Network Zoom Camera & Zoom Camera Module

User Manual

User Manual

COPYRIGHT ©2018 Hangzhou Hikvision Digital Technology Co., Ltd.

ALL RIGHTS RESERVED.

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be "Hikvision"). This user manual (hereinafter referred to be "the Manual") cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

About this Manual

This Manual is applicable to Network Zoom Camera & Zoom Camera Module.

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 in the company website (http://overseas.hikvision.com/en/).

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

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

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED "AS IS", WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS 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 OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITES 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.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

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

0505201080315

© Hikvision

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

CE This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU, the ATEX Directive 2014/34/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.

© Hikvision

- 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.

© Hikvision

Table of Contents

CHAPTER 1 OVERVIEW 1

1.1 System Requirement 1
1.2 Functions 1

CHAPTER 2 NETWORK CONNECTION 3

2.1 Setting the Network Camera over the LAN 3
2.1.1 Wiring over the LAN 3
2.1.2 Activating the Camera 4
2.1.3 (Optional) Setting Security Question 9
2.2 Setting the Network Camera over the WAN 9
2.2.1 Static IP Connection 9
2.2.2 Dynamic IP Connection 10

CHAPTER 3 ACCESSING TO THE NETWORK CAMERA 12

3.1 Accessing by Web Browsers 12
3.2 Accessing by Client Software 13

CHAPTER 4 BASIC OPERATIONS 15

4.1 Configuring Local Parameters 15
4.2 Live View Page 16
4.3 Starting Live View 17
4.4 Operating PTZ Control 19
4.4.1 PTZ Control Panel 20
4.4.2 Auxiliary Functions 21
4.4.3 Setting/Calling a Preset 23
4.4.4 Setting/Calling a Patrol 25
4.4.5 One-touch Patrol 26
4.4.6 Setting/Calling a Pattern 27
4.5 Playback 28
4.5.1 Play Back Video Files 28
4.5.2 Downloading Video Files 30
4.6 Pictures 30

CHAPTER 5 SYSTEM CONFIGURATION 32

5.1 Storage Settings 32
5.1.1 Configuring Recording Schedule 32
5.1.2 Configuring Capture Schedule 34
5.1.3 Configuring Net HDD 35
5.2 Basic Event Configuration 38
5.2.1 Configuring Motion Detection 38
5.2.2 Configuring Video Tampering Alarm 43
5.2.3 Configuring Alarm Input 44
5.2.4 Configuring Alarm Output 46

© Hikvision

5.2.5 Handling Exception *47*
5.3 SMART EVENT CONFIGURATION 47
5.3.1 Detecting Audio Exception *48*
5.3.2 Configuring Intrusion Detection *49*
5.3.3 Configuring Line Crossing Detection *50*
5.4 PTZ CONFIGURATION 52
5.4.1 Configuring Basic PTZ Parameters *52*
5.4.2 Configuring Park Actions *52*

CHAPTER 6 CAMERA CONFIGURATION 54

6.1 CONFIGURING NETWORK SETTINGS 54
6.1.1 Basic Settings *54*
6.1.2 Advanced Settings *59*
6.2 CONFIGURING VIDEO AND AUDIO SETTINGS 68
6.2.1 Configuring Video Settings *68*
6.2.2 Configuring Audio Settings *70*
6.2.3 Configuring ROI Settings *70*
6.3 CONFIGURING IMAGE SETTINGS 72
6.3.1 Configuring Display Settings *72*
6.3.2 Configuring OSD Settings *77*
6.3.3 Configuring Text Overlay Settings *79*
6.3.4 Configuring Privacy Mask *79*
6.4 CONFIGURING SYSTEM SETTINGS 80
6.4.1 System Settings *80*
6.4.2 Maintenance *84*
6.4.3 Security *87*
6.4.4 User Management *89*

APPENDIX 94

SADP SOFTWARE INTRODUCTION 94

© Hikvision

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 and above version, Apple Safari 5.02 and above version, Mozilla Firefox 5 and above version and Google Chrome 18 and above versions.

1.2 Functions

The functions vary depending on different camera models.

- **Privacy Mask**

This function allows you to block or mask certain area of a scene, for preventing the personal privacy from recording or live viewing.

- **Auto Focus**

The auto focus enables the camera to focus automatically to maintain clear video images.

- **Day/Night Auto Switch**

The cameras deliver color images during the day. And as light diminishes at night, the cameras switch to night mode and deliver black and white images with high quality.

- **Slow Shutter**

In slow shutter mode, the shutter speed will automatically slow down in low illumination conditions to maintain clear video images by extending the exposure time. The feature can be enabled or disabled.

- **Backlight Compensation (BLC)**

If you focus on an object against strong backlight, the object will be too dark to be seen clearly. The BLC (Backlight Compensation) function can compensate light to the object in the front to make it clear, but this causes the over-exposure of the background where the light is strong.

- **Wide Dynamic Range (WDR)**

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.

- **White Balance (WB)**

White balance can remove the unrealistic color casts. White balance is the white rendition

© Hikvision

function of the camera to adjust the color temperature according to the environment automatically.

- **User Management**

The camera allows you to edit users with different levels of permission, in the admin login status. Multiple users are allowed to access and control the same camera via network simultaneously.

- **3D Digital Noise Reduction**

Comparing with the general 2D digital noise reduction, the 3D digital noise reduction function processes the noise between two frames besides processing the noise in one frame. The noise will be much less and the video will be clearer.

© Hikvision

Chapter 2 Network Connection

- 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 of the network camera.

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.

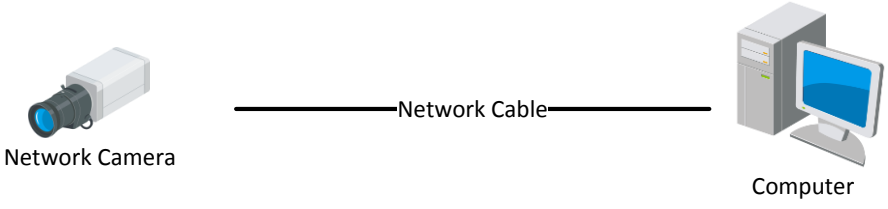


Figure 2-1 Connecting Directly

© Hikvision

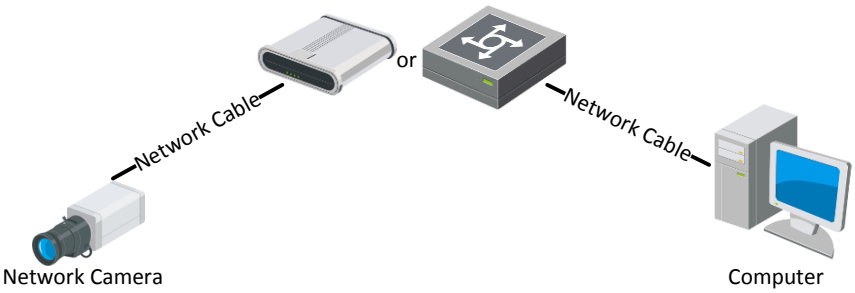


Figure 2-2 Connecting via a Switch or a Router

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.

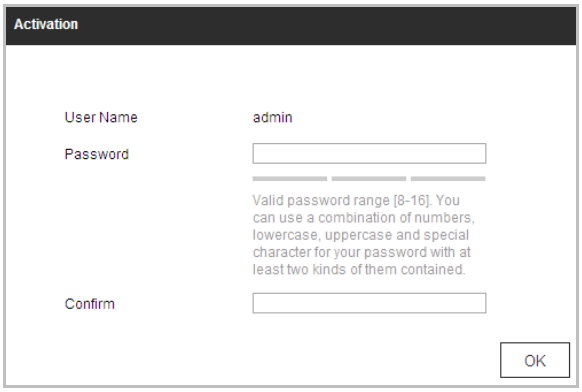


Figure 2-3 Activation Interface (Web)

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.

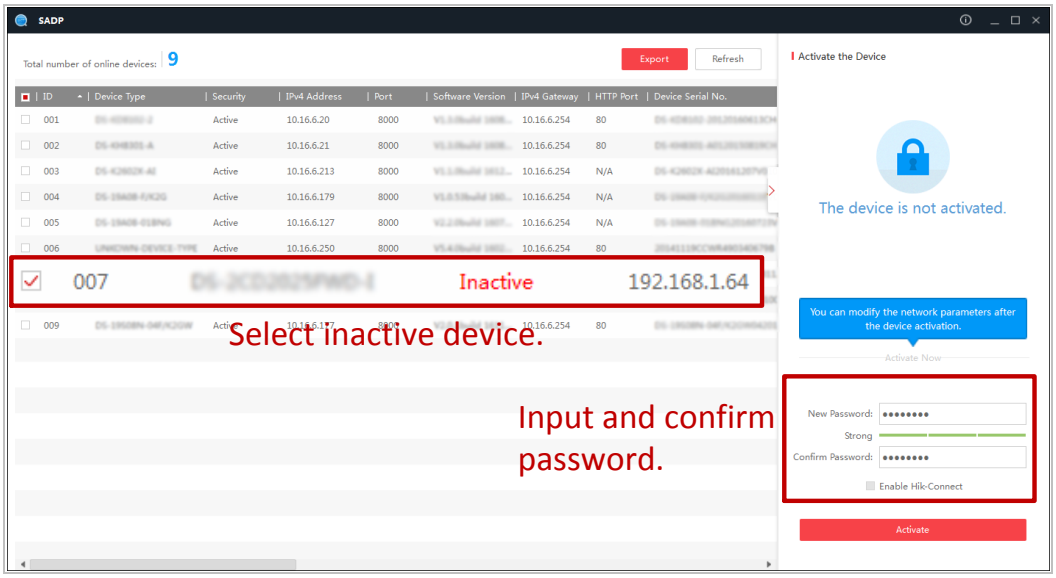


Figure 2-4 SADP Interface

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.

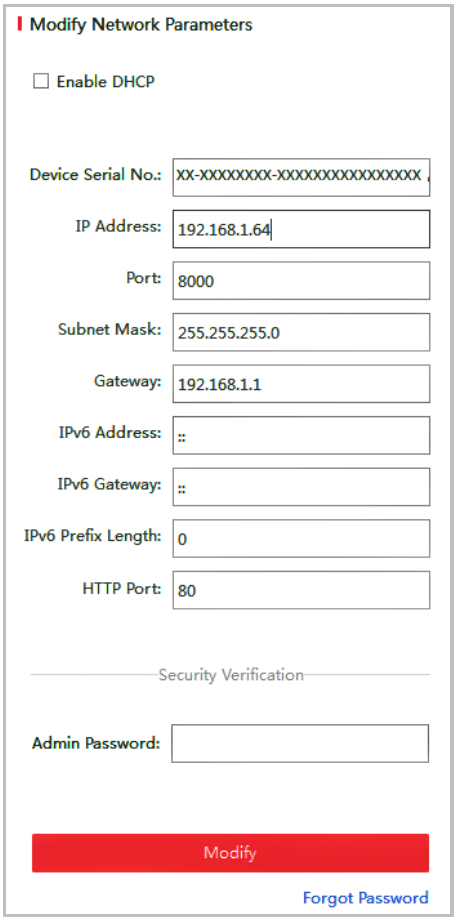


Figure 2-5 Modify the IP Address

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 the figure below.

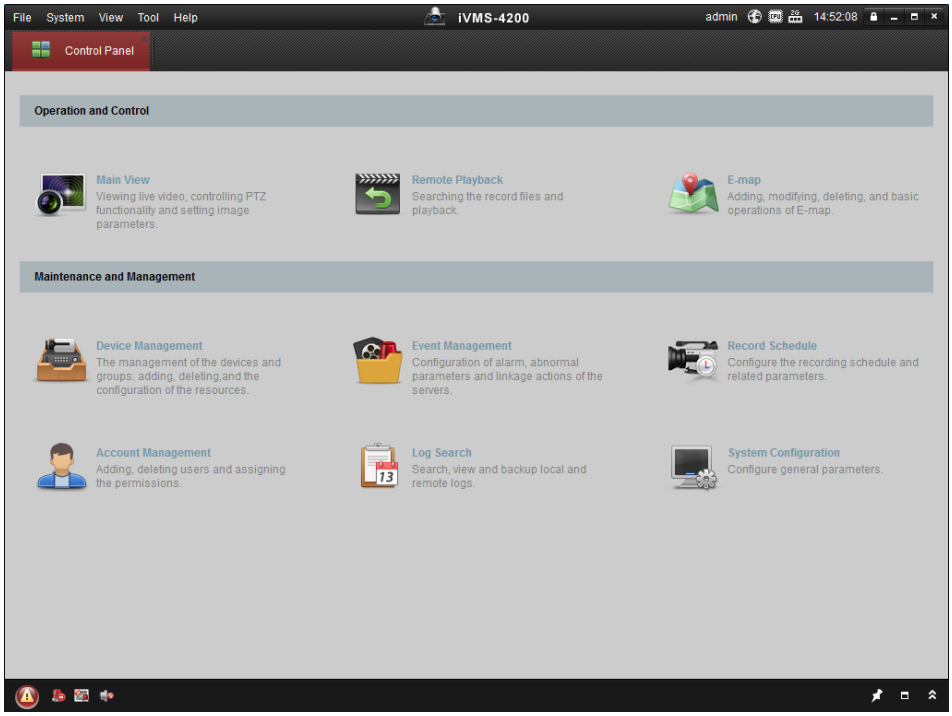


Figure 2-6 Control Panel

2. Click **Device Management** to enter the Device Management interface, as shown in the figure below.

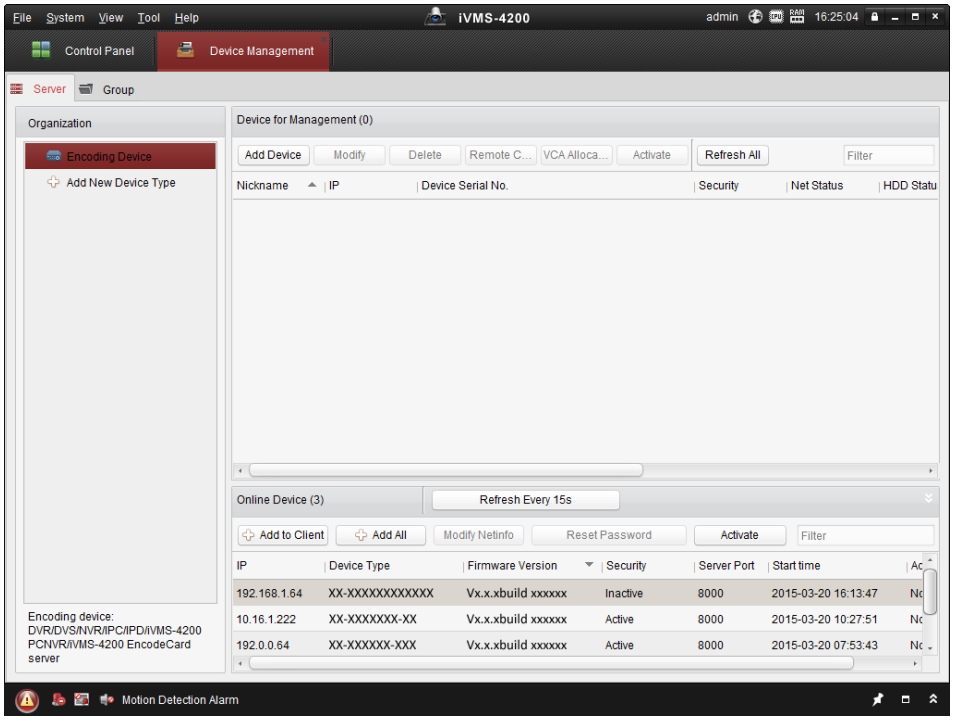


Figure 2-7 Device Management Interface

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.*

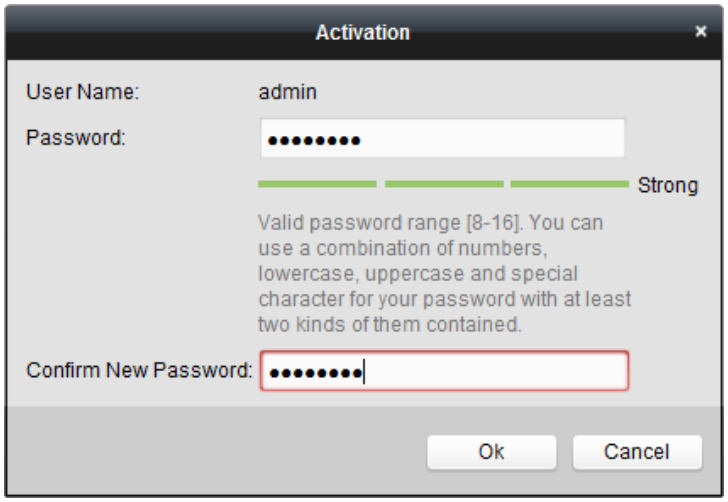


Figure 2-8 Activation Interface

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

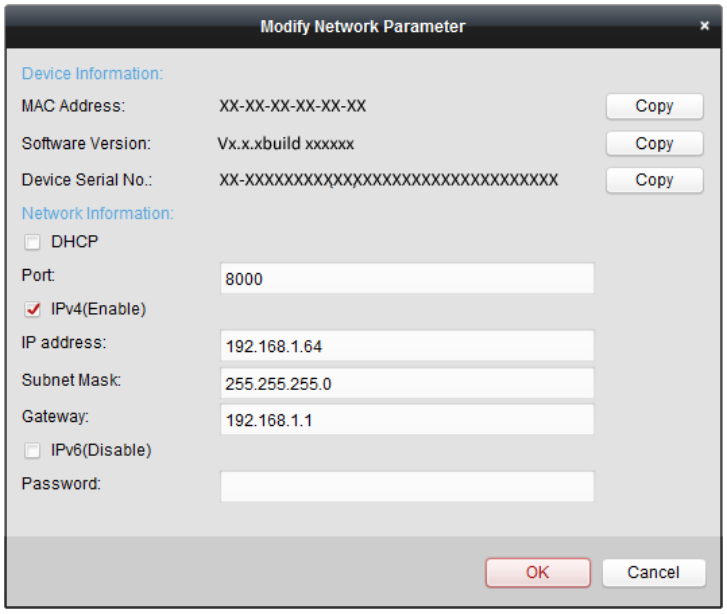


Figure 2-9 Modifying the Network Parameters

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

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.

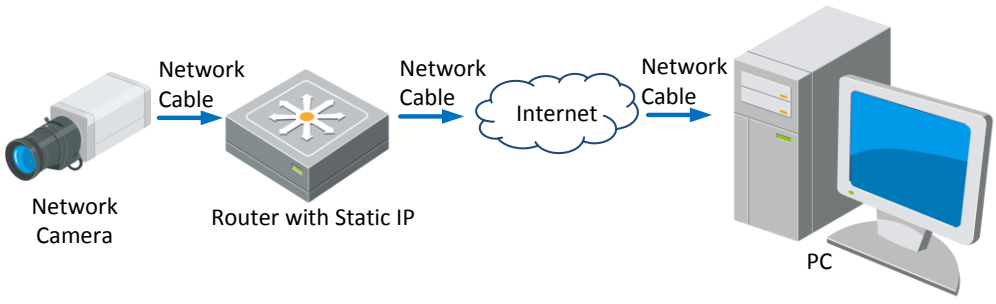


Figure 2-10 Accessing the Camera through Router with Static IP

- **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.

