HIKVISION

Thermal & Optical Bi-spectrum Network Bullet / Turret Camera

User Manual

This Manual is the property of Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision"), and it cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise expressly stated herein, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual, any information contained herein.

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 (http://www.hikvision.com/en/).

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

Trademarks Acknowledgement

- 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.

LEGAL 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 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 INSPECTION, 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 LATER PREVAILS.

Regulatory Information

FCC Information

FCC compliance: This equipment has been tested and found to comply with the limits for 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 EMC Directive 2004/108/EC, 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.

Safety Instruction

These instructions are intended to ensure that the user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into 'Warnings' and 'Cautions':

Warnings: Serious injury or death may be caused if any of these warnings are neglected.

Cautions: Injury or equipment damage may be caused if any of these cautions are neglected.

⚡	⚠
Warnings Follow these safeguards to prevent serious injury or death.	**Cautions** Follow these precautions to prevent potential injury or material damage.

⚡**Warnings:**

- Please adopt the power adapter which can meet the safety extra low voltage (SELV) standard. And source with 12 VDC or 24 VAC (depending on models) according to the IEC60950-1 and Limited Power Source standard.
- To reduce the risk of fire or electrical shock, do not expose this product to rain or moisture.
- This installation should be made by a qualified service person and should conform to all the local codes.
- Please install blackouts equipment into the power supply circuit for convenient supply interruption.
- Please make sure that the ceiling can support more than 50(N) Newton gravities

if the camera is fixed to the ceiling.

- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the camera yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

⚠ **Cautions:**

- Make sure the power supply voltage is correct before using the camera.
- Do not drop the camera or subject it to physical shock.
- Do not touch sensor modules with fingers. If cleaning is necessary, use a clean cloth with a bit of ethanol and wipe it gently. If the camera will not be used for an extended period of time, put on the lens cap to protect the sensor from dirt.
- Do not aim the camera lens at the strong light such as sun or incandescent lamp. The strong light can cause fatal damage to the camera.
- The sensor may be burned out by a laser beam, so when any laser equipment is being used, make sure that the surface of the sensor not be exposed to the laser beam.
- Do not place the camera in extremely hot, cold temperatures (the operating temperature should be between -30°C to +60°C, or -40°C to +60°C if the camera model has an "H" in its suffix), dusty or damp environment, and do not expose it to high electromagnetic radiation.
- To avoid heat accumulation, ensure there is good ventilation to the device.
- Keep the camera away from water and any liquids.
- While shipping, pack the camera in its original, or equivalent, packing materials. Or packing the same texture.
- Improper use or replacement of the battery may result in hazard of explosion. Please use the manufacturer recommended battery type.

Notes:

For the camera supports IR, you are required to pay attention to the following precautions to prevent IR reflection:

- Dust or grease on the Turret cover will cause IR reflection. Please do not remove the Turret cover film until the installation is finished. If there is dust or grease on the Turret cover, clean the Turret cover with clean soft cloth and isopropyl alcohol.
- Make certain the installation location does not have reflective surfaces of objects too close to the camera. The IR light from the camera may reflect back into the lens causing reflection.
- The foam ring around the lens must be seated flush against the inner surface of the bubble to isolate the lens from the IR LEDS. Fasten the Turret cover to camera body so that the foam ring and the Turret cover are attached seamlessly.

Table of Contents

Chapter 1 System Requirement

Operating System: Microsoft Windows XP SP1 and above version

CPU: 2.0 GHz or higher

RAM: 1G or higher

Display: 1024×768 resolution or higher

Web Browser: Internet Explorer 8.0 and above version, Apple Safari 5.0.2 and above version, Mozilla Firefox 5.0 and above version and Google Chrome 18 and above version.

Chapter 2 Network Connection

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:

- If you want to set the network camera via a LAN (Local Area Network), please refer to *Section 2.1* ***Set the Network Camera over the LAN****.*
- If you want to set the network camera via a WAN (Wide Area Network), please refer to *Section 2.2* ***Set the Network Camera over the WAN****.*

2.1 Set 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:

- 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.

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

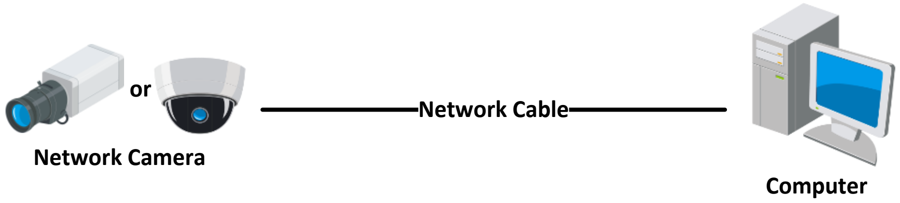


Figure 2-1 Connecting Directly

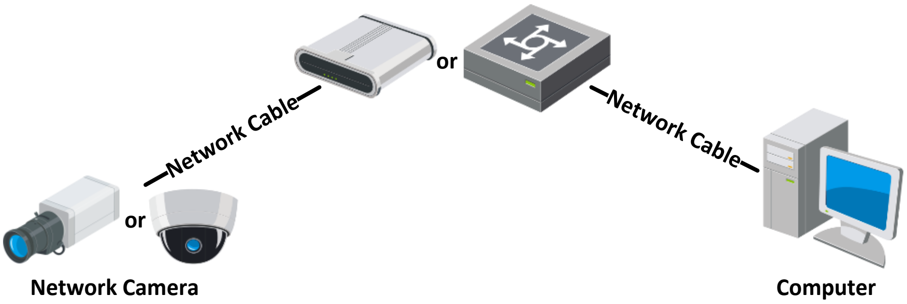


Figure 2-2 Connecting via a Switch or a Router

2.1.2 Activate 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.

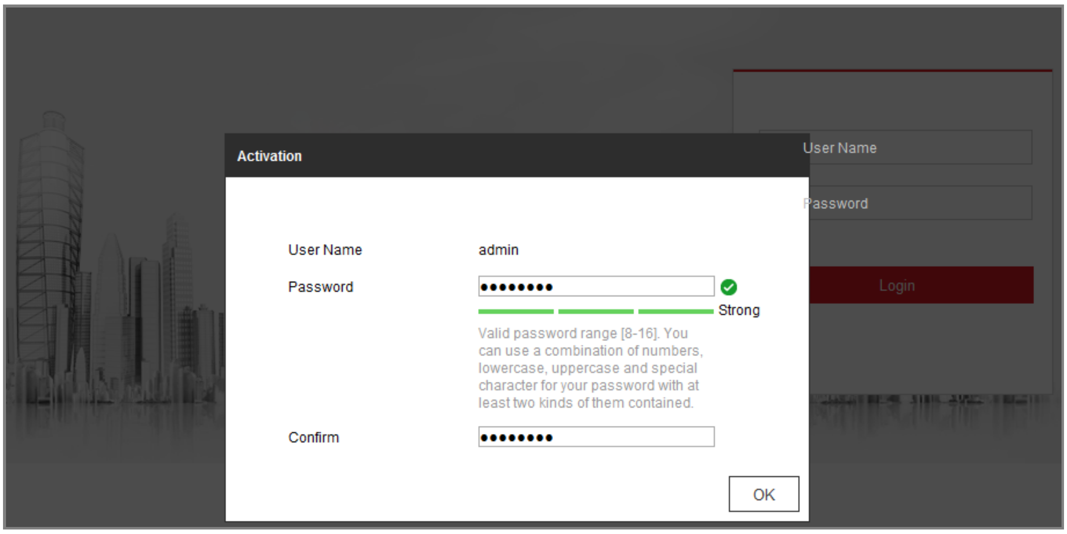
❖ Activation via Web Browser

Steps:

1. Power on the camera, and connect the camera to the network.
2. Input the IP address into the address bar of the web browser, and click **Enter**.

Notes:

- 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.



User Name: admin

Password: ••••••••

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 2-3 Activation via Web Browser

3. Create a password and input the password into the password field.

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.

4. Confirm the password.

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

❖ Activation via SADP Software

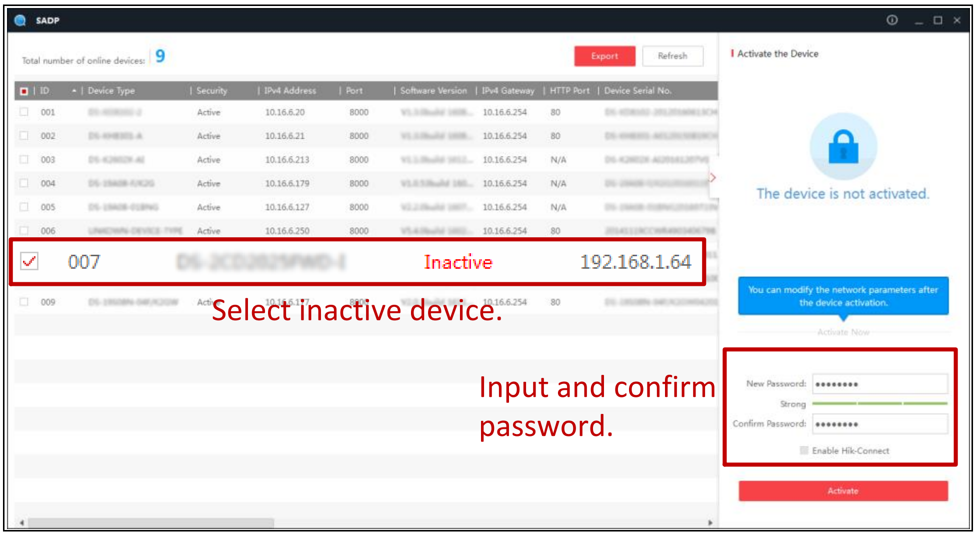
SADP software is used for detecting the online device, activating the camera, and resetting the password.

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

Steps:

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

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	[redacted]	Active	10.16.6.20	8000	[redacted]	10.16.6.254	80	[redacted]
□	002	[redacted]	Active	10.16.6.21	8000	[redacted]	10.16.6.254	80	[redacted]
□	003	[redacted]	Active	10.16.6.213	8000	[redacted]	10.16.6.254	N/A	[redacted]
□	004	[redacted]	Active	10.16.6.179	8000	[redacted]	10.16.6.254	N/A	[redacted]
□	005	[redacted]	Active	10.16.6.127	8000	[redacted]	10.16.6.254	N/A	[redacted]
□	006	[redacted]	Active	10.16.6.250	8000	[redacted]	10.16.6.254	80	[redacted]
☑	007	[redacted]	Inactive	192.168.1.64					
□	009	[redacted]	Acti	10.16.6.177	8000	[redacted]	10.16.6.254	80	[redacted]

Select inactive device.

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

New Password: ••••••••

Strong

Confirm Password: ••••••••

□ Enable Hik-Connect

Input and confirm password.

Figure 2-4 SADP Interface

Note:

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

3. Create a password and input the password in the password field, and confirm the password.

> **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.

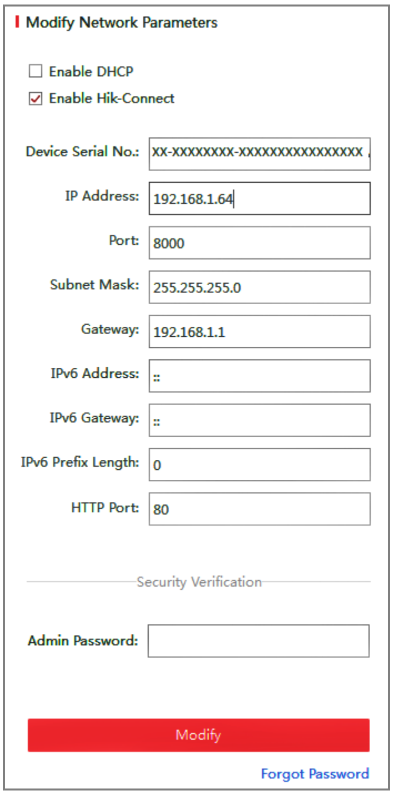
Note:

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

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.

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 2-5 Modify the IP Address

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

The batch IP address modification is supported by the SADP. Refer to the user manual of SADP for details.

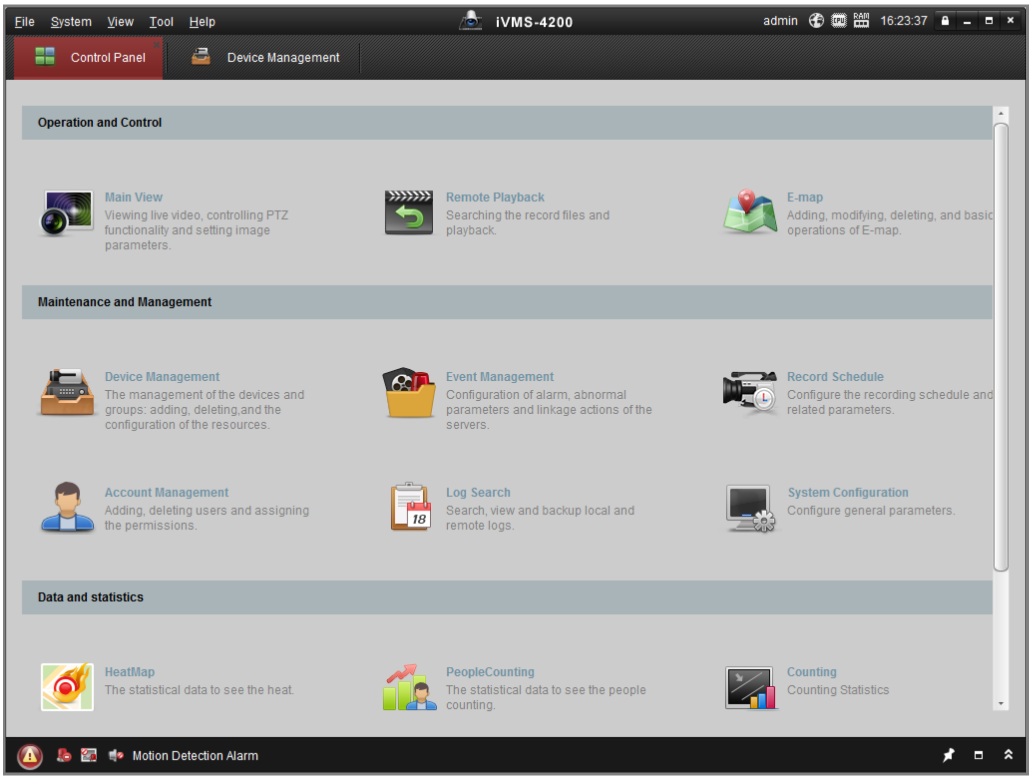
❖ Activation via Client Software

The client software is versatile video management software for multiple kinds of devices.

Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the camera**.**

Steps:

1. Run the client software and the control panel of the software pops up, as shown in the figure below.



Operation and Control

Main View
Viewing live video, controlling PTZ functionality and setting image parameters.

Remote Playback
Searching the record files and playback.

E-map
Adding, modifying, deleting, and basic operations of E-map.

Maintenance and Management

Device Management
The management of the devices and groups: adding, deleting,and the configuration of the resources.

Event Management
Configuration of alarm, abnormal parameters and linkage actions of the servers.

Record Schedule
Configure the recording schedule and related parameters.

Account Management
Adding, deleting users and assigning the permissions.

Log Search
Search, view and backup local and remote logs.

System Configuration
Configure general parameters.

Data and statistics

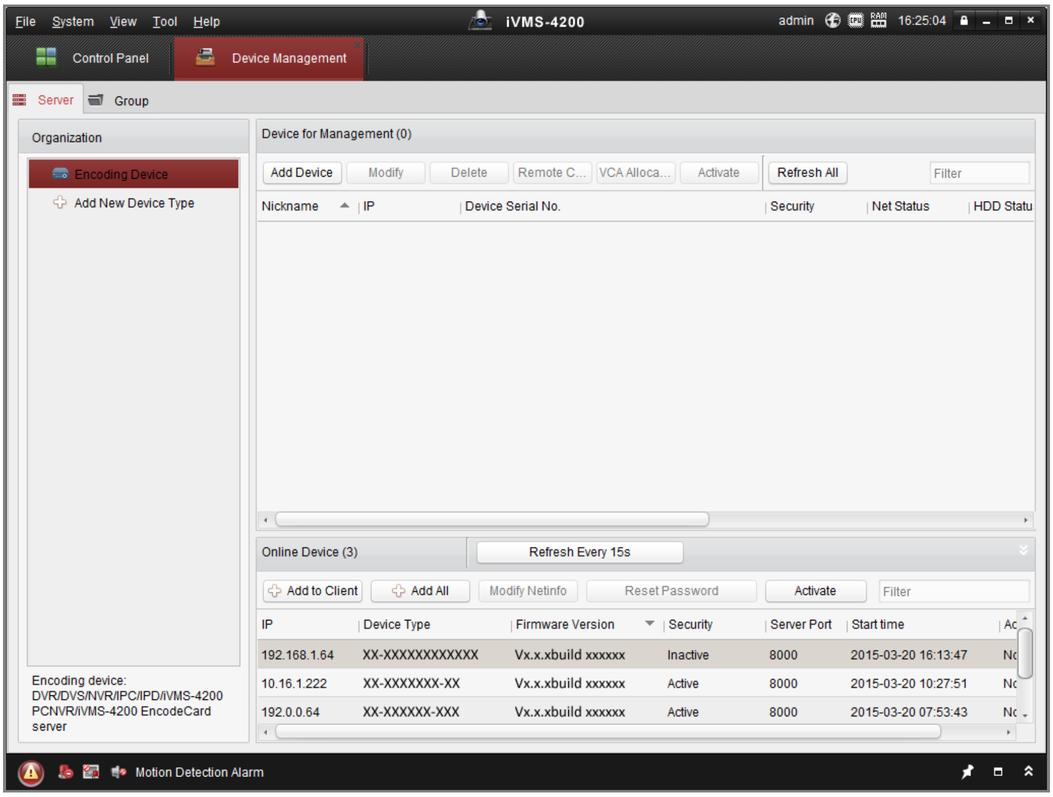
HeatMap
The statistical data to see the heat.

PeopleCounting
The statistical data to see the people counting.

Counting
Counting Statistics

Figure 2-6 Control Panel

2. Click **Device Management**.



Encoding device: DVR/DVS/NVR/IPC/IPD/iVMS-4200 PCNVR/iVMS-4200 EncodeCard server

IP	Device Type	Firmware Version	Security	Server Port	Start time	Ac
192.168.1.64	XX-XXXXXXXXXXXX	Vx.x.xbuild xxxxxx	Inactive	8000	2015-03-20 16:13:47	Nc
10.16.1.222	XX-XXXXXXX-XX	Vx.x.xbuild xxxxxx	Active	8000	2015-03-20 10:27:51	Nc
192.0.0.64	XX-XXXXXX-XXX	Vx.x.xbuild xxxxxx	Active	8000	2015-03-20 07:53:43	Nc

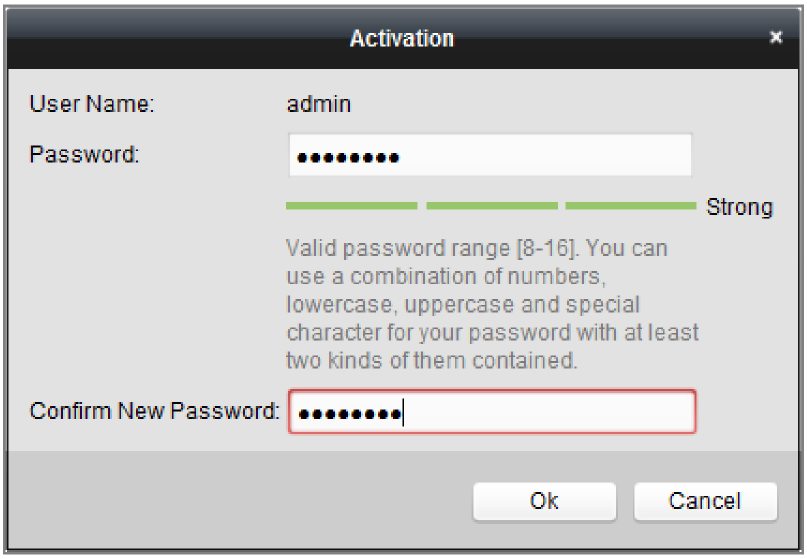
Figure 2-7 Device Management Interface

3. Check the device status from the device list, and select an inactive device.

4. Click the **Activate** button to pop up the Activation interface.

5. Create a password and input the password in the password field, and confirm the password.

⚠ **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. We recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.



Activation

User Name: admin

Password: ••••••••

Strong

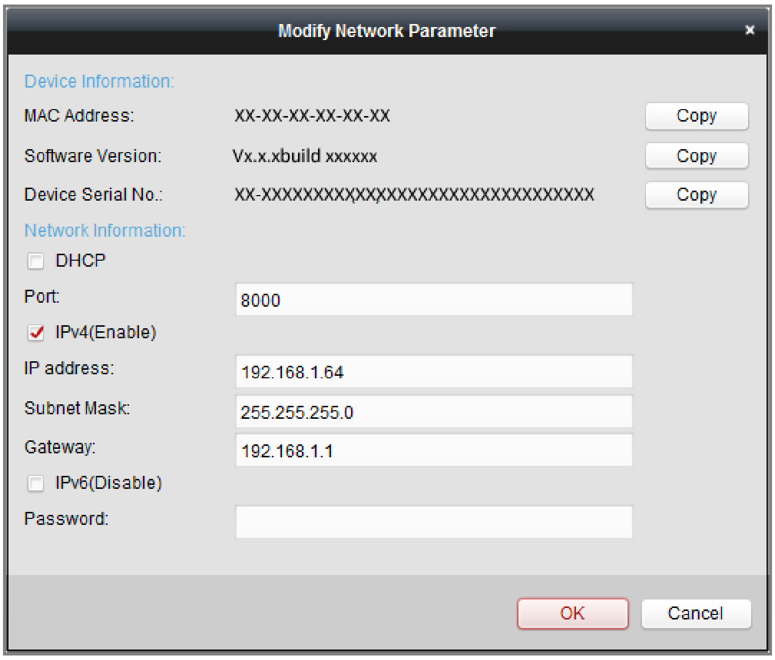
Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

Confirm New Password: ••••••••

Figure 2-8 Activation Interface (Client Software)

6. Click **OK**.

7. Click **Modify Netinfo** to pop up the Network Parameter Modification interface, as shown in the figure below.



Device Information:

MAC Address: XX-XX-XX-XX-XX-XX

Software Version: Vx.x.xbuild xxxxxx

Device Serial No.: XX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Network Information:

□ DHCP

Port: 8000

☑ IPv4(Enable)

IP address: 192.168.1.64

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

□ IPv6(Disable)

Password:

Figure 2-9 Modifying the Network Parameters

8. 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.

9. Input the password to activate your IP address modification.

2.2 Set the Network Camera over the WAN

Purpose:

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

2.2.1 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.

- **Connect the network camera via a router**

Steps:

1. Connect the network camera to the router.

2. 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.
3. Save the static IP in the router.
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.

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

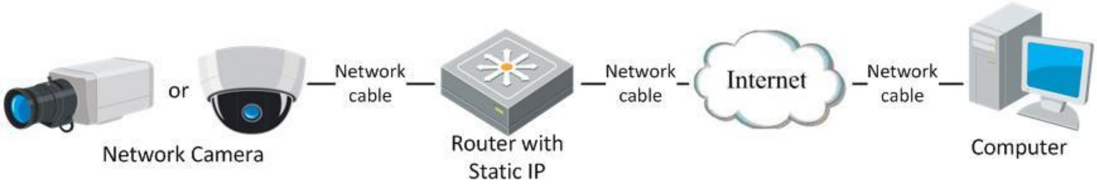


Figure 2-10 Accessing the Camera through Router with Static IP

- **Connect 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 2.1.2 for detailed IP address configuration of the network camera.

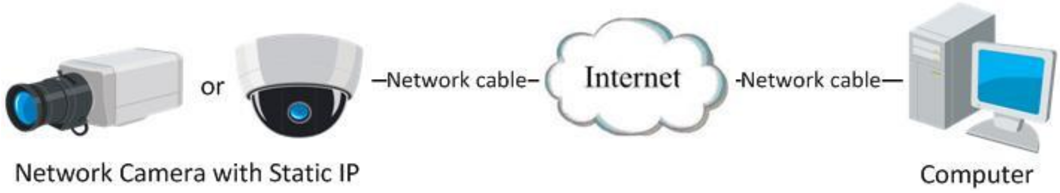


Figure 2-11 Accessing the Camera with Static IP Directly

2.2.2 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.

- **Connect the network camera via a router**

Steps:

1. Connect the network camera to the router.
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.
3. In the router, set the PPPoE user name, password and confirm the password.
4. 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.

5. Apply a domain name from a domain name provider.
6. Configure the DDNS settings in the setting interface of the router.
7. Visit the camera via the applied domain name.

- **Connect the network camera via a modem**

Purpose:

This camera supports the PPPoE auto dial-up function. The camera gets a public IP address by ADSL dial-up after the camera is connected to a modem. You need to configure the PPPoE parameters of the network camera. Refer to *Section 6.1.3* ***Configuring PPPoE Settings*** for detailed configuration.

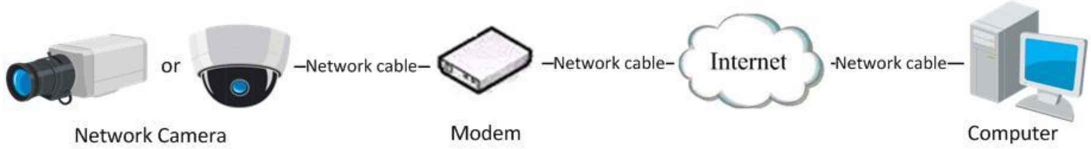


Figure 2-12 Accessing the Camera with Dynamic IP

Note: The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the camera. To solve the inconvenience of the dynamic IP, you need to get a domain name from the DDNS provider (E.g. DynDns.com). Please follow the steps below for normal domain name resolution and private domain name resolution to solve the problem.

- Normal Domain Name Resolution

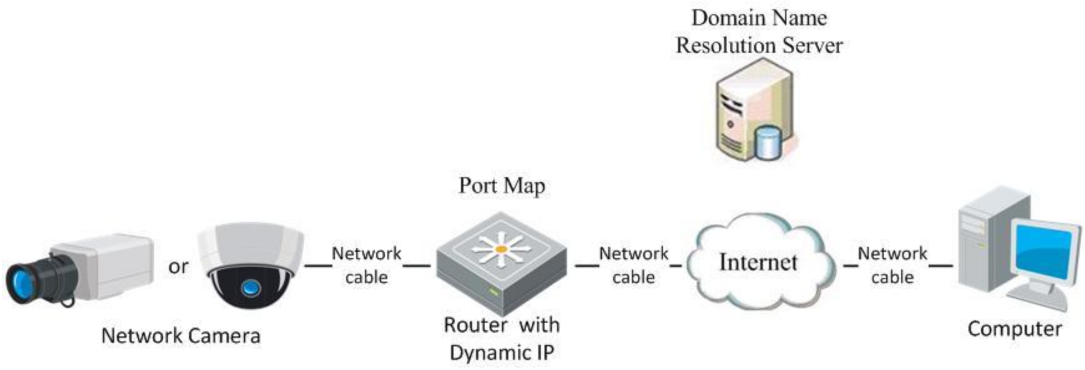


Figure 2-13 Normal Domain Name Resolution

Steps:

1. Apply a domain name from a domain name provider.
2. Configure the DDNS settings in the **DDNS Settings** interface of the network camera. Refer to *Section 6.1.2* ***Set DDNS*** for detailed configuration.
3. Visit the camera via the applied domain name.

♦ Private Domain Name Resolution

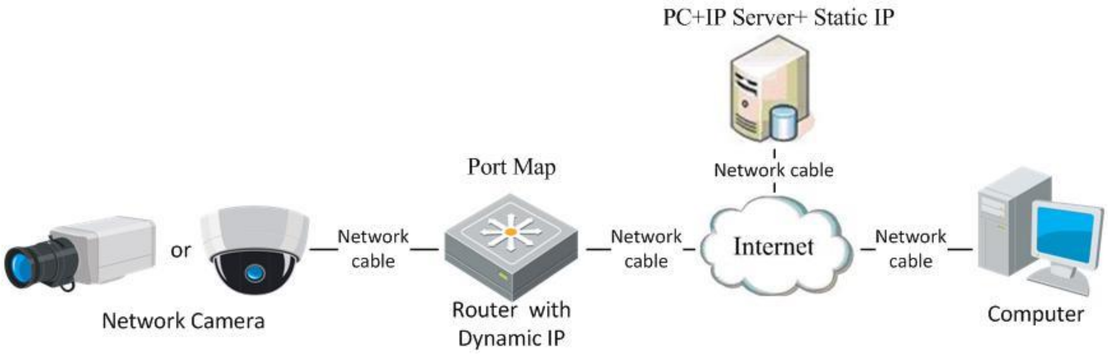


Figure 2-14 Private Domain Name Resolution

Steps:

1. Install and run the IP Server software in a computer with a static IP.
2. Access the network camera through the LAN with a web browser or the client software.
3. Enable DDNS and select IP Server as the protocol type. Refer to *Section 6.1.2* ***Set DDNS*** for detailed configuration.

Chapter 3 Access to the Network Camera

3.1 Accessing by Web Browsers

Steps:

1. Open the web browser.
2. In the browser address bar, input the IP address of the network camera, and press **Enter**.

   Note:

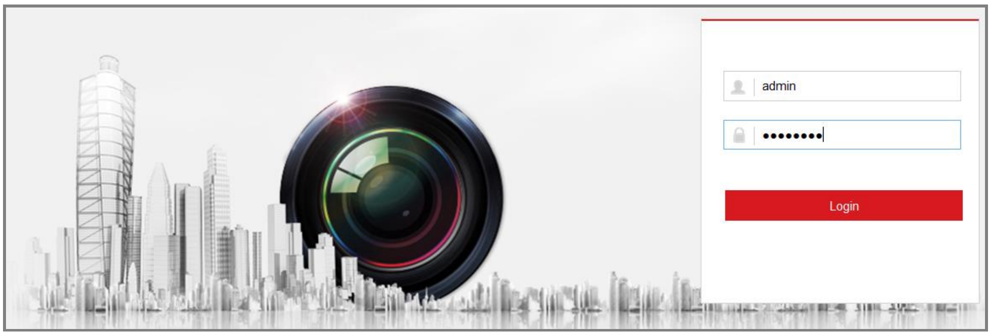
   The default IP address is 192.168.1.64. You are recommended to change the IP address to the same subnet with your computer.

3. Input the user name and password and click **Login**.

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).

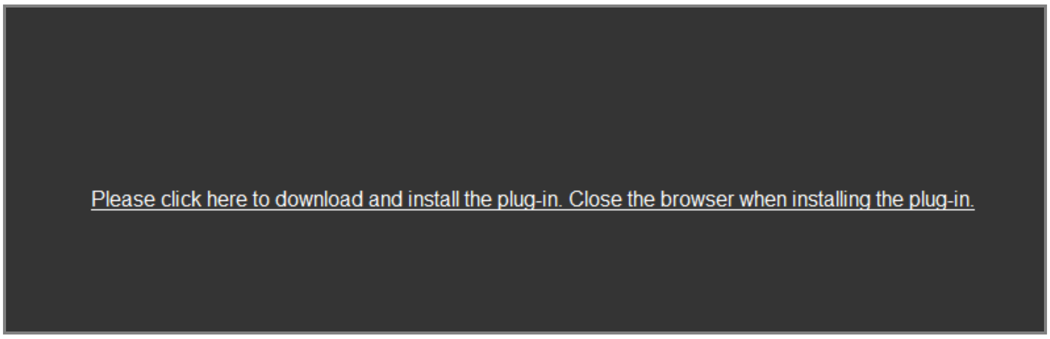


admin

••••••••

Figure 3-1 Login Interface

4. Click **Login**.
5. Install the plug-in before viewing the live video and operating the camera. Follow the installation prompts to install the plug-in.



Please click here to download and install the plug-in. Close the browser when installing the plug-in.

Figure 3-2 Download and Install Plug-in

Note: You may have to close the web browser to finish the installation of the plug-in.

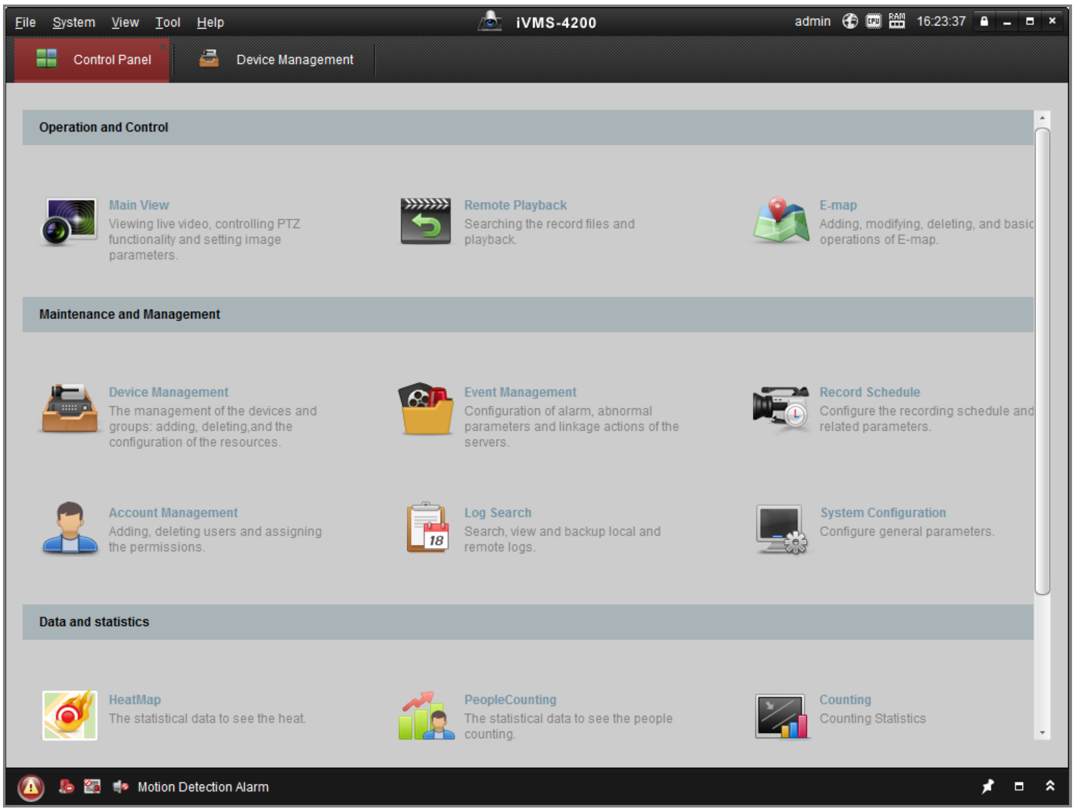
6. Reopen the web browser after the installation of the plug-in and repeat steps 2 to 4 to login.

Note: For detailed instructions of further configuration, please refer to the user manual of network camera.

3.2 Accessing by Client Software

The product CD contains the iVMS-4200 client software. You can view the live video and manage the camera with the software.

Follow the installation prompts to install the software. The control panel and live view interface of iVMS-4200 client software are shown as below.



Operation and Control

Main View
Viewing live video, controlling PTZ functionality and setting image parameters.

Remote Playback
Searching the record files and playback.

E-map
Adding, modifying, deleting, and basic operations of E-map.

Maintenance and Management

Device Management
The management of the devices and groups: adding, deleting,and the configuration of the resources.

Event Management
Configuration of alarm, abnormal parameters and linkage actions of the servers.

Record Schedule
Configure the recording schedule and related parameters.

Account Management
Adding, deleting users and assigning the permissions.

Log Search
Search, view and backup local and remote logs.

System Configuration
Configure general parameters.

Data and statistics

HeatMap
The statistical data to see the heat.

PeopleCounting
The statistical data to see the people counting.

