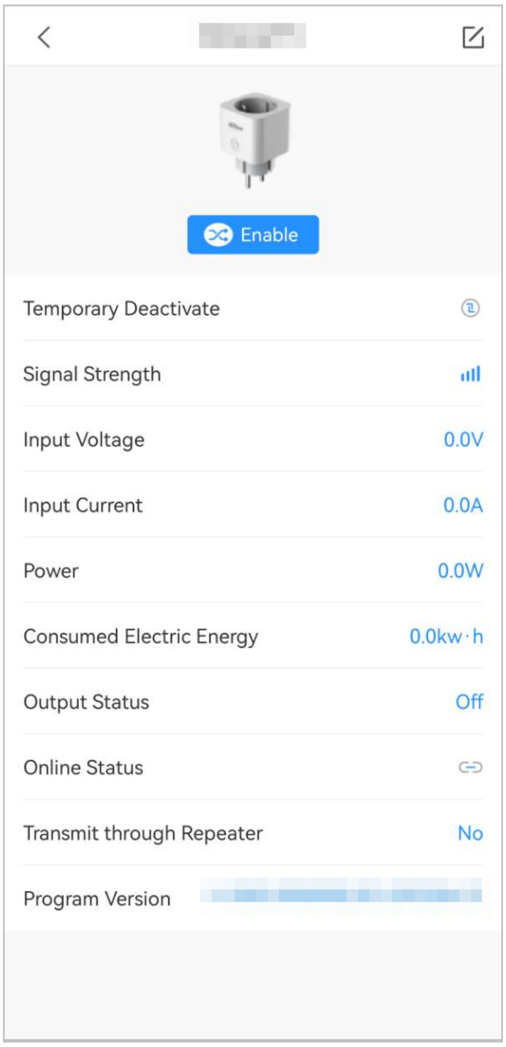


Device Information

On the home screen, tap the plug to view the signal strength, input voltage, input current, power, consumed electric energy and other information.

Temporary Deactivate: If enabled, all information will be sent to the alarm hub. Enable or disable this function in the configuration screen.

Figure 2-4 Device Information



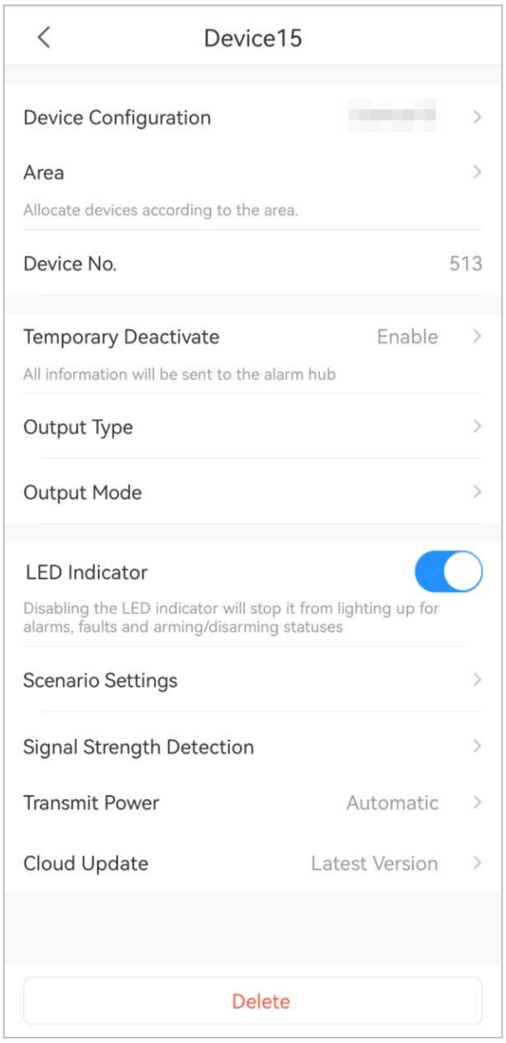
Enable

Temporary Deactivate	
Signal Strength	
Input Voltage	0.0V
Input Current	0.0A
Power	0.0W
Consumed Electric Energy	0.0kw·h
Output Status	Off
Online Status	
Transmit through Repeater	No
Program Version	

Device Configuration

Tap ☑ to configure the parameters.

