**Distributed Microphone**

**Quick Operation Manual**

|  |
| --- |
| V1.0.0 |



Preface

Overview

The manual describes the instructions for quick configuration and operation of the distributed microphone.

Symbols and Meanings

The following signs might appear in the manual, with the following defined meanings.

| **Symbol** | **Meaning** |
| --- | --- |
|  | Indicates a potential hazard with high level of risk which, if not avoided, will result in death or serious injury. |
|  | Indicates a potential hazard with medium or low level of risk which, if not avoided, could result in minor or moderate injury. |
|  | Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result. |
|  | Indicates a static-sensitive device. |
|  | Indicates a high voltage hazard. |
|  | Indicates intense laser radiation. |
|  | Indicates dangerous moving parts (such as a moving fan blade) from which a safe distance shall be maintained. |
|  | Indicates the possibility of mechanical injuries to persons in close range caused by parts of device. |
|  | Indicates a tip that may help you solve a problem or save your time. |
|  | Indicates additional information as the emphasis and supplement to the text. |

Revision History

| Version | Revision Content | Issuance Date |
| --- | --- | --- |
| V1.0.0 | First release. | November 21, 2023 |

Safety Instructions

The following is about the correct product usage intended to guard against dangers and prevent property loss. Before usage, please carefully read through this document and strictly follow its instructions. Please keep the manual properly after reading for easy access.

Usage requirements

* Do not place and install the device in direct sunlight or near heating devices.
* Do not install the device in a humid, dusty place, or a place with smoke from burning coal.
* Install the device horizontally, or install it in a stable place to prevent the product from falling.
* Do not have liquids splashing or dripping to the device, and make sure that no articles fully filled with liquids are placed on the device, to prevent liquids from flowing into the device.
* Install the device in a ventilated place, and do not block the air vent of the device.
* Always use this device according to its rated input/output range.
* Do not dismantle this device at will.
* Transport, use, and store the device within the allowed temperature range and humidity range.

Power supply requirements

* Use the battery as required! Otherwise, the battery might catch fire, explode, or burn!
* Always replace the battery with exactly the same type!
* Use the electrical wire (power cable) assembly recommended for the device in your region, and use it within specifications!
* Always use the standard power adapter specifically designed for the device. Otherwise any personal injury or device damages caused shall be borne the users themselves.
* Use SELV (safety extra low voltage) power supply to supply power of rated voltage according to GB8898 (IEC60065) or GB4943.1 (IEC60950-1, conforming to Limited Power Source). The power supply requirements are as specified on the device labels.
* If a power adapter is to be used for charging, a CCC-certified power adapter that conforms to the standards shall be purchased and used.
* Please connect devices of Type I structure to a grid power supply output socket that has protective grounding connections.
* The appliance coupler is a disconnecting component. Keep the coupler at an angle that is easy for operation during usage.

Contents

[Preface I](#_Toc154499109)

[Safety Instructions II](#_Toc154499110)

[Chapter 1 Product Overview 4](#_Toc154499111)

[1.1 Brief Introduction 4](#_Toc154499112)

[1.2 Features 4](#_Toc154499113)

[Chapter 2 Product Structure 5](#_Toc154499114)

[Chapter 3 Product List 7](#_Toc154499115)

[Chapter 4 System Operation 8](#_Toc154499116)

[4.1 Connection Method 8](#_Toc154499117)

[4.1.1 Connection to the Conference TV Terminal 8](#_Toc154499118)

[4.1.2 Connection to the PC/Conference Tablet 8](#_Toc154499119)

[4.1.3 Cascading Illustration 9](#_Toc154499120)

[4.2 Volume Adjustment 9](#_Toc154499121)

[4.3 Turning On/Off the Microphone 10](#_Toc154499122)

[4.4 Answering or Ending a Call 10](#_Toc154499123)

[4.5 OTA Software Upgrade Tool 10](#_Toc154499124)

[Annex 1 Technical Parameters 11](#_Toc154499125)

[Annex 2 Legal Statement 12](#_Toc154499126)

[Annex 3 Cybersecurity Recommendations 13](#_Toc154499127)

# Product Overview

## Brief Introduction

This product is a wired high-performance distributed microphone with amplification. It supports 360° omni-directional pickup with a pickup radius of 6 m and up to 4-stage cascading. It can be used with the Hitry video conference hard terminal, conference tablet, PC client, Tencent Conference, and other software. It brings new high-fidelity sound experience for users by using the 3A intelligent algorithm.

