



PanoVu PT Series
Target Capture Camera
User Manual

User Manual

© 2023 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

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>).

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 LATTER

PREVAILS.

05052320221222

Regulatory Information

FCC Information

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

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

FCC Conditions

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

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

EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the Low Voltage Directive 2015/35/EU, the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU.



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



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

Industry Canada ICES-003 Compliance

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



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:

- Adopt the power adapter which can meet the safety extra low voltage (SELV) standard. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as an adapter overload may cause over-heating and can be a fire hazard.
- When the product is installed on a wall or ceiling, the device should be firmly fixed.
- To reduce the risk of fire or electrical shock, do not expose the indoor used product to rain or moisture.
- This installation should be made by a qualified service person and should conform to all the local codes.
- Install blackouts equipment into the power supply circuit for convenient supply interruption.
- If the product does not work properly, contact your dealer or the nearest service center. Never attempt to disassemble the product yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)



Cautions:

- If the camera fails to synchronize local time with that of the network, you need to set up camera time manually. Visit the camera (via web browser or client software) and enter system settings interface for time settings.
- Make sure the power supply voltage is correct before using the product.
- Do not drop the product or subject it to physical shock. Do not install the product on vibratory surface or places.
- Do not expose it to high electromagnetic radiating environment.

- Do not aim the lens at the strong light such as sun or incandescent lamp. The strong light can cause fatal damage to the product.
- 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.
- For working temperature, refer to the specification manual for details.
- To avoid heat accumulation, good ventilation is required for a proper operating environment.
- While shipping, the product should be packed in its original packing.
- Use the provided glove when open up the product cover. Do not touch the product cover with fingers directly, because the acidic sweat of the fingers may erode the surface coating of the product cover.
- Use a soft and dry cloth when clean inside and outside surfaces of the product cover. Do not use alkaline detergents.
- Improper use or replacement of the battery may result in hazard of explosion. Use the manufacturer recommended battery type.

Table of Contents

CHAPTER 1	OVERVIEW	1
1.1	SYSTEM REQUIREMENT	1
1.2	FUNCTIONS.....	1
CHAPTER 2	NETWORK CONNECTION	2
2.1	SETTING THE NETWORK CAMERA OVER THE LAN	2
2.1.1	<i>Wiring over the LAN</i>	<i>2</i>
2.1.2	<i>Activating the Camera</i>	<i>3</i>
2.1.3	<i>(Optional) Setting Security Question</i>	<i>8</i>
2.2	SETTING THE NETWORK CAMERA OVER THE WAN.....	8
2.2.1	<i>Static IP Connection</i>	<i>8</i>
2.2.2	<i>Dynamic IP Connection</i>	<i>9</i>
CHAPTER 3	ACCESSING TO THE NETWORK CAMERA.....	11
3.1	ACCESSING BY WEB BROWSERS	11
3.2	ACCESSING BY CLIENT SOFTWARE	12
CHAPTER 4	BASIC OPERATIONS	14
4.1	CONFIGURING LOCAL PARAMETERS	14
4.2	LIVE VIEW PAGE.....	15
4.3	STARTING LIVE VIEW	16
4.4	OPERATING PTZ CONTROL	18
4.4.1	<i>PTZ Control Panel.....</i>	<i>18</i>
4.4.2	<i>Auxiliary Functions.....</i>	<i>20</i>
4.4.3	<i>Setting/Calling a Preset.....</i>	<i>20</i>
4.4.4	<i>Setting/Calling a Patrol.....</i>	<i>22</i>
4.5	PLAYBACK.....	24
4.5.1	<i>Play Back Video Files</i>	<i>24</i>
4.5.2	<i>Downloading Video Files.....</i>	<i>26</i>
4.6	PICTURES	26
4.7	SMART DISPLAY	27
CHAPTER 5	SYSTEM CONFIGURATION.....	28
5.1	STORAGE SETTINGS.....	28
5.1.1	<i>Configuring Recording Schedule</i>	<i>28</i>
5.1.2	<i>Configuring Capture Schedule</i>	<i>30</i>
5.1.3	<i>Configuring Net HDD</i>	<i>31</i>
5.1.4	<i>Configuring Cloud Storage.....</i>	<i>33</i>
5.2	BASIC EVENT CONFIGURATION	34
5.2.1	<i>Configuring Motion Detection</i>	<i>35</i>
5.2.2	<i>Configuring Video Tampering Alarm.....</i>	<i>39</i>
5.2.3	<i>Configuring Alarm Input.....</i>	<i>40</i>
5.2.4	<i>Configuring Alarm Output.....</i>	<i>41</i>

5.2.5	<i>Handling Exception</i>	42
5.3	SMART EVENT CONFIGURATION	43
5.3.1	<i>Scene Change Detection</i>	43
5.4	PTZ CONFIGURATION	44
5.4.1	<i>Configuring Basic PTZ Parameters</i>	44
5.4.2	<i>Configuring PTZ Limits</i>	46
5.4.3	<i>Configuring Initial Position</i>	47
5.4.4	<i>Configuring Park Action</i>	47
5.4.5	<i>Configuring Scheduled Tasks</i>	48
5.4.6	<i>Clearing PTZ Configurations</i>	49
5.4.7	<i>Configuring Panorama Tracking</i>	50
5.4.8	<i>Configuring Rapid Focus</i>	51
CHAPTER 6	CAMERA CONFIGURATION	53
6.1	CONFIGURING NETWORK SETTINGS	53
6.1.1	<i>Basic Settings</i>	53
6.1.2	<i>Advanced Settings</i>	58
6.2	CONFIGURING VIDEO AND AUDIO SETTINGS	69
6.2.1	<i>Configuring Video Settings</i>	69
6.2.2	<i>Configuring Audio Settings</i>	71
6.3	CONFIGURING IMAGE SETTINGS	71
6.3.1	<i>Configuring Display Settings</i>	71
6.3.2	<i>Configuring OSD Settings</i>	77
6.3.3	<i>Configuring Image Parameters Switch</i>	78
6.4	CONFIGURING SYSTEM SETTINGS.....	80
6.4.1	<i>System Settings</i>	80
6.4.2	<i>Maintenance</i>	84
6.4.3	<i>Security</i>	87
6.4.4	<i>User Account</i>	89
CHAPTER 7	VCA CONFIGURATION	94
7.1	CONFIGURING FACE CAPTURE.....	94
7.1.1	<i>Overlay & Capture</i>	94
7.1.2	<i>Rule</i>	95
7.1.3	<i>Advanced Configuration</i>	97
7.2	CONFIGURING MULTI-TARGET-TYPE DETECTION	99
7.2.1	<i>PTZ Channel Configuration (Camera 01)</i>	100
7.2.2	<i>Panoramic Channel Configuration (Camera 02)</i>	103
7.3	FACE COMPARISON AND MODELING.....	105
7.3.1	<i>Configure Face Picture Library</i>	105
7.3.2	<i>Configuring Face Picture Comparison</i>	107
7.3.3	<i>Configuring Face Modeling Rule</i>	108
7.3.4	<i>Search and Download Face Pictures</i>	108
APPENDIX	109

SADP SOFTWARE INTRODUCTION 109
DEVICE COMMUNICATION MATRIX 111
DEVICE COMMAND..... 111

Chapter 1 Overview

1.1 System Requirement

System requirement of web browser accessing is as follows:

Operating System: Microsoft Windows XP SP1 and above version/Vista/Win7/Server 2003/Server 2008 32bits

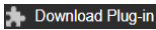
CPU: Intel Pentium IV 3.0 GHz or higher

RAM: 1G or higher

Display: 1024 × 768 resolution or higher

Web Browser: Internet Explorer 8.0 to 11.0, Apple Safari 11.0 and above version, Mozilla Firefox 30.0 and above version, Google Chrome 31.0 and above version.

Note:

If you are using Google Chrome 57 and its above version or Mozilla Firefox 52 and its above version, plug-in installation is not compulsory. But **Picture** and **Playback** of the camera are not available. If you want to use the mentioned function, change the web browser to Internet Explorer, or click  to download and install plug-in (only for Windows operation system).

1.2 Functions

Note:

The functions vary depending on different camera models.

- **Linked Capture**

The panoramic channel can be linked with PTZ channel to quickly locate and capture the target.

- **Face Capture**

The device can detect, track, capture, grade, and filter moving faces, and then output the captured picture.

- **Multi-Target Type Detection**

The device can capture different types of target, such as faces, human bodies, and vehicles, and then abstract the attributes.

- **Face Comparison**

Compare the captured face with the pictures in the library, and output the result.

Chapter 2 Network Connection

Notes:

- 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, strengthen your own protection. If the product does not work properly, 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), refer to **Section 2.1 Setting the Network Camera over the LAN.**
- If you want to set the network camera via a WAN (Wide Area Network), refer to **Section 2.2 Setting the Network Camera over the WAN.**

2.1 Setting the Network Camera over the LAN

Purpose:

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

Note:

For the detailed introduction of SADP, refer to Appendix.

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 the network camera over the LAN via a switch or a router.

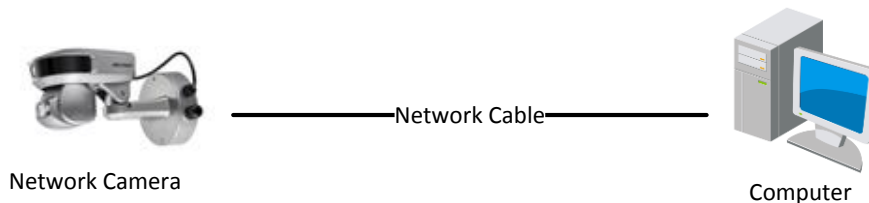


Figure 2-1 Connecting Directly

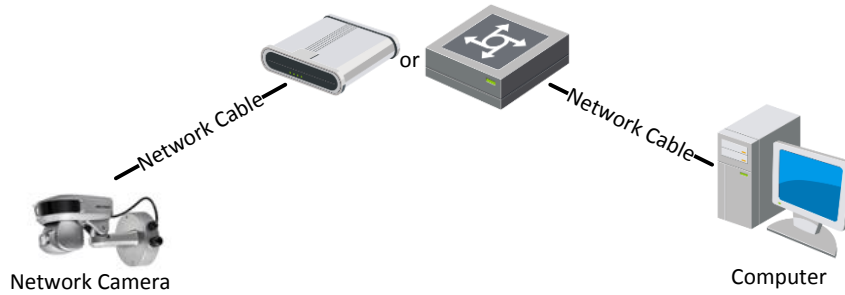


Figure 2-2 Connecting via a Switch or a Router

2.1.2 Activating the Camera

Purpose:

You are required to activate the camera first before you can use the camera.

Activation via web browser, activation via SADP, and activation via client software are 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** to enter the activation interface.

Note:

The default IP address of the camera is 192.168.1.64.

The screenshot shows a web browser window titled 'Activation'. It contains the following fields and text:

- User Name:** admin
- Password:** An empty text input field.
- Confirm:** An empty text input field.
- OK:** A button at the bottom right.
- Text below Password field:** 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.

Figure 2-3 Activation Interface (Web)

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



- *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 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. Confirm the password.
 5. Click **OK** to activate the camera and enter the live view interface.

◆ Activation via SADP Software

SADP software is used for detecting the online device, activating the device, 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 an inactive device.

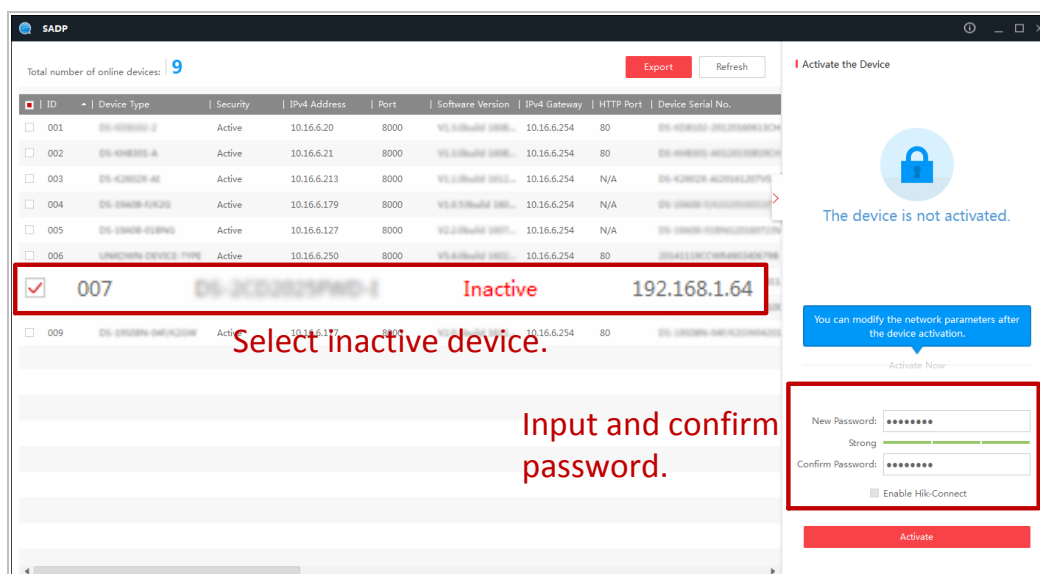


Figure 2-4 SADP Interface

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.



- *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 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 **Activate** to start activation. You can check whether the activation is completed on the popup window. If activation failed, make sure that the password meets the requirement and then 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 **Enable DHCP** checkbox.

Modify Network Parameters

Enable DHCP

Device Serial No.: XX-XXXXXXXX-XXXXXXXXXXXXXXXXXX

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: _____

Modify

[Forgot Password](#)

Figure 2-5 Modify the IP Address

6. Input the 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 Figure 2-6.

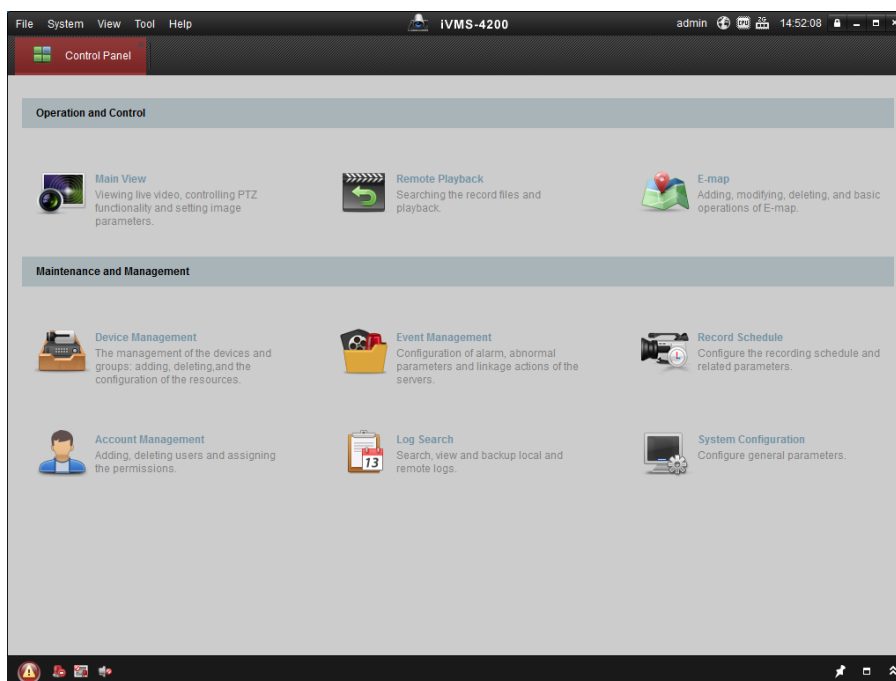


Figure 2-6 iVMS-4200 Control Panel

2. Click **Device Management** to enter Device Management interface, as shown in Figure 2-7.

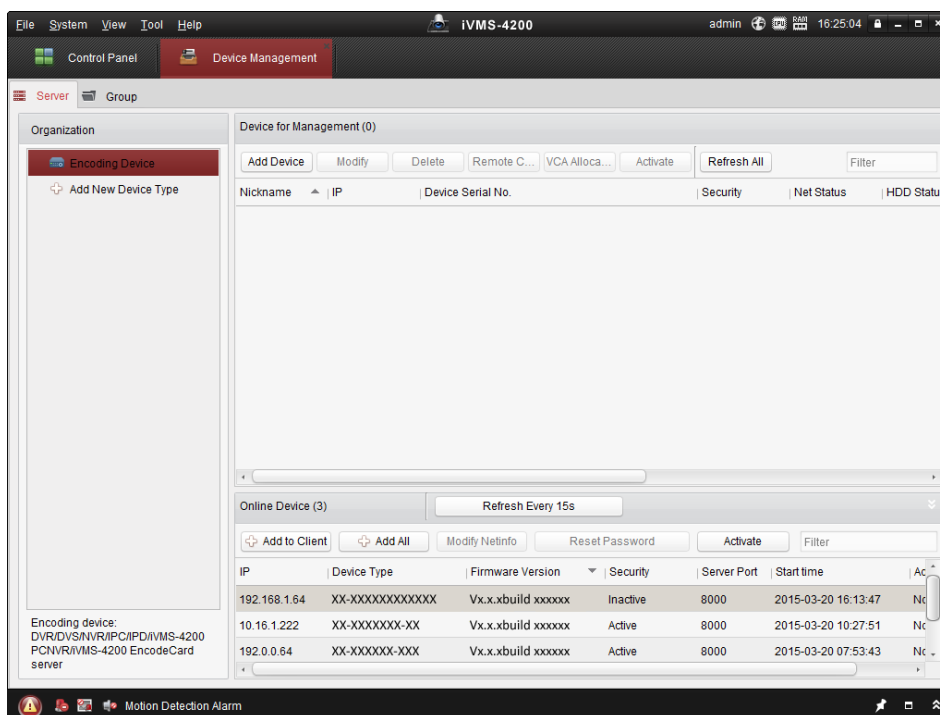
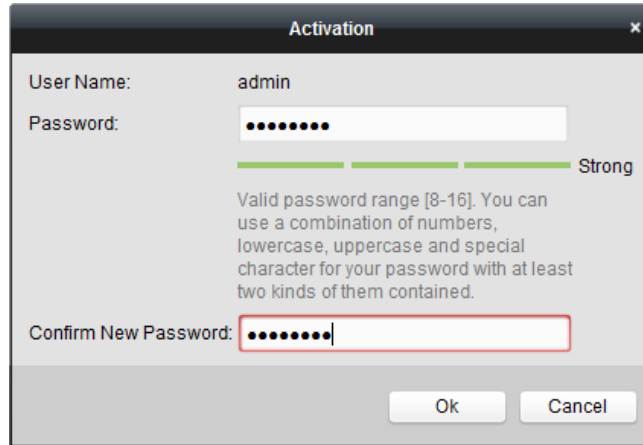


Figure 2-7 Device Management Interface

3. Check the device status from the device list, and select an inactive device.
4. Click **Activate** to pop up the Activation interface.
5. Create a password and input the password in the password field, and confirm the 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 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.

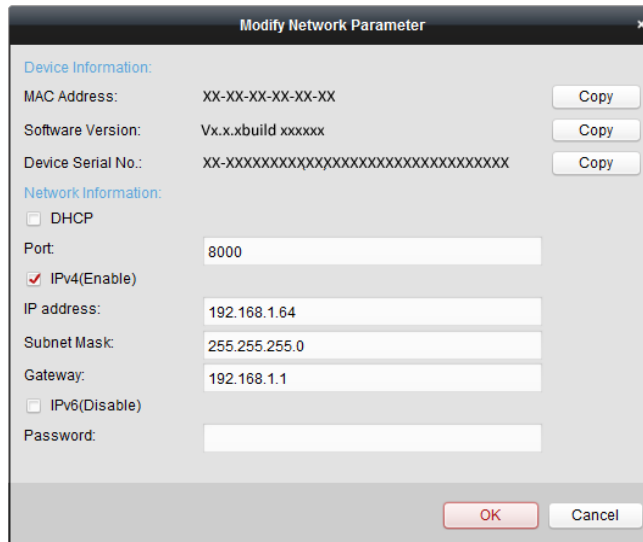


The image shows a dialog box titled "Activation". It contains the following fields and text:

- User Name: admin
- Password: [Redacted with dots]
- Strength indicator: A green progress bar is shown, labeled "Strong".
- Text: "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: [Redacted with dots]
- Buttons: "Ok" and "Cancel"

Figure 2-8 Activation Interface

6. Click **OK** to start activation.
7. Click **Modify Netinfo** to pop up the Network Parameter Modification interface, as shown in Figure 2-9.



The image shows a dialog box titled "Modify Network Parameter". It contains the following fields and text:

- Section: Device Information:
 - MAC Address: XX-XX-XX-XX-XX-XX [Copy]
 - Software Version: Vx.x.xbuild xxxxxx [Copy]
 - Device Serial No.: XX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX [Copy]
- Section: 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: [Redacted]
- Buttons: "OK" and "Cancel"

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.

2.1.3 (Optional) Setting Security Question

Security question is used to reset the admin password when admin user forgets the password. Admin user can follow the pop-up window to complete security question settings during camera activation. Or, admin user can go to User Management interface to set up the function.

2.2 Setting 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:

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

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

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 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 depending on different routers. Call the router manufacturer for assistance with port mapping.
5. Visit the network camera through a web browser or the client software over the internet.

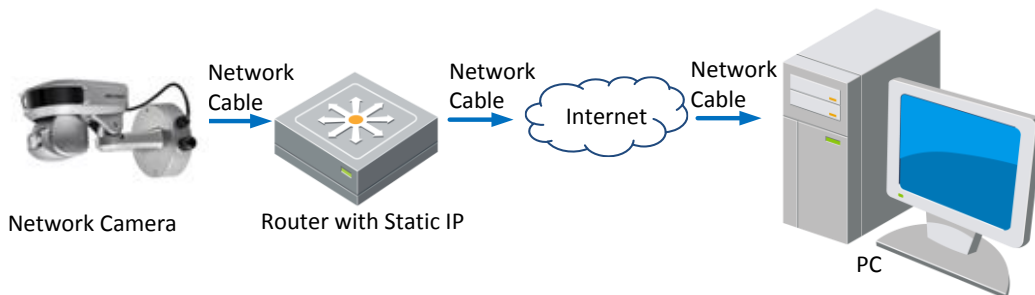


Figure 2-10 Accessing the Camera through Router with Static IP

- **Connecting the network camera with static IP directly**

You can also save the static IP in the camera and directly connect it to the internet without using a router. Refer to **Section 2.1.2** for detailed IP address configuration of the camera.

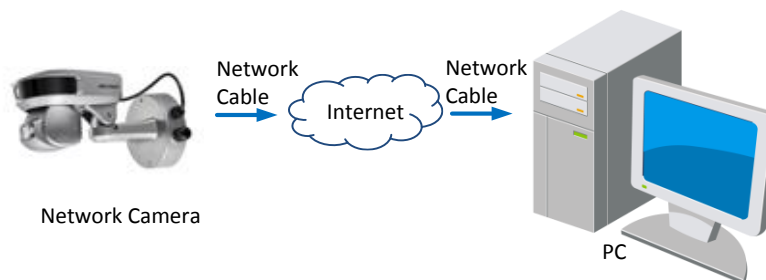


Figure 2-11 Accessing the Camera with Static IP Directly

2.2.2 Dynamic IP Connection

Before you start:

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

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

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 LAN configuration.
3. In the router, set the PPPoE user name, password and confirm the 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 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 port mapping. E.g. 80, 8000 and 554 ports. The steps for port mapping vary depending on different routers. Call the router manufacturer for assistance with 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.

- **Connecting 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 6.1.1 Configuring PPPoE Settings** for detailed configuration.

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). Follow the steps below for normal domain name resolution and private domain name resolution to solve the problem.

◆ 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 6.1.1 Configuring DDNS Settings** for detailed configuration.
3. Visit the camera via the applied domain name.

Chapter 3 Accessing to the Network Camera

3.1 Accessing by Web Browsers

Steps:

1. Open the web browser.
2. In the address field, input the IP address of the network camera, e.g., 192.168.1.64 and press the **Enter** key to enter the login interface.
3. Activate the camera for the first time using, refer to the **section 2.1.2 Activating the Camera**.
4. Select English as the interface language on the top-right of login interface.
5. Input the user name and password and click .

