

All-in-one AI Traffic Camera

Quick Start Guide



V1.0.0

Foreword

General

This manual introduces the installation, functions and operations of the All-in-one AI Traffic Camera (hereinafter referred to as "the Camera"). Read carefully before using the Camera, 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 electrical 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.



- 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.
- Please follow the electrical requirements to power the device.
 - ◇ Following are the requirements for selecting a power adapter.
 - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
 - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
 - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
 - ◇ We recommend using the power adapter provided with the device.

- ◇ When selecting the power adapter, the power supply requirements (such as rated voltage) 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.
- Operating temperature: -40°C to $+65^{\circ}\text{C}$ (-32°F to $+149^{\circ}\text{F}$).
- The rated current of the device is 3 A and the rated power is 20 W.
- An emergency disconnect device must be installed during installation and wiring at a readily accessible location for emergency power cut-off.
- Disconnect the device when installing and connecting the lens.
- Only applicable for use in altitudes below 2,000 meters.

Operation Requirements



WARNING

- Eye or skin irritation may result from exposure to the embedded illuminator. Use appropriate shielding during operation.
- Do not stare at the illuminator during operation to avoid the risk of harming to the eyes.
- Operating the device in a domestic environment may cause radio interference.



- Make sure that 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.
- Do not aim the device at strong light sources (such as lamplight, and sunlight) when focusing it.
- Do not vibrate, squeeze or immerse the device in liquid during transportation, storage or installation.
- Do not block the ventilation near the device.
- 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 (grounding cable or lightning surge protector) 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.
- The device must be used with the protective cover for outdoor scenarios to avoid the risk of water damage to the device.
- 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.
- Modify the default password of the device after first-time login to prevent the device from being stolen.

Maintenance Requirements

- Pack the device with packaging provided by its manufacturer or packaging of the same quality before sending it back for repair.
- Please do not touch the photosensitive device with your hands. Use an air blower to clean off the dust and filth on the lens.

- Clean the surface of 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 Introduction.....	1
2 Structure.....	2
3 Quick Configuration.....	3
3.1 Initializing the Camera.....	3
3.2 Changing IP Address.....	4
3.3 Upgrading the Camera	5
3.4 Login.....	5
3.5 Resetting Password.....	6
4 Web Client Operations.....	7
4.1 Configuring Illegal Capture.....	7
4.1.1 Lane Parameters.....	7
4.1.2 Car Detect.....	8
4.1.3 Rule Configuration.....	8
4.2 Radar Configuration.....	8
4.2.1 Configuring Radar Visualization.....	8
4.2.2 Calibrating by Radar & Video.....	9
4.3 Image Search.....	9
4.3.1 Searching for SD Card Image.....	9
4.3.2 Setting Downloading Attribute.....	10
4.3.3 PC Picture.....	10
Appendix 1 Reference for Filling in Allowlist and Blocklist Template.....	11
Appendix 2 Cybersecurity Recommendations.....	14

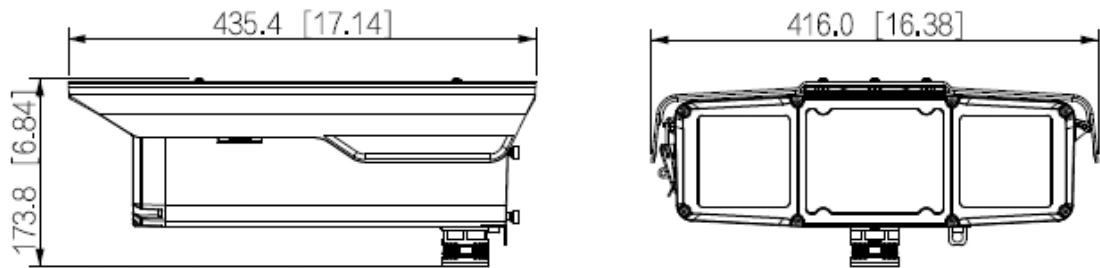
1 Product Introduction

With its high-performance AI processor, All-in-one AI Traffic Camera delivers excellent quality images even in the toughest weather conditions. For monitoring, it uses deep learning algorithms and traffic-specific, GS-CMOS image sensors with a wide dynamic range and high frame rate.

The Camera is ideal for use in intelligent traffic management and for smart city businesses. It is capable of detecting traffic violations, capturing license plates, generating passing vehicle records, collecting traffic data, and detecting events.

2 Structure

Figure 2-1 Dimensions (mm [inch])



3 Quick Configuration

You can use the ConfigTool to quickly configure the Camera, including initialization, system update and web client login.



