Video Door Phone & Access Control Case

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces the appearance, features and cable connection of the Video Door Phone & Access Control Case.

Safety Instructions

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

Signal Words	Meaning
📖 Note	Provides additional information as the emphasis and supplement to the text.
⚠CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.

Revision History

Version	Revision Content	Release Date
V1.0.0	First release.	May 2020

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 jurisdictions. For detailed information, refer to 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, 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 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 occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

The following description is the correct application method of the device. Read the manual carefully before use, in order to prevent danger and property loss. Strictly conform to the manual during application and keep it properly after reading.

Operating Requirements

- Do not place and install the device in an area exposed to direct sunlight or near heat generating device.
- Do not install the device in a humid, dusty or fuliginous area.
- Keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Do not drip or splash liquids onto the device; do not put on the device anything filled with liquids to prevent liquids from flowing into the device.
- Install the device at well-ventilated places; do not block its ventilation opening.
- Use the device only within rated input and output range.
- Do not dismantle the device arbitrarily.
- The device shall be used with screened network cables.

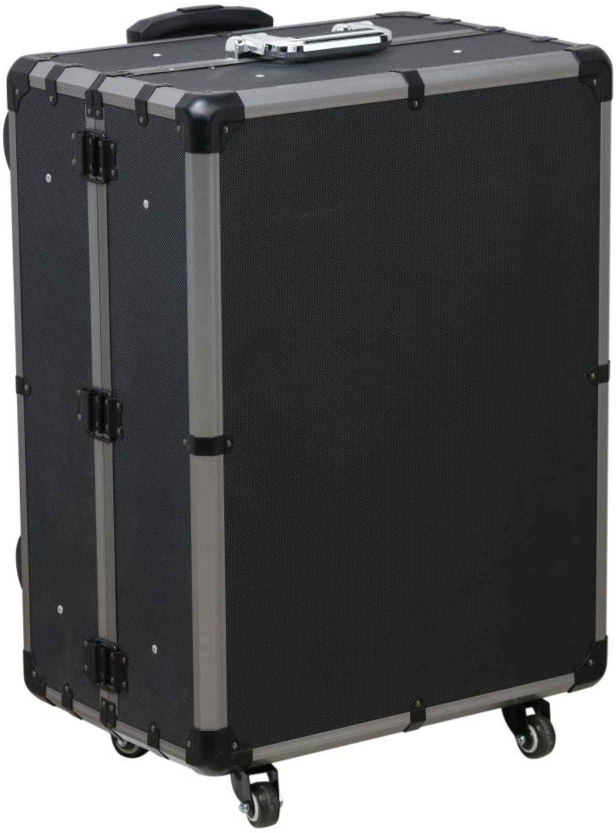
Power Requirements

- Use electric wires (power wires) recommended by this area, which shall be used within its rated specification!
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, refer to device labels.
- Appliance coupler is a disconnecting device. During normal use, keep an angle that facilitates operation.
- Do not cut off power supply during device upgrade. Power supply can be cut off only after the device has completed upgrade and has rebooted.

Table of Contents

1 Appearance

Figure 1-1 Appearance



2 Overview

2.1 Introduction

Video door phone and access control devices can be put in the case, and be connected to the power source. You can carry the case to promote products to clients in solution demonstrations, exhibitions, and more. This case will provide sales persons with great convenience.

2.2 Features

- Suitcase-shaped, portable.
- Made of aluminium alloy; durable frames and corners.
- Multidirectional wheel and braking system.
- Black acrylic surface board makes the suitcase more lustrous.
- Telescopic handle.
- Two handles.

