

Speed Measuring Device

Quick Start Guide



V1.0.0

Foreword

General

This manual introduces the basic information, functions, and operations of the speed measuring device (hereinafter referred to as "the Device"). 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.	September 2024

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.

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



WARNING

- 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 that the ambient voltage is stable and meets the power supply requirements of the Device.
- Do not connect the Device to 2 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 a safety belt.
- 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.
- Please do not touch the photosensitive device with your hands. Use an air blower to clean off the dust and filth on the lens.
- 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.
- Charge the lithium battery with a standard adapter.
- We recommend you pull out the battery after use to avoid excessive battery consumption.

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 Product Information.....	1
2 Structure.....	2
2.1 Dimensions.....	2
2.2 Panel.....	2
3 GUI Operations.....	4
3.1 Introduction.....	4
3.1.1 Login.....	4
3.1.2 Main Interface.....	4
3.2 Live Snapshot.....	4
3.2.1 Live.....	4
3.2.2 Snapshot.....	5
3.3 Image Manager.....	5
3.3.1 Search.....	5
3.3.2 Backup.....	6
3.4 Config.....	6
3.4.1 Intelligent Plan.....	6
3.4.2 AI Settings.....	7
3.4.3 Radar Settings.....	8
3.4.4 Camera.....	10
4 Webpage Operations.....	11
4.1 Initializing the Device.....	11
4.2 Webpage Functions.....	12
Appendix 1 Cybersecurity Recommendations.....	13

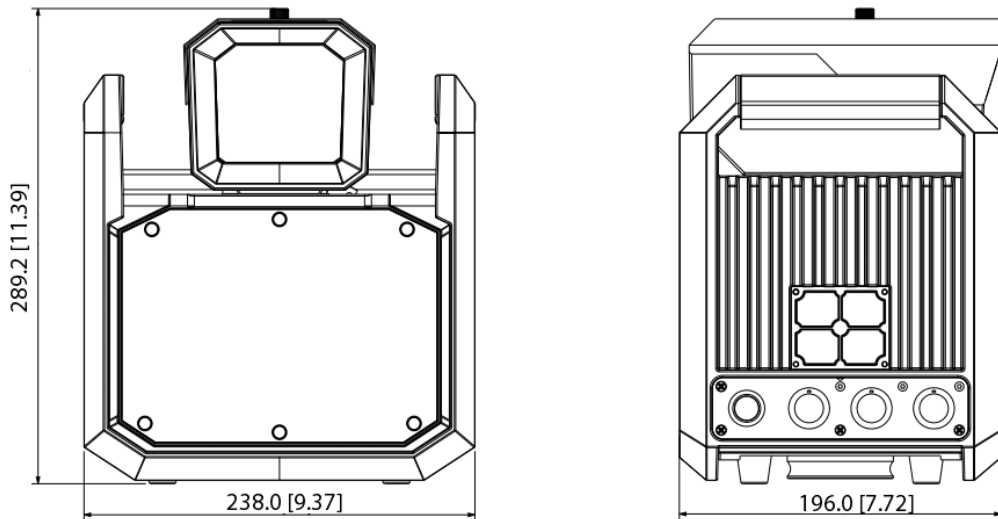
1 Product Information

The Device adopts a fully embedded system with functions such as vehicle speed measurement, image capture, video surveillance, and automatic recognition of license plate number, lane, color, and vehicle model. Compared with traditional radar systems that separate industrial PC and IP camera, the Device combines the company's technical advantages in intelligent traffic field to provide you with stable performance, powerful functions, and ease of installation.

2 Structure

2.1 Dimensions

Figure 2-1 Dimensions (mm [inch])



2.2 Panel

Figure 2-2 Panel



Table 2-1 Port description

No.	Description
1	Power switch
2	24 VDC power input port
3	Ethernet port and USB port
4	RS-232 port and RS-485 port

3 GUI Operations

After you install the Device, you can set parameters on the graphic user interface (GUI) of the Device.

3.1 Introduction

3.1.1 Login

Procedure

Step 1 Start the Device after it is installed and all wires are connected.

