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 defined meaning may appear in the manual.

signal words	Meaning
CAVEAT	Indicates a hazard of medium or low potential which, if not avoided, could result in minor injury or moderate.
CAUTION	Indicates a potential risk that, if not avoided, could cause property damage, loss of data, poor performance, or other unpredictable result.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provide additional information such as emphasis or complement to the text.

revision history

Version	Content of the review	Release date
V1.0.0	First pitch.	October 2020

About the manual

- The manual is just a reference. If you find any discrepancy between the manual and the actual product, the actual product shall prevail.
- We will not accept any responsibility for losses caused by using the device without following the instructions in the manual.
- The manual will be updated in accordance with the latest laws and regulations of the related jurisdictions. For more information, please refer to the printed manual, CD-ROM, QR code or our official website. In the event of a discrepancy between the printed manual and the electronic version, the electronic version will prevail.
- All designs and software included herein are subject to change without prior written notice. Product updates may cause discrepancies between the actual product and the manual. Contact customer service requesting the updated program and supplementary documentation.
- Even so, there may be some deviation in technical data, functions and description of operations, or printing errors. If there is any doubt or controversy, we reserve the right of final explanation.
- Please update the reader software or try other conventional reader software if 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 dealer or customer service if you have problems using the device.
- If there are uncertainties or controversies, we reserve the right of final explanation.

Safety Warnings and Precautions

important

electrical safety

- All instructions for use and installation must be carried out in accordance with the electrical safety regulations 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 source requirement in accordance with IEC60950-1. Power supply requirements are indicated on the device label.
- Make sure the power supply is adequate before using the device.
- An easily accessible disconnect device must be incorporated into the building installation wiring.
- Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the device.

operating environment

- Do not point the device directly at strong light when focusing, such as lamplight and sunlight; otherwise, it may cause excessive brightness or light streaks, 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 internal components.
- Please keep the indoor device away from rain or moisture to avoid fire or lightning.
- Maintain good ventilation to prevent heat buildup.
- Transport, use and store the device within the permissible 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, store it in the factory package or use equivalent materials.
- Install the device in a place that can only be accessed by professional personnel with relevant knowledge of safety protections and warnings. Failure to do so may cause damage to non-professionals entering the installation area when the device is operating normally.

Use and daily maintenance

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

- Carefully follow the instructions in the manual when performing any device disassembly operations; 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 condensation mist on the lens after taking the product out of the box or if the desiccant turns green. (Not all models include desiccant.)

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

- You can clean the casing of the device with a soft, dry cloth, and for tougher stains, use the cloth with a mild detergent. To avoid possible damage to the coating of the device casing which could cause a decrease in performance, do not use volatile solvents such as alcohol, benzene, white spirit, etc. to clean the device casing, nor can you use a strong abrasive detergent .
- The domed cover is an optical component. Do not touch or clean the cover with your hands directly during installation or operation. To remove dust, grease, or fingerprints, wipe gently with diethyl-moistened oil-free cotton or a soft, damp cloth. You can also remove dust with an air blower.

CAVEAT

- Strengthen the 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 of the computer network. For some devices with old firmware versions, the ONVIF password will not be changed automatically along with system password change, and you need to update the firmware or manually update the ONVIF password.

- Please use components or accessories supplied by the manufacturer, and make sure that professional engineers perform the installation and maintenance of the device.
- The image sensor surface must not be exposed to laser beam radiation in an environment where a laser beam device is used.
- Do not provide two or more power sources for the device unless otherwise specified. Failure to follow these instructions could damage the device.

Index of contents

1 Overview

1.1 Introduction

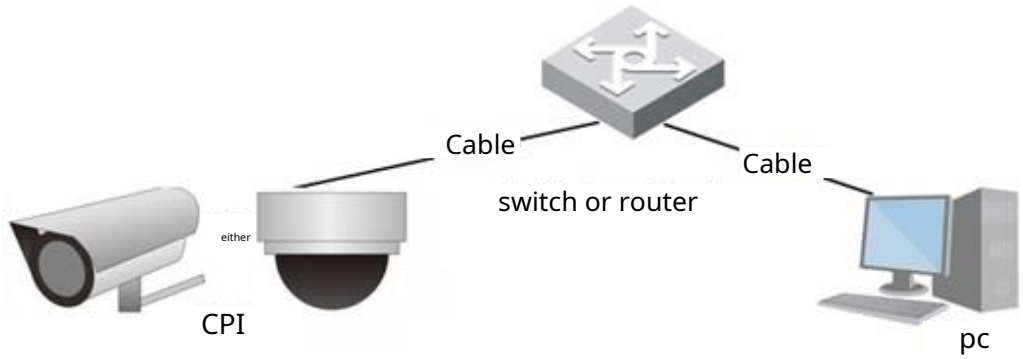
An IP camera (Internet Protocol camera), is a type of digital video camera that receives control data and sends image data over the Internet. They are commonly used for surveillance and do not require a local recording device, just a local area network.

The 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 the 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 overall IPC network



Obtain the IP address by searching in the ConfigTool, and then you can start to access 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 setup flow

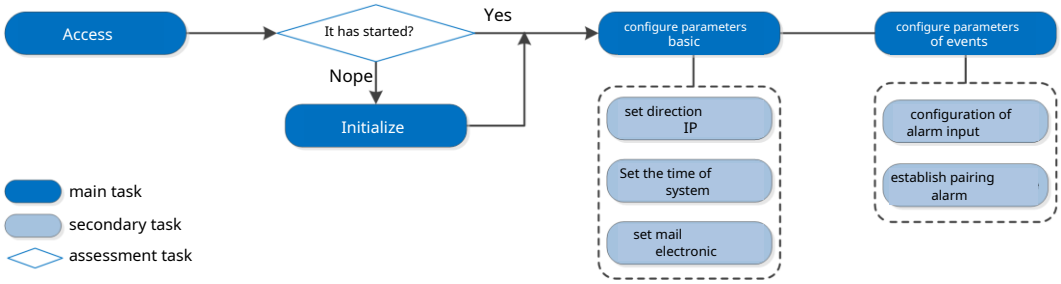


Table 1:1 flow description

Setting		Description	Reference
Access		Open the IE browser and input the IP address to log in the web interface. The IP address of the camera is 192.168.1.108 by default.	" 3 Access".
initialization		Start the camera when you use it for the first time.	" 2 Initializing the device"
parameters basic	IP adress	Please change the IP address according to the network planning to use the product for the first time or during the network setting.	" 5.1.1 TCP/IP"
	date and hour	Set the date and time to make sure the recording time is correct.	" 5.3.1.2 Date and hour"

two device initialization

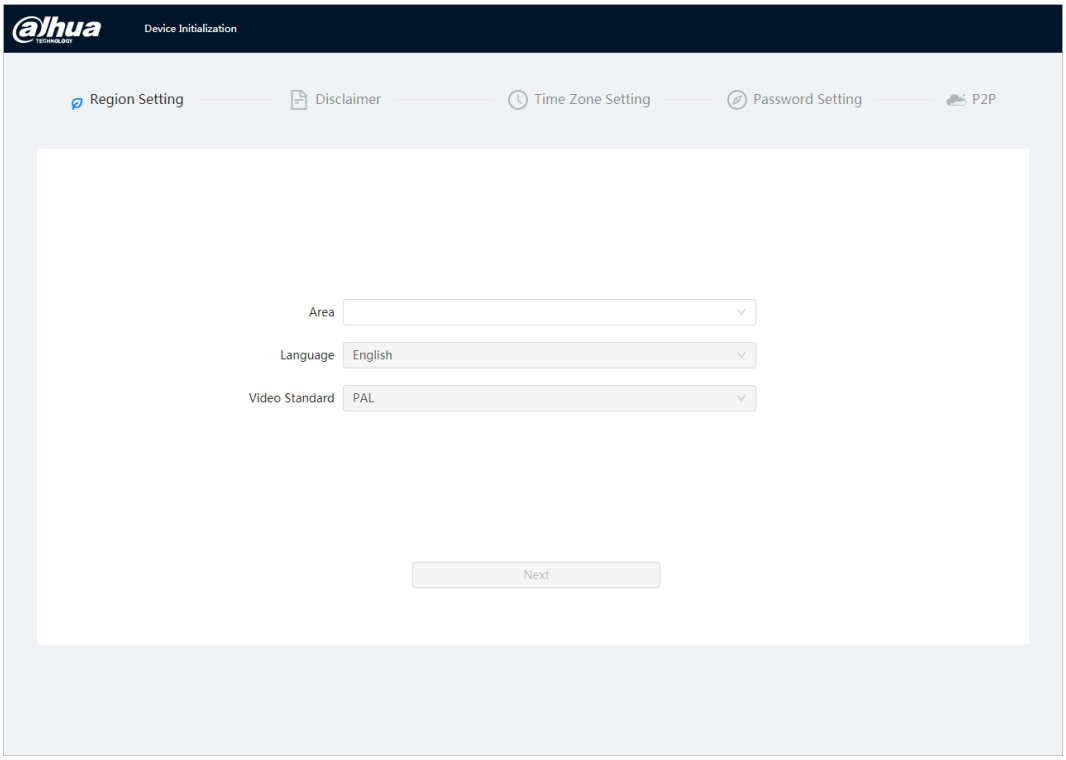
It is necessary to start the device for the first use. This manual is based on the operation of the web interface. You can also start the device via ConfigTool or NVR.