3 Cable Connection

3.1 Cables

Figure 3-1 Patch cord

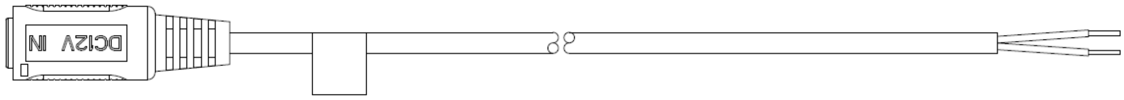
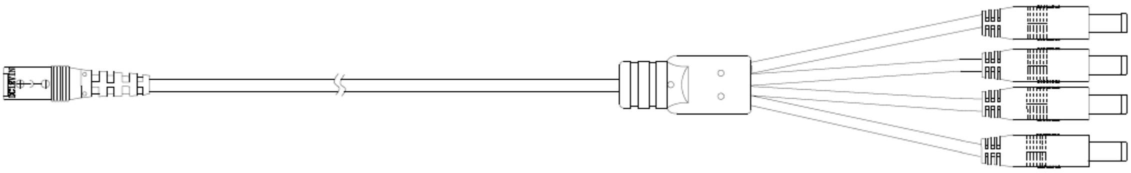


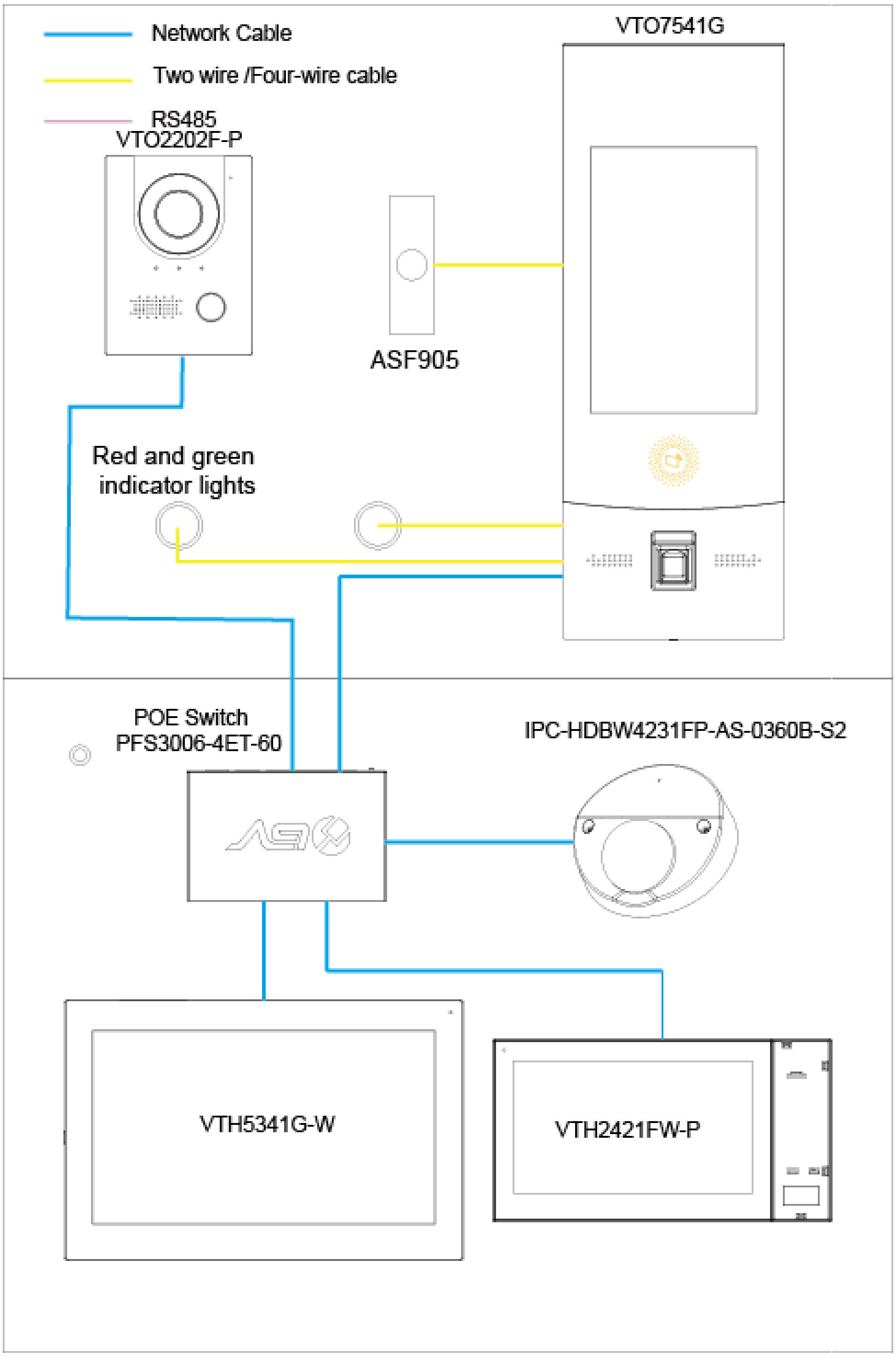
Figure 3-2 4-port power cable



3.2 Video Door Phone Cable Connection

Video Door Phone Cable Connection (1)

Figure 3-3 Video door phone cable connection (1)



If the indicator light is red, it means that the door is locked; if the indicator light is green, it means that the door is unlocked.

Step 1 Connect the first 4-port power cable to the power port on the acrylic board of the lower part of the case.

Step 2 Connect one port of the 4-port power cable mentioned in Step 1 to the IPC-HDBW4231FP-AS-0360B-S2, and then connect another port to the second 4-port power cable (provided with the case) to provide power for the door station VTO7541G.

Step 3 Connect one port of the second 4-port power cable to the patch cord, use the black and red power cable to provide power to the red and green indicator lights, connect the two indicator lights to the VTO7541G door station, and then connect the exit button to VTO7541G by using the black and red power cable.