The **Login** dialog box appears.

Step 2 In the **Login** dialog box, enter the username and password, and then tap **Enter**.

3.1.2 Main Interface

The main interface of the GUI includes 4 parts: **Live Snapshot**, **Image Manager**, **Config**, and **Manage Info**.

- **Live Snapshot**: You can view real-time video and captured images, rotate the PTZ, and configure the parameters of zoom & focus and image display.
- **Image Manager**: You can search for and back up captured images.
- **Config**: You can configure various parameters of the Device.
- **Manage Info**: You can view system information, manage users, and search for logs and traffic flow data.

3.2 Live Snapshot

3.2.1 Live

Tap **Live Snapshot** on the main interface, and the **Live** tab appears.

Table 3-1 Parameters on the Live tab

Module	Parameter	Description
PTZ	Speed	The speed at which the PTZ moves. Click ◀ or ▶ to make the PTZ horizontally move to the left or right.
Zoom & Focus	Auto Focus	After you tap the icon, the system automatically focuses the camera.
	Area Focus	After you tap the icon and select an area on the video, the system focuses the camera for the selected area.
	Reset	After you tap the icon, the system resets zoom and focus parameters.

Module	Parameter	Description
Image Adjustment	Brightness	The brightness of the image.
	Contrast	The contrast of the image.
	Prevalue	The preset value of brightness.
	Mode	● Color: The image is always colored. ● Auto: When the brightness is higher than the preset value, the image automatically changes to color. When it is below the preset value, the image changes to black and white. ● B/W: The image is always black and white.
	ICR Switch	● Auto: You need to pre-set the brightness in this mode. When the ambient brightness is higher than the preset value, the polarizer will start to work. ● Polarizer: The polarizer is always running. Applicable to scenarios with high brightness. ● IR Mode: Applicable to scenarios with low brightness.

3.2.2 Snapshot

Tap **Live Snapshot** on the main interface, and then tap **Snapshot**. The **Snapshot** tab displays snapshots and related information including date, plate number, vehicle speed, vehicle type, lane number, and the number of snapshots on the current day.



- Tap **Previous** to view the previous snapshot.
- Tap **Next** to view the next snapshot.
- Tap **Snapshot** to take a snapshot.

3.3 Image Manager

3.3.1 Search

Procedure

- Step 1 Tap **Image Manager** on the main interface, and then the **Search** tab appears.
- Step 2 Set filter conditions, including period, image type, lane number, speed range, and plate number.
- Step 3 Select **BlockList** and **Composite Pic** as needed, and then tap **OK**.
The search results are displayed in a list.
- Step 4 Tap a search result, and then the related image and its information are displayed.

3.3.2 Backup

Procedure

- Step 1 Tap **Image Manager** on the main interface, and then tap **Backup**.
- Step 2 Set filter conditions, including period, image type, lane number, speed range, and plate number.
- Step 3 Select **BlockList** and **Composite Pic** as needed, and then tap **OK**.
- The images that meet the filter conditions are backed up.

3.4 Config

3.4.1 Intelligent Plan

3.4.1.1 ANPR

Procedure

- Step 1 Select **Config** > **Intelligent Plan** > **ANPR**.
- Step 2 Configure the parameters.

Table 3-2 Description of ANPR parameters

Parameter	Description
ANPR Enable	Specifies whether to enable the ANPR mode.
Snap Mosaic	Specifies whether to enable image mosaic.
IFS	The frame interval of capturing 2 images.

- Step 3 Enable traffic rules for different lanes, and then tap **Save**.

3.4.1.2 E-police

Procedure

- Step 1 Select **Config** > **Intelligent Plan** > **E-police**.
- Step 2 Configure the parameters.

Table 3-3 Description of E-police parameters

Parameter	Description
E-police Enable	Specifies whether to enable E-police mode.
Snap Mosaic	Specifeis whether to enable image mosaic.
Signal Detector	Select Net Version to enable the light connected through the network.

