



Web 5.0 network camera

Operation Manual







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 hazard which, if not avoided, could result in minor or minor injury. moderate.
 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.
 NOTE	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 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 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 contained 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 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 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.

Safety warnings and precautions

important

Electrical safety

- All instructions for use and installation must comply 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 supply 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.
- Avoid pinching or pinching the power cord, especially at the connector, outlet, and where it exits 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 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 lightning.
- 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 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 device case with a soft, dry cloth, and for more stubborn stains, 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 the protection of your 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 older firmware versions, the ONVIF password will not be changed automatically along with changing the system password, and you will need to update the firmware or manually update 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

Foreword	I
Important safety warnings and precautions.....	III 1
Overview.....	1
1.1 Introduction.....	1
1.2 Network connection	1
1.3 Configuration flow.....	1
2 Device initialization	3
3 Access.....	7
3.1 Login to the device.....	7
3.2 Reset the password.....	8
4 Straight	10
4.1 Live Interface.....	10
4.2 Encoding settings	eleven
5 Settings	12
5.1 Network.....	12
5.1.1 TCP/IP.....	12
5.1.2 Port	fifteen
5.1.3 Email	17
5.1.4 Basic service.....	19
5.2 Event.....	twenty
5.2.1 Alarm input configuration	twenty-one
5.2.2 Establish alarm linkage	22
5.2.2.1 Add programming.....	2. 3
5.2.2.2 Recording Linkage	24
5.2.2.3 Snapshot Linking	25
5.2.2.4 Alarm output linkage	25
5.2.2.5 Email Linking.....	26
5.3 System.....	26
5.3.1 General.....	26
5.3.1.1 Basic	26
5.3.1.2 Date and time	27
5.3.2 Account	28
5.3.2.1 User.....	28
5.3.2.1.1 Add users	28
5.3.2.1.2 Reset password	31
5.3.2.2 ONVIF User.....	32
5.3.3 Managers.....	33

5.3.3.1 Requirements.....	33
5.3.3.2 Maintenance.....	3. 4
5.3.3.3 Import/Export.....	35
5.3.3.4 Default.....	35
5.3.4 Update	36
Appendix 1 Cybersecurity recommendations.....	37

1 Overview

1.1 Introduction

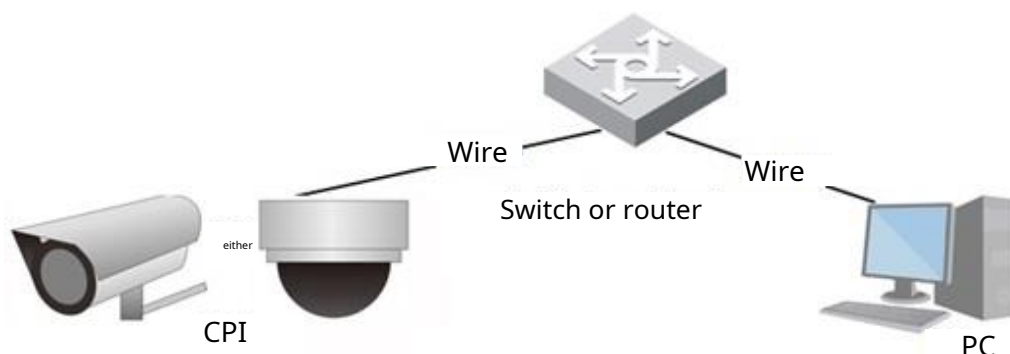
An IP camera (Internet Protocol Camera) is a type of digital video camera that receives control data and sends image data over the Internet. They are commonly used for surveillance and do not require a local recording device, but only a local area network.

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

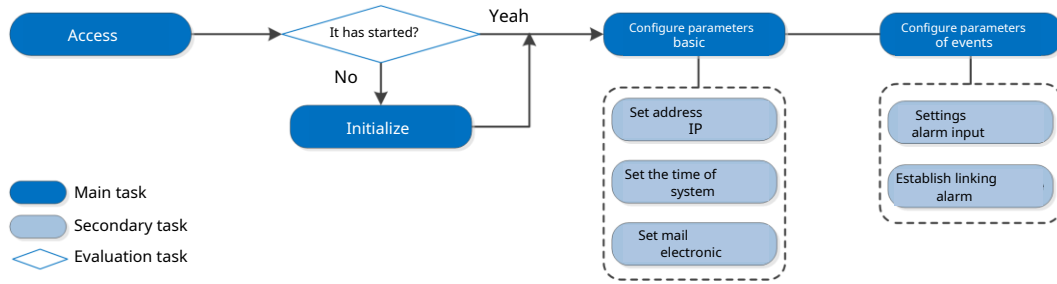


Table 1:1 flow description

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 Initialization of the device"
Parameters basic	IP adress	" 5.1.1 TCP/IP"
	Date and hour	" 5.3.1.2 Date and hour"

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.



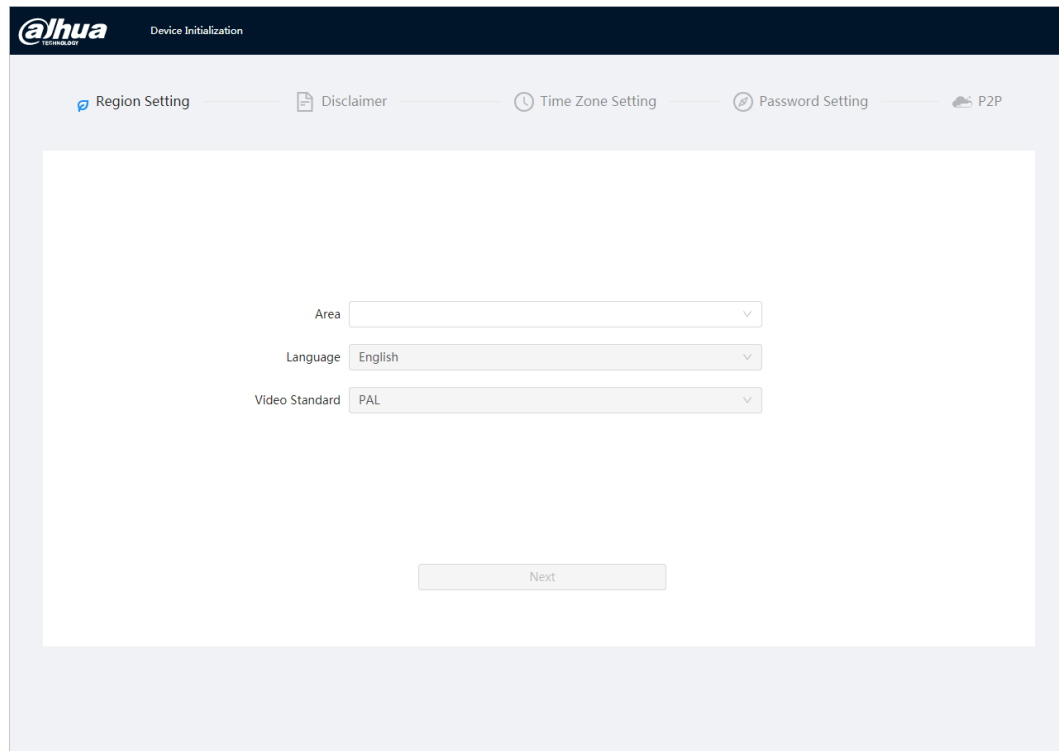
- To ensure device security, please keep the password correctly after startup and change it regularly.
- When starting the device, keep the PC IP and the device IP on the same network.

