HIKVISION

Mobile Network Camera

User Manual

Legal Information

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (https://www.hikvision.com/).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the RE Directive 2014/53/EU, EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
ℹ Note	Provides additional information to emphasize or supplement important points of the main text.
⚠ Caution	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
⚠ Danger	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Instructions

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet limited power source or PS2 requirements according to the IEC60950-1 or IEC 62368-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause over-heating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

TABLE OF CONTENTS

Chapter 1 Introduction

1.1 Product Features

This network camera is a digital monitoring product that integrates video and audio acquisition, intelligent coding and compression, network transmission and other functions. With embedded operating system and high-performance hardware processing platform, it has high stability and reliability, and can meet the needs of various industries that require the recognition of license plate.

Based on Ethernet control, the network camera can realize image compression and transmit it to different users through the network. Centralized storage based on NAS can greatly facilitate the storage and call of data.

You can control the webcam through the browser, and set the webcam parameters, intelligent functions, audio and video parameters, image parameters, etc. through the browser. Please refer to the actual equipment for specific function parameters.

1.2 Product Function

License Plate Recognition Function

When the object vehicle entered the License Plate Recognition area and reached the trigger line, the camera will capture and recognize the license plate. License numbers from Asia Pacific, Africa and America, Europe and Middle East are supported.

The recognition function can be configured in the alarm input by specifying its triggering condition.

- Alarm Input

Support the setting of the alarm input number, trigger level, alarm type and name.

Support showing the IP address (if nonlocal) and the alarm status.

Event detection function

The camera supports only exception alarm.

- Exception.

Support the alarm in the case of network disconnection, IP conflict and Illegal login.

System function

- Video recording and capturing pictures

The camera supports instant capture and video recording during preview, and can also configure video recording and capture plan after installing memory card or configuring network storage disk, so as to realize planned video recording and capture.

- User Management

You can manage many different users through the administrator "admin" user, and configure different permissions for each user.

Network function

The camera supports TCP/IP, DHCP, UDP, MCAST, FTP, and other network communication protocols; it also supports open interconnection protocols such as ONVIF.

The function of the product depends on the model, please refer to the technical parameters of the actual product.

Chapter 2 Operation Instructions

Note

- You shall acknowledge that the use of the product with Internet access might be under network security risks. For avoidance of any network attacks and information leakage, please strengthen your own protection. If the product does not work properly, please contact with your dealer or the nearest service center.
- To ensure the network security of the network camera, we recommend you to have the network camera assessed and maintained termly. You can contact us if you need such service.

Before you start:

Step 1 If you want to set the network camera via a LAN (Local Area Network), please refer to Section 2.1 Setting the Network Camera over the LAN.

Step 2 If you want to set the network camera via a WAN (Wide Area Network), please refer to Section 2.2 Setting the Network Camera over the WAN.

2.1 Setting the Network Camera over the LAN

Purpose:

To view and configure the camera via a LAN, you need to connect the network camera in the same subnet with your computer, and install the SADP or iVMS-4200 software to search and change the IP of the network camera.

Note

For the detailed introduction of SADP, please refer to Appendix 1.

2.1.1 Wiring over the LAN

The following figures show the two ways of cable connection of a network camera and a computer:

Purpose:

Step 1 To test the network camera, you can directly connect the network camera to the computer with a network cable as shown in Figure 2-1.

Step 2 Refer to the Figure 2-2 to set network camera over the LAN via a switch or a router.

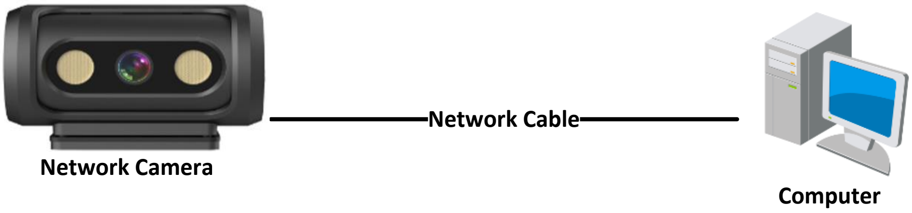


Figure 2-1 Connecting Directly

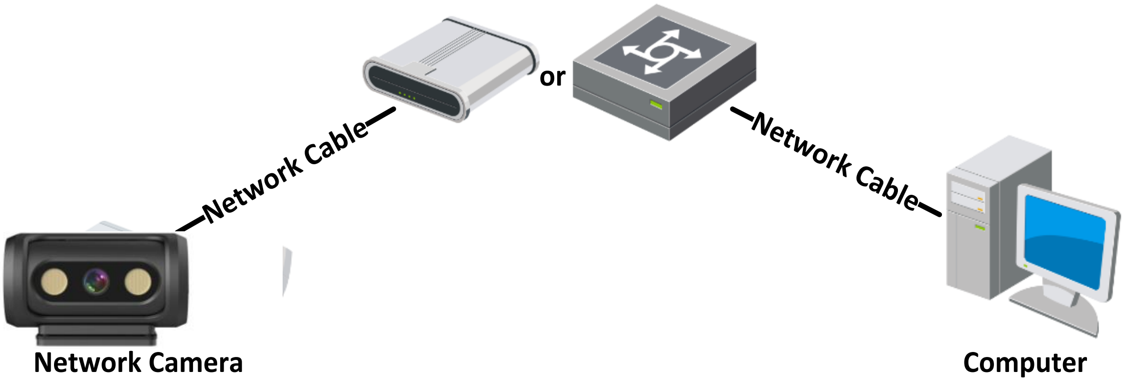


Figure 2-2 Connecting via a Switch or a Router

2.2 Activating the Camera

You are required to activate the camera first by setting a strong password for it before you can use the camera.

Activation via Web Browser, Activation via SADP, and Activation via Client Software are all supported.

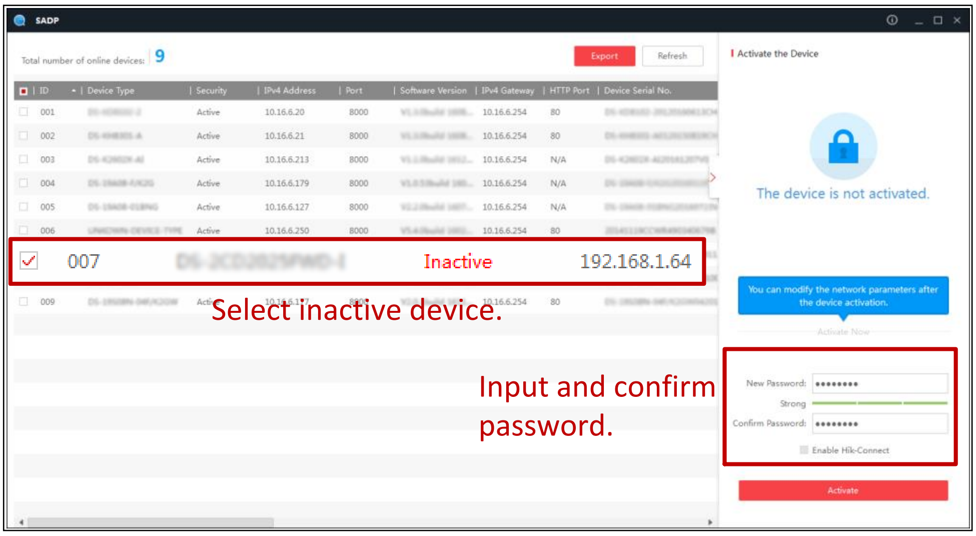
2.2.1 Activation via SADP Software

SADP software is used for detecting the online device, activating the camera, and resetting the password.

Get the SADP software from the official website, and install the SADP according to the prompts. Follow the steps to activate the camera.

Step 1 Run the SADP software to search the online devices.

Step 2 Check the device status from the device list, and select the inactive device.



Total number of online devices: 9

☐	ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
☐	001	[illegible]	Active	10.16.6.20	8000	[illegible]	10.16.6.254	80	[illegible]
☐	002	[illegible]	Active	10.16.6.21	8000	[illegible]	10.16.6.254	80	[illegible]
☐	003	[illegible]	Active	10.16.6.213	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐	004	[illegible]	Active	10.16.6.179	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐	005	[illegible]	Active	10.16.6.127	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐	006	[illegible]	Active	10.16.6.250	8000	[illegible]	10.16.6.254	80	[illegible]
☑	007	[illegible]	Inactive	192.168.1.64					
☐	009	[illegible]	Active	10.16.6.177	8000	[illegible]	10.16.6.254	80	[illegible]

Select inactive device.

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

Activate Now

Input and confirm password.

New Password: ••••••••

Strong

Confirm Password: ••••••••

☐ Enable Hik-Connect

Figure 2-3 SADP Interface

Note

The SADP software supports activating the camera in batch. Refer to the user manual of SADP software for details.

Step 3 Create and input the password in the password field, and confirm the password. A password with user name in it is not allowed.

Caution

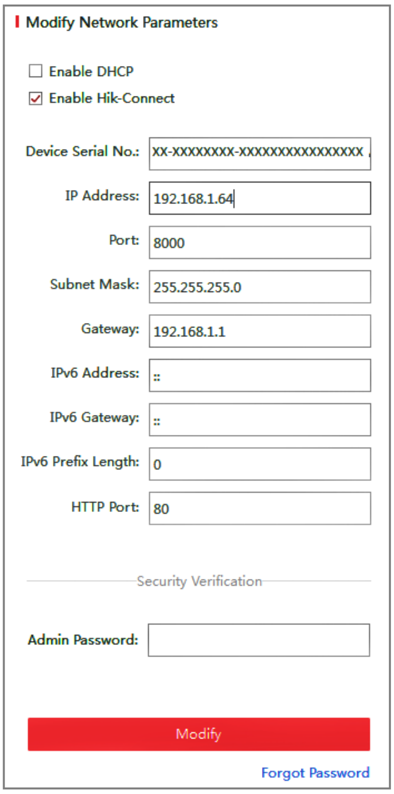
STRONG PASSWORD RECOMMENDED

- We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

You can enable the Hik-Connect service for the device during activation.

Step 4 Click Activate to start activation. You can check whether the activation is completed on the popup window. If activation failed, please make sure that the password meets the requirement and try again.

Step 5 Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.



Modify Network Parameters

□ Enable DHCP

☑ Enable Hik-Connect

Device Serial No.: XX-XXXXXXXX-XXXXXXXXXXXXXXXX

IP Address: 192.168.1.64

Port: 8000

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

IPv6 Address: ::

IPv6 Gateway: ::

IPv6 Prefix Length: 0

HTTP Port: 80

Security Verification

Admin Password:

Figure 2-4 Modify the IP Address

Step 6 Input the admin password and click Modify to activate your IP address modification.

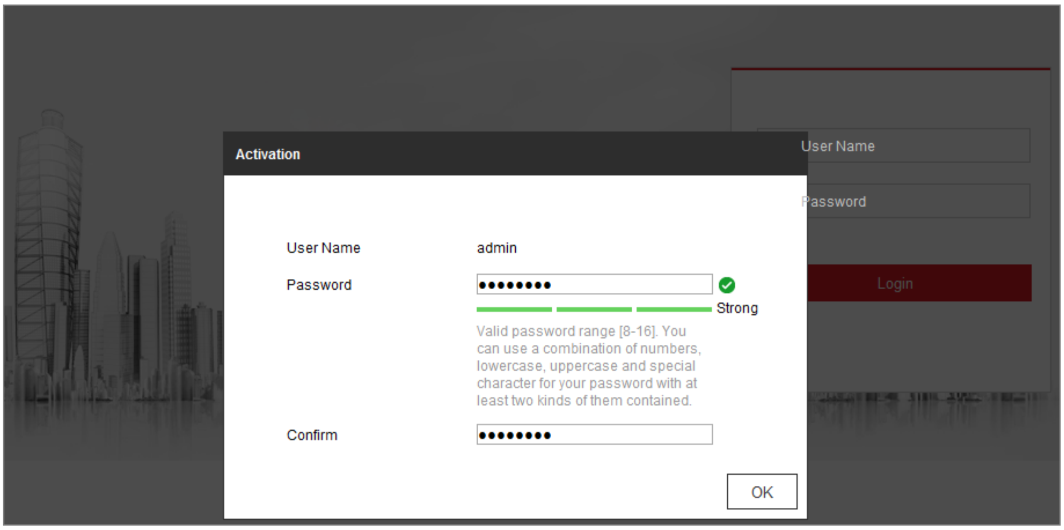
2.2.2 Activation via Web Browser

Step 1 Power on the camera, and connect the camera to the network.

Step 2 Input the IP address into the address bar of the web browser, and click Enter to enter the activation interface.

Note

- The default IP address of the camera is 192.168.1.64.
- The computer and the camera should belong to the same subnet.
- For the camera enables the DHCP by default, you need to use the SADP software to search the IP address.



Activation

User Name admin

Password •••••••• Strong

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Confirm ••••••••

Figure 2-5 Activation via Web Browser

Step 3 Create and input a password into the password field. A password with user name in it is not allowed.

Caution

STRONG PASSWORD RECOMMENDED

We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Step 4 Confirm the password.

Step 5 Click OK to save the password and enter the live view interface.

2.2.3 (Optional) Setting Security Question

Security question is used to reset the admin password when admin user forgets the password.

Admin user can follow the pop-up window to complete security question settings during camera activation. Or, admin user can go to User Management interface to set up the function.

2.3 Login and Logout

2.3.1 Login

For certain camera models, HTTPS is enabled by default and the camera creates an unsigned certificate automatically. When you access to the camera the first time, the web browser prompts a notification about the certificate issue.

To cancel the notification, install a signed-certificate to the camera.

Step 1 Open the web browser.

Step 2 In the browser address bar, input the IP address of the network camera, and press the Enter key to enter the login interface.

Note

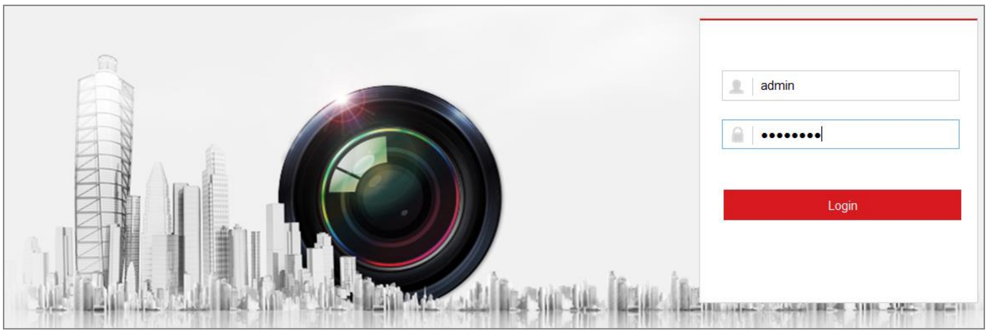
The default IP address is 192.168.1.64. You are recommended to change the IP address to the same subnet with your computer.

Step 3 Input the user name and password.

The admin user should configure the device accounts and user/operator permissions properly. Delete the unnecessary accounts and user/operator permissions.

Note

The IP address gets locked if the admin user performs 7 failed password attempts (5 attempts for the user/operator).



admin

••••••••

Figure 2-6 Login Interface

Step 4 Click **Login**.

Step 5 (Optional) Install the plug-in before viewing the live video and operating the camera. Follow the installation prompts to install the plug-in.

Table 2-1 Install Plugins

OS	Browser Version	Plugin
Windows	● IE 8 and upper ● Google Chrome 57 and lower ● Mozilla Firefox 52 and lower	Install the plugin according to instructions.
	● Google Chrome 57 and upper ● Mozilla Firefox 52 and upper	Click in the preview page to download and install the plugin for high quality view and device functions.
Mac OS	● Google Chrome 57 and upper ● Mozilla Firefox 52 and upper ● Mac Safari 16 and upper	To preview, enter Configuration > Network > Advanced Setting > Network Service, and enbale WebSocket. Some functions will be limited after enbling this function, such as video play. The actual equipment shall prevail.

Note

For camera that supports plug-in free live view, if you are using Google Chrome 57 and its above version or Mozilla Firefox 52 and its above version, plug-in installation is not required. But Picture and Playback functions are hidden. To use mentioned function via web browser, change to their lower version, or change to Internet Explorer 8.0 and above version.

2.3.2 Logout

To logout, click the icon.

2.4 Main Interface

The main interface is shown as follows.

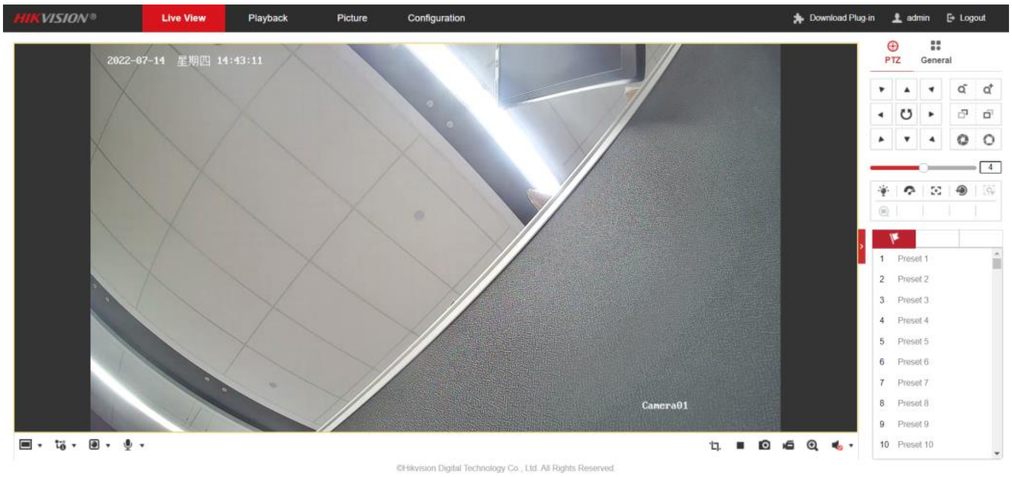


Figure 2-7 Main Interface

Live View: to view the camera and set parameters.

Playback: to play recordings according to their type and time.

Picture: to search, view and download the pictures stored in the SD Card of the network camera.

Configuration: to set the system and function parameters.

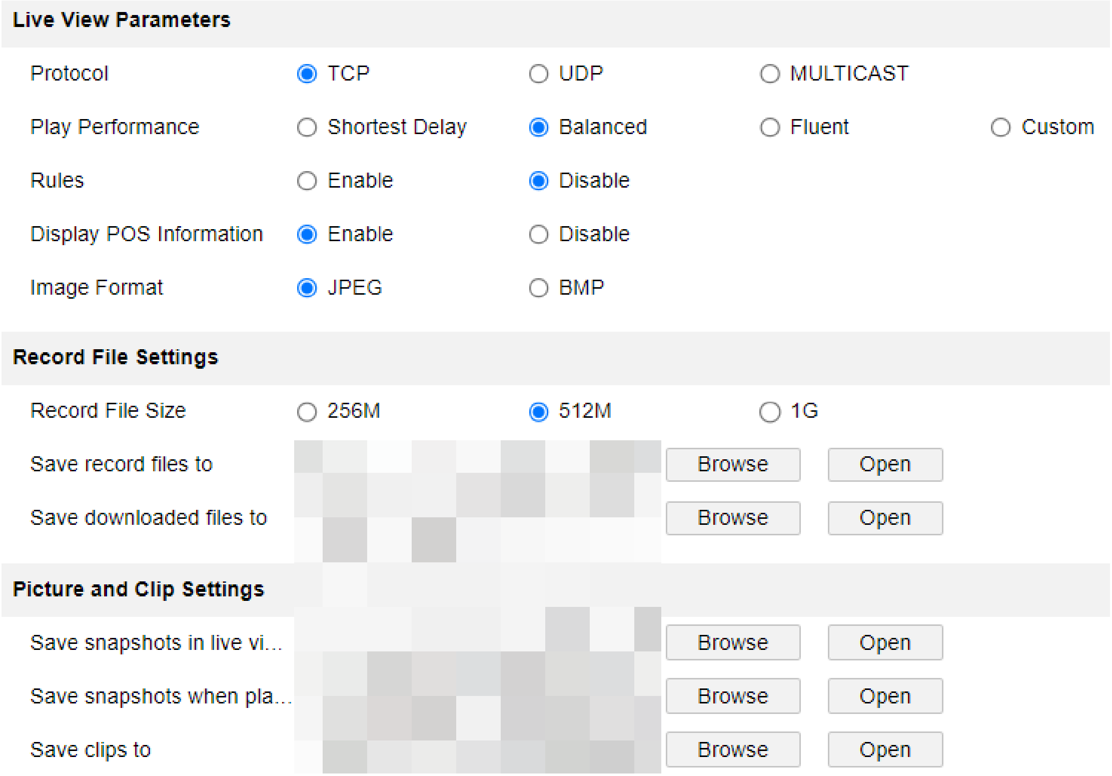
Note

The interface may vary according to the model of the camera.