- Step 3 Enable rules for different lanes, and then tap **OK**.

3.4.2 AI Settings

3.4.2.1 Scene Config

Procedure

- Step 1** Select **Config** > **AI Settings** > **Scene Config**.
- Step 2** Select a lane for which you want to draw lines or regions.
- Tap **Lane Line**, and then draw a lane line.
 - Tap **Detect Line**, and then draw a detection line.
 - Tap **Region**, and then draw a region.
 - Tap  to delete the lines or regions you have drawn.
- Step 3** Tap **Save**.

3.4.2.2 Recognition

Procedure

- Step 1** Select **Config** > **AI Settings** > **Recognition**.
- Step 2** Configure the parameters.

Figure 3-1 Recognition

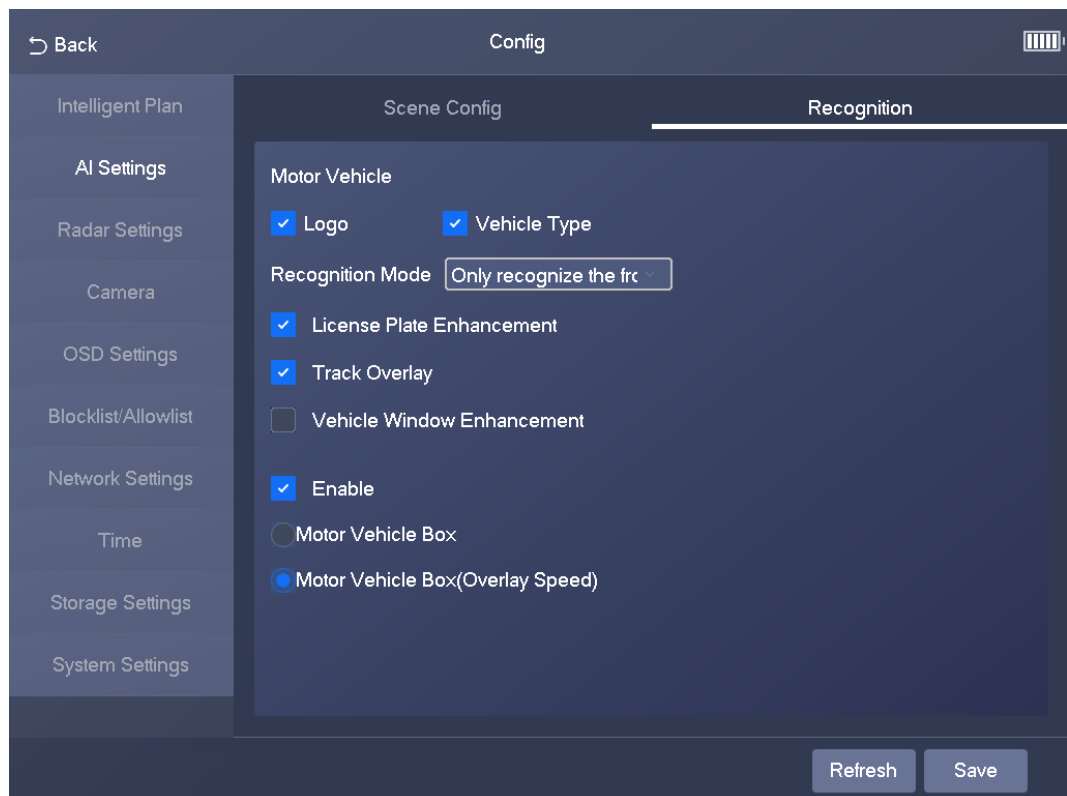


Table 3-4 Description of recognition parameters

Parameter	Description
Motor Vehicle	Supports recognizing vehicle logs and vehicle types.

Parameter	Description
License Plate Enhancement	Select the checkbox to enhance the effect of license plate images.
Vehicle Window Enhancement	Select the checkbox to enhance the effect of vehicle window images.
Track Overlay	Select the checkbox to enable Track Overlay .
Recognition Mode	● Only recognize the front plate : Recognizes and captures the license plate on the vehicle head. ● Only recognize the rear plate : Recognizes and captures the license plate on the vehicle rear. ● Front plate priority : Head plate has the priority. ● Rear plate priority : Rear plate has the priority.