## Features

|  |
| --- |
| * AI-based noise reduction, AI-based echo cancellation, and AI-based de-reverberation * Omni-directional 8-microphone array |
| * Full duplex technology * USB plug and play * Support 4-stage PoE cascading |

# Product Structure

The distributed microphone is cylindrical in appearance, with 8 array microphones distributed on the sides and an answer/hang-up button, volume adjustment buttons, and a mute button at the top. The touch buttons enable control of the microphone at any time to achieve real-time synchronization of the microphone with the conference status. The structure is as shown in Figure 2-1 and Figure 2-2.

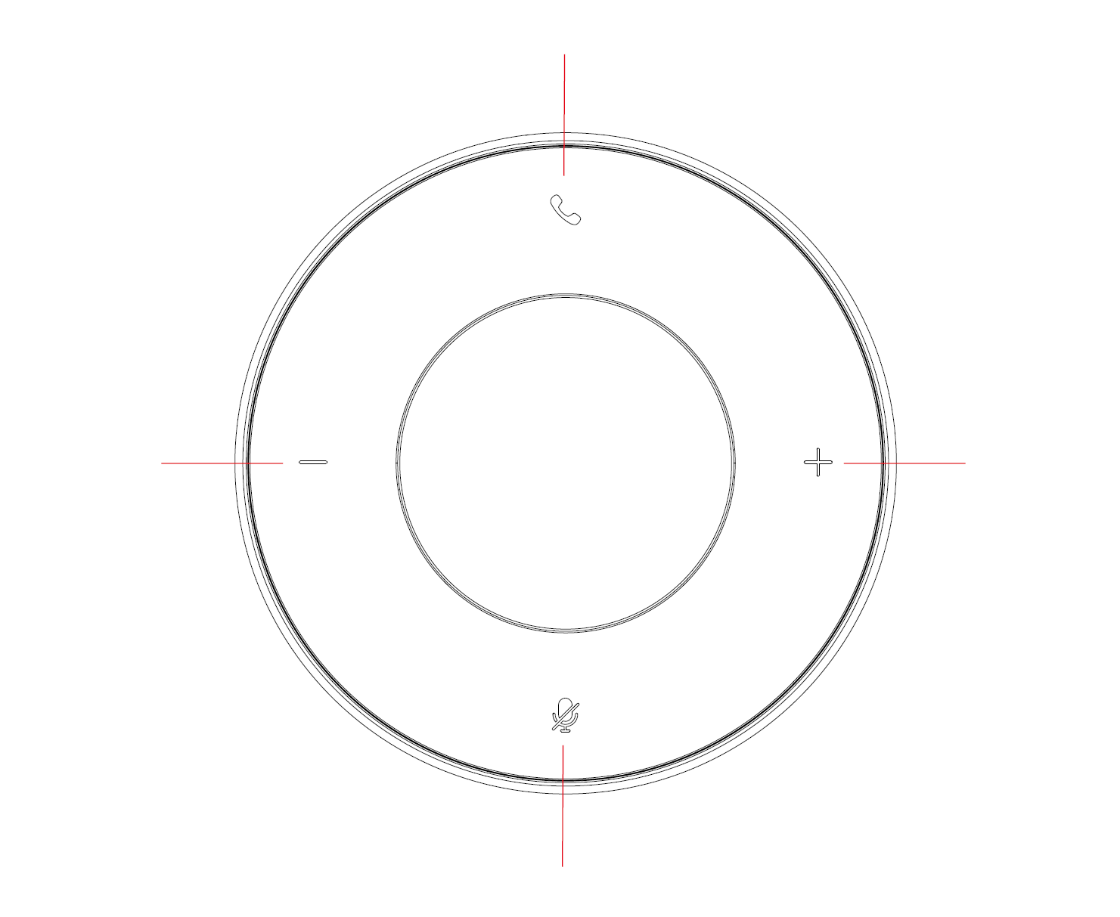
Top view

Answer/Hang-up