Counting
Counting Statistics

Figure 3-3 iVMS-4200 Control Panel

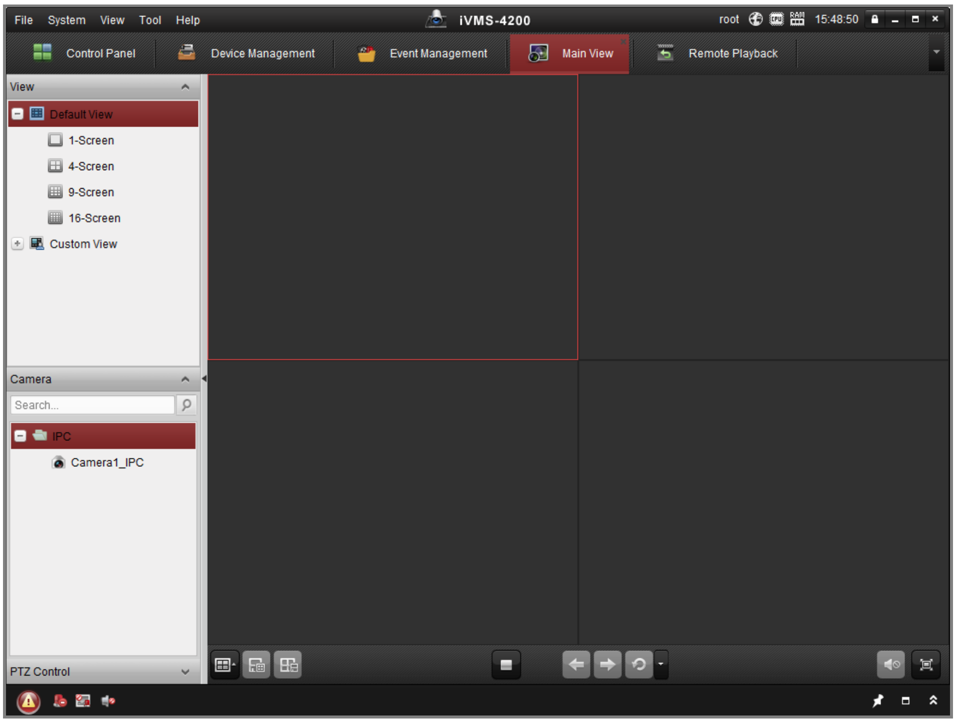


Figure 3-4 iVMS-4200 Main View

Chapter 4 Live View

4.1 Live View Page

Purpose:

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

Log in the network camera to go to 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:

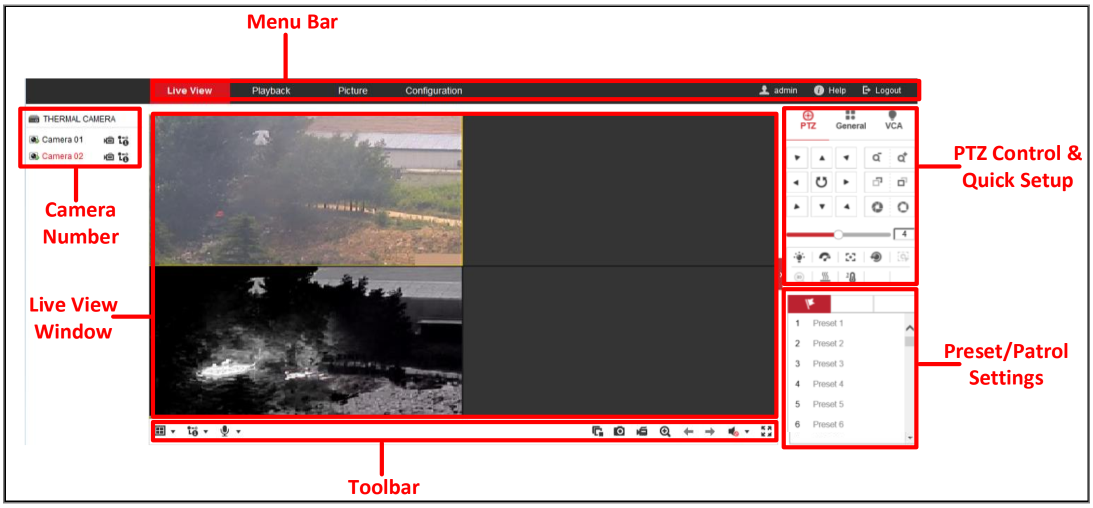


Figure 4-1 Live View Page

Menu Bar:

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

Camera Number:

For camera models which have more than one camera channels, you can control the display layout. Click a display screen, and double-click the desired camera channel to show its live view on the screen.

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.

PTZ Control:

Perform panning, tilting and zooming actions of the camera. Control the light and the wiper (only available for cameras supporting PTZ function).

Quick Setup

It allows quick setup of image, video, and VCA related parameters on live view.

Preset/Patrol Settings:

Set/call/delete the presets or patrols for PTZ cameras.

4.2 Start 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.

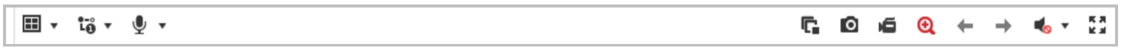


Figure 4-2 Live View Toolbar

Table 4-1 Descriptions of the Toolbar

Icon	Description
▶ / ■	Start/Stop live view.
▦	Display in 4×4 window.
▦	Display in 3×3 window.
⊞	Display in 2×2 window.
■	Display in 1×1 window.
1	Live view with the main stream.
2	Live view with the sub stream.
3	Live view with the third stream.
📷	Manually capture the picture.
🎥 / 🎥	Manually start/stop recording.
🔊 ▾ / 🔇	Audio on and adjust volume /Mute.

Icon	Description
🎙 / 🎙	Turn on/off microphone.
🔍 / 🔍	Start/stop digital zoom function.
← / →	View previous / next page.
⛶	Show full screen

Note: The icons vary according to the different camera models.

4.3 Record and Capture Pictures Manually

In the live view interface, click 📷 on the toolbar to capture the live pictures or 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 *Section 10.1*.

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

4.4 Operate PTZ Control

Note: Certain models do not support the PTZ control. This section only applies to the camera that supports PTZ control.

Purpose:

In the live view interface, you can use the PTZ control buttons to realize pan/tilt/zoom control of the camera.

Note: To realize PTZ control, the camera connected to the network must support the PTZ function or have a pan/tilt unit installed to the camera. Please properly set the PTZ parameters on RS485 settings page referring to *Section5.2.3.*

4.4.1 PTZ Control Panel

On the live view page, click › next to the right side of the live view window to show the PTZ control panel and click ‹ to hide it.

Click the direction buttons to control the pan/tilt movements.

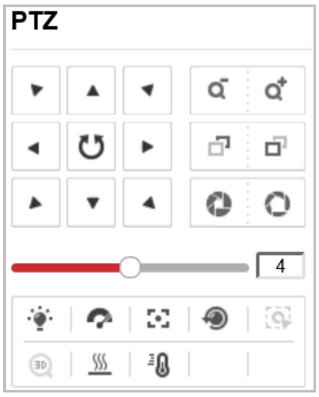


Figure 4-3 PTZ Control Panel

Click the zoom/focus/iris buttons to realize lens control.

***Notes*:**

- There are eight direction arrows (↑, ↓, ←, →, ↘, ↙, ↗, ↖) in the control panel. Click the arrows to realize adjustment in the relative positions.
- For the cameras which support lens movements only, the direction buttons are invalid.

Table 4-2 Descriptions of PTZ Control Panel

Icon	Description
	Zoom in/out
	Focus near/far
	Iris +/-
4	PTZ speed adjustment
	Light on/off
	Wiper on/off
	Auxiliary focus
	Initialize lens
	Start Manual Tracking
3D	Drag a rectangular to start 3D zoom.
	Enable De-icing Heater
	Enable manual thermometry
	Preset
	Patrol

- Light

  Click to enable/disable the light supplement of the speed Turret. This function is reserved.

- Wiper

  Click to move the wiper once.

- Auxiliary Focus

  The auxiliary focus function is reserved.

-

  Click and the lens operates the movements for initialization.

-

  Click to enable manual De-Icing function of the device.

  Note:

  The de-icing function takes effect when the device inner temperature is ≤ 30°C (86°F).

-

  Click to enable/disable the manual thermometry function of the device. You can click any position on the interface to show the real temperature.

- Manual Tracking

Before you start:

Go to **Configuration > System > Maintenance > VCA Resource Type** and select the VCA Resource as **Temperature Measurement + Behavior Analysis**.

Then Go to the VCA Information Configuration interface:

Configuration > VCA Configuration > VCA Info and enable Intelligent Analysis first.

Steps:

1. Click on the toolbar of live view interface.
2. Click a moving object in the live video.
   The speed Turret will track the object automatically.

- 3D Positioning

Steps:

1. Click on the toolbar of live view interface.
2. Operate the 3D positioning function:
3. Click a position of the live video. The corresponding position will be moved to the center of the live video.
4. Hold down the left mouse button and drag the mouse to the lower right on the live video. The corresponding position will be moved to the center of the live

video and zoomed in.

5. Hold down the left mouse button and drag the mouse to the upper left on the live video. The corresponding position will be moved to the center of the live video and zoomed out.

4.4.2 Set/Call a Preset

- **Set a Preset:**

1. In the PTZ control panel, select a preset number from the preset list.

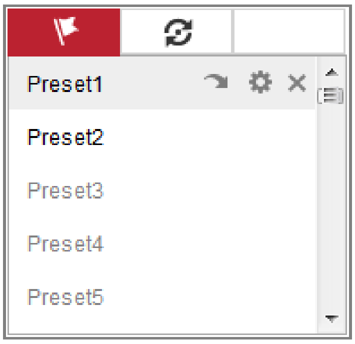


Figure 4-4 Set a Preset

2. Use the PTZ control buttons to move the lens to the desired position.
   - Pan the camera to the right or left.
   - Tilt the camera up or down.
   - Zoom in or out.
   - Refocus the lens.
3. Click ⚙ to finish the setting of the current preset.
4. You can click × to delete the preset, or double-click to edit the preset name.

- **Call a Preset:**

This feature enables the camera to point to a specified preset scene manually or when an event takes place.

For the defined preset, you can call it at any time to the desired preset scene.

In the PTZ control panel, select a defined preset from the list and click ↷ to call the preset.

Or you can place the mouse on the presets interface, and call the preset by typing the preset No. to call the corresponding presets.

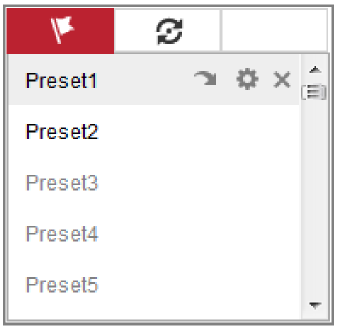


Figure 4-5 Calling a Preset

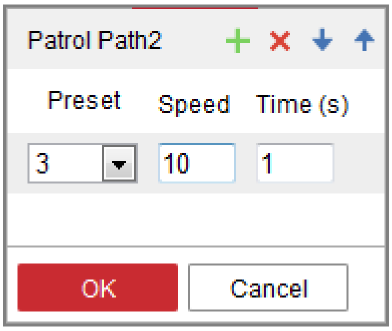
4.4.3 Set/Call a Patrol

Note:

No less than 2 presets have to be configured before you set a patrol.

Steps:

1. Click ⟳.
2. Select a path No., and click + to add the configured presets.
3. Select the preset, and input the patrol duration and patrol speed.
4. Click OK to save the first preset.
5. Follow the steps above to add the other presets.



Patrol Path2

Preset	Speed	Time (s)
3	10	1

Figure 4-6 Add Patrol Path

6. Click **OK** to save a patrol.
7. Click ▶ to start the patrol, and click ■ to stop it.
8. (Optional) Click ✕ to delete a patrol.

4.5 Live View Quick Setup

It allows quick setup of image/video related parameters on live view page.

Steps:

1. Click ‹ button on the right of the live view window to show the PTZ control panel. Click › to hide it.
2. Specify **Display**, **OSD** and **Video/Audio** and **VCA** resource parameters. For more settings, go to **Configuration** -> **Image**, **Configuration** -> **Video/Audio** and **Configuration** -> **VCA**.

- **Display Settings**

  Set the brightness, contrast, palettes, DNR, DDE, etc.

- **OSD (On Screen Display)**

  Set text information displayed on screen. Save the settings after configuration.

- **Video/Audio**

  Resolution and Max. Bit rate are adjustable. Click ❶ ❷ to change stream.

- **VCA Resource**

  Select VCA resource type as required.

  Note:

  - VCA Resource function varies according to different camera models.
  - VCA options are mutually exclusive.
  - The function may not be supported by some camera models.

Chapter 5 Network Camera Configuration

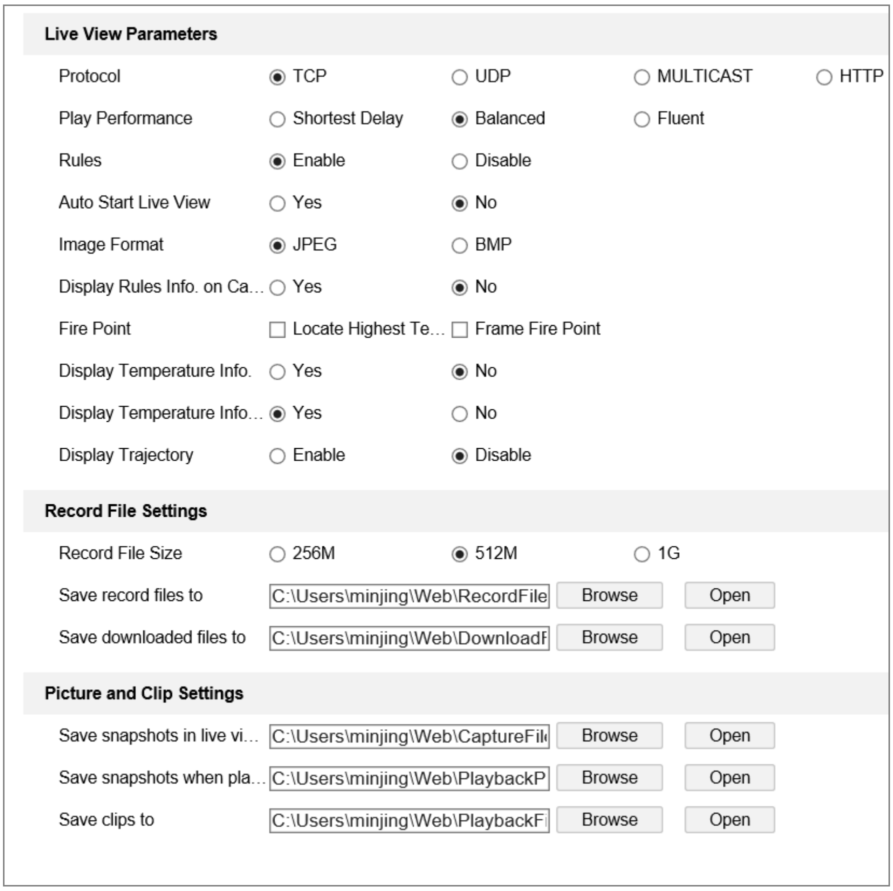
5.1 Set Local Parameters

Purpose:

The local configuration refers to the parameters of the live view, record files and captured pictures. The record files and captured pictures are the ones you record and capture using the web browser and thus the saving paths of them are on the PC running the browser.

Steps:

1. Go to the Local Configuration interface: **Configuration** > **Local**.



Live View Parameters

Protocol ● TCP ○ UDP ○ MULTICAST ○ HTTP
Play Performance ○ Shortest Delay ● Balanced ○ Fluent
Rules ● Enable ○ Disable
Auto Start Live View ○ Yes ● No
Image Format ● JPEG ○ BMP
Display Rules Info. on Ca… ○ Yes ● No
Fire Point □ Locate Highest Te… □ Frame Fire Point
Display Temperature Info. ○ Yes ● No
Display Temperature Info… ● Yes ○ No
Display Trajectory ○ Enable ● Disable

Record File Settings

Record File Size ○ 256M ● 512M ○ 1G
Save record files to C:\Users\minjing\Web\RecordFile Browse Open
Save downloaded files to C:\Users\minjing\Web\DownloadF Browse Open

Picture and Clip Settings

Save snapshots in live vi… C:\Users\minjing\Web\CaptureFil Browse Open
Save snapshots when pla… C:\Users\minjing\Web\PlaybackP Browse Open
Save clips to C:\Users\minjing\Web\PlaybackF Browse Open

Figure 5-1 Local Configuration Interface

2. Configure the following settings:

- **Live View Parameters:** Set the protocol type and live view performance.
  - ♦ **Protocol Type:** TCP, UDP, MULTICAST and HTTP are selectable.

    TCP: Ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected.

    UDP: Provides real-time audio and video streams.

    HTTP: Allows the same quality as of TCP without setting specific ports for streaming under some network environments.

    MULTICAST: It's recommended to select MCAST type when using the Multicast function. For detailed information about Multicast, refer to 6.1.1.
  - ♦ **Play Performance:** Set the play performance to Shortest Delay or Auto.
  - ♦ **Rules:** It refers to the rules on your local browser, select enable or disable to display or not display the colored marks when the motion detection, face detection, or intrusion detection is triggered. E.g., enabled as the rules are, and the face detection is enabled as well, when a face is detected, it will be marked with a green rectangle on the live view.
  - ♦ **Image Format:** Choose the image format for picture capture.
  - ♦ **Display Rules Info. on Capture:** Display rules information on the capture or not.
  - ♦ **Fire Point: Locate Highest Temperature Point**, and **Frame Fire Point** are selectable. Display the highest temperature area as point or frame.
  - ♦ **Display Temperature Info.:** Display temperature information or not with temperature measurement rule configured.
  - ♦ **Display Temperature Info. on Capture:** Display temperature information on the capture or not.
  - ♦ **Display Trajectory**: Show the target movement on the display by hikvision player.
  - ♦ **Record File Settings:** Set the saving path of the recorded video files. Valid for the record files you recorded with the web browser.
  - ♦ **Record File Size:** Select the packed size of the manually recorded and

downloaded video files to 256M, 512M or 1G. After the selection, the maximum record file size is the value you selected.

- ♦ **Save record files to:** Set the saving path for the manually recorded video files.
- ♦ **Save downloaded files to:** Set the saving path for the downloaded video files in playback mode.

- **Picture and Clip Settings:** Set the saving paths of the captured pictures and clipped video files. Valid for the pictures you capture with the web browser.
  - ♦ **Save snapshots in live view to:** Set the saving path of the manually captured pictures in live view mode.
  - ♦ **Save snapshots when playback to:** Set the saving path of the captured pictures in playback mode.
  - ♦ **Save clips to:** Set the saving path of the clipped video files in playback mode.

Note: You can click **Browse** to change the directory for saving the clips and pictures, and click Open to open the set folder of clips and picture saving.

3. Click Save.

5.2 Configure System Settings

Purpose:

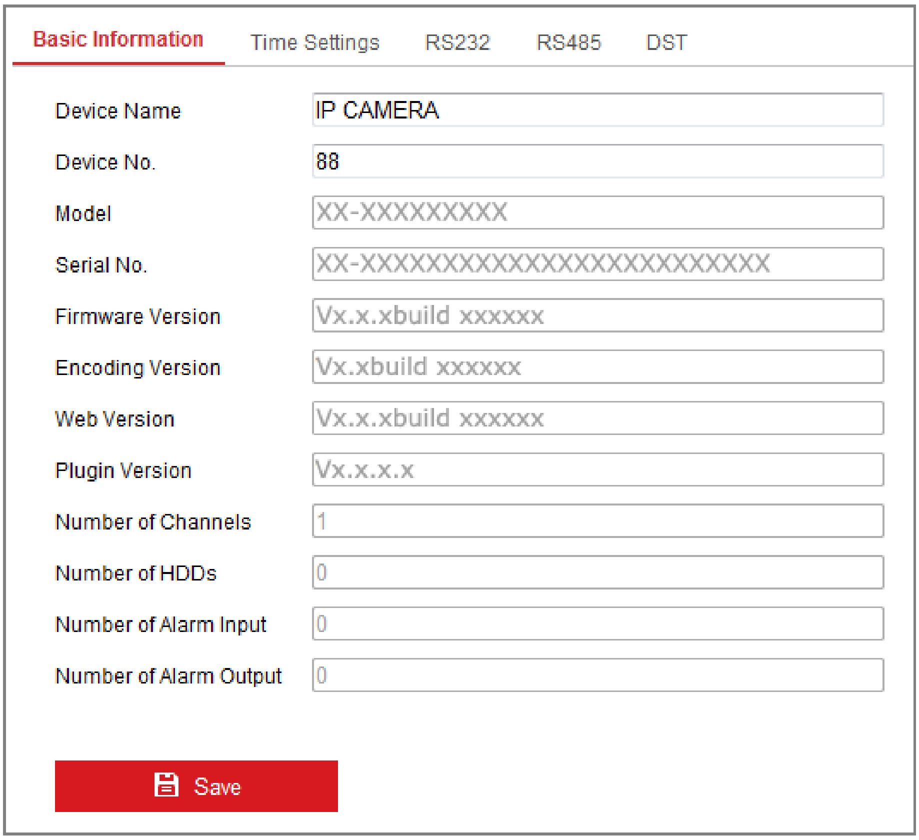
Follow the instructions below to configure the system settings, include System Settings, Maintenance, Security, and User Management, etc.

5.2.1 Set Basic Information

Go to the Device Information interface: **Configuration** > **System** > **System Settings** > **Basic Information**.

In the **Basic Information** interface, you can edit the Device Name and Device No.

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. It is the reference for maintenance or modification in future.

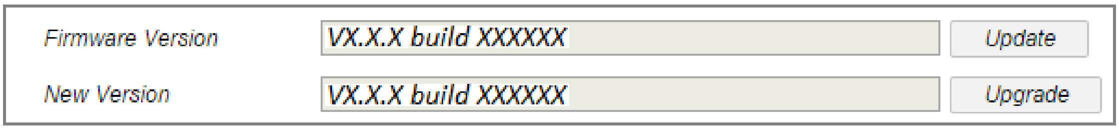


Device Name	IP CAMERA
Device No.	88
Model	XX-XXXXXXXXX
Serial No.	XX-XXXXXXXXXXXXXXXXXXXXXXXXX
Firmware Version	Vx.x.xbuild xxxxxx
Encoding Version	Vx.xbuild xxxxxx
Web Version	Vx.x.xbuild xxxxxx
Plugin Version	Vx.x.x.x
Number of Channels	1
Number of HDDs	0
Number of Alarm Input	0
Number of Alarm Output	0

Figure 5-2 Basic Information

Online Upgrade

For some camera models, when memory card is mounted, you can click the **Update** button that appears on the right of **Firmware Version** text field to see if there is a new version available. If a new version is available, the version number will be displayed in the **New Version** text field below, and you can click the **Upgrade** button to upgrade the firmware for the camera.



Firmware Version	VX.X.X build XXXXXX
New Version	VX.X.X build XXXXXX

Figure 5-3 Online Upgrade

Note: When the camera is upgrading, don't power off the camera. During upgrading, the camera may not be accessible. You need to wait 1 or 2 minutes before the upgrade finishes.

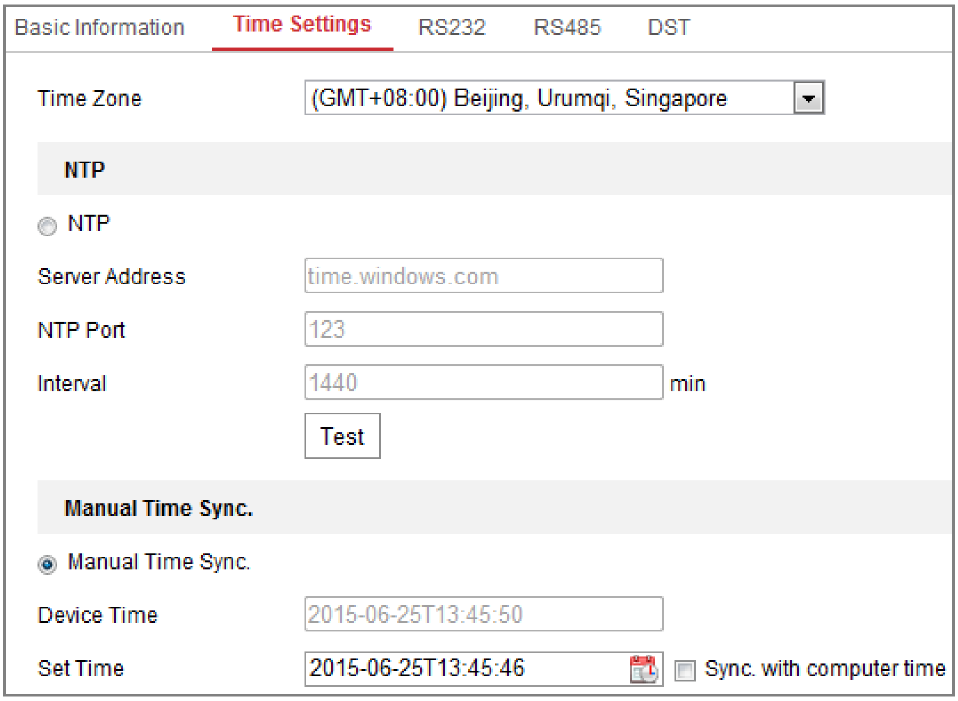
5.2.2 Set Time

Purpose:

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

Steps:

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



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

NTP

○ NTP

Server Address: time.windows.com

NTP Port: 123

Interval: 1440 min

Manual Time Sync.

● Manual Time Sync.

Device Time: 2015-06-25T13:45:50

Set Time: 2015-06-25T13:45:46 □ Sync. with computer time

Figure 5-4 Time Settings

2. Select the Time Zone of your location from the drop-down menu.
3. Configure the NTP settings.

   (1) Click to enable the **NTP** function.

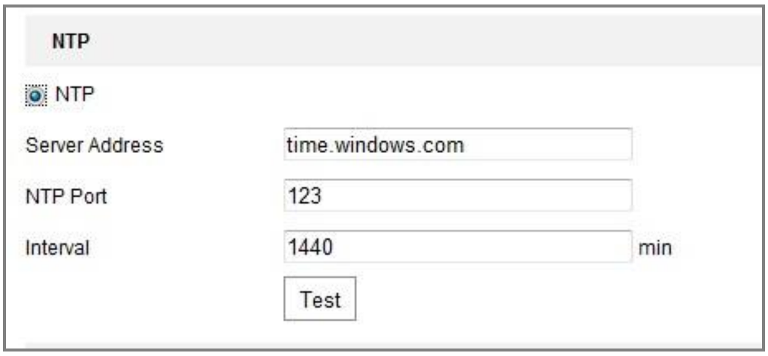
   (2) Configure the following settings:

   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.

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



NTP

● NTP

Server Address	time.windows.com
NTP Port	123
Interval	1440 min

Figure 5-5 Time Sync by NTP Server

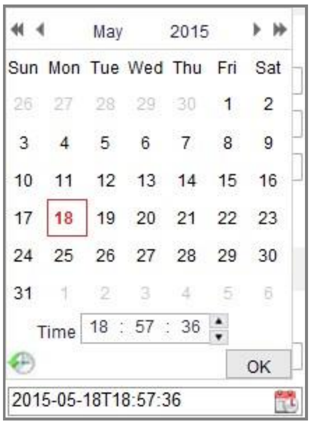
Note: If the camera is connected to a public network, you should use a NTP server that has a time synchronization function, such as the server at the National Time Center (IP Address: 210.72.145.44). If the camera is set in a customized network, NTP software can be used to establish a NTP server for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

- 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.



May 2015

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	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
31	1	2	3	4	5	6

Time 18 : 57 : 36

2015-05-18T18:57:36

Figure 5-6 Time Sync Manually

- Click Save.

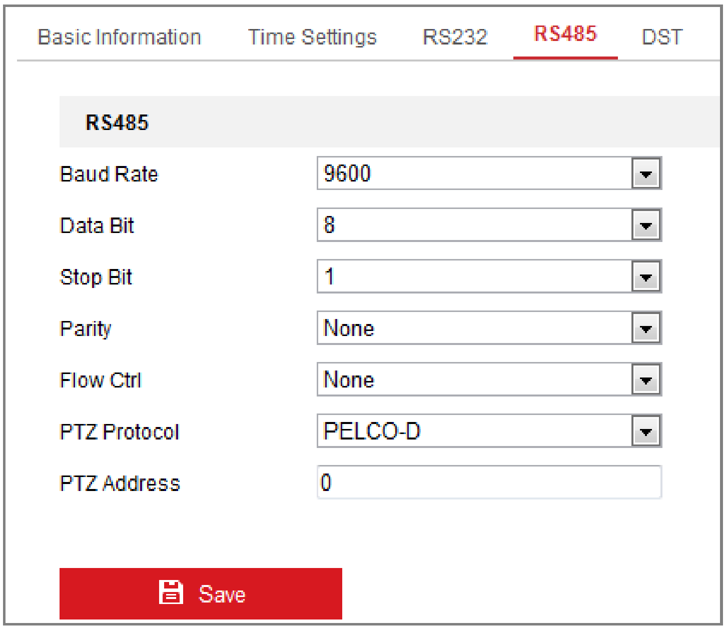
5.2.3 Set RS-485

Purpose:

The RS-485 serial port is used to control the PTZ of the camera. The configuring of the PTZ parameters should be done before you control the PTZ unit.

Steps:

1. Enter RS-485 Port Setting interface: **Configuration** > **System** > **System Settings** > **RS-485**.



RS485

Baud Rate: 9600
Data Bit: 8
Stop Bit: 1
Parity: None
Flow Ctrl: None
PTZ Protocol: PELCO-D
PTZ Address: 0

Figure 5-7 RS-485 Settings

2. Set the RS485 parameters and Click Save.

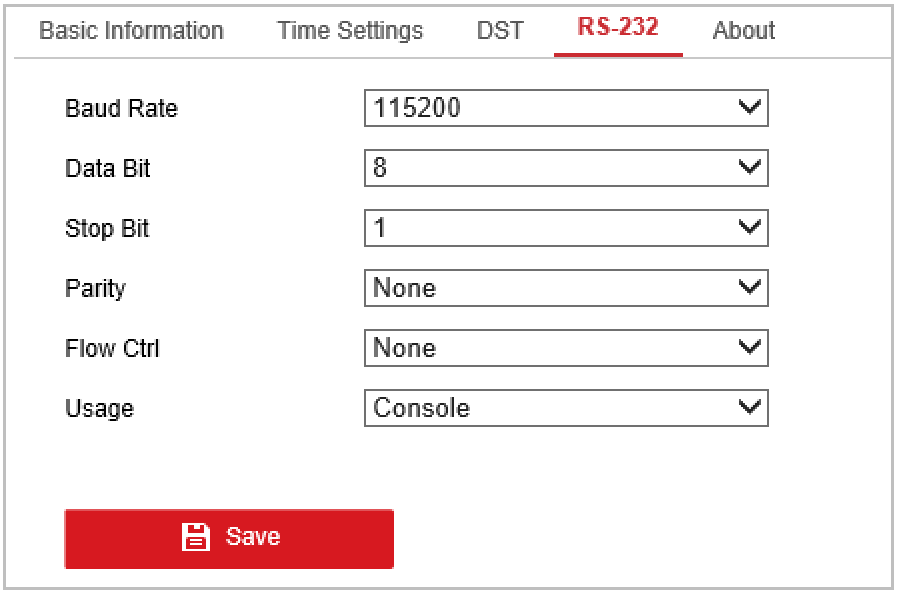
   By default, the Baud Rate is set as 9600 bps, the Data Bit is 8, the stop bit is 1 and the Parity and Flow Control is None.

Note: The Baud Rate, PTZ Protocol and PTZ Address parameters should be exactly the same as the PTZ camera parameters.

5.2.4 Set RS-232

Steps:

1. Enter RS-232 Port Setting interface: **Configuration** > **System** > **System Settings** > **RS-232**.



Baud Rate: 115200
Data Bit: 8
Stop Bit: 1
Parity: None
Flow Ctrl: None
Usage: Console

Figure 5-8 RS-232 Settings

2. Set the RS-232 parameters and click Save.

5.2.5 Set DST

Purpose:

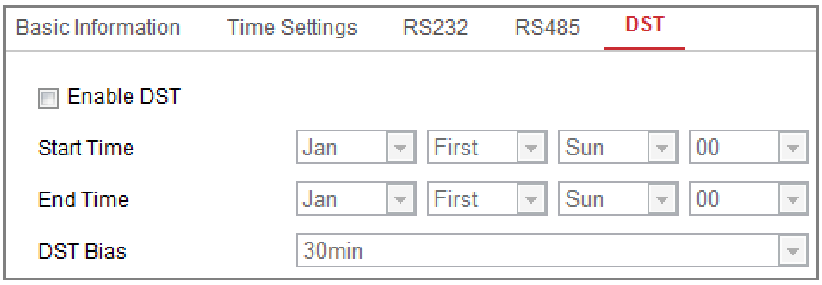
Daylight Saving Time (DST) is a way of making better use of the natural daylight by setting your clock forward one hour during the summer months, and back again in the fall.

Configure the DST according to your actual demand.

Steps:

1. Go to the DST configuration interface.

   Configuration > **System** > **System Settings** > **DST**



□ Enable DST
Start Time: Jan, First, Sun, 00
End Time: Jan, First, Sun, 00
DST Bias: 30min

Figure 5-9 Set DST

2. Select the start time and the end time.

3. Select the DST Bias.
4. Click **Save** to activate the settings.

5.2.6 View License

Purpose:

You can view the open source software licenses that are applied to the IP camera.

Steps:

1. Go to **Configuration** > **System** > **System Settings** > **About Device**.
2. Click **View Licenses.**

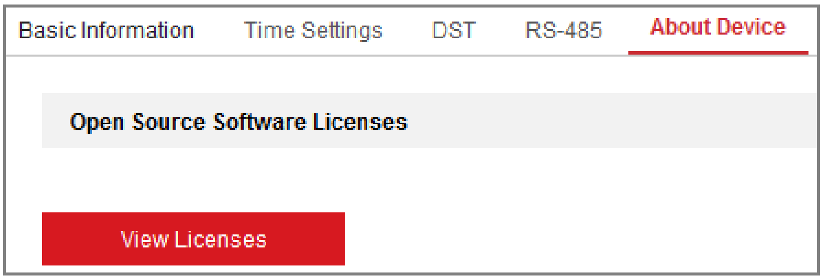


Figure 5-10 About Device Interface

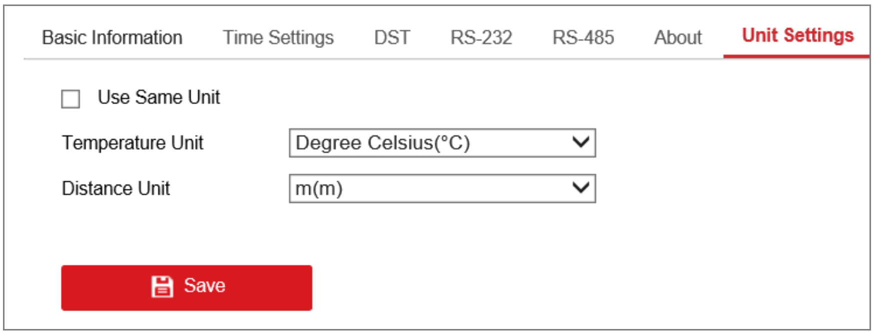
5.2.7 Set Same Unit

Purpose:

Set the same temperature unit and distance unit in this page. When you enable this function, the unit cannot be configured separately in other setting pages.

Steps:

1. Go to **Configuration** > **System** > **System Settings** > **Unit Settings**.
2. Check **Use Same Unit.**
3. Set the temperature unit and distance unit.
4. Click **Save.**



□ Use Same Unit

Temperature Unit: Degree Celsius(°C)

Distance Unit: m(m)

Figure 5-11 Unit Settings

5.3 Maintenance

5.3.1 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.

Go to the Maintenance interface: **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.

- **Export/Import Config. File:** Configuration file is used for the batch configuration of the camera, which can simplify the configuration steps when there are a lot of cameras needing configuring.

  Steps:

  1. Click **Device Parameters** to export the current configuration file, and save it to certain place.
  2. Click **Browse** to select the saved configuration file and then click **Import** to

start importing configuration file.

Note: You need to reboot the camera after importing configuration file.

- **Upgrade**: Upgrade the device to a certain version.

Steps:

1. 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.

2. 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.

5.3.2 Log

Purpose:

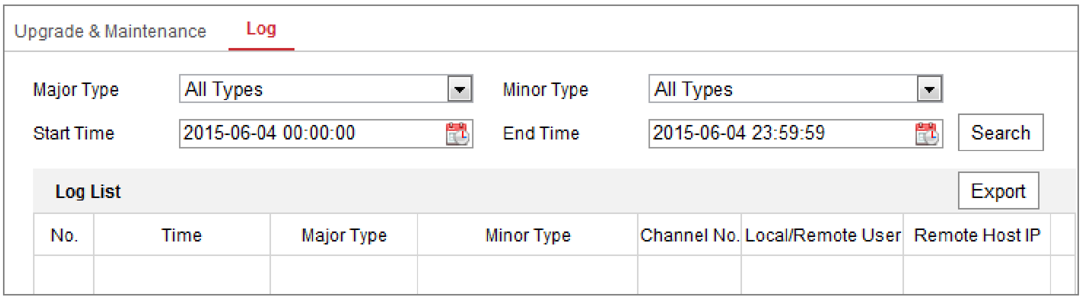
The operation, alarm, exception and information of the camera can be stored in log files. You can also export the log files on your demand.

Before you start:

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

Steps:

1. Enter log searching interface: **Configuration** > **System** > **Maintenance** > **Log**.

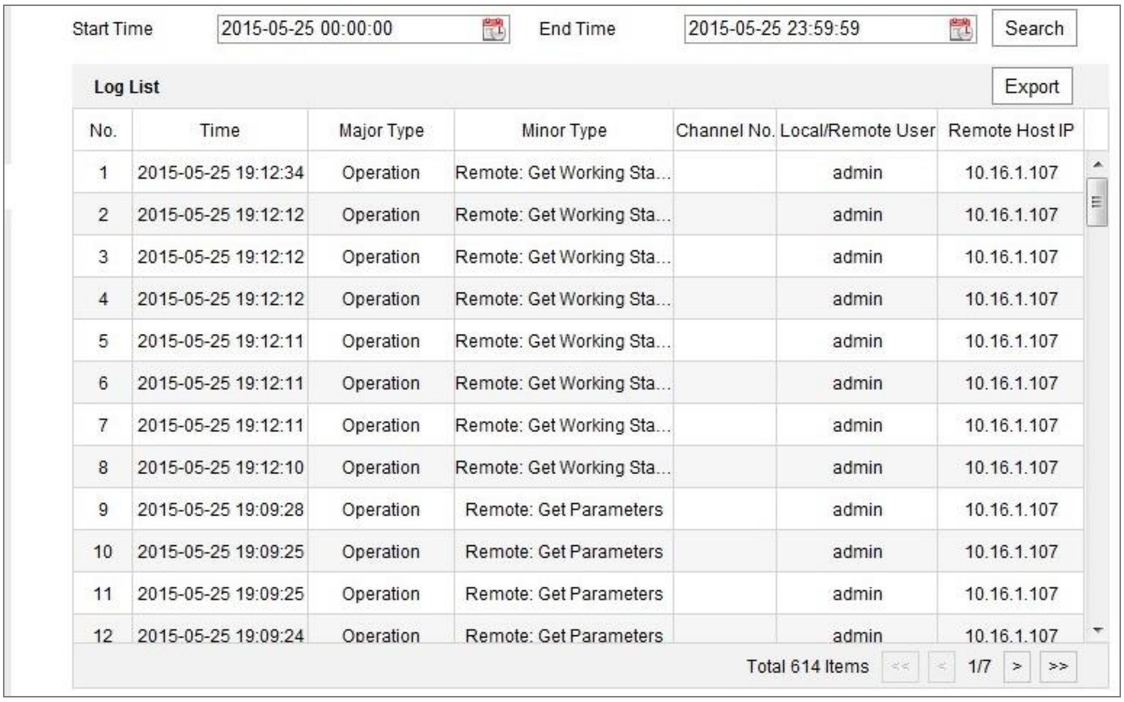


Major Type: All Types
Minor Type: All Types
Start Time: 2015-06-04 00:00:00
End Time: 2015-06-04 23:59:59

No.	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP

Figure 5-12 Log Searching Interface

2. Set the log search conditions to specify the search, including the Major Type, Minor Type, Start Time and End Time.
3. Click **Search** to search log files. The matched log files will be displayed on the log list interface.



