ILB-340-BL-F

ILB-340-BL-V

ILB-340-VD-F

ILB-340-VD-V

Intellio Initio Cameras

User Manual

User Manual

About this Manual

This Manual is applicable to Intellio Initio IP cameras.

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (www.intellio.hu).

Please use this user manual under the guidance of professionals.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED "AS IS", WITH ALL FAULTS AND ERRORS, AND OUR COMPANY MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL OUR COMPANY, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF OUR COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. OUR COMPANY SHALL NOT TAKE ANY RESPONSIBILITES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER

ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, OUR COMPANY WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

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

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

Notice:

If camera fails to synchronize local time with that of the network, you need to set up camera time manually. Visit the camera and enter system setting interface for time setting.

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 PoE according to the IEC60950-1 and Limited Power Source standard.
- To reduce the risk of fire or electrical shock, do not expose this product to rain or moisture.
- The 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. 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 (refer to product

specification for working temperature), dusty or damp environment, and do not expose it to high electromagnetic radiation.

- To avoid heat accumulation, ensure there is good air ventilation to the device.
- Keep the camera away from water and any liquids.
- While shipping, pack the camera in its original, or equivalent packing materials. Or packing the same texture.
- Improper use or replacement of the battery may result in hazard of explosion. Please use the manufacturer recommended battery type.

Notes:

The camera supports 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 sure 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

System Requirement

Operating System

Microsoft Windows 7 and above version

CPU

2.0 GHz or higher

RAM

1G or higher

Display

1024×768 resolution or higher

Web Browser

Internet Explorer 8.0 and above version is recommended

Chapter 1 Network Connection

Note:

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

Before you start:

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

1.1 Setting the Camera over the LAN

Purpose:

To view and configure the camera via a LAN, you need to connect the camera in the same subnet with your computer, and reach the camera via Web Browser or via the Intellio Video System software to search and change the IP of the camera.

1.1.1 Activating the Camera

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

Activation via Web Browser and activation via Intellio Video System software are all supported.

- **Activation via Web Browser**

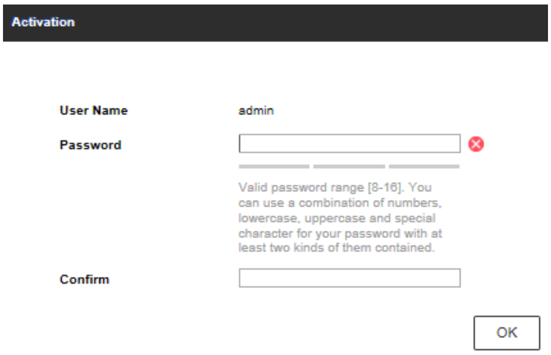
Steps:

1. Power on the camera, and connect the camera to your computer or the switch/router which your computer connects to.

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

Notes:

- The default IP address of the camera is 192.168.1.11.
- The computer and the camera should belong to the same subnet.



Activation

User Name: admin

Password:

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

Confirm:

Figure 1-1 Activation via Web Browser

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

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

4. Confirm the password.

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

❖ Activation via Intellio Video System software

For activation via Intellio Video System software, refer to the Installation manual of

Intellio Video System software.

1.1.2 Modifying the IP Address

Purpose:

To view and configure the camera via LAN (Local Area Network), you need to connect the camera in the same subnet with your PC.

Use the Web Browser or Intellio Video System software to search and change the IP address of the device. We take modifying the IP Address via Web Browser as an example to introduce the IP address modification.

For IP address modification via Intellio Video System software, refer to the Installation manual of Intellio Video System software.

Steps:

1. Open the web browser.
2. In the browser address bar, input the IP address of the camera, and press the **Enter** key to enter the login interface.

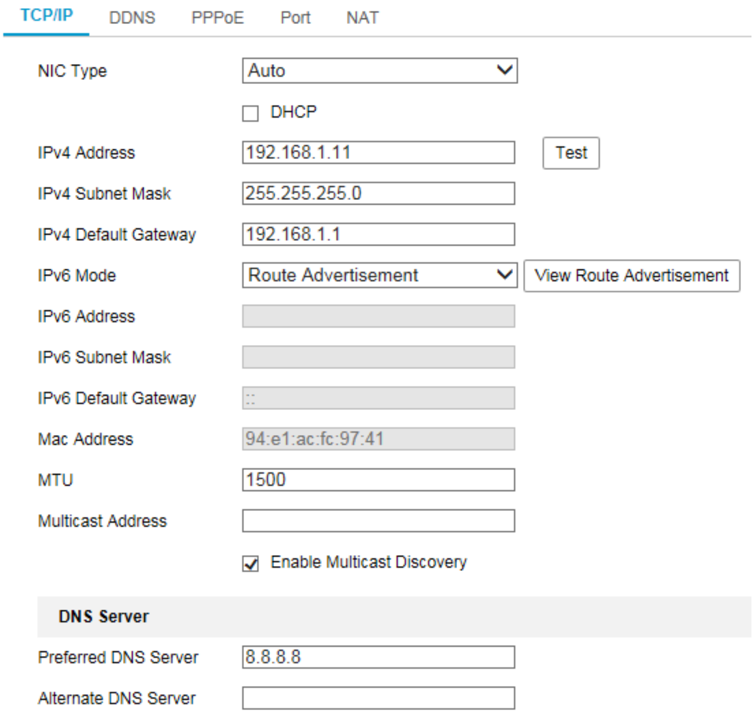
Note: The default IP address is 192.168.1.11. You are recommended to change the IP address to the same subnet with your computer.

3. Input the user name and password.

Note: The admin user should configure the device accounts and user/operator permissions properly. Delete the unnecessary accounts and user/operator permissions. The device IP address gets locked if the admin user performs 7 failed password attempts (5 attempts for the user/operator).

4. Click **Login**.
5. Select the Configuration / Network / Basic Settings menu to change the IP address of the camera.

Note: Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of enable DHCP.



NIC Type	Auto
	□ DHCP
IPv4 Address	192.168.1.11
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	192.168.1.1
IPv6 Mode	Route Advertisement
IPv6 Address	
IPv6 Subnet Mask	
IPv6 Default Gateway	::
Mac Address	94:e1:ac:fc:97:41
MTU	1500
Multicast Address	
	☑ Enable Multicast Discovery
Preferred DNS Server	8.8.8.8
Alternate DNS Server	

1.1.3 (Optional) Setting Security Question

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

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

1.2 Setting the Camera over the WAN

Purpose:

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

1.2.1 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 camera via a router or connect it to the WAN directly.

- **Connecting the camera via a router**

Steps:

1. Connect the camera to the router.
2. Assign a LAN IP address, the subnet mask and the gateway. Refer to ***Section 2.1.2 Modifying the IP Address*** for detailed IP address configuration of the camera.
3. Save the static IP in the router.
4. Set port mapping, e.g., 80, 8000, and 554 ports. The steps for port mapping vary according to the different routers. Please call the router manufacturer for assistance with port mapping.
5. Visit the camera through a web browser or the Intellio Video System software over the internet.

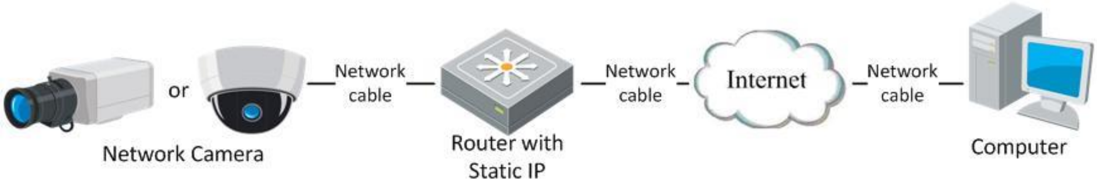


Figure 1-2 Accessing the Camera through Router with Static IP

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

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

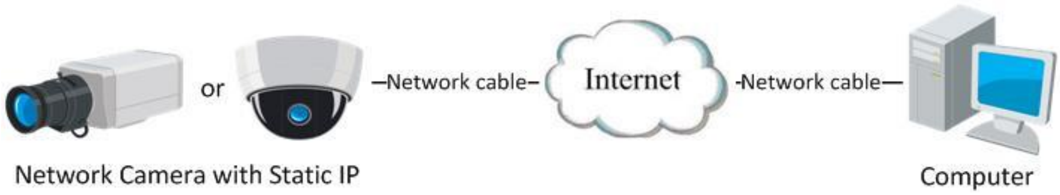


Figure 1-3 Accessing the Camera with Static IP Directly

1.2.2 Dynamic IP Connection

Before you start:

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

- **Connecting the camera via a router**

Steps:

1. Connect the camera to the router.
2. In the camera, assign a LAN IP address, the subnet mask and the gateway. Refer to ***Section 2.1.2 Modifying the IP Address*** for detailed IP address configuration of the camera.
3. In the router, set the PPPoE user name, password and confirm the password.
4. Set port mapping. E.g. 80, 8000, and 554 ports. The steps for port mapping vary depending on different routers. Please call the router manufacturer for assistance with port mapping.
5. Apply a domain name from a domain name provider.
6. Configure the DDNS settings in the setting interface of the router.
7. Visit the camera via the applied domain name.

- **Connecting the camera via a modem**

Purpose:

The 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 camera. Refer to ***Section 5.1.3 PPPoE Settings*** for detailed configuration.

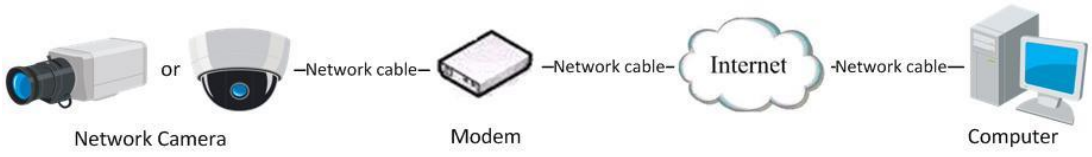


Figure 1-4 Accessing the Camera with Dynamic IP

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 a DDNS provider (E.g. DynDns.com). Please follow the steps below for normal domain name resolution and private domain name resolution to solve the problem.

♦ Normal Domain Name Resolution

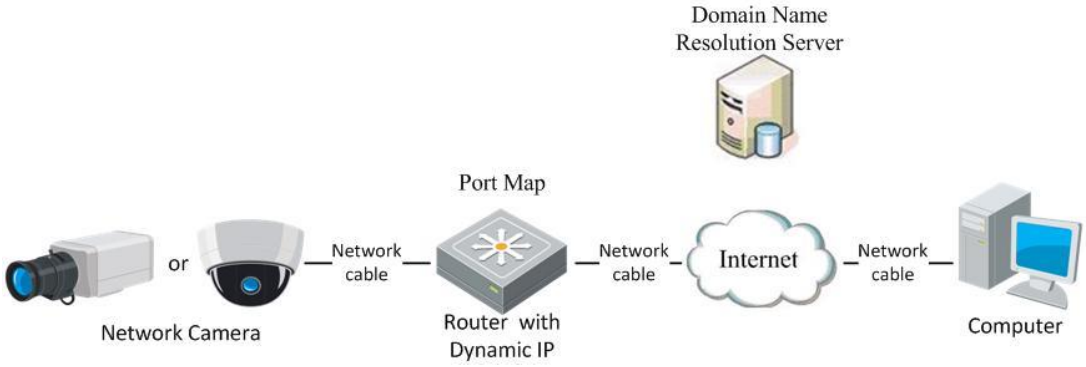


Figure 1-5 Normal Domain Name Resolution

Steps:

1. Apply a domain name from a domain name provider.
2. Configure the DDNS settings in the **DDNS Settings** interface of the camera. Refer to ***Section 5.1.2 DDNS Settings*** for detailed configuration.
3. Visit the camera via the applied domain name.

Chapter 2 Access to the Camera

2.1 Accessing by Web Browsers

Steps:

1. Open the web browser.
2. In the browser address bar, input the IP address of the camera, and press the **Enter** key to enter the login interface.

   Note: The default IP address is 192.168.1.11. You are recommended to change the IP address to the same subnet with your computer.
3. Input the user name and password and click **Login**.

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

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

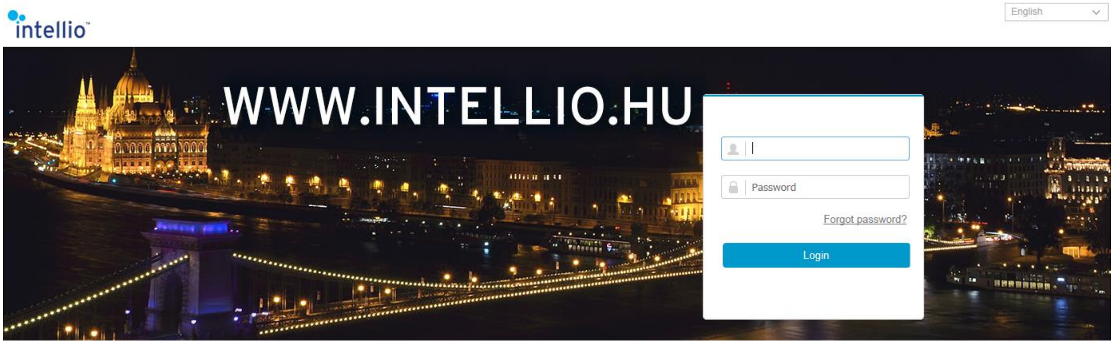


Figure 2-1 Login Interface

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

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

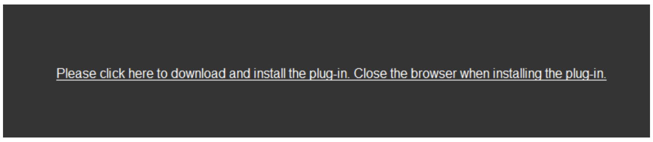

Please click here to download and install the plug-in. Close the browser when installing the plug-in.

Figure 4-1 Download Plug-in

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

Note: If you are using Google Chrome 45 and its above version or Mozilla Firefox 52 and its above version, plug-in installation is not required. But **Picture** and **Playback** functions are hidden. To use mentioned function via web browser, change to their lower version, or change to **Internet Explorer 8.0 and above version**.

Chapter 3 Live View

3.1 Live View Page

Purpose:

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

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

Descriptions of the live view page:

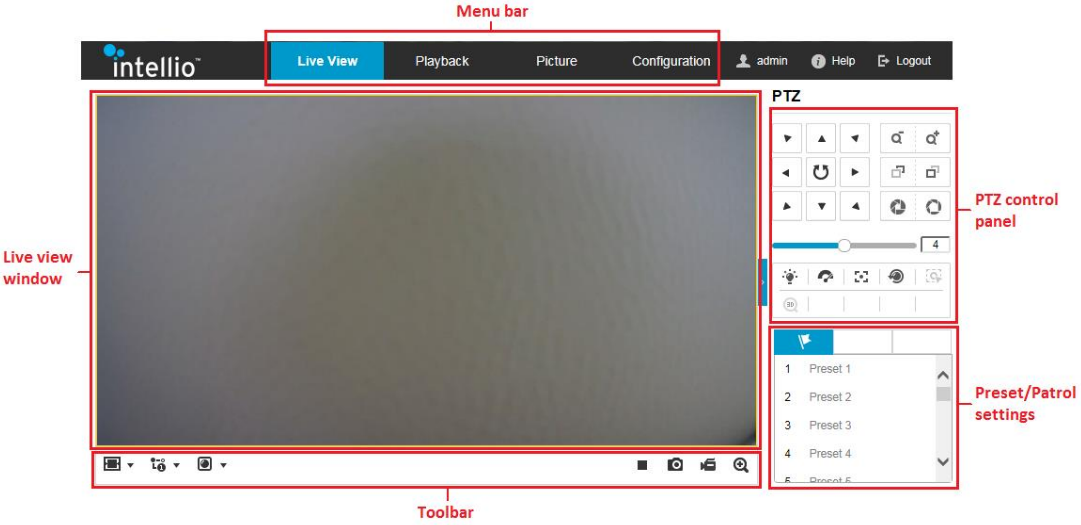


Figure 3-1 Live View Page

Menu Bar:

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

Live View Window:

Display the live video.