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

Note:

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

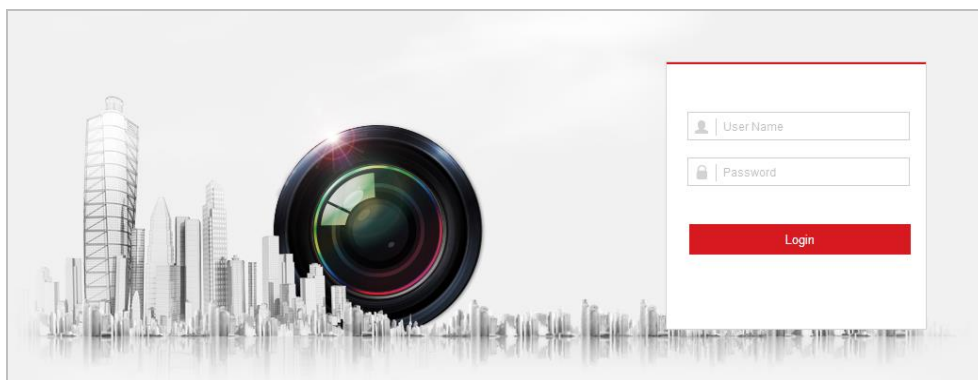


Figure 3-1 Login Interface

6. Install the plug-in before viewing the live video and operating the camera. Follow the installation prompts to install the plug-in.

Note:

You may have to close the web browser to install the plug-in. Reopen the web browser and log in again after installing the plug-in.

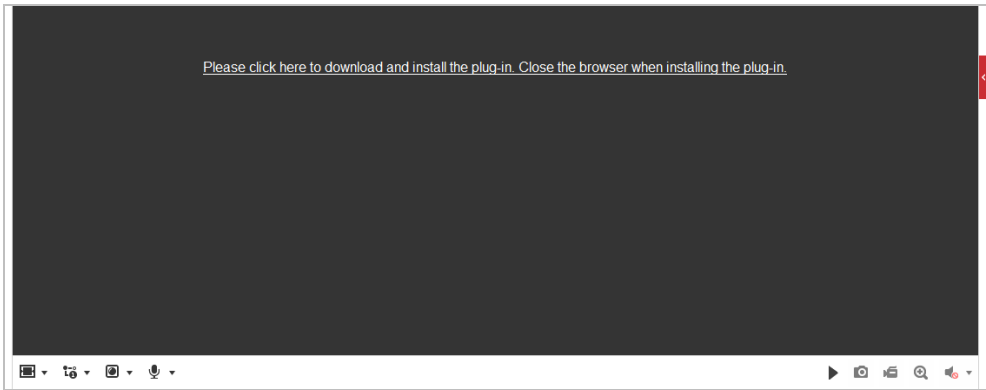


Figure 3-2 Download and Install Plug-in

3.2 Accessing by Client Software

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

Follow the installation prompts to install the client software and WinPcap. The configuration interface and live view interface of client software are shown in Figure 3-3.

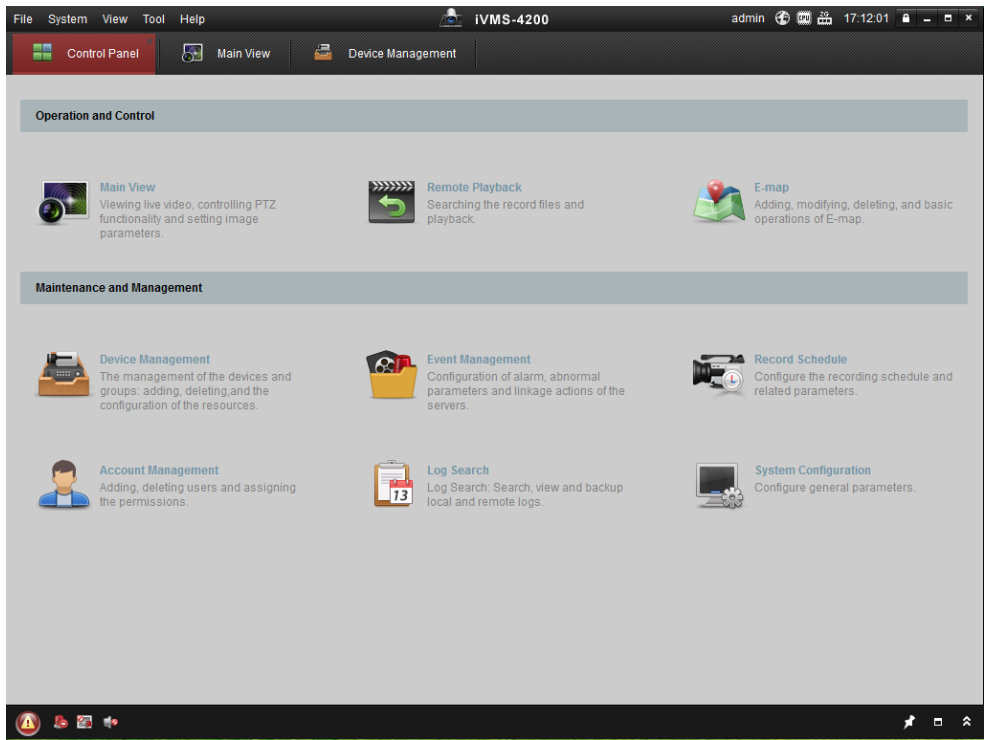


Figure 3-3 iVMS-4200 Control Panel

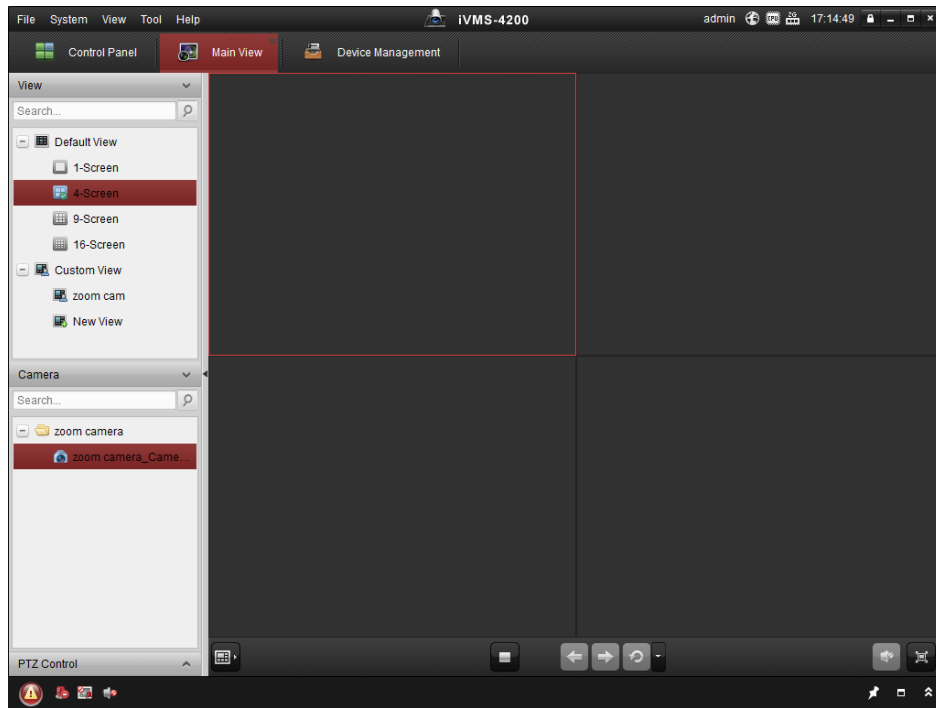


Figure 3-4 iVMS-4200 Live View Interface

Note:

- If you use third party VMS software, contact technical support of our branch for camera firmware.
- For detailed information about client software of our company, refer to the user manual of the software. This manual mainly introduces accessing to the network camera by web browser.

Chapter 4 Basic Operations

In this and the following chapters, operation of the camera by the web browser will be taken as an example.

4.1 Configuring Local Parameters

Note:

The local configuration refers to the parameters of the live view and other operations using the web browser.

Steps:

1. Enter Local Configuration interface:

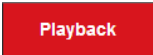

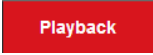
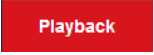

Configuration > Local

The screenshot shows the 'Local Configuration' interface with the following settings:

- Live View Parameters:**
 - Protocol: TCP, UDP, MULTICAST, HTTP
 - Play Performance: Shortest Delay, Balanced, Fluent, Custom
 - Rules: Enable, Disable
 - Display POS Information: Enable, Disable
 - Auto Start Live View: Yes, No
 - Image Format: JPEG, BMP
- Record File Settings:**
 - Record File Size: 256M, 512M, 1G
 - Save record files to: [Text Box] [Browse] [Open]
 - Save downloaded files to: [Text Box] [Browse] [Open]
- Picture and Clip Settings:**
 - Save snapshots in live vi...: [Text Box] [Browse] [Open]
 - Save snapshots when pla...: [Text Box] [Browse] [Open]
 - Save clips to: [Text Box] [Browse] [Open]

Figure 4-1 Local Configuration Interface

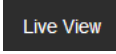
2. Configure the following settings:
 - **Live View Parameters:** Set the protocol type, play performance, rules and image format.
 - ◆ **Protocol Type:** TCP, UDP, MULTICAST and HTTP are selectable.
 - TCP:** Ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected.
 - UDP:** Provides real-time audio and video streams.
 - MULTICAST:** It's recommended to select the protocol type to **MULTICAST** when using the Multicast function.
 - HTTP:** Allows the same quality as of TCP without setting specific ports for streaming under some network environments.
 - ◆ **Play Performance:** Set the play performance to Shortest Delay, Balanced, Fluent, or Custom. For Custom, you can set the frame rate for live view.
 - ◆ **Rules:** You can enable or disable the rules of dynamic analysis for motion here.

- ◆ **Display POS Information:** When the detection is not accurate, you can enable **Display POS Information** and the video record will be automatically sent to the technician.
 - ◆ **Auto Start Live View:** Set it as Yes or NO. If this function is selected, live view will start automatically when you go to live view interface.
 - ◆ **Image Format:** The captured pictures can be saved as different format. JPEG and BMP are available.
 - **Record File Settings:** Set the saving path of the video files.
 - ◆ **Record File Size:** Select the packed size of manually recorded and downloaded video files. The size can be set to 256M, 512M or 1G.
 - ◆ **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  interface.
 - **Picture and Clip Settings:** Set the saving paths of the captured pictures and clipped video files.
 - ◆ **Save snapshots in live view to:** Set the saving path of the manually captured pictures in  interface.
 - ◆ **Save snapshots when playback to:** Set the saving path of the captured pictures in  interface.
 - ◆ **Save clips to:** Set the saving path of the clipped video files in  interface.
- Notes:**
- You can click **Browse** to change the directory for saving video files, clips and pictures.
 - You can click **Open** to directly open the video files, clips and pictures.
3. Click  to save the settings.

4.2 Live View Page

Purpose:

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

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

Note:

The functions vary depending on different camera models. Refer to the actual interface as standard.

Descriptions of the live view page:

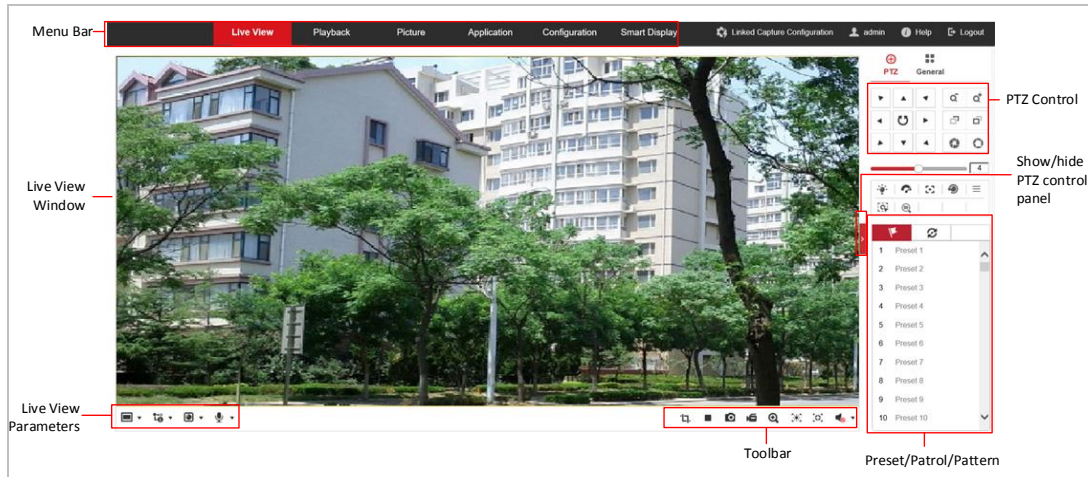




Figure 4-2 Live View Page

Menu Bar:

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

Click  to display the help file of the network camera.

Click  to logout the system.

Click  to enter quick setup, and follow the instruction to complete the settings of complex functions.

Live View Window:

Display the live video.

Toolbar:

Operations on the live view page, e.g., live view, capture, record, audio on/off, regional exposure, regional focus, etc.

PTZ Control:

Panning, tilting, focusing and zooming actions of the network. The lighter, wiper, one-touch focus and lens initialization control.

Preset/patrol/pattern:

Set and call the preset/patrol/pattern for the camera.

Live View Parameters:

Configure the image size, stream type, plug-in type, and two-way audio of the live video.

4.3 Starting Live View


In the live view window as shown in Figure 4-3, click  on the toolbar to start the live view of the network.



Figure 4-3 Start Live View

Table 4-1 Descriptions of the Toolbar

Icon	Description	Icon	Description
	Panoramic camera		Tracking PTZ camera
	Display in 1*1/2*2/PIP (Picture-in-Picture).		Live view with the main/sub/third stream.
	Start/stop two-way audio.		Start/stop all live view.
	Manually capture the pictures.		Start/stop all recording.
	Start/stop digital zoom.		Start POS information display
	Enable/disable regional focus		Enable/disable regional exposure
	Mute/audio on and adjust volume		Display in full screen

- Click to enable digital zoom function and the icon turns into . Then drag the mouse towards low right direction to draw a rectangle on the image as the desired zoom. After viewing it you can click any place of the picture to get back to normal picture.
- Click the on the toolbar to enter the regional exposure operation mode and the icon turns into . Then drag the mouse to draw a rectangle on the image as the desired exposure region.
- Click the on the toolbar to enter the regional focus operation mode and the icon turns into . Then drag the mouse to draw a rectangle on the image as the desired focus region.

Note:

Before using the two-way audio or recording with audio functions, set the **Stream Type** to **Video & Audio** referring to **Section 6.2.1 Configuring Video Settings**.

Refer to the following sections for more information:

- Configuring remote recording in **Section 5.1.1 Configuring Recording Schedule**.
- Setting the image quality of the live video in **Section 6.3 Configuring Image Settings** and **Section 6.2.1 Configuring Video Settings**.
- Setting the OSD text on live video in **Section 6.3.2 Configuring OSD Settings**.

4.4 Operating PTZ Control



Purpose:

In the live view interface, you can use the PTZ control buttons to control panning, tilting and zooming.

Note:

PTZ functions vary depending on different camera models.

4.4.1 PTZ Control Panel

On the live view page, click  to show the PTZ control panel or click  to hide it.

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

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

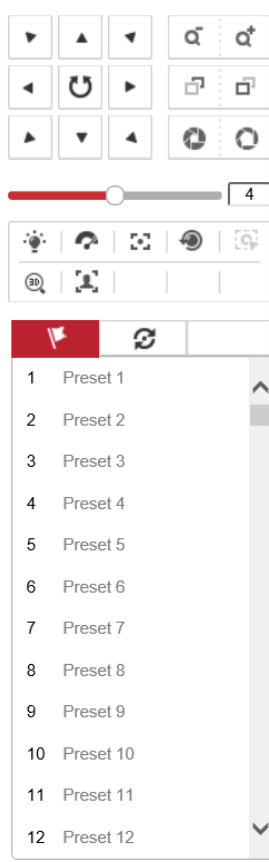




















Figure 4-4 PTZ Control Panel





Table 4-2 Descriptions of PTZ Control Panel

Button	Name	Description
	PTZ Control Panel	Hold and press the direction button to pan/tilt the camera. Click  and the camera keeps panning, the icon turns into  . Click the icon again to stop the camera.
	Zoom out/in	Click  , the lens zooms in, click  , and the lens zooms out.
	Focus near/far	Click  , the lens focus far and the items far away gets clear. Click  , the lens focus near and the items nearby gets clear.
	Iris close/open	When the image is too dark, click  to open the iris. When the image is too bright, click  to close the iris.
	Auxiliary Functions	The auxiliary functions include light, wiper, auxiliary focus, lens initialization, manual tracking, and 3D positioning.
	Speed Adjustment	Adjust speed of pan/tilt movements.
	Preset	Refer to 4.4.3 for detailed information of setting preset.
	Patrol	Refer to 4.4.4 for detailed information of setting patrol.

- **Buttons on the Preset/Patrol/Patterns interface:**

Table 4-3 Descriptions of Buttons

Buttons	Description
	Start the selected patrol/pattern.
	Stop current patrol/pattern.

	Set the selected preset/patrol.
	Delete the selected preset/patrol/pattern.
	Start recording a pattern.
	Stop recording the pattern.

4.4.2 Auxiliary Functions

The Auxiliary functions panel is shown in Figure 4-5.

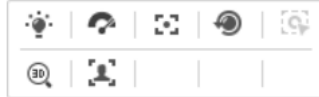









Figure 4-5 Auxiliary Functions

-  Light
Click  to enable/disable the light supplement of the camera. This function is reserved.
-  Wiper
Click  to move the wiper once.
-  Auxiliary Focus
The auxiliary focus function is reserved.
-  3D Positioning

Steps:

1. Click  on the toolbar of live view interface.
2. Operate the 3D positioning function:
 - Click a position of the live video. The corresponding position will be moved to the center of the live video.
 - 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.
 - 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.

4.4.3 Setting/Calling a Preset

Purpose:

A preset is a predefined image position. For the defined preset, you can click the calling button to quickly view the desired image position.

- **Setting a Preset:**

Steps:

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

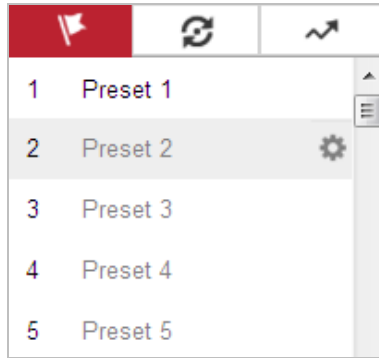




Figure 4-6 Setting a Preset

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. Edit a preset name by double clicking on the default name such as preset 1. (The pre-defined presets are named already and not configurable. Refer to the user manual for detailed function description.)
5. You can click  to delete the preset.

Note:

You can configure up to 256 presets.

- **Calling a Preset:**

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

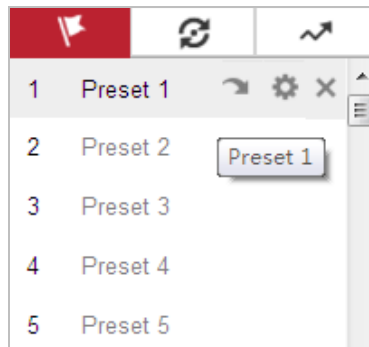


Figure 4-7 Calling a Preset

For convenient preset selection, refer to the following steps to navigate to the preset you want.

Steps:

1. Select any preset from the list.
2. Click the preset number you need on the keyboard.

Notes:

- The following presets are predefined with special commands. You can only call them but not configure them. For instance, preset 34 is the “Back to origin”. If you call the preset 34, the camera moves to the initial position.
- Pattern function varies depending on different camera models.

Table 4-4 Special Presets

Preset	Function	Preset	Function
34	Back to initial position	93	Save manual limits
35	Call patrol 1	94	Remote reboot
36	Call patrol 2	102	Call patrol 5
37	Call patrol 3	103	Call patrol 6
38	Call patrol 4	104	Call patrol 7
39	Day mode (IR cut filter in)	105	Call patrol 8
40	Night mode (IR cut filter out)	106	Fan normally open
46	Day/Night Auto Mode	107	Fan normally close
92	Set manual limits	108	Fan temp ctrl

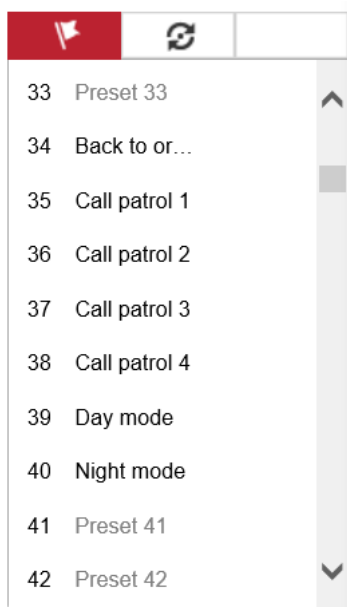


Figure 4-8 Special Preset

4.4.4 Setting/Calling a Patrol

Purpose:



A patrol is a memorized series of preset function. It can be configured and called on the patrol settings interface. There are up to 8 patrols for customizing. A patrol can be configured with 32 presets.

Before you start:

Make sure that the presets you want to add into a patrol have been defined.

● **Setting a Patrol:**

Steps:

1. In the PTZ control panel, click  to enter the patrol settings interface.
2. Select a patrol number from the list and click .

3. Click **+** to enter the adding interface of preset, as shown in Figure 4-9.



Figure 4-9 Adding Presets

4. Configure the preset number, patrol time and patrol speed.

Name	Description
Patrol Time	It is the duration staying on one patrol point. The camera moves to another patrol point after the patrol time.
Patrol Speed	It is the speed of moving from one preset to another.

5. Click **OK** to save a preset into the patrol.
 6. Repeat the steps from 3 to 5 to add more presets.
 7. Click **OK** to save all the patrol settings.

● **Calling a Patrol:**

In the PTZ control panel, select a defined patrol from the list and click **▶** to call the patrol, as shown in Figure 4-10.