No.	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP
1	2015-05-25 19:12:34	Operation	Remote: Get Working Sta...		admin	10.16.1.107
2	2015-05-25 19:12:12	Operation	Remote: Get Working Sta...		admin	10.16.1.107
3	2015-05-25 19:12:12	Operation	Remote: Get Working Sta...		admin	10.16.1.107
4	2015-05-25 19:12:12	Operation	Remote: Get Working Sta...		admin	10.16.1.107
5	2015-05-25 19:12:11	Operation	Remote: Get Working Sta...		admin	10.16.1.107
6	2015-05-25 19:12:11	Operation	Remote: Get Working Sta...		admin	10.16.1.107
7	2015-05-25 19:12:11	Operation	Remote: Get Working Sta...		admin	10.16.1.107
8	2015-05-25 19:12:10	Operation	Remote: Get Working Sta...		admin	10.16.1.107
9	2015-05-25 19:09:28	Operation	Remote: Get Parameters		admin	10.16.1.107
10	2015-05-25 19:09:25	Operation	Remote: Get Parameters		admin	10.16.1.107
11	2015-05-25 19:09:25	Operation	Remote: Get Parameters		admin	10.16.1.107
12	2015-05-25 19:09:24	Operation	Remote: Get Parameters		admin	10.16.1.107

Figure 5-13 Log Searching

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

5.3.3 System Service

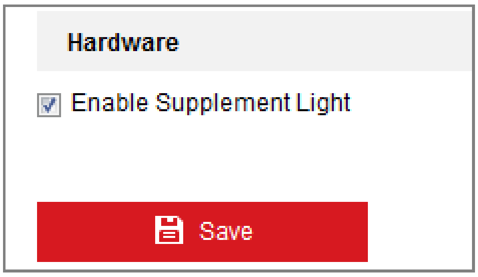
Purpose:

System service settings refer to the hardware service the camera supports. Supported functions vary according to the different cameras. For the cameras support IR LED, Supplement 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.

Supplement Light: For some models, you can check the checkbox of **Enable**

Supplement Light to reboot the system and enable the supplement light.



Hardware

☑ Enable Supplement Light

Figure 5-14 Enable Supplement Light

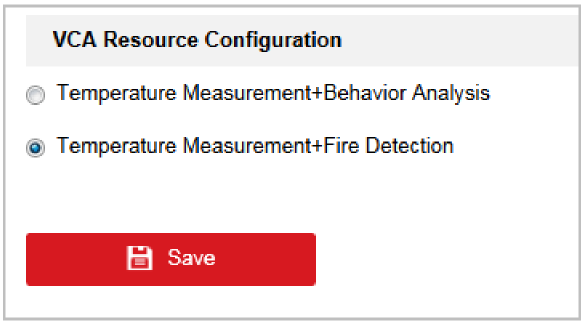
5.3.4 VCA Resource Type

Purpose:

VCA resource offers you options to enable certain VCA functions according to actual need when several VCA functions are available. It helps allocate more resources to the wanted functions.

Steps:

1. Enter VCA Resource Type interface: **Configuration** > **System** > **Maintenance** > **VCA Resource Type**.



VCA Resource Configuration

○ Temperature Measurement+Behavior Analysis

● Temperature Measurement+Fire Detection

Figure 5-15 VCA Resource Type

2. Check the checkbox to enable the desired VCA resource type.
3. Click **Save**. A reboot is required after setting the VCA Resource.

Notes:

- VCA Resource function varies according to different camera models.
- The function may not be supported by some camera models.

5.4 Security Settings

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

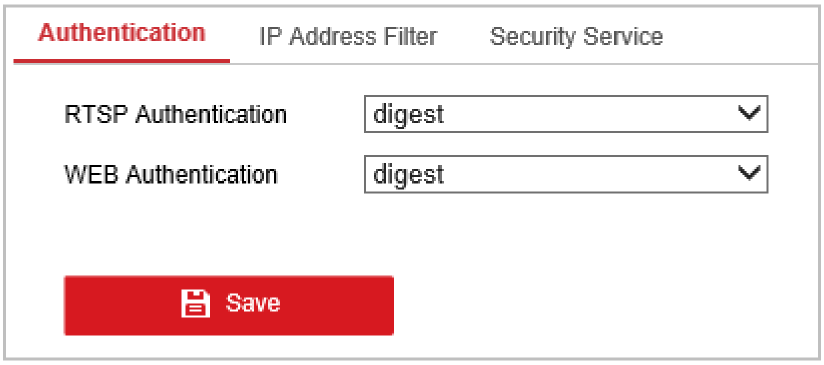
5.4.1 Authentication

Purpose:

You can specifically secure the stream data of live view.

Steps:

1. Go to the Authentication interface: **Configuration** > **System** > **Security** > **Authentication.**



RTSP Authentication: digest

WEB Authentication: digest

Figure 5-16 RTSP / WEB Authentication

2. Select the RTSP /WEB **Authentication** type **digest** or **digest/basic** in the drop-down list.
3. Click Save.

5.4.2 IP Address Filter

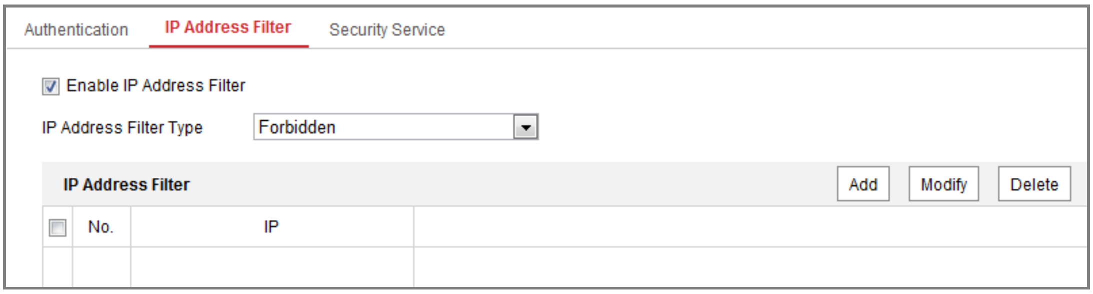
Purpose:

This function makes it possible for access control.

Steps:

1. Go to the IP Address Filter interface: **Configuration** > **System** > **Security** > **IP**

Address Filter



☑ Enable IP Address Filter

IP Address Filter Type: Forbidden

Figure 5-17 IP Address Filter Interface

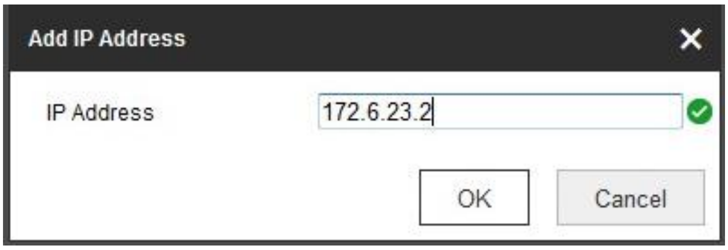
2. Check the checkbox of **Enable IP Address Filter**.
3. Select the type of IP Address Filter in the drop-down list, **Forbidden** and **Allowed** are selectable.
4. Set the IP Address Filter list.

- Add an IP Address

  Steps:

(1) Click the **Add** to add an IP.

(2) Input the IP Adreess.



IP Address: 172.6.23.2

Figure 5-18 Add an IP

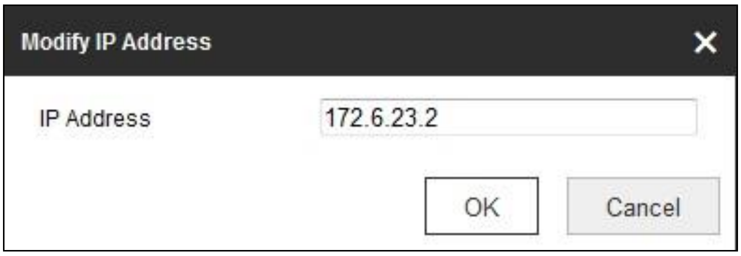
(3) Click the **OK** to finish adding.

- Modify an IP Address

  Steps:

(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

Figure 5-19 Modify an IP

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

- Delete an IP Address or IP Addresses.

  Select the IP address(es) and click **Delete**.

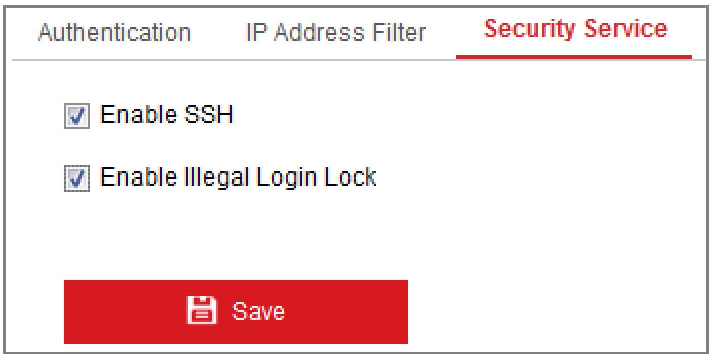
5. Click Save.

5.4.3 Security Service

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

Steps:

1. Go to the security service configuration interface: **Configuration** > **System** > **Security** > **Security Service**.



Authentication | IP Address Filter | Security Service

☑ Enable SSH

☑ Enable Illegal Login Lock

Figure 5-20 Security Service

2. Check the checkbox of **Enable SSH** to enable the data communication security, and uncheck the checkbox to disable the SSH.
3. Check the checkbox of **Enable Illegal Login Lock**, and then the IP address will be locked if the admin user performs 7 failed user name/password attempts (5 times for the operator/user).

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

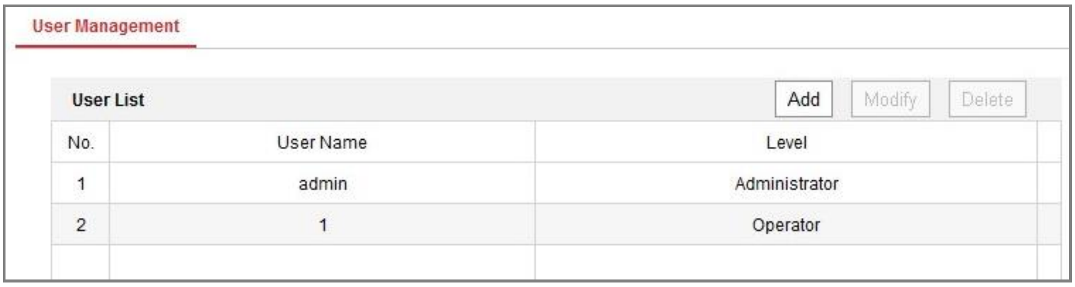
5.5 User Management

Purpose:

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.

Steps:

1. Go to the User Management interface: **Configuration >System >User Management**



No.	User Name	Level
1	admin	Administrator
2	1	Operator

Figure 5-21 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.

Steps:

1. Click **Add** to add a user.
2. Input the **User Name**, select **Level** and input **Password.**

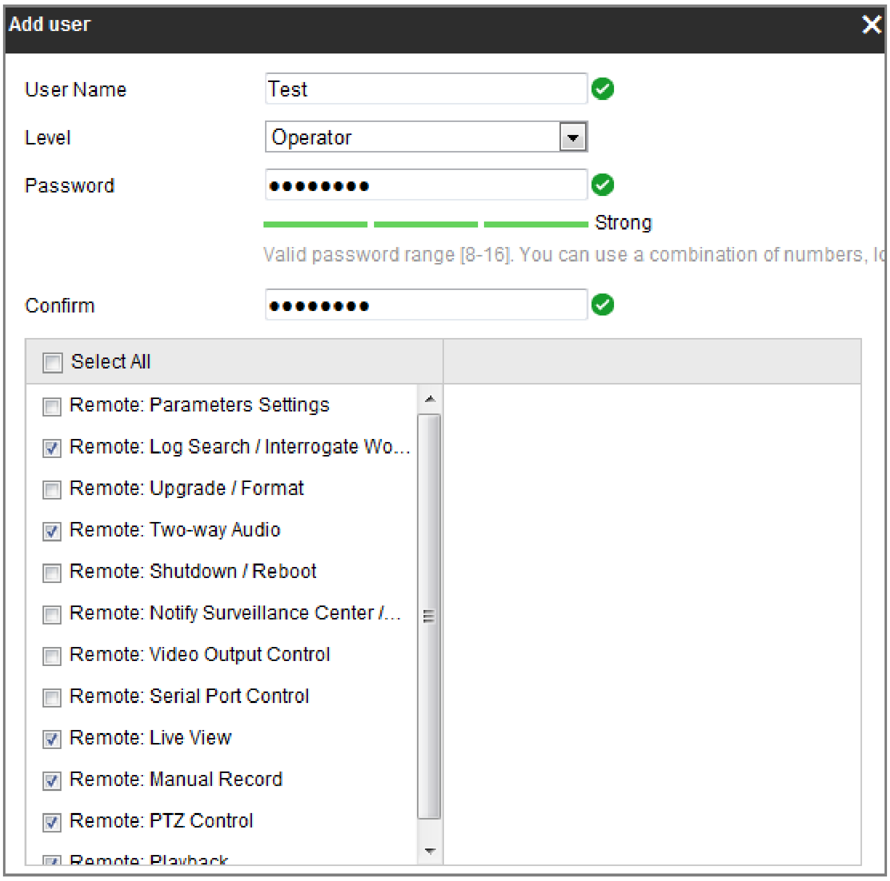
Notes:

- Up to 31 user accounts can be created.
- Users of different levels own different default permissions. Operator and user are selectable.

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.

3. You can check or uncheck the permissions for the new user.

4. Click **OK** to finish the user addition.



Add user

User Name: Test ✓

Level: Operator

Password: •••••••• ✓

Strong

Valid password range [8-16]. You can use a combination of numbers, lo

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 5-22 Add a User

- **Modifying a User**

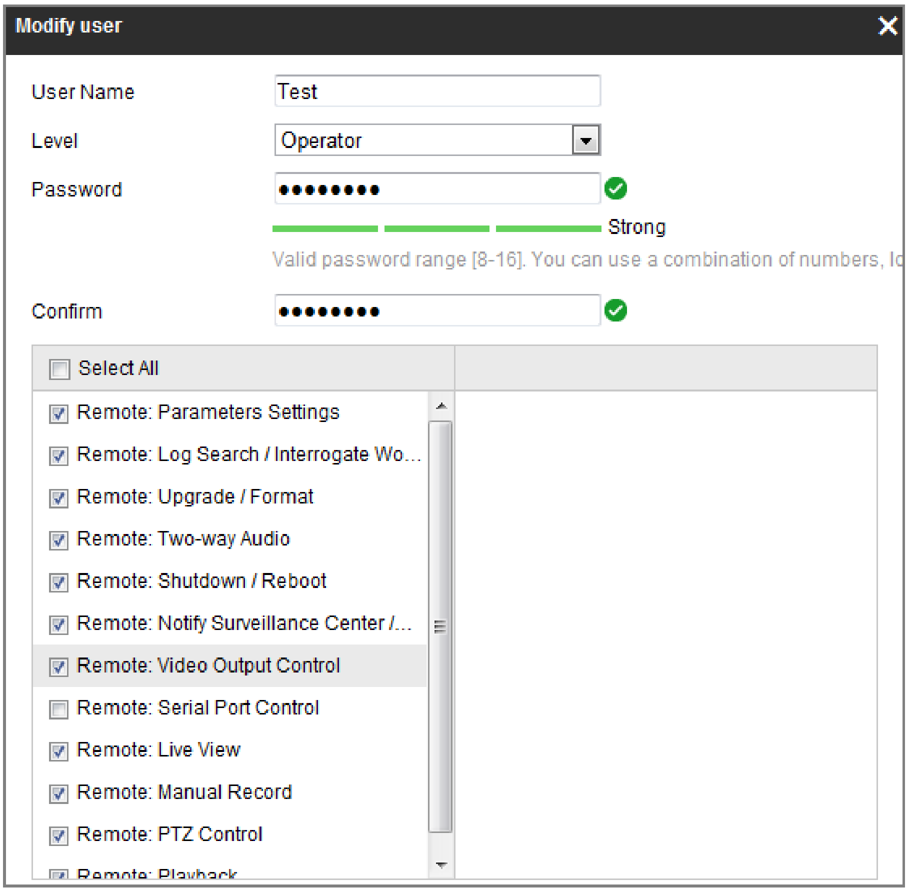
Steps:

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

2. Modify the **User Name**, **Level** and **Password**.

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.

4. You can check or uncheck the permissions.
5. Click **OK** to finish the user modification.



Modify user

User Name: Test

Level: Operator

Password: •••••••• ✓

Strong

Valid password range [8-16]. You can use a combination of numbers, lo

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 5-23 Modify a User

- **Deleting a User**

Steps:

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.

Chapter 6 Network Settings

Purpose:

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

6.1 Basic Settings

Purpose:

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

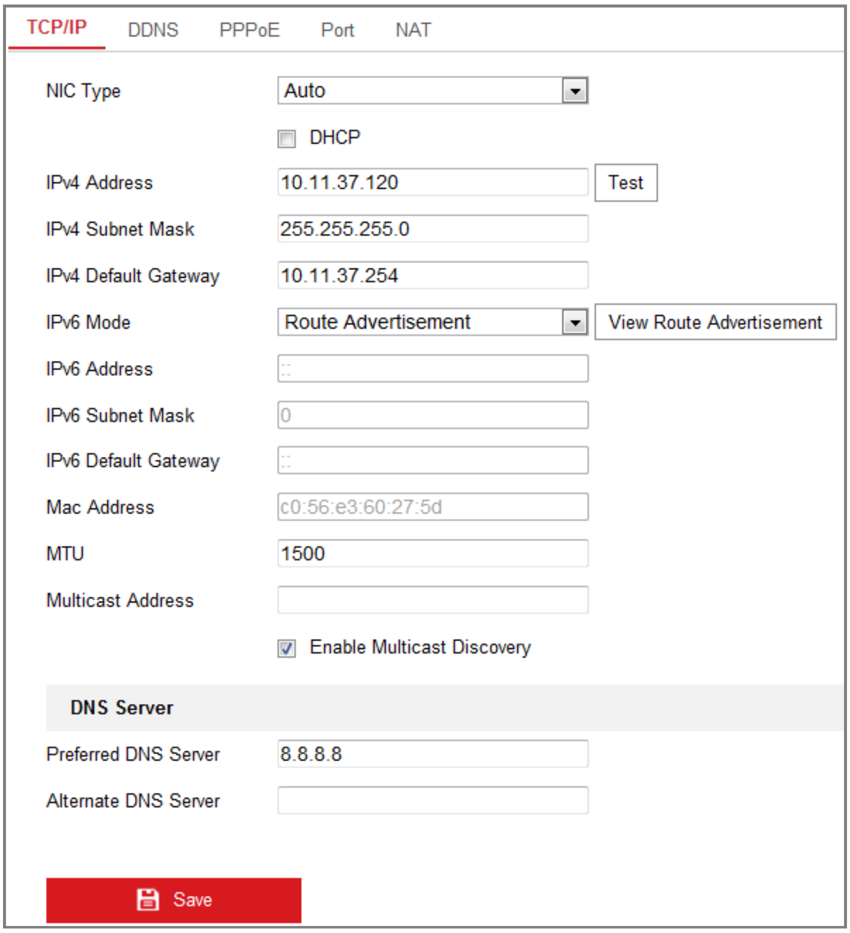
6.1.1 Set TCP/IP

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.

Steps:

1. Enter TCP/IP Settings interface: **Configuration > Network > Basic Settings > TCP/IP**



NIC Type: Auto

□ DHCP

IPv4 Address: 10.11.37.120

IPv4 Subnet Mask: 255.255.255.0

IPv4 Default Gateway: 10.11.37.254

IPv6 Mode: Route Advertisement

IPv6 Address: ::

IPv6 Subnet Mask: 0

IPv6 Default Gateway: ::

Mac Address: c0:56:e3:60:27:5d

MTU: 1500

Multicast Address:

☑ Enable Multicast Discovery

DNS Server

Preferred DNS Server: 8.8.8.8

Alternate DNS Server:

Figure 6-1 TCP/IP Settings

2. Configure the basic network settings, including the NIC Type, IPv4 or IPv6 Address, IPv4 or IPv6 Subnet Mask, IPv4 or IPv6 Default Gateway, MTU settings and Multicast Address.
3. (Optional) Check the checkbox of **Enable Multicast Discovery**, and then the online network camera can be automatically detected by client software via private multicast protocol in the LAN.
4. Configure the DNS server. Input the preferred DNS server, and alternate DNS server.
5. Click **Save** to save the above settings.

Notes:

- The valid value range of MTU is 1280 ~ 1500.
- 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.

- A reboot is required for the settings to take effect.

6.1.2 Set DDNS

Purpose:

If your camera is set to use PPPoE as its default network connection, you can use the Dynamic DNS (DDNS) for network access.

***Before you start*:**

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

Steps:

1. Go to the DDNS Settings interface: **Configuration > Network > Basic Settings > DDNS**.
2. Check the **Enable DDNS** checkbox to enable this feature.
3. Select **DDNS Type**. Two DDNS types are selectable: DynDNS and NO-IP.
   - DynDNS:

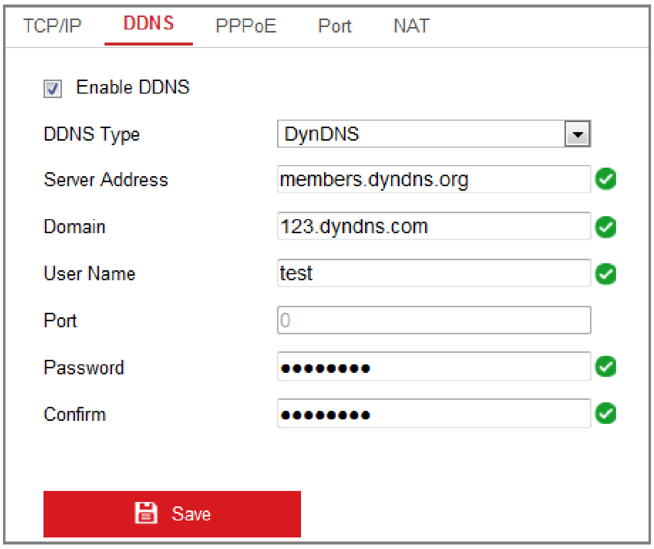
   Steps:

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

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

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

   (4) Click Save.



☑ Enable DDNS

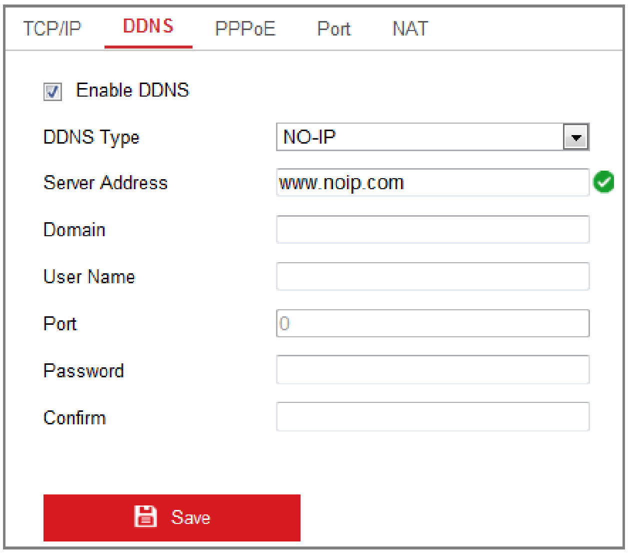
DDNS Type	DynDNS
Server Address	members.dyndns.org ✓
Domain	123.dyndns.com ✓
User Name	test ✓
Port	0
Password	•••••••• ✓
Confirm	•••••••• ✓

Figure 6-2 DynDNS Settings

- NO-IP:

Steps:

(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 6-3 NO-IP DNS Settings

(2) Enter the Server Address as www.noip.com

(3) Enter the Domain name you registered.

(4) Enter the User Name and Password.

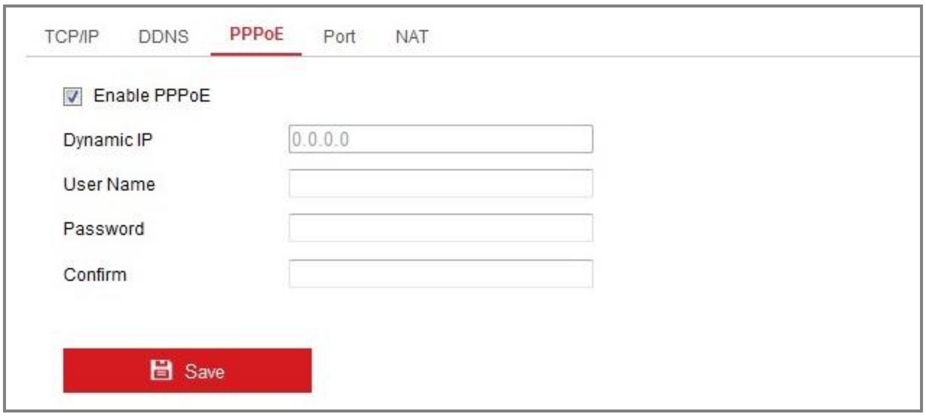
(5) Click **Save** and then you can view the camera with the domain name.

Note: Reboot the device to make the settings take effect.

6.1.3 Set PPPoE

Steps:

1. Go to the PPPoE Settings interface: **Configuration > Network > Basic Settings > PPPoE**



☑ Enable PPPoE

Dynamic IP 0.0.0.0

User Name

Password

Confirm

Figure 6-4 PPPoE Settings

2. Check the **Enable PPPoE** checkbox to enable this feature.
3. Enter **User Name**, **Password**, and **Confirm** password for PPPoE access.

Note: The User Name and Password should be assigned by your ISP.

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something 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.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

4. Click **Save** to save and exit the interface.

Note: A reboot is required for the settings to take effect.

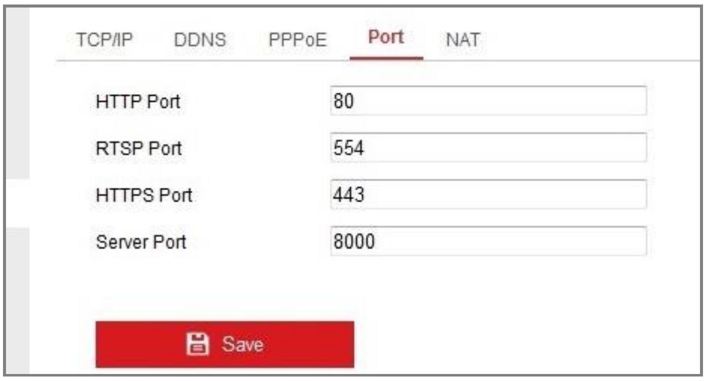
6.1.4 Set Port

Purpose:

You can set the port No. of the camera, e.g., HTTP port, RTSP port and HTTPS port.

Steps:

1. Go to the Port Settings interface, **Configuration > Network > Basic Settings > Port**



HTTP Port: 80
RTSP Port: 554
HTTPS Port: 443
Server Port: 8000

Figure 6-5 Port Settings

2. Set the HTTP port, RTSP port, HTTPS port and server port 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.

3. Click Save.

***Note*:** A reboot is required for the settings to take effect.

6.1.5 Set NAT (Network Address Translation)

Purpose:

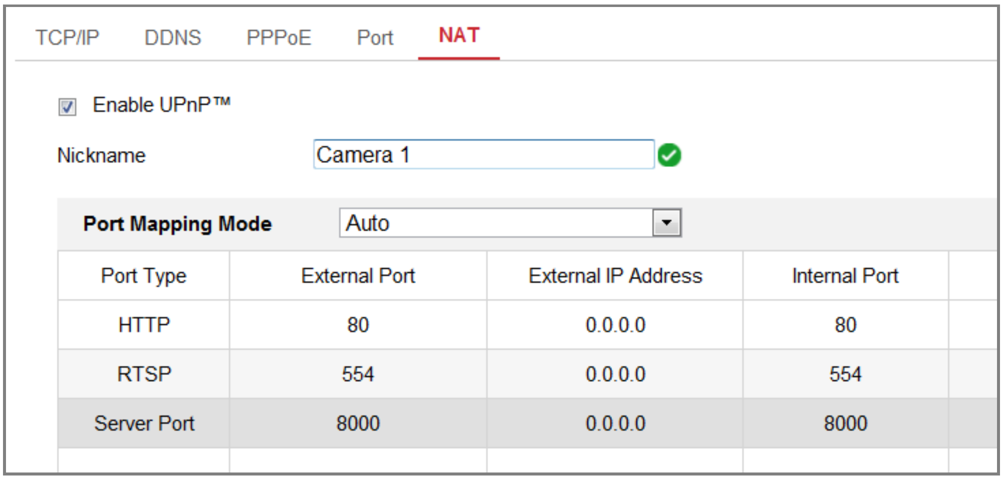
NAT interface allows you to configure the UPnP™ parameters.

Universal Plug and Play (UPnP™) is a networking architecture that provides compatibility among networking equipment, software and other hardware devices. The UPnP protocol allows devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments.

With the function enabled, you don't need to configure the port mapping for each port, and the camera is connected to the Wide Area Network via the router.

Steps:

1. Go to the NAT settings interface. **Configuration > Network > Basic Settings > NAT.**
2. Check the checkbox to enable the UPnP™ function.
3. Choose a nickname for the camera, or you can use the default name.
4. Select the port mapping mode. Manual and Auto are selectable. And for manual port mapping, you can customize the value of the external port.
5. Click Save.



☑ Enable UPnP™

Nickname: Camera 1

Port Mapping Mode: Auto

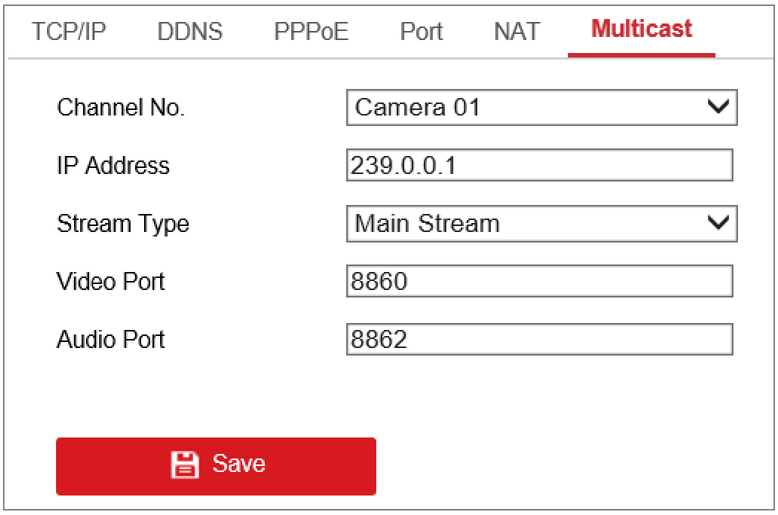
Port Type	External Port	External IP Address	Internal Port
HTTP	80	0.0.0.0	80
RTSP	554	0.0.0.0	554
Server Port	8000	0.0.0.0	8000

Figure 6-6 UPnP Settings

6.1.6 Set Multicast

Purpose:

Multicast is group communication where data transmission is addressed to a group of destination devices simultaneousl.



Channel No. Camera 01

IP Address 239.0.0.1

Stream Type Main Stream

Video Port 8860

Audio Port 8862

Figure 6-7 Set Multicast

Steps:

1. Go to the Multicast setting interface: **Configuration** > **Network** > **Basic Settings** > **Multicast.**
2. Select the channel number.
3. Set **IP Address, Stream Type, Video Port,** and **Audio Port** of the camera.

   Notes:

- IP Address stands for the address of multicast.
- Video port and audio port of each video stream of each camera channel can be specified by selecting a stream in Video Stream and inputting port number in Video Port and Audio Port.

4. Click **Save**.

6.2 Advanced Settings

Purpose:

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

6.2.1 Set SNMP

Purpose:

You can set the SNMP function to get camera status, parameters and alarm related information, and manage the camera remotely when it is connected to the network.

Before you start:

Before setting the SNMP, please download the SNMP software and manage to receive the camera information via SNMP port. By setting the Trap Address, the camera can send the alarm event and exception messages to the surveillance center.

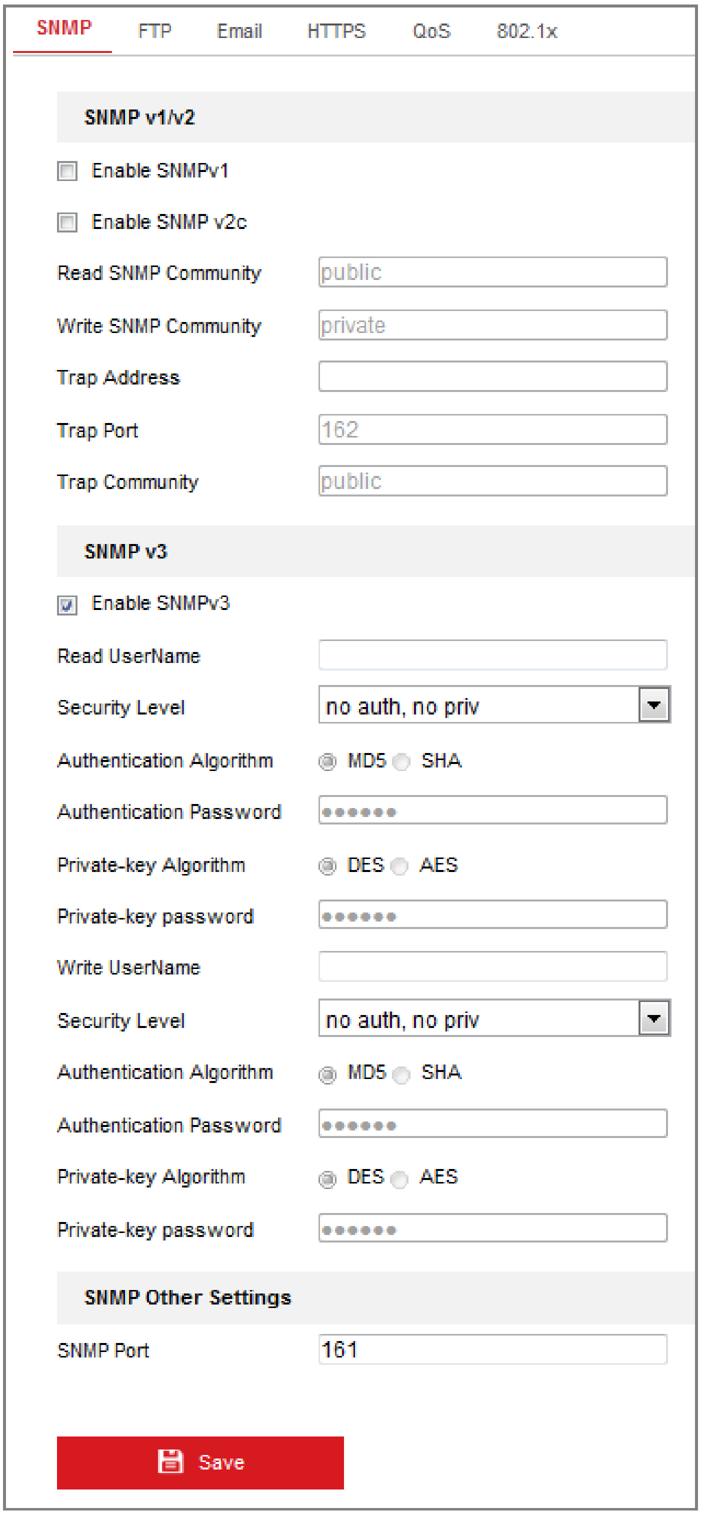
Note: The SNMP version you select should be the same as that of the SNMP software. And you also need to use the different version according to the security level you required. SNMP v1 provides no security and SNMP v2 requires password for access. And SNMP v3 provides encryption and if you use the third version, HTTPS protocol must be enabled.

⚠

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something 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.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Steps:

1. Go to the SNMP Settings interface: **Configuration > Network > Advanced Settings > SNMP**.



SNMP v1/v2

☐ Enable SNMPv1

☐ Enable SNMP v2c

Read SNMP Community	public
Write SNMP Community	private
Trap Address	
Trap Port	162
Trap Community	public

SNMP v3

☑ Enable SNMPv3

Read UserName	
Security Level	no auth, no priv
Authentication Algorithm	● MD5 ○ SHA
Authentication Password	••••••
Private-key Algorithm	● DES ○ AES
Private-key password	••••••
Write UserName	
Security Level	no auth, no priv
Authentication Algorithm	● MD5 ○ SHA
Authentication Password	••••••
Private-key Algorithm	● DES ○ AES
Private-key password	••••••

SNMP Other Settings

SNMP Port	161

Figure 6-8 SNMP Settings

2. Check the checkbox of Enable SNMPv1, Enable SNMP v2c, Enable SNMPv3 to enable the feature correspondingly.

3. Configure the SNMP settings.

Note: The settings of the SNMP software should be the same as the settings you configure here.

4. Click **Save** to save and finish the settings.

***Notes*:**

- A reboot is required for the settings to take effect.
- To lower the risk of information leakage, you are suggested to enable SNMP v3 instead of SNMP v1 or v2.

