



VISIX S-Series Network Camera

User Manual V7

This manual applies to the following camera models:

Camera Type	Model	
Box camera	<ul style="list-style-type: none"> ■ VX-4M-F-AWD *New* ■ VX-3M-F-AWD (DC) ■ VX-3S-FE-POE 	
Dome camera	<ul style="list-style-type: none"> ■ VX-4S28-MD-I ■ VX-3S-OD3-RIAH ■ VX-2M-OD3-RIAH *New* ■ VX-2M-OD2-RIAH (DC) ■ VX-4M-OD3-RIAWD *New* ■ VX-3M-OD2-RIAWD (DC) ■ VX-6S-OD3-RIAWD ■ VX-8S-180-AWD ■ VX-2M-D2-RIA ■ VX-3M-D2-RIAWD ■ VX-SMBK-D ■ VX-2S-D4-RIA *New* ■ VX-2V-MD-RIWH ■ VX-4V-ID-RIAWD *New* ■ VX-3P4-MD-I (DC) ■ VX-3P28-MD-I (DC) ■ VX-3P28-MD-IA (DC) ■ VX-3S28-OD-I-3 (DC) ■ VX-2S-D3-RIA (DC) 	
Bullet Camera	<ul style="list-style-type: none"> ■ VX-3PV-B-I (DC) ■ VX-3M-B-RIAWD ■ VX-3M20-B-RIAWD ■ VX-3P28-MB-I ■ VX-3P4-MB-I (DC) ■ VX-4S4-MB-I ■ VX-SMBK-B 	

(DC) – Discontinued Model

NOTE: The VISIX (VSX) line of cameras has been discontinued and has been replaced with the VISIX S-Series line. Although the majority of this manual will be accurate in regards to older VISIX-line cameras, some inaccuracies may exist due to features being added in firmware versions released after the discontinuation of the VISIX line. Please contact your 3xLOGIC support representative for more info.

Thank you for purchasing our product. If there are any questions, or requests, please do not hesitate to contact the dealer.

NOTE: This manual may contain technical inaccuracies or printing errors. The content is subject to change without notice. The manual will be amended if there are any hardware updates or changes.

DISCLAIMER STATEMENT

“Underwriters Laboratories Inc. (“UL”) has not tested the performance or reliability of the security or signaling aspects of this product. UL has only tested for fire, shock or casualty hazards as outlined in UL’s Standard(s) for Safety, UL60950-1. UL Certification does not cover the performance or reliability of the security or signaling aspects of this product. UL MAKES NO REPRESENTATIONS, WARRANTIES OR CERTIFICATIONS WHATSOEVER REGARDING THE PERFORMANCE OR RELIABILITY OF ANY SECURITY OR SIGNALING RELATED FUNCTIONS OF THIS PRODUCT.”

Regulatory Information

FCC Information

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

FCC Conditions

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

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

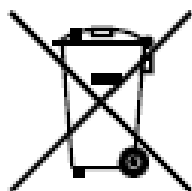
EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the Low Voltage Directive 2006/95/EC, the EMC Directive 2004/108/EC, the RoHS Directive 2011/65/EU.



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



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



Safety Instruction

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

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

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

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

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



Warnings:

- Please adopt the power adapter which can meet the safety extra low voltage (SELV) standard. And source with 12 VDC or 24 VAC (depending on models) according to the IEC60950-1 and Limited Power Source standard.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the camera yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)
- To reduce the risk of fire or electrical shock, do not expose this product to rain or moisture.
- This installation should be made by a qualified service person and should conform to all the local codes.
- Please install blackouts equipment into the power supply circuit for convenient supply interruption.
- Please make sure that the ceiling can support more than 50(N) Newton gravities if the camera is fixed to the ceiling.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the camera yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

**Cautions:**

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

NOTE: For cameras that support IR, you are required to pay attention to the following precautions to prevent IR reflection.

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

Table of Contents

1 SYSTEM REQUIREMENTS.....	9
2 NETWORK CONNECTION	10
2.1 SETTING THE NETWORK CAMERA OVER THE LAN	10
2.1.1 <i>Wiring over the LAN.....</i>	<i>10</i>
2.1.2 <i>Detecting, Activating Changing the Camera IP Address</i>	<i>11</i>
2.2 SETTING THE NETWORK CAMERA OVER THE WAN	12
2.2.1 <i>Static IP Connection</i>	<i>12</i>
2.2.2 <i>Dynamic IP Connection</i>	<i>13</i>
2.2.3 <i>Normal Domain Name Resolution</i>	<i>14</i>
2.2.4 <i>Private Domain Name Resolution.....</i>	<i>15</i>
3 ACCESSING THE NETWORK CAMERA.....	16
3.1 ADDING A VISIX S-SERIES CAMERA TO VIGIL SERVER	16
3.2 ACCESS UI VIA WEB BROWSER.....	18
4 BASIC OPERATION.....	20
4.1 CONFIGURING LOCAL PARAMETERS	20
4.2 LIVE VIEW	21
4.2.1 <i>Live view page – COMPONENT DESCRIPTIONS.....</i>	<i>21</i>
4.3 RECORDING AND CAPTURING PICTURES MANUALLY	22
4.4 OPERATING PTZ CONTROL	22
4.4.1 <i>PTZ Control Panel.....</i>	<i>23</i>
4.4.2 <i>Setting a Preset.....</i>	<i>24</i>
4.4.3 <i>Calling a Preset</i>	<i>24</i>
4.4.4 <i>Setting/Calling a Patrol.....</i>	<i>25</i>
4.4.5 <i>Setting/Calling a Pattern</i>	<i>26</i>
4.5 PLAYBACK.....	28
4.6 PICTURE.....	30
5 SYSTEM CONFIGURATION	31
5.1 STORAGE SETTINGS	31
5.1.1 <i>Configuring Recording Schedule</i>	<i>31</i>
5.1.2 <i>Configuring Capture Schedule</i>	<i>32</i>
5.1.3 <i>Configuring Net HDD</i>	<i>34</i>
5.1.4 <i>Memory Card Detection.....</i>	<i>35</i>
5.1.5 <i>Configuring Lite Storage</i>	<i>37</i>
5.2 BASIC EVENT CONFIGURATION	38
5.2.1 <i>Configuring Motion Detection</i>	<i>38</i>
5.2.2 <i>Configuring Video Tampering Alarm</i>	<i>43</i>

5.2.3 Configuring Video Loss.....	43
5.2.4 Configuring Alarm Input	44
5.2.5 Configuring Alarm Output	45
5.2.6 Handling Exceptions.....	46
5.3 SMART EVENT CONFIGURATION.....	47
5.3.1 Detecting Audio Exceptions	47
1.1.1 Configuring Defocus Detection	48
1.1.2 Configuring Scene Change Detection.....	49
5.3.2 Configuring Face Detection.....	50
5.3.3 Configuring Intrusion Detection.....	50
5.3.4 Configuring Line Crossing Detection	52
5.3.5 Configuring Region Entrance Detection.....	53
5.3.6 Configuring Region Exiting Detection	54
5.4 PTZ CONFIGURATION	56
5.4.1 Configuring Basic PTZ Parameters.....	56
5.4.2 Configuring PTZ Limits	57
5.4.3 Configuring Initial Position	58
5.4.4 Configuring Park Actions	58
5.4.5 Configuring Privacy Mask	59
5.4.6 Configuring Scheduled Tasks	60
5.4.7 Clearing PTZ Configurations	61
5.4.8 Configuring Smart Tracking.....	61
5.4.9 Prioritize PTZ.....	62
5.4.10 Position Settings	62
6 CAMERA CONFIGURATION.....	64
6.1 CONFIGURING NETWORK SETTINGS	64
6.1.1 Basic Settings.....	64
6.1.2 Advanced Settings	68
6.2 CONFIGURING VIDEO AND AUDIO SETTINGS.....	75
6.2.1 Configuring Video Settings.....	75
6.2.2 Custom Video.....	77
6.2.3 Configuring Audio Settings	78
6.2.4 Configuring ROI Settings.....	78
6.2.5 Display Info. on Stream.....	80
6.2.6 Configuring Target Cropping	80
6.3 CONFIGURING IMAGE SETTINGS.....	81
6.3.1 Configuring Display Settings	81
6.3.2 Configuring OSD Settings.....	85
6.3.3 Configuring Text Overlay Settings.....	86
6.3.4 Configuring Image Parameters Switch	87

6.4 CONFIGURING SYSTEM SETTINGS88

6.4.1 System Settings.....88

6.4.2 Maintenance.....91

6.4.3 Security93

6.4.4 User Management.....95

1 System Requirements

- **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 6.0 and above version, Safari 5.02 and above version, Mozilla Firefox 3.5 and above version and Google Chrome8 and above versions.

2 Network Connection

Before you start:

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

2.1 Setting the Network Camera over the LAN

To view and configure the camera via a LAN, you need to connect the network camera in the same subnet with your computer, and install the 3xLOGIC VISIX detection software. This will allow you to search and change the IP address of the detected network cameras.

2.1.1 WIRING OVER THE LAN

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

- To test the network camera, you can directly connect the network camera to the computer with a network cable as shown in Figure 2-1.
- Refer to the Figure 2-2 to set network camera over the LAN via a switch or a router.

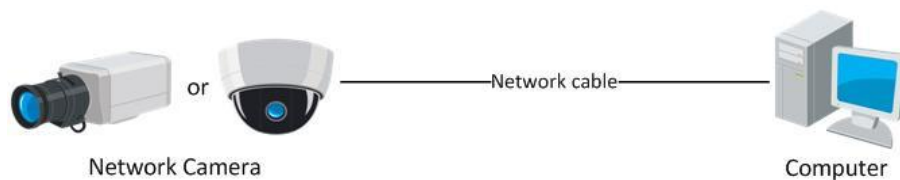


Figure 2-1 Connecting Directly

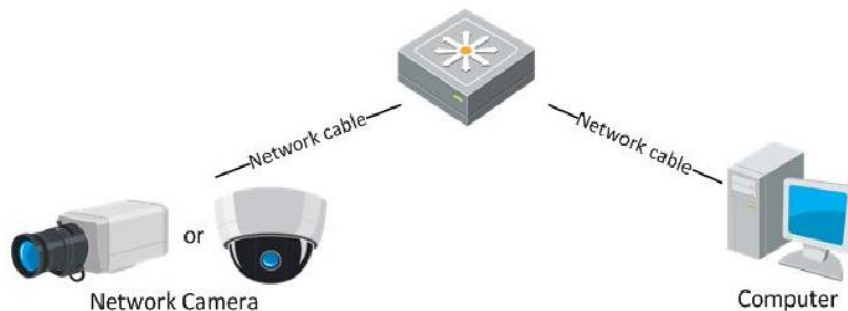


Figure 2-2 Connecting via a Switch or a Router

2.1.2 DETECTING, ACTIVATING CHANGING THE CAMERA IP ADDRESS

After networking the camera with the LAN, the user must obtain the camera's IP address to connect to the device. To obtain the IP address, the 3xLOGIC Camera (VISIX IP) Setup Utility, a software tool which can automatically detect online network cameras on the LAN, add these devices to VIGIL Server and list the device information including IP address, subnet mask, port number, device serial number, device version, etc... is recommended. An example is shown in Figure 2-3.

This utility is installed alongside VIGIL Server or can be downloaded separately. If on a VIGIL Server system, launch utility from *Start>Programs>VIGIL>Utility* or download the utility from the 3xLOGIC website's *Software Support Center > VIGIL Utilities* (<http://www.3xlogic.com/software-center>) to a Windows PC.

Steps:

1. Launch the utility.
2. Click **Detect Online Devices / Change IP Address**.

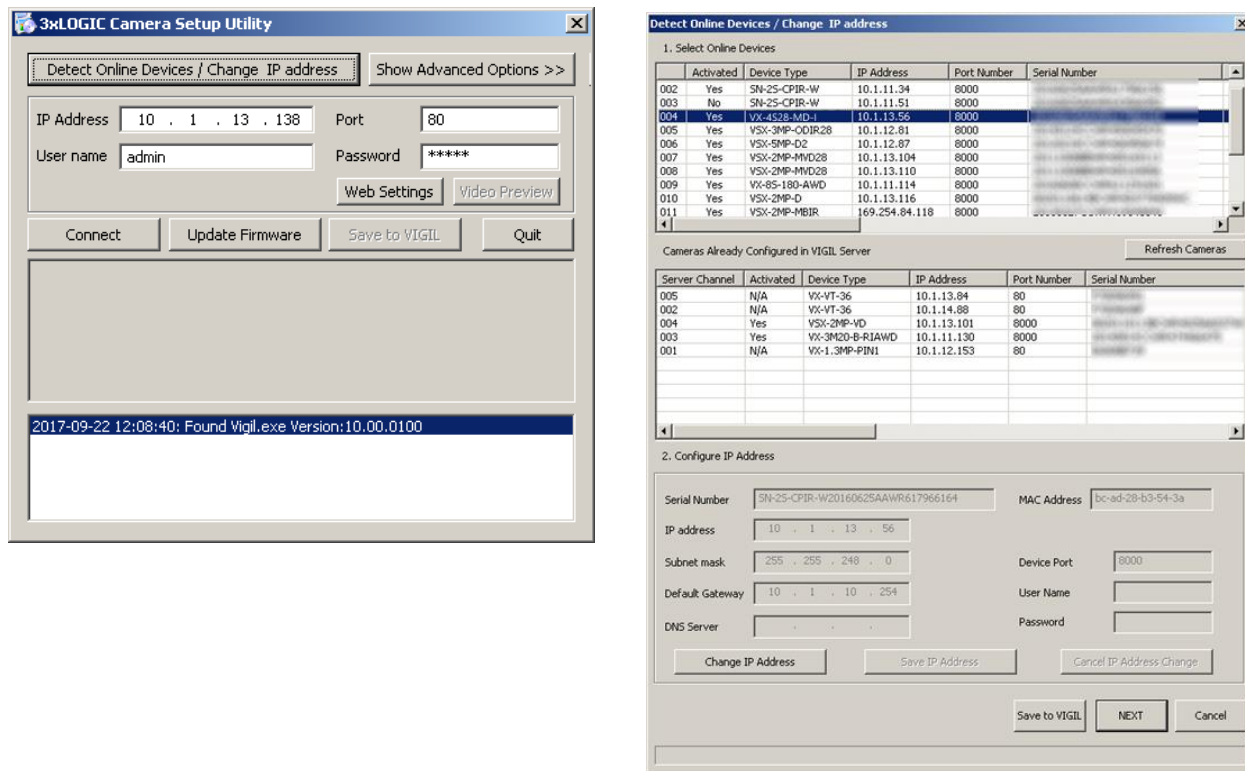


Figure 2-3 : 3xLOGIC Camera (VISIX IP) Setup Utility

3. Select the camera from the list of online devices.
4. If you are configuring the camera for initial setup, click **Activate** to assign a new password. This step is required for security purposes and must be completed before continuing. If the camera has previously been configured, skip to Step 5.

- Once you have assigned a new password to the camera, click **Change IP Address** and change the IP address and subnet mask to the same subnet as that of your computer. Save the settings.

Figure 2-4 : 3xLOGIC Camera (VISIX IP) Setup Utility – Changing Device IP Address

- Enter the IP address of network camera in the address field of the web browser to access the camera's web UI.

- The default IP address is 192.0.0.64 and the port number is 8000.
- NOTE:**
- For accessing the network camera from different subnets, please set the gateway for the network camera after you logged in. For detailed information, please refer to **Section 6.1.1 – Basic Settings – Configuring TCP/IP Settings**

2.2 Setting the Network Camera over the WAN

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

2.2.1 STATIC IP CONNECTION

Before you start:

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

Connecting the network camera via a router:

Steps:

- Connect the network camera to the router.

Assign a LAN IP address, the subnet mask and the gateway. Refer to [Detecting and Changing the IP Address](#) for detailed IP address configuration of the camera.

Save the static IP in the router.

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

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

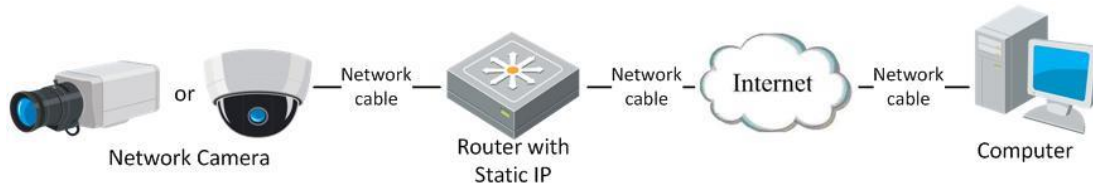


Figure 2-5 Accessing the Camera through Router with Static IP

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 [Detecting and Changing the IP Address](#) for detailed IP address configuration of the camera.

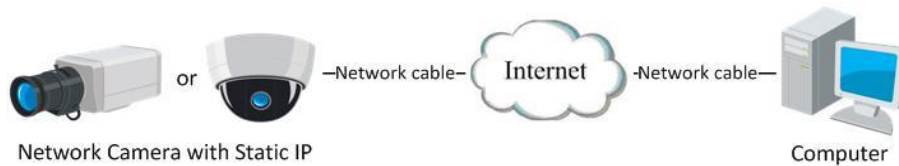


Figure 2-6 Accessing the Camera with Static IP Directly

2.2.2 DYNAMIC IP CONNECTION**Before you start:**

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

Connecting the network camera via a router:**Steps:**

1. Connect the network camera to the router.

In the camera, assign a LAN IP address, the subnet mask and the gateway. Refer to [Detecting and Changing the IP Address](#) for detailed LAN configuration.

In the router, set the PPPoE user name, password and confirm the password.

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

Apply a domain name from a domain name provider.

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

Visit the camera via the applied domain name.

Connecting the network camera via a modem:

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 [Configuring PPPoE Settings](#) for detailed configuration.

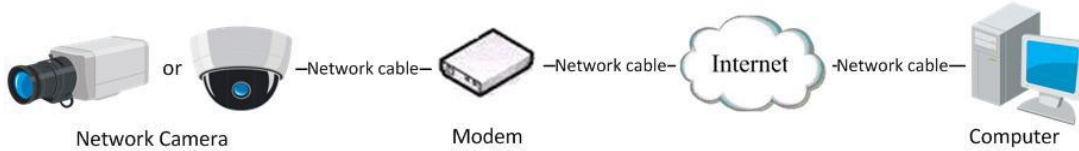


Figure 2-7 Accessing the Camera with Dynamic IP

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

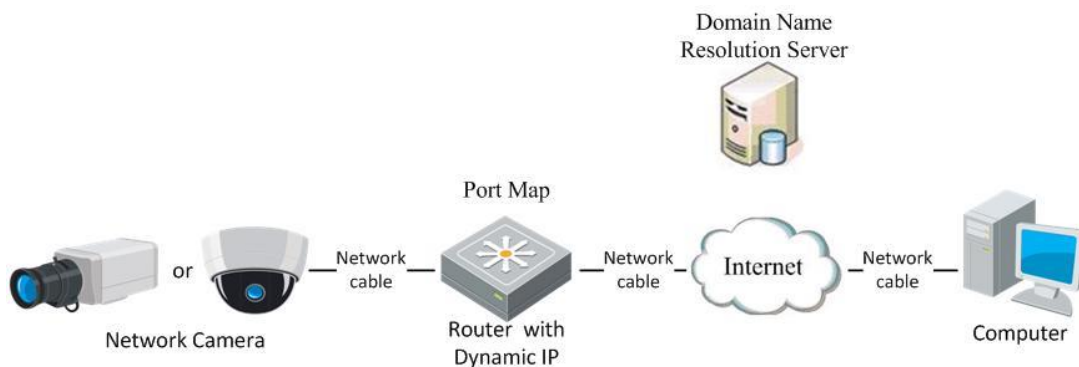
2.2.3 NORMAL DOMAIN NAME RESOLUTION

Figure 2-8 Normal Domain Name Resolution

Steps:

1. Apply a domain name from a domain name provider.

Configure the DDNS settings in the **DDNS Settings** interface of the network camera. Refer to [Configuring DDNS Settings](#) for detailed configuration.