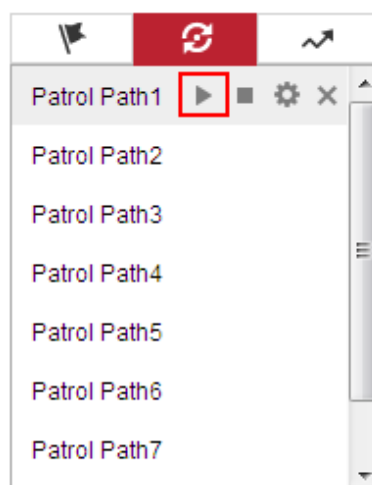


Figure 4-10 Calling a Preset

4.5 Playback

Purpose:

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

4.5.1 Play Back Video Files

Steps:

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

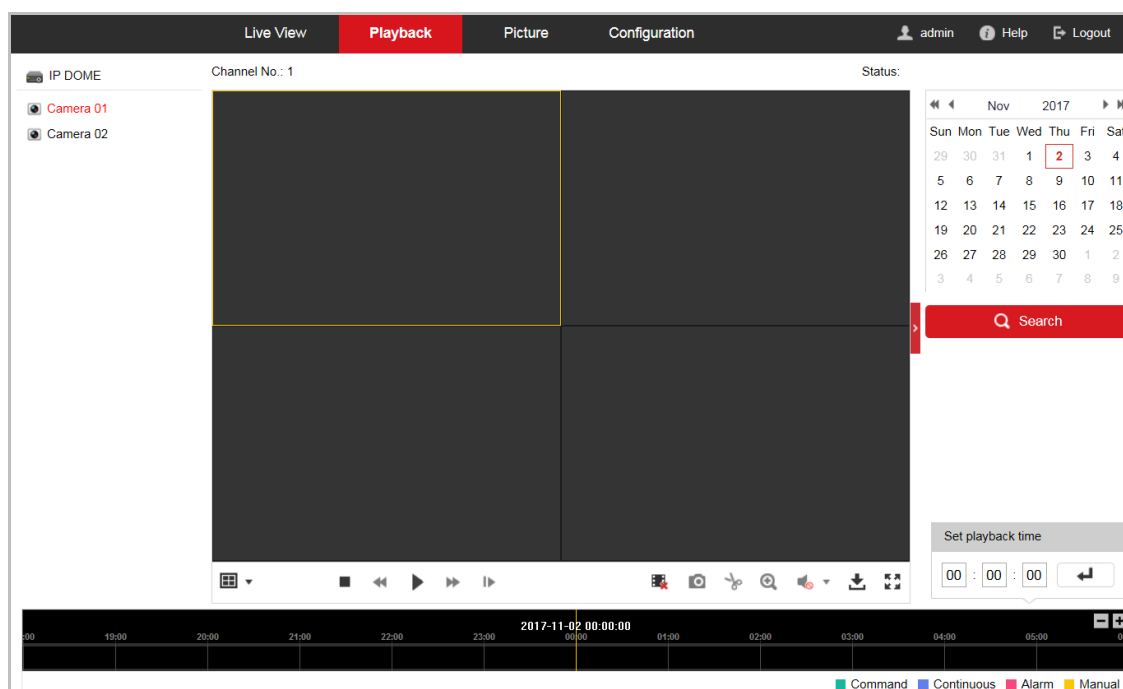


Figure 4-11 Playback Interface

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

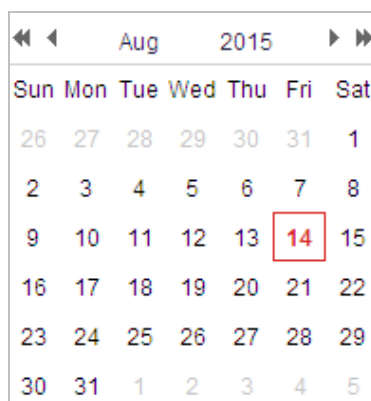



Figure 4-12 Search Video













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 4-13 Playback Toolbar

Table 4-5 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
	Enable/Disable digital zoom		Stop all playback

Note:

You can choose the file paths locally for downloaded playback video files and pictures in Local Configuration interface. Refer to **Section 4.1 Configuring Local Parameters** for details.

Drag the progress bar with the mouse to locate the exact playback point. 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.

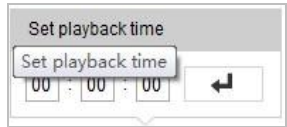


Figure 4-14 Set Playback Time

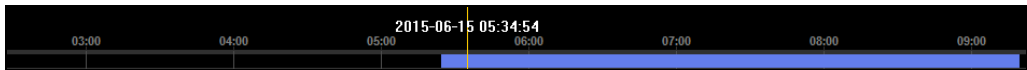


Figure 4-15 Progress Bar

The different colors of the video on the progress bar stand for the different video types as shown in Figure 4-16.

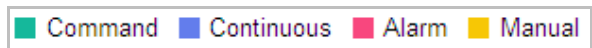



Figure 4-16 Video Types

4.5.2 Downloading Video Files

Steps:

1. Click  on the playback interface. The pop-up menu is shown in Figure 4-17.
2. Set the start time and end time. Click **Search**. The corresponding video files are listed on the left.

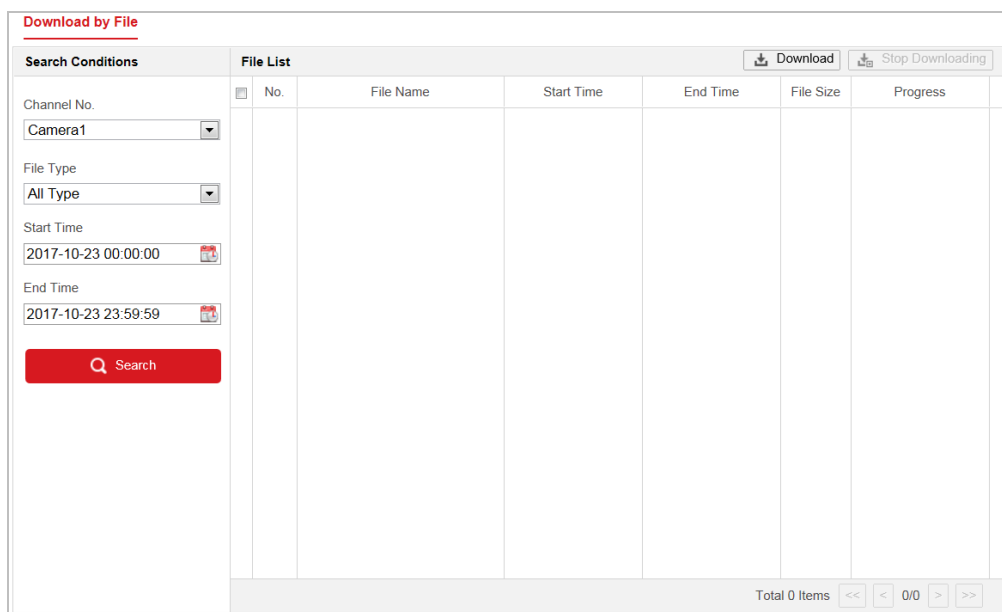
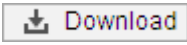


Figure 4-17 Video Downloading interface

3. Check the checkbox in front of the video files that you need to download.
4. Click  to download the video files.

4.6 Pictures

Purpose:

This section explains how to view the captured picture files stored in the network disks or the memory cards and download the captured pictures.

Steps:

1. Click  on the menu bar to enter picture interface.

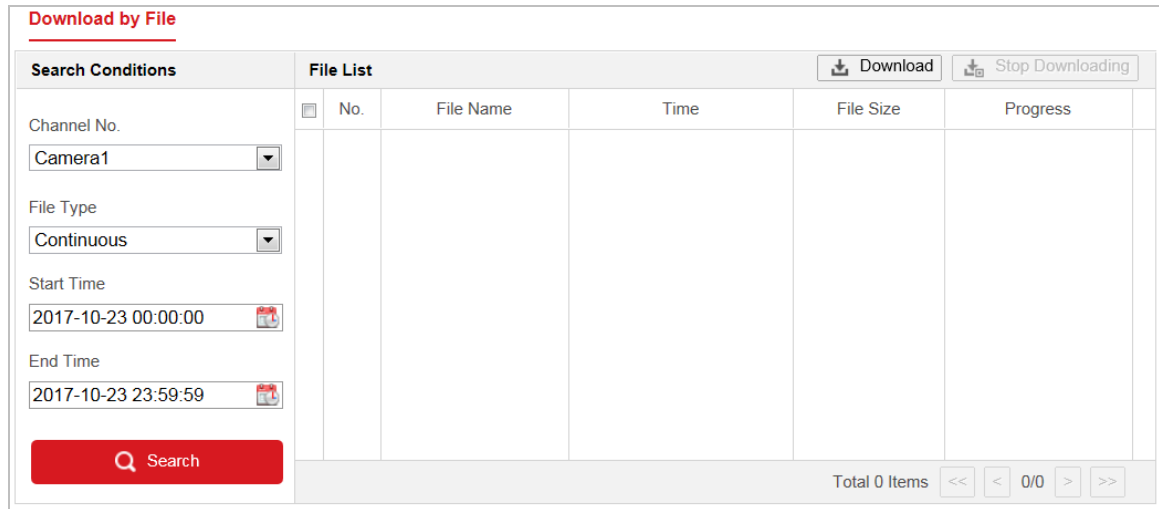
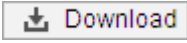


Figure 4-18 Picture Interface

2. Select the file type of capturing the pictures from the list as timing, alarm, motion, etc.
3. Set the start time and end time. Click **Search**. The corresponding picture files will be listed.
4. Check the checkbox in front of the files that you need to download.
5. Click  **Download** to download the files.

4.7 Smart Display

Click  **Smart Display** to display captured pictures in smart functions.






Note:

The function requires the support of camera and certain web browser. Adjust your browser settings according to the pop-up notification.


Preview Mode

Choose a mode to preview captured pictures.


Table 4-6 Description of the icons

Icon	Description
	View the captured pictures in single window.
	View the captured pictures in two window.
	Select different channel.
	View the captured pictures in Camera 01.
	View the captured pictures in Camera 02.

Layout

Click  to show the configuration page, and click **Layout** to check the picture kind as you needed.

Detect Feature

Click  to show the configuration page, and click **Detect Feature** to check corresponding features.

Chapter 5 System Configuration

5.1 Storage Settings

Before you start:

To configure record settings, make sure that you have the network storage device within the network or the memory card inserted in your camera.

5.1.1 Configuring Recording Schedule

Purpose:

There are two kinds of recording for the camera: 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 memory card (if supported) or in the network disk.

Steps:

1. Enter Record Schedule settings interface:

Configuration > Storage > Schedule Settings > Record Schedule

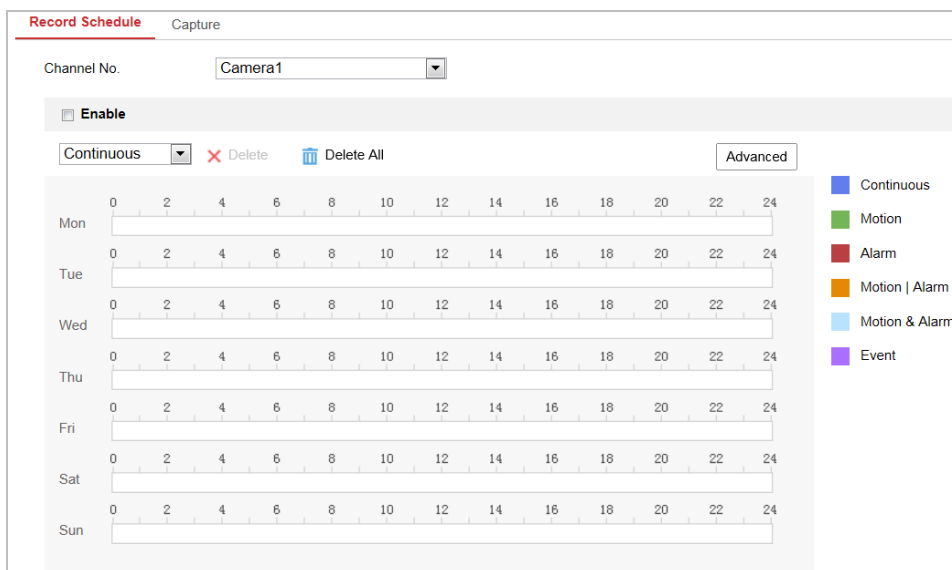


Figure 5-1 Recording Schedule Interface

2. Select the camera channel No. from the dropdown list.
3. Check the checkbox of **Enable** to enable scheduled recording.
4. To set the advanced settings of the camera, click **Advanced** to enter the advanced settings interface.

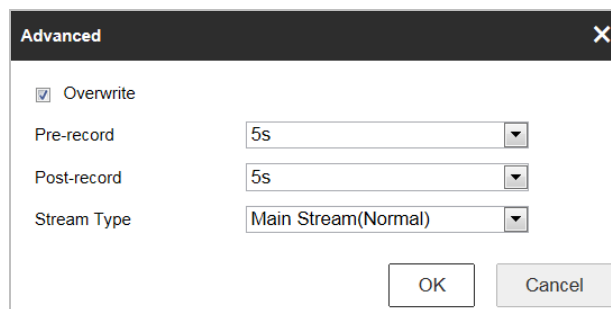


Figure 5-2 Record Parameters

- **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, 5 s, 10 s, 15 s, 20 s, 25 s, 30 s or not limited.

Note:

The pre-record time changes according to the video bitrate.

- **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 5 s, 10 s, 30 s, 1 min, 2 min, 5 min or 10 min.

- **Stream Type:** You can select the stream type for recording; Main Stream, Sub-Stream and Third Stream are selectable. If you select the sub-stream, you can record for a longer time with the same storage capacity.

Note:

The Pre-record and Post-record parameters vary depending on different camera models.

5. Click **OK** to save the advanced setting.
6. Select a Record Type. The record type can be Continuous, Motion, Alarm, Motion | Alarm, Motion & Alarm, and Event.
 - **Normal:** 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, 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, refer to Section **Motion Detection**.
 - **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, refer to Section **Alarm Input**.
 - **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.

- 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.
- Record Triggered by Event: If you select to record by event, the video will be recorded when any of the events is triggered.

7. Click  to save the settings.

5.1.2 Configuring 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. Enter Snapshot settings interface:

Configuration > Storage > Storage Settings > Capture

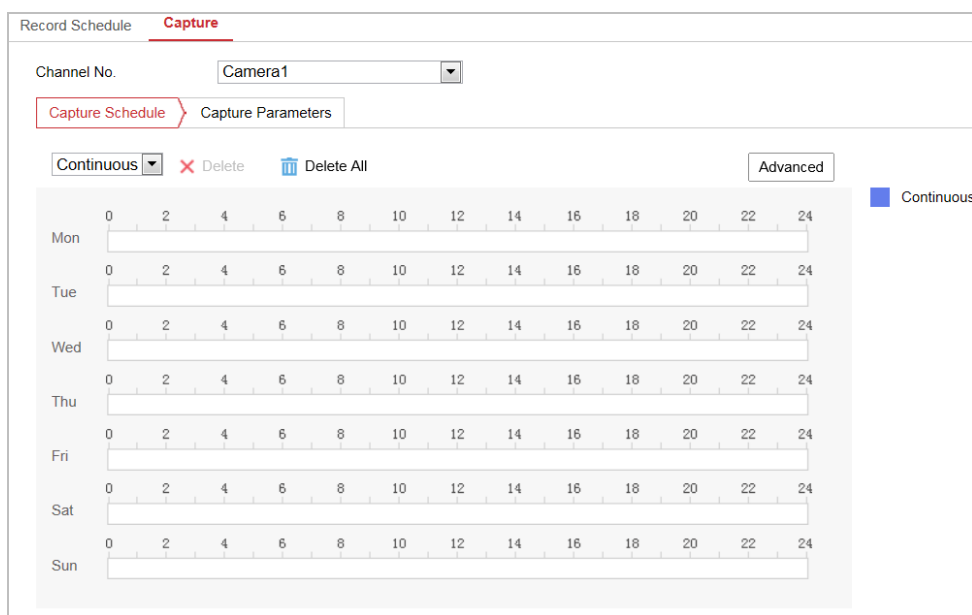




Figure 5-3 Snapshot Settings

2. Select the camera channel No. from the dropdown list.
3. Click  to enter Capture Schedule interface.
4. Select the timeline of a certain day, and drag the left button of the mouse to set the capture schedule (the start time and end time of the recording task).
5. After you set the scheduled task, you can click  and copy the task to other days (optional).
6. After setting the capture schedule, you can click a capture segment to display the segment capture settings interface to edit the segment capture parameters. (optional)

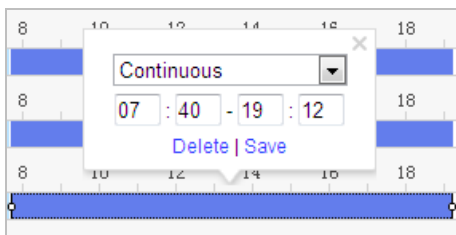


Figure 5-4 Segment Snapshot Settings

7. Click **Advanced** to enter the advanced setting interface. You can select the stream type of the capture.
8. Click **Capture Parameters** to enter Capture Parameters Interface.
9. Check the **Enable Timing Snapshot** checkbox to enable continuous snapshot, and configure the schedule of timing snapshot. Check the **Enable Event-triggered Snapshot** checkbox to enable event-triggered snapshot.
10. Select the format, resolution, quality of the snapshot.
11. Set the time interval between two snapshots.
12. Click **Save** to save the settings.

Uploading to FTP

Note:

Make sure that the FTP server is online.

You can follow below configuration instructions to upload the snapshots to FTP.

● Upload continuous snapshots to FTP

Steps:

- 1) Configure the FTP settings and check **Upload Picture** checkbox in FTP Settings interface. Refer to **Section 6.1.2 Configuring FTP Settings** for more details to configure FTP parameters.
- 2) Check the **Enable Timing Snapshot** checkbox.
- 3) Click **Edit** to set the snapshot schedule. Refer to **Section 5.2.1 Configuring Motion Detection**.

● Upload event-triggered snapshots to FTP

Steps:

- 1) Configure the FTP settings and check **Upload Picture** checkbox in FTP Settings interface. Refer to **Section 6.1.2 Configuring FTP Settings** for more details to configure FTP parameters.
- 2) Check **Upload to FTP** checkbox in Motion Detection Settings or Alarm Input interface. Refer to **Section 5.2.1 Configuring Motion Detection**.
- 3) Check the **Enable Event-triggered Snapshot** checkbox.

5.1.3 Configuring Net HDD

Before you start:

The network disk should be available within the network and properly configured to store the

recorded files, log files, etc.

Steps:

● **Add the network disk**

1. Enter NAS (Network-Attached Storage) 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	✘
Mounting Type <input type="text" value="SMB/CIFS"/> User Name <input type="text" value="cxy1"/> Password <input type="password" value="••••••"/> <input type="button" value="Test"/>				
2	10.10.36.252	/dvr/yanjian_1	NAS	✘
3			NAS	✘

Figure 5-5 Select Net HDD Type

2. Input the IP address and the file path of the network disk.
3. Select the mounting type. NFS and SMB/CIFS are selectable. You can set the user name and password to guarantee the security if SMB/CIFS is selected.

Note:

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 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  to add the network disk.

Note:

After having saved successfully, you need to reboot the camera to activate the settings.

● **Initialize the added network disk.**

1. Enter 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								Format
<input checked="" type="checkbox"/>	HDD No.	Capacity	Free space	Status	Type	Property	Progress	
<input checked="" type="checkbox"/>	9	9.84GB	0.00GB	Normal	NAS	R/W		
<input checked="" type="checkbox"/>	10	10.00GB	6.75GB	Normal	NAS	R/W		

Quota	
Max. Picture Capacity	<input type="text" value="4.50GB"/>
Free Size for Picture	<input type="text" value="0.00GB"/>
Max. Record Capacity	<input type="text" value="14.25GB"/>
Free Size for Record	<input type="text" value="6.75GB"/>

Figure 5-6 Storage Management Interface

- 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** as shown in Figure 5-7.

HDD Management								Set	Format
<input checked="" type="checkbox"/>	HDD No.	Capacity	Free space	Status	Type	Property	Progress		
<input checked="" type="checkbox"/>	9	20.00GB	0.00GB	Formatting	NAS	R/W			

Figure 5-7 View Disk Status

- **Define the Quota for Record and Pictures**

- Input the quota percentage for picture and for record.
- Click **Save** and refresh the browser page to activate the settings.

Quota	
Max. Picture Capacity	<input type="text" value="0.00GB"/>
Free Size for Picture	<input type="text" value="0.00GB"/>
Max. Record Capacity	<input type="text" value="0.00GB"/>
Free Size for Record	<input type="text" value="0.00GB"/>
Percentage of Picture	<input type="text" value="25"/> %
Percentage of Record	<input type="text" value="75"/> %

Figure 5-8 Quota Settings

Note:

- Up to 8 NAS disks can be connected to the camera.
- To initialize and use the memory card after insert it to the camera, refer to the steps of NAS disk initialization.

5.1.4 Configuring Cloud Storage

Purpose:

The captured pictures can be saved on cloud in order to view and analysis pictures faster.

Figure 5-9 Cloud Storage configuration

Step:

1. Enter Cloud Storage setting interface:
Configuration > Storage > Storage Management > Cloud Storage
2. Input the IP address and port of the storage server.
3. Input the user name, password and confirm password for the authentication of the storage server via **Cloud 1.0**. Input AccessKey and SecretKey via **Cloud2.0**.
4. Input picture storage pool ID on the server.
5. (Optional) You can click **Test** to test the cloud storage settings.
6. Click **Save** to save the settings.



5.2 Basic Event Configuration

Purpose:

This section explains how to configure the network camera to respond to alarm events, including motion detection, video tampering alarm input, alarm output and exception. These events can trigger the alarm actions, such as Send Email, Notify Surveillance Center, etc.

For example, when motion detection is triggered, the network camera sends a notification to an e-mail address.

Notes:

- On the event configuration page, click  to show the PTZ control panel or click  to hide it.
- Click the direction buttons to control the pan/tilt movements.
- Click the zoom/iris/focus buttons to realize lens control.
- The functions vary depending on different camera models.

5.2.1 Configuring Motion Detection

Purpose:

Motion detection is a feature which can trigger alarm actions and actions of recording videos when the motion occurred in the video security scene.

Steps:

1. Enter Motion Detection setting interface:

Configuration > Event > Basic Event > Motion Detection

2. Check **Enable Motion Detection** to enable this function.
3. (Optional) Check **Enable Motion Detection in PTZ Control** to detect the target when the device is in PTZ movement.
4. You can check the **Enable Dynamic Analysis for Motion** checkbox if you want the detected object get marked with rectangle in the live view.
5. Select the configuration mode as **Normal** or **Expert** and set the corresponding motion detection parameters.

● Normal

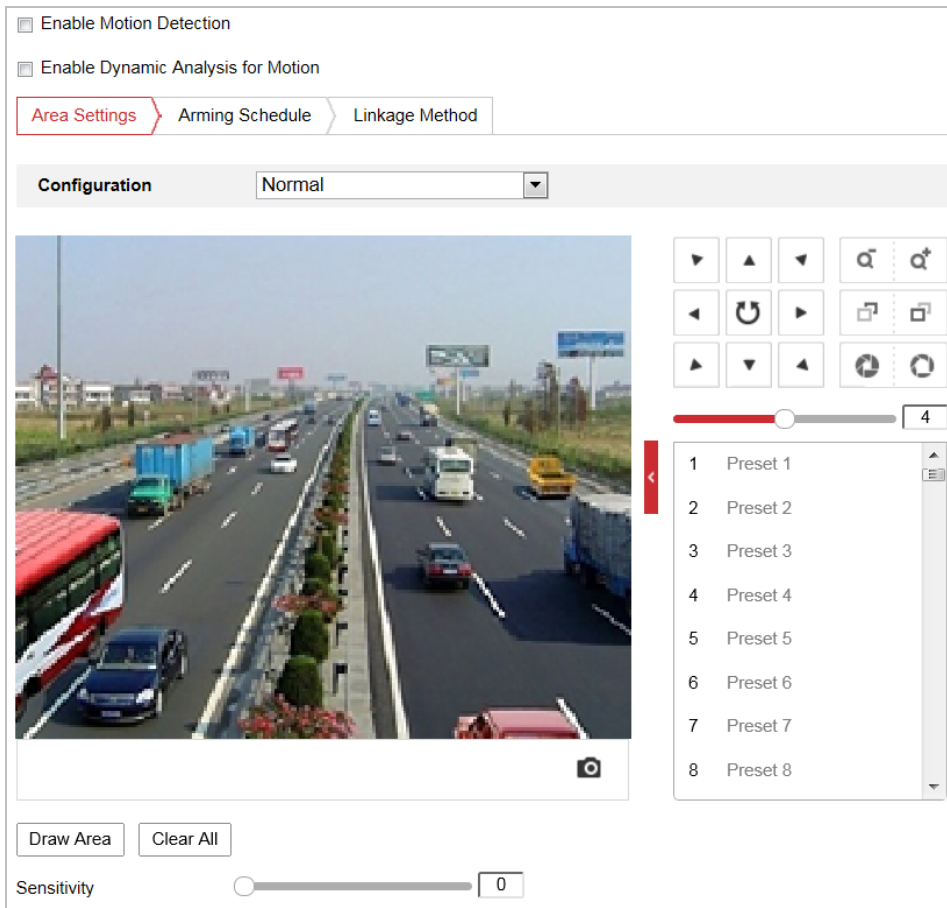


Figure 5-10 Motion Detection Settings-Normal

Steps:

- (1) Click **Draw Area** and drag the mouse on the live video image to draw a motion

detection area.

- (2) Click **Stop Drawing** to finish drawing.

Note:

You can click **Clear All** to clear all of the areas.

- (3) Move the slider **Sensitivity** to set the sensitivity of the detection.