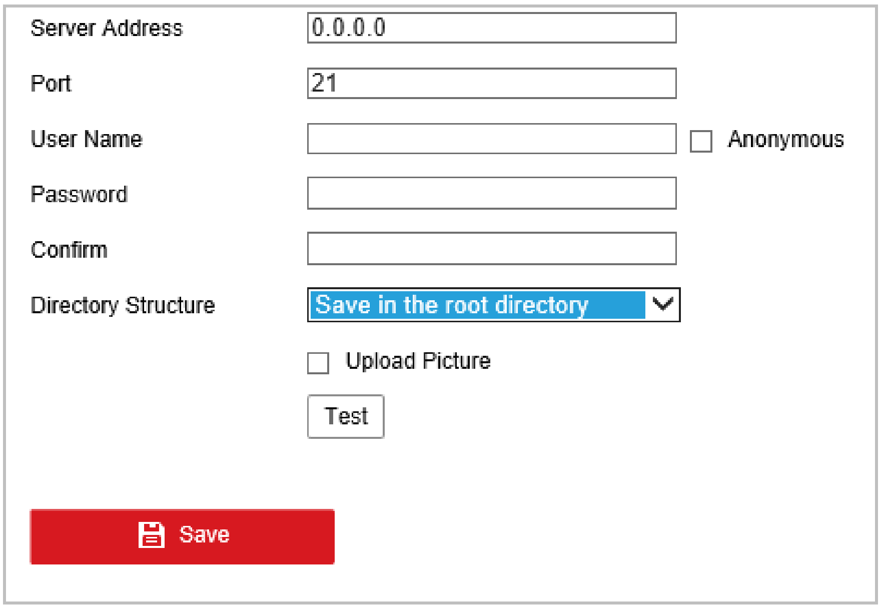
6.2.2 Set FTP

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.

Steps:

1. Go to the FTP Settings interface: **Configuration > Network > Advanced Settings > FTP**.



Server Address	0.0.0.0
Port	21
User Name	□ Anonymous
Password	
Confirm	
Directory Structure	Save in the root directory
	□ Upload Picture

Figure 6-9 FTP Settings

2. Input the FTP address and port.
3. Configure the FTP settings; and the user name and password are required for the FTP server login.

⚠

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something 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.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

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.

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.

6. Click Save.

6.2.3 Set 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:

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

Steps:

1. Go to the TCP/IP Settings (**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 ***6.1.1***for detailed information.

2. Go to the Email Settings interface: **Configuration** > **Network** >**Advanced Settings** > **Email**.

3. 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, SSL, and TLS are selectable. When you select SSL or TLS and disable STARTTLS, e-mails will be sent after encrypted by SSL or TLS. The SMTP port should be set as 465 for this encryption method. When you select SSL or TLS 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.

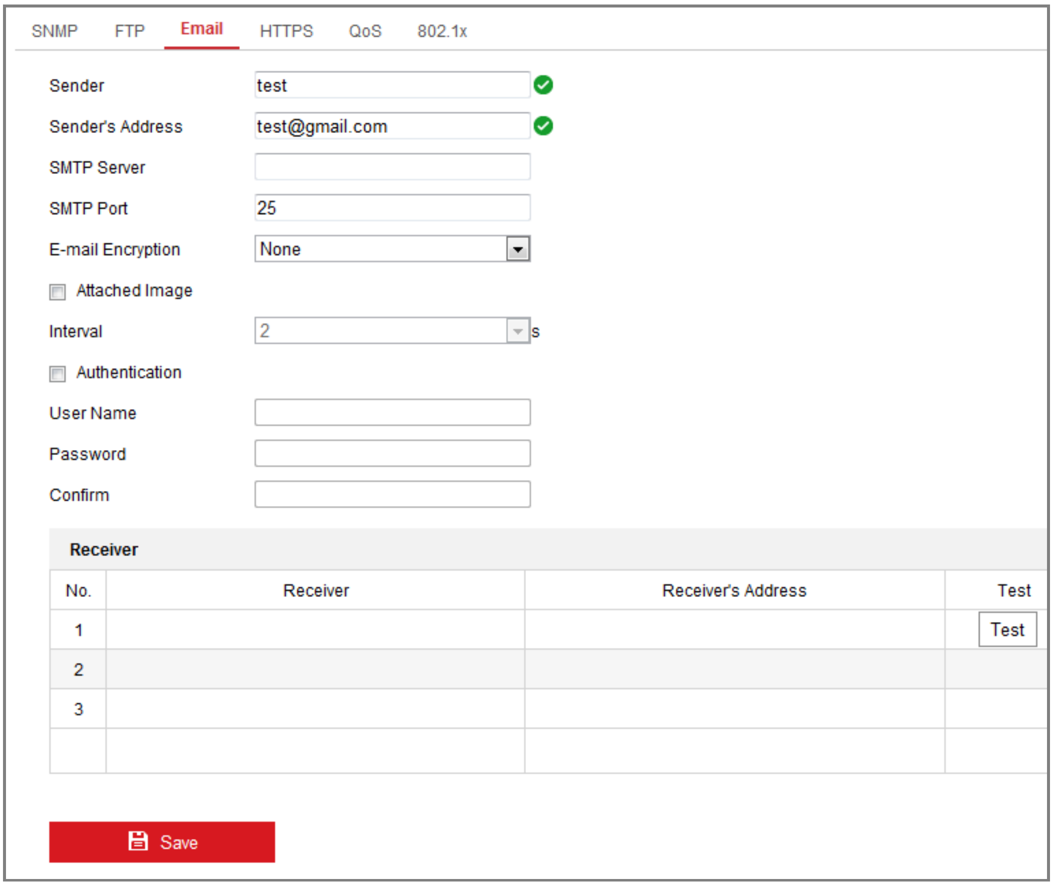
⚠

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something 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.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

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

Receiver: The name of the user to be notified.

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 6-10 Email Settings

4. Click Save.

6.2.4 Set Platform Access

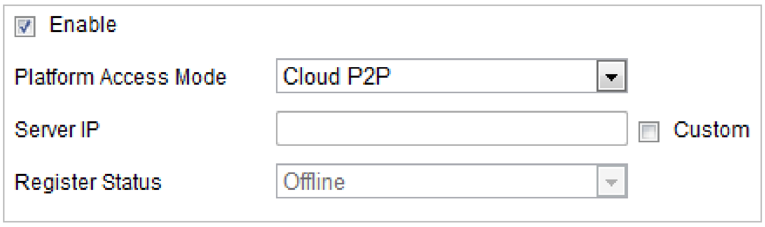
Purpose:

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

Steps:

1. Go to the Platform Access interface.

   Configuration > Network > Advanced Settings > Platform Access



☑ Enable

Platform Access Mode	Cloud P2P
Server IP	□ Custom
Register Status	Offline

Figure 6-11 Platform Access Settings

2. Check the checkbox of **Enable** to enable the platform access function of the device.
3. Select the Platform Access Mode from the dropdown list.

4. Set the Server IP.
5. Click Save to save the settings

6.2.5 Set HTTPS

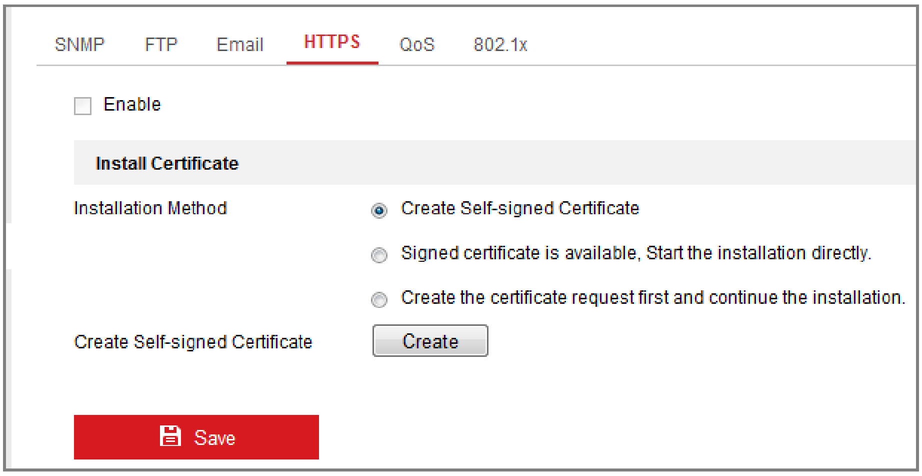
Purpose:

HTTPS provides authentication of the web site and its associated web server, which protects against Man-in-the-middle attacks. Perform the following steps to set the port number of https.

E.g., If you set the port number as 443 and the IP address is 192.168.1.64, you may access the device by inputting https://192.168.1.64:443 via the web browser.

Steps:

1. Go to the HTTPS settings interface. **Configuration > Network > Advanced Settings > HTTPS**.
2. Check the checkbox of Enable to enable the function.



□ Enable

Install Certificate

Installation Method
● Create Self-signed Certificate
○ Signed certificate is available, Start the installation directly.
○ Create the certificate request first and continue the installation.

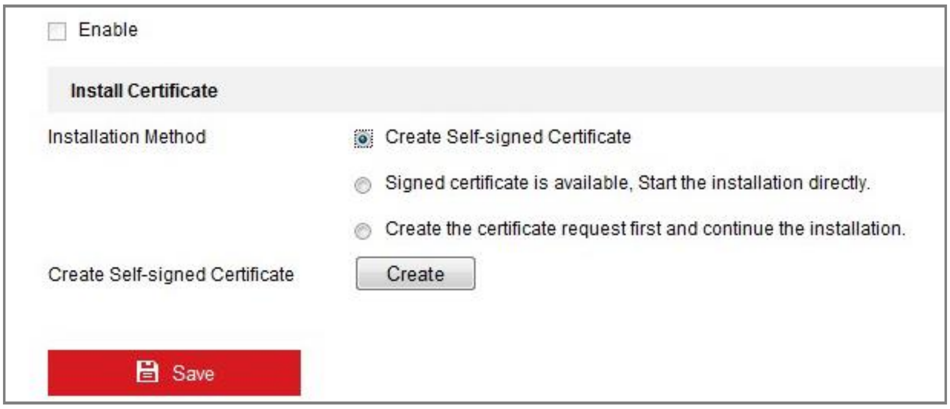
Create Self-signed Certificate: Create

Figure 6-12 HTTPS Configuration Interface

3. Create the self-signed certificate or authorized certificate.
   - Create the self-signed certificate

   (1) Select **Create Self-signed Certificate** as the Installation Method.

   (2) Click **Create**.



□ Enable

Install Certificate

Installation Method
● Create Self-signed Certificate
○ Signed certificate is available, Start the installation directly.
○ Create the certificate request first and continue the installation.

Create Self-signed Certificate — Create

Figure 6-13 Create Self-signed Certificate

(3) Enter the country, host name/IP, validity and other information.

(4) Click **OK** to save the settings.

Note: If you already had a certificate installed, the Create Self-signed Certificate is grayed out.

- Create the authorized certificate

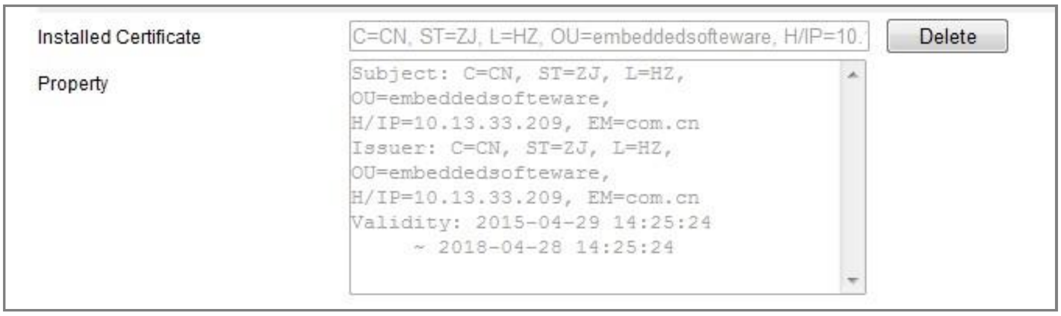
(1) Select **Create the certificate request first and continue the installation** as the Installation Method.

(2) Click **Create** button to create the certificate request. Fill in the required information in the popup window.

(3) Download the certificate request and submit it to the trusted certificate authority for signature.

(4) After receiving the signed valid certificate, import the certificate to the device.

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



Installed Certificate: C=CN, ST=ZJ, L=HZ, OU=embeddedsofteware, H/IP=10.

Property:

```
Subject: C=CN, ST=ZJ, L=HZ,
OU=embeddedsofteware,
H/IP=10.13.33.209, EM=com.cn
Issuer: C=CN, ST=ZJ, L=HZ,
OU=embeddedsofteware,
H/IP=10.13.33.209, EM=com.cn
Validity: 2015-04-29 14:25:24
     ~ 2018-04-28 14:25:24
```

Figure 6-14 Installed Certificate

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

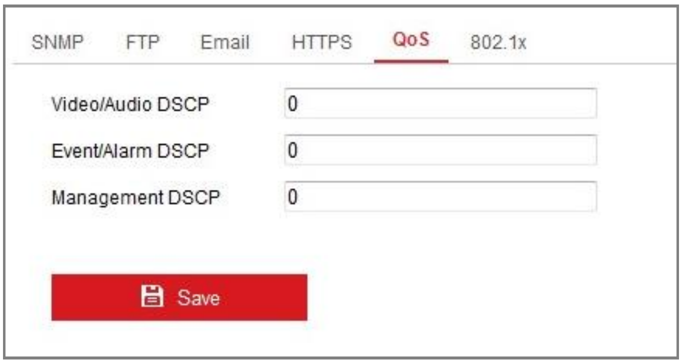
6.2.6 Set QoS

Purpose:

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

Steps:

1. Go to the QoS Settings interface: **Configuration > Network > Advanced Settings > QoS**



Video/Audio DSCP: 0

Event/Alarm DSCP: 0

Management DSCP: 0

Figure 6-15 QoS Settings

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.

3. Click Save.

Note: A reboot is required for the settings to take effect.

6.2.7 Set 802.1X

Purpose:

The IEEE 802.1X standard is supported by the network cameras, and when the feature is enabled, the camera data is secured and user authentication is needed when connecting the camera to the network protected by the IEEE 802.1X.

Before you start:

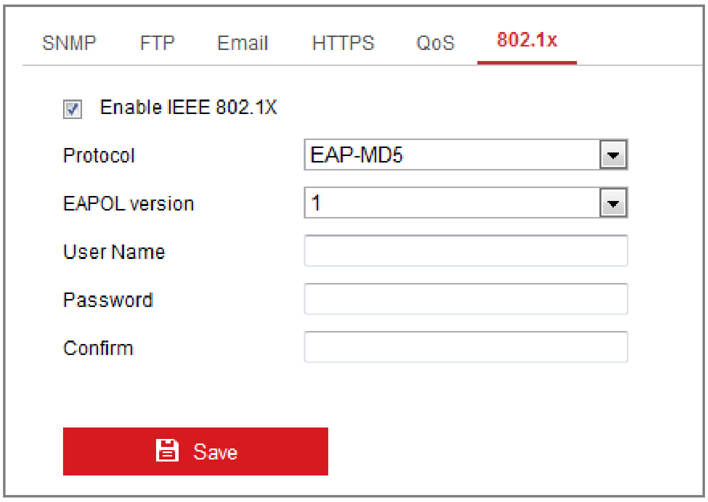
The authentication server must be configured. Please apply and register a user name and password for 802.1X in the server.

⚠

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something 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.*
- *Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.*

Steps:

1. Go to the 802.1X Setting interface, **Configuration > Network > Advanced Settings > 802.1X**



☑ Enable IEEE 802.1X

Protocol	EAP-MD5
EAPOL version	1
User Name	
Password	
Confirm	

Figure 6-16 802.1X Settings

2. Check the **Enable IEEE 802.1X** checkbox to enable the feature.
3. Select the protocol. EAP-TLS and EAP-MD5 are available.
4. Enter the EAPOL version.

Note: The EAPOL version must be identical with that of the router or the switch.

5. Enter the user name and password to access the server.
6. If you set the protocol to EAP-TLS, you should enter the identify, private key password, upload the CA certificate, user certificate and private key.
7. Click **Save**.

Note: A reboot is required for the settings to take effect.

6.2.8 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.

● **CGI**

Check the **Enable Hikvision_CGI** checkbox and then select the authentication from the drop-down list.

Note: Digest is the recommended authentication method.

● **ONVIF**

Steps:

1. Check the Enable ONVIF checkbox to enable the function.
2. Add ONVIF users. Up to 32 users are allowed.
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.

4. Save the settings.

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

Chapter 7 Video/Audio Settings

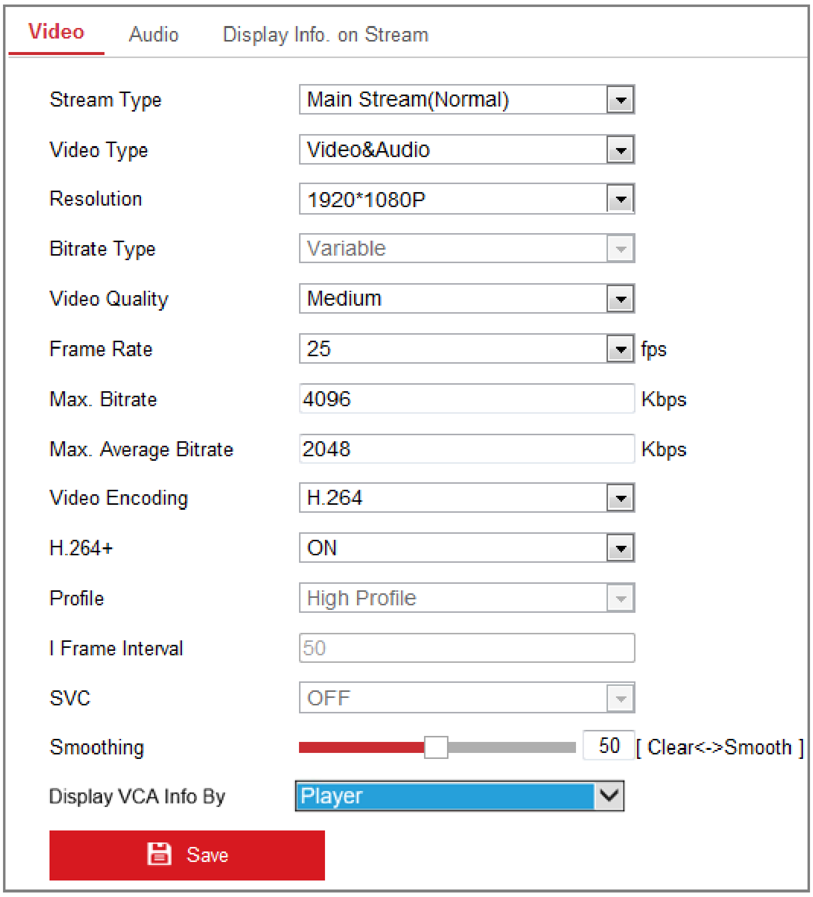
Purpose:

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

7.1 Set Video

Steps:

1. Go to the Video Settings interface: **Configuration > Video/Audio > Video**



Stream Type	Main Stream(Normal)	
Video Type	Video&Audio	
Resolution	1920*1080P	
Bitrate Type	Variable	
Video Quality	Medium	
Frame Rate	25	fps
Max. Bitrate	4096	Kbps
Max. Average Bitrate	2048	Kbps
Video Encoding	H.264	
H.264+	ON	
Profile	High Profile	
I Frame Interval	50	
SVC	OFF	
Smoothing	50	[Clear<->Smooth]
Display VCA Info By	Player	

Figure 7-1 Video Settings

2. Select the Stream Type of the camera to main stream (normal), sub-stream or third stream.

Notes:

- For some models, to enable the third stream, go to System > Maintenance >

System Service> Software and check the checkbox of Enable Third Stream to reboot the system and enable the third stream.

- 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.
- To enable the third stream, go to System>Maintenance>System Service> Software and check the checkbox of Enable Third Stream to reboot the system and enable the third stream.

3. 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:

If the Stream Type is set to main stream, H.264 and H.265 are selectable, and if the stream type is set to sub stream or third stream, H.264, MJPEG, and H.265 are selectable. 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.

Notes:

- Upgrade your video player to the latest version if live view or playback does not work properly due to compatibility.
- The bitrate type must be variable if you want to use H.264+ or H.265+.
- With H.264+/H.265+ enabled, the parameters such as profile, I frame interval, video quality, and SVC are greyed out if the bitrate type is variable.
- 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 3 days 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:

Basic profile, Main Profile, and High Profile for coding are selectable.

I Frame Interval:

Set I Frame Interval from 1 to 400.

SVC:

Scalable Video Coding is an extension of the H.264/AVC 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

Display VCA Info By: Select the display media as Player or Video. Player means the VCA info can displayed only by Hikvision player. Video means the VCA info can displayed by any general video player.

4. Click **Save**.

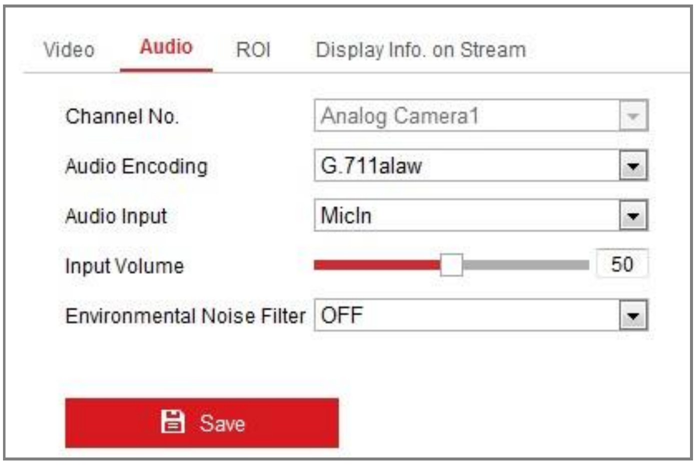
Note:

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

7.2 Set Audio

Steps:

1. Go to the Audio Settings interface: **Configuration > Video/Audio > Audio**.



Channel No. Analog Camera1

Audio Encoding G.711alaw

Audio Input MicIn

Input Volume 50

Environmental Noise Filter OFF

Figure 7-2 Audio Settings

2. Configure the following settings.

   Note: Audio settings vary according to different camera models.

   Audio Encoding: G.722.1, G.711 ulaw, G.711alaw, G.726, MP2L2 and PCM are selectable. For MP2L2, the Sampling Rate and Audio Stream Bitrate are configurable. For PCM, the Sampling Rate can be set.

   Audio Input: MicIn and LineIn are selectable for the connected microphone and pickup respectively.

   Input Volume: 0-100 adjustable.

   Environmental Noise Filter: Set it as OFF or ON. When the function is enabled, the noise in the environment can be filtered to some extent.

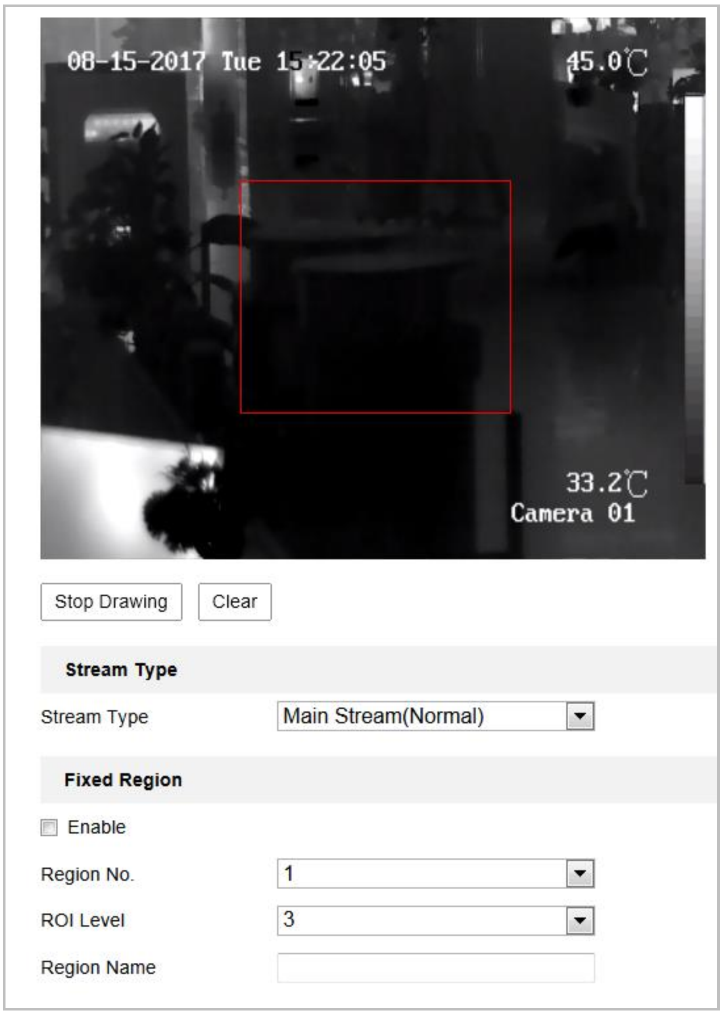
3. Click **Save**.

7.3 Set ROI Encoding

Purpose:

ROI (Region of Interest) encoding helps to discriminate the ROI and background information in video compression, which means, the technology assigns more encoding resource to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

Note: ROI function varies according to different camera models.



Stream Type

Stream Type: Main Stream(Normal)

Fixed Region

☐ Enable

Region No.: 1

ROI Level: 3

Region Name:

Figure 7-3 Region of Interest Settings

Steps:

1. Go to the ROI settings interface: **Configuration > Video/Audio > ROI**.
2. Select the channel No.
3. Select the Stream Type for ROI encoding.
4. Check the checkbox of **Enable** under Fixed Region item.
5. Set **Fixed Region** for ROI.

   (1) Select the Region No. from the drop-down list.

(2) Check the **Enable** checkbox to enable ROI function for the chosen region.

(3) Click **Drawing**. Click and drag the mouse on the view screen to draw a red rectangle as the ROI region. You can click **Clear** to cancel former drawing. Click **Stop Drawing** when you finish.

(4) Select the ROI level.

(5) Enter a region name for the chosen region.

(6) Click **Save** the save the settings of ROI settings for chosen fixed region.

(7) Repeat steps (1) to (6) to setup other fixed regions.

6. Set **Dynamic Region** for ROI.

   (1) Check the checkbox to enable **Face Tracking**.

   Note: To enable face tracking function, the face detection function should be supported and enabled.

   (2) Select the ROI level.

7. Click **Save**.

Note: ROI level means the image quality enhancing level. The larger the value is, the better the image quality would be.

7.4 Set metadata

Before you start:

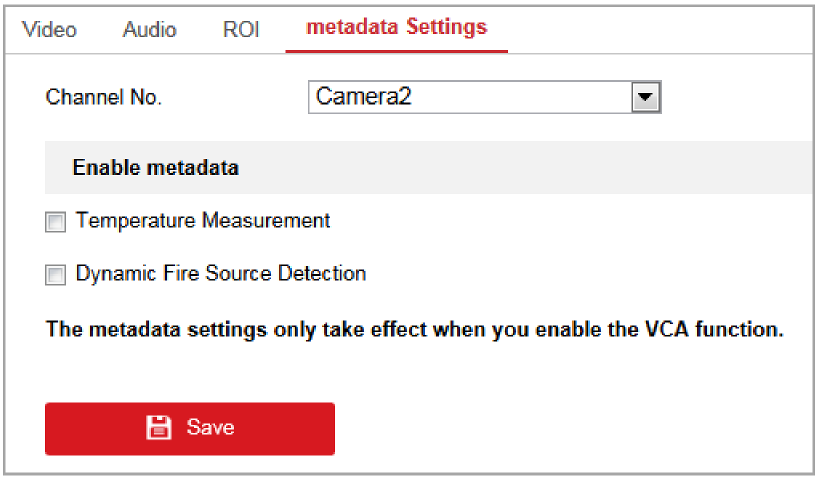
Go to **5.3.4 VCA Resource Type** to set the VCA (Video Content Analysis) resource type of your device.

Purpose:

To use the metadata for your third-party management platform, you should enable metadata first.

Steps:

1. Go to Configuration > Video/Audio > metadata Settings.
2. Check the VCA type for metadata enabling.
3. Click **Save**.



Channel No. Camera2

Enable metadata

□ Temperature Measurement

□ Dynamic Fire Source Detection

The metadata settings only take effect when you enable the VCA function.

Figure 7-4 metadata Settings

Note: The metadata settings only takes effect when you enable the VCA function. E.g, when you enabled the Temperature Measurement metadata, it only works when you configured the temperature measurement rules and saved.

Chapter 8 Image Settings

Purpose:

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

8.1 Set Display Parameters

Purpose:

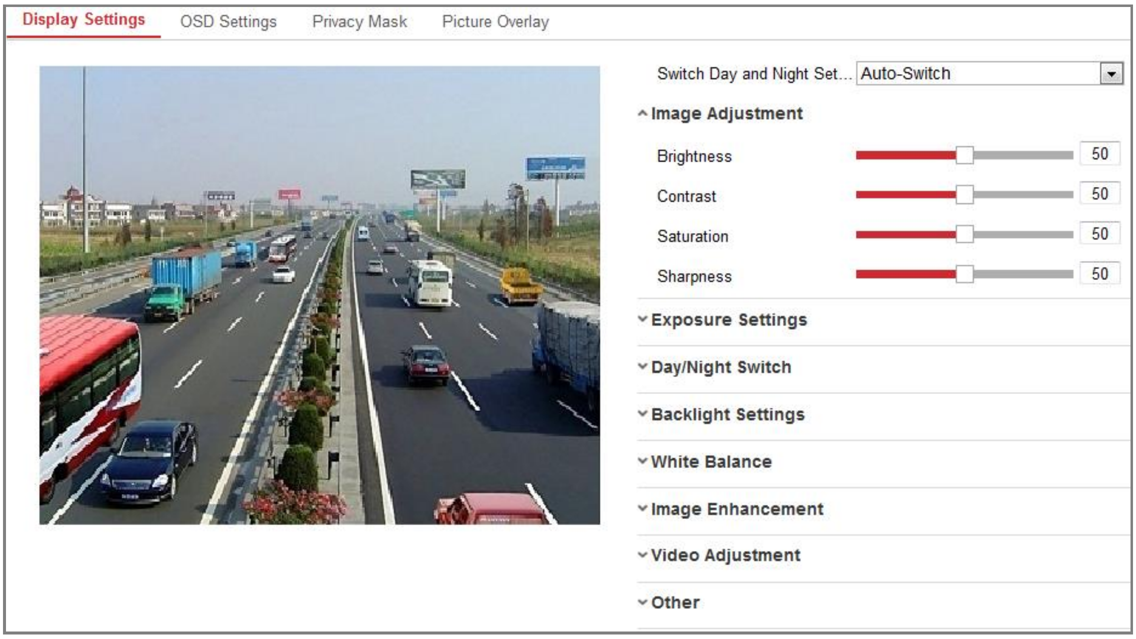
Configure the image adjustment, exposure settings, day/night switch, backlight settings, white balance, image enhancement, video adjustment, and other parameters in display settings.

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

8.1.1 Set Display Parameters (Visible Channel)

Steps:

1. Go to the Display Settings interface, **Configuration > Image > Display Settings**.



Switch Day and Night Set... Auto-Switch

Brightness 50

Contrast 50

Saturation 50

Sharpness 50

Figure 8-1 Display Settings of Day/Night Auto-Switch

2. Set the image parameters of the camera.

Note: In order to guarantee the image quality in different illumination, it provides two sets of parameters for users to configure.

- **Image Adjustment**

  Brightness describes bright of the image, which ranges from 1 to 100.

  Contrast describes the contrast of the image, which ranges from 1 to 100.

  Saturation describes the colorfulness of the image color, which ranges from 1 to 100.

  Sharpness describes the edge contrast of the image, which ranges from 1 to 100.

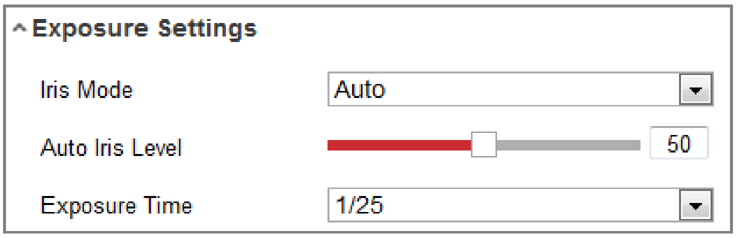
- **Exposure Settings**

  If the camera is equipped with the fixed lens, only **Manual** is selectable, and the iris mode is not configurable.

  If **Auto** is selected, you can set the auto iris level from 0 to 100.

  The **Exposure Time** refers to the electronic shutter time, which ranges from 1 to 1/100,000s. Adjust it according to the actual luminance condition.

  Gain of image can also be manually configured from 0 to 100. The bigger the value is, the brighter would the image be, and the noise would also be amplified to a larger extent.



Exposure Settings

Iris Mode: Auto

Auto Iris Level: 50

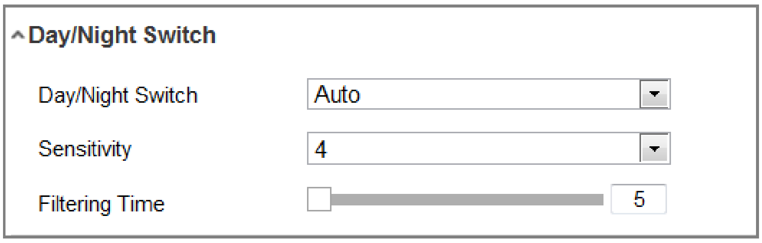
Exposure Time: 1/25

Figure 8-2 Exposure Settings

- **Day/Night Switch**

  Select the Day/Night Switch mode according to different surveillance 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

Figure 8-3 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.

Triggered by Alarm Input: The switch is triggered by alarm input. You can set the triggered mode to day or night.

Note:

This function varies depending on the models of camera.

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:

This function varies depending on the models of camera.

- **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.

Note:

This function varies depending on the models of camera.

- **White Balance**

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

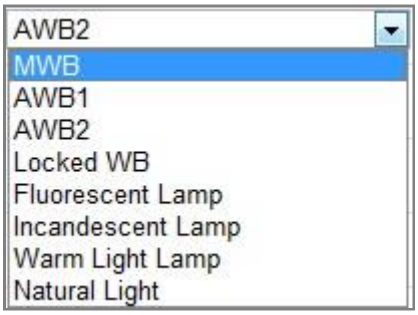


Figure 8-4 White Balance

- **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.

Defog Mode: You can enable the defog function when the environment is foggy and the image is misty. It enhances the subtle details so that the image appears clearer.

Grey Scale: You can choose the range of the grey scale as [0-255] or [16-235].

- **Video Adjustment**

  Mirror: It mirrors the image so you can see it inversed. Left/Right, Up/Down, Center, and OFF are selectable.

  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.

  Note:
  This function varies depending on the models of camera.

- **Others**

  Some camera models support CVBS, SDI, or HDMI output. Set the local output ON or OFF according to the actual device.

8.1.2 Set Display Parameters (Thermal Channel)

Purpose:

Configure the image adjustment, 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.

Steps:

1. Go to the Display Settings interface, **Configuration > Image > Display Settings**.

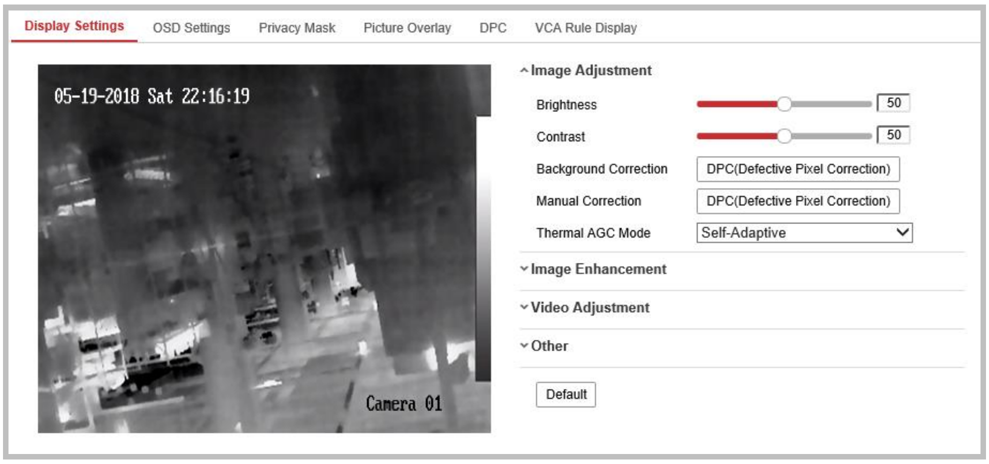


Image Adjustment

Brightness 50

Contrast 50

Background Correction: DPC(Defective Pixel Correction)

Manual Correction: DPC(Defective Pixel Correction)

Thermal AGC Mode: Self-Adaptive

Figure 8-5 Image Settings (Thermal View)

2. Set the image parameters of the camera.

Note: In order to guarantee the image quality in different illumination, it provides two sets of parameters for users to configure.

- **Image Adjustment**

  Brightness describes bright of the image, which ranges from 1~100, and the default value is 50.

  Contrast describes the contrast of the image, which ranges from 1~100, and the default value is 50.

  Background Correction: Fully cover the lens with an object (lens cover is recommended) and click the Manual Background Correction button, and then the camera adjusts the image according to the current environment.

  Manual Correction: Click the Manual Correction button and then the camera adjusts the image according to the temperature of the camera itself.