Step 1: Open the 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.

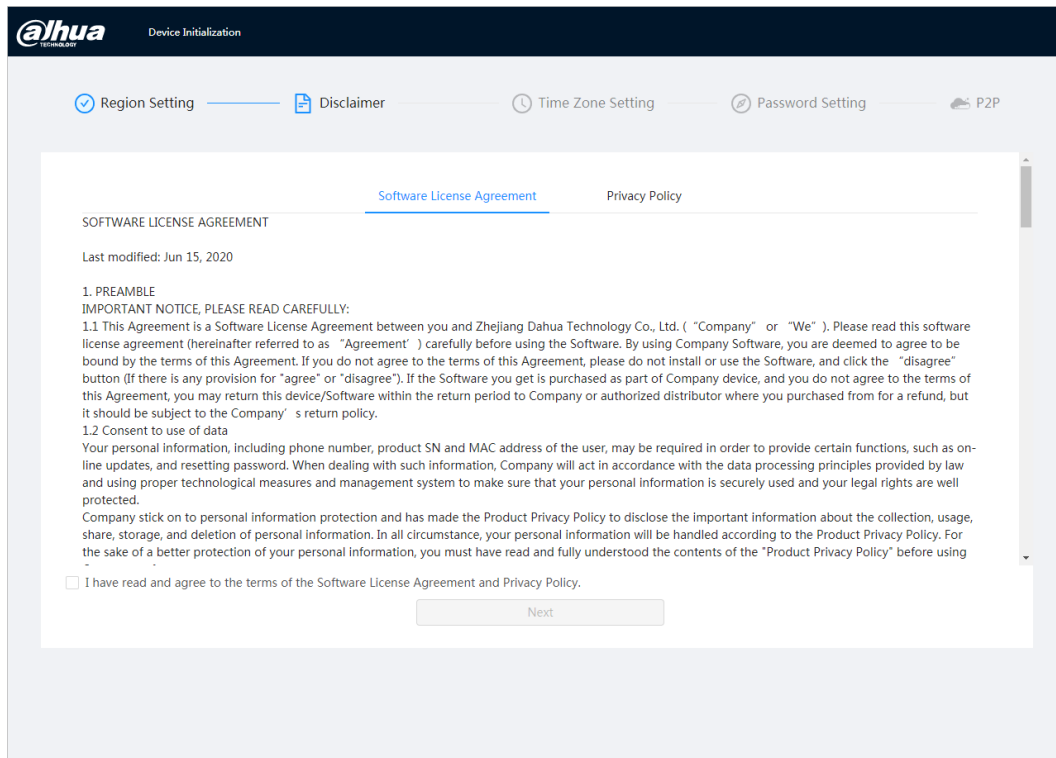
Figure 2:1 region settings



The screenshot shows the 'Device Initialization' web interface. At the top, there is a breadcrumb trail: 'Region Setting' (active), 'Disclaimer', 'Time Zone Setting', 'Password Setting', and 'P2P'. Below the breadcrumb, there are three dropdown menus for configuration: 'Area' (empty), 'Language' (set to 'English'), and 'Video Standard' (set to 'PAL'). At the bottom center of the configuration area, there is a 'Next' button.

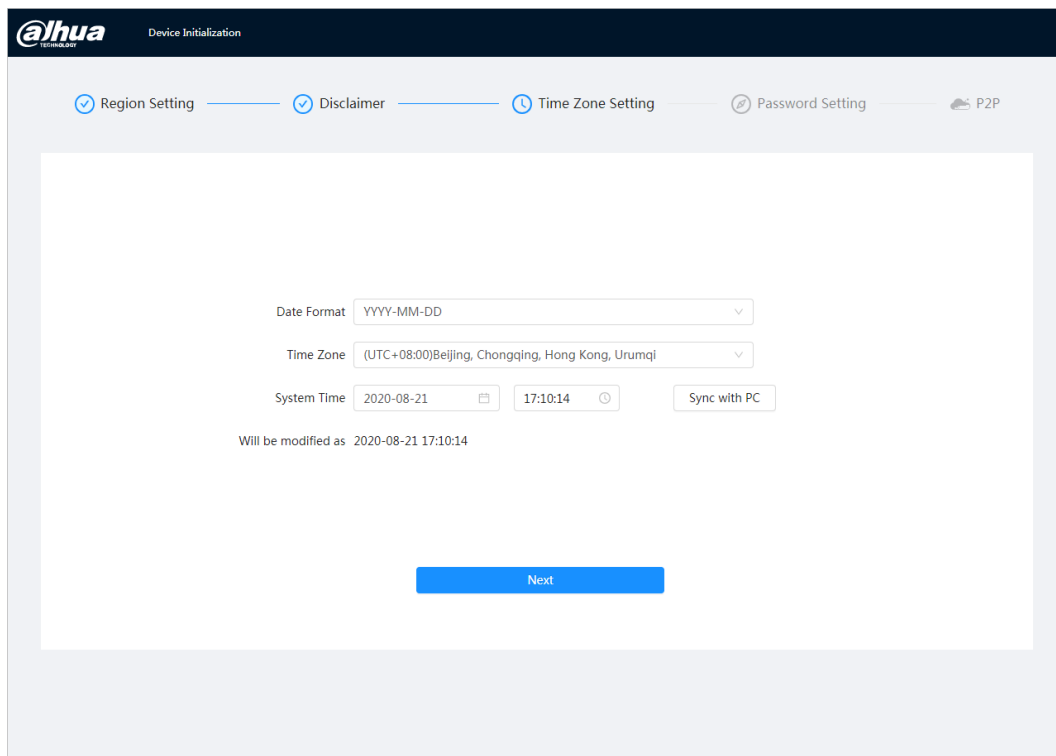
Step 2: Select the area, language and video standard according to the actual situation, and then click **Following**(Next).

Figure 2:2 disclaimer



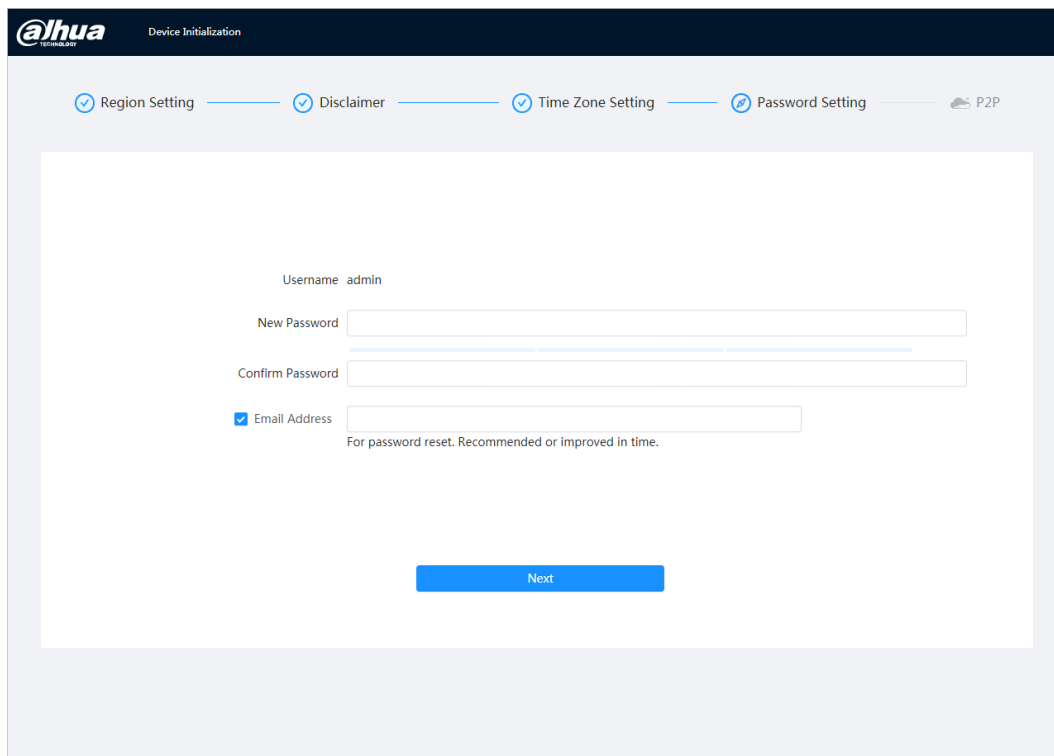
Step 3: Select the check box **I have read and accept the terms of the Software License Agreement and Privacy Policy**(I have read and agree to the terms of the Software License Agreement and Privacy Policy), and then click **Following** (Next).

