Web 5.0 network camera

Operation Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

V1.0.0

Foreword

General

This manual covers the functions, configuration, general operation and maintenance of the network camera system.

Security instructions

The following classified signal words with a defined meaning may appear in the manual.

Signal words	Meaning
⚠ WARNING	Indicates a medium or low potential risk which, if not avoided, could result in minor or moderate injury.
⚠ CAUTION	Indicates a potential hazard that, if not avoided, could result in property damage, loss of data, poor performance, or other unpredictable results.
🔑 TIPS	Provides methods to help you solve a problem or save time.
📖 USE	Provides additional information as emphasis or complement to the text.

Revision history

Version	Review content	Release date
V1.0.0	First launch.	October 2020

About the manual

- The manual is just a reference. If you detect any discrepancy between the manual and the actual product, the actual product shall prevail.
- We will not accept any responsibility for any losses caused by the use of the device without following the instructions in the manual.
- The manual will be updated in accordance with the latest laws and regulations of related jurisdictions. For more information, please refer to the printed manual, CD-ROM, QR code or our official website. If there is a discrepancy between the printed manual and the electronic version, the electronic version will prevail.
- All designs and software contained herein are subject to change without prior notice by written. Product updates may cause discrepancies between the actual product and the manual. Contact customer service requesting the updated program and supplemental documentation.
- There may still be some deviations in technical data, functions and description of operations, or printing errors. If there is any doubt or controversy, we reserve the right to final explanation.
- Please update the reader software or try other conventional reader software in case of that you cannot open the manual (in PDF format).

- All trademarks, registered trademarks and company names in the manual are the property of their respective owners.
- Please visit our website, contact your seller or customer service if you have problems using the device.
- If there are uncertainties or disputes, we reserve the right to final explanation.

Important Safety Warnings and Precautions

Electrical safety

- All instructions for use and installation must be carried out in accordance with the standards of electrical safety of your country.
- The power supply must comply with the Safety Low Voltage (SELV) standard and supply power with a nominal voltage that meets the limited power supply requirement in accordance with IEC60950-1. Power supply requirements are indicated on the device label.
- Make sure the power supply is suitable before using the device.
- It is necessary to incorporate an easily accessible disconnect device in the wiring of the building installation.
- Prevent the power cord from being pinched or pinched, especially in the connector, the power outlet and at the junction point that comes out of the device.

Operating environment

- Do not point the device directly at strong light when focusing, like the light of a lamp and sunlight; Otherwise, it may cause excessive glare or light marks, which will not be caused by device malfunction, and may affect the life of the complementary metal oxide semiconductor (CMOS).
- Do not place the device in a humid, dusty, extremely hot or cold environment, or in places with strong electromagnetic radiation or unstable lighting.
- Keep the device away from any liquid to prevent damage to the internal components.
- Keep the indoor device away from rain or moisture to avoid fire or good heavens.
- Maintain good ventilation to avoid heat buildup.
- Transport, use and store the device within the permitted limits of humidity and temperature.
- Do not subject the unit to high pressure, strong vibration or splashing water during transportation, storage and installation.
- When transporting the device, keep it in the factory packaging or use equivalent materials.
- Install the device in a location that can only be accessed by professional personnel with appropriate knowledge of safety protections and warnings. Otherwise, injury may occur to non-professionals entering the installation area when the device is operating normally.

Daily use and maintenance

- Do not touch the heat dissipation component of the device to avoid burns.

- Carefully follow the instructions in the manual when performing any disassembly operations on the device; Otherwise, it may cause water leakage or poor image quality due to unprofessional disassembly. Please contact after-sales service to replace the desiccant if there is condensed fog on the lens after taking the product out of the box or if the desiccant turns green. (Not all models include desiccant).

- It is advisable to use the device together with a lightning rod, to improve the lightning effect. lightning protection.
- It is recommended to ground the device to improve reliability.
- Do not touch the image sensor (CMOS) directly. Dust and dirt can removed with an air blower, or you can wipe the lens gently with a soft cloth moistened with alcohol.

- You can clean the device case with a soft, dry cloth, and for stains more complicated, use the cloth with a mild detergent. To avoid possible damage to the coating of the device's case that could result in decreased performance, do not use volatile solvents such as alcohol, benzene, turpentine, etc., to clean the device's case, nor can you use a strong, abrasive detergent. .

- The domed cover is an optical component. Do not touch or clean the cover with hands directly during installation or operation. To remove dust, grease, or fingerprints, wipe gently with an oil-free cotton swab moistened with diethyl or a soft, damp cloth. You can also remove dust with an air blower.

⚠ **WARNING**

- Strengthen protection of network, device data and personal information by taking measures including, but not limited to, using strong passwords, changing passwords regularly, updating firmware to the latest version, and isolating the computer network. For some devices with old firmware versions, the ONVIF password will not be changed automatically along with the system password change, and you will need to update the firmware or update

  manually enter the ONVIF password.
- Please use components or accessories supplied by the manufacturer and ensure that professional engineers carry out the installation and maintenance of the device.
- The surface of the image sensor should not be exposed to laser beam radiation in an environment where a laser beam device is used.
- Do not provide two or more power supplies for the device unless otherwise specified. Failure to follow these instructions could damage the device.

Index of contents

1 Overview

1.1 Introduction

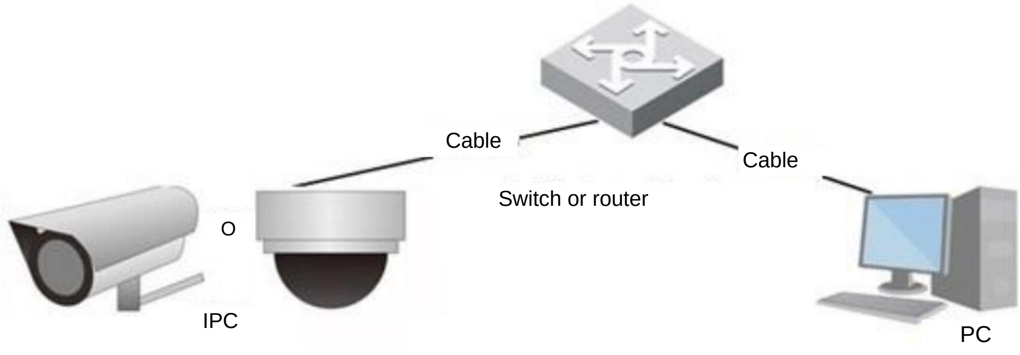
An IP camera (Internet Protocol Camera) is a type of digital video camera that receives control data and sends image data over the Internet. They are commonly used for surveillance and do not require a local recording device, but rather only a local area network.

IP camera is divided into single-channel camera and multi-channel camera according to the number of channels. For multi-channel camera, you can set parameters for each channel.

1.2 Network connection

In the general IP Camera (IPC) network topology, the IPC connects to the PC through a network switch or router.

Figure 1:1 General IPC network



Get the IP address by searching ConfigTool and then you can start accessing the IPC over the network.

1.3 Configuration flow

For more information, see Figure 1:2. For details, see Table 1:1.

Please configure the device according to the actual situation.

Figure 1:2 configuration flow

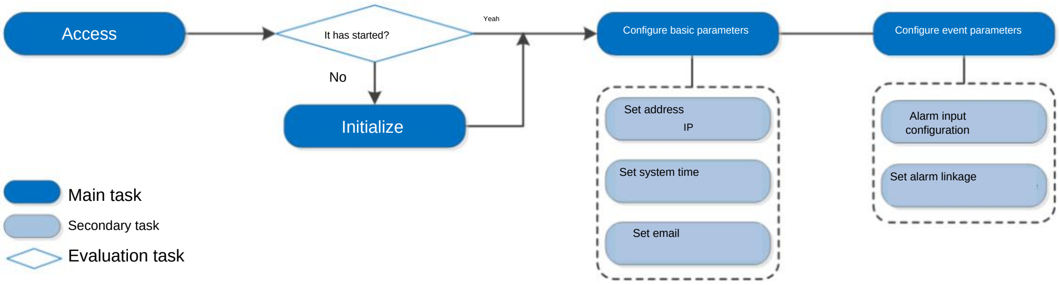


Table 1:1 flow description

Setting		Description	Reference
Access		Open IE browser and enter the IP address to log in to the web interface. The IP address of the camera is 192.168.1.108 by default.	"3 Access".
Initialization		Please start the camera when you use it for the first time.	"2 Device initialization"
Parameters basic	IP adress	Change the IP address according to network planning when using the product for the first time or during network setup.	"5.1.1 TCP/IP"
	Date and Time	Set the date and time to ensure the recording time is correct.	"5.3.1.2 Date and time"

2 Device initialization

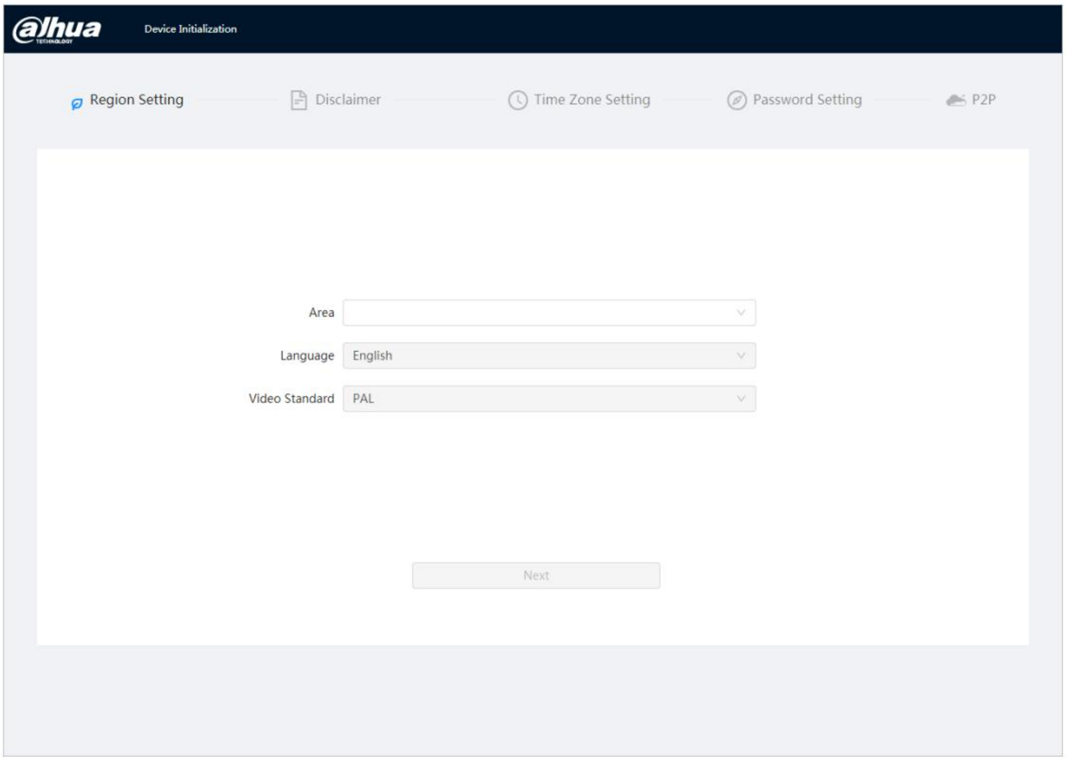
It is necessary to start the device for the first use. This manual is based on the operation of the web interface. You can also boot the device via ConfigTool or NVR.

- To ensure the security of the device, please keep the password correctly after startup and change it regularly.
- When starting the device, keep the PC IP and the device IP on the same network.

Step 1: Open Chrome browser, enter the device's IP address in the address bar, and then press the Enter key.

The IP is 192.168.1.108 by default.