Visit the camera via the applied domain name.

2.2.4 PRIVATE DOMAIN NAME RESOLUTION

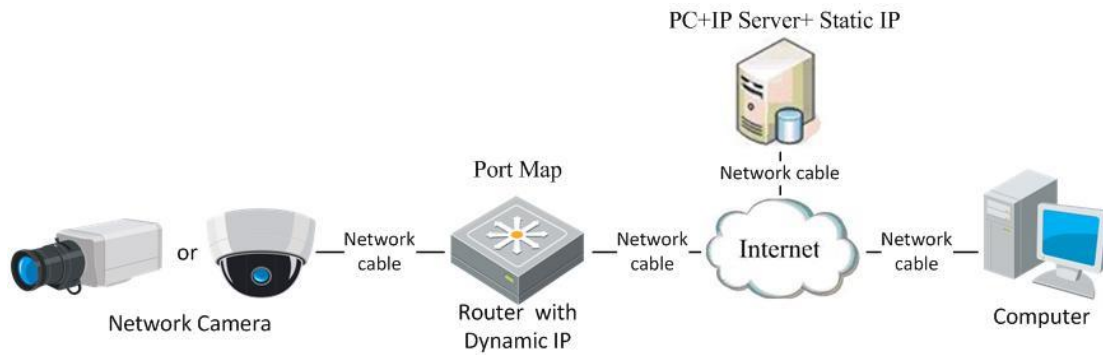


Figure 2-9 Private Domain Name Resolution

Steps:

1. Install and run the IP Server software in a computer with a static IP.

Access the network camera through the LAN with a web browser or the client software.

Enable DDNS and select IP Server as the protocol type. Refer to [Configuring DDNS Settings](#) for detailed configuration.

3 Accessing the Network Camera

3.1 Adding a VISIX S-Series Camera to VIGIL Server

Purpose:

By following the steps outlined in this section, a user can add a camera to VIGIL Server using the 3xLOGIC Camera (VISIX IP) Setup Utility. The utility was previously utilized in Section 2.1.2 to detect and change the camera's IP address. This utility is installed alongside VIGIL Server and will launch automatically when following the below steps.

Steps:

1. Login to VIGIL Server.
2. Open the **Settings > Camera Setup** Tab.
3. Select an unused camera channel to associate with the camera.
4. Toggle the **Network Camera** checkbox. The *Network Camera Settings* form will deploy. If the form does not deploy automatically, click the **Network Camera - Settings** button.
5. Click the **Detect Cameras** button located next to the *Type* field. The 3xLOGIC Camera Setup Utility will deploy and will automatically begin detecting devices on the network.

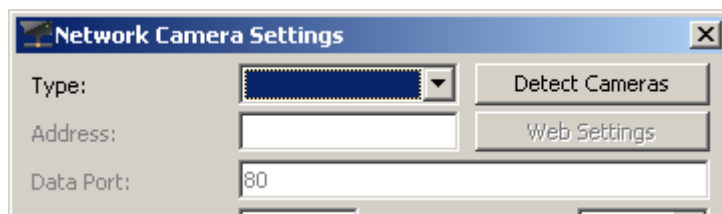


Figure 3-1 Launching the 3xLOGIC Camera Setup Utility

6. Select the desired camera from the list of online devices and click **Next**.

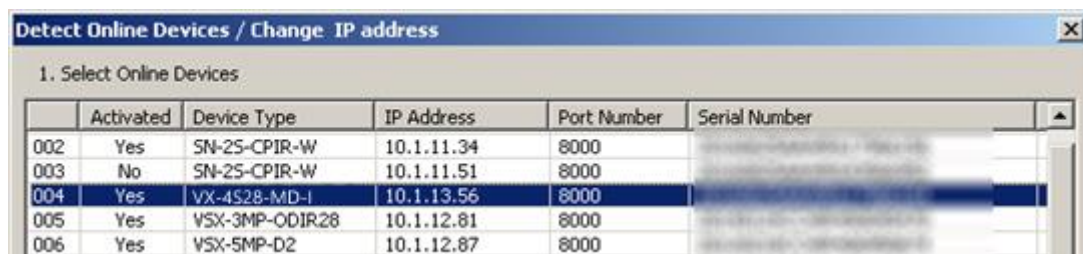


Figure 3-2 3xLOGIC Camera (VISIX IP) Setup Utility – Selecting Camera from Online Devices List

7. After the utility successfully accesses the camera, click **Save to VIGIL**. A window will deploy where the user can assign the camera's stream profiles.

NOTE: If the utility fails to access the camera, confirm the utility is using the correct log-in credentials for the camera (created during camera activation) and re-attempt saving to VIGIL. If issues persist, contact [3xLOGIC Support](#).

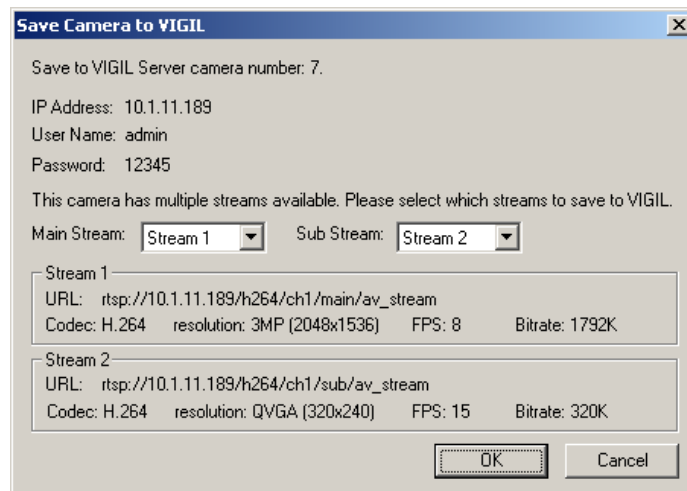
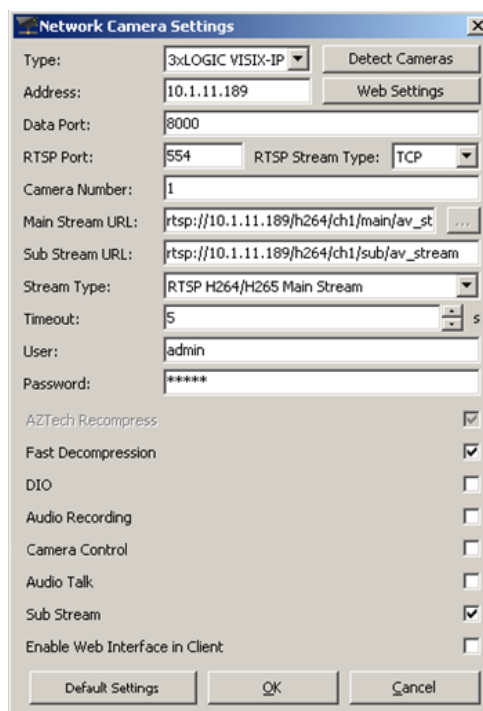


Figure 3-3 Assigning Stream Profiles

8. Assign the streams as desired and click **OK**.

The user will be returned to the Network Camera Settings form.

9. Configure additional settings as desired.



Click **OK** to on the Network Camera Settings form then click **Apply** on the VIGIL Server Settings window to save the new settings.

The camera will now be saved to VIGIL and can be accessed and controlled via the VIGIL Server UI. Any other applicable VIGIL utilities (VIGIL Client, View Lite II) that have been interfaced with the VIGIL Server will also be able to access and control the camera. See the VIGIL Server and VIGIL Client User Guides for more information on interacting with the camera and its footage. Visit the [3xLOGIC Document Library](#) for the latest available support documentation.

3.2 Access UI via Web Browser

Steps:

1. Open a web browser.
2. Input the IP address of the network camera in the URL address bar, e.g., 192.0.0.64 and press the **Enter** key to enter the login interface. Alternatively, if the camera is interfaced with VIGIL Server, the web UI can be instantly deployed by opening the camera's *Network Settings* form in VIGIL Server Settings > Cameras Tab and clicking the **Web Settings** button.
3. Input the user name and password and click **Login**.

NOTE: The username/password for the camera will have been configured during camera activation. If the camera has already been configured using one of 3xLOGIC's setup tools (VIGIL Easy Setup Wizard, 3xLOGIC Camera Setup Utility) then default credentials will have been changed by the installer (this is a standard security precaution enforced by the setup tools). Contact your security network administrator for credentials.

NOTE: English is the only supported language.



Figure 3-4 Login Interface

4. To view video and have full access to the camera's configuration settings, you will need to install the Web Components plug-in. Click "Activate Web Components" to start the plug-in installation.

NOTE: Depending on your web browser, you may be required to authorize the installer to run.

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.

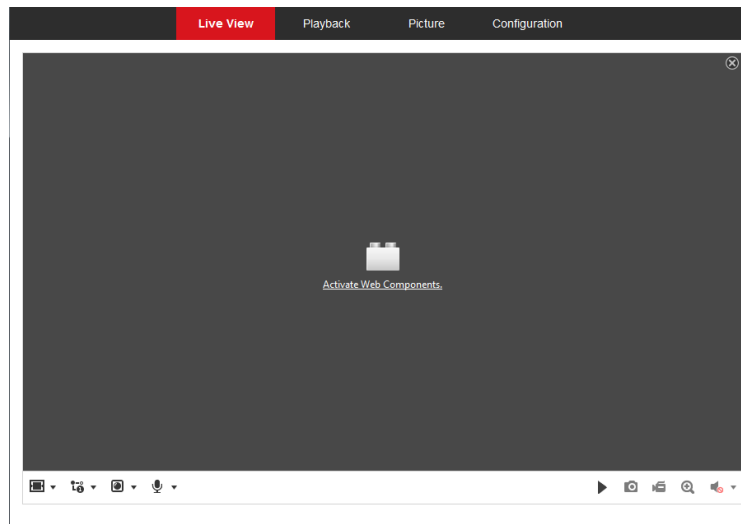


Figure 3-5 Download and Install Plug-in

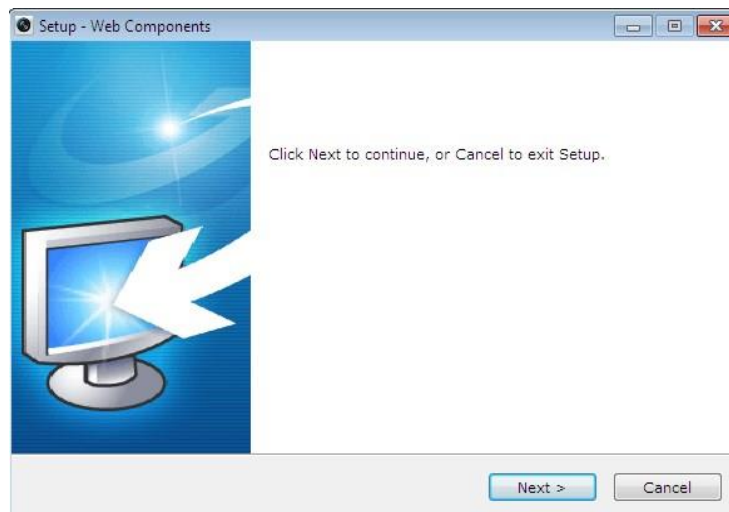


Figure 3-6 Install Plug-in (1)

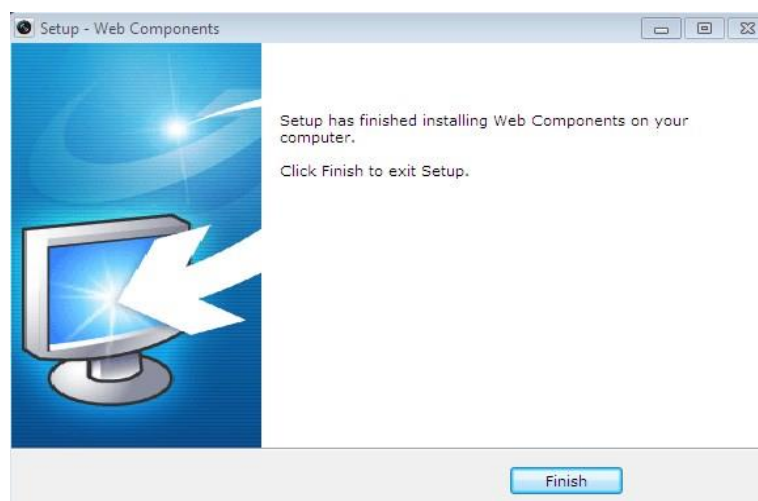


Figure 3-7 Install Plug-in (2)

4 Basic Operation

4.1 Configuring Local Parameters

The Local Configuration settings allow the user to set the parameters for live view, recorded files and captured pictures/stills. The recorded files and captured pictures/stillshots can be captured using the camera's browser UI and are saved to a destination path on your local system.

Steps:

1. Enter the Local Configuration interface: *Configuration > Local*.

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

- Live View Parameters:**
 - Protocol: ☒ TCP, ☐ UDP, ☐ MULTICAST, ☐ HTTP
 - Play Performance: ☐ Shortest Delay, ☒ Auto
 - Rules: ☐ Enable, ☒ Disable
 - Image Format: ☒ JPEG, ☐ BMP
- Record File Settings:**
 - Record File Size: ☐ 256M, ☒ 512M, ☐ 1G
 - Save record files to: C:\Users\test\RecordFiles [Browse] [Open]
 - Save downloaded files to: C:\Users\test\DownloadFiles [Browse] [Open]
- Picture and Clip Settings:**
 - Save snapshots in live view to: C:\Users\test\CaptureFiles [Browse] [Open]
 - Save snapshots when playback to: C:\Users\test\PlaybackPics [Browse] [Open]
 - Save clips to: C:\Users\test\PlaybackFiles [Browse] [Open]

A red 'Save' button is located at the bottom left of the configuration area.

Figure 4-1 Local Configuration Interface

2. Configure the following settings:

Live View Parameters:

Set the Protocol Type and Live View Performance settings.

- **Protocol Type:** TCP, UDP, MULTICAST and HTTP are selectable.
 - ▶ **TCP:** Ensures complete delivery of streaming data and better video quality, however, real-time transmission will be affected (skipped frames, etc...)
 - ▶ **UDP:** Provides real-time audio and video streams though video quality may be lowered due to bandwidth limitations.
 - ▶ **HTTP:** Allows the same quality as TCP without setting specific ports for streaming under some network environments.
 - ▶ **MULTICAST:** It's recommended to select MCAST type when using the Multicast function. For detailed information about Multicast, refer to [Section 9.1 Configuring Basic Settings – Configuring TCP/IP Settings](#).
- **Play Performance:** Set the play performance to Shortest Delay or Auto.
- **Rules:** Refers to on-screen tracking for rules configured on the camera. Select enable or disable to display or not display colored trackers when motion detection, face detection, or intrusion detection is triggered. E.g., If face detection is enabled and this option is active, when a face is detected it will be marked with a green rectangle on the live view.
- **Image Format:** Choose the image format for picture/stillshot capture.

Record File Settings

Set the destination of recorded video files. Applies only for video recorded manually via the browser UI.

- **Record File Size:** Select the packed size of the manually recorded and downloaded video files to

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

- **Save record files to:** Set the destination for manually recorded video files.
- **Save downloaded files to:** Set the destination for files downloaded/exported via playback mode.

Picture and Clip Settings

Set the destination of captured pictures/stillshots and clipped video files. Valid only for media captured manually via the web browser UI.

- **Save snapshots in live view to:** Set the destination of the manually captured pictures in live view mode.
- **Save snapshots when playback to:** Set the destination of the captured pictures in playback mode.
- **Save clips to:** Set the destination of clipped video files in playback mode.

NOTE: The user can click Browse to change the directory for saving the clips and pictures, and click Open to select the desired folder.

3. Click Save to save the settings.

4.2 Live View

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

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

4.2.1 LIVE VIEW PAGE – COMPONENT DESCRIPTIONS

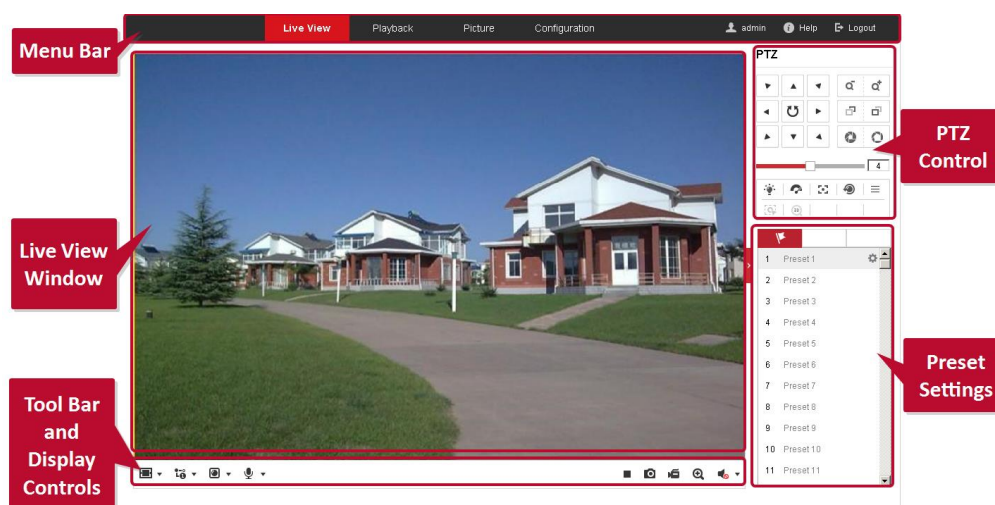


Figure 4-2 View Page

- **Menu Bar:** Click each tab to enter Live View, Playback, Log and Configuration page respectively.
- **Display Control:** Click available buttons to open corresponding tabs to change stream type and aspect ratio. Click the plug-ins drop-down to select available plug-in
- **Live View Window:** Displays live video from the camera.
- **Toolbar:** Operations on the live view page, e.g., live view, capture, record, audio on/off, two-way audio, etc.
- **PTZ Control:** Panning, tilting and zooming functions for the camera and the lighter and wiper control (if aux PTZ functions are supported or an external pan/tilt unit has been installed).

- **Preset Setting/Calling:** Set and call the preset for the camera (if supports PTZ preset functionality is supported or an external pan/tilt unit has been installed). Starting Live View

In the live view window as shown in Figure 7-1, click  on the toolbar to start the live view of the camera.



Figure 4-3 Live View Toolbar

















Icon	Description
	Start/Stop live view.
	Self-adaptive window size.
	Aspect Ratio: 4:3.
	Aspect Ratio: 16:9.
	Default aspect ratio.
	Live view main stream.
	Live view sub stream.
	Live view third stream.
	<ul style="list-style-type: none"> ■ Third-party plugins: Click to choose an active third-party plug-in. For IE (internet explorer) users, WebComponents and QuickTime are available. For Non-IE users, WebComponents, QuickTime, VLC or MJPEG are selectable if they are supported by the web browser.
	Manually take a stillshot.
	Manually start/stop recording.
	Audio on and adjust volume /Mute.
	Engage two-way audio (multiple channels available on applicable devices)
	Turn on/off digital zooming function.

Table 5-1 Live View Toolbar - Descriptions

4.3 Recording and Capturing Pictures Manually

In the live view interface, click  on the toolbar to capture live stillshots or click  to manually trigger recording. Destination paths for captured pictures and clips can be set on the **Configuration > Local Configuration** page.

NOTE: The captured image will be saved as JPEG file or BMP file to the defined destination path.

4.4 Operating PTZ Control



In the live view interface, you can use the PTZ control buttons to issue pan/tilt/zoom commands to applicable cameras.