- The operation pages vary depending on different versions.
- Get the ConfigTool installation package from technical support and install it on your local computer.

3.1 Initializing the Camera

Background Information

You can initialize the Camera, and cameras connected to the Camera in batches through the ConfigTool.



Uninitialized devices are not available for any operations and are displayed in gray on the Camera list.

Procedure

- Step 1 Start the ConfigTool, and then click **Modify IP**.
The ConfigTool automatically searches for devices on the same network segment with the computer.
- Step 2 Select a device to be initialized, and then click **Initialize**.

Figure 3-1 Device initialization

Device initialization

1 device(s) have not been initialized

Username admin

New Password

Weak Medium Strong

Confirm Password

Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them. (excluding Single quote('), double quote("), colon(:), semicolon(;), connection symbol(&))

☒ Email Address 1****6@gmail.comR (for password reset)

Select P/N PAL

*After you have set new password, please set password again in "Search Setting".

Next

Step 3 Set and confirm the password, and enter an email for future password reset.



The pages are for reference only, and might differ from the actual page.

Step 4 Click **Initialize**, and the system starts initializing the Camera.



is displayed for successful initialization, and  is displayed for initialization failure. Click the icon to view details.

Step 5 Click **Finish**.

3.2 Changing IP Address

Background Information

You can acquire and change the IP address of devices accessed through wired network. This section uses changing IP address with the ConfigTool as the example.

Procedure

Step 1 Start the ConfigTool.

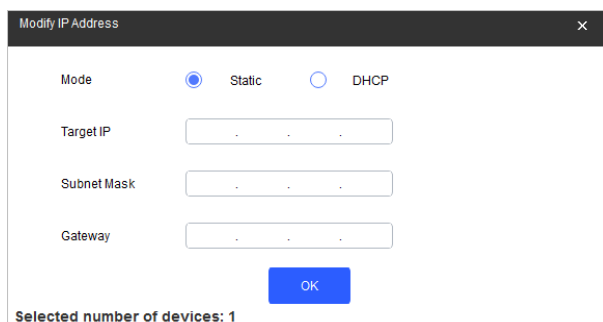
Step 2 Click **Modify IP**.

Step 3 Select the device(s) whose IP need(s) to be changed.

- Change one IP address: Click **Edit** corresponding to the device.
- Change IP addresses in batches: Select the devices, and then click **Batch Modify IP**.

- Step 4 Set mode, IP, subnet mask and gateway.
- Step 5 Click **Confirm**.

Figure 3-2 Change IP addresses in batches



3.3 Upgrading the Camera

Background Information

Single upgrade and batch upgrade are supported.

Procedure

- Step 1 Start the ConfigTool.
- Step 2 Click **Device Upgrade**.
- Step 3 Select the Camera to be updated.
- Update one by one: Click  corresponding to the Camera.
 - Update in batches: Select multiple devices, and then click **Batch Upgrade**.
- Step 4 Select the update file.
- Step 5 Update the Camera.
- Update one by one: Click  to start updating.
 - Update in batches: Click **OK** to start updating.



During update, if the Camera is disconnected, as long as the ConfigTool stays on the update page, the upgrade will continue when the Camera is reconnected.

3.4 Login

Background Information



- For first-time login or login after the Camera is restored to factory defaults, initialization is required.
- Make sure that the IP address of the computer and that of the Camera are on the same network segment. Otherwise, the initialization might fail.

Procedure

- Step 1 Open the browser and enter the IP address of the Camera, and then press the Enter key.
- Step 2 Enter and confirm the password.



Change the password from **Setting > System > Account > Account > Username**.

Step 3 Select **Email Address**, and then enter an email address.

The email address is used for resetting password.

Step 4 Click **Confirm**.

Step 5 Enter **Username** and **Password** on the login window, and then click **Login**.



The account will be locked for five minutes after five failed username or password attempts.

Step 6 On the **Live** page, click **Please click here to download and install the plug-in** to download and install the plug-in.

The **Live** page is normally displayed.

3.5 Resetting Password

Background Information

When you forget the password, you can set a new password.



- You need to enter an email address during device initialization to receive the security code. Otherwise, password reset is not available. You can also change the email address from **Setting > System > Account > Account > Username**.
- The password of a device can only be reset up to 10 times a day.
- You can only get two security codes for each QR code.
- Use the security code to reset the password within 24 hours after you receive it. Otherwise the security code will become invalid.

Procedure

Step 1 Open the browser and enter the IP address of the Camera, and then press Enter.