Figure 2:3 time zone settings



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

Figure 2:4 password settings



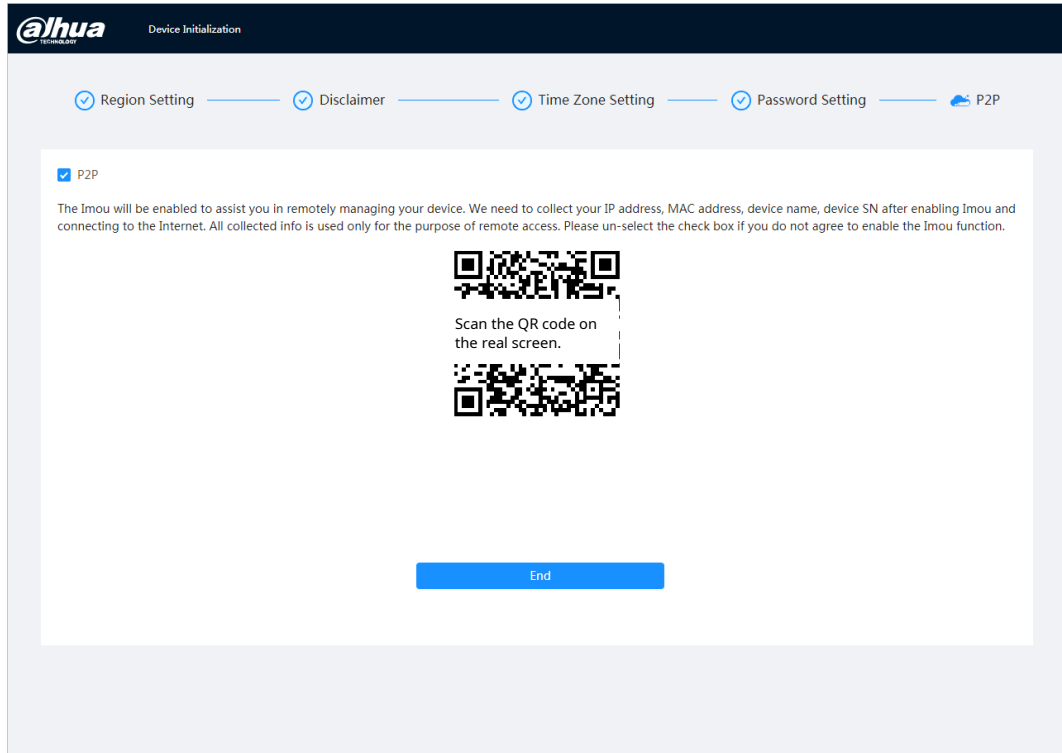
Step 5: Set the password for the administrator account.

Table 2:1 description of password settings

Parameter	Description
Username	The default username is admin.
Password	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 ' " ; &). Set a password with a high security level according to the password security notice.
Confirm Password	
Email saved	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 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 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.

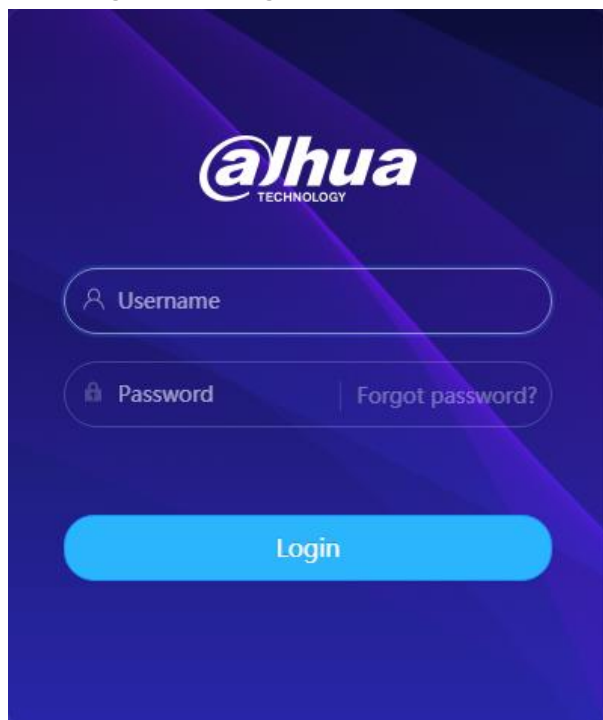
Step 1: Open the Chrome browser, enter the camera's IP address (192.168.1.108 by default) in the address bar and press Enter.


Step 2: Enter the username and password. The username is admin by default.



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

Figure 3-1 Login

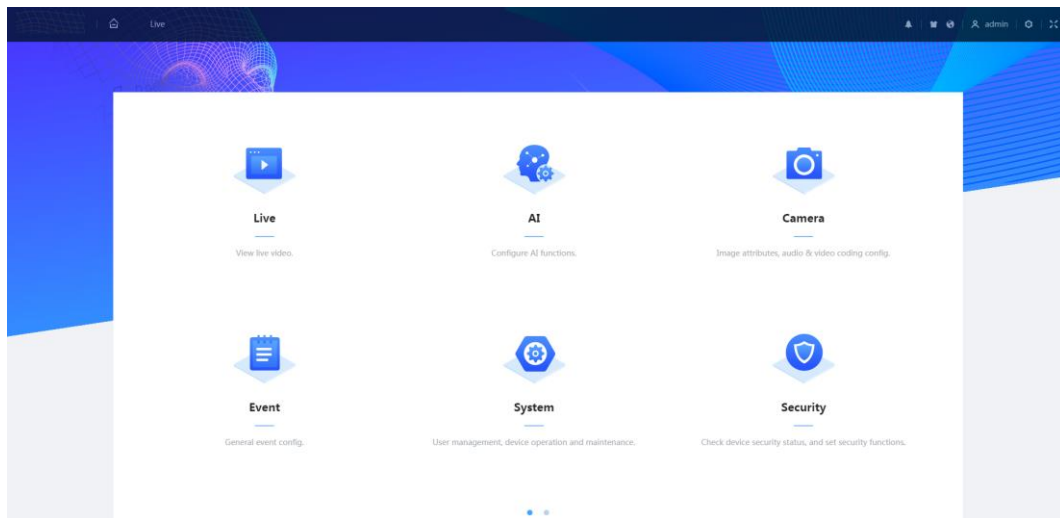


Step 3: Click on **Log in**(Login). The interface will appear **Live**(Live). Click the interface to bring up the  in the upper left corner of main interface.