Toolbar:

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

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

Note:

If you are using Google Chrome 45 and its above version or Mozilla Firefox 52 and its above version, plug-in installation is not required. But **Picture** and **Playback** functions are hidden. To use mentioned function via web browser, change to their lower version, or change to **Internet Explorer 8.0 and its above version**.

PTZ Control:

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

Preset/Patrol Settings:

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

3.2 Starting Live View

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

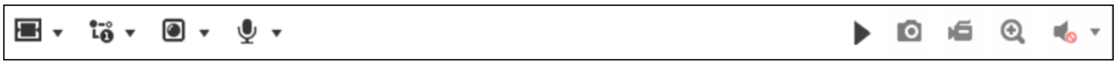


Figure 3-2 Live View Toolbar

Table 3-1 Descriptions of the Toolbar

Icon	Description
▶/■	Start/Stop live view.
4:3	The window size is 4:3.
16:9	The window size is 16:9.
1×	The original widow size.
▣	Self-adaptive window size.
①, ②, ③, etc.	Live view with the different video streams. Supported video streams vary according to camera models.
◙	Click to select the third-party plug-in.
📷	Manually capture the picture.

Icon	Description
🎥 / 🎥	Manually start/stop recording.
🔊 ▾/ 🔇	Audio on and adjust volume /Mute.
🎙 / 🎙	Turn on/off microphone.
🔍 / 🔍	Start/stop digital zoom function.

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

3.3 Recording and Capturing Pictures Manually

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

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

3.4 Operating Zoom/Focus Control

Purpose:

In the live view interface, you can use the PTZ control buttons to realize zoom/focus control of the camera. The zoom/focus control is supported only in ILB-340-VD-V, ILB-340-BL-V camera models.

3.4.1 PTZ Control Panel

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

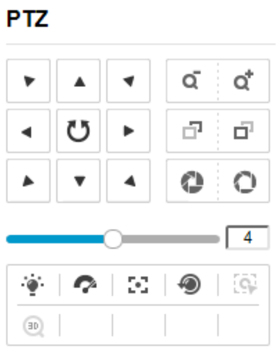


Figure 3-3 PTZ Control Panel

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

***Notes*:**

- There are eight direction arrows (△, ▽, ◁, ▷, ◸, ◹, ◿, ◺) in the control panel. For the cameras which support lens movements only, the direction buttons are invalid.

Table 3-2 Descriptions of PTZ Control Panel

Icon	Description
🔍- 🔍+	Zoom in/out
⧉ ⧉	Focus near/far
◐ ○	Iris +/-
━━━○─── 4	PTZ speed adjustment
💡	Light on/off
⌒	Wiper on/off
⛶	Auxiliary focus
◉	Initialize lens
≡	Adjust speed of pan/tilt movements
⛶	Start Manual Tracking
3D	Start 3D Zoom

Chapter 4 Camera Configuration

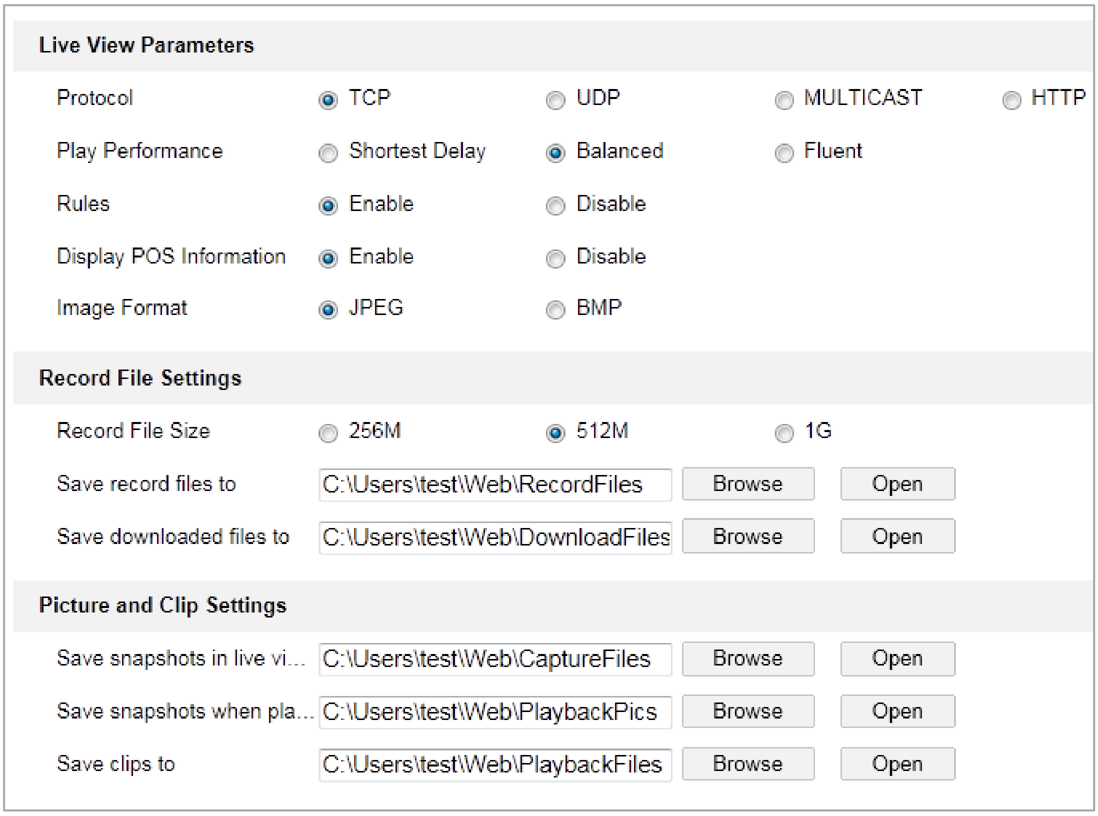
4.1 Configuring Local Parameters

Purpose:

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

Steps:

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



Live View Parameters

Protocol ● TCP ○ UDP ○ MULTICAST ○ HTTP

Play Performance ○ Shortest Delay ● Balanced ○ Fluent

Rules ● Enable ○ Disable

Display POS Information ● Enable ○ Disable

Image Format ● JPEG ○ BMP

Record File Settings

Record File Size ○ 256M ● 512M ○ 1G

Save record files to C:\Users\test\Web\RecordFiles

Save downloaded files to C:\Users\test\Web\DownloadFiles

Picture and Clip Settings

Save snapshots in live vi... C:\Users\test\Web\CaptureFiles

Save snapshots when pla... C:\Users\test\Web\PlaybackPics

Save clips to C:\Users\test\Web\PlaybackFiles

Figure 4-1 Local Configuration Interface

2. Configure the following settings:

- **Live View Parameters:** Set the protocol type and live view performance.

  ♦ **Protocol Type:** TCP, UDP, MULTICAST and HTTP are selectable.

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

UDP: Provides real-time audio and video streams.

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

MULTICAST: It's recommended to select MCAST type when using the Multicast function. For detailed information about Multicast, refer to ***Section 6.1.1 TCP/IP Settings***.

- ♦ **Play Performance:** Set the play performance to Shortest Delay, Balanced or Fluent.
- ♦ **Rules:** It refers to the rules on your local browser, select enable or disable to display or not display the colored marks when the motion detection, face detection, or intrusion detection is triggered. E.g., enabled as the rules are, and the face detection is enabled as well, when a face is detected, it will be marked with a green rectangle on the live view.
- ♦ **Display POS Information:** Enable the function, feature information of the detected target is dynamically displayed near the target in the live image.
  The feature information of different functions are different. For example, ID and waiting time for Queue Management, etc.
- ♦ **Image Format:** Choose the image format for picture capture.

- **Record File Settings:** Set the saving path of the recorded video files. Valid for the record files you recorded with the web browser.
  - ♦ **Record File Size:** Select the packed size of the manually recorded and downloaded video files to 256M, 512M or 1G. After the selection, the maximum record file size is the value you selected.
  - ♦ **Save record files to:** Set the saving path for the manually recorded video files.
  - ♦ **Save downloaded files to:** Set the saving path for the downloaded video files in playback mode.
- **Picture and Clip Settings:** Set the saving paths of the captured pictures and clipped video files. Valid for the pictures you capture with the web browser.
  - ♦ **Save snapshots in live view to:** Set the saving path of the manually captured pictures in live view mode.

- **Save snapshots when playback to:** Set the saving path of the captured pictures in playback mode.
- **Save clips to:** Set the saving path of the clipped video files in playback mode.

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

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

4.2 System Settings

Purpose:

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

4.2.1 Basic Information

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

In the **Basic Information** interface, you can edit the Device Name and Device No.. Other information of the camera, such as Model, Serial No., Firmware Version, Encoding Version, Number of Channels, Number of HDDs, Number of Alarm Input and Number of Alarm Output are displayed. The information cannot be changed in this menu. It is the reference for maintenance or modification in future.

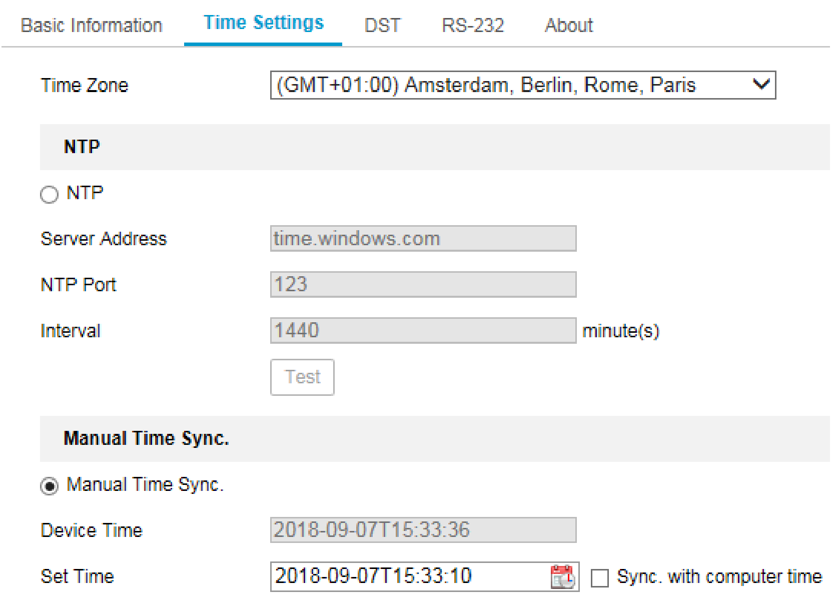
4.2.2 Time Settings

Purpose:

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

Steps:

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



Basic Information | Time Settings | DST | RS-232 | About

Time Zone: (GMT+01:00) Amsterdam, Berlin, Rome, Paris

NTP

○ NTP

Server Address: time.windows.com

NTP Port: 123

Interval: 1440 minute(s)

Test

Manual Time Sync.

● Manual Time Sync.

Device Time: 2018-09-07T15:33:36

Set Time: 2018-09-07T15:33:10 📅 □ Sync. with computer time

Figure 4-2 Time Settings

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

3. Configure the NTP settings.

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

   (2) Configure the following settings:

   Server Address: IP address of NTP server.

   NTP Port: Port of NTP server.

   Interval: The time interval between the two synchronizing actions with NTP server.

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

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

- Configure the manual time synchronization.

  (1) Check the **Manual Time Sync.** item to enable the manual time synchronization function.

  (2) Click the icon 📅 to select the date, time from the pop-up calendar.

  (3) (Optional) You can check **Sync. with computer time** item to synchronize the

time of the device with that of the local PC.

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

4.2.3 DST Settings

Purpose:

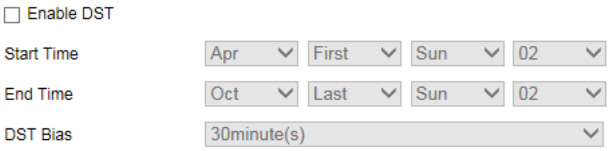
Daylight Saving Time (DST) is a way of making better use of the natural daylight by setting your clock forward one hour during the summer months, and back again in the fall.

Configure the DST according to your actual demand.

Steps:

1. Enter the DST configuration interface.

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



☐ Enable DST

Start Time: Apr, First, Sun, 02

End Time: Oct, Last, Sun, 02

DST Bias: 30minute(s)

Figure 4-3 DST Settings

2. Select the start time and the end time.
3. Select the DST Bias.
4. Click **Save** to activate the settings.

4.2.4 Open Source Software License

Information about the open source software that applies to the IP camera can be checked if required. Go to **Configuration > System Settings > About.**

4.3 Maintenance

4.3.1 Upgrade & Maintenance

Purpose:

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

Enter the Maintenance interface:

Configuration > **System** > **Maintenance** > **Upgrade & Maintenance**

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

  Notes:

  After restoring the default settings, the IP address is also restored to the default IP address, please be careful for this action.
- **Information Export**

  Device Parameters: click to export the current configuration file of the camera. This operation requires admin password to proceed.

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

  Diagnose Information: click to download log and system information.
- **Import Configuration File**

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

  Steps:

  1. Click **Browse** to select the saved configuration file.
  2. Click **Import** and input encryption password to start importing configuration file.

  Note: You need to reboot the camera after importing configuration file.
- **Upgrade**: Upgrade the device to a certain version.

  Steps:

  1. Select firmware or firmware directory to locate the upgrade file.

     Firmware: Locate the exact path of the upgrade file.

     Firmware Directory: Only the directory the upgrade file belongs to is required.

2. Click **Browse** to select the local upgrade file and then click **Upgrade** to start remote upgrade.

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

4.3.2 Log

Purpose:

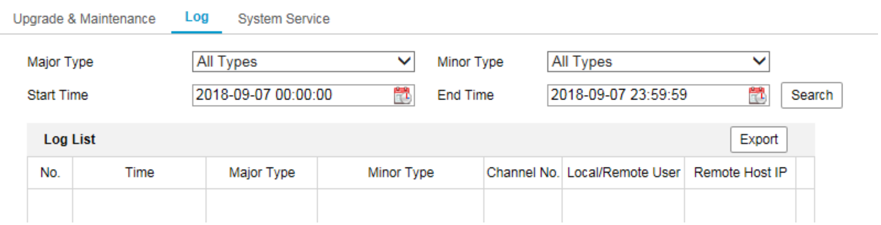
The operation, alarm, exception and information of the camera can be stored in log files. You can also export the log files on your demand.

Before you start:

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

Steps:

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



Major Type: All Types
Minor Type: All Types
Start Time: 2018-09-07 00:00:00
End Time: 2018-09-07 23:59:59

Log List

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

Figure 4-4 Log Searching Interface

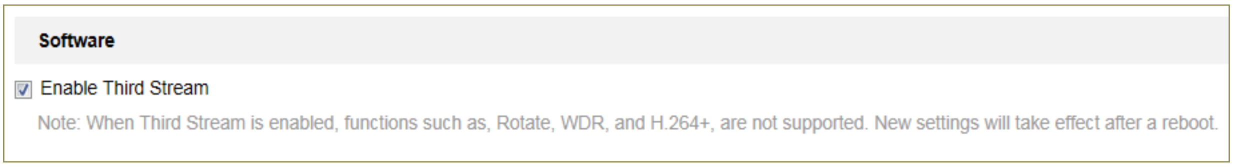
2. Set the log search conditions to specify the search, including the Major Type, Minor Type, Start Time and End Time.
3. Click **Search** to search log files. The matched log files will be displayed on the log list interface.
4. To export the log files, click **Export** to save the log files.

4.3.3 System Service

Purpose:

System service settings refer to the software and hardware service the camera supports. The cameras support IR LED, so you can select to enable or disable the corresponding service according to the actual demands.

Third Stream: You can check the checkbox of **Enable Third Stream** to reboot the system and enable the third stream.



Software

☑ Enable Third Stream

Note: When Third Stream is enabled, functions such as, Rotate, WDR, and H.264+, are not supported. New settings will take effect after a reboot.

Figure 4-5 Enable Third Stream

4.4 Security Settings

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

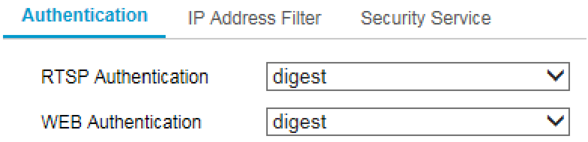
4.4.1 Authentication

Purpose:

You can specifically secure the stream data of live view.