Before you start:

To utilize PTZ control, the camera connected to the network must support the PTZ function or a pan/tilt unit has been installed to the camera. Please properly set the PTZ parameters on the RS-485 settings page. Refer to **Section 6.4.1 System Settings - Configuring RS-485** for more information.

4.4.1 PTZ CONTROL PANEL

Steps:

1. On the live view page, click  to show the PTZ control panel or click  to hide it.
2. Click the direction buttons to control the pan/tilt movement.

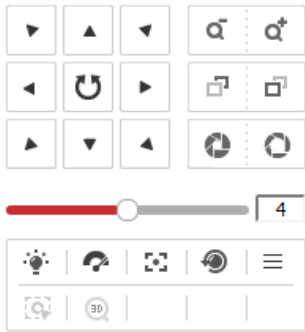



Figure 4-4 PTZ Control Panel

3. Click the zoom/iris/focus buttons to utilize lens control.
- There are 8 direction arrows () in the live view window when you click and drag the mouse in the relative positions.
 - For cameras which support lens movement only, the direction buttons are invalid.












Icon	Description
	Zoom in/out
	Focus near/far
	Iris +/-
	Light on/off
	Wiper on/off
	One-touch focus
	Initialize lens
	Adjust speed of pan/tilt movements
	Adjust speed of pan/tilt movements
	Start Manual Tracking
	Start 3D Zoom

Table 5-2 Descriptions of PTZ Control Panel

4.4.2 SETTING A PRESET

Steps:

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

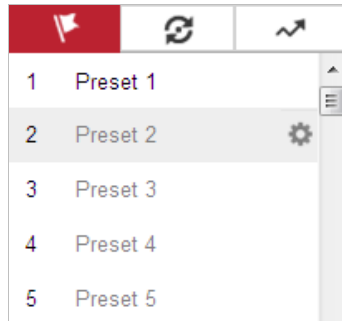





Figure 4-5 Setting a Preset

2. Use the PTZ control buttons to aim the camera toward 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 save the current camera position to the selected preset.

The user can click  to delete the preset.

NOTE: The user can configure up to 128 presets.

4.4.3 CALLING A PRESET

This feature enables the camera to point to a specified preset scene manually or when an event takes place. A user can call a preset at any time to shift position to the desired preset coordinates. In the PTZ control panel, select a defined preset from the list and click  to call the preset. Alternatively, select the Presets interface, and call the preset by manually typing the preset No.

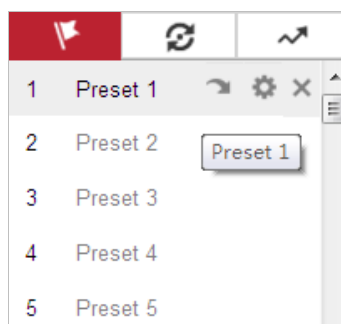


Figure 4-6 Calling a Preset

- The following presets are predefined with special commands. These presets can be called but are not customizable. For instance, preset 99 is “Start auto scan”. If you call the preset 99, the camera initiates the auto scan function.
- Pattern function varies depending on different camera models.

Table 1-1 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

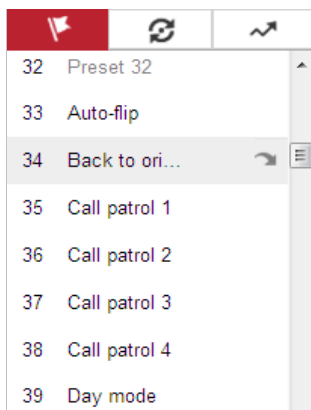




Figure 4-7 Special Preset

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.

4.4.4 SETTING/CALLING A PATROL

NOTE: No less than 2 presets must be configured before you set a patrol.

Steps:

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

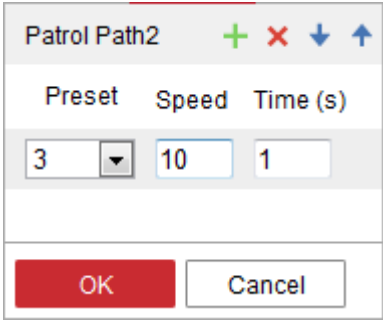





Figure 4-8 Add Patrol Path

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

4.4.5 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 4-9.

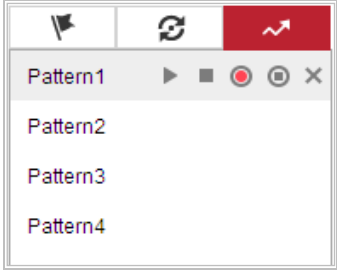










Figure 4-9 Patterns Settings Interface

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 REMAINING 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.

NOTE 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 recorded video files stored on a configured network drive or the camera's local SD card via the camera's browser interface.

Note: Playback footage can also be retrieved via VIGIL Client and other VIGIL VMS clients that have been properly interfaced with the camera.

Steps:

- Click Playback on the menu bar to enter the playback interface.

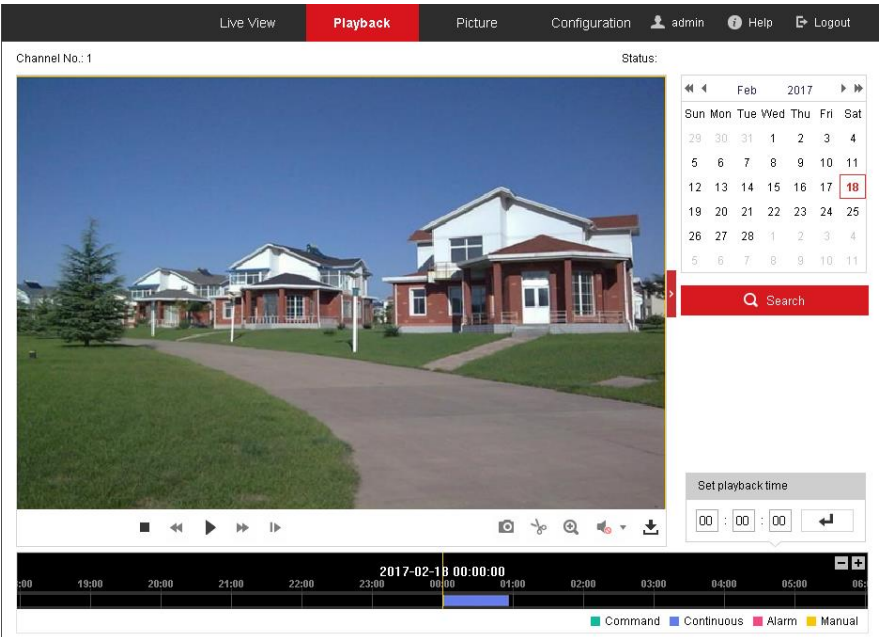


Figure 4-10 Playback Interface

Select the date and click Search.

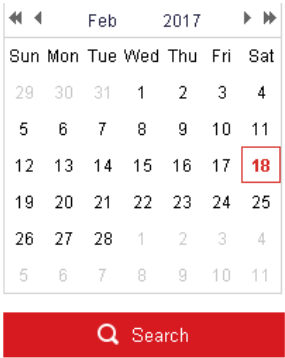


Figure 4-11 Search Video


Click  to play the video files found on this date. The toolbar on the bottom of Playback interface can be used to control the active playback footage.



Figure 4-12 Playback Toolbar














Button	Operation	Button	Operation
	Play		Capture and download a stillshot.
	Pause		Start/Stop clipping video files
	Stop		Audio on and adjust volume/Mute
	Increase / Decrease playback speed		Download files
	Playback by frame		Enable/Disable digital zoom

Table 8-1 Description of the buttons

NOTE: The user can choose the local file paths for downloaded playback files and snapshots/pictures via the Local Configuration interface. Please refer to **Section 4.1 – Local Configuration** for details. Drag the progress bar with the mouse to locate your desired playback point. The user can also input the time in the **Set playback time** field and click  to locate the playback point. Click   to zoom out of or into the progress bar.

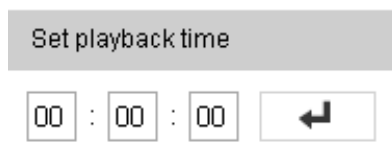


Figure 4-13 Set Playback Time



Figure 4-14 Progress Bar

The different colors for video in the progress bar represent the different recording modes.





 Command  Continuous  Alarm  Manual

Figure 4-15 Recording Modes

4.6 Picture

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

NOTES:

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

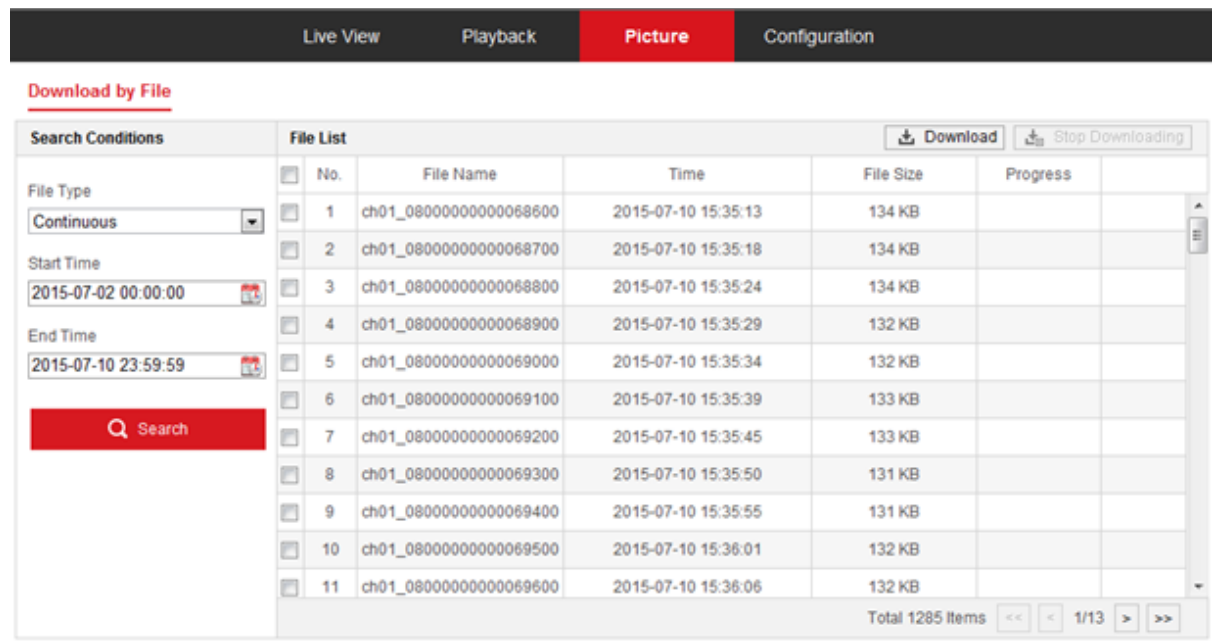


Figure 4-16 Picture Search Interface

Steps:

1. Select the file type from the dropdown list. *Continuous, Motion, Alarm, Motion | Alarm, Motion & Alarm, Line Crossing, Intrusion Detection, and Scene Change Detection* are selectable.
2. Select the start time and end time.
3. Click Search to display a list of results.
4. Check off desired snapshots and click Download to download the selected images.

NOTE: Up to 4000 images can be available in the search index simultaneously.

5 System Configuration

5.1 Storage Settings

Before you start:

To configure recording settings, make sure that you have the network storage device within the network or the memory card inserted in your camera. If the camera is interfaced with VIGIL Server, footage recorded by the VIGIL Server will be stored on the VIGIL Server's media drive.

5.1.1 CONFIGURING RECORDING SCHEDULE

Purpose:

There are two kinds of recording for the camera: manual recording and scheduled recording. In this section, follow the instructions to configure scheduled recording. By default, files recorded via scheduled recording are stored in the memory card (if supported) or on the network disk. If interfaced with a VIGIL Server, recorded files will be stored in the VIGIL Server's media drive.

Steps:

1. Enter the Record Schedule settings interface: **Configuration > Storage > Schedule Settings > Record Schedule**

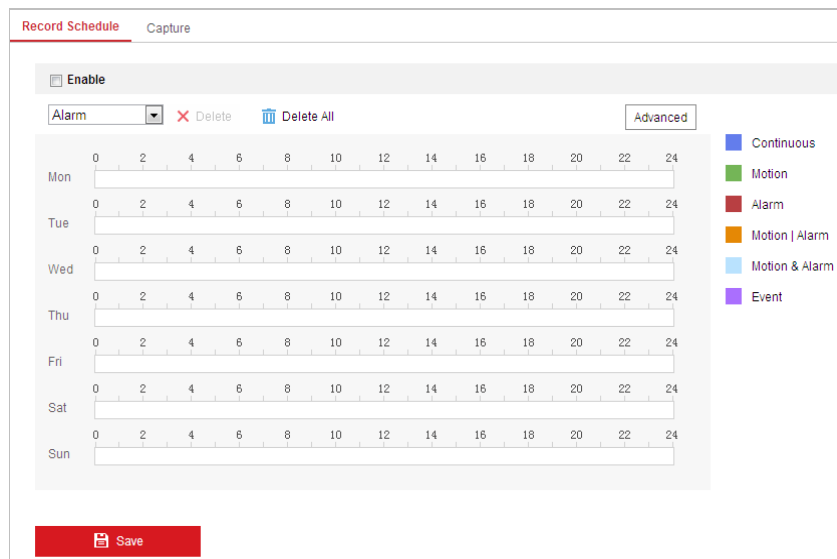


Figure 5-1 Recording Schedule Interface

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

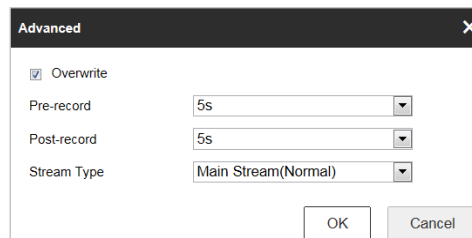


Figure 5-2 Record Parameters

- **Pre-record:** The time you set to start recording before the scheduled time or 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 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:** The user 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 longer with the same storage capacity.

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

- Click **OK** to save advanced settings.
- 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 toggle the **Trigger Channel** checkbox in the Linkage Method of Motion Detection settings interface. For detailed information, refer to **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 toggle **Trigger Channel** checkbox in the Linkage Method of Alarm Input settings interface. For detailed information, refer to **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 if 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 are triggered.
- Click  Save to save the settings.

5.1.2 CONFIGURING CAPTURE SCHEDULE

Purpose:

The user can configure scheduled snapshots and event-triggered snapshots. Captured stillshots can be stored in local storage or network storage.

Steps:

- Enter the Snapshot settings interface: **Configuration > Storage > Storage Settings > Capture**

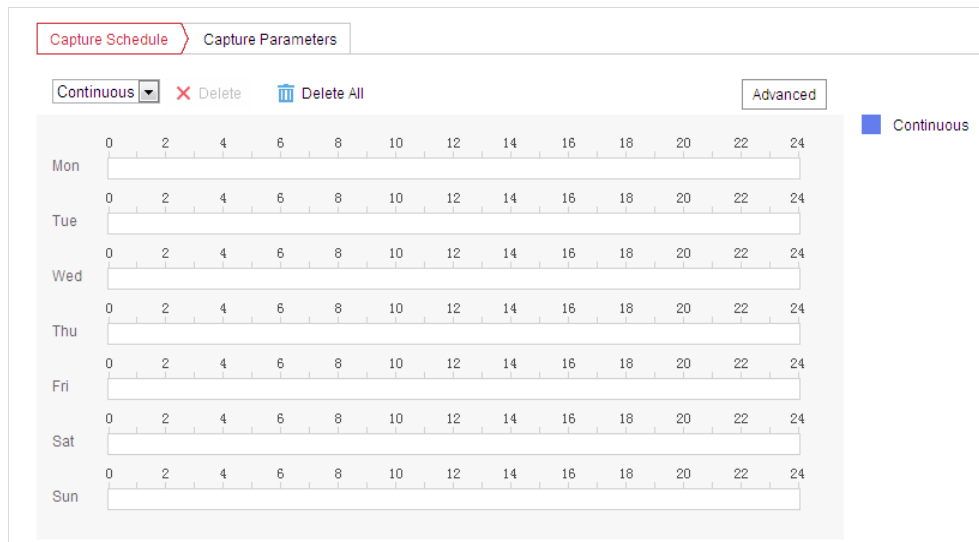



Figure 5-3 Snapshot Settings

- Click **Capture Schedule** to enter the Capture Schedule interface.
- Select the timeline of a specific day, and drag the left button of the mouse to set the capture schedule (the start time and end time of the recording task).
- After you set the scheduled task, you can click  and copy the task to other days (optional).
- 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)

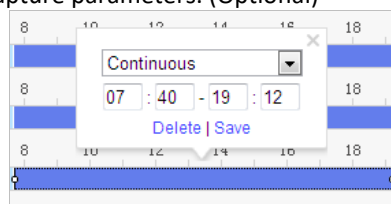



Figure 5-4 Segment Snapshot Settings

- Click **Advanced** to enter the advanced settings interface. The user can select the stream type from this interface.
- Click **Capture Parameters** to enter the Capture Parameters interface.
- Toggle the **Enable Timing Snapshot** checkbox to enable continuous snapshots and configure the schedule for this mode accordingly. Toggle the **Enable Event-triggered Snapshot** checkbox to enable event-triggered snapshot.
- Select the format, resolution and quality of the snapshot.
- Set the time interval between two snapshots.

- Click  to save the settings.

Uploading to FTP

NOTE: Make sure that the FTP server is online.

Follow the below configuration instructions to upload snapshots to an FTP server.

Upload continuous snapshots to FTP

Steps:

- 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.
- Toggle the **Enable Timing Snapshot** checkbox.
- Click **Edit** to set the snapshot schedule. Refer to **Section 5.2.1 Configuring Motion Detection** for details on configuring schedules.

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 on configuring 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** for more details.
3. Toggle the **Enable Event-triggered Snapshot** checkbox.

5.1.3 CONFIGURING NET HDD

Before you start:

The network disk should be available on 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**

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

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

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. The user can set the user name and password to guarantee security if SMB/CIFS is selected.

NOTE: Refer to the *NAS User Manual* for creating the file path.



Warning

- 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.

NOTE: 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 properties of the disk.

HDD Management Net HDD

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

Quota

Max. Picture Capacity

Free Size for Picture

Max. Record Capacity

Free Size for Record

Figure 5-6 Storage Management Interface

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

HDD Management

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

Figure 5-7 View Disk Status

■ Define the Quota for Record and Pictures

- Input the quota percentage for pictures/ stillshots and for recording.
- Click **Save** and refresh the browser page to activate the settings.

Quota

Max. Picture Capacity

Free Size for Picture

Max. Record Capacity

Free Size for Record

Percentage of Picture %

Percentage of Record %

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 inserting it into the camera, refer to the NAS disk initialization steps.

5.1.4 MEMORY CARD DETECTION

Purpose:

With memory card detection, you can view the memory card status, lock your memory card, and receive notifications when your issues with the memory card are detected.

- NOTE:** The Memory card detection function is only supported by certain types of memory cards and camera models. If this tab page doesn't show on your web page, it means either that your camera

doesn't support the function, or your installed memory card is not supported for this function.
You can contact the dealer or the retailer for the information on supported memory cards.