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

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

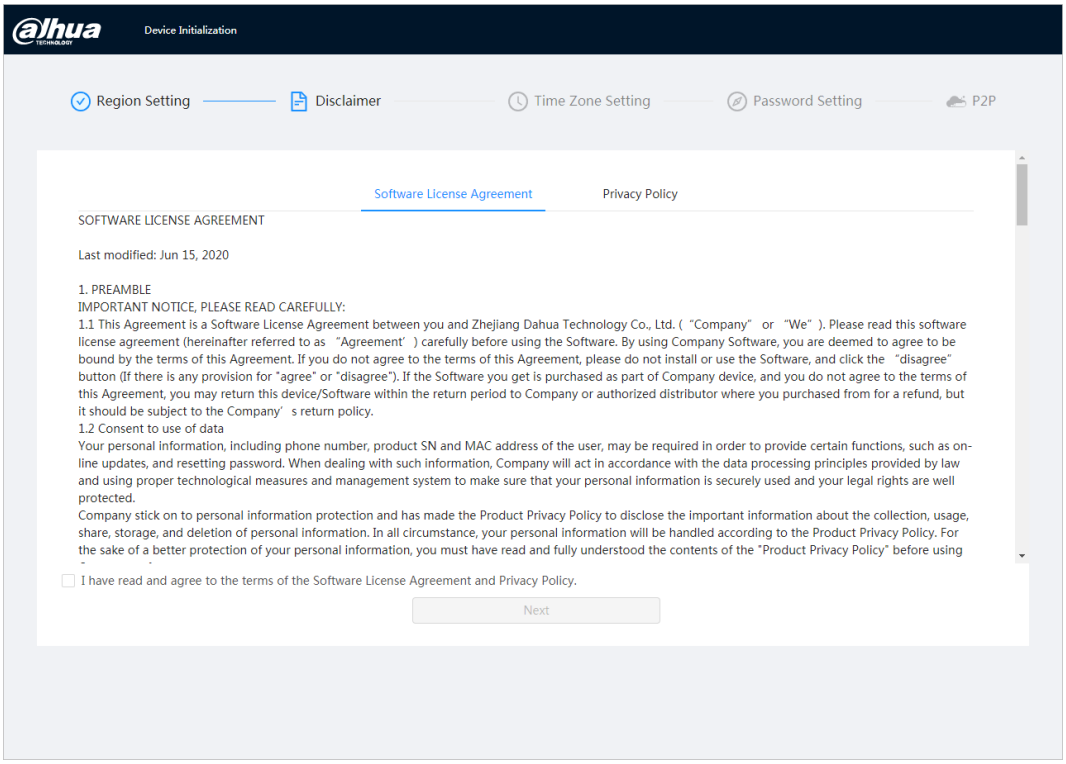
The IP is 192.168.1.108 by default.

Figure 2:1 region settings



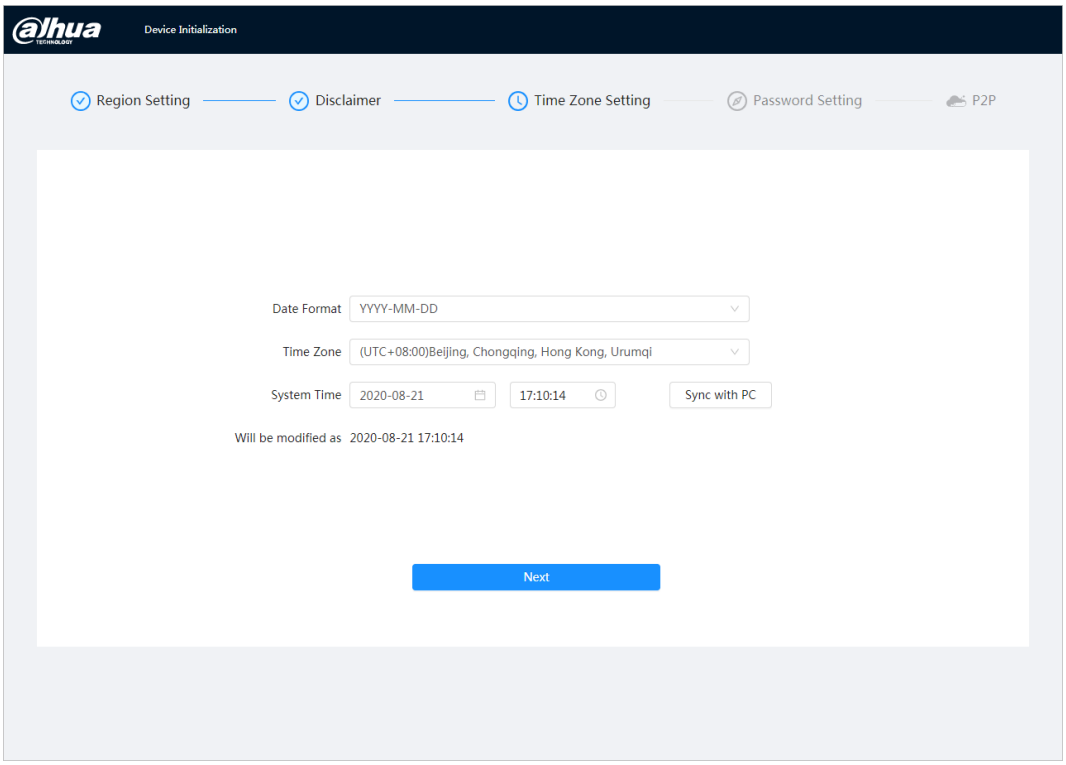
Step 2: Please select the area, language and video standard according to the actual situation, and then click**Following**(Next).

Figure 2:2 Disclaimer



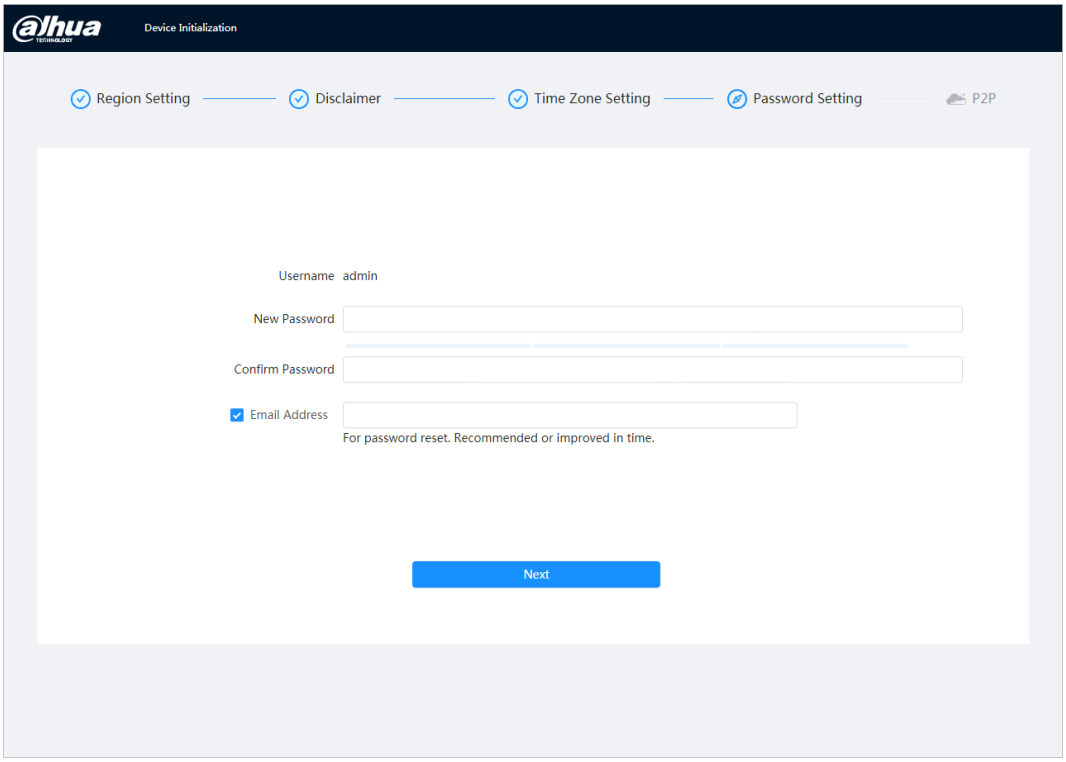
Step 3: Select the check box**I have read and accept the terms of the Software License Agreement and the Privacy Policy**(I have read and agree to the terms of the Software License Agreement and Privacy Policy), and then click**Following** (Next).

Figure 2:3 Time zone settings



Step 4: Set the time parameters, and then click**Following**(Next).

Figure 2:4 password settings



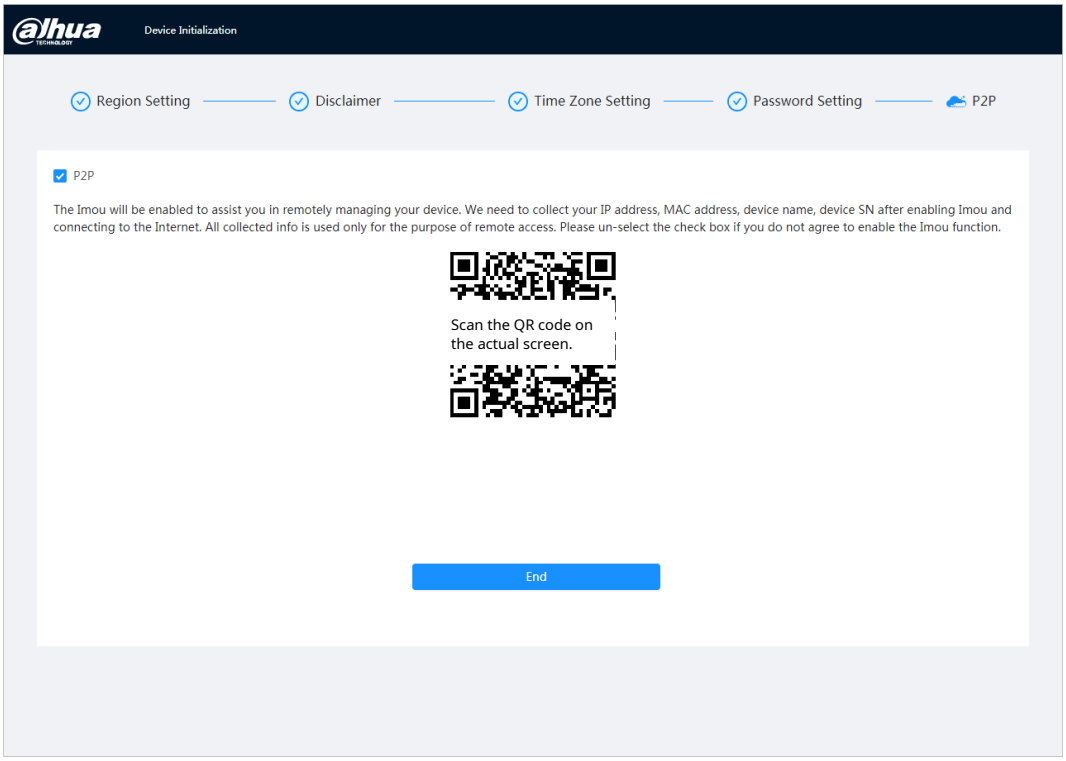
Step 5: Set the password for the administrator account.

Table 2:1 description of password settings

Parameter	Description
Username	The default username is admin.
Password	Password must consist of 8 to 32 non-empty characters and contain at least two types of characters including uppercase, lowercase, numbers, and special characters (excluding ' " ; : &). Set a password with a height security level according to the password security notice.
Confirm Password	
Email saved	Enter a password reset email address 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 on**Following**(Next) and then the interface will appear**P2P**.