Steps:

1. Enter the Authentication interface: **Configuration** > **System** > **Security** > **Authentication.**



RTSP Authentication: digest

WEB Authentication: digest

2. AuthenticationSet up authentication method for RTSP authentication and WEB authentication.

   Caution:

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

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

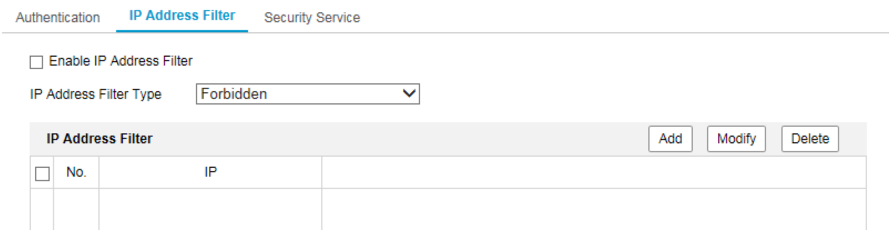
4.4.2 IP Address Filter

Purpose:

This function makes it possible for access control.

Steps:

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



☐ Enable IP Address Filter

IP Address Filter Type: Forbidden

IP Address Filter

☐	No.	IP

Figure 4-6 IP Address Filter Interface

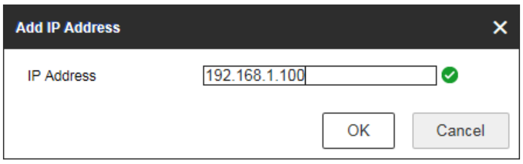
2. Check the checkbox of **Enable IP Address Filter**.
3. Select the type of IP Address Filter in the drop-down list, **Forbidden** and **Allowed** are selectable.
4. Set the IP Address Filter list.

- Add an IP Address

Steps:

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

(2) Input the IP Adreess.



IP Address: 192.168.1.100 ✓

Figure 4-7 Add an IP

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

- Modify an IP Address

Steps:

(1) Left-click an IP address from filter list and click **Modify**.

(2) Modify the IP address in the text filed.

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

- Delete an IP Address or IP Addresses.

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

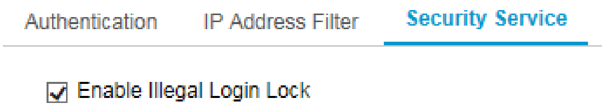
5. Click **Save** to save the settings.

4.4.3 Security Service

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

Steps:

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



Authentication | IP Address Filter | Security Service

☑ Enable Illegal Login Lock

Figure 4-8 Security Service

2. Check the checkbox of **Enable Illegal Login Lock**.

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

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

4.5 User Management

4.5.1 User Management

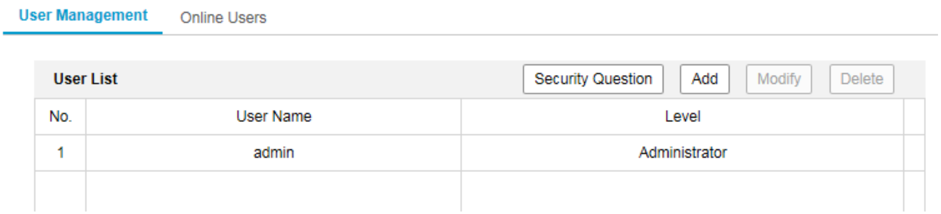
- **As Administrator**

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

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

Note:

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



No.	User Name	Level
1	admin	Administrator

Figure 4-9 User Management Interface

- **Adding a User**

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

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

Steps:

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

   Notes:

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

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

3. You can check or uncheck the permissions for the new user.
4. Click **OK** to finish the user addition.

- **Modifying a User**

Steps:

1. Left-click to select the user from the list and click **Modify**.
2. Modify the **User Name**, **Level** and **Password**.

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

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

- **Deleting a User**

Steps:

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

- **As Operator or User**

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

4.5.2 Security Question

Purpose:

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

Set Security Question:

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

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

Steps:

1. Enter setting interface:

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

Reset Admin Password:

Before you start:

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

Steps:

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

Note:

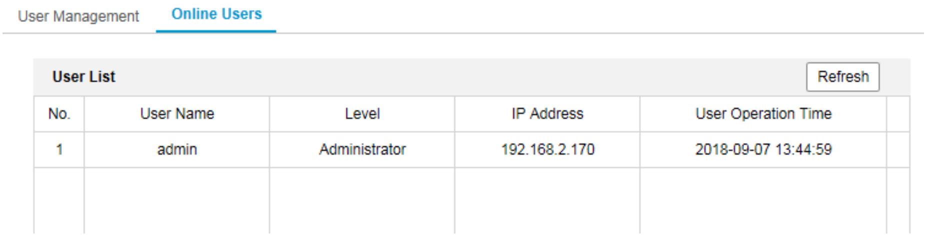
User IP address is locked for 30 minutes after 7 failed attempts of answering security questions.

4.5.3 Online Users

Purpose:

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

Click **Refresh** to refresh the list.



No.	User Name	Level	IP Address	User Operation Time
1	admin	Administrator	192.168.2.170	2018-09-07 13:44:59

Figure 4-10 View the Online Users

Chapter 5 Network Settings

Purpose:

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

5.1 Basic Settings

Purpose:

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

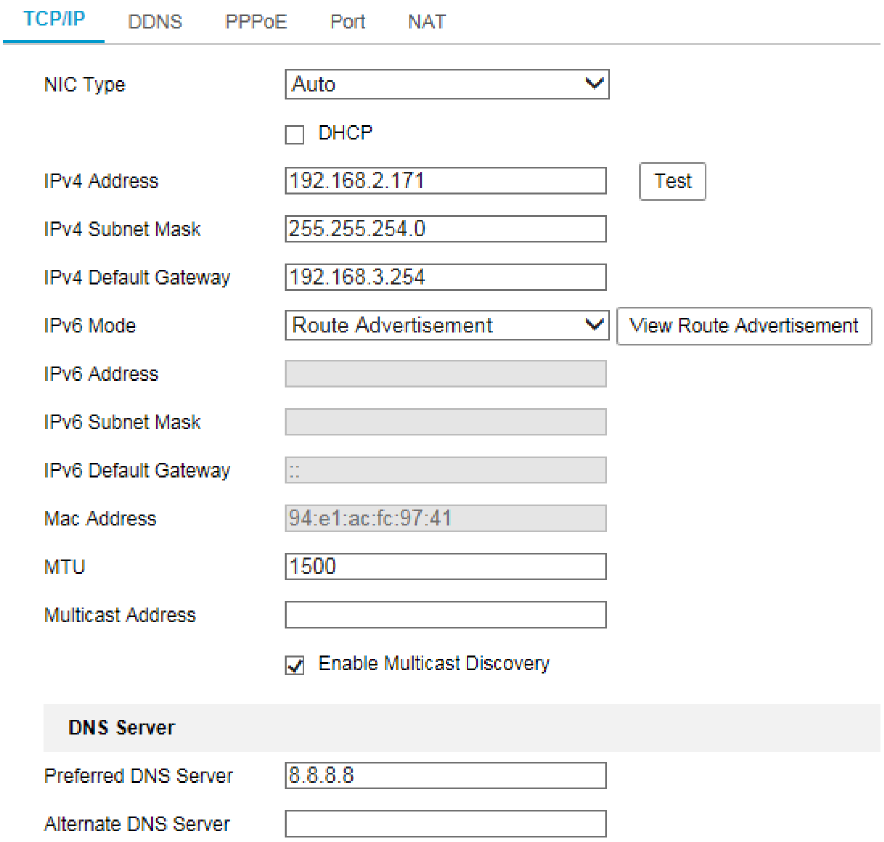
5.1.1 TCP/IP Settings

Purpose:

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

Steps:

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



NIC Type	Auto
	□ DHCP
IPv4 Address	192.168.2.171
IPv4 Subnet Mask	255.255.254.0
IPv4 Default Gateway	192.168.3.254
IPv6 Mode	Route Advertisement
IPv6 Address	
IPv6 Subnet Mask	
IPv6 Default Gateway	::
Mac Address	94:e1:ac:fc:97:41
MTU	1500
Multicast Address	
	☑ Enable Multicast Discovery

DNS Server

Preferred DNS Server	8.8.8.8
Alternate DNS Server	

Figure 5-1 TCP/IP Settings

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

***Notes*:**

- The valid value range of MTU is 1280 to 1500.
- The Multicast sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Before utilizing this function, you have to enable the Multicast function of your router.

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

5.1.2 DDNS Settings

Purpose:

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

***Before you start*:**

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

Steps:

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

   - DynDNS:

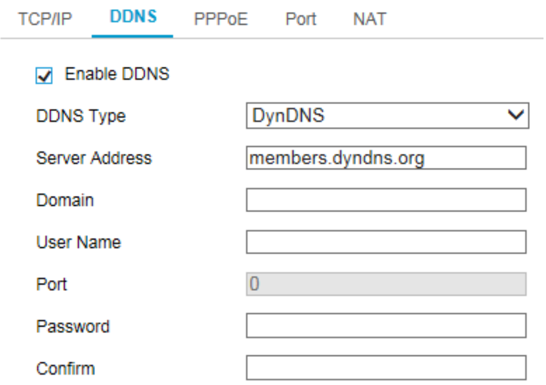
   Steps:

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

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

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

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



☑ Enable DDNS

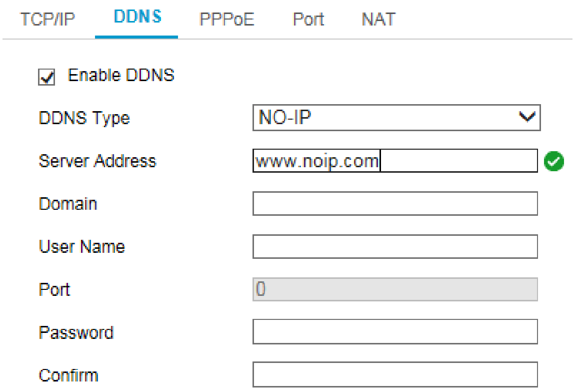
DDNS Type	DynDNS
Server Address	members.dyndns.org
Domain	
User Name	
Port	0
Password	
Confirm	

Figure 5-2 DynDNS Settings

- NO-IP:

Steps:

(1)Choose the DDNS Type as NO-IP.



☑ Enable DDNS

DDNS Type: NO-IP

Server Address: www.noip.com

Domain:

User Name:

Port: 0

Password:

Confirm:

Figure 5-3 NO-IP DNS Settings

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

(3)Enter the Domain name you registered.

(4)Enter the User Name and Password.

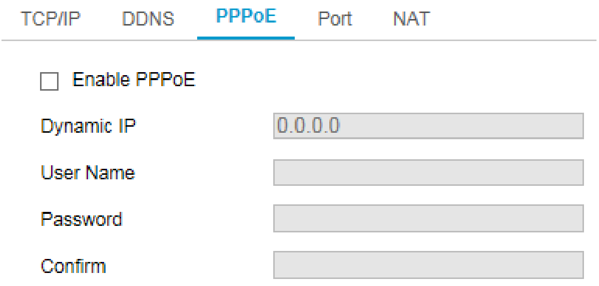
(5)Click **Save** and then you can view the camera with the domain name.

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

5.1.3 PPPoE Settings

Steps:

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



□ Enable PPPoE

Dynamic IP: 0.0.0.0

User Name:

Password:

Confirm:

Figure 5-4 PPPoE Settings

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

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

⚠

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

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

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

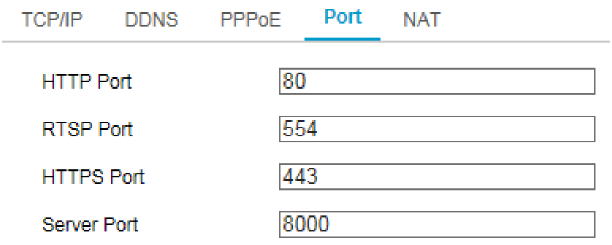
5.1.4 Port Settings

Purpose:

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

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 5-5 Port Settings

2. Set the ports of the camera.

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

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

ranges from 1 to 65535.

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

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

Note:

When you use Intellio Video System software to manage the camera and you have changed the server port number, you have to input the correct server port number in login interface to access to the camera.

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

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

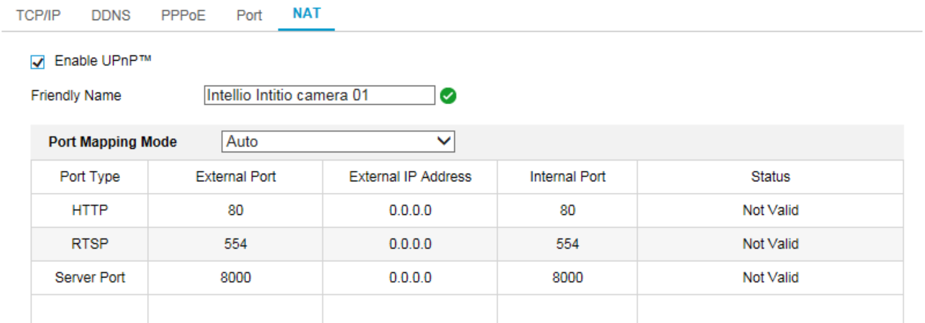
5.1.5 Configure NAT (Network Address Translation) Settings

Purpose:

NAT interface allows you to configure the UPnP™ parameters.

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

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



☑ Enable UPnP™

Friendly Name: Intellio Intitio camera 01 ✓

Port Mapping Mode: Auto

Port Type	External Port	External IP Address	Internal Port	Status
HTTP	80	0.0.0.0	80	Not Valid
RTSP	554	0.0.0.0	554	Not Valid
Server Port	8000	0.0.0.0	8000	Not Valid

Figure 5-6 UPnP Settings

Steps:

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

NAT.

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

   Note:

   Only when the UPnP™ function is enabled, ports of the camera are active.

3. Choose a friendly name for the camera, or you can use the default name.
4. Select the port mapping mode. Manual and Auto are selectable.

   Note:

   If you select Auto, you should enable UPnP™ function on the router.

   If you select Manual, you can customize the value of the external port and complete port mapping settings on router manually.