Figure 2:1 region configuration



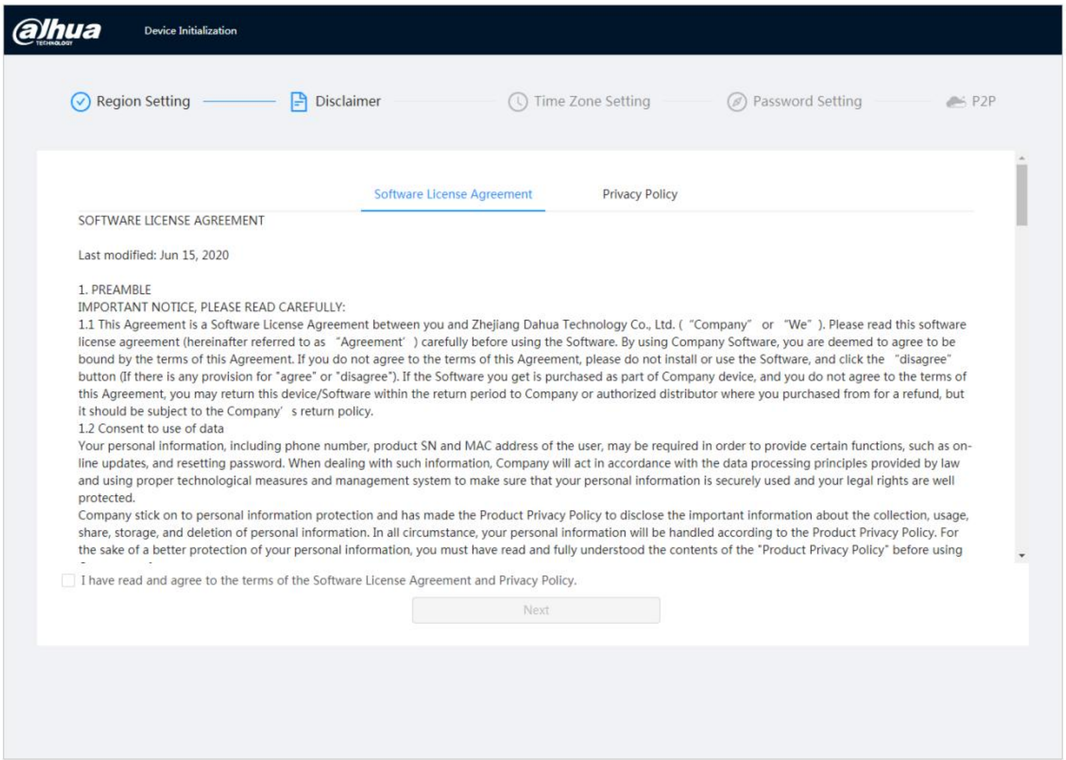
Area:

Language: English

Video Standard: PAL

Step 2: Select the area, language and video standard according to the actual situation, and then click **Next .**

Figure 2:2 disclaimer



SOFTWARE LICENSE AGREEMENT

Last modified: Jun 15, 2020

1. PREAMBLE

IMPORTANT NOTICE, PLEASE READ CAREFULLY:

1.1 This Agreement is a Software License Agreement between you and Zhejiang Dahua Technology Co., Ltd. ("Company" or "We"). Please read this software license agreement (hereinafter referred to as "Agreement') carefully before using the Software. By using Company Software, you are deemed to agree to be bound by the terms of this Agreement. If you do not agree to the terms of this Agreement, please do not install or use the Software, and click the "disagree" button (If there is any provision for "agree" or "disagree"). If the Software you get is purchased as part of Company device, and you do not agree to the terms of this Agreement, you may return this device/Software within the return period to Company or authorized distributor where you purchased from for a refund, but it should be subject to the Company' s return policy.

1.2 Consent to use of data

Your personal information, including phone number, product SN and MAC address of the user, may be required in order to provide certain functions, such as on-line updates, and resetting password. When dealing with such information, Company will act in accordance with the data processing principles provided by law and using proper technological measures and management system to make sure that your personal information is securely used and your legal rights are well protected.

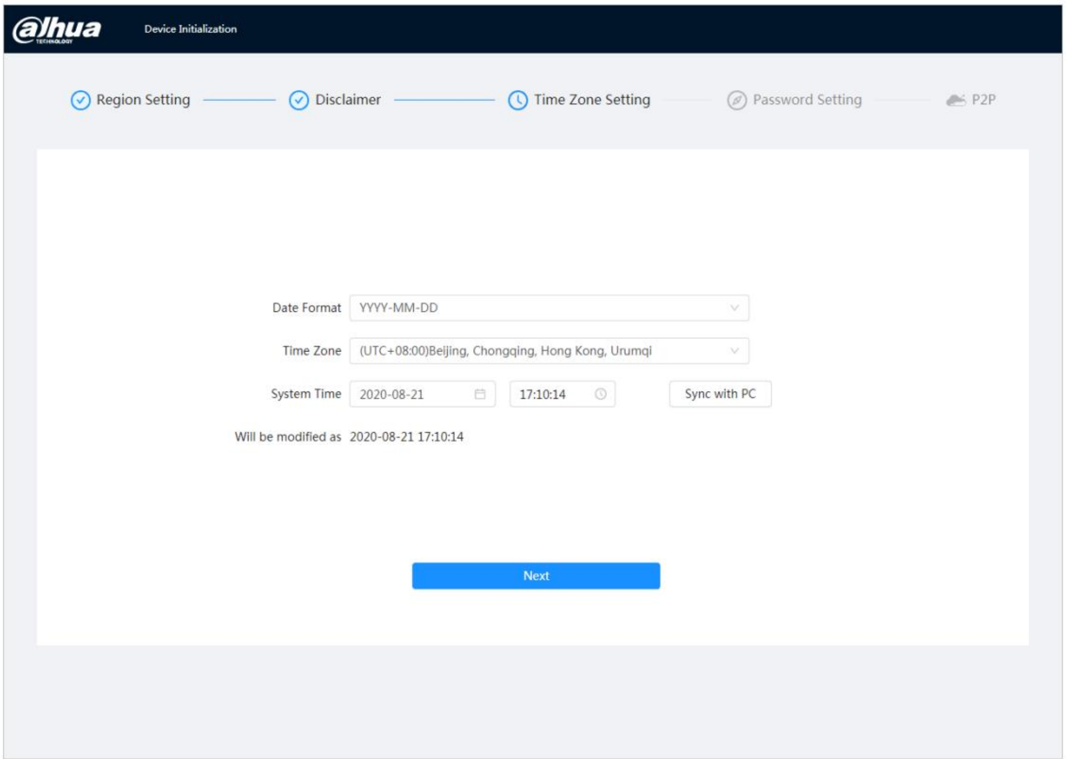
Company stick on to personal information protection and has made the Product Privacy Policy to disclose the important information about the collection, usage, share, storage, and deletion of personal information. In all circumstance, your personal information will be handled according to the Product Privacy Policy. For the sake of a better protection of your personal information, you must have read and fully understood the contents of the "Product Privacy Policy" before using

□ I have read and agree to the terms of the Software License Agreement and Privacy Policy.

~~Step 3: S~~elect the **I have read and agree to the terms of the Software License Agreement and Privacy Policy** check box , and then click in **Next**

(Next).

Figure 2:3 time zone configuration



Date Format YYYY-MM-DD

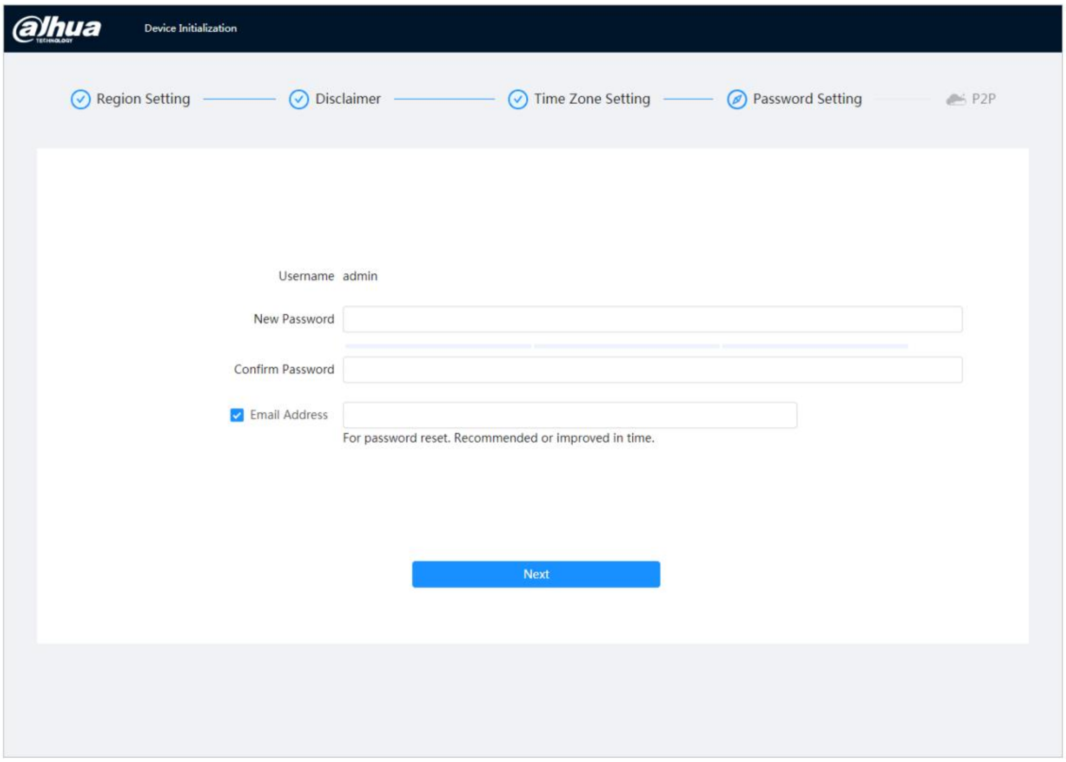
Time Zone (UTC+08:00)Beijing, Chongqing, Hong Kong, Urumqi

System Time 2020-08-21 17:10:14

Will be modified as 2020-08-21 17:10:14

~~Step 4: C~~onfigure the time parameters, and then click **Next .**

Figure 2:4 password settings



Device Initialization

Username admin

New Password

Confirm Password

☑ Email Address

For password reset. Recommended or improved in time.

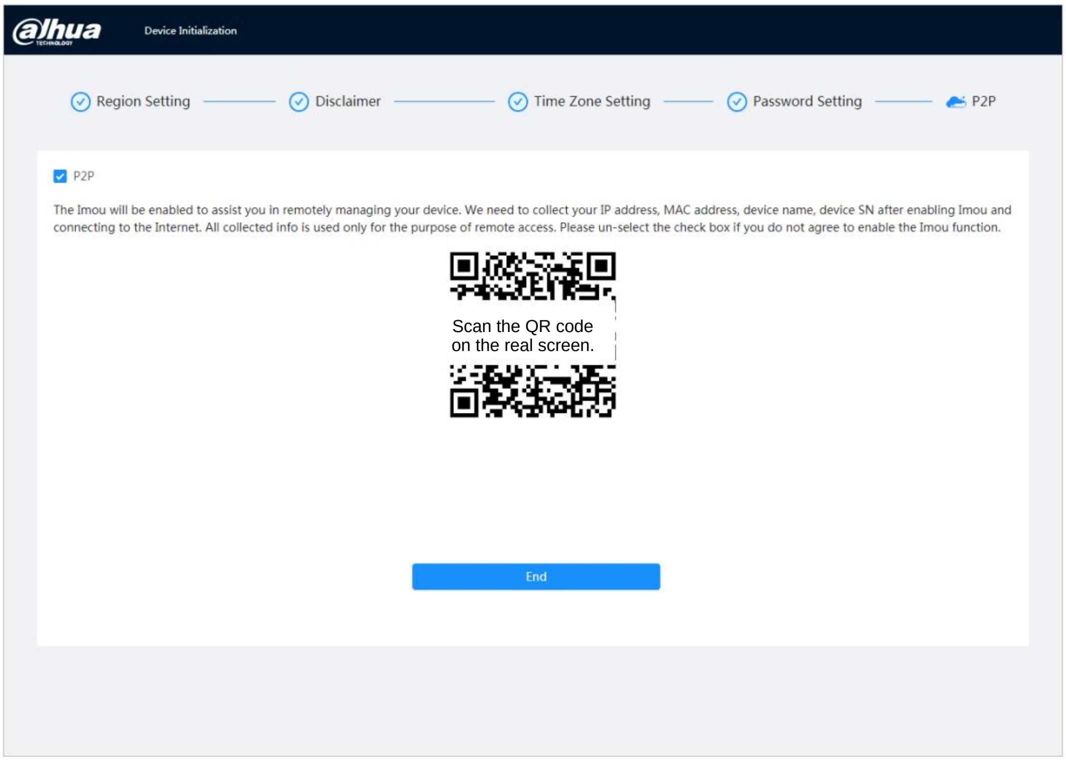
Step 5: Set the password for the administrator account.

Table 2:1 description of password settings

Parameter	Description
Username	The default username is admin.
Password	The password must consist of 8 to 32 non-empty characters and contain at least two character types including uppercase, lowercase, numbers, and special characters (excluding 'ÿ"ÿ;ÿ:ÿ&).ÿSet a password with a high security level according to the password security notice.
Confirm Password	
Saved Email	Enter an email address to reset your password and it will be selected by default. When you need to reset the administrator account password, a password reset security code will be sent to the saved email address.

Step 6: Click **Next ,** then the **P2P interface will appear.**

Figure 2–5 P2P



☑ P2P

The Imou will be enabled to assist you in remotely managing your device. We need to collect your IP address, MAC address, device name, device SN after enabling Imou and connecting to the Internet. All collected info is used only for the purpose of remote access. Please un-select the check box if you do not agree to enable the Imou function.

Scan the QR code on the real screen.

3 Access

3.1 Sign in to the device

This section explains how to log in and out of the web interface. This section takes the Chrome browser as an example.

- You must start the camera before logging in to the web interface. For details, see "2 Device Initialization".
- When starting the camera, keep the PC IP and device IP in the same network.
- Follow the instructions to download and install the first-time startup plug-in. session.