3.4.3 Radar Settings

3.4.3.1 Parameters

Procedure

Step 1 Select **Config** > **Radar Settings** > **Parameters**.

Figure 3-2 Parameters

Back Config

Intelligent Plan

AI Settings

Radar Settings

Camera

OSD Settings

Blocklist/Allowlist

Network Settings

Time

Storage Settings

System Settings

Parameters Radar Visualization Radar Calibrate

Lane Config

Lane No.	Width	Detection Direction
1	380 cm(200~500)	Approaching
2	380 cm(200~500)	Approaching
3	380 cm(200~500)	Approaching
4	380 cm(200~500)	Approaching

Radar Setting Lane 1 Max Speed 255 km/h(0~255)

InstalHeight 160 cm(0~1000) Sensitivity 5 (0~30) Working Mode Work Mod

For Size Highest Speed Limit 70 km/h(0~255) + 0 km/h(0~255)

Lowest Speed Limit 20 km/h(0~255) - 10 km/h(0~255)

Default Refresh Save

Step 2 Configure the parameters.

Table 3-5 Description of radar parameters

Parameter	Description
Width	The width of the lane.
Detection Direction	The driving direction that triggers detection.
Max Speed	The maximum vehicle speed that can be recognized by the radar.
InstallHeight	The installation height of the Device.
Working Mode	● Work Mode : Use this mode in actual situation. ● Soak Mode : Use this mode for product certification.
For Size	After you select the checkbox, the Device can distinguish large vehicles from small vehicles.
Highest Speed Limit	The allowed highest vehicle speed. If a vehicle runs over the highest speed, the vehicle is overspeed.
Lowest Speed Limit	The lowest vehicle speed. If a vehicle runs below the lowest speed, the vehicle is underspeed.

Step 3 Tap **Save**.

3.4.3.2 Radar Visualization

Background Information

On the **Radar Visualization** tab, you can view the effect of radar detection in real time and modify some of the radar parameters.

Procedure

Step 1 Select **Config** > **Radar Settings** > **Radar Visualization**.

Step 2 Adjust the value of angle correction and horizontal offset.

Step 3 Tap **Save**.

3.4.3.3 Radar Calibration

Background Information

Make sure that the camera can capture right targets when the radar sends signals to the camera.



Radar calibration on the GUI is similar to that on the webpage.

Procedure

Step 1 Select **Config** > **Radar Settings** > **Radar Calibrate**.

Step 2 Set **Area Width** to the width of the actual road.

After you set the width of the calibration area to the width of the actual road, the algorithm will automatically calibrate the radar.

Step 3 Tap **Save**.

3.4.4 Camera

3.4.4.1 Shutter

Background Information

You can configure shutter mode, exposure mode, and gain mode.

Procedure

Step 1 Select **Config** > **Camera** > **Shutter**.

Step 2 Configure the parameters.

Shutter parameters on the GUI are similar to those on the webpage.

Step 3 Tap **Save**.

3.4.4.2 Flashing Light Config

Background Information

You can configure the work mode of the flashing lights and strobes connected to the Device.

Procedure

Step 1 Select **Config** > **Camera** > **Flashing Light Config**.

Step 2 Configure the parameters.

Flashing light parameters on the GUI are similar to those on the webpage.

Step 3 Tap **Save**.