Steps:

1. Enter Memory Card Detection configuration interface:

Configuration > Storage > Storage Management > Memory Card Detection

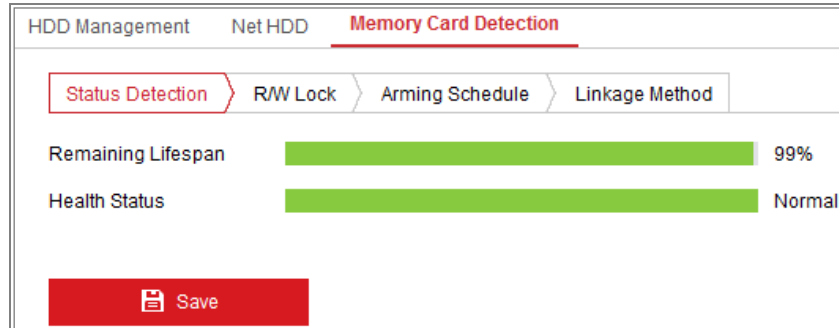


Figure 5-9 Memory Card Detection

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

- **Remaining Lifespan:** It shows the percentage of the remaining lifespan. The lifespan of a memory card may be influenced by factors such as its capacity and the bitrate. You need to change the memory card if the remaining lifespan is not enough.
- **Health Status:** It shows the condition of your memory card. There are three status descriptions, good, bad, and damaged. You will receive a notification if the health status is anything other than good when the **Arming Schedule** and **Linkage Method** are set.

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

3. Click **R/W Lock** tab to add a lock to the memory card. With the R/W lock added, the memory card can only be read and write when it is unlocked.

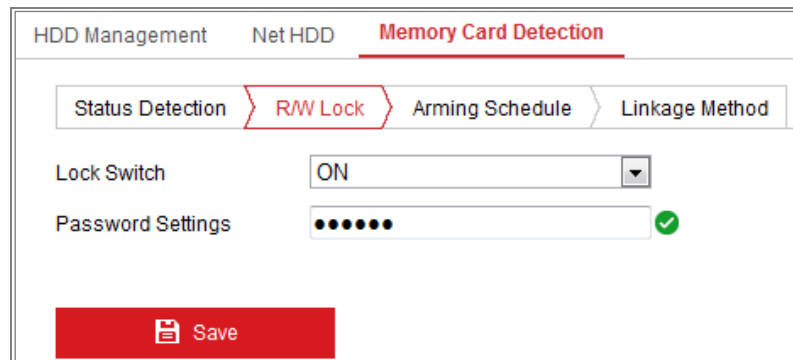


Figure 5-10 R/W Lock Setting

Add a Lock

1. Set the Lock Switch to **ON**.
2. Input the password.
3. Click **Save** to save the settings.

Unlock

1. If you use the memory card on the camera that auto-locks the card, unlocking will occur automatically, and no unlocking procedures are required on the part of users.
2. If you use the memory card (with a lock) on a different camera, you can go to **HDD Management** interface to unlock the memory card. Select the memory card, and click the **Unlock** button shown next to the **Format**

button. Lastly, input the correct password to unlock it.

- The memory card can only be read and written in when it is unlocked.

NOTE: ■ If the camera, which adds a lock to a memory card, is restored to the factory settings, you can go to the HDD Management interface to unlock the memory card.

Remove the Lock

1. Select the **Lock Switch** as **OFF**.
2. Input the correct password in **Password Settings** text field.
3. Click **Save** to save the settings.
4. Set the **Arming Schedule** and **Linkage Method**, if you want to receive a notification when the health status of the memory card is anything other than "Good".
5. Click **Save** to save the settings.

5.1.5 CONFIGURING LITE STORAGE

Purpose:

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

- NOTES:**
- Lite storage function varies according to different camera models.
 - The video files recorded in lite storage mode will be played back in full frame rate (25fps/30fps), and thus the playback process is speeded up to the eye.



1. Enter the Lite Storage interface:
Configuration > Storage > Storage Management > Lite Storage
2. Check off **Enable** to enable the lite storage function.
3. Input the storage time in the text field. You can view the available space of the SD card on the page.
4. Click **Save** to save the settings.

5.2 Basic Event Configuration

Purpose:

This section explains how to configure the network camera to respond to alarm events, including motion detection, video tampering alarm input, alarm output and exceptions. These events can trigger 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 detects object movement in the configured surveillance area, and a series of actions can be taken when the alarm is triggered.

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

Steps:

1. Enter the motion detection setting interface: **Configuration > Event > Basic Event > Motion Detection**
2. Toggle the **Enable Motion Detection** checkbox.
 - ▶ When **Enable Motion Detection in PTZ Control** is toggled on, motion detection can also trigger alarms when the speed dome is performing PTZ actions.
 - ▶ When **Enable Dynamic Analysis for Motion** is toggled on, detected objects are marked with a tracking rectangle in the live view.
3. Select the configuration mode as **Normal** or **Expert** then set the corresponding motion detection parameters.
 - **Normal**

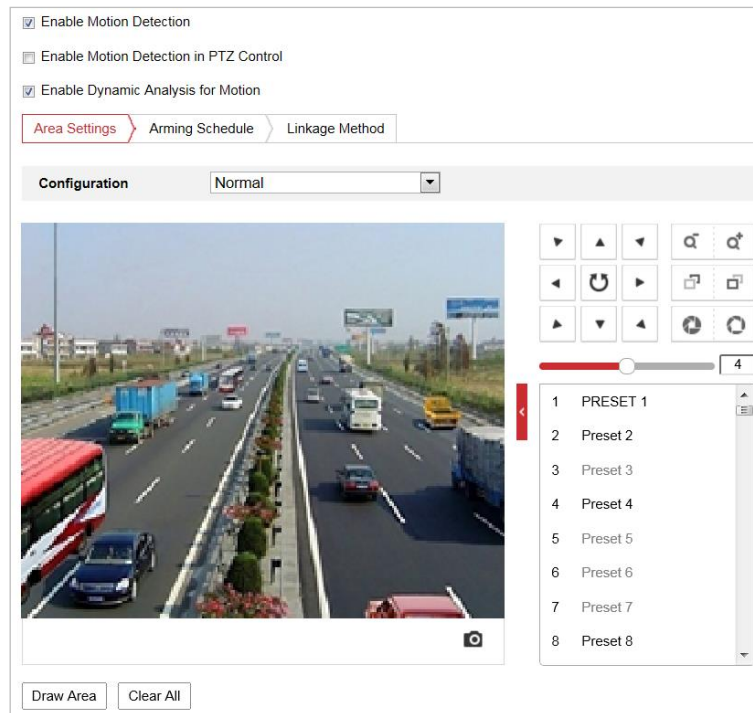


Figure 5-11 Motion Detection Settings-Normal

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: The user can click **Clear All** to clear all motion areas.

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

■ **Expert**

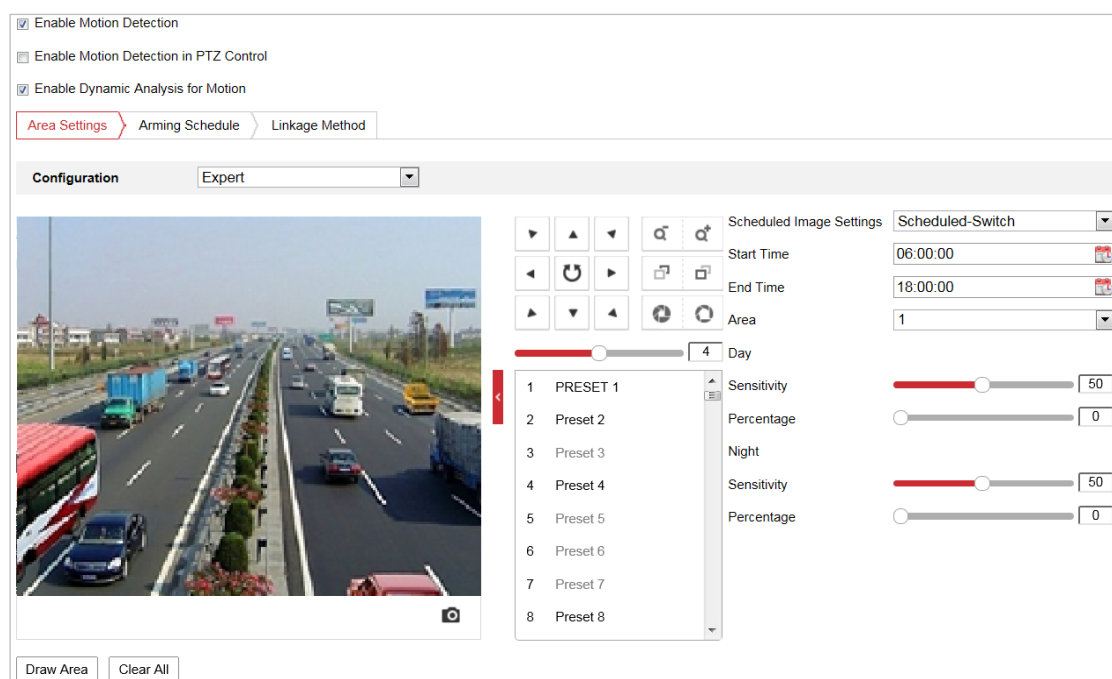


Figure 5-12 Motion Detection Settings-Expert

Steps:

- (1) **Schedule Image Settings, OFF, Auto-Switch** and **Scheduled-Switch** modes are available. If the schedule image switch mode is enabled, you can configure the detection rule for day and night separately.
 - (2) **OFF:** Disable the day and night switch.
 - (3) **Auto-Switch:** Switch the day and night mode according to illumination automatically.
 - (4) **Scheduled-Switch:** Switch to the day / night mode according to the configured time. You need to set the start time and end time.
 - (5) Select Area from the dropdown list to configure.
 - (6) Set the sensitivity and percentage values.
 - (7) **Sensitivity:** The greater the value is, the easier the alarm will be triggered.
 - (8) **Percentage:** When the proportional size of the moving object exceeds the predefined value, the alarm will be triggered. The smaller the value, the easier the alarm will be triggered.
4. Set the **Arming Schedule** for Motion Detection.
- (1) Click the **Arming Schedule** tab to enter the arming schedule setting interface.

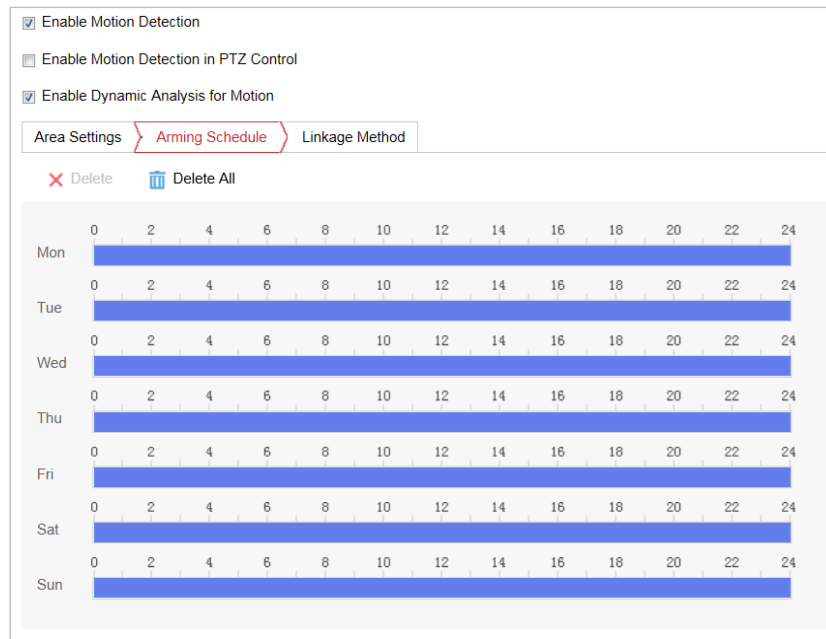



Figure 5-13 Arming Schedule

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

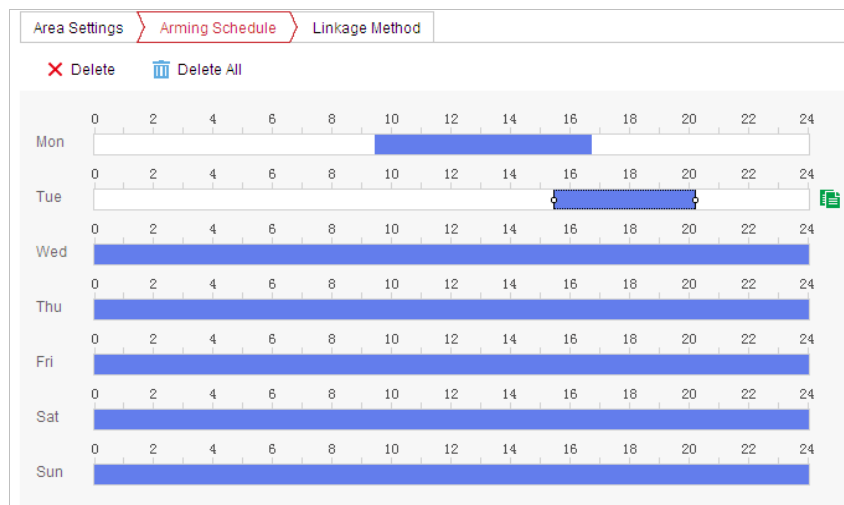



Figure 5-14 Arming Time Schedule

- (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 5-15 Segment Arming Settings

- (5) Click  to save settings.

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

- Set the **Alarm Actions** for Motion Detection. Click **Linkage Method** tab to enter the **Linkage Method** interface.

The user can specify the camera's response when an event occurs. This is referred to as a linkage method. The following contents are about how to configure the different types of linkage methods.

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

Figure 5-16 Linkage Method

Toggle the checkbox to select the linkage method. Notify Surveillance Center, Send Email, Upload to FTP/Memory/NAS, Trigger Alarm Output and Trigger Recording methods can be selected..

■ 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 an Email when an event occurs, you need to refer to **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 an FTP server.

NOTE: FTP parameters must be configured. Refer to **Configuring FTP Settings** for setting FTP parameters.

■ Trigger Alarm Output

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

NOTE: To trigger an alarm output when an event occurs, refer to **Section 5.2.5 Configuring Alarm Output** to set the alarm output parameters.

■ Trigger Recording

Record a video when an event occurs.

NOTE: You have to set the recording schedule to utilize this function. Refer to **Section 5.1.1 Configuring Recording Schedule** for setting the recording schedule.

5.2.2 CONFIGURING VIDEO TAMPERING ALARM

Purpose:

The user can configure the camera to trigger an alarm when the lens is covered / obscured and also configure certain alarm response actions when tampering is detected.

Steps:

1. Enter the Video Tampering settings interface: **Configuration > Event > Basic Event > Video Tampering**

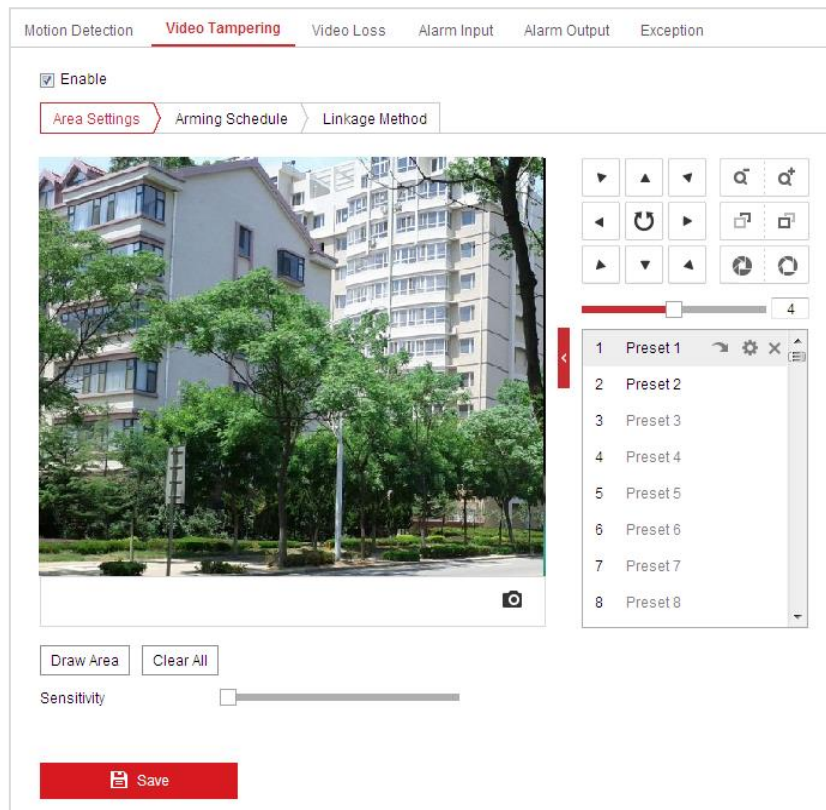


Figure 5-17 Tampering Alarm

2. Check **Enable** checkbox to enable the tampering detection.
3. Click **Arming Schedule** tab to enter the arming schedule settings interface. The arming schedule configuration is identical to configuring 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** for more information on configuring linkage methods.
5. Click **Save** to save the settings.

5.2.3 CONFIGURING VIDEO LOSS

Steps:

1. Enter the Video Loss settings interface: **Configuration > Event > Basic Event > Video Loss**

The screenshot shows the 'Video Loss' configuration page. At the top, there is an 'Enable' checkbox which is checked. Below it are two tabs: 'Arming Schedule' (highlighted with a red border) and 'Linkage Method'. To the left of the calendar grid are two buttons: 'Delete' (with a red X icon) and 'Delete All' (with a trash can icon). The calendar grid shows days of the week (Mon to Sun) on the left and time slots (0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24) on the top. Each time slot is represented by a blue bar, indicating that video loss detection is armed for all times on all days. At the bottom of the interface is a red 'Save' button.

Figure 5-18 Video Loss

2. Toggle the **Enable** checkbox to enable video loss detection.
3. Click the **Arming Schedule** tab to enter the arming schedule settings interface. The arming schedule configuration process is identical to configuring an arming schedule for motion detection. Refer to **Section 5.2.1 Configuring Motion Detection** for more details.
4. Click the **Linkage Method** tab to select the linkage method taken for the video loss alarm. Notify surveillance center, send email and trigger alarm output are available. Refer to **Section 5.2.1 Configuring Motion Detection** for details on configuring linkage methods.
5. Click **Save** to save settings.

5.2.4 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).

Figure 5-19 Alarm Input Settings

- Click the **Arming Schedule** tab to enter the arming schedule setting interface. The arming schedule configuration is identical to configuring the arming schedule for motion detection. Refer to **Section 5.2.1 Configuring Motion Detection** for more details.
- Click the **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** for details on configuring linkage methods.
- The user can also choose a PTZ linkage for the alarm input. Toggle the corresponding checkbox and select the No. to enable Preset Calling, Patrol Calling or Pattern Calling.
- Copy settings to other alarm inputs as desired.
- Click **Save** to save the settings.

Figure 5-20 Linkage Method

5.2.5 CONFIGURING ALARM OUTPUT

Steps:

- Enter the Alarm Output settings interface: Configuration > Event > Basic Event > Alarm Output.
- Select one alarm output channel in the **Alarm Output** dropdown list.

- Set a name in (cannot copy) for the alarm output (optional).
- 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.
- Click the **Arming Schedule** tab to enter the arming schedule setting interface. The time schedule configuration is identical to configuring an arming schedule for motion detection. Refer to **Section 5.2.1 Configuring Motion Detection** for more details.

Alarm Output No. IP Address

Delay Alarm Name

Alarm Status (cannot copy)

Arming Schedule

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

Figure 5-21 Alarm Output Settings

- If desired, copy the settings to other alarm outputs.
- Click to save the settings.

5.2.6 HANDLING EXCEPTIONS

Available exception types: HDD full, HDD error, Network disconnected, IP address conflict and Illegal camera login.

Steps:

- Enter the Exception settings interface: Configuration > Event > Basic Event > Exception
- Check off the corresponding checkbox for desired Exception alarm linkages. Refer to **Section 5.2.1 Configuring Motion Detection** for details on configuring linkage methods.

Exception Type

HDD Full

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

Save

Figure 5-22 Exception Settings

3. Click

Save

 to save the settings.

5.3 Smart Event Configuration

NOTE: The functions vary depending on different camera models.

5.3.1 DETECTING AUDIO EXCEPTIONS

Purpose:
When you enable this function and an audio exception occurs, the configured alarm action will be triggered.