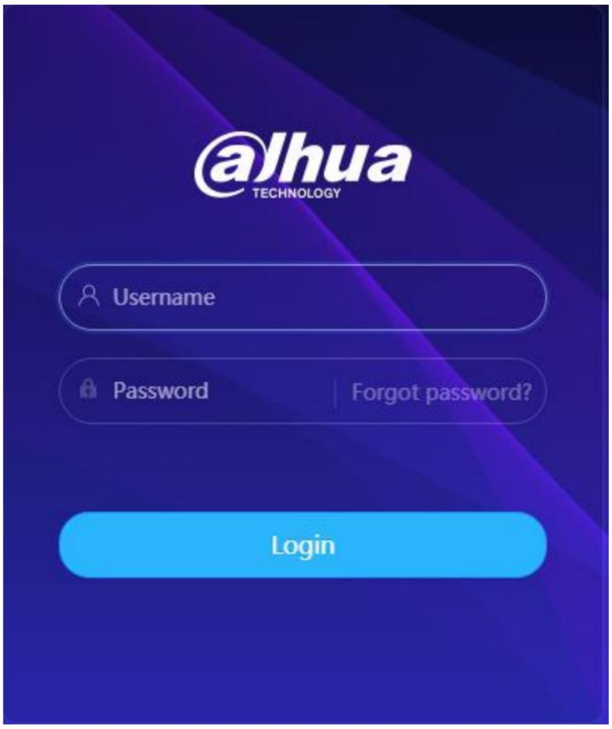
Step 1: Open Chrome browser, enter the IP address of the camera (192.168.1.108 by default) in the address bar and press Enter.

Step 2: Enter the username and password.

The username is admin by default.

Click **Forgot your password?** (Forgot password?) to reset the password via the email address that was set at startup. For details, see "3.2 Reset Password."

Figure 3–1 Login

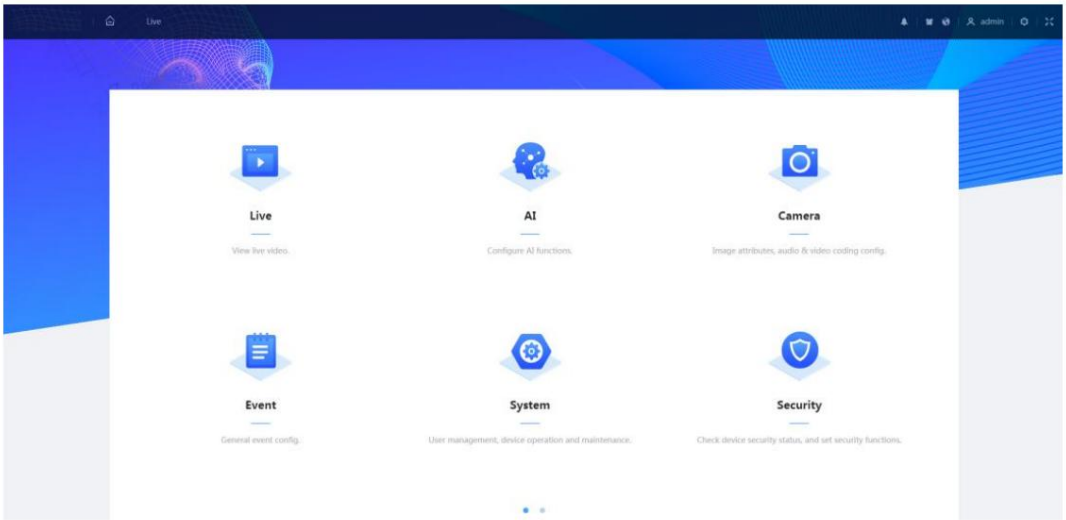


Step 3: Click **Login .**

The **Live** interface will appear . Click the interface to bring ⌂ in the upper left corner of up the main interface.

To log in for the first time, install the plugin by following the instructions on the screen.

Figure 3-2 Main screen


Live
admin
Live
View live video.
AI
Configure AI functions.
Camera
Image attributes, audio & video coding config.
Event
General event config.
System
User management, device operation and maintenance.
Security
Check device security status, and set security functions.

- Live: View the monitoring image in real time.
- AI: Set the camera's AI functions.
- Camera: Set camera parameters, including image parameters, encoder parameters, and audio parameters.
- Event: Configure general events, including linking exception. alarm, video detection and audio detection.
- System: Set system parameters, including general, date and time, account, security, PTZ settings, default, import/export, remote, auto maintenance and update.
- Security: Check the security status of the device and configure the security features.
- Recording: Play or download recorded videos.
- Image: Play or download image files.
- Report: Find the AI Events Report and System Report.

3.2 Reset password

When you need to reset the administrator account password, a security code will be sent to the email address you entered, which can be used to reset the password.

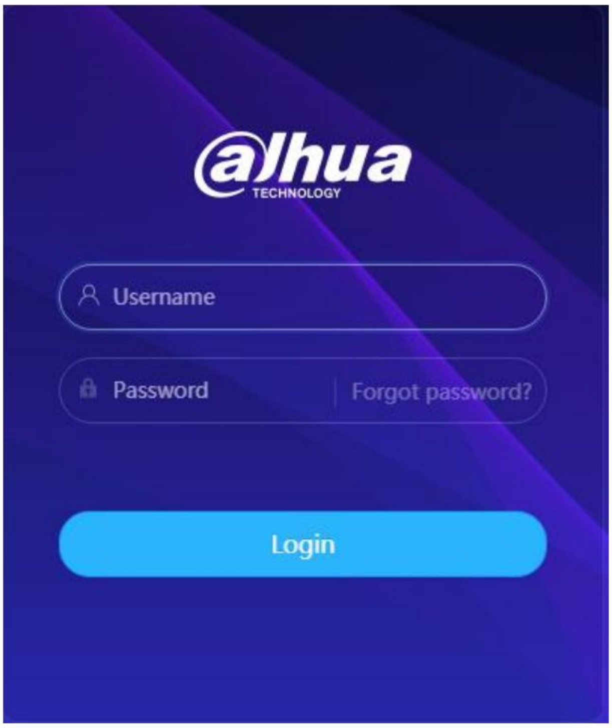
Previous requirements

You have enabled the password reset service ⚙ > **System** (System) > **Account** (Account) > **User** (User) .

Procedure

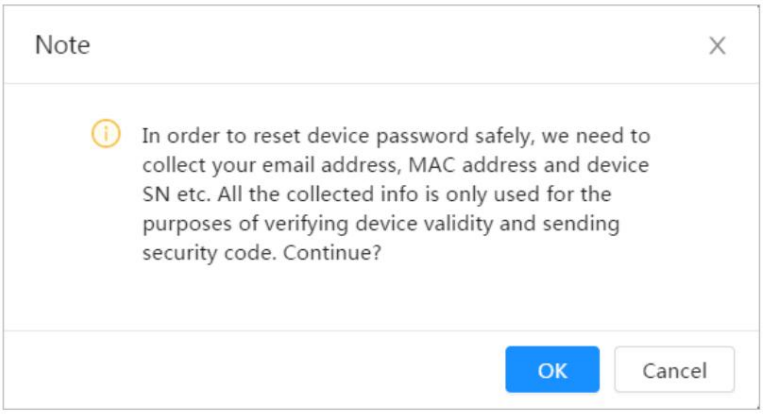
Step 1: Open Chrome browser, enter the device's IP address in the address bar, and then press the Enter key.

Figure 3–3 Login



~~Step 2: C~~lick **Forgot your password?** (Forgot password?) to reset the password via the email address that was set at startup.

Figure 3–4 Login



In order to reset device password safely, we need to collect your email address, MAC address and device SN etc. All the collected info is only used for the purposes of verifying device validity and sending security code. Continue?

4 Direct

This section introduces the interface design and function configuration.

4.1 Live Interface

Sign in or click the **Live** tab .

The interface may vary according to different models and the actual interface shall prevail.

Figure 4:1 live (single channel)

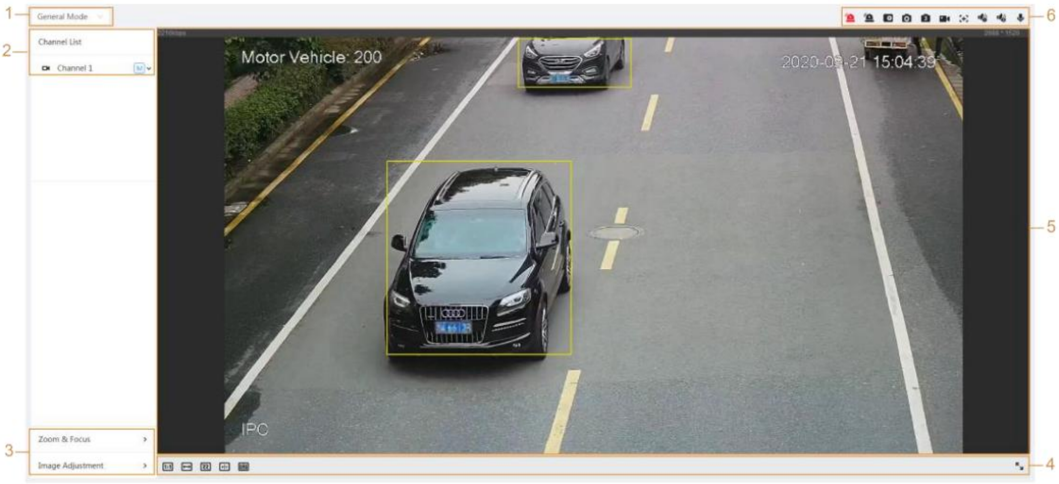


Figure 4:2 live (multi-channel)

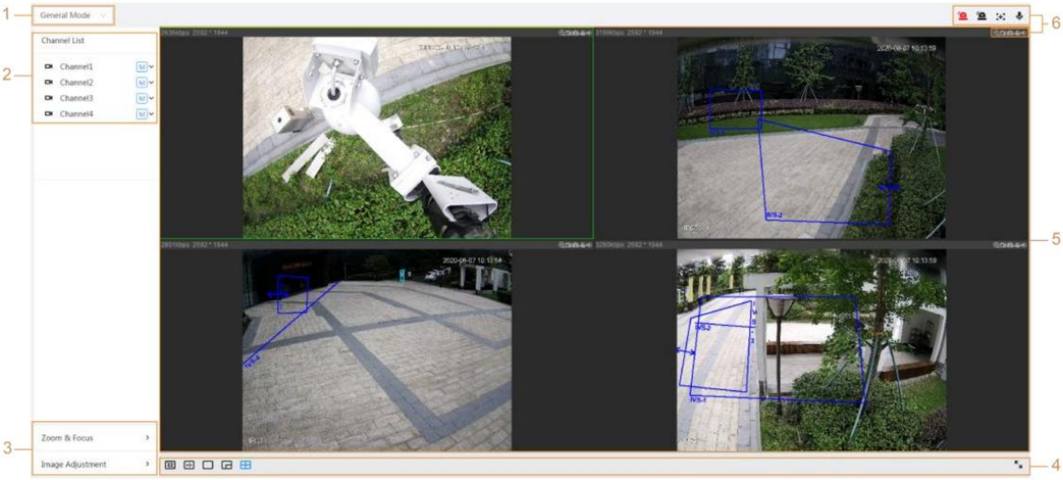


Table 4:1 description of the function bar

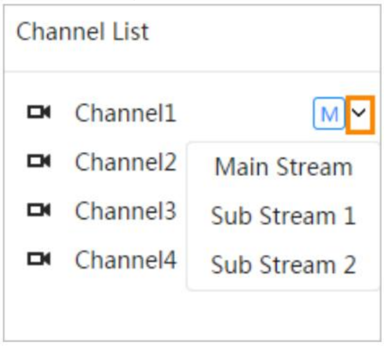
No.	Function	Description
1	Display mode	You can select the display mode between **General Mode** and **Face Mode .**
2	Channel list	Shows all channels. You can select the channel as needed and set the broadcast type.

No.	Function	Description
3	Image adjustment	Adjustment operations in live viewing.
4		
5	Live viewing	Shows the monitoring image in real time.
6	Live View Function Bar	Functions and operations in live viewing.

4.2 Encoding settings

Click on ⌄ and then select the stream as needed.

Figure 4:3 coding bar



- **Main transmission:** It has great bit and image transmission value with high resolution, but also requires high bandwidth. This option can be used for storage and monitoring.

- **Secondary stream:** It has a small bit stream value and an image fluid, and requires less bandwidth. This option is typically used to replace the main stream when bandwidth is not sufficient. means the current stream is the main

- M stream; current stream is secondary stream 1; S1 means that the S2 means that the current transmission

It is secondary transmission 2.

5 Config.

This section presents the basic settings of the camera, including Network, Event and System settings.

5.1 Red

This section presents the network configuration.

5.1.1TCP/IP

You can configure the IP address and DNS (Domain Name System) server and so on according to network planning.