Figure 2–5 P2P



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 you can log in to the web interface. To know the details, see " 2 device initialization ".
- When starting the camera, please keep the PC IP and device IP in the same network.
- Follow the instructions to download and install the plugin for the first start of session.

Step 1: Open the 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.

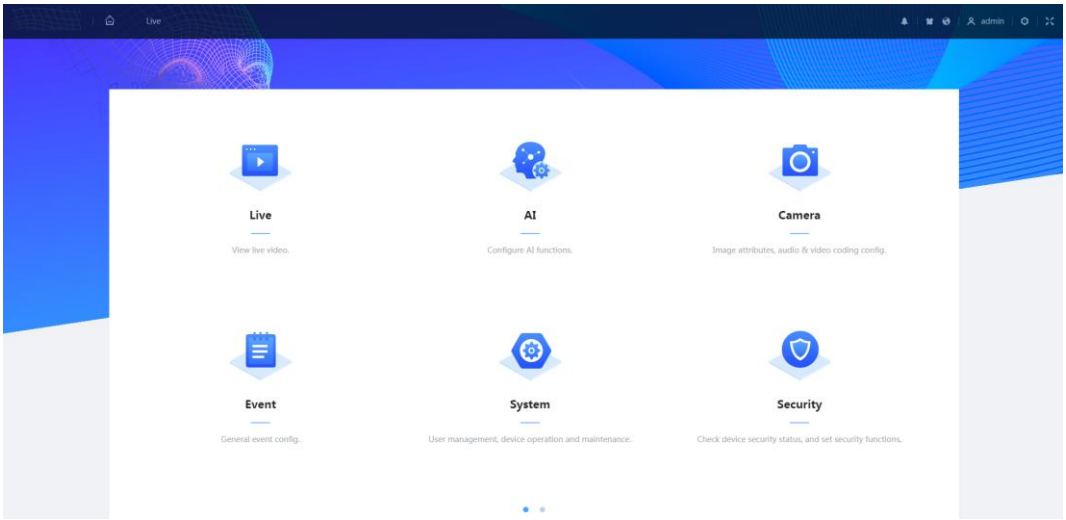
Click on**Forgot password?**(Forgot password?) to reset the password to through the email address that was established at the beginning. To know the details, please refer to " 3.2 reset the password ."

Figure 3–1 Login

Step 3: Click on**Log in**(Login). interface will appear **Live**(live). Click the interface to pop up the main interface. in the upper left corner of

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

Figure 3–2 Main Screen



- Direct: view the monitoring image in real time.
- AI: Set the AI features of the camera.
- Camera: Configure the camera parameters, including image parameters, encoder parameters, and audio parameters.
- Event: Configure general events, including exception for alarm linkage, video detection, and audio detection.
- System: Set system parameters, including general, date and time, account, security, PTZ setting, default, import/export, remote, auto maintenance, and update.
- Security: Check the security status of the device and configure security features.
- Recording: Play or download recorded videos.
- Image: Play or download image files.
- Report: Find the AI event 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 entered email address, which can be used to reset the password.

Previous requirements

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

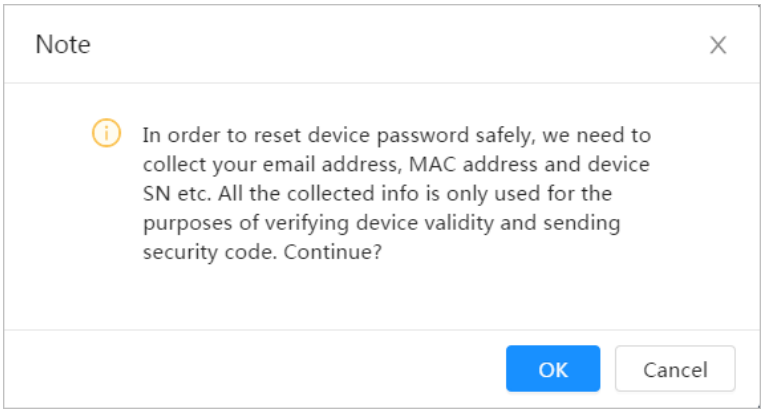
Process

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

Figure 3–3 Login

Step 2: Click on**Forgot password?**(Forgot password?) to reset the password via the email address that was set at startup.

Figure 3–4 Login



4 Straight

This section introduces the interface design and function configuration.

4.1 Live interface

Sign in or click the tab**Live**(live).

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

Figure 4:1 live (single channel)

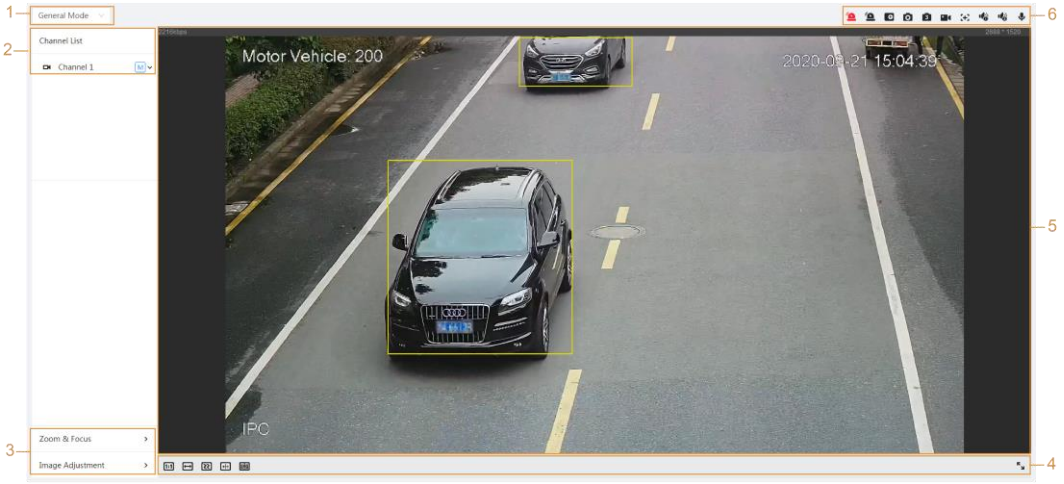


Figure 4:2 live (multi-channel)

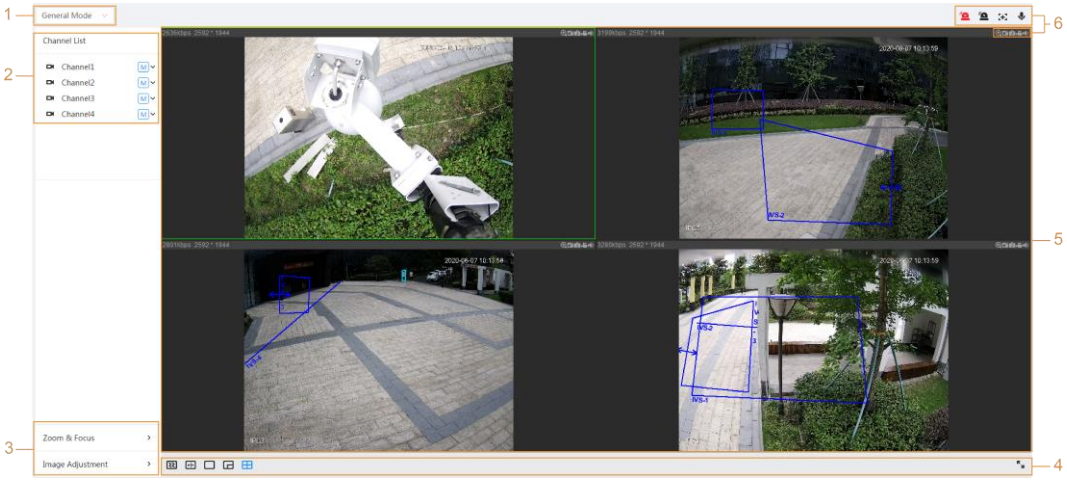


Table 4:1 description of the function bar

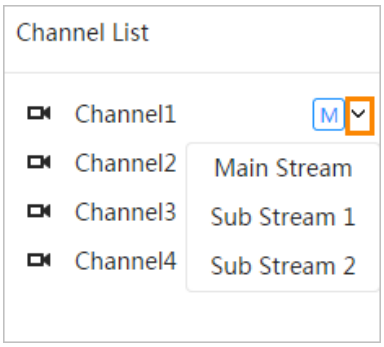
No.	Function	Description
1	display mode	You can select the display mode between **general mode**(General Mode) and**face mode** (FaceMode).
two	channel list	Show all channels. You can select the channel as needed and set the type of transmission.

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

4.2 Encryption Settings

Click on and then select the stream as needed.

Figure 4:3 code bar



- **main stream:**It has high bit and image transmission value with high resolution, but also requires high bandwidth. This option can be used for storage and monitoring.
- **Secondary transmission:**It has a small bit rate and fluent image, and requires less bandwidth. This option is normally used to replace the main stream when the bandwidth is not enough.
- M means that the current stream is the main stream; S1 means that the current stream is sub stream 1; means the current stream is sub stream 2.

5 config.

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

5.1 Network

This section introduces the network settings.

5.1.1 TCP/IP

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

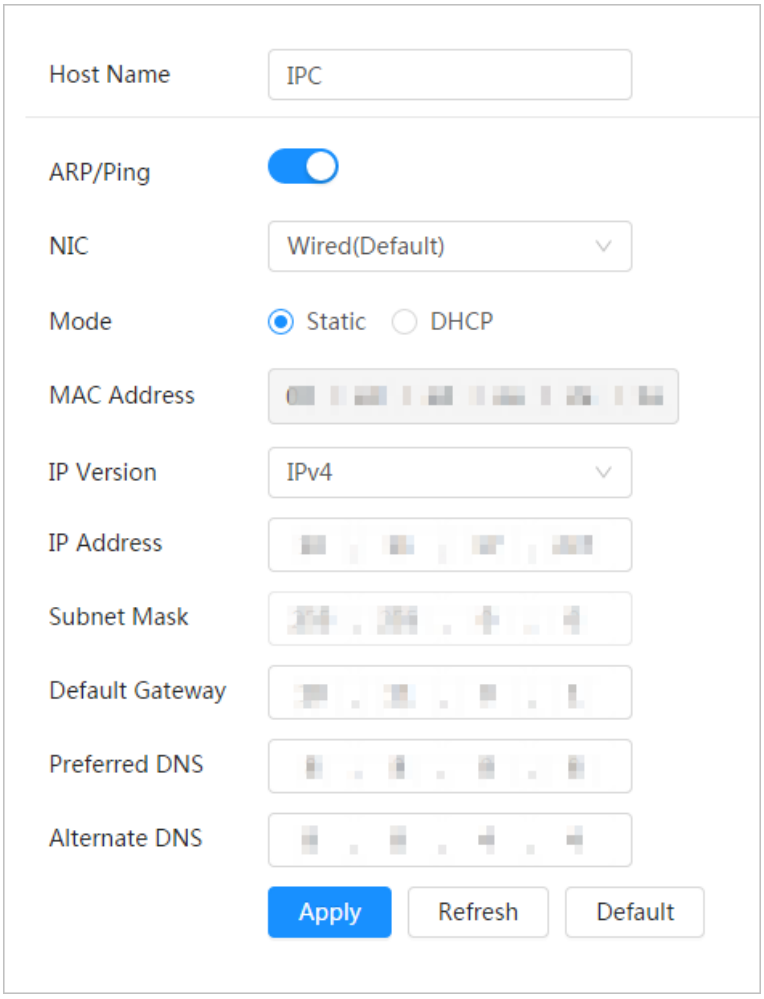
Previous requirements

The camera has connected to the network.