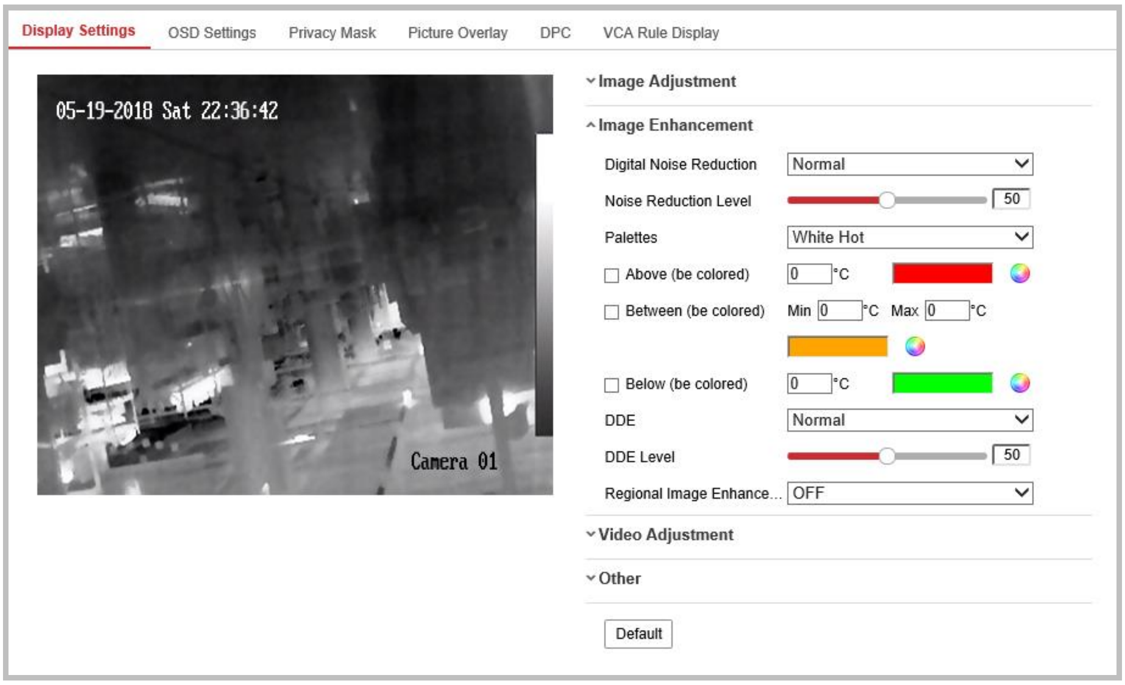
  Thermal AGC (optional): Choose the AGC mode according to different scenes to balance and improve the image quality.

  •Histogram: Choose for scene with obvious WDR and high temperature difference, can improve image contrast and enhance image. E.g. the scene contains both indoor and outdoor scenes.

  •Linear: Choose for scene with low temperature difference and the target is not obvious, can improve image contrast and enhance image. E.g. the bird in forest.

•Self-Adaptive: Choose AGC mode automatically according to current scene.

- **Image Enhancement**



˅ Image Adjustment

˄ Image Enhancement

Digital Noise Reduction	Normal
Noise Reduction Level	50
Palettes	White Hot
□ Above (be colored)	0 °C 🟥
□ Between (be colored)	Min 0 °C Max 0 °C 🟧
□ Below (be colored)	0 °C 🟩
DDE	Normal
DDE Level	50
Regional Image Enhance...	OFF

˅ Video Adjustment

˅ Other

Figure 8-6 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.

Palettes: The palettes allow you to select the desired colors. white hot, black hot, fusion 1, rainbow, fusion 2, ironbow 1, ironbow 2, sepia, color 1, color 2, ice fire, rain, red hot, and green hot are selectable.

In **White Hot** Mode, you can customize different colors for objects in different temperature section.

- Check **Above (be colored)**, and set the temperature, the objects in the scene whose temperature is above the value will be colored in red (by default).
- Check **Between (be colored)**, and set the temperature, the objects in the scene whose temperature is between the two values will be colored in sienna (by default).
- Check **Below (be colored)**, and set the temperature, the objects in the scene

whose temperature is below the value will be colored in green (by default).

DDE: The DDE (Digital Detail Enhancement) can adjust the details of the image. And you can set it to OFF or Normal mode. And DDE Level can be adjusted from 1 to 100 when in normal mode.

Brightness Sudden Change: (Only works with Behavior Analysis VCA Resource) When the brightness of target and the background is hugely different (the temperature difference of target and background is huge), the system reduces the difference for viewing.

Regional Image Enhancement (optional): You can select the desired area of image to show a red rectangle, in which the coding quality will be improved and the image will be more detailed and clear.

Select up, down, left, right, center_50%, center_70% to show a red rectangle, image will be enhanced in this area.

Select custom area to draw a red rectangle by yourself.

Select off to disable this function.

Grey Scale: You can choose the range of the grey scale as [0-255] or [16-235].

- **Video Adjustment**

  Mirror: It mirrors the image so you can see it inversed. Left/Right, Up/Down, Center, and OFF are selectable.

  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.

  Capture Mode: It’s the selectable video input mode to meet the different demands of field of view and resolution.

  Digital Zoom: Select digital zoom as OFF, 2X, 4X or 8X to display live view in original size, 2X size digital zoomed, 4X size digital zoomed, or 8X size digital zoomed.

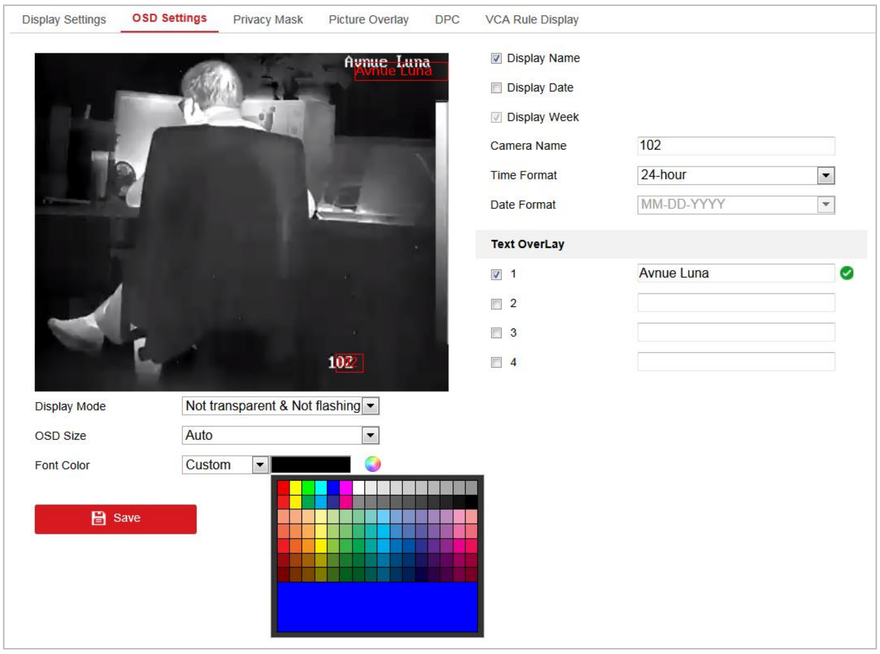
- **Other**

Local Output: Turn on or off the local output of device.

8.2 Set OSD

Purpose:

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



☑ Display Name

☐ Display Date

☑ Display Week

Camera Name	102
Time Format	24-hour
Date Format	MM-DD-YYYY

Text OverLay

☑ 1	Avnue Luna
☐ 2	
☐ 3	
☐ 4	

Display Mode	Not transparent & Not flashing
OSD Size	Auto
Font Color	Custom

Save

Figure 8-7 OSD Settings

Steps:

1. Go to the OSD Settings interface: **Configuration > Image > OSD Settings**.
2. Select the channel No.
3. Check the corresponding checkbox to select the display of camera name, date or week if required.
4. Edit the camera name in the text field of **Camera Name**.
5. Select from the drop-down list to set the time format and date format.
6. Select from the drop-down list to set the time format, date format, display mode, OSD size and OSD color.
7. 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 8 text overlays are configurable.

8. 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.

9. Click **Save**.

8.3 Set Privacy Mask

Purpose:

Privacy mask enables you to cover certain areas on the live video to prevent certain spots in the surveillance area from being live viewed and recorded.

Steps:

1. Go to the Privacy Mask Settings interface: **Configuration** > **Image** > **Privacy Mask**.
2. Select the channel No.
3. Check the checkbox of **Enable Privacy Mask** to enable this function.
4. Click **Draw Area**.

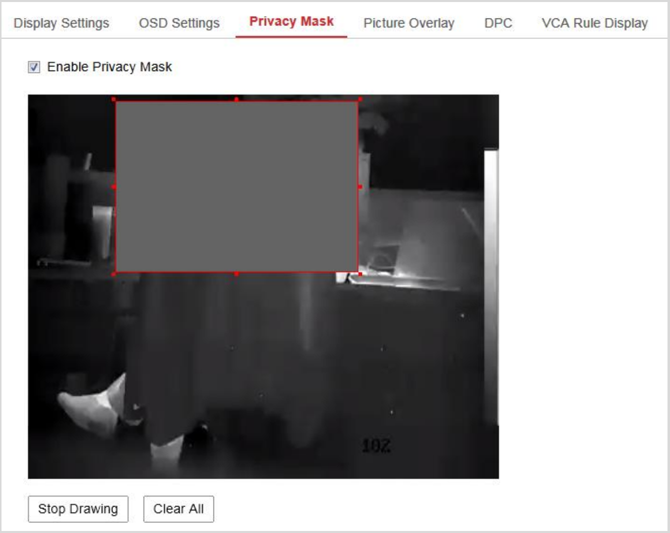


Figure 8-8 Privacy Mask Settings

5. Click and drag the mouse in the live video window to draw the mask area.

Note: You are allowed to draw up to 4 areas on the same image.

6. Click **Stop Drawing** to finish drawing or click **Clear All** to clear all of the areas you set without saving them.
7. Click Save.

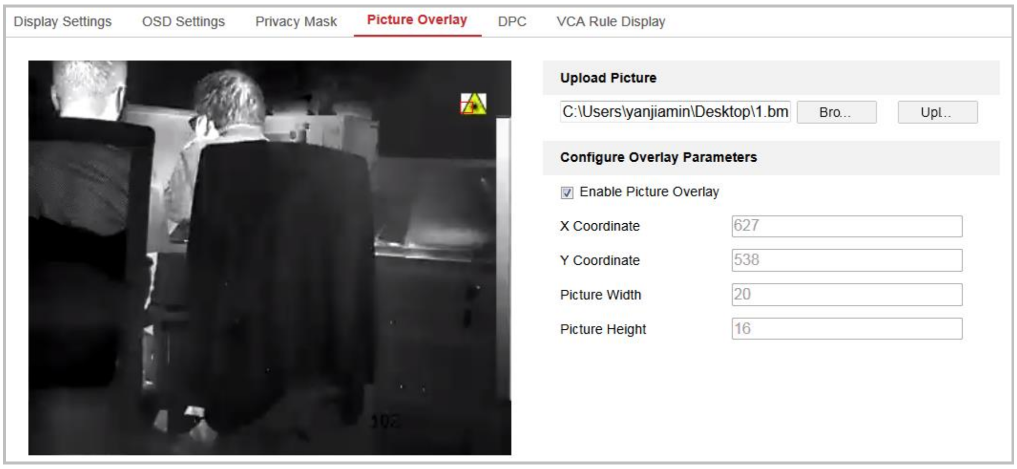
8.4 Set Picture Overlay

Purpose:

Picture overlay enables you to overlay a picture on the image. This function enables a certain enterprise or users to overlay their logo on the image.

Steps:

1. Go to the Picture Overlay Settings interface, **Configuration** > **Image** > **Picture Overlay**.



C:\Users\yanjiamin\Desktop\1.bm

☑ Enable Picture Overlay

X Coordinate	627
Y Coordinate	538
Picture Width	20
Picture Height	16

Figure 8-9 Picture Overlay

2. Select the channel No.
3. Click **Browse** to select a picture.
4. Click **Upload** to upload it.
5. Check **Enable Picture Overlay** checkbox to enable the function.
6. Set X Coordinate and Y Coordinate values adjust the picture position on the image. Adjust Picture Width and Picture Height to the desired size.
7. Click Save.

Note: The picture must be in RGB24 bmp format and the maximum picture size is 128*128.

8.5 Set DPC (Defective Pixel Correction)

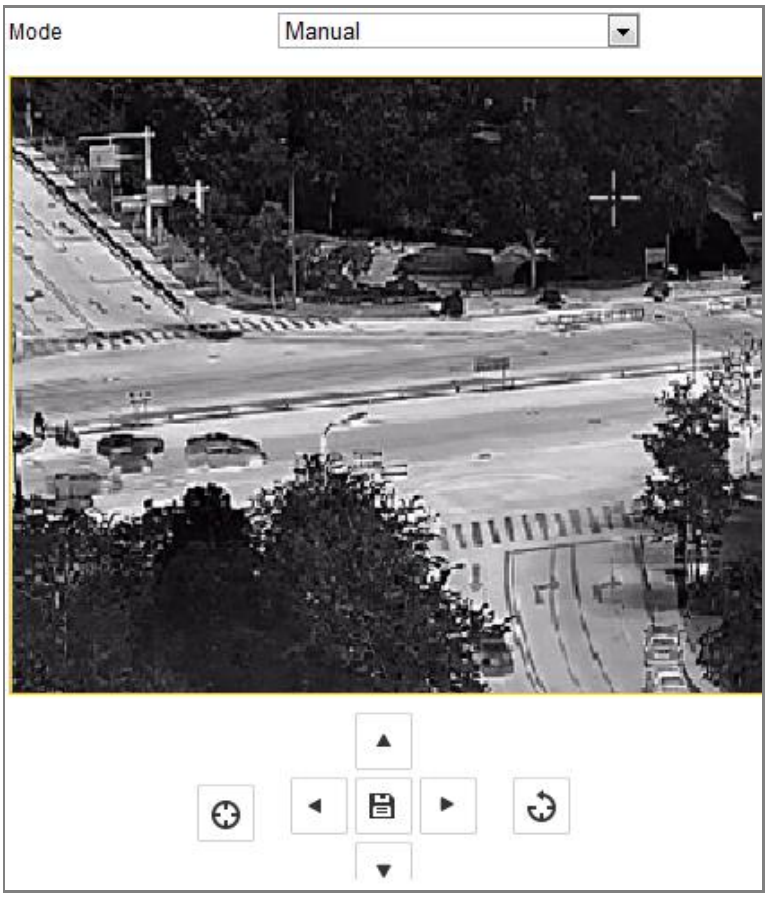
Purpose:

DPC (Defective Pixel Correction) refers to the function that the camera can correct the defective pixels on the LCD which are not performing as expected.

Note: This function is only available to certain camera models.

Steps:

1. Go to the DPC Settings interface: **Configuration > Image > DPC**



Mode: Manual

Figure 8-10 Defective Pixel Correction

2. Select the mode. The following takes manual mode as an example.
3. Click on the image to select the defective pixel. The cursor on the image will

move to the clicked position. You can click ▲◄💾►▼ to slightly adjust the cursor position.

4. Click ⊕ to start correction.

5. Click ↻ to cancel the correction, or click 💾 to save.

8.6 Picture in Picture

Purpose:
The system plays the live view of thermal channel and optical channel at the same time.

8.6.1 Overlap Mode

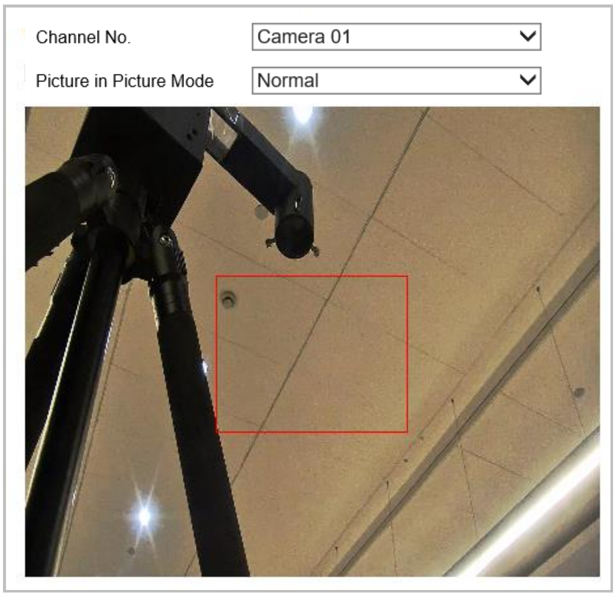
Steps:

1. Select the channel No. **Camera 01** from the list.

NOTE

Select Camera 1 and the device plays the live view of Camera 2 inside the live view of Camera 1.

2. Select **Overlap Mode** from **Picture in Picture Mode**



Channel No. Camera 01

Picture in Picture Mode Normal

Figure 8-11 Picture in Picture

3. Drag the red frame to adjust the picture in picture site.

4. Click **Save** to activate above settings.

8.6.2 Details Overlay Mode

Steps:

1. Select the channel No. **Camera 02** from the list.

2. Select **Details Overlay** from **Picture in Picture Mode**

3. Adjust the **Image Fusion Ratio** and **Border Fusion Ratio**. The setting range is 0-100.

4. Click **Save** to activate above settings.

8.7 Set VCA Rule Display

Purpose:

For temperature measurement rules, you can customize the displayed overlay information of the VCA rule (e.g. temperature measurement) which includes the font size and line and frame color.

Note: This function is only available to certain camera models.

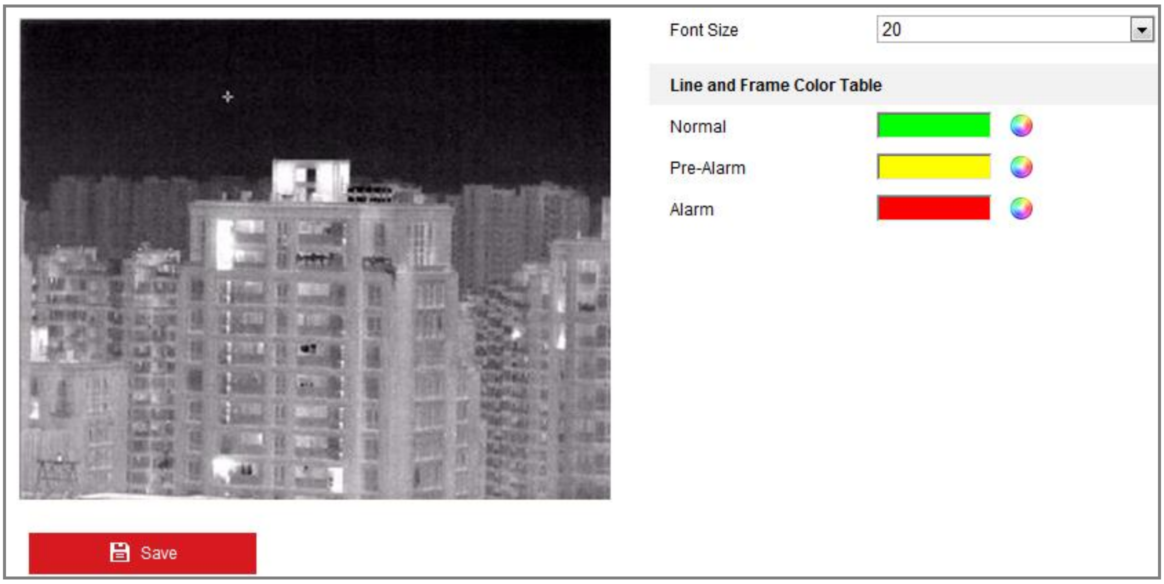
Steps:

1. Go to the VCA Rule Display Settings interface: **Configuration > Image > VCA Rule Display**

2. Select the desired font size and the line and frame color for the normal, pre-alarm and alarm.

   Note: When the VCA information is displayed by Video, the setting of font size cannot take effect.

3. Click **Save**.



Font Size: 20

Line and Frame Color Table

Normal	🟩
Pre-Alarm	🟨
Alarm	🟥

Figure 8-12 VCA Rule Display

Chapter 9 Event Settings

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

9.1 Basic Events

You can configure the basic events by following the instructions in this section, including motion detection, video tampering, alarm input, alarm output, and exception, etc. These events can trigger the linkage methods, such as Notify Surveillance Center, Send Email, Trigger Alarm Output, etc.

Note: Check the checkbox of Notify Surveillance Center if you want the alarm information to be pushed to PC or mobile client software as soon as the alarm is triggered.

9.1.1 Set Motion Detection

Purpose:

Motion detection detects the moving objects in the configured surveillance area, and a series of actions can be taken when the alarm is triggered.

In order to detect the moving objects accurately and reduce the false alarm rate, normal configuration and expert configuration are selectable for different motion detection environment.

- **Normal Configuration**

Normal configuration adopts the same set of motion detection parameters in the daytime and at night.

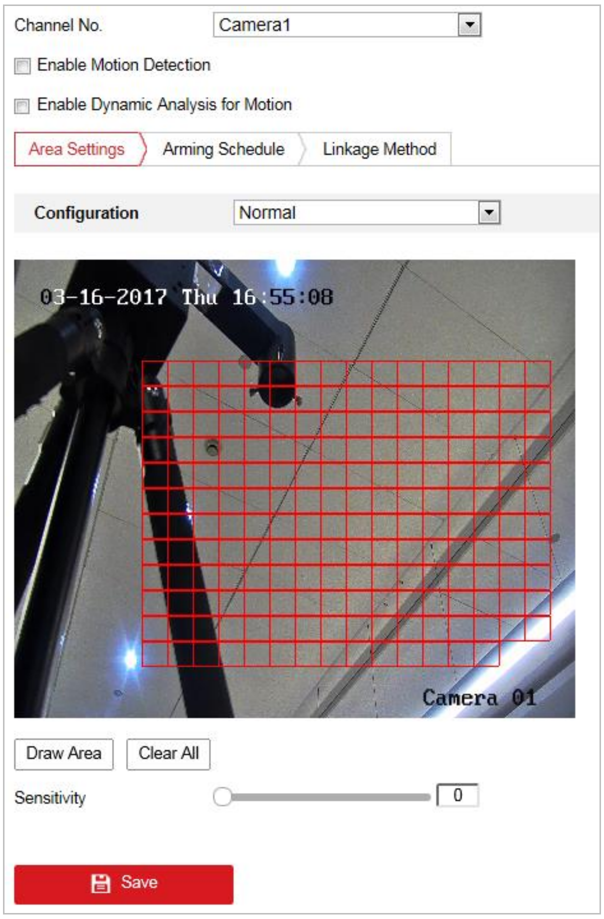
Tasks 1: Set the Motion Detection Area

Steps:

1. Go to the motion detection settings interface: **Configuration > Event > Basic Event > Motion Detection**.

2. Select the channel to set the motion detection.
3. Check the checkbox of **Enable Motion Detection**.
4. Check the checkbox of **Enable Dynamic Analysis for Motion** if you want to mark the detected objects with green rectangles.

   Note: Select Disable for rules if you don't want the detected objected displayed with the green rectangles. Select disable rules from **Configuration > Local Configuration > Live View Parameters-rules**.



Channel No. Camera1

□ Enable Motion Detection

□ Enable Dynamic Analysis for Motion

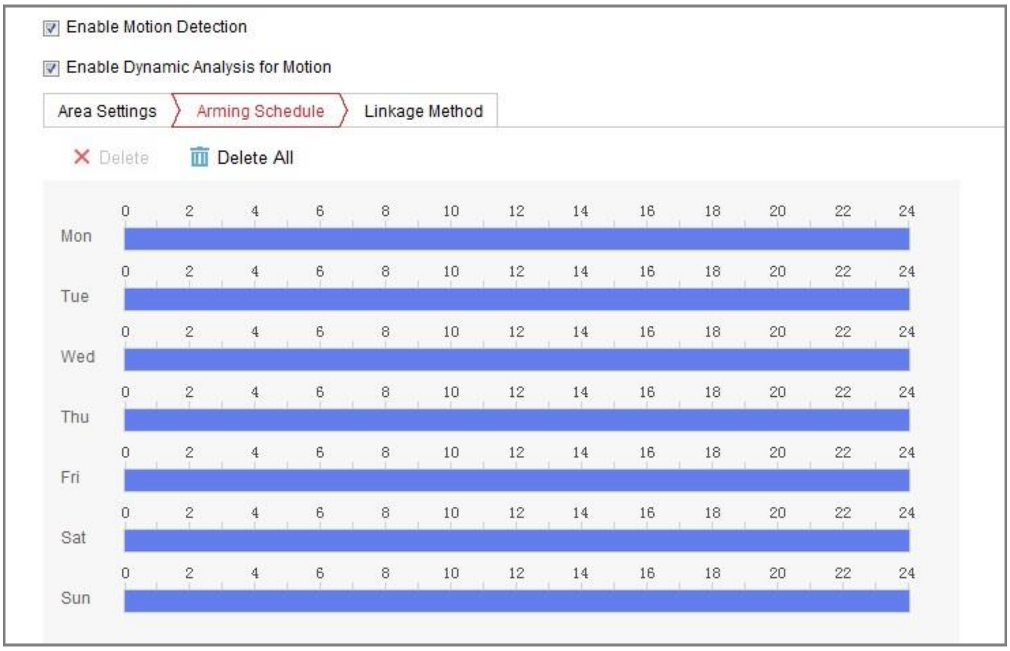
Configuration Normal

Sensitivity 0

Figure 9-1 Enable Motion Detection

5. Click **Draw Area**. Click and drag the mouse on the live video to draw a motion detection area. Click **Stop Drawing** to finish drawing one area.
6. (Optional) Click **Clear All** to clear all of the areas.
7. (Optional) Move the slider to set the sensitivity of the detection.

Task 2: Set the Arming Schedule for Motion Detection



☑ Enable Motion Detection

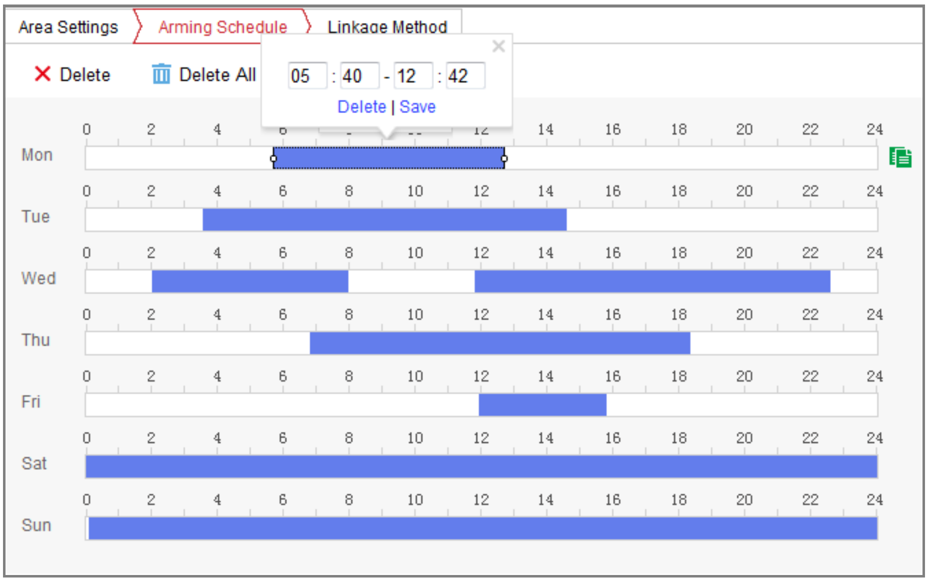
☑ Enable Dynamic Analysis for Motion

Figure 9-2 Arming Schedule

Steps:

1. Click **Arming Schedule** to edit the arming schedule.

2. Click on the time bar and drag the mouse to select the time period.



05 : 40 - 12 : 42

Figure 9-3 Arming Schedule

Figure 9-4 ***Note:*** Click on the selected time period, you can adjust the time period to the desired time by either moving the time bar or input the exact time period.

3. (Optional) Click Delete to delete the current arming schedule, or Click Save.

4. Move the mouse to the end of each day, a copy dialogue box pops up, and you

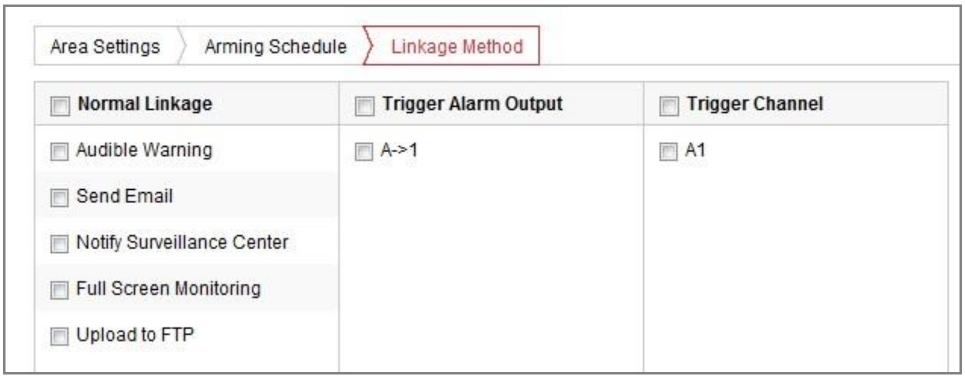
can copy the current settings to other days.

5. Click Save.

Note: The time of each period can’t be overlapped. Up to 8 periods can be configured for each day.

Task 3: Set the Linkage Method for Motion Detection

Check the checkbox to select the linkage method. Audible Warning, Send Email, Notify Surveillance Center, Upload to FTP/Memory Card/NAS, Trigger Channel and Trigger Alarm Output are selectable. You can specify the linkage method when an event occurs.



□ Normal Linkage	□ Trigger Alarm Output	□ Trigger Channel
□ Audible Warning	□ A->1	□ A1
□ Send Email		
□ Notify Surveillance Center		
□ Full Screen Monitoring		
□ Upload to FTP		

Figure 9-5 Linkage Method

Note: The linkage methods vary according to the different camera models.

- **Audible Warning**

  Trigger the audible warning locally. And it only supported by the device that have the audio output.

- **Notify Surveillance Center**

  Send an exception or alarm signal to remote management software when an event occurs.

- **Send Email**

  Send an email with alarm information to a user or users when an event occurs.

  Note: To send the Email when an event occurs, please refer to *Section 6.2.3* to complete Email setup in advance.

- **Upload to FTP/Memory Card/NAS**

  Capture the image when an alarm is triggered and upload the picture to a FTP server.

Notes:

- Set the FTP address and the remote FTP server first. Refer to *Section 6.2.2* ***Configuring FTP Settings*** for detailed information.
- Go to **Configuration > Storage > Schedule Settings> Capture > Capture Parameters** page, enable the event-triggered snapshot, and set the capture interval and capture number.
- The captured image can also be uploaded to the available SD card or network disk.

- **Trigger Channel**

  The video will be recorded when the motion is detected. You have to set the recording schedule to realize this function. Please refer to *Section 10.1* for detailed information.

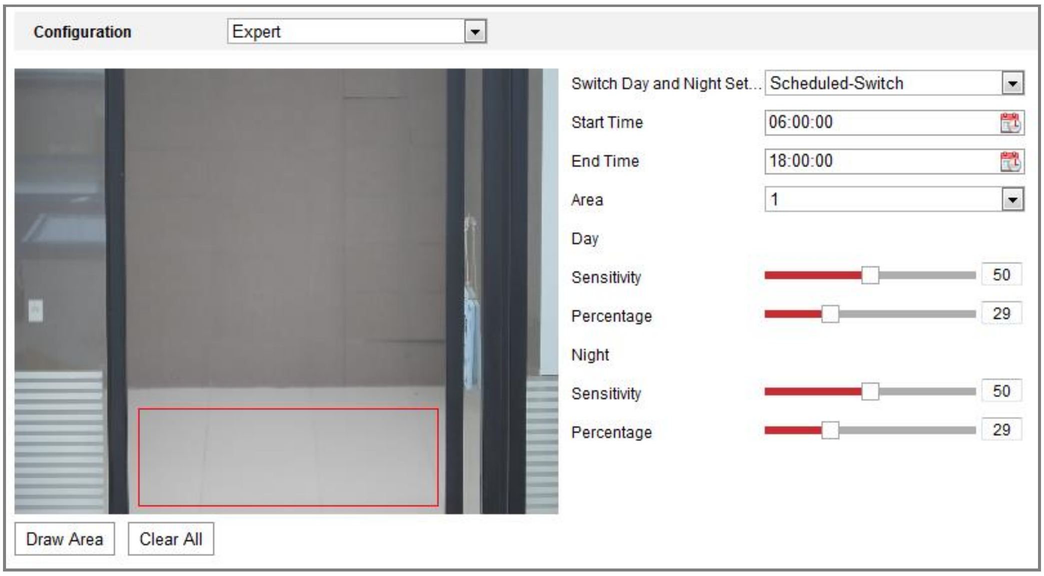
- **Trigger Alarm Output**

  Trigger one or more external alarm outputs when an event occurs.

  Note: To trigger an alarm output when an event occurs, please refer to *Section 9.1.4* ***Configuring Alarm Output*** to set the related parameters.

Expert Configuration

Expert mode is mainly used to configure the sensitivity and proportion of object on each area for different day/night switch.



Configuration: Expert

Switch Day and Night Set...: Scheduled-Switch

Start Time: 06:00:00

End Time: 18:00:00

Area: 1

Day

Sensitivity: 50

Percentage: 29

Night

Sensitivity: 50

Percentage: 29

Figure 9-6 Expert Mode of Motion Detection

- Day/Night Switch OFF

Steps:

1. Draw the detection area as in the normal configuration mode. Up to 8 areas are supported.
2. Select **OFF** for **Switch Day and Night Settings**.
3. Select the area by clicking the area No.
4. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area.
5. Set the arming schedule and linkage method as in the normal configuration mode.
6. Click Save.

- Day/Night Auto-Switch

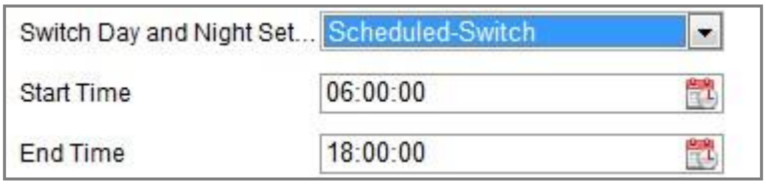
Steps:

1. Draw the detection area as in the normal configuration mode. Up to 8 areas are supported.
2. Select **Auto-Switch** for **Switch Day and Night Settings**.
3. Select the area by clicking the area No..
4. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area in the daytime.
5. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area at night.
6. Set the arming schedule and linkage method as in the normal configuration mode.
7. Click Save.

- Day/Night Scheduled-Switch

Steps:

1. Draw the detection area as in the normal configuration mode. Up to 8 areas are supported.
2. Select **Scheduled-Switch** for **Switch Day and Night Settings**.



Switch Day and Night Set... Scheduled-Switch

Start Time 06:00:00

End Time 18:00:00

Figure 9-7 Day/Night Scheduled-Switch

3. Select the start time and the end time for the switch timing.
4. Select the area by clicking the area No..
5. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area in the daytime.
6. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area at night.
7. Set the arming schedule and linkage method as in the normal configuration mode.
8. Click Save.

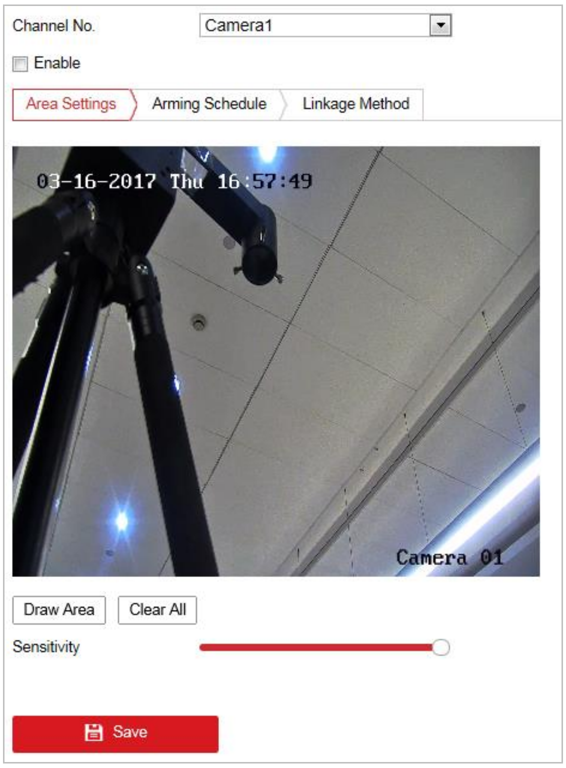
9.1.2 Set Video Tampering Alarm

Purpose:

You can configure the camera to trigger the alarm when the lens is covered and take certain alarm response actions.

Steps:

1. Go to the video tampering Settings interface, **Configuration > Event > Basic Event > Video Tampering**.
2. Select the channel to set the video tampering alarm.