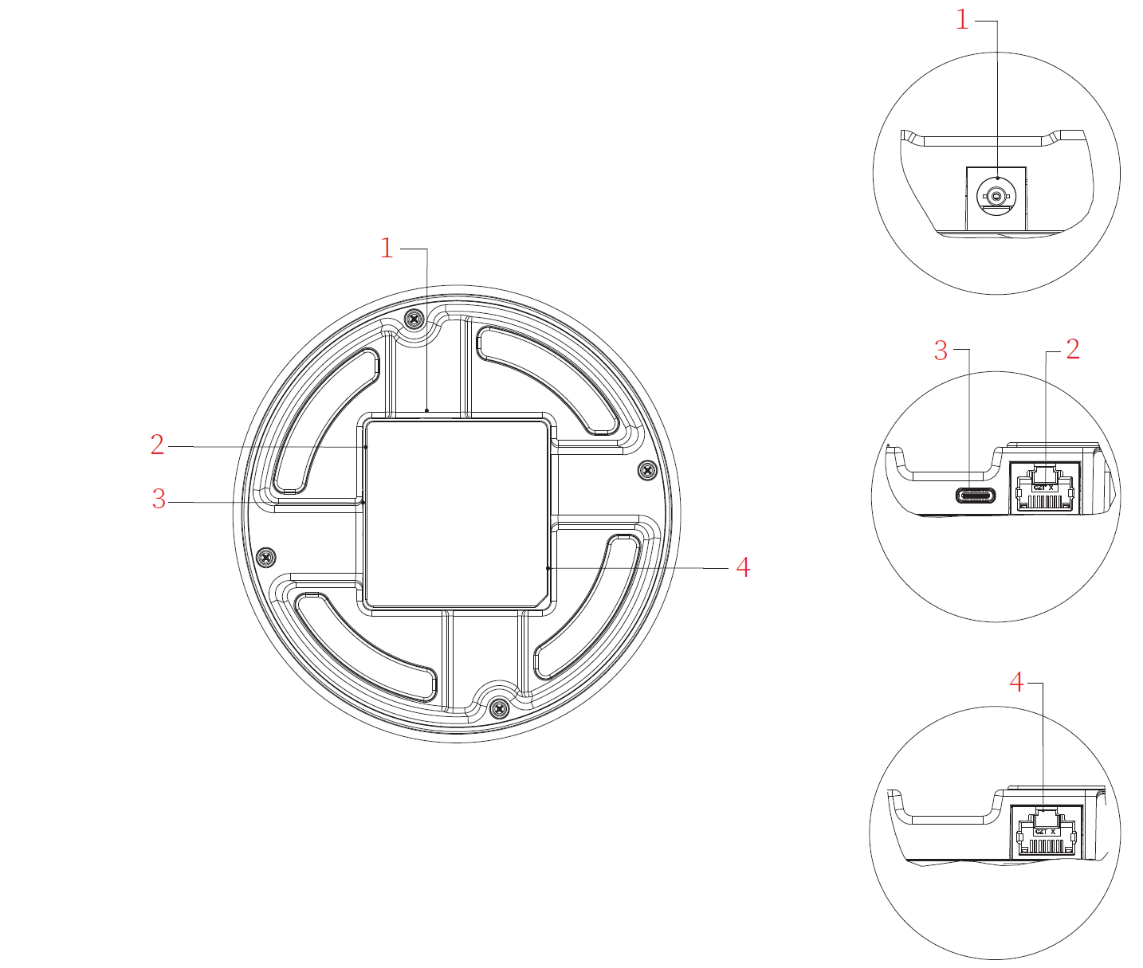
Vol down

Vol up

Turn on/off the microphone



Bottom view



Power supply interface

Network port PREVIOUS

Type C interface

Network port NEXT

Interface description

| Interface No. | Name | Meaning |
| --- | --- | --- |
| 1 | Power supply interface | Connects the power adapter for power supply to the device |
| 2 | Network interface PREVIOUS | Cascades the previous device |
| 3 | Type C interface | Performs data transfer and power supply through USB-type C |
| 4 | Network interface NEXT | Cascades the next device |



The power adapter and Type C interface connect only the first device.

# Product List

Before connecting the device, verify items in the package against Table 3-1.