● **Expert**

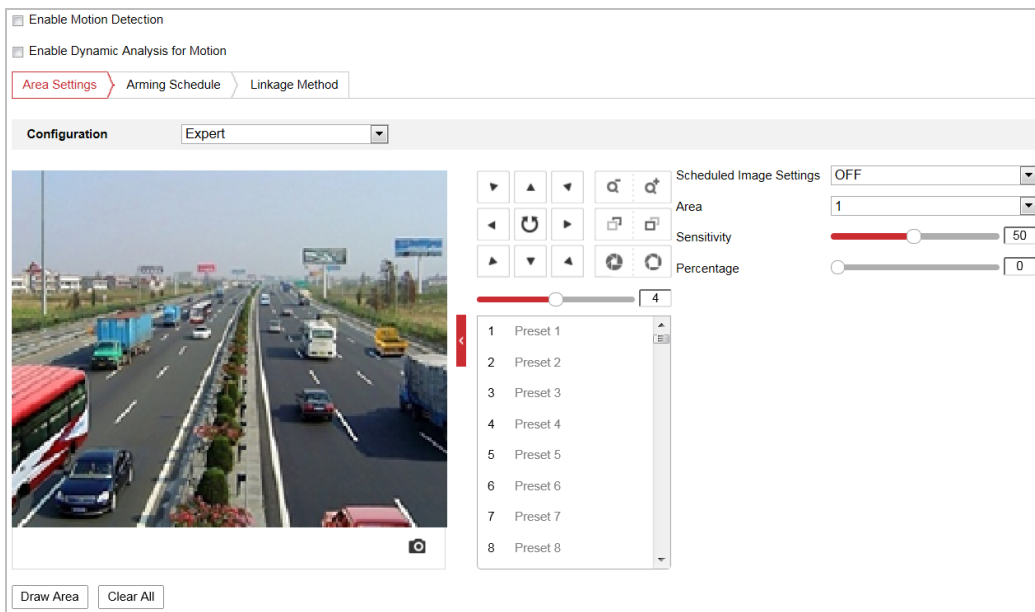


Figure 5-11 Motion Detection Settings-Expert

Steps:

- (1) Set the **Schedule Image Settings**, there are **OFF**, **Auto-Switch** and **Scheduled-Switch** selectable. If the schedule image switch mode is enabled, you can configure the detection rule for the day and night separately.

OFF: Disable the day and night switch.

Auto-Switch: Switch the day and night mode according to the illumination automatically.

Scheduled-Switch: Switch to the day mode and the night mode according to the configured time. You need to set the start time and end time.

- (2) Select **Area** from the dropdown list to configure.
 (3) Set the values of sensitivity and percentage.

Sensitivity: The greater the value is, the easier the alarm will be triggered.

Percentage: When the size proportion of the moving object exceeds the predefined value, the alarm will be triggered. The less the value is, the easier the alarm will be triggered.

6. Set the **Arming Schedule** for Motion Detection.

- (1) Click **Arming Schedule** tab to enter the arming schedule setting interface.



Figure 5-12 Arming Schedule


- (2) Select the timeline of a certain day, and drag the mouse to set the arming schedule (the start time and end time of the arming task).
- (3) After you set the scheduled task, you can click  and copy the task to other days (optional).



Figure 5-13 Arming Time Schedule

- (4) After setting the arming schedule, you can click a segment to display the segment arming settings interface to edit the segment record parameters (optional).

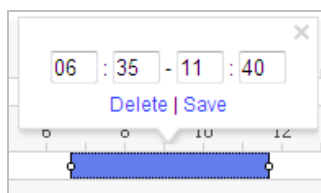


Figure 5-14 Segment Arming Settings

- (5) Click  to save the settings.

Note:

The time of each period cannot be overlapped. Up to 8 periods can be configured for each day.

7. Set the **Alarm Actions** for Motion Detection.

Click **Linkage Method** tab to enter **Linkage Method** interface.

You can specify the linkage method when an event occurs. The following contents are about how to configure the different types of linkage method.

<input type="checkbox"/> Normal Linkage	<input type="checkbox"/> Trigger Alarm Output	<input type="checkbox"/> Trigger Recording
<input type="checkbox"/> Send Email	<input type="checkbox"/> A->1	<input type="checkbox"/> A1
<input type="checkbox"/> Notify Surveillance Center		
<input type="checkbox"/> Upload to FTP/Memory Card/...		

Figure 5-15 Linkage Method

Check the checkbox to select the linkage method. Notify Surveillance Center, Send Email, Upload to FTP/Memory/NAS, Trigger Alarm Output and Trigger Recording are selectable.

- **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, you need to refer to **Section Configuring Email Settings** to set the Email parameters.

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

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

Note:

You need a FTP server and set FTP parameters first. Refer to **Section Configuring FTP Settings** for setting FTP parameters.

- **Trigger Alarm Output**

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

Note:

To trigger an alarm output when an event occurs, refer to **Section 5.2.4 Configuring Alarm Output** to set the alarm output parameters.

- **Trigger Recording**

Record a video when an event occurs.

Note:

You have to set the recording schedule to realize this function. Refer to **Section 5.1.1 Configuring Recording Schedule** for settings the recording schedule.

5.2.2 Configuring Video Tampering Alarm

Purpose:

You can configure the camera to trigger the alarm actions when the lens is covered.

Steps:

1. Enter Video Tampering settings interface :

Configuration > Event > Basic Event > Video Tampering

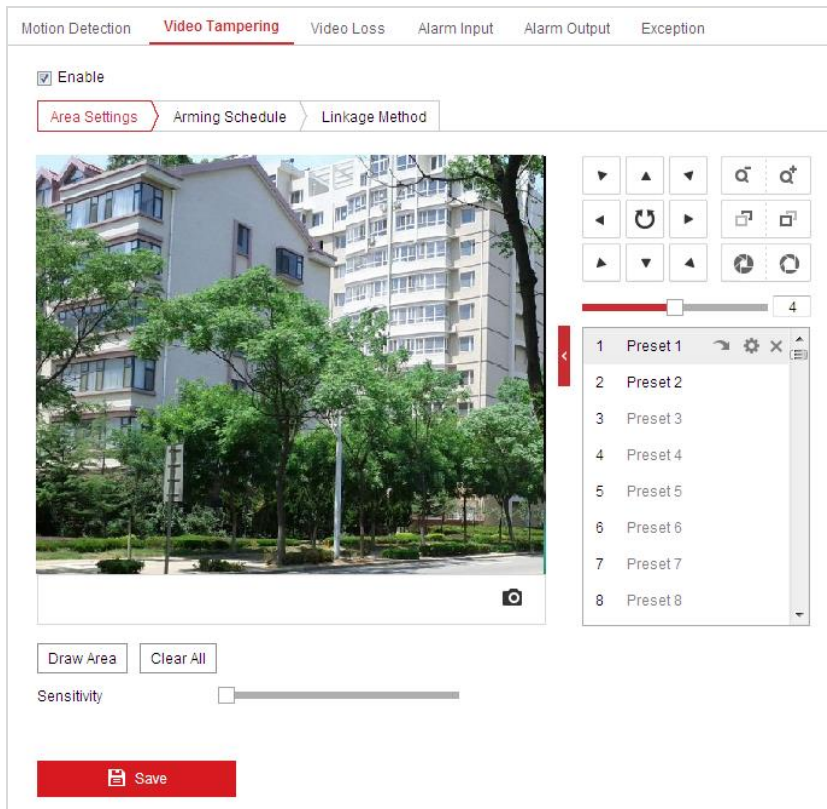


Figure 5-16 Tampering Alarm

2. Check **Enable** checkbox to enable the tampering detection.
3. Click **Arming Schedule** tab to enter the arming schedule setting interface. The arming schedule configuration is the same as the setting of the arming schedule for motion detection. Refer to **Section 5.2.1 Configuring Motion Detection**.

- Click **Linkage Method** tab to select the linkage method taken for tampering, notify surveillance center, send email and trigger alarm output are selectable. Refer to **Section 5.2.1 Configuring Motion Detection**.
- Click **Save** to save the settings.


5.2.3 Configuring Alarm Input

Steps:

- Enter Alarm Input settings interface:
Configuration > Event > Basic Event > Alarm Input
- Choose the Alarm Input No. and the Alarm Type. The alarm type can be NO (Normally Open) and NC (Normally Closed).
- Edit the name in **Alarm Name** (cannot copy) to set a name for the alarm input (optional).

Figure 5-17 Alarm Input Settings

- Click **Arming Schedule** tab to enter the arming schedule setting interface. The arming schedule configuration is the same as the setting of the arming schedule for motion detection. Refer to **Section 5.2.1 Configuring Motion Detection**.
- Click **Linkage Method** tab to select the linkage method taken for alarm input, including Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Alarm Output and Trigger Recording. Refer to **Section 5.2.1 Configuring Motion Detection**.
- You can also choose the PTZ linking for the alarm input. Check the relative checkbox and select the No. to enable Preset Calling, Patrol Calling or Pattern Calling.

7. You can copy your settings to other alarm inputs.
8. Click  to save the settings.

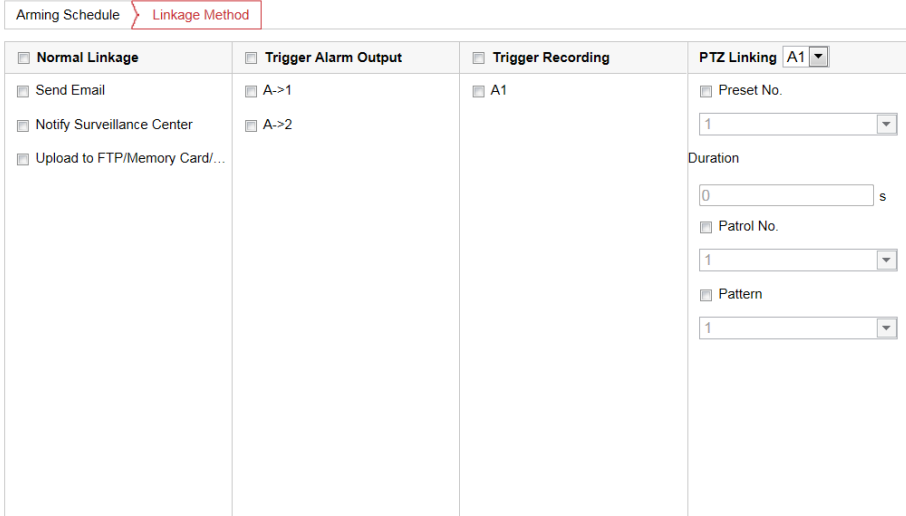



Figure 5-18 Linkage Method

5.2.4 Configuring Alarm Output

Steps:

1. Enter Alarm Output settings interface:
Configuration > Event > Basic Event > Alarm Output
2. Select one alarm output channel in the **Alarm Output** dropdown list.
3. Set a name in (cannot copy) for the alarm output (optional).
4. 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.
5. Click  tab to enter the arming schedule setting interface. The time schedule configuration is the same as the settings of the arming schedule for motion detection. Refer to **Section 5.2.1 Configuring Motion Detection**.

Alarm Output No. IP Address

Delay Alarm Name

Alarm Status (cannot copy)

Arming Schedule

Mon	0	2	4	6	8	10	12	14	16	18	20	22	24
Tue	0	2	4	6	8	10	12	14	16	18	20	22	24
Wed	0	2	4	6	8	10	12	14	16	18	20	22	24
Thu	0	2	4	6	8	10	12	14	16	18	20	22	24
Fri	0	2	4	6	8	10	12	14	16	18	20	22	24
Sat	0	2	4	6	8	10	12	14	16	18	20	22	24
Sun	0	2	4	6	8	10	12	14	16	18	20	22	24

Figure 5-19 Alarm Output Settings

- You can copy the settings to other alarm outputs.
- Click to save the settings.

5.2.5 Handling Exception

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

Steps:

- Enter Exception settings interface:
Configuration > Event > Basic Event > Exception
- Check the checkbox to set the actions taken for the Exception alarm. Refer to **Section 5.2.1 Configuring Motion Detection**.

Exception Type: HDD Full	
<input type="checkbox"/> Normal Linkage	<input type="checkbox"/> Trigger Alarm Output
<input type="checkbox"/> Send Email	<input type="checkbox"/> A->1
<input type="checkbox"/> Notify Surveillance Center	<input type="checkbox"/> A->2

Save

Figure 5-20 Exception Settings

3. Click Save to save the settings.

5.3 Smart Event Configuration

Purpose:

The event below explains how to configure the network camera to respond to smart alarm event. The event can trigger the alarm actions, such as Notify Surveillance Center, Send Email, etc. For example, when an external alarm is triggered, the network camera sends a notification to an email address.

5.3.1 Scene Change Detection

Purpose:

Scene change detection function detects the change of surveillance environment affected by the external factors; such as the intentional rotation of the camera, and some certain actions can be taken when the alarm is triggered.

Steps:

1. Enter the **Scene Change Detection** settings interface:

Configuration > Event > Smart Event > Scene Change Detection

2. Check **Enable** to enable the function.
3. Click and drag the slider to set the detection sensitivity. The higher the value is, the more easily the change of scene can trigger the alarm.
4. Click **Arming Schedule** to set the arming schedule. Refer to **Section 5.2.1 Configuring Motion Detection**.
5. Click **Linkage Method** to select the linkage methods. Refer to **Section 5.2.1 Configuring Motion Detection**.
6. Click **Save** to save the settings.

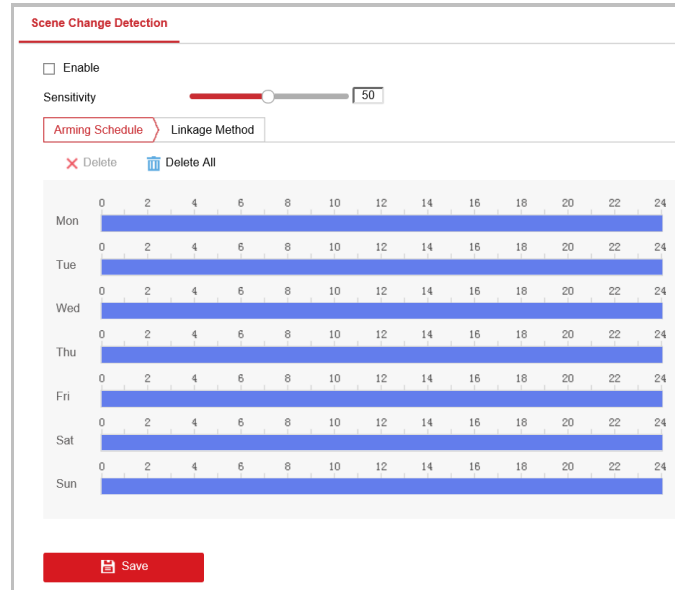




Figure 5-21 Scene Change Detection

5.4 PTZ Configuration

Note:

- On the event configuration page, click  to show the PTZ control panel or click  to hide it.
- Click the direction buttons to control the pan/tilt movements.
- Click the zoom/iris/focus buttons to realize lens control.
- The functions vary depending on different camera models.

5.4.1 Configuring Basic PTZ Parameters

You can configure the basic PTZ parameters, including proportional pan, preset freezing, preset speed, etc.

1. Enter Basic Settings interface:

Configuration > PTZ > Basic Settings


Basic Parameter	
<input checked="" type="checkbox"/>	Enable Proportional Pan
Preset Speed	4
Manual Control Speed	Auto
Keyboard Control Speed	Medium
Max. Tilt-angle	(-22 - 22)Degree
Zooming Speed	3
PTZ OSD	
Zoom Status	2s
PT Status	2s
Preset Status	2s
Power Off Memory	
Set Resume Time Point	30s
	

Figure 5-22 Basic Settings

2. Configure the following settings:

- **Basic Parameters:** Set the basic parameters of PTZ.
 - ◆ **Proportional Pan:** If you enable this function, the pan/tilt speeds change according to the amount of zoom. When there is a large amount of zoom, the pan/tilt speed will be slower for keeping the image from moving too fast on the live view image.
 - ◆ **Preset Speed:** You can set the speed of a defined preset. The higher the value is, the faster you can call the preset.
 - ◆ **Manual Control Speed:** The manual control speed can be set as Compatible, Pedestrian, Non-motor Vehicle, Motor Vehicle or Auto.
 - ◆ Compatible: The control speed is same as the Keyboard Control Speed.
 - ◆ Pedestrian: Choose the **Pedestrian** when you monitor the pedestrians.
 - ◆ Non-motor Vehicle: Choose the **Non-motor Vehicle** when you monitor the non-motor vehicles.
 - ◆ Motor Vehicle: Choose the **Motor Vehicle** when you monitor the motor vehicles.
 - ◆ Auto: You are recommended to set it as **Auto** when the application scene of the camera is complicated.
 - ◆ **Keyboard Control Speed:** Define the speed of PTZ control by a keyboard as Low, Medium or High.
 - ◆ **Max. Tilt-angle:** Set the tilt-angle of the camera from the dropdown list.
 - ◆ **Zooming Speed:** The zoom speed is adjustable from level 1 to 3.
- **PTZ OSD:** Set the on-screen display duration of the PTZ status.
 - ◆ **Zoom Status:** Set the OSD duration of zooming status as 2 seconds, 5 seconds, 10 seconds, NC (Normally Closed), or NO (Normally Open).
 - ◆ **PT Status:** Set the azimuth angle display duration while panning and tilting as 2 seconds, 5 seconds, 10 seconds, NC (Normally Closed), or NO (Normally Open).
 - ◆ **Preset Status:** Set the preset name display duration while calling the preset as 2 seconds,

5 seconds, 10 seconds, NC (Normally Closed), or NO (Normally Open).

- **Power-off Memory:** The camera can resume its previous PTZ status or actions after it restarted from a power-off. You can set the time point of which the dome resumes its PTZ status. You can set it to resume the status of 30 seconds, 60 seconds, 300 seconds or 600 seconds before power-off.

3. Click  to save the settings.

5.4.2 Configuring PTZ Limits

Purpose:

The camera can be programmed to move within the configurable PTZ limits (left/right, up/down).


Steps:

1. Enter Limit configuration interface:

Configuration > PTZ > Limit



Figure 5-23 Configure the PTZ Limit

2. Click the **Enable Limit** checkbox and choose the limit type.
 - Manual Stops:** When manual limit stops are set, you can operate the PTZ control panel manually only in the limited video security area.
3. Click the PTZ control buttons to find the left/right/up/down limit stops; you can also call the defined presets and set them as the limits of the camera.
4. Click **Set** to save the limits or click **Clear** to clear the limits.
5. Click  to save the settings.

5.4.3 Configuring Initial Position

Purpose:

Initial position refers to the relative initial position of the device azimuth. You can set the initial position if you need to select one point in the scene as the base point.

- **Customize an Initial Position:**

Steps:

1. Enter the Initial Position configuration interface:

Configuration > PTZ > Initial Position

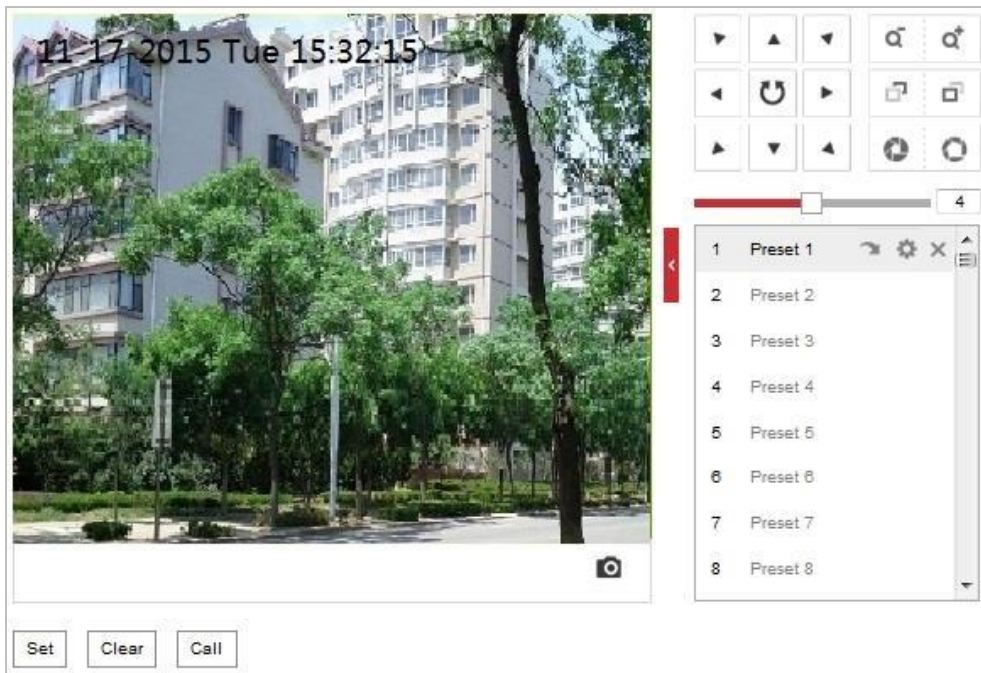


Figure 5-24 PTZ Configuration

2. Click the PTZ control buttons to find a position as the initial position of the speed dome; you can also call a defined preset and set it as the initial position of the speed dome.
3. Click **Set** to save the position.
4. Click **Call**, and the device moves to the set initial position.
5. You can click **Clear** to delete the set initial position.

5.4.4 Configuring Park Action

Purpose:

This feature allows the camera to start a predefined park action (preset and patrol) automatically after a period of inactivity (park time).

Notes:


- **Scheduled Tasks** function is prior to **Park Action** function. When these two functions are set at the same time, only the **Scheduled Tasks** function takes effect.
- Park function varies depending on different camera models.

Steps:

1. Enter Park Action settings interface:

Configuration > PTZ > Park Action

Figure 5-25 Set the Park Action

2. Check the **Enable Park Action** checkbox.
3. Set the **Park Time** as the inactivity time of the camera before it starts the park actions.
4. Choose the **Action Type** from the dropdown list. If you select **Patrol** or **Preset** as Action Type, you need to select **Action Type ID** from the dropdown list.
5. Click  **Save** to save the settings.

5.4.5 Configuring Scheduled Tasks

Purpose:

You can configure the network camera to perform a certain action automatically in a user-defined time period.


Steps:

1. Enter Scheduled Task settings interface:

Configuration > PTZ > Scheduled Tasks

Figure 5-26 Configure Scheduled Tasks

2. Check the **Enable Scheduled Task** checkbox.
3. Set the **Park Time**. You can set the park time (a period of inactivity) before the camera starts the scheduled tasks.

4. Select the task type from the dropdown list.
5. Select the timeline of a certain day, and drag the mouse to set the recording schedule (the start time and end time of the recording task).
6. After you set the scheduled task, you can click  and copy the task to other days (optional).

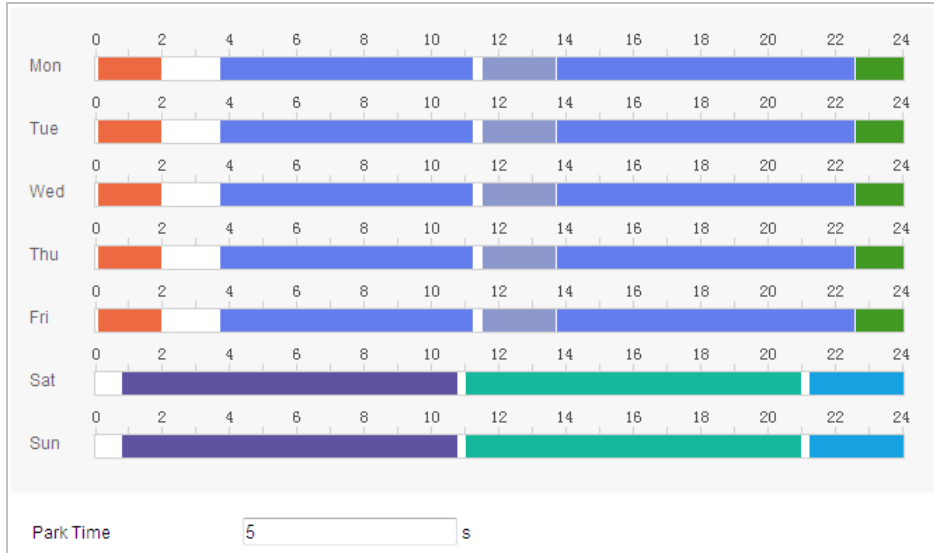


Figure 5-27 Edit the Schedule and Task Type

7. Click  to save the settings.

5.4.6 Clearing PTZ Configurations

Purpose:

You can clear PTZ configurations in this interface, including all presets, patrols, PTZ limits, scheduled tasks and park actions.