Channel No. Camera1

□ Enable

Sensitivity

Figure 9-8 Video Tampering Alarm

3. Check **Enable Video Tampering** checkbox to enable the video tampering detection.

4. Set the video tampering area. Refer to ***Task 1: Set the Motion Detection Area*** in *Section 9.1.1.*

5. Click **Edit** to edit the arming schedule for video tampering. The arming schedule configuration is the same as the setting of the arming schedule for motion detection. Refer to ***Task 2: Set the Arming Schedule for Motion Detection*** in *Section 9.1.1.*

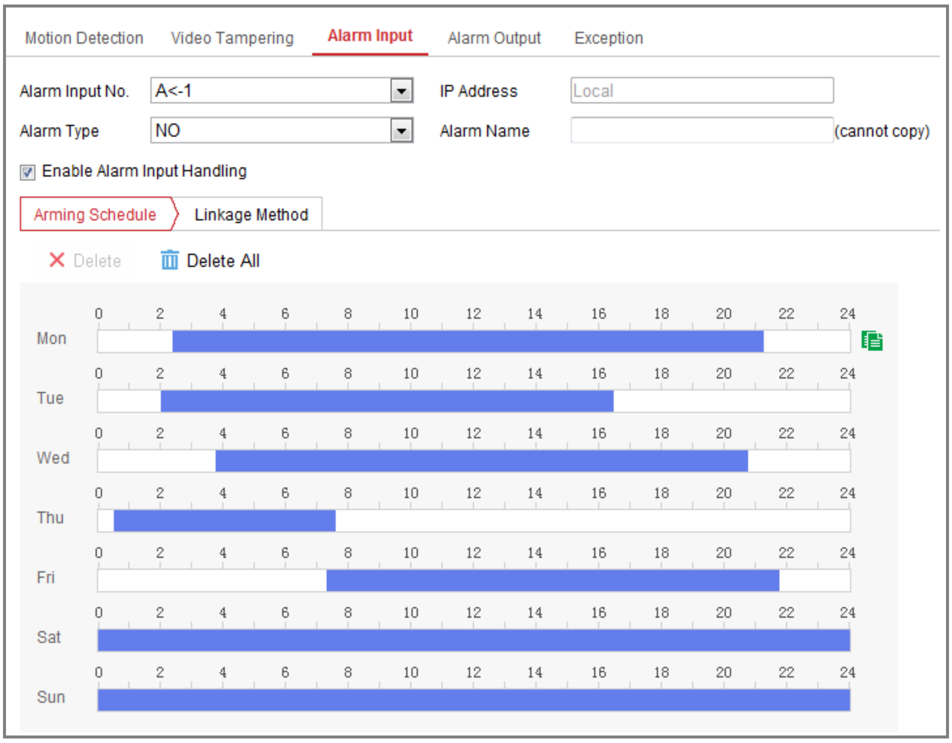
6. Check the checkbox to select the linkage method taken for the video tampering. Audible warning, notify surveillance center, send email and trigger alarm output are selectable. Please refer to ***Task 3: Set the Linkage Method for Motion Detection*** in *Section 9.1.1.*

7. Click Save.

9.1.3 Set Alarm Input

Steps:

1. Go to the Alarm Input Settings interface: **Configuration > Event > Basic Event > Alarm Input**.
2. Choose the alarm input No. and the Alarm Type. The alarm type can be NO (Normally Open) and NC (Normally Closed). Edit the name to set a name for the alarm input (optional).



Alarm Input No. A<-1

Alarm Type NO

IP Address Local

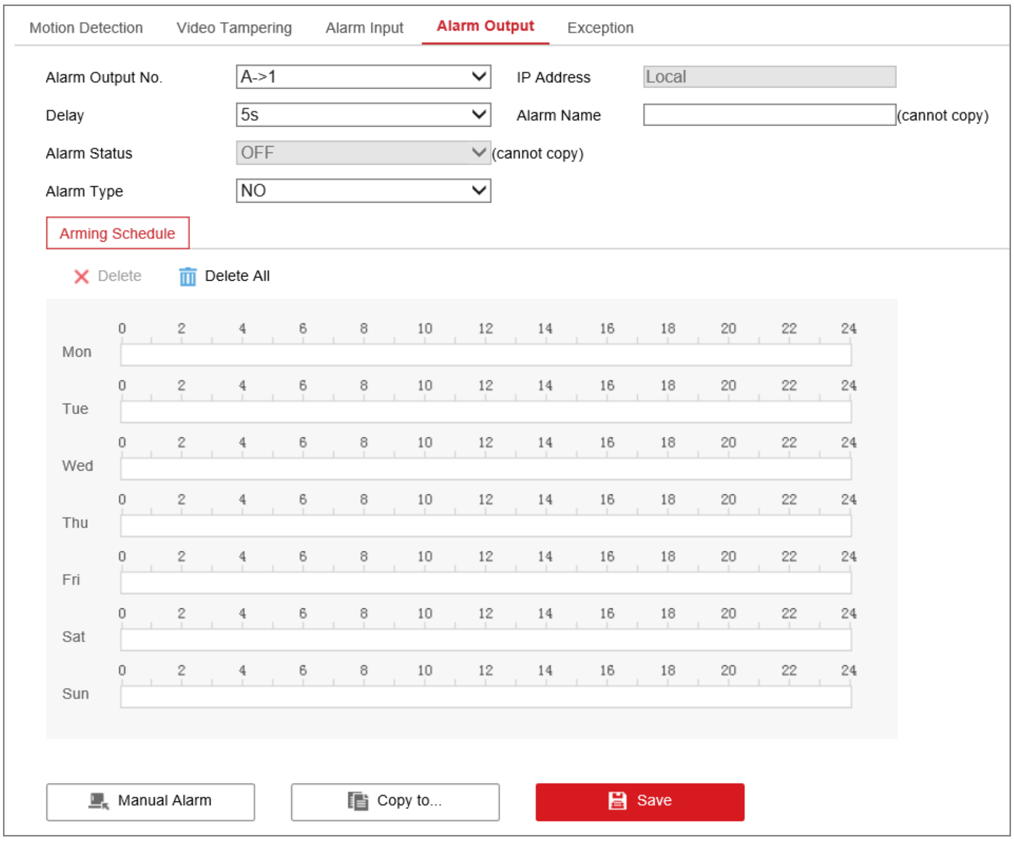
Alarm Name (cannot copy)

☑ Enable Alarm Input Handling

Figure 9-9 Alarm Input Settings

3. Click **Arming Schedule** to set the arming schedule for the alarm input. Refer to ***Task 2: Set the Arming Schedule for Motion Detection*** in *Section 10.1.1.*
4. Click **Linkage Method** and check the checkbox to select the linkage method taken for the alarm input. Refer to ***Task 3: Set the Linkage Method for Motion Detection*** in *Section 9.1.1.*
5. You can copy your settings to other alarm inputs.
6. Click Save.

9.1.4 Set Alarm Output



Alarm Output No. A->1

IP Address Local

Delay 5s

Alarm Name (cannot copy)

Alarm Status OFF (cannot copy)

Alarm Type NO

Figure 9-10 Alarm Output Settings

Steps:

1. Go to the Alarm Output Settings interface: **Configuration> Event > Basic Event > Alarm Output**.
2. Select one alarm output channel in the **Alarm Output** drop-down list. You can also set a name for the alarm output (optional).
3. The Delay time can be set to 5sec, 10sec, 30sec, 1min, 2min, 5min, 10min or Manual. The delay time refers to the time duration that the alarm output remains in effect after alarm occurs.
4. Select the Alarm Type. The alarm type can be **NO** (Normally Open) and **NC** (Normally Closed)
5. Click **Arming Schedule**. The time schedule configuration is the same as the settings of the arming schedule for motion detection Refer to ***Task 2: Set the Arming Schedule for Motion Detection*** in *Section 9.1.1.*

6. You can copy the settings to other alarm outputs.

7. Click Save.

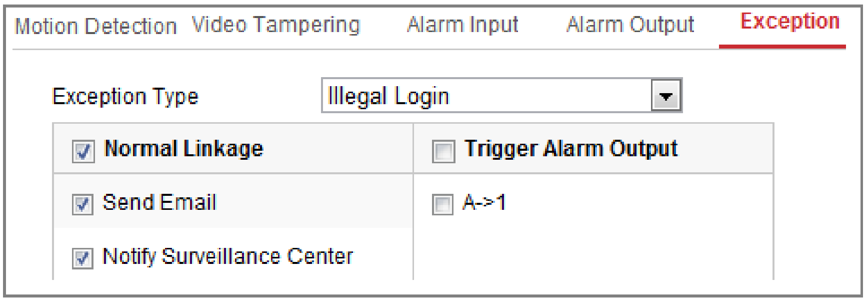
9.1.5 Set Exception

The exception type can be HDD full, HDD error, network disconnected, IP address conflicted and illegal login to the cameras.

Steps:

1. Go to the Exception Settings interface: **Configuration > Event > Basic Event > Exception**.

2. Check the checkbox to set the actions taken for the Exception alarm. Refer to ***Task 3: Set the Linkage Method for Motion Detection*** in *Section 9.1.1.*



Exception Type: Illegal Login

☑ **Normal Linkage**

☑ Send Email

☑ Notify Surveillance Center

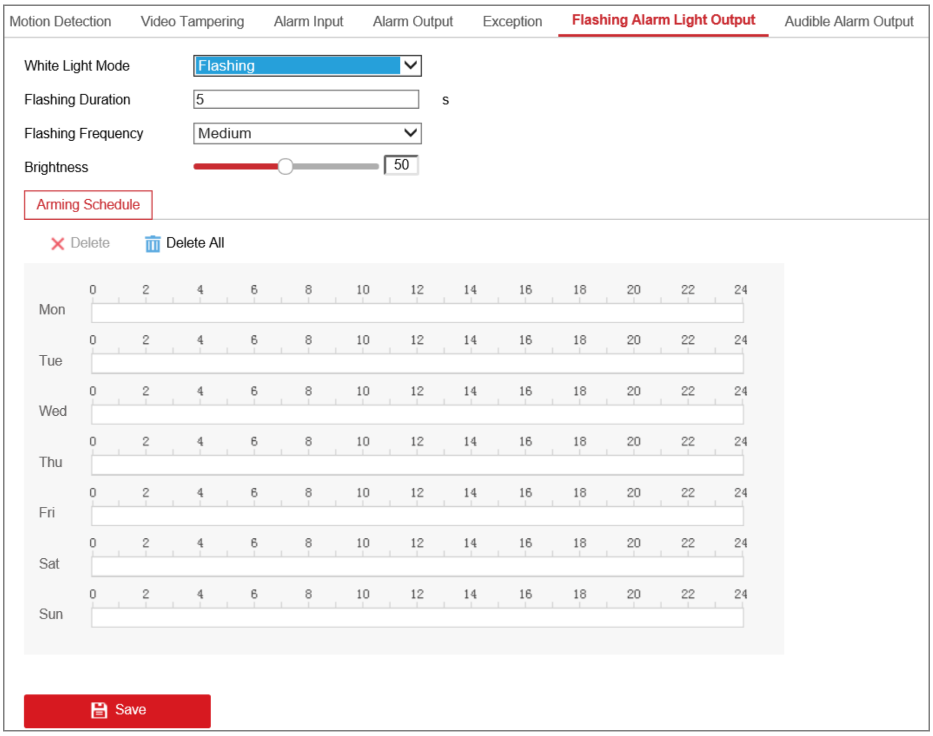
☐ **Trigger Alarm Output**

☐ A->1

Figure 9-11 Exception Settings

3. Click **Save**.

9.1.6 Set Flashing Alarm Light Output



White Light Mode: Flashing

Flashing Duration: 5 s

Flashing Frequency: Medium

Brightness: 50

Figure 9-12 Flashing Alarm Light Output Settings

Steps:

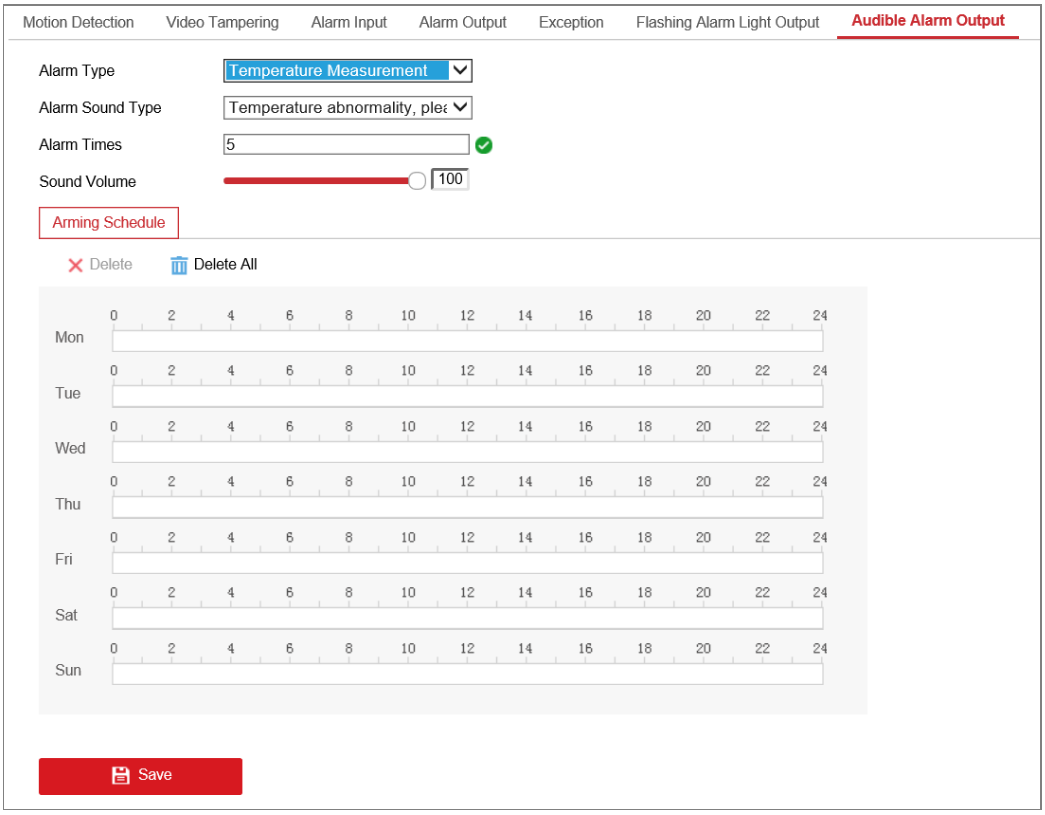
1. Go to the **Flashing Alarm Light Output** settings interface: **Configuration > Event > Basic Event > Flashing Alarm Light Output**.

- **White Light Mode: Solid** and **Flashing** are selectable. In flashing mode, you can set the flashing frequency.
- **Flashing Duration**: The time period the flashing lasts when one alarm happens.
- **Flashing Frequency**: The flashing speed of the light. High, Medium, and Low are selectable.
- **Brightness**: The brightness of the light.

2. Set the flashing duration, flashing frequency and brightness.
3. Edit the arming schedule.
4. Click **Save**.

Note: Only certain camera models support the function.

9.1.7 Set Audible Alarm Output



Alarm Type: Temperature Measurement

Alarm Sound Type: Temperature abnormality, plea

Alarm Times: 5

Sound Volume: 100

Figure 9-13 Audible Alarm Output Settings

Steps:

1. Go to the **Audible Alarm Output** settings interface: **Configuration > Event > Basic Event > Audible Alarm Output**.

- Alarm Sound Type: The content of audible warning.
- Alarm Times: The repeating times of the warning.

2. Select the alarm type.
3. Select the alarm sound type.
4. Set the alarm times and sound volume.
5. Edit the arming schedule.
6. Click **Save**.

Note: Only certain camera models support the function

9.2 Smart Events

You can configure the smart events by following the instructions in this section, including audio exception detection, defocus detection, scene change detection, intrusion detection, and line crossing detection, etc. These events can trigger the linkage methods, such as Notify Surveillance Center, Send Email, Trigger Alarm Output, etc.

9.2.1 Set Audio Exception Detection

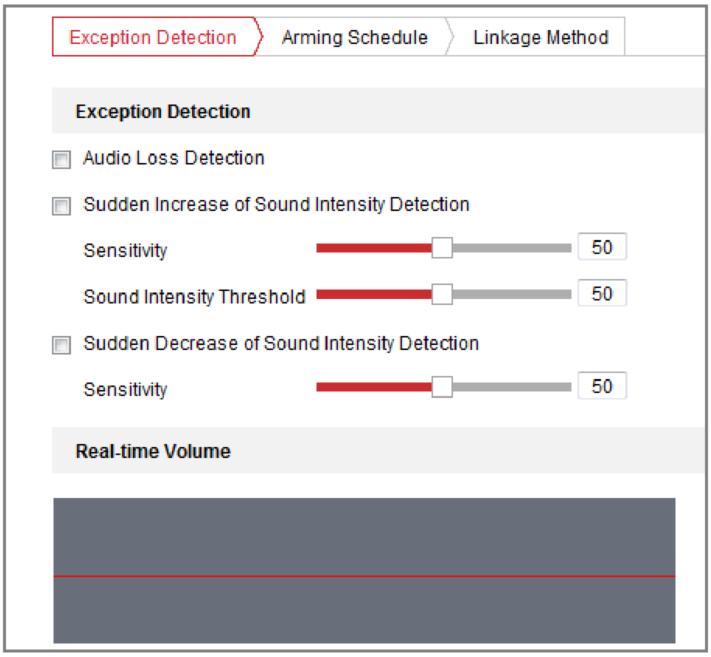
Purpose:

Audio exception detection function detects the abnormal sounds in the surveillance scene, such as the sudden increase/decrease of the sound intensity, and some certain actions can be taken when the alarm is triggered.

Note: Audio exception detection function varies according to different camera models.

Steps:

1. Go to the Audio Exception Detection settings interface, **Configuration > Event > Smart Event > Audio Exception Detection**.



□ Audio Loss Detection

□ Sudden Increase of Sound Intensity Detection

Sensitivity 50

Sound Intensity Threshold 50

□ Sudden Decrease of Sound Intensity Detection

Sensitivity 50

Figure 9-14 Audio Exception Detection

2. Check the checkbox of **Audio Loss Exception** to enable the audio loss detection function.
3. Check the checkbox of **Sudden Increase of Sound Intensity Detection** to detect the sound steep rise in the surveillance scene. You can set the detection sensitivity and threshold for sound steep rise.
4. Check the checkbox of **Sudden Decrease of Sound Intensity Detection** to detect the sound steep drop in the surveillance scene. You can set the detection sensitivity and threshold for sound steep drop.

   Notes:

   - Sensitivity: Range [1-100], the smaller the value is, the more severe the change should be to trigger the detection.
   - Sound Intensity Threshold: Range [1-100], it can filter the sound in the environment, the louder the environment sound, the higher the value should be. You can adjust it according to the real environment.
   - You can view the real-time volume of the sound on the interface.
5. Click **Arming Schedule** to set the arming schedule. Refer to ***Task 2 Set the Arming Schedule for Motion Detection*** in *Section 9.1.1* for detailed steps.
6. Click **Linkage Method** and select the linkage methods for audio exception, including Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Channel for recording and Trigger Alarm Output.
7. Click Save.

9.2.2 Set Dynamic Fire Source Detection

Purpose:

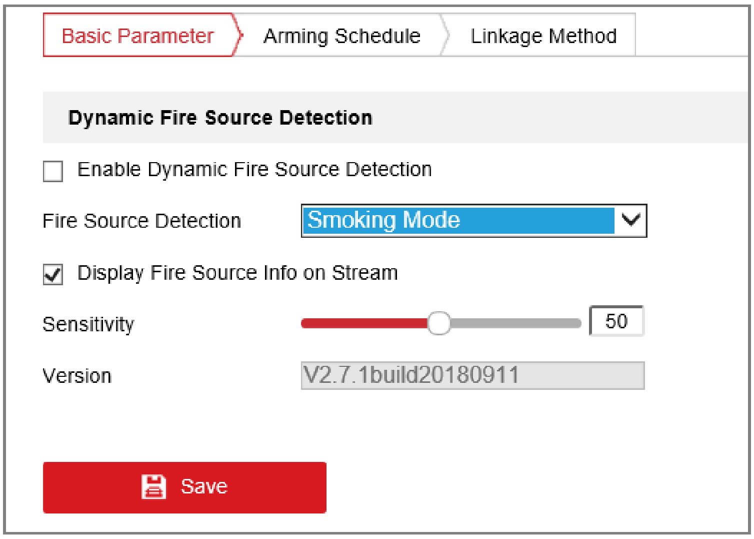
When you enable this function and fire source is detected, the alarm actions will be triggered. You can set different detection mode, fire source zoom mode, and so on.

Steps:

1. Go to **Configuration** > **System** > **Maintenance** > **VCA Resource Type** to select

Dynamic Fire Source Detection as VCA Resource Type.

2. Go to **Configuration** > **Event** > **Smart Event** > **Dynamic Fire Source Detection**.



Dynamic Fire Source Detection

□ Enable Dynamic Fire Source Detection

Fire Source Detection: Smoking Mode

☑ Display Fire Source Info on Stream

Sensitivity: 50

Version: V2.7.1build20180911

Figure 9-15 Fire Source Detection

3. Check the checkbox of **Enable Dynamic Fire Source Detection** to enable the fire detection function.
4. Select detection mode from the dropdown list. **Smoking Mode** and **Dynamic Fire** are selectable. Smoking mode is used to detect smoking behavior and the dynamic fire detection mode is used to detect the fire source.
5. Check the checkbox of **Display Fire Source Frame on Stream** to display a red frame around the fire source on stream when fire occurs. (Optional)
6. You can drag the slider to adjust the sensitivity degree of dynamic fire source detection from 1 to 10. The bigger the number is, the more sensitive the detecting would be.
7. Click **Arming Schedule** to set the arming schedule for the fire detection. Refer to ***Task 2: Set the Arming Schedule for Motion Detection*** in *Section 9.1.1.*
8. Click **Linkage Method** and check the checkbox to select the linkage method taken for the fire detection. Refer to ***Task 3: Set the Linkage Method for Motion Detection*** in *Section 9.1.1* for detailed steps.
9. Click Save.

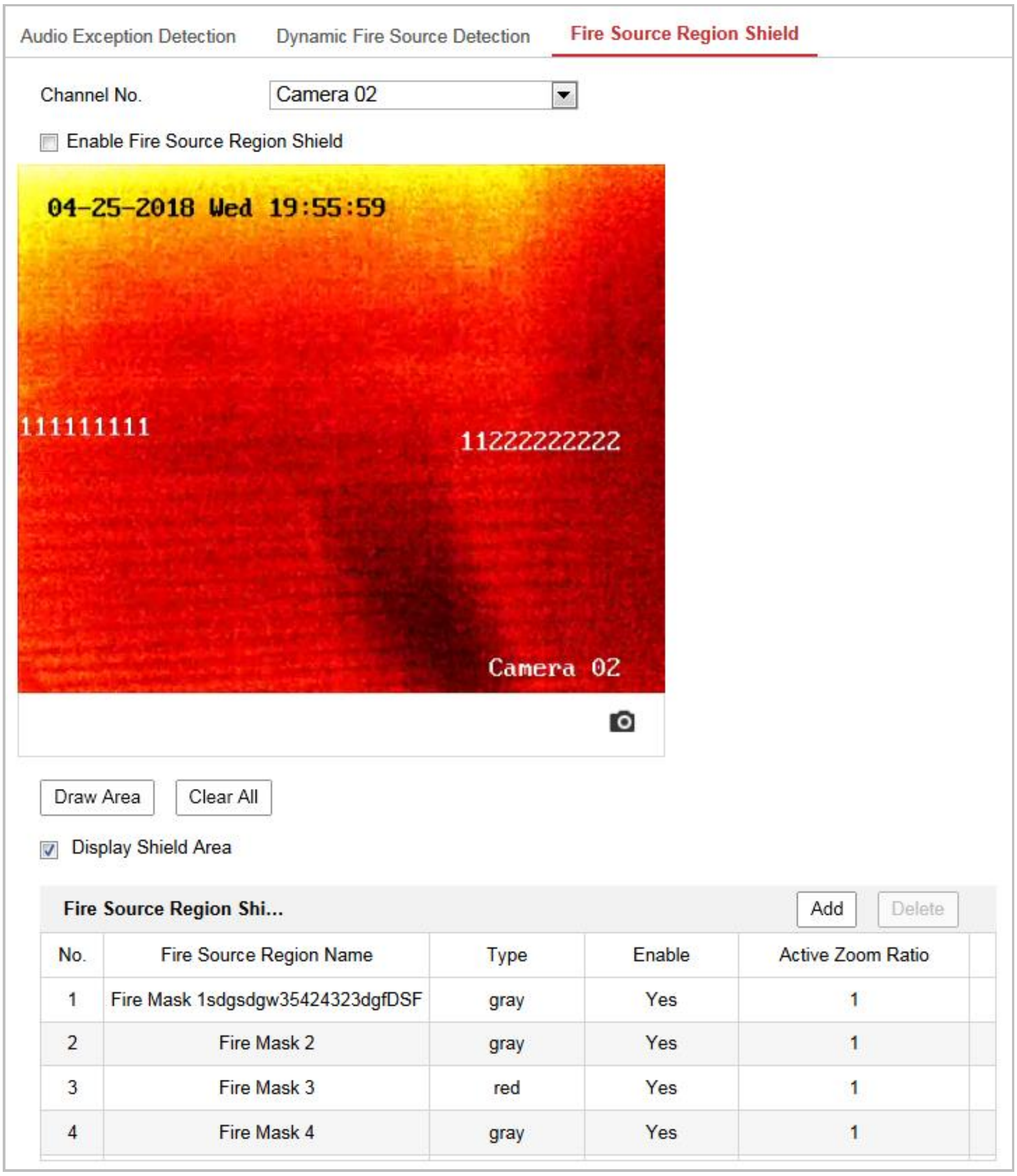
9.2.3 Set Fire Source Detection Shield

Purpose:

Fire Source Shield enables you to shield certain areas from being detected in fire source detection.

Steps:

1. Enter **Configuration** > **Event** > **Smart Event** > **Fire Source Detection Shield**.
2. Check the checkbox to enable the Fire Source Region Shield.
3. Click **Draw Area**; click and drag the mouse in the live video window to draw the area.



Audio Exception Detection
Dynamic Fire Source Detection
Fire Source Region Shield
04-25-2018 Wed 19:55:59
111111111
11222222222
Camera 02
Draw Area
Clear All
Add
Delete

Channel No. Camera 02

□ Enable Fire Source Region Shield

☑ Display Shield Area

Fire Source Region Shi...

No.	Fire Source Region Name	Type	Enable	Active Zoom Ratio
1	Fire Mask 1sdgsdgw35424323dgfDSF	gray	Yes	1
2	Fire Mask 2	gray	Yes	1
3	Fire Mask 3	red	Yes	1
4	Fire Mask 4	gray	Yes	1

Figure 9-16 Fire Source Detection Shield

4. You can drag the corners of the red rectangle area to change its shape and size.
5. Click **Stop Drawing** to finish drawing or click **Clear All** to clear all of the areas you set without saving them.
6. Set the value of Active Zoom Ratio on your demand, and then the shield will only appear when the zoom ratio is greater than the predefined value.
7. Click **Add** to save the fire source detection shield, and it will be listed in the Fire Source Detection Shield List area; you can select a region and click **Delete** to delete it from the list; you can also define the color of the regions.

8. Check the checkbox of **Enable Fire Source Detection Shield** to enable this function.

Note: You are allowed to draw up to 24 areas on the same image.

9.3 VCA Configuration

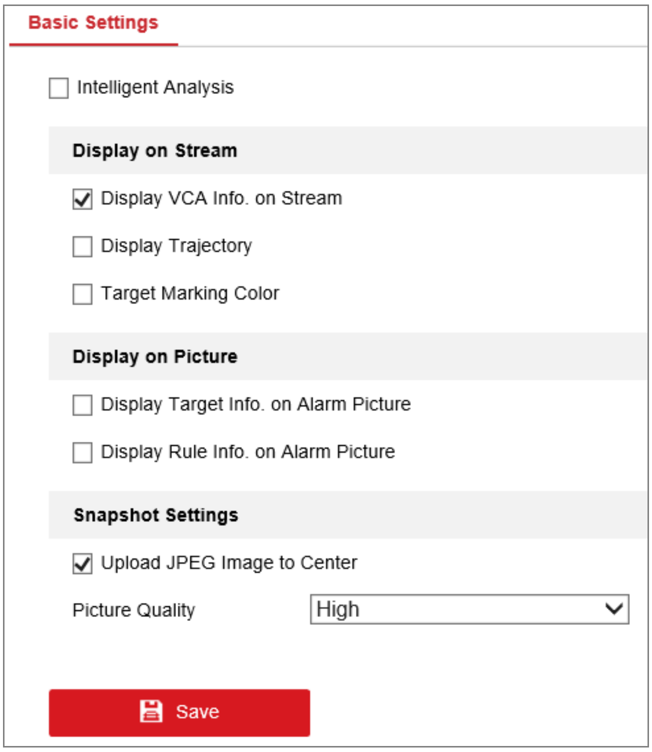
9.3.1 Basic Settings

Purpose:

You can enable to display the VCA information on stream or target information on alarm picture and set the snapshot quality and resolution.

Steps:

1. Enter **Configuration** > **VCA** > **Basic Settings.**
2. Check the checkbox to enable the Intelligent Analysis. And you can view the current version for the behavior analysis.
3. Check the desired checkbox of display settings and select the snapshot quality and resolution.



Basic Settings

□ Intelligent Analysis

Display on Stream

☑ Display VCA Info. on Stream

□ Display Trajectory

□ Target Marking Color

Display on Picture

□ Display Target Info. on Alarm Picture

□ Display Rule Info. on Alarm Picture

Snapshot Settings

☑ Upload JPEG Image to Center

Picture Quality: High

Figure 9-17 Basic Settings

Display information includes the display on picture and display on stream.

Display VCA info. on Stream: The green frames will be displayed on the target if in a live view or playback.

Display Trajectory: Check to enable the trajectory display. The target's moving trajectory will be shown in the live view.

Target Marking Color: There will be a frame on the target. Enable this function to show the frame color of human as orange, show the frame color of vehicle as purple.

Trajectory Display Duration: Duration is adjustable when you enable the trajectory display: 5s, 10s, 20s, 30s are selectable. The system only shows the trajectory of selected duration.

Display Target info. on Alarm Picture: There will be a frame on the target on the uploaded alarm picture if the checkbox is checked.

Display Rule info. on Alarm Picture: The captured target and the configured area will be framed on the alarm picture.

Note: Make sure the rules are enabled in your local settings. Go to **Configuration** > **Local Configuration** > **Rules** to enable it.

Snapshot Setting: You can set the quality and resolution for the captured picture.

Upload JPEG Image to Center: Check the checkbox to upload the captured image to the surveillance center when a VCA alarm occurs.

Picture Quality: High, Medium and Low are selectable.

Picture Resolution: CIF, 4CIF, 720P, and 1080P are selectable.

9.3.2 Set Camera Calibration

Perform the following steps to three-dimensionally measure and quantize the image from the camera, and then calculate the size of every target. The VCA detection will be more accurate if the camera calibration is configured.

- ***TASK 1: Auto Calibration***

Steps:

1. Enter **Configuration** > **VCA** > **Camera Calibration**.

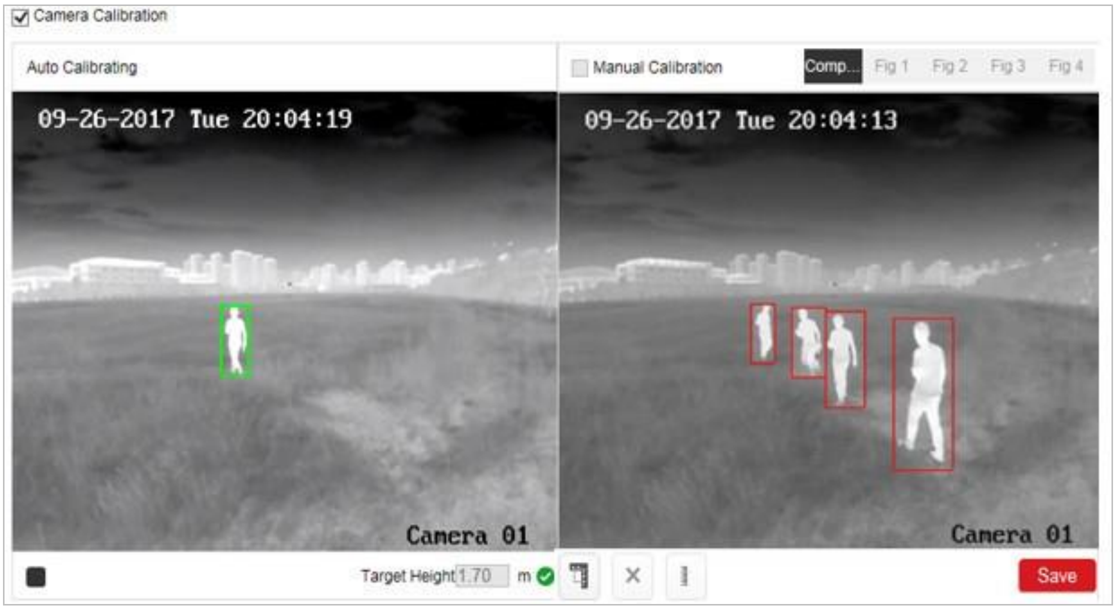
2. Make sure only one person appears in the live view, and input the person's height in the **Target Height** text field.

3. Click ▶ to start auto calibration.

   Notes:

   - Make sure there is no moving objects in the view except for the person.
   - The auto calibration starts when the person is totally seen in the camera's view, and ends when the person is in the endpoint (The endpoint-to-camera distance(m) equals 4 times the lens focal length(mm)). E.g, for 7mm lens, the recommended endpoint is 28m (7*4).
   - Once auto calibration started, the person should start to walk in a zigzag course.
   - Make sure the walking route covers the left, middle, right of image.
   - The auto calibration duration should be no shorter than 10s, and no longer than 10min.Walking in a double Z zigzag is theoretically enough.
   - For leave/tree interference in the live view, shield settings is recommended.

4. When the person exits, Click ■ to stop auto calibration.



☑ Camera Calibration

Auto Calibrating

□ Manual Calibration

Target Height 1.70 m

Figure 9-18 Auto Calibration

Verification:

i. Click the **Enable Verification** button.

Notes:

- Verify not only person, but also other objects appeared in the view. Such as car, street lamp, etc.
- The verifying result value is only the height of the line. The horizontal width is not measured.

ii. Click the **Vertical Verify** button, and drag a vertical line in the view.

iii. Click the **Calibration** + − × ÷ button to calculate the length.

iv. Compare the calculated line length to the actual length to verify the calibration settings.

Note:

If the Auto Calibration failed, or the verified result turns bad, click Fig 1 to Fig 4 to examine whether they are valid person/object in the figures or not. If so, refer to the Manual Calibration.

- ***TASK 2: Manual Calibration***

Steps:

1. Check **Manual Calibration**.
2. Select Fig 1.

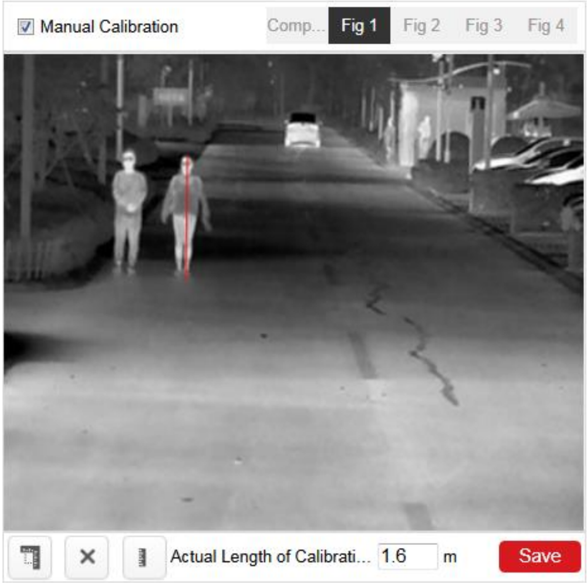


Figure 9-19 Manual Calibration (1)

3. Click ▮ and drag the vertical line until it fits the target.
4. Input the actual length of the calibration line.
5. (Optional) you can click × to delete the calibration line.
6. When the √ appears, select Fig 2 to 4 and repeat step 3.

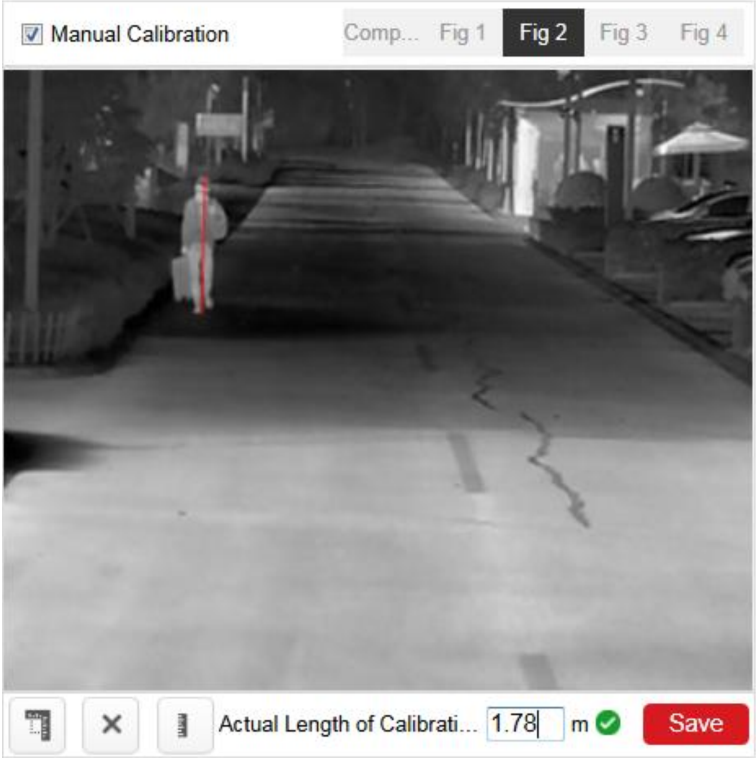


Figure 9-20 Manual Calibration (2)

7. Click **Save**.

Notes:

- Separate 4 vertical lines at the left, middle and right of the image respectively.
- Separate 4 vertical lines in the optical-axis direction at the close site, middle and far site respectively.
- In the four figures, the calibrated object doesn't need to be the same. Select a proper object in each figure.
- If manual calibration's result is incorrect, reset the target to recalibrate.

Verification:

i. Click the **Enable Verification** button.

Notes:

- Verify not only person, but also other objects appeared in the view. Such as car, street lamp, etc.
- The verifying result value is only the height of the line. The horizontal width is not measured.

ii. Click the **Vertical Verify** button, and drag a vertical line in the view.

iii. Click the **Calibration** + − × ÷ button to calculate the length.