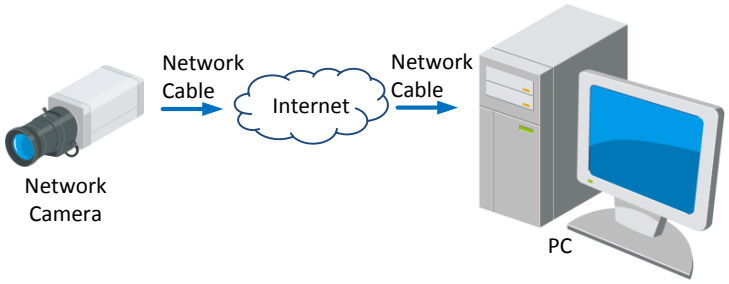


Figure 2-11 Accessing the Camera with Static IP Directly

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.

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 Login.

   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.

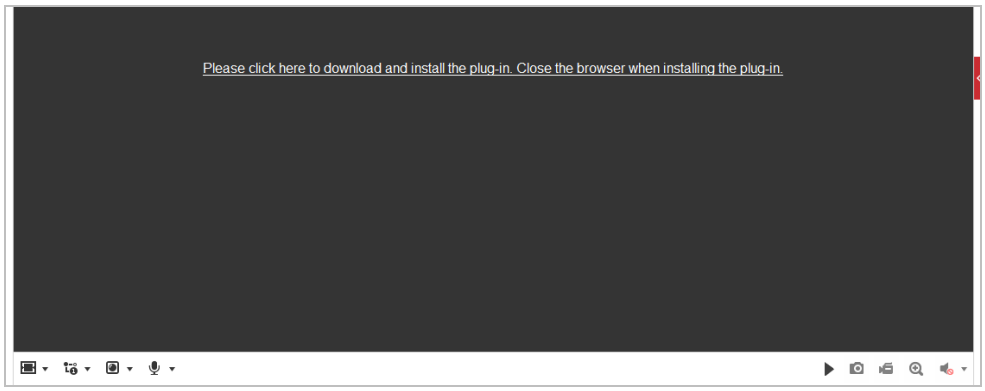


Figure 3-2 Download and Install Plug-in

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 below.

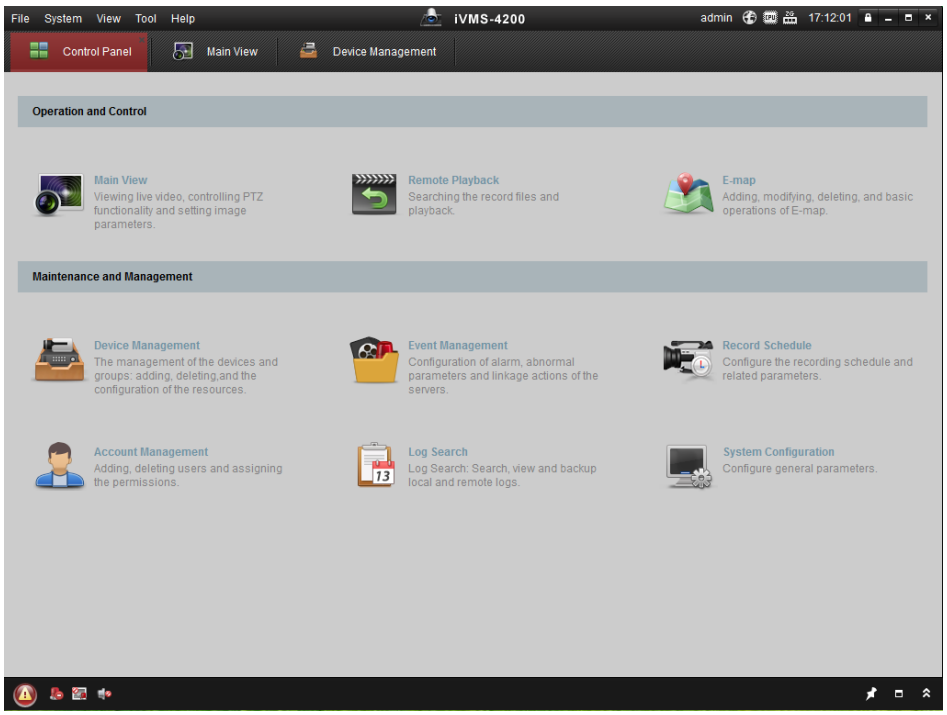


Figure 3-3 iVMS-4200 Control Panel

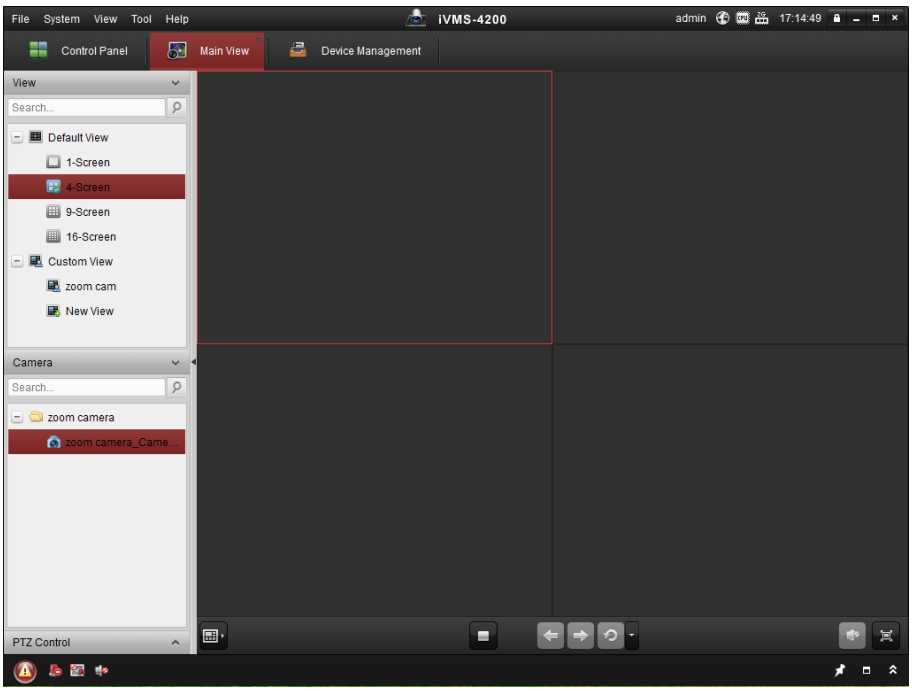


Figure 3-4 iVMS-4200 Live View Interface

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 the Local Configuration interface:

   Configuration > Local

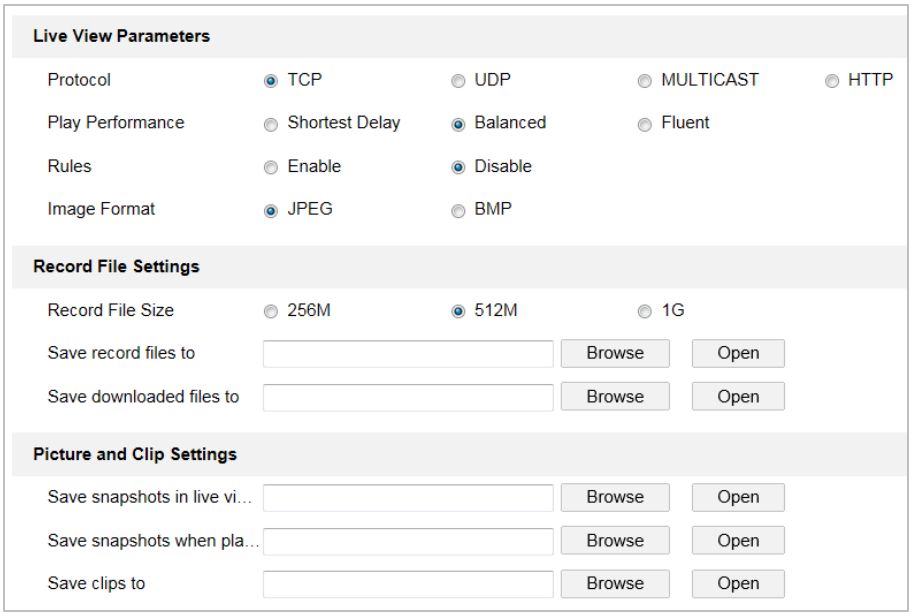


Figure 4-1 Local Configuration Interface

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.

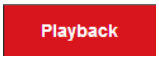
    TCP: Ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected.

    UDP: Provides real-time audio and video streams.

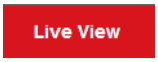
    MULTICAST: It's recommended to select the protocol type to **MULTICAST** when using the Multicast function.

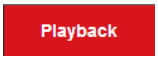
    HTTP: Allows the same quality as of TCP without setting specific ports for streaming under some network environments.
  - **Play Performance:** Set the play performance to Shortest Delay, Balanced, or Fluent.
  - **Rules:** You can enable or disable the rules of dynamic analysis for motion here.

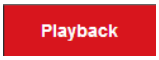
- **Image Format:** The captured pictures can be saved as different format. JPEG and BMP are available.

- **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.

  - 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.

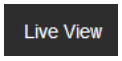
3. Click

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.

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

Descriptions of the live view page:

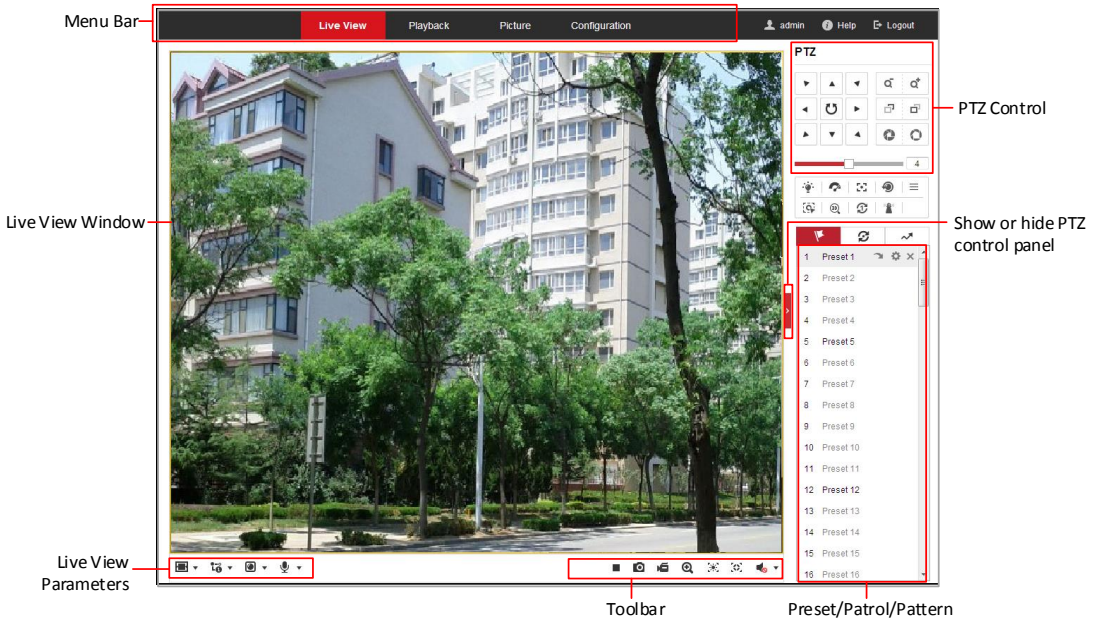


Figure 4-2 Live View Page

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.

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.

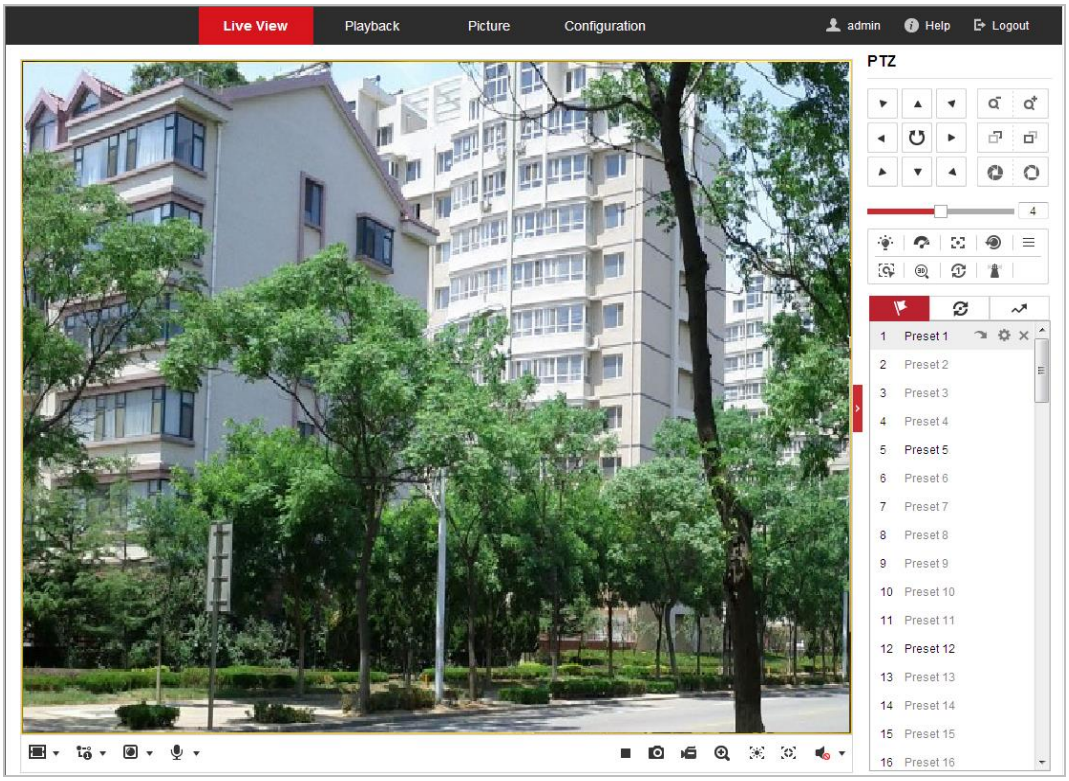


Figure 4-3 Start Live View

Table 4-1 Descriptions of the Toolbar

Icon	Description	Icon	Description
/	Start/stop Live view.		Manually capture the pictures.
/ / /	Display in 4:3/16:9/ original/ self-adaptive window size.	/ /	Live view with the main/sub/third stream.
/	Play via webcomponents/ quick time.	/	Start/stop two-way audio.
/	Manual start/stop recording.	/	Mute/audio on and adjust volume
/	Start/stop digital zoom.	/	Enable/disable regional exposure
/	Enable/disable regional focus		

- Double-click on the live video to switch the current live view into full-screen or return to normal mode from the full-screen.
- Click to select from and display live video in 4:3/16:9/ original/self-adaptive window size.
- Click to select from and display live video with the main/ sub/third stream. The main stream is with a relatively high resolution and needs much bandwidth. The default setting of stream type is .

© Hikvision

- Click to select between and play the live video via player **Webcomponents** or **Quick Time**. The live video is played via webcomponents by default, and other types of players are supported for the browser, such as MJPEG, and VLC. You are required to download and install the player to play the live video.
- Click and it displays . Click to enable two-way audio and the icon turns into . Click the icon again to stop two-way audio.
- Click to start live view and the icon turns into . Click the icon again to stop live view.
- Click to capture the picture.
- Click to start recording and the icon turns into . Click the icon again to stop recording.
- 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.
- Click to display the . Drag the slider to adjust the volume.

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.

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.

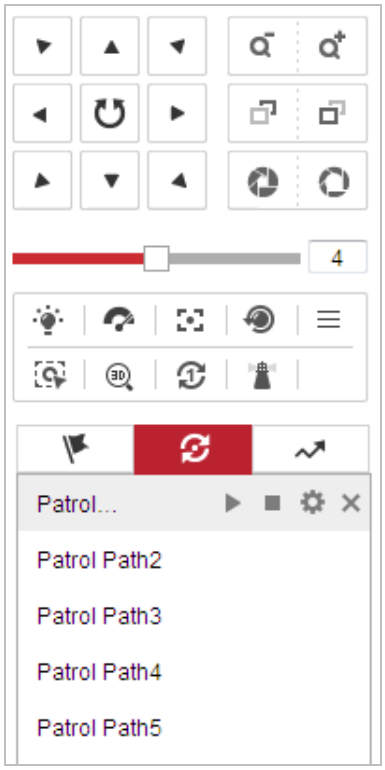


Figure 4-4 PTZ Control Panel

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.

Button	Name	Description
	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, 3D positioning, one-touch patrol, and one-touch park.
	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.
	Pattern	Refer to***4.4.6*** for detailed information of setting pattern.

- **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 the figure below:

© Hikvision

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.

- Manual Tracking

Before you start:

Enter the Smart Tracking settings interface and enable smart tracking first.

Configuration > PTZ > Smart Tracking

Steps:

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

- 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.

- One-touch Patrol

  Click to call one-touch patrol. For detailed information of setting one-touch patrol, refer to ***4.4.5 One-touch Patrol***.

- One-touch Park

  Click to save the current view as the preset No. 32 and start park at the the current position.

© Hikvision

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.

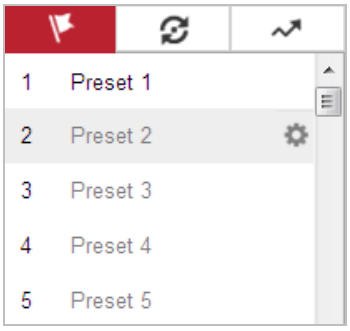


Figure 4-6 Setting a Preset

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.

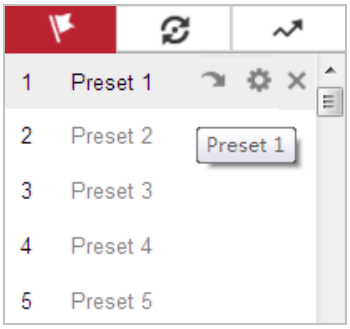


Figure 4-7 Calling a Preset

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.

NOTE

- The following presets are predefined with special commands. You can only call them but not configure them. For instance, preset 99 is the “Start auto scan”. If you call the preset 99, the camera starts auto scan function.
- Pattern function varies depending on different camera models.

Table 4-4 Special Presets

Preset	Function	Preset	Function
33	Auto flip	92	Start to set limit stops
34	Back to initial position	93	Set limit stops manually
35	Call patrol 1	94	Remote reboot
36	Call patrol 2	95	Call OSD menu
37	Call patrol 3	96	Stop a scan
38	Call patrol 4	97	Start random scan
39	Day mode (IR cut filter in)	98	Start frame scan
40	Night mode (IR cut filter out)	99	Start auto scan
41	Call pattern 1	100	Start tilt scan
42	Call pattern 2	101	Start panorama scan
43	Call pattern 3	102	Call patrol 5
44	Call pattern 4	103	Call patrol 6
45	One-touch Patrol	104	Call patrol 7
90	Wiper	105	Call patrol 8

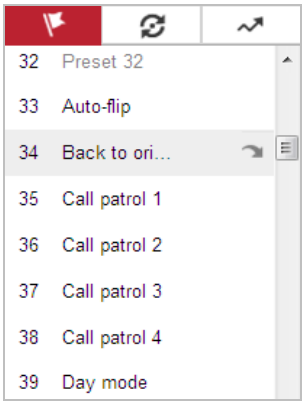


Figure 4-8 Special Preset

NOTE

You may need to use the OSD (On Screen Display) menu when controlling the camera remotely. To display the OSD menu on the live view screen, you can call the preset number 95.