Steps:

1. Enter Clearing Configuration interface:
Configuration > PTZ > Clear Config
2. Check the checkbox of the items you want to clear.

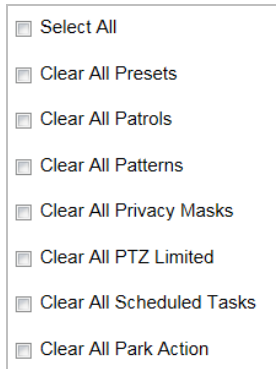


Figure 5-28 Clear Config

3. Click  Save to clear the settings.

5.4.7 Configuring Panorama Tracking

Note:

Panorama tracking function is not supported when face capture is enabled.

Purpose:

After you enable this function, when the camera detects the moving object in the panoramic view, the Camera 02 will track the detected target. Camera 02 automatically adjusts PTZ to ensure that the target is in the center of live view with detailed information.

Steps:

1. Enter Panorama Tracking settings interface:

Configuration > PTZ > Panorama Tracking

2. Check the **Track** check box to enable panorama tracking function.
3. Select the calibration mode and perform calibration.

- **Auto Calibration**


Steps:

- 1) Select the calibration mode as **Auto**.
- 2) Click **Start Calibration** and the calibration window pops up. The camera starts calibration automatically.
- 3) After calibration finished, click **Stop Calibration** and exit the calibration interface.


- **Manual Calibration**



Steps:

- 1) Select the calibration mode as Manual.
- 2) Select a calibration point in **Calibration Parameter** list.

A numbered green cross displayed on the panoramic image. Drag  to adjust its position.

- 3) Click **Add** to save the cross position on panoramic channel.
- 4) Adjust PTZ to place the green cross in the PTZ camera channel to the same position as

the green cross in panoramic camera channel. 1x is recommended. You can use  to quickly locate the desired point.

- a) Click  to enable the function.
 - b) Click the same point as the numbered crossed marked on panoramic camera channel.
The PTZ camera place the clicked point in the middle of the image automatically.
 - c) Click the button again to turn it off.
- 5) Click  to save current PTZ position and show in the calibration parameter list.
 - 6) Repeat the steps above to add more calibration points for the panoramic camera channel.

- 7) Click **Start Calibration**.
4. Click  to save the settings.

5.4.8 Configuring Rapid Focus

Purpose:

Enable rapid focus and configure calibration, the camera can focus rapidly.

Steps:

1. Check **Enable** to enable rapid focus function.
2. (Optional) If the mounting height of the camera is lower than 3 meters, check the **Enable Height Compensation** to guarantee focus accuracy.

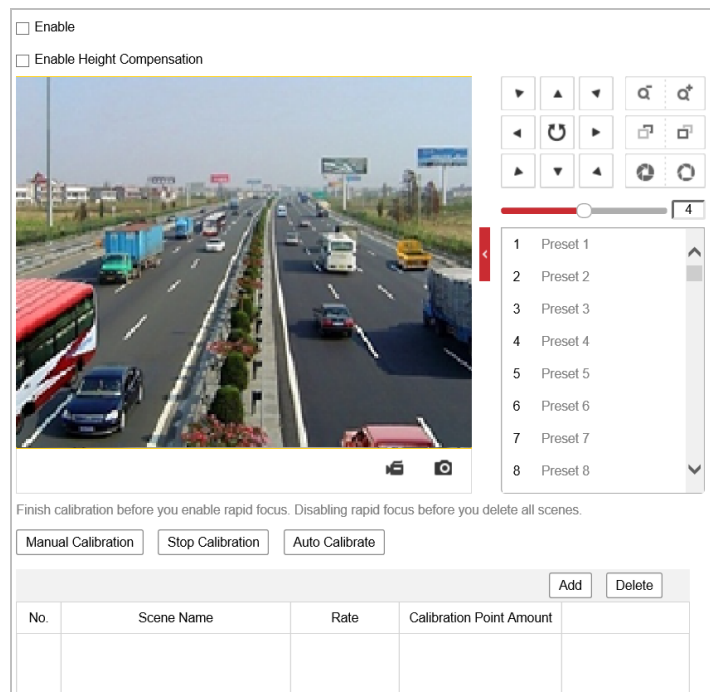


Figure 5-29 Configuring Rapid Focus

3. Calibrate the camera. There are two modes of calibration, manual and auto.
 - **Auto Calibration:** The device can automatically find the appropriate position to calibrate according to the area you drawn in panoramic channel.


Note:
Auto calibration will delete the current scene parameters.
 - **Manual Calibration**

Steps:

 - 1) Add scenes for calibration.
 - a) Adjust the camera to a desired scene via PTZ control buttons.
 - b) Click **Add** to add the scene, and input **Rate** and **Calibration Point Amount** of the scene.
 - c) Repeat above steps to add other scenes.
 - 2) Adjust calibration line.

- a) Select an added scene, and a red line displays on live image.
- b) Adjust the length and position of the line by dragging its two endpoints.

Note:

- The red line is recommended to stay in the center of the scene and to cover ground at the same time.
 - If the line is not in the center, use PTZ control to adjust the scene.
- 3) Click **Start Calibration**, and the calibration status displays on the live image.
 4. (Optional) Repeat the steps above to add more scenes and perform calibration for the scenes.
 5. Click  to save the settings.

Chapter 6 Camera Configuration

6.1 Configuring Network Settings

Note:

The functions vary depending on different camera models.

6.1.1 Basic Settings

Configuring TCP/IP Settings

Purpose:

TCP/IP settings must be properly configured before you operate the camera over network. IPv4 and IPv6 are both supported.

Steps:


1. Enter TCP/IP settings interface:

Configuration > Network > Basic Settings > TCP/IP

The screenshot displays the 'TCP/IP' configuration page. At the top, there are tabs for 'TCP/IP', 'DDNS', 'PPPoE', 'Port', and 'NAT'. The 'TCP/IP' tab is active. The settings are organized into several sections:

- NIC Type:** A dropdown menu set to 'Auto'.
- DHCP:** A checkbox that is currently unchecked.
- IPv4 Settings:**
 - IPv4 Address: 10.16.1.250 (with a 'Test' button)
 - IPv4 Subnet Mask: 255.255.255.0
 - IPv4 Default Gateway: 10.16.1.254
- IPv6 Settings:**
 - IPv6 Mode: A dropdown menu set to 'Route Advertisement' (with a 'View Route Advertisement' button)
 - IPv6 Address: ::
 - IPv6 Subnet Mask: 0
 - IPv6 Default Gateway: ::
- Other Settings:**
 - Mac Address: c0:56:e3:b3:bc:c0
 - MTU: 1500
 - Multicast Address: (empty field)
 - Enable Multicast Discovery
- DNS Server Section:**
 - Preferred DNS Server: 8.8.8.8
 - Alternate DNS Server: (empty field)

Figure 6-1 TCP/IP Settings

2. Configure the NIC settings, including the **IPv4(IPv6) Address**, **IPv4(IPv6) Subnet Mask** and **IPv4(IPv6) Default Gateway**.
3. Click  to save the above settings.

4. You can click **Test** to make sure that the IP address is valid.

Notes:

- If the DHCP server is available, you can check DHCP to automatically obtain an IP address and other network settings from that server.
- The valid value range of Maximum Transmission Unit (MTU) is 1280 to 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 and configure the gateway of the network camera.
- If the DNS server settings are required for some applications (e.g., sending email), you should properly configure the **Preferred DNS Server** and **Alternate DNS server**.

DNS Server	
Preferred DNS Server	8.8.8.8
Alternate DNS Server	

Figure 6-2 DNS Server Settings

Note:

The router must support the route advertisement function if you select **Route Advertisement** as the IPv6 mode.

Configuring DDNS Settings

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.



- *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 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. Enter 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, input the domain name obtained from the DynDNS website.
- (3) Input the **Port** of DynDNS server.
- (4) Input the **User Name** and **Password** registered on the DynDNS website.
- (5) Click  to save the settings.

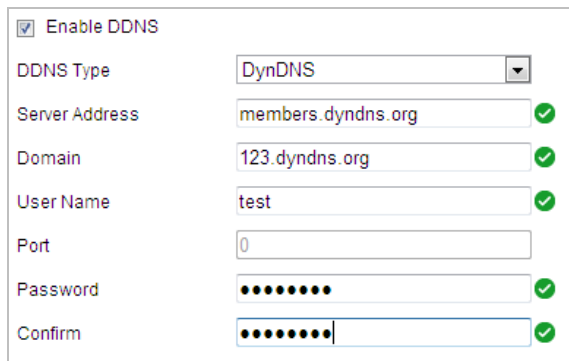



Figure 6-3 DynDNS Settings

- **NO-IP:**

Steps:

- (1) Enter **Server Address** of NO-IP.
- (2) In the **Domain** text field, input the domain name obtained from the NO-IP website.
- (3) Input the **Port** of NO-IP server.
- (4) Input the **User Name** and **Password** registered on the NO-IP website.
- (5) Click  to save the settings.

Configuring PPPoE Settings

Purpose:

If you have no router but only a modem, you can use Point-to-Point Protocol over Ethernet (PPPoE) function.

Steps:

1. Enter PPPoE settings interface:

Configuration > Network > Basic Settings > PPPoE



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 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  to save and exit the interface.

Configuring Port Settings

Purpose:

If there is a router and you want to access the camera through Wide Area Network (WAN), you need to forward the 3 ports for the camera.

Steps:

1. Enter Port settings interface:

Configuration > Network > Basic Settings > Port


TCP/IP	DDNS	PPPoE	Port	NAT
HTTP Port <input type="text" value="80"/>				
RTSP Port <input type="text" value="554"/>				
HTTPS Port <input type="text" value="443"/>				
Server Port <input type="text" value="8000"/>				
Enhanced SDK Service P... <input type="text" value="8443"/>				
WebSocket Port <input type="text" value="7681"/>				
WebSockets Port <input type="text" value="7682"/>				
 Save				

Figure 6-5 Port Settings

2. Set the HTTP port, RTSP port and port of the camera.
 - **HTTP Port:** The default port number is 80.
 - **RTSP Port:** The default port number is 554.
 - **HTTPS Port:** The default port number is 443.
 - **Server Port:** The default port number is 8000.

Note:

When you use client software to visit the camera and you have changed the server port number, you have to input the correct server port number in login interface to access to the camera.

- **Enhanced SDK Service Port:** The default server port number is 8443, and it can be

changed to any port number ranges from 2000 to 65535.

- **WebSocket Port:** The default port number is 7681.
- **WebSockets Port:** The default server port number is 7682.

Note:

WebSocket and WebSockets protocol are used for plug-in free live view. For detailed information, see **Network Service** in **Section 6.1.2**.

3. Click  to save the settings.

Configuring NAT (Network Address Translation) Settings

Purpose:

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 house 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. Enter UPnP™ settings interface.

Configuration > Network > Basic Settings > NAT

2. Check the checkbox to enable the UPnP™ function.

Note:

You can edit the **Friendly Name** of the camera. This name can be detected by corresponding device, such as a router.

3. Set the port mapping mode:

To port mapping with the default port numbers:

Choose **Port Mapping Mode**

To port mapping with the customized port numbers:

Choose **Port Mapping Mode**

And you can customize the value of the port number by yourself.

<input type="checkbox"/> Enable UPnP™				
Friendly Name		<input type="text" value="HIKVISION IDS-2PT9144MXS-D"/>		
Port Mapping Mode		<input type="text" value="Auto"/>		
Port Type	External Port	External IP Address	Internal Port	Status
HTTP	80	0.0.0.0	80	Not Valid
HTTPS	443	0.0.0.0	443	Not Valid
RTSP	554	0.0.0.0	554	Not Valid
Server Port	8000	0.0.0.0	8000	Not Valid
Enhanced SDK Se	8443	0.0.0.0	8443	Not Valid
Websocket	7681	0.0.0.0	7681	Not Valid
Websockets	7682	0.0.0.0	7682	Not Valid

Figure 6-6 Port Mapping Mode

4. Click  to save the settings.

6.1.2 Advanced Settings

Configuring SNMP Settings

Purpose:

You can use SNMP to get camera status and parameters related information.

Before you start:

Before setting the SNMP, use 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.

Steps:

1. Enter SNMP settings interface:

Configuration > Network > Advanced Settings > SNMP

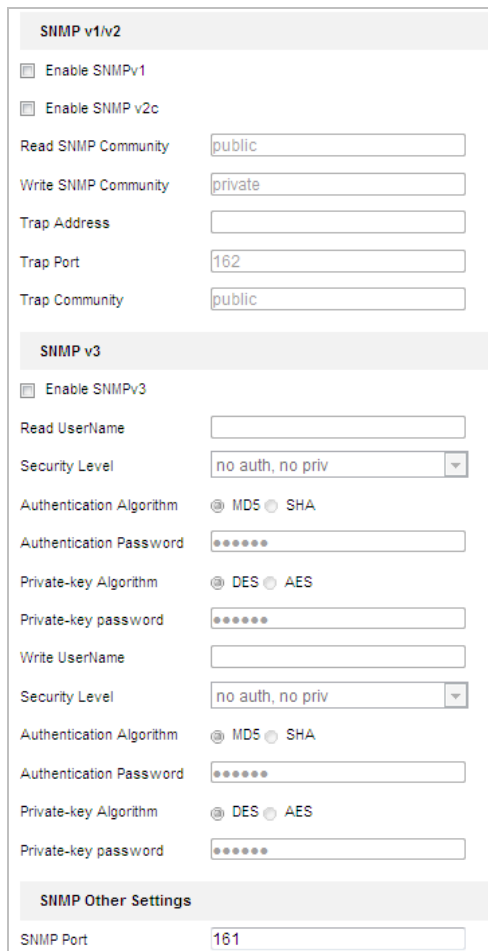


Figure 6-7 SNMP Settings


2. Check the corresponding version checkbox (**Enable SNMP v1**, **Enable SNMP v2c**, **Enable**

SNMP v3) to enable the feature.

- Configure the SNMP settings.

Note:

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

- Click  to save and finish the settings.

Configuring FTP Settings

Purpose:

You can set a FTP server and configure the following parameters for uploading captured pictures.

Steps:

- Enter FTP settings interface:

Configuration > Network > Advanced Settings > FTP

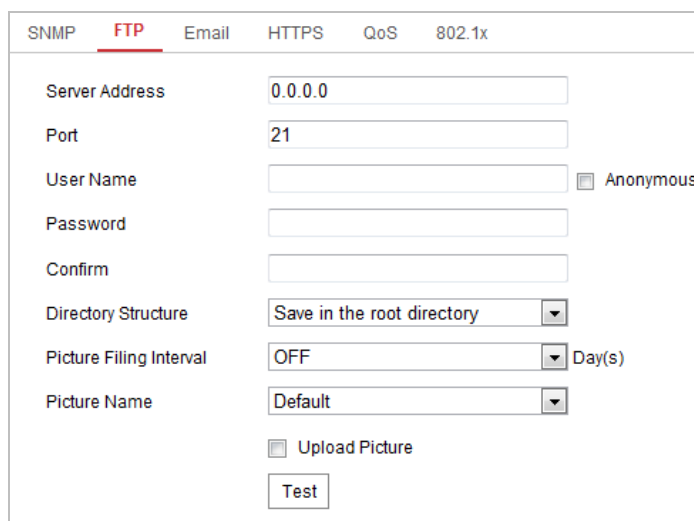


Figure 6-8 FTP Settings

- Configure the FTP settings, including server address, port, user name, password, directory, and upload type.

Note:

The server address supports both the domain name and IP address formats.



- 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 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.
- Setting the directory in FTP server for saving files:**

In the **Directory Structure** field, you can select the root directory, parent directory and child directory.

- ◆ **Root directory:** The files will be saved in the root of FTP server.
- ◆ **Parent directory:** The files will be saved in a folder in FTP server. The name of folder can be defined as shown in Figure 6-9.

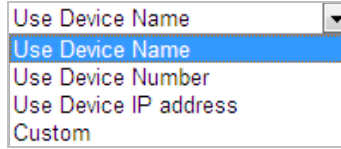


Figure 6-9 Parent Directory

- ◆ **Child directory:** It is a sub-folder which can be created in the parent directory. The files will be saved in a sub-folder in FTP server. The name of folder can be defined as shown in Figure 6-10.

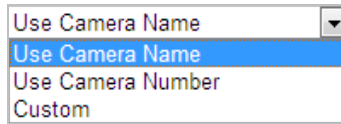



Figure 6-10 Child Directory

- **Upload type:** To enable uploading the captured picture to the FTP server.

3. Click  to save the settings.
4. You can click **Test** to confirm the configuration.

Note:

If you want to upload the captured pictures to FTP server, you also have to enable the continuous snapshot or event-triggered snapshot in **Snapshot** interface.

Configuring Email Settings

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:

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

Steps:

1. Enter Email settings interface:
Configuration > Network > Advanced Settings > Email

Sender	<input type="text"/>
Sender's Address	<input type="text"/>
SMTP Server	<input type="text"/>
SMTP Port	25
E-mail Encryption	None
<input type="checkbox"/> Attached Image	
Interval	2
<input type="checkbox"/> Authentication	
User Name	<input type="text"/>
Password	<input type="text"/>
Confirm	<input type="text"/>

Receiver			
No.	Receiver	Receiver's Address	Test
1			<input type="button" value="Test"/>
2			
3			

Figure 6-11 Email Settings

2. Configure the following settings:

Sender: The name of the email sender.

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

SMTP Server: The SMTP Server IP address or host name (e.g., smtp.263xmail.com).

SMTP Port: The SMTP port. The default TCP/IP port for SMTP is 25.

E-mail 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:

STARTTLS protocol must be supported by the email server for e-mail encryption with STARTTLS. When it is not supported by the email server and the checkbox of Enable STARTTLS is checked, the email 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 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.*

Receiver: Select the receiver to which the email is sent. Up to 2 receivers can be configured.

Receiver: The name of the user to be notified.

Receiver's Address: The email address of user to be notified. (Optional: click **Test** to make sure

that the email server can send email out.)

- Click  to save the settings.

Configuring Platform Settings

Purpose:

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

Note:

This function varies depending on different speed dome models.

Steps:

- Enter the Platform settings interface:

Configuration > Network > Advanced Settings > Platform Access

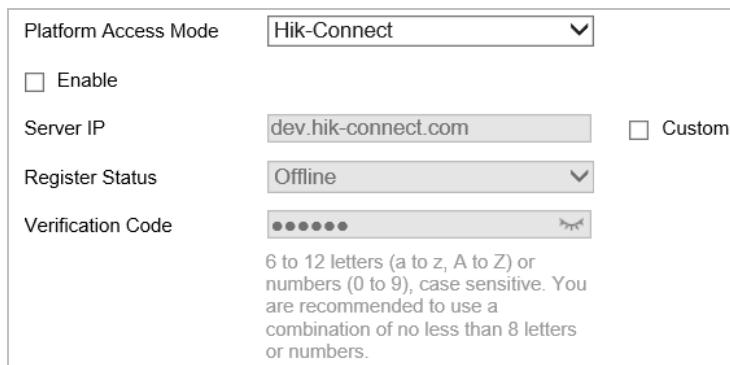


Figure 6-12 Platform Access

- Check the **Enable** checkbox to enable the platform access function of the device.
- Select the **Platform Access Mode**.

If you select **Platform Access Mode** as **Hik-Connect**,

- Click and read "Terms of Service" and "Privacy Policy" in pop-up window.
- Create a verification code or change the verification code for the camera.

Notes:

- The verification code is required when you add the camera to Hik-Connect app.
- For more information about the Hik-Connect app, refer to Hik-Connect Mobile Client User Manual.
- 3) You can use the default server address. Or you can check the **Custom** checkbox on the right and input a desired server address.

If you select **Platform Access Mode** as **Ehome**,

- Select Protocol Version from the dropdown list.
- Set **Server Address**, **Port**, **Device ID**, and **Key** for the camera.

- Click  to save the settings.

Configuring HTTPS Settings

Purpose:

HTTPS is consisted by SSL&HTTP. It is used for encryption transmission, identity authentication

network protocol which enhances the security of WEB accessing.



- *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 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. Enter HTTPS settings interface.

Configuration > Network > Advanced Settings > HTTPS

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

Figure 6-13 Create Certificate

OPTION 1: Create the self-signed certificate

- 1) Select Create Self-signed Certificate.
- 2) Click **Create** to create the following dialog box.

Figure 6-14 Create Self-signed Certificate

- 3) Input the country, host name/IP, validity and other information.
- 4) Click **OK** to save the settings.

OPTION 2: Start the installation when signed certificate is available.

- 1) Select Signed certificate is available, Start the installation directly.

- 2) Click **Browse** to upload the available certificate.
- 3) Click **Install** button to install the certificate.
- 4) Click **OK** to save the settings.

OPTION 3: Create certificate request first and continue the installation.

- 1) Select Create certificate request first and continue the installation.
 - 2) Click **Create** to create the certificate request, and fulfill the required information.
 - 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.
 - 5) Click **OK** to save the settings.
3. There will be the certificate information after you successfully create and install the certificate.

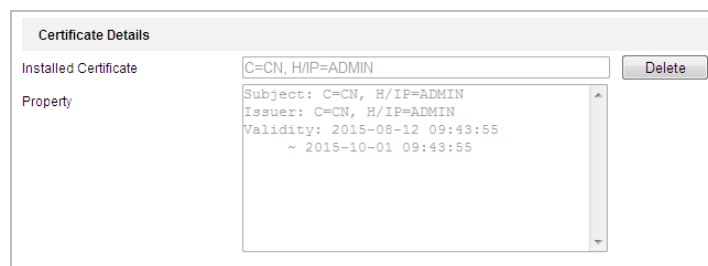


Figure 6-15 Installed Certificate Property



- The default port number of HTTPS is 443. The port value ranges from 1 to 65535.
- When the port number is the default number 443, the format of the URL is **https://IP address**, eg., **https://192.168.1.64**.
- When the port number is not the default number 443, the format of the URL is **https://IP address:port number**, eg., **https://192.168.1.64:81**.

Configuring QoS Settings

Purpose:

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

Steps:

1. Enter QoS settings interface:

Configuration > Advanced Configuration > Network > QoS

The screenshot shows the QoS Settings interface with three input fields, each with a value of 0:

Video/Audio DSCP	0
Event/Alarm DSCP	0
Management DSCP	0

Figure 6-16 QoS Settings

2. Configure the QoS settings, including video / audio DSCP, event / alarm DSCP and Management DSCP.

The valid DSCP value ranges from 0 to 63. The DSCP value is bigger, the priority is higher.

- Click  to save the settings.

Note:

- Make sure that you enable the QoS function of your network device (such as a router).
- It will ask for a reboot for the settings to take effect.

Configuring 802.1x Settings

Purpose:

The camera supports IEEE 802.1x standard.

IEEE 802.1x is a port-based network access control. It enhances the security level of the LAN. When devices connect to this network with IEEE 802.1x standard, the authentication is needed. If the authentication fails, the devices don't connect to the network.

The protected LAN with 802.1x standard is shown in Figure 6-17.

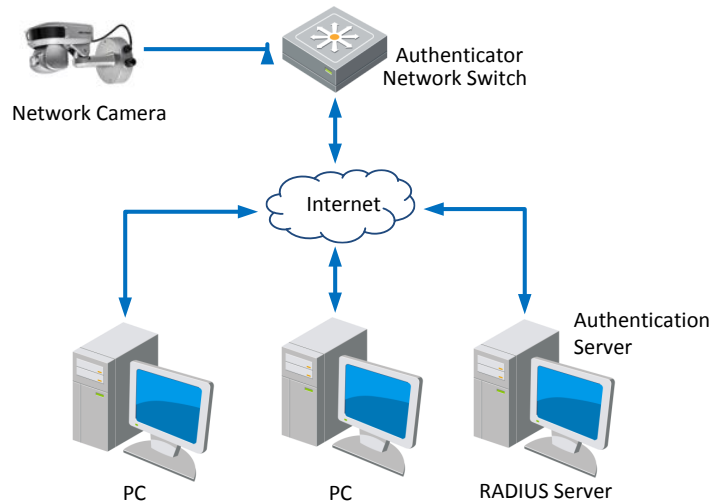


Figure 6-17 Protected LAN

- Before connecting the Network Camera to the protected LAN, apply a digital certificate from a Certificate Authority.
- The network camera requests access to the protected LAN via the authenticator (a switch).
- The switch forwards the identity and password to the authentication server (RADIUS server).
- The switch forwards the certificate of authentication server to the network camera.
- If all the information is validated, the switch allows the network access to the protected network.