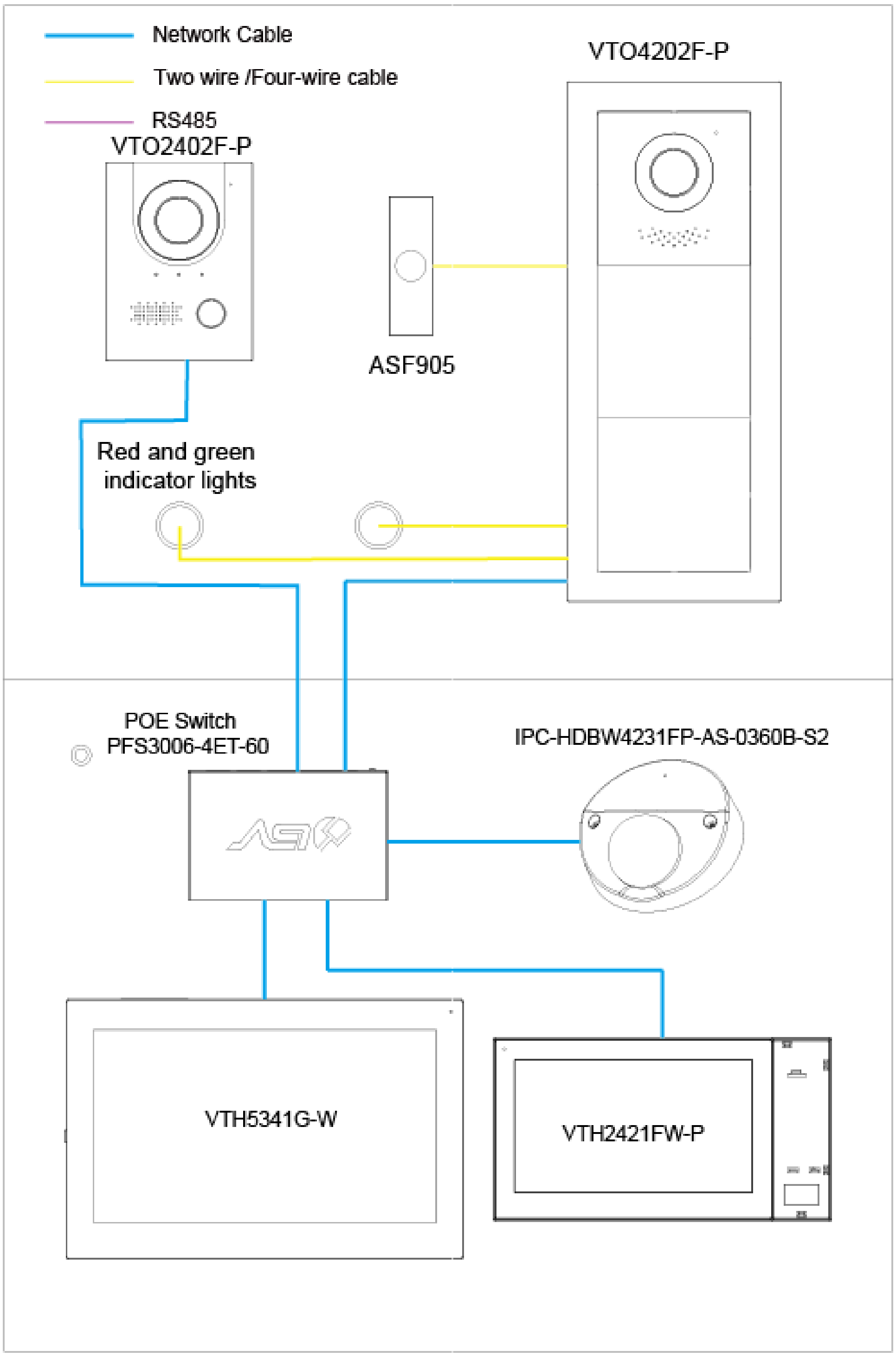
📖

For the cable connection of indicator lights and exit buttons, see the quick start guide of VTO7541G door station.

Step 4 Connect the five network cables to the two indoor monitors, one door station, one villa station, and one IPC.

Video Door Phone Cable Connection (2)

Figure 3-4 Video door phone cable connection (2)



If the indicator light is red, it means that the door is locked; if the indicator light is green, it means that the door is unlocked.