- Steps:**
1. Enter the video audio exception detection interface: **Configuration > Event > Smart Event > Audio Exception Detection**

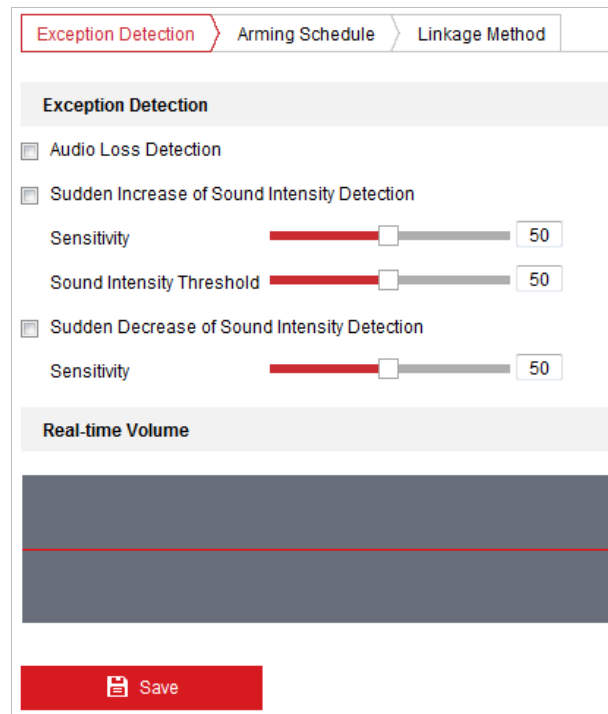


Figure 5-23 Audio Exception Detection

2. Toggle the Audio Loss Detection checkbox to enable the audio input exception detection.
3. Toggle the Sudden Increase of Sound Intensity Detection checkbox to enable sudden rise detection.
 - ▶ **Sensitivity:** Range [1-100]. Smaller values will require a more severe sound change to trigger detection.
 - ▶ **Sound Intensity Threshold:** The sound intensity range is [1-100]. The louder the environment, the higher the value should be.
4. Toggle the Sudden Decrease of Sound Intensity Detection checkbox to enable the sudden drop detection.
 - ▶ **Sensitivity:** Range [1-100]. Smaller values will require a more severe sound change to trigger detection.
5. Click the **Arming Schedule** tab to enter the arming schedule setting interface. The time schedule configuration is identical to configuring an arming schedule for motion detection. Refer to Section 5.2.1 Configuring Motion Detection for more details.
6. Click the **Linkage Method** tab to select the linkage method taken for the audio input exception. Available linkages include Notify Surveillance Center, Send Email, Trigger Alarm Output and Trigger Recording. Refer to Section 5.2.1 Configuring Motion Detection.
7. Click **Save** to save the settings.

1.1.1 CONFIGURING DEFOCUS DETECTION

Purpose:

The image blur caused by a defocused lens can be detected, and specific actions can be taken in response to defocus detection.

NOTE: Defocus detection function varies according to different camera models.

Steps:

1. Enter the Defocus Detection settings interface: **Configuration > Event > Smart Event > Defocus Detection**.

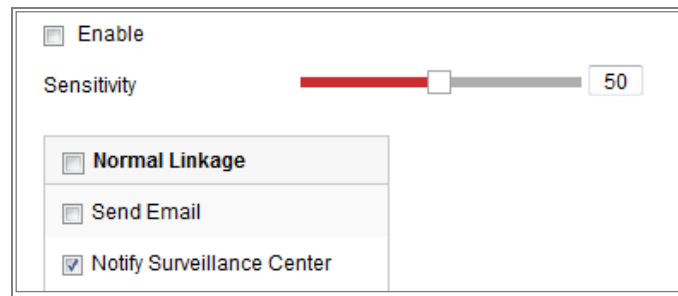


Figure 5-24 Configuring Defocus Detection

2. Check off **Enable** to enable the function.
3. Click-and-drag the slider to set the detection sensitivity. The sensitivity value ranges from 1 to 100. The higher the value is, the more easily the defocused image can trigger the alarm.
4. Select the linkage methods for defocus.
5. Click **Save** to save the settings.

1.1.2 CONFIGURING SCENE CHANGE DETECTION

Purpose:

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

NOTE: Scene change detection function varies according to different camera models.

Steps:

1. Enter the Scene Change Detection settings interface, **Configuration > Event > Smart Event > Scene Change Detection**.



Figure 5-25 Scene Change Detection

2. Check off **Enable** to enable the function.
3. Click-and-drag the slider to set the detection sensitivity. The sensitivity value ranges from 1 to 100. The higher the value, the more sensitive the alarm trigger will be to minor scene changes.
4. Click **Arming Schedule** to set the arming schedule.
5. Click **Linkage Method** to select the linkage methods for scene change.
6. Click **Save** to save the settings.

5.3.2 CONFIGURING FACE DETECTION

Purpose:

After face detection is enabled, when a face appears in the surveillance area, it can be detected by the camera. Certain actions may be triggered by the detection.

Steps:

1. Toggle the **Enable Face Detection** checkbox.
2. (Optional) The user can toggle the **Enable Dynamic Analysis for Face Detection** checkbox if you want the detected face marked with a tracking rectangle in the live view.

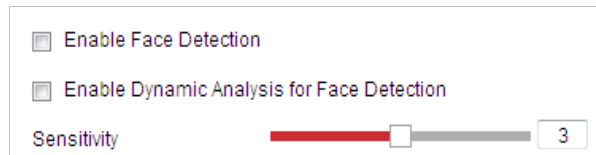


Figure 1-2 Configuring Face Detection

3. Configure the sensitivity for face detection.
 - ▶ **Sensitivity:** Range [1-5]. 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.
4. Click the **Arming Schedule** tab to enter the arming schedule setting interface. The time schedule configuration is identical to configuring an arming schedule for motion detection. Refer to **Section 5.2.1 Configuring Motion Detection** for more details.
5. Click the **Linkage Method** tab to select the linkage method taken for the video loss alarm. Available linkages include Notify surveillance center, Send email, Upload to FTP, Trigger channel, Smart tracking and Trigger alarm output. Refer to **Section 5.2.1 Configuring Motion Detection** for details on configuring linkage methods.
6. Click **Save** to save the settings.

5.3.3 CONFIGURING INTRUSION DETECTION

Intrusion detection can set an area in the camera's field of vision and once the area is entered, a set of alarm action(s) are triggered.

Steps:

1. Enter the intrusion detection interface: **Configuration > Events > Smart Event > Intrusion Detection**
2. Toggle the **Enable** checkbox.

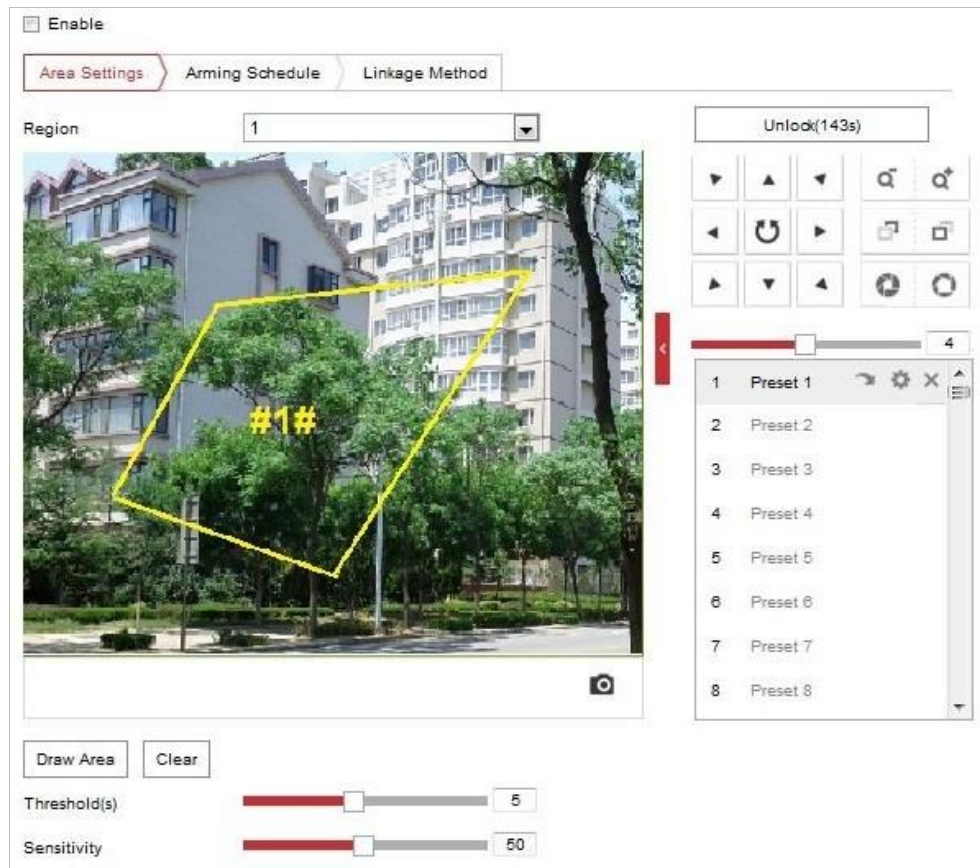


Figure 5-26 Configuring Intrusion Area

3. Any 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 detection region.
 - 3) Click on the image to specify a corner of the rectangle, and right-click the mouse after four corners are configured.
5. Configure the parameters for each 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 enters 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 the **Arming Schedule** tab to enter the arming schedule setting interface. The time schedule configuration is identical to configuring an arming schedule for motion detection. Refer to **Section 5.2.1 Configuring Motion Detection** for more details.
7. Click the **Linkage Method** tab to select the linkage method taken for intrusion detection. Available

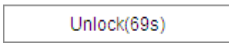
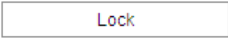
linkages include Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Alarm Output and Trigger Recording are selectable. Refer to **Section 5.2.1 Configuring Motion Detection** for more detail on configuring linkage methods.

8. Click  to save the settings.

5.3.4 CONFIGURING LINE CROSSING DETECTION

Virtual plane (line) detection can be adopted as an intrusion detection method. Once the camera detects the line being crossed according to the configured direction, a set of alarm action(s) are triggered.

Steps:

1. Enter the Line Crossing Detection interface: **Configuration > Event > Smart Event > Line Crossing Detection**.
2. Toggle the **Enable** checkbox to enable the line crossing detection function.
3. Select the Line to configure from the drop-down list.
4. Any 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  button to manually activate the movement. Movement can be re-locked by clicking the  button.

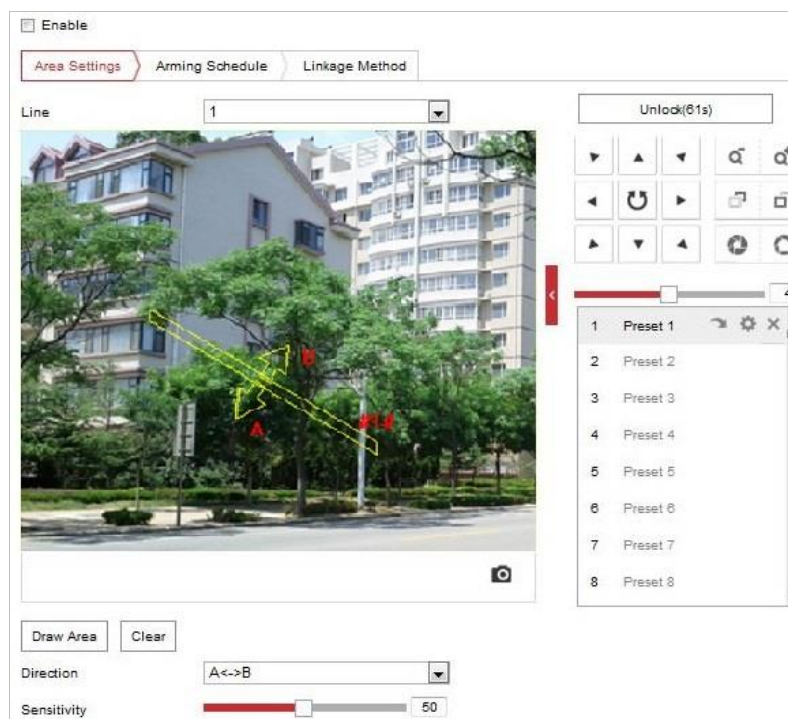
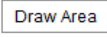


Figure 5-27 Configuring Line

5. Draw area.
 - 1) Click  to draw a line on the image.
 - 2) Click the line to switch to editing mode.
 - 3) Drag an end to the desired coordinate to adjust the length and angle of the line. Click and drag the line from the middle to adjust the location.
6. Configure the parameters for each detection region separately.

- **Direction:** Select the detection direction in the dropdown list. Available directions include:
 - ▶ A<->B
 - ▶ A->B
 - ▶ B->A
 - **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 the **Arming Schedule** tab to enter the arming schedule setting interface. The time schedule configuration is identical to configuring an arming schedule for motion detection. Refer to **Section 5.2.1 Configuring Motion Detection** for more details.
 8. Click the **Linkage Method** tab to select the linkage methods for line crossing detection. Available linkages include 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** for more details on configuring linkages.
 9. Click **Save** to save the settings.

5.3.5 CONFIGURING REGION ENTRANCE DETECTION

Purpose:

The Region entrance detection function detects people, vehicles or other objects which enter a pre-defined virtual region from the outside of the defined region. Certain actions can be taken when the alarm is triggered.

Steps:

1. Enter the Region Entrance Detection settings interface: **Configuration> Event > Smart Event> Region Entrance Detection**
2. Toggle the **Enable** checkbox to enable the Region Entrance Detection function.

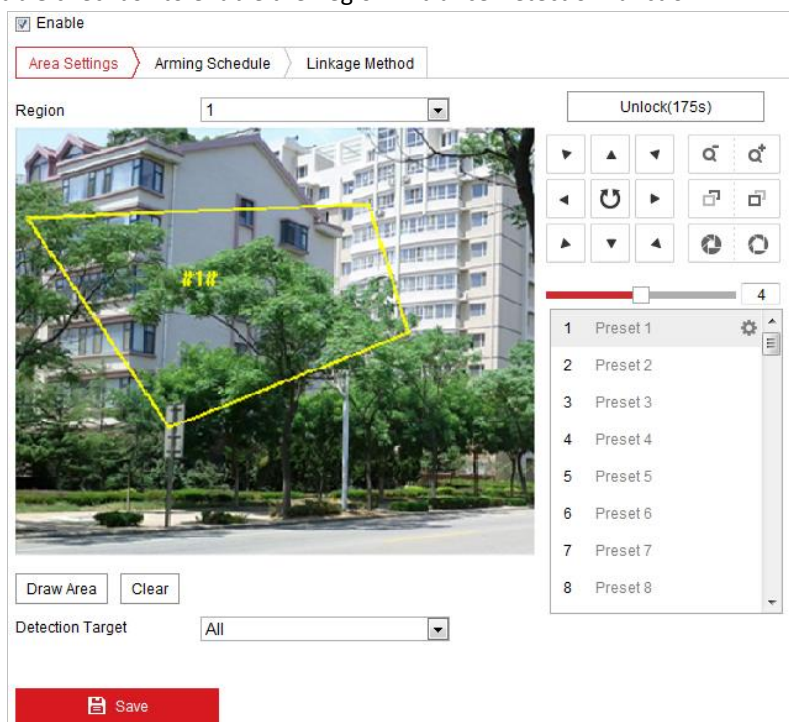


Figure 5-28 Configuring Region Entrance Detection

3. Select the region from the dropdown list for detection settings.
4. Click the **Draw Area** button to start drawing the region.
5. Click on the live video to specify the four vertexes of the detection region. Right click to complete drawing. Repeat the step to configure other regions. The user can click the **Clear** button to clear all pre-defined regions.
6. Set the detection target for region entrance detection. The user can select human, vehicle, or all (human & vehicle) as the detection target from the dropdown list. If Human is selected, only human beings will be identified as detection objects, etc...
7. Click the **Arming Schedule** tab to enter the arming schedule settings interface. The time schedule configuration is identical to configuring an arming schedule for motion detection. Refer to **Section 5.2.1 Configuring Motion Detection** for more details.
8. Click the **Linkage Method** tab to select the linkage method taken for the video loss alarm. Available linkages include Notify surveillance center, Send email, Upload to FTP, Trigger channel, Smart tracking and Trigger alarm output. Refer to **Section 5.2.1 Configuring Motion Detection** for more details on configuring linkages.
9. Click **Save** to save the settings.

5.3.6 CONFIGURING REGION EXITING DETECTION

Purpose:

The Region Exiting detection function detects people, vehicles or other objects which exit from a pre-defined virtual region. Certain actions can be taken when the alarm is triggered.

Steps:

1. Enter the Region Exiting Detection settings interface: **Configuration > Event > Smart Event > Region Exiting Detection**
2. Toggle the checkbox of **Enable** to enable the Region Exiting Detection function.

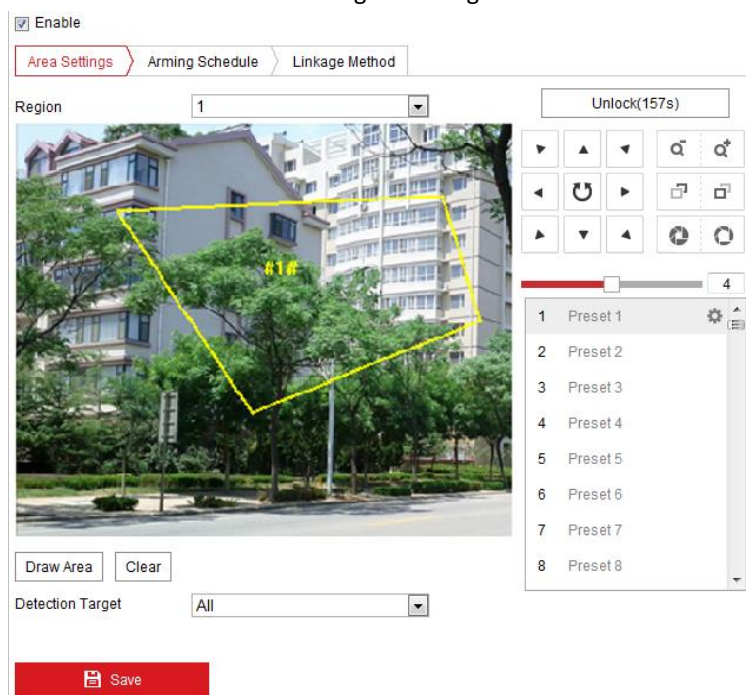


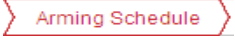






Figure 5-29 Configuring Region Exiting Detection

3. Select the region from the dropdown list for detection settings.
4. Click the  button to begin drawing the region.
5. Click on the live video to specify the four vertexes of the detection region. Right click to complete the drawing. Repeat the steps to configure other regions. Up to 4 regions can be set. The user can click the  button to clear all pre-defined regions.
6. Set the detection target for the region entrance detection. The user can select human, vehicle, or all (human & vehicle) as the detection target. If human is selected, only human beings will be identified as detection objects, etc...
7. Click the  tab to enter the arming schedule setting interface. The time schedule configuration is identical to configuring an arming schedule for motion detection. Refer to **Section 5.2.1 Configuring Motion Detection** for more details.
8. Click the  tab to select the linkage method taken for the video loss alarm. Notify surveillance center, send email, upload to FTP, trigger channel, smart tracking and trigger alarm output are selectable. Refer to **Section 5.2.1 Configuring Motion Detection** for more details on configuring linkages.
9. Click the  button 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

The user can configure basic PTZ parameters, including proportional pan, preset freezing, preset speed, etc.