List of Items

| No. | Name | Quantity | Meaning |
| --- | --- | --- | --- |
| 1 | Distributed Microphone | 1 set | Microphone device |
| 2 | Standard external cable - (USB 2.0, AM to CM) - black - 5 m | 1 piece | Connects the microphone to the conference TV terminal/PC/conference tablet for data transfer and power supply. |
| 3 | Standard external cable - (Cat. 6 network cable, RJ45 to RJ45, shielded, flat) - black - 3000 mm | 1 piece | Used for microphone device cascading. |
| 4 | Wall-inserted power adapter (53 V 1 A) | 1 piece | Used for device power supply. |
| 5 | Product QR code | 1 piece | Product operation instructions |
| 6 | Warranty card with certificate of conformity | 1 piece | Warranty card with certificate of conformity |
| 7 | Stored general harmful substance content table | 1 piece | Stored general harmful substance content table |

# System Operation

This product supports USB cable and network port cascading as well as multiple usage scenarios. It can be connected to the conference TV terminal, PC, and conference tablet as a microphone or as a speaker to play music or perform an audio call.

## Connection Method

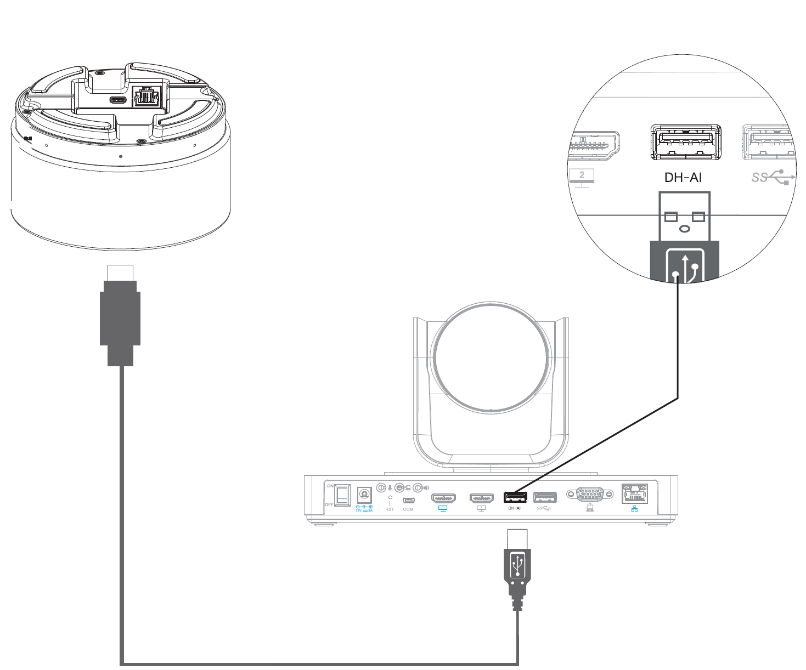
### Connection to the Conference TV Terminal

Use a USB cable to connect the USB-type C interface of the microphone to the USB or DH-AI interface of the conference TV terminal. The microphone can be set to an audio device of the conference TV terminal. Figure 4-1 shows the connection method.

Connection to the Conference TV Terminal

Distributed microphone

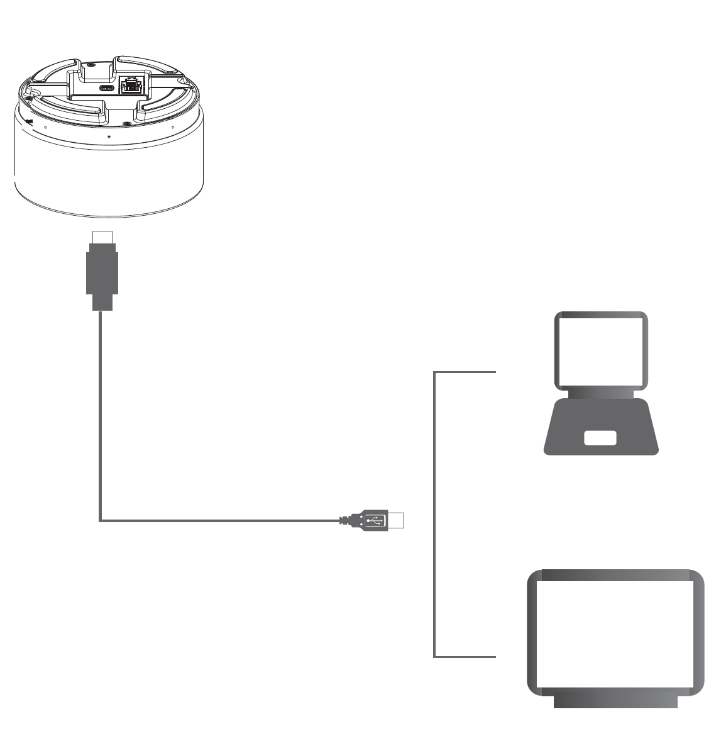
Conference TV terminal



### Connection to the PC/Conference Tablet

Use a USB cable to connect the USB-type C interface of the microphone to the USB interface of the PC. Set the microphone as the default audio device of the PC. Figure 4-2 shows the connection method.