Chapter 3 Basic Functions

3.1 Local Parameters

Go to **Configuration > Local** to configure local configurations. Live View Parameters, Record File Settings, Picture and Clip Settings can be configured.



Live View Parameters

Protocol	● TCP	○ UDP	○ MULTICAST	
Play Performance	○ Shortest Delay	● Balanced	○ Fluent	○ Custom
Rules	○ Enable	● Disable		
Display POS Information	● Enable	○ Disable		
Image Format	● JPEG	○ BMP		

Record File Settings

Record File Size	○ 256M	● 512M	○ 1G
Save record files to	[redacted]	Browse	Open
Save downloaded files to	[redacted]	Browse	Open

Picture and Clip Settings

Save snapshots in live vi...	[redacted]	Browse	Open
Save snapshots when pla...	[redacted]	Browse	Open
Save clips to	[redacted]	Browse	Open

Figure 3-1 Local Parameters

3.1.1 Live View Parameters

- Protocols

TCP, UDP and MULTICAST protocols are supported.

- – The default protocol is TCP
- – UDP is suitable for the situation that the requirement of video fluency is not high and the network environment is unstable.
- – MULTICAST is suitable for multicast addresses with many customers and need to be configured before selection.

- Playback performance:

You can choose the shortest delay, Balanced, Fluent and Custom, and the default is Custom.

- Minimum delay: Real-time is good, but it may affect the fluency of video.
- Balance: Give consideration to the real-time and fluency of video playback.

- Good fluency: In the same network situation, it takes up less network resources, and the video is smoother than other modes.
- Custom: the frame rate can be set according to the network conditions.
- Information: You can choose to enable or disable it. When enabled, information boxes will appear on the live screen, including the dynamic analysis box of motion detection and the face target box.
- POS information overlay: it can be enabled or disabled. When enabled, when a target triggers a rule, the live screen will display the attribute information of the target.
- Picture and Clip Settings: set the format of captured pictures, with optional JPEG and BMP.

3.1.2 Record File Setting

- Record File Size: it can be set to 256 M, 512 M and 1 G, indicating the size of a single video file stored locally.
- Save record files to: the path where video files are stored locally. You can choose Browse to change the path, and click Open Folder to open the folder under the archive path.
- Save downloaded files to: the path where the video files saved during playback are stored locally. You can choose Browse to change the path, and click Open Folder to open the folder under the archive path.

3.1.3 Picture and Clip Setting

- Save snapshots in live view to: the path where the captured pictures are stored locally during preview. You can choose Browse to change the path, and click Open Folder to open the folder under the archive path.
- Save snapshots when playback to: the path where captured pictures are stored locally during playback. You can choose Browse to change the path, and click Open Folder to open the folder under the archive path.
- Save clips to: the path where the cut video files are stored locally during playback. You can choose Browse to change the path, and click Open Folder to open the folder under the archive path.

3.2 Live View

3.2.1 Live View Page

Purpose:

The live view page allows you to view the real-time video, capture images, realize PTZ control, set/call presets and configure video parameters.

Log in the network camera to enter the live view page, or you can click Live View on the menu bar of the main page to enter the live view page.

Descriptions of the live view page:

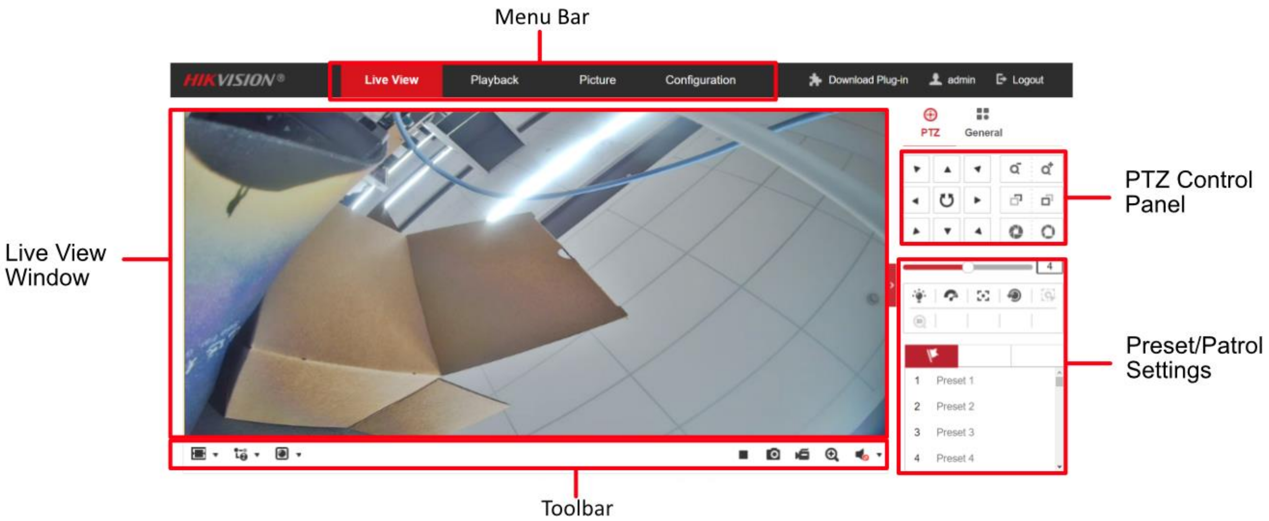


Figure 3-2 Live View Page

- Menu Bar

Click each tab to enter Live View, Playback, Picture, Application, and Configuration page respectively.

- Live View Window

Display the live video.

- Toolbar

Toolbar allows you to adjust the live view window size, the stream type, and the plug-ins. It also allows you to process the operations on the live view page, e.g., start/stop live view, capture, record, audio on/off, two-way audio, start/stop digital zoom, etc.

For IE (Internet Explorer) users, plug-ins as webcomponents and quick time are selectable. And for Non-IE users, webcomponents, quick time, VLC or MJPEG are selectable if they are supported by the web browser.

Note

For camera that supports plug-in free live view, when Google Chrome 45 and its above version or Mozilla Firefox 52 and its above version are used, plug-in installation is not required. But Picture and Playback functions are hidden. To use mentioned function via web browser, change to their lower versions, or change to Internet Explorer 8.0 and its above version.

3.2.2 Starting Live View

In the live view window as shown in Figure 4-2, click ▶ on the toolbar to start the live view of the camera.

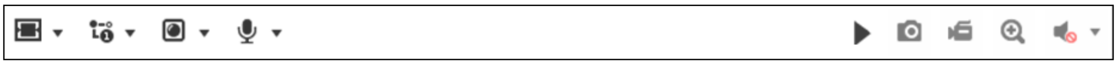


Figure 3-3 Live View Toolbar

Table 3-1 Descriptions of the Toolbar

Icon	Description
▶/■	Start/Stop live view.
4:3	The window size is 4:3.
16:9	The window size is 16:9.
1×	The original widow size.
▣	Self-adaptive window size.
①, ②, ③, etc.	Live view with the different video streams. Supported video streams vary according to camera models.
◉	Click to select the third-party plug-in.
📷	Manually capture the picture.
🎥 / 🎥	Manually start/stop recording.
🔊 ▾/ 🔇	Audio on and adjust volume /Mute.
🎤 / 🎤	Turn on/off microphone.
🔍 / 🔍	Start/stop digital zoom function.

Note

The icons vary according to the different camera models.

3.2.3 Record and Capture Pictures Manually

In the live view interface, click 📷 on the toolbar to capture the live pictures; click 🎥 to record the live view. The saving paths of the captured pictures and clips can be set on the Configuration > Local page. To configure remote scheduled recording, please refer to 10.1 Capture Schedule.

Note

The captured image will be saved as a JPEG file or BMP file in your computer.

3.3 Playback

Purpose:

This section explains how to view the remotely recorded video files stored in the network disks or SD cards.

Step 1 Click **Playback** on the menu bar to enter playback interface.

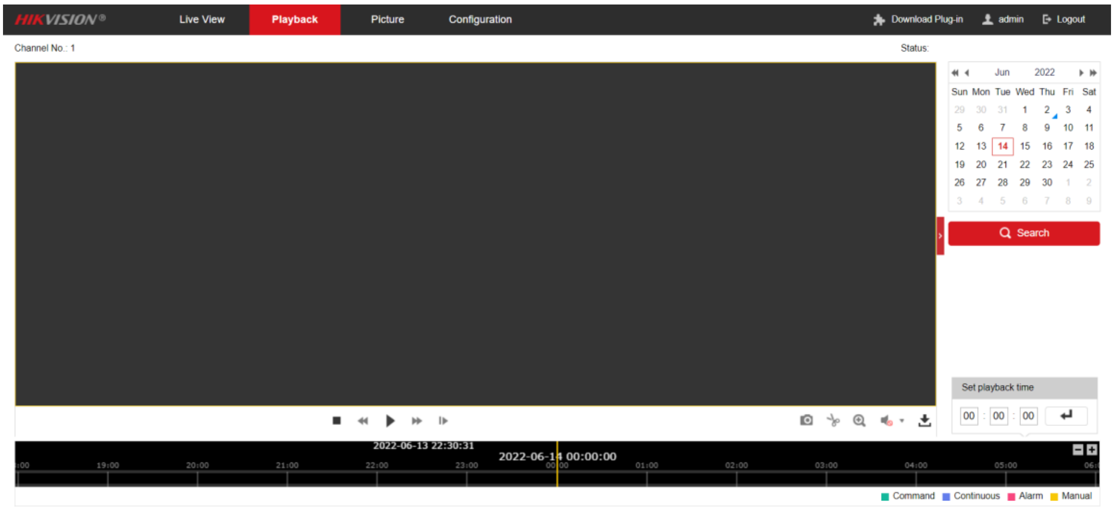
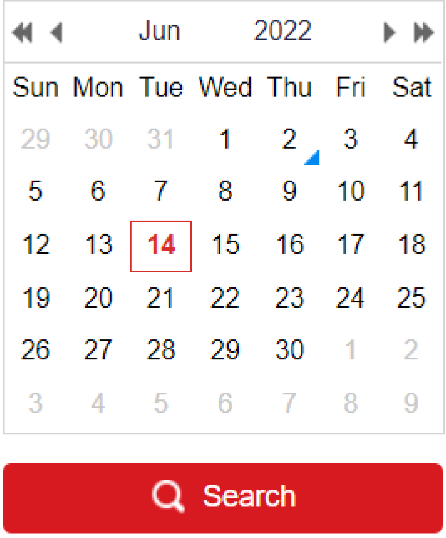


Figure 3-4 Playback Interface

Step 2 Select the date and click **Search**.



Jun 2022

Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2
3	4	5	6	7	8	9

Figure 3-5 Search Video

Step 3 Click ▶ to play the video files found on this date.

The toolbar on the bottom of Playback interface can be used to control playing process.

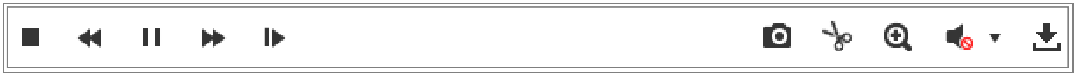


Figure 3-6 Playback Toolbar

Table 3-2 Description of the buttons

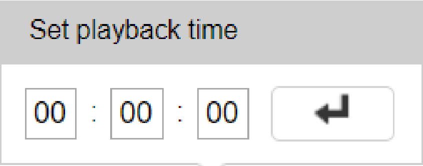
Button	Operation	Button	Operation
▶	Play	📷	Capture a picture
❚❚	Pause	✂ / ✂	Start/Stop clipping video files
■	Stop	🔈	Audio on and adjust volume

⏪	Speed down	🔇	Mute
⏩	Speed up	⬇	Download
🔍 / 🔍	Enable/Disable digital zoom	⏵	Playback by frame

Note

You can choose the file paths locally for downloaded playback video files and pictures in Local Configuration interface.

You can also input the time and click ↵ to locate the playback point in the **Set playback time** field. You can also click ⊟⊞ to zoom out/in the progress bar.



Set playback time

00 : 00 : 00 ↵

Figure 3-7 Set Playback Time

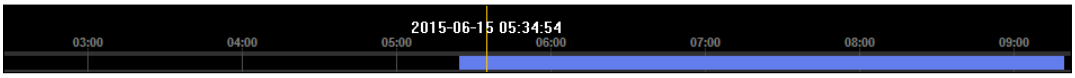
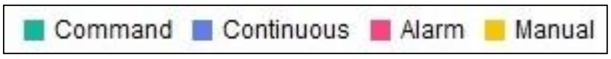


Figure 3-8 Progress Bar

The different colors of the video on the progress bar stand for the different video types.



🟩 Command 🟦 Continuous 🟥 Alarm 🟨 Manual

Figure 3-9 Video Types

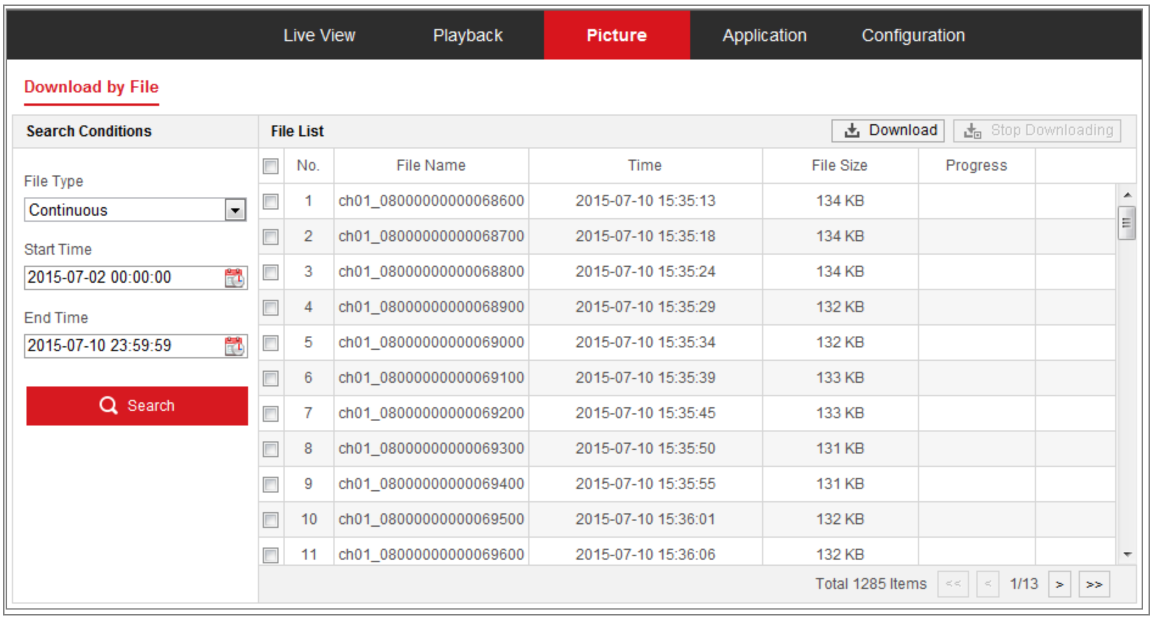
3.4 Picture

Purpose:

Click Picture to enter the picture searching interface. You can search, view, and download the pictures stored in the local storage or network storage.

Note

- Make sure HDD, NAS or memory card are properly configured before you process the picture search.
- Make sure the capture schedule is configured. Go to **Configuration > Storage** > **Schedule Settings** > **Capture** to set the capture schedule.



File Type: Continuous

Start Time: 2015-07-02 00:00:00

End Time: 2015-07-10 23:59:59

□	No.	File Name	Time	File Size	Progress
□	1	ch01_08000000000068600	2015-07-10 15:35:13	134 KB	
□	2	ch01_08000000000068700	2015-07-10 15:35:18	134 KB	
□	3	ch01_08000000000068800	2015-07-10 15:35:24	134 KB	
□	4	ch01_08000000000068900	2015-07-10 15:35:29	132 KB	
□	5	ch01_08000000000069000	2015-07-10 15:35:34	132 KB	
□	6	ch01_08000000000069100	2015-07-10 15:35:39	133 KB	
□	7	ch01_08000000000069200	2015-07-10 15:35:45	133 KB	
□	8	ch01_08000000000069300	2015-07-10 15:35:50	131 KB	
□	9	ch01_08000000000069400	2015-07-10 15:35:55	131 KB	
□	10	ch01_08000000000069500	2015-07-10 15:36:01	132 KB	
□	11	ch01_08000000000069600	2015-07-10 15:36:06	132 KB	

Total 1285 Items << < 1/13 > >>

Figure 3-10 Picture Search Interface

Step 2 Select the file type from the dropdown list. Continuous, Motion, Alarm, Motion | Alarm, Motion & Alarm, Line Crossing, Intrusion Detection, and Scene Change Detection are selectable.

Step 3 Select the start time and end time.

Step 4 Click **Search** to search the matched pictures.

Step 5 Check the checkbox of the pictures and then click **Download** to download the selected pictures.

Note

Up to 4000 pictures can be displayed at one time.

Chapter 4 System Configuration

4.1 Configure System Settings

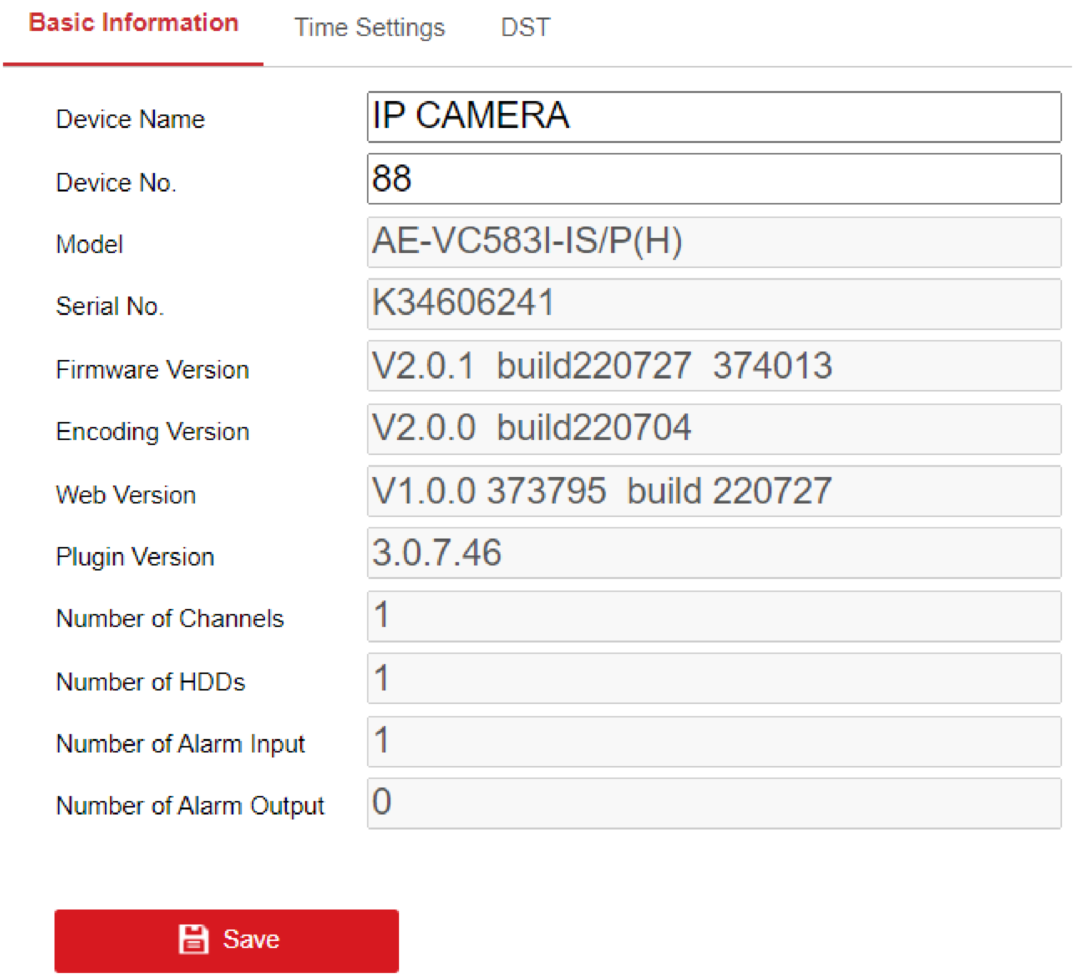
Purpose:

Follow the instructions below to configure the system settings, include System Settings, Maintenance, Security, and User Management, etc.