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

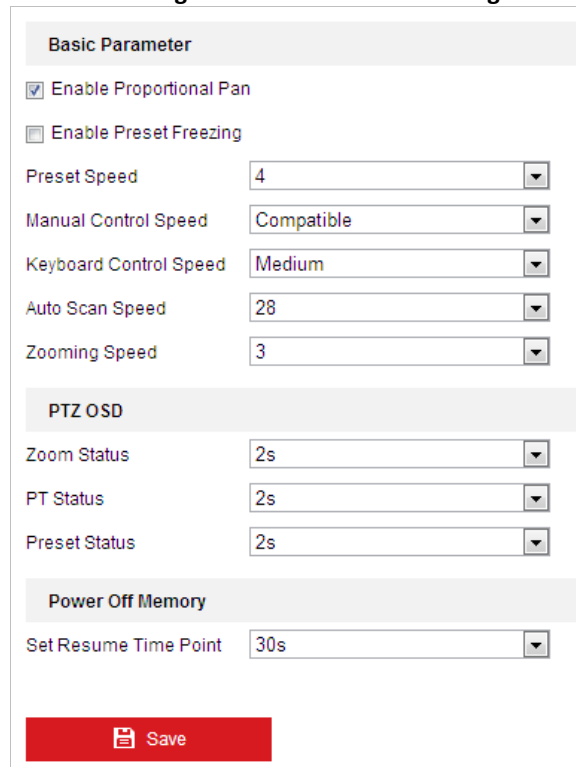


Figure 5-30 Basic Settings

2. Configure the following settings:

- **Basic Parameters:** Set the basic PTZ parameters.
 - ▶ **Proportional Pan:** If you enable this function, the pan/tilt speeds change according to the amount of zoom. When the camera is zoomed in, the pan/tilt speed will be slower to keep the image from moving too fast on the live view image.
 - ▶ **Preset Freezing:** This function enables the live view to switch directly from one scene defined by a preset to another, without showing the middle areas between these two, to ensure surveillance efficiency. It can also reduce the use of bandwidth in a digital network system.
- NOTE:** Preset freezing function is invalid when calling a pattern.
- ▶ **Preset Speed:** The user can set the speed of a defined preset from 1 to 8.
- ▶ **Manual Control Speed:** The manual control speed can be set as Compatible, Pedestrian, Non-motor Vehicle, Motor Vehicle or Auto.
 - ▶ **Compatible:** Using this option ensures the control speed is set the same as the Keyboard Control Speed.
 - ▶ **Pedestrian:** Choose **Pedestrian** when the camera is intended to monitor pedestrians/people.
 - ▶ **Non-motor Vehicle:** Choose **Non-motor Vehicle** when monitoring objects larger than people but smaller than vehicles (bicycles, motorcycles, etc...)

- ▶ **Motor Vehicle:** Choose **Motor Vehicle** when monitoring motor vehicles.
 - ▶ **Auto:** The **Auto settings** is recommended when the application scene of the speed dome is variable.
 - ▶ **Keyboard Control Speed:** Define PTZ control speed via keyboard input. Available speeds are Low, Medium or High.
 - ▶ **Auto Scan Speed:** The scan speed can be set from level 1 to 40.
 - ▶ **Max. Tilt-angle:** Set the tilt-angle of the speed dome from the dropdown list.
 - ▶ **Zooming Speed:** The zoom speed is adjustable from level 1 to 3.
- **PTZ OSD:** Set the on-screen display duration of PTZ status information.
 - ▶ **Zoom Status:** Set the OSD duration of zooming status as 2 seconds, 5 seconds, 10 seconds, NC (Normally Closed), or NO (Normally Open).
 - ▶ **PT Status:** Set the azimuth angle display duration while panning and tilting as 2 seconds, 5 seconds, 10 seconds, NC (Normally Closed), or NO (Normally Open).
 - ▶ **Preset Status:** Set the preset name display duration while calling the preset as 2 seconds, 5 seconds, 10 seconds, NC (Normally Closed), or NO (Normally Open).
 - **Power-off Memory:** The speed dome can resume its previous PTZ status or actions after it restarts from a powered down state. The user can set the time at which the dome resumes its PTZ status. Available times include 30 seconds, 60 seconds, 300 seconds or 600 seconds after power has resumed

3. Click  to save the settings.

5.4.2 CONFIGURING PTZ LIMITS

Purpose:

The speed dome can be programmed to move within the configurable PTZ coordinates (pan/tilt).

Steps:

1. Enter the Limit configuration interface: **Configuration > PTZ > Limit**

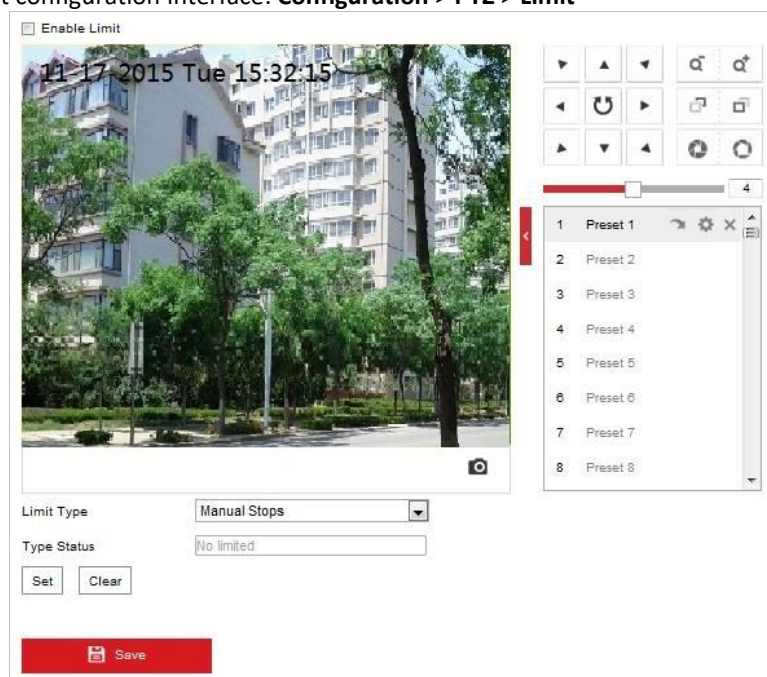



Figure 5-31 Configure the PTZ Limit

2. Toggle the **Enable Limit** checkbox and choose the limit type as manual stops or scan stops.
 - ▶ **Manual Stops:** When manual limit stops are set, you can operate the PTZ control panel manually within the limited surveillance area.
 - ▶ **Scan Stops:** When scan limit stops are set, random scan, frame scan, auto scan, tilt scan, panorama scans are performed in the limited surveillance area only.

NOTE: **Manual Stops of Limit Type** is prior to **Scan Stops**. When you set these two limit types at the same time, **Manual Stops** overrides **Scan Stops**.

- Click the PTZ control buttons to find the left/right/up/down limit stops; you can also call the defined presets and set them as the limits of the speed dome.
- Click **Set** to save the limits or click **Clear** to clear the limits.
- Click  **Save** to save the settings.

5.4.3 CONFIGURING INITIAL POSITION

Purpose:

The initial position is the origin of PTZ coordinates. It can be the factory default initial position. The user can also customize the initial position according to your own needs.

■ **Customize an Initial Position:**

Steps:



- Enter the Initial Position configuration interface: **Configuration > PTZ > Initial Position**



Figure 5-32 PTZ Configuration

- Click the PTZ control buttons to find and set an initial position for the speed dome. The user can also call a defined preset and set it as the initial position of the speed dome.
- Click **Set** to save the position.

■ **Call/delete an Initial Position:**

The user can click  to call the initial position or click  to delete the initial position and restore the factory default initial position.

5.4.4 CONFIGURING PARK ACTIONS

Purpose:

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 to 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 1-3 Set the Park Action

2. Toggle the Enable Park Action checkbox.
3. Set the Park Time value.
4. Choose Action Type the from the dropdown list.
5. If you select Patrol, Pattern, or Preset as Action Type, you need to select an Action Type ID from the dropdown list.
6. Click  Save to save the settings.

5.4.5 CONFIGURING PRIVACY MASK**Purpose:**


The Privacy mask enables you to cover certain areas of the field-of-vision to prevent these areas from being visible in live and recorded footage.

Steps:

7. Enter the Privacy Mask settings interface: **Configuration > PTZ > Privacy Mask**

No.	Name	Type	Enable	Active Zoom Ratio

Figure 5-33 Draw the Privacy Mask

8. Click the PTZ control buttons to find the area you want to obscure with the privacy mask.
9. Click  then drag the mouse in the live video window to draw the area.
10. The user can drag the corners of the red rectangle area to draw a polygon mask.

11. Click **Stop Drawing** to finish drawing or click **Clear All** to clear all of the areas you set without saving them.
12. Click **Add** to save the privacy mask, and it will be listed in the **Privacy Mask List** area. Set the value of **Active Zoom Ratio** to define at which zoom ratio the mask will appear.

Privacy Mask List					Add	Delete
No.	Name	Type	Enable	Active Zoom Ratio		
1	Privacy Mask 1	gray	Yes	1		

Figure 5-34 Privacy Mask List

13. Toggle the checkbox of **Enable Privacy Mask** to enable this function.

5.4.6 CONFIGURING SCHEDULED TASKS

Purpose:

The user can configure the network speed dome to perform an action automatically at a user-defined time period.

Steps:

1. Enter the Scheduled Task settings interface: **Configuration > PTZ > Scheduled Tasks**


Enable Scheduled Task ☐ OFF ✖ Delete 🗑 Delete All

Task Legend:

- OFF
- Auto Scan
- Frame Scan
- Random Scan
- Patrol
- Pattern
- Preset
- Panorama Scan
- Tilt Scan
- Dome Reboot
- Dome Adjust
- Aux Output

Park Time: 5 s

Figure 5-35 Configure Scheduled Tasks

2. Toggle the Enable Scheduled Task checkbox.
3. Set the **Park Time**. Park time is a period of inactivity before the speed dome starts the scheduled tasks.
4. Select the task type from the dropdown list.
5. Select the timeline of the desired day and drag the mouse to set the recording schedule (the start time and end time of the recording task).
6. After you set the scheduled task, you can click  and copy the task to other days (optional).

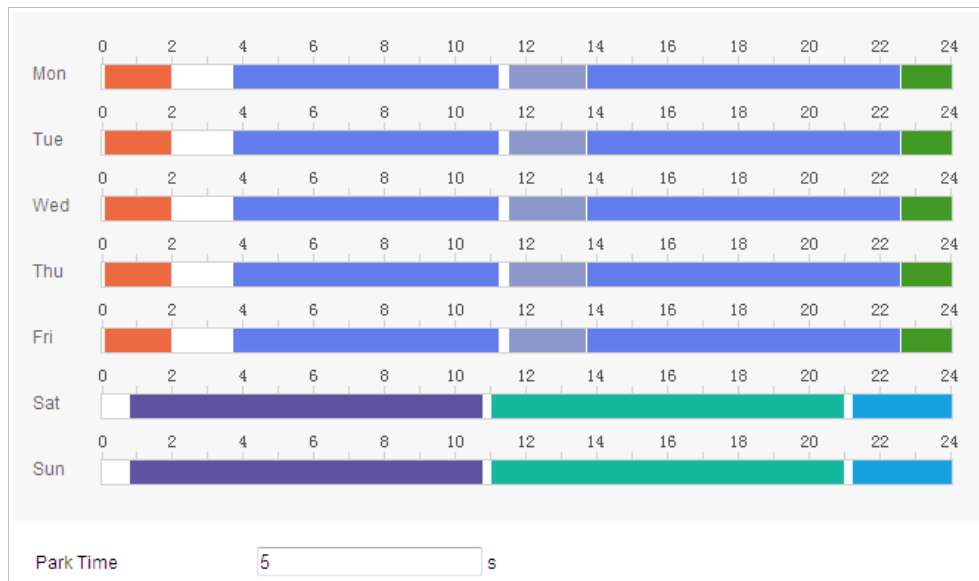


Figure 5-36 Edit the Schedule and Task Type

7. Click  to save the settings.

5.4.7 CLEARING PTZ CONFIGURATIONS

Purpose:

The user can clear PTZ configurations in this interface, including all presets, patrols, privacy masks, PTZ limits, scheduled tasks and park actions.

Steps:

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

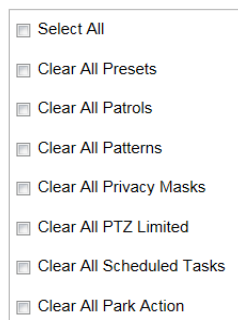


Figure 5-37 Clear Config

3. Click  to clear the settings.

5.4.8 CONFIGURING SMART TRACKING

Purpose:

Smart tracking utilizes motion detection to automatically track objects for a pre-defined period of time using the camera's PTZ functionality.

Steps:

1. Enter the Smart Tracking settings interface: **Configuration > PTZ > Smart Tracking**

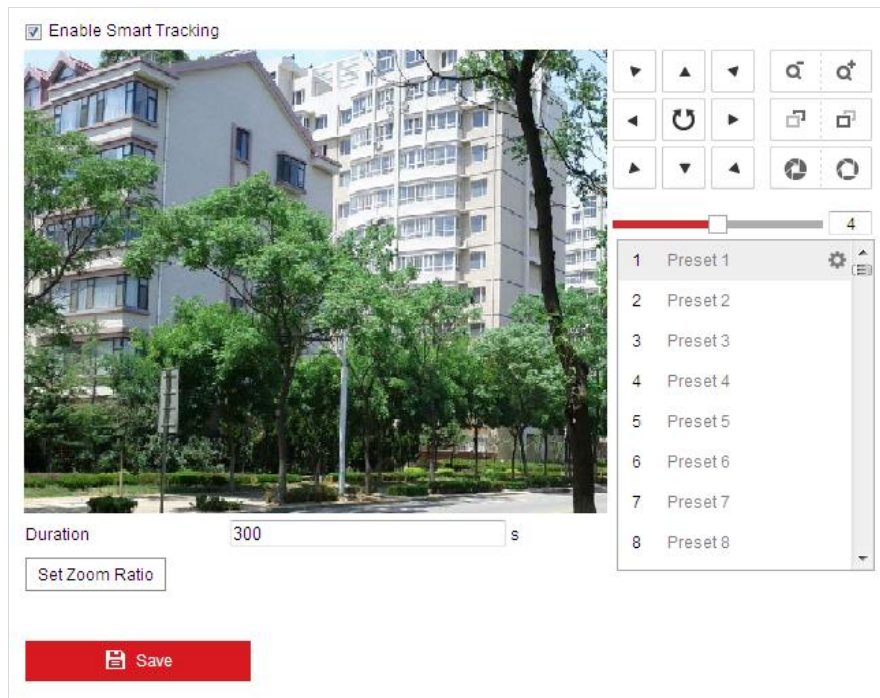


Figure 5-38 Configure Smart Tracking

2. Toggle the **Enable Smart Tracking** check box to enable the smart tracking function.
3. Click the PTZ buttons to select an object.
4. Click **Set Zoom Ratio** to set the current zoom ratio as the tracking zoom ratio.
5. Set the tracking duration. The speed dome stops tracking when the duration time is up. The duration ranges from 0 to 300 seconds.


NOTE:

- Setting the duration to 0 will cause the smart tracking to continuously track detected objects.
- This function varies depending on different camera models.

6. Click  **Save** to clear the settings.

5.4.9 PRIORITIZE PTZ

Steps:

1. Enter the Prioritize PTZ interface: Configuration > PTZ > Prioritize PTZ.
2. Select Network or RS-485 from the dropdown list
3. Set the delay time (Range 2-200s).
4. Click  **Save** to save the settings.

5.4.10 POSITION SETTINGS

Purpose:

The user can set the camera's directional compass and position information in this interface.

Steps:

1. Enter the Position Settings interface: **Configuration > PTZ > Position Settings**

Compass

PT ModeManualSet as NorthPoint to North

GPS

Longitude-Latitude ModeManual

LongitudeEast0° 0~1790' 0~590.00" 0.00~59.99

LatitudeNorth0° 0~890' 0~590.00" 0.00~59.99

Figure 5-39 Position Settings

- 2. Manually find the north position for the speed dome in Live View interface, and click **Set at North** to set the north direction.
- 3. After the speed dome changes directions, click **Point to North** to return the speed dome to the north facing position.
- 4. If desired, manually set GPS information including longitude and latitude.
- 5. Click

Save

 to save the settings.

6 Camera Configuration

6.1 Configuring Network Settings

NOTE: Functions and settings configurations 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 the 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.

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 1280 to 1500.
- 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.

- DNS server settings are required for some applications (e.g., sending email). Be sure to properly configure the **Preferred DNS Server** and **Alternate DNS server** settings.

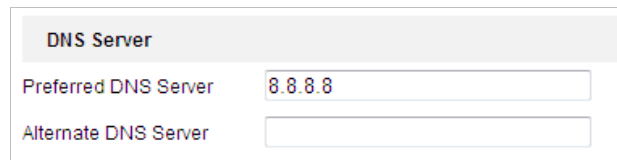


Figure 6-2 DNS Server Settings

NOTE: The network 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 Dynamic DNS (DDNS) for network access.

Before you start:

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



Warning:

- 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. Toggle the **Enable DDNS** checkbox to enable this feature.
3. Select **DDNS Type**. Two DDNS types are available: 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 number of the 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:

- Enter Server Address of NO-IP.
- In the **Domain** text field, enter the domain name obtained from the NO-IP website.
- Enter the **Port** of the NO-IP server.
- Enter the **User Name** and **Password** registered on the NO-IP website.
- Click  to save the settings.

Configuring PPPoE Settings

Purpose:

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

Steps:

- Enter the PPPoE settings interface: Configuration > Network > Basic Settings > PPPoE

Figure 6-4 PPPoE Settings

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

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



Warning:

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

4. Click  to save and exit the interface.

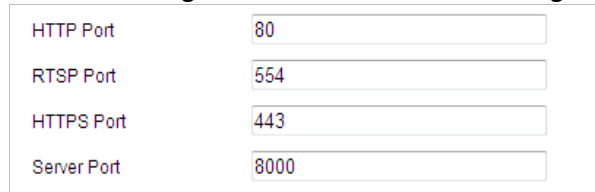
Configuring Port Settings

Purpose:

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

Steps:

1. Enter the Port settings interface: **Configuration > Network > Basic Settings > Port**



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

Figure 6-5 Port Settings

2. Set the HTTP port, RTSP port 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  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 for home and corporate environments.

With the function enabled, individual port configuration is not required and the camera is connected to the Wide Area Network via router.

Steps:

1. Enter the UPnP™ settings interface: **Configuration > Network > Basic Settings > NAT**
2. Toggle the checkbox to enable the UPnP™ function.

NOTE: The user can edit the Friendly Name of the camera. This name can be detected by corresponding devices, such as a router.

3. Set the port mapping mode:

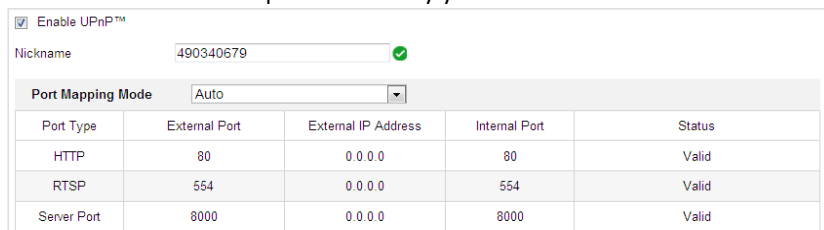
To port mapping with the default port numbers:

Choose **Port Mapping Mode** Auto

To port mapping with the customized port numbers:

Choose **Port Mapping Mode** Manual

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



☒ Enable UPnP™

Nickname: 490340679

Port Mapping Mode: Auto

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

Figure 6-6 Port Mapping Mode

4. Click  to save the settings.

6.1.2 ADVANCED SETTINGS

Configuring SNMP Settings

Purpose:

The user can use SNMP to get camera status, parameters and other related information.