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

5.2 Advanced Settings

Purpose:

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

5.2.1 SNMP Settings

Purpose:

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

Before you start:

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

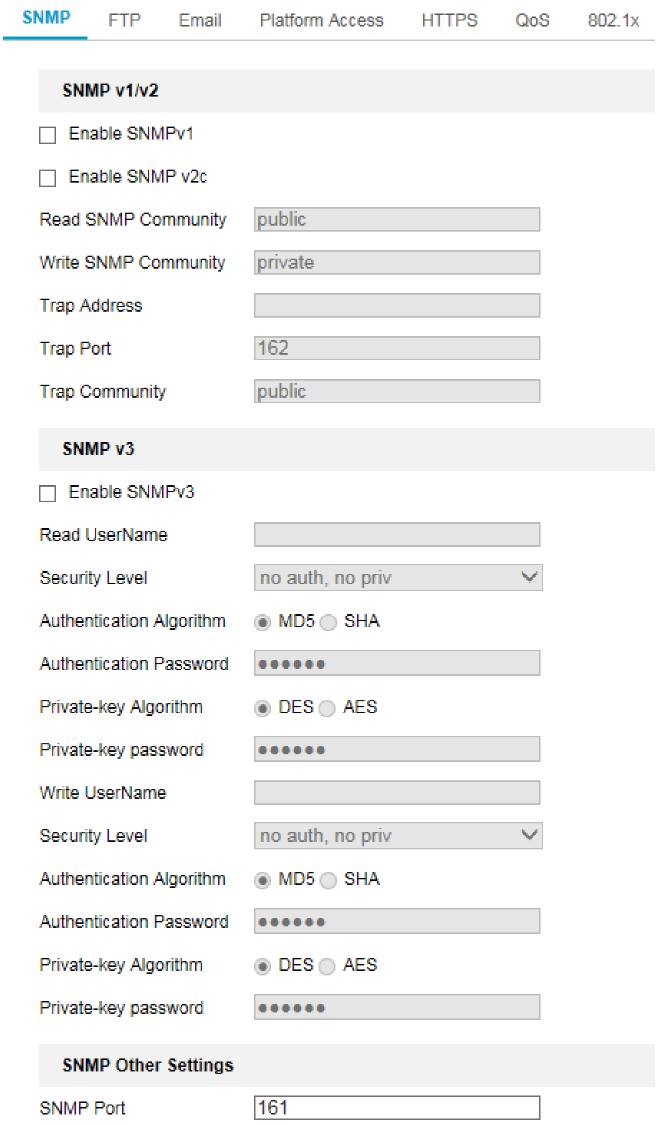
Note: The SNMP version you select should be the same as that of the SNMP software. And you also need to use the different version according to the security level you required. SNMP v1 provides no security and SNMP v2 requires password for access. And SNMP v3 provides encryption and if you use the third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

⚠

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

Steps:

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



SNMP v1/v2

□ Enable SNMPv1

□ Enable SNMP v2c

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

SNMP v3

□ Enable SNMPv3

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

SNMP Other Settings

SNMP Port	161

Figure 5-7 SNMP Settings

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

3. Configure the SNMP settings.

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

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

Notes:

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

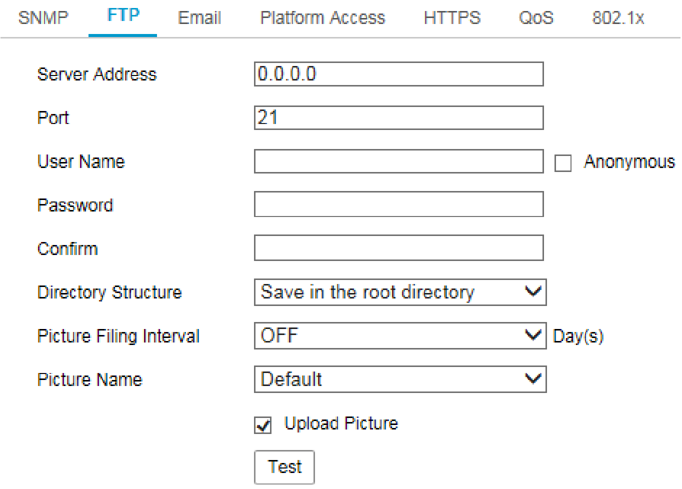
5.2.2 FTP Settings

Purpose:

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

Steps:

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



Server Address	0.0.0.0
Port	21
User Name	□ Anonymous
Password	
Confirm	
Directory Structure	Save in the root directory
Picture Filing Interval	OFF Day(s)
Picture Name	Default
	☑ Upload Picture

Figure 5-8 FTP Settings

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

⚠

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

responsibility of the installer and/or end-user.

4. Set the directory structure and picture filing interval.

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

   Picture Filing Interval: For better picture management, you can set the picture filing interval from 1 day to 30 days. Pictures captured in the same time interval will be saved in one folder named after the beginning date and ending date of the time interval.

   Picture Name: Set the naming rule for captured picture files. You can choose **Default** in the drop-down list to use the default rule, that is,

   IP address_channel number_capture time_event type.jpg

   (e.g., *10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg*).

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

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

   Upload Picture: To enable uploading the captured picture to the FTP server.

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

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

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

5.2.3 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:

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

Steps:

1. Enter the TCP/IP Settings (**Configuration > Network > Basic Settings > TCP/IP**) to set the IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway and the Preferred DNS Server.

   Note: Please refer to ***Section 6.1.1 TCP/IP Settings*** for detailed information.

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

3. Configure the following settings:

   Sender: The name of the email sender.

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

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

   SMTP Port: The SMTP port. The default TCP/IP port for SMTP is 25 (not secured). And the SSL SMTP port is 465.

   Email Encryption: None, SSL, and TLS are selectable. When you select SSL or TLS and disable STARTTLS, e-mails will be sent after encrypted by SSL or TLS. The SMTP port should be set as 465 for this encryption method. When you select SSL or TLS and enable STARTTLS, emails will be sent after encrypted by STARTTLS, and the SMTP port should be set as 25.

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

   Attached Image: Check the checkbox of Attached Image if you want to send emails with attached alarm images.

   Interval: The interval refers to the time between two actions of sending attached pictures.

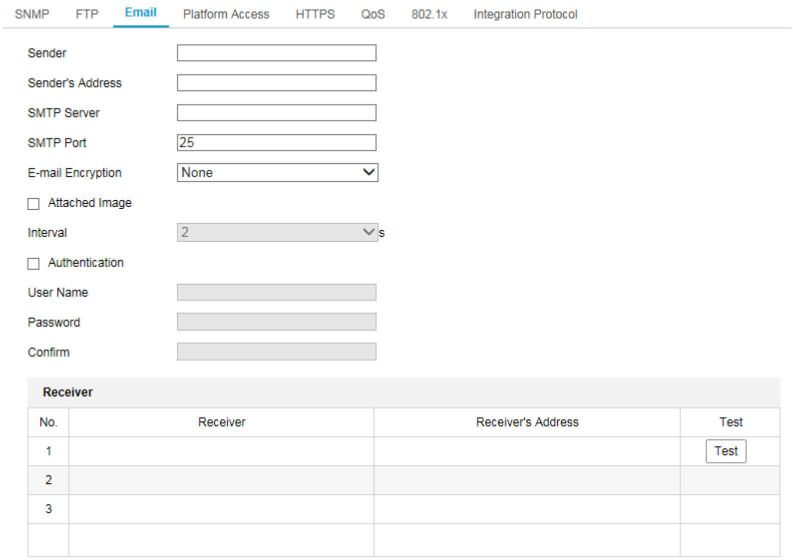
   Authentication (optional): If your email server requires authentication, check this checkbox to use authentication to log in to this server and input the login user name and password.

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

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

Receiver: The name of the user to be notified.

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



Sender

Sender's Address

SMTP Server

SMTP Port 25

E-mail Encryption None

□ Attached Image

Interval 2 s

□ Authentication

User Name

Password

Confirm

Receiver

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

Figure 5-9 Email Settings

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

5.2.4 HTTPS Settings

Purpose:

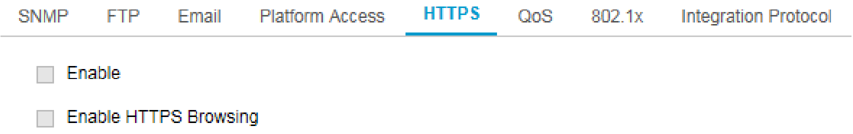
HTTPS provides authentication of the web site and its associated web server, which protects against Man-in-the-middle attacks.

Note:

- HTTPS is enabled by default for some camera models.
- If HTTPS is enabled, the camera creates an unsigned certificate automatically. When accessing via HTTPS, the web browser will send a prompt that installing a signed certificate is recommended.

Steps:

1. Enter the HTTPS settings interface. **Configuration > Network > Advanced Settings > HTTPS**.
2. Check **Enable** to access the camera via HTTP or HTTPS protocol.
3. Check **Enable HTTPS Browsing** to access the camera only via HTTPS protocol.

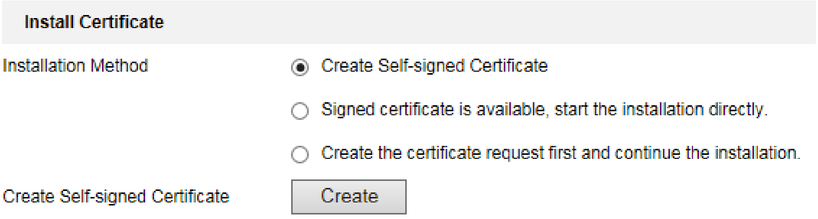


□ Enable

□ Enable HTTPS Browsing

Figure 5-10 HTTPS Configuration Interface

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



Install Certificate

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

Create Self-signed Certificate

Figure 5-11 Create Self-signed Certificate

- Create the self-signed certificate

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

(2) Click **Create** button to enter the creation interface.

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

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

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

- Create the request and import the authorized certificate

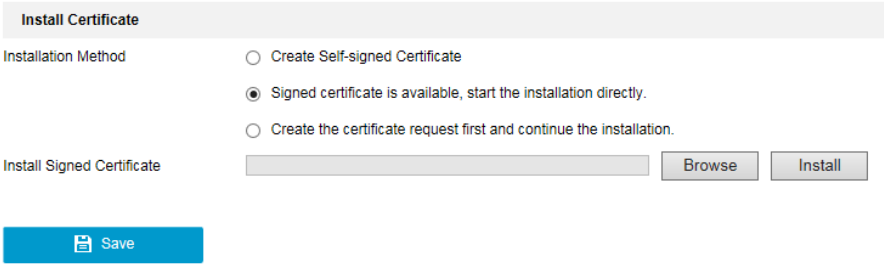
(1) Select **Create the certificate request first and continue the installation** as the Installation Method.

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

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

(4) After receiving the signed valid certificate, you can import the certificate in two ways:

a) Select **Signed certificate is available, Start the installation directly**. Click **Browse** and **Install** to import the certificate to the device.



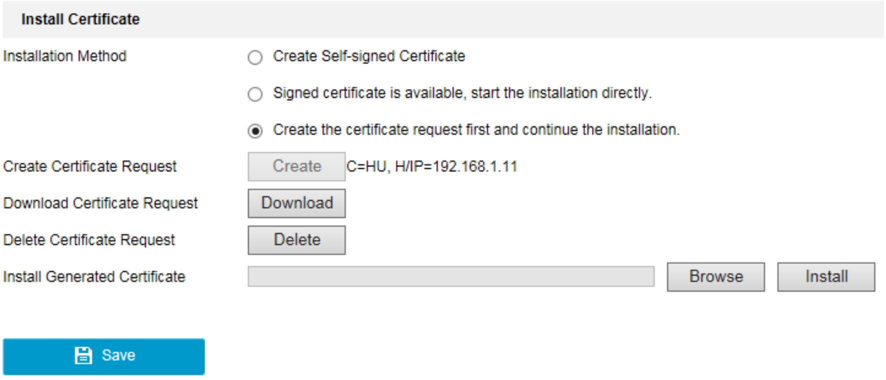
Install Certificate

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

Install Signed Certificate

Figure 5-12 Import the Certificate (1)

b) Select **Create the certificate request first and continue the installation**. Click **Browse** and **Install** to import the certificate to the device.



Install Certificate

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

Create Certificate Request: Create C=HU, H/IP=192.168.1.11

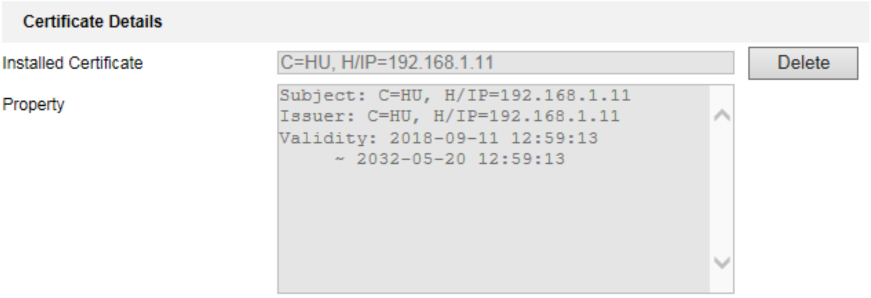
Download Certificate Request: Download

Delete Certificate Request: Delete

Install Generated Certificate

Figure 5-13 Import the Certificate (2)

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



Certificate Details

Installed Certificate: C=HU, H/IP=192.168.1.11

Property:

```
Subject: C=HU, H/IP=192.168.1.11
Issuer: C=HU, H/IP=192.168.1.11
Validity: 2018-09-11 12:59:13
     ~ 2032-05-20 12:59:13
```

Figure 5-14 Installed Certificate

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

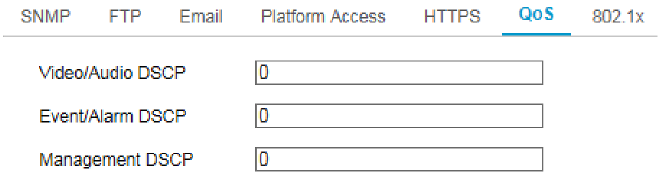
5.2.5 QoS Settings

Purpose:

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

Steps:

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



Video/Audio DSCP: 0

Event/Alarm DSCP: 0

Management DSCP: 0

Figure 5-15 QoS Settings

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

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

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

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

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

5.2.6 802.1X Settings

Purpose:

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

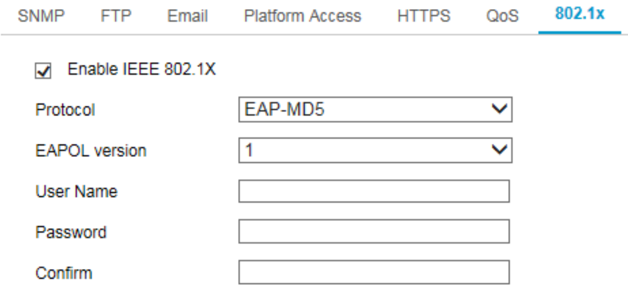
Before you start:

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

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

Steps:

1. Enter the 802.1X Settings interface, **Configuration > Network > Advanced Settings > 802.1X**



☑ Enable IEEE 802.1X

Protocol	EAP-MD5
EAPOL version	1
User Name	
Password	
Confirm	

Figure 5-16 802.1X Settings

2. Check the **Enable IEEE 802.1X** checkbox to enable the feature.
3. Configure the 802.1X settings, including Protocol, EAPOL version, User Name, Password and Confirm.

   Note: The **EAPOL version** must be identical with that of the router or the switch.
4. Enter the user name and password to access the server.
5. Click **Save** to finish the settings.

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

5.2.7 Integration Protocol

Purpose:

If you need to access to the device through ONVIF protocol, you can configure ONVIF user in this interface. Refer to ONVIF standard for detailed configuration rules.

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

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

   Note: ONVIF user account is different from the camera user account. You have set ONVIF user account independently.
3. Save the settings.

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

Chapter 6 Video/Audio Settings

Purpose:

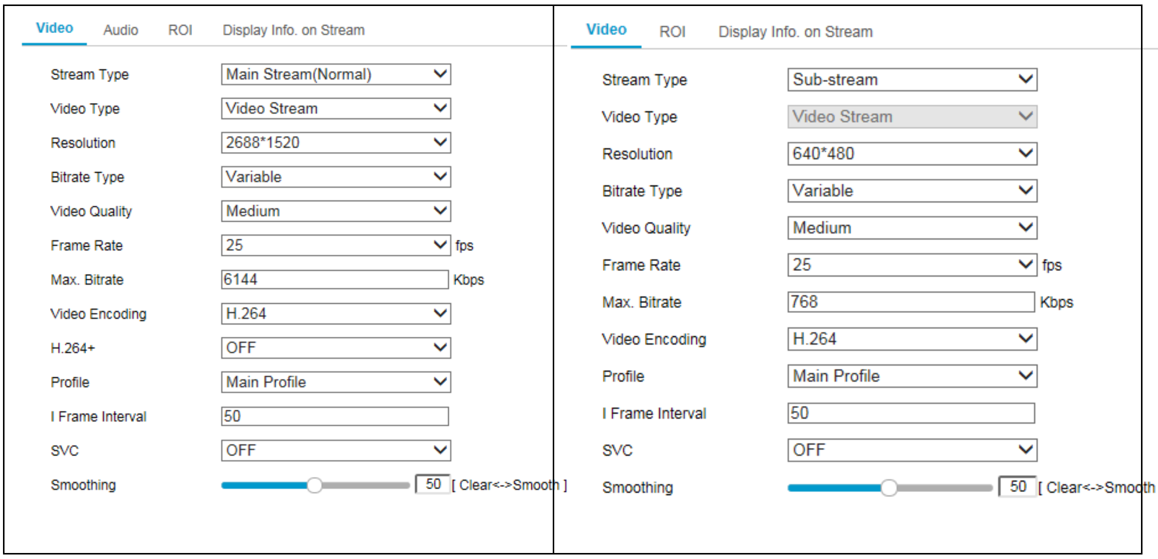
Follow the instructions below to configure the video setting, audio settings, ROI, Display info. on Stream, etc.