© Hikvision

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.

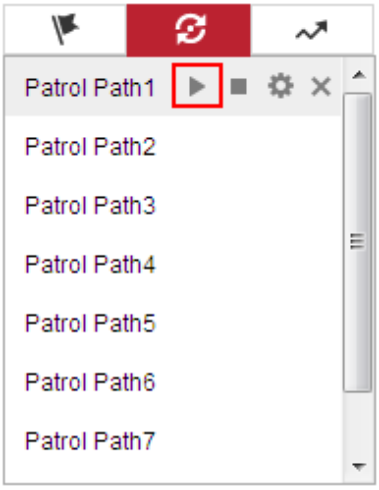


Figure 4-10 Calling a Preset

4.4.5 One-touch Patrol

Purpose:

One-touch patrol is an automatically created patrol. The system automatically add preset No.1 to No.32 to the patrol path 8. You can call the one-touch patrol and the camera moves as the patrol path 8 automatically.

Steps:

1. Set preset No.1 to No.32. Refer to ***4.4.3 Setting/Calling a Preset*** for detailed information of setting preset.
2. Call preset No. 45, and the camera moves as patrol path 8.
3. Click to enter the patrol settings interface and start/stop one-touch patrol, edit the patrol time and the speed.
4. You can click of the PTZ control panel to start one-touch patrol.

Figure 4-11 Patrol Path 8

4.4.6 Setting/Calling a Pattern

Purpose:

A pattern is a memorized series of pan, tilt, zoom, and preset functions. It can be called on the pattern settings interface. There are up to 4 patterns for customizing.

NOTE

Pattern function varies depending on different camera models.

- **Setting a Pattern:**

Steps:

1. In the PTZ control panel, click to enter the pattern settings interface.
2. Select a pattern number from the list as shown in Figure 4-12.

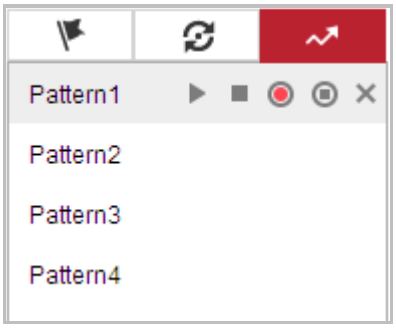


Figure 4-12 Patterns Settings Interface

3. Click to enable recording the panning, tilting and zooming actions.
4. Use the PTZ control buttons to move the lens to the desired position after the information of **PROGRAM PATTERN REMAINNING MEMORY(%)** is displayed on the screen.
   - Pan the camera to the right or left.
   - Tilt the camera up or down.
   - Zoom in or out.
   - Refocus the lens.
5. Click to save all the pattern settings.

- **Buttons on the Patterns interface:**

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.

© Hikvision

- These 4 patterns can be operated separately and with no priority level.
- When configuring and calling the pattern, proportional pan is valid; the limit stops and auto flip will be invalid; and the 3D positioning operation is not supported.

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.

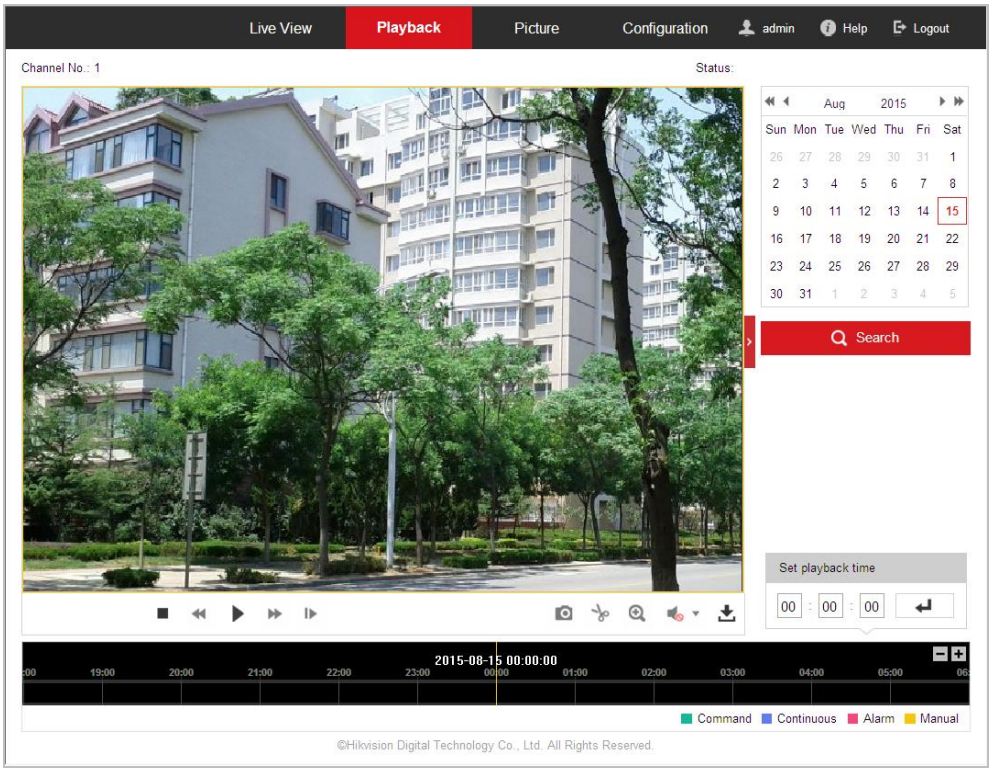


Figure 4-13 Playback Interface

2. Select the date and click Search.

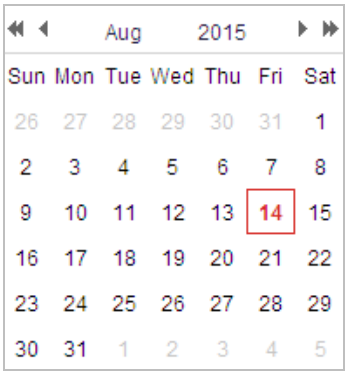


Figure 4-14 Search Video

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 4-15 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		

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.

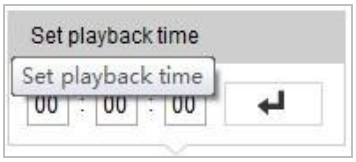


Figure 4-16 Set Playback Time

© Hikvision

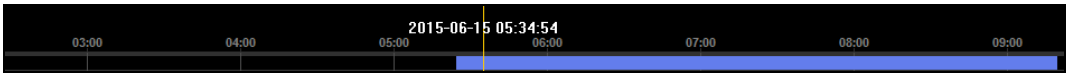


Figure 4-17 Progress Bar

The different colors of the video on the progress bar stand for the different video types as shown in Figure 4-18.

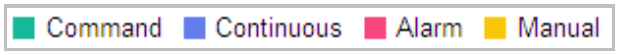


Figure 4-18 Video Types

4.5.2 Downloading Video Files

Steps:

1. Click on the playback interface. The pop-up menu is shown in Figure 4-19.
2. Set the start time and end time. Click **Search**. The corresponding video files are listed on the left.

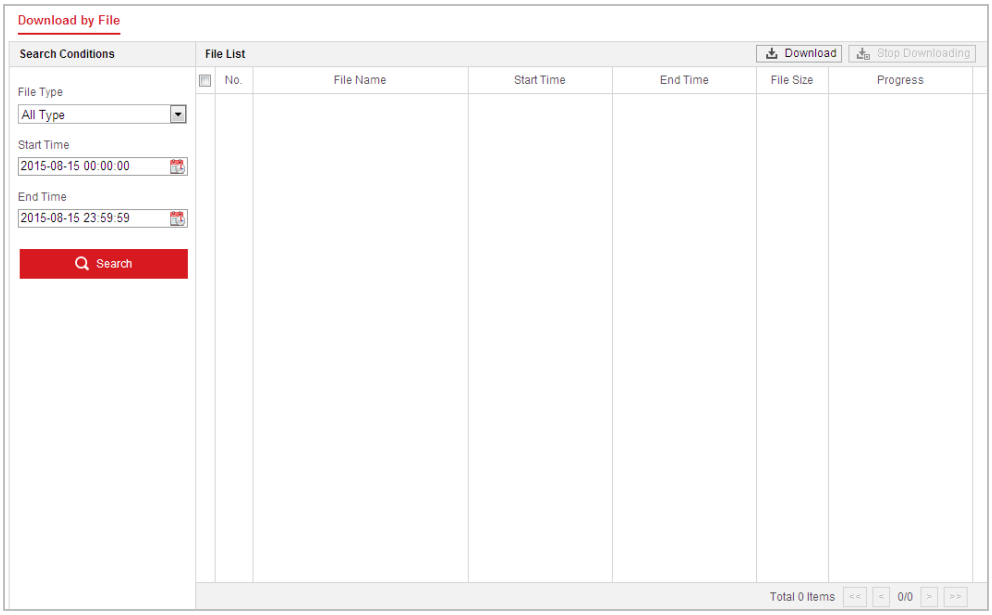


Figure 4-19 Video Downloading interface

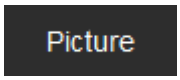
3. Check the checkbox in front of the video files that you need to download.
4. Click Download to download the video files.

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.

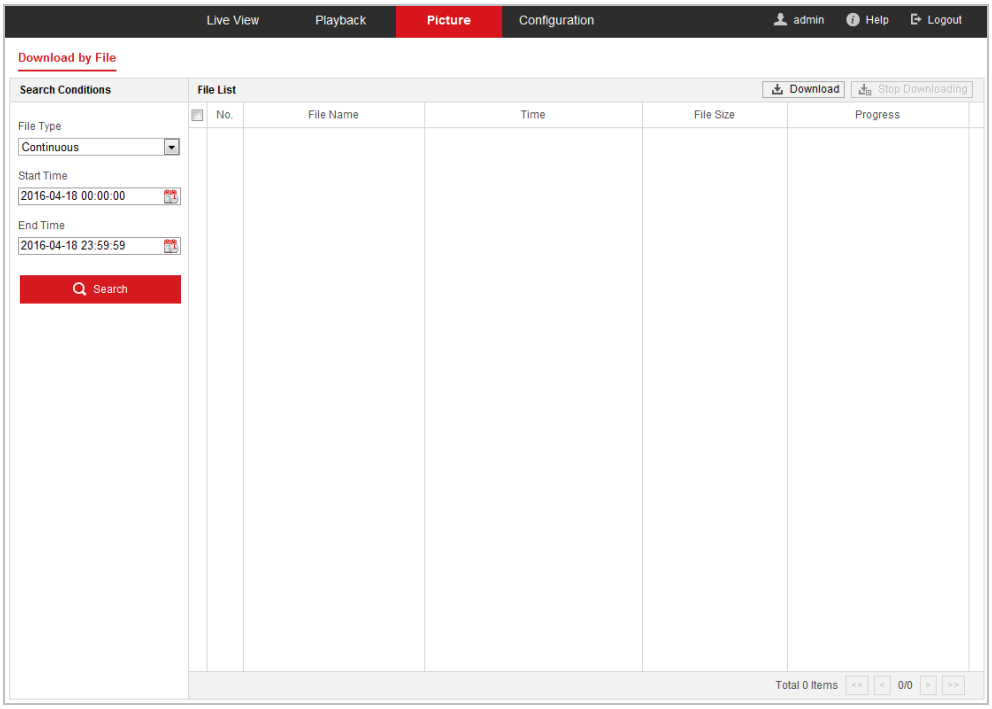


Figure 4-20 Picture Interface

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

to download the files.

© Hikvision

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 the Record Schedule settings interface:
   Configuration > Storage > Schedule Settings > Record Schedule

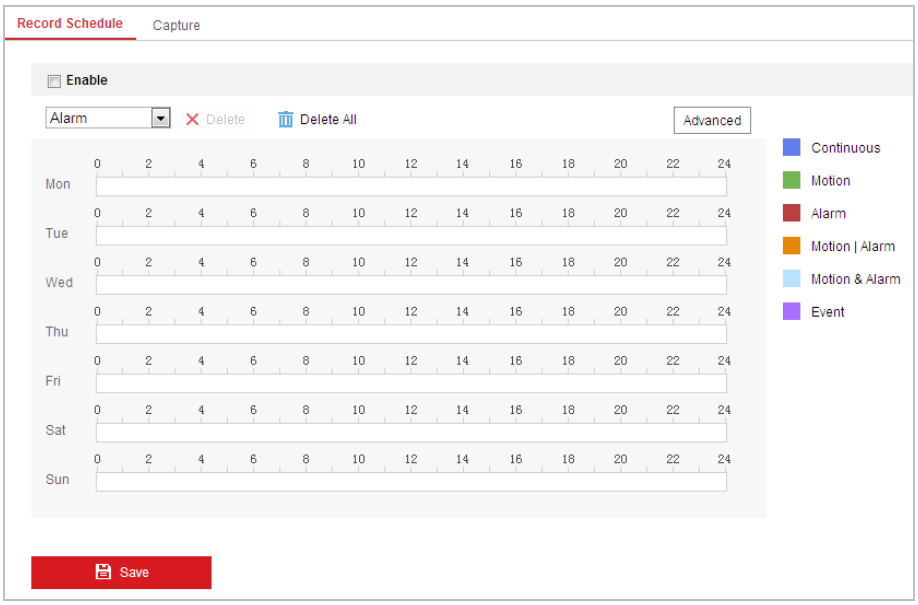


Figure 5-1 Recording Schedule Interface

2. Check the checkbox of **Enable** to enable scheduled recording.
3. To set the advanced settings of the camera, click Advanced to enter the advanced settings interface.

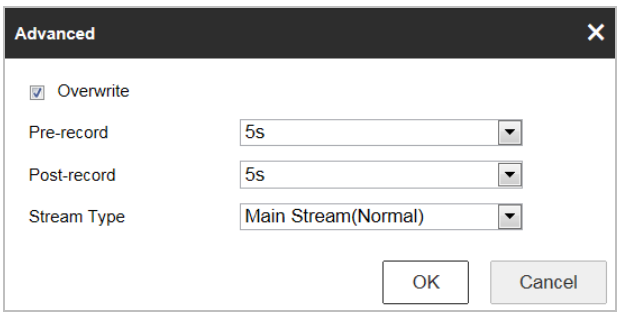


Figure 5-2 Record Parameters

- **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.

4. Click **OK** to save the advanced setting.
5. 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.

6. 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 the Snapshot settings interface:

   Configuration > Storage > Storage Settings > Capture

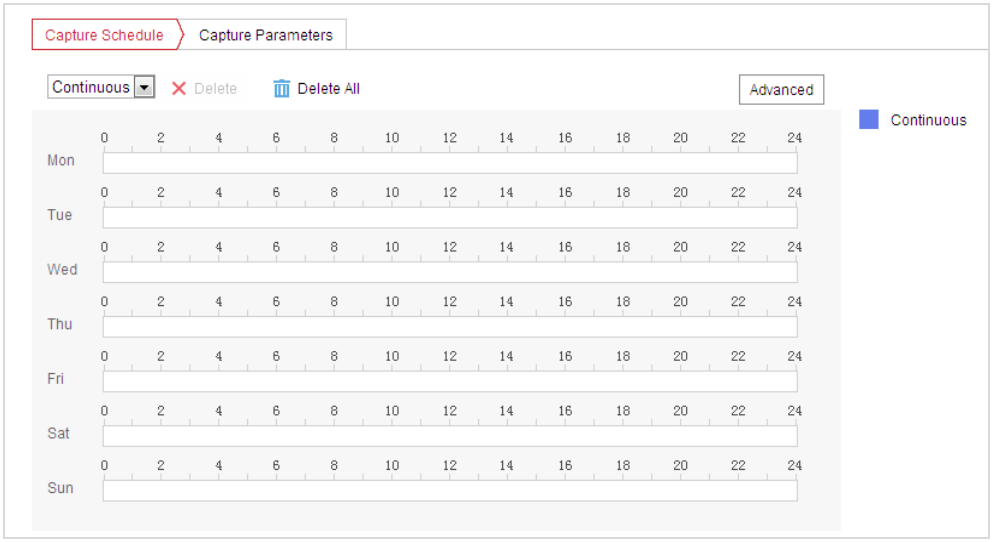
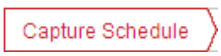


Figure 5-3 Snapshot Settings

2. Click 

to enter the Capture Schedule interface.
3. 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).
4. After you set the scheduled task, you can click and copy the task to other days (optional).
5. 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)

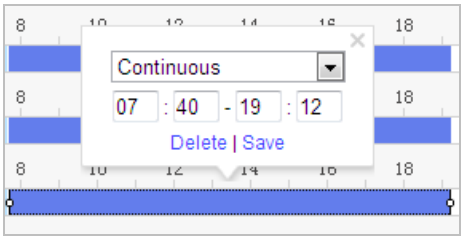


Figure 5-4 Segment Snapshot Settings

6. Click Advanced to enter the advanced setting interface. You can select the stream type of the capture.
7. Click Capture Parameters to enter the Capture Parameters Interface.
8. 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.
9. Select the format, resolution, quality of the snapshot.
10. Set the time interval between two snapshots.
11. 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:

© Hikvision

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 the NAS (Network-Attached Storage) settings interface:
   Configuration > Storage > Storage Management > Net HDD

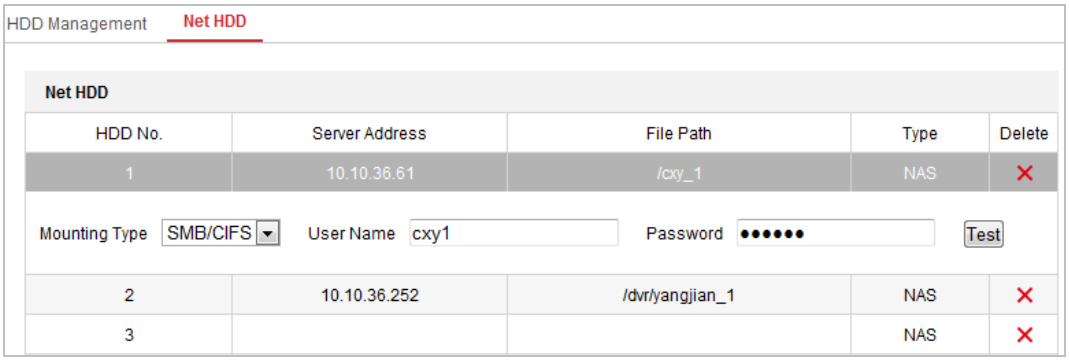


Figure 5-5 Select Net HDD Type

2. Enter 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.

   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 Save to add the network disk.

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

- **Initialize the added network disk.**

1. Enter the HDD settings interface (**Configuration > Storage > Storage Management > HDD Management**), in which you can view the capacity, free space, status, type and property of the disk.