4.1.1 Basic Information

Step 1 Go to **Configuration** > **System** > **System Settings** > **Basic Information**.

Step 2 Edit the Device Name and Device No.



Device Name	IP CAMERA
Device No.	88
Model	AE-VC583I-IS/P(H)
Serial No.	K34606241
Firmware Version	V2.0.1 build220727 374013
Encoding Version	V2.0.0 build220704
Web Version	V1.0.0 373795 build 220727
Plugin Version	3.0.7.46
Number of Channels	1
Number of HDDs	1
Number of Alarm Input	1
Number of Alarm Output	0

Figure 4-1 Basic Information

Note

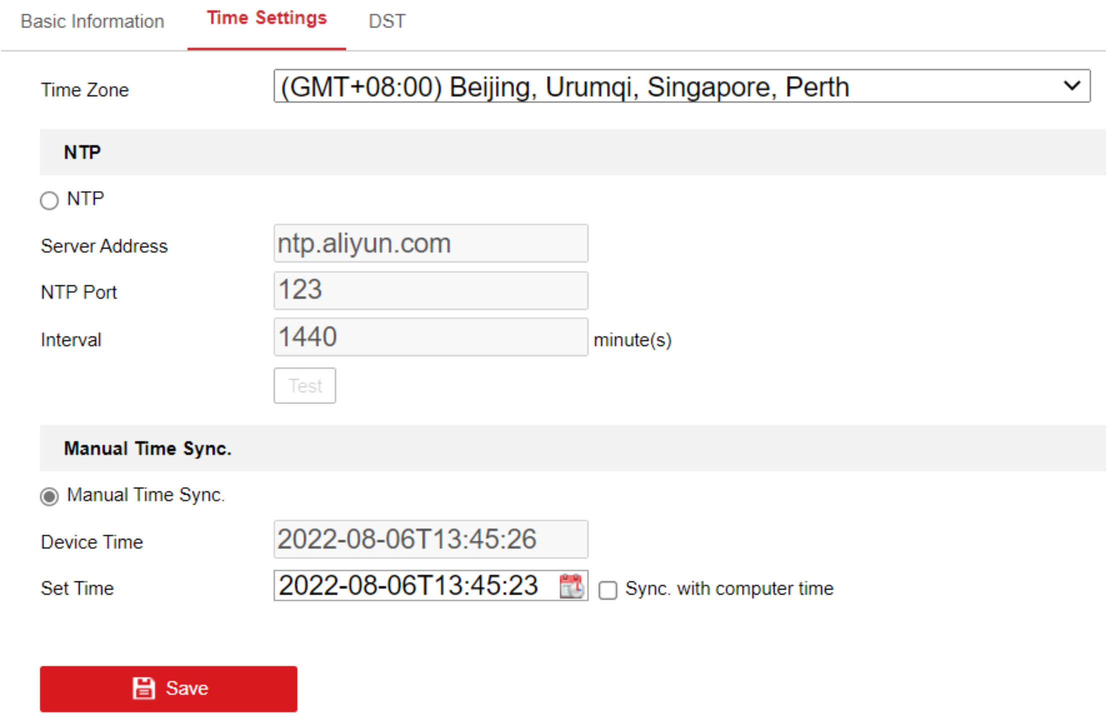
Other information of the network camera, such as Model, Serial No., Firmware Version, Encoding Version, Number of Channels, Number of HDDs, Number of Alarm Input and Number of Alarm Output are displayed. The information cannot be changed in this menu. These options are the reference for maintenance or modification in future.

4.1.2 Time Settings

Purpose:

You can follow the instructions in this section to configure the time synchronization and DST settings.

Step 1 Go to **Configuration** > **System**> **System Settings** > **Time Settings**.



Time Zone: (GMT+08:00) Beijing, Urumqi, Singapore, Perth

NTP

○ NTP

Server Address: ntp.aliyun.com

NTP Port: 123

Interval: 1440 minute(s)

Manual Time Sync.

● Manual Time Sync.

Device Time: 2022-08-06T13:45:26

Set Time: 2022-08-06T13:45:23 □ Sync. with computer time

Figure 4-2 Time Settings

Step 2 Select the Time Zone of your location from the drop-down menu.

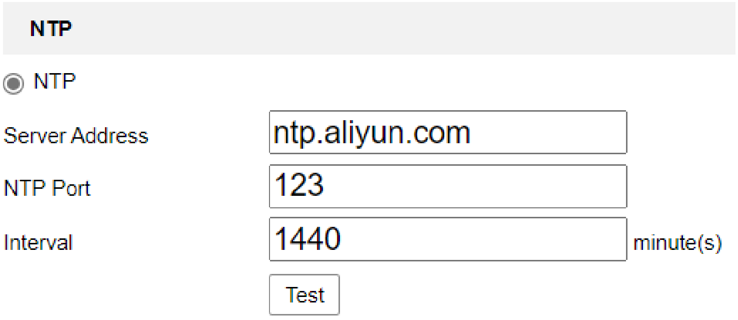
Step 3 Configure the NTP settings.

Step 4 Click to enable the NTP function.

Step 5 Configure the following settings:

- Server Address: IP address of NTP server.
- NTP Port: Port of NTP server.
- Interval: The time interval between the two synchronizing actions with NTP server.

Step 6 (Optional) You can click the Test button to test the time synchronization function via NTP server.



NTP

● NTP

Server Address: ntp.aliyun.com

NTP Port: 123

Interval: 1440 minute(s)

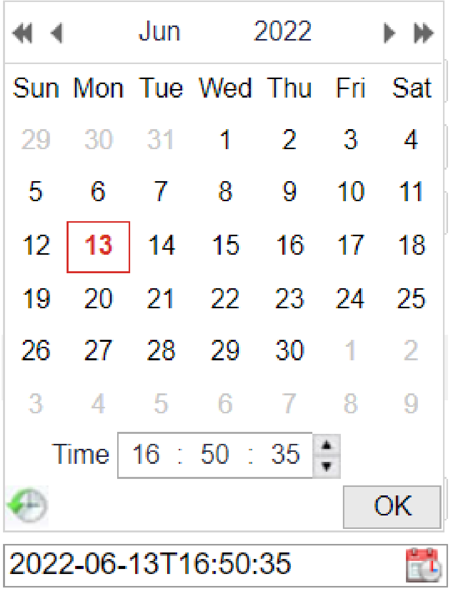
Time Sync by NTP Server

Note

If the camera is connected to a public network, you should use a NTP server that has a time synchronization function, such as the server at the National Time Center (IP Address: 210.72.145.44). If the camera is set in a customized network, NTP software can be used to establish a NTP server for time synchronization.

Step 7 Configure the manual time synchronization.

1) Check the Manual Time Sync. item to enable the manual time synchronization function.
2) Click the icon to select the date, time from the pop-up calendar.
3) (Optional) You can check Sync. with computer time item to synchronize the time of the device with that of the local PC.



Jun 2022

Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2
3	4	5	6	7	8	9

Time 16 : 50 : 35

2022-06-13T16:50:35

Figure 4-3 Time Sync Manually

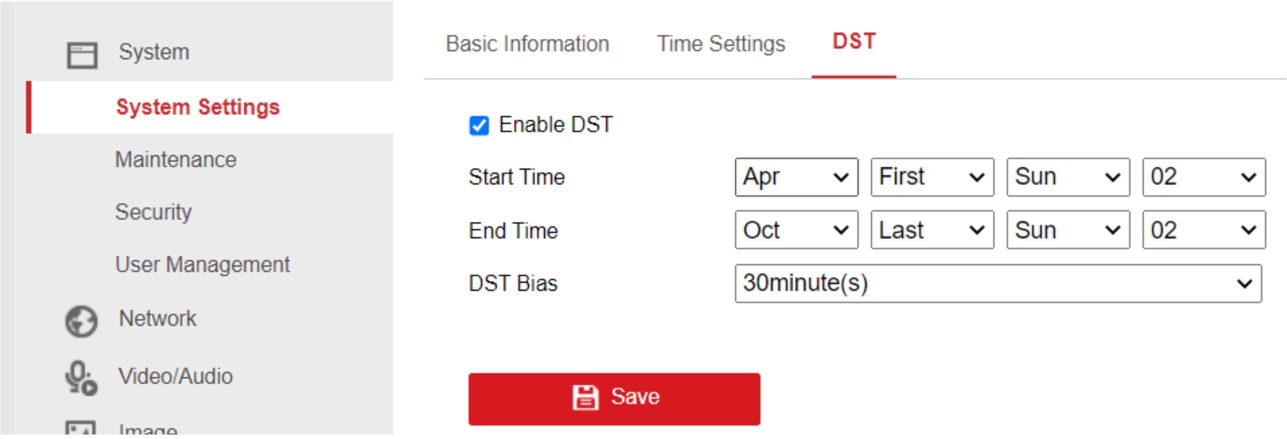
Step 8 Click Save to save the settings.

4.1.3 DST

Purpose:

Daylight Saving Time (DST) is a way of making better use of the natural daylight by setting your clock forward one hour during the summer months, and back again in the fall.

Step 1 Go to **Configuration** > **System** > **System Settings** > **DST**.



☑ Enable DST

Start Time Apr First Sun 02

End Time Oct Last Sun 02

DST Bias 30minute(s)

Figure 4-4 DST Settings

Step 2 Check Enable DST.

Step 3 Select the start time and the end time.

Step 4 Select the DST Bias.

Step 5 Click **Save** to activate the settings.

4.2 Maintenance

4.2.1 Upgrade & Maintenance

Purpose:

The upgrade & maintenance interface allows you to process the operations, including reboot, partly restore, restore to default, export/import the configuration files, and upgrade the device.

Step 1 Go to **Configuration** > **System** > **Maintenance** > **Upgrade & Maintenance**.

- Reboot: Restart the device.
- Restore: Reset all the parameters, except the IP parameters and user information, to the default settings.
- Default: Restore all the parameters to the factory default.

Note

- After restoring the default settings, the IP address is also restored to the default IP address, please be careful for this action.
- For camera that supports Wi-Fi, wireless dial, or wlan function, Restore action does not restore the related settings of mentioned functions to default.

- Information Export

Device Parameters: click to export the current configuration file of the camera.

This operation requires admin password to proceed.

For the exported file, you also have to create an encryption password. The encryption password is required when you import the file to other cameras.

Diagnose Information: click to download log and system information.

- Import Config. File

Configuration file is used for the batch configuration of the cameras.

Step 2 Click Browse to select the saved configuration file.

Step 3 Click Import and input the encryption password that you set during exporting.

Note

The camera needs rebooting after importing configuration file.

Upgrade: Upgrade the device to a certain version.

Step 4 Select firmware or firmware directory to locate the upgrade file.

- Firmware: Locate the exact path of the upgrade file.
- Firmware Directory: Only the directory the upgrade file belongs to is required.

Step 5 Click Browse to select the local upgrade file and then click Upgrade to start remote upgrade.

Note

The upgrading process will take 1 to 10 minutes. Please don't disconnect power of the camera during the process, and the camera reboots automatically after upgrade.

4.2.2 Log

Purpose:

The operation, alarm, exception and information of the camera can be stored in log files. You can also export the log files on your demand.

Before you start:

Please configure network storage for the camera or insert a SD card in the camera.

Step 1 Go to **Configuration** > **System** > **Maintenance** > **Log**.

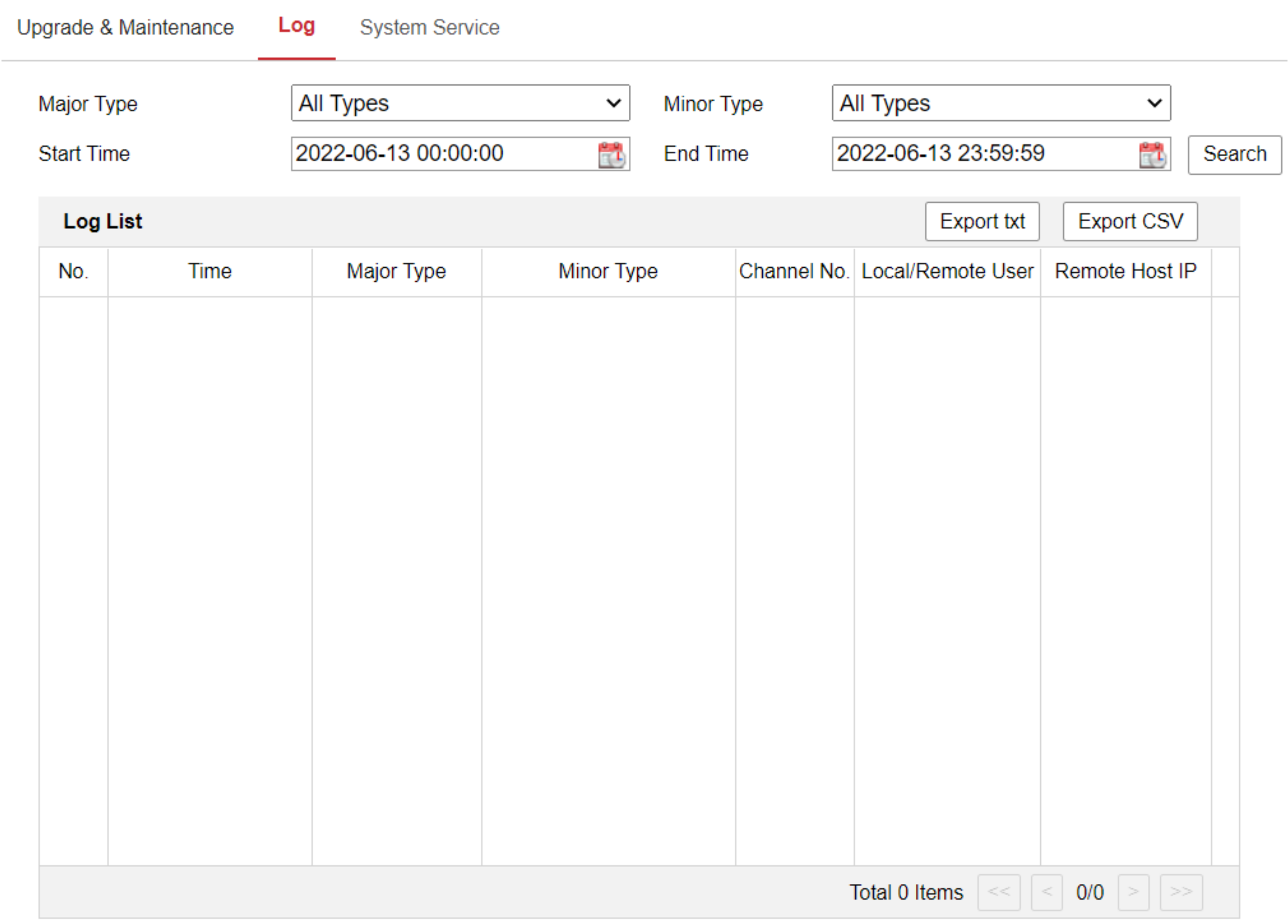
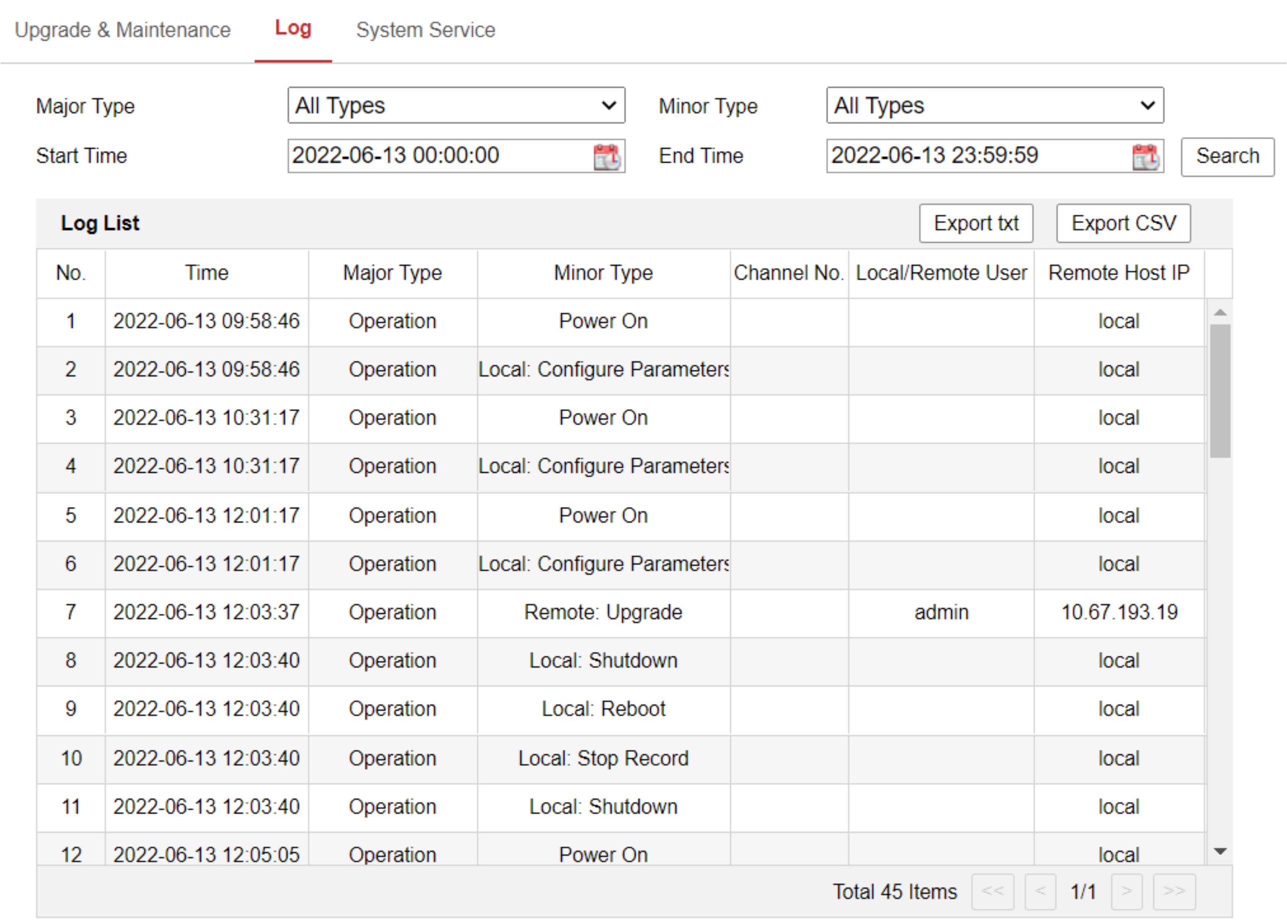


Figure 4-5 Log Searching Interface

Step 2 Set the log search conditions to specify the search, including the Major Type, Minor Type, Start Time and End Time.

Step 3 Click **Search** to search log files. The matched log files will be displayed on the log list interface.