Connection to the PC/conference tablet



Distributed microphone

PC

Conference tablet

### Cascading Illustration

The microphone supports up to 4-stage cascading. The master cascading device needs to be connected to the power adapter and the USB cable. One end of the USB cable is connected to the USB-type C interface of the microphone and the other end is connected to the USB interface of the conference TV terminal/PC/conference tablet. The slave cascading device is connected using the network cable. Figure 4-3 shows the connection method.

Cascading diagram

Power adapter

PC

Power supply interface

USB (AM to CM) cable

Master device

Network port NEXT

Network port PREVIOUS

Network port NEXT

Network cable

Slave device 1

Slave device 2

Network cable

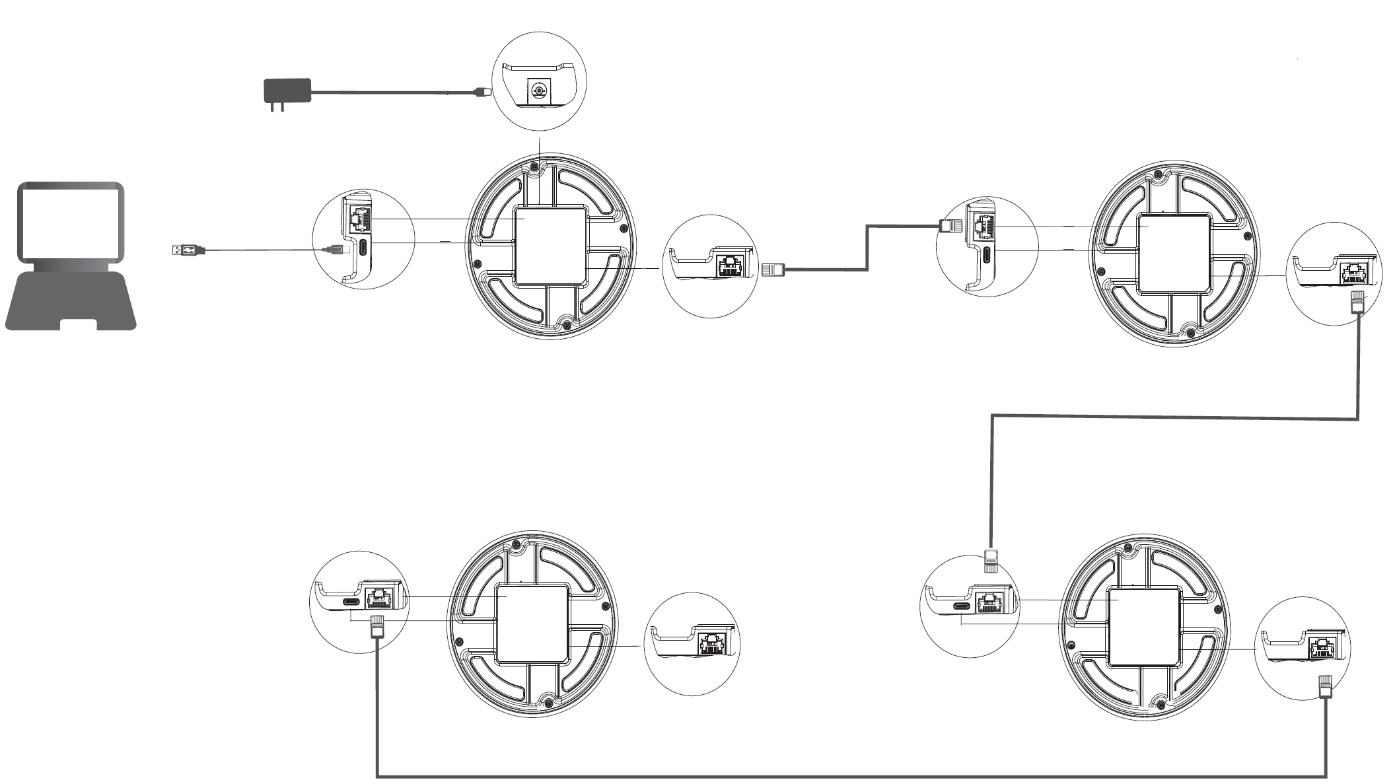
Network port PREVIOUS

Network port NEXT

Network cable

Slave device 3

Network port PREVIOUS



## Volume Adjustment

* Press the **+** or **-** button to adjust the volume;
* By default, the volume at startup is the volume when the product is last turned off.