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

Figure 3-2 Main Screen




- 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 alarm binding exception, video detection, and audio detection.
- System: Configure system parameters, including general, date and time, account, security, PTZ settings, default, import/export, remote, auto maintenance and update.
- Security: Check the device security status and configure 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.

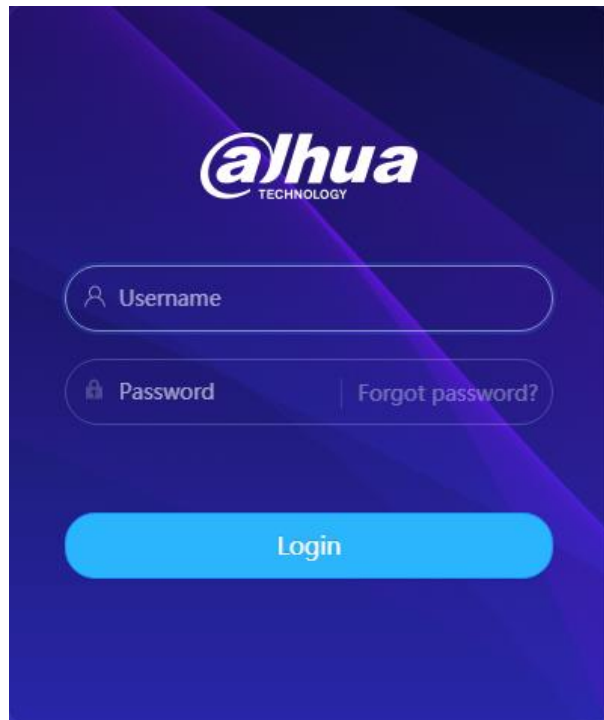
Previous requirements

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

Procedure

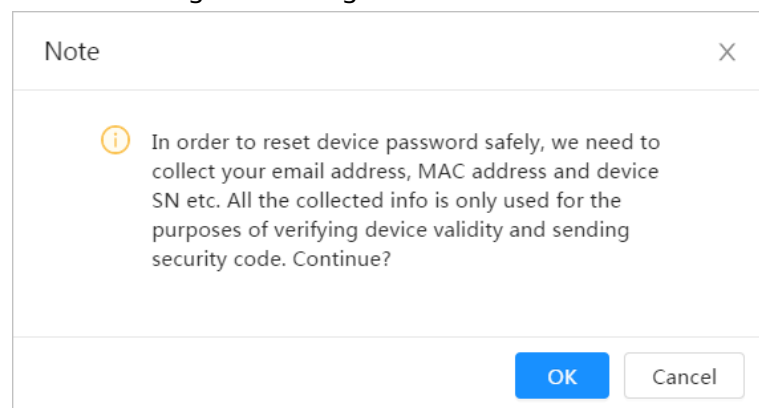
Step 1: Open the Chrome browser, enter the device's IP address in the address bar, and then press the Enter key.

Figure 3-3 Login



Step 2: Click on **Forgot your 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)

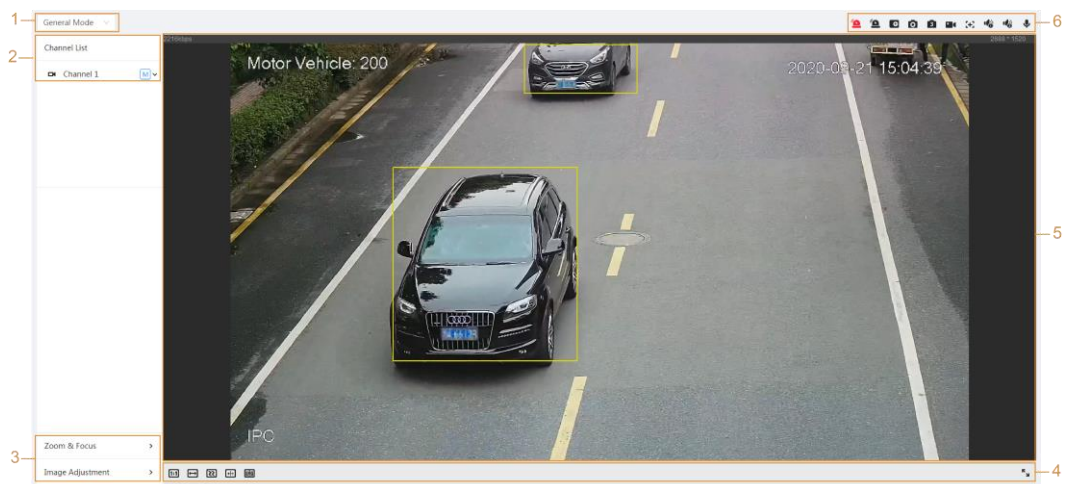


Figure 4:2 live (multi-channel)

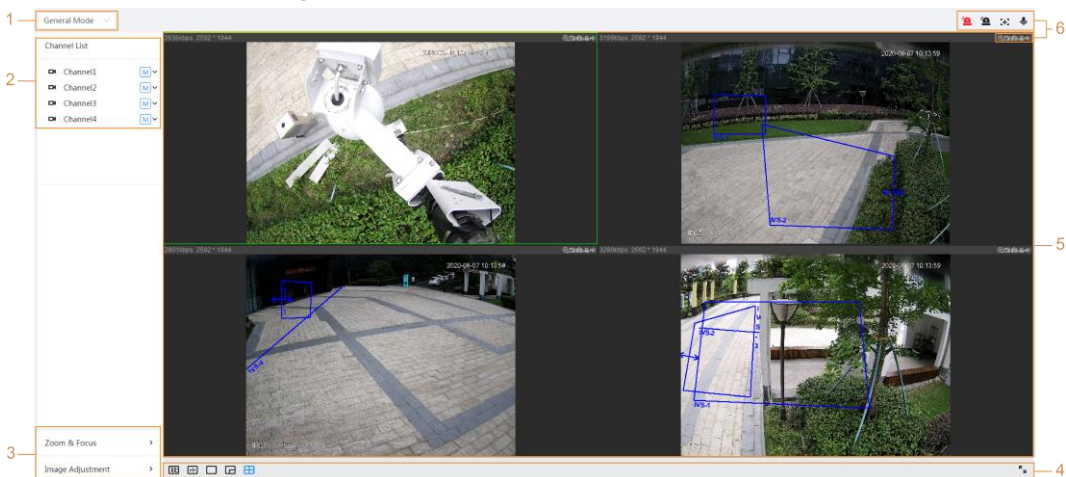


Table 4:1 description of the function bar

No.	Function	Description
1	Display mode	You can select the display mode from General mode (General Mode) and Face mode (FaceMode).
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


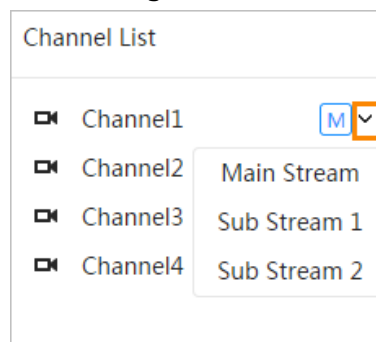



Click on  and then select the stream as needed.