Major Type: All Types
Minor Type: All Types
Start Time: 2022-06-13 00:00:00
End Time: 2022-06-13 23:59:59

No.	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP
1	2022-06-13 09:58:46	Operation	Power On			local
2	2022-06-13 09:58:46	Operation	Local: Configure Parameters			local
3	2022-06-13 10:31:17	Operation	Power On			local
4	2022-06-13 10:31:17	Operation	Local: Configure Parameters			local
5	2022-06-13 12:01:17	Operation	Power On			local
6	2022-06-13 12:01:17	Operation	Local: Configure Parameters			local
7	2022-06-13 12:03:37	Operation	Remote: Upgrade		admin	10.67.193.19
8	2022-06-13 12:03:40	Operation	Local: Shutdown			local
9	2022-06-13 12:03:40	Operation	Local: Reboot			local
10	2022-06-13 12:03:40	Operation	Local: Stop Record			local
11	2022-06-13 12:03:40	Operation	Local: Shutdown			local
12	2022-06-13 12:05:05	Operation	Power On			local

Total 45 Items

Figure 4-6 Log Searching

Step 4 To export the log files, click **Export** to save the log files.

4.2.3 System Service

Purpose:

System service settings refer to the hardware service the camera supports. Supported functions vary according to the different cameras. For the cameras support IR Light, ABF (Auto Back Focus), Auto Defog, or Status LED, you can select to enable or disable the corresponding service according to the actual demands.

- **ABF:** When ABF function is enabled, you can click ⛶ on PTZ control panel to realize auxiliary focus.
- **Third Stream**: For some models, third stream is not enabled by default. Check **Enable Third Stream** to enable the function. When the Third Stream is enabled, the smart event will not be supported.

4.3 Security

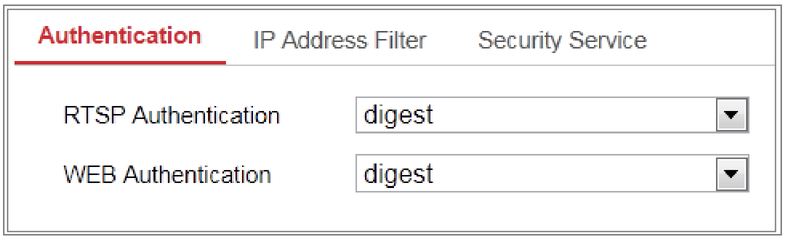
Configure the parameters, including Authentication, IP Address Filter, and Security Service from security interface.

4.3.1 Authentication

Purpose:

You can specifically secure the stream data of live view.

Step 1 Go to **Configuration** > **System** > **Security** > **Authentication**.



RTSP Authentication: digest

WEB Authentication: digest

Figure 4-7 Authentication

Step 2 Set up authentication method for RTSP authentication and WEB authentication.

Caution

Digest is the recommended authentication method for better data security. You must be aware of the risk if you adopt basic as the authentication method.

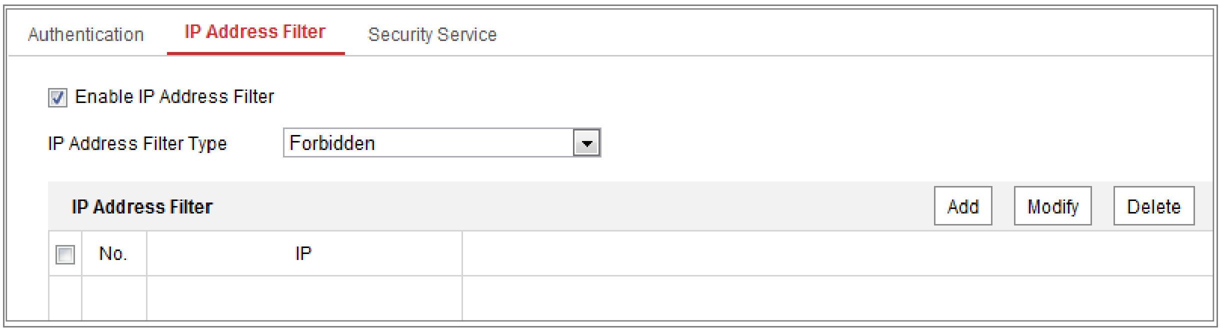
Step 3 Click **Save**.

4.3.2 IP Address Filter

Purpose:

This function makes it possible for access control.

Step 1 Go to **Configuration** > **System** > **Security** > **IP Address Filter**



☑ Enable IP Address Filter

IP Address Filter Type: Forbidden

IP Address Filter

□	No.	IP

Figure 4-8 IP Address Filter Interface

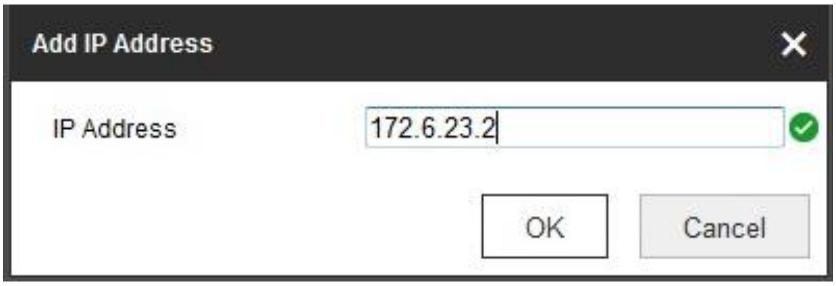
Step 2 Check the checkbox of Enable IP Address Filter.

Step 3 Select the type of IP Address Filter in the drop-down list, **Forbidden** and **Allowed** are selectable.

Step 4 Set the IP Address Filter list.

- Add an IP Address

1) Click the **Add** to add an IP.
2) Input the IP Adreess.



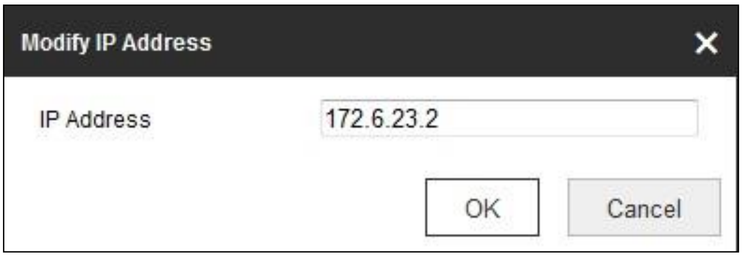
IP Address: 172.6.23.2

Add an IP

3) Click the **OK** to finish adding.

- Modify an IP Address

1) Left-click an IP address from filter list and click **Modify**.
2) Modify the IP address in the text filed.



IP Address: 172.6.23.2

Modify an IP

3) Click the **OK** to finish modifying.

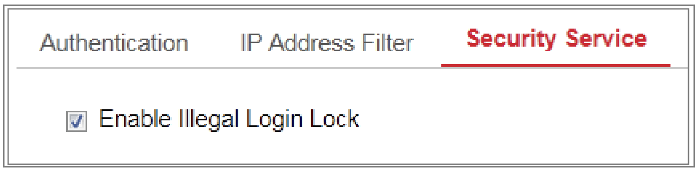
- Delete an IP Address or IP Addresses.

1) Select the IP address(es) and click **Delete**.
2) Click **Save** to save the settings.

4.3.3 Security Service

To enable the remote login, and improve the data communication security, the camera provides the security service for better user experience.

Step 1 Go to Configuration > System > Security > Security Service.



☑ Enable Illegal Login Lock

Figure 4-9 Security Service

Step 2 Check the checkbox of Enable Illegal Login Lock.

Step 3 Illegal Login Lock: it is used to limit the user login attempts. Login attempt from the IP address is rejected if admin user performs 7 failed user name/password attempts (5 times for the operator/user).

Note

If the IP address is rejected, you can try to login the device after 30 minutes.

4.4 User Management

4.4.1 User Management

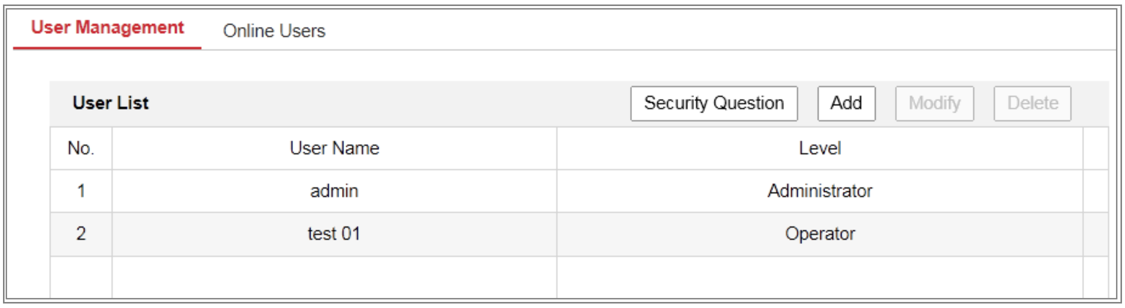
Administrator

The admin user can add, delete or modify user accounts, and grant them different permissions. We highly recommend you manage the user accounts and permissions properly.

Step 1 Go to **Configuration** > **System** > **User Management**.

Note

Admin password if required for adding and modifying a user account.



No.	User Name	Level
1	admin	Administrator
2	test 01	Operator

Figure 4-10 User Management Interface

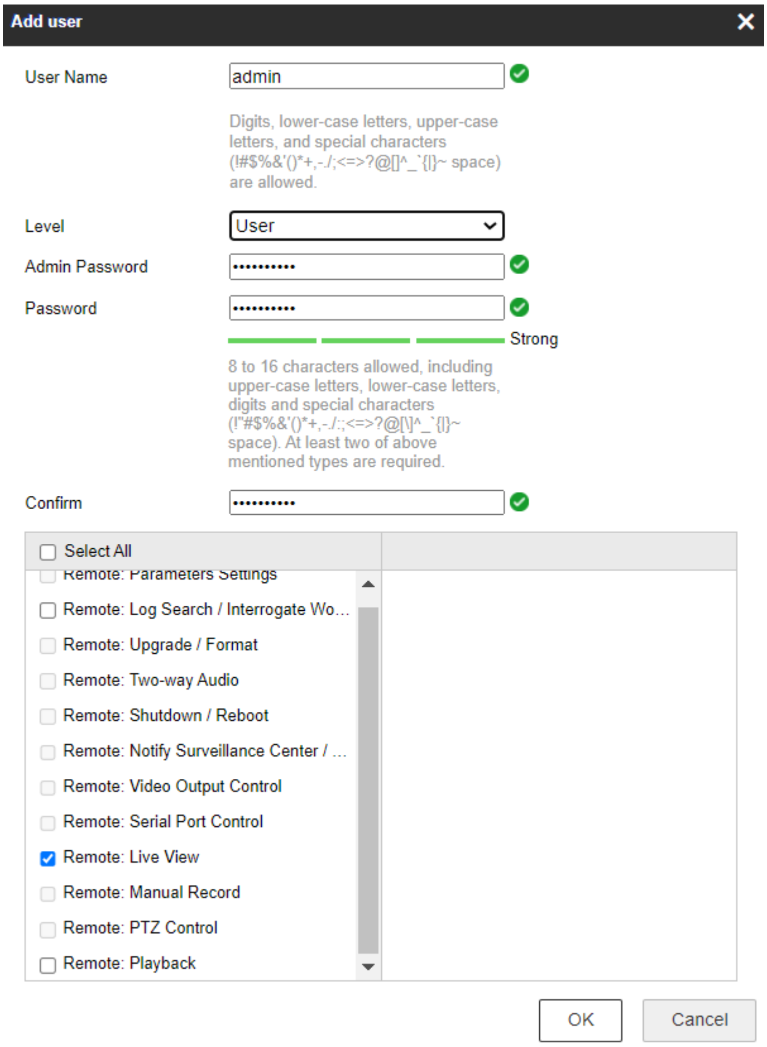
Adding a User

The *admin* user has all permissions by default and can create/modify/delete other accounts.

The *admin* user cannot be deleted and you can only change the *admin* password.

Step 2 Click **Add** to add a user.

Step 3 Input the Admin Password, User Name, select Level and input Password.



Add user ✕

User Name: admin ✓

Digits, lower-case letters, upper-case letters, and special characters (!#$%&'()*+,-./;<=>?@[]^_`{|}~ space) are allowed.

Level: User

Admin Password: •••••••••• ✓

Password: •••••••••• ✓

Strong

8 to 16 characters allowed, including upper-case letters, lower-case letters, digits and special characters (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ space). At least two of above mentioned types are required.

Confirm: •••••••••• ✓

□ Select All

□ Remote: Parameters Settings
□ Remote: Log Search / Interrogate Wo…
□ Remote: Upgrade / Format
□ Remote: Two-way Audio
□ Remote: Shutdown / Reboot
□ Remote: Notify Surveillance Center / …
□ Remote: Video Output Control
□ Remote: Serial Port Control
☑ Remote: Live View
□ Remote: Manual Record
□ Remote: PTZ Control
□ Remote: Playback

Figure 4-11 Add a User

Note

Up to 16 user accounts can be created.

Users of different levels own different default permissions. Operator and user are selectable.

Caution

Strong Password recommended

We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Step 4 You can check or uncheck the permissions for the new user.

Step 5 Click **OK** to finish the user addition.

Modify a User

Step 6 Left-click to select the user from the list and click **Modify**.

Step 7 Modify the User Name, Level and Password.

⚠ **Caution**

Strong Password recommended

We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Step 8 You can check or uncheck the permissions.

Step 9 Click **OK** to finish the user modification.

Step 10 Deleting a User

1) Click to select the user you want to delete and click **Delete**.
2) Click **OK** on the pop-up dialogue box to confirm the deletion.

Operator/User

Operator or user can modify password. Old password is required for this action.

4.4.2 Security Question

Purpose:

Security question is used to reset the admin password when admin user forgets the password.

Set Security Questions

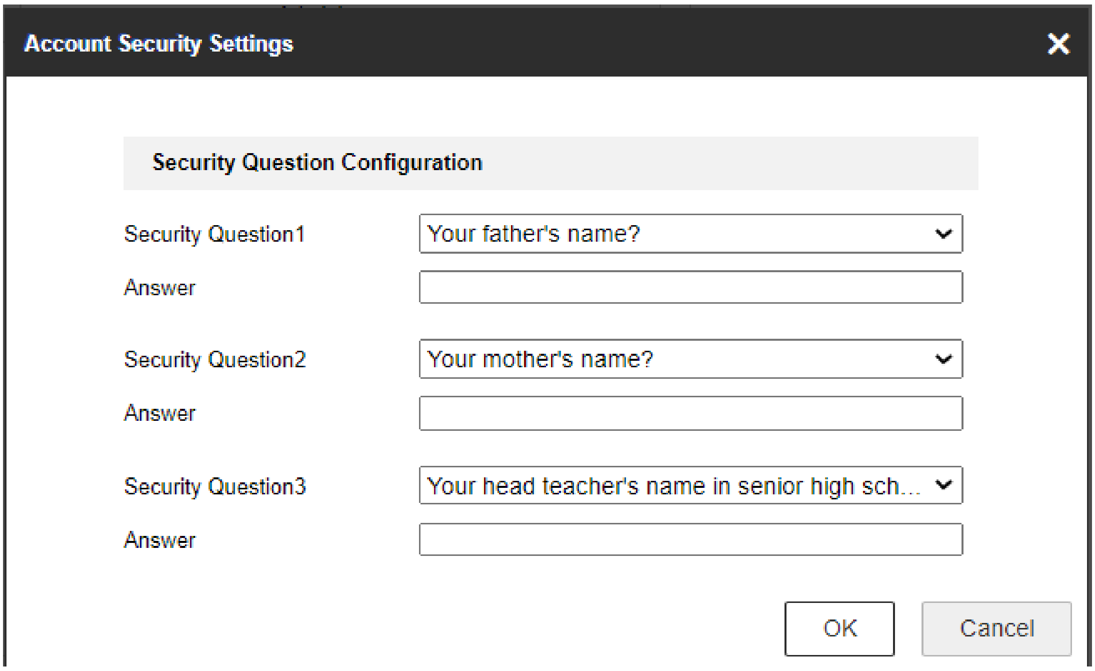
You can set the security questions during camera activation. Or you can set the function at user management interface.

Security question setting is not cleared when you restore the camera (not to default).

Steps:

Step 1 Go to **Configuration** > **System** > **User Management**.

Step 2 Click Account Security Question.



Account Security Settings

Security Question Configuration

Security Question1: Your father's name?

Answer:

Security Question2: Your mother's name?

Answer:

Security Question3: Your head teacher's name in senior high sch...

Answer:

Figure 4-12 Account Security Question

Step 3 Select questions and input answers.

Step 4 Click **OK** to save the settings.

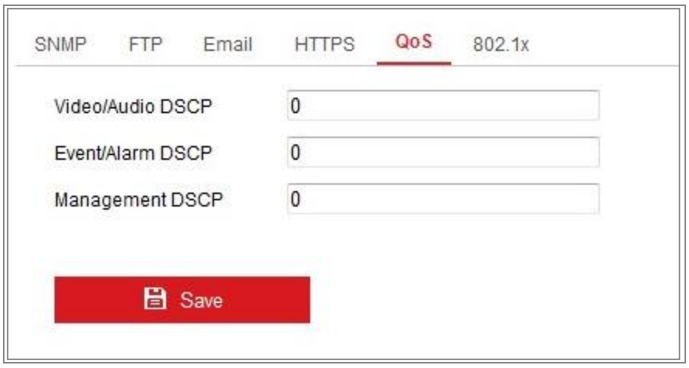
Reset Admin Password:

Before you start:

The PC used to reset password and the camera should belong to the same IP address segment of the same LAN.

Steps:

Step 5 Go to **Configuration** > **Network** > **Advanced Settings** > **QoS**



Video/Audio DSCP: 0

Event/Alarm DSCP: 0

Management DSCP: 0

Figure 4-13 QoS Settings

Step 6 Configure the QoS settings, including Video/Audio DSCP, Event/Alarm DSCP and Management DSCP.

Step 7 The valid value range of the DSCP is 0 to 63. The bigger the DSCP value is, the higher the priority is.

Note

DSCP refers to the Differentiated Service Code Point; and the DSCP value is used in the IP header to indicate the priority of the data.

Step 8 Click **Save** to save the settings.

Note

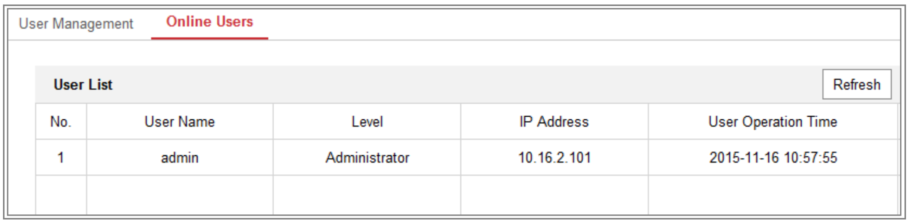
A reboot is required for the settings to take effect.

4.4.3 Online Users

Purpose:

You can see the current users who are visiting the device through this interface. User information, such as user name, level, IP address, and operation time, is displayed in the User List.

Click **Refresh** to refresh the list.



No.	User Name	Level	IP Address	User Operation Time
1	admin	Administrator	10.16.2.101	2015-11-16 10:57:55

Figure 4-14 View the Online Users

Chapter 5 Network Settings

Purpose:

Follow the instructions in this chapter to configure the basic settings and advanced settings.

5.1 Basic Settings

Purpose:

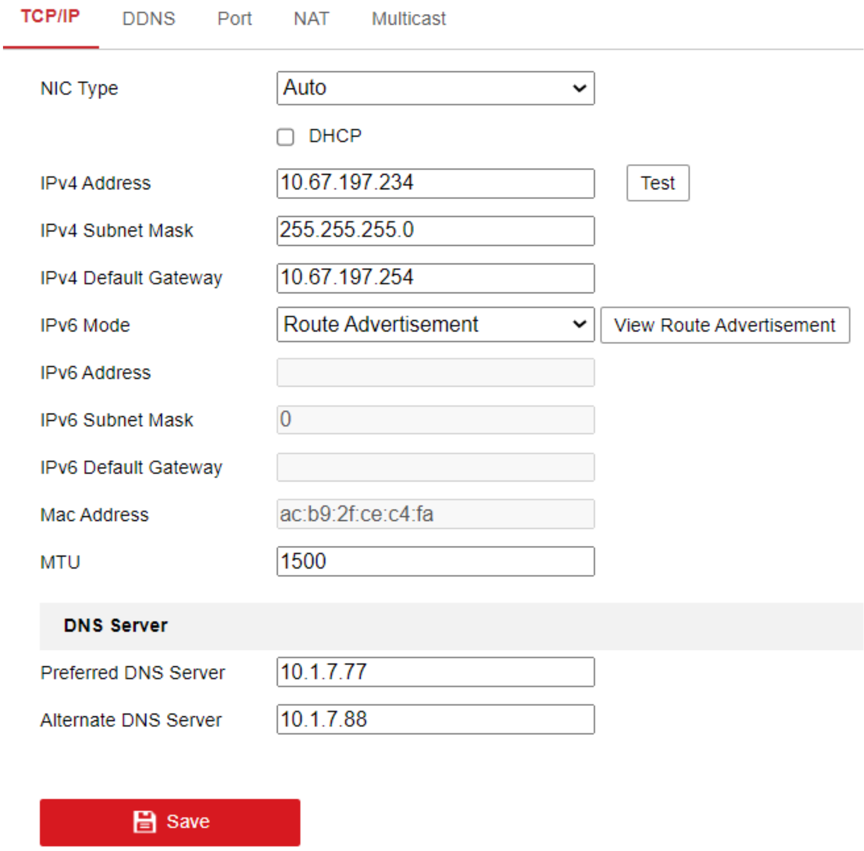
You can configure the parameters, including TCP/IP, DDNS, Port, and NAT, etc., by following the instructions in this section.