## Turning On/Off the Microphone

Short press the **Mute** button to mute the microphone or cancel the mute.

* When the microphone is on, the button is green;
* When the microphone is off, the button is red.

## Answering or Ending a Call

* The answer/hang-up button can only be used in the conference.
* Short press the **Answer/Hang-up** button  to answer or end a call.

## OTA Software Upgrade Tool

* The downloading path of the supporting software upgrade tool is as follows:
* <https://www.hitry.com/service/detail/33.html>

1. Technical Parameters

|  |  |  |
| --- | --- | --- |
| Parameter Category | Parameter | Meaning |
| Microphone | Pickup mode | 360° omni-directional pickup |
| Microphone quantity | 8-microphone array |
| Pickup distance | 6 m pickup radius |
| Sampling frequency | 48 kHz |
| Speaker | Speaker quantity | 1 piece |
| Speaker power | 2 W (rated power) |
| Frequency range | 100 Hz to 20 kHz |
| Cascading function | Cascading mode | PoE network cable cascading |
| Cascading quantity | Maximum 4-stage |
| Other parameters | Other interfaces | 1 × PoE IN 1 × PoE OUT |
| USB interface | 1 × USB 2.0 Type-C |
| Power supply mode | 1 × power supply interface (DC 53 V) or USB power supply |
| Installation method | Desktop |
| Supported operating system | Windows 7 or higher, Android, Mac, and Linux |
| Usage scenario | Used with the Hitry 1080P/4K hardware terminal Used with the PC cloud conference software such as Hitry Cloud Conference and Tencent Conference |
| Applicable conference room area | Small, medium, and large conference rooms |
| Environment | Operating temperature: 0 to 45 °C |
| Product dimensions (mm) | 126 mm × 66 mm (diameter × height) |

1. Legal Statement

Trademark Statement

* VGA is the trademark of IBM.
* The Windows logo and Windows wording are the trademarks or registered trademarks of Microsoft.
* Other trademarks and company names possibly be cited in this document are properties of their respective owners.

Liability Statement

* To the extent permitted by applicable laws, under no circumstances shall our company be liable for any special, incidental, indirect, or secondary loss, or for any loss of profit, data, goodwill, files, or expected savings resulting from the relevant contents and described products in this document.
* All products described in this document are provided on an "as-is" basis. Unless required by applicable laws, our company does not give any explicit or implicit guarantee to any contents in this document for, including but not limited to, the marketability, quality satisfaction, fit for a particular purpose, and non-infringement of third party rights.

Privacy Protection Reminder

When installed, this product might be used to collect personal information such as facial features, fingerprints, license plate numbers, emails, phone numbers, and GPS data. When using this product, you must abide by the laws and regulations in your country or region for privacy protection so as not to violate the lawful rights and benefits of other people. For this purpose, you are recommended to take the following actions, such as providing legible and conspicuous sign of this product, advising relevant persons of the existence of the video surveillance zone of this product, and providing corresponding contact information.

About This Document

* This document is for reference only. The actual product might differ.
* Our company reserves the right to update any information in this document from time to time without giving extra notice. The updated contents will be added to new versions of this document.
* Our company has the right of final interpretation to this document in case any information in this document is inaccurate, non-exhaustive, or has typo mistakes.
* This document is a reference for multiple models. The specific operations for each model will not be listed separately Please operate as per the actual model available.
* Any loss caused by failure to follow the instructions in this document during operations shall be borne by the users.
* If the PDF provided with the product cannot be opened, please update your reading tool to the latest version, or use another popular reading tool.