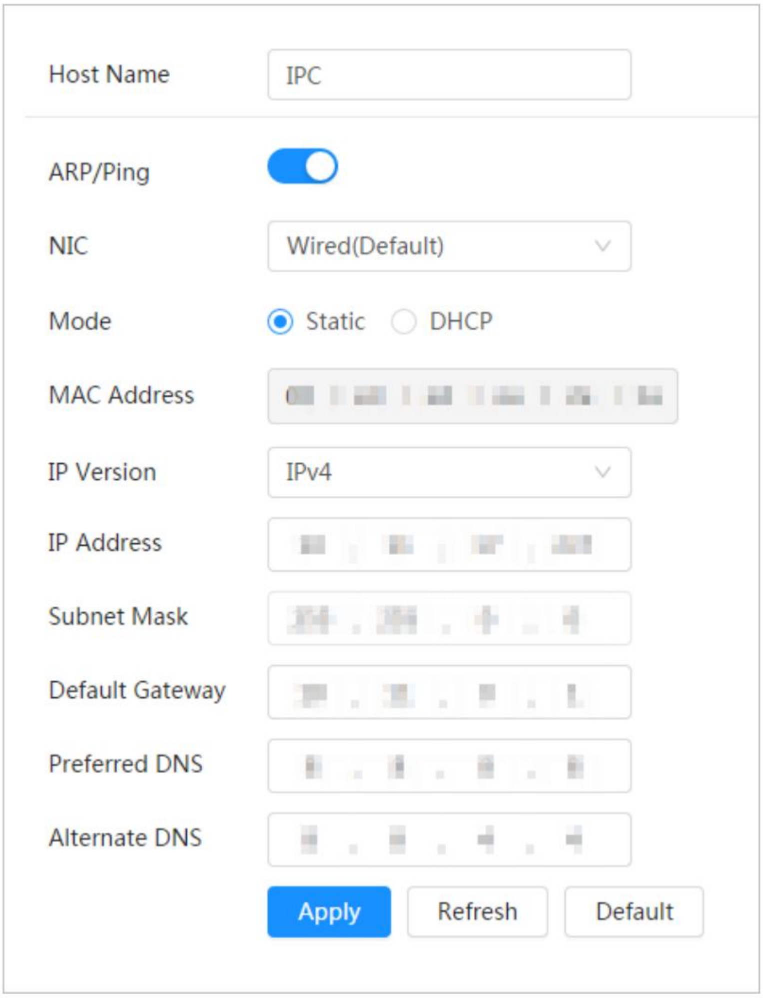
Previous requirements

The camera has connected to the network.

Procedure

Step 1: Select ⚙ > **Red** (Network) > **TCP/IP** (TCP/IP).

Figure 5–1 TCP/IP

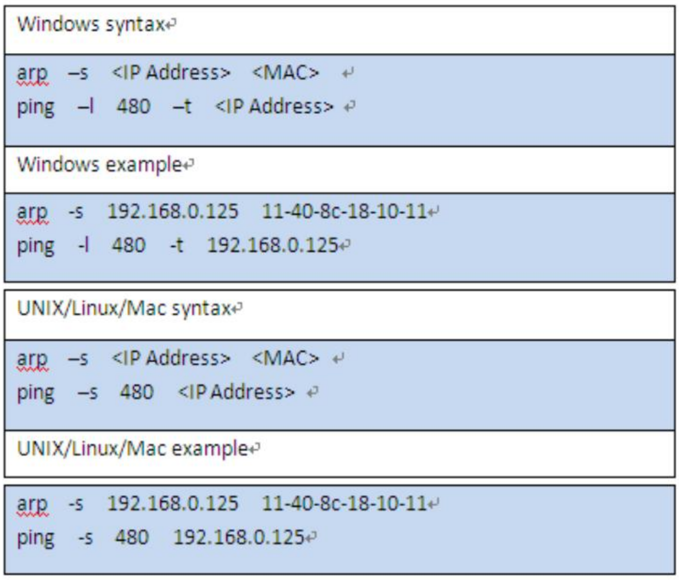


Host Name	IPC
ARP/Ping	●
NIC	Wired(Default)
Mode	● Static ○ DHCP
MAC Address	[redacted]
IP Version	IPv4
IP Address	[redacted]
Subnet Mask	[redacted]
Default Gateway	[redacted]
Preferred DNS	[redacted]
Alternate DNS	[redacted]

Step 2: Configure TCP/IP parameters.

Table 5:1 description of TCP/IP parameters

Parameter	Description
Hostname	Enter the host name; The maximum length is 15 characters.

Parameter	Description
ARP/Ping	Click to enable ARP/Ping and configure the IP address service. Obtain the MAC address of the camera so you can change and configure the device's IP address with the ARP/ping command. This feature is enabled by default. During the reboot, you will have no more than 2 minutes to configure the device's IP address using a ping packet with a certain length; The server will shut down within 2 minutes or shut down immediately after the IP address is set successfully. If not enabled, the IP address cannot be configured with the ping packet. **Demonstration of how to configure the IP address with ARP/Ping.** 1. Keep the camera that needs to be set up and the PC inside from the same local network, and then obtain a usable IP address. 2. Obtain the camera's MAC address from the device label. 3. Open the command editor on the PC and enter the next command.  Windows syntax arp –s <IP Address> <MAC> ping –l 480 –t <IP Address> Windows example arp -s 192.168.0.125 11-40-8c-18-10-11 ping -l 480 -t 192.168.0.125 UNIX/Linux/Mac syntax arp –s <IP Address> <MAC> ping –s 480 <IP Address> UNIX/Linux/Mac example arp -s 192.168.0.125 11-40-8c-18-10-11 ping -s 480 192.168.0.125 4. Restart the camera. 5. Check the PC command line; if the informational message **Reply from** 192.168.0.125…(Replyÿfromÿ) appears 192.168.0.125…),ÿtheÿconfigurationÿwillÿbeÿdoneÿ correctly and you can turn off the camera. 6. Enter http://(IP Address) in the address bar of the browser to log in.
NOTHING	Select the Ethernet card to be configured and the default is **Wired .**

Parameter	Description
Way	The way the camera obtains the IP: • **Static** Configure the **IP Address , Subnet Mask ,** and Default **Gateway** manually, and then click **Save ;** The login interface will appear with the configured IP address. • **DHCP** When there is a DHCP server on the network, select **DHCP** and the camera will obtain the IP address automatically.
MAC address	Shows the MAC address of the host.
IP version	Select **IPv4** or **IPv6.**
IP adress	When you select **Static** in **Mode ,** enter the IP address and subnet mask you need. • IPv6 does not have a subnet mask. • The default gateway must be on the same network segment as the IP address.
Subnet mask	
Default access portal	
Preferred DNS	Preferred DNS IP address
Alternative DNS	Alternate DNS IP Address

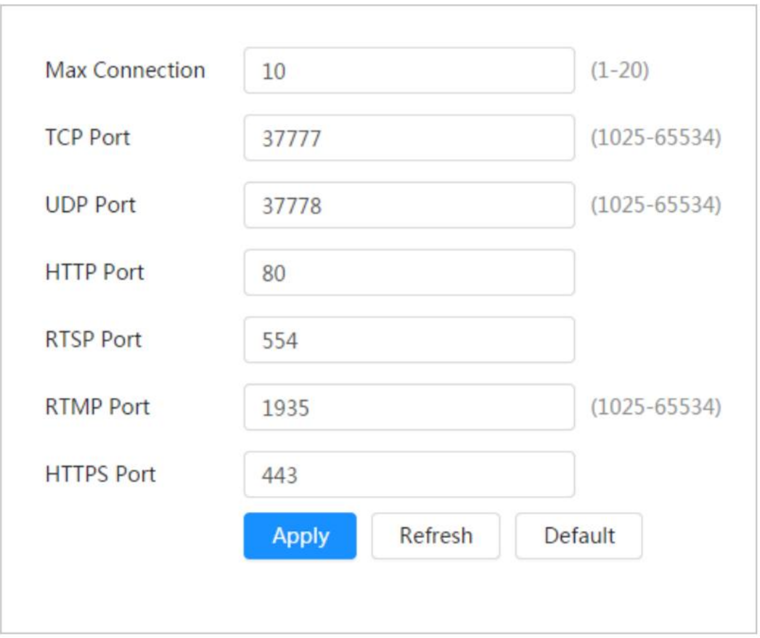
Step 3: Click on **Apply .**

5.1.2Puerto

Configure the port numbers and the maximum number of users (includes web, platform client, and mobile phone client) that can connect to the device simultaneously.

Step 1: Select ⚙ > **Red** (Network) > **TCP/IP** (TCP/IP).

Figure 5:2 port



Max Connection: 10 (1-20)

TCP Port: 37777 (1025-65534)

UDP Port: 37778 (1025-65534)

HTTP Port: 80

RTSP Port: 554

RTMP Port: 1935 (1025-65534)

HTTPS Port: 443

Step 2: Configure the port parameters.

- 0–1024, 1900, 3800, 5000, 5050, 9999, 37776, 37780–37880, 39999, 42323 are occupied for specific uses.
- Do not use the same value of any other port during port configuration.

Table 5:2 description of port parameters

Parameter	Description
Maximum connections	The maximum number of users (web client, platform client, or mobile phone client) that can connect to the device simultaneously. The default value is 10.
Puerto TCP	Transmission control protocol port. The default value is 37777.
Puerto UDP	User datagram protocol port. The default value is 37778.
Puerto HTTP	Hypertext transfer protocol port. The default value is 80.

Parameter	Description
Puerto RTSP	• Real-time streaming protocol port, and the default value is 554. If you play live viewing with QuickTime, VLC, or a Blackberry smartphone, the following URL format is available. • When the URL format requires RTSP, you must specify the channel number and bitstream type in the URL, and also the username and password if necessary. URL format example: rtsp://username:password@ip:port/cam/realmonitor?channel=1& subtype=0 Among that: • Username: The username, which would be admin. • Password: The password, which would be admin. • IP: The IP of the device, which would be 192.168.1.112. • Port: Leave it if the value is the default value 554. • Channel: The channel number, starting at 1. For example, if you are using channel 2, then channel = 2. • Subtype: The type of bit transmission; 0 means primary stream (subtype = 0) and 1 means secondary stream (subtype = 1). Example: If you need the secondary stream of channel 2 from a certain device, the URL should be: rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel= 21&=1 If the username and password are not required, the URL can be: rtsp://ip:port/cam/realmonitor?channel=11&=0
Puerto RTMP	Real-time messaging protocol. The port that RTMP provides service. It is 1935 by default.
Puerto HTTPS	HTTPS communication port. It is 443 by default.

Step 3: Click on **Apply .**

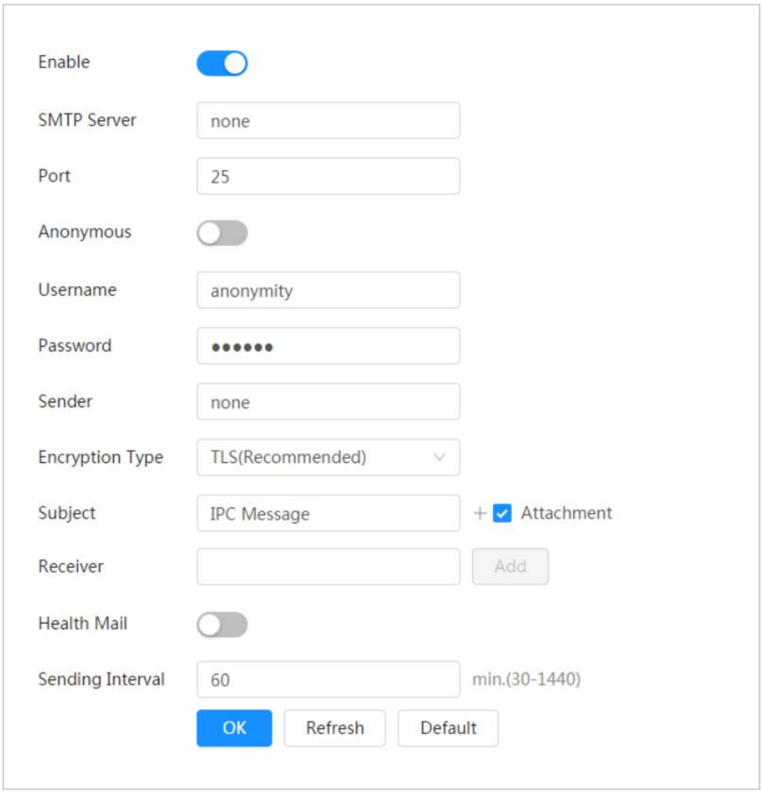
The **Max Connections** setting (Max Connection) takes effect immediately, and the others will take effect after reboot.

5.1.3Email

Configure the email parameter and enable email binding. He system sends an email to the defined address when the alarm is activated correspondent.

Step 1: Select ⚙ > **Network** (Netwok) > **Email** (Email).

Figure 5:3 email



Enable: on

SMTP Server: none

Port: 25

Anonymous: off

Username: anonymity

Password: ••••••

Sender: none

Encryption Type: TLS(Recommended)

Subject: IPC Message + ☑ Attachment

Receiver:

Health Mail: off

Sending Interval: 60 min.(30-1440)

Step 2: Click to enable the feature.

Step 3: Configure email parameters

Table 5:3 description of email parameters

Parameter	Description	
Servidor SMTP	SMTP server address	For details, see Table 5:4.
Puerto	The port number of the SMTP server.	
Username	The SMTP server account.	
Password	The SMTP server password.	
Anonymous	Click in the ◯ and the sender information will not be displayed email.	
Sender	Sender email address.	
Encryption type	Select between None **SSL and** TLS . For details, see Table 5:4.	
Title	Enter a maximum of 63 characters in Chinese, English, and Arabic numerals. Click to select the title type, including **Device Name , Device** ID, and **Event Type** (EventType); You can set a maximum of 2 titles.	
Attached data	Check the checkbox to be able to attach files to the email.	

Parameter	Description
Recipient	• Email address of the recipient. Supports 3 addresses at most. • After entering the email address of the recipient, the **Test** button will appear . Click **Test** to test whether emails can be sent and received correctly.
verification email	The system sends a test email to verify that the connection has been configured correctly. Click and set the **Sending Interval ,** and then the system will send the test mail at the set interval.

For the configuration of the main mailboxes, see. Table 5:4.