5.1.1 TCP/IP

Purpose:

TCP/IP settings must be properly configured before you operate the camera over network. The camera supports both the IPv4 and IPv6. Both versions can be configured simultaneously without conflicting to each other, and at least one IP version should be configured.

Step 1 Go to **Configuration > Network > Basic Settings > TCP/IP**.



NIC Type	Auto
	□ DHCP
IPv4 Address	10.67.197.234
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	10.67.197.254
IPv6 Mode	Route Advertisement
IPv6 Address	
IPv6 Subnet Mask	0
IPv6 Default Gateway	
Mac Address	ac:b9:2f:ce:c4:fa
MTU	1500
DNS Server	
Preferred DNS Server	10.1.7.77
Alternate DNS Server	10.1.7.88

Figure 5-1 TCP/IP Settings

Step 2 Configure the basic network settings, including the NIC Type, IPv4 or IPv6 Address, IPv4 or IPv6 Subnet Mask, IPv4 or IPv6 Default Gateway, and MTU settings.

Step 3 Configure the DNS server. Input the preferred DNS server, and alternate DNS server.

Step 4 Click **Save** to save the above settings.

Note

- The valid value range of MTU is 1280 to 1500.
- A reboot is required for the settings to take effect.

5.1.2 DDNS

Purpose:

As most public internet users in use dynamic IP, Dynamic DNS (DDNS) for network access is best for camera.

Before you start:

Registration on the DDNS server is required before configuring the DDNS settings of the camera.

Step 1 Go to Configuration > Network > Basic Settings > DDNS.

Step 2 Check the Enable DDNS checkbox to enable this feature.

Step 3 Select DDNS Type. Two DDNS types are selectable: DynDNS and NO-IP.

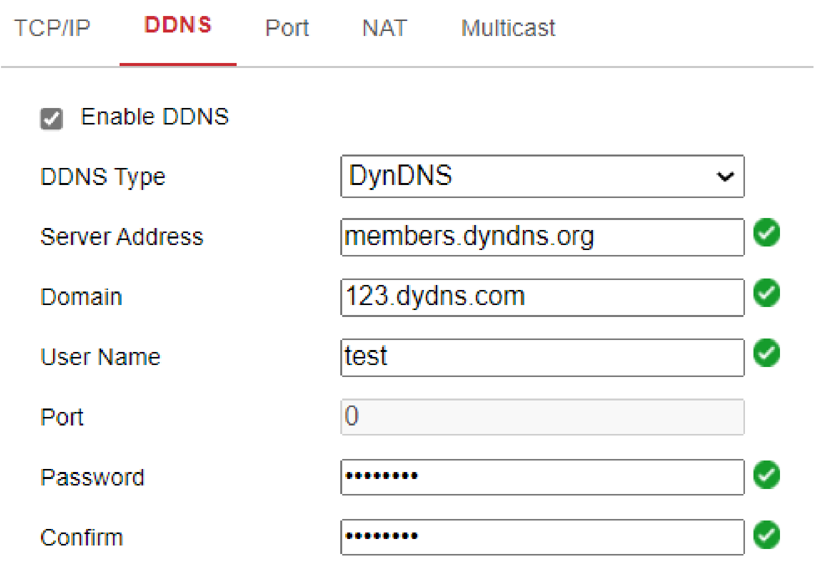
- DynDNS:

Step 1 Enter **Server Address** of DynDNS (e.g. members.dyndns.org).

Step 2 In the **Domain** text field, enter the domain name obtained from the DynDNS website.

Step 3 Enter the **User Name** and **Password** registered on the DynDNS website.

Step 4 Click **Save** to save the settings.



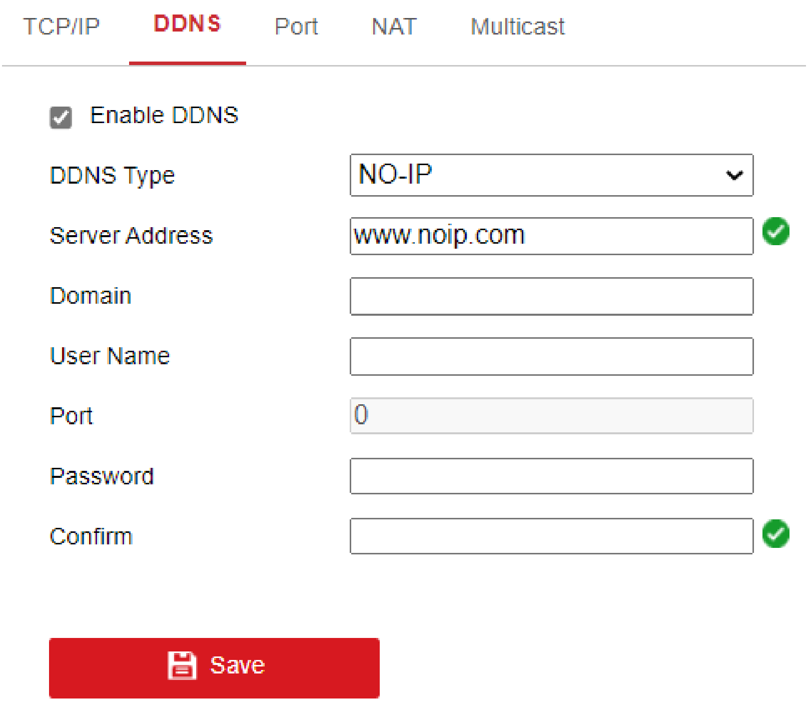
☑ Enable DDNS

DDNS Type	DynDNS
Server Address	members.dyndns.org ✓
Domain	123.dydns.com ✓
User Name	test ✓
Port	0
Password	•••••••• ✓
Confirm	•••••••• ✓

Figure 5-2 DynDNS Settings

- NO-IP:

Step 1 Choose the DDNS Type as NO-IP.



☑ Enable DDNS

DDNS Type	NO-IP
Server Address	www.noip.com ✓
Domain	
User Name	
Port	0
Password	
Confirm	✓

Figure 5-3 NO-IP DNS Settings

Step 2 Enter the Server Address as www.noip.com

Step 3 Enter the Domain name you registered.

Step 4 Enter the User Name and Password.

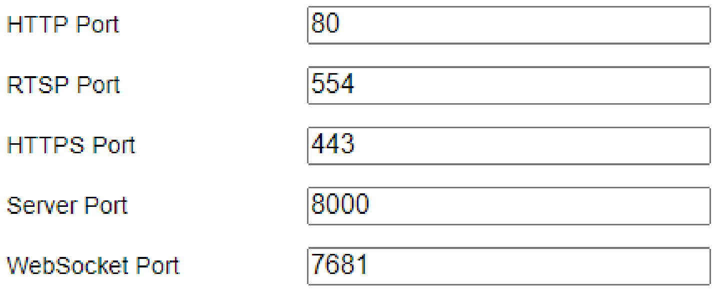
Step 5 Click **Save** and then you can view the camera with the domain name.

Note

Reboot the device to make the settings take effect.

5.1.3 Port

Step 1 Go to **Configuration > Network > Basic Settings > Port**.



HTTP Port	80
RTSP Port	554
HTTPS Port	443
Server Port	8000
WebSocket Port	7681

Figure 5-4 Port Settings

Step 2 Set the ports of the camera.

HTTP Port: The default port number is 80, and it can be changed to any port No. which is not occupied.

RTSP Port: The default port number is 554 and it can be changed to any port No. ranges from 1 to 65535.

HTTPS Port: The default port number is 443, and it can be changed to any port No. which is not occupied.

Server Port: The default server port number is 8000, and it can be changed to any port No. ranges from 2000 to 65535.

WebSocket Port: The default port number is 7681. It can be changed to any port No. ranges from 1 to 65535.

Note

The WebSocket protocol is used for plug-in free live view. For detailed information, see *5.2.7* .

Step 3 Click **Save** to save the settings.

Note

A reboot is required for the settings to take effect.

5.1.4 Multicast

The Multicast sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Before utilizing this function, you have to enable the Multicast function of your router.

Step 1 Go to **Configuration > Network > Basic Settings > Multicast**.

Step 2 Configure the parameters for Multicast.

- IP Address: The IP address of the multicast host.

Note

The range for multicast IP address is 224.0.0.19~239.255.255.255

- Stream Type
  Choose the type of stream according to your needs.

Note

- For some models, the **Third Stream** is not enabled by default. Go to **System** > **Maintenance** > **System Service**> **Software** to enable the function is required.
- The main stream is usually for recording and live view with good bandwidth, and the sub-stream can be used for live view when the bandwidth is limited.
- You can customize the following parameters for the selected stream type.

- Video Port and Audio Port

Step 3 Click **Save**.

5.2 Advanced Settings

Purpose:

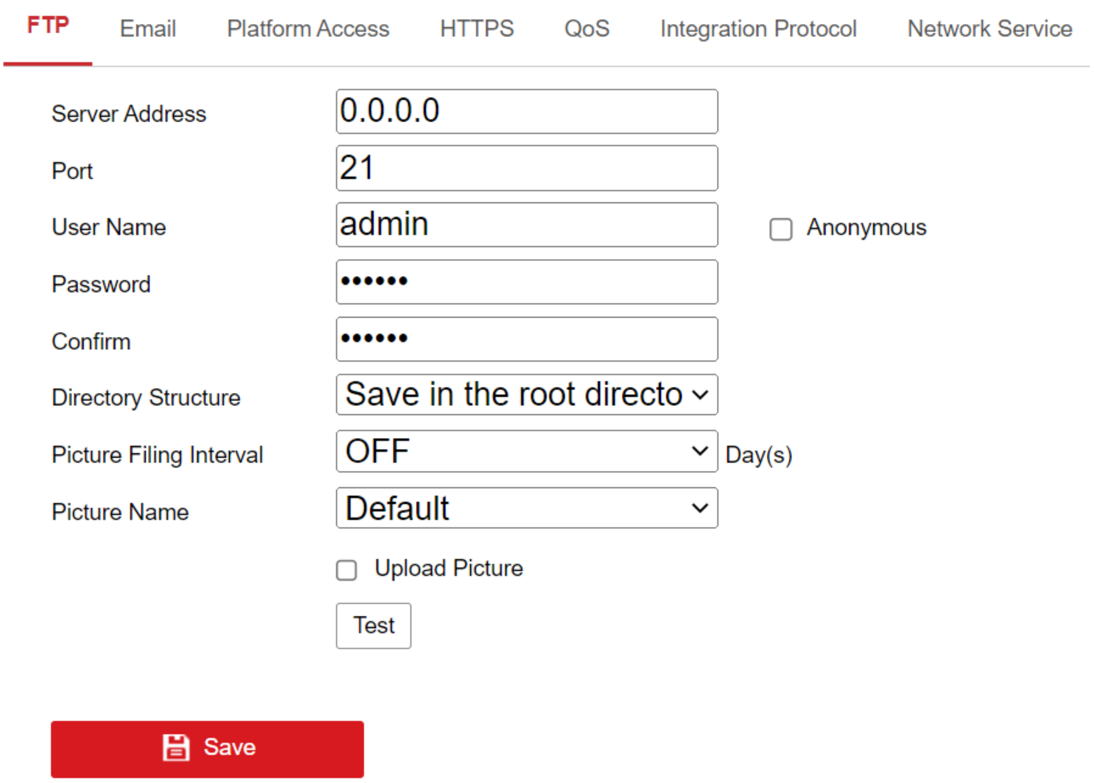
You can configure the parameters, including SNMP, FTP, Email, HTTPS, QoS, 802.1x, etc., by following the instructions in this section.

5.2.1 FTP

Purpose:

You can configure the FTP server related information to enable the uploading of the captured pictures to the FTP server. The captured pictures can be triggered by events or a timing snapshot task.

Step 1 Go to **Configuration** > **Network** > **Advanced Settings** > **FTP**.



Server Address 0.0.0.0

Port 21

User Name admin □ Anonymous

Password ••••••

Confirm ••••••

Directory Structure Save in the root directo

Picture Filing Interval OFF Day(s)

Picture Name Default

□ Upload Picture

Figure 5-5 FTP Settings

Step 2 Input the FTP address and port.

Step 3 Configure the FTP settings; and the user name and password are required for the FTP server login.

Caution

STRONG PASSWORD RECOMMENDED

- We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Step 4 Set the directory structure and picture filing interval.

- **Directory**: In the **Directory Structure** field, you can select the root directory, parent directory and child directory. When the parent directory is selected, you have the option to use the Device Name, Device Number or Device IP for the name of the directory; and when the Child Directory is selected, you can use the Camera Name or Camera No. as the name of the directory.

- **Picture Filing Interval:** For better picture management, you can set the picture filing interval from 1 day to 30 days. Pictures captured in the same time interval will be saved in one folder named after the beginning date and ending date of the time interval.
- **Picture Name:** Set the naming rule for captured picture files. You can choose **Default** in the drop-down list to use the default rule, that is, *IP address channel number capture time event type.jpg* (e.g., *10.11.37.189_01_20150917094425492_OBJCT_DETECTION.jpg*).

Or you can customize it by adding a **Custom Prefix** to the default naming rule.

Step 5 Check the Upload Picture checkbox to enable the function.

- **Upload Picture:** To enable uploading the captured picture to the FTP server.
- **Anonymous Access to the FTP Server (in which case the user name and password won't be required**.**):** Check the **Anonymous** checkbox to enable the anonymous access to the FTP server.

Note

The anonymous access function must be supported by the FTP server**.**

Step 6 Click **Save** to save the settings.

5.2.2 Email

Purpose:

The system can be configured to send an Email notification to all designated receivers if an alarm event is detected, e.g., motion detection event, video loss, video tampering, etc.

Before you start:

Step 1 Please configure the DNS Server settings under **Configuration** > **Network** > **Basic Settings** > **TCP/IP** before using the Email function.

Step 2 Go to **Configuration** > **Network** > **Basic Settings** > **TCP/IP** to set the IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway and the Preferred DNS Server.

Note

Please refer to Section 7.1.1 **Configure TCP/IP Settings** for detailed information.

Step 3 Go to **Configuration** > **Network** >**Advanced Settings** > **Email**.

Step 4 Configure the following settings:

- **Sender:** The name of the email sender.
- **Sender's Address:** The email address of the sender.

- **SMTP Server:** IP address or host name (e.g., smtp.263xmail.com) of the SMTP Server.
- **SMTP Port:** The SMTP port. The default TCP/IP port for SMTP is 25 (not secured). And the SSL SMTP port is 465.
- **Email Encryption:** None and SSL are selectable. When you select SSL and disable STARTTLS, e-mails will be sent after encrypted by SSL. The SMTP port should be set as 465 for this encryption method. When you select SSL and enable STARTTLS, emails will be sent after encrypted by STARTTLS, and the SMTP port should be set as 25.

Note

If you want to use STARTTLS, make sure that the protocol is supported by your e-mail server. If you check the Enable STARTTLS checkbox when the protocol is not supported by your e-mail sever, your e-mail will not be encrypted.

- **Attached Image:** Check the checkbox of Attached Image if you want to send emails with attached alarm images.
- **Interval:** The interval refers to the time between two actions of sending attached pictures.
- **Authentication** (optional): If your email server requires authentication, check this checkbox to use authentication to log in to this server and input the login user name and password.

Caution

STRONG PASSWORD RECOMMENDED

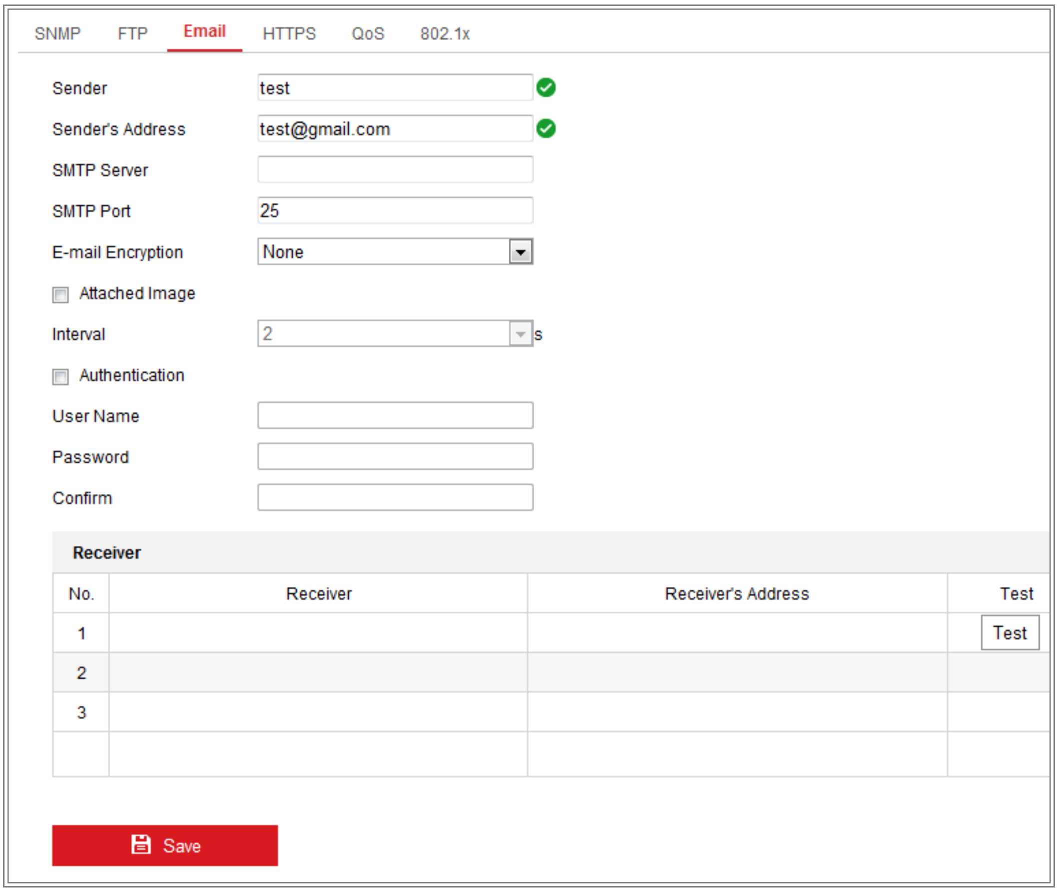
- We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Step 5 Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Step 6 The **Receiver** table**:** Select the receiver to which the email is sent. Up to 3 receivers can be configured.

Step 7 **Receiver:** The name of the user to be notified.

Step 8 **Receiver's Address**: The email address of user to be notified.



Sender	test ✓
Sender's Address	test@gmail.com ✓
SMTP Server	
SMTP Port	25
E-mail Encryption	None
□ Attached Image	
Interval	2 s
□ Authentication	
User Name	
Password	
Confirm	

Receiver

No.	Receiver	Receiver's Address	Test
1			Test
2			
3			

Figure 5-6 Email Settings

Step 9 Click **Save** to save the settings.

5.2.3 Platform Access

Purpose:

Platform access provides you an option to manage the devices via platform.

Step 1 Go to **Configuration > Network > Advanced Settings > Platform Access.**

Step 2 Check the checkbox of Enable to enable the platform access function of the device.

Step 3 Currently the Platform Access Mode supports only ISUP 5.0.