1. Cybersecurity Recommendations

Necessary measures for protecting the basic network security of devices:

* + 1. Use strong passwords

Recommendations for a strong password are as follows:

* + - * The length of the password shall be at least 8 characters.
      * A strong password shall contain at least two character types, including uppercase letters, lowercase letters, numbers, and symbols.
      * A strong password must not contain the account name, or the account name in reverse sequence.
      * A strong password must not contain logically consecutive characters, such as 123 or abc.
      * A strong password must not contain repeated characters, such as 111 or aaa.
    1. Timely update the firmware and client software
       - According to the SOPs of the technological industry, the firmware of devices must be updated to the latest version, so that the devices have the latest functions and security capabilities. If a device is connected to a public network, you are recommended to enable the function of automatic online upgrade detection, so that you can get the firmware update notices from the manufacturers in a timely manner.
       - You are recommended to download and use client software of the latest versions.

Recommended measures for enhancing network security of devices:

* + 1. Physical protection

You are recommended to physically protect your devices (especially storage devices), such as placing them in an exclusive machine room or cabinet that are properly protected by an access control system and key management system, preventing unauthorized personnel from sabotaging the hardware, connecting external devices (e.g., USB flash drive, serial ports, etc.) or contacting the devices in other means.

* + 1. Change password regularly

You are recommended to change passwords regularly to reduce the risk of your passwords being guessed out or cracked.

* + 1. Set and update password reset information in a timely manner

The device supports password reset. To reduce the risk of this function being exploited by hackers, you are recommended to set password reset information in a timely manner, including the phone number, email, and security questions. If there is any change to such information, please update in a timely manner. When setting a security question, avoid setting an answer that can be easily guessed out.

* + 1. Enable account locking

The account locking function is enabled by default upon factory delivery. You are recommended to keep this function enabled to protect your account. A hacker who fails multiple times in entering the correct password will have his/her account and source IP locked.

* + 1. Change the HTTP ports and default ports of other services

You are recommended to change the HTTP port and the default ports of other services to any port between 1024 and 65535, to reduce the risk of your ports being guested out by hackers.

* + 1. Enable HTTPS

You are recommended to enable HTTPS and access Web service through safe channels.

* + 1. Enable allowlist

You are recommended to enable the allowlist function. Once this function is enabled, only IPs in the allowlist are allowed to access your devices. Therefore, you must add the IP address of your PC and IP addresses of supporting devices to the allowlist.

* + 1. Bind with MAC address

You are recommended to bind the IP addresses of gateway devices with the MAC address on the device, to reduce the risk of ARP cheating.

* + 1. Reasonably allocate accounts and permissions

Based on business and management requirements, add users and reasonably assign the minimum set of permissions to them.

* + 1. Disable non-essential services and use the safety mode

You are recommended to disable SNMP, SMTP, and UPnP functions if they are not essential, to reduce the safety threats to your devices.

If necessary, you are strongly recommended to use the safety mode, including but not limited to:

* + - * SNMP: Select SNMP v3 and set up complex encryption passwords and authentication passwords.
      * SMTP: Select TLS method for connection with the email server.
      * FTP: Select SFTP and set up complex passwords.
      * AP hotspot: Select WPA2-PSK encryption mode and set up complex passwords.
    1. Encrypted audio/video transmission

If your audio/video data contains important or sensitive contents, you are recommended to enable encrypted transmission, to reduce the risk of audio/video data being stolen during transmission.

* + 1. Use PoE method for device connection

If the device supports PoE, use this method to establish connection with the device, to isolate the cameras from other networks.

* + 1. Safety audit
       - Check online users: You are recommended to check online users from time to time and check for logins of illegal users.
       - Check device logs: By checking logs, you can get information of IPs that tried to log into your device and information of critical operations of logged-in users.
    2. Cloud log

Due to the limited device storage capacity, logs cannot be stored without limitation. If you want to store logs for a long time, you are recommended to enable the cloud log function, so that critical logs can be synced to the cloud log server for easy tracing of issues.

* + 1. Construction of a safe network environment

To keep the device safer and reduce network security risks, you are recommended to:

* + - * Disable the router port mapping function to avoid direct access through external networks to the services provided by the intranet devices of the router.
      * Based on actual needs, the network can be divided into isolated sub-networks. Two sub-networks with no communication needs to each other can be separated preferably through VLAN or gatekeeper, to achieve the network isolation effect.
      * Establish the 802.1x connection authentication system to reduce the risk of an illegal terminal from being connected with the private network.
      * Enable the firewall or allowlist/blocklist function of the device to reduce the risk of the device being hacked.