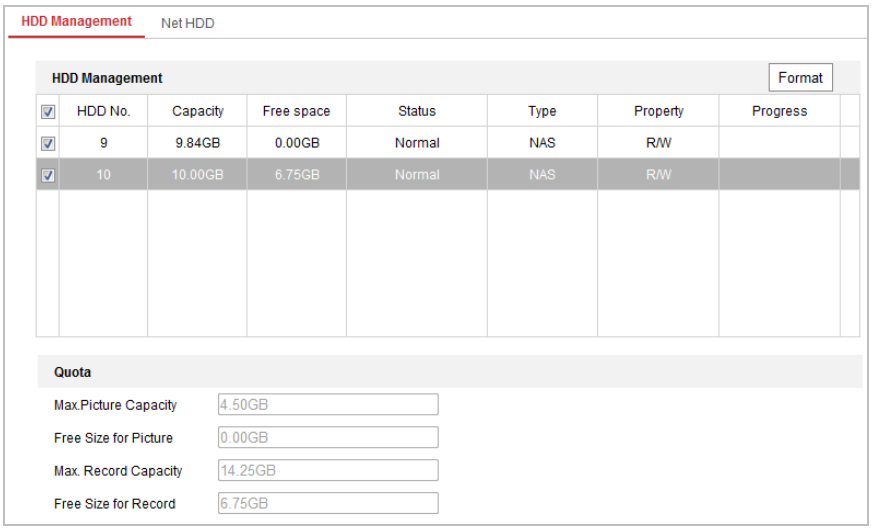


Figure 5-6 Storage Management Interface

2. If the status of the disk is **Uninitialized**, check the corresponding checkbox to select the disk and click **Format** to start initializing the disk.
3. When the initialization completed, the status of disk will become **Normal** as shown in Figure 5-7**.**

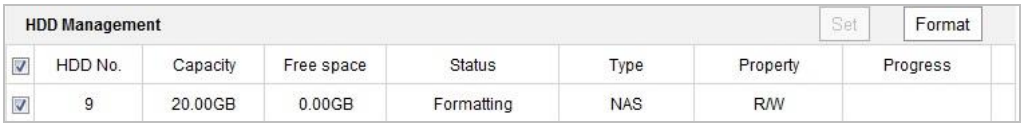


Figure 5-7 View Disk Status

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

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

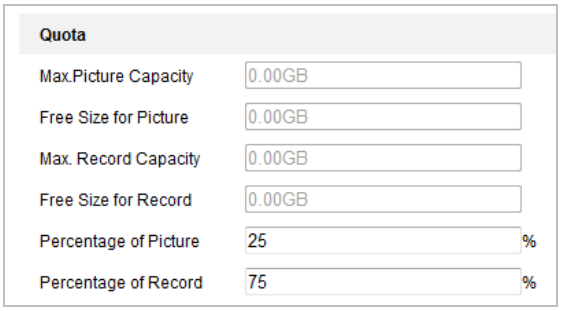


Figure 5-8 Quota Settings

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

5.2 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.

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.

5.2.1 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 surveillance scene.

Steps:

1. Enter the motion detection setting interface:
   Configuration > Event > Basic Event > Motion Detection
2. Check the checkbox of the **Enable Motion Detection** to enable this function.
   You can check the **Enable Dynamic Analysis for Motion** checkbox if you want the detected object get marked with rectangle in the live view.
3. Select the configuration mode as **Normal** or **Expert** and set the corresponding motion detection parameters.
   - **Normal**

Figure 5-9 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 draw up to 8 motion detection areas on the same image.
- You can click Clear All to clear all of the areas.

(3) Move the slider Sensitivity 0 to set the sensitivity of the detection.

- **Expert**

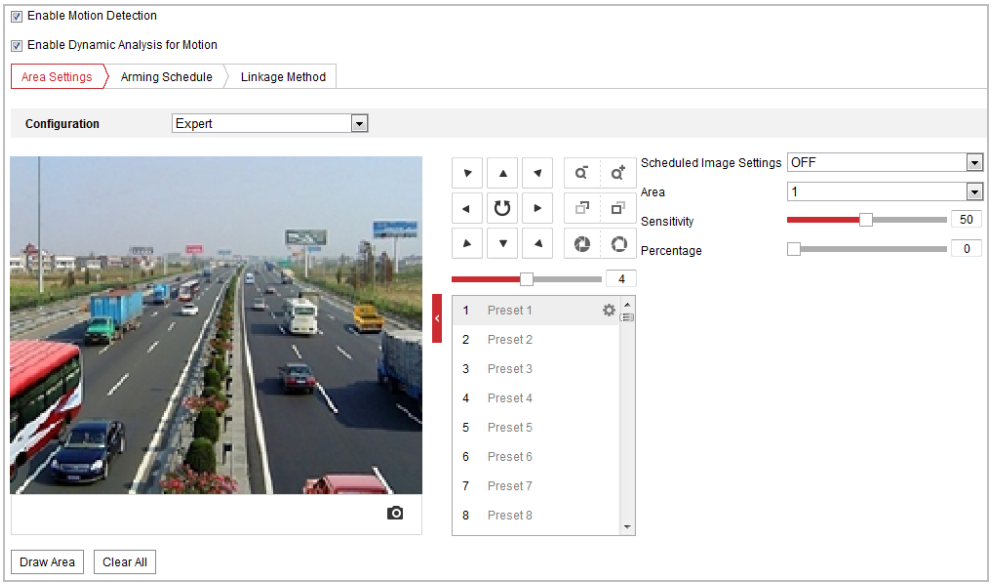


Figure 5-10 Motion Detection Settings-Expert

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 at 6:00 a.m., and switch to the night mode at 18:00 p.m..

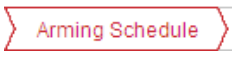
(2) Select **Area No.** to configure in the dropdown list.

(3) Set the values of sensitivity and proportion of object on area.

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

Proportion of Object on Area: 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.

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

(1) Click 

tab to enter the arming schedule setting interface.

Figure 5-11 Arming Schedule

(2) Select the timeline of a certain day, 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).

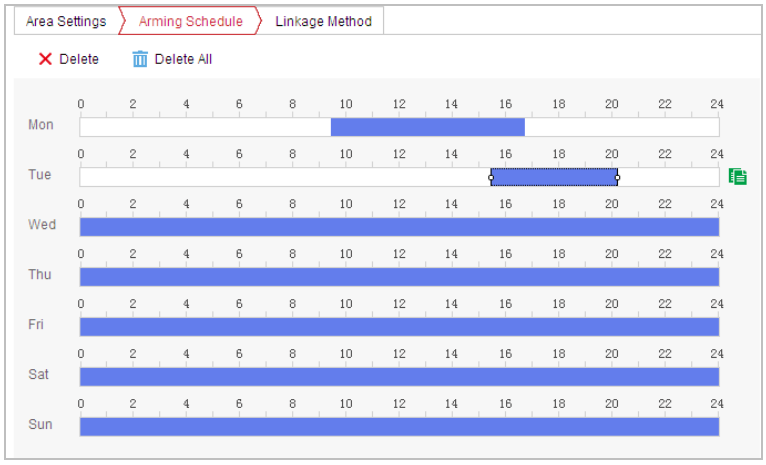


Figure 5-12 Arming Time Schedule

(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).

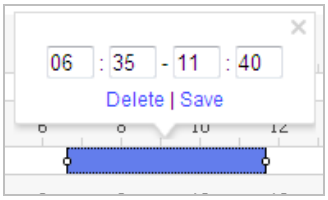


Figure 5-13 Segment Arming Settings

(5) Click Save to save the settings.

NOTE

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

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

Click Linkage Method tab to enter the **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.

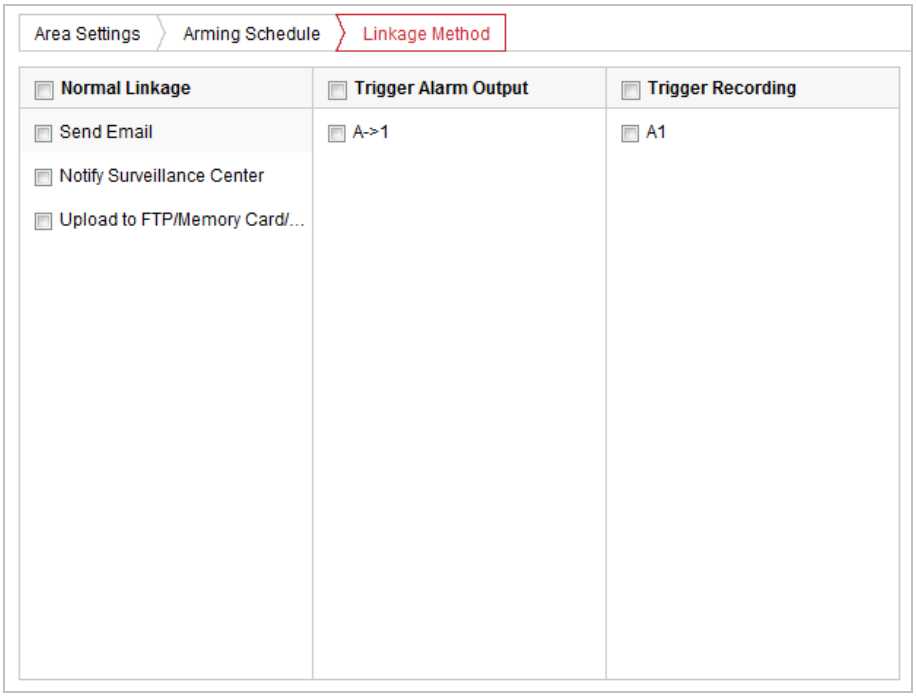


Figure 5-14 Linkage Method

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.

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.

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.

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 the Video Tampering settings interface ：
   Configuration > Event > Basic Event > Video Tampering

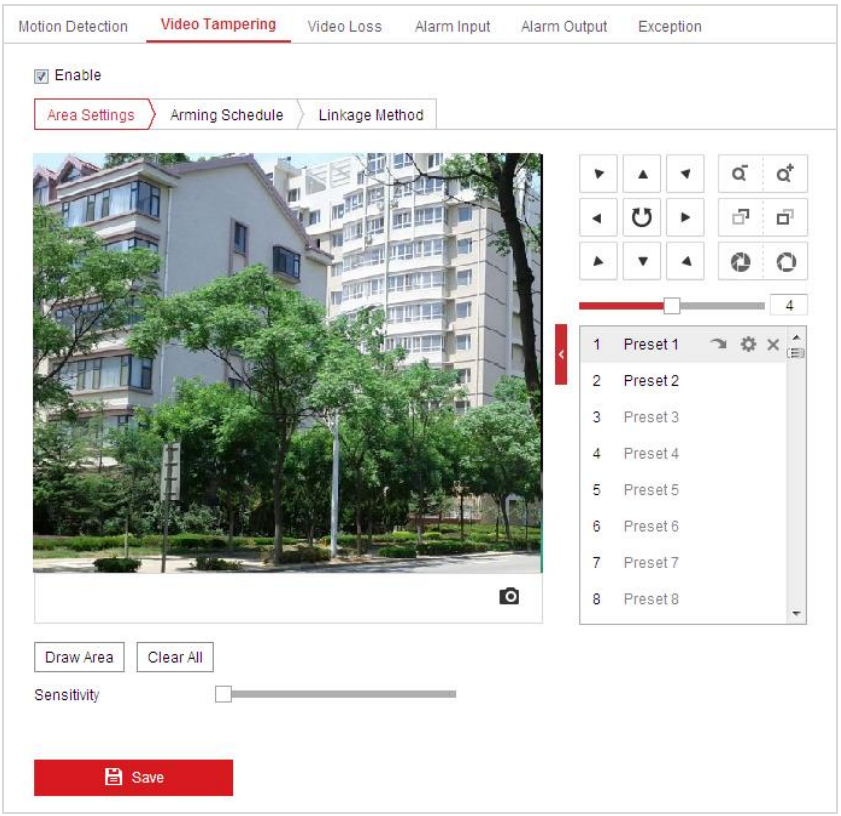


Figure 5-15 Tampering Alarm

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

5.2.3 Configuring Alarm Input

Steps:

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

© Hikvision

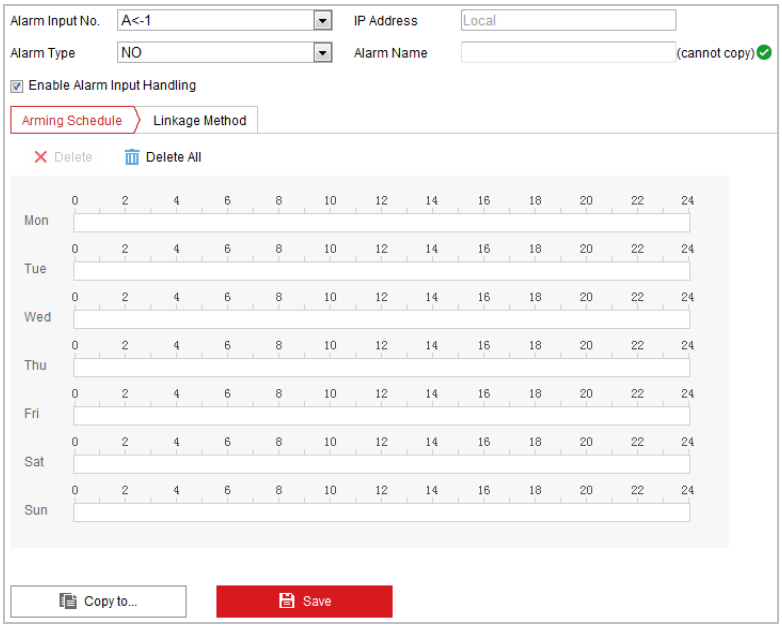


Figure 5-16 Alarm Input Settings

4. 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***.

5. 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***.

6. 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 Save to save the settings.

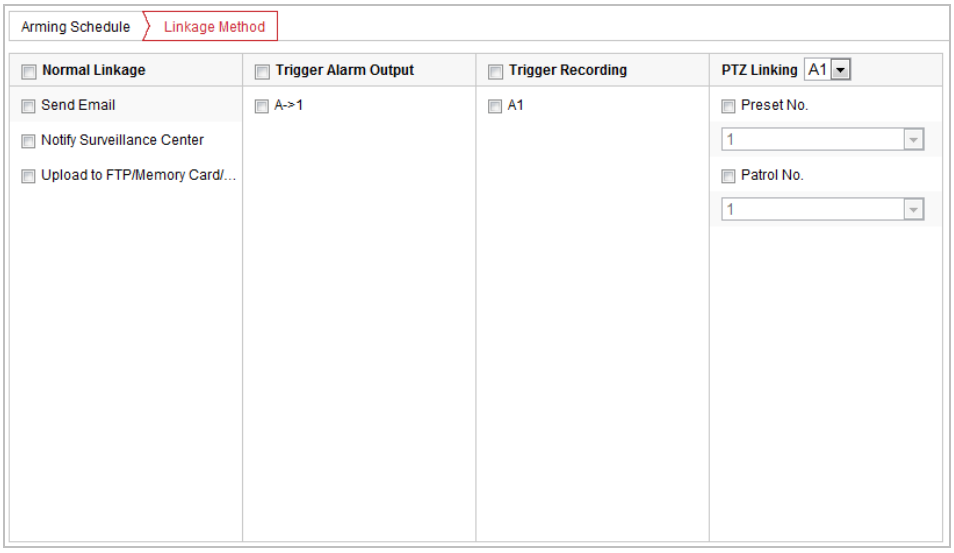
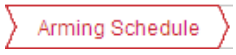


Figure 5-17 Linkage Method

5.2.4 Configuring Alarm Output

Steps:

1. Enter the 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

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***.

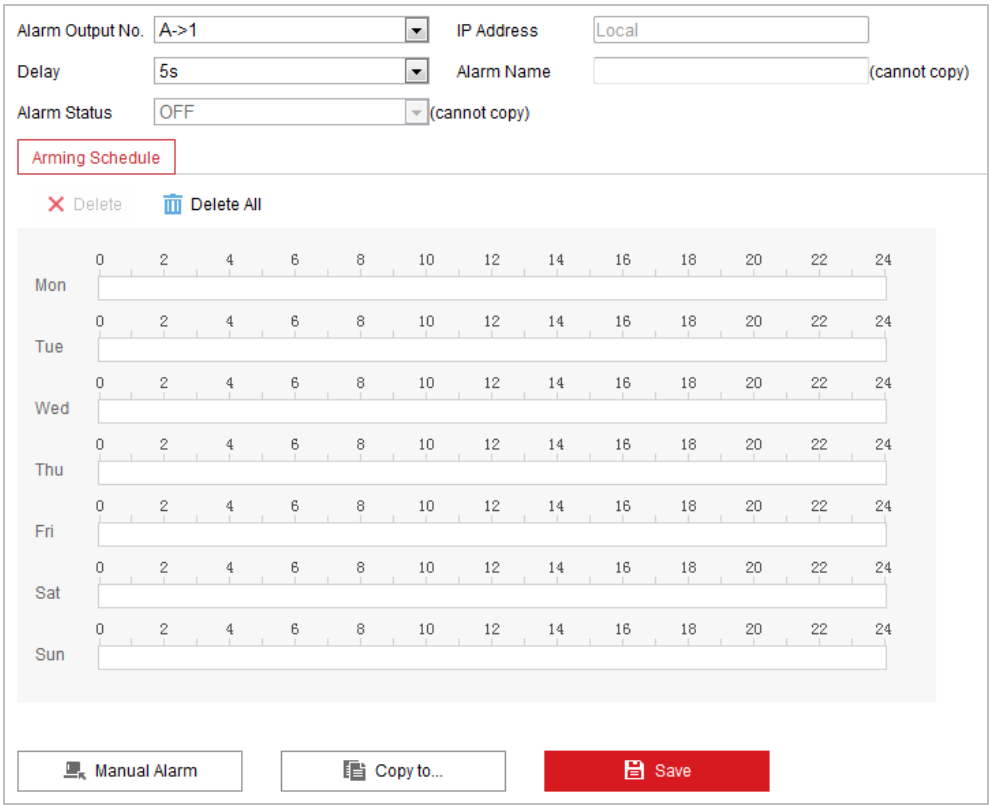


Figure 5-18 Alarm Output Settings

6. You can copy the settings to other alarm outputs.
7. 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:

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

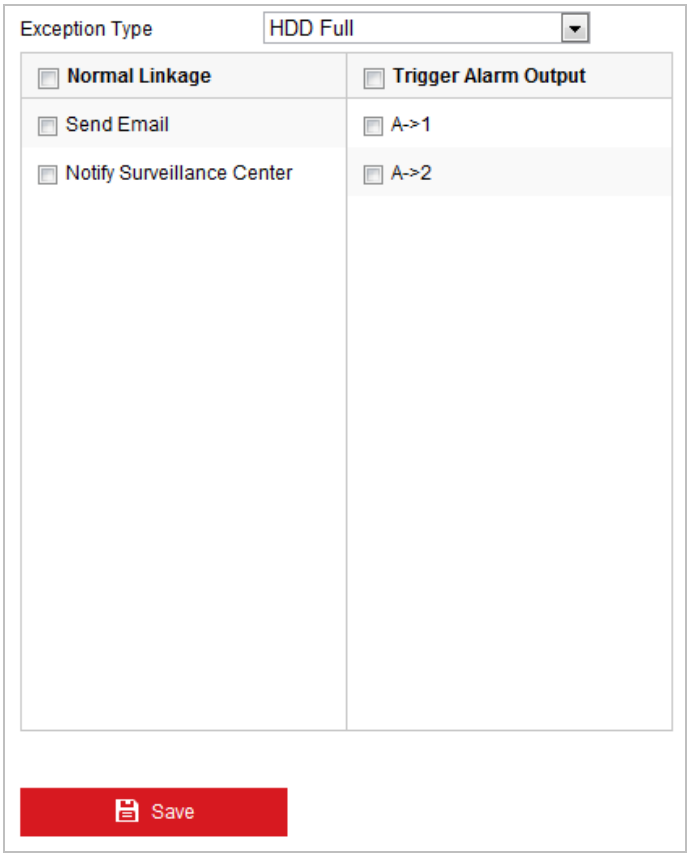


Figure 5-19 Exception Settings

3. Click to save the settings.

5.3 Smart Event Configuration

NOTE

The functions vary depending on different camera models.