6.1 Video Settings

You can configure parameters for available video streams, for example, the main stream, the sub-stream, etc.

Steps:

1. Enter the Video Settings interface, **Configuration > Video/Audio > Video**



Stream Type	Main Stream(Normal)
Video Type	Video Stream
Resolution	2688*1520
Bitrate Type	Variable
Video Quality	Medium
Frame Rate	25 fps
Max. Bitrate	6144 Kbps
Video Encoding	H.264
H.264+	OFF
Profile	Main Profile
I Frame Interval	50
SVC	OFF
Smoothing	50 [Clear<->Smooth]

Stream Type	Sub-stream
Video Type	Video Stream
Resolution	640*480
Bitrate Type	Variable
Video Quality	Medium
Frame Rate	25 fps
Max. Bitrate	768 Kbps
Video Encoding	H.264
Profile	Main Profile
I Frame Interval	50
SVC	OFF
Smoothing	50 [Clear<->Smooth]

Figure 6-1 Video Settings

2. Select the Stream Type.

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

   Notes:

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

3. You can customize the following parameters for the selected stream type.

Video Type:

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

Resolution:

Select the resolution of the video output.

Bitrate Type:

Select the bitrate type to constant or variable.

Video Quality:

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

Frame Rate:

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

Max. Bitrate:

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

Note: The maximum limit of the max. bitrate value varies according to different camera platforms.

Video Encoding:

The camera supports multiple video encodings types, such as H.264 and H.265. H.265 is a new encoding technology. Compared with H.264, it reduces the transmission bitrate under the same resolution, frame rate and image quality, although it increases the load of the client PC.

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

H.264+ and H.265+:

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

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

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

Notes:

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

Max. Average Bitrate:

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

Profile:

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

I Frame Interval:

Set I Frame Interval from 1 to 400. If you use the camera with Intellio Video System, do not exceed 50.

SVC:

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

Smoothing:

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

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

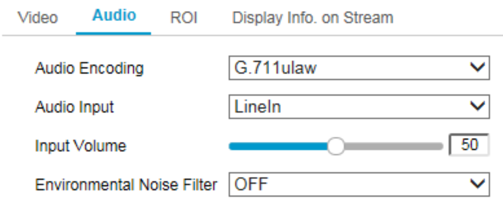
Note:

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

6.2 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 6-2 Audio Settings

2. Configure the following settings.

   Note: Audio settings vary according to different camera models.

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

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

Input Volume: 0-100 adjustable.

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

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

6.3 ROI Encoding

Purpose:

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

Note: ROI function varies according to different camera models.

Steps:

1. Enter the ROI settings interface: **Configuration > Video/Audio > ROI**.
2. Select the Stream Type for ROI encoding.
3. Check the checkbox of **Enable** under Fixed Region item.
4. Set **Fixed Region** for ROI.
   (1) Select the Region No. from the drop-down list.
   (2) Check the **Enable** checkbox to enable ROI function for the chosen region.
   (3) Click **Drawing**. Click and drag the mouse on the view screen to draw a red rectangle as the ROI region. You can click **Clear** to cancel former drawing. Click **Stop Drawing** when you finish.
   (4) Select the ROI level.
   (5) Enter a region name for the chosen region.

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

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

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

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

6.4 Display Info on Stream

Check the checkbox of **Enable Dual-VCA**, and the information of the objects (e.g. human, vehicle, etc.) will be marked in the video stream. Then, you can set rules on the connected rear-end device to detect the events including line crossing, intrusion, etc.

Chapter 7 Image Settings

Purpose:

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

7.1 Display Settings

Purpose:

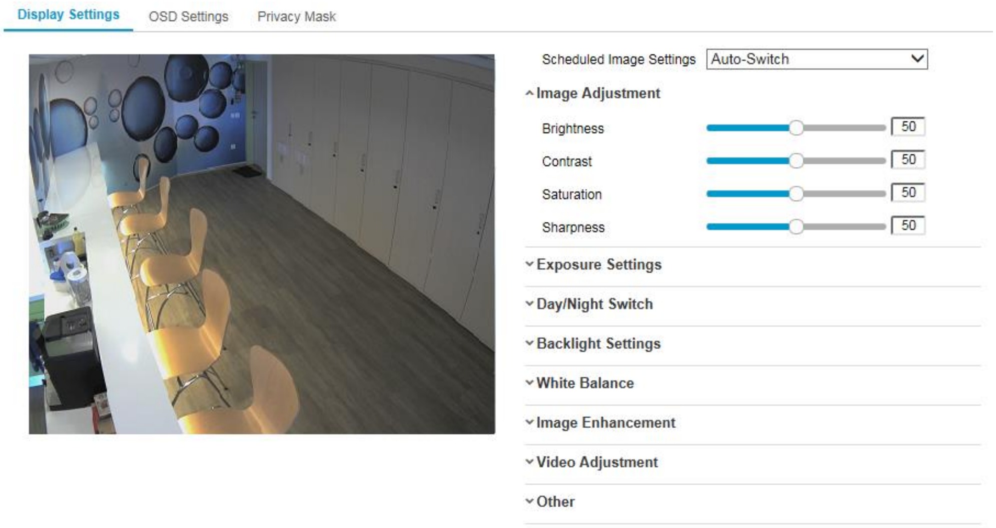
Configure the image adjustment, exposure settings, day/night switch, backlight settings, white balance, image enhancement, video adjustment, and other parameters in display settings.

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

7.1.1 Day/Night Auto-Switch

Steps:

1. Enter the Display Settings interface, **Configuration > Image > Display Settings**.



Scheduled Image Settings: Auto-Switch

Image Adjustment

Brightness	50
Contrast	50
Saturation	50
Sharpness	50

Figure 7-1 Display Settings of Day/Night Auto-Switch

2. Set the image parameters of the camera.

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

- **Image Adjustment**

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

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

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

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

- **Exposure Settings**

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

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

  The **Exposure Time** refers to the electronic shutter time, which ranges from 1/3 to 1/100,000s. Adjust it according to the actual luminance condition.

- **Day/Night Switch**

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

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

  Day: the camera stays at day mode.

  Night: the camera stays at night mode.

  Auto: the camera switches between the day mode and the night mode according to the illumination automatically. The sensitivity ranges from 0 to 7, the higher the value is, the easier the mode switches. The filtering time refers to the interval time between the day/night switch. You can set it from 5s to 120s.

  Scheduled-Switch: Set the start time and the end time to define the duration for day/night mode.

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

  Smart Supplement Light: Set the supplement light as ON, and Auto and Manual are selectable for light mode.

Select Auto, and the supplement light changes according to the actual luminance. E.g., if the current scene is bright enough, then the supplement light adjusts itself to lower power; and if the scene is not bright enough, the light adjusts itself to higher power.

Select Manual, and you can adjust the supplement by adjusting the distance. E.g., if the object is near the camera, the device adjusts the supplement light to lower power, and the light is in higher power if the object is far away.

- **Backlight Settings**

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

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

WDR: Wide Dynamic Range can be used when there is a high contrast of the bright area and the dark area of the scene.

HLC: High Light Compression function can be used when there are strong lights in the scene affecting the image quality.

- **White Balance**

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

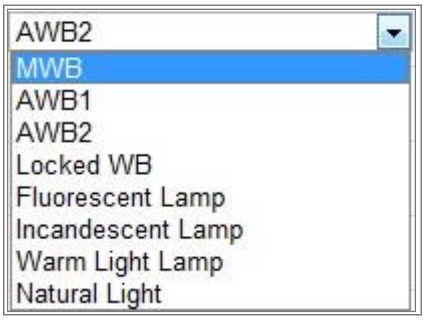


Figure 7-2 White Balance

- **Image Enhancement**

Digital Noise Reduction: DNR reduces the noise in the video stream. OFF, Normal and Expert are selectable. Set the DNR level from 0 to 100 in Normal Mode. Set the DNR level from both space DNR level [0-100] and time DNR level [0-100] in Expert Mode.

- **Video Adjustment**

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

Rotate: To make a complete use of the 16:9 aspect ratio, you can enable the rotate function when you use the camera in a narrow view scene.

When installing, turn the camera to the 90 degrees or rotate the 3-axis lens to 90 degrees, and set the rotate mode as on, you will get a normal view of the scene with 9:16 aspect ratio to ignore the needless information such as the wall, and get more meaningful information of the scene.

Scene Mode: Choose the scene as indoor or outdoor according to the real environment.

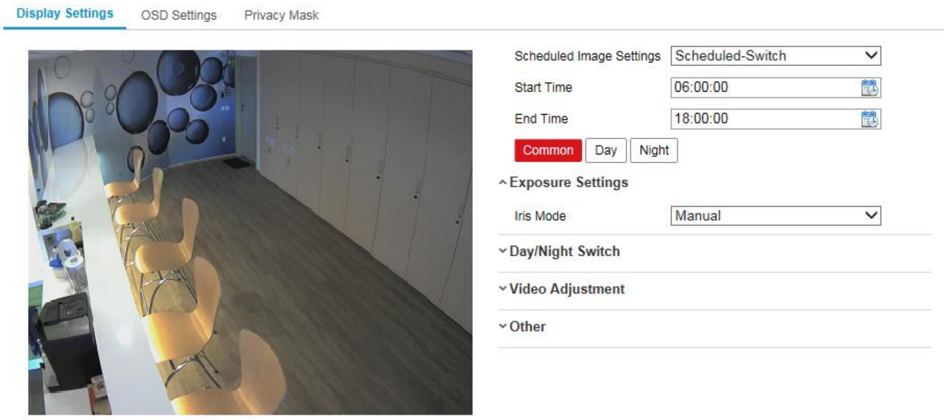
Video Standard: 50 Hz and 60 Hz are selectable. Choose according to the different video standards; normally 50 Hz for PAL standard and 60 Hz for NTSC standard.

- **Others**

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

7.1.2 Day/Night Scheduled-Switch

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



Scheduled Image Settings: Scheduled-Switch

Start Time: 06:00:00

End Time: 18:00:00

Iris Mode: Manual

Figure 7-3 Day/Night Scheduled-Switch Configuration Interface

Steps:

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

   Notes:

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

2. Click Common tab to configure the common parameters applicable to the day mode and night mode.

   Note: For the detailed information of each parameter, please refer to ***Section 8.1.1 Day/Night Auto-Switch***.

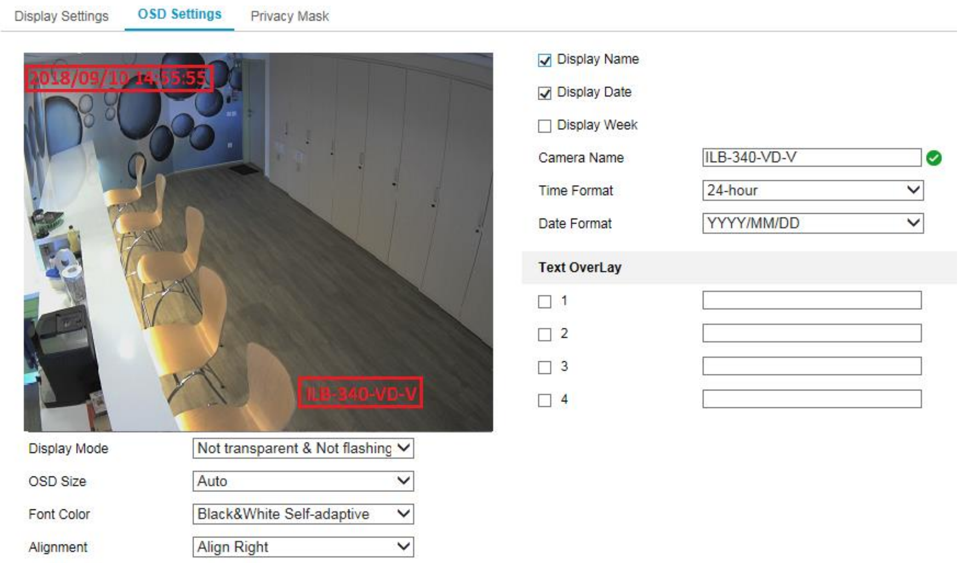
3. Click Day tab to configure the parameters applicable for day mode.
4. Click Night tab to configure the parameters applicable for night mode.

Note: The settings saved automatically if any parameter is changed.

7.2 OSD Settings

Purpose:

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



☑ Display Name

☑ Display Date

☐ Display Week

Camera Name	ILB-340-VD-V ✓
Time Format	24-hour
Date Format	YYYY/MM/DD

Text OverLay

☐ 1

☐ 2

☐ 3

☐ 4

Display Mode	Not transparent & Not flashing
OSD Size	Auto
Font Color	Black&White Self-adaptive
Alignment	Align Right

Figure 7-4 OSD Settings

Steps:

1. Enter the OSD Settings interface: **Configuration** > **Image** > **OSD Settings**.
2. Check the corresponding checkbox to select the display of camera name, date or week if required.
3. Edit the camera name in the text field of **Camera Name**.
4. Select from the drop-down list to set the time format and date format.
5. Select from the drop-down list to set the time format, date format, display mode, OSD size and OSD color.
6. Configure the text overlay settings.

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

   (2) Input the characters in the textbox.

   Note: Up to 8 text overlays are configurable.
7. Adjust the position and alignment of text frames.

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

   Note: The alignment adjustment is only applicable to Text Overlay items.
8. Click **Save** to save the settings.

7.3 Privacy Mask

Purpose:

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

Steps:

1. Enter the Privacy Mask Settings interface: **Configuration** > **Image** > **Privacy Mask**.
2. Check the checkbox of **Enable Privacy Mask** to enable this function.
3. Click **Draw Area**.

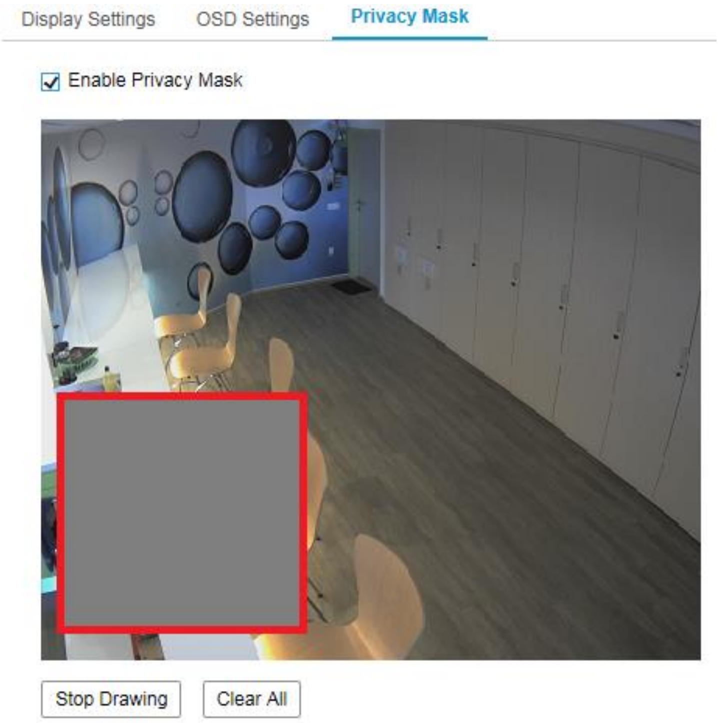


Figure 7-5 Privacy Mask Settings

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

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

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

Chapter 8 Event Settings

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

8.1 Basic Events

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

***Note*:** Check the checkbox of Notify Surveillance Center if you want the alarm information to be pushed to the Intellio Video System software as soon as the alarm is triggered.