Step 1 Connect the first 4-port power cable to the power port on the acrylic board of the lower part of the case.

Step 2 Connect one port of the 4-port power cable mentioned in Step 1 to IPC-HDBW4231FP-AS-0360B-S2.

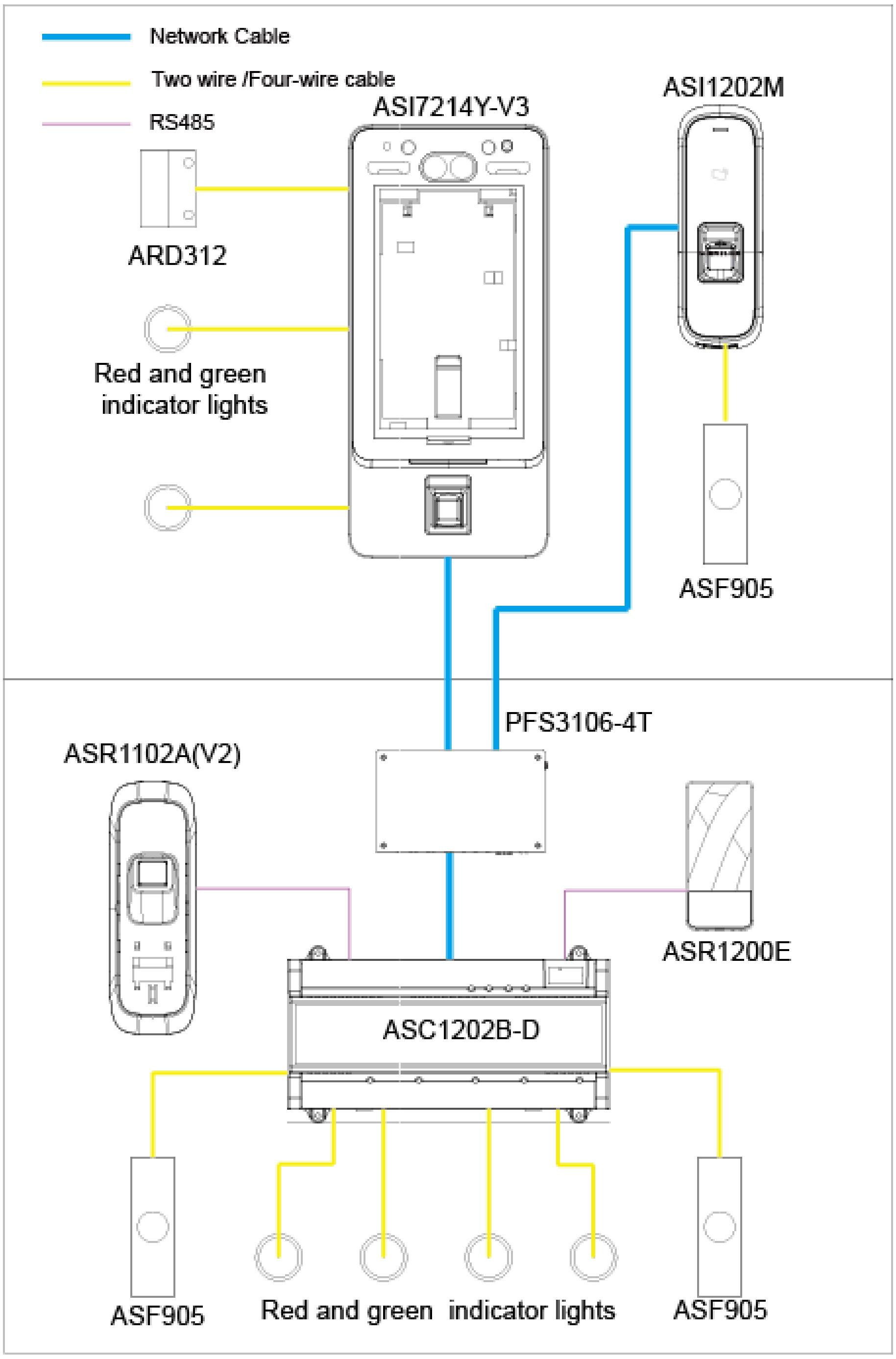
Step 3 Connect another port of the 4-port power cable to the patch cord, use the black and red power cable to provide power to the red and green indicator lights, connect the two indicator lights to the VTO4202F-P door station, and then connect the exit button to VTO4202F-P by using the black and red power cable.