5.3.1 Detecting Audio Exception

Purpose:

When you enable this function and audio exception occurs, the alarm actions will be triggered.

Steps:

1. Enter the video audio exception detection interface:

   Configuration > Event > Smart Event > Audio Exception Detection

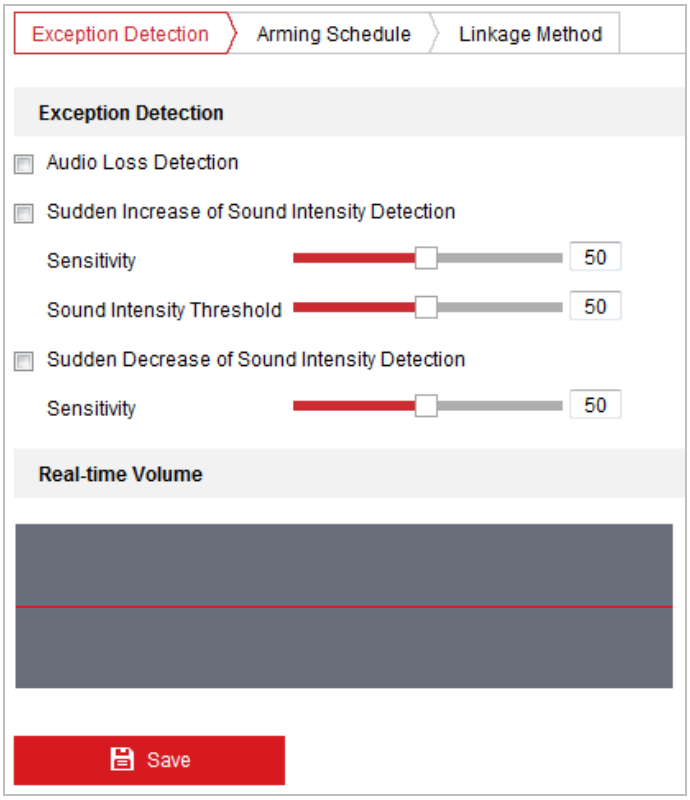


Figure 5-20 Audio Exception Detection

2. Check the checkbox of **Audio Loss Detection** to enable the audio input exception detection.
3. Check the checkbox of **Sudden Increase of Sound Intensity Detection** checkbox to enable the sudden rise detection.
   - **Sensitivity**: Range [1-100], the smaller the value the more severe the sound change will trigger the detection.
   - **Sound Intensity Threshold**: Range [1-100], it can filter the sound in the environment, the louder the environment sound, the higher the value should be. You can adjust it according to the actual environment.
4. Check the checkbox of **Sudden Decrease of Sound Intensity Detection** checkbox to enable the sudden drop detection.

   Sensitivity: Range [1-100], the smaller the value the more severe the sound change will trigger the detection.
5. Click Arming Schedule 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***.

6. Click Linkage Method tab to select the linkage method taken for the audio input exception, Notify Surveillance Center, Send Email, Trigger Alarm Output and Trigger Recording are selectable. Refer to ***Section 5.2.1 Configuring Motion Detection***.

7. Click Save to save the settings.

5.3.2 Configuring Intrusion Detection

Intrusion detection can set an area in the surveillance scene and once the area is entered, a set of alarm action is triggered.

Steps:

1. Enter the intrusion detection interface:

   Configuration > Events > Smart Event >Intrusion Detection

2. Check the **Enable Intrusion Detection** checkbox.

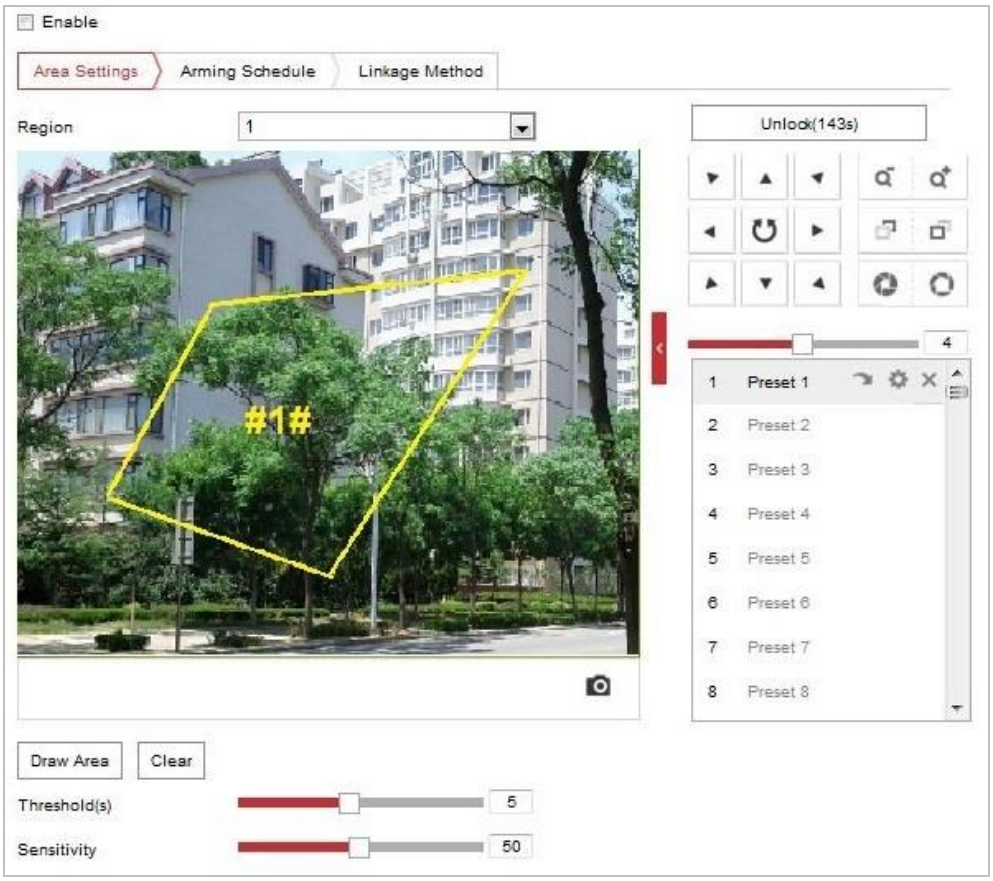


Figure 5-21 Configuring Intrusion Area

3. The event triggered and park action related PTZ movement will be locked for 180 seconds after you enter the intrusion detection interface. Optionally, you can click the Unlock(69s) button to manually activate the movement, or lock the movement

when the button turns to Lock by clicking it.

4. Draw area.
   1) Select the Region No.in dropdown list.
   2) Click Draw Area to draw a rectangle on the image as a defense region.
   3) Click on the image to specify a corner of the rectangle, and right-click the mouse after four corners are configured.

NOTE

Up to four areas are supported. You can click Clear to clear the areas you drawn.

5. Configure the parameters for each defense region separately.
   - **Threshold:** Range [0-10s], the threshold for the time of the object loitering in the region. If you set the value as 0, alarm is triggered immediately after the object entering the region.
   - **Sensitivity:** Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm, when the sensitivity is high, a very small object can trigger the alarm.
6. Click Arming Schedule 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***.
7. Click Linkage Method tab to select the linkage method taken for intrusion detection, Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Alarm Output and Trigger Recording are selectable. Refer to ***Section 5.2.1 Configuring Motion Detection***.
8. Click Save to save the settings.

5.3.3 Configuring Line Crossing Detection

The virtual plane detection can be adopted for the intrusion detection. Once the virtual plane is detected being traversed according to the configured direction, a set of alarm action is triggered.

Steps:

1. Enter the Line Crossing Detection interface:

   Configuration >Event > Smart Event > Line Crossing Detection
2. Check the **Enable** checkbox to enable the line crossing detection function.
3. Select the Line in dropdown list to configure.
4. The event triggered and park action related PTZ movement will be locked for 180 seconds after you enter the line crossing detection interface. Optionally, you can click the Unlock(69s) button to manually activate the movement, or lock the movement

when the button turns to Lock by clicking it.

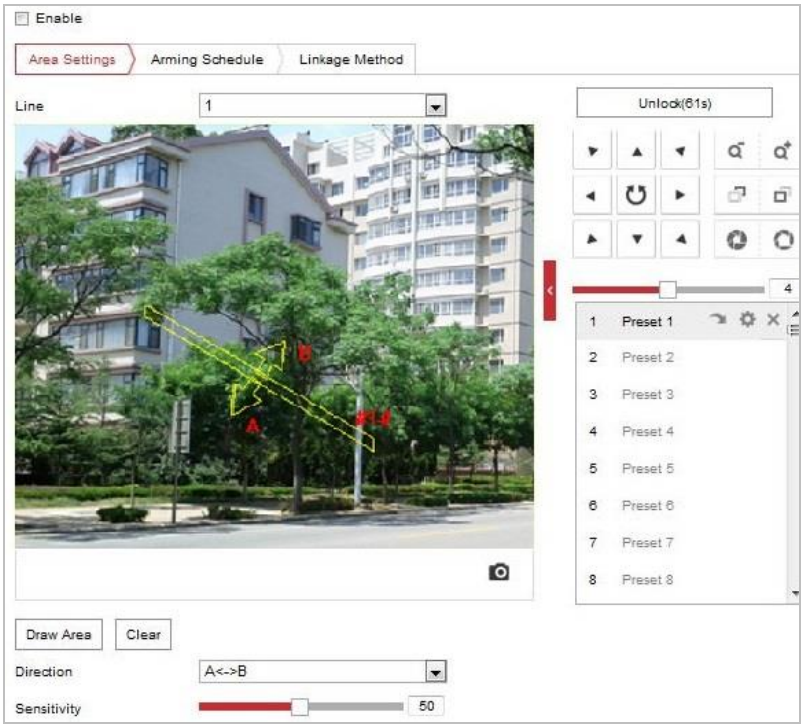


Figure 5-22 Configuring Line

5. Draw area.

   1) Click Draw Area to draw a line on the image.

   2) Click the line to switch to the editing mode.

      Drag an end to the desired place to adjust the length and angle of the line. And drag the line to adjust the location.

NOTE

Up to four lines are supported.

6. Configure the parameters for each defense region separately.

   - **Direction:** Select the detection direction in the dropdown list, there are A<->B, A->B and B->A selectable.
   - **Sensitivity:** Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm, when the sensitivity is high, a very small object can trigger the alarm.

7. Click Arming Schedule 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***.

8. Click Linkage Method tab to select the linkage method taken for the line crossing detection, Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Alarm

Output and Trigger Recording are selectable. Refer to ***Section 5.2.1 Configuring Motion Detection***.

9. Click Save to save the settings.

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

Purpose:

You can configure the basic PTZ parameters, including zooming speed and power off memory.

1. Enter the Basic PTZ Parameter Configuration interface:
   Configuration > **PTZ** > **Basic Settings**

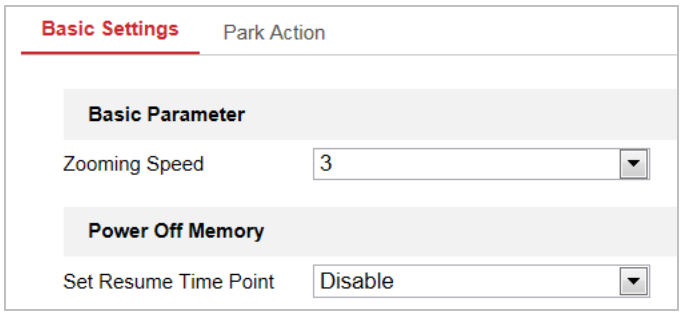


Figure 5-23 Basic PTZ Configuration Interface

2. Configure the following settings:

- **Basic Parameters**: Set the zooming speed from the dropdown list.
- **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 camera 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 Save to save the settings.

5.4.2 Configuring Park Actions

Purpose:

© Hikvision

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

NOTE

- **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 the Park Action settings interface:
   Configuration > **PTZ** > **Park Action**

Figure 5-24 Set the Park Action

2. Check the checkbox of **Enable Park Action**.
3. Set the **Park Time** as the inactivity time of the camera before it starts the park actions.
4. Choose **Action Type** the from the dropdown list.

Figure 5-25 Action Types

5. Select the **Action Type ID** from the dropdown list.
6. Click Save 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

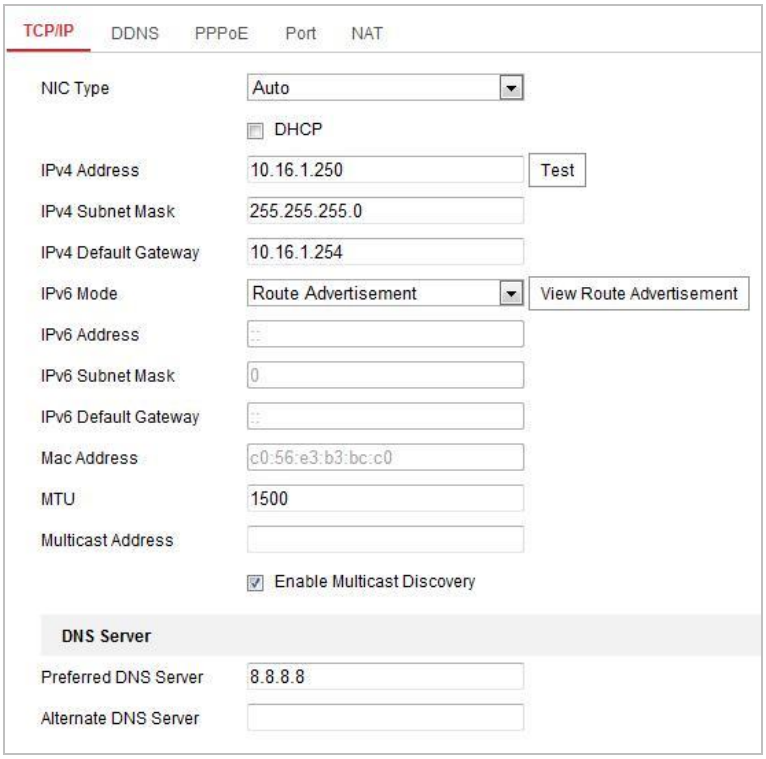


Figure 6-1 TCP/IP Settings

2. Configure the NIC settings, including the **IPv4(IPv6) Address**, **IPv4(IPv6) Subnet Mask** and **IPv4(IPv6) Default Gateway**.

3. Click Save to save the above settings.

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

NOTE

- 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 500 ~ 1500. The default value is 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**.

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 the DDNS settings interface:
   Configuration > Network > Basic Settings > DDNS

2. Check the **Enable DDNS** checkbox to enable this feature.
3. Select **DDNS Type**. Two DDNS types are selectable: DynDNS and NO-IP.

- **DynDNS:**

Steps:

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

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

(3) Enter the **Port** of DynDNS server.

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

(5) Click Save to save the settings.

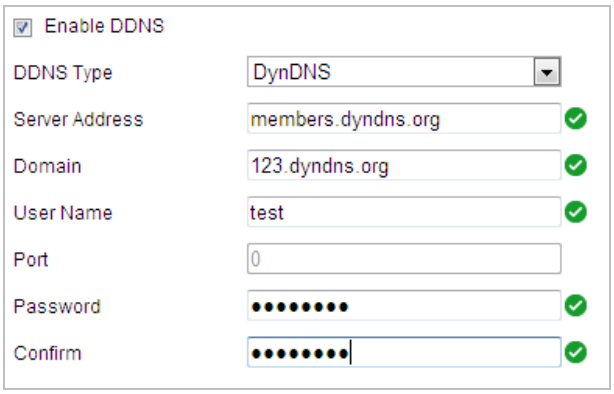


Figure 6-3 DynDNS Settings

- **NO-IP:**

Steps:

(1) Enter **Server Address** of NO-IP.

(2) In the **Domain** text field, enter the domain name obtained from the NO-IP website.

(3) Enter the **Port** of NO-IP server.

(4) Enter the **User Name** and **Password** registered on the NO-IP website.

(5) Click Save 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 the 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 Save 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 the Port settings interface:

   Configuration > Network > Basic Settings > Port

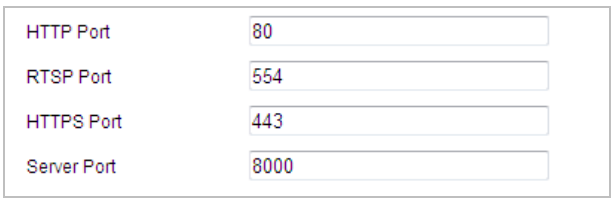


Figure 6-5 Port Settings

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.

3. Click Save 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 the UPnP™ settings interface.

   Configuration >Network > Basic Settings > NAT

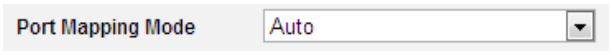
2. Check the checkbox to enable the UPnP™ function.

   NOTE

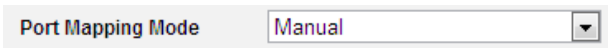
   You can edit the Friendly Name of the camera. This name can be detected by corresponding device, such as a router.