Step 4 You can use the default server address.

Step 5 Click **Save** to save the settings.

5.2.4 HTTPS

Purpose:

HTTPS provides authentication of the web site and its associated web server, which protects against Man-in-the-middle attacks.

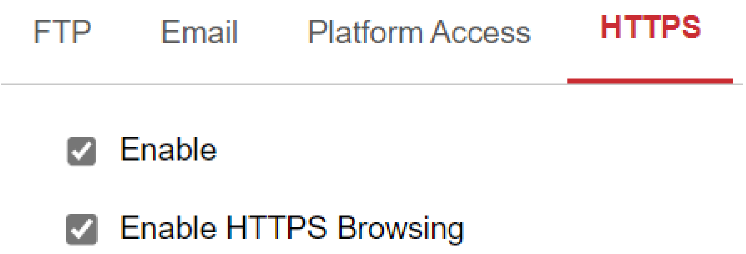
Note

- If HTTPS is enabled by default, the camera creates an unsigned certificate automatically. When you visit the camera via HTTPS, the web browser will send a notification about the certificate issue. Install a signed-certificate to the camera to cancel the notification.

Step 1 G to **Configuration > Network > Advanced Settings > HTTPS**.

Step 2 Check Enable to access the camera via HTTP or HTTPS protocol.

Step 3 Check Enable HTTPS Browsing to access the camera only via HTTPS protocol.

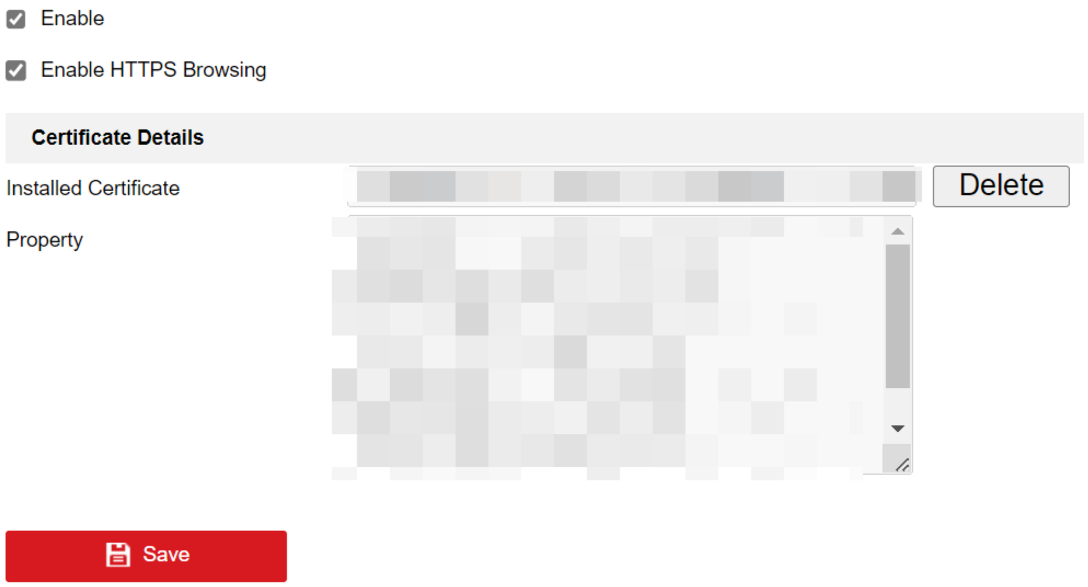


☑ Enable

☑ Enable HTTPS Browsing

Figure 5-7 HTTPS Configuration Interface

There will be the certificate information after your successfully creating and installing the certificate.



☑ Enable

☑ Enable HTTPS Browsing

Figure 5-8 Installed Certificate

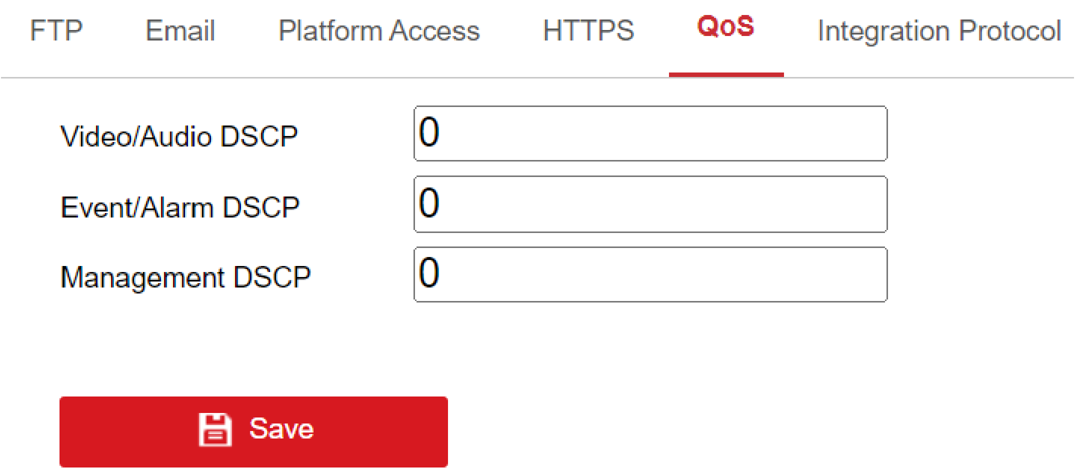
Step 4 Click **Save** to save the settings.

5.2.5 QoS

Purpose:

QoS (Quality of Service) can help solve the network delay and network congestion by configuring the priority of data sending.

Step 1 Enter the QoS Settings interface: **Configuration** > **Network** > **Advanced Settings** > **QoS**.



Video/Audio DSCP: 0

Event/Alarm DSCP: 0

Management DSCP: 0

Figure 5-9 QoS Settings

Step 2 Configure the QoS settings, including Video/Audio DSCP, Event/Alarm DSCP and Management DSCP.

The valid value range of the DSCP is 0 to 63. The bigger the DSCP value is, the higher the priority is.

Note

DSCP refers to the Differentiated Service Code Point; and the DSCP value is used in the IP header to indicate the priority of the data**.**

Step 3 Click **Save** to save the settings.

Note

A reboot is required for the settings to take effect.

5.2.6 Integration Protocol

Purpose:

If you need to access to the camera through the third party platform, you can enable CGI function. And if you need to access to the device through ONVIF protocol, you can configure ONVIF user in this interface. Refer to ONVIF standard for detailed configuration rules.

ONVIF

Step 1 Check the Enable ONVIF checkbox to enable the function.

Step 2 Add ONVIF users. Up to 32 users are allowed.

Step 3 Set the user name and password, and confirm the password. You can set the user as media user, operator, and administrator.

Note

ONVIF user account is different from the camera user account. You have set ONVIF user account independently.

Step 4 Click **Save** to save the settings.

Note

User settings of ONVIF are cleared when you restore the camera.

5.2.7 Network Service

You can control the ON/OFF status of certain protocol that the camera supports.

Note

- Keep unused function OFF for security concern.
- Supported functions vary according to camera models.

- WebSocket

WebSocket protocol should be enabled if you use Google Chrome 45 and its above version or Mozilla Firefox 52 and its above version to visit your camera. Otherwise, live view, image capture, and digital zoom function can not be used.

  - If the camera uses HTTP, enable **WebSocket**.

- SDK Service and Enhanced SDK Service

If you want to add the device to the client software, you should enable SDK Service or Enhanced SDK Service.

  - **SDK Service:** SDK protocol is used.
  - **Enhanced SDK Service:** SDK over TLS protocol is used. Communication between the device and the client software is secured by using TLS (Transport Layer Security) protocol.

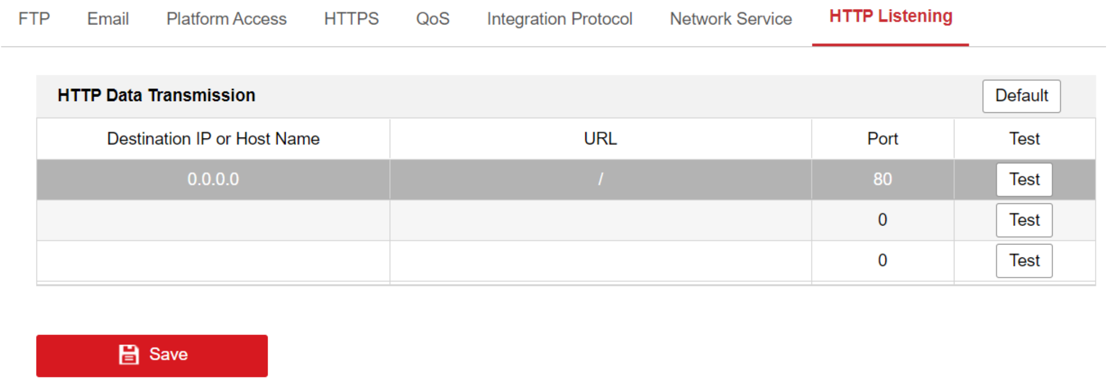
- TLS (Transport Layer Security)

The device offers TLS 1.1 and TLS 1.2. Enable one or more protocol versions according to your need.

5.2.8 HTTPS Listening

Purpose:

The HTTPS Listening supports uploading the alarm information to a target IP or domain, one that supports http protocal transmission.



HTTP Data Transmission

Destination IP or Host Name	URL	Port	Test
0.0.0.0	/	80	Test
		0	Test
		0	Test

Figure 5-10 HTTPS Listening

Step 1 Click Destination IP or Host Name, URL and Port to enter the target service (Up to 3 services can be set).

Step 2 Click **Test** to test the target service.

Step 3 Click **Default** to reset the entered data.

Step 4 Click **Save** to save the settings.

Chapter 6 Video Settings

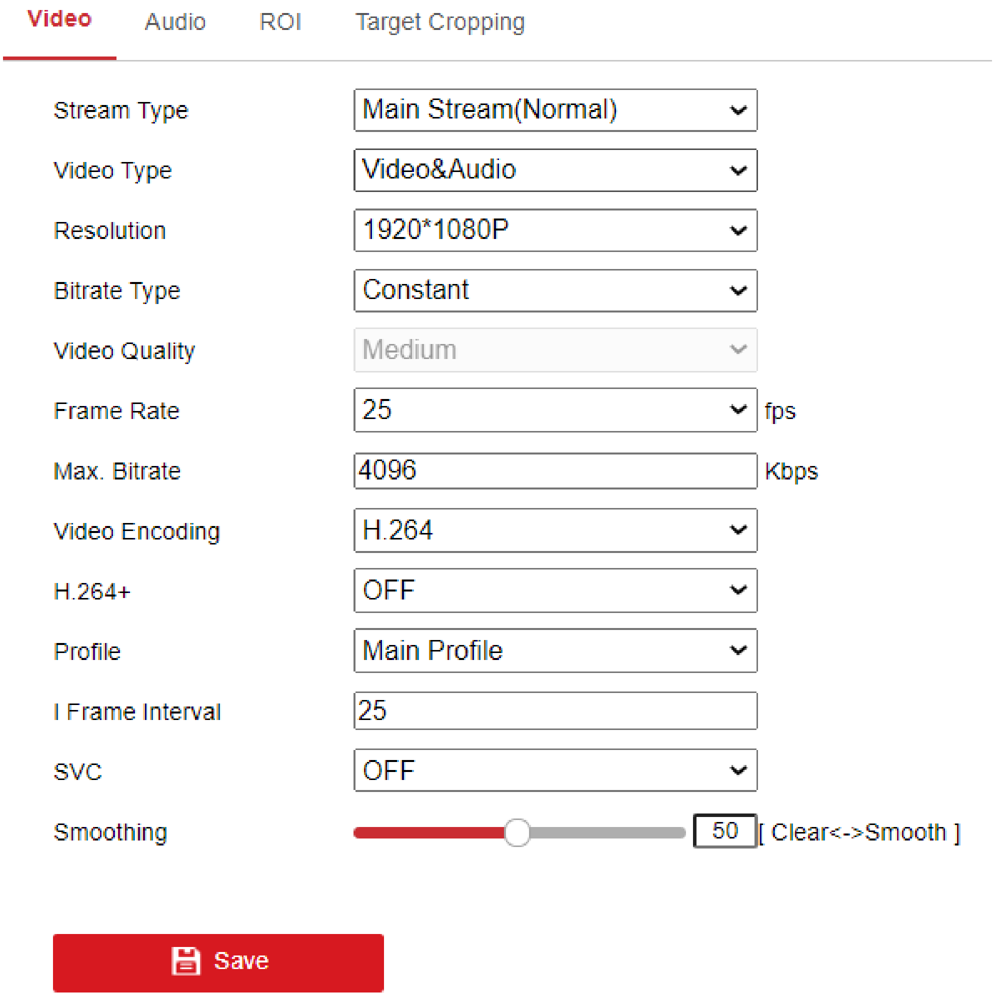
Purpose:

Follow the instructions below to configure the video setting, audio settings, ROI, Display info. on Stream, etc.

For certain camera models, you can configure parameters for available video streams, for example, the main stream, the sub-stream, etc. And you can also customize additional video streams for further needs.

- On **Video** page, set-up available video streams.
- On **Custom Video** page, add extra video streams

Step 1 Go to **Configuration** > **Video/Audio** > **Video**



Stream Type	Main Stream(Normal)
Video Type	Video&Audio
Resolution	1920*1080P
Bitrate Type	Constant
Video Quality	Medium
Frame Rate	25 fps
Max. Bitrate	4096 Kbps
Video Encoding	H.264
H.264+	OFF
Profile	Main Profile
I Frame Interval	25
SVC	OFF
Smoothing	50 [Clear<->Smooth]

Figure 6-1 Video Settings

Step 2 Select the Stream Type.

Supported stream types are listed in the drop-down list.

Note

- For some models, the **Third Stream** is not enabled by default. Go to **System** > **Maintenance** > **System Service**> **Software** to enable the function is required.
- The main stream is usually for recording and live view with good bandwidth, and the sub-stream can be used for live view when the bandwidth is limited.
- You can customize the following parameters for the selected stream type.

- Video Type:

Select the stream type to video stream, or video & audio composite stream. The audio signal will be recorded only when the **Video Type** is **Video & Audio**.

- Resolution:

Select the resolution of the video output.

- Bitrate Type:

Select the bitrate type to constant or variable.

- Video Quality:

When bitrate type is selected as Variable, 6 levels of video quality are selectable.

- Frame Rate:

Set the frame rate. The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

- Max. Bitrate:

Set the max. bitrate from 32 to 16384 Kbps. The higher value corresponds to the higher video quality, but the better bandwidth is required.

Note

The maximum limit of the max. bitrate value varies according to different camera platforms. For certain cameras, the maximum limit is 8192 Kbps or 12288 Kbps.

- Video Encoding:

The camera supports multiple video encodings types, such as H.264, H.265, and MJPEG. Supported encoding type for different stream types may differ. H.265 is a new encoding technology. Compared with H.264, it reduces the transmission bitrate under the same resolution, frame rate and image quality.

Note

Selectable video encoding types may vary according to different camera modes.

- H.264+ and H.265+:
  - H.264+: If you set the main stream as the stream type, and H.264 as the video encoding, you can see H.264+ available. H.264+ is an improved compression coding technology based on H.264. By enabling H.264+, users can estimate the HDD consumption by its maximum average bitrate. Compared to H.264, H.264+ reduces storage by up to 50% with the same maximum bitrate in most scenes.
  - H.265+: If you set the main stream as the stream type, and H.265 as the video encoding, you can see H.265+ available. H.265+ is an improved compression coding technology based on H.265. By enabling H.265+, users can estimate the HDD consumption by its maximum average bitrate. Compared to H.265, H.265+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

You need to reboot the camera if you want to turn on or turn off the H.264+/H.265+. If you switch from H.264+ to H.265+ directly, and vice versa, a reboot is not required by the system.

Note

- Upgrade your video player to the latest version if live view or playback does not work properly due to compatibility.
- With H.264+/H.265+ enabled, the parameters such as profile, I frame interval, video quality, and SVC are greyed out.
- With H.264+/H.265+ enabled, some functions are not supported. For those functions, corresponding interfaces will be hidden.
- H.264+/H.265+ can spontaneously adjust the bitrate distribution according the requirements of the actual scene in order to realize the set maximum average bitrate in the long term. The camera needs at least 24 hours to adapt to a fixed monitoring scene.

- Max. Average Bitrate:

When you set a maximum bitrate, its corresponding recommended maximum average bitrate will be shown in the Max. Average Bitrate box. You can also set the maximum average bitrate manually from 32 Kbps to the value of the set maximum bitrate.

- Profile:

When you select H.264 or H.265 as video encoding, you can set the profile. Selectable profiles vary according to camera models.

- I Frame Interval:

Set I Frame Interval from 1 to 400.

- SVC:

Scalable Video Coding is an extension of the H.264/AVC and H.265 standard. Select OFF/ON to disable/enable the SVC function. Select Auto and the device will automatically extract frames from the original video when the network bandwidth is insufficient.

- Smoothing:

It refers to the smoothness of the stream. The higher value of the smoothing is, the better fluency of the stream will be, though, the video quality may not be so satisfactory. The lower value of the smoothing is, the higher quality of the stream will be, though it may appear not fluent.

Step 3 Click **Save** to save the settings.

Note

The video parameters vary according to different camera models. Refer to the actual display page for camera functions.

Chapter 7 Image Settings

Purpose:

Follow the instructions in this chapter to configure the image parameters, including display settings and OSD settings.

7.1 Display Settings Parameters

Purpose:

- Configure the image adjustment, exposure settings, day/night switch, backlight settings, white balance, image enhancement, video adjustment, and other parameters in display settings.

Note

The display parameters vary according to the different camera models. Please refer to the actual interface for details.

7.1.1 Mounting Scenario

Dynamic Scene and Fixed Scene are available.

Choose Dynamic Scene if the vehicle is moving and monitoring the other vehicles, for instance, the police car.

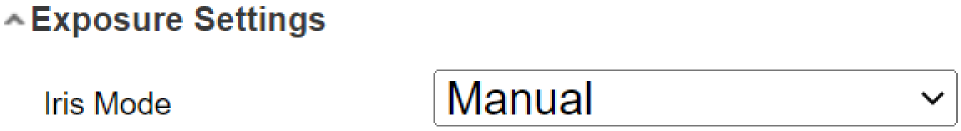
Choose Fixed Scene if the vehicle stays at a fixed position. For instance, when students are boarding the school bus, the camera can be used to look for cars that do not stop.

7.1.2 Image Adjustment

- **Brightness** describes how bright the image is, which ranges from 1 to 100.
- **Contrast** describes the contrast of the image, which ranges from 1 to 100.
- **Saturation** describes how colorful of the image is, which ranges from 1 to 100.
- **Sharpness** describes the edge contrast of the image, which ranges from 1 to 100.

7.1.3 Exposure Settings

Only **Manual** is selectable, and the iris mode is not configurable.



Exposure Settings

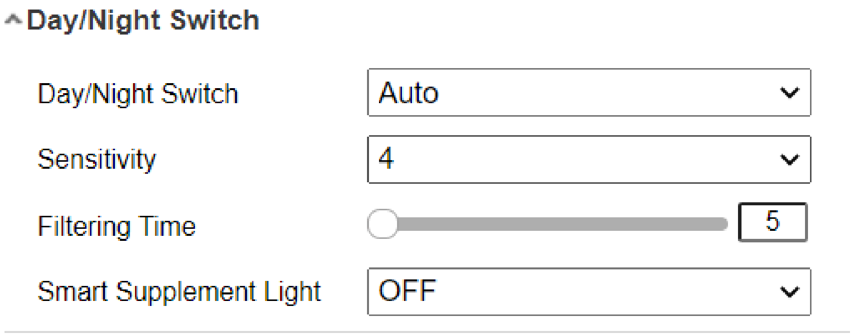
Iris Mode: Manual

Figure 7-1 Exposure Settings

7.1.4 Day/Night Switch

Select the Day/Night Switch mode according to different monitoring demand.

Day, Night, Auto, Scheduled-Switch, and Triggered by alarm input are selectable for day/night switch.