For the cable connection of indicator lights and exit buttons, see quick start guide of VTO4202F-P door station.

Step 4 Connect the five network cables to the two indoor monitors, one door station, one villa station, and one IPC.

3.3 Access Control Device Cable Connection

Figure 3-5 Access control cable connection



📖

If the indicator light is red, it means that the door is locked; if the indicator light is green, it means that the door is unlocked.

Step 1 Connect the first 4-port power cable to the power port on the acrylic board of the lower part of the case.

Step 2 Connect one port of the 4-port power cable mentioned in Step 1 to the second 4-port power cable, and then connect the second 4-port power cable to the ASI7214Y-V3 access controller.

Step 3 Connect the other three ports of the 4-port power cable to the patch cord, use the black and red power cable to provide power for ASI1202M access controller and the red and green indicator lights, and then connect the two indicator lights to the ASI7214Y-V3 access controller.

📖

For indicator light cable connection, see quick start guide of the ASI7214Y-V access controller.

Step 4 Connect access controller of model ASI7214Y-V3, ASI1202M, and ASC1202B-D to the PFS3005-5ET-L switch with the three network cables.

Step 5 Connect the two 4-port power cables to power port on the acrylic board of the lower part of the case, and then use two of the ports to connect access controller ASR1200E and ASR1102A(V2) to the patch cord.

Step 6 Use the other ports, power cords, and black and red power cable to provide power for ASC1202B-D access controller and the four red and green indicator lights, and then connect the four indicator lights to the ASC1202B-D access controller.

📖

For indicator light cable connection, see quick start guide of ASC1202B-D access controller.

Step 7 Connect the RS-485 ports of access controllers of model ASR1200E and ASR1102A(V2) to the RS-485 port of access controller of model ASC1202B-D.

📖

For RS-485 cable connection, see quick start guide of the ASC1202B-D access controller.

Step 8 Connect the two exit buttons of model ASF905 to access controller of model ASC1202B-D with the black and red power cable, and then connect one exit button of model ASF905 to ASI1202M with the black and red power cable.

📖

For the cable connection of exit button of model ASF905, see quick start guide of the ASC1202B-D and ASI1202M.

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.