3. Set the port mapping mode:

   To port mapping with the default port numbers:

   Choose 

   To port mapping with the customized port numbers:

   Choose 

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

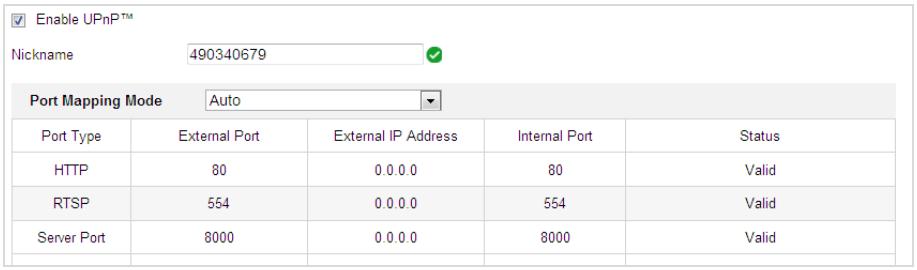


Figure 6-6 Port Mapping Mode

4. Click Save 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 the SNMP settings interface:

   Configuration > Network > Advanced Settings > SNMP

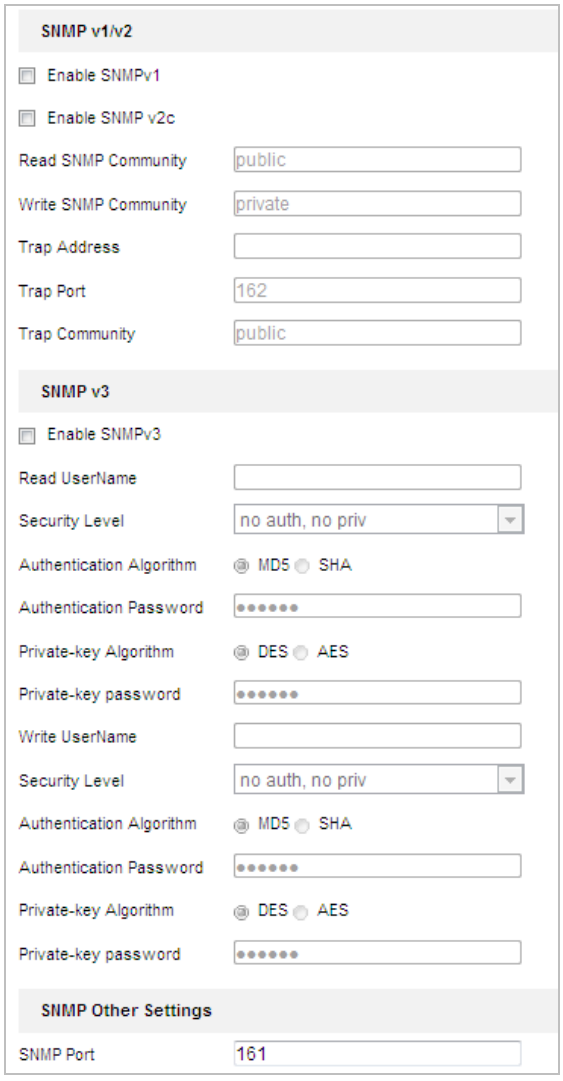


Figure 6-7 SNMP Settings

2. Check the corresponding version checkbox (**Enable SNMP v1**, **Enable SNMP v2c**, **Enable SNMP v3**) to enable the feature.
3. Configure the SNMP settings.

NOTE

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

4. Click Save 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:

1. Enter the FTP settings interface:

   Configuration > Network > Advanced Settings > FTP

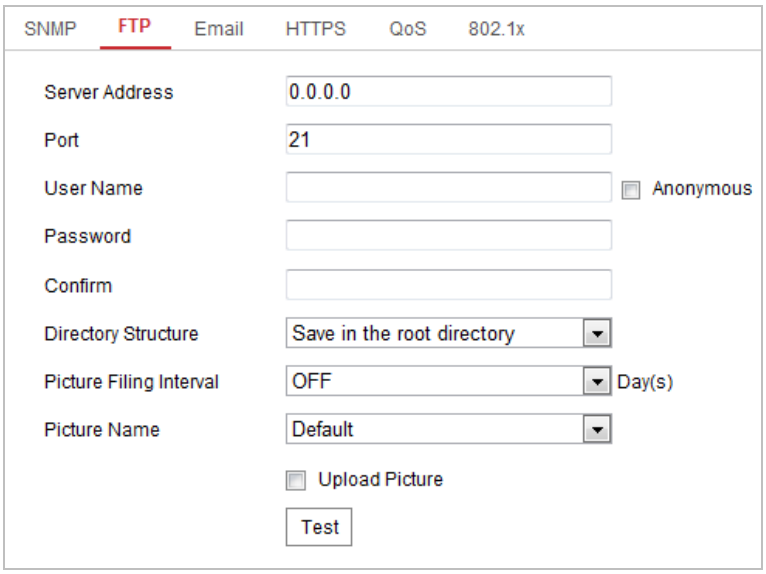


Figure 6-8 FTP Settings

2. 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 following Figure 6-9.

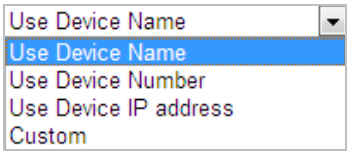


Figure 6-9 Parent Directory

  - **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 following Figure 6-10.

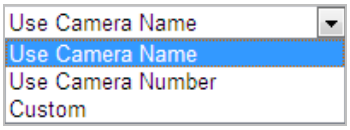


Figure 6-10 Child Directory

- **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 the Email settings interface:

   Configuration> Network > Advanced Settings > Email

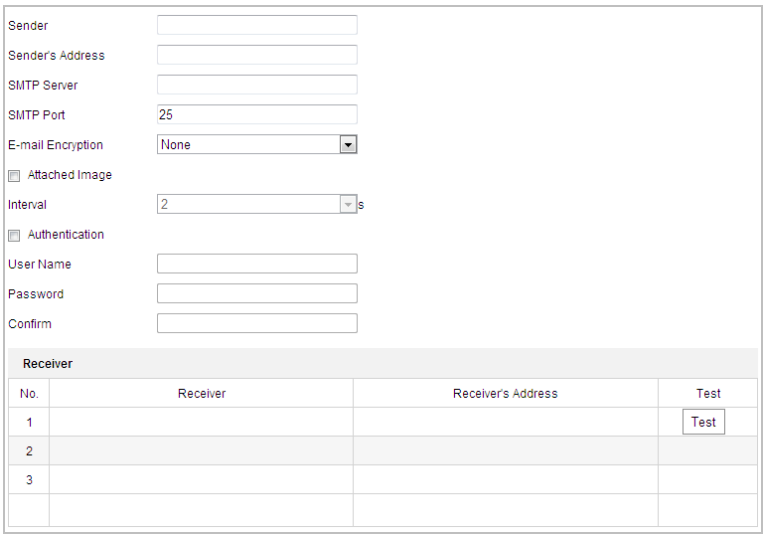


Figure 6-11 Email Settings

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 enter 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.)

3. Click Save 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 the HTTPS settings interface.
   Configuration > Network > Advanced Settings > HTTPS
2. Create the self-signed certificate or authorized certificate.

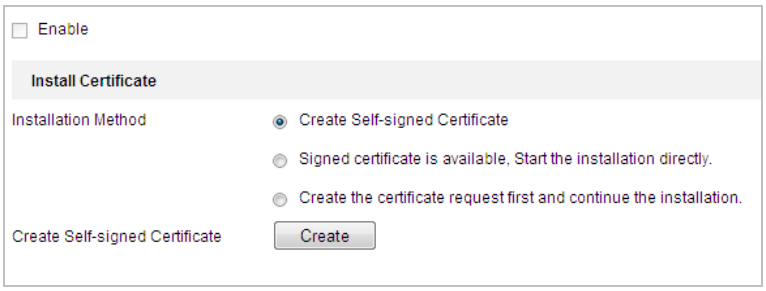


Figure 6-12 Create Certificate

OPTION 1: Create the self-signed certificate

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

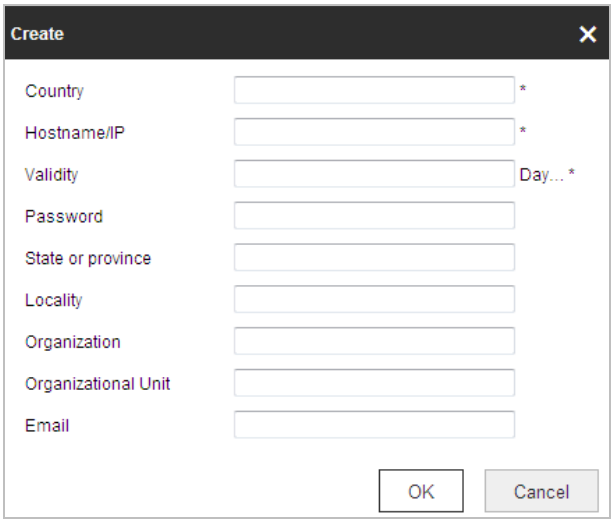


Figure 6-13 Create Self-signed Certificate

3) Enter 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.

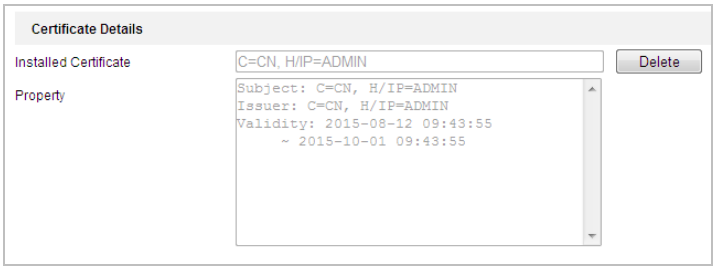


Figure 6-14 Installed Certificate Property

NOTE

- 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 the QoS settings interface:
   Configuration >Advanced Configuration > Network > QoS

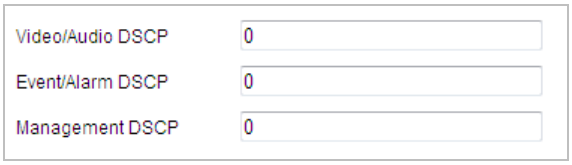


Figure 6-15 QoS Settings

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.
3. Click

to save the settings.

- 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 as follows:

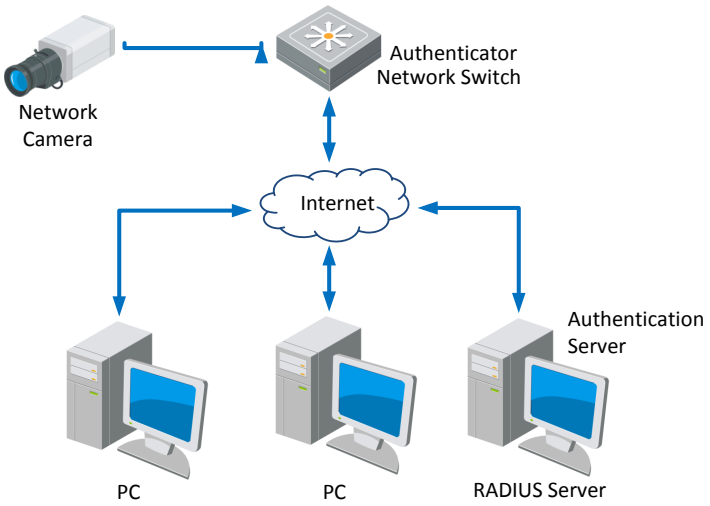


Figure 6-16 Protected LAN

- 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 the 802.1X settings interface:
   Configuration > Network > Advanced Settings > 802.1X

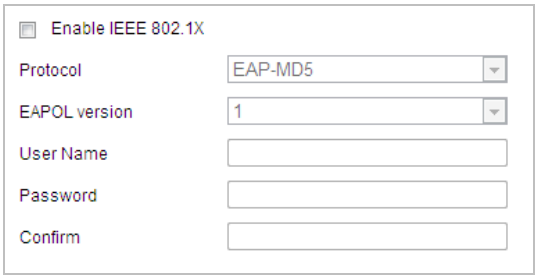


Figure 6-17 802.1X Settings

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

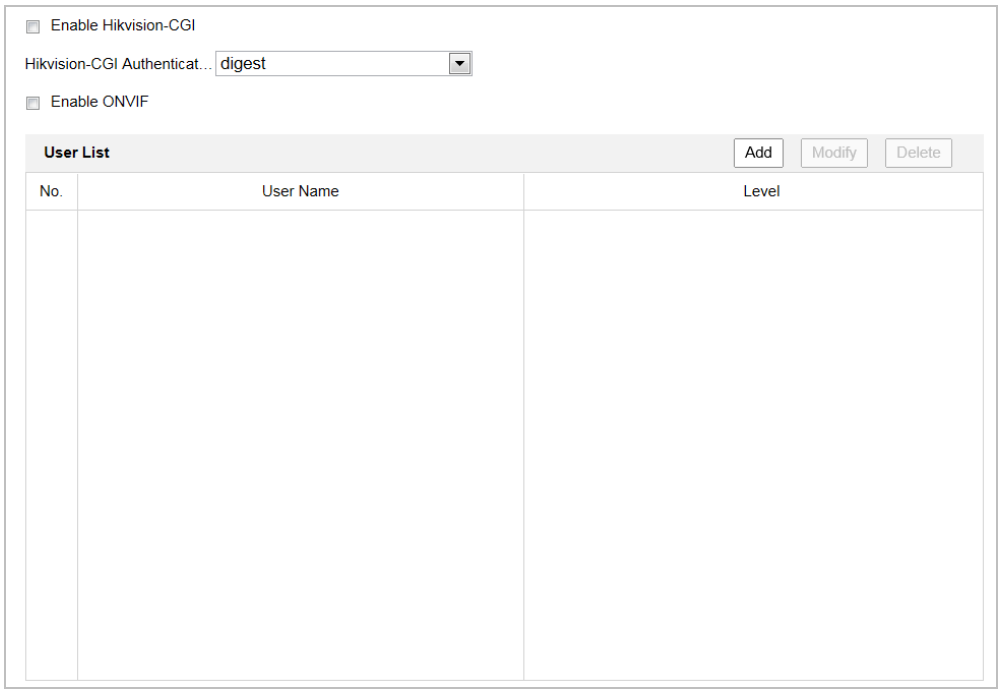


Figure 6-18 Integration Protocol Settings

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 Save to save the settings

6.2 Configuring Video and Audio Settings

6.2.1 Configuring Video Settings

Steps:

1. Enter the Video settings interface:
   Configuration > Video/Audio > Video

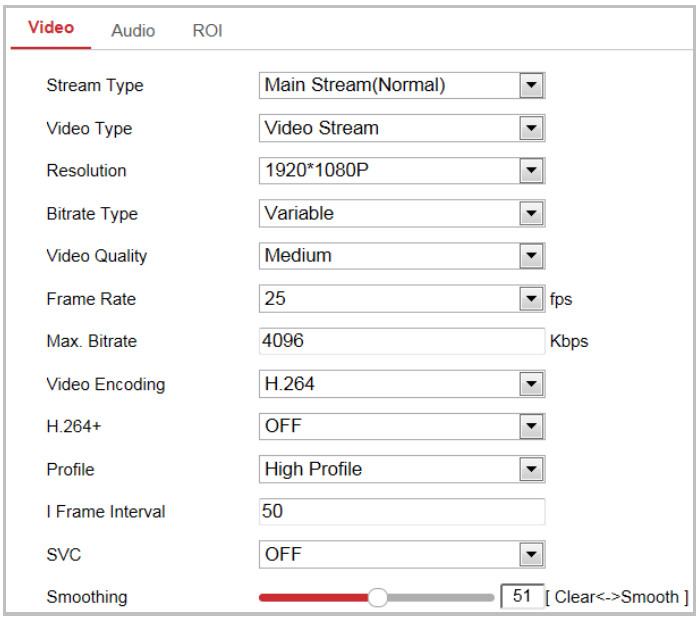


Figure 6-19 Configure Video Settings

2. 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 main stream and sub-stream for live viewing.
3. 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.

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.

4. Click

to save the settings.

6.2.2 Configuring Audio Settings

Steps:

1. Enter the Audio settings interface
   Configuration > Video/Audio > Audio

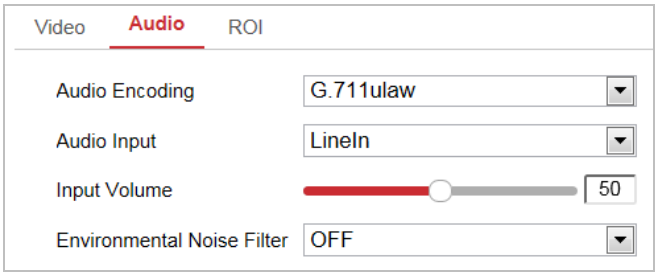


Figure 6-20 Audio Settings

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.

6.2.3 Configuring ROI Settings

Purpose:

ROI (Region of Interest) encoding is used to enhance the quality of images which are specified in advance. When **Fixed Region** is enabled, image quality of ROI area will be enhanced and image quality of other areas will be reduced.

ROI function varies depending on different camera models.

Steps:

1. Enter the ROI settings interface:
   Configuration >Video/Audio > ROI

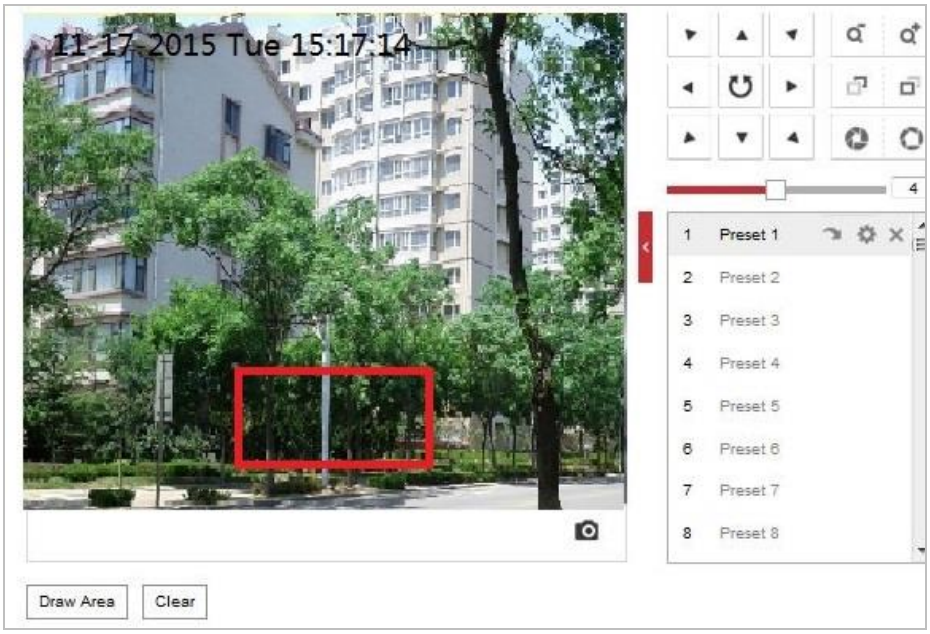


Figure 6-21 Region of Interest (1)

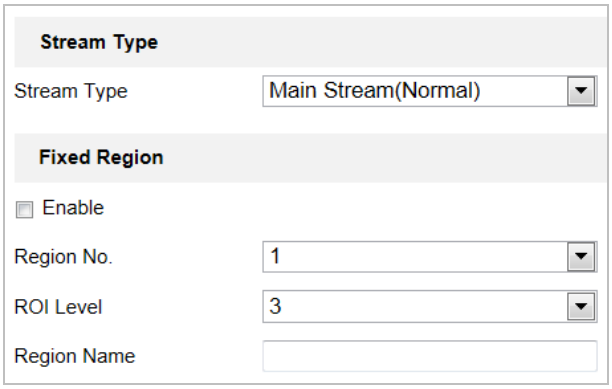


Figure 6-22 Region of Interest (2)

2. Select a stream type from the dropdown lsit. You can set the ROI function for main stream, sub-stream or third stream.
3. Click Draw Area and then drag the mouse to draw a red frame in the live view image. You can click Clear to clear it.

NOTE

The number of areas supported in ROI function varies depending on different camera models.

4. Select the **Region No.** from the dropdown list.
5. Adjust the **ROI level** from 1 to 6. The higher the value, the better image quality in the red frame.
6. Enter a **Region Name**.
7. Check the **Enable** box to enable the function and click Save to save the settings.