4 Webpage Operations

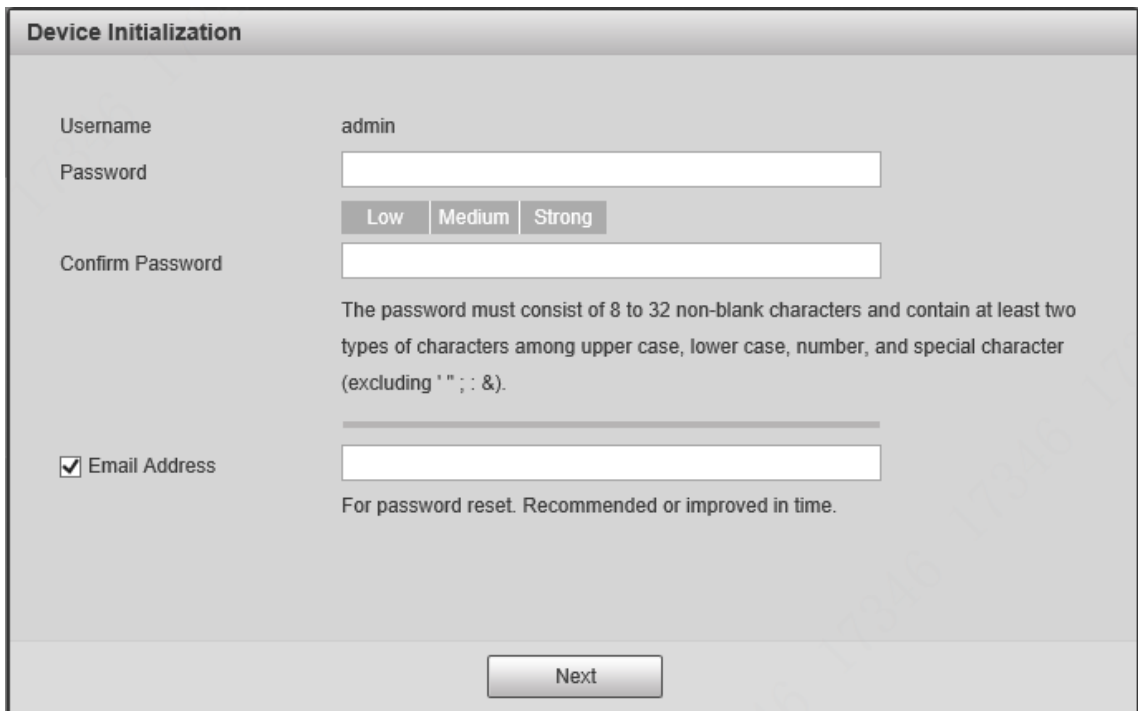
4.1 Initializing the Device

The Device is delivered in the uninitialized state. You must initialize the Device before you can use it.

Procedure

- Step 1** Use ping X.X.X.X (IP address of the Device) command to check whether the network is connected.
- Step 2** Open a browser, enter the IP address of the Device in the address bar, and then press the Enter key.
- 
- Make sure that the IP address of the PC and that of the Device are on the same network segment.
- Step 3** In the **Device Initialization** dialog box, enter your new password.
- Step 4** Select **Email Address**, and then enter your email address. This helps you reset your password when you forgot your password.
- Step 5** Click **Next**.

Figure 4-1 Device initialization



Device Initialization

Username admin

Password

Low Medium Strong

Confirm Password

The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' ' ; : &).

☒ Email Address

For password reset. Recommended or improved in time.

Next

- Step 6** In the **Online Upgrade** dialog box, select **Auto-check for updates** and click **Confirm**.
- Step 7** In the **Configuration Wizard** dialog box, set the parameters as needed, and then click **Next Frame**.
- Step 8** Set **IP Address**, **Subnet Mask**, and **Default Gateway**, and then click **Complete**.
- Step 9** For first-time login, click **Please click here to download and install the plug-in**, and then install the plug-in.

4.2 Webpage Functions

Figure 4-2 Top navigation bar



Table 4-1 Webpage functions

Function	Description
Live	You can view real-time video and image, record videos and capture images, and configure video play and image settings.
Radar	You can configure radar settings and debug detection results in a visualized manner.
Search	You can search for vehicles and recorded videos.
Setting	You can configure intelligent traffic rules, basic information of the Device, network settings, event management, storage management, and system management.
Alarm	You can configure how the Device responds when alarms occur.
Logout	Log out of the webpage.

Appendix 1 Cybersecurity Recommendations

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.