8.1.1 Motion Detection

Purpose:

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

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

- **Normal Configuration**

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

Task 1: Set the Motion Detection Area

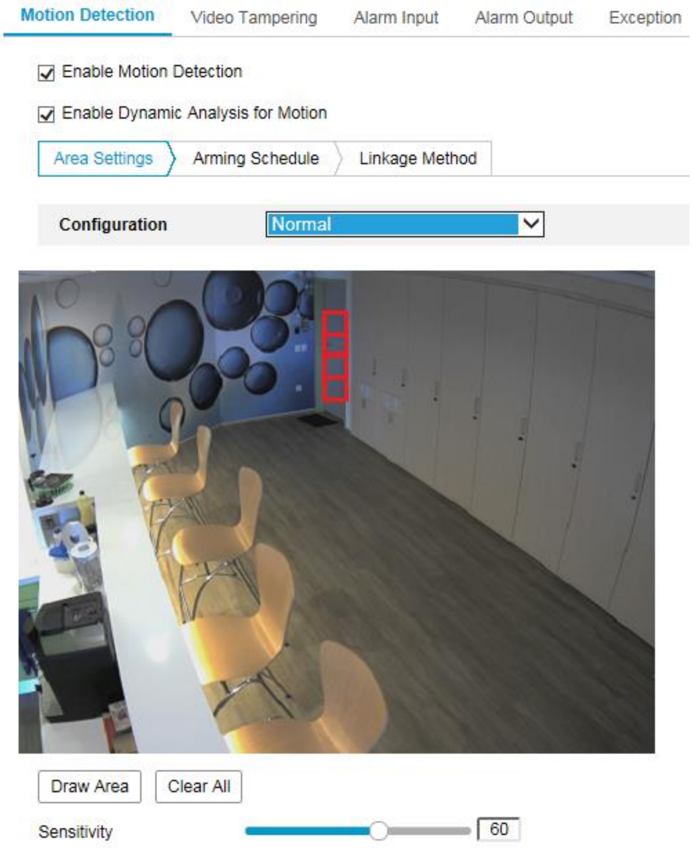
Steps:

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

2. Check the checkbox of **Enable Motion Detection**.

3. Check the checkbox of **Enable Dynamic Analysis for Motion** if you want to mark the detected objects with green rectangles.

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



☑ Enable Motion Detection

☑ Enable Dynamic Analysis for Motion

Configuration: Normal

Sensitivity: 60

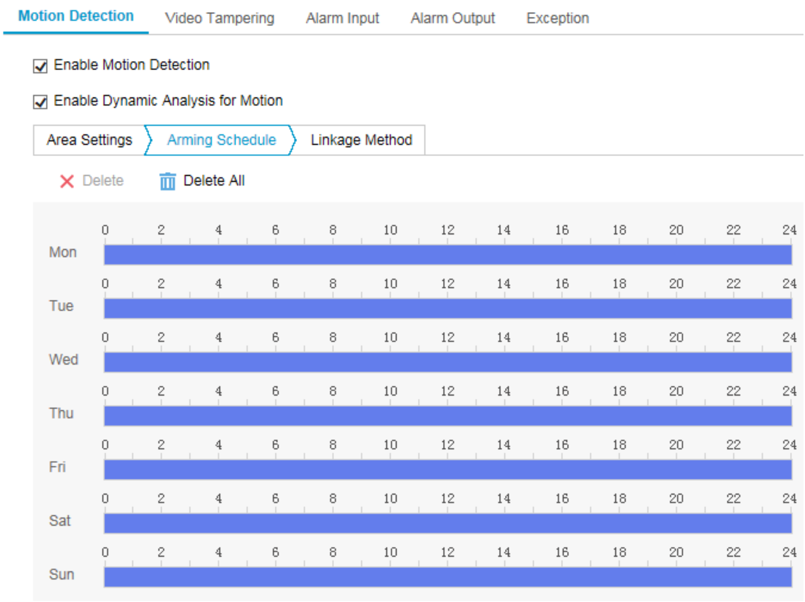
Figure 8-1 Enable Motion Detection

4. Click **Draw Area**. Click and drag the mouse on the live video to draw a motion detection area. Click **Stop Drawing** to finish drawing one area.

5. (Optional) Click **Clear All** to clear all of the areas.

6. (Optional) Move the slider to set the sensitivity of the detection.

Task 2: Set the Arming Schedule for Motion Detection



☑ Enable Motion Detection

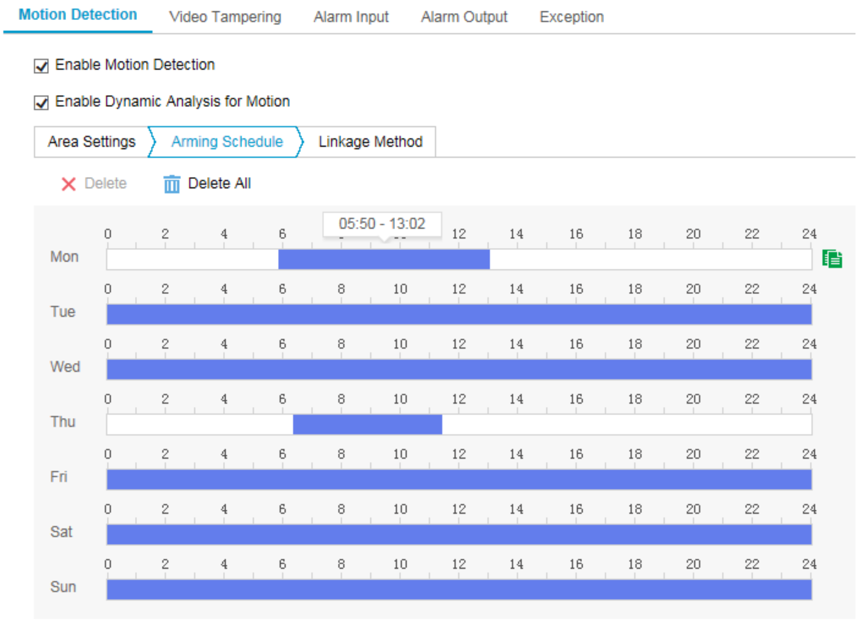
☑ Enable Dynamic Analysis for Motion

Figure 8-2 Arming Schedule

Steps:

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

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



☑ Enable Motion Detection

☑ Enable Dynamic Analysis for Motion

05:50 - 13:02

Figure 8-3 Arming Schedule

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

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

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

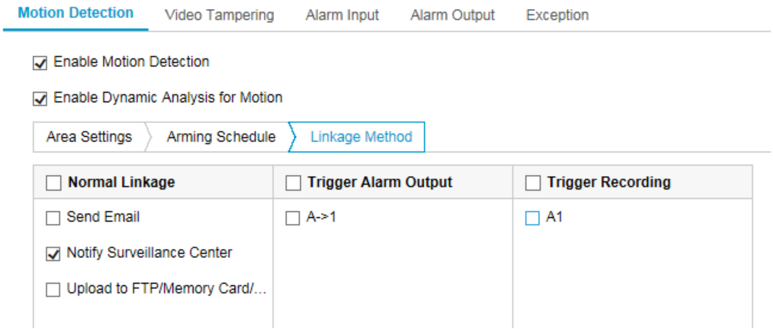
can copy the current settings to other days.

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

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

Task 3: Set the Linkage Method for Motion Detection

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



☑ Enable Motion Detection

☑ Enable Dynamic Analysis for Motion

□ **Normal Linkage**	□ **Trigger Alarm Output**	□ **Trigger Recording**
□ Send Email	□ A->1	□ A1
☑ Notify Surveillance Center		
□ Upload to FTP/Memory Card/...		

Figure 8-4 Linkage Method

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

- **Notify Surveillance Center**

  Send an exception or alarm signal to Intellio Video System software when an event occurs.

- **Send Email**

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

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

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

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

  Notes:

  - Set the FTP address and the remote FTP server first. Refer to ***Section 6.2.2 FTP Settings*** for detailed information.

  - Go to **Configuration** > **Storage** > **Schedule Settings**> **Capture** > **Capture Parameters** page, enable the event-triggered snapshot, and set the capture interval and capture number.
  - The captured image can also be uploaded to the available SD card or network disk.

- **Trigger Recording**

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

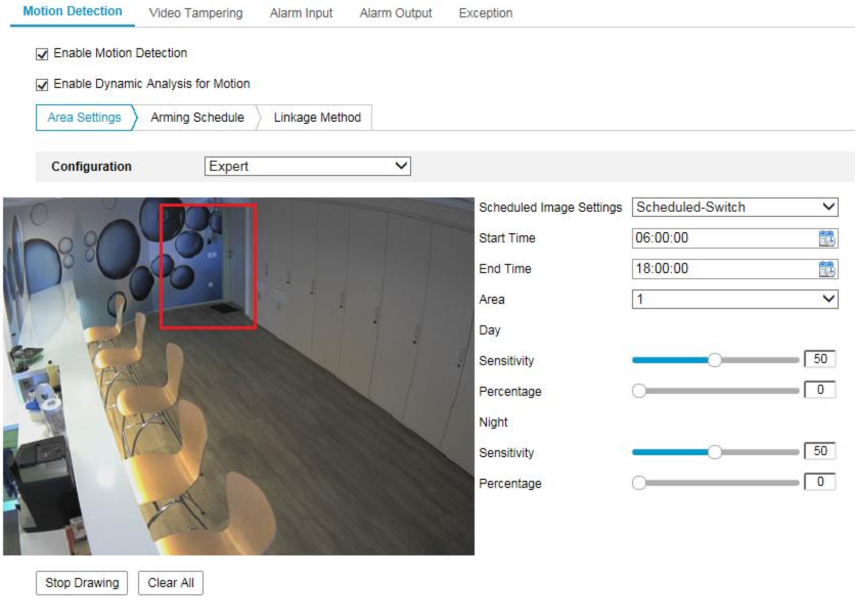
- **Trigger Alarm Output**

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

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

- **Expert Configuration**

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



☑ Enable Motion Detection

☑ Enable Dynamic Analysis for Motion

Configuration: Expert

Scheduled Image Settings: Scheduled-Switch

Start Time: 06:00:00

End Time: 18:00:00

Area: 1

Day

Sensitivity: 50

Percentage: 0

Night

Sensitivity: 50

Percentage: 0

Figure 8-5 Expert Mode of Motion Detection

- Day/Night Switch OFF

Steps:

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

- Day/Night Auto-Switch

Steps:

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

- Day/Night Scheduled-Switch

Steps:

1. Draw the detection area as in the normal configuration mode. Up to 8 areas are supported.
2. Select **Scheduled-Switch** for **Switch Day and Night Settings**.
3. Select the start time and the end time for the switch timing.
4. Select the area by clicking the area No..
5. Slide the cursor to adjust the sensitivity and proportion of object on the area for

the selected area in the daytime.

6. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area at night.
7. Set the arming schedule and linkage method as in the normal configuration mode.
8. Click **Save** to save the settings.

8.1.2 Video Tampering Alarm

Purpose:

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

Detection area for this alarm is the whole screen.

Steps:

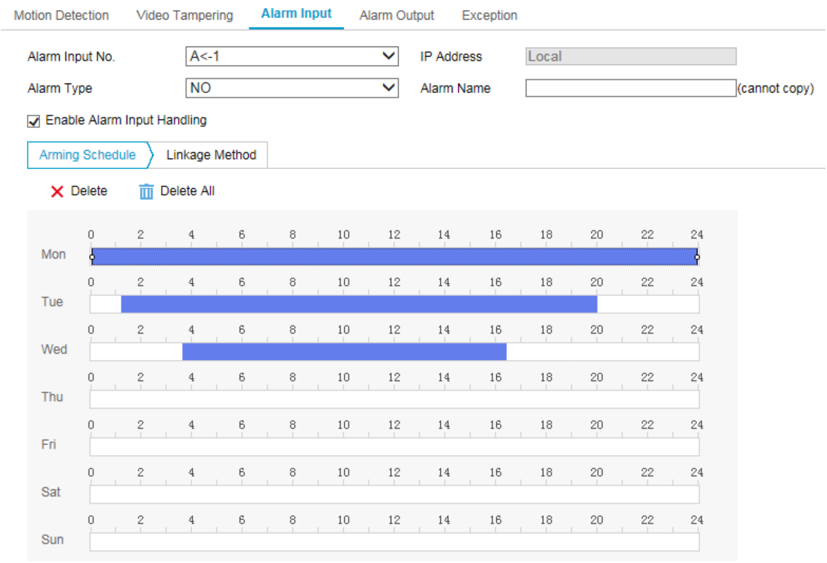
1. Enter the video tampering Settings interface, **Configuration > Event > Basic Event > Video Tampering**.
2. Check **Enable Video Tampering** checkbox to enable the video tampering detection.
3. Click **Edit** to edit the arming schedule for video tampering. The arming schedule configuration is the same as the setting of the arming schedule for motion detection. Refer to ***Task 2: Set the Arming Schedule for Motion Detection*** in ***Section 9.1.1***
4. Check the checkbox to select the linkage method taken for the video tampering. Please refer to ***Task 3: Set the Linkage Method for Motion Detection*** in ***Section 9.1.1***
5. Click **Save** to save the settings.

8.1.3 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). Edit the name to set a name for the alarm input (optional).



Alarm Input No. A<-1

Alarm Type NO

IP Address Local

Alarm Name (cannot copy)

☑ Enable Alarm Input Handling

Figure 8-6 Alarm Input Settings

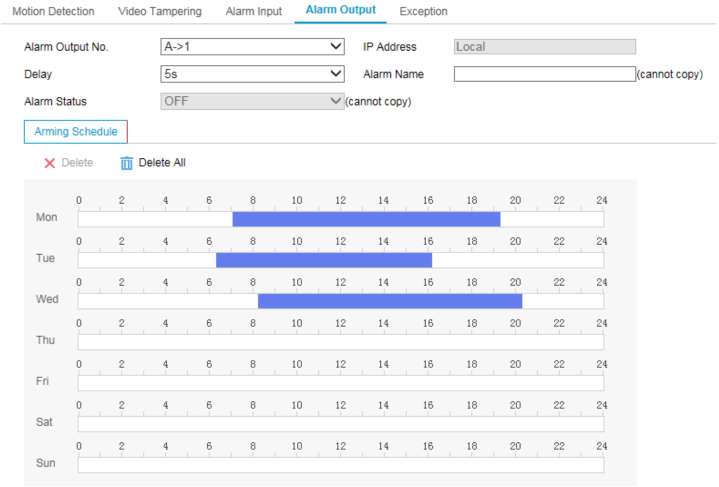
3. Click **Arming Schedule** to set the arming schedule for the alarm input. Refer to ***Task 2: Set the Arming Schedule for Motion Detection*** in ***Section 9.1.1***

4. Click **Linkage Method** and check the checkbox to select the linkage method taken for the alarm input. Refer to ***Task 3: Set the Linkage Method for Motion Detection*** in ***Section 9.1.1***

5. You can copy your settings to other alarm inputs.

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

8.1.4 Alarm Output



Alarm Output No. A->1

IP Address Local

Delay 5s

Alarm Name (cannot copy)

Alarm Status OFF (cannot copy)

Figure 8-7 Alarm Output Settings

Steps:

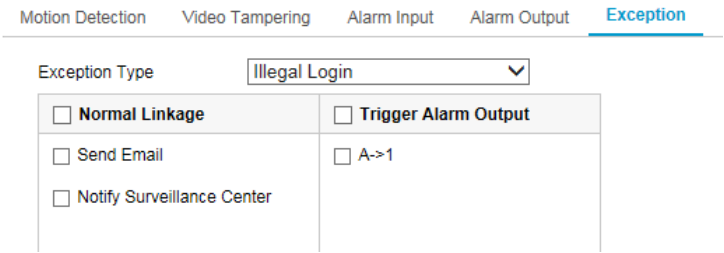
1. Enter the Alarm Output Settings interface: **Configuration> Event > Basic Event > Alarm Output**.
2. Select one alarm output channel in the **Alarm Output** drop-down list. You can also set a name for the alarm output (optional).
3. The Delay time can be set to 5sec, 10sec, 30sec, 1min, 2min, 5min, 10min or Manual. The delay time refers to the time duration that the alarm output remains in effect after alarm occurs.
4. Click **Arming Schedule** to enter the Edit Schedule Time interface. The time schedule configuration is the same as the settings of the arming schedule for motion detection Refer to ***Task 2: Set the Arming Schedule for Motion Detection*** in ***Section 9.1.1***
5. You can copy the settings to other alarm outputs.
6. Click **Save** to save the settings.