6.3 Configuring Image Settings

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.

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.

NOTE

- 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.

Day/Night Auto-Switch

Steps:

1. Enter the Display settings interface, and select Auto-Switch from the dropdown list.
   Configuration > Image> Display Settings

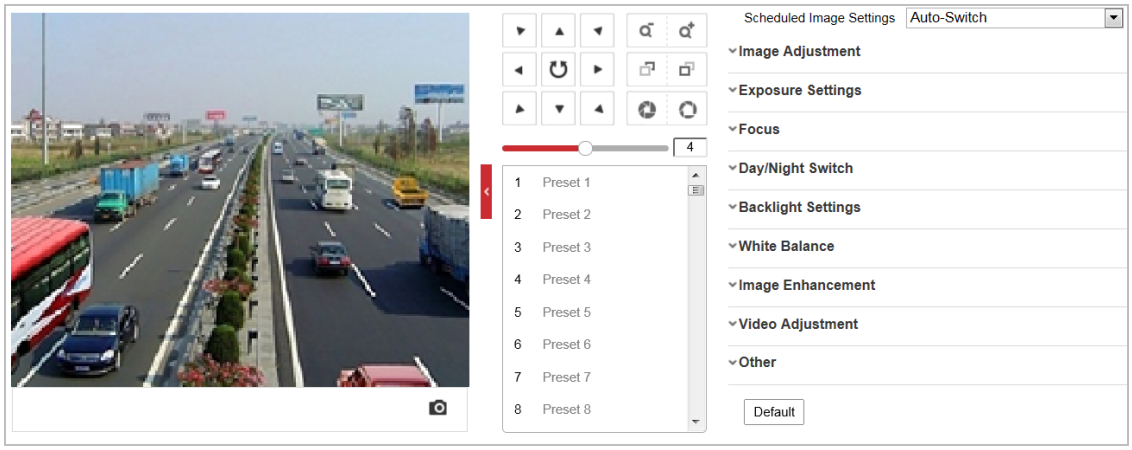


Figure 6-23 Display Settings - Auto-Switch

2. Set the image parameters of the camera.
   - **Image Adjustment**
     Brightness describes bright of the image, which ranges from 1 to 100.
     Contrast describes the contrast of the image, which ranges from 1 to 100.
     Saturation describes the colorfulness of the image color, which ranges from 1 to 100.

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

- **Exposure Settings**

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.

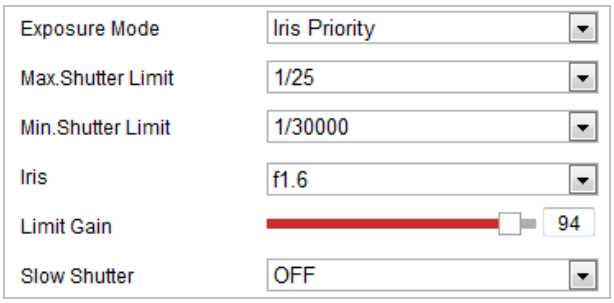


Figure 6-24 Manual Iris

◆ 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.

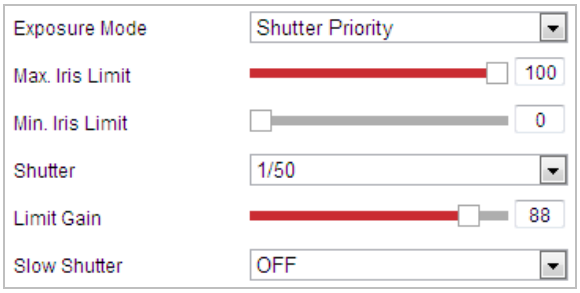


Figure 6-25 Manual Shutter

◆ Manual:

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

- **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**.

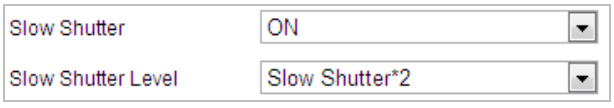


Figure 6-26 Slow Shutter

© Hikvision

- **Focus Settings**

  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.

- **Day/Night Switch**

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

  ◆ **Auto**:

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

Figure 6-27 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-Switch** mode, you can set the time schedule for day mode as shown in Figure 6-28. The rest time out of the schedule is for night mode.

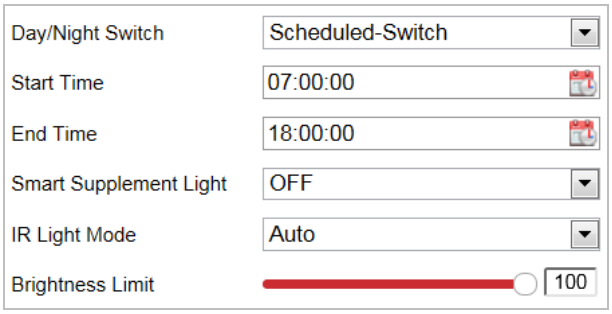


Figure 6-28 Day Night Schedule

◆ **Triggered by Alarm Input**

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

- **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 6-29. The wide dynamic level ranges from 0 to 100.

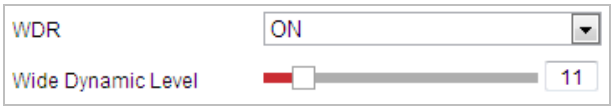


Figure 6-29 WDR

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**

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

◆ **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 6-30.

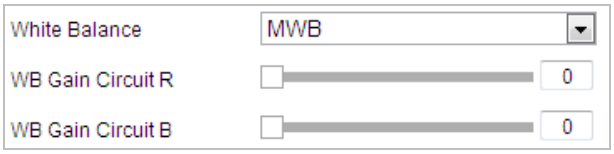


Figure 6-30 Manual White Balance

◆ **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.

NOTE

This function varies depending on different camera models.

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 6-31. The level ranges from 0 to 100.

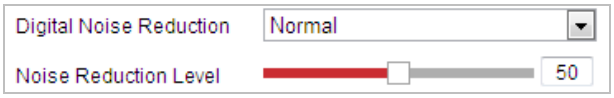


Figure 6-31 3D Digital Noise Reduction

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 6-32 Expert Mode

◆ Defog Mode

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

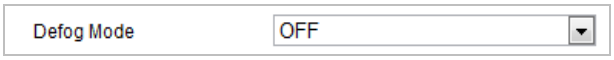


Figure 6-33 Defog Mode

◆ Optical Image Stabilization

You can set the **OIS** (Optical Image Stabilization) to OFF, Normal, or Expert. If you select Expert mode, you can select OIS level and OIS sensitivity from the drop-down list.

NOTE

This function varies depending on different camera models.

Video Adjustment

◆ Mirror

If you turn the **MIRROR** function on, the image will be flipped. It is like the image in the mirror.

◆ 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

It's the selectable video input mode to meet the different demands of field of view and resolution.

Other

◆ Lens Initialization

The lens operates the movements for initialization when you check the check box of **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.

◆ **Local Output**

Set the local output **ON** or **OFF** according to the actual device.

Day/Night Scheduled-Switch

Day/Night scheduled-switch configuration interface enables you to set the camera parameters for day and night separately, guaranteeing the image quality in different illumination.

Steps:

1. Enter the Display settings interface, and select Scheduled-Switch from the dropdown list.
   Configuration > Image> Display Settings

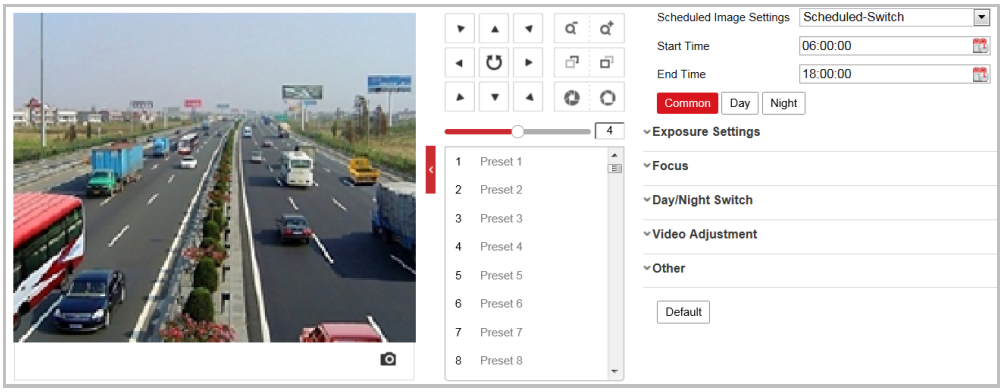


Figure 6-34 Display Settings - Scheduled-Switch

2. Click the calendar icon to select the start time and the end time of the switch.

   NOTE

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

3. Click **Common** to configure the common parameters applicable to the day mode and night mode. For the detailed information of each parameter, refer to section ***Day/Night Auto-Switch***.
4. Click **Day** tab to configure the parameters applicable for day mode.
5. Click **Night** tab to configure the parameters applicable for night mode.

   NOTE

   The settings saved automatically if any parameter is changed. You can click Default to restore the settings.

6.3.2 Configuring OSD Settings

Purpose:

The camera supports following on screen displays:

Time: Supports for time display.

Camera Name: Identifies the name of camera.

You can customize the on screen display of time.

Steps:

1. Enter the OSD settings interface:

   Configuration > Image > OSD Settings

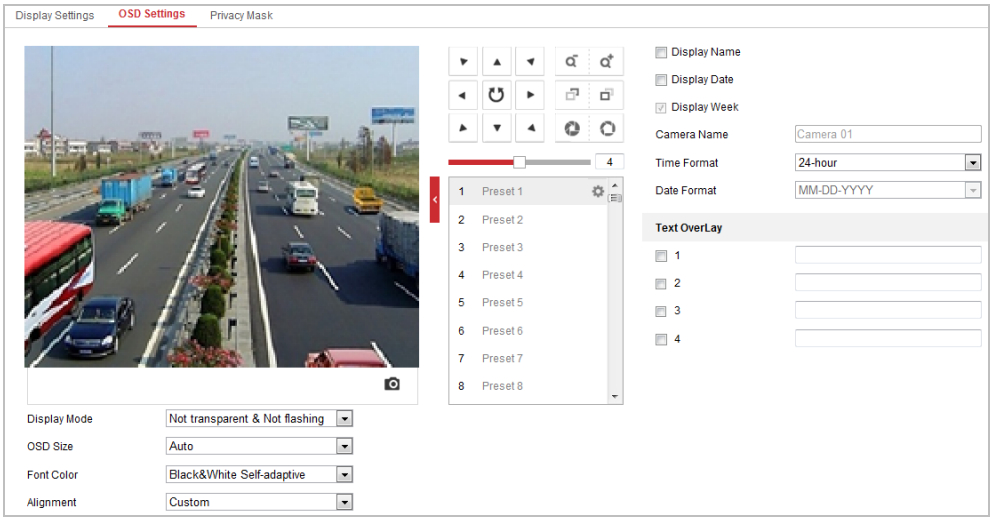


Figure 6-35 OSD Settings

2. Check the corresponding checkbox to select the display of camera name, date or week if required.
3. Edit the camera name in the text field of **Camera Name**.
4. Select from the dropdown list to set the time format, date format, display mode, OSD size and Font color.
5. You can use the mouse to drag the text frame IPdome in the live view window to adjust the OSD position.

Figure 6-36 Adjust OSD Location

© Hikvision

6. Click Save to activate above settings.

6.3.3 Configuring Text Overlay Settings

Purpose:

You can customize the text overlay.

Steps:

1. Enter the 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 Text in the live view window to adjust the text overlay position.
5. Click Save to save the settings.

6.3.4 Configuring Privacy Mask

Purpose:

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

Steps:

1. Enter the Privacy Mask settings interface:
   Configuration > Image > Privacy Mask

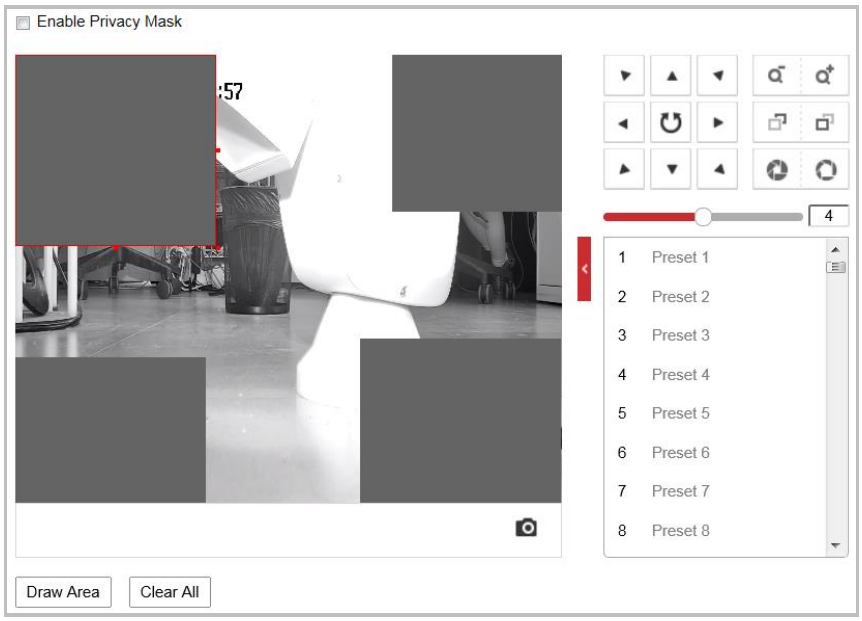


Figure 6-37 Privacy Mask

2. Check the **Enable Privacy Mask** checkbox to enable this function.

3. Click **Draw Area** and drag the mouse in the live video window to draw the mask area.
4. Click **Stop Drawing** to finish drawing or click **Clear All** to clear all of the areas you set without saving them.
5. Click

to save the settings

6.4 Configuring System Settings

6.4.1 System Settings

Viewing Basic Information

Enter the Device Information interface:

Configuration > System > System Settings > Basic Information

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

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

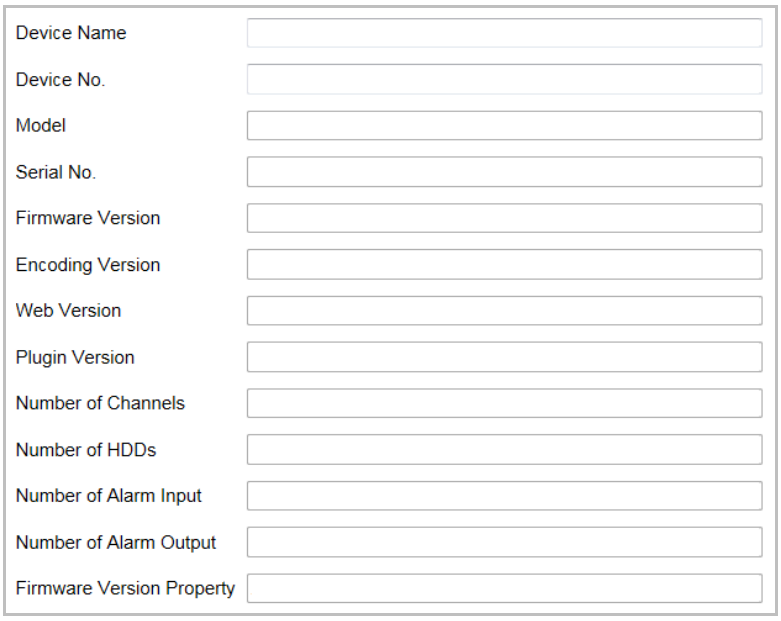


Figure 6-38 Device Information

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 the Time Settings interface:

Configuration > System > System Settings > Time Settings

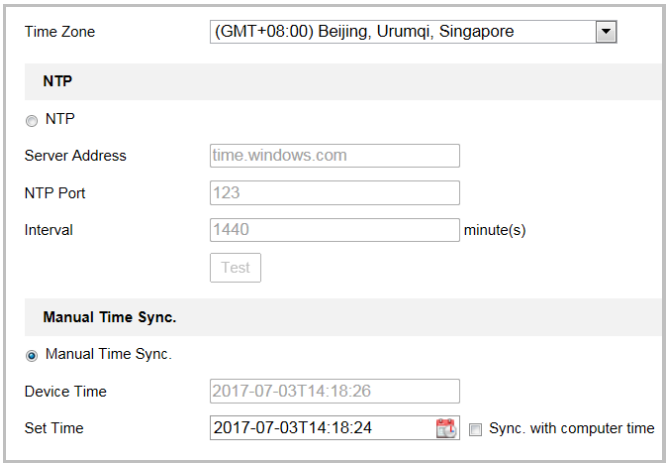


Figure 6-39 Time Settings

- **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.

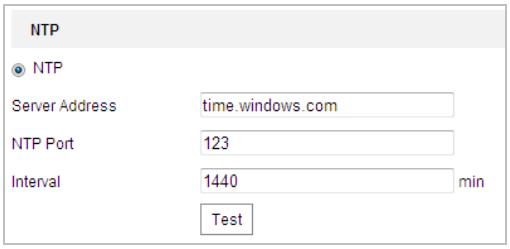


Figure 6-40 Time Sync by NTP Server

You can click Test 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 Save 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.

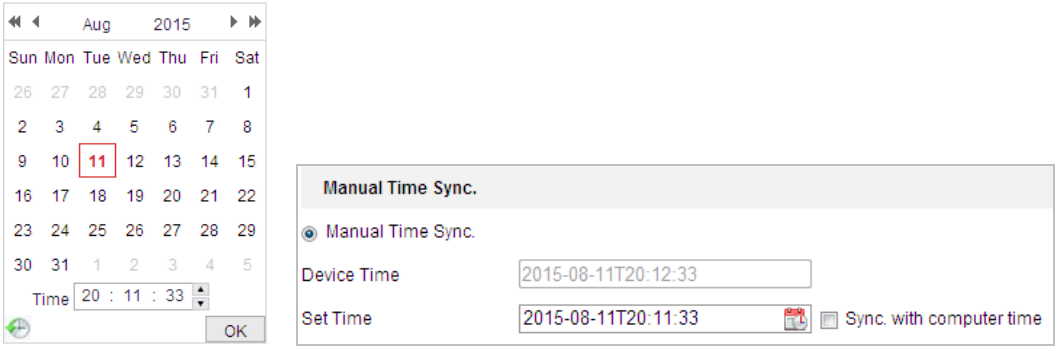


Figure 6-41 Time Sync Manually

- **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 6-42, select the Time Zone in which the camera locates.

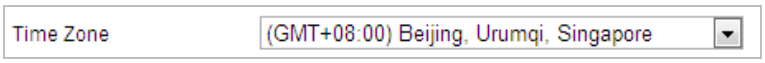


Figure 6-42 Time Zone Settings

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 the **DST** interface by **Configuration > Advanced Configuration > System > DST**

Figure 6-43 DST Settings

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

Configuring RS-232

The RS-232 port can be used in two ways:

- Parameters Configuration: Connect a computer to the camera through the serial port. Device parameters can be configured by using software such as HyperTerminal. The serial port parameters must be the same as the serial port parameters of the camera.
- Transparent channel: Connect a serial device directly to the camera. The serial device will be controlled remotely by the computer through the network.