Step 2 Click **Forgot password?** on the login page, and then click **OK** in the pop-up window.



If Internet Explorer is used, **Stop running this script** is displayed. In this case, click **No** to continue to run the script.

Step 3 Scan the QR code, and the scan result will be sent to the reserved email.

Step 4 Send the received scan result to support_gpwd@htmicrochip.com through the reserved email address to get the security code.

Step 5 Enter the security code, and then click **Next**.

Step 6 Enter and confirm the new password.



Follow the password security prompt to set a password with a high security level.

Step 7 Click **OK**.

4 Web Client Operations

You can access and manage connected devices, such as cameras and radars through the web client of the Camera.



The web pages displayed in this section are for reference only, and might differ from the actual model.

4.1 Configuring Illegal Capture

Configure the video detection parameters for detecting traffic violations.



Click to select a lane on the list in the **Lane Config** section, and then all configurations on the **Illegal Capture** page are for this lane.

4.1.1 Lane Parameters

Background Information

Configure the information of the lanes the Camera is monitoring, such as drawing the lane lines on the image, select the lane direction and set the lane line type according to the actual situation.

Procedure

Step 1 Select **Setting > Event > ANPR Snap > Illegal Capture**.

Step 2 In the **Lane Config** section, configure the lane lines.

- If the default lane lines on the image do not meet the actual detection requirements, you can draw new lane lines.

1. Select a lane from the list, and then delete the lines by clicking .



You can also click  next to **LaneLine /Detect Line/Channelization Lane Line** to delete the corresponding lines on the image.

2. Click **LaneLine /Detect Line/Channelization Lane Line**, and then draw lines on the image.



Install the plug-in and then click **Auto Drawing**, the Camera draws the lane lines automatically.

- If the default lane lines can be adjusted to match the actual lane lines, you can adjust them.
 1. Select **Graphic Adjustment** to enable lane line adjustment, and then select a lane from the list.
 2. Drag to adjust the lane lines and detection lines according to the actual situation.

Step 3 For the selected lane, select **Lane Direction**.

The direction of the lane line on the image needs to be the same as that of the travelling vehicle.

Step 4 Double-click the selected lane on the list under **Left Lane Line Type**, **Right Lane Line Type** and **CarWay Type** to change the lane lines and lane type as needed.

Step 5 Click **Confirm**.

4.1.2 Car Detect

Background Information

Draw the regions for vehicle detection on the image.

Procedure

Step 1 Select **Setting > Event > ANPR Snap > Illegal Capture**.

Step 2 In the **Car Detect** section, click a line or region type, and then draw on the video image.

- To draw a line, click the line type and then draw on the image.
- To draw a region, click the region type, and then click on the image to set the four points of the region.



To clear the lines that you have drawn, click .

Table 4-1 Car detect description (1)

Parameter	Description
Region	The region of detection.
Car Region	The region for detecting vehicle volume.
Line segment measurement	Used to verify the accuracy of calibration results. Click Line segment measurement to draw the calibration segment in the calibration area, enter the actual length of the calibration segment in the pop-up page, and then click Calibration Validation .

Step 3 Click **Confirm**.

4.1.3 Rule Configuration

You can select the traffic violation types and configure the corresponding parameters of the snapshot, trigger source, and flashing light as needed.

4.2 Radar Configuration

Configure the radar to accurately capture events during bad weathers and poor light conditions.

4.2.1 Configuring Radar Visualization

Background Information

See the effect of your configurations on radar detection in real time. You can also adjust some of the radar parameters and view the changes.

Procedure

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

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

Click the image at the lower-right corner to see the correction standards.

Step 3 Click   to display **Target Trajectory**.
You can see the trajectory of targets the radar detects.

Step 4 Click , you can see the detection points of the radar on targets.



When the target is large and the detection sensitivity is set high, the radar might recognize it as two targets.

4.2.2 Calibrating by Radar & Video

Background Information

Calibrate the radar. Make sure when the radar sends signals to the camera, the camera can capture the right target.

Procedure

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

Step 2 Click **Calibrate by Radar & Video**.

Step 3 Select a channel on the prompted page, and then select the **Splicing Calibration** checkbox.

You can also calibrate the radar manually without enabling splicing calibration. In this case, you need to manually measure the distance between the drawn calibration area and the Camera.

Step 4 Calibrate the radar calibration mode.

1. Select **Manual** next to **Calibration Mode**, and then adjust the calibration frame on the image based on the on-site measurement.

You can also click , and then click **Calibration Area** to draw an area on the image.