- *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 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. Connect the network camera to your PC directly with a network cable.
2. Enter 802.1X settings interface:

Configuration > Network > Advanced Settings > 802.1x

Figure 6-18 802.1x Settings

3. Check the **Enable IEEE 802.1x** checkbox to enable it.
4. Configure the 802.1x settings, including user name and password.

Note:

The EAP-MD5 version must be identical with that of the router or the switch.

5. Click  Save to finish the settings.

Note:

The camera reboots when you save the settings.

6. After the configuration, connect the camera to the protected network.

Integration Protocol

Purpose:

If you need to access to the camera through the third party platform, you can enable Hikvision-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.


Steps:

1. Enter the Integration Protocol configuration interface.

Configuration > Network > Advanced Settings > Integration Protocol

No.	User Name	Level

Figure 6-19 Integration Protocol Settings

2. Check the **Enable Hikvision-CGI** checkbox and then select the authentication from the dropdown list. Then you can access to the camera through the third party platform.
3. Check the **Enable ONVIF** checkbox to enable the function.
4. Click **Add** to add a new ONVIF user. Set the user name and password, and confirm the password. You can set the user as media user, operator, and administrator.
5. Click **Modify** to modify the information of the added ONVIF user.
6. Click **Delete** to delete the selected ONVIF user.
7. Click  to save the settings.

Network Service

Purpose:

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

Notes:

Supported services vary according to camera models.

Keep unused function OFF for security concern.

- **WebSocket** or **WebSockets** protocol are used for plug-in-free live view.
When you use Google Chrome 57 and its above version or Mozilla Firefox 52 and its above version to visit your camera, you should enable WebSocket or Websokets protocol. Otherwise, live view function is not usable.
If the camera uses HTTP, enable **WebSocket**.
If the camera uses HTTPS, enable **WebSockets**.
- **SDK Service** and **Enhanced SDK Service**
If you want to add the device to the client software, you should enable SDK Service or Enhanced SDK Service.
SDK Service: SDK protocol is used.
Enhanced SDK Service: SDK over TLS protocol is used. Communication between the device and the client software is secured by using TLS (Transport Layer Security) protocol.
- **TLS (Transport Layer Security)**
The device offers TLS 1.1 and TLS 1.2. Enable one or more protocol versions according to your need.

HTTP Listening

Purpose:

Alarm information can be sent to destination IP or Host via HTTP protocol.

Steps:

1. Input destination IP or host name, URL, and port number.
2. Click **Test** to see if the service is available.

Note:

HTTP data transmission should be supported by the destination IP or Host.

3. Save the settings.

HTTP Data Transmission			Default
Destination IP or Host Name	URL	Port	Test
0.0.0.0	/	80	Test




Figure 6-20 HTTP Listening

TCP Acceleration

Purpose:

TCP acceleration is used to improve latency and reduce packet loss caused by network congestion in poor network condition, and guarantee the fluency of live view.

Steps:

1. Enter the **TCP Acceleration** interface.
Configuration > Network > Advanced Settings > TCP Acceleration
2. Check to enable the function.
3. Save the settings.

Enable TCP Acceleration




Figure 6-21 TCP Acceleration

Traffic Shaping

Purpose:

Traffic shaping is used to shape and smooth video data packet before transmission. It helps improve latency and reduce packet loss caused by network congestion and ensure the video quality as well.

Steps:

1. Enter the **Traffic Shaping** interface.
Configuration > Network > Advanced Settings > Traffic Shaping
2. Check to enable the function.

Note:

Traffic shaping takes effect only when UDP or TCP is used.

3. Save the settings.

Figure 6-22 Traffic Shaping

6.2 Configuring Video and Audio Settings

6.2.1 Configuring Video Settings

Steps:

1. Enter Video settings interface:

Configuration > Video/Audio > Video

Figure 6-23 Configure Video Settings

2. Select the camera channel No. from the dropdown list.
3. Select the **Stream Type** of the camera to main stream (normal), sub-stream or third stream. The main stream is usually for recording and live viewing with good bandwidth, and the sub-stream can be used for live viewing when the bandwidth is limited. Refer to the **Section 4.1 Configuring Local Parameters** for switching the stream type for live viewing.
4. You can customize the following parameters for the selected stream.

Note:

The parameters vary depending on different camera models.

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:

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. The higher value corresponds to the higher video quality, but the higher bandwidth is required.

Video Encoding:

Select **Video Encoding** from the dropdown list for different stream type.

H.264+/H.265+:

Set it as ON or OFF.

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.

Note:

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.

Profile:

Basic Profile, Main Profile and High Profile are selectable.

I Frame Interval:

Set the 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, the better fluency of the stream, though, the video quality may not be so satisfied. The lower value of the smoothing, the higher quality of the stream, though it may appear not fluent.

5. Click  to save the settings.

6.2.2 Configuring Audio Settings

Steps:

1. Enter Audio settings interface

Configuration > Video/Audio > Audio

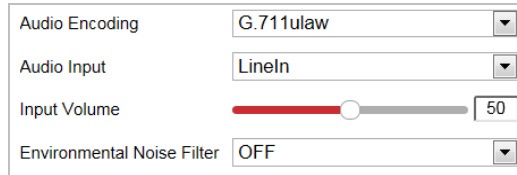


Figure 6-24 Audio Settings

2. Configure the following settings.

Audio Encoding: G.722.1, G.711ulaw, G.711alaw, MP2L2, G.726 and PCM are selectable.

Audio Input: When an intercom is connected to the camera, you need to set this option to **LineIn**. When a microphone is connected to the camera, you need to set this option to **MicIn**.

Audio Stream Bitrate: When the Audio Encoding is selected as MP2L2, you can configure the Audio Stream Bitrate in the dropdown list. The greater the value is, the better the audio quality will be.

Sampling Rate: When the Audio Encoding is selected as MP2L2, you can configure the Sampling Rate in the dropdown list. The greater the value is, the better the audio quality will be.



Input Volume: Slid the **bar** to turn up/down the volume. The value ranges from 0 to 100.

Environmental Noise Filter: Select ON or OFF in the dropdown list to enable or disable the function. It's recommended to enable the function when sampling rate is lower than 32 kHz.

3. Click  to save the settings.

6.3 Configuring Image Settings

Notes:

- On the event configuration page, click  to show the PTZ control panel or click  to hide it.
- Click the direction buttons to control the pan/tilt movements.
- Click the zoom/iris/focus buttons to realize lens control.
- The functions vary depending on different camera models.

6.3.1 Configuring Display Settings

Purpose:

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

Notes:

- The parameters in **Display Settings** interface vary depending on different camera models.
- You can double click the live view to enter full screen mode and double click it again to exit.

Steps:

1. Enter Display settings interface:
Configuration > Image> Display Settings
2. Select the camera channel No. from the dropdown list.
3. You can select the **Scene** in the dropdown list with different predefined image parameters.
4. Set the image parameters of the camera.

Image Adjustment

● Brightness

This feature is used to adjust brightness of the image. The value ranges from 0 to 100.

● Contrast

This feature enhances the difference in color and light between parts of an image. The value ranges from 0 to 100.

● Saturation

This feature is used to adjust color saturation of the image. The value ranges from 0 to 100.

● Sharpness

Sharpness function enhances the detail of the image by sharpening the edges in the image. The value ranges from 0 to 100.

Exposure Settings

● Exposure Mode

The **Exposure Mode** can be set to **Auto**, **Iris Priority**, **Shutter Priority**, and **Manual**.

◆ Auto:

The iris, shutter and gain values will be adjusted automatically according to the brightness of the environment.

◆ Iris Priority:

The value of iris needs to be adjusted manually. The shutter and gain values will be adjusted automatically according to the brightness of the environment.

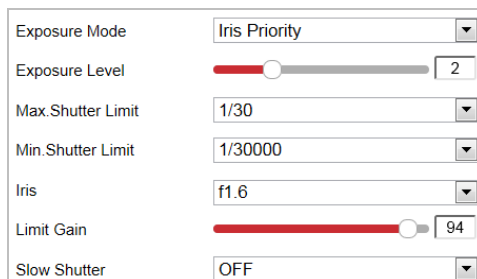


Figure 6-25 Manual Iris

◆ Shutter Priority:

The value of shutter needs to be adjusted manually. The iris and gain values will be adjusted automatically according to the brightness of the environment.

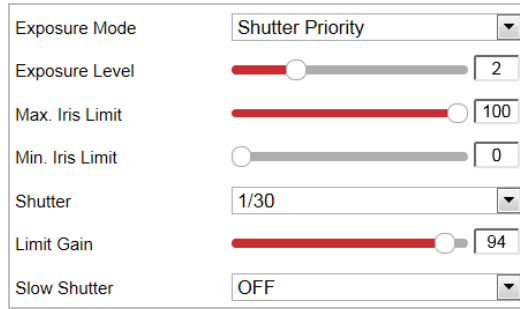


Figure 6-26 Manual Shutter

◆ **Manual:**

In **Manual** mode, you can adjust the values of **Gain**, **Shutter**, **Iris** manually.

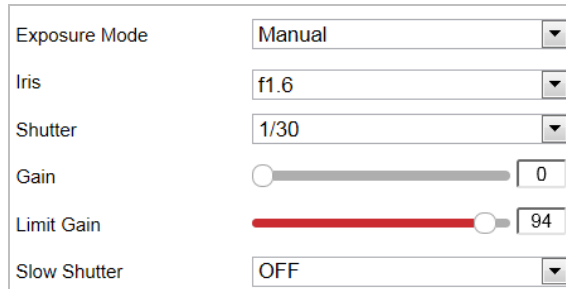


Figure 6-27 Manual Mode

- **Limit Gain**

This feature is used to adjust gain of the image. The value ranges from 0 to 100.

- **Slow Shutter**

This function can be used in underexposure condition. It lengthens the shutter time to ensure full exposure.

- **Slow Shutter Level**

When slow shutter is set as ON, you can select the slow shutter level from the dropdown list. The slow shutter lever can be set to **Slow Shutter*2**, ***3**, ***4**, ***6**, ***8**.

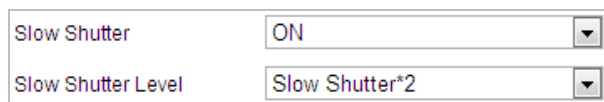


Figure 6-28 Slow Shutter

Focus Settings

- **Focus Mode**

The **Focus Mode** can be set to **Auto**, **Manual**, and **Semi-auto**.

- ◆ **Auto:**

The camera focuses automatically at any time according to objects in the scene.

- ◆ **Semi-auto:**

The camera focuses automatically only once after panning, tilting and zooming.

- ◆ **Manual:**

In **Manual** mode, you need to use   on the control panel to focus manually.

- **Min. Focus Distance**

This function is used to limit the minimum focus distance. The value can be set to 10cm, 50cm, 1.0m, 1.5m, 3m, 6m, 10m and 20m.

Note:

The minimum focus value varies depending on different camera models.

Day/Night Switch

- **Day/Night Switch**

The **Day/Night Switch** mode can be set to **Auto**, **Day**, **Night** and **Scheduled-Switch**.

Note:

This function varies depending on the models of camera.

- ◆ **Auto:**

In **Auto** mode, the day mode and night mode can switch automatically according to the light condition of environment.



Figure 6-29 Auto Mode Sensitivity

- ◆ **Day:**

In **Day** mode, the camera displays color image. It is used for normal lighting conditions.

- ◆ **Night:**

In **Night** mode, the image is black and white. **Night** mode can increase the sensitivity in low light conditions.

- ◆ **Scheduled-Switch:**

In **Schedule** mode, you can set the time schedule for day mode as shown in Figure 6-30.

The rest time out of the schedule is for night mode.

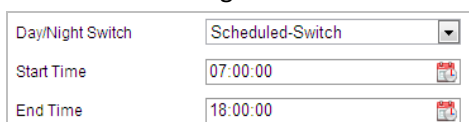


Figure 6-30 Day Night Schedule

Backlight Settings

- **BLC (Back Light Compensation)**

If there's a bright backlight, the subject in front of the backlight appears silhouetted or dark. Enabling **BLC** (back light compensation) function can correct the exposure of the subject. But the backlight environment is washed out to white.

- **WDR (Wide Dynamic Range)**

The wide dynamic range (WDR) function helps the camera provide clear images even under back light circumstances. When there are both very bright and very dark areas simultaneously in the field of view, WDR balances the brightness level of the whole image and provide clear images with details.

You can enable or disable the WDR function as shown in Figure 6-31. The wide dynamic level

ranges from 0 to 100.



Figure 6-31 WDR

- **HLC**

HLC (High Light Compensation) makes the camera identify and suppress the strong light sources that usually flare across a scene. This makes it possible to see the detail of the image that would normally be hidden.

White Balance

The **White Balance** mode can be set to **Auto**, **MWB**, **Outdoor**, **Indoor**, **Fluorescent Lamp**, **Sodium Lamp** and **Auto-Tracking**.

- ◆ **Auto:**

In **Auto** mode, the camera retains color balance automatically according to the current color temperature.

- ◆ **Manual White Balance:**

In **MWB** mode, you can adjust the color temperature manually to meet your own demand as shown in Figure 6-32.

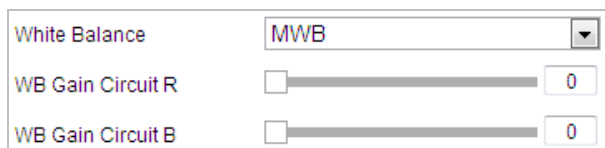


Figure 6-32 Manual White Balance

- ◆ **Outdoor**

You can select this mode when the camera is installed in outdoor environment.

- ◆ **Indoor**

You can select this mode when the camera is installed in indoor environment.

- ◆ **Fluorescent Lamp**

You can select this mode when there are fluorescent lamps installed near the camera.

- ◆ **Sodium Lamp**

You can select this mode when there are sodium lamps installed near the camera.

- ◆ **Auto-Tracking**

In **Auto-Tracking** mode, white balance is continuously being adjusted in real-time according to the color temperature of the scene illumination.

Image Enhancement

- **3D Digital Noise Reduction**

You can set **Digital Noise Reduction** function to **Normal** and adjust the **Noise Reduction Level** as shown in Figure 6-33. The level ranges from 0 to 100.

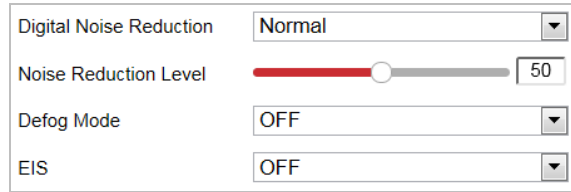


Figure 6-33 3D Digital Noise Reduction

If you are a professional technician, you can set it to **Expert Mode** then adjust **Space DNR Level** and **Time DNR Level**. The level ranges from 0 to 100.

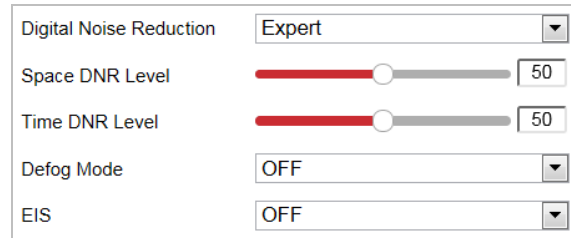


Figure 6-34 Expert Mode

- **Defog Mode**

You can set the **Defog Mode** to ON or OFF as you need.



Figure 6-35 Defog Mode

- **EIS (Electronic Image Stabilization)**

You can set the **EIS** to ON or OFF as you need.

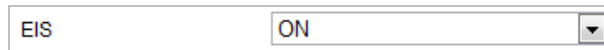


Figure 6-36 Electronic Image Stabilization

Video Adjustment

Note:

The functions vary depending on different camera models.

- **Mirror**

If you turn the **MIRROR** function on, the image will be flipped. It is like the image in the mirror. The flip direction can be set to OFF or CENTER.

- **Video Standard**

You can set the **Video Standard** to 50 Hz (PAL) or 60 Hz (NTSC) according to the video system in your country.

- **Capture Mode**

You can disable this function or select the capture mode from the list.

Other

Note:

The functions vary depending on different camera models.

- **Lens Initialization**

The lens operates the movements for initialization when you enable **Lens Initialization**.

- **Zoom Limit**

You can set **Zoom Limit** value to limit the maximum value of zooming. The value can be selected from the list.

6.3.2 Configuring OSD Settings

Purpose:

OSD (On-screen Display) refers to the camera name, time/date, customized information displayed on the live view.

Note:

This function varies according to different camera models.

Steps:

1. Enter OSD settings interface:

Configuration > Image > OSD Settings

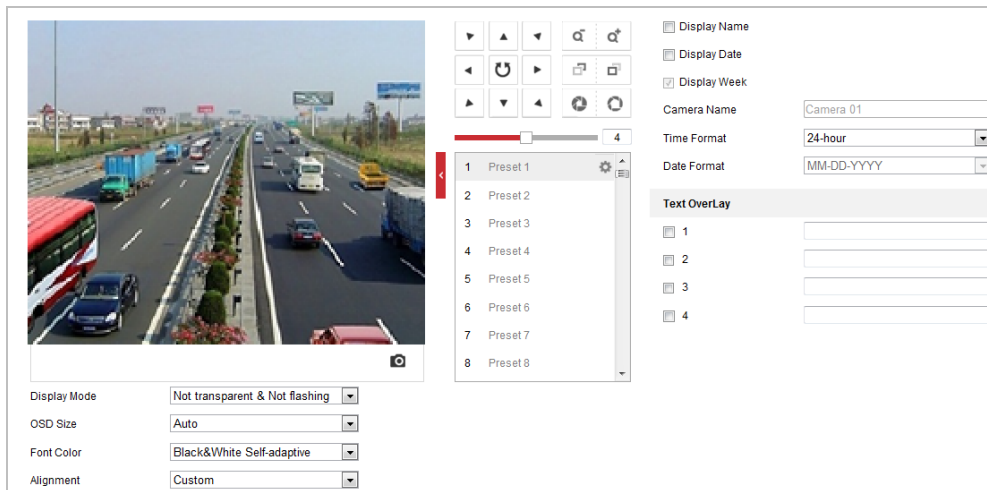


Figure 6-37 OSD Settings

2. Select Character Set. If Korean is required to display on screen, select EUC-KR. Otherwise, select GBK.

Note:

Changing character set requires device reboot.

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 dropdown list to set the time format, date format, display mode, OSD size and Font color.
6. You can use the mouse to drag the text frame **IPdome** in the live view window to adjust the OSD position.



Figure 6-38 Adjust OSD Location



7. Click  to activate above settings.

Configuring Text Overlay Settings

Purpose:

You can customize the text overlay.

Steps:

1. Enter Text Overlay settings interface:
Configuration > Image > OSD Settings
2. Check the checkbox in front of textbox to enable the on-screen display.
3. Input the characters in the textbox.
4. Use the mouse to drag the red text frame  in the live view window to adjust the text overlay position.
5. Click  to save the settings.

6.3.3 Configuring Image Parameters Switch

Note:

This function varies depending on different camera models

Purpose:

Camera 01 and Camera 02 can be configured separately. You can configure **Link to Preset** or **Scheduled-Switch** in this interface.

- **Link to Preset:** Set the time period and linked scene for the preset and check the

corresponding checkbox to go to the linked scene in the configured time period.

- **Scheduled-Switch:** Set the time period and linked scene and it will go to the linked scene in the configured time period when you check the corresponding checkbox.

Steps:

1. Enter Image Parameters Switch interface:

Configuration > Image > Image Parameters Switch

2. Check the checkbox of **Link to Preset** or **Scheduled-Switch** to enable the function. (Only one function can be enabled in the same time.)
3. When you enable the function of **Link to Preset**, select one preset from the dropdown list, check the corresponding checkbox, set the time period and the linked scene for the selected preset. (Up to 4 periods can be configured for one preset.)

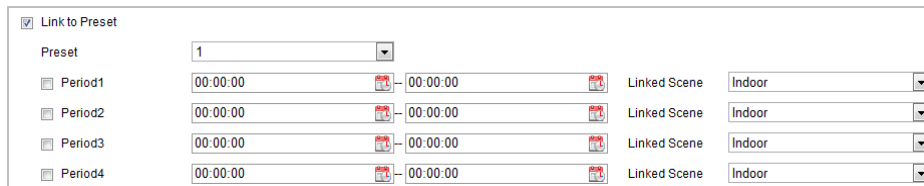


Figure 6-39 Link to Preset

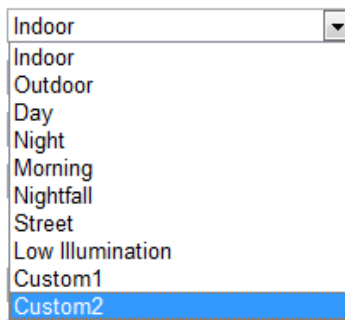


Figure 6-40 Linked Scene

4. When you enable the function of **Scheduled-Switch**, check the corresponding checkbox, set the time period and the linked scene.

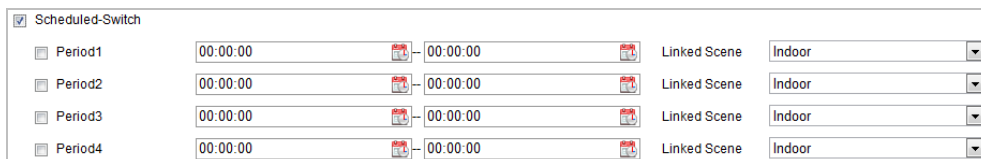



Figure 6-41 Schedule-Switch

5. Click  to save the settings.

Note:

The two functions are not enabled by default.

6.4 Configuring System Settings

6.4.1 System Settings

Viewing Basic Information

Enter 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 camera, such as Model, Serial No., Firmware Version, Encoding Version, Web Version, Plugin 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	<input type="text"/>
Device No.	<input type="text"/>
Model	<input type="text"/>
Serial No.	<input type="text"/>
Firmware Version	<input type="text"/>
Encoding Version	<input type="text"/>
Web Version	<input type="text"/>
Plugin Version	<input type="text"/>
Number of Channels	<input type="text"/>
Number of HDDs	<input type="text"/>
Number of Alarm Input	<input type="text"/>
Number of Alarm Output	<input type="text"/>

Figure 6-42 Device Information

Time Settings

Purpose:

You can follow the instructions in this section to configure the time which can be displayed on the video. There are Time Zone, Time Synchronization, and Daylight Saving Time (DST) functions for setting the time. Time Synchronization consists of auto mode by Network Time Protocol (NTP) server and manual mode.

Enter Time Settings interface:

Configuration > System > System Settings > Time Settings

Figure 6-43 Time Settings

● Configuring Time Synchronization by NTP Server

Steps:

(1) Check the radio button 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 by NTP server. It can be set from 1 to 10080 minutes.

Figure 6-44 Time Sync by NTP Server

You can click  to make sure that the NTP server is connected.


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.

● Configuring Time Synchronization Manually

Steps:

(1) Check the **Manual Time Sync** radio button.

(2) Click  to set the system time from the pop-up calendar.

(3) Click  to save the settings.

Note:

You can also check the **Sync with local time** checkbox to synchronize the time of the camera with the time of your computer.