Steps:

1. Enter RS-232 Port setting interface:
   Configuration> Advanced Configuration> System > RS-232

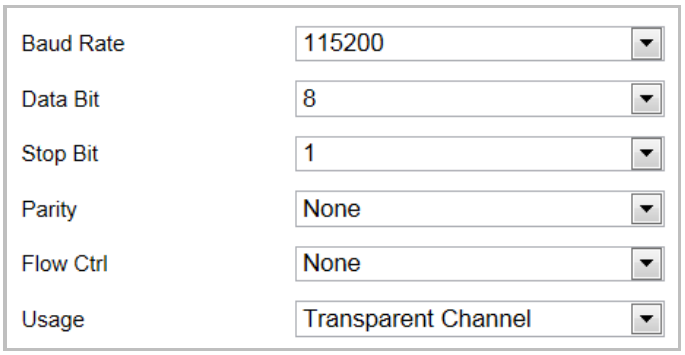


Figure 6-44 RS-232 Settings

2. Configure the Baud Rate, Data Bit, Stop Bit, Parity, Flow Control, and Usage.

   NOTE

   If you want to connect the camera through RS-232 port, the parameters of the RS-232 should be exactly the same with the parameters you configured here.

3. Click Save 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.

Steps:

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

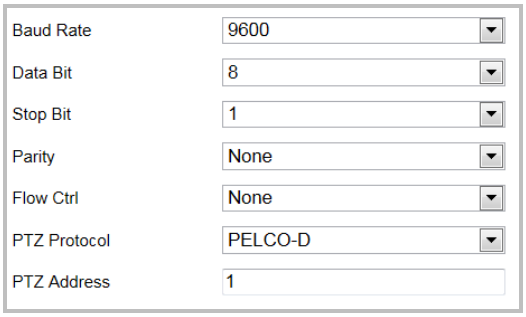


Figure 6-45 RS-485 Settings

2. Set the RS-485 parameters and click Save 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.

About

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

6.4.2 Maintenance

Upgrade & Maintenance

- **Rebooting the Camera**

Steps:

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

- **Restoring Default Settings**

Steps:

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

NOTE

© Hikvision

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

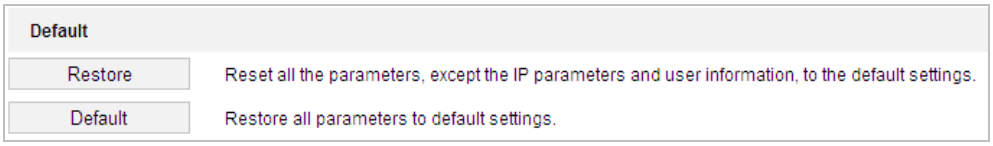


Figure 6-46 Restore Default Settings

- **Exporting Configuration File**

Steps:

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

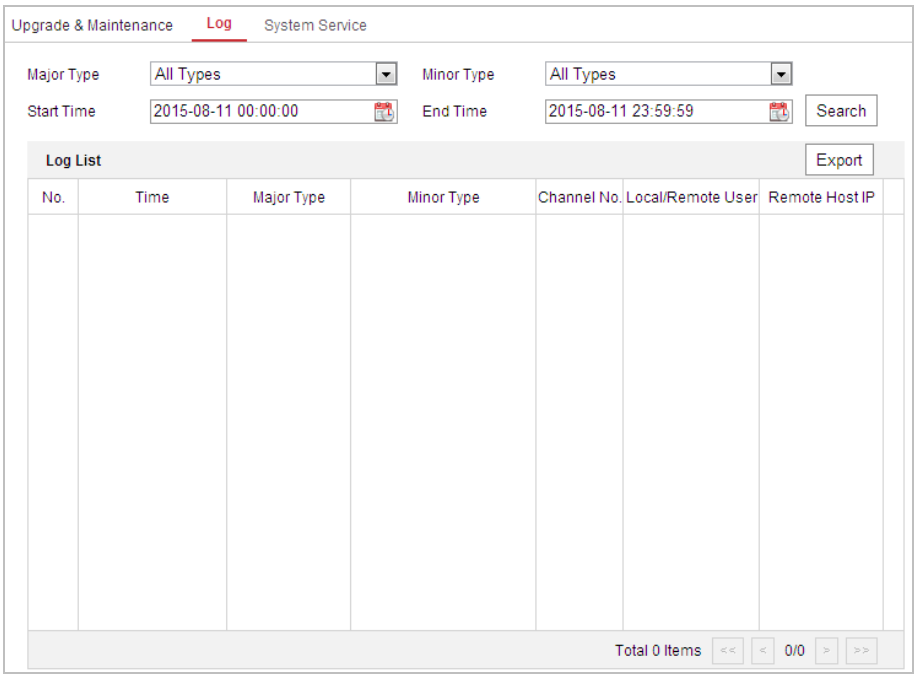


Figure 6-47 Log Searching Interface

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 6-47.
3. Click Search 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 the 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.

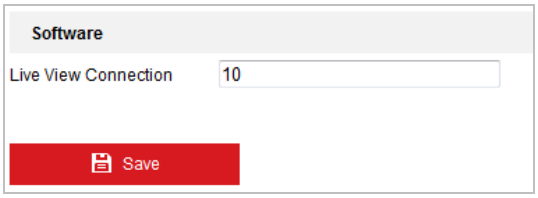


Figure 6-48 Live View Connection Settings

4. Click Save button to activate the settings.

6.4.3 Security

Configuring Authentication Security

Purpose:

You can specifically secure the stream data of live view.

Steps:

1. Enter the Authentication interface:
   Configuration> **System**> **Security** > **Authentication**
2. Set the **RTSP Authentication/WEB Authentication** type from the dropdown list. Digest and digest/basic are selectable.
3. Click Save 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:

1. Enter IP Address Filter interface:
   Configuration > **System** > **Security** > **IP Address Filter**

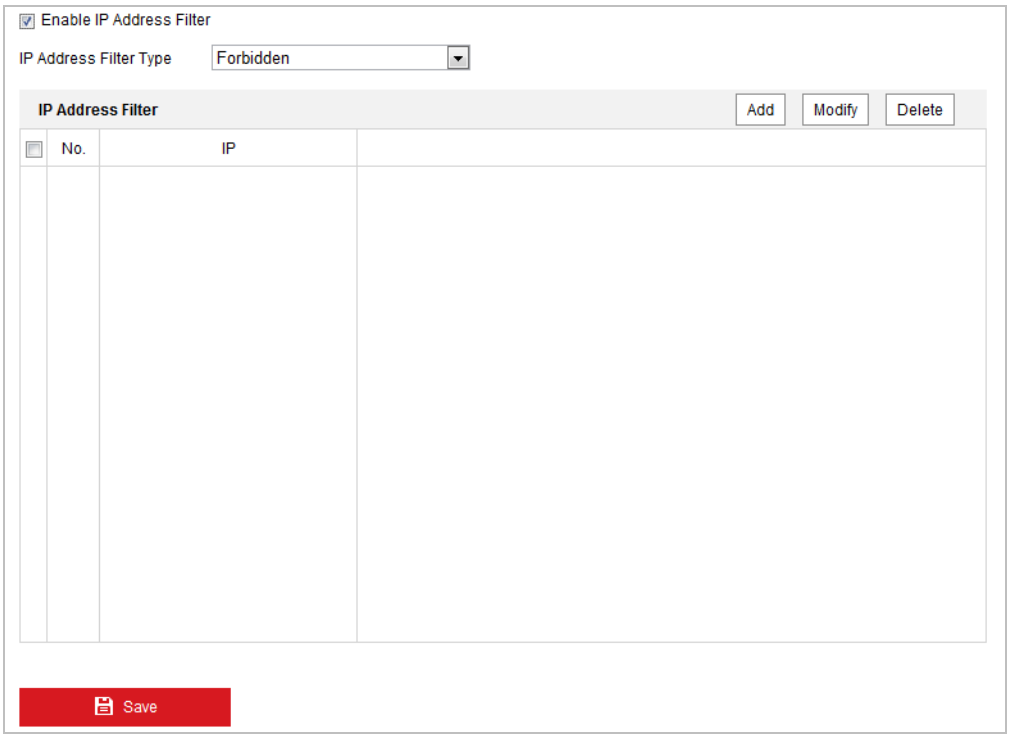


Figure 6-49 IP Address Filter

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

- **Add an IP Address**

Steps:

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

(2) Input the IP Adreess.

Figure 6-50 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 6-51 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 Save to save the settings.

Configure Security Service Settings

Steps:

1. Enter the Security Service interface:
   Configuration> **System** > **Security** > **Security Service**
2. Check the checkbox to enable the 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 Save to save the settings.

6.4.4 User Management

Enter the User Management interface**:**
Configuration > **System** > **User Management**

User Management

The **admin** user has access to create, modify or delete other accounts. Up to 32 user accounts can be created.

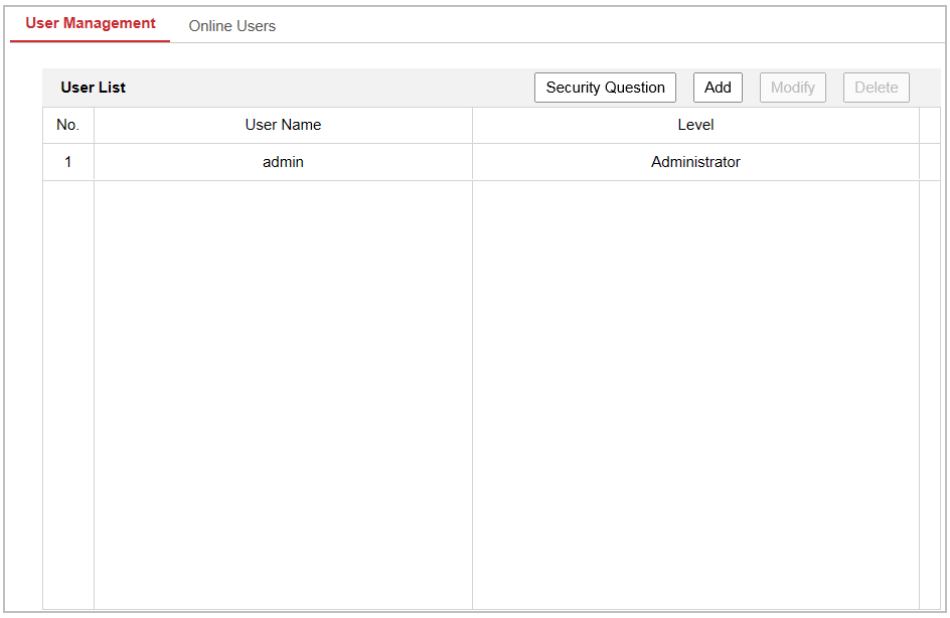


Figure 6-52 User Information

- **Add a User**

Steps:

1. Click Add 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 OK to finish the user addition.

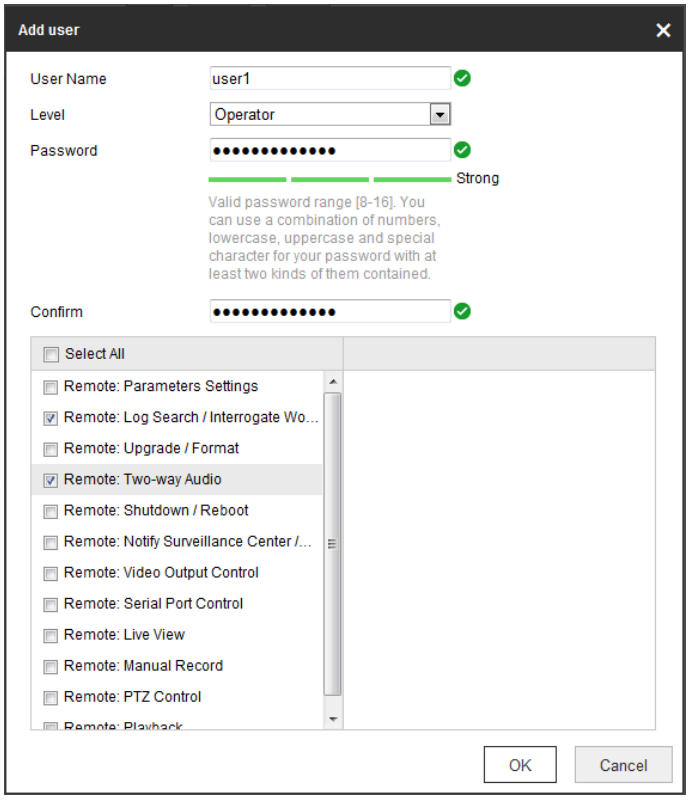


Figure 6-53 Add a User

- **Modify a User**

Steps:

1. Left-click to select the user from the list and click Modify.
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 OK to finish the user modification.

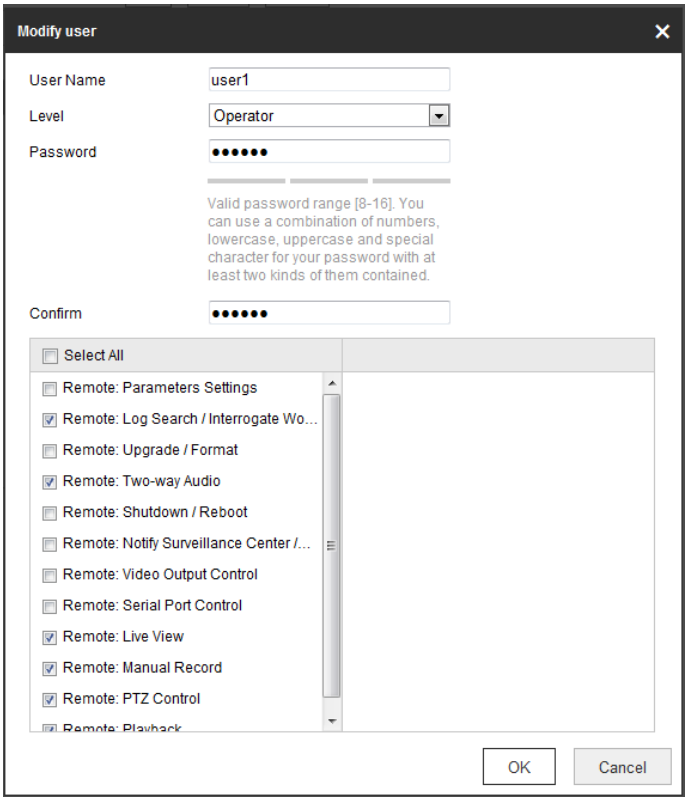


Figure 6-54 Modify a User

- **Delete a User**

Steps:

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

Setting Security Question

Purpose:

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

Set Security Question:

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

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

Steps:

1. Enter setting interface:
   Configuration > System > User Management > User Management
2. Click **Security Question.**
3. Input correct admin password.
4. Select questions and input answers.
5. Click **OK** to save the settings.

Reset Admin Password:

Before you start:

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

Steps:

1. Enter login interface via web browser.
2. Click **Forget Password**.
3. Answer security question.
4. Create new password.

Note:

User IP address is locked for 30 minutes after 7 failed attempts of answering security questions.

Online Users

Enter the Online Users configuration interface**:**

Configuration > **System** > **User Management** > **Online Users**

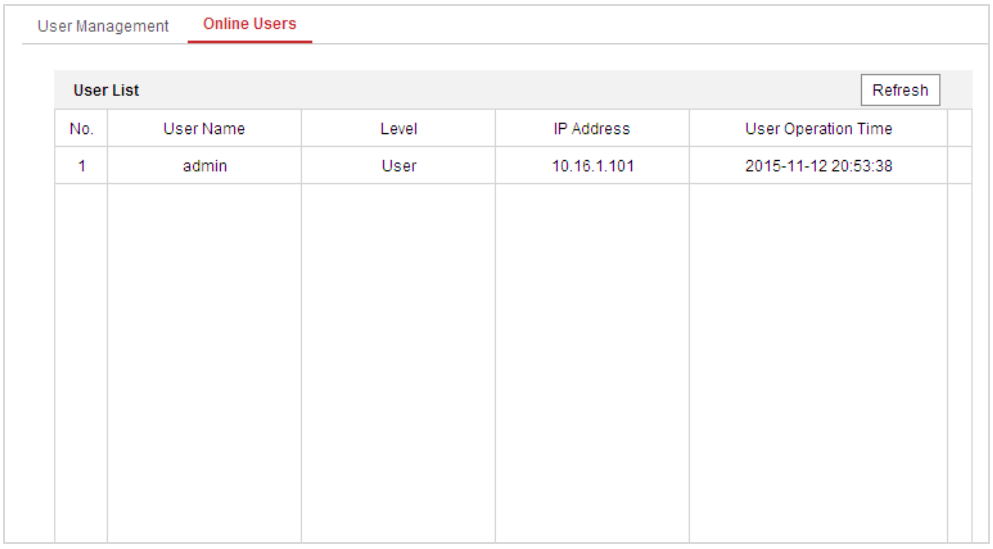


Figure 6-55 Online Users

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.

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.

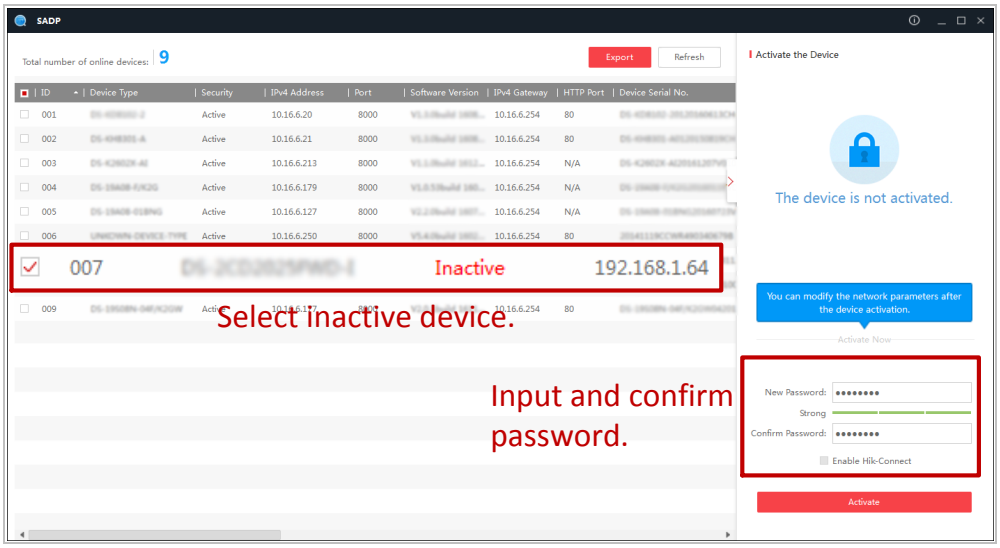


Figure A.1.1 Searching Online Devices

NOTE

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

♦ **Search online devices manually**

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

NOTE

You can click ▲ or ▼ on each column heading to order the information; you can

click to expand the device table and hide the network parameter panel on the right side, or click to show the network parameter panel.

Modify network parameters

Steps:

1. Select the device to be modified in the device list and the network parameters of the device will be displayed in the **Modify Network Parameters** panel on the right side.
2. Edit the modifiable network parameters, e.g. IP address and port number.
3. Enter the password of the admin account of the device in the **Password** field and click Save 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 Parameters

See Far, Go Further