8.1.5 Handling Exception

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

Steps:

1. Enter the Exception Settings interface: **Configuration > Event > Basic Event > Exception**.
2. Check the checkbox to set the actions taken for the Exception alarm. Refer to ***Task 3: Set the Linkage Method for Motion Detection*** in ***Section 9.1.1***



Exception Type: Illegal Login

□ **Normal Linkage**	□ **Trigger Alarm Output**
□ Send Email	□ A->1
□ Notify Surveillance Center	

Figure 8-8 Exception Settings

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

8.2 Smart Events

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

8.2.6 Face Detection

Purpose:

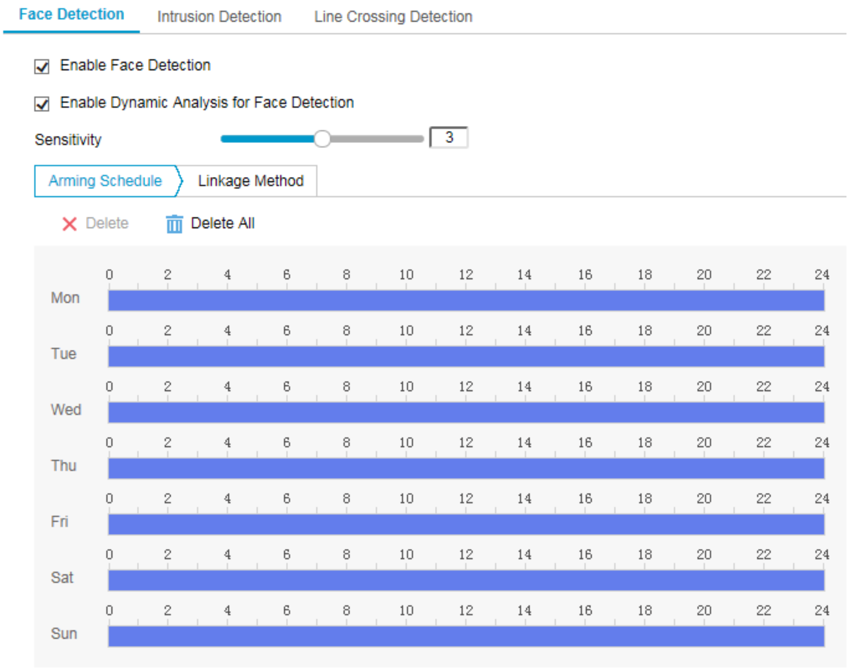
Face detection function detects the face appears in the surveillance scene, and some certain actions can be taken when the alarm is triggered.

Steps:

1. Enter the Face Detection settings interface, **Configuration > Event > Smart Event > Face Detection**.
2. Check the **Enable Face Detection** checkbox to enable the function.
3. Check the checkbox of **Enable Dynamic Analysis** for Face Detection, and then the detected face is marked with green rectangle on the live video.

Note: To mark the detected face on the live video, go to **Configuration** > **Local** to enable the **Rules**.

4. Click-and-drag the slider to set the detection sensitivity. The Sensitivity ranges from 1 to 5. The higher the value is, the more easily the face can be detected.
5. Click **Arming Schedule** to set the arming schedule. Refer to ***Task 2 Set the Arming Schedule for Motion Detection*** in ***Section 9.1.1*** for detailed steps.
6. Click **Linkage Method** to select the linkage methods for face detection. Refer to ***Task 3: Set the Linkage Method Taken for Motion Detection*** in ***Section 9.1.1***


Face Detection | Intrusion Detection | Line Crossing Detection

☑ Enable Face Detection

☑ Enable Dynamic Analysis for Face Detection

Sensitivity 3

Arming Schedule | Linkage Method

Figure 8-9 Face Detection

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

8.2.7 Intrusion Detection

Purpose:

Intrusion detection function detects people, vehicle or other objects which enter and loiter in a pre-defined virtual region, and some certain actions can be taken when the alarm is triggered.

Note: Intrusion detection function varies according to different camera models.

Steps:

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

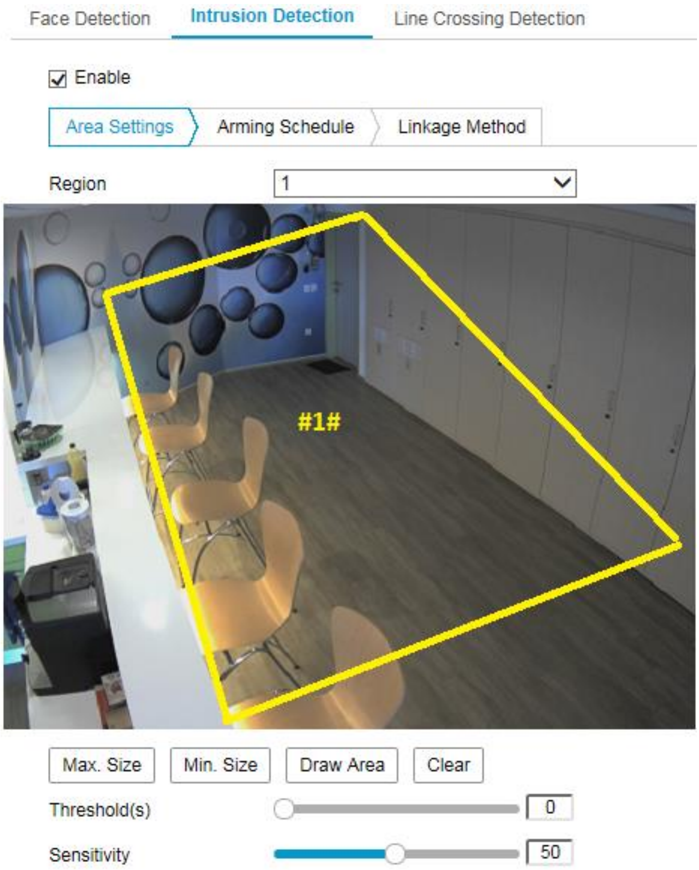


Figure 8-10 Intrusion Detection

2. Check the checkbox of **Enable** to enable the function.
3. Select a region number from the drop-down list of **Region**.

   Region: A pre-defined vertexes area on the live view image. Targets, such as, people, vehicle or other objects, who enter and loiter in the region will be detected and trigger the set alarm.
4. Click **Area Settings** tab and click **Draw Area** button to start the region drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.
6. Set the Max. Size and Min. Size for valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.

   Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.

Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.

7. Click **Stop Drawing** when finish drawing.
8. Set the time threshold for intrusion detection.

   Threshold: Range [0s-10s], the threshold for the time of the object loitering in the region. If you set the value as 0, alarm is triggered immediately after the object entering the region.
9. Drag the slider to set the sensitivity value.

   Sensitivity: Range [1-100]. Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region.

   Sensitivity = 100 – S_1/S_T*100

   S_1 stands for the target body part that goes across the pre-defined region. S_T stands for the complete target body.

   Example: if you set the value as 60, the action can be counted as an intrusion only when 40 percent body part enters the region.

   Note: The **Sensitivity** of the detection is supported by certain models. Refer to actual display for details.
10. Repeat the above steps to configure other regions. Up to 4 regions can be set. You can click the **Clear** button to clear all pre-defined regions.
11. Click **Arming Schedule** to set the arming schedule.
12. Click **Linkage Method** to select the linkage methods for intrusion detection, including Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Channel and Trigger Alarm Output.
13. Click **Save** to save the settings.

8.2.8 Line Crossing Detection

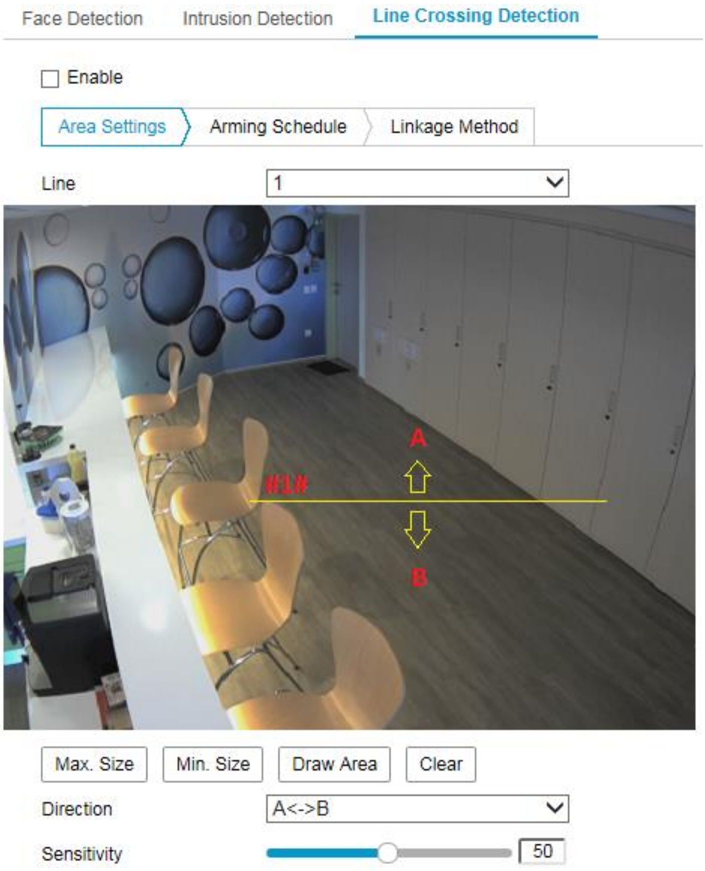
Purpose:

Line crossing detection function detects people, vehicle or other objects which cross a pre-defined virtual line, and some certain actions can be taken when the alarm is triggered.

Note: Line crossing detection function varies according to different camera models.

Steps:

1. Enter the Line Crossing Detection settings interface, **Configuration** > **Event** > **Smart Event > Line Crossing Detection**.



Face Detection | Intrusion Detection | Line Crossing Detection

□ Enable

Area Settings | Arming Schedule | Linkage Method

Line: 1

Max. Size | Min. Size | Draw Area | Clear

Direction: A<->B

Sensitivity: 50

Figure 8-11 Line Crossing Detection

2. Check the checkbox of **Enable** to enable the function.
3. Select the line from the drop-down list.
4. Click **Area Settings** tab and click **Draw Area** button, and a virtual line is displayed on the live video.
5. Drag the line, and you can locate it on the live video as desired. Click on the line, two red squares are displayed on each end, and you can click-and-drag one of the red squares to define the shape and length of the line.

6. Set the Max. Size and Min. Size for valid targets. Targets smaller or larger than the valid target size are not able to trigger detection.

   Max. Size: The maximum size of a valid target. Targets with larger sizes would not trigger detection.

   Min. Size: The minimum size of a valid target. Targets with smaller sizes would not trigger detection.

7. Select the direction for line crossing detection. And you can select the directions as A<->B, A ->B, and B->A.

   A<->B: The object going across the plane with both directions can be detected and alarms are triggered.

   A->B: Only the object crossing the configured line from the A side to the B side can be detected.

   B->A: Only the object crossing the configured line from the B side to the A side can be detected.

8. Click **Stop Drawing** when finish drawing.

9. Drag the slider to set the sensitivity value.

   Sensitivity: Range [1-100]. It stands for the percentage of the body part of an acceptable target that goes across the pre-defined line.

   Sensitivity = 100 – S_1/S_T*100

   S_1 stands for the target body part that goes across the pre-defined line. S_T stands for the complete target body.

   Example: if you set the value as 60, the action can be counted as a line crossing action only when 40 percent or more body part goes across the line.

   Note: The **Sensitivity** of the detection is supported by certain models. Refer to actual display for details.

10. Repeat the above steps to configure other lines. Up to 4 lines can be set. You can click the **Clear** button to clear all pre-defined lines.

11. Click the **Arming Schedule** to set the arming schedule.

12. Select the linkage methods for line crossing detection, including Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger

Channel and Trigger Alarm Output.

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

Chapter 9 Storage Settings

Before you start:

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

9.1 Record Schedule

Purpose:

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

Steps:

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

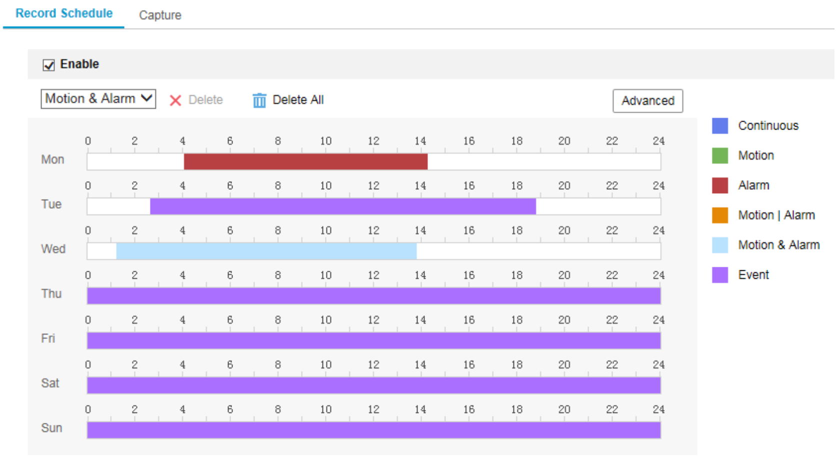
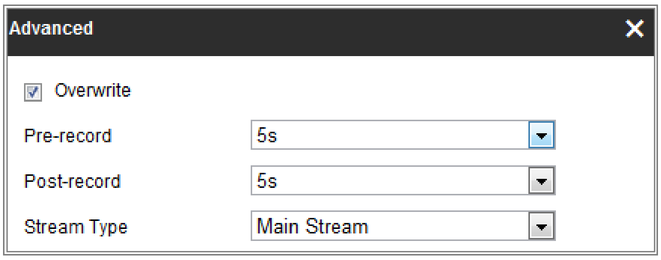


Figure 9-1 Recording Schedule Interface

2. Check the checkbox of **Enable** to enable scheduled recording.
3. Click **Advanced** to set the camera record parameters.



Advanced

☑ Overwrite

Pre-record: 5s

Post-record: 5s

Stream Type: Main Stream

Figure 9-2 Record Parameters

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

  The Pre-record time can be configured as No Pre-record, 5s, 10s, 15s, 20s, 25s, 30s or not limited.
- Post-record: The time you set to stop recording after the scheduled time or the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set as 5 seconds, the camera records until 11:00:05.

  The Post-record time can be configured as 5s, 10s, 30s, 1 min, 2 min, 5 min or 10 min.
- Stream Type: Select the stream type for recording.

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

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

- **Continuous**

  If you select **Continuous**, the video will be recorded automatically according to the time of the schedule.
- **Record Triggered by Motion Detection**

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

  Besides configuring the recording schedule, you have to set the motion detection area and check the checkbox of Trigger Channel in the Linkage Method of Motion Detection Settings interface. For detailed information, please refer to the ***Task 1: Set the Motion Detection Area*** in the ***Section 9.1.1***

Motion Detection

- **Record Triggered by Alarm**

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

  Besides configuring the recording schedule, you have to set the **Alarm Type** and check the checkbox of **Trigger Channel** in the **Linkage Method** of **Alarm Input Settings** interface. For detailed information, please refer to ***Section 9.1.3. 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. Please refer to ***Section 9.1.1 Motion Detection*** and ***9.1.3. Alarm Input*** for detailed information.

- **Record Triggered by Motion | Alarm**

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

  Besides configuring the recording schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces. Please refer to ***Section 9.1.1 Motion Detection*** and ***9.1.3. Alarm Input*** for detailed information.

- **Record Triggered by Events**

  If you select **Event**, the video will be recorded if any of the events is triggered.

  Besides configuring the recording schedule, you have to configure the event settings.