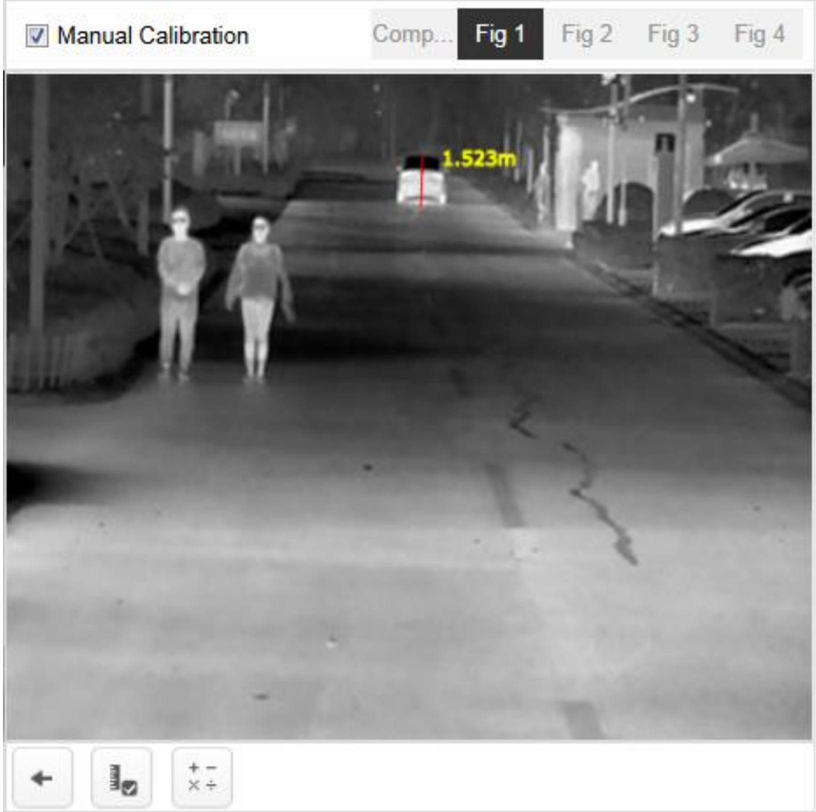


Figure 9-21 Verification

iv. Compare the calculated line length to the actual length to verify the calibration settings.

9.3.3 Set Shield Region

The shield region allows you to set the specific region in which the behavior analysis will not function. Up to 4 shield regions are supported.

Steps:

1. Enter **Configuration** > **VCA** > **Shield Region**.
2. Click **Shield Region**.
3. Click the hexagons sign ⬡ to draw shield area by left click end-points in the live view window, and right click to finish the area drawing.

Notes:

- Polygon area with up to 10 sides is supported.
- Click ✕ to delete the drawn areas.
- If live view is stopped, there is no way to draw the shield regions.

4. Click Save.

9.3.4 Set Rule

The behavior analysis supports a series of behaviors, including line crossing detection, intrusion, region entrance, and region exiting, etc.

Note: Please refer to each chapter for detailed information of each behavior.

Steps:

1. Go to **Configuration** > **VCA** > **Rule**.
2. Click **Rule**.
3. Check the checkbox of the single rule to enable the rule for behavior analysis.
4. Select the rule type, set the filter type, and then draw the line/area on the live video for the single rule.

   Note: Click 📋 to copy the same settings to other rules.

   Example:

   i. Select the rule type of **Line Crossing**.
   ii. Set the filter type to **Actual Size** when the camera calibration is configured.
   iii. Input the width and height of the Max. Size and Min. Size. Only the target whose size is between the Max. Size and Min. Size value will trigger the alarm.
   iv. Set the **Detection Target** as *Human*, *Vehicle*, or *Human & Vehicle*. Only the target of selected type will trigger the alarm.

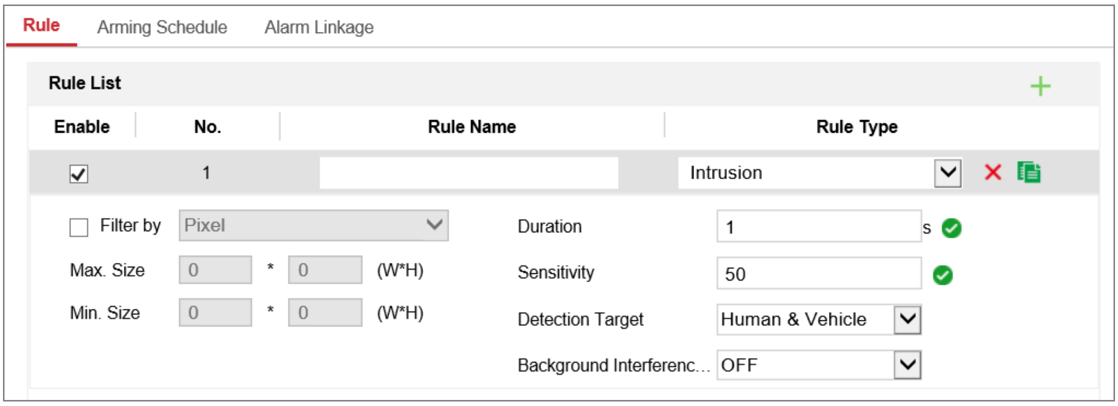
   Note:

   If you want to detect human whose size is 0.5 meters wide, 1.8 meters high probably, the recommend settings are shown below.

   Min. Size: 0.4*0.8(m)

   Max. Size: 1.5*2.5(m)

   Detection Target: Human.



Enable	No.	Rule Name	Rule Type
☑	1		Intrusion

☐ Filter by: Pixel

Max. Size: 0 * 0 (W*H)

Min. Size: 0 * 0 (W*H)

Duration: 1 s

Sensitivity: 50

Detection Target: Human & Vehicle

Background Interferenc...: OFF

Figure 9-22 Configure the Rule

Filter type: Pixels and Actual Size are selectable. If Pixels is selected, draw the area of maximum size and minimum size on the live video for each rule. If Actual Size is selected, input the length and width of the maximum size and minimum size. Only the target whose size is between the minimum value and maximum value will trigger the alarm.

Note: Make sure the camera calibration is configured if actual size is selected.

Sensitivity. The higher the value is, the more likely to trigger the alarm.

Detection Target: Select Human, Vehicle, or Human & Vehicle as the detection target. You can also select all to detect all moving objects as the target.

Background Interference Suppression: Eliminate the environment interference to reduce the false alarm. For example, the wind blow grass. **ON, OFF** and **Self-Adaptive** are selectable.

Draw line/area: For line crossing detection, you have to draw a line, and select the crossing direction, which is bidirectional, A-to-B, or B-to-A. For other events such as intrusion, region entrance, region exiting, etc., you have to left click on the live video to set the end points of the area and right click to finish the area drawing.

Note: If the live view is stopped, the detection area / line cannot be draw and the rules cannot be set.

Notes:

- If you select the rule type as None, the rule option is invalid, and no behavior analysis can be configured.

- Up to 8 single rules and 2 combined rules are configurable. And the line crossing, intrusion, region exiting and region entrance are supported for the combined rules.

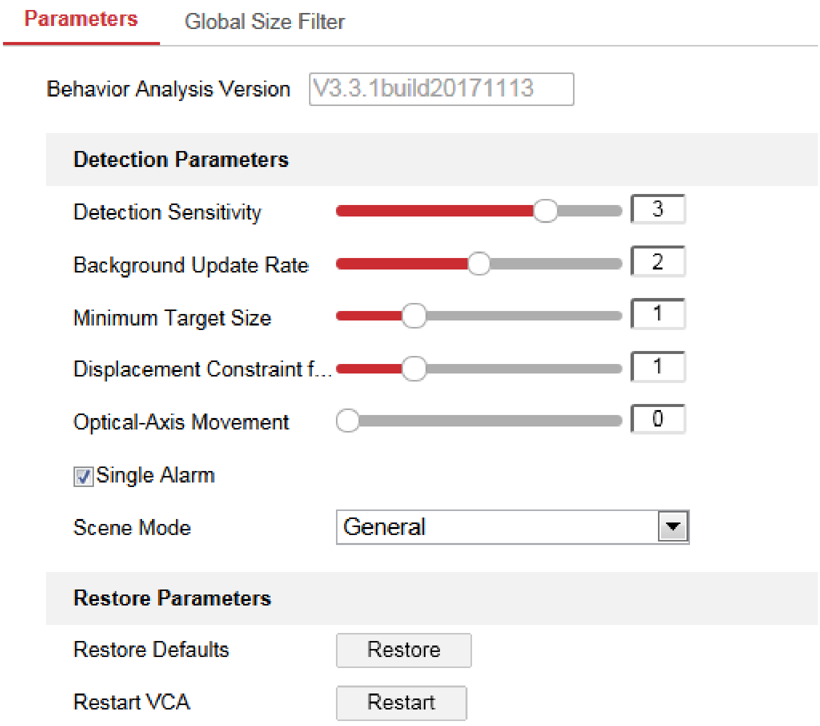
5. Click Save.
6. Click **Arming Schedule** tab to set the schedule time for each rule, and Click Save.
7. Click **Linkage Method** tab, check the checkbox of corresponding linkage method for each rule, and Click Save.

9.3.5 Advanced Settings

Behavior Analysis Version: It lists the version of the algorithms library.

- **Parameter**

Configure the following parameters to detail the configuration.



Behavior Analysis Version: V3.3.1build20171113

Detection Parameters

Detection Sensitivity: 3

Background Update Rate: 2

Minimum Target Size: 1

Displacement Constraint f...: 1

Optical-Axis Movement: 0

☑ Single Alarm

Scene Mode: General

Restore Parameters

Restore Defaults

Restart VCA

Figure 9-23 Advanced Configuration

Detection Sensitivity [0~4]: Refers to the sensitivity of the camera detects a target. The higher the value, the easier a target be recognized, and the higher the misinformation is. The default value of 3 is recommended.

Background Update Rate [0~4]: It refers to the speed of the new scene replaces the previous scene. The default value of 3 is recommended.

Minimum Target Size: Range [0-4], The system will filter out the object smaller than the minimum target size.

Displacement Constraint for Target Generation: Range [0-4], the higher the value is, the slower the target is generated, and the higher accuracy the analysis will get.

Light Change Suppression: Check the checkbox to suppress the impact caused by the illumination change.

Leave Interference Suppression: Check this checkbox to stop the interference caused by the leaves in the configured area.

Scene Modes: The scene mode is set to be General by default. Select Distant View when you are far from the targets. Select Indoor when you are indoor.

Optical-axis Movement: Check the checkbox when the target moves in the direction of camera's optical -axis.

Single Alarm: If single alarm is selected, the target in the configured area will trigger the alarm for only once. If it is not checked, the same target will cause the continuous alarm in the same configured area.

Restore Default: Click to restore the configured parameters to the default.

Restart VCA: Restart the algorithms library of behavior analysis.

- **Global Size Filter**

  Note: Compared with the size filter under rule, which is aiming at each rule, the global size filter is aim at all rules.

  Steps:

  1. Enter **Configuration** > **VCA** > **Advanced Configuration**.
  2. Check the checkbox of **Global Size Filter** to enable the function.
  3. Select the Filter Type as Actual Size or Pixel.

  Actual Size: Input the length and width of both the maximum size and the minimum size. Only the target whose size is between the minimum value and maximum value will trigger the alarm.

Notes:

- Camera calibration has to be configured if you select the filter by actual size.
- The length of the maximum size should be longer than the length of the minimum size, and so does the width.

Pixel: Click Minimum Size to draw the rectangle of the min. size on the live view. And click Maximum Size to draw the rectangle of the max. size on the live view. The target is smaller than the min. size or larger than the max. size will be filtered.

Notes:

- The drawn area will be converted to the pixel by the background algorithm.
- The global size filter cannot be configured if the live view is stopped.
- The length of the maximum size should be longer than the length of the minimum size, and so does the width.

4. Click **Save**.

9.4 Temperature Measurement

9.4.1 Basic Settings

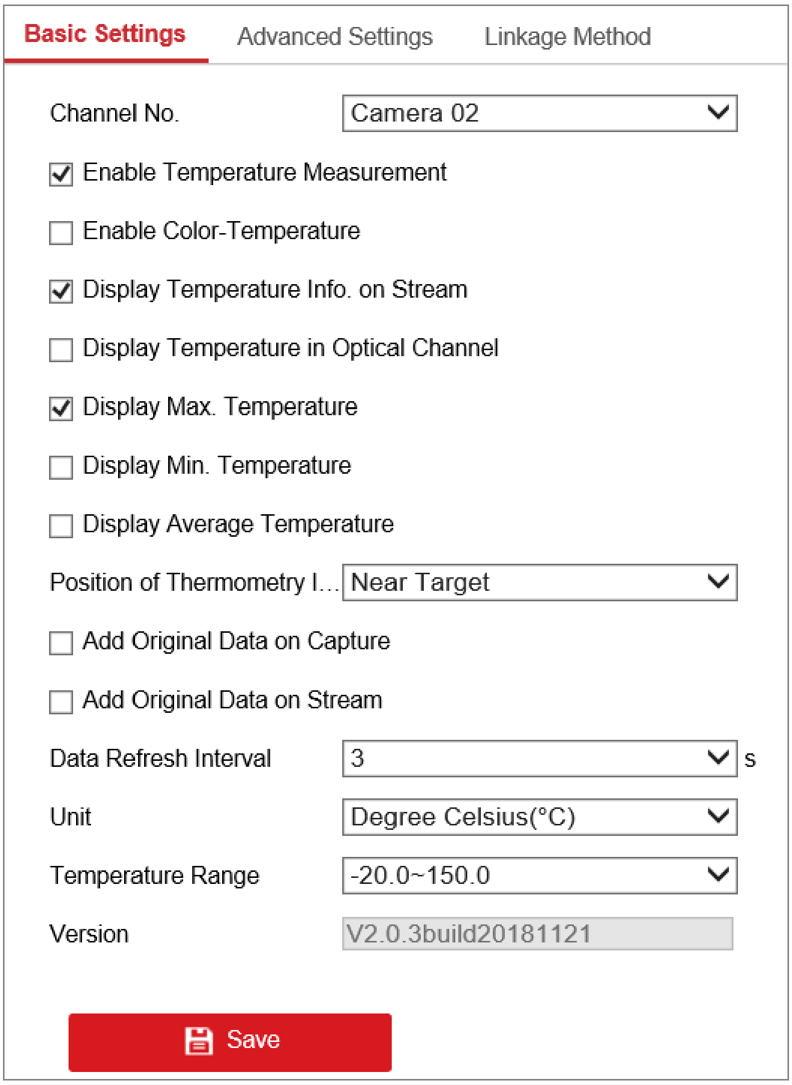
Purpose:

The device can measure the actual temperature of the spot being monitored. The device alarms when temperature exceeds the temperature threshold value.

Note: Before you use the temperature measurement function, enter **Configuration** > **System** > **Maintenance** > **VCA Resource Type** to select **Temperature Measurement + Behavior Analysis** as VCA Resource Type.

Steps:

1. Enter **Configuration** > **Temperature Measurement** > **Basic Settings**.



Channel No. Camera 02

☑ Enable Temperature Measurement

□ Enable Color-Temperature

☑ Display Temperature Info. on Stream

□ Display Temperature in Optical Channel

☑ Display Max. Temperature

□ Display Min. Temperature

□ Display Average Temperature

Position of Thermometry I… Near Target

□ Add Original Data on Capture

□ Add Original Data on Stream

Data Refresh Interval 3 s

Unit Degree Celsius(°C)

Temperature Range -20.0~150.0

Version V2.0.3build20181121

Figure 9-24 Basic Settings

2. Check the checkboxes of the interface to set the temperature measurement configurations.

    - **Enable Temperature Measurement**: Check the checkbox to enable temperature measurement function.
    - **Enable Color-Temperature**: Check the checkbox to display temperature pallet in live view.
    - **Display Temperature Info. on Stream**: Check the checkbox to display temperature information in live view.
    - **Display Temperature in Optical Channel**: Check the checkbox to display temperature information in the optical channel.
    - **Display Max. Temperature**: Check the checkbox to display maximum temperature information in thermal view when the temperature

measurement rule is line or area.

- **Display Min. Temperature**: Check the checkbox to display minimum temperature information in thermal view when the temperature measurement rule is line or area.
- **Display Average Temperature**: Check the checkbox to display average temperature information in thermal view when the temperature measurement rule is line or area.
- **Position of Thermometry Info**: Select the position of temperature measurement information showed on the live view interface. Select Top Left to display the information on the top left of screen. Select Near Target to display the information around the temperature measurement rule.
- **Add Original Data on Capture**: Check the checkbox to add original data on capture.
- **Add Original Data on Stream**: Check the checkbox to add original data on stream.
- **Data Refresh Interval**: Select the data refresh interval from 1s to 5s.
- **Unit**: Display temperature with Degree Celsius (°C)/ Degree Fahrenheit (°F)/ Degree Kelvin (K).
- **Temperature Range**: Set the temperature range.
- **Version**: View the version of current algorithm.

3. Click Save.

9.4.2 Set Temperature Measurement Rule

Before you start:

The temperature measurement function is usually used together with alarm function. You can set the alarm linkage so that any alarm/pre-alarms can trigger the connected alarm. You can double click current screen to show full of it, and double click again to exit full screen.

Purpose:

This function is used for measuring the temperature of detected spot and the device compares temperature of selected regions and alarms.

Steps:

- *(For Normal Mode)*

1. Go to **Configuration > Temperature Measurement > Advanced Settings**.
2. Select the configuration mode as **Normal**.
3. Configure the parameters.

   Emissivity: Set the emissivity of your target. Note: The emissivity of each object is different.

   Distance (m): The straight-line distance between the target and the device.

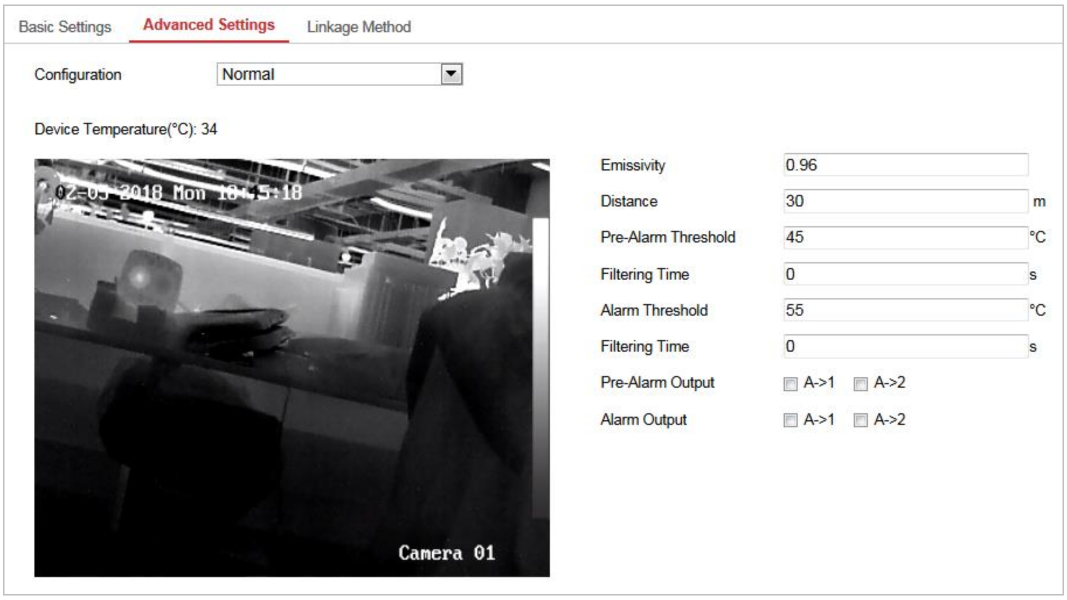
   - **Pre-Alarm:** When the temperature of target exceeds the **Pre-Alarm Threshold**, and this status keeps NOT shorter than the **Filtering Time**, it triggers the Pre-Alarm.

     Check the checkbox of Pre-Alarm Output to set link the pre-alarm with the connected alarm device.

   - **Alarm**: When the temperature of target exceeds the **Alarm Threshold**, and this status keeps NOT shorter than the **Filtering Time**, it triggers the Alarm.

     Check the checkbox of **Alarm Output** to set link the pre-alarm with the connected alarm device.

4. Click **Save**.



Configuration: Normal

Device Temperature(°C): 34

Emissivity	0.96	
Distance	30	m
Pre-Alarm Threshold	45	°C
Filtering Time	0	s
Alarm Threshold	55	°C
Filtering Time	0	s
Pre-Alarm Output	□ A->1 □ A->2	
Alarm Output	□ A->1 □ A->2	

Figure 9-25 Temperature Measurement Configuration

- *(For Expert Mode)*

1. Enter **Configuration > Temperature Measurement > Advanced Settings**.
2. Select the configuration mode as **Expert**.
3. Configure the parameters.

Name: You can customize the rule name.

Type: Select **Point**, **Line**, or **Area** as rule type.

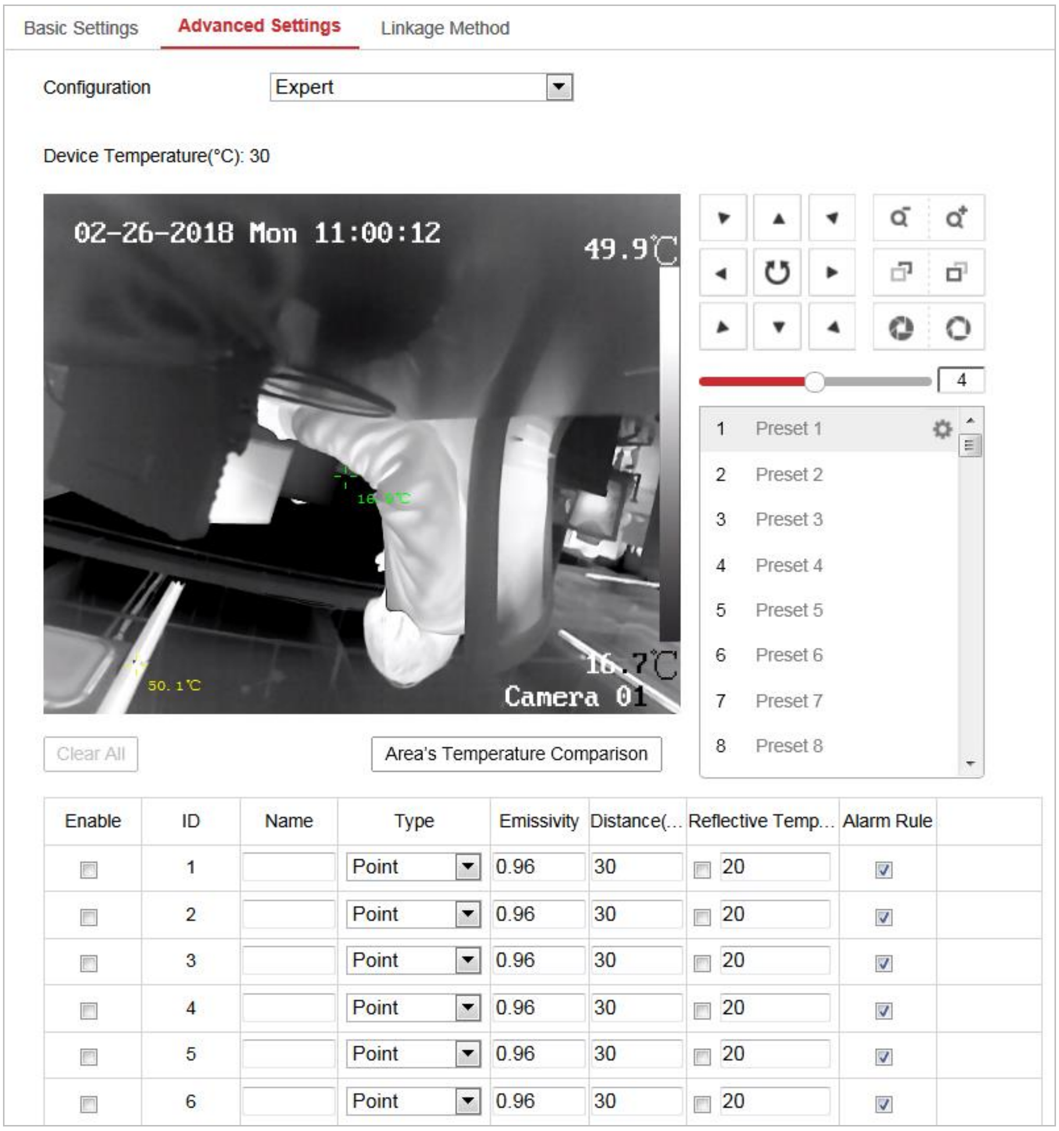
Emissivity: Set the emissivity of your target. The emissivity of each object is different, you can refer to the Appendix for details.

Distance (m): The straight-line distance between the target and the device.

Reflective Temperature: If there is any object reflecting to the target, e.g., a mirror, enter the background temperature value/the reflecting object's temperature value. If not, uncheck the checkbox.

Tolerance Temperature: The triggered alarm does NOT stop until the temperature/temperature difference is lower/higher than rule temperature by tolerance temperature.

Example: set tolerance temperature as 3°C, set alarm temperature as 55°C. It alarms when its temperature reaches 55°C and only when the temperature is below 52°C will the alarm be cancelled.



Configuration: Expert

Device Temperature(°C): 30

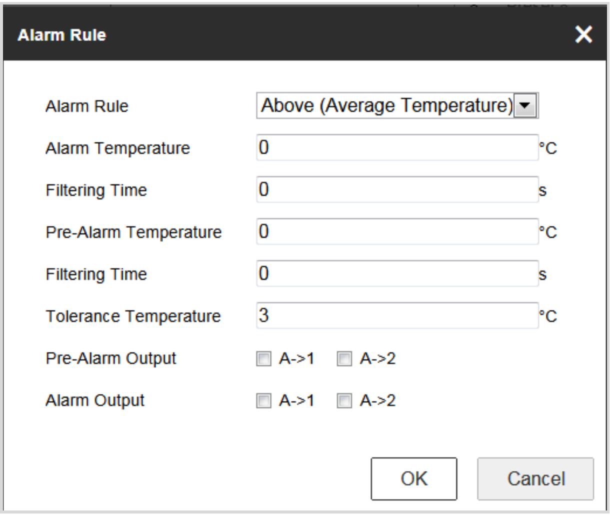
Enable	ID	Name	Type	Emissivity	Distance(...	Reflective Temp...	Alarm Rule
☐	1		Point	0.96	30	☐ 20	☑
☐	2		Point	0.96	30	☐ 20	☑
☐	3		Point	0.96	30	☐ 20	☑
☐	4		Point	0.96	30	☐ 20	☑
☐	5		Point	0.96	30	☐ 20	☑
☐	6		Point	0.96	30	☐ 20	☑

Figure 9-26 Temperature Measurement Configuration

4. Check the Enable checkbox to enable the alarm rule.

For Point Rule:

a) Click ⚙ to show the Alarm Rule setting interface.



Alarm Rule

Alarm Rule	Above (Average Temperature)
Alarm Temperature	0 °C
Filtering Time	0 s
Pre-Alarm Temperature	0 °C
Filtering Time	0 s
Tolerance Temperature	3 °C
Pre-Alarm Output	□ A->1 □ A->2
Alarm Output	□ A->1 □ A->2

Figure 9-27 Alarm Rule Settings (Point)

b) Set the **Alarm Rule**.

c) Set the **Alarm Temperature**, **Pre-Alarm Temperature**, and **Tolerance Temperature**.

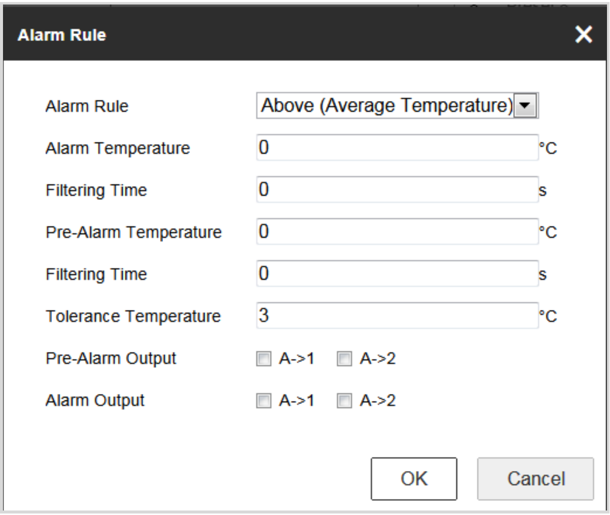
d) Set the **Filtering Time**.

e) Set the **Pre-Alarm Output** and **Alarm Output** with the connected alarm sensor and alarm device.

Example: select **Alarm Rule** as **Above (Average Temperature)**, set the **Alarm Temperature** to 50 °C and **Filtering Time** as 5 s, and then the device alarms when its average temperature keeps being above 50 °C for over 5 s.

For Line and Area Rule:

a) Click ⚙ to show the Alarm Rule setting interface.



Alarm Rule

Alarm Rule	Above (Average Temperature)
Alarm Temperature	0 °C
Filtering Time	0 s
Pre-Alarm Temperature	0 °C
Filtering Time	0 s
Tolerance Temperature	3 °C
Pre-Alarm Output	□ A->1 □ A->2
Alarm Output	□ A->1 □ A->2

Figure 9-28 Alarm Rule Settings (Line)

b) Set the **Alarm Rule**.

c) Set the **Alarm Temperature**, **Pre-Alarm Temperature**, and **Tolerance Temperature**.

d) Set the **Filtering Time**.

e) Set the **Pre-Alarm Output** and **Alarm Output** with the connected alarm sensor and alarm device.

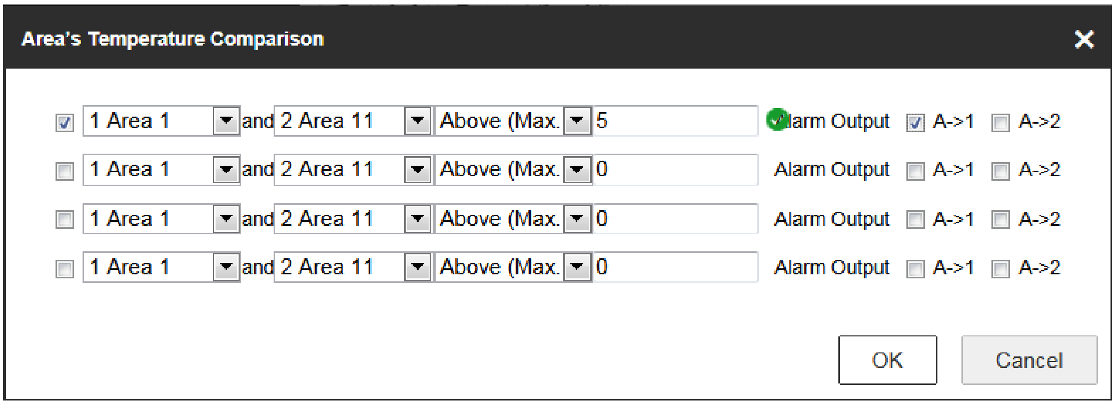
Example: select Alarm Rule as Min. Temperature is Lower than, and set the Alarm Temperature to 40 °C, and the device alarms when the minimum temperature is lower than 40 °C.

For Area Temperature Comparison:

Make sure you have enabled the areas for comparison.

a) Click **Area's Temperature Comparison.**

b) Select the areas.



Area's Temperature Comparison

☑	1 Area 1	and	2 Area 11	Above (Max.	5	Alarm Output	☑ A->1	□ A->2
□	1 Area 1	and	2 Area 11	Above (Max.	0	Alarm Output	□ A->1	□ A->2
□	1 Area 1	and	2 Area 11	Above (Max.	0	Alarm Output	□ A->1	□ A->2
□	1 Area 1	and	2 Area 11	Above (Max.	0	Alarm Output	□ A->1	□ A->2

Figure 9-29 Area Temperature Comparison Alarm

c) Select the comparison rule.

d) Set the temperature difference threshold value.

Example: select **Area 1** and **Area 11**, and set the comparison rule as **Above (Max. Temperature)**, and set the temperature difference threshold to 5 °C. The device alarms when the difference of two areas' maximum temperature is above 5 °C.

9.4.3 Linkage Method

Purpose:

Set the linkage method of the alarm.

Steps:

1. Enter **Configuration** > **Temperature Measurement** > **Linkage Method**.
2. Set the arming schedule and linkage method.
   - **Arming Schedule**: Click on the time bar and drag the mouse to select the time period.
   - **Linkage Method**: Click Linkage Method and check the checkbox to select the linkage method. Audible warning, notify surveillance center, send email, upload to FTP, trigger channel and trigger alarm output are selectable. You can specify the linkage method when an event occurs.
3. Click Save.

After the settings, you can view the current temperature and humidity on the top of this interface.

Chapter 10 Storage Settings

Before you start:

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

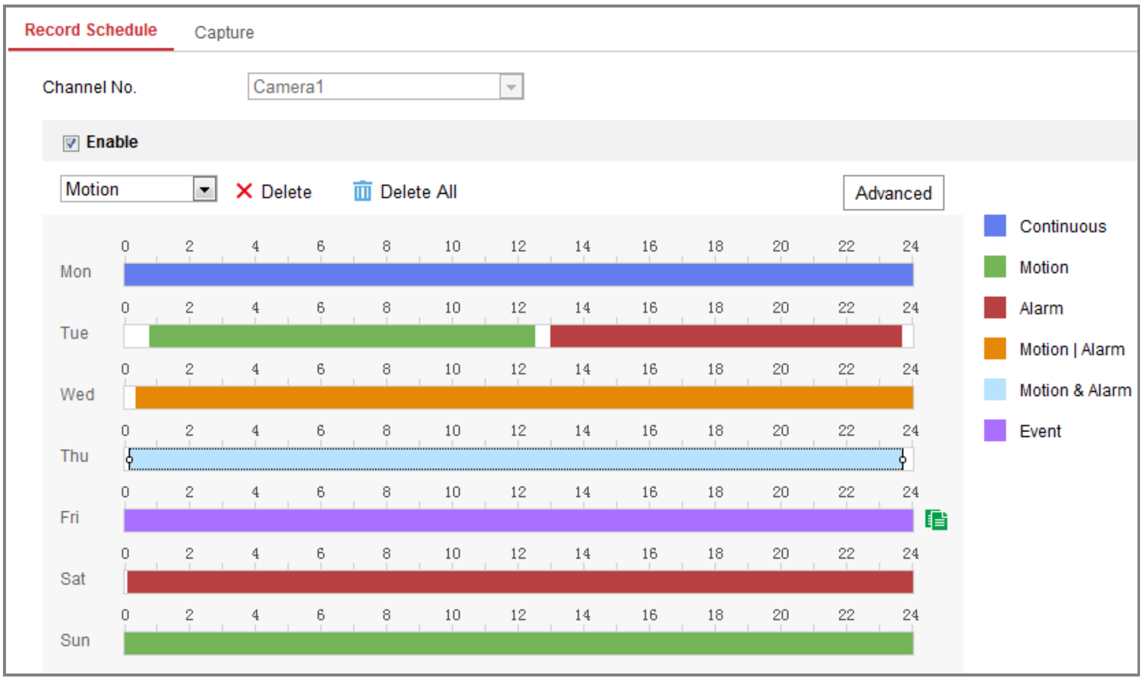
10.1 Set Record Schedule

Purpose:

There are two kinds of recording for the cameras: manual recording and scheduled recording. In this section, you can follow the instructions to configure the scheduled recording. By default, the record files of scheduled recording are stored in the local storage or in the network disk.

Steps:

1. Go to the Record Schedule Settings interface: **Configuration** > **Storage** > **Schedule Settings > Record Schedule**.



Record Schedule | Capture

Channel No. Camera1

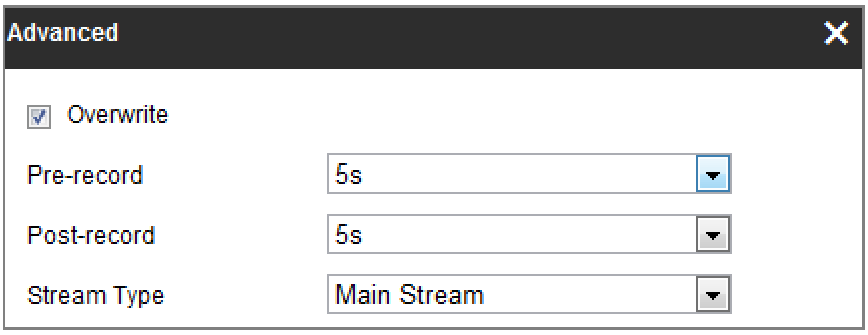
☑ Enable

Motion

Figure 10-1 Recording Schedule Interface

2. Check the checkbox of **Enable** to enable scheduled recording.

3. Click **Advanced** to set the camera record parameters.



Advanced

☑ Overwrite

Pre-record: 5s

Post-record: 5s

Stream Type: Main Stream

Figure 10-2 Record Parameters

- Pre-record: The time you set to start recording before the scheduled time or the event. For example, if an alarm triggers recording at 10:00, and the pre-record time is set as 5 seconds, the camera starts to record at 9:59:55.

  The Pre-record time can be configured as No Pre-record, 5s, 10s, 15s, 20s, 25s, 30s or not limited.

- Post-record: The time you set to stop recording after the scheduled time or the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set as 5 seconds, the camera records until 11:00:05.

  The Post-record time can be configured as 5s, 10s, 30s, 1 min, 2 min, 5 min or 10 min.

- Stream Type: Select the stream type for recording.

Note: The record parameter configurations vary depending on the camera model.

4. Select a **Record Type**. The record type can be Continuous, Motion Detection, Alarm, Motion | Alarm, Motion & Alarm, and Event.

   - **Continuous**

     If you select **Continuous**, the video will be recorded automatically according to the time of the schedule.

   - **Record Triggered by Motion Detection**

     If you select **Motion Detection**, the video will be recorded when the motion is detected.

     Besides configuring the recording schedule, you have to set the motion detection area and check the checkbox of Trigger Channel in the Linkage

Method of Motion Detection Settings interface. For detailed information, please refer to the ***Task 1: Set the Motion Detection Area*** in the *Section 9.1.1*.