Figure 2-5 Device configuration



Device15

Device Configuration [redacted]

Area

Allocate devices according to the area.

Device No. 513

Temporary Deactivate Enable

All information will be sent to the alarm hub

Output Type

Output Mode

LED Indicator

Disabling the LED indicator will stop it from lighting up for alarms, faults and arming/disarming statuses

Scenario Settings

Signal Strength Detection

Transmit Power Automatic

Cloud Update Latest Version

Table 2-1 Parameters description

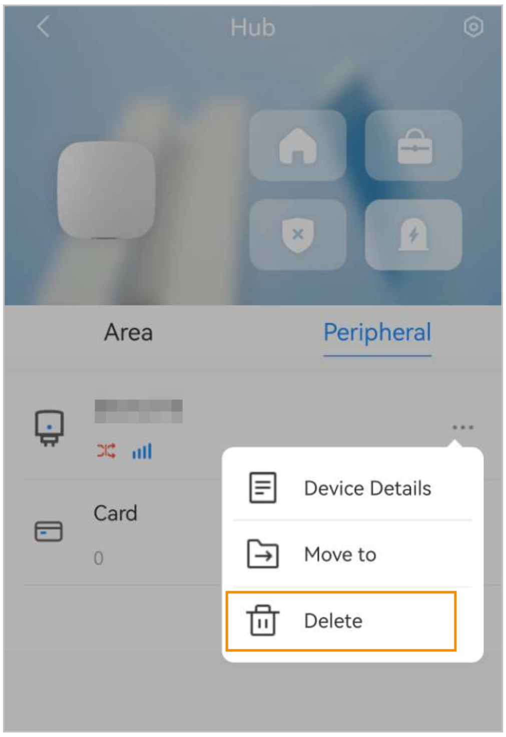
Parameter	Description
Device Configuration	Tap to configure the device name and view the type, SN and device model.
Area	View the current area. Supports adding the new areas.
Device No.	The number to distinguish the devices.
Temporary Deactivate	If enabled, all information will be sent to the alarm hub.
Output Type	Select from **Normally Open** and **Normally Closed**.
Output Mode	● Bistable: When you select this mode, the remote operations will not be changed until you operate the device again. ● Pulse: When you select this mode, configure the pulse durations. For example, if you configure the pulse duration as 60 seconds and configure the output type as normally open, the plug will normally open for 60 seconds.
LED Indicator	You can enable or disable the LED indicator.

Parameter	Description
Scenario Settings	Tap to configure arming/disarming linkage scenario, alarm linkage scenario and scheduled linkage scenario.
Signal Strength Detection	Check the current signal strength.
Transmit Power	Select from **High** , **Low** and **Automatic**.
Cloud Update	View the current version and check that if there is new version to be updated.

Deleting the device

- On the device configuration screen, tap **Delete**.
- On the home screen, tap hub device, tap ··· next to the corresponding device, and then tap **Delete**.

Figure 2-6 Deleting the device



2.3 Maintenance

- Have the device regularly inspected when operating it.
- Cut off the power before cleaning the surface of the device. To clean the device, wipe its surface with a soft dry cloth or other replacements. Do not use liquid detergents on the device to avoid the risk of short circuits caused by water ingress and dampness.
- Make sure your hands are dry when using the device to avoid being shocked.

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 from Dahua on how to create a more secured security system.

Mandatory actions to be taken for basic device 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 device (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 device 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 device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device 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 device (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 device 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. **MAC Address Binding**

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

8. **Assign Accounts and Privileges Reasonably**

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

9. **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.

10. **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.

11. **Secure Auditing**

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

12. **Network Log**

    Due to the limited storage capacity of the device, 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.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device 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.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188