Figure 4:3 coding bar



- **Main transmission:** It has great bit and image transmission value with high resolution, but also requires large bandwidth. This option can be used for storage and monitoring.
- **Secondary transmission:** It has a small bit rate and smooth image, 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 stream;  means that the current stream is secondary stream 1;  means the current stream is sub stream 2.

5 Settings

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

5.1 Network

This section presents the network configuration.

5.1.1 TCP/IP

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

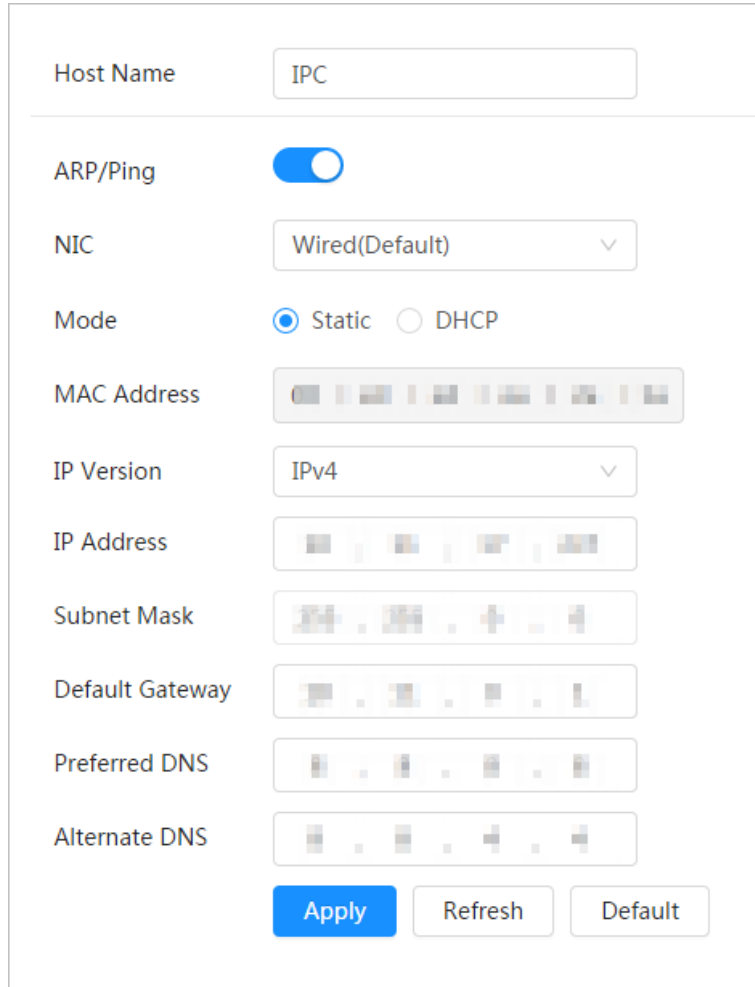
Previous requirements

The camera has connected to the network.

Procedure

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

Figure 5-1 TCP/IP



Host Name: IPC

ARP/Ping:

NIC: Wired(Default)

Mode: Static DHCP

MAC Address: [Hexadecimal string]

IP Version: IPv4

IP Address: [Dotted decimal]

Subnet Mask: [Dotted decimal]

Default Gateway: [Dotted decimal]

Preferred DNS: [Dotted decimal]


Alternate DNS: [Dotted decimal]


Buttons: Apply, Refresh, Default

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	<p>Click on  to enable ARP/Ping and configure the service of IP address. Obtain the MAC address of the camera so you can change and configure the device's IP address with the ARP/ping command.</p> <p>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 set with the ping packet.</p> <p>Demonstration of how to configure the IP address with ARP/Ping.</p> <ol style="list-style-type: none"> 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 camera's MAC address from the device label. 3. Open the command editor on the PC and enter the following command. <div data-bbox="676 972 1353 1541" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre>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↵</pre> </div> 4. Restart the camera. 5. Check the PC command line; if the informational message appears Reply 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 address bar to log in.
NIC	<p>Select the Ethernet card to be configured and the default is With cable(Wired).</p>

Parameter	Description
Mode	The way the camera obtains the IP: <ul style="list-style-type: none"> ● Static Set the IP address(IP Address), the subnet mask(Subnet Mask) and the Default Gateway(Default Gateway) manually, and then click Keep(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 obtain the IP address automatically.
MAC address	Shows the MAC address of the host.
IP version	Select IPv4 either IPv6 .
IP address	When you select Static (Static) in Mode (Mode), enter the IP address and subnet mask you need.
Subnet mask	
Access portal predetermined	 <ul style="list-style-type: none"> ● IPv6 does not have a subnet mask. ● The default gateway must be on the same network segment than the IP address.
Preferred DNS	Preferred DNS IP address
Alternative DNS	Alternate DNS IP Address

Step 3: Click on **Apply**(Apply).

5.1.2Port

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 >  **Grid**(Network) > **TCP/IP**(TCP/IP).

Figure 5:2 port

Max Connection	<input type="text" value="10"/>	(1-20)
TCP Port	<input type="text" value="3777"/>	(1025-65534)
UDP Port	<input type="text" value="3778"/>	(1025-65534)
HTTP Port	<input type="text" value="80"/>	
RTSP Port	<input type="text" value="554"/>	
RTMP Port	<input type="text" value="1935"/>	(1025-65534)
HTTPS Port	<input type="text" value="443"/>	
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>		

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.
TCP port	Transmission control protocol port. The default value is 37777.
UDP port	User datagram protocol port. The default value is 37778.
HTTP port	Hypertext transfer protocol port. The default value is 80.

Parameter	Description
RTSP port	<ul style="list-style-type: none"> ● 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. <p>URL format example: <code>rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0</code></p> <p>Among that:</p> <ul style="list-style-type: none"> ● 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). <p>Example: If you need the secondary stream of channel 2 from a certain device, the URL should be: <code>rtsp://admin: admin@10.12.4.84 :554/cam/realmonitor?channel=21&=1</code></p> <p>If the username and password are not required, the URL can be: <code>rtsp://ip:port/cam/realmonitor?channel=11&=0</code></p>
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) takes effect 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 activated.

Step 1: Select  > **Grid**(Network) > **Email**(E-mail).

Figure 5:3 email

Step 2: Click on to enable the feature.