Before you start:

Before setting the SNMP, use the SNMP software and 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

The screenshot displays the 'SNMP v1/v2' and 'SNMP v3' configuration sections. The 'SNMP v1/v2' section includes checkboxes for 'Enable SNMPv1' and 'Enable SNMP v2c', and text input fields for 'Read SNMP Community' (public), 'Write SNMP Community' (private), 'Trap Address', 'Trap Port' (162), and 'Trap Community' (public). The 'SNMP v3' section includes a checkbox for 'Enable SNMPv3', and text input fields for 'Read UserName', 'Security Level' (no auth, no priv), 'Authentication Algorithm' (MD5, SHA), 'Authentication Password', 'Private-key Algorithm' (DES, AES), 'Private-key password', 'Write UserName', 'Security Level' (no auth, no priv), 'Authentication Algorithm' (MD5, SHA), 'Authentication Password', 'Private-key Algorithm' (DES, AES), and 'Private-key password'. The 'SNMP Other Settings' section includes a text input field for 'SNMP Port' (161).

Figure 6-7 SNMP Settings

2. Toggle 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:

The user 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**

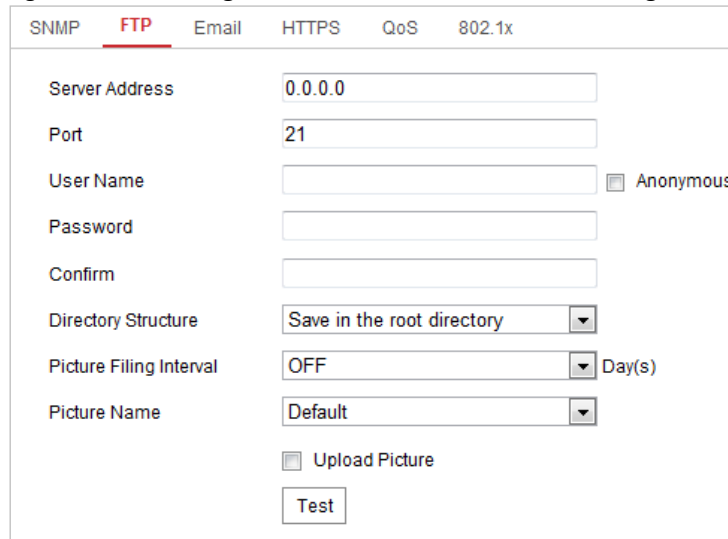


Figure 6-8 FTP Settings

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

NOTE: The server address supports both domain name and IP address formats.



Warning:

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

Setting the directory in FTP server for saving files:

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

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

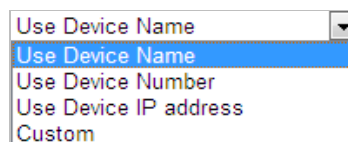


Figure 6-9 Parent Directory

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

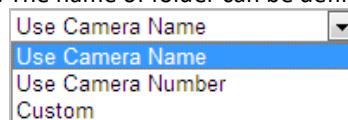



Figure 6-10 Child Directory

- **Upload type:** To enable uploading the captured picture to the FTP server.
3. Click  to save the settings.
 4. The user 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:

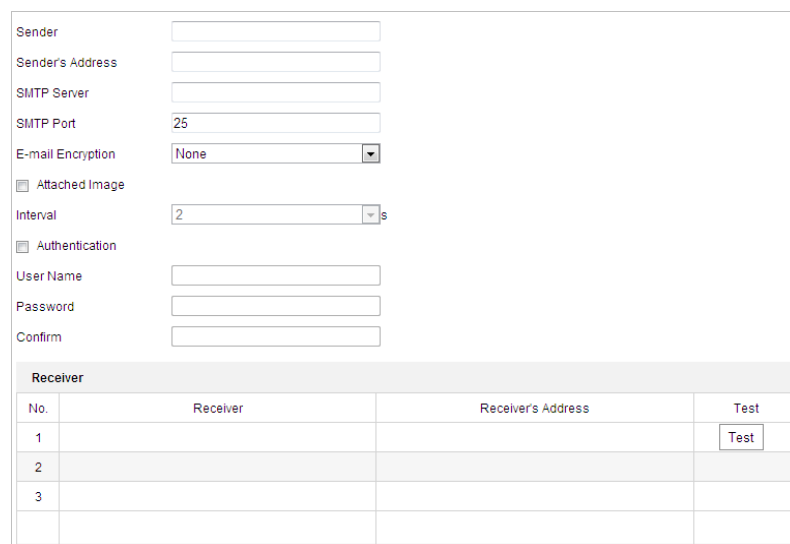
The system can be configured to send an Email notification to all designated receivers if an alarm event is detected, e.g., motion detection event, video loss, video-tampering, etc.

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:
 - f. Configuration > Network > Advanced Settings > Email



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

Figure 6-11 Email Settings

2. Configure the following settings:
 - g. **Sender:** The name of the email sender.
 - h. **Sender's Address:** The email address of the sender.
 - i. **SMTP Server:** The SMTP Server IP address or host name (e.g., smtp.263xmail.com).
 - j. **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 to function. When it is not supported by the email server and the Enable STARTTLS checkbox has been toggled on, the email will not be encrypted.

- ▶ **Attached Image:** Toggle the **Attached Image** checkbox 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.



Warning:

- 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.
 - a. **Receiver:** Select the receiver to which the email is sent. Up to 2 receivers can be configured.
 - b. **Receiver:** The name of the user to be notified.
 - c. **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 Platform Settings

Purpose:

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

NOTE: This function varies depending on different speed dome models.

Steps:

1. Enter the Platform settings interface: Configuration > Network > Advanced Settings > Platform Access
2. Toggle the **Enable** checkbox to enable the platform access function of the device.
3. Select the Platform Access Mode.
4. The user can use the default server address. Alternately, toggle the **Custom** checkbox on the right and input a desired server address.
5. Click  **Save** to save the settings.
 - a. Guarding Vision is an application for mobile devices. With the App, you can view live image of the camera, receive alarm notification and so on.

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.

**Warning:**

- 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

- a) Select **Create Self-signed Certificate**.
- b) Click **Create** to launch the following dialog box.

Figure 6-13 Create Self-signed Certificate

- c) Enter the country, host name/IP, validity and other information.
- d) Click **OK** to save the settings.

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

- a) Select **Signed certificate is available** and start the installation directly.
- b) Click **Browse** to upload the available certificate.
- c) Click **Install** button to install the certificate.
- d) Click **OK** to save the settings.

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

- a) Select **Create certificate request first** and continue the installation.
 - b) Click **Create** to create the certificate request, and enter the required information.
 - c) Download the certificate request and submit it to the trusted certificate authority for signature.
 - d) After receiving the signed valid certificate, import the certificate to the device.
 - e) Click **OK** to save the settings.
3. Certificate information will be available after you successfully create and install the certificate.

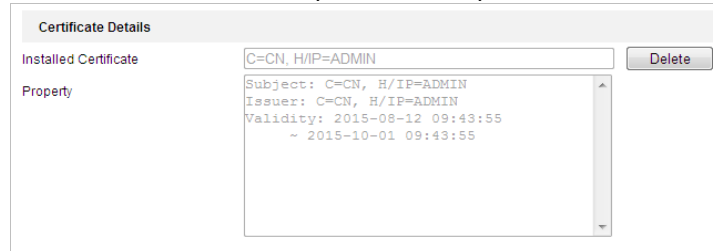


Figure 6-14 Installed Certificate Property

- 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:

Configuring QoS (Quality of Service) settings can help solve network delay and network congestion by configuring data transfer priority.

Steps:

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

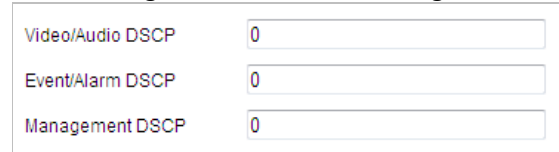



Figure 6-15 QoS Settings

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 larger the DSCP value, the higher its priority will be.
3. Click  **Save** to save the settings.

- NOTE:**
- Make sure that you enable the QoS function for your network device (such as a router).
 - A reboot is required for 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 standard. It enhances the security level of a LAN. When devices connect to this network with IEEE 802.1X standard, authentication is needed. If the authentication fails, the devices cannot connect to the network.

The protected LAN with 802.1X standard is shown in Figure 6-16

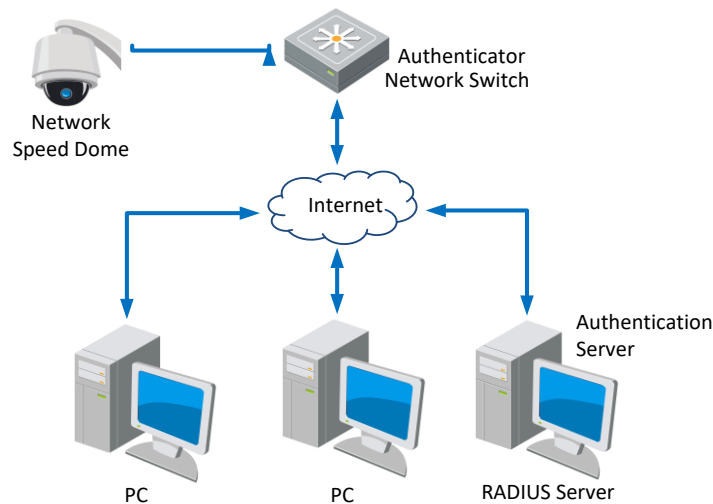


Figure 6-16 Protected LAN

- 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.

**Warning:**

- 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**

<input type="checkbox"/> Enable IEEE 802.1X	
Protocol	EAP-MD5
EAPOL version	1
User Name	
Password	
Confirm	

Figure 6-17 802.1X Settings

3. Toggle 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 will reboot when you save the settings.

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

Integration Protocol

Purpose:

If you need to access the camera through a the third party platform, you can enable ****-CGI function. If you need to access to the device through ONVIF protocol, you can configure ONVIF users 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**

☐ Enable CGI


CGI Authentica...

☐ Enable ONVIF

User List

No.	User Name	Level

Figure 6-18 Integration Protocol Settings

2. Toggle the **Enable ****-CGI** checkbox and then select the authentication from the dropdown list. Access to the camera through a third party platform can then be granted.
3. Toggle 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. The user can set the user as media user, operator, or 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**

Stream Type	Main Stream(Normal)	
Video Type	Video&Audio	
Resolution	2048*1536	
Bitrate Type	Variable	
Video Quality	Medium	
Frame Rate	30	fps
Max. Bitrate	6045	Kbps
Video Encoding	H.264	
H.264+	OFF	
Profile	Main Profile	
I Frame Interval	19	
SVC	OFF	
Smoothing	<input type="range"/> 51 [Clear<->Smooth]	

Figure 6-19 Configure Video Settings

- Set 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 in environments with ample bandwidth. Sub-stream can be used for live viewing when bandwidth is limited. Refer to the **Section 4.1 Error! Reference source not found.** for info on switching between main stream and sub-stream for live viewing.
- The user can customize the following parameters for the selected stream.


NOTE: Parameters and related functionality vary depending on different camera models.

- **Video Type:** Select the stream type: 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 describes 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, however, higher bandwidth is required.
- **Video Encoding:** Select **Video Encoding** from the dropdown list for different stream type.
- **H.264+/H.265+:** Set the compression type to ON or OFF.
 - ▶ **H.264+:** If you set the main stream as the stream type, and H.264 as the video encoding, H.264+ will be 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, H.265+ will be available. H.265+ is an improved compression coding technology based on H.265. By enabling H.265+, users can estimate the HDD consumption by its maximum average bitrate. Compared to H.265, H.265+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

NOTE:

- ▶ H.265+/H.265 functionality varies depending on different camera models.
- ▶ You need to reboot the camera if you want to turn on or turn off the

H.264+/H.265+ compression. If you switch from H.264+ to H.265+ directly, and vice versa, a reboot is not required by the system

- **Max. Average Bitrate:** When you set a maximum bitrate, its corresponding recommended maximum average bitrate will be shown in the Max. Average Bitrate box. You can also set the maximum average bitrate manually from 32 Kbps to the value of the set maximum bitrate.
 - **Profile:** Basic Profile, Main Profile and High Profile 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:** Configure the smoothness, or fluency of the stream. The higher smoothing value, the better fluency of the stream, though, the video quality may not be satisfactory. The lower the smoothing value, the higher quality of the stream, though video may appear choppy and lack fluency.
4. Click  to save the settings.

6.2.2 CUSTOM VIDEO

Purpose:

You can set up to 5 additional video streams if required. For custom video streams, you can live view them, but cannot record or playback them.

- NOTE:**
- ▶ Custom video function requires the support of the camera.
 - ▶ After a camera restore action (not restore to default setting), quantity of custom video streams and their names are kept, but the related parameters are restored.

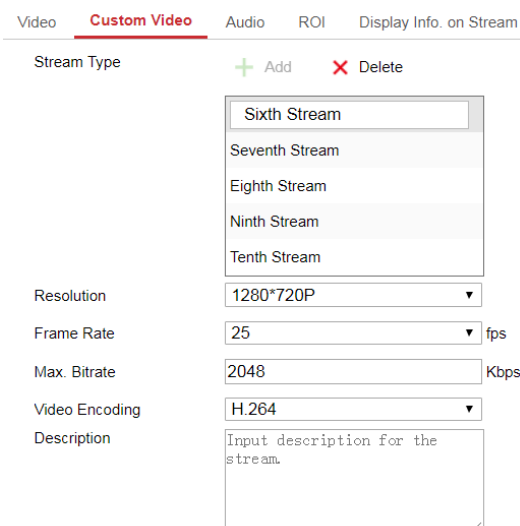



Figure 6-20 Custom Video Settings

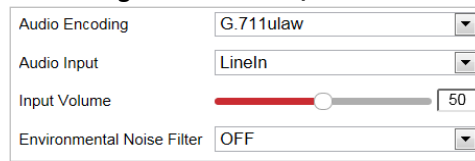
Steps:

1. Click  to add a stream.
2. Change the stream name if needed.
 - ▶ **Note:** Up to 32 letters and symbols (except &, <, >, ', or ") are allowed for the stream name.
3. Customize the stream parameters (resolution, frame rate, max. bitrate, video encoding). For more on these parameters, see Section 6.2.1.
4. (Optional) Add stream description if needed.
5. Save the settings.

6.2.3 CONFIGURING AUDIO SETTINGS

Steps:

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



Audio Encoding	G.711ulaw
Audio Input	LineIn
Input Volume	50
Environmental Noise Filter	OFF

Figure 6-21 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 value is set 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:** Slide 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 this function. It is recommended to enable the function when the sampling rate is lower than 32 kHz.

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

6.2.4 CONFIGURING ROI SETTINGS

Purpose:

ROI (Region of Interest) encoding is used to enhance the quality of images for a specified region. There are two different ROI methods: **Fixed Region** and **Dynamic Region**.

When **Fixed Region** is enabled, image quality of the ROI area will be enhanced, and image quality of other areas will be reduced.

When **Dynamic Region** is enabled, image quality of tracking target will be enhanced.

NOTE: ROI function varies depending on different camera models.

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



Figure 6-22 Region of Interest (1)

Figure 6-23 Region of Interest (2)

► ROI for Fixed Region

Steps:

- Toggle the **Enable** checkbox to enable the **Fixed Region** function.
- Select a stream type. The user can set the ROI function for main stream, sub-stream or third stream.
- Click **Draw Area** and then drag the mouse to draw a red frame in the live view image. Click **Clear** to clear it.

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

- Select the Region No. from the dropdown list.
- Adjust the ROI level from 1 to 6. The higher the value, the better the image quality in the ROI region.
- Enter a Region Name.

► ROI for Dynamic Region

- Toggle the **Enable Face Tracking** checkbox to enable face tracking, and the captured face picture is set as region of interest. Adjust the **ROI level** from 1 to 6.
- Toggle the **Enable Target Tracking** checkbox to enable target tracking with the target set as region of interest. Adjust the ROI level from 1 to 6.
- Click **Save** to save the settings.

6.2.5 DISPLAY INFO. ON STREAM

Toggle the **Enable Dual-VCA** checkbox, Object information will be marked in the video stream. The user can then set rules on the connected rear-end device to detect the events including line crossing, intrusion, etc.

Figure 6-24 Display Info on Stream Settings

6.2.6 CONFIGURING TARGET CROPPING

Purpose:

You can specify a target area on the live video, and then the specified video area can be displayed via the third stream in certain resolution, providing more details of the target area if needed.



NOTE: Target cropping function varies according to different camera models.

Steps

1. Enter the **Target Cropping** settings interface.
2. Check **Enable Target Cropping** checkbox to enable the function.
3. Set Third Stream as the stream type.
4. Select the cropping resolution for the video display of target area. A red rectangle
5. is displayed on the live video to mark the target area, and you can click-and-drag
6. the rectangle to locate the target area as desired.
7. 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:

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

NOTE:

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

Steps:

1. Enter the Display Settings interface: **Configuration > Image> Display Settings**
2. Select the **Scene** from the dropdown list, each containing different predefined image parameters.
3. Set the image parameters of the speed dome.

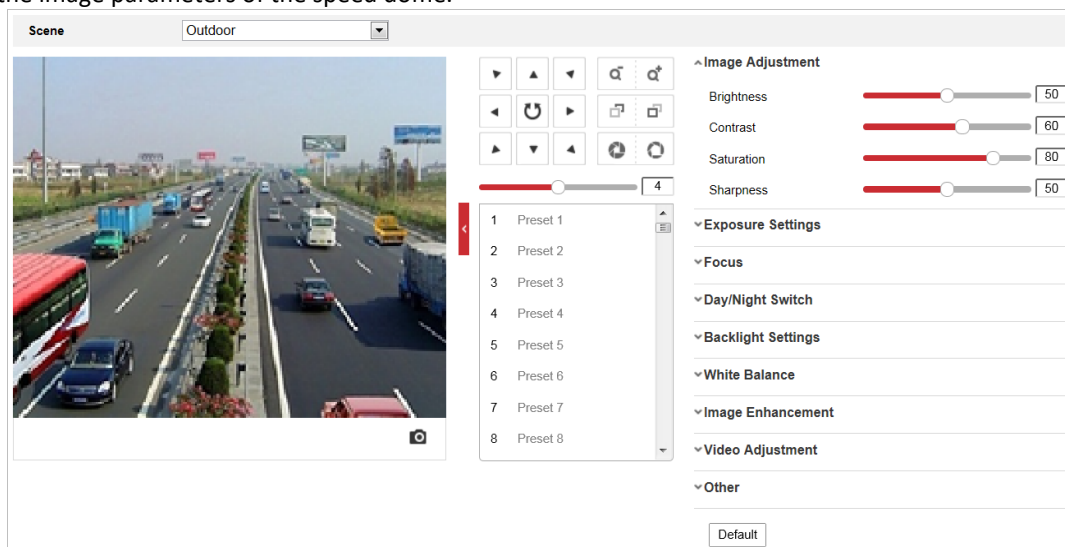


Figure 6-25 Display Settings

Image Adjustment

■ Brightness

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

■ Contrast

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

■ Saturation

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

■ Sharpness

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

Exposure Settings

■ Exposure Mode

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

► Auto:

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

► Iris Priority:

In this mode, 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.

The screenshot shows the 'Iris Priority' exposure mode settings. The 'Exposure Mode' dropdown is set to 'Iris Priority'. The 'Exposure Level' is a slider set to 2. The 'Max. Shutter Limit' is set to 1/30 and the 'Min. Shutter Limit' is set to 1/30000. The 'Iris' is set to f1.6. The 'Limit Gain' is a slider set to 94. The 'Slow Shutter' dropdown is set to OFF.

Figure 6-26 Manual Iris

► Shutter Priority:

In this mode, the shutter rate needs to be adjusted manually. The iris and gain values will be adjusted automatically according to the brightness of the environment.