Table 5:4 Mailbox configuration description

Mailbox	SMTP Server	Authentication	Port	Description
gmail	smtp.gmail.com	SSL	465	• You need to have the service activated SMTP in your mailbox mail. • The code is required authentication. The email password electronic is not application. Authentication code: The code you receive when you enable the SMTP service.
		TLS	587	

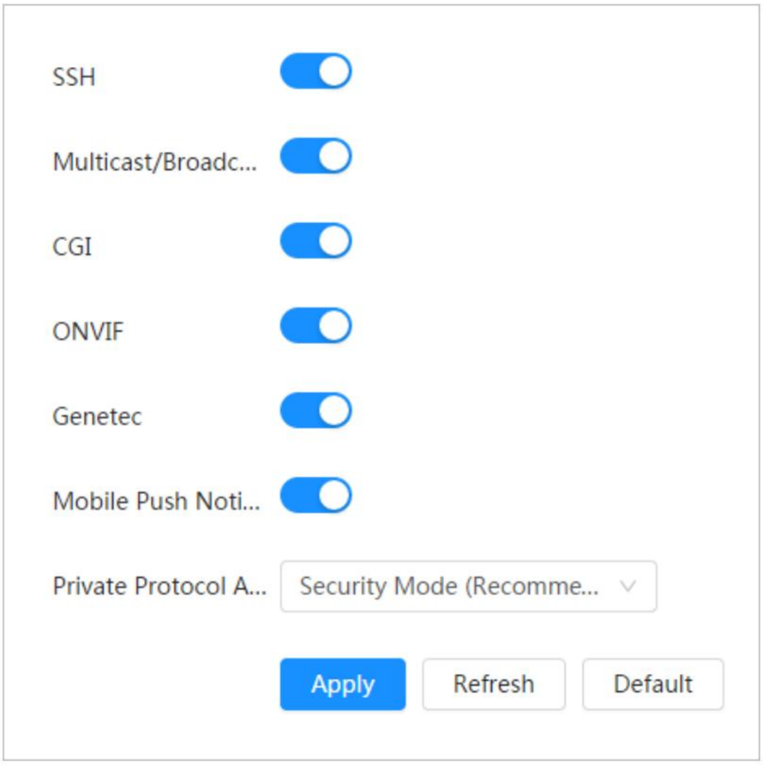
Step 4: Click on **Apply .**

5.1.4Basic service

Configure basic services to improve network and data security.

Step 1: Select ⚙ > **Network** > **Basic Service .**

Figure 5:4 basic service



SSH ●

Multicast/Broadc... ●

CGI ●

ONVIF ●

Genetec ●

Mobile Push Noti... ●

Private Protocol A... Security Mode (Recomme...

Step 2: Enable the basic service according to actual needs.

Table 5:5 description of basic service parameters

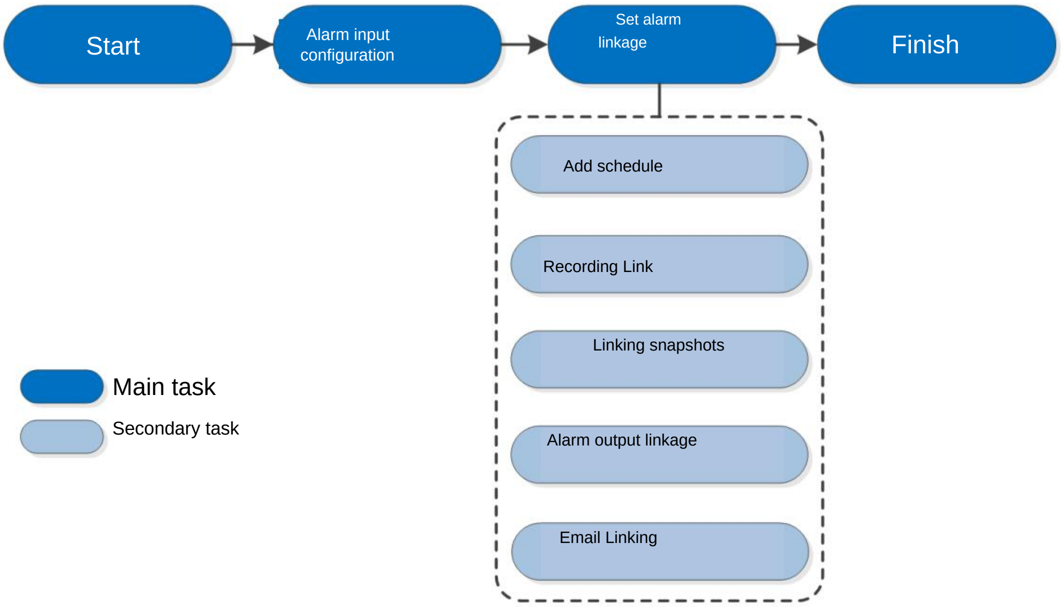
Function	Description
SSH	You can enable SSH authentication to manage security.
Multicast/ broadcast search	Enable this function, and then when multiple users are viewing the device's video image simultaneously over the network, they can find your device with the multicast/broadcast protocol.
CGI	Enable the feature and then other devices can access it through this service. The feature is enabled by default.
Onvif	
Genetec	
*******Push mobile notifications*******	Enable this feature and then the system will send the snapshot that was taken when the alarm was triggered to your phone, this is enabled by default.
Private protocol authentication mode	Select the authentication mode between **Security Mode** and **Compatible Mode .** Safety mode is recommended.

Step 3: Click on **Apply .**

5.2 Event

This section takes alarm input, for example, to present alarm linkage configuration.

Figure 5:5 alarm event configuration



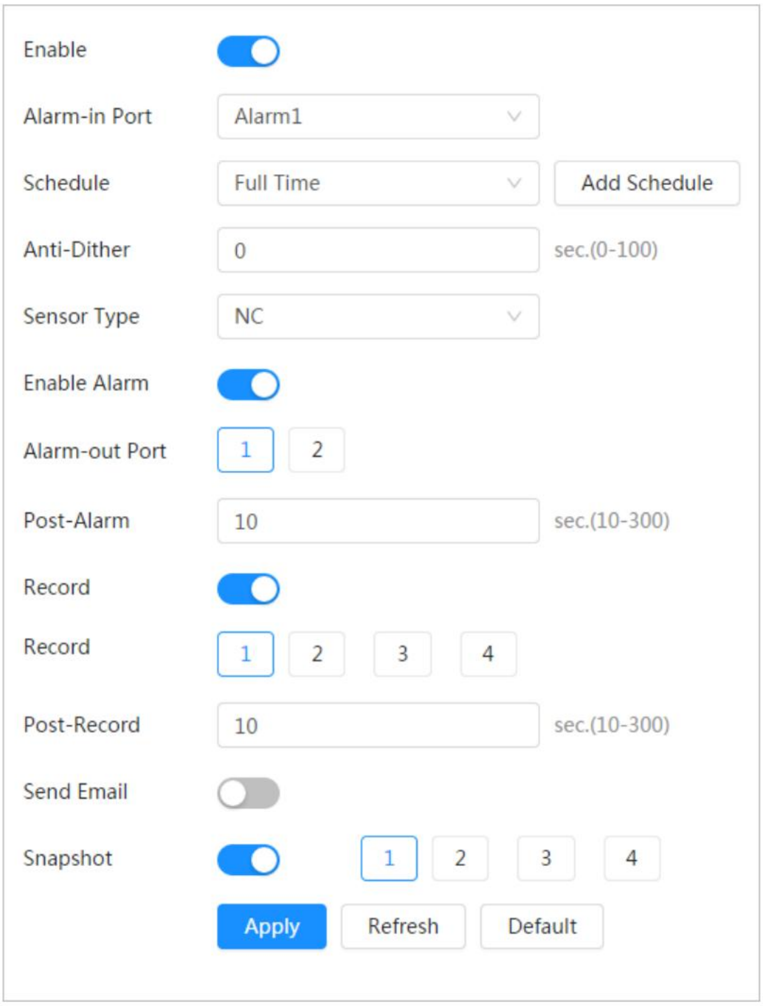
5.2.1Alarm input configuration

When the device connected to the alarm input port triggers an alarm, the system performs the set alarm linkage.

Step 1: Select ⚙ > **Event** > **Alarm .**

Step 2: Click ○ next to **Enable** to enable alarm linking.

Figure 5-6 Alarm Linkage



Enable	●	
Alarm-in Port	Alarm1	
Schedule	Full Time	Add Schedule
Anti-Dither	0	sec.(0-100)
Sensor Type	NC	
Enable Alarm	●	
Alarm-out Port	1 2	
Post-Alarm	10	sec.(10-300)
Record	●	
Record	1 2 3 4	
Post-Record	10	sec.(10-300)
Send Email	○	
Snapshot	● 1 2 3 4	

Apply Refresh Default

Step 3: Select an alarm input port and sensor type.

- Sensor type: NO or NC.
- Anti-jitter: Only record one alarm event during the alarm period.
  anti-interpolation.

Step 4: Select the schedule and arming periods and alarm linkage action. For details, see "5.2.2 Set Alarm Linkage."

If the existing schedules cannot meet the scene requirement, you can click **Add Schedule** to add a new schedule.

For details, see "5.2.2.1 Add Schedule."

Step 5: Click on **Apply .**

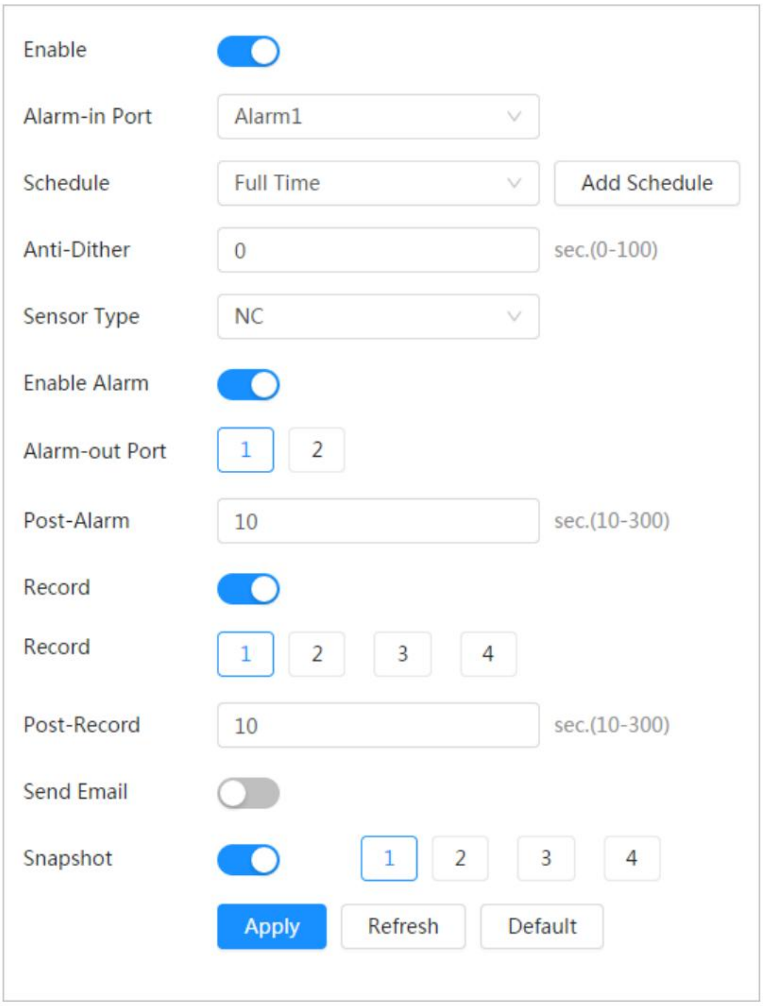
5.2.2Set alarm linkage

When configuring alarm events, select alarm links (such as log, snapshot).

When the corresponding alarm is activated in the configured arming period, the system will issue an alarm.

Select ⚙ > **Event** > **Alarm ,** ○ next to **Enable** to enable alarm linking.

Figure 5-7 Alarm Linkage



Enable ●

Alarm-in Port Alarm1

Schedule Full Time

Anti-Dither 0 sec.(0-100)

Sensor Type NC

Enable Alarm ●

Alarm-out Port [✓ 1] 2

Post-Alarm 10 sec.(10-300)

Record ●

Record [✓ 1] 2 3 4

Post-Record 10 sec.(10-300)

Send Email ○

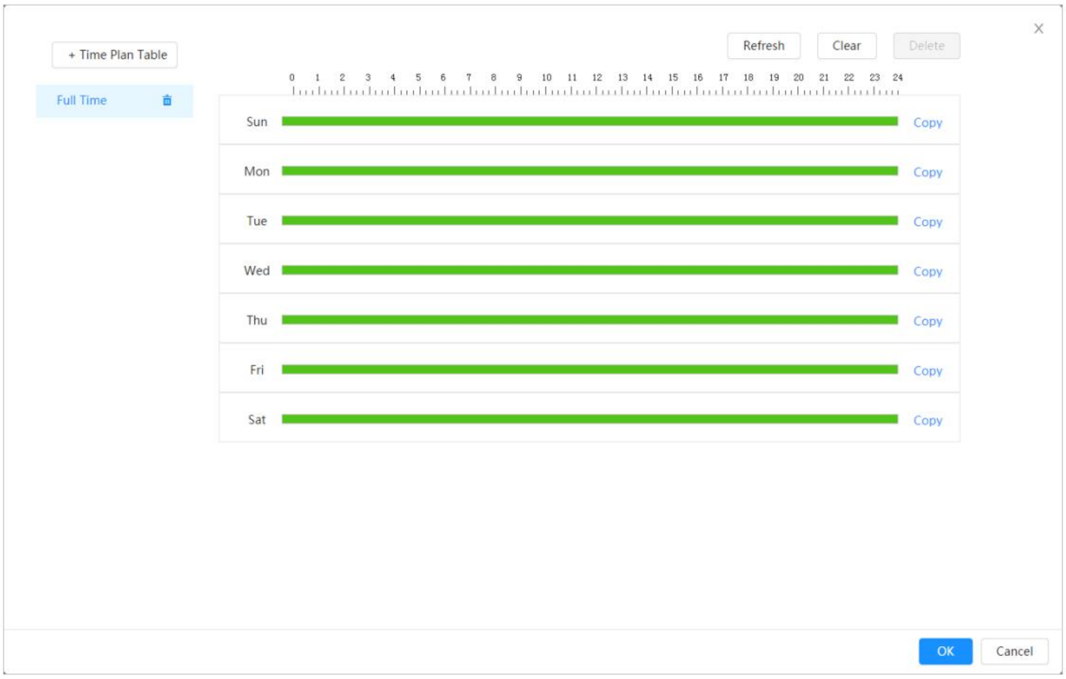
Snapshot ● [✓ 1] 2 3 4

5.2.2.1Add schedule

Establish arming periods. The system only performs the corresponding linking action in the configured period.