Process

Step 1: select  > **Net**(network) >**TCP/IP**(TCP/IP).

Figure 5–1 TCP/IP



Step 2: Configure the TCP/IP parameters.

Table 5:1 description of TCP/IP parameters

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

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>ARP/Ping</td><td>Click on  to enable ARP/Ping and configure the service of IP address. Obtain the MAC address of the camera so that you can change and configure the IP address of the device with the ARP/ping command.
This feature is enabled by default. During the reboot, you will have no more than 2 minutes to set the IP address of the device using a ping packet with a certain length; The server will shutdown in 2 minutes or shutdown immediately after the IP address is set successfully. If it is not enabled, the IP address cannot be set with the ping packet.

Demonstration of how to configure IP address with ARP/Ping.
1. Keep the camera to be configured and the PC within the same local network, and then obtain a usable IP address.
2. Obtain the MAC address of the camera from the device label.
3. Open the command editor on the PC and enter the following 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. Reboot the camera.
5. Check the PC command line; if the informational message appearsReply from 192.168.0.125...(Reply from 192.168.0.125...), the setup will be done successfully, and you can turn off the camera.
6. Enter http://(IP Address) in the browser's address bar to log in.</td></tr>
<tr><td>IAS</td><td>Select the Ethernet card to be configured and the default isWith cable(Wired).</td></tr>
</table>

Parameter	Description
Mode	The way the camera gets the IP: ● **static** set the**IP adress**(IP address), the**subnet mask**(Subnet Mask) and the**Default Gateway**(Default Gateway) manually, and then click**Save**(save); The login interface with the configured IP address will appear. ● **DHCP** When there is a DHCP server on the network, select**DHCP**and the camera will get the IP address automatically.
MAC address	Shows the MAC address of the host.
IP version	select**IPv4**either**IPv6**.
IP adress	When you select**static**(Static) in**Mode**(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 than the IP address.
Subnet mask	
access portal predetermined	
preferred DNS	Preferred DNS IP address
alternate DNS	Alternate DNS IP address

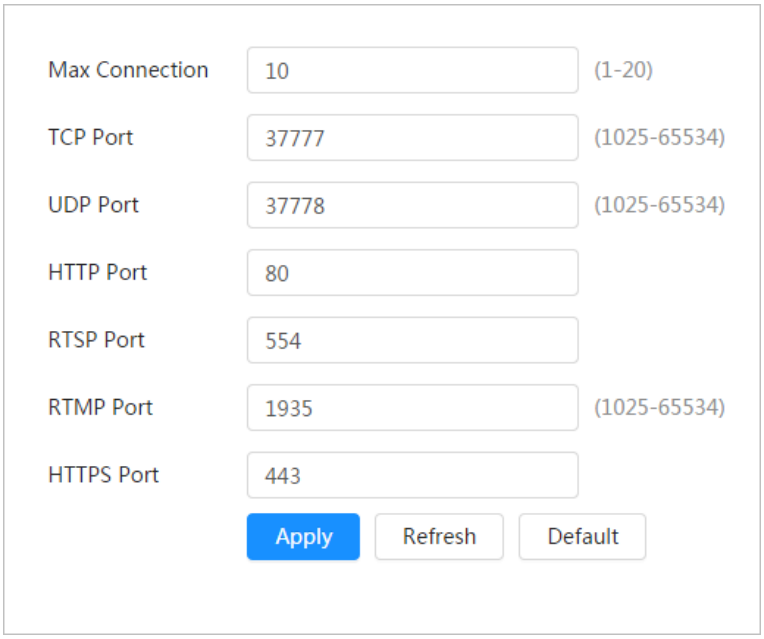
Step 3: click on**Apply**(apply).

5.1.2 Port

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 > **Net**(network) >**TCP/IP**(TCP/IP).

Figure 5:2 port



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 port parameter description

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

Parameter	Description
RTSP port	● Streaming protocol port, and the default is 554. If you play the live view 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 bit rate in the URL, and also the username and password if required. URL format example: rtsp://username: password@ip :port/cam/realmonitor?channel=1&subtype=0 Between 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 if the value is the default 554 value. ● 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 main transmission (subtype = 0) and 1 means secondary transmission (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
RTMP port	Real-time messaging protocol. The port that RTMP provides service. It is 1935 by default.
HTTPS port	HTTPS communication port. It is 443 by default.

Step 3: click on**Apply**(apply).

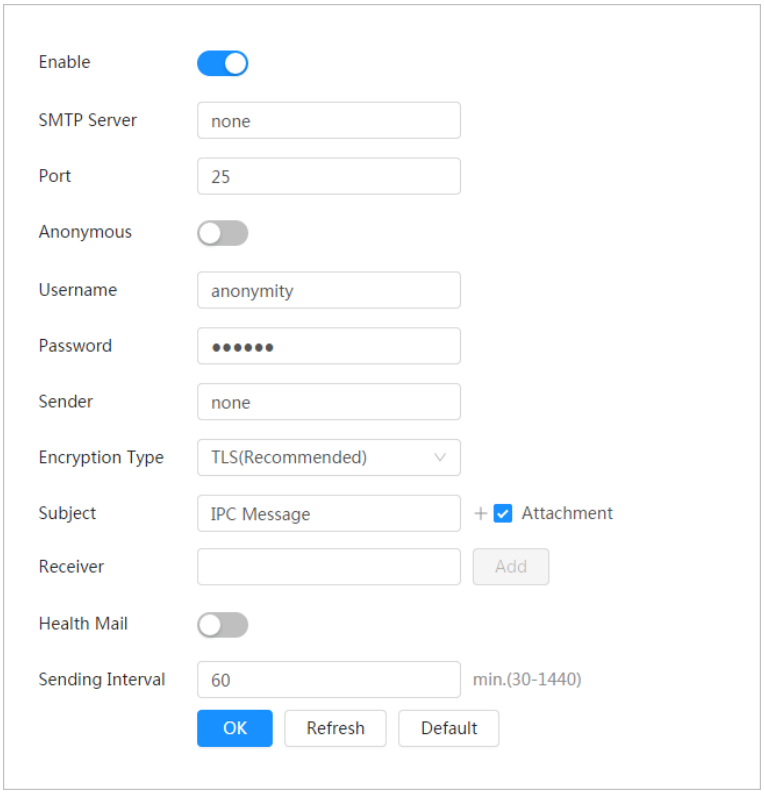
The configuration of**Connections Max.**(Max Connection) is effective immediately, and the others will take effect after the reboot.

5.1.3 Email

Configure the email parameter and enable email binding. The system sends an email to the defined address when the corresponding alarm is triggered.

Step 1: select > **Net**(netwok) >**Email**(E-mail).

Figure 5:3 email



Step 2: Click on to enable the function.

Step 3: Configure email parameters

Table 5:3 description of email parameters

Parameter	Description	
SMTP server	SMTP server address	For details, see Table 5:4.
Port	The port number of the SMTP server.	
Username	The SMTP server account.	
Password	The password of the SMTP server.	
Anonymous	Click on and the sender information will not be displayed in the email.	
Sender	Sender's email address.	
encryption type	Select between**None**(None)**SSL**Y**TLS**. For details, see Table 5:4.	
Title	Please enter a maximum of 63 characters in Chinese, English and Arabic numerals. Click to select the type of title, included**device name**(Device Name), the **Device identification**(Device ID) and the**event type** (EventType); You can set a maximum of 2 titles.	
Attachments	Check the checkbox to be able to attach files in the email.	

Parameter	Description
Addressee	● Email address of the recipient. Supports 3 addresses at most. ● After entering the recipient's email address, the button will appear.**Try**(Test). Click on **Try**(Test) to test if emails can be sent and received correctly.
mail from verification	The system sends a test email to verify that the connection has been configured correctly. Click configure the**shipping interval**(Y Sending Interval), and then the system will send the test email at the set interval.

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

Table 5:4 Description of Mailbox settings

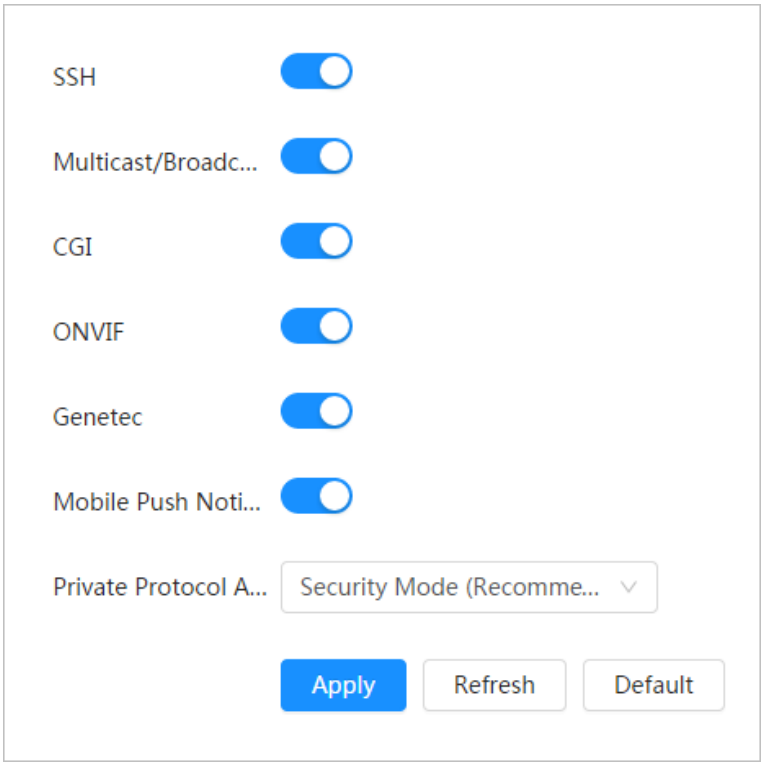
mailbox	SMTP server	Authentication	Port	Description
gmail	smtp.gmail.com	SSL	465	● You need to have the service activated SMTP in your mailbox. ● Authentication code is required. The mail password email does not apply. Authentication code: The code you receive when enabling the SMTP service.
		TLS	587	

Step 4 : Click on**Apply**(apply).