The screenshot shows the 'Shutter Priority' exposure mode settings. The 'Exposure Mode' dropdown is set to 'Shutter Priority'. The 'Exposure Level' is a slider set to 2. The 'Max. Iris Limit' is a slider set to 100 and the 'Min. Iris Limit' is a slider set to 0. The 'Shutter' is set to 1/30. The 'Limit Gain' is a slider set to 94. The 'Slow Shutter' dropdown is set to OFF.

Figure 6-27 Manual Shutter

► Manual:

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

The screenshot shows the 'Manual' exposure mode settings. The 'Exposure Mode' dropdown is set to 'Manual'. The 'Iris' is set to f1.6. The 'Shutter' is set to 1/30. The 'Gain' is a slider set to 0. The 'Limit Gain' is a slider set to 94. The 'Slow Shutter' dropdown is set to OFF.

Figure 6-28 Manual Mode

■ Limit Gain

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

■ Slow Shutter

This function can be used in underexposed conditions. 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**.

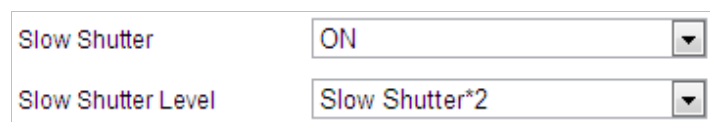




Figure 6-29 Slow Shutter

Focus Settings

■ Focus Mode

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

- ▶ **Auto:** The speed dome focuses automatically at any time according to objects in the scene.
- ▶ **Semi-auto:** The speed dome focuses automatically only once after panning, tilting and zooming.
- ▶ **Manual:** In **Manual** mode, you need to use   on the control panel to focus manually.

■ Min. Focus Distance

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

NOTE: The minimum focus value varies depending on different camera models.

Day/Night Switch

■ Day/Night Switch

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

NOTE: This function varies depending on the models of speed dome.

▶ Auto:

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



Figure 6-30 Auto Mode Sensitivity

▶ Day:

In **Day** mode, the speed dome displays a standard color image. It is used for normal lighting conditions.

▶ Night:

In **Night** mode, the image is black and white. **Night** mode can increase sensor sensitivity in low light conditions to provide a clearer image.

▶ Scheduled-Switch:

In **Schedule** mode, you can set the time schedule for day mode as shown in Figure 6-31. The rest time out of the schedule is for night mode.

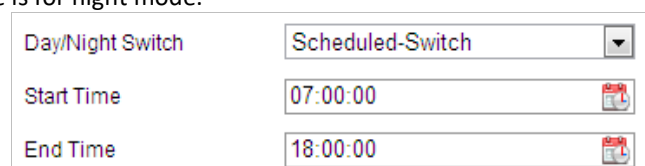


Figure 6-31 Day Night Schedule

Backlight Settings

■ BLC (Back Light Compensation)

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

■ 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.

The user can enable or disable the WDR function as shown in Figure 6-32. The wide dynamic level ranges from 0 to 100.



Figure 6-32 WDR

■ HLC

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

■ White Balance

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

▶ Auto:

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

▶ Manual White Balance:

In **MWB** mode, you can adjust the color temperature manually to meet your own demand as shown in Figure 6-33.

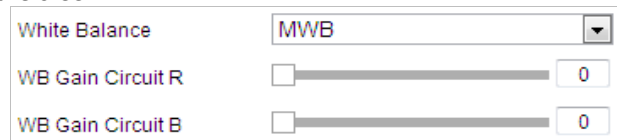


Figure 6-33 Manual White Balance

▶ Outdoor

Select this preset mode when the speed dome is installed in outdoor environment.

▶ Indoor

Select this preset mode when the speed dome is installed in indoor environment.

▶ Fluorescent Lamp

Select this preset mode when there are fluorescent lamps installed near the speed dome.

▶ Sodium Lamp

Select this preset mode when there are sodium lamps installed near the speed dome.

▶ Auto-Tracking

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

Image Enhancement

■ 3D Digital Noise Reduction

The user can set **Digital Noise Reduction** function to **Normal** and adjust the **Noise Reduction Level** as shown in Figure 6-34. The level ranges from 0 to 100.

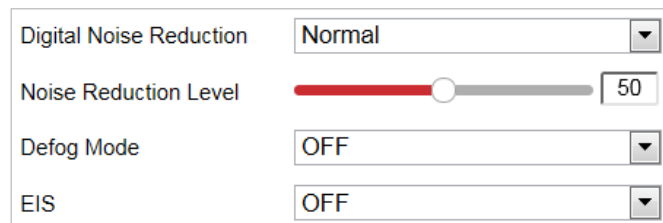


Figure 6-34 3D Digital Noise Reduction

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.

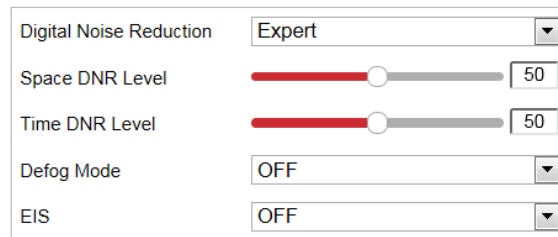


Figure 6-35 Expert Mode

■ Defog Mode

The user can set the **Defog Mode** to ON or OFF as required by the environment.

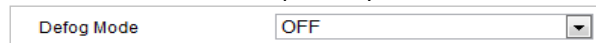


Figure 6-36 Defog Mode

■ EIS (Electronic Image Stabilization)

The user can set the **EIS** to ON or OFF as required.

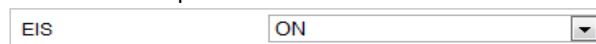


Figure 6-37 Electronic Image Stabilization

Video Adjustment

NOTE: Functionality may vary depending on different camera models.

■ Mirror

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

■ Video Standard

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

■ Capture Mode

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

Other

NOTE: Functionality and available settings may vary depending on different camera models.

■ Local Output

The user can select the local video output mode. For example, the VX-2V-MD-RIWH features an HDMI cable for use with a public view monitor or other HDMI video display. Local output can be set to *HDMI_1080P60* to actively display video via the HDMI output.

■ Lens Initialization

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

■ Zoom Limit

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

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.

The user can customize the on-screen display of the camera timestamp.

Steps:

1. Enter the OSD settings interface: **Configuration > Image > OSD Settings**

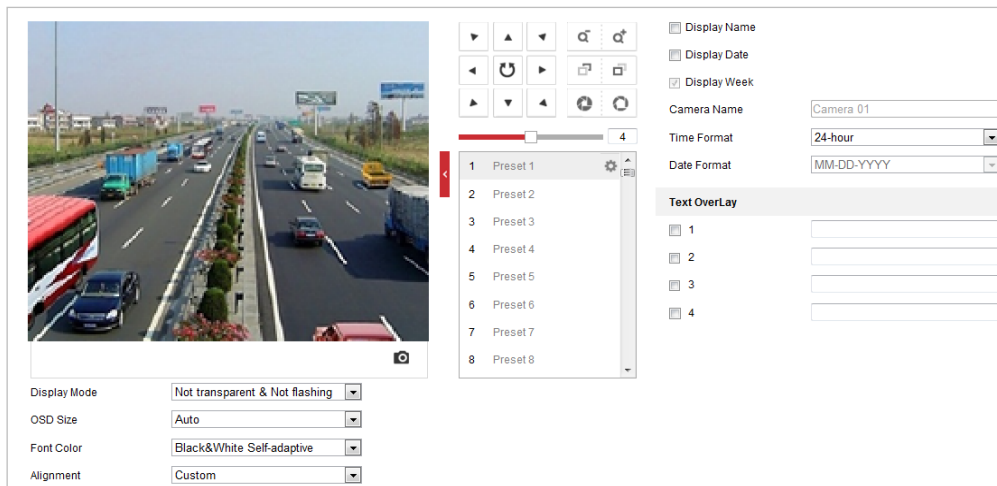


Figure 6-38 OSD Settings

2. Toggle the corresponding checkbox to enable the on-screen display of the camera name, date or week if required.
3. Edit the camera name as displayed in OSD in the **Camera Name** field.
4. Select from the dropdown list to set the time format, date format, display mode, OSD size and Font color.
5. Use the mouse to drag the text frame **IPdome** in the live view window to adjust the OSD position.



Figure 6-39 Adjust OSD Location


6. Click  Save to activate above settings.

6.3.3 CONFIGURING TEXT OVERLAY SETTINGS

Purpose:

The user can customize the text overlay in this interface.

Steps:

1. Enter the Text Overlay settings interface: **Configuration > Image > OSD Settings**
2. Toggle the checkbox in front of the textbox to enable 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  to save the settings.

6.3.4 CONFIGURING IMAGE PARAMETERS SWITCH

NOTE: This function varies depending on different camera models.

Purpose:

The user can configure **Link to Preset** or **Scheduled-Switch** in this interface.

- **Link to Preset:** Set the time period and linked scene for the preset and toggle the corresponding checkbox to go to the linked scene in the configured time period.
- **Scheduled-Switch:** Set the time period and linked scene and it will go to the linked scene in the configured time period when you toggle the corresponding checkbox.

Steps:

1. Enter the Image Parameters Switch interface: **Configuration > Image > Image Parameters Switch**
2. Toggle the checkbox of **Link to Preset** or **Scheduled-Switch** to enable the function. (Only one function can be enabled at a time.)
3. When you enable **Link to Preset**, select one preset from the dropdown list, toggle the corresponding checkbox, set the time period and the linked scene for the selected preset. (Up to 4 periods can be configured for one preset.)

Figure 6-40 Link to Preset

Figure 6-41 Linked Scene

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

Figure 6-42 Schedule-Switch

5. Click  to save the settings.
- NOTE:** These two functions are not enabled by default.

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 camera information 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.

Device Name	<input type="text"/>
Device No.	<input type="text"/>
Model	<input type="text"/>
Serial No.	<input type="text"/>
Firmware Version	<input type="text"/>
Encoding Version	<input type="text"/>
Web Version	<input type="text"/>
Plugin Version	<input type="text"/>
Number of Channels	<input type="text"/>
Number of HDDs	<input type="text"/>
Number of Alarm Input	<input type="text"/>
Number of Alarm Output	<input type="text"/>
Firmware Version Property	<input type="text"/>

Figure 6-43 Device Information

Time Settings

Purpose:

Follow the instructions in this section to configure the timestamp to 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.

Steps:

1. Enter the Time Settings interface: **Configuration > System > System Settings > Time Settings**


Figure 6-44 Time Settings

Configuring Time Synchronization by NTP Server

Steps:

- (1) Toggle 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 synchronization interval. It can be set from 1 to 10080 minutes.



Figure 6-45 Time Sync by NTP Server

- Click  to make sure that the NTP server is connected.

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

Configuring Time Synchronization Manually

Steps:

- (1) Toggle the **Manual Time Sync** radio button.
- (2) Click  to set the system time from the pop-up calendar.
- (3) Click  to save the settings.

NOTE: The user can also toggle the **Sync with local time** checkbox to synchronize the time of the camera with the time of your computer.

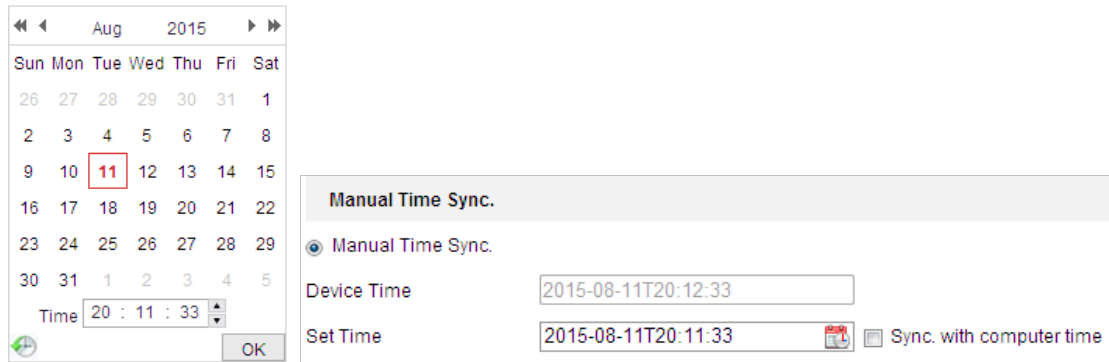


Figure 6-46 Time Sync Manually

Select the Time Zone

- c. **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.
- d. From the **Time Zone** dropdown menu as shown in Figure 6-47, select the Time Zone in which the the camera resides.

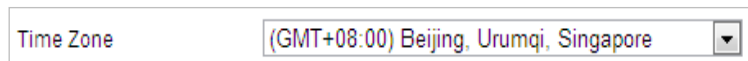


Figure 6-47 Time Zone Settings

Configuring DST (Daylight Saving Time)

- e. **Purpose:** Daylight Savings 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.
- f. If your country observes Daylight Savings Time, turn this function on. The time will be adjusted automatically on DST.

Steps:

1. Enter the DST interface: Configuration > Advanced Configuration > System > DST

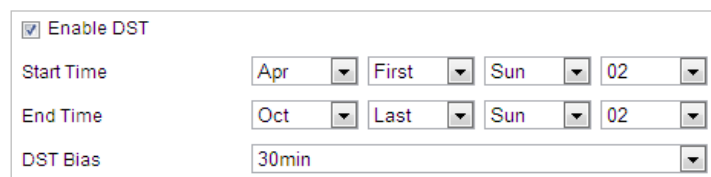



Figure 6-48 DST Settings

2. Toggle 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.

NOTE: RS-232 function varies depending on different speed dome models.

Steps:

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

Baud Rate	115200	▼
Data Bit	8	▼
Stop Bit	1	▼
Parity	None	▼
Flow Ctrl	None	▼
Usage	Transparent Channel	▼

Figure 6-49 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 the RS-232 port, the RS-232 settings should be identical to the parameters you configured here.

3. Click  to save the settings.

Configuring RS-485

Purpose:

The RS-485 serial port is used to control the camera's PTZ module. The camera's PTZ parameters should be configured before controlling the PTZ unit.

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

Steps:

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

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

Figure 6-50 RS-485 Settings

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

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

About

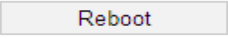
Click **View License**, you can check Open Source Software Licenses.

6.4.2 MAINTENANCE

Upgrade & Maintenance

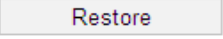
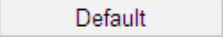
Rebooting the Camera

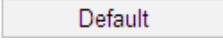
Steps:

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

Restoring Default Settings

Steps:

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

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

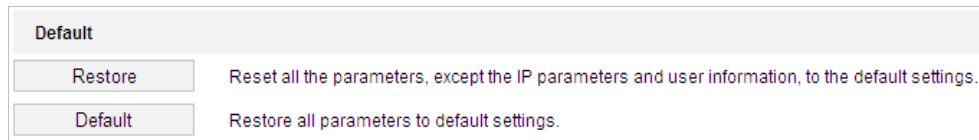


Figure 6-51 Restore Default Settings

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 save path to save the configuration file to 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 on your computer to upgrade the device.
 - ▶ **Firmware Directory:** Define the location of the firmware directory where the firmware is located. 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 a 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. The user can also export the log files on-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 6-52 Log Searching Interface

- Set the log search conditions to specify the search, including the Major Type, Minor Type, Start Time and End Time as shown in Figure 6-52.
- Click **Search** to search log files. The matched log files will be displayed on the **Log** interface.
- To export the log files, click **Save Log** to save the log files to your computer.

System Service

Steps:

- Enter the System Service interface: Configuration > System > Maintenance > System Service
- Toggle the checkbox to enable supplement light function if the device supports this function.
- 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, the number cannot exceed 10 live view connections.

Figure 6-53 Live View Connection Settings

- Click **Save** button to activate the settings.

6.4.3 SECURITY

Configuring Authentication Security

Purpose:

From this interface, you can specifically secure the stream data of live view.

Steps:

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

The screenshot shows the 'IP Address Filter' configuration window. At the top, there is a checkbox labeled 'Enable IP Address Filter' which is checked. Below it is a dropdown menu for 'IP Address Filter Type' with 'Forbidden' selected. A table with two columns, 'No.' and 'IP', is present. To the right of the table are buttons for 'Add', 'Modify', and 'Delete'. At the bottom of the window is a red 'Save' button.

Figure 6-54 IP Address Filter

2. Toggle the checkbox of **Enable IP Address Filter**.
3. Select the type of IP Address Filter in the dropdown list: Available filters include Forbidden and Allowed.
4. Set the IP Address Filter list.

► Add an IP Address

Steps:

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

The screenshot shows the 'Add IP Address' dialog box. It has a title bar with the text 'Add IP Address' and a close button (X). The main area contains a text input field labeled 'IP Address' with the value '172.6.23.2' and a green checkmark icon to its right. At the bottom, there are two buttons: 'OK' and 'Cancel'.

Figure 6-55 Add an IP

- c. Click **OK** to finish adding.

► Modify an IP Address

Steps:

- a. Left-click an IP address from filter list and click **Modify**.
- b. Modify the IP address in the text field.

The screenshot shows the 'Modify IP Address' dialog box. It has a title bar with the text 'Modify IP Address' and a close button (X). The main area contains a text input field labeled 'IP Address' with the value '172.6.23.2'. At the bottom, there are two buttons: 'OK' and 'Cancel'.

Figure 6-56 Modify an IP

- c. Click **OK** to finish modifying.

► Delete an IP Address

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


▶ **Delete all IP Addresses**

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

5. Click  to save the settings.

Configure Security Service Settings

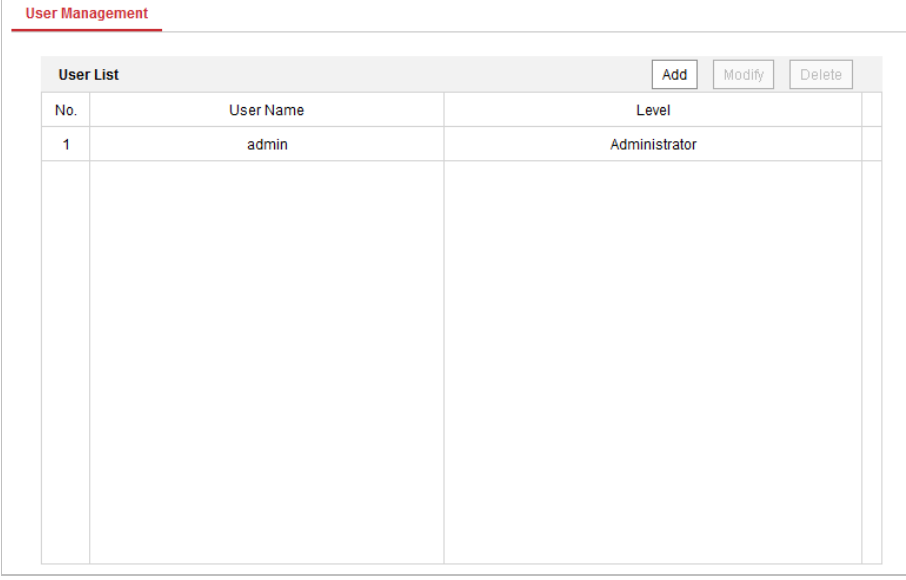
Steps:

1. Enter the Security Service interface:
Configuration > System > Security > Security Service
2. Toggle 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  to save the settings.

6.4.4 USER MANAGEMENT

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

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




User Management		
User List		
No.	User Name	Level
1	admin	Administrator

Figure 6-57 User Information

Add a User

Steps:

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



Warning:

- 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. Available profiles include **Operator** or **User**.

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

Figure 6-58 Add a User

Modify a User

Steps:

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

Modify user

User Name: user1

Level: Operator

Password: •••••

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

Confirm: •••••

☐ Select All



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

OK Cancel

Figure 6-59 Modify a User

Delete a User


Steps:

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

Online Users

Enter the Online Users configuration interface: **Configuration > System > User Management > Online Users**

User Management **Online Users**

User List 

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

Figure 6-60 Online Users

The user 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.