~~Step 1: C~~lick **Add Schedule** next to **Schedule .**

Figure 5:8 programming



Step 2: Press and drag the left mouse button on the timeline to set arming periods.
Alarms will be triggered in the time period in green on the timeline.

- Click **Copy** next to a day and select the days you want to copy on the prompt interface; You can copy the settings to the selected days. Select the **Select All** check box to select every day to copy the settings.

- You can set 6 time periods per day.

Step 3: Click on **Apply .**
Step 4: (Optional) Click **Time Plan Table** to add a new time plan table.

Can:

- Double-click the table name to edit it.
- Click 🗑 to delete history as needed.

5.2.2.2Recording linkage

The system can link the recording channel when an alarm event occurs. After the alarm, the system stops recording after a long period of time according to the **Post** -Record setting.

Previous requirements

- Once the corresponding alarm type is enabled **(Normal, Motion** or **Alarm** (Alarm), the recording channel links the recording.
- Enable auto recording mode, recording linkage will be applied.

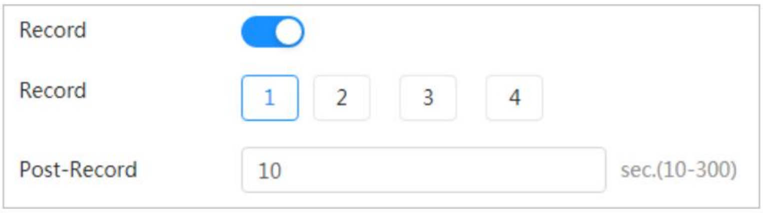
Set recording linkage

In the **Alarm** interface , click select the ○ to enable link recording, channel as necessary and set **Post** -Record to

Set alarm linkage and recording delay.

Once Post-Record is set , alarm recording continues for an extended period after the alarm ends.

Figure 5:9 recording link



Record ●

Record 1 2 3 4

Post-Record 10 sec.(10-300)

5.2.2.3Linking snapshots

Once snapshot linking is set up, the system can activate the alarm and automatically take photos when an alarm is triggered.

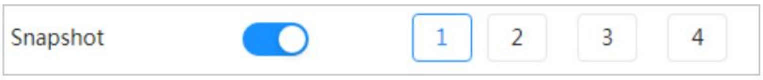
Previous requirements

Once the corresponding alarm type is enabled **(Normal, Motion** or **Alarm** (Alarm)), the snapshot channel links the image capture.

Set recording linkage

In the **Alarm** interface , click snapshot and select the to enable linking channel as necessary.

Figure 5:10 snapshot link



Snapshot ● 1 2 3 4

5.2.2.4Alarm output linkage

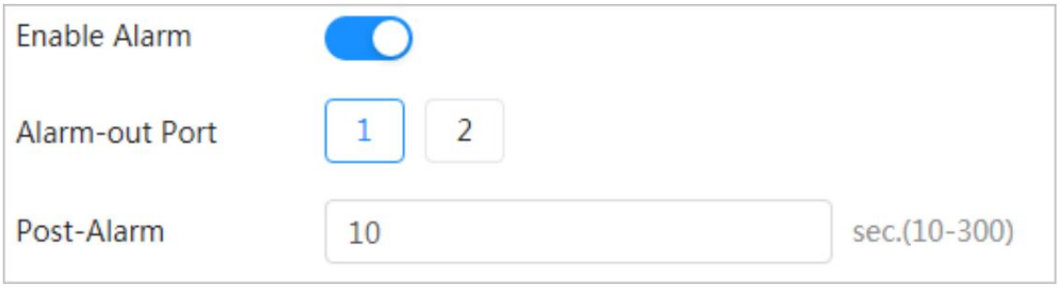
When an alarm is triggered, the system can automatically link with the alarm output device.

In the **Alarm** interface , click alarm, select the channel as to enable outbound binding needed, and then set **Post alarm**

(Post alarm).

When the alarm delay is set, the alarm continues for an extended period after the alarm ends.

Figure 5:11 alarm output link



Enable Alarm

Alarm-out Port: 1 2

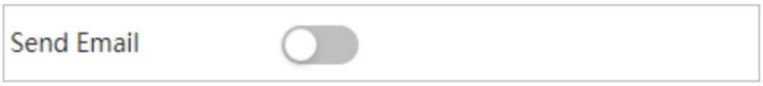
Post-Alarm: 10 sec.(10-300)

5.2.2.5 Email Linking

When an alarm is triggered, the system will automatically send an email to users.

Email binding takes effect only when SMTP is configured. For details, see "5.1.3 Email."

Figure 5:12 email link



Send Email

5.3 System

This section presents the system settings, including general, date and time, account, security, PTZ settings, default, import/export, remote, auto maintenance and update.

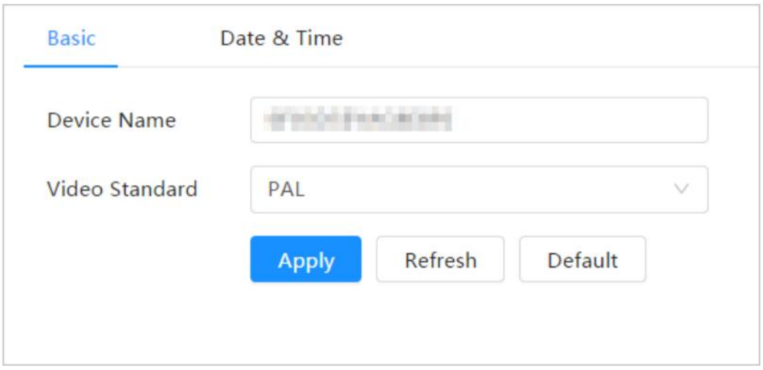
5.3.1General

5.3.1.1Basic

You can set the device name, language and video standard.

Step 1: Select ⚙ > **System** > **General** > **Basic .**

Figure 5:13 basic



Device Name

Video Standard: PAL

Step 2: Configure general parameters

Table 5:6 description of general parameters

Parameter	Description
Name	Enter device name
Video standard	Select the video standard between **PAL** and **NTSC.**

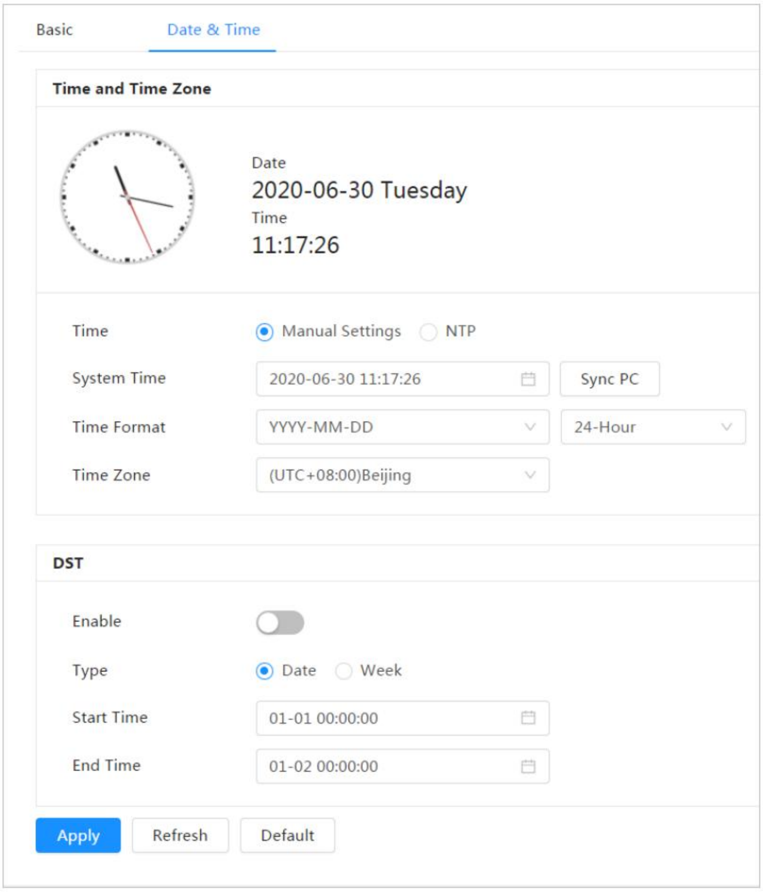
Step 3: Click on **Apply .**

5.3.1.2Date and time

You can set the date and time format, time zone, current time, DST (daylight saving time), or NTP server.

Step 1: Select ⚙ > **System** > **General** > **Basic** > **Date and Time** (Date & Time).

Figure 5:14 date and time



Time and Time Zone

Date
2020-06-30 Tuesday
Time
11:17:26

Time ● Manual Settings ○ NTP
System Time 2020-06-30 11:17:26
Time Format YYYY-MM-DD 24-Hour
Time Zone (UTC+08:00)Beijing

DST

Enable
Type ● Date ○ Week
Start Time 01-01 00:00:00
End Time 01-02 00:00:00

Step 2: Set the date and time parameters.

Table 5:7 description of date and time parameters

Parameter	Description
Date format	Set the date format.

Parameter	Description
Hour	• **Manual configuration:** configure parameters manually manual. • **NTP:** When you select NTP, the system synchronizes the time with the Internet server in real time. You can also enter the IP address, time zone, port, and range of a PC with NTP server to use NTP.
Time format	Set the time format. You can select between **12 hours** (12-Hour) or **24-Hour** (24-Hour).
Time zone	Set the time zone the camera is in.
Current time	Set the system time. Click **Sync PC** and the system will adopt the PC time.
DST	Enable DST as needed. Click , and set the start and end time of daylight savings time with **Date** or **Week .**

Step 3: Click on **Apply .**

5.3.2Account

You can manage users, such as adding, deleting, or editing them. Users include administrators, added users, and ONVIF users.

User and group management is only available for administrator users.

- The maximum length of the user or group name is 31 characters, which consists of number, letter, underline, hyphen, period and @.
- The password must consist of 8 to 32 non-empty characters and contain at least two character types including uppercase, lowercase, numbers, and special characters (excludingÿ'ÿ"ÿ;ÿ:ÿ ÿ &).
- You can have a maximum of 18 users and 8 groups.
- You can manage users through a single user or group and no duplicate usernames or group names are allowed. A user can only be in one group, and users in the group can have permissions within the group's authority range.
- Online users cannot edit their own permission.
- There is a default administrator who has the maximum authorization.
- Select Anonymous **Login ,** and then log in with only the IP address instead of the username and password. Anonymous users only have preview authorization. During anonymous login, click **Logout** and then you can log in with another username.

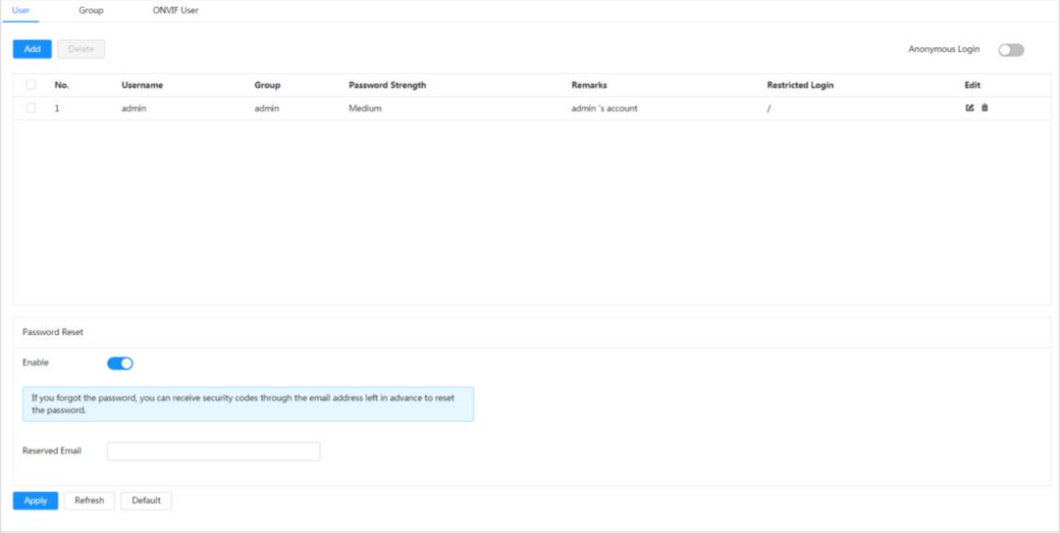
5.3.2.1Usuario

5.3.2.1.1 Add users

You are an administrator user by default. You can add users and configure different permissions.