2. Set the coordinates of the calibration area.

3. In the **Snapshot Setting** section, click **Snapshot Triggering Line**, and then draw the lines on each lane.

The distance between the triggering line and the Camera is displayed on the bottom.

4. Adjust the triggering distance as needed, and then click **Confirm**.

5. Click **Calibrate**, and then click **Confirm**.

Step 5 Click **Back**.

4.3 Image Search

4.3.1 Searching for SD Card Image

Background Information

On the **SD Card Image** page, you can search for and download the images stored in the TF card of the Camera.



Make sure the TF card is inserted into the Camera; otherwise, there might be no results.

Procedure

Step 1 Select **Query** > **Image Search** > **SD Card Image**.

Step 2 Configure the parameters, and then click **Search**.

- Step 3 Select the images that you need, and click **Open** to view the images in photo viewer.
- Step 4 Select the images that you want to download, and then click **Download**.
- Step 5 Select the path to save the images, and the system starts downloading the images to your computer.

4.3.2 Setting Downloading Attribute

Background Information

You can configure the image information.

Procedure

- Step 1 Select **Query > Image Search > Downloading Attribute**.
- Step 2 Set **Download Snapshot by** to download snapshots based on their **Creation Time** or **Capture Time**.
- Step 3 Select **Download Mode**.
- **Selected File** : Download the selected snapshots.
 - **Selected Time** : Download all images captured during the set time period. You can set the time in the **SD Card Image** tab.
- Step 4 Select cutouts that you want to download from **All , Plate Cutout, Binarized Plate, Assistant Driver Face** (cutout of front-seat passenger's face), **Driver Face**, and **Vehicle Body Matting**.
- Step 5 Name the snapshots. Click **Help...** to view the image naming rule. Click **Restore** to go back to default.
- Step 6 Click **Confirm**.

4.3.3 PC Picture

Background Information

You can view images saved on your computer and verify whether the image was tampered with a watermark.



To view or set the save path of images on your computer, go to **Setting > Storage > Destination > Save Path**.

Procedure

- Step 1 Select **Query > Image Search > PC Picture**.
- Step 2 Click **Browse** to select a picture.
- Step 3 Click **Watermark** , and view result under **Watermark Verification**.
- When the result is **Error**, the picture is tampered.
 - When the result is **Normal**, the picture is not tampered.



Click **Open** or double-click the picture if you need to preview the picture.

Appendix 1 Reference for Filling in Allowlist and Blocklist Template

Appendix Table 1-1 Plate color number

Plate Color	Plate Color No.
Yellow Plate with Black Text	1
Blue Plate with White Text	2
Black Plate with White Text	3
White Plate with Black Text	4
Black	5
Blue	6
Cyan	7
Red	8
Gradient Green	9
White	10
Yellow and Green	11
Yellow	12

Appendix Table 1-2 Vehicle color number

Vehicle Color	Vehicle Color No.
White	A
Black	B
Red	C
Yellow	D
Gray	E
Green	F
Blue	G
Pink	H
Purple	I
Brown	J
Yellow Green	K
Cyan	L
Dark Blue	M
Dark Brown	N
Dark Cyan	O
Dark Golden	P

Vehicle Color	Vehicle Color No.
Dark Green	Q
Dark Olive	R
Dark Orange	S
Dark Pink	T
Dark Purple	U
Dark Red	V
Dull Purple	W
Dark Yellow	X
Deep Sky Blue	Y
Others	Z
Dark Gray	a
Forest Green	b
Golden	c
Green Yellow	d
Chestnut	e
Light Rosy	f
Olive	g
Orange	h
Ocean Green	i
Silver Gray	j
Tomato Red	k
White Smoke	l

Appendix Table 1-3Vehicle type number

Vehicle Type	Vehicle Type No.
Large Vehicle	1
Small Vehicle	2
Tractor	14
Bus	23
Heavy Truck	24
MPV	25
Light Truck	26
Van	27
Medium Bus	28
Medium Truck	29
Minicar	30

Vehicle Type	Vehicle Type No.
Two-wheeled Vehicle	31
Tank Truck	32
Public Bus	33
Pickup	34
SUV	35
Sedan	36
SUV-MPV	37
Taxi	38
Tricycle	39
Unknown	40
Ambulance	41
Mixer Truck	42
Construction Truck	43
Fire Truck	44
General	45
Engineering Truck	46
Fuel Tank Truck	47
Police Car	48
Pulverized Material Vehicle	49
Tank Truck	50
Sewage Suction Truck	51
Hazardous Chemicals Truck	52
Sanitation Truck	53

Appendix 2 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.