Step 3: Configure email parameters


Table 5:3 description of email parameters

Parameter	Description
SMTP server	SMTP server address
Port	The port number of the SMTP server.
Username	The SMTP server account.
Password	The SMTP server password.
Anonymous	Click on <input type="checkbox"/> and the sender information will not be displayed in the email.
Sender	Sender email address.
Encryption type	Select between None (None) SSL and TLS . For details, see Table 5:4.
Qualification	Enter a maximum of 63 characters in Chinese, English, and Arabic numerals. Click to select the title type, including the device name (Device Name), the Device identification (Device ID) and the 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
Addressee	<ul style="list-style-type: none"> ● Recipient's email address. Supports 3 addresses maximum. ● After entering the recipient's email address, the button will appear Prove(Test). Click on Prove(Test) to test whether emails can be sent and received correctly.
Mail of verification	The system sends a test email to verify that the connection has been configured correctly. Click configure the Shipping interval (and Sending Interval), and then the system will send the test email at the established 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	<ul style="list-style-type: none"> ● You need to have the service activated SMTP in your mailbox. ● The authentication code is required. The email password Electronic is not applicable.  Authentication code: code you receive when you enable the SMTP service.
		TLS	587	

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

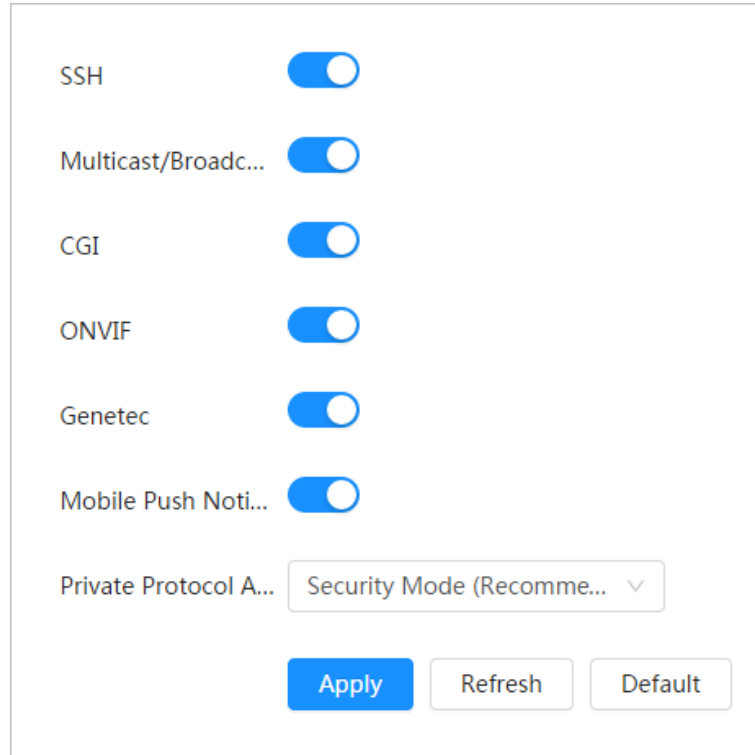
5.1.4 Basic service

Configure basic services to improve network and data security. Step 1: Select >



Grid(Network) > **Basic service**(Basic Service).

Figure 5:4 basic service



Step 2: Enable basic service based on actual needs.

Table 5:5 description of basic service parameters

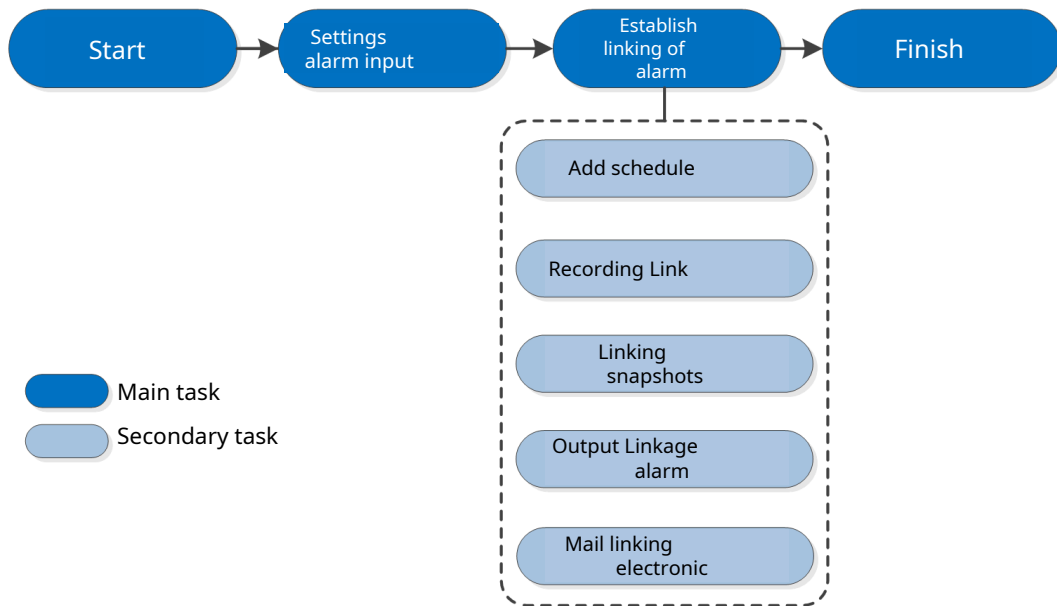
Function	Description
SSH	You can enable SSH authentication to manage security.
Search multicast/broadcast	Enable this function, and then when multiple users are viewing the device's video image simultaneously over the network, they can find your device with the multicast/broadcast protocol.
CGI	Enable the feature and then other devices can access it through this service. The feature is enabled by default.
Onvif	
Genetec	
***** Automatic notifications from the mobile*****	Enable this function 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 (Security Mode) Supported mode (Compatible Mode). Safety mode is recommended.

Step 3: Click on **Apply**(Apply).

5.2 Event

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

Figure 5:5 alarm event configuration



5.2.1 Alarm 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  next to **Enable**(Enable) to enable alarm linking.

Figure 5-6 Alarm Linkage

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

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

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** (Add Schedule) to add a new schedule. For details, see "5.2.2.1 Add Schedule."

Step 5: Click on **Apply** (Apply).

5.2.2 Set 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**(Event)>**Alarm**(Alarm),  next to **Enable**(Enable) for enable alarm linking.

Figure 5-7 Alarm Linkage

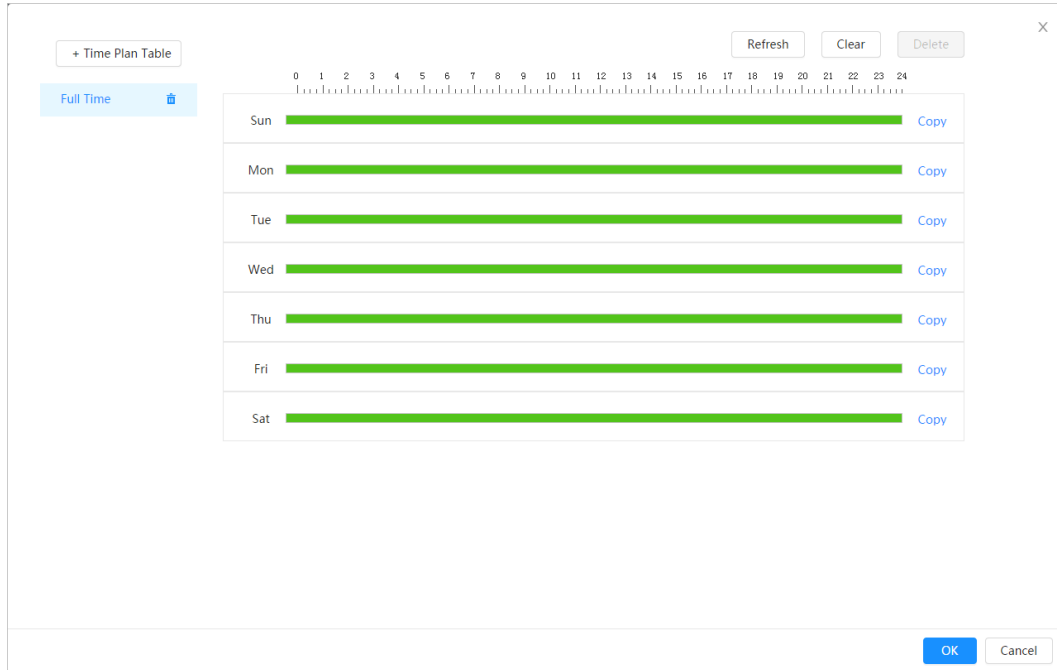
Enable	<input checked="" type="checkbox"/>
Alarm-in Port	Alarm1 <input type="button" value="v"/>
Schedule	Full Time <input type="button" value="v"/> <input type="button" value="Add Schedule"/>
Anti-Dither	0 sec.(0-100)
Sensor Type	NC <input type="button" value="v"/>
Enable Alarm	<input checked="" type="checkbox"/>
Alarm-out Port	<input type="button" value="1"/> <input type="button" value="2"/>
Post-Alarm	10 sec.(10-300)
Record	<input checked="" type="checkbox"/>
Record	<input type="button" value="1"/> <input type="button" value="2"/> <input type="button" value="3"/> <input type="button" value="4"/>
Post-Record	10 sec.(10-300)
Send Email	<input type="checkbox"/>
Snapshot	<input checked="" type="checkbox"/> <input type="button" value="1"/> <input type="button" value="2"/> <input type="button" value="3"/> <input type="button" value="4"/>
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>	