Step 1: Select ⚙ > **System** (System) > **Account** > (Account) **User** (User).

Figure 5:15 user



□	No.	Username	Group	Password Strength	Remarks	Restricted Login	Edit
□	1	admin	admin	Medium	admin 's account	/	

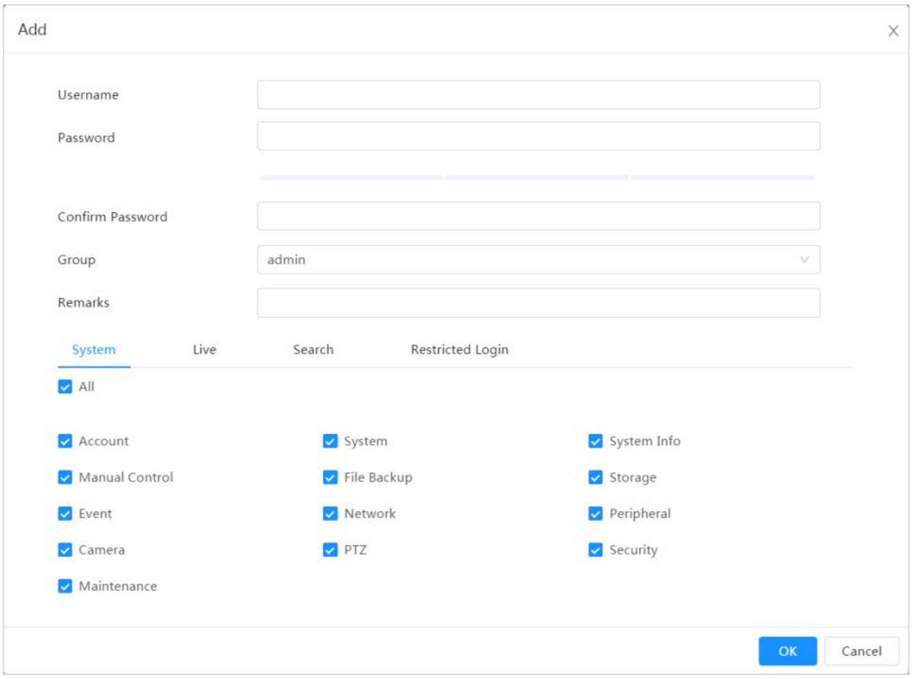
Enable: ●

If you forgot the password, you can receive security codes through the email address left in advance to reset the password.

Reserved Email:

Step 2: Click **Add .**

Figure 5:16 add user (system)



Add

Username

Password

Confirm Password

Group: admin

Remarks

System | Live | Search | Restricted Login

☑ All

☑ Account ☑ System ☑ System Info

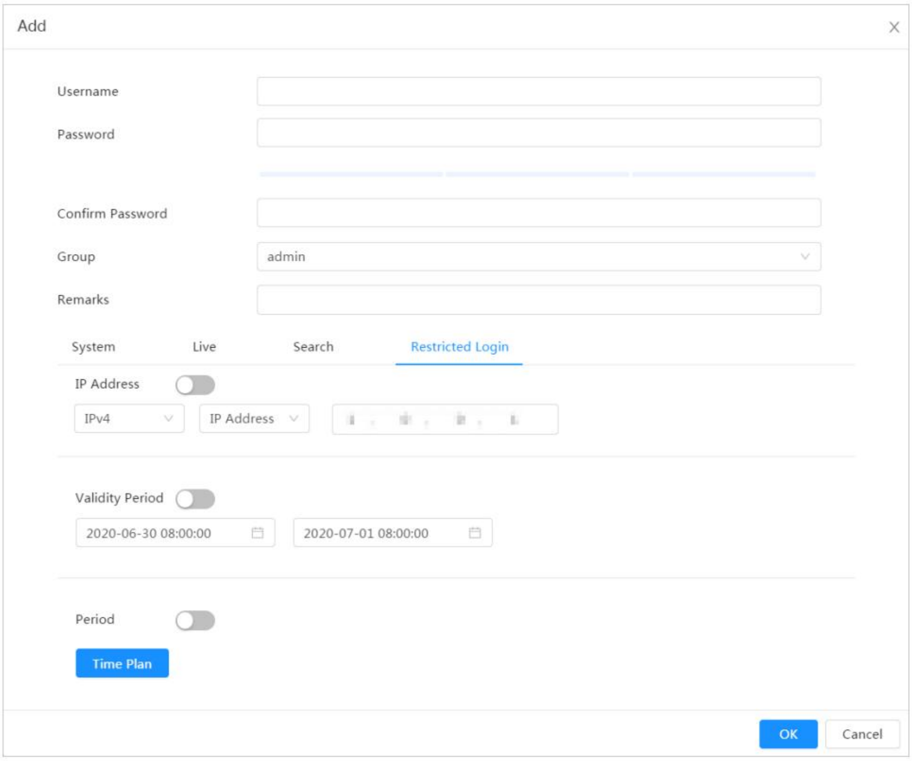
☑ Manual Control ☑ File Backup ☑ Storage

☑ Event ☑ Network ☑ Peripheral

☑ Camera ☑ PTZ ☑ Security

☑ Maintenance

Figure 5:17 add user (restricted login)



Add

Username

Password

Confirm Password

Group: admin

Remarks

System | Live | Search | Restricted Login

IP Address ○

IPv4 | IP Address

Validity Period ○

2020-06-30 08:00:00 | 2020-07-01 08:00:00

Period ○

Step 3: Configure user parameters

Table 5:8 description of user parameters (1)

Parameter	Description
Username	Unique user identification. You cannot use the existing username.
Password	Enter the password and confirm it again.

Parameter	Description
Confirm Password	The password must consist of 8 to 32 non-empty characters and contain at least two types of characters between uppercase, lowercase, numbers, and special characters (excluding "ÿ"ÿ;ÿ:ÿ&).
Group	The group to which the users belong. Each group has different permissions.
Observation	Describe the user.
System	Select permissions as necessary. It is recommended to grant fewer permissions to regular users than to premium users.
Straight	Select the live viewing permission for the user to be added.
Look for	Select the search permission for the user to be added.
Restricted login	Set the PC address that allows the user to log in to the camera and the validity period and time range. You can log in to the web interface with the IP set in the time range set as the validity period. • IP Address: You can log in to the web through PC with the set IP. • Validity period: You can log in to the web at the established validity period. • Time range: You can log in to the web in the interval of established time. Set as follows 1. IP Address: Enter the IP address of the host to be add. 2. IP segment: enter the starting address and address end of the host to be added.

Step 4: Click on **Apply .**

The newly added user appears in the username list.

Related operations

- Click ✎ to edit the password, group, note, or permissions.

For administrator account, you can only edit the password.

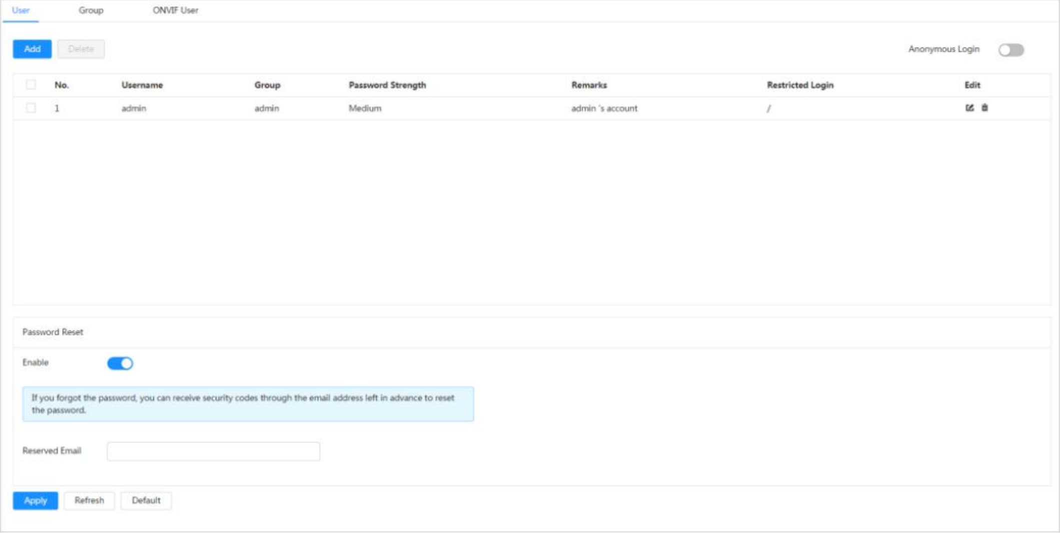
- Click 🗑 to delete the added users. The administrator user cannot be eliminate.

The administrator account cannot be deleted.

5.3.2.1.2 Reset password

Enable the feature and you can reset your password by clicking **Forgot your password?** (Forget password?) in the login interface. For details, see "3.2 Reset Password."

Step 1: Select > **System** (System) > **Account** > (Account) **User** (User).



□	No.	Username	Group	Password Strength	Remarks	Restricted Login	Edit
□	1	admin	admin	Medium	admin 's account	/	

If you forgot the password, you can receive security codes through the email address left in advance to reset the password.

Figure 5:18 user

Step 2: Click (Password next to **Enable** in **Reset Password** Reset).

If the feature is not enabled, you can only reset the password by resetting the camera.

Step 3: Enter the reserved email address.

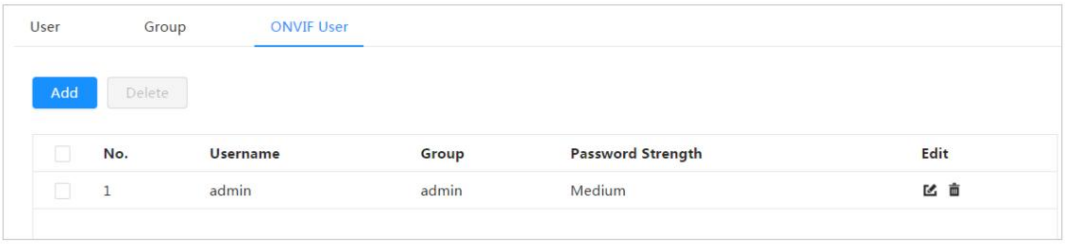
Step 4: Click on **Apply .**

5.3.2.2Usuario ONVIF

You can add, remove ONVIF users and change their passwords.

Step 1: Select > **System** > **Account** > **ONVIF User** (ONVIF User).

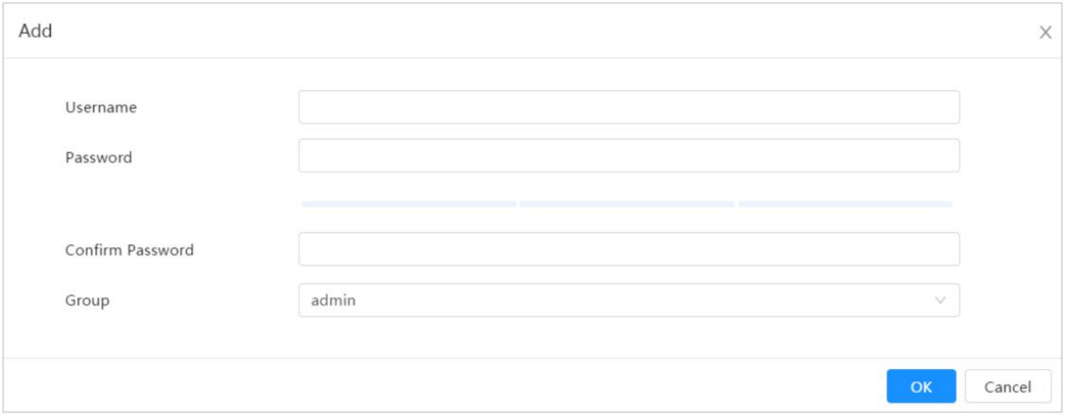
Figure 5-19 ONVIF User



□	No.	Username	Group	Password Strength	Edit
□	1	admin	admin	Medium	

Step 2: Click **Add .**

Figure 5:20 add ONVIF user


Add

Username

Password

Confirm Password

Group admin

Step 3: Configure user parameters

Table 5:9 description of ONVIF user parameters

Parameter	Description
Username	Unique user identification. You cannot use the existing username.
Password	Enter the password and confirm it again. The password must consist of 8 to 32 non-empty characters and contain at least two character types including uppercase, lowercase, numbers, and special characters (excluding 'ÿ"ÿ;ÿ:ÿ&).
Confirm Password	
Group name	The group to which the users belong. Each group has different permissions.

Step 4: Click on **Accept** (OK).

The newly added user appears in the username list.

Related operations

- Click ✎ to edit the password, group, note, or permissions.

For the administrator account, you can only change the password.

- Click to delete the 🗑 added users. The administrator user cannot be deleted.

The administrator account cannot be deleted.

5.3.3 Carriers

5.3.3.1Requirements

To ensure that the system works correctly, perform the following actions:

- Check surveillance footage regularly.
- Regularly delete unused user and user group information

frequently.