Day/Night Switch

Day/Night Switch: Auto

Sensitivity: 4

Filtering Time: 5

Smart Supplement Light: OFF

Figure 7-2 Day/Night Switch

- **Day:** the camera stays at day mode.
- **Night:** the camera stays at night mode.
- **Auto:** the camera switches between the day mode and the night mode according to the illumination automatically. The sensitivity ranges from 0 to 7, the higher the value is, the easier the mode switches. The **Filtering Time** refers to the interval time between the day/night switch. You can set it from 5s to 120s.
- **Scheduled-Switch:** Set the start time and the end time to define the duration for day/night mode.

Note

- The start time and end time refer to the valid time for day mode.
- The time period can start and end on two days in a row. For example, if you set start time as 10:00 and end time as 1:00, the day mode will be activated at 10 o'clock in the morning and stopped at 1 o'clock early in the next morning.

- **Triggered by alarm input:** The switch is triggered by alarm input. You can set the triggered mode to day or night.
- **Smart Supplement Light:** Set the supplement light as ON, and Auto and Manual are selectable for light mode.
- Select **Auto**, and the supplement light changes according to the actual luminance. E.g., if the current scene is bright enough, then the supplement light adjusts itself to lower power; and if the scene is not bright enough, the light adjusts itself to higher power.
- Select **Manual**, and you can adjust the supplement by adjusting the distance. E.g., if the object is near the camera, the device adjusts the supplement light to lower power, and the light is in higher power if the object is far away.

Note

- The start time and end time refer to the valid time for day mode.
- The time period can start and end on two days in a row. For example, if you set start time as 10:00 and end time as 1:00, the day mode will be activated at 10 o'clock in the morning and stopped at 1 o'clock early in the next morning.

7.1.5 Backlight Settings

- **BLC Area**: If you focus on an object against strong backlight, the object will be too dark to be seen clearly. BLC compensates light to the object in the front to make it clear. OFF, Up, Down, Left, Right, Center, Auto, and Custom are selectable.

Note

If BLC mode is set as Custom, you can draw a red rectangle on the live view image as the BLC area.

- **WDR**: Wide Dynamic Range can be used when there is a high contrast of the bright area and the dark area of the scene.
- **HLC:** High Light Compression function can be used when there are strong lights in the scene affecting the image quality.

7.1.6 White Balance

White balance is the white rendition function of the camera used to adjust the color temperature according to the environment.

- Manual white balance supports adjustable r and b gains.
- "Lock White Balance" locks the current color correction matrix. If the actual scene is a fixed light type, the last four options can be selected according to the actual situation.
- "Fluorescent lamp" is suitable for around 6500K color temperature environment.
- "Incandescent lamp" is suitable for around 3000K color temperature environment.
- "Warm-light lamp" is suitable for color temperature around 4000K.
- "Natural light" is suitable for the color temperature environment around 5500K.

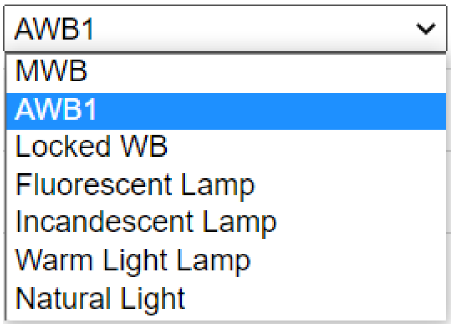


Figure 7-3 White Balance

7.1.7 Image Enhancement

- **Digital Noise Reduction**: DNR reduces the noise in the video stream. OFF, Normal and Expert are selectable. Set the DNR level from 0 to 100 in Normal Mode. Set the DNR level from both space DNR level [0-100] and time DNR level [0-100] in Expert Mode.
- **Grey Scale**: You can choose the range of the grey scale as [0-255] or [16-235].

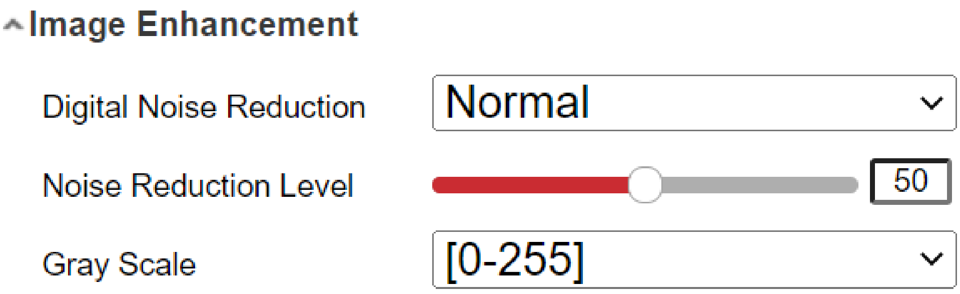


Image Enhancement

Digital Noise Reduction: Normal

Noise Reduction Level: 50

Gray Scale: [0-255]

Figure 7-4 Image Enhancement

7.1.8 Video Adjustment

- **Mirror**: It mirrors the image so you can see it inversed. Left/Right, Up/Down, Center, and OFF are selectable.
- **Rotate**: To make a complete use of the 16:9 aspect ratio, you can enable the rotate function when you use the camera in a narrow view scene.
- When installing, turn the camera to the 90 degrees or rotate the 3-axis lens to 90 degrees, and set the rotate mode as on, you will get a normal view of the scene with 9:16 aspect ratio to ignore the needless information such as the wall, and get more meaningful information of the scene.
- **Scene Mode**: Choose the scene as indoor or outdoor according to the real environment.
- **Video Standard**: 50 Hz and 60 Hz are selectable. Choose according to the different video standards; normally 50 Hz for PAL standard and 60 Hz for NTSC standard.
- **Lens Distortion Correction**: For cameras equipped with motor-driven lens, image may appear distorted to some extent. Turn on this function to correct the distortion.

7.2 OSD Settings

Purpose:

You can customize the camera name, time/date format, display mode, and OSD size displayed on the live view.

Step 1 Go to **Configuration** > **Image** > **OSD Settings**.

Step 2 Check the corresponding checkbox to select the display of camera name, date or week if required.

Step 3 Edit the camera name in the text field of **Camera Name**.

Step 4 Select from the drop-down list to set the time format and date format.

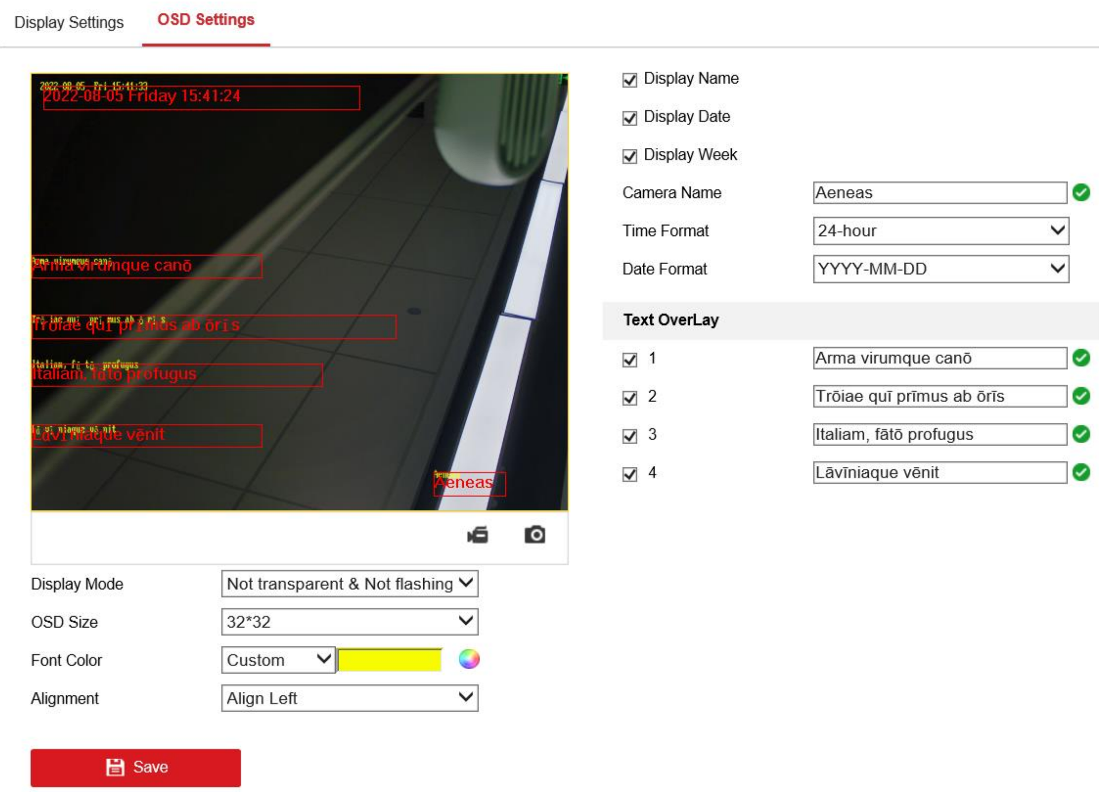
Step 5 Select from the drop-down list to set the time format, date format, display mode, OSD size and OSD color.

Step 6 Configure the text overlay settings.

1) Check the checkbox in front of the textbox to enable the on-screen display.
2) Input the characters in the textbox.

Note

Up to 4 text overlays are configurable.



☑ Display Name

☑ Display Date

☑ Display Week

Camera Name	Aeneas
Time Format	24-hour
Date Format	YYYY-MM-DD

Text OverLay

☑ 1	Arma virumque canō
☑ 2	Trōiae quī prīmus ab ōrīs
☑ 3	Italiam, fātō profugus
☑ 4	Lāvīniaque vēnit

Display Mode	Not transparent & Not flashing
OSD Size	32*32
Font Color	Custom
Alignment	Align Left

Save

Figure 7-5 OSD Settings

Step 7 Adjust the position and alignment of text frames.

Left align, right align and custom are selectable. If you select custom, you can use the mouse to click and drag text frames in the live view window to adjust their positions.

Note

The alignment adjustment is only applicable to Text Overlay items.

Step 8 Click **Save** to save the settings and view the result on the **Live View**.

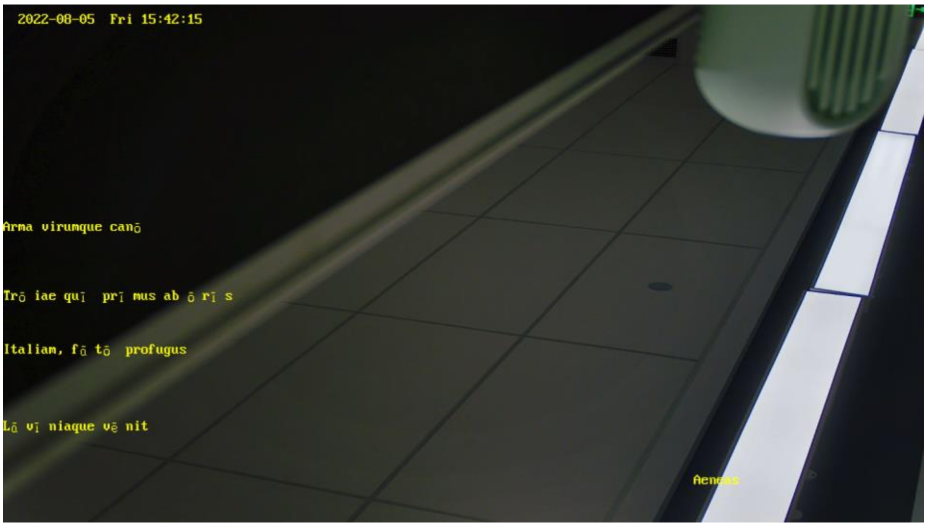


Figure 7-6 4 Lines of Text Overlay: Not Transparent&Not Flashing

Chapter 8 Basic Event Settings

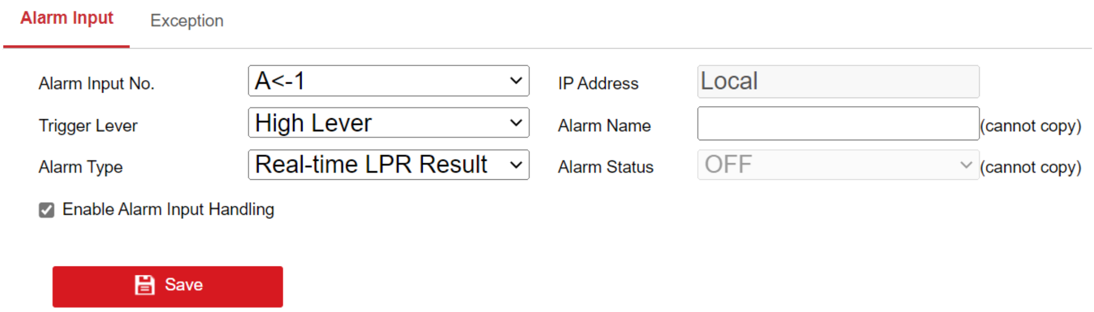
This section explains how to configure the network camera to respond to alarm events, including basic event and smart event.

8.1 Alarm Input

To recognize license plate, first set up the alarm input.

Step 1 Go to **Configuration** > **Event** > **Basic Event** >**Alarm Input**.

Step 2 Check **Enable Alarm Input Handling**.



Alarm Input | Exception

Alarm Input No.: A<-1

Trigger Lever: High Lever

Alarm Type: Real-time LPR Result

IP Address: Local

Alarm Name: (cannot copy)

Alarm Status: OFF (cannot copy)

☑ Enable Alarm Input Handling

Save

Figure 8-1 Configure Alarm Input

- Alarm Input No: The line for alarm input, currently supporting only one road.
- Trigger Lever: depends on the trigger level of the vehicle.
- Alarm Type: currently only support license plate recognition result.
- Alarm Name: choose a specific name for each type of alarm.
- IP Address and Alarm Status displays whether the IP address is local and whether the alarm is on.

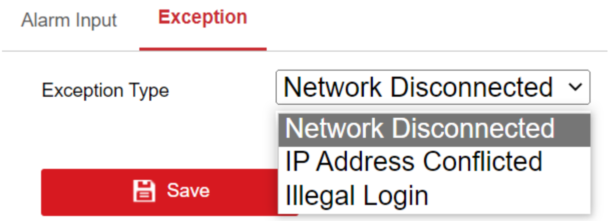
8.2 Exception

The network exception will trigger an alarm. Currently only support Network Disconnection, IP Conflict and Illegal Login.

Step 1 Go to **Configuration** > **Event** > **Basic Event** > **Exception**.

Step 2 Chose the exception type to set alarm for.

Step 3 Click **Save** to save the settings.



Alarm Input | Exception

Exception Type: Network Disconnected

Network Disconnected
IP Address Conflicted
Illegal Login

Save

Figure 8-2 Exceptions

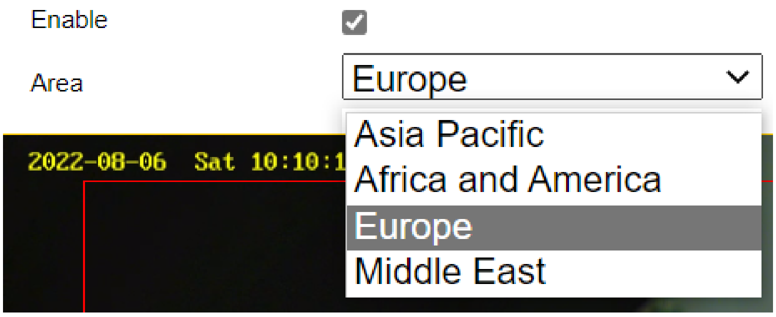
Chapter 9 Plate License Recognition

The Plate License Recognition function will capture and recognize the plate license number according to the region that the license belongs to.

Step 1 Go to **Configuration** > **Plate License Recognition**.

Step 2 Check **Enable** to enable the function.

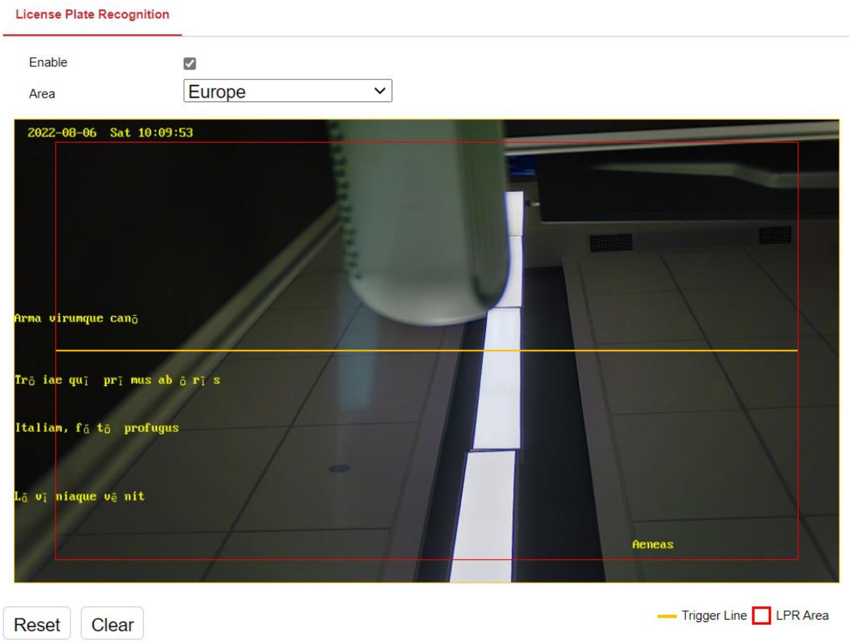
Step 3 Choose the area where the plate license belongs. Four areas are selectable: Asia Pacific, Africa and America, Europe and Middle East.



Enable ☑

Area Europe

Figure 9-1 Area of the Plate



License Plate Recognition

Enable ☑

Area Europe

Figure 9-2 License Recognition Area and Trigger Line

Step 4 Click “Save” to enable setting.

Chapter 10 Storage Settings

Before you start:

To configure record settings, make sure that you have the network storage device or local storage device configured.

10.1 Capture Schedule

Purpose:

You can configure the scheduled snapshot and event-triggered snapshot. The captured picture can be stored in the local storage or network storage.

Step 1 Go to **Configuration** > **Storage** > **Schedule Settings** > **Capture**.

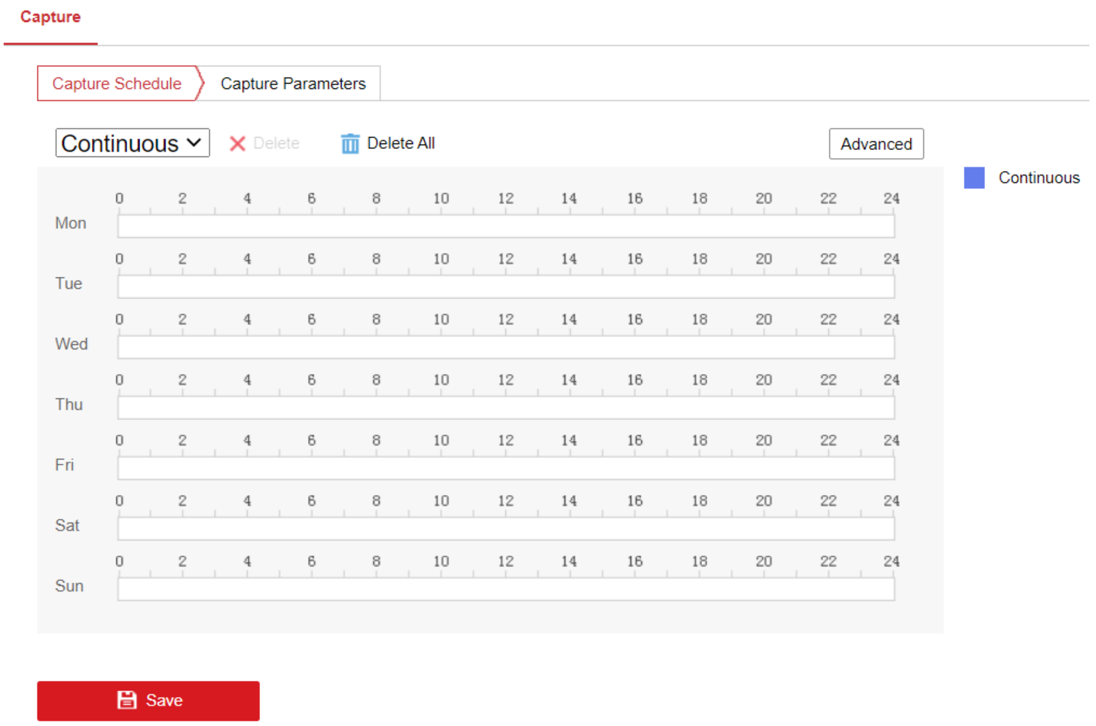


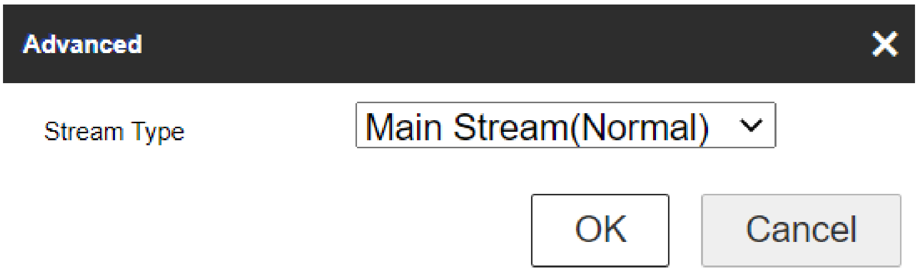
Figure 10-1 Capture Schedule Interface

Step 2 Select a **Record Type**. The record type supports only Continuous.