5.1.4 Basic service

Configure basic services to improve network and data security. Step 1: Select > **Net**(network) >**basic service**(BasicService).

Figure 5:4 basic service



Step 2: Enable the basic service based on actual needs.

Table 5:5 description of basic service parameters

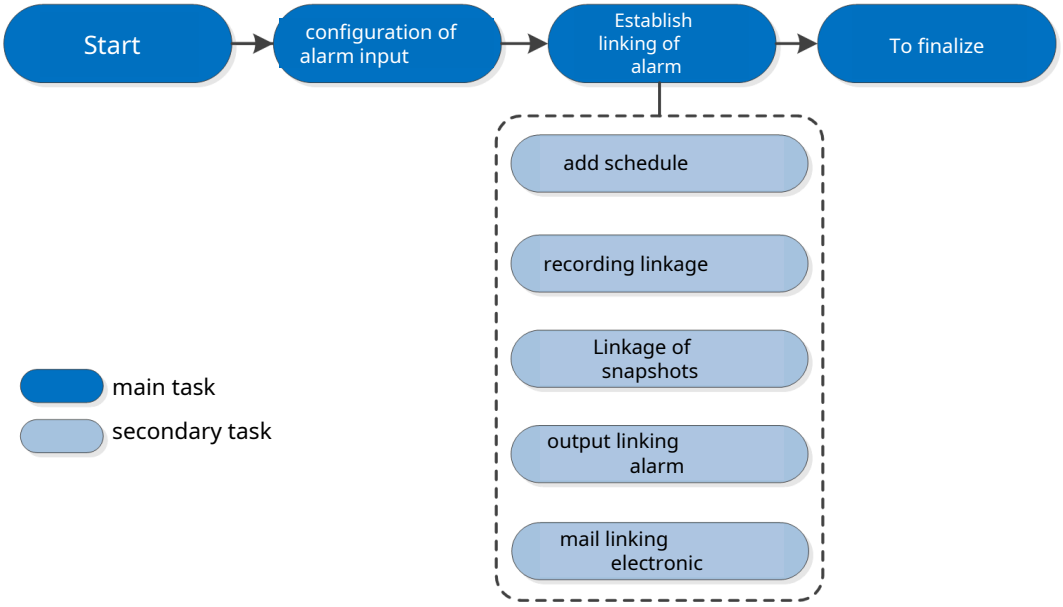
Function	Description
SSH	You can enable SSH authentication to manage security.
Search multicast/broadcast	Please enable this function, and then when multiple users are watching the video image of the device simultaneously through the network, they can find your device with the multicast/broadcast protocol.
CGI	Please enable the feature, and then other devices can access through this service. The feature is enabled by default.
Onvif	
Genetec	
* * * * * * * Automatic notifications of the mobile*******	Please enable this function, and then the system will send the snapshot 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**(Security Mode)y**compatible mode**(Compatible Mode). Security mode is recommended.

Step 3: click on**Apply**(apply).

5.2 Event

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

Figure 5:5 alarm event configuration



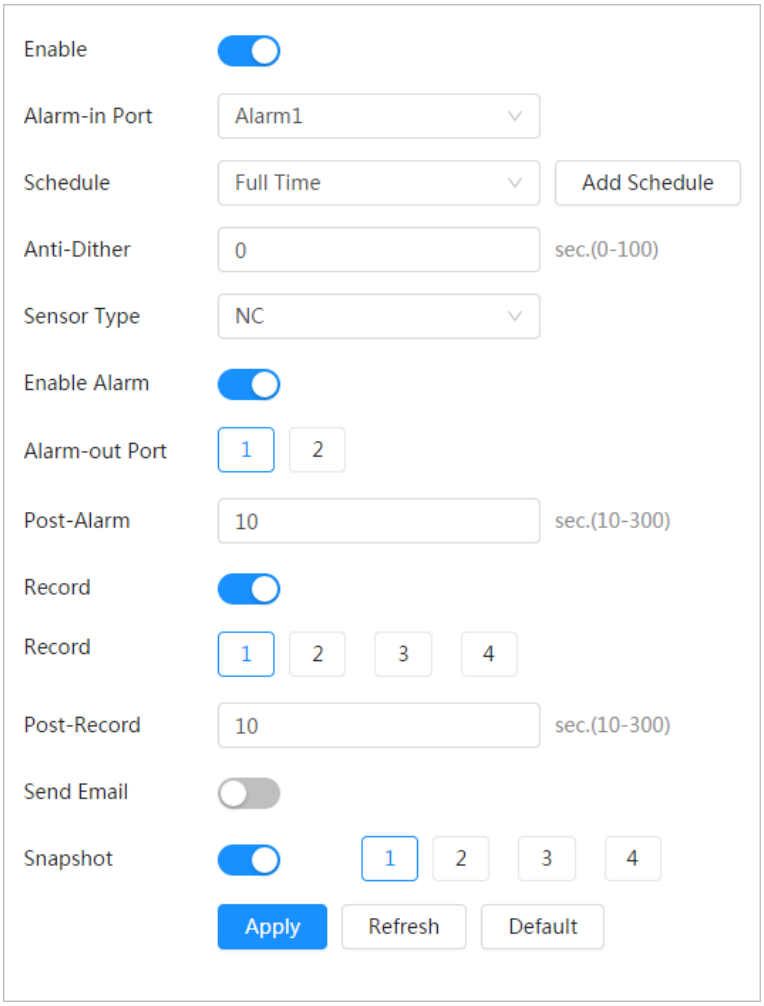
5.2.1Alarm input configuration

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

Step 1: select > **Event**(event) >**Alarm**(alarm).

Step 2: Click on beside**Enable**(Enable) to enable alarm linkage.

Figure 5–6 Alarm Linkage



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

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

Step 4: Select the schedule and arming periods and the 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**(Add Schedule) to add a new schedule. For details, see " 5.2.2.1 Add Schedule."

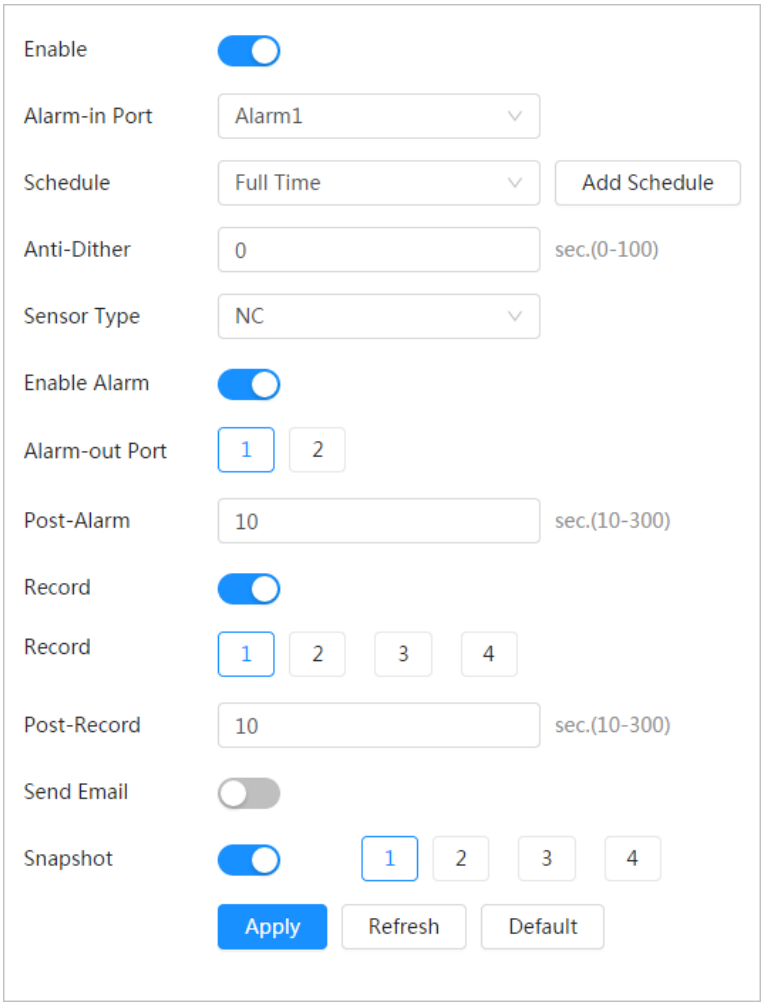
Step 5: click on**Apply**(apply).

5.2.2Set alarm linkage

When setting alarm events, select alarm links (such as log, snapshot). When the corresponding alarm is triggered in the set arming period, the system will issue an alarm.

Select > **Event**(event)>**Alarm**(Alarm), beside**Enable**(Enable) for enable the linking of alarms.

Figure 5–7 Alarm Linkage

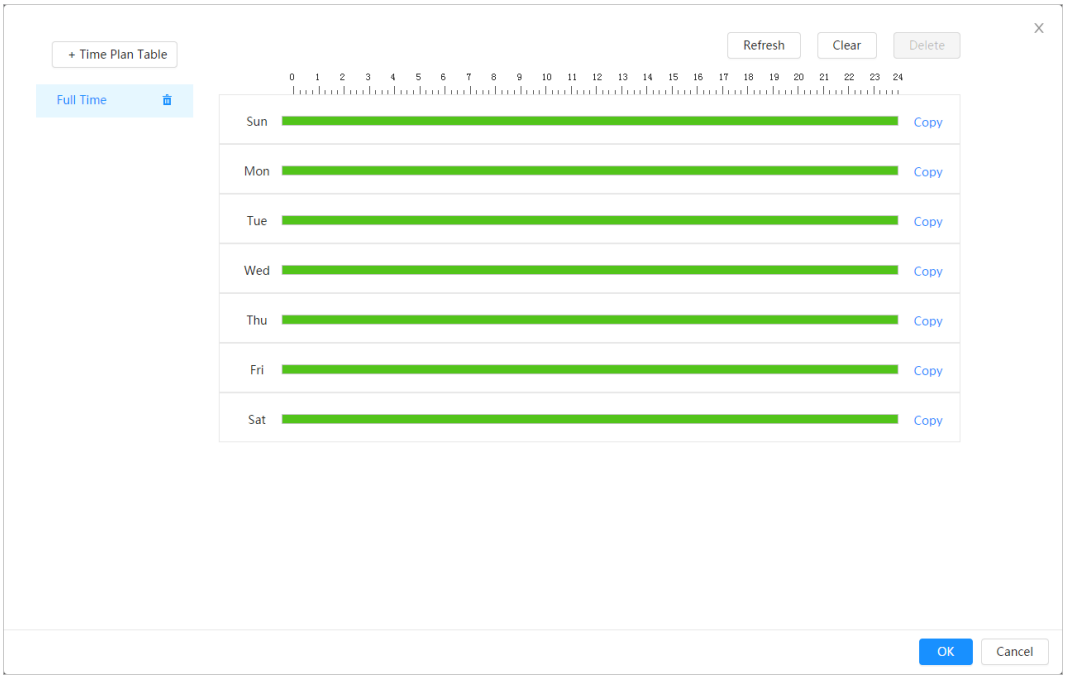


5.2.2.1Add schedule

Set arming periods. The system only performs the corresponding binding action in the configured period.