- Change the password every three months. For details, see "5.3.2 Account."

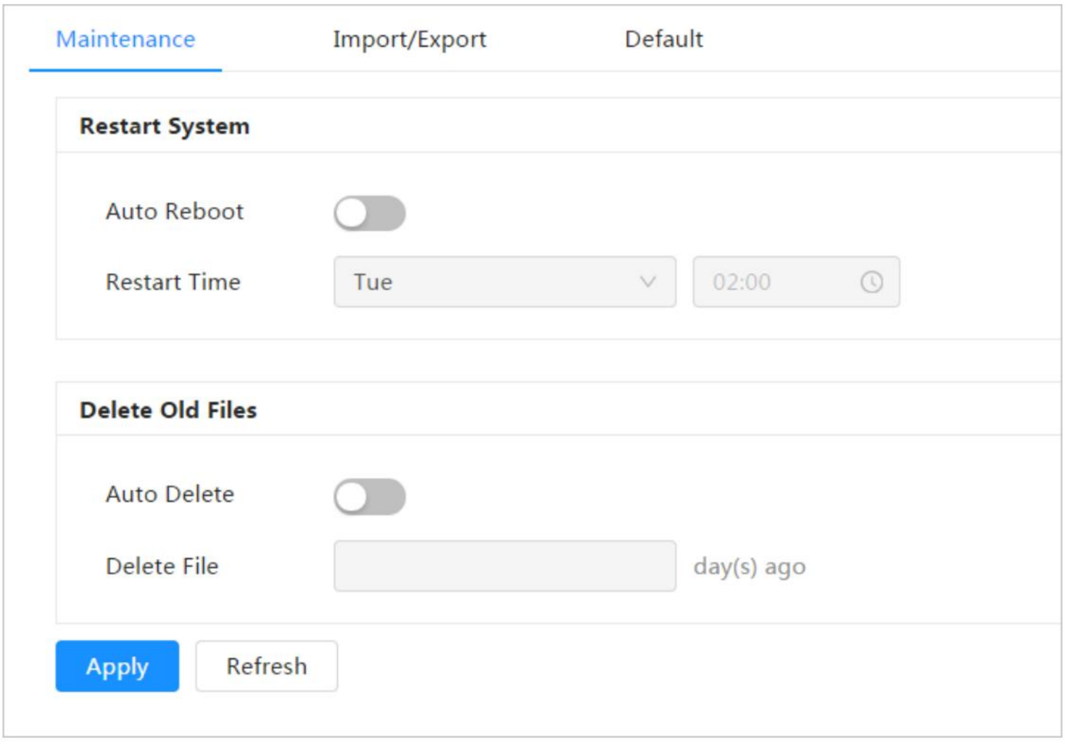
- View and analyze system logs, and fix errors in a timely manner.
- Back up system settings regularly.
- Restart your device and delete old files regularly.
- Update the firmware accordingly.

5.3.3.2Maintenance

You can restart the system manually and set the automatic restart time, in addition to automatically deleting old files. This feature is disabled by default.

Step 1: Select ⚙ > **System** (System) > **Account** (Account) > Maintenance (Maintenance).

Figure 5:21 maintenance



Restart System

Auto Reboot ○

Restart Time Tue 02:00

Delete Old Files

Auto Delete ○

Delete File day(s) ago

Step 2: Configure the parameters for automatic maintenance.

- Click (Restart ○ next to **Auto Reboot** in **Reboot System** System) and set the restart time; the system reboots automatically as the established time each week.
- Click ○ next to **Auto Delete** in **Delete Old Files** and set the time; The system automatically deletes old files according to the set time. The time range is 1 to 31 days.

When you enable and confirm the Auto **Delete** function , deleted files cannot be restored. Carry out the procedure carefully.

Step 3: Click on **Apply .**

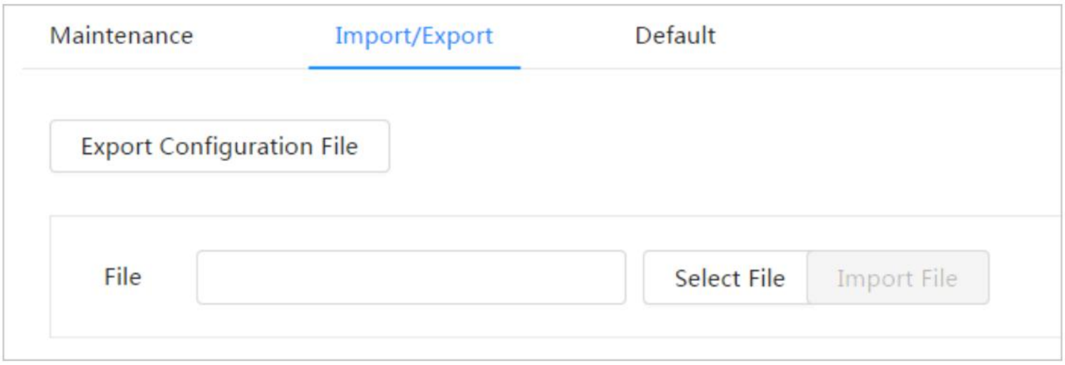
5.3.3.3Import/Export

- Export the system configuration file to backup system configuration.

- Import the system configuration file to perform quick configuration or recover system settings.

Step 1: Select ⚙ > **System** (System) > **Account** (Account) > Import/Export (Import/Export).

Figure 5-22 Import/Export



Step 2: Import and export.

- Import: Select the local configuration file and click **Import File** to import the local system configuration file to the system.
- Export: Click **Export Configuration File** to export the system configuration file to local storage.

5.3.3.4Default

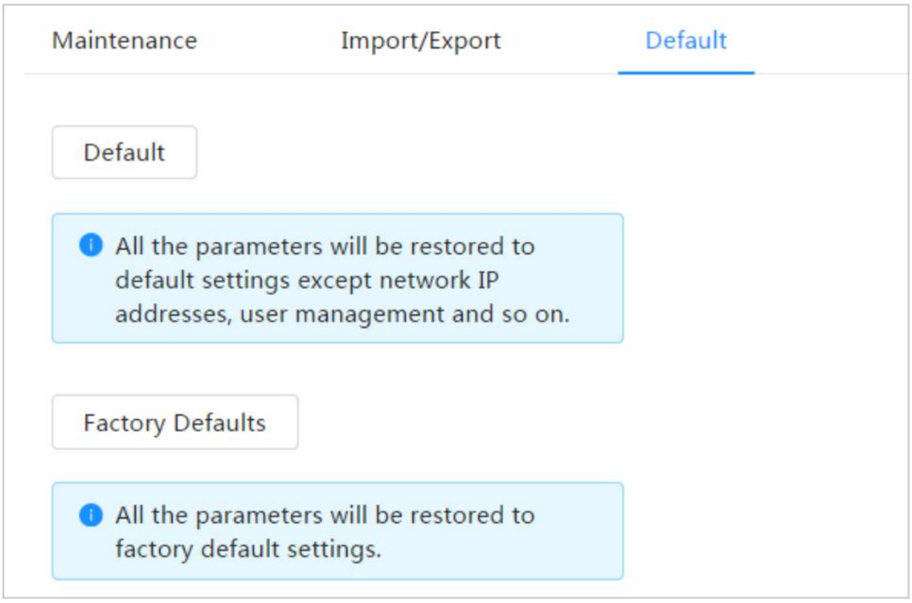
Restore the device to default settings or factory settings.
This feature will restore the device to default settings or factory settings.

Select ⚙ > **System** (System) > **Account** > (Account) **Default** (Defautl).

- Click **Default ,** then all settings except IP address and account will be reset to default values.

- Click **Factory Default** and all settings
  Settings will be reset to factory settings.

Figure 5:23 default



All the parameters will be restored to default settings except network IP addresses, user management and so on.

All the parameters will be restored to factory default settings.

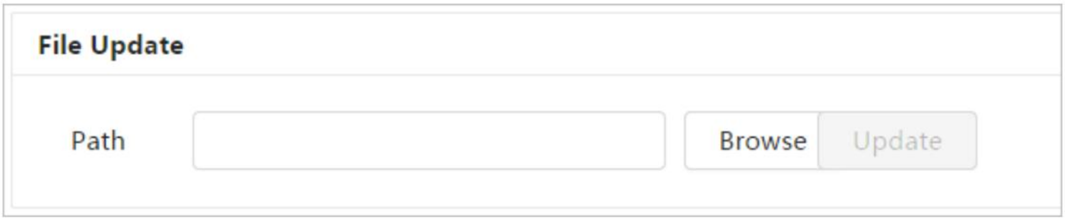
5.3.4Update

Updating to the latest version may improve camera features and stability.

If an incorrect update file has been used, restart the device; Otherwise, some functions may not work properly.

Step 1: Select ⚙ > **System** > **Upgrade .**

Figure :24 update



Step 2: Click **Browse** and then upload the update file.

The update file must be a .bin file.

Step 3: Click **Upgrade .**

The update will start running.

Appendix 1 Cybersecurity recommendations

Cybersecurity is more than a buzzword: it's something that belongs to all devices that are connected to the Internet. IP video surveillance is not immune to cyber risks, but taking basic steps to protect and harden networks and network-connected devices will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secure security system.

Mandatory measures you must take for basic computer network security:

1. **Use strong passwords**

   See the following tips for setting passwords:

   - The length cannot be less than 8 characters;
   - Include at least two types of characters: upper and lower case letters, numbers, and symbols;
   - Do not use the account name or the account name backwards.
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use continuous repeating characters, such as 111, aaa, etc.;

2. **Update firmware and client software promptly**

   - As per standard procedure in the technology industry, we recommend

     Keep your equipment firmware (such as NVR, DVR, IP camera, etc.) updated to ensure the system is equipped with the latest security patches and fixes. When the computer is connected to the public network, it is recommended to enable the "automatic update check" function to obtain timely information about firmware updates released by the manufacturer.

   - We suggest that you download and use the latest version of the client software.

Recommended steps to improve your computer's network security:

1. **Physical protection**

   We suggest that you physically protect your equipment, especially storage devices. For example, place the computer in a special computer room and closet and implement proper access control permission and key management to prevent unauthorized personnel from physically accessing the computer and damaging the hardware, unauthorized connection to computers. removable (such as a USB flash disk, serial port), etc.

2. **Change passwords periodically**

   We suggest that you change your passwords periodically to reduce the risk of passwords being guessed or cracked.

3. **Establish and promptly update the reset information passwords**

   The device supports the password reset function. Configure information related to timely password resets, including password protection questions and the end user's email address. If the information changes, please modify it immediately. When setting password protection questions, we suggest that you do not use those that can be easily guessed.

4. **Enable account lock**

   The account lock feature is enabled by default, and you

We recommend that you keep it activated to ensure account security. If an attacker tries to log in with the wrong password multiple times, the corresponding account and source IP address will be blocked.

5. **Change HTTP and other default service ports**

We suggest that you change the default HTTP and other service ports to any series of numbers between 1024 and 65535, reducing the risk that outsiders can guess which ports you are using.

6. **Enable HTTPS**

We suggest that you enable HTTPS so that it visits the web service over a secure communication channel.

7. **MAC address binding**

We recommend that you bind the IP and MAC address of the gateway to the computer, reducing the risk of ARP redirection.

8. **Assign accounts and privileges reasonably**

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

9. **Disable unnecessary services and choose safe modes**

If they are not necessary, it is recommended to disable some services such as SNMP, SMTP, UPnP, etc., to reduce the risks.

If necessary, it is strongly recommended that you use safe modes, including but not limited to the following services:

• SNMP: Select SNMP v3 and set strong encryption passwords and passwords authentication.

• SMTP: Select TLS to access the Mailbox server.

• FTP: Select SFTP and set strong passwords. • AP Access Point: Select WPA2-PSK encryption mode and set strong passwords.

10.**Encrypted audio and video transmission**

If your audio and video data content is very important or sensitive, we recommend that you use the encrypted transmission function to reduce the risk of audio and video data theft during transmission.

Remember: Encrypted transmission will cause some loss in transmission efficiency.

11.**Secure audit**

• Check online users: We suggest that you check online users periodically to see if anyone has logged in to the device without authorization. • Check device log: By checking the logs, you can know the IP addresses that have been used to log in to your devices and their key operations.

12.**Network registration**

Due to the limited storage capacity of the computer, the log stored is limited. If you need to save the log for a long time, we recommend that you enable the network log function to ensure that important logs are synchronized with the network log server for tracking.

13.**Create a secure network environment**

To better ensure equipment security and reduce potential cyber risks, we recommend:

- Disable the router's port mapping feature to prevent direct access to intranet devices from an external network.
- Partition and isolate the network according to the actual needs of the network. If there is no communication requirement between two subnets, we suggest that you use VLAN, network GAP and other technologies to partition the network, so as to achieve the effect of network isolation.
- Establish 802.1x access authentication system to reduce the risk of Unauthorized access to private networks.
- Enable the IP/MAC address filtering feature to limit the range of hosts allowed to access the device.

HELPING CREATE A SAFER SOCIETY AND A WAY OF SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address:ÿNo.1399ÿBin'anÿRoad,ÿBinjiangÿDistrict,ÿHangzhou,ÿP.ÿR.ÿChinaÿ|ÿWebsite: www.dahuasecurity.com | Zip code: 310053
Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel.: +86-571-87688883