5.2.2.1 Add schedule

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

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

Figure 5:8 programming




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

- Click on **Copy**(Copy) next to a day and select the days you want to copy to in the application interface; You can copy the settings to the selected days. Select the check box **Select all**(Select All) to select every day 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 the table name to edit it.
- Click to delete  history as necessary.


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

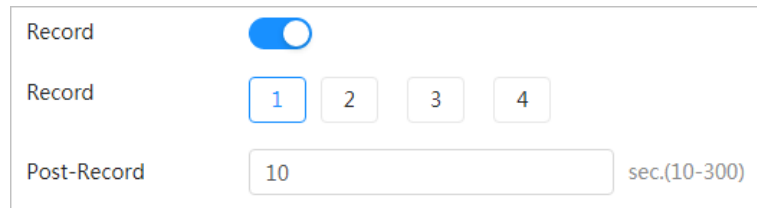
Set recording linkage

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

Set alarm linkage and recording delay.

Once configured **Post-recording**(Post-Record), alarm recording continues for an extended period after the alarm ends.

Figure 5:9 recording link



5.2.2.3 Linking 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**(Motion) or **Alarm** (Alarm)), the snapshot channel links the image capture.

Set recording linkage



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

Figure 5:10 Snapshot link



5.2.2.4 Alarm 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 outbound binding alarm, select the channel as necessary, 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

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

5.3.1 General

5.3.1.1 Basic

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: Configure general parameters

Table 5:6 description of general parameters

Parameter	Description
Name	Enter device name
Video standard	Select the video standard from PAL and 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 (daylight saving 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: Configure 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	<ul style="list-style-type: none"> ● Manual configuration:configure the parameters manually. ● 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 hours (24-Hour).
Time zone	Set the time zone the camera is in.
Current time	Set the system time. Click on Sync PC (Sync PC) and the system will adopt the PC time.
DST	Enable DST as needed. Click on <input type="checkbox"/> , 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 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, consisting of number, letter, underscore, 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 (excluding ' ' ; : &).
- 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**(Anonymous Login), and then log in with just the IP address instead of the username and password. Anonymous users only have preview authorization. During anonymous login, click **Sign off**(Logout) and then you can log in with another username.

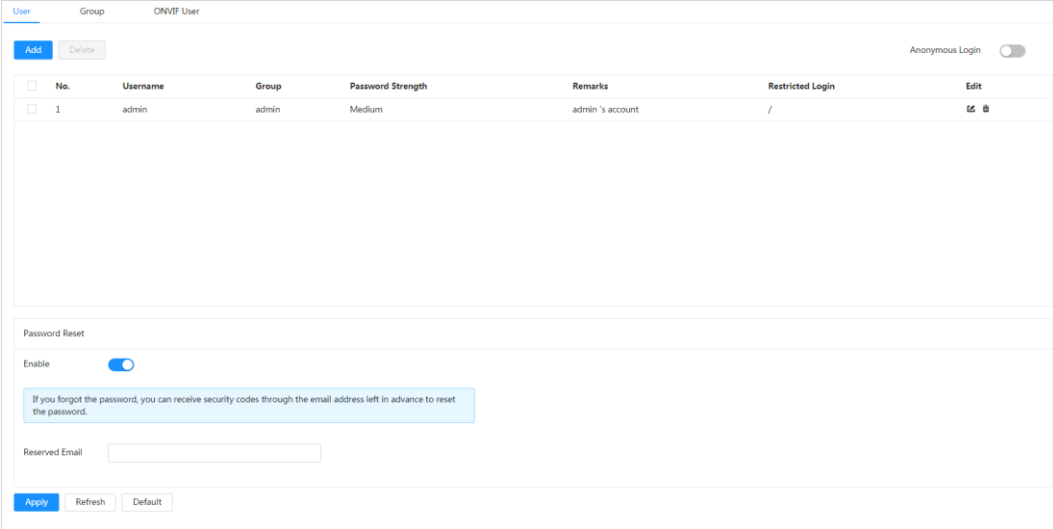
5.3.2.1 User

5.3.2.1.1 Add users



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

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

Figure 5:15 user



The screenshot displays the 'User' management page. At the top, there are tabs for 'User' and 'Group', and a breadcrumb path 'ONVIF User'. Below the breadcrumb, there are 'Add' and 'Delete' buttons, and an 'Anonymous Login' toggle switch. The main content is a table with the following columns: No., Username, Group, Password Strength, Remarks, Restricted Login, and Edit. The table contains one entry with No. 1, Username 'admin', Group 'admin', Password Strength 'Medium', Remarks 'admin's account', and Restricted Login '/'. Below the table, there is a 'Password Reset' section with an 'Enable' toggle switch (checked), a text box containing the instruction: 'If you forgot the password, you can receive security codes through the email address left in advance to reset the password.', and a 'Reserved Email' input field. At the bottom of the section are 'Apply', 'Refresh', and 'Default' buttons.

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

Step 2: Click on**Add(Add)**.


Figure 5:16 add user (system)

Figure 5:17 add user (restricted login)

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 " " ; : &).
Cluster	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.
Login restricted	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. <ul style="list-style-type: none"> ● IP Address: You can log in to the web through PC with the set IP. ● Validity period: You can log in to the website within the set validity period. ● Time Range: You can log in to the web in the set time range. Set as follows <ol style="list-style-type: none"> 1. IP Address: Enter the IP address of the host to be added. 2. IP Segment: Enter the start address and end 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 administrator account, you can only edit the password.

- Click on  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 the password by clicking **Forgot your password?** (Forget password?) in the login interface. For details, see " 3.2 Reset Password."