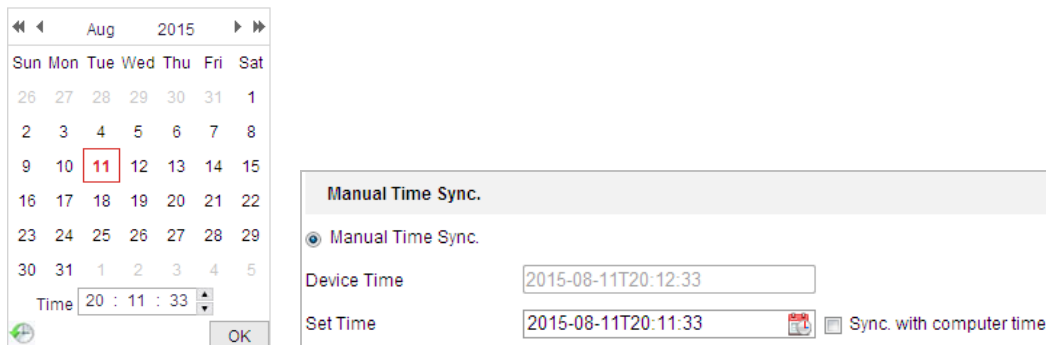


Figure 6-45 Time Sync Manually

● Select the Time Zone

Purpose:

When the camera is taken to another time zone, you can use the **Time Zone** function to adjust the time. The time will be adjusted according to the original time and the time difference between the two time zones.

From the **Time Zone** dropdown menu as shown in Figure 6-46, select the Time Zone in which the camera locates.

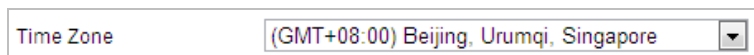


Figure 6-46 Time Zone Settings

Configuring DST (Daylight Saving Time)

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.

If there is the habit of adjusting clocks forward in your country in certain time period of a year, you can turn this function on. The time will be adjusted automatically when the Daylight Saving Time (DST) comes.

Steps:

1. Enter **DST** interface by **Configuration > Advanced Configuration > System > DST**

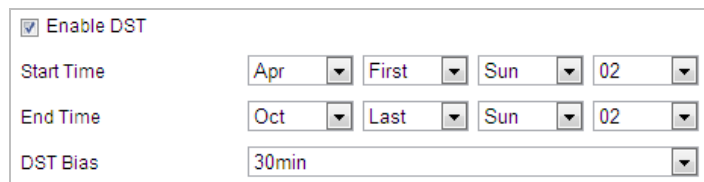



Figure 6-47 DST Settings

2. Check the **Enable DST** checkbox to enable the DST function.
3. Set the date of the DST period.
4. Click  to save the settings.

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.

Note:

RS-485 function varies depending on different speed dome models.

Steps:

1. Enter RS-485 Port Setting interface:

Configuration > System > System Settings > RS-485

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

Figure 6-48 RS-485 Settings

2. Set the RS-485 parameters and click  to save the settings.

Note:

The Baud rate, PTZ Protocol and PTZ Address parameters of the camera should be exactly the same as those of the control device.

VCA Resource

Purpose:

VCA resource offers users options to enable certain VCA function and disable others when several VCA functions are available. It helps allocate more resources to the wanted functions.

Steps:

1. Enter the VCA Resource interface:
Configuration > System > System Settings > VCA Resource
2. Select the desired VCA option.
3. Save the settings. A reboot is needed for the settings to take effect.

Note:

The function may not be supported by some camera models.

About

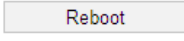
Click **View License**, you can check Open Source Software Licenses.

6.4.2 Maintenance

Upgrade & Maintenance

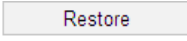

● Rebooting the Camera

Steps:

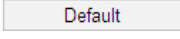
1. Enter Maintenance interface:
2. **Configuration > System > Maintenance > Upgrade & Maintenance:**
3. Click  to reboot the network camera.

● Restoring Default Settings

Steps:

1. Enter Maintenance interface:
Configuration > System > Maintenance > Upgrade & Maintenance:
2. Click  or  to restore the default settings.

Note:

Clicking  restores all the parameters to default settings including the IP address and user information. Use this button with caution.

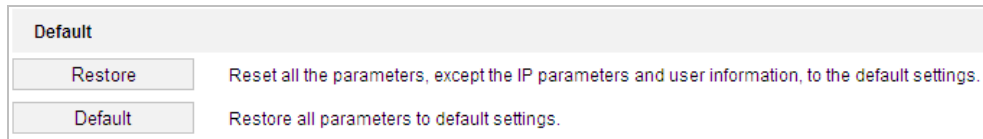


Figure 6-49 Restore Default Settings

● Exporting Configuration File

Steps:

1. Enter Maintenance interface:
Configuration > System > Maintenance > Upgrade & Maintenance
2. Click **Device Parameters** and set the encryption password to export the current configuration file.
3. Set the saving path to save the configuration file in local storage.
4. Click **Diagnose Information** to download the log and system information.

● Importing Configuration File

1. Enter Maintenance interface:
Configuration > System > Maintenance > Upgrade & Maintenance
2. Click **Browse** to select the saved configuration file.
3. Input the encryption password you have set when exporting the configuration file.
4. Click **Import** to import configuration file.

Note:

You need to reboot the camera after importing configuration file.

● Upgrading the System

Steps:

1. Enter Maintenance interface:
Configuration >System > Maintenance > Upgrade & Maintenance
2. Select Firmware or Firmware Directory.
 - **Firmware:** when you select **Firmware**, you need to find the firmware in your computer to upgrade the device.
 - **Firmware Directory:** You need to find the directory where the firmware locates. The device can find the firmware in the directory automatically.
3. 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. Don't disconnect power of the camera during the process. The camera reboots automatically after upgrading.

Log Searching**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:

Configure network storage for the camera or insert a memory card in the camera.

Steps:

1. Enter Log interface:
Configuration >System > Maintenance > Log

The screenshot displays the 'Log' interface under 'Upgrade & Maintenance'. It features search filters for Major Type (All Types), Minor Type (All Types), Start Time (2015-08-11 00:00:00), and End Time (2015-08-11 23:59:59). A 'Search' button is located to the right of the End Time field. Below the filters is a 'Log List' table with columns: No., Time, Major Type, Minor Type, Channel No., Local/Remote User, and Remote Host IP. An 'Export' button is positioned to the right of the table header. At the bottom of the interface, it indicates 'Total 0 Items' and includes navigation arrows and a '0/0' counter.

Figure 6-50 Log Searching Interface

2. Set the log search conditions to specify the search, including the Major Type, Minor Type, Start Time and End Time as shown in Figure 6-50.
3. Click to search log files. The matched log files will be displayed on the **Log** interface.

4. To export the log files, click **Save Log** to save the log files in your computer.

System Service

Steps:

1. Enter interface of configuring the remote connection:
Configuration > System > Maintenance > System Service
2. Check the checkbox to enable supplement light function if the device supports the function.
3. Input a number in text field as the upper limit of the remote connection number. E.g. when you specify the remote connection number as 10, then the 11th remote connection cannot be established.



Figure 6-51 Live View Connection Settings

4. Click  button to activate the settings.

Security Audit Log

Purpose:

The Security Audit Log refers to the security operation logs. You can search and analyze the security log files of the camera so that to find out the illegal intrusion and troubleshooting the security events.

Security audit logs can be saved on device flash. The log will be saved every half hour after device booting.

Due to limited saving space of the flash, you can also save the logs on a log server. Configure the server settings at Advanced Settings.

● Searching Logs

Steps:

1. Enter the Security Audit Log interface:
Configuration > System > Maintenance > Security Audit Log
2. Set the log search conditions to specify the search, including the Major Type, Minor Type, Start Time and End Time.

No.	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP
Total 0 Items						

Figure 6-52 Log Query Interface

- Click Search to search log files. The matched log files will be displayed on the Log list interface.
- To export the log files, click Export to save the log files in your computer.

● Setting Log Server

Steps:

- Check Enable Log Upload Server.
- Input Log Server IP and Log Server Port.
- Click Test to test settings.
- Install certificates. Client certificate and CA certificate are required.
 - ◆ Client Certificate
 - Click Create button to create the certificate request. Fill in the required information in the popup window.
 - Click Download to download the certificate request and submit it to the trusted certificate authority for signature.
 - Install the signed certificate to the device.
 - ◆ CA Certificate
 - Install the CA certificate to the device.

6.4.3 Security

Configuring Authentication Security

Purpose:

You can specifically secure the stream data of live view.

Steps:

- Enter Authentication interface:
Configuration > System > Security > Authentication
- Set the **RTSP Authentication/WEB Authentication** type from the dropdown list.

- Click  to save the settings.

Configuring IP Address Filter

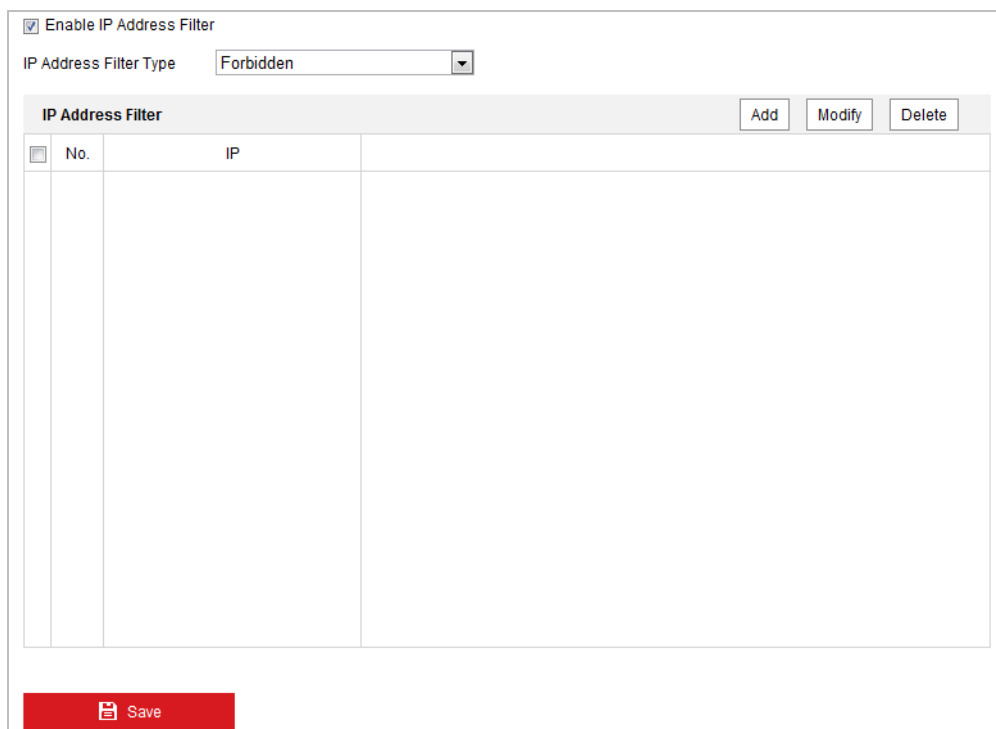
Purpose:

With this function on, the camera allows certain IP addresses whether to log in or not.

Steps:

- Enter IP Address Filter interface:

Configuration > System > Security > IP Address Filter



Enable IP Address Filter

IP Address Filter Type: Forbidden

No.	IP
-----	----

Buttons: Add, Modify, Delete

Save

Figure 6-53 IP Address Filter

- Check the checkbox of **Enable IP Address Filter**.
- Select the type of IP Address Filter in the dropdown list, Forbidden and Allowed are selectable.
- Set the IP Address Filter list.

- **Add an IP Address**

Steps:

- Click **Add** to add an IP.
- Input the IP Address.



Add IP Address

IP Address: 172.6.23.2

Buttons: OK, Cancel

Figure 6-54 Add an IP

(3) Click **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.



Figure 6-55 Modify an IP

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

- **Delete an IP Address**

Left-click an IP address from filter list and click **Delete**.


- **Delete all IP Addresses**

Click **Clear** to delete all the IP addresses.

5. Click  to save the settings.

Configure Security Service Settings

Steps:

1. Enter Security Service interface:
Configuration > System > Security > Security Service
2. Check the checkbox to enable the SSH or Illegal Login Lock function.
Illegal Login Lock: Enabling illegal login lock function is to automatically lock the device IP after the admin user performing 7 failed password attempts (5 attempts for the user/operator).
3. Click  to save the settings.

6.4.4 User Account

Manage Users

Enter the User Management interface:

Configuration > System > User Management

The **admin** user has access to create, modify or delete other accounts, and grant different permission to different user levels. We highly recommend administrator to manage the device accounts and user permissions properly. Up to 31 user accounts can be created.

User Management		Online Users	
User List		Add	Modify
No.	User Name	Delete	General
1	admin		Account Security Settings

Figure 6-56 User Information

● Add a User

Steps:

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

Note:

The level indicates the permissions you give to the user. You can define the user as **Operator** or **User**.

3. In the **Basic Permission** field and **Camera Configuration** field, you can check or uncheck the permissions for the new user.
4. Click to finish the user addition.

Add user

User Name: user1 ✓

Level: Operator

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: ●●●●●●●● ✓

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

OK Cancel

Figure 6-57 Add a User

● Modify a User



Steps:

1. Click to select the user from the list and click .
2. Modify the **User Name**, **Level** or **Password**.
3. In the **Basic Permission** field and **Camera Configuration** field, you can check or uncheck the permissions.
4. Click to finish the user modification.

Figure 6-58 Modify a User

- **Delete a User**

Steps:

1. Click the user name you want to delete and click .
2. Click  on the pop-up dialogue box to delete the user.

Recover Admin Password

Purpose:

The camera allows admin password recovery via security question. Recovery password operation is only available to administrator.

- **Setup Security Question for Verification Code**

Steps

1. Click **Account Security Settings** to enter setting interface.
Configuration > System > User Management > Account Security Settings
2. Select security questions and input your answers.
3. Save the settings.

- **Password Recovery Operation**

Before you start:

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

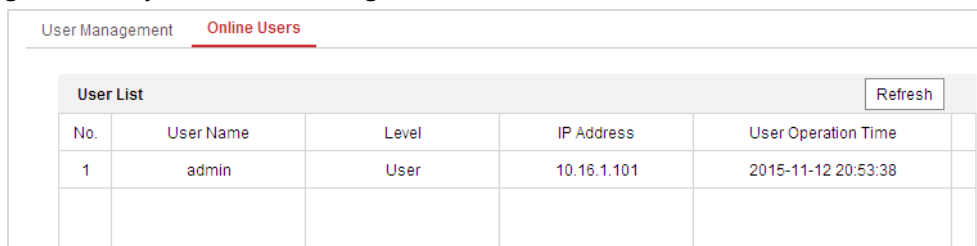
Steps:

1. Enter login interface via web browser.
2. Click **Forget Password**.
3. Follow pop-up message to complete operation.

Online Users

Enter the Online Users configuration interface:

Configuration > System > User Management > Online Users



The screenshot shows the 'Online Users' configuration page. At the top, there is a breadcrumb trail: 'User Management > Online Users'. Below this, there is a 'User List' section with a 'Refresh' button. The table below contains the following data:

No.	User Name	Level	IP Address	User Operation Time
1	admin	User	10.16.1.101	2015-11-12 20:53:38

Figure 6-59 Online Users

You can see the current users who are visiting the device through this interface.

User information, such as user name, level, IP address, and operation time, is displayed in the User List. Click **Refresh** to refresh the list.

Note:

Administrator can control the **Simultaneous Login**. Click **General** on **User Management** page, and set desired number. Admin password is required for this operation.

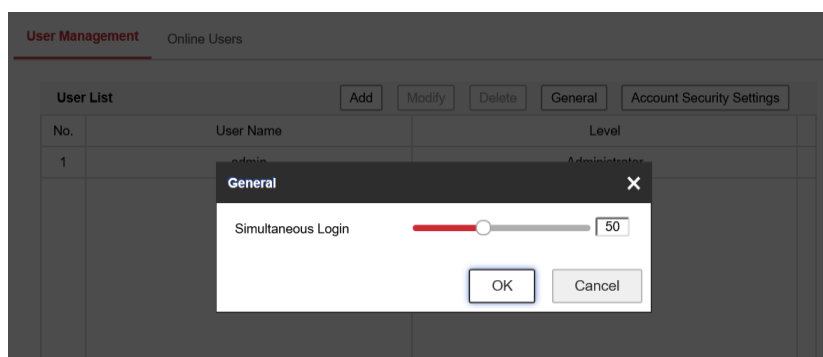


Figure 6-60 Simultaneous Login

Chapter 7 VCA Configuration

7.1 Configuring Face Capture

Purpose:

Face capture function detects and captures faces in video security scenes. When the grading of the detected face exceeds an algorithm-defined value, the PTZ camera channel captures the face and triggers linkage actions. Set up Overlay & Capture, Rule and Advanced Configuration before using the function.

Before you start:

For certain camera models, you need to select Face Capture on VCA Resource page first.

Configuration > System > System Settings

Notes:

- This function is only supported by Camera 01.
- Face capture is only supported by certain camera models.

7.1.1 Overlay & Capture

Purpose:

You can choose to configure Display on Stream, Display on Picture, Snapshot Settings, Camera Information, and Text Overlay on stream/picture.

Enter the Overlay & Capture configuration interface:

Configuration > Face Capture > Overlay & Capture

Figure 7-1 Overlay & Capture interface

- **Display on Stream:** Check the checkbox, then the green frames will be displayed on the target if in a live view or playback.


- **Display on Picture:** Check the checkbox, then there will be a frame on the target on the uploaded alarm picture if the checkbox is checked.
 - **Snapshot Settings:**
 - ◆ **Target Picture Settings:** You can set the face picture type by selecting Custom, Head Shot, Half-Body Shot, or Full-Body Shot. If you select Custom, you can define detailed picture width and height of a picture freely. If the captured pictures should have the same picture height, check Fixed Value and input desired picture height.
 - ◆ **Background Picture Settings:** Comparing to target picture, background picture is the scene image offers extra environmental information. You can set the background picture quality and resolution. If the background image need to be uploaded to surveillance center, check **Background Upload**.
- Note:**
Background upload is only available for face capture camera.
- **Camera Information:** Enter Device No. and Camera Info.
 - **Text Overlay:** Check Device No., Capture Time, and Camera Info, and these camera information can be overlaid on captured picture. You can check desired items and adjust their order to display on captured pictures by clicking the up arrow or down arrow.

Text Overlay	
<input checked="" type="checkbox"/> Device No.	<input checked="" type="checkbox"/> Capture Time <input checked="" type="checkbox"/> Camera Info.
Type	Sorting
Camera Info.	↑ ↓
Capture Time	↑ ↓
Device No.	↑ ↓

Figure 7-2 Picture Overlay Information

7.1.2 Rule

Steps:

1. Check **Enable** to enable the function.
2. Click  to set up face capture rule.

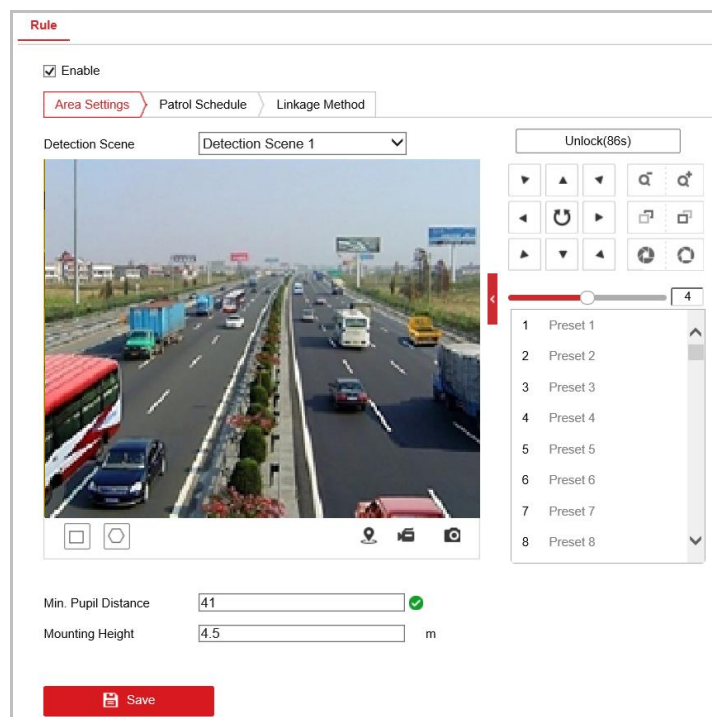






Figure 7-3 Area Settings

- (1) Select a **Detection Scene** from the dropdown list.
 - (2) Adjust the live image to a desired scene. You can use PTZ control panel or click  to locate a scene with a face. Click **Lock** to lock PTZ for further settings.
 - (3) Click  and draw detection area on live image.
 - (4) Click  and draw **Min. Pupil Distance** on live image.
 - (5) Input **Mounting Height** of the camera.
 - (6) Save the settings for the detection scene.
 - (7) Repeat the steps to set other detection scenes.
 - (8) Save the settings
3. Click  to enable camera patrols the detection scenes following configured order and dwell time, and capture faces during its patrol.

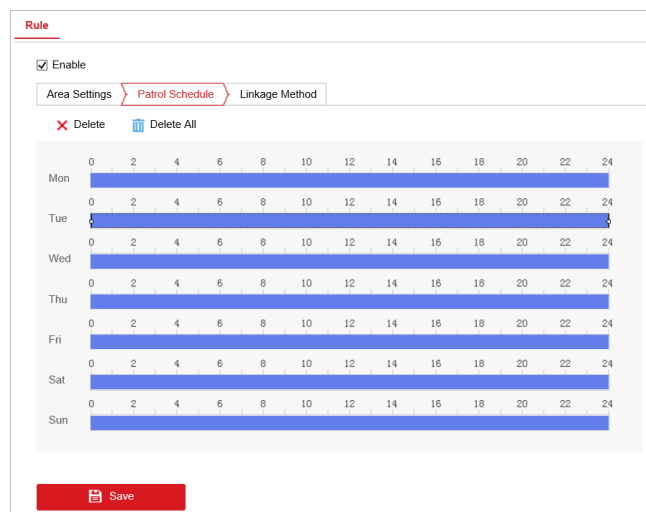




Figure 7-4 Patrol Schedule

- (1) Click the set blue time bar.
 - (2) Click **Configuration** in the pop-up bubble.
 - (3) Add detection scenes, adjust the patrol sequence and set dwell time for each detection scene.
 - (4) Save the settings by clicking **OK**.
 - (5) You can copy the settings of a day to other days by click  on right end of the time bar.
4. Click  to set linkage method. Refer to **Section 5.2.1 Configuring Motion Detection** for detailed configuration.

7.1.3 Advanced Configuration

Purpose:

The following contents are about how to configure the parameters of face capture algorithm.

Note:

Face Capture Version shows current algorithm version, which cannot be edited.

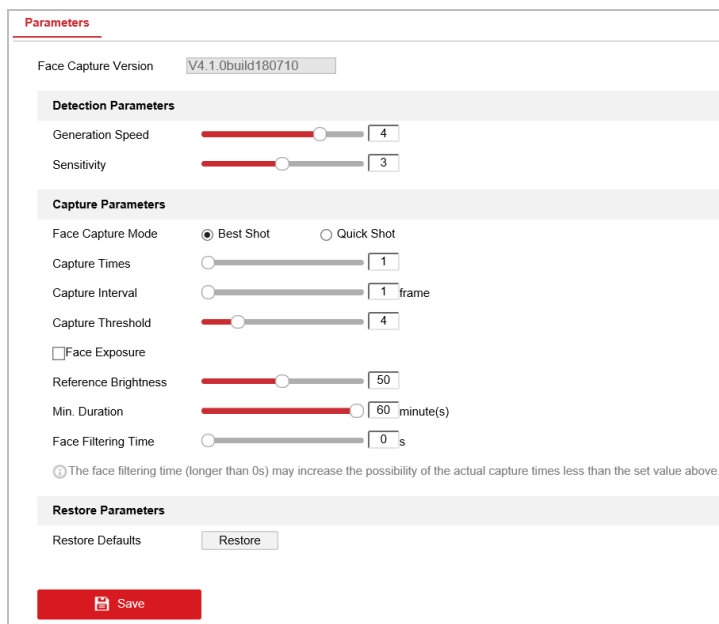


Figure 7-5 Advanced Face Capture Parameters


Following parameters can be configured on this interface:

- **Generation Speed:** The speed to identify a target can be set by adjusting the slider, ranging from 1 to 5. The higher the value is, the faster the target will be recognized. The default value is recommended.
- **Sensitivity:** The sensitivity to identify a target can be set by adjusting the slider, ranging from 1 to 5. The higher the value is, the easier a face will be detected, and the higher possibility of misinformation would be. The default value of 3 is recommended.
- **Upload Feature:** Feature stands for the feature information the algorithm can tell from face pictures. Check the function to upload the information.
- **Face Capture Mode:** Best Shot and Quick Shot are available.
 - ◆ **Best Shot** stands for the best picture after the target leaving the detection area.
 - **Capture Times:** Refers to the capture times a face will be captured during its stay in the detection area.
 - **Capture Threshold:** It stands for the quality of face to trigger capture and alarm. Higher value means better quality should be met to trigger capture and alarm.
 - **Remove Duplicated Faces:** This function can filter out repeated captures of certain face.