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

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

9.2 Capture Schedule

Purpose:

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

Steps:

1. Enter the Capture Settings interface: **Configuration** > **Storage** > **Storage Settings** > **Capture**.

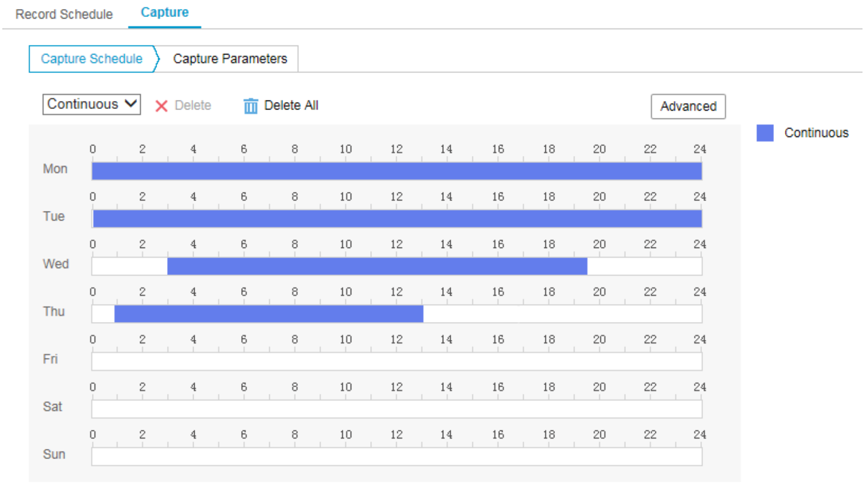


Figure 9-3 Capture Configuration

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

3. Click **Advanced** to select stream type.

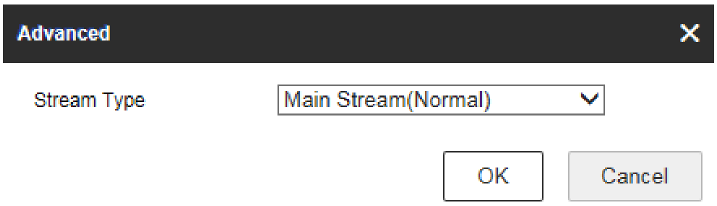


Figure 9-4 Advanced Setting of Capture Schedule

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

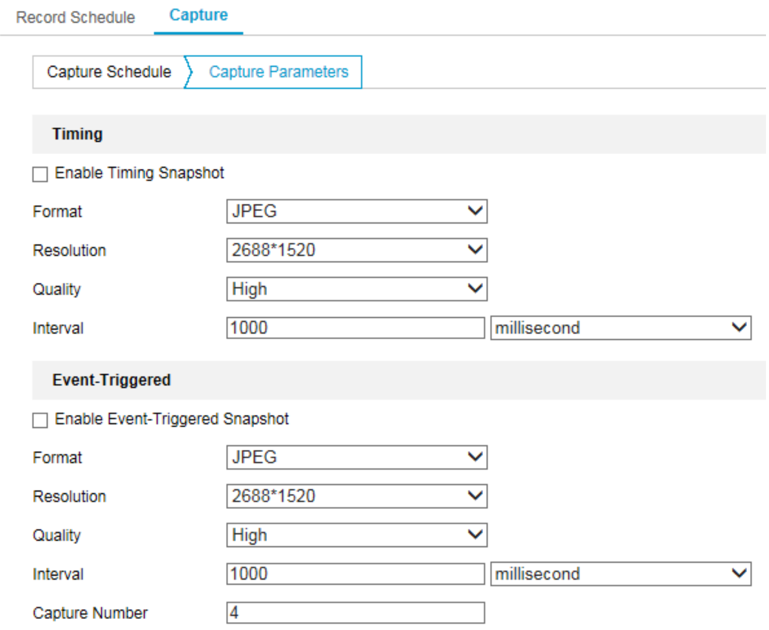
5. Go to **Capture Parameters** tab to configure the capture parameters.

   (1) Check the **Enable Timing Snapshot** checkbox to enable continuous snapshot.

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

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

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



Timing

□ Enable Timing Snapshot

Format: JPEG
Resolution: 2688*1520
Quality: High
Interval: 1000 millisecond

Event-Triggered

□ Enable Event-Triggered Snapshot

Format: JPEG
Resolution: 2688*1520
Quality: High
Interval: 1000 millisecond
Capture Number: 4

Figure 9-5 Set Capture Parameters

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

9.3 Net HDD

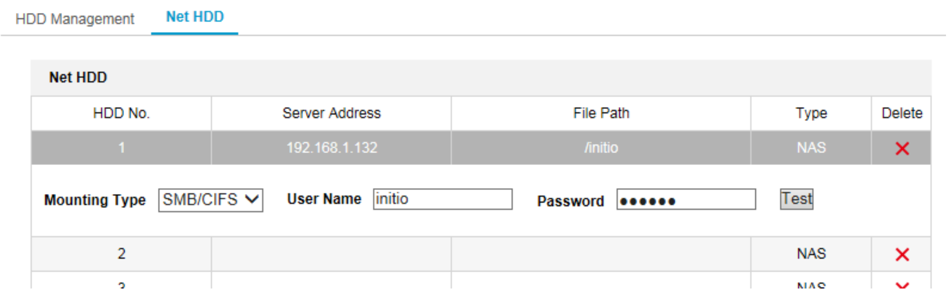
Before you start:

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

Steps:

1. Add Net HDD.

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



Net HDD

HDD No.	Server Address	File Path	Type	Delete
1	192.168.1.132	/initio	NAS	✕
2			NAS	✕

Mounting Type: SMB/CIFS
User Name: initio
Password: ●●●●●●

Figure 9-6 Add Network Disk

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

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

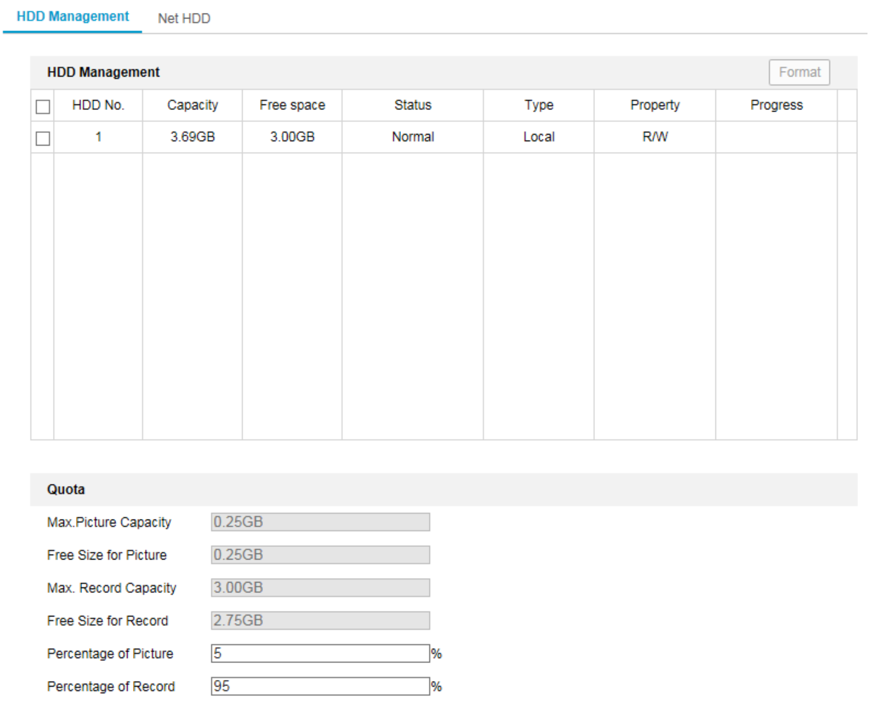
Note: Please refer to the *NAS User Manual* for creating the file path.

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

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

2. Initialize the added network disk.

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



HDD Management

Format

□	HDD No.	Capacity	Free space	Status	Type	Property	Progress
□	1	3.69GB	3.00GB	Normal	Local	R/W	

Quota

Max.Picture Capacity	0.25GB
Free Size for Picture	0.25GB
Max. Record Capacity	3.00GB
Free Size for Record	2.75GB
Percentage of Picture	5 %
Percentage of Record	95 %

Figure 9-7 Storage Management Interface

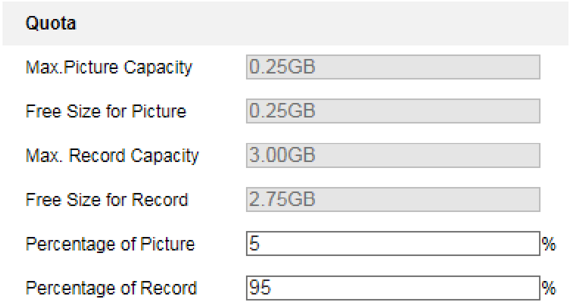
(2) If the status of the disk is **Uninitialized**, check the corresponding checkbox to select the disk and click **Format** to start initializing the disk.

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

3. Define the quota for record and pictures.

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

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



Quota

Max.Picture Capacity	0.25GB
Free Size for Picture	0.25GB
Max. Record Capacity	3.00GB
Free Size for Record	2.75GB
Percentage of Picture	5 %
Percentage of Record	95 %

Figure 9-8 Quota Settings

Note:

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

Chapter 10 Playback

Purpose:

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

Steps:

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

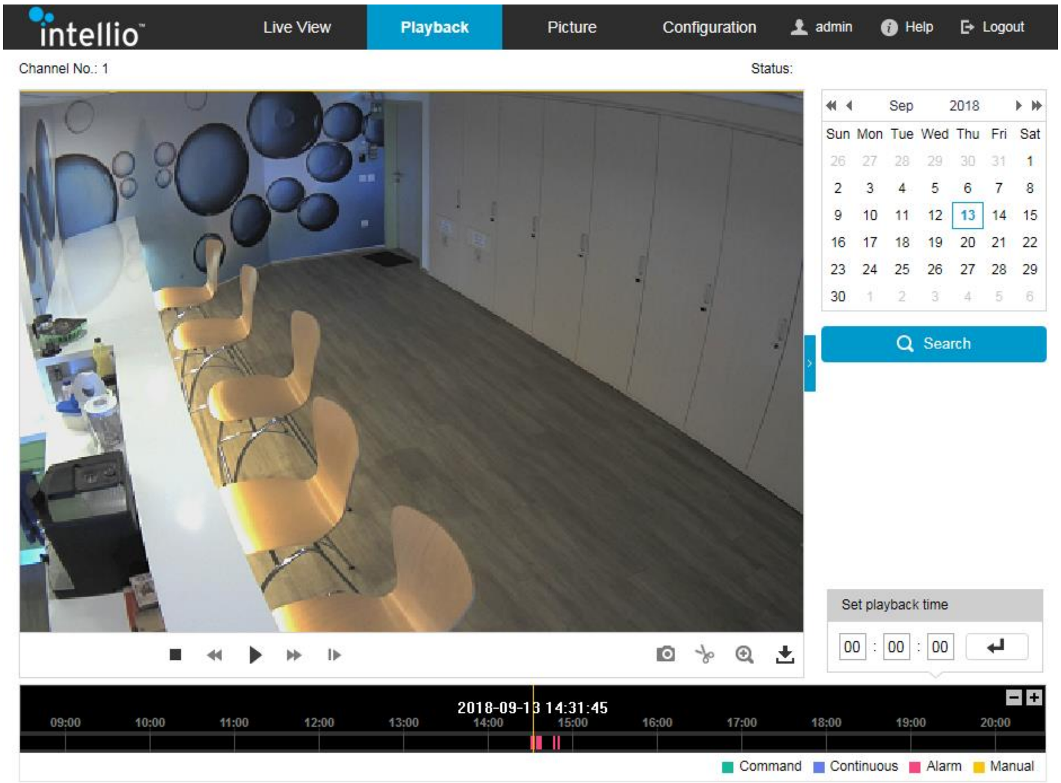


Figure 10-1 Playback Interface

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

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

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

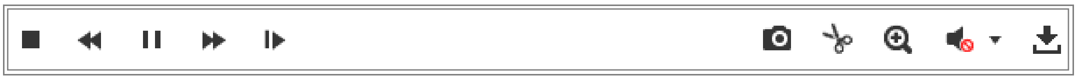


Figure 10-2 Playback Toolbar

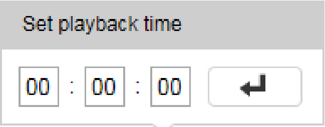
Table 10-1 Description of the buttons

Button	Operation	Button	Operation

▶	Play	📷	Capture a picture
❚❚	Pause	✂ / ✂	Start/Stop clipping video files
■	Stop	🔊 ━━○── / 🔇	Audio on and adjust volume/Mute
⏪	Speed down	⬇	Download
⏩	Speed up	❙▶	Playback by frame
🔍 / 🔍	Enable/Disable digital zoom		

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

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



Set playback time

00 : 00 : 00 ↵

Figure 10-3 Set Playback Time

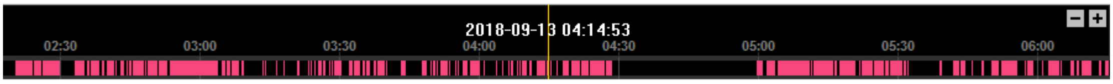
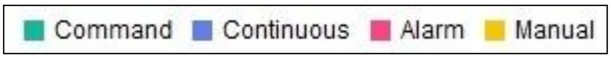


Figure 10-4 Progress Bar

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



🟩 Command 🟦 Continuous 🟥 Alarm 🟨 Manual

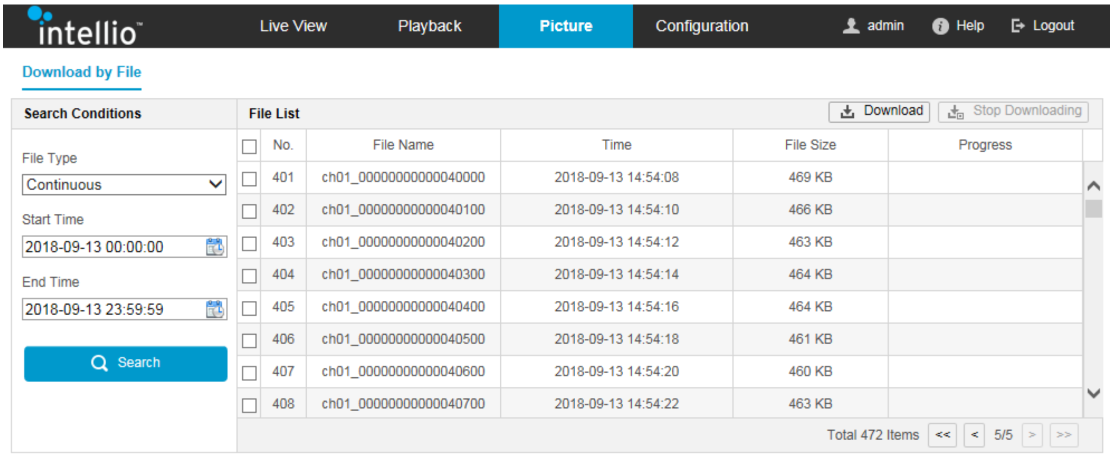
Figure 10-5 Video Types

Chapter 11 Picture

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

Notes:

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



File Type: Continuous

Start Time: 2018-09-13 00:00:00

End Time: 2018-09-13 23:59:59

☐	No.	File Name	Time	File Size	Progress
☐	401	ch01_0000000000040000	2018-09-13 14:54:08	469 KB	
☐	402	ch01_0000000000040100	2018-09-13 14:54:10	466 KB	
☐	403	ch01_0000000000040200	2018-09-13 14:54:12	463 KB	
☐	404	ch01_0000000000040300	2018-09-13 14:54:14	464 KB	
☐	405	ch01_0000000000040400	2018-09-13 14:54:16	464 KB	
☐	406	ch01_0000000000040500	2018-09-13 14:54:18	461 KB	
☐	407	ch01_0000000000040600	2018-09-13 14:54:20	460 KB	
☐	408	ch01_0000000000040700	2018-09-13 14:54:22	463 KB	

Total 472 Items << < 5/5 > >>

Figure 11-1 Picture Search Interface

Steps:

1. Select the file type from the dropdown list. Continuous, Motion, Alarm, Motion | Alarm, Motion & Alarm, Line Crossing, Intrusion Detection, and Scene Change Detection are selectable.
2. Select the start time and end time.
3. Click **Search** to search the matched pictures.
4. Check the checkbox of the pictures and then click **Download** to download the selected pictures.

Note:

Up to 4000 pictures can be displayed at one time.