Step 1: Click on**add schedule**(Add Schedule) next to**Programming** (Schedule).

Figure 5:8 programming



Step 2: Click and drag the left mouse button on the timeline to set arming periods. Alarms will go off at the time period in green on the timeline.

- Click on**Copy**(Copy) next to a day, and select the days you want to copy in the request interface; you can copy the settings to the selected days. Select the check box**Select all**(Select All) to select all days to copy the settings.

- You can set 6 time periods per day. Step 3: click on**Apply**(apply).

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

Can:

- Double click on the table name to edit it.
- Click to delete the history as required.

5.2.2.2Record 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 setting**post recording**(Post Record).

Previous requirements

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

Set recording linkage

In the interface of**Alarm**(Alarm), click to enable recording linkage, select the channel as needed and set**post recording**(Post-Record) for

set alarm linkage and recording delay.

Once the**post recording**(Post-Record), alarm recording continues for a long period after the alarm ends.

Figure 5:9 recording link

5.2.2.3 Linking Snapshots

Once the snapshot linkage is set, the system can trigger the alarm and automatically take photos when an alarm is triggered.

Previous requirements

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

Set recording linkage

In the interface of**Alarm**(Alarm), click snapshot and to enable linking select the channel as required.

Figure 5:10 snapshot link

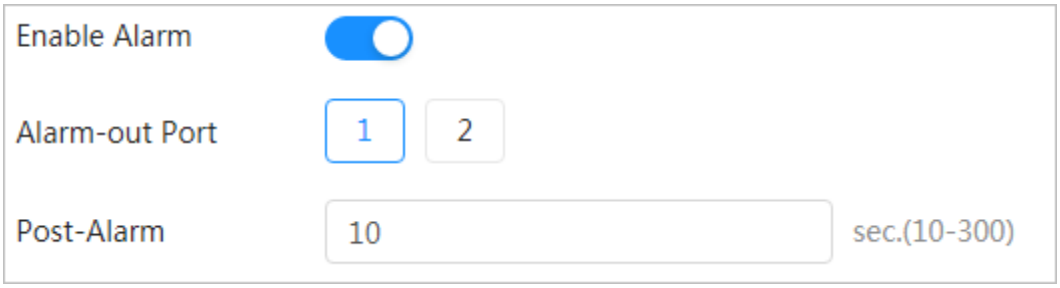
5.2.2.4Alarm output linkage

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

In the interface of**Alarm**(Alarm), click to enable output binding of alarm, select the channel as needed, and then set**Post alarm** (Post alarm).

When the alarm delay is set, the alarm continues for a long period after the alarm ends.

Figure 5:11 alarm output link



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

5.3 System

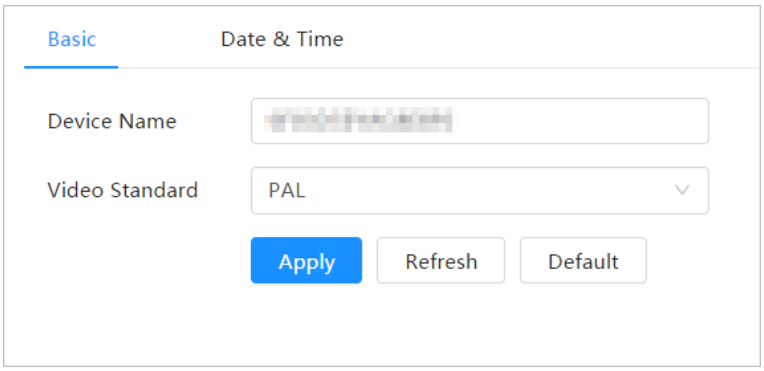
This section introduces the system settings, including general, date and time, account, security, PTZ setting, default, import/export, remote, auto maintenance, and update.

5.3.1 General

5.3.1.1Basic

You can set the device name, language and video standard. Step 1: Select > **System**(System) >**General**(General) >**Essential**(BASIC).

Figure 5:13 basic



Step 2: Set the general parameters

Table 5:6 description of general parameters

Parameter	Description
Name	Enter the device name
video standard	Select the video standard from**PAL**Y**NTSC**.

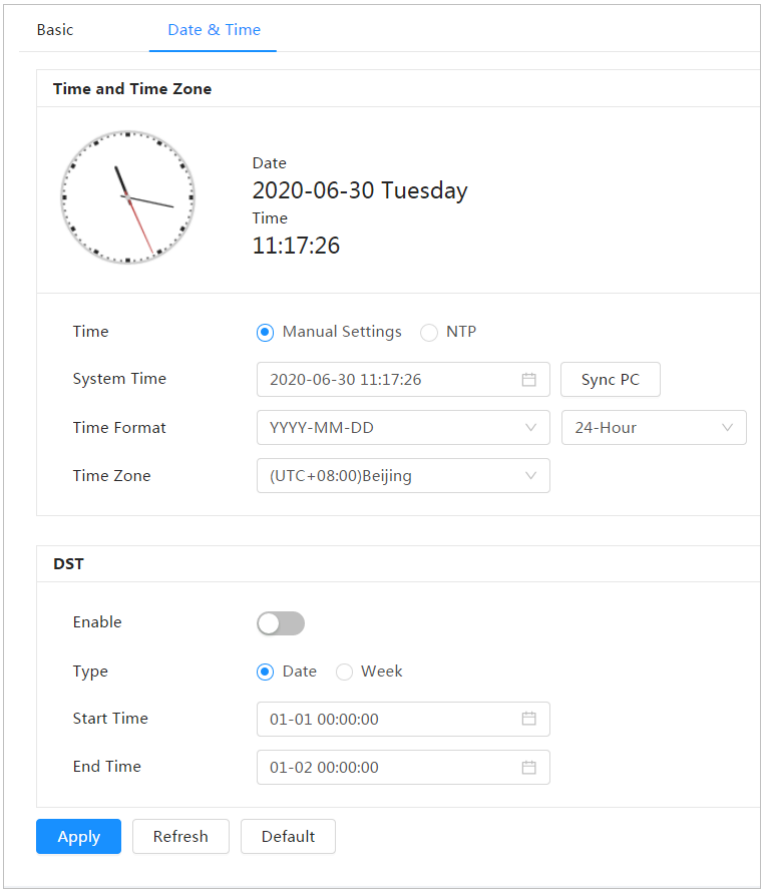
Step 3: click on**Apply**(apply).

5.3.1.2 Date and time

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

Step 1: select > **System**(System) >**General**(General) >**Essential**>**Date and Time** (Date & Time).

Figure 5:14 date and time



Step 2: Set the date and time parameters.

Table 5:7 description of date and time parameters

Parameter	Description
Format of the date	Set the date format.

Parameter	Description
Hour	● **Manual configuration:**set the parameters manually. ● **NTP:**By selecting NTP, the system synchronizes the time with the Internet server in real time. You can also enter the IP address, time zone, port and interval 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 hours**(24-Hour).
Time zone	Set the time zone in which the camera is located.
Current time	Set the system time. Click on**Synchronize PC**(Sync PC) and the system will adopt the PC time.
DST	Enable DST as necessary. Click on , and set the start and end time of the summer time with**Date**either**Week**(Date or Week).

Step 3: click on**Apply**(apply).

5.3.2 Account

You can manage users, such as add, delete or edit 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, consisting of number, letter, underscore, hyphen, period, and @.
- Password must consist of 8 to 32 non-empty characters and contain at least two types of characters including uppercase, lowercase, numbers, and special characters (excluding ' " ; : &).
- You can have 18 users and 8 groups at most.
- You can manage users through a single user or group, and duplicate user names or group names are not allowed. A user can only be in one group, and users in the group can have permissions within the group's range of authority.
- Online users cannot edit their own permission.
- There is a default administrator who has maximum authority.
- select**anonymous login**(Anonymous Login) and then log in with just the IP address instead of the username and password. Anonymous users are only allowed to preview. During anonymous login, click**Sign off**(Logout) and then you can log in with another username.

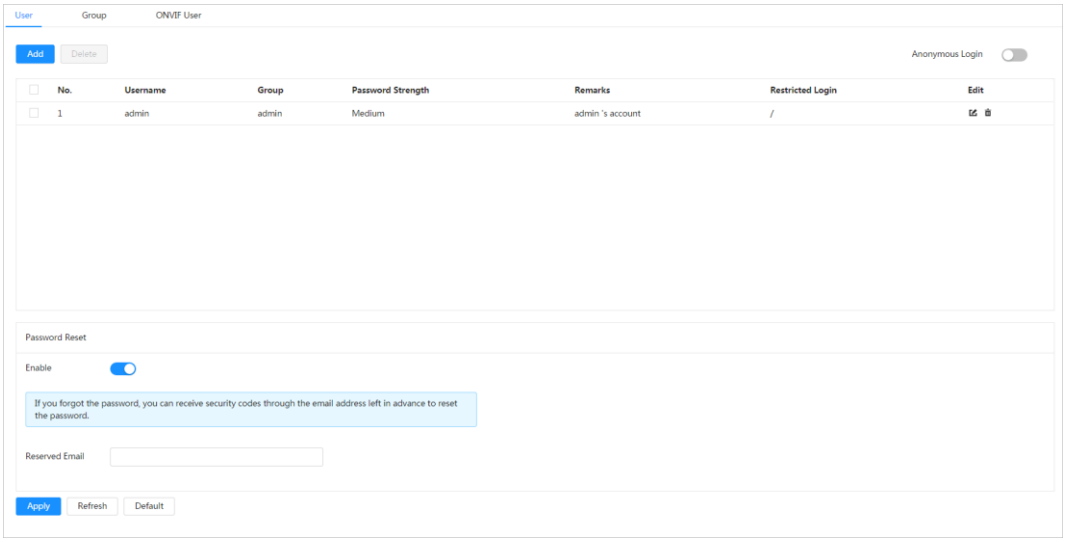
5.3.2.1 User

5.3.2.1.1 Add users

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

Step 1: select > **System**(System) >**Bill**> (Account)**User**(user).