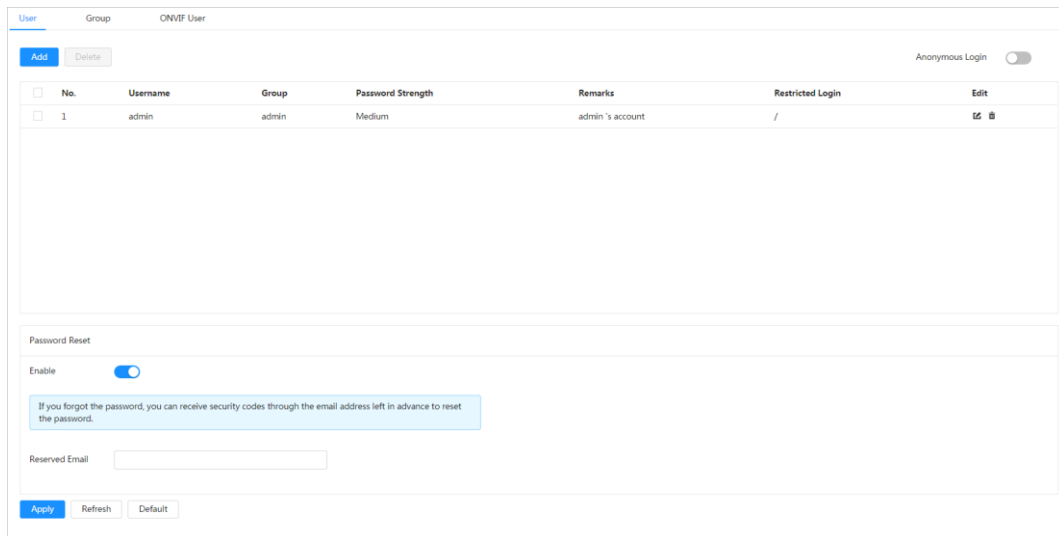

Step 1: Select  > **System(System) >Account>** (Account)**User(User).**

Figure 5:18 user



Step 2: Click  next to **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.


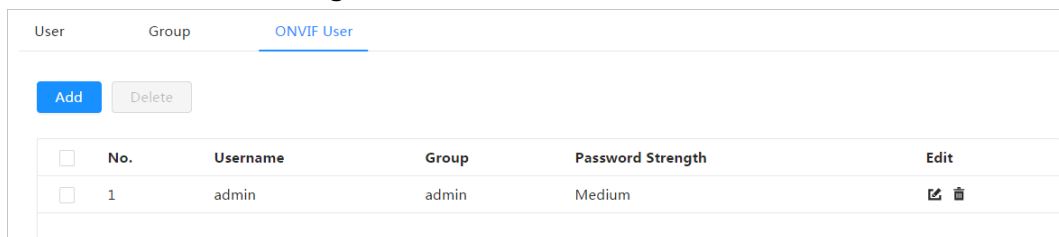
Step 1: Select >  **System(System) >Account(Account) >ONVIF user** (ONVIF User).

Figure 5-19 ONVIF User



Step 2: Click on **Add(Add).**

Figure 5:20 add ONVIF user

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.
Confirm 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 ' " ; : &).
Group name	The group to which the users belong. Each group has different permissions.

Step 4: Click on **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 delete the added users. The administrator user is not can delete.



The administrator account cannot be deleted.

5.3.3Managers

5.3.3.1Requirements

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

- Check surveillance footage regularly.
- Regularly delete information from users and user groups that are not used frequently.
- Change your 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.
- Please update the firmware accordingly.

5.3.3.2 Maintenance

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

Step 2: Set the parameters for automatic maintenance.

- Click on  next to **Automatic restart**(Auto Reboot) on **Restart system** (Restart System) and set the restart time; The system automatically restarts as the set time every week.
- Click on  next to **Delete automatically**(Auto Delete) in **Eliminate old files**(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 **Delete automatically**(Auto Delete), the Deleted files cannot be restored. Carry out the procedure carefully.

Step 3: Click on **Apply**(Apply).

5.3.3.3 Import/Export

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


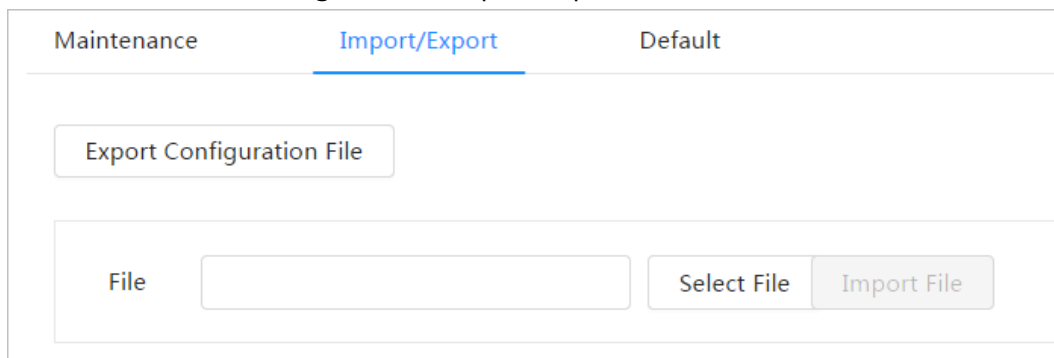
Step 1: Select >  **System**(System)>**Account**(Account) > **Import/Export**(Import/Export).

Figure 5–22 Import/Export



Step 2: Import and export.

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

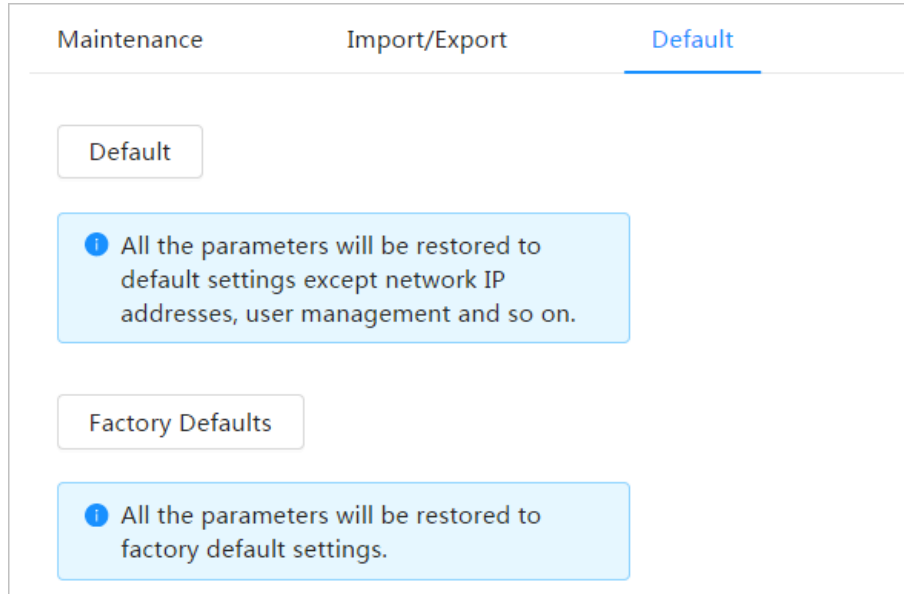
5.3.3.4 Default

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

Select  > **System**(System) > **Account**> (Account) **Predetermined**(Defaultl).

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

Figure 5:23 default



5.3.4 Update

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(System) > Update(Upgrade).**

Figure :24 update



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

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

Appendix 1 Recommendations cybersecurity

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 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 that you keep the firmware of your equipment (such as NVR, DVR, IP camera, etc.) updated to ensure that the system is equipped with the latest patches and security 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. Set and promptly update password reset information

The device supports the password reset function. Configure information related to prompt 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 configure 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 function 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 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 log

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 real 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: No.1399 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Zip code: 310053 Email:
overseas@dahuatech.com | Fax: +86-571-87688815 | Tel.: +86-571-87688883