Note: Remove Duplicated Faces, Face Picture Comparison, and Face Modeling cannot be turned on simultaneously, and the device can support only one function at a time. The last one you turned on can eventually take effect, and the other two turn off automatically.

Duplicates Removing Triggering Threshold: When the face grading is higher than the value you set, the captured picture can be uploaded to duplicates removing library, and compare with the picture that already in the library.

Duplicates Removing Threshold: The threshold is used to compare the similarity between captured face and the picture in the duplicates removing library. When the similarity is higher than the value you set, the device will remove the duplicated face.

- ◆ **Quick Shot:** You can define quick shot threshold and max. capture interval.
 - **Quick Shot Threshold:** It stands for the quality of face to trigger quick shot.
 - **Max. Capture Interval:** It describes the max. time occupation for one quick shot.
 - **Capture Times:** It refers to the capture times a face will be captured during its stay in the configured area.
- **Face Exposure:** Check the checkbox to enable the Face Exposure. The device automatically adjusts exposure level when human faces appear in the scene.
 - **Reference Brightness:** The reference brightness of a face in the face exposure mode. If a face in the actual scene is brighter than the set reference brightness, the device lower the exposure level. If a face in the actual scene is darker than the set reference, the device increases the exposure level.
 - **Minimum Duration:** The extra time the device keeps the face exposure level after the face disappears in the scene.
- **Face Filtering Time:** It means the time interval between the camera detecting a face and taking a capture action. If the detected face stays in the scene for less than the set filtering time, capture will not be triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the detected face when the face keeps staying in the scene for 5 seconds.
- **Face Posture Filter:** To filter out face of certain postures. The figure on the right of the slider stands for the posture angle which is acceptable in the face capture action. Click  to display the diagram illustrating the face turning direction when setting up this filter.
- **Face Covering Filter :** To filter out face with different kinds of coverings. Checked options are not count in face capture.
- **Restore Default:** Click to restore all the settings in advanced configuration to the factory default.

7.2 Configuring Multi-Target-Type Detection

Purpose:

Multi-Target-Type Detection is a function to detect, capture and upload image of targets of multiple types.

Before you start:

Go to **Configuration > System > VCA Resource**, and select **Multi-Target Type Detection**.

Note:

Settings for Camera 01 and Camera 02 are different. Select a camera channel from navigation bar on left to start configuration.

7.2.1 PTZ Channel Configuration (Camera 01)

Rule

Set corresponding parameters and rules to capture the desired targets.

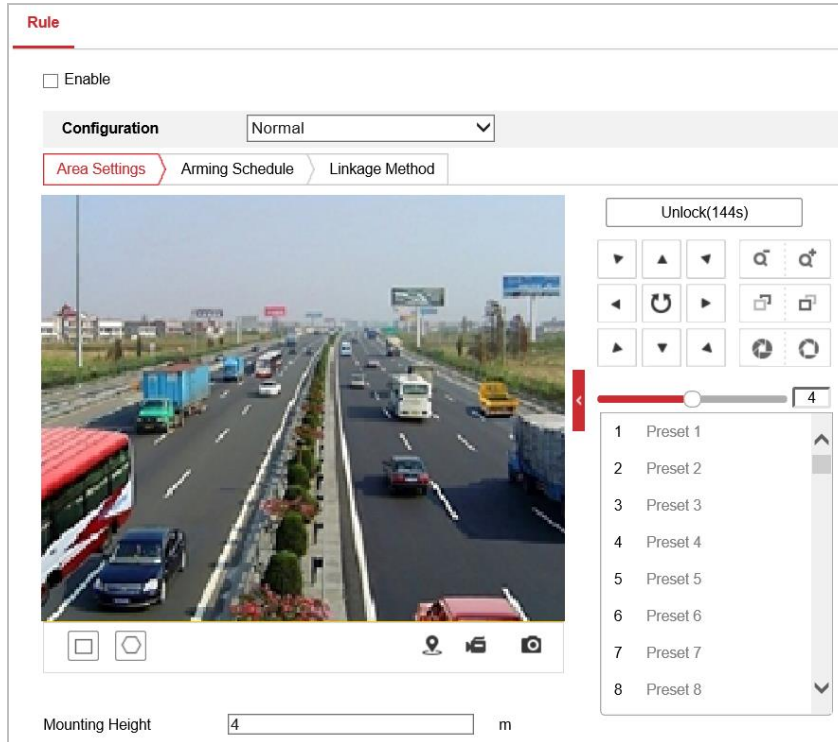







Figure 7-6 Detection Rule Configuration

Steps:

1. Check **Enable** to enable the function.
2. Set up detection areas.
 - (1) Adjust the live image to a desired scene. you can use PTZ control panel or click  to locate a scene with a face. Click **Lock** to lock PTZ for further settings.
 - (2) Click  and draw detection area on live image.
 - (3) Click  and draw **Min. Pupil Distance** on live image.
 - (4) Input **Mounting Height** of the camera.
 - (5) Save the settings for the detection scene.
 - (6) Repeat the steps to set other detection scenes.
 - (7) Save the settings
3. Set arming schedule.
 - (1) Click **Arming Schedule** or **Patrol Schedule** tab.
 - (2) Draw blue time bar.
 - (3) You can copy the settings of a day to other days by click  on right end of the time bar.
 - (4) Save the settings
4. Click  to set linkage method. Refer to **Section 5.2.1 Configuring Motion**

Detection for detailed configuration.

Overlay & Capture

Purpose:

Overlay and Capture offers options to specify overlay information on captured picture, picture type and quality, etc.

Enter the Overlay & Capture configuration interface:

Configuration > Multi-Target-Type Detection > Overlay & Capture

- **Display on Stream:** Check the checkbox, then the green frames will be displayed on the target if in a live view or playback.
- **Display on Picture:** Check the checkbox, then there will be a frame on the target on the uploaded alarm picture if the checkbox is checked.
- **Snapshot Settings:**
 - ◆ **Target Picture Settings:** You can set the face picture type by selecting Custom, Head Shot, Half-Body Shot, or Full-Body Shot. If you select Custom, you can define detailed picture width and height of a picture freely. If the captured pictures should have the same picture height, check Fixed Value and input desired picture height.
 - ◆ **Background Picture Settings:** Comparing to target picture, background picture is the scene image offers extra environmental information. You can set the background picture quality and resolution. If the background image need to be uploaded to surveillance center, check **Background Upload**.

Note:

Background upload is only available for face capture camera.

- **Camera Information:** Enter Device No. and Camera Info.

Text Overlay: Check Device No., Capture Time, and Camera Info, and these camera information can be overlaid on captured picture. You can check desired items and adjust their order to display on captured pictures by clicking the up arrow or down arrow.

Advanced Configuration

Purpose:

Set parameters for multi-target-type detection algorithm.

Following parameters can be configured on this interface:

- **HMSVersion:** It shows current algorithm version.
- **Generation Speed:** The speed to identify a target can be set by adjusting the slider, ranging from 1 to 5. The higher the value is, the faster the target will be recognized. The default value is recommended.
- **Sensitivity:** The sensitivity to identify a target can be set by adjusting the slider, ranging from 1 to 5. The higher the value is, the easier a face will be detected, and the higher possibility of misinformation would be. The default value of 3 is recommended.
- **Face Capture Mode:** Best Shot and Quick Shot are available.
 - ◆ **Best Shot** stands for the best picture after the target leaving the detection area.
 - **Capture Times:** Refers to the capture times a face will be captured during its stay

in the detection area.

- **Capture Threshold:** It stands for the quality of face to trigger capture and alarm. Higher value means better quality should be met to trigger capture and alarm.
- **Remove Duplicated Faces:** This function can filter out repeated captures of certain face.

Note: Remove Duplicated Faces, Face Picture Comparison, and Face Modeling cannot be turned on simultaneously, and the device can support only one function at a time. The last one you turned on can eventually take effect, and the other two turn off automatically.

Duplicates Removing Triggering Threshold: When the face grading is higher than the value you set, the captured picture can be uploaded to duplicates removing library, and compare with the picture that already in the library.

Duplicates Removing Threshold: The threshold is used to compare the similarity between captured face and the picture in the duplicates removing library. When the similarity is higher than the value you set, the device will remove the duplicated face.

- ◆ **Quick Shot:** You can define quick shot threshold and max. capture interval.
 - **Quick Shot Threshold:** It stands for the quality of face to trigger quick shot.
 - **Max. Capture Interval:** It describes the max. time occupation for one quick shot.
 - **Capture Times:** It refers to the capture times a face will be captured during its stay in the configured area.
- **Face Exposure:** Check the checkbox to enable the Face Exposure. The device automatically adjusts exposure level when human faces appear in the scene.
 - **Reference Brightness:** The reference brightness of a face in the face exposure mode. If a face in the actual scene is brighter than the set reference brightness, the device lower the exposure level. If a face in the actual scene is darker than the set reference, the device increases the exposure level.
 - **Minimum Duration:** The extra time the device keeps the face exposure level after the face disappears in the scene.
- **Face Filtering Time:** It means the time interval between the camera detecting a face and taking a capture action. If the detected face stays in the scene for less than the set filtering time, capture will not be triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the detected face when the face keeps staying in the scene for 5 seconds.
- **Data Upload:** Select one or more desired target types configured in the Multi-Target-Type Detection for picture uploading.

Restore Default: Click Restore to restore all the settings in advanced configuration to the factory default.

7.2.2 Panoramic Channel Configuration (Camera 02)

Rule



Purpose:

Set corresponding parameters and rules to capture the desired targets.



Figure 7-7 Detection Rule Configuration

Steps:

1. Check **Rule** to start configuration.
2. Click  and draw detection area on live image.
3. Click  and draw **Min. Pupil Distance** on live image.
4. Click **Save** to save the settings.

Overlay & Capture

Purpose:

Overlay and Capture offers options to specify overlay information on captured picture, picture type and quality, etc.

Enter the Overlay & Capture configuration interface:

Configuration > Multi-Target-Type Detection > Overlay & Capture

- **Display on Stream:** Check the checkbox, then the green frames will be displayed on the target if in a live view or playback.
- **Display on Picture:** Check the checkbox, then there will be a frame on the target on the uploaded alarm picture if the checkbox is checked.
- **Snapshot Settings:**
 - ◆ **Target Picture Settings:** You can set the face picture type by selecting Custom, Head Shot, Half-Body Shot, or Full-Body Shot. If you select Custom, you can define detailed picture width and height of a picture freely. If the captured pictures should have the

same picture height, check Fixed Value and input desired picture height.

- ◆ **Background Picture Settings:** Comparing to target picture, background picture is the scene image offers extra environmental information. You can set the background picture quality and resolution. If the background image need to be uploaded to surveillance center, check **Background Upload**.

Note:

Background upload is only available for face capture camera.

- **Camera Information:** Enter Device No. and Camera Info.


Text Overlay: Check Device No., Capture Time, and Camera Info, and these camera information can be overlaid on captured picture. You can check desired items and adjust their order to display on captured pictures by clicking the up arrow or down arrow.

Shield Region

Purpose:

Configure the display information, snapshot settings and advanced configurations.

Steps:

1. Click **Shield Region** tab to enter the shield region configuration interface
2. Click . Draw area by left click end-points in the live view window, and right click to finish the area drawing. Polygon area with up to 10 sides is supported.
3. Click **Save** to save the settings.

Advanced Parameters

Following parameters can be configured on this interface:

- **HMSVersion:** It shows current algorithm version.
- **Generation Speed:** The speed to identify a target can be set by adjusting the slider, ranging from 1 to 5. The higher the value is, the faster the target will be recognized. The default value is recommended.
- **Sensitivity:** The sensitivity to identify a target can be set by adjusting the slider, ranging from 1 to 5. The higher the value is, the easier a face will be detected, and the higher possibility of misinformation would be. The default value of 3 is recommended.
- **Face Capture Mode:** Best Shot and Quick Shot are available.
 - ◆ **Best Shot** stands for the best picture after the target leaving the detection area.
 - **Capture Times:** Refers to the capture times a face will be captured during its stay in the detection area.
 - **Capture Threshold:** It stands for the quality of face to trigger capture and alarm. Higher value means better quality should be met to trigger capture and alarm.
 - ◆ **Quick Shot:** You can define quick shot threshold and max. capture interval.
 - **Quick Shot Threshold:** It stands for the quality of face to trigger quick shot.
 - **Max. Capture Interval:** It describes the max. time occupation for one quick shot.
 - **Capture Times:** It refers to the capture times a face will be captured during its stay in the configured area.

- **Face Filtering Time:** It means the time interval between the camera detecting a face and taking a capture action. If the detected face stays in the scene for less than the set filtering time, capture will not be triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the detected face when the face keeps staying in the scene for 5 seconds.
- **Capture Ratio Factor:** It stands for the coverage of the human body in a captured picture. Lower value means larger coverage of human body in the picture, in other words, more a zoomed-in human body.
- **Capture Vertical Offset Factor:** It stands for the human body relative position in the scene of PTZ camera channel when the tracking happens. Human body from head to feet is marked from 0 to 100 by algorithm. The body part the set value stands for stays in the center of PTZ camera channel.
- **Dwell Time for Capture:** The dwell time after a capture.
- **Data Upload:** Select one or more desired target types configured in the Multi-Target-Type Detection for picture uploading.
- **Restore Default:** Click Restore to restore all the settings in advanced configuration to the factory default.

7.3 Face Comparison and Modeling

Face comparison and modeling serves two alternative purposes in the monitoring scenario, that is, realizing face detection, capture and comparison, or collecting face information and creating face models.

Face Comparison

- Face picture library, see 7.3.1
- Face picture comparison, see 7.3.2

Face Modeling

To realize face information collection and model creation, you should set up:

- Face modeling rule, see 7.3.3

7.3.1 Configure Face Picture Library

Purpose:

Face picture library is used to store modeled human faces with face information.

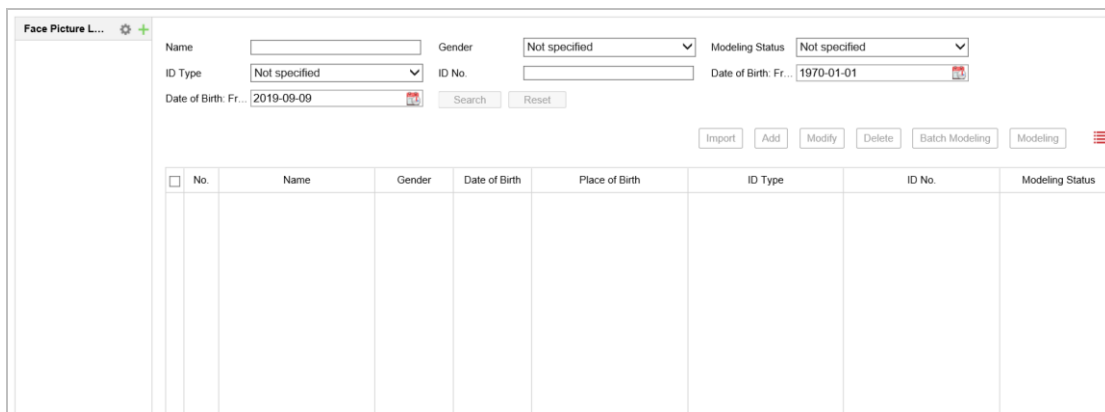





Figure 7-8 Face Picture Library

Steps:

1. Go to **Configuration --> Face Picture Library**.
2. Create a face picture library.

- a) Click  to add a face picture library.
- b) Input library name, threshold and remarks.
Threshold: Face similarity higher than the set threshold triggers face picture comparison alarm uploading.
- c) Click **OK**.
- d) (Optional) Modify a face picture library. Select desired library, click  and modify related parameters.
- e) (Optional) Delete a face picture library, click .

3. Add face pictures to the library.

Note: The picture format should be JPEG, and the size no larger than 300 K per file.

Add one face picture	Click Add and upload the face picture with detailed face information.
Import face pictures in batch	Click Import and select picture path. Note: When you import face pictures in batch, the picture name is saved as the face name. For other face information, you should modify one by one manually. The verification code for exporting and importing should be a combination of 8 to 16 digits, containing numeric, upper case and lower case letters.

4. Modify face information.
 - a) Select a face picture library.
 - b) Select the target face picture. You can use the search function to locate the picture by inputting search conditions, and click **Search**.
 - c) Click **Modify**.
 - d) Edit detailed information. Face picture is not allowed to change.
 - e) Click **OK**.
5. Create models for each face picture in library.

Modeling process builds up face model for each face picture. Face model is compulsory for face picture comparison to take effect.

Modeling	Select one or more face pictures, and click Modeling.
Batch Modeling	Select a face picture library, and click Batch Modeling .

- Repeat to create more face libraries.

7.3.2 Configuring Face Picture Comparison

Purpose:

The function compares captured pictures with face pictures in library and output comparison result. Comparison result can trigger certain actions when arming schedule and linkage method are set.

Before you start:

- For certain camera models, you need to enable the **Comparison Mode** on **VCA Resource** (Configuration > System > System Settings > VCA Resource) page to show the function.
- You should first create a face picture library and add face pictures. Get detailed instruction on **Face Picture Library** page.

Steps:

- Go to **Configuration > Comparison and Modeling > Face Comparison and Modeling**
- Check **Face Picture Comparison**.
- Select a face picture library as the reference.
- (Optional) If you want to receive face comparison information during Multi-Target-Type Capture alarm, check **Report Face Comparison Information During Multi-Target-Type Capture Alarm**.
- Set desired information to upload for face comparison.
- Select a comparison mode.
 - Best Comparison:** the device captures and compares the target face continuously when the face target stays in the detection area, and upload the best scored face picture and related alarm information when the target face leaves the area.
 - Quick Comparison:** the device capture and compares the target face when the face grading exceeds the set **Face Grading Threshold for Capture**.
Face Grading Threshold for Capture: the face grading threshold for the device to judge whether to capture and upload the face or not.
Max. Capture Interval: the max. interval between two captures when the target is in the detection area. The camera makes the capture when it reaches the max. interval even if the face grading does not reach the set threshold.
Quick Setup Mode: Custom, Face Attendance, and Face Recognition are selectable. Select according to actual using scenarios. In custom mode, you can set **Comparison Timeout** and **Comparison Times**.
- Set arming schedule for face comparison.
- Set linkage action for face comparison.

Note:

To see the comparison results, go to **Application** page.

7.3.3 Configuring Face Modeling Rule

Purpose:

The function is to capture qualified face pictures, create face models and upload data to surveillance center.

Steps:

1. Enter configuration page, and select **Face Modeling**.
Configuration > Comparison and Modeling > Face Comparison and Modeling
2. Check **Enable Face Modeling**.
3. Set parameters for modeling rules.
 - **Report Face Modeling Information in Multi-Target-Type Capture Alarm:** when a person triggers the multi-target-type detection, the alarm information will include the face modeling information of the detected face if the function is enabled.
 - **Enable Quick Capture:** with this function enabled, the device starts face modeling as soon as it detects a face which scores higher than the set Face Grading Threshold for Capture.
 - **Face Grading Threshold for Capture:** the face grading threshold for the device to judge whether to capture and upload the face or not.
 - **Max. Capture Interval:** the max. interval between two captures when the target is in the detection area. The camera makes the capture when it reaches the max. interval even if the face grading does not reach the set threshold.
4. Set arming schedule for face modeling.
5. Set linkage action for face modeling.

7.3.4 Search and Download Face Pictures

Purpose:

Search and output face picture comparison result on this page. **Face Picture Library** and **Face Comparison and Modeling** should be set before searching comparison results.

Steps:

1. Input search condition.
2. Click **Counting**. Result is shown in **Face Picture Comparison Statistics** area.

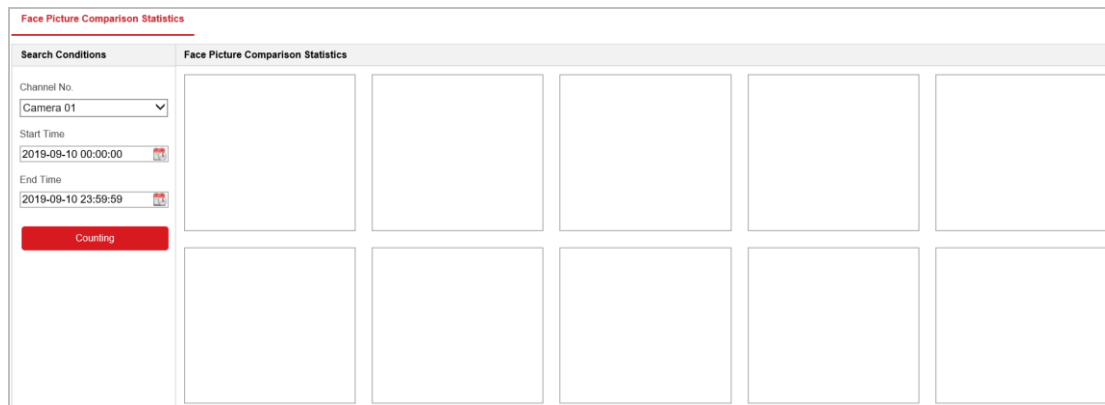


Figure 7-9 Application

Appendix

SADP Software Introduction

● Description of SADP

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

● Search active devices online

◆ 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.

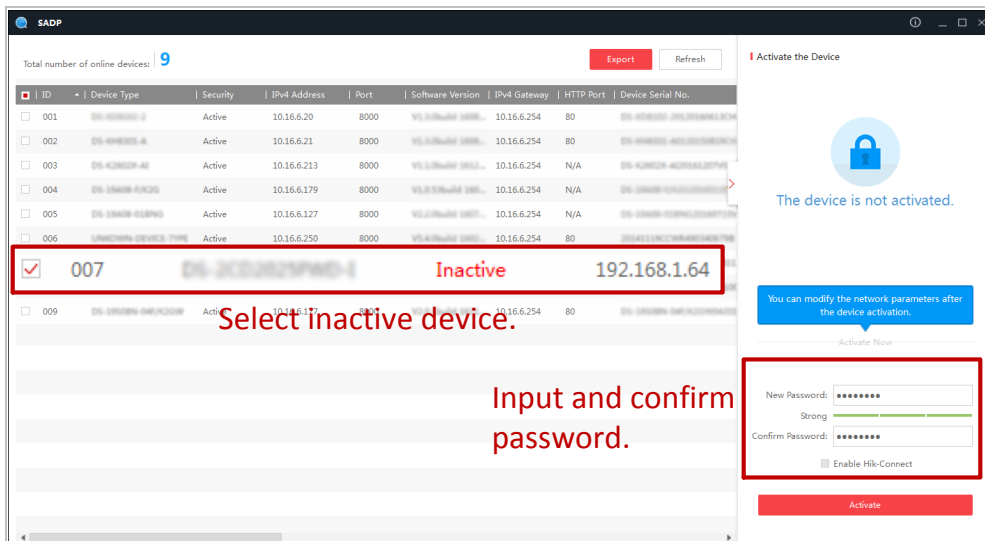



Figure A.1.1 Searching Online Devices







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  to refresh the online device list manually. The newly searched devices will be added to the list.



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. Input the password of the admin account of the device in the **Password** field and click

 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 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.*

Figure A.1.2 Modify Network Parameter

Device Communication Matrix

Scan the following QR code to get device communication matrix.

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





See Far, Go Further