Figure 5:15 user



Step 2: click on**Add**(add).

Figure 5:16 add user (system)

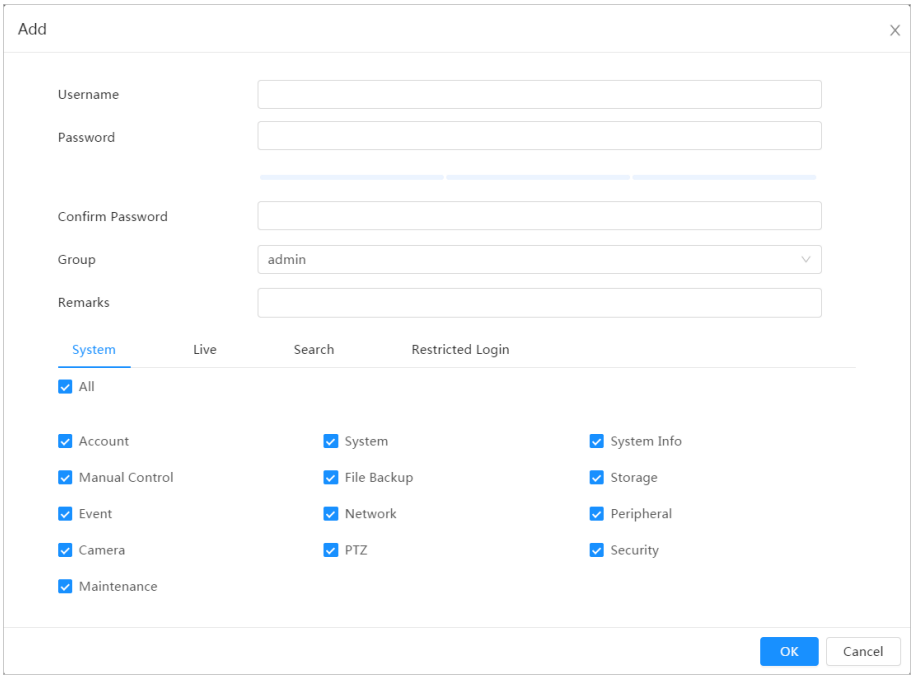
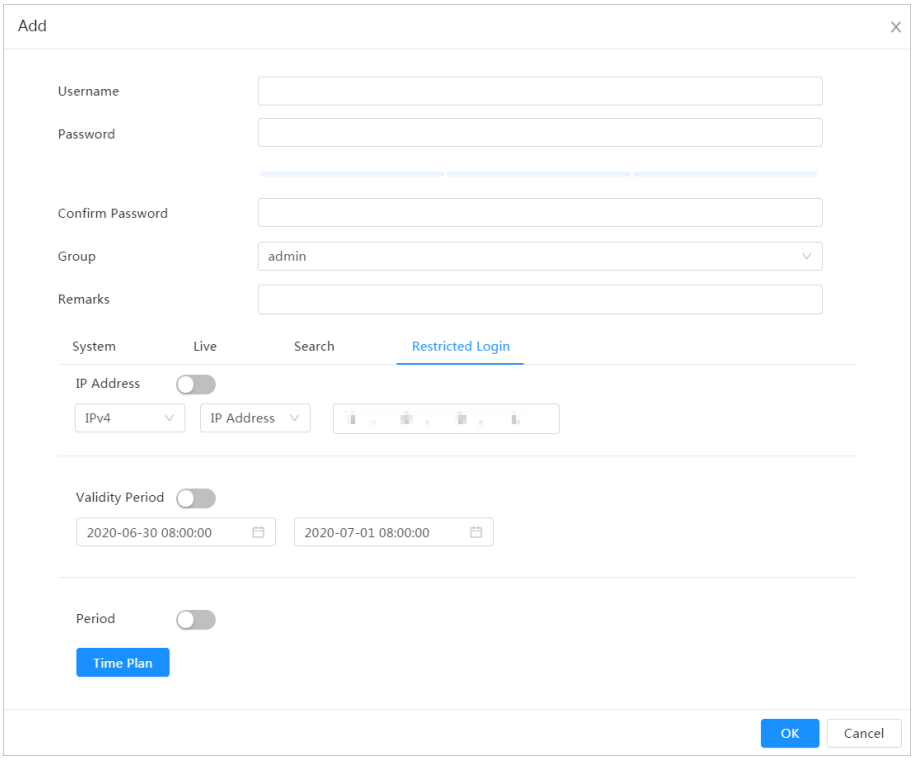


Figure 5:17 add user (login restricted)



Step 3: Set user parameters

Table 5:8 description of user parameters (1)

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

Parameter	Description
Confirm Password	Password must consist of 8 to 32 non-empty characters and contain at least two types of characters including uppercase, lowercase, numbers, and special characters (excluding ``&').
Cluster	The group to which the users belong. Each group has different permissions.
Observation	Describe the user.
System	Select permissions as required. It is recommended to give regular users fewer permissions than premium users.
Straight	Select the live view permission for the user to be added.
Search	Select the search permission for the user to add.
Login restricted	Set the address of the PC that allows the set to log in to the camera and the validity period and time range. You can log in the web interface with the IP set in the time range set as the validity period. ● IP Address: You can login to the web through the PC with the set IP. ● Validity period: You can log in to the web in the established validity period. ● Time range: You can login to the web in the set time interval. Set as follows 1. IP Address: Enter the IP address of the host to be added. 2. IP Segment: Enter the starting address and ending address of the host to be added.

Step 4: click on**Apply**(apply).

The newly added user appears in the username list.

Related operations

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

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

- Click on to remove the added users. The admin user cannot be remove.

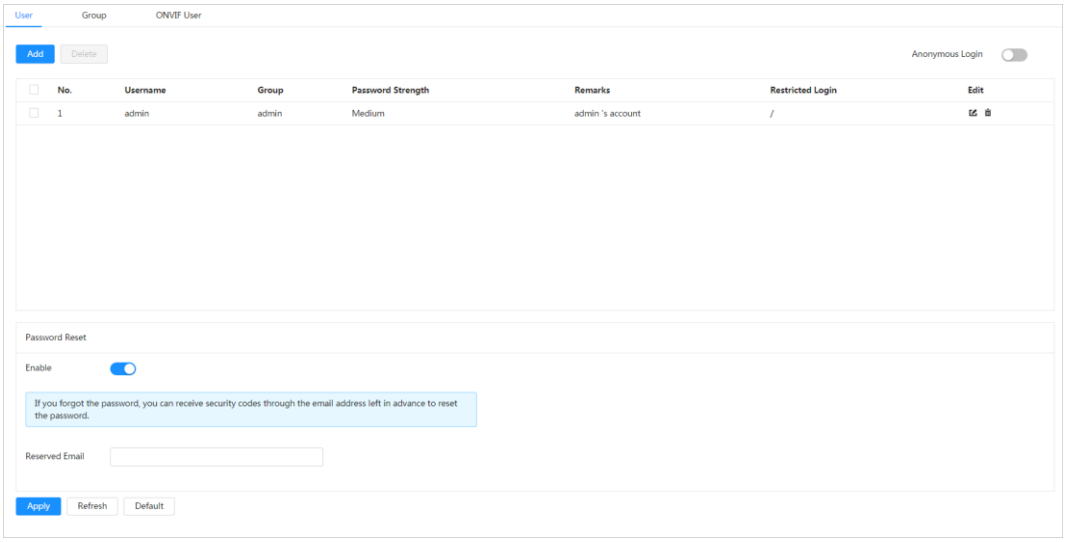
  The administrator account cannot be deleted.

5.3.2.1.2 Reset password

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

Step 1: select > **System**(System) >**Bill**> (Account)**User**(user).

Figure 5:18 user



Step 2: Click beside**Enable**(Enable) on**Restore password** (Password Reset).

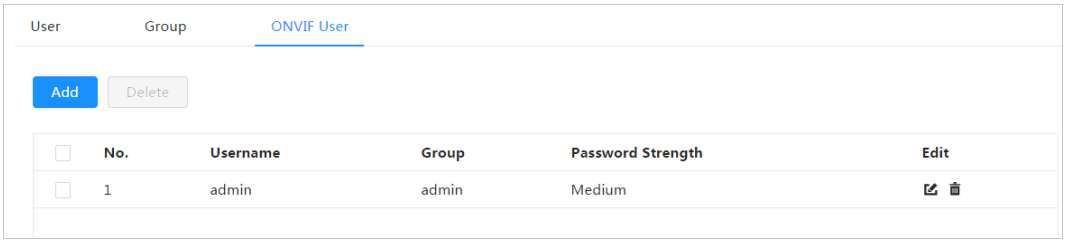
If the function is not enabled, you can only reset the password by resetting the camera. Step 3: Enter the reserved email address. Step 4: click on**Apply**(apply).

5.3.2.2 ONVIF user

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

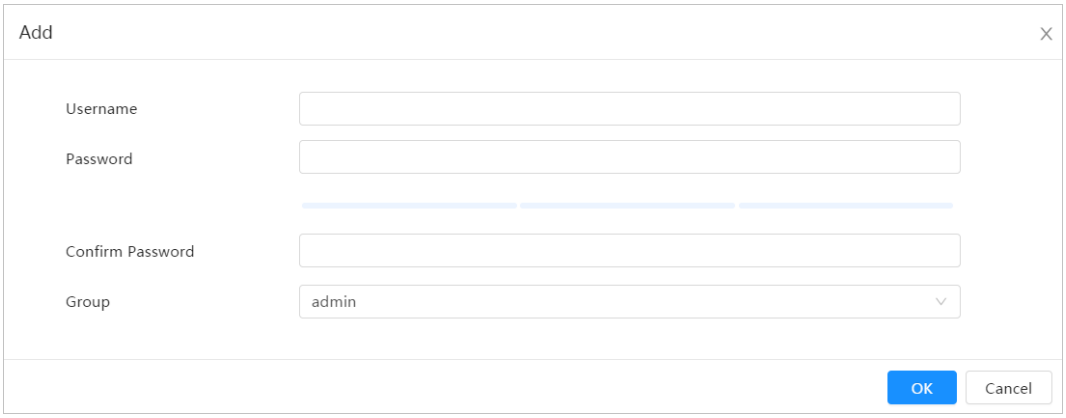
Step 1: Select > **System**(System) >**Bill**(Account) >**ONVIF user** (ONVIF User).