- **Record Triggered by Alarm**

  If you select **Alarm**, the video will be recorded when the alarm is triggered via the external alarm input channels.

  Besides configuring the recording schedule, you have to set the **Alarm Type** and check the checkbox of **Trigger Channel** in the **Linkage Method** of **Alarm Input Settings** interface. For detailed information, please refer to *Section 9.1.1*

- **Record Triggered by Motion & Alarm**

  If you select **Motion & Alarm**, the video will be recorded when the motion and alarm are triggered at the same time.

  Besides configuring the recording schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces. Please refer to *Section 9.1.1* for detailed information.

- **Record Triggered by Motion | Alarm**

  If you select **Motion | Alarm**, the video will be recorded when the external alarm is triggered or the motion is detected.

  Besides configuring the recording schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces. Please refer to *Section 9.1.1* for detailed information.

- **Record Triggered by Events**

  If you select **Event**, the video will be recorded if any of the events is triggered. Besides configuring the recording schedule, you have to configure the event settings.

5. Select the record type, and click-and-drag the mouse on the time bar to set the record schedule.
6. Click Save.

10.2 Set 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.

Steps:

1. Go to the Capture Settings interface: **Configuration** > **Storage** > **Storage Settings** > **Capture**.

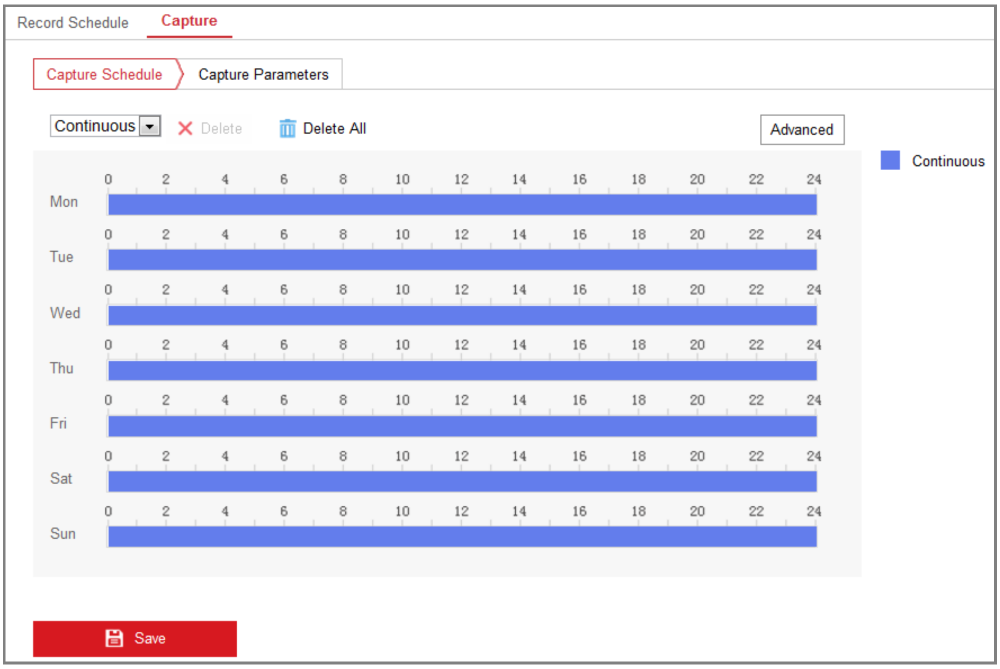
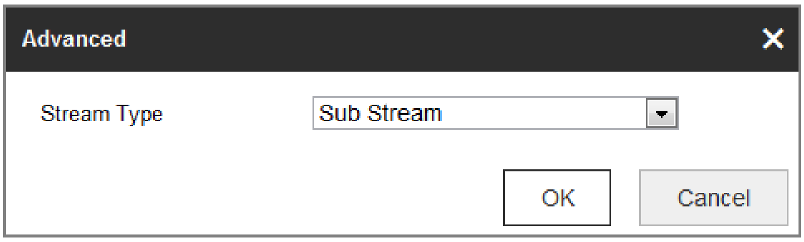


Figure 10-3 Capture Configuration

2. Go to **Capture Schedule** tab to configure the capture schedule by click-and-drag the mouse on the time bar. You can copy the record schedule to other days by clicking the green copy icon on the right of each time bar.
3. Click **Advanced** to select stream type.



Stream Type: Sub Stream

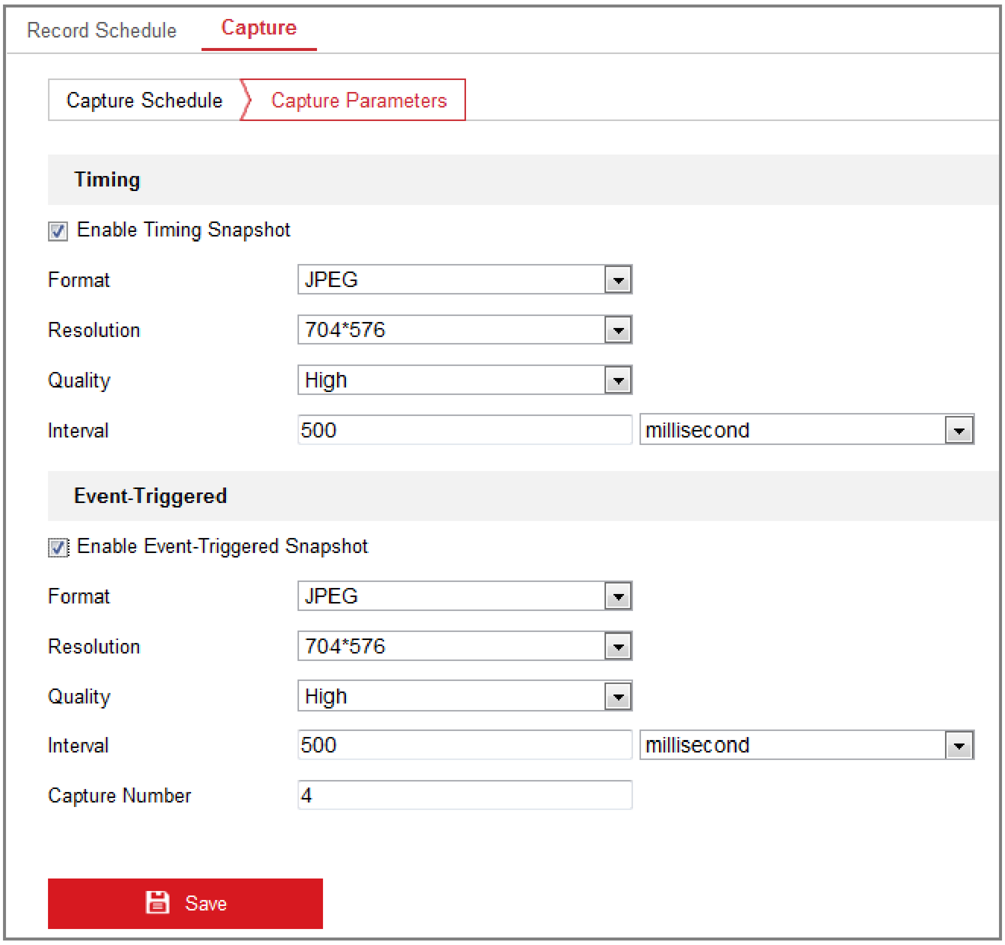
Figure 10-4 Advanced Setting of Capture Schedule

4. Click **Save**.

5. 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.
   (3) Check the **Enable Event-triggered Snapshot** checkbox to enable event-triggered snapshot.

   Note: Behavior analysis, fire detection, and temperature measurement can not trigger the snapshots.

   (4) Select the picture format, resolution, quality, capture interval, and capture number.



Timing

☑ Enable Timing Snapshot

Format: JPEG

Resolution: 704*576

Quality: High

Interval: 500 millisecond

Event-Triggered

☑ Enable Event-Triggered Snapshot

Format: JPEG

Resolution: 704*576

Quality: High

Interval: 500 millisecond

Capture Number: 4

Figure 10-5 Set Capture Parameters

6. Set the time interval between two snapshots.
7. Click **Save**.

10.3 Set Net HDD

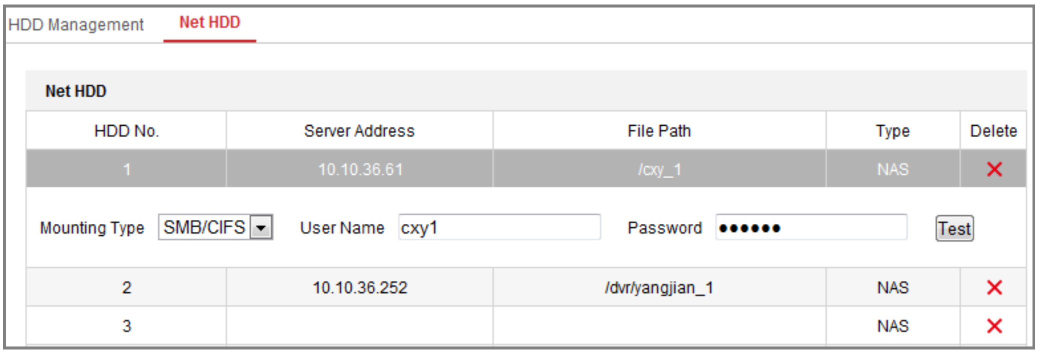
Before you start:

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

Steps:

1. Add Net HDD.

(1) Go to the Net HDD settings interface, **Configuration** > **Storage** > **Storage Management** > **Net HDD**.



Net HDD

HDD No.	Server Address	File Path	Type	Delete
1	10.10.36.61	/cxy_1	NAS	✕
2	10.10.36.252	/dvr/yangjian_1	NAS	✕
3			NAS	✕

Mounting Type SMB/CIFS User Name cxy1 Password ••••••

Figure 10-6 Add Network Disk

(2) Enter the IP address of the network disk, and the file path.

(3) Select the mounting type. NFS and SMB/CIFS are selectable. And you can set the user name and password to guarantee the security if SMB/CIFS is selected.

Note: Please refer to the *NAS User Manual* for creating the file path.

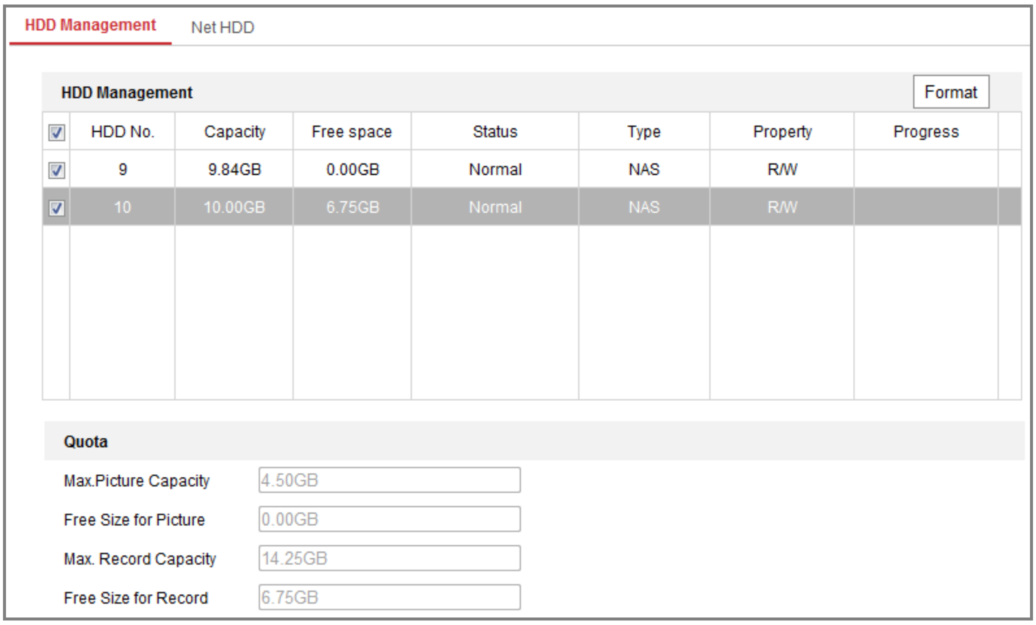
- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.*
- *Proper configuration of all passwords and other security settings is the*

responsibility of the installer and/or end-user.

(4) Click **Save** to add the network disk.

2. Initialize the added network disk.

(1) Go to the HDD Settings interface, **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	Property	Progress
☑	9	9.84GB	0.00GB	Normal	NAS	R/W	
☑	10	10.00GB	6.75GB	Normal	NAS	R/W	

Quota

Max.Picture Capacity: 4.50GB

Free Size for Picture: 0.00GB

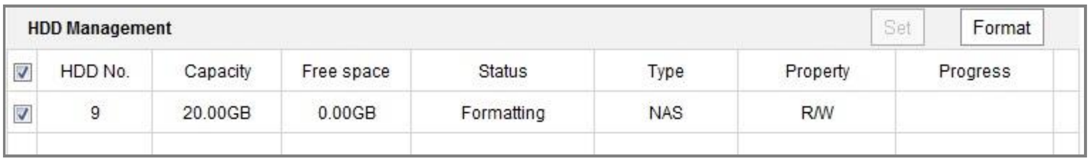
Max. Record Capacity: 14.25GB

Free Size for Record: 6.75GB

Figure 10-7 Storage Management Interface

(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.

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



HDD Management

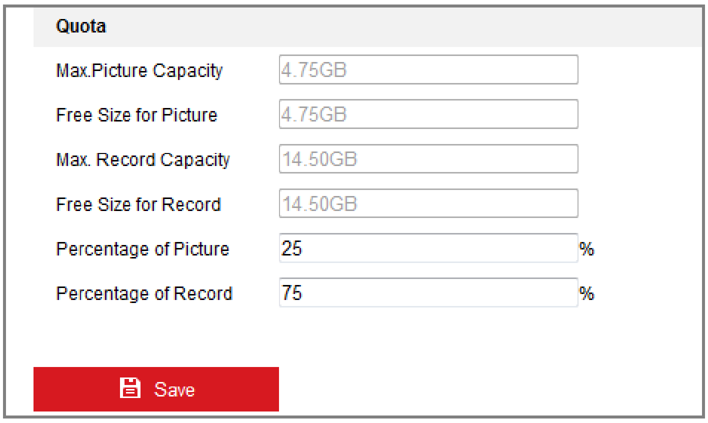
☑	HDD No.	Capacity	Free space	Status	Type	Property	Progress
☑	9	20.00GB	0.00GB	Formatting	NAS	R/W	

Figure 10-8 View Disk Status

3. Define the quota for record and pictures.

(1) Input the quota percentage for picture and for record.

(2) Click **Save** and refresh the browser page to activate the settings.



Quota

Max.Picture Capacity	4.75GB
Free Size for Picture	4.75GB
Max. Record Capacity	14.50GB
Free Size for Record	14.50GB
Percentage of Picture	25 %
Percentage of Record	75 %

Figure 10-9 Quota Settings

Note:

Up to 8 NAS disks can be connected to the camera.

10.4 Set Memory Card Detection

Purpose:

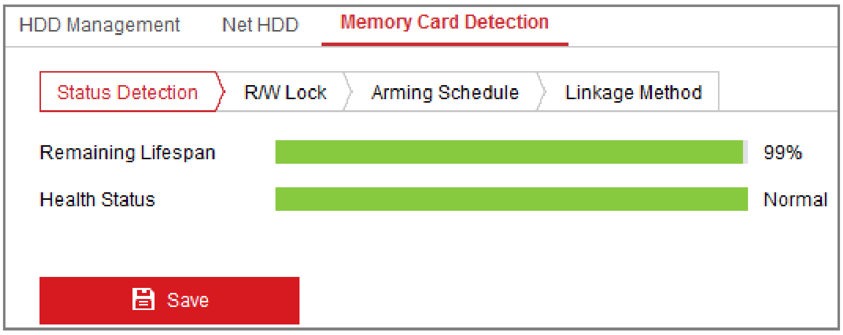
With memory card detection, you can view the memory card status, lock your memory card, and receive notification when your memory card is detected abnormal.

Note: Memory card detection function is only supported by certain types of memory cards and camera models. If this tab page doesn't show on your web page, it means either that your camera doesn't support the function, or your installed memory card is not supported for this function. You can contact the dealer or the retailer for the information of memory card that supports the function.

Steps:

1. Enter Memory Card Detection configuration interface:

   Configuration > Storage > Storage Management > Memory Card Detection



Remaining Lifespan	99%
Health Status	Normal

Figure 10-10 Memory Card Detection

2. View the memory card status on **Status Detection** tab.

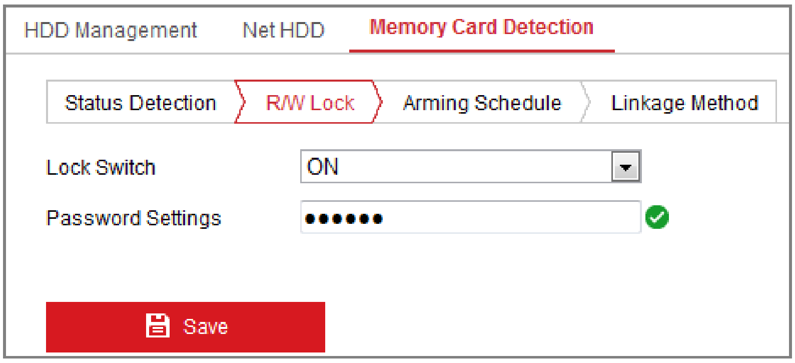
   Remaining Lifespan: It shows the percentage of the remaining lifespan. The lifespan of a memory card may be influenced by factors such as its capacity and the bitrate. You need to change the memory card if the remaining lifespan is not enough.

   Health Status: It shows the condition of your memory card. There are three status descriptions, good, bad, and damaged. You will receive a notification if the health status is anything other than good when the **Arming Schedule** and **Linkage Method** are set.

   Note: It is recommended that you change the memory card when the health status is not "good".

3. Click **R/W Lock** tab to add a lock to the memory card.

   With the R/W lock added, the memory card can only be read and write when it is unlocked.



Lock Switch: ON

Password Settings: ●●●●●●

Figure 10-11 R/W Lock Setting

- Add a Lock

(1) Select the **Lock Switch** as ON.

(2) Input the password.

(3) Click Save.

- Unlock

(1) If you use the memory card on the camera that locks it, unlocking will be done automatically and no unlocking procedures are required on the part of

users.

(2) If you use the memory card (with a lock) on a different camera, you can go to **HDD Management** interface to unlock the memory card manually. Select the memory card, and click the **Unlock** button shown next to the **Format** button. Then input the correct password to unlock it.

Notes:

- The memory card can only be read and written in when it is unlocked.
- If the camera, which adds a lock to a memory card, is restored to the factory settings, you can go to the HDD Management interface to unlock the memory card.

- Remove the Lock

(1) Select the **Lock Switch** as **OFF**.

(2) Input the correct password in **Password Settings** text field.

(3) Click Save.

4. Set the **Arming Schedule** and **Linkage Method**, if you want to receive a notification when the health status of the memory card is anything other than good. Refer to ***Task 2: Set the Arming Schedule for Motion Detection*** and ***Task 3: Set the Linkage Method for Motion Detection*** in *Section 9.1.1.*
5. Click **Save**.

10.5 Set Lite Storage

Purpose:

When there is no moving object in the monitoring scenario, the frame rate and bitrate of the video stream can be reduced to lengthen the storage time of the memory card.

Notes:

- Lite storage function varies according to different camera models.
- The video files recorded in lite storage mode will be played back in full frame

rate (25fps/30fps), and thus the playback process is speeded up to the eye.

1. Go to the Lite Storage interface:

   Configuration > Storage > Storage Management > Lite Storage

2. Check the Checkbox of **Enable** to enable the lite storage function.
3. Input the storage time in the text field. You can view the available space of the SD card on the page.
4. Click **Save**.

Chapter 11 Playback

Purpose:

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

Steps:

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

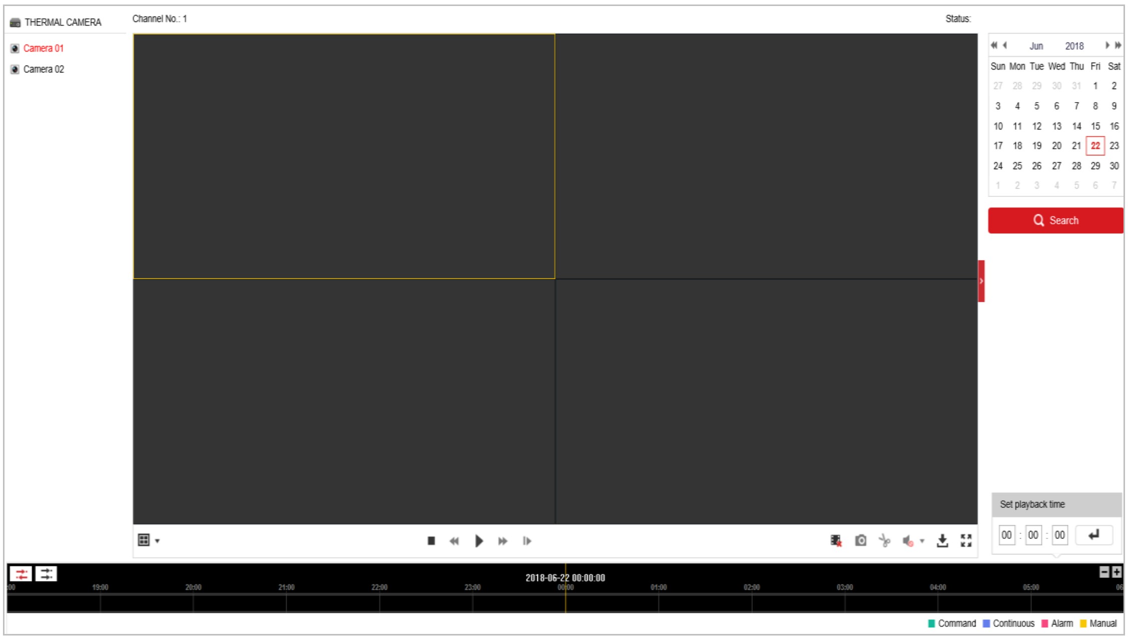
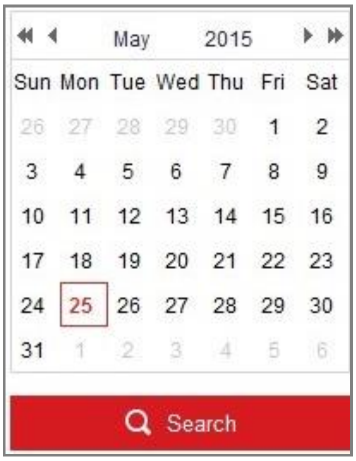


Figure 11-1 Playback Interface

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



May 2015

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	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
31	1	2	3	4	5	6

Figure 11-2 Search Video

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.

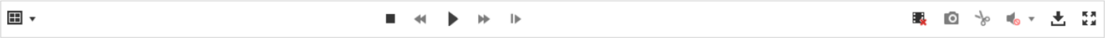


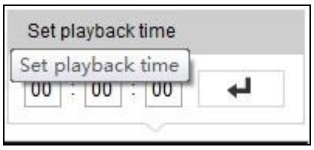
Figure 11-3 Playback Toolbar

Table 11-1 Description of the buttons

Button	Operation	Button	Operation
▶	Play	📷	Capture a picture
❚❚	Pause	✂ / ✂	Start/Stop clipping video files
■	Stop	🔊 / 🔇	Audio on and adjust volume/Mute
◀◀	Speed down	⬇	Download
▶▶	Speed up	▮▶	Playback by frame
▣/⊞/▦/▦	Display in 1×1/2×2/3×3/4×4 window.	⛶	Show full screen
✖	Stop all Playback	⇄	Play recorded videos of different cameras asynchronously.
⇄	Play recorded videos of different cameras synchronously.		

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

Set playback time

00 : 00 : 00 ↵

Figure 11-4 Set Playback Time

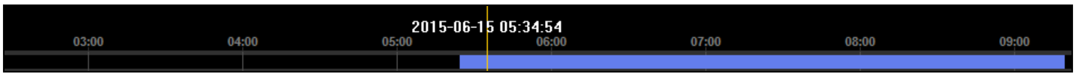
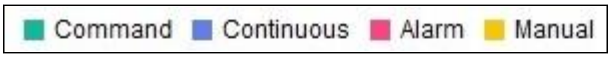


Figure 11-5 Progress Bar

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



🟩 Command 🟦 Continuous 🟥 Alarm 🟨 Manual

Figure 11-6 Video Types

Synchronously play recorded videos of different channels

Steps:

1. Click ⇉ to enable synchronous playback function.
2. Choose camera channels.
3. Setting date and time of recorded videos.
4. Click ▶ to view the videos of optical channel and thermal channel synchronously.

Asynchronously play recorded videos of different channels

Steps:

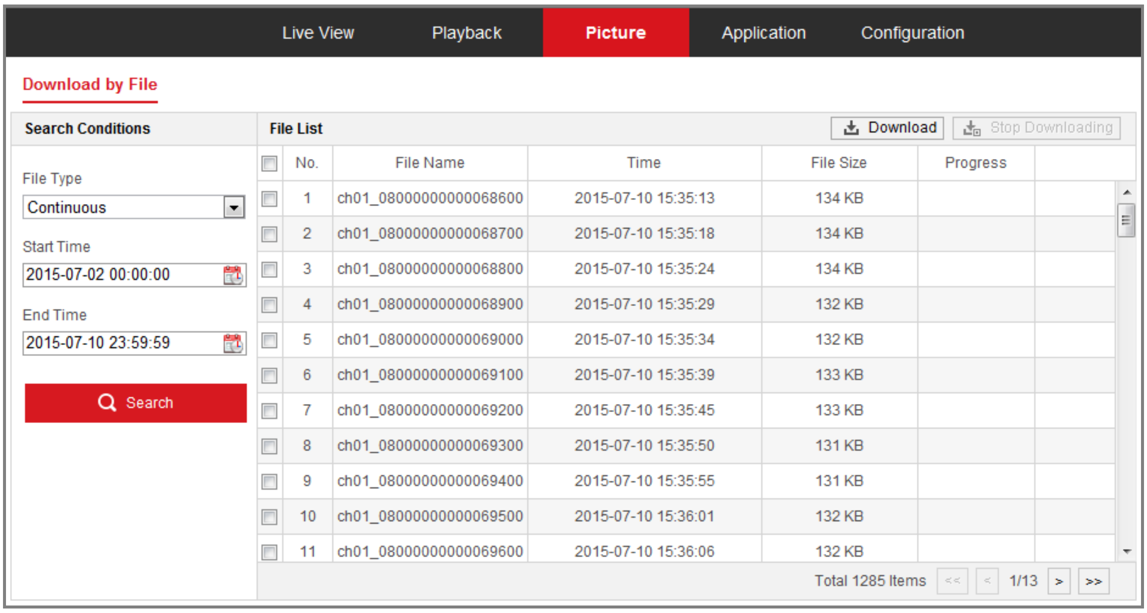
1. Click ⇄ to enable asynchronous playback function.
2. Choose Channel No: 1.
3. Setting date and time of recorded videos.
4. Choose Channel No: 2.
5. Setting date and time of recorded videos.
6. Repeat step 2-5 to configure the date and time for different channels separately.
7. Click ▶ to view the videos of optical channel and thermal channel asynchronously.

Chapter 12 Picture

Click **Picture**. You can search, view, and download the pictures stored in the local storage or network storage.

Notes:

- 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.



Search Conditions

File Type: Continuous

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

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

File List

□	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 12-1 Picture Search Interface

Steps:

1. 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.
2. Select the start time and end time.
3. Click **Search** to search the matched pictures.
4. 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.

Appendix

Appendix 1

SADP Software Introduction

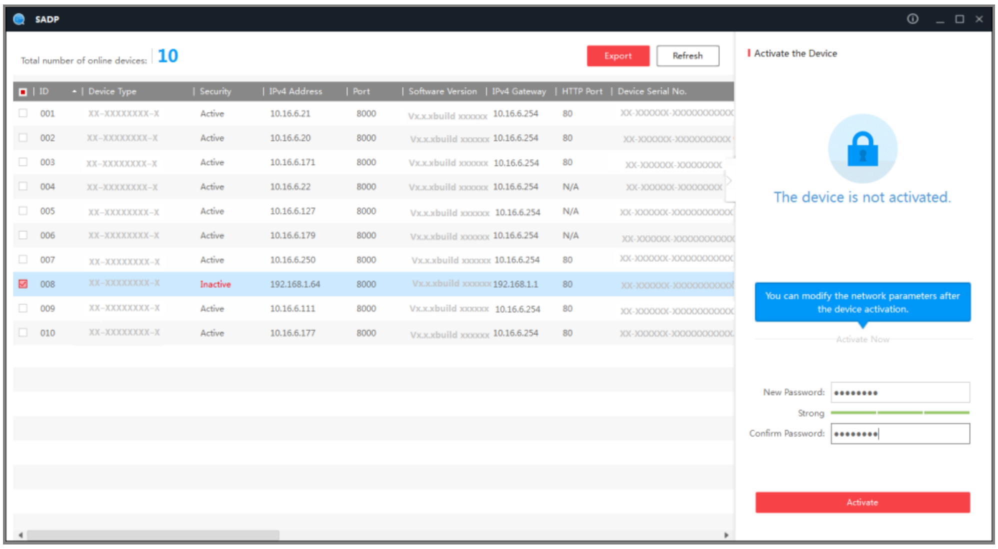
- ### Description of SADP

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

♦ **Search online devices automatically**

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.

Activate Now

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.

- **Search online devices manually**

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

  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.

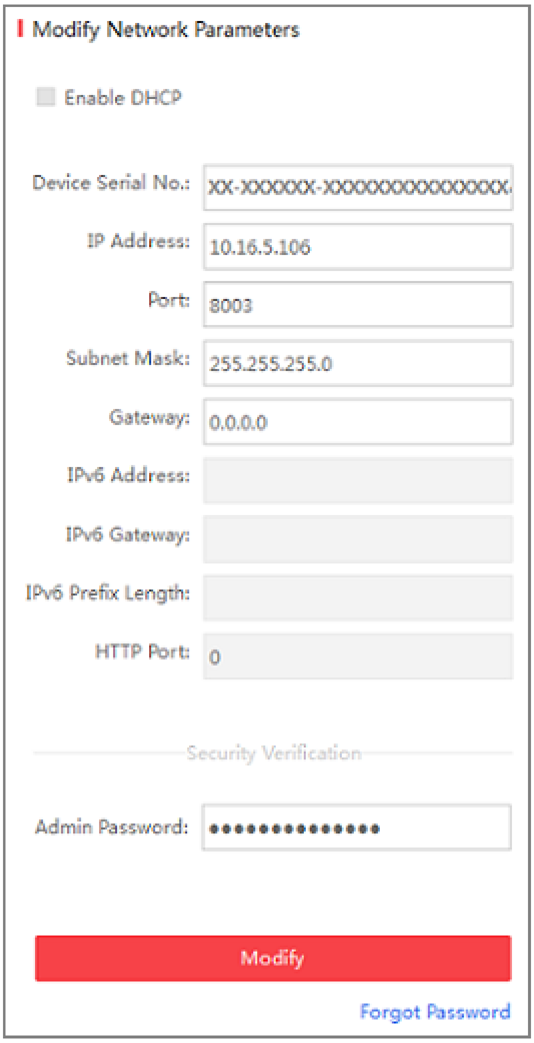
● Modify network parameters

Steps:

1. 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.
2. Edit the modifiable network parameters, e.g. IP address and port number.
3. Enter the password of the admin account of the device in the **Admin Password** field and click Modify to save the changes.

⚠

- *For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and network devices. The password should be something 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.*
- *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

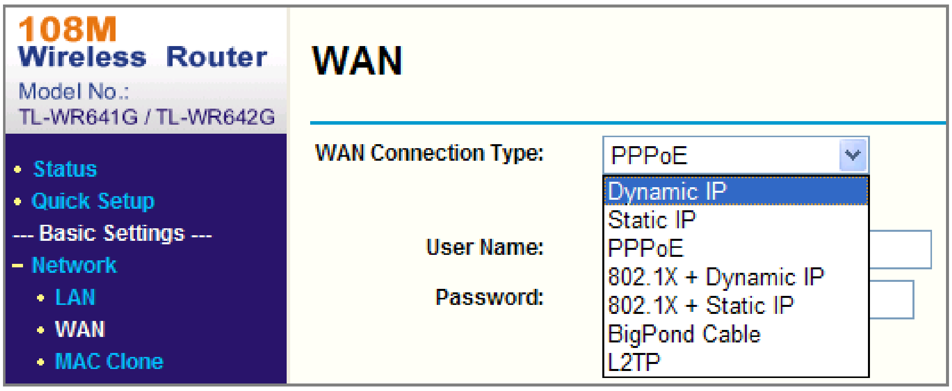
Appendix 2

Port Mapping

The following settings are for TP-LINK router (TL-WR641G). The settings vary depending on different models of routers.

Steps:

1. Select the **WAN Connection Type**, as shown below:



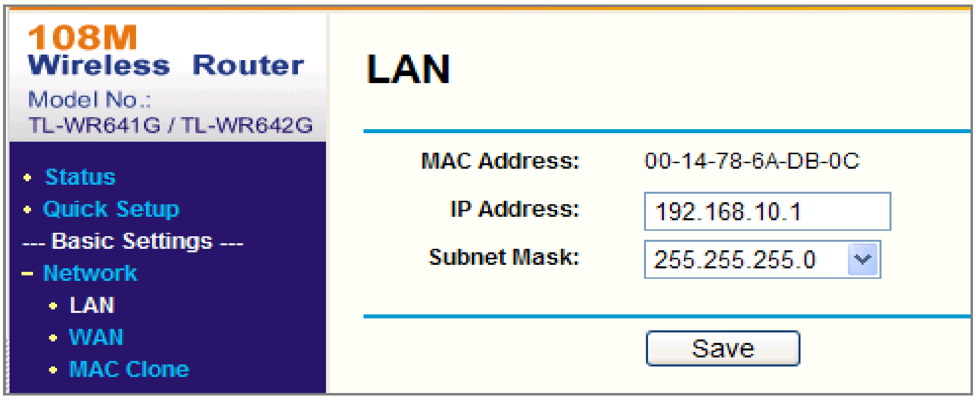
WAN Connection Type: PPPoE

User Name:

Password:

Figure A.2.1 Select the WAN Connection Type

2. Set the **LAN** parameters of the router as in the following figure, including IP address and subnet mask settings.



MAC Address: 00-14-78-6A-DB-0C

IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0

Figure A.2.2 Set the LAN parameters

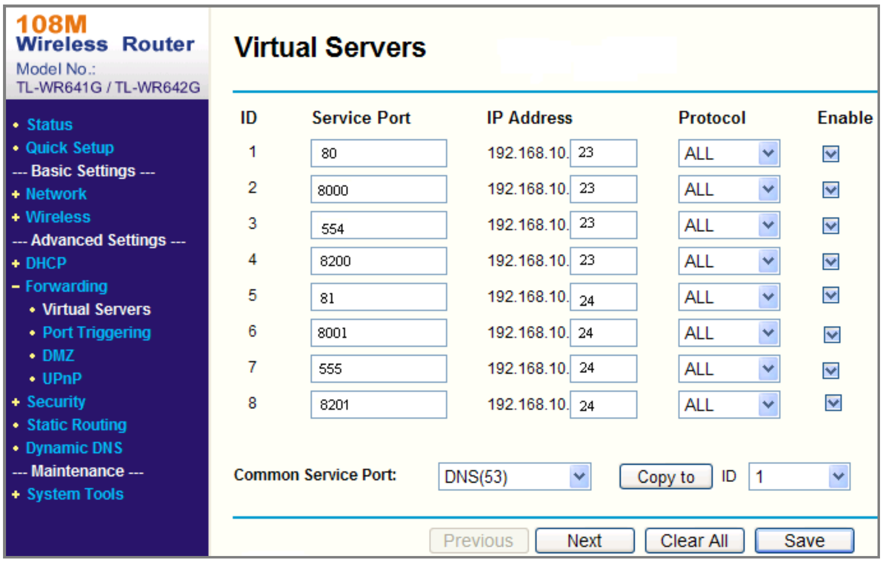
3. Set the port mapping in the virtual severs of **Forwarding**. By default, camera uses port 80, 8000 and 554. You can change these ports value with web browser or client software.

Example:

When the cameras are connected to the same router, you can configure the ports of a camera as 80, 8000, and 554 with IP address 192.168.1.23, and the ports of another camera as 81, 8001, 555, 8201 with IP 192.168.1.24. Refer to the steps as below:

Steps:

1. As the settings mentioned above, map the port 80, 8000, 554 and 8200 for the network camera at 192.168.1.23
2. Map the port 81, 8001, 555 and 8201 for the network camera at 192.168.1.24.
3. Enable **ALL** or **TCP** protocols.
4. Check the **Enable** checkbox and Click Save.



Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10. 23	ALL	☑
2	8000	192.168.10. 23	ALL	☑
3	554	192.168.10. 23	ALL	☑
4	8200	192.168.10. 23	ALL	☑
5	81	192.168.10. 24	ALL	☑
6	8001	192.168.10. 24	ALL	☑
7	555	192.168.10. 24	ALL	☑
8	8201	192.168.10. 24	ALL	☑

Common Service Port: DNS(53) Copy to ID 1

Figure A.2.3 Port Mapping

Note: The port of the network camera cannot conflict with other ports. For example, some web management port of the router is 80. Change the camera port if it is the same as the management port.

Appendix 3

Device Communication Matrix

Scan the following QR code to get device communication matrix.

Note that the matrix contains all communication ports of Hikvision thermal cameras.

Device Command

Scan the following QR code to get device common serial port commands.

Note that the command list contains the commonly used serial port commands for Hikvision thermal cameras.

See Far, Go Further