- Continuous

The video will be recorded automatically according to the time of the schedule.

Step 3 Click **Advanced** to set the stream type.



Stream Type: Main Stream(Normal)

Figure 10-2 Stream Type

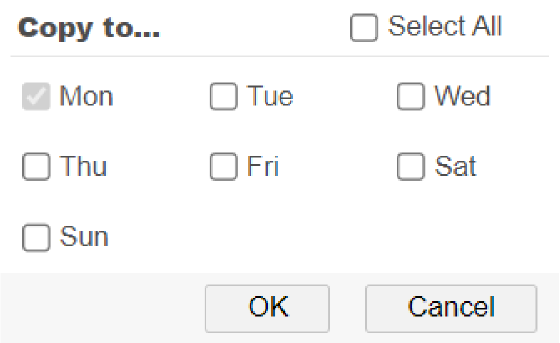
- Stream Type: Select the stream type for recording.

Note

The record parameter configurations vary depending on the camera model.

Step 4 Click-and-drag the mouse on the time bar to set the record schedule.

Step 5 (optional) To duplicate the setting of one day to another, click ⧉ that appears when the mouse hover over the time bar, and choose the date to apply the same setting. Check **Select All** if the setting is to be applied to all dates.



□ Select All

☑ Mon □ Tue □ Wed

□ Thu □ Fri □ Sat

□ Sun

Figure 10-3 Copy Setting to Another Date

Step 6 Delete the setting of one day by selecting that date and click **Delete**. You can also click **Delete All** to remove all settings.

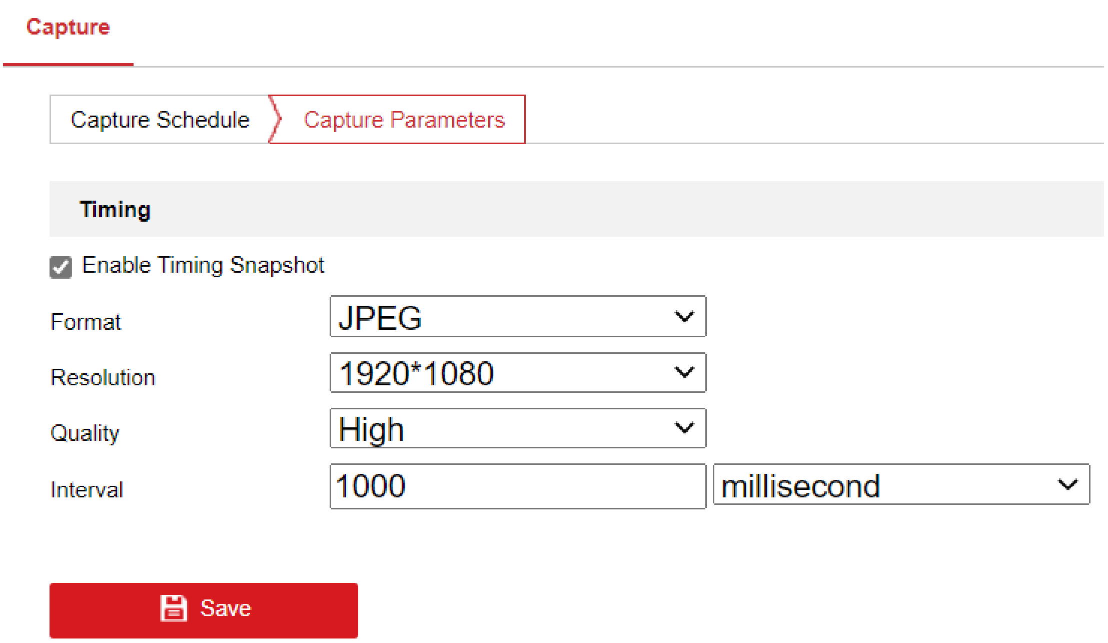
Step 7 Select the record type, and click-and-drag the mouse on the time bar to set the record schedule.

Step 8 Click **Save** to save the settings.

10.2 Capture Parameters

Step 1 Go to Capture Parameters tab to configure the capture parameters.

1) Check the **Enable Timing Snapshot** checkbox to enable continuous snapshot.
2) Select the picture format, resolution, quality and capture interval.



Capture

Capture Schedule | Capture Parameters

Timing

☑ Enable Timing Snapshot

Format: JPEG

Resolution: 1920*1080

Quality: High

Interval: 1000 millisecond

Figure 10-4 Set Capture Parameters

Step 2 Set the time interval between two snapshots.

Step 3 Click **Save** to save the settings.

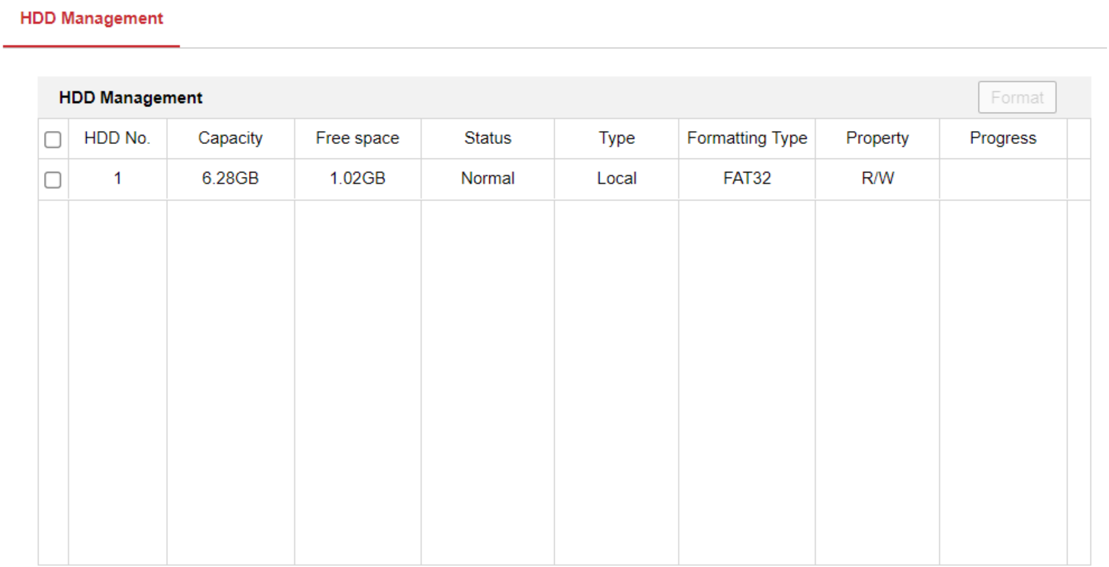
10.3 Storage Management

Before you start:

The network disk should be available within the network and properly configured to store the recorded files, log files, pictures, etc.

Steps:

Step 1 Go to **Configuration** > **Storage** > **Storage Management** > **HDD Management**, in which you can view the capacity, free space, status, type and property of the disk.



HDD Management

□	HDD No.	Capacity	Free space	Status	Type	Formatting Type	Property	Progress
□	1	6.28GB	1.02GB	Normal	Local	FAT32	R/W	

Figure 10-5 Storage Management Interface

Step 2 If the status of the disk is **Uninitialized**, check the corresponding checkbox to select the disk and click **Format** to start initializing the disk.

Step 3 When the initialization completed, the status of disk will become **Normal**.

10.4 Advanced Settings

Currently, the advanced settings only support the setting of whether to print logs.

Step 1 Go to **Configuration** > **Storage** > **Storage Management** > **HDD Management Advanced Settings** > **Other**.

Step 2 Check **Enable Print Log**.

Chapter 11 Access to the Network Camera

Purpose:

This section explains how to connect the network camera to the WAN with a static IP or a dynamic IP.

11.1.1 Via Static IP Connection

Before you start:

Please apply a static IP from an ISP (Internet Service Provider). With the static IP address, you can connect the network camera via a router or connect it to the WAN directly.

Connecting the network camera via a router

Step 1 Connect the network camera to the router.

Step 2 Assign a LAN IP address, the subnet mask and the gateway. Refer to Section 5.1.1 TCP/IP for detailed IP address configuration of the network camera.

Step 3 Save the static IP in the router.

Step 4 Set port mapping, e.g., 80, 8000, and 554 ports. The steps for port mapping vary according to the different routers. Please call the router manufacturer for assistance with port mapping.

Note

Refer to Appendix 2 for detailed information about port mapping.

Step 5 Visit the network camera through a web browser or the client software over the internet.

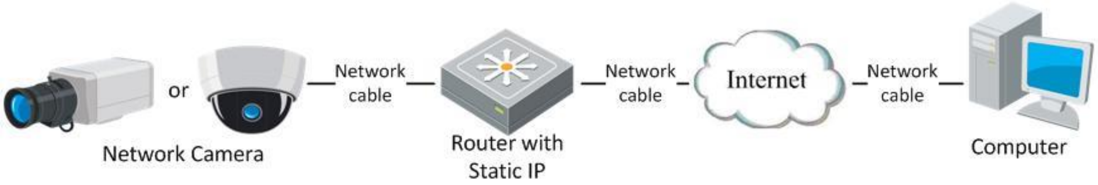


Figure 11-1 Accessing the Camera through Router with Static IP

Connecting the network camera with static IP directly

You can also save the static IP in the camera and directly connect it to the internet without using a router. Refer to Section 5.1.1 TCP/IP for detailed IP address configuration of the network camera.

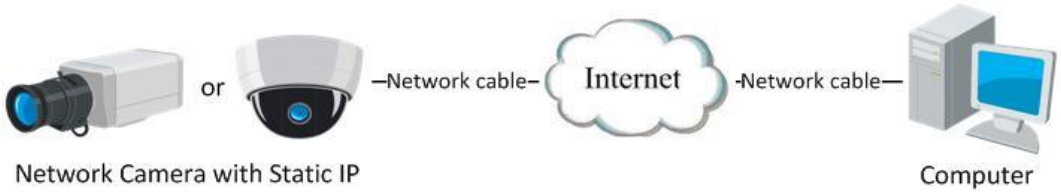


Figure 11-2 Accessing the Camera with Static IP Directly

11.1.2 Via Dynamic IP Connection

Before you start:

Please apply a dynamic IP from an ISP. With the dynamic IP address, you can connect the network camera to a modem or a router.

Connecting the network camera via a router

Step 1 Connect the network camera to the router.

Step 2 In the camera, assign a LAN IP address, the subnet mask and the gateway. Refer to Section 2.1.2 for detailed IP address configuration of the network camera.

Step 3 Set port mapping. E.g. 80, 8000, and 554 ports. The steps for port mapping vary depending on different routers. Please call the router manufacturer for assistance with port mapping.

Note

Refer to Appendix 2 for detailed information about port mapping.

Step 4 Apply a domain name from a domain name provider.

Step 5 Configure the DDNS settings in the setting interface of the router.

Step 6 Visit the camera via the applied domain name.

Step 7 Connecting the network camera via a modem

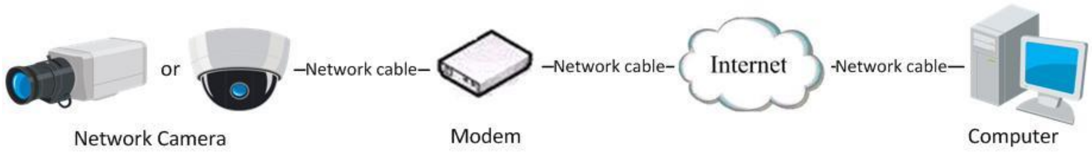


Figure 11-3 Accessing the Camera with Dynamic IP

Chapter 12 Appendix: SADP Software Introduction

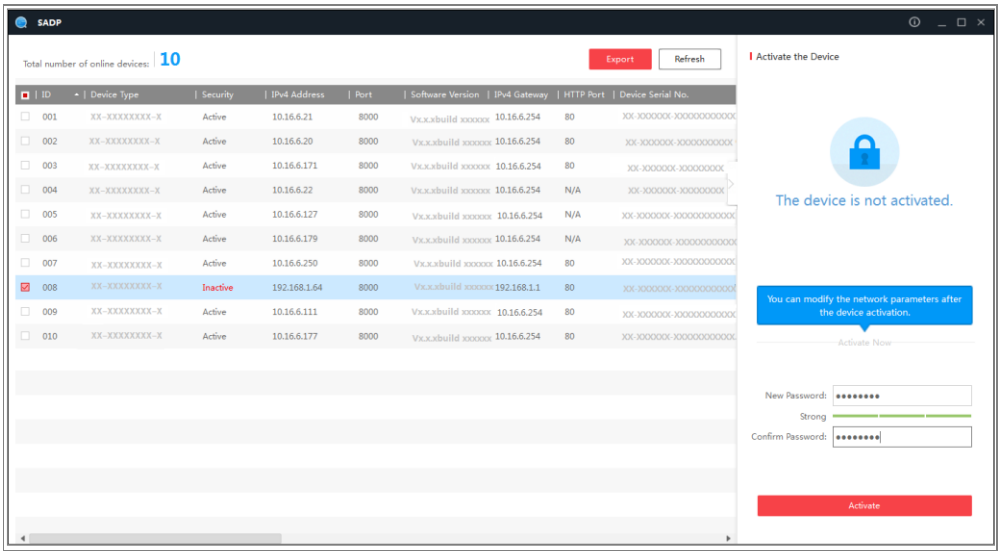
● Description of SADP

SADP (Search Active Devices Protocol) is a kind of user-friendly and installation-free online device search tool. It searches the active online devices within your subnet and displays the information of the devices. You can also modify the basic network information of the devices using this software.

● Search active devices online

Step 1 Search online devices automatically

Step 2 After launch the SADP software, it automatically searches the online devices every 15 seconds from the subnet where your computer locates. It displays the total number and information of the searched devices in the Online Devices interface. Device information including the device type, IP address and port number, etc. will be displayed.



Total number of online devices: 10

■	ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
□	001	XX-XXXXXXXX-X	Active	10.16.6.21	8000	Vx.x.xbuild xxxxxx	10.16.6.254	80	XX-XXXXXX-XXXXXXXXXXX
□	002	XX-XXXXXXXX-X	Active	10.16.6.20	8000	Vx.x.xbuild xxxxxx	10.16.6.254	80	XX-XXXXXX-XXXXXXXXXX
□	003	XX-XXXXXXXX-X	Active	10.16.6.171	8000	Vx.x.xbuild xxxxxx	10.16.6.254	80	XX-XXXXXX-XXXXXXXX
□	004	XX-XXXXXXXX-X	Active	10.16.6.22	8000	Vx.x.xbuild xxxxxx	10.16.6.254	N/A	XX-XXXXXX-XXXXXXXX
□	005	XX-XXXXXXXX-X	Active	10.16.6.127	8000	Vx.x.xbuild xxxxxx	10.16.6.254	N/A	XX-XXXXXX-XXXXXXXXXXX
□	006	XX-XXXXXXXX-X	Active	10.16.6.179	8000	Vx.x.xbuild xxxxxx	10.16.6.254	N/A	XX-XXXXXX-XXXXXXXXXXX
□	007	XX-XXXXXXXX-X	Active	10.16.6.250	8000	Vx.x.xbuild xxxxxx	10.16.6.254	80	XX-XXXXXX-XXXXXXXXXXX
☑	008	XX-XXXXXXXX-X	Inactive	192.168.1.64	8000	Vx.x.xbuild xxxxxx	192.168.1.1	80	XX-XXXXXX-XXXXXXXXXXX
□	009	XX-XXXXXXXX-X	Active	10.16.6.111	8000	Vx.x.xbuild xxxxxx	10.16.6.254	80	XX-XXXXXX-XXXXXXXXXXX
□	010	XX-XXXXXXXX-X	Active	10.16.6.177	8000	Vx.x.xbuild xxxxxx	10.16.6.254	80	XX-XXXXXX-XXXXXXXXXXX

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

New Password: ••••••••

Strong

Confirm Password: ••••••••

Figure A.1.1 Searching Online Devices

Note

Device can be searched and displayed in the list in 15 seconds after it went online; it will be removed from the list in 45 seconds after it went offline.

Step 3 Search online devices manually

Step 4 You can also click Refresh to refresh the online device list manually. The newly searched devices will be added to the list.

Step 5 NOTE You can click ▲ or ▼ on each column heading to order the information; you can click ▶ to expand the device table and hide the network parameter panel on the right side, or click ◀ to show the network parameter panel.

- ## Modify network parameters

Step 6 Select the device to be modified in the device list and the network parameters of the device will be displayed in the **Modify Network Parameters** panel on the right side.

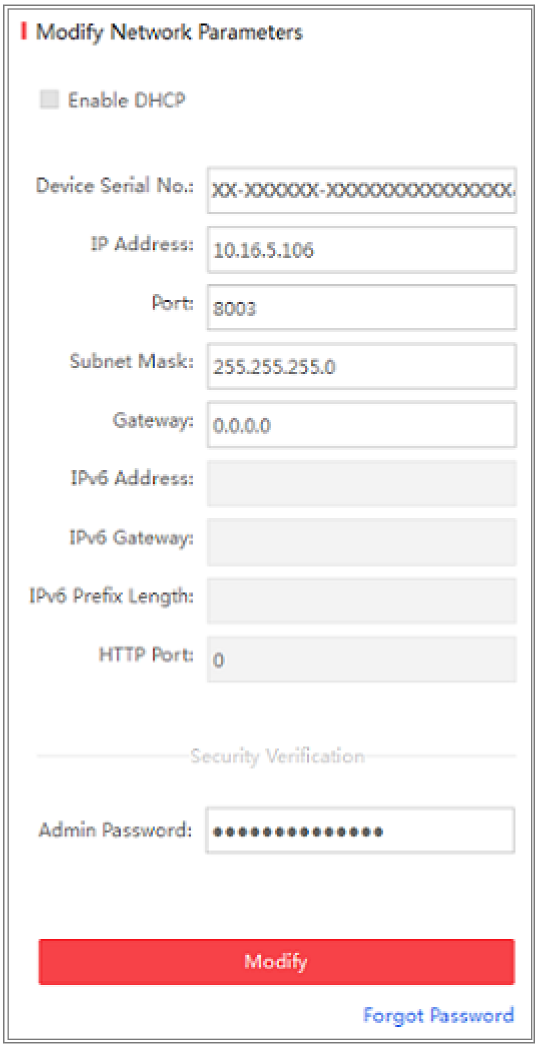
Step 7 Edit the modifiable network parameters, e.g. IP address and port number.

Step 8 Enter the password of the admin account of the device in the **Admin Password** field and click Modify to save the changes.

⚠ **Caution**

STRONG PASSWORD RECOMMENDED

- We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.



Modify Network Parameters

□ Enable DHCP

Device Serial No.: XX-XXXXXX-XXXXXXXXXXXXXXX

IP Address: 10.16.5.106

Port: 8003

Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

IPv6 Address:

IPv6 Gateway:

IPv6 Prefix Length:

HTTP Port: 0

Security Verification

Admin Password: ••••••••••••••

Figure A.1.2 Modify Network Parameters

See Far, Go Further