Figure 5–19 ONVIF User



Step 2: click on**Add**(add).

Figure 5:20 add ONVIF user



Step 3: Set user parameters

Table 5:9 description of ONVIF user parameters

Parameter	Description
Username	Unique identification of the user. 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 types of characters including uppercase, lowercase, numbers, and special characters (excluding ' " ; : &).
Confirm Password	
Group name	The group to which the users belong. Each group has different permissions.

Step 4: click on**To accept**(OKAY).

The newly added user appears in the username list.

Related operations

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

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

- Click on to remove the added users. The administrator user is not can delete.

  The administrator account cannot be deleted.

5.3.3 Managers

5.3.3.1 Requirements

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

- Check surveillance footage regularly.
- Regularly delete the information of users and user groups that are not used frequently.
- Change the password every three months. For details, please refer to " 5.3.2 Account."

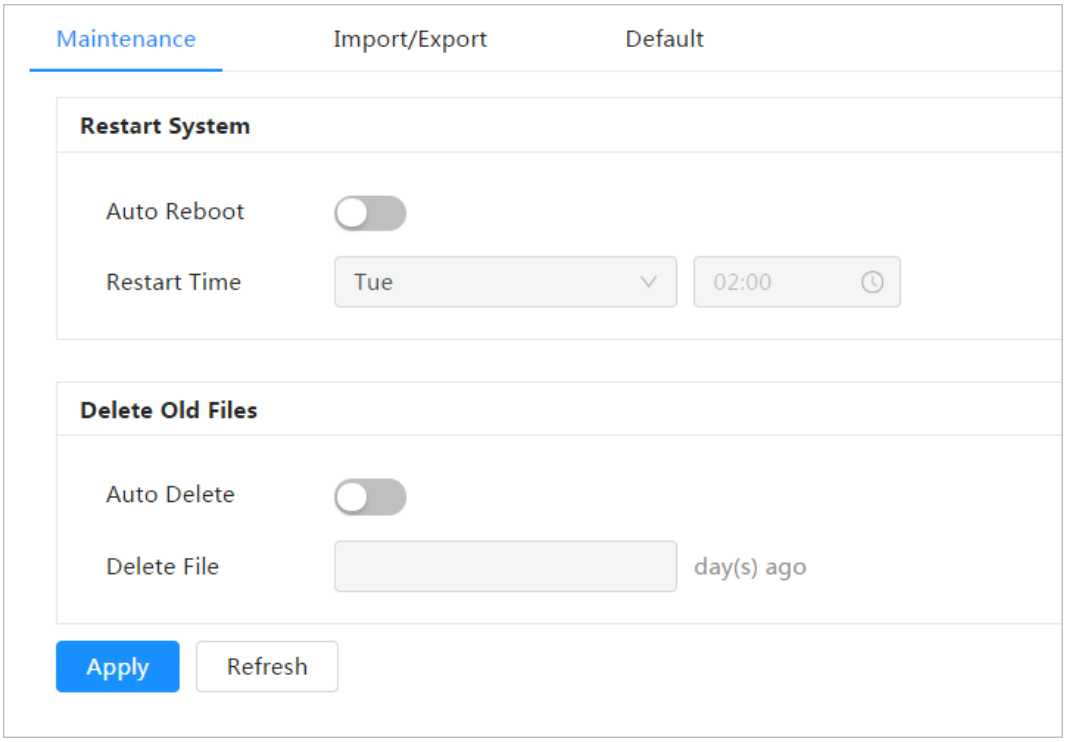
- View and analyze system logs, and fix errors in a timely manner.
- Back up your system settings regularly.
- Reboot the device and remove old files regularly.
- Update the firmware accordingly.

5.3.3.2 Maintenance

You can manually reboot the system and set the time for automatic reboot, as well as automatic deletion of old files. This feature is disabled by default.

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

Figure 5:21 maintenance



Step 2: Set the parameters for automatic maintenance.

- Click on beside**auto reset**(Auto Reboot) on**Restart system** (Restart System) and set the restart time; the system automatically reboots as the set time every week.
- Click on beside**delete automatically**(Auto Delete) on**Remove old files**(Delete Old Files) and set the time; the system automatically deletes old files according to the set time. The time range is from 1 to 31 days.

When you enable and confirm the function of**delete automatically**(Auto Delete), the Deleted files cannot be restored. Carry out the procedure carefully.

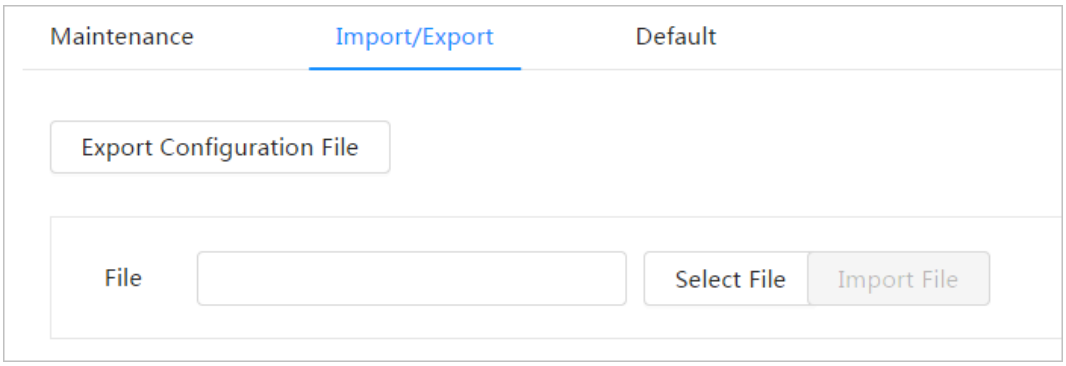
Step 3: click on**Apply**(apply).

5.3.3.3Import/Export

- Export the system configuration file to back up your system configuration.
- Import system configuration file to perform quick configuration or recover system configuration.

Step 1: Select > **System**(System)>**Bill**(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** (Import File) to import the configuration file from the local system to the system.
- Export: click**Export configuration file**(Export Configuration File) to export the system configuration file to local storage.

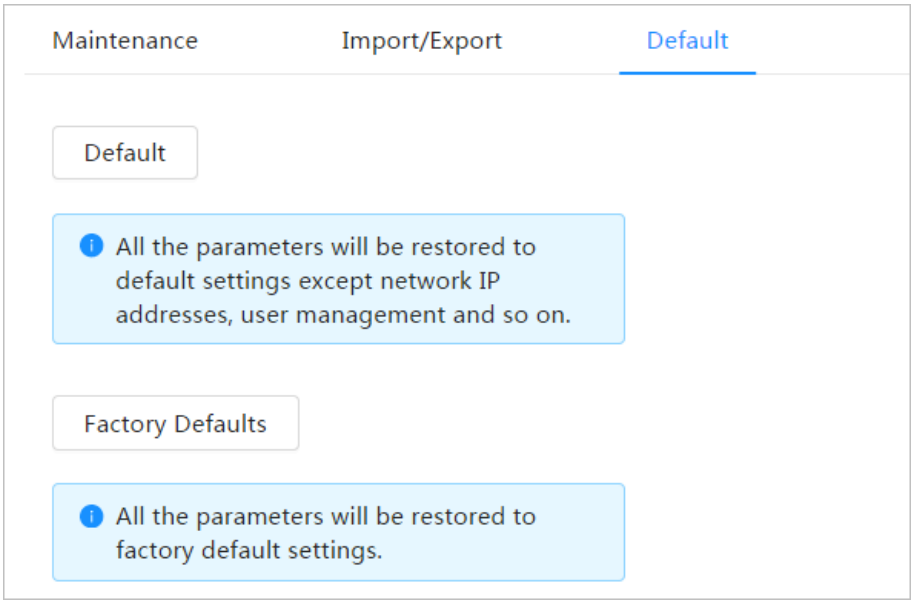
5.3.3.4Default

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

select > **System**(System) >**Bill**> (Account)**Predetermined**(Defautl).

- Click on**Predetermined**(Default) and then all settings except IP address and account will be reset to default.
- Click on**Factory Defaults**(Factory Default) and all settings will be restored to factory defaults.

Figure 5:23 default



5.3.4Update

Updating to the latest version may improve camera features and stability. If the wrong update file was used, please reboot the device; otherwise, some functions may not work properly.

Step 1: Select > **System**(System) >**To update**(Upgrade).

Figure :24 update

Step 2: Click on**Review**(Browse) and then upload the update file. The update file must be a .bin file.

Step 3: Click on**To update**(Upgrade). The update will begin to run.

Appendix 1 Recommendations for cybersecurity

Cybersecurity is more than just a buzzword – it is something that pertains to every device that is connected to the Internet. IP video surveillance is not immune to cyber risks, but taking basic steps to protect and harden networks and network-connected devices will make them less susceptible to attack. Below are some tips and recommendations on how to create a more secure security system. **Mandatory measures that you must take for the security of the basic equipment network:**

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 account name or account name backwards.
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use continuous repeating characters, such as 111, aaa, etc.;

two.**Update firmware and client software on time**

- As per the standard procedure in the technology industry, we recommend that you keep the firmware of your equipment (such as NVR, DVR, IP camera, etc.) up to date to ensure that the system is equipped with the latest patches and security fixes. When the equipment is connected to the public network, it is recommended to enable the "automatic update checking" function to obtain timely information about firmware updates published by the manufacturer.
- We suggest that you download and use the latest version of the client software.

Recommended measures to improve the security of your computer's network:

1.**physical protection**

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

two.**Change passwords periodically**

We suggest that you change your passwords periodically to reduce the risk that they can be guessed or cracked.

3.**Establish and promptly update password reset information**

The equipment supports the password reset function. Set up related information for timely password reset, including password protection questions and end-user email address. If the information changes, change it immediately. When setting password protection questions, we suggest that you do not use easily guessed ones.

Four.**Enable account lockout**

The account lockout feature is enabled by default, and allows you to

We recommend that you keep it enabled 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 locked.

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

We suggest that you change the default HTTP and other service ports to any number series 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 you visit the web service through 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**

Based on 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 needed, it is recommended to disable some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If they are needed, 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 authentication passwords.
- 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 feature to reduce the risk of audio and video data theft during transmission.

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

eleven.**secure audit**

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

12.**network log**

Due to the limited storage capacity of the computer, the stored record 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 monitoring.

13.**Create a secure network environment**

To better ensure the security of your computers and reduce potential cyber risks, we recommend:

- Disable the port mapping feature of the router 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 are no communication requirements 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 MODE OF SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Zip Code: 310053 Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Phone: +86-571-87688883